Release Notes
ArcSight Logger™

Version 4.5 GA (Build L4892)

July 22, 2010

Release Notes ArcSight Logger™, Version 4.5 GA (Build L4892)

Revision History

Date	Product Version	Description
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 Patch1	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 Patch1	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.
09/30/09	Logger v3.0 SP1 Patch 1	Patch 1 for Service Pack 1. (Release supports new hardware)
08/27/09	Logger v3.0 SP1	Updated Database Migration instructions.
08/03/09	Logger v3.0 SP1	Service Pack 1 for v3.0.

Release Notes template version: 2.0.0

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://support.arcsight.com
Protect 724 Community	https://protect724.arcsight.com

Contents

ArcSight Logger™ v4.5 GA

These release notes provide information about the ArcSight Logger v4.5 GA (L4892) 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 Version 4.5 GA

Logger v4.5 GA is the first Logger release that is available for two form factors: the Logger appliance and a software version, which can be installed on a supported platform. The features available in both form factors are identical except for a few differences in the platform management functionality (accessed through the System Admin menu item). In addition, licensing requirements for both are unique and are described in this section. This section also lists the new features and enhancements introduced in Logger v4.5 GA.

Software Version of Logger

This release introduces the first Logger in a software form factor. You can download and install this software version of Logger on a supported platform. You can also install the software on a VM image of a supported platform. You need a valid license file to install and use the software version of Logger.

The Logger software is available for download from the ArcSight Customer Support web site at https://support.arcsight.com. You can also obtain a valid license, which is required to use the product, from ArcSight Customer Support. For details about supported platforms and installation instructions, see "Installing the Software Version of Logger v4.5 GA" on page 8.

License Enforcement

Both form factors of Logger require valid license files. A license file enforces validity and limits on the time, maximum amount of data stored per day, and aggregated storage used on the system. On the software version of Logger, limits depend on the type of license you purchased from ArcSight.

For a detailed description of how licensing works on the software version of Logger, see the topic "How Licensing Works on the Software Version of Logger" in the *Logger v4.5 Administrator's Guide*.

Saved Search Alert

In addition to real-time alerts, Saved Search alerts are now available on Logger. The Saved Search alerts are saved queries that run on a preconfigured schedule and send alerts when a specified number of matches occur within the specified threshold. Alerts can be sent to preconfigured e-mail, SNMP, ESM, or syslog destinations.

Queries for these alerts are defined using the flow-based search language (new in Logger v4.5) that allows you to specify multiple search commands in a pipeline format, including regular expressions. Aggregation operators such as chart and top cannot be included in the search query.

For more information about Saved Search Alerts, see the topic "Alerts" in the *Logger v4.5 Administrator's Guide*.

Storage Volume Increase

You can extend the storage volume size you established during Logger initialization at any time. Once extended, the volume size cannot be reduced.

For more information, see the topic "Storage Volume Size Increase" in the *Logger v4.5 Administrator's Guide*.

Search Operators and Regex Helper

The significant usability and functionality improvements made in Logger v4.0 for searching events are taken a step further in this release. A flow-based search language that allows you to specify multiple search commands in a pipeline format, including regular

expressions, has been introduced in this release. The language includes several operators that enable you to extract data of interest from matching queries, process it, and (optionally) create charts and reports from it.

The following pipeline operators have been introduced in this release:

- chart
- eval
- fields
- head
- rare
- regex*
- rex
- sort
- tail
- top
- where

* not a new operator in this release, but follows a new syntax.

For more information about search operators, see the topic "Search Operators" in the *Logger v4.5 Administrator's Guide*.

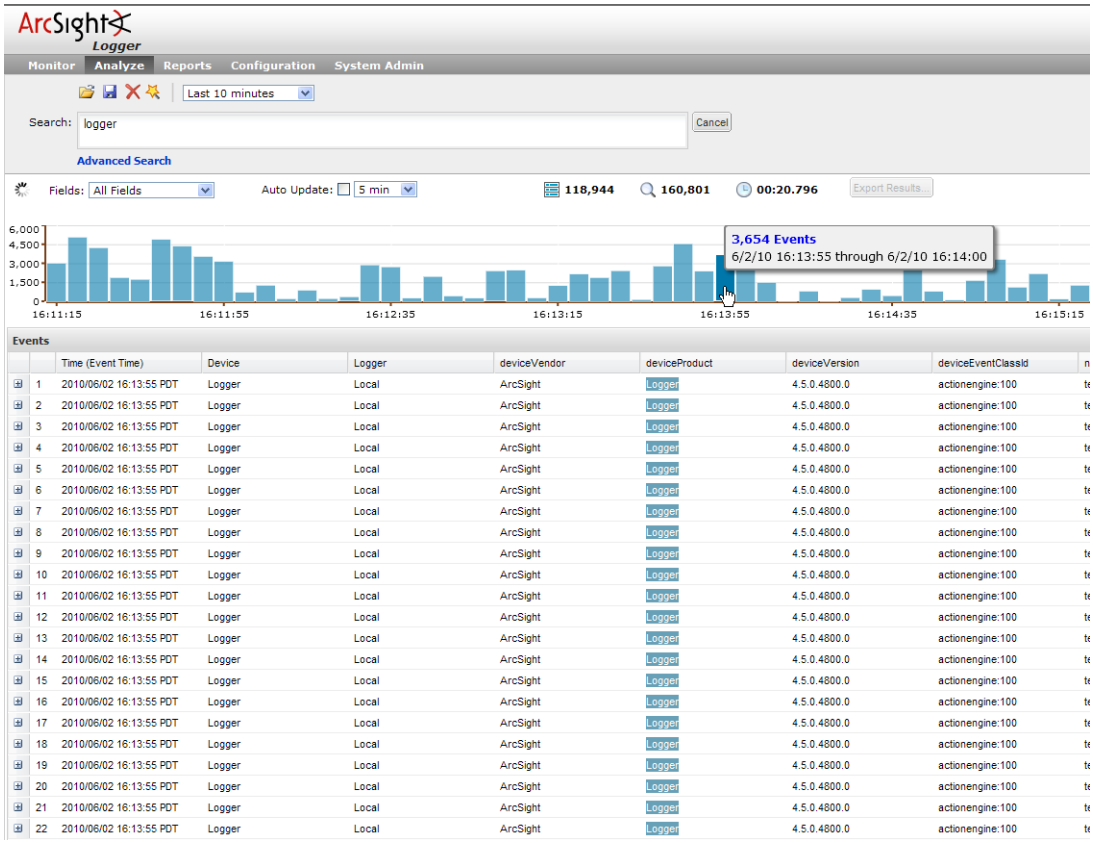
To ease the task of creating regular expressions for the `rex` operator, a Regex Helper tool is available in this release. The tool makes inserting rex expressions in a search query more efficient and less error prone. The tool parses a raw or non-CEF event into fields and displays them as a list. You select the fields that you want to include in the `rex` expression of a query. The selected fields are automatically inserted in a search query as a rex expression.

