

Release Notes HP ArcSight Logger™

Version 5.3

April 11, 2013



Release Notes HP ArcSight Logger™, Version 5.3

Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

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

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

This document is confidential.

Revision History

Date	Product Version	Description
04/11/13	Logger 5.3	Added notice about Global Summary Persistence issue.
09/27/12	Logger 5.3	5.3 GA.
02/10/12	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.
07/22/10	Logger 4.5 GA	Version 4.5 GA release. First software-only version option for Logger.

Release Notes template version: 2.1.0

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.arcsight.com

Contents

HP ArcSight Logger™ 5.3 5

 Important Notice 5

 What's New in 5.3 6

 Supported Browsers 9

 Converting a Single Path LUN to a Multipath LUN 10

 Localization Information 11

 Logger 5.3 Documentation 12

 Documentation Errata 12

 Upgrade Paths to 5.3 14

 Upgrading to 5.3 (L6684) 15

 Fixed Issues 21

 Open Issues 31

HP ArcSight Logger™ 5.3

These release notes provide information about the HP ArcSight Logger 5.3 (L6684) release. Read this document in its entirety before using a Logger installed with this release.

This document covers the following topics:

- [“Important Notice” on page 5](#)
- [“What’s New in 5.3” on page 6](#)
- [“Supported Browsers” on page 9](#)
- [“Converting a Single Path LUN to a Multipath LUN” on page 10](#)
- [“Localization Information” on page 11](#)
- [“Logger 5.3 Documentation” on page 12](#)
- [“Documentation Errata” on page 12](#)
- [“Upgrade Paths to 5.3” on page 14](#)
- [“Upgrading to 5.3 \(L6684\)” on page 15](#)
- [“Fixed Issues” on page 21](#)
- [“Open Issues” on page 31](#)

Important Notice

HP ArcSight has identified an issue with the global summary persistence functionality added in this release (See [“Global Summary Persistence” on page 8](#)). This feature enables the statistics reported in the global summary section of Logger to persist through a reboot. The HP ArcSight Support team has seen incidents where disk space has been affected due to the persistence behavior. We recommend that you upgrade to Logger 5.3 SP1 as soon as possible, to turn this feature off.

What's New in 5.3

This section lists the new features and enhancements introduced in the Logger 5.3 release. **See the *Logger 5.3 Administrator's Guide* for details of these features**, which is available at the HP Customer Support site at <http://support.openview.hp.com> or at the Protect 724 community at <https://protect724.arcsight.com>.

In addition, this release introduces fixes for a large number of bugs. See *"Fixed Issues"* on [page 21](#) for a complete list of fixes.

If you have an L3XXX model Logger (an integrated Logger and Connector Appliance product), refer to the Connector Appliance 6.3 Release Notes for additional information about the Connector Appliance functionality.

Improved Installation Workflow

To reduce initial setup time and make the initial configuration more intuitive, following improvements have been made to the appliance and software workflows:

- Smaller software Logger installation file for easier delivery and shortened download time
- Simpler and fewer installation steps for faster installation
- More default and automatically configured setup parameters
- Enhanced user interface text and messages for clarity and understanding
- Out-of-the-box configuration settings, such as preconfigured receivers for improved time to value
- Ability to enable collection of Logger's internal logs as event data

The updated workflows are documented in the *Logger 5.3 Administrator's Guide*.

Virtual Form Factor for Logger Appliance

You can now deploy Logger on an instance of Hyper-V on Windows Server 2008 R2. The Hyper-V installation of Logger comes integrated with the following three connectors, which you configure during the installation process:

- Microsoft Audit Collection System
- Microsoft System Center Operations Manager
- Microsoft System Center Operations Manager 2005 and 2007

Similar to other form factors of Logger, a valid license is required to install Logger on Hyper-V.

For more information, see *Logger 5.3 Quick Start Guide for Hyper-V*.

Chart and Dashboard Drill Down

To enable deeper analysis of charts and dashboards, Logger introduces the chart and dashboard drill down feature. This feature enables you to quickly filter down to events with specific field values. You identify the value on a search results chart and click it to drill-down to events that match the value.

For more information, see *"Chart Drill Down"* in the *Logger 5.3 Administrator's Guide*.

Automatic Parsing Based on Source Types

Logger 5.3 provides the ability to parse raw events (unstructured, non-CEF) received from any event source on your network. The event source can generate discrete events or log files. The unstructured, textual event data is parsed into specific fields (according to the parser definition), just like the CEF data. Once parsed, you can specify these fields to perform search operations and charting, just like you would use CEF fields. The search results display the parsed fields as columns, similar to CEF field columns. However, the parsed fields are available only for search operations, and are not added to the Logger schema.

Logger provides a number of preconfigured parsers for common source types such as Apache and VMWare ESX. If you want to send events from such a source type, you only need to define a receiver on Logger to receive the event data. You can also define custom parsers and source types for event sources in your network.

Once a parser is defined and associated with a source type, parsing occurs automatically on event data received through file receivers—file receivers, file transfer receivers, and folder follower receivers. Additionally, a new operator, `parse`, has been introduced in this release for on-the-fly parsing of events received from TCP or UDP receivers on Logger and any data stored on Logger version 5.2 or earlier, when the parser feature did not exist. You can also use the `parse` operator to override the parser associated by default with an event that came from a known source type.

For more information about parsers and source types, see the topic “Parsers” in the *Logger 5.3 Administrator's Guide*.

Folder Follower Receivers

Logger can now monitor active textual log files, as they are updated, using a new receiver type—Folder Follower receiver. Once a Folder Follower receiver is configured on your Logger, it monitors files in a specified directory and continuously uploads new events to Logger. Folder follower receivers recognize file rotation.

When you use this receiver in conjunction with the parsing feature, you can continuously upload and monitor log files from servers in your network.

Logger comes preconfigured with Folder Follower receivers for Logger's Apache URL Access Error Log on appliance and the software Logger, and the system Messages Log and Audit Log (when auditing is enabled) on the software Logger. You must enable these receivers to use them.

Folder Follower receivers are designed to read textual log files only; therefore, make sure that the input directory does not contain binary files.

For more information about folder follower receivers, see “Folder Follower Receivers” in the *Logger 5.3 Administrator's Guide*.

Improved System Filters Content

Your Logger ships with a number of predefined filters, also known as system filters. These filters define queries for commonly searched events. Filters for Windows-related events have been updated to include Windows 2003 and Windows 2008 formats.

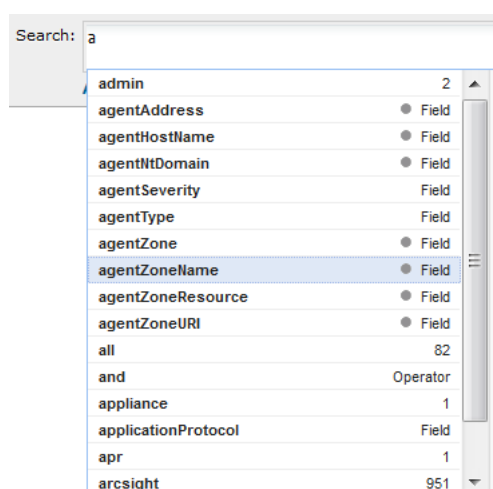
Managing In-progress Search Jobs

A newly introduced Running Tasks page (Configuration > Search > Running Tasks) displays any active search jobs on Logger. Additionally, you can now end an active job if it is taking too long to run, or appears to be stuck and slowing the overall Logger performance. Only users with admin-level privileges can end a running search job.

For more information, see “Ending Currently Running Search Tasks” in the *Logger 5.3 Administrator's Guide*.

Enhanced Search AutoComplete Function

The search autocomplete function has been enhanced in this release to include matching full-text keywords and field values for Logger schema fields based on the currently entered text, as shown in the following figure.



Enhanced WHERE Operator

The search WHERE operator has been re-implemented in this release to improve search performance significantly.

Enhanced Reports and Report Categorization

New reports for Netflow data, such as bandwidth monitoring, are now available by default now. Additionally, the existing reports have been organized in intuitive categories.

Global Summary Persistence

The global summary data available on the Summary dashboard now persists across reboots and upgrades.



HP ArcSight has identified an issue with the global summary persistence functionality introduced above. We recommend that you upgrade to Logger 5.3 SP1 as soon as possible, to turn this feature off. See [“Important Notice” on page 5](#) for more information.

