Micro Focus Security ArcSight Logger

Software Version: 7.1.1

Release Notes

Document Release Date: November, 2020
Software Release Date: November, 2020

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:

ArcSight Product Documentation on the Micro Focus Security Community

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 7.1.1 Release Notes

Standalone ArcSight Logger version 7.1.1 (L8343) 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 7.1.1 (L8343) is a maintenance release, addressing security vulnerabilities and other issues found in Logger 7.1.

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

- "Fixed Issues" on page 22
- "Open Issues" on page 24
- "Security Fixes " on page 34

For details about these features, see the ArcSight Logger 7.1.1 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) 6.8, 6.9, 6.10, 7.6, 7.7, 7.8, and 8.1 For more information, see Editing the logind Configuration File for RHEL 7.X. • CentOS 6.9, 6.10, 7.6, 7.7, 8.1. For appliance upgrade: Red Hat Enterprise Linux 6.10, 7.8.
VM Instances	• 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.

Supported Platforms

Refer to the Logger Support Matrix, available on Micro Focus Community site for details on Logger 7.1.1 platform support.

Note: Be sure to upgrade your operating system (OS) to get the latest security updates. Upgrade your OS first, and then upgrade Logger. For Logger Appliances, an OS upgrade file is included in your upgrade package.

Connecting to the Logger User Interface

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the Logger Support Matrix available on Micro Focus Community site for details on Logger 7.1.1 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 7.1.1 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 7.1.1 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* 7.1.1 *Administrator's Guide:* Provides information on how to administer and use Logger. Also accessible from the integrated online Help.
- *Logger* 7.1.1 *Web Services API Guide:* Provides information on how to use Logger's web services. Also accessible from the integrated online Help.
- *Logger* 7.1.1 *Installation Guide:* Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM.
- *Logger* 7.1.1 *Best Practices Guide:* Provides information on how to configure and use Logger for best performance.

Localization Information

Localization support for these languages is available for this release:

- Japanese
- Traditional Chinese
- Simplified Chinese

You can either install Logger in one of the above languages as a fresh install or upgrade an existing English installation to one of these languages. The locale is set when you first install Logger. Once set, it cannot be changed.

Known Limitations in Localized Versions

The following are the currently known limitations in the localized versions of Logger:

- Only ASCII characters are acceptable for full-text search and the Regex Helper tool. Therefore, full-text search is not supported for Japanese, Simplified Chinese, or Traditional Chinese characters.
- The Login field on the Add User page does not accept native characters. Therefore, a Logger user cannot have a login name that contains native characters.
- The Report Parameter and the Template Style fields do not accept native characters.
- The following Logger UI sections are not localized: Field Summary and Search Page.
- The Certificate Alias field for ESM Destinations cannot contain native characters. Use only ASCII characters in the Certificate Alias field. (To open the Certificates page, type Certificates in the **Take me to...** search box, and click **Certificates** in the dropdown list.)

Upgrading to Logger 7.1.1(L8343)

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 21, "Fixed Issues" on page 22, and "Open Issues" on page 24 before upgrading your logger.

Upgrade Paths

The following table lists the upgrade paths to Logger 7.1.1. 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 7.1.1 Upgrade Paths	
Software Versions	7.1 **Note:** The Logger 7.1.1 upgrade will support both 7.1.0.8336.0 and 7.1.0.8337.0 builds.
Appliance Models	L350X, L750X, L750X-SAN, 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 7.1.1.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- You must be on Logger 7.1 prior to upgrading to Logger 7.1.1.
- Make a configuration backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the current Logger version.
- 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 prior the upgrade as it fixes additional security vulnerabilities. Logger 7.1.1 includes OS Upgrade files for this purpose.
- For OS upgrades, download the appropriate file:

  If you are upgrading an Lx500 series appliance, download the following file:
  `osupgrade-logger-rhel610-<timestamp>.enc`

  If you are upgrading an L7600 series appliance, download the following file:
  `osupgrade-logger-rhel78-<timestamp>.enc`

  If you are upgrading an L7700 series appliance, download the following file:
  `osupgrade-logger-rhel78-<timestamp>.enc`

- 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-8343.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 Logger as described in "To upgrade Logger Appliances remotely through ArcMC:" on the next page

- Logger documentation is not included in your download package. Download your documentation from the Micro Focus Community.

