Micro Focus Security ArcSight Connectors

SmartConnector for Snort Multiple File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Snort Multiple File

June, 2018

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.
06/30/2014	Payload support is now available for this connector.
11/15/2013	Removed payload support information.
11/15/2012	Added support for IPv6 address mappings with Snort 2.9.
05/15/2012	Added new installation procedure.
02/15/2011	Added support for Snort 2.9.

SmartConnector for Snort Multiple File

This guide provides information for installing the SmartConnector for Snort Multiple File and configuring the device for event collection. Snort versions 1.8-2.0, 2.1, 2.2, 2.4, 2.5, 2.6, 2.8, and 2.9 are supported. Payload retrieval support is available for the latest supported Snort version.

Product Overview

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Configure Snort to Generate ULF

1. Edit `snort.conf` and a line to enable FAST mode for the identified log file; for example:

   ```
   Output alert_fast: <logfilename>
   ```

   where `<logfilename>` is the name of your log file.

2. Run Snort from `snort` home as:

   ```
   snort -l logsBin -c /etc/snort/etc/snort.conf -d
   ```

   `-l logsBin` generates the snort log file in the `logsBin` directory. (The `logsBin` directory is standard; you can specify any directory for logs.) The `-K` option is used to specify the logging mode. `pcap` is the default value. `-c` reads the configuration file identified, and `-d` runs Snort inline in daemon mode.

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.

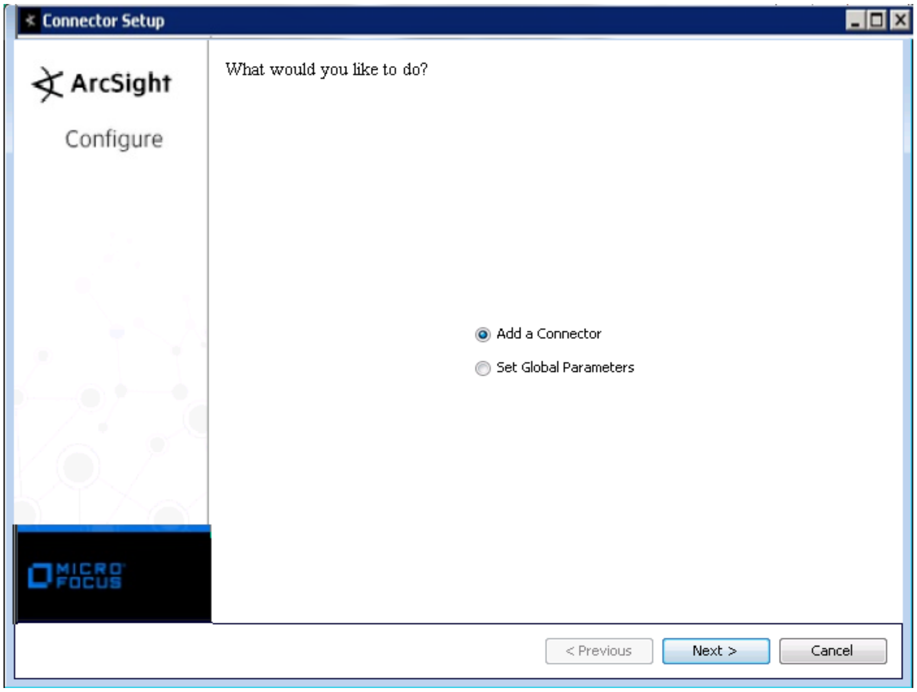
1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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:



What would you like to do?

● Add a Connector

○ Set Global Parameters

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.

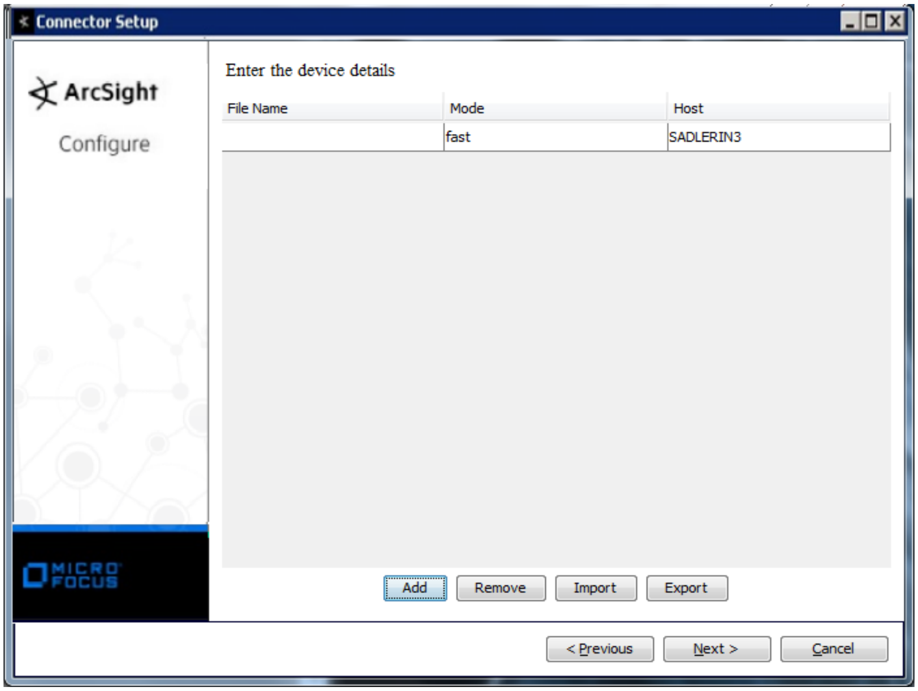
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **Snort Multiple File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the device details

