

Release Notes ArcSight Logger™

Version 5.0 GA (Build L5139)

September 19, 2010



Release Notes ArcSight Logger™, Version 5.0 GA (Build L5139)

Copyright © 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
09/19/10	Logger v5.0 GA	First Logger - Downloadable Version release.
07/22/10	Logger v4.5 GA	Version 4.5 GA release. First software-only version option for Logger.
05/21/10	Logger v4.0 SP1 Patch1	Update to the original Patch 1 for v4.0 SP1 to include additional checks in the upgrade process for references to non-existent resources.
03/01/10	Logger v4.0 SP1 Patch1	Patch 1 for v4.0 SP1.
02/04/10	Logger v4.0 SP1	Added information about supported browsers.
01/29/10	Logger v4.0 SP1	Service Pack 1 for version 4.0.
11/15/09	Logger v4.0 GA	Version 4.0 GA release.
09/30/09	Logger v3.0 SP1 Patch 1	Patch 1 for Service Pack 1. (Release supports new hardware)
08/27/09	Logger v3.0 SP1	Updated Database Migration instructions.
08/03/09	Logger v3.0 SP1	Service Pack 1 for v3.0.

Release Notes template version: 2.0.0

ArcSight Customer Support

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

Contents

- ArcSight Logger™ v5.0 GA 1**
 - What’s New in Version 5.0 GA 2
 - Logger v5.0 - Downloadable Version 2
 - Updated System Administration User Interface 2
 - Performance Improvement for Export Operation 3
 - Additional Platform Audit Events 3
 - Enhanced Internal Event 3
 - Other Information You Need to Know 3
 - Installing the Software Logger v5.0 (L5139) 4
 - Logger v5.0 GA Documentation and Help 4
 - Issues Fixed in this Release 4
 - Known Behaviors in this Release 5
 - Open Issues in this Release 8

ArcSight Logger™ v5.0 GA

These release notes provide information about the ArcSight Logger v5.0 GA (L5139) release. Read this document in its entirety before using a Logger installed with this release.

This document covers the following topics:

- [“What’s New in Version 5.0 GA” on page 2](#)
- [“Installing the Software Logger v5.0 \(L5139\)” on page 4](#)
- [“Logger v5.0 GA Documentation and Help” on page 4](#)
- [“Issues Fixed in this Release” on page 4](#)
- [“Known Behaviors in this Release” on page 5](#)
- [“Open Issues in this Release” on page 8](#)

What's New in Version 5.0 GA

Starting with this release, you can purchase and download the software Logger (Logger v5.0 - Downloadable Version) from ArcSight's corporate web site at <http://www.arcsight.com>. Additionally, this release introduces a simple, easy-to-use, Installation and Configuration wizard for the software form factor Logger. The wizard guides you through the installation and configuration process. If you accept most default settings, the total time it takes to install the software Logger is reduced to minutes thus allowing you to start using the Logger product quickly.

Logger v5.0 - Downloadable Version

(Available from <http://www.arcsight.com>)

The *Logger v5.0 - Downloadable Version* software can now be purchased and downloaded from ArcSight's corporate web site at <http://www.arcsight.com>. For the Enterprise version of Logger software, contact ArcSight Sales or your Channel Representative.

You can install the software Logger on a supported platform or on a VM image of a supported platform. You need a valid license file to install and use the software version of Logger, which is sent to you in an email from ArcSight once you have purchased the software.

Once you have received a license from ArcSight, follow the instructions in the *Quick Start Guide* or the *Logger Administrator's Guide* to install and configure Logger on a supported platform. The guides are available at the same location from where you download the software. This release introduces a simple, easy-to-use, Installation and Configuration wizard for the software Logger. The wizard guides you through the installation and configuration process. A console mode installation of this product is not supported.

Once you purchase the Logger software from ArcSight, you can also download ArcSight SmartConnectors that can collect and forward syslog data from your network to Logger in Common Event Format (CEF).

Updated System Administration User Interface

The System Admin tab menu has been reorganized to improve user experience. Some of the settings have moved to improve logical fit. For example, now SMTP is a separate option under the System category. The *Logger Administrator's Guide* contains updated procedures that can guide you through administration tasks. Please note that even though the menu has been reorganized, the features and functionality available under the System Admin tab have not changed.

