Micro Focus Security ArcSight Connectors

Software Version: 7.14.0.8241.0

Micro Focus SmartConnector Release Notes

Document Release Date: December 9, 2019
Software Release Date: December 9, 2019

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

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/ctp/productdocs**

Contents

SmartConnector Release 7.14.0.8241.0

These notes describe how to apply the latest release of ArcSight SmartConnectors, as well and provide information about recent changes and open and closed issues.

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, 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)

Integrated into this Release

Parser update releases 7.12.1.8159.0 and 7.12.1.8163.0 have been integrated into this framework release. These releases contain version updates, fixed issues, and enhancements for a number of SmartConnectors. For details, see the corresponding release notes on the Micro Focus Security Community:

- 7.13.1.8184.0 Release Notes
- 7.13.2.8187.0 Release Notes

The SmartConnectors listed below were updated in these monthly parser update releases.

Release 7.13.1.8184.0
-MS Windows Event Log Native -MS Exchange PowerShell -Rapid7 NeXpose XML File -McAfee ePolicy Orchestrator DB -Oracle WebLogic Server File -Juniper JUNOS Syslog -Cisco IOS Syslog -Check Point Syslog -MS DNS Trace Log Multiple Server File

Release 7.13.2.8187.0
-MS Windows Event Log Native -McAfee ePolicy Orchestrator DB -Oracle Audit Vault DB for version 12.2.X -McAfee Network Security Manager DB (ID-based) for version 9.2 -McAfee Network Security Manager DB (Time-based) for version 9.2 -IP Flow (Netflow/J-Flow) -F5 BIG-IP Syslog -MS Office 365 -Cisco IOS Syslog -Cisco ASA Syslog -IBM SiteProtector DB

To Apply This Release

Download the appropriate executable for your platform from the Support Web site, as well as the separate downloadable zip file that contains the SmartConnector Configuration Guides.
When downloading the documentation zip file, create a folder for the documentation (such as `C:\ArcSight\Docs`) and unzip the file there. Then double-click `index.html` in the `agentdocinstall` directory to access the individual configuration guides.

A 64-bit executable is available for download for Windows and Linux platforms. Only a 64-bit executable is provided 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.

New SmartConnector

SmartConnector for	Number	Description
MIC for Malware Information Sharing Platform Solution	CON-22464	New Model Import Connector for MISP (Malware Information Sharing Platform Solution)
Checkpoint OPSEC NG 32-bit.	CON-22511	Relaunched Checkpoint 32-bit connectors.

New Device, Component, or OS Version Support

SmartConnector for	Number	Description
Dell EMC Unity and VNXe Storage	CON-21717	Added support for NFS Events along with CIFS events.
McAfee ePolicy Orchestrator DB	CON-22669	Added support for McAfee Active Response (MAR) version 2.3 and 2.4 with ePO 5.10
Oracle Audit Vault DB	CON-21858	Added support for Oracle Audit Vault DB v 12.2.x
Symantec Endpoint Protection	CON-22289	Added support for Symantec Endpoint Protection
Microsoft Azure Monitor Event Hub	CON-23019	The section *Setting User Permissions in Azure* in the configuration guide was modified.
All SmartConnectors	CON-23259	This framework release includes event categorization updates up to the release of October R1 2019. Later AUP Packages can be downloaded from SSO and ESM will take

		precedence over them.
Rapid7 NeXpose XML File	CON-22948	Added support for version 6.5.43.

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 "**Fixed Issues**" section of these release notes, be aware that installing the updated SmartConnector can impact your created content.

SmartConnector for	Number	Description
Microsoft Azure Monitor Event Hub	CON-22766	Added new destination to send CEF events to Azure Event Hubs. Destination name: Microsoft Azure Event Hub
ArcSight Kafka FlexConnector	CON-22970	Added new parameter to enable/disable ActiveMQ.
MS DNS Trace Log Multiple Server File	CON-22818	Added support for the following timestamp formats: 1) AM and PM 2) a.m. and p.m. 3) a.m and p.m 4) am and pm
	CON-22882	Added support for timestamp format yyyy/MM/dd HH:mm:ss (eg:2019/07/24 16:03:11)
All SmartConnectors	CON-22786	The ESM 7.2.x option is now visible by default on the Transformation Hub destination of the connector without having to add the parameters into the `agent.properties` file.

Fixed Issues

SmartConnector for	Number	Description
MS Windows Event Log Native	CON-20719	WINC connector kept requesting a WEF file despite selecting other methods. Fix: The wizard flow was modified and the issue has been fixed.
FlexConnectors	CON-22479	A licensing issue was generated with jconn3.jar. Fix: The driver name and url names were replaced after the jtds implementation.
Sybase Adaptive Server Enterprise DB		
Novell Nsure Audit DB		
FlexConnectors	CON-22482	Updated MySQL JDBC driver information.
Novell Nsure Audit DB		
PureSight Content Filter DB		
All SmartConnectors	CON-23002	An Apache ActiveMQ security vulnerability was fixed by upgrading the jar from activemq-client-5.9.0.jar to activemq-client-5.15.10.jar and its dependency jar.
Linux Audit Syslog	CON-22974	Some events were not being parsed. A new pattern and submessages were added to parse those events.

