Micro Focus Security ArcSight Logger

Software Version: 6.7

Release Notes

Document Release Date: January 25, 2019
Software Release Date: January 25, 2019

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2019 Micro Focus or one of its affiliates.

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

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Logger 6.7 Release Notes

These release notes apply to the Security ArcSight Data Platform (ADP) Logger and standalone ArcSightLogger, version 6.7 (L8242) 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 release (L 8242) introduces the following new features and enhancements.

GlobalEvent ID

Based on generator IDs, GlobalEvent ID enables the user to set unique identifiers for incoming and existent internal events. This union between event and unique identifier is immutable and cannot be detached.

Report Improvements

- New delivery options FTP and Secure FTP are available in Scheduled Reports > Shared Folder.
- The new Home Page provides direct access to Smart Report Designer, View Dashboard, Job Execution Status, Report Execution Status, Recent Reports, iPackager, Deploy Report Bundle, Published Reports, and the list of Favorite report objects.
- In Report Configuration, the Scheduler Job Dispatch Threads and Maximum Concurrent Reports options have been added.
- The user can configure the legend position in the Smart Report.
- In Smart Report Designer section, a query object menu and refresh option have been added.
- Report Status tab has been added to the report vertical menu.
- Charts can be split into one per element on an x-axis field.

Unified Query for Search Group Filter

The user is able to create new Search Group filters based on AUSM search type of query. This is supported on searches and reports.

Logger SMB v2 support with CIFS

Samba servers V2 have CIFS remote file system support.

CIFS mount from Logger to Windows 2008/2012 R2 server (hardened)

Logger supports CIFS over Windows Server 2008/2012 R2 (hardened) by using special security flags.

Retention Policy for Archives

Similar to Live Event Data's retention policy, a new feature has been introduced to manage the retention of archives in days.

Collecting Logger deployment environment information

A new feature is added in the Retrieve logs page. The user can now either include the customer environment deployment info/stats as part of the retrieve logs package or add it without retrieving all the logs.

Custom Fields Enhancement

CEF fields with auto suggestion in addition to "ad." fields" can be added to the Logger event schema.

Increased Storage Volume Size on a Software Logger

Users can extend their storage volume size up to 16TB contrasting with the previous 12TB limitation.

For details about these features, see the ArcSight Logger 6.7 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	• CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12–24 GB (24 GB recommended) • Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data. • Root partition: 40 GB (minimum) • Temp directory: 1 GB **Note:** Using a network file system (NFS) as primary event storage is not recommended.
CPU, Memory, and Disk Space for Trial Logger and VM Instances	• CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4–12 GB (12 GB recommended) • Disk Space: 10 GB (minimum) in the Logger installation directory • Temp directory: 1 GB
VM Instances	• 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 7.4 configured with 12 GB RAM and four physical (and eight logical) cores. • Micro Focus ArcSight strongly recommends allocating a minimum of 4 GB RAM per VM instance. • The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.
Other Applications	• For optimal performance, make sure no other applications are running on the system on which you install Logger.

Supported Platforms

Refer to the ADP Support Matrix, available on the Protect 724 site for details on Logger 6.7 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 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 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 (L8242)

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

Note: Be sure to review the sections "Known Issues" on page 22, "Fixed Issues" on page 23, and "Open Issues" on page 28 before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 6.7. 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 Upgrade Paths	
Software Versions	6.6.x
Appliance Models	L350X, L750X, L750X-SAN, L760X
Operating System Upgrades	• The OS your Logger is running on may vary. Be sure to check the OS version and upgrade the OS to a supported version if necessary, before upgrading Logger. • Refer to the ADP Support Matrix document available on the Protect 724 site for a list of supported Operating Systems.

Verifying Your Upgrade Files

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 6.6.x prior to upgrading to Logger 6.7.
- 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 includes OS Upgrade files for this purpose.)

  This is important even if you upgraded your OS when upgrading to Logger 6.6.1, 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-8242.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-rhel75-<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-rhel75-<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 7.5 for Logger 6.6.1, because the latest OS distribution fixes additional security vulnerabilities.
2. Deploy the Logger upgrade by using the file `logger-8242.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-rhel75-<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 7.5

for Logger 6.6.1, because the latest OS distribution fixes additional security vulnerabilities.

