Cisco Advanced Web Security Reporting 7.5.3 Installation, Setup, and User Guide

First Published: 2025-04-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

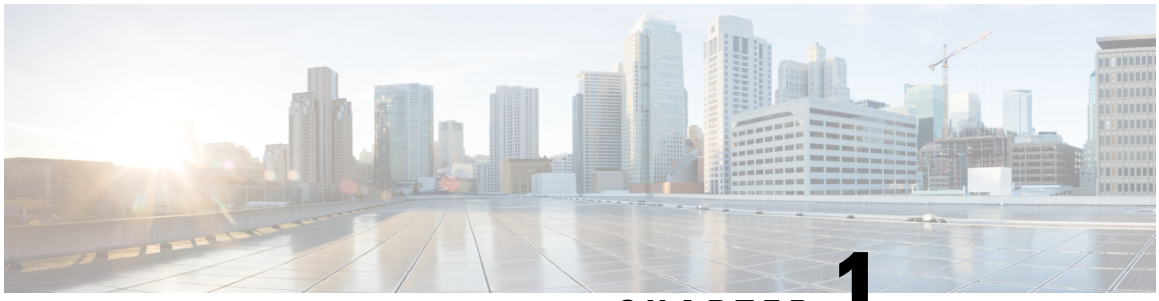
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Installation and Setup

This chapter covers the following sections:

- Introduction, on page 1
- System Requirements and Sizing and Scaling Recommendations, on page 6
- Set-up Overview, on page 6
- Installing Cisco Advanced Web security Reporting 7.5.3, on page 7
- Upgrading to Cisco Advanced Web Security Reporting 7.5.3, on page 12
- Post Installation Tasks, on page 15
- Licensing and Migration, on page 17
- Create the Folder Structure for Access and Traffic Monitor Log Files, on page 20
- Import and Index Historical Data, on page 20
- Set Up On-going Data Transfers, on page 21
- Umbrella Log Updates, on page 25
- Set Up Department Membership Query (Optional), on page 26
- Set Up Scheduled PDF Reporting (Optional), on page 29
- Schedule Summary Index Generation, on page 30
- Create or Modify Users, on page 31
- Delete Users, on page 31
- Create or Modify Roles, on page 32

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, 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), and an Umbrella host.

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 7.5.3, on page 2

- New in Release 7.5.2, on page 2
- New in Release 7.5.1
- New in Release 7.5
- New in Release 7.0
- New in Release 6.6
- New in Release 6.4
- New in Release 6.3
- New in Release 6.2
- New in Release 6.1
- New in Release 6.0

New in Release 7.5.3

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 9.2.1. **Note** Splunk engine 9.2.1 supports only Python 3 and is compatible with SWA 12.5, 14.0, 14.5, 15.0, and 15.2.

New in Release 7.5.2

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 8.2.5.
Python Upgrade	The Python version is upgraded from 2.7 to 3.7.
UI Updates	You can now access the Access Control page using the following navigation paths for 7.5.2: • **Settings** > **Users and Authentication** > **Access Controls Users** • **Settings** > **Users and Authentication** > **Access Controls Roles**. • **Settings** > **Users and Authentication** > **Access Controls Password Management**.
Summary Index	Summary Index has been enabled in the **Overview** page to improve the performance.

New in Release 7.5.1

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 7.3.5.
Syslog Parser Update	Syslog parser update for Web Security Appliance 12.0.1-334.

New in Release 7.5

Feature	Description
Splunk Engine Upgrade	The Splunk engine is upgraded to version 7.3.3.
User Drilldown page displays report of AD group details.	In the **User Analysis** > **User Drilldown** page, a new filter is added to search by AD Group name. The AD group details are displayed in the search results. It displays the following details: AD Group, User ID, Destination Domain, Bandwidth Used, and Time Spent.

New in Release 7.0

Feature	Description
AWSR proxy services display events with no WBRS Score in search results	New filter for no WBRS score (Show WBRS: No Score) is added in the **Web Tracking** > **Proxy Services** dashboard. With this filter, you can view the search results for AWSR proxy services with no WBRS score.
Department Membership Reporting displays detailed results for AD Group report	You can now view the following results for AD group reports under **User Analysis** > **Overview**: • Top Groups by Transactions Blocked • Transactions Blocked Summary • Top Groups by Bandwidth Used • Bandwidth Used Summary • Top Groups by User • Bandwidth Used Summary • AD Group Summary • AD Group per User Details

New in Release 6.6

Feature	Description
Search in Custom Dashboards	Searching for data in Custom Dashboards is supported. • You can search for data using the main search field with the submit button. • You can filter the search results using the secondary search field in the results pane.
Export from any page	You can export data (non graphical data) from any dashboard as a comma-separated values (csv) file, an XML file, or a JavaScript Object Notation (json) file. You must hover over the dashboard data display pane to view this option to download.

New in Release 6.4

Feature	Description
Web Tracking Dashboard Updates	• New filters—**User, Client IP, WBRS** minimum and maximum score ranges, and **SNI** are added in the **Web Tracking** > **Proxy Services** dashboard. • You can view and export 10000 transactions from the Proxy Services dashboard.

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 private AWS S3 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 and Restrict Access to Department Reports by Role.

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 and 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

The following ports that are used by AWSR must be open. Ensure that these ports are not blocked in the enterprise firewall.

- 8887/TCP - port number(s) for the python-based application server to listen. This port is called as app server ports.
- 8888/TCP - port to access Cisco Advanced Web Security Reporting GUI. This port is also called as web port.
- 8889/TCP - port that Cisco Advanced Web Security Reporting web use to communicate with the daemon process. This port is called as management port.
- 8886/TCP - mongodb - port that daemon uses to connect to the KV Store server.
- 22/TCP - SSH/SCP/WGET
- 514/TCP - Syslog
- 21/TCP - FTP

Note You can also enable nmap/netstat/iptables to control and verify the system configuration, and RDP on windows.

Set-up Overview

- Install Cisco Advanced Web Security Reporting for the first time:
  - –Installing Cisco Advanced Web security Reporting 7.5.3, on page 7
  - – Licensing and Migration
  - – Create the Folder Structure for Access and Traffic Monitor Log Files
  - – Import and Index Historical Data
  - – Set Up On-going Data Transfers (Including setup of Web Security Appliance.)
  - – Umbrella Log Updates
- Upgrading to Cisco Advanced Web Security Reporting 7.5.3

Installing Cisco Advanced Web security Reporting 7.5.3

Note Make sure that you clear the cookies and cache in the browser before installing/upgrading.

Note For AWSR 7.5.3, login credentials are created during installation. Credentials created during installation will have 'administrator' roles and capabilities/privileges.

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

- On Linux
- On Windows

On Linux

Perform the following tasks in order.

Procedure

Step 1 Download the installer for the version of the Cisco Advanced Web Security Reporting required:
https://software.cisco.com/download/home/284806698/type/283998384/release/7.5.3

Step 2 Extract the installer software at /opt using the below command.

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218.tgz -C /opt
```

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

```
cd /opt/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
```

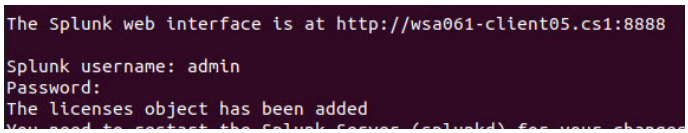
b. Re-run the script.

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

Step 4 Create the administrator username and password and confirm password.

