



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for IBM BigFix REST API SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

- Configuration Guide for IBM BigFix REST API SmartConnector 4
- Product Overview 5
- Installing the SmartConnector 6
 - Preparing to Install Connector 6
 - Installing and Configuring the SmartConnector 6
- Device Event Mapping to ArcSight Fields 9
 - Device Event Mapping to ArcSight Fields 9
- Send Documentation Feedback 11

Configuration Guide for IBM BigFix REST API SmartConnector

This guide provides information for installing the SmartConnector for IBM BigFix REST API and configuring the connector for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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.

Installing the SmartConnector

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

Preparing to Install Connector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, ensure that you have the following:

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

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.

3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **IBM BigFix REST API** as the type of connector, then click **Next**.
5. Specify values for the following parameters , then click **Next**:

ot Connector Setup

opentext
ArcSight

Configure

Enter the parameter details

Proxy Host

Proxy Port

Proxy User Name

Proxy Password

Bigfix Host Name

Bigfix Port 52311

Bigfix User Name

Bigfix Password

Client Properties File C:\Users\skadganche\Desktop\ume\current\system\agent\config\bigfix_ar ...

< Previous Next > Cancel

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.

Parameter	Description
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**.

1. Select a [destination and configure parameters](#).
2. Specify a name for the connector.
3. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

4. Select whether you want to install the connector as a service or in the standalone mode.
5. Complete the installation.
6. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

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")

ArcSight ESM Field	Device-Specific Field
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
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

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on Configuration Guide for IBM BigFix REST API SmartConnector
(SmartConnectors 8.4.3)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!