



ArcSight SmartConnectors

Software Version: CE 24.3

SmartConnector Release Notes

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

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

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

- Release Highlights 4

- What's New 5
 - New SmartConnectors and Modules 5
 - Cloud Updates 6
 - Security Updates 6
 - Version Updates 7
 - Platform Support 7
 - SmartConnector Enhancements 8
 - Software Fixes 8
 - Event Categorization Updates 12

- SmartConnector Parser Support Policy 14

- Installing SmartConnectors 15
 - System Requirements 15
 - Downloading the SmartConnector Installation Packages 15

- Upgrading SmartConnectors 18
 - Upgrading to CE 24.3 (8.4.6) 18
 - Deleting Older Vulnerable Libraries after Upgrading a Connector 18

- Known Issues 21

- Connector End-of-Life Notices 32
 - SmartConnector End of Support Announcements 32
 - SmartConnectors No Longer Supported 32

- Send Documentation Feedback 34

Release Highlights

The SmartConnector CE 24.3 (8.4.6) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- New [SmartConnector for Integrated Dell Remote Access Controller \(iDRAC\) Syslog](#)
- Certified parser for [Cisco IronPort Web Security Appliance Syslog](#) version 12.5.5
- Certified parsers for the [Cisco IronPort Email Security Appliance Syslog \(AMP\)](#) and the [Cisco IronPort Email Security Appliance File \(AMP\)](#) version 14.3.0
- Certified [Microsoft Network Policy Server File](#) for Microsoft Windows Server 2022
- Certified parsers for , [Apache Tomcat File](#), [Apache HTTP Server Error File](#), and [Apache HTTP Server Access Multiple File](#) version 9.0.56
- Certified parser for [RedHat JBoss Security Audit Multiline](#) version 4.3.0 GA_CP03_EAP
- Support for the 'Octet-Counting Framing' mode standard for the RFCs 6587 event formats
- Support for the following [Microsoft Azure Event Hub](#) resource logs modules:
 - App Service HTTP Logs
 - App Service IP Sec Audit Logs
- Added support for the following [Trellix Endpoint Security modules](#):
 - Trellix MOVE Antivirus 4.1
 - McAfee Security for Microsoft Exchange (MSME) 8.8
 - Data Loss Prevention Administrative 11.x
 - Trellix Agent 5.7
- Upgrade of Zulu OpenJDK to 8u412
- Upgrade of Tomcat version to 9.0.89

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 our 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 24.3 (8.4.6) 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
Integrated Dell Remote Access Controller (iDRAC)	<p>The SmartConnector for Integrated Dell Remote Access Controller (iDRAC) Syslog receives logs from iDRAC and converts them to CEF format.</p> <p>iDRAC is a hardware component found in Dell servers. It is a remote management and monitoring tool that allows administrators to manage and monitor Dell servers remotely, even when the server is offline or in a non-operational state.</p> <p>For more information, see Configuration Guide for Integrated Dell Remote Access Controller (iDRAC).</p>
Microsoft Azure Event Hub	<p>Added support for the following Azure Event Hub resource logs modules:</p> <ul style="list-style-type: none">• App Service HTTP Logs• App Service IP Sec Audit Logs <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in the Configuration Guide for Microsoft Azure Event Hub SmartConnector.</p>

New SmartConnectors/Application Module	Description
Trellix ePolicy Orchestrator DB	<p>Added support for the following Trellix Endpoint Security modules:</p> <ul style="list-style-type: none">• Trellix MOVE Antivirus 4.1• McAfee Security for Microsoft Exchange (MSME) 8.8• Data Loss Prevention Administrative 11.x• Trellix Agent 5.7 <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in the Configuration Guide for Trellix ePolicy Orchestrator DB SmartConnector.</p>

Cloud Updates

No updates at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.89.
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u412.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none">• CVE-2023-41993• CVE-2024-21011• CVE-2024-21068• CVE-2024-21085• CVE-2024-21094• CVE-2024-21003• CVE-2024-21005• CVE-2024-21002• CVE-2024-21004

