



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for McAfee Email Gateway
Syslog

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for McAfee Email Gateway Syslog

November 30, 2016

Copyright © 2005 – 2016 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://www.protect724.hpe.com/docs/DOC-13026>.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Removed "legacy" and reference to vendor's Common Event Format version.
02/15/2016	Updated link to Customer Alliance site. Marked this connector as legacy; for future version support, use the vendor's Common Event Format version.
05/15/2015	Added information regarding version support with CEF Certified connector. Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
11/15/2012	Added mapping for Device Host Name.
05/15/2012	Added new installation procedure.
02/15/2011	Updated agent severity, device product, and device vendor field mappings.

Contents

Product Overview.....	4
Configuration.....	4
Configuring Email Gateway to Send Syslog Events.....	4
Configure the Syslog SmartConnectors.....	4
The Syslog Daemon SmartConnector.....	5
The Syslog Pipe and File SmartConnectors	5
Configure the Syslog Pipe or File SmartConnector.....	5
Install the SmartConnector.....	6
Syslog Installation	6
Prepare to Install Connector	7
Install Core Software.....	7
Set Global Parameters (optional).....	8
Select Connector and Add Parameter Information.....	8
Select a Destination	9
Complete Installation and Configuration	10
Run the SmartConnector	10
Device Event Mapping to ArcSight Fields	11
McAfee Email Gateway Mappings to ArcSight ESM Fields.....	11
Action Codes and Process IDs	11
Action Codes.....	11
Process IDs.....	12

SmartConnector for McAfee Email Gateway Syslog

This guide provides information for installing the SmartConnector for McAfee Email Gateway Syslog (formerly Secure Computing IronMail Syslog) and configuring the device for event collection. Email Gateway Security versions 4.5, 5.0, 6.1, 6.5, and 6.7 are supported.

Product Overview

McAfee Email Gateway combines the five critical email security components of spam and fraud prevention, virus and worm protection, policy and content compliance, email privacy, and secure email gateway capabilities into a single platform. Designed to secure the gateway by controlling all incoming and outgoing email messages, Email Gateway addresses a full spectrum of unwanted email activity and intrusion-based threats.

Configuration

Configuring Email Gateway to Send Syslog Events

Email Gateway can generate and transmit the same data it generates for its Summary Log in syslog format for integration with a network syslog logging system. In addition to configuring Email Gateway to communicate with the syslog server, the syslog server must be configured to recognize Email Gateway's data.

Email Gateway uses the syslog User facility and Info level for the data it sends; therefore, a `user.info` variable must be created for `/var/log/ironmailname_syslog` on the receiving host.



If syslog is turned on, no information will be available on the Email Gateway unit in the Summary log.

Configure Email Gateway's syslog output using these four user input fields:

- **Send Summary Logs to SysLog Server:** Select the Send Summary Logs to SysLog Server check box to enable Email Gateway's syslog output.
- **Protocol Type:** Select the network protocol to be used by the syslog server, TCP or UDP. (Ordinarily, syslog uses UDP.).
- **Syslog Host:** Enter the IP address or host name of the syslog server. Note that a syslog server configuration determines whether an IP address or host name should be used here. If the Server is configured for IP address and its host name is entered here, Email Gateway may not be able to deliver its data to the server.
- **Syslog Port:** Enter the port number Email Gateway should use to connect to the syslog server.

Click **Submit** to save user input.

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.

