

Release Notes ArcSight Logger™

Version 5.1 GA

June 15, 2011



Release Notes ArcSight Logger™, Version 5.1 GA

Copyright © 2011 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
06/15/11	Logger v5.1 GA	Added a bug to the Open Issues section.
06/08/11	Logger v5.1 GA	Added the section "Information You Should Know".
05/31/11	Logger v5.1 GA	v5.1 GA.
11/12/10	Logger v5.0 Patch 2	Patch 2 for v5.0.
10/12/10	Logger v5.0 Patch 1	Patch 1 for v5.0.
09/19/10	Logger v5.0 GA	First Logger - Downloadable Version release.
07/22/10	Logger v4.5 GA	Version 4.5 GA release. First software-only version option for Logger.
05/21/10	Logger v4.0 SP1 Patch 1	Update to the original Patch 1 for v4.0 SP1 to include additional checks in the upgrade process for references to non-existent resources.
03/01/10	Logger v4.0 SP1 Patch 1	Patch 1 for v4.0 SP1.
02/04/10	Logger v4.0 SP1	Added information about supported browsers.
01/29/10	Logger v4.0 SP1	Service Pack 1 for version 4.0.
11/15/09	Logger v4.0 GA	Version 4.0 GA release.

Release Notes template version: 2.1.0

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://www.arcsight.com/supportportal
Protect 724 Community	https://protect724.arcsight.com

Contents

ArcSight Logger™ v5.1 GA	5
What's New in v5.1 GA	6
New Hardware Platform Support	6
Installation and Configuration Enhancements	6
Software Logger Receiver Ports	6
Search Operators	7
Search Helper	7
Logger API	7
Event Archival Enhancements	7
Additional Field in Logger Schema	8
Enhanced Peer Search	8
Multi-line File Receiver	8
Multi-series Charts	8
Scheduled PDF Exports	9
System Health Events -- New and Improved	9
Additional System Filters	10
Additional Filter Type	10
Localization Support	10
Reports Enhancement	10
SAN Multipath Support	10
Improved SSH Login	11
One Time Password for ESM Authentication	11
Supported Browsers	11
Information You Should Know	12
Default Directory for Software Logger Installation	12
Configuration Backup of Multipath SAN	12
Doc Errata	12
Upgrading to v5.1 GA (L5887)	13
Logger Appliance	13
Prerequisites	13
Upgrade Instructions	13
Software Logger	14
Prerequisites	14
Upgrading Instructions	15

Restarting Software Logger Upgrade After a Failure	19
Logger v5.1 GA Documentation	19
Converting a Single Path LUN to a Multipath LUN	19
Localization: Known Limitations	20
Issues Fixed in this Release	22
Alerts/Filters	22
Appliance Upgrade	22
Audit Events	22
Authentication/Certificates	23
Configuration Backup and Restore	23
Event Archive	23
Event Input/Output	24
Logger Appliance Platform	24
Reports	25
Search	26
Storage	27
System Administration	27
Open Issues in this Release	28
Known Behaviors From Previous Releases	34
Open Issues From Previous Releases	36

ArcSight Logger™ v5.1 GA

These release notes provide information about the ArcSight Logger v5.1 GA (L5887) 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 v5.1 GA” on page 6](#)
- [“Supported Browsers” on page 11](#)
- [“Information You Should Know” on page 12](#)
- [“Upgrading to v5.1 GA \(L5887\)” on page 13](#)
- [“Logger v5.1 GA Documentation” on page 19](#)
- [“Converting a Single Path LUN to a Multipath LUN” on page 19](#)
- [“Localization: Known Limitations” on page 20](#)
- [“Issues Fixed in this Release” on page 22](#)
- [“Open Issues in this Release” on page 28](#)
- [“Known Behaviors From Previous Releases” on page 34](#)
- [“Open Issues From Previous Releases” on page 36](#)

What's New in v5.1 GA

This section lists the new features and enhancements introduced in Logger v5.1 release. See the *Logger v5.1 Administrator's Guide* for details of these features, which is available at the ArcSight Customer Support site at <http://www.arcsight.com/supportportal>.

In addition, this release introduces fixes for a large number of bugs. See ["Issues Fixed in this Release" on page 22](#) for a complete list of fixes.

If your Logger appliance is integrated with a Connector Appliance (L3XXX models), also refer to the Connector Appliance Release Notes for additional information about the Connector Appliance functionality.

New Hardware Platform Support

This release is designed to run on the new Logger hardware platforms available from ArcSight, as well as the existing platforms (Lx200). The new platforms (L3400, L7400, and L7400-SAN) are the next-generation Logger appliance systems for the existing platforms available from ArcSight. These platforms offer greater processing power and increased memory.

Installation and Configuration Enhancements

To ease the installation and configuration of software Logger, following improvements have been made:

- Starting with this release, you can install software Logger as a root user or as a non-root user. When you install the software as a root user, you can select the port on which Logger listens for secure web connections. However, when you install it as a non-root user, Logger can only listen for connections on port 9000. Additionally, you can configure Logger to start as a service when you install as a root user.

The ability to install as a root user is new in version 5.1; only non-root user installation was supported prior to this release. Therefore, if you are upgrading from a previous version of Logger to 5.1, you cannot change the previous install to a root-user installation. You will need to use the previously configured port 9000 for accessing software Logger.
- You can install software Logger in three different installation modes—GUI, Console, and Silent. The GUI mode enables you to input information as the installation proceeds. The Console mode enables you to install software Logger from a console. The steps followed are the same as the GUI mode, except that the installation occurs from the command line. In Silent mode, you can input information in a properties file (created using the GUI mode) and the installation occurs without requiring any further interaction from you. This mode is conducive for environments where multiple Loggers need to be installed.
- A very small footprint software Logger installation is now available. This installation requires only 10 GB of disk space.
- Software Logger configuration wizard has been enhanced for ease of installation and flexibility. Three configuration modes—minimal, standard, and custom—are now available. Each configuration mode has a different disk space requirement, thus providing flexibility. Similarly, in the minimal and standard modes, the configuration wizard automatically configures storage volume, storage groups, indexing, and a TCP and a UDP receiver, thus easing installation.

Software Logger Receiver Ports

If you install software Logger as root, you can configure the receivers on it to use ports lower than 1024. This capability did not exist prior to this release because software Logger could not be installed as root.

Search Operators

Additional search operators have been added and existing ones have been enhanced to enable deeper and statistical analysis of search results. Specifically, the following operators have been added or enhanced:

- top N
- extract
- keys
- rename
- replace
- Additional chart functions: average, mean, minimum, maximum, span, standard deviation

Search Helper

Search Helper is a search-specific utility that provides the following features:

- Search History—Displays the recently run queries on Logger, thus enabling you to select and reuse previously run queries without typing them again.
- Search Operator History—Displays the fields used previously with the search operator that is currently typed in the Search text box.
- Examples—Lists examples relevant to the latest query operator you have typed in the Search text box.
- Suggested Next Operators—List of operators that generally follow the currently typed query. For example, if you type `logger |`, the operators that often follow are `cef`, `rex`, `extract`, or `regex`.
- Help—Provides context-sensitive help for the last-listed operator in the query that is currently typed in the Search text box.
- List of Fields and Operators—Depending on the current query in the Search text box, a complete list of fields that possibly match the field name you are typing or a list of operators that are available on Logger is displayed.

Logger API

Logger now provides Web Services for its search and reporting functions. These services enable you to log in, perform searches, or run reports on Logger from a Web Service client that you write using Java, Perl, Python, Ruby, and so on.

Three Web Services are available:

- Login Service—to log in to a Logger and establish a cookie that is used for all search and report service calls.
- Search Service—to run a search query on Logger.
- Report Service—to run a report on Logger.

See the *WebServices API Guide* for Logger for details and available methods. This guide is available for download from the ArcSight Customer Support web site at <http://www.arcsight.com/supportportal>.

Event Archival Enhancements

Starting with Logger v5.1, events are archived on a per storage group basis. That is, each storage group is individually archived to a separate location everyday. Archiving events from each storage group to a separate archive location enables you to keep data in specific storage groups longer than others.

In addition, you can bulk archive events—that is, specify a range of dates to archive events in a single archive operation. Similarly, you can now perform bulk load, unload, and delete operations on archives.

Additional Field in Logger Schema

An additional field, `sourceUserPrivileges`, is available for indexing in the Logger schema. The field is not indexed by default. Therefore, if you want Logger to index on this field, make sure you add it for indexing on the Edit Search Index page (Configuration > Search Optimization).