Upgrade Instructions

Follow the instructions listed below to upgrade your Logger. Ensure that you meet the "Prerequisites" on the previous page before you begin.

- To upgrade Logger from Logger, 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 Logger 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-8343.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. Log into Logger and click **System Admin >System > License & Update**.
2. Upgrade your OS as appropriate.
   - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel610-<timestamp>.enc`.
   - If you are upgrading an L7600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel78-<timestamp>.enc`.

- If you are upgrading an L7700 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel78-<timestamp>.enc`.

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

3. Look for the `logger-8343.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.

4. 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.

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 7.1.1, available for download from the Micro Focus Community.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- You must be on Logger 7.1 prior to upgrading to Logger 7.1.1.
- Stop any event flow in Logger before upgrading to 7.1.1 version.
- Make a configuration backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the current Logger version.
- 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 7.8.

If your system is running on RHEL or CentOS 6.X, upgrade to the latest version of 6.10.

- If not already done on the system, perform the following procedures:
  - Increase the user process limit on the Logger's OS. (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 page 15.
- 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 Logger, download the following file: `logger-sw-8343-remote.enc`
  - For local upgrades, download the following file: `ArcSight-logger-7.1.1.0.8343.0.bin`
- Logger documentation is not included in your download package. Download your documentation from the Micro Focus Community
- Verify the upgrade files, as described in "Verifying Your Upgrade Files" on page 9

Increasing the User Process Limit

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

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

To increase the default user process limit:

1. Open the file `/etc/security/limits.d/<NN>-nproc.conf`. (<NN> is 90 for RHEL or CentOS 6.10 and 20 for RHEL and CentOS 7.8.)
   - 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`

Upgrade Instructions

Follow the instructions listed below to upgrade Logger. Ensure that "Prerequisites" on page 13 are met before you begin.

- To upgrade Logger from Logger, 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 Logger 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-8343-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-7.1.1.0.8343.0.bin
   ./ArcSight-logger-7.1.1.0.8343.0.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-7.1.1.0.8343.0.bin
./ArcSight-logger-7.1.1.0.8343.0.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
7.1.1.

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.

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, L7500, L7500-SAN, and L3500 series Loggers:

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

A similar message is posted to the `dmesg` file. 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/

Fixed Issues

The following issues are fixed in this release.

Installation

Issue	Description
LOG-25306	After upgrading a software Logger from ArcMC, the ArcMC system displays an error message: Failed to bring up some processes successfully. The ArcMC Management process is not found. Fix: Now, Logger can be successfully upgraded.

Configuration

Issue	Description
LOG-25903 LOG-25848	TCP connections between Apache and internal processes were never closed and used again. Apache server was not disposing of these connections correctly, causing them to stay alive with the status CLOSE_WAIT. Symptoms, slow response of the system. Fix: Enable the Apache Proxy Pass Configuration, the keepalive, and TCP parameters in the OS, so the Apache server will correctly close the connections and release resources for the new connections.
LOG-25571	Postgresql upgrade was not working with the IPV6 disabled in the OS of Software Logger. Fix: The issue has been fixed.

Reports

Issue	Description
LOG-25774	Unable to sent a report via email using secure SMTP. Fix: Now, reports via email can be sent using secure SMTP.
LOG-25185	In Reports, when selecting a parameter with a boolean data type, the ReportClientLogs.log showed an exception causing the UI to refresh continuously. However, the report was not executed. Fix: Exception is no longer displayed.
LOG-25173	When a MaxMind report deployed from the cab file, the fieldset was configured to a report. However, if you checked the Data Source from outside, it showed the correct fieldset was set to the MaxMind field set. Fix: Now, the correct fieldset is assigned.

