# Micro Focus Security ArcSight Logger

Software Version: 7.2

## Release Notes

Document Release Date: September, 2021
Software Release Date: May, 2021

# Legal Notices

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

https://www.microfocus.com

# Copyright Notice



# Trademark Notices



# 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:

https://www.microfocus.com/support-and-services/documentation

# 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 |

# Logger 7.2 Release Notes

Standalone ArcSight Logger version 7.2 (L8372) release is available in two form factors: appliance and software. 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 7.2 (L8372) introduces the following feature enhancements and bug fixes.

- Logger data can now be searched on Recon 1.2.
- MySQL has been upgraded to the 5.7.21 version to address security fixes.
- Zstd compression and decompression improve the storage up to 15% compared to previous releases.
- Search UI:

  - Migration to new search UI is now complete and the classic search UI is deprecated.

  - Improved Peer Search, Saved results , and Search UI response time.
- A dedicated Apache instance for events ingestion has been enabled to support high traffic Loggers.
- Report improvements:

  - Ability to export the list of scheduled reports.

  - Ability to retrieve more than 100 000 and up to 1 000 000 results when using grouping or sorting.
- One step upgrade from supported Logger versions to Logger 7.2.
- Updated localizations.
- Various security fixes, bug fixes, and library updates have been made.

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

- "Fixed Issues" on page 26
- "Open Issues" on page 33

For details about these features, see the ArcSight Logger 7.2 Administrator's Guide, available from the Micro Focus Community.

# 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<br>• Memory: 12–24 GB (24 GB recommended)<br>• Disk Space: 65 GB (minimum) in the Software Logger installation directory. If you allocate more space, you can store more data.<br>• Root partition: 40 GB (minimum)<br>• Temp directory: 1 GB<br>**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<br>• Memory: 4 –12 GB (12 GB recommended)<br>• Disk Space: 10 GB (minimum) in the Logger installation directory<br>• Temp directory: 1 GB |
| Server | For Software form factor:<br>• Red Hat Enterprise Linux (RHEL) 7.7, 7.8, 7.9, 8.1, and 8.2 For more information, see Editing the logind Configuration File for RHEL 7.X.<br>• CentOS 7.7, 7.8, 7.9, 8.1, and 8.2.<br>For appliance upgrade: Red Hat Enterprise Linux 7.9. |
| 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 7.9 configured with 12 GB RAM and four physical (and eight logical) cores.<br>• Micro Focus ArcSight strongly recommends allocating a minimum of 4 GB RAM per VM instance.<br>• 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 | • To avoid file permissions, ownership, ports, and resource consumption issues, make sure no third-party applications are installed on the same system as Logger.<br>• For optimal performance, make sure no other applications are running on the system where Logger is installed. |

## Supported Platforms

Refer to the Logger Support Matrix, available on Micro Focus Community site for details on Logger 7.2 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 Logger Support Matrix available on Micro Focus Community site for details on Logger 7.2 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. 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 Logger Support Matrix. The complete Logger 7.2 documentation set also applies to this release. All documents are available for download from the Micro Focus Community.

> **Tip:** The most recent versions of these guides are not included with your download. Please check Micro Focus Community for updates.

- Logger 7.2 Online Help: Provides information on how to use and administer Logger. It is integrated in the Logger product and accessible through the user interface. Click the help hyperlink on any user interface page to access context-sensitive Help for that page.
- *Logger Support Matrix:* Provides integrated support information such as upgrade, platform, and browser support for Logger.
- *Logger* 7.2 *Administrator's Guide:* Provides information on how to administer and use Logger. Also accessible from the integrated online Help.
- *Logger* 7.2 *Web Services API Guide:* Provides information on how to use Logger's web services. Also accessible from the integrated online Help.
- *Logger* 7.2 *Installation Guide:* Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM.
- *Logger* 7.2 *Best Practices Guide:* Provides information on how to configure and use Logger for best performance.

Additional Logger documentation, including the Logger Data Migration and Best Practices Guide can be downloaded from the Micro Focus 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 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 7.2(L8372)

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 23, "Fixed Issues" on page 26, and "Open Issues" on page 33 before upgrading your logger.

# Upgrade Paths

The following table lists the upgrade paths to Logger 7.2. For more information about upgrading from a version of another appliance model or an earlier software version, review the documents available in Micro Focus Community 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.

> **IMPORTANT:** Logger version 7.2 has been designed to allow direct upgrades from all the software versions listed in the next table. If you are unsure about which one is the right upgrade file for you, please contact Micro Focus Support.

| **Logger 7.2 Upgrade Paths** | |
|---|---|
| Software Versions | 6.6.0/ 6.6.1/ 6.7.1/ 7.0.1/ 7.1.0 / 7.1.1/ 7.1.2 |
| Appliance Models | L760X, L7700 |
| 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.<br>• Refer to the Logger Support Matrix document available on Micro Focus Community 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. For fresh installation instructions, refer to the Installation Guide for Logger 7.2.

## Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- You must be in Connectors 8.0 version or later, and with peering relationships (Logger in 7.1 version or later, or ESM working as a node) before upgrading. Otherwise, add the Cipher Suites as described in "Adding Cipher Suites " on page 25
- When upgrading to Logger 7.2 version, the event flow will be automatically stopped.
- 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 one of the following Logger versions prior upgrading to Logger 7.2:

  6.6.0.8204

  6.6.1.8214

  6.7.1.8253

  7.0.1.8316

  7.1.0.8336

  7.1.1.8343

  7.1.2.8354

- Logger requires a root password. If your Logger does not have a root password already, set one before performing the upgrade.
- Upgrade your OS to the latest supported RHEL distribution to fix additional security vulnerabilities. Logger 7.2 includes OS Upgrade files for this purpose. To successfully upgrade to the latest OS Operating System (OS) from older RHEL versions (7.4, 7.5, 7.6, 7.7, or 7.8), use the following file:

  `osupgrade-logger-rhel79.1-20210430111327.enc`

- Download the upgrade files from the Micro Focus Entitlement Site to a computer from which you connect to the Logger UI.

- No preupgrade file needs to be downloaded for 7.0 version or later. For upgrades prior than the 7.0 version, download the `preupgrade-logger-20210212.enc` file and click **Upload Update**.
- For local or remote appliance upgrades, download the following file: `logger-8372.enc`.
- Verify the upgrade files, as described in "Verifying Your Upgrade Files" on page 9.
- Modify the timeout value in the `logger.properties` file in the ArcMC as described in "To upgrade Logger Appliances remotely through ArcMC:" below
- Logger documentation is not included in your download package. Download your documentation from the Micro Focus 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:" on the next page

### To upgrade Logger Appliances remotely through ArcMC:

1. Modify the timeout value in the `logger.properties` file in the ArcMC following the steps below:
   - Run the following command: `cd /$ARCMC_HOME/userdata/arcmc`
   - If `<instal_dir>/userdata/arcmc/logger.properties` does not exist, create the file as a non/root user.
   - Add the new property: `node.upgrade.thread.timout= 10800` (unit value in seconds).
   - Update the `logger.properties` file using the following commands:
     ```
     Chown <non –root user>:<non-root user> logger.properties
     Chmod 660 logger.properties
     ```
   - Restart ArcMC.
2. Deploy the Logger upgrade using the `logger-8372.enc` file and following the instructions in the ArcSight Management Center Administrator's Guide.
3. If you encountered an NTP issue, see "The Network Time Protocol (NTP) service ntpd.service fails." on page 23

### 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 L7600 or L7700 series appliance, deploy the OS upgrade by using the file:

   `osupgrade-logger-rhel79.1-20210430111327.enc`
3. No preupgrade file needs to be downloaded for 7.0 version or later. For upgrades prior than the 7.0 version, download the `preupgrade-logger-20210212.enc` file and click **Upload Update**.
4. Look for the `logger-8372.enc` file you previously downloaded and click **Upload Update**.

   The **ArcSight License & System Update** page displays the update progress. Once the upgrade is complete, Logger reboots automatically.
5. If you encountered an NTP issue, see "The Network Time Protocol (NTP) service ntpd.service fails." on page 23

# Upgrading Software Logger and Logger on a VMWare VM

This section describes how to upgrade Logger. For fresh installation instructions, refer to the Installation Guide for Logger 7.2, available for download from the Micro Focus Community.

## Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- You must be in Connectors 8.0 version or later, and with peering relationships (Logger in 7.1 version or later, or ESM working as a node) before upgrading. Otherwise, add the Cipher Suites as described in "Adding Cipher Suites " on page 25
- When upgrading to Logger 7.2 version, the event flow will be automatically stopped.
- 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 one of the following Logger versions prior upgrading to Logger 7.2:

    6.6.0.8204

    6.6.1.8214

    6.7.1.8253

    7.0.1.8316

    7.1.0.8336

    7.1.0.8337

    7.1.1.8343

    7.1.2.8354
- Remote OS upgrade is not supported for Software Logger. Instead, manually 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 *Logger Support Matrix* available for download from the Micro Focus Community.
- If your system is running on RHEL or CentOS 7.X, upgrade to the latest version of 7.9.
- To upgrade from CentOS/RHEL 7.X to CentOS/RHEL 8.1 or 8.2, validate the following packages are installed:

  ```
  yum install libnsl
  yum install compat-openssl10
  yum install ncurses-compat-libs
  ```

- Before installing or upgrading Logger in Linux, you must modify four TCP properties of the OS environment as described in "Configuring TCP keepalive parameters for Linux OS" on page 16.
- Before installing or upgrading Logger, you must add the `rng-tools` package and enable the `rngd.service` as described in "Install package rng-tools" on page 16.
- If not already done on the system, perform the following procedures:
  - Increase the user process limit on the Logger's OS. (This is not required for a VMWare VM installation). For more information, see "Increasing the User Process Limit" below.
  - 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 the next page.
- A non-root user account must exist on the system in which you are installing Logger. The installer will ask you to provide one, even if you install as root. 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-8372-remote.enc`
  - For local upgrades, download the following file: `ArcSight-logger-7.2.0.8372.0.bin`
- Logger documentation is not included in your download package. Download your documentation from the Micro Focus Community
- Verify the upgrade files, as described in "Verifying Your Upgrade Files" on page 9