Version Updates

Application Module Version Updates	Description
<ul style="list-style-type: none">Apache Tomcat FileApache HTTP Server Error FileApache HTTP Server Access Multiple File	Certified parsers for Apache Tomcat File, Apache HTTP Server Error File, and Apache HTTP Server Access Multiple File version 9.0.56.
<ul style="list-style-type: none">Cisco IronPort Email Security Appliance Syslog (AMP)Cisco IronPort Email Security Appliance File (AMP)	Certified parsers for Cisco AMP logs for Cisco IronPort Email Security Appliance Syslog and Cisco IronPort Email Security Appliance File version 14.3.0.
Cisco IronPort Web Security Appliance Syslog	Certified parser for Cisco IronPort Web Security Appliance Syslog version 12.5.5.
JBoss Security Audit File	Certified parser for RedHat JBoss Security Audit Multiline version 4.3.0 GA_CP03_EAP.
Microsoft Network Policy Server File	Added support for Microsoft Network Policy Server File for Microsoft Windows Server 2022.

Platform Support

No updates at this time.

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
All SmartConnectors	All the previous clear text passwords have now been encrypted and the new passwords can be specified in the agent.properties file using the .encrypted property extension.
Syslog NG Daemon	<p>Added support for the Octet-Counting Framing mode standard for the RFCs 6587 event formats.</p> <p>The new property syslog.framing.type is added in the agent.defaults.properties file of the Syslog connectors to support the Octet-counting enabled syslog messages.</p> <p>For more information, see RFC Compliance Support and Installing the SmartConnector to Use the Raw TCP or UDP Protocol in the Configuration Guide for Syslog NG Daemon SmartConnector.</p>

Software Fixes

The following issues are fixed in the CE 24.3 release:

Application Modules Software Fixes	Number	Description
All SmartConnectors	OCTCR33I883014	<p>The connector repeatedly generated an internal event called Event Transport Fail Over with the Device Event Class ID of agent:51 , even though no destination failover occurred.</p> <p>Fix: The issue has been fixed to ensure that the internal event is generated only when a destination failover occurs.</p>
All SmartConnectors	OCTCR33I889075	<p>The following warning messages were displayed in the connector’s log file because of the duplicate entries in one of the internal configuration files:</p> <pre>[WARN][com.arcsight.agent.cx.b] [loadLookUpTable]Duplicate Unique Id [GEMALTO SAFENET PROTECTDB] near tokens [[Gemalto, SafeNet ProtectDB, Content Security]] at line [278] found, ignoring [WARN][com.arcsight.agent.cx.b] [loadLookUpTable]Duplicate Unique Id [HP TIPPINGPOINT NEXT GENERATION FIREWALL] near tokens [[HP TippingPoint, Next Generation Firewall, Firewall]] at line [288] found, ignoring</pre> <p>Fix: The issue has been fixed by removing the duplicate entries in the configuration file.</p>
<ul style="list-style-type: none"> • Apache Tomcat File • Apache HTTP Server Error File 	OCTCR33I863046	<p>The events for the following modules of Apache Tomcat File and Apache HTTP Server with version 9.0.56 were not getting parsed:</p> <ul style="list-style-type: none"> • localhost • Catalina • localhost access <p>These modules utilize the Apache Tomcat File and Apache HTTP Server Error File connectors for parsing.</p> <p>Fix: Modified the parser to resolve the issue.</p>

Application Modules Software Fixes	Number	Description
AWS CloudTrail	OCTCR33I871053	<p>When the AWS CloudTrail connector received CloudTrail logs with IPv6 values, the Source Address field remained empty.</p> <p>Fix: Modified the mapping of the Source Address field in the parser to resolve the issue.</p>
AWS Security Hub	OCTCR33I534008	<p>The AWS Security Hub connector was unable to parse the JSON format logs that contained line feed characters such as \n, because the logs were fragmented into multiple lines.</p> <p>Fix: This issue has been fixed.</p>
Cisco IronPort Web Security Appliance Syslog	OCTCR33I685003	<p>The Destination Port field of the Cisco IronPort Web Security Appliance Syslog connector was empty and not being parsed.</p> <p>Fix: To fix this issue:</p> <ul style="list-style-type: none"> • Added support for the Cisco IronPort Web Security Appliance Syslog version 12.5.5 logs. • Modified the parser for the 12.5.5 version wherein the port number is extracted from the URL and populated in the Destination Port field. Now, the Destination Port field is not empty.
Cisco PIX/ ASA Syslog	OCTCR33I900239	<p>The Cisco PIX/ ASA Syslog SmartConnector was unable to parse events containing the following message IDs:</p> <p>109201, 109202, 109203, 109204, 109205, 109206, 109207, 109208, 109209, 1092010, 1092011, 1092012, and 109213</p> <p>Fix: The parser has been updated with the regex to parse session-based authentication logs of Cisco Secure PIX Firewall with the message ids from 109201 to 109213.</p>

