Release Notes
ArcSight Logger

Version 5.5

April 22, 2014

ArcSight
An HP Company

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
04/22/14	Logger 5.5	Revision for Logger 5.5 release
03/26/14	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.
09/19/10	Logger 5.0 GA	First Logger - Downloadable Version release.

Contents

ArcSight Logger 5.5

These release notes provide information about the ArcSight Logger 5.5 (L7049) release. Read this document in its entirety before using a Logger installed with this release.

This document covers the following topics:

What's New in Logger 5.5

This section lists the new features and enhancements introduced in the Logger 5.5 release. For details of these features, see the ArcSight Logger 5.5 Administrator's Guide, available from the Protect 724 community at https://protect724.hp.com.

Logger is available in three form factors, as an appliance, as software, and as a virtualized image. A new VM image, Logger for VMware VM, provides software Logger installation files and a preinstalled operating system to enable quick deployment on an ESXi server.

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 release includes the following enhancements:

- Faster search speed for needle-in-a-haystack searches

  Through the use of new super indexes on certain fields, queries for rare values in super-indexed fields are much faster. Furthermore, queries for values that have never occurred in the super-indexed fields return in constant time. Refer to the Logger Administrator's guide for details.

- Improved local and peer searchs

  Improvements in the search engine and user interface enhance the performance and usability of local and peer searches.

- Improved stability

  Fixes for defects and more robust storage engine for reports provide improved stability and reliability.

In addition, this release introduces fixes for a number of bugs. Refer to the "Fixed Issues" on page 16 section of the Release Notes for a complete list of fixes.

Updated User Interface Behavior

Some customers have, with the assistance of Customer Support, completely disabled the Global Summary feature, and not just the Global Summary Persistence functionality that is automatically disabled in this release. If the Global Summary feature is disabled on your Logger, this information applies to you.

The User Interface (UI) automatically adjusts its behavior based on whether the Global Summary feature is enabled on your Logger.

- If Global Summary is enabled, the Summary page is the landing page, and displays summary data.
- If the Global Summary feature was disabled in Logger 5.3 SP1, the Summary page was the default landing page, but displayed no data. After you upgrade to Logger 5.5, this behavior will change.
- If the Global Summary feature is disabled on Logger 5.5 (both newly installed and upgraded systems), the Summary page is not displayed and the Dashboards page is the default landing page. If you re-enable the Global Summary feature, the Summary page is restored and will be the default landing page again.

Supported Platforms

You can install Logger 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. Additional information about installing Logger on VMware is available in the Logger for VMware VM Quick Start Guide.

- 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	• 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 and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first followed by the OS. For example, upgrade from Logger 5.3 SP1 to Logger 5.5 followed by an upgrade from RHEL 6.2 to 6.5.
CPU, Memory, and Disk Space	**For the Trial Version 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) • Temp directory: 1 GB **For the Enterprise Version** • 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 on software Logger is not recommended.
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

These browsers are supported for accessing Logger 5.5:

- **Firefox:** Version ESR 24
- **Internet Explorer:** Versions 9 and 10

For Internet Explorer browsers:

- If you use IE 9, turn on Compatibility View to ensure that Logger user interface displays correctly.
- Enable the SSLv3 or TLSv1 option to access the software Logger user interface. If neither of these options is enabled, you will not be able to connect to the software Logger.

  To access the SSLv3 and TLSv1 settings, in your IE browser, click Tools > Internet Options > Advanced > Scroll down to locate SSL 3.0 and TLS 1.0 under the Security section.

An Adobe Flash Player plug-in is required on these browsers for some of the features, such as Histogram and charts, to work.

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.

You can change the locale when installing Logger or before upgrading to Logger 5.5. Once set, the locale cannot be changed. If the locale is not set, a banner message on your Logger UI is displayed. If you have not yet configured the locale, you can do so from the Locale page under the System Admin tab.

