

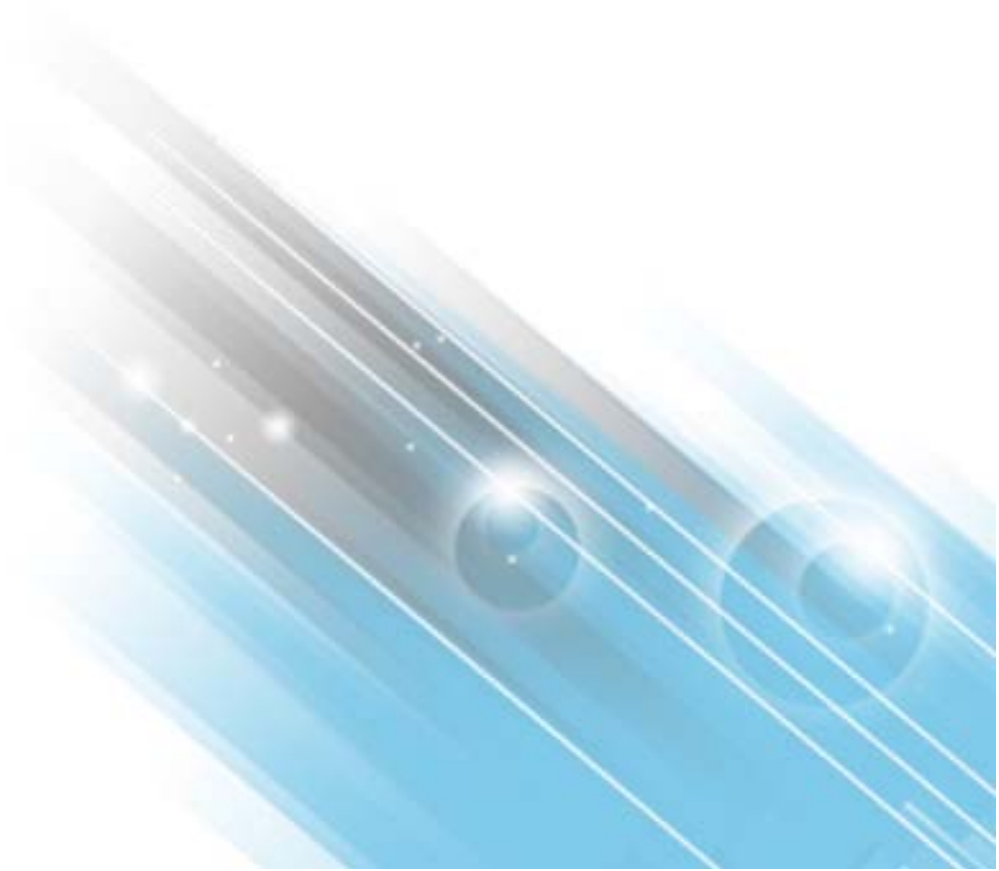


HP ArcSight Logger

Software Version: 6.1 Patch 1

Release Notes

December 17, 2015



Copyright © 2015 Hewlett Packard Enterprise Development LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://protect724.hp.com/docs/DOC-13026>

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
12/17/2015	Logger 6.1 Patch1	Patch 1 for 6.1
09/30/2015	Logger 6.1	Added support for CentOS 6.6.
09/02/2015	Logger 6.1	6.1 release.
06/25/15	Logger 6.0 Patch 2	Added Web Services API update.
06/19/15	Logger 6.0 Patch 2	Patch 2 for 6.0
11/19/14	Logger 6.0 Patch1	Patch 1 for 6.0.
09/26/14	Logger 6.0	Update for 6.0 release.
09/19/14	Logger 6.0	6.0 release.
04/24/14	Logger 5.5 Patch 1	Patch 1 for 5.5.
03/19/14	Logger 5.5	5.5 release.
05/30/13	Logger 5.3 SP1	Added new appliance platforms and Logger for VMware.
03/08/13	Logger 5.3 SP1	5.3 SP1 release.
09/27/12	Logger 5.3	5.3 GA.
01/2012	Logger 5.2 Patch 1	Patch 1 for 5.2.
12/11/11	Logger 5.2 GA	5.2 GA.

Contents

ArcSight Logger 6.1 Patch 1 Release Notes 5

 What's New in Logger 6.1 Patch 1 5

 Supported Platforms 7

 Browser Support 8

 Localization Information 9

 Logger Documentation 9

 Upgrade Paths 10

 Upgrading to Logger 6.1 Patch 1 (L7504) 11

 Known Issues 18

 Fixed Issues 18

 Open Issues 19

ArcSight Logger 6.1 Patch 1 Release Notes

These release notes provide information about the ArcSight Logger 6.1 Patch 1 (L7504) release. Logger is available in three form factors: as an appliance, as software, and as a virtualized image. Read this document in its entirety before using a Logger installed with this release.

If you have an L3XXX model Logger (an integrated Logger and Connector Appliance), refer to the Connector Appliance 6.4 documentation for additional information about the Connector Appliance functionality.

This document covers the following topics:

- [“What’s New in Logger 6.1 Patch 1” on page 5](#)
- [“Supported Platforms” on page 7](#)
- [“Browser Support” on page 8](#)
- [“Localization Information” on page 9](#)
- [“Logger Documentation” on page 9](#)
- [“Upgrade Paths” on page 10](#)
- [“Upgrading to Logger 6.1 Patch 1 \(L7504\)” on page 11](#)
- [“Known Issues” on page 18](#)
- [“Fixed Issues” on page 18](#)
- [“Open Issues” on page 19](#)

What’s New in Logger 6.1 Patch 1

The Logger 6.1 Patch 1 release (L7504) provides the same functionality as Logger 6.1 (L7491), and includes important security updates.

The following enhancements were introduced in Logger 6.1 and are included in this release. For details of these features, see the ArcSight Logger 6.1 Administrator’s Guide, available from the Protect 724 community at <https://protect724.hp.com>.

- Improved Summary page includes:
 - ◆ An enhanced look and feel.
 - ◆ Donut Charts on the summary page by default. You can change the chart type as desired. Available chart types for the summary page are donut, column and table.
 - ◆ Improved Charts that update in real time as events come in.
- Improved Search page includes:
 - ◆ The ability to select multiple fields in the search results to add them to the query.
 - ◆ The ability to expand all Raw events with one click.

