Micro Focus Security ArcSight Logger

Software Version: 7.0.1

Release Notes

Document Release Date: February, 2020
Software Release Date: February, 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

Contents

Logger 7.0.1 Release Notes

Standalone ArcSight Logger version 7.0.1 (L8316) releases are available in three 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 7.0.1 release (L8316) introduces the following features enhancements and bug fixes.

- Indexing has been improved to process up to 30% more events per second.
- Search Improvements:
  - The local only box can now be disabled in both, Classic and Search page by updating the `search.localOnlyChecked` property accordingly.
  - Superindexing is now available for search based on event time allowing to execute searches much faster.
- Logger now supports up to 1 000 HTTPS simultaneous connections.
- Various security fixes, feature updates, and bug fixes have been made.

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

- "Fixed Issues" on page 22
- "Open Issues" on page 24

For details about these features, see the ArcSight Logger 7.0.1 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) 6.10, 6.9, 6.8, 7.7, 7.6, 7.5. For more information, see Editing the logind Configuration File for RHEL 7.X. • CentOS 6.9, 6.10, 7.4, 7.5, 7.6, 7.7. For appliance upgrade: Red Hat Enterprise Linux 6.10, 7.7.
VM Instances	• You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger installer on a 64-bit CentOS 7.7 configured with 12 GB RAM and four physical (and eight logical) cores. • Micro Focus ArcSight strongly recommends allocating a minimum of 4 GB RAM per VM instance. • The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.
Other Applications	• For optimal performance, make sure no other applications are running on the system on which you install Logger.

Supported Platforms

Refer to the Logger Support Matrix, available on Micro Focus Community site for details on Logger 7.0.1 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 7.0.1 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 7.0.1 documentation set also applies to this release.

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

- Logger 7.0.1 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 **Options > Help** tab on any Logger user interface page to access context-sensitive Help for that page. Also available in PDF format as the Logger Administrator's Guide and Logger Web Services API Guide.
- *Logger Support Matrix:* Provides integrated support information such as upgrade, platform, and browser support for Logger. Available for download from the Micro Focus Community
- *Logger 7.0.1 Administrator's Guide:* Provides information on how to administer and use Logger. Available for download from the Micro Focus Community. Also accessible from the integrated online Help.
- *Logger 7.0.1 Web Services API Guide:* Provides information on how to use Logger's web services. Available for download from the Micro Focus Community. Also accessible from the integrated online Help.
- *Logger Getting Started Guide:* Applicable for Logger Appliances only. Provides information about connecting the Logger Appliance to your network for the first time and accessing it through a web browser. Available for download from the Micro Focus Community. Additionally, a printed copy is packaged with the Logger Appliance.
- *Logger 7.0.1 Installation Guide:* Provides information on how to initialize the Logger Appliance and how to install Software Logger on Linux or VMware VM. Available for download from the Micro Focus Community.

Localization Information

Localization support for these languages is available for this release:

- Japanese
- Traditional Chinese
- Simplified Chinese

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

Known Limitations in Localized Versions

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

- Only ASCII characters are acceptable for full-text search and the Regex Helper tool. Therefore, full-text search is not supported for Japanese, Simplified Chinese, or Traditional Chinese characters.
- The Login field on the Add User page does not accept native characters. Therefore, a Logger user cannot have a login name that contains native characters.
- The Report Parameter and the Template Style fields do not accept native characters.
- The 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 7.0.1 (L8316)

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 7.0.1. For more information about upgrading from a version of another appliance model or an earlier software version, consult the Release Notes, Data Migration Guide, and Support Matrix for that version, or contact Micro Focus Support.

Note: To determine your current Logger version, hover the mouse pointer over the ArcSight Logger logo in the upper-left corner of the screen.

Logger 7.0.1 Upgrade Paths	
Software Versions	7.0
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. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 7.0.1 available for download from the Micro Focus Community.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a configuration backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- You must be on Logger 7.0 prior to upgrading to Logger 7.0.1.
- 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 7.0.1 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 Lx600 series appliance, download the following file:
  `osupgrade-logger-rhel77-<timestamp>.enc`

- Download the upgrade files from the Micro FocusEntitlement Site to a computer from which you connect to the Logger UI.
- For local or remote appliance upgrades, download the following file: **`logger-8316.enc`**.
- Verify the upgrade files, as described in "Verifying Your Upgrade Files" on the previous page.
- Logger documentation is not included in your download package. Download your documentation from the Micro Focus Community.

