opentext™

ArcSight SmartConnectors

Software Version: CE 24.1

SmartConnector Release Notes

Document Release Date: January 2024
Software Release Date: January 2024

Legal Notices

Open Text Corporation

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

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

Contents

Release Highlights

The SmartConnector CE 24.1 (v8.4.4) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Rebranded both the documents and products to OpenText
- New SmartConnector for GitHub Enterprise Audit Log
- Support for the following new device sources:
  - VMware Carbon Black EDR
  - CyberArk Privileged Access Security version 11.3
  - OpenText Network Detection & Response (Bricata)
- Certified version 9.2 for Red Hat Enterprise Linux (RHEL) logs for the Linux Audit File, Linux Audit Syslog, UNIX Login/Logout File, and UNIX OS Syslog connectors
- Support for the following Trellix Endpoint Security modules:
  - SolidCore 8.3
  - Threat Intelligence Exchange Server 4.0
  - Trellix Security for SharePoint 3.5
- Certified version 9.2 for Rocky Linux as the installation platform
- Support for registration URL for the **ArcSight SaaS** destination
- Certified version 15.1 for Juniper JUNOS Syslog
- Certified version 7200-05 for IBM AIX Audit Syslog
- Certified version(s) 8.5.161.0 and 8.3.14.0 for Cisco Wireless LAN Controller Syslog
- Certified version 5 v2.72 for HPE Integrated Lights-Out Syslog
- Upgrade of Zulu OpenJDK to 8u392
- Upgrade of Tomcat version to 9.0.82

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 CE 24.1 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
CyberArk Privileged Access Security	SmartConnector for CyberArk Privileged Access Security collects the CEF formatted logs and parse them to the desired destination. The key agent in this facility is **syslog connector**. It receives messages and routes them to their destination based on configuration information provided in the `/etc/syslog.conf` file. The CyberArk's Privileged Access Security (PAS) solution is a full life-cycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities. For more information, see Configuration Guide for CyberArk Privileged Access Security SmartConnector.
GitHub Enterprise Audit Log	SmartConnector for GitHub Enterprise Audit Log retrieves audit trail events through the GitHub Rest API, normalizes the events, and then sends them to the configured destinations. For more information, see Configuration Guide for GitHub Enterprise Audit Log SmartConnector.

New SmartConnectors/ Application Module	Description
OpenText Network Detection & Response (Bricata)	SmartConnector for OpenText Network Detection & Response (Bricata) collects the logs from Bricata and leads the next generation of advanced network detection and response solutions for the enterprise. With fusing detection, forensic analysis and proactive threat hunting, OpenText NDR empowers high-performance enterprise security teams with total visibility into network traffic and also empowers security teams to effectively defend against known threats and to illuminate those otherwise unseen. For more information, see Configuration Guide for OpenText Network Detection & Response (Bricata) SmartConnector.
VMware Carbon Black EDR	SmartConnector for VMware Carbon Black EDR collects the CEF formatted logs and parse them to the desired destination. The key agent in this facility is **syslog connector**. It receives messages and routes them to their destination based on configuration information provided in the `/etc/syslog.conf` file. VMware Carbon Black EDR is an incident response and threat hunting solution designed for Security Operations Center teams with offline environments or on-premises requirements. Carbon Black EDR continuously records and stores endpoint activity data so security professionals can hunt threats in real time and visualize the complete attack kill chain, using the VMware Carbon Black Cloud's aggregated threat intelligence. For more information, see Configuration Guide for VMware Carbon Black EDR SmartConnector.

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u392. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: • CVE-2023-22067 • CVE-2023-22081
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.82.

Version Updates

Application Module Version Updates	Description
Cisco Wireless LAN Controller Syslog	Certified version(s) 8.5.161.0 and 8.3.14.0 for Cisco Wireless LAN Controller Syslog logs.
Juniper JUNOS Syslog	Certified version 15.1 for Juniper JUNOS Syslog logs.
IBM AIX Audit Syslog	Certified version 7200-05 for IBM AIX Audit Syslog logs.
• Linux Audit File • Linux Audit Syslog • UNIX Login/Logout File • UNIX OS Syslog	Certified version 9.2 for Red Hat Enterprise Linux (RHEL).
HPE Integrated Lights-Out Syslog	Certified version 5 v2.72 for HPE Integrated Lights-Out Syslog logs.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 9.2.