The system administration options available on your user interface depend on the form factor on which Logger is installed. The following figure provides examples of both form factors: Logger appliance and Logger software.

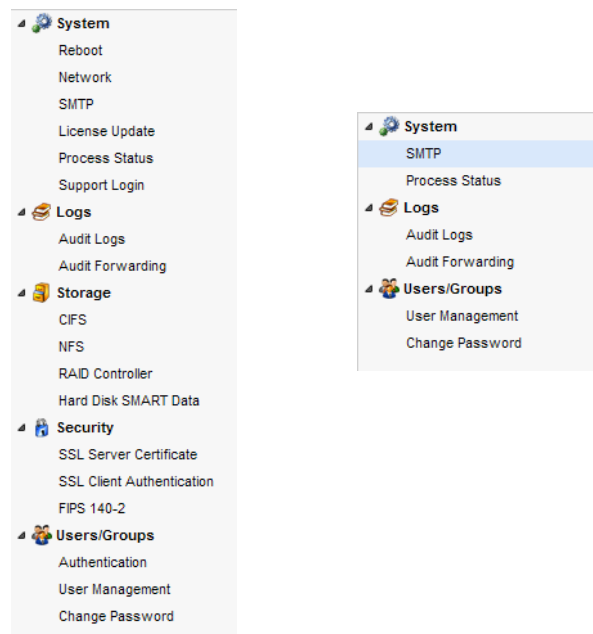


Figure 2-1 System Admin - Appliance (left); System Admin - Software (right)

Performance Improvement for Export Operation

The operation for exporting search results has been enhanced to improve performance of CSV and PDF exports. Both, CSV and PDF exports are now significantly faster than in the previous releases.

Additional Platform Audit Events

A number of new platform audit events are now generated on Logger. Additionally, the platform events are now stored in the Internal Storage Group thus allowing you to search on them using the Logger search UI and creating reports.

A complete list of audit events is available in the *Logger Administrator's Guide* in Appendix, "Logger Audit Events".

Enhanced Internal Event

The Logger Internal Event, Storage Group Usage (/Monitor/StorageGroup/Space/Used), has been enhanced to display the bytes (in MB) used per storage group.

Other Information You Need to Know

- A v5.0 software Logger cannot peer with a Logger (appliance or software) running v4.x. For detailed information about peering, see the *Logger Administrator's Guide*.
Additionally, the time and date on the system on with the software Logger is installed must be set correctly with respect to its timezone to peer with other Loggers. ArcSight recommends that you configure the Logger system to synchronize its time with an NTP server regularly.
- If you need to update your license on software Logger, make sure you restart the Logger service and related processes after applying the license. Use this command to restart the service and processes:

```
<install_dir>/current/arcsight/logger/bin/loggerd restart
```

- The *Logger Administrator's Guide* lists the system health events that Logger generates. Out of the listed events, the events of the following device event categories are generated only for the Logger appliance:
 - ◆ /Monitor/Sensor
 - ◆ /Monitor/RAIDController

Installing the Software Logger v5.0 (L5139)

See the instructions in the *Quick Start Guide* or the *Logger Administrator's Guide*, which are available from ArcSight Download Center at <https://arcsight.subscribenet.com>



You must use the Installation Wizard to install software Logger. Console mode installation of the product is not supported.

Logger v5.0 GA Documentation and Help

The Logger online Help 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.

The PDF version of Logger Administrator's Guide is available for download from the ArcSight Download Center at <http://arcsight.subscribenet.com>.

In addition, a *Quick Start Guide* is available from the ArcSight Download Center at <http://arcsight.subscribenet.com>. This guide provides information on how to download, install, and quickly start using your software Logger.

Issues Fixed in this Release

This release includes the fixes listed in the following table.

Issue Number	Description
LOG-5603 65439	Logger would not allow users to log in after the Logger time was changed due to DST in the Sao Paulo timezone. FIX: The product software has been updated to fix this issue.
LOG-5643 65725	Scheduled report jobs stopped running after upgrading to Logger v4.0 SP1. FIX: The product software has been updated to fix this issue.
LOG-5782 66710	The list of Logger audit events in the Logger v4.0 GA Administrator's Guide was not complete. FIX: The <i>Logger Administrator's Guide</i> has been updated and the list of internal events is now current.
LOG-5800 66826	When a new SQL query was created for a report, it was being run during validation using the parameters used for the last report run. FIX: The query is no longer run during validation.
LOG-6047 68059	Intermittently a report would return no data after it was run. FIX: The product software has been updated to fix this issue.

