



Cisco Advanced Web Security Reporting 6.3 Installation, Setup, and User Guide

Published: April 23, 2018

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

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: www.cisco.com/go/trademarks. 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. (1110R)

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 Advanced Web Security Reporting 6.3 Installation, Setup, and User Guide
© 2013-2018 Cisco Systems, Inc. All rights reserved.



Installation and Setup	1-1
Introduction	1-1
What's New	1-2
New in Release 6.3	1-2
New in Release 6.2	1-2
New in Release 6.1	1-2
New in Release 6.0	1-3
Supported and Unsupported Features	1-3
System Requirements and Sizing & Scaling Recommendations	1-3
Set-up Overview	1-3
Installing Cisco Advanced Web Security Reporting 6.2 and Later	1-4
On Linux	1-4
On Windows	1-5
Upgrading to Cisco Advanced Web Security Reporting 6.2 and Later	1-6
Upgrading from Version 4.0 or Later	1-6
On Linux	1-6
On Windows	1-7
Upgrading from Version 3.0 to Version 6.x	1-7
Users	1-8
Administrative Users	1-8
Creating New Users	1-8
Notes about Authentication/Authorization	1-8
Enterprise Basic Authentication	1-9
Configuration Best Practices	1-9
Commands To Start and Stop the Cisco Advanced Web Security Reporting Application	1-9
On Linux	1-9
On Windows	1-10
Licensing and Migration	1-10
Migration from v3.0 (Web Security Appliance) to v4.0 (Web Security Appliance-only) Reporting	1-10
Migration from v3.0 (Web Security Appliance-only) to v4.0 Hybrid Reporting	1-10
New Hybrid Reporting License	1-11
Hybrid Reporting License Issues	1-11
Licensing Considerations for Version 4.0 and Later Upgrades	1-11

License Installation	1-12
Create the Folder Structure for Access and Traffic Monitor Log Files	1-12
Import and Index Historical Data	1-12
(Optional) Configure the Application to Delete Log Files After Indexing	1-13
Set Up On-going Data Transfers	1-13
Configure Data Inputs for Web Security Appliance Logs	1-14
Configuration Of Data Input for Web Security Appliance Syslogs	1-14
Establish Log Transfers from A Web Security Appliance	1-15
Configure CWS or Umbrella Log Updates	1-17
Set Up Department Membership Query (Optional)	1-17
Set Up Department Membership Reporting	1-17
Restrict Access to Department Reports by Role	1-19
Troubleshooting Department Membership Reporting	1-19
Set Up Scheduled PDF Reporting (Optional)	1-20
Configure Email Alerts	1-20
Schedule PDF Report Generation	1-20
Filters and Dashboards	2-1
Overview of Filters and Dashboards	2-1
Viewing Dashboards	2-1
Predefined Dashboards	2-2
Save As Dashboard	2-4
Editing A Custom Dashboard	2-4
Creating A Custom Filter	2-5
Changing and Saving the Custom Filter Display	2-6
Saving a Custom Filter as a Dashboard	2-7
Exporting Data	2-8
Exporting the Current Custom Filter Panel	2-8
Exporting the Current Dashboard to a PDF File	2-9
Data Formats	2-9
Time Ranges	2-9
Timing of Data Availability	2-9
Troubleshooting	2-11
Usage Scenarios	2-11
User Investigation	2-11
Viewing Web Usage Trends	2-12
Viewing Transaction History	2-12
URLs Visited	2-12

Viewing Most Visited Web Sites	2-12
URL Categories Visited	2-12
Viewing Most Common URL Categories	2-13
CEF Extractor	3-1
About the CEF Extractor Service	3-1
Setting Up the CEF Extractor Service	3-1
Setting Up a CEF Peer	3-1
Configuring the AWSR Master	3-2
Configuring Licensing	3-3
Peer Licensing	3-3
Master Licensing	3-3
CEF Extractor Initial Configuration	3-4
Restart the Master System	3-4
Configure Mapping of Access Logs to CEF Output Fields	3-4
Configure Data Input for the CEF Extractor Service	3-6



Installation and Setup

- [Introduction, page 1-1](#)
- [System Requirements and Sizing & Scaling Recommendations, page 1-3](#)
- [Set-up Overview, page 1-3](#)
- [Installing Cisco Advanced Web Security Reporting 6.2 and Later, page 1-4](#)
- [Upgrading to Cisco Advanced Web Security Reporting 6.2 and Later, page 1-6](#)
- [Licensing and Migration, page 1-10](#)
- [Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-12](#)
- [Import and Index Historical Data, page 1-12](#)
- [Set Up On-going Data Transfers, page 1-13](#)
- [Configure CWS or Umbrella Log Updates, page 1-17](#)
- [Set Up Department Membership Query \(Optional\) , page 1-17](#)
- [Set Up Scheduled PDF Reporting \(Optional\), page 1-20](#)

Introduction

The Cisco Cisco Advanced Web Security Reporting application provides filters and dashboards that are designed to give insight into very large volumes of data from multiple Web Security Appliances, Cloud Web Security (CWS) gateways, and Cisco Umbrella. The Cisco Advanced Web Security Reporting application includes a data collection-and-display application, and a related server that forwards log data collected from Web Security Appliances (WSAs), CWS services, and an Umbrella host.



Note

Cloud Web Security is sometimes referred to as “ScanSafe.”

The Cisco Advanced Web Security Reporting application receives log data and stores it in data models. You can view these data using searches, or “filters,” that you define.

What's New

- [New in Release 6.3, page 1-2](#)
- [New in Release 6.2, page 1-2](#)
- [New in Release 6.1, page 1-2](#)
- [New in Release 6.0, page 1-3](#)

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 Cisco 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 [Configuration Best Practices, page 1-9](#) and [Restrict Access to Department Reports by Role, page 1-19](#).

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 WSAs 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.”
Web Security appliance AsyncOS 10.0 changes	AMP enhancements and Referrer header-related support.

Supported and Unsupported Features

Component	Supported	Not Supported
Server	Single-server deployments	Multiple-server deployments
Transport Methods	FTP (files and directories) TCP (syslogs)	
PDF	Integrated PDF generation Scheduled PDF Reporting	
Custom Dashboards	For each predefined report, use Save As Dashboard to create a custom dashboard for selected time range, source type and host (limited). For each custom filter, use Save As Dashboard to create a custom dashboard for selected Filter fields from access, SOCKS or AMP logs.	

System Requirements and Sizing & Scaling Recommendations

System requirements, as well as sizing and scaling recommendations, are detailed in the *Cisco Advanced Web Security Reporting Release Notes*, available from

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html>

Set-up Overview

- Install Cisco Advanced Web Security Reporting for the first time:
 - [Installing Cisco Advanced Web Security Reporting 6.2 and Later](#), page 1-4
 - [Licensing and Migration](#), page 1-10
 - [Create the Folder Structure for Access and Traffic Monitor Log Files](#), page 1-12
 - [Import and Index Historical Data](#), page 1-12
 - [Set Up On-going Data Transfers](#), page 1-13 (Including setup of Web Security Appliance.)
 - [Configure CWS or Umbrella Log Updates](#), page 1-17

- [Upgrading to Cisco Advanced Web Security Reporting 6.2 and Later, page 1-6](#)

Installing Cisco Advanced Web Security Reporting 6.2 and Later

Follow the steps in this section to install Cisco Advanced Web Security Reporting.

- [On Linux, page 1-4](#)
- [On Windows, page 1-5](#)

On Linux

Perform the following tasks in order.

Step 1 Download the installer for the version of the Cisco Advanced Web Security Reporting required:
<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=282803425&softwareid=283998384>

Step 2 Extract the installer software.

- To install into the current working directory, use this command:

```
tar zxvf cisco_wsa_reporting-x.x.x.tgz.
```

x.x.x - Enter the version number of software.

Example

```
tar zxvf cisco_wsa_reporting-6.3.0.tgz.
```

- To install into `/opt/cisco-wsa_reporting/` directory, use the following command:

```
tar zxvf cisco_wsa_reporting-x.x.x.tgz -C /opt
```

x.x.x - Enter the version number of software.