- ◆ The ability to clear search filter with one click.
- Improved Search includes:
 - ◆ Case insensitive search for super-indexed fields.
 - ◆ A new Insubnet Operator that enables you to search for IP addresses using subnetting.
 - ◆ New Eval Operator functions that improve searchability.
 - ◆ Lookup file updates, including the ability to schedule automatic lookup file update.
- Improved Archiving includes:
 - ◆ The ability to index archived data, which improves query performance for existing archives.
 - ◆ An updated Event Archive page that displays Index status and Archive size.
- Improved Reporting includes:
 - ◆ A new GB / Day report.
 - ◆ Added support for ArcSight Interactive Discovery.
 - ◆ The ability to display report run parameters on the report result.
 - ◆ Report templates that have been updated to include query start and end time in header/footer.
 - ◆ A new drop-down menu for reports.
 - ◆ An improved layout of the menu options for Reports.
- Improved Dashboard page includes:
 - ◆ A new look and feel for all dashboards.
 - ◆ Dashboards that update in real time as events come in.
 - ◆ A new Event Count dashboard that displays details of received and forward events in the past day.
 - ◆ A new Monitor Dashboard that provides easy way to monitor Logger status.
- Improved Configuration options include:
 - ◆ An updated Data Volume Restrictions page that includes a color-coded bar graph that displays the last 30 days of usage.
 - ◆ The option to email yourself the Data validation result.
 - ◆ An updated license page that displays the units of ingestion in GB/day.
 - ◆ A new option to copy configuration backups to a selected location such as a USB drive, local machine, or remotely mounted file system.
 - ◆ Receivers are now enabled by default when you create them.
- Improved Administration includes:
 - ◆ A new net-SNMP implementation that provides updated SNMP polling and notifications and supports SNMP v2c, SNMP v3, and MIB II.
 - ◆ Updated Self-Signing SSL certificates that now use SHA-256.
- Improved Manageability through ArcMC includes:
 - ◆ The ability to set up and deploy multiple Loggers quickly and uniformly with Initial Configurations.
 - ◆ The ability to manage Logger peering centrally across multiple Loggers.
 - ◆ The ability to manage Logger Forwarder configuration including Logger Connector Forwarder, Logger ESM Forwarder, Logger TCP Forwarder, and Logger UDP Forwarder.

- ◆ The ability to upgrade Loggers in bulk from v6.0 to 6.1
- ◆ The ability to manage users, privileges, and roles centrally across multiple Loggers.
- ◆ The ability to monitor, report on, and create alerts for Logger usage and license entitlements.

For more information on ArcMC features and installation, refer to the ArcSight Management Center Administrator's Guide.

- Other enhancements include:
 - ◆ The maximum number of real time alerts you can enable at any time has been increased from 5 to 25.
 - ◆ Cumulative output of the ESM forwarders has been increased to 7.5K EPS.
 - ◆ Scalable distributed searches across up to 40 peers.

Supported Platforms

You can install or upgrade the Logger software on platforms with the hardware specifications and supported Operating Systems outlined below, according to the indicated deployment scenarios.

Information on how to upgrade Logger is included in these release notes.

- For information on how to install Software Logger on a Linux system or on a VMWare VM, refer to the Logger Installation Guide.
- For information on how to initialize a new Logger Appliance, refer to the Logger Installation Guide.
- For information on how to install the Trial Logger, refer to the Trial Logger Quick Start Guide.

Specification	Details
Supported Operating Systems	<p>For Logger Appliances:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux (RHEL) version 6.6 • For older LX400 series models only, RHEL 5.5 <p>For Software Loggers:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux (RHEL) versions 6.6 and 7.1 (64-bit) • CentOS versions 6.6 and 7.1 (64-bit) <p>For Logger on VMWare VM:</p> <ul style="list-style-type: none"> • CentOS version 7.1 (64-bit) <p>Note: Upgrading to Logger version 6.1 may require upgrading your Operating System (OS). If you need to upgrade your current OS as well as Logger, you must upgrade your OS first, and then upgrade Logger.</p>
CPU, Memory, and Disk Space for the Trial Logger and VM Instances	<ul style="list-style-type: none"> • CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4 - 12 GB (12 GB recommended) • Disk Space: 10 GB (minimum) in the Logger installation directory • Temp directory: 1 GB

Specification	Details
CPU, Memory, and Disk Space for the Enterprise Version of Software Logger	<ul style="list-style-type: none"> • CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12 - 24 GB (24 GB recommended) • Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data. • Root partition: 40 GB (minimum) • Temp directory: 1 GB <p>Note: Using a NFS as primary event storage is not recommended.</p>
Other Applications	<ul style="list-style-type: none"> • For optimal performance, make sure no other applications are running on the system on which you install Logger. • You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger installer on a 64-bit CentOS 7.1 configured with 12 GB RAM and four physical (and eight logical) cores. • HP ArcSight strongly recommends allocating 4 GB RAM per VM instance. • The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.

For a detailed capacity planning guide, see the Capacity Planning for Software Version of Logger document that is available for download from the Protect 724 Community at <https://protect724.hp.com>.

Browser Support

The Logger user interface (UI) is a password-protected web browser application using an encrypted HTTPS connection.

Logger 6.1 Patch 1 supports access through the following browsers:

- IE 10, IE 11
- FF ESR 39
- Chrome (current)
- Safari 8.x (on OS X 10.9)

Ensure that Logger's publicly-accessible ports are allowed through any firewall rules that you have configured.

- For root installs, allow access to port 443 as well as the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.
- For non-root installs, allow access to port 9000 as well as the ports for any protocol that the Logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.



Note

The ports listed here are the default ports. Your Logger may use different ports.

Localization Information

Localization support for these languages is available for this release:

- Japanese
- Traditional Chinese
- Simplified Chinese

You can either install Logger in one of the above languages as a fresh install or upgrade an existing English installation to one of these languages. The locale is set when you first install Logger. Once set, it cannot be changed.

Known Limitations

The following are the currently known limitations in the localized versions of Logger:

- A Logger running on L3XXX model does not support the integrated Connector Appliance functionality in the localized language.
- Only ASCII characters are acceptable for full-text search and the Regex Helper tool. Therefore, full-text search is not supported for Japanese, Simplified Chinese, or Traditional Chinese characters.
- The Login field on the Add User page does not accept native characters. Therefore, a Logger user cannot have a login name that contains native characters.
- Reports are localized for Japanese only.
- The Report Parameter and the Template Style fields do not accept native characters.
- Some Logger user interface sections are not localized. For example, the following sections are available in English only:

Reboot	Network
License & Update	CIFS
NFS	RAID controller
SSL Server Certificate	Authentication
Summary	Dashboards
Field Summary (Search Results page)	

- The Certificate Alias field for ESM Destinations cannot contain native characters. Use only ASCII characters in the Certificate Alias field. (To open the Certificates page, type Certificates in the **Take me to...** search box, and click **Certificates** in the dropdown list.)

Logger Documentation

In addition to these Release Notes, the following documentation is available for the Logger 6.1 release. These:

Logger Online Help: Integrated in the Logger product and accessible through the user interface. Click the **Options > Help** link on any Logger user interface page to access context-sensitive Help for that page. This information is also accessible from the Logger Administrator's Guide and Web Services API Guide.

Logger Support Matrix: Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Logger Administrator's Guide: Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>. This information is also accessible from the integrated online Help.

Logger Web Services API Guide: Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>. This information is also accessible from the integrated online Help.

Logger Getting Started Guide: Applicable for new Logger Appliances. Provides information about connecting the Logger Appliance to your network for the first time and accessing it through a web browser. A printed copy of this guide is packaged with the Logger Appliance. Also available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Logger Installation Guide: Applicable for initializing the Logger Appliance and installing the Software Logger on Linux or VMware VM. Available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Trial Logger Quick Start Guide: Applicable for installing the Trial Logger and Trial Logger for VMware VM. Provides a high-level understanding of Trial Software Logger and helps you install it. This document is packaged with the Trial Logger and available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.1 Patch 1. If you need to upgrade from a version of Logger earlier than 6.0, refer to the release notes for that version or contact HP Support. For more information about upgrade paths to earlier versions, refer to the Logger Support Matrix and the Release Notes for that version.



