



Hewlett Packard
Enterprise

HPE Security ArcSight Logger

Software Version: 6.2 Patch 1

Release Notes

June 23, 2016

Legal Notices

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 shall not be liable for technical or editorial errors or 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.

HPE Security ArcSight 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 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.

Copyright Notice

© Copyright 2016 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

Support

Contact Information

| | |
|------------------------------|---|
| Phone | A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list |
| Support Web Site | https://softwaresupport.hpe.com |
| Protect 724 Community | https://www.protect724.hpe.com |

Contents

| | |
|---|----|
| ArcSight Logger 6.2 Patch 1 | 5 |
| What's New in this Release | 5 |
| Supported Platforms | 5 |
| Browser Support | 5 |
| System Requirements | 6 |
| Logger Documentation | 6 |
| Localization Information | 8 |
| Known Limitations in Localized Versions | 8 |
| Upgrading to Logger 6.2 Patch 1 (L7648) | 9 |
| Upgrade Paths | 9 |
| Verifying Your Upgrade Files | 9 |
| Logger Appliance | 10 |
| Prerequisites | 10 |
| Upgrade Instructions | 11 |
| Software Logger and Logger on VMWare VM | 12 |
| Prerequisites | 12 |
| Upgrade Instructions | 12 |
| Known Issues | 17 |
| Kernel Warning Message During Boot | 17 |
| Fixed Issues | 18 |
| Configuration | 18 |
| General | 18 |
| Reports | 18 |
| Open Issues | 20 |
| Analyze/Search | 20 |
| Configuration | 25 |

| | |
|-----------------------------------|----|
| Dashboards | 27 |
| General | 28 |
| Localization | 29 |
| Reports | 29 |
| Summary | 31 |
| System Admin | 32 |
| Upgrade | 33 |
| Send Documentation Feedback | 34 |

ArcSight Logger 6.2 Patch 1

These release notes provide information about the ArcSight Logger 6.2 Patch 1 (L7648) release. Logger is available in three form factors: as an appliance, as software, and as a virtualized image. Read this document in its entirety before using a Logger installed with this release.

What's New in this Release

The ArcSight Logger 6.2 Patch 1 (7648) release provides the same functionality as Logger 6.2, introduces fixes for a number of bugs, and includes important security updates.

Resolved issues are described under ["Fixed Issues" on page 18](#). For information about Logger 6.2 features and functionality, refer to the Release Notes, Administrator's Guide, and other Logger 6.2 documentation, available from the [ArcSight Product Documentation Community on Protect 724](#).

Supported Platforms

Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.2 Patch 1 platform support.

Note: Upgrading to Logger version 6.2 Patch 1 may require upgrading your Operating System (OS). If you need to upgrade your current OS as well as Logger, you must upgrade your OS first, and then upgrade Logger. For Logger Appliances, an OS upgrade file is included in your upgrade package.

Browser Support

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.2 Patch 1 browser support.

Ensure that Logger's publicly-accessible ports are allowed through any firewall rules that you have configured.

- For root installs, allow access to port 443/tcp as well as the ports for any protocol that the logger receivers need, such as port 514/udp for the UDP receiver and port 515/tcp for the TCP receiver.
- For non-root installs, allow access to port 9000/tcp as well as the ports for any protocol that the Logger receivers need, such as port 8514/udp for the UDP receiver and port 8515/tcp for the TCP

receiver.

Note: The ports listed here are the default ports. Your Logger may use different ports.

System Requirements

Logger requires the following minimum system setup.

| Specification | Details |
|---|--|
| CPU, Memory, and Disk Space for Enterprise Version of Software Logger | <ul style="list-style-type: none">• CPU: 2 x Intel Xeon Quad Core or equivalent• Memory: 12 - 24 GB (24 GB recommended)• Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data.• Root partition: 40 GB (minimum)• Temp directory: 1 GB <p>Note: Using a network file system (NFS) as primary event storage is not recommended.</p> |
| CPU, Memory, and Disk Space for Trial Logger and VM Instances | <ul style="list-style-type: none">• CPU: 1 or 2 x Intel Xeon Quad Core or equivalent• Memory: 4 - 12 GB (12 GB recommended)• Disk Space: 10 GB (minimum) in the Logger installation directory• Temp directory: 1 GB |
| VM Instances | <ul style="list-style-type: none">• You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger installer on a 64-bit CentOS 7.2 configured with 12 GB RAM and four physical (and eight logical) cores.• HP ArcSight strongly recommends allocating a minimum of 4 GB RAM per VM instance.• The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server. |
| Other Applications | <ul style="list-style-type: none">• For optimal performance, make sure no other applications are running on the system on which you install Logger. |

Logger Documentation

The new documentation for this release comprises these Release Notes, and updated versions of the ArcSight Data Platform Support Matrix, Logger Installation Guide, Trial Logger Quick Start Guide, and the Logger 6.2 Best Practices Guide. The complete documentation set published with Logger version 6.2 also applies to this release.

Tip: The most recent versions of these guides may not be included with your download. Please check Protect 724 for updates.

- **Logger 6.2 Online Help:** Provides information on how to use and administer Logger. Integrated in the Logger product and accessible through the user interface. Click the Options > Help link on any Logger user interface page to access context-sensitive Help for that page. Also available in PDF format as the Logger Administrator's Guide and Logger Web Services API Guide.
- **ArcSight Data Platform Support Matrix** (formerly the *Logger Support Matrix*): Provides integrated support information such as upgrade, platform, and browser support for Logger, ArcMC, and relevant SmartConnectors. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).
- **Logger 6.2 Administrator's Guide:** Provides information on how to administer and use Logger. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). Also accessible from the integrated online Help.
- **Logger 6.2 Web Services API Guide:** Provides information on how to use Logger's web services. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). Also accessible from the integrated online Help.
- **Logger Getting Started Guide:** Applicable for Logger Appliances only. Provides information about connecting the Logger Appliance to your network for the first time and accessing it through a web browser. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). Additionally, a printed copy is packaged with the Logger Appliance.
- **Logger 6.2 Patch 1 Installation Guide:** Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).
- **Logger 6.2 Patch 1 Quick Start Guide:** Provides information on how install and configure the Trial Software Logger on Linux or VMware VM. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).
- **Logger 6.2 Data Migration Guide:** Provides information on how migrate Logger data from one Logger Appliance to another or to a Software Logger. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).
- **Logger 6.2 Best Practices Guide:** Provides information on how to configure and use Logger for best performance. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).

Additional Logger documentation, including the Logger Data Migration and Best Practices Guide can be downloaded from the [ArcSight Product Documentation Community on Protect 724](#).

