Release Notes for Cisco IronPort AsyncOS 7.2.3 for the Security Management Appliance

Published: May 14, 2012

Contents

This document contains information for this release of AsyncOS for Security Management. This document includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in Cisco IronPort AsyncOS 7.2 for Security Management

New features in this release of AsyncOS for Security Management include:

Table 1 New Features for Async OS 7.2 for Security Management

Feature	Description
GUI Enhancements	
Web Reporting and Web Tracking pages	The Security Management appliance now has several new interactive web reporting pages that support web reporting and tracking. New pages include: • Users page • Web Sites page • URL Categories page • Application Visibility page • Anti-Malware page • Client Malware Risk page • Web Reputation Filter page • L4 Traffic Monitor page • Reports by User Location page • Web Tracking page • System Capacity page • Data Availability page • Scheduled Reports page • Archived Reports page To access any of these pages on the Security Management appliance, choose **Web > Reporting**.

Table 1 New Features for Async OS 7.2 for Security Management

Feature	Description
Web Status page	The Security Management appliance now provides a Web Status page that allows you to see the status of your Web Security appliances that are being managed by the Security Management appliance. To access the Web Status page, choose **Web > Utilities > Web Appliance Status**.
Interactive Columns	On the Security Management appliance, you can now click the column headings on each Report page to sort the data according to the values in that column. To access any of the Web Reporting pages, choose **Web > Reporting**.
General Features	
Web Reporting and Web Tracking	The Security Management appliance now supports web reporting and web tracking in AsyncOS 7.1 for Web Security appliances. This feature provides a centralized view of web traffic across multiple Web Security appliances. The web reporting and tracking feature gives you a broad view of what is happening on your Web Security appliances and allows you to refine reports down to the transaction level. The web reporting feature also allows you to generate reports (scheduled or otherwise) that provide information at an organizational, group, and individual level. This gives you an all-in-one support system for evaluating functionality from a single WSA appliance. Web tracking allows you to track the workload of Web Security appliances on the Security Management appliance. The Web tracking page allows you to see basic information such as time ranges, and UserID and Client IP addresses, but also includes information such as the type of web traffic that is being handled by the Web Security appliance, tracking certain types of URLs, tracking how much bandwidth that each connection is taking up, or tracking a specific user's web usage. To enable centralized web reporting and tracking on the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

Table 1 New Features for Async OS 7.2 for Security Management

Feature	Description
Scheduled and Archived Reports	The Security Management appliance allows you to generate scheduled reports from the data coming from your Web Security appliance. Scheduled reports can be configured to include data for the previous day, previous seven days, previous month, previous calendar day (up to 250), previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months). The Security Management appliance can also archive and store reports that have been generated. The appliance stores up to 12 instances of each scheduled report (up to 1000 reports). Archived reports are stored in the **/periodic_reports** directory on the appliance. Additionally, you can now generate on-demand data displays for each report type using the Generate Now option on the Archived Reports page. Scheduled or archived report pages can be accessed on the Security Management appliance at **Web > Reporting > Scheduled Reports** or **Web > Reporting > Archived Reports**.
Custom Time Ranges	The Security Management appliance allows you to define a customized range for reporting data. The customized time range menu can be accessed from the time range drop-down list on most web reporting pages.
User Roles	The Security Management appliance now allows you to assign specific user roles so that an administrator can define who has permission for various access policies and custom categories. To assign user roles, see **Management Appliance > System Administration > User Roles.**
Anonymized User Names on Reporting pages	You can now configure web reporting to anonymize user names and roles on all web reports.
Active Sessions	You can now view all active web and email appliance sessions from the Security Management appliance. This allows you to see who is logged in, for how long, and user information from one page. To view all active sessions, see **Options > Active Sessions**.

Table 1 New Features for Async OS 7.2 for Security Management

Feature	Description
Backup and Restore Enhancements	The Security Management appliance allows you to copy its active dataset from the 'source' appliance to a 'target' Security Management appliance with minimum disruption on the originating 'source' Security Management appliance. You can also cancel, restore, or schedule a periodic or instant backup at a time of your choosing. The following command was introduced to support the new back up and restore enhancements: **backupconfig**.
Disaster Recovery	You can now set up your environment for disaster recovery if Security Management appliances on your system fail.
Configuration Master 7.1	New support for Configuration Master 7.1 enables you to configure authentication identities, SaaS policies, define web policies including decryption policies, routing policies, access policies, defined time ranges, and overall bandwidth limits. Also included in this Configuration Master are the following: AVC, Sophos, credential encryption, Mobile User Security (MUS). You can also define IronPort data security policies, and external DLP policies; bypass the web proxy; and create custom URL categories including extended URL policies. To enable the new Configuration Master 7.1, choose **Management Appliance > Centralized Services > Centralized Configuration Manager**, then go to **Web > Utilities > Configuration Masters**.
Publishing a Configuration Master Enhancement	A new CLI command, **publishconfig**, has been introduced that allows you to publish a Configuration Master for a specified configuration. The command syntax is **publishconfig config_master** [*job_name*] [*host_list* | *host_ip*].
Printable PDF Reports Enhancements	Each report page on the Security Management appliance has a Printable PDF link at the top-right of the page. Click this link to generate a printer-friendly formatted PDF version of any report page. Additionally, you can export graphs and other data to comma-separated values (CSV) format by clicking the Export link. Most reports allow scheduling of CSV. However, you cannot schedule a CSV of extended reports. To access any of the Web Reporting pages, choose **Web > Reporting**.

