



# **Micro Focus Security ArcSight Logger**

Software Version: 7.0

## **Release Notes**

Document Release Date: December, 2019

Software Release Date: December, 2019

## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## 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 US 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 CFR. 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 US Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 CFR. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This US 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 US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

## 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 7.0 Release Notes ..... 6
  - What's New in this Release ..... 6
  - Technical Requirements ..... 7
    - Supported Platforms ..... 8
  - Connecting to the Logger User Interface ..... 8
  - Logger Documentation ..... 9
  
- Localization Information ..... 10
  - Known Limitations in Localized Versions ..... 10
  
- Upgrading to Logger 7.0 (L8280) ..... 11
  - Upgrade Paths ..... 11
  - Verifying Your Upgrade Files ..... 11
  - Upgrading the Logger Appliance ..... 12
    - Prerequisites ..... 12
    - Upgrade Instructions ..... 13
  - Upgrading Software Logger and Logger on a VMWare VM ..... 15
    - Prerequisites ..... 15
    - Increasing the User Process Limit ..... 16
    - Editing the logind Configuration File for RHEL 7.X ..... 17
    - Upgrade Instructions ..... 17
  
- Known Issues ..... 21
  
- Fixed Issues ..... 22
  - Upgrade ..... 22
  - System Admin ..... 22
  - Localization ..... 23
  - Reports ..... 23
  - Analyze /Search ..... 24
  - Configuration ..... 26

Open Issues .....	27
Localization .....	27
Dashboards .....	27
System Admin .....	27
Upgrade .....	28
Analyze/Search .....	28
Configuration .....	31
Reports .....	33
Security Fixes .....	35
Send Documentation Feedback .....	36

# Logger 7.0 Release Notes

SODP Logger and standalone ArcSight Logger version 7.0 (L8280) releases are available in three form factors: appliance, 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 7.0 release (L8280) introduces the following new features and enhancements.

- 24TB of event storage per Logger

Logger 7.0 will support up to 24 TB of storage capacity on software and L7700 appliance form factors.

- EPS License Support

EPS licenses use a post-filtering and pre-aggregation pricing model.

- Search Improvements
  - A new UI for Logger search with features like color-coded query strings, event details, event comparisons, grid view, raw event view, column view, and so on. This UI is available in addition to the Classic Search UI of Logger.
  - Starting with the data collected by Logger 7.0, you can now create searches based on the time the event occurred (End Time) in addition to the Logger receipt time.
  - Number of concurrent searches can be modified up to 25 maximum concurrent searches.
  - Search hit limits functionality can now be increased to display up to 10 million events per search.
- Report Improvements
  - Data Science – Ability to use Python's Data Science/Predictive analytics capabilities with reporting.
  - Reporting on ArcSight Investigate – Uses the ArcSight Investigate Vertica database as a data source in Logger reporting. This enables you to create reports on Investigate data.
  - IP to GeoMapping – Ability to convert IP address to geo location and create maps within reports.
  - Scheduled empty reports can be suppressed if needed.
  - Ability to save the reports as Private or Public.

- Out of the Box Content
  - New reports cover up-to-date threats, including cloud attacks, latest vulnerabilities, OWASP top 10 Framework, as well as additional security scenarios across the defense-on-depth layer.
  - 8 new dashboards display a holistic overview of organizational risks, as well as different security scenarios such as malware and attacks, MITRE ATT&CK events reported from ESM and DGA events.

- Bonding /Trunking of NICs Appliances

Logger appliance can now receive events from the 2 network interfaces simultaneously from a single IP.

- Various security fixes, feature updates, and bug fixes have been made.

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

- ["Fixed Issues" on page 22](#)
- ["Open Issues" on page 27](#)
- ["Security Fixes " on page 35](#)

For details about these features, see the ArcSight Logger 7.0 Administrator's Guide, available from the [MF Community](#).

## 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>
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 SODP Support Matrix, available on [MF Community](#) site for details on Logger 7.0 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 Secure Open Data Platform Support Matrix available on [MF Community](#) site for details on Logger 7.0 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 Secure Open Data Platform Matrix and SODP 2.5 Release Notes. The complete Logger 7.0 documentation set also applies to this release.

**Tip:** The most recent versions of these guides may not be included with your download. Please check [MF Community](#) for updates.

