



Cisco Advanced Web Security Reporting v.7.x Release Notes

First Published: 2016-08-31

Last Modified: 2022-04-29

About Web Security Appliance

The Cisco Web Security Appliance intercepts and monitors Internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other Internet-based threats.

What's New

- [New in Release 7.5.2, on page 1](#)
- [New in Release 7.5.1, on page 2](#)
- [New in Release 7.5, on page 2](#)
- [New in Release 7.0, on page 2](#)
- [New in Release 6.6, on page 3](#)
- [New in Release 6.5, on page 3](#)
- [New in Release 6.4, on page 3](#)
- [New in Release 6.3, on page 4](#)
- [New in Release 6.2, on page 4](#)
- [New in Release 6.1, on page 4](#)
- [New in Release 6.0, on page 4](#)

New in Release 7.5.2

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 8.2.5.
Python Upgrade	The Python version is upgraded from 2.7 to 3.7.

Feature	Description
UI Updates	You can now access the Access Control page using the following navigation paths for 7.5.2: <ul style="list-style-type: none"> • Settings > Users and Authentication > Access Controls Users • Settings > Users and Authentication > Access Controls Roles. • Settings > Users and Authentication > Access Controls Password Management.
Summary Index	Summary Index has been enabled in the Overview page (Top Malware Categories - Panel) to improve the performance.

New in Release 7.5.1

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 7.3.5.
Syslog Parser Update	Syslog parser update for Web Security Appliance 12.0.1-334.

New in Release 7.5


Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 7.3.3.
User Drilldown page displays report of AD group details.	In the User Analysis > User Drilldown page, a new filter is added to search by AD Group name. The AD group details are displayed in the search results. It displays the following details: AD Group, User ID, Destination Domain, Bandwidth Used, and Time Spent.

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.

Feature	Description
Department Membership Reporting displays detailed results for AD Group report	<p>You can now view the following results for AD group reports under User Analysis > Overview:</p> <ul style="list-style-type: none"> – 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	<p>Searching for data in Custom Dashboards is supported.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

New in Release 6.5

This release contains a bug fix; see the [Fixed Issues](#).

New in Release 6.4

Feature	Description
Web Tracking Dashboard Updates	<ul style="list-style-type: none"> • 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
7.5.2	12.0, 12.5, 14.0,14.5
7.5.1	10.0, 10.1, 10.5, 11.0, 11.5, 11.7, 11.8, 12.0, 12.5, 14.0
7.5	10.0, 10.1, 10.5, 11.0, 11.5, 11.7, 11.8, 12.0
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

The Splunk hardware specification is a baseline for scoping and scaling the Splunk platform for your use. The specification is a performance guide for handling search and indexing loads.

Performance Recommendations

The Daily Indexing Volume table summarizes the performance recommendations that were given in the performance checklist. The table shows the number of reference machines on Splunk enterprise that you need to index and on which you need to search data in Splunk Enterprise, depending on the number of concurrent users and the amounts of data that the instance indexes.

The table is only a guideline. Modify these figures based on your use case.

Table 1: Performance Recommendation based on Daily Indexing Volume

Total Users	Daily Indexing Volume					
	< 2GB/day	2 to 300GB/day	300 to 600GB/day	600GB to1TB/day	1 to 2TB/day	2 to 3TB/day

Total Users	Daily Indexing Volume					
< 4	1 combined instance	1 combined instance	1 Search Head, 2 Indexers	1 Search Head, 3 Indexers	1 Search Head, 7 Indexers	1 Search Head, 10 Indexers
Up to 8	1 combined instance	1 Search Head, 1 Indexers	1 Search Head, 2 Indexers	1 Search Head, 3 Indexers	1 Search Head, 8 Indexers	1 Search Head, 12 Indexers
Up to 16	1 Search Head, 1 Indexers	1 Search Head, 1 Indexers	1 Search Head, 3 Indexers	2 Search Heads, 4 Indexers	2 Search Heads, 10 Indexers	2 Search Heads, 15 Indexers
Up to 24	1 Search Head, 1 Indexers	1 Search Head, 2 Indexers	2 Search Heads, 3 Indexers	2 Search Heads, 6 Indexers	2 Search Heads, 12 Indexers	3 Search Heads, 18 Indexers
Up to 48	1 Search Head, 2 Indexers	1 Search Head, 2 Indexers	2 Search Heads, 4 Indexers	2 Search Heads, 7 Indexers	3 Search Heads, 14 Indexers	3 Search Heads, 21 Indexers

