Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.6.4.8029.0

September 20, 2017

HPE Security ArcSight
SmartConnector Parser Update Release Notes

7.6.4.8029.0

September 20, 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

Contents

SmartConnector Parser Release 7.6.4.8029.0

These notes list SmartConnectors for which parser changes have been made and describe how to apply this latest ArcSight SmartConnector parser release.

Installation of the updated SmartConnectors can impact your created content. HPE advises you to verify the content you created before deploying the SmartConnector into your production environment.

Configuration guides for the SmartConnectors updated with this release are available from HPE Software Community Home: https://community.saas.hpe.com/t5/ArcSight-Connectors/Connector-Overview-documentation-index/ta-p/1592476

For successful SmartConnector configuration, follow the procedures documented in the individual SmartConnector configuration guides.

Supported SmartConnector Version

This parser update has been certified with SmartConnector Framework release 7.6.0.8009.0. Use of this update with earlier framework releases is not supported.

Obtain Parser Release AUP File

ArcSight Marketplace

The monthly ArcSight SmartConnector parser update releases are posted to the ArcSight Marketplace. ArcSight Marketplace is an app store that enables rapid provisioning of your ArcSight SIEM deployment with content updates and trusted security content packages.

An ArcSight Marketplace administrative account is required to download and install the monthly connector parser updates. Browse to the Marketplace at https://marketplace.saas.hpe.com/arcsight to set up your administrative account.

HPE SSO

The monthly ArcSight SmartConnector parser update releases are also posted to HPE Software Support Online (SSO) (https://softwaresupport.hpe.com/). All HPE Software contract customers have access to Software Support Online through their HPE Passport.

New Component, Version, or OS Support

SmartConnector for	Version
Check Point Syslog	Modules: ESOD, Eventia Analyzer Server, Identity Logging, and VPN-1 Edge for R77.30
F5 BIG-IP Syslog	Access Policy Module (APM) 11.6
Juniper JUNOS Syslog	15.1 MX Series Virtual Chassis (MX960 router)
Linux Audit File Linux Audit Syslog	RHEL 6.7
UNIX OS Syslog	RHEL 6.7 and 7.3

SmartConnector Enhancements

Linux Audit Syslog
Special characters can now be used and parsed correctly in 'sourceUserName'. [CON-19221]

Symantec Endpoint Protection DB
OS information is now included in alerts events. [CON-19098]

Fixed Issues

SmartConnector for	Number	Description
All Syslog Connectors	CON-17126	The connector selected the wrong subagent for some events from Linux servers. This issue has been fixed.
Cisco ASA Syslog	CON-19423	Some events were not being parsed. This issue has been fixed.
	CON-19231	Some events were not being parsed properly. This issue has been fixed.
F5 BIG-IP Syslog	CON-17422 CON-17837 CON-18626	Some v11.6 events were not being parsed. This issue has been fixed.
	CON-19194 CON-19275	Some TMOS v12.1 events were not being parsed. This issue has been fixed.
Juniper JUNOS Syslog	CON-19452	Added support for previously unparsed events from JUNOS v15.1R3-S2.2.
	CON-19359	Some JUNOS v12.3 events were not being parsed. This issue has been fixed.
	CON-18747	Some JUNOS v14.2 events were not being parsed. This issue has been fixed.
IBM SiteProtector DB	CON-19259	Special characters in the database caused fatal exceptions to occur. This issue has been fixed.
McAfee ePolicy Orchestrator DB	CON-19446	Added mapping changes for ePO Security for Exchange events affecting five modules: HIPS, MSME, DLP, MOVE, ENS: - Event name remains unchanged - deviceCustomString1 is mapped to 'threatname' - deviceCustomString4 is mapped to 'DetectingProductID'
Pulse Secure Pulse Connect Secure Syslog	CON-18773	Device Custom String 6 was not mapped to deviceHostName field. This issue has been fixed.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

Support Ending 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 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.

QoSient ARGUS (Legacy) – Support ending 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 Ending 4/28/2018

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

SmartConnectors Support Recently Ended

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.

Updated Configuration Guides

SmartConnector configuration guides for the following devices have been updated for this release and are posted to the ArcSight Connector Documentation page on HPE Software Community at: https://community.saas.hpe.com/t5/ArcSight-Connectors/tkb-p/connector-documentation.

ArcSight CEF Cisco FireSIGHT Syslog
Updated link to sample perl script for configuring the CEF Agent.

Check Point Syslog
Added support for the following modules: ESOD, Eventia Analyzer Server, Identity Logging, and VPN-1 Edge.

F5 BIG-IP Syslog
Added support for Access Policy Module (APM) 11.6.

Juniper JUNOS Syslog
Added support for previously unsupported JUNOS 15.1 MX Series Virtual Chassis (MX960 router) events.

Linux Audit File
Added support for RHEL version 6.7 as a source device.

Linux Audit Syslog
Added support for RHEL version 6.7 as a source device.

McAfee ePolicy Orchestrator DB
Added support for v5.0 in the RSD mapping table. Removed support for Host Data Loss Prevention 9.0, 9.1, 9.2 Events with ePO 5.1. Updated Data Loss Prevention Events with ePO 5.3 mappings for DCS1 and DCS4.

Pulse Secure Pulse Connect Secure Syslog
Updated mapping for 'Device Host Name' in the Pulse Connect Secure Syslog Event mappings table.

Symantec Endpoint Protection DB
Added troubleshooting information about English-language only support for virus names. Added mappings in the Alerts Events Mappings tables (v12 and v14) for collecting OS information.

UNIX OS Syslog
Added support for event collection from RHEL versions 6.7 and 7.3.

