



# Micro Focus Security ArcSight Logger

Software Version: 6.7.1

## Release Notes

Document Release Date: May, 2019

Software Release Date: May, 2019

## Legal Notices

### Copyright Notice

© Copyright 2019 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

# Contents

- Logger 6.7.1 Release Notes ..... 5
  - What's New in this Release ..... 5
  - Technical Requirements ..... 6
    - Supported Platforms ..... 6
  - Connecting to the Logger User Interface ..... 7
  - Logger Documentation ..... 8
  
- Localization Information ..... 9
  - Known Limitations in Localized Versions ..... 9
  
- Upgrading to Logger 6.7.1 (L8253) ..... 10
  - Upgrade Paths ..... 10
  - Verifying Your Upgrade Files ..... 10
  - Upgrading the Logger Appliance ..... 11
    - Prerequisites ..... 11
    - Upgrade Instructions ..... 12
  - Upgrading Software Logger and Logger on a VMWare VM ..... 14
    - Prerequisites ..... 14
    - Increasing the User Process Limit ..... 15
    - Editing the logind Configuration File for RHEL 7.X ..... 16
    - Upgrade Instructions ..... 16
  
- Known Issues ..... 21
  
- Fixed Issues ..... 22
  - Upgrade ..... 22
  - Analyze/ Search ..... 22
  - System Admin ..... 23
  - Configuration ..... 23
  - Dashboards ..... 23
  - Reports ..... 24

General .....	24
Open Issues .....	25
Alerts/Filters .....	25
Analyze/Search .....	26
Configuration .....	30
Dashboards .....	32
General .....	33
Localization .....	33
Reports .....	33
Summary .....	36
System Admin .....	36
Upgrade .....	37
Security Fixes .....	38
Documentation Errata .....	39
Send Documentation Feedback .....	40

# Logger 6.7.1 Release Notes

These release notes apply to the Security ArcSight Data Platform (ADP) Logger and standalone ArcSightLogger, version 6.7.1 (L8253) releases. 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 Security ArcSight Logger 6.7.1 release (L8253) is a maintenance release, addressing and resolving issues found in Logger 6.70.

In addition, an improvement has been made for **Event Broker** :

Without additional configuration, the user is now able to add an EB receiver in an IP Address or hostname format.

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

- ["Fixed Issues" on page 22](#)
- ["Open Issues" on page 25](#)
- ["Security Fixes " on page 38](#)

For details about these features, see the ArcSight Logger 6.7.1 Administrator's Guide, available from the [ArcSight Product Documentation Community on Protect 724](#).

# Technical 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"><li>• CPU: 2 x Intel Xeon Quad Core or equivalent</li><li>• Memory: 12–24 GB (24 GB recommended)</li><li>• Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data.</li><li>• Root partition: 40 GB (minimum)</li><li>• Temp directory: 1 GB</li></ul> <p><b>Note:</b> 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"><li>• CPU: 1 or 2 x Intel Xeon Quad Core or equivalent</li><li>• Memory: 4–12 GB (12 GB recommended)</li><li>• Disk Space: 10 GB (minimum) in the Logger installation directory</li><li>• Temp directory: 1 GB</li></ul>
VM Instances	<ul style="list-style-type: none"><li>• 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 7.6 configured with 12 GB RAM and four physical (and eight logical) cores.</li><li>• Micro Focus ArcSight strongly recommends allocating a minimum of 4 GB RAM per VM instance.</li><li>• The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.</li></ul>
Other Applications	<ul style="list-style-type: none"><li>• For optimal performance, make sure no other applications are running on the system on which you install Logger.</li></ul>

## Supported Platforms

Refer to the ADP Support Matrix, available on the Protect 724 site for details on Logger 6.7.1 platform support.

**Note:** Be sure to upgrade your operating system (OS) to get the latest security updates. Upgrade your OS first, and then upgrade Logger. For Logger Appliances, an OS upgrade file is included in your upgrade package.

## Connecting to the Logger User Interface

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 6.7.1 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.

**Note:** While logged in to the Logger UI, be careful not to click on suspicious links from external sources (e.g. emails, websites) as they may contain malicious code that could get executed by the browser.

# Logger Documentation

The new documentation for this release comprises these Release Notes, and updated versions of the ArcSight Data Platform Support Matrix and ADP 2.4.1 Release Notes. The complete Logger 6.7 documentation set also applies to this release.

