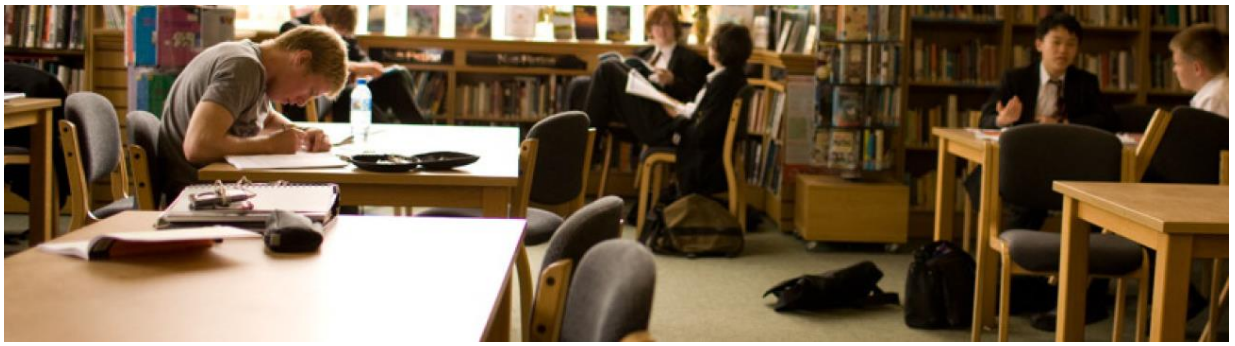
Cisco Cloud Web Security Log Extraction



Cisco Cloud Web Security (CWS) Log Extraction allows CWS customers to automatically pull web usage data quickly and securely for analysis using an S3 compatible HTTPS API.

Overview

CWS reporting in ScanCenter allows customers to report on all aspects of employee browsing activity. It also provides views on blocked threats, top sites visited, social media usage, bandwidth usage and many other aspects of online activity.

With the explosion of Big Data in organizations today, customers want a way to integrate and correlate the data from CWS with other data in the customer organization. The primary use case for integrating CWS browsing log data with customer on-premises systems is integration with 'Security Information and Event Management' (SIEM) systems. However, Log Extraction can be used with a variety of reporting and analysis tools.

With Log Extraction on CWS reporting and analysis tools will be able to automatically pull web usage data quickly and securely for analysis using an HTTPS programmable interface.

The log data is compiled in W3C text format and log information consisting of 28 attributes. Typically, the log information is available within 15 minutes of the event occurring.

Table 1. 28 Accessible Attributes Provided by Log Extraction

28 Accessible Attributes Provided by Log Extraction			
1	datetime	**15**	sc-status
2	c-ip	**16**	sc(Content-Type)
3	cs(X-Forwarded-For)	**17**	s-ip
4	Cs-username	**18**	x-ss-category
5	cs-method	**19**	x-ss-last-rule-name
6	cs-uri-scheme	**20**	x-ss-last-rule-action
7	cs-host	**21**	x-ss-block-type
8	cs-uri-port	**22**	x-ss-block-value

9	cs-uri-path	**23**	x-ss-referer-host
10	cs-uri-query	**24**	x-ss-external-ip
11	cs(User-Agent)	**25**	x-avc-app-id
12	cs(Content-Type)	**26**	x-avc-app
13	cs-bytes	**27**	x-amp-score
14	sc-bytes	**28**	x-amp-sha

S3 compatible API

Cisco CWS Log Extraction is using an open source implementation of the S3 API, which is a popular Application Programming Interface (API) used by Amazon Web Services. Cloud Web Security log extraction is hosted on Cisco's own infrastructure and the S3 compatible API enables compatibility with other S3 compatible tools.

Where can I find information more information about the S3 API?

http://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html

Licensing and User Count

The Log Extraction subscription follows the existing CWS framework of 1, 3, and 5 year terms with user-based pricing tiers. Subscriptions are available for customers with 25 users and all the way to 100,000 or more users.

Try Log Extraction Today

Log Extraction can be evaluated for free. Contact your Cisco Sales Account Manager today to get started.

For More Information

For more information on Cisco Cloud Web Security, visit www.cisco.com/go/cws.

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 www.cisco.com/go/offices.

Printed in USA C11-733817-00 02/15