Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Extreme Networks Dragon Export Tool File

Configuration Guide

February 15, 2017

Configuration Guide

SmartConnector for Extreme Networks Dragon Export Tool File

February 15, 2017

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
02/15/2017	End of support for versions 6.0 and 6.3 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/14/2014	Added support for device version 8.2. Changed connector name from “Enterasys Dragon Export Tool File” to “Extreme Networks Dragon Export Tool File”.
03/29/2013	Added support for device version 8.0.
05/15/2012	Added new installation procedure.
06/30/2011	General availability of version 7.4 support; support added for IPv6 address fields.
05/15/2011	Added beta support for device version 7.4.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Added global update to installation procedure.
02/11/2009	Updated Revision History for 11/12/2008 from version 7.2.3 to 7.3.

Contents

SmartConnector for Extreme Networks Dragon Export Tool File

This guide provides information for installing the SmartConnector for Extreme Networks Dragon Export Tool File (formerly Enterasys Dragon Export Tool File) and configuring the device for log file event collection. Extreme Networks Dragon versions 7.0, 7.3, 7.4, 8.0, and 8.2 are supported.

Product Overview

Designed to meet the unique security requirements of the enterprise environment, the Dragon Intrusion Defense System (IDS) offers comprehensive features that minimize network vulnerabilities and bring improved security to the enterprise.

Configuration

The Export Log (a flat rotating list of files named `dragon.log.001`, `dragon.log.002` and so on) produces a one-line log for each Dragon event including the event name, the IP addresses involved and other information. The log file is stored in a chronological directory such as `~/DB/2006Nov05` (or `~/DB/06Nov05` when the Y2K keyword is not present).

Configuring the Export Log

Recording of events to the log files is influenced by the rotation attribute. The rotation attribute indicates how often (in days) to rotate to a new log file. A series of tokens are available that are used to indicate which fields from a Dragon event should be included in the export log file.

The Export Log agent is available only on Linux and Solaris platforms.

To configure the Export Log agent:

1. Click the **Enterprise View** icon and the **Enterprise View** tab.
2. Expand the tree to reveal the agents under the desired device.
3. Click **Export Log**. The display area is populated.
4. Enter the desired criteria. Export Log Format specifies which of the available fields should be included in each export log record written to the log file. It can also be used to indicate the ordering of those fields. Fields are identified by listing one or more tokens to represent the available data fields. The available data fields are:

%T	Event Date/Time (YYYY-MM-DD-HH:MM:SS)
%t	Event Date (YYYY-MM-DD)
%h	Event Time (HH:MM:SS)
%N	Sensor Name
%E	Event Name
%S	Source IP Address (dotted quad representation)
%s	Source IP Address (numeric representation)
%D	Destination IP Address (dotted quad representation)

%d	Destination IP Address (numeric representation)
%G	Source Port
%H	Destination Port
%A	Event Header
%B	Event Direction
%P	Event Protocol
%C	Event Flags Field
%F	Filler Field (using filler-value)
%X	Event Data

The separator is used to indicate a character to be used as a field separator between data fields in the export log.

The Filler Value is used to pad export log records with filler fields with a specific filler value.

Log File Rotation indicates how often (in days) to rotate to a new log file. Initially, log file names are appended with the sequence number 001. As each rotation in days is reached, a new file is created with the extension incremented by one (for example, .002). By specifying a large value (such as 2000000), the export log can be forced to never rotate to a new log file.

Configure Payload Support

Extra information can be retrieved by using the on-demand payload feature on the ArcSight ESM Console. Click on any of the vulnerability events sent by the SmartConnector and you will see in the Event Inspector that Payload data is available; click on the **Payload** tab for additional information, including **Description** and **Recommendation**. For services events, **Description** and **Detail** information is displayed.

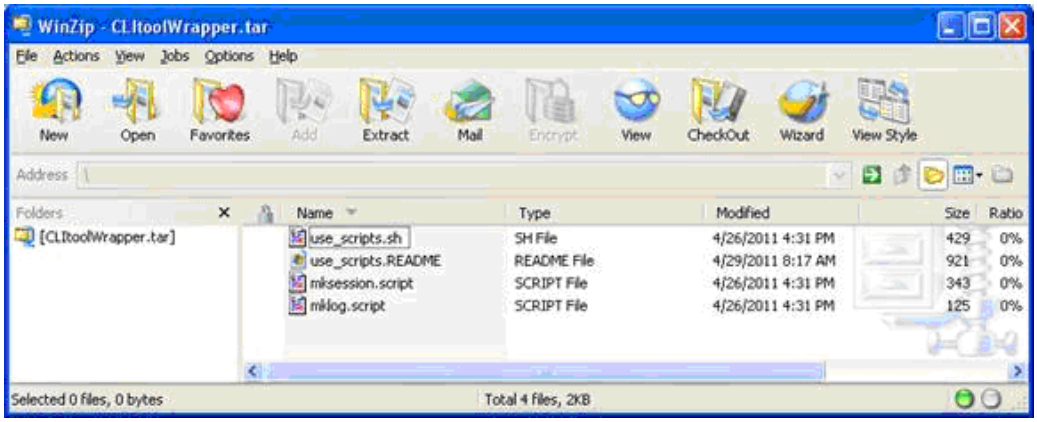
Configuring for v8.0 and v8.2 Payload Retrieval