# 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 20 for RHEL and CentOS 7.9.)
   - 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. Make sure the `RemoveIPC` line is active and set to **no**. Remove the # (if it appears).
   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
```

# Configuring TCP keepalive parameters for Linux OS

Before installing or upgrading Logger, you must modify four TCP properties of the OS environment in `/etc/sysctl.conf` file. Add the TCP OS configuration properties using the following steps:

1. Edit the system file and press Shift + G: `vi /etc/sysctl.conf`.
2. Add and modify the following timeout properties and their recommended values:
   - `net.ipv4.tcp_fin_timeout = 30`
   - `net.ipv4.tcp_keepalive_time = 60`
   - `net.ipv4.tcp_keepalive_intvl = 2`
   - `net.ipv4.tcp_keepalive_probes = 2`
3. Exit and save (`wq!`)
4. Apply the changes by running the command `sysctl -p`

# Install package rng-tools

Before installing or upgrading Logger, you must add the `rng-tools` package and enable the `rngd.service`.

Make sure to follow the steps below:

1. Install the package by running the following command:
   `yum install -y rng-tools`.
2. To see the status of the `rngd.service` after an install, run:
   `systemctl status rngd`.
3. Run the commands to start or enable the service:
   `systemctl start rngd.service`.
   `systemctl enable rngd.service`.

# Upgrade Instructions

Follow the instructions listed below to upgrade Logger. Ensure that "Prerequisites" on page 13 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. Modify the timeout value in the `logger.properties` file in the ArcMC following the steps below:
   - Run the following command: `cd /$ARCMC_HOME/userdata/arcmc`
   - If `<instal_dir>/userdata/arcmc/logger.properties` does not exist, create the file as a non/root user.
   - Add the new property: `node.upgrade.thread.timout= 10800` (unit value in seconds).
   - Update the `logger.properties` file using the following commands:
     ```
     Chown <non –root user>:<non-root user> logger.properties
     Chmod 660 logger.properties
     ```
   - Restart ArcMC.
2. Upgrade your OS to the latest distribution as it fixes additional security vulnerabilities.
3. Deploy the downloaded upgrade file `logger-sw-8372-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-7.2.0.8372.0.bin
   ./ArcSight-logger-7.2.0.8372.0.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, this may delete your `/tmp` directory.

- VMWare:

From the `/opt/arcsight/installers` directory,

```
chmod u+x ArcSight-logger-7.2.0.8372.0.bin
./ArcSight-logger-7.2.0.8372.0.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
7.2.

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

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

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

PRESS <ENTER> TO CONTINUE:
```

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 Logger 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.

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 Administrator's Guide.

# Nullify Logger Upgrade

Whenever a Logger upgrade fails, it is necessary to reverse the changes and go back to the previous version. After reversing the changes, sometimes the permissions could be incorrect causing Logger to not initialize correctly. Fix the Logger permissions for non-root loggers by following steps below:

### To uninstall the Logger software upgrade:

1. Set Logger as non-root

   ```
   find /opt/ -type f -name "httpd.conf"
   ```

   ```
   /opt/logger/current/local/apache/conf/httpd.conf
   ```

2. Confirm the ServerName property is `arcsight:9000`:

   ```
   grep "ServerName" /opt/logger/current/local/apache/conf/httpd.conf
   ```

3. Make sure the `<Installation path>` folder has the right permission:

   ```
   sudo chown -fR arcsight:arcsight /opt/logger/
   ```

4. Run the following command from the `/opt/logger/current/arcsight/logger/bin/` folder:

   ```
   chmod 755 arcsight filetransfer loggerd permissionFix receiverstart
   retrievelogs runner scripts
   ```

5. Run the following command from the `/opt/logger/current/local/monit/watchdog` folder:

   ```
   chmod 600 apache.monitrc aps.monitrc monitrc mysql.monitrc
   postgresql.monitrc
   ```

   ```
   chmod 700 logger.monitrc
   ```

   ```
   chmod 664 connector.monitrc
   ```

6. Run the following command from the `/opt/logger/current/local/monit/bin` folder:

```
chmod 755 monit
```

7. Run the following command from the `/opt/logger/data/pgsql` folder:

```
chmod 700 base global pg_commit_ts pg_dynshmem pg_logical pg_multixact pg_
notify pg_replslot pg_serial pg_snapshots pg_stat
```

```
pg_stat_tmp pg_subtrans pg_tblspc pg_twophase pg_wal pg_xact
```

```
chmod 664 dbinit.log init.store.log pg_hba.conf postgresql.conf
```

```
chmod 600 pg_hba.conf.orig pg_ident.conf PG_VERSION postgresql.auto.conf
postgresql.conf.orig postmaster.opts postmaster.pid
```

8. Run the following command from the `/opt/logger/current/arcsight/service` folder:

```
chmod 775 apache aps arcsight_logger functions monit mysql mysql_ctl
postgresql postgresql_ctl snmp
```