Upgrade Instructions

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

- To upgrade Logger from ArcMC, see "To upgrade Logger Appliances remotely through ArcMC:" below
- To upgrade Logger locally, see "To upgrade a Logger Appliance locally:" below

To upgrade Logger Appliances remotely through ArcMC:

1. Upgrade your OS as appropriate.
   - If you are upgrading an Lx500 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel610-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.
   - If you are upgrading an Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel77-<timestamp>.enc` and following the instructions in the ArcSight Management Center Administrator's Guide.

   Note: Be sure to upgrade to the latest OS distribution as this one fixes additional security vulnerabilities.
2. Deploy the Logger upgrade using the `logger-8316.enc` file and following the instructions in the ArcSight Management Center Administrator's Guide.
3. Reboot the ArcMC for the upgrade to take effect.
4. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide 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 Lx600 series appliance, deploy the OS upgrade by using the file `osupgrade-logger-rhel77-<timestamp>.enc`.

   Note: Be sure to upgrade to the latest OS distribution as it fixes additional security vulnerabilities.
3. Browse to the `logger-8316.enc` file you downloaded previously and click **Upload Update**.

The **ArcSight License & System Update** page displays the update progress. Once the upgrade is complete, Logger reboots automatically.

4. Make a configuration backup immediately after the upgrade is complete. For instructions, refer to the Logger Administrator's Guide of the Logger version you are currently running.

Upgrading Software Logger and Logger on a VMWare VM

This section describes how to upgrade Logger. The instructions are different for fresh installations. For installation instructions, refer to the Installation Guide for Logger 7.0.1, available for download from the Micro Focus Community.

Prerequisites

Be sure that you meet these prerequisites before upgrading Logger:

- Make a configuration backup before upgrading to this release. For instructions, refer to the Logger Administrator's Guide for the Logger version you are currently running.
- You must be on Logger 7.0 prior to upgrading to Logger 7.0.1.
- 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 7.7.

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

- If not already done on the system, perform the following procedures:
  - Increase the user process limit on the Logger's OS. (You do not need to do this for Logger on VMWare VM) 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 17.
- A non-root user account must exist on the system in which you are installing Logger. The installer will ask you to provide one, even if you install as root. The user id and its primary group id should be the same for this account. The UID for the non-root user should be 1500 and the GID should be 750. For example, to create the non-root user, run these commands as **root**:

  ```
  groupadd -g 750 arcsight
  useradd -m -g arcsight -u 1500 arcsight
  ```

  These commands create a non-root user named **arcsight** that will work with a Logger software installation.
- Download the Software Logger upgrade files from the Micro Focus Customer Support Site.
  - For remote upgrades using ArcMC, download the following file:
    logger-sw-8316-remote.enc
  - For local upgrades, download the following file:
    ArcSight-logger-7.0.1.8316.0.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 11

Increasing the User Process Limit

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

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

To increase the default user process limit:

1. Open the file `/etc/security/limits.d/<NN>-nproc.conf`.
   (<NN> is 90 for RHEL or CentOS 6.10 and 20 for RHEL and CentOS 7.7.)
   - 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
   ```

Upgrade Instructions

Follow the instructions listed below to upgrade Logger. Ensure that "Prerequisites" on page 15 are met before you begin.

- To upgrade Logger from ArcMC, see "To upgrade Software or VMWare Loggers remotely through ArcMC:" 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. Upgrade your OS to the latest distribution as it fixes additional security vulnerabilities.

   Note: Remote OS upgrade is not supported for Software Logger. Perform the OS upgrade manually before upgrading Logger.
2. Deploy the downloaded upgrade file `logger-sw-8316-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-7.0.1.8316.0.bin
./ArcSight-logger- 7.0.1 8316.0.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: The `/opt/arcsight/installers` directory.

