CISCO
SECURE

Data sheet
Cisco public

Cisco Advanced Web Security Reporting

January 2021

The bridge to possible

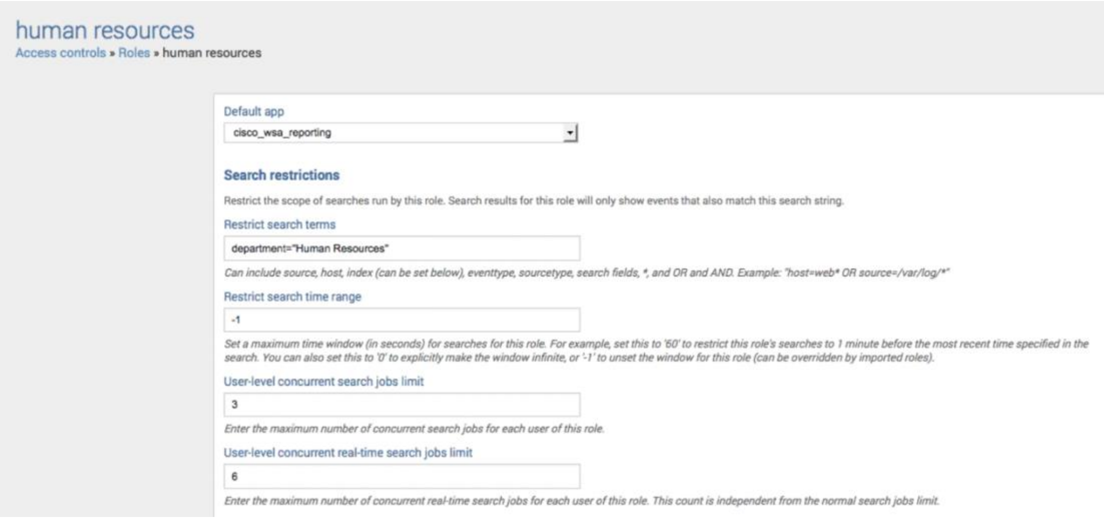
Contents

Introduction

Cisco® Advanced Web Security Reporting Application is a reporting solution that rapidly indexes and analyzes logs produced by Cisco Secure Web Appliance (formerly Web Security Appliance) and Cisco Umbrella. This tool provides scalable reporting for customers with high traffic and storage needs. It allows reporting administrators to gather detailed insight into web usage and malware threats.

Directory-Group-Based Reporting

With Advanced Web Security Reporting Application, administrators can generate reports based on a group or user ID, as defined within a central authentication server such as Active Directory. Reports can be created easily along functional or geographical boundaries that have been defined by the authentication groups. Roles can be created to allow managers to view reports only for a defined set of directory groups (such as the groups that they manage), protecting the privacy of individuals who are not within those groups.



human resources

Access controls » Roles » human resources

Default app

cisco_wsa_reporting

Search restrictions

Restrict the scope of searches run by this role. Search results for this role will only show events that also match this search string.

Restrict search terms

department="Human Resources"

*Can include source, host, index (can be set below), eventtype, sourcetype, search fields, *, and OR and AND. Example: "host=web* OR source=/var/log/*"*

Restrict search time range

-1

Set a maximum time window (in seconds) for searches for this role. For example, set this to '60' to restrict this role's searches to 1 minute before the most recent time specified in the search. You can also set this to '0' to explicitly make the window infinite, or '-1' to unset the window for this role (can be overridden by imported roles).

User-level concurrent search jobs limit

3

Enter the maximum number of concurrent search jobs for each user of this role.

User-level concurrent real-time search jobs limit

6

Enter the maximum number of concurrent real-time search jobs for each user of this role. This count is independent from the normal search jobs limit.

Setting up the directory-group-based reporting

Detailed Layer 4 Traffic Monitor Visibility

Administrators can run reports on activities on nonweb ports. These Layer 4 Traffic Monitor (L4TM) reports connect hosts associated with particular ports and users, and they can be used to identify malicious behavior on nonstandard ports - behavior that would evade many traditional web-security solutions.

