CEF Extractor

This chapter covers the following sections:

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.

Step 1 Choose **Settings** > **Data** > **Forwarding and Receiving**.

Step 2 On the **Forwarding and receiving** page, click the **Add new** link in the **Configure receiving** row of the **Receive data** section of this page.

If the desired listener port is already configured, you can click the **Configure receiving** link to go directly to the **Receive data** page to enable the port.

Step 3 On the **Add new – Configure receiving** page, enter the number of the port to listen on.

Step 4 Click **Save**.

You are returned to the **Receive data** page which lists the available listen-on ports—you can enable/disable and delete individual ports. You also can add new ports from this page.

Configuring the AWSR Master

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

Before you begin

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

Step 1 To enable Distributed Search:

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.

Step 1 On the indexer system, choose **Settings** > **System** > **Licensing** to open the Licensing page.

A notification of this server's licensing role is displayed at the top of this page. The server's role can be either "associated with a remote master license server," or "acting as a master license server."

Step 2 If this peer's displayed role is **acting as a master license server**, click the **Change to slave** button.

Step 3 On the **Change master association** page, select **Designate a different AWSR instance as the master license server**.

Step 4 Provide the master license server access information: either the *server_name:management_port or IP_address:management_port* of the desired server.

Step 5 Click **Save**.

Master Licensing

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

Step 1 On the search head, choose **Settings** > **System** > **Licensing** to access the Licensing page.

A notification of this server's licensing role is displayed at the top of this page. The server's role can be either "associated with a remote master license server," or "acting as a master license server."

Step 2 If this peer's displayed role is **associated with a remote master license server**, click the **Change to master** button and designate this server as the master license server in the Change master association 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.

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.

Step 1 Choose **Settings** > **System** > **Server Controls** to access the Server controls page.

Step 2 Click the **Restart AWSR** button and follow the instructions to restart the system.

Step 3 When restart is completed; log in again.

Configure Mapping of Access Logs to CEF Output Fields

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

Step 1 Choose **Settings** > **Third Party Services** > **CEF Extractor** to access the **CEF Extractor** page.

Step 2 Click **New** to launch the **CEF Extractor data-search set-up** wizard.

Step 3 Choose the **Data Model** from which to retrieve data; in this case, choose **Web_Access_Data**.

Step 4 Choose **Web_Access_Event** from the **Object** drop-down list indicating the data fields are to be obtained from Web Security appliance's Web access logs.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  Note If you are planning to output syslog data, you cannot use TCP port 514 here, as it is already in use; see Configuration Of Data Input for Web Security Appliance Syslogs.

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.

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.