```
chmod u+x ArcSight-logger-7.0.1.8316.0.bin
./ArcSight-logger-7.0.1.8316.0.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
7.0.1.

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/

Outdated MaxMind DB

MaxMind DB version in Logger 7.0.1 will override the version you had prior the update. If you had the latest MaxMind DB, manually download the geolocation file from the Micro Focus Entitlement. For instructions on how to manually import the geolocation file, see the Import Geolocation Files section in the Logger Administator's Guide.

Fixed Issues

The following issues are fixed in this release.

Installation

Issue	Description
LOG-20265	The Monit log indicated that APS and PostgreSQL processes were restarted after running Monit stop all. Fix: Monit stop all comand now works for all processes.

Configuration

Issue	Description
LOG-20963	After increasing the storage volume size, the incoming events were not saved in the Default Storage Group. NullPointerException was displayed in logger_server.log. Fix: Events can be saved in the default storage group successfully.

System Admin

Issue	Description
LOG-23489	10G interfaces did not appear under System Admin > Network page. Fix: 10G interfaces are now listed in the System Admim>Network page.
LOG-23481	When initializing the L7700, the 10G NIC configuration could only be done manually outside ArcSight CLI. Fix: ArcSight tool works properly now.

Issue	Description
LOG-20364	When disabling the SNMP destination, Logger displayed the following message: "Error communicating to web server. Please reload browser and retry operation". Fix: The issue has been fixed.
LOG-19436	Before upgrading to Logger 7.0, Logger did not count the incoming events from some connectors appropriately. Fix: Logger is now able to count all statistics sent by any connector. An increase in the consumption of licensing process is expected.

Reports

Issue	Description
LOG-20360	When a user added the field "name" while SecureData Configuration is enabled, the grid view of the report displayed duplicate padlocks. Fix: Duplicate padlocks are not longer displayed.

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.

Analyze/Search

Issue	Description
LOG-23429	When adding a query with where clause and without "is not null" condition, Logger does not return events. Workaround: Add a query with "is not null" condition.
LOG-23419	If the operators chart and span are used together without any query before the pipe (example: chart count by deviceEventCategory span (deviceReceiptTime) = 5m"), with a time range that includes many days (example: $CurrentMonth), Logger has to scan a lot of events for that search which increases the levels of CPU usage causing the search to fail. Workaround: Filter the events before the pipe, specially if some fields that you would use with the chart and span operator could be null on some events, like "deviceEventCategory is not null AND deviceReceiptTime is not null | chart count by deviceEventCategory span (deviceReceiptTime) = 5m". Also, avoid to use of chart and span operators combined when the time range is considerable long time span, like months.
LOG-23167	Aggregate functions such as *avg* and *stdev* are not working in peer mode. Workaround: None available at this time.
LOG-23062	During peer search, the peer node is skipped permanently after it fails to communicate with the initializing Logger resulting in possible open sessions. After 160 open sessions, the peer node is unable to conduct a new peer search. 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: On the machine that is reporting destinationAddress and deviceAddress as 127.0.0.1, do the following: 1. Get network adapter real names with: ls /sys/class/net/ or ifconfig -s | cut -d' ' -f1 . For example, It returns ens32 or eno1 depend of the device 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. For example, add logger.network.interface.name=ens32 or logger.network.interface.name=eno1. 3. Restart logger. Note: The destinationAddress and deviceAddress will be change after adding this property. Take into account that everything written before changing the property will look the same

Issue	Description
LOG-18945	If an insubnet parameter has the wrong syntax, no error is reported when running peer searches. For local searches, the error is reported as expected. Workaround: For peer searches that contain the insubnet operator, first run a local search to check for any syntax errors. If no error is reported, then the peer search can be executed properly.
LOG-17806	After running a search from the Live Event Viewer in Internet Explorer or Firefox, searches that are loaded by clicking a dashboard from the Summary page may fail. Workaround: Use the Live Event Viewer from Chrome. For Firefox or Internet Explorer, copy the failing query from the search box, reopen the search screen, and paste the query into the search box to run the search manually.
LOG-17318	If you check the Rerun Query checkbox when exporting search results, the download may not include all search results. "In the current release, exported searches download a maximum of 10 million search results. However, when exporting search results close to or over 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 try to 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 Source Types with a common dependent parser are exported with the property "overwrite.same.content" turned on, Source Types imported will only keep the most recent one with its parser. The other Source Types will not have their parser included in their definition. Workaround: Turn off "overwrite same content" before importing.
LOG-16347	Pipeline queries that include the 'where' operator, and exclude the 'user' field from a custom field list, display no results for the custom fields. For example, this query is missing the 'user' field from the custom field list and therefore has no results: _deviceGroup IN ["192.164.16.202 [SmartMessage Receiver]"])) | where deviceEventClassId = "agent:050" Does not return the value 'agent:050' in the deviceEventClassId field of the search results. Workaround: Include the 'user' field from the custom field list in the query.
LOG-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".

