



Micro Focus Security ArcSight Connectors

SmartConnector for Rapid7 NeXpose XML File

Configuration Guide

August 21, 2019

Configuration Guide

SmartConnector for Rapid7 NeXpose XML File

August 21, 2019

Copyright © 2005 – 2019 Copyright 2019 Micro Focus or one of its affiliates.

Legal Notices

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.

Revision History

Date	Description
08/21/2019	Added support for version 6.5.43.
01/23/2018	Added support for version 6.4.42.

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
06/15/2017	Removed support for version 4.0 through 4.12. Added support for version 6.3.
05/15/2017	Removed Device Custom IPv6 Address 3 mapping.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2015	Added support for reading compressed report files. Added configuration information regarding trigger files.
11/14/2014	Added support for version 5.9.
03/31/2014	Added support for version 5.8.
02/14/2014	Added support for version 5.7 XML v2.
09/30/2013	Updated configuration information for version 5.5.
06/28/2013	Added support for version 5.5.

SmartConnector for Rapid7 NeXpose XML File

This guide provides information for installing the SmartConnector for Rapid7 NeXpose XML File and configuring the device for vulnerability scanner report event collection. NeXpose Scanner versions 5.5 through 6.3 (with XML 2.0), as well as version 6.4.42 and 6.5.43 (with XML 2.0) are supported.

Product Overview

NeXpose is a sophisticated enterprise vulnerability assessment, policy compliance and remediation management solution designed to eliminate false positives and provide faster and more accurate reporting across the entire enterprise network.

Configuring the Device for Event Collection

Configure your scanner to copy generated XML reports to the folder that is being monitored by the ArcSight SmartConnector as described in the *Rapid 7 NeXpose User's Guide*.

For versions 5.5 through 6.3, 6.4.42 and 6.5.43

Log into the NeXpose Security Console and select a Report format as follows:

- 1** Click the **Reports** tab.
- 2** Click **Create a report**.
- 3** Provide a name for the report and select a time zone.
- 4** Click **Export** as the template type.
- 5** If not already selected, click **XML Export or XML Export 2.0**.



"XML Export 2.0 is supported with NeXpose versions 5.7, 6.3 and 6.5.43 only."

6 Click **Save** to save the report configuration.

Modes of Operation

The SmartConnector for SmartConnector for Rapid7 NeXpose XML File supports the following modes of operation:

Interactive: In this mode, the NeXpose Security Console interface is displayed; click on **Reports** to view a list of the XML Export reports that are available for importing. Select individual reports to send to the connector, and click the **Send** button.

Automatic: This mode is designed to be used in conjunction with an automated procedure to periodically run scans with the NeXpose scanner. To use Automatic mode, create a script to schedule when NeXpose should run scans. At the end of the scan, after the report is saved, create an empty file called **{reportname}.xml_done**. This indicates to the SmartConnector that the report is ready for importing. The connector continues looking for .xml_done files and processes the reports. See "File Processing in Automatic Mode" for more information.

File Processing in Automatic Mode

When the value of `useTriggerFile` set to `true` (the default), the connector will process `[FileName].xml`, `[FileName].xml.gz`, `[FileName].xml.zip`, and

[FileName].xml_done based on the value in the `afterprocessingaction` property.

- If the `afterprocessingaction` property is set to `Move` (the default value), [FileName].xml_done will be deleted and [FileName].xml, [FileName.xml.gz], and [FileName].xml.zip will be renamed to [FileName].xml_processed, [FileName].xml_processed.gz, and [FileName].xml_processed.zip.
- If the `afterprocessingaction` property is set to `Delete`, [FileName].xml_done, [FileName].xml, [FileName].xml.gz, and [FileName].xml.zip will be deleted.

When `userTriggerFile` is set to `false`, the connector will process [FileName].xml, [FileName].xml.gz, and [FileName].xml.zip based on the value of the `afterprocessingaction` property. (If [FileName].xml_done exists in the report folder, it is ignored when `useTriggerFile` is `false`.)

- If the `afterprocessaction` property is set to `Move`, [FileName].xml, [FileName.xml.gz], and [FileName].xml.zip will be renamed to [FileName].xml_processed, [FileName].xml_processed.gz, and [FileName].xml_processed.zip.
- If the `afterprocessingaction` is set to `Delete`, [FileName].xml, [FileName].xml.gz, and [FileName].xml.zip will be deleted.

To change the value of `useTriggerFile` or `afterprocessingaction` parameters, edit the `agent.properties` file after connector installation, located at `$ARCSIGHT_HOME/current/user/agent`.

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256  
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024  
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

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

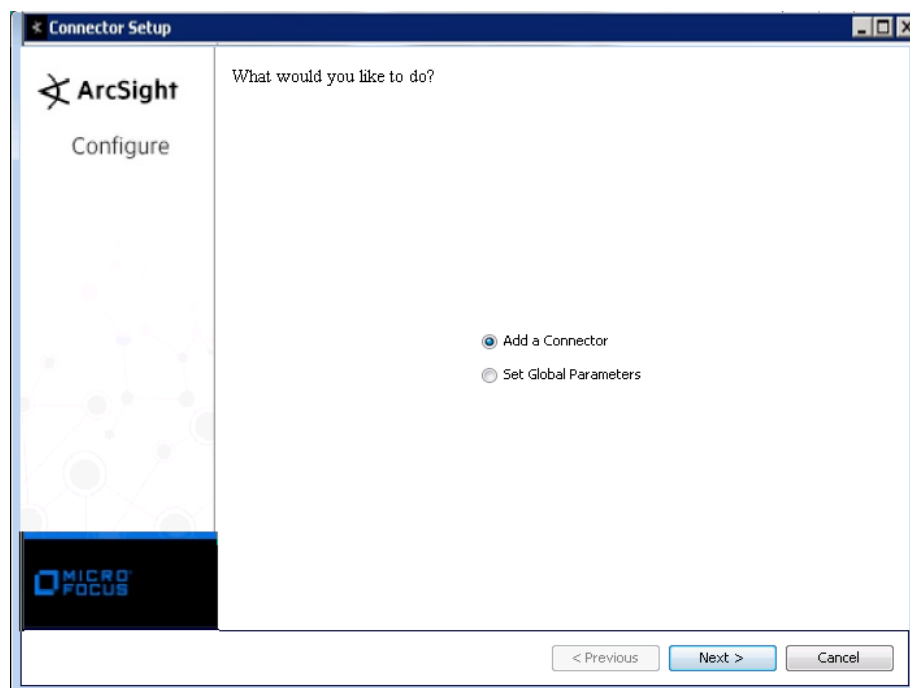
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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
-----------	---------

