Micro Focus Security ArcSight Connectors

SmartConnector for Juniper Network and Security Manager Syslog

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Juniper Network and Security Manager Syslog

June, 2018

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	Removed support for versions 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
09/30/2014	Added IPv6 address mappings.
05/15/2013	Added support for Juniper NSM 2012.2.
12/21/2012	Added support for Juniper NSM 2012.1.
11/15/2012	Support ended for Juniper NSM 2010.2 and earlier versions.
09/28/2012	Added mappings for Device Custom IPv6 address fields.
08/15/2012	Added support for Juniper NSM version 2011.4. Added and updated mappings.

SmartConnector for Juniper Network and Security Manager Syslog

This guide provides information for installing the SmartConnector for Juniper Network and Security Manager (NSM) Syslog and configuring the device for syslog event collection. Juniper NSM version 2012.2 is supported.

Product Overview

Juniper Network and Security Manager is a management system that integrates your individual devices into a single security system controlled from a central location. With NSM, you can manage your network at the system level, using policy-based central management, as well as at the device level, managing all device parameters for devices.

Configuration

Configure the Device for Logging

For complete information about Network and Security Manager logging, see the chapter "Configuring the Device for Logging" in the Juniper *Network and Security Manager Administration Guide*. Information in this section has been extracted from that document.

Configure the device and the NSM system for logging so your device can generate log entries and log data. You can configure an individual device to generate attack, alarm, configuration, information, and self-log entries for specific destinations. You can configure how and where the device sends its log entries. For each destination you can define the category of log entries you want the device to generate and forward to a specific destination, and the severity of log entries you want the device to forward. The severity setting applies to all log types for that destination.

To log an event for a rule, enable logging. Each time your security device matches network traffic to the rule, the device creates a traffic log entry that describes that event. You can enable logging when a session is initialized, closed or both on a security device.

Direct Logs to a Syslog Server

The managed device can generate syslog messages for system events at predefined severity levels and optionally for traffic that policies permit across a firewall. It sends these messages via UDP (port 514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the devices use to send syslog packets.

To send log entries to a Syslog server, click the **Syslog** option. NSM displays the **Syslog** dialog box. Enter appropriate data into the following fields.

Field	Description
Enable Syslog Messages	Initiates the logging of system event messages to the syslog server.
Port Number	Indicates the port number from where the messages are sent to the syslog server.

Field	Description
Use Trust Zone Interface as Source IP for VPN	Specifies using the interface mapped to the Trust zone as the source of traffic for a VPN.
Include Traffic Log	Specifies that all traffic log events are included as part of the messages sent to the syslog server.
Config Host	Indicates the name of the host device.

Forward Logs

You can forward your log records using one of the following methods:

- Use the Action Manager, a node on the main UI, to configure the management system to forward logs generated within a specific domain or subdomain in NSM.

- Use the log2Action Utility located on the NSM Device Server.

Use the Action Manager

Use the **Action Manager** node to configure the management system to perform actions (such as syslog) on log data based on the criteria you specify. These actions occur for all the managed devices in a specific domain or subdomain.

To enable the management system to export logs, you must configure:

- Action parameters, which define the default log export settings for the management system and determine how the system handles qualified log entries (log entries that match specified log criteria).

- Device log action criteria, which specifies the category and severity of the log entries you want to export. When a log entry meets the specified criteria, it is considered qualified and NSM performs the specified actions defined in the criteria.

To configure action parameters, from the **Action Manager**, select **Action Parameters** to define the default log export settings for the management system. To enable the management system to export qualified logs to the system log, configure the export settings for syslog format.

For exporting to the system log, configure the IP address and the server facility for all of multiple syslog servers to which you want to send qualified logs. NSM uses the specified server when exporting qualified log entries to the system log. To actually export logs to a system log server, you must select **Syslog Enable** using the **Actions** tab in the **Device Log Action Criteria** node.

Use the log2Action Utility

The syslog action directs the system to send logs to a syslog server in syslog format. Specify the IP address of the syslog server that receives the exported log records and the syslog facility.

To export:

1 Login to the Device Server as root, then change to the utility directory by entering:

```
cd /usr/netscreen/DevSvr/utils
```

2 To export to a file, enter:

```
sh devSvrCli.sh --log2action --action --syslog <server>
<facility>
```

The Device Server exports all log records to the specified IP address for the syslog server.

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

> ✎ Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a *file* or a system *pipe* and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the **/etc/rsyslog.conf** file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the **/etc/rsyslog.conf** file to send events to it.

For syslog pipe:

1   Create a pipe by executing the following command:

```
mkfifo /var/tmp/syspipe
```

2   Add the following line to your **/etc/rsyslog.conf** file:

```
*.debug   /var/tmp/syspipe
```

or

```
*.debug   |/var/tmp/syspipe
```

depending on your operating system.

3   After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid´
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

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

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

Syslog Daemon
Syslog Pipe
Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

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.