```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/rtestuser/AWSR7.5/cisco_wsa_reporting/etc/openlda
```

Step 5 Enter the username and password created above in the previous step to login.

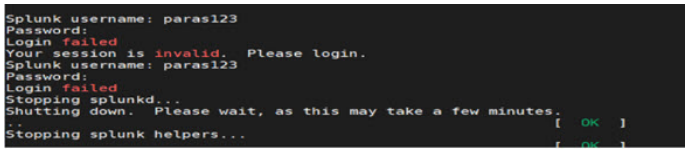


Step 6 Launch Cisco Advanced Web Security Reporting, and log in with the credentials created during installation:

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

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

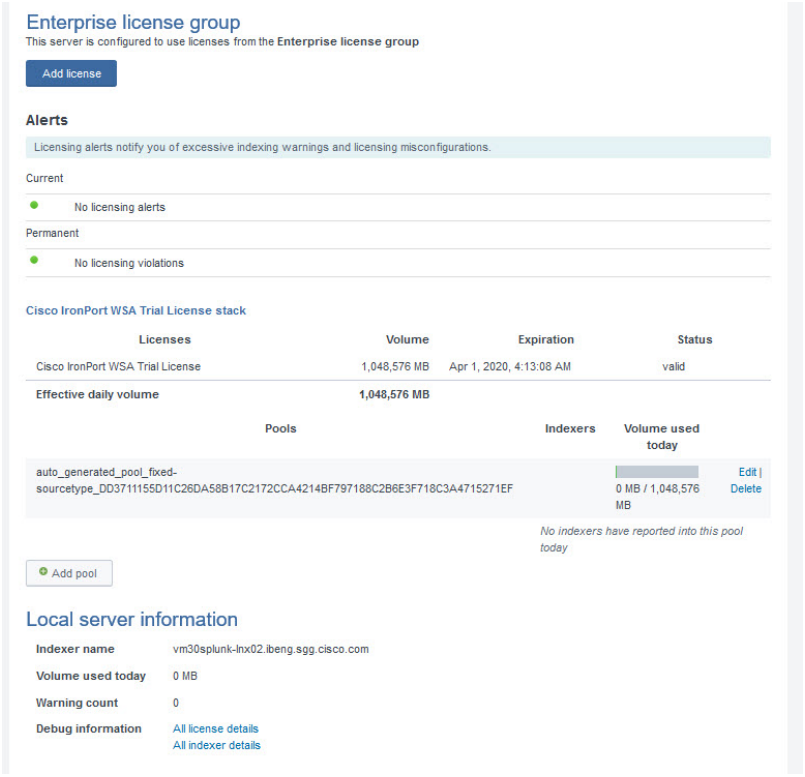
Note
If the username and password is provided incorrectly twice during Splunk login, during the execution of **setup.sh** command, the license does not get added.



To add the license file manually, follow the below steps:

From the `<INSTALL_HOME>` directory, for example, `/opt/cisco_wsa_reporting`:

- Copy the content of the file '**Splunk-eval-120d-500GB.License**' and login to AWSR GUI as administrator.
- Navigate to **Settings** > **SYSTEM** > **Licensing** > **Add license** > click **Copy & paste the license XML directly** and paste the content of '**Splunk-eval-120d-500GB.License**' > **Install** and then restart.



- Post Installation Tasks
- Licensing and Migration

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.

Procedure

Step 1 Download the installer for the version of the Cisco Advanced Web Security Reporting required:

https://software.cisco.com/download/home/284806698/type/283998384/release/7.5.3

Step 2 Extract the installer. You can use applications such as 7-Zip, WinZip, etc.

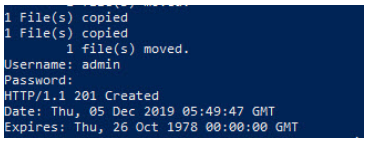
Note

Files related to digital signature can be seen in the directory where the package was extracted. For example, `C:\Users\<UserDirectory>\Downloads\CiscoAdvancedWebSecurityReporting-Windows_7-5-3-0-218.tgz`

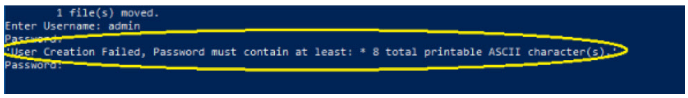
Step 3 Launch a command-line shell (PowerShell) as Administrator, and change the directory to which you extracted the installer.

Step 4 Run the installation command `./install.bat`.

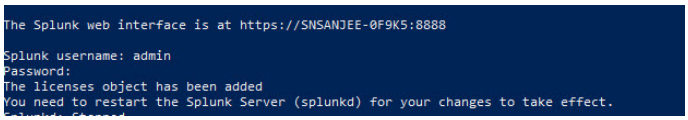
Step 5 Create the administrator username and password and then confirm password.



Note
In case of an invalid length of password, you might get an error message “Password must contain at least 8 total printable ASCII characters”. Ensure that the password contains minimum of 8 ASCII characters for successful user creation.



Step 6 Enter the username and password created above in the previous step to login.



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

Step 7 Reboot the Cisco Advanced Web Security Reporting server.

Step 8 Launch the Cisco Advanced Web Security Reporting application and log in:

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

b. Log in with the username and password created during installation.

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

What to do next

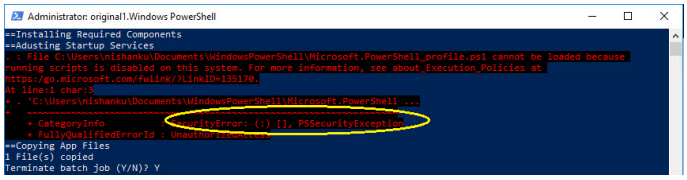
- Post Installation Tasks
- Licensing and Migration

Handling Errors During Installation

The following error might appear during installation. This section describes the common errors that can occur during installation and the steps that you need to be perform to resolve these errors.

Security Error: PSSecurityException

The PSSecurityException error occurs in some cases when you install Cisco Advanced Web Security Reporting on a fresh appliance.

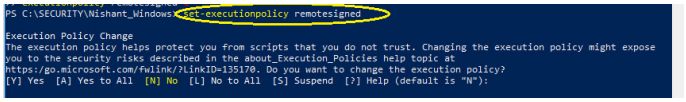


Perform the following steps to resolve this error.

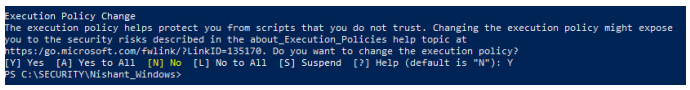
Procedure

Step 1 Run the following command in the prompt:

```
set-executionpolicy remotesigned
```

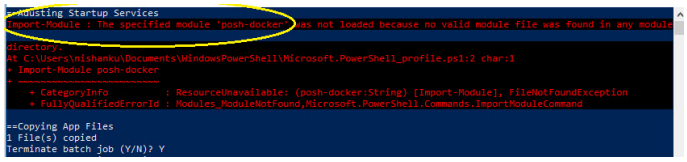


Step 2 Select [Y] yes for any prompt that appear.



Step 3 Re-run the installation command `./install.bat`

Import Module Error: posh-docker

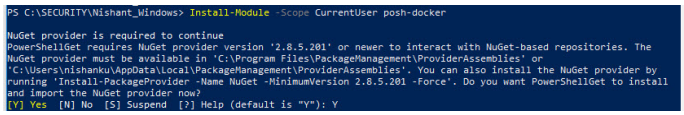


Perform the following steps to resolve this error.

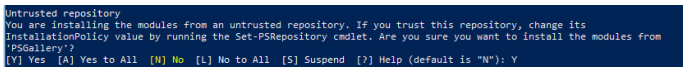
Procedure

Step 1 Run the following command in the prompt:

```
Install-Module -Scope CurrentUser posh-docker
```

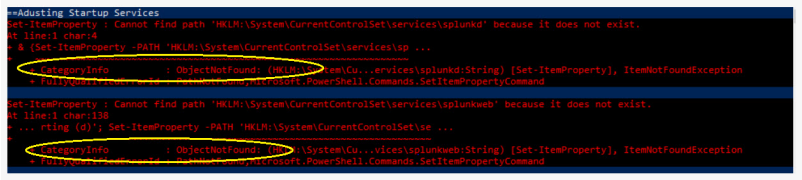


Step 2 Select **[Y]** yes for any prompt that appear.



Step 3 Re-run the installation command `./install.bat`

ObjectNotFound: Cannot find path



Perform the following steps to resolve this error.

Procedure

Step 1 Run the following command in the prompt:

```
New-Item -Path HKLM:\System\CurrentControlSet\services\splunkd -Force | Out-Null
```

```
New-Item -Path HKLM:\System\CurrentControlSet\services\splunkweb -Force | Out-Null
```

Step 2 Re-run the installation command `./install.bat`

Upgrading to Cisco Advanced Web Security Reporting 7.5.3

- On Linux
- On Windows

On Linux

These tasks must be performed in order:

Procedure

Step 1 Navigate to the directory of previous version of installed Cisco Advanced Web Security Reporting.

Step 2 Shutdown the previous session using the `chmod 777 ./shutdown` command.

Step 3 Check if the AWSR is still running through the browser by navigating to `https://<hostname>:8888`.

Step 4 Download new installer for the version of the Cisco Advanced Web Security Reporting in `/opt/` directory from:

https://software.cisco.com/download/home/284806698/type/283998384/release/7.5.3

Step 5 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 file in the `/opt/` directory.

Step 6 Change directory to the installation's base directory (for example, `/opt/`).

Step 7 Untar the new installer from `CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218-rel.tgz` to `CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218.tgz` using the below command:

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218-rel.tgz
```

Step 8 Use the command below to extract the installer. Use appropriate version number.