For more information about the Regex Helper tool, see the topic "Regex Helper Tool" in the *Logger v4.5 Administrator's Guide*.

For more information about searching and analyzing events, see the topic "Searching for Events on Logger" in the *Logger v4.5 Administrator's Guide*.

Histogram for Search Results

A histogram provides a graphical representation of the distribution of events that match a search query. The distribution is based on the time range specified in the query. That is, the X-axis represents event time and Y-axis represents the number of matching events, as shown in the following figure. Histogram enables you to randomly drill-down to events in a specific time period. For example, to investigate a spike in failed logins during a particular time, or a drop in the number of TCP connections to a server within a time period.



Histograms are automatically generated for search queries run through the Search page. Scheduled searches do not output a histogram.

Once a histogram is displayed, you can hide it by clicking the Show/Hide icon ( ) in the right-hand corner of the Search Results page.

- The first one million matching events are plotted on the histogram. If a search query matches more than one million events, an informational message is displayed on the screen.

  If you need to use the histogram view for event analysis for a search query that matches more than one million events, ArcSight suggests that you either adjust the time range specified in your search query such that less than one million events are matched to obtain a complete and meaningful histogram or refine the query such that the total number of hits is under one million events.
- Histograms are only displayed for local searches and not for peer searches.

For detailed information about histograms, see the topic "Guidelines for Using the Histogram" in the *Logger v4.5 Administrator's Guide*.

System Content Update

This release includes system content applicable for IT operations and application development environments. A number of predefined filters for commonly searched event

types are available. For example, Net-DHCP Lease Events, Net-Port Links Up and Down, bandwidth utilization, failed logins, Unix-Password Changes, and so on.

You can use these filters to quickly find events of interest without defining queries first. You can also use these filters as a starting point for creating customized filters for your environment.

For a complete list of available filters, see the topic "System Filters/Predefined Filters" in the *Logger v4.5 Administrator's Guide*.

Exporting Search Results

Search results can now be also exported in PDF form. The PDF format is useful in generating a quick report of the search results. The report includes a table of search results and any charts generated for the results. Both, raw and CEF events, can be included in the exported report.

For more information, see the topic "Exporting Search Results" in the *Logger v4.5 Administrator's Guide*.

New Internal Event

The following new internal event for the amount of storage space used by a storage group has been added.

Device Event Category: /Monitor/StorageGroup/Space/Used

Device Event Class ID: storagegroup:100

In the following example "storagegroup:100" event, the "fsize" field provides total GB space, the "cn1" field provides the percent of space used, and the "fname" field provides the storage group name.

```
CEF:0| ArcSight|Logger|4.5.0.4862.0|storagegroup:100|Logger
Internal Event|1| cat=/Monitor/StorageGroup/Space/Used
fileType=storageGroup cs2=CurrentValue cnt=1 dvc=192.168.36.232
fsize=10 type=0 cn2=7 cn1=70 rt=1278516044208 cn1Label=value
cn2Label=retention period (days) fname=Default Storage Group
cs2Label=timeframe
```

Peer Search Update

Peer Loggers can run different versions and peers can be configured on different form factors. However, these are the only supported paths for running a search across peers:

- A search from a v4.0.x Logger to v4.5
- A search from v4.5 Logger to v4.0.x
- A search from v4.5 Logger to v4.5

Search operators (such as cef, chart, top, and so on) cannot be used for searches across peer Loggers.

For more information about peer searching, see the topic "Searching Peer Loggers (Distributed Search)" in the *Logger v4.5 Administrator's Guide*.

Number of Reports that can Run Concurrently

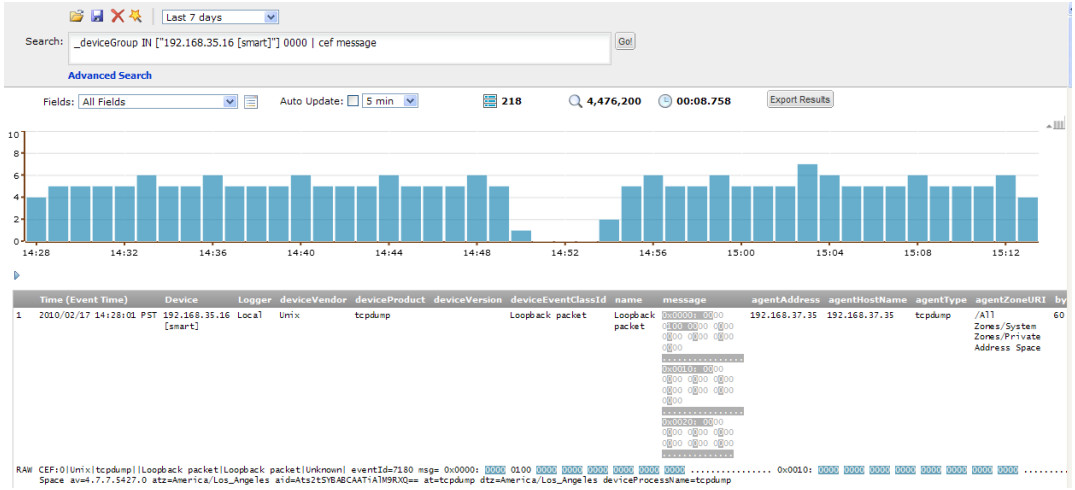
In earlier versions of Logger, you could run up to two report concurrently. Starting with this release, you can run up to five concurrent reports on a Logger.

Multi-line Data Display

An event message might span multiple lines separated by characters such as newline (\n) or carriage return (\r). For example,

0x0000: 0000 0100 0000 0000 0000 0000 0000 0000 ....
0x0010: 0000 0000 0000 0000 0000 0000 0000 0000 ....
0x0020: 0000 0000 0000 0000 0000 0000 0000 ....

Logger v4.5 user interface displays such a message in the expected multi-line format and does not remove the line separators and collapse the message into one line, as shown in the following figure.



