



Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform Logger and ArcSight Logger

Software Version: 6.3

Release Notes

October 27, 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.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Logger 6.3 Release Notes	5
What's New in this Release	5
Search Improvements	5
A New Approach to Logger Licenses	6
Updated User Interface	6
New and Enhanced Logger Receivers	6
Updated Trial Logger	6
Other New Features and Capabilities	7
New Type of License	7
Licensing Update Impact on Upgraded Loggers	7
Trial License Information	8
Uploading a License	8
Firewall Rules	9
Supported Platforms	9
Browser Support	9
System Requirements	10
Logger Documentation	10
Localization Information	12
Known Limitations in Localized Versions	12
Upgrading to Logger 6.3 (L7861)	13
Upgrade Paths	13
Verifying Your Upgrade Files	14
Upgrading the Logger Appliance	14
Prerequisites	14
Editing the logind Configuration File for RHEL 7.X	15
Upgrade Instructions	16
Upgrading Software Logger and Logger on VMWare VM	18
Prerequisites	18
Increasing the User Process Limit	19
Editing the logind Configuration File for RHEL 7.X	20
Upgrade Instructions	20

Known Issues	27
Daily Data Limit for Newly Upgraded Software Loggers	27
Kernel Warning Message During Boot	27
Fixed Issues	28
Analyze/Search	28
Configuration	29
Dashboards	30
Localization	31
Reports	31
System Admin	31
Upgrade	32
Open Issues	33
Analyze/Search	33
Configuration	37
Dashboards	40
Localization	40
Reports	40
Summary	43
System Admin	44
Upgrade	45
Send Documentation Feedback	46

Logger 6.3 Release Notes

These release notes apply to the ArcSight Data Platform (ADP) Logger and standalone ArcSight Logger, version 6.3 (L7861) releases. In this document, the term *Logger* refers to both the ADP Logger and the standalone Logger.

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 the Logger release.

Note: Where there are no specific differences, all types of Logger are called *Logger* in this document. Where there are differences, the specific type of Logger is indicated.

What's New in this Release

The HPE Security ArcSight Logger 6.3 release (L7861) introduces the following new features and enhancements.

Search Improvements

- Enhanced Logger peer search capabilities and support:
 - Up to 100 peers,
 - Up 100 concurrent peer searches,
 - Improved peer search performance.

Refer to the Configuration chapter of the Logger Administrator's Guide for more information.

- Search fields are now color coded for easy identification and index status:
 - Indexed fields: green,
 - Super indexed fields: dark green,
 - Metadata fields: light gray,
 - CEF fields: light green.

Refer to the Configuration chapter of the Logger Administrator's Guide for more information.

A New Approach to Logger Licenses

- Independent license support for ADP ArcSight Loggers and standalone ArcSight Loggers.
- All new and upgraded Loggers include a trial license. After installing or upgrading to Logger 6.3, you must apply the production license to enable full access. See ["New Type of License" on the next page](#) for more information.

STOP: After upgrading to Logger 6.3, your existing ArcSight license will no longer work. To avoid any loss of functionality, you must obtain a new license prior to upgrading Logger, and apply it immediately after the upgrade.

STOP: Because of the new type of license, the SSH challenge-response mechanism is no longer available on Logger appliances. If you used to rely on this mechanism, it is imperative that you change the default root password before upgrading the Logger appliance.

Updated User Interface

- A new License Volume page for ADP Loggers.
- Updated License Volume page for standalone ArcSight Loggers. Refer to the Configuration chapter of the Logger Administrator's Guide for more information.
- Improved usability and updated look and feel.

New and Enhanced Logger Receivers

- New Event Broker receiver enables support for ADP Event Broker.
- For Logger Appliances, an automatic firewall configuration script makes updating the firewall fast and easy. See ["Firewall Rules" on page 9](#) for more information.

Updated Trial Logger

- Trial license valid for 90 days.
- Storage Capacity 90 GB.
- Daily Data Ingestion 5 GB per day.
- A fresh installation is not required when you want a full Logger; just apply the new license.
- Only Reporting features are disabled.

See ["Trial License Information" on page 8](#) for more information.

Other New Features and Capabilities

- Capacity pooling support for ADP Loggers is now available to help redistribute and manage the total capacity of your environment.
- Users can now use HTTP Strict Transport Security Protocol (HSTS) to ensure that their browsers always connect to Logger over HTTPS.
- Digital signature support for Logger reports is now available on reports configured with this option.

For details about these features, see the ArcSight Logger 6.3 Administrator's Guide, available from the [ArcSight Product Documentation Community on Protect 724](#).

For more information about this release, review the following sections:

- ["Known Issues" on page 27](#).
- ["Fixed Issues" on page 28](#).
- ["Open Issues" on page 33](#).

New Type of License

The licensing change impacts all upgraded Loggers until you apply the new license.

Licensing Update Impact on Upgraded Loggers

After upgrading to Logger 6.3, existing ArcSight licenses will no longer work. This happens because ArcSight Data Platform Logger and ArcSight Logger 6.3 implement a new type of license. The old license will no longer apply. You must obtain a new license prior to upgrading, and apply it immediately after the system has been upgraded in order to avoid any loss of functionality.

Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSightLogger or ArcSight Data Platform (ADP) Logger license.

Because of the new type of license, the SSH challenge-response mechanism is no longer available on Logger appliances. If you used to rely on this mechanism, it is imperative that you change the default root password before upgrading the Logger appliance.

Trial License Information

The trial license is valid for a 90-day evaluation period. After that period is over, you will not be able to access any Logger features until you upload your new license.

