

Release Notes **ArcSight Logger™**

Version 4.0 SP1 Patch 1 (Build L4265)

May 21, 2010



Release Notes ArcSight Logger™, Version 4.0 SP1 Patch 1 (Build L4265)

Copyright © 2008-2010 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
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.
03/26/09	Logger v3.0 Patch 1	Added cautions about not changing the license file name.
01/22/09	Logger v3.0 Patch 1	Added information about fixed issue #54715, open issue #54854, and #54822.
01/14/09	Logger v3.0 Patch 1	Patch 1 release.

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™ v4.0 SP1 Patch 1	1
What's New in Various Logger v4.0 Versions	2
Logger v4.0 SP1 Patch 1	2
Logger v4.0 SP1	2
Logger v4.0 GA	4
Upgrading to Logger v4.0 SP1 Patch 1 (L4265)	13
Understanding the Upgrade Process	13
Upgrade Files	15
Prerequisites and Caveats	15
Upgrading the Logger	16
From v3.0 SP1 or v3.0 SP1 Patch 1 to v4.0 SP1 Patch 1	16
From v4.0 GA or v4.0 SP1 to Logger v4.0 SP1 Patch 1	17
Post upgrade tasks:	17
Logger v4.0 SP1 Patch 1 Documentation and Help	18
Connector Appliance Documentation	18
Issues Fixed in this Release	18
Known Behaviors in this Release	21
Open Issues in this Release	24

ArcSight Logger™ v4.0 SP1 Patch 1

These release notes provide information about the ArcSight Logger v4.0 SP1 Patch 1 (L4265) release. Read this document in its entirety before installing this release.

If your Logger platform is a Logger-Connector Appliance integrated solution, make sure you also read the release notes available for the specific release of Connector Appliance installed on your appliance. The Connector Appliance release notes are available from the ArcSight Customer Support site at <https://support.arcsight.com>. The upgrade section in the Connector Appliance release notes does not apply to the Logger-Connector Appliance integrated solution.

This document covers the following topics.

- [“What’s New in Various Logger v4.0 Versions” on page 2](#)
- [“Upgrading to Logger v4.0 SP1 Patch 1 \(L4265\)” on page 13](#)
- [“Logger v4.0 SP1 Patch 1 Documentation and Help” on page 18](#)
- [“Issues Fixed in this Release” on page 18](#)
- [“Known Behaviors in this Release” on page 21](#)
- [“Open Issues in this Release” on page 24](#)

What's New in Various Logger v4.0 Versions

Logger v4.0 SP1 Patch 1

This version of Logger introduces a number of bug fixes, including bugs that were preventing a successful upgrade to v4.0 SP1. The *Logger v4.0 SP1 Administrator's Guide* is applicable to the Logger v4.0 SP1 Patch1 release.

For a complete list of bugs fixed in this release, see ["Issues Fixed in this Release" on page 18](#) and list of open bugs, see ["Open Issues in this Release" on page 24](#).



If your Logger is currently running v4.0 SP1 and it was upgraded from v4.0 GA with FIPS-mode enabled, make sure you read the details of issues [65327 / 65357](#) in ["Open Issues in this Release" on page 24](#).

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

Note: This information overrides the one in the *Logger v4.0 SP1 Administrator's Guide*.

Other Information You Need to Know

The following change was made to the product that might impact your current configuration.

TCP Port 80 Redirect

Starting with Logger v4.0 GA, HTTP requests to TCP port 80 are automatically redirected to SSL port 443. This enables you to access the login page of your appliance by simply entering the appliance hostname or IP address, without specifying the https:// prefix in the URL field of your browser.

If any receiver on your Logger appliance is configured to use TCP port 80, make sure you reconfigure it to use another port before upgrading to this release. Otherwise, that receiver will stop receiving events after the upgrade.

Logger v4.0 SP1

This section lists the features, enhancements, and changes that were introduced in Logger v4.0 SP1 and **are applicable to Logger v4.0 SP1 Patch1 as well**.

Audit Event Update

In addition to the introduction of new platform events, the message string and device event categories associated with existing audit events have been updated in Logger v4.0, as shown in the following example. For a complete list of events, see Appendix D, Logger Audit Events in the *Logger v4.0 SP1 Administrator's Guide*.

3.0 Audit events:

Device Event Class ID	Message	Device Event Category
logger:510	Device has been /Add	Logger/Resource/Device/Configuration
logger:511	Device has been /Delete	Logger/Resource/Device/Configuration

4.0 Audit events:

Device Event Class ID	Message	Device Event Category
logger:510	Device [deviceName] has been added	Logger/Resource/Device/Configuration/Add
logger:511	Device [deviceName] has been deleted	Logger/Resource/Device/Configuration/Delete

When a v3.0.x Logger is upgraded to v4.0 SP1, existing filters that use these message strings or device event categories are not automatically converted to use the new name or category because these filters are still valid for the audit events that were generated on your Logger before the upgrade. However, these filters will not work for the audit events that are generated on the Logger after the upgrade. To circumvent this situation, follow these guidelines:

- Use the existing filters for events generated before the upgrade
- Define new filters that are similar to the existing filters except that they use the new message strings and device event categories. Use the new filters for events generated after the upgrade. A list of events is available in the appendix "Logger Audit Events" in the *Logger Administrator's Guide* for this release.
- When you use a filter to search for events, either ensure that you select a time range in which that filter is valid or modify the search query to include two filters—one that searches for pre-upgrade events and the other that searches for post-upgrade events.

For example, you upgrade your Logger at 10 a.m. At 11:30 a.m., you use a saved filter S1 (see definition below) to search for events in the "Last 2 hours" (from 9:30 to 11:30 in this case). This query will not return a complete search result because the audit events generated after 10 a.m. are named "Device added"; therefore, they will not be included in the results.

In the above case, make sure that your search query includes two filters combined with an OR operand, as follows:

S1 OR S2

where S1: `name="Device has been /Add"`

S2: `name="Device added"`

Supported Browsers

Starting with 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

Note: This information overrides the one in the *Logger v4.0 SP1 Administrator's Guide*.

Other Significant Changes in This Release

If you are upgrading from v4.0 GA, make sure you understand the following changes in this release. If you are upgrading from any other release, you can skip this section.

- Starting with this release, if a search query includes the boolean operator OR and the metadata identifiers (discussed in the "Constraints" topic in the *Logger Administrator's Guide* for this release), the expression to be evaluated with OR must be enclosed in parentheses, as shown in this example:

```
(success OR fail) _storageGroup IN ["Default Storage Group"]
```

If the expression is not enclosed in parentheses, an error message is displayed on the user interface screen. This change has been made to ensure that the metadata identifiers (_storageGroup, _deviceGroup, _peerLogger) are correctly applied to the entire OR expression.

