Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Release Notes

7.7.0.8036.0

October 17, 2017

HPE Security ArcSight
SmartConnector Release Notes

7.7.0.8036.0

October 17, 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://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

Software Support Contact Information
https://softwaresupport.hpe.com/support-contact-information

Contents

SmartConnector Release 7.7.0.8036.0

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 7.6.1.8019 through 7.6.4.8029 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 on Protect 724:

- 7.6.1 Release Notes: https://community.saas.hpe.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-6-1-8019/ta-p/1594670
- 7.6.2 Release Notes: https://community.saas.hpe.com/t5/ArcSight-Connectors/SmartConnector-Release-Notes-7-6-2-8023/ta-p/1600230
- 7.6.3 Release Notes: https://community.saas.hpe.com/t5/ArcSight-Connectors/SmartConnector-Parser-Update-7-6-3-8026-Release-Notes/ta-p/1609460
- 7.6.4 Release Notes: https://community.saas.hpe.com/t5/ArcSight-Connectors/SmartConnector-Parser-Update-7-6-4-8029-Release-Notes/ta-p/1614868

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

Release 7.6.1.8019	**Release 7.6.2.8023**
• Syslog SmartConnectors issues • Barracuda Email Security Gateway Syslog (v8.0) • Blue Coat Proxy SG Syslog • Check Point OPSEC NG • Cisco ASA Syslog • Cisco IOS Syslog • Cisco IronPort Email Security Appliance File (v10.0) • Cisco IronPort Email Security Appliance Syslog (v10.0) • Citrix NetScaler Syslog • F5 BIG-IP Syslog • Fortinet FortiGate Syslog • HPE H3C Syslog • HPE Operations Manager I Web Services • HPE ProCurve Syslog • HPE UX Syslog • McAfee ePolicy Orchestrator DB (DLP 10.0 with ePO 5.3) • Rapid7 NeXpose XML File (v6.3)	• Blue Coat Proxy SG Syslog • Citrix NetScaler Syslog • Juniper JUNOS Syslog • Linux Audit Syslog • McAfee ePolicy Orchestrator DB (Orion Audit Log v5.1 and Policy Auditor v6.2, both on ePO v5.3) • Microsoft Office 365 (OneDrive) • Microsoft SQL Server Audit Windows Event Log Native (Microsoft SQL Server 2016) • Pulse Secure Pulse Connect Secure Syslog • Symantec Endpoint Protection DB (v14.0 Anti-Virus and Anti-Spyware Protection Events)

Release 7.6.3.8026	Release 7.6.4.8029
• Check Point Syslog • Cisco ASA Syslog • Cisco IOS Syslog • Cisco IronPort Email Security Appliance Syslog • Cisco Secure ACS Syslog • Cisco Wireless LAN Controller Syslog • McAfee ePolicy Orchestrator DB (Data Exchange Layer 3.0.1 with ePO 5.3) • Symantec Endpoint Protection DB • VMware Web Services (vCenter 6.5 on ESXi 6.5)	• Syslog SmartConnectors issues • Check Point Syslog (Modules: ESOD, Eventia Analyzer Server, Identity Logging, and VPN-1 Edge for R77.30) • Cisco ASA Syslog • F5 BIG-IP Syslog (Access Policy Module (APM) 11.6) • Juniper JUNOS Syslog (15.1 MX Series Virtual Chassis, MX960 router) • IBM SiteProtector DB • Linux Audit File (RHEL 6.7) • Linux Audit Syslog (RHEL 6.7) • McAfee ePolicy Orchestrator DB • Pulse Secure Pulse Connect Secure Syslog • Symantec Endpoint Protection DB • UNIX OS Syslog (RHEL 6.7 and 7.3)

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://community.saas.hpe.com/t5/ArcSight-Connectors/HPE-ArcSight-SmartConnectors-with-64-bit-Platform-Support/ta-p/1587669) 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 SmartConnector Support

SmartConnector for	New Device, Component, or OS Version
Barracuda Firewall NG F-Series Syslog	Barracuda NextGen Firewall F-Series version 7

New Device, Component, or OS Version Support

SmartConnector for	New Device, Component, or OS Version
Microsoft Exchange PowerShell	Exchange 2016 Access Auditing

Alpha 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 release. It is up to your discretion whether to update your installed connectors with this feature through ArcSight Management Console. Contact ArcSight Customer Support for more information if you are interested in this item.

Connectors in Event Broker (alpha release)

Collectors provide the ability to collect syslog events and send raw events to an Event Broker topic. A connector can be run within the Event Broker environment that reads events from an Event Broker topic to which the collector has sent raw events. It performs normal connector event processing and writes events to an Event Broker topic. Connectors in Event Broker are deployed and managed using ArcSight Management Center (ArcMC). See the ArcSight Data Platform Event Broker Administrator's Guide and ArcSight Management Center Administrator's Guide for more information. [CON-18622]

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.

