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

Version 4.5

Published: June 22, 2015
Revised: December 11, 2015

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.

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

CHAPTER 1 **Installation and Setup** 1-1

Introduction 1-1

What's New in 4.5 1-2

Supported and Unsupported Features 1-2

System Requirements and Sizing & Scaling Recommendations 1-3

Set-up Overview 1-3

Upgrade the Advanced Web Security Reporting Application 1-3

Upgrading from Version 4.0 to Version 4.5 1-3

Upgrading from Version 3.0 to Version 4.5 1-4

Upgrading from Version 3.0 to Version 4.0 1-4

Install and Configure the Advanced Web Security Reporting Application 1-5

On Linux 1-6

On Windows 1-6

Administrative Users 1-7

Configuration Best Practices 1-7

Commands To Start and Stop the Advanced Web Security Reporting Application 1-8

On Linux 1-8

On Windows 1-8

Licensing and Migration 1-8

Migration from v3.0 WSA to v4.0 WSA-only Reporting 1-8

Migration from v3.0 WSA-only to v4.0 Hybrid Reporting 1-9

New Hybrid Reporting License 1-9

Hybrid Reporting License Issues 1-9

Licensing Considerations for Version 3.0 to Version 4.0 and Later Upgrades 1-9

License Installation 1-10

Create the Folder Structure for Access and Traffic Monitor Log Files 1-10

Import and Index Historical Data 1-10

(Optional) Configure the Advanced Web Security Reporting Application to Delete Log Files After Indexing 1-11

Set Up On-going Data Transfers 1-12

Configure Data Inputs for WSA Logs 1-12

Configuration Of Data Input for WSA Syslogs 1-12

Establish Log Transfers from A Web Security Appliance 1-13

Configure CWS Log Updates 1-14
Set Up Department Membership Query (Optional) 1-15
Set Up Department Membership Reporting 1-15
Restrict Access to Department Reports by Role 1-16
Troubleshooting Department Membership Reporting 1-16
Set Up Scheduled PDF Reporting (Optional) 1-17
Configure Email Alerts 1-17
Schedule PDF Report Generation 1-17
Edit the List of URL Categories (Optional) 1-18

CHAPTER 2 **Reports** 2-1
Overview of Reports 2-1
Accessing Reports 2-1
Data Formats 2-2
Time Ranges 2-2
Timing of Data Availability 2-2
Export 2-3
Exporting to a .CSV File 2-3
Exporting to a PDF File 2-3
General Versus Specific Data 2-3
Viewing Specifics 2-3
Search 2-4
Search Tips 2-4
Troubleshooting Searches 2-4
Predefined Reports 2-5
General Reports 2-5
Other Report Categories 2-5
Usage Scenarios 2-6
User Investigation 2-6
Viewing Web Usage Trends 2-6
Viewing Transaction History 2-7
URLs Visited 2-7
Viewing Most Visited Web Sites 2-7
URL Categories Visited 2-7
Viewing Most Common URL Categories 2-7

CHAPTER 3 **Field Extractions** 3-1
Access Logs 3-1

Traffic Monitor Logs 3-2
AMP Logs 3-2

Installation and Setup

- Introduction, page 1-1
- System Requirements and Sizing & Scaling Recommendations, page 1-3
- Set-up Overview, page 1-3
- Upgrade the Advanced Web Security Reporting Application, page 1-3
- Install and Configure the Advanced Web Security Reporting Application, page 1-5
- Licensing and Migration, page 1-8
- Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-10
- Import and Index Historical Data, page 1-10
- Set Up On-going Data Transfers, page 1-12
- Set Up Department Membership Query (Optional) , page 1-15
- Edit the List of URL Categories (Optional), page 1-18

Introduction

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

Note Cloud Web Security is sometimes referred to as "ScanSafe."

The Advanced Web Security Reporting application receives log data and stores it in the default/main index. You can view these data using predefined reports, and you can also perform ad hoc searches using the "flashtimeline" view and the Web tracking forms.

