

Release Notes

ArcSight Logger 6.0

October 24, 2014



Copyright © 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP 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.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
10/24/14	Logger 6.0	Added information about upgrade support on Lx200 models.
09/19/14	Logger 6.0	6.0 release.
04/24/14	Logger 5.5 Patch 1	Patch 1 for 5.5.
03/19/14	Logger 5.5	5.5 release.
05/30/13	Logger 5.3 SP1	Adding new appliance platforms and Logger for VMware.
03/08/13	Logger 5.3 SP1	5.3 SP1 release.
09/27/12	Logger 5.3	5.3 GA.
01/2012	Logger 5.2 Patch 1	Patch 1 for 5.2.
12/11/11	Logger 5.2 GA	5.2 GA.
06/15/11	Logger 5.1 GA	Added a bug to the Open Issues section.
06/08/11	Logger 5.1 GA	Added the section "Information You Should Know".
05/31/11	Logger 5.1 GA	5.1 GA.
11/12/10	Logger 5.0 Patch 2	Patch 2 for 5.0.
10/12/10	Logger 5.0 Patch 1	Patch 1 for 5.0.

Contents

- ArcSight Logger 6.0 5**
 - What's New in Logger 6.0 5
 - Managing Logger through ArcMC 6
 - Supported Platforms 7
 - Supported Browsers 8
 - Localization Information 9
 - Logger Documentation 9
 - Known Limitations 10
 - Upgrade Paths 11
 - Upgrading to Logger 6.0 (L7285) 12
 - Known Issues 17
 - Issues Fixed in this Release 18
 - Open Issues in this Release 23

ArcSight Logger 6.0

These release notes provide information about the ArcSight Logger 6.0 (L7285) 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.

If you have an L3XXX model Logger (an integrated Logger and Connector Appliance), refer to the Connector Appliance 6.4 documentation for additional information about the Connector Appliance functionality.

This document covers the following topics:

- ["What's New in Logger 6.0" on page 5](#)
- ["Managing Logger through ArcMC" on page 6](#)
- ["Supported Platforms" on page 7](#)
- ["Supported Browsers" on page 8](#)
- ["Localization Information" on page 9](#)
- ["Known Limitations" on page 10](#)
- ["Logger Documentation" on page 9](#)
- ["Upgrade Paths" on page 11](#)
- ["Upgrading to Logger 6.0 \(L7285\)" on page 12](#)
- ["Known Issues" on page 17](#)
- ["Issues Fixed in this Release" on page 18](#)
- ["Open Issues in this Release" on page 23](#)

What's New in Logger 6.0

This section lists the new features and enhancements introduced in the Logger 6.0 release (L7285). For details of these features, see the ArcSight Logger 6.0 Administrator's Guide, available from the Protect 724 community at <https://protect724.hp.com>.

The following new features and enhancements are included in this release.

- Improved User Interface (UI), including:
 - ◆ New Take me to... search box for menu navigation.
 - ◆ Improved menu structure.
 - ◆ Updated digital gauges.
 - ◆ New ability to add a customized logo.
- Improved scalability, including:
 - ◆ Doubled local storage size. Each instance can support up to 8TB.

Logger storage is the lesser of the available space (in bytes) for the data directory or the value set in the license (which is 8 TB in Logger 6.0). The following table lists the approximate available storage for the Lx500 series Loggers.

Model	Available Storage* (Compressed Data)
L7500	7.8 TB
L3500	800 GB

* The meta data for indexes generated on Logger are stored in the same storage space, and consume less than 10% of the total size of the event data.

- ◆ Increased speed of data indexing.
- Improved performance, including:
 - ◆ Faster UI response times.
 - ◆ Reduction in the size of the metadata generated. This decreases both the time it takes to retrieve the metadata and the amount of storage space the metadata requires. This improves archive search speed.
- New and improved data analytics, including:
 - ◆ New lookup operator enables you to augment data in Logger with data from an external file. This enables geo-tagging, asset tagging, user identification, and so on, through static correlation.
 - ◆ New and improved version of the reporting engine.
- Faster searches in peered deployments, including:
 - ◆ Scalable distributed searches across up to 20 peers. Search speeds increase linearly with the number of peers searched.
 - ◆ Performance enhancement to distributed searches for non-pipeline searches. To realize these enhancements, all peers must be on Logger 6.0 or later, and the query must not include the regex, rex, parse, keys, transaction, extract, or lookup operators.
- Improved Data Access, including:
 - ◆ New RESTful Login and Search APIs.
 - ◆ API support for including peers in searches.
- New content, including:
 - ◆ New dashboards and fieldsets for security use-cases.
 - ◆ Added ability to import and export fieldsets.
- Other enhancements, including:
 - ◆ New hash validation of stored data.
 - ◆ Removal of the challenge response for SSH access to the Logger appliance.

In addition, this release introduced fixes for a number of bugs. See ["Issues Fixed in this Release" on page 18](#) for details.

Managing Logger through ArcMC

Logger 6.0 supports management through ArcMC 2.0. However, a new ArcMC Agent is required to manage it. In order to manage Logger 6.0 through ArcMC, you must install the ArcMC Agent on Logger. If you are managing Logger through ArcMC already, you must

install the newest version of the ArcMC Agent before performing any management operations on Logger from ArcMC.

Follow these steps to manage a fresh installation of Logger 6.0 through ArcMC 2.0:

- 1 Download the latest ArcMC Agent (ArcSight-ArcMCAGENT-2.0.0.1167.1 or later) and its accompanying ReadMe from the HP Customer Support site (SSO) at <http://support.openview.hp.com>.
- 2 Upload the new ArcMC Agent to ArcMC by following the instructions in the ReadMe that comes with the ArcMC Agent.
- 3 Install Logger 6.0 by following the instructions in the Logger Installation Guide.
- 4 Add the Logger as a host by following the instructions in the ArcMC 2.0 Administrator's Guide.



Note

If you are already managing Logger version 5.5 through ArcMC, and you want to upgrade to Logger 6.0, you must install the newest version of the ArcMC Agent on Logger before you upgrade it to version 6.0. See the steps below.

Follow these steps to install the new ArcMC Agent when upgrading to Logger 6.0:

- 1 Upgrade to ArcMC 2.0 if you are not already at that level.
- 2 Download the latest ArcMC Agent (ArcSight-ArcMCAGENT-2.0.0.1167.1 or later) and its accompanying ReadMe from the HP Customer Support site (SSO) at <http://support.openview.hp.com>.
- 3 Upload the new Agent to ArcMC by following the instructions in the ReadMe that comes with the ArcMC Agent.
- 4 Install the ArcMC Agent on Logger by following the instructions in the ReadMe that comes with the ArcMC Agent.
 - ◆ For Logger appliances, update the ArcMC Agent onto the remote Logger from ArcMC, by following the instructions in the ArcMC 2.0 Administrator's Guide.
 - ◆ For Software Loggers, install the ArcMC Agent on Logger by following the instructions in the ReadMe that comes with the ArcMC Agent.
- 5 Upgrade Logger to version 6.0 by following the instructions in ["Upgrading to Logger 6.0 \(L7285\)" on page 12](#).

Supported Platforms

You can install the Logger software on platforms with the hardware specifications and supported operating systems outlined below, according to the indicated deployment scenarios. This information applies to both physical and virtual machines.

You can deploy Logger for VMware VM on a VMware ESXi server. The VM image includes the Logger installer on a 64-bit CentOS 6.5 system configured with 12 GB RAM and four physical (and eight logical) cores. VM installation on the operating systems listed in the table below is supported.



Note

- HP strongly recommends allocating 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.

