Micro Focus Security ArcSight Connectors

SmartConnector for IP Flow (NetFlow/J-Flow)

Configuration Guide

February 19, 2019

Configuration Guide

SmartConnector for IP Flow (NetFlow/J-Flow)

February 19, 2019

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
02/19/2019	Updated mappings for IP Flow Version 9.
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).
02/15/2017	Clarified the description of supported versions.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Added support for Cisco ASA 8.5 with NetFlow version 9. Updated mappings for IP Flow Version 9.
09/30/2013	Updated mappings for Device Custom Number 3 and Device Custom String 6.
05/15/2012	Added new installation procedure.
05/15/2011	Corrected connector installer name.
06/25/2010	Renamed connector and added support for Juniper J-Flow.
03/31/2010	Added support for NetFlow Flexible IOS 15.0 and ASA 8.2 events.

SmartConnector for IP Flow (NetFlow/J-Flow)

This guide provides information for installing the SmartConnector for IP Flow (NetFlow/J-Flow) and configuring the device for event collection. Cisco NetFlow version 9 and flexible NetFlow from IOS 15.0 are supported. Older Cisco IOS versions might produce unsupported events. Cisco ASA 8.2 and 8.5 are supported with Juniper J-Flow version 9 support.

Product Overview

Juniper J-Flow

The Juniper Networks J-Flow feature provides a method by which you can collect IP traffic flow statistics on your routing devices. J-Flow requires no special protocol for connection setup. It also does not require any external changes to networked traffic, packets, or any other devices in the network.

The Juniper Networks implementation of J-Flow lets you export data to the UDP port of a remote workstation for data collection and further processing. Because you can enable J-Flow on an individual virtual router or interface, you can collect network statistics for specific locations within your network.

Cisco NetFlow

Cisco NetFlow technology provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, and network planning, as well as Denial Services monitoring capabilities, network monitoring, outbound marketing, and data mining capabilities for both service provider and enterprise customers.

Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction, perform post-processing, and provide easy access to NetFlow data to end-user applications.

Cisco IOS NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial-of-Service monitoring capabilities, and network monitoring. NetFlow provides information about network users and applications, peak usage times, and traffic routing.

Cisco's NetFlow version 9 is a flexible and extensible method to record network performance data. It is the basis of a new IETF standard. Cisco is currently working with a number of partners to provide customers with comprehensive solutions for NetFlow-based, planning, monitoring and billing.

NetFlow was introduced in IOS version 11.1CA and continued to evolve over the years (v1 through v9). The formats that gained popular acceptance were NetFlow v5 (introduced in 11.1CA) and v9 (which was introduced in 12.3(1)).

Between IOS versions 12.4(9)T and 15.0(1)M, Cisco introduced Flexible NetFlow (later versions added support for advanced features such as application recognition). Although the steps to configure Flexible NetFlow on IOS devices is completely different, it exports NetFlow data in the same formats (v5 or v9, with v9 being the recommended export format).

Cisco ASA (which does not run IOS) added a feature to support fixed format NetFlow export, starting version 8.2.

For more information about the history of NetFlow, see the following sites:

http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html
http://www.cisco.com/en/US/docs/ios/12_3/feature/gde/nfv9expf.html

Configure the Device to Send Events

Configure J-Flow

Before you configure J-Flow statistics, you should have created IP interfaces from which J-Flow will extract traffic flow information.

See the Juniper Networks product documentation for J-Flow operation and configuration information.

Configure NetFlow

There are three sections involving configuration for NetFlow devices, as follows:

- Configure Fixed-Format (non-flexible) Export on IOS
- Configure Flexible NetFlow on IOS
- Configure Fixed-Format Export on ASA

Configure Fixed-Format (non-flexible) Export on IOS

Perform the following task to configure a router to export NetFlow data to the SmartConnector for SmartConnector for IP Flow (NetFlow/J-Flow) when a flow expires.

