



Hewlett Packard
Enterprise

HPE Security ArcSight Logger

Software Version: 6.2

Release Notes

May 24, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2016 Hewlett Packard Enterprise Development, LP

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

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

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

ArcSight Logger 6.2 Release Notes	5
What's New in this Release	5
Supported Platforms	6
Browser Support	8
Logger Documentation	8
Localization Information	10
Known Limitations	10
Upgrading to Logger 6.2 (L7633)	11
Upgrade Paths	11
Verifying Your Upgrade Files	12
Logger Appliance	12
Prerequisites	12
Upgrade Instructions	13
L3XXX Only: Migrating Connector Appliance Data to ArcSight Management Center	14
Before Performing the Migration	14
The L3XXX Migration Process	15
Backing Up Your Connector Appliance Data on Logger	15
Restoring Your Connector Appliance Data to ArcMC	16
Note: Repositories and Data Backup	17
Software Logger and Logger on VMWare VM	17
Prerequisites	17
Upgrade Instructions	18
Known Issues	23
Kernel Warning Message During Boot	23
Fixed Issues	24
Analyze/Search	24
Configuration	24
Dashboards	25

General	26
Reports	27
System Admin	28
Upgrade	28
Open Issues	29
Analyze/Search	29
Configuration	33
Dashboards	35
General	36
Localization	41
Reports	41
Summary	43
System Admin	44
Send Documentation Feedback	45

ArcSight Logger 6.2 Release Notes

These release notes provide information about the ArcSight Logger 6.2 (L7633) 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.

This document covers the following topics:

- ["What's New in this Release" below](#)
- ["Supported Platforms" on the next page](#)
- ["Browser Support" on page 8](#)
- ["Localization Information" on page 10](#)
- ["Logger Documentation" on page 8](#)
- ["Upgrade Paths" on page 11](#)
- ["Upgrading to Logger 6.2 \(L7633\)" on page 11](#)
- ["Known Issues" on page 23](#)
- ["Fixed Issues" on page 24](#)
- ["Open Issues" on page 29](#)

What's New in this Release

This section lists the new features and enhancements introduced in the HPE Security ArcSight Logger 6.2 release (L7633). This release supports the L7600 line of Logger Appliances, with enhancements of scale, performance, and security. This release also marks the first step towards the convergence of Logger, ArcSight Management Center (ArcMC), and ArcSight SmartConnectors into a more integrated ArcSight Data Platform (ADP).

Note: Logger version 6.2 does not support integrated Connector Appliances. See ["L3XXX Only: Migrating Connector Appliance Data to ArcSight Management Center" on page 14](#) for information on how to migrate your Connector Appliance data to ArcSight Management Center.

The following new features and enhancements are included in this release.

Improved Performance

The search speed of the Logger L7600 Appliance is significantly improved over the L7500:

- Super-indexed search is 49% faster
- Indexed search is 32% faster

- Keyword search is 27% faster

Chart Operator search speed is now 1500% faster running on the ArcSight L7500:

- 5 million events—from 20 minutes to 10 seconds
- 355 million events—from nearly 5 hours to 19 minutes

Improved scale

- Storage capacity increased from 8 TB to 12 TB per instance
- Super-indexed search maximum partition size increased to accommodate 12 TB

Enhanced Encryption

- Logger L7600 Appliances support RAID-level encryption with no performance impact
- Encrypted Appliances support data migration

Other Features

- All ESM fields now available in Logger field sets
- Content override option
- Migration support for Connector Appliance data to ArcMC for L3X00 appliances.
- Forced initial password change
- Digitally signed reports
- Updated CIPs Packages for PCI 4.0 and ITGov
- Improved Reports performance
- Support for Federal Information Processing Standard (FIPS)

For details about these features, see the ArcSight Logger 6.2 Administrator's Guide, available from the ArcSight Product Documentation Community on [Protect 724](#).

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>L7600 series Logger Appliances:</p> <ul style="list-style-type: none"> Red Hat Enterprise Linux (RHEL) version 7.1 <p>L7500 and L3500 Logger Appliances:</p> <ul style="list-style-type: none"> Red Hat Enterprise Linux (RHEL) version 6.7 <p>For Software Loggers:</p> <ul style="list-style-type: none"> Red Hat Enterprise Linux (RHEL) versions 6.7 and 7.1 (64-bit) CentOS versions 6.7 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 6.2 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. For Logger Appliances, an OS upgrade file is included in your upgrade package.</p>
CPU, Memory, and Disk Space for 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
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 network file system (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.

Specification	Details
	<ul style="list-style-type: none">• 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 a minimum of 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.

Browser Support

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Logger 6.2 supports access through the following browsers:

- Chrome (current)
- Edge (on Windows 10)
- Firefox 41, ESR 38.3.0
- Internet Explorer 11
- Safari 9.0.1 (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.

Logger Documentation

In addition to these Release Notes, the following documentation is available for the Logger 6.2 release.

Logger 6.2 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 available in PDF format from the Logger Administrator's Guide and Web Services API Guide.

ArcSight Data Platform Support Matrix (formerly the Logger Support Matrix): Provides integrated support information such as upgrade, platform, and browser support for Logger, ArcMC, and relevant SmartConnectors. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).

Logger 6.2 Administrator's Guide: Provides information on how to administer and use Logger. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). This information is also accessible from the integrated online Help.

