Release Notes

ArcSight Logger 6.0 Patch 1

November 19, 2014

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://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
11/19/14	Logger 6.0 Patch1	Patch 1 for 6.0.
09/26/14	Logger 6.0	Update for 6.0 release.
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.

Contents

ArcSight Logger 6.0 Patch 1 5

What's New in Logger 6.0 Patch 1 5
Supported Platforms 8
Supported Browsers 9
Localization Information 9
Logger Documentation 10
Upgrade Paths 11
Upgrading to Logger 6.0 Patch 1 (L7307) 12
Known Issues 17
Fixed Issues 17
Open Issues 18

ArcSight Logger 6.0 Patch 1

These release notes provide information about the ArcSight Logger 6.0 Patch 1 (L7307) 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 Patch 1" on page 5
- "Supported Platforms" on page 8
- "Supported Browsers" on page 9
- "Localization Information" on page 9
- "Logger Documentation" on page 10
- "Upgrade Paths" on page 11
- "Upgrading to Logger 6.0 Patch 1 (L7307)" on page 12
- "Known Issues" on page 17
- "Fixed Issues" on page 17
- "Open Issues" on page 18

What's New in Logger 6.0 Patch 1

The Logger 6.0 Patch 1 release (L7307) provides the same functionality as Logger 6.0 (L7285), and includes important time zone (TZData) and security updates.

For information about Logger 6.0 functionality, refer to the Release Notes for that version and the Logger 6.0 documentation described in "Logger Documentation" on page 10.

Time Zone Update

This release provides updated time zones including support for Russia's 2014 time zone changes. The update version is tzdata 2014g.

- For Software Loggers, the TZData update requires that the operating system's time zone RPM is 2014f or later before upgrading to this release.
- HP ArcSight offers the TZData hotfix separately. Therefore, if you cannot update the operating system's time zone RPM to 2014f or later before you upgrade to this release, you can apply HP ArcSight's TZData hotfix later. The hotfix contains the same time zone update and is available from HP ArcSight Customer Support.

- If you applied HP ArcSight's TZData hotfix prior to upgrading to this release, your TZData update will remain unchanged, and you can safely upgrade to get the other fixes included in this release.

Security Updates

This release includes the following security updates:

- Distributes latest version of OpenSSL, 0.9.8zc, which addresses multiple vulnerabilities including CVE-2014-0224.
- Resolves the Bourne-Again Shell (Bash) Code Injection Vulnerability, including CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278.
- Disables support for SSL v3.0 encryption, to address the Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability (CVE-2014-3566).

Features Introduced in Logger 6.0

The following enhancements were introduced in Logger 6.0 and are included in this release. 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.

- 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.
  - 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 Patch 1 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.

Managing Logger through ArcMC

Logger 6.0 Patch 1 supports management through ArcMC 2.0.

- If you do not manage Logger through ArcMC, no action is necessary. You can skip this section.
- If you are currently managing Logger 6.0 through ArcMC, no action required for this patch. You can continue managing Logger after you upgrade it to version 6.0 Patch 1. You do not need to reinstall the ArcMC Agent, and can skip this section.
- If you are performing a fresh installation of Logger 6.0 Patch 1 and want to manage it through ArcMC, follow the instructions in "To manage a fresh installation of Logger 6.0 Patch 1 through ArcMC 2.0:" on page 7.
- If you are currently managing Logger 5.5 Patch 2 through ArcMC, you must install the latest version of the ArcMC Agent before you upgrade Logger to version 6.0 Patch 1. For instructions, see "To install the new ArcMC Agent when upgrading to Logger 6.0 Patch 1:" on page 7.

To manage a fresh installation of Logger 6.0 Patch 1 through ArcMC 2.0:

1. Install ArcMC 2.0 if have not already done so.
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 ArcMC Agent to ArcMC by following the instructions in the ReadMe that comes with the ArcMC Agent.
4. Install Logger 6.0 Patch 1 by following the instructions in the Logger Installation Guide.
5. Add the Logger as a host by following the instructions in the ArcMC 2.0 Administrator's Guide.

To install the new ArcMC Agent when upgrading to Logger 6.0 Patch 1:

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 on 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 Patch 1 by following the instructions in "Upgrading to Logger 6.0 Patch 1 (L7307)" 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. VM installation on the operating systems listed in the table below is supported.

