
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.4.1

SmartConnector Release Notes

Document Release Date: March 2023

Software Release Date: March 2023



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2010 - 2022 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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

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://www.microfocus.com/documentation/arcsight/

Contents

- Release Highlights 5

- What's New 6
 - Cloud Updates 6
 - Security Updates 6
 - Version Updates 7
 - Platform Support 7
 - SmartConnector Enhancements 8
 - Software Fixes 8
 - Event Categorization Updates 11

- Updated Support Policy 12

- Installing SmartConnectors 13
 - System Requirements 13
 - Downloading the SmartConnector 8.4.1 Installation Packages 13
 - Upgrading to 8.4.1 14
 - Deleting Older Vulnerable Libraries after Upgrading a Connector 15

- Known Issues 18

- Connector End-of-Life Notices 25
 - SmartConnector End of Support Announcements 25
 - SmartConnectors No Longer Supported 26

- Send Documentation Feedback 27

Release Highlights

The SmartConnector 8.4.1 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Support for the McAfee Web Gateway 9 events
- Support for Oracle 21C
- Support for AWS Linux 2
- Support for Infoblox NIOS 8.3
- Support for Symantec Endpoint Protection Syslog logs for version 14.3
- Support for Cisco Ironport 14.0.0 modules
- Support for Microsoft server 2019 support for Multiple Instance Audit DB
- Support for Microsoft Windows Event log – Native (WiNC): Microsoft SQL Server Audit Application
- Upgrade of Tomcat version to 9.0.69
- Deprecation of the **Authorization Code** and **Password** grant types for Okta SmartConnector

For detailed information, see the ["What's New" on the next page](#) section of this guide.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help and prioritize and plan new features for next release.

What's New

SmartConnector 8.4.1 incorporates the following SmartConnector 8.4 patch releases, and content and categorization updates:

- [SmartConnector 8.4 Patch 1](#)
- [February R1 and R2 Event Content-Categorization updates 2023](#)
- [January R1 and R2 Event Content-Categorization updates 2023](#)

Cloud Updates

Application Module	Description
Amazon S3	<p>Added support for the amazons3.allowed.eventName parameter.</p> <p>The connector now successfully reads and parses the SQS messages with the eventName=ObjectCreated:Copy object.</p> <p>For more information, refer to the Additional Parameters section in Configuration Guide for Amazon S3 SmartConnector.</p>

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u352.</p> <p>The following CVEs (Common Vulnerabilities and Exposures) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none">• CVE-2022-21626• CVE-2022-21628• CVE-2022-21619• CVE-2022-21624
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.69

Version Updates

Application Module Version Updates	Description
IBM DB2 Multiple Instance UDB Audit File	Added support for IBM DB2 Multiple Instance UDB Audit File for version 11.5.
Infoblox NIOS Syslog	Added support for Infoblox NIOS 8.3.
Microsoft SQL Server Multiple Instance Audit DB	Added Microsoft server 2019 support for Microsoft SQL Server Multiple Instance Audit DB.
Microsoft Windows Event log – Native (WiNC): Microsoft SQL Server Audit Application	Added Microsoft server 2019 support for Microsoft Windows Event log – Native (WiNC): Microsoft SQL Server Audit Application.
Oracle Audit DB	Added support for Oracle 21C.
Symantec Endpoint Protection Syslog	Added support for Symantec Endpoint Protection logs for version 14.3.
Cisco IronPort Email Security Appliance File Cisco IronPort Email Security Appliance Syslog	Added support for the following Cisco Ironport 14.0.0 modules: <ul style="list-style-type: none">• Audit Logs• Consolidated Event Logs
Microsoft Windows Event log – Native (WiNC): Windows Server 2022 – Microsoft ADFS	Added support for the following events: <ul style="list-style-type: none">• 100• 102• 103• 106• 249• 309• 342• 510

Platform Support

Application Module Platform Support	Description
All SmartConnectors	Added certified OS version support for Amazon Linux 2.