When you upgrade to this release, existing saved searches and filters are not automatically converted to comply with this requirement. You need to manually update that content. The default System Filters (available as standard content) on Logger are automatically converted.

Additionally, if this Logger peers with a Logger that runs v4.0 GA, make sure that the queries sent from that Logger to this Logger also follow this guideline.

- The index data generated as a result of enabling full-text indexing, available starting with Logger v4.0 GA, is stored on your Logger (similar to field-based indexing). Due to the search flexibility that full-text searching enables, the index data can be large and thus consume more storage space than you expect. Additionally, when this data is archived to a Logger archive destination, it consumes storage space on the archive destination. Although the space consumed depends on your data, ArcSight's internal tests indicate that about 50% additional space is needed. For example, if 30 GB space is used without full-text indexing, 45 GB will be required with full-text indexing.

Logger v4.0 GA

This section lists the new features/enhancements introduced in the Logger v4.0 release and **are applicable to Logger v4.0 SP1 Patch1 as well**. See the *Logger v4.0 GA Administrator's Guide* (or *Logger v4.0 SP1 Administrator's Guide*) for details of these features. These guides are available at the ArcSight Customer Support site at <https://support.arcsight.com>.

Next Generation Hardware Platform

Logger v4.0 GA runs on the new Logger hardware platforms available from ArcSight. The new platforms (L3200, L3200-PCI, L7200s, L7200x, and L7200-SAN) are the next-generation Logger hardware systems for the existing platforms available from ArcSight.

Enhanced Search function

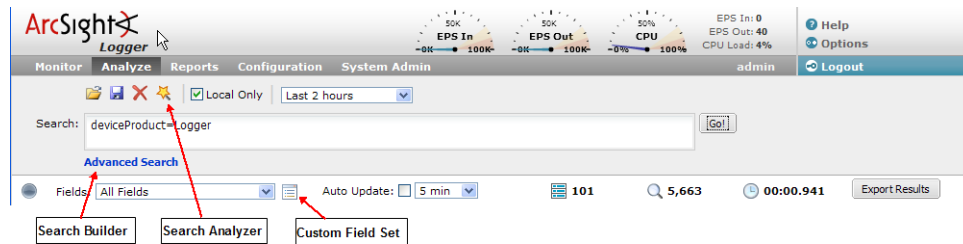
Logger v4.0 introduces significant usability and functionality improvements for searching events. The Search user interface for field-based and regular expression queries has been unified to simplify user interaction. The queries for these search methods can be part of a

single query expression, in which the field-based query searches for matching events and the regular expression query helps further refine search results.

Additionally, **a third search method called full-text search (also known as "keyword search") has been introduced.** When using this search method, you enter queries in plain English, as you would when using any of the popular Internet search engines.

The full-text search queries can be specified standalone or in conjunction with the field-based and regular expression queries. For example, a simple full-text search query searches for the word "failed" in the events stored on Logger, while a more complex version, which combines the three search methods, can be as follows:

```
failed AND name="*[4924TestAlert]*" AND ("192.168.*" OR
categoryBehavior CONTAINS Stop) | REGEX=":\d31"
```

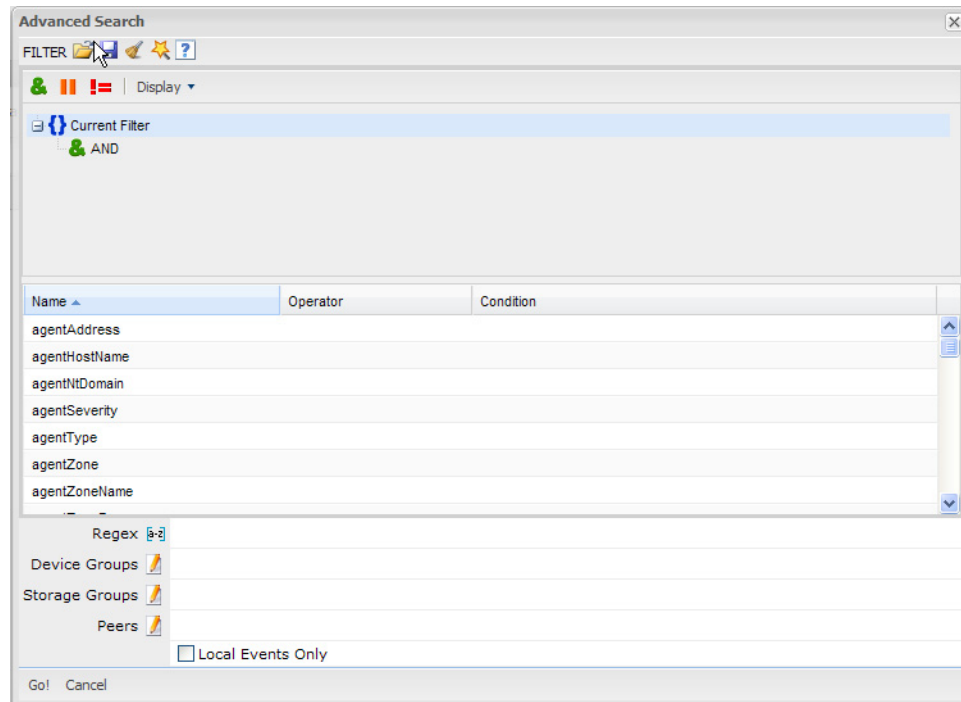


Other significant improvements related to search are:

- Search Builder tool (Advanced Search tool)

This tool is a boolean-logic conditions editor that enables you to quickly and accurately build keyword, field-based, and regular expression search queries, as shown in the following figure. The tool provides a visual representation of the conditions you are including in a query. For more information, see "Using the Search Builder Tool" in the *Logger v4.0 Administrator's Guide*.

To access this tool, click **Advanced Search**, right below the Search text box.



- Search Analyzer tool

The Search Analyzer tool analyzes a query to determine if any of the fields included in the query are non-indexed for the time range specified and thus impact the query's performance.

- Auto-suggest facility

Although you can use the Search Builder tool to build your queries, if you choose to type them in the Search text box, Logger's auto-suggest facility enables you to quickly build query expression by automatically providing suggestions, possible matches, and applicable operators for the following:

- ◆ Fields in Logger schema

(See "Indexing" in the *Logger v4.0 Administrator's Guide* for a complete list of fields.)

