Micro Focus Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.14.1.8253.0

January 16, 2020

Micro Focus Security ArcSight
SmartConnector Parser Update Release Notes

7.14.1.8253.0

January 16, 2020

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical SupportPage: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation

Contents

SmartConnector Parser Release 7.14.1.8253.0

These notes list SmartConnectors for which parser changes have been made and describe how to apply this latest ArcSight SmartConnector parser release.

To Verify Your Upgrade Files

Micro Focus provides a digital public key for you 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.
Visit the following site for information and instructions:
https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do

Note: If a Parser Override was provided, see if the Bug or Feature Request number is included in the Fixed or Enhancements Section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your environment PROD (production).

Supported SmartConnector Version

This parser update has been certified with SmartConnector Framework release 7.14.0.8241.0. Use of this update with earlier framework releases is not supported.

Obtain Parser Release AUP File

ArcSight Marketplace

The monthly 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.

An ArcSight Marketplace administrative account is required to download and install the monthly connector parser updates. Browse to the Marketplace at https://marketplace.microfocus.com/arcsight to set up your administrative account.

MICRO FOCUS PROTECT 7/24

The monthly ArcSight SmartConnector parser update releases are also posted on the Micro Focus Security Community.

New Component or Version

SmartConnector for	Number	Description
MS Windows Event Log Native	CON-18594	Added support for Microsoft Defender Antivirus
	CON-20235	Added support for event 104 (Log clear event)
McAfee ePolicy Orchestrator DB	CON-22264	Added support for Threat Intelligence Exchange Server 2.3 with ePO 5.3.
McAfee ePolicy Orchestrator DB	CON-22662	Added support for module Policy Auditor File (PA File) and Policy Auditor Rule (PA Rule) version 6.4 with ePO 5.10

	CON-22871	Added support for Azure AD events.
	CON-22872	Added support for Exchange Online events.
	CON-2273	Added support for Sharepoint Online events.
MS Office 365	CON-22874	Added support for One Drive events.
	CON-22883	Added support for WAF and WAF-Regional services.
	CON-22889	Added support for SecurityHub services.
	CON-22893	Added support for AWS Inspector services.
AWS CloudTrail	CON-22894	Added support for CloudFormation services.

Fixed Issues

SmartConnector for	Number	Description
MS Office 365	CON-18936	When installing Microsoft Office 365, the error *Bad Request* is displayed. Fix: This issue was been fixed in Framework Release 7.13.0. Users must upgrade the connector to either version 7.13 or 7.14.0 to get the connector installed without any errors.
	CON-22292	Some events for Cisco ASA 8.4 were not being parsed correctly. Fix: Added mappings for Cisco ASA 8.4 in order to parse these events.
Cisco Asa Syslog	CON-23124	Some Cisco ASA messages were not being parsed correctly.
Barracuda Firewall NG F-Series Syslog	CON-22687	Some events were not being parsed. Fix: Added new pattern and submessages to parse those events.
Cisco Wireless LAN Controller Syslog	CON-22703	Some events were not being parsed for Cisco Wireless LAN Controller 8.2. Fix: Added mappings to parse those events.
TippingPoint SMS Syslog	CON-22991	A parser error was generated with Tippingpoint event logs. Fix: Added new pattern and submessages to parse those events.
Check Point Syslog	CON-23153	Some events were not being parsed correctly.
Proofpoint Enterprise Protection and Enterprise Privacy Syslog	CON-23210	Some events were not being parsed correctly.
Sybase Adaptive Server Enterprise DB	CON-23235	Description: The Device Host Name is empty for Sybase Adaptive Server DB Fix: Updated mappings to support the field.
Linux Audit Syslog	CON-23323	Some events are not being parsed. Fix: Added new pattern and submessages to parse those events.
F5 BIG-IP Syslog	CON-22929	Some events were not categorized correctly.

Enhancements

SmartConnector for	Number	Description
Cisco ISE Syslog	CON-22928	Cisco ISE version 2.4 mappings were updated.
MS WINS Server Windows Event Log Native	CON-23361 CON-23360	Sysmon parser mappings did not match Windows Audit Event parsers.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

SmartConnectors Support Recently Ended

Support Ended 8/21/2019

Support ended for Oracle Audit DB v9 – end of support by vendor.
[CON-22834]

Support Ended 4/28/2018

Support ending for all 32-bit SmartConnectors – Use 64-bit SmartConnectors.

