Micro Focus Security ArcSight Connectors

SmartConnector for IBM BigFix REST API

Configuration Guide

July 24, 2019

Configuration Guide

SmartConnector for IBM BigFix REST API

July 24, 2019

Legal Notices

Trademark Notices

Revision History

Date	Description
07/24/2019	First edition of the guide.

SmartConnector for IBM BigFix REST API

This guide provides information for installing the SmartConnector for IBM BigFix REST API and configuring the connector for event collection. IBM BigFix version 9.5.4 is supported with this connector.

Product Overview

IBM BigFix REST API is a system-management software product developed by IBM for managing large groups of machines running in Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as in various mobile operating systems such as Windows Phone, Symbian, iOS and Android.

IBM BigFix REST API provides system administrators with remote control, patch management, software distribution, operating system deployment, network access protection and hardware and a software inventory functionality.

Install the SmartConnector

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

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 Micro Focus SSO and Protect 724 sites.

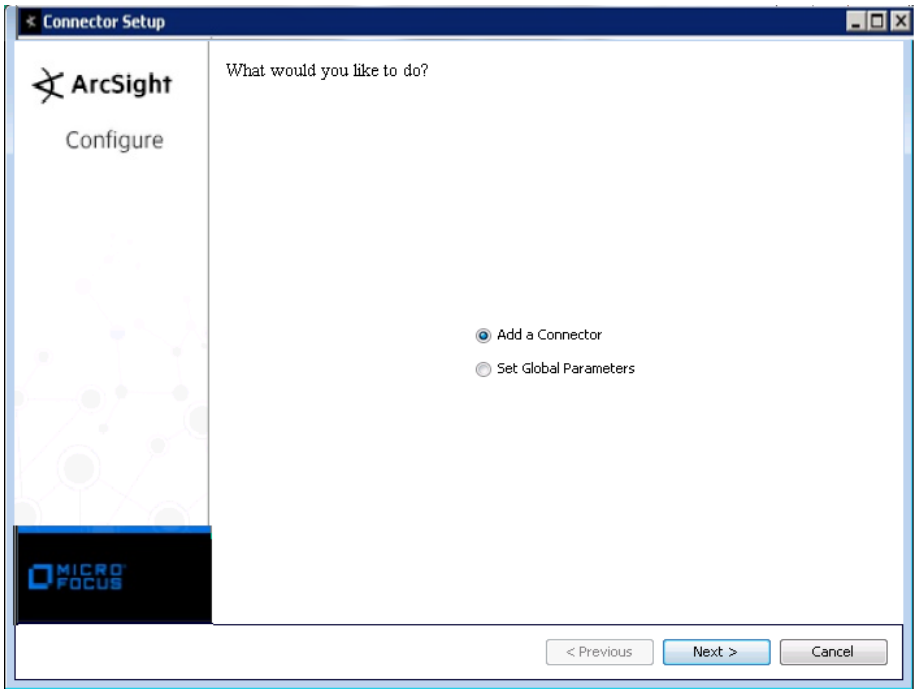
1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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:



IBM BigFix REST API collects and reads events from the management servers in your network. Access privileges are required to connect and query data from the server. Ensure the following conditions are met:

1. The WebReports service must be running. If you installed multiple Web Reports servers (locally or remotely), the Web Reports server, previously selected to use the REST API connector, will be first entry displayed in the table dbo.AGGREGATEDBY contained in the database BFEnterprise.

2.The user logging in to the REST API must be defined as a BigFix Console operator with the **Can use REST API** and the **Custom Content** permissions set to YES in its definition or in one of the assigned roles.

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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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.
Format Preserving Identity	The Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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.

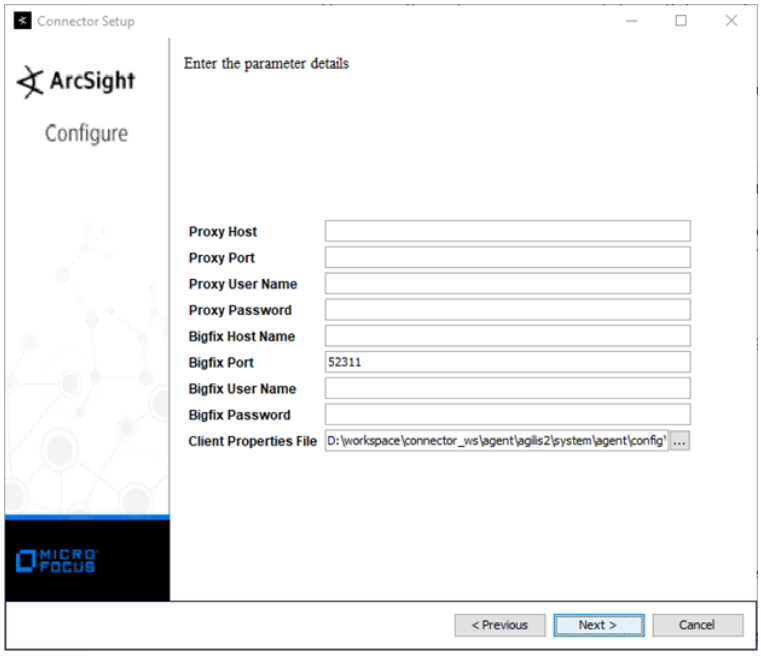
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 BigFix REST API** and click **Next**.

