



Micro Focus Security ArcSight Smart Connectors

Software Version: 7.15.1.8305.0

Parser Update Release Notes

Document Release Date: May 21, 2020

Software Release Date: May 21, 2020

Legal Notices

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

<https://www.microfocus.com>

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.

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:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

- Overview 6
 - Supported SmartConnector Version 6
 - Obtain Parser Release AUP File 6
 - What's New in this Release 6
 - New SmartConnector 6
 - New Device, Component, or OS Version Support 7
- SmartConnector Enhancements 8
- Closed Issues 9
- System Requirements 11
 - Hardware Requirements 11
- Known Limitations 12
- Upgrading to 7.15.1.8305.0 16
 - Upgrade Locally to this Parser Release 16
 - Upgrade Remotely to this Parser Release Using ArcMC 17
 - From Marketplace Directly 17
 - From SSO or Marketplace, then Apply from the ArcMC Repository 18
 - Roll Back to a Previous Version 19
 - Verify the Parser Version AUP in Use 19
- To Apply this Release 20
- Connector End-of-Life Notices 21
 - SmartConnector Support Ending Soon 21
 - SmartConnector Support Recently Ended 21
 - Support Ended 11/22/2019 21
 - Support Ended 8/21/2019 21
 - Support Ended 4/28/2018 21
 - Support Ended 02/21/2018 21

Send Documentation Feedback22

Overview

These notes list SmartConnectors for which parser changes have been made and describe how to apply this latest ArcSight SmartConnector parser release as well as providing other information about recent changes and open and closed issues (generated by various vendor devices) to the ArcSight ESM Manager, Logger, or other destinations.

Supported SmartConnector Version

This parser update has been certified with SmartConnector Framework release 7.15.0.8295.0. 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](#).

What's New in this Release

SmartConnector 7.15.1 includes the following capabilities:

New SmartConnector

None at this time.

New Device, Component, or OS Version Support

SmartConnector for	Number	New Device, Component, or OS Version
IBM AIX Audit Syslog	CON-22074	Added support for IBM AIX Audit syslog version 7.2.
Microsoft Windows Event Log Native	CON-23623	Added support to the following events: Microsoft-Windows-Security-Auditing:5379 Microsoft-Windows-Security-Auditing:5380 Microsoft-Windows-Security-Auditing:5381 Microsoft-Windows-Security-Auditing:5382
	CON-19524	Added support for Microsoft DNS Server Analytics.

SmartConnector Enhancements

In each SmartConnector release, various security fixes, feature updates, and bug fixes are made to the field mappings for individual SmartConnectors. If you use any of the SmartConnectors listed in the "Closed Issues" section of these release notes, be aware that installing the updated SmartConnector can impact your created content.

None at this time.

Closed Issues

SmartConnector for	Number	Description
Check Point Syslog	CON-23932	Added support for R80 Application Control, R80 Email Security, R80 Identity Logging, R80 SmartDefense, R80 VPN-1 and FireWall-1, R80 Anti Malware, R80 New Anti Virus, R80 Identity Awareness, R80 URL Filtering, R80 DLP, R80 HTTPS Inspection, R80 Syslog and "Unknown Product" Product mappings.
Cisco ASA Syslog	CON-15902	Added support to some events with IPv6 addresses.
	CON-19976	Event Id 113005 was not being parsed correctly.
	CON-20077	Add support for event Id 434004.
	CON-20784	Updated mappings for source/destination address and source/destination translated address to support some unparsed events.
	CON-22087	Some events were not being parsed correctly.
	CON-22158	Some events for Cisco Router were not being parsed correctly.
	CON-22621	Some events were not being parsed.
	CON-21392	Some events were not mapped correctly.
Cisco ACS Syslog	CON-23250	Added new mappings for Cisco Secure ACS Administrative and Operational Audit.
Cisco Meraki Syslog	CON-23860	Some events were not being parsed.
	CON-23870	
Cisco Wireless LAN Controller Syslog	CON-19884	Added support to some unparsed events.
Dell SonicWALL Syslog	CON-19271	Some events were not being parsed correctly.
	CON-19421	
	CON-19880	
HPE Integrated Lights-Out Syslog	CON-23869	Some events were not being parsed.
Infoblox NIOS Syslog	CON-23653	Some events were not being parsed.
Juniper Firewall ScreenOS Syslog	CON-19879	Some events for version 6.3 were not being parsed correctly.

