Hewlett Packard
Enterprise

HPE Security ArcSight Logger

Software Version: 6.4

Release Notes

April 14, 2017

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

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.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Logger 6.4 Release Notes

These release notes apply to the HPE Security ArcSight Data Platform (ADP) Logger and standalone ArcSightLogger, version 6.4 (L8117) releases. 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 the Logger release.

Note: Where there are no specific differences, all types of Logger are called *Logger* in this document. Where there are differences, the specific type of Logger is indicated.

What's New in this Release

The HPE Security ArcSight Logger 6.4 release (L8117) introduces the following new features and enhancements.

Search Improvements

Improved Search capabilities and updated search interface enable users to do the following:

- Search for IPv6 data.
- Index the requestURL field.

  Caution: Consider the impact to storage when deciding whether to index this field. Refer to the Logger Administrator's guide for information on indexing this field.

- Run multiple searches in the same browser session.
- View and access searches from the Active Search list on the Search main page.
- Administrators can set the number of concurrent searches and the search expiry time value.

Reporting Improvements

The integration of new features provides a greatly improved reporting experience, including the following improvements:

- Open up to ten Report tabs, so you can move easily from screen to screen as you create, manage, and generate concurrent reports.
- Create Smart reports that can support multiple queries, offer new chart types, and create Smart dashboards.

- Create Smart dashboards that display the results of multiple queries on one dashboard, as well as rich text, slide show, and web page widgets.
- Create new report chart types, including Sunburst, Funnel, Pyramid, Tree maps, Counter, Gauge, and Packed circles.

Other Updates

- Updated Event Broker receiver adds support for Event Broker 2.0, including TLS Client Authentication.
- Logger can now send and receive data in CEF v0.1, v1.0 and raw data formats. CEF 1.0 enables Logger to send and receive IPv6 data.
- Incorporated FIPS Bouncy Castle libraries provide improved security and enables support for TLS 1.2.
- Updated localization for supported languages (Japanese, Traditional Chinese and Simplified Chinese).

For details about these features, see the ArcSight Logger 6.4 Administrator's Guide, available from the ArcSight Product Documentation Community on Protect 724.

For more information about this release, review the following sections:

- "Known Issues" on page 22.
- "Fixed Issues" on page 23.
- "Open Issues" on page 30.

Technical Requirements

Logger requires the following minimum system setup.

Specification	Details
CPU, Memory, and Disk Space for Enterprise Version of Software Logger	• 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 **Note:** Using a network file system (NFS) as primary event storage is not recommended.
CPU, Memory, and Disk Space for Trial Logger and VM Instances	• 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	• 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 7.3 configured with 12 GB RAM and four physical (and eight logical) cores. • HPE 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	• For optimal performance, make sure no other applications are running on the system on which you install Logger.

Supported Platforms

Refer to the ADP Support Matrix, available on the Protect 724 site for details on Logger 6.4 platform support.

Note: Be sure to upgrade your operating system (OS) to get the latest security updates. Upgrade your OS first, and then upgrade Logger. For Logger Appliances, an OS upgrade file is included in your upgrade package.

Connecting to the Logger User Interface

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 6.4 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.

Logger Documentation

The new documentation for this release comprises these Release Notes, and updated versions of the ArcSight Data Platform Support Matrix and ADP 2.1 Release Notes. The complete Logger 6.4 documentation set 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 6.4 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:* Provides integrated support information such as upgrade, platform, and browser support for Logger, ArcMC, and SmartConnectors. Available for download from the ArcSight Product Documentation Community on Protect 724.
- *Logger 6.4 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 6.4 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 6.4 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.

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 6.4 (L8117)

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

Note: Be sure to review the sections "Known Issues" on page 22, "Fixed Issues" on page 23, and "Open Issues" on page 30 before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.4. 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 6.4 Upgrade Paths	
Software Versions	6.3.1 (7874)
Appliance Models	L350X, L750X, L750X-SAN, L760X
Operating System Upgrades	• 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

Upgrading the Logger Appliance

This section describes how to upgrade the Logger appliance. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 6.4, available for download from the ArcSight Product Documentation Community on Protect 724.

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 6.3.1 prior to upgrading to Logger 6.4.
- Logger requires a root password. If your Logger does not have a root password already, give it one before performing the upgrade.
- Upgrade your OS to the latest RHEL distribution before you upgrade Logger. (Logger 6.4 includes OS Upgrade files for this purpose.)

  This is important even if you upgraded your OS when upgrading to Logger 6.3.1, because the latest OS distribution fixes additional security vulnerabilities.

  Tip: When upgrading through multiple releases, don't skip applying the OS upgrade files. You must apply each in turn when you upgrade to that version. Refer to the Support Matrix and Release Notes for the upgrade version for more information.

- Download the upgrade files from the HPE Customer Support site to a computer from which you connect to the Logger UI.
  - For local or remote appliance upgrades, download the following file: `logger-8117.enc`.
- For OS upgrades, download the appropriate file:
  - If you are upgrading an Lx500 series appliance, download the following file: `osupgrade-logger-rhel68-<timestamp>.enc`
  - If you are upgrading an Lx600 series appliance, download the following file: `osupgrade-logger-rhel73-<timestamp>.enc`
- Verify the upgrade files, as described in "Verifying Your Upgrade Files" on the previous page.
- Logger documentation is not included in your download package. Download your documentation from the ArcSight Product Documentation Community on Protect 724.

