
Micro Focus Security ArcSight Logger

Software Version: 7.3

Release Notes



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

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

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

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

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

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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://www.microfocus.com/en-us/contact-support/stackb
Support Web Site	https://www.microfocus.com/en-us/support
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/#gsc.tab=0

Logger 7.3 Release Notes

Standalone ArcSight Logger version 7.3 (L8422) release is available in two form factors: Appliance and Software.

Logger 7.3 supports two types of appliance models, L7700 or L8000. Whenever instructions for one or the other differ, you will need to follow the ones that apply to your specific model.

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.



IMPORTANT: You can verify the type of Logger you have from the console, by executing either or both of these commands (as needed):

```
cat /etc/arcsight_model
```

```
cat /etc/OpenText_model
```

The output of these commands would be either your appliance model (**L7700** or **L8000**) or **No such file or directory** if you have a Software Logger.

This section contains the following topics:

What's New

The Security ArcSight Logger 7.3 (L8422) is a maintenance release, addressing security vulnerabilities and other issues found in Logger 7.2.2.

In addition, the following improvements have been made:

- The SSL Server Certificate generation now offers the option to specify additional host names (Subject Alternative Names: SANs), providing an extra layer of certificate security when connecting to certified browsers
- Search now can be narrowed down to multiple or specific peers, storage groups or device groups

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

- ["Fixed Issues" on page 27](#)
- ["Open Issues" on page 28](#)
- ["Known Issues" on page 23](#)

For details about these features, see the [ArcSight Logger 7.3 Administrator's Guide](#).

Technical Requirements

Logger requires the following minimum system setup.

Specification	Details
CPU, Memory, and Disk Space for Enterprise Version of Software Logger	<ul style="list-style-type: none">• 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 <p>Note: Using a network file system (NFS) as primary event storage is not recommended.</p>
CPU, Memory, and Disk Space for Trial Logger and VM Instances	<ul style="list-style-type: none">• CPU: 1 or 2 x Intel Xeon Quad Core or equivalent• Memory: 4 –12 GB (12 GB recommended). <p>Logger will take up 60% of the available memory, so in a 12 GB setup, this will amount to 7.2 GB of RAM.</p> <ul style="list-style-type: none">• Disk Space: 10 GB (minimum) in the Logger installation directory• Temp directory: 1 GB
Server	<p>For Software form factor:</p> <ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 7.9, 8.6, Rocky Linux 8.6. For more information, see Editing the logind Configuration File for RHEL 7.X. <p>For L7700 Appliance upgrade:</p> <ul style="list-style-type: none">• Red Hat Enterprise Linux 7.9. <p>The appliance model L8000 is being introduced with the Logger 7.3 version.</p>
VM Instances	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.



Customers running on platforms not provided in the Technical Requirements or with untested configurations will be supported until the point Micro Focus determines the root cause is the untested platform or configuration. According to the standard defect-handling policies, Micro Focus will prioritize and fix issues we can reproduce on the tested platforms.

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 and L7600 are no longer supported.



The appliance model L8000 is being introduced with the Logger 7.3 version.

- 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
7.3	May, 2023	L7700	Certified on: RHEL Linux 7.9 RHEL Linux 8.6 Rocky Linux 8.6 Supported on: RHEL Linux 7.8 RHEL Linux 8.4 VM instance The VM image includes the Logger installer on a 64-bit CentOS 7.9.	Microsoft Edge * Firefox * Chrome *	7.2.2 (L8402) 7.2.1 (L8395) 7.2 (L8372) 7.1.2 (L8354) 7.1.1 (L8343) 7.1 (L8336)
7.3	July, 2023	L8000	Certified on: RHEL Linux 8.6	Microsoft Edge * Firefox * Chrome *	N/A

Connecting to the Logger User Interface

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection.

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 the complete Logger 7.3 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 7.3 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.
- **[ArcSight Logger 7.3 Administrator's Guide](#):** Provides information on how to administer and use Logger. Also accessible from the integrated online Help.
- **[Logger 7.3 Web Services API Guide](#)** : Provides information on how to use Logger's web services. Also accessible from the integrated online Help.
- **[Logger 7.3 Installation Guide](#)** : Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM.
- **[Logger 7.3 Best Practices Guide](#)** : Provides information on how to configure and use Logger for best performance.