- ◆ Metadata terms (`_storageGroup`, `_deviceGroup`, `_peerLogger`)

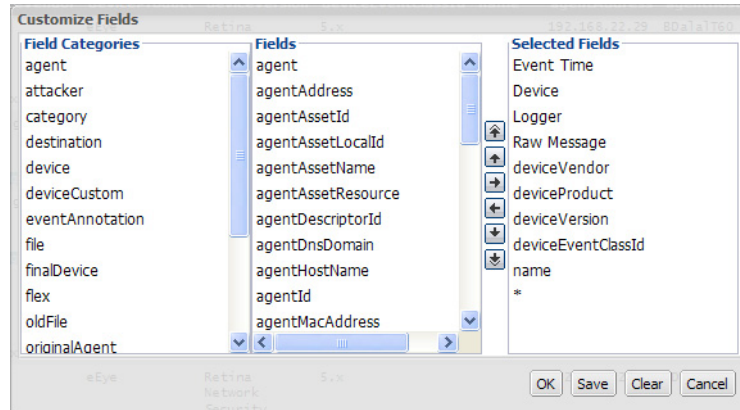
Type "_s" (for storage group), "_d" (for device group), or "_p" (for peerLogger) in the Search text box to obtain a drop-down list of constraint terms and operators.

- ◆ Regular expression term (`| REGEX=`)

- Custom field sets

A field set determines the fields that are displayed in the search results for each event that matches a search query. Starting with Logger v4.0, you can create your own field sets. By doing so, you can hide the event fields you do not need in the search results, and use the available screen space on your computer more efficiently to only view event fields you need.

The Logger user interface offers a simple and intuitive interface to select and move event fields you want to include in a field set, as shown in the following figure.



■ Nested conditions

Starting with this release, you can include different boolean operators in a query. That is, you can include AND and OR in a single search query, or you can include AND, OR, and NOT in a single search query, and so on.

Consequently, you can create nested conditions by mixing any of the applicable operators.

For example, you can nest full-text search keywords using boolean operators. Similarly, you can nest field-based search queries using string, boolean, numeric, and so on operators. For example, `(name="John Doe" OR name="Jane Doe") AND message!="success"`.

When nesting conditions, metadata identifiers (`_storageGroup`, `_deviceGroup`, and `_peerLogger`) can only appear at the top level in a query expression.

■ Drill-down search results

You can drill-down the search results to further refine them. Click a green-highlighted term in the search results to add it to the current query. For example, if you search for "login" and roll over the word "fail" in the search results, "fail" will highlight in green. Click the word "fail" to change the query to "login AND fail." You can select only the indexed fields from the search results.

Expanded LUN Storage Capacity

Logger platforms that support SAN now have the ability to support up to 5 TB volumes. To make use of this enhanced capacity, make sure you allocate a 5.4 TB LUN when initializing your Logger. The additional 0.4 TB need to be allocated to accommodate Logger system files.

If you are upgrading to v4.0 SP1 and already have a LUN configured for primary storage on your v3.0.x appliance, you cannot change its size to make use of the expanded capacity. This enhancement only applies to new appliances and existing appliances that are installed from scratch.



- Even if your LUN is larger than 5.4 TB in size, you can only allocate a maximum of 5.4 TB and pre-allocate a maximum of 5TB.
- The size of a LUN cannot be changed after it has been set during Logger initialization.

Storage Groups—Additional and Resizing

Logger can have a maximum of 6 storage groups now—two that pre-exist on your Logger (Internal Storage Group and Default Storage Group) and **four that you can create**. As a result, now you have **five** storage groups available for event storage and one for Logger's internal events. (In Logger v3.x, you could only create two more storage groups in addition to the pre-existing ones, thus resulting in three for event storage.)

The storage groups need to be created during the Logger initialization phase and cannot be created or deleted once Logger has been initialized, as described in "Initialization Sequence" in the *Logger v4.0 Administrator's Guide*. **However, a Storage Group's size can be increased and decreased any time (if there is sufficient disk space available on the Logger to perform the operation); therefore, create additional groups of minimal size even if you don't need them at this point.**

For more information, see "Storage Groups" in the *Logger v4.0 Administrator's Guide*.

NFS and CIFS

Starting with this release, Logger can also mount a CIFS remote file system (Windows share) **for secondary storage**—for archiving data such as events, exported filters and alerts, and saved searches.

Starting with Logger v4.0, use of NFS as the primary storage device for storing Logger events is **not** recommended. However, you can continue to use NFS mounts to archive data such as events, exported filters and alerts, and saved searches.

For more information, see "Storage" in the *Logger v4.0 Administrator's Guide*.

Configuration Audit Events

Logger now generates configuration audit events that provide greater visibility and change control for monitoring the activity of users and administrators who have access to Logger. For example, storage volume has been added, certificate added, and search indices added.

For more information, see Appendix D, Logger Audit Events, in the *Logger v4.0 Administrator's Guide*.

Expanded Logger Schema

Fifteen additional fields such as `customerName` and `requestUrl` have been added to the Logger schema for enhanced searchability and reporting.

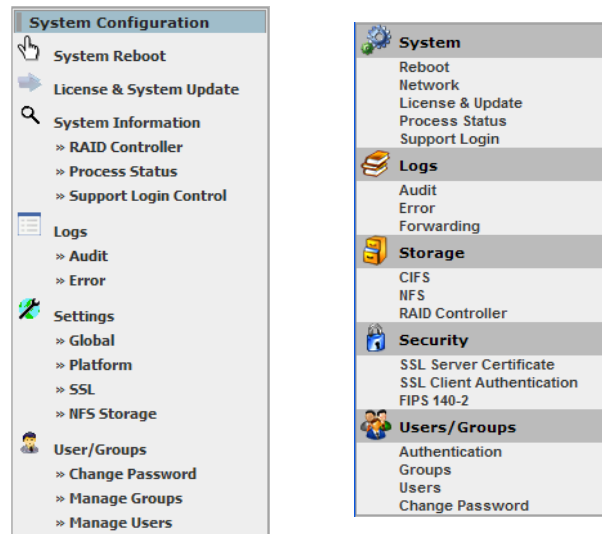
The `requestUrl` field cannot be indexed.

For a complete list of fields, see "Indexing" in the *Logger v4.0 Administrator's Guide*.

System Admin Menu Changes

The System Admin menu has been reorganized to improve usability. The following figure illustrates the before (left figure) and after (right figure) layout. The system administration

procedures in Chapter 7, System Admin, in the *Logger v4.0 Administrator's Guide* have been updated to reflect these changes.