```
chmod 664 arcsight.config
```

# Known Issues

The following known issues apply to this release.

## Kernel Warning Message During Boot

The following error message is displayed during the initial startup screen of Red Hat Linux on L7600 Loggers:

```
[Firmware Bug]: the BIOS has corrupted hw-PMU resources
```

A similar message is posted to the `dmesg` file. The functionality and performance of both Logger and the operating system are not affected by this error message. For more information, refer to the Micro Focus Customer Advisory document: https://www.microfocus.com/support-and-services/

## PostgressSQL upgrade for 6.6.1.8214, 6.7.1.8253 and 7.0.1.8316 versions

For upgrades prior to 7.1 version, the PostgreSQL will be upgraded, which is a time-consuming process. Upgrade time can be increased approximately one hour, depending on the logger data size and hardware specifications. If you experience any issue, open a support ticket before restarting Logger or performing any other action.

## The Network Time Protocol (NTP) service ntpd.service fails.

For some appliances, the `chronyd.service` starts automatically causing the NTP service connection to not work properly. Some of the issues encountered are:

• The information displayed in the **System Admin > Network Settings > Time/NTP > Test Servers** is incorrect. The information corresponds to a default server and not the one that the user added.

• The chrony.service is running in your environment but the Chrony sources or Chrony tracking are not retrieving details. Run the following commands to confirm those details:

Chrony sources: [IP]$ chronyc sources

Chrony tracking: [IP]$ chronyc tracking

If no issues are present, do not perform any action. Otherwise, follow the steps below.

**To apply the post upgrade:**

1. Log into Logger. Navigate to the **System Admin > License & Update** option.
2. Select the `postupgrade-logger-7.2.0-chrony-fix.enc` file and click **Upload Update**.
3. Reboot the server.

   > Micro Focus strongly recommends rebooting the server to ensure the post upgrade is applied successfully within the change window.

4. Set the NTP. Check the Chrony is not enabled automatically.
5. Make sure all the logger services start correctly, confirm the following scenarios:
   a. The Logger UI displays no discrepancies for each of the servers added.
   b. The server time is back to the current time under the NTP Servers list after adjusting the time settings, refreshing the page, and waiting up to 15 minutes

**To rollback the post upgrade:**

If you are still encountering NTP issues after applying the post upgrade and the scenarios above are not happening, restore the Logger.

1. Stop the APS service.
2. Enter the `/opt/updates/postupgrade-logger-7.2.0-chrony-fix/backup` folder and decompress the backup into the proper location:

   ```
   tar -xzvf platform-service-orig.tar.gz --directory /
   ```

3. Restore the backup for the NTP service

   ```
   tar -xzvf ntp.conf-orig.tar.gz --directory /
   ```

4. Stop the ntpd service and disable it from starting automatically

   ```
   systemctl stop ntpd
   systemctl disable ntpd
   ```

5. Enable the chronyd service to start automatically

   ```
   systemctl enable chronyd
   ```

6. Start the chronyd and check the status

   ```
   systemctl start chronyd
   systemctl status chronyd
   ```

7. Start the APS service and check the status

# Adding Cipher Suites

Error messages related to cipher suites will appear for connectors with a version prior than 8.0 or peers ( Logger prior than 7.1 version or ESM working as a node). Follow the instructions below to add the cipher suites.

1. Go to the `logger.defaults.properties` file.
2. Replace with the property below:

   `fips.ssl.enabledciphersuites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA`
3. Once the property has been added, stop and restart the Logger services by entering the following commands one after the other:

| For Logger Appliance | For Software Logger |
|---|---|
| `/opt/local/monit/bin/monit stop all` | `<install-path>/current/arcsight/logger/loggerd stop all` |
| `/opt/local/monit/bin/monit summary` | `<install-path>/current/arcsight/logger/loggerd status` |
| `/opt/local/monit/bin/monit start all` | `<install-path>/current/arcsight/logger/loggerd start all` |

   > **Tip:** Cipher suite should be added in both Logger and ESM properties when adding ESM as a peer node.

4. (Conditional) If having performed the above steps you still face any issues, you might need to add or replace the cipher suites on the `httpd.conf` file, as follows:

   `SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES128-SHA256`

# Fixed Issues

The following issues are fixed in this release.

## Installation

| Issue | Description |
|---|---|
| LOG-25306 | After upgrading a software Logger from ArcMC, the ArcMC system displayed an error message: Failed to bring up some processes successfully. The ArcMC Management process was not found.<br>Fix: Software Logger from ArcMC can be upgraded correctly. |
| LOG-25010 | An error occurred when upgrading OS in Logger L7700. This was a random error.<br>Fix: The issue has been fixed. |

## System Admin

| Issue | Description |
|---|---|
| LOG-24446 | Monit restarted Postgres after an OS clean-up removed files from /tmp. This left the system in an unstable state.<br>Fix: The issue has been fixed. |
| LOG-24445 | Improper permissions on /home and /home/arcsight directories caused Logger not to initialize properly.<br>Fix: The issue has been fixed. |
| LOG-24173 | After a reboot of the appliance, the "monit summary" command displays "Execution failed" for receivers, processors, and web processes. However, the monit summary output flips into running immediately when navigating to the 'System Admin > Process Status' page.<br>Fix: The issue has been fixed. |

## General

| Issue | Description |
|---|---|
| LOG-25273 | In some instances, Logger switched from light to dark after updating the theme right after install or upgrade. This caused Logger to freeze.<br>Fix: Light and dark theme is properly updated after install or upgrade. |

