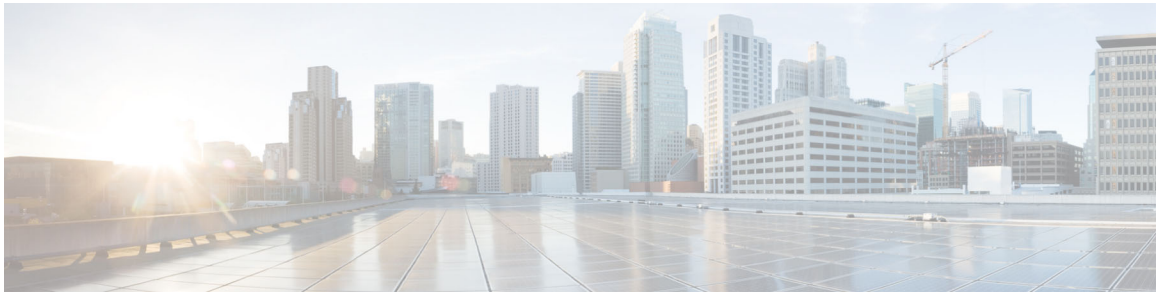

Release Notes for Advanced Web Security Reporting (Release 7.x)

Published: August 31, 2016
Revised: September 16, 2019

Contents

What's New

Cisco Systems, Inc.
www.cisco.com

New in Release 7.0

Feature	Description
AWRS proxy services display events with no WBRS Score in search results	New filter for no WBRS score (Show WBRS: No Score) is added in the **Web Tracking > Proxy Services** dashboard. With this filter, you can view the search results for proxy services with no WBRS score.
Department Membership Reporting displays detailed results for AD Group report	You can now view the following results for AD group reports under **User Analysis > Overview**: – Top Groups by Transactions Blocked – Transactions Blocked Summary – Top Groups by Bandwidth Used – Bandwidth Used Summary – Top Groups by User – Bandwidth Used Summary – AD Group Summary – AD Group per User Details

New in Release 6.6

Feature	Description
Search in Custom Dashboards	Searching for data in Custom Dashboards is supported. • You can search for data using the main search field with the submit button. • You can filter the search results using the secondary search field in the results pane.
Export from any page	You can export data (non graphical data) from any dashboard as a comma-separated values (csv) file, an XML file, or a JavaScript Object Notation (json) file. You must hover over the dashboard data display pane to view this option ↓ to download.

New in Release 6.5

This release contains a bug fix; see the Fixed Issues, page 8.

New in Release 6.4

Feature	Description
Web Tracking Dashboard Updates	• New filters - **User**, **Client IP**, **WBRS** minimum and maximum score ranges, and **SNI** are added in the **Web Tracking** > **Proxy Services** dashboard. • You can view and export 10000 transactions from the Proxy Services dashboard.

New in Release 6.3

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 6.6.6.

New in Release 6.2

Feature	Description
Cisco Umbrella reports support	You can point the Advanced Web Security Reporting application to the AWS bucket containing logs provided by Umbrella. You can view the reports in the Consolidated Web Security Reports dashboards.
Splunk Engine Upgrade	The Splunk engine is upgraded to the latest version.

Note Role based reporting works only on the data models that are not accelerated. Since disabling acceleration increases the time to load reports, enable data model acceleration if role based reporting is not used. See the "Configuration Best Practices" and "Restrict Access to Department Reports by Role" chapters in the user guide.

New in Release 6.1

Feature	Description
CEF Extractor	The Common Event Format (CEF) Extractor service lets you transform access logs received from one or more Web Security appliances into CEF-formatted output data.
Web Security Appliance AsyncOS 10.1 support	Support for changes to Archive Scan access logs, included in the AsyncOS 10.1 for Web Security Appliances release.

New in Release 6.0

Feature	Description
Custom Filters	Define custom searches of the available access, SOCKS and AMP log data, in a process known as “filtering.”
Updated interface	Updated “look and feel” for the application.