Upgrade Paths

Qualified upgrade paths to Cisco IronPort AsyncOS 7.2.3-039 for Security Management are:

- 6.7.3-229
- 6.7.6-076
- 6.7.7-202
- 6.7.8-009
- 7.2.0-390
- 7.2.1-036
- 7.2.2-028
- 7.2.2-106
- 7.2.3-038

SMA Compatibility Matrix

This section describes the compatibility between the Security Management appliance and various releases of the Email Security appliance and the Web Security appliance.

Table 1-2 AsyncOS 7.2 for Security Management Compatibility with AsyncOS for Email

Version	Reporting	Tracking	SafeList/ BlockedList	ISQ
ESA 6.0	No Support	No Support	No Support	Support
ESA 6.3	No Support	No Support	No Support	Support
ESA 6.4	Support	Support	Support	Support
ESA 6.5	Support	Support	Support	Support
ESA 6.6	Feature not Available	Feature not Available	Feature not Available	Feature not Available

Version	Reporting	Tracking	SafeList/ BlockedList	ISQ
ESA 7.0	Support	Support	Support	Support
ESA 7.1	Support	Support	Support	Support

Table 1-3 AsyncOS 7.2 for Security Management Compatibility with AsyncOS for Web Security

Version	Centralized Reporting	Tracking	Publish a Configuration Master to Web Security appliances	Advanced File Publish to Web Security appliances
WSA 5.7	Feature not Available	Feature not Available	Supported by 5.7 Configuration Master	Configuration file version must match target WSA version
WSA 6.3	Feature not Available	Feature not Available	Supported by 5.7 and 6.3 Configuration Master. 6.3 Configuration Master can publish only to WSAs running AsyncOS 6.3.8.	Configuration file version must match target WSA version to three digits of specificity (for example, 6.3.3)
WSA 7.0	Feature not Available	Feature not Available	Supported by 6.3 Configuration Master	Configuration file version must match target WSA version
WSA 7.1	Support	Support	Supported by 6.3 and 7.1 Configuration Master 7.1 Configuration Master can publish only to WSAs running AsyncOS 7.1.4-053.	Configuration file version must match target WSA version exactly, including the build number (for example, 7.1.4-052). See also Known Issue number 78045, page 11.

Table 1-4 (For Deployments with WSAs Only) Compatibility for Configuration Master Imports

Populate settings for Configuration Master version:	Populate settings by copying existing Configuration Master version:	Populate settings by importing a configuration file from Web Security appliance version:
Configuration Master 5.7	Not Supported	Configuration file from WSA 5.7 only
Configuration Master 6.3	5.7 Configuration Master	Configuration file from WSA 6.3.8 only
Configuration Master 7.1	6.3 Configuration Master	Configuration file from WSA 7.1.4-053 only

Installation Notes

Upgrade Web Security Appliances to AsyncOS 7.1.4-053

When you upgrade your Security Management appliance to this release, you must also upgrade your managed Web Security appliances to AsyncOS 7.1.4-053. Earlier releases of AsyncOS 7.1 are not compatible with this release.

Disk Space

This issue applies only to M160 hardware.

AsyncOS for Security Management releases prior to this release had more disk space available for data storage than is available in this release, as detailed in Table 5:

Table 5 Total Maximum Disk Space on M160, in GB

Release	Total Maximum Disk Space
AsyncOS 6.5.x	195
AsyncOS 6.7.x	186
AsyncOS 7.2.x	180

When upgrading to AsyncOS 7.x, if your M160 has more than 180 GB of existing data, any data above this amount will be lost upon upgrade, starting with the oldest data first.

Configuration File Backup

Before upgrading, save the XML configuration file off the Security Management appliance.

Upgrading to This Release

Warning **If you are upgrading from an AsyncOS release earlier than 7.2.1 and you have M160 hardware:**
You may need to upgrade the hard drive firmware before you upgrade AsyncOS. To verify whether or not your M160 requires the firmware upgrade, run the upgrade command at the command line prompt. If the M160 requires the firmware upgrade, "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" will be listed as an upgrade option. If listed, run the firmware upgrade, and then upgrade AsyncOS.
See the *Cisco IronPort Hard Driver Firmware Upgrade for C160, S160, and M160 Appliances Release Notes* on Cisco.com for more information.

Step 1 On the Security Management appliance, click **System Administration > Configuration File**.

Step 2 Save the XML configuration file off the Security Management appliance.

Step 3 If you are using the Safelist/Blocklist feature, export the list off the appliance.

Step 4 On the Security Management appliance, click **System Administration > System Upgrade.**

Step 5 Click **Available Upgrades**.

The page displays a list of available AsyncOS for Security Management upgrade versions.

Step 6 Click **Begin Upgrade** to start the upgrade process.

Answer the questions as they appear.

Step 7 Click **Reboot Now** to reboot the Security Management appliance.

Documentation Updates

Requirements for Backups

In addition to any requirements already stated in the user guide, note the following requirement:

The source and target Security Management appliances must be able to communicate using SSH. Therefore:

- Port 22 must be open on both appliances. By default, this port is opened when you run the System Setup Wizard.
- The Domain Name Server (DNS) must be able to resolve the host names of both appliances using both A records and PTR records.

Known Issues

The following list describes the known issues in this release of AsyncOS for Security Management.

Security Management Appliance Issues

Table 6 describes the known issues for the Security Management appliance for this release.

