# MICRO FOCUS®

# Micro Focus Security ArcSight Connectors

## SmartConnector for IBM System Log for z/OS File

## Configuration Guide

**June, 2018**

Configuration Guide

SmartConnector for IBM System Log for z/OS File

June, 2018

Copyright © 2005 – 2017; 2018 Micro Focus and its affiliates and licensors.

## Revision History

| Date | Description |
| --- | --- |
| 10/17/2017 | Added encryption parameters to Global Parameters. |
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 02/14/2014 | Updated parameter screen image. |
| 05/15/2012 | Added new installation procedure. |
| 09/24/2010 | Clarified event type supported. |
| 02/11/2010 | Added support for FIPS Suite B and CEF File transport. |
| 06/30/2009 | Global update to installation procedure for FIPS support. |
| 02/11/2009 | Updated configuration information under "Exporting Log Files." |

## SmartConnector for IBM System Log for z/OS File

This guide provides information for installing the SmartConnector for IBM System Log for z/OS File and configuring the device for system log security event collection.

## Product Overview

IBM's z/OS is a secure, scalable, high-performance enterprise operating system on which to build and deploy Internet and Java-enabled applications, providing a comprehensive and diverse application execution environment.

The SmartConnector for IBM System Log for z/OS File can parse the information contained in system exported files transferred from the OS/390 system to the host running the SmartConnector. Typically, administrators create a script that exports and transfers the log file periodically to the host running the SmartConnector. The SmartConnector will monitor a configurable folder for new files transferred; once a new file is detected, the SmartConnector will process it (and rename it after it has been processed completely).

## Configuration

### Exported Log Files

The SmartConnector for SmartConnector for IBM System Log for z/OS File can parse the information contained in exported files transferred from the OS/390 system to the host running the SmartConnector. Typically, OS/390 administrators will create a script to export and transfer the log file periodically to the host running the SmartConnector. The SmartConnector will monitor a configurable folder for new files transferred; once a new file is detected, the connector processes it (and renames it after it has been processed completely). If there are any problems with the file (for example, if the file was not in the correct format), the connector will move the file to the subfolder **Bad** so the problem can be investigated further.

### Creating Export Files

The export files must be sent in a specific format, as shown in the following example.

```
M 0080000 S26A      04282 07:46:28.50 AAA40027 00000091
ICH408I USER(ABC0324 ) GROUP(AAAAAAAC) NAME(AAAAS, BBBBBBBS
) 754

E                                    754 00000091
LOGON/JOB INITIATION – INVALID PASSWORD ENTERED AT TERMINAL
CCCCCCC

N 0000000 S26A      04282 07:46:34.67 TTT10324 00000091
IEF126I ZZZZZZZ – LOGGED OFF – TIME=07.46.34
```

## Differing Primary Languages

Be aware of the following when using FTP in an environment with different primary languages.

When data is transferred using EBCDIC, the data is stored as is and therefore will be in the EBCDIC code page of the file from which it came. This can result in the stored file being tagged with an inappropriate CCSID value when the primary language of the two servers is different.

For example, when data in code page 237 is sent using TYPE E to the QSYS.LIB file system on a machine where the file does not exist, the data is stored as is in a new file tagged with CCSID 65535. If the receiving file already exists, then the data will be received as is and tagged with the existing file CCSID which may not be 237.

To avoid incorrect CCSID tagging, you can use the TYPE C CCSID subcommand (for example, TYPE C 237) to specify the CCSID of the data being transferred. When a CCSID is specified on a transfer and the data is written to an existing file, the data is converted to the CCSID of the existing file. If no target file exists before the transfer, a file is created and tagged with the specified CCSID.

In the preceding example, if the target file does not exist, a file with a CCSID of 237 is created on the receiving system. When the target file already exists, the data is converted from CCSID 237 to the CCSID of the target file.

When starting the FTP client, message TCP3C14: Unable to convert data from CCSID &1 to CCSID &2, may be displayed. This occurs if no character conversion is available between the EBCDIC CCSID specified by your job and the ASCII CCSID specified for the this FTP session.

