Micro Focus Security ArcSight Connectors

Software Version: 7.8.0

Micro Focus SmartConnector Release Notes

Document Release Date: April 16, 2018
Software Release Date: April 16, 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 7.8.0.8070.0

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://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

Integrated into this Release

Parser update releases 7.7.1.8037 through 7.7.6.8063 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:

- 7.7.1 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ParserUpdate-7-7-1-8037-Release-Notes/ta-p/1619388
- 7.7.2 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ParserUpdate-7-7-2-8042-Release-Notes/ta-p/1622827
- 7.7.3 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ReleaseNotes-7-7-3-8053/ta-p/1626753
- 7.7.4 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ParserUpdate-Release-Notes-7-7-4-8056-0/ta-p/1630010
- 7.7.5 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ReleaseNotes-7-7-5-8060-0/ta-p/1634457
- 7.7.6 Release Notes: https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-ReleaseNotes-7-7-6-8063-0/ta-p/1638508

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

Release 7.7.1.8037	**Release 7.7.2.8042**
• Syslog SmartConnectors issues • Barracuda Email Security Gateway Syslog (v8.0) • Blue Coat Proxy SG Syslog • Check Point OPSEC NG • Cisco ASA Syslog • Cisco IOS Syslog • Cisco IronPort Email Security Appliance File (v10.0) • Cisco IronPort Email Security Appliance Syslog (v10.0) • Citrix NetScaler Syslog • F5 BIG-IP Syslog • Fortinet FortiGate Syslog • HPE H3C Syslog • HPE Operations Manager I Web Services	• Blue Coat Proxy SG Syslog • Citrix NetScaler Syslog • Juniper JUNOS Syslog • Linux Audit Syslog • McAfee ePolicy Orchestrator DB (Orion Audit Log v5.1 and Policy Auditor v6.2, both on ePO v5.3) • Microsoft Office 365 (OneDrive) • Microsoft SQL Server Audit Windows Event Log Native (Microsoft SQL Server 2016) • Pulse Secure Pulse Connect Secure Syslog • Symantec Endpoint Protection DB (v14.0 Anti-Virus and Anti-Spyware Protection Events).

• HPE ProCurve Syslog • HPE UX Syslog • McAfee ePolicy Orchestrator DB (DLP 10.0 with ePO 5.3) • Rapid7 NeXpose XML File (v6.3)	

Release 7.7.3.8053	**Release 7.7.4.8056**
• Check Point Syslog • Cisco ASA Syslog • Cisco IOS Syslog • Cisco IronPort Email Security Appliance Syslog • Cisco Secure ACS Syslog • Cisco Wireless LAN Controller Syslog • McAfee ePolicy Orchestrator DB (Data Exchange Layer 3.0.1 with ePO 5.3) • Symantec Endpoint Protection DB • VMware Web Services (vCenter 6.5 on ESXi 6.5)	• Syslog SmartConnectors issues • Check Point Syslog (Modules: ESOD, Eventia Analyzer Server, Identity Logging, and VPN-1 Edge for R77.30) • Cisco ASA Syslog • F5 BIG-IP Syslog (Access Policy Module (APM) 11.6) • Juniper JUNOS Syslog (15.1 MX Series Virtual Chassis, MX960 router) • IBM SiteProtector DB • Linux Audit File (RHEL 6.7) • Linux Audit Syslog (RHEL 6.7) • McAfee ePolicy Orchestrator DB • Pulse Secure Pulse Connect Secure Syslog • Symantec Endpoint Protection DB • UNIX OS Syslog (RHEL 6.7 and 7.3)

Release 7.7.5.8060	**Release 7.7.6.8063**
• HPE Aruba Mobility Controller Syslog • Blue Coat Proxy SG Syslog • Proofpoint Enterprise Protection and Enterprise Privacy Syslog • Citrix NetScaler Syslog Config	• McAfee ePolicy Orchestrator DB • Microsoft SQL Server Multiple Instance Audit DB

To Apply This Release

Download the appropriate executable for your platform from the Support Web site (https://softwaresupport.hpe.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.