Enhanced Peer Search

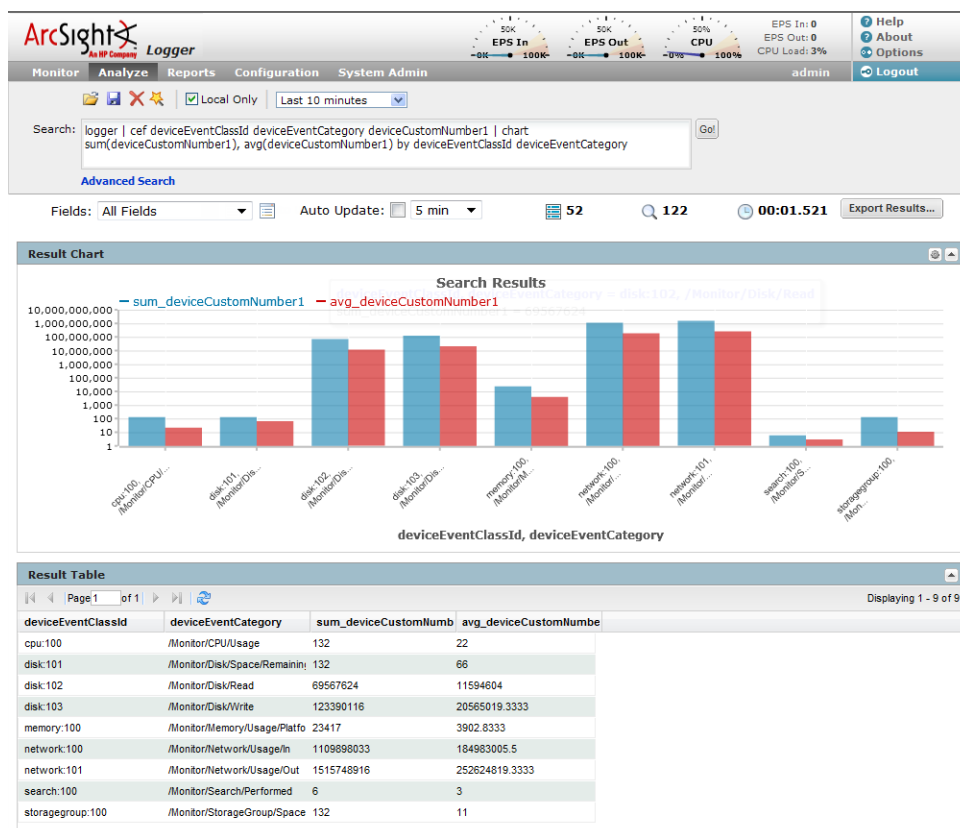
Starting with this release, pipeline operators in search queries run across peers are supported. For this functionality to work, the peers must be running Logger v5.1.

Multi-line File Receiver

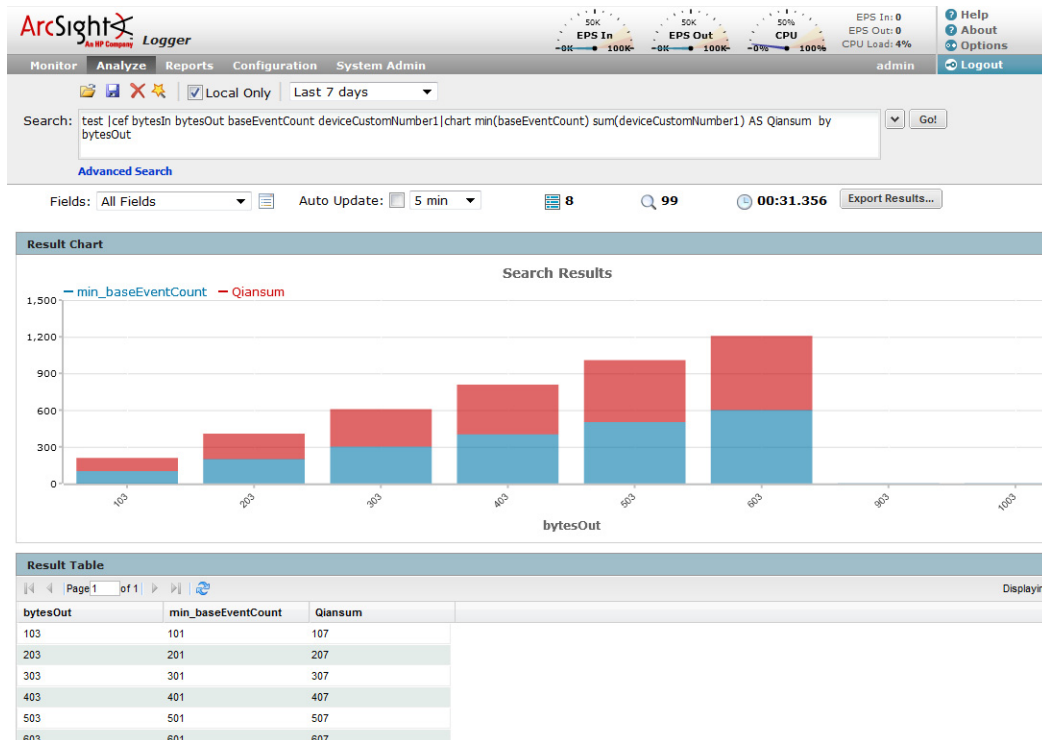
A multi-line file receiver is a type of file or file transfer receiver that can read multi-line log files. This receiver is useful in reading events that span more than one line, such as exceptions in a server log. A multi-line file receiver is useful in finding exceptions in a server log. In such logs, the entire stack trace can be treated as one event instead of each line as a single event.

Multi-series Charts

A multi-series chart can plot the values of multiple aggregation functions in a single chart. For example, when you include `average` and `sum` in a `chart` command, a multi-series chart is generated that plots the values of these functions along the Y-axis in a single chart.



Alternatively, you can choose to plot a multi-series chart as a stacked chart—Stacked column or Stacked Bar—in which multiple values are plotted in a stack form, as shown in the following figure.



Scheduled PDF Exports

Prior to this release the results of scheduled saved searches could be exported only in CSV format. Starting with this release, the results can also be exported in PDF format. This format is useful for exporting a report-style file that contains search results as charts and in tables.

System Health Events – New and Improved

System Health Events, also known as Internal Events, provide the system health status of your Logger. Starting with Logger v5.1, the format in which system health events are generated has changed to provide more meaningful information. Some of the changes are:

- Addition of new events. For example, Current and Voltage events.
- Instead of referring to all system health events as Logger Internal Event in the `name` field, meaningful names are used. For example, Fan OK, Temperature OK.
- Three severity levels for each event have been added to the `agentSeverity` field—1 (OK), 5 (Degraded), and 8 (Severe).
- The `deviceCustomString` and `deviceCustomStringLabel` field mappings have changed. Refer to a specific event to identify changes.
- Device Event Class ID (`deviceEventClassId`) and Device Event Category (`deviceEventCategory`) of the events have changed. See the *Logger v5.1 Administrator's Guide* for the updated list.
- All hardware-related events are classified as `hardware:nnn` events, where `nnn` is a three-digit number that identifies the hardware component. For example, `hardware:13x` identifies the fan events.

When you upgrade to Logger v5.1, any existing filters or queries based on earlier events will not work on the events collected after the upgrade. However, those filters and queries will continue to work on the events collected prior to the upgrade. Note that the predefined System Filters are compatible with the new and the old format.

Additional System Filters

Your Logger ships with a number of predefined filters, also known as system filters. These filters define queries for commonly searched events. The following additional system filters were added in this release in the Unified and regular expression formats:

- Root Partition Below 10 Percent
- Root Partition Below 5 Percent
- Bad Fan
- Disk Failure

Additionally, all existing system filters were enhanced such that they are compatible with the new and old format of logging system health events.

Additional Filter Type

You can now save shared filters as regular expression queries. (Shared filters are visible to all Logger users. Once created, any Logger user can use it to search for events.)

Prior to this release, these filters could only be saved as Unified queries (that use keywords and field names). This enhancement enables you to save and share filters for alerts and forwarders, which require regular expression queries, thus easing the effort to create alerts and forwarders that use common filters.

Localization Support

Starting with this release, localization support for these languages is available for Logger:

- Japanese
- Chinese (China)
- Chinese (Taiwan)

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 Logger will use after installing, initializing, or upgrading your Logger. Once set, locale cannot be changed. If locale is not set, a banner message on your Logger UI is displayed.

Reports Enhancement

A new template type, "BlankWithHeader", enables you to include the start time, end time, scan limit, device group, storage group, and devices information (used to run a report) in a report. Choose this template type when creating reports if you need the report to contain time and device and storage group information.

SAN Multipath Support

Prior to Logger v5.1, you could only connect one port to the LUN; however, starting with v5.1, you can connect both of those ports to the same LUN for multipathing.

When you multipath a LUN, you create two different network paths to it from the system to which the LUN connects. Doing so reduces the possibility of a single point of failure causing the LUN to become unavailable.