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the "Prerequisites" on the previous page before you begin.

- To upgrade Logger from ArcMC, see "To upgrade Logger Appliances remotely through ArcMC:" below
- To upgrade Logger locally, see "To upgrade a Logger Appliance locally:" below

To upgrade Logger Appliances remotely through ArcMC:

1. Upgrade your OS as appropriate.
   - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel68-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
   - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel73-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.

   Note: Be sure to apply the OS upgrade even if you already upgraded to the OS to 6.8 or 7.2 for Logger 6.3.1, because the latest OS distribution fixes additional security vulnerabilities.
2. Deploy the Logger upgrade by using the file `logger-8117.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Reboot the Logger for the upgrade to take effect.
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.

To upgrade a Logger Appliance locally:

1. Log into Logger and click System Admin | System > **License & Update**.
2. Upgrade your OS as appropriate.
   - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel68-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
   - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel73-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.

   Note: Be sure to apply the OS upgrade even if you already upgraded to the OS to 6.8 or 7.2 for

Logger 6.3.1, because the latest OS distribution fixes additional security vulnerabilities.

3. Browse to the `logger-8117.enc` file you downloaded previously and click **Upload Update.**

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

Upgrading Software Logger and Logger on a VMWare VM

This section describes how to upgrade Logger. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 6.4, available for download from the ArcSight Product Documentation Community on Protect 724.

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 6.3.1 prior to upgrading to Logger 6.4.
- Upgrade your Operating System (OS) to a supported version before upgrading Logger. This is important even if you upgraded your OS when upgrading to Logger 6.3.1, because the latest OS includes important security updates. 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.X, upgrade to the latest version of 7.3.
  - If your system is running on RHEL or CentOS 6.X, upgrade to the latest version of 6.8.
  - If not already done on the system, perform the following procedures:
    - Increase the user process limit on the Logger's OS. (You do not need to do this for Logger on VMWare VM, it is already done on the provided VM.) For more information, see "Increasing the User Process Limit" on the next page.
    - If you are on RHEL 7.X , modify the logind configuration file. For more information, see "Editing the logind Configuration File for RHEL 7.X" on page 17.
- A non-root user account must exist on the system on which you are installing Logger, or the installer will ask you to provide one. Even if you install as root, a non-root user account is still required. The userid and its primary groupid should be the same for this account. The UID for the non-root user should be 1500 and the GID should be 750. For example, to create the non-root user, run these commands as `root`:

  ```
  groupadd –g 750 arcsight
  useradd –m –g arcsight –u 1500 arcsight
  ```

  These commands create a non-root user named `arcsight` that will work with a Logger software installation.
- Download the Software Logger upgrade files from the HPE Customer Support site.

- For remote upgrades using ArcMC, download the following file:
  `logger-sw-8117-remote.enc`
- For local upgrades, download the following file:
  `ArcSight-logger-6.4.8117.0.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 11.

Increasing the User Process Limit

Before installing or upgrading Logger, you must increase default user process limit while logged in as user *root*. This ensures that the system has adequate processing capacity.

Note: This change is only necessary when installing Software Logger on your own Linux system. It has is already been done for Logger on VMWare VM.

To increase the default user process limit:

1. Open the file `/etc/security/limits.d/<NN>-nproc.conf`.
   (<NN> is 90 for RHEL or CentOS 6.8 and 20 for RHEL and CentOS 7.3.)
   - If you do not already have a `/etc/security/limits.d/<NN>-nproc.conf file,` create one (and the `limits.d` directory, if necessary).
   - If the file already exists, delete all entries in the file.
2. Add the following lines:

```
*    soft     nproc     10240
*    hard     nproc     10240
*    soft     nofile    65536
*    hard     nofile    65536
```

   Caution: Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system run time errors.

3. Reboot the machine.
4. Run the following command to verify the new settings:

```
ulimit -a
```

5. Verify that the output shows the following values for “open files” and “max user processes”:

```
open files                  65536
max user processes          10240
```

Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7.X, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the logind.conf file for RHEL 7.X:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the `RemoveIPC` line. `RemoveIPC` should be active and set to **no**.
   Remove the # if it is there, and change the `yes` to no if appropriate. The correct entry is:

   ```
   RemoveIPC=no
   ```
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect:

   ```
   systemctl restart systemd-logind.service
   ```

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the "Prerequisites" on page 15 before you begin.

- To upgrade Logger from ArcMC, see "To upgrade Software or VMWare Loggers remotely through ArcMC:" below.
- To upgrade Software Logger locally, see "To upgrade Software Logger locally:" on the next page.
- To upgrade Logger on VMWare locally, see "To upgrade Logger on VMWare VM:" on page 20.

To upgrade Software or VMWare Loggers remotely through ArcMC:

1. Upgrade your OS to the latest distribution. This is important even if you upgraded your OS when upgrading to Logger 6.3.1, because the latest OS distribution fixes additional security vulnerabilities.