1. Enable privileged EXEC mode: `Router>enable`
   Enter your password if prompted.
2. Enter global configuration mode: `Router#configure terminal`
3. Enable the export of information in NetFlow cache entries:

   ```
   ip flow-export version 5 [origin-as | peer-as]
   ```

   or

```
ip flow-export version 9 [origin-as | peer-as]
```

Example:

```
Router(config)# ip flow-export version 5 peer-as
```

or

```
Router(config)# ip flow-export version 9
```

The **origin-as** option specifies that export statistics include the originating autonomous system (AS) for the source and destination.

The **peer-as** option specifies that export statistics include the peer AS for the source and destination.

4 Specify the export destination IP address and UDP port of the SmartConnector for IP Flow (NetFlow/J-Flow) SmartConnector:

```
ip flow-export destination ip-address udp-port
```

Example:

```
Router(config)# ip flow-export destination 172.22.23.7 9997
```

The **ip-address** argument is the IP address of the workstation on which the SmartConnector is installed; this is where the NetFlow information is to be sent.

The **udp-port** argument is the UDP protocol-specific port number specified in the SmartConnector installation.

5 (Optional) Display the statistics for the data export, including the main cache and all other enabled caches. Enter this command to verify that the router is exporting NetFlow data.

```
show ip flow export
```

Example:

```
Router# show ip flow export
```

6 Exit to privileged EXEC mode: `exit`

Example:

```
Router# exit
```

Enter the following commands to verify NetFlow operation.

```
enable
show ip interface [type number] [brief]
```

```
show ip cache [prefix mask] flow
show ip cache [prefix mask] verbose flow
show ip flow export
exit
```

Configure Flexible NetFlow on IOS Devices

This task consists of:

- Configuring a customized flow record
- Verifying the flow record configuration
- Configuring the Flow Exporter
- Creating a customized flow monitor
- Applying a flow monitor to an interface

Configure a Customized Flow Record

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one match criterion for use as the key field and typically has at least one collect criterion for use as a non-key field.

There are hundreds of possible permutations of customized flow records. This task explains the steps that are used to create one of the possible permutations. Modify the steps in these tasks as appropriate to create a customized flow record for your requirements.

Enter the following basic commands for configuring a customized flow record for IPv4 or IPv6 traffic follow:

```
enable
configure terminal
flow record record-name
description description
match {ipv4 | ipv6} {destination | source} {address | {mask
| prefix} [minimum-mask mask]}
```

Repeat the `match` command as required to configure additional non-key fields for the record.

```
collect {ipv4 | ipv6} source {address | {mask | prefix}
[minimum-mask mask]}
```

Repeat the `collect` command as required to configure additional non-key fields for the record.

```
end
```

For detailed information, see "Configuring a Customized Flow Record for IPv4 or IPv6 Traffic" in *Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors*.

To display the current status of a flow record:

```
enable
show flow record
```

Verify the Flow Record Configuration

To verify the configuration commands you entered:

```
enable
show running-config flow record
```

Configure the Flow Exporter

Follow these steps to configure the Flow Exporter:

```
enable
configure terminal
flow exporter exporter-name
description string
destination {ip-address | hostname} [vrf vrf-name]
export-protocol {netflow-v5 | netflow-v9}
dscp dscp
source interface_name
option {{exporter-stats | interface-table | sampler-table |
vrf-table | application table} [timeout seconds]}
output-features
template data timeout seconds
transport udp udp-port
ttl ttl
end
```

To verify the Flow Exporter:

```
enable
show flow exporter
show running-config flow exporter
```

Create a Customized Flow Monitor

To create a customized flow monitor:

```
enable
configure terminal
flow monitor monitor-name
```

```
description string
record {record-name | netflow-original | netflow {ipv4 |
ipv6} record [peer]}
cache {entries number | timeout {active seconds | inactive
seconds | update seconds} | type {immediate | normal |
permanent}}
Repeat Step 6 as required to finish modifying the cache
parameters for this flow monitor.
statistics packet protocol
statistics packet size
exporter exporter-name
end
```