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218.tgz
cisco_wsa_reporting/SeamlessUpgrade.sh; cp -f cisco_wsa_reporting/SeamlessUpgrade.sh./
```

Step 9 Run the upgrade script. Use appropriate version number.

```
./SeamlessUpgrade.sh CiscoAdvancedWebSecurityReporting-Linux_7-5-3-0-218.tgz
```

- If the result of this command is:

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

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

  ```
  chmod 777 cisco_wsa_reporting/SeamlessUpgrade.sh
  ```

  b. Re-run the script

Step 10 In a browser, open `https://<wsa_reporting_server_host_name>:8888` and log in with the username and password.

On Windows

These tasks must be performed in order:

Procedure

Step 1 Download the installer for the version of the Cisco Advanced Web Security Reporting required:

https://software.cisco.com/download/home/284806698/type/283998384/release/7.5.3

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.

Step 5 In a browser, open `https://<wsa_reporting_server_host_name>:8888` and log in with the username and password.

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.

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:

Procedure

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.

Step 4 Set a password.

Step 5 Click **Save**.

Configuration Best Practices

- Set time zones consistently across Web Security 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.
  1. Choose **Settings** > **Data** > **Data Acceleration**.
  2. Click **Edit**.
  3. Select **Edit Acceleration**.

4. Check the **Accelerate** check box, and select 3 months as **Summary Range**.
5. 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`.

Post Installation Tasks

Enable HTTPS with AWSR

Procedure

Step 1 In Cisco Advanced Web Security Reporting application, choose **Settings** > **System** > **Server Settings**.

Step 2 Click **General Settings**.

Step 3 Click **Yes** for **Enable SSL (HTTPS) in Cisco Advanced Web Security Reporting application**.

By default, AWSR deployments point to the default certificates when encryption is turned on. See Generate and Sign Certificates to sign the certificates.

Step 4 Log into the CLI as `root` user and navigate to `$AWSR_Home/etc/system/local/`

Step 5 Edit **web.conf** file and make sure that the entry `enableSplunkWebSSL = 1` is present in it.

Step 6 Navigate to the `$AWSR_HOME` directory and run the **shutdown.sh** command to stop the AWSR process.

Step 7 Start the AWSR process by executing the **startup.sh** command.

Step 8 You must now add `https://` before the URL you use to access Cisco Advanced Web Security Reporting application.

Disable Client-Initiated Renegotiation

Procedure

Step 1 Log into the CLI as `root` user and navigate to `$AWSR_Home/etc/system/local/`

Step 2 Open the **web.conf** file and append the text `allowSslRenegotiation = false` at the end.

Step 3 Navigate to the `$AWSR_HOME` directory and run the **shutdown.sh** command to stop the AWSR process.

Step 4 Start the AWSR process by executing the **startup.sh** command.

Generate and Sign Certificates

See Generate and Sign Certificates for more details.

Send Strict Transport Security Header

Procedure

Step 1 Log into the CLI as `root` user and navigate to `$AWSR_Home/etc/system/local/`

Step 2 Open the **server.conf** file and append the following text:

```
[httpServer]
replyHeader.X-XSS-Protection= 1; mode=block
replyHeader.Content-Security-Policy = script-src 'self'; object-src 'self'
[sslConfig]
sendStrictTransportSecurityHeader = true
```

Step 3 Open the **web.conf** file and append the following text:

```
sendStrictTransportSecurityHeader = true
replyHeader.X-XSS-Protection= 1; mode=block
```

Step 4 Navigate to the `$AWSR_HOME` directory and run the **shutdown.sh** command to stop the AWSR process.

Step 5 Start the AWSR process by executing the **startup.sh** command.

Restrict Password Length

This topic describes how to configure minimum permitted password length in characters when passwords are set or modified.

Procedure

Step 1 Log into the CLI as `root` user and navigate to `$AWSR_Home/etc/system/local/`

Step 2 Open the **authentication.conf** file and append the following text at the end:

```
[splunk_auth]
minPasswordLength = <positive integer>
```

where, `positive integer` can be a positive number such as 12, 127, 256 etc.

Note
If the **authentication.conf** file is not present in `$AWSR_HOME/etc/system/local` path, then copy the file from `$AWSR_HOME/etc/system/default` path to `$AWSR_HOME/etc/system/local` path and make the changes specified in step 2 above.

Step 3 Navigate to the `$AWSR_HOME` directory and run the **shutdown.sh** command to stop the AWSR process.

Step 4 Start the AWSR process by executing the **startup.sh** command.

Disable Compression Algorithms

The following steps address the SSL/TLS Compression Algorithm Information Leakage Vulnerability.

Procedure

Step 1 Log into the CLI as `root` user and navigate to `$AWSR_Home/etc/system/local/`

Step 2 Open the **server.conf** file and `append allowSslCompression = false` under **[sslConfig]** section.

Step 3 Navigate to the `$AWSR_HOME` directory and run the **shutdown.sh** command to stop the AWSR process.

Step 4 Start the AWSR process by executing the **startup.sh** command.

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 WSA 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 `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.

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`, and `wsa_amplogs`.

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):

Procedure

Step 1 Launch the Cisco Advanced Web Security Reporting application (enter `https://<hostname>:8888` in abrowser 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 7.5.3, on page 12 .
- Know the folder structure. See Create the Folder Structure for Access and Traffic Monitor Log Files.

Procedure

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.

(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`.

Procedure

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
- Know the path to your log files: Create the Folder Structure for Access and Traffic Monitor Log Files.
- 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.

Procedure

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 7.5.3** 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

Procedure

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 7.5.3** 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. You cannot use the same port for two different data inputs. 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
- Determine the frequency of transfers, no more than 60-minute increments.
- Open the web interface for the Web Security Appliance.

Procedure

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.

Setting	Log Type	Value
(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).
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.

Setting	Log Type	Value
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.

Umbrella Log Updates

Before you begin

- Log into the Cisco Advanced Web Security Reporting application as `admin`.
- You must have a private AWS S3 bucket. To configure private S3 bucket, see https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket

Procedure

Step 1 In the Cisco Advanced Web Security Reporting application:

Choose **Settings** > **Data** > **Data inputs** > **Cisco 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 Umbrella. The **client_id** is the AWS bucket name for Umbrella.

Step 5 Click the **More settings** check box and provide the time **Interval** in seconds at which 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 `ciscoumbrella` (for Umbrella reports).

Step 8 Click **Next**.

Step 9 A success screen is displayed.

Note
Not supported on Cisco managed AWS S3 bucket.

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 Information:

- Restrict Access to Department Reports by Role

Set Up Department Membership Reporting

Before you begin

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

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

Procedure

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`.

Procedure

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. 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.

Related Information:

- Users

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
- Schedule PDF Report Generation

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`.

Procedure

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:

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

b. **Email security** (Optional)—Select an email security option. The 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

You can schedule regular generation and emailing of a PDF report for any custom dashboard. See Save As Dashboard for information about creating custom dashboards.

Before you begin

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

Procedure

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.

Schedule Summary Index Generation

Before you begin

rpt_awsr_top_malware_categories will run everyday 0:00 hours for last 24 hours.

Note You can change the schedule based on the requirement.

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

Procedure

Step 1 Go to *https://<host>:8888/en-US/manager/search/saved/searches?app=cisco_wsa_reporting*.

Step 2 Change the owner as **All**.

Step 3 Choose **rpt_awsr_top_malware_categories**.

Step 4 Choose **Edit** > **Edit Schedule**.

Step 5 Change the **Schdule Time** and **Time Range** based on the requirement.

Step 6 Click **Save**.

Create or Modify Users

To create a new user

Procedure

Step 1 Login to Cisco Advanced Web Security Reporting application as an admin user.

Step 2 Choose **Settings** > **USERS AND AUTHENTICATION** > **Access Controls Users- Add New**

Step 3 Enter the following details

a. Username: Enter a unique username (mandatory)

b. Full Name: Enter the first name and last name

c. email address: Enter the email address

d. Time zone: Choose the time zone

e. Default app: **cisco_wsa_reporting** (Advanced Web Security Reporting 7.5.3)

f. Assign to roles or Create a role for this user: To create a new user role, see Create or Modify Roles (mandatory).

g. Password (mandatory): Enter a password.

h. Confirm Password (mandatory): Retype the password

Step 4 Click **Save**.

Delete Users

To delete an existing user:

Procedure

Step 1 Login to Cisco Advanced Web Security Reporting application as an admin user.

Step 2 Choose **Settings** > **USERS AND AUTHENTICATION** > **Access Controls Users**

Step 3 Click **Delete** next to each user to remove that user.

Note
You cannot delete the admin user.

Create or Modify Roles

To create or modify a user role

Procedure

Step 1 Login to Cisco Advanced Web Security Reporting application as an admin user.

Step 2 Choose **Settings** > **USERS AND AUTHENTICATION** > **Access Controls Users- Add New**

Step 3 Enter following details to create a new role

a. **Role Name:** Enter a unique name for the role.

b. **Default app:** cisco_wsa_reporting

c. **Search Restrictions:** Restrict the scope of searches run by this role. Search results for this role will only display events that matches this search string.

– Restrict search terms (Can include source, host, index (can be set below), eventtype, sourcetype, search fields, *, and OR and AND). For example, “host=web* OR source=/var/log/*”

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

– User-level concurrent search jobs limit (Enter the maximum number of concurrent search jobs for each user of this role).

– Real-time search jobs for each user of this role. (This count is independent from the normal search jobs limit).

– Role-level concurrent search jobs limit (Enter the maximum number of cumulative concurrent search jobs for this role).

– Role-level concurrent real-time search jobs limit (Enter the maximum number of cumulative concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit).

– Limit total jobs disk quota (Enter the total disk space in MB that can be used by a user's search jobs. For example, '100' would limit this role to 100 MB total).

d. **Inheritance:** Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities from the parent with broadest permissions. Below are the list of predefined roles that varies depending on the capabilities:

– admin

– can_delete

– power

– splunk_system_role

– user

– wsa_admin

e. **Capabilities:** See the List of Capabilities table below for the available list of capability names.

f. **Indexes searched by default:** Set the index(es) that searches default to when no index is specified. User with this role can search other indexes using index= (For example, “index=special_index”).

g. **Indexes:** Restrict this role's searches to the specified index(es).

h. Click **Save**.

List of Capabilities

Capability name	What it lets you do
accelerate_datamodel	Enable or disable acceleration for data models. Set acceleration to true to enable automatic acceleration of this data model. Additional space is required depending on the number of events, fields, and distinct field values in the data. See the Knowledge Manager Manual for more information.
accelerate_search	Lets the user enable or disable acceleration for reports. The user must also have the schedule_search capability assigned. Works for searches that use transforming commands. See the Knowledge Manager Manual for more information.
admin_all_objects	Lets the user access and modify any object in the system regardless of any restrictions set in the objects. For example user objects, search jobs, reports, and knowledge objects. Allows the user to bypasses any ACL restrictions, much the way root access in a Linux environment does.
change_authentication	Lets the user change authentication settings and reload authentication. See the Securing Splunk Enterprise Manual for more about authentication.
change_own_password	Lets the user change their own password.
delete_by_keyword	Lets the user use the "delete" operator. The "delete" command marks all of the events returned by the search as deleted. This masks the data from showing up in search results but does not actually delete the raw data on disk. See the Search Manual for more information.
dispatch_rest_to_indexers	Lets a user dispatch the REST search command to indexers.
edit_deployment_client	Lets the user change deployment client settings. See the Managing Indexers and Clusters of Indexers Manual for more about the deployment client.

Capability name	What it lets you do
edit_deployment_server	Lets the user change deployment server settings. User can change or create remote inputs that are pushed to the forwarders and other deployment clients. See the Managing Indexers and Clusters of Indexers manual for more about the deployment server.
edit_dist_peer	Lets the user add and edit peers for distributed search. See the Managing Indexers and Clusters of Indexers Manual for more information.
edit_forwarders	Lets the user change forwarder settings, including settings for SSL, backoff schemes, etc. Also used by TCP and Syslog output admin handlers.
edit_httpauths	Lets the user edit and end user sessions through the httpauth-tokens endpoint.
edit_indexer_cluster	Lets the user edit indexer clusters. See the Managing Indexers and Clusters of Indexers Manual for more about indexers.