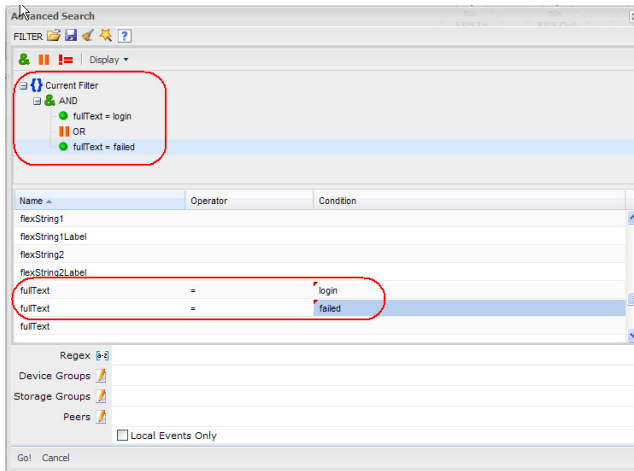
Issue Number	Description
LOG-6642 67266	<p>Logger search would fail with the following error:</p> <p>"Error: Database Connection"</p> <p>Understanding: If an event contained 127 or more tokens that started with the same character, an error was generated. In some cases, indexing on Logger could stop.</p> <p>FIX: The product software has been updated to allow more tokens that start with the same character.</p>
LOG-6643 65490	<p>For Event Archives, if the Time for the Daily Archive to Start was set to "Disabled", an error would generate.</p> <p>FIX: The product software has been updated to fix this issue.</p>
LOG-6646 61503	<p>The backup file created as a result of a scheduled backup was incorrectly named—the timestamp in the file name was when the backup was scheduled, not when the process actually ran. For example, the file name for a backup that ran on Dec 25 was 18Dec09_151559.configs.tar.gz.</p> <p>FIX: The files are now named based on the time when the backup runs, and not on the time when it is scheduled on Logger.</p>
LOG-6647 65721	<p>The report name of a scheduled report name could not be updated.</p> <p>FIX: The report name is appropriately updated now.</p>
LOG-6821	<p>Documentation on event archives and retention policy was not clear.</p> <p>FIX: Information on event archives and how retention policy relates to the archives has been updated in the <i>Logger Administrator's Guide</i>.</p>
LOG-6857	<p>The chart operator did not work when two fields were specified for it; the operator did work if one or more than two fields were specified.</p> <p>FIX: The product software has been updated to fix this issue.</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 real-time alerts at any time on Logger. When you try to exceed this limit, the following message is displayed:</p> <p><i>The maximum number (5) of active alerts has been reached. To activate this alert, please de-activate at least one other first.</i></p> <p>However, you can configure Saved Search alerts if you need more than five alerts. See the Logger Administrator's Guide for more information.</p>

Function	Issue Number	Description
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>
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 real-time alerts as well as from Forwarders. Therefore, if you have Alerts configured on your Logger, EPS Out can be greater than zero.</p>
	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	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 v4.5 release and will be addressed in a future release. Use the workaround noted, where available.

Function	Issue Number	Description and Workaround
Appliance	LOG-6697 63420	On the Logger appliance, the postgres process may not start when it can not write any files to the XFS filesystem. As a result, Logger is non-functional.
	LOG-3517 54065	A sudden power outage when Logger is actively receiving events may result in pgsql corruption on Logger. As a result, Logger may be non-functional.
	LOG-6346 69311	Logger UI does not provide information about the health of a drive. Workaround: Configure system alerts using the pre-defined System Filters. See the Logger Administrator's Guide for more information.
	LOG-5845 67216	After a v3.x Logger on which Storage Volume is not configured is upgraded to Logger v4.0.x, Logger fails to start. Workaround: Make sure a storage volume is configured on the v3.x Logger before you upgrade it.
	LOG-5572 65321	On the Logger appliance, it is not possible to enter a root password to get a prompt to run the <code>fsck</code> command manually.
	LOG-7111	On software Logger, the <code>openssl</code> command cannot be used. Therefore, the procedure described in the Logger Administrator's Guide, "Using a CA-signed Certificate on Software Version of Logger" is invalid for Logger v5.0.
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.
	LOG-5252 63607	When an Event Archive is deleted from the Logger UI, its corresponding events on a remote storage are not deleted. Understanding: This behavior is by design. Once events are archived to a remote storage, they cannot be deleted with ArcSight Customer Support's assistance.