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.
- 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.
- The Certificate Alias field for ESM Destinations (Configuration > Event Input/Output > Certificates) cannot contain native characters. Use only ASCII characters in the Certificate Alias field.

- 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)	

- Reports are localized for Japanese only.
- The Report Parameter (Reports > Parameters) and the Template Style (Reports > Templates) fields do not accept native characters.

Logger Documentation

The following documentation is available for this release:

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 Help 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.

Logger Web Services API Guide — Available for download from the ArcSight Product Documentation community at https://protect724.hp.com.

Logger Getting Started Guide — Applicable for new Logger appliance installations. 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 for VMware VM Quick Start Guide — Applicable for installing Logger on VMware VM. Provides a high-level understanding of Logger and helps you install it on VMware. Available for download from the ArcSight Product Documentation community at https://protect724.hp.com.

Upgrade Paths to 5.5

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. Upgrade for these appliances will be supported in an upcoming Logger release.

A tool to determine whether your appliance can be upgraded to version 5.5 is available from the same location you get the upgrade files.

The following table lists the upgrade paths to Logger 5.5:

Upgrade Paths to 5.5	
Logger Appliance	
Most common upgrade paths	3.0 GA (L3308) -> 3.0 SP1 (L3393) -> 4.0 SP1 Patch 1 (L_2c-4265) -> 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).
Other upgrade paths	• 3.0 SP1 Patch 1 (L3406) -> 4.0 SP1 Patch 1 (L_2c-4265) -> Follow the upgrade path as described in the “Most common upgrade path” • 4.0 GA (L4105) -> 4.0 SP1 Patch 1 (L_2c-4265) -> Follow the upgrade path as described in the “Most common upgrade path” • 4.0 SP1 (L4248) -> 4.0 SP1 Patch 1 (L_2c-4265) -> Follow the upgrade path as described in the “Most common upgrade path” • 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”
Software Logger	
Most common upgrade paths	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)
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” • 5.2 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”
Notes	
• If you need to upgrade a 3.0 GA or earlier Logger, refer to the release notes of the version you are upgrading to or contact HP Support. • You cannot upgrade the 4.5 GA installation of software Logger. • The following Logger appliance releases were interim versions that you should not upgrade to any longer: 3.0 Patch 1 (L3353), 4.0 SP1 (L4248), 5.0 Patch 1 (L5215). Instead, upgrade to the closest release version listed in the Most Common Upgrade Paths above. • Logger 5.0 Patch 3 release is only available on some Logger appliances shipping from HP.	

Upgrading to 5.5 (L7049)

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

Note

Be sure to review the "Known Issues" on page 15, "Fixed Issues" on page 16, and "Open Issues" on page 21, before upgrading your Logger.

Logger Appliance

Refer to the "Upgrade Paths to 5.5" on page 9 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. On a Logger appliance, you can also click the **System Admin** tab, then click L**icense & System Update** and look for the `arcsight-logger` component.

Prerequisites

If you have an older appliance, run the Logger 5.5 Upgrade Check tool to confirm whether you can upgrade the appliance to Logger 5.5. See "Upgrade Paths to 5.5" on page 9 for more information.

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.

Upgrade Instructions

To upgrade your Logger appliance:

1. Download the `logger-7049.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.
2. Click **System Admin** > **License & Update**.
3. Browse to the `logger-7049.enc` file you downloaded in the previous step and click **Upload Update**. The ArcSight Appliance Update page displays the update progress.

   Once the upgrade is complete, Logger reboots automatically.

Note

If you encounter a page that asks to upload a license and set the time zone at this stage, contact Customer 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 Customer 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 "Connecting to Logger Using SSH" in the ArcSight Logger 5.5 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 to 5.5” on page 9 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.

Prerequisite

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.

