Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.4.0.7963.0

November 30, 2016

HPE Security ArcSight
SmartConnector Release Notes

7.4.0.7963.0

November 30, 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 7.4.0.7963.0 1
To Verify Your Upgrade Files 1
Integrated into this Release 1
To Apply This Release 1
New Device, Component, or OS Version Support 2
SmartConnector Enhancements 2
Fixed Issues 2
Known Limitations 3
Connector End-of-Life Notices 3
SmartConnector Support Ending Soon 3
Support Ending 02/15/2017 3
SmartConnectors Support Recently Ended 3
Support Ended 11/30/2016 3
Support Ended 08/30/2016 4
Support Ended 6/30/2016 4
New and Updated SmartConnector Documentation 4
General Connector Documentation 4
SmartConnector Configuration Guides 5

SmartConnector Release 7.4.0.7963.0

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

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

Integrated into this Release

Parser update releases 7.3.1.7910 and 7.3.2.7947 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:

- 7.3.1 Release Notes: https://www.protect724.hpe.com/docs/DOC-14563
- 7.3.2 Release Notes: https://www.protect724.hpe.com/docs/DOC-14671

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

Release 7.3.1	**Release 7.3.2**
• Dell ChangeAuditor DB (v6.7) • F5 BIG-IP Syslog • HPE Integrated Lights Out Syslog • Juniper JUNOS Syslog • McAfee ePolicy Orchestrator DB (MOVE 3.6 with ePO 5.3) • McAfee Firewall Enterprise Syslog • McAfee Network Security Manager Syslog • NetApp Filer Syslog • Microsoft IIS Syslog (v10.0) • Tenable Nessus .nessus File (v6.6)	• Blue Coat Proxy SG Syslog • Cisco PIX/ASA Syslog (v9.6) • Dell ChangeAuditor DB • Microsoft Windows Event Log – Native Security Event Mappings • Pulse Secure Pulse Connect Secure Syslog • Tenable Nessus .nessus File (v6.8) • Tenable SecurityCenter XML File • UNIX OS Syslog

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.

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
McAfee ePolicy Orchestrator DB	Applications and Change Control 7.0.1 with ePO 5.3
McAfee Network Security Manager DB (ID-based) McAfee Network Security Manager DB (Time-based)	8.3
Microsoft IIS File Microsoft IIS Multiple Server File Microsoft IIS Multiple Site File	10.0
Microsoft Windows Event Log – Native	Windows Server 2016 remote security event collection support Windows Server 2016 system event support (Network Policy Server, Remote Access, Service Control Manager, and WINS)
Symantec Data Center Security DB (formerly Symantec Critical System Protection DB)	6.5

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 on CentOS

Upgraded the Java Service Wrapper to the latest stable version 3.5.29. Previous versions showed memory leak. [CON-17141]

All SmartConnectors supporting IPv6

Enhanced IPv6 address platform support, including ability to select IP address mode during connector installation process. For a list of platforms supported and connectors supporting IPv6 address mapping, see "SmartConnectors with IPv6 Support" available on Protect 724 (https://www.protect724.hpe.com/docs/DOC-11637) [CON-16909, CON-15177]

Fixed Issues

SmartConnector for	Number	Description
All Connectors on Windows platform using ArcMC for remote upgrade	CON-17874	When performing a parser upgrade for connectors residing on a Windows platform through ArcMC, the upgrade would fail when there was a space in the path to the connector location. This issue has been fixed.
Amazon Web Services CloudTrail	CON-17252 CON-17749	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 (JRE). With this connector release, the connector can now download the log file and collect events when running JRE 8.

SmartConnector for	Number	Description
Amazon Web Services CloudTrail	CON-17327	In some cases, the connector failed to retrieve SNS and SQS events with connector release 7.2.1, displaying the following error message: "Unable to verify integrity of data download. Client calculated content hash didn't match hash calculated by Amazon S3. The data may be corrupt." This issue has been fixed.
Symantec Critical System Protection DB	CON-17704	EVENT_ID events greater than 2147483647 were not being received and parsed when EVENT_ID was mapped to "?". This issue has been fixed.