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	Added support for registration URL for the **ArcSight SaaS** destination. If **ArcSight SaaS** is configured as a destination, all security events are sent in the **Avro** format to Amazon MSK that is managed by ArcSight's SaaS offering. For more information about the destinations parameters to be selected during installation, see ArcSight SaaS.
All SmartConnectors	The CEF 1.2 schema has now been updated with the following new CEF fields: **Note**: The **ParserVersion** and **ParserIdentifier** parameters are applicable only for **CEF Version 1.0**. • **ParserVersion** This field contains the release timestamp (YY-MM-DD) of the parser file that processed the events. The release timestamp is updated as and when any new enhancement is done to the content of the parser. • **ParserIdentifier** This field contains a unique ID assigned to each of the parser file. The **agent:049** event containing this specific unique ID can be used to extract information such as the name of the parser file, signature of the parser file, and to determine whether it is an overridden parser file and so on. For information about the **agent:049** event, see SmartConnector Audit Events. **Note**: The **agent:049** event generation is currently set to disabled. This will be enabled when the Avro based destinations are supported. For more information, see ArcSight Common Event Format (CEF) Implementation Standard.
Trellix ePolicy Orchestrator DB	Added support for the following Trellix Endpoint Security modules: • SolidCore 8.3 • Threat Intelligence Exchange Server 4.0 • Trellix Security for SharePoint 3.5

Software Fixes

The following issues are fixed in the CE 24.1 release:

Application Modules Software Fixes	Description
All SmartConnectors	While receiving `IPAddress` instead of a `hostname`, or vice-versa, the connector was interpreting the events as two separate events. Because of this, the connector was sending duplicate `agent:043` as Connector device status signals for the same device. **Fix**: This issue has been fixed as now the connector will send only one message if it is able to resolve the `hostname` and `IPAddress` issue.
All SmartConnectors	After upgrading the connector through ArcMC, the uninstall variable file of the Connectors which is `installvariables.properties`, was not getting updated. The value of the `PRODUCT_VERSION_NUMBER` property remained same as the base version even after upgrading the connector. **Fix**:The issue has now been fixed as the value of the `PRODUCT_VERSION_NUMBER` property under `ArcsightHome/uninstallerData/installvaribles.properties` will get updated from the base version to the current version after upgrading the connector.
All SmartConnectors managed by containerized ArcMC	Connector required a manual restart for the events to display the custom zones in the ESM Active Channels after the network zone information was pushed from ArcMC **Fix**: This issue has been fixed by implementing a listener for this event, ensuring that network zones are updated automatically without the need for a manual restart of a Connector.
Cisco ASA Syslog	The Cisco PIX event type **`302303`** for Cisco ASA Syslog connector was not being parsed. **Fix**: The issue has been resolved by modifying the regex.
Cisco ISE Syslog	The Cisco ISE Syslog connector was unable to parse the Cisco ISE (Identity Services Engine) service logs for `CISE_PROFILER`, as it was encountering the number format exceptions. This happened because the delimiter in `CISE_PROFILER` was **\,** instead of **,**. **Fix**: The issue has been resolved by retrieving the required data and excluding the special characters.