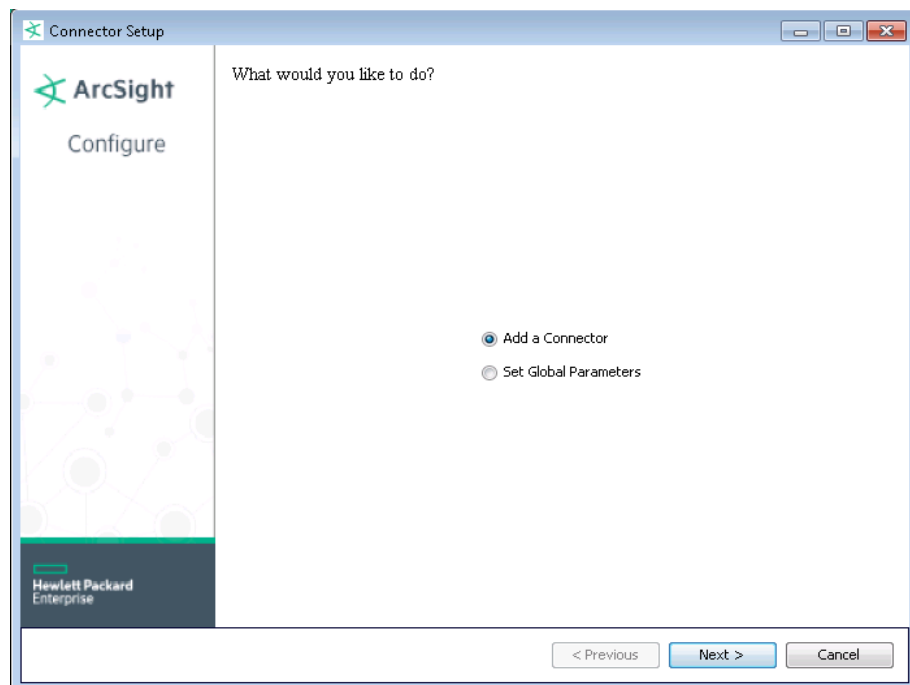


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' 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 'Disable'.
Set Remote Management	Set to 'Enable' 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 'Disable'.
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	If 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. When both values are present, the initial setting is IPv4.

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 the "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, Syslog File, or Syslog 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: /var/tmp/syspipe
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: \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: <code>filename 'yyyy-MM-dd' .log;</code> 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: <code>filename '%d,1,99,true' .log;</code> 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 Email Gateway Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	errorMessage
Agent (Connector) Severity	100, 104, 105, 106, 107, 112 = Medium; 101,109,114,102,103,108,110,111,113,115,118 = Low
Destination DNS Domain	Destination DNS domain
Destination User Name	Destination user name
Device Action	ActionCode
Device Custom Number 1	RuleID
Device Custom Number 2	ErrorCode
Device Custom String 1	Both (ProcessID, ProcessReturnMessage)
Device Custom String 2	ActionDetails
Device Custom String 3	MatchedCondition
Device Custom String 4	Route Domain
Device Custom String 5	Route Host
Device Event Class ID	Both (ProcessID, ActionCode)
Device Host Name	One of (HostName, _SYSLOG_SENDER)
Device Process Name	processID
Device Product	'Email Gateway'
Device Receipt Time	Date, Time
Device Severity	ActionCode
Device Vendor	'McAfee'
Device Version	_DEVICE_VERSION
External ID	One of (MessageID1, MessageID)
Message	ProcessReturnInfo
Name	ProcessID
Source Address	Address
Source DNS Domain	Domain
Source Port	Port
Source User Name	Name

Action Codes and Process IDs

Action Codes

Action Code	Meaning
100	No action
101	Multiple actions
102	Drop message
103	Drop part

Action Code	Meaning
104	Forward as attachment
105	Forward
106	Copy as attachment
107	Copy
108	Quarantine
109	Log
110	Rewrite Subject
111	Re-route
112	Encrypt
113	Change part
114	Add header
115	Retry message
118	Remote quarantine

Process IDs

Process ID	Meaning
10	*
21	SMTPPI Service
22	SMTPIS Service
30	SMTPO Service
41	POP3 Service
42	POP3S Service
51	IMAP4 Service
52	IMAP4S Service
90	Apache Web Server
91	WebMailProtection
100	Tomcat (JavaScript Interpreter)
110	Admin (internal service that runs scripts)
120	Alert Manager
130	Cleanup Schedule
140	Health Monitor
150	Report Generator
151	Policy Configuration
160	Schedule (running periodic scheduled tasks)
161	Schedule for FTP
163	Archive
164	LDAP Synchronization
165	Nightly Schedule (running nightly scheduled tasks)
166	Statistics Collector
170	Optimize
180	Mail-IPS
190	Anomaly Detection Engine
200	Anti-Virus Queue

Process ID	Meaning
210	Content Filtering Queue
220	Envelope Analysis Queue
230	Rip Queue
240	Join Queue
250	Quarantine Queue
260	Spam Queue
270	SSH Command Line Interface
280	SSH Maintenance (monitoring the SSH port)
290	Secure Web Delivery Queue
300	Audit
330	Bootport
340	Verity File Translator Queue
360	Corporate Compliance
900	Check Tool
910	Updater