Both 32-bit and 64-bit executables are available for download for Windows and Linux platforms. Only a 64-bit executable is provided for Solaris platforms. The 32-bit Solaris image is no longer supported. 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.saas.hpe.com/t5/ArcSight-Connectors/HPE-ArcSight-SmartConnectors-with-64-bit-PlatformSupport/ta-p/1587669) 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.

Reduced EPS to Logger Destination

Important: If you have not upgraded to 7.8.0, this step is not necessary.

A degradation in performance over time has been observed while using SmartConnector 7.8. with Logger. Please refer to the following Oracle links for more details:

Java Release notes - http://www.oracle.com/technetwork/java/javase/8u161-relnotes-4021379.html

JDK Bug - https://bugs.openjdk.java.net/browse/JDK-8199463

To avoid this issue:

Perform these steps preferably before upgrading the Connector to 7.8.

1. Update the `agent.wrapper.conf` file.

   For ArcMC Managed Connectors Use the Diagnostics Wizard to update the agent.wrapper.conf. See "Running Diagnostics on a Container" (page 118) on A*rcSight Management Center Administrator's Guide).*

   For Unmanaged Connectors, use the `agent.wrapper.conf` file located in ***CONNECTOR_HOME/user/agent***.

   a. Add `-Djdk.tls.useExtendedMasterSecret=false` *in* `agent.wrapper.conf`

   b. Add the following line and specify the correct (incremental) number after the `wrapper.java.additional` property.

```
# Mode in which the service is installed.  AUTO_START or DEMAND_START
wrapper.ntservice.starttype=AUTO_START
wrapper.java.command=../../../jre/bin/java

wrapper.java.additional.1=-server
wrapper.java.additional.2=-XX:MaxNewSize=128m
wrapper.java.additional.3=-verbose:gc
wrapper.java.additional.4=-DARCSIGHT_HOME=../../../
wrapper.java.additional.5=-Djava.security.policy=../../../config/agent/agent.policy
wrapper.java.additional.6=-Djsse.enableSNIExtension=false
wrapper.java.additional.7=-XX:+HeapDumpOnOutOfMemoryError
wrapper.java.additional.8=-XX:HeapDumpPath=../../../user/agent
wrapper.java.additional.9=-Djava.security.egd=file:/dev/urandom
wrapper.java.additional.10=-Djdk.tls.useExtendedMasterSecret=false

wrapper.ntservice.name=arc_SyslogArcMC_b8070_PerfIssue
wrapper.ntservice.displayname=ArcSight SyslogArcMC_b8070_PerfIssue
wrapper.ntservice.description=ArcSight SyslogArcMC_b8070_PerfIssue
wrapper.ntservice.starttype=DEMAND_START
```

   c. Restart the Connector.

2. Restart <u>all</u> Logger Apache servers, including single Logger destinations and Logger pool. This step may be executed once all the connectors pointing to logger/logger pool are updated.

   Note: Ensure the parameter is applied to <u>all</u> the 7.8.0 <u>connectors that send events</u> to Logger/Logger Pool.

New SmartConnector Support

SmartConnector for	New Device, Component, or OS Version
Microsoft Windows Event Log	Windows Event Log
CA ACF2 for IBM z/OS File	CA ACF2 REL 15
ArcSight FlexConnector JSON Multiple Folder Follower	

New Device, Component, or OS Version Support

SmartConnector for	Version
Check Point Syslog	R80.10 (15 modules – See the configuration guide for details.)
SNMP Unified	8.2 (RSA Authentication Manager/Identity Management Service)
VMware ESXi Syslog	6.5
McAfee ePolicy Orchestrator DB	VSE 8.8 and ENS 10.5 with ePO 5.9
McAfee ePolicy Orchestrator DB	HIPS 8.0 with ePO 5.9 [CON-19547]
UNIX OS Syslog	RHEL 7.4 [CON-19541]
McAfee Network Security Manager DB (ID-based)	Network Security Manager 9.1 [CON-19438]
McAfee Network Security Manager DB (Time-based)	Network Security Manager 9.1 [CON-19438]
McAfee Network Security Manager Syslog	Network Security Manager 9.1 [CON-19439]
Rapid 7 NeXpose XML File	Rapid 7 NeXpose 6.4.42 [CON-19451]