To display the current status of a flow monitor:

```
enable
show flow monitor monitor-name
```

To verify the configuration commands that you entered:

```
enable
show running-config flow monitor monitor-name
```

Apply a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. To activate a flow monitor:

```
enable
configure terminal
interface type number
{ip | ipv6} flow monitor monitor-name {input | output}
Repeat the flow monitor command to activate a flow monitor
on any other interfaces in the router over which you want
to monitor traffic.
end
```

To verify that Flexible NetFlow is enabled on an interface:

```
enable
show flow interface [ type number ]
```

Payload Sampling

Payload data is available in two unmapped additional data fields: `ip_section_header` and `ip_section_payload`. If required, these fields can be mapped to the flexString fields. See the following Cisco publication for information about NetFlow Flow sampling.

Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic.

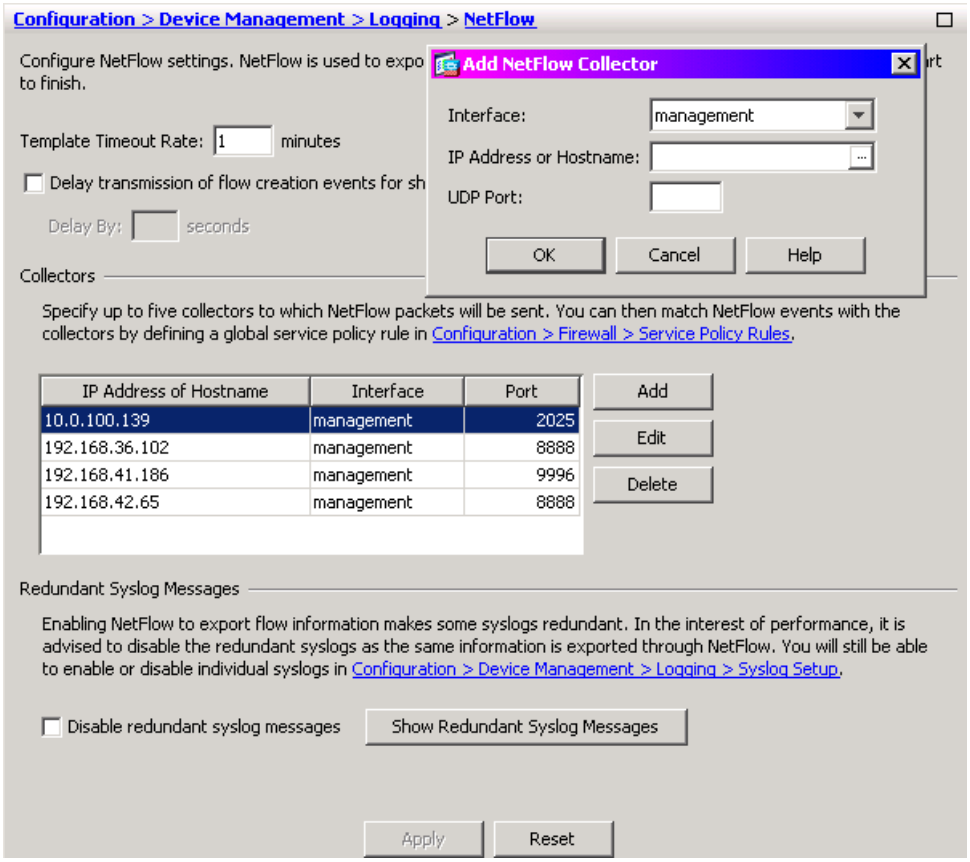
Configure Fixed-Format Export on ASA

The first step is to add a NetFlow collector, then to add a service policy to be applied to the collector.

Add a Collector

To add a collector:

1. Login to your Cisco ASDM user interface.
2. Click Configuration at the top of the window. Then, from the left pane, select **Device Management -> Logging -> NetFlow**. Click **Add**.



