Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.6.0.8009.0

May 15, 2017

HPE Security ArcSight
SmartConnector Release Notes

7.6.0.8009.0

May 15, 2017

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 7.6.0.8009.0

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 7.5.1.7996 and 7.5.2.8001 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:

- 7.5.1 Release Notes: https://www.protect724.hpe.com/docs/DOC-14966
- 7.5.2 Release Notes: https://www.protect724.hpe.com/docs/DOC-15044

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

Release 7.5.1	**Release 7.5.2**
• Cisco ASA Syslog • Cisco IOS Syslog (v15.6) • Cisco IronPort Web Security Appliance File (AsyncOS v10 - Apache and Squid formats) • Cisco ISE Syslog • Cisco Wireless LAN Controller Syslog • F5 BIG-IP Syslog (F5 TMOS v12.0, v12.1) • Juniper JUNOS Syslog • Microsoft DNS Trace Log Multiple Server File • Microsoft Exchange Message Tracking Log Multiple Server File (Microsoft Exchange Server 2016) • Microsoft Windows Event Log – Native • Proofpoint Enterprise Protection and Enterprise Privacy Syslog (v8.4) • Symantec Endpoint Protection DB (v14: Server Admin Log, Behavior, and Virus categories)	• Cisco NX OS Syslog • Cisco Secure ACS Syslog • Juniper JUNOS Syslog • Infoblox NIOS Syslog (v7.2, v7.6) • Microsoft Office 365 • Oracle Audit Syslog • Symantec Endpoint Protection DB (v14: System Events)

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://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 Connector Support

SmartConnector for	New Device, Component, or OS Version
Apache HTTP Server Access Multiple File	Replaces the Apache HTTP Server Access File connector, providing the ability to specify multiple files for event collection. Apache HTTP Server versions 1.3 and 2.4 are supported.
Cisco IronPort Web Security Syslog	Provides ability to monitor Web Security appliance events through syslog. Web Security AsyncOS version 9.0 is supported.
IBM Security Access Manager Syslog	Replaces the IBM Tivoli Access Manager connectors to monitor protected information and resources as well as authentication, authorization, data security, and resource management capabilities. ISAM versions 8.0 and 9.0 for audit and system logs are supported.
McAfee Web Gateway Syslog	Provides ability to monitor Web Gateway events through syslog for protection against web-born threats. Web Gateway version 7.6 for Access Log is supported.
Sun ONE Web Access Multiple Server File	Replaces the Sun ONE Web Access File connector, providing the ability to specify multiple files for event collection. Sun ONE Web Access Server Version 6.0 SP8 is supported.

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
McAfee ePolicy Orchestrator DB	McAfee Endpoint Security (ENS) 10.5 with ePO 5.3
Symantec Endpoint Protection DB	14.0 (Network Threat Protection, Scan, Notification Alert, and Server Policy Events)
Syslog NG Daemon using Customer-supplied Certificates	The usual syslog-ng.cert may be replaced with CA or self-signed certificates. See the updated configuration guide for procedures for using this feature. Customers supplying their own certificate and running in FIPS mode must follow the procedure for using the customer-supplied certificate for both remote management and Syslog NG Daemon.

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 FIPS-enabled SmartConnectors with an ESM destination
In the FIPS enable mode, ESM manager certificate can now be downloaded and imported to the connector's FIPS trust store automatically during the connector agent configuration. [CON-18681]

All SmartConnectors with TCP CEF Syslog destinations
A parameter has been added to disconnect/reconnect, which is useful for distributing events evenly when a load balancer is used in a multi-tiered connector installation. [CON-17418]

All parser upgrades with a user-provided AUP file
Before performing a parser AUP upgrade on the software connector framework, the user-provided parser AUP file is first copied to the `<smartconnectorinstalldir>\user\agent\upgrade directory`, and then the upgrade is performed with that copied AUP file. The user provided original AUP file now remains in place. Previously, it was deleted. [CON-18385]

Amazon Web Services CloudTrail
Added support for 'us-east-2' region. [CON-18815]
Added support for Key Management Service (KMS) events. [CON-17927]
Added support for EC2 role-based access. [CON-17838]

Filtering before event collection
Added the ability to filter out events before they are counted by the connector. See details in the “Customized Events Filtering” section in Chapter 4 of the *SmartConnector User Guide*. [CON-18559]

IP Flow Information Export (IPFIX)/IP Flow (NetFlow/J-Flow)
For the purposes of licensing limits, the reported number of bytes read by the IPFIX (IP Flow Information Export) and IP Flow (NetFlow/J-Flow) connectors was calculated by the connector as higher than original bytes read. A new mechanism was developed for these specific connectors to improve this problem. [CON-18863]

Microsoft Windows Event Log—Native
Added FIPS support. [CON-16586]

