

# **Release Notes ArcSight Logger™**

---

Version 4.0 GA (Build L4105)

November 15, 2009



## Release Notes ArcSight Logger™, Version 4.0 GA (Build L4105)

Copyright © 2008-2009 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
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.
11/10/08	Logger v3.0	Added the known issue about ESM forwarder.
10/23/08	Logger v3.0	Added instructions to upgrade L3000.
10/21/08	Logger v3.0	Description, contents, upgrade instructions, fixed issues, known behaviors, and open issues.

Release Notes template version: 2.0.0

### ArcSight Customer Support

<b>Phone</b>	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
<b>E-mail</b>	<a href="mailto:support@arcsight.com">support@arcsight.com</a>
<b>Support Web Site</b>	<a href="https://support.arcsight.com">https://support.arcsight.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

# Contents

---

**ArcSight Logger™ v4.0 GA ..... 1**

    What’s New in Logger v4.0 GA ..... 2

    Upgrading to Logger v4.0 GA (L4105) ..... 10

    Logger v4.0 GA Documentation and Help ..... 10

        Connector Appliance Documentation ..... 10

    Issues Fixed in this Release ..... 11

    Known Behaviors in this Release ..... 12

    Open Issues in this Release ..... 14



# ArcSight Logger™ v4.0 GA

---

These release notes provide information about the ArcSight Logger v4.0 GA (L4105) release. Read this document in its entirety before using a Logger installed with this release.

This document covers the following topics.

- [“What’s New in Logger v4.0 GA” on page 2](#)
- [“Upgrading to Logger v4.0 GA \(L4105\)” on page 10](#)
- [“Logger v4.0 GA Documentation and Help” on page 10](#)
- [“Issues Fixed in this Release” on page 11](#)
- [“Known Behaviors in this Release” on page 12](#)
- [“Open Issues in this Release” on page 14](#)

## What's New in Logger v4.0 GA

This section lists the new features/enhancements introduced in the Logger v4.0 release. See the *Logger v4.0 Administrator's Guide* for details of these features, which is 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.