Localization Information

Localization support for these languages is available for this release:

- Japanese
- Traditional Chinese
- Simplified Chinese

You can either install Logger in one of the above languages as a fresh install or upgrade an existing English installation to one of these languages. The locale is set when you first install Logger. Once set, it cannot be changed.

Known Limitations in Localized Versions

The following are the currently known limitations in the localized versions of Logger:

- Only ASCII characters are acceptable for full-text search and the Regex Helper tool. Therefore, full-text search is not supported for Japanese, Simplified Chinese, or Traditional Chinese characters.
- The Login field on the Add User page does not accept native characters. Therefore, a Logger user cannot have a login name that contains native characters.
- Reports are localized for Japanese only.
- The Report Parameter and the Template Style fields do not accept native characters.
- Some Logger user interface sections are not localized. For example, the following sections are available in English only:

| | |
|-------------------------------------|-----------------|
| Reboot | Network |
| License & Update | CIFS |
| NFS | RAID controller |
| SSL Server Certificate | Authentication |
| Summary | Dashboards |
| Field Summary (Search Results page) | |

- The Certificate Alias field for ESM Destinations cannot contain native characters. Use only ASCII characters in the Certificate Alias field. (To open the Certificates page, type Certificates in the **Take me to...** search box, and click **Certificates** in the dropdown list.)

Upgrading to Logger 6.2 Patch 1 (L7648)

This section includes upgrade information for the Logger Appliance, Software Logger, and Logger on VMWare VM.

- ["Verifying Your Upgrade Files" below](#)
- ["Logger Appliance" on the next page](#)
- ["Software Logger and Logger on VMWare VM" on page 12](#)

Note: Be sure to review the sections ["Known Issues" on page 17](#), ["Fixed Issues" on page 18](#), and ["Open Issues" on page 20](#) before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.2 Patch 1. For more information about upgrading from a version of another appliance model or an earlier software version, consult the Release Notes, Data Migration Guide, and Support Matrix for that version, or contact HPE Support.

Note: To determine your current Logger version, hover the mouse pointer over the ArcSight Logger logo in the upper left corner of the screen.

| Logger 6.2 Patch 1 Upgrade Paths | |
|----------------------------------|---|
| Software Versions | 6.2 (7633) |
| Appliance Models | L350X L750X L750X-SAN L7600 |
| Operating System Upgrades | <ul style="list-style-type: none">• The OS your Logger is running on may vary. Be sure to check the OS version and upgrade the OS to a supported version if necessary, before upgrading Logger.• Refer to the ADP Support Matrix document available on the Protect 724 site for a list of supported Operating Systems. |

Verifying Your Upgrade Files

HPE provides a digital public key to enable 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>

Logger Appliance

Read the following prerequisites carefully before upgrading your Logger Appliance.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a Configuration Backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- You must be on Logger 6.2 prior to upgrading to Logger 6.2 Patch 1.
- You may need to upgrade your OS before you upgrade Logger. Refer to the ADP Support Matrix document available on the Protect 724 site for a list of supported Operating Systems.
 - If you are upgrading an Lx500 series appliance, do not upgrade the OS. The required OS is the same as it was for Logger 6.2.
 - If you are upgrading an Lx600 series appliance, you must upgrade your OS to RHEL 7.2. (Logger 6.2 Patch 1 includes an OS Upgrade file for this purpose.)
- Download the upgrade files from the HPE Customer Support site at: <https://softwaresupport.hpe.com> to a computer from which you connect to the Logger UI.
 - For both local upgrades and remote upgrades using ArcMC, download the following file: `logger-7648.enc`
 - For OS upgrades, download the following file, if needed: `osupgrade_logger_rhel72_<timestamp>.enc`
 - Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).
- Verify the upgrade files, as described in "[Verifying Your Upgrade Files](#)" on the previous page.

Upgrade Instructions

To upgrade Logger Appliances remotely through ArcMC:

1. Upgrade your OS if necessary.
 - If you are upgrading an Lx500 series appliances do not upgrade the OS.
 - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade_logger_rhel72_<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
2. Deploy the Logger upgrade by using the file `logger-7648.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

To upgrade a Logger Appliance locally:

1. Log into Logger and click System Admin | System > **License & Update**.
2. Upgrade your OS if necessary.
 - If you are upgrading an Lx500 series appliance do not upgrade the OS.
 - If you are upgrading an Lx600 series appliance, browse to the `osupgrade_logger_rhel72_<timestamp>.enc` file you downloaded previously and click **Upload Update**.

This will upgrade the OS to RHEL 7.2.

3. The **ArcSight License & System Update** page displays the update progress. Once the upgrade is complete, Logger reboots automatically.

Note: If prompted to upload a license and set the time zone at this stage, contact HPE Support for assistance.

4. Make a Configuration Backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

Software Logger and Logger on VMWare VM

Read the following prerequisites carefully before upgrading your Software Logger or Logger VM.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a Configuration Backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- You must be on Logger 6.2 prior to upgrading to Logger 6.2 Patch 1.
- You may need to upgrade your Operating System (OS) to a supported version before upgrading Logger. For a list of supported Operating Systems, refer to the *ArcSight Data Platform Support Matrix*, available for download from the [ArcSight Product Documentation Community on Protect 724](#).
 - If your system is running on RHEL or CentOS 7.1, upgrade to version 7.2.
 - If your system is running on RHEL or CentOS 6.7, you do not need to upgrade your OS.
 - For Software Loggers, if not already done on the system, increase the user process limit on the Logger's OS. Refer to "Increasing the User Process Limit" section of the ArcSight Installation Guide. You do not need to do this for Logger on VMWare VM, it is already done on the provided VM.
- Download the Software Logger upgrade files from the HPE Customer Support site at [HPE Software Support](#).
 - For remote upgrades using ArcMC, download the following file:
`logger-sw-7648-remote.enc`
 - For local upgrades, download the following file:
`ArcSight-logger-6.2.0.7648.1.bin`
 - Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).
- Verify the upgrade files, as described in "[Verifying Your Upgrade Files](#)" on [page 9](#).

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger.

- To upgrade Logger remotely, see "[To upgrade Software and VMWare Loggers remotely through ArcMC:](#)" on the next page.

- **Note:** Remote OS upgrade is not supported for Software Logger. If OS upgrade is required for your Logger upgrade, perform the OS upgrade manually before upgrading Logger.
- To upgrade Software Logger locally, see ["To upgrade Software Logger locally:"](#) below.
- To upgrade Logger on VMWare locally, see ["To upgrade Logger on VMWare VM:"](#) on page 15.