> ✎   When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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:
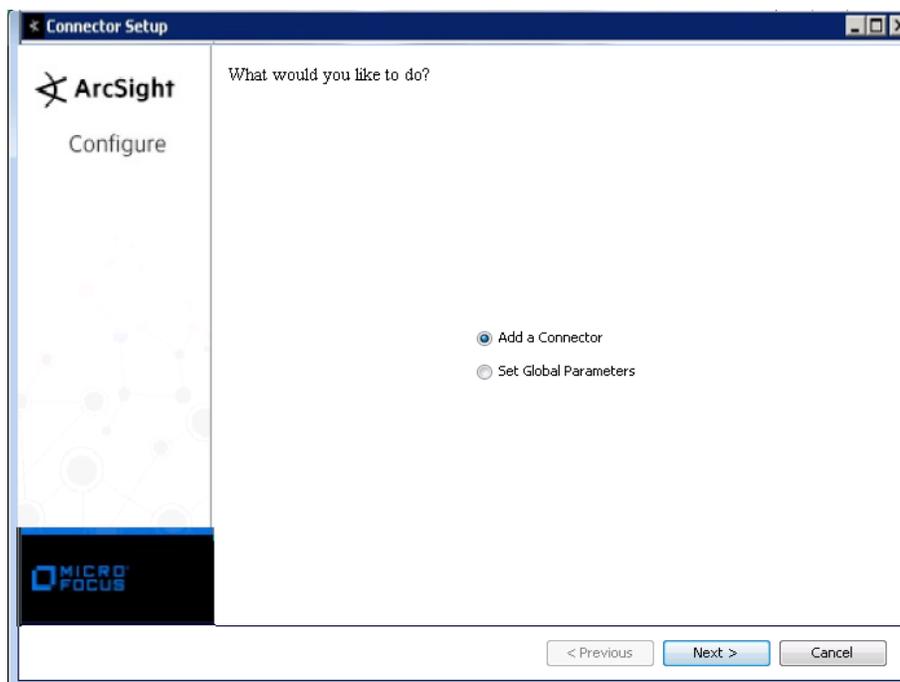
Set Global Parameters (optional)

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.
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 **Syslog Daemon (Windows), Syslog File, or Syslog Pipe** and click **Next**.

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

Syslog Daemon Parameters	*Network port*	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux).

A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation.

For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example:

`filename'yyyy-MM-dd'.log;`

For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:

`filename'%d,1,99,true'.log;`

Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional. |
	Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

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.

Juniper Network and Security Manager Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	bytesTotal
Additional data	ICMPSequenceNumber=srcPort
Additional data	ICMPIdentifier=dstPort
Additional data	NamePrefix
Additional data	NetScreenSignature
Additional data	packetsTotal
Additional data	UrlCategory
Additional data	varData
Additional data	Zone
Agent (Connector) Severity	info, warning, none, debug, informational, notice = Low; minor, alert, device_warning_log = Medium; major = High, critical, device_critical_log, emergency, error = Very High
Base Event Count	repeatCount+1
Bytes In	bytesIn
Bytes Out	bytesOut
Destination Address	dstAddr
Destination Port	dstPort
Destination Process Name	appliService
Destination Translated Address	dstNatAddr
Destination Translated Port	dstNatPort
Destination User Name	user
Device Action	action
Device Address	deviceIP, localIP or dvcAddr
Device Custom Date 1	NsmReceivedTime
Device Custom IPv6 Address 1	Device IPv6 Address
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	elapsedInSecs (Duration)

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	packetsIn
Device Custom Number 3	packetsOut
Device Custom String 1	All of (ruleDomain, ruleDomainVersion, policy, ruleBase, ruleNumber, policyId)
Device Custom String 2	LogDayId
Device Custom String 3	srcZone (Source Zone)
Device Custom String 4	dstZone (Destination Zone)
Device Custom String 5	isAlert
Device Custom String 6	hasPacketData
Device Domain	Both (deviceDomain,deviceDomainVersion)
Device Event Category	category
Device Event Class ID	subCategory
Device Host Name	deviceHostName
Device Inbound Interface	srcIntf
Device Outbound Interface	dstIntf
Device Process Name	app
Device Product	'NSM'
Device Receipt Time	deviceGeneratedTime
Device Severity	severity
Device Vendor	'Juniper'
External ID	logRecordId
File Name	FileName
Message	All of (subcategory, details)
Name	One of (subcategory, Action)
Request Method	method
Request URL	URL or URI
Source Address	srcAddr
Source Port	srcPort
Source Translated Address	srcNatAddr
Source Translated Port	srcNatPort
Transport Protocol	protocol

Connector Verification and Troubleshooting

For basic syslog and Communication issues, see the troubleshooting section of the *SmartConnector for UNIX OS Configuration Guide.*

You may encounter the following NetScreen and NSM specific issues during installation.

Syslog Daemon on SmartConnector machine is not receiving messages from NetScreen.

Verification and Action:

- Be sure the NetScreen devices are configured for sending log information to NSM. This includes the log destination, log types, and severities.

- Be sure NSM is configured for syslog reporting as described in the section "Configuring the Juniper NSM Device." Be sure the syslog settings are configured on the correct interface to reach the SmartConnector machine.

- Be sure none of the basic syslog and communication problems as described in the troubleshooting section of the *SmartConnector for UNIX OS Configuration Guide* apply to the current issue.

- Review the policies or rules configured on the NSM and NetScreen devices and the order in which they are applied. Ensure that no rule or policy is defined that blocks the outgoing syslog messages on the interface defined for syslog reporting.

- Review the various log entry viewers on NSM and ensure that some events are being logged.