McAfee ePolicy Orchestrator DB	• Added support for McAfee MOVE AV Agentless 4.5.1 with ePO 5.9. • Added support for McAfee Application and Change Control 8.0 with ePO 5.9. • Added support Data Exchange Layer module version 4.0 for McAfee ePolicy Orchestrator DB version 5.9. • Added support Policy Auditor module version 6.2 for McAfee ePolicy Orchestrator DB version 5.9. • Added Support RSD module version 5.0.5 for McAfee ePolicy Orchestrator DB version 5.9. • Added support for SiteAdvisor Enterprise (SAE) 3.5.5 with ePO 5.9. • Added support for McAfee Drive Encryption 7.2.3 with ePO 5.9. • Added support for MSME 8.5 with ePO 5.9. • Added support TIE for VSE module version 1.0 for McAfee ePolicy Orchestrator DB version 5.3.
Microsoft SQL Server Multiple Instance Audit DB	Added support for Microsoft SQL Server 2016.

SmartConnector Enhancements

In each SmartConnector release, updates and enhancements 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.

McAfee ePolicy Orchestrator DB

Added support for SourceFilePath (available in EPExtendedEventMT table) and SourceProcessName (available in EPOEvents view). Also made updates to the main query and added the following new mappings:
- event.sourceProcessName=ThreatSourceProcessName
- event.oldFilePath=ThreatSourceFilePath [CON-19379]

McAfee ePolicy Orchestrator DB

Added a new mapping for the database name for “File Type” in Endpoint Security module. [CON-19613]

Pulse Secure Pulse Connect Secure Syslog

Added support for some v8.1 events using the WebTrends Enhanced Log File (WELF) event format that were previously unparsed. [CON-17405] ***VMWare ESX Syslog***

Added additional mappings. [CON-19877]

Fixed Issues

SmartConnector for	Number	Description
Cisco NX-OS Syslog	CON-19195	Some v7.3 events were not being parsed. This issue has been fixed.
Amazon Web Services CloudTrail	CON-19019	Updated mapping for event.deviceReceiptTime.
F5 BIG-IP Syslog	CON-13550	Some v10.2.4 events were not being parsed correctly. This issue has been fixed.
McAfee ePolicy Orchestrator DB	CON-19597 CON-19614	The UTC string in 'Device Custom Date 1 Label' has been removed from the following modules to indicate a more general timestamp: dlpdiscover, dlpincident, epoevents, hips 'Device Receipt Time' and 'Device Custom [1]Date 1' values had been converted incorrectly. This issue has been addressed and corrected in the following modules: siteadvisor, virusscan, epoevents, virusscan, dlpadministrative, dlpdiscover, dlpincident, solidcore, hips, msme, dlp, move, endpointsecurity
Pulse Secure Pulse Connect Secure Syslog	CON-19820	Added support for some v8.1 events that were previously unparsed.
	CON-19540 CON-19766	Added support for some v8.2 events that were previously unparsed.
McAfee Network Security Manager Syslog	CON-19339	Events containing four character timezones where parsing incorrectly. This issue has been fixed.
Cisco ASA Syslog	C478	Mapping information for additional fields was incorrect; should map to DCS. This issue has been fixed.
	CON-19652	Event ID 751025 was showing as an unparsed event. This issue has been fixed.
	CON-19606	Some events were unparsed. This issue has been fixed.
	CON-19781	Events for Shun Added/Deleted needed different mapping. This issue has been fixed.
	CON-19778	Some events were unparsed. This issue has been fixed.
	CON-19738	For version 9.1, some events were unparsed. This issue has been fixed.
	CON-19373	Some events were unparsed. This issue has been fixed.