The trial license gives you access to the following:

- All Logger features except Reporting.
- 5 GB per day ingested data volume. (Software Loggers only.)
- 90 GB Storage Volume. (For upgraded systems, the license will display 90 GB, but the Storage Volume on your Logger is not lowered to that limit.)

Depending on whether your license entitles you to management by ArcMC, you can update the trial license with either a standalone ArcSight Logger license or an ADP license. (ArcMC manages ADP Loggers.) Uploading either license enables the Reporting feature and increases the licensed daily data volume and storage volume to the capacity of the license.

Uploading a License

Once you apply a standalone Logger license, you can upgrade to an ADP Logger license later. Please contact support if you need to go back to a standalone Logger license from an ADP Logger license.

To upload your new license:

1. If you have not already done so, redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to Logger. For more information, refer to the software delivery confirmation email you received from HPE.
2. From the computer to which you downloaded the update file, log in to Logger using an account with administrator (upgrade) privileges.
3. Click **System Admin** from the top-level menu bar.
4. Click **License & Update** in the **System** section.
5. Browse to the license file you downloaded earlier, and click **Upload Update**. The Update in Progress page displays the update progress.
6. **Important:** After you upload your license, you must reboot the Logger Appliance or restart Software Logger. This restarts all Logger processes with the new license settings.

Refer to the System Admin chapter of the Logger System Administrator's Guide for more information.

Firewall Rules

Before Logger can receive data, some ports must be opened through the firewall.

- For Software Logger, you are responsible for setting up the firewall. After you first install or upgrade to Logger 6.3, you should configure the firewall to be open only for the ports required for your configuration.

Caution: HPE ArcSight strongly recommends that you configure your firewall so that only the required ports are open.

- For the Logger Appliance, the firewall is preconfigured. HPE ArcSight provides a script you can use to update the firewall.

Tip: Be sure to update the firewall configuration whenever you add or remove any service that requires an open port for incoming traffic, such as a receivers or SNMP polling.

Refer to the System Admin chapter of the Logger Administrator's Guide for a list of default ports and other information.

Supported Platforms

Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.3 platform support.

Note: Upgrading to Logger version 6.3 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.

Browser Support

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.3 browser support.

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

receiver.

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

System Requirements

Logger requires the following minimum system setup.

Specification	Details
CPU, Memory, and Disk Space for 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>
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
VM Instances	<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 7.2 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.
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.

Logger Documentation

In addition to these Release Notes, the following documentation is available for the Logger 6.3 release.

Tip: The most recent versions of these guides may not be included with your download. Please check Protect 724 for updates.

- **Logger 6.3 Online Help:** Provides information on how to use and administer Logger. 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. Also available in PDF format as the *Logger Administrator's Guide* and *Logger Web Services API Guide*.
- *ArcSight Data Platform 2.0 Support Matrix* (formerly the *Logger Support Matrix*): Provides integrated support information such as upgrade, platform, and browser support for Logger, ArcMC, and SmartConnectors. Available for download from the [ArcSight Product Documentation Community on Protect 724](#).
- *Logger 6.3 Administrator's Guide:* Provides information on how to administer and use Logger. Available for download from the [ArcSight Product Documentation Community on Protect 724](#). Also accessible from the integrated online Help.
- *Logger 6.3 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](#). 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 6.3 Installation Guide:* Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM. Available for download 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 in Localized Versions

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 6.3 (L7861)

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

- ["Verifying Your Upgrade Files" on the next page](#)
- ["Upgrading the Logger Appliance" on the next page](#)
- ["Upgrading Software Logger and Logger on VMWare VM" on page 18](#)

Note: Be sure to review the sections ["Known Issues" on page 27](#), ["Fixed Issues" on page 28](#), and ["Open Issues" on page 33](#) before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.3. For more information about upgrading from a version of another appliance model 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 6.3 Upgrade Paths	
Software Versions	6.2 (7633), 6.2 Patch 1 (7648)
Appliance Models	L350X L750X L750X-SAN L7600
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.• Refer to the ADP Support Matrix document available on the Protect 724 site 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>

Upgrading the Logger Appliance

Caution: The upgrade prerequisites have changed considerably with this release. Read them carefully before beginning the upgrade.

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.
- You must be on Logger 6.2 (7633) or 6.2 Patch 1 (7648) prior to upgrading to Logger 6.3.
- Logger requires a root password. If your Logger does not have a root password already, give it one before performing the upgrade.

STOP: Because of the new type of license, the SSH challenge-response mechanism is no longer available on Logger appliances. If you used to rely on this mechanism, it is imperative that you change the default root password before upgrading the Logger appliance.

- You may need to upgrade your OS before you upgrade Logger. For a list of supported Operating Systems, refer to the *ArcSight Data Platform Support Matrix*, available for download from the [ArcSight Product Documentation Community on Protect 724](#).
 - If you are upgrading an Lx500 series appliance, you must upgrade your OS to RHEL 6.8. (Logger 6.3 includes an OS Upgrade file for this purpose.)
 - If you are upgrading an Lx600 series appliance, you must upgrade your OS to RHEL 7.2. (Logger 6.3 includes an OS Upgrade file for this purpose.)
 - If you are on RHEL 7.X, modify the logind configuration file. For more information, see ["Editing the logind Configuration File for RHEL 7.X" on the next page](#).

- Download the upgrade files from the HPE [Customer Support site](#) to a computer from which you connect to the Logger UI.
 - For both local upgrades and remote upgrades using ArcMC, download the following file:
`logger-7861.enc`
 - For OS upgrades, download the appropriate file:
 - `osupgrade-logger-rhel68-<timestamp>.enc`
 - `osupgrade-logger-rhel72-<timestamp>.enc`
 - Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).
- Redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to Logger. For more information, refer to the confirmation email you received from HPE.