- **Logger 7.0 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.
- **Secure Open 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 [MF Community](#)
- **Logger7.0 Administrator's Guide:** Provides information on how to administer and use Logger. Available for download from the [MF Community](#). Also accessible from the integrated online Help.
- **Logger 7.0 Web Services API Guide:** Provides information on how to use Logger's web services. Available for download from the [MF Community](#). 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 [MF Community](#). Additionally, a printed copy is packaged with the Logger Appliance.
- **Logger 7.0 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 [MF Community](#).

# 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 UI sections are not localized: Field Summary and Search 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 7.0 (L8280)

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 15](#)

**Note:** Be sure to review the sections ["Known Issues" on page 21](#), ["Fixed Issues" on page 22](#), and ["Open Issues" on page 27](#) before upgrading your logger.

## Upgrade Paths

The following table lists the upgrade paths to Logger 7.0. 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 7.0 Upgrade Paths	
Software Versions	7.0
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 SODP Support Matrix document available on MF Community 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 7.0 available for download from the [MF Community](#).

## 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 6.7x prior to upgrading to Logger 7.0.
- Logger requires a root password. If your Logger does not have a root password already, set one before performing the upgrade.
- To retrieve logs correctly and prevent rotation, Software Logger requires 2 Linux OS pre-installed packages (zip and unzip). If these are unavailable, use the following commands to install:
  - `yum install - unzip`
  - `yum install -y fontconfig \ dejavu-sans-fonts`
- Upgrade your OS to the latest supported RHEL distribution prior the upgrade as it fixes additional security vulnerabilities. Logger 7.0 includes OS Upgrade files for this purpose.
- 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-rhel77-<timestamp>.enc**
- 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-8280.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 [MF Community](#).

## 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-rhel177-<timestamp>.enc** and following the instructions in the ArcSight Management Center Administrator's Guide.

**Note:** Be sure to upgrade to the latest OS distribution as this one fixes additional security vulnerabilities.

2. Deploy the Logger upgrade using the **logger-8280.enc** file and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Increase the connector appliance.upload.max to 1200 in the **logger.defaults.properties** file located in ArcMC.
4. Reboot the Logger for the upgrade to take effect.
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.

### 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**.
  - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file **osupgrade-logger-rhel177-<timestamp>.enc**.

**Note:** Be sure to upgrade to the latest OS distribution as this one fixes additional security vulnerabilities.

3. Browse to the **logger-8280.enc** file you downloaded previously and click **Upload Update**.

**Note:** During the upgrade process, Logger performs a data integrity check to find and fix inconsistencies in your stored data. This data integrity check improves the efficiency and effectiveness of the searches, but it might increase the upgrade time between 10 to 20 minutes. More data integrity check statistics are available at `<path_to_File>/logger_check_metadata_health_status.log`. To check for an estimated execution time, you can run the following script: `./chunkverifier.sh $ARCSIGHT_HOME/lib -data-integrity-check`. It is recommended to extend your session time out to 30 minutes to prevent being logged out after 15 minutes of inactivity and successfully complete the upgrade. For more information, see Chapter 6 in the [Logger Administrator's Guide](#).

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 7.0, available for download from the [MF Community](#).

## 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 6.7x prior to upgrading to Logger 7.0.
- To retrieve logs correctly and prevent rotation, Software Logger requires 2 Linux OS pre-installed packages (zip and unzip). If these are unavailable, use the following commands to install:
  - `yum install - unzip`
  - `yum install -y fontconfig \ dejavu-sans-fonts`
- Upgrade your Operating System (OS) to a supported version before upgrading Logger. The latest OS distribution fixes additional security vulnerabilities. For a list of supported Operating Systems, refer to the Secure *Open Data Platform Support Matrix* available for download from the [MF Community](#).
  - If your system is running on RHEL or CentOS 7.X, upgrade to the latest version of 7.7.
  - 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 login configuration file. For more information, see "[Editing the logind Configuration File for RHEL 7.X](#)" on page 17.
- 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 user id and its primary group id 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-8280-remote.enc**
  - For local upgrades, download the following file:  
**ArcSight-logger-7.0.8280.0.bi**
- Logger documentation is not included in your download package. Download your documentation from the [MF Community](#)
- Verify the upgrade files, as described in "[Verifying Your Upgrade Files](#)" on page 11

## 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 7.7.)
  - 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 Logger. Ensure that "[Prerequisites](#)" on [page 15](#) are met 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:](#)" below.
- To upgrade Logger on VMWare locally, see "[Upgrade Instructions](#)" above.