Enhancements to Search Results Display

The following enhancements have been made to the search results display page:

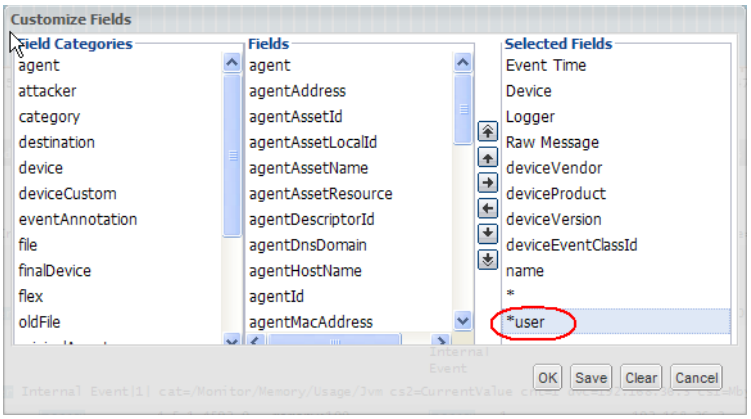
- A well layed out, columnar, grid-like search results display that is easier to read.
- Ability to adjust the widths of displayed columns to suit your needs.
- Ability to display the raw form of a single event or all events.
- Abillity to skip to the last page or to a specific page number in the search results display.

For more information about these enhancements, see the topic "Understanding the Search Results Display" in the *Logger v4.5 Administrator's Guide*.

User-Defined Field Set

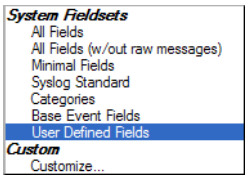
When you use a search operator that defines a new field, such as cef, rex, or eval, a new column for each field is added to the currently selected display. These newly defined fields are displayed by default. A new field ,*user (shown below), in field sets controls the display

of fields defined by search operators. When *user is included in the Selected Fields list of a custom field set, the newly defined fields are displayed.



A new field set, User-Defined Fields, is also available in this release that enables you to view only the newly defined fields.

The "User-Defined Fields" field set is available as a drop-down option from the "Fields:" menu on the page where search reults are displayed.



For detailed information, see the topic "Field Set" in the *Logger v4.5 Administrator's Guide*.

Other Information You Need to Know

- Prior to Logger v4.5, audit events generated for alerts were written to the Internal Storage group and forwarded to ArcSight ESM (if forwarding was configured) by default. Starting with v4.5, audit events for alerts are only written to the Internal Storage group and not forwarded to ESM by default. If you need to forward these audit events to ESM, please contact ArcSight Customer Support for assistance. Please note that this change only applies to audit events generated for alerts; other audit events are unaffected.
- To ensure system performance, a maximum of 200 alerts are allowed per saved search alert job. Therefore, if a saved search alert job triggers more than 200 alerts, only the first 200 alerts are sent out for that job iteration; the rest are not sent. Additionally, the job is aborted so it does not trigger more alerts for that iteration and the status for that job is marked "Failed" in the Finished Tasks tab (Configuration > Scheduled Tasks > Finished Tasks). The job runs as scheduled at the next scheduled interval and alerts are sent out until the maximum limit is reached.

  This limit does not exist on the real-time alerts.
- The description in the "How Licensing Works on the Software Version of Logger" topic lists "Time Limit" as one of the limits enforced by a license. This information is incorrect. Only data limit and aggregated storage limit are enforced.

Supported Browsers

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

- Internet Explorer: Versions 7 and 8
- Firefox: Versions 3.0 and 3.5

Documentation for Logger

Documentation for Loggers in both form factors is available as online Help and a PDF formatted Administrator's Guide. Both forms of documentation are integrated in the product.

The *Logger Administrator's Guide* now contains information pertinent to both form factors of Logger. Whenever an option or a field is handled differently on the appliance than the software version of Logger, the document explains the action for both form factors.

Example: Logger **appliance** can export events that match the current query locally, to an NFS mount, a CIFS mount, a SAN (on select Logger appliance models), or to the browser as a file to be downloaded. Events from a **software version of Logger** can be only exported locally to Logger (to the `/opt/data/logger` directory) or to the browser from which you connect to Logger.

Whenever there are significant differences between the two form factors, the information has been divided into sections, with one section containing information about the appliance and the other section containing information about the software form factor. For example, the System Administration chapter is divided in two sections—Section 1 for the options available on the appliance, and Section 2 for options available on the software version of Logger.

Installing the Software Version of Logger v4.5 GA

The information in this section is applicable for installing the software version of Logger on a supported platform of your choice. If you have a Logger appliance, see instructions in "Upgrading the Logger Appliance to v4.5 GA (L4892)" on page 11 to upgrade it to Logger v4.5GA.

The software version of Logger is available for download from the ArcSight Customer Support web site at https://support.arcsight.com. You need to have a server with supported operating system and storage available to install the sofware Logger. A valid license is required to use the product, which is also available from ArcSight Customer Support.

Supported Platforms and Browsers

You can install the software version of Logger on a platform with the following specifications. For a detailed capacity planning guide, see the *Capacity Planning for*

Software Version of Logger document that is available for download from the ArcSight Customer Support site at https://support.arcsight.com.

Specification	Details
Certified Operating Systems	• Red Hat Enterprise Linux (RHEL), version 5.4, 64-bit • CentOS, version 5.4, 64-bit **NOTE:** A VM installation of the above listed operating systems is supported.
Other Supported Operating Systems	• Oracle Enterprise Linux (OEL) 5.4 • Red Hat Enterprise Linux (RHEL), version 4.x, 64-bit • CentOS, version 4.x, 64-bit **NOTE:** A VM installation of the above listed operating systems is supported.
CPU, Memory, Disk Space	**For Small to Medium Deployments** • CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4 - 12 GB (12 GB is recommended) • Disk Space: 100 - 120 GB (120 GB is recommended) **For Medium to Large Deployments** • CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12 - 24 GB (24 GB is recommended) • Disk Space: 120 - 400 GB (400 GB is recommended) **NOTES:** • The disk space needs to be on the partition where the `/opt` directory exists. Specifically, most of this space should be available for `/opt/data/logger` directory. • Make sure that there is an additional 780 MB of free space available in the `/tmp` directory; otherwise, installation will fail and the installer will prompt you to specify another location with sufficient free space. • SAN can be used for storing events, however, this LUN must be mapped to the `/opt/data/logger` directory on the system on which the software version of Logger is installed. Using NFS as primary storage for events on the software version of Logger is not recommended.
Browsers	• Internet Explorer: Versions 7 and 8 • Firefox: Versions 3.0 and 3.5 Adobe Flash Player v9.0.x plug-in is required on these browsers for some of the features, such as Histogram and charts, to work.
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install the software version of Logger.