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

- **Logger 6.7 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 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 6.7 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 6.7 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 6.7 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.
- The Report Parameter and the Template Style fields do not accept native characters.
- The following Logger user interface section is not localized: Field Summary.
- 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 6.7.1 (L8253)

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

- ["Verifying Your Upgrade Files" below](#)
- ["Upgrading the Logger Appliance" on the next page](#)
- ["Upgrading Software Logger and Logger on a VMWare VM" on page 14](#)

**Note:** Be sure to review the sections ["Known Issues" on page 21](#), ["Fixed Issues" on page 22](#), and ["Open Issues" on page 25](#) before upgrading your logger.

## Upgrade Paths

The following table lists the upgrade paths to Logger 6.7.1. 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 Micro Focus 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 6.7.1 Upgrade Paths	
Software Versions	6.7
Appliance Models	L350X, L750X, L750X-SAN, L760X
Operating System Upgrades	<ul style="list-style-type: none"><li>• 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.</li><li>• Refer to the ADP Support Matrix document available on the Protect 724 site for a list of supported Operating Systems.</li></ul>

## Verifying Your Upgrade Files

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

Visit the following site for information and instructions:

<https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do>

# Upgrading the Logger Appliance

This section describes how to upgrade the Logger appliance. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 6.7, available for download from the [ArcSight Product Documentation Community on Protect 724](#).

## 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 6.7 prior to upgrading to Logger 6.7.1.
- Logger requires a root password. If your Logger does not have a root password already, give it one before performing the upgrade.
- Upgrade your OS to the latest supported RHEL distribution before you upgrade Logger. (Logger 6.7.1 includes OS Upgrade files for this purpose.)

This is important even if you upgraded your OS when upgrading to Logger 6.7, because the latest OS distribution fixes additional security vulnerabilities.

**Tip:** When upgrading through multiple releases, don't skip applying the OS upgrade files. You must apply each in turn when you upgrade to that version. Refer to the Support Matrix and Release Notes for the upgrade version for more information.

- Download the upgrade files from the Micro Focus [Customer Support site](#) to a computer from which you connect to the Logger UI.
  - For local or remote appliance upgrades, download the following file:  
**logger-8253.enc**
- For OS upgrades, download the appropriate file:
  - If you are upgrading an Lx500 series appliance, download the following file:  
**osupgrade-logger-rhel610-`<timestamp>`.enc**
  - If you are upgrading an Lx600 series appliance, download the following file:  
**osupgrade-logger-rhel176-`<timestamp>`.enc**
- Verify the upgrade files, as described in "[Verifying Your Upgrade Files](#)" on the [previous page](#).
- Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).

## Upgrade Instructions

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the ["Prerequisites"](#) on the [previous page](#) before you begin.

- To upgrade Logger from ArcMC, see ["To upgrade Logger Appliances remotely through ArcMC:"](#) below
- To upgrade Logger locally, see ["To upgrade a Logger Appliance locally:"](#) below

### To upgrade Logger Appliances remotely through ArcMC:

1. Upgrade your OS as appropriate.
  - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file **osupgrade-logger-rhel610-`<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-rhel176-`<timestamp>`.enc** and following the instructions in the ArcSight Management Center Administrator's Guide.

**Note:** Be sure to apply the OS upgrade even if you already upgraded to the OS to 6.10 or 7.6 for Logger 6.7, because the latest OS distribution fixes additional security vulnerabilities.

2. Deploy the Logger upgrade by using the file **logger-8253.enc** and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Reboot the Logger for the upgrade to take effect.
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.

### To upgrade a Logger Appliance locally:

1. Log into Logger and click System Admin | System > **License & Update**.
2. Upgrade your OS as appropriate.
  - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file **osupgrade-logger-rhel610-`<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-rhel176-`<timestamp>`.enc** and following the instructions in the ArcSight Management Center Administrator's Guide.

**Note:** Be sure to apply the OS upgrade even if you already upgraded to the OS to 6.10 or 7.6 for Logger 6.7, because the latest OS distribution fixes additional security vulnerabilities.

3. Browse to the **logger-8253.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.

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.

# Upgrading Software Logger and Logger on a VMWare VM

This section describes how to upgrade Logger. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 6.7, available for download from the [ArcSight Product Documentation Community on Protect 724](#).

