



Micro Focus Security ArcSight Connectors

SmartConnector for Linux Audit File

Configuration Guide

September 17, 2020

Configuration Guide

SmartConnector for Linux Audit File

September 17, 2020

Copyright © 2009 – 2017; 2019; 2020 Micro Focus or one of its affiliates.

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

<https://www.microfocus.com>.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs>

Revision History

Date	Description
09/17/2020	Added support for RHEL 8.1 Linux Audit file events. Added and updated Linux Audit mappings.
05/17/2019	Added and updated Mappings to ArcSight Fields.
10/17/2017	Added encryption parameters to Global Parameters.
10/17/2017	Added encryption parameters to Global Parameters.
09/15/2017	Added support for RHEL version 6.7 as a source device.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Added support for RHEL version 7.2 and for event merging. Added a new mapping item.
11/17/2015	Added support for RHEL version 7.1. Removed support for RHEL versions 5.7, 6.1, and 6.2.
08/15/2014	Added support for Red Hat Linux versions 6.4 and 6.5.
09/30/2013	Updated mappings.
09/28/2012	Updated mappings for Source User Name and Destination User Name.
05/15/2012	Added new installation procedure.
02/15/2012	Added support for Red Hat Linux 6.0 and 6.1.
02/11/2010	Added support for FIPS Suite B and CEF File transport. Added support for Red Hat Linux Enterprise 5.0; updated mappings for Name field.
11/11/2009	First edition of this Configuration Guide.

SmartConnector for Linux Audit File

This guide provides information for installing the SmartConnector for Linux Audit File and configuring the device for event collection. Linux auditd is supported for pulling events from Red Hat Linux 6.4, 6.5, 6.7, 7.1, 7.2, 7.4, 7.5, and 8.1.

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.

Configuration

For complete information about the Linux auditd daemon, see the man pages for [auditd](#), [auditd.conf](#), and [auditctl](#). You can access these manual pages by running `man auditd` or `man auditctl`, for example, from the command line of your Linux system.

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

- [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/audit/audit.rules`.
- [auditd](#) adds events to the audit log file as they occur. By default, the system stores audit logs in `/var/log/audit/`.

Configure 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 contain 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 according to the instructions in "Install the SmartConnector".
- 2 Edit the `fcv.version` parameter in the `agent.properties` file (located in the `$ARCSIGHT_HOME/current/user/agent` folder) as follows:
`agents[0].fcv.version=1`
- 3 Start the connector as described in "Run the SmartConnector".

Install the SmartConnector

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



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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

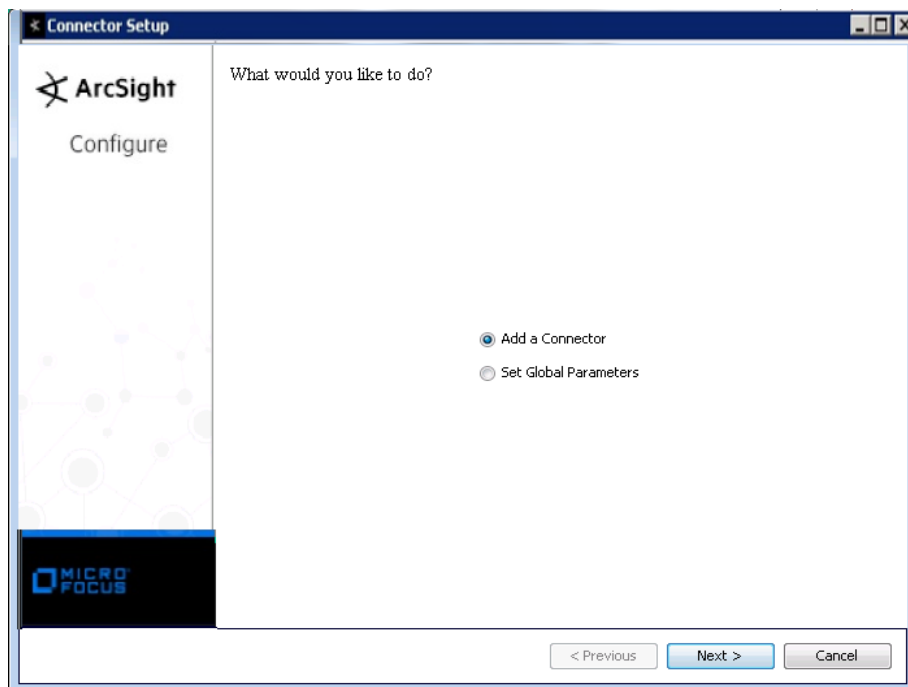
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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.