# Configuration

| Issue | Description |
|---|---|
| LOG-26580 | Whenever the receivers' services start and are running, 2 zombie processes appeared.<br>Fix: Zombie processes do no longer appear. |
| LOG-25292 | The file "updateFile" and the smtp_certs did not have the correct owner. The Report-Engine did not properly update the properties file.<br>Fix: The issue has been fixed. |
| LOG-24658 | When a category report was renamed, the change was not reflected under User Management groups.<br>Fix: This issue has been fixed. |
| LOG-22922 | Logger displayed a completion status when emailing a report despite no SMTP was configured.<br>Fix: The issue has been fixed. |
| LOG-21971 | When a storage group did not have a mount configured, Logger disabled the button table in the Event Archive pages.<br>Fix: Messages are displayed during and after storage group settings. Only the configured storage settings can be selected when archiving events. |
| LOG-21546 | When creating a configuration backup, sourceAddress, sourceHostName, and fiePath CEF are not shown for audit events logger:660 and logger:665.<br>Fix: sourceAddress, sourceHostName, and fiePath CEF fields have been added to the audit events logger:660 and logger:665. |
| LOG-17841 | Unable to display the firewall's current status and configuration.<br>Fix: The option is available. For details on how to display the information, see the Administrator's Guide. |
| LOG-15235 | Previously, Logger did not allow to change of MySQL password.<br>Fix: Now, you can change the password from the Maintenance Operations > MySQL password. |

| Issue | Description |
|---|---|
| LOG-10140 | Unable to determine in Logger how much space each archive occupied. The Logger admin did not have access to the NFS/CIFS file server and the file server restricted share permissions to only the logger.<br>Fix: Once Logger archives the event, it displays the size of the archived files(s). |
| LOG-9124 | The documentation did not explain that in order to enable multipath SAN connectivity to the appliance, you need to make sure that the multipathd service is configured to start on boot.<br>Fix: The issue has been fixed. For details on how to display the information, see the Administrator's Guide. |
| LOG-8007 | Unable to configure jumbo frames on appliances.<br>Fix: The issue has been fixed. For details on how to display the information, see the Administrator's Guide. |

# Analyze/ Search

| Issue | Description |
|---|---|
| LOG-26552 | Unable to view running searches unless "View Security Settings" permission was checked.<br>Fix: Searches can be viewed successfully without the view or configure security settings. |
| LOG-26501 | The searches executed on the new search page expired as soon as they were executed.<br>Fix: The issue has been fixed. |
| LOG-26020 | The search page count was different between the hit count and grid table since the head only counted the summarized events.<br>Fix: The issue has been fixed. |
| LOG-25957 | When the hit limit was reached, the peer statistics screen and logs for peer nodes in version 7.0 or lower were displayed as failed.<br>Fix: It is recommended to use a peer head 7.1.1 and peer node version 7.1.1. |
| LOG-25931 | After restarting only the server's service, the logger was unable to save platform events.<br>Fix: Now, the platform events can be saved. |
| LOG-25869 | When you canceled a search, the Configuration > Searches > Running Searches page showed the search was still running and never expired.<br>Fix: Now, the canceled searches appear with the correct status and they expire accordingly. |
| LOG-25841 | The searches executed on the new search page expired as soon as they were executed.<br>Fix: The issue has been fixed. |
| LOG-25485 | ArcMC was not able to read logger nodes stats like the dashboards page.<br>Fix: ArcMC is now able to pull stats from Logger. |

| Issue | Description |
|---|---|
| LOG-25370 | The retention period for the saved search results was not enforced automatically, it required another search result to be persisted to trigger the search deletion.<br>Fix: Searches are removed automatically after the retention period. |
| LOG-25325 | Unable to retrieve results from a persisted search with a peer that was temporarily powered down.<br>Fix: Peer results are properly retrieved. |
| LOG-25324 | Unable to retrieve results from a persisted search with a peer that was subsequently removed.<br>Fix: Peer results are properly retrieved. |
| LOG-25305 | Search result references were removed from the system 1 day after the retention was expired.<br>Fix: Results are removed after the retention period expires. |
| LOG-25304 | Search and search dashboards did not work as expected when opened in maintenance mode. In maintenance mode, you could only do the selected maintenance operation.<br>Fix: Search and Search dashboards are now working correctly in maintenance mode. |
| LOG-25291 | The field summary tab was not persisted by Logger on search results. Therefore, neither the Field Summary information nor the Discover Fields were displayed in such search results.<br>Fix: Now, Field Summary and Discover fields information is retrieved in the search results. |
| LOG-25290 | Unable to open an item from the list of active searches if the event details window was also open.<br>Fix: Logger supports more than one emergent window at a time. |
| LOG-25289 | After executing a chart query and clicking any option from the results grid, the chart was moved to the right.<br>Fix: Chart is correctly displayed. |
| LOG-25272 | Unable to rename the active search.<br>Fix: Active searches can now be renamed. |
| LOG-25270 | Search results were not retrieved after the original search expired.<br>Fix: Search results are properly retrieved. |
| LOG-25245 | Unable to export the \| chart command in csv format from the Search page.<br>Fix: Chart command can now be exported in CSV format. |