## 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 6.7 prior to upgrading to Logger 6.7.1.
- Upgrade your Operating System (OS) to a supported version before upgrading Logger. This is important even if you upgraded your OS when upgrading to Logger 6.7, because the latest OS includes important security updates. 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 the latest version of 7.6.
  - If your system is running on RHEL or CentOS 6.X, upgrade to the latest version of 6.10.
  - If not already done on the system, perform the following procedures:
    - 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 16.
- A non-root user account must exist on the system on which you are installing Logger, or the installer will ask you to provide one. Even if you install as root, a non-root user account is still required. The userid and its primary groupid should be the same for this account. The UID for the non-root user should be 1500 and the GID should be 750. For example, to create the non-root user, run these commands as **root**:  

```
groupadd -g 750 arcsight  
useradd -m -g arcsight -u 1500 arcsight
```

These commands create a non-root user named **arcsight** that will work with a Logger software installation.
- Download the Software Logger upgrade files from the Micro Focus [Customer Support site](#).

- For remote upgrades using ArcMC, download the following file:  
**logger-sw-8253-remote.enc**
- For local upgrades, download the following file:  
**ArcSight-logger-6.7.1.8253.0.bin**
- Logger documentation is not included in your download package. Download your documentation from the [ArcSight Product Documentation Community on Protect 724](#).
- Verify the upgrade files, as described in ["Verifying Your Upgrade Files" on page 10](#).

## 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 6.10 and 20 for RHEL and CentOS 7.6.)
  - 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.X, 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

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the "[Prerequisites](#)" on [page 14](#) before you begin.

- To upgrade Logger from ArcMC, see "[To upgrade Software or VMWare Loggers remotely through ArcMC:](#)" below.
- To upgrade Software Logger locally, see "[To upgrade Software Logger locally:](#)" on the next page.
- To upgrade Logger on VMWare locally, see "[To upgrade Logger on VMWare VM:](#)" on [page 18](#).

### To upgrade Software or VMWare Loggers remotely through ArcMC:

1. Upgrade your OS to the latest distribution. This is important even if you upgraded your OS when upgrading to Logger 6.7, because the latest OS distribution fixes additional security vulnerabilities.

**Note:** Remote OS upgrade is not supported for Software Logger. Perform the OS upgrade manually before upgrading Logger.

2. Deploy the downloaded upgrade file, **logger-sw-8253-remote.enc**, by following the instructions in the ArcSight Management Center Administrator's Guide.



## To upgrade Software Logger locally:

1. Log in with the same user name as the one used to install the previous version of Logger.
2. Run these commands from the directory where you copied the Logger software:

```
chmod u+x ArcSight-logger-6.7.1.8253.0.bin  
./ArcSight-logger- 6.78253.0.bin
```

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.

3. 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.
4. Select **I accept the terms of the License Agreement** and click **Next**.
5. 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.
6. 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:** Micro Focus 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.

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

7. 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.

8. 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.  
Click **Upgrade** to continue or **Back** to specify another location.
9. 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.
10. Click **Next** to initialize Logger components.  
Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
11. 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.
12. Make a note of the URL and then click **Done** to exit the installer.
13. Restart Logger to put the upgrade changes into effect.
14. You can now connect to the upgraded Logger.
15. 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. Log in with the same user name as the one used to install the previous version of Logger.
2. Run these commands from the `/opt/arcsight/installers` directory:

```
chmod u+x ArcSight-logger-6.7.1.8253.0.bin  
./ArcSight-logger-6.7.1.8253.0.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  
6.7.1.
```

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

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

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

PRESS <ENTER> TO CONTINUE:

3. 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:** Micro Focus 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.
  - 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. Restart Logger to put the upgrade changes into effect.

14. You can now connect to the upgraded Logger.

15. 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 issue applies 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 Micro Focus Customer Advisory document: <https://www.microfocus.com/support-and-services/>

## **SMTP Server Settings**

SMTP configuration in the report section was available for Logger v.6.6. However, this option has been removed for v.6.6.1 as the SMTP server settings are now centralized. SMTP is configured from the **System Admin> SMTP** option. If you are upgrading to this version, make sure to update the settings from **System Admin** section. If no configuration is made, it can cause an impact on schedule reports, as SMTP settings from admin overrides the SMTP settings from reporting.

## **L7600 appliance storage volume extension:**

After an upgrade to Logger 6.7.1, the appliance displays by default a 12TB of storage volume limit. Set to true the flag `eventstore.G9.size.extension` to extend the storage volume size to 16TB. Otherwise, **Configuration> Maintenance operations** will display a message of insufficient free space to increase storage volume size. Other initialization processes will automatically display 16TB as storage volume limit.

## Fixed Issues

The following issues are fixed in this release.