Example

```
tar zxvf cisco_wsa_reporting-6.3.0.tgz -C /opt
```

Step 3 Change directory to `/cisco_wsa_reporting/` and run the set-up script:

```
cd cisco_wsa_reporting  
./setup.sh
```

- If the result of this command is:

```
./setup.sh: Permission denied
```

- a. Change the permission level of the script `/setup.sh` by using the following command:

```
chmod 777 /setup.sh
```

- b. Re-run the script.

The progress, and milestone statements are displayed during set-up.

- Step 4** Launch Cisco Advanced Web Security Reporting, and log in:
- Navigate to `http://<hostname>:8888` in a browser window.



Note Earlier versions used port 8000; since version 4.0, the port 8888 is used.

- Log in with the user name `admin` and `Cisco@dmin` as the password.
 - Change the `admin` password.
-

Next Steps

- [Licensing and Migration, page 1-10](#)

On Windows

Before You Begin

Windows allows only one installed version of Cisco Advanced Web Security Reporting. If you have an earlier version installed, you must back-up your existing data and uninstall the previous version before installing the new version.

-
- Step 1** Download the installer for the version of the Cisco Advanced Web Security Reporting required:
- <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=282803425&softwareid=283998384>
- Step 2** Extract the installer. You can use applications such as 7-Zip, WinZip, etc.
- Step 3** Launch a command-line shell (PowerShell) as Administrator, and change the directory to which you extracted the installer.
- Step 4** Use the `\install.bat` command to run `install.bat`.
- The application is installed in the folder `C:\Program Files\Cisco\CiscoWSAReporting`.
- Step 5** Reboot the Cisco Advanced Web Security Reporting server.
- Step 6** Launch the Cisco Advanced Web Security Reporting application and log in:
- Navigate to `http://<hostname>:8888` in a browser window.



Note Earlier versions used port 8000; since version 4.0, the port 8888 is used.

- Log in with the user name `admin` and `Cisco@dmin` as the password.
 - Change the `admin` password.
-

Next Steps

- [Licensing and Migration, page 1-10](#)

Upgrading to Cisco Advanced Web Security Reporting 6.2 and Later

- [Upgrading from Version 4.0 or Later, page 1-6](#)
- [Upgrading from Version 3.0 to Version 6.x, page 1-7](#)

Upgrading from Version 4.0 or Later

As part of the upgrade process, an evaluation license is applied for using Umbrella logs.

Follow the steps in this section to upgrade from version 4.0 or version 4.5 to a 6.x version.

- [On Linux, page 1-6](#)
- [On Windows, page 1-7](#)

On Linux

These tasks must be performed in order:

-
- Step 1** Download the installer for the version of the Cisco Advanced Web Security Reporting required:
- <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=282803425&softwareid=283998384>
- Step 2** Copy the downloaded installer file into the base directory for the `cisco_wsa_reporting` directory. For example, if the earlier version of Cisco Advanced Web Security Reporting is installed in `/opt/cisco_wsa_reporting/`, then place the `.tgz` file in the `/opt/` directory.
- Step 3** Change directory to the installation's base directory (for example, `/opt/`).
- Step 4** Use the command below to extract the installer. In the example below, version 6.2 is used. You will have to use the appropriate version number with the command.
- ```
tar -zxvf CiscoAdvancedWebSecurityReporting_Linux_6_2_0-002.tgz
cisco_wsa_reporting/SeamlessUpgrade.sh; cp -f cisco_wsa_reporting/SeamlessUpgrade.sh
```
- Step 5** Run the upgrade script. In the example below, version 6.2 is used. You will have to use the appropriate version number with the command.
- ```
./SeamlessUpgrade.sh CiscoAdvancedWebSecurityReporting_Linux_6_2_0-002.tgz
```
- If the result of this command is:


```
./SeamlessUpgrade.sh: Permission denied
```

 - Change the permission level of the script `SeamlessUpgrade.sh` by issuing the following command:


```
chmod 777 SeamlessUpgrade.sh
```
 - Re-run the script.
-

On Windows

These tasks must be performed in order:

-
- Step 1** Download the installer for the version of the Cisco Advanced Web Security Reporting required:
<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=282803425&softwareid=283998384>
- Step 2** Extract the installer; you can use applications such as 7-Zip, WinZip, etc.
- Step 3** Launch a command-line shell (PowerShell) as Administrator and change directory to the directory to which you extracted the installer.
- Step 4** Use the command `.\WinSeamlessUpgrade.ps1` to upgrade Cisco Advanced Web Security Reporting.
-

Upgrading from Version 3.0 to Version 6.x

You must follow the steps in this section to upgrade your version 3.0 installation for version 6.x. Upgrading from a version 3.0 installation involves these basic steps:

- Make a back-up copy of the existing version 3.0 indexed data.
- Shut down the newly installed version 6.x application.
- Copy the version 3.0 back-up data to the new data directory.
- Restart the version 6.x application.

Detailed steps follow.

For these instructions, we assume that version 3.0 is running in `/opt/splunk` and the new version is in `/opt/cisco_wsa_reporting`. Adjust your paths accordingly.

-
- Step 1** Stop the old version:
- ```
/opt/splunk/bin/splunk stop
```
- Step 2** Edit the old `inputs.conf` file  
(`/opt/splunk/etc/apps/SplunkforCiscoIronportWSA/local/inputs.conf`) and disable all inputs.
- Step 3** Restart the old version:
- ```
/opt/splunk/bin/splunk start
```
- Step 4** Verify that there are no hot buckets left in the main index:
- ```
cd /opt/splunk/var/lib/splunk/defaultdb/db
ls -la hot* (verify no results)
```
- Step 5** Stop the old version again:
- ```
/opt/splunk/bin/splunk stop
```
- Step 6** Verify that the new version is not running:
- ```
/opt/cisco_wsa_reporting/shutdown.sh
```
- Step 7** Clean the indexes folders of the new version:
- ```
cd /opt/cisco_wsa_reporting/var/lib/splunk
```

```
rm -rf *
```

Step 8 Copy indexes from old version to new version:

```
cd /opt/cisco_wsa_reporting/var/lib/splunk
cp -r /opt/splunk/var/lib/splunk/defaultdb .
cp -r /opt/splunk/var/lib/splunk/fishbucket .
```

Step 9 Start the new version of Cisco Advanced Web Security Reporting:

```
/opt/cisco_wsa_reporting/startup.sh
```

Step 10 In a browser, open `http://<wsa_reporting_server_host_name>:8888` and log in with the user name `admin` and password `Cisco@dmIn`.

Users

The Cisco Advanced Web Security Reporting application provides two administrative users. You can also create users and assign roles already available or create a new role. See [Restrict Access to Department Reports by Role, page 1-19](#).

Administrative Users

The Cisco Advanced Web Security Reporting application provides two administrative users:

- The “default admin” (user name: `admin` and password: `Cisco@dmIn`) will have access to all administration functionality.

The `admin` user can install licenses and configure the distributed environment. Use this account to configure, test, and troubleshoot.

- The second administrative user (name: `wsa_admin` and password: `Ironp0rt`) has access to a subset of administration functionality.

We recommend that you change both passwords immediately after installation (**Settings > Users and Authentication > Access Controls > Users**).

Creating New Users

Apart from administrative users, you can also create new users:

Step 1 Choose **Settings > Users and Authentication > Access controls > Users**.

Step 2 Click **New**.

Step 3 Enter a **Username**, and assign a role. See [Restrict Access to Department Reports by Role, page 1-19](#).

Step 4 Set a password.

Step 5 Click **Save**.

Notes about Authentication/Authorization

- Enterprise basic authentication
- AD/LDAP

Enterprise Basic Authentication

Local authentication supersedes any other authentication option configured.

Default authentication set up:

- As `admin`, define users and their privileges.
- Add users to an Enterprise-specific group in the directory services.
- Import that group DN into the Enterprise application.
- Either map the most appropriate default Enterprise 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 Enterprise data, then using local authentication may be sufficient.

