Understand Secure Web Appliance Release Changes

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Change History Per Release

Open Source Components

Related Content

Introduction

This document describes the main changes and added features in different versions of Secure Web Appliance (SWA).

Prerequisites

Requirements

There are no special requirements for this article.

Abbreviations used is this Articles are:

LD: Limited Deployment.

GD: General Deployment.

MD: Maintenance Deployment

ED: Early Deployment.

HP: Hot Patch.

CLI: Command Line Interface.

GUI: Graphical User Interface

HTTP: Hypertext Transfer Protocol.

HTTPS: Hypertext Transfer Protocol Secure.

ECDSA: Elliptic Curve Digital Signature Algorithm.

PID: Process Identifier.

CTR: Cisco Threat Response.

AMP: Advanced Malware Protection.

URL: Uniform Resource Locator.

CDA: Context Directory Agent.

ISE: Identity Services Engine

SaaS: Software as a Service

DLP: Data Loss Prevention

AVC: Application Visibility and Control

DCA: Dynamic Content Analysis

ADC: Application Discovery and Control

WBRS: Web Reputation Score

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Change History Per Release

Version	Type	Changes in Behavior	Enhancements / Added Features
12.0.1-268	LD	- The system CPU and memory requirements are changed from 12.0 release onwards. - By default, TLSv1.3 is enabled on the appliance. - Cipher "_AES_256_GCM_SHA384" is added to the default cipher list.	- The Cisco AsyncOS 12.0 release provides Web Security Appliance with High Performance (HP) for platforms S680, S690, and S695. - A new sub-command **highperformance** is added under the main **advancedproxyconfig** command to enable and disable the high performance mode. - Integration the SWA with Cisco Threat Response (CTR) Portal. - The appliance supports TLSv1.3 version. - The configuration file backup feature is moved from the sub menu **Log Subscriptions** to **Configuration File** under **System Administration**. - The appliance now supports the upload of ECDSA certificate for HTTPS proxy. - A new diagnostic **CLI proxyscannermap** sub-command is added under **diagnostic > proxy**. To displays PID mapping between each proxy and correspond scanner process. - New option **searchdetails is added under the CLI** command **authcache**. - New sub command **CTROBSERVABLE** is added under the **CLI** command **reportingconfig** to enable or disable the **CTR** observable based indexing.
12.0.1-334	GD		- A new sub-command scanners is added under the main **advancedproxyconfig** command to exclude the MIME types to be scanned by the AMP engine.
12.0.2-004	MD	- Use TLS 1.2 or later versions to connect the appliance to the AMP File Reputation server. - AMERICAS (Legacy) cloud-sa.amp.sourcefire.com cannot be configured on the appliance.	- A new option Enter the number of concurrent scans to be supported by AMP is added in the main **CLI** command **advancedproxyconfig > scanners > AMP.** you can change the default Unscannable verdict of long running scan eviction to Timeout and

			vice-versa from new **CLI** sub-command **eviction** in the main **CLI** command **advancedproxyconfig > scanners**.
12.02-012	MD		- Alert messages are triggered on the web user interface of the appliance when the proxy Malloc Memory crosses 90% of proxy Malloc Memory limit and an Email notification is sent to all Alert recipients configured to receive Web Proxy critical alerts. - The new web interface provides a new look for monitoring reports and tracking web services.
12.0.3-005	MD		
12.0.3-007	MD		- New URL Categories Update notification
12.0.4-002	MD		
12.0.5-011	MD	- TLSv1.2 is enabled by default for Appliance Management Web User Interface. - **Session Resumption** is disabled by default.	- Message is added to indicate the end of support for CDA in the CDA configuration section.
12.5.1-011	LD	- By default, the Cisco Success Network feature is enabled on the appliance. - These logs are modified to include more details: The access logs now display the user name when authentication fails. The authentication framework logs now display the client IP address for these failed authentication protocols: NTLM, BASIC, SSO (Transparent).	- The Cisco AsyncOS 12.5 release provides Web Security Appliance with High Performance (HP) for platforms S680, S690, and S695. This increases the traffic performance of the current high-end appliances. - You can now upgrade to 12.5 version and avail the High Performance mode on the models (S680, S690, S695, S680F, S690F, and S695F), even if you have enabled these features on your appliance: • Web Traffic Tap • Volume and Time Quotas • Overall Bandwidth Limits - You can now configure Web Proxy IP Spoofing by create an IP spoofing profile and add it to the routing policies. - You can now create a custom URL category for YouTube and set policies on the YouTube