Parser Update Release Notes
 Closed Issues

SmartConnector for	Number	Description
Juniper JUNOS Syslog	CON-22864	Some events were not being parsed. (This issue was fixed during parser release 7.14.3)
	CON-23780	Added support to Junos logs that contain different number of opening and closing double quotations.
Linux Audit Syslog	CON-22731	Unix rsyslogd events were not being parsed correctly.
McAfee ePolicy Orchestrator DB	CON-23657	A catalog was removed from the parser to increase the connector performance.
Microsoft DNS Trace Log Multiple Server File	CON-23912	The attacker and target address fields were being parsed incorrectly.
Microsoft Office 365	CON-23156	An incorrect device product issue in the MS Office schema connector has been resolved.
Microsoft Windows Event Log Native: MS Sysmon Logs	CON-23771	Some mappings for event Id 22 were parsed incorrectly.
MS IIS Multiple Server File	CON-22064	Regex mismatch messages were being recorded into the agent log file.
Microsoft Windows Event Log Native: Security Event Mappings	CON-23959	Added support for event Id 5145
Symantec Messaging Gateway Syslog	CON-22816	Some events for version 10.5 were not being parsed.
UNIX OS Syslog	CON-23584	Some events were not being parsed.
	CON-23665	Linux DNS events were not being parsed correctly.
VMware Web Services	CON-23864	Timestamp formats were not displayed correctly.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to the [ArcSight Security Open Data Platform \(SODP\) Support Matrix](#) guide available on the [Micro Focus Software Community page](#).

Hardware Requirements

- CPU: 2 CPU X 4 Cores each (2 x Intel E5620, quad core, 2.4 Ghz or better)
- RAM: 16 GB
- Disk: 60 GB
- Number of network interfaces—1 Dedicated Gig Ethernet interface

Note: To achieve better performance, use a server with higher system specifications.

Known Limitations

ArcMC Managed SmartConnectors

One-Click installation is failing on RHEL 8.1 and CentOS 8.1 through ArcMC 2.9.4.

Workaround:

Pre-requisites for instant connector/ collector deployment for 8.1 O:

- Python2
- Libselinux-python

Unlike Linux 6.x and 7.x, the prerequisites above are not integrated by default in Linux 8.x. If you are installing/ have installed ArcMC in a RHEL/CentOS 8.1 machine, perform the following steps. Also, apply these changes to the target Linux host (the VM where the connector/ collector will be deployed):

1. Install python2:

```
sudo yum install -y python2
```

2. Create a symlink:

```
sudo ln -s /usr/bin/python2 /usr/bin/python
```

3. Install the libselinux-python package:

```
sudo yum install -y libselinux-python
```

Note: Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm

[CON-23909]

IBM Big Fix REST API

While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file:

"E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.

Workaround.

Manually set the correct path, which is: \$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties

[CON-23907]

Malware Information Sharing Platform Model Import Connector

When running the MISP connector in FIPS mode, the following error is displayed on the console:

```
java.security.KeyManagementException: FIPS mode: only SunJSSE TrustManagers  
may be used  
  
at sun.security.ssl.SSLContextImpl.chooseTrustManager  
(SSLContextImpl.java:120)  
  
at sun.security.ssl.SSLContextImpl.engineInit(SSLContextImpl.java:83)  
  
at javax.net.ssl.SSLContext.init(SSLContext.java:282)  
  
at org.apache.http.conn.ssl.SSLContextBuilder.build  
(SSLContextBuilder.java:164)  
  
at org.apache.http.conn.ssl.SSLSocketFactory.<init>  
(SSLSocketFactory.java:303)  
  
at com.arcsight.agent.dm.f.b.q(b.java:581)  
at com.arcsight.agent.dm.f.b.r(b.java:555)  
at com.arcsight.agent.dm.f.b.d(b.java:173)  
at com.arcsight.agent.Agent.a(Agent.java:674)  
at com.arcsight.agent.Agent.a(Agent.java:1171)  
at com.arcsight.agent.Agent.e(Agent.java:948)  
at com.arcsight.agent.Agent.main(Agent.java:1960)
```

Workaround:

This message can be ignored. It does not affect the functionality.

[CON-23875]

Microsoft Windows Event Log (WiSC)

WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. We have experienced the following issues:

- Issue #1: High CPU utilization on the monitored Windows host (log endpoint)

High CPU utilization has been detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).

- Issue #2: WinRM inherent EPS limitations

Given the circumstances with WinRM, the event rate has a limit of around 140 EPS (sustained). Therefore, we do not recommend the use of the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.