Missing AD/LDAP section. Provide info please

Configuration Best Practices

- Set time zones consistently across Web Security appliances, CWS appliances, and the Umbrella host.
The time displayed in the search results reflects the 'local' time of the Cisco Advanced Web Security Reporting instance. By default, all inputs for the appliance logs are set to TZ = GMT.
- Document the local `admin` account password (regardless of the chosen authentication method).
- Enable data model acceleration if role based reporting is not used.
 - a. Choose **Settings > Data > Data Acceleration**.
 - b. Click **Edit**.
 - c. Select **Edit Acceleration**.
 - d. Check the **Accelerate** check box, and select 3 months as **Summary Range**.
 - e. Click **Save**.

Commands To Start and Stop the Cisco Advanced Web Security Reporting Application

On Linux

To stop the Cisco Advanced Web Security Reporting application:

Change directory to `/cisco_wsa_reporting/` and issue this command:

```
./shutdown.sh
```

To start the Cisco Advanced Web Security Reporting application:

Change directory to `/cisco_wsa_reporting/` and issue this command:

```
/startup.sh
```

On Windows

To stop the Cisco Advanced Web Security Reporting application:

Change directory to `<install_home>\` and issue this command:

```
shutdown.bat
```

To start the Cisco Advanced Web Security Reporting application:

Change directory to `<install_home>\` and issue this command:

```
startup.bat
```



Note

On Windows, `<install_home>\` is `C:\Program Files\Cisco\CiscoWSAReporting`.

Licensing and Migration

The three AMP reports added in version 4.5 are supported for Web Security appliance AMP logs only.

Since version 4.0, the Advanced Web Security Reporting application provides support for both WSA and CWS log reports, which is referred to as “hybrid reporting.” To use hybrid reporting, you must install a new license. You can continue to use Web Security appliance-only reporting with your existing license. The various licensing and migration scenarios are:

- [Migration from v3.0 \(Web Security Appliance\) to v4.0 \(Web Security Appliance-only\) Reporting](#)
- [Migration from v3.0 \(Web Security Appliance-only\) to v4.0 Hybrid Reporting](#)
- [New Hybrid Reporting License](#)

Migration from v3.0 (Web Security Appliance) to v4.0 (Web Security Appliance-only) Reporting

You can install the version 4.0 or later software and your previously installed license will continue to provide Web Security appliance reporting. Further, an evaluation license is embedded in the version 4.0 and later software; this license includes the additional reporting source types that will let you evaluate hybrid reporting.

Migration from v3.0 (Web Security Appliance-only) to v4.0 Hybrid Reporting

As mentioned in the previous section, you can install the version 4.0 or later software and your previously installed license will continue to provide Web Security appliance reporting. In addition, the embedded evaluation license will let you evaluate the hybrid reporting feature.

In order to migrate from Web Security appliance-only to hybrid reporting, you must open a [Cisco Technical Assistance Center \(TAC\)](#) support case to remove your existing license and install a new hybrid-reporting license that includes the complete list of source types including `ciscocws` and `ciscoumbrella`. <https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case>

**Note**

Contacting TAC is necessary only if you are upgrading from version 3.0 Web Security appliance-only reporting to version 4.0 or later hybrid reporting.

New Hybrid Reporting License

After installing the version 4.0 or later software as a new Cisco Advanced Web Security Reporting user, to utilize Web Security appliance and Hybrid Web Security reporting, you can use the embedded evaluation license with no limitations during the term of the evaluation. To continue after the evaluation term, or to provide reporting beyond the evaluation limits, you must acquire a master hybrid license. With a new installation, utilize the infodoc supplied with your order to request the license.

Hybrid Reporting License Issues

If you encounter hybrid-reporting issues, before contacting Cisco, verify that you have purchased the appropriate Umbrella package. For CWS, ensure that you have a CWS Log Extraction license (L-CWS-LOG-LIC=), and that you have set up your environment to import CWS logs.

In addition, ensure that the reporting-application license (issued with purchase of SMA-WSPL-LIC=, SMA-WSPL-LOW-LIC=, or SMA-WSPL-HIGH-LIC=) includes **only** the following source types: `wsa_trafmonlogs`, `wsa_accesslogs`, `wsa_w3clogs`, `wsa_syslog`, `wsa_amplogs`, and especially `ciscocws`.

Using Cisco's Cisco Advanced Web Security Reporting application to process logs of any other source type, for example `ps`, will produce a license-violation error. This can happen if you install other applications which produce logs with alternate source types.

Licensing Considerations for Version 4.0 and Later Upgrades

Initially, you will need at least an evaluation license good for a large volume of data to handle the historical data transfer. After that, you will need an Cisco Advanced Web Security Reporting license.

1. Consider the quantity of data to be indexed both during initial historical data upload, and on an on-going daily basis.
2. Acquire and upload an evaluation license sufficient for the historical data transfer.
3. Acquire and upload an Cisco Advanced Web Security Reporting license sufficient for the anticipated data of the applicable source type to be indexed.
4. Change the license type from Trial to Evaluation or Cisco Advanced Web Security Reporting.
5. Ensure that indexes are reported to the correct pool:
 - a. Navigate to **Settings > System > Licensing** and find the "Pools Indexers Volume used today" row under the appropriate license stack.
 - b. If necessary, you can click **Edit** to change the maximum daily volume allocation, and the indexers assigned.
 - c. Click **Cancel** if you made no changes, or **Submit** if you made changes.

License Installation

To obtain licenses, please refer to the information provided when you placed your order. Follow these steps to install Cisco Advanced Web Security Reporting license(s):

-
- Step 1** Launch the Cisco Advanced Web Security Reporting application (enter `http://<hostname>:8888` in a browser window) and log in as the default `admin` user.
 - Step 2** Navigate to **Settings > System > Licensing**.
 - Step 3** Click **Add license**.
 - Step 4** Browse to your XML license file.
 - Step 5** Click **Install**.
-

Create the Folder Structure for Access and Traffic Monitor Log Files

Log	Default Path	Variables
Traffic Monitor	/\$Input_base/wsa_hostname/trafmonlogs/	\$Input_base=path of root FTP folder host_name=Web Security appliance
Access	/\$Input_base/wsa_hostname/accesslogs/	\$Input_base=deployment host_name=Web Security appliance
AMP	/\$Input_base/wsa_hostname/amplogs/	\$Input_base=deployment host_name=Web Security appliance

Import and Index Historical Data

Before You Begin

- Complete configuration tasks listed in [Upgrading to Cisco Advanced Web Security Reporting 6.2 and Later, page 1-6](#).
- Know the folder structure. See [Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-12](#).

-
- Step 1** Copy the historical log files into the folder structure for log files.
 - Step 2** In the Cisco Advanced Web Security Reporting application, log in as `admin`.
 - Step 3** Verify that data is being imported:
 - a. Select **Settings > Data > Indexes**.
 - b. Scroll down to the summary row.

- c. Verify that the Earliest event and Latest event columns display reasonable dates. If the historical data import was run under an evaluation license, install the default license downloaded for the account, and remove any non-production licenses.

**Tip**

If you find that the application is not indexing files for any type of configured input because of a checksum error, add the line `crcSalt = <source>` to each input stanza in the `inputs.conf` file. (The following section, [\(Optional\) Configure the Application to Delete Log Files After Indexing](#), describes editing the `inputs.conf` file.)

What to Do Next

- [Configure Data Inputs for Web Security Appliance Logs](#), page 1-14.

(Optional) Configure the Application to Delete Log Files After Indexing

Before You Begin

If the file `inputs.conf` does not exist in the directory

`<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/`, create the input-configuration file:

`<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf`.

Step 1 Using a text editor, open

`<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf`.