SNMP Unified
The IP address of the listening device can now be configured with the added IP Address parameter. [CON-15458]

Fixed Issues

SmartConnector for	Number	Description
ArcSight Common Event Format Syslog	CON-17802	Events were not being picked up to be processed when forwarding syslog events to a second syslog for forwarding to ESM or Logger appliances. This issues has been fixed.
All SmartConnectors with Event Broker destinations	CON-18648	When multiple event broker destinations were configured, events were not being sent to the appropriate topic in correct format. This issue has been fixed.
All SmartConnectors using ArcSight Keytool Wrapper	CON-18636	The command line tool, ArcSight Keytool Wrapper, was not working properly in release 7.5.0 and was made unavailable. It has been fixed and made available again in 7.6.0.
All SmartConnectors using FIPS mode with Client Authentication enabled	CON-18737 CON-18708	The connector key pair for Client Authorization was not automatically migrated from the legacy FIPS store (NSS) to the new FIPS store (BouncyCastle). This issue has been fixed.
All FIPS-enabled SmartConnectors installed on Windows platform	CON-16720	ESM AUP remote upgrades would sometimes fail on FIPS-Suite B mode. This issue has been fixed.

SmartConnector for	Number	Description
All SmartConnectors using FIPS Suite B	CON-12107 CON-18485	The certificate auto-import feature did not work for FIPS Suite B. This issue has been fixed.
All SmartConnectors on Windows 2016	CON-17676	Although Windows 2016 was supported as an installation platform, an “unsupported platform” message displayed when starting the installation wizard. This issue has been fixed.
All FlexConnectors	CON-18643	FlexConnectors would not process log files on Windows 2016 platforms. This issue has been fixed.
All Syslog SmartConnectors	CON-18634	Setting ‘transport.cefsyslog.threads’ to a value higher than one creates multiple transport threads. With this setting, it was possible for two events to be "merged" from the standpoint of the receiver. This issue has been fixed.
All SmartConnectors using Logger Secure Pool	CON-18009	When there was a Logger communication error and the connector disconnected from that Logger pool member, it would stop sending to any Logger pool member even though some are available. When this happened the connector would cache events. This issue has been fixed.
Microsoft Office 365	CON-18868	When running the connector, received a "Failed to parse the available content expiration date" error, which prevented events from being collected. This issue has been fixed.

Known Limitations

All JSON FlexConnectors

The processed file is always renamed despite the correct parameters having been set. This issue will be fixed in an upcoming connector release. [CON-18382]

All SmartConnectors

When remotely upgrading a SmartConnector with FIPS disabled from SmartConnector release v7.5.0.7983 using an ESM in "password and SSL" mode, the upgrade may fail. The ‘upgrade-from’ instance will continue to run. [CON-19084]

Workaround: Perform a local upgrade.

Microsoft Office 365

During connector installation, a parameter error message showing several [Bad Request] labels will display. This error message can be ignored. Click ‘Yes’ to successfully complete the installation. [CON-18936]

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 08/15/2017

QoSient ARGUS (Legacy) – Support ending due to lack of customer demand.

Support Ending 11/15/2017

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 ending 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.

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.

Support ending 4/28/2018

All 32-bit SmartConnectors – Support ending. Use 64-bit SmartConnectors.

SmartConnectors Support Recently Ended

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 02/15/2017

Barracuda Spam Firewall NG Syslog– Support ended for v3.4 due to end of support by vendor.

Check Point OPSEC NG – Support ended for Check Point Security Gateway versions R71, R75 and R76 due to end of support by vendor.

Cisco ASA Syslog (PIX removed from name) – Support ended for versions 6.2, 6.3, 7.0, 7.1, 7.2, 8.0, and 8.1 due to end of support by vendor.

Cisco IronPort Email Security File – Support ended for versions 7.5 and 7.6 due to end of support by vendor.

Cisco IronPort Email Security Syslog – Support ended for v7.6 due to end of support by vendor.

Cisco Secure ACS Syslog – Support ended for versions 5.1 and 5.2 due to end of support by vendor.

Cisco Secure IPS SEEE – Support ended for versions 5.0, 5.1, 6.0, 6.1, 7.0, and 7.1 due to end of support by vendor.

Citrix NetScaler Syslog – Support ended for versions 8.1, 9.2, and 9.3 due to end of support by vendor.

Dell ChangeAuditor DB – Support ended for versions 5.8 and 6.5 due to end of support by vendor.

Dell InTrust for Windows DB – Support ended for v10.5 due to end of support by vendor.

Extreme Networks Dragon Export Tool File – Support ended for versions 6.0 and 6.3 due to end of support by vendor.

Extreme Networks Dragon IDS File – Support ended for v5.0 due to end of support by vendor.

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

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.

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 notices about ODBC connections not being supported after release 7.2.1. See guide for details.

