



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for McAfee Network Security Manager Syslog

Configuration Guide

January 23, 2018

Configuration Guide

SmartConnector for McAfee Network Security Manager Syslog

January 23, 2018

Copyright © 2003 – 2018 Hewlett Packard Enterprise Development LP

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>.

Revision History

Date	Description
01/23/2018	Added version 9.1 support.
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Updated device configuration information.
05/15/2017	End of support for IntruShield versions 1.2, 1.8, and 2.1, and NSM versions 5.1 and 6.0 due to end of support by vendor.
02/15/2017	Added version 8.3 support.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2016	Added support for Layer 7 (L7) data.
05/15/2015	Added new parameters for Syslog File.
03/31/2015	Added version 8.1 support.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
03/31/2014	Updated format string to be entered in NSM; updated mappings.
02/14/2014	Corrected typo in format string to be entered in NSM.

SmartConnector for McAfee Network Security Manager Syslog

This guide provides information for installing the SmartConnector for McAfee Network Security Manager Syslog and configuring the device for syslog event collection. McAfee Network Security Manager versions 8.1, 8.3 and 9.1 are supported.

Product Overview

McAfee Network Security Manager is a 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.

Configuration

Forwarding Events to Syslog

Configure the sensor to do one of the following:

- Send syslog events to the McAfee NSM (and then have the manager forward the syslog events to your syslog server.)
- Configure the McAfee sensor to send the syslog events directly to your syslog server.

Follow the Documentation in the McAfee online help or the latest "IPS Administration Guide." Depending on your selection from above, customize the **Message** field in the appropriate location in McAfee NSM with the values in the following steps.

Follow this procedure to enter text in the Message field:

- 1 Select **Manager** from the main menu.
- 2 Select **Setup -> Notification -> IPS Events -> Syslog**.
- 3 Enter the following text in the message format text box under Syslog Message:

```
| $IV_ALERT_ID$ | $IV_ALERT_TYPE$ | $IV_ATTACK_TIME$ | "$IV_ATTACK_NAME$" | $IV_AT
TACK_ID$ | $IV_ATTACK_SEVERITY$ | $IV_ATTACK_SIGNATURE$ | $IV_ATTACK_CONFIDENCE
$ | $IV_ATTACK_COUNT$ | $IV_ADMIN_DOMAIN$ | $IV_SENSOR_NAME$ | $IV_INTERFACE$ | $IV
_SOURCE_IP$ | $IV_SOURCE_PORT$ | $IV_SOURCE_NAME$ | $IV_VLAN_ID$ | $IV_DESTINATIO
N_CRITICALITY$ | $IV_TARGET_IP$ | $IV_TARGET_NAME$ | $IV_TARGET_PORT$ | $IV_TARGE
T_OS$ | $IV_DETECTION_MECHANISM$ | $MALWARE_CONFIDENCE$ | $MALWARE_FILE_LENGTH$
| $MALWARE_FILE_MDS_HASH$ | $MALWARE_VIRUS_NAME$ | $IV_PROTOCOL$ | $IV_RESULT_ST
ATUS$ | $
MALWARE_FILE_TYPE$ | $MALWARE_FILE_NAME$ | $LAYER_7_DATA$ | $CC_DOMAIN$ | $CALLBA
CK_ACTIVITY$ |
```

Note that there should be no new-line characters in the field. After installing the connector, the format to be specified can also be found in the following file:

```
$ARCSIGHT_HOME/config/agent/intruvert/Intrushieldsyslogreadme.txt
```

where \$ARCSIGHT_HOME is the folder where you installed the SmartConnector for McAfee Network Security Manager Syslog. You can use a text editor to copy the text of the file and paste it into Network Security Manager's message format text area.

- 4 Click **Save**.

Configuring the Log Host to Receive Syslog Messages

The log host can be configured in one of the following ways:

- An existing syslog daemon (Unix/Linux) is configured to write to a pipe or a file, from where the ArcSight SmartConnector picks it up.
- In the absence of a syslog daemon on the log host, the ArcSight SmartConnector can listen on a UDP socket for incoming syslog messages.