Step 2 Add a segment as below:-

```
[batch:///home/logger/incoming/wsa176.wga/accesslogs/*]
host_segment = 4
disabled = false
sourcetype = wsa_accesslogs
move_policy = sinkhole
```

Where the first line is the FTP directory path where Web Security appliance logs are sent. The second line is the part of the FTP path containing the host name. The third line enables this FTP input. The fourth line specifies the source of this input. The final line, `move_policy = sinkhole`, enables deletion of the original data once it is indexed.

Step 3 Save the `inputs.conf` file and then restart the Cisco Advanced Web Security Reporting application by navigating to **Settings > System > Server controls** and clicking **Restart**.

Set Up On-going Data Transfers

Before You Begin

- [Import and Index Historical Data](#), page 1-12
- Know the path to your log files: [Create the Folder Structure for Access and Traffic Monitor Log Files](#), page 1-12.

- Log into the Cisco Advanced Web Security Reporting application as `admin`.

Configure Data Inputs for Web Security Appliance Logs



Note To configure data input from multiple WSAs, repeat the following steps for each host.

-
- Step 1** In the Cisco Advanced Web Security Reporting application:
- Choose **Settings > Data > Data inputs > Files & directories**.
- Step 2** Disable any inputs labeled `CiscoWSA`.
- Step 3** Click **New**.
- Step 4** Enter the full path to the FTP directory to which Web Security appliance logs will be sent. This path, and the FTP path provided on the Web Security appliance's Log Subscription page must match.
- Step 5** Click **Next**.
- Step 6** Click **New**.
- Step 7** Enter the **Source Type**, select the **Source Type Category**, and enter the **Source Type Description**.
- `wsa_accesslogs` - These are used for all reports except layer 4 traffic monitor & Advanced Malware Protection reports.
- `wsa_trafmonlogs` - These are used for layer 4 traffic monitor reports.
- `wsa_amplogs` - These are used for Advanced Malware Protection reports.
- Step 8** Choose **Advanced Web Security Reporting 6.2.0** from the App Context drop-down list.
- Step 9** Click **Constant value** and enter the Web Security appliance host name in the **Host field value** field.
- Step 10** Choose **Main** as the destination **Index**.
- Step 11** Click **Review** and review the values you provided.
- Step 12** Click **Submit**.



Note You can navigate to **Settings > Data > Data inputs > Files & directories** to confirm the new data input entry.

Configuration Of Data Input for Web Security Appliance Syslogs

-
- Step 1** In the Cisco Advanced Web Security Reporting application:
- Choose **Settings > Data > Data inputs > TCP**.
- Step 2** Click **New**.
- Step 3** Click the **TCP** button and enter `514` in the **Port** field; leave the rest of the fields blank.
- Step 4** Click **Next**.
- Step 5** Click **New**.
- Step 6** Enter `wsa_syslog` in the **Source type** field.

- Step 7** Choose **Advanced Web Security 6.2.0** as the **App Context**.
- Step 8** In the Host section, click **Custom** as the **Method**, and then enter the Web Security appliance host name as the **Host field value**.
- Step 9** Choose **Main** as the destination Index.
- Step 10** Click **Review** and review the values you provided.
- Step 11** Click **Submit**.
- Step 12** Navigate to **Settings > Data Inputs > TCP** to confirm the new input entry.

**Note**

With a multiple-appliance configuration, you must repeat these steps from the Cisco Advanced Web Security Reporting application for each appliance. However, you also can configure multiple appliances by editing the `inputs.conf` file.

Nandhu is going to determine if there is a way to configure multiple appliances in one go in the UI

Establish Log Transfers from A Web Security Appliance

Before You Begin

- Know the path to your log files: [Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-12](#).
- Determine the frequency of transfers, no more than 60-minute increments.
- Open the web interface for the Web Security Appliance.

- Step 1** In the Web interface for the Web Security Appliance, navigate to **System Administration > Log Subscriptions**.
- Step 2** Click **Add Log Subscription**, or click the name of an existing subscription to edit it.
- Step 3** Configure the subscription (this example refers specifically to access, AMP engine and traffic-monitor logs):

Setting	Log Type	Value
Log Type	Access	accesslogs
	Traffic Monitor	trafmonlogs
	AMP Engine	amp_logs
Log Name	Any one	Name for the log directory.
(Depending on your AsyncOS release) Rollover by File Size Maximum File Size	Any one	Recommend no more than 500 MB.

Setting	Log Type	Value
(Availability of this option varies by AsyncOS release) Rollover by Time	Any one	Recommend custom rollover interval of one hour (1h) or more frequent rollovers. For AMP logs, recommend one minute (1m).
Log Style	Access	Squid
	Traffic Monitor	N/A
	AMP Engine	N/A
Log Level	Access	N/A
	Traffic Monitor	N/A
	AMP Engine	Select Debug . Note It is important to change Log Level to Debug for AMP reporting, or little to no information will be reported.
(Optional) Custom Fields	Access only	%XK (Adds a web reputation threat reason.)
Retrieval Method FTP on Remote Server	Any one	Hostname: IP address or host name of the Cisco Advanced Web Security Reporting host. Directory: name of Cisco Advanced Web Security Reporting instance directory. Username/Password: FTP user name and password for access to application. Note If connection between Cisco Advanced Web Security Reporting and Web Security appliance is lost, logs for that period are not available until connection is restored.
Retrieval Method Syslog Push	Either	Hostname: IP address or host name of the Cisco Advanced Web Security Reporting host. Protocol: TCP . Facility: choose auth . Note If connection between Cisco Advanced Web Security Reporting and Web Security appliance is lost, logs for that period are not available until connection is restored.

**Note**

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

Configure CWS or Umbrella Log Updates

Before You Begin

- Log into the Cisco Advanced Web Security Reporting application as `admin`.

-
- Step 1** In the Cisco Advanced Web Security Reporting application:
- Choose **Settings > Data > Data inputs > Cisco CWS/Umbrella Logs**.
- Step 2** Click **New**.
- Step 3** Enter a **name** for this data input.
- Step 4** Enter the **client_id**, **s3_key** and **s3_secret** that have been provided by CWS or Umbrella. The **client_id** is the bucket ID used in CWS, or the AWS bucket name for Umbrella.
- Step 5** Click the **More settings** check box and provide the time **Interval** in seconds at which CWS or Umbrella logs can be pulled; default is 3600.
- Step 6** Choose **Manual** in the **Set sourcetype** drop-down list.
- Step 7** Enter the **Source type**. Enter `ciscocws` (for CWS reports), or `ciscoumbrella` (for Umbrella reports).
- Step 8** Click **Next**.
- Step 9** A success screen is displayed.
-



Note You can navigate to **Settings > Data > Data inputs > Cisco CWS Logs** to confirm the new data input entry.

Set Up Department Membership Query (Optional)

Perform the set-up procedure for department membership requirements under these conditions:

- You will use AD/LDAP groups bound to roles in the Cisco Advanced Web Security Reporting application.
- You will run reports on data that are based on organizational roles.

Related Topic

- [Restrict Access to Department Reports by Role, page 1-19](#)

Set Up Department Membership Reporting

Before You Begin

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

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

-
- Step 1** Choose **Settings > Data > Data inputs > AD/LDAP Server Details**.

- Step 2** Click **LDAP AD Server Details**.
- Step 3** On the LDAP AD Server Details page, provide the following server information, and then click **Save**:
- AD/LDAP Server Name
 - AD/LDAP User Name
 - AD/LDAP User Password and Confirm
 - AD/LDAP Group Name (Specify the Group DN)
- Step 4** Choose **Settings > Data > Data inputs > scripts** to enable the membership script:
- On Linux, the script name is `discovery.py`.
 - On Windows, the script name is `discovery.vbs`.

The membership script is set to run every day by default. The interval is set in seconds and can be changed by navigating to **Settings > Data > Data inputs > scripts** and editing the interval in the `discovery` file.

You can verify that the script populated the file `departments.csv` with the user data by examining the file `<install_home>/etc/apps/cisco_wsa_reporting/lookups/departments.csv`.