Note

To determine your current Logger version, hover the mouse pointer over the ArcSight logo in the upper left of the screen.

Upgrade Paths	
You can upgrade to Logger 6.1 Patch 1 from	Logger 6.1 (L7491) Logger 6.1 with Logger Hot Fix 14898
Operating System Upgrades	<ul style="list-style-type: none"> Make sure that your Logger is on a supported Operating System (OS). The OS your Logger is running on may vary. Be sure to check the OS version and upgrade the OS to a supported version if necessary, before upgrading Logger. For older Logger Appliances only, if your instance of Logger is on RHEL5.5, do not upgrade the OS. See "Supported Platforms" on page 7 for a list of supported Operating Systems.

Upgrading to Logger 6.1 Patch 1 (L7504)

This section includes upgrade information for the Logger Appliance, Software Logger, and Logger on VMWare VM.

- “Verifying Your Upgrade Files” on page 11
- “Logger Appliance” on page 11
- “Software Logger and Logger on VMWare VM” on page 12



Be sure to review the “Known Issues” on page 18, “Fixed Issues” on page 18, and “Open Issues” on page 19, before upgrading your Logger.

Note

Verifying Your Upgrade Files

HP provides a digital private key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

Logger Appliance

Please read the prerequisites carefully, as they have changed.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Back up your configuration before and after upgrading to this release. For instructions on backing up your Logger configuration, refer to the Logger Administrator’s Guide for the Logger version you are currently running.
- Depending on the Operating System (OS) your appliance is currently running on, you may need to upgrade your OS before you upgrade Logger. (An OS upgrade file is included in your upgrade package.)

Be sure to check the OS version before upgrading Logger:

- ◆ If your instance of Logger is on RHEL 6.1, 6.2, or 6.5, upgrade the OS before upgrading Logger. (Logger 6.1 include an OS Upgrade file for this purpose.)
- ◆ If your instance of Logger is on RHEL 5.5, do not upgrade the OS.
- Download the upgrade files from the HP Customer Support site at <https://softwaresupport.hp.com> to a computer from which you connect to the Logger UI.



Logger documentation is no longer included in your download package. Instead, you can download your documentation from the ArcSight Product Documentation community at <https://protect724.hp.com>.

Note

- ◆ For local upgrades and remote upgrades using ArcMC, download the following file:

Logger-7504.enc

- ◆ For OS upgrades, download the following file:

osupgrade-logger-rhel66-<timestamp>.enc

- Verify that you have the correct upgrade files, as described in ["Verifying Your Upgrade Files" on page 11](#).

Upgrade Instructions

To upgrade Logger Appliances remotely through ArcMC:

- 1 Upgrade your OS if necessary.
 - ◆ If your instance of Logger is on RHEL 5.5, do not upgrade the OS.
 - ◆ If your instance of Logger is on RHEL 6.1, 6.2, or 6.5, deploy the OS upgrade by using the file osupgrade-logger-rhel66-<timestamp>.enc and following the instructions in the ArcSight Management Center Administrator's Guide.
- 2 Deploy the Logger upgrade by using the file Logger-7504.enc and following the instructions in the ArcSight Management Center Administrator's Guide.

To upgrade a Logger Appliance locally:

- 1 Log into Logger and click **System Admin | System > License & Update**.
- 2 Depending on the OS your appliance is currently running on, you may need to upgrade your OS before you upgrade Logger.
 - ◆ If your instance of Logger is on RHEL 5.5, do not upgrade the OS.
 - ◆ If your instance of Logger is on RHEL 6.1, 6.2, or 6.5, browse to the osupgrade-logger-rhel66-<timestamp>.enc file you downloaded previously and click Upload Update. This will upgrade the OS to RHEL 6.6.

The ArcSight Appliance Update page displays the update progress. Once the upgrade is complete, Logger reboots automatically.
- 3 Browse to the logger-7504.enc file you downloaded in the previously and click **Upload Update**.

The ArcSight Appliance Update page displays the update progress. Once the upgrade is complete, Logger reboots automatically.



Note

If prompted to upload a license and set the time zone at this stage, contact HP Support for assistance.

Software Logger and Logger on VMWare VM

Please read the prerequisites carefully, as they have changed.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Back up your configuration before and after upgrading to this release. For instructions on backing up your Logger configuration, refer to the Logger Administrator's Guide for the Logger version you are currently running.

- Depending on the OS Logger is running on, you may need to upgrade your OS to a supported version before upgrading Logger. For a list of supported Operating Systems, see [“Supported Platforms” on page 7](#).



Remote OS upgrade is not supported for Software Logger. If OS upgrade is required for your Logger upgrade, perform the OS upgrade manually before upgrading Logger.

- Download the Software Logger upgrade file from the HP Customer Support site at <https://softwaresupport.hp.com>.

- ◆ For remote upgrades using ArcMC, download the following file:

`logger-sw-7504-remote.enc`

- ◆ For local upgrades, download the following file:

`ArcSight-logger-6.1.0.7504.1.bin`



Logger documentation is no longer included in your download package. Instead, you can download your documentation from the ArcSight Product Documentation community at <https://protect724.hp.com>.

- Verify that you have the correct upgrade file, as described in [“Verifying Your Upgrade Files” on page 11](#).
- Increase the user process limit on the Logger's OS as described in [“Increasing the User Process Limit” on page 13](#).

Increasing the User Process Limit

Before installing or upgrading Logger, you must increase default user process limit while logged in as user *root*. This ensures that the system has adequate processing capacity.



This change is only necessary when installing Software Logger on your own Linux system. It has already been done for Logger on VMWare VM.

To increase the default user process limit:

- 1 Open the file `/etc/security/limits.d/<NN>-nproc.conf`. (`<NN>` is 90 for RHEL or CentOS 6.6 and 20 for RHEL and CentOS 7.1.)
 - ◆ If you do not already have a `/etc/security/limits.d/<NN>-nproc.conf` file, create one (and the `limits.d` directory, if necessary).
 - ◆ If the file already exists, delete all entries in the file.
- 2 Add the following lines:

*	soft	nproc	10240
*	hard	nproc	10240
*	soft	nofile	65536
*	hard	nofile	65536



Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system runtime errors.

- 3 Reboot the machine.
- 4 Run the following command to verify the new settings:


```
ulimit -a
```
- 5 Verify that the output shows the following values for "open files" and "max user processes":


```
open files          65536
max user processes  10240
```

After you increase the user process limit, you will be able to upgrade Logger.

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger.

- To upgrade Logger remotely, see ["To upgrade Software and VMWare Loggers remotely through ArcMC:" on page 14.](#)
- To upgrade Software Logger locally, see ["To upgrade Software Logger:" on page 14.](#)
- To upgrade Logger on VMWare locally, see ["To upgrade Logger on VMWare VM:" on page 16.](#)

To upgrade Software and VMWare Loggers remotely through ArcMC:

- 1 Upgrade your OS to a supported version before upgrading Logger, if needed. For a list of supported Operating Systems, see ["Supported Platforms" on page 7.](#) Be sure to shut down Logger while you are upgrading the OS.