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors (Windows Installer)	The SmartConnector Installer is now Windows-signed and displays the publisher name as Micro Focus.
Okta Connector	<p>The Authorization Code and Password grant types have been deprecated in this release. Now, the grant type feature is offered only by using the API Token mechanism to authenticate requests to Okta APIs.</p> <p>For more information, see Configuration Guide for SmartConnector for Okta.</p>

Software Fixes

The following issues are fixed in the 8.4.1 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>After enabling the Device Time Auto-Correction, the connector throws IP Address Exception and breaks the event flow for events which do not include the Device Hostname and Device Address.</p> <p>Fix: The issue is fixed by creating a placeholder IP address without causing any breaks in the event flow.</p>
All SmartConnectors (File-based)	<p>The connector was throwing multiple as file not found exceptions if the destination was not available for a file-based destination(such as CEF or Avro). Also, the connector was not caching events that were not reaching the destination, and therefore must get cached.</p> <p>Fix: The issue is fixed by adding a flag to check if the connector destination is present or not. If not, it throws the system cannot find the specified path error and starts caching events to the agentdata folder. If the destination is present, it starts writing all the events to the destination.</p>
AWS Cloudtrail	<p>The end time in the ESM console was incorrect.</p> <p>Fix:The issue is fixed by correcting the Manager Receipt Time which must always be greater than the end time in the ESM console.</p>

Application Modules Software Fixes	Description
<p>Cisco IOS Syslog</p>	<p>The events for Cisco IOS were not being parsed.</p> <p>Fix: The following fixes have been implemented to handle the unparsed events:</p> <ul style="list-style-type: none"> • Added support for the following modules of Cisco IOS events: <ul style="list-style-type: none"> ◦ DOT1X-5-FAIL ◦ SSH-3-NO_MATCH ◦ IOSXE-3-PLATFORM ◦ SESSION_MGR-5-FAIL ◦ CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_RUN_STATE ◦ CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_DELETE_STATE ◦ CLIENT_ORCH_LOG-7-CLIENT_IP_UPDATED ◦ CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE ◦ CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN ◦ DMI-5-AUTH_PASSED ◦ CLIENT_EXCLUSION_SERVER-5-ADD_TO_EXCLUSIONLIST_REASON_DYNAMIC ◦ SYS-5-CONFIG_P ◦ IOSXE_SDWAN_CONFIG-5-MASTER_KEY_PRESENT • Regex was added to handle log events along with new module support.
<p>F5 BIG-IP Syslog</p>	<p>The F5 events of the F5 BIG-IP Syslog were not being parsed.</p> <p>Fix: Added new sub-messages to handle the unparsed events.</p> <p>The authentication logs from F5 BIG-IP Syslog were not being parsed.</p> <p>Fix: Added support to handle the unparsed authentication logs from F5 BIG-IP Syslog.</p>
<p>HPE Integrated Lights-Out Syslog</p>	<p>The GEN10 - ILO version 5 of HPE Integrated Lights-Out Syslog was not being parsed.</p> <p>Fix: Added support to handle the unparsed events of HPE ILO's GEN10 for version 5.</p> <p>The latest firmware events for ILO versions 4 and 5 of HPE Integrated Lights-Out Syslog were not being parsed.</p> <p>Fix: Added support to handle the latest firmware unparsed events of HPE ILO versions 4 and 5.</p>

Application Modules Software Fixes	Description
Juniper JUNOS Syslog	<p>The events for Juniper JUNOS Syslog were not being parsed.</p> <p>Fix: The base regex of JunOS SDsyslog parser file was changed to handle the unparsed events.</p>
Linux Audit Syslog	<p>The rsyslog logs of Linux Audit Syslog were not being parsed.</p> <p>Fix: The base regex of linux auditd parser file was changed to handle the unparsed events.</p> <p>The audit events of RHEL of Linux Audit Syslog were not being parsed.</p> <p>Fix: The base regex of linux auditd parser file was changed by adding support for audispd module of RHEL audit events.</p>
Load Balancer	<p>Errors were logged in the lb.out.wrapper.log log file after upgrading the bash version to 4.4.</p> <p>Fix: Added support for bash 4.4.</p>
McAfee Web Gateway Syslog	<p>Events were not being parsed for McAfee Web Gateway 9.</p> <p>Fix: Added support for the McAfee Web Gateway 9 events.</p>
Microsoft Azure Monitor Event HubConnector	<p>For all the Azure Event Hub logs of SignInLogs, the category outcome was set to value /attempt instead of success/failure.</p> <p>Fix: The issue is fixed by correcting the value of category outcome as success/ failure according to the resulttype value received from the logs of SignInLogs.</p> <p>The Function App was displaying a warning message after upgrading the connector.</p> <p>Fix: Now, the Function App version is upgraded from 2.x to 4.x. And the Always on property will be set to On after the connector has upgraded.</p> <p>For more information, see Upgrading the Connector, in <i>Microsoft Azure Monitor Event Hub Connector</i> configuration guide.</p>
Microsoft DNS DGA Trace Log Multiple Server File	<p>The events for regional date format containing space were not being parsed for DNS DGA Trace Log Multiple Server File.</p> <p>Fix: Added framework code to handle the parsing issue of the events.</p>
Microsoft Office 365 Management Activity	<p>In the Microsoft Office 365 connector, the sourceUserId field was not mapped correctly.</p> <p>Fix: The issue is fixed by changing the mapping value for the field SourceUserId to deviceCustomString. This change is reflected in both, the parser file and in the document of the Microsoft Office 365 connector.</p>

