Micro Focus Security ArcSight Logger

Software Version: 7.2.1

Release Notes

Document Release Date: December, 2021
Software Release Date: December, 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 7.2.1 Release Notes

Standalone ArcSight Logger version 7.2.1 (L8395) 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 7.2.1 (L8395) is a maintenance release, addressing security vulnerabilities and other issues found in Logger 7.2.

In addition, the following improvements have been made:

- MySQL has been upgraded to the 5.7.33 version to address security fixes.
- The Logger data can be imported and searched on Recon 1.4 with Logger processes shut down.
- Archive files can be migrated from an old to a new mount. The archive metadata will be restored allowing archives to be scanned and allocated to the storage group of your selection. Additionally, you can also validate the integrity of your archive files.
- The SNMP destination can be configured using v3.

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

- "Fixed Issues" on page 28
- "Open Issues" on page 31

For details about these features, see the ArcSight Logger 7.2.1 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 • 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
Server	For Software form factor: • Red Hat Enterprise Linux (RHEL) 7.8, 7.9, 8.2, and 8.4 For more information, see Editing the logind Configuration File for RHEL 7.X. • CentOS 7.8, 7.9, 8.2, and 8.4. 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. • 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	• To avoid file permissions, ownership, ports, and resource consumption issues, make sure no third-party applications are installed on the same system as Logger. • For optimal performance, make sure no other applications are running on the system where Logger is installed.
Logger to Recon Data Import	• The system directory must have enough space. Logger requires 20 GB of free space for temporal files of 15 k EPS with an average event size of 1800 bytes.

Supported Platforms

> **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.

The following table lists the supported appliance models, operating systems, supported browsers, and upgrade paths for each currently supported Logger version.

Guidelines:

- An asterisk (*) next to a browser version indicates that the browser version supported is the one current at the date of release.
- The appliance models L350X, L750X, L750X-S are no longer supported.
- The OS 6.x versions are no longer supported.
- The VM image on 32-bit is no longer supported.

Version	Release Date	Appliance Models	Operating Systems	Supported Browsers	Upgrade Path
7.2.1	December, 2021	L7600 L7700	**Certified on** : CentOS/RHEL Linux 7.9 CentOS/RHEL Linux 8.4 **Supported on:** CentOS/RHEL Linux 7.8 CentOS/RHEL Linux 8.2 **VM instance** The VM image includes the Logger installer on a 64-bit CentOS 7.9.	Microsoft Edge * Firefox ESR 52 Chrome	7.2.0 (8372)

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 7.2.1 browser support.

Ensure that Logger's publicly-accessible ports are allowed through any firewall rules that you have configured.

- For root installs, allow access to port 443/tcp as well as the ports for any protocol that the logger receivers need, such as port 514/udp for the UDP receiver and port 515/tcp for the TCP receiver.
- For non-root installs, allow access to port 9000/tcp as well as the ports for any protocol that the Logger receivers need, such as port 8514/udp for the UDP receiver and port 8515/tcp for the TCP receiver.

> **Note:** The ports listed here are the default ports. Your Logger may use different ports. 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 7.2.1 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 7.2.1 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* 7.2.1 *Administrator's Guide:* Provides information on how to administer and use Logger. Also accessible from the integrated online Help.
- *Logger* 7.2.1 *Web Services API Guide:* Provides information on how to use Logger's web services. Also accessible from the integrated online Help.
- *Logger* 7.2.1 *Installation Guide:* Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM.
- *Logger* 7.2.1 *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.)
- Login banner is not dislplayed in Chinese or Japanese languages.

Upgrading to Logger 7.2.1 (L8395)

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 25, "Fixed Issues" on page 28, and "Open Issues" on page 31 before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 7.2.1. 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.

Logger 7.2.1 Upgrade Paths	
Software Versions	7.2
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. • 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 7.2.1.

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 7.2.1 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 7.2.0.8372 Logger version prior upgrading to Logger 7.2.1.
- Apply the Logger 7.2 post upgrade prior the OS upgrade and 7.2.1 build. For more information, see "Logger 7.2 Post Upgrade" on the next page.
- 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 7.2.1 includes OS Upgrade files for this purpose.
  - Download the upgrade files from the Micro Focus Entitlement Site to a computer from which you connect to the Logger UI.
  - For local or remote appliance upgrades, download the following file: `logger-8395.enc`.
  - Verify the upgrade files, as described in "Verifying Your Upgrade Files" on the previous page.
  - Modify the timeout value in the `logger.properties` file in the ArcMC as described in "To upgrade Logger Appliances remotely through ArcMC:" on page 13
  - Logger documentation is not included in your download package. Download your documentation from the Micro Focus Community.

