Micro Focus Security ArcSight Connectors

SmartConnector for IP Flow Information Export (IPFIX)

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for IP Flow Information Export (IPFIX)

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.
08/30/2016	First release of this connector.

SmartConnector for IP Flow Information Export (IPFIX)

This guide provides information for installing the SmartConnector for IP Flow Information Export (IPFIX) and configuring the device for event collection. IPFIX Version 10 is supported.

Product Overview

Internet Protocol Flow Information Export (IPFIX) is an IETF protocol and the name of the IETF working group defining the protocol. It was created based on the need for a common, universal standard of export for Internet Protocol flow information from routers, probes, and other devices used by mediation systems, accounting/billing systems, and network management systems to facilitate services such as measurement, accounting, and billing.

The IPFIX standard defines how IP flow information is to be formatted and transferred from an exporter to a collector.

Similar to the NetFlow protocol, IPFIX considers a flow to be any number of packets observed in a specific timeslot and sharing a number of properties (same source, same destination, and same protocol). Using IPFIX, devices such as routers can inform a central monitoring station about their view of a potentially larger network.

IPFIX is a push protocol; each sender will periodically send IPFIX messages to configured receivers without any interaction by the receiver.

IPFIX can integrate information that would normally be sent to Syslog or SNMP directly in the IPFIX packet, thus eliminating the need for these additional services collecting data from each network device. This lets hardware vendors specify a Vendor ID and put any proprietary information into a Flow and export it out of the collector/analyzer for further dissecting and monitoring.

IPFIX also allows fields of a variable length, which means IDs do not have to conform to a fixed length. Netflow does not allow variable length fields. Variable length fields let you save information such as URLs (which differ from site to site), messages, HTTP hosts, and more.

Configuration

For instructions on configuring IPFIX for event collection, see the vendor documentation for your IPFIX-supported device.

Install the SmartConnector

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

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

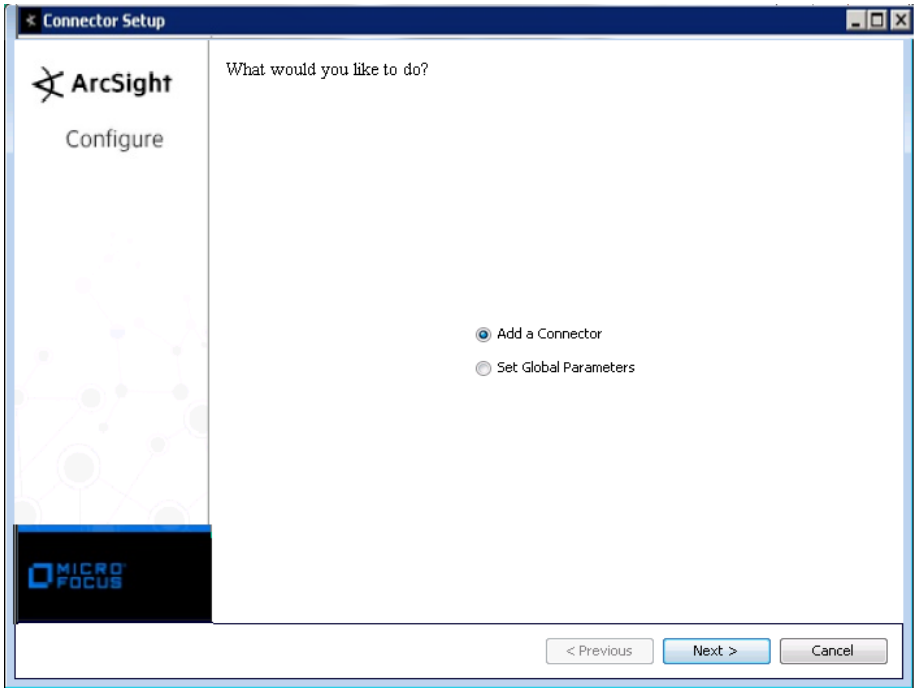
Install Core Software

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.

