Micro Focus Security ArcSight SmartConnector

Software Version: 8.3.3

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 Parsers

This Release Notes document lists SmartConnectors for which parser changes have been made. It also describes the procedure to apply the latest ArcSight SmartConnector parser release and provides other information about recent changes and open and closed issues (generated by various vendor devices) to the ArcSight ESM Manager, Logger, Transformation Hub, Recon, and other destinations.

Important: The 8.3 patch overwrites parser updates or Parser Override. If you want to install the latest patch, then you must install it before you install the parser updates. If any parser override is present, you can test the upgrade in a STAGE (staging) to ensure it works as expected before you upgrade your PROD (production) environment.

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 every SmartConnectors release, various security fixes, feature updates, and bug fixes are made to the field mappings for individual SmartConnectors.

Important: If you use any of the SmartConnectors listed, be aware that installing the updated SmartConnector can impact your created content.

SmartConnector 8.3.3

Support for New Devices or Version Updates

SmartConnector for	New Device, Component, or OS Version
Check Point Syslog	Added support for the following Check Point R81 modules: • DLP • Forensics Added support for the following Check Point R80.40 module: • Application Control Content Awareness • Application Control URL Filtering Content Awareness • CloudGuard IaaS • Content Awareness • SmartDefense VPN-1 & FireWall-1 • URL Filtering Content Awareness • URL Filtering VPN-1 & FireWall-1 • VPN-1 & FireWall-1 Application Control • VPN-1 & FireWall-1 Content Awareness • VPN-1 & FireWall-1 URL Filtering • WEB_API
Microsoft Windows Event log - Native	Added support for the following modules of Windows Server 2022: • Microsoft-Windows-Security-Auditing • Service Control • NPS
AWS Security Hub	Added support for Macie Services.

Software Fixes

SmartConnector for	Description
Infoblox NIOS Syslog	The Infoblox 8.4 events for Infoblox NIOS Syslog were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.
Microsoft Office 365 Management Activity	Some of the events for Microsoft Office 365 Management Activity were unable to parse a few additional fields. **Fix**: Added token and mapping support for the additional fields to improve the parsing capability.
F5 BIG-IP Syslog	The F5 BIG-IP Syslog logs were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.
IBM AIX Audit Syslog	The IBM AIX 7.2 logs were not being parsed. **Fix**: Added new sub-message regex to handle the unparsed events.
Pulse Secure Pulse Connect Secure Syslog	The Pulse secure events were not being parsed. **Fix**: Modified the sub-message regex to handle the unparsed events.

SmartConnector 8.3.2

Support for New Devices or Version Updates

SmartConnector for	Description
VMware ESXi Server Syslog	Added support for the following VMWare ESX 7.0 modules: • apiForwarder • cfgAgent • esxtokend • fdm • hostd • kmxa • localcli • nestdb-server • nsxavim • nsx-exporter • nsx-opsagent • nsx-proxy • nsx-sfhc • nsx-sha • osfsd • smartd • vmkwarning • Vpxa • VSANMGMTSVC
Check Point Syslog	Added support for the following Check Point R81 modules: • New Anti Virus • Threat Extraction • Anti-Bot • Content Awareness • Identity Awareness

Software Fixes

SmartConnector for	Description
Symantec Endpoint Protection DB	All the Symantec Endpoint Protection DB events were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.
Fortinet Fortigate Syslog	The Fortinet Fortigate Syslog event keys were not being parsed. **Fix**: The regex associated with **additionaldata.ui** has been modified to handle the unparsed events.
UNIX OS Syslog	The Solaris events for UNIX OS Syslog were not being parsed. **Fix**: Added new submessages to handle the unparsed events.
Microsoft DNS DGA Trace Log Multiple Server File	Some of the events for Microsoft DNS DGA Trace Log Multiple Server File were unable to handle timestamp. **Fix**: Added a new regex to handle the timestamp.