You can change the ASCII CCSID by specifying a value for the coded character set identifier parameter of the STRTCPFTP CL command. CCSID 850, which contains the IBM Personal Computer Latin-1 coded character set, is an ASCII CCSID for which character conversions are available to all valid job CCSID values.

## Specify Mapping Tables in the FTP Command

For FTP client, the ASCII mapping tables are specified in the FTP command. For FTP server this is done in the Change FTP Attributes (CHGFTPA) command. To specify the FTP client mapping tables:

1 Enter the command FTP.

2 Press PF4. The **Start TCP/IP FTP** screen is displayed.

3 Press F10. The prompts for outgoing and incoming ASCII/EBCDIC tables are displayed.

```
|                                                                              |
|                   Start TCP/IP File Transfer (FTP)                           |
|                                                                              |
| Type choices, press Enter.                                                   |
|                                                                              |
| Remote system  . . . . . . . . .                                             |
|                                                                              |
|                                                                              |
|                                                                              |
| Internet address . . . . . . . .                                             |
| Coded character set identifier     *DFT          1-65533, *DFT               |
|                                                                              |
|                         Additional Parameters                                |
|                                                                              |
| Outgoing EBCDIC/ASCII table  . .   *CCSID        Name, *CCSID, *DFT          |
|   Library . . . . . . . . . . .                  Name, *LIBL, *CURLIB        |
| Incoming ASCII/EBCDIC table  . .   *CCSID        Name, *CCSID, *DFT          |
|   Library . . . . . . . . . . .                  Name, *LIBL, *CURLIB        |
|                                                                              |
|                                                                              |
|                                                                     Bottom   |
|  F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display |
|  F24=More keys                                                               |
|                                                                              |
|                                                                              |
|_____|
```

Specify the CCSID (and hence the mapping tables) to be used for the FTP client. When the *DFT value is not changed, the CCSID value 00819 (ISO 8859-1 8 bit ASCII) is used. You may also specify a specific CCSID for both inbound and outbound transfers. The use of CCSIDs is discussed in National Language Support considerations for FTP.

> ✎  Double-byte character set (DBCS) CCSID values are not permitted for the CCSID parameter on the CHGFTPA command. The DBCS CCSID values can be specified using the TYPE (Specify File Transfer Type) subcommand.
>
> IBM includes mapping support in FTP to ensure compatibility with releases prior to V3R1. Use of mapping tables for incoming TYPE A file transfers results in the loss of CCSID tagging if the target file must be created. IBM strongly recommends that you use CCSID support for normal operations.

## 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 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:
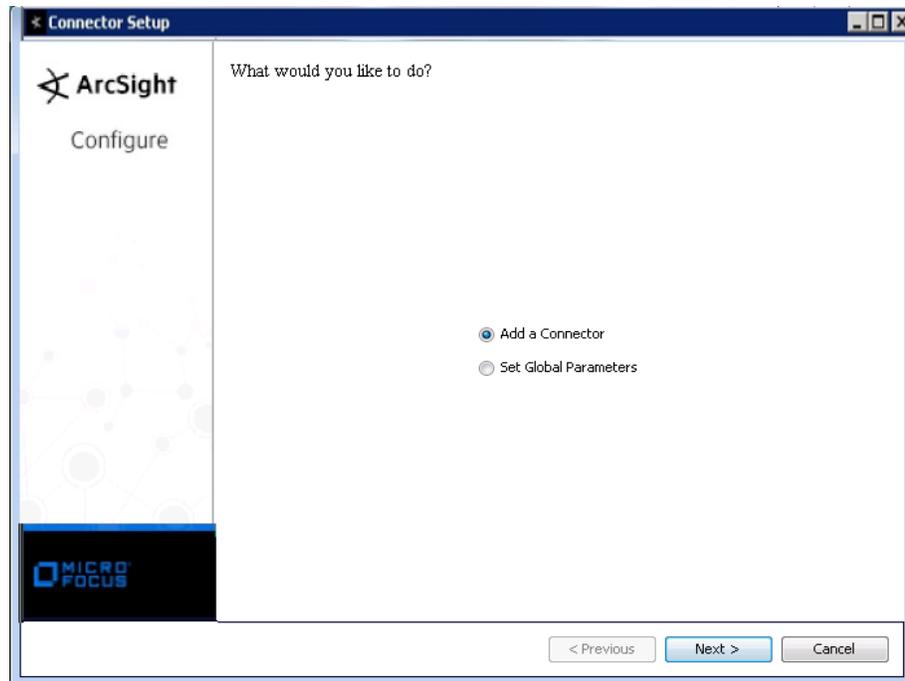
## Set Global Parameters (optional)