3. Browse to the `logger-8242.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 6.6.1 prior to upgrading to Logger 6.7.
- 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 6.6.1, 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 7.5.
  - 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 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 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-8242-remote.enc`
- For local upgrades, download the following file:
  `ArcSight-logger-6.7.8242.0.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 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 is 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 7.5.)
   - 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 15 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 19.

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 6.6.1, 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-8242-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-6.7.8242.0.bin
   ./ArcSight-logger- 6.78242.0.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-6.7.8242.0.bin
   ./ArcSight-logger-6.7.8242.0.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.
   ```

```
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.6.61 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.

General

Issue	Description
LOG-20977	Customer was unable to confirm if updates on RHEL were applied to Logger 6.7. Fix: Updates have been applied.
LOG-20592	After a fresh Install and some time of Logger usage, in invalid license error was displayed: "Logger has exceeded its data volume limit 0 times in the last 30 days.". Fix: Restart the Logger Services.
LOG-20461	Client requested Device Custom IPV6 address 1-4 to be added to Logger so it can be indexed. Fix: Device Custom IPV6 addresses have been added
LOG-20198	Error messages reporting that several default SSH keys could not be loaded by SSHD. These messages were harmless, but showed up in the logs. Fix: Changed the method that SSH keys are generated to support more key types.
LOG-15794	Customer was unable to confirm if RHEL used was affected by issue described at http://www.kb.cert.org/vuls/id/576313. Fix: JDK and Java versions used are not among the affected versions.
LOG-11256	Stored attributes for events logger:520 and logger:525 were not accurate in comparison with documentation. Fix: The issue has been fixed.
LOG-11794	Customer requested Add sourceTranslatedPort as an indexable field on Logger. Fix: Custom field has been added.

Analyze/ Search

Issue	Description
LOG-20492	Deleted search group filters still appeared when running a report causing the following error: "Unable to save additional parameters". Fix: A new validation has been added. Deleted filter in the Report Category is automatically removed from reports.
LOG-20402	If fields contained Event Time, an error "code: 1100" was displayed on Search Restful API. Fix: Search Restful API returns correctly the events even when fields contains Event Time.
LOG-18018	Cells from columns with square brackets in the field name were not displayed correctly. Fix: The issue has been fixed.
LOG-19635	If you performed a search in Logger using the pipe to fields option, the results were populated as expected. However, if results were exported to a .csv file, all the timestamps were in epoch time format. Fix: Results are now exported in csv file format.

Configuration

Issue	Description
LOG-20725	CategoryDeviceType field were not added in the logger schema as a predefined field. Fix: Field parameters have been inserted.
LOG-20685	On ArcMC 2.8 appliance, the SNMPV3 feature did not work. Fix: The feature works now properly.
LOG-20688	When Logger appliance/ArcMC appliance was enabled using SNMPV3 + snmp-agents, it displayed an AuthenicationFailure Trap. Fix: snmp-agents are now configured using V3.
LOG-20504	Certificate SMTP fields did not change from enabled to disable when the Enable SMTP AUTH Mode checkbox was unchecked. Disabled fields did not become gray. Fix: Upload Cert File SMTP Primary and Upload Cert File SMTP Backup are correctly disabled.
LOG-20503	User entered and saved invalid data in the Backup SMTP Server Port without any error message being displayed. Fix: System displays a error message if attempting to save invalid data.

Issue	Description
LOG-18920	Unable to add Lookup Files (from the Configuration menu). Fix: Add the following rights: "View Lookup Files" and "Edit, save and remove Lookup Files."
LOG-18779	When upgrading from 6.1 patch 1 to 6.3 patch 1 some Japanese characters were not viewed in Setting > Schedule Task> Completed task. Fix: Japanese characters are correctly displayed.
LOG-17782	On 6.3 Logger Appliance, deviceEventClassid Storagegroup:100 showed loopback address instead of Logger IP. Fix: The issue has been fixed
LOG-21224	When attempting to create an EB receiver using Logger 6.5 or 6.6.1 and EB 2.21, the following error on UI was displayed: "Failed to retrieve meta data from eb". Same error happened when trying to enable the created receiver. Fix: A new EB receiver is created and enabled and can receive events from eb-cef topic.