Specification	Details
Supported Operating Systems	<ul style="list-style-type: none"> Red Hat Enterprise Linux (RHEL) versions 6.2 and 6.5 (64-bit) CentOS versions 5.5 and 6.5 (64-bit) <p>Notes:</p> <ul style="list-style-type: none"> HP ArcSight recommends RHEL 6.5 for fresh installs. If you are planning to upgrade your current OS and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first, and then the OS. For example, upgrade from Logger 5.3 SP1 to Logger 5.5 and then upgrade from RHEL 6.2 to RHEL 6.5.
CPU, Memory, and Disk Space	<p>For the Enterprise Version of Software Logger:</p> <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: 400 GB Temp directory: 1 GB <p>Note: Using NFS as primary event storage is not recommended.</p>
CPU, Memory, and Disk Space	<p>For the Trial Logger and VM Instances:</p> <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 <p>Note: Using NFS as primary event storage is not recommended.</p>
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install Logger.

For a detailed capacity planning guide, see the Capacity Planning for Software Version of Logger document that is available for download from the Protect 724 Community at <https://protect724.hp.com>.

Supported Browsers

The Logger user interface (UI) is a password-protected web browser application using Secure Sockets Layer (SSL) encryption.

Logger 6.0 supports access through the following browsers:

- **Firefox:** Version ESR 31
- **Internet Explorer:** Versions 10 and 11
- **Chrome:** Latest version
- **Safari:** version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at <http://www.adobe.com/products/flashplayer.html>

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

- For root installs, access to the port 443 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.
- For non-root installs, access to port 9000 must be allowed, plus the ports for any protocol that the Logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.



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

JavaScript and cookies must be enabled.

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.

If you are upgrading a pre-5.1 Logger, you must set the locale when upgrading to Logger 5.1. The locale can be changed at this point. If you are upgrading from Logger 5.1 or later, the locale is already set and cannot be changed.

Logger Documentation

New documentation for this release includes these Release Notes and the Logger Installation Guide. The following documentation is available:

Logger Administrator's Guide: Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>. This information is also accessible from the integrated online Help.

Logger Online Help: 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. This information is also accessible from the Logger Administrator's Guide and Web Services API Guide.

Logger Web Services API Guide: Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>. This information is also accessible from the integrated online Help.

Logger Getting Started Guide: Applicable for new Logger Appliances. Provides information about connecting the Logger Appliance to your network for the first time and accessing it through a web browser. A printed copy of this guide is packaged with the Logger Appliance. Also available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Logger Installation Guide: Applicable for initializing the Logger Appliance and installing the Software Logger on Linux or VMware VM. Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Trial Logger Quick Start Guide: Applicable for installing the Trial Logger and Trial Logger for VMware VM. Provides a high-level understanding of Logger and helps you install it. Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Known Limitations

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

- A Logger running on L3XXX model does not support the integrated Connector Appliance functionality in the localized language.
- Only ASCII characters are acceptable for full-text search and the Regex Helper tool. Therefore, full-text search is not supported for Japanese or Chinese characters.
- A Logger user cannot have a login name that contains native characters. That is, the Login field on the Add User page does not accept 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 (To open the Certificates page, type Certificates in the **Take me to...** search box, and click Certificates in the dropdown list..) cannot contain native characters. Use only ASCII characters in the Certificate Alias field.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.0.

Logger Appliance	
Most common upgrade path	4.5 GA (L4892) -> 5.0 Patch 2 (L5355) -> 5.1 GA (L5887) -> 5.2 Patch 1 (L6307) -> 5.3 GA (L6684) -> 5.3 SP1 (L6838) -> 5.5 (L7049) -> 5.5 Patch 1 (L7067) -> Logger 6.0 (L7285)
Other upgrade paths	<ul style="list-style-type: none"> 5.0 Patch 1 (L5215) -> 5.0 Patch 2 (L5355) -> Follow the upgrade path as described in the "Most common upgrade path" 5.0 Patch 3 (L5414) -> 5.1 GA -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 Hotfix (L6295) -> 5.2 Patch 1 (L6307) -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 GA (L6288) -> 5.3 GA (L6684) -> Follow the upgrade path as described in the "Most common upgrade path" 5.3 SP1 -> 5.3 SP1 Hotfix (L6841), 5.3 SP1 Hotfix (L6849), or 5.3 SP1 Hotfix 12232 (which does not update the build number) -> Follow the upgrade path as described in the "Most common upgrade path" 5.3 SP1 (L6838) -> 5.5 Patch 1 (L7067) -> Logger 6.0 (L7285) 5.5 (L7049) -> Logger 6.0 (L7285)
Notes	<ul style="list-style-type: none"> The Lx200 models cannot be upgraded to Logger 6.0. The following Logger Appliance release was an interim version that you should not upgrade to any longer: 5.0 Patch 1 (L5215). Instead, upgrade to the closest release version listed in the Most Common Upgrade Paths. Logger 5.0 Patch 3 release is only available on some Logger Appliances shipping from HP. Logger 5.5 upgrade is not supported for non-SAN Logger Appliances purchased prior to July 11, 2011 that were originally running versions earlier than Logger 5.1. Instead, upgrade such appliances directly to Logger 5.5 Patch 1.
Software Logger	
Most common upgrade path	5.0 GA (L5139) -> 5.0 Patch 2 (L5355) -> 5.1 GA (L5887) -> 5.2 Patch 1 (L6307) -> 5.3 GA (L6684) -> 5.3 SP1 (L6838) -> 5.5 (L7049) -> 5.5 Patch 1 (L7067) -> Logger 6.0 (L7285)
Other upgrade paths	<ul style="list-style-type: none"> 5.0 Patch 1 (L5215) -> 5.0 Patch 2 (L5355) -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 Hotfix (L6295) -> 5.2 Patch 1 (L6307) -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 GA (L6288) -> 5.3 GA (L6684) -> Follow the upgrade path as described in the "Most common upgrade path" 5.3 SP1 -> 5.3 SP1 Hotfix (L6847) or 5.3 SP1 Hotfix 11854 (which does not update the build number) -> Follow the upgrade path as described in the "Most common upgrade path" 5.3 SP1 (L6838) -> 5.5 Patch 1 (L7067) -> Logger 6.0 (L7285) 5.5 (L7049) -> Logger 6.0 (L7285)
Note	You cannot upgrade the 4.5 GA installation of Software Logger.

Upgrading to Logger 6.0 (L7285)

This section includes upgrade information for the Logger Appliance and Software Logger.

- [“Verifying Your Upgrade Files” on page 12](#)
- [“Logger Appliance” on page 12](#)
- [“Software Logger” on page 14](#)



Be sure to review the [“Known Issues” on page 17](#), [“Issues Fixed in this Release” on page 18](#), and [“Open Issues in this Release” on page 23](#), before upgrading your Logger.

Verifying Your Upgrade Files

HP provides code signing to enable you to verify that the software you receive is indeed from HP and has not been manipulated in any way by a third party. To do this, the software has been signed with a digital private key only held by HP.

Access the following link to download HP's public certificate:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

The site also provides the step by step instructions for how to import HP's public certificate and verify the signature file.

Logger Appliance

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Refer to [“Upgrade Paths” on page 11](#) for supported upgrade paths and appliance models.
- Back up your configuration before and after upgrading to this release. For instructions on backing up your Logger configuration, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- Download the `logger-7285.enc` file from the HP Customer Support site at <http://support.openview.hp.com/downloads.jsp> to a computer from which you connect to the Logger UI.
- Verify that you have the correct upgrade file, as described in [“Verifying Your Upgrade Files” on page 12](#).
- If you plan to manage Logger through ArcMC, follow the steps described in [“Managing Logger through ArcMC” on page 6](#) before upgrading Logger.

Upgrade Instructions

To upgrade your Logger Appliance:

- 1 Log into Logger and click **System Admin | System > License & Update**.
- 2 Browse to the `logger-7285.enc` file you downloaded in the previously and click **Upload Update**. The ArcSight Appliance Update page displays the update progress.