Additional Logger documentation, including the Logger Data Migration 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.

This section contains the following topics:

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 7.3 (L8422)

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

This section contains the following topics:



Note: Be sure to review the sections "[Known Issues](#)" on page 23, "[Fixed Issues](#)" on page 27, and "[Open Issues](#)" on page 28 before upgrading your logger.

Upgrade Paths


The following table lists the upgrade paths to Logger 7.3. 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, point to the ArcSight Logger logo in the upper-left corner of the screen.



IMPORTANT: Logger version 7.3 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 7.3 Upgrade Paths	
Software Versions	7.1/7.1.1/7.1.2/7.2.0/7.2.1/7.2.2
Appliance Models	L7700  The appliance model L8000 is being introduced with the Logger 7.3 version, and therefore cannot be upgraded from previous versions
Operating System Upgrades	<ul style="list-style-type: none">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.

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.

To download your upgrade files, visit:


<https://www.microfocus.com/en-us/support/downloads/>

Form Factor	Files to download
Appliance	<p>For local or remote L7700 appliance upgrades:</p> <p>logger-8422.enc</p> <p>logger-8422.enc.sig</p> <p> The appliance model L8000 is being introduced with the Logger 7.3 version, and therefore cannot be upgraded from previous versions</p>
Software	<p>For local upgrades:</p> <p>ArcSight-logger-7.3.0.8422.0.bin</p> <p>ArcSight-logger-7.3.0.8422.0.bin.sig</p> <p>For remote upgrades using ArcMC:</p> <p>logger-sw-8422-remote.enc</p> <p>logger-sw-8422-remote.enc.sig</p>

And for instructions on how to verify the signature, see:

<https://support.microfocus.com/kb/doc.php?id=7025140>


Upgrading the Logger Appliance

 This topic applies to the L7700 Logger Appliance models only.

This section describes how to upgrade the Logger appliance. For fresh installation instructions refer to the [Logger 7.3 Installation Guide](#).

This section contains the following topics:

Prerequisites

 This topic applies to the L7700 Logger Appliance models only.

Be sure that you meet these prerequisites before upgrading Logger:

- When upgrading to Logger 7.3 version, the event flow will be automatically stopped.
- Make a configuration backup before upgrading to this release. For instructions, refer to the [ArcSight Logger 7.3 Administrator's Guide](#).

- 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 7.3 includes OS Upgrade files for this purpose.



If you plan to upgrade to version 7.2.1 prior to version 7.3.0, **do not apply** the latest OS update until after the Logger upgrade is completed

- For local or remote appliance upgrades, download the files described in [Verifying Your Upgrade Files](#), and follow the instructions to verify the signature. The files must be downloaded into a computer from which you connect to the Logger UI.
- Modify the timeout value in the `logger.properties` file in the ArcMC as described in [To upgrade Logger Appliances remotely through ArcMC](#).

Logger documentation is not included in your download package. Download your documentation from the [Micro Focus Community](#).

Upgrade Instructions



This topic applies to the L7700 Logger Appliance models only.

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:



IMPORTANT: You can verify the type of Logger you have from the console, by executing either or both of these commands (as needed):

```
cat /etc/arcsight_model
```

```
cat /etc/OpenText_model
```

The output of these commands would be either your appliance model (**L7700** or **L8000**) or **No such file or directory** if you have a Software Logger.

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 `<install_dir>/userdata/arcmc/logger.properties` does not exist, create the file as a non-root user.
- Add the new property (unit value in seconds):

```
node.upgrade.thread.timeout= 10800
```

- Update the `logger.properties` file using the following commands:

```
Chown <non -root user>:<non-root user> logger.properties
```

```
Chmod 660 logger.properties
```

2. Deploy the Logger upgrade using the `logger-8422.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 [ArcSight Logger 7.3 Administrator's Guide](#).

To upgrade a Logger Appliance locally:



IMPORTANT: You can verify the type of Logger you have from the console, by executing either or both of these commands (as needed):

```
cat /etc/arcsight_model
```

```
cat /etc/OpenText_model
```

The output of these commands would be either your appliance model (**L7700** or **L8000**) or **No such file or directory** if you have a Software Logger.