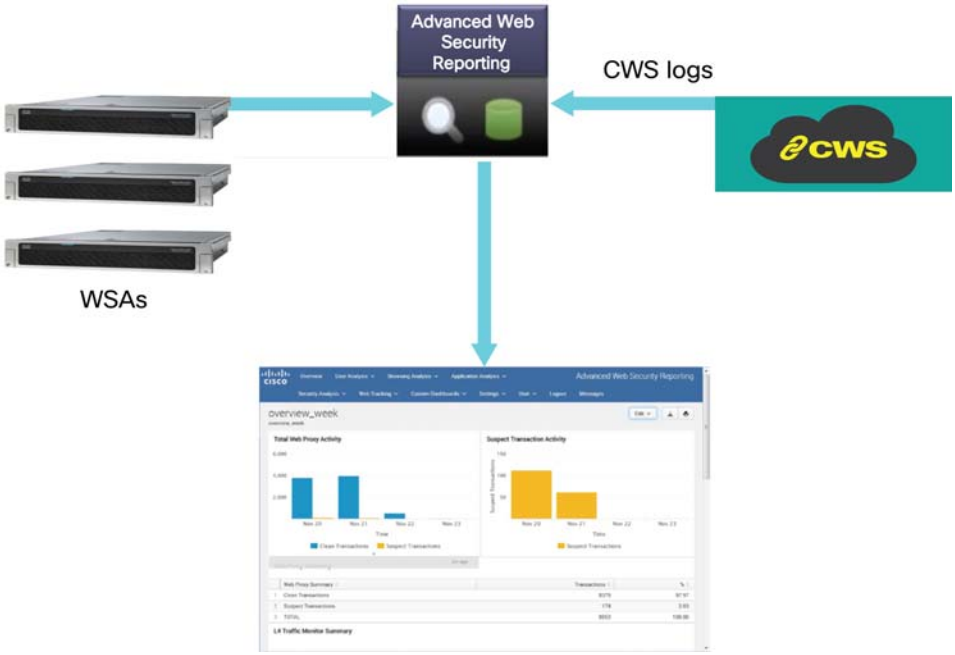

Figure 1-1 General architecture of the Advanced Web Security Reporting system.

What's New in 4.5

- Reporting based on WSA's Advanced Malware Protection (AMP) and File Analysis logs.

Supported and Unsupported Features

Component	Supported	Not Supported
Reports	Reports included in the Advanced Web Security Reporting application	Custom reports
Search	Form-based search/web tracking tool included with the Advanced Web Security Reporting application	N/A
Server	Single-server deployments	Multiple-server deployments
Transport Methods	FTP (files and directories) TCP (syslogs)	N/A
PDF	Integrated PDF generation Scheduled PDF Reporting (limited)	N/A

System Requirements and Sizing & Scaling Recommendations

System requirements, as well as sizing and scaling recommendations, are detailed in the *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

Step 1 Upgrade the Advanced Web Security Reporting Application, page 1-3

If you are **not** upgrading from an existing Advanced Web Security Reporting installation, perform these steps before upgrading:

a. Install and Configure the Advanced Web Security Reporting Application, page 1-5
b. Licensing and Migration, page 1-8
c. Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-10
d. Import and Index Historical Data, page 1-10
e. Set Up On-going Data Transfers, page 1-12 (Including setup of Web Security Appliance.)
f. Configure CWS Log Updates, page 1-14

Upgrade the Advanced Web Security Reporting Application

- Upgrading from Version 4.0 to Version 4.5, page 1-3
- Upgrading from Version 3.0 to Version 4.5, page 1-4
- Upgrading from Version 3.0 to Version 4.0, page 1-4

Upgrading from Version 4.0 to Version 4.5

To upgrade from version 4.0 to version 4.5 of the Advanced Web Security Reporting application, you must download an additional file and add it to your existing version 4.0 installation. After obtaining this file and copying it to the Advanced Web Security Reporting host, follow these steps to install it.

