Micro Focus Security ArcSight Connectors

Software Version: 7.12.0.8149.0

Micro Focus SmartConnector Release Notes

Document Release Date: May 8, 2019
Software Release Date: May 8, 2019

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

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

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 7.12.0.8149.0

These notes describe how to apply this latest release of ArcSight SmartConnectors, as well as providing other 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, 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 may test the upgrade in a STAGE (staging) environment to make sure it works as expected prior to upgrading it in PROD (production)

Integrated into this Release

Parser update release 7.11.1.8143.0 has been integrated into this framework release. This release contains version updates, fixed issues, and enhancements for a number of SmartConnectors. For details, see the corresponding release notes on Protect 724:

- 7.11.1.8143.0 Release Notes: https://community.microfocus.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-11-1-8143-0/ta-p/1687107

All the SmartConnectors listed below were updated in this monthly parser update release. SmartConnectors with version numbers in parenthesis have updated version support.

Release 7.11.1.8143.0
-Cisco ASA Syslog -Cisco Secure ACS Syslog -Juniper JUNOS Syslog -IP Flow (Netflow/J-Flow) -McAfee ePolicy Orchestrator DB -Proofpoint Enterprise Protection and Enterprise Privacy Syslog -Symantec Endpoint Protection DB -VMware ESXi Server Syslog

To Apply This Release

Download the appropriate executable for your platform from the Support Web site (https://softwaresupport.softwaregrp.com/), as well as the separate downloadable zip file of 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.

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 Protect 724 (https://community.softwaregrp.com/t5/ArcSight-Connectors/ArcSight-SmartConnectors-with-64-bit-Platform-Support/ta-p/1587669?nm=) 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

None at this time.

New Device, Component, or OS Version Support

SmartConnector for	Number	Version
Symantec Endpoint Protection DB	CON-22187	New support added to SONAR on SEP v14.
	CON-22192	Added support for "Downloaded by" information for Symantec Endpoint Protection DB 14.
Micro Focus SmartConnector for Microsoft Windows Event Log	CON-22295 CON-16956	FIPS mode can be enabled on WISC.
McAfee ePolicy Orchestrator DB	CON-20643	Support for Microsoft SQL Server 2016 with ePO 5.9.

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-21784	Added support for Private IPs.
ArcSight FlexConnector	CON-21962	Installation and Configuration section of the FlexConnector REST Developer's Guide was updated.
VMware Web Services	CON-20500 CON-22027	Some events were not being parsed correctly.
Cisco Secure ACS Syslog	CON-20834	Updated Cisco Secure ACS Failed Attempts and Cisco Secure ACS Passed Authentications event mappings
IP Flow (Netflow/J-Flow)	CON-19978	Updated mappings for IP Flow Version 9
McAfee ePolicy Orchestrator DB	CON-21813	Updated Endpoint Security (ENS) Events with ePO 5.3/5.9 session event mappings.
Symantec Endpoint Protection DB	CON-21391 CON-20100	Support for "Downloaded by" information.

Fixed Issues

SmartConnector for	Number	Description
Cisco ASA Syslog	CON-20575 CON-19489 CON-18048 CON-20017	Some events were being parsed incorrectly
Juniper JUNOS Syslog	CON-16495	Some events were being parsed incorrectly
McAfee ePolicy Orchestrator DB	CON-18310	Some events were being parsed incorrectly.
Proofpoint Enterprise Protection and Enterprise Privacy Syslog	CON-21255	Some events were being parsed incorrectly
Symantec Endpoint Protection DB	CON-16271 CON-20918	Some events were being parsed incorrectly
VMware ESXi Server Syslog	CON-19912	Some events were being parsed incorrectly
Microsoft Windows Event Log - Native	CON-20566	Some events were not being parsed correctly.
	CON-21771	Encryption strength of passwords was modified.
MS Forefront Threat Management Gateway File	CON-21825	Some files were being reprocessed after the connector was restarted.
MS DHCP File	CON-21408	Some lines on the log files were being skipped after the connector was restarted.

Known Limitations

All SmartConnectors

Microsoft Windows Server 2019 is a supported platform. Currently, a message pops, indicating otherwise.
Workaround: Click OK and continue with the installation.
[CON-22453]

All Windows Event Log Connectors, both Native and Unified

If the connector cannot process events fast enough and the internal queue is filled up, it r may stop processing.
Workaround:
None at this time. Users may re-configure the MQ parameters in `agent.properties` to prevent the queue from being filled up.
[CON-19425]

All SmartConnectors

You may not be able to install your connector due to some missing packages.
Workaround:
Make sure 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 workaround:

For Solaris Connectors installed as a Standalone:

1. If Solaris connector is already installed as a standalone, locally upgrade to 7.12.0.8149.0

Solaris Connectors 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 7.12.0.8149.0.
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 setter in the `<connector_install_location>\current\user\agent\map location`, and the connector runs out of memory, then you can add the following property to `agent.properties` to work-around the problem:

```
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, then 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]

EPS rates

The smart connector should be considered for collecting data from multiple Windows endpoints, each of the end points generating around 200 EPS. As normal, EPS rates will vary with the size of the events processed. For reaching higher EPS rates, you could configure more endpoints or consider using the native connector.

File reader connectors may use the highest processing power available to make fast readings, reaching the highest achievable EPS rate. Other factors such as additional destinations, may reduce EPS for these particular connector types. Also, running other third-party processes may compete with the connector running at the same or lower the priority. The result might be less CPU cycles which lead to reduced EPS.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 10/22/2019

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

SmartConnectors Support Recently Ended

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.