opentext™

ArcSight SmartConnectors

Software Version: CE 24.4.1

SmartConnector Release Notes

Document Release Date: November 2024
Software Release Date: November 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

Documentation Updates

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

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

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

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

Contents

Release Notes for ArcSight SmartConnector CE 24.4.1 4

Release Highlights 6

What's New 7

- Security Updates 7
- Software Fixes 7
- Event Categorization Updates 9

Known Issues 11

Downloading and Applying the Patch 12

- Deleting Older Vulnerable Libraries after Upgrading a Connector 12

Send Documentation Feedback 15

Release Notes for ArcSight SmartConnector CE 24.4.1

This Release Notes document describes how to apply this latest release of ArcSight SmartConnector and ArcSight SmartConnector Load Balancer, and provides other information about the most recent changes, known limitations, and software fixes.

SmartConnector is an application that collects log messages from log sources, processes them into ArcSight security events, and transports them to destination consumers for analytic, storage, and compliance reporting.

You can apply SmartConnectors CE 24.4.1 (8.4.7.P1) to:

- Perform a fresh install of the SmartConnectors.
- Upgrade the SmartConnectors from SmartConnectors 8.x to any later versions. For example, you can directly upgrade from version 8.2 to 8.4.7.P1.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Release Highlights

The SmartConnector CE 24.4.1 (8.4.7.P1) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Upgrade of Zulu OpenJDK to 8u432.
- Software fixes for Microsoft 365 Defender, Syslog NG Daemon, and all SmartConnectors.

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

SmartConnectors CE 24.4.1 (8.4.7.P1) incorporates the following SmartConnector updates:

- Security Updates
- Software Fixes
- Event Categorization Updates

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u432. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: • CVE-2023-42950 • CVE-2024-25062 • CVE-2024-21235 • CVE-2024-21208 • CVE-2024-21210 • CVE-2024-21217

Software Fixes

The following issues are fixed in the CE 24.4.1 (8.4.7.P1) release:

Application Modules Software Fixes	Number	Description
All SmartConnectors	NA	This patch release resolves a known issue wherein custom passwords that are stored in plain text are lost when you upgrade the SmartConnector from version 24.2 (8.4.5) or earlier to version 24.3 (8.4.6) or later and then start the SmartConnector. For more information about this issue, see the Known Issues section in ArcSight SmartConnector Release Notes CE 24.4. **Fix**: This issue has been resolved. Custom passwords stored in plain text for the keystore, truststore, or remote management are now retained and encrypted during the upgrade process. These passwords are stored in the corresponding property appended with the suffix **.encrypted** in the **agent.properties** file. For example: If you have the following property before upgrade: `remote.management.ssl.key.password=<custom password in clear text>` After upgrading the SmartConnector to 24.4.1(8.4.7.P1) or later, it will be replaced with the following encrypted password property: `remote.management.ssl.key.password.encrypted=<encrypted custom password>` For more information, see the Password Management section in ArcSight SmartConnector Installation Guide
Microsoft 365 Defender	OCTCR33I941067	The Microsoft 365 Defender connector was receiving an incomplete response when the **mdeDeviceId** field was null. **Fix:** The logic has been updated to make sure the complete response is returned when the **mdeDeviceId** field is null.

Application Modules Software Fixes	Number	Description
Microsoft 365 Defender	OCTCR33I941068	The connector was unable to parse the complete JSON object because it encountered multiple instances of the "evidence" objects or attributes in the original JSON result. This resulted in the loss of data. **Fix:** Added a regex to fix this issue.
Microsoft 365 Defender	OCTCR33I956110	The SmartConnector for Microsoft 365 Defender did not parse all the data related to security for the Graph API alert type. **Fix:** The issue has been fixed. The following are the fixes: • The following mappings have been added to the Device Evidence events: **lastExternalIpAddress**, **lastIpAddress**, **ipInterfaces**, **loggedOnUsers** (**accountName** and **domainName**). • The parser file has been updated to parse a new event type **analysedMessageEvidence**. For more information about the Device Evidence events and the new event type, see Configuration Guide for Microsoft 365 Defender SmartConnector
Syslog NG Daemon	NA	The Syslog NG Daemon connector was unable to receive events, encountering multiple instances of the CLOSE_WAIT status over the TCP communication. **Fix**: The code has been modified to close the TCP connection if a broken pipe error occurs. An additional check has also been implemented to ensure the detection of an invalid connection.

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.4.1 (8.4.7.P1) release:

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

- CISCO Pix 6.3
- Juniper IDP Content Version 3757
- Palo Alto Networks PAN-OS 11.2
- Snort 3.0
- Sourcefire SEU 31470

- Symantec Network Security 7100 1972
- TippingPoint SMS IPS DV9967

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

Known Issues

This section contains issues that are identified in 24.4.1 patch release.

Application Module	Description
All SmartConnectors	In the FIPS mode, the connection to a destination failed when different custom passwords were set for the keystore, truststore, and remote management properties. **Workaround:** Set the same custom password for the keystore, truststore, and remote management files and then update the same password for the corresponding properties in the **agent.properties** file.

Downloading and Applying the Patch

Download the appropriate executable for your platform from the Software Licenses and Downloads (SLD).

The 64-bit executable is available for download for Windows and Linux platforms. Only the 64-bit executable is available for Solaris platforms. Users should move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides available on the ArcSight Documentation website.

To apply the patch for:

- SmartConnectors, see Upgrading SmartConnectors.
- Load Balancer, see the Upgrading Load Balancer section in *Configuration Guide for SmartConnector 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.

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 24.4.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!