Search

Issue	Description
LOG-25767	For data that was retrieved from an archive, only the non-indexed searches were selected, even for queries that were indexed when using live data. Fix: Now, the queries are executed using the correct search type without affecting the forwarding of the events.
LOG-25709	When you canceled a search, the Configuration > Searches > Running Searches page showed the search was still running and never expired Fix: Now, the canceled searches appear with the correct status and they expire accordingly.
LOG-25485	ArcMC was not able to read logger nodes stats. Fix: ArcMC is now able to pull stats from Logger.

Open Issues

This release contains the following open issues.

Localization

Issue	Description
LOG-15905	The Logger configuration backup file has the format: <date>_<time>.configs.tar.gz. When the locale is set to Chinese traditional, the <date> element contains Chinese characters. This causes the Secure Copy Protocol (SCP) command to fail, if you use SCP only in the target backup server for Secure Copy. Workaround: Use openSSH for configuration backups.

Dashboards

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

General

Issue	Description
LOG-25273	In some instances, Logger will switch from light to dark after updating the theme right after install or upgrade. This might cause Logger to freeze. Workaround: Close the Logger browser tab and open it again.

Analyze/Search

Issue	Description
LOG-25370	Rentention period for the saved search results is not enforced automatically, it requires another search result to be persisted in order to trigger the removal of these searches. Workaround: Save an extra search result in order to remove the search results that have already passed their retention period.
LOG-25325	Unable to retrieve results from a persisted search with a peer that subsequently is temporarily powered down. Workaround: Ensure that the peer is up and reachable. Retrieve the search one more time.
LOG-25324	Unable to retrieve results from a persisted search with a peer that subsequently is removed. Workaround: None available at this time.
LOG-25305	Search result references are removed from the system 1 day after the retention has expired. Workaround: Subtract a day from the actual retention period.
LOG-25304	Search and search dashboards do not work as expected when opened in maintenance mode. In maintenance mode, you are only allowed to do the selected maintenance operation. Workaround: Reboot using the corresponding link.
LOG-25291	The field summary tab is not persisted by Logger on search results. Therefore, neither the Field Summary information nor the Discover Fields are displayed in such search results. Workaround: None available at this time.
LOG-25290	Unable to open an item from the list of active searches if the event details window is also open. Logger only supports one emergent window at a time. Workaround: Close the event details window.

Issue	Description
LOG-25272	Unable to rename the active search. Workaround: None available at this time.
LOG-25271	When a search result with peers is retrieved in the search dashboard, the page shows a wrong alias instead of the name chosen when persisting the search. Workaround: None available at this time.
LOG-25270	Search results are not retrieved after the original search has expired. Workaround: Log out from Logger and then log in. Try to retrieve the search again.
LOG-25245	Unable to export the | chart command in csv format from the Search page. The chart is unable to be represented in this format. Workaround: Make sure to select PDF format only.
LOG-25238	In search UI with the Field Summary and Discover Fields parameters checked, the field summary tab and results are not displayed even though the events retrieved have discovery fields results but are not CEF. Workaround: Use the Classic Search.
LOG-25224	In Firefox browser, the Save icon sometimes disappears when refreshing the page. Workaround: Refresh the page using Ctrl+F5.
LOG-25217	When running chartable queries, a session ID error may appear. However, the search is executed correctly and with no errors. Workaround: None available at this time.
LOG-25209	When you run a peer search with Discover Fields enabled, the hit count limit is ignored and the search is not completed affecting the search concurrency. Workaround: None available at this time.
LOG-25205	Some canceled searches, mostly peers, are still displayed (In Progress or Completed status) in the Search Dashboard after expired. However, search resources are no longer in use. Workaround: Remove the canceled searches manually if required. Then, wait about 10 seconds for Search Dashboard to reflect the correct status.
LOG-25157	When exporting a file from a Logger, the hit count does not match the limit hit count in the UI. However, if you download the file, all events are downloaded according to the hit count limit. Workaround: None available at this time.
LOG-25144	When exporting a report in PDF format, the report does not display a title. Workaround: If possible, select All Fields when exporting.
LOG-25129	The oldFileHash custom field is not searchable in a search query. If you use oldFileHash field as filter, no events are retrieved. Workaround: None available at this time.

