Micro Focus Security ArcSight SmartConnectors

Software Version: 8.4.2

SmartConnector Release Notes

Document Release Date: July 2023
Software Release Date: July 2023

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

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

The SmartConnector 8.4.2 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Support for a new SmartConnector named ServiceNow
- Support for a new SmartConnector named Microsoft Azure Event Hub
- Support for the Apache Tomcat File logs for version 10.1.2
- Support for IBM Security Access Manager Syslog logs for version 10.0.1
- Support for Cisco IronPort Web Security Syslog AsyncOS 12.0.1
- Support for Microsoft Server SharePoint DB 2019
- Support for the Check Point Syslog R81.40 modules
- Support for Rocky Linux 8.6 as the installation platform
- Support for Citrix NetScaler 13.0.0
- Support for Linux Kernel-based Virtual Machine (KVM) 9.0
- Support for Microsoft Windows Hyper-V logs
- Support for Red Hat Enterprise Linux (RHEL) 9.0 and 9.1 logs for the Linux Audit File, Linux Audit Syslog, UNIX Login/Logout File, and UNIX OS Syslog connectors
- Support for the Microsoft Windows Server 2019 and Microsoft Windows Server 2022 events for Microsoft ADFS
- Upgrade of Zulu OpenJDK to 8u372
- Upgrade of Tomcat version to 9.0.74
- Updates of ArcSight Event Content-Categorization till May 2023. These updates are now a monthly release.

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 8.4.2 incorporates the following SmartConnector releases, and content and categorization updates:

- SmartConnector 8.4.1 Patch 1
- Event Content-Categorization updates May 2023

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
Microsoft Azure Event Hub	Microsoft Azure is a set of cloud services to helps organizations build, manage, and deploy applications on a massive, global network using their favorite tools and frameworks. The Microsoft Azure Event Hub SmartConnector helps you monitor the activities on Microsoft Azure Cloud services. The Microsoft Azure Event Hub SmartConnector is a better alternative version of Microsoft Azure Monitor Event Hub Connector, which can be deployed on both cloud and off cloud, to monitor the activities on Microsoft Azure Cloud services. It provides the following benefits: • Overall cost reduction • Better performance • More log type support • No deployment complexity For more information, see Configuration Guide for Microsoft Azure Event Hub SmartConnector.
ServiceNow	The SmartConnector for ServiceNow retrieves events from ServiceNow, normalizes the events, and then sends them to the configured destinations. For more information, see Configuration Guide for SmartConnector for ServiceNow.

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u372. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: • CVE-2023-21930 • CVE-2023-21954 • CVE-2023-21967 • CVE-2023-21939 • CVE-2023-21937 • CVE-2023-21938 • CVE-2023-21968
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.74.

Version Updates

Application Module Version Updates	Description
Apache Tomcat File	Added support for the Apache Tomcat File logs for version 10.1.2.
IBM Security Access Manager Syslog	Added support for IBM Security Access Manager Syslog logs for version 10.0.1.
• Linux Audit File • Linux Audit Syslog • UNIX Login/Logout File • UNIX OS Syslog	Added support for Red Hat Enterprise Linux (RHEL) 9.0 and 9.1.

Application Module Version Updates	Description
Microsoft Windows Event Log - Native	Added support for the following Microsoft Windows Server 2019 and Microsoft Windows Server 2022 events for Microsoft ADFS. • `Event 105` • `Event 111` • `Event 221` • `Event 227` • `Event 298` • `Event 352` • `Event 397` • `Event 575` • `Event 1000`
• UNIX Login/Logout File • UNIX OS Syslog	Added support for Linux Kernel-based Virtual Machine (KVM) 9.0.
WiNC on Connector Hosting Appliance	Added support for Red Hat Enterprise Linux Server (RHEL) 7.9.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.6.

For details about hardware, software or platform, and SmartConnector requirements, refer to Technical Requirements for SmartConnectors.