- [Upgrade](#) .....22
- [Analyze/ Search](#) ..... 22
- [System Admin](#) .....23
- [Configuration](#) .....23
- [Dashboards](#) ..... 23
- [Reports](#) ..... 24
- [General](#) ..... 24

## Upgrade

Issue	Description
LOG-21441	One of the Logger validation processes was not updated with the correct OS version supported. Fix: Issue has been fixed.
LOG-21259	When Parser was upgraded on SmartConnector, only the framework version was updated on Logger device Version Column. Fix: Logger Parser version is correctly displayed in the device.
LOG-17404	When a non-root Logger that were running as a service upgraded OS to RHEL 7.2, the receiver process failed to start. Fix: Log in as root and run the command '/sbin/ldconfig' before starting Logger.

## Analyze/ Search

Issue	Description
LOG-21471	"Enable Global ID" box was not checked after fresh install or 6.7 upgrade despite it was set by default. Fix: Save the Global ID configuration. Once it is saved, the actual behavior and the UI of Global ID configuration is consistent.
LOG-21808	When the Global ID was enabled, a lot of BufferOverflowException were displayed in Logger Receiver. Fix: Issue has been fixed.

## System Admin

Issue	Description
LOG-21517	User was disconnected from SSH session after a 60 second period of inactivity. Fix: Now, user is disconnected after a 15 minute period of inactivity.

## Configuration

Issue	Description
LOG-21437	When saving the information for the first time, SMTP data synchronization displayed an error. Logger and Report Engine synchronization took more time than time out range period. Fix: Time out period has been extended.
LOG-21432	"User was unable to save a SMTP configuration after it retrieved an exception. Logger displayed the following message: We encountered a problem saving the data. Try saving the data again. Error SMTP is on synchronization, please try again later. Fix: SMTP configuration can be saved.
LOG-21398	After an upgrade from Logger 6.6.x to 6.7.0, Backup SMTP server port was not seen in the UI. Fix: Backup SMTP server port is visible in the UI after upgrade to 6.7.1.
LOG-21377	Logger Web Process was running out of memory when Logger Dashboard was refreshed constantly. Fix: memory has been increased.
LOG-12227	When it was configured eth0 with a static IP netmask and gateway & eth1 with a different static IP in a Logger with RHEL 6.1, one of the NCIS configured interface dropped the incoming packets. Fix: Issue has been fixed.
LOG-21339	User was unable to create an eventbroker receiver as an error message was displayed when entered the hostname for the eventbroker Kafka node servers. Fix: Receiver with EB broker nodes in either an IP Address or hostname format can be successfully added.

## Dashboards

Issue	Description
LOG-21402	Cancel button on Dashboard > Saved Search disappeared while saved search was being executed. Fix: Cancel button remains available until saved search process is completed.

## Reports

Issue	Description
LOG-21580	<p>When Logger search result was exported to a CSV format, odd characters were displayed instead of the original Chinese characters.</p> <p>Fix: Chinese characters are displayed correctly.</p>
LOG-21541	<p>Customer was unable to generate a report with graphics in PDF format. If a report was previously executed and later exported in PDF or Word, graphic was not retrieved.</p> <p>Fix: Reports with graphics are now executed and exported in any format.</p>
LOG-20126	<p>When Logger search result was exported to a CSV format, original Chinese characters were not correctly displayed.</p> <p>Fix: Chinese characters are displayed correctly.</p>
LOG-21223	<p>When exporting an SMART report in MS Excel format, results were in blank.</p> <p>Fix: results are correctly displayed in all formats.</p>
LOG-19646	<p>Upcoming jobs were displayed in Job Execution Status page.</p> <p>Fix: Upcoming jobs are not longer displayed in Job Execution Status page</p>

## General

Issue	Description
LOG-21472	<p>The following sections were not updated in the 6.7 online help:</p> <ol style="list-style-type: none"><li>1. Retrieve Logs.</li><li>2. Storage Volume.</li><li>3. SSH Access to Appliance.</li><li>4. Using Global ID.</li><li>5. The Smart Report Designer.</li><li>6. Report Filters.</li></ol> <p>Fix: Information has been added</p>



# Open Issues

This release contains the following open issues.