Step 1 Launch the Advanced Web Security Reporting 4.0 application (enter `http://<hostname>:8888` in a browser window) and log in as the default `admin` user.

Step 2 Click the Manage Apps button in the top-left corner of the application window.

Step 3 On the Apps page, click the **Install app from file** button.

Step 4 Browse to and select the `.zip` or `.tar` file for the Advanced Web Security Reporting 4.5 application.

Step 5 Select the **Upgrade app** checkbox. Checking this will allow the existing application to be overwritten; otherwise you will receive an “app with this name already exists” error.

Step 6 Click **Upload**.

Step 7 Following notification that the file was imported successfully, restart the application:

a. Navigate to **Settings > Server Controls**.

b. Click **Restart Splunk**.

Step 8 Log into the Advanced Web Security Reporting application.

Step 9 Verify that the application was upgraded to version 4.5: the launch button in the left pane of the application window will display "Cisco Advanced Web Security Reporting 4.5.0."

You also can confirm by clicking the Manage Apps button in the top-left corner of the application window, and locating the "Cisco Advanced Web Security Reporting 4.5.0" listing.

Upgrading from Version 3.0 to Version 4.5

Upgrading from version 3.0 to version 4.5 is a two-step process:

1. Complete the steps in the following section to upgrade from version 3.0 to version 4.0 ("Upgrading from Version 3.0 to Version 4.0").
2. Complete the steps in the previous section to upgrade from version 4.0 to version 4.5: Upgrading from Version 4.0 to Version 4.5, page 1-3.

Upgrading from Version 3.0 to Version 4.0

With the release of version 4.0, with Single Installer and the architecture re-design, you must follow the steps in this section to upgrade your version 3.0 installation for version 4.0 or later. 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 4.0 application.
- Copy the version 3.0 back-up data to the new data directory.
- Restart the version 4.0 or later 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/bin/splunk stop
```

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 Advanced Web Security Reporting:

```
/opt/cisco_wsa_reporting/bin/splunk start
```

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

Step 11 On the application home page, click **Cisco WSA - Advanced Reporting** (left sidebar) to navigate to that App; verify that data exists (change the time frame if necessary).

Step 12 Rebuild the Data Model accelerations:

a. Return the Advanced Web Security Reporting home page, and then select **Settings > Data Models**.

b. One at a time, for both the **SOCKS Access Model** and the **Web Access Model**:

   a. Click the arrow preceding the Data Model label to expand that model entry.

   b. Click **Rebuild** under Acceleration.

   In both cases, the rebuild process could take some time.

Install and Configure the Advanced Web Security Reporting Application

- On Linux, page 1-6
- On Windows, page 1-6

Note To run version 4.5 of the Advanced Web Security Reporting application, you simply upgrade a version 4.0 installation by adding a file to the existing installation, as described in Upgrading from Version 4.0 to Version 4.5, page 1-3. (Upgrading from a version 3.0 installation is a two-step process, as described in Upgrading from Version 3.0 to Version 4.5, page 1-4.)

On Linux

These tasks must be performed in order:

Step 1 Download the Single Installer for the Advanced Web Security Reporting 4.0 software:

https://software.cisco.com/download/release.html?mdfid=283503844&flowid=39823&softwareid=283998384&release=CiscoWSAReporting4.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 Extract the installer software.

To install into the current working directory, issue this command:

```
tar zxvf cisco_wsa_reporting-4.0.0.tgz.
```

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

