Micro Focus Security ArcSight Connectors

SmartConnector for IBM RACF for z/OS File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for IBM RACF for z/OS File

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

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.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
08/12/2009	Updated field mappings. JOB_NAME is now mapped to Destination Process Name rather than Device Process Name.
06/30/2009	Global update to installation procedure for FIPS support.
03/27/2009	Updated field mappings.
09/25/2008	Update to connector name.
03/01/2008	Update to installation procedure.
09/30/2006	First edition of this Configuration Guide.

SmartConnector for IBM RACF for z/OS File

This guide provides information for installing the SmartConnector for IBM RACF for z/OS File and configuring the device for event collection. IBM RACF for z/OS and OS/390 are supported.

Product Overview

Working closely with your operating system's existing features, IBM's Resource Access Control Facility (RACF) licensed program provides improved security for an installation's data. RACF protects vital system resources and controls what users can do on the operating system. As a key component of the z/OS Security Server, RACF supports both OS/390 and z/OS.

Configuration

Configuration Overview

To help you to audit access control and accountability, RACF provides:

- Logging routines that record the information you require
- Audit control functions that let you specify the information RACF is to log

To specify the audit control functions, use either the RACF ISPF panels or the RACF commands to direct RACF to log any events relevant to your installation's data security.

For more information about logging and auditing, see IBM's *z/OS Security Server RACF Auditor's Guide*. For information about how to specify logging and auditing functions, see IBM's *z/OS Security Server RACF Command Language Reference*.

Activating Auditing for Security Levels

If you have the AUDITOR attribute, you can activate auditing of access attempts to all RACF-protected resources. To activate this option, specify the SECLEVELAUDIT operand with an installation-defined security level name on the SETROPTS command. Auditing is done if the profile protecting a resource is equal to or greater than the security level you specify on the SECLEVELAUDIT operand.

The following example shows how to activate auditing based on the security level CONFIDENTIAL. (This example assumes that the installation has defined the level CONFIDENTIAL in the SECLEVEL profile.)

```
SETROPTS  SECLEVELAUDIT(CONFIDENTIAL)
```

When you specify a security level, RACF audits all attempts to access resources with the specified security level and higher. If you do not specify a security level, RACF audits all access attempts to all resources for which your installation has defined a security level (SECLEVEL).

Logging RACF Audit Messages

RACF writes SMF type 80 log records to SMF. Which events are logged depends upon the auditing in effect. For example, events requested by the AUDIT or GLOBALAUDIT operand in the resource profile, or by the SETROPTS AUDIT or SETROPTS LOGOPTIONS command, can be logged.

When issuing the SETROPTS command as a RACF operator command, you might require sufficient authority to the proper resource in the OPERCMDS class. See "z/OS Security Server RACF Security Administrator's Guide" for further information.

For more information about logging and auditing, see IBM's *z/OS Security Server RACF Auditor's Guide*. For information about how to specify logging and auditing functions, see IBM's *z/OS Security Server RACF Command Language Reference*.

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.

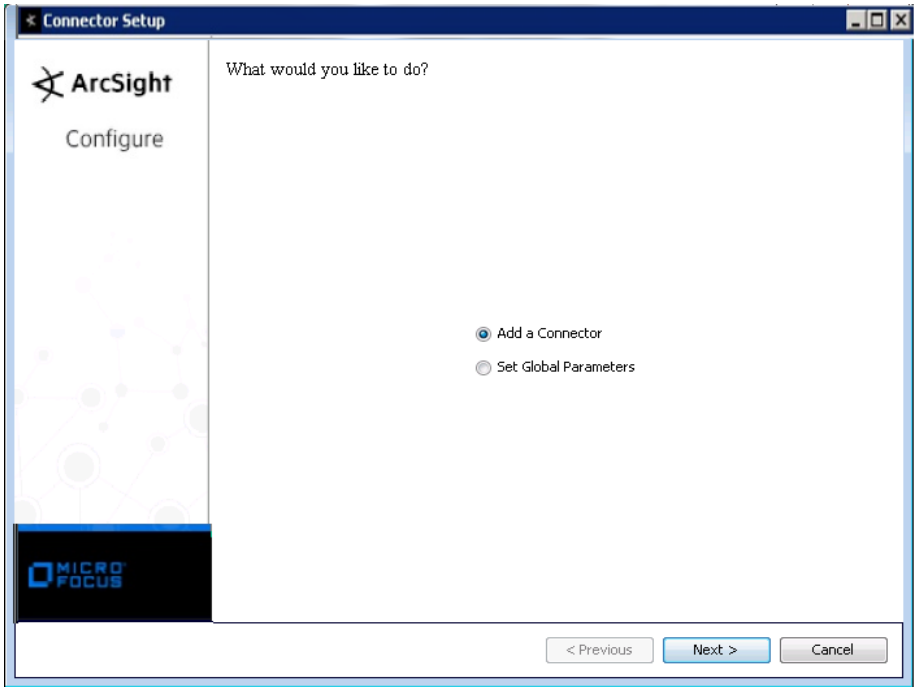
1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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.