edit_input_defaults	Lets the user use the server settings endpoint to change default hostnames for input data.
edit_monitor	Lets the user add inputs and edit settings for monitoring files. Also used by the standard inputs endpoint and the one-shot input endpoint.
edit_roles	Lets the user edit roles and change user/role mappings. Used by both the user and role endpoint.
edit_roles_grantable	Lets the user edit roles and change user/role mappings for a limited set of roles. Can assign any role to other users. To limit this ability, configure grantableRoles in authorize.conf. For example: grantableRoles = role1;role2;role3
edit_scripted	Lets the user create and edit scripted inputs.
edit_search_head_clustering	Lets the user edit search head clustering settings.
edit_search_schedule_priority	Lets the user assign a search a higher-than-normal schedule priority. For information about the search scheduler, see the Knowledge Manager Manual.
edit_search_schedule_window	Lets the user assign schedule windows to scheduled reports. Requires the schedule_search capability. For more about the search scheduler, see the Knowledge Manager Manual.
edit_search_scheduler	Lets the user enable and disable the search scheduler. See the Knowledge Manager Manual.
edit_search_server	Lets the user edit general distributed search settings like timeouts, heartbeats, and blacklists.

Capability name	What it lets you do
edit_server	Lets the user edit general server settings like server name, log levels, etc.
edit_server_crl	Lets the user edit general server settings like server name, log levels, etc. Inherits the ability to read general server and introspection settings.
edit_sourcetypes	Lets the user edit sourcetypes. See the Knowledge Manager manual for more information about sourcetypes.
edit_splunktcp	Lets the user change settings for receiving TCP inputs from another Splunk instance.
edit_splunktcp_ssl	Lets the user view or edit any SSL-specific settings for Splunk TCP input.
edit_splunktcp_token	Lets the user edit the Splunktcp token.
edit_tcp	Lets the user change settings for receiving general TCP inputs.
edit_tcp_token	Lets the user change TCP tokens. This is an admin capability and should only be assigned to system administrators.
edit_telemetry_settings	Opt in or out of product instrumentation.
edit_token_http	Lets the user create, edit, display, and remove settings for HTTP token input. Also enables the HTTP Event Collector feature.
edit_udp	Lets the user change settings for UDP inputs.
edit_user	Lets the user create, edit, or remove users. A role with the edit_user capability can assign any role to other users. To limit this ability, configure grantableRoles in authorize.conf. For example, grantableRoles = role1;role2;role3. Also lets a user manage certificates for distributed search.
edit_view_html	Lets the user create, edit, or modify HTML-based views.
edit_web_settings	Lets the user change settings for web.conf through the system settings endpoint.
embed_report	Lets the user embed reports and disable embedding for embedded reports.
export_results_is_visible	Lets the user display or hide the **Export Results** button in Splunk Web. The default value is to display the button.
extra_x509_validation	Lets the user add additional x509 validation.
get_diag	Lets the user get a remote diag from a Splunk instance using the /streams/diag endpoint.

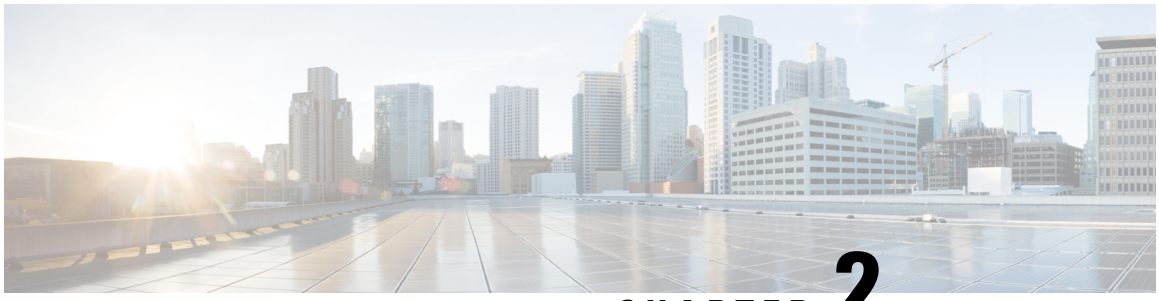
Capability name	What it lets you do
get_metadata	Lets the user use the "metadata" search processor.
get_typeahead	Lets the user use typeahead in the endpoint and the typeahead search field.
indexes_edit	Lets the user change any index settings such as file size and memory limits.
input_file	Lets the user add a file as an input through inputcsv (except for dispatch=t mode) and inputlookup.
license_edit	Lets the user edit the license.
license_tab	Lets the user access and change the license. This attribute is deprecated.
license_view_warnings	Lets the user see a warning message when they are exceeding data limits or reaching the expiration date of their license. These warnings appear on the system banner.
list_accelerate_search	Lets the user view accelerated reports. User cannot accelerate reports.
list_deployment_client	Lets the user view deployment client settings.
list_deployment_server	View deployment server settings.
list_forwarders	Lets a user list and view settings for data forwarding. Can be used by TCP and Syslog output admin handlers.
list_httpauths	Lets the user view user sessions through the httpauth-tokens endpoint.
list_indexer_cluster	Lets the user view the list of indexer clusters as well as indexer cluster objects such as buckets, peers, etc.
list_indexerdiscovery	Lets the user view settings for indexer discovery. Also used by indexer discovery handlers.
list_inputs	Lets the user view lists of various inputs, including input from files, TCP, UDP, scripts, etc.
list_introspection	Lets the user read introspection settings and statistics for indexers, search, processors, queues, etc.
list_search_head_clustering	Lets the user list and view search head clustering objects like artifacts, delegated jobs, members, captain, etc.
list_search_scheduler	Lets the user view lists of search scheduler jobs.
list_settings	Lets the user list and view server and introspection settings such as the server name, log levels, etc.

Capability name	What it lets you do
list_storage_passwords	Lets the user list and view the /storage/passwords endpoint, lets the user perform GETs. The admin_all_objects capability must added to the role for the user to perform POSTs to the /storage/passwords endpoint.
output_file	Lets the user create file outputs, including outputcsv (except for dispatch=t mode) and outputlookup.
pattern_detect	Lets the user see and use the Patterns tab in the Search view.
request_remote_tok	Lets the user obtain a remote authentication token, which lets the user perform some distributed peer management and bundle replication and distribute searches to old 4.0.x Splunk instances.
rest_apps_management	Lets the user edit settings for entries and categories in the python remote apps handler. See restmap.conf for more information.
rest_apps_view	Lets the user list and view various properties in the Python remote apps handler. See restmap.conf for more information.
rest_properties_get	Lets the user get information from the services/properties endpoint.
rest_properties_set	Lets the user edit the services/properties endpoint.
restart_splunkd	Lets the user restart Splunk Enterprise through the server control handler.
rtsearch	Lets the user run real-time searches.
run_debug_commands	Lets the user run debug commands. For example "Summarize".
run_multi_phased_searches	Lets the user run searches with the redistribute command, which invokes parallel reduce search processing in distributed search environments. This capability is not assigned to any role by default.
schedule_search	Lets the user schedule saved searches, create and update alerts, and review triggered alert information.
search	Lets the user run a search. See the Search Manual for more information.
search_process_config_refresh	Lets the user use the "refresh search-process-config" CLI command to manually flush idle search processes.
srchFilter	Lets the user manage search filters. See the Search Manual for more information.
srchIndexesAllowed	Lets the user run search indexes. See the Search Manual for more information.

Capability name	What it lets you do
srchIndexesDefault	Lets the user set default search indexes.
srchJobsQuota	Lets the user set search job quotas.
srchMaxTime	Lets the user set the maximum time for a search.
use_file_operator	Lets the user use the "file" search operator. The "file" search operator is deprecated.
web_debug	Lets the user debug Web files.

Table 1: Windows Specific Capabilities

Capability name	What it lets you do
edit_modinput_admon	Edit modular inputs in admon.conf.
edit_modinput_perfmon	Edit modular inputs in perfmon.conf.
edit_modinput_winhostmon	Add and edit inputs for monitoring Windows host data
edit_modinput_winnetmon	Add and edit inputs for monitoring Windows network data.
edit_modinput_winprintmon	Required to add and edit inputs for monitoring Windows printer data.
edit_win_admon	(Deprecated)
edit_win_eventlogs	Edit windows eventlogs.
edit_win_perfmon	(Deprecated)
edit_win_regmon	(Deprecated)
edit_win_wmiconf	Edit wmi.conf.
list_pdfserver	View PDF server files
list_win_localavailablelogs	List all local Windows event logs.
srchTimeWin	Set search time limits.
write_pdfserver	Write to PDF server files.



CHAPTER 2

Filters and Dashboards

This chapter covers the following sections:

- Overview of Filters and Dashboards, on page 39
- Viewing Dashboards, on page 40
- Creating A Custom Filter, on page 44
- Exporting Data, on page 47
- Data Formats, on page 49
- Time Ranges, on page 49
- Troubleshooting, on page 50
- Usage Scenarios, on page 50

Overview of Filters and Dashboards

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

Viewing Dashboards

Before you begin

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

Procedure

Step 1 Sign into the Cisco 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 for a list of dashboards provided with Cisco Advanced Web Security Reporting. Using the **Custom Filter** option is described in Creating A Custom Filter.

Step 3 Select a time range, data source and host, if applicable.

Note
Searching for data in Custom Dashboards is supported. You can search for data using the main search field with the submit button. You can filter the search results using the secondary search field in the results pane.

Predefined Dashboards

The following dashboards are provided with the Cisco 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 Information:

- Viewing Dashboards

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. These dashboards can be accessed and edited like any other custom dashboard.

Procedure

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.

Procedure

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 aslo 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 Cisco 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:

Procedure

Step 1 Click **Custom Filter** in the Cisco 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.
dnsquery_fixed	Type of DNS request made.

Field	Umbrella Log Data
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 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. SeeSaving a Custom Filter as a Dashboard 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.
  - You can select another data Object from the currently selected Data Model; as described in Creating A Custom Filter.
  - 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.

Procedure

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
- Exporting the Current Dashboard to a PDF File

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.

Procedure

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 Cisco Advanced Web Security Reporting administrator has enabled PDF output.

Procedure

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.

Exporting the Current Dashboard to Other File Formats

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