```
tar zxvf cisco_wsa_reporting-4.0.0.tgz -C /opt
```

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

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

Progress and milestone statements are displayed during set-up.

You can also check the log file `$WSA_REPORTING_HOME/var/log/cisco_wsa_reporting/splunkd.log` for any issues during installation, and to confirm that the set-up script completed successfully.

Step 4 Launch the Advanced Web Security Reporting application and log in:

a. Navigate to `http://<hostname>:8888` in a browser window.

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

b. Log in with the user name `admin` and `Splunk@dmin` as the password.

c. Change the `admin` password.

d. Navigate to **Manager > Apps** to verify that the Cisco Advanced Web Security Reporting application is visible and enabled.

Next Steps

- Licensing and Migration, page 1-8

On Windows

Before You Begin

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

Step 1 Download the Single Installer for the Advanced Web Security Reporting 4.0 software:

https://software.cisco.com/download/release.html?mdfid=283503844&flowid=39823&softwareid=283998384&release=CiscoWSAReporting4.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 Unzip and extract the installer software.

Step 3 Launch PowerShell or a Command Prompt window as Administrator.

Step 4 Navigate to the unzipped directory.

Step 5 Run `install.bat`.

The application is installed in the folder `C:\Program Files\Cisco\CiscoWSAReporting`.

Step 6 Reboot the Advanced Web Security Reporting server.

Step 7 Launch the Advanced Web Security Reporting application and log in:

a. Navigate to `http://<hostname>:8888` in a browser window.

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

b. Log in with the user name `admin` and `Splunk@dmin` as the password.

c. Change the `admin` password.

d. Navigate to **Manager > Apps** to verify that the Cisco Advanced Web Security Reporting application is visible and enabled.

Next Steps

- Licensing and Migration, page 1-8

Administrative Users

The Advanced Web Security Reporting application provides two administrative users:

- The “default admin” (user name: `admin` and password: `Splunk@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.

  The `wsa_admin` user cannot install licenses and configure the distributed environment.

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

Configuration Best Practices

- Set time zones consistently across WSA and CWS appliances.

  The time displayed in the search results reflects the “local” time of the 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).

Commands To Start and Stop the Advanced Web Security Reporting Application

On Linux

To stop the Advanced Web Security Reporting application

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

```
./shutdown.sh
```

To start the Advanced Web Security Reporting application

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

```
/startup.sh
```

On Windows

To stop the Advanced Web Security Reporting application

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

```
wsa_reporting.exe stop
```

To start the Advanced Web Security Reporting application

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