Multipath user interface (UI) is available by default on Logger models that support SAN. However, you must connect the LUN to both HBA ports on your Logger and configure multipath configuration in the UI for it to function. Once enabled, **multipath cannot be disabled on Logger.**

If you are an existing Logger SAN customer, upgrading from a version prior to Logger v5.1, and want to enable multipath on your Logger, see ["Converting a Single Path LUN to a Multipath LUN" on page 19.](#)

Improved SSH Login

Previously known as support login, this feature enables you and ArcSight Customer Support to access your appliance for troubleshooting and diagnostics in situations such as an upgrade failure, unresponsive appliance, and so on.

Starting with this release, the options required to enable the feature and how the feature works has changed. If you are an existing Logger customer who is familiar with the previous implementation, note the following change in process:

Instead of enabling SSH access and entering the activation code you receive from ArcSight Customer Support in Logger UI, you only enable SSH access in the UI. The rest of the steps are performed using an SSH client. Use the SSH client to connect to Logger and call ArcSight Customer Support. Upon connection to the appliance, you receive a challenge prompt, to which ArcSight Customer Support will provide you a response. When prompted for the password, enter any text and press Enter. You are then prompted for a response. Enter the string you obtained from Customer Support. You are then connected to Logger as root. The session is valid for the amount of time specified in the option you selected to enable SSH.

For step-by-step instructions of this process, see "Connecting to Logger using SSH" in the *Logger v5.1 Administrator's Guide*.

One Time Password for ESM Authentication

Prior to Logger v5.1, only basic authentication (user name and password) was available for authenticating users who could perform searches from ESM Console on Logger; however, starting with Logger v5.1, a One Time Password (OTP) option is available. This option makes the user authentication between Logger and ESM Console highly secure. For OTP option to work, Logger must be running v5.1 or later, and the ESM Console must be running ESM v5.0 SP1 Patch 2 or later.

Supported Browsers

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

- Internet Explorer: Versions 7 and 8
- Firefox: Versions 3.5 and 3.6

These versions supersede the browser versions mentioned in the *Logger v5.1 Administrator's Guide*.



For IE 7 and 8 browsers, make sure that 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.

Information You Should Know

The following information is late-breaking. Read it in its entirety before installing software Logger or restoring a configuration backup to a multipath SAN Logger.

Default Directory for Software Logger Installation

When installing as the root user, make sure you change the default directory location ("/root") displayed in the software Logger installation wizard to a directory location that the non-root user (the one you enter during software Logger installation) can access. If you accept the default value and install the software Logger in the "/root" directory, users will not be able to connect to the Logger UI and will see the following error message:

```
"Error 403 Forbidden. You don't have permission to access / on this server"
```

Configuration Backup of Multipath SAN

Logger v5.1 does not back up the multipath SAN configuration when you create a configuration backup (Configuration > Configuration Backup). As a result, when you restore a factory-reset Logger from such a backup, the Logger fails to start. If you need to restore configuration for a multipath SAN Logger, use the following steps to ensure that Logger will correctly access its SAN storage and start as expected.

- 1 Ensure that the LUN is physically connected but not attached to your Logger (System Admin > SAN).
- 2 In the Logger UI, click **System Admin > Multipath**.
- 3 Select the appropriate SAN Multipathing Configuration from the drop-down menu or refer to the *Logger v5.1 Administrator's Guide* and your SAN documentation to enter the multipath configuration specific to your setup and environment.
- 4 Click **Test** to ensure the multipath configuration you chose or the changes you made are valid.
- 5 Click **Save**.
- 6 Restore the configuration from backup.

Doc Errata

In the "Enabling Multipath" topic in the Logger v5.1 Administrator's Guide, Step 1 is described as follows:

- 1 Ensure that a LUN is attached to the Logger, as described in "SAN" on page 318.

This step should be as follows:

- 1 Ensure that a LUN is **not** attached to the Logger, as described in “SAN” on page 318.

Upgrading to v5.1 GA (L5887)

Logger Appliance

An upgrade to Logger v5.1 GA is supported from v5.0 Patch 2 and v5.0 Patch 3.

For all other versions, you need to first upgrade to v5.0 Patch2 release before upgrading to v5.1 GA.



- 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.
- Logger v5.0 Patch 3 release is only available on new Logger appliances shipping from ArcSight.

Prerequisites

Make sure you 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.

Additionally, make a note of custom Report Configuration settings (Reports > Reports Administration) you have configured on your Logger because after the upgrade those settings are set to the default values. To reinstate the customized value, you need to re-enter them.

When you upgrade to Logger v5.1, any existing filters or queries based on the previous system health events will not work on the events collected after the upgrade. However, those filters and queries will continue to work on the system health events collected prior to the upgrade. Therefore, you will need to define additional filters or queries after the upgrade to search for system health events collected after the upgrade.

Upgrade Instructions

- 1 Download the [logger-5887.enc](#) file from the ArcSight Download Center at <https://arcsight.subscribenet.com> to a computer from which you connect to the Logger UI.
- 2 Click **System Admin > License & Update**.
- 3 Browse to the [logger-5887.enc](#) file you downloaded in the previous step and click **Upload Update**.

Once the upgrade is complete, the Logger login prompt is displayed.

- 4 Log in to the appliance.

The following banner message is displayed.

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 above message to display a page with the "Start Reboot Now" button.
- 6 Click **Start Reboot Now**.
- 7 After the reboot, log in again and click the link in the banner bar on top to configure your locale or navigate to **System Admin > System Locale**. You can choose from these locales:
 - ◆ English
 - ◆ Japanese
 - ◆ Chinese (China)
 - ◆ Chinese (Taiwan)Once locale is set, it cannot be changed.
- 8 Click **System Admin > Reboot > Start Reboot Now** to reboot your Logger once again.
- 9 If you had custom Report Configuration settings (Reports > Reports Administration) configured prior to the upgrade, re-enter those settings because after the upgrade those settings are set to the default values.
- 10 If you had defined filters or queries to search for system health events, define additional filters and queries to search for system health events collected after the upgrade.

Software Logger

An upgrade to software Logger v5.1 GA is supported from v5.0 Patch 2 only. If you are using any other version, you need to first upgrade to v5.0 Patch 2 before upgrading to v5.1 GA.

If you are installing software Logger as a fresh install, see the *Logger v5.1 Administrator's Guide* for information.

Prerequisites

Make sure you read and follow all prerequisites applicable to your setup and environment before proceeding with the upgrade:

- 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.
- The location to which events are archived is mounted on your software Logger machine before you begin the upgrade. If the event archive location is not mounted, upgrade will fail. If that occurs, see ["Restarting Software Logger Upgrade After a Failure" on page 19](#) for instructions on how to restart the upgrade process.
- Make a note of custom Report Configuration settings (Reports > Reports Administration) you have configured on your Logger because after the upgrade those settings are set to the default values. To reinstate the customized value, you need to re-enter them.
- **When you upgrade to Logger v5.1, any existing filters or queries based on the previous system health events will not work on the events collected after the upgrade.** However, those filters and queries will continue to work on the system health events collected prior to the upgrade. Therefore, you will need to define additional filters or queries after the upgrade to search for system health events collected after the upgrade.

- If you have customized report templates or have Compliance Insight Package(s) installed, make sure you are familiar with the "LOG-8863" on page 28.

Upgrading Instructions

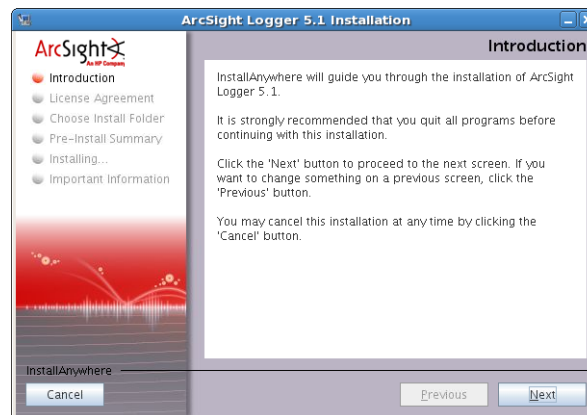
- 1 Ensure that you are logged in with the same user name as the one used to install the previous version of software Logger.

Note: Even though the ability to install a software Logger as root user is available in this release, you cannot change an existing install to a root-user installation. Therefore, when upgrading an existing software Logger, you must be logged in as the same non-root user that was used to install it initially.

- 2 Download the v5.1 GA software Logger upgrade file ([ArcSight-logger-5.1.0.5887.0.bin](https://arcsight.subscribenet.com)) from <https://arcsight.subscribenet.com>.
- 3 Run these commands from the directory where you copied the Logger software:

```
chmod +x ArcSight-logger-5.1.0.5887.0.bin
./ArcSight-logger-5.1.0.5887.0.bin
```

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

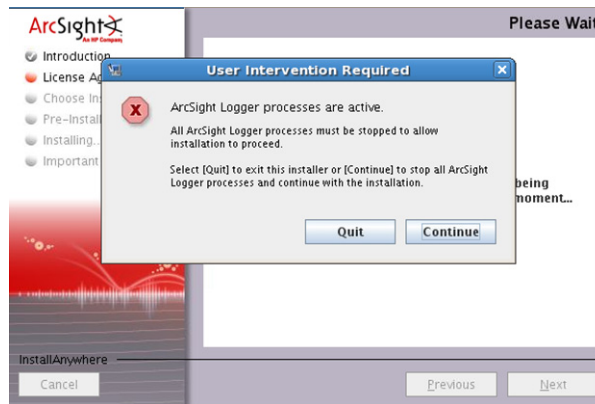


- 4 Click **Next**.