Updated Configuration Guides

SmartConnector configuration guides for the following devices have been updated for this release and are posted to the ArcSight Connector Documentation page on Micro Focus Software Community at:

https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation

Verify Your Upgrade Files Obtained from SSO

After you obtain the parser release file from SSO, and before you upgrade, Micro Focus provides a digital public key for you 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.

Visit the following site for information and instructions:

https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do

Upgrading to the 7.14.1.8253.0 Parser Release

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

- Upgrade Locally to this Parser Release
- Upgrade Remotely

Upgrade Locally to this Parser Release

Before starting this procedure, verify that you are running the SmartConnector framework version 7.14.1.8253.0 Applying this parser AUP release update to any SmartConnector release earlier than 7.14.1.8253.0 is not supported by Micro Focus ArcSight Parser Upgrade 7.14.1.8253.0 .

To upgrade locally to this parser release:

1. Download the appropriate parser release upgrade AUP file from the ArcSight Marketplace site (https://marketplace.microfocus.com/arcsight) at **Categories > SmartConnectors** or from SSO (https://softwaresupport.softwaregrp.com/).
2. Stop the SmartConnector.
3. To perform the parser upgrade, run the 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 (the file downloaded in step 1.) This file will be moved by the upgrade script. Verify that no other process is holding this file. Verify that the logged in user has both execute and write permissions for the selected directory.
- **[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. The connector will be started automatically after upgrade has completed.

Upgrade Remotely to this Parser Release Using ArcMC

Before upgrading, have the latest version of the *Micro Focus Security ArcSight Management Center Administrator's Guide* available for any questions.

Note: Updating the parser AUP with ArcMC requires ArcMC version 2.5 or later.

You can upgrade to the new parser release from ArcMC either directly from Marketplace using ArcMC or from your ArcMC repository. See the following sections for details:

1. From Marketplace Directly
2. From SSO or Marketplace, then Apply from the ArcMC Repository

From Marketplace Directly

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

To upgrade directly from 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. (If not logged into Marketplace) On the upgrade page, click on "Save ArcSight Marketplace User" to enter your Marketplace credentials. This is a one-time task, unless you need to update your credentials.
6. Under **Select Upgrade Type**, choose **Parser upgrade**.
7. From the **Select Upgrade Version** down-down list, select the **7.14.1.8253.0** (Latest) parser upgrade AUP file.
8. Click **Upgrade**.
9. Verify in the Details column, under "Parser upgrade file push status", that the file was successfully pushed to the container. It signifies that the parser upgrade file was automatically downloaded to your repository. Status will show "Successful."
10. Wait while connectors restart automatically.
11. Use the Verify the Parser Version AUP in Use procedure to determine the parser AUP file in use.

From SSO or Marketplace, then Apply from the ArcMC Repository

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

This is a two-part process:

- Uploading the parser release AUP file to the repository from Marketplace or SSO
- Applying the parser upgrade to all connectors in a container

  Note: If the new parser release AUP file (7.14.1.8253.0) already exists the repository, go to the next procedure to apply the parser upgrade.

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

1. Download the parser release upgrade AUP file for the connector from the ArcSight Marketplace (https://marketplace.microfocus.com/arcsight) by selecting **Categories > SmartConnectors** or go to SSO (https://softwaresupport.softwaregrp.com/).
2. Log in to the ArcMC browser-based interface.
3. Go to **Administration > Repositories**.
4. In the navigation tree, pick **Upgrade Files.**
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier. Click **Open**.
7. 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. On the Containers tab, select one or more containers to upgrade.
5. Click Upgrade.
6. On the upgrade page, under Select Upgrade Type, choose Parser upgrade.
7. Under Select Upgrade Version, from the drop-down list, choose the parser release AUP file version to which you want to use to upgrade the selected containers.
8. Click Upgrade. The upgrade is performed on all containers.

See “Upgrading All Connectors in a Container” in the *Micro Focus Security ArcSight Management Center Administrator’s Guide* for complete upgrade instructions.

Roll Back to a Previous Version

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

1. Apply the previous version of parser AUP locally.
2. Apply the previous version of parser AUP directly from Marketplace
3. Upload the previous version of the parser AUP to the ArcMC repository from SSO or Marketplace, then apply from ArcMC repository.

Verify the Parser Version AUP in Use

The parser upgrade file in use can be verified 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 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: '7.14.0.8241.0.'>
<ArcSight Connector Version: 7.14.0.8241.0.>
<ArcSight Parser Version: 7.14.1.8253.0 >
```