```
wsa_reporting.exe start
```

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 WSA 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 WSA-only reporting with your existing license. The various licensing and migration scenarios are:

- Migration from v3.0 WSA to v4.0 WSA-only Reporting
- Migration from v3.0 WSA-only to v4.0 Hybrid Reporting
- New Hybrid Reporting License

Migration from v3.0 WSA to v4.0 WSA-only Reporting

You can install the version 4.0 or later software and your previously installed license will continue to provide WSA 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 WSA-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 WSA reporting. In addition, the embedded evaluation license will let you evaluate the hybrid reporting feature.

In order to migrate from WSA-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—that is, the `ciscocws` source type is included. https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case

Note Contacting TAC is necessary only if you are upgrading from version 3.0 WSA-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 Advanced Web Security Reporting user, to utilize WSA 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 a CWS Log Extraction license (L-CWS-LOG-LIC=), and that you have set up your Advanced Web Security Reporting 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 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 3.0 to 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 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. The evaluation license provided with the application may be
3. After your version 3.0 data has been transferred, acquire and upload an 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 Web Security Reporting.

5. Ensure that indexes are reported to the correct pool:

a. Navigate to **Settings > 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 Advanced Web Security Reporting license(s):

Step 1 Launch the 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 > 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/	$Input_base=path of root FTP folder host_name=WSA device
Access	/$Input_base/wsa_hostname/accesslogs/	$Input_base=deployment host_name=WSA device
AMP	/$Input_base/wsa_hostname/amplogs/	$Input_base=deployment host_name=WSA device

Import and Index Historical Data

Before You Begin

- Complete configuration tasks listed in Install and Configure the Advanced Web Security Reporting Application, page 1-5.
- Verify that field extractions are correct. See Chapter 3, "Field Extractions".

- Know the folder structure. See Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-10.

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

Step 2 On the Advanced Web Security Reporting Web page, log in as `admin`.

Step 3 Verify that data is being imported:

a. Select **Settings** > **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 Advanced Web Security Reporting default license downloaded for the account, and remove any non-production licenses.

Tip If you find that the Advanced Web Security Reporting 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 Advanced Web Security Reporting Application to Delete Log Files After Indexing, describes editing the `inputs.conf` file.)

What to Do Next

- Configure Data Inputs for WSA Logs, page 1-12.

(Optional) Configure the Advanced Web Security Reporting Application to Delete Log Files After Indexing

Step 1 Navigate to your install directory and copy the file `/cisco_wsa_reporting/etc/apps//cisco_wsa_reporting/inputs.conf` to the directory `/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/`.

Step 2 Using a text editor, open `/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf`.

Step 3 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 Advanced Web Security Reporting FTP directory path where WSA 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 4 Save the `inputs.conf` file and then restart the application by navigating to **Settings** > **Server controls** and clicking **Restart Splunk**.

Set Up On-going Data Transfers

Before You Begin

- Import and Index Historical Data, page 1-10
- Know the path to your log files: Create the Folder Structure for Access and Traffic Monitor Log Files, page 1-10.
- Log into the Enterprise Web as `admin`.

Configure Data Inputs for WSA Logs

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

Step 1 In the Advanced Web Security Reporting application:

- Choose **Settings** > **Data inputs** > **Files & directories**.

Step 2 Disable any inputs labeled `CiscoWSA`.

Step 3 Click **New**.

Step 4 Click **Continuously Monitor** and provide the full path to the Advanced Web Security Reporting FTP directory to which WSA logs will be sent.

This path and the FTP path provided on the WSA's Log Subscription page must match.

Step 5 Click Next.

Step 6 Click **Manual** as the Sourcetype and provide the Sourcetype label (`wsa_accesslogs`, `wsa_trafmonlogs`, or `wsa_amplogs`).

Step 7 Choose **Cisco WSA - Advanced Reporting 4.5.0** from the App Context menu.

Step 8 Click **Constant value** and provide the Advanced Web Security Reporting host name in the **Host field value** field.

Step 9 Choose **Default** as the destination Index.

Step 10 Click **Review** and review the values you provided.

Step 11 Click **Submit**.

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

Configuration Of Data Input for WSA Syslogs

Step 1 In the Advanced Web Security Reporting application:

- Choose **Settings** > **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 **Manual** and then enter `wsa_syslog` in the Sourcetype field.