STOP: After upgrading to Logger 6.3, your existing ArcSight license will no longer work. To avoid any loss of functionality, you must obtain a new license prior to upgrading Logger, and apply it immediately after the upgrade.

- Before starting the upgrade, check that you have your new license available. You must apply it as soon as possible.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

- Verify the upgrade files, as described in "[Verifying Your Upgrade Files](#)" on the previous page.

Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7.1 or 7.2, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.X:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the `RemoveIPC` line. `RemoveIPC` should be active and set to `no`.
Remove the `#` if it is there, and `=` change the `yes` to `no` if appropriate. The correct entry is:

`RemoveIPC=no`
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind`

service and put the change into effect:

```
systemctl restart systemd-logind.service
```

Upgrade Instructions

The upgrade prerequisites have changed considerably with this release. Read them carefully before beginning the upgrade. Review the ["Prerequisites" on page 14](#) before proceeding.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

You must upload your new license as soon as possible. See ["New Type of License" on page 7](#) for more information and instructions.

To upgrade Logger Appliances remotely through ArcMC:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 14](#).
2. Upgrade your OS if necessary.
 - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel68-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
 - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel72-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Deploy the Logger upgrade by using the file `logger-7861.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
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.
5. Upload your new licenses by following the instructions in the ArcSight Management Center Administrator's Guide.

Caution: After you upload the licenses, you must reboot your appliances.

To upgrade a Logger Appliance locally:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 14](#).
2. Log into Logger and click System Admin | System > **License & Update**.
3. Upgrade your OS if necessary.

- If you are upgrading an Lx500 series appliance, browse to the `osupgrade_logger_rhel168_<timestamp>.enc` file you downloaded previously and click **Upload Update**.
- If you are upgrading an Lx600 series appliance, browse to the `osupgrade_logger_rhel172_<timestamp>.enc` file you downloaded previously and click **Upload Update**.

This will upgrade the OS.

4. Browse to the `logger-7861.enc` file you downloaded previously and click **Upload Update**.

The **ArcSight License & System Update** page displays the update progress. Once the upgrade is complete, Logger reboots automatically.

5. 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.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

6. Upload your new license by following the instructions in ["Uploading a License" on page 8](#).

Caution: After you upload the license, you must reboot your appliance.

Upgrading Software Logger and Logger on VMWare VM

Caution: The upgrade prerequisites have changed considerably with this release. Read them carefully before beginning the upgrade.

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.
- You must be on Logger 6.2 (7633) or 6.2 Patch 1 (7648) prior to upgrading to Logger 6.3.
- You may need to upgrade your Operating System (OS) to a supported version before upgrading Logger. For a list of supported Operating Systems, refer to the *ArcSight Data Platform Support Matrix*, available for download from the [ArcSight Product Documentation Community on Protect 724](#).
 - If your system is running on RHEL or CentOS 7.X, upgrade to version 7.2.
 - If your system is running on RHEL or CentOS 6.X, upgrade to version 6.8.
 - If not already done on the system,
 - Increase the user process limit on the Logger's OS. (You do not need to do this for Logger on VMWare VM, it is already done on the provided VM.) For more information, see ["Increasing the User Process Limit" on the next page](#).
 - If you are on RHEL 7.X, modify the logind configuration file. For more information, see ["Editing the logind Configuration File for RHEL 7.X" on page 20](#).
- Download the Software Logger upgrade files from the HPE [Customer Support site](#).
 - For remote upgrades using ArcMC, download the following file:
`logger-sw-7861-remote.enc`
 - For local upgrades, download the following file:
`ArcSight-logger-6.3.0.7861.0.bin`
 - Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).

- Redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to Logger. For more information, refer to the confirmation email you received from HPE.

STOP: After upgrading to Logger 6.3, your existing ArcSight license will no longer work. To avoid any loss of functionality, you must obtain a new license prior to upgrading Logger, and apply it immediately after the upgrade.

- Before starting the upgrade, check that you have your new license available. You must apply it as soon as possible.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

- Verify the upgrade files, as described in ["Verifying Your Upgrade Files" on page 14](#).

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.

Note: 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
```

Caution: 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 run time 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
```

Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7.1 or 7.2, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.X:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the `RemoveIPC` line. `RemoveIPC` should be active and set to `no`.
Remove the `#` if it is there, and `=` change the `yes` to `no` if appropriate. The correct entry is:

`RemoveIPC=no`
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect:

```
systemctl restart systemd-logind.service
```

Upgrade Instructions

The upgrade prerequisites have changed considerably with this release. Read them carefully before beginning the upgrade. Review the ["Prerequisites" on page 18](#) before proceeding.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

You must upload your new license as soon as possible. See ["New Type of License" on page 7](#) for more information and instructions.

Follow the instructions listed below to upgrade your Logger.

- To upgrade Logger remotely, see ["To upgrade Software or VMWare Loggers remotely through ArcMC:" on the next page](#).

- To upgrade Software Logger locally, see ["To upgrade Software Logger locally:" below](#).
- To upgrade Logger on VMWare locally, see ["To upgrade Logger on VMWare VM:" on page 24](#).

To upgrade Software or VMWare Loggers remotely through ArcMC:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 18](#).
2. Upgrade your OS if appropriate.

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.

3. Deploy the downloaded upgrade file, `logger-sw-7861-remote.enc`, by following the instructions in the ArcSight Management Center Administrator's Guide.
4. Upload your new licenses by following the instructions in the ArcSight Management Center Administrator's Guide.