SOCKS Reporting

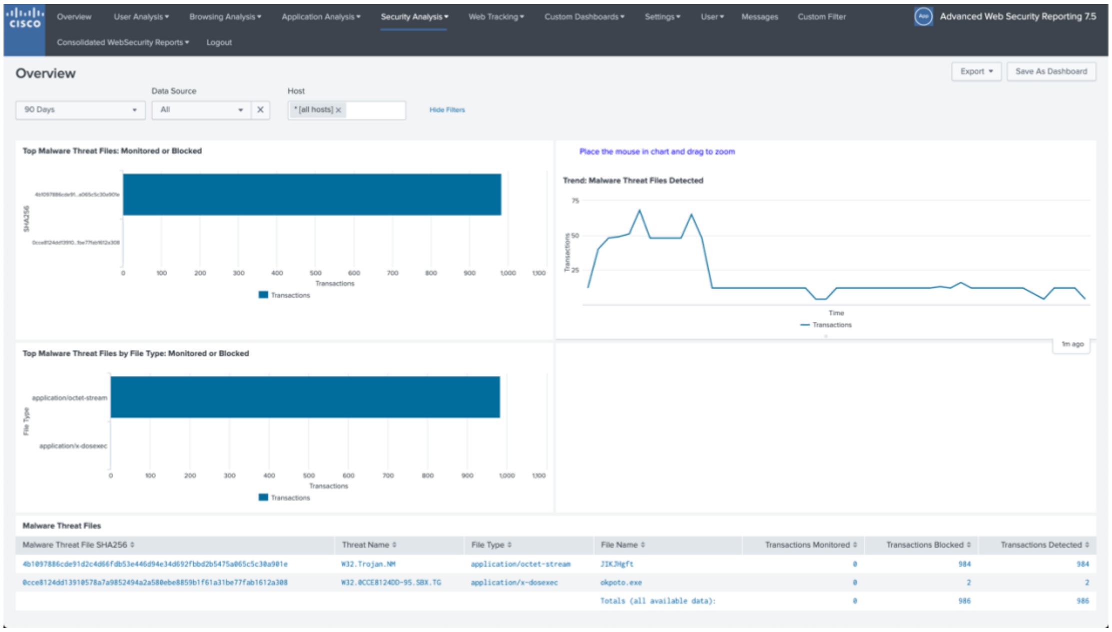
For customers using Socket Secure (SOCKS) proxy settings, administrators get information about SOCKS traffic.

Historical Data Import

Historical logs can be imported during forensic investigations. Logs from any time period can be imported into the reporting tool for analysis, allowing human resources and legal personnel to conduct forensic investigations spanning several years. Administrators can focus on a specific user's web activity, if needed.

Advanced Malware Protection Reporting

Featuring file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the Secure Web Appliance. This reporting application consolidates data provided by the Cisco Advanced Malware Protection solution that produces a single pane of glass for even richer analysis for administrators to gather more detailed insight into web usage and malware threats.