Application Modules Software Fixes	Number	Description
F5 BIG-IP Syslog	OCTCR33I883013	<p>The User Agent value for the tmm module for the F5 BigIP logs was incorrectly mapped to an additional data field of the F5 BIG-IP Syslog connector.</p> <p>Fix: The mapping has been modified to fix this issue. Now, the User Agent value is getting correctly mapped to the Request Client Application field as expected.</p>
Fortinet Fortigate Syslog	OCTCR33I876081	<p>The Fortinet Fortigate Syslog connector was facing parsing issues with the bandwidth token because the values of the bandwidth field were getting mapped to the bytesin and bytesout fields.</p> <p>Fix: The mappings have been modified to fix this issue. Now, the bandwidth field is getting mapped to the additionaldata fields. For more information about the additionaldata fields, see the FortiGate Event Mappings table in Configuration Guide for Fortinet FortiGate Syslog SmartConnector.</p>
Infoblox NIOS Syslog	OCTCR33I901220	<p>The events of the Infoblox NIOS Syslog module were not being parsed</p> <p>Fix: Added new sub-messages to handle the parsing issue.</p>
Microsoft Azure Event Hub	OCTCR33I826024	<p>The Microsoft Azure Event Hub connector encountered the following fatal exception when the events (such as metric data) did not contain the category field:</p> <pre>[ERROR][com.arcsight.agent.ee.f] [getJsonParser]Unable to initialize Json Parser for category [resource], file [ul]</pre> <p>Fix: Added the following warning message in the agent.log file when the category field is not found in the Azure Event Hub logs:</p> <p>"The received events do not match SmartConnector supported log format from Azure Event Hub, Event will be skipped."</p>

Application Modules Software Fixes	Number	Description
Microsoft Azure Event Hub	OCTCR33I883062	<p>Microsoft Azure Event Hub diagnostic logs were not getting parsed.</p> <p>Fix: Added support for the following Azure Event Hub resource logs modules:</p> <ul style="list-style-type: none"> • App Service HTTP Logs • App Service IP Sec Audit Logs <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in Configuration Guide for Microsoft Azure Event Hub SmartConnector.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I873076	<p>The Pulse Secure events that are generated from the Pulse Secure device version 9.1R18 were getting parsed as Unix events because of an extra set of square brackets in the message.</p> <p>Fix: Updated the parser containing the regex to enable the parsing of the pulse secure events.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I647077	<p>The Pulse Secure events that are generated from the Pulse Secure device versions 9.1R14.1 and 9.1R16.2 were not getting parsed.</p> <p>Fix: Updated the parser containing the regex to enable the parsing of the pulse secure events.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I901108	<p>The Pulse Secure events generated from the Pulse Secure device version 9.1R18.5 were not getting parsed. The parsing issue started where the events were displayed as Unix events and showed only "su failed".</p> <p>Fix: Modified the base regex to parse all the logs of each module of the Pulse Secure device version 9.1R18.5.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.3 (8.4.6) release:



Note: From May 2024 onwards, a new Category named **DDoS** has been introduced under Techniques.

- Fortinet Fortigate 5.2 Content 3.086
- Juniper IDP Content Version 3703
- McAfee Network Security Manager 11.10.14.4
- Microsoft AzureActiveDirectory
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1847
- TippingPoint SMS IPS DV9899

For more information, see [Event Content-Categorization updates May 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 24.3 (8.4.6) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.6.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.6.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.6.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.6.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.6.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.6.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.6.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.6.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.6.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.6.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.6.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.6.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.