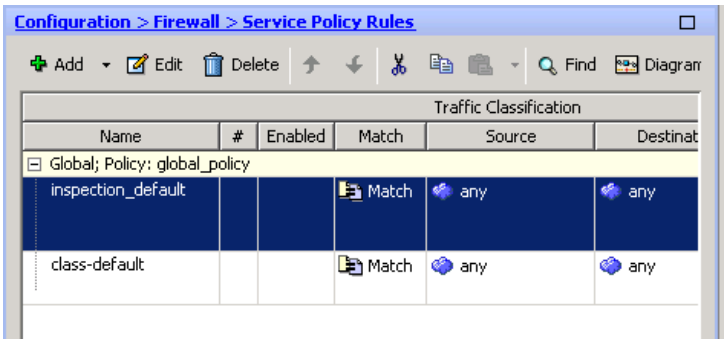
2. Select the type of interface and enter the IP address or host name and UDP port to be used, then click **OK**.
3. Click **Apply** for your change to take effect.

Add a Service Policy

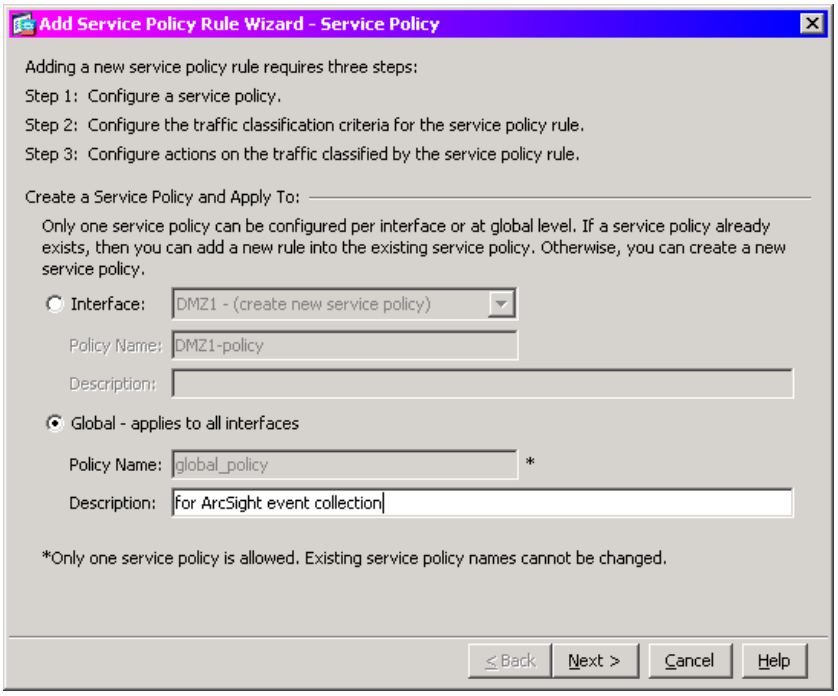
To add a service policy:

1 Login to your Cisco ASDM user interface.

2 Under **Collectors** on the NetFlow window, click **Configuration > Firewall > Service Policy Rules** to add policy rules for collectors.