UI Enhancement and Change

Following UI enhancements and changes were introduced in this release:

- The Event Input/Output menu, under Configuration in the top-level menu bar, has been separated into two menu options—Event Input and Event Output. The Event Input menu includes these tabs: Receivers, Source Types, and Parsers. The Event Output menu includes these tabs: Forwarders, ESM Destinations, and Certificates.
- The search results table provides a new option, Events per page, to select the number of events to show on a page. By default, 25 is selected. Other options include 10, 50, and 100.
- The “Search Optimization” menu item in the left panel (under Configuration) has been renamed to “Search” to be in-line with the search-related configuration settings you can configure.

System Administration Enhancements

The following system administration related enhancements were made in this release:

- Ability to use LDAP over SSL authentication method
- Redesigned UI screen for external authentication methods to improve user experience
- An expanded list of protocols for RADIUS are supported—CHAP, EAP-MD5, MS-CHAPv2, PAP
- Ability to specify an alias for a network interface card (NIC) on Logger appliance
- Ability to use the License & Update page to apply a new license on the software Logger
- Uniform look and feel for the Login screen on the appliance and software Logger
- Option to specify additional attributes such as Fax and Alternate Number when creating a user account to capture additional information for the user
- Ability to configure software Logger to start as service after initial setup is complete

Supported Browsers

For this release, these browser versions are supported for accessing Logger's user interface:

- Internet Explorer: Versions 8 and 9
- Firefox: Versions 12 and 13



For IE browsers, make sure that:

- You turn on Compatibility View if you use IE 9 to ensure that Logger user interface displays correctly.
 - The SSLv3 or TLSv1 option is enabled to access the software Logger user interface. If none of these options are 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.
-

Converting a Single Path LUN to a Multipath LUN

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 ArcSight 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 *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 steps 5 and 6 until the multipath devices are correctly listed.
  - 8 Run this command:
- ```
./mpath_enable.sh <path_to_your_multipath.conf>
```
- 9 Reboot your appliance.

Localization Information

Localization Support

Localization support for these languages is available for Logger:

- Japanese
- Traditional Chinese
- Simplified Chinese

You can install Logger in one of the above languages either as a fresh install or upgrade an existing English installation to one of these languages.

You can set the locale when freshly installing Logger or before upgrading to Logger 5.3. Once set, locale cannot be changed. If locale is not set, a banner message on your Logger UI is displayed.

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.
- 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, on the Search Results page
- 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.
- Reports are currently localized for Japanese only.
- The Report Parameter (Reports > Parameters) and the Template Style (Reports > Templates) fields do 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.

Logger 5.3 Documentation

The following documentation is available for this release:

- Administrator's Guide—Available for download from the HP ArcSight Product Documentation community at <https://protect724.arcsight.com>. This link is also accessible from the integrated online Help.
- Online Help—Integrated in the Logger product and accessible through the Logger user interface. To access the online Help, click Help on any Logger user interface page to access context-sensitive Help for that page.
- WebServices API Guide—Available for download from the HP ArcSight Product Documentation community at <https://protect724.arcsight.com>.
- 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 HP ArcSight Product Documentation community at <https://protect724.arcsight.com>.
- Quick Start Guide for Software Logger—Applicable for new software Logger **Downloadable Version** installations, which are downloaded through the HP Software Depot at <http://software.hp.com>. This guide is the first document to use to understand software Logger in a nutshell and install it.
- Quick Start Guide for Hyper-V Logger—Applicable for installing Logger on a **Hyper-V** instance. This guide is the first document to use to understand Logger in a nutshell and install it on Hyper-V.

Documentation Errata

In the Audit Log appendix of the *Logger 5.3 Administrator's Guide*, the following audit log event is listed under Storage Volume. Instead, it should be listed under Syslog Destinations.

Device Event Class ID	Message	Device Event Category (cat)	Additional Fields
Syslog Destinations			
logger: 647	Syslog destination [name] has been added	/Logger/Resource/SyslogDestination/Configuration/Add	fname=syslogDestinationName duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Syslog Destination fileId=syslogDestinationId dvc=syslogDestinationIp dvchost=syslogDestinationHost cn1Label=Syslog Destination Port cn1=syslogDestinationPort

In the Audit Log appendix of the *Logger 5.3 Administrator's Guide*, the audit log events listed in the Loggers section are incorrect. Instead, they should be included in a Peer Loggers section and described as follows.

Device Event Class ID	Message	Device Event Category (cat)	Additional Fields
Peer Loggers			
logger:570	Peer Logger authorization [name] has been added	/Logger/Resource/PeerLogger/Authorizations/Configuration/Add	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger Authorization
logger:571	Peer Logger authorization [name] has been deleted	/Logger/Resource/PeerLogger/Authorizations/Configuration/Delete	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger Authorization fileId=LoggerId
logger:550	Peer Logger [name] has been added	/Logger/Resource/PeerLogger/Configuration/Add	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger fileId=LoggerId
logger:551	Peer Logger [name] has been deleted	/Logger/Resource/PeerLogger/Configuration/Delete	fname=Name duser=UserName duid=userId cs4=sessionIdfile cs4Label=Session ID fileType=Peer Logger fileId=LoggerId

Upgrade Paths to 5.3

The following table lists the upgrade paths available to Logger 5.3.

Upgrade Paths to 5.3	
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)
Other upgrade paths	<ul style="list-style-type: none"> 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)
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)
Other upgrade paths	<ul style="list-style-type: none"> 5.0 Patch 1 (L5215) -> 5.0 Patch 2 (L5355) -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 HotFix (L6295) -> 5.2 Patch 1 (L6307) -> Follow the upgrade path as described in the "Most common upgrade path" 5.2 GA (L6288) -> 5.3 GA (L6684)
Notes	
<ul style="list-style-type: none"> 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 ArcSight. 	

Upgrading to 5.3 (L6684)

Logger Appliance

Refer to the “[Upgrade Paths to 5.3](#)” on [page 14](#) section for the supported upgrade paths for your Logger.



To determine your current Logger version, hover the mouse 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 **License & System Update** and look for the `arcsight-logger` component.

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

To upgrade your Logger appliance:

- 1 Download the `logger-6684.enc` file from the HP Customer Support site at <http://support.openview.hp.com> to a computer from which you connect to the Logger UI.
- 2 Click **System Admin > License & Update**.
- 3 Browse to the `logger-6684.enc` file you downloaded in the previous step and click **Upload Update**. The ArcSight Appliance Update page displays the update progress.
- 4 Once the upgrade is complete, you will be asked to reboot Logger.

If you remained connected to the appliance while it was being upgraded, the following message is displayed.

Result of Update: Success
Reboot Required: Yes

IN ORDER FOR THE UPDATE TO TAKE EFFECT, PLEASE REBOOT THE SERVER.

If you disconnected, the following banner message is displayed after you log in and accept the license agreement.

NOTE: The system has recently been updated and a reboot is required.

Use the **Reboot** page to restart the appliance.

- 5 Click the **Reboot** link in the message to display a page with the “Start Reboot Now” button, and then click **Start Reboot Now**.



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

Software Logger

Refer to the [“Upgrade Paths to 5.3” on page 14](#) section for the supported upgrade paths for your Logger.

If you are installing software Logger as a fresh install, refer to the *Logger 5.3 Administrator's Guide* for information.

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.

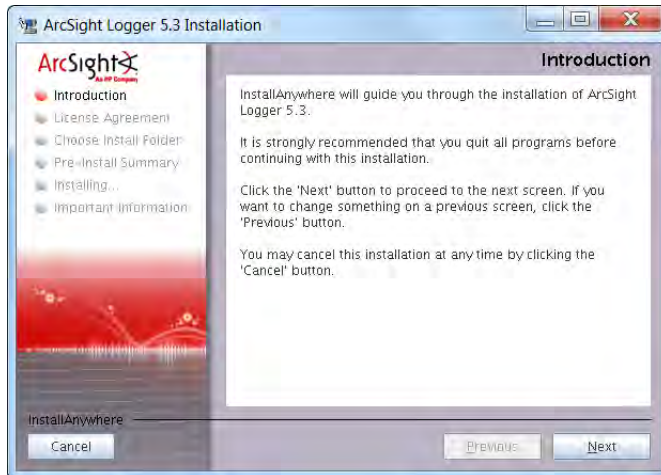
Upgrade Instructions

To upgrade your software Logger:

- 1 Ensure that you are logged in with the same user name as the one used to install the previous version of software Logger.
- 2 Download the 5.3 software Logger upgrade file.
- 3 Run these commands from the directory where you copied the Logger software:

```
chmod +x ArcSight-logger-5.3.0.6684.0.bin
```

```
./ArcSight-logger-5.3.0.6684.0.bin
```
- 4 The installation wizard launches, as shown in the following figure. This wizard also upgrades your software Logger installation. Click **Next**.



