ArcSight SmartConnectors

Software Version: CE 24.2

SmartConnector Release Notes

Document Release Date: April 2024
Software Release Date: April 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

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

The SmartConnector CE 24.2 (8.4.5) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Certified parser for Cisco IOS Syslog 15.9
- Certified parsers for HPE UX Syslog and HPE UX Audit File version 11.0
- Certified version 8.9 for Rocky Linux as the installation platform
- Certified Red Hat Enterprise Linux (RHEL) version 7.8.0 for UNIX Login/Logout File and UNIX OS Syslog
- Support for the following Trellix Endpoint Security modules:
    - Data Loss Prevention 11.10
    - Data Loss Prevention Incident Events 11.10
    - Advanced Threat Defense and Intelligent Sandbox 5.2
    - Data Loss Prevention Discover 11.10
- Upgrade of Zulu OpenJDK to 8u402
- Upgrade of Tomcat version to 9.0.86
- Upgrade of PostgreSQL JDBC version to 42.4.4

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 24.2 (8.4.5) 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
Trellix ePolicy Orchestrator DB	Added support for the following Trellix Endpoint Security modules: • Data Loss Prevention 11.10 • Data Loss Prevention Incident Events 11.10 • Advanced Threat Defense and Intelligent Sandbox 5.2 • Data Loss Prevention Discover 11.10

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors	Upgraded PostgreSQL JDBC version to 42.4.4.
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.86.

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u402. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: • CVE-2024-20918 • CVE-2024-20952 • CVE-2024-20919 • CVE-2024-20921 • CVE-2024-20926 • CVE-2024-20945 • CVE-2024-20923 • CVE-2024-20925 • CVE-2024-20922

Version Updates

Application Module Version Updates	Description
Cisco IOS Syslog	Certified parser for Cisco IOS Syslog 15.9.
• HPE UX Syslog • HPE UX Audit File	Certified parsers for HPE UX Syslog and HPE UX Audit File version 11.0.
• UNIX Login/Logout File • UNIX OS Syslog	Certified RHEL version 7.8.0 for UNIX Login/Logout File and UNIX OS Syslog logs.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.9.

For details about hardware, software or platform, and SmartConnector requirements, see Compatibility Matrix of SmartConnector section in the Technical Requirements for SmartConnectors guide.

SmartConnector Enhancements

Application Module Enhancements	Description
Load Balancer	Added support for the following global properties of Load Balancer: • read.timeout • retry.count • retry.delay For more information, see the Configuration Parameters section in the Configuration Guide for SmartConnector Load Balancer.

Software Fixes

The following issues are fixed in the CE 24.2 release:

Application Modules Software Fixes	Description
All SmartConnectors	While starting the connector, a fatal exception error that **No password has been defined** occurred. This error occurred because `Remote Management` was enabled, and the password for Remote Management was not specified in the properties file. **Fix**: The issue has been resolved by changing the log level from **`FATAL`** to **`WARN`**.
All SmartConnectors	After upgrading the Connector on Linux OS, the zipped file of the build of the previously installed Connector failed to preserve the correct file permissions. As a result, the user was unable to execute the old build to roll back to the previously installed version of the Connector. **Fix**: The previously installed Connector's installation folder has now been Tar.GZipped for Linux OS, enabling it to retain the file permissions after an upgrade. This issue has not been observed for connectors installed on Windows OS.
Amazon S3	The Amazon S3 connector with AWS CloudTrail log was displaying a fatal exception and was unable to parse the timestamp format "yyyy-MM-dd'T'HH:mm:ssZ". **Fix**: The parser has been modified by adding support for the "yyyy-MM-dd'T'HH:mm:ssZ" timestamp format.
ArcSight FlexConnector JSON Multiple Folder Follower	The ArcSight FlexConnector JSON Multiple Folder Follower connector was unable to parse compressed files, such as `.gz`. **Fix**: The issue has now been resolved.