Reporting Enhancements

The reporting section introduces the following enhancements:

- **User-definable templates:** In addition to using pre-defined templates, now you can create your own templates.
- **Search:** Queries, Parameters, Parameter Value Groups, and templates include a search function to search for an existing element. For example, you can search for a query by specifying the letter its name starts with or by specifying a letter or a word that it contains in its name.
- **Point Labels:** When creating charts, you can include point labels that indicate the number of matches for each plotted element on the X-axis.
- **Default Dashboard:** If a dashboard is not defined, a Report Execution Status page indicates the status of recently run or accessed reports.
- **Device Monitoring Reports:** A new report group that address common device monitoring user cases for systems and devices on your network.
- **Standard and Custom Reports:** These reports are not listed on separate tabs. Instead, they are combined on a single screen.
- **Run in Background:** Reports that take longer to run or are not required immediately can be run in the background. This option enables you to perform other activities on Logger while a report is being generated.
- **Report Title:** Each report can be given a meaningful title. This title appears at the top of the report when it is generated.
- **Adhoc Report Designer:** Once you edit a report, you can run a report before saving it to ensure that the report output is as you expected.
- **SQL Editor:** The Design tab in the SQL Editor has been enhanced to improve usability.

For more information, see Chapter 5, Reporting, in the *Logger v4.0 Administrator's Guide*.

Logger-ESM Integration

Starting with this release, Logger search is available as an integrated command in the ArcSight ESM Console. You can perform a Logger search operation directly from your ESM Console if you have ArcSight Logger and ArcSight ESM v4.5 SP2 deployed in your network infrastructure.

There are two ways to perform a search operation on Logger from an ESM Console:

- Search—a regular search operation in which you can specify search options
- Quick search—a search operation based on field and value you select in an ESM Console active channel; you are not prompted for any search options.

To run a Logger search, you right click on an event in an active channel of the ESM Console to display a menu. You select the search method—Logger Search or Logger Quick Search—from the menu.

You can use this feature when FIPS is enabled on your Logger. However, you cannot use this feature when SSL client authentication (CAC authentication) is enabled on the Logger.

For more information, see Appendix G, Logger Search From An ESM Console, in the *Logger v4.0 Administrator's Guide*.

Security Enhancements

The following security enhancements have been made in this release:

FIPS Support

Logger supports the Federal Information Processing Standard 140-2 (FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components.

If your Logger needs to be FIPS 140-2 compliant, you can enable FIPS on it. Once you do so, the Logger uses the cryptographic algorithms defined by the NIST for FIPS 140-2 for all encrypted communication between its internal and external components.

FIPS mode is supported on SmartConnectors running version 4.7.5.5372 or later. Follow instructions in "Installing or Updating a SmartConnector to be FIPS-compliant" in the *Logger v4.0 Administrator's Guide* to ensure that your connector is FIPS compliant.

Once FIPS is enabled on your Logger, the SmartMessage receiver (if configured) stops receiving events from non-FIPS connectors if those connectors are not running version 4.7.5.5372 and later.

Additionally, the SCP and SFTP protocols (for setting up File Transfer Receivers) are not FIPS compliant. Therefore, configure your File Transfer Receivers to use FTP.

CAC Support

Logger supports client authentication using SSL certificates. SSL client authentication is a form of two-factor authentication that can be used *as an alternate* or *in addition to* local (user name and password) and RADIUS authentication. As a result, Logger can be configured for SmartCards, such as Common Access Card (CAC) based authentication.



All SSL client certificates used for authentication and the SSL server certificate on the Logger must be FIPS compliant (that is, hashed with FIPS compliant algorithms) even if FIPS is not enabled on your Logger. If any of the certificates is MD5 hashed, CAC authentication to Logger will not succeed.

Support Login

Starting with this release, when ArcSight Customer Support needs access to your appliance for troubleshooting and diagnostics, they work with you to assign a single-use password to the appliance. Doing so enables Support Login access to the appliance. This password is valid only for one support session and is automatically disabled after the session ends.

For more information, see "Support Login" in the *Logger v4.0 GA Administrator's Guide*.

ESM Manager as an Alert Destination

Alerts can be forwarded to an ESM Manager, in addition to the previously supported SNMP, Syslog, and E-mail destinations. For more information, see "ESM Destinations" in the *Logger v4.0 GA Administrator's Guide*.

Performance Enhancements

This release includes many system- and application-level enhancements to improve performance and reliability of various Logger operations. For example:

- As a result of file system optimization in this release, pre-allocation now takes significantly lesser time than before.
- The enhanced Logger forwarding software enables you to pause and resume forwarding at any point in time. Additionally, if a forwarder fails during a forwarding operation and is restarted, event forwarding resumes from the point at which the failure had occurred. For more information, see "Forwarders" in the *Logger v4.0 GA Administrator's Guide*.
- Due to Search optimizations implemented in this release, search queries that contain multiple search components—full-text (keyword), field-based, regular expression—run faster than before.


Documentation—System Health Events

The system health events that Logger generates are stored in the Internal Storage Group, which is created by default. Until now, these events were not documented. Starting with this release, a list of these events is available. See "System Health Events" in the *Logger v4.0 GA Administrator's Guide* for more information.

Documentation Access

This information only applies to you if your Logger platform is a Logger-Connector Appliance integrated solution.

Connector Appliance documentation is now available as follows:

- 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>.

If your Logger platform is a Logger-Connector Appliance integrated solution, make sure you also read the release notes available for the specific release of Connector Appliance installed on your appliance. The Connector Appliance release notes are available from the ArcSight Customer Support site at <https://support.arcsight.com>. The upgrade section in the Connector Appliance release notes does not apply to the Logger-Connector Appliance integrated solution.

Other Information You Need to Know

- **Hardware Installation:** The sliding rails shipped with the L3200 appliances do not work properly with the 2-post equipment racks. ArcSight recommends that you use a 4-post rack instead.
- **Initialization/Indexing:** When you enable indexing on your Logger and accept the default recommended fields for indexing, the "Enable Full Text Indexing" checkbox is automatically selected. If you want to enable only field-based indexing and not full-

text indexing, you need to uncheck the Full Text indexing checkbox before proceeding further. Once indexing has been enabled, it cannot be disabled.

Add Search Indexes

Important

Once a field is indexed, it cannot be removed. Significantly exceeding ArcSight's default recommended indexed fields could result in performance issues. If you need to exceed the default number of fields, only index those additional fields which are necessary for your use.