HPE C7000 Virtual Connect Module Syslog

Updated the parser to support the new timestamp format by removing the mapping for the 'deviceReceiptTime' field. [CON-18348]

Instant Connector Deployment

Added support for the new Instant Connector Deployment feature, which allows a remote, silent installation of connectors on a host from the ArcSight Management Center (ArcMC) Deployment View and does not require a connector to have been previously installed. See the *ArcSight Management Center Administrator's Guide* and the *SmartConnector User Guide* for more information. [CON-17543, CON-18560]

PulseSecure Pulse Connect Secure Syslog

Updated two parsers (PulseSecure Pulse Connect Secure Syslog and Key Value Syslog) to support the new timestamp format by removing the mappings for the 'deviceReceiptTime' fields. [CON-18348]

SecureData Event Encryption

Added support for format-preserving encryption for all SmartConnectors. See the *SmartConnector User Guide* and the *Format-Preserving Encryption Environment Setup Guide* on Protect 724 for more information. [CON-19368]

Symantec Endpoint Protection DB

Mapped event type to oldFilePermission field to differentiate event types. [CON-16202]

For all SEP modules:
1) For modules having information for both GROUP_NAME and GROUP_TYPE:
   - GROUP_NAME is mapped to 'oldFileName' AND 'deviceCustomString6'
   - GROUP_TYPE is mapped to 'oldFileType'
   - For modules that were already mapped for 'deviceCustomString6', the mapping remains as is, and then GROUP_NAME maps to the 'oldFileName' only.
2) For modules having only information for group name:
   - GROUP_NAME is mapped to oldFileType and deviceCustomString6. [CON-17129]

Syslog SmartConnectors

Updated the parser to support the new timestamp format by removing the mappings for the 'event.deviceHostName' and 'deviceReceiptTime' fields. [CON-18348]

Fixed Issues

SmartConnector for	Number	Description
All v7.6 SmartConnectors	CON-19228	In prior releases, some very complicated map files could encounter an ArrayIndexOutOfBoundsException when loading, preventing the SmartConnector from starting at all. This issue has been fixed.
All Syslog Connectors	CON-18423	Kernel/SSHD events sent as generic syslog events with positive offset timestamp were not being parsed. This issue has been fixed.
ArcMC Onboard Connectors	CON-18987	The Event Broker is now added to the destination list after the ArcMC container upgrade.
Cisco IronPort Web Security Appliance File	CON-18410	Added new mappings for deviceHostName and deviceAddress to fix a parsing issue.
McAfee Network Security Manager DB (ID-based) McAfee Network Security Manager DB (Time-based)	CON-16423	Due to a connection pooling change, the connector failed to retrieve payload after running for some time. This issue has been fixed.
	CON-16587	Connector stopped querying events from the database because of a timeout setting on the MySQL Server and previously required a restart to resume parsing. This issue has been fixed.
McAfee ePolicy Orchestrator DB	CON-19409	Because the connector supported hdlp in version 4.6 and not version 5.1, the hdlp event type has been removed. The currently supported module and event type for ePO 5.3 is dlp, as renamed by vendor.

Known Limitations

All SmartConnectors

If you are using a map file with an expression setter in the `<connector_install_location>\current\user\agent\map location`, and the connector runs out of memory, then you can add the following property to `agent.properties` to work-around the problem:
`parser.operation.result.cache.enabled=false`

If this problem happens with Windows Event Log Native, and if the above work-around does not completely solve the problem, then reduce the value of the Native connector parameter '`eventprocessorthreadcount`'. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:
`agents[0].eventprocessorthreadcount=5` or
`agents[0].eventprocessorthreadcount=1,` etc..
where 0 is the index of the WINC connector in the container. [CON-19234, CON-18977]

Microsoft Office 365

When configuring the Office 365 connector, if you get the following error: `"HTTP/1.1 400 Bad Request" with the message: "{"error":{"code":"AF20024","message":" The subscription is already enabled. No property change."}}"`, you can ignore the error, continue configuration, and then run the connector to collect events.

The error is caused by an undocumented change in the Office 365 API response behavior. Before this change, when connector requested to start an already started subscription, the API would return a 200 OK response, and it would work fine. Office 365 API has changed the behavior to respond with HTTP error 400, instead of 200. Neither the change in API behavior, nor the new Error# AF20024, have been documented by Microsoft at: https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference [CON-18936]

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 11/20/2017

Lumension PatchLink Scanner DB – Product no longer available.

Support Ending 4/28/2018

Support ending for all 32-bit SmartConnectors – Use 64-bit SmartConnectors.

SmartConnectors Support Recently Ended

Support Ended 10/17/2017

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 ended 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.

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

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 Ended 08/15/2017

VMware Web Services – Support ended for vCenter versions 2.5, 3.5, 4.0, and 5.0 and ESX/ESXi servers 3.0, 4.0, and 5.0 due to end of support by vendor.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

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.

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 encryption parameters to Global Parameters. Updated information for downloading SQL Server JDBC drivers. Several mapping changes. See the Revision History table in the guide for details.

ArcSight FlexConnector REST Developer's Guide
Corrected JSON parser example. Added encryption parameters to Global Parameters.

SmartConnector Platform Support
Updated certified platforms for connector 7.7.0 release.

SmartConnector User Guide
- Added Format Preserving Encryption parameter information.
- Added description of Data Encryption.
- See the Revision History table in the guide for details.

SmartConnector Configuration Guides

All SmartConnector Configuration Guides
Added encryption parameters to Global Parameters.

Amazon Web Services CloudTrail
Updated descriptions for AWS SQS Region and AWS S3 Region.

Barracuda Firewall NG F-Series Syslog
First edition of this Configuration Guide.

Check Point Syslog
Added time zone mapping to common event mappings.

Cisco IronPort Web Security Appliance File
Added mappings for Device Address and Device Host Name.

HPE c7000 Virtual Connect Module Syslog
Removed Device Receipt Time mapping.

McAfee ePolicy Orchestrator DB
Removed hdlp event type.

Microsoft Exchange PowerShell
Added support for 2016 Access Auditing events.

Microsoft Windows Event Log – Native

Added statement that users are responsible for maintaining custom parsers that they created.

Pulse Secure Pulse Connect Secure Syslog

Removed mapping for Device Receipt Time.

Symantec Endpoint Protection DB

Added Old File Name, Old File Type, and Old File Permission mappings for group names and types.

Syslog NG Daemon

Updated IP Address parameter description.

UNIX OS Syslog

Removed Device Host Name and Device Receipt Time from general mappings. Added Device Time Zone mapping.