Cisco Web Security Appliance Advanced Reporting Installation, Setup, and User Guide

November 20, 2014

Cisco Systems, Inc.
www.cisco.com

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco Web Security Appliance Advanced Reporting Installation, Setup, and User Guide

CONTENTS

CHAPTER 1

Installation and Setup

Introduction

The Cisco Web Security Appliance Advanced Reporting application provides reports and dashboards that are designed to give insight into very large volumes of data from the Cisco Web Security Appliance. The application includes a customized Splunk application and a Splunk server that polls log data collected from a Cisco Web Security Appliance.

The application receives data from a Cisco Web Security Appliance and stores the data in the default/main index. It generates summaries and stores them in the summary index. Customers can view these data using predefined reports. Customers can also perform ad hoc searches using the flashtimeline view and the web tracking forms.

Version 2.0 of this application was referred to in the documentation as "Splunk Application for Cisco Web Security Appliance".

Supported and Unsupported Splunk Features

Component	Supported	Not Supported
Reports	Reports included in the Cisco Web Security Appliance Advanced Reportingapplication	Custom reports
Search	Form-based search/web tracking tool included with the Cisco Web Security Appliance Advanced Reporting application	Native Splunk search engine
Server	Single-server deployments	Multiple-server deployments
Transport Method	FTP (Files and Directories)	TCP
Virtualization	N/A	Virtualization of any core function of Splunk referenced within this document
PDF Server Application	On Linux	On Windows

System Requirements

System requirements are detailed in the *Cisco Web Security Appliance Advanced Reporting Release Notes*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Sizing & Scaling Recommendations

Sizing and scaling recommendations are detailed in the *Cisco Web Security Appliance Advanced Reporting Release Notes*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Setup Overview

Step 1 Install and Configure Splunk, page 1-3

Step 2 Install or Upgrade the Cisco Web Security Appliance Advanced Reporting Application, page 1-4

Step 3 Create the Folder Structure for Log Files, page 1-6

Step 4 Import and Index Historical Data, page 1-6

Step 5 Set Up Ongoing Data Transfers, page 1-8 (Including setup of Cisco Web Security Appliance.)

Install and Configure Splunk

These tasks are out of the scope of this document but must be performed in order to use Cisco Web Security Appliance Advanced Reporting. See Splunk documentation on the Splunk web site for help performing these tasks.

Task	More Information
Download and install the free Splunk software. Follow instructions in the Splunk documentation.	www.splunk.com docs.splunk.com
Login to Splunk using the admin account and change the password.	docs.splunk.com
Licensing: **1.** Consider the quantity of data to be indexed both during initial historical data upload and on a daily basis ongoing. **2.** Acquire and upload a Splunk evaluation license sufficient for the historical data upload. **3.** Acquire and upload a Splunk enterprise licence sufficient for the anticipated data of the applicable source type to be indexed. **4.** Change the licence type from Trial to Evaluation or Enterprise. **5.** Edit license pool to ensure that the index is reporting to the correct pool. First, customer may need an evaluation license good for a large volume of data to handle historical data input. Then,	docs.splunk.com See also: Additional Reading, page 1-13.
Set Cisco WSA Advanced Reporting as the default app for all users/roles.	docs.splunk.com
(Optional) Enable SSL within Splunk.	docs.splunk.com
(Optional) Prepare associations with AD/LDAP: **1.** Configure Splunk to use AD/LDAP for authentication. **2.** Verify that Splunk can connect to your AD/LDAP server. **3.** Map Existing AD/LDAP groups to Splunk roles **4.** Add and edit roles within Splunk as needed. **5.** (Optional) Enable SSL on your AD/LDAP server.	Notes about Authentication/Authorization, page 1-3 docs.splunk.com
(Best practice) Verify Splunk services are set to restart automatically and test.	docs.splunk.com

Notes about Authentication/Authorization

- Splunk basic authentication
- AD/LDAP

Splunk Basic Authentication

Local Splunk authentication supersedes any other authentication option configured.

Default setup:

- Three roles: Define user privileges.
- One user account: admin, which is permanent. Use this account to configure, test, and troubleshoot.

Tip

- Add users to a splunk-specific group in the directory services.
- Import that group DN into Splunk.
- Either map the most appropriate default Splunk role to that group DN or create and map to a more appropriate role.

If your requirements are simple, for example, only a few people can view Splunk data, then using local authentication may be sufficient.