Issue	Description
LOG-12290	When searching Logger with a query that includes the rename operator, if the original field name is included in the fieldset used in the search, the original field renamed by the operator is still displayed as a column in the search results, but will not have any values. For example, if the search uses the All Fields fieldset, which has device EventClassId, and its query includes "rename deviceEventClassId as eventCID", then both device EventClassId and eventCID will be shown in the search results, but device EventClassId will be empty and only eventCID will show the values of deviceEventClassId. Workaround: Since this issue is caused by the fields included in the fieldset used for the search, remove any renamed fields from the fieldset.
LOG-11225	When using the auto complete feature on the search page, if the inserted query has a double quote followed by bracket ("[ ), it will not be executed. Workaround: Remove the backslash followed by a double quote on both sides of the string. For example, if the query inserted by the auto complete is "\"[/opt/mnt/soft/logger_server.log.6] successfully.\"", then after removing them, the query becomes "[/opt/mnt/soft/logger_server.log.6] successfully." You can also do this when double quote is followed by any special character such as "\, "/, "[, "], or ",.
LOG-5181	Search results are not highlighted when there are multiple values that match the IN operator in a query. Workaround: None available at this time. Highlighting works if there is only one item in the square brackets. As soon as there is more than one, no highlighting occurs.

Configuration

Issue	Description
LOG-23699	If the remote system and Logger are set in different time zones (IST and EST), the user cannot sanitize their archives due to a discrepancy in id dates. Logger is unable to locate the .xml file and displays an error message. Workaround: None available at this time .
LOG-21171	When an UDP receiver is configured using a encoding different than UTF-8 or ASCII, Logger drops the non-cef events sent to that receiver. Workaround: change the encoding of the receiver to UTF-8.

Issue	Description
LOG-18753	When client authentication is enabled, Logger connects to one Event Broker cluster only. If client authentication is disabled, Logger connects to an indefinite number of Event Broker clusters. Workaround: When connecting another cluster with client authentication, clear the keystore before configuring. This can be done with the commands: 1) List the keypairs by alias: <install_dir>/current/local/jre/bin/keytool -list -keystore <install_dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar | grep -i private 2) Delete the keypair with the alias from the previous command: <install_dir>/current/local/jre/bin/keytool -delete -keystore <install_dir>/current/arcsight/logger/user/logger/fips/receiver/bcfks_ks -storetype BCFKS -storepass 'changeit@123' -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath <install_dir>/current/arcsight/logger/lib/modules/org.bouncycastle-bc-fips-1.0.0.jar -J-Djava.security.egd=<a href="file:/dev/urandom" class="external-link" rel="nofollow">file:/dev/urandom -alias <alias(es) from previous command>
LOG-18542	When using the Scheduled Archive drop-down filter on the Configuration > Finished Tasks page, the UI displays an error message. Workaround: See the finished archive tasks, file the archived results on the Configuration > Event Archives page.
LOG-17433	When deleting a Logger TCP or UDP receiver, the XML file (receiver parameters) is not deleted. Workaround: When deleting a receiver, manually delete the xml file too.
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-14778	When running a search for a receiver deleted and re-created in the summary UI page (later redirected to Search Page and query by Device Groups) the search results do not include events after recreation. Workaround: Create a Receiver with different name and drill-down the events on the Summary page using the Device Group containing the new Receiver.
LOG-14650	You cannot export a filter that has been previously imported. The export fails and Logger displays an error. This issue does not affect other export contents, such as Alerts, Saved Searches, or Dashboards. Workaround: None available at this time.
LOG-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.