Table 6 Security Management Appliance Known Issues for This Release

Defect ID	Description
85389	**Error in some situations when importing 6.3 configuration to initialize a 6.3 Configuration Master** If you receive the error "Configuration conflict detected!" when trying to import a 6.3 configuration to initialize a Configuration Master, try the following workaround: Abandon the changes, then try importing the configuration again.
78045	**Compatibility issues with configuration files from AsyncOS 7.1.2 for Web Security** • Advanced file publish cannot be used to publish a configuration file from AsyncOS 7.1.2 for Web Security to Web Security appliances running AsyncOS 7.1.0 or 7.1.1. • For an additional impact of this issue that affects only AsyncOS 7.2.0 and 7.2.1, see the release notes for those versions at http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.
74487	**Identities on Web Security appliance are erroneously set to "No Surrogate" when Credential Encryption is disabled on the Security Management appliance** When the Web Security appliance is enabled for Credential Encryption, and the configuration master is configured to disable Credential Encryption, Identities on Web Security appliance are erroneously set to "No Surrogate" after publishing the configuration master. Workaround: After publishing the configuration master, edit each Identity that uses authentication and change the surrogate type setting as necessary. Submit and commit your changes.

Table 6 Security Management Appliance Known Issues for This Release (continued)

Defect ID	Description
74943	**Some reports show perceived data loss after upgrading from a previous build in version 7.2.0 in some cases** When you upgrade from a previous build of version 7.2.0 and view a report for an email reporting group that shows monthly data or more, the report might show less data compared to viewing the same report in the previous 7.2.0 build. This issue occurs as a result of the fix for Defect ID 74819 that rolls up hourly data into daily data in the reporting database. If the oldest hourly data begins to be deleted due to the configured report settings, that data will not be included in the daily report data and therefore will not appear in reports based on month (and more) data. Over time, depending on the appliance model and configured reporting settings, there will be no more perceived data loss.
37034	**The Items per Page search is not functioning properly.** When you select the number of items per page to be displayed in a report on the Security Management appliance, the incorrect number of items are displayed.
47358	**The ICCM pending tasks list is not updated if the Web Security appliance has been removed from the system.** If you remove a Web Security appliance, the ICCM task list is not updated on the Security Management appliance.
54664	**The Security Management appliance and the Web Security appliance send two different groups LDAP queries even though they are configured exactly the same.** The Security Management appliance and the Web Security appliance send two different groups LDAP queries, even though they are configured exactly the same. Additionally, the Security Management appliance is only including the user attribute value, not the entire user domain name.
56026	**The left angle bracket is not interpreted properly when creating a custom DLP policy name.** When creating a custom DLP policy name on the Security Management appliance, the left angle bracket is not interpreted properly. This results in the details on the Message tracking page not being displayed properly on the printed PDF report.

Table 6 Security Management Appliance Known Issues for This Release (continued)

Defect ID	Description
67839	**After upgrading the Email Security appliance to 7.1.0-058, the user still gets warnings from Security Management appliance running 6.7.6-070.** After upgrading the Email Security appliance server to 7.1.0-058, the user still gets warnings from Security Management appliance running 6.7.6-070. Additionally, Email Centralized Reporting is receiving data that cannot be processed by the Security Management appliance.
69601	**An extra column appears on overview report when switching to Daylight Savings Time (DST).** An extra column appears on the **Web > Overview** page when you change the time to Daylight Savings Time (DST).
69895	**Web reporting creates an erroneous URL categories group ' - ' if the Acceptable Use Controls is disabled.** When using the Web reporting feature, an erroneous URL category ' - ' is created in the URL Categories Matched table when you have disabled the Acceptable Use Controls.
70038	**The report data exceeds the table cell in PDF format when all columns are selected for displaying in interactive report.** If you click on the Printable PDF link from the **Web > Reporting > Users** page, the report data exceeds the table cell in PDF report, when all available columns are selected to be displayed.
70925	**Disaster Recovery Feature needs a progress meter with ETA to enable tracking of how much time it will take.** The Disaster Recovery feature does not have a progress bar to indicate how much of the backup has been completed. Additionally, it does not have a time estimation to indicate how much time it will take to complete this action.
71470	**The loadconfig command fails if the hostname specified in SaaS Policy can not be resolved.** The **loadconfig** command fails if hostname specified in SaaS Application Authentication Policy can not be resolved and throws the following error: `Error - Configuration File was not loaded. Parse Error on element "prox_acl_sp_group_acs_location"`

Table 6 Security Management Appliance Known Issues for This Release (continued)

Defect ID	Description
71565	**Disk allocation does not prevent the user from importing a configuration file with larger Disk Allocation values than possible.** When you import a configuration file from a system running on a different hardware platform, there is a possibility to incorrectly configure the disk management so that the Security Management appliance is configured to use more space than is available.
71694	**The secondaryconfig command needs to be enabled on both the Security Management appliance and the Web Security appliance.** The **secondaryconfig** command needs to be enabled on both the Security Management appliance and the Web Security appliance.
71720	**The Master Configuration with different Auth Realm in Identities is published to WSA without any warning.** A Master configuration file that has different authentications realms set in the Identity policies, is published to the Web Security appliance without any warning.
72050	**Loading URL Category Details report can be very slow the first time it is loaded.** Loading URL Category Details report can be very slow the first time it is loaded onto the Security Management appliance.
72071	**User Reports shows more than 24 hours in time spent when using day as time range.** On the Security Management appliance, the User reports page is showing more than 24 hours in time spent when using day as time range selection.
72332	**The Filter by User-Requested Transactions option on Web Tracking report page does not work as expected.** The **Filter by User-Requested Transactions** option on **Web > Web Tracking** report page does not work as expected.
72432	**The Web Tracking Printable PDF report does not contain Related Transactions information.** When a user clicks on the Printable PDF link from the **Web > Reporting > Web Tracking** page, the report does not contain the Related Transactions information.