Specification	Details
Supported Operating Systems	• Red Hat Enterprise Linux (RHEL) versions 6.2 and 6.5 (64-bit) • CentOS versions 5.5 and 6.5 (64-bit) **Notes:** • HP ArcSight recommends RHEL 6.5 for fresh installs. • If you are planning to upgrade your current OS as well as Logger, HP ArcSight recommends upgrading the Logger 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	**For the Trial Logger and VM Instances:** • CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4 - 12 GB (12 GB recommended) • Disk Space: 10 GB (minimum) in the Logger installation directory • Temp directory: 1 GB **For the Enterprise Version of Software Logger:** • CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12 - 24 GB (24 GB recommended) • Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data. • Root partition: 400 GB • Temp directory: 1 GB **Note:** Using NFS as primary event storage is not recommended.
Other Applications	• For optimal performance, make sure no other applications are running on the system on which you install Logger. • You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger installer on a 64-bit CentOS 6.5 configured with 12 GB RAM and four physical (and eight logical) cores. • HP ArcSight 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.

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 an encrypted HTTPS connection.

Logger 6.0 Patch 1 supports access through the following browsers:

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

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome already includes a Flash player.) Some Logger 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, allow access to port 443 as well as 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, allow access to port 9000 as well as 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.

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.
- The Login field on the Add User page does not accept native characters. Therefore, a Logger user cannot have a login name that contains native characters.
- Reports are localized for Japanese only.
- The Report Parameter and the Template Style fields do not accept native characters.
- Some Logger user interface sections are not localized. For example, the following sections are available in English only:

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

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

Logger Documentation

The new documentation for this release includes these Release Notes. The complete documentation set published with Logger version 6.0 also applies to this release.

- **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.

  When installing this release, use ArcSight-logger-6.0.0.7307.1.bin instead of the software logger installation file in that document.
- **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.

- **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.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.0 Patch 1. If you need to upgrade a 4.0 SP1 Patch 1 or earlier version of Logger, refer to the release notes of the version you are upgrading to or contact HP Support.

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) -> 6.0 (L7285) -> 6.0 Patch 1 (L7307).
Other upgrade paths	• 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 (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) -> Follow the upgrade path as described in the “Most common upgrade path.” • 5.5 (L7049) -> 6.0 (L7285) ->6.0 Patch 1 (L7307). • 5.5 Patch 2 (L7085) -> 6.0 Patch 1 (L7307). • 6.0 (L7285) -> TZData Hotfix (does not update the build number) -> 6.0 Patch 1 (L7307).
Notes	• The Lx200 models are not upgradable to the Logger 6.0 series. • The 5.0 Patch 1 (L5215) Logger Appliance release is an interim version that you should not upgrade to any longer. 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) -> 6.0 (L7285) -> 6.0 Patch 1 (L7307).

Other upgrade paths	• 5.0 Patch 1 (L5215) -> 5.0 time zone 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) -> Follow the upgrade path as described in the “Most common upgrade path.” • 5.5 (L7049) -> 6.0 (L7285) ->6.0 Patch 1 (L7307). • 5.5 Patch 2 (L7085) -> 6.0 Patch 1 (L7307). • 6.0 (L7285) -> TZData Hotfix (does not update the build number) -> 6.0 Patch 1 (L7307).
Note	You cannot upgrade the 4.5 GA installation of Software Logger.

Upgrading to Logger 6.0 Patch 1 (L7307)

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

- “Verifying Your Upgrade Files” on page 12
- “Logger Appliance” on page 12
- “Software Logger and Logger on VMWare VM” on page 14

Be sure to review the “Known Issues” on page 17, “Fixed Issues” on page 17, and “Open Issues” on page 18, before upgrading your Logger.

Verifying Your Upgrade Files

HP provides a digital private key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:
https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

Logger Appliance

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- 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-7307.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 are currently managing Logger 5.5 Patch 2 through ArcMC, you must install the latest version of the ArcMC Agent before you upgrade Logger to version 6.0 Patch 1. For instructions, see "To install the new ArcMC Agent when upgrading to Logger 6.0 Patch 1:" on page 7.

Upgrade Instructions

To upgrade a Logger Appliance:

1. Log into Logger and click **System Admin | System > License & Update**.
2. Browse to the `logger-7307.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 prompted to upload a license and set the time zone at this stage, contact HP Support for assistance.

