
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Type80 SMA_RT Syslog SmartConnector

Document Release Date: February 2022

Software Release Date: February 2022



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2022 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

- Configuration Guide for Type80 SMA_RT Syslog SmartConnector 5
- Product Overview 6
- Configuration 7
 - Configuring the Syslog SmartConnectors 7
- Installing the SmartConnector 11
 - Preparing to Install the SmartConnector 11
 - Installing and Configuring the SmartConnector 11
- Device Event Mapping to ArcSight Fields 15
 - Type80 SMA_RT V3 Mappings 15
 - Type80 SMA_RT ACF2 Mappings 15
 - Type80 SMA_RT RACF Mappings 16
 - Type80 SMA_RT Top Secret Mappings 16
 - Type80 SMA_RT v2 Field Mappings 17
 - Additional Data Mappings 18
- Send Documentation Feedback 24

Configuration Guide for Type80 SMA_RT Syslog SmartConnector

This guide provides information for installing and configuring the SmartConnector for Type80 SMA_RT Syslog and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

Product Overview

Type80 SMA_RT for IBM z/OS Operating Systems is a program product that looks for patterns of abuse and sends real-time alerts. It supports the z/OS operating system environment across multiple processors and over geographically diverse locations. SMA_RT tracks activity, monitors systems resources, and records vital information.

Type80 Syslog for z/OS enables extension of all mainframe console messages and write-to-operator messages to be routed to external log retention servers using the standard TCP/IP Syslog protocol.

Configuration

Syslogd processing is controlled by the `/etc/syslog.conf` configuration file, in which you define logging rules and output destinations for error messages, authorization violation messages, and trace data. You can specify the name of a previously created file to be used for all log messages (for example: `/tmp/syslogd/auth.log`) or send log message events to a syslog daemon on another host (for example, `@mya1xserver`). File names are case sensitive.

For information about configuring Type80 SMA_RT for syslog event collection, see your Type80 product documentation.

Configuring the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: `local1.warning @@10.0.0.1:514`