Application Modules Software Fixes	Description
AWS CloudTrail	The AWS CloudTrail connector was displaying a fatal exception and was unable to parse the following timestamp formats: "yyyy-MM-dd'T'HH:mm:ssZ" and "yyyy-MM-dd" . **Fix**: The parser has been modified by adding support for the "yyyy-MM-dd'T'HH:mm:ssZ" and "yyyy-MM-dd" timestamp formats.
Cisco IronPort Email Security Appliance Syslog	The Cisco IronPort Email Security Appliance Syslog connector was experiencing the following issues: • The Cisco IronPort Email Security Appliance encountered parsing issues with the **Device Custom String 6** field when it was parsing logs using the Cisco IronPort Email Security Appliance Syslog connector. The parser also inserted other data apart from the Subject into the Device Custom String 6 field. • When there were more than **~125** other lines between the start and the finish events for the message, the Subject that was saved in the Device Custom String 6 gets lost and does not appear in the final aggregated message. **Fix**: To fix this issue: • Modified the mapping of the **Device Custom String 6** field for the specific events. Now, the non-subject values will appear in the **Flex String 2** field. • When a message has more than **~125** other lines between the start and the finish events of the message with the same MID, the Subject that was saved in the **Device Custom String 6** field will now remain valid and appear in the final aggregated message as expected. **Note:** Ensure the following for successfully merging the events: • The **Start** and **Message Finished** strings must be present at the beginning and the end, respectively. • All the email logs must have the same MID.
Cisco ISE Syslog	The **Remote-Address** field for the Cisco ISE Syslog connector was not mapped for the **CISE_Failed_Attempts** event. **Fix**: The issue has now been resolved by mapping the **Remote-Address** field to the **Source Address** field for both **CISE_Failed_Attempts** and **Cisco ISE TACACS Diagnostics** events.
Cisco NX-OS Syslog	The events of the **ARP-3-DUP_SRC_IP_PROBE** module for the CISCO NX-OS Syslog connector were not being parsed. **Fix**: Modified a sub-message to enable the parsing of the events of the **ARP-3-DUP_SRC_IP_PROBE** module.
Cisco PIX/ ASA Syslog	The events of the **ASA-6-302025** module for the Cisco PIX/ ASA Syslog connector were not being parsed. **Fix**: Modified sub-messages to enable the parsing of the events of the **ASA-6-302025** module.

Application Modules Software Fixes	Description
Cisco PIX/ ASA Syslog	The Cisco PIX/ ASA Syslog connector was not parsing the events properly for the following message IDs: 402143, 725006, 302025, 302027, 434004, and 303002. **Fix**: The parser has been modified to fix the parsing issue of these message IDs.
Citrix NetScaler Syslog	The Citrix NetScaler Syslog connector was incorrectly parsing the timestamp format "DD/MM/YYYY" for the "AAA TM session logged out" events. **Fix**: The parser has been modified by adding support for the following timestamp formats for the "AAA TM session logged out" events: • MM/dd/yyyy:HH:mm:ss z • MM/dd/yyyy:HH:mm:ss • yyyy/MM/dd:HH:mm:ss z • yyyy/MM/dd:HH:mm:ss **Note**: If users need support for the "dd/MM" format, they must obtain the override parser file from Customer Support.
F5 BIG-IP Syslog	The F5 BIG events for F5 BIG-IP Syslog connector were not being parsed. **Fix**: Added regex to handle the parsing issue of the events.
F5 BIG-IP Syslog	The source username of F5 BIG-IP logs for the F5 BIG-IP Syslog connector was getting parsed with closed parenthesis. **Fix**: Modified the regex to parse the source username.
Fortinet Fortigate Syslog	The **eventtime** field's value of the Fortinet Fortigate Syslog was mapped incorrectly to the **Device Receipt Time** field in the Fortigate parser. Because the **eventtime** field value was in nanoseconds for some customers and in seconds for other customers, the value was parsed into an incorrect date time format. In addition, customers were also not able to use the function '**Store Original Time In | Flex Date 1**' of the connector's destination setting. The function was displaying a random value and taking an incorrect timestamp. Therefore, an aggregation issue was encountered when piping the logs. **Fix**: This issue has been resolved by considering the first 10 digits of **eventtime** and converting it using epoch.