1. Make a configuration backup before the upgrade. For instructions, refer to the [ArcSight Logger 7.3 Administrator's Guide](#).
2. Log into Logger and click **System Admin > System > License & Update**.
3. Upgrade your OS as appropriate. If you are upgrading an L7700 series appliance, deploy the OS upgrade by using the file:

```
osupgrade-logger-rhel179_202304170755.enc
```
4. Look for the `logger-8422.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 7.3, available for download from the [Micro Focus Community](#).

This section contains the following topics:

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- When upgrading to Logger 7.3 version, the event flow will be automatically stopped.
- Make a configuration backup before upgrading to this release. For instructions, refer to the [ArcSight Logger 7.3 Administrator's Guide](#).
- 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.
- If your system is running on RHEL 7.X, upgrade to the latest version of 7.9.
- Before installing or upgrading to Logger 7.3 (and when upgrading from RHEL 7.X to RHEL 8.4), you must connect through SSH to the Logger console to validate the presence of the packages in the following table. Use the command in the **Verification command** column for each package.

If all packages are already installed, you already comply with the requirements and can proceed with the Logger 7.3 installation/upgrade (make sure to check the rest of the prerequisites in this list).

If any of the packages are missing, proceed to install them by using the command in the **Installation command** column. Once the installation of all the packages is finished, restart the Logger processes and proceed with the upgrade (make sure to check the rest of the prerequisites in this list).

Package	Verification command	Installation command
libnsl	<code>rpm -qa grep libnsl</code>	<code>yum install libnsl</code>
compat-openssl10	<code>rpm -qa grep compat-openssl10</code>	<code>yum install compat-openssl10</code>
ncurses-compat-libs	<code>rpm -qa grep ncurses-compat-libs</code>	<code>yum install ncurses-compat-libs</code>

- 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 17](#).
- 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.

- For local or remote software upgrades, download the files described in [Verifying Your Upgrade Files](#), and follow the instructions to verify the signature. The files must be downloaded into a computer from which you connect to the Logger UI.

Increasing the User Process Limit

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



Note: This change is only necessary when installing Software Logger on your own Linux system. It has already been done for Logger on VMWare VM.

To increase the default user process limit:

1. Open the file `/etc/security/limits.d/<NN>-nproc.conf`.



Where `<NN>` is 20 for RHEL 7.X and 8.6, and Rocky Linux 8.6.

- If you do not already have a `/etc/security/limits.d/<NN>-nproc.conf` file, create one (and the `limits.d` directory, if necessary).
- If the file already exists, delete all entries in the file.

2. Add the following lines:

```
* soft nproc 10240
* hard nproc 10240
* soft nofile 65536
* hard nofile 65536
```



Caution: Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system run time errors.

3. Reboot the machine.
4. Run the following command to verify the new settings:

```
ulimit -a
```

5. Verify that the output shows the following values for “open files” and “max user processes”:

```
open files          65536
max user processes  10240
```

Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7.X, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.X:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. 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 the `/etc/sysctl.conf` file. Add the TCP OS configuration properties using the following steps:

1. Edit the system file by executing this command:

```
vi /etc/sysctl.conf
```

Next, press `Shift + G` to reach the end of file.

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 the ["Prerequisites" on page 14](#) 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 `<install_dir>/userdata/arcmc/logger.properties` does not exist, create the file as a non-root user.
- Add the new property :

```
node.upgrade.thread.timeout= 10800
```

- Update the `logger.properties` file using the following commands:

```
Chown <non -root user>:<non-root user> logger.properties
```

```
Chmod 660 logger.properties
```

2. Upgrade your OS to the latest distribution as it fixes additional security vulnerabilities.
3. Deploy the downloaded upgrade file `logger-sw-8422-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:
From the Logger's installer directory:

```
chmod u+x ArcSight-logger-7.3.0.8422.0.bin
```

```
./ArcSight-logger-7.3.0.8422.0.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-7.3.0.8422.0.bin
```

```
./ArcSight-logger-7.3.0.8422.0.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 7.3.0

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

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

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

PRESS <ENTER> TO CONTINUE:
```

3. The License Agreement screen is displayed. To review the agreement

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

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

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

4. To accept the terms :
Software: Select **I accept the terms of the License Agreement** and click **Next**
VMWare: Type **Y** and press **Enter**. To exit the installer at any point during the installation process, type **quit** and press **Enter**.
5. If Logger is currently running on this machine, an intervention required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the upgrade, or click **Quit** to exit the installer.
6. Once all Logger processes are stopped, the installer checks that the installation prerequisites are met:
 - Operating system check—The installer checks to see if your device is running a supported operating system, otherwise, a warning will be displayed (this will not prevent the installation process).

