Micro Focus Security ArcSight Connectors

Software Version: 7.13.0.8178.0

Micro Focus SmartConnector Release Notes

Document Release Date: July 24, 2019
Software Release Date: July 24, 2019

Legal Notices

Copyright Notice

Trademark Notices

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 7.13.0.8178.0

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:

- 7.12.1.8159.0 Release Notes
- 7.12.2.8163.0 Release Notes

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

Release 7.12.1.8159.0
-Apache HTTP Server Syslog -Dell Change Auditor DB 6.9 -Cisco ASA Syslog -Cisco IronPort Email Security Appliance File -Cisco ISE Syslog -Cisco Secure ACS Syslog -CitrixNet Scaler Syslog -HPE Aruba Mobility Controller Syslog -IBM Site Protector DB -Juniper JUNOS Syslog -Juniper Firewall ScreenOS Syslog -Linux Audit File -Linux Audit Syslog -McAfee ePolicy Orchestrator DB -McAfee Network Security Manager ID based -McAfee Network Security Manager DB (Time-based) -MS DNS Trace Log Multiple Server File -MS Forefront Threat Management Gateway File -MS Office 365 -Oracle Audit DB -Oracle Audit XML File -Oracle SYSDBA Audit Multiple Folder DB -Oracle Audit Syslog -Oracle Audit Windows Event Log Native -Symantec Endpoint Protection DB -Symantec Data Center Security DB-UNIX Login/Logout File

Release 7.12.2.8163.0
-Check Point Syslog -Cisco IronPort Email Security Appliance Syslog -Cisco ISE Syslog -HPE H3C Syslog -HPE Aruba Mobility Controller Syslog -McAfee ePolicy Orchestrator DB for ENS 10.5 with ePO 5.10. -McAfee ePolicy Orchestrator DB for MSME 8.6 with ePO 5.10. -MS DNS Trace Log Multiple Server File for MS Windows Server 2019 -MS Windows Event Log Native: -Microsoft Windows Update Events -Microsoft-Windows PowerShell/Operational -Oracle Unified Audit Trail DB -Proofpoint Enterprise Protection and Enterprise Privacy Syslog -Pulse Secure Pulse Connect Secure Syslog -Sophos Anti-Virus DB version 10.8 -Tenable Nessus .nessus File -Windows Powershell

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
IBM Big Fix REST API	CON-17034	IBM BigFix, is a system-management software product developed by IBM for managing large groups of machines running in Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android.

Kafka FlexConnector	CON-20491	This new connector can subscribe to a Kafka server, receive and process data.

New Device, Component, or OS Version Support

This release contains a new version of Load Balancer, for more information see:

Load Balancer 1.4 Release Notes
Load Balancer 1.4 Configuration Guide

SmartConnector for	Number	Description
All SmartConnectors	CON-22444	Zulu JRE 8u212 has been integrated to resolve several security vulnerabilities
Tenable Nessus .nessus File	CON-22426	Added support for Tenable Nessus .nessus File version 8.3.1
Microsoft Windows Event Log - Native	CON-22406	Added support for Windows PowerShell in WINC connector for the following log types: -Windows Powershell -Microsoft-Windows-PowerShell/Operational
Oracle SYSDBA Audit Multiple Folder DB	CON-21871	Added support for Oracle SYSDBA Audit Multiple Folder DB v18c
	CON-20551	Added support to Multitenant Architecture
Oracle Audit XML File	CON-21861	Added support for Oracle Audit XML File v18c
Oracle Audit Windows Event Log Native	CON-21859	Added support for Oracle Audit Windows Event Log - Native v18c
Oracle Audit Syslog	CON-21857	Added support for Oracle Audit Syslog v18c
Oracle Audit DB	CON-21856	Added support for Oracle Audit DB v18c
	CON-20552	Added support to Multitenant Architecture
Symantec Endpoint Protection DB	CON-21477	Added support for SEP DB 14.2 x SmartConnector 7.9
McAfee ePolicy Orchestrator DB	CON-21192	Added support for McAfee Application and Change Control (SolidCore) 6.2 with ePO 5.3
	CON-20175	
Dell ChangeAuditor DB	CON-20510	Added support for Dell Change Auditor DB 6.9
Symantec Data Center Security DB	CON-20062	Added support for Symantec Data Center Security DB vs.6.7
IBM Site Protector DB	CON-18978	Added support for Proventia Network Intrusion Prevention System and Security Network Protection
MS DHCP File	CON-21839	Added support for MS DHCP File with Windows Server 2019
AWS Cloudwatch	CON-22502	Users can now create custom text maps to parse events in text format.
	CON-22389	Users can now create custom JSON maps to parse events in JSON format.