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



Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is required for proxy configuration in order to access the BigFix Server.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password for the proxy user specified in the Proxy User Name field. This value is optional for additional proxy authentication. This field is required only if you have specified a proxy user name.
BigFix Host Name	Enter BigFix server's host name or IP address.
BigFix Port	Enter BigFix server's port (Default: 52311).
BigFix User Name	Enter the User name of a valid BigFix Console operator.
BigFix Password	Enter Password of the user name specified in the BigFix User Name field.
Client Properties File	Location of properties file that stores the query statement to get events from the BigFix server.(Default: ARCSIGHT_HOME/system/agent/config/bigfix_api/relevancequeryfile.properties).

If you do not need a proxy to access the Internet, leave the proxy fields blank and click **Next**.

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.

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
deviceCustomDate1	__safeToDate(source-release-date,"EEE, dd MMM yyyy")
deviceCustomDate1Label	__stringConstant(Source Release Date)
deviceCustomIPv6Address2	__stringToIPv6Address(__regexToken(ipv6-addresses,"([^\\,]+)"))
deviceCustomIPv6Address2Label	__stringConstant("Source IPv6 Address")
deviceCustomString1	__concatenate("ID: ",computer-id,", Name: ",computer-name,", OS: ",operating-system,", Computer Type: ",computer-type,", Device Type: ",device-type,", CPU: ",cpu,", RAM: ",ram,", Free Space on System Drive: ",free-space-on-system-drive,", Total Size of System Drive: ",total-size-of-system-drive,", BIOS: ",bios)
deviceCustomString1Label	__stringConstant("Computer's Information")
deviceCustomString2	cve-id-list
deviceCustomString2Label	__stringConstant("CVE")
deviceCustomString3	sans-id-list
deviceCustomString3Label	__stringConstant("SANS")
deviceCustomString5	__concatenate("Agent Type: ",agent-type,", Agent Version: ",agent-version,", License Type: ",license-type)
deviceCustomString5Label	__stringConstant("Agent Information")
deviceEventCategory	category
deviceEventClassId	name-of-site
deviceReceiptTime	__safeToDate(last-report-time,"EEE, dd MMM yyyy HH:mm:ss Z")
deviceSeverity	__ifThenElse(source-severity,"","low",source-severity)
endTime	_safeToDate(last-became-relevant,"EEE, dd MMM yyyy HH:mm:ss Z")
fileCreateTime	__safeToDate(creation-time,"EEE, dd MMM yyyy HH:mm:ss Z")
fileHash	__concatenate("Device Type: ",device-type)
fileId	source-id
fileModificationTime	__safeToDate(modification-time,"EEE, dd MMM yyyy HH:mm:ss Z")
fileName	digest-file-name
filePath	source
filePermission	__concatenate("Client Administrators: ",client-administrators)
fileSize	__safeToLong(download-size)
fileType	__ifThenElse(locked-flag,"",__ifThenElse(lock-expiration,"",,__concatenate("Lock Expiration: ",lock-expiration)),__concatenate("Locked: ",locked-flag,__ifThenElse(lock-expiration,"",,__concatenate(", Lock Expiration: ",lock-expiration))))
message	fixlet-name
name	name-of-site

ArcSight ESM Field	Device-Specific Field
oldFileHash	__concatenate("Source Address: ",ip-addresseses)
oldFileId	fixlet-id
oldFileName	__concatenate("Subnet Address: ",subnet-address)
oldFilePath	__concatenate("Source IPv6 Address: ",ipv6-addresses)
oldFilePermission	__concatenate("Applicable Computer Count: ",applicable-computer-count,", Open Action Count: ",open-action-count,", Unlocked Computer Count: ",unlocked-computer-count)
oldFileType	__concatenate("Custom Fixlet: ",custom-flag,", From custom site: ",custom-site-flag,", Visible: ",visible-flag,", Globally Visible: ",globally-visible-flag)
requestClientApplication	__concatenate("Relay Selection Method: ",relay-selection-method,", Relay Service Installed: ",relay-service-installed,", Distance to Relay: ",relay-distance,", Relay: ",relay,", Relay Name of Client: ",relay-hostname)
requestCookies	__concatenate("Active Directory Path: ",active-directory-path)
sourceAddress	__oneOfAddress(__regexToken(ip-addresseses,"(\\d+.\\d+.\\d+.\\d+)"))
sourceHostName	hostname
sourceUserName	user-name