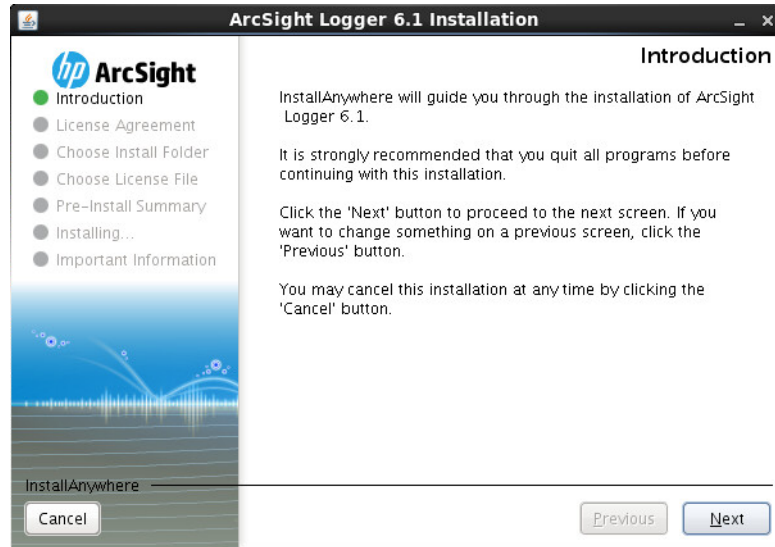
Remote OS upgrade is not supported for Software Logger. If OS upgrade is required for your Logger upgrade, perform the OS upgrade manually before upgrading Logger.

- 2 Deploy the downloaded upgrade file, logger-sw-7504-remote.enc, by following the instructions in the ArcSight Management Center Administrator's Guide.

To upgrade Software Logger:

- 1 Upgrade your OS to a supported version before upgrading Logger, if needed. For a list of supported Operating Systems, see ["Supported Platforms" on page 7.](#) Be sure to shut down Logger while you are upgrading the OS.
- 2 Log in with the same user name as the one used to install the previous version of Logger.
- 3 Run these commands from the directory where you copied the Logger software:


```
chmod +x ArcSight-logger-6.1.0.7504.1.bin
./ArcSight-logger-6.1.0.7504.1.bin
```
- 4 The installation wizard launches, as shown in the following figure. This wizard also upgrades your Software Logger installation. Click **Next**.



You can click **Cancel** to exit the installer at any point during the upgrade process.



Do not use the Ctrl+C to close the installer. If you use Ctrl+C to exit the installer and then uninstall Logger, uninstallation may delete your /tmp directory.

- 5 The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the "I accept the terms of the License Agreement" button.
- 6 Select **I accept the terms of the License Agreement** and click **Next**.
- 7 If Logger is currently running on this machine, an Intervention Required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the upgrade, or click **Quit** to exit the installer.

If you click Continue, the installer stops the running Logger processes and checks for other installation prerequisites. Once all Logger processes are stopped and the checks complete, the next screen is displayed.
- 8 Navigate to or specify the location where you want to install Logger. By default, the /opt directory is specified.
- 9 If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Click **Back** to specify another location or **Quit** to exit the installer.
- 10 If Logger is already installed at the location you specify, a User Intervention message is displayed telling you that the selected directory already contains an installation of Logger, and asking if you want to upgrade.
- 11 Click **Upgrade** to continue or **Back** to specify another location.



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

- 12 Review the pre-install summary and click **Install**.

Installing the upgrade may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

- 13 Click **Next** to initialize Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.

- 14 Click **Next** to configure Logger.

Configuration may take a few minutes. Please wait. Once the configuration is complete, Logger starts up and the next screen is displayed.

- 15 Click **Done** to exit the installer.

- 16 You can now connect to the upgraded Logger.

To upgrade Logger on VMWare VM:

- 1 Upgrade your OS to a supported version before upgrading Logger, if needed. Be sure to shut down Logger while you are upgrading the OS. For a list of supported Operating Systems, see ["Supported Platforms" on page 7](#).

- 2 Log in with the same user name as the one used to install the previous version of Logger.

- 3 Run these commands from the /opt/arcsight/installers directory:

```
chmod +x ArcSight-logger-6.1.0.7504.1.bin
./ArcSight-logger-6.1.0.7504.1.bin
```

- 4 The installation wizard launches in command-line mode, as shown below. Press **Enter** to continue.

```
Introduction
-----
```

```
InstallAnywhere will guide you through the installation of
ArcSight Logger 6.1 Patch 1.
```

```
It is strongly recommended that you quit all programs before
continuing with this installation.
```

```
Respond to each prompt to proceed to the next step in the
installation. If you want to change something on a previous
step, type 'back'.
```

```
You may cancel this installation at any time by typing 'quit'.
```

```
PRESS <ENTER> TO CONTINUE:
```

- 5 The next several screens display the end user license agreement. Installation and use of Logger 6.1 Patch 1 requires acceptance of the license agreement. Press Enter to display each part of the license agreement, until you reach the following prompt:

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N) :
```

- 6 Type Y and press Enter to accept the terms of the License Agreement.

You can type quit and press Enter to exit the installer at any point during the installation process.

- 7 The installer checks that installation prerequisites are met. If a check fails, it displays a message. You will need to fix the issue before proceeding. For example, if Logger is currently running on this machine, an Intervention Required message is displayed. In that case, type `Y` and press enter to stop all current Logger processes and proceed with the installation, or type `quit` and press Enter to exit the installer. Once all checks complete, the next screen is displayed.
- 8 The Choose Install Folder screen is displayed. Type the installation path for Logger and then press Enter.

The installation path on the VM image is `/opt/arcsight/logger`. You must use this location. Do not specify a different location.
- 9 Type `Y` and press Enter to confirm the installation location.
- 10 If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Type `quit` and press Enter to exit the installer and reconfigure your VM.
- 11 Type the absolute path to the license file and then press Enter.
- 12 Review the pre-install summary and press Enter to install Logger.

Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.
- 13 **If you are logged in as root**, the following prompts will be displayed. Type responses and press Enter after each.

Field	Notes
User Name	Use the non-root user "arcsight" that comes preconfigured on your VM image.
HTTPS Port	The port number to use when accessing the Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI.
Choose if you want to run Logger as a system service.	Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone. Select this option to create a service called <code>arcsight_logger</code> , and enable it to run at levels 2, 3, 4, and 5. If you do not enable Logger to start as service during the installation process, you still do so later. For instructions on how to enable Logger to start as a service after installation, refer to the Logger Administrator's Guide.

- 14 Type the number that describes the desired locale, and pressed Enter.
- 15 Press Enter to initialize Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
- 16 Press Enter to configure storage groups and storage volume and restart Logger automatically.

Configuration may take a few minutes. Please wait. Once configuration is complete, Logger starts up and the next screen displays the URL you should use to connect to Logger.

- 17 Make a note of the URL and then press Enter to exit the installer.

Known Issues

The following known issues apply to this release.

Upgrading Containers on Integrated Connector Appliance

On models with an integrated Connector Appliance (L3X00), you should be aware of the following issues:

- Upgrading containers to SmartConnector build 6.0.1.6574 is not supported. Instead, upgrade to SmartConnector build 6.0.2.6627 or later.
- The Model and Version columns on the Hosts page display the value "Unknown". This issue exists on the local host as well as when the integrated Connector Appliance is remotely managed from another appliance, and will prevent remote appliance upgrade. To resolve these issues, upgrade Container 1 to SmartConnector build 6.0.2.6627 or later.

For instructions on how to upgrade a container, refer to the ArcSight Connector Appliance Administrator's Guide.

Kernel Warning Message During Boot

The following message is displayed during the initial startup screen of Red Hat Linux on L3500, L7500, and L7500-SAN series Loggers:

```
[Firmware Bug]: the BIOS has corrupted hw-PMU resources
```

A similar message is posted to the dmesg file. These messages do not affect the functionality or performance of Logger or the OS and can be safely ignored. For more information, refer to the HP Customer Advisory document at:

http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=4268690&docId=emr_na-c03265132

Fixed Issues

Logger 6.1 Patch 1 includes the fixes in the table below.

Analyze/Search

Issue	Description
LOG-15589	<p>When performing a distributed search for rare events across multiple peers, if one of the peer was returning results slowly, the search process could time out, causing inconsistent peer search results.</p> <p>FIX: The search process has been updated and the correct search results will now be returned.</p>
LOG-15576	<p>When you exported events from a search and the export all fields box was checked, some fields were not included in the exported .csv file.</p> <p>Fix: Fields are now correctly populated when the export all fields box is checked.</p>

Issue	Description
LOG-14538	<p>The Query Explorer did not allow you to open and edit previously saved queries containing '\' character.</p> <p>Fix: Queries containing the '\' character can now be opened and edited from the query explorer.</p>

Open Issues

Logger 6.1 Patch 1 includes the open issues listed in the following tables. Use the noted workaround where one is available.

Analyze/Search

Issue	Description
LOG-15761	<p>When "Traditional Chinese" is used for the interface language, the type of chart cannot be changed in the UI. Whichever chart type you choose, it always displays column type.</p> <p>Workaround: None at this time.</p>
LOG-15091	<p>The insubnet operator is not supported in the Advanced Search query editor.</p> <p>Workaround: To add a condition with insubnet operator, enter the search manually.</p>
LOG-15079	<p>Loading a Saved Search or Filter by using the Folder icon (Load a Saved Filter) fails if the query includes the INSUBNET operator.</p> <p>Workaround: In the text box, type \$\$\$<SavedSearchName> or \$filter\$<FilterName> and then click Saved Search or Filter in the dropdown list to load it.</p>
LOG-14896	<p>There is no visible distinction between searchable and non-searchable columns in the User Interface. When a user performs a full-text (keyword) search on raw syslog data, the search results displays the system-defined columns, such as parser, source, and sourceType, in addition to columns displaying event data. The user interface does not differentiate between fields that are system-defined, which cannot be searched, and searchable event data columns such as device, DeviceHostName, message, and so on.</p> <p>Understanding: The parser, source, and sourceType columns are system-defined and not searchable fields because they contain no event data.</p> <p>Workaround: While these fields are included in the search results with no immediately visible distinction, they are not highlighted when you hover over them, while searchable terms are highlighted. So, to tell if a field is searchable, hover your pointer over it. If it becomes highlighted, it is searchable, if it does not, you cannot search on that term. These differences are discussed in the Searching and Analyzing Events chapter of the Search Logger administrator's Guide.</p>
LOG-14814	<p>Null values are not included in the Search results. For example, when performing a search on event data such as "NOT deviceCustomString1=bar", the search returns results that match deviceCustomString1 not equal to "bar", but does not return events where the deviceCustomString1 value is NULL.</p> <p>Understanding: With Logger's out-of-box configuration, you must explicitly call out NULL values with <field> IS NOT NULL or <field> IS NULL.</p> <p>Workaround: Logger can be configured to make NOT search conditions include NULL values. This implementation is available through Customer Support.</p>

Issue	Description
LOG-13046	<p>When you export search results on a localized Logger, there can be gibberish strings in the exported CSV file, if you open it in the English version of Microsoft Excel.</p> <p>Understanding: This can happen if Excel does not detect the correct character encoding of the CSV file.</p> <p>Workaround: In order to display the localized characters in the exported CSV file in Microsoft Excel correctly, import the CSV as follows:</p> <ol style="list-style-type: none"> 1. Launch Excel. 2. Click the Data tab. 3. Click "From Text" in the "Get External Data" menu to import a CSV file to open the Text Import Wizard. 4. Select the exported CSV file and click the Import button. 5. In the Text Import Wizard, make sure that: <ol style="list-style-type: none"> a. In the File Origin dropdown, select UTF-8. b. Under Delimiters, check Comma. c. In the Text Qualifier dropdown, select " (double quote). 6. Follow the Wizard to finish the import. <p>For more details of how to import in Excel, please refer to this page: http://office.microsoft.com/en-us/excel-help/import-or-export-text-txt-or-csv-files-HP010099725.aspx#BMimport_data_from_a_text_file_by_openi</p>
LOG-12524	<p>If the value for a discovered field contains a colon, the query generated by clicking on it will escape the colon, even though it should not.</p> <p>Workaround: Remove the backslash from in front of the colon. For example, if the query inserted by the clicking on the field is "IdentityGroup=IdentityGroup\All", then after removing the backslash, the query becomes "IdentityGroup=IdentityGroup:All".</p>
LOG-12290	<p>When searching Logger with a query that includes the rename operator, the original field renamed by the operator is still displayed as a column in the search results, but will not have any values, if the original field name is included in the Fieldset used in the search.</p> <p>For example, if the search uses the All Fields field set, which has deviceEventClassId, and its query includes "rename deviceEventClassId as eventCID", then both deviceEventClassId and eventCID will be shown in the search results but deviceEventClassId will be empty and only eventCID will show the values of deviceEventClassId.</p> <p>Workaround: Since this issue is caused by the fields included in the Fieldset used for the search, remove any renamed fields from the Fieldset.</p>
LOG-11957	<p>If you have events stored on one Logger and forward them to another Logger at a later date, you cannot use search to match the events being forwarded. This is because Logger uses different timestamps for forwarding and searching.</p> <p>Workaround: None at this time. We have added some information about the different time stamps to the Logger Administrator's guide.</p>
LOG-11299	<p>If you uncheck the Rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail.</p> <p>Workaround: The Rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.</p>

Issue	Description
LOG-11225	<p>When using the auto complete feature on the Search page, if the query has a double quote followed by bracket (i.e. "[]), the query inserted by the auto complete cannot be executed because of incorrectly escaped quotes and backslashes.</p> <p>Workaround: Remove the backslash followed by a double quote on both sides of the string. For example, if the query inserted by the auto complete is "\"[/opt/mnt/soft/logger_server.log.6] successfully.\"\"", then after removing them, the query becomes "[/opt/mnt/soft/logger_server.log.6] successfully."</p> <p>This workaround can be also used when double quote is followed by any special character such as "\", "/", "[", "]", or ",.</p>
LOG-10126	<p>When using the replace operator, if the "from" string is included in the replacement string, the "from" string will be replaced twice. For example, the following command, when run against the data "john smith" will result in "johnnyny smith":</p> <pre> replace "**john*" with "**johnny"</pre> <p>Workaround: None available at this time.</p>
LOG-9420	<p>When using the search term "transaction" on data that was received out of order, the duration may appear to be negative.</p> <p>Workaround: Include the term "sort _eventTime" before the transaction term.</p>
LOG-9025	<p>When running Logger from an ESM console, a Logger quick search using One-Time Password (OTP) in the embedded browser fails after the Logger session has been inactive for 'Logger Session Inactivity Timeout'. The default timeout is 15 minutes.</p> <p>Workaround: Use an external browser to see results.</p>