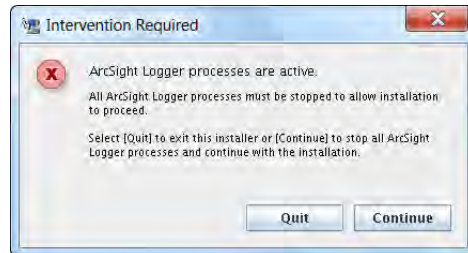
You can click **Cancel** to exit the installer at any point during the upgrade process.



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.

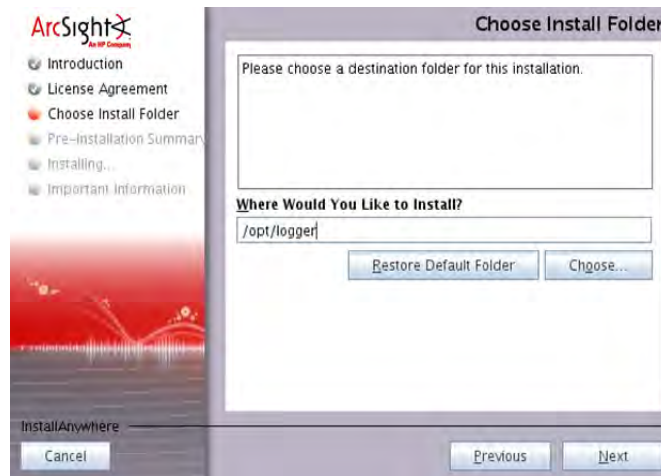
- 5 The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the “I accept the terms of the License Agreement” button.

- 6 Select **I accept the terms of the License Agreement** and click **Next**.
- 7 If Logger is currently running on this machine, an Intervention Required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the installation, or click or **Quit** to exit the installer.



The installer stops the running Logger processes and checks for other installation prerequisites. A message is displayed asking you to wait. Once all Logger processes are stopped and the checks complete, the next screen is displayed.

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



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

- 10 If Logger is already installed at the location you specify, a message is displayed. Click **Upgrade** to continue or **Back** to specify another location.



Note

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

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



- 12 Installation may take a few minutes. Please wait.

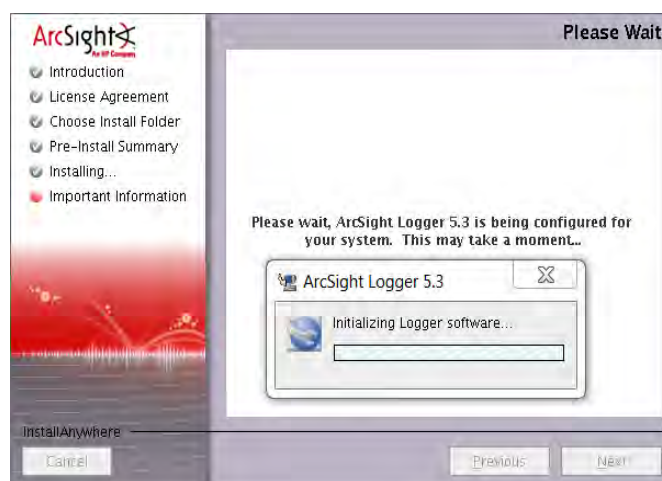


Once installation is complete, the next screen is displayed.

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

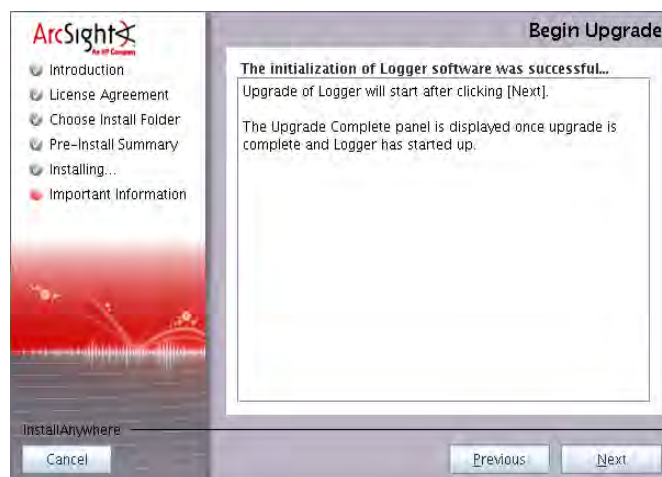


Initialization may take a few minutes. Please wait.

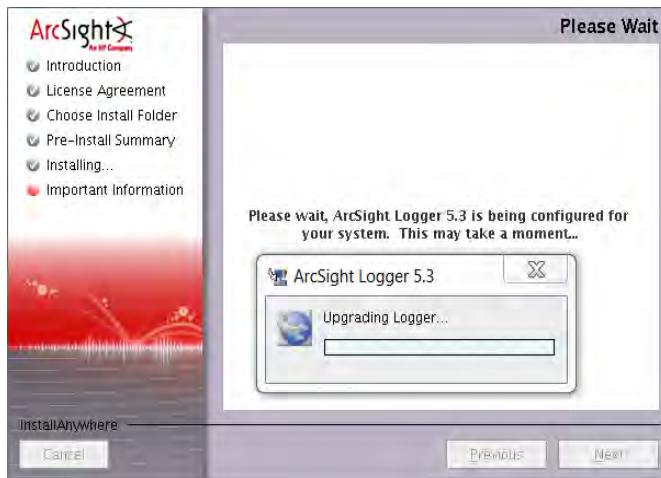


Once initialization is complete, the next screen is displayed.

14 Click **Next** to upgrade Logger.

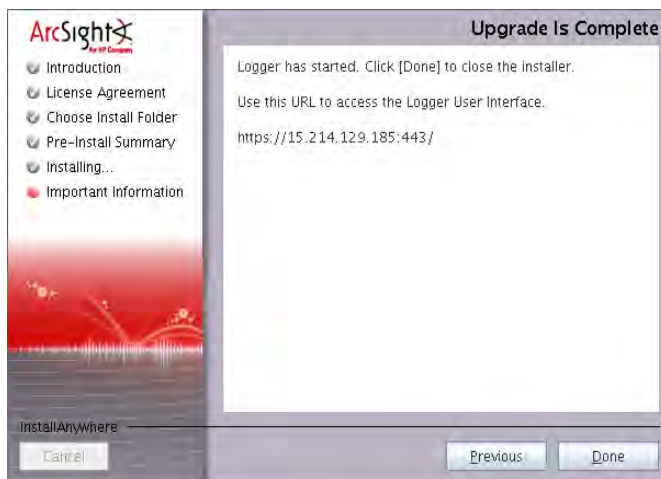


The upgrade may take a few minutes. Please wait.



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.

Fixed Issues

Analyze/Search

Issue	Description
LOG-10984	<p>Export jobs did not release the reference to the result of retired search sessions.</p> <p>FIX: Logger now cleans up export jobs after running them.</p>
LOG-10258	<p>Searching on a peer Logger was very slow when a search group filter was applied.</p> <p>FIX: This issue has been mitigated in this release of Logger. Search performance is not compromised when a search group filter is applied to peer search.</p>
LOG-10246	<p>A field that was renamed using the RENAME operator could not be used in the "by" clause of the chart operator. For example, rename priority as new_priority chart _count by new_priority resulted in an error.</p> <p>FIX: Fields that have been renamed no longer cause an error when used in a "by" clause.</p>
LOG-10129	<p>The rename operator failed to rename a CEF field unless the original field appeared in a cef operator.</p> <p>FIX: The rename operator now correctly renames CEF fields when the original field does not appears in a cef operator.</p>
LOG-10128	<p>Data for specific time fields was exported in epoch time format.</p> <p>FIX: Data for the following time fields is now exported in human-readable format: deviceReceiptTime, startTime, endTime, agentReceiptTime.</p>
LOG-10122	<p>When using a rex operator with the clause "field=<field name>", you could receive an error message that the search cannot be run because of an error in the query.</p> <p>FIX: Running a search when using the rex operator with the clause "field=<field name>" now works properly.</p>
LOG-10038	<p>Duplicate events were sometimes exported from the Live Event Viewer.</p> <p>FIX: Logger now exports from the Live Event Viewer without duplications.</p>
LOG-9752	<p>After exporting the search results of long-run queries many times, an OutOfMemoryError occurred.</p> <p>FIX: Logger now cleans up export jobs after running them.</p>
LOG-9635	<p>Logger 5.2 histograms did not refresh correctly when viewed using Internet Explorer 9 on 64 bit Windows 7 systems.</p> <p>Understanding: Logger 5.2 did not support Internet Explorer 9.</p> <p>FIX: Logger now supports Internet Explorer 9.</p>