To upgrade Software and VMWare Loggers remotely through ArcMC:

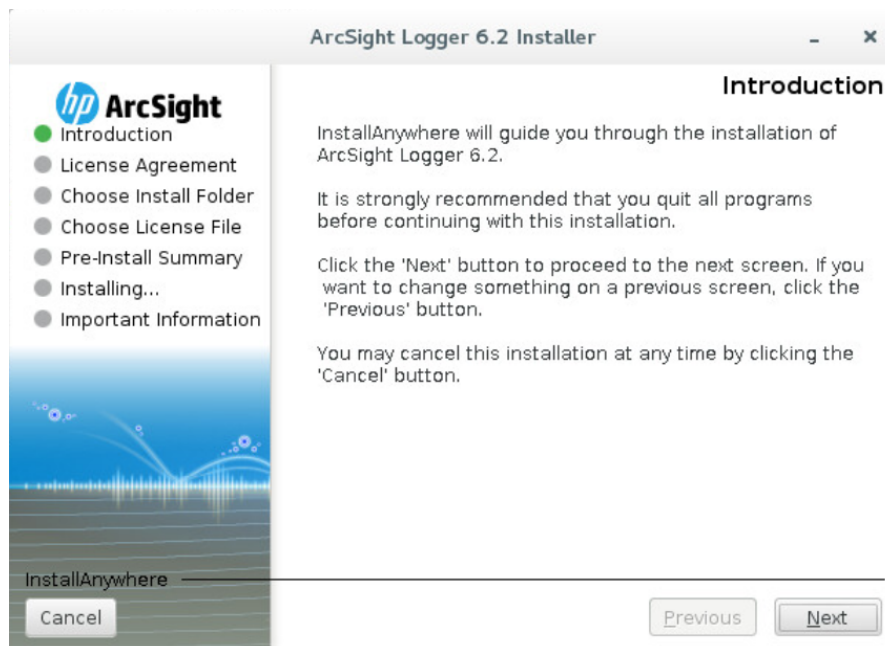
1. Before you begin, ensure that you meet the ["Prerequisites" on the previous page](#).
2. Deploy the downloaded upgrade file, `logger-sw-7648-remote.enc`, by following the instructions in the ArcSight Management Center Administrator's Guide.

To upgrade Software Logger locally:

1. Before you begin, ensure that you meet the ["Prerequisites" on the previous page](#).
2. Log in with the same user name as the one used to install the previous version of Logger.
3. Run these commands from the directory where you copied the Logger software:

```
chmod u+x ArcSight-logger-6.2.0.7648.1.bin  
./ArcSight-logger-6.2.0.7648.1.bin
```

The installation wizard launches, as shown in the following figure. This wizard also upgrades your Software Logger installation. Click **Next**.



You can click **Cancel** to exit the installer at any point during the upgrade process.

Caution: Do not use the Ctrl+C to close the installer. If you use Ctrl+C to exit the installer and then uninstall Logger, uninstallation may delete your `/tmp` directory.

4. The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the “I accept the terms of the License Agreement” button.
5. Select **I accept the terms of the License Agreement** and click **Next**.
6. If Logger is currently running on this machine, an Intervention Required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the upgrade, or click **Quit** to exit the installer.

If you click Continue, the installer stops the running Logger processes and checks for other installation prerequisites. Once all Logger processes are stopped and the checks complete, the next screen is displayed.
7. Navigate to or specify the location where you want to install Logger. By default, the /opt directory is specified.
8. If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Click **Back** to specify another location or **Quit** to exit the installer.
9. If Logger is already installed at the location you specify, a User Intervention message is displayed telling you that the selected directory already contains an installation of Logger, and asking if you want to upgrade.
10. Click **Upgrade** to continue or **Back** to specify another location.

Note: When you upgrade an existing installation, the upgraded Logger has access to the data store of the previous version. However, if you install Logger in a new location, it is the equivalent of installing a fresh instance of Logger, which will not have access to the data store of the previous version.

11. Review the pre-install summary and click **Install**.

Installing the upgrade may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.
12. Click **Next** to initialize Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
13. Click **Next** to configure Logger.

Configuration may take a few minutes. Please wait. Once the configuration is complete, Logger starts up and the next screen is displayed.
14. Click **Done** to exit the installer.
15. You can now connect to the upgraded Logger.
16. Make a Configuration Backup immediately after the upgrade. For instructions, refer to the Logger Administrator’s Guide for the Logger version you are currently running.

To upgrade Logger on VMWare VM:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 12](#).
2. Log in with the same user name as the one used to install the previous version of Logger.
3. Run these commands from the /opt/arcsight/installers directory:

```
chmod u+x ArcSight-logger-6.2.0.7648.1.bin
./ArcSight-logger-6.2.0.7648.1.bin
```

The installation wizard launches in command-line mode, as shown below. Press **Enter** to continue.

Introduction

InstallAnywhere will guide you through the installation of ArcSight Logger 6.2.

It is strongly recommended that you quit all programs before continuing with this installation.

Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:

The next several screens display the end user license agreement. Installation and use of Logger 6.2 Patch 1 requires acceptance of the license agreement. Press **Enter** to display each part of the license agreement, until you reach the following prompt:

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):

4. Type Y and press **Enter** to accept the terms of the License Agreement.
You can type quit and press **Enter** to exit the installer at any point during the installation process.
5. The installer checks that installation prerequisites are met. If a check fails, it displays a message. You will need to fix the issue before proceeding. For example, if Logger is currently running on this machine, an Intervention Required message is displayed. In that case, type Y and press **Enter** to stop all current Logger processes and proceed with the installation, or type quit and press **Enter** to exit the installer. Once all checks complete, the next screen is displayed.
6. The Choose Install Folder screen is displayed. Type the installation path for Logger and then press **Enter**.
The installation path on the VM image is /opt/arcsight/logger. You must use this location. Do not specify a different location.
7. Type Y and press **Enter** to confirm the installation location.
8. If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Type quit and press **Enter** to exit the installer and reconfigure your VM.