Upgrade Instructions

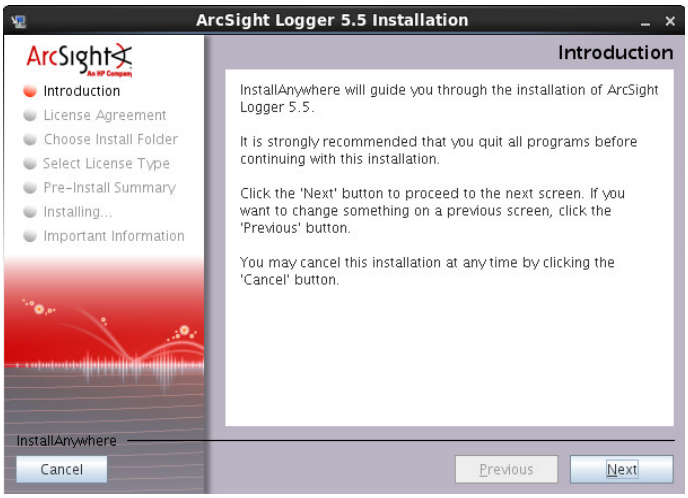
> **Note** If you are planning to upgrade your current OS and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first followed by the OS.

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. Download the 5.5 software Logger upgrade file.
3. Run these commands from the directory where you copied the Logger software:

```
chmod +x ArcSight-logger-5.5.7049.0.bin
./ArcSight-logger-5.5.7049.0.bin
```

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



5 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.

6 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.

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

8 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 installation, or click or **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.

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

10 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.

11 If Logger is already installed at the location you specify, a message is displayed. 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**.

Installation 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 upgrade Logger.

The upgrade may take a few minutes. Please wait. Once the upgrade 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 5.5. Refer to the Logger 5.5 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

Fixed Issues

Logger 5.5 includes the fixes listed in the following tables.

Analyze/Search

Issue	Description
LOG-12058	When many queries were executed it was possible to run out of threads in the server, thus causing the Logger process to die. FIX: The search process has been fixed so that it does not create too many threads.

Dashboards

Issue	Description
LOG-12139	Monitor dashboard graphs did not support durations that were longer than a week. FIX: Logger now supports the following additional durations for the Monitor dashboard graphs: 30 days, 90 days, and 365 days. Also, Daily and Weekly have been renamed to 24 hours and 7days respectively.

Event Input/Output

Issue	Description
LOG-12481	On software Loggers, the warning message displayed when the limits specified in your license were exceeded told you only that you would be unable to search and run reports if you exceed your license limits more than the <maximum-violations> within the <violation days> period. It did not explain that all search related features, including forwarding, are disabled. The Logger Administrator's Guide did not clarify this either. FIX: Now, the warning message and the Logger Administrator's Guide both explain that all search features, including forwarding, are disabled if you exceed your license limits more than the <maximum- violations> within the <violation days> period as stated in your license.
LOG-12305	ESM destinations failed if configured with passwords that contained the symbols % (percent), = (equal to), ; (semi-colon), " (double quote), ' (single quote), < (less than), or > (greater than). This happened because even though ESM passwords may contain those characters, Logger passwords may not. FIX: Updated the Logger Administrator's Guide to explain that when adding an ESM destination, you must first ensure that the ArcSight Manager's password does not contain those characters.

General

Issue	Description
LOG-10115	Trying to reboot Logger through the user interface was unsuccessful because the connector process was hung. FIX: You can now reboot through the the user interface even if the on-board connector is unresponsive.

Logger Appliance Platform

Issue	Description
LOG-11854	Attempting to create an NFS mount via the user interface times out. FIX: This update extends the timeout for mount requests from three to nine seconds.

Peer Logger

Issue	Description
LOG-12052	When a user configured greater than 5 peers and then attempts to search or report across those peers, performance was degraded. FIX: Increased the number of connections for peers from 5 devices to 20.