The License Agreement screen is displayed. Read through the License Agreement details. Click **I accept the terms of the License Agreement**. Then, click **Next**.

Note: You need to scroll down to the end of the License Agreement details to enable the "I accept the terms of the License Agreement" button.

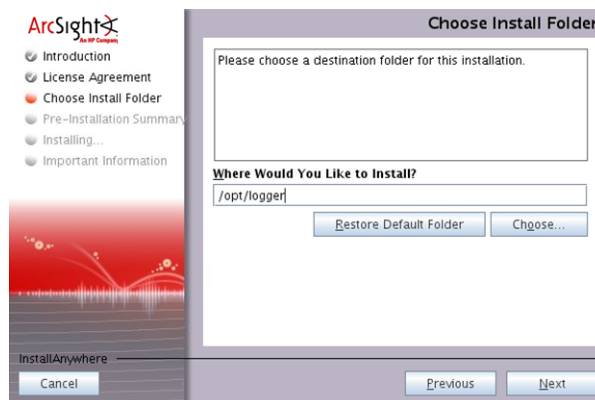
- 5 If the installer detects a currently running instance of Logger on the machine, the following message is displayed.



- 6 Click **Continue** to stop the currently running Logger processes. Or **Quit** to quit the upgrade process.

Next, the installer stops the running Logger processes and checks for other installation prerequisites.

- 7 Specify or browse to a folder where you want to install Logger, as shown in the following figure. By default, the home directory of the user who is logged in is specified.

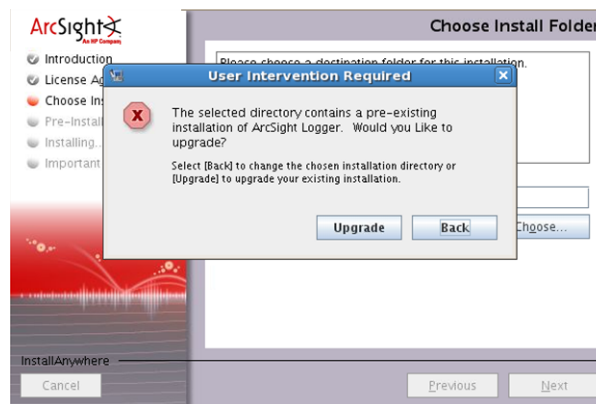


If you specify a directory in which a Logger is already installed, the following error message is displayed. You can either click **Upgrade** to upgrade the existing installation or **Back** to specify a different directory for installation.

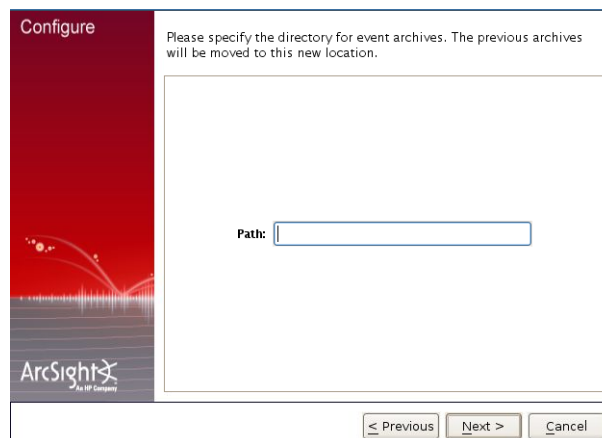


When you upgrade an existing installation, the upgraded Logger has access to the data store of the previous version. However, if you install Logger in a new location, it is the equivalent of installing a fresh instance of Logger, which will not have access to the data store of the previous version.

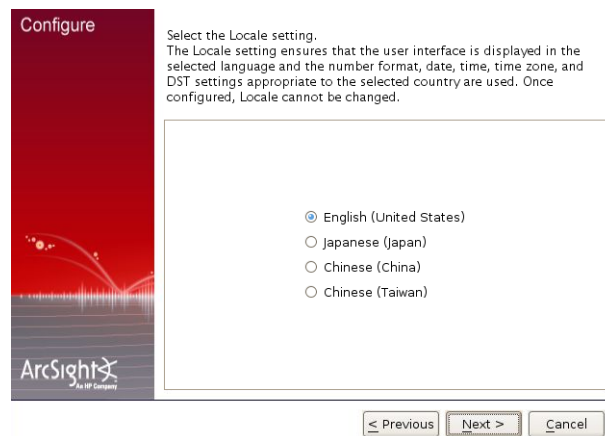
If you specify a new location, follow instructions in the *Logger v5.1 Administrator's Guide* to complete the installation of the new Logger instance.



- 8 Click **Upgrade**. Then, click **Next** on the Logger Update Wizard screen to proceed with update tasks.
- 9 If your existing archives are under the "<install_dir>/current/..." directory, you are prompted to specify a different location for the new archives that will be created after the upgrade, as shown in the following figure. This location needs to be above the "/current" directory level. For example, if your existing archives are at <install_dir>/current/logger_5.0P2/myarchives, the new location can be <install_dir>/logger_5.1/myarchives or any other location above the <install_dir> directory, but not <install_dir>/current/logger_5.1/myarchives. Also note that the existing archives are moved to the new location you specify. Any future archives (created after the upgrade is complete) are also written to the new location.



- 10** Select the Locale for your Logger, as shown in the following figure.



You can choose from these locales:

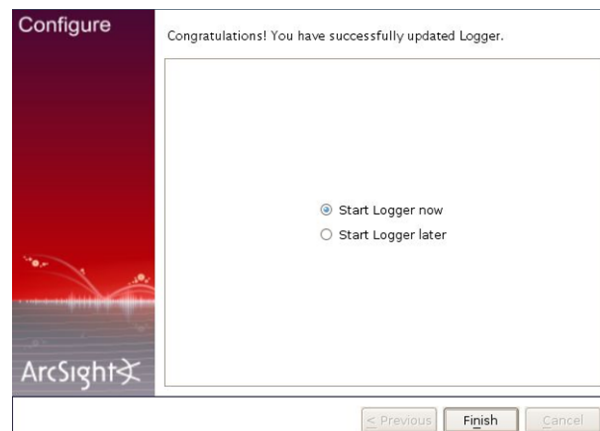
- ◆ English
- ◆ Japanese
- ◆ Chinese (China)
- ◆ Chinese (Taiwan)

Once locale is set, it cannot be changed.

- 11** You have installed Logger. Click **Start Logger Now**.

OR click **Start Logger later** and click **Finish**.

- 12** If you selected "Start Logger Now", the following screen is displayed.



You can click **Finish** to exit the wizard. Logger continues to start service and processes in the background. Once the service and processes have started, you can connect to the upgraded Logger.

- 13** Once the upgrade is successful, make sure you follow the instructions in ["LOG-8863" on page 28](#), if the issue applies to your setup.

Restarting Software Logger Upgrade After a Failure

The information in this section only applies to the case when the upgrade fails because the configured event archive location is not mounted on the software Logger machine when the upgrade is started.

- 1 Locate the archives folder under the `<install_dir>/L5355` directory.
- 2 Mount it to your software Logger machine.
- 3 Run the following command:

```
<install_dir>/current/arcsight/bin/arcsight loggersetup -u
L5355
```

The Installation Wizard is launched, which also upgrades your software Logger. Follow the wizard screens to complete the upgrade, as described in "Upgrading Instructions" on page 15.

Note: When prompted to enter an archive location in this wizard, enter any path except `<install_dir>`. Do not store archives in the same directory where Logger is installed.

Logger v5.1 GA Documentation

The following Logger documentation is available for this release:

- Administrator's Guide—Available for download from the ArcSight Customer Support site at <http://www.arcsight.com/supportportal>. 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 ArcSight Customer Support site at <http://www.arcsight.com/supportportal>.
- 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 Customer Support site at <http://www.arcsight.com/supportportal>.
- Quick Start Guide for Software Logger—Applicable for new software Logger Downloadable Version installations, which are purchased through the ArcSight web site (<http://www.arcsight.com/products/products-logger/>). This guide is the first document to use to understand software Logger in a nutshell and install it.

Converting a Single Path LUN to a Multipath LUN

Starting with Logger v5.1, you can configure a LUN for multipathing on Loggers that support SAN. 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 v5.0 Patch 2 or earlier, 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. However, if the multipath conversion does not succeed or another circumstance requires you to revert to single path, contact ArcSight Customer Support for assistance.