9. Type the absolute path to the license file and then press **Enter**.
10. Review the pre-install summary and press **Enter** to install Logger.
Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

11. If you are logged in as root, the following prompts will be displayed. Type responses and press **Enter** after each.

| Field | Notes |
|---|--|
| User Name | Use the non-root user "arcsight" that comes preconfigured on your VM image. |
| HTTPS Port | The port number to use when accessing the Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI. |
| Choose if you want to run Logger as a system service. | Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone. Selecting option 1 creates a service called arcsight_logger, and enables it to run at levels 2, 3, 4, and 5. If you do not enable Logger to start as service during the installation process, you can still do so later. For instructions on how to enable Logger to start as a service after installation, refer to the Logger Administrator's Guide. |

12. Type the number that describes the desired locale, and press **Enter**.
13. Press **Enter** to initialize Logger components.
Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
14. Press **Enter** to configure storage groups and storage volume and restart Logger automatically.
Configuration may take a few minutes. Please wait. Once configuration is complete, Logger starts and the next screen displays the URL you should use to connect to Logger.
15. Make a note of the URL and then press **Enter** to exit the installer.
16. You can now connect to the upgraded Logger.
17. Make a Configuration Backup immediately after the upgrade. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

Known Issues

The following known issues apply to this release.

Kernel Warning Message During Boot

The following message is displayed during the initial startup screen of Red Hat Linux on L7600, L7500, L7500-SAN, and L3500 series Loggers:

[Firmware Bug]: the BIOS has corrupted hw-PMU resources

A similar message is posted to the dmesg file. These messages do not affect the functionality or performance of Logger or the operating system, and can be safely ignored. For more information, refer to the HPE Customer Advisory document:

http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=4268690&docId=emr_na-c03265132

Fixed Issues

The following issues are fixed in this release.

- [Configuration](#)18
- [General](#)18
- [Reports](#)18

Configuration

| Issue | Description |
|-----------|--|
| LOG-16649 | <p>When Logger forwarded events to ESM, the EPS could drop to zero over a period of time. This happened because of a <code>java.util.ConcurrentModificationException</code> error.</p> <p>FIX: The <code>java.util.ConcurrentModificationException</code> error no longer occurs when forwarding to ESM, and the EPS rate no longer drops to zero.</p> |

General

| Issue | Description |
|-----------|--|
| LOG-15402 | <p>On Logger L7500 and L7600 appliances, platform audit events did not reflect the correct destination address for the Logger appliance.</p> <p>Fix: Platform audit events now populate the correct location in the <code>destinationAddress</code> field.</p> |

Reports

| Issue | Description |
|-----------|--|
| LOG-16324 | <p>In some cases, Logger Reports were not working after a Backup and Restore. This happened because Logger accepted too high a value for the Scheduled Report timeout limit. Some very high numbers caused the report engine to fail.</p> <p>FIX: The new limit on 'Database Connection Timeout' setting is 48 hrs (172800 seconds). The default value for the 'Database Connection Timeout' is 600 seconds.</p> |
| LOG-15916 | <p>Report category filters were not effective for peer queries. The result contained all events, whether or not they matched the filter.</p> <p>Fix: Report category filters are propagated to peer queries.</p> |

| Issue | Description |
|-----------|---|
| LOG-15229 | <p>The Logger Report iPackager feature did not load on later versions of Chrome.</p> <p>FIX: The iPackager is no longer a Java Applet, and can now open browsers that dropped Java applet support (Chrome 48, as well as Firefox 44 and IE 11 browsers.)</p> |
| LOG-14948 | <p>When exporting Reports to Excel, some letters were dropped in fields containing formatted data, such as multi-line SQL statements with indentation.</p> <p>FIX: Letters are no longer dropped in formatted data fields when Reports are exported to Excel.</p> |

Open Issues

This release contains the following open issues.

| | |
|--|----|
| • Analyze/Search | 20 |
| • Configuration | 25 |
| • Dashboards | 27 |
| • General | 28 |
| • Localization | 29 |
| • Reports | 29 |
| • Summary | 31 |
| • System Admin | 32 |
| • Upgrade | 33 |

Analyze/Search

| Issue | Description |
|-----------|--|
| LOG-16739 | <p>On rare occasions, indexing stops completely, causing severe performance degradation for the Logger.</p> <p>Workaround: Restart the server processes for the Logger, or reboot Logger to start indexing again. If your Logger database hasn't been defragmented in a while, performing one may help prevent this problem.</p> |
| LOG-16348 | <p>When exporting search results with all fields included, custom fields are not exported.</p> <p>Workaround: Avoid using the custom fields and use fields such as deviceCustomString1, deviceCustomNumber1, and so forth, to store the customized values.</p> |
| LOG-16347 | <p>When you search deviceEventClassId using the "where" clause, no search values are returned, even when matching events exist.</p> <p>Workaround: Use the AUSM query "_deviceGroup IN [value] AND deviceEventClassId=[value]"</p> |
| LOG-16325 | <p>In the Live Event Viewer, when a user adds a filter to search for a particular storage group, the filter does not work. The live event viewer search returns events from other storage groups that were not selected.</p> <p>Workaround: None available at this time.</p> |
| LOG-15972 | <p>If you are doing a forensic search on data that has been archived, a search may be unable to load an Event Archive from a day that has been partially archived from local storage, for example, events prior to a certain time on June 1, or if local memory has events already loaded from an archive from that same date.</p> <p>Workaround: Query around the affected time range, or reduce storage group retention to remove previously restored archived events from that date in local storage.</p> |

| Issue | Description |
|-----------|---|
| LOG-15079 | <p>Loading a Saved Search or Filter by using the Folder icon (Load a Saved Filter) fails if the query includes the INSUBNET operator.</p> <p>Workaround: In the text box, type \$\$\$<SavedSearchName> or \$filter\$<FilterName> and then click Saved Search or Filter in the dropdown list to load it.</p> |
| LOG-14814 | <p>Null values are not included in the Search results. For example, when performing a search on event data such as "NOT deviceCustomString1=bar", the search returns results that match deviceCustomString1 not equal to "bar", but does not return events where the deviceCustomString1 value is NULL.</p> <p>Understanding: With Logger's out-of-box configuration, you must explicitly call out NULL values with <field> IS NOT NULL or <field> IS NULL.</p> <p>Workaround: Logger can be configured to make NOT search conditions include NULL values. This implementation is available through HPE ArcSight Technical Support.</p> |
| LOG-14778 | <p>If a Receiver is deleted and re-created, search drill-down on that Receiver in the summary UI page will go to the Search page and query by Device Group, but search results do not include events received after re-creation of the Receiver.</p> <p>Workaround: Create a Receiver with different name and drill-down the events on the Summary page using the Device Group containing the new Receiver.</p> |
| LOG-14625 | <p>When a query calls more than ten fields using the "top" expression, Logger generates no results, but also does not give the user an error message that the supported number of fields has been exceeded. For example, "deviceProduct = "Logger" top deviceVendor, deviceVersion, deviceEventClassId, name,..." and so on.</p> <p>Workaround: Reduce your "Top" search queries to ten fields or less, or contact HPE ArcSight Technical Support for a more detailed workaround.</p> |
| LOG-14266 | <p>After updating the daily Archive task setting, you may not be able to see the event with a query like: message = "Daily archive task settings updated".</p> <p>Workaround: Use either of the following two queries to find the event:</p> <ul style="list-style-type: none"> - message CONTAINS "Daily archive task settings updated" - message STARTSWITH "Daily archive task settings updated" |
| LOG-14020 | <p>When performing a peer search, occasionally the search may terminate prematurely, with the error "[Local] Error: Database Connection displayed on the UI. This seems more likely to happen if you initiate a peer search on one of the Loggers, then immediately initiate peer search on the other Logger.</p> <p>Workaround: Run the query again.</p> |
| LOG-13752 | <p>If you check the Rerun Query checkbox when exporting search results, the download may not include all search results if it is started before the query finishes running.</p> <p>Understanding: In the current release, exported searches download a maximum of 1 million search results. However, when exporting search results with close to or over 1M hits with the re-run query checked, Logger may display the "Download results" link before the export file has finished populating. If you try to download the report during this period, the downloaded file might have only 100K or 600K lines instead of the final 800K or 1M lines.</p> <p>Workaround: There is no current way to tell when the file is ready for download from the User Interface. Wait a few minutes before downloading to get the full export file.</p> |