Application Modules Software Fixes	Description
IBM WebSphere File	The IBM WebSphere File connector was encountering parsing issues with timestamps in Websphere SystemOut logs. **Fix**: To fix this issue: • Added support for the following date formats in the parser: ○ M/dd/yy HH:mm:ss:SSS z ○ yyyy/M/dd HH:mm:ss:SSS z • Added support for the following Websphere SystemOut message types in the parser: ○ FISCSocketClientListener ○ PMRM0003I ○ ConfigFileHelper
• Linux Audit File • Linux Audit Syslog	For the **proctitle** type of logs, the value of the **proctitle** field was assigned to the **fileHash** field. However, the proctitle field value does not accurately represent the hash of the file, leading to a parsing issue. **Fix**: The decoded value of the **proctitle** has been mapped to **`Device Custom String 1`** to resolve the issue.
Load Balancer	Load Balancer was experiencing issues because of an elevated number of threads, leading to a crash. **Fix**: The following fixes have been implemented to resolve the issue: • A read timeout has now been implemented on the input stream to prevent blocking of threads after processing all the data. This fix has been applied to those customer environments where the end of the stream or fin packet was not being received. • The number of retry attempts for failed messages has now been limited to **5** when the destination is unavailable. However, once the destination becomes available, all new messages are redirected to it.
Load Balancer	Load Balancer was experiencing issues when the **Aggregation Preferred** routing policy was selected. **Fix**: The code that obtains the connector's statistics to determine its overload status has been fixed to solve the issue. Load Balancer now retrieves the connector statistics in case of overloading and relocates the events to a source that is away from the connector.
Load Balancer	The **`HTTP OPTIONS`** method was enabled for the Load Balancer server. **Fix**: The issue has been resolved by disabling the **`HTTP OPTIONS`** method in the Load Balancer.

Application Modules Software Fixes	Description
Microsoft 365 Defender	The new Microsoft 365 Defender Graph APIs were not parsing the events properly for the following ESM fields: • oldFileType • deviceExternalId • destinationHostName • oldFilePermission • sourceUserName • sourceNtDomain • healthStatus **Fix**: The parser has been modified to fix the parsing issue of these ESM fields.
Microsoft Azure Event Hub	The Microsoft schema for the Microsoft Azure Event Hub connector was changed, resulting in the Azure Diagnostic logs not being parsed. **Fix**: Code changes were made for the new schema to enable the parsing of the Azure Diagnostic logs.
Microsoft Azure Event Hub	The Azure Event Hub connector encountered the fatal exception error of **type mismatch**. This error occurred because the `durationMS` token was set to **string** instead of **long**. **Fix**: The issue has now been resolved by making changes in the parser to convert the value of the `durationMS` token to the **long** format. This will now successfully store the value to **deviceCustomNumber1**.
Microsoft Azure Event Hub	The Microsoft schema for the Microsoft Azure Event Hub connector was changed, resulting in the Azure Activity logs not being parsed. **Fix**: Code changes were made for the new schema to enable the parsing of the Azure Activity logs.
Microsoft DNS Trace Log Multiple Server File	The Microsoft DNS Trace Log Multiple Server File SmartConnector was receiving the following warning message when the **Answer Section** or **TTL** field was empty in the event sent from the DNS server: `[com.arcsight.agent.parsers.operation.regexTokenAsLongOperation] [getResult]No match between string [XID 0x9175 Flags 0x0100 QR 0 (QUESTION) OPCODE 0 (QUERY) AA 0 TC 0 RD 1 RA 0 Z 0 CD 0 AD 0 RCODE 0 (NOERROR) QCOUNT 1 ACOUNT 0 NSCOUNT 0 ARCOUNT 0 QUESTION SECTION: Offset = 0x000c, RR count = 0 Name "(2)uk(2)ng(3)msg (5)teams(9)microsoft(3)com(0)" QTYPE A (1) QCLASS 1 ANSWER SECTION: empty AUTHORITY SECTION: empty ADDITIONAL SECTION: empty] and regex [.*TTL\s+(\d+)\s+.*]` **Fix**: The parser has been modified to handle the cases when the **Answer Section** or **TTL** field is empty and now the exception is not being received in the **agent.log** file.

