Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.2.1.7714

February 16, 2016

HPE Security ArcSight
SmartConnector Release Notes

7.2.1.7714

February 16, 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 Package 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 Package 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 Package Enterprise Development LP copyrights, trademarks and acknowledgements:

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

Contents

SmartConnector Release 7.2.1.7714

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.

Important Upgrade Note: Support Ends for ODBC and Other Databases

Java 8 was implemented with this SmartConnector release. Java 8 does not support ODBC connections; therefore, database connectors using MS SQL databases can only use JDBC connections. For the same reason, the MS Access database and the embedded database for the Symantec Endpoint Protection connector are no longer supported with this connector release. If your connector uses an unsupported database, a warning message displays during local upgrades. Remote upgrades will fail, and automatically roll back to the previous version, possibly losing up to five minutes of events. HPE does not recommend upgrading until you are using a database connection supported by Java 8.

To Apply This Release

Download the appropriate executable for your platform from the Support Web site (https://www.hpe.com/software/support), 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. The 64-bit installation executables contain a subset of available SmartConnectors. See your platform's 64-bit SmartConnector installer for the list of available connectors, or see the document "SmartConnectors Available with 64-Bit Support" listed on the SmartConnector Documentation page on Protect 724 (https://www.protect724.hpe.com/community/arcsight/productdocs/connectors) or 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
Check Point Syslog	R77.30 supports 64-bit platform and the following modules: Anti-bot, Anti-spam and Email Security, Anti-virus, Application Control, Data Loss Prevention, Firewall, Identity Awareness, IPS, and URL Filtering
PulseSecure Pulse Connect Secure Syslog	8.1

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
All SmartConnectors	Java 8 (See Important Upgrade Note)
	Red Hat Linux Enterprise 6.7 and CentOS 6.7 64-bit platforms
Barracuda Networks Spam Firewall NG Syslog	7.0
Cisco IronPort Email Security Appliance File	9.6
Cisco IronPort Web Security Appliance Syslog	9.6
Cisco PIX/ASA Syslog	ASA 9.5
Fortinet FortiGate Syslog	FortiOS 5.2
HP OpenVMS File	8.3, 8.4
Juniper JUNOS Syslog	Web URL Filtering – 12.1 SRX anti-virus events - 15.1
McAfee ePolicy Orchestrator DB	RSD 5.0, VSE 8.8, and HIPS 8.0 with ePO 5.3
Microsoft System Center Configuration Manager DB	2012 R2
Microsoft Windows Event Log – Native	Windows 10 event collection support for Security, Remote Access, and Service Control Manager events
Tenable Nessus .nessus File	6.5
UNIX OS Syslog	RHEL 7.1 64-bit platform

Beta Support for SmartConnectors

For the enhancements or fixes for SmartConnectors listed in this section, formal release after testing and documenting will be available in a future SmartConnector release. It is up to your discretion whether to update your installed connectors with this release. Contact HP Customer Support for more information if you are interested in any of these items.

ArcSight Common Event Format REST (Beta)

This connector collects CEF events from CEF certified cloud vendors. It also extracts assets and vulnerability information from the CEF events.

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 on RHEL 6.5

The connector commons-collection jar file has been upgraded to remove a possible vulnerability issue. [CON-16563]

Box

New BOX API changes related to stream_position and Event ID datatype have been tested and validated. [CON-16113]

Checkpoint OPSEC NG
Updated configuration guide with troubleshooting information for “IP address incorrect” error when pulling certificate. [CON-16624]

FlexConnectors for File, Regex File, Regex Folder File, Multiple Folder File, and Scanner Text Reports
Added connector framework capability to detect and log unparsed events into a separate log file. [CON-15508]

Microsoft Windows Event Log – Native
Added the ability to remotely manage connectors from ArcSight Management Center (ArcMC) v2.2. [CON-16353, CON-15749]