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 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 and Logger on VMWare VM

Refer to the "Upgrade Paths" on page 11 section for the supported upgrade paths for your Logger.

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:

- 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 want this upgrade to apply the TZData fix, make sure the operating system's time zone RPM is 2014f or later.
- If you are planning to upgrade your current operating system as well as Logger, upgrade Logger first, and then upgrade the operating system.
- Increase the user process limit on the Logger's OS as described in "Increasing the User Process Limit" on page 14.
- 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.
- If you are currently managing Logger 5.5 Patch 2 through ArcMC, you must install the latest version of the ArcMC Agent before you upgrade Logger to version 6.0 Patch 1. For instructions, see "To install the new ArcMC Agent when upgrading to Logger 6.0 Patch 1:" on page 7.

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
```

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

The following information applies to both physical and virtual machines.

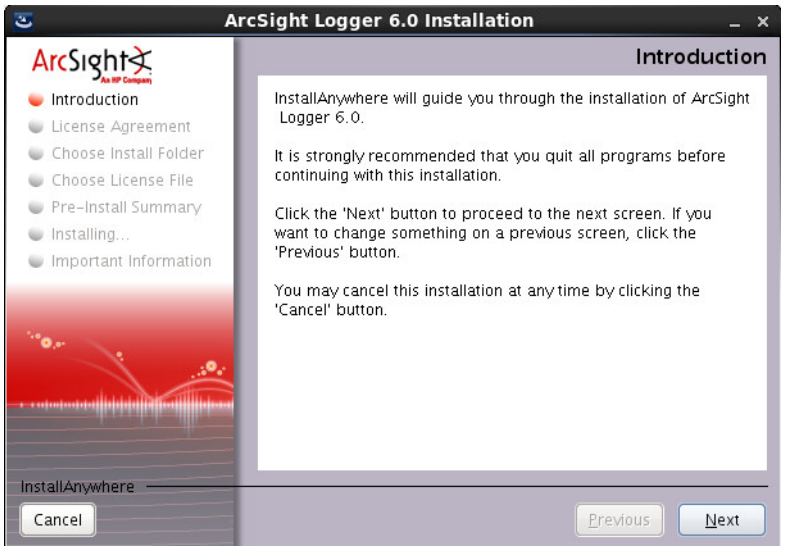
To upgrade a Software Logger:

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-6.0.0.7307.1.bin
./ArcSight-logger-6.0.0.7307.1.bin
```

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



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

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

4 The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the “I accept the terms of the License Agreement” button.

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

6 If Logger is currently running on this machine, an Intervention Required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the upgrade, or click **Quit** to exit the installer.

If you click Continue, the installer stops the running Logger processes and checks for other installation prerequisites. Once all Logger processes are stopped and the checks complete, the next screen is displayed.

7 Navigate to or specify the location where you want to install Logger. By default, the /opt directory is specified.

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

9 If Logger is already installed at the location you specify, a User Intervention message is displayed telling you that the selected directory already contains an installation of Logger, and asking if you want to upgrade.

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

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

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

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

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

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

13 Click **Next** to configure Logger.

Configuration may take a few minutes. Please wait. Once the configuration is complete, Logger starts up and the next screen is displayed.

14 Click **Done** to exit the installer.

15 You can now connect to the upgraded Logger.

Known Issues

The following known issues apply to this release.

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. 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 L3500, L7500, and L7500-SAN series Loggers:

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

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

Fixed Issues

Logger 6.0 Patch 1 includes the fixes listed in the table below.

Issue	Description
LOG-13510	Lx200 models are not supported for upgrade to Logger 6.0. However, if you attempted to run the upgrade, the process upgraded some packages before failing, leaving you with a partially upgraded system. FIX: The upgrade process now checks the Logger model number and prevents attempts at upgrading Lx200 models to Logger 6.0.
LOG-13585	If you ran multiple distributed reports, the first report ran fine, but subsequent reports could hang. Fix: Subsequent reports now run as well as the first report if you run multiple distributed reports.

Open Issues

Logger 6.0 Patch 1 includes the open issues listed in the following tables. Use the noted workaround where one is available.