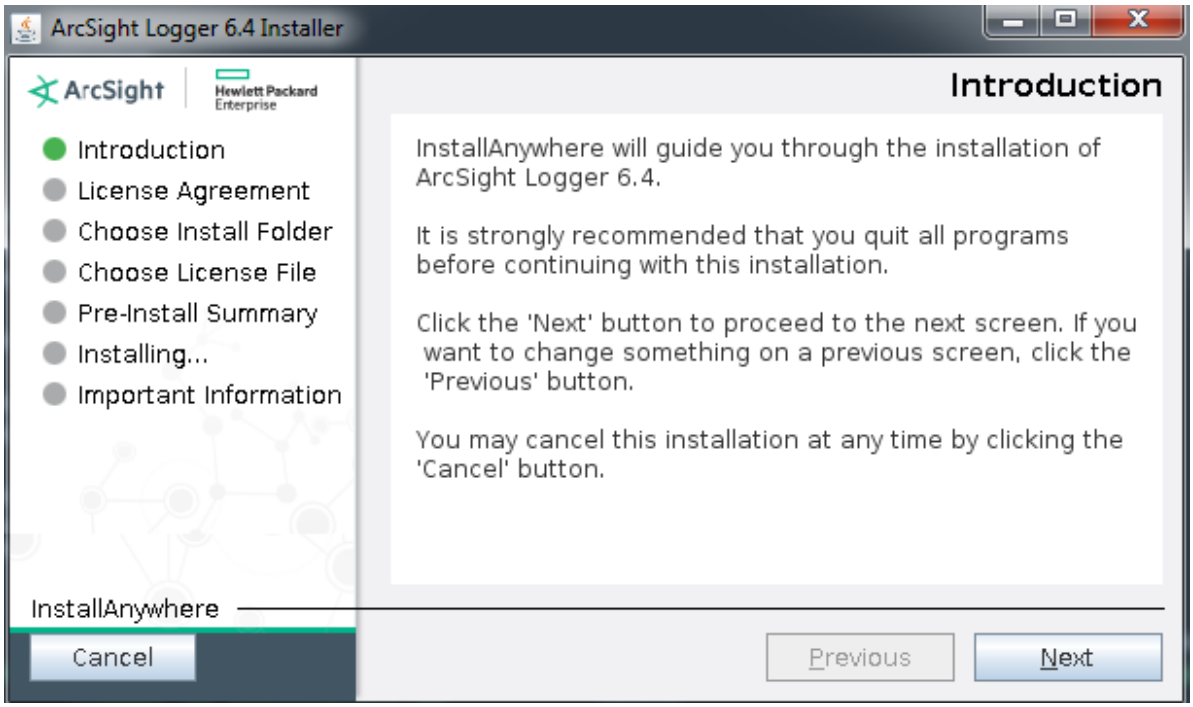
   Note: Remote OS upgrade is not supported for Software Logger. Perform the OS upgrade manually before upgrading Logger.
2. Deploy the downloaded upgrade file, `logger-sw-8117-remote.enc`, by following the instructions in the ArcSight Management Center Administrator's Guide.

To upgrade Software Logger locally:

1. Log in with the same user name as the one used to install the previous version of Logger.
2. Run these commands from the directory where you copied the Logger software:

   ```
   chmod u+x ArcSight-logger-6.4.8117.0.bin
   ./ArcSight-logger-6.4.8117.0.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.

3. 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.
4. Select **I accept the terms of the License Agreement** and click **Next**.
5. 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.
6. Once all Logger processes are stopped, the installer checks that installation prerequisites are met:
   - Operating system check—the installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing

Logger software. Press Click **Continue** to proceed with the upgrade or **Quit** to exit the installer and upgrade your OS.

Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before upgrading Logger. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

- Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

Once all the checks are complete, the Choose Install Folder screen is displayed.

7. Navigate to or specify the location where you want to install Logger.

   The default installation path is `/opt`. You can install into this location or another location of your choice.

   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.

8. Click **Next** to install into the selected location.
   - If there is not enough space to install the software at the location you specified, a message is displayed. To proceed with the installation, specify a different location or make sufficient space available at the location you specified. Click **Previous** to specify another location or **Quit** to exit the installer.
   - 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.

     Click **Upgrade** to continue or **Back** to specify another location.

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

   Installing Logger may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

10. Click **Next** to initialize Logger components.

    Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.

11. Click **Next** to upgrade Logger.

    Upgrading Logger may take a few minutes. Please wait. Once the upgrade is complete, the next screen displays the URL you should use to connect to Logger.

12. Make a note of the URL and then click **Done** to exit the installer.
13. Restart Logger to put the upgrade changes into effect.
14. You can now connect to the upgraded Logger.

15. 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. Log in with the same user name as the one used to install the previous version of Logger.
2. Run these commands from the `/opt/arcsight/installers` directory:

   ```
   chmod u+x ArcSight-logger-6.4.8117.0.bin
   ./ArcSight-logger-6.4.8117.0.bin -i console
   ```

   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
   6.4.

   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:
   ```

3. The next several screens display the end user 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. Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS. To continue, type 1 and press **Enter**. To quit so that you can upgrade your OS, type 2 and press **Enter**.

   Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before upgrading Logger. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.
6. The installer checks that installation prerequisites are met:

- Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software.
- Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

Example

If Logger is running on this machine, an Intervention Required message displays:

```
================================================================================

Intervention Required

--------------------

ArcSight Logger processes are active.

All ArcSight Logger processes must be stopped to allow installation to
proceed.

Type 'Quit' to exit this installer or 'Continue' to stop all ArcSight
Logger processes and continue with the installation.

->1- Continue

  2- Quit

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
```

In this case, you would enter 1 (or hit **Enter**) to stop Logger processes, or 2 to quit the installer.

Once all checks complete, the installation continues, and the Choose Install Folder screen is displayed.

7. 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.

8. Type Y and press **Enter** to confirm the installation location.
   - If there is not enough space to install the software at the location you specified, a message is displayed. Type `quit` and press **Enter** to exit the installer and reconfigure your VM.
   - 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. Type 2 and press **Enter** to continue with the upgrade.
9. 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.

10. Press **Enter** to initialize the Logger components.

    Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.

11. Press **Enter** to upgrade and restart Logger.

    The upgrade may take a few minutes. Please wait.

    Once the upgrade is complete, Logger starts up and the next screen displays the URL you should use to connect to Logger.

12. Make a note of the URL and then press **Enter** to exit the installer.
13. Restart Logger to put the upgrade changes into effect.
14. You can now connect to the upgraded Logger.
15. 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 issue applies 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.hpe.com/hpsc/doc/public/display?sp4ts.oid=4268690&docId=emr_na-c03265132

Fixed Issues

The following issues are fixed in this release.

Analyze/Search

Issue	Description
LOG-17465	It was taking 20 minutes to open the Configuration > Scheduled Searches/Alerts page. A bug triggered a new search for each Scheduled search or alert when opening the page. Fix: Opening the Scheduled Searches/Alerts page no longer triggers new searches, reducing the time it takes to load the page.
LOG-17440	If the first 30 characters of a report chart column heading or stacked column were the same, Logger would sometimes stack the data incorrectly. Fix: Logger now compares the entire column name, and data columns stack correctly.
LOG-17419	Previously, when you indexed a field, the correct field type color icon would not display until Logger restarted. Fix: The indexed field displays the correct color icon for an indexed field without restarting Logger.
LOG-16498	Previously, users were unable to run multiple searches in one browser session. Fix: Users can now run multiple simultaneous searches in the same browser session.
LOG-16348	When exporting search results with all fields included, custom fields are not exported. Fix: Custom fields are now exported correctly.

Issue	Description
LOG-14262	Some internal Logger events used incorrect field notation. Fix: The Logger internal events now use correct notation for the fields.
LOG-7864	The time in the agentReceiptTime fields was not in human-readable format when exported. Understanding: Logger records time field values in UNIX epoch format (long values). Fixed: Now the agentReceiptTime is exported in human-readable format.
LOG-5618	Searches on the requestURL field were very slow because that field could not be indexed. Fix: You can now index requestURL field. If you do this, searching on requestURL will be much faster. When indexed, the requestURLfield requires a lot of storage space. Be sure to account for the increased storage requirements in your planning.

Configuration

Issue	Description
LOG-18384	In Logger v.6.3, some users were unsure of where to upload the LDAP over SSL trusted certificate. Fix: A cross-reference was added to the 6.4 "LDAPS Authentication" documentation, referencing the "Uploading Trusted Certificates" topic.
LOG-17734	Data Volume calculations were not accurate in Logger 6.3. Consequently, the Configuration > Data Volume page displayed inaccurate data and the 5-day license violation feature lockout could be triggered erroneously. Fix: Data Volume calculations have been fixed. The Configuration > Data page now displays the accurate Data Volume information and the license violation feature now works as expected.
LOG-17049	Parser-created search event fields were not displaying in the search results. Fix: Parser-created fields now display as expected.

General

Issue	Description
LOG-17664	Logger did not have the option to remain permanently on Daylight Savings Time (DST), which customers in Turkey now require. Fix: Software Logger now provides an option to install an updated tzdata file during installation or upgrade, which resolves the issue. Users who do not need this fix can continue without the time zone upgrade. For Logger appliances, the upgrade automatically installs the 2016g timezone data if has not already been installed on the system.
LOG-15114	Logger could show ULAT instead of ULAST during Mongolia time zone Daylight Saving time. Fix: Logger updated to tzdata2016g in release 6.3.1, and to tzdata2016j in release 6.4 which resolved the problem. For Software Logger to get the full fix, update the Logger host OS tzdata rpm files prior to upgrading Logger.

Installation

Issue	Description
LOG-17470	The Logger 6.3 GUI installation wizard could stall during the "configuring" stage. Fix: Logger v6.4 installs correctly when using the GUI mode installer.
LOG-17436	The Logger documentation did not explain how to set the group ID and user ID when installing and upgrading Logger. Fix: This information was added to the Logger 6.4 Installation Guide and Release Notes.

Related Products

Issue	Description
LOG-18268	Some Active Loggers managed by ArcMC 2.5 failed to report their data consumption. Fix: This issue is not reproducible in this release.
LOG-17869	ArcMC Dashboard incorrectly reported Loggers in Warning state. Fix: ArcMC Dashboard will show Loggers in warning state only when one or more enabled receivers are in unhealthy state.