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'.

Parameter	Setting
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.

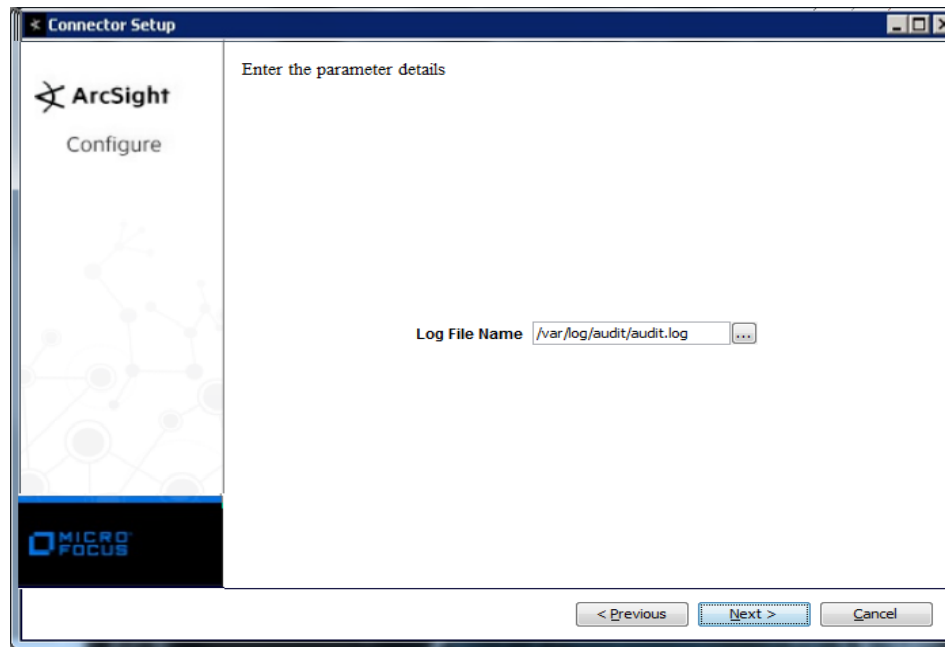
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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 **Linux Audit File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log File Name	Enter the path to and name of the log file. The default value is '/var/log/audit/audit.log'

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.

Linux Audit 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 Port	One of (dest, dport, lport)
Destination Process ID	egid
Destination Process Name	One of (exe,comm,cmd)
Destination Service Name	One of (comm,grantors)
Destination User ID	One of (auid, new auid, old auid)
Destination User Name	One of (new-seuser, acct)
Destination User Privilege	new-role
Device Action	op
Device Custom Number 1	calipso_doi
Device Custom Number 2	One of (ses,new ses,old ses,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)
Device Custom String 4	One of (syscall,SYSCALL,op)
Device Custom String 5	subj
Device Custom String 6	One of (terminal, tty)
Device Event Category	type
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, selected-context)
File Path	cwd One of (cwd,root_dir)
File Permission	One of (mode, perm)
File Size	ksize
Flex String 2	One of (ppid,direction)
Message	msg

ArcSight ESM Field	Device-Specific Field
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
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 (suid, uid, AUID)
Source User Name	One of (user, old-seuser, EUID)
Source User Privileges	One of (old-role, EGID)