SmartConnector Release Notes

Installing SmartConnectors

ArcSightSmartConnectorLoadBalancer-opensource-8.4.6.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.6.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.6.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.3 (8.4.6)



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 24.3 (8.4.6)

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 24.3 (8.4.6)

For information about upgrading Load Balancer to CE 24.3 (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
Microsoft Azure Monitor Event Hub	<p>The certs folder does not get created after deploying the Azure Monitor Event Hub connector</p> <p>After a new deployment of the Azure Monitor Event Hub, the certs folder is not created in the following location:</p> <p>Storage accounts > <Storage account name> > Data Storage > File shares > <function app name> > <function app name>.</p> <p>Workaround</p> <p>To fix this issue:</p> <ol style="list-style-type: none">1. After the deployment of the new connector, go to the newly created storage account.2. In the navigation pane, click Settings > Configuration.3. In the Allow Blob anonymous access option, click Enabled and then click Save.4. Run the <code>DeployFunction.ps1</code> file again.5. At the command prompt, "The deployment already exists. Do you want the installation to verify and update the resources? Y/N," enter Y and press ENTER. <p>After the deployment process is completed, the certs folder will be created.</p>

All SmartConnectors	<h3>SmartConnector Services are not restarting automatically when the server is restarted</h3> <p>When the SmartConnector is installed as a service and the sever is restarted, the SmartConnector service does not start automatically even though the Start the service automatically option is set to Yes. This issue is reproducible in RHEL 9.x and Rocky Linux 9.x.</p> <h4>Workaround</h4> <p>To keep the SmartConnector service running automatically after the server is restarted:</p> <ol style="list-style-type: none">1. Install the chkconfig package as a root user: <pre>yum install chkconfig</pre> <div data-bbox="480 621 1414 806" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f9f9f9;"> Note: You might encounter the error “unpacking rpm package error” when installing the chkconfig package. For more information, see Issue while installing the chkconfig package. Make sure that you read through it all before installing chkconfig.</div> <ol style="list-style-type: none">2. Install the SmartConnector as a root user. Ensure that you have set the Start the service automatically option to Yes.3. Run the following command: <pre>chcon system_u:object_r:bin_t:s0 /etc/init.d/service_name</pre><p>This command changes the security context of the /etc/init.d/service_name file to system_u:object_r:bin_t:s0.</p><p>The chcon command is used to change the SELinux security context of a file.</p> <h3>Issue while installing the chkconfig package</h3> <p>When the chkconfig package is installed, it fails with the following error message: “Error unpacking rpm package”</p> <h4>Root Cause</h4> <ul style="list-style-type: none">• The /etc/init.d directory was created in system during the installation of some third-party applications.• Later on, when you install the chkconfig package, the system attempts to create a symbolic link /etc/init.d and point to /etc/rc.d/init.d.• Because the /etc/init.d/ directory already exists , the installation of the chkconfig package fails because the system is unable to create the symbolic link for the installation. <h4>Workaround</h4> <p>Remove the /etc/init.d directory or any other '/etc/rc*' directories (except rc.d) or move it to the other location by running either of the following commands:</p> <ul style="list-style-type: none">• <pre># rm -rf /etc/init.d/</pre>• <pre># mv /etc/init.d /tmp/init.d.bk</pre>
------------------------	---

Note: An error occurs if the cleanup is not appropriate. Therefore, the **chkconfig** package might end up creating a file with the wrong name instead of **init.d**:

```
[root@rhel192 ~]# ls -l /etc/ | grep init.d
drwxr-xr-x. 2 root root 6 Apr 5 12:42 init.d
lrwxrwxrwx. 1 root root 11 May 23 2023 init.d;660f733f -> rc.d/init.d <==
```

In such cases, remove the file manually:

```
# rm init.d\;660f733f
```

Diagnostic Steps

- Check if the content of chkconfig RPM already exists as directories. The links appear as follows:

```
# ll /etc/rc*
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc0.d -> rc.d/rc0.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc1.d -> rc.d/rc1.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc2.d -> rc.d/rc2.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc3.d -> rc.d/rc3.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc4.d -> rc.d/rc4.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc5.d -> rc.d/rc5.d
lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc6.d -> rc.d/rc6.d
lrwxrwxrwx. 1 root root 13 Aug 22 2023 /etc/rc.local -> rc.d/rc.local
# ll /etc/init.d
lrwxrwxrwx. 1 root root 11 May 23 2023 /etc/init.d -> rc.d/init.d
```