- To read all Syslog events, use *.*.
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as messages.log rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the */etc/rsyslog.conf* file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug |/var/tmp/syspipe
```

3. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the */etc/rsyslog.conf* file
The syslog daemon is forced to reload the configuration and start writing to the pipe.
3. Restart the syslog daemon in one of the following methods:

- a. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

Installing the SmartConnector

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

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus 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, make sure that the following are available:

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

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next**, the specify the following paramenters:

Parameters	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .

- b. Click **Next**.

- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, then specify the following parameters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> .
File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none"> • Solaris: <code>\var\adm\messages</code> • Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none"> • Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code> • Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename '%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional.

Parameters	Description
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension.

- b. Click **Next**.
5. Select a destination and configure parameters.
6. Specify a name for the connector.
7. 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.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

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

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.

Type80 SMA_RT V3 Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	RED = High; YEL = Medium
Destination Host Name	LPAR
Destination Process Name	ProcessName
Device Custom Number 1	EscalationValue
Device Custom Number 2	EscalationThreshold
Device Custom Number 3	AlertCount
Device Custom String 3	AlertAction
Device Custom String 4	CPUSerialNumber
Device Product	'Type80'
Device Receipt Time	Timestamp
Device Severity	Alert Type (RED, YEL)
Device Vendor	'Type80'
Message	Message
Source Service Name	MessageType

Type80 SMA_RT ACF2 Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	DestUserId, UserId
Destination User Name	DestUserId, UserId
Device Custom String 1	RuleName, RuleType

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	Both (Function, SubType)
Name	Both (Function, SubType)
Source Process Name	UserId
Source User ID	UserId
Source User Name	UserId

Type80 SMA_RT RACF Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	UserId
Destination User Name	UserId
Device Custom String 2	DeptId
Device Custom String 5	EventQualifier
Device Custom String 6	GroupName
Device Event Class ID	Both (EventCode, EventQualifierCode)
Name	Event
Source User ID	UserId
Source User Name	UserId

Type80 SMA_RT Top Secret Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	UserID
Name	Message

Type80 SMA_RT v2 Field Mappings

ArcSight ESM Field	Device-Specific Field
ArcSight Severity - High	Device Severity = RED
ArcSight Severity - Medium	Device Severity = YEL
Bytes In	incoming bytes in transaction
Bytes Out	outgoing bytes in transaction
Destination Process Name	process
Destination User Id	destination user
Destination User Privileges	destination user privileges
Device Custom Number 1	EscalationValue
Device Custom Number 2	RunningCount
Device Custom Number 3	Count
Device Custom String 1	Return code or Error Code
Device Custom String 2	Terminal
Device Custom String 3	Rule1
Device Custom String 4	Rule2
Device Custom String 5	JobName
Device Custom String 6	Keyword, Function, or Command
Device Event Category	Type
Device Event Class ID	MessageId
Device External ID	LPAR
Device Product	'Type80'
Device Receipt Time	Timestamp
Device Severity	Severity
Device Vendor	'Type80'
Device Version	version
File Name	fileName
File Path	filePath

ArcSight ESM Field	Device-Specific Field
Message	Message
Name	Type
Source Address	source ip
Source Host Name	source host name

Additional Data Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	ACID
Additional Data	adabas
Additional Data	adminid
Additional Data	adsp
Additional Data	attributes
Additional Data	aud
Additional Data	audit_filepath
Additional Data	authority
Additional Data	autoerase
Additional Data	backup_status
Additional Data	bypass
Additional Data	cancel_code
Additional Data	chng
Additional Data	classname
Additional Data	cpf
Additional Data	cpftarget
Additional Data	cpfwait
Additional Data	currbuf
Additional Data	date
Additional Data	ddn

ArcSight ESM Field	Device-Specific Field
Additional Data	debug_code
Additional Data	defacid
Additional Data	diagtrap
Additional Data	display
Additional Data	dlib_code
Additional Data	down_code
Additional Data	dufpgm
Additional Data	exec
Additional Data	extsec
Additional Data	facility
Additional Data	facmatrx
Additional Data	facmode
Additional Data	gtrace
Additional Data	hpbpw
Additional Data	id
Additional Data	inactive
Additional Data	infomation_code
Additional Data	init
Additional Data	initpgm
Additional Data	iotrace
Additional Data	jes_indev
Additional Data	jes_level
Additional Data	jes_route
Additional Data	jes_ssid
Additional Data	jes_type
Additional Data	jobacid
Additional Data	key
Additional Data	lock

ArcSight ESM Field	Device-Specific Field
Additional Data	locktime
Additional Data	log
Additional Data	logbuf
Additional Data	lwait
Additional Data	mask
Additional Data	maxsign
Additional Data	maxuser
Additional Data	min
Additional Data	mindays
Additional Data	mode
Additional Data	mrc
Additional Data	msg
Additional Data	msuspend
Additional Data	mvs
Additional Data	newname
Additional Data	njeuser
Additional Data	npwrthersh
Additional Data	oldacid
Additional Data	oldname
Additional Data	option
Additional Data	parameter
Additional Data	pcdsdays
Additional Data	pcidle
Additional Data	pclgtype
Additional Data	pcminpwd
Additional Data	pcoptions
Additional Data	pctcmdsec
Additional Data	pctextsec

ArcSight ESM Field	Device-Specific Field
Additional Data	prft
Additional Data	product
Additional Data	pthresh
Additional Data	pwexp
Additional Data	pwhist
Additional Data	pwview
Additional Data	r15
Additional Data	read
Additional Data	reader
Additional Data	reason
Additional Data	recovery_filepath
Additional Data	recv
Additional Data	req
Additional Data	resclass
Additional Data	resname
Additional Data	resource
Additional Data	resource_name
Additional Data	sec9
Additional Data	sectrace
Additional Data	shrfile
Additional Data	sfdiag
Additional Data	smf
Additional Data	statement
Additional Data	status
Additional Data	subacid
Additional Data	swap_code
Additional Data	sysout
Additional Data	tape_code

ArcSight ESM Field	Device-Specific Field
Additional Data	tempds
Additional Data	texttss
Additional Data	time
Additional Data	timer
Additional Data	time_zone_adjustment_factor
Additional Data	tran_id
Additional Data	transaction
Additional Data	uidacid
Additional Data	value
Additional Data	vax
Additional Data	vaxcmd
Additional Data	vaxdept
Additional Data	vaxid
Additional Data	vaxpfx
Additional Data	vaxsrch
Additional Data	vaxwait
Additional Data	viol
Additional Data	vmjeslnk
Additional Data	volume
Additional Data	vthresh
Additional Data	warn
Additional Data	write
Additional Data	xappc
Additional Data	xcmd
Additional Data	xdct
Additional Data	xfct
Additional Data	xjct
Additional Data	xpct

ArcSight ESM Field	Device-Specific Field
Additional Data	xppt
Additional Data	xpsb
Additional Data	xreq
Additional Data	xtran
Additional Data	xtst

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 Type80 SMA_RT Syslog SmartConnector (SmartConnectors 8.3.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!