Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for IBM WebSphere File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for IBM WebSphere File

October 17, 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://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	End of support for IBM WebSphere versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2014	Added support for WebSphere 8.5.
05/15/2012	Added new installation procedure.
02/15/2011	Added support for WebSphere 6.0, 6.1, and 7.0.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
08/12/2009	Added support for multiple log files; updated field mappings.
06/30/2009	Global update to installation procedure for FIPS support.

Contents

SmartConnector for IBM WebSphere File

This guide provides information for installing the SmartConnector for IBM WebSphere File and configuring the device for log file event collection. IBM WebSphere versions 7.0 and 8.5 are supported.

Product Overview

WebSphere provides application integration by passing messages between applications and Web services, reducing the risk of information loss and the need to reconcile communicating IT systems by using queuing and transactional facilities that help preserve the integrity of messages across the network.

Configure WebSphere Application Server Logs

About WebSphere Logging

WebSphere Application Server can write system messages to several general purpose logs. These include the Java Virtual Machine (JVM) logs (system.err and system.out), the process logs (native.err and native.out), and the Start Server and Stop Server logs that are processed by the ArcSight SmartConnector.

JVM Logs

The JVM logs are created by redirecting the system.out and system.err streams of the JVM to independent log files. WebSphere Application Server writes formatted messages to the system.out stream. The system.err log contains exception stack trace information that can be used in problem analysis. Because each application server represents a JVM, there is one set of JVM logs for each application server and all its applications, located by default in the **installation_root/logs/server_name** directory. In the case of a WebSphere Application Server network deployment, JVM logs also are created for the deployment manager and each node manager, because they also represent JVMs.

Process Logs

The process logs are created by redirecting the stdout and stderr streams of the process to independent log files. Native code writes to these files. These files can contain information relating to problems in native code or diagnostic information written by the JVM. As with JVM logs, there is a set of process logs for each application server, since each JVM is an operating system process, and in the case of a WebSphere network deployment, a set of process logs for the deployment manager and each node manager.

Start Server Logs

You can use the **startServer** command to start an application server from the command line. You can run this command from the **install_root/bin** directory of a WebSphere Application Server application or a Network Deployment installation.

The following command starts the server, specifies a particular log file, and generates trace information into the file specified with the **logfile** option for debugging purposes:

```
startServer <server> logfile <filename> trace
```

Stop Server Logs

You can use the **stopServer** command to stop an application server from the command line. You can run this command from the **install_root/bin** directory of a WebSphere Application Server installation or a Network Deployment installation.

The following command stops the server, specifies a particular log file, and generates trace information into the file specified with the **logfile** option for debugging purposes:

```
stopServer <server> logfile <filename> trace
```

Server Plug-In Logs

Use this page from the administrative console to view or change the settings of a Web server plug-in configuration file. The plug-in configuration file, **plugin_cfg.xml**, provides properties for establishing communication between the Web Server and the Application Server.

From the administrative console page, select Plug-In Properties for your Web server. On the **Configuration** tab, you can edit fields. On the **Runtime** tab, you can look at read-only information. (The Runtime tab is available only when this Web server has accessed applications running on application servers and there is an http_plugin.log file.)

Plug-in log file name specifies the fully qualified path to the log file to which the plug-in will write error messages. The default file path is:

```
plugin_install_root/logs/web_server_name/http_plugin.log
```

If the file does not exist, it will be created. If the file already exists, it will be opened in append mode and the previous plug-in log messages will remain. This field corresponds to the RequestMetrics **loggingEnabled** element in the **plugin-cfg.xml** file.

Configure Logging

For complete information about WebSphere logging, see the IBM WebSphere Application Server Information Center for your version of WebSphere. Information in this section has been derived from the Administration section.

Be aware that performance degradation can occur when the WebSphere Application Server logging level is enabled at a level higher than INFO (for example, FINE, FINER, or FINEST).

Use the WebSphere Application Server Administrative console to set up and configure WebSphere logging and tracing. You can use the following URL to access the Administrative console:

```
http://server-name:admin-console-port-number/ibm/console
```

where `server-name` is the name of the CM Server computer and `admin-console-port-number` is the Administrative console port number (12060 by default with CM Server, or 9060 for other WebSphere Application Server versions).

To configure WebSphere Application Server logging and tracing:

1. From the Administration console, click **Troubleshooting -> Logging and Tracing** and select the server to configure.

2 Select **Change Log Detail Level** and click the **Runtime** tab. Changes made to the **Runtime** tab take effect as soon as you save them. Changes made to the **Configuration** tab do not take effect until you restart the server.

   a Select the **Save runtime changes to configuration as well** check box if you want the changes to persist.

   b Click the **Components** link. Note that ***=info** is listed in the box.

   c Open the option **com.ibm.rational.*** and select **com.ibm.rational.stp.*** for all CM Server packages. Or, select one of the packages listed under **com.ibm.rational.stp.*** to change the logging level for only that package.

   d Click the **Message and Trace Levels** option to select the level.

   e Click **OK**. Then click **Save** in the **Messages** area at the top of the page that opens. Changes take effect without restarting the server.