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	Added support for **Default AWS Credentials Provider** for the **Amazon S3** destination to use the Default Credential Provider Chain. For more information about the **Default AWS Credentials Provider** parameter, see Amazon S3 Parameters.
All SmartConnectors with **Microsoft Event hub**as destination	Added support for **Certificate** and **Client secret** based authentication to authenticate Microsoft Azure Event Hub. Azure Event hub access using connection string having **SharedAccessKey** information have been deprecated in this release. When configuring the Kafka FlexConnector, if the source type is selected as **Azure Event Hub**, then the **Microsoft Event hub** destination needs to be reconfigured to use any one of the authentication mechanisms. For more information about the destination parameter details, see Installation and User Guide for SmartConnector. For more information about Azure Event Hub, see Configuration Guide for Microsoft Azure Event Hub.
ArcSight Threat Acceleration Program (ATAP)	ATAP connector, previously known as Galaxy Threat Acceleration Program (GTAP) is now available with the latest security fixes.
Developer's Guide to FlexConnector for Kafka	Added support for **Certificate** and **Client secret** based authentication to authenticate Microsoft Azure Event Hub. Azure Event hub access using connection string having **SharedAccessKey** information have been deprecated in this release. When configuring the Kafka FlexConnector, if the source type is selected as **Azure Event Hub**, then the **Microsoft Event hub** destination needs to be reconfigured to use any one of the authentication mechanisms. For more information about the destination parameter details, see Installation and User Guide for SmartConnector. For more information about Azure Event Hub, see Configuration Guide for Microsoft Azure Event Hub.

Application Module Enhancements	Description
Microsoft 365 Defender	Added support for the Certificate-based authentication method for the Microsoft 365 Defender SmartConnector. The connector will make the access token request with the Client Certificate and the same can be used for pulling the APIs. For more information, see the Configuration Guide for Microsoft 365 Defender.
Microsoft Message Trace REST API	Added support for the **OAuth2-Client Credentials** authentication type to secure REST APIs to collect events from Microsoft Office 365 Message Trace REST API. For more information, see parameter details in the Configuration Guide for Message Trace Rest API Connector.
Microsoft SharePoint Server DB	Added support for Microsoft Server SharePoint DB 2019. Added support for the following events: • `Event 1` • `Event 10`
Microsoft Windows Event Log - Native	Added support for Microsoft Windows Hyper V logs. For more information about configuring the Microsoft Windows Hyper V log source, see Microsoft Windows Hyper V. For more information about supported event mappings, see Event Mappings for Microsoft Windows Hyper V.

Software Fixes

The following issues are fixed in the 8.4.2 release:

Application Modules Software Fixes	Description
All SmartConnectors	The `runagentsetup` was throwing errors after changing the remote management password from the Command Line (CLI) as the password in `connector_config.xml` was not getting updated with new password.. Only default credentials must be used for remote management password of the smartconnector. **Fix**: The issue is resolved by changing the remote management password of the connector by adding `remote.management.password=new password` to `agent.properties` and then running the `runagentsetup`.
All SmartConnectors	The connector was sending failover event **agent:051** to only the first instance of failover of primary ESM and not for every failover event. **Fix**: This issue was fixed by removing a condition in the code, that was set to send the failover event only on the first occurrence.
All SmartConnectors (Syslog files)	After restarting, the connector stops reading the events from the log files from the last position to which it was saved. The connector was only reading the events from the end of the file. **Fix**: The issue has been fixed, as now the connector will start reading the log files from the point where it stopped.
ArcSight Common Event Format REST	A few minutes after the ArcSight Common Event Format REST connector starts receiving events from the Qualys API, the **vm_scan_since** parameter in the **eventsurl** property of the agent.properties file gets automatically updated. This results in the **href** field in the URL of the API being empty, which, in turn, leads to the connector not receiving events anymore. **Fix**: The issue has been fixed by updating the value of the **vm_scan_since** parameter to the timestamp of the URL of the API.
	The ArcSight Common Event Format REST connector polls the Digital Shadows API endpoint frequently in a minute, thus reaching the API's call rate limit. This results in the locking of the API key. **Fix**: The issue has been fixed by introducing a new property called **maxqueriesperminute** in the `RestApiConstants.java` file. This property specifies the maximum number of times per minute that the connector can poll the API. The default value of the property is **60**. When the API polling count reaches the **maxqueriesperminute** value in a minute, then, for the remaining seconds of that minute, the polling is paused.