Dashboards

Issue	Description
LOG-18272	Logger dashboard was limited to only display the graphs for the first hard disk named SDA. " No data available" message appeared for graphs from other disks. Fix: Now Dashboard can show the proper graphs of each disks if the user has more than one hard drive.
LOG-16998	The system filters "Root Partition Below 10 Percent" and "Root Partition Below 5 Percent" were missing a space in the default query which can result in incorrect search results. Fix: missing space has been added before query is executed.

System admin

Issue	Description
LOG-20687	After successful upgrade from Logger 6.5.0 to 6.5.1, if non-root user name contained [_], the system Admin page got blocked. Logger WebUI displayed a message stating data volume limit was reached locking the Logger. Fix: The issue has been fixed.
LOG-18388	On G8, SNMP polling for power supply, fan, and temperature was not supported on ArcSight appliances. Fix: Polling for hardware parameters is supported.
LOG-17474	"SNMP Polling Configuration failed using GUI, Error on the pooler indicated that the username did not exist. Fix: SNMP configuration is set without any errors throughout the GUI

Issue	Description
LOG-17230	SNMP Health statistics fix did not contain the necessary information to resolve the issue. Fix: Issue has been fixed updating LOG-16759
LOG-16759	For G9, SNMP polling for power supply, fan and temperature parameters was not supported on Micro Focus Proliant appliances. Fix: 1. Install the following two RPM files on your ArcSight appliance: hp-health-10.80-1855.21.rhel7.x86_64.rpm hp-snmp-agents-10.80-2965.21.rhel7.x86_64.rpm Download available at: https://microfocusinternational.sharepoint.com/teams/IMG-TSG-I 2. Download the following MIB files and copy them to the /usr/share/snmp/mibs folder on your ArcSight appliance: cpqhlth.mib cpqhost.mib cpqsinfo.mib 3. From https://microfocusinternational.sharepoint.com, import the MIB files into the network management system
LOG-10196	Ocasionally, the System Admin -> RAID Controller page on an L7400 and L7400-SAN got truncated and only displayed "General Controller Information" Fix: Issue no longer appears in Logger 6.7 on G8 nor G9.
LOG-21396	User is disconnected from SSH session after a 60 second period of inactivity. Workaround: Configure sending keepalive packets in the SSH client.

Reports

Issue	Description
LOG-20937	Logger reports did not display correctly AM/PM date formats. Fix: The issue has been fixed.
LOG-20887	"Device group" and "Storage Group" sections were not displayed while scheduling a report. Fix: The issue has been fixed.

Issue	Description
LOG-20441	When previewing/exporting Classic Reports in dark theme, the reports were displayed in a dark background and consequently printed in the same way increasing not only the amount of dark toner used but also its cost. Fix: The dark theme is no longer enabled in the preview/export option and these reports are printed in a white background.
LOG-20442	When Search Group Filter was deleted, the Map File (/opt/arcsight/userdata/logger/user/logger) was not removed and entries still existed causing running AdHoc Reports to fail (Error “Unable to load additional parameters”). Fix: Map Files are removed after Search Group Filter is deleted.
LOG-19765	When exporting the results of a report in a CSV file, some column names were different from the ones in the exported search CSV. Fix: The underscores are now displayed correctly.

Open Issues

This release contains the following open issues.

Alerts/Filters

Issue	Description
LOG-7658	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. 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.
LOG-21143	The Report Engine does not support the operators like join, union, filter and sort for Logger Search data source. Workaround: Use the MySQL data source, this data source supports these operators (join, union, filter and sort).

Analyze/Search

Issue	Description
LOG-19261	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. Workaround: On the machine that is reporting destinationAddress and deviceAddress as 127.0.0.1, do the following: 1- Get network adapter real names with: . ls /sys/class/net/ or . ifconfig -s | cut -d' ' -f1 . It returns, for example: ens32. 2- Change Logger property with real network adapter name. Property file is located at /opt/arcsight/logger/config/logger/logger.defaults.properties and for appliances, and at <install_dir>/current/arcsight/logger/config/logger/logger.defaults.properties for software logger. Property name is logger.network.interface.name. default network adapter name is eth0 . Set it with the value obtained from the previous step. For example, change it to logger.network.interface.name=ens32. 3- Restart logger.
LOG-18945	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. 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.
LOG-18189	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. Workaround: A user with System Admin rights can set the search expiration time in the Configuration > Search Options page. The search expiration time can be increased up to 60 minutes.
LOG-17806	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. 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.