Enable full text indexing ☐

To add indexed fields, select one or more fields below

Indexable fields

- deviceVendor
- deviceProduct
- deviceVersion
- deviceEventClassId
- name
- agentSeverity
- agentAddress
- agentHostName
- agentNtDomain
- agentType
- agentZoneURI
- applicationProtocol
- baseEventCount
- bytesIn
- bytesOut
- categoryBehavior
- categoryDeviceGroup
- categoryObject
- categoryOutcome
- categorySignificance
- categoryTechnique
- customerName
- destinationAddress
- destinationDnsDomain

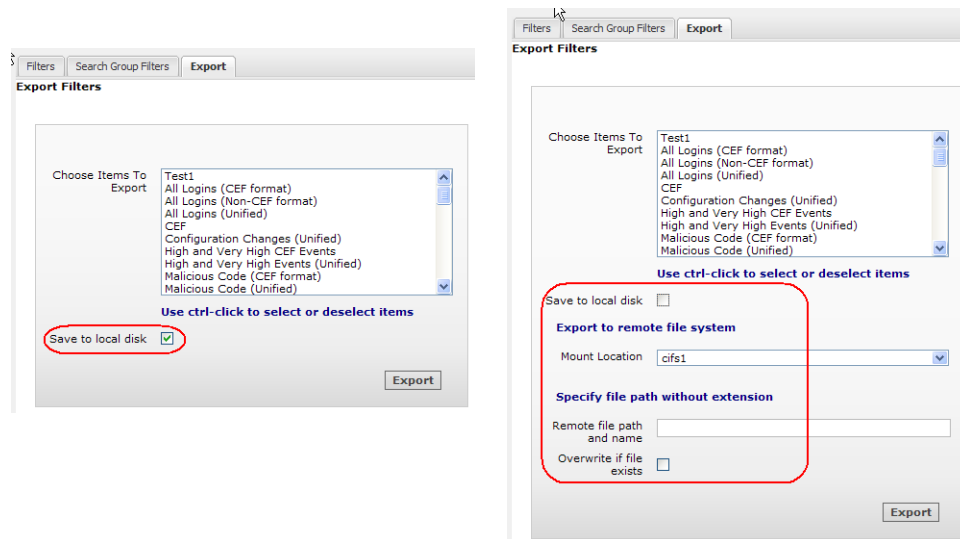
Use ctrl-click to select or deselect items

Select Recommended Fields

Apply Changes

- **Reports:** For Logger Reports, the data type for the IP Address field is CHAR by default. This data type enables you to input the IP address in dotted-decimal notation. Do not change this data type to another value; otherwise, you will not be able to enter an IP address in the format you expect.
- **Search:** The Local Only check box on the Search UI pages only displays when a peer Logger is configured on the Logger.
- **Content Export:** In addition to exporting to a remote location, you can now export filters and alerts to the local disk of the computer from which you connect to the

Logger. This option is enabled by default. If you still want to export to a remote location, you need to uncheck this option to display the remote location options.



Upgrading to Logger v4.0 SP1 Patch 1 (L4265)

You can upgrade to Logger v4.0 SP1 Patch 1 from the following versions.



To determine your current Logger version, hover the mouse over the ArcSight logo in the upper left of the screen, or click the **System Admin** tab, then click **License & System Update** and look for the [arcsight-logger](#) component.

- Logger v4.0 SP1 (L4248)
- Logger v4.0 GA (L4105)
- Logger v3.0 SP1 Patch 1 (L3406)
- Logger v3.0 SP1 (L3393)

These are the only supported upgrade paths. If you are using other versions, you need to upgrade to a supported version before upgrading to v4.0 SP1 Patch 1, or contact ArcSight Customer Support.

Understanding the Upgrade Process

If you are upgrading from Logger v4.0 GA or v4.0 SP1, you can skip this section.

If you are upgrading from Logger v3.0 SP1 or v3.0 SP1 Patch 1, read this section to understand the upgrade process in detail as it is different from the previous upgrades you have performed on your Logger.

An upgrade from Logger v3.0.x to Logger v4.0 SP1 Patch 1 takes a longer time than the previous releases because this process includes an upgrade of the database on your Logger. The amount of time it takes to upgrade is proportional to the amount of data. The time it will take to complete the upgrade on your Logger is automatically calculated and displayed on your Logger screen when you initiate the upgrade process.

When you upload the upgrade .enc file and click Upload Update, the upgrade process first determines the following:

- Are there any internal processes currently running that might conflict with the upgrade?

If such a process is found, this message is displayed:

"A process is currently running that may interfere with the upgrade. Please try upgrading later."

- Is there sufficient free space to proceed with the upgrade?

If sufficient space is not found, a warning message indicating the amount of space required and the amount of space available is displayed.

However, if sufficient space is found, an estimate of the time it would take to complete the upgrade is displayed.

- If the Logger is an L7100 appliance, was its database migrated (as described in the *Logger v3.0 SP1 Release Notes*)?

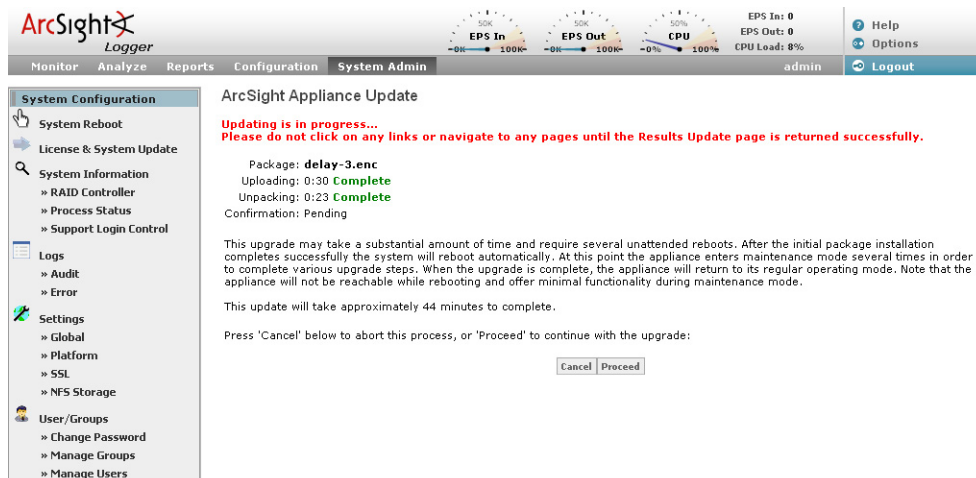
If the database has not been migrated, a warning message is displayed.

- If the saved searches or any filters reference resources such as devices, device groups, or peers that are no longer configured on the Logger.

An error message is displayed, which lists the filters and saved searches that reference non-existent resources. You need to either update or delete those filters and saved searches before proceeding with the upgrade.

If any of the above checks is not met and a warning or an error message is displayed, upgrade cannot proceed. You need to take appropriate action to resolve the issue before retrying the upgrade.

However, if all of the above checks are met, the following message is displayed that requires you to select whether to proceed with the upgrade or cancel it. If you proceed with the upgrade, the rest of the process is automatic and does not require interaction from you.



Once the upgrade starts, it is performed in the following three phases. Each phase is followed by an automatic reboot of the Logger.