Analyze/Search

Issue	Description
LOG-13532	When the time change due to the end of Daylight Savings Time (DST) takes place in the fall, and time is set back one hour, the search results may not display properly. This happens because Logger is not able to distinguish the event times in the overlap period. Workaround: To ensure that all events are returned and can be displayed, specify a start time of 12:59:59 or earlier and end time of 2:00:01 or later.
LOG-13538	After the TZData fix is applied to Logger, the time zone for Europe/Kaliningrad may continue to show FET instead of EET in the search results. This is a display issue. The time on Logger is correctly adjusted to be in the EET time zone. Workaround: None available at this time.
LOG-13046	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. Understanding: This can happen if Excel does not detect the correct character encoding of the CSV file. Workaround: In order to display the localized characters in the exported CSV file in Microsoft Excel correctly, import the CSV as follows: 1. Launch Excel. 2. Click Data tab. 3. Click “From Text” in “Get External Data” menu to import a CSV file. 4. Select the exported CSV file and click the Import button. 5. In the Text Import Wizard, make sure that a. UTF-8 is selected in the File origin; b. Comma is checked as Delimiters; c. " (double quote) is selected as Text qualifier. 6. Follow the Wizard to finish the import. For more details of how to import in Excel, please refer to this page: 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
LOG-12524	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. 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".

Issue	Description
LOG-12290	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. 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. Workaround: Since this issue is caused by the fields included in the Fieldset used for the search, remove any renamed fields from the Fieldset.
LOG-12175	When running searches that use certain functions, the user may see the error message, "java.lang.NumberFormatException". Understanding: Aggregation functions such as avg, stdev, stdevp, and sum only work on numeric fields.
LOG-11871	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. Workaround: Make the Device Group used in the query match the Search Group Filter exactly.
LOG-11824	During a Search, the Server Java Virtual machine (JVM) reports "Unable to Create New Native Thread" due to it going Out of Memory. 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.
LOG-11785	The Java Virtual Machine (JVM) reports running out of memory during searches/reporting. 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.
LOG-11299	If you uncheck the Rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail. Workaround: The Rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.
LOG-11225	When using the Auto Complete feature on the Search page, if the query has a double quote followed by bracket (i.e. "[), then the query inserted by the Auto Complete cannot be executed because of incorrectly escaped quotes and backslashes. Workaround: Remove the backslash followed by a double quote on both sides of the string. For example, if the query inserted by the Auto Complete is "\"[/opt/mnt/soft/logger_server.log.6] successfully.\"", then after removing them, the query becomes "[/opt/mnt/soft/logger_server.log.6] successfully." This workaround can be also used for the double quote followed by any special character such as "\ "/ "["] ",

Issue	Description
LOG-10662	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". 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.
LOG-10130	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 <fieldname> as the title. 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.
LOG-10126	When using the replace operator, if the "from" string is included in the replacement string, the "from" string will be replaced twice. For example, the following command, when run against the data "john smith" will result in "johnnyny smith": | replace "*john*" with "*johnny" Workaround: None available at this time.
LOG-9420	When using the search term "transaction" on data that was received out of order, the duration may appear to be negative. Workaround: Include the term "sort _eventTime" before the transaction term.
LOG-9025	When running Logger from an ESM console, a Logger quick search using One-Time Password (OTP) in the embedded browser fails after a Logger session has been inactive for 'Logger Session Inactivity Timeout', (default is 15 minutes.) Workaround: Use an external browser to see results.
LOG-8760	Only one search operation per browser can be run on Logger at any time. Workaround: Open another instance of Logger and run your search there. For Firefox, use the add-on called Multifox, available at http://br.mozdev.org/multifox/. For Internet Explorer 9 or later, use IE's File > New session menu. If the File menu is not displayed, then click ALT key. 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.
LOG-8751	When search results are exported, the "Fields" field may be empty. 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.
LOG-8484	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. Workaround: None at this time.
LOG-8076	The Regex Helper tool does not support native characters, such as Traditional Chinese characters. Workaround: None at this time.
LOG-8003	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 <ns1:data>". Workaround: None at this time.