Issue	Description
LOG-17318	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. 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.
LOG-17215	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. Workaround: None at this time.
LOG-16429	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. Workaround: Turn off "overwrite same content" before importing.
LOG-16347	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: _deviceGroup IN ["192.164.16.202 [SmartMessage Receiver]"])) | where deviceEventClassId = "agent:050" Does not return the value 'agent:050' in the deviceEventClassId field of the search results. Workaround: Include the 'user' field from the custom field list in the query.
LOG-15972	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. Workaround: Query around the affected time range, or reduce storage group retention to remove previously restored archived events from that date in local storage.
LOG-15079	Loading a saved search or filter by using the folder icon (Load a Saved Filter) fails if the query includes the insubnet operator. Workaround: In the text box, type SS<SavedSearchName> or $filter$<FilterName> and then click Saved Search or Filter in the dropdown list to load it.
LOG-14266	After updating the daily archive task setting, you may not be able to see the event with a query like: message = "Daily archive task settings updated". Workaround: Use either of the following two queries to find the event: 1) message CONTAINS "Daily archive task settings updated" or 2) message STARTSWITH "Daily archive task settings updated."

Issue	Description
LOG-13532	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. Workaround: To ensure that all events are returned and can be displayed, specify a start time of 12:59:59 or earlier and an end time of 2:00:01 or later.
LOG-12524	If the value for a discovered field contains a colon (:), an ampersand (&), or angle brackets (<>), the query generated by clicking on it will escape the character with an added backslash (\ ). Workaround: Remove the backslash in front of the character. For example, if the query inserted by clicking the field is "IdentityGroup=IdentityGroup\:All", then after removing the backslash, the query becomes "IdentityGroup=IdentityGroup:All".
LOG-12290	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. Workaround: Since this issue is caused by the fields included in the fieldset used for the search, remove any renamed fields from the fieldset.
LOG-12030	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. Workaround: To export search results without the All Fields requirement, add another field. This will export all of the corresponding events correctly.
LOG-11299	If you uncheck the rerun query option when exporting search results of a search performed on peer Loggers, the export operation might fail. Workaround: The rerun query option is checked by default. Do not uncheck it when exporting results of a search performed on peer Loggers.
LOG-11225	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. 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 ",.

Issue	Description
LOG-11066	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. Workaround: Change the system time zone to something more specific, such as /America/Los_Angeles.
LOG-10126	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 "johnnyny smith": | replace "john" with "*johnny" Workaround: None available at this time.
LOG-9420	When using the search term "transaction" on data that is received out of order, the duration may appear to be negative. Workaround: Include the term "sort _eventTime" before the transaction term.
LOG-9025	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. Workaround: Use an external browser to see results.
LOG-6965	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. Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.
LOG-5181	Search results are not highlighted when there are multiple values that match the IN operator in a query. 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.
LOG-21471	"Enable Global ID" checkbox is not checked after fresh install or after upgrading to 6.7 despite is enable by default. Workaround: Save the Global ID configuration. Once it is saved, the actual behavoir and the UI of Global ID configuraton is consistent.

Configuration

Issue	Description
LOG-18753	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. Workaround: When connecting another cluster with client authentication, clear the keystore before configuring. This can be done with the commands: 1) List the keypairs by alias: <install_dir>/current/local/jre/bin/keytool -list -keystore <install_ dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_ dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar | grep -i private 2) Delete the keypair with the alias from the previous command: <install_dir>/current/local/jre/bin/keytool -delete -keystore <install_dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar -J-Djava.security.egd=<a href="file:/dev/urandom" class="external-link" rel="nofollow">file:/dev/urandom -alias <alias(es) from previous command>
LOG-18542	When using the Scheduled Archive drop-down filter on the Configuration > Finished Tasks page, the UI displays an error message. Workaround: See the finished archive tasks, file the archived results on the Configuration > Event Archives page.
LOG-17433	When deleting a Logger TCP or UDP receiver, the XML file (receiver parameters) is not deleted. Workraround: When deleting a receiver, manually delete the xml file too.
LOG-16379	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. Workaround: Option 1: Push the configuration again to the destination Logger. Option 2: Manually add the SNMP destination on the target Logger.
LOG-16349	For a newly-installed Logger, report objects and queries are not available until you navigate to the Reports Dashboard (Reports > Dashboard) for the first time. Workaround: Before attempting to create a query or report, navigate to the Reports dashboard to provision the report objects.
LOG-15530	Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail. 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 > Authentication > External Authentication page.