Reports

Issue	Description
LOG-17120	Non-ASCII characters in a report name were sometimes corrupted when customizing the report. The behavior occured only on Internet Explorer 11, and depends on the timing of user actions. Fix: Report's name do not show unreadable characters when title is changed.
LOG-16880	Logger reports published in iHTML format generated an empty file. Fix: iHTML reports showing data as expected.
LOG-16825	Users could not modify field values on-the-fly when creating reports. Fix: You are now able to modify search values on-the-fly while creating reports. For example, to modify the value of sourceServiceName field from COR to change to Core, follow these steps. 1. Open the report´s Query. Drag and drop a Formula Field step in the Transformation Area. - Select the Formula Field step. - Add a Formula Field. - Create the formula. (See example below.) - Link the steps correctly (Data Source -> Formula Fields -> Format). 2. Save the Query. 3. On the report, select the Formula Field instead of the arc_sourceServiceName field. 4. Save and run the report. Example Formula Field Formula: var temp = "COR"; FormulaField1 = arc_sourceServiceName; if (arc_sourceServiceName.toUpperCase().localeCompare(temp .toUpperCase()) == 0) {FormulaField1 = "Core";}
LOG-16824	Previously, Logger reports could not display charts from more than one query at a time. Fix: The 6.4 Logger Reporting upgrade features Smart Reports, which can display many queries in the same report or dashboard.
LOG-16597	When search results for the arc_destinationProcess name field are more than 30 characters long, Logger Reports may truncate the field. Fix: This update increases the size of the field arc_destinationProcess displayed in a Logger Report from 30 to 256 characters so all characters are displayed.

Issue	Description
LOG-15829	You could only display 50 values on the X-axis in Logger reports. This prevented you from being able to display hourly counts for a week. Fix: You can now display 168 values on X-axis (7*24) To display hourly counts for a week: 1. Select the Create New Report tab or customize the desired report. 2. Navigate to the Chart tab. 3. In the Sort Order section, select the desired field and set Show (N) values to "All". 4. Save the changes and run the report.
LOG-13750	In reports exported in PDF format, time was displayed in 12 hour format but the AM/PM was not included. Fix: AM/PM is now included in PDF reports.
LOG-13372	If you clicked on the graph at the top of the "Job Execution Status" page and then clicked "Last Run Status" table in the popup window, an error message appeared. Fix: Clicking on the graph now shows the status of the reports.
LOG-12392	You could not enable a user access published reports without also enabling them to write or edit report configuration such as queries, parameters, and scheduling. Fix: A user right called "View all published reports" enables you to provide a user with access to published reports and not the rest of the reporting tool.
LOG-12124	You could not see published reports without having to drill down into each specific report. Fix: You can now use the Report Explorer to search for published reports by name.
LOG-11535	The sourceServiceName and destinationServiceName fields were limited to 30 characters. Fix: The size of the sourceServiceName and destinationServiceName fields were increased from 30 to 1023.
LOG-7867	The start time and end time of the period during which a report ran could not be not shown in the report. Fix: Start time and end time are now shown in Ad-hoc Reports.
LOG-6264	You could not add a logo to Logger reports. Fix: You can select the report template from the Template Styles menu option, edit the layout to add an image of your choice, and position it.

System Admin

Issue	Description
LOG-18603	The RADIUS client library did not support RFC 2865. Fix: The RADIUS client library has been updated to support RFC 2865.
LOG-18586	On some L7600/C6600 appliances running RHEL 7.2, the OS was crashing or hanging. Fix: Applying the RHEL 7.3 OS upgrade file included with this release will upgrade the kernel to a more stable version and resolve this issue.
LOG-18413	After applying an OS upgrade on a Logger appliance, an error message about a missing tzdata rpm file would sometimes display on the Retrieve Logs page. Fix: When you apply an OS upgrade on a Logger appliance, it does not trigger the error message.
LOG-18375	In Logger 6.3, customized logos were not always rendering to a correct display size. Fix: Customized Logos can now be rendered to the correct display size for Logger. ArcSight suggests that you use the recommended logo size of 150 X 30 pixels.
LOG-16446	Previously, when a Logger that was receiving events was shut down, between 3-5% of events sent to it were dropped. Fix: Now, when Logger is shut down correctly, no events are lost. - To shut down Software Logger, use the loggerd stop or quit commands. For more information, refer to the Software Logger command line options section of the Logger Administrator's guide. - To shut down Logger Appliances, perform a Shutdown from the System Reboot UI. For more information refer to the System Reboot section of the Logger Administrator's guide.
LOG-16266	On L7600 Logger Appliances, the first time you visited the System Admin > Process Status page after a reboot, some processes could appear to be in "Execution failed" state. Fix: The UI displays the correct state of the processes on System Admin > Process Status page.

Upgrade

Issue	Description
LOG-18026	After applying an OS upgrade on a Logger appliance, log files did not rotate as expected. Fix: When you apply an OS upgrade on a Logger appliance, it does not interfere with log file rotation.
LOG-17827	Logger upgrades were resetting report configuration settings to their defaults. Fix: Report configuration settings are not affected by Logger upgrades.
LOG-17617	After upgrading to Logger 6.3, G8 appliances no longer responded to ICMP requests, such as ping requests. Fix: This is resolved by upgrading to Logger 6.3.1. After the upgrade, ICMP requests function as expected.