Issue	Description
LOG-7864	The time in several fields is not in human readable format when exported. These fields include deviceReceiptTime, startTime, endTime, and agentReceiptTime. Understanding: Logger records time field values in UNIX epoch format (long values). Workaround: Use an epoch formula in Excel to convert the time value from epoch time.
LOG-7651	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. 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.
LOG-7099	When values for user fields such as sourceUserId, sourceUserName, destinationUserId, and cs1 contain "\n" character, the search results are not displayed correctly. 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". Workaround: Disable the multi-line feature by adding the following properties to /user/logger/logger.properties. The following examples use the default values. - To turn on/off multiline support, use: search.multiline.fields.supported=true - To turn on/off \\n and \\t support, use: search.double.backslash.newlines.supported=false - To turn on/off DOS/Windows path support for CEF and/or syslog, use: search.keep.windows.path.cef=true search.keep.windows.path.syslog=true
LOG-7046	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. 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. sudo ln -s /usr/share/zoneinfo/<timezone> /etc/localtime

Issue	Description
LOG-6965	When the time change due to the start of Daylight Savings Time (DST) takes place in the spring, and time is set ahead one hour, the following issues are observed: - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket. - Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram. - If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results. Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.
LOG-6273	When search results are exported, the time elapsed to export the events is not displayed. Workaround: For the search elapsed time, please refer to the elapsed time shown in the stats on the search page.
LOG-5958	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. Workaround: This only happens if you use the <- arrow to remove the field. If you double click on it, it will go back to the correct list.
LOG-5181	Search results are not highlighted when there are multiple values that match the IN operator in a query. 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.
LOG-4775	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. 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. Workaround: If you do not see the full-text search field, scroll down.

Issue	Description
LOG-4329	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. Query 1: "ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00" Query 2: "192.168.10.153" Query 3: "192.168.10.255" <166>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 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.
LOG-2325	The hits count on the Alerts page (Analyze > Alerts) is not accurate. Workaround: None at this time. Currently, there is no way to know the correct hits count on the Alert page.

Configuration

Issue	Description
LOG-13411	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." Logger 6.0 adds the following System Saved Searches. They all use aggregated operators. Therefore, they cannot be used to schedule an alert. - Configuration Changes by Product - Failed Logins by Product - Failed Logins by User - Firewall Drops by Source - Malicious Code Activity - SSH Authentications - VPN Connections - Windows Account Creations 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. 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.

Issue	Description
LOG-11691	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". 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.
LOG-11176	When you enable a receiver, Logger does not validate the RFS mount it referenced. Workaround: Make sure the RFS mount is valid by clicking edit button for this receiver. Alternatively, check the Admin page.
LOG-10605	The Source Types tab (Configuration > Source Types) is not visible for non-admin users. Workaround: Add 'Read Only Default Admin Group' privileges to the user.
LOG-10581	When a parser associated with a Source Type and Folder Follower Receiver is deleted, no warning message is displayed indicating the dependency. Workaround: None at this time.
LOG-10353	High incoming event rates can have an effect on the indexing rate of the Logger. Workaround: If you notice that indexing is falling behind, decrease the incoming event rates.
LOG-10173	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. Workaround: Disable any banners or configure the SSH server to communicate in a quiet mode.
LOG-10058	Sending events targeted to an IPv6 address on Logger is not supported. The system state is unknown once it happens. Workaround: Restart the "receiver" process.
LOG-10056	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. Workaround: To avoid this problem, do not create receivers with same names as any deleted receivers.
LOG-9658	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." Workaround: Click Restart. No further action is required. However, if you need to increase the storage limit, please contact HP Support.
LOG-9498	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. Workaround: Edit the parser to make it work for the newer headers.

Issue	Description
LOG-9305	Connectors send values of date/time-type fields in the following format: 07/09/0169 09:57:35.000 PST Understanding: This is a format that Logger does not understand. It expects time field values to be in epoch format (long values). Workaround: Convert the time value into epoch time for Logger to be able to process them correctly.
LOG-8790	When the community string contains non-ASCII characters, the SNMP trap sent out displays "??" in the community field. Understanding: This is a UI issue and does not affect SNMP authentication on Logger. Workaround: Avoid using non-ASCII characters in the community string.
LOG-8194	After restoring Logger from a backup configuration, the CIFS share failed to mount because the user name and password fields are empty. Workaround: Edit the setting of the CIFS share and re-enter the username and password.
LOG-6786	Events may be missed when a receiver on Logger is disabled. Workaround: None at this time.
LOG-6209	If the Finished Tasks page (Configuration > Finished Tasks) contains a very large number of entries, the page sometimes takes a while to load or stops loading. Workaround: If the pages stops loading, refresh the browser window to continue loading.
LOG-5024	If the system that Logger backs up its configuration to is reinstalled or its SSH hosts key is changed, the configuration backup fails because the SSH hosts key cannot be refreshed from the Logger UI. Workaround: Log in to the Command Line Interface and delete the entry in the /home/arcsight/.ssh/known_hosts file. Then refresh the config backup configuration.
LOG-4986	If there is an improper tear-down of the peering relationship, Loggers in the relationship might not detect it. Consequently, when you try to reestablish the relationship, it might not succeed. Examples of improper tear-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). Workaround: If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from the peer Loggers before re-initiating the relationship.
LOG-4885	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. To open the Certificates page, type "Cer" in the Take me to search box, and click Certificates in the list. Workaround: Refresh the page to update the list. The deleted certificate is no longer displayed in the list.
LOG-3944	A configuration backup is not successful if the Remote Directory name contains a space. Workaround: Ensure that the Remote Directory name does not contain a space.

