# Micro Focus Security
# ArcSight Logger

Software Version: 7.3

## Installation and Configuration Guide

MICRO FOCUS®

# Legal Notices

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

https://www.microfocus.com

# Copyright Notice

# Trademark Notices

# Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

# Support

## Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the Technical Support Page: https://www.microfocus.com/en-us/contact-support/stackb |
| **Support Web Site** | https://www.microfocus.com/en-us/support |
| **ArcSight Product Documentation** | https://www.microfocus.com/documentation/arcsight/#gsc.tab=0 |

# Contents

# About this Guide

This guide describes how to install and initialize version 7.3 of standalone ArcSight Logger and managed by ARCMC Logger. It includes information on how to initialize the Logger Appliance and how to install the Software Logger on Linux and VMware VM.

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

```
cat /etc/arcsight_model
```

```
cat /etc/OpenText_model
```

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

**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.

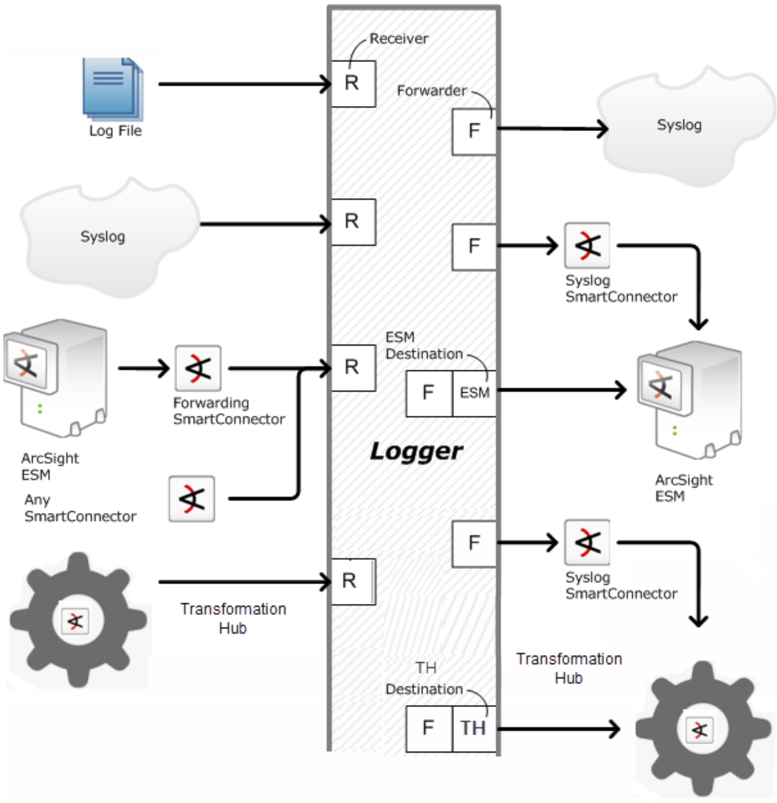
# Chapter 1: Overview

ArcSight Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. An event is a time-stamped log entry, such as a syslog message sent by a host, or a line appended to a log file. Logger receives and stores events; supports search, retrieval, and reporting; and can forward selected events for correlation and analysis to destinations such as a syslog server.

## How Logger Works

Logger stores time-stamped log entries and called events at high sustained-input rates. Logger compresses raw data, but can always retrieve unmodified data on demand, for forensics-quality litigation data. Logger can receive data in the form of normalized CEF events from ArcSight SmartConnectors, syslog messages, and log files directly from a device. Logger can then forward received events to a syslog server or ArcSight ESM.

SmartConnectors are the interface between Logger and devices on your network that generate events you want to store on Logger. SmartConnectors collect event data and normalize it into a Common Event Format (CEF).



Once events have been stored on a Logger, you can do the following:

- Search for events that match a specific query.
- Generate reports of events of interest.
- Generate alerts when a specified number of matches occur within a given time threshold. Alerts can notify you by e-mail, an SNMP trap, or a Syslog message.
- Establish dashboards that display events that match a specific query.
- Forward selected events to ArcSight ESM for correlation and analysis.
- Forward events to Transformation Hub or other tools.