To convert a single path LUN to multipath:

- 1 Upgrade your Logger appliance to version 5.1.
- 2 After a successful upgrade, connect to your Logger using SSH, as described in "Connecting to Logger Using SSH" in the *Logger v5.1 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 v5.1 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, 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: 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 in this release. For example, the following sections are available in English only:
 - ◆ Reboot
 - ◆ Network
 - ◆ License & Update
 - ◆ CIFS
 - ◆ NFS
 - ◆ RAID controller
 - ◆ SSL Server Certificate

◆ Authentication

- 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.

Issues Fixed in this Release

The following customer-reported issues were fixed in this release.

Alerts/Filters

Issue	Description
LOG-7415	<p>Alert event did not contain event IDs of all the triggering events. Additionally, the baseEventCount field in the event did not reflect the true number of matching events for such alert events.</p> <p>Understanding: To maintain an optimal size of an alert event, the event does not contain event IDs of all the triggering events if a match count of 101 or higher is specified. As a result, the baseEventCount field in the event does not reflect the true number of matching events for such alert events. Triggering events are truncated in multiples of 100. Therefore, if you specify a match count of 101, only one event is included in the alert event and the baseEventCount field value is 1. Similarly, if you specify a match count of 720, only 20 events are included and the baseEventCount field value is 20.</p>
LOG-7203	<p>The filter criteria specified in the "Select Filter Criteria" section of a report was ignored when a report was run in the background.</p> <p>FIX: The product has been updated to fix the issue.</p>

Appliance Upgrade

Issue	Description
LOG-7434	<p>After an upgrade to Logger v4.5 GA, 5.0 Patch 1, or 5.0 Patch 2, a custom heap size that had been defined for the built-in connector was not preserved.</p> <p>FIX: The product has been updated such that a non-default value is preserved after the upgrade.</p>
LOG-7074	<p>When a Logger appliance was upgraded, a non-default heap size that was configured for the built-in connector was not preserved.</p> <p>FIX: The product has been updated such that a non-default value is preserved after the upgrade.</p>

Audit Events

Issue	Description
LOG-3581 TTP#54524	<p>Logger was not generating platform events when the GUI user login session expired.</p> <p>FIX: A platform event is generated when a user session expires.</p>

Authentication/Certificates

Issue	Description
LOG-7836	Passwords with more than 30 characters could not be created. FIX: The product has been updated to fix this issue.
LOG-7603	An email address could not contain an apostrophe (') when adding a user on Logger. FIX: The product has been updated to fix this issue.
LOG-7414	In certain situations, when a user was prompted to change their password after logging in to Logger and the user attempted to do so, an internal server error was generated. FIX: The cause of this issue has been fixed.

Configuration Backup and Restore

Issue	Description
LOG-5249 TTP#63584	Logger configuration backup included connector cache data (from the built-in connector), thus resulting in a larger than expected configuration backup file. FIX: The product has been updated such that connector cache data is no longer included in the configuration backup file.

Event Archive

Issue	Description
LOG-7954	Event Archives information has been updated in the Admin Guide in accordance with the enhancements made in this release.

Event Input/Output

Issue	Description
LOG-7881	<p>When a connector is caching and the cache is full, the oldest cache is dropped and the estimated cache value is reported in the logs. However, after the connector started dropping cache, it reported a negative value for the estimated cache size.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-7668	<p>When large events were forwarded from Logger to ESM and the additional data field was too long, the built-in connector would go down intermittently.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6722	<p>Performance issues would be experienced on Logger because established sockets would not time out.</p> <p>FIX: The product has been updated to fix this issue.</p>

Logger Appliance Platform

Issue	Description
LOG-7589	<p>If the Logger Postgres database became fragmented and filled up the partition where it resides, Logger would not start.</p> <p>FIX: The product has been updated to include a UI banner warning that informs you about Postgres fragmentation and if the disk is 100% full. When this message is displayed, run database defragmentation as described in the Logger Administrator's Guide.</p>
LOG-7313	<p>Stopping the connector via the monit CLI utility caused the appliance to reboot.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6697 TTP#63420	<p>On the Logger appliance, the postgres process would not start when it could not write any files to the XFS filesystem. As a result, Logger was non-functional.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6346 TTP#69311	<p>When a drive would fail, Logger did not provide any message on the UI.</p> <p>FIX: A banner message is now generated to indicate a failed drive.</p>

Reports

Issue	Description
LOG-8644	<p>Reports were failing and Monitor GUI page displayed this error message:</p> <p>"There was a problem configuring the report engine user rights. Please check that the report engine process is running successfully".</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-8408	<p>Only five scheduled reports could run at any time. Therefore, if more than five reports were scheduled to run for any given time, some of the reports would not run.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-8354	<p>When creating a new report, no selectable query was available in the pull-down menu.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-7342	<p>When the user created a new report, they are not able to associate a query to that report.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6838	<p>Saving a scheduled report redirected you to a page with frame/target problems.</p> <p>FIX: The product has been updated to fix the issue.</p>
LOG-6749	<p>When editing or saving scheduled reports, the Logger user interface exhibited unexpected behavior such as the Save button would not display, browser would display the main Logger menu in the Reports frame on the right-hand side, and so on.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6671 TTP#57690	<p>Members of the report group could not view scheduled reports.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6649 TTP#61498	<p>The Attributes list in Reports shows a few attributes that are internal to Logger. When these attributes are used, the resulting report contains unexpected results. All attributes listed after arc_sourceZoneResource are internal, including arc_eventTime, arc_deviceName, arc_rowId, and arc_others.</p> <p>FIX: Documentation has been updated to indicate that these attributes should not be used in queries.</p>

Search

Issue	Description
LOG-8264	<p>Search Group filter was not being enforced when searching by devices/device group.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-7864	<p>Epoch Time fields should be converted to human readable format in event exports.</p> <p>FIX: The product has been updated to display human-readable time formats.</p>
LOG-7837	<p>Display the accurate number of hits on the first page of the search results.</p> <p>FIX: The product has been updated to display accurate results.</p>
LOG-7447	<p>A full-text search for an IP address would run successfully but the search results would not export. The search results required the full-text string to be enclosed in parenthesis [()]. For example, XXX.XXX.XXX.XXX OR XXX.XXX.XXX.XXX would yield search results, but you could not export the results unless the query enclosed the IP addresses in parenthesis, as shown: (XXX.XXX.XXX.XXX OR XXX.XXX.XXX.XXX)</p> <p>FIX: The product has been updated to fix the issue.</p>
LOG-6726	<p>Peer search would not enforce the search group filter when a search was performed on local and peer Logger events.</p> <p>FIX: Search group filters are correctly enforced now.</p>
LOG-6650 TTP#65945	<p>When trying to use advanced search feature the following error would display:</p> <p>The search cannot be run, there is an error in your query: Invalid metadata declaration: [_deviceGroup]. Metadata terms cannot be evaluated before OR's. Make sure parentheses are properly put around OR clauses.</p> <p>Here is the example of the query generated automatically (which is incorrect): (destinationAddress = "192.168.36.12") OR (destinationAddress = "192.168.36.100") OR (destinationAddress = "192.168.36.201") _deviceGroup IN ["Prod-East", "Prod-East"]</p> <p>FIX: The product has been updated to fix this issue.</p>

Storage

Issue	Description
LOG-6640 TTP#63473	<p>If Logger's Storage Volume filled up to capacity, it would stop forwarding events.</p> <p>FIX: The product has been updated such that Logger's forwarding operation is not impacted even if the Storage Volume is approaching capacity.</p>
LOG-5582 TTP#65350	<p>If you created more than 40 storage rules, the following exception was generated:</p> <p>"com.arcsight.logger.common.persist.PersistenceException: org.postgresql.util.PSQLException: ERROR: value too long for type character varying(1000) "</p> <p>FIX: The product has been updated such that no exception is generated when more than 40 rules are created.</p>

System Administration

Issue	Description
LOG-7692	<p>After an upgrade to 5.0 Patch1 or Patch 2, the user would be unable to access System Admin panel intermittently, encountering a username/password prompt that couldn't be bypassed.</p> <p>FIX: The product has been updated to fix the issue.</p>
LOG-7411	<p>When logs were retrieved, it could result in an unusually high load average on Logger.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-7356	<p>In certain situations, deleting a static route would fail.</p> <p>FIX: The product has been updated to resolve this issue.</p>
LOG-7292	<p>After an upgrade to version 5.0, the System Admin page would take a long time to load.</p> <p>FIX: The product has been updated to fix the issue.</p>
LOG-6236 TTP#68919	<p>User account lockout feature (System Admin > Authentication > Password: Enable Password Lockout) was not working.</p> <p>FIX: The product has been updated to fix this issue.</p>
LOG-6060 TTP#68202	<p>Logger would only use the first resolved SMTP server IP address. If the first server was unavailable, Logger would not try the other resolved IP addresses.</p> <p>FIX: The product has been enhanced to include a Backup SMTP Server field. Logger will use this server if the primary one is not available.</p>

Issue	Description
LOG-5594 TTP#65414	If CAC authentication was enabled, Logger's login banner would not display when the CAC login was successful. The UI would display the "Monitor" page directly without first displaying the login banner.