Once the upgrade is complete, Logger reboots automatically.

- 3 To use the new schema introduced with the release, run a defrag. For instructions, refer to the Logger Administrator's guide.



If you encounter a page that asks to upload a license and set the time zone at this stage, contact HP Support for assistance.

Note

Multi-Pathing Considerations for SAN Logger Upgrades

SAN Multipath support was enabled in Logger 5.1. This functionality is configured at the time of Logger initialization before attaching the LUN to the Logger. However, if you are an existing Logger SAN customer, upgrading from Logger 5.1 or an earlier release, and want to enable this functionality on your existing single-path LUN, follow the instructions in this section to convert the LUN. Once you have converted to a multipath LUN, you cannot revert the changes. If the multipath conversion does not succeed or another circumstance requires you to revert to single path, contact HP Support for assistance.

To convert a single path LUN to multipath:

- 1 Upgrade your Logger Appliance to version 5.1 or later.
- 2 After a successful upgrade, connect to your Logger using SSH, as described in the ArcSight Logger 6.0 Administrator's Guide.

- 3 Run these commands:

```
cd /opt/arcsight/aps/mpath
./mpath_prepare.sh
```

- 4 Connect the second fiber cable to the second port on the HBA card.
- 5 Create the `multipath.conf` file for your SAN.

The contents of this file will vary depending on your SAN vendor and configuration. The Logger user interface includes a default multipath configuration for EMC Clariion SANs that can be used as a starting point to populate the `multipath.conf` file. However, consult your SAN documentation for information specific to your setup and environment.

To view the default multipath configuration for EMC Clariion SAN, connect to the Logger UI, go to System Admin > Multipath, copy the configuration from the UI, and then paste the copied configuration in the `/opt/arcsight/aps/mpath/multipath.conf` file.

- 6 Run this command:

```
./mpath_test.sh <path_to_your_multipath.conf>
```

Review the output of the test command to ensure that multipath devices that will be created are listed at the bottom of the output.

- 7 If test output is not correct, repeat [Step 5](#) and [Step 6](#) until the multipath devices are correctly listed.
 - 8 Run this command:
- ```
./mpath_enable.sh <path_to_your_multipath.conf>
```
- 9 Reboot your appliance.

## Software Logger

Refer to the [“Upgrade Paths” on page 11](#) section for the supported upgrade paths for your Logger.



Note

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

## Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Refer to [“Upgrade Paths” on page 11](#) for supported upgrade paths.
- Back up your configuration before and after upgrading to this release. For instructions on backing up your Logger configuration, refer to the Logger Administrator’s Guide for the Logger version you are currently running.
- If you are planning to upgrade your current operating system (OS) and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first followed by the OS.
- Increase the user process limit on the Logger’s OS as described in [“Increasing the User Process Limit” on page 14](#).
- If you plan to manage Logger through ArcMC, follow the steps described in [“Managing Logger through ArcMC” on page 6](#) before upgrading Logger.
- Download the Software Logger upgrade file from the HP Customer Support site at <http://support.openview.hp.com/downloads.jsp>.
- Verify that you have the correct upgrade file, as described in [“Verifying Your Upgrade Files” on page 12](#).

## 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.

### To increase the default user process limit:

- 1 If you do not already have a file `/etc/security/limits.d/90-nproc.conf`, 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 runtime 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

After you increase the user process limit, you will be able to upgrade Logger.

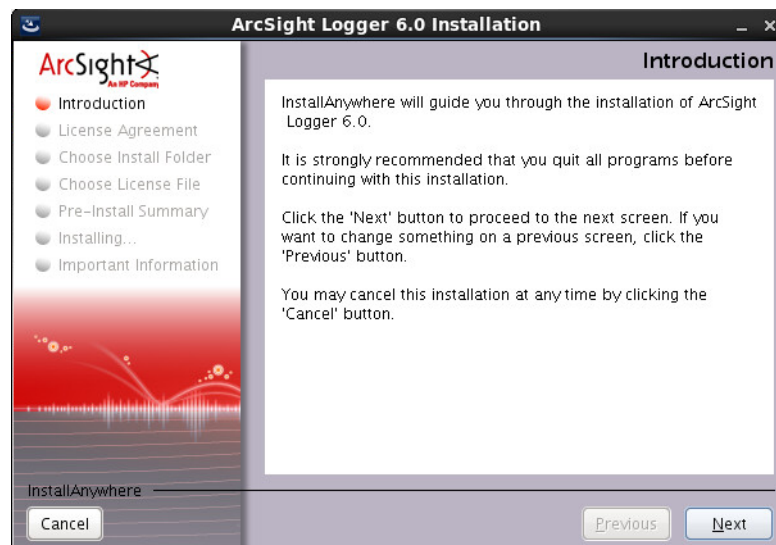
## Upgrade Instructions

Before upgrading Logger, be sure that you have met the prerequisites listed in ["Prerequisites" on page 14](#).

### To upgrade your Software Logger:

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

```
chmod +x ArcSight-logger-6.0.0.7285.0.bin
./ArcSight-logger-6.0.0.7285.0.bin
```
- 3 The installation wizard launches, as shown in the following figure. This wizard also upgrades your Software Logger installation. Click **Next**.



- 4 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.

- 5 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.
- 6 Select **I accept the terms of the License Agreement** and click **Next**.
- 7 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.

- 8 Navigate to or specify the location where you want to install Logger. By default, the /opt directory is specified.
- 9 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.
- 10 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.
- 11 Click **Upgrade** to continue or **Back** to specify another location.



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.

---

- 12 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.

- 13 Click **Next** to initialize Logger components.

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

- 14 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.

- 15 Click **Done** to exit the installer.

- 16 You can now connect to the upgraded Logger.



## Known Issues

The following known issues apply to this release.

### Global Summary Persistence

There was a known issue with the Global Summary Persistence functionality in Logger 5.3. This feature was designed to persist the statistics reported in the global summary section of Logger through a reboot. In some environments, disk space or server memory was affected due to this feature.

The Global Summary Persistence functionality is disabled in this release. As soon as possible after upgrading to Logger 5.3 SP1, enter system maintenance mode and defragment the Global Summary table. If you defragmented the table after upgrading to 5.3 SP1, you do not need to repeat the procedure upon upgrade to Logger 6.0. Refer to the Logger 6.0 Administrator's Guide for instructions.

### Upgrading Containers on Integrated Connector Appliance

On models with an integrated Connector Appliance (L3X00), you should be aware of the following issues:

- Upgrading containers to SmartConnector build 6.0.1.6574 is not supported. Do not upgrade to SmartConnector build 6.0.1.6574. Instead, upgrade to SmartConnector build 6.0.2.6627 or later.
- The Model and Version columns on the Hosts page display the value "Unknown". This issue exists on the local host as well as when the integrated Connector Appliance is remotely managed from another appliance, and will prevent remote appliance upgrade. To resolve these issues, upgrade Container 1 to SmartConnector build 6.0.2.6627 or later.

For instructions on how to upgrade a container, refer to the ArcSight Connector Appliance Administrator's Guide.

### Kernel Warning Message During Boot

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

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

A message similar is posted to the dmesg file. These messages do not affect the functionality or performance of the operating system or the server and can be safely ignored. For more information, refer to the HP Customer Advisory document at: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03265132&lang=en&cc=us&taskId=101&prodSeriesId=4268690&prodTypeId=3709945>

## Issues Fixed in this Release

Logger 6.0 includes the fixes listed in the following tables.