Open Issues

This release contains the following open issues.

Alerts/Filters

Issue	Description
LOG-7658	If a real-time alert and a saved search alert is created for the same event, the scheduled search alert may not trigger for several minutes after a real-time alert has triggered. Understanding: Because saved search alerts are scheduled, there is a delay due to the schedule set for the alert. In addition, if a saved search alert depends on internal events, which are flushed every 10 minutes, there might be an additional delay before the events are detected and the alert is triggered. Workaround: ArcSight recommends that you set the search time range to $now-X minutes or higher, where X is the time set in the Schedule field for a saved search alert to ensure that saved search alerts that depend on internal events will trigger as expected.

Analyze/Search

Issue	Description
LOG-18189	Searches can now expire while a user is still active on Logger. Understanding: Logger now supports concurrent searches in multiple tabs. Because all searches are held in memory, the default expiry time for searches is 10 minutes. Once the search completes, the search expiry time begins counting down. Workaround: A user with System Admin rights can set the search expiry time in the Configuration > Search Options page. You can increase the search expiry time to up to 60 minutes.
LOG-18048	Long IPv6 addresses may be partially hidden in the search results display. Workaround: Adjust the column width to see the full IPv6 address.
LOG-17806	In Internet Explorer or Firefox, after you run a search from the Live Event Viewer, searches that are loaded by clicking a dashboard from the Summary page may fail. Workaround: Use Chrome to log into Logger to use the Live Event Viewer, or to use Firefox or Internet Explorer, copy the query that failed from the search box, and then reopen the search screen and paste the query into the search box to run the search manually.
LOG-17318	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. 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. 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.
LOG-17215	When you perform a lookup search query including an IP data type field and top or chart operator, you may see an "unsupported data type" error. Workaround: None at this time.
LOG-17191	When searching using a lookup file, Logger generates parsing errors for IP data type fields. Workaround: None at this time.
LOG-16739	On rare occasions, indexing stopped completely, causing severe performance degradation for the Logger. Workaround: Improvements have been made to avoid indexing function failure in high EPS ingestion. Should this error still occur, restart the servers process to resume indexing.

Issue	Description
LOG-16429	When Source Types sharing a common dependent parser are exported with the property "overwrite.same.content" turned on, importing such source types will only keep the most recently imported one having its parser: the other source types won't have their parser included in their definition. Workaround: Turn off "overwrite same content" before importing.
LOG-16347	Pipeline queries that include the WHERE operator, and exclude the '*user' field from a custom field list, display no results for the custom fields. For example, this query (missing the '*user' field from the custom field list): _deviceGroup IN ["192.164.16.202 [SmartMessage Receiver]"])) | where deviceEventClassId = "agent:050" Does not return the value 'agent:050' in the deviceEventClassId field of the search results. Workaround: Include the '*user' field from the custom field list in the query.
LOG-15972	If you run a forensic search using an Event Archive that has been partially archived from local storage, the archive may not load. Examples include searching for events prior to a certain time on the first day of the month, or if local memory already contains events from that archive for that date. Workaround: Query around the affected time range, or reduce storage group retention to remove previously restored archived events from that date in local storage.
LOG-15091	The insubnet operator is not supported in the Advanced Search query editor. Workaround: To add a condition with insubnet operator, enter the search manually.
LOG-15079	Loading a Saved Search or Filter by using the Folder icon (Load a Saved Filter) fails if the query includes the insubnet operator. Workaround: In the text box, type SS<SavedSearchName> or $filter$<FilterName> and then click Saved Search or Filter in the dropdown list to load it.
LOG-14625	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. Workaround: Reduce your "Top" search queries to ten fields or less, or contact HPE ArcSight Technical Support for a more detailed workaround.
LOG-14266	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". Workaround: Use either of the following two queries to find the event: 1) message CONTAINS "Daily archive task settings updated" or 2) message STARTSWITH "Daily archive task settings updated"
LOG-13532	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. 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.

Issue	Description
LOG-12524	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 (\). 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".
LOG-12290	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. 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. Workaround: Since this issue is caused by the fields included in the fieldset used for the search, remove any renamed fields from the fieldset.
LOG-12030	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. Workaround: To export search results without the All Fields requirement, add another field, to export all of the corresponding events correctly.
LOG-11299	If you uncheck the Rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail. Workaround: The Rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.
LOG-11225	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. 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 ",.
LOG-11066	If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues: 1) On the Search page, the Events grid in the search results will be empty for any search, 2) GMT displays in timestamps with timezones, 3) In the Global Summary on the Summary page, the Indexing is reported one hour behind the current time stamp. Workaround: Change the system time zone to something more specific, such as /America/Los_ Angeles.

Issue	Description
LOG-10126	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": | replace "*john*" with "*johnny" Workaround: None available at this time.
LOG-9420	When using the search term "transaction" on data that was received out of order, the duration may appear to be negative. Workaround: Include the term "sort _eventTime" before the transaction term.
LOG-9025	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. Workaround: Use an external browser to see results.
LOG-6965	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: - 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. Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.
LOG-5181	Search results are not highlighted when there are multiple values that match the IN operator in a query. 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.