FIX: The product has been updated to fix the issue.

Open Issues in this Release

This release contains the following open issues. Use the workarounds, where available.

Issue	Description
LOG-8863	When a software Logger running v5.0 Patch 2 is upgraded to v5.1, user-created and Compliance Insight Package(s) related report templates are not copied to the location where v5.1 is installed. As a result, when a report that uses one of these templates is run, the resulting report does not contain expected contents.

Workaround: Make sure you are logged in as the user who was used to perform the upgrade. Run the following command:

```
cp -rf  
<INSTALL_DIR>/L5355/arcsight/logger/Intellicus/reportengine/templates/adhoc  
<INSTALL_DIR>/current/arcsight/logger/Intellicus/reportengine/templates
```

Then, run the following commands to restart the web and report processes:

```
<INSTALL_DIR>/current/arcsight/logger/bin/loggerd restart web  
<INSTALL_DIR>/current/arcsight/logger/bin/loggerd restart reportengine
```

Issue	Description
LOG-8824	<p>If the current archive path on a software Logger is <install_dir>/current and the new archive path, specified during software Logger upgrade, is <install_dir>, the following error message is displayed:</p> <pre>"ArchivePostUpgrade: Error while moving archive. Exit code[1] stdout[] stderr[/bin/mv: cannot move 'INSTALL_DIR/L5355/UninstallerData' to a subdirectory of itself, 'INSTALL_DIR/UninstallerData']"</pre> <p>Once the above error is displayed, entering any path results in "Error (null)" error.</p> <p>Workaround: Run the following commands to re-launch the Upgrade Wizard so that you can enter a different archive location:</p> <ol style="list-style-type: none">1. Make sure you are using the same user as previous Logger installation.2. Move the archives files back to the original location. The archive files are named in YYYYMMDD format. For example, 20110529 <pre>mv <install_dir>/20110529 <install_dir>/L5355</pre>Repeat the above command until you have moved all the archives back to the original location.3. <pre>mv <install_dir>/arcsight <install_dir>/L5355 <install_dir>/current/arcsight/logger/bin/arcsight loggersetup -u L5355</pre>4. When prompted to enter an archive location in the Upgrade Wizard, enter any path except <install_dir>.

Issue	Description
LOG-8823	<p>The UI displays the following error message: "The application is currently unavailable. Please retry shortly."</p> <p>Understanding: This issue occurs when the web process on Logger runs out of memory. When this issue occurs, the logger_web.log log file will contain one or many of the following entries: java.lang.OutOfMemoryError: PermGen space</p> <p>If this log entry is found, follow the steps described in the Workaround section. Otherwise, call ArcSight Customer Support.</p> <p>Workaround: Logger appliance customers, please call ArcSight Customer Support.</p> <p>Software Logger customers, follow these steps:</p> <ol style="list-style-type: none">1. Run this command to stop the web process: <installdir>/current/arcsight/logger/bin/loggerd stop web2. Add a new JVM parameter in the <installdir>/current/arcsight/logger/bin/scripts/web.sh file. Look for the line that starts with "export JAVA_OPTS". Add the following parameter to the end of it, within the double quotes: "-XX:MaxPermSize=192m"3. Run this command to restart the web process: <installdir>/current/arcsight/logger/bin/loggerd start web
LOG-8807	<p>Software Logger processes fail to start fully after a restore from a backup configuration. The following message is displayed on the Logger UI:</p> <p>"Logger server could not be reached, please check the page System Admin Process Status."</p> <p>Understanding: This issue is specific to Logger software configuration in which the Reports dashboard is the default start page for all users, when they log in.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Stop all logger process manually from the command using loggerd command: <install_dir>/current/arcsight/logger/bin/loggerd quit2. Start logger process: <install_dir>/current/arcsight/logger/bin/loggerd start
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>

Issue	Description
LOG-8790	When the community string contains non-ASCII characters, the SNMP trap sent out has "?" in the community field.
LOG-8782	Although a Logger v4.5 appliance cannot peer with a software Logger running version 5.1, this combination may work in certain cases. Therefore, you might observe that saved searches running on this combination of peers are succeeding without any user interface error, but if you run the same search in interactive mode, from the Search box, the user interface displays an error to indicate that the search was run on incompatible versions of peers.
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-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/. Alternatively and for IE, 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>
LOG-8742	<p>If there is a long time gap (in the order of hours) between configuring the storage volume on your Logger and creating and configuring storage groups, the Logger can generate a large number of BufferOverflow Exceptions which fill up the Logger server.</p> <p>Understanding: This situation occurs because Logger's internal events are continuously generated but an internal storage group has not been created yet to store them.</p> <p>Workaround: Re-image the appliance using the Factory Reset instructions in the Logger Administrator's Guide.</p>
LOG-8740	<p>When beginning a maintenance operation, a blank screen is shown for a few seconds while waiting for maintenance mode to start.</p> <p>Workaround: The page refreshes itself and clear up the problem after maintenance mode has started.</p>
LOG-8728	<p>The chart operator does not accept a field that has been renamed using the rename operator. For example, rename priority as new_priority chart count(new_priority) by agentZoneURI, results in an error.</p> <p>Workaround: Include the rename operator after the chart command in such cases.</p>

Issue	Description
LOG-8709	<p>Admin user cannot delete a user who is either currently logged in or recently logged out (a few minutes ago).</p> <p>Workaround: Edit the user account to make it inactive. Wait a few minutes, then delete the account.</p>
LOG-8701	<p>The SQL editor in the Reports section displays arc_search_tmp Entities.</p> <p>Understanding: These are internal tables. Ignore them. Only use the displayed Events Entity.</p>
LOG-8660	<p>Context-sensitive Help for the integrated Connector Appliance module does not load. Instead, the Logger Administrator's Guide's table of content is displayed.</p> <p>Workaround: In the left-side pane, navigate to "Managing Connectors on Connector Appliance", or "Managing Repositories in Connector Appliance" to locate the relevant information. This issue will be fixed in a future release of Logger.</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 browser cache (on IE: Tools -> Internet Options -> Delete...) before going to System Locale page (and after rebooting appliance).</p>
LOG-8519	<p>If a SmartMessage receiver name includes native characters, the receiver cannot receive the incoming events.</p>
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>
LOG-8428	<p>The Trusted Certificates page (System Admin > SSL Client Authentication) fails to load. Except for a small graphic icon on the page, the page is blank.</p> <p>Workaround: Refresh the blank page and access it again by clicking SSL Client Authentication from the left pane.</p>
LOG-8231	<p>The list of SNMP destinations might not show the newly added destination right away.</p> <p>Workaround: Refresh the page after a few seconds and the destination is listed.</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: You to need edit the setting of the CIFS share and re-enter the username and password.</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 :</p> <p>"Unexpected EOF; was expecting a close tag for element <ns1:data>"</p>

Issue	Description
LOG-7658	<p>If a real-time alert and a saved search alert is created for the same event, the scheduled search alert may not trigger for several minutes after a real-time alert has triggered.</p> <p>Understanding: Because saved search alerts are scheduled, there is a delay due to the schedule set for the alert. In addition, if a saved search alert depends on internal events, which are flushed every 10 minutes, there might be an additional delay before the events are detected and the alert is triggered. ArcSight recommends that you set the search time range to \$now-X minutes or higher, where X is the time set in the Schedule field for a saved search alert to ensure that saved search alerts that depend on internal events will trigger as expected.</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:</p> <p>"Could not find an archive."</p> <p>Workaround: Perform a hard refresh of your browser window. For IE, use Ctrl-F5. For Firefox, use Ctrl-R.</p>
LOG-7297	<p>When viewing a scheduled report's output, drill-down clicks do not work.</p> <p>Workaround: Re-run the report manually to use drill downs. This issue doesn't affect ad-hoc reports.</p>
LOG-7165	<p>The privileges for pre-built reports on Logger are missing from the Add Group page if the Logger is a fresh install and you have not yet loaded the Reports page after installing this Logger.</p> <p>Workaround: Go to the Reports page. (This triggers the population of group privileges in the Add Group.) Go back to Add Group. The privileges for pre-built reports are displayed now.</p>
LOG-7099	<p>When values for 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>
LOG-6399 TTP#69852	<p>Reports restored from another Logger fail with the following error:</p> <p>"Failed to get scheduled job details as no record found for requested job in database."</p> <p>Workaround: Delete the scheduled job, re-create it with a NEW NAME, let it run. A scheduled job with the original name will fail with the above error.</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>
LOG-5348 TTP#64425	<p>A user with "Edit and Save Reports" right set to No is able to edit and save reports.</p>