All SmartConnectors	CON-23007	An Apache Hadoop security vulnerability was fixed by upgrading the jar from hadoop-common-2.5.1.jar to hadoop-common-2.9.2.jar and its dependency jar.
	CON-23008	An Apache ActiveMQ security vulnerability was fixed by upgrading the jar from activemq-broker-5.9.0.jar to activemq-broker-5.15.10.jar and its dependency jar.
	CON-23009	A security vulnerability was fixed by upgrading library commons-httpclient-3.1.jar to 4.3.6 or higher.
	CON-23014	A security vulnerability was fixed by upgrading lib httpclient-4.5.1 to latest version 4.5.10.
	CON-23015	A security vulnerability was fixed by upgrading lib httpclient-4.5.2 to latest version 4.5.10.
	CON-23028 CON-23029 CON-23030	A Json injection security vulnerability was fixed by adding a new verifyJsonData.
ArcSight Common Event Format REST	CON-23032	
All SmartConnectors	CON-23122	An Apache Kafka security vulnerability was fixed by upgrading library from kafka-clients-2.1.0.jar to upgrade to 2.3.0.
AirMagnet Enterprise Syslog	CON-23151	Upgraded zulu openjdk to 8u232
All SmartConnectors	CON-23220	Removed os-05Nov2002.jar file
	CON-23229	A TLS warning is sometimes displayed when running a connector. Fix: Modify the agent.default.properties: remote.management.ssl.enabled.protocols=TLSv1.2,+TLSv1.1,+TLSv1 remote.management.ssl.fips.enabled.protocols=TLSv1.2,+TLSv1.1,+TLSv1
All SmartConnectors	CON-23001	A critical vulnerability was found in the jackson-databind-2.9.5.jar Fix: The jar was fixed by upgrading the jar from jackson-databind-2.9.5.jar to jackson-databind-2.9.6.jar
Juniper JUNOS Syslog	CON-22802	Some events were not being parsed. Fix: A new pattern and some submessages were added to parse those events

Known Limitations

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 **7.14.0.8241.0**

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 **7.14.0.8241.0**
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]

Microsoft Office 365

When configuring the Office 365 connector, if you get the following error: `"HTTP/1.1 400 Bad Request" with the message: "{"error":{"code":"AF20024","message":" The subscription is already enabled. No property change."}}"`, you can ignore the error, continue configuration, and then run the connector to collect events.

The error is caused by an undocumented change in the Office 365 API response behavior. Before this change, when connector requested to start an already started subscription, the API would return a 200 OK response, and it would work fine. Office 365 API has changed the behavior to respond with HTTP error 400, instead of 200. Neither the change in API behavior, nor the new Error# AF20024, have been documented by Microsoft at: https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference [CON-18936]

Connector End-of-Life Notices

SmartConnector Support Ending Soon

SmartConnectors Support Recently Ended

Support Ending 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.

Support Ended 11/20/2017

Lumension PatchLink Scanner DB – Product no longer available.

Support Ended 11/15/2017

Lumension PatchLink Scanner DB – Product no longer available.

Support Ended 10/17/2017

Apache HTTP Server Access File (Legacy) – Use the SmartConnector for Apache HTTP Server Access Multiple File.

Cisco Content Services Switch Syslog (Legacy) – Support ended due to end of support by vendor.

Cisco Firewall Services Module Syslog (Legacy) – Support ended due to end of support by vendor.

Cisco Router non-IOS Syslog (Legacy) – Use the SmartConnector for Cisco IOS Syslog.

Cisco VPN Syslog (Legacy) – Use the SmartConnector for Cisco ASA Syslog.

eEye REM Security Management Console DB (Legacy) – Support ended due to end of support by vendor.

IBM Lotus Domino DB (Legacy) – Support ended due to lack of ODBC support with Java 8.

IBM Tivoli Access Manager File (Legacy) – Support ended due to end of support by vendor. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

IBM Tivoli Access Manager XML File (Legacy) – Support ended due to end of support by vendor. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

QoSient ARGUS (Legacy) – Support ended due to lack of customer demand.

RSA Identity Management Service SNMP (Legacy) – Use the SmartConnector for SNMP Unified.

Sun ONE Web Access Server File (Legacy) – Use the SmartConnector for Sun ONE Web Access Server Multiple File.

VMware ESXi Syslog – Support ended for vCenter versions 2.5, 3.5, 4.0, and 5.0 and ESX/ESXi servers 3.0, 4.0, and 5.0 due to end of support by vendor.