Platform Requirements

Reference Host Specification—Single-Instance Deployments

The following requirements represent the basic building blocks of a Splunk Enterprise deployment:

- Intel x86 64-bit chip architecture
- 12 CPU cores at 2Ghz or greater speed per core
- 12GB RAM
- Standard 1Gb Ethernet NIC, optional second NIC for a management network
- Standard 64-bit Linux or Windows distribution

Disk Subsystem

The disk subsystem for a reference machine should be capable of handling a high number of average **Input/Output Operations Per Second (IOPS)**.

IOPS is measurement of how much data throughput a hard drive can produce. There are IOPS values for disk reads and writes since a hard drive reads and writes at different speeds, The average IOPS is the blend between those two figures.

The higher the average IOPS that a hard drive can produce, the more data it can index and search in a given duration. While there are many variable factors that account for the IOPS that a hard drive can produce, the following are the most important:

- Rotational speed in revolutions per minute.
- Average latency, which is the amount of time it takes to spin its platters half a rotation.
- Average seek time, which is the amount of time it takes to retrieve a requested block of data.

The drives that are capable of producing the highest IOPS have high rotational speeds and low average latency and seek times. Every drive manufacturer provides this information, and some manufacturers provide much more information.

This specification uses eight 146GB, 15,000 RPM, serial-attached SCSI (SAS) HDs in a Redundant Array of Independent Disks (RAID) 1+0 fault tolerance scheme as the disk subsystem. Each hard drive is capable of about 200 average IOPS. The combined array produces a little over 800 average IOPS.

Insufficient disk I/O is the most common limitation in Splunk infrastructure. For the best results in indexing your data, review the disk subsystem requirements before provisioning your hardware.

Reference Host Specification—Search Head

A search head uses CPU resources more consistently than an indexer, but does not require the fast disk throughput or a large pool of local storage for indexing.

The following requirements represent the Search Head deployment:

- Intel 64-bit chip architecture
- 16 CPU cores at 2GHz or greater speed per core.
- 12GB RAM
- 2 x 300GB, 10,000 RPM SAS hard disks, configured in RAID 1
- A 1Gb Ethernet NIC, optional 2nd NIC for a management network
- A 64-bit Linux or Windows distribution

A search request uses up to 1 CPU core while the search is active. When provisioning a search head, you must account for scheduled searches in addition to ad-hoc searches that users run. More active users and higher concurrent search loads require additional CPU cores.

When you distribute the indexing process, the Splunk platform can scale to consume terabytes of data in a day. When you add more indexers, you distribute the work of search requests and data indexing across those indexers. Additional indexers significantly increase performance.

Ratio of Indexers to Search Heads

There is no practical limitation on the number of search heads that an indexer can support, or on the number of indexers that a search head can search against. The use case determines what Splunk instance role (search head or indexer) the infrastructure needs to scale to while maintaining performance.

The following are the reference indexer specifications:

Reference Host Specification—Indexer

The following requirements represent the host specification of an Indexer:

- Intel 64-bit chip architecture.
- 12 CPU cores at 2GHz or greater per core.
- 12GB RAM.
- Disk subsystem capable of a minimum of 800 average IOPS. For details, see the topic Disk subsystem.
- A 1Gb Ethernet NIC, with an optional second NIC for a management network.

- A 64-bit Linux or Windows distribution.