Install or Upgrade the Cisco Web Security Appliance Advanced Reporting Application

Download the Cisco Web Security Appliance Advanced Reporting Application

Release	Link
3.0	https://software.cisco.com/download/release.html?mdfid=283503844&flowid=39823&softwareid=283998384&release=Splunk%20Reporting%203.0&relind=AVAILABLE&rellifecycle=&reltype=latest
2.0	http://software.cisco.com/download/release.html?mdfid=283503844&flowid=39823&softwareid=283998384&release=Splunk%20Reporting%202.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Upgrade Overview

Upgrading from Release 2.0 to Release 3.0

Step 1 Install Cisco Web Security Appliance Advanced Reporting.

Step 2 Run the cleanup script (described below.)

Step 3 Import and index historical data.

Step 4 Restart Splunk.

Upgrading from Release 1.0 to Release 2.0

Step 1 Uninstall the older version of the Cisco Web Security Appliance Advanced Reporting.

Step 2 Install the new version.

Step 3 Import and index historical data even if you are upgrading from the previous release of the application.

If you skip the importing and indexing of historical data, three reports will only display new data:

- top_url_categories
- top_application_types
- top_malware_categories

Install or Upgrade Cisco Web Security Appliance Advanced Reporting

Before You Begin

- Install and Configure Splunk, page 1-3
- Download the Cisco Web Security Appliance Advanced Reporting Application, page 1-4.
- If you are upgrading from a previous version of Cisco Web Security Appliance Advanced Reporting, see Upgrade Overview, page 1-4.

Step 1 Open Splunk Web.

Step 2 Do the following:

- Splunk version 6.1.4: Select **Apps** and click **Install app from file**.
- Splunk version 5.0.10: Select **Manager > Apps > Install App from File**.

Step 3 Browse to and select the zip or tar .file for the Cisco Web Security Appliance Advanced Reporting application.

Step 4 Watch for notification that the application was imported successfully.

Step 5 Restart Splunk:

- Splunk version 6.1.4: Select **Settings > Server Controls > Restart Splunk**.
- Splunk version 5.0.10: Select **Manager > Server Controls > Restart**.

Step 6 Log into Splunk Web.

Step 7 Verify that Cisco Web Security Appliance Advanced Reporting is visible and enabled:

- Splunk version 6.1.4: Select **Apps > Cisco WSA Advanced Reporting**.
- Splunk version 5.0.10: Select **Manager > Apps**.

What to Do Next

- (Upgrades from Release 2.0 to Release 3.0 Only) Run the Upgrade Cleanup Script, page 1-6
- Import and Index Historical Data, page 1-6.

(Upgrades from Release 2.0 to Release 3.0 Only) Run the Upgrade Cleanup Script

Step 1 Access the Splunk command-line interface.

Step 2 Change directory:

```
$ cd $SPLUNK_HOME/etc/apps/SplunkforCiscoIronportWSA/bin
```

Step 3 Run the cleanup script:

```
$ ../../../../bin/splunk cmd python upgrade_from_v2.py
```

In most cases, this script completes without providing feedback. This is expected.

Step 4 If you have modified any of the cleaned-up files (very unlikely), the script creates a new directory and moves the files to it. If this happens, you will see a message like:

```
Moving local/viewstates.conf to local.old.YYYYMMDD-HHMMSS/viewstates.conf
```

Step 5 Restart Splunk.

Step 6 Check to see if files were backed up:

```
$ SPLUNK_HOME/etc/apps/SplunkforCiscoIronportWSA/local.old.YYYYMMDD-HHMMSS
```

If no files were moved, this directory does not exist.

Configuration Best Practices

- Set time zones consistently across Cisco Web Security Appliance appliances.

  The time displayed in the search results reflects the ‘local’ time of the Splunk instance. By default, all Splunk inputs for the Cisco Web Security Appliance logs are set to TZ = GMT.
- Document the local admin account password (regardless of the chosen authentication method).

Create the Folder Structure for Log Files

Log	Default Path	Variables
Traffic Monitor	/$Input_base/wsa_hostname/trafmonlogs/	$Input_base=Splunk deployment host_name=WSA device
Access	/$Input_base/wsa_hostname/accesslogs/	$Input_base=deployment host_name=WSA device

Import and Index Historical Data

The default for the summary script is to summarize up to 90 days of history. By default, the summary script uses 8 cores.

(Optional) Estimate the Import Time

The historical summary can take up to 9 hours to complete

Step 1 Allow 4 minutes per 5 million events (2GB of raw data) per summary job based upon the platform hardware recommendations.