Application Modules Software Fixes	Description
Microsoft Windows Event Log - Native	<p>The Microsoft Windows Event Log-Native connector is unable to receive events after upgrading the version to 8.4.0.</p> <p>Fix: The issue is fixed by generating a new set of certificates as follows for internal communication:</p> <ul style="list-style-type: none">• <code>winc_management.p12</code>• <code>winc_management.cert</code> <p>For more information related to the workaround, see Troubleshooting section, in <i>Microsoft Windows Event Log-Native</i> configuration guide.</p>
UNIX OS Syslog	<p>The CentOS and RHEL device events of Unix OS Syslog were not being parsed.</p> <p>Fix: Added support for the following modules of CentOS and RHEL device audit events:</p> <ul style="list-style-type: none">• <code>python3.6</code>• <code>Container_ImageInventory</code>• <code>dockerd</code>• <code>rsyslogd</code>• <code>sudo</code> <p>The Unix events of the Unix OS Syslog were not being parsed.</p> <p>Fix: Added new sub-messages to handle the unparsed events.</p>
VMware ESXi Server Syslog	<p>The events for VMware ESXi were not being parsed.</p> <p>Fix: The following fixes have been implemented to handle the unparsed events:</p> <ul style="list-style-type: none">• New sub-messages were added to handle the VMware 6.5 Server events.• Existing sub-message was edited to handle the issue.

Event Categorization Updates

For more information, see [Release Notes for ArcSight Content AUP -Categorization Updates 2023](#).

Updated Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).


Downloading the SmartConnector 8.4.1 Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.1.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.1.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.1.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.1.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.1.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.1.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.1.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.1.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.1.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.1.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

ArcSight-8.4.1.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.1.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.1.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-8.4.1.xxxx.0-MispModelConnector-Linux64.bin	This is the installer file for MISP Connector support for Linux.
ArcSight-8.4.1.xxxx.0-MispModelConnector-Win64.exe	This is the installer file for MISP Connector support for Windows.
ArcSight-AWS-CloudWatch-Connector-8.4.1.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.1.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.1.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.1.xxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.1.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.1.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for Galaxy Threat Acceleration Program Connector support for Linux.
ArcSight-8.4.1.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for Galaxy Threat Acceleration Program Connector support for Windows.

Upgrading to 8.4.1

 **Important:** If you use any of the SmartConnectors listed in the [Software Fixes](#) section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

For information and instructions, see [Verifying Micro Focus Signatures with gpg or rpm](#).



Note: If a Parser Override was provided, determine whether the Bug or Feature Request number is included in the Fixed or Enhancements section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your environment PROD (production)

Upgrading SmartConnector to 8.4.1

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to 8.4.1

For information about upgrading Load Balancer to 8.4.1, see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command: `cd Xxxxx/lib/agent`
 3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
 4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
 5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
 6. Run the following command: `cd Xxxxx/lib/agent/axis`
 7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to \$Arcsight_Home.
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Open the Xxxxx\lib\agent folder.
3. Search for **log4j** and delete all the entries.
4. Open the Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\ folder.
5. Search for **log4j** and delete all the entries.
6. Open the Xxxxx\lib\agent\axis folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to \$Arcsight_Home.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnectors	<p>SmartConnector or Collector remote connections fail due to low entropy</p> <p>All SmartConnectors or Collectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector or Collector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none">1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code>2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code>3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code>4. Start the rngd package as root user: <code>service rngd start</code>5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code>6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code>7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code> <p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none">1. <code>yum install -y unzip</code>2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>

<p>All SmartConnectors installed on Solaris</p>	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute ./runagentsetup. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service. <p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cefkafka.extra.prod.props '</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <connector_install_location> \counterintelligence location and the connector runs out of memory, add the following property to agent.properties as a workaround: <code>parser.operation.result.cache.enabled=false</code></p> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents [0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the WiNC connector in the container.</p>
<p>All File SmartConnectors</p>	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ct!r+c</pre>