### Analyze/Search

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12859 | <p>You could not select the Fieldset until after you had run a search in the current user session.</p> <p>FIX: With the new Search UI, the Fieldset menu is available before you run a search.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| LOG-12765 | <p>If you set the Case Sensitive search option to No and appended an additional field-based search term by using the AND operator, the search did not return any results.</p> <p>FIX: Case insensitive searches now return results as expected, even when using the AND operator.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| LOG-12746 | <p>An error would result you drilled down from a chart on a Search or Dashboard page that was created by a query where the count was renamed by the chart operator (...   chart count as NEvents by name) and the renamed count was then used to sort the chart results (...   sort -NEvents). This happened because the query resulting from the drill-down still kept the sort term using the renamed count.</p> <p>FIX: Any sort term used after the chart operator is now removed after the chart drill-down.</p>                                                                                                                                                                                                                                                                                                                                         |
| LOG-12685 | <p>Archive search was slow due to the slowness of retrieving metadata.</p> <p>FIX: Metadata retrieval is improved with this release. Hence, the slow search for archive data is also improved.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| LOG-12581 | <p>Saved Search files had to be manually deleted one by one.</p> <p>FIX: When you try to schedule a Saved Search, there is now a "Delete Files After" field. After the time specified in that field expires, Logger deletes the Saved Search files.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOG-12577 | <p>When the user searched with a chartable query, such as "rare deviceEventClassId   sort - _count   where _count &gt;88", and drilled down from the resulting chart by clicking a bar (or other clickable chart element), the resulting (non-chartable) query generated by the drill down was invalid. This happened because the "_count" field cannot be used in searches without any chart result.</p> <p>FIX: The drill down has been improved to remove any query terms using _count after chartable operators so that the resulting query is valid.</p> <p>Note: When the _count is renamed and then the renamed count is used to limit the chart results (...   chart count as "Num of Events" by name   rename name as Name   where "Num of Events" &gt; 30), the resulting query after the drill-down will be still invalid even after this fix.</p> |
| LOG-12542 | <p>The Go button on the Search page could disappear if you canceled a search and then clicked the histogram.</p> <p>FIX: The Go button remains available when you cancel a search and then click the histogram.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12343 | <p>Logger Web service searches that included   regex ",," or other special characters could cause an exception when the events in the search results contains special characters such as &amp;#xEC; &lt;&gt;&amp;#xEE; . This is happened because the Logger Web service cannot handle the special characters in the transported events without proper encoding.</p> <p>FIX: Added instructions for how to turn on base64 encoding on the Logger side and use base64 decoding on the client side to the Logger Best Practices Guide.</p> |
| LOG-12222 | <p>If you drilled down from a chart generated by a query that used both the chart and the rename operators, then the new search created by drilling down would fail.</p> <p>FIX: Drilling down in a chart now works when the rename operator is used.</p>                                                                                                                                                                                                                                                                                |
| LOG-12044 | <p>If you used the eval operator after the chart operator in a query, the new column added by the eval was not properly displayed in the chart. For example, if the query was   chart sum(baseEventCount) as SUM by categoryBehavior   eval NEWSUM = SUM + 1000, then the chart would only show SUM, and it would be the wrong color.</p> <p>FIX: The colors in a chart created using the eval operator now reflect the colors shown in its legend.</p>                                                                                  |
| LOG-11904 | <p>When you opened Search page from the navigation menu, it automatically started running the previously executed search. You had to cancel the search if you did not want it to run.</p> <p>FIX: The search page no longer starts running the previously executed search when you open it.</p>                                                                                                                                                                                                                                          |
| LOG-11839 | <p>When you logged into Logger, the Field set drop-down on the Search page was not displayed until you had run at least one search.</p> <p>FIX: Now the Field set drop-down is available next to the Time Range drop-down so that the Field set can be selected before any search.</p>                                                                                                                                                                                                                                                   |
| LOG-10695 | <p>When a Logger user received an exported file's URL from another Logger user and tried to download the file, the user could download the CSV file successfully, but the file was empty. Since the file was not generated by the user, the download failed without any error message to the user.</p> <p>FIX: Logger now displays an error message that states the user does not have the permissions to download the CSV file instead of letting the user download a 0-byte file.</p>                                                  |
| LOG-10224 | <p>Using the hostname for Peer Authorization can cause an error when performing a peered search.</p> <p>FIX: Using the hostname for Peer Authorization now works as expected.</p>                                                                                                                                                                                                                                                                                                                                                        |
| LOG-7758  | <p>If you use the eval operator after the chart operator, the chart results do not match the results in the table. No bar is shown for the column added by the eval.</p> <p>FIX: Logger now displays chart results properly when the eval operator is used after the chart operator</p>                                                                                                                                                                                                                                                  |

## Configuration

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12854 | <p>Logger Configuration Backup files could exceed the default limit of 10 MB, which could cause the restore operation to fail. This happened because Logger erroneously included some hprof files and the Forwarding Connector AUP backup update files in the Configuration Backup.</p> <p>FIX: Logger Configuration Backup now excludes the hprof files in \$ARCSIGHT_HOME and in the forwarding Connector's user/agent folder. It also excludes the AUP Backup files from user/agent/aup folder of the Connector, but still includes the current AUP update file.</p> |
| LOG-12724 | <p>If you ran a Configuration Backup and set the Backup Content to "Report Content Only", when you tried to restore the backed-up content, the restore failed with the error message, "The version of the backup file is not restorable." This happened because the backup did not include the correct path, and so the restore could not find the version file.</p> <p>Fix: Restoring backups where the Backup Content is "Report Content Only" now works as expected.</p>                                                                                             |
| LOG-11704 | <p>If you attempted to restore a Logger Configuration Backup and the backup's Logger version did not match the local Logger version, the following error message was displayed: "The version of the backup file is not restorable."</p> <p>FIX: When a Configuration Backup cannot be restored because the Configuration Backup's Logger version the local Logger do not match, the message is now more helpful and tells you the Configuration Backup Logger Version and the Local Logger version.</p>                                                                 |
| LOG-11088 | <p>Logger archival process would hang and terminate with an error, such as permission denied.</p> <p>FIX: This issue occurred in setups that enforce lockout of files, which Logger had created in preparation for the archive, after a certain period of time. To avoid such issues, Logger has been updated to create archive files on need basis.</p>                                                                                                                                                                                                                |

## Dashboards

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-13161 | <p>Some dashboard graphs would only display data for seven days, even when you selected to display data for a longer period. For example, if you selected the CPU usage graph for a period of 30 days, you only see data in the graph going back one week.</p> <p>FIX: The dashboard graphs now properly display data for periods longer than 7 days.</p>                                                                                                                                               |
| LOG-11907 | <p>The Logger monitor dashboard duration drop-down, available after you select a category (such as Platform), provided only "4 hour", "Daily", and "Weekly" durations. There was no way to select durations longer than Weekly.</p> <p>FIX: The duration drop-down has been improved to provide more durations. Now you can select "4 hours", "24 hours", "7 days", "30 days", "90 days", and "365 days". All the durations have been changed to use hours/days. For example, Weekly is now 7 days.</p> |

## General

| Issue     | Description                                                                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12713 | In order to install Logger, you first had to install the 32-bit glibc libraries.<br>FIX: Logger no longer has a dependency on the 32-bit glibc libraries, so you do not need to install them before installing Logger.                                                                    |
| LOG-12566 | The Logger SAN model only supported a 5.4TB LUN.<br>FIX: Logger 6.0 supports up to 8TB of storage volume.                                                                                                                                                                                 |
| LOG-11760 | The Logger Administrator's Guide documented Device Event Class ID: platform:204, which was not implemented.<br>FIX: Removed unused Device Event Class ID: platform:204 from the documentation.                                                                                            |
| LOG-11168 | Users sometimes encountered firewall issues when trying to access Logger after installation.<br>FIX: Added information to the installation instructions telling users to ensure that Logger's publicly-accessible ports are allowed through any firewall rules that they have configured. |