Example: Expect a 10GB file representing 25 million historical events to take 20 minutes to run against each summary job.

Step 2 Allow for the 27 summary jobs used by Cisco Web Security Appliance Advanced Reporting.

Import and Index Historical Data

Before You Begin

- Complete configuration tasks listed in Install and Configure Splunk, page 1-3.
- Verify that field extractions are correct. SeeChapter 3, “Field Extractions”.
- Know the folder structure. See Create the Folder Structure for Log Files, page 1-6.
- (Optional) See (Optional) Customize the Summary Script, page 1-8.

Step 1 Copy the historical log files into the folder structure for log files.

Note By default, these logs will be deleted after the data is indexed.

Step 2 From a command prompt run the summary script:

Linux: `$SPLUNK_HOME/etc/apps/CiscoWSA/bin/summary.sh`

Windows: `X:\$SPLUNK_HOME\etc\apps\CiscoWSA\bin\summary.vbs`

Step 3 Navigate to the Splunk folder and enter the local Splunk administrator credentials when prompted.

Note You may not see immediate results.

Step 4 In Splunk Web, login as admin.

Step 5 Verify that data is being imported:

In Splunk 5.0.10:

a. Select **App > Search**.

b. Select **Status > Index Activity > Index Activity Overview**.

c. Look in the report for summary index growth.

In Splunk 6.1.4:

a. Go to the search app.

b. Select **Settings > Indexes.**

c. Scroll down to the **summary** row.

d. Verify that the **Earliest event** and **Latest event** columns display reasonable dates.

Step 6 If the historical data import was run under a Splunk evaluation license, install the Enterprise default license downloaded for the account and remove any non-Production licenses.

What to Do Next

- Configure Data Inputs in Splunk, page 1-8.

(Optional) Customize the Summary Script

Step 1 Open the summary script for editing:

- Linux: `$SPLUNK_HOME/etc/apps/CiscoWSA/bin/summary.sh`
- Windows: `X:\$SPLUNK_HOME\etc\apps\CiscoWSA\bin\summary.vbs`

Step 2 Search for this string:

time $Spath/bin/splunk cmd python $Spath/bin/fill_summary_index.py -app SplunkforCiscoIronportWSA -namefile $Spath/etc/apps/SplunkforCiscoIronportWSA/bin/summary.jobs -et -90d -lt now -j 8 -dedup true

Step 3 Customize the start and end dates and the number of cores used by the summary script:

Setting	Default	Description
-et	-90d	Start day. Number of historical days at which to begin summarizing. The default value of -90d begins at 90 days prior to the current day.
-lt	now	End day. Number of historical days at which to stop summarizing. The default value of now stops with the current day. A default of -1d would stop with yesterday's data.
-j	8	Number of cores to be used by the summary script.

Set Up Ongoing Data Transfers

Configure Data Inputs in Splunk

Before You Begin

- Import and Index Historical Data, page 1-6
- Know the path to your log files: Create the Folder Structure for Log Files, page 1-6.
- Open Splunk Web.

Step 1 In Splunk Web:

- Splunk version 6.1.4: Select **Settings > Data Inputs > Files and Directories**.

- Splunk version 5.0.10: Select **Manager > Data Inputs > Files and Directories**.

Step 2 Disable any inputs labeled CiscoWSA.

Step 3 Copy the file: $SPLUNK_HOME/etc/apps/CiscoforIronportWSA/default/inputs.conf
to the folder: $SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/

Step 4 Using a text editor, open $SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/inputs.conf.

Step 5 Locate the appropriate stanza for the input method and log source and edit the path.

Input Method	Stanza in inputs.conf File	More Information

Batch	sourcetype=wsa_accesslogs
	interval=60
	move_policy = sinkhole
		This is the default. Reads and deletes the data.
		Only add move_policy = sinkhole if you want the original data to be deleted.
		Do not use Splunk as the primary log storage with batch input configuration.

Monitor	[monitor://<path>]	Splunk monitors a file or directory for changes. [batch:///data1/splunklogs/*] (folder that is being monitored.]

Step 6 Within the same stanza, edit the value for disabled: `disabled = false`.

Step 7 For every additional Cisco Web Security Appliance added, create a separate input stanza.

Wildcards are not supported here.

Step 8 Save the file.

Step 9 Restart Splunk.