Function	Issue Number	Description and Workaround
Alerts/Filters	44219	When multiple filters are selected for alerts, alerts might not generate because the selected filters are ANDed together, which might return an empty result set.
Certificates	61134	<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>
	68448	When an SSL Client Authentication certificate is removed or added to the Certificate Revocation List (CRL), any open SSL sessions remain valid until the browser window is explicitly closed.
Configuration Backup and Restore	36373	<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 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
Configuration Backup and Restore	LOG-5024 61517	If the system to which Logger is configured to back up its configuration is reinstalled or its SSL key is changed, the configuration backup fails because the SSL key cannot be refreshed from the Logger UI.
Connector Appliance	61457	During a bulk upgrade of Containers, if a Container is unavailable (status 'Down'), it is skipped, and thus it is not upgraded. Workaround: Ensure that the Container status is 'Up' before starting the upgrade.
	64031	The Logs link in the left side menu (Configuration > Repositories) is missing when a user belongs to only the System Admin Group. Workaround: Assign the user to the Logger Rights Group in addition to the System Admin Group.
Content Export/Import	51630	The type associated with imported filters cannot be changed from shared to saved search.
	51657 / 52201	If content is imported on a Logger that does not have the same configuration setup (devices, device groups, storage groups) as the exporting Logger, content that relies on that configuration cannot be used. Understanding: This behavior is in accordance with the Content Import/Export feature design. Therefore, make sure the importing Logger has the same configuration setup as the exporting Logger.
	61779	When content (filters or alerts) is exported to a remote file system, two files are generated instead of one—an empty file and a file with extension .xml.gz. Workaround: Use the file with the extension as it contains the exported content and ignore the empty file. Or export the content to the local disk of the computer from which you connect to Logger.
Defragmentation	57638	A blank screen might display when you enter maintenance mode for database defragmentation. Workaround: Refresh the screen manually using your browser refresh function.
ESM-Logger integration	60168	If the field value in a search query URL contains any special characters (such as), the query fails to run on the ESM Manager. Workaround: Enclose the field values in the URL of the search query as follows: <code>"{value}"</code> For example, <code>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}"</code>

Function	Issue Number	Description and Workaround
FIPS 140-2	61941	The SCP and SFTP protocols (for setting up File Transfer Receivers) are not FIPS compliant. Documentation does not indicate this fact. Workaround: Configure File Transfer Receivers to use FTP.
	65327 / 65357	When a FIPS-enabled Logger is upgraded from v4.0 GA to v4.0 SP1, FIPS gets disabled on the ESM Forwarder (System Admin > FIPS 140-2). An attempt to reenabling FIPS on the forwarder is unsuccessful. Action: Contact ArcSight Customer Support for further assistance.
Forwarder	47758	A forwarder configured with a filter might not forward events that match the specified end time. Workaround: Extend the end time by 1 second to ensure that all events are forwarded appropriately.
	LOG-6640 63473	Logger may stop forwarding events if the Storage Volume is full.
	LOG-6235 68912	Logger may stop forwarding events if excessive number of real-time alerts (in hundreds) are generated at the same time.
	LOG-6290 69066	Logger does not impose a limit on the number of forwarders that can be configured. However, configuring a large number of forwarders can have a severe impact on system performance. Understanding: The maximum number of forwarders is limited by your system's resources—memory, CPU, disk input/output.
Maintenance Mode	57474	The System Maintenance option (Configuration > System Maintenance) might not be available if your system has been upgraded from v2.5 or earlier. Understanding: When a Logger is upgraded from an older release, the Enable Maintenance Mode permission might not be automatically set for the System Admin group. Workaround: Set the Enable Maintenance Mode permission to Yes for the System Admin group.
Maintenance Mode	LOG-7048	When you click on Restart or Reboot after performing an action in maintenance mode, the following error is displayed: "The application is currently unavailable. Please retry shortly." Understanding: Logger is continuing to restart or reboot, therefore, keep refreshing the UI screen until the login screen is displayed.