Fixed Issues

SmartConnector for	Number	Description
All FlexConnectors	CON-15719	The parser operation for parseMutableTimeStamp occasionally caused the timezone to be interpreted incorrectly. The issue has been fixed.
All EOL’ed SmartConnectors	CON-16281	Prior to this release, connectors would fail to start after an upgrade if EOL’ed connectors were installed. With this release, upgrades are stopped on systems with EOL’ed connectors.
All SmartConnectors	CON-16383	If the connector password credentials were changed by using ArcSight Management Center or Connector Appliance, the local connector setup program could not log in successfully. This issue has been fixed.
All SmartConnectors using Logger Pool and Failover Destinations	CON-16408	When both a logger pool and a failover destination were configured, a problem occurred if all logger pool destinations were down when the connector was initially started. In this case, even when one or more logger pool destination members recovered, events were still not sent to them. The issue has been fixed.
All SmartConnctors with Multiple CEF File Destinations	CON-16515	Previously, different CEF File destinations could not have independent properties. This issue has been fixed.
All Syslog Connectors	CON-16318	Message patterns have been added to the parser to address parsing problems with pam_tally events.
Cisco PIX/ASA Syslog	CON-16117	Some Cisco ASA events were not being parsed. This issue has been fixed.
HP-UX Audit File	CON-16319	Parsing issues with authentication events have been resolved.
HP-UX Audit File, FlexConnectors (specifically: Flex Regex Folder Follower, DB2 Folder Follower)	CON-15708	The "wildcard" property default value has been changed to "*" to accommodate any file name on any UNIX-type or Windows OS. This property change affects only new installations (not upgrades). For existing connectors, the default value will not be altered in the agent.properties file during an upgrade, so installed connectors will not have any change in behavior.
FF-BIG-IP Syslog	CON-15999	Some events were not being parsed. This issue has been fixed.
Juniper JUNOS Syslog	CON-16003	Minor improvements made in sub-message parsing to correct parsing errors.

SmartConnector for	Number	Description
Juniper Pulse Secure Access Syslog	CON-16644	A problem in SmartConnector Release 7.1.4 caused syslog event flow to come to a halt for specific events. This issue has been fixed.
	CON-16672	Some events containing double quotation marks caused the connector to stop processing events. This issue has been fixed.
Microsoft System Center Configuration Manager DB	CON-15169	Connector was not getting events for any locale other than English-United States. This issue has been fixed.
Microsoft Windows Event Log -- Native	CON-16045	Connector was not mapping some fields for event ID 4648. This issue has been fixed.
Symantec Endpoint Protection DB	CON-15965	The destination host name was not set because the local host name was not being extracted. This issue has been fixed.
	CON-16201	GROUP_NAME for agent-security events was not being mapped correctly. This issue has been fixed.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 03/31/2016

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

Support Ending 09/30/2016

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

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

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

McAfee Email Gateway Syslog (Legacy) -- use the vendor's Common Event Format version

McAfee StoneSoft StoneGate Firewall Syslog (Legacy) -- use the vendor's Common Event Format version

McAfee Web Gateway File (Legacy) -- use the vendor's Common Event Format version

NIKSUN NetDetector 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

SmartConnectors Support Recently Ended

Support Ended 02/15/2016

CA eTrust Antivirus Windows Event Log (Legacy) – Vendor no longer supports this product.

Fortinet FortiGate Syslog -- Support ended for versions 3.0 and 4.0 due to end of support by vendor.

McAfee ePO Asset Scanner DB -- Vendor no longer supports this product. Use the SmartConnector for Microsoft ePolicy Orchestrator DB.

McAfee ePolicy Orchestrator DB -- Support ended for versions 4.5, 4.6, and 5.0 due to end of support by vendor.

Microsoft Active Directory Windows Event Log (Legacy) – Vendor no longer supports this product.

Microsoft Windows 2003 Security Event Mappings – Vendor no longer supports this product.

Microsoft Windows Event Log – Domain (Legacy) – Use the SmartConnector for Microsoft Windows Event Log – Unified or Microsoft Windows Event Log – Native.

Microsoft Windows Event Log – Local (Legacy) – Use the SmartConnector for Microsoft Windows Event Log – Unified or Microsoft Windows Event Log – Native.

Microsoft WINS Server Windows Event Log (Legacy) – Vendor no longer supports this product.

Oracle Audit Windows Event Log (Legacy) – Vendor no longer supports this product.

RSA Authentication Manager Windows Event Log (Legacy) – Vendor no longer supports this product.

SmartConnector for Microsoft Windows Event Log – Domain and SmartConnector for Microsoft Windows Event Log – Local — HPE suggests using the SmartConnector for Microsoft Windows Event Log – Unified or the SmartConnector for Microsoft Windows Event Log – Native for future Windows event log collection.

Snort Barnyard (Snort IDS) File (Legacy) – Use the SmartConnector for Snort Multiple File or the SmartConnector for Snort Syslog.

Symantec Mail Security Windows Event Log (Legacy) – Vendor no longer supports this product.

Trend Micro Control Manager Multiple DB – Support ended for Control Manager versions 3.5 and 5.5 due to end of support by the vendor.