- Alerts/Filters .....25
- Analyze/Search .....26
- Configuration .....30
- Dashboards .....32
- General .....33
- Localization .....33
- Reports .....33
- Summary .....36
- System Admin .....36
- Upgrade .....37

## Alerts/Filters

Issue	Description
LOG-7658	<p>If a real-time alert and a saved search alert are created for the same event, the scheduled search alert may not trigger for several minutes after a real-time alert has triggered. Because saved search alerts are scheduled, there is a delay. In addition, if a saved search alert depends on internal events, which are flushed every 10 minutes, there might be an additional delay before the events are detected and the alert is triggered.</p> <p>Workaround: ArcSight recommends that you set the search time range to now-X minutes or higher, where X is the time set in the Schedule field for a saved search alert, to ensure that saved search alerts that depend on internal events are triggered as expected.</p>
LOG-21143	<p>The Report Engine does not support the operators like join, union, filter and sort for Logger Search data source.</p> <p>Workaround: Use the MySQL data source, this data source supports these operators (join, union, filter and sort).</p>

## Analyze/Search

Issue	Description
LOG-19261	<p>For Logger health events generated internally every minute, the values of destinationAddress and deviceAddress are 127.0.0.1 instead of the real IP address. This issue only affects Logger running under RHEL 7.X on software and appliance form factors.</p> <p>Workaround: On the machine that is reporting destinationAddress and deviceAddress as 127.0.0.1, do the following:</p> <ol style="list-style-type: none"><li>1- Get network adapter real names with: <code>.ls /sys/class/net/ or .ifconfig -s   cut -d'-' -f1</code> . It returns, for example: ens32.</li><li>2- Change Logger property with real network adapter name. Property file is located at <code>/opt/arcSight/logger/config/logger/logger.defaults.properties</code> and for appliances, and at <code>&lt;install_dir&gt;/current/arcSight/logger/config/logger/logger.defaults.properties</code> for software logger. Property name is <code>logger.network.interface.name</code>. default network adapter name is <code>eth0</code> . Set it with the value obtained from the previous step. For example, change it to <code>logger.network.interface.name=ens32</code>.</li><li>3- Restart logger.</li></ol>
LOG-18945	<p>If an insubnet parameter has the wrong syntax, no error is reported when running peer searches. For local searches, the error is reported as expected.</p> <p>Workaround: For peer searches that contain the insubnet operator, first run a local search to check for any syntax errors. If no error is reported, then the peer search can be executed properly.</p>
LOG-18189	<p>Searches expire while user is still active on Logger. Logger now supports concurrent searches in multiple tabs. Since all searches are kept in memory, the default expiration time for searches is ten minutes. Once the search is completed, the expiration time begins counting down.</p> <p>Workaround: A user with System Admin rights can set the search expiration time in the Configuration &gt; Search Options page. The search expiration time can be increased up to 60 minutes.</p>
LOG-17806	<p>After running a search from the Live Event Viewer in Internet Explorer or Firefox, searches that are loaded by clicking a dashboard from the Summary page may fail.</p> <p>Workaround: Use the Live Event Viewer from Chrome. For Firefox or Internet Explorer, copy the failing query from the search box, reopen the search screen, and paste the query into the search box to run the search manually.</p>
LOG-17318	<p>If you check the Rerun Query checkbox when exporting search results, the download may not include all search results. In the current release, exported searches download a maximum of 1 million search results. However, when exporting search results 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>

Issue	Description
LOG-17215	<p>When performing a lookup search query including an IP data type field and a top or chart operator, you may see an "unsupported data type" error.</p> <p>Workaround: None at this time.</p>
LOG-16429	<p>When Source Types with a common dependent parser are exported with the property "overwrite.same.content" turned on, Source Types imported will only keep the most recent one with its parser. The other Source Types will not have their parser included in their definition.</p> <p>Workaround: Turn off "overwrite same content" before importing.</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. For example, this query is missing the 'user' field from the custom field list and therefore has no results: <code>_deviceGroup IN ["192.164.16.202 &lt;span class="error"&gt;#91;SmartMessage Receiver#93;&lt;/span&gt;"]   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 saved 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>\$\$\$ &lt;SavedSearchName&gt;</code> or <code>\$filter\$ &lt;FilterName&gt;</code> and then click Saved Search or Filter in the dropdown list to load it.</p>
LOG-14266	<p>After updating the daily archive task setting, you may not be able to see the event with a query like: <code>message = "Daily archive task settings updated"</code>.</p> <p>Workaround: Use either of the following two queries to find the event: 1) <code>message CONTAINS "Daily archive task settings updated"</code> or 2) <code>message STARTSWITH "Daily archive task settings updated"</code>.</p>
LOG-13532	<p>When the time changes due to the end of Daylight Saving Time (DST) during 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 <code>12:59:59</code> or earlier and an end time of <code>2:00:01</code> or later.</p>
LOG-12524	<p>If the value for a discovered field contains a colon (:), an ampersand (&amp;), or angle brackets (&lt; &gt;), the query generated by clicking on it will escape the character with an added backslash (\).</p> <p>Workaround: Remove the backslash in front of the character. For example, if the query inserted by clicking the field is <code>IdentityGroup=IdentityGroup\;All</code>, then after removing the backslash, the query becomes <code>IdentityGroup=IdentityGroup;All</code>.</p>