LOG-8751	<p>When search results are exported, the "Fields" field may be empty. This situation does not occur consistently.</p> <p>Workaround: To export the "Fields" field correctly when this happens, select All Fields in the "Fields" fieldset on the Search Results page. Then click Export Results.</p>
LOG-8076	<p>The Regex Helper tool does not support native characters, such as Traditional Chinese characters.</p> <p>Workaround: None at this time.</p>
LOG-7864	<p>The time in the deviceReceiptTime, startTime, endTime, and agentReceiptTime fields is not in human readable format when exported.</p> <p>Understanding: Logger records time field values in UNIX epoch format (long values).</p> <p>Workaround: Use an epoch formula in Excel to convert the time value from epoch time.</p>
LOG-7651	<p>On the Internet Explorer browser, data is truncated in the Advanced Search calendar popup window. This issue affects users' ability to select a date using the date picker (icon) when setting CCE rules in the Advanced Search feature. When a user clicks the date picker, the calendar widget that comes up is not wide enough to display the full calendar content, truncating columns with the latter days of the week.</p> <p>Workaround: Use the Tab key to scan along the part of the calendar that is initially hidden, then use Shift+Tab to scan back in the other direction. Alternatively, use another browser, such as Firefox.</p>

Issue	Description
LOG-7099	<p>When values for user 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> <p>Workaround: Disable the multi-line feature by adding the following properties to /user/logger/logger.properties. The following examples use the default values.</p> <p>To turn on/off multiline support, use:</p> <pre>search.multiline.fields.supported=true</pre> <p>To turn on/off \n and \t support, use:</p> <pre>search.double.backslash.newlines.supported=false</pre> <p>To turn on/off DOS/Windows path support for CEF and/or syslog, use:</p> <pre>search.keep.windows.path.cef=true search.keep.windows.path.syslog=true</pre>
LOG-7046	<p>The time displayed on the histogram might not match the event time. This can happen when the /etc/localtime file is not symbolically linked to the correct time zone.</p> <p>Workaround: Make sure that the /etc/localtime file is symbolically linked to the correct time zone in the /usr/share/zoneinfo file as shown in the following example. Then, restart the system.</p> <pre>sudo ln -s /usr/share/zoneinfo/<timezone> /etc/localtime</pre>
LOG-6965	<p>When the time change due to the start of Daylight Savings Time (DST) takes place in the spring, and time is set ahead one hour, the following issues are observed:</p> <ul style="list-style-type: none"> - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket. - Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram. - If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results. <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p>
LOG-6273	<p>When search results are exported, the time elapsed to export the events is not displayed.</p> <p>Workaround: For the search elapsed time, please refer to the elapsed time shown in the stats on the search page.</p>
LOG-5958	<p>When a field is removed from the Selected Fields list in the Customize FieldSet Editor, the field might not be displayed in the available fields list.</p> <p>Workaround: This only happens if you use the <- arrow to remove the field. If you double click on it, it will go back to the correct list.</p>

Issue	Description
LOG-5181	<p>Search results are not highlighted when there are multiple values that match the IN operator in a query.</p> <p>Workaround: None at this time. Highlighting works if there is only one item in the square brackets. As soon as there is more than one, no highlighting occurs.</p>
LOG-4775	<p>The user interface for the Advanced Search link (on the Search page) to create a query is not intuitive about how to enter a keyword (full-text) term.</p> <p>Understanding: To specify a keyword (full-text search), use the fullText field under the Name column. This field is displayed at the bottom of the pane.</p> <p>Workaround: If you do not see the full-text search field, scroll down.</p>
LOG-4329	<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: Search for the term/word that precedes the equal to (=) character in the event followed by the IP address or MAC address For example: search for "SRC=192.168.10.153" when looking for 192.168.10.153 and "DST=192.168.10.255" when looking for 192.168.10.255. Alternatively, you could run these data through a SmartConnector to convert to CEF format. Then run either a full-text or field-based search.</p>

Configuration

Issue	Description
LOG-15905	<p>The Logger Config Backup file has the format: <date>_<time>.configs.tar.gz. When the locale is set to Chinese Traditional, the <date> contains Chinese characters, which make scp command fail if you use scp only in target backup server for secure copy.</p> <p>Workaround: Use openSSH for Config Backups.</p>
LOG-14650	<p>You cannot re-export a filter that has been previously imported. If you try to export such a filter, the export fails and Logger will display the following message: "There was an error saving your changes: com.arcsight.logger.distributed.RemoteArcSightException: Remote exception (com.arcsight.logger.common.persist.PersistenceException: Path to root could not be found for resource <FilterName>)".</p> <p>Note: This issue affects only Filters, but does not affect other export contents such as Alerts, Saved Searches, or Dashboards.</p> <p>Workaround: None at this time.</p>
LOG-11176	<p>When you enable a receiver, Logger does not validate the RFS mount it references.</p> <p>Workaround: Make sure the RFS mount is valid by clicking edit button for this receiver. Alternatively, check the mount on the System > Admin Remote File Systems page.</p>

Issue	Description
LOG-10605	<p>The Source Types tab (Configuration > Source Types) is not visible for non-admin users.</p> <p>Workaround: Add 'Read Only Default Admin Group' privileges to the user.</p>
LOG-10581	<p>If you delete a parser that has an associated Source Type and is being used by a Folder Follower Receiver, no warning message is displayed indicating the dependency.</p> <p>Workaround: None at this time.</p>
LOG-10090	<p>You can only download 40K events per hour using the Web Service API on Logger 5.1.</p> <p>Workaround: None at this time.</p>
LOG-10056	<p>You may see a duplicate device name if a receiver was removed and a new one was created with the same name as old one. When you search on this device, Logger uses the old device and you will not be able to search on the new device.</p> <p>Workaround: To avoid this problem, do not create receivers with same names as any deleted receivers.</p>
LOG-9658	<p>If you have already increased your storage volume to the maximum limit allowed by your license, and you attempt to increase the volume further, the error message displayed is incorrect. Instead of notifying you that you have reached the limit of your license the message says, "Sufficient free space is not available to increase the storage volume size. To restore normal Logger operation, click Restart."</p> <p>Workaround: Click Restart. No further action is required. However, if you need to increase the storage limit, please contact HP Support.</p>
LOG-8790	<p>When forwarding alerts to SNMP, if the community string contains non-ASCII characters, the SNMP trap sent out displays "???" in the community field.</p> <p>Understanding: This is a display issue and does not affect SNMP authentication on Logger.</p> <p>Workaround: Avoid using non-ASCII characters in the community string.</p>
LOG-8194	<p>After restoring Logger from a backup configuration, the CIFS share failed to mount because the user name and password fields are empty.</p> <p>Workaround: Edit the setting of the CIFS share and re-enter the username and password.</p>
LOG-6786	<p>Events may be missed when a receiver on Logger is disabled.</p> <p>Workaround: None at this time.</p>
LOG-6209	<p>If the Finished Tasks page (Configuration > 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>