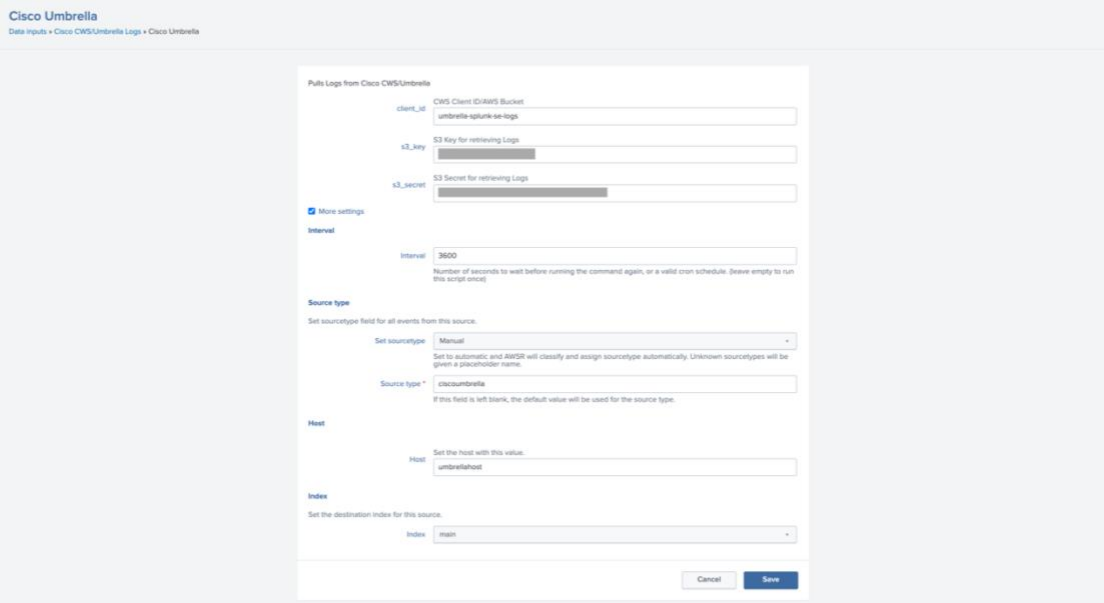
Malware Threat Files

Malware Threat File SHA256	Threat Name	File Type	File Name	Transactions Monitored	Transactions Blocked	Transactions Detected
4b1097886cde91d2c4d66fdb53e446d94e34d692fbbd2b5475a065c5c30a901e	W32.Trojan.NM	application/octet-stream	JIKJHgft	0	984	984
0cce8124dd13910578a7a9852494a2a580ebe8859b1f61a31be77fab1612a308	W32.0CCE8124DD-95.SBX.TG	application/x-dosexec	okpoto.exe	0	2	2
			Totals (all available data):	0	986	986

Advanced Malware Protection reporting

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.



Cisco Umbrella

Data inputs » Cisco CWS/Umbrella Logs » Cisco Umbrella

Pulls Logs from Cisco CWS/Umbrella

client_id — CWS Client ID/AWS Bucket: umbrella-splunk-se-logs

s3_key — S3 Key for retrieving Logs: [redacted]

s3_secret — S3 Secret for retrieving Logs: [redacted]

☑ More settings

Interval

Interval: 3600

Number of seconds to wait before running the command again, or a valid cron schedule. (leave empty to run this script once)

Source type

Set sourcetype field for all events from this source.

Set sourcetype: Manual

Set to automatic and AWSR will classify and assign sourcetype automatically. Unknown sourcetypes will be given a placeholder name.

Source type *: ciscoumbrella

If this field is left blank, the default value will be used for the source type.

Host

Host — Set the host with this value.: umbrellahost

Index

Set the destination index for this source.