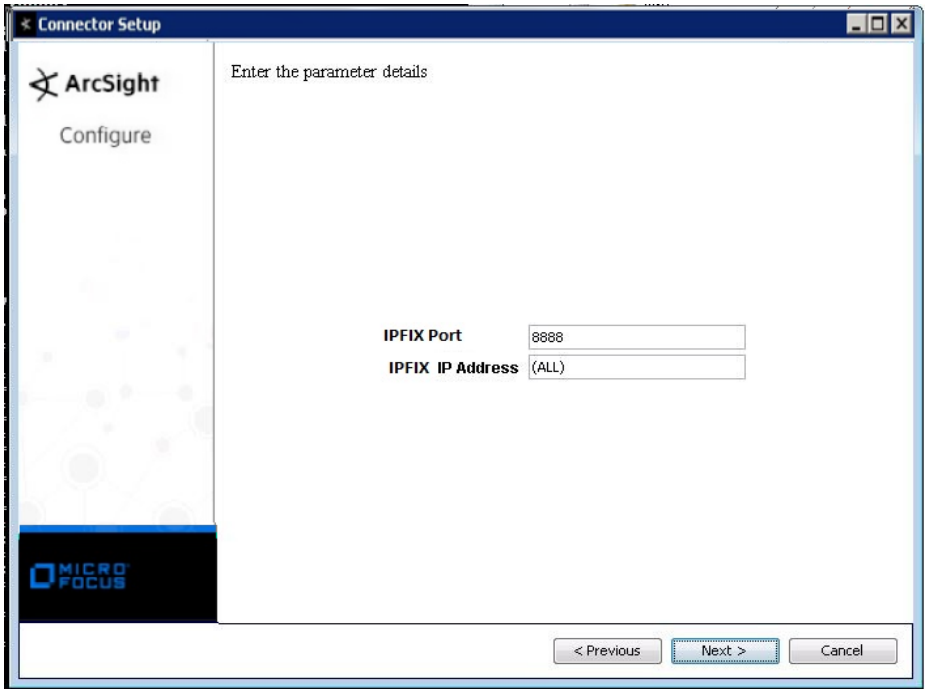
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of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



Parameter	Description
IPFIX Port	Enter the number of the port to which the SmartConnector will listen.
IPFIX IP Address	The only currently supported value for this field is (ALL), meaning the connector will listen to all IP addresses on the specified port. Individual IP addresses cannot be specified at this time.

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.

IPFIX Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Base Event Count	flows
Bytes In	bytes
Destination Address	ip_dst_addr
Destination Port	l4_dst_port
Device Address	DeviceAddress
Device Custom IPv6 Address 2	ipv6_src_addr (Source IPV6 Address)
Device Custom IPv6 Address 3	ipv6_dst_addr (Destination IPV6 Address)
Device Custom Number 1	pkts (packets)
Device Custom Number 2	tcp_flags (tcp_flags)
Device Custom String 1	ip_next_hop (nexthop)
Device Custom String 2	src_as (Source BGP autonomous system number)
Device Custom String 3	dst_as (Destination BGP autonomous system number)
Device Custom String 4	src_mask (src_mask)
Device Custom String 5	dst_mask (dst_mask)
Device Custom String 6	tcp_flags descr
Device Event Class Id	'flow'
Device Inbound Interface	interface_input_snmp
Device Outbound Interface	interface_output_snmp

ArcSight ESM Field	Device-Specific Field
Device Product	'IPFIX'
Device Receipt Time	pkthdr_unix_secs
Device Vendor	'IPFIX'
Device Version	pkthdr_version
End Time	last_switched
Name	'IPFIX event'
Request Url	undefined_32769
Source Address	ip_src_addr
Source Port	l4_src_port
Start Time	first_switched
Transport Protocol	protocol