Issue	Description
LOG-3156	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. Workaround: None at this time. The feature assumes that importing Logger has the same configuration setup as the exporting Logger.
LOG-2941	The type associated with imported filters cannot be changed from shared to saved search. Workaround: Imported filter types cannot be changed. However, you can copy the filter definition and create a new filter out of it.
LOG-2387	The EPS Out gauge reports a non-zero value even when no Forwarders are enabled. 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.
LOG-2244	A forwarder configured with a filter might not forward events that match the specified end time. Workaround: Extend the end time by one second to ensure that all events are forwarded appropriately.
LOG-370	The Configuration Backup (Configuration > Configuration Backup > Name_of_Backup) and File Transfer Receivers (Configuration > 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. Workaround: The error is written to the log in this case, so use Retrieve Logs page (Configuration > 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.

Connector Appliance

Issue	Description
LOG-12658	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. Workaround: Since this issue occurs when scrolling down the page, maximize the window to prevent the need to scroll.
LOG-12340	If user tries to upload a file that has space in its name to the repositories, an error message will be displayed. Workaround: Remove space from the filename and try to upload again.
LOG-12339	The EPS IN/OUT values for connectors may be displayed as "unknown" in the list of Connectors on the Container page. 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.

Issue	Description
LOG-11732	After backup/restore on L3200 and L3400 appliances, the Connector shows as empty. Workaround: Restart the connector. You can do this from the Manage Connectors tab or from the System Admin Process Status page. To restart the connector from the Manage Connectors tab: 1. On the Manage Connectors tab, click the container in the left side tree. 2. Click the "Send Container Command" icon. 3. Select "Restart" command from the list of commands. When the container restarts, you should see the connector up and running. To restart the connector from the process status pane: 1. Open the System Admin > Process Status. 2. Click the connector and restart it. You should now see the connector up and running.
LOG-11731	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. Workaround: Please contact HP Support for the steps to emergency restore the local connector.
LOG-10029	On Logger Appliances that have integrated Connector Appliances, users cannot access the Connector Appliance module after upgrading to Logger 5.2. 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. Workaround: Assign users who need to access the Connector Appliance module to "Connector Appliance Rights Group".

Dashboards

Issue	Description
LOG-11730	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. Workaround: Rename the other dashboards so that they all have different names.
LOG-9332	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. 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.

General

Issue	Description
LOG-13445	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. Workaround: None at this time.
LOG-13299	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. Workaround: Use Internet Explorer 11, which does not have the issue.
LOG-11659	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. Workaround: If you are installing the SOX v4.0 solution package as the root user, install it last.
LOG-11473	Initial appliance configuration, such as uploading the license, setting the locale, date/time and configuring SAN, could fail if some requirements were not met. Workaround: If needed, configure the Logger's date/time before uploading the license.
LOG-2433	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. Workaround: Wait for the current page to finish loading before clicking another one.

Reports

Issue	Description
LOG-11954	If the underlying Query of a Report changes, then viewing published reports will result in an error. Workaround: None at this time.
LOG-11502	Report Engine logs indicate that MySQL Tables are "Marked as Crashed" and need repair. 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.
LOG-11279	Restoring configuration backup does not preserve the report templates original file ownership and causes report execution without proper templates. Workaround: Follow these steps to fix the permissions. 1. SSH to Logger. (Appliance users should contact HP support for help with this.) Note: In Logger 6.0, SSH can be enabled from navigating to System Admin > System > SSH menu item. 2. Navigate to the following directory, <$ARCSIGHT_HOME>/logger/Intellicus/reportengine/templates/adhoc, where <$ARCSIGHT_HOME> is the directory in which Logger is installed. 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.