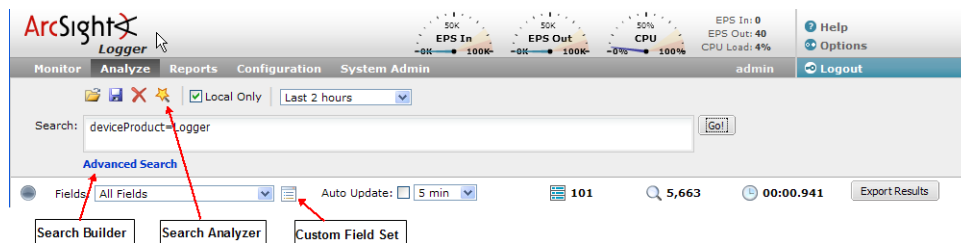
### ■ Enhanced Search function

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"
```

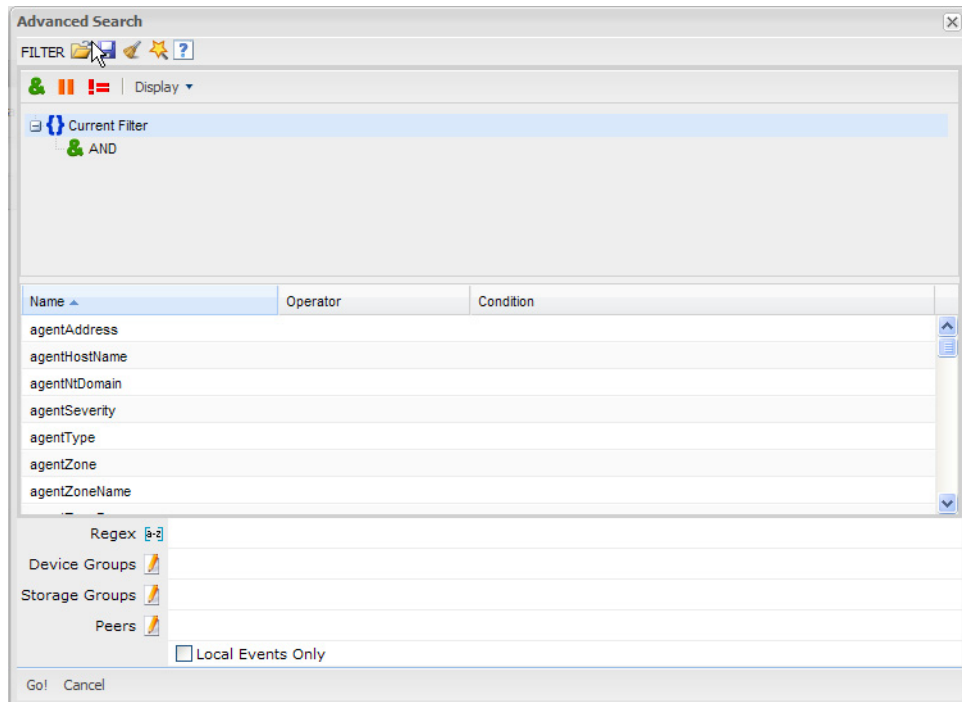


Other significant improvements related to search are:

#### ◆ 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`)

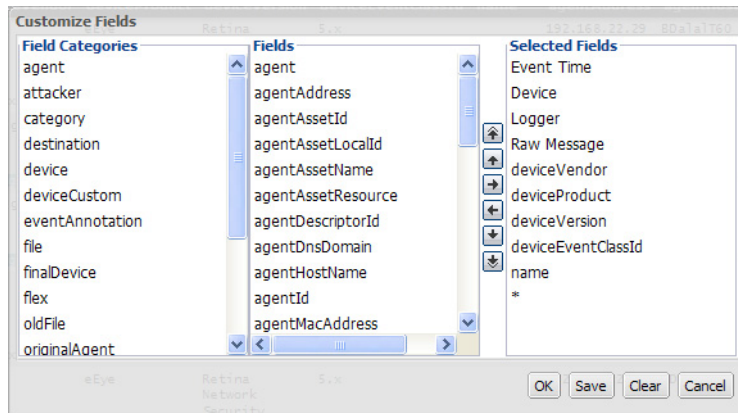
Type "\_s" (for storage group), "\_d" (for device group), or "\_p" (for peerLogger) in the Search text box to obtain a drop-down list of constraint terms and operators.

- 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.



- 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.

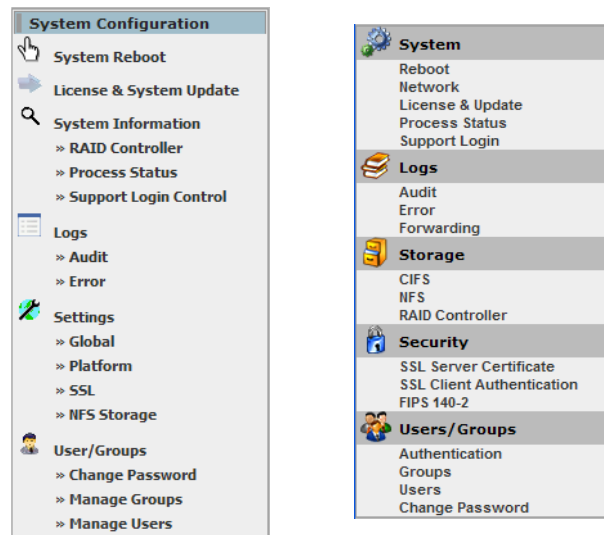
The `requestUrl` field cannot be indexed.

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 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 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 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 in this document, *Logger Administrator's Guide*. See "System Health Events" in the *Logger v4.0 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>.

## ■ 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 case.

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

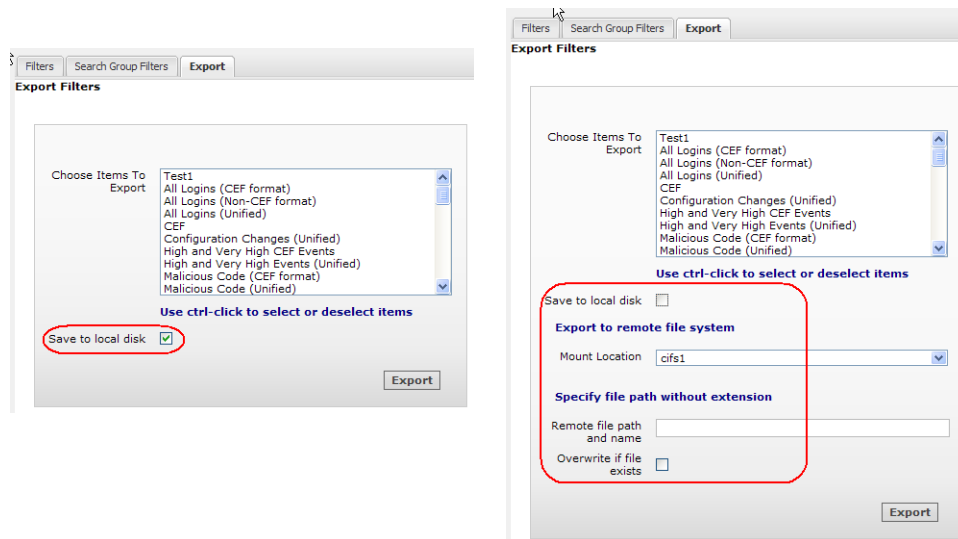
Use ctrl-click to select or deselect items

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 GA (L4105)

You cannot upgrade from a previous Logger version to Logger v4.0 GA. This release is only available on new Loggers shipping from ArcSight.

## Logger v4.0 GA Documentation and Help

The *Logger v4.0 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:

- 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
44580	<p>A Delete button appeared in the Published Reports list even if the current user had only View privileges.</p> <p><b>Fix:</b> 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><b>Fix:</b> Users without delete privileges cannot delete any reports now.</p>
44715	<p>Reports were limited to show no more than the first 100,000 events.</p> <p><b>Fix:</b> The product software has been enhanced to show greater than 100,000 events.</p>
45959	<p>In a Japanese language PDF-format report, the report titles did not display in Japanese.</p> <p><b>Fix:</b> The report titles are displayed in Japanese now.</p>
50353	<p>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.</p> <p>"Device Receipt Time from "device name .." may be incorrect - Device Receipt Time is greater than Agent Receipt Time (Events are in the future).</p> <p><b>Fix:</b> 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.</p>
50366	<p>After attaching to a SAN, the SAN Storage Administration page would list the Attachment Status as <code>unavailable</code>.</p> <p><b>Fix:</b> The Attachment Status is correctly displayed now.</p>
50405	<p>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.</p> <p><b>Fix:</b> The issue has been fixed to correctly establish the remote file system mount points after a restore.</p>
51661	<p>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.</p> <p><b>Fix:</b> The pages display up-to-date lists of alerts and filters now.</p>
52008	<p>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.</p> <p><b>Fix:</b> 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.</p>

Number	Description
52191	<p>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.</p> <p><b>Fix:</b> A blank page is no longer displayed.</p>
52388	<p>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.</p> <p><b>Fix:</b> The product enhancements made in this release eliminate this issue.</p>