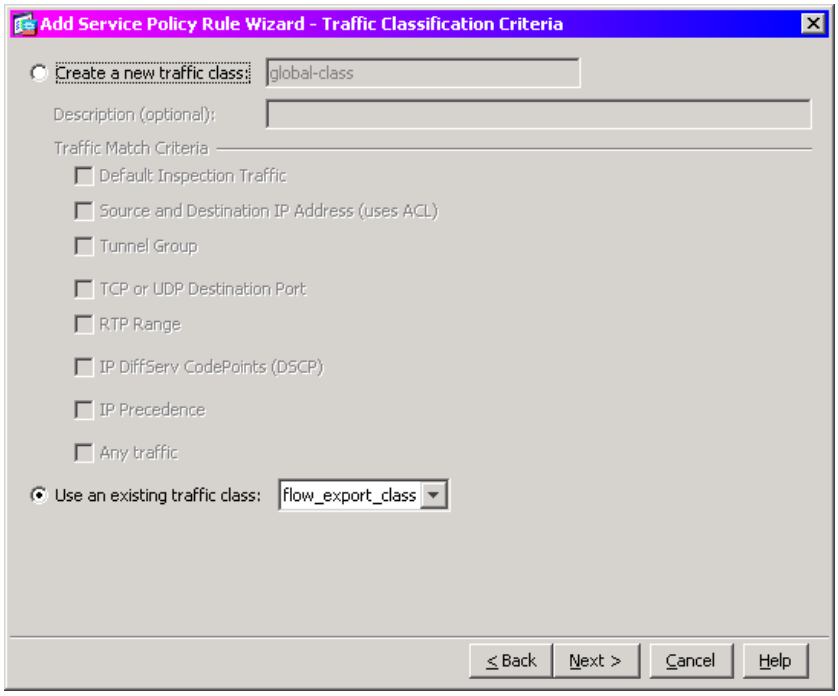


3 Click **Add**. Comprehensive how-to information is available when you click **Help** on the **Add Service Policy Rule Wizard – Service Policy** window.

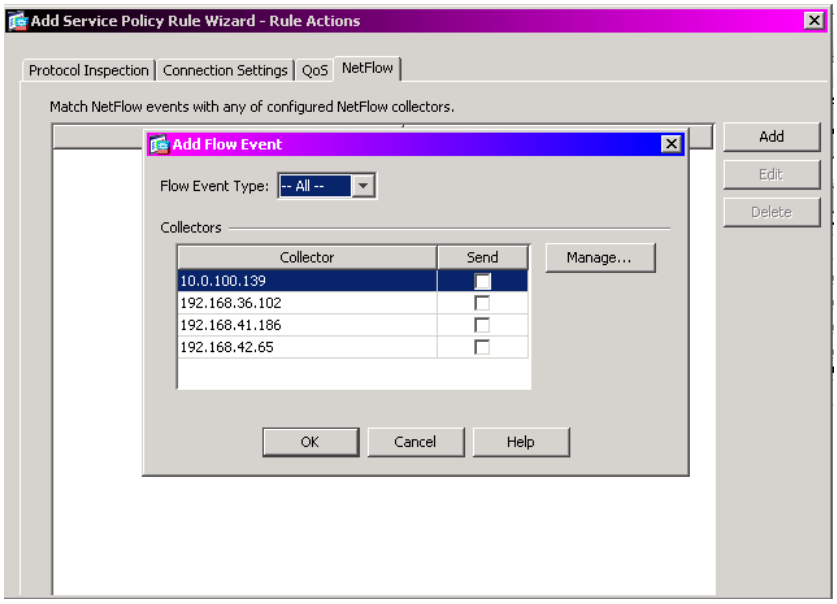


4 Select **Global – applies to all interfaces**. Enter a meaningful description for the policy as desired. Click **Next** to continue.

5 On the **Add Service Policy Rule Wizard – Traffic Classification Criteria** window, select **Use an existing traffic class** and be sure **flow_export_class** is selected. Click **Next**.



6 The **Add Service Policy Rule Wizard – Rule Actions** window is displayed. Click the **NetFlow** tab. NetFlow packets can be sent to up to five collectors. Click **Add**; check the **Send** box for the collector you added so that it will receive NetFlow events.



7 Click **OK** on the **Add Flow Event** window.

8 Click **Finish** to exit the **Add Service Policy Rule Wizard**.

Configure ASA Devices Using the Command Line

Enter the following commands from the command line interface to select collectors and policy rules for event collection.

```
flow-export destination management ip-address udp-port
flow-export destination management ip-address udp-port
flow-export destination management ip-address udp-port
flow-export destination management ip-address udp-port
      .
      .
      .
class-map flow_export_class
 match any
      .
      .
      .
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class class-default
  flow-export event-type all destination ip-address ip-
address2 ip-address3 ip-address4
      .
      .
      .
policy-map flow_export_policy
 class flow_export_class
  flow-export event-type all destination ip-address ip-
address2 ip-address3 ip-address4
```