			custom category for secure access control. - In the new web interface, the appliance has a new page (**Monitoring > System Status**) to display the current status and configuration of the appliance. - The Cisco Success Network (CSN) feature enables Cisco to collect telemetry of feature usage information of the appliance. - REST API for Network, Log Subscription, and Other Configurations.
12.5.1-035	GD	- Deprecation of TLS 1.0/1.1 : • Use TLS 1.2 or later versions to connect the appliance to the AMP File Reputation server. AMERICAS (Legacy). • cloud-sa.amp.sourcefire.com is removed from the AMP File Reputation server list, so AMERICAS (Legacy). • cloud-sa.amp.sourcefire.com cannot be configured on the appliance.	- The configuration of cache size for authentication (**Network > Authentication > Authentication Settings > Credential Cache Options**) is not supported from AsyncOS 12.5.1-035 and later versions.
12.5.1-043	GD		- The alert messages are displayed on the web user interface of the appliance (**System Administration > Alerts > View Top Alerts** • When the proxy Malloc memory crosses 90% of proxy Malloc memory limit. • When the proxy gets restarted on 100% of Malloc memory In both cases, an e-mail notification is sent to all Alert recipients configured to receive Web Proxy critical alerts.
12.5.2-007	MD		- A new URL Categories Update notification is introduced in the banner. An email notification on the upcoming URL category updates is also sent to the users.
12.5.2-011	MD		
12.5.3-002	MD		

12.5.4-005	MD	- From Cisco AsyncOS 12.5.4 version, TLSv1.2 is enabled by default for Appliance Management Web User Interface. - After an upgrade to Cisco AsyncOS 12.5.4 version, session resumption is disabled by default. - The message is added to indicate the end of support for CDA in the CDA configuration section.	
12.5.4-011	MD-Refresh		
12.5.5-004	MD		- After an upgrade to Cisco AsyncOS 12.5, you receive a prompt to restart the proxy process when you execute the **networktuning** command for the first time.
12.5.5-008	MD-Refresh		
12.5.6-008	MD		
14.0.1-014	LD	- By default, the HTTP 2.0 feature is disabled. To enable this feature, use the <**HTTP2**> command. - The AsyncOS 14.0 for Cisco Web Security Appliance supports TLSv1.3 session resumption in client and server. - The validity periods of these certificates are modified: • HTTPS • ISE • SaaS • Appliance Certificates • Demo/Management Certificate - The CLI and the GUI of the appliance now displays message when an upgrade fails due to invalid log name and file name in the log subscriptions.	- Cisco Web Security appliance now supports integration with Cisco SecureX. - You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. - You can now configure the Header Based Authentication scheme for an active directory. The client and the Web Security Appliance consider the user as authenticated and does not prompt again for authentication or user credentials. The X-Authenticated feature works when the Web Security Appliance acts as an upstream device. - The System Status Dashboard of the appliance has been enhanced: • Capacity Tab—A that provides details on Time Range, System CPU and Memory Usage, Bandwidth and RPS, CPU Usage by Function, and Client or Server Connections.

		- By default the polling interval is set to 24 hours. - After you upgrade to this release, you cannot perform the Start Test for LDAP authentication if the Base DN (Base Distinguished Name) field (Network > Authentication > Add Realm) is empty.	• The Proxy Traffic Characteristics under the Status tab provides client and server connections details. • The Service Response Time now includes more details on bar charts and also legend data for previous dates. - You can now retrieve configuration information, and perform changes (such as modify current information, add a new information, or delete an entry) in the configuration data of the appliance use REST APIs for Management Policies, Access Policies, and Bypass Policies. - Cisco AsyncOS 14.0 version supports HTTP 2.0 for web request and response over TLS. HTTP 2.0 support requires TLS ALPN based negotiation which is available only from TLS 1.2 version onwards. In this release, the HTTPS 2.0 is not supported for these features: • Web Traffic Tap • External DLP • Overall Bandwidth and Application Bandwidth - A new CLI command <HTTP2> is introduced to enable or disable HTTP 2.0 configurations. You cannot enable or disable HTTP 2.0 and restrict domain for HTTP 2.0 through the appliance web user interface. - The configuration of HTTP 2.0 is not supported through Cisco Secure Email and Web Manage - The CLI displays the new warning message when you try to use the default certificate of any of these features: • Appliance certificate (In the web user interface, navigate to **Network > Certificate Management > Appliance Certificate**) • Credential Encryption certificate (In the web user interface, navigate to **Network > Authentication > Edit Settings > Advanced section**) • HTTPS Management UI certificate (In the command line interface, use **certconfig > SETUP**)