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

1. Upgrade your OS to the latest distribution as it 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-8280-remote.enc**. Follow 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 the following commands from the below directories:

Software:

```
chmod u+x ArcSight-logger-7.0.8280.0.bin  
./ArcSight-logger- 7.0 8280.0.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.

VMWare: The **/opt/arcsight/installers** directory.

```
chmod u+x ArcSight-logger-7.0.8280.0.bin  
./ArcSight-logger-7.0.8280.0.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 7.0.

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 License Agreement screen is displayed. To review the agreement

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

Software: Scroll to the bottom of the license agreement and enable the "I accept the terms of the License Agreement" button.

VMWare: Press **Enter** to display each part of the license agreement.

4. To accept the terms :

Software: Select **I accept the terms of the License Agreement** and click **Next**

VMWare: Type **Y** and press **Enter**. To exit the installer at any point during the installation process, type **quit** and press **Enter**.

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.

6. Once all Logger processes are stopped, the installer checks that the installation prerequisites are met:
  - Operating system check—The installer checks to see if your device is running a supported operating system, otherwise, a warning will be displayed (this will not prevent the installation process).

To proceed with the upgrade:

Software: Click **Continue**. To exit the installer, click **Quit** and upgrade your OS.

VMWare: Type **1** and press **Enter**. To exit the installer and continue to upgrade the 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 Secure Open Data Platform Support Matrix for a list of supported operating system platforms.

- Installation prerequisite check—If the check fails, Logger will display a warning. Make sure to address the issue before proceeding.

### Example

=====

#### 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:

Once all checks are complete, the installation continues.

7. The Choose Install Folder screen is displayed. Navigate to or specify the location where you want to install Logger.

Software: The default installation path is **/opt**, Logger can be installed at another location if needed.

**Note:** When you upgrade Logger, it will continue to have access to the data store of the previous version, however, a fresh install (Logger installed in a new location) will not.

VMWare: Type the installation path for Logger **/opt/arcsight/logger** and press **Enter**. Do not specify a different location.

8. To confirm the installation location:

VMWare: Type **Y** and press **Enter**. To exit the installer and configure the console, type **Quit** and press **Enter**.

Software: Click **Next**.

- If there is not enough space to install the software at the specified location, a message will be displayed. To proceed with the installation, specify a different location or make sufficient space available. Click **Previous** to specify another location or **Quit** to exit the installer.
- If Logger is already installed at the location you previously specified, a user intervention message will be displayed warning about the selected directory already containing an installation of Logger, and asking if you want to upgrade.

Software: To continue with the operation, click **Upgrade**. Click **Back** to specify another location.

VMWare: Type **2** and press **Enter** to continue with the upgrade.

9. Review the pre-install summary and install:

Software: Click **Install**

VMWare: Press **Enter**

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

10. To initialize Logger components:

Software: Click **Next**

VMWare: Type **Enter**

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

11. Upgrade Logger:

Software: Click **Next**

VMWare: Type **Enter**

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.

**Note:** During the upgrade process, Logger performs a data integrity check to find and fix inconsistencies in your stored data. This data integrity check improves the efficiency and effectiveness of the searches, but it might increase the upgrade time between 10 to 20 minutes. More data integrity check statistics are available at `<path_to_File>/logger_check_`

```
metadata_health_status.log
```

To check for an estimated execution time, you can run the following script: `./chunkverifier.sh $ARCSIGHT_HOME/lib -data-integrity-check`.

12. Make a note of the URL. To exit the installer:  
Software: Click **Done**  
VMWare: Press **Enter**
13. Restart Logger to save changes.
14. You can now connect to the upgraded Logger.
15. Make a configuration backup immediately after the upgrade. For instructions, refer to the [Logger 7.0 Administrator's Guide](#).

## 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.

## Fixed Issues

The following issues are fixed in this release.

- [Upgrade](#) .....22
- [System Admin](#) .....22
- [Localization](#) .....23
- [Reports](#) ..... 23
- [Analyze /Search](#) ..... 24
- [Configuration](#) .....26

## Upgrade

Issue	Description
LOG-23194	Tzdata2018g did not work for countries exempted of daylight saving (Brazil). Fix: Tzdata2019b has been updated in this release.
LOG-22244	In a remote upgrade of Logger managed by ArcMC, the pre-flight check did not stop the upgrade install when the requirements were not met. Fix: The remote installation evaluation check works as expected.
LOG-21550	Unable to upgrade to Logger 6.7x as Cloud Linux images (AWS EC2 and Azure VM images) were light by nature (RH7.5 and CentOS 7.5) lacking some required packages. Fix: Logger installer starts properly.