Application Modules Software Fixes	Description
Check Point Syslog	The Check Point Syslog connector was unable to parse the logs for the **Application Control** and **Smart Defense** modules, because a new key **resource** was introduced in the logs. **Fix**: The base regex of the Check Point Syslog parser file has been modified to provide support for the **resource** key in the **Application Control** and **Smart Defense** modules of Check Point logs.
Cisco IOS Syslog	The Cisco IOS Syslog connector was unable to retrieve the value of the **hostname** field. **Fix**: The parser file has been modified to retrieve the value of the **hostname** field.
Cisco IronPort Web Security Appliance Syslog	The logs of Cisco IronPort Web Security Syslog AsyncOS version 12.0.1 were not being parsed. **Fix**: Added support for Cisco IronPort Web Security Syslog AsyncOS 12.0.1.
Citrix NetScaler Syslog	The timestamp of `citrix netscaler` events for the following modules was not getting converted from GMT to PST: • `SSLVPN HTTPREQUEST` • `AAATM HTTPREQUEST` **Fix**: The issue has been fixed by making changes in the regex of `SSLVPN HTTPREQUEST` and `AAATM HTTPREQUEST` modules to adjust the time.
Citrix NetScaler Syslog	The Citrix NetScaler Syslog connector was unable to parse some of the events for Citrix NetScaler Version 13.0.0. **Fix**: Added support for Citrix NetScaler 13.0.0.
Fortinet Fortigate Syslog	The `Fortinet Key_value` parser for Fortinet Fortigate Syslog was using the **date** and **time** field for the **Device Receipt Time** field. **Fix**: The issue is fixed by making changes in parser to prioritize `eventtime` or `log time timestmap` over **date** and **time** for the **Device Receipt Time** field.
Juniper Firewall ScreenOS Syslog	The Source and Destination fields in the system-warning-00518 module logs from Juniper ScreenOS were not being parsed. **Fix**: An existing sub-message for the system-warning-00518 module has been modified to handle the parsing issue for Juniper ScreenOS logs.

Application Modules Software Fixes	Description
Microsoft Windows Event Log - Native	The Microsoft Windows Event Log - Native connector was unable to parse **Event ID 411** correctly, due to the presence of multiple addresses in %5. It was resulting in the **Source Address** field to remain empty. **Fix**: The **Source Address** field is now being populated with the first of the two addresses, while both addresses are being stored in **Device Custom String 3**.
Oracle Unified Audit Trail DB	After applying the fix for the **ORA-22835 error**, the following error is displayed: **ORA-01401: inserted value too large for column**. This error occurs because the size of the text fields provided in the fix for the **ORA-22835 error** is too large (4000). **Fix**: To fix this issue, the Oracle admin must reduce the size of the text fields by replacing all instances of "4000" with "2000" in the fix provided for the **ORA-22835** error. For more information, refer to the Troubleshooting section of the *Configuration Guide for Oracle Unified Audit Trail DB SmartConnector*.
Tenable Nessus .nessus File	The Tenable Nessus .nessus File connector was unable to process events from long reports in the `.nessus` format from a Nessus source device. When the connector was configured to use ESM as a destination, it was displaying `'byte array size too long'` error. This error caused the connector to prevent the other Nessus reports from being processed. **Fix**: The issue was occurring because of lengthy Nessus report values that were being compared with the `'Short.MAX'` value of Java. This resulted in throwing an exception. The issue has been resolved now, as the incoming value is truncated to the maximum size allowed in the `'writeString'` method of `'PrimitiveOutputStream.java'`.