3 If the version or class of Websphere Application Server on your CM Server system does not provide a **Runtime** tab that enables real-time configuration changes, use the **Configuration** tab. Then restart the server to affect the saved changes.

4 Increasing the default settings for the log file size and the number of log files to rotate may be necessary. Set the number of log files to rotate through to at least 20, and set the log file size to at least 20 MB. Use the WebSphere Administrative console to change the JVM log file size and file rotation settings:

   a Select **Troubleshooting -> Logging and Tracing**.

   b Select the relevant server from the list of servers to configure.

   c Select **JVM Logs**. Then click the **Configuration** tab. (You can use the **Runtime** tab to view the current `SystemOut.log` and `SystemErr.log` file contents.)

   d Modify the `SystemOut` and `SystemErr` locations, file sizes (should be at least 20 MB), and how many historical files to maintain (should be at least 20 MB).

   e Click **OK**. Then click **Save** in the **Messages** area at the top of the page that opens.

WebSphere Application Server log files are written to the following locations:

```
UNIX: /opt/rational/common/CM/profiles/cmprofile/logs/server1/

Windows: \Program
Files\IBM\RationalSDLC\common\CM\profiles\cmprofile\logs\server1\
```

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.

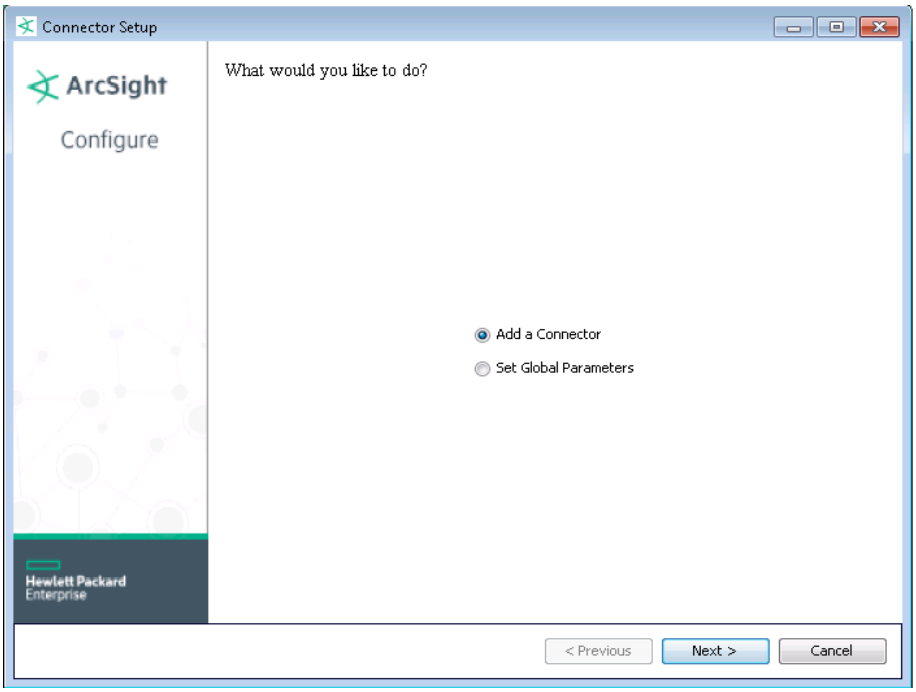
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
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	When 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. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

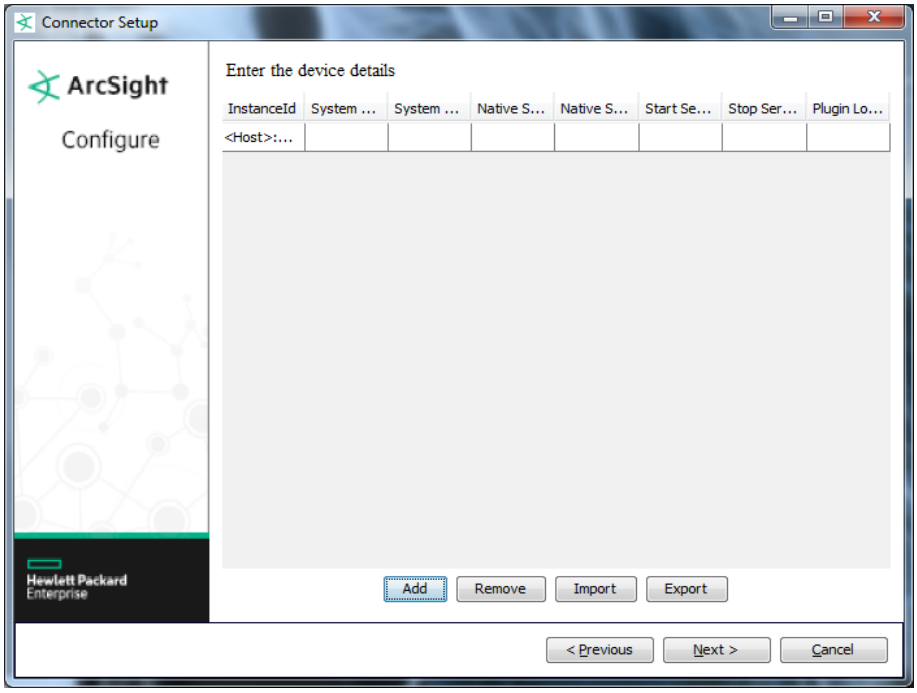
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.