<p>Galaxy Threat Acceleration Program Connector</p>	<p>Possibility of Time Difference While Comparing ESM Lists Against Events from the MISP Instance</p> <p>While comparing the <code>firstDetectTime</code> and <code>lastDetectTime</code> of ESM Threat Intelligence Platform lists against the event and attribute dates from the MISP Instance, you might notice time difference. This is because of the difference in timezone where the MISP Instance is hosted.</p> <p>Workaround:</p> <p>None.</p>
<p>Malware Information Sharing Platform Model Import Connector</p>	<p>When running the MISP connector in FIPS mode, the following error is displayed on the console:</p> <pre>java.security.KeyManagementException: FIPS mode: only SunJSSE TrustManagers may be used at sun.security.ssl.SSLContextImpl.chooseTrustManager(SSLContextImpl.java:120) at sun.security.ssl.SSLContextImpl.engineInit(SSLContextImpl.java:83) at javax.net.ssl.SSLContext.init(SSLContext.java:282) at org.apache.http.conn.ssl.SSLContextBuilder.build(SSLContextBuilder.java:164) at org.apache.http.conn.ssl.SSLSocketFactory.<init>(SSLSocketFactory.java:303) at com.arcsight.agent.dm.f.b.q(b.java:581) at com.arcsight.agent.dm.f.b.r(b.java:555) at com.arcsight.agent.dm.f.b.d(b.java:173) at com.arcsight.agent.Agent.a(Agent.java:674) at com.arcsight.agent.Agent.a(Agent.java:1171) at com.arcsight.agent.Agent.e(Agent.java:948) at com.arcsight.agent.Agent.main(Agent.java:1960)</pre> <p>Workaround:</p> <p>This message can be ignored. It does not affect the functionality.</p>

<p>Google Cloud SmartConnector</p>	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check youriat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--	---

ArcMC Managed
SmartConnectors

SmartConnectors cannot be bulk-upgraded on a Linux server

Workaround:

Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the `rng-tools` on the corresponding Linux OS.

Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.

To install and configure the `rng-tools` package after a fresh install, follow the steps mentioned for [SmartConnector or Collector remote connections fail due to low entropy](#).

One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4

This issue might occur in other ArcMC versions.

Workaround:

Pre-requisites for instant connector or collector deployment:

- Python2
- Libselinux-python

Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.

To manually install Python:

Apply these changes to the target Linux host (the VM where the connector or collector will be deployed):

1. Install python2 by the following command:

```
sudo yum install -y python2
```
2. Create a symlink by the following command:

```
sudo ln -s /usr/bin/python2 /usr/bin/python
```
3. Install the libselinux-python package by the following command:

```
sudo yum install -y libselinux-python
```



Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from:

http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm

IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file: "E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually: \$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</p>
Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. it has the following issues:</p> <ul style="list-style-type: none">• Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).• Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Windows Native Connector (WiNC) SmartConnector. For more information, see the Technical Note on WinRM-related Issues.</p>

<p>Microsoft Windows Event log - Native (WiNC)</p>	<p>WiNC SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT_HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents[0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
<p>Microsoft Azure Monitor Event Hub</p>	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.
<p>Load Balancer</p>	<p>Load Balancer arc_conn1b service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_conn1b service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_conn1b service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:</p> <ol style="list-style-type: none"> 1. After you install Load Balancer as a service, before you upgrade, stop the arc_conn1b service by using the following command: <pre># /etc/init.d/arc_conn1b stop</pre> <p>or</p> <pre>service arc_conn1b stop</pre> 2. After Load Balancer is successfully upgraded, start the arc_conn1b service by using the following command: <pre># /etc/init.d/arc_conn1b start</pre> <p>or</p> <pre>service arc_conn1b start</pre>

Connector End-of-Life Notices

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	11/30/2025	The Connectors in Transformation Hub (CTH) and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector 8.4.0 release.
Model Import Connector for MISP (Malware Information Sharing Platform)	02/2022	The MISP Connector is supported for the ArcSight Connector 8.4.1 release and has been deprecated as of 8.3. MISP Connector will be removed in an upcoming release, by June 2023, and will have limited support for customers already using these components until the end of support date for the ArcSight Connector 8.4.1 release. Customers using MISP today are strongly advised to migrate to the Galaxy Threat Acceleration Program (GTAP), which includes support for MISP and premium intelligence feeds. For more information, see the Configuration Guide for Galaxy Threat Acceleration Program Connector .

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - Galaxy Threat Acceleration Program Connector, which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/14/2020	End of support by vendor.
Windows Server 2008 R2	01/14/2020	End of support by vendor.
Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/22/2019	Lack of customer demand.
Oracle Audit DB version 9	8/21/2019	End of support by vendor.
All 32-bit SmartConnectors	4/28/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/21/2018	End of support by vendor.
Solaris 10 Premier support	01/31/2018	End of support by vendor.

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 Release Notes (SmartConnectors 8.4.1)

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!