The `departments.csv` file is used as part of the role-based reporting. This file contains:

- user (cs-username - Authenticated username) in the first column
- displayname, groupname in subsequent columns, retrieved from the Active Directory or LDAP server using scripts. For the user present in access log (user_id field), the corresponding display name and group will be displayed in the displayname and department fields.

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 Linux and Windows.

- Ensure the file exists in the application's look-up folder.
- If the Linux version is used, ensure the CLI command `ldapsearch` is installed and in the application user's path.
- If the Windows version is used, "option explicit" may be commented out to reveal more specific information regarding why and from where an error might 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.



Note On Windows, if the `departments.csv` file is not populated with data at this point, change directory to `<install_home>\etc\apps\cisco_wsa_reporting\bin`, and run `cscript discovery.vbs`, where `<install_home>` is `C:\Program Files\Cisco\CiscoWSAReporting`.

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.
- Log into the Cisco Advanced Web Security Reporting application as `admin`.

Step 1 Choose **Settings > Users and authentication > 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, enter `department=sales`.

Step 4 Click **Save**.

Step 5 Choose **Settings > Data > Data Acceleration**.

Step 6 Click **Edit**.

Step 7 Select **Edit Acceleration**.

Step 8 Uncheck the **Accelerate** check box, and click **Save**.

To verify the new role's search restrictions, you can create a new user and run searches. See [Creating New Users, page 1-8](#). Search results for a user, assigned to the role created in Step 4, will only show events that match the search strings specified in the role.



Note Enable data model acceleration if role based reporting is not used. This will enhance reporting performance. See [Configuration Best Practices, page 1-9](#).

Related Topic

- [Users, page 1-8](#)

Troubleshooting Department Membership Reporting



Tip

- Linux users: Verify that `ldapsearch` tool is in the Cisco Advanced Web Security Reporting 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 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.

Set Up Scheduled PDF Reporting (Optional)

Cisco Advanced Web Security Reporting application users can schedule PDF output generation from any dashboard, view, search or report. Follow these configuration steps to set up scheduled PDF reporting:

- [Configure Email Alerts, page 1-20](#)
- [Schedule PDF Report Generation, page 1-20](#)

Configure Email Alerts

You can configure the Cisco Advanced Web Security Reporting application to send email alerts following PDF report generation.

Before You Begin

- Log into the Cisco Advanced Web Security Reporting application as `admin`.

-
- Step 1** In the Cisco Advanced Web Security Reporting application:
- Choose **Settings > System > Server Settings > Email Settings**.
- Step 2** Enter or update the necessary Mail Server Settings in order to send alert emails:
- Mail host** – Enter the SMTP server host name.
 - Email security** (Optional) – Select an email security option. The application can use SSL or TLS when it communicates with the SMTP server.
 - Username** – Enter the name to use during SMTP server authentication.
 - Password** – The password configured for the specified user name.
 - Confirm password** – Re-enter the password.
- Step 3** Provide the necessary Email Format information:
- Link hostname** – Host name of the server used to create outgoing results.
 - Send email as** – Sender name displayed as email originator.
 - Email footer** – The note presented as a footer in sent emails.
- Step 4** Change the PDF Report Settings if necessary: choose a **Report Paper Size** and a **Report Paper Orientation**.
- Step 5** Click **Save**.
-

Schedule PDF Report Generation

You can schedule regular generation and emailing of a PDF report for any custom dashboard. See [Save As Dashboard, page 2-2](#) for information about creating custom dashboards.

Before You Begin

- Log into the Cisco Advanced Web Security Reporting application as `admin`.

-
- Step 1** Choose the desired dashboard from the **Custom Dashboards** menu.
- Step 2** Choose **Edit > Schedule PDF Delivery**.
- Step 3** In the Edit PDF Schedule dialog box, check **Schedule PDF** and provide schedule, email and page options.
- Step 4** (Optional) Click **Send Test Email** to confirm that the generated PDF is sent as an attachment to the specified email address.
- Step 5** (Optional) Click **Preview PDF** to preview the generated PDF.
-



Filters and Dashboards

- [Overview of Filters and Dashboards, page 2-1](#)
- [Viewing Dashboards, page 2-1](#)
- [Creating A Custom Filter, page 2-5](#)
- [Exporting Data, page 2-8](#)
- [Data Formats, page 2-9](#)
- [Time Ranges, page 2-9](#)
- [Troubleshooting, page 2-11](#)
- [Usage Scenarios, page 2-11](#)

Overview of Filters and Dashboards

Advanced Web Security Reporting lets you define custom searches of the available access, SOCKS and AMP log data, displaying the results of each search separately. This process is also known as “filtering.” As much as possible this filtering is consistent with the native reporting of the Web Security Appliance. Each custom search is displayed on its own page or “panel,” which you can save for future access.

The Advanced Web Security Reporting application also provides a number predefined searches, which you can choose to view at any time. These existing searches, as well as any saved filters, are referred to as “dashboards”; in fact, saved filters are accessed via the Custom Dashboards menu. Further, the pages or panels on which these searches are displayed are also sometimes referred to as dashboards.



Note

Data presented using Advanced Web Security Reporting may show more information than is available through the Web Security Appliance alone.

Viewing Dashboards

Before You Begin

Advanced Web Security Reporting administrators can control the Web Security appliances (hosts) that you see on the various dashboards. Contact your Advanced Web Security Reporting administrator with details of any hosts you would like to add, remove, or rename.

-
- Step 1** Sign into the Advanced Web Security Reporting application using a Web browser.
The Overview dashboard presenting summary information is displayed.
- Step 2** Either choose an existing dashboard from the other menus, including the **Custom Dashboards** menu, or choose **Custom Filter** to define a new search, which you can then save as a custom dashboard.
See [Predefined Dashboards, page 2-2](#) for a list of dashboards provided with Advanced Web Security Reporting. Using the **Custom Filter** option is described in [Creating A Custom Filter, page 2-5](#).
- Step 3** Select a time range, data source and host, if applicable.



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

Predefined Dashboards

The following dashboards are provided with the Advanced Web Security Reporting application by default:

- Overview
- User Analysis
 - Overview
 - Location Based
 - User Drilldown
- Browsing Analysis
 - Domain
 - Overview
 - Location Based
 - Domain Drilldown
 - URL Category
 - Overview
 - Location Based
 - URL Category Drilldown
- Application Analysis
 - Overview
 - Application
 - Location Based
 - Application Drilldown
 - Application Type
 - Application Type Drilldown

- Security Analysis
 - L4 Traffic Monitor
 - Overview
 - L4 TM Drilldown
 - Anti Malware
 - Overview
 - Client Malware Risk
 - Location Based
 - Malware Category Drilldown
 - Malware Threat Drilldown
 - Web Reputation Filters
 - Overview
 - Location Based
 - Advanced Malware Protection
 - Overview
 - Location Based
 - File Analysis – You can click the file ID (SHA256) for any entry in the “Completed Analysis Requests from This Appliance” table to open the File Analysis Detail page for that file. The File Analysis Detail page includes a File Analysis Server URL text box in which you can specify the File Analysis server for which you wish to view data. Generally, this URL is `https://intel.api.sourcefire.com` across all Web Security appliance versions through 8.5.

However, if you used another server for analysis of this particular file (demonstrations perhaps), you can change the server URL here to view the details for this file (as identified by its SHA, which you clicked to arrive at this drill-down report).
 - AMP Verdict Updates
- Web Tracking
 - Proxy Services
 - SOCKS
 - SOCKS Drilldown
- Settings
 - Distributed Environment
 - System
 - Data
 - Users and Authentication
 - Third Party Services
- User
 - Edit Account

- Consolidated Web Security Reports - You can view consolidated reports from Cisco Umbrella and Cisco Web Security appliances under following categories:
 - Overview
 - Activity Search
 - Security Activity
 - Top Domains
 - Top Categories
 - Top Users
 - Top Security Categories

Related Topics

- [Viewing Dashboards, page 2-1](#)

Save As Dashboard

On each predefined report page, you can save the displayed report as a another dashboard, in effect cloning the currently displayed dashboard.