## Reports

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12181 | When the account or a user that had created reports was deleted, those reports were orphaned and could not be run nor deleted.<br>FIX: These reports can now be access by the administrator and either run or modified. Also, when a user whose account has created reports, a warning is displayed saying that the user's reports will no longer be available.      |
| LOG-11876 | When a Report timed out (after 4 hours for a Scheduled Report and 1 hour for an Ad hoc Report), it was killed with no notice to the user.<br>FIX: Logger now notifies the user of Report timeouts and other important information. This is dependent on the "Job Error Mail To" field being filled in with a valid email address at Reports > Report Administration. |
| LOG-9991  | Specifying a "Scan Limit" with a value larger than the default 100K did not take effect. Since the filter only applied to the first 100K records matched from the report query, the generated report did not display the correct filtered records.<br>FIX: Specifying a "Scan Limit" with a value larger than the default 100K now works as expected.                |

## Summary

| Issue     | Description                                                                                                                                                                                                                                                                                            |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-11698 | The user session did not time out on Logger's Summary page and custom Dashboards. This happened because any panel that updated its contents automatically extended the user session.<br>FIX: Logger has been improved so that the user session is not extended by the Summary/Dashboards page updates. |

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-10084 | <p>The Count value displayed on the Summary page may be slightly different from the Hit value on the Search page for the same field.</p> <p>Understanding: These differences can occur for various reasons including the following:</p> <ul style="list-style-type: none"><li>- There may have been a delay between the time when the count was displayed on the Summary page and when the search query was run on the Search page.</li><li>- Indexing can lag behind when there are large number of incoming events, thus causing a discrepancy between the Count on the Summary page and Hit value on the Search page.</li></ul> |

---

## System Admin

---

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-13397 | <p>After upgrading to Logger 5.5, 6.0, or any version with an open appliance, there will no longer be a challenge response when you log into the appliance as root via SSH.</p> <p>FIX: SSH access to the appliance is disabled by default.</p> <p>Important: HP strongly recommends that you must change the root password for your appliance as soon as the upgrade completes.</p>                          |
| LOG-12931 | <p>NFS mounts with special characters in their Name could be created but not deleted.</p> <p>FIX: NFS mounts with characters in their Name others than alphanumeric, dash and underscore can no longer be created.</p>                                                                                                                                                                                        |
| LOG-11712 | <p>Certificates that had spaces in their names did not work correctly. If you clicked the link to view the details of the certificate, the certificate appeared to have no content. If you tried to delete that certificate, it still remained in the list of certificates.</p> <p>FIX: Now Logger checks the certificate alias so that only alphanumeric characters and hyphen are allowed in the alias.</p> |
| LOG-10187 | <p>The Device Event Class ID of the system health event Disk /Monitor/Disk/Space/Remaining/ in the Logger Administrator's Guide was incorrect.</p> <p>FIX: Updated the documentation to include the correct Device Event Class ID: Disk /Monitor/Disk/Space/Remaining/Root disk: 101.</p>                                                                                                                     |

## Open Issues in this Release

Logger 6.0 includes the open issues listed in the following tables. Use the noted workaround where one is available.

### Analyze/Search

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-13046 | <p>When you export search results on a localized Logger, gibberish strings could be seen in the exported CSV file if opened in the English version of Microsoft Excel.</p> <p>Understanding: This can happen if Excel does not detect the correct character encoding of the CSV file.</p> <p>Workaround: In order to display the localized characters in the exported CSV file in Microsoft Excel correctly, import the CSV as follows:</p> <ol style="list-style-type: none"> <li>1. Launch Excel.</li> <li>2. Click Data tab.</li> <li>3. Click "From Text" in "Get External Data" menu to import a CSV file.</li> <li>4. Select the exported CSV file and click the Import button.</li> <li>5. In the Text Import Wizard, make sure that             <ol style="list-style-type: none"> <li>a. UTF-8 is selected in the File origin;</li> <li>b. Comma is checked as Delimiters;</li> <li>c. " (double quote) is selected as Text qualifier.</li> </ol> </li> <li>6. Follow the Wizard to finish the import.</li> </ol> <p>For more details of how to import in Excel, please refer to this page:<br/> <a href="http://office.microsoft.com/en-us/excel-help/import-or-export-text-txt-or-csv-files-HP010099725.aspx#BMimport_data_from_a_text_file_by_openi">http://office.microsoft.com/en-us/excel-help/import-or-export-text-txt-or-csv-files-HP010099725.aspx#BMimport_data_from_a_text_file_by_openi</a></p> |
| LOG-12524 | <p>If the value for a discovered field contains a colon, the query generated by clicking on it, will escape the colon, even though it should not.</p> <p>Workaround: Remove the backslash from in front of the colon. For example, if the query inserted by the 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, the original field renamed by the operator is still displayed as a column in the search results, but will not have any values, if the original field name is included in the Fieldset used in the search.</p> <p>For example, if the search uses the All Fields field set, 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-12175 | <p>When running searches that use certain functions, the user may see the error message, "java.lang.NumberFormatException".</p> <p>Understanding: Aggregation functions such as avg, stdev, stdevp, and sum only work on numeric fields.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-11871 | <p>When a user has a Search Group Filter that includes a Device Group, if the search query also includes a Device Group constraint that differs from the Search Group constraint, the query fails. Suppose that Device Group Z with device members A, B, C and D is used in the Search Group Filter. If a search is performed for just device A within Device Group Z, a MySQL error is generated and the search returns zero results. This problem does not occur when it is a peer query.</p> <p>Workaround: Make the Device Group used in the query match the Search Group Filter exactly.</p>                                                                                               |
| LOG-11824 | <p>During a Search, the Server Java Virtual machine (JVM) reports "Unable to Create New Native Thread" due to it going Out of Memory.</p> <p>Understanding: HP ArcSight investigated the issue but did not find a definitive pattern. However, the product software has been fortified to mitigate issues of this nature.</p>                                                                                                                                                                                                                                                                                                                                                                   |
| LOG-11785 | <p>The Java Virtual Machine (JVM) reports running out of memory during searches/reporting.</p> <p>Understanding: HP ArcSight investigated the issue but did not find a definitive pattern. However, the product software has been fortified to mitigate issues of this nature.</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 (i.e. "[), then 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."</p> <p>This workaround can be also used for the double quote followed by any special character such as "\ / "[ ] ",</p> |
| LOG-10662 | <p>The following error sometimes occurred when a search was run against a specific period of time: "Got error 122 'Successfully connected to TCP server 127.0.0.1:8089' from ARC_LOGGER".</p> <p>Understanding: HP ArcSight investigated the issue but did not find a definitive pattern. However, the product software has been fortified to mitigate issues of this nature.</p>                                                                                                                                                                                                                                                                                                               |
| LOG-10130 | <p>The Fields command leaves the field name even though all the values from that field are removed. Therefore, an empty column appears in the search results with the &lt;fieldname&gt; as the title.</p> <p>Workaround: Make sure you use the CEF operator to define the field before using the FIELDS operator. Doing so ensures that the field and its associated values are removed.</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>                                                                                                                                                                                                                                                                                                                                             |



| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 a Logger session has been inactive for 'Logger Session Inactivity Timeout', (default is 15 minutes.)</p> <p>Workaround: Use an external browser to see results.</p>                                                                                                                                                                                                                                                                                                                                              |
| LOG-8760 | <p>Only one search operation per browser can be run on Logger at any time.</p> <p>Workaround: Open another instance of Logger and run your search there.</p> <p>For Firefox, use the add-on called Multifox, available at <a href="http://br.mozdev.org/multifox/">http://br.mozdev.org/multifox/</a>.</p> <p>For Internet Explorer 9 or later, use IE's File &gt; New session menu. If the File menu is not displayed, then click ALT key.</p> <p>For earlier versions of Internet Explorer, create multiple DNS entries in the hosts file for the same IP address so that you can run different sessions at the same time.</p>                     |
| LOG-8751 | <p>When search results are exported, the "Fields" field may be empty.</p> <p>Workaround: Although this situation does not occur consistently, if it does occur, ensure that All Fields is selected in the "Fields" field set on the Search Results page. Then, click Export Results.</p>                                                                                                                                                                                                                                                                                                                                                             |
| LOG-8484 | <p>The stdev function in the chart operator does not work on fields that have more than ten digits. The result of such computations is a blank field.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| LOG-8076 | <p>The Regex Helper tool does not support native characters, such as Traditional Chinese characters.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOG-8003 | <p>When a search operation is run using the Web Services API and the search results contain binary data, the search operation generate the following exception: "Unexpected EOF; was expecting a close tag for element &lt;ns1:data&gt;".</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                  |
| LOG-7864 | <p>The time in several fields is not in human readable format when exported. These fields include deviceReceiptTime, startTime, endTime, and agentReceiptTime.</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-7651 | <p>On the Internet Explorer browser, data is truncated in the Advanced Search calendar popup window. This issue affects users' ability to select a date using the date picker (icon) when setting CCE rules in the Advanced Search feature. When a user clicks the date picker, the calendar widget that comes up is not wide enough to display the full calendar content, truncating columns with the latter days of the week.</p> <p>Workaround: Use the Tab key to scan along the part of the calendar that is initially hidden, then use Shift+Tab to scan back in the other direction. Alternatively, use another browser, such as Firefox.</p> |

| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-7099 | <p>When values for user fields such as sourceUserId, sourceUserName, destinationUserId, and cs1 contain "\n" character, the search results are not displayed correctly.</p> <p>Understanding: The current software interprets a value that contains "\n" as a newline character. For example, user name "nancy" in example domain, "example\nancy", is interpreted as "example[newline]ancy".</p> <p>Workaround: Disable the multi-line feature by adding the following properties to /user/logger/logger.properties. The following examples use the default values.</p> <ul style="list-style-type: none"> <li>- To turn on/off multiline support, use:<br/>search.multiline.fields.supported=true</li> <li>- To turn on/off \n and \t support, use:<br/>search.double.backslash.newlines.supported=false</li> <li>- To turn on/off DOS/Windows path support for CEF and/or syslog, use:<br/>search.keep.windows.path.cef=true<br/>search.keep.windows.path.syslog=true</li> </ul>                                                                                                                                                         |
| LOG-7046 | <p>The time displayed on the histogram might not match the event time. This can happen when the /etc/localtime file is not symbolically linked to the correct time zone.</p> <p>Workaround: Make sure that the /etc/localtime file is symbolically linked to the correct time zone in the /usr/share/zoneinfo file as shown in the following example. Then, restart the system.</p> <pre>sudo ln -s /usr/share/zoneinfo/&lt;timezone&gt; /etc/localtime</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LOG-6965 | <p>When the time change due to Daylight Savings Time (DST) takes place, the following issues are observed:</p> <ul style="list-style-type: none"> <li>- The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram.</li> <li>- The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period.</li> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> </ul> <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p> |
| LOG-6273 | <p>When search results are exported, the time elapsed to export the events is not displayed.</p> <p>Workaround: For the search elapsed time, please refer to the elapsed time shown in the stats on the search page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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 &lt;- arrow to remove the field. If you double click on it, it will go back to the correct list.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 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-4775 | <p>The user interface for the Advanced Search link (on the Search page) to create a query is not intuitive about how to enter a keyword (full-text) term.</p> <p>Understanding: To specify a keyword (full-text search), use the fullText field under the Name column. This field is displayed at the bottom of the pane.</p> <p>Workaround: If you do not see the full-text search field, scroll down.</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: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>&lt;166&gt;Sep 9 14:48:22 beach kernel: Killed bad incoming packet: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00 SRC=192.168.10.153 DST=192.168.10.255 LEN=229</p> <p>Workaround: This problem only occurs for a very small number of devices, which use this particular format. The workaround is to search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255. Alternatively, you could run these data through a SmartConnector to convert to CEF format. Then run either a full-text or field-based search.</p> |
| LOG-2325 | <p>The hits count on the Alerts page (Analyze &gt; Alerts) is not accurate.</p> <p>Workaround: None at this time. Currently, there is no way to know the correct hits count on the Alert page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Configuration