System Requirements

AsyncOS Version Compatibility

Advanced Web Security Reporting Application	AsyncOS for Web Security Appliances
7.0	10.0, 10.1, 10.5, 11.0, 11.5, 11.7, 11.8
6.6	10.0, 10.1, 10.5, 11.0, 11.5, 11.7
6.5	10.0, 10.1, 10.5, 11.0, 11.5, 11.7
6.4	10.0, 10.1, 10.5, 11.0, 11.5, 11.7
6.3	8.5.3, 8.7.0, 8.8.0, 9.0.0, 9.1.0, 10.0, 10.1, 10.5, 11.0, 11.5
6.2	8.5.3, 8.7.0, 8.8.0, 9.0.0, 9.1.0, 10.0, 10.1, 10.5, 11.0.
6.1	8.5.3, 8.7.0, 8.8.0, 9.0.0, 9.1.0, 10.0, 10.1.
6.0	8.5.3, 8.7.0, 8.8.0, 9.0.0, 9.1.0, 10.0.

Requirements for Advanced Web Security Reporting

Operating System Requirements on a virtual appliance

- Linux (64-bit)
- Windows (64-bit) - Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Server 2016, Windows 8, Windows 8.1, Windows 10

Platform Requirements. Reference hardware can be commodity-grade, and must have the following minimum specifications to be eligible for Cisco support:

- Intel x86 64-bit chip architecture with two CPUs, 12 cores per CPU, 2.0 Ghz or higher per core (minimum)
- 16 GB RAM
- Four 300-GB SAS hard disks at 10,000 rpm each, in RAID1+0 (800 IOPS or better)
- Standard 1-Gb Ethernet NIC, optional second NIC for a management network

Assumptions:

- Operating System is installed with root or administrative permissions.
- IPV4 configured as IPV6 is not supported in the current release.
- Operating system/Kernel related vulnerabilities are taken care of by applying all necessary patches.

Note Advanced Web Security Reporting is often constrained by disk I/O first, so always consider disk infrastructure first when selecting the storage hardware.

A separate OS volume should be created per industry best practices. The Enterprise installation should reside on its own logical volume whenever possible.

Supported file systems:

Platform	File Systems
Linux	ext2, ext3, ext4, btrfs, XFS, NFS 3/4
Windows	NTFS, FAT32

System-wide resource limits on Unix based systems

The following table shows the system-wide resources that the software uses. It provides the minimum recommended settings for these resources for instances that are not forwarders (such as indexers, search heads, cluster masters, license masters, deployment servers, and Monitoring Consoles (MC)).

System-wide Resource	ulimit Invocation	Recommended minimum value
Open files	ulimit -n	64000
User processes	ulimit -u	16000
Data segment size	ulimit -d	1073741824

This consideration is not applicable to Windows based systems.

Sizing & Scaling Recommendations

- The base configuration is a single-tier architecture with one server offering all three parts of the core functionality of a typical Advanced Web Security Reporting deployment:
  - a search instance
  - an indexer
  - a monitor for data sources
- By adding another Advanced Web Security Reporting instance and adjusting the configuration, the new infrastructure would offer an increase in aggregate indexing and search performance (once the data is load-balanced), and an increase in storage and retention capacity.
- A dedicated forwarder server would also be added to the infrastructure and configured to monitor the Web Security appliance log files and forward the log data across multiple indexers using load balancing.
- To facilitate the implementation and configuration of an environment that has huge Daily indexing Volume see Table 1Infrastructure recommendation based on Daily Indexing Volume, page 7. It is recommended that you engage Splunk Professional Services for infrastructure setup of Distributed Deployment.

Note **Scaling requires an infrastructure of distributed deployment setup which has to be incorporated through engagement of Splunk Professional services. This infrastructure is not tested / validated by AWSR as it is setup/configured and validated at customer site through Splunk Proffesional services only.**

Based upon log volume estimates against a Web Security Appliance with 10K users, the amount of data collected is 10 GB/day uncompressed. Once indexed, the data compresses to an estimated 2.5 GB/day indexed storage used. The Advanced Web Security Reporting instance would retain approximately 200 days of indexed data based upon a volume size of 500 GB.

