



ArcSight SmartConnectors

Software Version: 8.4.3

SmartConnector Release Notes

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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>

Contents

- Release Highlights 4

- What's New 5
 - New SmartConnectors and Modules 6
 - Cloud Updates 7
 - Security Updates 8
 - Version Updates 8
 - Platform Support 8
 - SmartConnector Enhancements 9
 - Software Fixes 9
 - Event Categorization Updates 11

- SmartConnector Parser Support Policy 13

- Installing SmartConnectors 14
 - System Requirements 14
 - Downloading the SmartConnector 8.4.3 Installation Packages 14

- Upgrading SmartConnectors 16
 - Upgrading to 8.4.3 16
 - Deleting Older Vulnerable Libraries after Upgrading a Connector 16

- Known Issues 19

- Connector End-of-Life Notices 27
 - SmartConnector End of Support Announcements 27
 - SmartConnectors No Longer Supported 27

- Send Documentation Feedback 29

Release Highlights

The SmartConnector 8.4.3 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Created a new [SmartConnector for Mulesoft Audit](#)
- Created a new [SmartConnector for Terraform Cloud](#)
- Created a new [SmartConnector for Trellix ePolicy Orchestrator DB](#)
- Added Amazon Security Lake log source for the Amazon S3 SmartConnector
- Certified RHEL versions 8.8, 9.0, 9.1, and 9.2 as installation platforms
- Certified Rocky Linux 8.8 as installation platform
- Certified F5 BIG-IP Syslog version 14.1.5
- Certified Tenable Nessus .nessus File version 10.4.0
- Certified Fortinet Fortigate Syslog version 6.2.0
- Certified Cisco ISE Syslog version 3.1
- Certified IBM eServer iSeries Audit Journal File V5R3 Type 5 version 7.4
- Certified Microsoft DHCP File logs for Microsoft Windows Server 2019
- Certified Microsoft DNS Trace Log Multiple Server File for Microsoft Windows Server 2022
- Upgraded Zulu OpenJDK to 8u382
- Upgraded Tomcat version to 9.0.76

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

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

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

What's New

SmartConnector 8.4.3 incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
Mulesoft Audit	<p>SmartConnector for Mulesoft Audit Logs aims at retrieving the audit logs through the Audit logging query API. Mulesoft is a platform that gives IT administrators the tools to automate everything in their organization. This includes integrating data and systems and automating workflows and processes. It creates high-quality digital experiences, all on a single, easy-to-use platform. With the unique approach offered by Mulesoft, IT creates the digital building blocks that can be used as required, with all the right security, governance, and compliance measures built in.</p> <p>For information about installing and configuring Mulesoft Audit SmartConnector, see Configuration Guide for SmartConnector for Mulesoft Audit.</p>
Terraform Cloud	<p>Terraform Cloud enables infrastructure automation for provisioning, compliance, and management of any cloud, data center, and service.</p> <p>The Audit Trails API provides access to a continuous flow of audit events that detail modifications made to application entities (such as workspaces, runs, etc.) associated with a Terraform Cloud organization.</p> <p>Access to audit trails requires a paid subscription, which is included in the Terraform Cloud for a Business (TFCB) upgrade package. For more information, refer to the Terraform Cloud pricing page.</p> <p>For information about installing and configuring the Terraform Cloud SmartConnector, see Configuration Guide for SmartConnector for Terraform Cloud.</p>

New SmartConnectors/ Application Module	Description
Trellix ePolicy Orchestrator DB	<p>The Trellix Endpoint Security (ENS) protect and empower your workforce with an integrated security framework that protects every endpoint. Endpoint Security intercepts threats, monitors overall system health, and reports detection and status information. Client software is installed on each system to perform these tasks.</p> <p>The Trellix Endpoint Security connector is installed on the client computers to connect to the Trellix DB where it gathers and reports the overall system health, reports detection and status information. Install one or more Endpoint Security modules on client systems, manage detections, and configure settings that determine how product features work.</p> <p>For information about installing and configuring Trellix SmartConnector, see Configuration Guide for SmartConnector for Trellix ePolicy Orchestrator DB.</p>