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. |

| Parameter | Setting |
|---|---|
| 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 System Log for z/OS File** and click **Next**.

3  Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.
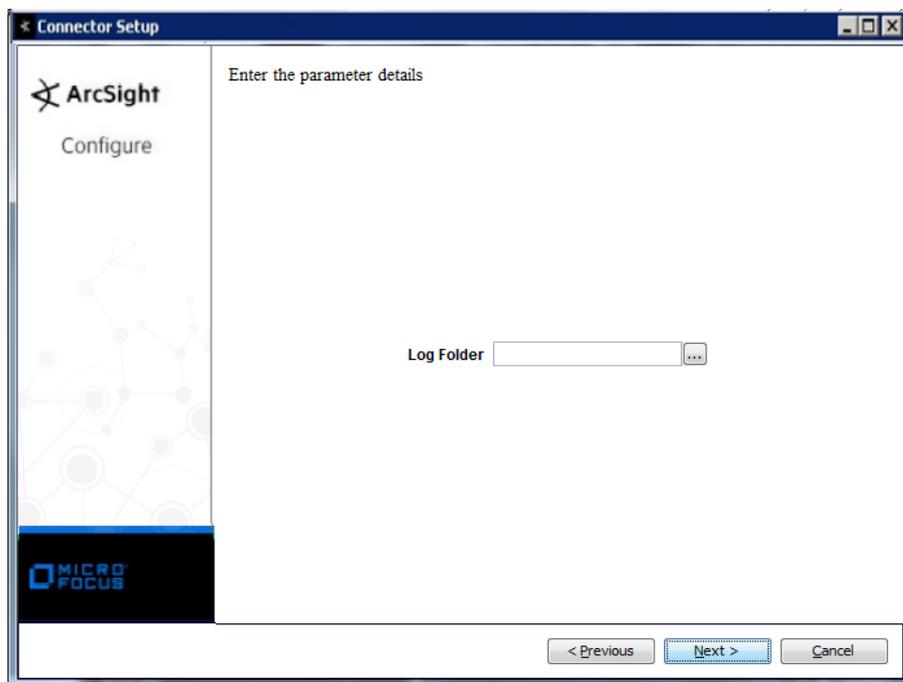
| Parameter | Description |
|-----------|-------------|
| Log Folder | Absolute path to the folder containing the log files. |

## 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.

### IBM System Log for z/OS Event Mappings to ArcSight ESM Fields

| ArcSight ESM Field | Device-Specific Field |
| --- | --- |
| Destination Process Name | OS390 process name |
| Destination User Id | OS390 userid |
| Device Custom Number 1 | Event type number |
| Device Custom Number 2 | Event sequence number |
| Device Custom Number 3 | Event sequence number |
| Device Custom String 1 | Event type code |
| Device Custom String 4 | Event sequence number |
| Device Custom String 5 | Event type id |
| Device Event Category | Record Type |
| Device Event Class ID | OS390 Message ID |
| Device Host Name | OS390 originating host |
| Device Process Name | OS390 destination process name |
| Device Product | OS390_syslog |
| Device Receipt Time | Event time |
| Device Vendor | IBM |
| External ID | OS390 event ID |
| File Name | OS390 cmd |
| Message | OS390 message |

| ArcSight ESM Field | Device-Specific Field |
| --- | --- |
| Name | Event name or event type ID |
| Source Process Name | OS390 originator process name |
| Source Service Name | OS390 service |
| Source User Name | OS390 username |