Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.5.1.7996.0

March 22, 2017

HPE Security ArcSight
SmartConnector Parser Update Release Notes

7.5.1.7996.0

March 22, 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 Parser Release 7.5.1.7996.0

Note: Parser Release 7.5.1.7994.0 did not parse syslog events correctly. If you are using parser AUP build 7994, you should upgrade to parser AUP build 7996.

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 Protect 724: https://www.protect724.hpe.com/community/arcsight/productdocs/connectors

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

Supported Version

This parser update has been certified with SmartConnector Framework release 7.5.0.7983.0. 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
Cisco IOS Syslog	15.6
Cisco IronPort Web Security Appliance File	10 (Apache and Squid formats)
F5 BIG-IP Syslog	F5 TMOS 12.0, 12.1
Microsoft Exchange Message Tracking Log Multiple Server File	Microsoft Exchange Server 2016
Proofpoint Enterprise Protection and Enterprise	8.4

SmartConnector for	Version
Privacy Syslog	
Symantec Endpoint Protection DB	14 (Server Admin Log, Behavior, and Virus categories)

SmartConnector Enhancements

SmartConnector for	Number	Description
Symantec Endpoint Protection DB	CON-16232	Now supports new host name fields for v12.
	CON-17060	Added event mappings for mappings for the fileHash and filePath. Corrected mapping for fileName.
	CON-16195	Added "Device Version" mapping support to the Traffic parser.

Fixed Issues

SmartConnector for	Number	Description
Cisco ASA Syslog	CON-17731	Some events were not being parsed. This issue has been fixed.
Cisco IOS Syslog	CON-18059	Some events were not being parsed. This issue has been fixed.
Cisco ISE Syslog	CON-17860	Some keys were not supported in the Cisco ISE parser. This issue has been fixed.
Cisco Wireless LAN Controller Syslog	CON-17198	Some events from v8.2 were not being parsed. This issue has been fixed.
F5 BIG-IP Syslog	CON-18298	When parsing a specific event, the connector stopped working. This issue has been fixed.
	CON-18482	Agent severity for some events were 'UNKNOWN'. This issue has been fixed.
	CON-18488	An event name contained variables. This issue has been fixed.
Juniper JUNOS Syslog	CON-18345	Some v12.1 events were not being parsed in the 7.3.0 connector release. This issue has been fixed.
Microsoft DNS Trace Log Multiple Server File	CON-17708	Some events were being parsed incorrectly. This issue has been fixed.
Microsoft Windows Event Log – Native	CON-17953	Source IP/Hostname was mapped incorrectly. This issue has been fixed.

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 Protect 724 at: https://www.protect724.hpe.com/community/arcsight/productdocs/connectors.

Cisco IOS Syslog
Added support for Cisco IOS version 15.6.

Cisco IronPort Web Security Appliance File
Added support for version 10 (Apache and Squid formats only).

Cisco ISE Syslog
Updated mapping definition for Device Receipt Time in the Cisco ISE Syslog Mappings table.

F5 BIG-IP Syslog
Added support for F5 TMOS version 12.0 and 12.1.

Microsoft Exchange Message Tracking Log Multiple Server File
Added support for Microsoft Exchange Server 2016. Updated the information about enabling message tracking for Exchange 2016 and about the configuration for internal to external email traffic.

Microsoft Windows Event Log – Native: Windows Security Event Mappings
Updated mappings for Event 4624. Removed support for Windows Server 2003 because vendor ended support.

Proofpoint Enterprise Protection and Enterprise Privacy Syslog
Added support for v8.4.

Symantec Endpoint Protection DB
Updated to support v14 events in the following mapping tables: Server Admin Log, Behavior, and Virus. Updated the Agent mappings table to extra support v12 events. Added "Device Version" support to the Traffic, Behavior, Server-Admin, and Virus mappings. Added support for File Path and File Hash to the Alerts mappings.

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 7.5.1.7996.0 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 7.5.0.7983.0. Applying this parser AUP release update to any SmartConnector release earlier that 7.5.0.7983.0 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 7.5.1.7996.0 (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 (7.5.1.7996.0) 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: '7.5.0.7983.0'>
   <ArcSight Connector Version: 7.5.0.7983.0>
   <ArcSight Parser Version: 7.5.1.7996.0>
   ```