The `mklog` and `mksession` commands, used by the connector for payload retrieval, cannot be executed from outside the Tools directory of the Dragon installation. For example, executing `/opt/dragon/tools/mklog` from the `/root` directory does not work; it must be executed from `/opt/dragon/tools/`. In addition, the interface for the `mklog` and `mksession` commands have changed with Dragon v7.4.

Extreme Networks has developed wrapper scripts that address these issues. Download the scripts as follows.

1. Log in to your Extreme Networks account.
2. From https://extranet.extremenetworks.com/downloads/pages/IPS.aspx, click the **Utilities** tab. Expand **Tools**.
3. Download the **CLI Tool Compatibility Scripts**.

This .tar file contains `mksession.script` and `mklog.script` files as well as a readme telling you how these files are to be used.



Handling Event Payload

During SmartConnector installation and configuration, you can set a **Payload Timeout** parameter. The default value for this parameter is 60 seconds. If you enter a value greater than 60 seconds for this parameter, certain properties also must be added to the `console.properties` file for the ESM Console and the `server.properties` file for the ESM Manager.

Add the following property to the `console.properties` file in the `config` folder on each ArcSight ESM Console machine:

```
console.payloadTimeout=value
```

where *value* is the number of seconds you will specify for the Payload Timeout parameter during connector installation.

Add the following properties to the `server.properties` file in the `config` folder of the ArcSight ESM Manager machine:

```
payload.eventrequest.timeout=value
payload.eventrequest.maxretry=value
payloadservice.requests.timeout=value
```

where *value* is the number of seconds you will specify for the Payload Timeout parameter during connector installation.

You can retrieve, preserve, view, or discard payloads using the ArcSight Console. Because event payloads are relatively large, ArcSight does not store them by default. Instead, you can request payloads from devices for selected events through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console.

Payloads are downloaded and stored only on demand; you must configure ESM to log these packets. By default, 256 bytes of payload will be retrieved.

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view. In an ArcSight Console Viewer panel grid view, right-click a column header and choose **Add Column -> Device -> Payload ID**. Look for events showing a Payload ID in that column.

In a Viewer panel grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab, then click **Retrieve Payload**.

In a grid view, right-click an event with an associated payload, select **Payload**, then **Preserve**. Alternatively, in the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

In a grid view, right-click an event with an associated payload and select **Payload**, then **Discard Preserved**. You also can use the Event Inspector: In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Discard Preserved Payload**.

In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Save Payload**. In the **Save** dialog box, navigate to a directory and enter a name in the **File name** text field. Click **Save**.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

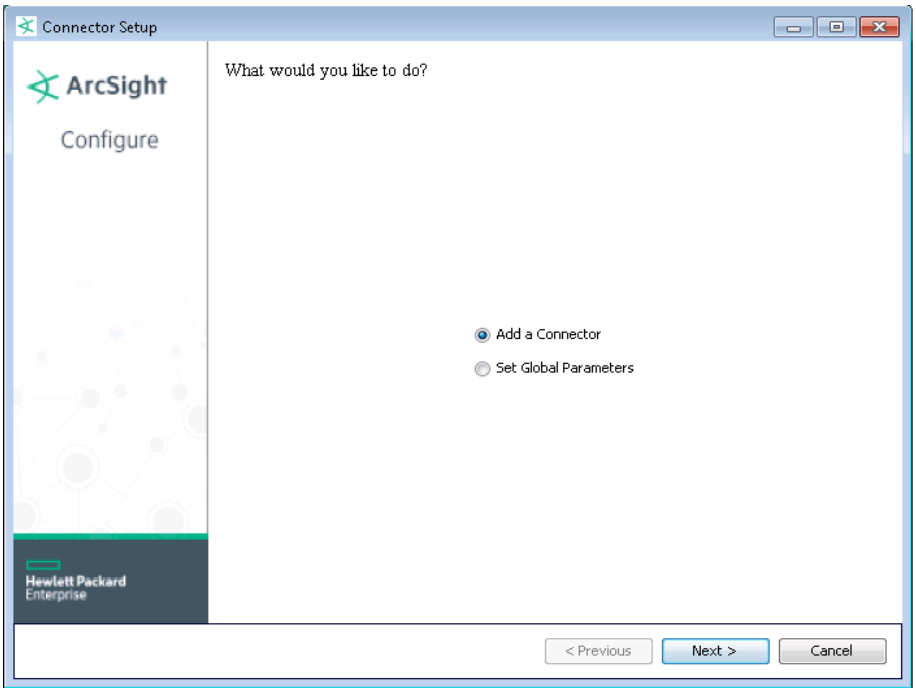
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is IPv4.