Cisco IOS Syslog	CON-19277	Some events were unparsed. This issue has been fixed.
	CON-19463	Some events were unparsed. This issue has been fixed.
	CON-19377	Some events were unparsed. This issue has been fixed.
Check Point Syslog	CON-19930	Performance issue after upgrade. This issue has been fixed.
Cisco ISE Syslog	CON-19557	Some events were unparsed. This issue has been fixed.
HPE Aruba Mobility Controller Syslog	CON-19967	Some events were unparsed. This issue has been fixed.
	CON-19968	
	CON-19969	
	CON-19974	
	CON-19979	
	CON-19093	
	CON-19931	
	CON-19942	
	CON-19943	
	CON-19944	
	CON-19946	
	CON-19948	
	CON-19949	
	CON-19950	
	CON-19959	
	CON-19960	
	CON-19961	
	CON-19963	
	CON-19997	
	CON-19999	
	CON-20000	

SmartConnector for	Number	Description
	CON-20001	
	CON-20002	
	CON-20019	
	CON-20020	
	CON-20022	
	CON-20023	
Pulse Secure Pulse Connect Secure Syslog	CON-19580	Some events were unparsed. This issue has been fixed.
HPE Aruba Mobility Controller Syslog	CON-19841	Some events were unparsed. This issue has been fixed.
Blue Coat Proxy SG Syslog	CON-19279 CON-19272 CON-19916	Some events were unparsed. This issue has been fixed.
Proofpoint Enterprise Protection and Enterprise Privacy Syslog	CON-19575	Some events were unparsed. This issue has been fixed.
Citrix NetScaler Syslog Config	CON-19686	Some events were unparsed. This issue has been fixed.
BlueCoat Proxy SG Multiple Server File	CON-19225	Added support for Blue Coat Advanced Security Gateway (ASG) v9 events.
Amazon Web Services CloudTrail	CON-19846	Added support for AWS S3 events.
Amazon Web Services CloudTrail	CON-19952	Added support for some new tokens in AWS S3 events that were not being captured.
Amazon Web Services CloudTrail	CON-20120	Added support for some new tokens in AWS S3 events that were not being captured.
F5 Big-IP syslog	CON-19806	Added support for F5 Traffic Management Operations System (TMOS) v13 events.
F5 BIG-IP Syslog	CON-13550	Some v10.2.4 events were unparsed. This issue has been fixed.
	CON-19378	Some F5 TMOS v12.1.2 events were unparsed. This issue has been fixed.
	CON-19422	Some F5 TMOS v12.1.2 events were unparsed. This issue has been fixed.
	CON-19647	Some F5 TMOS v12.1.2 events were unparsed. This issue has been fixed.
	CON-19790	Some F5 TMOS v11.4.0 events were unparsed. This issue has been fixed.

McAfee ePolicy Orchestrator DB	CON-19517	HIPS 8.0 events on ePO 5.3 were captured incorrectly. This issue has been fixed.
	CON-19597	Timestamps were not being parsed correctly. This issue has been fixed.
	CON-19614	Time zones were not being parsed correctly. This issue has been fixed. This fix applies for the following modules: siteadvisor, virusscan, epoevents, virusscan, dlpadministrative, dlpdiscover, dlpincident, solidcore, hips, msme, dlp, move, endpointsecurity.

Known Limitations

All SmartConnectors

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]

RHEL 7.4 and CentOS 6.9

The connector ignores the preservestate flag. So every time that the connector is restarted, it will start collecting events, as per the startatend flag status, and not from where it last stopped event collection. This may cause event loss or duplication depending on the startatend flag status. Please contact Support to get a hotfix build for this issue. [CON-20697]

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.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 4/28/2018

Support ending for all 32-bit SmartConnectors – Use 64-bit SmartConnectors.