Configuration

Issue	Description
LOG-18753	Logger supports connecting to only one Event Broker cluster when client authentication is enabled. Logger can connect to any number of Event Broker clusters without client authentication. Workaround: If you need to connect to another cluster with client authentication, you need to clear the keystore before configuring. This can be done with the commands: # list the keypairs by alias <install_dir>/current/local/jre/bin/keytool -list -keystore <install_ dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar | grep -i private # delete the keypair with the alias from the previous command <install_dir>/current/local/jre/bin/keytool -delete -keystore <install_ dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar -J-Djava.security.egd=file:/dev/urandom -alias <alias(es) from previous command>
LOG-18749	Logger 6.4 Administrator's guide does not include the correct list of possible peers. Workaround: Logger 6.4 can peer with Logger 6.4, Logger 6.3.1 and earlier versions of Logger, with the exception of Logger 6.3. Additionally, Logger 6.4 can peer with ESM versions 6.9.1 and 6.11. This information will be updated in in an upcoming release of the Logger Administrator's guide.
LOG-17828	If you create a realtime alert, and later, you try to create a Logger Forwarder with the same name as the alert, you will get an error message. Workaround: Give Forwarders a unique name.
LOG-17433	When you delete a Logger TCP or UDP receiver, the port on which the receiver was listening will remain open in the firewall. Workaround: None at this time.
LOG-16379	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. Workaround: Option 1: Push the config again to the destination Logger. Option 2: Manually add the SNMP destination on the target logger.
LOG-16349	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. Workaround: Before attempting to create a query or report, navigate to the Reports dashboard to provision the Report objects.

Issue	Description
LOG-16024	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. Workaround: None available at this time.
LOG-15530	Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail. 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.
LOG-14778	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. Workaround: Create a Receiver with different name and drill-down the events on the Summary page using the Device Group containing the new Receiver.
LOG-14650	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. Workaround: None available at this time.
LOG-13834	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". Workaround: Specify the Logger Appliance time zone by location. For example, set the time zone as "Taipei" or "Los Angeles."
LOG-13226	A user can edit a forwarder while the forwarded is enabled. This can cause the forwarder to stop sending events. Workaround: Before editing the forwarder, disable it. Then edit it and re-enable it to have the forwarder send events to its target destination.
LOG-11473	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 cause the setup program to fail. Workaround: Enter valid values for all required Setup Wizard fields.
LOG-11290	When you delete a Receiver, the Receiver's numeric ID still displays in the Summary page, although it is correctly deleted from the Dashboards. Workaround: Restart the Logger.
LOG-11176	When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references. 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.

Issue	Description
LOG-10056	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. Workaround: Do not create a receiver with a name you have used for a deleted receiver.
LOG-8790	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. Workaround: Avoid using non-ASCII characters in the community string.
LOG-8194	After restoring Logger from a backup configuration, the CIFS share cannot be mounted because the user name and password fields are empty. Workaround: Edit the setting of the CIFS share and re-enter your username and password.
LOG-6786	Events may be missed when a receiver on Logger is disabled. Workaround: None at this time.
LOG-5024	If the system that Logger backs up its configuration to is reinstalled or its SSH hosts key is changed, the Configuration Backup fails because the SSH hosts key cannot be refreshed from the Logger UI. Workaround: Log in to the Command Line Interface and delete the entry in the /home/arcsight/.ssh/known_hosts file. Then refresh the Configuration Backup configuration.
LOG-4986	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). 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.
LOG-2941	The type associated with imported filters cannot be changed from shared to saved search. Workaround: Imported filter types cannot be changed. However, you can copy the filter definition and create a new filter out of it.
LOG-370	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. 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.

Dashboards

Issue	Description
LOG-17393	When creating a new dashboard, Logger might show the validation error "Dashboard name already exists," even though the user does not have a dashboard with that name. Workaround: Give the dashboard a different name.
LOG-16998	The system filters "Root Partition Below 10 Percent" and "Root Partition Below 5 Percent" are missing a space in the default query, which can result in incorrect search results. Workaround: Add the missing space before running the query. For example, for this query: cn1=([0-9]|0[0-9]).* Add a space between the closed parenthesis and the period (cn1=([0-9]|0[0-9]) .*) to generate correct results.

General

Issue	Description
LOG-18489	The Mongolia time zone update in tzdata2017a is not included in Logger 6.4. Logger 6.4 only supports up to tzdata2016j. The tzdata2017a update will be supported in a future release. Workaround: None at this time.

Localization

Issue	Description
LOG-15905	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. Workaround: Use openSSH for configuration backups.

Related Products

Issue	Description
LOG-17842	On rare occasions, the event flow between a Logger and a Smart Message Connector stops when the Logger Connector configuration is set to "Logger pool destination." Workaround: The event flow can be restored by restarting the Logger Apache process. The root cause of the issue is being investigated as a connector defect.