SmartConnector Platform Support
Added support for Red Hat Enterprise Linux (RHEL) and CentOS Linux v6.9 64-bit platforms.

SmartConnector User Guide
- Added a new section for Customized Events Filtering.
- Added the disconnect and reconnect functionality for CEF Syslog destination.
- Added Cloud and Web Services connectors are not certified to be FIPS compliant.
- Added note to refer to FIPS documentation for Event Broker and ESM client authentication steps.
- Updated the Destination Parameters with descriptions.
- Updated the FIPS Compliant SmartConnectors appendix with the latest instructions.

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

SmartConnector Configuration Guides

Amazon Web Services CloudTrail
Added support for event collection from Key Management Service (KMS). The connector can now use EC2 role-based access.

Apache HTTP Server Access File (Legacy)
Marked connector as Legacy. Use the SmartConnector for Apache HTTP Server Access Multiple File.

Apache HTTP Server Access Multiple File
First release of this configuration guide.

ArcSight CEF Folder Follower Scanner

Updated parameter description for CEF Log File Directory to mention the log files containing the CEF events must be UTF-8 encoded.

Blue Coat Proxy SG Multiple Server File

Corrected parameter name from monitorinterval to monitoringinterval in Advanced Parameters section.

Check Point OPSEC NG

Added note regarding upgrade of connector to configuration section.

Cisco Content Services Switch Syslog (Legacy)

Marked connector as Legacy as CSS is no longer supported by Cisco.

Cisco Firewall Services Module Syslog (Legacy)

Marked connector as Legacy as FWSM is no longer supported by Cisco.

Cisco IronPort Web Security Syslog

First release of this configuration guide.

Cisco non-IOS Syslog (Legacy)

Marked connector as Legacy; use the SmartConnector for Cisco IOS Syslog.

Cisco VPN Syslog (Legacy)

Marked connector as Legacy; use the SmartConnector for Cisco ASA Syslog.

Citrix NetScaler Syslog

Updated mappings.

eEye REM Security Management Console DB (Legacy)

Marked connector as Legacy as REM is no longer supported by the vendor.

IBM Lotus Domino DB (Legacy)

Marked connector as Legacy because an ODBC connection is not supported by Java 8.

IBM Security Access Manager Syslog

First release of this configuration guide.

IBM SiteProtector DB

End of support for versions 2.0, 2.9, and 3.0 due to end of support by vendor.

IBM Tivoli Access Manager File (Legacy)

Marked this connector as Legacy. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

IBM Tivoli Access Manager XML File (Legacy)

Marked this connector as Legacy. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

IBM WebSphere File

End of support for IBM WebSphere 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

End of support for BIND versions 9.3 and 9.5 due to end of support by vendor.

Juniper JUNOS Syslog

End of support for JUNOS versions 9.6, 10.1, 10.4, 11.1, 11.2, and 11.4 due to end of support by vendor.

Juniper Network and Security Manager Syslog

Removed support for versions 2010.3, 2010.4, 2011.1, 2011.4, and 2012.1 due to end of support by vendor.

McAfee ePolicy Orchestrator DB

Added support for McAfee Endpoint Security (ENS) 10.5 with ePO 5.3.

McAfee Network Security Manager Syslog

End of support for IntruShield versions 1.2, 1.8, and 2.1, and NSM versions 5.1 and 6.0 due to end of support by vendor.

McAfee Vulnerability Manager DB

End of support for versions 6.8, and 7.0 due to end of support by vendor.

McAfee Web Gateway Syslog

First release of this configuration guide.

Microsoft Windows Event Log—Native

Removed Windows 2003 due to end of support. Added support for Windows 2016 as an installation platform. Added support for FIPS.

Microsoft Windows Event Log—Unified

Removed Windows 2003 due to end of support. Added a troubleshooting issue for reading event logs from Windows 2012 R2 systems.

Oracle Audit DB

Updated troubleshooting information regarding TCPS and SSL v3 support.

Rapid7 NeXpose XML File

Removed Device Custom IPv6 Address 3 mapping.

RSA Identity Management Service SNMP (Legacy)

Marked connector as Legacy; use the SmartConnector for SNMP Unified.

SNMP Unified

Added configuration parameter for IP address. Removed support for IBM Lotus Domino versions 7.0 and 8.0 due to end of support by vendor.

Sun ONE Web Access Server File (Legacy)

Marked connector as Legacy; use the SmartConnector for Sun ONE Web Access Server Multiple File.

Sun ONE Web Access Multiple Server File

First release of this configuration guide.

Symantec Endpoint Protection DB

Added v14.0 support for Network Threat Protection, Scan, Notification Alert, and Server Policy Events.

Tenable Nessus .nessus File

Removed Device Custom IPv6 Address 3 mapping.

Tenable SecurityCenter XML File

Removed Device Custom IPv6 Address 3 mapping.