Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Extreme Networks Dragon IDS File

Configuration Guide

February 15, 2017

Configuration Guide

SmartConnector for Extreme Networks Dragon IDS 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

Revision History

Date	Description
02/15/2017	End of support for version 5.0 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/14/2014	Renamed vendor for this connector.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Added global update to installation procedure.
11/12/2008	Added support for device version 7.3.
03/01/2008	Update to installation procedure.
12/18/2007	Updated configuration information.
03/01/2007	General content update.
10/31/2006	Added payload information.

SmartConnector for Extreme Networks Dragon IDS File

This guide provides information for installing the SmartConnector for Extreme Networks Dragon Intrusion Defense System (IDS) and configuring the device for log file event collection. Extreme Networks Dragon IDS versions 6.0, and 7.3 are supported.

Product Overview

The Dragon Network Sensor identifies misuse and attacks across the network. Dragon's Intrusion Prevention (IPS) technology is designed to block attackers, mitigate denial-of-service attacks, and prevent information theft while remaining totally invisible to the network.

Configuration

Configuration notes:

1. Dragon can be configured to store alerts on the sensor. The ArcSight SmartConnector must reside on the same machine (sensor or manager) that contains the dragon alerts.
2. The user running the ArcSight connector process (usually the `arcsight` user) must have read access to both the Dragon alerts file and the Dragon payload database. To accomplish this, assign both Dragon and ArcSight users to the same group, or use the same user to run both processes.

Configuring Dragon

The network sensor policy consists of a variety of modules that configure the protected network, protocol analysis, covert channel analysis, and many other detailed configuration items that determine exactly what your sensor analyzes.

Dragon Logging Module

This module defines where logs are stored and how they are displayed.

1. Click the **Network Sensor Policy View** icon and the **Network Policies View** tab.
2. Expand the tree by and select the desired custom policy name. The modules for that policy are displayed in the tree.
3. Click the **Logging Module** in the tree. The display area is populated with the entry fields.
4. Select from the following (because the connector reads from a log file, do not select 'Syslog Only'):

Field	Description
Ring Buffer	Configures the sensor to write to a shared memory ring buffer.
Alarm Log Display	Enables alarmlog attributes by sending events to standout output for live monitoring.
Alarm Log File	Configures the sensor to log events in a syslog style format, where one line is used for every recorded event. Information is stored in chronological directories such as ~/DB/2000Nov02.

Field	Description
Syslog Only	Configures the sensor to log output and debugging information to the system log rather than to stdout or a file.
Local DB	Allows full packet logging to the local file system.
Swatch	Forces the alarmlog file attribute to log to a single file in the main directory.

Alarmtool Agent

The Alarmtool agent sends notifications when the sensors detect an anomaly. The type of notification and conditions for notification are configurable. This agent runs on Solaris and Linux only.

The Alarmtool policies provides a quick and easy method to configure alerts. You can copy master Alarmtool policies to new custom policies, letting you provide minimal configurations and get new alarms up and running quickly.

To configure this agent:

1 Click the **Alarmtool View** icon. A list of master and custom policies is displayed.

2 Right-click a desired master policy. and select **Copy**. A window is displayed requesting the name of the new policy.

3 Enter the policy name and click **OK**.

4 The policy is added under **Custom Policies**.

5 Expand the tree to reveal the newly added policy and click it. The display area is populated with the last tab selected on top.

6 Enter the desired criteria in the **Global Options** tab. These settings are rarely changed after initial configuration for your environment.

- The Main tab configures operations such as where the tool should dump events it does not understand, specify from where the agent gets events, and how to send mail on the system.
- The SNMP tab lets you set the interface the agent uses as the source IP for SNMP Traps.

7 Enter the desired criteria in the **Event Groups** tab. This tab provides a grouping of event names into a collection for use in alarms and threshold settings to limit the need for repeating a long list of events in several places in the file. It has a name attribute that allows the group to be referenced in other elements. Click **New** or **Edit** to invoke a window letting you add or modify events in the list.

8 Enter the desired criteria in the **Alarms** tab. This tab provides a grouping of event names into a collection for use in alarms and threshold settings to limit the need for repeating a long list of events in several places in the file. It has a name attribute that allows the group to be referenced in other elements. Click **New** or **Edit** to invoke a window letting you add or modify events in the list.

9 Enter the desired criteria in the **Alarm Filters** tab. This tab defines a filter for fine-tuning the scope of an alarm beyond just a list of event names within a timeframe. It allows for inclusion by IP or sensor name and other items within the event.

10 Enter the desired criteria in the **Notification Rules** tab. This tab defines how an alarm is sent. It contains a time period within which these notifications are sent, as well as one or more methods with which to send the alarm.

To add a new rule, click the **New** button in the **Notifications** rule list. A window is displayed in which you can enter a rule name and the time period for which the rule applies. For each rule you can add a notification method. You can select one or more methods by clicking its tab and then the **New** button. For example, **Log** specifies a flat file into which the alarm information is to be written.

11 Enter the desired criteria in the **Time Period** tab. This tab contains the necessary elements to define a weekly period of time within which an event can trigger an alarm. You can add new time periods and define the attributes for that period.

12 Enter the desired criteria in the **Thresholds** tab. This tab provides another scope-limiting definition to prevent a likely event from generating an overwhelming number of alarms. It contains an Event Group by name or definition, and then the number of occurrences within an interval that must happen for an alarm to be generated. Click the **New** bullton to add new thresholds to the list.