# Logger for Security, Compliance, and IT Operations

Although Logger's applicability spans a wide array of industries, its search, reporting, and alerting capabilities are directly applicable to security and compliance reporting, and for IT operations search.

Logger ships with predefined content filters that define queries for commonly searched security, IT operations, and application development events. These include unsuccessful login attempts, the number of events by source, and SSH authentications on UNIX servers. Therefore, you do not need to define queries to search for many commonly searched events. You can also copy the predefined content filters and modify them to suit your needs, thus saving the time and effort required to start writing queries from scratch. In addition, Logger also contains predefined reports for common security and device monitoring use cases.

For a complete list of predefined content filters and predefined reports, refer to the ArcSight Logger 7.3  Administrator's Guide. Information about how to use predefined filters is included in "System Filters (Predefined Filters)" on page 79.

# Chapter 2: Deployment Planning

Before installing Logger, you should plan how you will store events and how long you need to retain them. Consider the information in the sections below when planning your deployment.

## Getting the Latest Documentation

The latest version of the documentation for this release is available for download (in PDF format) from the Micro Focus Documentation.

You can also access the online help available in the Logger user interface (UI) by clicking **Help** in the right top corner of the page.

## Trial Licenses

All ArcSight Loggers come with a trial license (for EPS and GB per day) that you can use for a 90 day evaluation period. You can manage licenses both by ArcMC or as Standalone ArcSight Logger. After the evaluation period is over, you will not be able to access any Logger features until you insert a valid license.

**Note:** Once the license is updated to EPS, the GB license (Logger Standalone or managed by ArcMC) cannot be longer selected.

The trial license gives you access to the following:

- All Logger features except Reporting.
- 20 EPS per day ingested license usage.
- Up to 24TB in bigger capacity Logger Appliances L7700, or 48TB in Logger Appliances L8000.

After you upload a license, the reporting feature is enabled; the licensed daily usage and storage volume are increased to the capacity of the license. The ingested daily license usage of your Logger is displayed under **Configuration > Advanced > License Usage**. You can view your daily data limit and other license information under **System Admin > License & Update**.

To upload a new license, refer to the **System Admin** chapter of the ArcSight Logger 7.3 Administrator’s Guide.

## Acquiring a License for a Logger

A valid license file must be applied to Logger before you can access Logger's report functionality. For information and restrictions, see "Trial Licenses" above. To acquire the software license, follow the instructions in the Electronic Delivery Receipt you received from Micro Focus in an email after you placed the order. Contact Customer Support in case you no longer have the document.

### Logger managed by ArcMC:

Several Loggers cannot use the same license unless they are managed by ArcMC. The same license needs to be added in each Logger and also in ArcMC (which will act as the License Server). For more information on how to add a license in ArcMC, refer to the ArcSight Management Center Administrator's Guide .

### Standalone Logger:

Make sure to add a separate, not re-used, license file for each Logger (License compliance will be determined by each Logger). For more information on how to add a license in Logger, see **System Admin** chapter in ArcSight Logger 7.3  Administrator's Guide.

To view more details about the current license (after Logger's installation), please go to **System Admin >License & Update** page and **Configuration > Advanced > License Information**. For more information, refer to the **Configuration** and **System Admin** chapters of the ArcSight Logger 7.3  Administrator's Guide.

# Initial Configuration

The installation and initialization process sets up your Logger with an initial configuration described in the sections below. You can do additional configuration on Logger to implement your retention policies. See "Configuring Logger" on page 60. For further information, refer to the **Configuration** chapter of the ArcSight Logger 7.3  Administrator's Guide.

Logger's initial configuration is described in the sections below:

## Storage Volume

Logger storage volume varies not only by version but also by initialization process. For Software Logger, the storage volume is set up to 24TB or the available disk space, whichever is smaller. For appliances, the storage volume is set to the model´s capacity (24TB being the maximum for L7700 models, and 48TB the maximum for L8000 models). You can expand the storage volume in **Configuration > Maintenance Operations > Storage Volume Size Increase**. Storage volume can be extended after installation, but not reduced.