Step 10 In Splunk Web:

- Splunk version 6.1.4: Select **Settings > Data Inputs > Files and Directories**.
- Splunk version 5.0.10: Select **Manager > Data Inputs > Files and Directories**.

Step 11 In Splunk Web, verify that the inputs are listed, enabled, and have the correct path.

Step 12 In Splunk Web, for each input:

a. Click the input name.

b. Select the **More settings** check box.

c. **Set the Source Type** to **Manual**,

d. Set **Source Type** to **wsa_accesslogs**,

e. Set the **destination index** to **Default**.

f. Click **Save**.

Establish Log Transfers from Cisco Web Security Appliance

Before You Begin

- Know the path to your log files: Create the Folder Structure for Log Files, page 1-6.
- Determine the frequency of transfers, no more than 60 minute increments.

- Open the web interface for the Cisco Web Security Appliance.

Step 1 In the web interface for the Cisco Web Security Appliance, navigate to **System Administration > Log Subscriptions**.

Step 2 Click **Add Log Subscription...**

Step 3 Configure the subscription

Setting	Log Type	Value
Log directory	Access	accesslogs
	Traffic Monitor	trafmonlogs
(Depending on your AsyncOS release) Rollover by File Size Maximum File Size	Either	Recommend no more than 500 Mb.
(Availability of this option varies by AsyncOS release) Rollover by Time	Either	Recommend custom rollover interval of one hour (1h) or more frequent rollovers.
Log Style	Access	Squid
	Traffic Monitor	N/A
(Optional) Custom Fields	Either	%XK (Adds a web reputation threat reason.)
Filename	Either	<user defined>
Retrieval Method	Either	FTP on <hostname_splunk_instance>

Note Accessing online help from the Add Log Subscription page brings up detailed information about all settings.

(Optional) Set Up Department Membership Query

Perform the setup procedure for department membership requirements under these conditions:

- You will use AD/LDAP groups bound to roles in Splunk.
- You will run reports on data that is based on organizational roles.

Related Topics

- Restrict Access to Department Reports by Role, page 1-11

Set Up Department Membership Reporting

Before You Begin

- Linux users: Install ldapsearch tool using the following command:

```
sudo yum install openldap-clients
```

Step 1 Identify the AD/LDAP Group Base DNs in the Membership Script:

a. Open the appropriate membership script in a text editor:

- Linux: $SPLUNK_HOME/etc/apps/CiscoWSA/bin/discovery.py
- Windows: X:\$SPLUNK_HOME\etc\apps\CiscoWSA\bin\discovery.vbs

b. Edit the first four fields at the top of the header:

```
strComputer = 'ad_ldap_host'
strUser = 'cn=service_account,cn=Users,dc=my_directory,dc=net'
strPassword = 'service_account_password'
strGroupOUs = 'Group base DN;Group base DN;Group base DN'
```

c. Save the file.

Step 2 Enable use of the membership script by the inputs.conf Script:

a. Open the inputs.conf script in a text editor:

```
$SPLUNK_HOME/etc/apps/CiscoforIronportWSA/local/inputs.conf
```

b. Search for the appropriate string:

- # membership script Windows
- # membership script Linux

c. Set disabled to false: `disabled = false`

Step 3 Restart Splunk.

Step 4 Verify that the script populated departments.csv with the user data:

```
$SPLUNK_HOME/etc/apps/CiscoWSA/lookups/departments.csv
```

The membership script is set to run every day by default. The interval is set in seconds and can be changed as per the deployment requirements.

Restrict Access to Department Reports by Role

Before You Begin

- Understand that if users are restricted to viewing data from specific departments or groups, Layer 4 Transport Monitor (L4TM) data will only be available to administrators because L4TM data is not linked to a department or role.
- Open Splunk Web

Step 1 In Splunk Web,

- Splunk version 6.1.4: Select **Settings > Access controls > Roles**.
- Splunk version 5.0.10: Select **Manager > Access controls > Roles**.

Step 2 Click New or edit an existing role.

Step 3 Define search restrictions for the role.

Example: To restrict a role to viewing data for the Sales Department, in the Restrict search terms field, type “department=sales”.

Step 4 Click **Save**.

Troubleshooting Department Membership Reporting

Tip

- Linux users: Verify that ldapsearch tool is in the Splunk user’s path.
- Verify that the departments.csv file exists in the application’s lookup folder.
- Windows users: Comment out “option explicit” to reveal more specific information the origin and and cause of an error.
- Verify the LDAP paths are syntactically correct.
- Verify the bind service account name is correct.
- Verify the correct bind password is entered.
- Test connection to the remote machine over port 389.
- Verify the correct attribute was configured for the member name.
- Verify the correct attribute was used for group membership.
- Verify the correct attribute was configured for group name.