Logger 6.2 Web Services API Guide: Provides information on how to use Logger's web services. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). This information is also accessible from the integrated online Help.

Logger Getting Started Guide: Applicable for Logger Appliances only. Provides information about connecting the Logger Appliance to your network for the first time and accessing it through a web browser. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). Additionally, a printed copy is packaged with the Logger Appliance.

Logger 6.2 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 on Protect 724](#).

Logger 6.2 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. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).

Additional Logger documentation, including Logger data migration and best practices can be downloaded from the [ArcSight Product Documentation Community on Protect 724](#).

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:

- 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.)

Upgrading to Logger 6.2 (L7633)

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

- ["Verifying Your Upgrade Files" on the next page](#)
- ["Logger Appliance" on the next page](#)
- ["Software Logger and Logger on VMWare VM" on page 17](#)

Note: Be sure to review the sections ["Known Issues" on page 23](#), ["Fixed Issues" on page 24](#), and ["Open Issues" on page 29](#) before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.2. For more information about upgrading from a version of another model of Logger or an earlier software version, consult the Release Notes, Data Migration Guide, and Support Matrix for that version, or contact HPE Support.

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

Logger 6.2 Upgrade Paths	
Software Versions	6.1 (7491) 6.1 Patch 1 (7504)
Appliance Models	L350X L750X L750X-SAN
Operating System Upgrades	<ul style="list-style-type: none">• 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.• See "Supported Platforms" on page 6 for a list of supported Operating Systems.

Verifying Your Upgrade Files

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

Visit the following site for information and instructions:

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

Logger Appliance

Read the following prerequisites carefully before upgrading your Logger Appliance.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a Configuration Backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- If you have an L3XXX model appliance, review "[L3XXX Only: Migrating Connector Appliance Data to ArcSight Management Center](#)" on page 14.
- Check the OS version. Existing Logger Appliances should be upgraded to RHEL 6.7. If your instance of Logger is on an earlier version, upgrade the OS before upgrading Logger. (An OS upgrade file is included in your upgrade package.)
- Download the upgrade files from the HPE Customer Support site at:
<https://softwaresupport.hpe.com> to a computer from which you connect to the Logger UI.

Note: Logger documentation is not included in your download package. You can download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).

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

`logger-7633.enc`

- b. For OS upgrades, download the following file:

`osupgrade_logger_rhel67_<timestamp>.enc`

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

Upgrade Instructions

If you have an L3XXX model appliance, follow the instructions in "[L3XXX Only: Migrating Connector Appliance Data to ArcSight Management Center](#)" on the next page before performing the upgrade.

To upgrade Logger Appliances remotely through ArcMC:

1. Upgrade your OS if necessary. Logger 6.2 appliance upgrade requires RHEL 6.7. If your instance of Logger is on an earlier version, deploy the OS upgrade by using the file `osupgrade_logger_rhel67_<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
2. Deploy the Logger upgrade by using the file `logger-7633.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

To upgrade a Logger Appliance locally:

1. Log into Logger and click System Admin | System > **License & Update**.
2. Upgrade your OS if necessary. Logger 6.2 appliance upgrade requires RHEL 6.7. If your instance of Logger is on an earlier version, deploy the OS upgrade by browsing to the `osupgrade_logger_rhel67_<timestamp>.enc` file you downloaded previously and clicking **Upload Update**.
The ArcSight Appliance Update page displays the update progress. Once the upgrade is complete, Logger reboots automatically.
3. Browse to the `logger-7633.enc` file you downloaded 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 HPE Support for assistance.

4. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

L3XXX Only: Migrating Connector Appliance Data to ArcSight Management Center

Note: If you do not use the Connector Appliance for remote management of connectors on Logger L3XXX, skip this section.

Connectors can no longer be managed on L3XXX appliances. Your Connector Appliance data must be migrated to ArcSight Management Center, (also called ArcMC) 2.2 or later.

ArcMC is the successor product to Connector Appliance, which includes all the functionality of Connector Appliance and much more. You can retain all of your existing Connector Appliance data and simply migrate the data to the new ArcMC platform. However, unlike Connector Appliance, your new ArcMC will need to run on a separate host from your Logger.

Upgrading to Logger 6.2 removes all Connector Appliance and remote connector data from the appliance. It also removes the Default and Read Only Connector Appliance Rights Groups from Logger. After the upgrade, information about those groups will be logged in `upgrade.log`, but will not be in the backup file.

As part of the upgrade process, you need to migrate Connector Appliance and remote connector data (if any) from your L3XXX Logger to ArcMC) which will manage this data going forward. The following topics describe this process.

Connector Appliance data migration is supported on the following ArcMC form factors:

- Fresh install of software ArcMC version 2.2
- Upgrade to software ArcMC version 2.2
- Fresh deployment of hardware ArcMC version 2.2 (C6600)
- Upgrade to hardware ArcMC version 2.2 (C65XX)

Before Performing the Migration

Before performing your Connector Appliance and connector data migration from Logger, do each of the following.

- Download and review the ArcSight Management Center Administrator's Guide, available from the [ArcSight Product Documentation Community on Protect 724](#). The guide explains the management and administration of ArcMC in detail. Consult the Installation chapter for any prerequisites to installation.
- Download and review the ArcMC Release Notes for system requirements for installation. Ensure your new ArcMC host meets these requirements.
- Prepare a secure, appropriate, and technically sufficient host for running ArcMC 2.2 or later.