Prerequisites for Installation

Make sure these prerequisites are met before you install the software version of Logger:

- The hostname of the machine on which you are installing Logger v4.5 cannot be "localhost". If it is, change the hostname before proceeding with the installation.

- You must not have an instance of PostgreSQL installed on the Linux machine on which you will install Logger v4.5. If pgSQL exists on that machine, uninstall it before proceeding with the installation.
- Ensure that the umask setting in the `/etc/bashrc` file and your local `.bashrc` file has not been modified on the system which you are installing the Logger software. If this setting is modified, Logger might not function as expected.

Installation Steps

To install the software version of Logger:

1. Make sure the machine on which you will be installing the software-downloadable Logger complies with the requirements listed in "Supported Platforms and Browsers" on page 8 and the prerequisites listed in "Prerequisites for Installation" on page 9 are met.
2. Obtain these files from the ArcSight Customer Support and copy them to the machine on which you will be installing Logger v4.5:

   Software-downloadable Logger installer: `logger_4892.install`

   License file: `<license_file>.zip`
3. Run this command from the directory where you copied the software-downloadable Logger installer and license file:

   ```
   perl logger_4892.install <license_file>.zip
   ```

   The installer prompts you to select whether you want to proceed with a Typical or a Custom installation.

   If you choose the "Typical" installation, you do not need to initialize Logger after installation is complete because indexing, storage groups, and storage volume are automatically configured during the installation and the Logger service is automatically started once installation is complete. Additionally, you do not need to reboot the system on which you are installing the software version of Logger after completing the installation.

   Note: If you install Logger using the "Typical" option, you can change the names of the storage groups and increase the storage volume size, however, you cannot disable indexing, or add or remove storage groups post installation.

   The "Custom" installation enables you to customize and configure indexing, storage groups, and storage volume after the installation is complete.

   Whether you choose Typical or Custom installation, the installer prompts you to confirm the following requirements before proceeding with the installation.

   ```
   Please select installation type:
        1. Typical Installation
        2. Custom Installation
   Choice[1 or 2]: 1
   Installing license.
   Before proceeding with the installation, please ensure the
   following:
   1. The system time is correctly set: Tue Jun  8 12:40:59 2010
   2. An NTP server has been configured and confirmed to work.
   Are these requirements met [y/N]? y
   NOTE: You are about to begin the installation.
   Proceed [y/N]? y
   ```

This installation program also generates an uninstaller in the same directory, which you can use to uninstall the software version of Logger at any time.

Once the installation in the previous step is complete, reboot your machine when prompted to do so.

Once the machine is back up and running, launch a supported browser on another computer to connect to the software-downloadable Logger using this URL:

`https://<IP address or hostname of Logger v4.5 machine>/`

4 Use these credentials to log in for the first time:

Username: `admin`

Password: `password`

If you chose Custom installation when installing Logger, you are prompted to set up a Storage Volume, which is the first step of Logger initialization process. Follow the initialization sequence described in the *Logger v4.5 Administrator's Guide*, in the section "Initialization for all Loggers" on page 26 to complete Logger initialization. Once you have initialized your Logger, you are ready to use it.

However, if you chose Typical installation, you do not need to do anything further and can start using Logger.

Upgrading the Logger Appliance to v4.5 GA (L4892)

The information in this section only applies to Logger appliances. If you are installing the software version of Logger, see "Installing the Software Version of Logger v4.5 GA" on page 8 for instructions.

You can upgrade to Logger v4.5 GA only from Logger v4.0 SP1 Patch 1 (L4265). If you are using any other version, you need to first upgrade to Logger v4.0 SP1 Patch 1 before upgrading to v4.5.

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

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.

Upgrade Instructions

1 Download the `logger-4892.enc` file from the ArcSight Customer Support download site at https://software.arcsight.com.

2 Browse to the `logger-4892.enc` file you downloaded in the previous step and click **Upload Update**.

Wait until the user interface displays a message indicating that the upload was successful and advises you to reboot Logger.

3 On the System Admin tab, click **System Admin** > **Reboot** > **Start Reboot Now**.

4 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.

Logger v4.5 GA Documentation and Help

The *Logger v4.5 GA Administrator's Guide* and the online Help are integrated in the Logger product and is 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. To access the Administrator's Guide, click **Help** on any Logger user interface page, followed by the **PDF** icon to access the guide.

The *Logger Administrator's Guide* is also available for download from the ArcSight Customer Support web site at https://support.arcsight.com.

Connector Appliance Documentation

For a Logger platform with an integrated ArcSight Connector Appliance, documentation is available as follows:

- Chapter 8 and 9 in the *Logger v4.5 Administrator's Guide*.
- Through the Help icon ( ) on any user interface page, when you are in the Connector Appliance context. When you click this icon, a PDF of the *Connector Appliance Administrator's Guide* is displayed. **All information in this guide except system administration is applicable to your product.**
- Through the ArcSight Customer Support site at https://support.arcsight.com.

Issues Fixed in this Release

This release includes the fixes listed in the following table.

Number	Description
56303	STIG1: An outdated JAVA version was in use on Logger. **FIX:** The Logger software has been updated to install the latest JAVA version.
56277	STIG1: The Ctrl-Alt-Del sequence is not commented out in the `/etc/inittab` file. **FIX:** The sequence is now commented.
56281	STIG1: The bzip2 version used on Logger was bzip2 1.0.2-13.EL4.3, which is considered vulnerable. **FIX:** The Logger software has been updated to use the a bzip2 version that is not considered vulnerable.
56273	STIG1: Special privilege accounts such as halt and shutdown existed on Logger. **FIX:** These accounts have been removed.