| Issue | Description |
|-----------|---|
| LOG-13532 | <p>When the time change due to the end of Daylight Savings Time (DST) takes place in the fall, (time is set back one hour), the search results may not display properly. This happens because Logger is not able to distinguish the event times in the overlap period.</p> <p>Workaround: To ensure that all events are returned and can be displayed, specify a start time of 12:59:59 or earlier and end time of 2:00:01 or later.</p> |
| LOG-12524 | <p>If the value for a discovered field contains a colon (:), an ampersand (&), or angle brackets (<>), the query generated by clicking on it will escape the character with an added slash (\).</p> <p>Workaround: Remove the backslash from in front of the character. For example, if the query inserted by clicking on the field is "IdentityGroup=IdentityGroup\All", then after removing the backslash, the query becomes "IdentityGroup=IdentityGroup:All".</p> |
| LOG-12290 | <p>When searching Logger with a query that includes the rename operator, if the original field name is included in the fieldset used in the search, the original field renamed by the operator is still displayed as a column in the search results, but will not have any values.</p> <p>For example, if the search uses the All Fields fieldset, which has deviceEventClassId, and its query includes "rename deviceEventClassId as eventCID", then both deviceEventClassId and eventCID will be shown in the search results, but deviceEventClassId will be empty and only eventCID will show the values of deviceEventClassId.</p> <p>Workaround: Since this issue is caused by the fields included in the fieldset used for the search, remove any renamed fields from the fieldset.</p> |
| LOG-12030 | <p>If you export Search results with just the three fields Event Time, Device, and Logger, you must check the All Fields check box or the export will not succeed.</p> <p>Workaround: To export search results without the All Fields requirement, add another field to export all of the corresponding events correctly.</p> |
| LOG-11299 | <p>If you uncheck the Rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail.</p> <p>Workaround: The Rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.</p> |
| LOG-11225 | <p>When using the auto complete feature on the Search page, if the query has a double quote followed by bracket ("[]), the query inserted by the auto complete cannot be executed because of incorrectly escaped quotes and backslashes.</p> <p>Workaround: Remove the backslash followed by a double quote on both sides of the string. For example, if the query inserted by the auto complete is "\"[/opt/mnt/soft/logger_server.log.6] successfully.\"\"", then after removing them, the query becomes "[/opt/mnt/soft/logger_server.log.6] successfully." You can also do this when double quote is followed by any special character such as "\", "/", "[", "]", or ".,</p> |

| Issue | Description |
|-----------|--|
| LOG-11066 | <p>If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues:</p> <ul style="list-style-type: none"> - On the Search page, the Events grid in the search results will be empty for any search, - GMT displays in timestamps with timezones. - In the Global Summary on the Summary page, the Indexing is reported one hour behind the current time stamp. <p>Workaround: Change the system time zone to something more specific, such as /America/Los_Angeles.</p> |
| LOG-10126 | <p>When using the replace operator, if the "from" string is included in the replacement string, the "from" string will be replaced twice. For example, the following command, when run against the data "john smith" will result in "johnnyny smith":</p> <p> replace "*john*" with "*johnny"</p> <p>Workaround: None available at this time.</p> |
| LOG-9420 | <p>When using the search term "transaction" on data that was received out of order, the duration may appear to be negative.</p> <p>Workaround: Include the term "sort_eventTime" before the transaction term.</p> |
| LOG-9025 | <p>When running Logger from an ESM console, a Logger quick search using One-Time Password (OTP) in the embedded browser fails after the Logger session has been inactive for the value 'Logger Session Inactivity Timeout'. The default timeout is 15 minutes.</p> <p>Workaround: Use an external browser to see results.</p> |
| LOG-7864 | <p>The time in the agentReceiptTime fields is not in human-readable format when exported.</p> <p>Understanding: Logger records time field values in UNIX epoch format (long values).</p> <p>Workaround: Use an epoch formula in Excel to convert the time value from epoch time.</p> |
| LOG-6965 | <p>When the time change due to the start of Daylight Savings Time (DST) takes place in the spring, and time is set ahead one hour, the following issues are observed:</p> <ul style="list-style-type: none"> - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket. - Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram. - If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results. <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p> |

| Issue | Description |
|----------|---|
| LOG-5958 | <p>When a field is removed from the Selected Fields list in the Customize FieldSet Editor, the field might not be displayed in the available fields list.</p> <p>Workaround: This only happens if you use the <- arrow to remove the field. If you double click on it, it will go back to the correct list.</p> |
| LOG-5181 | <p>Search results are not highlighted when there are multiple values that match the IN operator in a query.</p> <p>Workaround: None available at this time. Highlighting works if there is only one item in the square brackets. As soon as there is more than one, no highlighting occurs.</p> |
| LOG-4329 | <p>The full-text (keyword) search cannot find events that contain an IP or a MAC address that is prefixed with an equal to (=) character in the actual event. For example, these full-text queries will not locate the following event.</p> <p>Query 1: "ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00"</p> <p>Query 2: "192.168.10.153"</p> <p>Query 3: "192.168.10.255"</p> <p><166>Sep 9 14:48:22 beach kernel: Killed bad incoming packet: IN=eth1 OUT=</p> <p>MAC=ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00</p> <p>SRC=192.168.10.153 DST=192.168.10.255 LEN=229</p> <p>Workaround: Search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address. For example, you could search for "SRC=192.168.10.153" when looking for 192.168.10.153 in the source address field or "DST=192.168.10.255" when looking for 192.168.10.255 in the destination address field. Alternatively, you could run the data through a SmartConnector to convert to CEF format, and then run either a full-text or field-based search.</p> |