- a. For software ArcMC, following the instructions in the ArcSight Management Center Administrator's Guide and Release Notes, install ArcMC on the host.
- b. For ArcMC appliance, follow the instructions shipped with the appliance for setup of the appliance.
- From the HPE download site, download and store the following two files in a secure network location:
 - a. The script `L3XX_conapp_data_backup.sh` which performs the data backup.
 - b. The migration scripts tar file `<L3XX_Migration_Package.tar>` This tar file contains the scripts needed for data migration.

The L3XXX Migration Process

To perform the migration, you must perform these tasks:

1. Back up all of your Connector Appliance and connector data on your existing Logger L3XXX.
2. Copy the backup to your new ArcMC system, and then restore your backed-up data to the new ArcMC system.

Each of these tasks is explained in detail below.

Backing Up Your Connector Appliance Data on Logger

To back up your Connector Appliance data on Logger L3XXX:

1. In Logger, in the Connector Appliance UI, and browse to **Repositories > Backup Files > Retrieve Container Files**.
2. Choose **Local Connectors**. This saves your connector data in the repositories folder.
3. SSH to Logger and log in as user `arcsight`.
4. Copy the backup script (`L3XX_conapp_data_backup.sh`) to a directory on your Logger, such as `/home/arcsight`.
5. Run the backup script to back up your Connector Appliance data, as follows:

```
.<script_path>/L3XX_conapp_data_backup.sh
```

where `<script_path>` is the directory to which you copied the script, such as `/home/arcsight`.

Your backed-up data will be contained in a file called `backup_<L3XX_IP>_<timestamp>.tar.gz`.

Restoring Your Connector Appliance Data to ArcMC

You are now ready to run the restore script on your new ArcSight Management Center (ArcMC), which you prepared before performing the data migration. Before continuing, note the following:

- You must run the script using the same user account that was used to install ArcMC.
- Ensure that the XSLT proc libraries exist in the ArcMC installation directory. (These libraries are normally part of the OS installation.)

To run the restore script on ArcMC:

1. Log in to ArcSight Management Center with the same user account you used to install it.
2. Copy the L3XXX migration package (L3XX_Migration_Package.tar) to the ArcSight Management Center host.
3. Copy the backup file (backup_<L3XX_IP>_<timestamp>.tar.gz.) to the ArcSight Management Center host.

Untar the L3XXX migration package by executing the following command:

```
tar -xzf /<script_path>/L3XX_Migration_Package.tar
```

Where <script_path> is the directory to which you copied the script, such as /home/arcsight.

This will extract two files to the same location:

```
L3XX_conapp_data_migration_to_ArcMC.sh  
L3XX_conapp_data_migration.xsl
```

4. In the directory where you copied the restore script, enter the following command to make the script executable:

```
chmod +x L3XX_conapp_data_migration_to_ArcMC.sh
```

5. Run the restore script as follows:

```
./L3XX_conapp_data_migration_to_ArcMC.sh <ArcMC_install_dir> <backup_path>
```

Where:

- <ArcMC_install_dir> is the absolute path of the installation directory for ArcSight Management Center. For the ArcMC appliance, this is /opt/arcsight.
- <backup_path> is the absolute path of the file containing your backed-up data, backup_<L3XX_IP>_<timestamp>.tar.gz.

The script untars the backup file, backup_<L3XX_IP>_<timestamp>.tar.gz. It also stops the ArcMC web process, adds the remote configuration into ArcMC, and then restarts the web process. The restore will be in effect after the restart of the web service.

The restore process is logged to <ArcMC install directory>/userdata/logs/arcmc/L3XX_conapp_migration.log.

Note: Repositories and Data Backup

A new repository created prior to L3xxx data migration from Connector Appliance to ArcMC 2.2 will not show up in the data restored to ArcMC 2.2. (It will, however, be available if you SSH to /opt/arcsight/userdata/arcmc/repository).

The workaround is to manually create repositories with the exact same name as the ones from the old L3XXX system. After creating, the files in the repositories will automatically be loaded by the web application on system restart.

Software Logger and Logger on VMWare VM

Read the following prerequisites carefully before upgrading your Software Logger or Logger VM.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a configuration backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- Depending on the OS that Logger 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 6.

Note: 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 HPE Customer Support site at [HPE Software Support](#).

For remote upgrades using ArcMC, download the following file: logger-sw-7633-remote.enc

For local upgrades, download the following file:

ArcSight-logger-6.2.0.7633.0.bin

Note: Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).

- Verify that you have the correct upgrade file, as described in "[Verifying Your Upgrade Files](#)" on page 12.

- For Software Loggers, if not already done on the system, increase the user process limit on the Logger's OS. Refer to "Increasing the User Process Limit" section of the ArcSight Installation Guide. You do not need to do this for Logger on VMWare VM, it is already done on the provided VM.

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:" below](#).
- To upgrade Software Logger locally, see ["To upgrade Software Logger:" below](#).
- To upgrade Logger on VMWare locally, see ["To upgrade Logger on VMWare VM:" on page 20](#).

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 6](#). Be sure to shut down Logger while you are upgrading the OS.

Note: 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.