Web Security Appliance Users	Estimated Log Volume (2,500 transactions/user/day)	Estimated Indexed Volume	Estimated retention (500 GB volume)
10 K	10 GB/day	2.5 GB	200 days
50 K	50 GB/day	13 GB	40 days
100 K	100 GB/day	25 GB	20 days

Note Guidelines based upon estimated log volumes and mid-capacity drives in an array.

Daily Volume	77 GB/day	140 GB/day	180 GB/day
Total Transactions	172 Million	325 Million	417 Million
Predefined Report Load time	< 5 seconds	< 10 seconds	< 15 seconds

Total Volume	2.3 TB
Business days retention @70 GB/day	33
Predefined Report Loading time	< 20 seconds

Table 1 Infrastructure recommendation based on Daily Indexing Volume

Total Users	Daily Indexing Volume						
	< 2 GB/day	2 to 250 GB/day	250 to 500 GB/day	500 to 750 GB/day	750GB to 1 TB/day	1 to 2 TB/day	2 to 3 TB/Day
< 4	1 combined instance	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	1 Search instance 8 Indexers	1 Search instance 12 Indexers
up to eight	1 combined instance	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 4 Indexers	1 Search instance 5 Indexers	1 Search instance 10 Indexers	1 Search instance 15 Indexers
up to 16	1 Search instance 1 Indexer	1 Search instance 1 Indexer	1 Search instance 3 Indexers	1 Search instance 4 Indexers	2 Search instance 6 Indexers	2 Search instance 12 Indexers	2 Search instance 18 Indexers
up to 24	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	2 Search instance 6 Indexers	2 Search instance 12 Indexers	2 Search instance 18 Indexers
up to 48		1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	3 Search instance 8 Indexers	3 Search instance 16 Indexers	3 Search instance 24 Indexers

Install and Upgrade Instructions

For essential instructions, including scripts to be run, see the *Advanced Web Security Reporting Installation, Setup, and User Guide,* available from the location shown in Related Documentation, page 8.

Setting Main as the Destination Index

Unlike earlier releases, you must choose **Main** as the destination Index when setting up on-going data transfers. This is described in the *Advanced Web Security Reporting Installation, Setup, and User Guide.*

Licensing

This release provides “hybrid reporting”; that is, support for both Web Security appliance and CWS log reports. To use hybrid reporting, you must upgrade your licenses; however, you can continue to use Web Security appliance-only reporting with your existing license. Refer to the Licensing and Migration section of the *Cisco Advanced Web Security Reporting Installation, Setup, and User Guid*e for more information.

Note To migrate from Web Security appliance-only to hybrid reporting, you must open a Cisco Technical Assistance Center (TAC) case to remove your existing license and install a new hybrid-reporting license that contains the complete list of reporting source types (that is, the `ciscocws` source type is included). This is not necessary if you are a new user of Advanced Web Security Reporting version 4.0 or later.

Open Issues

- CWS support for Advanced Malware Protection report added, but not for File Analysis report.
- SPLUNK open issues can be found at https://www.splunk.com/page/securityportal.

Fixed Issues

- CSCvn65880 - AWSR not parsing all the access logs
- CSCvn97489 - In proxy service screen, unable to see value for field policy due to bad parsing of the WSA log.
- CSCvn97502 - Policy_type is not displaying any value with some wsa log format because issue is in Regex.
- CSCvo04664 - AWSR is unable to generate report due to ACL Tag issue.
- CSCvn97441 - AWSR is unable to parse some WSA log format for field full_decision.
- CSCvo24110 - AMP verdict is not updating any result in AWSR 6.5.

Related Documentation

The following documentation is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

- *Advanced Web Security Reporting Installation, Setup, and User Guide*
- User Guide for your supported release of AsyncOS for Web Security Appliances

Support

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community for web security and associated management at the following URL:

https://community.cisco.com/t5/web-security/bd-p/5786-discussions-web-security

Customer Support

International: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: Visit http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

---

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