Issue	Description
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. The most likely cause is a problem with configuration parameters, such as Remote Directory, User, or Password. If an error occurs, the command appears to succeed but it does not. Workaround: The error is logged. Check the log (Configuration > Retrieve Logs) if you suspect a problem with the backup. When a Configuration Backup is scheduled, the error status is shown in the Finished Tasks status field.

Installation

Issue	Description
LOG-23709	When attempting to run an OS upgrade from RHEL 7.5 to 7.6, the installation got stuck. Workaround: None available at this time.
LOG-23479	ENC files larger than 1100MB cannot be uploaded to ArcMC. Workaround: Update will be implemented in ArcMC 2.9.4 1. Modify the logger.defaults.properties file to increase the connectorappliance.upgrade.upload.max located at: software: <ARCMC HOME>/current/arcsight/arcmc/config/logger/logger.defaults.properties appliance: /opt/arcsight/arcmc/config/logger/logger.defaults.properties. 2. Reboot ArcMC 3. Try to upload the ENC file

System Admin

Issue	Description
LOG-23889	After an appliance is deployed, the IP address cannot be reached in the network since it is not correctly assigned to the connected interface of the machine. Workaround: Manually assign the IP address to the interface.
LOG-23471	When executing the python3 manage_ bonding.py script, the option 2 does not restore the appliance back to the old configuration. Workaround: Update will be implemented in Platform 1.2 version. Run the following set of commands in the appliance: 1) rm -f /etc/sysconfig/network-scripts/ifcfg-bond0 /etc/modprobe.d/bonding.conf 2) mv /opt/updates/backup_int/ifcfg-* /etc/sysconfig/network-scripts/ 3) rm -rf /opt/updates/backup_int/ 4) rm -rf /etc/sysconfig/network-scripts/ifcfg-bond0 5) echo "-bond0" > /sys/class/net/bonding_masters 6) ifup <previous default interface>

Reports

Issue	Description
LOG-23962	Unable to upload a MaxMind DB within the same month. Logger cannot store 2 backups with the same name reference of the previous month. Workaround: 1. Go to <logger Installation>/arcsight/logger/config/logger/server/. 2. Delete or name the backup MaxMind DB differently. 3. Upload again.
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.

Issue	Description
LOG-23922	MaxMind database in Logger 7.0.1 is outdated and dates back from October 2019. Workaround: Manually import the geolocation file following the instructions: 1. Download the file from the Micro Focus Entitlement page 2. From the Configuration menu, go to import content. 3. Click choose file and look for the Arcsight_Context_Update_CurrentMonth_year.xxxxxx.zip package. 4. Click import. Verify the file has been correctly imported in <loggerInstallation>/config/logger/server/.
LOG-23913	After performing a Data Base Defragmentation, only the first scheduled report is executed properly. The subsequent scheduled reports fail. The report failures are not displayed in the report status but they are seen in the finished tasks from UI as failed. Workaround: After performing a DB defragmentation, execute an Ad-Hoc report. You can then run schedule reports.
LOG-23839	The skip.report.not.data=true flag suppress all reports (even if these contain or not data) in Fast CSV format. Workaround: Set the flag to false or do not schedule Fast CSV format reports
LOG-23430	After running a simple report that and then running it in the background, the report got stuck at "Running - Fetching Data" even when the MySQL log showed that the query was finished. Workaround: None available at this time.
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.
LOG-21067	Split charts cannot be exported. Workaround: None available at this time.
LOG-19469	When using a filter or a saved search to create reports from Logger Search Queries, the report is executed correctly. However, when the user updates the filter or the saved search with a different query, the report does not run properly. Workaround: Re-create reports using the same query object.
LOG-16405	From the Logger user interface, users can be assigned rights to view, run or schedule specific reports that may not be part of their default privileges. When the same report is run through the SOAP API, those rights do not apply; the report can only be run when the individual has the right to "View, run, and schedule all reports." Workaround: None at this time.

Issue	Description
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.
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.

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 7.0.1)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!