Micro Focus Security ArcSight Connectors

Software Version: 7.11.0.8139.0

Micro Focus SmartConnector Release Notes

Document Release Date: January 25, 2019
Software Release Date: January 25, 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 7.11.0.8139.0

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 releases 7.10.1.8123.0 through 7.10.2.8128.0 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 Protect 724:

- 7.10.1.8123.0 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-10-1-8123-0/ta-p/1675327
- 7.10.2.8128.0 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-10-2-8128-0/ta-p/1679668

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

Release 7.10.1.8123.0	**Release 7.10.2.8128.0**
-Microsoft Office 365 -Cisco ASA Syslog -Check Point Syslog -Cisco Syslog Connectors -NetApp Filer Syslog -Fortinet Fortigate -CheckPoint Syslog -Tenable Nessus File -Microsoft IIS Multiple Server -McAfee ePolicy Orchestrator -Microsoft SCCMDB -Linux Audit File -MS SharePoint Server DB -Cisco Wireless LAN Controller Syslog -Cisco ISE Syslog	-Microsoft Office 365 -IBM AIX Audit Syslog -IBM WebSphere File -IBM eServer iSeries Audit Journal File -McAfee Network Security Manager IDbased DB -McAfee Network Security Manager Timebased DB -Check Point Syslog -Fortinet Fortigate -Snort Syslog -Cisco IOS Syslog -Pulse Secure Connect Syslog -Juniper JUNOS Syslog -All Cisco Syslog Connectors -Cisco ASA Syslog -Symantec Endpoint -Oracle WebLogic Server File -Pulse Secure Connect 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

SmartConnector for	Description
AWS Cloudwatch	New support for Diagnostic, Audit, Sign-In Log and Activity Log.
Microsoft DNS DGA Trace Log Multiple Server File	New support for map files.

New Device, Component, or OS Version Support

SmartConnector for	Number	Version
All Smart Connectors	CON-21268	New feature: Global Event ID
Linux Audit File	CON-20809 CON-20818	Added support for RHEL 7.5
	CON-20817 CON-20691	Added support for RHEL 7.4
MS SharePoint Server DB	CON-19573	Added support for SharePoint 2016
Cisco Wireless LAN Controller Syslog	CON-21036	Added support for Cisco Wireless IAN controller 8.3.141.0
Cisco ISE Syslog	CON-18576	Added support for Cisco ISE 2.2
Oracle WebLogic Server File	CON-21531	Support for WebLogic Server version 10.3.6
Pulse Secure Connect Syslog	CON-20423	Support for Pulse Secure v 8.3
Microsoft Azure Monitor Event Hub	CON-21784	Support for private IPs with VNET

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
CheckPoint Syslog	CON-20770	Added support for R80 FG module. Updated mappings for R80 VPN-1 and FireWall-1, R80 Application Control, R80 Identity Awareness, R80 URL Filtering, R80 Log Update and R80 VPN-1
	CON-21564	Updated R80 and R77 Common Syslog Event Mappings
Snort Syslog	CON-19789	Added support for Snort Key-Value Events

Tenable Nessus File	CON-21107	Added support for Nessus 7.0
McAfee ePolicy Orchestrator DB	CON-19553	Added support McAfee Data Loss Prevention 11.0 for McAfee ePolicy Orchestrator (ePO) DB 5.9
MS Office 365	CON-20909	Updated mappings for Exchange Online Admin
IBM AIX Audit Syslog	CON-21406	Updated IBM AIX Audit Event Mappings to ArcSight Fields
IBM WebSphere File	CON-20978	Updated some mappings for WebSphere System.out Field Mappings
McAfee Network Security Manager ID based DB McAfee Network Security Manager Timebased DB	CON-20920	Updated NSM 9.x Mappings Updated NSM 9.x Payload Mappings
Fortinet Fortigate Syslog	CON-21006	Updated Fortigate Mappings to ArcSight ESM Fields
Symantec Endpoint Protection DB	CON-21437	Added new mappings for Agent Events

Fixed Issues

SmartConnector for	Number	Description
Microsoft Office 365	CON-20811 CON-20919 CON-21195	Some events were being parsed incorrectly.
Cisco ASA Syslog	CON-21293 CON-21277 CON-21096 CON-20923	Some events were being parsed incorrectly.
HPE Aruba Mobility Controller Syslog	CON-20822	Some events were being parsed incorrectly.
MS DNS Trace Log Multiple Server File	CON-17482	Some events were being parsed incorrectly.
Check Point Syslog	CON-20966	Some events were being parsed incorrectly.
Cisco Syslog Connectors	CON-21005	Some events were being parsed incorrectly.
UNIX OS Syslog	CON-21176	Some events were being parsed incorrectly.
Pulse Connect Secure Syslog	CON-21011	Some events were being parsed incorrectly.
NetApp Filer Syslog	CON-17630	Some events were being parsed incorrectly.
Oracle Weblogic Server File	CON-21068	Some events were being parsed incorrectly.
Fortinet Fortigate Syslog	CON-21284	Some events were being parsed incorrectly.
MS IIS Multiple Server File	CON-17301	Some events were being parsed incorrectly.
Juniper JUNOS Syslog	CON-21149	Events with new timestamp will be supported in CON-20064.
Microsoft SCCMDB	CON-21285	Some events were being parsed incorrectly.
Cisco IOS Syslog	CON-20645	Some events were being parsed incorrectly.
Pulse Secure Connect Syslog	CON-21210	Some events were being parsed incorrectly

Juniper JUNOS Syslog	CON-21516	Some events were being parsed incorrectly
All Cisco Syslog Connectors	CON-20067	Some events were being parsed incorrectly
	CON-21395	Some events were being parsed incorrectly
Symantec Endpoint Protection DB	CON-21416	Some events were being parsed incorrectly
Cisco Wireless LAN Controller Syslog	CON-21448	Some events were being parsed incorrectly
IBM eServer iSeries Audit Journal File	CON-21294 CON-15112	Updated Audit Journal TYPE 5 Mappings

Known Limitations

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 7.11.0.8139.0

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 7.11.0.8139.0 .
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

None at this time.

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.