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.

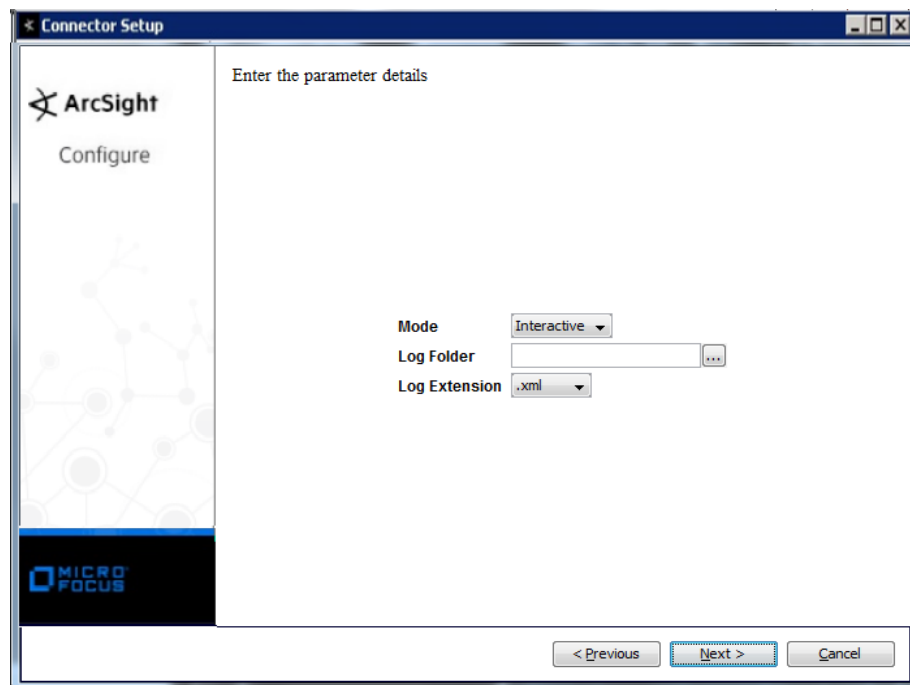
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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 **Rapid7 NeXpose XML File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Mode	Select Interactive or Automatic mode. In Interactive mode, a graphical UI is displayed showing the reports available for sending to the ArcSight Manager. In Automatic mode, the new reports are sent automatically to the ArcSight Manager.
Log Folder	Folder in which XML reports will be stored.
Log Extension	Leave the default value of .xml or select .xml.gz or .xml.zip.

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.

NeXpose Scanner Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Destination Address	address
Destination Host Name	hostname
Destination Mac Address	macaddress

NeXpose Open Ports Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	medium = Medium
Category Technique	VulnerabilityCategory
Destination Address	address
Destination Host Name	hostname
Destination Mac Address	macaddress
Destination Port	port
Destination Service Name	serviceName
Device Domain	'Network'
Device Event Class Id	Open Ports
Device Product	'NeXpose'
Device Receipt Time	startTime
Device Severity	Medium
Device Vendor	'Rapid7'
Device Version	deviceversion
End Time	endTime
Name	'Open Port'
Old File Path	_FILE_PATH
Transport Protocol	protocol

NeXpose URIs Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Veryhigh = Very High, high = High; medium = Normal; low = Low, Very Low
Category Technique	VulnerabilityCategory
Destination Address	address
Destination Host Name	hostname
Destination Mac Address	macaddress
Device Custom Floating Point 1	Risk Score
Device Domain	'Network'
Device Product	'NeXpose'
Device Receipt Time	startTime
Device Severity	siteImportance
Device Vendor	'Rapid7'
Device Version	deviceversion
End Time	endTime

ArcSight ESM Field	Device-Specific Field
External ID	deviceId
File Path	One of (product, both (product,version))
Name	'Operating System'
Old File Path	_FILE_PATH

NeXpose Vulnerabilities Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 9, 10; High = 7, 8; Medium = 4 - 6; Low = 1 - 3
Category Technique	VulnerabilityCategory
Destination Address	address
Destination Host Name	hostname
Destination Mac Address	macaddress
Device Custom Date 1	Vulnerable Since
Device Custom Floating Point 1	Risk Score
Device Custom String 1	Malware Kit Name
Device Custom String 2	CVE
Device Custom String 3	Descriptive
Device Custom String 4	Mitigation
Device Custom String 5	PCI Compliance Status
Device Custom String 6	CVSS Score
Device Domain	'Network'
Device Event Class Id	id, #, title, severity, description, solution, references
Device Product	'NeXpose'
Device Receipt Time	startTime
Device Severity	severity
Device Vendor	'Rapid7'
Device Version	deviceversion
End Time	endTime
External ID	exploitId
Message	proof
Name	title
Old File Path	_FILE_PATH
Request URL	exploitLink