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><code>[Peer Logger IP address] Error: Get Query Statistics</code>  <code>[Peer Logger IP address] Error: Remote exception (Peer does not authorize the request. Please check if remote peer has peer relationship with your logger)</code></p> <p><b>Fix:</b> 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><b>Fix:</b> 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 &amp; System Update page instead of displaying Help or a meaningful error message.</p> <p><b>Fix:</b> 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><b>Fix:</b> 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><b>Fix:</b> The complete user interface is now displayed.</p>

## Known Behaviors in this Release

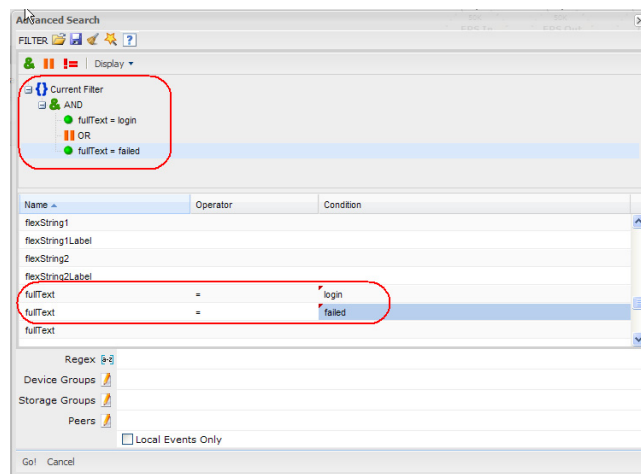
The following items represent characteristics of the product that work as-designed, as-expected, are not bugs, or are known issues that involve third-party products.

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><code>The maximum number (5) of active alerts has been reached. To activate this alert, please de-activate at least one other first.</code></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 &gt; 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"> <li>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.</li> <li>Logger Rights Group with the <i>View Scheduled Tasks</i> user right set to Yes.</li> </ul>
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><b>Understanding:</b> 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><b>Understanding:</b> 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><b>Workaround:</b> Wait until the CSV file has been downloaded, or use another browser to access Logger.</p>
Platform	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><b>Workaround:</b> Manually change the port, if desired.</p>
Reports	44952	<p>Base Foundation and Solution report queries can be edited.</p> <p><b>Workaround:</b> ArcSight recommends that you first make a copy of these reports and then edit them.</p>
	57690	<p>A user belonging to the Default Logger Report Group and the Default Logger Search Group cannot view the scheduled reports (Reports &gt; Scheduled Reports).</p> <p><b>Understanding:</b> The user also needs to belong to the Logger Rights Group to view the scheduled reports.</p>
	61526	<p>Report Execution Status (Reports &gt; Default Dashboard) page does not list scheduled reports.</p> <p><b>Workaround:</b> View the scheduled reports that have run on the Finished Tasks page (Configuration &gt; Scheduled Tasks &gt; Finished Tasks).</p>

Function	Issue Number	Description
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.
	60354 / 60716	<p>When using the Search Builder (accessed using the Advanced Search link on the Search page) to create a query, user interface is not intuitive about how to enter a keyword (full-text) term.</p> <p><b>Understanding:</b> To specify a keyword (full-text search), use the <i>fullText</i> field under the Name column, as shown in the following figure. To locate the <i>fullText</i> field, scroll down.</p>



## Open Issues in this Release

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

The following open issues have existed in the product since Logger v3.0 SP1. Use the workaround noted, where available.

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.

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><b>Configuration &gt; Event Input/Output &gt; Certificates</b></p> <p><b>Configuration &gt; Alerts &gt; Certificates</b></p> <p><b>Workaround:</b> 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 &gt; SSL Server Certificate &gt; View Results) displays the following error instead of the installation results for an SSL certificate:</p> <p>--- No Results Exist ---</p> <p><b>Workaround:</b> Because this issue is only experienced in the Firefox browser, use Internet Explorer to view these results.</p>
