Micro Focus Security ArcSight Connectors

Software Version: 7.10.0.8114.0

Micro Focus SmartConnector Release Notes

Document Release Date: October 22, 2018
Software Release Date: October 22, 2018

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 7.10.0.8114.0

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 7.9.1.8098.0 through 7.9.2.8100.0 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:

- 7.9.1.8098.0 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-9-1-8098-0/ta-p/1658653
- 7.9.2.8100.0 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-9-2-8100-0/ta-p/1662478

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

Release 7.9.1.8098.0	**Release 7.9.2.8100.0**
MS Windows Event Log Native Microsoft Exchange MailBox Store Snort Multiple File Connector NetApp Filer Syslog McAfee Network Security Manager Syslog Symantec Endpoint Protection DB Config IBM AIX Syslog Microsoft DNS Multiple Server File Linux Audit Syslog Fortinet FortiGate Syslog MS Office 365 Checkpoint Syslog MS SQL Server Audit Win Event Log Native Config	Oracle Audit Syslog Cisco ASA Syslog Cisco IOS Syslog Linux Audit Syslog F5 BIG-IP Syslog Citrix NetScaler Syslog Juniper Firewall ScreenOS Syslog Juniper JUNOS Syslog Checkpoint Syslog CiscoPIX-ASA-Syslog CiscoIronPortSyslog NetAppFilerSyslog JuniperFWScreenOS SyslogSendmailConfig HPE Integrated Lights-Out Syslog Microsoft SQL Server Audit Windows Event Log Native

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/tap/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 Support

SmartConnector for	Description
Microsoft Azure Event Hubs	New support for Diagnostic, Audit, Sign-In Log and Activity Log. **Note:** This Connector is currently using a beta library: Microsoft Azure Functions Java Core Types 1.0.0-beta-5

New Device, Component, or OS Version Support

SmartConnector for	Version
ApacheTomcatFileConfig	Apache Tomcat file support for Tomcat version 8.0 and 9.0.
MS Windows Event Log Native	New support for MailBox Store - Microsoft Exchange 2010 EventID 1016.
	Added support for Windows 2008 R2 EventID 1074.

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
Oracle Audit Syslog	CON-20928	Added support for Decoding of SES_ACTIONS Field.
	CON-20237	Added support for complete ACTION Fields.
MicrosoftIISMultiServerConfig	CON-19919	Added mapping for "X-Forwarded-For" field to source address.
MicrosoftSQLServerAuditWinEvtLogNativeConfig	CON-20561 CON-20511	Mappings were updated.
MicrosoftExchangeMailBoxStoreWinEvtLogNativeConfig	CON-20260	New support for MailBox Store - Microsoft Exchange 2010 EventID 1016.
Symantec Endpoint Protection DB	CON-18790 CON-19662	Updated event mappings for agent-behaviour, virus-category and alerts.
Linux Audit Syslog	CON-19758 CON-19746 CON-20081	Mappings were updated.
Fortinet Fortigate Syslog	CON-20168	Mappings were updated.
MS Windows Event Log Native	CON-21154	Mappings were updated.
MS Office 365	CON-20101 CON-20725	Mappings were updated.
Microsoft Windows Event Log	CON-21086	Custom Parser or override limitation.
Checkpoint Syslog	CON-20078 CON-19923	Added support for: Connectra, Anti Virus, Security Gateway/Management, Linux OS,

	CON-20502 CON-21157 CON-21160	Syslog, Threat Emulation, Anti Bot and Anti Virus.
	CON-20623 CON-20635 CON-20757 CON-20628 CON-21219	Added support for VPN-1 and Log Update Modules. Updated R80 VPN-1 and R80 Log Update Event Mappings. Updated R77 Threat Emulation Event Mappings.
HPE Integrated Lights-Out Syslog	CON-20821	Added support for Gen10 and iLO 5.
CiscoPIX-ASA-Syslog, CiscoIOSSyslog, JuniperJUNOSSyslog, CiscoIronPortSyslog, NetAppFilerSyslog, JuniperFWScreenOSSyslog, SendmailConfig	CON-20403	Added/Updated Device Facility field.
Applicable to all connectors	CON-21347	Voltage Simple API Java 5.20 client is now supported for both Linux and Windows. If deploying Voltage client through ArcMC, (Instant deployment and Voltage client upgrade/install), the only client version available is 5.10.

Fixed Issues

Reduced EPS to Logger Destination was fixed for **7.10.0.8114.0**

SmartConnector for	**Number**	**Description**
F5BIG-IPsyslogConfig	CON-21327	There are some new event of F5 BIG-IP connector need to be supported. Device event category.
	CON-20939 CON-17218 CON-20717 CON-17994	Some events were being parsed incorrectly.
McAfee Network Security Manager Syslog	CON-19900	Some events were not being parsed.
NetApp Filer Syslog	CON-18612	Some events were not being parsed.
Microsoft DNS Multiple Server File	CON-19055 CON-21174	Some events were not being parsed.
IBM AIX Syslog	CON-20677	Some events were not being parsed.
Snort Multiple File Connector	CON-18789	Some events were not being parsed.
Symantec Endpoint Protection DB Config	CON-20507	Some events were not being parsed.
Citrix NetScaler Syslog	CON-20787	Some events were being parsed incorrectly.
Juniper Firewall ScreenOS Syslog	CON-20945	Some events were being parsed incorrectly.
Juniper JUNOS Syslog	CON-20354 CON-19891 CON-19604 CON-20011	Some events were being parsed incorrectly.
Cisco ASA Syslog	CON-21019 CON-20775 CON-20555	Some events were being parsed incorrectly.

Cisco IOS Syslog	CON-20776	Some events were being parsed incorrectly.
Linux Audit Syslog	CON-21090	Some events were being parsed incorrectly.
SAPAuditConfig	CON-19913 CON-21417	Some events were being parsed.
IBMWebSphere	CON-21288	Some events were being parsed.
BroIDSNGFile	CON-20088	When using Bro IDS NG File Connector, new. Gz files not picked up to be processed.
Syslog File	CON-15207	To hide the port and protocol in agent.properties.
	CON-20724	Some events were being parsed incorrectly.

Known Limitations

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

SmartConnector for Microsoft Windows Event Log should be considered for collecting data from multiple Windows endpoints; each of the end points generates 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.