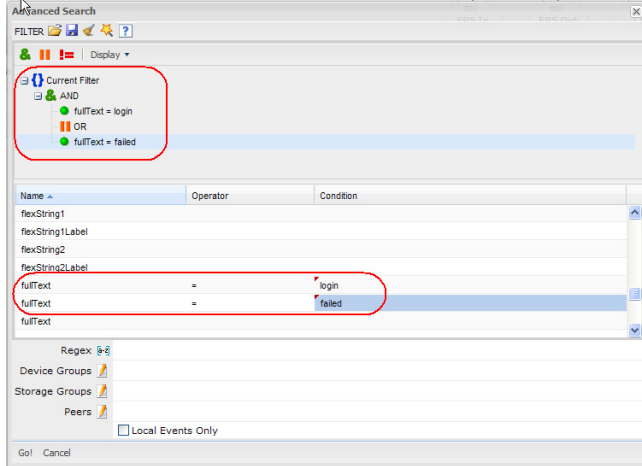
Issue	Description
LOG-4990 TTP#61378	<p>Changes made to existing SMTP information (System Admin > Network > SMTP) are not automatically detected and effective.</p> <p>Documentation on SMTP configuration indicates a reboot is not required when information is configured. However, that is valid only when the information is configured the first time. Any updates to existing information are not effective automatically.</p> <p>Workaround: Restart the forwarder process for the new information to take effect. To restart the process:</p> <ol style="list-style-type: none"> 1. Click System Admin > Process Status. 2. Click processors from the Process list. 3. Click Restart in the bottom right corner of the screen.
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>Understanding: This behavior is in accordance with the Content Import/Export feature design. Therefore, make sure the importing Logger has the same configuration setup as the exporting Logger.</p>

Known Behaviors From Previous Releases

The following items represent characteristics of the product that work as-designed, as-expected, are not bugs, or are known issues that involve third-party products.

Function	Issue Number	Description
Database Migration	LOG-4234 59324	<p>On an L7100 Logger, the storage volume size and the storage group size decrease by 230 GB when database is migrated on it.</p> <p>Understanding: About 230 GB of space is allocated to the migrated database; therefore, the storage volume size and group size decrease.</p>
Group Administration	LOG-1738 44570	<p>If a user belongs to a Logger Reports group with <i>Global access to all report objects and permission to change report engine configuration</i> privileges, the user does not see the Scheduled Reports menu item (Reports > Scheduled Reports). The user needs to belong to the following two groups with the specified privileges to see the Scheduled Reports menu item.</p> <ul style="list-style-type: none"> • Logger Reports Group with the <i>Global access to all report objects and permission to change report engine configuration and View, run, and schedule all reports</i> user rights set to Yes. • Logger Rights Group with the <i>View Scheduled Tasks</i> user right set to Yes.

Function	Issue Number	Description
Logs	LOG-6638 54669	<p>The Retrieve Logs action (Configuration > Retrieve Logs) would fail when large files were part of the set of files to be retrieved.</p> <p>Understanding: The product has been updated such that the Retrieve operation does not fail when large files are part of the set of files to be retrieved; however, files that are too large to be handled by the zip tool are skipped and not retrieved.</p>
Monitor	LOG-2387 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-4998 61405	<p>During the hour of Daylight Savings Time (DST) adjustment, the CPU Usage and Event Flow gauges report only three hours worth of data instead of four hours.</p> <p>Understanding: This issue arises only at DST adjustment time and lasts only for one hour.</p>
Performance - System	LOG-1222 41683	<p>Downloading a large CSV file can make the browser unresponsive.</p> <p>Workaround: Wait until the CSV file has been downloaded, or use another browser to access Logger.</p>
Platform	LOG-2683 50364	<p>When adding a disk or changing a SAN configuration, you need to reboot Logger to refresh the LUN table and reflect the current state of the SAN.</p>
Receiver	LOG-765 39300	<p>The default port for a File Transfer Receiver is 22. Selecting the FTP protocol (typically port 21) does not automatically change the port.</p> <p>Workaround: Manually change the port, if desired.</p>
Reports	LOG-1888 44952	<p>Base Foundation and Solution report queries can be edited.</p> <p>Workaround: ArcSight recommends that you first make a copy of these reports and then edit them.</p>
Search	LOG-1203 41632	<p>Search uses an event's Event Time (if known) to determine if it is in a given time range, while Forwarders use the time that the event was received by Logger. The difference between Event Time and Receipt Time will be small if events are sent to Logger in real time, but can be significant if events are aggregated before being sent to Logger. The time difference can also be significant if the source devices timestamp events incorrectly.</p>

Function	Issue Number	Description
Search	LOG-4654 / LOG-4775 60354 / 60716	<p>When using the Search Builder (accessed using the Advanced Search link on the Search page) to create a query, user interface is not intuitive about how to enter a keyword (full-text) term.</p> <p>Understanding: To specify a keyword (full-text search), use the <i>fullText</i> field under the Name column, as shown in the following figure. To locate the <i>fullText</i> field, scroll down.</p> 
Storage	LOG-3200 52377	<p>Storage groups that are smaller than the minimum of 5GB might lose data due to retention policy enforcement.</p> <p>Workaround: ArcSight strongly recommends that you archive events in those storage groups before upgrading. Additionally, use the storage group resizing feature available starting with Logger v4.0 GA to ensure that the group size is at least 5 GB. For more information about storage group resizing, see <i>Logger v4.0 SP1 Administrator's Guide</i>.</p>

Open Issues From Previous Releases

The following table lists the open issues from previous releases. These issues will be addressed in a future release. Use the workaround noted, where available.

Function	Issue Number	Description and Workaround
Alerts/Filters	LOG-1608 44219	When multiple filters are selected for alerts, alerts might not generate because the selected filters are ANDed together, which might return an empty result set.

Function	Issue Number	Description and Workaround
Certificates	61134 LOG-4885	<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</p> <p>Configuration > Alerts > Certificates</p> <p>Workaround: Refresh the page to update the list. The deleted certificate is removed from the list.</p>
	61631 LOG-5052	<p>SSL Certificate Installation Results page (System Admin > SSL Server Certificate > View Results) displays the following error instead of the installation results for an SSL certificate:</p> <p>--- No Results Exist ---</p> <p>Workaround: Because this issue is only experienced in the Firefox browser, use Internet Explorer to view these results.</p>
Configuration Backup and Restore	LOG-370 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. Also, see bug 57778.</p>
	LOG-3279 52540	Published reports are not included in a Report backup.
	LOG-3944 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-5239 63513	<p>If you rebuild a Logger, enable indexing on it, and then restore its configuration from a backup, you might receive the following error when running a query:</p> <p>"Database connection error when running a query"</p> <p>Understanding: This error occurs because the restore process restores the backed up indices. These indices conflict with the indices initialized when Logger was rebuilt.</p> <p>Workaround: Do not enable indexing on a Logger whose configuration will be restored from a backup that was made on a Logger on which indexing was enabled.</p>
Configuration Backup and Restore	LOG-5024 61517	<p>If the system to which Logger is configured to back up its configuration is reinstalled or its SSL key is changed, the configuration backup fails because the SSL key cannot be refreshed from the Logger UI.</p>

Function	Issue Number	Description and Workaround
Connector Appliance	LOG-5300 CONAPP-2413 64031	The Logs link in the left side menu (Configuration > Repositories) is missing when a user belongs to only the System Admin Group. Workaround: Assign the user to the Logger Rights Group in addition to the System Admin Group.
Content Export/Import	LOG-2941 51630	The type associated with imported filters cannot be changed from shared to saved search.
Defragmentation	LOG-3926 57638	A blank screen might display when you enter maintenance mode for database defragmentation. Workaround: Refresh the screen manually using your browser refresh function.
FIPS 140-2	65357	When a FIPS-enabled Logger is upgraded from v4.0 GA to v4.0 SP1, FIPS gets disabled on the ESM Forwarder (System Admin > FIPS 140-2). An attempt to reenale FIPS on the forwarder is unsuccessful. Action: Contact ArcSight Customer Support for further assistance.
Forwarder	LOG-2244 47758	A forwarder configured with a filter might not forward events that match the specified end time. Workaround: Extend the end time by 1 second to ensure that all events are forwarded appropriately.
	LOG-6290 69066	Logger does not impose a limit on the number of forwarders that can be configured. However, configuring a large number of forwarders can have a severe impact on system performance. Understanding: The maximum number of forwarders is limited by your system's resources—memory, CPU, disk input/output.
Maintenance Mode	LOG-7048	When you click on Restart or Reboot after performing an action in maintenance mode, the following error is displayed: "The application is currently unavailable. Please retry shortly." Understanding: Logger is continuing to restart or reboot, therefore, keep refreshing the UI screen until the login screen is displayed.