Issue	Description
LOG-9626	<p>Search group filter failed when searching for devices.</p> <p>Understanding: This can happen if you set filters from two different places and the filters conflict with each other. In such cases, no event may be returned.</p>
LOG-9236	<p>The built-in search filters did not include Windows 2008 security events.</p> <p>FIX: The built-in search filters for Windows now include Windows 2008 security events.</p>
LOG-9230	<p>Searching with strings that contain special character causes unexpected results.</p> <p>Understanding: When searching for strings that contain these characters-- =, ., :, /, \, @, -, ?, #, \$, &, _ , % --you must specify the first character of the string that occurs after a primary delimiter (space, tab, newline, comma, semi-colon, (,), [,], {, }, ", , *, >, <, !) in the search query. Otherwise, search query will not find the matching event. For example, to search for hp.com in a URL string "... http://www.hp.com", where the URL is preceded by a space (one of the primary delimiters), specify h*hp.com. Specifying, "hp.com" as the search string will not return matching events.</p>
LOG-8998	<p>No results were returned when you selected the User Defined Columns field set and the query included a WHERE operator, which included the fields that were not defined by a preceding CEF operator.</p> <p>FIX: The product has been updated to include user defined columns when validating a search.</p>
LOG-8277	<p>The endTime field showed up in the search results, but was empty in the export file.</p> <p>FIX: The content of the endTime field is now exported properly.</p>
LOG-8264	<p>Search Group filter was not being enforced when searching by devices/device group.</p> <p>FIX: The device group filter settings now work correctly.</p>
LOG-7201	<p>The ampersand character, &, became &; when displayed in Logger web UI.</p> <p>FIX: The ampersand (&) is now displayed correctly.</p>
LOG-6903	<p>Logger user interface did not allow the user to choose more than 25 rows to display in the Search results window.</p> <p>FIX: This release of Logger includes a new feature that allows the user to select the number of events to display (10, 25, 50, 100) from a drop-down.</p>
LOG-6297 TTP#69095	<p>When a where operator was included in a query, the query performance could be significantly impacted. As a result, the query did not always complete and the user interface could hang.</p> <p>FIX: The performance of queries using the where operator has been improved.</p>

Configuration

Issue	Description
LOG-10405	<p>Continuous unified query Forwarder with ESM destination failed unless Full-text indexing was enabled.</p> <p>FIX: Continuous unified query Forwarders now forward events to ESM destination whether or not full-text indexing is enabled.</p>
LOG-9748	<p>When the database required defragmentation and Logger returned a message saying that the required amount of free storage was not available, the logger_server.log reported that the space required to perform the defragmentation was greater than the space the database itself is using (/opt/local/pgsql/data).</p> <p>Understanding: This is as designed. Defragmentation needs additional temporary space while it is running. If you do not have enough space to perform the defragmentation, you can increase the amount of available space by deleting the database indices. If there is still not enough space to perform the defragmentation, or if you chose not to delete the indices, you need to mount additional storage. Contact HP ArcSight customer support for help with this.</p>
LOG-9307	<p>Malformed CEF messages could cause Logger Forwarders to fail.</p> <p>FIX: The product robustness has been increased to handle malformed CEF messages.</p>
LOG-8740	<p>When beginning a maintenance operation, a blank screen was shown for a few seconds while waiting for maintenance mode to start.</p> <p>FIX: Logger no longer displays a blank screen when entering maintenance mode.</p>
LOG-7048	<p>Clicking on Restart or Reboot after performing an action in maintenance mode sometimes caused the following error message to be displayed: "The application is currently unavailable. Please retry shortly."</p> <p>Fix: Logger now displays progress messages while rebooting/restarting after performing an action in maintenance mode. Users no longer need to refresh repeatedly to determine the current status.</p>
LOG-6365 TTP#69487	<p>If a long regex query was entered during Forwarder configuration, it would display with extraneous spaces in the Query column on the Forwarders page. This was a display-only issue; query continued to be correctly run.</p> <p>FIX: The display issue has been fixed.</p>
LOG-5612 TTP#65492	<p>Performance of a time-range bound forwarder was slow when very large amount of data was forwarded through it.</p> <p>FIX: The product has been enhanced to fix performance issues.</p>

Connector Appliance

Issue	Description
LOG-10078	<p>After an emergency restore on a container using connector build 5.1.7.6606, and applying certificate on it, the container showed an incorrect configuration message and continuously restarted.</p> <p>FIX: Containers now behave properly after an emergency restore.</p>
LOG-7239	<p>System health events from Connector Appliance to Logger To ArcSight ESM were not getting forwarded reliably.</p> <p>FIX: The product has been updated to ensure that the health events reach ArcSight ESM reliably.</p>

General

Issue	Description
LOG-9945	<p>After setting Chinese locale, the Logger appliance did not display the values for days of the week when selecting any category in the Monitor tab. Instead, it displayed squares.</p> <p>FIX: Appliances shipping with Logger 5.3 or later will now correctly display Chinese characters in Monitor graphs.</p>
LOG-8823	<p>The UI occasionally displayed the following error message: "The application is currently unavailable. Please retry shortly." This issue occurred when the web process on Logger ran out of memory. When this happened, the logger_web.log log file contained one or many of the following entries: java.lang.OutOfMemoryError: PermGen space.</p> <p>FIX: The product has been updated to remediate the out of memory error.</p>
LOG-8661	<p>During the Console Mode install of a Software Logger, there may a situation where the "Custom code execution" message is printed multiple times. This is limitation in the Install Anywhere script that is used to install the product and is benign in nature.</p> <p>Workaround: You can ignore this message.</p>
LOG-7401	<p>The documentation of devices in auto-discovery was unclear when referring to the Device that sends events to Logger.</p> <p>FIX: The documentation has been updated to clarify that when an event is sent through a SmartConnector the event source is the system on which the SmartConnector is running and not the device that sent the event to the SmartConnector.</p>
LOG-4227 TTP#59302	<p>On Internet Explorer, another Logger browser opened while downloading a zipped version of a report. It did not close after the zip file was saved.</p> <p>Understanding: After the file is downloaded, close the browser page manually.</p>

Issue	Description
LOG-3561 TTP#54435	Documentation did not describe any special requirements for specifying values in the Select Filter Criteria field. FIX: This field does not impose any special requirements thus no documentation update was needed.

Reports

Issue	Description
LOG-10921	A distributed report query that included a non-indexed column as a search result could trigger out of memory errors if one of the columns has empty string. FIX: Distributed report queries now handle empty strings correctly.
LOG-10371	When a device group filter was applied to an admin user and a report was run by another user (with admin or non-admin privileges) and the report included one or more non-indexed fields, the report did not return any events. FIX: The reports appropriately filter out events now instead of filtering out all events.
LOG-10043	On IE 8.x, when you clicked on the Reports menu item in the top-level menu bar, the following error was displayed: "Parent Object not Found". Understanding: This issue is experienced when you have configured your browser to use custom security settings, it may still occur with some security settings. If you encounter this issue either click OK to clear the error message, or update the browser security settings to use the default settings. FIX: The Logger's Reports page is now displayed without the alert message with the most common security settings.
LOG-9950	After a configuration restore is performed on a software Logger, the following error message is displayed when on a report dashboard: "Failed to generate report from rpg because server failed to deserialize the Report Pages". Understanding: Published reports are not included in the configuration backup, hence they are not available upon a restore. To view the report, you will need to either publish the report again or reschedule it to be published.
LOG-9820	The classic Reports Dashboard does not display any sub-categories. Understanding: The classic Reports Dashboard is for backward compatibility. Do not use it for creating new dashboards. Refer to the Logger Administrator's Guide for more information.