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-13411 | <p>When creating or editing a scheduled alert, if the selected saved search uses an aggregated operator such as chart or top in the query, the schedule cannot be saved, and you see the error "Scheduled alerts do not support aggregated search operators."</p> <p>Logger 6.0 adds the following System Saved Searches. They all use aggregated operators. Therefore, they cannot be used to schedule an alert.</p> <ul style="list-style-type: none"> <li>- Configuration Changes by Product</li> <li>- Failed Logins by Product</li> <li>- Failed Logins by User</li> <li>- Firewall Drops by Source</li> <li>- Malicious Code Activity</li> <li>- SSH Authentications</li> <li>- VPN Connections</li> <li>- Windows Account Creations</li> </ul> <p>Currently there is no way to know which Saved Searches use aggregated operators when scheduling an alert, so the user may frequently hit the above error by selecting the system saved searches.</p> <p>Workaround: Do not use any of the System Saved Searches to schedule an alert. Make sure that any Saved Search you use to create or edit a scheduled alert does not use any aggregated operators.</p> |
| LOG-11691 | <p>On L7500 appliances, after you finish the initial configuration and click Save, the Logger may fail to reboot automatically. It will continue to display "Configuring".</p> <p>Workaround: If the display does not change from "Configuring" to "Rebooting" and then show the Login dialog box within 20 minutes, then refresh the page to cause a reboot.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LOG-11176 | <p>When you enable a receiver, Logger does not validate the RFS mount it referenced.</p> <p>Workaround: Make sure the RFS mount is valid by clicking edit button for this receiver. Alternatively, check the Admin page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG-10605 | <p>The Source Types tab (Configuration &gt; Source Types) is not visible for non-admin users.</p> <p>Workaround: Add 'Read Only Default Admin Group' privileges to the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| LOG-10581 | <p>When a parser associated with a Source Type and Folder Follower Receiver is deleted, no warning message is displayed indicating the dependency.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG-10353 | <p>High incoming event rates can have an effect on the indexing rate of the Logger.</p> <p>Workaround: If you notice that indexing is falling behind, decrease the incoming event rates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG-10173 | <p>When Logger performs a configuration to a remote host, it expects an SSH log-in prompt followed by a password prompt. If the remote system contains banners or other extraneous data before the password prompt, the remote log in will fail.</p> <p>Workaround: Disable any banners or configure the SSH server to communicate in a quiet mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LOG-10058 | <p>Sending events targeted to an IPv6 address on Logger is not supported. The system state is unknown once it happens.</p> <p>Workaround: Restart the "receiver" process.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-10056 | <p>You may get a duplicate device name if a receiver was removed and a new one was created with the same name as 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: To avoid this problem, do not create receivers with same names as any deleted receivers.</p>                                                                                                                                                                                                                   |
| LOG-9658  | <p>If you have already increased your storage volume to the maximum limit allowed by your license, and you attempt to increase the volume further, the error message displayed is incorrect. Instead of notifying you that you have reached the limit of your license the message says, "Sufficient free space is not available to increase the storage volume size. To restore normal Logger operation, click Restart."</p> <p>Workaround: Click Restart. No further action is required. However, if you need to increase the storage limit, please contact HP Support.</p> |
| LOG-9498  | <p>Logger only parses syslog headers that are in the format specified by RFC3164 (traditional syslog headers). Newer syslog header formats specified by RFC3339 (syslog-ng headers) are not supported.</p> <p>Workaround: Edit the parser to make it work for the newer headers.</p>                                                                                                                                                                                                                                                                                         |
| LOG-9305  | <p>Connectors send values of date/time-type fields in the following format:<br/>07/09/0169 09:57:35.000 PST</p> <p>Understanding: This is a format that Logger does not understand. It expects time field values to be in epoch format (long values).</p> <p>Workaround: Convert the time value into epoch time for Logger to be able to process them correctly.</p>                                                                                                                                                                                                         |
| LOG-8790  | <p>When the community string contains non-ASCII characters, the SNMP trap sent out displays "???" in the community field.</p> <p>Understanding: This is a UI 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 failed to mount because the user name and password fields are empty.</p> <p>Workaround: Edit the setting of the CIFS share and re-enter the username and password.</p>                                                                                                                                                                                                                                                                                                                                 |
| LOG-6786  | <p>Events may be missed when a receiver on Logger is disabled.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LOG-6209  | <p>If the Finished Tasks page (Configuration &gt; Finished Tasks) contains a very large number of entries, the page sometimes takes a while to load or stops loading.</p> <p>Workaround: If the pages stops loading, refresh the browser window to continue loading.</p>                                                                                                                                                                                                                                                                                                     |
| LOG-5024  | <p>If the system that Logger backs up its configuration to is reinstalled or its SSL key is changed, the configuration backup fails because the SSL key cannot be refreshed from the Logger UI.</p> <p>Workaround: Log in to the Command Line Interface and delete the entry in the /home/arcSight/.ssh/known_hosts file. Then refresh the config backup configuration.</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.</p> <p>Examples of improper tear-down: One of the Loggers is replaced with a new appliance or 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 open the Certificates page and delete a certificate, After a certificate is deleted, the deleted certificate is still displayed in the list, leading to an impression that the certificate is still loaded on the system.</p> <p>To open the Certificates page, type "Cer" in the Take me to search box, and click Certificates in the list.</p> <p>Workaround: Refresh the page to update the list. The deleted certificate is no longer displayed in the list.</p>                                                                                                                                                          |
| LOG-3944 | <p>A configuration backup is not successful if the Remote Directory name contains a space.</p> <p>Workaround: Ensure that the Remote Directory name does not contain a space.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOG-3156 | <p>If content is imported on a Logger that does not have the same configuration setup (devices, device groups, storage groups) as the exporting Logger, content that relies on that configuration cannot be used.</p> <p>Workaround: None at this time. The feature assumes that importing Logger has the same configuration setup as the exporting Logger.</p>                                                                                                                                                                                                                                                                         |
| LOG-2941 | <p>The type associated with imported filters cannot be changed from shared to saved search.</p> <p>Workaround: Imported filter types cannot be changed. However, you can copy the filter definition and create a new filter out of it.</p>                                                                                                                                                                                                                                                                                                                                                                                              |
| LOG-2387 | <p>The EPS Out gauge reports a non-zero value even when no Forwarders are enabled.</p> <p>Understanding: This gauge reports traffic from real-time alerts as well as from Forwarders. Therefore, if you have Alerts configured on your Logger, EPS Out can be greater than zero.</p>                                                                                                                                                                                                                                                                                                                                                    |
| LOG-2244 | <p>A forwarder configured with a filter might not forward events that match the specified end time.</p> <p>Workaround: Extend the end time by one second to ensure that all events are forwarded appropriately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LOG-370  | <p>The Configuration Backup (Configuration &gt; Configuration Backup &gt; Name_of_Backup) and File Transfer Receivers (Configuration &gt; Receivers) may fail silently. 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 in this case, so use Retrieve Logs page (Configuration &gt; Retrieve Logs) if you suspect a problem with the backup. When Configuration Backup is scheduled, error status is shown in the Finished Tasks status field.</p> |

## Connector Appliance

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-12658 | <p>When using Internet Explorer 11 to access Connectors on a Logger L3x00 appliance, there is a display issue when you add ten or more rows to the extra mappings table on the parser page of the Flex Connector Wizard. In that case, the Event Field drop-downs may not be properly aligned within the table if you scroll down the page.</p> <p>Workaround: Since this issue occurs when scrolling down the page, maximize the window to prevent the need to scroll.</p>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LOG-12340 | <p>If user tries to upload a file that has space in its name to the repositories, an error message will be displayed.</p> <p>Workaround: Remove space from the filename and try to upload again.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| LOG-12339 | <p>The EPS IN/OUT values for connectors may be displayed as "unknown" in the list of Connectors on the Container page.</p> <p>Workaround: Click the connector in the list to open the Connector's page. That will ping the connector. Click the container to go back to the list and the EPS IN/OUT values should be reflected.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOG-11732 | <p>After backup/restore on L3200 and L3400 appliances, the Connector shows as empty.</p> <p>Workaround: Restart the connector. You can do this from the Manage Connectors tab or from the System Admin Process Status page.</p> <p>To restart the connector from the Manage Connectors tab:</p> <ol style="list-style-type: none"> <li>1. On the Manage Connectors tab, click the container in the left side tree.</li> <li>2. Click the "Send Container Command" icon.</li> <li>3. Select "Restart" command from the list of commands.</li> </ol> <p>When the container restarts, you should see the connector up and running.</p> <p>To restart the connector from the process status pane:</p> <ol style="list-style-type: none"> <li>1. Open the System Admin &gt; Process Status.</li> <li>2. Click the connector and restart it.</li> </ol> <p>You should now see the connector up and running.</p> |
| LOG-11731 | <p>Emergency Restore places the local connector in the wrong location. Therefore, the old local connector is never overwritten with the new connector information and emergency restore operation fails. The connector still points to old connector version.</p> <p>Workaround: Please contact HP Support for the steps to emergency restore the local connector.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| LOG-10029 | <p>On Logger Appliances that have integrated Connector Appliances, users cannot access the Connector Appliance module after upgrading to Logger 5.2.</p> <p>Understanding: A new "Connector Appliance Rights Group" was introduced in this release. A user who needs to access the Connector Appliance module must be assigned to this group.</p> <p>Workaround: Assign users who need to access the Connector Appliance module to "Connector Appliance Rights Group".</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Dashboards

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-11730 | <p>When there are two or more Dashboards with the same name, after you select one of them from the Dashboard dropdown, there is no way to show the other from the dropdown. This is because when you select one of the dashboards with the same name, the dropdown thinks the first entry of those dashboards is always selected.</p> <p>Workaround: Rename the other dashboards so that they all have different names.</p>                                                                                                                                                                                                               |
| LOG-9332  | <p>When the Monitor graph panel is not wide enough to show the entire graph in the Monitor or Custom Dashboards, the graph is cut off and no scroll bar is shown in the panel, in the Firefox browser. In the Internet Explorer 9 browser, the panel is blank.</p> <p>Workaround: For Custom Dashboards, make the browser window wider or change the layout of the panels so that each graph panel will have enough width to show the graph (For example, If the row including a Monitor graph panel has 3 panels, move at least one of the other panels to the other row). For the Monitor Dashboard, make the browser window wider.</p> |

## General

| Issue     | Description                                                                                                                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-13445 | <p>Logger 6.0 adds the ability to upload a custom log to replace the default HP logo. The logo is replaced on the regular UI pages, but not on the initial Log-In and Log-out splash screens.</p> <p>Workaround: None at this time.</p>                                                                                                   |
| LOG-13299 | <p>For Internet Explorer 10 only, if you enter your password in the Log in screen and then move to another tab before logging in, the some of the dots that represent your password are no longer displayed, however the password you typed is unchanged.</p> <p>Workaround: Use Internet Explorer 11, which does not have the issue.</p> |
| LOG-11659 | <p>In software Loggers, the installation of multiple Solution Packages may fail if the SOX v4.0 solution package is installed in the wrong order by the root user.</p> <p>Workaround: If you are installing the SOX v4.0 solution package as the root user, install it last.</p>                                                          |
| LOG-11473 | <p>Initial appliance configuration, such as uploading the license, setting the locale, date/time and configuring SAN, could fail if some requirements were not met.</p> <p>Workaround: If needed, configure the Logger's date/time before uploading the license.</p>                                                                      |
| LOG-2433  | <p>If you click on another tab or page before a UI page is fully loaded, the UI attempts to load the latter page, but eventually displays the former page.</p> <p>Workaround: Wait for the current page to finish loading before clicking another one.</p>                                                                                |