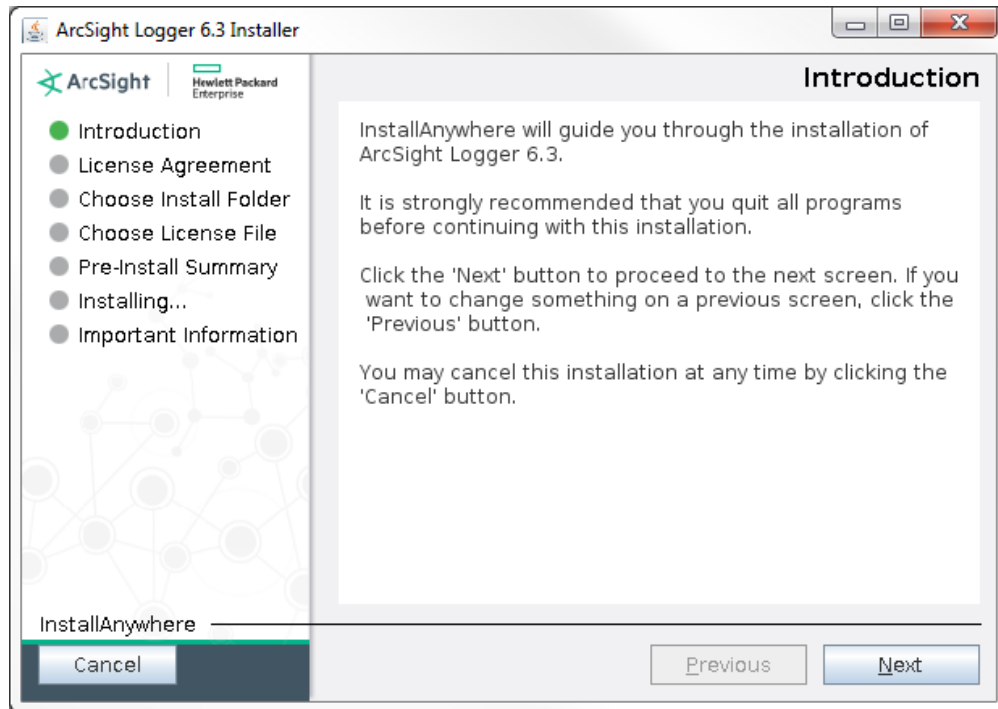
Caution: After you upload the licenses, you must reboot your appliances.

To upgrade Software Logger locally:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 18](#).
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 u+x ArcSight-logger-6.3.0.7861.0.bin  
./ArcSight-logger-6.3.0.7861.0.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.
7. Once all Logger processes are stopped, the installer checks that installation prerequisites are met:
 - Operating system check—the installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. Press Click **Continue** to proceed with the upgrade or **Quit** to exit the installer and upgrade your OS.

Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before upgrading Logger. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

- Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

Example

An Intervention Required message displays, informing you that a parameter needs to be changed from `yes` to `no` in the `etc/logind.conf` file. The message tells you what needs to be done. In this example, quit the installer, and follow the instructions in ["Editing the logind Configuration File for RHEL 7.X" on page 20](#). When the file has been modified and saved, enter the installation command again.

Once all the checks are complete, the Choose Install Folder screen is displayed.

8. Navigate to or specify the location where you want to install Logger.

The default installation path is `/opt`. You can install into this location or another location of your choice.

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.

9. Click **Next** to install into the selected location.
 - If there is not enough space to install the software at the location you specified, a message is displayed. To proceed with the installation, specify a different location or make sufficient space available at the location you specified. Click **Previous** to specify another location or **Quit** to exit the installer.
 - 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.

Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before upgrading. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

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

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

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

11. Click **Next** to initialize Logger components.

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

12. Click **Next** to upgrade Logger.

Upgrading Logger may take a few minutes. Please wait. Once the upgrade is complete, the next screen displays the URL you should use to connect to Logger.

13. Make a note of the URL and then click **Done** to exit the installer.

14. Restart Logger to put the upgrade changes into effect.

15. You can now connect to the upgraded Logger.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

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.
17. Upload your new license by following the instructions in ["Uploading a License" on page 8](#).

Caution: After you upload your license, you must restart Software Logger.

To upgrade Logger on VMWare VM:

1. Before you begin, ensure that you meet the ["Prerequisites" on page 18](#).
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 u+x ArcSight-logger-6.3.0.7861.0.bin
./ArcSight-logger-6.3.0.7861.0.bin -i console
```

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 6.3.

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:

- a. The next several screens display the end user 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. Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS. To continue, type 1 and press **Enter**. To quit so that you can upgrade your OS, type 2 and press **Enter**.

Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before upgrading Logger. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

6. The installer checks that installation prerequisites are met:
 - Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software.

Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

- Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

Example

If Logger is running on this machine, an Intervention Required message displays:

=====

Intervention Required

ArcSight Logger processes are active.

All ArcSight Logger processes must be stopped to allow installation to proceed.

Type 'Quit' to exit this installer or 'Continue' to stop all ArcSight Logger processes and continue with the installation.

->1- Continue

2- Quit

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

In this case, you would enter 1 (or hit **Enter**) to stop Logger processes, or 2 to quit the installer.

Once all checks complete, the installation continues, and the Choose Install Folder screen is displayed.

7. 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.

8. Type Y and press **Enter** to confirm the installation location.
 - If there is not enough space to install the software at the location you specified, a message is displayed. Type quit and press **Enter** to exit the installer and reconfigure your VM.
 - 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. Type 2 and press **Enter** to continue with the upgrade.
9. 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.
10. Press **Enter** to initialize the Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
11. Press **Enter** to upgrade and restart Logger.

The upgrade may take a few minutes. Please wait.

Once the upgrade is complete, Logger starts up and the next screen displays the URL you should use to connect to Logger.
12. Make a note of the URL and then press **Enter** to exit the installer.
13. You can now connect to the upgraded Logger.

Caution: Immediately after upgrading your Logger to version 6.3, you will have only a trial license, and will be subject to the trial license limitations until you apply your standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

14. 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.
15. Upload your new license by following the instructions in ["Uploading a License" on page 8](#).

Caution: After you upload your license, you must restart Software Logger.

Known Issues

The following known issues apply to this release.

Daily Data Limit for Newly Upgraded Software Loggers

Logger 6.3 implements a new type of license file. Immediately on upgrade to Logger 6.3, this new type of license is in effect. A trial Logger license, with the trial license limitations, is in place until you upload your 6.3 standalone ArcSight Logger or ArcSight Data Platform (ADP) Logger license.

Until you update to the full license, the daily data limit is *5 GB per day*. Logger displays a "Licensed Data Volume Limit Exceeded" warning banner each day you exceed the 5 GB daily data limit.

Caution: If the data limit has been exceeded six times in 30 days, you cannot use any search-related features until the listed 30 days have five or fewer violations. The disabled search-related features include forwarders as well as all searching and reporting functionality.

For more information and instructions on how to apply the full license, see ["New Type of License" on page 7](#).

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	28
• Configuration	29
• Dashboards	30
• Localization	31
• Reports	31
• System Admin	31
• Upgrade	32

Analyze/Search

Issue	Description
LOG-16739	<p>On rare occasions, indexing stopped completely, causing severe performance degradation for the Logger.</p> <p>FIX: The Indexing function now works as expected.</p>
LOG-16439	<p>The documentation did not explain clearly how to use the RESTful Search Web service to return aggregate search data from the sort, tail, and head operators.</p> <p>FIX: The following information was added to the Logger documentation: Use the chart_data HTTP POST to return aggregate search data. The chart_data service returns the data you can use to display a chart and the table under the chart. It can also be used to return the results of aggregate operators like sort, tail, and head.</p>
LOG-16431	<p>The documentation did not explain how to run concurrent searches.</p> <p>FIX: The documentation now mentions that you can run concurrent searches by using two different browsers or a browser with a plugin that allows you to open different sessions, such as Multifox in Firefox.</p>
LOG-16325	<p>Previously, when you tried to limit events in the Live Event Viewer to a particular storage group, the filter didn't work, and the search returned events from other storage groups.</p> <p>FIX: The storage group filter for the Live Event Viewer now works as expected.</p>
LOG-14897	<p>The documentation did not clearly explain what can and cannot be searched for in a field-based search.</p> <p>FIX: The search documentation has been updated to include this information. See "Things You Should Know About Logger Searches" in the "Searching and Analyzing Events" section of the Logger Admin Guide.</p>

Issue	Description
LOG-14896	<p>Previously, when performing a full-text (keyword) search, the user interface did 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>FIX: Event data is now color-coded, to help identify indexed, super-indexed, and other searchable fields. System-defined fields are included in the search results, but they are not searchable, because they contain no event data. To tell if a field is searchable, hover over it. If it highlights, it is searchable, if it does not, you cannot search on that term.</p>
LOG-14814	<p>By default, NULL values were not included in Logger search results, and you had to explicitly call out NULL values with <field> IS NOT NULL or <field> IS NULL. If you wanted to change this, you had to contact support.</p> <p>FIX: Logger can now be configured to make NOT search conditions include NULL values from the Configuration > Search Options menu.</p>
LOG-14020	<p>When performing a peer search on one peer and then immediately performing a peer search on the other peer, the search occasionally terminated prematurely and displayed the error "[Local] Error: Database Connection".</p> <p>FIX: Consecutive peer searches now execute correctly.</p>
LOG-13752	<p>The Search UI stops when it reaches a maximum of 1 million results. However, when exporting search results, if the Rerun Query checkbox was enabled, the query continued to the end, which could be well beyond 1 million results.</p> <p>FIX: The Export Search Results function now stops when it reaches the 1 million result maximum.</p>
LOG-12624	<p>Previously, local search queries that were supposed to stop when search results hit 1 million, continued to run to completion.</p> <p>FIX: Local search queries now stop when Logger reaches 1 million results.</p>