Issue	Description
LOG-8913	<p>The DHCP Mac address may not show within Logger report in Mac Address output format, instead it shows as a number value.</p> <p>Understanding: This happens because the output format is not set correctly. To correct the issue, set the output format in the underlying query.</p> <p>To set the output format:</p> <ol style="list-style-type: none"> 1 Select the column and then select Output Format. 2 In the Data Format select Network Id and then select Mac Address. 3 Click OK and then Save the Query.
LOG-8356	<p>Some report queries would not return data reliably.</p> <p>FIX: This issue had no specific symptoms, however, it has not been reproduced in this release of Logger as the reporting engine has been enhanced to run more number of reports concurrently.</p>
LOG-8218	<p>The default reports were missing after uploading Compliance Insight Package Logger ITGov 4.0-4016.</p> <p>FIX: Unable to reproduce this issue in the current release.</p>
LOG-7914	<p>When you ran the "Requirement 8-Windows Account Lockouts by System Report" in v2.1 PCI Compliance package, the results returned did not report on Windows 2008 Domain Controllers.</p> <p>FIX: Windows 2008 Domain Controllers are now included in the "Requirement 8-Windows Account Lockouts by System Report".</p>
LOG-7662	<p>If you enabled only the view only permissions on a report folder for a user, the user was not able to view reports.</p> <p>Understanding: A user needs the right to see the parent node of the report tree in order to be able see the child node. An admin can edit permissions for individual Report folders without enabling access to levels higher on the tree. If this happens, users can not run or edit the reports.</p> <p>FIX: The report permissions are now all displayed on the System Admin page and carry over to the Reports page as expected. Additional information on how to set all the necessary permissions was added to the Reporting chapter of the Logger Administrator's Guide.</p>
LOG-7579	<p>Scheduled reports were sometimes blank.</p> <p>Understanding: This may still happen if there is no data that matches the query.</p> <p>FIX: Unable to reproduce this issue in the current release.</p>
LOG-7237	<p>Drill-down report did not work in reports created by a scheduled report.</p> <p>FIX: Drill-down now works as expected in reports created by a scheduled report.</p>

Issue	Description
LOG-7121	<p>Thirty minutes after execution, reports are not listed in the report execution status list.</p> <p>Understanding: Ad hoc reports are removed from the execution status list after 30 minutes by design. Scheduled reports, which run in background, will stay on the list longer. If you need to increase the default values for how long to retain ad hoc reports in the execution status list, please contact HP Customer Support.</p>
LOG-5901 TTP#67449	<p>The Logger Report permissions set on the System Admin page were not carried over to the Reports Tab.</p> <p>Understanding: A user needs the right to see the parent node of the report tree in order to be able see the child node. An admin can edit permissions for individual Report folders without enabling access to levels higher on the tree. If this happens, users can not run or edit the reports.</p> <p>FIX: The report permissions are now all displayed on the System Admin page and carry over to the Reports page as expected. Additional information on how to set all the necessary permissions was added to the Reporting chapter of the Logger Administrator's Guide.</p>
LOG-5849 TTP#67277	<p>PDF reports with thousands of pages truncated the current page number (page xxx of xxxx).</p> <p>FIX: The size of the current page number field was increased to accommodate larger numbers.</p>
LOG-5674 TTP#65898	<p>The Upload Image function for Report templates (Reports > Template Style > Edit Layout > Tools > Upload Image) was not working.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-5348 TTP#64425	<p>A user with the "Edit and Save Reports" right set to "No" was able to edit and save reports.</p> <p>FIX: User permissions for editing and saving reports are now properly enforced.</p>
LOG-4573 TTP#60074	<p>Scan limit details were missing from the report header.</p> <p>FIX: The report header now includes scan limit details.</p>
LOG-2120 TTP#45954	<p>Report start and end time details were missing from the report header.</p> <p>FIX: The report templates have been updated to include start and end time details in the header of each report.</p>
LOG-1991 TTP#45447	<p>Some predefined report templates did not support international characters.</p> <p>FIX: The predefined report templates now support international characters.</p>
LOG-1901 TTP#44974	<p>Users were not able to present query start and end times in header/footer of a report.</p> <p>FIX: The report templates have been updated to correctly reflect the query start and end times.</p>

Summary

Issue	Description
LOG-10332	<p>Receiver panel in UI global summary dashboard became empty if there more than 30 receivers received data during the storage retention period.</p> <p>FIX: Data is now returned and displayed properly when more than 30 receivers have received data during the retention period.</p>
LOG-10186	<p>On the summary page, when the number of events for a field was greater than 2,147,483,647, the event count showed up as negative.</p> <p>FIX: The event count is now correct when there are more than 2,147,483,647 events.</p>
LOG-10114	<p>The Summary page showed local time (the time from the system from which you are accessing Logger) when Logger was configured to another time zone. This issue was evident only when the system from which you were accessing Logger was in a different time zone than the Logger.</p> <p>FIX: The Summary page now displays the time and time zone of the remote Logger, instead of the time of the local system that you are using to access it.</p>

System Admin

Issue	Description
LOG-11154	<p>Documentation for interpreting SNMP traps generated for system health needed to be enhanced.</p> <p>FIX: The SNMP information in the System Administration chapter has been enhanced.</p>
LOG-10967	<p>The order in which SNMP data was reported changed every time the appliance was polled using SNMP WALK.</p> <p>FIX: The index for a specific data element (for example, cpu0) now remains the same every time the appliance is polled, thus ensuring consistent ordering of SNMP-reported data.</p>
LOG-10704	<p>The default administrative account that comes with Logger must remain enabled in order for the application to function correctly. There was a bug in Logger that allowed you to incorrectly mark that user account as inactive.</p> <p>FIX: The default user account can no longer be marked as inactive.</p>
LOG-10369	<p>When creating a CIFS mount on a Logger appliance, if the password contained certain special characters, the attempt to create the CIFS mount would fail.</p> <p>FIX: Using special characters in the password when creating a CIFS mount on a Logger appliance now works properly.</p>

Issue	Description
LOG-10368	<p>When creating a CIFS mount on a Logger appliance, if the password contained certain special characters, the attempt to create the CIFS mount would fail.</p> <p>FIX: Using special characters in the password when creating a CIFS mount on a Logger appliance now works properly.</p>
LOG-10288	<p>Logger did not provide a way to bind multiple IP addresses with a single NIC.</p> <p>FIX: IP aliasing feature has been added to this release, which addresses this issue.</p>
LOG-10192	<p>In certain configurations, a multipath LUN would fail to mount due to a duplicate volume label.</p> <p>FIX: Logger appliances now remove devices with duplicate labels before attempting to attach the LUN. This resolves the issue of duplicate labels causing the LUN to fail to mount.</p>
LOG-10188	<p>If the process failed during conversion from single-path to multi-path SAN, there was no fall back mechanism to restore/keep single path configuration</p> <p>FIX: A fallback mechanism has been provided to restore single path configuration should the conversion to multipath configuration fail.</p>
LOG-9636	<p>On Logger appliances, audit events for login/logout were not getting sent to the Logger's internal storage group, so that information was not searchable within the Logger application.</p> <p>FIX: The Logger appliance has been updated so that audit events for login/logout are searchable from within the application.</p>
LOG-8955	<p>Earlier versions of Logger only supported LDAP authentication.</p> <p>FIX: Logger 5.3 supports LDAPS authentication.</p>
LOG-8231	<p>The list of SNMP destinations did not always display newly added destinations right away.</p> <p>FIX: Newly added SNMP destinations are now displayed immediately.</p>
LOG-8021	<p>In earlier versions of Logger, if there was an error while establishing an NFS mount, the user was not notified of the error.</p> <p>FIX: Logger now displays an appropriate error message if it is unable to establish an NFS mount.</p>
LOG-7311 TTP#64001	<p>Previous versions of Logger did not support CIFS mounts that used NTLMv2 authentication.</p> <p>FIX: Logger 5.3 supports NTLMv2 authentication.</p>
LOG-6983	<p>In previous versions of the Logger appliance, there was a size limit imposed when editing the system's hosts file. This prevented the use of a large hosts file.</p> <p>FIX: You can now successfully edit a large hosts file on the Logger appliance.</p>

Issue	Description
LOG-5192 TTP#63205	<p>The L3200 Logger appliance generated an incorrect system health event, which indicated that one of the power supplies has failed.</p> <p>FIX: L3200 Logger appliances no longer generate an incorrect system health event for power supply status.</p>
LOG-3580 TTP#54523	<p>On Logger appliances, audit events for login/logout were not getting sent to the Logger's internal storage group, so that information was not searchable within the Logger application.</p> <p>FIX: Logger appliances now store login/logout audit events in the internal storage group so that they now searchable from within the application.</p>

Upgrade

Issue	Description
LOG-10334	<p>The upgrade from Logger 5.0 Patch 2 to Logger 5.1 could fail.</p> <p>FIX: This problem does not occur when upgrading to version 5.3.</p>
LOG-10131	<p>After upgrading Logger, some drill-down graphs are garbled or display old data.</p> <p>FIX: The Logger now displays the drill down graphs properly even after upgrading to the newer version.</p>
LOG-9479	<p>When upgrading SAN logger from 3.0 SP1 Patch 1 (L3406) to 4.0 SP1 Patch 1 (L_2c-4265) you could attempt to upgrade the Logger without the SAN attached, which caused an insufficient disk space error.</p> <p>FIX: The product has been updated to fix this issue.</p>