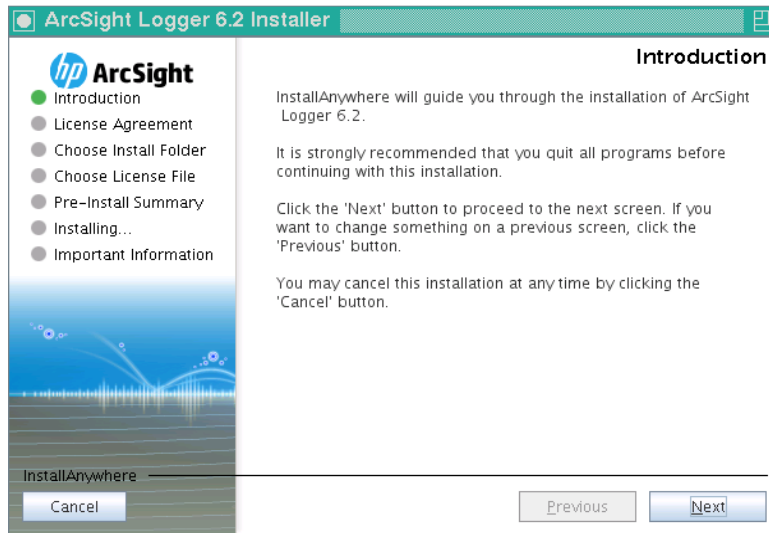
2. Deploy the downloaded upgrade file, `logger-sw-7633-remote.enc`, by following the instructions in the ArcSight Management Center Administrator's Guide.

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 6](#). 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-6.2.0.7633.0.bin  
./ArcSight-logger-6.2.0.7633.0.bin
```

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.

Caution: 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.

4. 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.
5. Select **I accept the terms of the License Agreement** and click **Next**.
6. 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.

7. Navigate to or specify the location where you want to install Logger. By default, the /opt directory is specified.
8. 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.
9. 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.

10. Click **Upgrade** to continue or **Back** to specify another location.

Note: 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.

11. 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.
12. Click **Next** to initialize Logger components.
Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
13. 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.
14. Click **Done** to exit the installer.
15. You can now connect to the upgraded Logger.
16. Make a Configuration Backup immediately after the upgrade. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

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 6](#).
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:

```
./ArcSight-logger-7633.0.XXXX.0.bin
```

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 6.2.
```

```
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:
```

The next several screens display the end user license agreement. Installation and use of Logger 6.2 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):

4. 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.

5. 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.
6. 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.

7. Type Y and press Enter to confirm the installation location.
8. 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.
9. Type the absolute path to the license file and then press Enter.
10. 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.

11. 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 arcsight_logger, and enable it

Field	Notes
	<p>to run at levels 2, 3, 4, and 5.</p> <p>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.</p>

12. Type the number that describes the desired locale, and pressed Enter.
13. Press Enter to initialize Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
14. 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 is displays the URL you should use to connect to Logger.
15. Make a note of the URL and then press Enter to exit the installer.
16. You can now connect to the upgraded Logger.
17. Make a configuration backup immediately after the upgrade. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.

Known Issues

The following known issues apply to this release.

Kernel Warning Message During Boot

The following message is displayed during the initial startup screen of Red Hat Linux on L7600, L7500, L7500-SAN, and L3500 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 operating system, and can be safely ignored. For more information, refer to the HPE Customer Advisory document:

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

Fixed Issues

The following issues are fixed in this release.

• Analyze/Search	24
• Configuration	24
• Dashboards	25
• General	26
• Reports	27
• System Admin	28
• Upgrade	28

Analyze/Search

Issue	Description
LOG-15089	<p>New filters created on the Search page were not appearing in the auto-complete list when you typed '\$filter\$<FilterName>' to show the available filters. (Filters created on the Configuration > Filters page work properly.)</p> <p>FIX: New filters created on the Search page now appear in the autocomplete list.</p>

Configuration

Issue	Description
LOG-15083	<p>An error message was appearing on the page when you closed the Edit Parser menu.</p> <p>FIX: The error message no longer displays.</p>
LOG-15052	<p>Configuration menus "Peer Loggers" and "Peer Authorizations" were listed in the Configuration Search category.</p> <p>FIX: These menus now are grouped in the Configuration Advanced category.</p>
LOG-13411	<p>When creating or editing a scheduled alert, you could select a query that contained aggregated operators (such as "chart" and "top"), which would return an error. Scheduled alerts do not support aggregated search operators.</p>

Issue	Description
	FIX: The query list now displays only queries not containing those aggregated search operators.
LOG-11771	<p>Previously, Logger scheduled reports were restricted to daily or weekly scheduling options.</p> <p>FIX: You can now schedule reports monthly by specifying the day of the month and the hour of day (in 24-hour format) when you want the report to run. Monthly scheduling is not available for all report options.</p>
LOG-8233	<p>Previously, there was no warning in the documentation that during a configuration backup, the Logger license is backed up, and may overwrite a newer license when the configuration is restored.</p> <p>FIX: The Logger Administrator's guide now clearly instructs users about this issue.</p>
LOG-6667	<p>Previously, the only backup and restore option was via Secure Copy Protocol (SCP).</p> <p>FIX: You now have the option to write a configuration backup to a thumb drive or local device. For this release however, you will still need to use SCP to restore Logger after a configuration backup.</p>

Dashboards

Issue	Description
LOG-15451	<p>After upgrading to Logger 6.1, some Dashboards were reporting that there was no data available, instead of displaying the available data correctly.</p> <p>FIX: All Dashboards display available data correctly after upgrading to Logger 6.1.</p>
LOG-15097	<p>When using Software Logger running on either RHEL 7.1 or CentOS 7.1, some graphs were not displaying, due to changes within the operating systems for Ethernet interfaces, from "eth-n" to "ens32."</p> <p>FIX: Irrespective of the network interface name, the Dashboard graphs display correctly.</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 would only see data in the graph going back one week.</p>

Issue	Description
	FIX: Logger Dashboard graphs now display more than seven days of data when a longer period is selected and the data is available.

