
Micro Focus Security

ArcSight Micro Focus Security

Software Version: 8.2.1

SmartConnector for Linux Audit Syslog

Document Release Date: August 2021

Software Release Date: August 2021



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 Linux Audit Syslog	5
Product Overview	6
Installing the SmartConnector	7
Installing Syslog	7
Preparing to Install Connector	7
Installing and Configuring the SmartConnector by Using the Wizard	8
Configuration	12
Configuring Event Merging	12
Configure the Syslog SmartConnectors	13
The Syslog Daemon SmartConnector	13
The Syslog Pipe and File SmartConnectors	14
Configuring the Syslog Pipe or File SmartConnector	14
Device Event Mapping to ArcSight Fields	16
Mappings to ArcSight Fields	16
Send Documentation Feedback	19

SmartConnector for Linux Audit Syslog

This guide provides information for installing the SmartConnector for Linux Audit Syslog and configuring the device for event collection.

Product Overview

The Linux auditd daemon can help you detect violations of your security policies. It detects violations of security policy but does not enforce it. Rather, it is similar to network-based intrusion detection systems and host-based intrusion detection systems. Because the audit daemon is part of the Linux kernel, it is included in most major Linux distributions by default.

Supported versions for Linux auditd to collect events from Red Hat Linux Enterprise (RHEL) are:

6.4, 6.5, 6.7, 7.1, 7.2, 7.4, 7.5, 7.6, 8.1, 8.2, and 8.3

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	<p>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).</p> <p>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.</p> <ul style="list-style-type: none"> 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'.

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](#).

Configuration

For complete information about the Linux auditd daemon, see the man pages for auditd, auditd.conf, and auditctl. You can access these man pages by running the `man auditd` or `man auditctl` commands, from the command line of your Linux system.

Linux auditd does not log to syslog by default. To enable syslog logging, edit `# /etc/audit/plugins.d/syslog.conf` and change the line `active = no` to `active = yes`.

- `auditctl` is responsible for controlling the status and some basic system parameters of auditd. Using audit rules, `auditctl` controls which components of your system are subjected to the audit and to what extent they are audited. Audit rules can be passed to auditd on the `auditctl` command line as well as by composing a rule set and instructing auditd to process this file.
- auditd has built-in functions to watch access attempts to files without needing to monitor the applicable system calls. Administrators can add rules by amending the provided configuration files or at run time using the command line. The default location for the audit daemon rules in `/etc/auditd/audit.rules`.

Before you can start generating audit logs and processing them, configure the audit daemon itself. Configure how it is started in the `/etc/sysconfig/auditd` configuration file and configure how the audit system functions once the daemon has been started in `/etc/auditd.conf`.

Configuring Event Merging

The Linux Audit system provides a way to track security-relevant information on the system. Based on pre-configured rules, Linux Audit generates log entries to record as much information as possible about the events happening on your system. These events often contains multiple sub-events that can span multiple lines. The event merging feature aggregates the related sub-events into one large event with a concatenated long message.

To enable event merging:

1. Set up Linux Audit connector. See [Installing the SmartConnector](#).
2. Edit the `syslog.subagent.parsers` parameter in the `agent.properties` file (located in the `$ARCSIGHT_HOME/current/user/agent` folder) as follows:

```
agents[0].syslog.subagent.parsers=linux_auditd_syslog\:merge
```

3. [Run the SmartConnector.](#)

Configure 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.

Configuring 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.

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.

Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	proto
Destination Address	One of (daddr,laddr,dst)
Destination Mac Address	dmac
Destination NT Domain	One of (new-seuser,acct)
Destination NT Domain	One of (new-seuser,acct)
Destination Port	One of (dest, dport, lport)
Destination Process ID	One of (egid,opid)
Destination Process Name	One of (exe, comm, cmd ,ocomm)
Destination Service Name	One of (com, ocomm, grantors)
Destination User ID	One of (auid, new auid, old auid, old-auid, oid)
Destination User Name	One of (new-seuder, acct, OUID)
Destination User Privilege	new-role
Device Action	op
Device Custom IPv6 Address 2	src
Device Custom IPv6 Address 3	dst
Device Custom Number 1	calipso_doi
Device Custom Number 2	One of (oses,ses,new ses, oldses,old-ses)
Device Custom Number 3	uid
Device Custom String 1	One of (dev, old, nsec)
Device Custom String 2	One of (key, calipso_type, new, sec)
Device Custom String 3	One of (success, res)

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	One of(syscall,SYSCALL,op)
Device Custom String 5	subj
Device Custom String 6	One of (terminal, tty)
Device Event Class ID	One of (res, type, both (type, res))
Device Host Name	node
Device Inbound Interface	inif
Device Outbound Interface	outif
Device Process Name	'auditd'
Device Product	'auditd'
Device Receipt Time	timestamp
Device Vendor	'Unix'
Device Version	One of (ver, kernel)
Event Destination	ProcessId egid
Event Outcome	One of (result, res, __simpleMap(success,"yes=Successful","no=Failed"))
Event Reason	One of (reason, cause)
External ID	callid
File Hash	One of (proctitle, data, cmd, fp)
File ID	One of (watch_inode, cap_fver, sw)
File Name	One of (path, name, watch, obj)
File Path	One of (cwd, root_dir)
File Permission	One of (mode, perm)
File Size	ksize
Flex String2	One of (ppid, direction)
Message	msg
Name	One of (res, type, both (res, type), 'Linux Audit Message')
Old File Hash	mac
Old File ID	All of (a0, a1, a2, ...)
Old File Name	cipher
Old File Path	cmdline
Request URL	pfs

ArcSight ESM Field	Device-Specific Field
Source Address	One of (addr,saddr,src)
Source Host Name	hostname
Source Mac Address	smac
Source Port	One of (sport, rport)
Source Process ID	One of (pid, Spid, spid)
Source User ID	One of (saudit, uid, oaudit,AUID)
Source User Name	One of (user, old-seuser, EUID,OAUID)
Source User Privileges	One of (old-role, EGID)



Note: The connector will not receive events if MySQL JDBC driver 5.1.38 was used when you configured it. To fix this issue, apply MySQL JDBC driver 5.0.8.

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 Linux Audit Syslog (Micro Focus Security ArcSight Connectors 8.2.1)

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!