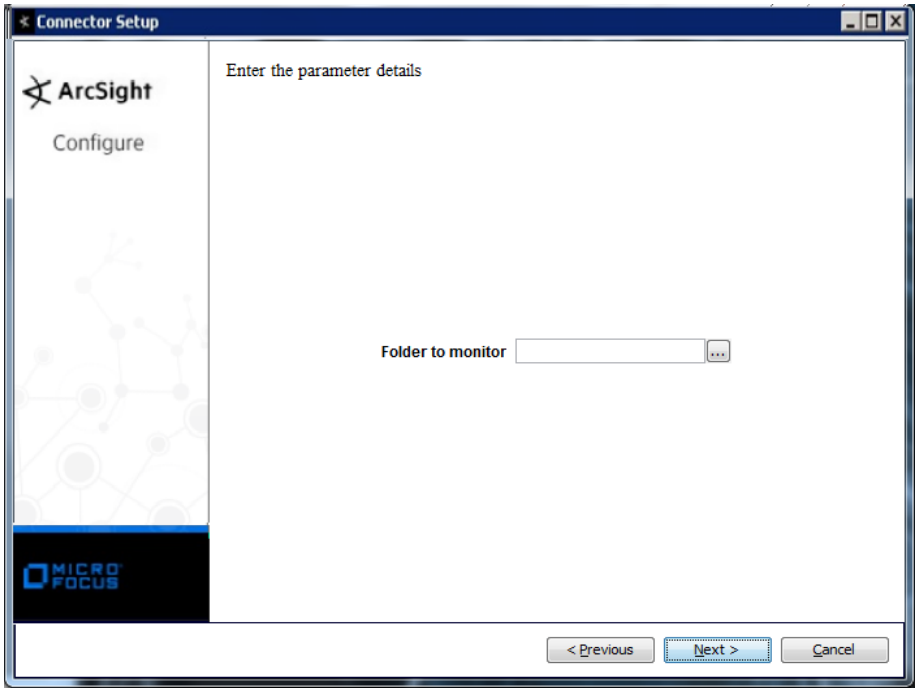
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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.
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 RACF for z/OS File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder to monitor	Enter the name of and path to the folder in which RACF files will be stored.

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 RACF for z/OS Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Process Name	JOB_NAME
Destination User ID	Destination user
Device Action	EVENT_QUAL
Device Custom String 1	VIOLATION
Device Custom String 2	USER_WARNING
Device Custom String 3	Auth_Special
Device Custom String 4	AUTH_AUDIT
Device Custom String 5	TERM (Terminal_ID)
Device Custom String 6	EVT_GRP_ID
Device Event Category	category
Device Event Class ID	EVENT_TYPE
Device Facility	Device facility
Device Host Name	SYSTEM_SMFID
Device Inbound Interface	Device inbound interface
Device Procuct	'RACF'
Device Receipt Time	DATE_TIME_WRITTEN
Device Vendor	'IBM'
Device Version	RACF_VERSION
File Name	File name
File Path	File path
File Permission	AUTH_OPER
File Type	File type
Flex String 1	'Resource_Name'
Flex String 2	'LOGSTR'
Name	EVENT_TYPE
Old File Name	Old file name
Request Context	Request context
Request Method	Request method
Source User ID	EVT_USER_ID
Source User Name	Source user name
Start Time	READ_TIME_DATE