Logger 7.2 Post Upgrade

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

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the "Prerequisites" on page 11 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. 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-8395.enc` file and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator’s Guide of the Logger version you are currently running.

To upgrade a Logger Appliance locally:

1. Make a configuration backup before the upgrade. For instructions, refer to the Logger Administrator’s Guide of the Logger version you are currently running.
2. Log into Logger and click **System Admin >System > License & Update**.
3. 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_20211129220710.enc`

4. Look for the `logger-8395.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.

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 7.2.1, 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 7.2.1 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 7.2.0.8372 Logger version prior upgrading to Logger 7.2.1.
- 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 17.
- 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 18.
- 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" on the

next page.

- If you are on RHEL 7.X , modify the login configuration file. For more information, see "Editing the logind Configuration File for RHEL 7.X" on 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-8395-remote.enc`
  - For local upgrades, download the following file: `ArcSight-logger-7.2.1.0.8395.0.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 10

Increasing the User Process Limit

Before installing or upgrading Logger, you must increase default user process limit while logged in as user *root*. This ensures that the system has adequate processing capacity.

> **Note:** This change is only necessary when installing Software Logger on your own Linux system. It has 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 15 are met before you begin.

- To upgrade Logger from ArcMC, see "To upgrade Software or VMWare Loggers remotely through ArcMC: " on the next page.
- To upgrade Software Logger locally, see "To upgrade Software Logger locally:" on the next page.
- 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-8395-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-7.2.1.0.8395.0.bin
   ./ArcSight-logger-7.2.1.0.8395.0.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-7.2.1.0.8395.0.bin
   ./ArcSight-logger-7.2.1.0.8395.0.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
7.2.1.

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

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

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

PRESS <ENTER> TO CONTINUE:
```

3. The 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/

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
```

Remote Upgrade Issue

To successfully upgrade to the latest Logger 7.2.1 version, it is required to apply the 7.2 post upgrade and OS upgrade first. These additional steps will fix any security vulnerabilities and get the latest security updates.

1. You must be on 7.2.0.8372 Logger version prior upgrading to Logger7.2.1.
2. Log into Logger and click **System Admin >System > License & Update**.
3. Apply the `postupgrade-logger-7.2.0-chrony-fix.enc` file. Make sure all the logger services have started correctly. A failure in the post upgrade could result in Logger failure. For further details, see "Logger 7.2 Post Upgrade" on page 12.
4. Upgrade your OS as appropriate. Deploy the `osupgrade-logger-rhel79_20211129220710.enc` file.
5. Look for the `logger-8395.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.

Publishing Reports to CSV Format Produce an Empty File

When running a report in Explorer and publishing to CSV format, the output CSV file is empty when opened. To work around this issue, follow these steps:

1. Right-click the report you want to publish to a CSV file in Reports > Explorer, and select **Run with delivery options**.
2. Select **Publish**, and choose **Comma Separated** from the Report Format menu.
3. Name the report, and click **Publish Now**.
4. Specify the report parameters, and click **Run Now**.
5. After you get a Success status, find and right-click your published report in Explorer, and select **View**.
   You will now be able to download your report as a CSV file.

Random Failure When Adding an SNMP Destination

An error may produced when adding an SNMP destination in Logger. If this occurs, follow these workaround steps:

1. Turn down connector services from loggerd or monit.
2. Search the `remote.management.password.hashed` property in `agent.properties` under `.../arcsight/connector/current/user/agent/agent.properties`
3. Comment out the property or remove it, and add a new one with an updated value provided by Tech Support or a Logger of the same version that is working.
   For example: `20307E218D28F4BE107D95E451C688E716A8ACFC0EF9DBD12D1A422F05A2A62`
4. Save your changes.
5. Search the `connector.cwsapi.password` property in the `logger.properties` under `...userdata/logger/user/logger/logger.properties`
6. Comment out the property or remove it, and add a new one with an updated value provided by Tech Support or a Logger of the same version that is working.
   For example: `OBFUSCATE.4.0.2:UKuXLA241MMC575GFvpSNw==`
7. Save your changes, and restart all services.