Reports

Issue	Description
LOG-12309	The Logger Administrator's Guide included a screen capture of a custom report at the beginning of the section on designing reports. This is confusing because we say to start with a pre-defined report. FIX: Updated the image to show a predefined report.
LOG-12119	Possible MySQL corruption when running reports in Logger. When attempting to run a report, the following warning banner sometimes occurred: "There was a problem configuring the report engine user rights. Please check that the report engine process is running successfully." When checked, the ReportEngine.log reported table corruption. FIX: Converted the MySQL used by the Report Engine from ISAM to InnoDB format to help prevent this issue.
LOG-11755	After an upgrade from 5.3 to 5.3 SP1 the user was unable to access the default Dashboards page of the Reports tab in the UI. FIX: This was due to file permission issues that have been resolved.
LOG-11586	Accessing the Reporting user interface is very slow. FIX: Updated the Reporting filter mechanism to speed up performance.

Scheduled Jobs

Issue	Description
LOG-11812	When saving a scheduled report where the name has a slash "/" in it such as "Login Success and Failure - Unix/Linux", it creates the report job silently even though it states the slash is an invalid character for a report name. Then when looking in the list of scheduled jobs, the report job is not listed; however, it runs against the report originally chosen. The only way to stop the hidden report job is to delete the report, which causes the scheduled job to fail, or to restart the web process or all the Logger related processes. FIX: Logger now checks the report job name before creating the job so that there will be no hidden report job created when the job is failed to save.

Search

Issue	Description
LOG-12513	After running multiple searches or auto-refreshes on the Search page for a long time (about a week, but it depends on the machine's specification), the Search page became unresponsive. This happened because when the new search started, the previous search was not cleaned up properly and took some amount of memory in Logger. Therefore, after running a large number of searches, the Logger's web process could run out of memory and the Logger user interface could become unresponsive. FIX: Logger now cleans up non-active searches properly whenever a new search starts.
LOG-7366	The Search user interface displayed a pause (grey circle) icon next to the Fields dropdown while searching, especially for peer searches. However, it was not clear to the user that the search had paused. Instead, it gave the impression that the search had completed. FIX: The Search user interface no longer displays the pause icon while searching. Instead, it continues to display the searching icon.

Software Logger

Issue	Description
LOG-11345	The Software Logger PCI Compliance Insight Package (CIP) installer is not supported console mode FIX: The Software Logger PCI Compliance Insight Package (CIP) installer now supports console mode.

Summary

Issue	Description
LOG-9829	When you drilled down from the Summary page, the time range that the search query ran with was not exactly the same as the one shown on summary page. Therefore, the event counts were not always the same in both places. Understanding: This happens because the time range on the search page is calibrated in seconds, while the time range on the summary page only handles milliseconds. FIX: The time range used when performing the drill-down search from the Summary page was adjusted so that the hit count by the drill-down search closely matches the count on the Summary page.

System Administration

Issue	Description
LOG-12312	The Logger documentation did not mention that polling system health event information from Logger requires the community string. Neglecting the community string while polling the MIB will result in a 'connection timeout' error. FIX: Added information regarding the community string to the Logger Administrator's Guide.
LOG-12311	The Logger documentation did not explain that SNMP polling supports walk operations. FIX: Added information about SNMP walk operations to the Logger Administrator's Guide.
LOG-12310	The Logger Administrator's Guide documented Device Event Class ID: platform:204, which was not implemented. FIX: Removed unused Device Event Class ID: platform:204 from the documentation.
LOG-12308	The documentation did not explain that you need to in order to multipath SAN connectivity to the appliance, you need to make sure that the multipathd service is configured to start on boot. FIX: Added more information on how to set up multipath SAN connectivity to the Logger Administrator's Guide.
LOG-12307	The Device Event Class ID of the system health event Disk /Monitor/Disk/Space/Remaining/ was documented incorrectly in some places in the Logger Administrator's Guide. FIX: Updated the Logger Administrator's Guide to include the correct Device Event Class ID: Disk /Monitor/Disk/Space/Remaining/Root disk:101 in all locations where it is mentioned.
LOG-11818	Re-generating a self-signed certificate or installing a CA-signed certificate could result in an error. FIX: Re-generating self-signed certificates and installing CA-signed certificates now both work as expected.
LOG-10251	When adding a CIFS share, the tooltip for the Location field was not correct. FIX: The tooltip for the CIFS share Location field has been corrected to show valid location examples.