Number	Description
63527	The `/opt/arcsight/aps/logs/catalina.out` log files were not being rotated. As a result, the files were consuming a large amount of space on the filesystem and impacting system performance. **FIX:** A maximum of ten log files of 10 MB each are retained.
63801	The Configuration Backup feature (Configuration > Configuration Backup) does not back up connector configuration information on the L3000 and L3200 model Loggers. **FIX:** Connector configuration information is now backed up.
64824	Even though a user belongs to a Logger Rights group with "Edit, save, remove shared filters" setting configured to "No", the "Save the current filter" icon () is available as an option on the Search Results screen. **FIX:** The "Save the current filter" icon () is no longer available for users who do not have edit, save, and remove rights to shared filters.
64833	A search is run on a peer Logger even if "Local Only" option is checked when search results are exported. **FIX:** Search is no longer run on a peer Logger when exporting search results if "Local Only" option is checked.
64981 / 66110	After upgrading to Logger v4.0 GA, Logger v4.0 SP1, or Logger v4.0 SP1 Patch1, the ESM Forwarder performance would degrade. As a result, the rate at which events were forwarded (EPS out) would decrease. **FIX:** The product has been updated to ensure that the forwarder performance is not impacted after an upgrade.
65020	A network share with the dash ("-") character in its name could not be mounted on Logger. **FIX:** The product has been updated to enable mounting shares that contain the dash character.
65532	When a number was specified for the day of week in the File Transfer receiver schedule, the number was converted to the abbreviated weekday name and listed as the abbreviated name under Scheduled Tasks. If you edit the scheduled task and save it, an error was generating indicating that the abbreviated name was not recognized. **FIX:** The scheduler has been updated to allow abbreviated names of weekdays, numbers, or a mix of both.
66242	If an event contained 127 or more tokens that started with the same character, an error was generated. In some cases, indexing on Logger could stop. **FIX:** The product software has been updated to allow more tokens that start with the same character.

Number	Description
66253	When you exported search results on a Logger using the dynamic time range option, the query you had run to obtain those results was rerun and the results of the rerun operation were exported. Therefore, the data exported would not exactly match the one displayed in the Search Results screen because the underlying data set could have changed (especially if there was a long delay between the time you run a search query and exported its search results, or your Logger was receiving a very high number of events per second). **FIX:** The export behavior has been changed to export the search results obtained when the query was run instead of rerunning the query at the time of export. Therefore, the search results you see on the screen are the ones that are exported and the export operation performance is improved.
66336	Information in the *Logger v4.0 Administrator's Guide* about SAN attachment statuses was incorrect. **FIX:** The SAN attachment status table has been updated in the *Logger v4.5 Administrator's Guide*.
66681 / 63713	Logger Internal events always indicated the disk space usage as 100% (eventclassId=disk:100), which was not meaningful. **FIX:** A new set of internal events that provide the percent used per storage group have been added. For these events: • deviceEventClassId is "storagegroup:100" • deviceEventCategory is "/Monitor/StorageGroup/Space/Used" • fileName field provides the name of the storage group • deviceCustomNumber1 provides the percent of the space used In the following example "storagegroup:100" event, the "fsize" field provides total GB space, the "cn1" field provides the percent of space used, and the "fname" field provides the storage group name. `CEF:0|ArcSight|Logger|4.5.0.4862.0|storagegroup:100|Logger Internal Event|1| cat=/Monitor/StorageGroup/Space/Used fileType=storageGroup cs2=CurrentValue cnt=1 dvc=192.168.36.232 fsize=10 type=0 cn2=7 cn1=70 rt=1278516044208 cn1Label=value cn2Label=retention period (days) fname=Default Storage Group cs2Label=timeframe`
66966 / 66967	If a SmartMessage receiver received an event that was larger than 1MB, the event was dropped. **FIX:** The receiver has been updated to truncate the event instead of dropping it. Additionally, when a device sends events that are greater than 1 MB in size, it is logged in the receiver log.
67249	An upgrade to Logger v4.0 SP1 Patch 1 would fail if the saved searches or any filters referenced resources such as devices, device groups, or peers that were no longer configured on Logger. **FIX:** The upgrade process has been enhanced to check for non-existent resources. If such resources are found an error message is displayed, which lists the filters and saved searches that reference those resources.
67284	Events are not stamped with the correct date when they are forwarded through a Syslog Forwarder to ESM. **FIX:** Events are now correctly stamped.

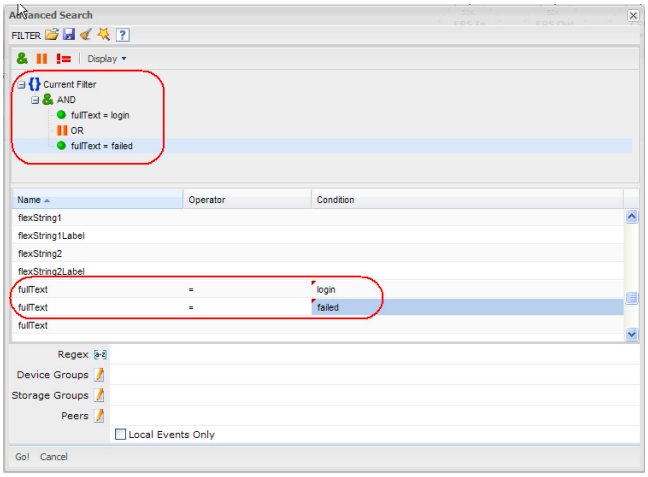
Number	Description
67779	After upgrading from v3.x to v4.0 SP1, reports run slower even though the all fields are indexed. **Understanding:** Before Logger v4.0 GA, the `endTime` field in an event was mapped to "rt". After v4.0 GA, it is mapped to "end" and "rt" is mapped to `deviceReceiptTime`. Therefore, the `endTime` field indexing begins only after you upgrade. When you include `endTime` in a query for a time range before the upgrade, this field is unindexed and thus impacts the performance of the query **FIX:** The v4.5 GA upgrade script ensures after upgrading the previously indexed “rt” information is assigned to “end”; therefore, the indexing information before the upgrade is preserved and thus used for queries to run faster.
67932	If password policy is configured on Logger (System Admin > Authentication > Password), users connecting from an ArcSight ESM Console to Logger cannot be authenticated. **FIX:** Users can now be authenticated even if a password policy is configured on Logger. However, the following characters cannot be used in a password when connecting from an ArcSight ESM Console to Logger: & # + % "
68227	When a search from ArcSight ESM was initiated on a Logger that was in peer relationship, a peer authorization error was generated even if Local only option was checked. **FIX:** An error is no longer generated and you can search from ESM to Logger as expected.
68269	When a user name with a hyphen (-) is created, the following error message is displayed: `"Login may only contain alphanumeric characters, spaces, dots, underscores, dashes or the @ symbol.”` The message indicates a hyphen (or dash) is allowed, however, creation of such as user name fails. **FIX:** User name with a hyphen can now be created.
68659	Installer for the software version of Logger would abort if sufficient space was not found in the /tmp directory to complete the installation. **FIX:** The installer has been enhanced to check for free space on the `/tmp` directory. If sufficient space is not found, the installer prompts you to point to another location where free space is available. To install version 4.5 of the software Logger, 780 MB of free space is required.
68660	Installer for the software version of Logger required that the group to which the arcsight user belongs is named arcsight. **FIX:** The installer has been updated to remove this requirement.