Binding Policies

Once you have created the policy, you must bind it to the Dragon agent. To bind your new policy:

1 Click the **Enterprise View** icon and the **Enterprise View** tab.

2 Right-click the **Alarmtool Agent** and select **Associate Alarmtool Policy**. The Associate Alarmtool Policy window is displayed.

3 Select the desired policy.

4 Click **OK**.

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.

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.

Locate Payload-Bearing Events

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.

Retrieve Payloads

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**.

Preserve Payloads

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**.

Discard Payloads

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**.

Save Payloads to Files

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

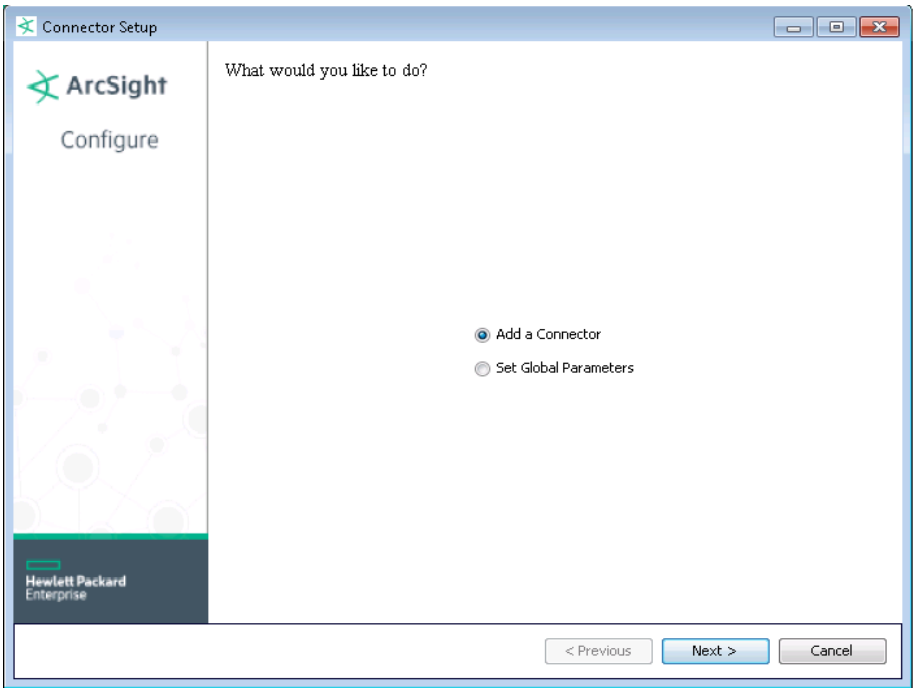
Install Core Software

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.

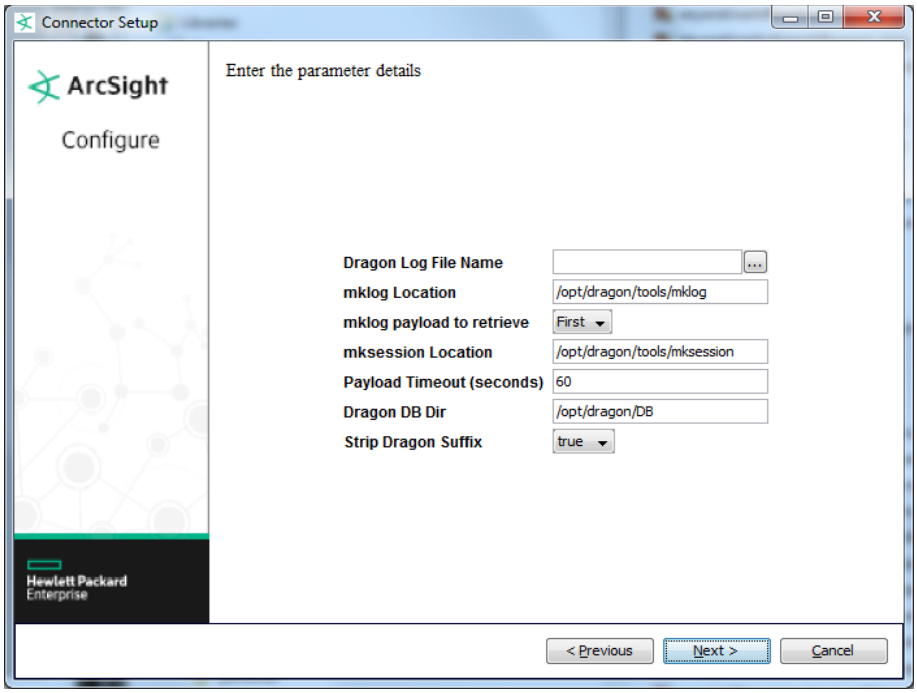
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 IDS File** and click **Next**.

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



Parameter	Description
Dragon Log File Name	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).
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 Option	mklog processes a list of events rom a dragon.db fileSelect '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(s)	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.

Extreme Networks Dragon IDS Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Custom String 1	DragonEventName
Detect Time	LocalDatestamp, LocalTimestamp
Device Product	'Dragon'
Device Vendor	'Extreme Networks'
Event Name	DragonEventName
Protocol	DragonProtocol
Source Address	DragonSourceIP
Source Port	DragonSourcePort
Target Address	DragonTargetIP
Target Port	DragonTargetPort