Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.2.2.7742.0

March 31, 2016

HPE Security ArcSight
SmartConnector Release Notes

7.2.2.7742.0

March 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 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 7.2.2.7742.0

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.

Important Upgrade Note: Support Ends for ODBC and Other Databases

Beginning with SmartConnector release 7.2.1, SmartConnectors are using Java 8. 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 connector release 7.2.1 or later. 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
CA SiteMinder Single Sign-on File	12, 12.5

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
Arbor Networks Peakflow Syslog	Peakflow SP 7.5
Intersect Alliance SNARE Syslog	SNARE for Windows version 4.3
UNIX Login/Logout	Oracle Solaris 11 SPARC Oracle Solaris 11 64-bit

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

When you resize the wizard configuration window on the SmartConnector platform, the text boxes automatically resize for greater ease in entering and viewing parameter information. [CON-16834]

Blue Coat Proxy SG Syslog

More sub-message patterns were added for authentication events. [CON-16317]

Test Alert Connector

Test Alert connector is now supported on 64-bit platforms. [CON-16347]

Fixed Issues

SmartConnector for	Number	Description
All SmartConnectors	CON-16786	An issue that could cause Logger Secure Pool to get a null pointer exception has been fixed.
All SmartConnectors with CEF Syslog destination type	CON-16783	The CEF Syslog destination type sends events in CEF format using syslog protocols, but does not include the normal syslog header. That is still true by default, but because under some circumstances a header is desirable or even necessary, there is now a way to enable the inclusion of an RFC 3164 header. Specifically, the transport.cefsyslog.header=true property can be added to agent.properties.
All File FlexConnectors	CON-15719	The parser operation ‘parseMutableTimeStamp’ occasionally caused the time zone to be interpreted incorrectly. The issue has been fixed.
Citrix NetScaler Syslog	CON-16638	Connector was not parsing a few messages from Citrix NetScaler 10.5. This issue has been fixed.
F5 BIG-IP Syslog	CON-16872	Missing information regarding support for F5 TMOS version 11.6 has been restored in the configuration guide.
Microsoft IIS Multiple Server File	CON-16626	A parsing issue related to source and destination address fields has been fixed.
Microsoft Windows Event Log – Native	CON-16541	Connector was not mapping event 4689 correctly. This issue has been fixed.

SmartConnector for	Number	Description
Symantec Endpoint Protection DB	CON-16760	Current_login_user was not mapped in alerts. This issue has been fixed.
Tenable Nessus .nessus File	CON-15743	Corrected upgrade issue to work for both an older connector release (up to 6.0.4.6719) and newer releases. Default is Nessus file format v2. Nessus file format v1 is not supported.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 09/30/2016

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

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

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

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 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

Support Ended 02/15/2016 or earlier

SmartConnector Support or Version Support Ended	Date Ended
Fortinet FortiGate Syslog versions 3.0 and 4.0	02/15/2016
McAfee ePO Asset Scanner DB	02/15/2016
McAfee ePolicy Orchestrator DB versions 4.5, 4.6, 5.0	02/15/2016
Microsoft Windows Event Log – Domain	02/15/2016
Microsoft Windows Event Log – Local	02/15/2016
Snort Barnyard (Snort IDS) File	02/15/2016
Trend Micro Control Manager Multilpe DB versions 3.5 and 5.5	02/15/2016
ActivCard AAA Server Accounting Log	12/31/2015
ActivCard AAA Server Authentication Log	12/31/2015
McAfee Secure Internet GatewaySyslog	12/31/2015
Microsoft Audit Collection System (ACS)	12/31/2015
Microsoft Forefront for Exchange Server DB	12/31/2015
nCircle Scanner XML2 File	12/31/2015
Symantec Enterprise Security Manager DB	12/31/2015
Symantec Enterprise Security Manager Reporting DB	12/31/2015
Trend Micro Control Manager DB	12/31/2015
SNMP SmartConnectors (replaced by SNMP Unified connector)	12/31/2015

New and Updated SmartConnector Documentation

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

Arbor Networks Peakflow Syslog
Added support for Peakflow SP version 7.5. End of support for Peakflow SP 3.4 due to end of support by vendor.

ArcSight FlexConnector Developer's Guide
Added chapter about advanced parameters, added configuration properties for JSON folder follower FlexConnectors, clarified SQL query usage, and removed agents[x].maxfilesize parameter.

CA SiteMinder Single Sign-on File
First edition of this Configuration Guide. Supports version 12 and12.5.

CA SiteMinder File (Legacy)
Marked this connector as legacy. For current support, use the SmartConnector for CA SiteMinder Single Sign-On File.

CA SiteMinder Profiler Trace File (Legacy)
Marked this connector as legacy. For current support, use the SmartConnector for CA SiteMinder Single Sign-On File.

Check Point OPSEC NG
Added troubleshooting information for required Microsoft Visual Studio redistributable.

HP-UX Audit File
Updated HP-UX Audit 11i v3 Device Custom Number 1 mapping.

Intersect Alliance SNARE Syslog
Added support for SNARE for Windows version 4.3.

Microsoft IIS File

Updated mappings for Source Address, Destination Address, Device Custom IPv6 Address 2, and Device Custom IPv6 Address 3. End of support for IIS versions 4.0, 5.0, and 6.0 due to end of support by Microsoft.

Microsoft IIS Multiple Server File

Updated mappings for Source Address, Destination Address, Device Custom IPv6 Address 2, and Device Custom IPv6 Address 3. End of support for IIS versions 4.0, 5.0, and 6.0 due to end of support by Microsoft.

Microsoft IIS Multiple Site File

Updated mappings for Source Address, Destination Address, Device Custom IPv6 Address 2, and Device Custom IPv6 Address 3. End of support for IIS versions 4.0, 5.0, and 6.0 due to end of support by Microsoft.

Microsoft IIS Syslog

Updated mappings for Source Address, Destination Address, Device Custom IPv6 Address 2, and Device Custom IPv6 Address 3. End of support for IIS version 6.0 due to end of support by Microsoft.

Microsoft Windows Event Log – Native

Editorial updates regarding Windows 10 support..

SmartConnector Product and Platform Support

Support added for Red Hat Enterprise Linux (RHEL) and CentOS Linux 7.2 64-bit platforms.

SmartConnector with 64-Bit Support

Added support for CentOS Linux and Red Hat Linux Enterprise (RHEL) 7.2.

UNIX Login/Logout

Added support for Oracle Solaris 11 SPARC and x86 64-bit platforms.