Open Issues

Analyze/Search

Issue	Description
LOG-11299	<p>When searching peer Loggers, the export may fail you and can get an error message if you uncheck the Rerun query option when exporting the search results.</p> <p>Workaround: The Rerun Query option on the Export screen is checked by default. Do not uncheck it when exporting the results from searches when there are peer Loggers.</p> <p>There are 5 Peers define on this logger, which include: 5.3 appliance, 5.3 SW, 5.2 GA, 5.2 P1 and 5.2 P1 SW.</p> <p>1. first perform Global peer search using time range: last 1 hr or last 30 minutes. Unlock: local.</p> <p>2. after the search is done from the Search UI, click on EXPORT.</p> <p>3. From the EXPORT menu, un-check the: Re-RUN option, then click on GO.</p> <p>4. this export will take a few minutes then the ERROR message will shown to export menu: "Search export failed: Scheduled export failed due to export failed on unable to retrieve events"</p> <p>Information:</p> <p>1. Work-a-round is: during export: check the: re-run search.</p> <p>2. this is only happen</p> <p>3. Issues has shown to:Selina</p> <p>User should NOT uncheck the : Rerun Query option from the data export Menu.</p>
LOG-11294	<p>When a user defined rex field name contains a space, an error message will show up and the field summary will not be displayed.</p> <p>Understanding: The rex operator does not support spaces in user defined field names.</p> <p>Workaround: None at this time.</p>

Issue	Description
LOG-11225	<p>When using the Auto Complete feature on the Search page, if the query has a double quote followed by bracket (i.e. "[), then the query inserted by the Auto Complete cannot be executed because of incorrectly escaped quotes and backslashes.</p> <p>Workaround: Remove the backslash followed by a double quote on both sides of the string. For example, if the query inserted by the Auto Complete is "\"[/opt/mnt/soft/logger_server.log.6] successfully.\"\"", then after removing them, the query becomes "[/opt/mnt/soft/logger_server.log.6] successfully."</p> <p>This workaround can be also used for the double quote followed by any special character such as "\" / "[] ",</p>
LOG-10130	<p>The Fields command leaves the field name even though all the values from that field are removed. Therefore, an empty column appears in the search results with the <fieldname> as the title.</p> <p>Workaround: Make sure you use the CEF operator to define the field before using the FIELDS operator. Doing so ensures that the field and its associated values are removed.</p>
LOG-10126	<p>When using the replace operator, if the "from" string is included in the replacement string, the "from" string will be replaced twice. For example, the following command, when run against the data "john smith" will result in "johnny smith":</p> <pre> replace "*john*" with "*johnny"</pre> <p>Workaround: None available at this time.</p>
LOG-9420	<p>When using transaction on data which has been received out of order, the duration may appear to be negative.</p> <p>Workaround: Include the term "sort _eventTime" before the transaction term.</p>
LOG-9025	<p>A quick logger search using One-Time Password (OTP) in the embedded browser fails after a Logger session has been inactive for 'Logger Session Inactivity Timeout', for which the default is 15 minutes.</p> <p>Workaround: Use an external browser to see results.</p>
LOG-8760	<p>Currently, only one search operation per browser can be run on Logger at any time.</p> <p>Workaround: For FireFox, use the add-on called Multifox, available at http://br.mozdev.org/multifox/. For Internet Explorer, create multiple DNS entries in the hosts file for the same IP address so that you can run different sessions at the same time.</p>
LOG-8751	<p>When search results are exported, the "Fields" field is empty.</p> <p>Workaround: Although this situation does not occur consistently, if it does occur, ensure that All Fields is selected in the "Fields" field set on the Search Results page. Then, click Export Results.</p>

Issue	Description
LOG-8484	<p>The stdev function in the chart operator does not work when operating on data that has more than 10 digits. The result of this computation will display a blank field.</p> <p>Workaround: None at this time.</p>
LOG-8076	<p>The Regex Helper tool doesn't support native characters.</p> <p>Workaround: None at this time.</p>
LOG-8003	<p>When a search operation is run using the WebServices 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>".</p> <p>Workaround: None at this time.</p>
LOG-7864	<p>The time in several fields is not in human readable format when exported. These fields include: deviceReceiptTime, startTime, endTime, and agentReceiptTime.</p> <p>Understanding: Logger records time field values in UNIX epoch format (long values).</p> <p>Workaround: Use an epoch formula in Excel to convert the time value from epoch time.</p>
LOG-7758	<p>When the eval operator is used after the chart operator, the chart results don't match the results in the table (i.e. No bar will be shown for the column added by the eval).</p> <p>Workaround: Since the eval used after the chart operator creates this issue, use the eval before the chart operator if possible.</p>
LOG-7651	<p>On the Internet Explorer browser, data is truncated in the Advanced Search calendar popup window. This issue affects users' ability to select a date using the date picker (icon) when setting CCE rules in the Advanced Search feature. When the date picker is clicked, 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. This issue does not happen on Firefox. When a user navigates along the top menu: Analyze > Search, the hyperlink labeled "Advanced Search" brings up the CCE. Entering a rule based on a field which represents a date presents the date picker in the Condition field.</p> <p>Workaround: Use the Tab key to scan along the part of the calendar which is initially hidden, then use Shift+Tab to scan back in the other direction.</p>

Issue	Description
LOG-7099	<p>When values for user fields such as sourceUserId, sourceUserName, destinationUserId, and cs1 contain "\n" character, the search results are not displayed correctly.</p> <p>Understanding: The current software interprets a value that contains "\n" as a newline character. For example, user name "nancy" in example domain, "example\nancy", is interpreted as "example[newline]ancy".</p> <p>Workaround: Disable the multi-line feature by adding the following properties to /user/logger/logger.properties. The following examples use the default values.</p> <ul style="list-style-type: none"> - 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	<p>On a software Logger, the time displayed on the histogram might not match the event time. This behavior is observed when the /etc/localtime file is not symbolically linked to the correct timezone.</p> <p>Workaround: Make sure that the /etc/localtime file is symbolically linked to the correct timezone in the /usr/share/zoneinfo file as shown in the following example. Then, restart the system on which software Logger is installed.</p> <pre>sudo ln -s /usr/share/zoneinfo/<timezone> /etc/localtime</pre>
LOG-6965	<p>When the time change due to Daylight Savings Time (DST) takes place, the following issues are observed on Logger:</p> <ul style="list-style-type: none"> - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket. - Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram. - If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results. <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p>

Issue	Description
LOG-6273 TTP#69023	<p>When search results are exported, the time elapsed to export the events is not displayed.</p> <p>Workaround: For the search elapsed time, please refer to the elapsed time shown in the stats on the search page.</p>
LOG-6199 TTP#68780	<p>When the time change due to Daylight Savings Time (DST) takes place, the following issues are observed on Logger:</p> <ul style="list-style-type: none"> - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket. - Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram. - If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results. <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p>
LOG-5958 TTP#67643	<p>When a field is removed from the Selected Fields list in the Customize FieldSet Editor, the field might not be displayed in the available fields list.</p> <p>Workaround: This only happens if you use the <- arrow to remove the field. If you double click on it, it will go back to the correct list.</p>
LOG-5181 TTP#63055	<p>Search results are not highlighted for values that match the IN operator in a query.</p> <p>Workaround: None at this time. Highlighting works if there's only 1 item in the square brackets. As soon as there's more than 1, no highlighting occurs.</p>
LOG-4888 TTP#61139	<p>When the Color Block View in the Search Builder tool (accessed using the Advanced Search link on the main Search page) is used to build a query with only one condition, the following warning is displayed: "Failed to construct a legal query, please check your query elements and try again!" Additionally, once this warning is displayed, you cannot switch to Tree View to build a single condition query.</p> <p>Workaround: Right-click and delete the starting "AND" condition that Logger enters. Then, enter the condition into the grid. Alternatively, you can also right-click on the "undefined" node that remains after you delete "AND", then select the option to add a new condition.</p>