### Storage Volume Space Increasing:

When setting the disk space, the reservation percentage needs to be included. For instance, if you want to use a storage volume size of 24 TB in Logger, you must allocate 24TB and a minimum 10% of reservation (26.4 TB in total) of disk space in the bigger capacity storage L7700 appliances. To allocate storage volume properly, obtain the initial storage volume space (initial storage volume multiplied for 0.93). View the assigned space based on the license and, set the storage group disk space. For more information, see ArcSight Logger 7.3 Administrator’s Guide.

## Storage Groups

Two storage groups, the Default Storage Group and the Internal Event Storage Group, are created automatically during Logger initialization.

These storage groups come preconfigured with the following settings:

**Preconfigured Default Storage Group Settings**

| Attribute | Appliance Logger | Software Logger |
|---|---|---|
| Size | 1/2 Storage volume capacity | 1/2 Storage volume capacity |
| Retention Period | 180 days | 180 days |

**Pre-configured Internal Storage Group Settings**

| Attribute | Appliance Logger L7700 | Software Logger or Logger Appliance L8000 |
|---|---|---|
| Size | 5 GB | 3 GB |
| Retention Period | 365 days | 365 days |

Logger can have a maximum of 50 storage groups— 2 that pre-exist on your Logger (Internal Storage Group and Default Storage Group) and 48 that you can create.

Adding more storage groups in Logger is determined by the partition size and the storage volume available (up to 48 custom storage groups).

Each storage group can have different settings. You can change the retention policy and size for all storage groups, but you can only change the name of the user-defined storage groups. For more information, see the **Configuration** chapter of the ArcSight Logger 7.3 Administrator’s Guide.

## Search Indexes

Logger comes prepared for full-text searches, also frequently used fields are indexed during initialization. You can add additional fields to the index, but once a field has been added, you cannot undo the action. For more information, see the **Search** chapter of the ArcSight Logger 7.3  Administrator’s Guide.

## Receivers

The default installation includes several receivers. To start receiving events, direct your events to the default receivers. After initialization, you can create additional receivers to listen for events. Before a receiver can receive data, open the port through the firewall. For more information, see "Firewall Rules" on the next page.

You can also change and delete receivers or disable and enable them as needed.

> ✓ **Tip:** Be sure to update the firewall configuration whenever you add or remove a receiver.

The following receivers are set up and enabled with the default installation:

- A UDP receiver: Enabled by default.

  The UDP receiver is on port 514/udp for L7700 and L8000 Logger Appliances. If you are installing Software Logger as root, the UDP receiver is on port 514/udp. For non-root installs, it is on port 8514/udp. If this port is already occupied, the initialization process selects the next higher unoccupied port.

- A TCP receiver: Enabled by default.

  The TCP receiver is on port 515/tcp for L7700 and L8000 Logger Appliances. If you are installing Software Logger as root, the TCP receiver is on port 515/tcp. For non-root installs, it is on port 8515/tcp. If this port is already occupied, the initialization process selects the next higher unoccupied port.

- A SmartMessage receiver: Enabled by default.

  To receive events from a SmartConnector, download the SmartConnector and set the **Receiver Name** to be “SmartMessage Receiver” when configuring the destination. The SmartMessage receiver listens on the same port as the User Interface, 443/tcp on Logger appliances, and typically 443/tcp on Software Logger installed as root, and 9000/tcp on Software Logger installed as non-root. The Software Logger ports may vary.

Logger also comes pre-configured with folder follower receivers for Logger’s Apache URL Access Error log, the system Messages log, and the system Audit log (when auditing is enabled on your Linux OS). You must enable these receivers in order to use them.

**Note:** Logger's Apache URL Access Error Log, http_error_log, is similar in format to the Apache access_log. Only failed access attempts are included in the Apache URL Access Error Log.

For Software Logger, the preconfigured folder follower receivers include:

- Var Log Messages: `/var/log/messages`
- Audit Log: `/var/log/audit/audit.log`
- Apache URL Access Error Log:

  `<install_dir>/userdata/logs/apache/http_error_log`

  **Note:** The folder (follower receiver) for `/var/log/audit/audit.log` will only be created if `/var/log/audit/` already exists on your system.