Splunk has introduced two new specifications that help improve user experience by providing additional CPU cores for better indexing performance and search concurrency.

A single indexer carries the same disk I/O bandwidth requirements as a group of indexers.

Reference Host Mid-Range Specification–Indexer

The mid-range specification is similar to the base reference specification. This specification improves indexing capacity and search concurrency over a distributed Splunk Enterprise deployment.

The following requirements represent the mid-range host specification of an Indexer:

- Intel 64-bit chip architecture
- 24 CPU cores at 2GHz or greater speed per core
- 64GB RAM
- Disk subsystem capable of a minimum of 800 average IOPS
- A 1Gb Ethernet NIC, with optional second NIC for a management network
- A 64-bit Linux or Windows distribution

Reference High-Performance Specification–Indexer

The high-performance specification is a further improvement upon the mid-range specification.

The following requirements represent the high-performance host specification of an Indexer:

- Intel 64-bit chip architecture
- 48 CPU cores at 2GHz or greater speed per core
- 128GB RAM
- Disk subsystem capable of a minimum of 1200 average IOPS
- A solid state disk (SSD) subsystem as a minimum requirement for hot and warm
- Index buckets
- A 1Gb Ethernet NIC with optional second NIC
- A 64-bit Linux or Windows distribution

Disk Subsystem Information for Higher-Performance Specifications

When indexers retrieve data for searches, there are many disk seeks and bulk reads. At higher daily volumes, local disk might not provide cost-effective storage for the time frames in cases where you want a fast search. Fast attached storage or networked storage, such as storage area networks (SAN) over fiber, can provide the required IOPS for each indexer in these cases.

When you plan your storage infrastructure, analyze based on the following points:

- More disks (specifically, more spindles) are better for indexing performance.
- Total throughput of the entire system is important.

- The ratio of disks to disk controllers in a particular system should be higher, similar to the provisioning of a database host.

Network Latency Limits for Clustered Deployments

A Splunk environment with search head or indexer clusters must have fast, low-latency network connectivity between clusters and cluster nodes. This connectivity is particularly important in environments that have clusters in multiple sites.

For indexer cluster nodes, network latency should not exceed 100 milliseconds. Higher latencies can significantly slow indexing performance and hinder recovery from cluster node failures.

Impact of network latency on clustered deployment operations.

The impact of latency can vary based on the individual configurations.

Network Latency	Cluster Index time (1 TB of data)	Cluster Node Recovery Time
< 100 ms	6202 s	143 s
300 ms	6255 s (+ 1%)	1265 s (+ 884%)
600 ms	7531 s (+ 21%)	3048 s (+ 2131%)

For search head clusters, latency should not exceed 200 milliseconds. Higher latencies can impact how fast a search head cluster elects a cluster captain.

Confirm with your network administrator that the networks that will support the clustered Splunk environments meet or exceed these latency guidelines. If reduction of latency below these levels is not possible, then contact Splunk Support or Professional Services to discuss tuning cluster timeout settings on the cluster nodes to handle the increased latency.

Virtual Hardware

Splunk supports use of its software in virtual hosting environments. An indexer on a hypervisor (such as VMware) with reserved resources that meet one of the hardware specifications can consume data about 10 to 15 percent more slowly than an indexer hosted on a bare-metal host. Search performance in a virtual hosting environment is a close match to bare-metal computers.

The performance that a virtual host provides is a best-case scenario that does not account for resource contention with other active virtual hosts that share the same physical host or storage array. The performance also does not account for certain vendor-specific I/O enhancement techniques, such as Direct I/O or Raw Device Mapping.

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

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

This consideration is not applicable to Windows based systems.

Sizing and 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 2 Infrastructure recommendation based on Daily Indexing Volume](#). 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 Professional 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	

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](#).

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*.

Open Issues

- SPLUNK open issues can be found at <https://www.splunk.com/page/securityportal>.

Fixed Issues

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2022 Cisco Systems, Inc. All rights reserved.