Issue	Description
LOG-14778	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. Workaround: Create a Receiver with different name and drill-down the events on the Summary page using the Device Group containing the new Receiver.
LOG-14650	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. Workaround: None available at this time.
LOG-13834	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". Workaround: Specify the Logger Appliance time zone by location. For example, set the time zone as "Taipei" or "Los Angeles."
LOG-13226	A user can edit a Forwarder while the feature is enabled. This can cause the Forwarder to stop sending events. Workaround: Before editing the Forwarder, disable it. Then edit it and re-enable it to have the Forwarder send events to its target destination.
LOG-11473	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. Workaround: Enter valid values for all required Setup Wizard fields.
LOG-11290	When you delete a Receiver, the Receiver's numeric ID still displays in the Summary page despite it is correctly deleted from the Dashboards. Workaround: Restart the Logger.
LOG-11176	When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references. Workaround: Edit the Receiver to verify that the RFS mount is valid. Alternatively, verify the mount on the System Admin > Remote File Systems page.
LOG-10056	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. Workaround: Do not create a receiver with a name you have previously used .
LOG-8790	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. Workaround: Avoid using non-ASCII characters in the community string.
LOG-8194	After restoring Logger from a backup configuration, the CIFS share cannot be mounted because the user name and password fields are empty. Workaround: Edit the setting of the CIFS share and re-enter your username and password.

Issue	Description
LOG-4986	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). 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.
LOG-370	The Configuration Backup (Configuration > Configuration Backup > Backup_name) and File Transfer Receivers (Configuration > Receivers) may fail without notification. The most likely cause is a problem with configuration parameters, such as Remote Directory, User, or Password. If an error occurs, the command appears to succeed but it does not. Workaround: The error is logged. Check the log (Configuration > Retrieve Logs) if you suspect a problem with the backup. When a Configuration Backup is scheduled, the error status is shown in the Finished Tasks status field.
LOG-21171	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. Workaround: change the encoding of the receiver to UTF-8.
LOG-21339	When the user attempts to create an eventbroker receiver and enters the hostname for the eventbroker Kafka node servers, the operation fails with a message saying the entered value is not a valid hostname. Workaround: Include a master worker node and IP.
LOG-21432	User is unable to save a SMTP configuration after it retrieves an exception. Logger displays the following message: We encountered a problem saving the data. Try saving the data again. Error SMTP is on synchronization, please try again later Workaround: Go to /installation path/userdata/platform/smtp_certs/ and touch updateFile. Save the changes again.
LOG-21346	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. Workaround: None at this time

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.
LOG-21377	Logger Web Process is running out of memory when Logger Dashboard is refreshed constantly. Workaround: Restart all Logger processes.

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.
LOG-21472	The following sections are not updated in the online help: 1. Retrieve Logs. 2. Storage Volume. 3. SSH Access to Appliance. 4. Using Global ID. 5. The Smart Report Designer. 6. Report Filters. Workaround: See Documentation errata in the RN

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-20126	When exporting a Logger search result to a CSV format, odd characters appear in the fields instead of the original Chinese characters from the original Logger search results. Workaround: None at this time.

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.
LOG-19423	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". Workaround: Contact support.
LOG-16589	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. Workaround: Check all scheduled reports and assign peers after making changes to peer configuration.
LOG-16405	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." Workaround: None at this time.
LOG-16281	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. Workaround: None available at this time.
LOG-15726	Some reports contain translation errors when they are displayed in Japanese. Workaround: None at this time
LOG-15462	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. Workaround: Check the amount of free space periodically.