(Optional) Set Up Scheduled PDF Reporting

Splunk Web users can generate a scheduled PDF output from any dashboard, view, search or report.

Requirements

Scheduled PDF reporting requires a Linux-based instance of Splunk running on the network. For a minimal installation. However, a standard Linux image with an installation of Splunk configured as a forwarder (no indexing or web interface required) can serve multiple Splunk instances for PDF generation.

Step 1 Download and install the PDF Report Server add-on from Splunk into a Splunk instance on a single Linux host:

http://splunk-base.splunk.com/apps/22348/pdf-report-server-install-on-linux-only

Step 2 Ensure that the Xvfb X server, xauth and fonts for your Linux distribution are installed. These are included with most Linux distributions, but not installed by default. On Red Hat, type:

```
yum install Xvfb xauth bitstream-vera-fonts
```

Step 3 Launch Splunk Web on the Linux host.

Step 4 Do the following:

- Splunk version 6.1.4: Select **Settings > System Settings > Email Settings**.
- Splunk version 5.0.10: Select **Manager > System Settings > Email Alert Settings**.

Step 5 Configure mail and report server settings:

a. Under Mail server settings, enter or update information related to the SMTP server that Splunk interacts with in order to send out alert emails.

b. Identify the SMTP mail host server.

c. Provide an authentication username/password if the SMTP server requires them.

d. (Optional) Specify that Splunk uses SSL or TLS when it communicates with the SMTP server.

e. Under Email format, configure the format of the emails that Splunk sends.

You can define the name that appears in the "sender" field (by default it is Splunk), and you can set up the format of the email subject line (by default it is Splunk Alert: $name$, where $name$ is the name of the search that the alert is based upon). You can also set at the Manager level the default email format for all alerts and whether or not alert emails provide inline results.

If the hostname of the Splunk Web instance that this PDF Report Server will talk to is not resolvable in DNS, enter its IP address or a hostname that resolves to that IP in the Link hostname field. This will ensure that Splunk Web can contact the PDF Report Server, and that links sent in emailed PDF reports work correctly. If the field is left empty, Splunk will try to autodetect the hostname.

f. Enter the **Remote PDF Report Server URL** and select paper options.

g. Click **Save**.

Step 6 To change the splunk core service port: From the %SPLUNK_HOME%\bin directory: splunk set splunkd-port ####

(Optional) Edit the List of URL Categories

Note Do not edit the category code in the first column.

To obtain the pathname to the **url_categories.csv** file:

- Splunk version 6.1.4: Select **Settings > Lookups > Lookup table files**
- Splunk version 5.0.10: Select **Manager > Lookups > Lookup table files**

Additional Reading

- Splunk License Installation:
http://www.splunk.com/base/Documentation/latest/Admin/Installalicense
- Splunk License Violations:
http://www.splunk.com/base/Documentation/latest/Admin/Aboutlicenseviolations

- Backup of Splunk data: http://www.splunk.com/base/Documentation/latest/admin/Backupindexeddata
- How to archive data: http://www.splunk.com/base/Documentation/latest/Admin/Automatearchiving

Reports

Overview of Reports

Cisco Web Security Appliance Advanced Reporting includes a set of predefined reports. As much as possible the reporting is consistent with the native reporting of Cisco Web Security Appliance.

Note Reports generated using Cisco Web Security Appliance Advanced Reporting may show more data than is available through Splunk due to the use of a summary index, which speeds the loading of reports.

Accessing Reports

Before You Begin

Splunk administrators can control the Web Security appliances (hosts) that you see on the Overview report and Web Tracking report. Contact your Splunk administrator with details of any hosts you would like to add, remove, or rename.

Step 1 Access Splunk in a web browser.

Step 2 Sign in.

Step 3 Select **App > Cisco WSA Advanced Reporting**.

Step 4 Choose a report from the **Cisco WSA** menu.

Step 5 Select a time range and WSA host(s), if applicable.

Tip Improve performance by choosing smaller time ranges and crafting searches to be as precise as possible.

Data Formats

In some cases, the formatting of data available through Cisco Web Security Appliance Advanced Reporting differs from the formatting of data available through native reporting functionalities.