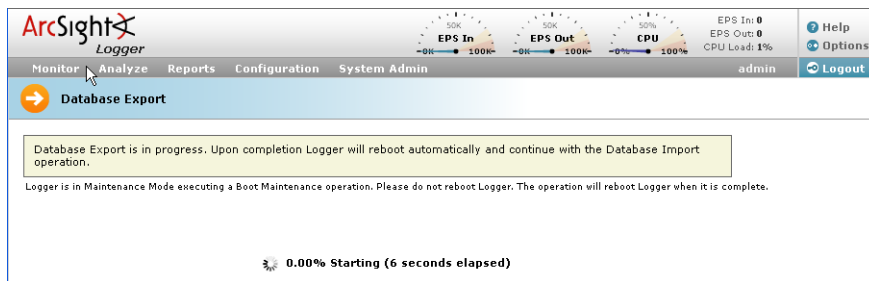
- Phase 1—Standard Version Upgrade

- Phase 2—Database Export
- Phase 3—Database Import

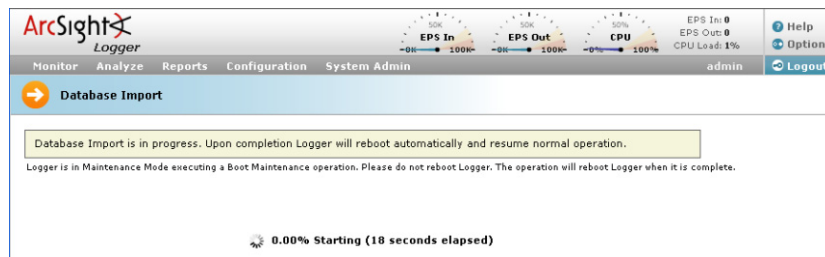
Phase 1 is the standard version upgrade that is performed on a Logger when you upload an [.enc](#) file on it. At the end of Phase 1, the Logger is automatically rebooted and all user sessions are disconnected.

After the Logger reboots, it enters maintenance mode to complete the remaining two upgrade phases. From this point on, you can only connect to it as a user with administrator-level privileges.

During Phase 2, data on the Logger is exported and the underlying database is upgraded. The following figure shows the message on your Logger screen at the end of Phase 2. At the end of Phase 2, Logger is automatically rebooted.



Once again, Logger enters maintenance mode for Phase 3 processing. During Phase 3, the exported data is imported back, as shown in the following figure.



At the end of Phase 3, Logger is once again rebooted automatically. At this point, the Logger returns to its regular operating mode and the Login screen is displayed.

Upgrade Files

You need the [logger_2c-4265.enc](#) file to upgrade your Logger. This file is available from the ArcSight Customer Support download site at <https://software.arcsight.com>.

Prerequisites and Caveats

Make sure you are familiar with the following information before upgrading.

- 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.
- Do not reboot or power cycle your Logger while the upgrade is in progress. If there is a power failure during the upgrade, generally Logger upgrade will resume once power is restored. However, if the upgrade does not resume, call ArcSight Customer Support for guidance.

- Although upgrading from v3.0.x might take some time, you can connect to your Logger at any time while it is upgrading to check the status except when it is automatically rebooting in between the three upgrade phases described in ["Understanding the Upgrade Process" on page 13](#).
- When upgrading from v3.0.x, all saved searches and shared and system filters on your Logger are converted to be compatible with the new, full-text search method introduced in Logger v4.0. Doing so ensures that the searches and filters will continue to function as they were prior to the upgrade. This conversion is automatically performed during the upgrade. After the upgrade, the Type field for the converted content is labeled "Unified Query". Note that the search group filters are not converted because only regular expressions are supported for these filters.
- Read the information in the ["Logger v4.0 SP1" on page 2](#) section in its entirety to determine the impact of upgrading to v4.0 SP1 on your existing content before you proceed with the upgrade.
- If you are upgrading an L7100 appliance, make sure you have migrated its database as described in the *Logger v3.0 SP1 Release Notes*. If you do not migrate the database prior to the upgrade, the upgrade process generates a warning and guides you to complete migration before proceeding further.

Upgrading the Logger

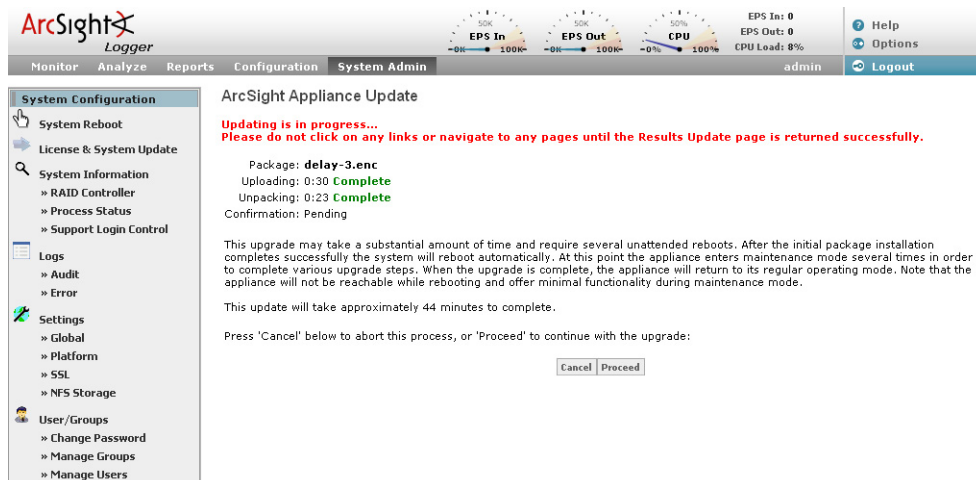
From v3.0 SP1 or v3.0 SP1 Patch 1 to v4.0 SP1 Patch 1

To upgrade the Logger:

- 1 Browse to the [logger_2c-4265.enc](#) file you downloaded earlier and click **Upload Update**.

The upgrade process runs the checks described in ["Understanding the Upgrade Process" on page 13](#) to determine whether it can proceed further.

- 2 **If sufficient space is found**, an estimate of the time it would take to complete the upgrade is displayed, as shown in the following figure.



If sufficient space is not found, a warning message indicating the amount of space required and the amount of space available is displayed. You need to make the required amount of space available before you can proceed with the upgrade. To make space available on your Logger, call ArcSight Customer Support for assistance.

In addition to the space check, the upgrade process also determines the following:

- ◆ Whether the database has been migrated on L7100 appliances (as described in *Logger v3.0 SP1 Release Notes*). If the database has not been migrated, the following warning message is displayed.

"The update process cannot proceed because the database on your Logger needs to be migrated. Please migrate the database and then restart the upgrade process. See *Logger v3.0 SP1 Release Notes* for information about database migration."

- ◆ Whether any internal processes that might conflict with the upgrade currently running?

3 Click **Proceed** to start the upgrade process.

If you don't take an action (that is, click Proceed or Cancel) within 2 minutes, the displayed screen will time out and you will need to restart the upgrade process from Step 1.

If you click Proceed, the rest of the upgrade process is automatic and does not require any interaction from you. Once the upgrade is complete, the Logger returns to its regular operating mode and the Login screen is displayed.