General

Issue	Description
LOG-16105	<p>For Logger 6.2 Beta, if a user has these permissions unchecked in: Logger Rights group "View registered peers" or in Logger Search group, "Search for events on remote peers", their local query attempts may fail with a <code>java.lang.NullPointerException</code> message, even if no peers are configured.</p> <p>FIX: The permissions issues have been corrected.</p>
LOG-16092	<p>Previously, when editing a CIFS mount, Logger allowed you to include special characters in the name, which prevented the mount from appearing on the list of Remote File Systems.</p> <p>FIX: Logger now accepts only alphanumeric characters, dashes (-) and underscores (_) within the CIFS mount name field. Dashes and underscores cannot be the first character in the field.</p>
LOG-15933	<p>On Logger appliances, when logging in to the ArcSight Platform Console following a reboot, the authentication could sometimes fail, even if the correct credentials were provided.</p> <p>FIX: The ArcSight Platform Console now takes a longer time to initialize, to ensure that the Logger will be ready to process authentication requests. This matches the behavior of the ArcMC ArcSight Platform Console.</p>
LOG-15900	<p>On G8 appliances, system health events like disk/cpu/raid/fan may not be generated on the first boot after upgrade to 6.1 P1. Work around was to reboot the system one more time after upgrade.</p> <p>FIX: The extra reboot is not required after upgrade.</p>
LOG-15547	<p>At times the Logger UI shows that Reports are in a "pending" state, even when they have already run successfully.</p> <p>FIX: The Logger UI now updates with the correct Report status.</p>
LOG-15483	<p>In situations where the earliest data file had the wrong receipt time, Logger could not overwrite the old data, causing Logger to hang and stop working.</p>

Issue	Description
	FIX: Logger will allow the data file to be recycled, even if the time stamp is incorrect.
LOG-15275	<p>In the Logger 6.1 Release Notes, CentOS 6.6 was not mentioned as a supported OS platform.</p> <p>FIX: Release Notes were reissued to include support for CentOS 6.6.</p>
LOG-15110	<p>The Logger report template header could not display Japanese characters.</p> <p>FIX: Logger report templates that display report parameters in the header can now display those parameters in Japanese and other languages.</p>
LOG-15088	<p>Previously, hypertext links on the Event Summary by Receiver panel of the Global Summary Device page were sometimes incorrect.</p> <p>FIX: These hypertext links now redirect correctly.</p>
LOG-13538	<p>The time zone for Europe/Kaliningrad was displaying FET instead of EET on the Summary page and in the search results. This is a UI display issue. The time on Logger is correctly adjusted to be in the EET time zone.</p> <p>FIX: EET now displays properly.</p>

Reports

Issue	Description
LOG-15446	<p>Expired, published reports were not being properly deleted from the file system.</p> <p>FIX: Expired reports are now properly deleted.</p>
LOG-15053	<p>The Configuration menu option for the Running Searches page was incorrectly labeled "Running Tasks."</p> <p>FIX: The Running Searches page is now available from the Configuration > Running Searches menu option.</p>
LOG-15028	<p>Description: When Japanese characters were used in a Report Caption X-axis field, the caption did not display properly when exported to PDF/XLS.</p> <p>FIX: Japanese Report captions now display correctly.</p>
LOG-14457	<p>Previously, if you tried to view the run options for a Scheduled Report after navigating to the Scheduled Tasks page via the Configuration menu, you could be redirected to the Intellicus Login Page. Navigating to the Scheduled Tasks page</p>

Issue	Description
	<p>from the Reports menu did not cause this redirect.</p> <p>FIX: The Scheduled Reports page is available only through the Reports menu.</p>

System Admin

Issue	Description
LOG-15025	<p>Previously, some of the labels on the System Admin Rights menu of the System Admin > User Management > Groups tab > Default System Admin Group > Edit Group page were unclear.</p> <p>FIX: The "Configure Software Installation" label is now "System Settings." The "Configure Software Installation Settings" label is now "Configure software startup options." The "System Configuration Settings" label is now "Software Startup Options."</p>
LOG-12727	<p>Previously, when creating a CIFS mount, Logger allowed you to include special characters in the name, which prevented the mount from appearing on the list of Remote File Systems.</p> <p>FIX: Logger now accepts only alphanumeric characters, dashes (-) and underscores (_) within the CIFS mount name field. Dashes and underscores cannot be the first character in the field.</p>
LOG-12591	<p>In previous Logger versions, when users requested a password reset, the URL in the generated email pointed to the IP address of the Logger's eth1 interface instead of eth0.</p> <p>FIX: The URL now points to the correct IP address of the eth0 network interface.</p>

Upgrade

Issue	Description
LOG-15722	<p>In Logger 6.0, the VMware Logger did not contain enough space on the /boot partition to allow OS upgrades.</p> <p>FIX: With Logger 6.2 and 6.1, the /boot partition now has enough space to allow such OS upgrades.</p>

Open Issues

This release contains the following open issues.