Workaround: To mitigate these issues, we recommend using the Windows Native Connector (WiNC) SmartConnector.

[CON-21601]

For more information, see the [Technical Note on WinRM-related Issues](#).

Microsoft Azure Monitor Event Hub

The Azure Event Hub Debug Mode for function apps should not be enabled during normal operation, only for support purposes. Enabling it, may cause parsing and mapping errors.

Workaround:

To change this setting:

1. Go to the Azure portal < Function app < Configuration.
2. Set the “DebugMode” application value to False.
3. Restart the Function App.

[CON-22784]

After deploying the connector, events are duplicated or out of order

[CON-22809]

All Windows Event Log Connectors, both Native and Unified

If the connector cannot process events fast enough and the internal queue fills up, it might stop processing.

Workaround:

None at this time. You can re-configure the MQ parameters in agent.properties to prevent the queue from filling up.

[CON-19425]

All SmartConnectors

You might not be able to install your connector because of some missing packages.

Workaround:

Ensure that the following packages are installed:

1. yum install -y unzip
2. yum install -y fontconfig \ dejavu-sans-fonts

[CON-22085]

All SmartConnectors installed on Solaris

When upgrading SmartConnectors on Solaris, a timeout error is displayed. Follow the applicable workaround:

If the Solaris connector is already installed as a standalone, locally upgrade to 7.15.0.8295.0.

If the Solaris Connector is installed as a service:

1. Stop the service.
2. Go to HOME/current/bin and execute. /runagentsetup.
3. Uninstall the service in Global Parameters and exit the wizard.
4. Perform a local upgrade to 7.15.0.8295.0.
5. Install the Connector as a service and exit the wizard.
6. Start the service.

[CON-22080]

All SmartConnectors

Connector logs show Fatal Exception error: Unable to find requested property 'transport.cefkafka.extra.prod.props'. This message does not impact the performance or the functionalities of the Connector.

If you are using a map file with an expression set in the <connector_install_location>

\current\user\agent\map location, and the connector runs out of memory, add the following property to agent.properties as a workaround:

```
parser.operation.result.cache.enabled=false
```

If this problem happens with Windows Event Log Native, and if the above work-around does not completely solve the problem, reduce the value of the Native connector parameter 'eventprocessorthreadcount'. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:

```
agents[0].eventprocessorthreadcount=5 or agents  
[0].eventprocessorthreadcount=1, etc..
```

where 0 is the index of the WINC connector in the container. [CON-19234, CON-18977]

Upgrading to 7.15.1.8305.0

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

1. Upgrade Locally to this Parser Release
2. Upgrade Remotely

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, determine whether 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)

Upgrade Locally to this Parser Release

Before starting this procedure, verify that you are running the SmartConnector framework version 7.15.0.8295.0. Applying this parser AUP release update to any SmartConnector release earlier than 7.15.0.8295.0 is not supported by Micro Focus ArcSight Parser Upgrade 7.15.1.8305.0.

To upgrade locally to this parser release:

1. Download the appropriate parser release upgrade AUP file from the [ArcSight Marketplace](#) site at **Categories > SmartConnectors** or from [SSO](#).
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 7.15.1.8305.0 (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 (7.15.1.8305.0) 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 appropriate parser release upgrade AUP file from the [ArcSight Marketplace](#) site at **Categories > SmartConnectors** or from [SSO](#).
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: '7.15.0.8295.0.'>  
<ArcSight Connector Version: 7.15.0.8295.0.>  
<ArcSight Parser Version: 7.15.1.8305.0 >
```

To Apply this Release

Download the appropriate executable for your platform and the "SmartConnector Configuration Guides .Zip" file from the [Support Web Site](#).

When downloading the documentation zip file, create a folder for documentation (such as C:\ArcSight\Docs) and unzip in that folder. Then double-click `index.html` in the `agentdocinstall` directory to access the individual configuration guides.

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.

All SmartConnectors are currently supported on 64-bit platforms other than those listed as exceptions in the "SmartConnectors with 64-Bit Support" document. This document is available on the [Micro Focus Security Community](#) as well as in the SmartConnector Configuration Guide zip file available for download from the Support Web Site.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

None at this time.

SmartConnector Support Recently Ended

Support Ended 11/22/2019

Solsoft Policy Server - Support ended due to lack of customer demand.

[CON-22478]

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.

Support Ended 02/21/2018

Symantec Endpoint Protection DB - SEP version 11 support ended by vendor.

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 Parser Update Release Notes (Smart Connectors 7.15.1.8305.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!