Note

You also can save a custom filter as a dashboard, as described in [Saving a Custom Filter as a Dashboard, page 2-7](#). These dashboards can be accessed and edited like any other custom dashboard.

-
- Step 1** On the current report page, modify the time, data-source and host parameters as desired, then click the **Save As Dashboard** button.
- Step 2** Provide the following information in the Save As Dashboard Panel dialog box:
- **Dashboard Title** – A display name for the new dashboard.
When saving any report page as a dashboard, you must provide a proper title to reflect the input selected in order to differentiate the custom dashboards.
 - **Dashboard ID** – Provide a file name for saving the dashboard; cannot be changed later.
 - **Dashboard Description** – (Optional) A short description.
 - **Dashboard Permissions** – Select **Private** or **Shared in App**. Private dashboards are visible only to you, while Shared dashboards are visible to all users.
- Step 3** Click **Save**.
-

The new dashboard is added to the **Custom Dashboards** menu; choose a custom dashboard from the menu to view and edit that dashboard.

Editing A Custom Dashboard

You can edit the currently displayed custom dashboard, repositioning and deleting individual report panels, changing the dashboard title and description, modifying the time range for search queries in those panels, modifying a panel's chart type, and so on.

-
- Step 1** Click the **Edit** button in the current custom dashboard and choose one of the following options:
- **Edit Panels** – Enable panel editing; drag a panel title bar to reposition it; click its close button to delete a panel; add a label above the panel’s title; click the appropriate button to:
 - Change the panel chart type.
 - Change chart parameters.
 - **Edit Title or Description** – Change the title and description of the entire dashboard.
 - **Edit Permissions** – Change the viewing permission for the entire dashboard.
 - **Schedule PDF Delivery** – Schedule regular generation of a report PDF from this dashboard; the generated PDF is then emailed to the address(es) you have specified.
 - **Delete** – Delete entire dashboard.
- Step 2** You also can click **Add Panel** to add a panel from similar custom dashboards to this dashboard. This button is displayed after you click the custom dashboard’s **Edit** button.
- Step 3** Click **Done** when you are finished editing this dashboard.
-

Creating A Custom Filter

When you configure a custom filter, the Advanced Web Security Reporting searches the “data model” you have selected, filtering and displaying the model’s data set by “data object(s),” or “attribute(s),” which you have also selected. Each available data model represents a set of logs of a specific type, while each data object represents a specific log type, or sometimes a data set, that is a child component of the current data model.

Follow these steps to filter and display a specific set of log data:

-
- Step 1** Click **Custom Filter** in the Advanced Web Security Reporting’s menu bar.
- Step 2** On the **Select a Data Model** page, choose the data model to search:
- **AMP Access Model** – all available Advanced Malware Protection logs.
 - **SOCKS Access Model** – all available SOCKS logs.
 - **Web Access Data** – all other available web-related logs (for example, access logs related to user and domain).
 - The following fields in this data model contain values from Cisco Umbrella logs. These fields can be used to create a custom dashboard for Umbrella logs by selecting the *sourcetype* as *ciscoumbrella* in the filter drop-down list:

Field	Umbrella Log Data
user_id_fixed	External or internal IP. Also contains Most Granular Identity, if available.
dest_domain	Domain requested.
odnsaction	Action taken against DNS requests.
x_wbrs_threat_type_fixed	Malware category if the DNS request was for a malicious domain.
x_webcat_code_full	URL category of the domain requested.

Field	Umbrella Log Data
dnsquery_fixed	Type of DNS request made.
dnsresp_fixed	DNS return code for the request.

Each data model represents the collected logs of the named type.

Step 3 On the **Select a Dataset** page:

- a. Expand the list of data objects available in the selected Data Model by clicking the right-arrow preceding the Data Model Event name (for example, “Web Access Event”).
- b. Click a data object (Event or Attribute) and then choose either **Top Values** or **Top Values by Time**.

If you choose **Top Values**, the chosen Attribute data is displayed in rows; each row presents a second column displaying the event count for that particular Attribute entry.

If you choose **Top Values by Time**, `_time` is the filter for **Split Rows**, and the chosen Attribute is the **Split Columns** filter. That is, each row represents an event time and each column represents a specific Attribute entry; thus, each table cell presents the number of occurrences of the given Attribute at a specific time.

Note The symbol preceding each Attribute entry indicates its type; for example, an alphanumeric or numeric value.

Step 4 If you chose **Top Values** in the previous step, you can additionally filter the displayed data by choosing another Attribute from the **Split Columns** menu.

Step 5 You can further adjust the information presented, and its presentation, on the custom filter dashboard, as desired. See [Changing and Saving the Custom Filter Display, page 2-6](#) for more information.

Step 6 To save this custom filter dashboard, choose **Save As > Dashboard Panel**; it will appear in the **Custom Dashboards** menu under the name you provide.



Note

Whenever the current filter’s table or chart is being loaded or refreshed, you can click the Pause or Stop buttons. You can click Reload at any other time to reload the filtered data.

Changing and Saving the Custom Filter Display

After creating a custom filter, you can use the options presented on the New Custom Filter page to successively apply additional filtering, thus further refining the information displayed. For example, in addition to using the **Split Rows** feature to split the current data set into rows, one per data entry, and then using **Split Columns** to add columns to each row, representing information extracted from each row entry, you can also apply parameters and attributes using the **Filters** and **Column Values** menus.

You can also select another Data Model, or another Data Object; you can change the formatting, and export and print the data on the page; you can change the chart type; and you can save this custom filter as a dashboard. The options on the New Custom Filter panel are:

- **Chart type** – Click a button in the data-display-type strip on the left side of the application window to change how the custom-filter data is displayed; for example, you might select a bar or a pie chart.
- **Save As** – Save the current filter as a dashboard; it will be added to the **Custom Dashboards** menu. See [Saving a Custom Filter as a Dashboard, page 2-7](#) for more information.

- **Clear** – clears the current custom filter parameters and the data display.
- **Web Access Event**
 - You can select another Data Model; as described in [Creating A Custom Filter, page 2-5](#).
 - You can select another data Object from the currently selected Data Model; as described in [Creating A Custom Filter, page 2-5](#).
 - Information about the currently displayed data set is also presented.
- **Filters** – For any displayed Filter, click the edit button (pencil icon) to change the parameters applied to that filter, or to remove that filter from the display. You can click the add (+) button to choose another data Object to the current set of Filters.
- **Split Rows** – You can edit current Row object parameters, delete a Row object, and add objects to the Split Rows as described for Filters.
- **Split Columns** – Similarly, you can edit current Column object parameters, delete a Column object, and add objects to the Split Columns.
- **Column Values** – You can also edit, delete and Column Values.

**Note**

If there are multiple objects displayed for any given option, you can drag the object boxes to re-order them. For example, if the currently chosen Filters, in order from left to right, are `All time`, `category is *`, and `dest_url`, you can drag `dest_url` between the other two so the order becomes `All time`, `dest_url`, and `category is *`.

Saving a Custom Filter as a Dashboard

On each custom filter page, you can save the displayed filter as a custom dashboard, making it readily available for future viewing.

-
- Step 1** On the current custom filter page, modify the search parameters as desired, click the **Save As** button and then choose **Dashboard Panel**.
- Step 2** In the Save As Dashboard Panel dialog box, specify a type for this dashboard: either **New** or **Existing**.
- a. If you selected **New**, provide the following information:
 - **Dashboard Title** – (Optional) A display name for the new dashboard.
When saving any report page as a dashboard, you must provide a proper title to reflect the input selected in order to differentiate the custom dashboards.
 - **Dashboard ID** – Provide a file name for saving the dashboard; this cannot be changed later.
 - **Dashboard Description** – (Optional) A short description.
 - **Dashboard Permissions** – Select **Private** or **Shared in App**. Private dashboards are visible only to you, while Shared dashboards are visible to all users.
 - **Panel Title** – (Optional) This is the title displayed at the top of the panel when you view this custom dashboard.
 - **Panel Powered By** – This is always **Inline Search**.
 - **Panel Content** – Select **Statistics** or `<chart type>` to display this filter's information as tabular data, or as the chart type currently used for display.
 - b. If you selected **Existing**, provide the following information:

- **Select** – Choose the name of the existing custom dashboard to which this filter data is to be added.
- **Panel Title** – (Optional) This is the title displayed at the top of the panel when you view this custom dashboard.
- **Panel Powered By** – This is always **Inline Search**.
- **Panel Content** – Select **Statistics** or *<chart type>* to display this filter’s information as tabular data, or as the chart type currently used for display.