Event Categorization Updates

For more information, see 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 8.4.2 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-8.4.2.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.2.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.2.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.2.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.2.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.2.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.2.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.2.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.2.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.2.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

ArcSight-8.4.2.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.2.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.2.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.2.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.2.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.2.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.2.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading to 8.4.2

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 8.4.2

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 8.4.2

For information about upgrading Load Balancer to 8.4.2, 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	**SmartConnector or Collector remote connections fail due to low entropy**
	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.
	Workaround:
	To ensure that the entropy value is at the desired level:
	1. Install the `rng-tools` package:
	`sudo yum install -y rng-tools`
	2. Add the following line to the `/etc/sysconfig/rngd` file:
	`EXTRAOPTIONS="-r /dev/urandom"`
	3. Check the entropy availability in the system:
	`cat /proc/sys/kernel/random/entropy_avail`
	4. Start the `rngd` package as root user:
	`service rngd start`
	5. Enable the `rngd` service to start at the system start-up:
	`systemctl enable rngd.service`
	`systemctl start rngd.service`
	6. Ensure that the `rngd` package is always running (even after a reboot) as `root` user:
	`chkconfig --level 345 rngd on`
	7. Check the entropy availability in the system, after starting the `rngd` service:
	`cat /proc/sys/kernel/random/entropy_avail`

	Unable to install connector because of missing packages **Workaround:** Ensure that the following packages are installed: 1. yum install -y unzip 2. yum install -y fontconfig \ dejavu-sans-fonts

All SmartConnectors installed on Solaris	**When upgrading SmartConnectors on Solaris, a timeout error is displayed** **Workaround**: - 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: 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.
	Connector logs show Fatal Exception error: Unable to find requested property `'transport.cefkafka.extra.prod.props'` This message does not impact the performance or the functionality of the Connector. **Workaround:** 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: `parser.operation.result.cache.enabled=false` 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: `agents[0].eventprocessorthreadcount=5 or agents [0].eventprocessorthreadcount=1, etc..` where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.

All File SmartConnectors	**When adding a log into a log file using the vi text editor, events are not sent to ESM**
	Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.
	Workaround:
	Use the cat command to append data:
	`Syntax:`
	`cat >> log_file_name [ Enter ]`
	`"your logs"`
	`ctlr+c`

Google Cloud SmartConnector	**The Google SmartConnector cannot authenticate tokens with Google API** The following error is displayed when the connector is used from ArcMc with the One-Click feature: `{ “error” : “invalid_grant”, “error_description” : "Invalid JWT: Token mustbe a short-lived token (60 minutes) and in a reasonable timeframe. Check youriat and exp values in the JWT claim." }` **Workaround:** 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.

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	**Connector installation fails when the client properties file is auto populated incorrectly** 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. **Workaround:** Set the following path manually: `$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties`
McAfee ePolicy Orchestrator DB	**Connector installation issue in FIPS mode** Unable to install the McAfee ePolicy Orchestrator DB SmartConnector in FIPS Mode. **Workaround**: You must install the SmartConnector in non-FIPS mode only.
Microsoft Message Trace REST API	**Issues with ArcMC upgrade behaviour in the Message Trace REST API connector** Unable to upgrade the Message Trace Rest API Connector through ArcMC. **Workaround:** You can upgrade the Message Trace REST API Connector either using ESM or locally.
Microsoft Windows Event Log (WiSC)	**WiSC SmartConnector issues** WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. it has the following issues: • 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. **Workaround**: To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.

Microsoft Windows Event log - Native	**The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2** The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS. **Workaround**: 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. To use 'Raw TCP', perform the following steps after installing the SmartConnector: 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.
Microsoft Azure Monitor Event Hub	**Azure Event Hub debug mode issue** Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors. **Workaround**: To configure the debug mode: 1. Go to **Azure portal** > **Function app** > **Configuration**. 2. Set the **DebugMode** application value to **False**. 3. Restart the Function App.

Load Balancer	**Load Balancer `arc_connlb` service does not start and displays an error message**
	When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer `arc_connlb` service does not start and displays an error message in the `lb.out.wrapper.log` even after you start the `arc_connlb` service manually.
	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:
	1. After you install Load Balancer as a service, before you upgrade, stop the `arc_connlb` service by using the following command:
	`# /etc/init.d/arc_connlb stop`
	or
	`service arc_connlb stop`
	2. After Load Balancer is successfully upgraded, start the `arc_connlb` service by using the following command:
	`# /etc/init.d/arc_connlb start`
	or
	`service arc_connlb start`

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.

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.

Publication Status

Released: July 2023

Updated: July 2023

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 8.4.2)

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!