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 Unified Audit Trail DB	CON-20014 CON-20085	Updated Oracle Unified Audit Trail 12c Database Field Mappings.
Apache HTTP Server Syslog	CON-22020	Updated parsing for "Message forwarded from" syslog messages. Fix: Added Apache HTTP Server Syslog Mappings.
FlexConnector REST	CON-20021	Updated multiple timestamp support
Oracle Unified Audit Trail DB	CON-22012	Device version and destination host name fields were not mapped correctly Fix: Updated Oracle Unified Audit Trail 12c Database Field Mappings.
MS Forefront Threat Management Gateway File	CON-22004	The data c-agent should be mapped to requestClientApplication. Fix: Updated Threat Management Gateway 2010 Web Proxy Service Log Mappings and Threat Management Gateway Firewall Service Log mappings.
Symantec Endpoint Protection DB	CON-21833	Added: -Additional fields for GROUP_NAME -GROUP_TYPE for virus category
McAfee ePolicy Orchestrator DB	CON-21389	Updated Endpoint Security (ENS) Events with ePO 5.3/5.9 mappings.
Linux Audit Syslog/ Linux Audit File	CON-21290	Updated Mappings to ArcSight fields in order to cover hash values.
All SmartConnectors	CON-22385	Users can now set a limit for unparsed events. When the number of unparsed events reaches the limit, the feature is temporarily disabled and as soon as the event queue normalizes, the feature is re-enabled and the destinations start receiving unparsed events again.
	CON-9866	Command groups are now placed and categorized by the Commands Queue feature, based on their priority. This prevents commands from conflicting among each other when being executed at the same time.

Fixed Issues

SmartConnector for	Number	Description
Pulse Secure Pulse Connect Secure Syslog	CON-22474	There was a mapping issue with the field event.deviceHostName. Fix: Updated the “Device Event Mapping to

		ArcSight Fields”
Check Point Syslog	CON-22472	Some audit events of Checkpoint R80 module CLI were not being parsed. Fix: Updated R80 Common Audit Event Mappings and R80 CLI Event Mappings.
McAfee Network Security Manager DB (Time-based)	CON-22277	Catalog query issue.The connector was displaying a “Severe Network Attack” when an old event was received. Fix: The “name” field was updated and the error is no longer being displayed.
Cisco Secure ACS Syslog	CON-22081	The length of raw events of the connector was reaching the limit. Fix: If a truncate error related to UNIX events is displayed, add the following parameter in "agent.properties".
Squid Web Proxy Server File	CON-22002	Client user name should be event.sourceUserName. Fix: Updated Squid Web Proxy Server Mappings.
Citrix NetScaler Syslog	CON-20596	“Unparsed Event” error was being displayed with PID 32 bit boundary. Fix: Updated Citrix NetScaler mappings to ArcSight fields.
McAfee ePolicy Orchestrator DB	CON-20404	Endpoint Security (ENS) events with ePO 5.3/5.9 did not have a SourcePort field, which prevented the connector from pulling data from that table. Fix: Updated event mappings for Endpoint Security (ENS) events with ePO 5.3/5.9 and VirusScan Enterprise 8.8 events with ePO 5.1/5.3/5.9 sections.
McAfee Network Security Manager DB (ID-based)	CON-19861	Catalog query issue.The connector was displaying a “Severe Network Attack” when an old event was received. Fix: The “name” field was updated and the error is no longer being displayed.
All SmartConnectors	CON-19495	When running `agentsetup`, the error “No connector found at the specified port” was displayed. Fix: 1. Go to `ARCSIGHT_HOME\user\connectorappliance\connector_config.xml`. 2. Replace the default port with the one in the error message. 3. Save the file and run `agentsetup` again.
Microsoft Azure Monitor Event Hub	CON-22071	Unexpected errors while the connector was running. This issue has been fixed.

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 **7.13.0.8178.0**

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 **7.13.0.8178.0.**
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

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.