• Analyze/Search	29
• Configuration	33
• Dashboards	35
• General	36
• Localization	41
• Reports	41
• Summary	43
• System Admin	44

Analyze/Search

Issue	Description
LOG-16348	<p>When exporting the search results with all fields included, the events' customized fields values are not exported.</p> <p>Workaround: Avoid using the customized fields and use customized fields (deviceCustomString1, deviceCustomNumber1, etc.) to store the customized values.</p>
LOG-16347	<p>When you search deviceEventClassId using the "where" clause, no search values are returned, even when matching events exist.</p> <p>Workaround: Use the AUSM query "_deviceGroup IN [value] AND deviceEventClassId=[value]".</p>
LOG-15972	<p>If you are doing a forensic search on data that has been archived, a search may be unable to load an Event Archive from a day that has been partially archived from local storage. For example, events prior to a certain time on June 1, or if local memory already has events loaded from an archive from that same date.</p> <p>Workaround: Query around the affected time range, or reduce storage group retention to remove previously restored archived events from that date in local storage.</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>

Issue	Description
	<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-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>
LOG-14778	<p>If a Receiver is deleted and re-created, a search drill-down on that Receiver in the Summary UI page will go to the Search page and query by Device Group, but search results do not include events received after re-creation of the Receiver.</p> <p>Workaround: Create a Receiver with different name and drill-down the events on the Summary page using the Device Group containing the new Receiver.</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 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 field set 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 field set used for the search, remove any renamed fields from the field set.</p>
LOG-11299	<p>If you uncheck the Rerun query option when exporting search results of a search</p>

Issue	Description
	<p>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>
LOG-11225	<p>When using the auto-complete feature on the Search page, if the query has a double quote followed by a bracket ("[), 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:</p> <pre>\ "[/opt/mnt/soft/logger_server.log.6] successfully.\ "</pre> <p>then after removing them, the query becomes:</p> <pre>[/opt/mnt/soft/logger_server.log.6] successfully.</pre> <p>This workaround can be also used when a double quote is followed by any special character. For example "\", "/", "[, "], or ",.</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-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-</p>

Issue	Description
	<p>Time Password (OTP) in the embedded browser fails after the Logger session has been inactive for the value 'Logger Session Inactivity Timeout'. The default timeout is 15 minutes.</p> <p>Workaround: Use an external browser to see results.</p>
LOG-7864	<p>The time in the agentReceiptTime fields is not in human-readable format when exported. 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-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-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>

Issue	Description
	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.
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-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> <pre><166>Sep 9 14:48:22 beach kernel: Killed bad incoming packet: IN=eth1 OUT=MAC=ff:ff:ff:ff:ff:ff:00:02:2d:0c:6f:d4:08:00 SRC=192.168.10.153 DST=192.168.10.255 LEN=229</pre> <p>Workaround: 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-15530	<p>Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail.</p> <p>Workaround: Do not configure LDAP on the system where the Software Logger is installed, and configure LDAP as the authentication method from the Logger system Admin > Authentication > External Authentication page.</p>
LOG-14650	<p>You cannot export a filter that has been previously imported. If you try to export such a filter, the export fails and Logger displays an error. This issue does not affect other export contents, such as Alerts, Saved Searches, or Dashboards.</p>

Issue	Description
	Workaround: None at this time.
LOG-13834	<p>When archiving data from a Logger Appliance, the "GMT+x" time zone incorrectly works like "GMT - x", while the "GMT - x" time zone works like "GMT+x".</p> <p>Workaround: Specify the Logger Appliance time zone by location. For example, set the time zone as "Taipei" or "Los Angeles."</p>
LOG-11176	<p>When you enable a Receiver, Logger does not validate the RFS mount it references.</p> <p>Workaround: Try to edit the Receiver to verify that the RFS mount is valid. Alternatively, verify the mount on the System Admin > Remote File Systems page.</p>
LOG-10605	<p>The Source Types page (Configuration > Source Types) is not visible to 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-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 the 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: Do not create a receiver with a name you have used for a deleted receiver.</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. 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 cannot be mounted, because the user name and password fields are empty.</p> <p>Workaround: Edit the setting of the CIFS share and re-enter your username and password.</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>

Issue	Description
	Workaround: If the pages stops loading, refresh the browser window to continue loading.
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 delete a certificate from the Configuration Data > Configuration page, the deleted certificate remains in the certificate list until the page is refreshed. This does not mean that the certificate was not correctly deleted.</p> <p>Workaround: Refresh the page, and the deleted certificate will not appear in the certificate list.</p>
LOG-370	<p>The Configuration Backup (Configuration > Configuration Backup > Backup_name) and File Transfer Receivers (Configuration > Receivers) may fail without notification. 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, so check the log (Configuration > Retrieve Logs) if you suspect a problem with the backup. When a Configuration Backup is scheduled, the error status is shown in the Finished Tasks status field.</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-11730	When there are two or more Dashboards with the same name, after you select one

Issue	Description
	<p>of them from the Dashboard dropdown menu, you will not be able to open and view the other Dashboard.</p> <p>Workaround: Rename any Dashboards with duplicate names.</p>