Reports

Issue	Description
LOG-18686	Some tasks and menu descriptions for the Smart designer and Ad hoc Powerviewer were not included the 6.4 release of the Logger Administrator's Guide. Workaround: Much of the configuration information is available from the Classic reports and dashboards sections. Additional topics will be available in an upcoming release.
LOG-16589	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. Workaround: Check all scheduled reports and assign peers after any changes made to the peer configuration.
LOG-16405	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." Workaround: None at this time.
LOG-16281	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. Workaround: None available at this time.
LOG-15462	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. Workaround: Check the amount of free space periodically.

Issue	Description
LOG-15056	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. 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. 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.
LOG-14386	If you open the Reports Dashboard in an Internet Explorer 11 window that is less than 1450px wide, the Reports menu is not displayed. Workaround: When working with Internet Explorer 11, always make your window wider than 1450px.
LOG-13373	Report "Execution Status" doesn't list the most recent Jobs by default. Workaround: Navigate to the first page manually by clicking on the appropriate icon.
LOG-11659	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. Workaround: If you are installing the SOX v4.0 solution package on Software Logger as the root user, install it last.
LOG-11137	If a user has privileges to View a Published Report Only, then the report will not be visible in the Report Explorer. 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.)
LOG-10923	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. Workaround: Use hard-coded SQL parameters to generate results over 100,000 lines.
LOG-10098	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. Workaround: None available at this time.
LOG-9860	When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it was copied. 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.
LOG-9620	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. Workaround: None available at this time.

Issue	Description
LOG-8901	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. 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.
LOG-8780	Reports generated using the Web Services API do not contain report titles. 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.
LOG-7186	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. 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. 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. 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." 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.
LOG-2012	Adding a scheduled report can reset the scan limit field of other reports. Workaround: Check that the scan limit is set as desired before running any report.

Summary

Issue	Description
LOG-9772	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. Understanding: The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different. Workaround: None available at this time. Currently, there is no way to specify the search time range in milliseconds.

System Admin

Issue	Description
LOG-18388	SNMP polling for power supply, fan and temperature parameters is not supported on ArcSight appliances. Workaround: 1. Install the following two RPM files on your ArcSight appliance: - hp-health-10.40-1777.17.rhel7.x86_64.rpm - hp-snmp-agents-10.40-2847.17.rhel7.x86_64.rpm 2. Download the following MIB files and copy them to the /usr/share/snmp/mibs folder on your ArcSight appliance: - cpqhlth.mib - cpqhost.mib - cpqsinfo.mib 3. Import the MIB files into the network management system. Download links: For HPE Health and HPE SNMP Agent RPMs: http://downloads.linux.hpe.com/SDR/repo/spp/RedHat/7/x86_64/current/ For Proliant MIB kit: http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04272529
LOG-17072	If you apply a Standalone Logger license on a Logger with an installed ADP license, or conversely, if you apply an ADP Logger license on a Logger with an installed standalone license, Logger won't work as expected. Workaround: Call Support for assistance in applying the proper license.

Issue	Description
LOG-16759	SNMP polling for power supply, fan and temperature parameters is not supported on HPE Proliant appliances. Workaround: 1. Install the following two RPM files on your ArcSight appliance: - hp-health-10.40-1777.17.rhel7.x86_64.rpm - hp-snmp-agents-10.40-2847.17.rhel7.x86_64.rpm 2. Download the following MIB files and copy them to the /usr/share/snmp/mibs folder on your ArcSight appliance: - cpqhlth.mib - cpqhost.mib - cpqsinfo.mib 3. Import the MIB files into the network management system. Download links: For HPE Health and HPE SNMP Agent RPMs: http://downloads.linux.hpe.com/SDR/repo/spp/RedHat/7/x86_64/current/ For Proliant MIB kit: http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04272529
LOG-16757	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. Workaround: To disable this feature and avoid the issue, open System Admin > Users/Groups > Authentication. On the Sessions tab, remove the check from the Disable Inactive Account After checkbox.
LOG-15490	In rare circumstances during a data migration to an L7600 appliance, some processes will not restart on the target machine after the reboot. Workaround: Use SSH to restart all processes manually using this command: /opt/local/monit/bin/monit restart all

Issue	Description
LOG-15456	The Apache process fails to start if "Client Certificate" or "Client Certificate AND User Password" has been enabled before Trusted Certificates are uploaded. 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.
LOG-14595	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. 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.
LOG-11700	Users may be unable to log in after they have been removed from a group. 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. Workaround: To avoid disabling a user account when removing the user from a group, check that the user is assigned to the correct groups.

Upgrade

Issue	Description
LOG-18017	When performing an OS upgrade on an appliance, the oldest kernel version is deleted in order to conserve space on the root partition, but the old version still shows as an option in the GRUB menu. Workaround: Select the latest version and ignore the option to select the obsolete kernel.
LOG-17404	For non-root Loggers that are running as a service, if the OS is upgraded to RHEL 7.2 after Logger is upgraded, the Receivers process will fail to start. Workaround: Log in as root and run the command '/sbin/ldconfig' before starting Logger.
LOG-17065	In some cases, the SmartMessage Receiver has significantly lower incoming EPS after an upgrade. This causes connectors to cache heavily. Workaround: Restart Apache process using 'loggerd restart apache' command.
LOG-16711	On Logger L7600 series appliances, the user interface may not refresh when the upgrade is finished. 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.

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 6.4)

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!