Table 6 Security Management Appliance Known Issues for This Release (continued)

Defect ID	Description
73133	**Domain-Based executive summary report counts stopped by reputation filtering incorrect.** The Stopped by Reputation Filtering results in the Domain-Based Executive Summary report on the Security Management appliance cannot be seen. **Workaround**: To see Stopped by Reputation Filtering results in your Domain-Based Executive Summary report on the Security Management appliance, you must have **hat_reject_info** enabled on both the Email Security appliance and the Security Management appliance. To enable the **hat_reject_info** on the Security Management appliance, run the **reportingconfig > domain > hat_reject_info** command.

Email Security Appliance Issues

There are no known issues for the Email Security appliance for this release.

Note For issues that identically affect both the Email Security appliance and the Security Management appliance, such as issues with reports, see the Release Notes for the Email Security appliance.

Web Security Appliance Issues

Table 7 describes the known issues for the Web Security appliance for this release.

Note Only Web Security appliance issues which uniquely affect the Security Management appliance are listed here. For full coverage of issues related to the Web Security appliance, please see the AsyncOS for Web Security release notes.

Table 7 Web Security Appliance Known Issues for 7.2

Defect ID	Description
71942	**Logging data is erroneously recorded on Web Security appliance after enabling Centralized Reporting** When you enable Centralized Reporting on the Web Security appliance, AsyncOS for Web records information in the Web Security appliance logging database as well as collects information for centralized reporting on the Security Management appliance. **Workaround**: After enabling Centralized Reporting on the Web Security appliance, reboot the Web Security appliance.
72332	**Filter by User-Requested Transactions option on the Web Tracking report page erroneously includes extra transactions.** The Filter by User-Requested Transactions option on the Web Tracking report page erroneously includes transactions that were not requested by the user. **Workaround**: Ignore the results in the Filter by User-Requested Transactions option.
72637	**Cannot upgrade from version 6.3 using Internet Explorer 6.** When you use Internet Explorer 6 to access the appliance to upgrade AsyncOS for Web from version 6.3, the System Upgrade page does not display the Continue button which prevents the upgrade from processing completely. Workaround: Use a different browser or browser version to access the web interface for upgrading.

Resolved Issues

The following list describes the resolved issues in this release of AsyncOS for Security Management:

- Security Management Appliance Issues
- Email Security Appliance Issues
- Web Security Appliance Issues