Known Behaviors in this Release

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
Alerts	51704	Currently, you can enable a maximum of five real-time alerts at any time on Logger. When you try to exceed this limit, the following message is displayed: `The maximum number (5) of active alerts has been reached. To activate this alert, please de-activate at least one other first.`
Database Migration	59324	On an L7100 Logger, the storage volume size and the storage group size decrease by 230 GB when database is migrated on it. **Understanding:** About 230 GB of space is allocated to the migrated database; therefore, the storage volume size and group size decrease.
Group Administration	44570	If a user belongs to a Logger Reports group with *Global access to all report objects and permission to change report engine configuration* 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. • Logger Reports Group with the *Global access to all report objects and permission to change report engine configuration* and *View, run, and schedule all reports* user rights set to Yes. • Logger Rights Group with the *View Scheduled Tasks* user right set to Yes.
Logs - Audit	49286	All Logger application audit events are logged to an internal database.
Monitor	48816	The EPS Out gauge reports a non-zero value even when no Forwarders are enabled. **Understanding:** This gauge reports traffic from real-time alerts as well as from Forwarders. Therefore, if you have Alerts configured on your Logger, EPS Out can be greater than zero.
	61405	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. **Understanding:** This issue arises only at DST adjustment time and lasts only for one hour.
Performance - System	41683	Downloading a large CSV file can make the browser unresponsive. **Workaround:** Wait until the CSV file has been downloaded, or use another browser to access Logger.

Function	Issue Number	Description
Platform	46104	Pressing the front panel reset button when Logger is running might result in data loss. On the L3000-series hardware, there is a known issue with the reset button: When the L3000-series system resets, the RAID controller might not see the hard disks. **Workaround:** If it is necessary to press the reset button, be prepared to power-down Logger (particularly the L3000) to restart smoothly. This problem only affects the reset button functionality and does not occur during a normal reboot.
	50364	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.
Receiver	39300	The default port for a File Transfer Receiver is 22. Selecting the FTP protocol (typically port 21) does not automatically change the port. **Workaround**: Manually change the port, if desired.
Reports	44952	Base Foundation and Solution report queries can be edited. **Workaround:** ArcSight recommends that you first make a copy of these reports and then edit them.
	57690	A user belonging to the Default Logger Report Group and the Default Logger Search Group cannot view the scheduled reports (Reports > Scheduled Reports). **Understanding:** The user also needs to belong to the Logger Rights Group to view the scheduled reports.
	61526	Report Execution Status (Reports > Default Dashboard) page does not list scheduled reports. **Workaround:** View the scheduled reports that have run on the Finished Tasks page (Configuration > Scheduled Tasks > Finished Tasks).
Search	41632	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.

Function	Issue Number	Description
Search	60354 / 60716	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. **Understanding:** To specify a keyword (full-text search), use the *fullText* field under the Name column, as shown in the following figure. To locate the *fullText* field, scroll down. 
Storage	52377	Storage groups that are smaller than the minimum of 5GB might lose data due to retention policy enforcement. **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 *Logger v4.0 SP1 Administrator's Guide*.

Open Issues in this Release

The following issues are open in the Logger v4.5 release and will be addressed in a future release. Use the workaround noted, where available.

Function	Issue Number	Description and Workaround
Archives	48048	If you navigate away from the Event Archives page (Configuration > Event Archives) while an archive is loading, the loading process stops. **Workaround:** Do not navigate away from the Event Archive page once an archive starts to load.

Function	Issue Number	Description and Workaround
Alerts/Filters	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.
Certificates	61134	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: **Configuration** > **Event Input/Output** > **Certificates** **Configuration** > **Alerts** > **Certificates** **Workaround:** Refresh the page to update the list. The deleted certificate is removed from the list.
	61631	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: `--- No Results Exist ---` **Workaround:** Because this issue is only experienced in the Firefox browser, use Internet Explorer to view these results.
	68448	When an SSL Client Authentication certificate is removed or added to the Certificate Revocation List (CRL), any open SSL sessions remain valid until the browser window is explicitly closed.
Configuration Backup and Restore	36373	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. **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.
	52540	Published reports are not included in a Report backup.
	57778	A configuration backup is not successful if the Remote Directory name contains a space. **Workaround:** Ensure that the Remote Directory name does not contain a space.
	63513	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: `"Database connection error when running a query"` **Understanding**: This error occurs because the restore process restores the backed up indices. These indices conflict with the indices initialized when Logger was rebuilt. **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.

Function	Issue Number	Description and Workaround
Connector	48329	On L3x00 models, it is possible to add a Logger receiver on the same port on which a connector is already configured. **Workaround:** Ensure that you are using unique ports for receivers and connectors configured on your Logger. Connectors use ports starting at 60000.
	52170	On the L3x00 platform, a duplicate connector is created under the localhost container after upgrading to v3.0. **Workaround:** Delete the duplicate connector created in the localhost container. **Note:** This bug does not affect the core system functionality.
Connector Appliance	61457	During a bulk upgrade of Containers, if a Container is unavailable (status 'Down'), it is skipped, and thus it is not upgraded. **Workaround:** Ensure that the Container status is 'Up' before starting the upgrade.
	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	51630	The type associated with imported filters cannot be changed from shared to saved search.
	51657 / 52201	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. **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.
	61779	When content (filters or alerts) is exported to a remote file system, two files are generated instead of one—an empty file and a file with extension .xml.gz. **Workaround:** Use the file with the extension as it contains the exported content and ignore the empty file. Or export the content to the local disk of the computer from which you connect to Logger.
Defragmentation	57638	A blank screen might display when you enter maintenance mode for database defragmentation. **Workaround:** Refresh the screen manually using your browser refresh function.