LOG-5958	<p>Previously, when you tried to remove a selected field in the Fieldset Editor with the left arrow button, the field did not return to the correct group.</p> <p>FIX: The Fieldset Editor now works as expected, and the selected items go back to the correct groups.</p>

Configuration

Issue	Description
LOG-14546	<p>Previously, when you saved a copy of a Saved Search containing a bad query type, the save would fail, and append the words "Copy of" many times in the Name field.</p> <p>FIX: Saved Search copies containing a bad query type no longer triggers multiple "Copy of" text to the Name field.</p>
LOG-13498	<p>Previously, When you tried to import an invalid file, the error message showed the file name along with the absolute path, which was not related to the error.</p> <p>FIX: When you attempt to import an invalid file, the error message now displays correctly.</p>

Issue	Description
LOG-10605	<p>The Source Types page (Configuration > Source Types) was not visible to non-Admin users who did not have the correct permissions assigned to them.</p> <p>FIX: The documentation now includes a reminder to assign rights from the Default Logger Rights Group and Default System Admin Group to non-Admin users who need access to Source Types.</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>FIX: A note was added to the Source Type Documentation to warn users to be cautious when deleting parsers.</p>
LOG-6209	<p>Previously, the Finished Tasks page could take a long time to load, due to an accumulation of finished tasks.</p> <p>FIX: You can now apply filter criteria to limit the search results. If the data that matches the provided criteria has more than 5000 rows, Logger will return only the first 5000 rows.</p>

Dashboards

Issue	Description
LOG-16877	<p>Custom dashboards with an individual receiver displayed "No data available," even when the Monitor > Receivers dashboard displayed valid information.</p> <p>FIX: Custom dashboards now display available data for the receiver.</p>
LOG-15827	<p>When creating a Dashboard from the Search page, if the dashboard name contained a slash (/), Logger displayed an error, but still created the Dashboard as named. This resulted in a Dashboard that users could not access or delete.</p> <p>FIX: The Search documentation has been modified to advise users not to include the slash character within Dashboard names.</p>
LOG-15500	<p>Previously, when mousing over data points on a Dashboard graph, the individual data point values did not display.</p> <p>FIX: When mousing over data points on a Dashboard, individual data point values now display correctly.</p>
LOG-14156	<p>When using Internet Explorer, the bottom of the Monitors Dashboard does not always render properly.</p> <p>FIX: Maximize the Internet Explorer window when viewing the Monitors Dashboard.</p>

Localization

Issue	Description
LOG-15761	<p>When the selected Logger interface language was something other than English, only Column-type charts displayed.</p> <p>FIX: The different chart types now display correctly in all languages.</p>

Reports

Issue	Description
LOG-16260	<p>Previously, when a single connector sent events to multiple destinations, the Daily Byte Count was sometimes inaccurate.</p> <p>FIX: The Daily Byte Count now works as expected.</p>
LOG-15392	<p>Previously, Logger did not support digitally signed PDF reports.</p> <p>FIX: You can now enable and configure digitally signed PDF reports in Reports > Report Administration > Report Configuration dialog under Sign Document.</p>
LOG-11292	<p>The documentation incorrectly included an option to package Scheduled Reports.</p> <p>Fix: The incorrect option was removed from the Logger Administrator's Guide.</p>

System Admin

Issue	Description
LOG-15501	<p>CentOS did not recognize the second hard disk you added to the VM. You had to mount it manually.</p> <p>FIX: The OVA installer now handles the second hard disk correctly. The drive is automatically recognized and mounted to the correct location.</p>

Upgrade

Issue	Description
LOG-17317	<p>Previously, the Logger System License/Update page did not prevent users from accidentally trying to upgrade their Logger Appliance using a Software Logger upgrade script.</p> <p>FIX: If a software .enc upgrade file is imported to a Logger Appliance, Logger will display the error message: "Upgrade failed. Invalid enc file".</p>
LOG-16576	<p>Appliance upgrade sometimes did not set file permissions correctly, causing the upgrade to fail.</p> <p>FIX: Appliance upgrades now handle permissions properly.</p>
LOG-16571	<p>When upgrading to Logger 6.2, the installer timed out if the mount locations if they were in the /opt/mnt directory.</p> <p>FIX: The Logger upgrade installer can now complete the upgrade even when the mount locations are in the /opt/mnt directory.</p>

Open Issues

This release contains the following open issues.

• Analyze/Search	33
• Configuration	37
• Dashboards	40
• Localization	40
• Reports	40
• Summary	43
• System Admin	44
• Upgrade	45

Analyze/Search

Issue	Description
LOG-17440	<p>Column and Stacked Column chart types improperly display in a single column when the search string includes the CHART operator or the TOP operator.</p> <p>Workaround: Use the chart settings icon to change the chart type to something else, such as a bar or pie chart.</p>
LOG-17419	<p>When you index a field, Logger will not display that field with coloring that indicates that the field is indexed. This issue can be seen in the following locations:</p> <p>Analyze > Search</p> <ul style="list-style-type: none">- Selected Fields list- Selected Fields detail window- Field set dropdown > Customize > Customized Fields dialog box <p>However, the column header in the search results will display the correct color.</p> <p>Workaround: Restart the Logger web and server processes to display the correct color in all locations.</p>

Issue	Description
LOG-17318	<p>If you check the Rerun Query checkbox when exporting search results, the download may not include all search results if it is started before the query finishes running.</p> <p>Understanding: In the current release, exported searches download a maximum of 1 million search results. However, when exporting search results with close to or over 1M hits with the re-run query checked, Logger may display the "Download results" link before the export file has finished populating. If you try to download the report during this period, the downloaded file might have only 100K or 600K lines instead of the final 800K or 1M lines.</p> <p>Workaround: There is no current way to tell when the file is ready for download from the User Interface. Wait a few minutes before downloading to get the full export file.</p>
LOG-17215	<p>When you perform a lookup search query including an IP data type field and top or chart operator, you may see an "unsupported data type" error.</p> <p>Workaround: None at this time.</p>
LOG-17191	<p>When searching using a lookup file, Logger generates parsing errors for IP data type fields.</p> <p>Workaround: None at this time.</p>
LOG-16429	<p>When Source Types sharing a common dependent parser are exported with the property "overwrite.same.content" turned on, importing such source types will only keep the most recently imported one having its parser: the other source types won't have their parser included in their definition.</p> <p>Workaround: Turn off "overwrite same content" before importing.</p>
LOG-16348	<p>When exporting search results with all fields included, custom fields are not exported.</p> <p>Workaround: Avoid using the custom fields and use fields such as deviceCustomString1, deviceCustomNumber1, and so forth, to store the customized values.</p>
