
Micro Focus Security

ArcSight Micro Focus Security

Software Version: 8.2.1

SmartConnector for UNIX Login and Logout

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.

Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, see [ArcSight SmartConnectors Documentation](#).

Document Changes

| Date | Description |
|------------|---|
| 07/09/2021 | Added support for RHEL 8.3 platform and RHEL 8.3 events. |
| 09/17/2020 | Added support for Unix Login/Logout with RHEL 8.1 events. |
| 05/17/2019 | This connector supports RHEL 7.6 events. |
| 07/18/2018 | Run the SmartConnector section was updated. |
| 10/17/2017 | Added encryption parameters to Global Parameters. |
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 08/30/2016 | Added reference to SmartConnector for IBM AIX Audit Syslog connector for AIX login/logout message support. |
| 05/16/2016 | Added support for RHEL 7.2 platform. |
| 03/31/2016 | Added support for Oracle Solaris 11 SPARC and x86 64-bit platforms. |
| 11/17/2015 | Added support for RHEL 7.1 platform. Removed support for AIX 5.3; RHEL 5.4 AS 32-bit and 64-bit; and Solaris 10 32-bit. |
| 05/15/2012 | Updated installation procedure. |

Contents

| | |
|---|----|
| Revision History | 4 |
| SmartConnector for UNIX Login and Logout | 6 |
| Product Overview | 7 |
| Installing the SmartConnector | 8 |
| Preparing to Install Connector | 8 |
| Installing and Configuring the SmartConnector by Using the Wizard | 8 |
| Device Event Mapping to ArcSight Fields | 10 |
| UNIX Login and Logout Mappings | 10 |
| Send Documentation Feedback | 11 |

SmartConnector for UNIX Login and Logout

This guide provides information for installing the SmartConnector for UNIX Login and Logout and provides mappings to ArcSight ESM events. All versions of UNIX Login and Logout messages are supported.

Product Overview

This SmartConnector provides Login and Logout security. No connector-specific configuration is required.

Supported platforms:

- Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.7, 7.1, 7.2, 7.4, 7.5, 7.6, 8.1, 8.2, and 8.3
- Oracle Solaris 10 x86 64-bit
- Oracle Solaris 11 SPARC and x86 64-bit
- SUSE Linux 11 Enterprise Server 64-bit



Note: Login and logout messages are supported for the AIX platform with the SmartConnector for IBM AIX Audit Syslog.

Installing the SmartConnector

The following sections provide instructions for installing and configuring the UNIX Login and Logout SmartConnector.

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 UNIX Login and Logout Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the UNIX Login and Logout 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 **UNIX Login/Logout** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

| Parameter | Description |
|------------------|---|
| Custom Host Name | Enter the name of the host for which events are being collected. This host name is used to map the given value to the Device Host Name field and not for collecting logs from the specified host. |

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. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

UNIX Login and Logout Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------|-----------------------|
| Destination Host Name | Host |
| Destination User Name | User |
| Device Custom String 1 | Line (Device Name) |
| Device Event Class ID | Action |
| Device Host Name | _CUSTOM_HOST_NAME |
| Device Product | 'Unix' |
| Device Receipt Time | Date |
| Device Vendor | 'Unix' |
| Name | Action |
| Source Host Name | Host |



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 UNIX Login and Logout (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!