To proceed with the upgrade:

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

VMWare: Type **1** and press **Enter**. To exit the installer and continue to upgrade the OS, type **2** and press **Enter**.



Note: Micro Focus ArcSight strongly recommends that you upgrade to a supported OS before upgrading Logger.

- 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:

- Type the installation path for Logger (the default installation path is /opt, but 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. Do not specify a different location.
- Press **Enter**

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 [ArcSight Logger 7.3 Administrator's Guide](#).

Known Issues

The following known issues apply to this release. Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit [Micro Focus Support](#), then select the appropriate product category.

- ["OCTCR33I383147 - Restarting a Logger Appliance takes a long time" below](#)
- ["OCTCR33I594049 - ESM and Transformation Hub forwarders might need the processors process restarted before events can be forwarded \(intermittent issue\)" on page 25](#)
- ["OCTCR33I637005 - The Logger Appliance network interface fails after a configuration backup is restored" on page 25](#)
- ["OCTCR33I635057 - Chinese characters in a chart title are not displayed correctly \(PDFs only\)" on page 26](#)

OCTCR33I383147 - Restarting a Logger Appliance takes a long time

Issue: When restarting a Logger Appliance, the `arcsight_server_ready` file is not created quickly enough, causing a delay.

Workaround:



This process requires stopping Logger processes and this will affect event ingestion. Therefore, these steps should be performed during a maintenance window, when there is low event ingestion and stopping Logger processes is allowed.

1. Open a ssh terminal connected to the Logger Appliance
2. Stop all data ingestion and all Logger processes except the `postgresql` process by executing the following steps:
 - Stop all processes:

```
/opt/arcsight/logger/bin/loggerd stop
```

- Start `postgresql`. This will also start `aps` and `servers`:

```
/opt/arcsight/logger/bin/loggerd start postgresql
```

3. Give some time for the processes included in the previous step to get started.
4. Stop aps and servers:

```
/opt/arcsight/logger/bin/loggerd stop aps
```

```
/opt/arcsight/logger/bin/loggerd stop servers
```

5. Make sure only the postgresql process is running by executing this command:

```
/opt/arcsight/logger/bin/loggerd status
```

6. Run the following command and query, and save the output to a log file:

```
/opt/local/pgsql/bin/psql -U web rwdb -c "select * from pg_stat_user_ tables;" > /opt/loggerusertabinfo_before.out
```

7. Run the following command and query, and save the output to a log file:

```
/opt/local/pgsql/bin/psql -U web rwdb -c "SELECT relname AS \"table_ name\", pg_size_pretty(pg_table_size(C.oid)) AS \"table_size\" FROM pg_ class C LEFT JOIN pg_namespace N ON (N.oid = C.relnamespace) WHERE nspname NOT IN ('pg_catalog', 'information_schema') AND nspname not like '^pg_ toast' AND relkind IN ('r') ORDER BY pg_table_size(C.oid) DESC;" > /opt/loggertableusage_before.out
```

8. Perform a VACUUM ANALYZE operation on your database to reclaim space and update the statistics. Be aware that this step can take some time to execute.

```
/opt/local/pgsql/bin/vacuumdb --analyze-in-stages --all --verbose -U web > /opt/loggerpsqlvacuum.out
```

9. Run the following command and query, and save the output to a log file:

```
/opt/local/pgsql/bin/psql -U web rwdb -c "select * from pg_stat_user_ tables;" > /opt/loggerusertabinfo_after.out
```

