Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.3.0.7886.0

August 31, 2016

HPE Security ArcSight
SmartConnector Release Notes

7.3.0.7886.0

August 31, 2016

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

https://www.protect724.hpe.com/docs/DOC-13026

Contents

SmartConnector Release 7.3.0.7886.0

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 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. All SmartConnectors other than those listed in the "SmartConnectors with 64-Bit Support" document are currently supported on 64-bit platforms. This document is available on Protect 724 (https://www.protect724.hpe.com/docs/DOC-9367) 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.

Verifying Your Upgrade Files

HPE provides a digital public key for you to verify that the signed software you received is indeed from HPE 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

New Connector Support

SmartConnector for	New Device, Component, or OS Version
IP Flow Information Export (IPFIX)	10

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
Cisco IOS Syslog	15.5
McAfee ePolicy Orchestrator DB	Microsoft Exchange (MSME) 8.5 with ePO 5.3.
Microsoft Windows Event Log—Native	.NET 4.6.1
Microsoft Windows Event Log—Native: Oracle Audit	Oracle database version 12cR1 with Microsoft Windows Server 2012
Pulse Secure Pulse Connect Secure Syslog	8.2
Tripwire IP360 File	7.5

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.

HPE advises you to verify the content you created before deploying the SmartConnector into your production environment.

All SmartConnectors

Provided API access to connectors and devices to facilitate remote monitoring in ArcMC version 2.5. [CON-15226]

All SmartConnectors, new Event Broker (CEF Kafka) Destination

Connectors can now send events to Apache Kafka as a destination to further distribute events to real-time analysis and data warehousing systems. [CON-17120, CON-16749, CON-16705, CON-17598]

Note: This new destination is supported in ArcMC version 2.5. Existing connectors with Kafka destinations can still be remotely managed.

Fixed Issues

SmartConnector for	Number	Description
All Syslog Connectors	CON-16715 CON-17730	For Syslog Daemon and Syslog NG Daemon connectors configured for TCP, beginning with release 7.2.4 the connector stopped processing events when a malformed UTF-8 character was received. The connector had to be restarted to resolve the issue. This issue has been fixed as of release 7.3.0 (this release).
Cisco IronPort Web Security Appliance File	CON-16950	Parsing did not occur in cases where the file header contained a token not defined in the code. This issue has been fixed.
Cisco NX-OS Syslog	CON-17173	Some events were not parsed correctly. This issue has been fixed.
Cisco PIX/ASA Syslog	CON-16178	Some events were not being parsed. This issue has been fixed.
F5 BIG-IP Syslog	CON-17154	Some events were not being parsed. This issue has been fixed.
Juniper JUNOS Syslog	CON-16853	Fixed a sub-message parsing issue.
Microsoft Windows Event Log—Native	CON-14684 CON-17366	This fix gracefully handles any errors encountered while getting the events from the Windows Event Log API. The error handling now makes sure fewer events are duplicated while retrying the event collection as part of the error recovery.

Known Limitations

All SmartConnectors with Event Broker (Kafka CEF) destinations

SmartConnectors require that Kafka brokers be running Kafka version 0.10.0.0; previous connector versions worked with Kafka 0.9.0.x, but that is no longer the case. [CON-17435]

Amazon Web Services

With SmartConnector releases 7.2.1 through 7.3.0, the Amazon Web Services CloudTrail connector is unable to receive events due to interoperability problems with the Java 8 Runtime Environment. This problem is being addressed and will be resolved in an upcoming connector release. [CON-17749]

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 11/30/2016

CA eTrust SiteMinder File (Legacy) -- Use the SmartConnector for CA SiteMinder Single Sign-On File

CA eTrust SiteMinder Profiler Trace File (Legacy) -- Use the SmartConnector for CA SiteMinder Single Sign-On File

Juniper M Series Syslog (Legacy) -- Use the SmartConnector for Juniper JUNOS Syslog

Sourcefire Syslog (Legacy) -- Use the SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog

Support Ending 02/28/2017

IBM AIX Version 7.1 64-bit as supported installation platform.

IBM AIX Audit File -- Use the SmartConnector for IBM AIX Audit Syslog

IBM AIX Realtime Audit File -- Use the SmartConnector for IBM AIX Audit Syslog

SmartConnectors Support Recently Ended

Support Ended 08/30/2016

Barracuda Spam Firewall Syslog -- Use the SmartConnector for Barracuda Spam Firewall NG Syslog

IBM DB2 Multiple Instance UDB Audit File – Support ended for versions 8.2 and 8.5 due to end of support by vendor.

Juniper IDP Series Syslog -- Support ended for versions 2.1 through 3.4 and version 4.1 due to end of support by vendor.

Juniper Pulse Secure Access Syslog (Legacy) - Use the SmartConnector for PulseSecure Pulse Connect Secure Syslog

McAfee Firewall Enterprise Syslog -- Support ended for versions 5.2 through 8.2 due to end of support by vendor.

Note: For vendor CEF support information, see the HPE Security Technology Alliances on Protect724 at: https://www.protect724.hpe.com/community/technology-alliances.