Configuration

| Issue | Description |
|-----------|---|
| LOG-16828 | <p>When Logger forwarded large events containing multi-byte characters to ESM, the EPS could drop to zero intermittently. A <code>StringIndexOutOfBoundsException</code> error appeared in the <code><...>/connector/logs/agent.out.wrapper.log</code> and eventually Logger could stop sending events to the ESM destination.</p> <p>Workaround: This release implements some improvements to prevent errors when events contain many multi-byte characters. We have been not been able to reproduce this issue in-house. After applying the patch please verify whether it resolves your issue.</p> |
| LOG-16379 | <p>For Software Logger installed on Redhat 7.1 or higher OS version, the configuration push by ArcMC fails to push the SNMP destination to the target Logger.</p> <p>Workaround:</p> <p>Option 1: Push the config again to the destination Logger.</p> <p>Option 2: Manually add the SNMP destination on the target logger.</p> |
| LOG-16024 | <p>When platform:230 and platform:201 events are forwarded from Logger to an ESM manager, the device host name and device address are converted to localhost and 127.0.0.1 respectively.</p> <p>Workaround: None available at this time.</p> |
| LOG-15530 | <p>Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail.</p> <p>Workaround: Do not configure LDAP on the system where the Software Logger is installed, and configure LDAP as the authentication method from the Logger system Admin > Authentication > External Authentication page.</p> |
| LOG-15454 | <p>Logger may experience failures to forward very large events to ESM.</p> <p>Workaround: Please contact HPE ArcSight Technical Support for help with this issue.</p> |
| LOG-14650 | <p>You cannot export a filter that has been previously imported. If you try to export such a filter, the export fails and Logger displays an error. This issue does not affect other export contents, such as Alerts, Saved Searches, or Dashboards.</p> <p>Workaround: None available at this time.</p> |
| LOG-14546 | <p>When you create a copy of a saved search, modify the query to have an invalid value, and try to save this new saved search, the system reverts the query and the name field keeps duplicating "Copy of". Every instance the name will have a new instance of "Copy of".</p> <p>Workaround: Correct the query, change the saved search name to remove the instances of "Copy of". Then save the search.</p> |

| Issue | Description |
|-----------|--|
| LOG-13834 | <p>When archiving data from a Logger Appliance, the "GMT+x" time zone incorrectly works like "GMT-x", while the "GMT-x" time zone works like "GMT+x".</p> <p>Workaround: Specify the Logger Appliance time zone by location. For example, set the time zone as "Taipei" or "Los Angeles."</p> |
| LOG-13226 | <p>A user can edit a forwarder while the forwarded is enabled. This can cause the forwarder to stop sending events.</p> <p>Workaround: Before editing the forwarder, disable it. Then edit it and re-enable it to have the forwarder send events to its target destination.</p> |
| LOG-11290 | <p>When you delete a Receiver, the Receiver's numeric ID still displays in the Summary page, although it is correctly deleted from the Dashboards.</p> <p>Workaround: Restart the Logger.</p> |
| LOG-11176 | <p>When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references.</p> <p>Workaround: Try to edit the Receiver to verify that the RFS mount is valid. Alternatively, verify the mount on the System Admin > Remote File Systems page.</p> |
| LOG-10605 | <p>The Source Types page (Configuration > Source Types) is not visible to non-Admin users.</p> <p>Workaround: To give users access to Source Types and Parsers Configuration pages, assign them Default Logger Rights Group and Default System Admin Group rights.</p> |
| LOG-10581 | <p>If you delete a parser that has an associated Source Type and is being used by a Folder Follower Receiver, no warning message is displayed indicating the dependency.</p> <p>Workaround: None available at this time.</p> |
| LOG-10056 | <p>You may see a duplicate device name if a receiver was removed and a new one was created with the same name as the old one. When you search on this device, Logger uses the old device and you will not be able to search on the new device.</p> <p>Workaround: Do not create a receiver with a name you have used for a deleted receiver.</p> |
| LOG-8790 | <p>When forwarding alerts to SNMP, if the community string contains non-ASCII characters, the SNMP trap sent out displays "??" in the community field. This is a display issue and does not affect SNMP authentication on Logger.</p> <p>Workaround: Avoid using non-ASCII characters in the community string.</p> |
| LOG-8194 | <p>After restoring Logger from a backup configuration, the CIFS share cannot be mounted because the user name and password fields are empty.</p> <p>Workaround: Edit the setting of the CIFS share and re-enter your username and password.</p> |

| Issue | Description |
|----------|--|
| LOG-4986 | <p>If there is an improper tear-down of the peering relationship, Loggers in the relationship might not detect it. Consequently, when you try to reestablish the relationship, it might not succeed. Examples of improper tear-downs include when one of the Loggers is replaced with a new appliance and when the peering relationship is deleted on one Logger while the other is unavailable (powered down).</p> <p>Workaround: If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from the peer Loggers before re-initiating the relationship.</p> |
| LOG-4885 | <p>If you delete a certificate from the Configuration Data > Configuration page, the certificate remains in the certificate list until the page is refreshed, even though the certificate was correctly deleted.</p> <p>Workaround: Refresh the page, and the deleted certificate will no longer appear in the certificate list.</p> |
| LOG-370 | <p>The Configuration Backup (Configuration > Configuration Backup > Backup_name) and File Transfer Receivers (Configuration > Receivers) may fail without notification. The most likely cause is a problem with configuration parameters, such as Remote Directory, User, or Password. If an error occurs, the command appears to succeed but it does not.</p> <p>Workaround: The error is written to the log, so check the log (Configuration > Retrieve Logs) if you suspect a problem with the backup. When a Configuration Backup is scheduled, the error status is shown in the Finished Tasks status field.</p> |

Dashboards

| Issue | Description |
|-----------|--|
| LOG-15827 | <p>When creating a Dashboard from the Search page, if the dashboard name contains a slash (/), Logger displays an error, but still creates the Dashboard as named. This results in a Dashboard that users cannot access or delete.</p> <p>Workaround: Do not use the slash character within Dashboard names.</p> |
| LOG-15500 | <p>When you hover over a Dashboard Monitor graph, you might see the data point label without the data point value. This problem does not exist for graphs in the New Monitor Dashboard.</p> <p>Workaround: Switch to New Monitor Dashboard to view the graph. Graphs with shorter time periods tend not to have this problem as often.</p> |
| LOG-14156 | <p>On Internet Explorer, the bottom of the Monitors Dashboard does not always render properly.</p> <p>Workaround: To avoid this rendering problem when viewing the Monitors Dashboard, maximize the Internet Explorer window.</p> |
| LOG-11730 | <p>When there are two or more Dashboards with the same name, after you select one of them from the Dashboard dropdown menu, you will not be able to open and view the other Dashboard.</p> <p>Workaround: Rename any Dashboards with duplicate names.</p> |