LOG-5024	<p>If the system that Logger backs up its configuration to is reinstalled or its SSH hosts key is changed, the Configuration Backup fails because the SSH hosts key cannot be refreshed from the Logger UI.</p> <p>Workaround: Log in to the Command Line Interface and delete the entry in the /home/arcsight/.ssh/known_hosts file. Then refresh the Configuration Backup configuration.</p>

Issue	Description
LOG-4986	<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 (powered down).</p> <p>Workaround: If there is an improper tear-down of a peering relationship and you need to reestablish it, delete the existing peer information from the peer Loggers before re-initiating the relationship.</p>
LOG-4885	<p>If you open the Certificates page and delete a certificate, After a certificate is deleted, the deleted certificate is still displayed in the list, leading to an impression that the certificate is still loaded on the system.</p> <p>To open the Certificates page, type "Cer" in the Take me to search box, and click Certificates in the list.</p> <p>Workaround: Refresh the page to update the list. The deleted certificate is no longer displayed in the list.</p>
LOG-3156	<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>Workaround: None at this time. The feature assumes that importing Logger has the same configuration setup as the exporting Logger.</p>
LOG-2941	<p>The type associated with imported filters cannot be changed from shared to saved search.</p> <p>Workaround: Imported filter types cannot be changed. However, you can copy the filter definition and create a new filter out of it.</p>
LOG-370	<p>The Configuration Backup (Configuration > Configuration Backup > Name_of_Backup) and File Transfer Receivers (Configuration > Receivers) may 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.</p>

Connector Appliance

Issue	Description
LOG-15108	<p>On Loggers with embedded Connector Appliances, the Help link on the Connector Appliance page goes to 404 Page Not Found.</p> <p>Workaround: For help on the embedded Connector Appliance, open the help from any Logger page and navigate to appropriate section of the Managing Connectors or Managing Repositories chapter, or search for the help you need. Alternatively, refer to the appropriate section of the Logger Administrator's guide, available for download from the Protect 724 Community at https://protect724.hp.com.</p>

Issue	Description
LOG-12658	<p>When using Internet Explorer 11 to access Connectors on a Logger L3x00 appliance, there is a display issue when you add ten or more rows to the extra mappings table on the parser page of the Flex Connector Wizard. In that case, the Event Field drop-downs may not be properly aligned within the table if you scroll down the page.</p> <p>Workaround: Since this issue occurs when scrolling down the page, maximize the window to prevent the need to scroll.</p>
LOG-12339	<p>The EPS IN/OUT values for connectors may be displayed as "unknown" in the list of Connectors on the Container page.</p> <p>Workaround: Click the connector in the list to open the Connector's page. That will ping the connector. Click the container to go back to the list and the EPS IN/OUT values should be reflected.</p>
LOG-11731	<p>Emergency Restore places the local connector in the wrong location. Therefore, the old local connector is never overwritten with the new connector information and emergency restore operation fails. The connector still points to old connector version.</p> <p>Workaround: Please contact HP Support for help with this issue.</p>

Dashboards

Issue	Description
LOG-14156	<p>On Internet Explorer, the bottom of the Monitors Dashboard does not always render properly.</p> <p>Workaround: To avoid this rendering problem when viewing the Monitors Dashboard, maximize the Internet Explorer window.</p>
LOG-13161	<p>After an upgrade, some dashboard graphs would only display data for seven days even when you selected to display data for a longer period. For example, if you selected the CPU usage graph for a period of 30 days, you only see data in the graph going back one week.</p> <p>Workaround: None at this time.</p>
LOG-11730	<p>When there are two or more Dashboards with the same name, after you select one of them from the Dashboard dropdown, there is no way to show the other from the dropdown. This is because when you select one of the dashboards with the same name, the dropdown thinks the first entry of those dashboards is always selected.</p> <p>Workaround: Rename the other dashboards so that they all have different names.</p>
LOG-9332	<p>In the Firefox browser, when the Monitor graph panel is not wide enough to show the entire graph in the Monitor or Custom Dashboards, the graph is cut off and no scroll bar is shown in the panel. In the Internet Explorer browser, the panel is blank.</p> <p>Workaround: For the Monitor Dashboard, make the browser window wider. For Custom Dashboards, make the browser window wider or change the layout of the panels so that each graph panel will have enough width to show the graph. For example, If the row including a Monitor graph panel has 3 panels, move at least one of the other panels to the other row.</p>

General

Issue	Description
LOG-15501	<p>After adding a second hard drive to the VMware template by following the directions in the install guide, when you go into CentOS 7.1, hard drive is not recognized.</p> <p>Workaround: Run following commands on the virtual machine console after the second disk is added.</p> <p>Note: In the following commands, replace "ARCSIGHT_HOME" with the path where logger software is going to be installed. Make a note of this location. When you run the Logger installer be sure to use it.</p> <ol style="list-style-type: none"> 1 Run the parted tool. <code>root@logger ~]# parted /dev/sdb</code> 2 Attach a label to the disk. <code>mklabel gpt</code> 3 Make an xfs partition utilizing the whole capacity of the drive. <code>mkpart primary xfs '0%' '100%'</code> 4 Exit parted. <code>q</code> 5 Create xfs file system and assign a label: <code>mkfs.xfs -L DATA /dev/sdb1</code> 6 Append following line to /etc/fstab file to mount this partition on boot: <code>LABEL=DATA ARCSIGHT_HOME/data xfs defaults,inode64 1 2</code> 7 Create a mount path. <code>mkdir ARCSIGHT_HOME/data</code> 8 Mount the file system. <code>mount -L DATA</code>
LOG-11473	<p>Initial appliance configuration, such as uploading the license, setting the locale, date/time and configuring SAN, could fail if some setup wizard are not met.</p> <p>Workaround: If needed, configure the Logger's date/time before uploading the license.</p>
LOG-8003	<p>When a search operation is run using the Web Services API and the search results contain binary data, the search operation generates the following exception: "Unexpected EOF; was expecting a close tag for element <ns1:data>".</p> <p>Workaround: None at this time.</p>

Reports

Issue	Description
LOG-15056	<p>If you install a Logger solution, such as Payment Card Solutions Guide (PCI), IT Governance (ITGov), or Sarbanes-Oxley (SOX), before you log into Logger and open the Reports page for the first time, when you then log in and open the Reports page, the Foundation, SANS Top5, and Device Monitoring report categories will be missing.</p> <p>Understanding: This happens if the Logger reports engine has not yet been initialized when the Solutions package is installed.</p> <p>Workaround: Log into Logger and open the Reports page before installing any solutions package. This information has been added to the Logger Administrator's guide and will also be included in the next versions of the PCI, ITGov, and SOX Compliance Insight Package Guides for Logger.</p>

Issue	Description
LOG-11954	<p>If the underlying Query of a Report changes, then viewing published reports will result in an error.</p> <p>Workaround: None at this time.</p>
LOG-11659	<p>In Software Loggers, the installation of multiple Solution Packages by the root user may fail if the SOX v4.0 solution package is installed before other packages.</p> <p>Workaround: If you are installing the SOX v4.0 solution package on Software Logger as the root user, install it last.</p>