Auditing is disabled on some Logger Appliance models. Logger Appliances that have auditing enabled will have the same pre-configured receivers as Software Logger.

When auditing is disabled on the system where Logger is installed, the pre-configured folder follower receivers include:

- Var Log Messages: `/var/log/messages`
- Apache URL Access Error Log:

`/opt/arcsight/userdata/logs/apache/http_error_log`

For instructions on how to enable the pre-configured receivers, see "Receivers" on page 60. For more information about all Logger receivers, refer to the ArcSight Logger 7.3 Administrator's Guide.

# Firewall Rules

Before Logger can receive data, some ports must be opened through the firewall.

- For Software Logger, you are responsible for setting up the firewall. After you first install or upgrade to Logger 7.3, you should configure the firewall to be open only for the ports required for your configuration.

  **Caution:** Micro Focus ArcSight strongly recommends that you configure your firewall and open only the required ports.

- For the Logger Appliance L7700, the firewall is pre-configured. Micro Focus ArcSight provides a script you can use to update the firewall.
- For the Logger Appliance L8000, the firewall is pre-configured.

✓ **Tip:** Be sure to update the firewall configuration whenever you add or remove any service that requires an open port for incoming traffic, such as a receivers or SNMP polling.

For more information, see ArcSight Logger 7.3  Administrator’s Guide.

# Chapter 3: Setting Up a Logger Appliance L7700

This section describes how to rack mount your Logger Appliance, and to configure an IP address and initial settings for it. You do not need to run an installer when setting up your appliance; the Logger software comes pre-installed on it. These basic steps enable you to start using your Logger Appliance.

For information on how to install Software Logger on Linux, see "Installing Software Logger on Linux" on page 31. For information about installing Software Logger on VMware VM, see, "Installing Software Logger on VMware" on page 50.

## Running Logger on Encrypted Appliances

✓ This topic applies to the L7700 Logger Appliance models only.

Logger can be run on encrypted hardware to help you to meet compliance regulations and privacy challenges by securing your sensitive data at rest.

You can encrypt L7700 Logger Appliance by using Micro Focus Secure Encryption, available from the Server Management Software > Micro Focus Secure Encryption web page.

L7700 Logger appliances come pre-installed with everything necessary to use Micro Focus Secure Encryption. The length of time encryption takes depends on the amount of data on the server being encrypted. You can continue using Logger while the encryption runs. You may notice some performance degradation after encrypting your existing Logger appliance.

⚠ **Caution:** After encryption, you cannot restore your Logger to its previously unencrypted state.

## Installing the Logger Appliance L7700

### Before you Begin:

- Redeem your license key by following the instructions in the documents you received when purchasing. Redeeming this key gets you the license that you need to access Logger functionality. For more information, see "Acquiring a License for a Logger" on page 10.

### To install the appliance:

1. Unpack the appliance and its accompanying accessories.

   > **Note:** Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.
3. Make the rear panel connections.
4. Power on the appliance.

## Configuring an IP Address for the L7700 Appliance

> ✓ This topic applies to the L7700 Logger Appliance models only.

The appliance ships with the default IP address 192.168.35.35 (subnet mask 255.255.255.0) on eno1 (ens1f0 for L7700 appliances). To begin setting up your appliance, follow the steps below to configure a new IP address on the Logger Appliance command line interface (CLI).

To run a command in the Logger CLI, type it at the prompt and press Enter. For more information on the command line interface, see "Using the Logger Appliance Command Line Interface" on page 22 or enter `help` at the prompt for a list of available commands.

> **Note:** You can configure your appliance with and IPv4 address, an IPv6 address or both.

### To set up a new IP address:

1. Use one of the following methods to connect to the Logger (not the operating system) CLI:
   - For appliance version L7700: Log into Micro Focus ProLiant Integrated Lights-Out (iLO) and launch the remote console feature. For more information, see "Setting Up the L7700 Appliance for Remote Access" on page 19.
   - Connect a keyboard and monitor to the ports on the rear panel of the appliance.
   - Connect a terminal to the serial port on the appliance using a null modem cable with DB-9 connector. The serial port expects a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control (9600/8/N/1/N).