## Reports

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-11954 | <p>If the underlying Query of a Report changes, then viewing published reports will result in an error.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG-11502 | <p>Report Engine logs indicate that MySQL Tables are "Marked as Crashed" and need repair.</p> <p>Understanding: HP ArcSight investigated the issue but did not find a definitive pattern. However, the product software has been fortified to mitigate issues of this nature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG-11279 | <p>Restoring configuration backup does not preserve the report templates original file ownership and causes report execution without proper templates.</p> <p>Workaround: Follow these steps to fix the permissions.</p> <ol style="list-style-type: none"> <li>1. SSH to Logger. (Appliance users should contact HP support for help with this.)</li> </ol> <p>Note: In Logger 6.0, SSH can be enabled from navigating to System Admin &gt; System &gt; SSH menu item.</p> <ol style="list-style-type: none"> <li>2. Navigate to the following directory, &lt;\$ARCSIGHT_HOME&gt;/logger/Intellicus/reportengine/templates/adhoc, where &lt;\$ARCSIGHT_HOME&gt; is the directory in which Logger is installed.</li> <li>3. Change the owner of the report templates [files with extension .irl and .sty] files from "root" to the same non-root user that was used during Logger installation.</li> </ol> |
| 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-10098 | <p>Reports display a - for null values. If this is displayed in a drilldown column, the column displays the - as a hyperlink, which usually opens with odd results since '-' does not match.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LOG-9860  | <p>When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it is 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-9798  | <p>When the Logger Compliance Insight Package (CIP) reports such as Logger ITGov 4.0 for ISO 27002 are exported in PDF format, the saved PDF shows that Chart component with the following error: "Error: No plotters/series have been defined"</p> <p>Workaround: None at this time.</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 at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| LOG-9584  | <p>After upgrading to Logger 5.2, you may see browser caching issues Reports pages. There may be errors in red in the dashboard viewer, you may not be able to create widgets, and the explorers may not work.</p> <p>Workaround: Restart your browser. If that does not work, manually clear the browser cache and delete temporary files.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-9216 | <p>Even when report categories are marked Hidden, they might be visible in Explorers and other report-related locations.</p> <p>Understanding: This is by design. The hidden categories are visible to admin users and users with appropriate access rights only. They remain hidden in the Report List page. In case of query explorer, they are displayed because this is where queries must be listed in order to be edited.</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 limit a user's rights to a specific report template, the user might be unable to run any reports at all and the following error messages might be displayed when the user tries to run reports:</p> <p>90141 No matching record found: Requested Report Object "xxxxxxx" Not Found</p> <p>90141 No matching record found: The Query Object used as the Datasource could not be fetched from the repository</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>Workaround: Enable global access to all reports, then the user will be able to edit and run all the reports.</p> |
| LOG-7165 | <p>The privileges for pre-built reports on Logger are missing from the Add Group page if the Logger is a fresh install and you have not yet loaded the Reports page after installing this Logger.</p> <p>Workaround: Go to the Reports page. (This triggers the population of group privileges in the Add Group.) Go back to Add Group. The privileges for pre-built reports are displayed now.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LOG-6652 | <p>In the Firefox browser, the Report Template editor (Reports &gt; Design - Template Styles &gt; Select a template &gt; Edit Layout) is not usable because the pull-out menus cannot be resized, the drop-down menus do not display the full list of options, and some windows open behind the editor.</p> <p>Workaround: Use the Internet Explorer browser.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOG-3244 | <p>In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report.</p> <p>Workaround: Use the Internet Explorer browser instead.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| LOG-3187 | <p>The time taken to run a scheduled report is not reported correctly in the Logger user interface.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| LOG-2355 | <p>The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| LOG-2350 | <p>The default report generated by clicking the hand icon is missing the report name and date.</p> <p>Workaround: Add a Report title to the Report Header section to include the title on the first page of the Report.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Issue    | Description                                                                                                                                                                                                |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-2012 | Adding a scheduled report can reset the scan limit field of other reports.<br>Workaround: Check that the scan limit is set as desired before running any report.                                           |
| LOG-1956 | The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.<br>Workaround: None at this time.          |
| LOG-1936 | Users who are granted only edit and save report styles privileges do not see the Template Styles link on the Reports tab.<br>Workaround: Grant users that need to access Template Styles admin privileges. |
| LOG-1703 | When a query used in an existing scheduled report is edited to add a mandatory filter, the report does not return any output when it runs and an error is generated.<br>Workaround: None at this time.     |

## Summary

| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-9955 | On the Summary page or in any of the Summary panels included in a custom dashboard, if the number of events in the Count column is very large (1 million or higher) and you drill down to view those events, your system may experience performance issues.<br><br>Workaround: If you need to drill down to view a large set of events (1 million or higher), HP highly recommends that you follow these steps to prevent the performance impact very large search results sets can have your system:<br><ol style="list-style-type: none"> <li>1. Cancel the search that automatically starts once you click on a resource (receiver, device, agent severity, or agent type).</li> <li>2. Change the Start and End time values for the search query such that they span a smaller time range. By default, these values are set to the last time your Logger was rebooted/restarted and the current time, respectively.</li> <li>3. Run the search with the new Start and End time values.</li> </ol> |
| 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.<br><br>Understanding: The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different.<br><br>Workaround: None at this time. Currently, there is no way to specify the search time range in milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## System Admin

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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>                                                                                                                                                       |
| LOG-11205 | <p>Some System Administration pages do not render correctly when using Microsoft Internet Explorer 9.</p> <p>Workaround: To use this version of the browser, ensure that Compatibility Mode is set On. This can be found under Tools &gt; F12 Developer Tools &gt; Browser Mode.</p>                                                                                                                                                                                                                                                                              |
| LOG-11066 | <p>If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues:</p> <ol style="list-style-type: none"><li>1. On the Search page, the Events grid in the search results will be empty for any search,</li><li>2. The timestamps with timezone will be shown using GMT,</li><li>3. In the Global Summary on the Summary page, the Indexing is reported one hour behind the current time stamp.</li></ol> <p>Workaround: Change the system time zone to something to more specific, such as /America/Los_Angeles.</p> |
| LOG-9288  | <p>The System Admin - FIPS 140-2 page can take several seconds to load.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| LOG-7664  | <p>If a single-path SAN Logger Appliance is rebooted and the previously attached LUN is not available, the Logger will fail to start. In case of a multi-path SAN Logger Appliance, the Logger fails to start only if the path that was in use when the Logger was rebooted is unavailable.</p> <p>Workaround: None at this time.</p>                                                                                                                                                                                                                             |
| LOG-1050  | <p>Under certain circumstances, users with restricted privileges might still see Device Group and Storage Group names.</p> <p>Understanding: If these users are also subject to a Search Group Filter (enforced filter), they will not be able to see events in those Device Groups or Storage Groups.</p> <p>Workaround: Provide Device Group and Storage Group names that do not reveal internal information.</p>                                                                                                                                               |

## Upgrade

| Issue     | Description                                                                                                                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-11136 | <p>After upgrading the Logger Appliance version 5.3, rebooting, and logging in, you may encounter a page that asks to upload a license and set the time zone.</p> <p>Workaround: Please contact HP Support for help with this issue.</p> |