4 Perform the post upgrade tasks described in "Post upgrade tasks:" on page 17.

From v4.0 GA or v4.0 SP1 to Logger v4.0 SP1 Patch 1

To upgrade the Logger:

1 Browse to the `logger_2c-4265.enc` file you downloaded earlier and click **Upload Update**.

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

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

3 After the reboot, perform the post upgrade tasks described in the next section.

Post upgrade tasks:

1 Log in to the Logger.

2 **For Loggers upgraded from v3.0.x:**

- a** **Full-text indexing** and the following fields are not added automatically for indexing even if indexing is enabled on your Logger:

- deviceReceiptTime
- deviceInboundInterface
- deviceOutboundInterface

Therefore, you need to add these fields manually. Doing so will ensure that search operations run with optimal performance.

To enable full-text indexing and add these fields, click **Configuration > Search Optimization > Search Indexes > "Select Recommended Fields"**.

- b** If you had changed the "Zone Population Mode" setting on the connectors sending events to this Logger from "Normal" to "Rezone" based on the information in the *SmartConnector User's Guide*, you need to reset that setting to "Normal". For more information, see the *SmartConnector User's Guide*.

- 3 Create a configuration backup of your Logger. For instructions on creating a configuration backup, refer to the *Logger v4.0 SP1 Administrator's Guide*.

Logger v4.0 SP1 Patch 1 Documentation and Help


The *Logger v4.0 SP1 Administrator's Guide* and the online Help are applicable to the v4.0 SP1 Patch1 release. This documentation is 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:

- 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 fixes the following issues.

Number	Description
67249	<p>Upgrade from version 3.x to v4.0 SP1 Patch1 would fail when the saved searches or any filters on a Logger referenced resources—devices, device groups, or peers—that no longer existed on it.</p> <p>FIX: The upgrade process now checks for the existence of resources that saved searches and filters on a Logger reference. If any of the resources is not found, the upgrade process generates an error message that includes a list of the saved searches and filters that must be updated or deleted before restarting the upgrade.</p>
64803	<p>Upgrade to Logger v4.0 SP1 would fail.</p> <p>FIX: The upgrade process has been updated to ensure that the upgrade does not fail due to internal process dependencies.</p>

Number	Description
65105	<p>Common Access Card (CAC) authentication did not work if chained certificates were used.</p> <p>Fix: The product software has been enhanced to allow chained certificates.</p> <p>Note: If the "Use client certificate" option is enabled on the Authentication tab before you upgrade to Logger v4.0 SP1 Patch 1, you need to re-confirm the authentication settings after you upgrade and reboot the appliance for the change to take effect.</p> <ol style="list-style-type: none"> 1 Click Setup > System Admin from the top-level menu bar. 2 Click Authentication from the Users/Groups section in the left panel. 3 On the Authentication tab, ensure that Yes is enabled next to the "Use client certificate" option. 4 Click Save Settings. 5 Reboot the appliance.
65210	<p>When Logger was in maintenance mode to perform a task such as database defragmentation, a resource contention between internal processes could stall the task indefinitely.</p> <p>Fix: The product software has been updated such that Logger will not enter maintenance mode if resource contention can occur. Also, additional checks have been included to ensure that internal processes do not compete for the same resources at the same time if Logger is in maintenance mode.</p>

The following issues were fixed in Logger v4.0 SP1.

Number	Description
58420	<p>The Maintenance Results page displays "System" as the Creator of the Database Migration task even if another user started it.</p> <p>Fix: The Maintenance Results page now displays the actual name of the user who started the process.</p>
61781	<p>Logger v4.0 Administrator's Guide does not discuss the "Save to Local Disk" option on the Export Filters and Export Alerts page (Configuration > Filters > Export and Configuration > Alerts > Export).</p> <p>Fix: The documentation has been updated to include this option. See the Logger v4.0 SP1 Administrator's Guide or refer to "Other Information You Need to Know" on page 11 in these release notes.</p>

In addition, the following issues were fixed in Logger v4.0 GA.

Number	Description
44580	<p>A Delete button appeared in the Published Reports list even if the current user had only View privileges.</p> <p>Fix: The Delete button has been removed.</p>
44597	<p>Users who did not have privileges to delete public reports could still delete their own private reports. Therefore, in a table of reports, some delete icons were enabled while others were disabled.</p> <p>Fix: Users without delete privileges cannot delete any reports now.</p>

Number	Description
44715	Reports were limited to show no more than the first 100,000 events. Fix: The product software has been enhanced to show greater than 100,000 events.
45959	In a Japanese language PDF-format report, the report titles did not display in Japanese. Fix: The report titles are displayed in Japanese now.
50353	If the time on a device was set incorrectly, such that the device time was ahead of the connector time, events received on the connector could have the Device Receipt Time greater than the Agent Receipt Time, resulting in error messages similar to the following. "Device Receipt Time from "device name .." may be incorrect - Device Receipt Time is greater than Agent Receipt Time (Events are in the future). Fix: No fixes to the Logger product are required for this issue. This issue is resolved if the connector is configured to use the "Time Correction" option.
50366	After attaching to a SAN, the SAN Storage Administration page would list the Attachment Status as <code>unavailable</code> . Fix: The Attachment Status is correctly displayed now.
50405	In a disaster recovery scenario, restoring a Logger that used a remote file system (RFS, CIFS, or SAN) for primary storage required you to perform a Configuration Restore before you set up a Storage Volume. This Restore would not set the Storage Volume to use the remote file system as before. Fix: The issue has been fixed to correctly establish the remote file system mount points after a restore.
51661	The Export Alerts and Export Filters pages were not displaying the most up-to-date list of alerts and filters respectively. That is, alerts/filters that had been recently deleted were displayed, while alerts/filters that were recently added were not listed. Fix: The pages display up-to-date lists of alerts and filters now.
52008	When a user ran a report that included a search group filter that restricted users from a device group, the report would still include internal events from devices in that device group. Fix: Internal events from the restricted device group are no longer included in the report run by the user who does not have privileges to the device group.
52328 / 52191	After configuring storage groups during the Logger initialization sequence, when you clicked the Configure Index fields.... link, a blank or partial page was displayed instead of the Add Search Indexes page. Fix: A blank page is no longer displayed.
52388	Mounting a very large (such as 4TB) LUN would take longer than the default Logger session timeout resulting in the administrator getting disconnected before the LUN was mounted. The SAN storage Administration page displayed <code>unavailable</code> in the Attachment Status column. Fix: The product enhancements made in this release eliminate this issue.