Security Management Appliance Issues

Table 8 describes the resolved issues for the Security Management appliance for AsyncOS 7.2 releases.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
Fixed in 7.2.3	
85865	**Fixed: Firefox user agents disappear from identity and policy membership after loading or publishing a configuration file** This issue has now been fixed. You must also upgrade managed Web Security appliances running AsyncOS 7.1 to build 7.1.4-053.
79127	**Fixed: Appliance can run out of swap memory and lock up** Publishing configurations to Web Security appliances would cumulatively trigger this issue over time. It has now been fixed.
78421	**Fixed: Appliance stops retaining new web tracking data and no alert is sent** This situation was not common and the issue has now been fixed.
80678	**Fixed: Infrequent race condition could lock up Security Management appliance** When this issue occurred, the Security Management appliance stopped communicating with associated Email and Web Security appliances, and stopped responding to input via GUI and CLI.
76787	**Fixed: SMA stops retaining new reporting data** If you see a stream of alerts stating “year is out of range” this may mean that your system has encountered the root cause leading to this problem. This situation was not common and the issue has now been fixed.
73469	**Fixed: Appliance sends out a non-applicable critical alert email in some cases** Previously, the appliance sent out a non-applicable critical alert email with the following message: `Counter group “MAIL_SYSTEM_CAPACITY” does not exist.` This no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
67828	**Fixed: Custom Log Entries are not appearing in Message Tracking** Previously, custom log entries created as a message filter or content filter action were not appearing on the Message Details page in Message Tracking on the SMA. Custom log entries now appear as expected.
82592 82692	**Fixed: CPU usage may unexpectedly run at maximum capacity** Previously, in rare circumstances, SNMP could drive CPU usage to 100%. This problem has now been fixed.
76789	**Fixed: After upgrading, both Feature Keys settings become enabled** Previously, both the "Automatically Check For New Feature Keys" and "Automatically Apply Downloaded Feature Keys" settings under Management Appliance > System Administration > Feature Keys Settings were enabled after upgrade. Now, these settings do not change after upgrade.
77726	**Fixed: Web reporting in the GUI may become sluggish** Previously, response to any action performed in the web reporting pages could become very slow until appliance reboot. This issue has been fixed.
77926	**Fixed: Publishing or copying Configuration Master 6.3 may change existing Access Policies** Previously, in the 'Web Reputation and Anti-Malware Filtering' settings for Access Policies, the action for the 'Other Malware' and 'Unscannable' categories changed from Block to Monitor when you did either of the following: • Published Configuration Master 6.3 to WSA 7.1.x . • Copied Configuration Master 6.3 to Configuration Master 7.1 These actions no longer change existing Access Policies.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
Fixed in 7.2.2	
79474	**Fixed: URLs are shown incorrectly on the Web Tracking page if data was generated on Web Security appliance 7.1.2 or later** For data from earlier Web Security appliances, URLs in simple view appear in Web Tracking results in the Security Management appliance as "http%3A". URLs in detail view precede the URL with "http%3A". If the Web Security appliance is running AsyncOS 7.1.2 or later, the Security Management appliance must be running AsyncOS 7.2.2 or later
77616	**Fixed: (Problem applies to M160, M660, M670, M1060, M1070 hardware only) Changing disk space quotas requires lowering spam quarantine allocation** For some hardware models, the maximum disk space allocation for spam quarantine in AsyncOS 6.7 was larger than the maximum allocation in AsyncOS 7.2.0 and 7.2.1. If you had more spam quarantine data at time of upgrade than the new maximum allowed, and you changed your disk space allocations after upgrade, you had to lower the quota for spam quarantine to the new maximum, resulting in loss of spam quarantine data over the new maximum amount. Starting in Release 7.2.2, this problem will not occur because the maximum disk space allocations for Spam Quarantine now match those of previous releases for all hardware models. Maximum spam quarantine allocations are: • M160: 70GB • M660 and M670: 150 GB • M1060 and M1070: 265 GB
71976	**Fixed: (M160 and M170 Hardware only) Disk fails with RAID alert.** Software RAID robustness has been improved, making these disk failures less likely to occur.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
Fixed in 7.2.1	
72120	**Fixed: System Status page does not update all data when reporting data is fetched from the Web Security appliance** Previously, the Security Appliance Data Transfer Status section on the Management Appliance > Centralized Services > System Status page did not update the Status column when reporting data was fetched from the Web Security appliance. This behavior no longer occurs.
72773	**Fixed: Security Management appliance does not show "Define Members by User Location" option in the configuration master Identities in some cases** Previously, the Security Management appliance did not show the "Define Members by User Location" option in the configuration master Identities when the configuration master was derived from a Web Security appliance that had Secure Mobility enabled and was configured to define remote users by integrating with a Cisco ASA. This behavior no longer occurs.
74482	**Fixed: CLI can erroneously be used to access the machine-level prompt** Previously, the CLI could erroneously be used to access the machine-level prompt. This no longer occurs.
74819	**Fixed: Monthly Group Reports Error Out** Previously, an application fault occurred if you tried to run a monthly report for an Email Appliance Reporting Group on your Security Management appliance. The appliance did not display any reporting data. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
55858, 70001, 70680	**Fixed: When accessing the Security Management appliance using clientless VPN, several reporting tables are not loading and this generates an application fault.** Previously, when you accessed the Security Management appliance using clientless VPN connection, several web reporting tables did not load, or reported the following: `"No data was found in the selected time range".` Additionally, attempting to make configuration changes on the Web Security appliance or Security Management appliance while using AnyConnect / SSL VPN caused an application fault. This behavior no longer occurs.
56082	**Fixed: The Security Management appliance do not do periodic checks.** Previously, the Security Management appliance was supposed to perform periodic checks for new feature keys in a variety of situations, but the checks did not happen. This behavior no longer occurs.
66838	**Fixed: Reports displaying results of Outbound Malware Scanning policies may have inaccurate itemized malware counts and totals.** Previously, the reports that displayed results for the Outbound Malware Scanning policies had inaccurate malware counts and totals. Additionally, Malware Threat and Malware Category results might have shown up with high counts as **Unknown** or **Unnamed** in Malware reports. This behavior no longer occurs.
67816	**Fixed: Upload fails when the web site uses NTLM authentication.** Previously, an upload may have failed when the web site used NTLM authentication. This behavior no longer occurs.
68022	**Fixed: The Web Security appliance displays 'Managed by:' even after it is deleted from Security Management appliance.** Previously, after a Web Security appliance was deleted on the Security Management appliance, a message appeared on the GUI of the Web Security appliance stating that it was still being centrally managed by the Security Management appliance. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
68017	**Fixed: The items that are displayed are not always carried over when creating Printable PDF reports.** Previously, the items that you select to be displayed on the Printable PDF reports are not always displayed. This behavior no longer occurs.
69002	**Fixed: Host name is not used on Web Tracking page for transaction details; the serial number is used instead.** Previously, when using **Web > Web Tracking** for transaction details, the serial number was being used when the hostname should have been used. This behavior no longer occurs.
69154	**Fixed: Displaying reports on the Security Management appliance using 'Year' as the Time Range value is slow.** Previously, the Security Management appliance ran slowly when you displayed reports using a time range value of a 'Year' from either the **Email > Reporting**, or **Web > Reporting** menu. This behavior no longer occurs.
69372	**Fixed: Full URL is displayed for the Printable PDF URL.** Previously, the Web Tracking page showed the full URL path in the **Transaction** column when search results were displayed. This behavior no longer occurs.
69383	**Fixed: The Configuration Master to Publish drop-down list for is incorrect.** Previously, on the **Web > Utilities > Configuration Masters** page, the 'Configuration Master to Publish' drop-down list displayed the Configuration Masters in the incorrect order. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
69391	**Fixed: Archived and scheduled reports ignore anonymized configuration for user roles.** Previously, when you configured the Usernames in your reports to be anonymous from the **Management Appliance > Centralized Services > Web > Centralized Reporting > Edit Settings page**, the reports still showed the real user names. This behavior no longer occurs.

69419	**Fixed: Apple Mac AnyConnect - secure gateway rejected connection,**
	
	Previously, when you installed AnyConnect on a Macintosh, the secure gateway rejects the connection attempt due to network connectivity issues between the local computer and the secure gateway. The following message is received from the secure gateway:
	
	`Other error`
	`Second Error message:`
	`AnyConnect was not able to establish a connection to the specified secure gateway. Please try connecting again.`
	
	This behavior no longer occurs.