Procedure

Step 1 Hover over the dashboard data display pane.

Step 2 Click the download icon .

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.

Related Information:

- Set Up Scheduled PDF Reporting (Optional)

Data Formats

In some cases, the presentation of data in Cisco 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 x 1011
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

Troubleshooting

- Cisco 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, Cisco 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
- AD Group Details

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

Procedure

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

Procedure

Step 1 Select **Web Tracking** from the **Cisco Advanced Web Security Reporting** drop-down menu.

Step 2 Select **Proxy Services**.

Step 3 You can search with the following criteria:

- Day
- Data Source
- User ID or Client IP
- User (Enter an authentication username as it appears in reports.)
- Client IP (The client IP address that you want to track. If you leave this field empty, the search returns results for all users.)
- Website
- Transaction Type (All transactions, completed, blocked, monitored, or warned)
- Hostname
- SNI (Retrieves hierarchy)
- WBRS: Min Score Range (You can filter by web reputation score and by a particular web reputation threat. (Select the lower value of the WBRS score range that you want to filter)
- WBRS: Max Score Range (Select the upper value of the WBRS score range that you want to filter)
- (Optional) Advanced (Select this check box to see additional filter options)
- Show WBRS: No Score (You can filter and see results that have no web reputation score. To see transactions that has no WBRS score, select **Show WBRS: No Score** as “True”. To see only those transactions that has no WBRS

score, select **WBRS: Min Score Range** and **WBRS: Min Score Range** as "NA" and select **Show WBRS: No Score** as "True".)

- URL Category
- Application
- Application Type
- Policy
- Malware Threat
- Malware Category
- Reputation Threat
- User Location
- AMP File Verdict
- Filename
- File SHA256

Step 4 (Optional) Click **Export** to export the data to a CSV file. You can view and export 10000 transactions from the **Proxy Services** dashboard.

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

Procedure

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

Procedure

Step 1 Select **URL Categories** from the **Cisco Advanced Web Security Reporting** drop-down menu.

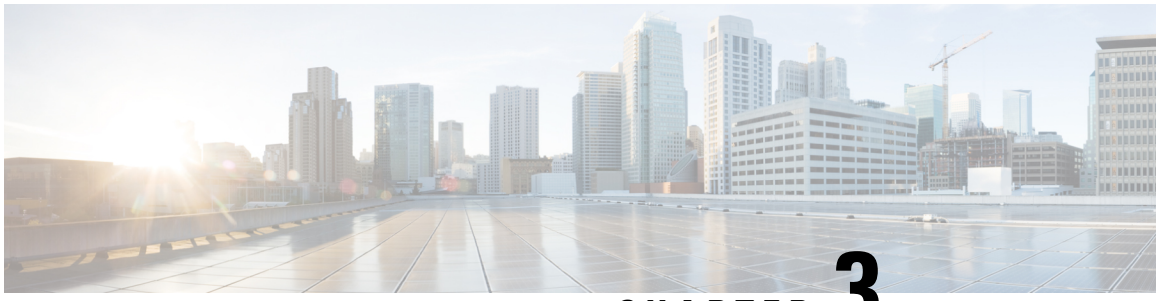
Step 2 View the top ten URL Categories by Total Transactions graph.

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.



CHAPTER 3

CEF Extractor

This chapter covers the following sections:

- About the CEF Extractor Service, on page 55
- Setting Up the CEF Extractor Service, on page 55

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 for more information.
- Configure the master AWSR instance, or "search head." See Configuring the AWSR Master.
- Set up licensing on all master and peer systems. See Configuring Licensing.
- Configure the CEF service on the master system. See CEF Extractor Initial Configuration.
- Restart the Master System
- Configure Mapping of Access Logs to CEF Output Fields
- Configure data inputs for the CEF service. See Configure Data Input for the CEF Extractor Service.

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.

Procedure

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.

Procedure

Step 1 To enable Distributed Search:

a. Click **Settings** > **Distributed Environment** > **Distributed Search**.

b. On the **Distributed search** page, click **Distributed search setup**.

c. On the **Distributed search set up** page, Select **Yes** for the **Turn on distributed search?** option.

d. Click **Save**.

You are returned to the **Distributed search** page.

Step 2 To add a search peer (that is, an indexer):

a. Click the **Add new** link in the **Search peers** row of the **Distributed search** page.

b. 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.

c. 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.

d. 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
- Master Licensing

Peer Licensing

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

Procedure

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.

Procedure

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 dailog 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.

Procedure

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.

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.

Procedure

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.

Procedure

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.

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, and syslog push as data inputs for the service. See Set Up On-going Data Transfers and Umbrella Log Updates for additional information.

Procedure

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).

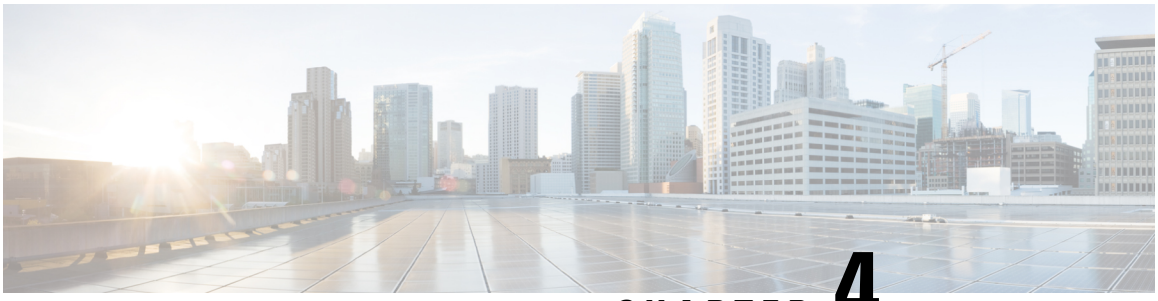
Step 8 For App context, choose **Advanced Web Security Reporting 6.1.0** from the **App context** drop-down list.

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.

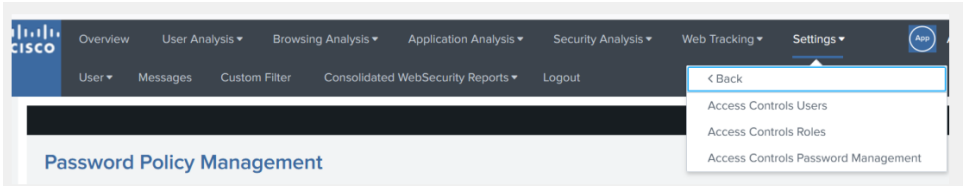
Step 11 Review the information you have entered and then click **Submit** to create the new data input instance.



CHAPTER 4

Password Policy Management

This chapter describes the password related settings that you can perform in the Cisco Advanced Web Security Reporting application web GUI. You need administrator privileges to perform these tasks. Go to the Password Policy Management page by navigating to **Settings** > **USERS AND AUTHENTICATION** > **Access Controls Password Policy Management**.



- Password Rules, on page 63
- Password Expiration, on page 64
- Password History, on page 64
- Login Settings, on page 65
- Password Lockout, on page 66

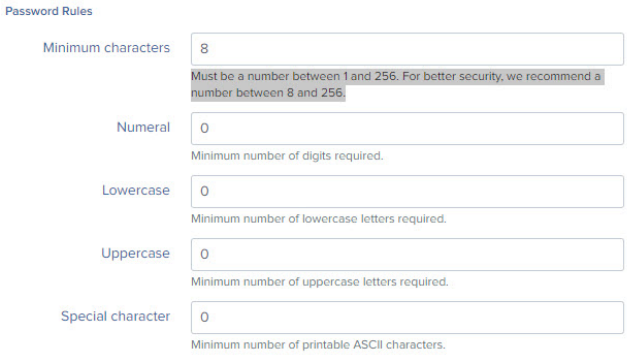
Password Rules

The password should be a combination of numbers, lowercase, uppercase, and alphanumeric characters. You can configure the following fields for setting the password:

- Minimum Characters: To set the minimum number of characters used in the password.

Note This must be a number between 1 and 256. Cisco recommends that you use a number above 8.

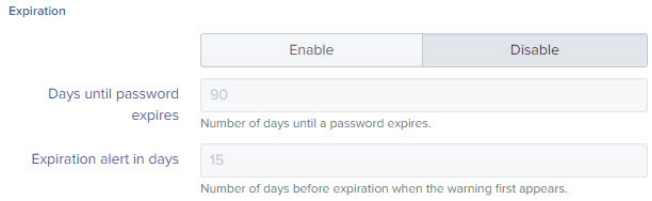
- Numerals: To set the minimum number of numeric characters in the password.
- Lowercase: To set the minimum number of lower case characters in the password.
- Uppercase: To set the minimum number of uppercase characters.
- Special character: To set the minimum number of special characters or alphanumeric characters.



Password Expiration

You can enable or disable the time period for Password expiration. The following fields can be configured:

- Date until password expires: To set the number of days until a password expires.
- Expiration alert in days: To set number of days before expiration when an alert for the user appears.



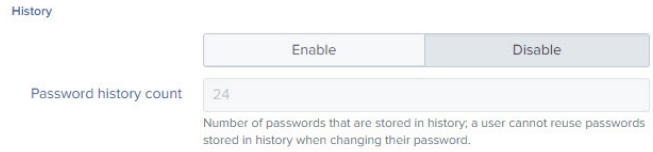
An example for an alert is shown below:

Password History

You can enable or disable the Password History option.

- Password History Count: Number of passwords that are stored in history.

Note A user cannot reuse the passwords stored in history when changing their password.

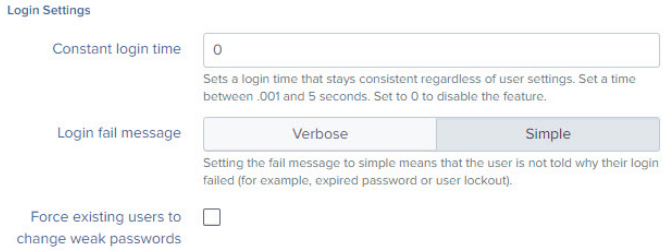


Login Settings

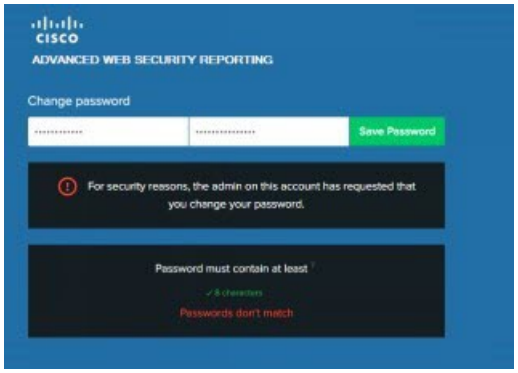
- Constant Login Time: To set a login time that stays consistent regardless of user settings.

Note Set to 0 to disable the feature.

- Login fail message: To set a fail message to the user. If you choose ‘Simple’, then the user is not informed why the login failed (for example, expired password or user lockout etc.).



If there is an error while changing the password, reasons for the error is displayed. Some examples are shown below.



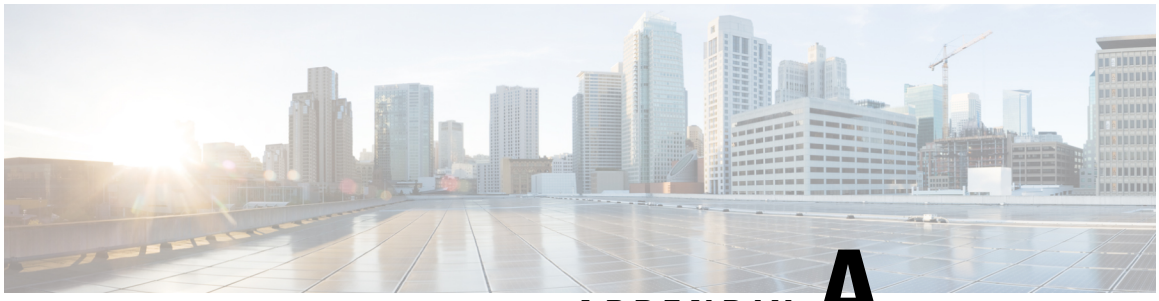
Password Lockout

This feature limits the credential tries per source per unit time to prevent brute force login attacks.

You can configure the following fields:

- Failed login attempts: Number of unsuccessful login attempts that can occur before a user is locked out.
- Lockout threshold in minutes: Time required after the first unsuccessful login for the counter to reset.
- Lockout duration in minutes: Time period of the lockout duration after which a user can try to login again.

After the unsuccessful login attempts, the user account will be locked for a lockout duration specified by Administrator.



APPENDIX A

Generate and Sign Certificates

This chapter covers the following sections:

- Self-sign certificates for Cisco Advanced Web Security Reporting application, on page 67
- Get certificates signed by a third-party for Cisco Advanced Web Security Reporting application, on page 71
- How to prepare your signed certificates for Cisco Advanced Web Security Reporting authentication, on page 73
- Secure your deployment server and clients using certificate authentication, on page 75
- Troubleshoot your Cisco Advanced Web Security Reporting authentication, on page 76

Self-sign certificates for Cisco Advanced Web Security Reporting application

This topic provides basic examples for creating the self-signed certificates in the command line using the version of OpenSSL included with Cisco Advanced Web Security Reporting application.

Since self-signed certificates are signed by your organization, they are not contained in browser certificate stores. As a result, web browsers consider self-signed certificates “untrusted”. This produces a warning page to users and may even prevent access for the user.

Self-signed certificates are best for browser to Cisco Advanced Web Security Reporting application communication that happens within an organization or between known entities where you can add your own CA to all browser stores that will contact Cisco Advanced Web Security Reporting application. For any other scenario, CA-signed certificates are recommended. See Get certificates signed by a third-party for Cisco Advanced Web Security Reporting application for more information.

Before You Begin

In this discussion, `$AWSR_HOME` refers to the AWSR Enterprise installation directory. We recommend that you follow this convention, but if you do not, you should replace `$AWSR_HOME` with your installation directory when using these examples.

For Windows, you might need to set this variable at the command line or in the Environment tab in the System Properties dialog. Default home directories depend on your platform:

- For Windows, the AWSR Enterprise directory is at `C:\Program Files\Cisco\` by default.
- For most Linux platforms, the default installation directory is at `/opt/`.

Generate a new root certificate to be your Certificate Authority

Procedure

Step 1 Create a new directory to host your certificates and keys. For this example we will use `$AWSR_HOME/etc/auth/mycerts`.

Step 2 Generate a new RSA private key. Cisco Advanced Web Security Reporting application supports 2048 bit keys, but you can specify larger keys if they are supported by your browser.

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

On Windows:

Note that in Windows you may need to append the location of the openssl.cnf file:

```
$AWSR_HOME\bin\splunk cmd openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

Cisco Advanced Web Security Reporting application supports 2048 bit keys, but you can specify larger keys if they are supported by your browser.

Step 3 When prompted, create a password.

The private key `myCAPrivateKey.key` appears in your directory. This is your root certificate private key.

Step 4 Generate a certificate signing request using the root certificate private key `myCAPrivateKey.key`:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

Step 5 Provide the password to the private key `myCAPrivateKey.key`.

A new CSR myCACertificate.csr appears in your directory.

Step 6 Use the CSR to generate a new root certificate and sign it with your private key:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out
myCACertificate.pem -days 3650
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out
myCACertificate.pem -days 3650
```

Step 7 When prompted, provide for the password to the private key `myCAPrivateKey.key`.

A new certificate `myCACertificate.pem` appears in your directory. This is your public certificate.

Create a new private key for Cisco Advanced Web Security Reporting application

Procedure

Step 1 Generate a new private key:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048 -config
```

Step 2 When prompted, create a password.

A new key, `myAWSRWebPrivateKey.key` appears in your directory.

Step 3 Remove the password from your key. (Cisco Advanced Web Security Reporting application does not support password-protected private keys.)

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

You can verify that your password was removed with the following command:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -text
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -text
```

You should be able to read the contents of your certificate without providing a password.

Create and sign a server certificate

Procedure

Step 1 Create a new certificate signature request using your private key `myAWSRWebPrivateKey.key`:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

The CSR `myAWSRWebCert.csr` appears in your directory.

Step 2 Self-sign the CSR with the root certificate private key `myCAPrivateKey.key`:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl x509 -req -in myAWSRWebCert.csr -CA myCACertificate.pem -CAkey
myCAPrivateKey.key -CAcreateserial -out myAWSRWebCert.pem -days 1095
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl x509 -req -in myAWSRWebCert.csr -CA myCACertificate.pem -CAkey
myCAPrivateKey.key -CAcreateserial -out myAWSRWebCert.pem -days 1095
```

Step 3 When prompted, provide the password to the root certificate private key `myCAPrivateKey.key`.

The certificate `myAWSRWebCert.pem` is added to your directory. This is your server certificate.

Create a single PEM file

Combine your server certificate and public certificates, in that order, into a single PEM file.

Here's an example of how to do this in Linux:

```
# cat myAWSRWebCert.pem myCACertificate.pem > myAWSRWebCertificate.pem
```

Here's an example in Windows:

```
# type myAWSRWebCert.pem myCACertificate.pem > myAWSRWebCertificate.pem
```

Set up certificate chains

To use multiple certificates, append the intermediate certificate to the end of the server's certificate file in the following order:

```
<div class=samplecode
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
</div>
```

So for example, a certificate chain might look like this:

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

Get certificates signed by a third-party for Cisco Advanced Web Security Reporting application

This topic provides basic examples for creating the third-party signed certificates necessary to configure Cisco Advanced Web Security Reporting application for SSL authentication and encryption.

Create a new private key for Cisco Advanced Web Security Reporting application

Procedure

Step 1 Create a new directory to host your own certificates and keys. In this example we will use `$AWSR_HOME/etc/auth/mycerts`.