Known Limitations

All SmartConnectors that run in a local container on an ArcMC appliance

Issue: Emergency Restore from ArcMC appliance using 7.4 connector leaves a blank destination on the GUI.
Workaround: Remove 'NSP' destination from transport.types property in agents.properties file and restart the connector. [CON-18018]

All SmartConnectors on AIX platforms

Because support for AIX as an installation platform will soon be reaching end-of-life, the latest JRE version as well as IPv6 support are not available for connectors running on AIX platforms. [CON-17399]

All SmartConnectors on Solaris platforms

The 32-bit connector executables for Solaris platforms do not support the latest JRE version. For the latest support, which includes JRE 101, use 64-bit connector executables. [CON-15642]

SmartConnector for Microsoft Windows Event Log – Native

Due to changes in Microsoft .NET support, with connector releases 7.3.0 and later, FIPS support must be disabled at the operating system level for the connector to work properly. See the SmartConnector for Microsoft Windows Event Log - Native Configuration Guide for instructions. [CON-18221]

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 02/15/2017

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 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

McAfee Network Security Manager DB (Time-based) – Support ended for versions 7.0 and 7.1 due to end of support by vendor.

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

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

Symantec Critical System Protection DB – End of support for versions 5.0 and 5.2 due to end of support by vendor.

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.

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

FlexConnector Developer's Guide
: Updated installation procedure for setting preferred IP address mode; updated information about IPv6-aware parsers.

SmartConnector 64-bit Support
: Updated list of connectors with 64-bit Beta support.

SmartConnector Product and Platform Support
: Updated certified platforms supported.

SmartConnector User Guide
: Added section for setting global parameters to the installation procedure; added procedure for configuring FIPS Suite B Mode; added connector filtering information.

SmartConnectors with IPv6 Support
: Updated list of connectors supporting IPv6 mapping and added supported platforms.

SmartConnector Configuration Guides

Amazon CloudTrail Web Services
Updated parameter descriptions for AWS regions.

ArcSight CEF Cisco FireSIGHT Syslog
Updated CEF Client configuration information.

Check Point OPSEC NG
Updated troubleshooting information regarding missing DLL file. Noted that IPv6 support is not available for this connector.

Check Point Syslog
Added note and troubleshooting information regarding obfuscated confidential fields.

EMC VNXe Series Storage Systems
Updated installation procedure to include downloading Microsoft Visual C++ Redistributable.

IBM AIX Audit Syslog
Moved script examples to a separate .txt file for ease of copying and pasting the information.

McAfee ePolicy Orchestrator DB
Added support for Application and Change Control 7.0 with ePO 5.3.

McAfee Network Security Manager DB (ID-based)
Added support for version 8.3.

McAfee Network Security Manager DB (Time-based)
Added support for version 8.3. Removed support for versions 7.0 and 7.1.

McAfee Web Gateway File
Updated device custom string mappings in Access mappings tables.

Microsoft IIS File
Microsoft IIS Multiple Server File
Microsoft IIS Multiple Site File
Added support for Microsoft IIS version 10.0 and removed the version parameter from configuration parameters.

Microsoft Windows Event Log – Native
Added support for Windows Server 2016 event collection for security and system events. Added new procedure for disabling FIPS support at the OS level. Updates also made to the Windows Event Log Native supplemental configuration guides for Remote Access, Service Control Manager, WINS Server, and Network Policy Server, and to Microsoft Windows Event Log Native Security Event Mappings.

Symantec Data Center Security DB (formerly Symantec Critical System Protection DB)
Renamed product from Critical System Protection to Data Center Security. Added support for version 6.5. End of support for versions 5.0 and 5.2 due to EOL by vendor.

Tripwire IP360 File
Added new configuration parameters to support SSL certification and hostname validation.