LOG-16347	<p>Pipeline queries that include the WHERE operator, and exclude the '*user' field from a custom field list, display no results for the custom fields.</p> <p>For example, this query (missing the '*user' field from the custom field list): <code>_deviceGroup IN ["192.164.16.202 [SmartMessage Receiver]]") where deviceEventClassId = "agent:050"</code> Does not return the value 'agent:050' in the deviceEventClassId field of the search results.</p> <p>Workaround: Include the '*user' field from the custom field list in the query.</p>
LOG-15972	<p>If you run a forensic search using an Event Archive that has been partially archived from local storage, the archive may not load. Examples include searching for events prior to a certain time on the first day of the month, or if local memory already contains events from that archive for that 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> <p>Workaround: In the text box, type <code>\$\$\$<SavedSearchName></code> or <code>\$filter\$<FilterName></code> and then click Saved Search or Filter in the dropdown list to load it.</p>

Issue	Description
LOG-14778	<p>If a Receiver is deleted and re-created, 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-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. 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 Technical Support for a more detailed workaround.</p>
LOG-14266	<p>After updating the daily Archive task setting, you may not be able to see the event with a query like: message = "Daily archive task settings updated".</p> <p>Workaround: Use either of the following two queries to find the event: 1) message CONTAINS "Daily archive task settings updated" or 2) message STARTSWITH "Daily archive task settings updated"</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-12524	<p>If the value for a discovered field contains a colon (:), an ampersand (&), or angle brackets (<>), the query generated by clicking on it will escape the character with an added slash (\).</p> <p>Workaround: Remove the backslash from in front of the character. 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, if the original field name is included in the fieldset used in the search, the original field renamed by the operator is still displayed as a column in the search results, but will not have any values.</p> <p>For example, if the search uses the All Fields fieldset, 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-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 export all of the corresponding events correctly.</p>

Issue	Description
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>
LOG-11225	<p>When using the auto complete feature on the Search page, if the query has a double quote followed by 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 "\"[opt/mnt/soft/logger_server.log.6] successfully.\"\"", then after removing them, the query becomes "[opt/mnt/soft/logger_server.log.6] successfully." You can also do this when double quote is followed by any special character such as "\", "/", "[", "]", 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) GMT displays in timestamps with timezones, 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 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": replace "**john*" with "**johnny"</p> <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 the value 'Logger Session Inactivity Timeout'. The default timeout is 15 minutes.</p> <p>Workaround: Use an external browser to see results.</p>

Issue	Description
LOG-7864	<p>The time in the 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-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-5181	<p>Search results are not highlighted when there are multiple values that match the IN operator in a query.</p> <p>Workaround: None available 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>

Configuration

Issue	Description
LOG-17433	<p>When you delete a Logger TCP or UDP receiver, the port on which the receiver was listening will remain open in the firewall.</p> <p>Workaround: None at this time.</p>
LOG-17356	<p>On Logger L7600 appliances, when Logger 6.2 Patch 1 is upgraded to Logger 6.3, the License information page under Configuration tab, the license properties appear unavailable.</p> <p>Workaround: When the appliance is rebooted, the license information page accurately shows the license properties.</p>

Issue	Description
LOG-17049	<p>Fields created by parsers are not displayed.</p> <p>Workaround: Use one of the following workarounds to see the data.</p> <ul style="list-style-type: none"> - View the Raw data in the Logger search results. - Export the search results and use an audit or compliance application to parse that data. - Use an ArcSight SmartConnector to parse the events and generate a csv file with the parsed fields.
LOG-16379	<p>For Software Logger installed on Redhat 7.1 or higher OS version, the configuration push by ArcMC fails to push the SNMP destination to the target Logger.</p> <p>Workaround: Option 1: Push the config again to the destination Logger. Option 2: Manually add the SNMP destination on the target logger.</p>
LOG-16024	<p>When platform:230 and platform:201 events are forwarded from Logger to an ESM manager, the device host name and device address are converted to localhost and 127.0.0.1 respectively.</p> <p>Workaround: None available at this time.</p>
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> <p>Workaround: None available at this time.</p>
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-13226	<p>A user can edit a forwarder while the forwarded is enabled. This can cause the forwarder to stop sending events.</p> <p>Workaround: Before editing the forwarder, disable it. Then edit it and re-enable it to have the forwarder send events to its target destination.</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 cause the setup program 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> <p>Workaround: Restart the Logger.</p>

Issue	Description
LOG-11176	<p>When you enable a Receiver, Logger does not validate the Research File System (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-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-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. Examples of improper tear-downs include when one of the Loggers is replaced with a new appliance and when 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-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-17393	<p>When creating a new dashboard, Logger might show the validation error "Dashboard name already exists," even though the user does not have a dashboard with that name.</p> <p>Workaround : Give the dashboard a different name.</p>
LOG-16998	<p>The system filters "Root Partition Below 10 Percent" and "Root Partition Below 5 Percent" are missing a space in the default query, which can result in incorrect search results.</p> <p>Workaround: Add the missing space before running the query. For example, for this query:</p> <pre>cn1=([0-9] 0[0-9]).*</pre> <p>Add a space between the closed parenthesis and the period (cn1=([0-9] 0[0-9]) .*) to generate correct results.</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> element contains Chinese characters. This causes the Secure Copy Protocol (SCP) command to fail, if you use SCP only in the Target backup server for Secure Copy.</p> <p>Workaround: Use openSSH for configuration backups.</p>

Reports

Issue	Description