10. Run the following command and query, and save the output to a log file:

```
/opt/local/pgsql/bin/psql -U web rwdb -c "SELECT relname AS \"table_ name\", pg_size_pretty(pg_table_size(C.oid)) AS \"table_size\" FROM pg_ class C LEFT JOIN pg_namespace N ON (N.oid = C.relnamespace) WHERE nspname NOT IN ('pg_catalog', 'information_schema') AND nspname not like '^pg_ toast' AND relkind IN ('r') ORDER BY pg_table_size(C.oid) DESC;" > /opt/loggertableusage_after.out
```

11. Restart the Logger processes:

```
/opt/arcsight/logger/bin/loggerd start
```

12. Create an archive with the log files created and upload them to the FTP site:


```
tar -cvzf /opt/stats.tar.gz /opt/loggerusertabinfo_before.out  
/opt/loggertableusage_before.out /opt/loggerusertabinfo_after.out  
/opt/loggertableusage_after.out /opt/loggerpsqlvacuum.out
```

OCTCR33I594049 - ESM and Transformation Hub forwarders might need the processors process restarted before events can be forwarded (intermittent issue)

Issue: After uploading the ESM/Transformation Hub certificate, adding them as a destination, and creating a Forwarder for them, the dashboard might show events reaching the receivers but not being forwarded to the destination (no **EPS Out** and **Forwarded Total Events** shows 0)

Workaround: Restart the process using the following commands:

- For Logger Appliance:

```
/opt/arcsight/logger/bin/./loggerd restart processors
```

- For Software Logger:

```
<LOGGER_HOME>/current/arcsight/logger/bin/./loggerd restart processors
```

Where <LOGGER_HOME> it's the path where your Software Logger is installed.

OCTCR33I637005 - The Logger Appliance network interface fails after a configuration backup is restored

Issue: After restoring a configuration backup the network interface fails to set the correct IP, and the Logger UI is inaccessible.

Workaround: Correct the IP value by performing the following steps:

1. Open up the `ifcfg-ens2f0` file with the following command:

```
nano /etc/sysconfig/network-scripts/ifcfg-ens2f0
```

2. Verify that the file contains the IPADDR and NETMASK values (if the values are not present, the corresponding lines must be added).
3. Correct the values with the default ones:

```
IPADDR=<Appliance_IP_Address>
```

```
NETMASK=255.255.224.0
```

OCTCR33I635057 - Chinese characters in a chart title are not displayed correctly (PDFs only)

Issue: For reports exported in PDF format, if the title of a chart contains Chinese characters, they won't be displayed correctly.

Workaround: Change the font family in the `bar.ict` file from:

```
chartObj.fontFamily="Verdana";
```

to

```
chartObj.fontFamily="roboto-light";
```

The `bar.ict` file location depends on your Logger form factor:

- For Logger Appliance:

```
/opt/arcsight/userdata/logger/Intellicus/reportengine/templates/charts/amchart_javascript/Default/bar.ict
```

- For Software Logger:

```
<LoggerInstallDir>/userdata/logger/Intellicus/reportengine/templates/charts/amchart_javascript/Default/bar.ict
```

Fixed Issues

The following issues are fixed in this release.

Configuration

Issue	Description
OCTCR33I502005	Enhance Logger CSR (Certificate Signing Request) to include S.A.N. (Subject Alternative Name) fields This option has been added to the CSR generation process.
OCTCR33I298825	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. This issue is not reproducible in version 7.3

Analyze/ Search

Issue	Description
OCTCR33I501012	Search results are not automatically sorted by endTime This issue is not reproducible in version 7.3
OCTCR33I301666	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. This issue is not reproducible in version 7.3
OCTCR33I313444	The insubnet operator is not supported in the Advanced Search query editor. This issue pertained to Classic Search, which has been deprecated in the 7.3 release.

Open Issues

This release contains the following open issues.