SmartConnector 8.3.1

Support for New Devices or Version Updates

SmartConnector for	New Device, Component, or OS Version
AWS Security Hub	Added support for IAM Access Analyzer Service.
Check Point Syslog	Added support for the following Check Point R81 modules: • Anti-Malware • Application Control • System Monitor • VPN-1 & FireWall-1 • HTTPS Inspection • Security Gateway/ Management • Smart Console • Smart Defense • URL Filtering • Threat Emulation

SmartConnector for	New Device, Component, or OS Version
VMware ESXi Server Syslog	Added support for the following VMWare ESX 7.0 modules: • sensord • Vsansystem • hostd-probe • Rhttpproxy • Clomd • nsx-opsagent • kmxa • vmkernel

Software Fixes

SmartConnector for	Description
Cisco IOS	Events for the IOSXE-6-PLATFORM module were not being parsed. **Fix**: The new sub-message has been provided to handle unpardsed events for the IOSXE-6-PLATFORM module.
Cisco Ironport Email Security	The mapping details for **Device Custom String 6** were missing. **Fix**: Modified the regex to handle the mapping details.
Cisco Wireless LAN Controller	Some of the events were not being parsed for Cisco Wireless LAN Controller. **Fix**: Added new sub-message and regex to handle the unparsed events.
Citrix NetScaler	The Citrix NetScalar 12.1 events were not being parsed. **Fix**: The regex has been modified for the unparsed events.
Intersect Alliance SNARE Syslog	Some of the events were not being parsed for Windows Snare 4.0. **Fix**: Provided support for the following events: 1, 3, 6, 12, 13, 14, 15, 16, 18, 20, 25, 27, 32, 35, 44, 55, 98, 109, 139, 143, 144, 153, 172, 1074, 4200, 5211, 6006, 6038, 7026, 10016, 10148, 10149, 14531, 14533, 15300, 15301, 16962, 16977, 16983, 36871, 50036, 50037, 51046, and 51047.
Linux Audit File	The RHEL 8.3 auditd events were not being parsed. **Fix**: The new sub-message has been provided to handle unparsed events.
Microsoft 365 Defender	The **mitreTechnique** field was not mapped correctly. **Fix**: The **mitreTechnique** mapping has been modified to **Device Custom String 6**.

SmartConnector for	Description
Microsoft Office 365 Management Activity	The **Source Username** and **Destination Username** fields were missing under Active Directory for the event **Change User Password**. **Fix**: Added the **Source Username** and **Destination Username** mappings to these fields.
Microsoft Windows Event Log - Native	The **Event ID: 403** for Microsoft ADFS was not being parsed. **Fix**: The parsing capability for the **destinationPort** and **oldFileId** fields have been improved for Event ID: 403 to handle unparsed event.
Pulse Secure Pulse Connect	Some of the events were not being parsed for Pulse Secure device. **Fix**: Added new sub-message and mapping details to handle the unparsed events.

Downloading Parser Files and Upgrading

The following sections contain information to download the latest parser AUP files and to upgrade the version:

Downloading Parser AUP Files

The ArcSight SmartConnector parser update releases are posted to the ArcSight Marketplace. ArcSight Marketplace is an app store that enables rapid provisioning of your ArcSight SIEM deployment with content updates and trusted security content packages.

It is mandatory to set up an ArcSight Marketplace administrative account to download and install the monthly connector parser updates.

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 must move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

Supported SmartConnector Version

Parser 8.3.3 update has been certified with SmartConnector Framework release 8.3. Use of this update with earlier framework releases is not supported.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to the Technical Requirements for SmartConnector guide.

Upgrading to 8.3.3

The following sections document the multiple options for upgrading to this release:

- Upgrading Locally
- Upgrading Remotely
  - From Marketplace Directly
  - From SLD or Marketplace

Micro Focus provides a digital public key to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

For information and instructions, visit the Micro Focus Partner Portal site.

Upgrading Locally

Before starting this procedure, verify that you are running the SmartConnector framework version 8.3. Applying this parser AUP release update to any SmartConnector release earlier than 8.3 is not supported by Micro Focus.

To upgrade locally:

1. Download the appropriate parser release upgrade AUP file using the process provided here.
2. Stop the SmartConnector.
3. Run the following command:

   ```
   arcsight parseraupupgradelocal [your_upgrade_to_parser].aup [your_ignore_warning_flag]
   ```

   Where:

   [your_upgrade_to_parser].aup is the full path of the upgrade to parser AUP file downloaded in step 1. This file will be moved by the upgrade script. Verify that no other process is using this file. Verify that the logged in user has both execute and write permissions for the selected file.