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 HPE SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the HPE SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

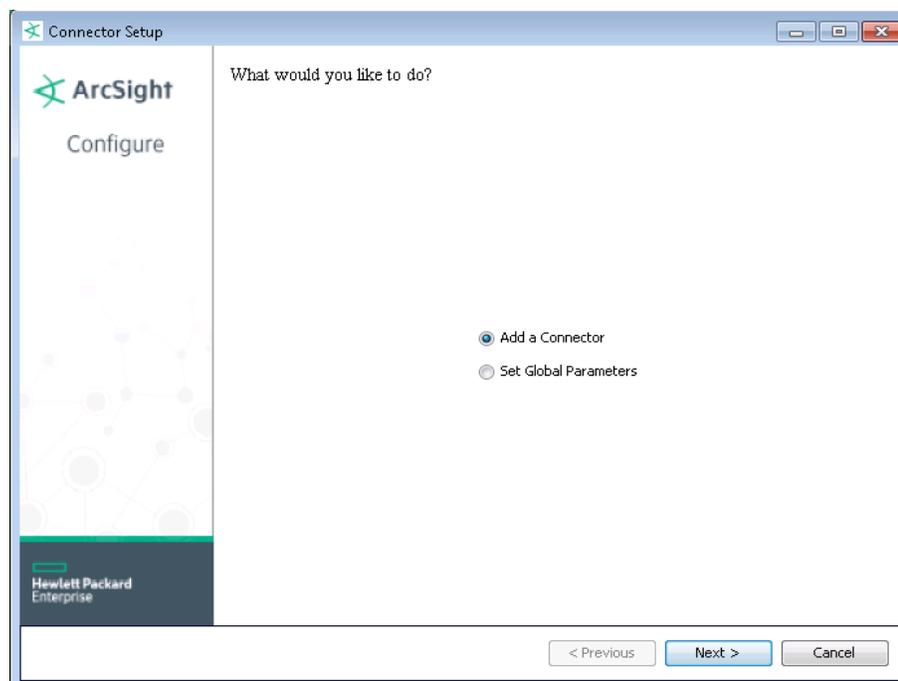


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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 HPE SecureData solutions to provide encryption. See the *HPE 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 HPE 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 HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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, File, or Pipe** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	<i>Network port</i>	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	<i>IP Address</i>	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).
	<i>Protocol</i>	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	<i>Forwarder</i>	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	<i>Pipe Absolute Path Name</i>	Absolute path to the pipe, or accept the default: <code>/var/tmp/syspipe</code>
Syslog File Parameters	<i>File Absolute Path Name</i>	Enter the full path name for the file from which this connector will read events or accept the default: <code>\var\adm\messages</code> (Solaris) or <code>\var\log\messages</code> (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.

<i>Reading Events Real Time or Batch</i>	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.
<i>Action Upon Reaching EOF</i>	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.
<i>File Extension if Rename Action</i>	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.

McAfee Network Security Manager Syslog Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity); Medium = Medium (Device Severity); Low = Low, Informational (Device Severity)
Application Protocol	PROTOCOL
Destination Address	TARGET_IP
Destination Port	TARGET_PORT
destinationNtDomain	CC_DOMAIN
destinationServiceName	LAYER_7_DATA(HTTP Server Type)
Device Custom IPv6 Address 2	Source IP Address
Device Custom IPv6 Address 3	Destination IP Address
Device Custom Number 1	ATTACK_COUNT

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	VLAN_ID
Device Custom Number 3	DESTINATION_CRITICALITY
Device Custom String 1	ALERT_TYPE
Device Custom String 2	ALERT_ID
Device Custom String 3	ATTACK_CONFIDENCE
Device Custom String 4	TARGET_OS
Device Custom String 5	DETECTION_MECHANISM
Device Custom String 6	DIRECTION
Device Event Category	ATTACK_SIGNATURE
Device Event Class ID	ATTACK_ID
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	ATTACK_SEVERITY
Device Vendor	'McAfee'
deviceAction	CALLBACK_ACTIVITY
eventOutcome	RESULT_STATUS
fileHash	MALWARE_MD5_HASH
fileName	MALWARE_VIRUS_NAME
filePermission	MALWARE_CONFIDENCE
fileSize	MALWARE_FILE_LENGTH
fileType	MALWARE_FILE_TYPE
Name	ATTACK_NAME
oldFileName	MALWARE_FILE_NAME
reason	LAYER_7_DATA(HTTP Return Code)
requestClientApplication	LAYER_7_DATA(HTTP User-Agent)
requestContext	LAYER_7_DATA(HTTP Response Content Type)
requestMethod	LAYER_7_DATA(HTTP Request Method)
requestUrl	LAYER_7_DATA(HTTP URI)
Source Address	SOURCE_IP
Source Host Name	SOURCE_NAME
Source NT Domain	ADMIN_DOMAIN
Source Port	SOURCE_PORT

Troubleshooting

When using the SmartConnector for Syslog Pipe, how can I check whether the log host is receiving messages from Network Security Manager and writing them to the pipe?

To verify the log host is receiving messages and writing them to the pipe:

- 1 Make sure no other process is listening on the pipe on the log host.

- 2 Start listing on the pipe:

```
cat /path/to/pipe
```

- 3 Make sure that Network Security Manager is generating events.

If everything is correctly configured, a message should now appear on the terminal where step 2 was performed.

Make sure that the cat process is killed before starting the connector, as only one process can read from the pipe.