



# **Micro Focus Security ArcSight Connectors**

SmartConnector Parser Update Release Notes

**7.14.2.8258.0**

February 21, 2020

7.14.2.8258.0

February 21, 2020

## Legal Notices

### Copyright Notice

© Copyright 2010 – 2020 Micro Focus or one of its affiliates.

**Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.**

**The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.**

**No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.**

**Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.**

**U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.**

### Trademark Notices

**Adobe™ is a trademark of Adobe Systems Incorporated.**

**Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.**

**UNIX® is a registered trademark of The Open Group.**

### Support

#### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation">https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation</a>

Contents

SmartConnector Parser Release 7.14.2.8258.0 .....	4
To Verify Your Upgrade Files .....	4
Supported SmartConnector Version .....	4
Obtain Parser Release AUP File.....	4
ArcSight Marketplace.....	4
MICRO FOCUS SECURITY COMMUNITY.....	4
New Component or Version .....	4
Fixed Issues.....	5
Enhancements .....	6
Known Limitations.....	6
Connector End-of-Life Notices .....	7
SMARTCONNECTOR SUPPORT ENDING SOON.....	7
SMARTCONNECTORS SUPPORT RECENTLY ENDED .....	7
Support Ended 8/21/2019 .....	7
Support Ended 4/28/2018 .....	7
Updated Configuration Guides.....	7
Verify Your Upgrade Files Obtained from SSO.....	7
Upgrading to the 7.14.2.8258.0 Parser Release.....	7
Upgrade Locally to this Parser Release .....	7
Upgrade Remotely to this Parser Release Using ArcMC .....	8
From Marketplace Directly.....	8
From SSO or Marketplace, then Apply from the ArcMC Repository .....	8
Roll Back to a Previous Version.....	9
Verify the Parser Version AUP in Use.....	9
In ArcMC .....	9
In the Agent Logs.....	9

# SmartConnector Parser Release 7.14.2.8258.0

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 SECURITY COMMUNITY

The monthly ArcSight SmartConnector parser update releases are also posted on the [Micro Focus Security Community](#).

## New Component or Version

SmartConnector for	Number	Description
UNIX OS Syslog	CON-21852	Added partial support for RHEL 7.6.
Symantec Endpoint Protection DB	CON-22217	Added support for Symantec EndPoint Protection 14.2
Microsoft Windows Event Log Native	CON-22520	Added Microsoft Windows Server 2019 as a supported installation platform.
	CON-22521	

**\*\*This new support is related to a known**

	CON-22522	<b>limitation detailed on the corresponding section of this document**.</b>
	CON-22523	
	CON-22524	
	CON-22896	

## Fixed Issues

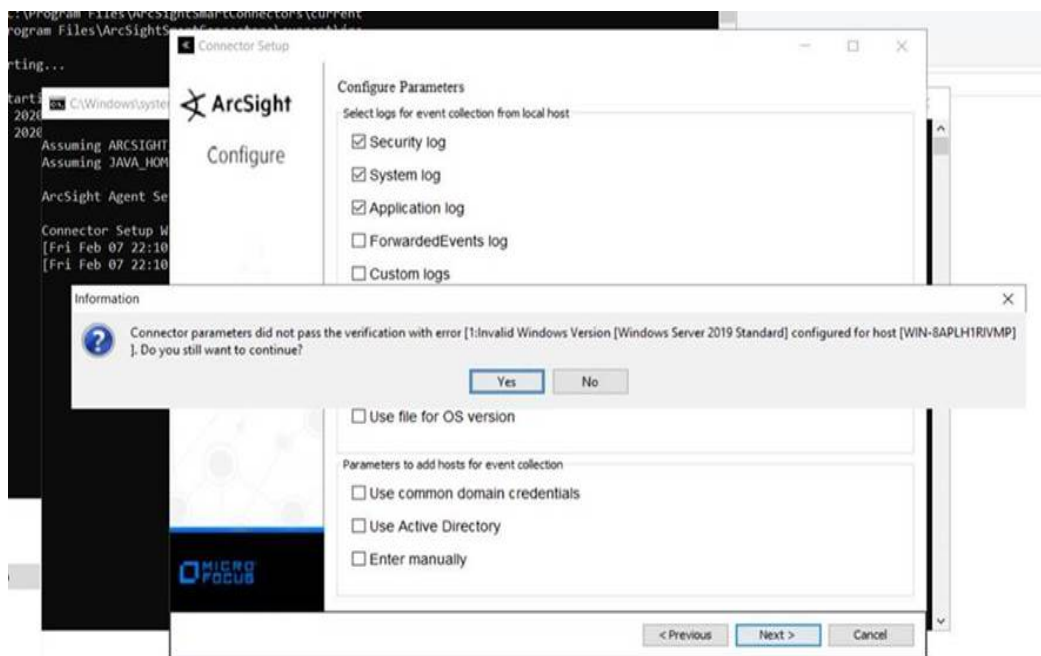
SmartConnector for	Number	Description
McAfee ePolicy Orchestrator DB	CON-22705	Catalog removed from the parser to increase performance.
	CON-23457	Some events appeared with different endTime.  Fix: Event mappings were updated.
IBM Security Access Manager Syslog	CON-23137	Some events were not being parsed for IBM Security Access Manager 9.0.5.  Fix: events were mapped to their respective fields.
Symantec Endpoint Protection DB	CON-22197	When the connector pulled events from the database, the tempdb got filled up.  This issue has been fixed.
	CON-23637	An Event ID was duplicated.  Fix: version 14 of the Alerts module for SymantecEndpoint Protection was updated.
Oracle Audit Syslog	CON-23373	The latest version of this configuration guide was revised.
Microsoft Office 365	CON-23544	Updated event mappings for SharePoint Online & OneDrive for Business.  Users can now share and access Request Activities and Exchange Online.
Amazon Web Services CloudTrail	CON-23596	The Device Custom Number1 field was not being parsed.  The field is now being parsed.

## Enhancements

SmartConnector for	Number	Description
MS Win Event Log Native Security Event Mappings	CON-23021	Added "Application" field mapping to the following audit events: 5152,5153,5154,5155,5156,5157,5158.
Amazon Web Services CloudTrail	CON-22891	Added support for new service: Trusted Advisor.
Microsoft Azure Monitor Event Hub	CON-23308	Troubleshooting section updated with topics:  Azure Datacenters with Stamps (Scale Units) without Premium V2 VMs  App Service Plan with Basic Pricing Tier Created on a Stamp That Does not Have Premium V2 VMs

## Known Limitations

An operating system compatibility error is displayed when installing the Windows Event Log Native SmartConnector.



Workaround:

1. Start the WINC SmartConnector installation.
2. Quit the installation before choosing the connector from the dropdown list.
3. Upgrade the SmartConnector framework version with the latest 7.14.2 AUP.

4. Run the `runagentsetup` file and continue with the connector installation.
  5. Run the connector, events can now be viewed on ESM.
- [CON-22522]

## 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 ended 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 7.14.2.8258.0 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 7.14.0.8241. Applying this parser AUP release update to any SmartConnector release earlier than 7.14.2.8258.0 is not supported by Micro Focus ArcSight Parser Upgrade 7.14.2.8258.0.

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 **7.14.2.8258.0** (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 (7.14.2.8258.0) 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/argsight>) 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: 7.14.2.8258.0 >
```