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

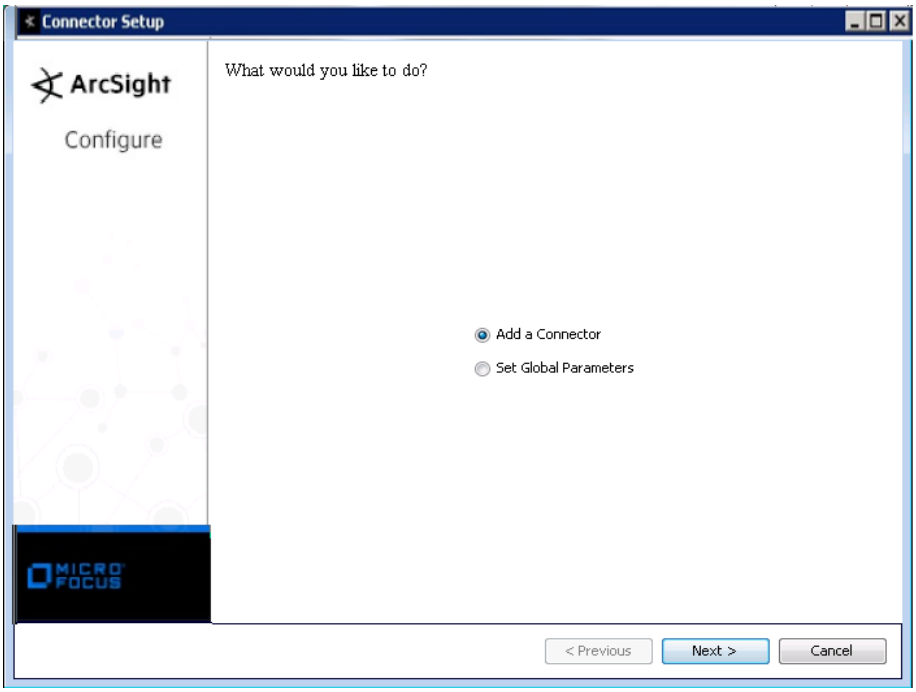
Install Core Software

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.

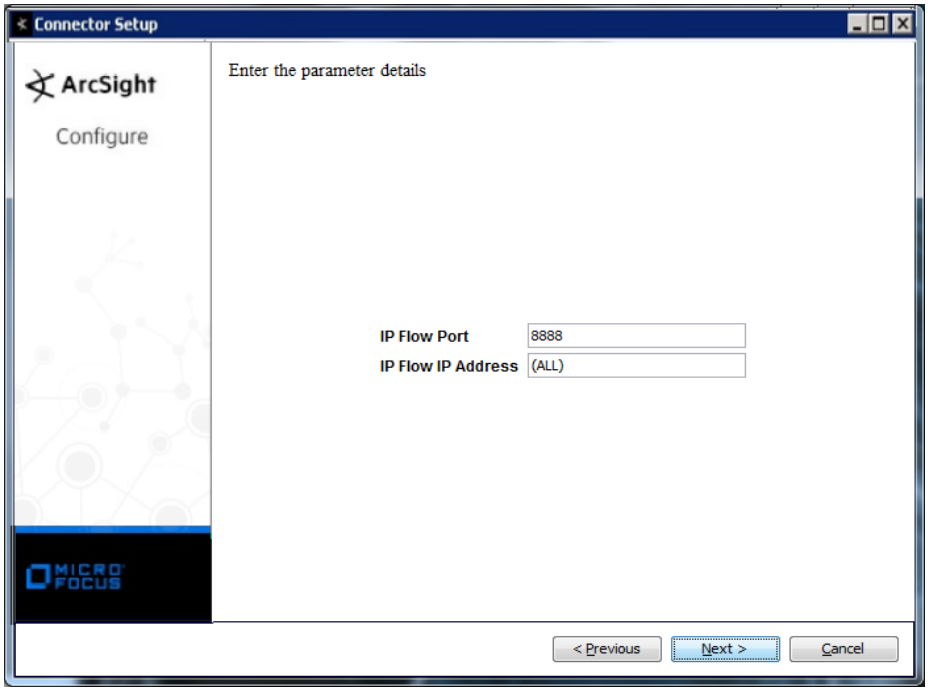
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of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



Parameter	Description

Parameter	Description
IP Flow Port	Enter the number of the port to which the SmartConnector will listen.
IP Flow IP Address	The connector listens 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.