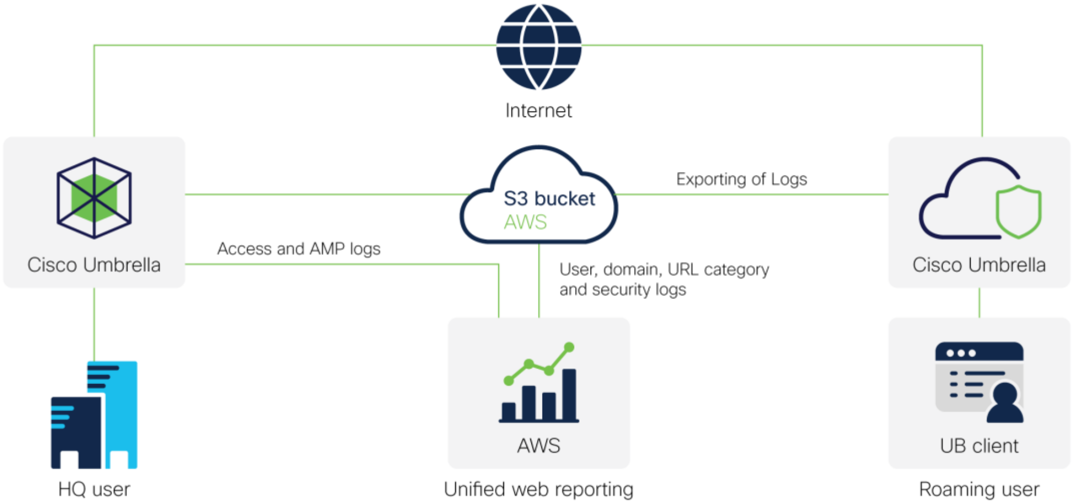
Index: main

Setting up the Cisco Umbrella S3 bucket configuration

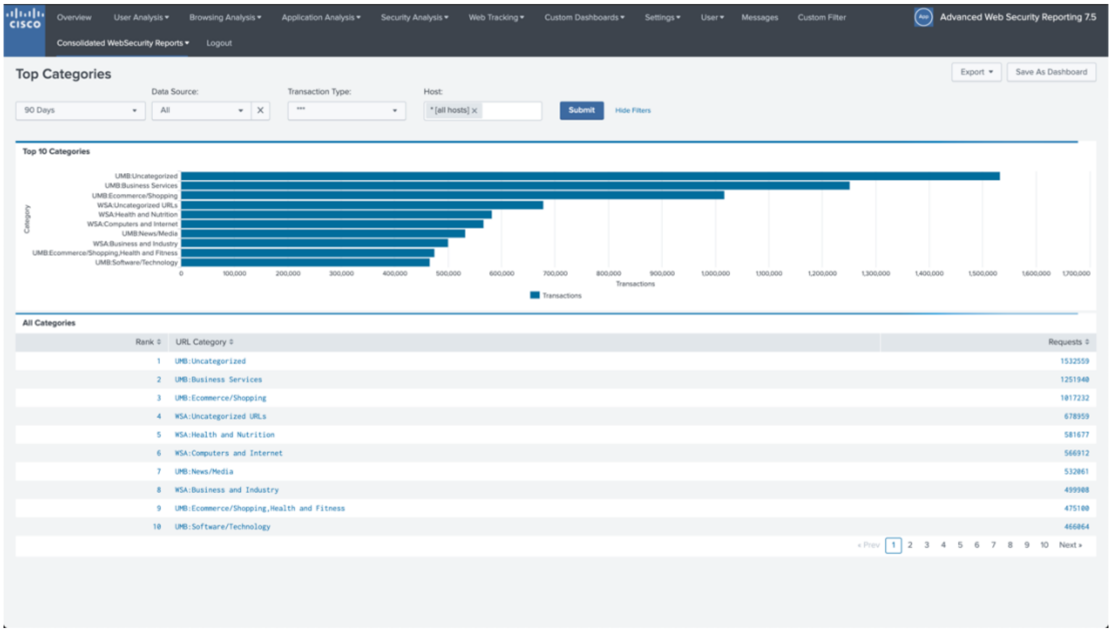
Consolidated Web Security Reports

You can view consolidated reports from Cisco Umbrella and Secure Web Appliances under following categories:

- Overview
- Activity Search
- Security Activity
- Top Domains
- Top Categories
- Top Users
- Top Security Categories



Consolidated web security reporting architecture



Top Categories

90 Days

Data Source: All

Transaction Type: ***

Host: * [all hosts]

All Categories

Rank	URL Category	Requests
1	UMB:Uncategorized	1532559
2	UMB:Business Services	1251940
3	UMB:Ecommerce/Shopping	1017232
4	WSA:Uncategorized URLs	678959
5	WSA:Health and Nutrition	581677
6	WSA:Computers and Internet	566912
7	UMB:News/Media	532061
8	WSA:Business and Industry	499908
9	UMB:Ecommerce/Shopping,Health and Fitness	475100
10	UMB:Software/Technology	466064

Consolidated Secure Web Appliance and Umbrella Top 10 URL Categories sample report

Who Should Use Web Reporting?

Built-in reporting capabilities on Cisco Web Security and Security Management Appliances fulfill the reporting needs of most Cisco customers. Advanced Web Security Reporting is an advance reporting solution for customers who need extended storage for high transaction volumes or directory-group-based reporting. It also serves as a "single pane of glass" for customers who have deployed a hybrid web security solution. The Cisco Web Reporting report format is identical to reports already available on Cisco S-Series and M-Series appliances.

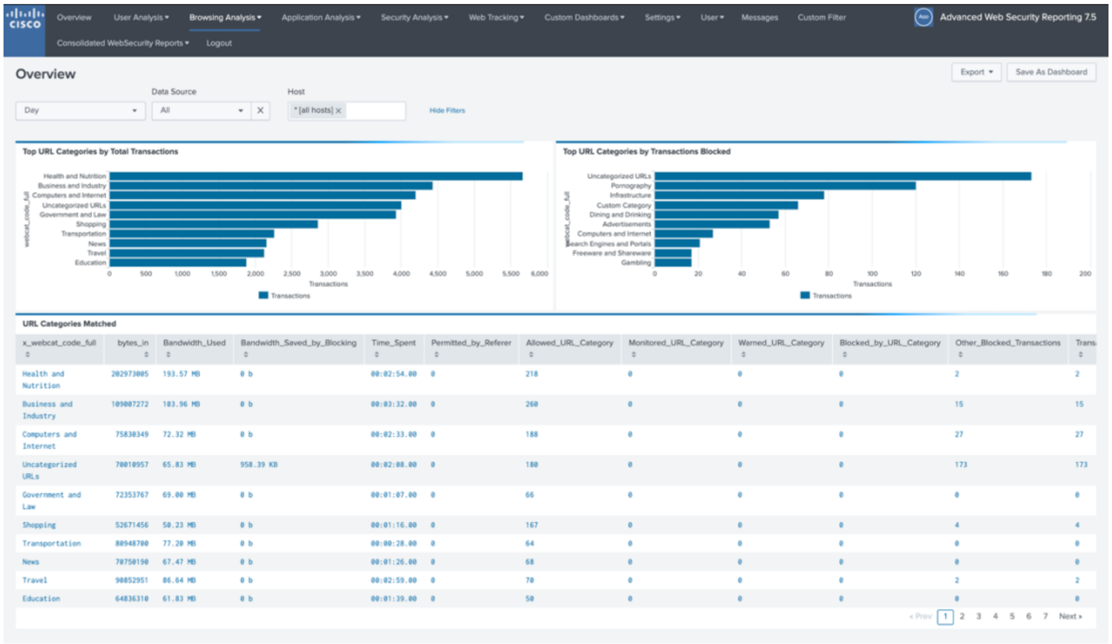
What Does the Latest Release of Cisco Web Reporting Include?