Step 3 Click **Save**.

The new dashboard is added to the **Custom Dashboards** menu; choose a custom dashboard from the menu to view and edit that dashboard.

Exporting Data

- [Exporting the Current Custom Filter Panel, page 2-8](#)
- [Exporting the Current Dashboard to a PDF File, page 2-9](#)

Exporting the Current Custom Filter Panel

You can export the currently displayed custom-filter data as a comma-separated values (csv) file, an XML file, or a JavaScript Object Notation (json) file.

Step 1 Click the **Export** button.

Step 2 In the **Export Results** dialog box:

- a. Choose the desired **Format**: **CSV**, **XML**, or **JSON**.
- b. (Optional) Provide a **File Name** if desired.
If you do not enter a file name, a random-number name is generated for you.
- c. Specify the **Number of Results** to be saved: click either **Unlimited** or **Limited**.
If you select **Unlimited**, all data returned by your current filter parameters are saved. If you select **Limited**, specify the **Max Results**—the maximum number of displayed values—to be saved.

Step 3 Click **Export** to close the dialog box and create the export file.

Step 4 An **Open/Save** dialog box appears; you can open the export file using the application defined on your system for files of the chosen **Format**, or you can elect to save the file to a location you specify.

Exporting the Current Dashboard to a PDF File

You can export the currently displayed dashboard as a PDF file.

Before You Begin

- Verify that the Advanced Web Security Reporting administrator has enabled PDF output.

Step 1 Click the Export PDF button.

Step 2 An Open/Save dialog box appears; you can open the PDF file using the application defined on your system for PDF files (usually Adobe Reader), or you can elect to save the file to a location you specify.

Related Topics

- [Set Up Scheduled PDF Reporting \(Optional\)](#), page 1-20

Data Formats

In some cases, the presentation of data in Advanced Web Security Reporting differs from the presentation of data available through the native reporting in source applications.

Data	Format Example
Large numbers (greater than seven digits)	2E11 represents 2×10^{11}
Time	d+hh:mm:ss.ms indicates elapsed days, hours, minutes, seconds, and milliseconds. For example, 1+03:22:36.00 represents one day, three hours, 22 minutes, 36 seconds, and zero milliseconds.

Time Ranges



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.

Range	Indexing Begins	Data Appears in Reports
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

Troubleshooting

- Advanced Web Security Reporting uses a set of files to populate menus. If you experience problems with the menus, verify that the application's look-ups folder contains all the necessary files including:
 - malware_categories.csv
 - transaction_types.csv
 - url_categories.csv
 - malware_categories_opendns.csv
 - url_categories_opendns.csv
- The administrator can edit the list of URL categories visible within the application. When a category appears within the access log, but is not present in the look-up file, Advanced Web Security Reporting displays “Custom Category.”
- Administrators can control the options available in the drop-down fields in the Web Tracking form.

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 Advanced Web Security Reporting drop-down menu.

Step 2 Click 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 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 Advanced Web Security Reporting drop-down menu.

Step 2 **Search** for the User ID/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 Advanced Web Security Reporting drop-down 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 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 all 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 the 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

-
- Step 1** Select **URL Categories** from the Cisco Advanced Web Security Reporting drop-down menu.
 - Step 2** View the top ten URL Categories by Total Transactions graph.
 - Step 3** (Optional) Click the **Export PDF** button. Save the PDF and send it to the appropriate people.
 - Step 4** View the Bytes Allowed column in the URL Categories Matches table.
 - Step 5** (Optional) Click the **Export PDF** button. Save the PDF and send it to the appropriate people.
 - Step 6** For finer granularity, select a specific URL Category.
-

CEF Extractor

- [About the CEF Extractor Service, page -1](#)
- [Setting Up the CEF Extractor Service, page -1](#)

About the CEF Extractor Service

The Common Event Format (CEF) Extractor service running in the Advanced Web Security Reporting (AWSR) application lets you transform access logs received from one or more WSAs into CEF-formatted output data that can be forwarded to other third-party security-information-management (SIM) systems, such as the ArcSight applications.

**Note**

The CEF Extractor service operates only in a distributed environment, meaning it requires at least two separate AWSR instances running on separate hosts. One AWSR instance operates as “master” or “search head,” providing dedicated search and license-sharing functions, while the other “listener” or “peer” instances operate as indexers, feeding the transformed syslog data into the AWSR databases.

Setting Up the CEF Extractor Service

Configuring the CEF Extractor service in Advanced Web Security Reporting involves these steps:

- Set one or more peer instances as “listeners,” ready to receive, transform and index syslog data from linked Web Security appliances. See [Setting Up a CEF Peer, page -1](#) for more information.
- Configure the master AWSR instance, or “search head.” See [Configuring the AWSR Master, page -2](#).
- Set up licensing on all master and peer systems. See [Configuring Licensing, page -3](#).
- Configure the CEF service on the master system. See [CEF Extractor Initial Configuration, page -4](#).
- [Restart the Master System, page -4](#)
- [Configure Mapping of Access Logs to CEF Output Fields, page -4](#)
- Configure data inputs for the CEF service. See [Configure Data Input for the CEF Extractor Service, page -6](#).

Before You Begin

- Be sure all necessary hosts have the AWSR software installed and are configured for basic operations and communications.

Setting Up a CEF Peer

Follow these steps on the server hosting the indexing peer to configure it as a “listener” by creating a new receiver entry and specifying the port on which to listen for Web Security appliance’s syslog data:

Before You Begin

- Launch an AWSR peer and log in as an admin user.

-
- Step 1** Choose **Settings > Data > Forwarding and Receiving**.
- Step 2** On the Forwarding and receiving page, click the **Add new** link in the **Configure receiving** row of the **Receive data** section of this page.
- If the desired listener port is already configured, you can click the **Configure receiving** link to go directly to the **Receive data** page to enable the port.
- Step 3** On the **Add new – Configure receiving** page, enter the number of the port to listen on.
- Step 4** Click **Save**.
- You are returned to the **Receive data** page which lists the available listen-on ports—you can enable/disable and delete individual ports. You also can add new ports from this page.
-

Configuring the AWSR Master

On the master (or search head) system, you must enable Distributed Search and add one or more Search peers to its peer roster.

Before You Begin

- Launch the AWSR master and log in as an admin user.

-
- Step 1** To enable Distributed Search:
- Click **Settings > Distributed Environment > Distributed Search**.
 - On the Distributed search page, click **Distributed search setup**.
 - On the Distributed search set up page, Select **Yes** for the **Turn on distributed search?** option.
 - Click **Save**.
- You are returned to the Distributed search page.
- Step 2** To add a search peer (that is, an indexer):
- Click the **Add new** link in the **Search peers** row of the Distributed search page.
 - On the Add new page, under Add search peers, enter the **Peer ID** in either *server_name:management_port* or *IP_address:management_port* format.
 - Provide Distributed search authentication parameters for connection to the peer:
 - **Remote username** – Provide the user name for an admin user on the remote search peer.
 - **Remote password** – Enter that user’s connection password.
 - **Confirm password** – Re-enter the password.
 - Click **Save**.
- You are returned to the Search peers page.
-

The Search peers page lists all currently configured peers. You can enable/disable and delete individual Search peers. You also can add new Search peers from this page. Access this page at any time by choosing **Settings > Distributed Environment > Distributed Search** and then clicking **Search peers**.

