



Micro Focus Security ArcSight Connectors

Software Version: 7.13.0.8194.1P1

Micro Focus SmartConnector Release Notes

Document Release Date: October 11, 2019

Software Release Date: October 11, 2019

Legal Notices

Copyright Notice

© Copyright 2010 - 2019 Micro Focus or one of its affiliates.

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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 7.13.0.8194.1** 4
 - Purpose of this patch** 4
 - To Verify Your Upgrade Files** 4
 - Integrated into this Release** 4
 - To Apply This Release** 5
- Fixed Issues**..... 5
- Known Limitations**..... 6
- Connector End-of-Life Notices** 7
 - Support Ending 10/22/2019 7
 - Support Ended 11/20/2017** 8
 - Support Ended 11/15/2017** 8
 - Support Ended 10/17/2017** 8

SmartConnector Release 7.13.0.8194.1

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.

Purpose of this patch

- To display the number of pre-aggregated events on the “ESM to ArcSight” event field: flexnumber1.
- To fix license counting related issues.
- To integrate parser updates from parser releases 7.13.1 and 7.13.2.

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.mfgr.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 7.13.1.8184.0 and 7.13.2.8187.0 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.

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.

Fixed Issues

SmartConnector for	Number	Description
All SmartConnectors	CON-22937	Description: The Flexnumber1 field now displays the number of pre-aggregated events to be SLC and the flexnumber1Label field shows "pre-aggregation Event count (SLC)".
	CON-22968	SmartConnectors 7.13.0 P1 now include the flexnumber1 in agent 050 by default.
	CON-22985	Description: reduces counting and licensing data loss, in case, the connector restarts before the generation of an agent 050.. Agent 050 has been decreased from 12 hours to 1 hour.

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 **7.13.0.8194.1**

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 **7.13.0.8194.1**.
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

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.

Micro Focus Connectors 7.13.0.8194.1

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.