



Micro Focus Security ArcSight Connectors

SmartConnector for IDMEF XML File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for IDMEF XML File

June, 2018

Copyright © 2003 – 2017; 2018 Micro Focus and its affiliates and licensors.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2016	Added mapping for Device Event Class ID.
05/15/2012	Added new installation procedure.
09/24/2010	Updated supported version.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
09/30/2009	Added section about increasing memory size for XML reports.
6/30/2009	Added global update to installation procedure.

SmartConnector for IDMEF XML File

This guide provides information for installing the SmartConnector for Intrusion Detection Message Exchange Format (IDMEF) XML File and configuring the device for event collection. Snort version 1.8 is supported. The Snort plug-in is supported on Linux and Solaris platforms.

Product Overview

The purpose of the IDMEF is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them.

Configuration

Snort is open source software, and has an architecture that supports plugins. Like other Snort plug-ins, the IDMEF XML plug-in can be configured in a standard Snort configuration file, allowing for flexibility with the use of IDMEF.

The ArcSight SmartConnector contains two connectors:

- A generic IDMEF connector for generic IDMEF XML log format
- A Snort IDMEF connector for Snort IDMEF XML plug-in.

By default, Snort 1.8 does not enable the IDMEF XML plug-in. You should recompile the Snort source code to turn it on by passing the '-enable-idmef' compile flag. For more information, go to the Snort web site at <http://www.snort.org>. Note that if future Snort releases enable the IDMEF XML plugin, this step will not be required.

After you update the Snort binary, update the snort.conf file to add the idmef plugin, for example:

```
output idmef: 192.168.1.0/24 logto=/var/log/snort/idmef.log
analyzerid=IDS123 dtd=/export/home/snort/idmef.dtd
category=dns
location=Oakland address=192.168.1.120 address.cat=ipv4-
addr
homenet_loc=Oakland_network homenet_cat=dns output=alert
```

Entries made in this conf file update the Snort rules file to trigger the IDMEF plugin. There is also a perl script, `append-idmef.pl`, available to do this. You can also get more information on this script from the Snort web site at <http://www.snort.org/>

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

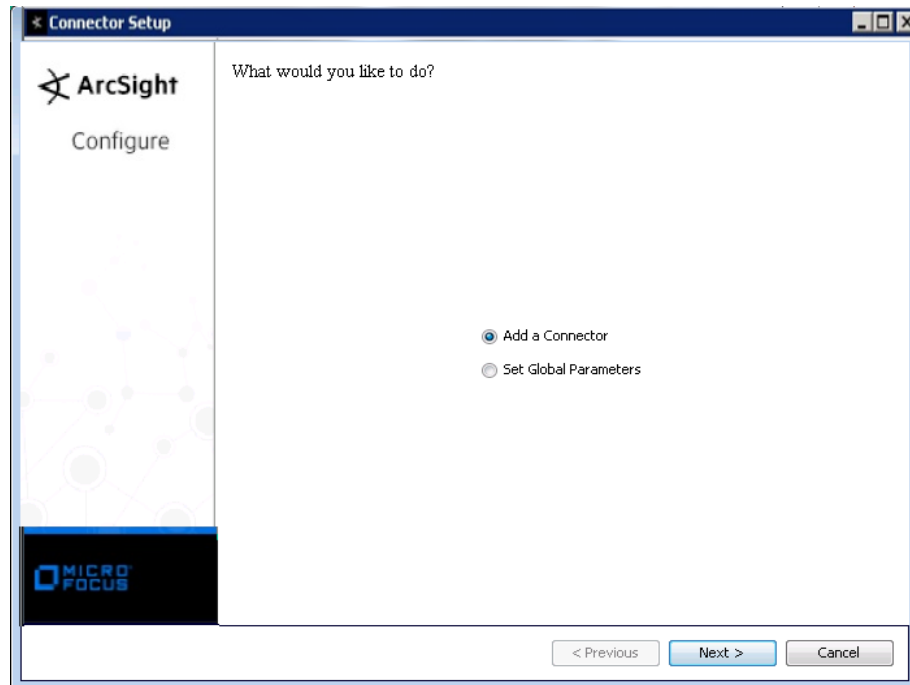
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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
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.

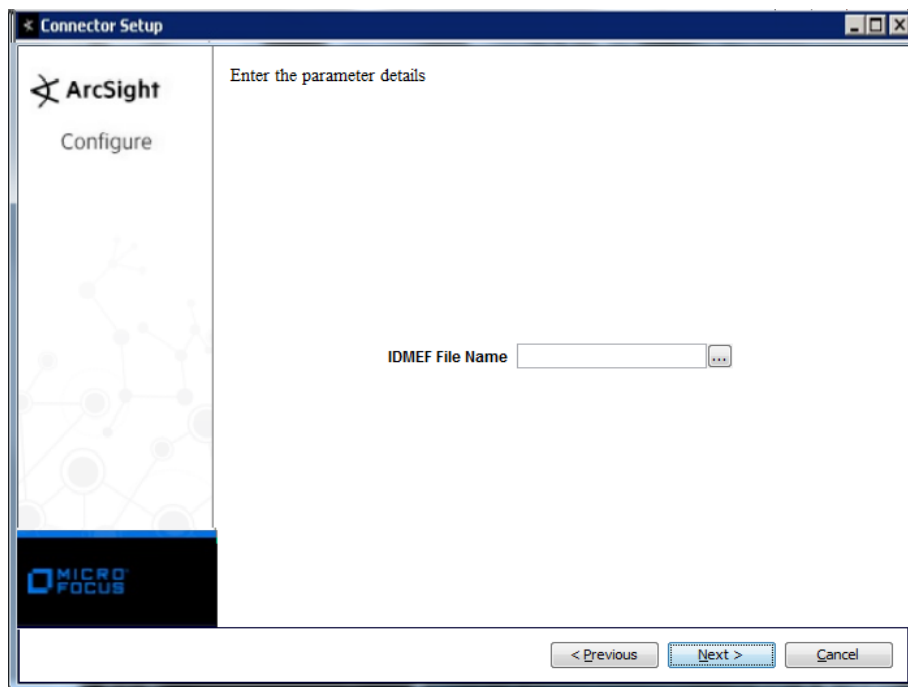
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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 **IDMEF XML File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
IDMEF File Name	Enter the name of the IDMEF XML log file.

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.

IDMEF Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Custom String 3	Classification.url
Detect Time	CreateTime
Device Address	Analyzer.Node.Address.address
Device Event Class ID	Both ('IDMEF', ident)
Device Host Name	Analyzer.Node.name
Device Location	Analyzer.Node.location
Event Name	Classification.name
Source Address	Source.Node.Address.address
Source Port	Source.Service.port
Target Address	Target.Node.Address.address
Target Port	Target.Service.port