SmartConnectors Support Recently Ended

Support Ended 11/20/2017

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

Support Ended 02/21/2018

Symantec Endpoint Protection DB – SEP version 11 support ended by vendor.

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

Support Ended 02/21/2018

Symantec Endpoint Protection DB – SEP version 11 support ended by vendor.

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.

Support Ended 08/15/2017

VMware Web Services – 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.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Support Ended 05/15/2017

IBM SiteProtector – Support ended for versions 2.0 through 3.0 due to end of support by vendor.

IBM WebSphere – Support ended for versions 4.0, 5.0, 6.0, and 6.1 due to end of support by vendor.

IP Flow (NetFlow/J-Flow) – End of support for NetFlow and J-Flow version 5. For most current IP flow support, use the SmartConnector for IP Flow Information Export (IPFIX).

ISC BIND Syslog — Support ended for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog – Support ended for versions 9.6 through 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog – Support ended for 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee Network Security Manager Syslog – Support ended for IntruShield versions 1.2, 1.8, and 2.1 and NSM 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB – Support ended for versions 6.8 and 7.0 due to end of support by vendor.

MessageGate Syslog – Support ended because company no longer exists.

SNMP Unified – Support ended for IBM Lotus Domino SNMP 7.0 and 8.0 due to end of support by vendor.

New and Updated SmartConnector Documentation

All SmartConnector configuration guides have been updated to reflect a change made to the installation procedure for IPv6 address support.

General Connector Documentation

ArcSight FlexConnector Developer's Guide

Added encryption parameters to Global Parameters. Updated information for downloading SQL Server JDBC drivers. Several mapping changes. See the Revision History table in the guide for details.

ArcSight FlexConnector REST Developer's Guide

Corrected JSON parser example. Added encryption parameters to Global Parameters.

SmartConnector Platform Support

Updated certified platforms for connector 7.7.0 release.

SmartConnector User Guide

- Added Format Preserving Encryption parameter information.
- Added description of Data Encryption.
- See the Revision History table in the guide for details.

SmartConnector Configuration Guides

Micro Focus Security ArcSight SmartConnector for Microsoft Windows Event Log

Check Point Syslog
Added support for R80.10.

McAfee ePolicy Orchestrator DB
Added Source Process Name and Old File Path mappings to Endpoint Security mappings table.

SNMP Unified
Added support for v8.2 RSA Authentication Management Services/RSA Identity Management.

VMware ESXi Syslog
Added support for version 6.5. Support ended for 5.0 due to end of support by vendor.

Amazon Web Services CloudTrail
Added mapping for 'Device Receipt Time' event in place of 'Start Time' event.

McAfee ePolicy Orchestrator DB
Added support for VSE 8.8 and ENS 10.5 with ePO 5.9.

McAfee ePolicy Orchestrator DB
Added support of HIPS 8.0 with ePO 5.9.

McAfee Network Security Manager DB (ID-Based) Added
NSM 9.1 mappings.

McAfee Network Security Manager DB (Time-Based) Added
NSM 9.1 mappings.

UNIX OS Syslog
Added RHEL 7.4 support.

McAfee Network Security Manager Syslog Added
support NSM 9.1.

Rapid 7 NeXpose XML File
Added Rapid 7 NeXpose 6.4.42 support.

Symantec Endpoint Protection DB Version
11 no longer supported.

McAfee ePolicy Orchestrator DB

Microsoft SQL Server Multiple Instance Audit DB

Microsoft Active Directory Windows Event Log Native

Microsoft Exchange Audit Windows Event Log Native

Microsoft Forefront Protection 2010 for Exchange Windows Event Log Native

Microsoft Network Policy Server Windows Event Log Native

Microsoft Remote Access Windows Event Log Native

Microsoft Service Control Manager Windows Event Log Native

Microsoft SQL Server Audit Windows Event Log Native
Microsoft Windows Event Log Native Security Event Mappings Microsoft

WINS Server Windows Event Log Native

Oracle Audit Windows Event Log Native

Symantec Mail Security Windows Event Log Native