Application Modules Software Fixes	Description
Symantec Endpoint Protection Syslog	The following types of events for the Symantec Endpoint Protection Syslog connector were not being parsed: • Administrator logout • Virus found **Fix**: The parser has been modified to support the parsing of these events.
Syslog NG Daemon	The Syslog NG Daemon SmartConnector was unable to parse the Solaris server events. **Fix** : The parsers have been modified to support the parsing of Solaris server events for the following message IDs: corntab, sshd, su, ftpd, rlogind, xntpd, syslogd, Had, reboot, /lib/inet/nwamd, vdc, mac, ldap_cachemgr, svc.startd,bash, nfs, iscsiadm, llt, cacao_launcher, rexec, AgentFramework, vxvm, hotplugd, explorer, ing, perl, pkgserv, ansible-setup, and ansible-command
Syslog NG Daemon	The numerous events that were previously supported experienced issues with categorization as a result of modifications made to the **Device Event Class ID** field. **Fix**: The issue has been resolved by restoring the original value of the **Device Event Class ID** field for the impacted events.
• UNIX Login/Logout File • UNIX OS Syslog	The following types of events of RHEL 7.8.0 and 7.5.0 for both the UNIX Login/Logout File and UNIX OS Syslog connectors were not being parsed: • Start session • Close session **Fix**: Added new sub-messages to enable the parsing of these types of events.
• UNIX Login/Logout File • UNIX OS Syslog	The following events that are generated in RHEL versions 7.8.0 and 7.5.0 were not getting parsed: sshd, EARL-SW1_DFC3-1-EXCESSIVE_PARITY_ERROR, winbindd, ftpd, journal,DMI-2-NETCONF_SSH_CRITICAL, insights-client, systemd, IIB, setroubleshoot, postfix/sendmail, snmpd, SEL, pendsect, syslog-ng, rhsmd, systemd-logind, SMART_LIC-3-COMM_FAILED, abrt-hook-ccpp, abrt-server, internal-sftp, PKI-6-AUTOCERTFAIL,PKI-6-CERT_RENEW_AUTO, sendmail, root, crond, rhnsd, sasauth, sssd, subscription-manager, postfix/local, postfix/pickup, sssd_be, nmbd, su **Fix**: Added new sub messages and modified the existing ones in the parser.

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.2 (8.4.5) release:

- HPE HP-UX
- Juniper IDP Content Version 3676
- McAfee Network Security Manager 11.10.14.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1786
- TippingPoint SMS IPS DV9874
- Trellix Data Loss Prevention 11.10

For more information, see Event Content-Categorization updates February 2024 in the Release Notes for ArcSight Content AUP - Categorization Updates 2024.

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 24.2 (8.4.5) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.5.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.5.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.5.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.5.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.5.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.5.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.5.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.5.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.5.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.5.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.5.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.5.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.

ArcSightSmartConnectorLoadBalancer-opensource-8.4.5.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.5.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.5.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.2 (8.4.5)

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 15.

Upgrading SmartConnector to CE 24.2 (8.4.5)

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 24.2 (8.4.5)

For information about upgrading Load Balancer to CE 24.2 (8.4.5), 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
Amazon S3	**Connector displays an error while processing digest files in the Amazon S3 bucket** While processing the CloudTrail events, if digest files are present in the S3 bucket, the connector displays a fatal exception stating, **Not a CloudTrail log**. **Workaround:** Disable the digest events from the S3 bucket where the CloudTrail events are streamed, and delete the existing digest events folder.

All SmartConnectors

SmartConnector remote connections fail due to low entropy

> **Note**: The CTH is supported in this release and are deprecated as of 8.4. **CTH functionality will be removed in an upcoming release, by March 31, 2024**

All SmartConnectors 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 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 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 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 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 365 Defender	**Command Line installation of the Microsoft 365 Defender SmartConnector mandates 'Certificate Path' value for the 'Shared Secret' authentication method** While installing the Microsoft 365 Defender SmartConnector from the command line, if the authentication method selected is **Shared Secret**, the connector installation script treats the optional **Certificate Path** parameter as mandatory, and therefore does not proceed with the installation if the parameter has no value. **Workaround**: Install the Microsoft 365 Defender SmartConnector by using the installation wizard. OR You can enter any sample value for the **Certificate Path** parameter to proceed with the installation.
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 24.2 Documentation page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	01/2027	The CTH and Collectors were deprecated with the SmartConnector release of 8.4. **Deployment of CTH and Collectors is now removed in CE 24.2**. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector CE 24.1 release, which is Jan 31, 2027.
Microsoft Azure Monitor Event Hub	04/2027	The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector. The Microsoft Azure Monitor Event Hub connector **will not be shipped after April 2025**. Therefore, it is highly recommended to switch to the Microsoft Azure Event Hub SmartConnector before April 2025.

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 24.2)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!