## System Admin

Issue	Description
LOG-21125	Logger License Usage page displayed a confusing disclaimer when license was managed by ArcMC. Fix: Logger UI shows a clear message now.

## Localization

Issue	Description
LOG-22479	Logger could not generate a schedule report in Chinese Traditional locale. Fix: Schedule report can be generated.
LOG-22186	Logger software with th_zw as a locale sent reports via email with the incorrect name and extension. Fix: Report attachments are sent with the correct name and .zip extension.
LOG-22173	In Chinese Traditional Logger, the job execution status page and graph data were not displayed. Error message "java.lang.NullPointerException" was shown instead. Fix: Job Execution page is working correctly with Chinese Traditional as locale.
LOG-21917 LOG-21910	Unable to upload a lookup file from a locale different than English. Fix: Lookup files can be uploaded in any language.
LOG-21628	CSV files exported from search reports displayed odd characters instead of the original Chinese characters. Fix: Chinese characters are correctly exported.
LOG-15726	When Logger was set in Japanese locale, translation errors were found in reports. Fix: Report strings in Japanese are displayed correctly .

## Reports

Issue	Description
LOG-22225	Unable to view query objects from UI Report Explorer. Page never completed loading the events. Fix: This issue has been fixed.
LOG-21757	Published reports were not displayed when using IE browser. Fix: The issue has been fixed.
LOG-21539	Logger Search Reports with peers ( the search parameters "discovery field" with the value true) had unsatisfactory performance in some environments. Fix: Logger Search Reports are executed with discovery field parameter with the value false. Also, it was implemented some improvements in the peer's communication.
LOG-21380	When the user created a filter and a report with a storage group, results were retrieved with a significant delay. Fix: Report creation is now proportional to the query execution time.

Issue	Description
LOG-20463	<p>If more than 2 Scheduled Logger Search Reports were executed simultaneously, the operation could fail.</p> <p>Fix: Scheduled reports can be run simultaneously.</p>
LOG-19958	<p>The Report Engine reached the capacity limits when several scheduled (3 or more) reports were set to run at the same time in different formats. Depending on the final size of the files generated, the system reached its capacity during the first or second scheduled execution. The following error messages displayed: "Report server reached the capacity limits error and not able to create reports." Similar error messages were shown based on different scenarios.</p> <p>Fix: Schedule Reports are executed successfully without error messages.</p>
LOG-19432	<p>cab file uploaded a report with a missing filter ID causing an error message while running a report.</p> <p>Fix: This issue has been fixed.</p>
LOG-11646	<p>In report status, you were unable to view a column with the report start execution time.</p> <p>Fix: "Report Statistics feature" offers this information. In the Explorer option, the customer can check the report execution statistics by format. Also in the "Report Status," there is a new column "Execution Time" where the customer can review the execution time of each report.</p>
LOG-11511	<p>There was not an option to save new Logger Reports as "Private". By default, reports are saved to be viewed publicly.</p> <p>Fix: Now, you can save a new Logger report as private if needed.</p>
LOG-7499	<p>There was no global setting in the UI that allowed you to update the amount of concurrent reports.</p> <p>Fix: Number of concurrent reports can be updated in the UI.</p>
LOG-6237	<p>Logger emailed an empty csv attachment when there was no event data to report.</p> <p>Fix: Scheduled empty reports can be suppressed by modifying the skip.report.not.data property in the properties file and then restart.</p>

## Analyze /Search

Issue	Description
LOG-23035	<p>When exporting results with the re-run query functionality enabled, there were differences in size and columns for RawMessage, Logger, Event Time &amp; Device.</p> <p>Fix: This issue has been fixed.</p>
LOG-22384	<p>When creating saved search files with identical modification time stamp, the page in Web UI retrieved no results.</p> <p>Fix: This issue has been fixed.</p>