UI/Browser Issues

Issue	Description
LOG-12482	User was unable to open the Logger UI after a successful installation. Understanding: This can happen if Logger's publicly-accessible ports are not allowed through your firewall. FIX: Added a note to the Logger Administrator's Guide explaining that you must ensure that Logger's publicly-accessible ports are allowed through any firewall running on the system where Logger is installed.

Upgrade

Issue	Description
LOG-12076	Upgrading to Software Logger from 5.3 SP1 to 5.3 SP1 6847 with Logger Hotfix 11413 deleted the ArcSight Management Center Agent process. FIX: The ArcSight Management Center Agent process is present and running as expected after you upgrade to Logger 5.5.

Open Issues

Logger 5.5 includes the open issues listed in the following tables. Use the noted workaround where one is available.

Analyze/Search

Issue	Description
LOG-12577	When the user searches with a chartable query such as "rare deviceEventClassId | sort - _count | where _count >88", and drills down from the search result's chart by clicking a bar (or a clickable chart element), the resulting (non-chartable) query generated by the drilldown is invalid. This happens because the "_count" field cannot be used in searches without any chart result. Workaround: Remove _count from the query term resulting from a chart drill down.
LOG-12542	The Go button on the Search page may disappear after you cancel a search and then click the histogram. Workaround: Reload the Search page by clicking F5 or CTRL + R to reset the search status.
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".
LOG-12522	Using chart functions over user-defined fields, such as when a field is specified with the rex command, will fail if the type of the user-defined field is not numeric. The following example will fail because "Number" is not a numeric field. _deviceGroup in ["localhost [file receiver LOG-12522 2014020701]"] |rex ".gif\s(?<Number>[^$]{4})"\|eval (bigint)N=Number\|eval Number=N+3\|Chart sum(Number) as sum by Number Workaround: Use the "eval" command to make another field with a strong type, such as bigint, and then apply chart functions over that field. The following example will give the correct result. _deviceGroup in ["localhost [file receiver LOG-12522 2014020701]"] \|rex ".gif\s(?<Number>[^$]{4})"|eval (bigint)N=Number|eval N=N+3|Chart avg(N) as sum by Number
LOG-12493	The search results toolbar can become inaccessible after you cancel a search and then click some links or buttons in the search results. You may, therefore, not be able enter a page number and navigate the search results. Workaround: Since the toolbar's loading status is wrong when this issue happens, reload the Search page by clicking F5 or CTRL + R to reset the status.

Issue	Description

LOG-12343	Logger Web service searches that include | regex "," or other special characters could cause an exception when the events in the search results contains special characters such as ì<>î. This is happens because the Logger Web service cannot handle the special characters in the transported events without proper encoding.
	Workaround: Turn on base64 encoding on the Logger side and use base64 decoding on the client side.
	To turn on base64 encoding on the Logger side:
	Add the following line in the /userdata/logger/user/logger/logger.properties and /userdata/logger/user/logger/logger_webservices.properties (Create this property file if it does not exist.)
	api.search.base64encode=true
	To use base64 decoding on the client side:
	Add the base64 decoding as shown in the highlighted location in the runSearch() method of the webservice client:
	Tuple[] tuples = searchService.getNextTuples(...);
	for (Tuple tuple : tuples) {
	String[] arr = tuple.getData();
	for(int j=0; j< header.length; j++){
	arr[j] = new String(Base64.decode(arr[j])); // <= Add this line to decode the received string using base 64.
	}
	}

LOG-12290	When searching Logger with a query that includes the rename operator, the original field renamed by the operator is displayed as a column in the search results, but will not have any values, if the original field name is part of the Fieldset applied for 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 the field that the user wants to rename from the Fieldset.
LOG-12222	If the user drills down from a chart generated from a query that uses both the chart and rename operators, then the new search created by the drilling down will fail. Workaround: Since this issue is caused by the rename operator, remove the rename term(s) from the query.
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.