Support Ended 12/31/2015

Support for the following connectors is now supported by the SmartConnector for SNMP Unified:

ArcSight FlexConnector SNMP (Legacy)

Cisco WIPS SNMP (Legacy)

Cisco Wireless Control System SNMP (Legacy)

Cisco Wireless LAN Controller SNMP (Legacy)

Extreme Networks Dragon SNMP (Legacy)

HP Network Node Manager I SNMP (Legacy)

HP ProCurve Ethernet Switch SNMP (Legacy)

IBM Lotus Domino SNMP (Legacy)

McAfee Email Gateway SNMP (Legacy)

nCircle Scanner SNMP (Legacy)

RSA Authentication Manager SNMP (Legacy)

Websense Web Security SNMP (Legacy)

Support also ending for the following connectors:

ActivCard AAA Server Accounting Log (Legacy) – Vendor no longer supports this product version.

ActivCard AAA Server Authentication Log (Legacy) – Vendor no longer supports this product version.

McAfee Secure Internet Gateway Syslog (Legacy) – Use the SmartConnector for McAfee Web Gateway File.

Microsoft Audit Collection System (ACS) (Legacy) – Use the SmartConnector for Microsoft ACS DB.

Microsoft Forefront for Exchange Server DB – Vendor no longer supports this product.

nCircle Scanner XML2 File (Legacy) – Use the SmartConnector for Tripwire IP360 File.

Symantec Enterprise Security Manager DB – Vendor no longer supports this product.

Symantec Enterprise Security Manager Reporting DB – Vendor no longer supports this product.

Trend Micro Control Manager DB (Legacy) – Use the SmartConnector for Trend Micro Control Manager Multiple DB.

Support Ended 11/17/2015

Cisco IronPort Email Security Appliance File – Support ended for SyncOS versions 4.7, 5.5, 6.1, 6.4, 7.0, and 7.5 due to end of life of these versions by vendor.

Cisco Ironport Web Security Appliance File – Support ended for versions AsyncOS 5.1, 5.5, 6.1, 6.3, and 7.1 Cisco Secure ACS Syslog – Support ending for versions 4.2 and 5.0 due to end of life of these versions by vendor.

CiscoWorks Syslog (Legacy) – Vendor no longer supports this product.

IBM Lotus Domino DB – Support ended for Lotus Domino version 6.5.

Linux Audit File – Support ended for RHEL version 5.7, 6.1, and 6.2.

Linux Audit Syslog – Support ended for RHEL version 5.7, 6.1, and 6.2.

Mazu Profiler DB (Legacy) – Vendor no longer supports this product.

McAfee Network Security Manager DB (Time-based) – Support ended for versions 5.1, 6.0, and 6.1 due to end of life of these versions by vendor

Mirage Counterpoint Appliance Syslog (Legacy) – Vendor no longer supports this product.

Secure Computing Gauntlet Syslog (Legacy) – Device no longer supported by vendor.

Secure Computing SafeWord File (Legacy) – Use the SmartConnector for McAfee Firewall Enterprise Syslog.

Snort DB (Legacy) – Use the SmartConnector for Snort Multiple File or the SmartConnector for Snort Syslog.

Tripwire IP360 File – Support ended for versions 6.4, 6.5, 6.6, 6.8, and 7.0.

UNIX Login/Logout – Support ended for AIX 5.3; RHEL 5.4 AS 32-bit and 64-bit; and Solaris 10 32-bit.

New and Updated SmartConnector Documentation

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

ArcSight CEF Encrypted Syslog (UDP)
Added algorithm used for encryption.

ArcSight Common Event Format Hadoop
Clarified statement about what events are collected.

ArcSight Common Event Format REST (Beta)
Added troubleshooting information regarding out of memory error.

ArcSight FlexConnector Developer's Guide
End of life for FlexConnector SNMP; use the SmartConnector for SNMP Unified. Added a new feature to detect and log unparsed events.

Barracuda Networks Spam Firewall NG Syslog
Added support for v7.0.

Barracuda Networks Spam Firewall Syslog (Legacy)
Marked this connector as legacy. Use the SmartConnector for Barracuda Networks Spam Firewall NG Syslog.

Bro IDS NG File
Updated parameters screenshot and table to describe Bro IDS Host Name parameter. Removed host name configuration from the Configuration section.

Check Point OPSEC NG
Added troubleshooting information for IP address incorrect error when pulling certificate. Changed incorrect specification of /export/home/$ARCSIGHT_HOME variable to /opt/arcsight/chkpoint in shared library examples.

Check Point Syslog
First release of SmartConnector documentation.

Cisco IronPort Email Security Appliance File
Added support for version 9.6.

