Micro Focus Security ArcSight Connectors

Software Version: 7.15.2

Micro Focus SmartConnector Release Notes

Document Release Date: June 18, 2020
Software Release Date: June 18, 2020

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:

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

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 COMMNUNITY

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

What's New in this Release

SmartConnector 7.15.2 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
Check Point Syslog	CON-23223	Added support for: R80 FDE R80 MEPP R80 Endpoint Security Console Refer to the SmartConnector for Check Point Syslog Configuration Guide for details of what has been updated.
Microsoft Office 365	CON-23393	Added support for Compliance events in Exchange & Data Insights REST API events. Refer to the SmartConnector for Microsoft Office 365 Configuration Guide for details of what has been updated.
	CON-23939	

SmartConnector for	Number	New Device, Component, or OS Version
Microsoft Windows Event Log Native	CON-23757	Added support for Microsoft Windows Bits Client Event Log. Refer to the SmartConnector for MS Win Event Log N-MS Win BITS Client Evt Logs Configuration Guide for details of what has been updated.
	CON-23878	Added the following events: Event 6 Event 8 Refer to the MS Sysmon Logs Windows Event Log Native Configuration Guide for details of what has been updated.
	CON-23944	Added support to ESENT application events Refer to the SmartConnector for MS Win Event Log N-MS Win ESENT Evt Logs Configuration Guide for details of what has been updated..
	CON-24042	Added the following events to Microsoft Sysmon Logs: Event 14 Event 19 Event 20 Event 21 Refer to the MS Sysmon Logs Windows Event Log Native Configuration Guide for details of what has been updated.
	CON-24032	Added support for Microsoft-Windows-WMI-Activity/Trace Log (only event Id 11). Refer to the SmartConnector for Windows Event Log N- MS Win WMI Activity Trace Configuration Guide for details of what has been updated.
	CON-24041	Added support for Microsoft Windows-WMI-Analytic and Operational. Refer to the SmartConnector for Windows Event Log N - MS Win WMI Analytic and Operational Configuration Guide for details of what has been updated.

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.

SmartConnector for	Number	Description
Microsoft Windows Event Log Native	CON-23878	Added new MITRE Id mappings for the following events: Event 1 Event 2 Event 3 Event 5 Event 7 Event 9 Event 10 Event 11 Event 12 Event 13 Event 15 Event 17 Event 18 Event 22 Refer to the SmartConnector for MS Windows Event Log - Native SmartConnector (WiNC) Configuration Guide for details of what has been updated.

Closed Issues

SmartConnector for	Number	Description
Cisco ASA Syslog	CON-20714	Messages with ID 722051 and 713228 were being parsed incorrectly Refer to the SmartConnector for Cisco ASA Syslog Configuration Guide for details of what has been updated.
	CON-23954	Some events were not being parsed correctly.
Cisco ISE Syslog	CON-20962	Some mappings have been removed to parse events correctly. Refer to the SmartConnector for Cisco ISE Syslog Configuration Guide for details of what has been updated.
Dell SonicWALL Syslog	CON-24122	Updated the severity definition in the parser file of the connector.
IP Flow (Netflow/J-Flow)	CON-19940	The connector was populating the agent.log with a fatal error message in data type mismatches. Refer to the SmartConnector for IP Flow (Netflow/J-Flow) Configuration Guide for details of what has been updated.
Microsoft Windows Event Log Native	CON-23487	Added new mappings for Security Channel event Id 4950. Refer to the Microsoft Windows Event Log Native Security Event Mappings Configuration Guide for details of what has been updated.
	CON-23910	Added new mapping for the event type field. Refer to the MS Sysmon Logs Windows Event Log Native Configuration Guide for details of what has been updated.
VMware ESXi Server Syslog	CON-20016	Added support for the following modules of version 6.5: Hostd, Vpxa, dhclient-uw, sfcb-sfcb, jumpstart, sfcb-CIMXML-Processor, vmauthd, smartd, sfcbd-init,sfcbd-config, and vmkernel. Refer to the SmartConnector for VMware ESXi Server Syslog Configuration Guide for details of what has been updated

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 hot (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 7.15.2.8312.0

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 7.15.2.8312.0.

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 7.15.2.8312.0 (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 (7.15.2.8312.0) 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: 7.15.2.8312.0 >
   ```

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 Micro Focus SmartConnector Release Notes (Connectors 7.15.2)

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!