Configuration Backup	36373	<p>The Configuration Backup (Configuration &gt; Configuration Backup &gt; Name_of_Backup) and File Transfer Receivers (Configuration &gt; Event Input/Output &gt; 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><b>Workaround:</b> The error is written to the log in this case, so use Retrieve Logs page (Configuration &gt; 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 <a href="#">57778</a>.</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><b>Workaround:</b> Ensure that the Remote Directory name does not contain a space.</p>
Connector	48329	<p>On L3x00 models, it is possible to add a Logger receiver on the same port on which a connector is already configured.</p> <p><b>Workaround:</b> Ensure that you are using unique ports for receivers and connectors configured on your Logger. Connectors use ports starting at 60000.</p>
	52170	<p>On the L3x00 platform, a duplicate connector is created under the localhost container after upgrading to v3.0.</p> <p><b>Workaround:</b> Delete the duplicate connector created in the localhost container.</p> <p><b>Note:</b> This bug does not affect the core system functionality.</p>
Connector Appliance	61457	<p>During a bulk upgrade of Containers, if a Container is unavailable (status 'Down'), it is skipped, and thus it is not upgraded.</p> <p><b>Workaround:</b> Ensure that the Container status is 'Up' before starting the upgrade.</p>

Function	Issue Number	Description and Workaround
Content Export/Import	51630	The type associated with imported filters cannot be changed from shared to saved search.
	51657 / 52201	<p>If content is imported on a Logger that does not have the same configuration setup (devices, device groups, storage groups) as the exporting Logger, content that relies on that configuration cannot be used.</p> <p><b>Understanding:</b> This behavior is in accordance with the Content Import/Export feature design. Therefore, make sure the importing Logger has the same configuration setup as the exporting Logger.</p>
	61779	<p>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.</p> <p><b>Workaround:</b> 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 <a href="#">"Other Information You Need to Know"</a> on page 8 in these release notes.</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 &gt; Filters &gt; Export and Configuration &gt; Alerts &gt; Export).</p> <p><b>Workaround:</b> Refer to <a href="#">"Other Information You Need to Know"</a> on page 8 in these release notes.</p>
Defragmentation	57638	<p>A blank screen might display when you enter maintenance mode for database defragmentation.</p> <p><b>Workaround:</b> Refresh the screen manually using your browser refresh function.</p>
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><b>Workaround:</b> 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&amp;pass=password&amp;url=/logger/search.ftl&amp;ausm_query=deviceEventClassId="{CVE GENERIC-MAP-NOMATCH}"&amp;from=1%20Sep%202009%200:00:00%20PDT&amp;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><b>Workaround:</b> Configure File Transfer Receivers to use FTP.</p>
Forwarder	47758	<p>A forwarder configured with a filter might not forward events that match the specified end time.</p> <p><b>Workaround:</b> Extend the end time by 1 second to ensure that all events are forwarded appropriately.</p>

Function	Issue Number	Description and Workaround
Peer Loggers	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><b>Workaround:</b> 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>
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	<p>In the Reports Designer, changing the parameter type TextBox to another type causes an error.</p> <p><b>Workaround:</b> Do not edit an existing parameter whose type is set to TextBox. Instead, delete that parameter and add a new one.</p>
	45091	<p>Users who are granted only edit and save report styles privileges do not see the Template Styles link on the Reports tab.</p> <p><b>Workaround:</b> Grant users that need to access Template Styles admin privileges.</p>