File Name	Mode	Host
	fast	SADLERIN3

Parameter	Description
File Name	Specify the full path to the directory containing the Snort log files as well as the Snort log file name; for example, /var/log/snort/alert.fast.
Mode	The mode to indicate the alert type of the Snort Log file. FAST mode is supported. Include the following line in the Snort configuration file (snort.conf) to make sure alert_fast logs are generated: 'output alert_fast:< log file name>'
Host	Specify the host name of the Snort server. This value does not specify the location of the Snort log files. It is used only to populate the ArcSight Device Host Name field.

You can click the 'Export' button to export the host name data you have entered into the able into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

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*.

Payload Support

Payload support is available with the latest Snort version. *Payload* refers to the information carried in the body of an event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload may also be forensically significant. You need not explicitly enable payload. However, payloads are downloaded and stored only on demand; you must configure ESM to log these packets. By default, 256 bytes of payload will be retrieved.

To get payload from the SmartConnector for Snort Multiple File, run the SmartConnector as a user who has permission to access the payload files generated by Snort. Otherwise, the SmartConnector will receive an access denied error when trying to read the payload files.

To ensure the payload is kept inside payload files as plain text, use the -K ascii option within the command line when Snort is started; for example `snort -K ascii -c /etc/snort/etc/snort.conf -d`.

You can retrieve, preserve, view, or discard payloads using the ArcSight Console. Because event payloads are relatively large, ArcSight does not store them by default. Instead, you can request payloads from devices for selected events through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console.

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

Locate Payload-Bearing Events

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view. In an ArcSight Console Viewer panel grid view, right-click a column header and choose **Add Column -> Device -> Payload ID**. Look for events showing a Payload ID in that column.

Retrieve Payloads

In a Viewer panel grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab, then click **Retrieve Payload**.

Preserve Payloads
In a grid view, right-click an event with an associated payload, select **Payload**, then **Preserve**. Alternatively, in the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discard Payloads
In a grid view, right-click an event with an associated payload and select **Payload**, then **Discard Preserved**. You also can use the Event Inspector: In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Discard Preserved Payload**.

Save Payloads to Files
In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Save Payload**. In the **Save** dialog box, navigate to a directory and enter a name in the **File name** text field. Click **Save**.

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.

Snort Multiple File Mappings to ArcSight ESM Data Fields

ArcSight ESM Field	Device-Specific Field
ArcSight Severity	Very High when Device Severity = 0 or 1; High when Device Severity = 2; Medium when Device Severity = 3; Low when Device Severity = 4, 5, or 6
Destination Address	Destination IP Address
Destination Port	Destination Port
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Revision
Device Custom String 6	OrigTimestamp
Device Event Category	Classification
Device Event Class Id	Both (GeneratorID, SnortID)
Device Host Name	Device Host Name
Device Product	'Snort'
Device Receipt Time	DetectTime
Device Severity	Priority
Device Vendor	'Snort'
Name	Message
Source Address	Source IP Address
Source Port	Source Port
Transport Protocol	Protocol

Troubleshooting

Notes about ArcSight Severity Mapping

The current ArcSight severity mapping is for Snort 1.8.3 or later version. If you are using the old version of Snort, you need to change the mapping manually using the following steps.

1. Open the agent properties file:

   ```
   ARCSIGHT_HOME/user/agent/flexagent/snort/
   snort*.sdkrfilereader.properties
   ```

2. Search for the following lines:

   ```
   severity.map.veryhigh.if.deviceSeverity=0,1
   severity.map.high.if.deviceSeverity=2
   severity.map.medium.if.deviceSeverity=3
   severity.map.low.if.deviceSeverity=4,5,6
   ```

3. Modify them to meet your needs. For example, following changes will work for Snort version 1.8.1.

   ```
   severity.map.veryhigh.if.deviceSeverity=9,10,11
   severity.map.high.if.deviceSeverity=6,7,8
   severity.map.medium.if.deviceSeverity=3,4,5
   severity.map.low.if.deviceSeverity=0,1,2
   ```

4. Save the properties file.

5. Restart the connector.