General

| Issue | Description |
|-----------|---|
| LOG-16439 | <p>The documentation does not explain clearly how to use the RESTful Search Web service to return aggregate search data from the sort, tail, and head operators.</p> <p>Workaround: Use the chart_data HTTP POST to return aggregate search data. The chart_data service returns the data you can use to display a chart and the table under the chart. It can also be used to return the results of aggregate operators like sort, tail, and head.</p> |
| LOG-15501 | <p>CentOS 7.1 does not automatically recognize a second hard drive to the VMware template after correctly adding it.</p> <p>Workaround: Run the following commands on the virtual machine console after adding the second hard drive:</p> <p>Note: In the following commands, replace "ARCSIGHT_HOME" with the path where the Logger software will be installed. Make a note of this location. When you run the Logger installer, be sure to use that path.</p> <ol style="list-style-type: none">1. Run the parted tool: parted /dev/sdb2. Attach a label to the disk: mklabel gpt3. Make an XFS partition utilizing the whole capacity of the drive: mkpart primary xfs '0%' '100%'4. Exit parted: q5. Create XFS file system and assign a label: mkfs.xfs -L DATA /dev/sdb16. Append the following line to the /etc/fstab file to mount this partition on boot: LABEL=DATA ARCSIGHT_HOME/data xfs defaults,inode64 1 27. Create a mount path: mkdir ARCSIGHT_HOME/data8. Mount the file system: mount -L DATA |
| LOG-15490 | <p>In some circumstances during a data migration to a 7600 appliance, some processes will not restart on the target machine after the reboot.</p> <p>Workaround: Use SSH to restart all processes manually using this command: /opt/local/monit/bin/monit restart all</p> |
| LOG-15291 | <p>The Logger L750x appliance may generate a kernel panic error.</p> <p>Workaround: Upgrade the iLO firmware on the appliance to version 1.51 or later. For more information, see the HPE customer advisory:</p> <p>http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04332584</p> |
| LOG-14595 | <p>On Logger appliances, the message "error: Bind to port 22 on 0.0.0.0 failed: Address already in use." gets logged every minute to /var/log/secure.</p> <p>Workaround: This message will appear only if SSH access has been enabled, and can be ignored. The SSH daemon is erroneously restarted every minute even if already running.</p> |
| LOG-11473 | <p>When using the Setup Wizard to enter a Logger Appliance initial configuration, Logger does not check that you have entered all the required information before submitting it. This can result in the setup to fail.</p> <p>Workaround: Enter valid values for all required Setup Wizard fields.</p> |

Localization

| Issue | Description |
|-----------|---|
| LOG-15905 | <p>The Logger configuration backup file has the format: <date>_<time>.configs.tar.gz. When the locale is set to Chinese Traditional, the <date> element contains Chinese characters. This causes the Secure Copy Protocol (SCP) command to fail, if you use SCP only in the Target backup server for Secure Copy.</p> <p>Workaround: Use openSSH for configuration backups.</p> |
| LOG-15761 | <p>When "Traditional Chinese" is configured as the interface language, the type of chart cannot be changed in the UI. Whichever chart type you choose, it always displays column type.</p> <p>Workaround: None available at this time.</p> |

Reports

| Issue | Description |
|-----------|---|
| LOG-16597 | <p>When search results for the arc_destinationProcess name field are more than 30 characters long, Logger Reports may truncate the field.</p> <p>Workaround: Please contact HPE ArcSight Technical Support for help with this issue.</p> |
| LOG-16589 | <p>When a peer is removed from a peer Logger configuration, scheduled peer reports may default to the "Local Only" option, and not search the remaining peers.</p> <p>Workaround: Check all scheduled reports and assign peers after any changes made to the peer configuration.</p> |
| LOG-16405 | <p>From the Logger user interface, users can be assigned rights to view, run or schedule specific reports that may not be part of their default privileges. When the same report is run through the SOAP API , those rights don't apply, and the report can only be run when the individual has the right to "View, run, and schedule all reports."</p> <p>Workaround: None at this time.</p> |
| LOG-16349 | <p>For a newly-installed Logger, Report objects and queries are not available until you navigate to the Reports Dashboard (Reports > Dashboard) for the first time.</p> <p>Workaround: Before attempting to create a query or report, navigate to the Reports dashboard to provision the Report objects.</p> |
| LOG-16346 | <p>When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it was copied.</p> <p>Workaround: None available at this time. Clicking Copy or Copy as Link will not give you a visual indication that anything has been copied, but you will be able to Paste, as needed.</p> |
| LOG-16281 | <p>Peer reports fail when Logger is peered with ESM 6.8c. This happens because the database type of the event field "arc_sourceAddress" is different for Logger and ESM.</p> <p>Workaround: None available at this time.</p> |