Function	Issue Number	Description and Workaround
Peer 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, Loggers in the relationship might not detect it. Consequently, when you try to reestablish the relationship, it might not succeed.</p> <p>Examples of improper tear-down: One of the Loggers is replaced with a new appliance, or the peering relationship is deleted on one Logger while the other is unavailable (power down).</p> <p>Workaround: If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from Loggers before reinitiating the relationship.</p>
	68987	<p>If a search group filter specifies the peer Loggers on which a user can search and the user query contains a different peer Logger (which is not specified in the filter), the query runs on the peer Loggers specified in the filter. For example,</p> <p><i>Search group filter:</i> peer("peer1", "peer2")</p> <p><i>User query:</i> _peerLogger IN ["peer3"]</p> <p><i>The actual query that run:</i> _peerLogger IN ["peer1", "peer2"]</p>
	LOG-7065	<p>On a software Logger, the menu item for peer Logger (Configuration > Peer Loggers) is not available even though the correct license is applied.</p> <p>Workaround: Restart the Logger service using this command:</p> <pre><install_dir>/current/arcsight/logger/bin/loggerd restart</pre>

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.
	45570	After upgrading to Logger v4.5 GA, custom Report Configuration settings (Reports > Reports Administration) are reset to the default values. Workaround: Re-enter the custom values after the upgrade is complete.
	46286 / 50564 / 52340 / 53070 / 52760	Report-formatting issues might occur in very large reports (containing over 100,000 lines) configured to render in the Single Page HTML format. Workaround: Use the Multi-Page HTML format to resolve such report formatting issues.
	48613	The default report generated by clicking the hand icon is missing the report name and date. Workaround: Add the Report title to the Report Header section to render the title on the first page of the Report.

Function	Issue Number	Description and Workaround
Reports	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>).
	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.
	LOG-5348 64425 LOG-6750	A user with "Edit and Save Reports" right set to No is able to edit and save reports.

Function	Issue Number	Description and Workaround
Reports	65374	Published reports cannot be viewed after upgrading to v4.0 SP1 Patch 1. The following error is generated when a published report is viewed post upgrade; "Failed to generate report from rpg because server failed to deserialize the Report Pages"
	68925	Enabling or disabling dashboard refreshing ("Enable Dashboard Refreshing", "Disable Dashboard Refreshing") disables the Design and Preference links for the Dashboard.
	69058	When a scheduled report is created, the report name selected from the Report Name drop-down menu does not persist after you save the report. Workaround: You need to click the GO button next to the drop-down menu after selecting a Report to persist the report selection. Note: Once you have defined a scheduled report, you cannot change the selected report. If you need to change the to a different report, delete the scheduled report and define a new one.
	69076	If the Format setting is configured to JVISTA in Widget Properties when designing a Dashboard, the Dashboard is blank. Understanding: Do not use JVISTA as this is not a supported option.
	LOG-6060 68202	Logger only uses the first IP address even if there are multiple IP addresses resolving to an SMTP server name specified in the SMTP Server field under Report Administration (Reports > Report Administration), resolves to more than one DNS server. Consequently, if the first server is unavailable, reports cannot be e-mailed.
	LOG-7078	On a software Logger machine, a printer configured with special characters such as "&" may prevent scheduled reports from running.
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
	69331	Alert Viewer (Analyze > Alerts) displays two alerts for each triggered Saved Search alert. This issue does not exist for Real-time alerts.