General

Issue	Description
LOG-16379	<p>When pushing an initial configuration containing SNMP destinations using ArcMC to a software logger upgraded from 6.1 to 6.2, the Logger onboard connector may fail to start after the push is completed and the Logger is rebooted.</p> <p>Workaround: Manually delete the pushed <code>agent.properties</code> file (and the associated <code>*.xml</code> file when there is an SNMP destination in the pushed configurations) from the following directory:</p> <pre>[Logger_install_dir] /current/arcsight/connector/current/user/agent</pre> <p>After this, the Logger onboard connector will auto-regenerate an initial <code>agent.properties</code> file, and the user can manually add the SNMP destinations through the Logger UI.</p>
LOG-16349	<p>For a newly-installed Logger, Report objects and queries are not available until you navigate to the Reports Dashboard (Reports > Dashboard) for the first time.</p> <p>Workaround: Before attempting to create a query or report, navigate to the Reports dashboard to provision the Report objects.</p>
LOG-16346	<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-16024	<p>When <code>platform:230</code> and <code>platform:201</code> events are forwarded from Logger to an ESM manager, the device host name and device address are converted to <code>localhost</code> and <code>127.0.0.1</code> respectively.</p> <p>Workaround: None at this time. Investigation is in progress.</p>
LOG-15827	<p>When creating a Dashboard from the Search page, if the dashboard name contains</p>

Issue	Description
	<p>a slash (/), Logger displays an error, but still creates the Dashboard as named. This results in a Dashboard that users cannot access or delete.</p> <p>Workaround: Do not use the slash character within Dashboard names.</p>
LOG-15501	<p>CentOS 7.1 does not automatically recognize a second hard drive to the VMware template after correctly adding it.</p> <p>Workaround: Run the following commands on the virtual machine console after adding the second hard drive:</p> <div data-bbox="423 642 1401 785" style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: In the following commands, replace "ARCSIGHT_HOME" with the path where the Logger software will be installed. Make a note of this location. When you run the Logger installer, be sure to use that path.</p> </div> <ol style="list-style-type: none"> 1. Run the parted tool. <pre>parted /dev/sdb</pre> <ol style="list-style-type: none"> 2. Attach a label to the disk. <pre>mklabel gpt</pre> <ol style="list-style-type: none"> 3. Make an XFS partition utilizing the whole capacity of the drive. <pre>mkpart primary xfs '0%' '100%'</pre> <ol style="list-style-type: none"> 4. Exit parted. <pre>q</pre> <ol style="list-style-type: none"> 5. Create XFS file system and assign a label: <pre>mkfs.xfs -L DATA /dev/sdb1</pre> <ol style="list-style-type: none"> 6. Append following line to /etc/fstab file to mount this partition on boot: <pre>LABEL=DATA ARCSIGHT_HOME/data xfs defaults,inode64 1 2</pre> <ol style="list-style-type: none"> 7. Create a mount path. <pre>mkdir ARCSIGHT_HOME/data</pre> <ol style="list-style-type: none"> 8. Mount the file system. <pre>mount -L DATA</pre>
LOG-15500	<p>When you hover over a Dashboard Monitor graph, you might see the data point label without the data point value. This problem does not exist for graphs in the New Monitor Dashboard.</p>

Issue	Description
	Workaround: Switch to New Monitor Dashboard to view the graph. Graphs with shorter time periods tend not to have this problem as often.
LOG-15490	<p>In some circumstances during a data migration to a L7600 Appliance, some processes will not restart on the target machine after the reboot.</p> <p>Workaround: Log into the appliance using Secure Shell (SSH) to restart all processes manually:</p> <pre data-bbox="423 583 951 615">/opt/local/monit/bin/monit restart all</pre>
LOG-15462	<p>Description: When the file system /opt/arcsight/userdata is full, Logger allows users to run reports, even though they necessarily fail. Also there is no mechanism that warns users in advance that the free space on their file system is exhausted. That is important for scheduled reports.</p> <p>Workaround: Check the amount of free space periodically.</p>
LOG-15456	<p>Apache process fails to start if "Client Certificate" or "Client Certificate AND User Password" has been enabled before Trusted Certificates are uploaded.</p> <p>Workaround: Apache will fail to start if the Trusted Certificates directory is empty. Upload Trusted Client certificates in the System Admin > Security > SSL Client Authentication > Trusted Certificates tab before enabling authentication methods from the System Admin > Users/Groups > Authentication > External Authentication tab.</p>
LOG-15454	<p>Logger may experience failures attempting to forward very large events to ESM.</p> <p>Workaround: Please contact HP Support for help with this issue.</p>
LOG-15402	<p>On Logger L7500 and L7600 Appliances, platform audit events are not reflecting the correct destination address for the appliance.</p> <p>Workaround: Disable any unused network interface cards.</p>
LOG-15352	<p>When Logger v6.0 on L7500 is upgraded to Logger v6.1, the CAC authentication doesn't work.</p> <p>Workaround: When logged into Logger as an Admin, navigate to System Admin > SSL Client Authentication. Delete and re-import all trusted certificates, and restart Apache.</p>
LOG-15291	<p>The L750X Appliance may suffer a kernel panic.</p> <p>Workaround: Upgrade the version of iLO firmware on the appliance to 1.51 or later. See the HPE customer advisory:</p>