IP Flow Version 9 Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Base Event Count	flows
Bytes In	One of (in_bytes, in_permanent_bytes, undefined_231)
Bytes Out	One of (out_bytes, undefined_232)
Destination Address	ipv4_dst_addr
Destination Mac Address	oneOf(in_dst_mac,out_dst_mac)
Destination Port	One of (14_dst_port, transport_tcp_destination-port, transport_udp_destination-port)
Destination Process Name	application_id_application_name
Destination Translated Address	xlate_dst_addr_ipv4
Destination Translated Port	xlate_dst_port
Destination User Name	username
Device Address	DeviceAddress
Device Custom Number 1	in_pkts
Device Custom Number 2	out_pkts
Device Custom Number 3	tcp_flags
Device Custom String 1	ipv4_next_hop
Device Custom String 2	src_as
Device Custom String 3	dst_as
Device Custom String 4	src_mask

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	dst_mask
Device Custom String 6	tcp_flags descr
Device Direction	direction
Device Event Class ID	'flow'
Device Inbound Interface	interface_input_snmp_interface_name
Device Outbound Interface	interface_output_snmp_interface_name
Device Product	'IP Flow'
Device Receipt Time	pkthdr_unix_secs
Device Vendor	'IP Flow'
Device Version	pkthdr_version
End Time	last_switched
External ID	connection_id
File Hash	napt_source_transport_port
File Type	nat_src_ipv4_address
Message	fw_ext_event
Name	oneOf(fw_event,firewallEvent,"NetFlow Event")
Old File Hash	napt_des_transport_port
Old File Type	nat_des_ipv4_address
Source Address	ipv4_src_addr
Source Mac Address	oneOf(in_src_mac,out_src_mac)
Source Port	oneOf(l4_src_port,transport_tcp_source-port,transport_udp_source-port)
Source Translated Address	xlate_src_addr_ipv4
Source Translated Port	xlate_src_port
Start Time	first_switched
Transport Protocol	protocol

Cisco ASA 5.2 NetFlow Only Mappings

ArcSight ESM Field	Device-Specific Field
Destination Translated Address	xlate_dst_addr_ipv4
Destination Translated Port	xlate_dst_port
Destination User Name	username
Device Custom Number 3	tcp_flags
Device Custom String 6	tcp_flags descr
External ID	connection_id
Message	fw_ext_event (1001=Ingress ACL, 1002=Egress ACL, 1003=Adaptive security appliance denied attempt to connect to interface service, 1004=First packet on the TCP was not a TCP SYN packet)
Name	One of (fw_event 'NetFlow Event' (fw_event, 1=Flow Created, 2=Flow Deleted, 3=Flow Denied))
Source Translated Address	xlate_src_addr_ipv4
Source Translated Port	xlate_dst_port

NetFlow Troubleshooting

Devices that send NetFlow data send the template information at a configured time interval. The default value for this time interval is 1800 seconds (30 mins). The NetFlow connector cannot process the NetFlow data unless it receives the corresponding template data. In these cases, a warning message such as the following is displayed in `agent.log`:

```
Did not add any records because template for flowsetid
[SOME NUMBER] is null
```

So, if the configured interval is large, the connector gets the template data less frequently and does not process the corresponding flow data. Reducing the value of this time interval lets the connector get templates more frequently, with more NetFlow events being processed.

To reduce this interval, execute the following commands:

Netflow from IOS:

```
template data timeout <SomeValueInSeconds>
```

NetFlow from ASA:

```
flow-export template timeout-rate <SomeValueInMinutes>
```