Function	Issue Number	Description and Workaround
ESM-Logger integration	60168	If the field value in a search query URL contains any special characters (such as |), the query fails to run on the ESM Manager. **Workaround:** Enclose the field values in the URL of the search query as follows: "{*value*}" For example, https://192.0.2.2/app/redirect?user=admin&pass=password&url=/logger/search.ftl&ausm_query=deviceEventClassId="{CVE|GENERIC-MAP-NOMATCH"&from=1%20Sep%202009%200:00:00%20PDT&to="8%20Sep%202009%2017:58:55%20PDT}"
FIPS 140-2	61941	The SCP and SFTP protocols (for setting up File Transfer Receivers) are not FIPS compliant. Documentation does not indicate this fact. **Workaround:** Configure File Transfer Receivers to use FTP.
	65327 / 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 reenable FIPS on the forwarder is unsuccessful. **Action:** Contact ArcSight Customer Support for further assistance.
Forwarder	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.
Maintenance Mode	57474	The System Maintenance option (Configuration > System Maintenance) might not be available if your system has been upgraded from v2.5 or earlier. Understanding: When a Logger is upgraded from an older release, the Enable Maintenance Mode permission might not be automatically set for the System Admin group. **Workaround:** Set the Enable Maintenance Mode permission to Yes for the System Admin group.

Function	Issue Number	Description and Workaround
Peer Loggers	59521	A peer user account whose password contains a "%" character cannot be used to establish a peer relationship between two Loggers, one of which is running Logger v4.0 GA or earlier. **Workaround:** Either change the peer user password such that it does not contain the "%" character or make sure both Loggers in a peer relationship are running Logger v4.0 SP1 Patch1.
	61369	If there is an improper tear-down of the peering relationship, Loggers in the relationship might not detect it. Consequently, when you try to reestablish the relationship, it might not succeed. Examples of improper tear-down: One of the Loggers is replaced with a new appliance, or the peering relationship is deleted on one Logger while the other is unavailable (power down). **Workaround:** If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from Loggers before reinitiating the relationship.
Peer Loggers	68987	If a search group filter specifies the peer Loggers on which a user can search and the user query contains a different peer Logger (which is not specified in the filter), the query runs on the peer Loggers specified in the filter. For example, *Search group filter:* peer("peer1", "peer2") *User query:* _peerLogger IN ["peer3"] *The acutal query that run:* _peerLogger IN ["peer1", "peer2"]
Reports	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.
	44793	In the Reports Designer, changing the parameter type TextBox to another type causes an error. **Workaround:** Do not edit an existing parameter whose type is set to TextBox. Instead, delete that parameter and add a new one.
	45091	Users who are granted only edit and save report styles privileges do not see the Template Styles link on the Reports tab. **Workaround:** Grant users that need to access Template Styles admin privileges.
	45163 / 48618	The time range and constraints information is not applied when accessing information from reports through the drilldown links of a scheduled published report.

Function	Issue Number	Description and Workaround
Reports	45253	The default date/time in reports does not include the time of day. **Workaround:** Choose a date format that includes HH:MM:SS, if needed.
	45447	Some predefined report templates do not support i18n characters. **Workaround:** Test the report template for the desired character set before production use. This issue will be fixed in a later release.
	45548	Adding a scheduled report can reset the scan limit field of other reports. **Workaround:** Check that the scan limit is set as desired before running any report.
	45568	The Dashboard does not have a scroll bar. Workaround: Set the "Show Scrollbar" property to "Yes" in the Widget Properties section of the External Links and Use Cases Dashboard Items.
	45570	After upgrading to Logger v4.5 GA, custom Report Configuration settings (Reports > Reports Administration) are reset to the default values. **Workaround:** Re-enter the custom values after the upgrade is complete.
	46286 / 50564 / 52340 / 53070 / 52760	Report-formatting issues might occur in very large reports (containing over 100,000 lines) configured to render in the Single Page HTML format. **Workaround:** Use the Multi-Page HTML format to resolve such report formatting issues.
	48613	The default report generated by clicking the hand icon is missing the report name and date. **Workaround:** Add the Report title to the Report Header section to render the title on the first page of the Report.
	50175	The Reports function tab disappears when a user authorized to only view published reports clicks the System Admin tab. **Workaround:** To make the Reports function tab reappear, go to the top-level Logger URL (https://<*IP address* or *hostname of Logger machine*>).
	52330	The time taken to run a scheduled report is not reported correctly in the Logger user interface.
	52382	When a report query includes aliases in the SELECT clause and you use those aliases in the Filter Criteria of a report, the report might fail to generate. **Workaround:** Remove the alias from the query. If you need to use aliases, include them in the Caption field of the report query editor.

Function	Issue Number	Description and Workaround
Reports	61410	The reports in Logger Content Information Packs (CIP) for PCI and SOX do not display the hour value in the Event Hour column; only the date is displayed. **Workaround:** If a report does not display the hour value in the Event Hour column, change the Data Type for the Event Hour field to CHAR in the report's query definition.
	61563	A report template with the alignment setting of "Center", creates a report with left-aligned data.
	61564	A report generated as a single page, PDF is blank when the report contains more than 800 records. **Workaround:** When generating a report in PDF format, set the Pagination setting to "Multiple Page".
	61619	When a large report that is running in the background is cancelled before it has finished running, the Report Execution Status page indicates that the report run was a failure. **Workaround:** Ignore the "Failure" status.
	61877	When you specify a filter at the time of running a report and run that report in the background, the filter is not applied correctly. **Workaround:** Include the filter in the report definition instead of applying it at run time.
	63398	If all user rights except the ones that start with "Report folder [folder name]" in a Logger Report group are set to "No," the Reports tab is missing when the System Admin tab is selected. **Workaround:** Click any other tab (such as Monitor or Configuration) and the Reports tab will display.
	64425	A user with "Edit and Save Reports" right set to No is able to edit and save reports.
	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"`
	68925	Enabling or disabling dashboard refreshing ("Enable Dashboard Refreshing", "Disable Dashboard Refreshing") disables the Design and Preference links for the Dashboard.
	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.

Function	Issue Number	Description and Workaround
Reports	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.
Saved Search	51897	The "Click here to configure now" link for configuring a remote export location for Saved Search jobs (Configuration > Saved Search > Saved Search Jobs) does not work. **Workaround:** Use any of the following ways to configure an export location: • System Admin > NFS > Add NFS Mount • System Admin > CIFS > Add CIFS Mount
	69331	Alert Viewer (Analyze > Alerts) displays two alerts for each triggered Saved Search alert. This issue does not exist for Real-time alerts.
Scheduled Jobs	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.
	68633	In the Internet Explorer browsers, versions 7 and 8, the Finished Tasks page (Configuration > Scheduled Tasks > Finished Tasks) displays the following warning: "Stop running the script? A script on this page is causing Internet Explorer to run slowely. If it continues to run, your computer might become unresponsive." **Workaround:** Ignore the warning and click Yes to proceed further.