Issue	Description
LOG-11137	If a user has privileges to View a Published Report Only, then the report will not be visible in the Report Explorer. Workaround: You can find and view published reports from the Category Explorer instead. To find a published report, open the Category Explorer and navigate to the Saved Reports folder under the report's Category. (The terms "saved report" and "published report" are used interchangeably.)
LOG-10098	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. Workaround: None at this time.
LOG-9860	When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it is copied. Workaround: None at this time. Clicking Copy or Copy as Link will not give you a visual indication that anything has been copied, but you will be able to Paste, as needed.
LOG-9798	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" Workaround: None at this time.
LOG-9620	If a distributed report fails to run in the background against fields that do not exist on the peer Logger, the error message does not clearly indicate the reason. Workaround: None at this time.
LOG-9584	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 create widgets, and the explorers may not work. Workaround: Restart your browser. If that does not work, manually clear the browser cache and delete temporary files.
LOG-9216	Even when report categories are marked Hidden, they might be visible in Explorers and other report-related locations. 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.
LOG-8780	Reports generated using the Web Services API do not contain report titles. Workaround: When generating reports through the Web Services API, ensure that you have entered the Report Title in the Report Editor (otherwise you will only see the Report ID) in the generated report.
LOG-7186	If you 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: 90141 No matching record found: Requested Report Object "xxxxxxxxx" Not Found 90141 No matching record found: The Query Object used as the Datasource could not be fetched from the repository 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. Workaround: Enable global access to all reports, then the user will be able to edit and run all the reports.

Issue	Description
LOG-7165	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. 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.
LOG-6652	In the Firefox browser, the Report Template editor (Reports > Design - Template Styles > Select a template > 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. Workaround: Use the Internet Explorer browser.
LOG-3244	In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report. Workaround: Use the Internet Explorer browser instead.
LOG-3187	The time taken to run a scheduled report is not reported correctly in the Logger user interface. Workaround: None at this time.
LOG-2355	The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report. Workaround: None at this time.
LOG-2350	The default report generated by clicking the hand icon is missing the report name and date. Workaround: Add a Report title to the Report Header section to include the title on the first page of the Report.
LOG-2012	Adding a scheduled report can reset the scan limit field of other reports. Workaround: Check that the scan limit is set as desired before running any report.
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. 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. 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. 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. 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: 1. Cancel the search that automatically starts once you click on a resource (receiver, device, agent severity, or agent type). 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. 3. Run the search with the new Start and End time values.
LOG-9772	The number of events indexed as shown on the Summary page may not match the number of events found when you run a search with the same time range as shown on the Summary page. Understanding: The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different. Workaround: None at this time. Currently, there is no way to specify the search time range in milliseconds.

System Admin

Issue	Description
LOG-11700	Users may be unable to log in after they have been removed from a group. Understanding: Removing all group assignments from a user effectively disables that user account. User accounts not assigned to any group will be unable to log in. Workaround: To avoid disabling a user account when removing the user from a group, check that the user is assigned to the correct groups.
LOG-11205	Some System Administration pages do not render correctly when using Microsoft Internet Explorer 9. Workaround: To use this version of the browser, ensure that Compatibility Mode is set On. This can be found under Tools > F12 Developer Tools > Browser Mode.
LOG-11066	If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues: 1. On the Search page, the Events grid in the search results will be empty for any search, 2. The timestamps with timezone will be shown using GMT, 3. In the Global Summary on the Summary page, the Indexing is reported one hour behind the current time stamp. Workaround: Change the system time zone to something to more specific, such as /America/Los_Angeles.
LOG-9288	The System Admin - FIPS 140-2 page can take several seconds to load. Workaround: None at this time.
LOG-7664	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. Workaround: None at this time.
LOG-1050	Under certain circumstances, users with restricted privileges might still see Device Group and Storage Group names. 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. Workaround: Provide Device Group and Storage Group names that do not reveal internal information.

Upgrade

Issue	Description
LOG-11136	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. Workaround: Please contact HP Support for help with this issue.