Issue	Description
LOG-25113	When overwriting a fieldset set without the default fieldset checked, the first fieldset still appears as the default one in the drop-down. Workaround: Refresh the page to view the new default fieldset.
LOG-25073	When trying to persist a search result (with a name chosen by another user), the dialog window shows an error in the database while the search was saving. Workaround: Use a different name for the search result.
LOG-25072	In the search persistence, a validation error occurs when you add an incorrect value. If you enter the correct values before the success message is displayed, there is a short period of time where a message with the last validation error is shown. Otherwise, if no changes are made, the window closes automatically without having the option of correcting the invalid value. Workaround: None available at this time.
LOG-25014	In the Search page, when the head peer executes a search on a field present in the head peer but not in the peer nodes, the search spinner never stops. Workaround: Use the Classic Search or maintain the same schema on all loggers.
LOG-25006	Once the search is completed with peer failures, you are unable to review the contribution of the failing peers. Workaround: Review the internal events of this search.
LOG-24989	When you run a peer search (with an ESM as a peer), the hit count limit might be ignored by the ESM. If the hit count reaches its limit before the ESM scanning, Logger will no longer continue scanning events. Otherwise, the limit will be exceeded. Workaround: None available at this time.
LOG-24987	When running a peer search from the search page, peer errors are not displayed Workaround: Open the peer stats to review the real status of each peer.
LOG-24831	Logger search results between peer nodes using | sort function are inaccurate. When running the search in local mode, the system displays the correct results. However, when comparing results on the different peers, the results are different. Workaround: None available at this time.
LOG-24059	The transaction operator does not work as expected. The deviceHostName operator is populated when running a local search on one peer Logger with base event fields fieldsets or a peer search on a search head Logger with minimal field fieldsets. However, running a peer search on a search head Logger with base event fields fieldsets does not populate deviceHostName. Workaround: None available at this time.

Issue	Description
LOG-23419	When Logger scans a lot of events (a search without a query before both chart and span operators + a time range that includes many days), high levels of CPU usage might cause the search to fail. Workaround: Filter the events before the pipe, especially if some fields used in the chart and span operator are null, like deviceEventCategory is not null AND deviceReceiptTime is not null | chart count by deviceEventCategory span (deviceReceiptTime) = 5m. Avoid using chart and span operators combined with a considerably wide time range (months).
LOG-21067	Split charts cannot be exported. Workaround: None available at this time.
LOG-19261	For Logger health events generated internally every minute, the values of destinationAddress and deviceAddress are 127.0.0.1 instead of the real IP address. This issue only affects Logger running under RHEL 7.X on software and appliance form factors. Workaround: Follow the steps described below. Take into account that everything written before changing the property will look the same. 1. Get network adapter real names with: ls /sys/class/net/ or ifconfig -s | cut -d' ' -f1 . 2. Add Logger property named “logger.network.interface.name” on /opt/arcsight/userdata/logger/user/logger/logger.properties for appliances, and <install_dir>/userdata/logger/user/logger/logger.properties for software logger and set it with the value obtained from the previous step. 3. Restart logger.
LOG-18945	If an insubnet parameter has the wrong syntax, no error is reported when running peer searches. For local searches, the error is reported as expected. Workaround: For peer searches that contain the insubnet operator, first run a local search to check for any syntax errors. If no error is reported, then the peer search can be executed properly.
LOG-17318	When exporting search results around the hit limit with the re-run query checked, Logger may display the “Download results” link before the export file has finished populating. If you download the report during this period, the downloaded file might be incomplete. Workaround: Wait a few minutes before downloading to get the full export file.
LOG-16429	When exporting Source Types with common dependent parsers and the property "overwrite.same.content" enabled, Logger only imports the latest Source Type with its parser. The other Source Types do not include their parsers. Workaround: Turn off "overwrite same content" before importing.