Cloud Updates

Application Module	Description
Amazon S3	<p>Added support for Amazon Security Lake log source.</p> <p>Amazon Security Lake Integration automates the collection of security-related log and event data from integrated AWS services and third-party services.</p> <p>The Amazon S3 SmartConnector collects and parses the Open Cybersecurity Schema Framework (OCSF) logs that are stored in an Amazon S3 bucket by Amazon Security Lake.</p> <p>For more information, see Amazon Security Lake in Configuration Guide for Amazon S3 SmartConnector.</p>

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u382. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: <ul style="list-style-type: none">• CVE-2023-22043• CVE-2023-22045• CVE-2023-22049
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.76.

Version Updates

Application Module Version Updates	Description
Cisco ISE Syslog	Added support for Cisco ISE Syslog version 3.1 logs.
F5 BIG-IP Syslog	Added support for Cisco ISE Syslog version 14.1.5 logs.
Fortinet Fortigate Syslog	Added support for Fortinet Fortigate Syslog version 6.2.0 logs.
IBM eServer iSeries Audit Journal File	Added support for IBM eServer iSeries Audit Journal File for V5R3 Type 5 version 7.4.
Microsoft DHCP File	Added support for the Microsoft DHCP File logs for Microsoft Windows Server 2019.
Microsoft DNS Trace Log Multiple Server File	Added support for Microsoft DNS Trace Log Multiple Server File for Microsoft Windows Server 2022.
Tenable Nessus .nessus File	Added support for Tenable Nessus .nessus File for version 10.4.0.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added platform support for RHEL 8.8, 9.0, 9.1, and 9.2.
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.8.

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

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	<p>Added a new property named remote.management.listener.client.ip.allow.</p> <p>This property is used to accommodate IPv4 addresses and is designated for ArcMc instances, which allows precise control over the access of the connector for the specific addresses.</p> <p>Note: The remote.management.listener.client.ip.allow property does not support hostnames.</p> <p>For more information, see Remotely Managing Software-Based Connectors in Installation and User Guide for SmartConnector.</p>

Software Fixes

The following issues are fixed in the 8.4.3 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>The connector could not be added as a host to ArcMC when using the the FQDN with 8.4.1 p3 and above.</p> <p>Fix: The issue has been fixed now.</p>
ArcSight Common Event Format File	<p>When the connector sent some events containing the dpriv field to the ESM destination, the Target User Privileges column for each of the events was not updated correctly in ESM. Instead, the Target User Privileges column was updated with a fixed value for all events.</p> <p>Fix: The ESM export now displays the correct values in the Target User Privileges column for all events.</p>
AWS Security Hub	<p>The AWS Security Hub connector was unable to parse the JSON format logs that contained line feed characters such as \n, because the logs were fragmented into multiple lines.</p> <p>Fix: The approach for parsing JSON logs has been changed to ensure that all occurrences of \n are removed. This effectively prevents the logs from being split into multiple lines.</p>