Function	Issue Number	Description and Workaround
Scheduled Jobs	68824	<p>If the Finished Tasks page (Configuration > Scheduled Tasks > Finished Tasks) contains a very large number of entries, the page sometimes takes a while to load or stops loading.</p> <p>Workaround: If the pages stops loading, refresh the browser window to continue loading.</p>
	68633	<p>In the Internet Explorer browsers, versions 7 and 8, the Finished Tasks page (Configuration > Scheduled Tasks > Finished Tasks) displays the following warning:</p> <p>"Stop running the script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer might become unresponsive."</p> <p>Workaround: Ignore the warning and click Yes to proceed further.</p>
Search	59612	<p>The full-text (keyword) search cannot find events that contain an IP or a MAC address that is prefixed with an equal to (=) character in the actual event. For example, these full-text queries will not locate the following event.</p> <p>Query 1: "ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00"</p> <p>Query 2: "192.168.10.153"</p> <p>Query 3: "192.168.10.255"</p> <p><166>Sep 9 14:48:22 beach kernel: Killed bad incoming packet: IN=eth1 OUT=MAC=ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00 SRC=192.168.10.153 DST=192.168.10.255 LEN=229</p> <p>Workaround: This problem only occurs for a very small number of devices, which use this particular format. The workaround is to search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255.</p> <p>Alternatively, you could run these data through a SmartConnector to convert to CEF format. Then run either a full text or field based search.</p>

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>
	60121	The Search Builder (accessed using the Advanced Search link on the Search page) when used in Tree view, allows you to enter invalid operators for conditions. The tool does not generate any warning.
	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>

Function	Issue Number	Description and Workaround
Search	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	Search results are not highlighted for values that match the IN operator in a query.
	64786	<p>The export operation does not work when specific fields that include *user and * are exported.</p> <p>Note: The export operation does work if all fields (with the "All Fields" box checked) are exported, including * and *user.</p> <p>Workaround: Either export all fields (with the "All Fields" box checked) or export specific fields excluding *user and *. That is, to export specific fields, remove *user and * from the list.</p>
	LOG-6641 LOG-7099 66065	<p>When values for fields such as sourceUserId, sourceUserName, destinationUserId, and cs1 contain "\n" character, the search results are not displayed correctly.</p> <p>Understanding: The current software interprets a value that contains "\n" as a newline character. For example, user name "nancy" in example domain, "example\nancy", is interpreted as "example[newline]ancy".</p>
	LOG-6644 66491	<p>At times a search operation would fail with the following message right after the search had been initiated:</p> <p>"Search timed out"</p>
	68941	When search results containing non-English characters are exported in the PDF format, the event fields that contains those characters are blank in the exported file.
	69023	When search results are exported, the time elapsed to export the events is not displayed.
	69044	If the timezone setting is changed from PDT to JST on the software version of Logger, the events displayed in the browsers that connect to it do not reflect the correct event time.
	LOG-7027	For search queries that involve pipeline operators, the Scanned events count might stop incrementing while the Hits count and the Elapsed time continue to increment , even though in bursts. This behavior is intermittent.

Function	Issue Number	Description and Workaround
Search	69048	If the timezone setting on the Logger machine is different from the (local) machine from which you are connecting to Logger, the time ranges in the histogram are based on the local machine timezone while events in the search results display the Logger timezone. For example, if Logger is configured in PDT, while the browser from which you are connecting to it is on a machine in JST, the histogram displayed in the browser shows time ranges in JST, while the events in the search results show the timestamp in PDT.
	69158	In the Search results display, raw event fields are not separated by tab characters even when the original event contains those characters. <i>Original raw event:</i> Information 7/6/2009 10:24:31 AM crypt32 None 2 N/A XDEV <i>Search results display:</i> Information7/6/200910:24:31 AMcrypt32None2N/AXDEV
	68820	If a single event matches a query that contains the <code>where</code> operator, the event is not displayed in the search results screen. However, the "Hits" counter and the histogram display the correct number (1). Workaround: Click the histogram to display the event in the search results screen.
	69283	The number of Hits displayed on top of the Search Results screen may differ from the number shown at the bottom right of the screen in the "Displaying 1 - x of x" message. Workaround: Refreshing the browser syncs the two counts and displays the actual count.
Search Operators	69095	When a <code>where</code> operator is included in a query, the query performance can be significantly impacted. As a result, the query may not complete running and the user interface may hang. Understanding: This is a known issue and will be addressed in a future release of Logger. Suggestive Action: You can Cancel the search when this situation occurs and rerun the query with these changes: <ul style="list-style-type: none"> • Reduce the time range of the query • Refine the query to increase the selectivity of the query
	69160	The <code>top</code> and <code>rare</code> operators only pass forward fields specified for the operators; any other fields that might have been defined previous to those operators are rendered undefined. For example, the following query does not complete successfully because field "b" is considered undefined for the <code>chart</code> operator; therefore, the query generates an error. <code> cef a b c top a c chart _count by b</code> Workaround: Include all fields you would like to use later in the pipeline in the top command. For example, change the above example to: <code> cef a b c top a b c chart _count by b</code>