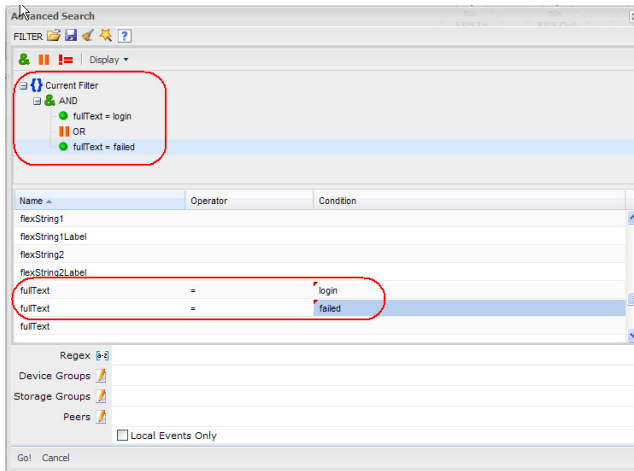
Number	Description
52710 / 52907	<p>When a peer Logger became unavailable during a search operation, the Search Results tab would display one of these errors:</p> <p>[Peer Logger IP address] Error: Get Query Statistics</p> <p>[Peer Logger IP address] Error: Remote exception (Peer does not authorize the request. Please check if remote peer has peer relationship with your logger)</p> <p>Fix: A number of software enhancements related to peer Loggers have been made in this release, which eliminate this issue.</p>
54539	<p>Chart Reports did not display Japanese captions.</p> <p>Fix: Japanese captions are now displayed in Chart reports.</p>
54893	<p>If an expired or invalid license was present on Logger, clicking the online Help link displayed the License & System Update page instead of displaying Help or a meaningful error message.</p> <p>Fix: Online Help is displayed irrespective of the license validity.</p>
57613	<p>If you specified a custom report name in the Save Report Layout As page, the name was overwritten when you selected a category from the Category List.</p> <p>Fix: The custom report name is no longer overwritten.</p>
60628	<p>Once pre-allocation started, the user interface screen would turn blank; only the top-level menu continued to be displayed.</p> <p>Fix: The complete user interface is now displayed.</p>

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	<p>Currently, you can enable a maximum of five alerts at any time on Logger. When you try to exceed this limit, the following message is displayed:</p> <p>The maximum number (5) of active alerts has been reached. To activate this alert, please de-activate at least one other first.</p>
Database Migration	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>

Function	Issue Number	Description
Group Administration	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</i> and <i>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.
Logs - Audit	49286	All Logger application audit events are logged to an internal database.
Monitor	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 alerts as well as from Forwarders. Therefore, if you have Alerts configured on your Logger, EPS Out can be greater than zero.</p>
	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	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	46104	<p>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.</p> <p>Workaround: If it is necessary to press the reset button, be prepared to power-down Logger (particularly the L3000) to restart smoothly.</p> <p>This problem only affects the reset button functionality and does not occur during a normal reboot.</p>
	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	<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>

Function	Issue Number	Description
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.
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 <i>fullText</i> field under the Name column, as shown in the following figure. To locate the <i>fullText</i> 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 <i>Logger v4.0 SP1 Administrator's Guide</i> .

Open Issues in this Release

The following issues are open in the Logger v4.0 SP1 Patch 1 release and will be addressed in a future release. Use the workaround noted, where available.

If your Logger platform is a Logger-Connector Appliance integrated solution, make sure you also read the release notes available for the specific release of Connector Appliance installed on your appliance. The Connector Appliance release notes are available from the ArcSight Customer Support site at <https://support.arcsight.com>. The upgrade section in the Connector Appliance release notes does not apply to the Logger-Connector Appliance integrated solution.

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.
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.

Function	Issue Number	Description and Workaround
Certificates	61134	<p>After a certificate is deleted from these pages, the deleted certificate is not removed from the list, leading to an impression that the certificate is still loaded on the system:</p> <p>Configuration > Event Input/Output > Certificates</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	<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	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>
	52540	Published reports are not included in a Report backup.
	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>
	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 the 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>

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 the Logger, as described in "Other Information You Need to Know" on page 11 in these release notes.
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	<p>If the field value in a search query URL contains any special characters (such as), the query fails to run on the ESM Manager.</p> <p>Workaround: Enclose the field values in the URL of the search query as follows:</p> <pre>"{value}"</pre> <p>For example,</p> <pre>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}"</pre>
FIPS 140-2	61941	<p>The SCP and SFTP protocols (for setting up File Transfer Receivers) are not FIPS compliant. Documentation does not indicate this fact.</p> <p>Workaround: Configure File Transfer Receivers to use FTP.</p>
	65327 / 65357	<p>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 reenabling FIPS on the forwarder is unsuccessful.</p> <p>Action: Contact ArcSight Customer Support for further assistance.</p>
Forwarder	47758	<p>A forwarder configured with a filter might not forward events that match the specified end time.</p> <p>Workaround: Extend the end time by 1 second to ensure that all events are forwarded appropriately.</p>
Peer Loggers	59521	<p>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.</p> <p>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.</p>
	61369	<p>If there is an improper tear-down of the peering relationship, the 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 the Loggers before reinitiating the relationship.</p>

Function	Issue Number	Description and Workaround
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.
	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.
	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 (<a href="https://<IP address or hostname of Logger machine>">https://<IP address or hostname of Logger machine>).

Function	Issue Number	Description and Workaround
Reports	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.
	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.
	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; <code>"Failed to generate report from rpg because server failed to deserialize the Report Pages"</code>
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: <ul style="list-style-type: none"> System Admin > NFS > Add NFS Mount System Admin > CIFS > Add CIFS Mount

Function	Issue Number	Description and Workaround
Search	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>
	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> <pre><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</pre> <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>
	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	61305 / 61338	<p>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:</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> <p>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.</p>
	61567	<p>A search query that includes an escaped double quotes in a regular expression (for example, REGEX="\logger\"") fails when run on a peer Logger.</p> <p>The query does run as expected on the local Logger.</p>
	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>
	63055	<p>Search results are not highlighted for values that match the IN operator in a query.</p>
Storage	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>
	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>
	56602	<p>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.</p> <p>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.</p>

Function	Issue Number	Description and Workaround
Storage	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 the Logger.</p>
Support Login	63224	<p>The Support Login page (System Admin > Support Login) does not load occasionally.</p> <p>Workaround: Click System Admin > Process Status > 'aps' (under the Processes list) > Restart.</p>
Maintenance Mode	57474	<p>The System Maintenance option (Configuration > System Maintenance) might not be available if your system has been upgraded from v2.5 or earlier.</p> <p>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.</p> <p>Workaround: Set the Enable Maintenance Mode permission to Yes for the System Admin group.</p>
System Admin - SMTP	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.
System Admin - SSL Client Auth	61980	<p>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.</p> <p>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.</p>
User Interface	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>
	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	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.
	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.
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.