Function	Issue Number	Description and Workaround
Peer Logger	LOG-4986 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 reinitiating the relationship.</p>
Reports	LOG-1703 44508	<p>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.</p>
	LOG-1936 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>
	LOG-1956 / LOG-2355 45163 / 48618	<p>The time range and constraints information is not applied when accessing information from reports through the drilldown links of a scheduled published report.</p>
	LOG-1991 45447	<p>Some predefined report templates do not support i18n characters.</p> <p>Workaround: Test the report template for the desired character set before production use. This issue will be fixed in a later release.</p>
	LOG-2012 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-2019 45570	<p>After upgrading to Logger v4.5 GA, custom Report Configuration settings (Reports > Reports Administration) are reset to the default values.</p> <p>Workaround: Re-enter the custom values after the upgrade is complete.</p>
	LOG-2350 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-3187 52330	<p>The time taken to run a scheduled report is not reported correctly in the Logger user interface.</p>

Function	Issue Number	Description and Workaround
Reports	LOG-5037 61563	A report template with the alignment setting of "Center", creates a report with left-aligned data.
	LOG-5588 65374	Published reports cannot be viewed after upgrading to v4.0 SP1 Patch 1. The following error is generated when a published report is viewed post upgrade; "Failed to generate report from rpg because server failed to deserialize the Report Pages"
	LOG-6288 69058	When a scheduled report is created, the report name selected from the Report Name drop-down menu does not persist after you save the report. Workaround: You need to click the GO button next to the drop-down menu after selecting a Report to persist the report selection. Note: Once you have defined a scheduled report, you cannot change the selected report. If you need to change the to a different report, delete the scheduled report and define a new one.
	LOG-6295 69076	If the Format setting is configured to JVISTA in Widget Properties when designing a Dashboard, the Dashboard is blank. Understanding: Do not use JVISTA as this is not a supported option.
	LOG-6652	In the FireFox browser, the Report Template editor (Reports > Design - Template Styles > <i>Select a template</i> > Edit Layout) is not usable because the pull-out menus cannot be re-sized, the drop-down menus do not display the full list of options, and some windows open behind the editor. Workaround: Use the IE browser.
	LOG-6661	If a report dashboard uses an HTTPS external URL, the Logger browser window is taken over by the external link.
Scheduled Jobs	LOG-7078	On a software Logger machine, a printer configured with special characters such as "&" may prevent scheduled reports from running.
	LOG-6209 68824	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.

Function	Issue Number	Description and Workaround
Search	LOG-4329 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:d4:08:00 SRC=192.168.10.153 DST=192.168.10.255 LEN=229</p> <p>Workaround: This problem only occurs for a very small number of devices, which use this particular format. The workaround is to search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address. For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255.</p> <p>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-4888 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:</p> <p>"Failed to construct a legal query, please check your query elements and try again!"</p> <p>Additionally, once this warning is displayed, you cannot switch to Tree View to build a single condition query.</p> <p>Understanding: Color Block View expects two conditions. Therefore, do not use this view if your query contains only one condition.</p> <p>Workaround: To get rid of the warning message so that you can use the Tree View:</p> <ol style="list-style-type: none"> 1 Switch to Tree View. 2 Include a second "placeholder" condition. 3 Click GO. <p>Once the query is displayed in the Search box (on the main Search page), remove the second, "placeholder" condition.</p>
	LOG-4584 60121	<p>The Search Builder (accessed using the Advanced Search link on the Search page) when used in Tree view, allows you to enter invalid operators for conditions. The tool does not generate any warning.</p>

Function	Issue Number	Description and Workaround
Search	LOG-4963 61305	<p>Results in the Search Analyzer window are repeated the same number of times as the number of peers on which the search is run. For example, the following are the Search Analyzer results for a search run on two Loggers:</p> <pre>Info "The field [\"full text search\"] is not indexed on host [127.0.0.1]","The field [\"full text search\"] is not indexed on host [192.168.35.140] "</pre> <pre>Info "The field [\"full text search\"] is not indexed on host [127.0.0.1]","The field [\"full text search\"] is not indexed on host [192.168.35.140] "</pre>
	LOG-5171 62955	<p>A user with default Logger search rights ("Yes" on local and peer search) cannot include storage groups, device groups, and peers in a query when building that query using the Search Builder (accessed using the Advanced search link on the Search page).</p> <p>Workaround: Enter the storage group, device group, or peer information in the Search text box on the main Search page.</p>
	LOG-5181 63055	Search results are not highlighted for values that match the IN operator in a query.
	LOG-6199 LOG-6965	<p>When the time change due to Daylight Savings Time (DST) takes place on November 7, 2010, 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. To ensure that all events are returned, specify an end time of 2:00:01 or later.
	LOG-6644 66491	At times a search operation would fail with the following message right after the search had been initiated: "Search timed out"
	LOG-6273 69023	When search results are exported, the time elapsed to export the events is not displayed.

Function	Issue Number	Description and Workaround
Search	LOG-6283 69044	If the timezone setting is changed from PDT to JST on the software version of Logger, the events displayed in the browsers that connect to it do not reflect the correct event time.
	LOG-7027	For search queries that involve pipeline operators, the Scanned events count might stop incrementing while the Hits count and the Elapsed time continue to increment , even though in bursts. This behavior is intermittent.
	LOG-7046	On a software Logger, the time displayed on the histogram might not match the event time. Understanding: This behavior is observed when the <code>/etc/localtime</code> file is not symbolically linked to the correct timezone. Workaround: Make sure that the <code>/etc/localtime</code> file is symbolically linked to the correct timezone in the <code>/usr/share/zoneinfo</code> file as follows: <pre>sudo ln -s /usr/share/zoneinfo/<timezone> /etc/localtime</pre> Then, restart the system on which software Logger is installed.
	LOG-6284 69048	If the timezone setting on the Logger machine is different from the (local) machine from which you are connecting to Logger, the time ranges in the histogram are based on the local machine timezone while events in the search results display the Logger timezone. For example, if Logger is configured in PDT, while the browser from which you are connecting to it is on a machine in JST, the histogram displayed in the browser shows time ranges in JST, while the events in the search results show the timestamp in PDT.
	LOG-6206 68820	If a single event matches a query that contains the <code>where</code> operator, the event is not displayed in the search results screen. However, the "Hits" counter and the histogram display the correct number (1). Workaround: Click the histogram to display the event in the search results screen.
	LOG-6343 69283	The number of Hits displayed on top of the Search Results screen may differ from the number shown at the bottom right of the screen in the "Displaying 1 - x of x" message. Workaround: Refreshing the browser syncs the two counts and displays the actual count.
	LOG-7243	A field created using the <code>rex</code> search operator is not exported in the CSV format if the "All Fields" option is unchecked. For example, in the following query, the field "assignedAddress" is not exported: <pre> cef name, cn1 rex field=cn1 " (?<assignedAddress>[0-9]+) "</pre> Workaround: To export such fields, prefix the field names with an asterisk (*) in the Export dialog. Therefore, for the above example, use <code>*assignedAddress</code> to export the values in the assignedAddress column.

Function	Issue Number	Description and Workaround
Search Operators	LOG-6297 69095	<p>When a where operator is included in a query, the query performance can be significantly impacted. As a result, the query may not complete running and the user interface may hang.</p> <p>Understanding: This is a known issue and will be addressed in a future release of Logger.</p> <p>Suggestive Action: You can Cancel the search when this situation occurs and rerun the query with these changes:</p> <ul style="list-style-type: none"> • Reduce the time range of the query • Refine the query to increase the selectivity of the query
	LOG-6314 69160	<p>The top and rare operators only pass forward fields specified for the operators; any other fields that might have been defined previous to those operators are rendered undefined. For example, the following query does not complete successfully because field "b" is considered undefined for the chart operator; therefore, the query generates an error.</p> <pre> cef a b c top a c chart _count by b</pre> <p>Workaround: Include all fields you would like to use later in the pipeline in the top command. For example, change the above example to:</p> <pre> cef a b c top a b c chart _count by b</pre>
Storage	LOG-2679 50338	<p>The size of RFS or SAN mounts might display as 0, especially when switching between RFS and SAN, when the mounting is initially done, or when access to a remote mount is delayed.</p> <p>Workaround: Refresh the browser or check the page again later.</p>
	LOG-3684 55676	<p>The Logger user interface does not prevent two Loggers from mounting the same NFS mount point.</p> <p>Recommendation: Make sure that only one Logger can write to one NFS mount point. If multiple Loggers (or other systems) mount to the same location and write to it, data will be corrupted.</p>
	LOG-4595 60152	<p>Even if pre-allocation of storage fails before the minimum requirement has been met, Logger allows you to skip pre-allocation and proceed to storage configuration.</p> <p>Recommendation: 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>
User Interface	LOG-1384 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>
	LOG-2433 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>

Function	Issue Number	Description and Workaround
User Interface	LOG-3244 52452	In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report. Workaround: Use the IE browser instead.
User Privileges	LOG-1050 40872	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. Workaround: Provide Device Group and Storage Group names that do not reveal internal information.