69420	**Fixed: Web Security appliance data is not exported to a CSV file from several reports.** Previously, the CSV files did not contain Web Security appliance data when exporting result from the following reports: URL Category Detail, Users, Web Sites Detail, Application Detail, Application Type Detail, Client Malware Risk, Web Proxy, Malware Threat Detail, Mobile User Security. This behavior no longer occurs.
69436	**Fixed: The warning about a mismatch between the Security Management appliance and the Web Security appliance should not be shown before you perform the Advanced File Publish operation.** Previously, the Security Management Appliance displayed a warning when you disabled some services on the Web Security Appliance, and still had those same services enabled on the Security Management Appliance. This warning could have appeared when you ran the Configuration Master publish operation and did not appear when you ran the Advanced File Publish operation. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
69402	**Fixed: Custom URL categories that are created on the Web Security appliance are not shown on the Security Management appliance.** Previously, if a user created custom URL Categories on the Web Security appliance, the custom URL categories were not shown in the **Web > Reporting > Web Tracking > Advanced** page on the Security Management Appliance. This behavior no longer occurs.
69546	**Fixed: When using Web > Web Tracking page, if the Transaction type is set to 'Blocked' the page view incorrectly stays enabled.** Previously, when using the **Web > Web Tracking** page, if the Transaction type was set to 'Blocked' the page view incorrectly stayed enabled. While it is irrelevant to the results displayed when searching on Blocked transactions, this might have caused some confusion. This behavior no longer occurs.
69932	**Fixed: Problems accessing any of the Mobile User Security Reports except the Summary Report when using Internet Explorer 6.0.** Previously, when using Internet Explorer version 6.0, problems were encountered when you attempted to access any of the Mobile Users Security reports (except for the Summary report). This behavior no longer occurs.
69941	**Fixed: When adding an Email Security appliance to a Security Management appliance, 'No' is displayed in the 'Connection Established' column.** Previously, when you added an Email Security appliance to a Security Management appliance, 'No' was incorrectly displayed in the 'Connection Established' column even though the connection had been established. This behavior no longer occurs.
69951	**Fixed: Page not displayed with certain Internet Explorer versions when persistent cookie with SCA is used.** Previously, certain pages were not displayed with certain Internet Explorer versions when persistent cookie with SCA is used. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
69955	**Fixed: The loadconfig command fails if there is WSA assigned to some configuration master and that WSA was added by hostname.** Previously, the **loadconfig** command failed if a Web Security appliance had been assigned to a particular Configuration Master and that Configuration Master was added using the hostname. This behavior no longer occurs.
70002	**Fixed: The loadconfig command fails if there is LDAP profile with external authentication query that was created before you upgraded to 7.2.1.** Previously, the **loadconfig** command failed if there was an LDAP profile with an external authentication query that was created before you upgraded to 7.2.1. This behavior no longer occurs.
70011	**Fixed: Incomplete time range indicators are not working due to incorrectly discarded data.** Previously, on the **Web > Reporting > User Details** page, the time range indicators were not working properly due to incorrectly discarded data. This behavior no longer occurs.
70020	**Fixed: For certain URLs, the Time Spent column on the report page may be overestimated.** Previously, when viewing certain URLs on the Security Management appliance, the Time Spent column used for reporting was overestimating the results. This was also happening on the Web Security appliance. This behavior no longer occurs.
70036	**Fixed: On some reports, searching with the 'Start With' string does not work correctly.** Previously, on some reports, searching with the 'Start With' string did not work correctly. For example, if you use 'Start With' on the **Web > Reporting > Web Sites** page, no results were displayed because the search works as 'End With'. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
70086	**Fixed: System logs do not always contain the commit comments.** Previously, the comments that the user entered in when committing changes on the Security Management appliance were not always stored in the system logs. This behavior no longer occurs.
70090	**Fixed: When all columns are selected to be displayed on a report, the reporting data exceeds the table cell in PDF format.** Previously, on the Security Management appliance, if all of the available columns were selected to be displayed on interactive reporting tables, the reporting data exceeded the table cells when using the Printable PDF format link. This behavior no longer occurs.
70119	**Fixed: The wording for an Alert sent for absent traffic is too alarming.** Previously, the wording for an Alert sent for absent web traffic was too alarming. The wording was as follows: The Critical message is TRANSFER: The following centralized services and hosts have been unreachable for file transfer: Centralized Service 'Centralized Web Reporting' has not connected to host". This behavior no longer occurs.
70205	**Fixed: The loadconfig command fails if the configuration file includes scheduled reports.** Previously, if you used the **loadconfig** command to load configuration files that included scheduled reports from the Web Security appliance to the Security Management appliance, the operation failed. This behavior no longer occurs.
70211	**Fixed: The list of appliances does not appear on the Publish Configuration Now page for users with custom roles.** Previously, after you have created users with custom roles and publish privileges, the list in the Select Appliance table from **Web > Utilities > Publish to Web Appliances > Publish Configuration Now > Select Appliance** did not show the correct list of appliances. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
70286	**Fixed: Warning message about insufficient disk quota for enabling Web Reporting Service is not clear enough.** Previously, when you enabled web reporting on the Security Management appliance, the amount of memory disk allocation was not clearly stated. This behavior no longer occurs.