| Issue | Description |
|-----------|--|
| LOG-16260 | <p>If a single connector is sending events to multiple destinations, then the Daily Byte Count report might show the wrong Daily Byte Count number.</p> <p>Workaround: None available at this time.</p> |
| LOG-15462 | <p>When the file system /opt/arcsight/userdata is full, Logger allows users to run reports, even though they necessarily fail. Logger does not warn users in advance that the free space on the file system is full. This is important for scheduled reports.</p> <p>Workaround: Check the amount of free space periodically.</p> |
| LOG-15056 | <p>If you install a Logger solution (such as Payment Card Solutions (PCI), IT Governance (ITGov), or Sarbanes-Oxley (SOX)) before you have opened the Reports page at least once, some report categories are not available.</p> <p>Understanding: This happens if the Logger reports engine has not yet been initialized when the Solutions package is installed. The Foundation, SANS Top5, and Device Monitoring reports are affected.</p> <p>Workaround: Log into Logger and open the Reports page before installing any solutions package. This information has been added to the Logger Administrator's guide and will also be included in the next versions of the PCI, ITGov, and SOX Compliance Insight Package Guides for Logger.</p> |
| LOG-14386 | <p>If you open the Reports Dashboard in an Internet Explorer 11 window that is less than 1450px wide, the Reports menu is not displayed.</p> <p>Workaround: When working with Internet Explorer 11, always make your window wider than 1450px.</p> |
| LOG-13373 | <p>Report "Execution Status" doesn't list the most recent Jobs by default.</p> <p>Workaround: Navigate to the first page manually by clicking on the appropriate icon.</p> |
| LOG-13372 | <p>When user clicks on the graph at the top of the "Job Execution Status" page and then clicks "Last Run Status" table in the popup window, an error message appears.</p> <p>Workaround: Click directly on the table at the bottom of the "Job Execution Status" page.</p> |
| LOG-11659 | <p>In Software Loggers, the installation of multiple Solution Packages by the root user may fail if the SOX v4.0 solution package is installed before other packages.</p> <p>Workaround: If you are installing the SOX v4.0 solution package on Software Logger as the root user, install it last.</p> |
| LOG-11137 | <p>If a user has privileges to View a Published Report Only, then the report will not be visible in the Report Explorer.</p> <p>Workaround: You can find and view published reports from the Category Explorer instead. To find a published report, open the Category Explorer and navigate to the Saved Reports folder under the report's Category. (The terms "saved report" and "published report" are used interchangeably.)</p> |
| LOG-10923 | <p>Using run-time parameter filters on Ad hoc Reports can limit results to 100,000 lines. The Admin guide mentions this limit for Group and Sort parameters, but the restrictions apply to all run-time parameters.</p> <p>Workaround: Use hard-coded SQL parameters to generate results over 100,000 lines.</p> |
| LOG-10098 | <p>Reports display a dash (-) for null values. If this is displayed in a drill-down column, the column displays the dash as a hyperlink, which usually opens with unexpected results, since '-' does not match the query.</p> <p>Workaround: None available at this time.</p> |

| Issue | Description |
|----------|--|
| LOG-9860 | <p>When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it was copied.</p> <p>Workaround: None at this time. Clicking Copy or Copy as Link will not give you a visual indication that anything has been copied, but you will be able to Paste, as needed.</p> |
| LOG-9620 | <p>If a distributed report fails to run in the background against fields that do not exist on the peer Logger, the error message does not clearly indicate the reason.</p> <p>Workaround: None available at this time.</p> |
| LOG-8901 | <p>If you are using an email address with more than three characters in the top-level domain (such as user@yourco.info), Logger may reject the email as invalid.</p> <p>Workaround: Use an email address with a three-character top-level domain name for the report, and set up email forwarding to the non-standard email address.</p> |
| LOG-8780 | <p>Reports generated using the Web Services API do not contain report titles.</p> <p>Workaround: When generating reports through the Web Services API, ensure that you have entered the Report Title in the Report Editor (otherwise you will only see the Report ID) in the generated report.</p> |
| LOG-7186 | <p>If you limited a user's rights to a specific report template, the user was not able to run any reports at all and error messages were displayed when the user tried to run reports.</p> <p>Understanding: A user needs the right to see the parent node of the report tree in order to be able see the child node. An admin can edit permissions for individual Report folders without enabling access to levels higher on the tree. If this happens, the user cannot run or edit the reports.</p> <p>This issue is partially fixed. Now, when a user's permissions are set properly, the user can view the restricted reports and run them ad-hoc, but cannot schedule the restricted reports to run later.</p> <p>If a user tries to schedule a restricted report, the user will see: "Unauthorized Operation: We're sorry, but you are not authorized for that operation."</p> <p>Workaround: Give the user global access to all reports, then the user will be able to schedule the reports, as well as view and run them ad-hoc.</p> |

Summary

| Issue | Description |
|----------|--|
| LOG-9772 | <p>The number of events indexed as shown on the Summary page may not match the number of events found when you run a search with the same time range as shown on the Summary page.</p> <p>Understanding: The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different.</p> <p>Workaround: None available at this time. Currently, there is no way to specify the search time range in milliseconds.</p> |

System Admin

| Issue | Description |
|-----------|---|
| LOG-16759 | <p>SNMP polling for power supply, fan and temperature parameters is not supported on HPE Proliant appliances. This will be fixed in an upcoming release.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Install the following two RPM files on your ArcSight appliance:<ul style="list-style-type: none">- hp-health-10.40-1777.17.rhel7.x86_64.rpm- hp-snmp-agents-10.40-2847.17.rhel7.x86_64.rpm3. Download the following MIB files and copy them to the /usr/share/snmp/mibs folder on your ArcSight appliance:<ul style="list-style-type: none">- cpqhlth.mib- cpqghost.mib- cpqsinfo.mib4. Import the MIB files into the network management system. <p>Download links:</p> <p>For HPE Health and HPE SNMP Agent RPMs: http://downloads.linux.hpe.com/SDR/repo/spp/RedHat/7/x86_64/current/</p> <p>For Proliant MIB kit: http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04272529</p> |
| LOG-16757 | <p>Logger users can be deactivated due to the date_last_active database field not updating when the user logs in. Expected behavior would be that the field gets updated anytime a user successfully authenticates.</p> <p>Workaround: None available at this time.</p> |

| Issue | Description |
|-----------|---|
| LOG-16266 | <p>On L7600 Logger Appliances, the first time you visit the System Admin -> Process Status page after a reboot, some processes may appear to be in "Execution failed" state.</p> <p>Workaround: You can most likely ignore this; the processes are probably in the "running" state. The UI will display the correct state at the next automatic refresh or if you manually click Refresh Status.</p> |
| LOG-15456 | <p>The Apache process fails to start if "Client Certificate" or "Client Certificate AND User Password" has been enabled before Trusted Certificates are uploaded.</p> <p>Workaround: Apache will fail to start if the Trusted Certificates directory is empty. Upload Trusted Client certificates in the System Admin > Security > SSL Client Authentication > Trusted Certificates tab before enabling authentication methods from the System Admin > Users/Groups > Authentication > External Authentication tab.</p> |
| LOG-11700 | <p>Users may be unable to log in after they have been removed from a group.</p> <p>Understanding: Removing all group assignments from a user effectively disables that user account. User accounts not assigned to any group will be unable to log in.</p> <p>Workaround: To avoid disabling a user account when removing the user from a group, check that the user is assigned to the correct groups.</p> |

Upgrade

| Issue | Description |
|-----------|---|
| LOG-16711 | <p>On Logger L7600 series appliances upgrading from Logger 6.2 to Logger 6.2 Patch1, the user interface may not refresh when the upgrade is finished and Logger is rebooting.</p> <p>Workaround: If the upgrade is in progress for a long time, refresh the screen. If the login screen appears, the upgrade is done and you can log back in.</p> |

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Logger 6.2 Patch 1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!