Issue	Description
LOG-4775 TTP#60716	<p>The user interface for the Advanced Search link (on the Search page) to create a query is not intuitive about how to enter a keyword (fulltext) term.</p> <p>Understanding: To specify a keyword (full-text search), use the fullText field under the Name column. This field is displayed at the bottom of the pane.</p> <p>Workaround: If you don't see the full-text search field, scroll down.</p>
LOG-4329 TTP#59612	<p>The full-text (keyword) search cannot find events that contain an IP or a MAC address that is prefixed with an equal to (=) character in the actual event. For example, these full-text queries will not locate the following event.</p> <p>Query 1: "ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00"</p> <p>Query 2: "192.168.10.153"</p> <p>Query 3: "192.168.10.255"</p> <p><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:d4:08:00SRC=192.168.10.153 DST=192.168.10.255 LEN=229</p> <p>Workaround: This problem only occurs for a very small number of devices, which use this particular format. The workaround is to search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255. Alternatively, you could run these data through a SmartConnector to convert to CEF format. Then run either a full text or field based search.</p>
LOG-2325 TTP#48498	<p>The hits count on the Alerts page (Analyze > Alerts) is not accurate.</p> <p>Workaround: None at this time. Currently, there is no way to know the correct hits count on the Alert page.</p>
LOG-1384 TTP#42662	<p>The Save to Logger operation overwrites an existing file of the same name.</p> <p>Workaround: Use unique file names when using the Save to Logger operation.</p>

Configuration

Issue	Description
LOG-11261	<p>When new custom fields are added in the maintenance mode, no audit event will be recorded.</p> <p>Workaround: There is no workaround for this issue.</p>
LOG-11176	<p>When you enable a receiver Logger does not validate the RFS mount it referenced. Make sure the RFS mount is valid by clicking edit button for this receiver. Alternatively, check the Admin page.</p> <p>Workaround: None at this time.</p>

Issue	Description
LOG-10996	<p>Logger Archive Events fails with (Permission denied) error.</p> <p>Workaround: None at this time</p>
LOG-10605	<p>The Source Types tab (Configuration > Event Input > Source Types) is not visible for non-admin users.</p> <p>Workaround: Add 'Read Only Default Admin Group' privileges to the user.</p>
LOG-10581	<p>When a parser associated with a Source Type and Folder Follower Receiver is deleted, no warning message is displayed indicating the dependency.</p> <p>Workaround: None at this time.</p>
LOG-10353	<p>High incoming event rates can have an effect on the indexing rate of the Logger.</p> <p>Workaround: If you notice that indexing is falling behind, decrease the incoming event rates.</p>
LOG-10058	<p>Sending events targeted to an IPv6 address on Logger is not supported. The system state is unknown once it happens.</p> <p>Workaround: Restart the "receiver" process.</p>
LOG-10056	<p>You may get a duplicate device name if a receiver was removed and a new one was created with the same name as old one. When you search on this device, Logger uses the old device and you won't be able to search on the new device.</p> <p>Workaround: To avoid this problem, do not create receivers with same names as any deleted receivers.</p>
LOG-9658	<p>If you have increased your storage volume to the maximum limit allowed by your license, and you attempt to further increase the volume, the error message displayed is incorrect: "Sufficient free space is not available to increase the storage volume size. To restore normal Logger operation, click Restart".</p> <p>Workaround: Click Restart. No further action is required. However, if you need to increase the storage limit, please contact HP.</p>
LOG-9498	<p>Logger only parses syslog headers that are in the format specified by RFC3164 (traditional syslog headers). Newer syslog header formats specified by RFC3339 (syslog-ng headers) are not supported.</p>
LOG-9305	<p>Connectors send values of date/time-type fields in the following format: 07/09/0169 09:57:35.000 PST</p> <p>Understanding: This is a format that Logger does not understand. It expects time field values to be in epoch format (long values).</p> <p>Workaround: Convert the time value into epoch time for Logger to be able to correctly process them.</p>

Issue	Description
LOG-8801	<p>Sometimes after changing the Event Archive mount locations, manually created archives may show an "Invalid Mount" message.</p> <p>Workaround: Refresh the page to clear this message.</p>
LOG-8790	<p>When the community string contains non-ASCII characters, the SNMP trap sent out has "??" in the community field.</p> <p>Understanding: This is a UI issue and does not affect SNMP authentication on Logger.</p> <p>Workaround: Avoid using non-ASCII characters in the community string.</p>
LOG-8194	<p>After restoring logger from backup configuration, the CIFS share failed to mount because the user name and password fields were empty.</p> <p>Workaround: Edit the setting of the CIFS share and re-enter the username and password.</p>
LOG-7445	<p>If the Archive Settings are changed from one mount point to another, the archives created after the mount point was changed may not display. In that case, the following error message is displayed: "Could not find an archive."</p> <p>Workaround: Use Ctrl-F5 to perform a hard refresh of your browser window.</p>
LOG-6786	<p>Events may be missed when a receiver on Logger is disabled.</p> <p>Workaround: None at this time.</p>
LOG-6209 TTP#68824	<p>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.</p> <p>Workaround: If the pages stops loading, refresh the browser window to continue loading.</p>
LOG-5024 TTP#61517	<p>If the system that Logger backs up its configuration to is reinstalled or its SSL key is changed, the configuration backup fails because the SSL key cannot be refreshed from the Logger UI.</p> <p>Workaround: Log in to the CLI and delete the entry in the /home/arcsight/.ssh/known_hosts file. Then refresh the config backup configuration.</p>
LOG-4986 TTP#61369	<p>If there is an improper tear-down of the peering relationship, Loggers in the relationship might not detect it. Consequently, when you try to reestablish the relationship, it might not succeed.</p> <p>Examples of improper tear-down: One of the Loggers is replaced with a new appliance, or the peering relationship is deleted on one Logger while the other is unavailable (power down).</p> <p>Workaround: If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from Loggers before re-initiating the relationship.</p>

Issue	Description
LOG-4885 TTP#61134	<p>After a certificate is deleted from these pages, the deleted certificate is not removed from the list, leading to an impression that the certificate is still loaded on the system:</p> <p>Configuration > Event Input/Output > Certificates Configuration > Alerts > Certificates</p> <p>Workaround: Refresh the page to update the list. The deleted certificate is removed from the list.</p>
LOG-4595 TTP#60152	<p>Even if pre-allocation of storage fails before the minimum requirement has been met, Logger allows you to skip preallocation and proceed to storage configuration.</p> <p>Workaround: If pre-allocation fails, try to resume it. Skipping pre-allocation before it has successfully completed may result in sub-optimal performance on Logger.</p>
LOG-3944 TTP#57778	<p>A configuration backup is not successful if the Remote Directory name contains a space.</p> <p>Workaround: Ensure that the Remote Directory name does not contain a space.</p>
LOG-3156 TTP#52201	<p>If content is imported on a Logger that does not have the same configuration setup (devices, device groups, storage groups) as the exporting Logger, content that relies on that configuration cannot be used.</p> <p>Workaround: None at this time. The feature assumes that importing Logger has the same configuration setup as the exporting Logger.</p>
LOG-2941 TTP#51630	<p>The type associated with imported filters cannot be changed from shared to saved search.</p> <p>Workaround: Imported filter types cannot be changed. However, you can copy the filter definition and create a new filter out of it.</p>
LOG-2387 TTP#48816	<p>The EPS Out gauge reports a non-zero value even when no Forwarders are enabled.</p> <p>Understanding: This gauge reports traffic from real-time alerts as well as from Forwarders. Therefore, if you have Alerts configured on your Logger, EPS Out can be greater than zero.</p>
LOG-2244 TTP#47758	<p>A forwarder configured with a filter might not forward events that match the specified end time.</p> <p>Workaround: Extend the end time by 1 second to ensure that all events are forwarded appropriately.</p>

Issue	Description
LOG-370 TTP#36373	<p>The Configuration Backup (Configuration > Configuration Backup > Name_of_Backup) and File Transfer Receivers (Configuration > Event Input/Output > Receivers) fail silently. The most likely cause is a problem with configuration parameters such as Remote Directory, User, or Password. If an error occurs, the command appears to succeed but it does not.</p> <p>Workaround: The error is written to the log in this case, so use Retrieve Logs page (Configuration > Retrieve Logs) if you suspect a problem with the backup. When Configuration Backup is scheduled, error status is shown in the Finished Tasks status field.</p>

Connector Appliance

Issue	Description
LOG-10029	<p>On Logger appliances that have integrated Connector Appliances, users cannot access the Connector Appliance module after upgrading to Logger 5.2.</p> <p>Understanding: A new "Connector Appliance Rights Group" was introduced in this release. A user who needs to access the Connector Appliance module must be assigned to this group.</p> <p>Workaround: Assign users who need to access the Connector Appliance module to "Connector Appliance Rights Group".</p>