| LOG-25238 | In search UI with the Field Summary and Discover Fields parameters checked, the field summary tab and results were not displayed even though the events retrieved have discovery fields results but were not CEF.<br>Fix: The issue has been fixed. |
| LOG-25224 | In the Firefox browser, the Save icon disappeared when refreshing the page.<br>Fix: Save icon is displayed correctly. |

| Issue | Description |
|---|---|
| LOG-25217 | When running chartable queries, a session ID error could appear. However, the search was executed correctly and with no errors.<br>Fix: Search is executed without any error messages. |
| LOG-25209 | When you run a peer search with Discover Fields enabled, the hit count limit was ignored and the search was not completed affecting the search concurrency.<br>Fix: The issue has been fixed. |
| LOG-25205 | Some canceled searches, mostly peers, were still displayed (In Progress or Completed status) in the Search Dashboard after expired. However, search resources were no longer in use.<br>Fix: Canceled searches are no longer displayed. |
| LOG-25201 | After executing a search from the Search page and press F5, values are set to default.<br>Fix: All search values are persisted once F5 is pressed. |
| LOG-25157 | When exporting a file from a Logger, the hit count did not match the limit hit count in the UI. However, if you download the file, all events were downloaded according to the hit count limit.<br>Fix: Hit count matches the limit hit count in the UI. |
| LOG-25144 | When exporting a report in PDF format, the report did not display a title.<br>Fix: The issue has been fixed. |
| LOG-25129 | The oldFileHash custom field could not be searched in a search query. If the oldFileHash field was used as a filter, no events were retrieved.<br>Fix: The oldFileHash custom field can be searched. |
| LOG-25113 | When overwriting a fieldset set without the default fieldset checked, the first fieldset appeared as the default one in the drop-down.<br>Fix: Fieldsets are correctly displayed. |
| LOG-25014 | In the Search page, when the head peer executed a search on a field present in the head peer but not in the peer nodes, the search spinner never stopped.<br>Fix: The issue has been fixed. |
| LOG-25006 | Once the search was completed with peer failures, you were unable to review the contribution of the failing peers.<br>Fix: Failing peers' information can now be reviewed. |
| LOG-24987 | When running a peer search from the search page, peer errors were not displayed.<br>Fix: Peer errors are correctly displayed. |
| LOG-24882 | When running a query to search in all peers, the chart and graph were not showing the peer down. On the other hand, a search with peer down displayed the events while the peer stats showed the peer as unreachable.<br>Fix: The peers showed on the graph and table when is unreachable and do not display events when doing the search directly to the peer node that is down. |

| Issue | Description |
|---|---|
| LOG-24831 | Sort parameter N was propagated to all peers causing inaccurate results.<br>Fix: Now, sort parameter N is not propagated to peers. If the user still experiences inaccurate values, tune the property: server.pipeline.sort.bash.count in all Loggers to a higher value. |
| LOG-23200 | No results were displayed when using INSUBNET operator within pipeline.<br>Fix: The issue has been fixed. |
| LOG-19261 | For Logger health events generated internally every minute, the values of destinationAddress and deviceAddress were 127.0.0.1 instead of the real IP address. This issue only affected Logger running under RHEL 7.X on software and appliance form factors.<br>Fix: The issue has been fixed. |
| LOG-15079 | Loading a saved search or filter by using the folder icon (Load a Saved Filter) failed if the query included the insubnet operator.<br>Fix: Saved search or filters can be loaded from the folder icon. |

# Reports

| Issue | Description |
|---|---|
| LOG-26206 | A query associated with a private report from another user was deleted without displaying any warning.<br>Fix: Logger displays a warning before deleting the query associated with private or public reports. |
| LOG-25774 | The new version of the PostgreSQL database sent the binary information with an expected encoding for the Logger system. Then, the authentication information was incorrectly shared with the Report system.<br>Fix: The binary information is shared with the correct encoding. |
| LOG-25185 | In Reports, when selecting a parameter with a boolean data type, ReportClientLogs.log showed an exception and the UI kept refreshing the data.<br>Fix: The boolean data type can be saved successfully. |
| LOG-25173 | When a MaxMind report is deployed from the cab file, the report was assigned to a different fieldset. However, if you check the Data Source from outside, it showed the correct fieldset was set to the MaxMind field set.<br>Fix: Fieldset can be correctly saved and deployed. |
| LOG-23958 | After a Logger upgrade, the Investigate Connection parameters were removed. Reports and query design associated with this connection were no longer available.<br>Fix: Investigate connection parameters will remain after an upgrade. |

| Issue | Description |
|---|---|
| LOG-23124 | The commented lines using the number sign (#Comment line) in MySQL queries caused the report execution to fail.<br>Fix: The issue has been fixed. |
| LOG-22307 | Private reports were available for users with certain permissions disabled (global access to all reports and view, run, and schedule all reports)<br>Fix: The issue has been fixed. |
| LOG-21405 | Logger did not allow to export a list of scheduled reports.<br>Fix: Task, Type, Schedule, and Next Run Time from a schedule report can be exported. |
| LOG-15879 | Unable to publish a report in the background. The report had to be completed or scheduled to publish it.<br>Fix: "Run with delivery options" allows to Publish and email reports in the background. |