Lancope StealthWatch Management Console Web Services (Legacy) -- Use the vendor's Common Event Format version

Lumeta IPsonar File (Legacy) -- Use the vendor's Common Event Format version

NIKSUN NetDetector Syslog (Legacy) -- Use the vendor's Common Event Format version

Stonesoft StoneGate Firewall Syslog (Legacy) – Use the vendor's Common Event Format version

Tripwire Enterprise Syslog (Legacy) -- Use the vendor's Common Event Format version

Vormetric Data Security Manager Syslog (Legacy) -- Use the vendor's Common Event Format version

Support Ended 6/30/2016

Aruba Mobility Controller Syslog -- Support ended for versions 3.0, 3.3, 5.0, and 6.1 due to end of support by vendor.

F5 BIG-IP Syslog -- Support ended for TMOS versions 4, 9, and 10 due to end of support by vendor.

HPE-UX Audit File -- Support ended for HPE-UX version 11.0 due to end of support by vendor.

Support Ended 05/16/2016

Symantec Messaging Gateway Syslog versions 5.0, 7.6, 8.0 due to end of support by vendor.

Support Ended 03/31/2016

Arbor Networks Peakflow Syslog -- Support ended for version 3.4 due to end of support by vendor

IBM DB2 UDB Audit File (Legacy) – Use the SmartConnector for IBM DB2 Multiple Instance UDB Audit File

Microsoft IIS File, Microsoft IIS Multiple Server File, and Microsoft IIS Multiple Site File – End of support for versions 4.0, 5.0, and 6.0 due to end of support by vendor

Microsoft IIS Syslog – End of support for version 6.0 due to end of support by vendor

New and Updated SmartConnector Documentation

The following SmartConnector documentation has been added or updated for this release.

ArcSight CEF Cisco FireSIGHT Syslog
Updated and enhanced overview and configuration information.

ArcSight FlexConnector Developer's Guide
Reorganized and expanded content for increased usability. Updated the "Configure the JDBC Driver and Windows Authentication" section. Updated information regarding preserver state parameters.

Check Point OPSEC NG
Added clarification to opsec_sscla_file parameter description.

Cisco IOS Syslog
Added support for Cisco IOS version 15.5.

Dell SonicWALL Firewall Syslog
Updated Device Vendor and Device Product.

HPE Aruba Mobility Controller Syslog
Updated Device Vendor to HPE and Device Product to Aruba Mobility Controller.

HPE c7000 Virtual Connect Module Syslog
HP changed to HPE, including Device Vendor mapping.

HPE H3C Syslog
Updated vendor name from HP to HPE.

HPE Operations Manager i Web Services
HP changed to HPE, including Device Vendor mapping.

HPE OpenVMS File
HP changed to HPE, including Device Vendor mapping.

HPE Operations Manager Incident Web Service
HP changed to HPE, including Device Vendor mapping.

HPE ProCurve Syslog
HP changed to HPE, including Device Vendor mapping.

HPE-UX Audit File
HP changed to HPE, including Device Vendor mapping.

HPE-UX Syslog
HP changed to HPE, including Device Vendor mapping.

IBM AIX Audit File (Legacy)
Marked this connector as Legacy. Use the SmartConnector for AIX Audit Syslog for continuing version support.

IBM AIX Realtime Audit File (Legacy)
Marked this connector as Legacy. Use the SmartConnector for AIX Audit Syslog for continuing version support.

IBM DB2 Multiple Instance UDB Audit File
Removed support for versions 8.x and 9.x in installer. End of life for DB2 UDB versions 8.2 and 8.5 due to end of support by vendor.

IP Flow Information Export (IPFIX)
First release of this connector.

Juniper Firewall ScreenOS Syslog
Changed Device Vendor name from NetScreen to Juniper.

Juniper IDP Series Syslog
Removed support for Juniper IDP versions 2.1 through 3.4 and version 4.1.

McAfee ePolicy Orchestrator DB
Added support for McAfee Security for Microsoft Exchange (MSME) 8.5 with ePO 5.3.

McAfee Firewall Enterprise Syslog
Updated mappings. Removed support for versions 5.2 through 8.2 due to end of support by vendor.

Microsoft Windows Event Log—Native
Added support for .NET 4.6.1.

Microsoft Windows Event Log – Native: Microsoft Exchange Access Auditing
Updated versions supported.

Microsoft Windows Event Log – Native: Microsoft Forefront Protection 2010
Updated versions supported.

Microsoft Windows Event Log—Native: Oracle Audit
Added support for Oracle database version 12cR1 with Microsoft Windows Server 2012.

Microsoft Windows Event Log—Native: Symantec Mail Security for Exchange Supplemental
Updated versions supported.

Pulse Secure Pulse Connect Secure Syslog
Added support for version 8.2.

RSA Identity Management Service SNMP
3DES option for Privacy parameter has been removed as SNMPv3 does not support this option.

SmartConnector Product and Platform Support Guide
Specified certified platforms for 7.3.0 release. Added support for CentOS and RHEL 6.8 64-bit platforms. Announced upcoming end of support for IBM AIX platform in 02/2017.

SmartConnector User Guide
Added information for Event Broker (CEF Kafka) receiver and Kafka key.

SNMP Unified
3DES option for Privacy parameter has been removed. Device Vendor has changed to HPE for HPE Network Node Manager i and HPE ProCurve Ethernet Switch products.

Trend Micro Control Manager Multiple DB
Updated Windows Authentication configuration information.

Tripwire IP360 File

Added support for version 7.5.

UNIX Login/Logout

Added reference to SmartConnector for IBM AIX Audit Syslog connector for AIX login/logout message support.