Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.3.1.7910.0

September 30, 2016

HPE Security ArcSight
SmartConnector Parser Update Release Notes

7.3.1.7910.0

September 30, 2016

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 7.3.1.7910.0

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 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 7.3.0.7886.0. 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
Dell ChangeAuditor DB	6.7
McAfee ePolicy Orchestrator DB	MOVE 3.6 with ePO 5.3
Microsoft IIS Syslog	10.0
Tenable Nessus .nessus File	6.6

SmartConnector Enhancement

SmartConnector for	Number	Description
McAfee Network Security Manager Syslog	CON-16336	Support for the $IV_LAYER_7_DATA$ field for L7 data has been added.

Fixed Issues

SmartConnector for	Number	Description
HPE Integrated Lights Out Syslog	CON-17489	Customer reported parsing issues have been fixed.
F5 BIG-IP Syslog	CON-17367	Parsing issues with "name" and "deviceEventClassID" fields have been fixed.
Juniper JUNOS Syslog	CON-17368	Some event types were not being parsed. This issue has been fixed.
McAfee Firewall Enterprise Syslog	CON-17483	Added mapping of dest_ip to Destination Address field.
NetApp Filer Syslog	CON-17535	With connector version 7.2.4, for some events the “Name” field was unparsed. This issue has been fixed.

Known Limitations

Upgrading remotely using ArcMC when Windows path to connector contains a space

When upgrading through ArcMC, where connectors reside on the Windows platform, the upgrade will fail when there is a space in the path to the connector location. This will be fixed in a future SmartConnector release. [CON-17874]

Workaround: Use the script and upgrade locally as described in Upgrade Locally to this Parser Release procedure.

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.

Dell ChangeAuditor DB

Added support for version 6.7.

McAfee ePolicy Orchestrator DB

Added support for MOVE AV Agentless 3.6 for ePO 5.3.

McAfee Firewall Enterprise Syslog

Updated mappings for 'Destination Address' and 'Destination Port.' Added a 'File Size' mapping.

McAfee Network Security Manager Syslog
Added support for Layer 7 (L7) data.

Microsoft IIS Syslog
Added support for IIS version 10.0.

Tenable Nessus .nessus File
Added support for version 6.6 and updated mappings.

Tenable SecurityCenter XML File
Updated mappings in SecurityCenter XML Vulnerabilities Mappings table.

Upgrading to the 7.3.1.7910.0 Parser Release

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

- Upgrade Locally to this Parser Release
- Upgrade Remotely Using ArcSight Management Center

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

Upgrade Locally to this Parser Release

Before starting this procedure, verify that you are running the SmartConnector framework version 7.3.0.7886.0. Upgrading to a 7.3 parser AUP release to a SmartConnector release earlier that 7.3.0.7886.0 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.

   [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.

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**.
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 7.3.1.7910.0 (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 Uploaded Parser Upgrade Version 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 (7.3.1.7910.0) 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) and select 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.

Verify the Parser Version AUP in Use

The parser upgrade file in use can be verified:

- In ArcMC
- 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. Check the `logstatus` in the agent logs.
2. Search for “Parser AUP Version=” in the log.

   Example: `Parser AUP Version=7.3.1.7901.0`