| LOG-15462 | When the file system /opt/arcsight/userdata was full, Logger allowed users to run reports, even though they necessarily failed. Logger did not warn users in advance that the free space on the file system was full.<br>Fix: Now, you can set a warning in options > storage section. |
| LOG-10149 | Unable to simply uninstall a reports CAB file.<br>Fix: The issue has been fixed. |
| LOG-6397 | When using the grouping or sorting options in a report, the results were limited to 100,000.<br>Fix: The issue has been fixed. |
| LOG-5728 | Previously, Logger did not support digitally signed PDF reports.<br>Fix: Reports can be digitally signed and attached with the emails. |
| LOG-3599 | Unable to include an URL link when creating a manual report.<br>Fix: Now, the link can be emailed from a manual report execution. |
| LOG-3354 | The upload option was not available for reports.<br>Fix: The upload option is now available and can generate the report in the user-specified format and make it available in the specified directory. |
| LOG-3085 | Unable to create additional report groups under user reports and configure the permissions to it.<br>Fix: The issue has been fixed. |

# Open Issues

This release contains the following open issues.

## 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.<br>Workaround: Use openSSH for configuration backups. |

## Dashboards

| Issue | Description |
|---|---|
| LOG-17393 | When creating a new dashboard, Logger might show the error message "Dashboard name already exists," even though the user does not have a dashboard with that name.<br>Workaround: Name the dashboard differently. |

## Analyze/Search

| Issue | Description |
|---|---|
| LOG-26704 | Peer searches with a pipe operator and a time range of 1 hour or more and latency period of +1 second search results tables become unresponsive causing discrepancies between the peer stats and UI.<br>Workaround: None available at this time. |
| LOG-26661 | When executing a peer search with a time range of +30 minutes, a name is not null and the Discover Fields enabled, the search becomes unresponsive.<br>Workaround: None available at this time. |
| LOG-26654 | The event count shows substantially high numbers when using the deviceEventClassId = "eps:102" query.<br>Workaround: None available at this time. |

| Issue | Description |
|---|---|
| LOG-25271 | When a search result with peers is retrieved in the search dashboard, the page shows a wrong alias instead of the name chosen when persisting the search.<br>Workaround: None available at this time. |
| LOG-25073 | When trying to persist a search result (with a name chosen by another user), the dialog window shows an error in the database while the search was saving.<br>Workaround: Use a different name for the search result. |
| LOG-25072 | In the search persistence, a validation error occurs when you add an incorrect value. If you enter the correct values before the success message is displayed, there is a short period of time where a message with the last validation error is shown. Otherwise, if no changes are made, the window closes automatically without having the option of correcting the invalid value.<br>Workaround: None available at this time. |
| LOG-24989 | When you run a peer search (with an ESM as a peer), the hit count limit might be ignored by the ESM. If the hit count reaches its limit before the ESM scanning, Logger will no longer continue scanning events. Otherwise, the limit will be exceeded.<br>Workaround: None available at this time. |
| LOG-24059 | The transaction operator does not work as expected. The deviceHostName operator is populated when running a local search on one peer Logger with base event fields fieldsets or a peer search on a search head Logger with minimal field fieldsets. However, running a peer search on a search head Logger with base event fields fieldsets does not populate deviceHostName.<br>Workaround: None available at this time. |
| LOG-23419 | If the chart and span operators are used together without any query before the pipe (e.g "\| chart count by deviceEventCategory span (deviceReceiptTime) = 5m" ) and with a time range that includes many days (e. g. $CurrentMoth), Logger has to scan a lot of events for that search. This caused high levels of CPU usage causing the search to fail.<br>Workaround: Filter the events before the pipe, specially if some fields that you use with the chart and span operator might 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 wide, like months. |
| LOG-23167 | Aggregate functions such as avg and stdev are not working in peer mode.<br>Workaround: None available at this time. |
| LOG-21067 | Split charts cannot be exported.<br>Workaround: None available at this time. |

| Issue | Description |
|---|---|
| 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.<br><br>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-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.<br><br>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. |
| LOG-17318 | When exporting search results around 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 download the report during this period, the downloaded file might be incomplete.<br><br>Workaround: Wait a few minutes before downloading to get the full export file. |
| LOG-16429 | When exporting Source Types with common dependent parsers and the property "overwrite.same.content" enabled, Logger only imports the latest Source Type with its parser. The other Source Types do not include their parsers.<br><br>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.<br><br>Workaround: Include the 'user' field from the custom field list in the query. |
| 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 ( \ ).<br><br>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 | A search with a query that includes the rename operator and the original field name included in the fieldset will display the original field renamed by the operator as a column in the search results, but with no values.<br><br>Workaround: Remove any renamed fields from the fieldset. |