Data	Format
Large numbers (greater than seven digits)	2E11 means $2x10^{11}$
Time	d+hh:mm:ss.ms Example: 1+03:22:36.00 1 day, 3 hours, 22 minutes, 36 seconds, 0 milliseconds

Time Range

Tip Select a smaller time range to return results more quickly.

Timing of Data Availability

Range	Indexing Begins	Data Appears in Reports
Hour	Just past the hour	60-90 minutes after indexing begins
Day	After midnight daily	One day after indexing begins
Week	After midnight Saturday (early Sunday morning)	One week after indexing begins
90 Days	After midnight of the 90th day.	90 days after indexing begins.
Custom: Less than hourly	Just past the hour	60-90 minutes after indexing begins
Custom: Less than daily	After midnight daily	One day after indexing begins
Custom: Less than weekly	After midnight Saturday (early Sunday morning)	One week after indexing begins

Tip Use the “jobs” menu to verify that scheduled searches are not running too long. “Too long” is in excess of its frequency, for example, a weekly search running more than a week.

Tip Select the Jobs menu. Each report’s search(es) will have a marker denoting search description & interval summary. For example, search `_dashboard_users_base-search(*,1d)` is leveraging the user’s 1 day summary.

Timing of Summary Index Generation

Summary indexes speed report generation. Summaries are generated once per hour. Each night, hourly summaries are aggregated into daily summaries. Each week, daily summaries are aggregated into weekly summaries.

Summary Search	Frequency
[_dashboard_SOCKS_base-sum-search-top-1h]	Hourly at 10 minutes past
[_dashboard_SOCKS_base-sum-search-top-1d]	Daily at 2:30 AM
[_dashboard_SOCKS_base-sum-search-top-1w]	Weekly at 1:45 AM
[_dashboard_anti-malware_base-sum-search-1h]	Hourly at 35 minutes past
[_dashboard_anti-malware_base-sum-search-1d]	Daily 1:30 AM
[_dashboard_anti-malware_base-sum-search-1w]	Sunday 2:15 AM
[_dashboard_application-visibility_base-sum-search-1h]	Hourly at 15 minutes past
[_dashboard_application-visibility_base-sum-search-1d]	Daily at 12:30 AM
[_dashboard_application-visibility_base-sum-search-1w]	Sunday at 2:45 AM
[_dashboard_overview_base-sum-search-bottom-1h]	Hourly at 50 minutes past
[_dashboard_overview_base-sum-search-bottom-1d]	Daily at 6:00 AM
[_dashboard_overview_base-sum-search-bottom-1w]	Weekly at 3:15 AM
[_dashboard_overview_base-sum-search-top-1h]	Hourly at the top of the hour.
[_dashboard_overview_base-sum-search-top-1d]	Daily at 5:00 AM
[_dashboard_overview_base-sum-search-top-1w]	Weekly at 3:45 AM
[_dashboard_overview_base-sum-search-uid-1h]	Hourly at 40 minutes past
[_dashboard_overview_base-sum-search-uid-1d]	Daily at 4:00 AM
[_dashboard_overview_base-sum-search-uid-1w]	Weekly at 4:15 AM
[_dashboard_url-categories_base-sum-search-1h]	Hourly at 30 minutes past
[_dashboard_url-categories_base-sum-search-1d]	Daily at 3:00 AM
[_dashboard_url-categories_base-sum-search-1w]	Weekly at 5:15 AM
[_dashboard_users_base-sum-search-1h]	Hourly at 20 minutes past
[_dashboard_users_base-sum-search-1d]	Daily at 2:00 AM
[_dashboard_users_base-sum-search-1w]	Weekly at 5:45 AM
[_dashboard_web-reputation-filters_base-sum-search-1h]	Hourly at 45 minutes past

Summary Search	Frequency
[_dashboard_web-reputation-filters_base-sum-search-1d]	Daily at 1:00 AM
[_dashboard_web-reputation-filters_base-sum-search-1w]	Weekly at 4:45 AM
[_dashboard_web-sites_base-sum-search-1h]	Hourly at 55 minutes past
[_dashboard_web-sites_base-sum-search-1d]	Daily at Midnight
[_dashboard_web-sites_base-sum-search-1w]	Sunday at 1:15 AM

Export

Exporting to a .CSV File

Step 1 Generate the report.

Step 2 Select **Export**.

Exporting to a PDF File

Before You Begin

- Verify that the Splunk administrator has enabled PDF output.

Step 1 Generate the report.

Step 2 Select **Save as PDF**.