Step 6 Choose `Cisco WSA - Advanced Reporting` as the **App Context**.

Step 7 In the Host section, click **Custom** as the Method field, and then enter the Advanced Web Security Reporting host name as the Host field value.

Step 8 Choose **Default** as the destination Index.

Step 9 Click **Review** and review the values you provided.

Step 10 Click **Submit**.

Step 11 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 Advanced Web Security Reporting application for each appliance. However, you also can configure multiple appliances by editing the `inputs.conf` file.

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 1-10.
- 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.
(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).

Setting	Log Type	Value
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 Select **FTP on Remote Server**	Any one	Hostname: IP address or host name of the Enterprise host. Directory: name of Advanced Web Security Reporting instance directory. Username/Password: FTP user name and password for access to the application. **Note** If connection between Advanced Web Security Reporting and WSA 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 Log Updates

Before You Begin

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

Step 1 In the Advanced Web Security Reporting application:

- Choose **Settings > Data inputs > Cisco CWS Logs**.

Step 2 Click **New**.

Step 3 Provide a meaningful **name** for this data input.

Step 4 Provide the **client_id**, **s3_key** and **s3_secret** that have been provided from CWS. The **client_id** is the bucket ID used in CWS.

Step 5 Click **More settings** check box and provide the time **Interval** in seconds at which CWS logs can be pulled; default is 3600.

Step 6 Click **Next**.

Step 7 A success screen is displayed.

Note You can navigate to **Settings > 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 Advanced Web Security Reporting application.
- You will run reports on data that are based on organizational roles.

Related Topics

- Restrict Access to Department Reports by Role, page 1-16

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: `<install_home>/etc/apps/cisco_wsa_reporting/bin/discovery.py`
- Windows: `X:\<install_home>\etc\apps\cisco_wsa_reporting\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:

`<install_home>/etc/apps/cisco_wsa_reporting/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 Advanced Web Security Reporting.

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

`<install_home>/etc/apps/CiscoWSA/lookups/departments.csv`

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`.

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.
- Log into Advanced Reporting's Enterprise Web as `admin`.

Step 1 In Enterprise Web,

- Select **Settings > 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**.

Troubleshooting Department Membership Reporting

Tip

- Linux users: Verify that `ldapsearch` tool is in the Enterprise 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 about 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)

Advanced Web Security Reporting 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 1-17
- Schedule PDF Report Generation, page 1-17

Configure Email Alerts

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

Before You Begin

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

Step 1 In the Advanced Web Security Reporting application:

- Choose **Settings > Server Settings > Email Settings**.

Step 2 Enter or update the necessary Mail Server Settings in order to send alert emails:

a. **Mail host** – Enter the SMTP server host name.

b. **Email security** (Optional) – Select an email security option. The Advanced Web Security Reporting application can use SSL or TLS when it communicates with the SMTP server.

c. **Username** – Enter the name to use during SMTP server authentication.

d. **Password** – The password configured for the specified user name.

e. **Confirm password** – Re-enter the password.

Step 3 Provide the necessary Email Format information:

a. **Link hostname** – Host name of the server used to create outgoing results.

b. **Send email as** – Sender name displayed as email originator.

c. **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

Before You Begin

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

Step 1 Navigate to the **Cisco WSA - Advanced Reporting** application.

Step 2 On any report page (Overview, Users, Websites, etc.), position the mouse pointer over the desired report to display its related toolbar, and then click the Open in Search icon.

Step 3 On that Search page, click **Save As** and choose **Dashboard Panel**.

Step 4 Provide the appropriate Save As Dashboard Panel options:

a. Dashboard – Click **New** or **Existing**:

Select **New** when creating a new custom dashboard. Provide the following:

- **Dashboard Title** (Optional) – Enter a name for the new dashboard.
- **Dashboard ID** – Provide a file name for saving the dashboard; cannot be changed later.
- **Dashboard Description** (Optional) – A description of the dashboard.
- **Dashboard Permissions** – Select **Private** or **Shared in App**.
- **Panel Title** (Optional) – Title displayed in the dashboard panel.
- **Panel Content** – How dashboard content is displayed, either as Statistics or as graphical Columns.

Select **Existing** to access a previously created custom dashboard:

- Choose the desired dashboard from the drop-down list.
- **Panel Title** (Optional) – Title displayed in the dashboard panel.