	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	<p>The default date/time in reports does not include the time of day.</p> <p><b>Workaround:</b> Choose a date format that includes HH:MM:SS, if needed.</p>
	45447	<p>Some predefined report templates do not support i18n characters.</p> <p><b>Workaround:</b> Test the report template for the desired character set before production use. This issue will be fixed in a later release.</p>
	45548	<p>Adding a scheduled report can reset the scan limit field of other reports.</p> <p><b>Workaround:</b> Check that the scan limit is set as desired before running any report.</p>
	45568	<p>The Dashboard does not have a scroll bar.</p> <p><b>Workaround:</b> Set the "Show Scrollbar" property to "Yes" in the Widget Properties section of the External Links and Use Cases Dashboard Items.</p>

Function	Issue Number	Description and Workaround
Reports	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. <b>Workaround:</b> 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. <b>Workaround:</b> 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. <b>Workaround:</b> To make the Reports function tab reappear, go to the top-level Logger URL ( <a href="https://&lt;IP address or hostname of Logger machine&gt;">https://&lt;IP address or hostname of Logger machine&gt;</a> ).
	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. <b>Workaround:</b> Remove the alias from the query. If you need to use aliases, include them in the Caption field of the report query editor.
	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. <b>Workaround:</b> 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. <b>Workaround:</b> Ignore the "Failure" status.

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><b>Understanding:</b> Color Block View expects two conditions. Therefore, do not use this view if your query contains only one condition.</p> <p><b>Workaround:</b> To get rid of the warning message so that you can use the Tree View:</p> <ol style="list-style-type: none"> <li>1 Switch to Tree View.</li> <li>2 Include a second "placeholder" condition.</li> <li>3 Click GO.</li> </ol> <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>&lt;166&gt;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><b>Workaround:</b> 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><b>61305:</b> 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><b>61338:</b> 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>
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><b>Workaround:</b> Refresh the browser or check the page again later.</p>
	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><b>Recommendation:</b> 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>
System Admin - SMTP	61378	<p>Changes made to existing SMTP information (System Admin &gt; Network &gt; 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><b>Workaround:</b> Restart the forwarder process for the new information to take effect. To restart the process:</p> <ol style="list-style-type: none"> <li>1 Click <b>System Admin &gt; Process Status</b>.</li> <li>2 Click <b>processors</b> from the Process list.</li> <li>3 Click <b>Restart</b> in the bottom right corner of the screen.</li> </ol>



Function	Issue Number	Description and Workaround
User Interface	42662	The Save to Logger operation overwrites an existing file of the same name. <b>Workaround:</b> 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. <b>Workaround:</b> 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. <b>Workaround:</b> 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. <b>Workaround:</b> 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. <b>Workaround:</b> 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. <b>Workaround:</b> Provide Device Group and Storage Group names that do not reveal internal information.