			- A new sub-command **OCSPVALIDATION_FOR_SERVER_CERT** is added under the **certconfig**. With this new sub-command you can enable the OCSP validation for LDAP and Updater server certificates. If the certificate validation is enabled, you can receive an alert if the certificates involved in communication are revoked. - A new CLI command **gathererdconfig** is added to configure the polling functionality between the appliance and the authentication server. - You can now choose between Management and Data Interface, while you configure smart license feature on the appliance.
14.0.1-040	LD	- When you enable smart software licensing and register your Web Security Appliance with the Cisco Smart Software Manager, the Cisco Cloud Services (**Network > Cloud Service Settings**) automatically enables and registers your Secure Web Appliance through the Cisco Cloud Services portal. - You cannot disable or deregister Cisco Cloud Service if smart licensing is registered on your appliance. - If you have already registered your appliances to Cisco Smart Software Manager, and have not configured Cisco Cloud Services, then Cisco Cloud Services is automatically enabled after you upgrade to AsyncOS 14.0.1-040. By default, the region is registered as Americas, and you can modify the region (Europe and APJC) as required. - You cannot disable or deregister Cisco Cloud Service if smart license is registered on your appliance.	- You can view the details of the smart account created in the Cisco Smart Software Manager portal from the **smartaccountinfo** command in the CLI. - If the Cisco Cloud Services certificate has expired or is about to expire, the Cisco Cloud Service auto renews the certificate after the upgrade to AsyncOS 14.0.1-040. - If the Cisco Cloud Services certificate is expired, you can now download a new certificate from the Cisco Talos Intelligence Services portal from the **cloudserviceconfig > fetchcertificate** sub-command in the CLI. - You can auto register the Web Security Appliance with the Cisco Cloud Service portal (**cloudserviceconfig > autoregister** sub command in the CLI). - You can load the certificate for virtual appliance and hardware appliances from **updateconfig > clientcertificate** sub command in the CLI. - A new URL Categories Update notification is introduced in the banner. An email notification is also sent to the users about the upcoming URL category updates.
14.0.1-053	GD		

14.0.1-503	HP		
14.0.2-012	MD	- In Cisco AsyncOS 14.0.2 version, TLSv1.2 is enabled by default for Appliance Management Web User Interface under **System Administrator > SSL Configuration**. - Session resumption is disabled by default.	- Message is added to indicate the end of support for CDA in the CDA configuration section. - You can now choose between Data or Management interface for Smart License Registration from the Test Interface drop-down list.
14.0.3-014	MD	- After an upgrade to Cisco AsyncOS 14.0, you receive a prompt to restart the proxy process when you execute the **networktuning** command for the first time.	
14.0.3-502	HP	- When Secure Web Appliance operates in high performance mode, the heap limit exhaustion disables the high latency and accept handlers. This results in lesser number of connections.	
14.0.4-005	MD		
14.5.0-498	LD	- Product Rebrand: • AMP for Endpoints, Advanced Malware Protection and AMP were changed to Secure Endpoint • Threat Grid (File Analysis) changed to Malware Analytics - The misclassification request is sent over HTTPS and hence you do not receive security alert notifications. - The Samba version has been upgraded to version 4.11.15. - TLSv1.2 is enabled by default for Appliance Management web user interface under **System Administrator > SSL Configuration**. - On a fresh installation of AsyncOS	- The Secure Web Appliance can now validate the DNS response received from the DNS server supports cryptographic signatures. - The Secure Web Appliance restricts the number of concurrent connections initiated by the client to a configured value. - With AsyncOS Release 14.5, Cisco Web Security Appliance has been rebranded to Cisco Secure Web Appliance. - The accesslog decision tag in the Decrypt Policy group is appended with End user Notification (EUN) when the EUN page appears on the client web browser. - The clone policy feature allows you to copy or clone the configurations of a policy and to create a new policy. - You can manage the traffic bandwidth by configure the bandwidth value in quota profile and map the quota profile in access policy URL