LOG-17120	<p>Non-ASCII characters in a report name can be corrupted when customizing the report. The behavior occurs only on IE11, and depends on the timing of user actions.</p> <p>Workaround: After saving the report, reload the browser. Navigate to Reports > Report Explorer, select the report, and check if the original report name is still correct. If not, fix the name in the report's Properties.</p>
LOG-16880	<p>Logger reports published in iHTML format generate an empty file.</p> <p>Workaround: None at this time. Use the HTML report format, or another report format of your choice, instead.</p>

Issue	Description
LOG-16597	<p>When search results for the arc_destinationProcess name field are more than 30 characters long, Logger Reports may truncate the field.</p> <p>Workaround: Please contact HPE ArcSight Technical Support for help with this issue.</p>
LOG-16589	<p>When a peer is removed from a peer Logger configuration, scheduled peer reports may default to the "Local Only" option, and not search the remaining peers.</p> <p>Workaround: Check all scheduled reports and assign peers after any changes made to the peer configuration.</p>
LOG-16405	<p>From the Logger user interface, users can be assigned rights to view, run or schedule specific reports that may not be part of their default privileges. When the same report is run through the SOAP API, those rights don't apply, and the report can only be run when the individual has the right to "View, run, and schedule all reports."</p> <p>Workaround: None at this time.</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 available 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-16281	<p>Peer reports fail when Logger is peered with ESM 6.8c. This happens because the database type of the event field "arc_sourceAddress" is different for Logger and ESM.</p> <p>Workaround: None available at this time.</p>
LOG-15462	<p>When the file system /opt/arcsight/userdata is full, Logger allows users to run reports, even though they necessarily fail. Logger does not warn users in advance that the free space on the file system is full. This is important for scheduled reports.</p> <p>Workaround: Check the amount of free space periodically.</p>
LOG-15056	<p>If you install a Logger solution (such as Payment Card Solutions (PCI), IT Governance (ITGov), or Sarbanes-Oxley (SOX)) before you have opened the Reports page at least once, some report categories are not available.</p> <p>Understanding: This happens if the Logger reports engine has not yet been initialized when the Solutions package is installed. The Foundation, SANS Top5, and Device Monitoring reports are affected.</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-14386	<p>If you open the Reports Dashboard in an Internet Explorer 11 window that is less than 1450px wide, the Reports menu is not displayed.</p> <p>Workaround: When working with Internet Explorer 11, always make your window wider than 1450px.</p>

Issue	Description
LOG-13373	<p>Report "Execution Status" doesn't list the most recent Jobs by default.</p> <p>Workaround: Navigate to the first page manually by clicking on the appropriate icon.</p>
LOG-13372	<p>When user clicks on the graph at the top of the "Job Execution Status" page and then clicks "Last Run Status" table in the popup window, an error message appears.</p> <p>Workaround: Click directly on the table at the bottom of the "Job Execution Status" page.</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 restrictions apply to all run-time parameters.</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 usually opens with unexpected results, since '-' does not match the query.</p> <p>Workaround: None available 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 available at this time.</p>

Issue	Description
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>
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 available at this time. Currently, there is no way to specify the search time range in milliseconds.</p>

System Admin

Issue	Description
LOG-17072	<p>If you apply a Standalone Logger license on a Logger with an installed ADP license, or conversely, if you apply an ADP Logger license on a Logger with an installed standalone license, Logger won't work as expected.</p> <p>Workaround: Call Support for assistance in applying the proper license.</p>
LOG-16759	<p>SNMP polling for power supply, fan and temperature parameters is not supported on HPE Proliant appliances.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Install the following two RPM files on your ArcSight appliance:<ul style="list-style-type: none">- hp-health-10.40-1777.17.rhel7.x86_64.rpm- hp-snmp-agents-10.40-2847.17.rhel7.x86_64.rpm2. Download the following MIB files and copy them to the /usr/share/snmp/mibs folder on your ArcSight appliance:<ul style="list-style-type: none">- cpqhlth.mib- cpqhost.mib- cpqsinfo.mib3. Import the MIB files into the network management system. <p>Download links:</p> <p>For HPE Health and HPE SNMP Agent RPMs:</p> <p>http://downloads.linux.hpe.com/SDR/repo/spp/RedHat/7/x86_64/current/</p> <p>For Proliant MIB kit:</p> <p>http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04272529</p>
LOG-16757	<p>Logger users can be deactivated due to the date_last_active database field not updating when the user logs in. Expected behavior would be that the field gets updated anytime a user successfully authenticates.</p> <p>Workaround: To disable this feature and avoid the issue, open System Admin > Users/Groups > Authentication. On the Sessions tab, remove the check from the Disable Inactive Account After checkbox.</p>
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. You can most likely ignore this; the processes are probably in the "running" state.</p> <p>Workaround: The UI will display the correct state at the next automatic refresh or if you manually click Refresh Status.</p>

Issue	Description
LOG-15490	<p>In rare circumstances during a data migration to an L7600 appliance, some processes will not restart on the target machine after the reboot.</p> <p>Workaround: Use SSH to restart all processes manually using this command: /opt/local/monit/bin/monit restart all</p>
LOG-15456	<p>The 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-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-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>

Upgrade

Issue	Description
LOG-17404	<p>If the OS is upgraded to RHEL 7.2 after Logger is upgraded, the Receivers process will fail to start.</p> <p>Workaround: Log in as root and run the command '/sbin/ldconfig' before starting Logger.</p>
LOG-17236	<p>Report Administration configuration values may revert to Logger defaults after upgrading a Software Logger to Logger 6.3.</p> <p>Understanding: Logger 6.3 implements a new type of license. Because of this, existing licenses are no longer valid. Upgraded Loggers will have a 90-day trial license, which disables reporting.</p> <p>Workaround: Apply the new license, and restart/reboot the upgraded Loggers. If not this does not restore the settings, you will have to manually restore them.</p>
LOG-17065	<p>In some cases, the SmartMessage Receiver has significantly lower incoming EPS after an upgrade. This causes connectors to cache heavily.</p> <p>Workaround: Restart Apache process using the 'loggerd restart apache' command.</p>
LOG-16711	<p>On Logger L7600 series appliances, the user interface may not refresh when the upgrade is finished.</p> <p>Workaround: If the upgrade is in progress for a long time, refresh the screen. If the login screen appears, the upgrade is done and you can log back in.</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 6.3)

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!