Issue	Description
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. For example, if the search uses the All Fields fieldset, which has device EventClassId, and its query includes "rename deviceEventClassId as eventCID", then both device EventClassId and eventCID will be shown in the search results, but device EventClassId 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 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. This will export all of the corresponding events correctly.</p>
LOG-11299	<p>If you uncheck the rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail.</p> <p>Workaround: The rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.</p>
LOG-11225	<p>When using the auto complete feature on the search page, if the inserted query has a double quote followed by bracket ("[]), it will not be executed.</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 "\" &lt;span class="error"&gt; &amp;#91;/opt/mnt/soft/logger_server.log.6&amp;#93;&lt;/span&gt; successfully.\" ", then after removing them, the query becomes " &lt;span class="error"&gt; &amp;#91;/opt/mnt/soft/logger_server.log.6&amp;#93;&lt;/span&gt; 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 may present the following issues: 1) On the Search page, the Events grid in the search results does not show any information. 2) GMT is displayed in timestamps with timezones. 3) In Global Summary on the Summary page, the Indexing is reported one hour behind the current timestamp.</p> <p>Workaround: Change the system time zone to something more specific, such as /America/Los_Angeles.</p>
LOG-10126	<p>While using the replace operator, the "from" string is replaced twice if included in the replacement string. For example, the following command, when run against the data "john smith" will result in "johnny 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 is received out of order, the duration may appear to be negative.</p> <p>Workaround: Include the term "sort _eventTime" before the transaction term.</p>

Issue	Description
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>
LOG-6965	<p>When the time changes due to the start of Daylight Savings Time (DST) during the spring, the time is set ahead one hour; Consequently, the following issues are observed: 1) The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. 2) The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. 3) 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. 4) 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. 5) 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> <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>
LOG-21135	<p>When running a top operator search combined with lookup operator, search sometimes delivers accurate results and sometimes returns empty fields. For example running the following search on distributed logger: *lookup mylookup myfield as destinationAddress output * Top sourceAddress,destinationAddress,destinationHostName* all of the fields except destinationAddress are empty.</p> <p>Workaround: Not available at this moment.</p>
LOG-21891	<p>If a peer search is performed against an unavailable peer, no error message is displayed.</p> <p>Workaround: Check the logger_server.log to confirm the available peers.</p>

## Configuration

Issue	Description
LOG-18753	<p>When client authentication is enabled, Logger connects to one Event Broker cluster only. If client authentication is disabled, Logger connects to an indefinite number of Event Broker clusters.</p> <p>Workaround: When connecting another cluster with client authentication, clear the keystore before configuring. This can be done with the commands:</p> <p>1) List the keypairs by alias: <code>&lt;install_dir&gt;/current/local/jre/bin/keytool -list -keystore &lt;install_dir&gt;/current/arc sight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath &lt;install_dir&gt;/current/arc sight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar   grep -i private</code></p> <p>2) Delete the keypair with the alias from the previous command: <code>&lt;install_dir&gt;/current/local/jre/bin/keytool -delete -keystore &lt;install_dir&gt;/current/arc sight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath &lt;install_dir&gt;/current/arc sight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar -JDjava.security.egd= &lt;a href="file:/dev/urandom" class="external-link" rel="nofollow" &gt;file:/dev/urandom -alias &lt;alias(es) from previous command &gt;</code></p>
LOG-18542	<p>When using the Scheduled Archive drop-down filter on the Configuration &gt; Finished Tasks page, the UI displays an error message.</p> <p>Workaround: See the finished archive tasks, file the archived results on the Configuration &gt; Event Archives page.</p>
LOG-17433	<p>When deleting a Logger TCP or UDP receiver, the XML file (receiver parameters) is not deleted.</p> <p>Workaround: When deleting a receiver, manually delete the xml file too.</p>
LOG-16379	<p>For software Logger installed on Red Hat 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 configuration again to the destination Logger. Option 2: Manually add the SNMP destination on the target Logger.</p>
LOG-16349	<p>For a newly-installed Logger, report objects and queries are not available until you navigate to the Reports Dashboard (Reports &gt; 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-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. Configure LDAP as the authentication method from the Logger system Admin &gt; Authentication &gt; External Authentication page.</p>