		14.5, the Expired and Mismatched Hostname certificate configurations value in the HTTPS Proxy page is selected by default as **Drop** instead of **Monitor**.	category or overall web activity quota. - REST API to configure management policies, decryption policies, routing policies, IP spoofing policies, Anti-Malware and reputation, Authentication realms, Cisco Smart Software License, Cisco Umbrella Seamless ID, Identity services, and System setup. - You can integrate ISE-SXP deployment with Cisco Secure Web Appliance for passive authentication. This allows you to get all defined mappings, includes SGT-to-IP address mappings that are published through SXP. - The Cisco Umbrella Seamless ID feature enables the appliance to pass the user identification information to the Cisco Umbrella Secure Web Gateway (SWG) after successful authentication. - Message is added to indicate the end of support for CDA in the CDA configuration section. - You can now choose between Data or Management interface for Smart License Registration from the Test Interface drop-down list. - After an upgrade to Cisco AsyncOS 14.5, you receive a prompt to restart the proxy process when you execute the **networktuning** command for the first time.
14.5.0-537	GD		- These policies with clone option in Secure Web Appliance can also be managed by Cisco Secure Email and Web Manager (SMA): • Access Policy • Identification profile • Decryption Policy • Routing Policy
14.5.1-008	MD		
14.5.1-016	MD		
14.5.2-011	HP		
14.6.0-108	LD		- AsyncOS 14.6 provides support to Cisco

			Umbrella with Cisco Secure Web Appliance (SWA). The integration of Umbrella and Secure Web Appliance facilitates deployment of common web policies from Umbrella to Secure Web Appliance.
15.0.0-322	LD	- FreeBSD version has been upgraded to FreeBSD 13.0. - Cisco SSL version 1.0.2 to Cisco SSL version 1.1.1: • Talos engines such as AVC, WBRS, DCA, and Beaker have been upgraded. • Scanner engines such as Webroot and McAfee have been upgraded.	- These enhancements made to the Smart Software Licensing feature: • License Reservation • Device Led Conversion—After you register Secure Web Appliance with smart license, all current valid classical licenses are automatically converted to smart licenses with the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal. - You can manage the traffic bandwidth by configure bandwidth value in quota profile and map the quota profile in decryption policy and access policy, URL category or overall web activity quota. - The clone policy feature allows you to copy or clone the configurations of a policy and to create a new policy. - Application Discovery and Control (ADC) engine: an acceptable use policy component which inspects web traffic to gain deeper understanding and control of web traffic used for applications. With AsyncOS 15.0, you can use either AVC or ADC engine to monitor web traffic. By default, AVC is enabled. The ADC engine supports high performance mode. - REST API for ADC Configuration - Admin can opt to configure custom SNMPv3 username other than the default username v3get. - The maximum length of the custom header is 16k. - Option to choose the secure tunnel interface and remote access connection.

15.0.0-355	GD	- Device Led Conversion—After you register Secure Web Appliance with smart licensing, all current valid classical licenses are automatically converted to smart licenses with the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal. - By default, AVC is enabled. - Cisco SSL version 1.0.2 to Cisco SSL version 1.1.1: • Talos engines such as AVC, WBRS, DCA, and Beaker have been upgraded. • Scanner engines such as Webroot and McAfee have been upgraded. • FreeBSD 13.0 is compatible with Cisco SSL version 1.1.1 only. - Only Cisco SSH compatible cipher, mac and kex algorithms, can be supported for SSH connectivity to FreeBSD 13.0. - The DCA feature is disabled in the AsyncOS 15.0 GD release and remains unsupported for enablement in this release. - The SNMPWALK/SNMPGET operations for SNMP OIDs for Proxy Malloc memory is not supported in the multi-prox SWAs (S690, S695, S1000V).	- License Reservation—You can reserve licenses for features enabled in Secure Web Appliance without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Web Appliance in a highly secured network environment with no communication to the Internet or external devices. - You can manage the traffic bandwidth by configuring the bandwidth value in quota profile and mapping the quota profile in decryption policy and access policy URL category or overall web activity quota. - The clone policy feature allows you to copy or clone the configurations of a policy and to create a new policy. - Supports Application Discovery and Control (ADC) engine, an acceptable use policy component which inspects web traffic to gain deeper understanding and control of web traffic used for applications. now you can use either AVC or ADC engine to monitor web traffic. - The ADC engine supports high performance mode. - You can now retrieve configuration information, and perform any changes (such as modify current information, add a new information, or delete an entry) in the access policy configuration data of the appliance with REST APIs. - Admin can opt to configure custom SNMPv3 username other than the default username v3get. - The maximum length of the custom headers to web requests is 16k. - Option to choose the secure tunnel interface and remote access connection
15.0.0-364	HP	Has been fixed for these Defects: • Cisco Bug ID CSCvz26149 • Cisco Bug ID CSCwf78874 • Cisco Bug ID CSCwf84371 • Cisco Bug ID CSCwh31573 • Cisco Bug ID CSCwh37834	