70319	**Fixed: Windows Live Messenger does not get detected in transparent mode with regards to login transaction.** Previously, Windows Live Messenger did not get detected when login process occurred. This behavior no longer occurs.
70334	**Fixed: Web Tracking shows non-zero bandwidth usage for completely blocked URLs.** Previously, after blocking certain URLs on the Web Security appliance, the Security Management appliance Web Tracking page erroneously reported non-zero results for sites that are blocked. This behavior no longer occurs.
70418	**Fixed: In the Domains Matched table, the Domain search does not work as expected.** Previously, the Domain search did not work as expected in the Domains Matched table. This behavior no longer occurs.
70429	**Fixed: Full URLs should be displayed in detailed web tracking results.** Previously, when using the **Web > Reporting > Web Tracking** feature, truncated URLs were being displayed instead of the full URLs. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
70431	**Fixed: When centralized reporting is enabled, the Web > Reporting tab should be renamed.** Previously, when centralized reporting was enabled, the **Web > Reporting** tab should have been renamed. The name is misleading since there was no reporting on the Web Security appliance anymore. This behavior no longer occurs.
70438	**Fixed: Reporting and Tracking data availability issue on Target Security Management appliance.** Previously, data availability reports did not always work due to the fact that there were no appliances added to the target Security Management appliance. Additionally, when viewing the message tracking results, the hostname for each message may be labeled as 'unresolved'. This behavior no longer occurs.
70453	**Fixed: Configuration Masters that have not been initialized are available on Publish, Custom Roles, and Add Web Appliance pages after upgrade from earlier releases.** Previously, Configuration Masters that were not being initialized were available on Publish, Custom Roles, and Add Web Appliance pages after upgrade from earlier releases. For example, if you were upgrading from 6.7.6-076, to the current release, the Configuration Masters were erroneously available on certain pages. This behavior no longer occurs.
70603	**Fixed: When you enable Centralized Web Reporting from the reportingconfig command, you cannot Anonymize the user names.** Previously, when you enabled web reporting using the **reportingconfig** command, you could not anonymize the user names. This behavior no longer occurs.
70681	**Fixed: When upgrading your Security Management appliance from 6.7.7-019 to 7.2.0-199, an application fault is thrown.** Previously, when you upgraded your Security Management appliance from 6.7.7-019 to 7.2.0-199, an application error was thrown. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
70775	**Fixed: Web sites that belong to different regional domains are shown as the same domain on web reports.** Previously, on the Security Management appliance in the **Web > Reporting > Web Sites** report, different domains were listed on the Web Sites report with the same domain name. As a workaround, you needed to differentiate the domains by adding a second level domain using the **reportingconfig tld** command. This behavior no longer occurs.
71049	**Fixed: The sort feature does not work for Centralized Web Reporting in certain versions of Internet Explorer.** Previously, the Sort feature did not work for Centralized Web Reporting on the following versions of Internet Explorer: • Internet Explorer 6.0.2 • Internet Explorer 7.0.5730.13 This behavior no longer occurs.
71377	**Fixed: The Configuration Master counts that are assigned to Web Security appliances are inaccurate.** Previously, the Configuration Master counts that were assigned to Web Security appliances were inaccurate when displayed on the Security Management appliance. This behavior no longer occurs.
71474	**Fixed: The Security Management appliance sends critical alert messages if the end-users search messages in Cisco IronPort Spam Quarantine while system backup is running.** Previously, if you ran a backup on your system, and you tried to search messages in the Cisco IronPort Spam Quarantine while the backup was running, you received the following error message: `Error: An error occurred while trying to process your transaction. Please wait a few moments and try again. If the problem persists, please contact your system administrator.` This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
71618	**Fixed: Invalid schema.json gets created if there is delay in Reportd/reportd.py main to register groups/counters.** Previously, an invalid **schema.json** was created if there was a delay in **Reportd/reoprtd.py main** to **register groups/counters**. Because of this, web tracking data was not being saved correctly. This behavior no longer occurs.
72514	**Fixed: An HTML tag is erroneously displayed in CSV, User column of Top Application Types - Extended Scheduled reports.** Previously, when generating a report from **Web > Reporting > Scheduled Reports > Top Application Type - Extended** page, an HTML tag, ** ** could be seen in the User column. This behavior no longer occurs.
72657	**Fixed: Application Scanning Bypass in 7.1 Configuration Master was not published to 7.1 Web Security Appliance.** Previously, bypass settings were not being published from the 7.1 Configuration Master on the Security Management appliance to the Web Security appliance. This behavior no longer occurs.
72071	**Fixed: User Reports shows more than 24 hours in time spent when using day as time range.** Previously, on the Security Management appliance **User** reports page, the Time Spent calculation erroneously showed more than 24 hours in the Time Spent column when you were using 'Day' as the selected time range. This behavior no longer occurs.
72405	**Fixed: The Security Management appliance receives different results than the Web Security appliance when asking for groups in directory server.** Previously, different results were given when trying to learn what the selected groups and users were for the Access Policies. When you chose **Web > Configuration Manager 7.1 > Access Policies** on the Security Management appliance, you received one set of results; but if you chose **Access Policies > Selected Groups and Users** on the Web Security appliance you received another result. This behavior no longer occurs.