| 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.<br><br>Workaround: Remove the backslash followed by a double quote on both sides of the string. You can also do this when double quote is followed by any special character such as "\, "/, "[ , "], or ",. |

# Configuration

| Issue | Description |
|---|---|
| LOG-26814 | Unable to correctly identify which user/group permissions have been granted to a category. All Report category permissions are labeled as "edit and save reports".<br>Workaround: None available at this time. |
| LOG-26689 | The logs do not rotate after sending events to the second Apache instance. Logs may grow higher than expected.<br>Workaround: delete second Apache instance logs periodically. |
| LOG-26782 | Real-time alerts cannot be enabled. The host is not appropriately registered.<br>Workaround: Enable the property corresponding to the component on the logger_ processor.properties file. Make sure to restart Logger afterward. |
| LOG-26779 | After tuning the memory Roles in logger UI, the default hit count is set to 50,000,000 for UI, API, and Histogram.<br>Workaround: Change the hit count for a more suitable value on Search Options. |
| LOG-26766 | When configuring the FIPS in a software fresh install, the certificates are not loaded in the bcfips_ks file not allowing to create Logger destinations.<br>Workaround:<br>1) Delete the /opt/arcsight/current/arcsight/connector/current/user/agent/fips/bcfips_ks file..<br>2) Disable and enable FIPS.<br>3) Restart the Logger processes. |
| LOG-24124 | NIC bonding information does not appear in the UI after configuring NIC bonding.<br>Workaround: None available at this time. |
| LOG-21530 | G10 appliances with fresh install will still have ReportEngine.dat file after deployment.<br>Workaround: Manually delete the file. |
| LOG-21171 | Logger drops the non-cef events sent to a UDP receiver configured using an encoding different than UTF-8 or ASCII.<br>Workaround: change the encoding of the receiver to UTF-8. |
| LOG-18753 | When client authentication is enabled, Logger connects to one TH cluster only. If client authentication is disabled, Logger connects to an indefinite number of TH clusters. |
| LOG-16627 | When creating a search group and applying search group filters, the refresh on the admin dashboard overrides the filter settings.<br>Workaround: None available at this time. |

| Issue | Description |
|---|---|
| LOG-15530 | Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail.<br><br>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. |
| 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.<br><br>Workaround: None available at this time. |
| LOG-13998 | When setting up Logger A and Logger B to the peer by hostname using authorization ID/codes, the peer queries initiated from Logger B to Logger A fail.<br><br>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".<br><br>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.<br><br>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.<br><br>Workaround: Enter valid values for all required Setup Wizard fields. |
| LOG-11176 | When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references.<br><br>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-370 | The Configuration Backup (Configuration > Configuration Backup > Backup_name) and File Transfer Receivers (Configuration > Receivers) may fail without notification. If an error occurs, the command appears to succeed but it does not.<br><br>Workaround: Check the log (Configuration > Retrieve Logs). When a configuration backup is scheduled, the error status is shown in the finished tasks status field. |

# Installation

| Issue | Description |
|---|---|
| LOG-26743 | After Uninstall the process in SW Logger, some files might not be found on the installation directory due to immutable attributes.<br>Workaround: remove the immutable flag, using command "chattr -Ri <install_path>", from all files that were not removed and clean the folder content again. |
| 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.<br>Workaround: If you are installing the SOX v4.0 solution package on Software Logger with a root user, leave this step for the end. |

# Reports

| Issue | Description |
|---|---|
| LOG-26647 | If you save a peer search (using the saved search option) from Search UI, and the peers have a significant delay, the report creation may fail due to timeout.<br>Workaround: Use a reduced time range when creating reports. |
| LOG-25993 | The Java CC parser cannot parse expressions with a =NOT condition after a SQL statement. This parsing can only be executed if you add the end time condition to the report.<br>Workaround: Create the query using the following structure: fieldName NOT LIKE "etckeepe%". |
| LOG-25274 | Schedule MaxMind reports are failing email delivery.<br>Workaround: Log into logger and extract the report manually. |
| LOG-25061 | When installing Software Logger in ReHat and CentOS version 8.X, the data science cannot be enabled.<br>Workaround: Install the Python 2.7.1 using the command "yum install python2". Then, enable the data science and restart logger. |

| Issue | Description |
|---|---|
| LOG-23111 | Duplicate columns name will not display in a logger search based report.<br>Workaround: None available at this time. |
| LOG-21378 | When creating a Logger Search Report based on a Logger filter with a peer operator, the system does not recognize the peer operator and checks the "local-only" option in the parameters form.<br>Workaround: Execute the Logger Search Report again with the "local-only" option unchecked. |
| LOG-16405 | From the user interface, rights to view, run, or schedule specific reports outside the user's default privileges can be assigned. However, those rights do not apply in SOAP API. The report can only be run when the user has rights to "View, run, and schedule all reports".<br>Workaround: None at this time. |

# 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 7.2)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!