We recommend that you place your new certificates in a different directory than `$AWSR_HOME/etc/auth/splunkweb` so that you don't overwrite the existing certificates. This ensures that you can use the certificates that ship with AWSR for other AWSR components as necessary.

Step 2 Generate a new private key. CISCO Advanced Web Security Reporting application supports 2048-bit keys or larger.

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

Step 3 Create a password when prompted to enter the passphrase for the original key.

A new private key `myAWSRWebPrivateKey.key` is added to your directory. You can use this key to sign your CSR.

Step 4 Remove the password from the private key. CISCO Advanced Web Security Reporting application does not support private key passwords.

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key -config
$AWSR_HOME\openssl.cnf
```

You can use to following command to make sure that your password was successfully removed:

```
# openssl rsa -in myAWSRWebPrivateKey.key -text
```

If the password was successfully removed, you can view the certificate contents without providing a password.

Create a Certificate Authority (CA) request and obtain your server certificate

Procedure

Step 1 Create a new certificate signature request using your private key `myAWSRWebPrivateKey.key`:

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

Note for Windows platforms: If you see an error similar to this:

```
Unable to load config info from

c:\\build-amd64-5.0.2-20130120-1800\\AWSR/ssl/openssl.cnf
```

Try typing the following in your command prompt then run the openssl command again:

```
set OPENSSL_CONF=c:/Program Files/AWSR/openssl.cnf
```

Step 2 Use the CSR `myAWSRWebCert.csr` to request a new signed certificate from your Certificate Authority (CA). The process for requesting a signed certificate varies depending on how your Certificate Authority handles a certificate signature request. Contact your CA for more information.

Step 3 Download the server certificate returned by your Certificate Authority. For this example, let's call it "`myAWSRWebCert.pem`".

Step 4 Download your Certificate Authority's public CA certificate. For this example, let's call it "`myCAcert.pem`".

Step 5 Make sure that both the server certificate and the public CA certificate are both in PEM format. If the certificates are not in PEM format, convert them using the `openssl` command appropriate to your existing file type. Here's an example of a command that you can use for DER formats:

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myAWSRWebCert.crt -inform DER -out myAWSRWebCert.pem
-outform PEM
```

```
$AWSR_HOME\bin\splunk cmd openssl x509 -in myCACert.crt -inform DER -out myCACert.pem -outform PEM
```

Step 6 Check both certificates to make sure they have the necessary information and are not password protected.

On Linux:

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myCACert.pem -text
```

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myAWSRWebCert.pem -text
```

On Windows:

```
$AWSR_HOME\bin\splunk cmd openssl x509 -in myCACert.pem -text
```

```
$AWSR_HOME\bin\splunk cmd openssl x509 -in myAWSRWebCert.pem -text
```

The issuer information for `myAWSRWebCert.pem` should be the subject information for `myCACert.pem` (unless you are using intermediary certificates).

Combine your certificate and keys into a single file

Combine your server certificate and public certificate, in that order, into a single PEM file.

Set up certificate chains

To use multiple certificates, append the intermediate certificate to the end of the server's certificate file in the following order:

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

So for example, a certificate chain might look like this:

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

Note that the root CA that signed the intermediate certificate and all intermediary certificates must be in the browser certificate stores.

How to prepare your signed certificates for Cisco Advanced Web Security Reporting authentication

Once you have your certificates, you must combine the server certificate and your keys into a single file that Cisco Advanced Web Security Reporting software can use.

Note Make sure your certificates and public key are in x509 format and that your private key is in RSA format.

Create a single PEM file

Combine your server certificate and public certificate, in that order, into a single PEM file. For the examples here, we are using the file names described in Self-sign certificates for Cisco Advanced Web Security Reporting application and Get certificates signed by a third-party for Cisco Advanced Web Security Reporting application.

The following is an example for Linux:

```
cat myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem >

myNewServerCertificate.pem
```

The following is an example for Windows:

```
type myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem >

myNewServerCertificate.pem
```

Once created, the contents of the file `myNewServerCertificate.pem` should contain, in the following order:

- The server certificate (`myServerCertificate.pem`)
- The private key (`myServerPrivateKey.key`)
- The certificate authority public key (`myCACertificate.pem`)

Here's an example of a properly concatenated certificate:

```
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Server Certificate>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CFCECC7976725DE5
S+DPcQ0l2Z1bk71N3cBqr/nwEXPNDQ4uqtecCd3iGMV3B/WSOWAQxcWzhe9JnIsl
...
<Server Private Key – Passphrase protected>
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Certificate Authority Public Key>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn
-----END CERTIFICATE-----
```

How to configure certificate chains

To use multiple certificates, append the intermediate certificate to the end of the server's certificate file. You can add as many certificates you need to in decreasing order of hierarchy, up to the root.

The certificates should be concatenated in the following order:

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

So for example, a certificate chain might look like this:

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

In another example, when using AWSR Forwarder to Indexer Certificates that contain a Private Key,the completed certificate file might look like this :

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
```

```
...<Server Private Key – Passphrase protected>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

Secure your deployment server and clients using certificate authentication

Authentication using signed certificates between deployment servers and clients is not recommended, because the configuration data pushed from the deployment server to client does not generally provide exploitable information. Configuring certificate authentication for a deployment server and clients impacts the rest of your configuration as follows:

- Cisco Advanced Web Security Reporting application will fail to authenticate unless you also configure it to use the certificate.
- The CLI will be not be able to communicate with the deployment server.

You may find certificate authentication necessary in certain distributed configurations, perhaps where extremely sensitive server configuration data is sent to a variety of locations outside your firewall. You can manually configure each indexer to communicate with your Deployment Server:

Note The deployment server cannot properly push certificates to peers. You must configure each member separately.

Procedure

Step 1 Create one or more certificates using the same root CA.

Step 2 Distribute the certificates to your deployment server and clients.

Step 3 Edit **server.conf** to provide the location of your certificates:

```
[sslConfig]

enableSplunkdSSL = true

sslVersions = Defaults to "*,-ssl2" (anything newer than SSLv2). This is the recommended
setting.

serverCert = The full path to the PEM format server certificate file. Default
certificates

($SPLUNK_HOME/etc/auth/server.pem) are generated by Splunk at start. To secure Splunk,
you should replace the default cert with your own PEM file.
```

```
sslPassword = password

sslRootCAPath = absolute path to the operating system's root CA (Certificate Authority)
PEM

format file containing one or more root CA. Do not configure this attribute on Windows.
```

Step 4 Edit server.conf to authenticate against your certificates by adding the following attribute to the [sslConfig] stanza in previous step:

```
requireClientCert = true
```

Note
This `requireClientCert` is set to “false” by default. If you change it to true to force Splunk to check your client's certificates, Cisco Advanced Web Security Reporting application and the CLI will also be checked for certificates. Your CLI connection will no longer work because your CLI is unable to present a certificate as a client.

Step 5 Edit web.conf to present a certificate signed by the same root CA so that Cisco Advanced Web Security Reporting application can connect to the server.

The following is an example of an edited settings stanza:

```
[settings]
enableSplunkWebSSL = true
privKeyPath = etc/auth/splunkweb/mySplunkWebPrivateKey.key
serverCert = etc/auth/splunkweb/mySplunkWebCertificate.pem
cipherSuite = <your chosen cipher suite (optional)>
```

Note
Cisco Advanced Web Security Reporting application does not support passwords, so you must remove the password from the private key.

Troubleshoot your Cisco Advanced Web Security Reporting authentication

If you are unable to verify your certificate configuration, you can use the **web_service.log** in `$AWSR_HOME/var/log/splunk` to view and troubleshoot any errors that occur upon restart.

Look for SSL configuration warnings. For example, if you provide an incorrect path to the server certificate declared in `serverCert`, Cisco Advanced Web Security Reporting application fails to start and the following error appears:

```
2010-12-21 16:25:02,804 ERROR [4d11455df3182e6710] root:442 - [Errno 2] No such file or
directory: '/opt/splunk/share/splunk/mycerts/mySplunkWebCertificate.pem'
```

Note If the private key is provided in `privKeyPath` is password protected, no error is provided but your browser won't load Cisco Advanced Web Security Reporting application.