



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.6.1.8019.0

June 15, 2017

**HPE Security ArcSight
SmartConnector Parser Update Release Notes**

7.6.1.8019.0

June 15, 2017

Copyright © 2010 – 2017 Hewlett Packard Enterprise Development LP

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 7.6.1.8019.0	4
Supported SmartConnector Version	4
Obtain Parser Release AUP File.....	4
ArcSight Marketplace.....	4
HPE SSO.....	4
Version Updates	4
SmartConnector Enhancements	5
Fixed Issues.....	5
Known Limitations.....	7
Connector End-of-Life Notices	7
SmartConnector Support Ending Soon.....	7
Support Ending 08/15/2017	7
Support Ending 11/15/2017	7
Support ending 4/28/2018.....	8
SmartConnectors Support Recently Ended	8
Support Ended 06/15/2017	8
Support Ended 05/15/2017	8
Support Ended 02/15/2017	8
Updated Configuration Guides.....	9
Verify Your Upgrade Files Obtained from SSO.....	9
Upgrading to the 7.6.1.8019.0 Parser Release	10
Upgrade Locally to this Parser Release.....	10
Upgrade Remotely to this Parser Release Using ArcMC.....	10
From Marketplace Directly	10
From SSO or Marketplace, then Apply from the ArcMC Repository	11
Roll Back to a Previous Version.....	12
Verify the Parser Version AUP in Use.....	12
In ArcMC	12
In the Agent Logs.....	13

SmartConnector Parser Release 7.6.1.8019.0

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](#).

Version Updates

SmartConnector for	Version
Barracuda Email Security Gateway Syslog (formerly Barracuda Networks Spam Firewall NG Syslog)	8.0
Cisco IronPort Email Security Appliance File	10.0
Cisco IronPort Email Security Appliance Syslog	10.0
McAfee ePolicy Orchestrator DB	DLP 10.0 with ePO 5.3
Rapid7 NeXpose XML File	6.3

SmartConnector Enhancements

Cisco IOS Syslog

Some additional gate events are now supported. [CON-18526]

Citrix NetScaler Syslog

Date parsing is supported for v11.1. [CON-18639]

HPE Operations Manager I Web Services

Some tokens and mappings have been added to enhance parsing. [CON-18674]

HPE ProCurve Syslog

The parser supports the new log format version. [CON-18381]

HPE UX Syslog

Enhanced parser to include additional event types/modules. [CON-18906]

Linux Audit Syslog

Added support for Destination Service Name, Event Outcome, and enhanced parsing of the Name event. [CON-18425]

Updated parser mapping for the Destination User Name event to be parsed correctly. [CON-18873]

Fixed Issues

SmartConnector for	Number	Description
All Syslog SmartConnectors	CON-18250	Some parsing for Linux events was incorrect. This issues has been fixed. Note: This change could affect customer content. Two older DECIDs of Linux events: <ul style="list-style-type: none"> • Arcsight:1:65 authentication success • Arcsight:1:65 ignoring max retries have been changed to two new DECIDs with new names: <ul style="list-style-type: none"> • Arcsight:1:89 authentication success • Arcsight:1:88 PAM service ignoring max retries
	CON-18437	Updated parser to support unparsed events.
	CON-18891	Updated parser to map sourceUserName.
Blue Coat Proxy SG Syslog	CON-18346	The parser did not support v6.6.4 log formats. This issue has been fixed.
Check Point OPSEC NG	CON-18518 CON-18695 CON-18704	Issues that occurred when parsing destinationTranslatedAddress have been fixed.
Cisco ASA Syslog	CON-17370	Updated the parser to support unparsed events.
	CON-17444	Some events were parsed not as expected