Application Modules Software Fixes	Description
Infoblox NIOS Syslog	Infoblox 8.5.2 device events were not getting parsed and the vendor and product names were erroneously getting labeled as UNIX. **Fix**: A code fix has been provided to ensure the successful parsing of Infoblox 8.5.2 events. Consequently, the corrected values for device Vendor and Product are now recognized as Infoblox and NIOS, respectively.
Windows Event Log SmartConnector (WiSC)	While reconfiguring the Windows Event Log SmartConnector (WiSC) by modifying the default connector parameter values, it throws an error leading to a deadlock. Whereas, while installing the connector with the default parameter values, it is getting through. **Fix**: This issue has now been fixed.
Fortinet Fortigate Syslog	The Fortinet Fortigate Syslog connector was parsing the bandwidth field value as an integer instead of long. This resulted in the incorrect mapping in the destination and an error message was displayed in the **`agent.log`** file. **Fix**: This issue has been resolved by changing the data type of the bandwidth field from integer to long while parsing. This change was required only for CEF 1.0 because it was working fine with CEF 0.1.
	The **`eventtime`** value of the Fortinet Fortigate Syslog connector was provided in nanoseconds. But the Fortigate parser was converting the epoch time from seconds. This resulted in incorrect field values for the **Device Receipt Time** and **End Time**. **Fix**: The issue has been resolved by updating the field value for the **Device Receipt Time** in the Fortigate parser. It now derives the date and time information present within the log that ensures the accuracy of the field value. And, the field value for **End Time** now depends on the Device Receipt Time for populating the accurate value.
F5 BIG-IP Syslog	Both **F5 Big IP** and **UNIX/ UNIX-like** systems have the `id` value as `systemd` because of which it was fetching the same value for the `device vendor` and `device product` that is **`F5 Big IP`**. **Fix**: The issue has been resolved by modifying the base regex to ensure that logs from `F5 Big IP` with `systemd` as the `id` value receives the accurate device vendor and device product values, that identifies as **F5 Big IP**. Similarly, logs from `Unix/ Unix-like` systems with `systemd` as the `id` value is now assigned the accurate device vendor and device product values, categorizing them as **Unix**.
	The F5 big events for F5 BIG-IP Syslog connector was not being parsed. **Fix**: Added regex to handle the parsing issue of the events.

Application Modules Software Fixes	Description
Microsoft Azure Event Hub	The Microsoft Azure Event Hub connector was observing a casting exception while trying to write `IPv4` address into custom string in the **`primaryIPv4Address`** field for **`Resource Event Logs`**. **Fix**: This issue has now been fixed.
	The Microsoft Azure Event Hub connector was unable to process certain events for Defender for Cloud. **Fix**: The issue has been resolved by modifying the log processing capability to handle the format of the unparsed events.
Microsoft IIS File	The Microsoft IIS File connector was locking and not releasing the previously created log files. **Fix**: The issue has now been fixed.
Microsoft 365 Defender	The `endTime` and `startTime` fields of the Microsoft 365 Defender connector were always being populated as 01/01/2023. **Fix**: This issue has now been fixed.

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.1 release:

- Cisco ISE
- F-Secure Anti-Virus 5.5
- Juniper IDP Content Version 3652
- McAfee Network Security Manager 11.10.11.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 2983
- Symantec Network Security 7100 1729
- TippingPoint SMS IPS DV9849
- Trellix SolidCore 8.3
- Trellix Security for SharePoint 3.5
- Trellix Threat Intelligence Exchange 4.0

For more information, see Event Content-Categorization updates November 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 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.

Signature Verification Procedure

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the OpenText Downloads website along with their associated signature files (*.sig).

   > Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

   OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the OpenText Code Signing site. If you discover a

file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact OpenText Customer Support.

4. Begin the installation.

SmartConnector CE 24.1 (v8.4.4) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.4.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.4.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.4.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight-8.4.4.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.4.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.4.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.4.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.4.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.4.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.4.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.4.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.4.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.4.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.

ArcSightSmartConnectorLoadBalancer-8.4.4.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.4.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.4.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.4.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.1 (v8.4.4)

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

For information and instructions, see "Signature Verification Procedure" on page 13.

Upgrading SmartConnector to CE 24.1 (v8.4.4)

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 CE 24.1 (v8.4.4)

For information about upgrading Load Balancer to CE 24.1, 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	**SmartConnector or Collector remote connections fail due to low entropy**
	
	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**
	
	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

CyberArk Privileged Access Security	**Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)** The issue occurs because the CyberArk logs do not contain a pipe symbol ('|') in the header section, after the **name** field. This results in mapping discrepancies across all the fields in some cases or issues in the **event.name** field in other cases. This parsing anomaly hinders the accurate extraction and representation of information from the logs. **Workaround** To address this issue, request modifications to the log formatas described in the ArcSight Common Event Format (CEF) Implementation Standard document, to ensure that the header section contains the pipe symbol ('|') after the **name** field.
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`
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`

Trellix ePolicy Orchestrator DB	**Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination** 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, **Workaround:** Perform the following steps for re-registering the connector on ESM using ArcMC: 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**. The connector is now linked to ESM with a new name.
	Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector 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. **Workaround:** While installing the connector, manually specify the parameters instead of importing them.

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 24.1 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.

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 CE 24.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!