Issue	Description
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-11294	When a user- defined rex field name contains a space, an error message shows up and the field summary is not displayed. Understanding: The rex operator does not support spaces in user-defined field names. Workaround: Do not include spaces when defining rex field names.
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 "\ "/ "["] ",
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.

Issue	Description
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 10 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.
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-7758	When the eval operator is used 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.) Workaround: Since using eval the after the chart operator causes this issue, use the eval before the chart operator, if possible.
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.

Issue	Description
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 on/off the multiline support search.multiline.fields.supported=true - To on/off the \\n and \\t support search.double.backslash.newlines.supported=false - To on/off the DOS/Windows path support for CEF and/or syslog 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
LOG-6965	When the time change due to Daylight Savings Time (DST) takes place, 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.

Issue	Description
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.
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.
LOG-1384	The Save to Logger operation overwrites an existing file of the same name. Workaround: Use unique file names when using the Save to Logger operation.

ArcSight Console

Issue	Description
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.

Configuration

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 > Event Input > 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: To work around this issue, 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 has "??" 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 > Scheduled Tasks > 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 SSL key is changed, the configuration backup fails because the SSL 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 (power 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	After a certificate is deleted from these pages, the deleted certificate is still displayed in the list, leading to an impression that the certificate is still loaded on the system: Configuration > Event Input/Output > Certificates Configuration > Alerts > Certificates 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 > Event Input/Output > 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-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".

Content Import and Export

Issue	Description
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.

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.

Issue	Description
LOG-11223	If the index is slightly behind, drilling down on the receiver may return no results. Workaround: Change the end time of the query to be slightly earlier (usually only a couple minutes) to obtain the results.
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.

Logger Appliance Platform

Issue	Description
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.

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.) 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.
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.)

Issue	Description
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.
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.

Issue	Description
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-11698	On Logger's Summary page and custom Logger Dashboards, the user's session will not time out. This is because any panel that updates the contents automatically extends the user's session. Workaround: Since Search Results panels do not refresh automatically after completing the search, if a custom dashboard has only Search Results panels, then the user's session will be able to time out after completing all the searches in the dashboard. Since the Summary and Dashboards pages auto-update the contents automatically, to take advantage of the auto-timeout feature, the move to a page that does not auto-refresh, such as the Search page.

Issue	Description
LOG-10084	The Count value displayed on the Summary page may be slightly different from the Hit value on the Search page for the same field. Understanding: These differences can occur for various reasons including the following: 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. 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. Workaround: None at this time.
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 Administration

Issue	Description
LOG-11712	Certificates that have spaces in their names do not work correctly. If you click the link to view the details of the certificate, the certificate appears to have no content. After you try to delete that certificate, it still remains in the list of certificates. Workaround: Instead of spaces, use underscores in the Certificate Alias so that the certificate can be viewed and removed properly.
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.

Issue	Description
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 multipath 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.

UI/Browser Issues

Issue	Description
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.

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.
LOG-8638	During an upgrade, you are asked to reboot the appliance and then select a Locale. Once the locale is saved, you see following message: "Locale is saved. System Reboot required to apply settings". The System Reboot should be a link that loads the Reboot page. However, the displayed message does not show it as a link but if you click the System Reboot text, it does take you to the Reboot page. Workaround: This bug affects Internet Explorer 7 and older versions of Internet Explorer 8. Clear the browser cache (on IE: Tools -> Internet Options -> Delete...) before going to System Locale page (and after rebooting the appliance).