Verify Your Upgrade Files Obtained from SSO

After you obtain the parser release file from SSO, and before you upgrade, 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

Upgrading to the 7.6.4.8029.0 Parser Release

The following sections document the multiple options for upgrading to this parser release:

- Upgrade Locally to this Parser Release
- Upgrade Remotely

Upgrade Locally to this Parser Release

Before starting this procedure, verify that you are running the SmartConnector framework version 7.6.0.8009.0. Applying this parser AUP release update to any SmartConnector release earlier that 7.6.0.8009.0 is not supported by HPE ArcSight.

To upgrade locally to this parser release:

1. Download the appropriate parser release upgrade AUP file from the ArcSight Marketplace site (https://marketplace.saas.hpe.com/arcsight) at **Categories > SmartConnectors** or from SSO (https://softwaresupport.hpe.com/)
2. Stop the SmartConnector.
3. To perform the parser upgrade, run the command:

   arcsight parseraupupgradelocal [your_upgrade_to_parser].aup [your_ignore_warning_flag]

   where:

   [your_upgrade_to_parser].aup is the full path of the upgrade to parser AUP file (the file downloaded in step 1.) This file will be moved by the upgrade script. Verify that no other process is holding this file. Verify that the logged in user has both execute and write permissions for the selected directory.

   [your_ignore_warning_flag] is the true/false flag indicating whether you want to ignore the “Parser AUP has later version than the connector” warning
4. The connector will be started automatically after upgrade has completed.

Upgrade Remotely to this Parser Release Using ArcMC

Before upgrading, have the latest version of the *HPE Security ArcSight Management Center Administrator's Guide* available for any questions.

Note: Updating the parser AUP with ArcMC requires ArcMC version 2.5 or later.

You can upgrade to the new parser release from ArcMC either directly from Marketplace using ArcMC or from your ArcMC repository. See the following sections for details:

- From Marketplace Directly
- From SSO or Marketplace, then Apply from the ArcMC Repository

From Marketplace Directly

Before starting this procedure, connector must be running. If you have not already done so, create your administrative account on the ArcSight Marketplace.

To upgrade directly from Marketplace:

1. Click **Node Management** in ArcMC.
2. In the navigation tree, navigate to the host on which the container resides.
3. Select the container to be upgraded.
4. Click the **Upgrade** button.
5. (If not logged into Marketplace) On the upgrade page, click on "Save ArcSight Marketplace User" to enter your Marketplace credentials. This is a one-time task, unless you need to update your credentials.
6. Under **Select Upgrade Type**, choose **Parser upgrade**.
7. From the **Select Upgrade Version** down-down list, select the 7.6.4.8029.0 (Latest) parser upgrade AUP file.
8. Click **Upgrade**.
9. Verify in the Details column, under "Parser upgrade file push status", that the file was successfully pushed to the container. It signifies that the parser upgrade file was automatically downloaded to your repository. Status will show "Successful."
10. Wait while connectors restart automatically.
11. Use the Verify the Parser Version AUP in Use procedure to determine the parser AUP file in use.

From SSO or Marketplace, then Apply from the ArcMC Repository

Prior to performing an upgrade of a container, you will need a connector AUP file of the new parser version in your ArcMC repository.

This is a two-part process:

- Uploading the parser release AUP file to the repository from Marketplace or SSO
- Applying the parser upgrade to all connectors in a container

Note: If the new parser release AUP file (7.6.4.8029.0) already exists the repository, go to the next procedure to apply the parser upgrade.

To upload the new parser release AUP file to your repository:

1. Download the parser release upgrade AUP file for the connector from the ArcSight Marketplace (https://marketplace.saas.hpe.com/arcsight) by selecting **Categories > SmartConnectors** or go to SSO (https://softwaresupport.hpe.com/).
2. Log in to the ArcMC browser-based interface.
3. Go to **Administration > Repositories**.
4. In the navigation tree, pick **Upgrade Files.**
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier. Click **Open**.
7. Click **Submit.** The file is uploaded.

You can now use the AUP upgrade file in the repository when you are ready to upgrade a container or containers to a specific version using the procedure.

To apply the parser upgrade AUP file to all connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to upgrade.
5. Click **Upgrade**.
6. On the upgrade page, under **Select Upgrade Type**, choose **Parser upgrade**.
7. Under **Select Upgrade Version**, from the drop-down list, choose the parser release AUP file version to which you want to use to upgrade the selected containers.
8. Click **Upgrade**. The upgrade is performed on all containers.

See “Upgrading All Connectors in a Container” in the *HPE Security ArcSight Management Center Administrator’s Guide* for complete upgrade instructions.

Roll Back to a Previous Version

Users can roll back to a previous version by using any of three methods suggested for upgrading:

1. Apply the previous version of parser AUP locally.
2. Apply the previous version of parser AUP directly from Marketplace
3. Upload the previous version of the parser AUP to the ArcMC repository from SSO or Marketplace, then apply from ArcMC repository.

Verify the Parser Version AUP in Use

The parser upgrade file in use can be verified in ArcMC or in the agent logs.

In ArcMC

1. Go to **Node Management > View All Nodes**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Verify that value in the **Parser Version** column matches the version number of the recent upgrade.

In the Agent Logs

1. Find the agent.log file at: `/ArcSight_Home/current/logs`
2. Search for the latest occurrence of the line in the log file that contains “ArcSight Parser Version.”

   Example:

   ```
   <CODE MAP: '7.6.0.8009.0'>
   <ArcSight Connector Version: 7.6.0.8009.0>
   <ArcSight Parser Version: 7.6.4.8029.0>
   ```