Issue	Description
LOG-16347	Pipeline queries that include the 'where' operator, and exclude the 'user' field from a custom field list, display no results for the custom fields. For example, this query is missing the 'user' field from the custom field list and therefore has no results: _ deviceGroup IN ["192.164.16.202 [SmartMessage Receiver]"])) | where deviceEventClassId = "agent:050" Does not return the value 'agent:050' in the deviceEventClassId field of the search results. Workaround: Include the 'user' field from the custom field list in the query.
LOG-15079	Loading a saved search or filter by using the folder icon (Load a Saved Filter) fails if the query includes the insubnet operator. Workaround: In the text box, type SS<SavedSearchName> or $filter$<FilterName> and then click Saved Search or Filter in the dropdown list to load it.
LOG-12524	If the value for a discovered field contains a colon (:), an ampersand (&), or angle brackets (<>), the query generated by clicking on it will escape the character with an added backslash (\ ). Workaround: Remove the backslash in front of the character. For example, if the query inserted by clicking the field is "IdentityGroup=IdentityGroup\:All", then after removing the backslash, the query becomes "IdentityGroup=IdentityGroup:All".
LOG-12290	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.
LOG-11225	When using the auto complete feature on the search page, if the inserted query has a double quote followed by bracket ("[ ), it will not be executed. Workaround: Remove the backslash followed by a double quote on both sides of the string. You can also do this when double quote is followed by any special character such as "\, "/, "[, "], or ",.

Configuration

Issue	Description
LOG-25114	On Appliance, when creating or deleting a TH/ESM destination, another instance of SmartAgents (Connector) process may suddenly start running, this prevents seeing, adding and deleting TH/ESM Destinations and Certificates. If any Forwarders are setup with a TH or ESM Destination, the events will no longer be forwarded. Workaround: Stop all Logger processes using *monit stop*. After they were all stopped, reboot the machine.
LOG-21171	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.
LOG-18753	When client authentication is enabled, Logger connects to one TH cluster only. If client authentication is disabled, Logger connects to an indefinite number of TH clusters. Workaround: When connecting another cluster with client authentication, clear the keystore before configuring. This can be done with the commands: 1) List the keypairs by alias: <install_dir>/current/local/jre/bin/keytool -list -keystore <install_dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar | grep -i private 2) Delete the keypair with the alias from the previous command: <install_dir>/current/local/jre/bin/keytool -delete -keystore <install_dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar -J-Djava.security.egd=<a href="file:/dev/urandom" class="external-link" rel="nofollow">file:/dev/urandom -alias <alias(es) from previous command>
LOG-15530	Configuring Lightweight Directory Access Protocol (LDAP) during a Software Logger installation might cause the installation to fail. Workaround: Do not configure LDAP on the system where the Software Logger is installed. Configure LDAP as the authentication method from the Logger system Admin > Authentication > External Authentication page.
LOG-14650	You cannot export a filter that has been previously imported. The export fails and Logger displays an error. This issue does not affect other export contents, such as Alerts, Saved Searches, or Dashboards. Workaround: None available at this time.

Issue	Description
LOG-13998	When setting up Logger A and Logger B to peer by hostname using authorization ID/codes, the peer queries initiated from Logger B to Logger A fail. Workaround: None available at this time.
LOG-13834	When archiving data from a Logger Appliance, the "GMT+x" time zone incorrectly appears as "GMT-x", while the "GMT-x" time zone appears as "GMT+x". Workaround: Specify the Logger Appliance time zone by location. For example, set the time zone as "Taipei" or "Los Angeles."
LOG-13226	A user can edit a Forwarder while the feature is enabled. This can cause the Forwarder to stop sending events. Workaround: Before editing the Forwarder, disable it. Then edit it and re-enable it to have the Forwarder send events to its target destination.
LOG-11473	When using the Setup Wizard to enter a Logger Appliance initial configuration, Logger does not check that you have entered all the required information before submitting it. This can cause the setup program to fail. Workaround: Enter valid values for all required Setup Wizard fields.
LOG-11176	When you enable a Receiver, Logger does not validate the Research File System (RFS) mount it references. Workaround: Edit the Receiver to verify that the RFS mount is valid. Alternatively, verify the mount on the System Admin > Remote File Systems page.
LOG-370	The Configuration Backup (Configuration > Configuration Backup > Backup_name) and File Transfer Receivers (Configuration > Receivers) may fail without notification. If an error occurs, the command appears to succeed but it does not. Workaround: Check the log (Configuration > Retrieve Logs). When a configuration backup is scheduled, the error status is shown in the finished tasks status field.

