Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3 Patch 3

Release Notes

Document Release Date: July 2022
Software Release Date: July 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

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

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

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

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Release Notes for ArcSight SmartConnector 8.3 Patch 3

This Release Notes document lists SmartConnectors for which patch changes have been made. It also describes steps to apply the current ArcSight SmartConnector patch release and provides other information about recent changes, enhancements, and software fixes.

This patch release contains cumulative updates from SmartConnector 8.3 Patch 1, SmartConnector 8.3 Patch 2, SmartConnector 8.3.1, and SmartConnector 8.3.2.

Note:

- SmartConnector 8.3 Patch 1 was a SaaS only release.
- The software fixes handled in the SmartConnector 8.3 Patch 2 release have been integrated into the SmartConnector 8.3.1 release.

You can apply 8.3 Patch 3 to:

- perform a fresh install of the SmartConnector.
- upgrade the SmartConnector from 8.2 or 8.3.

You can access the additional documents from the Micro Focus Product Documentation website.

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:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provide information about configuring SmartConnectors to collect events from different sources.

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

What's New in this Release

This patch update has been certified with SmartConnector Framework release 8.3.

Important: If you use any of the SmartConnectors listed in the "Software Fixes" sections, note that installing the updated SmartConnector can impact your created content.

SmartConnector 8.3 Patch 3

This patch release contains cumulative updates from SmartConnector 8.3 Patch 1, SmartConnector 8.3 Patch 2, SmartConnector 8.3.1, and SmartConnector 8.3.2.

Support for New Devices and Version Updates

SmartConnector for	Description
All DB Connectors using PostgreSQL JDBC Driver	Upgraded PostgreSQL JDBC version to 42.4.0.

SmartConnector Enhancements

None at this time.

Software Fixes

SmartConnector for	Octane ID	Description
ArcSight FlexConnector JSON Multiple Folder Follower	OCTCR33I281810	The JSON events were sent to a destination without being parsed. **Fix**: Now, the JSON events are parsed before being sent to the destination.
Windows Event Log - Native (WiNC)	OCTCR33I283741	The connector was unable to receive events from the hosts when one or more hosts were down. **Fix**: The `EventLogManager.cs` file has been modified to fix this issue.
Windows Event Log - Native (WiNC)	OCTCR33I427156	The authorization error was displayed and the Windows account was getting locked out when the incorrect password was entered multiple times. **Fix**: The issue has been fixed.

SmartConnector 8.3 Patch 2

This patch release contains cumulative updates from SmartConnector 8.3 Patch 1.

Support for New Devices and Version Updates

SmartConnector for	Description
All SmartConnectors and Load Balancer	• Upgraded Tomcat version to 9.0.62. • Upgraded Zulu OpenJDK to 8u332. • Upgraded Apache Log4j library version to 2.17.2.

SmartConnector Enhancements

SmartConnector for	Description
Microsoft Azure Monitor Event Hub	The Microsoft product name **Azure Security Center** has now been rebranded as **Microsoft Defender for Cloud**. For more information, see Configuration Guide for Microsoft Azure Monitor Event Hub.
Microsoft Azure Monitor Event Hub	All Microsoft support and development for the Azure Active Directory Authentication Library (ADAL), including security fixes, ends in December, 2022. The authorization functionality has now been migrated to Microsoft Authentication Library (MSAL) for token retrieval and authentication in the Azure Monitor Function application.
Microsoft Azure Monitor Event Hub	The upgrade scenario has been enhanced by modifying the PowerShell script. For more information, see *Step 7* of the Upgrading the Connector section in *Configuration Guide for Microsoft Azure Monitor Event Hub*.
Microsoft Azure Monitor Event Hub	The PowerShell script has been enhanced to verify that the key properties exist and contain appropriate values.

Software Fixes

SmartConnector for	Description
Microsoft Azure Monitor Event Hub	The Azure Monitor Function application was unable to start or stop the Cloud Function application. **Fix**: The Azure Monitor Function application requires the Contributor role on the resource group to start or stop the Cloud Function application. To assign the Contributor role, ensure that the user deploying the cloud Connector has the Owner role on the resource group. For more information, see the Setting User Permissions in Azure section in *Configuration Guide for Microsoft Azure Monitor Event Hub*.
Syslog NG Daemon	When the Linux Auditd event merging is enabled and the **Generate Unparsed Events** parameter is set to **Yes**, the Linux Auditd events were sent as unparsed events along with the parsed merged events. **Fix**: This issue has been fixed. The unparsed events are no longer sent with the parsed merged events.

SmartConnector 8.3 Patch 1

This patch release contains the following updates:

Note: SmartConnector 8.3 Patch 1 is a SaaS only release.

Support for New Devices and Version Updates

None at this time.

SmartConnector Enhancements

None at this time.

Software Fixes

SmartConnector for	Description
All Connectors (configured with Amazon S3 Destination)	The Connector was unable to upload AVRO files to Recon SaaS S3 bucket, even though the Connector service was up and running. **Fix**: The Connector is now able to upload AVRO files to Recon SaaS S3 bucket.

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 Micro Focus Product Documentation website.

To apply the patch for:

- The Microsoft Azure Monitor Event Hub SmartConnector, see Upgrading the Connector.
- The Syslog NG Daemon SmartConnector and other SmartConnectors, see Upgrading SmartConnectors.
- Load Balancer, see the Upgrading Load Balancer to 8.3 section in *Release Notes for ArcSight SmartConnector 8.3*.

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 Release Notes (SmartConnectors 8.3 Patch 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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!