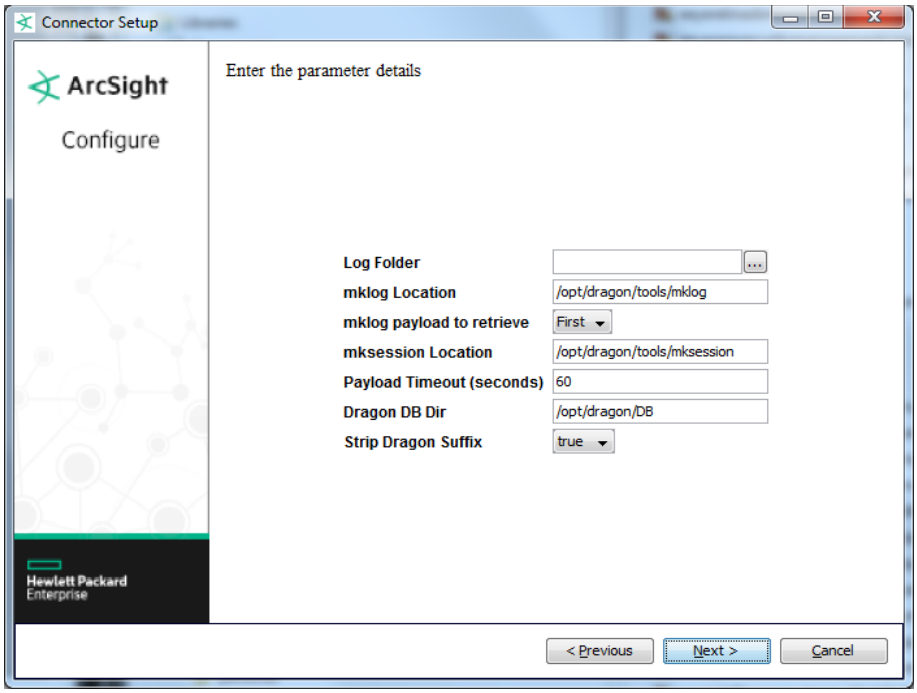
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **Extreme Networks Dragon Export Tool File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log Folder	Path to and name of the file to which Dragon IDS alerts are sent. All Dragon log files end with a .log extension and are usually found in the Dragon logs directory (for example, /home/dragon/logs/dragon.log.001).
mklog Location	Enter the path to the 'mklog' executable, which is used to retrieve payload data. The default location of the 'mklog' executable is the 'tools' directory under the Dragon installation directory (for example, /home/dragon/tools/mklog). 'mklog' produces lists of Dragon events, a hex dump of events, and based events.
mklog payload to retrieve	Select 'First', 'Last', or 'All' for the mklog report to filter the first event, the last event, or all events, respectively.
mksession Location	Enter the path to the 'mksession' executable, which is used to retrieve payload data. The default location of the 'mksession' executable is the 'tools' directory under the Dragon installation directory (for example, /home/dragon/tools/mksession). 'mksession' reconstructs TCP and UDP sessions from IP packets collected in the dragon DB file and also lists times, IP addresses, and ports of active sessions in a dragon db file.
Payload Timeout(seconds)	The default payload timeout value is 60 seconds. If you change this to any timeout value greater than 60 seconds, in addition to configuring it here, timeout properties must be set in the server.properties file for the ESM Manager and the console.properties file for the ESM Console. See "Payload Support" for complete information.
Dragon DB Dir	Enter the path to the Dragon payload database directory. This is usually the directory named 'DB' in the Dragon installation directory (for example, /home/dragon/DB).
Strip Dragon Suffix	Select 'true' or 'false'.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Dragon Export Log Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	Target
Destination Port	Target Port
Device Custom IPv6 Address 2	Source (Source IPv6 address)
Device Custom IPv6 Address 3	Target (Destination IPv6 address)
Device Custom String 1	Name plus Message
Device Custom String 5	Extra Info
Device Event Class Id	Name
Device Host Name	Device
Device Product	'Dragon'
Device Receipt Time	Date
Device Vendor	'Extreme Networks'
File Hash	MD5
File Name	File
Message	Message
Name	Name
Source Address	Source
Source Port	Source Port
Transport Protocol	Protocol