Related Topics

- (Optional) Set Up Scheduled PDF Reporting, page 1-12

General Versus Specific Data

Predefined general reports provide hyperlinks to predefined specific reports.

Viewing Specifics

Step 1 Select the most appropriate predefined general report.

For example, if you want specific information about a user, begin with the predefined Users report.

Step 2 Click on the hyperlink for the subject for which you want specifics.

For example, click on the hyper-linked user name or IP address for an individual user.

Related Topics

- Export, page 2-4

Search

Simple and advanced search options are available using the Web Tracking Report.

Search Tips

Timesaver Make the search as specific as possible and narrow the time range.

Tip Cisco Web Security Appliance Advanced Reporting uses a set of files to populate menus for the Web Tracking page. If you are experiencing problems with the Web Tracking page menus, verify that these files are in the application's lookups folder:

- malware_categories.csv
- transaction_types.csv
- url_categories.csv

Tip The Splunk administrator can edit the list of URL categories visible within Splunk. When a category appears within the access log, but is not present in the lookup file, Cisco Web Security Appliance Advanced Reporting displays "Custom Category".

Tip Splunk administrators can control the options available in the dropdown fields in the Web Tracking form.

Troubleshooting Searches

The departments.csv is a file used as part of the role based security functionality. This file may be edited manually or by configuring one of the role discovery scripts (available in the application's bin folder) as a scripted input. There is a script for both Linux and Windows.

- Ensure the file exists in the application's lookup folder
- If the Linux version is used, ensure the CLI ldapsearch is installed and in the Splunk user's path
- If the Windows version is used "option explicit" may be commented out to reveal more specific information regarding from where and why an error may have originated.
- Verify the LDAP paths are syntactically correct

- Verify the bind service account name is correct
- Verify the correct bind password is entered
- Test connection to the remote machine over port 389
- Verify the correct attribute was configured for the member name
- Verify the correct attribute was used for group membership
- Verify the correct attribute was configured for group name

Predefined Reports

List of General Reports

- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor

List of Specific Reports

- Malware Category
- Malware Threat
- Application
- Application Type
- Domain
- URL Category
- User
- Reports by Location
  - Overview by Location
  - URL Categories by Location
  - Anti-Malware by Location
  - Web Reputation Filters by Location
  - Application Visibility by Location
  - Users by Location

  - Websites by Location

Related Topics

- Search, page 2-5

Usage Scenarios

User Investigation

This example demonstrates how a system administrator would investigate a particular user at a company. In this scenario, a manager has received a complaint that an employee is visiting inappropriate web sites at work. To investigate this, the system administrator now needs to look at the employee's web usage trends and transaction history:

- URL Categories by Total Transactions
- Trend by Total Transactions
- URL Categories Matched
- Domains Matched
- Applications Matched
- Malware Threats Detected
- Policies Matched for a particular User ID or Client IP.

Using these reports, the system administrator can discover whether, for example, user "johndoe" was trying to access blocked URLs, which can be viewed in the Transactions Blocked column under the Domains section.

Viewing Web Usage Trends

Step 1 Select **Users** from the Cisco WSA Advanced Reporting dropdown menu.

Step 2 Click on the User ID or Client IP address.

Note If you do not see the User ID or Client IP address you want to investigate in the Users table, click on any User ID or Client IP. Then search for all or part of the User ID or Client IP address.

Step 3 (Optional) Select **Actions > Print**.

Viewing Transaction History

Step 1 Select **Web Tracking** from the Cisco WSA Advanced Reporting dropdown menu.

Step 2 **Search** for the User/Client IP Address.

Step 3 Click **Pick fields** above the transaction list to change the information displayed for each transaction.

Step 4 (Optional) Click **Export** to export the data to a CSV file.

URLs Visited

In this scenario, a Sales manager wants to discover the top five visited web sites at their company for the last week. Additionally, the manager wants to know which users are going to those websites.

Viewing Most Visited Web Sites

Step 1 Select **Web Sites** from the Cisco WSA Advanced Reporting dropdown menu.

Step 2 Select **Week** from the Time Range drop-down list.

Step 3 View the top 25 domains in the Domains Matched table.

Step 4 Click on a domain to view the users who have visited that domain in order of frequency.

URL Categories Visited

In this scenario, the Human Resources manager wants to know what the top three URL categories her employees have visited over the past 30 days. Additionally, a network manager wants to get this information to monitor bandwidth usage, to find out what URLs are taking up the most bandwidth on her network. The example below is to show how you can gather data for several people covering several points of interest, while only having to generate one report.