Issue	Description
LOG-22308	<p>Top 5000 operator did not show 5000 results regardless if a dynamic or custom time frame search was executed.</p> <p>Fix: This issue has been fixed.</p>
LOG-21891	<p>Logger did not show any error message when a peer search was performed against an unavailable peer.</p> <p>Fix: An error message is displayed.</p>
LOG-21135	<p>When running a top operator search combined with lookup operator, search sometimes delivered accurate results and sometimes returned 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 were empty</p> <p>Fix: Top and lookup operators combined now work correctly.</p>
LOG-20891	<p>When exporting results of a query with search operation filter as fields, columns missing asterisk [*] displayed no data.</p> <p>Fix: Logger now shows the data of the selected columns when you export a CSV file.</p>
LOG-20458	<p>Software Logger was unable to export a search result of 1 million events. The following error got displayed: "Search Export failed. Scheduled export failed due to export failed or unable to retrieve events". When the re-run query box was checked, the user was able to export in .csv format.</p> <p>Fix: One million events are being exported correctly in .csv format without the ALL FIELDS option.</p>
LOG-20169	<p>When upgrading Logger, sumO operator was not working in peering mode. Sum (bytesIn) was working for local search only.</p> <p>Fix: Sum is retrieving events while doing peer queries.</p>
LOG-19175	<p>When Logger executed scheduled searches, csv files stored in "saved search files" were limited to (or rather truncated to) 1,000,000 rows without any notice that such limit had been reached.</p> <p>Fix: Now, search hit limits functionality allows you to adjust search results up to 10 million events.</p>
LOG-16589	<p>When a peer was removed from a peer Logger configuration, scheduled peer reports changed to the default "Local Only" option, and did not search in the remaining peers.</p> <p>Fix: Peer reports can be executed after removing a peer.</p>
LOG-10061	<p>Logger was limited to export a maximum of 1 000 000 hit searches.</p> <p>Fix: Max number of search hits/exported fields and search using API can be configured in Logger 7.0 up to 10M maximum. 1M of searches has been set as default.</p>

## Configuration

Issue	Description
LOG-21660	<p>After upgrading an L7600 appliance to v6.7x, volume size could not be increased. Full disk space could be used when performing a factory restore though.</p> <p>Fix: After modifying the logger.default.properties flag, storage volume can be extended.</p>
LOG-21446	<p>Unable to start Logger Linux installation as Cloud Linux images (AWS EC2 and Azure VM images) were light by nature (RH7.5 and CentOS 7.5) lacking some required packages. Common errors of the problem were: 1) unzip: command not found 2) No Java virtual machine found from your PATH environment variable.</p> <p>Fix: Logger installer starts properly.</p>
LOG-21435	<p>Log information messages were labeled as error.</p> <p>Fix: Logs are categorized as warnings instead.</p>
LOG-21346	<p>After the Archive Path was updated, "Event archive settings added" message was displayed in the same quantity as storage groups.</p> <p>Fix: Logger displays the message only one time.</p>
LOG-20972	<p>When a password with characters "?" and "*" was added in the configuration backup, the characters were escaped twice causing an error in password verification.</p> <p>Fix: Password characters are properly escaped during the configuration backup.</p>
LOG-20535	<p>Logger still used the previously uploaded certificate even though the user updated the SMTP certificate.</p> <p>Fix: Logger recognizes the latest certificate uploaded after restarting APS service.</p>
LOG-19981	<p>Duplicate events might be forwarded to ESM when more than 1 Logger processor process was running.</p> <p>Fix: This issue has been fixed.</p>
LOG-19265	<p>After upgrading to Software Logger, license events were not registered correctly.</p> <p>Fix: Events are registered correctly after Logger upgrade.</p>
LOG-18095	<p>"Save and remove event archive" right implicitly allowed you to load/unload archives.</p> <p>Fix: Logger introduces a new right for event archives named "Load and unload event archive" which is independent from "save and remove event archive" right.</p>

# Open Issues

This release contains the following open issues.

- [Localization](#) .....27
- [Dashboards](#) .....27
- [System Admin](#) .....27
- [Upgrade](#) .....28
- [Analyze/Search](#) .....28
- [Configuration](#) .....31
- [Reports](#) .....33

## 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.

## Dashboards

Issue	Description
LOG-17393	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.  Workaround: Name the dashboard differently.

## System Admin

Issue	Description
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.