   [your_ignore_warning_flag] is the true/false flag indicating whether you want to ignore the “Parser AUP has later version than the connector” warning.
4. After the upgrade completes, connector starts automatically.

Upgrading Remotely

You can upgrade to the new parser release from ArcMC either directly from Marketplace using ArcMC or from your ArcMC repository.

Before upgrading, have the latest version of the ArcSight Management Center Administrator's Guide from the documentation site for ArcSight SmartConnectors available for any questions.

From Marketplace Directly

Before starting this procedure, connector must be running. Create your administrative account on the ArcSight Marketplace If you have not already done so.

To upgrade directly from the Marketplace:

1. Click **Node Management** in ArcMC.
2. In the navigation tree, navigate to the host on which the container resides.
3. Select the container to be upgraded.
4. Click the **Upgrade** button.
5. (Optional) If you have not logged in to Marketplace, on the upgrade page, click **Save ArcSight Marketplace User** to enter your Marketplace credentials. This is a one-time task, unless you need to update your credentials.
6. From **Upgrade Type**, choose **Parser upgrade**.
7. From the **Select Upgrade Version** drop-down list, select the 8.3.3 (Latest) parser upgrade AUP file.
8. Click **Upgrade**.
9. In the **Details** column, under **Parser upgrade file push status**, verify that the status is displayed as **Successful**, to indicate that the file was successfully pushed to the container. It signifies that the parser upgrade file was automatically downloaded to your repository.
10. Wait while connectors restart automatically.
11. To determine the parser AUP file in use, see Verifying the Parser Version AUP in Use.

From SLD or Marketplace

Prior to performing an upgrade of a container, you will need a connector AUP file of the new parser version in your ArcMC repository.

To upgrade from SLD or Marketplace and then to apply it from the ArcMC Repository, complete the following process:

1. Upload the parser release AUP file to the repository from Marketplace or SLD.
2. Apply the parser upgrade to all connectors in a container.

Note: For applying the parser upgrade, go to the next procedure if the new parser release AUP file already exists in the repository.

To upload the new parser release AUP file to your repository:

1. Download the appropriate parser release upgrade AUP file in one of the following methods:
   - Go to **Categories** > **SmartConnectors** in the ArcSight Marketplace.
   - Software Licenses and Downloads (SLD)
2. Log in to the ArcMC browser-based interface.
3. Go to **Administration** > **Repositories**.
4. In the navigation tree, select **Upgrade Files**.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Open**.
8. Click **Submit**. The file is uploaded.

You can now use the AUP upgrade file in the repository when you are ready to upgrade a container or containers to a specific version using the procedure.

To apply the parser upgrade AUP file to all connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. Select one or more containers to upgrade.
5. Click **Upgrade**.
6. From **Select Upgrade Type**, choose **Parser upgrade**.
7. From the **Select Upgrade Version** drop-down list, select the parser release AUP file version to which you want to upgrade the selected containers.
8. Click **Upgrade**. The upgrade is performed on all containers.

For complete upgrade instructions, see Upgrading All Connectors in a Container in the latest version of ArcSight Management Center Administrator's Guide available in the documentation site for ArcSight SmartConnectors.

Rolling Back to a Previous Version

Users can roll back to a previous version by using any of the following methods suggested for upgrading:

- Apply the previous version of parser AUP locally.
- Apply the previous version of parser AUP directly from Marketplace.
- Upload the previous version of the parser AUP to the ArcMC repository from SLD or Marketplace, then apply from ArcMC repository.

Verifying the Parser Version AUP in Use

You can verify the parser upgrade file in use either in ArcMC or in the agent logs.

In ArcMC

1. Go to **Node Management** > **View All Nodes**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Verify that the value in the **Parser Version** column matches the version number of the recent upgrade.

In the Agent Logs

1. Find the `agent.log` file at: `/ArcSight_Home/current/logs`.
2. Search for the latest occurrence of the line in the log file that contains “ArcSight Parser Version".

   Example:

   ```
   <CODE MAP: '8.3.0.xxxx.0>
   <ArcSight Connector Version: 8.3.0.xxxx.0>
   <ArcSight Parser Version: 8.3.3.xxxx.0>
   ```

Note: You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your PROD (production) environment.

Known Limitations

For a list of known limitations with the application, see Known Limitations.

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 (SmartConnector 8.3.3)

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!