Issue	Description
LOG-14778	<p>When running a search for a receiver deleted and re-created in the summary UI page (later redirected to Search Page and query by Device Groups) the search results do not include events after recreation.</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-14650	<p>You cannot export a filter that has been previously imported. 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 appears as "GMT-x", while the "GMT-x" time zone appears as "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 feature 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 despite it is correctly deleted from the Dashboards.</p> <p>Workaround: Restart the Logger.</p>
LOG-11176	<p>When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references.</p> <p>Workaround: Edit the Receiver to verify that the RFS mount is valid. Alternatively, verify the mount on the System Admin &gt; Remote File Systems page.</p>
LOG-10056	<p>You may see a duplicate device name if a receiver is removed and a new one is created with the same name as the old one. When you run a search, Logger uses the old device and you are not able to search on the new device.</p> <p>Workaround: Do not create a receiver with a name you have previously used.</p>
LOG-8790	<p>When forwarding alerts to SNMP, the trap displays "??" in the community field if the community string contains non-ASCII characters. 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>

Issue	Description
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>When the client tries to reestablish a relationship that contains an improper tear-down, Loggers involved may not detect it and operation 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 &gt; Configuration Backup &gt; Backup_name) and File Transfer Receivers (Configuration &gt; 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 logged. Check the log (Configuration &gt; 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>
LOG-21171	<p>When an UDP receiver is configured using a encoding different than UTF-8 or ASCII, Logger drops the non-cef events sent to that receiver.</p> <p>Workaround: change the encoding of the receiver to UTF-8.</p>
LOG-21346	<p>When you modify the Archive Path, the following message is displayed in the logs: "Event archive settings added". The quantity of messages shown depend on the number of existing storage groups.</p> <p>Workaround: None at this time</p>
LOG-21806	<p>Customized logo is not displayed when using IE browser.</p> <p>Workaround: Use Microsoft Edge or Google Chrome to view customized logo.</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: Name the dashboard differently.</p>



## General

Issue	Description
LOG-20698	When user update EB, previously configured running Logger receiver need to be disabled before or after upgrade, and re-enabled again to make sure receiver continue receiving events after EB upgrade.

## Localization

Issue	Description
LOG-15905	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.  Workaround: Use openSSH for configuration backups.
LOG-21628	When Logger search result is exported to a CSV format, odd characters are displayed instead of the original Chinese characters.  Workaround: Open CSV exported file from notepad. Otherwise, Export results in Excel format.

## Reports

Issue	Description
LOG-20360	When a user adds the field "name" while SecureData Configuration is enabled, the grid view of the report displays duplicate padlocks. The double line of padlocks does not affect this functionality.  Workaround: None at this time.
LOG-19958	The Report Engine could reach its capacity limits when several scheduled (3 or more) reports are configured to run at the same time in different formats. Depending on the final size of the files generated, the system reaches its capacity during the first or second scheduled execution. This is one of the error messages displayed: "Report server reached the capacity limits error and not able to create reports." Similar error messages are displayed based on different scenarios.  Workaround: Contact Support.
LOG-19469	When using a filter or a saved search to create reports from Logger Search Queries, the report is executed correctly. However, when the user updates the filter or the saved search with a different query, the report does not run properly.  Workaround: Re-create reports using the same query object.

Issue	Description
LOG-19423	<p>The Report Engine might reach its capacity limits when several scheduled reports (3 or more) are configured to run at the same time in different formats. Depending on the size of the files generated, the system reaches its capacity on the first or second scheduled execution and this error message (or similar) pops, "Report server reached the capacity limits error and not able to create reports".</p> <p>Workaround: Contact support.</p>
LOG-16589	<p>When a peer is removed from a peer Logger configuration, scheduled peer reports changed to the default "Local Only" option, and do not search in the remaining peers.</p> <p>Workaround: Check all scheduled reports and assign peers after making changes to 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 do not apply; 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-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-15726	<p>Some reports contain translation errors when they are displayed in Japanese.</p> <p>Workaround: None 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. This happens when the Logger reports engine has not yet been initialized during the Solutions package installation. 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 is now 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>Installation of multiple Solution Packages in Software Loggers with a root user may fail if the SOX v4.0 solution package is installed before others.</p> <p>Workaround: If you are installing the SOX v4.0 solution package on Software Logger with a root user, leave this step for the end.</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>