		• Cisco Bug ID CSCwh41379 • Cisco Bug ID CSCwh48523 • Cisco Bug ID CSCwh71926	
15.1.0-287	LD	- In AsyncOS 15.1 and later releases, Smart Software License is mandatory. - The integration of Cisco Umbrella and Cisco Secure Web Appliance facilitates deployment of common web policies from Umbrella to Secure Web Appliance. In addition, you can configure policies through the Umbrella dashboard and view logs.	
15.2.0-164	GD	- You must enable Smart Licensing before upgrading Secure Web Appliance to AsyncOS 15.2. - By default, the source interface in Secure Web Appliance Umbrella settings is set to **Management**. - The End-User Notification page always is enable in Secure Web Appliance as a global setting. - Mandatory Smart License for Secure Web Appliance: • The AsyncOS 15.2 and later releases do not support the classic license commands and UI options. • AsyncOS 15.2 does not support Federal Information Processing Standards (FIPS) mode, • Cisco SecureX, Cisco Cognitive Threat Analysis (CTA), and Cisco Cloudlock are decommissioned from AsyncOS 15.2. • Upgrading to AsyncOS 15.2 disables these features, and you cannot enable them from the Secure Web Appliance GUI - In the High Performance mode on SWA S396 model, Proxy instances in SWA S696 model increases from 3 to 5. - This scanning engines are replicated	- Hybrid policies support translation for rule actions Allow, Block, and Warn. - There is support for translation of Content Categories, Destination Lists, and Applications. - The AsyncOS 15.2 release introduces M6 hardware for Cisco Secure Web Appliances. These are the supported hardware models: • S196 • S396 • S696 • S696F

		as two instances for the S396 model and five instances for the S696 model while the appliance is in high performance mode: • Sophos • McAfee • Merlin • AVC • Archive scan • AMP - Data 1 and Data 2 interfaces are not supported. Instead, you can use the P1 and/or P2 interfaces. M2, Data 1, and Data 2 interfaces options are not available in etherconfig CLI.	
15.2.1-011	MD	- Transitioning from SecureX to XDR: SWA supports XDR Integration.	

Open Source Components

Here are the list of changes in open source component used in SWA:

Version	11.8.X	12.0.X	12.5.X	14.0.X	14.5.X	14.6.X	15.0.X
freebsd	10.4	10.4	10.4	11.2	11.2	11.2	13.0

Related Content

Release Notes for AsyncOS 12.0 for Cisco Web Security Appliances - Cisco

Release Notes for AsyncOS 12.5 for Cisco Web Security Appliances - Cisco

Release Notes for AsyncOS 14.0 for Cisco Web Security Appliances - Cisco

Release Notes for AsyncOS 14.5 for Cisco Secure Web Appliance - Cisco

What is the release terminology for content security? (cisco.com)

Cisco Secure Email and Web Virtual Appliance Installation Guide

Technical Support & Documentation - Cisco Systems

Release Notes for AsyncOS 15.1 for Cisco Secure Web Appliance - Cisco

Release Notes for AsyncOS 15.0 Hot Patch 1 for Cisco Secure Web Appliances - Cisco

Release Notes for AsyncOS 15.2 for Cisco Secure Web Appliance