Parameter	Setting
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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 **IBM WebSphere File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Instance ID	Custom Host Name and Instance ID; the default value is 'localhost'.

Parameter	Description
System Out Log File Path	Absolute path to the system.out Java Virtual Machine (JVM) log file.
System Err Log File Path	Absolute path to the system.err Java Virtual Machine (JVM) log file.
Native StdOut Log File Path	Absolute path to the native.stdout Process log file.
Native StdErr Log File Path	Absolute path to the native.stderr Process log file.
Start Server Log File Path	Absolute path to the Start Server log file.
Stop Server Log File Path	Absolute path to the Stop Server log file.
Plugin Log File Path	Absolute path to the Plugin log file.

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.

WebSphere Native StdErr Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Fatal; Medium = Error, Warning, Configuration; Low = Audit, Information, Detail, Written to System.out by Application, Written to System.Err by Application
Device Event Category	message
Device External ID	_CUSTOM_HOST_NAME
Device Host Name	_CUSTOM_HOST_NAME
Device Product	'WebSphere'
Device Receipt Time	Timestamp
Device Severity	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized)
Device Vendor	'IBM'
Name	One of (message, environment)

WebSphere Native Stdout Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Fatal; Medium = Error, Warning, Configuration; Low = Audit, Information, Detail, Written to System.out by Application, Written to System.Err by Application
Device Event Category	message
Device External ID	_CUSTOM_HOST_NAME
Device Host Name	_CUSTOM_HOST_NAME
Device Product	'WebSphere'
Device Receipt Time	Timestamp

ArcSight ESM Field	Device-Specific Field
Device Severity	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized)
Device Vendor	'IBM'
Name	message

WebSphere System.out Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Fatal, Medium = Error, Warning, Configuration; Low = Audit, Information, Detail, Written to System.out by Application, Written to System.Err by Application, Fine, Finer, Finest, Trace
Destination Process Name	threadID
Device Custom String 3	className
Device Event Class ID	component
Device External ID	_CUSTOM_HOST_NAME
Device Host Name	_CUSTOM_HOST_NAME
Device Product	'WebSphere'
Device Receipt Time	Timestamp
Device Severity	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized, 1\ = Fine, 2\ = Finer, 3\ = Finest, <\ = Trace, >\ = Trace)
Device Vendor	'IBM'
File Name	fileName
File Path	filePath
Message	One of (message, environment)
Name	One of (message, envName)

WebSphere System.err Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Fatal, Medium = Error, Warning, Configuration; Low = Audit, Information, Detail, Written to System.out by Application, Written to System.Err by Application
Destination Process Name	threadID
Device Custom String 2	shortName
Device Custom String 3	Class Name
Device Custom String 4	One of(Thread, More)
Device Custom String 5	Thread Name
Device Custom String 6	Line | 'failed to load webapp'
Device Event Class ID	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized)
Device External ID	_CUSTOM_HOST_NAME
Device Host Name	_CUSTOM_HOST_NAME
Device Product	'WebSphere'
Device Receipt Time	Timestamp

ArcSight ESM Field	Device-Specific Field
Device Severity	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized)
Device Vendor	'IBM'
Message	One of (message, environment)
Name	eventType (F\ = Fatal, E\ = Error, W\ = Warning, A\ = Audit, I\ = Information, C\ = Configuration, D\ = Detail, O\ = Written to System.out by Application, R\ = Written to System.Err by Application, Z\ = Unrecognized)

WebSphere Plugin Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium = ERROR; Low = PLUGIN, TRACE, DETAIL, DEBUG, STATS
Destination Process Name	threadID
Device Custom String 1	code
Device Event Category	messageType
Device Event Class ID	message
Device External ID	_CUSTOM_HOST_NAME
Device Host Name	_CUSTOM_HOST_NAME
Device Product	'WebSphere Plugin'
Device Receipt Time	date
Device Severity	messageType
Device Vendor	'IBM'
Message	message
Name	message