## Upgrade

Issue	Description
LOG-23479	<p>ENC files larger than 1100MB (Logger ENC file is 1.12GB) cannot be uploaded to ArcMC.</p> <p>Workaround:</p> <ol style="list-style-type: none"><li>1. Modify the logger.defaults.properties file located at &lt;ARCMCHOME&gt;/current/arc sight/arc mc/config/logger/logger.defaults.properties (software) or /opt/arc sight/arc mc/config/logger/logger.defaults.properties (appliances) to increase the connector appliance.upload.max.</li><li>2. Reboot ArcMC.</li><li>3. Try to upload the ENC file.</li></ol>

## Analyze/Search

Issue	Description
LOG-23419	<p>If the operators chart and span are used together without any query before the pipe (example: chart count by deviceEventCategory span (deviceReceiptTime) = 5m" ), with a time range that includes many days (example: \$CurrentMonth) , Logger has to scan a lot of events for that search. This caused high levels of CPU usage causing the search to fail.</p> <p>Workaround: Filter the events before the pipe, specially if some fields that you would use with the chart and span operator could be null on some events, like "deviceEventCategory is not null AND deviceReceiptTime is not null   chart count by deviceEventCategory span (deviceReceiptTime) = 5m". Also, avoid to use of chart and span operators combined when the time range is considerable long time span, like months.</p>
LOG-23167	<p>Aggregate functions such as *avg* and *stdev* are not working in peer mode.</p> <p>Workaround: None available at this time.</p>

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/</code> or <code>ifconfig -s   cut -d' '-f1</code>.</li> </ol> <p>For example, It returns ens32 or eno1 depend of the device</p> <ol style="list-style-type: none"> <li>2. Add Logger property named "logger.network.interface.name" on <code>/opt/arcshint/userdata/logger/user/logger/logger.properties</code> for appliances, and <code>&lt;install_dir&gt;/userdata/logger/user/logger/logger.properties</code> for software logger and set it with the value obtained from the previous step.</li> </ol> <p>For example, add <code>logger.network.interface.name=ens32</code> or <code>logger.network.interface.name=eno1</code>. <ol style="list-style-type: none"> <li>3. Restart logger.</li> </ol> <p>Note: The destinationAddress and deviceAddress will be change after adding this property. Take into account that everything written before changing the property will look the same</p> </p>
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-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 10 million search results. However, when exporting search results close to or over the hit limit 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 be incomplete.</p> <p>Workaround: Wait a few minutes before downloading to get the full export file.</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>

Issue	Description
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 [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 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; or \$filter\$ &lt;FilterName&gt;</code> and then click Saved Search or Filter in the dropdown list to load it.</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>
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 <code>"rename deviceEventClassId as eventCID"</code>, 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-11299	<p>If you uncheck the rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail.</p> <p>Workaround: The rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.</p>

Issue	Description
LOG-11225	<p>When using the auto complete feature on the search page, if the 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 "\"[/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-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>
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-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-20265	<p>The Monit log indicated that APS and PostgreSQL processes were restarted after running Monit stop all.</p> <p>Workaround: Execute the Monit stop all command one more time.</p>
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: &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</p> <p>2) Delete the keypair with the alias from the previous command: &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 -J-Djava.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;</p>

Issue	Description
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-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>
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>



Issue	Description
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-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-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>

## Reports

Issue	Description
LOG-23402	<p>When creating a query based on an InvestigateDB connection, the investigation.events table is not visible on the query designer window sometimes.</p> <p>Workaround: Restart the reportengine service on the Logger.</p>
LOG-23214	<p>Since Logger 6.7.0 version, the commented lines using the number sign (#Comment line) in MySQL queries cause the report execution to fail.</p> <p>Workaround: Use the block comment style (/* Comment line */) or line comment with double dash comment style (--line comment) instead.</p>
LOG-23111	<p>Duplicate column names are not displayed in a Logger search based report.</p> <p>Workaround: None available at this time.</p>
LOG-22922	<p>Logger displays a completion status when emailing a report despite no SMTP has been configured.</p> <p>Workaround: Configure SMTP settings before emailing a report.</p>
LOG-21067	<p>Split charts cannot be exported.</p> <p>Workaround: None available at this time.</p>
LOG-20360	<p>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.</p> <p>Workaround: None at this time.</p>

Issue	Description
LOG-19469	<p>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.</p> <p>Workaround: Re-create reports using the same query object.</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-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-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>

## Security Fixes

The following security fix was implemented in this release.

Description	CVE
Unrestricted file upload	CVE-2019-11655
Stored XSS	CVE-2019-11656
Cross Site Request Forgery (CSRF)	CVE-2019-11657

Special thanks to Michael Vieth, an Application Security Engineer at CME Group, for responsibly disclosing these vulnerabilities.

# 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 7.0)**

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!