Additional Information

The IBM SMFDUMP Program

The IBM SMFDUMP program is used to produce the IRRADU00 file the ArcSight SmartConnector reads. IRRADU00 is a sequential file that is cut from the SMF and then transmitted via FTP to the SmartConnector.

```
//*************************************************************
***********
 //*
*
 //* PROPRIETARY STATEMENT:
*
 //*    LICENSED MATERIALS - PROPERTY OF IBM
*
 //*    "RESTRICTED MATERIALS OF IBM"
*
 //*    5647-A01
*
 //*    (C) COPYRIGHT IBM CORP. 1996, 1997
*
 //*
*
 //* DESCRIPTIVE_NAME:
*
 //*
*
 //*    The SMF dump program (IFASMFDP) transfers the
contents of the *
 //*    full SMF data set to another data set, and resets
the         *
 //*    status of the dumped data set to empty so that SMF
can use it *
 //*    again for recording data.
*
 //*
*
 //* CHANGE ACTIVITY:
*
 //*
*
 //*    JF-02Mar04             Added process for daily CICS
processing*
 //*
*
 //*    JF-27Sep02             Changed Manin par to use
whole d/s     *
 //*                           name supplied by AO.
*
 //*
*
 //*    $C0=R430,HRM4430,,HBE: CREATED
*
```

```
 //*    $F1=R604,HRM6604,,GBO: ADDED COPYRIGHT
*
 //*    LG-12JUN02           : Adjustments for split of
RACF related  *
 //*                           security events by exits
IRRADU00/86   *
 //*                           for purposes of management
reporting   *
 //*                           on a daily basis.
*
 //*                           Note: Use of //OUTDD is
hardcoded un-  *
 //*                                 fortunately to
facilitate use of *
 //*                                 the IRRADU00/86 RACF
SMF exits   *
 //*                                 for purposes of
collecting the   *
 //*                                 security server
related events.  *
 //*                           NOTE: The following control
stmts      *
 //*                                 will invoke the smf
user exit    *
 //*                                 which allows
collection of RACF  *
 //*                                 event records:
*
 //*
INDD(INDD1,OPTIONS(ALL))    *
 //*
OUTDD(OUTDD1,TYPE(000:255)) *
 //*                                      ABEND(NORETRY)
*
 //*                                      USER2(IRRADU00)
*
 //*                                      USER3(IRRADU86)
*
 //*
*

//*************************************************************
***********
 //SMFDUMP PROC MANIN=DUMMY
 //S01     EXEC PGM=IFASMFDP,REGION=0M
 //INDD1    DD  DISP=SHR,DSN=&MANIN
```

```
//*
//OUTDD    DD  DISP=(MOD),
//             DSN=SYS3.RACF.SYSP.ADUDALY(+0),
//             DCB=(PC.GDG,RECFM=VB,LRECL=8192,DSORG=PS),
//             UNIT=(CART,,DEFER)
//*
//OUTDD1   DD  DISP=MOD,DSN=SYS3.SMFDUMPW.BACKUP(0)
//*
//OUTDD2   DD  DISP=MOD,DSN=SYS3.SMFDUMPM.SCRTDATA(0)
//*
//OUTDD3   DD  DISP=MOD,DSN=SYS3.SMFCICSD.BACKUP(0)
//*
//OUTDD4   DD  DISP=MOD,DSN=SYS3.SMF.CMF.PERFW.DATA(0)
//*
//OUTDD5   DD  DISP=MOD,DSN=SYS3.SMFCICSD.T110S2.DATA(0)
//*
//OUTDD6   DD  DISP=MOD,DSN=SYS3.SMFSLS.T255.DATA(0)
//*
//SYSPRINT DD  SYSOUT=9
//ADUPRINT DD  SYSOUT=9
//SMFOUT   DD  DUMMY
//SYSIN    DD  DISP=SHR,DSN=SYS3.SYSTEMS.CNTLLIB(SMF@SYSP)
```