Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.3.0

SmartConnector for McAfee Network Security Manager Syslog

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

SmartConnector for McAfee Network Security Manager Syslog

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.

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.

To enter text in the Message field:

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

   ```
   |$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_
   ATTACK_NAME$"|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_
   ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ATTACK_
   COUNT$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_
   INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_SOURCE_
   NAME$|$IV_VLAN_ID$|$IV_DESTINATION_CRITICALITY$|$IV_
   TARGET_IP$|$IV_TARGET_NAME$|$IV_TARGET_PORT$|$IV_TARGET_
   OS$|$IV_DETECTION_MECHANISM$|$IV_DIRECTION$|$MALWARE_
   CONFIDENCE$|$MALARE_FILE_LENGTH$|$MALWARE_FILE_MDS_
   HASH$|$MALWARE_VIRUS_NAME$|$IV_PROTOCOL$|$IV_RESULT_
   STATUS$|$MALWARE_FILE_TYPE$|$MALWARE_FILE_NAME$|$LAYER_7_
   DATA$|$CC_DOMAIN$|$CALLBACK_ACTIVITY$|
   ```

   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.

Configuring the Syslog SmartConnectors

The type of 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 SmartConnector for Syslog Daemon, add the following statement in the `rsyslog.conf` file to forward Oracle Audit events so that Syslog Daemon will start receiving events: `*.* @@(remote/local-host-IP):514`

Sample example: `local1.warning @@10.0.0.1:514`

You can either use *.* to read all Syslog events or you can filter specific events by replacing regex with the specific event name. For example: `*.* @@(remote/local-host-IP):514` and `local1.warning @@10.0.0.1:514`

Use @@ to send events over a TCP connection and use @ to send events over an UDP connection.

If you are running SmartConnector for Syslog Daemon on the same machine as the Oracle server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

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. Therefore, you must do additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.**

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.

Installing the SmartConnector

The following sections provide instructions for installing and configuring the McAfee Network Security Manager Syslog SmartConnector.

Installing Syslog

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 listens on port 514 (configurable) for UDP syslog events by default. You can configure the port number or use the TCP protocol manually. The Syslog Pipe and Syslog File connectors read events from a system pipe and file, respectively. You can select the appropriate connector as per the Syslog infrastructure setup.

Preparing to Install Connector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform* guide, available on ArcSight Documentation.

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 from step 3.

Before installing the SmartConnector, ensure that you have the following:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the McAfee Network Security Manager Syslog Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the McAfee Network Security Manager Syslog Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.

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

3. Specify the relevant Global Parameters, when prompted.
4. From the **Type** drop-down list, select **Syslog Daemon** or **Syslog File** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Connector	Parameter	Description
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

Connector	Parameter	Description
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.

Connector	Parameter	Description
	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'.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. For more information about the ArcSight data fields, refer to *ArcSight Console User's Guide* .

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
Device Custom IPv6 Address 2	Source IP Address
Device Custom IPv6 Address 3	Destination IP Address
Device Custom Number 1	ATTACK_COUNT
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

ArcSight ESM Field	Device-Specific Field
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	ATTACK_SEVERITY
Device Vendor	'McAfee'
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
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.
please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receivee events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for McAfee Network Security Manager Syslog (Micro Focus Security ArcSight Connectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!