Installation

Issue	Description
LOG-25010	An error might occur when upgrading OS in Logger L7700. This is a random error Workaround: Contact Support.
LOG-11659	Installation of multiple Solution Packages in Software Loggers with a root user may fail if the SOX v4.0 solution package is installed before others. Workaround: If you are installing the SOX v4.0 solution package on Software Logger with a root user, leave this step for the end.

System Admin

Issue	Description
LOG-24124	NIC bonding information does not appear in the UI after configuring NIC bonding. Workaround: None available at this time.

Reports

Issue	Description
LOG-25274	Schedule MaxMind reports are failing email delivery. Workaround: Log into logger and extract the report manually.
LOG-25061	When installing Software Logger in ReHat and CentOS version 8.X, the data science cannot be enabled. Workaround: Install the Python 2.7.1 using the command "yum install python2". Then, enable the data science and restart logger.
LOG-24679	In a report, arc_peerName always displays 127.0.0.1 when queried. Workaround: Use a logger search base report instead.
LOG-24658	When a category report is renamed, this change is not reflected under User Management groups. Workaround: None available at this time.
LOG-23958	After a Logger upgrade, the Investigate Connection parameters are automatically removed. Reports and query design associated with this connection are no longer available. Workaround: Add the parameters again after the upgrade.
LOG-23124	The commented lines using the number sign (#Comment line) in MySQL queries cause the report execution to fail. Workaround: Use the block comment style (/* Comment line */) or line comment with double dash comment style (-- line comment) instead.
LOG-23111	Duplicate column names are not displayed in a Logger search based report. Workaround: None available at this time.
LOG-22922	Logger displays a completion status when emailing a report despite no SMTP has been configured. Workaround: Configure SMTP settings before emailing a report.

Issue	Description
LOG-21378	When creating a Logger Search Report based on a Logger filter with a peer operator, the system does not recognize the peer operator and checks the "local-only" option in the parameters form. Workaround: Execute the Logger Search Report again with the "local-only" option unchecked.
LOG-16405	From the user interface, rights to view, run, or schedule specific reports outside the user's default privileges can be assigned. However, those rights do not apply in SOAP API. The report can only be run when the user has rights to "View, run, and schedule all reports". Workaround: None at this time.
LOG-16281	Peer reports fail when Logger is peered with ESM 6.8c. This happens because the database type of the event field "arc_sourceAddress" is different for Logger and ESM. Workaround: None available at this time.
LOG-15462	When the file system /opt/arcsight/userdata is full, Logger allows users to run reports, even though they necessarily fail. Logger does not warn users in advance that the free space on the file system is full. This is important for scheduled reports. Workaround: Check the amount of free space periodically.

Security Fixes

The following security fixes were implemented in this release.

Description	CVE
* Code Injection	CVE-2020-11851
** Reflected XSS	CVE-2020-11860
***Stored XSS	CVE-2020-25834

* Special thanks to Security Researcher Chinghz Saferli, for responsibly disclosing this vulnerability.

** Special thanks to ING Tech Poland, for responsibly disclosing this vulnerability.

*** Special thanks to Hidde Smit from Cyber Eagle and Wietse Boonstra from WBSec for responsibly disclosing this vulnerability.

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 7.1.1)

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!