Function	Issue Number	Description and Workaround

Search	59612	The full-text (keyword) search cannot find events that contain an IP or a MAC address that is prefixed with an equal to (=) character in the actual event. For example, these full-text queries will not locate the following event.
		`Query 1: "ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00"`
		`Query 2: "192.168.10.153"`
		`Query 3: "192.168.10.255"`
		`<166>Sep 9 14:48:22 beach kernel: Killed bad incoming packet: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00 SRC=192.168.10.153 DST=192.168.10.255 LEN=229`
		Workaround: This problem only occurs for a very small number of devices, which use this particular format. The workaround is to search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255.
		Alternatively, you could run these data through a SmartConnector to convert to CEF format. Then run either a full text or field based search.

	61139	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. **Understanding:** Color Block View expects two conditions. Therefore, do not use this view if your query contains only one condition. **Workaround:** To get rid of the warning message so that you can use the Tree View: 1 Switch to Tree View. 2 Include a second "placeholder" condition. 3 Click GO. Once the query is displayed in the Search box (on the main Search page), remove the second, "placeholder" condition.
	60121	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.

Function	Issue Number	Description and Workaround
Search	61305 / 61338	**61305:** 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: `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]"` `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]"` **61338:** Similarly, if some peer Loggers are running v3.x, multiple error messages are displayed in the Search Analyzer window, when a storage group is not found on the v3.x Loggers.
	61567	A search query that includes an escaped double quotes in a regular expression (for example, REGEX="\"logger\"") fails when run on a peer Logger. The query does run as expected on the local Logger.
	62955	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). **Workaround:** Enter the storage group, device group, or peer information in the Search text box on the main Search page.
	63055	Search results are not highlighted for values that match the IN operator in a query.
	64786	The export operation does not work when specific fields that include *user and * are exported. **Note:** The export operation does work if all fields (with the "All Fields" box checked) are exported, including * and *user. **Workaround:** Either export all fields (with the "All Fields" box checked) or export specific fields excluding *user and *. That is, to export specific fields, remove *user and * from the list.
	68941	When search results containing non-English characters are exported in the PDF format, the event fields that contains those characters are blank in the exported file.
	69023	When search results are exported, the time elapsed to export the events is not displayed.
	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.

Function	Issue Number	Description and Workaround
Search	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.
	69158	In the Search results display, raw event fields are not separated by tab characters even when the original event contains those characters. *Original raw event:* Information 7/6/2009 10:24:31 AM crypt32 None 2 N/A XDEV *Search results display:* Information7/6/200910:24:31 AMcrypt32None2N/AXDEV
	68820	If a single event matches a query that contains the `where` 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.
	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.
Search Operators	69095	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. **Understanding:** This is a known issue and will be addressed in a future release of Logger. **Suggestive Action:** You can Cancel the search when this situation occurs and rerun the query with these changes: • Reduce the time range of the query • Refine the query to increase the selectivity of the query

	69160	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.
		`| cef a b c | top a c | chart _count by b`
		Workaround: Include all fields you would like to use later in the pipeline in the top command. For example, change the above example to:
		`| cef a b c | top a b c | chart _count by b`

Function	Issue Number	Description and Workaround
Storage	50338	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. **Workaround:** Refresh the browser or check the page again later.
	55676	The Logger user interface does not prevent two Loggers from mounting the same NFS mount point. **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.
	56602	When archiving or exporting events from Logger, the user interface provides the option to store these events on Logger's primary storage (SAN or NFS). Although it is possible to store these events on the primary storage location, it is not a recommended practice. **Recommendation:** Do not select Logger's primary storage location for archiving or exporting events from Logger even if the user interface provides an option to do so.
	60152	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. **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.
	66514	On the software Logger, if the storage volume has 20% free space remaining, the following message is displayed: `The storage volume does not have adequate free space to store incoming events. Increase the free space immediately to prevent Logger from disabling event storage. At least 20% free space is recommended.` If 10% free space remains, Logger stops receiving events. **Workaround:** Free up space on your system to make more storage space available.
	65649	When software version of Logger is running out of storage space, the user interface screens accessible through the "Reports" and "System Admin" top-level menu do not display any warning. All other user interface screens do display the warning.
Support Login	63224	The Support Login page (System Admin > Support Login) does not load occasionally. **Workaround:** Click **System Admin** > **Process Status** > '**aps**' (under the Processes list) > **Restart**.

Function	Issue Number	Description and Workaround
System Admin - SMTP	61378	Changes made to existing SMTP information (System Admin > Network > SMTP) are not automatically detected and effective. 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. **Workaround:** Restart the forwarder process for the new information to take effect. To restart the process: 1 Click **System Admin** > **Process Status**. 2 Click **processors** from the Process list. 3 Click **Restart** in the bottom right corner of the screen.
System Admin - SSL Client Auth	61980	The two tabs (Trusted Certificates and Certificate Revocation List) available for System Admin > SSL Client Authentication contain "x" buttons, which when clicked close the tabs. **Understanding and workaround**: The "x" buttons are extraneous and should not be used. If you inadvertently close the tabs by clicking an "x" button, refresh your browser to open the tab again.
Uninstall Software Logger	68882	When the software version of Logger is uninstalled, the uninstall program removes all contents of the `/opt/arcsight` directory. If you have other ArcSight products such as Connectors installed in this directory, they will be removed as well. Workaround: Ensure that you do not have other ArcSight products such as Connectors installed in the `/opt/arcsight` directory before uninstalling the software version of Logger.
User Interface	42662	The Save to Logger operation overwrites an existing file of the same name. **Workaround:** Use unique file names when using the Save to Logger operation.
	49017	If you click on another tab or page before a UI page is fully loaded, the UI attempts to load the latter page, but eventually displays the former page. **Workaround:** Wait for the current page to fully load before clicking another one.
	52452	In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report. **Workaround:** Use the IE browser instead.
	60810	In the Firefox v2.x browsers, search Builder window (accessed from the Advanced Search link on the Search page) may not display correctly. For example, parts of the window may not display or might be missing. **Workaround:** Upgrade your browser to Firefox v3.x.

Function	Issue Number	Description and Workaround
User Interface	61869	When Firefox v2.x browser is used on a Linux system or Internet Explorer v8.0 is used on a Windows system, several UI pages (such as Support Login, FIPS 140-2, SSL Client Authentication) do not display. **Workaround:** Upgrade your Firefox browser to v3.x on Linux systems. Use IE v7.x on Windows systems.
	64311 / 68581	In the Internet Explorer 8.x browser, clicking the Configuration tab displays a blank screen. **Workaround:** When a blank screen displays, click the Configuration tab again from the top-level menu bar.
User Privileges	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.