Issue	Description
LOG-15056	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. 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.
LOG-11659	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. Workaround: If you are installing the SOX v4.0 solution package on Software Logger with a root user, leave this step for the end.
LOG-10098	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. Workaround: None available at this time.
LOG-9620	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. Workaround: None available at this time.
LOG-21358	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. Workaround: Allow time as report execution and rendering are slow-paced processes
LOG-21365	The user is not able to scroll down in the Classic Dashboard page. Workaround: None at this time
LOG-21389	When executing the Daily Byte Count Report, an unexpected error message is displayed. Workaround: 1. Login to Logger as Admin User 2. Click on Reports tab 3. Click on Explorer > Logger Administration 4. Customize Daily Byte Count report (Refer 9301_1.png) 5. Click on Data Source tab 6. Select Daily Byte Count query object again(Refer 9301_2.png) 7. Click on Save button and verify the behavior

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-20346	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. Workaround: Re-run and published the Logger Search report again.
LOG-20463	if 1 or more Scheduled Logger Search Reports are run simultaneously, the operation could fail. Workaround: Run the Logger Search Reports at different times. Also, you can combine Logger Search Report and MySQL Report when it is required to run at least two different reports at the same 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: /opt/local/monit/bin/monit restart all
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-17404	For non-root Loggers that are running as a service, if the OS is upgraded to RHEL 7.2 after Logger upgrade, the Receivers process fails to start. Workaround: Log in as root and run the command '/sbin/ldconfig' before starting Logger.
LOG-16711	On Logger L7600 series appliances, the user interface may not refresh once the upgrade has finished. 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.
LOG-21446	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. Workaround: Include the missing packages using the following commands: 1) yum install -y unzip 2) yum install -y fontconfig \ dejavu-sans-fonts
LOG-21441	One of the Logger validation processes is not updated with the correct OS version supported. Workaround: Update the Logger validation processes with the correct OS version supported.

Documentation Errata

Document Affected: Logger Online Help

- On GlobalEvent ID, replace note under GlobalEvent ID Creation with the following: " Internal events created, archived and stored before enabling this feature do not have a GlobalEvent ID. Logger does not generate one unless they are sent to a Connectors 7.11 Streaming Connector or ESM forwarder with the GlobalEvent ID property. Logger will not generate a GlobalEvent ID for events forwarded using TCP/UDP receivers".
- On the Smart Report Design section, information is omitted under the first paragraph: "To have the latest report version, right click and select the refresh option on each category. Additionally, the below menu will be displayed whenever you right click a query object."
- On Report Filters, Peer /Pipeline Operator section has been updated with the following: "It applies for Regex /Unified filter only. The query textbox in the search group category does not allow either [_ peer] or [|] to use pipeline expressions".
- On Storage Volume, the section titled "To allocate disk space" is not included:

1. Go to <LOGGER-FOLDER>/data and lok for the available storage volume.
2. Multiply the data- file folder space for .93. The result will be the initial storage volume space.
3. Obtain the storage volume space specified in your license. Logger 6.7 has assigned 16TB disk space for permanent license and 90 GB for Instant-On-License.

   Note: If the license disk space is greater than storage volume, no changes are needed.

4. Allocate the storage disk space:
   a. Default storage group: 50% of current storage volume
   b. Internal storage group: 5GB for Appliance or 3GB for Software.

- On Retrieve Logs, the section "Collecting Logger deployment environment information" is not included:

This option enables the user to compile the basic information in one single file allowing a more direct interaction with the Support Team. If you click the include deployment info/stats checkbox, you can additionally add your log retrieve search a json file attachment in the logs.zip. To get only the json file, click Download Environment info button.

Basic information retrieved: Current time. Logger information: Installation type (SW/Appliance), product version, model, ESP. OS information. Processor information. Memory information. Average EPS, current EPS. Receivers. Forwarders. Peers. Alerts. Storage Group. Storage Volume. Failed Archive. Data Volume.

- On SSH Access to the Appliance, a note is missing below Connecting to Your Appliance Using SSH. "For security purposes, SSH sessions time out after a 60 second period of inactivity. To extend SSH

connection, configure sending keepalive packets in the SSH client".

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)

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.

We appreciate your feedback!