Dashboards

Issue	Description
LOG-11223	<p>If the index is slightly behind, drilling down on the receiver may return no results.</p> <p>Workaround: Change the end time of the query to be slightly earlier (usually only a couple minutes) to obtain the results.</p>
LOG-9332	<p>When the monitor graph panel is not wide enough to show the entire graph in the monitor or custom dashboards, the graph will be cut off and no scroll bar is shown in the panel, in the Firefox browser. For the Internet Explorer 9 browser, the panel is blank.</p> <p>Workaround: For the 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 (i.e.: If the row including a monitor graph panel has 3 panels, move at least one of the other panels to the other row). For the monitor dashboard, make the browser window wider.</p>

General

Issue	Description
LOG-11279	<p>Restoring configuration backup doesn't preserve the report templates original file ownership and causes report execution without proper templates.</p> <p>Workaround: Follow these steps to fix the permissions.</p> <ol style="list-style-type: none">1. SSH to Logger. (Appliance users should contact customer support for help with this.)2. Navigate to the following directory, <code><\$ARCSIGHT_HOME>/logger/Intellicus/reportengine/templates/adhoc</code>, where <code><\$ARCSIGHT_HOME></code> is the directory in which Logger is installed.3. Change the owner of the report templates [files with extension <code>.irl</code> and <code>.sty</code>] files from "root" to the same non-root user that was used during Logger installation.
LOG-11263	<p>When new custom fields are added in the maintenance mode, no maintenance results for them will be added.</p> <p>Workaround: There is no workaround for this issue.</p>
LOG-2433 TTP#49017	<p>If you click on another tab or page before a UI page is fully loaded, the UI attempts to load the latter page, but eventually displays the former page.</p> <p>Workaround: Wait for the current page to fully load before clicking another one.</p>

Reports

Issue	Description
LOG-11137	<p>If a user has privileges to View a Published Report Only, then the report will not be visible in the Report Explorer.</p> <p>Workaround: You can find and view published reports from the Category Explorer instead. To find a published report, open the Category Explorer and navigate to the Saved Reports folder under the report's Category. (The terms "saved report" and "published report" are used interchangeably.)</p>
LOG-11071	<p>If the underlying Query of a Report changes, then viewing published reports will result in an error.</p> <p>Workaround: None at this time.</p>
LOG-10098	<p>Null values in reports will show up as '-' and if it's a drilldown column then the drilldown will usually open a report with misleading results. Since '-' doesn't match.</p> <p>Workaround: None at this time.</p>

Issue	Description
LOG-9860	<p>When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it is copied.</p> <p>Workaround: None. Clicking Copy or Copy as Link will not give you a visual indication that anything has been copied, but you will be able to Paste, as needed.</p>
LOG-9798	<p>When the Logger Compliance Insight Package (CIP) reports such as Logger ITGov 4.0 for ISO 27002 are exported in PDF format, the saved PDF shows that Chart component with the following error: "Error: No plotters/series have been defined"</p>
LOG-9620	<p>If a distributed report fails to run in the background against fields that do not exist on the peer Logger, the error message does not clearly indicate the reason.</p> <p>Workaround: None at this time.</p>
LOG-9584	<p>After upgrading to Logger 5.2, browser caching issues are seen in Reports pages. You may see errors in red in the dashboard viewer, and you might not be able to create widgets, and the explorers may not work.</p> <p>Workaround: Restart your browser. If that does not work, manually clear the browser cache and delete temporary files.</p>
LOG-9216	<p>Even when report categories are marked Hidden, they might be visible in Explorers and other report-related locations.</p> <p>Understanding: This is by design. The hidden categories are visible to admin users and users with appropriate access rights only. They remain hidden in the Report List page. In case of query explorer, they are displayed because this is where queries have to be listed to be edited.</p>
LOG-8780	<p>Reports generated using the WebServices API do not contain report titles.</p> <p>Workaround: When generating reports through the WebServices API, ensure that you have entered the Report Title in the Report Editor (otherwise you will only see the Report ID) in the generated report.</p>
LOG-7186	<p>After you limited a user's rights to a specific report template, the user might not be able to run any reports at all. The following error messages were displayed when users tried to run reports:</p> <p>90141 No matching record found: Requested Report Object "xxxxxxx" Not Found</p> <p>90141 No matching record found: The Query Object used as the Datasource could not be fetched from the repository</p> <p>Understanding: A user needs the right to see the parent node of the report tree in order to be able to 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, users can not run or edit the reports.</p> <p>FIX: The report permissions are now all displayed on the System Admin page and carry over to the Reports page as expected. Additional information on how to set all the necessary permissions was added to the Reporting chapter of the Logger Administrator's Guide.</p>

Issue	Description
LOG-7165	<p>The privileges for pre-built reports on Logger are missing from the Add Group page if the Logger is a fresh install and you have not yet loaded the Reports page after installing this Logger.</p> <p>Workaround: Go to the Reports page. (This triggers the population of group privileges in the Add Group.) Go back to Add Group. The privileges for pre-built reports are displayed now.</p>
LOG-6652	<p>In the FireFox browser, the Report Template editor (Reports > 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.</p> <p>Workaround: Use the IE browser.</p>
LOG-3244 TTP#52452	<p>In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report.</p> <p>Workaround: Use the IE browser instead.</p>
LOG-3187 TTP#52330	<p>The time taken to run a scheduled report is not reported correctly in the Logger user interface.</p> <p>Workaround: None at this time.</p>
LOG-2355 TTP#48618	<p>The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.</p> <p>Workaround: None at this time.</p>
LOG-2350 TTP#48613	<p>The default report generated by clicking the hand icon is missing the report name and date.</p> <p>Workaround: Add the Report title to the Report Header section to render the title on the first page of the Report.</p>
LOG-2012 TTP#45548	<p>Adding a scheduled report can reset the scan limit field of other reports.</p> <p>Workaround: Check that the scan limit is set as desired before running any report.</p>
LOG-1956 TTP#45163	<p>The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.</p> <p>Workaround: None at this time.</p>
LOG-1936 TTP#45091	<p>Users who are granted only edit and save report styles privileges do not see the Template Styles link on the Reports tab.</p> <p>Workaround: Grant users that need to access Template Styles admin privileges.</p>

Issue	Description
LOG-1703 TTP#44508	When a report query of 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-10084	<p>The Count value displayed on the Summary page may be slightly different from the Hit value on the Search page for the same field.</p> <p>Understanding: The difference occurs due to multiple reasons such as the delay between when the Count was displayed on the Summary page and when the search query was run on the Search page. Additionally, indexing may 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.</p> <p>Workaround: None at this time.</p>
LOG-9955	<p>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 (in the range of 1 million or higher) and you drill down to view those events, your system may experience performance issues.</p> <p>Workaround: If you need to drill down to view a large set of events (in the range of 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:</p> <ol style="list-style-type: none"> 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-9829	<p>When you drill-down from the Summary page, the time range that the search query runs with is not exactly the same as the one shown on the page from where you drill down.</p> <p>Understanding: The granularity of time used for the Summary page is different from the Search page, therefore, the numbers are different.</p> <p>Workaround: None at this time. Currently, there is no way to specify the search time range in milliseconds.</p>

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

System Admin

Issue	Description
LOG-11205	<p>Some System Administration pages do not render correctly when using Microsoft IE-9.</p> <p>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.</p>
LOG-11066	<p>If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues:</p> <ol style="list-style-type: none"> 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. <p>Workaround: Change the system time zone to something to more specific, such as /America/Los_Angeles.</p>
LOG-9288	<p>The System Admin - FIPS 140-2 page can take several seconds to load.</p> <p>Workaround: None at this time.</p>
LOG-7664	<p>If a single-path SAN logger appliance is rebooted and the previously attached LUN is not available, the Logger will fail to start. In case of a multipath SAN Logger appliance, the Logger fails to start only if the path that was in-use when the Logger was rebooted is unavailable.</p> <p>Workaround: None at this time.</p>
LOG-1050 TTP#40872	<p>Under certain circumstances, users with restricted privileges might still see Device Group and Storage Group names. If these users are also subject to a Search Group Filter (enforced filter), they will not be able to see events in those Device Groups or Storage Groups.</p> <p>Workaround: Provide Device Group and Storage Group names that do not reveal internal information.</p>

Upgrade

Issue	Description
LOG-11136	<p>After upgrading the Logger appliance version 5.3, rebooting and logging in, you may encounter a page that asks to upload a license and set the timezone.</p> <p>Workaround: Please contact support for help with this issue.</p>
LOG-8638	<p>During an upgrade, you are asked to reboot the appliance followed by Locale Selection. 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.</p> <p>Workaround: This bug affects IE7 and older versions of IE8. Clear the browser cache (on IE: Tools -> Internet Options -> Delete...) before going to System Locale page (and after rebooting the appliance).</p>