Fixed Issues

The following issues are fixed in this release.

Installation

Issue	Description
295435	After uninstalling the process in SW Logger, some files might not be found on the installation directory due to immutable attributes. Fix: The issue has been fixed. Installation is properly uninstalled.
296348	G10 appliances with fresh install had the ReportEngine.dat file after deployment. Fix: The issue has been fixed. No extra files are installed.
296943	Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation caused the installation to fail. Fix: The issue has been fixed.

Localization

Issue	Description
296909	When the locale is set to Chinese traditional, the <date> element contains Chinese characters. The locale issue is preset in config backup module. Fix: The issue has been fixed. Now, the Secure Copy Protocol (SCP) command functions properly when using the SCP Only in the backup server for secure copy.

General

Issue	Description
302272	When archiving data from a Logger Appliance, the "GMT+x" time zone incorrectly appeared as "GMT-x", while the "GMT-x" time zone appeared as "GMT+x". Fix: Appliances using GMT are inverted by design. Functionality has been documented.

Configuration

Issue	Description
304074	When enabling a Receiver, Logger did not validate the Research File System (RFS) mount it referenced. Fix: The issue has been fixed.
297661	When creating a search group and applying search group filters, the refresh on the admin dashboard overrode the filter settings. Fix: The issue has been fixed. Filter settings are correctly applied.
294505	Unable to correctly identify which user/group permissions was granted to a category. All Report category permissions were labeled as "edit and save reports". Fix: The issue has been fixed.
293620	After sending events to the Second Apache instance, the logs did not rotate and grew higher than expected. Fix: The issue has been fixed.

Analyze/ Search

Issue	Description
293615	Real-time alerts could not be enabled. The host was not appropriately registered. Fix: The issue has been fixed. Real-time alerts can be enabled.
313266	Peer searches with a pipe operator, a time range of 1 hour or more, and a latency period of +1 second caused discrepancies between the peer stats and UI as the search results tables became unresponsive. Fix: The issue has been fixed. The search is no longer stuck when having latency.
292746	When executing a peer search with some settings (a time range of +30 minutes, a "name is not null", and the Discover Fields enabled) the search became unresponsive. Fix: The issue has been fixed. The peer search can be executed properly.
294530	The event count shows substantially high numbers when using the deviceEventClassId = "eps:102" query. Fix: The issue has been fixed.
292832	The Java CC parser was not able to parse expressions with a =NOT condition after a SQL statement. Fix: The issue has been fixed.

Issue	Description
293761	From the New Search page, when executing a seach using deviceVendor=ArcSight OR deviceProduct=Logger AND message is not null, an exception message is displayed. Fix: The issue has been fixed. The exception is not longer displayed.
292943	If the user has an ESM as a peer, the peer stats tool will flag the ESM as running during the search even if the overall search already reached the hit limit. Fix: The issue has been fixed. Search will be stopped once reaching the maximum hit limit.
294821	The transaction operator did not work as expected. 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, the deviceHostName was not populated. Fix: The issue has been fixed. The deviceHostName operator is properly populated.
314213	Unable to see the Select Criteria in the properties tab when editing the filter in Query Explorer. Fix: The issue has been fixed. The Select criteria are available in the query explorer.
294894	Aggregate functions such as avg and stdev were not functional in peer mode. Fix: The issue has been fixed. Now, aggregate functions work in peer mode.
297682	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. However, from the SOAP API, a report can only be run when the individual has the right to view, run, and schedule all reports. Fix: The issue has been fixed. The same rights apply to Web UI and SOAP API.
298805	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 did not include events after recreation. Fix: The issue has been fixed.
301315	When Logger A and Logger B were configured to the peer by hostname using authorization ID/codes, the peer queries initiated from Logger B to Logger A failed. Fix: The issue has been fixed. The peer queries from all Loggers are correctly sent.

Reports

Issue	Description
296098	Binary columns included in the ArcSight DB datasource query were not displayed on Classic Reports. Fix: The issue has been fixed.
292749	If you saved a peer search (using the saved search option) from Search UI and the peers have a significant delay, the report creation failed due to timeout. Fix: The issue has been fixed. A message indicating the report cannot be saved is displayed in the Search page.

Open Issues

This release contains the following open issues.