Cisco IronPort Email Security Appliance Syslog
Added support for version 9.6.

Cisco PIX/ASA Syslog
Added support for ASA 9.5 events.

Fortinet FortiGate Syslog
Added support for FortiGate OS version 5.2. Removed support for versions 3.0 and 4.0 due to end of support by the vendor.

HP OpenVMS File
Added support for OpenVMS versions 8.3 and 8.4.

Juniper JUNOS Syslog
Added support for additional version 12.1 Web URL Filtering events (deviceAction, requestURLFilename, requestURLQuery, and deviceCustomString4-6). Added support for SRX anti-virus events, version 15.1.

Juniper Pulse Secure Access Syslog (Legacy)
Marked this connector as legacy. For future version support, use the SmartConnector for PulseSecure Pulse Connect Secure Syslog.

McAfee ePolicy Orchestrator DB
Added support for RSD 5.0, VSE 8.8, and HIPS 8.0 with ePO 5.3. Removed ODBC support due to Java 8 implementation. End of support for ePO versions 4.5, 4.6, and 5.0 and for SQL Server 2000 and 2005 due to end of support by vendor.

Microsoft Remote Access Windows Event Log Native
Added Windows 10 support.

Microsoft Service Control Manager Windows Event Log Native
Added support for Windows 10 system events.

Microsoft SQL Server Audit Windows Event Log Native
Added mappings for security events 17811, 49916, and 49917.

Microsoft System Center Configuration Manager DB
Added support for SCCM 2012 R2.

Microsoft Windows Event Log Native Security Event Mappings
Added Windows 10 support. Added fields to security event 4648 mappings.

Microsoft Windows Event Log – Native
Added support for Microsoft Windows 10, information about the remote management option, and new Advanced Container Configuration and Advanced Common Configuration Parameters. Removed requirement for Power User for setting up local user with a standard local user account from Windows Vista workgroup hosts.

Microsoft Windows Event Log – Unified
Removed requirement for Power User for setting up local user with a standard local user account from Windows Vista workgroup hosts.

Pulse Secure Pulse Connect Secure Syslog
First edition of this guide for new connector.

SmartConnector Product and Platform Support
Support ended for RHEL 6.4 64-bit, CentOS Linux 6.5 32-bit, and Oracle Solaris 11 32-bit platforms. Support added for RHEL and CentOS Linux 6.7 64-bit platforms.

SmartConnector with 64-Bit Support
Added supported connectors for Oracle Solaris 11.

SNMP Unified
Removed incorrect Device Vendor and Device Product mappings from HP NNMi mappings table.

Symantec Endpoint Protection DB
Updated Security and Traffic mappings. Removed support for ODBC drivers and embedded database due to Java 8 implementation.

Tenable Nessus .nessus File
Added support for version 6.5 and updated mappings.

Tenable SecurityCenter XML File
Updated mappings.

UNIX OS Syslog
Added support for RHEL 7.1 64-bit platform. Removed support for the following platforms: AIX 6.1, RHEL 6.0 and 6.1, Oracle Solaris 7, 8, and 9 SPARC, and Oracle Solaris 11 32-bit.

Removed ODBC support due to Java 8 implementation for the following SmartConnectors:

Application Security AppDetective DB

Dell ChangeAuditor DB

Dell InTrust for Windows DB

eEye REM Security Management Console DB

eEye Retina Network Security Scanner DB (DSN-Based) (MS Access no longer supported.)

eEye Retina Network Security Scanner DB (RTD File) (MS Access no longer supported.)

IBM SiteProtector DB

Kaspersky DB

Lumension PatchLink Scanner DB

McAfee Vulnerability Manager DB

Microsoft Audit Collection System DB

Microsoft Forefront DB

Microsoft System Center Operations Manager DB

Microsoft SharePoint Server DB

Microsoft SQL Server Multiple Instance Audit DB

Microsoft Forefront Protection Server Management Console DB

NetIQ Security Manager DB

Sophos Anti-Virus DB

Symantec Critical System Protection DB

Symantec Endpoint Protection DB

Trend Micro Control Manager Multiple DB

Updated the link to the Customer Alliance site and marked the following connectors as legacy. For future version support, use the vendor's Common Event Format version.

Lancope StealthWatch Management Console Web Services

Lumeta IPsonar File

McAfee Email Gateway Syslog

McAfee Web Gateway File

NIKSUN NetDetector Syslog

StoneSoft StoneGate Firewall Syslog

Tripwire Enterprise Syslog

Vormetric Data Security Manager Syslog