Issue	Description
	http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04332584
LOG-14948	<p>Some letters are dropped in XLS reports fields containing "pretty printed" data (e.g. multi-line SQL statements with indentation in deviceString field)</p> <p>Workaround: Do not use unnecessary whitespaces (e.g. newlines, tabs) in the data referred by reports</p>
LOG-14625	<p>When a query calls more than ten fields using the "top" expression, Logger generates no results, but also does not give the user an error message that the supported number of fields has been exceeded.</p> <p>For example, "deviceProduct = "Logger" top deviceVendor, deviceVersion, deviceEventClassId, name,..." and so on.</p> <p>Workaround: Reduce your "top" search queries to ten fields or less, or contact HPE ArcSight Customer Support for a more detailed workaround.</p>
LOG-14595	<p>On Logger appliances, the message "error: Bind to port 22 on 0.0.0.0 failed: Address already in use" gets logged every minute to /var/log/secure.</p> <p>Workaround: This message will appear only if SSH access has been enabled, and can be ignored. The SSH daemon is erroneously restarted every minute even if already running.</p>
LOG-14546	<p>When you create a copy of a saved search, and then modify the query to have an invalid value and try to save this new saved search, this will cause the system to return back the query and then the field, for the name keeps duplicating the "Copy of" and every instance of the name will have a new instance of "Copy of".</p> <p>Workaround: Correct the query and remove those duplicated "Copy of" from the saved search name. Then save it.</p>
LOG-14386	<p>When user opens the Reports Dashboard in an Internet Explorer 11 (IE 11) window less than 1450 pixels wide, the Reports menu is not displayed.</p> <p>Workaround: When working with IE 11, make the browser window wider than 1450 pixels.</p>
LOG-14266	<p>After updating daily archive task setting, user can not see the event when issuing the query: message = "Daily archive task settings updated".</p> <p>Workaround: Use either one of these queries:</p> <p>message CONTAINS "Daily archive task settings updated"</p>

Issue	Description
	message STARTSWITH "Daily archive task settings updated"
LOG-13752	<p>If you check the Rerun Query checkbox when exporting the search results, the download may not include all search results if it is started before the query finishes running. Large search exports, where the query has close to or over 1M hits and is exported with the re-run query checked, might display the "Download results" link before the export file has finished populating. Logger doesn't indicate when the file is ready for download from the User Interface.</p> <p>Workaround: Wait a few minutes before downloading to get the full export file.</p>
LOG-13532	<p>When the time change due to the end of Daylight Savings Time (DST) takes place in the fall, (time is set back one hour), the search results may not display properly. This happens because Logger is not able to distinguish the event times in the overlap period.</p> <p>Workaround: To ensure that all events are returned and can be displayed, specify a start time of 12:59:59 or earlier and end time of 2:00:01 or later.</p>
LOG-13373	<p>The Report "Execution Status" doesn't list the most recent Jobs by default.</p> <p>Workaround: Navigate to the first page manually by clicking the appropriate icon.</p>
LOG-13372	<p>If you click the "Job Execution Status" graph and then click the "Last Run Status" table in the pop-up window, an error message appears.</p> <p>Workaround: Click the table at the bottom of the Job Execution Status page.</p>
LOG-13226	<p>Editing a Forwarder while it is enabled can cause the Forwarder to stop sending events.</p> <p>Workaround: Disable the Forwarder before editing it.</p>
LOG-12030	<p>If you export search results with just the three fields Event Time, Device, and Logger, you must check the All Fields check box or the export will not succeed.</p> <p>Workaround: To export search results without the All Fields requirement, add another field to have all of the corresponding events exported correctly.</p>
LOG-11473	<p>When using the Setup Wizard to enter a Logger Appliance initial configuration, Logger does not check that you have entered all the required information before submitting it. This can result in the setup to fail.</p> <p>Workaround: Enter valid values for all required Setup Wizard fields.</p>
LOG-11290	<p>When you delete a Receiver, the Receiver's numeric ID still displays in the Summary page, although it is correctly deleted from the Dashboards.</p>

Issue	Description
	Workaround: Restart the Logger.
LOG-8901	<p>If you are using an email address with more than three characters in the top-level domain (such as user@yourco.info), Logger may reject the email as invalid.</p> <p>Workaround: Use an email address with a three-character top-level domain name for the report, and set up email forwarding to the non-standard email address.</p>

Localization

Issue	Description
LOG-15905	<p>The Logger configuration backup file has the format: <date>_<time>.configs.tar.gz. When the locale is set to Chinese Traditional, the <date> contains Chinese characters, causing the backup to fail if you are using SCP for secure copying to the target backup server.</p> <p>Workaround: Use OpenSSH for configuration backups.</p>
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>

Reports

Issue	Description
LOG-16260	<p>If a single connector is sending events to multiple destinations, then the Daily Byte Count report might show the wrong daily byte count number.</p> <p>Workaround : None at this time.</p>
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</p>

Issue	Description
	<p>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>
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-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-10923	<p>Using run-time parameter filters on Ad hoc Reports can limit results to 100,000 lines. The Admin guide mentions this limit for Group and Sort parameters, but the same limitations apply for all of the run-time parameter filters.</p> <p>Workaround: Use hard-coded SQL parameters to generate results over 100,000 lines.</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 opens with unexpected results, since it 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-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>

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 error messages were displayed when the user tried to run reports.</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.</p> <p>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. If a user tries to schedule a restricted report, the user will see: "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 as view and run them ad-hoc.</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-16266	<p>On L7600 Logger Appliances, the first time you visit the System Admin > Process Status page after a reboot, some processes may appear to be in "Execution failed" state.</p> <p>Workaround: You can ignore this; the processes are actually likely to be in "running" state. The UI will display the correct state at the next automatic refresh OR if you manually click Refresh Status.</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>

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Logger 6.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!