- Get a **strace** of the **yum** command and analyze the **strace** output:

```
strace -fttVvy -s 1024 -o /tmp/yum_install_chkconfig.out yum install
chkconfig -y
```

From the **strace** output, the following error can be found because the **/etc/init.d** directory already existed and the system was unable to create the symbolic link for the installation:

```
error: unpacking of archive failed on file /etc/init.d: cpio: File from
package already exists as a directory in system
```

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	<h3>SmartConnector remote connections fail due to low entropy</h3> <p>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</p> <p>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.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none">1. Install the <code>rng-tools</code> package: <code>sudo yum install -y rng-tools</code>2. Add the following line to the <code>/etc/sysconfig/rngd</code> file: <code>EXTRAOPTIONS="-r /dev/urandom"</code>3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code>4. Start the <code>rngd</code> package as a root user: <code>service rngd start</code>5. Enable the <code>rngd</code> service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code>6. Ensure that the <code>rngd</code> package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code>7. Check the entropy availability in the system, after starting the <code>rngd</code> service: <code>cat /proc/sys/kernel/random/entropy_avail</code> <h3>Unable to install connector because of missing packages</h3> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none">1. <code>yum install -y unzip</code>2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>
------------------------	--

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

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

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the <code>rng-tools</code> on the corresponding Linux OS.</p> <p>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.</p> <p>To install and configure the <code>rng-tools</code> package after a fresh install, follow the steps mentioned for SmartConnector remote connections fail due to low entropy.</p> <p>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</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p>Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <pre>sudo yum install -y python2</pre>2. Create a symlink by the following command: <pre>sudo ln -s /usr/bin/python2 /usr/bin/python</pre>3. Install the libselinux-python package by the following command: <pre>sudo yum install -y libselinux-python</pre> <p>Note: If the <code>yum</code> command fails when installing <code>libselinux-python</code>, the <code>rpm</code> 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</p>
-------------------------------	---


<p>CyberArk Privileged Access Security</p>	<p>Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)</p> <p>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.</p> <p>Workaround</p> <p>To address this issue, request modifications to the log format as 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.</p>
<p>IBM Big Fix REST API</p>	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file:</p> <p>"E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <p>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</p>
<p>Microsoft 365 Defender</p>	<p>Command Line installation of the Microsoft 365 Defender SmartConnector mandates 'Certificate Path' value for the 'Shared Secret' authentication method</p> <p>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.</p> <p>Workaround:</p> <p>Install the Microsoft 365 Defender SmartConnector by using the installation wizard.</p> <p>OR</p> <p>You can enter any sample value for the Certificate Path parameter to proceed with the installation.</p>
<p>Microsoft Message Trace REST API</p>	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>

<p>Microsoft Windows Event Log (WiSC)</p>	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. it has the following issues:</p> <ul style="list-style-type: none"> • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). • Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>
<p>Microsoft Windows Event log - Native</p>	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT_HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents[0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
<p>Microsoft Azure Monitor Event Hub</p>	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	Load Balancer arc_conn1b service does not start and displays an error message
	<p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_conn1b service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_conn1b service manually.</p>
	<p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop.</p>
	<p>Perform the following steps to fix this issue:</p>
	<p>1. After you install Load Balancer as a service, before you upgrade, stop the arc_conn1b service by using the following command:</p>
	<pre># /etc/init.d/arc_conn1b stop</pre>
	<p>or</p>
	<pre>service arc_conn1b stop</pre>
	<p>2. After Load Balancer is successfully upgraded, start the arc_conn1b service by using the following command:</p>
	<pre># /etc/init.d/arc_conn1b start</pre>
	<p>or</p>
	<pre>service arc_conn1b start</pre>

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

Connector End-of-Life Notices

 **Note:** For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 24.3 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	01/2027	<p>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.</p> <p>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.</p>
Microsoft Azure Monitor Event Hub	01/2027	<p>The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector.</p> <p>The Microsoft Azure Monitor Event Hub connector will not be shipped after January 2025. Therefore, it is highly recommended to switch to the Microsoft Azure Event Hub SmartConnector before January 2025.</p>

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.

SmartConnector Release Notes
Connector End-of-Life Notices

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 24.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!