- **Panel Content** – How dashboard content is displayed: either as Statistics or as graphical Columns.

Step 5 Click **Save** and then click **View Dashboard**.

Step 6 In this dashboard view, choose **Edit > Schedule PDF Delivery**.

Step 7 Select **Schedule PDF** and provide schedule, email and page parameters.

Step 8 (Optional) Click **Send Test Email** to confirm that the generated PDF is sent as an attachment to the specified email address.

Step 9 (Optional) Click **Preview PDF** to preview the generated PDF.

You can view your custom dashboards on the Other Dashboards page. You also can edit these dashboards later, including scheduling PDF Delivery.

Edit the List of URL Categories (Optional)

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

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

- Select **Settings > Lookups > Lookup table files**.

Reports

- Overview of Reports, page 2-1
- Accessing Reports, page 2-1
- Data Formats, page 2-2
- Time Ranges, page 2-2
- Export, page 2-3
- General Versus Specific Data, page 2-3
- Predefined Reports, page 2-5
- Usage Scenarios, page 2-6

Overview of Reports

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

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

Accessing Reports

Before You Begin

Advanced Web Security Reporting administrators can control the Web Security appliances (hosts) that you see on the Overview report and Web Tracking report. Contact your 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.

Step 2 Click **Cisco Web Security - Advanced Reporting** 4.5 under **Apps** in the navigation pane on the left side of the screen.

Summary information is displayed.

Step 3 Choose a report from the **Other Dashboards** menu. See General Reports, page 2-5 and Other Report Categories, page 2-5.

Step 4 Select a time range, data source and hosts, if applicable.

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

Data Formats

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

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.
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

Export

Exporting to a .CSV File

This option can be useful for tracking reports.

Step 1 Generate the report.

Step 2 Select **Export**.

Exporting to a PDF File

Before You Begin

- Verify that the Enterprise administrator has enabled PDF output.

Step 1 Generate the report.

Step 2 Select **Save as PDF**.

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 the hyperlink for the subject for which you want specifics.

For example, click the User ID for an individual user.

Related Topics

- Export, page 2-3

Search

Simple and advanced search options are available for most report pages.

Search Tips

- Make the searches as specific as possible, and narrow the time range.
- Advanced Web Security Reporting uses a set of files to populate menus. If experience problems with the menus, verify that the necessary files are in the application's look-ups folder, including:
  - `malware_categories.csv`
  - `transaction_types.csv`
  - `url_categories.csv`
- The Enterprise 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."
- Enterprise administrators can control the options available in the drop-down 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 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.

Predefined Reports

General Reports

These reports are available from links across the top of the application window.

- Overview
- Users
- Websites
- URL Categories
- Application Visibility

Other Report Categories

Available from the **Other Dashboards** menu.

- L4 Traffic Monitor (summary; WSA reporting only)
- SOCKS (summary; WSA reporting only)
- Web Tracking (summary); submenu includes:
  - Proxy Services
  - SOCKS (detail)
  - L4 Traffic Monitor (detail)
- Security (summary); detail submenu includes:
  - Anti Malware
  - Client Malware Risk
  - Web Reputation Filters
  - Advanced Malware Protection
  - File Analysis

    You can click the file ID (SHA256) for any entry in the "Completed Analysis Requests from This Appliance" table on the File Analysis page (Other Dashboards > Security > File Analysis) 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 WSA 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
- Location (summary); detail submenu includes:
  - Anti Malware by Location
  - Application Visibility by Location
  - Overview by Location

  - Users by Location
  - Web Reputation Filters by Location
  - Websites by Location
- Drilldown (summary); detail submenu includes:
  - Application Drilldown
  - Application Type Drilldown
  - Domain Drilldown
  - Malware Category Drilldown
  - Malware Threat Drilldown
  - URL Category Drilldown
  - User Drilldown
- Dashboards

Related Topics

- Accessing Reports, page 2-1
- Search, page 2-4

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.

Field Extractions

- Access Logs , page 3-1
- Traffic Monitor Logs, page 3-2
- AMP Logs, page 3-2

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 look-up 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 access logs, 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="!!!!"
```

AMP Logs

The AMP reports are generated from AMP logs. Field extractions will still need to be operable for these reports to function.

Tip Use these searches to verify that there are few or no results:

```
sourcetype=wsa_accesslogs  x_sha_256 = "*"  x_file_name = "*" x_threat_name = "*"

sourcetype=wsa_amplogs verdict_type="*" x_analysis_id="*" x_status="*" x_sha1="*"
x_sha256="*" x_md5="*" amp_score="*" x_start_time="*" amp_sha_value="*"
time_of_analysis="*" time_of_complete="*"
```