Dashboards

Issue	Description
OCTCR33I299394	<p>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.</p> <p>Workaround: Name the dashboard differently.</p>

Analyze/Search

Issue	Description
OCTCR33I550028	<p>Field summary shows "no records available" when the search uses the sort operator.</p> <p>There is no workaround at this time.</p>
OCTCR33I312588	<p>When using a filter or a saved search to create reports from Logger Search Queries, the report is executed correctly. However, when the user updates the filter or the saved search with a different query, the report does not run properly.</p> <p>Workaround: Re-create reports using the same query object.</p>
OCTCR33I304066	<p>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.</p> <p>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 ",.</p>
OCTCR33I303494	<p>Unable to view the fields you are looking for in the search results when searching non-default fields.</p> <p>Workaround: Create a custom field set or use the "All Fields" field set.</p>
OCTCR33I303442	<p>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.</p> <p>Workaround: Remove any renamed fields from the fieldset.</p>

Issue	Description
OCTCR33I302592	<p>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.</p> <p>Workaround: If you receive this error message, check your query, and add parenthesis if needed.</p>
OCTCR33I296859	<p>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.</p> <p>Workaround: Turn off "overwrite same content" before importing.</p>
OCTCR33I296739	<p>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.</p> <p>Workaround: Wait a few minutes before downloading to get the full export file.</p>
OCTCR33I296401	<p>Split charts cannot be exported.</p> <p>There is no workaround at this time.</p>
OCTCR33I294698	<p>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.</p> <p>Workaround: Use a different name for the search result.</p>

Configuration

Issue	Description
OCTCR33I683011	<p>The snmpd.conf file has the correct group but no permissions.</p> <p>Workaround: Go to System Admin > SNMP and click on the Save button.</p>
OCTCR33I315172	<p>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.</p> <p>Workaround: Re-import the new certificate and restart the connector.</p>
OCTCR33I303258	<p>A user can edit a Forwarder while the feature is enabled. This can cause the Forwarder to stop sending events.</p> <p>Workaround: Before editing the Forwarder, disable it. Then edit it and re-enable it to have the Forwarder send events to its target destination.</p>

Issue	Description
OCTCR33I301823	<p>When using the Setup Wizard to enter a Logger Appliance initial configuration, Logger does not check that you have entered all the required information before submitting it. This can cause the setup program to fail.</p> <p>Workaround: Enter valid values for all required Setup Wizard fields.</p>
OCTCR33I295431	<p>When configuring FIPS in a software fresh install, the certificates are not loaded in the bcfps_ks file, not allowing to create Logger destinations.</p> <p>Workaround:</p> <ol style="list-style-type: none">1) Delete the /opt/arcsight/current/arcsight/connector/current/user/agent/fips/bcfps_ks file.2) Disable and then re-enable FIPS.3) Restart the Logger processes.
OCTCR33I294922	<p>Logger license is displaying error messages on Reports using peers.</p> <p>Workaround: Restart the Logger.</p>

Installation

Issue	Description
OCTCR33I302670	<p>Installation of multiple Solution Packages in Software Loggers with a root user may fail if the SOX v4.0 solution package is installed before others.</p> <p>Workaround: If you are installing the SOX v4.0 solution package on Software Logger with a root user, leave this step for the end.</p>

Reports

Issue	Description
OCTCR33I295783	<p>Duplicate columns name will not display in a logger search based report.</p> <p>There is no workaround at this time.</p>
OCTCR33I292898	<p>Schedule MaxMind reports are failing email delivery.</p> <p>Workaround: Log into Logger and extract the report manually.</p>

Logger being managed by ArcMC

Issue	Description
OCTCR33I671021	<p>Pushing specific configuration values to a Logger from its managing ArcMC fails with Error: Failed to push configuration, "722SMreceiver1" to its Subscribers. See "Last Push Status" of each Subscriber for details.</p> <p>This affects the following configurations:</p> <ul style="list-style-type: none">• Storage group• Logger Configuration Backup• Logger SmartMessage Receiver <p>There is no workaround at this time.</p>

Security Fixes

The following security fixes were implemented in this release.

Description	CVE
Cross-Site Scripting (XSS)	CVE-2023-24469
XML External Entity Injection (XXE)	CVE-2023-24470

Additions to the Documentation

The information available from the documentation site supersedes the information available in the product's built-in context sensitive help.

Please refer to the guides listed here for the most up to date information:

<https://www.microfocus.com/documentation/arcsight/logger-7.3/>

Publication Status

Released: May 31, 2023

Updated: Thursday, October 12, 2023

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 7.3)

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!

Publication Status

Released: May 31, 2023

Updated: Thursday, October 12, 2023