Configuring Licensing

The master system can share one license with each indexer. That is, each indexer peer does not need a separate, individual license. Configuring licensing on all AWSR instances is described in the following sections:

- [Peer Licensing, page -3](#)
- [Master Licensing, page -3](#)

Peer Licensing

Each indexer is configured to access a license from a license pool maintained by the master system.

-
- Step 1** On the indexer system, choose **Settings > System > Licensing** to open the Licensing page. A notification of this server's licensing role is displayed at the top of this page. The server's role can be either "associated with a remote master license server," or "acting as a master license server."
- Step 2** If this peer's displayed role is **acting as a master license server**, click the **Change to slave** button.
- Step 3** On the **Change master association** page, select **Designate a different AWSR instance as the master license server**.
- Step 4** Provide the master license server access information: either the *server_name:management_port* or *IP_address:management_port* of the desired server.
- Step 5** Click **Save**.
-

Master Licensing

The master system can share one license with each indexer. Follow these steps to specify the license pool to share with all configured indexer systems.


-
- Step 1** On the search head, choose **Settings > System > Licensing** to access the Licensing page. A notification of this server's licensing role is displayed at the top of this page. The server's role can be either "associated with a remote master license server," or "acting as a master license server."
- Step 2** If this peer's displayed role is **associated with a remote master license server**, click the **Change to master** button and designate this server as the master license server in the Change master association dialog box; click **Save** in the dialog box to return to the Licensing page.
- Step 3** In the License stack section, click **Edit** in the row representing the license pool that you want to share with indexer peers.
- Step 4** On the Manage license pool page, select **Specific indexers** for the option "Which indexers are eligible to draw from this pool?" Available indexers are listed.
- Step 5** Click the green Add button in front of a desired indexer to add it to the Associated indexers list. Repeat this step as necessary.
- Step 6** Click **Submit**.
- Step 7** Click **OK** in the Update notification. You are returned to the Licensing page, where you can add licenses, and add, edit and delete license pools.
-

CEF Extractor Initial Configuration

After the AWSR CEF Extractor master and indexer systems have been set up, you must configure the CEF Extractor service.

Before You Begin

- Launch the AWSR master system and log in as an admin user.

-
- Step 1** Choose **Settings > Third Party Services > CEF Extractor** to access the CEF Extractor page. You are notified the CEF application has not yet been fully configured.
- Step 2** Click the **Continue to app setup page** button to continue to the AWSR CEF set-up page.
- Step 3** Check **Enable Indexed Realtime** to allow indexing and searching in real time. We recommend enabling this option to increase performance.
- Step 4** In the Indexer Setup section, enter the access ID information for each peer in the **Indexers** field in either *server_name:listener_port* or *IP_address:listener_port* format.
-  **Note** For each indexer entry, be sure to use the number of the listener port configured for that indexer system, as described in [Setting Up a CEF Peer, page -1](#).
-
- Step 5** Click **Save**.
-

Restart the Master System

After configuring the Advanced Web Security Reporting master system, setting up peer licensing sharing, and configuring the CEF Extractor service, you must restart the master server.

-
- Step 1** Choose **Settings > System > Server Controls** to access the Server controls page.
- Step 2** Click the **Restart AWSR** button and follow the instructions to restart the system.
- Step 3** When restart is completed; log in again.
-

Configure Mapping of Access Logs to CEF Output Fields

The next task is configuring the mapping of Web Security appliance's access logs to CEF output fields for the CEF Extractor service, and defining output destinations for this information.

-
- Step 1** Choose **Settings > Third Party Services > CEF Extractor** to access the CEF Extractor page.
- Step 2** Click **New** to launch the CEF Extractor data-search set-up wizard.
- Step 3** Choose the **Data Model** from which to retrieve data; in this case, choose **Web_Access_Data**.
- Step 4** Choose **Web_Access_Event** from the **Object** drop-down list indicating the data fields are to be obtained from Web Security appliance's Web access logs.

Step 5 Click **Next** to proceed to the Map Fields page of the wizard.

This page displays two columns: CEF Output Fields and Data-model attributes. The rows in the Output Fields column are drop-down lists containing all CEF output formats, while the Data-model attribute column presents a hard-coded listing of the attribute availables in the data model.

Step 6 Map CEF Output Fields to Web Access data-model attributes, as needed.

Some fields are automatically mapped (for example, the Data-model attribute `host` is automatically mapped to the CEF field `syslog_host`); auto-mapped and default mappings are displayed on this page; both can be altered.

To add or change a mapping, open the drop-down list in row representing the Output Field-to-Attribute mapping to be updates, and choose the CEF output field to be mapped to this Data-model attribute.

Step 7 Click **Next** to proceed to the Create Static Fields page of the wizard.

Use the fields on this page to provide situational static values for CEF output fields that have no corresponding Data-model attributes.

Step 8 Enter static Field Values for listed CEF Output Fields.

For example, you might enter a Field Value of `CISCO` for the CEF Output Field `dvc_vendor`, and `AWSR_CEF` for `dvc_product`.

Step 9 Click **Next** to proceed to the Define Outputs page of the wizard.

On this page, you create or select the output group to which CEF data is to be sent.

Step 10 Click **Create new output group**.

Step 11 In the New Output Group dialog box, provide the following new output group parameters:

- **Name** – an identifier for this output group.
- **Hosts to output data to** – the output server(s) to be sent CEF output data; enter in either *server_name:receive_port* or *IP_address:receive_port* format.



Note If you are planning to output syslog data, you cannot use TCP port 514 here, as it is already in use; see [Configuration Of Data Input for Web Security Appliance Syslogs, page 1-14](#).

Step 12 Click **Save** to close the New Output Group dialog box.

Step 13 Click **Next** to proceed to the Save Search page of the wizard.

Step 14 Identify this mapping or search set:

- **Search Name** – an identifier or mapping name for this CEF information search set.
- **Search Description** (optional) – a short description for this CEF information search.

Step 15 Click **Save** to complete the wizard.

The CEF Extractor page lists defined data-set mappings; you can add new sets and enable, disable or delete existing sets.

Configure Data Input for the CEF Extractor Service

The next task is configuring the data fields for the CEF Extractor service.



Note

This section describes setting up Web Security appliance access logs as data input for the CEF Extractor service. You can also set up FTP push, syslog push, and CWS logs as data inputs for the service. See [Set Up On-going Data Transfers, page 1-13](#) and [Configure CWS or Umbrella Log Updates, page 1-17](#) for additional information.

-
- Step 1** Choose **Settings > Data > Data inputs** to access the Data inputs page.
 - Step 2** Click **Add new** in the **Files & directories** row of the Data inputs page to launch the set-up wizard in which you will configure the field mappings and monitoring of a new data folder.
 - Step 3** Click the **Browse** button beside the **File or Directory** field.
 - Step 4** In the Select source dialog box, browse to and select the desired Web Security appliance access logs folder (for example, `home/logger/incoming/wsa_test/accesslogs`).
 - Step 5** Click **Select** to close the Select source dialog box.
 - Step 6** Click **Next** on the Select Source wizard page to go to the Input Setting page.
 - Step 7** For Source type, click **Select**, then click **Select Source Type** and choose `wsa_accesslogs` (you can start typing `wsa_accesslogs` into the filter field at the top of the Select Source Type drop-down list to quickly locate the entry).
 - Step 8** For App context, choose **Advanced Web Security Reporting 6.1.0** from the **App context** drop-down list.
 - Step 9** Scroll down to the Host entry, click **Segment in path**, and then enter a **Segment number**.
The Host entry specifies how the value of the host field is determined for events from this source. The Segment in path option means it is determined from a segment of the Source path specified earlier. The Segment number indicates which segment of the path is the host value. For example, in our earlier sample Source path, `home/logger/incoming/wsa_test/accesslogs`, the host name, `wsa_test`, is the fourth segment in the path, so the Segment number entered here would be 4.
 - Step 10** Click **Review** to proceed to the Review page of the wizard.
 - Step 11** Review the information you have entered and then click **Submit** to create the new data input instance.
-