SmartConnector for	Number	Description
	CON-18814	(or not parsed at all) and additional issues with hostname and IP address translation. These issues have been fixed. Note: The userdata mappings were changed as shown below to synchronize and unify all the mappings in the parser. Changes made could affect customer content: For CON-17444 & CON-18814: <ul style="list-style-type: none"> Mapped the last user data to the 'additionaldata.externalAuthenticationUser' field. Used the destination/source UserName field for the idfw_user data. The username is either source or destination, depending on the port and the host name associated with it. For CON-18814: <ul style="list-style-type: none"> Changes have been made to the following event IDs (DECIDs): 302013, 302014
	CON-17930	Event 720042 was not being parsed. This issue was fixed in the 7.5.2 SmartConnector release.
Cisco IOS Syslog	CON-18275	Some events were not being parsed. This issue has been fixed.
Citrix NetScaler Syslog	CON-18762 CON-17584	Updated the parser to support unparsed events.
F5 BIG-IP Syslog	CON-17703	Some v11.6 events were not being parsed. This issue has been fixed.
	CON-18420	Some v12.1 events were not being parsed. This issue has been fixed.
Fortinet FortiGate Syslog	CON-18411	Updated parser to support new keys.
HPE H3C Syslog	CON-18380	Some events were being parsed incorrectly. This issue has been fixed.
Juniper JUNOS Syslog	CON-18610	Updated the parser to support previously unparsed v12.3 events.
Pulse Secure Pulse Connect Secure Syslog	CON-17987	Some v8.1 events were not being parsed. This issue has been fixed.
	CON-18219	Some v8.2 R5 events were not being parsed. This issue has been fixed.
	CON-18279	Some events were not being parsed. This issue has been fixed.

SmartConnector for	Number	Description
	CON-18475	An event was not supported. This issue has been fixed.
	CON-18581	An event was not supported. This issue has been fixed.

Known Limitations

Check Point OPSEC NG

Check Point has updated their servers to be able to use SHA-256 certificates. A newer LEA client is needed to support these SHA-256 certificates. Because the SmartConnector for Check Point OPSEC NG does not use this new LEA client, the connector can no longer connect to collect events. The recommendation is to use the SmartConnector for Check Point Syslog to collect Check Point events. Note that the R77.30 Add-On on the Security Management Server or Multi-Domain Server is required for syslog event collection (see sk105412 at: <http://supportcontent.checkpoint.com/solutions?id=sk105412>). [CON-19222]

Oracle Audit Syslog

Time from original event is not parsed. End Time shows as time at which SmartConnector received the event and not the time from original event itself. [CON-18619]

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 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

Support Ended 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

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/Connector-Overview-documentation-index/ta-p/1592476>.

Barracuda Email Security Gateway Syslog

Changed connector name from Barracuda Networks Spam Firewall NG Syslog to Barracuda Email Security Gateway Syslog. Removed support for version 5.1. Added support for v8.0.

Check Point OPSEC NG

Added important information about LEA server and sha-256 certificate requirement.

Cisco ASA Syslog

Updated mappings for Destination Host Name, Destination User Name, Source Host Name, and Source User Name. Added information about user name mappings. See the fixed issues section of the release notes for details about how your content may be affected.

Cisco IronPort Email Security Appliance File

Added support for version 10.0.

Cisco IronPort Email Security Appliance Syslog

Added support for version 10.0.

Fortinet FortiGate Syslog

Updated Event mappings and UTM mappings.

HPE Operations Manager i Web Services

Updated mappings.

HPE H3C Syslog

Updated severity values in the mappings table.

Linux Audit Syslog

Updated mappings for Destination User Name and Destination NT Domain, and added mapping for Destination Service Name.

McAfee ePolicy Orchestrator DB

Added support for McAfee Data Loss Prevention (DLP) 10.0 with ePO 5.3.

Rapid7 NeXpose XML File

Removed support for version 4.0 through 4.12. Added support for version 6.3.

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 7.6.1.8019.0 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 than 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 7.6.1.8019.0 (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 (7.6.1.8019.0) 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/arc sight>) 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: 7.6.1.8019.0>
```