- **Unified Web Security Reporting:** The Cisco Advanced Web Security Reporting Application integrates diverse information into a single display for easier monitoring of your web security, regardless of deployment (Figure 1). The reporting application polls log data collected from multiple Secure Web Appliances and Umbrella for predefined reports. Customers can also perform ad-hoc searches using the flash timeline view and web-tracking forms.
- **Scale and Performance:** Advanced Cisco Web Security Reporting Application aligns with the introduction of data tiers across seat bands, allowing for purchase flexibility based on daily log volume requirements.
    - **Low tier:** This version meets the limited data needs of current customers who use 2 MB of data per user per day.
    - **High tier:** This version is for Hybrid Web Security and Enterprise License Agreement (ELA) customers whose users have higher data requirements (6 MB per user per day).

There are two types of deployment options are available for AWSR.

- Single-instance Deployment
- Distributed Deployment

** Please note that these options include only a license for Web Security Reporting. The offering does not include Configuration and Policy Management licenses.*



URL Categories Matched

x_webcat_code_full	bytes_in	Bandwidth_Used	Bandwidth_Saved_by_Blocking	Time_Spent	Permitted_by_Referer	Allowed_URL_Category	Monitored_URL_Category	Warned_URL_Category	Blocked_by_URL_Category	Other_Blocked_Transactions	Trans
Health and Nutrition	202973005	193.57 MB	0 b	00:02:54.00	0	218	0	0	0	2	2
Business and Industry	109007272	103.96 MB	0 b	00:03:32.00	0	260	0	0	0	15	15
Computers and Internet	75830349	72.32 MB	0 b	00:02:33.00	0	188	0	0	0	27	27
Uncategorized URLs	70010957	65.83 MB	958.39 KB	00:02:08.00	0	180	0	0	0	173	173
Government and Law	72353767	69.00 MB	0 b	00:01:07.00	0	66	0	0	0	0	0
Shopping	52671456	50.23 MB	0 b	00:01:16.00	0	167	0	0	0	4	4
Transportation	80948700	77.20 MB	0 b	00:00:28.00	0	64	0	0	0	0	0
News	70750190	67.47 MB	0 b	00:01:26.00	0	68	0	0	0	0	0
Travel	90852951	86.64 MB	0 b	00:02:59.00	0	70	0	0	0	2	2
Education	64836310	61.83 MB	0 b	00:01:39.00	0	50	0	0	0	0	0

Reports for URL Categories and Transactions Blocked

System requirements

Advanced Web Security Reporting runs on Microsoft Windows and Red Hat Linux. Refer to “Requirements for Advanced Web Security Reporting” section in release notes for details on the system requirements for specific release of Advanced Web Security Reporting application.

Please talk to your Cisco account team and refer to the documentation to understand the hardware specifications you will need to run the Cisco Web Reporting Application at your organization.

Ordering Information:

Ordering Cisco Advanced Web Security Reporting is simple. There are two bundles are available based on per day data limit.

The top level SKUs are:

Web Security Reporting – Lower Tier:
SMA-WSPL-LOW-LIC=; that this license has a data limit of 2 MB per user per day.

Web Security Reporting – Higher Tier:
SMA-WSPL-HIGH-LIC=; this license has a higher data limit of 6 MB per user per day.

Refer to the Cisco ordering guide for subscription SKU.

Cisco environmental sustainability

Information about Cisco’s environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the “Environment Sustainability” section of Cisco’s Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the “Environment Sustainability” section of the CSR Report) are provided in the following table:

Sustainability Topic	Reference
Information on product material content laws and regulations	**Materials**
Information on electronic waste laws and regulations, including products, batteries, and packaging	**WEEE Compliance**

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

More information can be found by referencing the ordering guide, release notes, and user guide.

Get Started: Download the Single Installer for Linux and Windows.

Questions: Please contact your Cisco Partner Account Manager.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

2306003 01/21