Issue	Description
LOG-9620	<p>If a distributed report in the background fails to run 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>
LOG-21052	<p>Several columns are not displayed in a report previously saved.</p> <p>Workaround: None available at this time.</p>
LOG-21067	<p>Split charts cannot be exported.</p> <p>Workaround: None available at this time.</p>
LOG-20346	<p>When the user attempts to export a published Logger Search Report close to be removed due to expiration time, an error occurs as the Report Engine is changing from dynamic to static.</p> <p>Workaround: Re-run and published the Logger Search report again.</p>
LOG-21358	<p>When the user executes any Smart report, the Report Server runs the Query and fetches the data to later provide format and serialize it. The status is set to completed as the execution is complete from Report Server. However, the front-end UI it is still loading in the grid.</p> <p>Workaround: Allow time as report execution and rendering are slow-paced processes</p>
LOG-21361	<p>In Dark Theme, "Dashboards" and "Dashboard Items" labels are not visible when dashboard page is displayed.</p> <p>Workaround: Use Light Theme instead.</p>
LOG-21365	<p>The user is not able to scroll down in the Classic Dashboard page.</p> <p>Workaround: None at this time</p>
LOG-21738	<p>When the user saves the report twice from Ad Hoc Report Designer, this one is not displayed in Explorer page nor it appears on Default Logger Search Reports.</p> <p>Workaround: In Administration &gt; Report Categories, look for the report and switch it from private to public.</p>
LOG-21380	<p>When the user creates a filter and a report with a storage group, results are retrieved with a significant delay.</p> <p>Workaround: Allow more time when creating filters and reports containing a storage group.</p>
LOG-21389	<p>When executing the Daily Byte Count Report, an unexpected error message is displayed.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Login to Logger as Admin User</li> <li>2. Click on Reports tab</li> <li>3. Click on Explorer &gt; Logger Administration</li> <li>4. Customize Daily Byte Count report (Refer 9301_1.png)</li> <li>5. Click on Data Source tab</li> <li>6. Select Daily Byte Count query object again(Refer 9301_2.png)</li> <li>7. Click on Save button and verify the behavior</li> </ol>

Issue	Description
LOG-21397	When you export a report, the labels are not being correctly exported in pdf and excel format. Workaround: Use the Word format to export a reports that include labels.
LOG-21757	Published reports are not displayed when using IE browser. Workaround: Use Microsoft Edge or Google Chrome to view published reports.
LOG- 21786	When the user drags and drops a category and also the report as a widget, no data is displayed. Workaround: None available at this time.

## Summary

Issue	Description
LOG-9772	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. The granularity of time used for the Summary page is different from the Search page. Therefore, the numbers are different. Workaround: None available at this time. Currently, there is no way to specify the search time range in milliseconds.

## System Admin

Issue	Description
LOG-15490	In rare circumstances during a data migration to an L7600 appliance, some processes do not restart on the target machine after the reboot. Workaround: Use SSH to restart all processes manually using this command: <code>/opt/local/monit/bin/monit restart all</code>
LOG-14595	The following message is displayed in Logger appliances: "error: Bind to port 22 on 0.0.0.0 failed: Address already in use." gets logged every minute to /var/log/secure. Workaround: This message appears only if SSH access has been enabled, and can be ignored. The SSH daemon erroneously restarts every minute even if already running.
LOG-11700	Users may be unable to log in after they have been removed from a group. For instance, removing all group assignments from a user, effectively disables that user account. Workaround: To avoid disabling a user account, check that the user is assigned to the correct groups.

## Upgrade

Issue	Description
LOG-16711	<p>On Logger L7600 series appliances, the user interface may not refresh once the upgrade has 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>
LOG-21446	<p>Unable to start Logger Linux installation as Cloud Linux images (AWS EC2 and Azure VM images) are light by nature (RH7.5 and CentOS 7.5) lacking some required packages. Common errors of the problem are: 1) unzip: command not found 2) No Java virtual machine is found from your PATH environment variable.</p> <p>Workaround: Install the packages using the following commands: 1) <code>yum install -y unzip</code> 2) <code>yum -y install unzip fontconfig dejavu-sans-fonts</code></p>

## Security Fixes

The following security fix was implemented in this release.

<b>PSRT Case</b>	<b>Description</b>	<b>CVE</b>
PSRT110646	Stored XSS	CVE-2019-3485

# Documentation Errata

## Document Affected: **Logger Online Help**

On Application > Archive Events, disregard the following information. Logger:529 will be implemented in Logger 7.0 release.

<b>Device Event Class ID</b>	<b>Device Event Category (cat)</b>	<b>Message</b>	<b>Additional Fields</b>
logger:529	/Logger/Resource/Archive/Index	Event Archive [archiveName] has been indexed	fname=archiveName duser=UserName duid=userId fileType=EventArchive indexed geid=0

The information has been corrected in Loger Administrator 's Guide. pdf document.

# 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 computer, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Release Notes (Logger 6.7.1)**

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 [arcsight\\_doc@microfocus.com](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!