Application Modules Software Fixes	Description
Linux Audit Syslog	<p>The connector was unable to merge and parse RHEL 8.3 logs by using the event merging function.</p> <p>Fix: The parser file has been modified to enhance the support for RHEL 8.3 event logs.</p>
McAfee ePolicy Orchestrator DB	<p>The devicecustomIPV6address field is being populated with an IPv4value instead of IPv6 value. This issue occurs because, for security reasons, the value of the ThreatsourceIpv6 field is a hash code present in the raw logs and the devicecustomIPV6address field is mapped to the ThreatsourceIpv6 field.</p> <p>Fix: Because the hash code cannot be directly converted to an IPv6 value and all the devicecustomstrings are already populated, the hash code is displayed as is in the SourceIPV6Address and DestinationIPV6Address fields, indicating that.</p> <p>The McAfee ePolicy Orchestrator DB 8.0 connector was unable to capture and accurately map the SourceDescription field to the corresponding ArcSight field.</p> <p>Fix: The endpoint security parser file has been updated to capture the SourceDescription field and to subsequently enable its mapping to a new ArcSight data field named SourceDescription.</p>
Microsoft Azure Event Hub	<p>The Microsoft Azure Event Hub connector presently limits the length of the rawEvent field for Defender for Endpoint. This results in the truncation of the field value if it's length exceeds the limit.</p> <p>Fix: A fix has been implemented to avoid the rawEvent field truncation.</p> <p>The Microsoft Azure Event Hub Connector was omitting the backslash character \ from the output field values.</p> <p>Fix: This issue has been resolved by populating the backslashes.</p>
Microsoft DNS Trace Log Multiple Server File	<p>The connector was not able to parse and process the event logs after upgrading it from 8.4.0 to 8.4.1. It was showing start and end file processing with no cache or errors.</p> <p>Fix: Added framework code to handle the parsing issue of the events.</p>

Application Modules Software Fixes	Description
Microsoft Windows Event Log - Native	<p>When the Microsoft Windows Event Log - Native connector was configured with the Windows Event Forwarder (WEF) mode, it was unable to receive events forwarded to a Windows Event Collector (WEC) host causing the WINC agent to crash. The connector was facing issues because of the Microsoft Windows Server 2022 changes.</p> <p>Fix: Now, the Microsoft Windows Event Log - Native connector receives events that are forwarded to a Windows Event Collector (WEC) host.</p>
MS Windows Event Log – Native SmartConnector (WiSC)	<p>The WiSC connector 8.4 was unable to receive events from remote hosts and was throwing a Java exception.</p> <p>Fix: The "Apache CXF Runtime" and "jaxb-impl" jar files and their dependencies have been upgraded to the compatible versions.</p>
Tenable Nessus .nessus File	<p>The connector was aggregating the vulnerabilities using the hostname, as there was no option to reconfigure the connector to aggregate the vulnerabilities while using IP address. This happens if the .nessus file does not contain hostname information but contains only IP for some assets in the file.</p> <p>Fix: A new property uselip has been added to <code>agent.properties</code>, which by default is false. If this property is set to true it will reconfigure the connector to aggregate the vulnerabilities using IP address. Based on this property, the vulnerabilities will be mapped using either hostname or IP.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the 8.4.3 release:

- Cisco ISE 1
- IBM X-Force XPU 4212.12221
- Juniper IDP Content Version 3622, 3614, and 3604
- McAfee Network Security Manager 11.10.8.1, 11.10.7.1, and 11.10.6.1
- Microsoft SharePoint 2010
- Microsoft Windows
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0

What's New

- Sourcefire SEU 31470, and 2983
- Symantec Network Security 7100 1659, 7100 1639, and 7100 1621
- TippingPoint SMS IPS DV9814, DV9807, and DV9800
- UNIX syslog

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

SmartConnector Parser 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 8.4.3 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-8.4.3.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.3.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.3.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.3.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.3.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.3.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.3.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.3.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.3.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.3.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

SmartConnector Release Notes

Installing SmartConnectors

ArcSight-8.4.3.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.3.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.3.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.3.xxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.3.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.3.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.3.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to 8.4.3



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

OpenText provides a digital public key for you to verify that the signed software you received is indeed from OpenText 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 8.4.3

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 8.4.3

For information about upgrading Load Balancer to 8.4.3, 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>Note: The 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</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 Microsoft Windows Event Log - Native 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" ctrlr+c</pre>

<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 Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</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 Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>

Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native 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 TCP3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<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.

Load Balancer	<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>or <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>or <pre>service arc_conn1b start</pre>
---------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Trellix ePolicy Orchestrator DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p>
	<p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>

Connector End-of-Life Notices

 **Note:** For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 8.4 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	11/2025	The 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.

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), 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	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.

SmartConnector Release Notes
Connector End-of-Life Notices

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	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	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 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!