Viewing Most Common URL Categories

Before You Begin

- (Optional) Set Up Scheduled PDF Reporting, page 1-12

Step 1 Select **URL Categories** from the Cisco WSA Advanced Reporting dropdown menu.

Step 2 View the top ten URL Categories by Total Transactions graph.

Step 3 Select **Actions>Schedule for PDF Delivery**.

Step 4 Send the PDF to the Human Resources manager.

Step 5 View the Bytes Allowed column in the URL Categories Matches table.

Step 6 Select **Actions>Schedule for PDF Delivery**.

Step 7 Send the PDF file to the Network Manager.

Step 8 For finer granularity, click on a specific URL Category.

CHAPTER 3

Field Extractions

Overview of Field Extractions

This application relies heavily on field extractions. As most reports are generated from summary data, it is important to ensure that fields are being extracted correctly to enable successful and accurate reporting.

Access Logs

Tip

- Ensure timestamps are correctly being indexed
- Search for "*" and ensure app-specific fields are populated in the field picker. The next bullet item contains a more thorough examination of extracted fields
- Copy and paste the below search. You should not see any results and especially not very many results. If 1000 results are returned – the transforms.conf will need to be adjusted for the unique log format being indexed…

```
sourcetype=wsa_accesslogs | head 1000 | fillnull value="!!!!"
x_webcat_code_abbr x_wbrs_score x_webroot_scanverdict
x_webroot_threat_name x_webroot_trr x_webroot_spyid
x_webroot_trace_id x_mcaffe_scanverdict x_mcafee_filename
x_mcafee_scan_error x_mcafee_detecttype x_mcafee_av_virustype
x_mcafee_virus_name x_sophos_scanverdict x x_sophos_filename
x_sophos_virus_name x_ids_verdict x_icap_verdict
x_webcat_req_code_abbr x_webcat_resp_code_abbr
x_resp_dvs_threat_name x_wbrs_threat_type x_avc_app x_avc_type
x_avc_behavior x_request_rewrite x_avg_bw x_bw_throttled
x_user_type
x_resp_dvs_verdictnamex_req_dvs_threat_namex_suspect_user_agent
x_wbrs_threat_reason dvc_time duration dvc_ip result http_status
bytes_in http_method dest_url user_id_dom hierarchy hierarchy_domain
```

```
mime_type acl_tag user_id user_domain dest_domain | stats count by
x_webcat_code_abbr x_wbrs_score x_webroot_scanverdict
x_webroot_threat_name x_webroot_trr x_webroot_spyid
x_webroot_trace_id x_mcaffe_scanverdict x_mcafee_filename
x_mcafee_scan_error x_mcafee_detecttype x_mcafee_av_virustype
x_mcafee_virus_name x_sophos_scanverdict x x_sophos_filename
x_sophos_virus_name x_ids_verdict x_icap_verdict
x_webcat_req_code_abbr x_webcat_resp_code_abbr
x_resp_dvs_threat_name x_wbrs_threat_type x_avc_app x_avc_type
x_avc_behavior x_request_rewrite x_avg_bw x_bw_throttled
x_user_type
x_resp_dvs_verdictnamex_req_dvs_threat_namex_suspect_user_agent
x_wbrs_threat_reason dvc_time duration dvc_ip result http_status
bytes_in http_method dest_url user_id_dom hierarchy hierarchy_domain
mime_type acl_tag user_id user_domain dest_domain | convert
ctime(dvc_time) | search user_id="!!!!" AND host="!!!!" AND
src_ip="!!!!" AND cause="!!!!" AND action="!!!!" AND
dest_domain="!!!!"
```

- Verify the host extractions are correct. This is part of the inputs strategy discussed in the installation guide. The folder structure should be appropriately established to allow proper host extractions to occur.
- Hosts may be renamed per the section of this guide that discusses the host lookup file

Traffic Monitor Logs

The L4TM reports are generated from L4TM data (not summary data). Field extractions will still need to be operable for those reports to function. Though the format is not as versatile as accesslogs, they may still be verified with the same technique.

Tip Use this search to verify that there are few or no results:

```
sourcetype=wsa_trafmonlogs | head 1000 | fillnull value="!!!!"
dvc_time log_level action proto src_ip src_port dest_ip dest_host
dest_port | stats count by dvc_time log_level action proto src_ip
src_port dest_ip dest_host dest_port | search src_ip="!!!!"
```

INDEX