Localization

Issue	Description
370065	Login banner is not displayed in Chinese or Japanese languages. Workaround: Manually add the banner information from the login_banner.html and refresh the page. Logger Software: <logger_installation_path>/userdata/platform/login_banner.html Logger Appliance: <logger_installation_path>/arcsight/userdata/platform/login_banner.html

Dashboards

Issue	Description
299394	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. Workaround: Name the dashboard differently.

Analyze/Search

Issue	Description
313444	The insubnet operator is not supported in the Advanced Search query editor. Workaround: To add a condition with insubnet operator, enter the search manually.
312588	When using a filter or a saved search to create reports from Logger Search Queries, the report is executed correctly. However, when the user updates the filter or the saved search with a different query, the report does not run properly. Workaround: Re-create reports using the same query object.

Issue	Description
304066	When using the auto complete feature on the search page, if the inserted query has a double quote followed by a bracket ("[ ), it will not be executed. Workaround: Remove the backslash followed by a double quote on both sides of the string. You can also do this when a double quote is followed by any special character such as "\, "/, "[, "], or ",.
303494	Unable to view the fields you are looking for in the search results when searching non-default fields. Workaround: Create a custom field set or use the "All Fields" field set.
303442	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. Workaround: Remove any renamed fields from the fieldset.
303398	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".
302592	Command Center search will return the error message "There is a problem: null" when charting the aggregation results certain fields, if you fail surround the field name with parenthesis. Workaround: If you receive this error message, check your query, and add parenthesis if needed.
301666	When a system has more than one peer and a peer stops responding, some pages in the user interface can become slow to display. The delay happens regardless of the reason the peer system is not responding. Workaround: Identify the peer that is not responding and remove its peer relationship. You can re-add the peer later when it is back in service.
297532	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.
296865	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.

Issue	Description
296859	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. Workaround: Turn off "overwrite same content" before importing.
296739	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. Workaround: Wait a few minutes before downloading to get the full export file.
296581	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.
296401	Split charts cannot be exported. Workaround: None available at this time.
295754	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. 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.
295565	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. Workaround: None available at this time.

Issue	Description
294699	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. Workaround: None available at this time.
294698	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. Workaround: Use a different name for the search result.
294661	ESM triggers a failed peer with a Logger prior than 7.1.1 version or ESM working as a node. Workaround: None available at this time.

Configuration

Issue	Description
378104	After uploading the license and update the process start, the system will display and error message. Workaround: Log out and Log in again. License will be consumed properly.
378033	SNMP functionality fails with authentication user errors . Workaround: Go to System Admin > SNMP page and save the persistent configurations displayed on the page.
348246	After a restore backup, the appliance IP address returned to default factory IP address causing data logs to not be sent or received. Workaround: Manually reconfigure the network interface.
315172	When the logger generates a new certificate connector can no longer forward events to it since it has lost the secure communication channel with the Logger destination. Workaround: Re-import the new certificate and restart the connector.
303258	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.
301823	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.

Issue	Description
299231	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. Workaround: When connecting another cluster with client authentication, clear the keystore before configuring. This can be done with the commands:
298825	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.
298124	Logger drops the non-cef events sent to a UDP receiver configured using an encoding different than UTF-8 or ASCII. Workaround: change the encoding of the receiver to UTF-8.
296731	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.
296070	NIC bonding information does not appear in the UI after configuring NIC bonding. Workaround: None available at this time.
294922	Logger License is displaying error messages on Reports using peers. Workaround: Restart the Logger.

Installation

Issue	Description
384017	When upgrading Logger, the Logger UI will be disabled while processes restart. However, the upgrade is executed as expected. Workaround: None available at this moment.
302670	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.

Reports

Issue	Description
384151	When publishing a smart report in CSV format from the Explorer right upper menu, it shows no data. Workaround: Reports can still be exported using CSV format using that same menu. Make sure the smart report is “run with delivery options” and published using the comma separated value as the report format.
295991	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. Workaround: Execute the Logger Search Report again with the "local-only" option unchecked.
295783	Duplicate columns name will not display in a logger search based report. Workaround: None available at this time.
294702	When installing Software Logger in ReHat and CentOS version 8. X, data science cannot be enabled. Workaround: Install Python 2.7.1 using the command "yum install python2". Then, enable the data science and restart the logger.
292898	Schedule MaxMind reports are failing email delivery. Workaround: Log into logger and extract the report manually.

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 7.2.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!