Function	Issue Number	Description and Workaround
Software Logger - Logger Service	LOG-6735	<p>When loggerd restart command is used to restart Logger service and process, the status message for the "aps" process displays this message:</p> <p><code>Process 'aps' Execution failed.</code></p> <p>The status and message change to the expected message after a few seconds:</p> <p><code>Process 'aps' running</code></p>
	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>
Storage	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>
	60152	<p>Even if pre-allocation of storage fails before the minimum requirement has been met, Logger allows you to skip pre-allocation and proceed to storage configuration.</p> <p>Recommendation: If pre-allocation fails, try to resume it. Skipping pre-allocation before it has successfully completed may result in sub-optimal performance on Logger.</p>
	66514	<p>On the software Logger, if the storage volume has 20% free space remaining, the following message is displayed:</p> <p><code>The storage volume does not have adequate free space to store incoming events. Increase the free space immediately to prevent Logger from disabling event storage. At least 20% free space is recommended.</code></p> <p>If 10% free space remains, Logger stops receiving events.</p> <p>Workaround: Free up space on your system to make more storage space available.</p>
	65649	<p>When software version of Logger is running out of storage space, the user interface screens accessible through the "Reports" and "System Admin" top-level menu do not display any warning. All other user interface screens do display the warning.</p>

Function	Issue Number	Description and Workaround
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>
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 - User Management	LOG-7113	<p>In the IE browser, hovering over a number in the Groups column on the Users page (System Admin > User Management) does not open up the Groups list in the first attempt. In the second attempt (by hovering again), the Groups list opens up, but the header for the list is missing.</p>
System Admin - Group Rights	LOG-7080 LOG- 7062	<p>On the software Logger, the Edit Group page for the System Admin Group allows you to set System Admin rights that are not applicable to it.</p> <p>On the "Logger - Downloadable Version" product, the Logger Search Group displays the "Search for events on remote peer" right, which is not applicable to this product.</p>
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>
	LOG-5594 65414	<p>If authentication is set to the following parameters:</p> <p>Use client certificate - Yes</p> <p>Require additional password - No</p> <p>Allow password fallback - Yes</p> <p>Then, the login banner does not display if SSL Client Authentication (CAC login) is successful. Logger displays the "Monitor" page directly.</p>

Function	Issue Number	Description and Workaround
Uninstall Software Logger	68882	<p>When the software version of Logger is uninstalled, the uninstall program removes all contents of the <code>/opt/arc sight</code> directory. If you have other ArcSight products such as Connectors installed in this directory, they will be removed as well.</p> <p>Workaround: Ensure that you do not have other ArcSight products such as Connectors installed in the <code>/opt/arc sight</code> directory before uninstalling the software version of Logger.</p>
	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>
User Interface	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>
	52452	<p>In the Firefox browser, the vertical scroll bar is missing from the PCI 2.1 Executive Report.</p> <p>Workaround: Use the IE browser instead.</p>
	60810	<p>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.</p> <p>Workaround: Upgrade your browser to Firefox v3.x.</p>
	61869	<p>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.</p> <p>Workaround: Upgrade your Firefox browser to v3.x on Linux systems. Use IE v7.x on Windows systems.</p>
	64311 / 68581	<p>In the Internet Explorer 8.x browser, clicking the Configuration tab displays a blank screen.</p> <p>Workaround: When a blank screen displays, click the Configuration tab again from the top-level menu bar.</p>
User Privileges	40872	<p>Under certain circumstances, users with restricted privileges might still see Device Group and Storage Group names. If these users are also subject to a Search Group Filter (enforced filter), they will not be able to see events in those Device Groups or Storage Groups.</p> <p>Workaround: Provide Device Group and Storage Group names that do not reveal internal information.</p>