LOG-11279	<p>Restoring configuration backup does not preserve the report templates original file ownership and causes report execution without proper templates.</p> <p>Workaround: Follow these steps to fix the permissions.</p> <ol style="list-style-type: none"> 1. SSH to Logger. (Appliance users should contact HP support for help with this.) <p>Note: In Logger 6.0, SSH can be enabled from navigating to System Admin > System > SSH menu item.</p> <ol style="list-style-type: none"> 2. Navigate to the following directory, <code><\$ARCSIGHT_HOME>/logger/Intellicus/reportengine/templates/adhoc</code>, where <code><\$ARCSIGHT_HOME></code> is the directory in which Logger is installed. 3. Change the owner of the report templates [files with extension .irl and .sty] files from "root" to the same non-root user that was used during Logger installation.
LOG-11137	<p>If a user has privileges to View a Published Report Only, then the report will not be visible in the Report Explorer.</p> <p>Workaround: You can find and view published reports from the Category Explorer instead. To find a published report, open the Category Explorer and navigate to the Saved Reports folder under the report's Category. (The terms "saved report" and "published report" are used interchangeably.)</p>
LOG-10098	<p>Reports display a dash (-) for null values. If this is displayed in a drill-down column, the column displays the dash as a hyperlink, which usually opens with unexpected results since '-' does not match the query.</p> <p>Workaround: None at this time.</p>
LOG-9860	<p>When you click "Copy Report" or "Copy Report as Link" icon, the UI does not give you any feedback that it was copied.</p> <p>Workaround: None at this time. Clicking Copy or Copy as Link will not give you a visual indication that anything has been copied, but you will be able to Paste, as needed.</p>
LOG-9798	<p>When the Logger Compliance Insight Package (CIP) reports such as Logger ITGov 4.0 for ISO 27002 are exported in PDF format, the saved PDF shows that Chart component with the following error: "Error: No plotters/series have been defined".</p> <p>Workaround: None at this time.</p>
LOG-9620	<p>If a distributed report fails to run in the background against fields that do not exist on the peer Logger, the error message does not clearly indicate the reason.</p> <p>Workaround: None at this time.</p>
LOG-9584	<p>After upgrading to Logger 5.2, you may see browser caching issues Reports pages. There may be errors in red in the dashboard viewer, you may not be able create widgets, and the explorers may not work.</p> <p>Workaround: Restart your browser. If that does not work, manually clear the browser cache and delete temporary files.</p>

Issue	Description
LOG-8780	<p>Reports generated using the Web Services API do not contain report titles.</p> <p>Workaround: When generating reports through the Web Services API, ensure that you have entered the Report Title in the Report Editor (otherwise you will only see the Report ID) in the generated report.</p>
LOG-7186	<p>If you limited a user's rights to a specific report template, the user was not able to run any reports at all and the following error messages were displayed when the user tried to run reports:</p> <p>90141 No matching record found: Requested Report Object "xxxxx" Not Found</p> <p>90141 No matching record found: The Query Object used as the Datasource could not be fetched from the repository</p> <p>Understanding: A user needs the right to see the parent node of the report tree in order to be able see the child node. An admin can edit permissions for individual Report folders without enabling access to levels higher on the tree. If this happens, the user cannot run or edit the reports. This issue is partially fixed. Now, when a user's permissions are set properly, the user can view the restricted reports and run them ad-hoc, but cannot schedule the restricted reports to run later.</p> <p>If a user tries to schedule a restricted report, the following error message can be displayed: "Unauthorized Operation: We're sorry, but you are not authorized for that operation"</p> <p>Workaround: Give the user global access to all reports, then the user will be able to schedule the reports as well a view and run them ad-hoc.</p>
LOG-7165	<p>The privileges for pre-built reports on Logger are missing from the Add Group page if you have not yet loaded the Reports page after installing Logger.</p> <p>Workaround: Open the Reports page. (This triggers the population of group privileges in the Add Group.) Then go back to the Add Group page. The privileges for pre-built reports will be displayed after that.</p>
LOG-6652	<p>In the Firefox browser, the Report Template editor (Reports > Design - Template Styles > Select a template > Edit Layout) is not usable because the pull-out menus cannot be resized, the drop-down menus do not display the full list of options, and some windows open behind the editor.</p> <p>Workaround: Use the Internet Explorer browser.</p>
LOG-3187	<p>The time taken to run a scheduled report is not reported correctly in the Logger user interface.</p> <p>Workaround: None at this time.</p>
LOG-2355	<p>The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.</p> <p>Workaround: None at this time.</p>
LOG-2350	<p>The default report generated by clicking the hand icon is missing the report name and date.</p> <p>Workaround: Add a Report title to the Report Header section to include the title on the first page of the Report.</p>
LOG-2012	<p>Adding a scheduled report can reset the scan limit field of other reports.</p> <p>Workaround: Check that the scan limit is set as desired before running any report.</p>
LOG-1956	<p>The time range and constraints information is not applied when accessing information from reports through the drill-down links of a scheduled published report.</p> <p>Workaround: None at this time.</p>

Issue	Description
LOG-1703	<p>When a query used in an existing scheduled report is edited to add a mandatory filter, the report does not return any output when it runs and an error is generated.</p> <p>Workaround: None at this time.</p>

Summary

Issue	Description
LOG-9772	<p>The number of events indexed as shown on the Summary page may not match the number of events found when you run a search with the same time range as shown on the Summary page.</p> <p>Understanding: The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different.</p> <p>Workaround: None at this time. Currently, there is no way to specify the search time range in milliseconds.</p>

System Admin

Issue	Description
LOG-13299	<p>For Internet Explorer 10, if you enter your password in the Login screen and then move to another tab before logging in, the some of the dots that represent your password are no longer displayed, however the password you typed is unchanged.</p> <p>Workaround: Use Internet Explorer 11, which does not have the issue.</p>
LOG-11700	<p>Users may be unable to log in after they have been removed from a group.</p> <p>Understanding: Removing all group assignments from a user effectively disables that user account. User accounts not assigned to any group will be unable to log in.</p> <p>Workaround: To avoid disabling a user account when removing the user from a group, check that the user is assigned to the correct groups.</p>
LOG-11066	<p>If the system time zone is set to /US/Pacific-New, then the software Logger will have the following issues:</p> <ol style="list-style-type: none"> 1. On the Search page, the Events grid in the search results will be empty for any search, 2. The timestamps with timezone will be shown using GMT, 3. In the Global Summary on the Summary page, the Indexing is reported one hour behind the current time stamp. <p>Workaround: Change the system time zone to something to more specific, such as /America/Los_Angeles.</p>
LOG-7664	<p>If a single-path SAN Logger Appliance is rebooted and the previously attached LUN is not available, the Logger will fail to start. In case of a multi-path SAN Logger Appliance, the Logger fails to start only if the path that was in use when the Logger was rebooted is unavailable.</p> <p>Workaround: None at this time.</p>

Upgrade

Issue	Description
LOG-15903	<p>If Logger that was installed by the root user is upgraded to 6.1 or 6.1 P1, uninstalling the upgraded Logger leaves some immutable files in place.</p> <p>Workaround: After running uninstaller, execute the following command as root:</p> <pre>chattr -R -i {Logger installation directory}</pre> <p>Then remove the whole Logger installation directory.</p>