Table 8 Security Management Appliance Resolved Issues

Defect ID	Description
72835	**Fixed: No export link in report by User Location (Summary) report under 'Suspect Transactions Detected' charts for Remote and Local Users.** Previously, if you tried to navigate to the **Web > Reporting > Report By User Location** window on the Security Management appliance, the **Export** link was not visible under the Suspect Transactions Detected charts for Remote and Local Users. This behavior no longer occurs.
73195	**Fixed: The Security Management appliance should not disable Centralized services for such a long time.** Previously, on the Security Management appliance, the Centralized Services became disabled during the backup process. These services were only set to be enabled when the backup was complete. However, when a problem was encountered which caused the backup to take an inordinate amount of time, there was a possibility that there could be data loss. This behavior no longer occurs.

Email Security Appliance Issues

Note For issues that identically affect both the Email Security appliance and the Security Management appliance, such as issues with reports, see the Release Notes for the Email Security appliance.

There are no resolved issues for the Email Security appliance for this release.

Web Security Appliance Issues

Note For issues that identically affect both the Web Security appliance and the Security Management appliance, such as issues with reports, see the Release Notes for the Web Security appliance.

Table 9 describes the resolved issues for the Web Security appliance for this release.

Table 9 Web Security Appliance Resolved Issues for 7.2

Defect ID	Description
Fixed in Release 7.2.2	
72796	**The coeuslogd keeps starting and then exiting on a particular Web Security appliance.** Access Logging may not be available for a few minutes immediately after upgrading to 7.2.1 on the Web Security appliance.
Fixed in Release 7.2.1	
67674	**Anti-Malware not included in total on web site activity.** Previously, transactions that were counted as detected by anti-malware were not included in the total high-risk transactions detected. This behavior no longer occurs.
68088	**Deleting a PAC file on the Web Security appliance causes an application failure on the GUI.** Previously, when you deleted a PAC file, committed the changes, then chose '**Abandon Changes**' on the GUI, the Web Security appliance threw an application error. This behavior no longer occurs.
68150	**Malware Categories 'unknown' shows up in the reports for detected malware requests.** Previously, in the Malware Categories column, 'unknown' appeared in Web reports for detected malware. This behavior no longer occurs.
68416	**The Monitor > Overview page displays integers in the Top Malware Categories.** Previously, on the **Monitor > Overview** page on the Web Security appliance, the Top Malware Categories column displayed integers instead of the names of the virus categories. This behavior no longer occurs.

Table 9 Web Security Appliance Resolved Issues for 7.2 (continued)

Defect ID	Description
69203	**Viewing the contents of uploaded XML file with settings that are associated with a SaaS policy is not possible.** Previously, when viewing the contents of an uploaded XML file that is associated with a SaaS policy on the Web Security appliance, you could not preview the file until the policy was submitted. This behavior no longer occurs.
69317	**Web Security appliance does not display the last data transfer information correctly.** Previously, when you attempted to transfer multiple amounts of data from the Web Security appliance to the Security Management appliance, the Web Security appliance **Status Page** did not display the Last Data Transfer information correctly. This behavior no longer occurs.
69342	**Editing the name of a SaaS Application Authentication Policy on the Web Security appliance erroneously creates a new policy.** Previously, when editing the name of an existing SaaS Application Authentication Policy on the Web Security appliance, this action created a new policy instead of changing the name of the old policy. This behavior no longer occurs.
69863, 70606	**Unicode characters encountered in the URL cause parsing to fail.** Previously, if a Unicode character was encountered in a URL, the Web Security appliance was unable to parse the URL correctly. This behavior no longer occurs.
69917	**Filezilla files are not scanned by Outbound Malware filter.** Previously, even though Access Policies had been applied, Filezilla files were not being detected by the Outbound Malware filter on the Web Security appliance. This behavior no longer occurs.

Table 9 Web Security Appliance Resolved Issues for 7.2 (continued)

Defect ID	Description
70059	**Web Reputation Threat Types by Scanned Further Transactions at page Reporting -> Web reputation filters does not collect data without WBRS score.** Previously, if the 'Web Reputation Threat Types by Scanned Further Transactions' option was enabled, the Web Security appliance only reported on threat types discovered by WBRS. If Sophos detected malware, the malware threat did not show up in the Web Reputation Threat Types by Scanned Further Transactions table. It showed up in the Anti-Malware report instead. This behavior no longer occurs.
70128	**Extra text is displayed in upgrade output if you are upgrading from 7.1.0-96 to 7.1.0-100.** Previously, when you upgraded your Web Security appliance from 7.1.0-96 to 7.1.0-100, extra text was being generated and displayed in the upgrade output file. This behavior no longer occurs.
70229	**AVC does not support AOL AIM.** Previously on the Web Security appliance, the AVC filter blocked AOL IM packets. This behavior no longer occurs.
70407	**On the Web Security Appliance, the HTTPS Proxy page needs to translated for applications that use HTTPS.** Previously, when you enabled an HTTP proxy from the Web Security appliance, the settings on HTTPS proxy page that pertain to AVC were not translated. This behavior no longer occurs.
70479	**After a CIWUC feature key expires, when the AVC filter is enabled on the Web Security appliance, all transactions run very slow.** Previously, after a CIWUC feature key expired, when the AVC filter was enabled on the Web Security appliance, all transactions ran very slowly. A work around to this known issue was to disable AVC before expiring the CIWUC feature key. If AVC is disabled before expiring the CIWUC feature key, the Web Security appliance functions normally without any perceptible slowdown. This behavior no longer occurs.

Table 9 Web Security Appliance Resolved Issues for 7.2 (continued)

Defect ID	Description
70614	**When the Web Security appliance proxies data between the application client and application server, an encrypted connection can get disrupted.** Previously, when the Web Security appliance proxied data between application client and application server, an encrypted connection got disrupted and the client application eventually timed out. This behavior no longer occurs.
72535	**Client requests stall and time out when upgrading from a previous version with an expired Webroot feature key in some cases**. Previously, after upgrading from a previous version that had an expired Webroot feature key and an Access Policy that enabled the Webroot scanning engine, client requests stalled for about a minute and then failed with an 'Error 403 Forbidden response'. This behavior no longer occurs.

Service and Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

During customer support hours (24 hours per day, Monday through Friday excluding U.S. holidays), an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, please contact Cisco IronPort using one of the following methods:

U.S. toll-free: 1(877) 641- 4766

International: http://cisco.com/web/ironport/contacts.html

Support Portal: http://cisco.com/web/ironport/index.html