     Once you are connected to the CLI, a log in prompt is displayed.
2. Enter the following default credentials to log in as the administrator:

```
Login: admin

Password: password
```

> The log-in process must be started when you have the time to finish the setup. If you log in and then leave the appliance unattended for some time, you might encounter the **Could not process authentication request at this time. Use local authentication <yes/no>?** error. If this happens, please reboot the appliance and log-in again.

3. To begin the setup, follow the steps below to configure a new IP address on the Logger Appliance command line interface (CLI).

   Configure an IPv4 address either by providing static IPv4 address or choosing auto (SLAAC) configuration.

   > The Logger Appliance ships with the default IP addresses `192.168.35.[35-38]` (subnet mask `255.255.255.0`).

   In the following commands, the `<your value>` variable used to configure the Ethernet adapters depends on your needs: for 10 GB Ethernet adapters use `ens1f[0-1]` or `ens2f[0-1]`, and for 1 GB Ethernet adapters use `eno[1-4]`.

   - For Static IPv4 configuration, use the following command format:

     ```
     set ip <your value><ip>/<prefix>
     ```

     Example for 10 GB Ethernet adapters:

     ```
     set ip ens2f0 192.0.2.5/24
     ```

     Example for 1 GB Ethernet adapters:

     ```
     set ip eno1 192.0.2.5/24
     ```

   - For Auto IPv4 configuration use the following command format:

     ```
     set ip <your value><ip> <subnet mask>
     ```

     Example for 10 GB Ethernet adapters:

     ```
     set ip ens2f0 192.0.2.5 255.255.255.0
     ```

     Example for 1 GB Ethernet adapters:

     ```
     set ip eno1 192.0.2.5 255.255.255.0
     ```

4. Execute the following command, `replacing <ip> with your default gateway IP address:`

   ```
   set defaultgw <ip>
   ```

5. Execute the following command, replacing `<domain>.<company.com>` with the fully-qualified domain name (FQDN) of the desired host:

   ```
   set hostname <domain>.<company.com>
   ```

6. Execute the following command, replacing each `<search_domainN>` with a search domain, and each `<nameserverN>` with the IP address of a name server:

   ```
   set dns <search_domain1>,<search_domain2> <nameserver1> <nameserver2>
   ```

   Example:

   ```
   set dns domain1.company.com,domain2.company.com 192.0.2.1 192.0.2.2
   ```

   ✓ **Tip:** When using multiple search domains, separate them with a comma, but no space. When using multiple name servers, separate them with a space but no comma.

7. Execute the following command, replacing `<ntp_serverN>` with the NTP server you want to use to set the time:

   ```
   set ntp <ntp_server1> <ntp_server2> <ntp_server3>
   ```

   Example:

   ```
   set ntp time.nist.gov
   ```

8. Execute the following command to review the configuration settings you entered in previous steps. If needed, change the settings:

   ```
   show config
   ```

## Setting Up the L7700 Appliance for Remote Access

✓ This topic applies to the L7700 Logger Appliance models only.

All ArcSight L7700 appliances are equipped with an Micro Focus ProLiant Integrated Lights-Out (iLO) Advanced remote management card. Micro Focus strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you or Customer Support (with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and power control.

To set up your appliance for remote access, follow the instructions in the ProLiant Integrated Lights-Out User Guide available on the product's website.

# Connecting to the Logger Appliance L7700

> ✓ This topic applies to the L7700 Logger Appliance models only.

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the Release Notes for details on Logger 7.3 browser support.

Logger’s publicly-accessible ports must be allowed through any firewall rules. For Software Logger, you must set up the firewall. Firewall rules are pre-configured on the Logger Appliance. See "Firewall Rules" on page 14 for more information.

- 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.

  > **Note:** The ports listed here are the default ports. Your Logger may use different ports.

- JavaScript and cookies must be enabled.

### To connect and Log in for the first time:

1. Connect to Logger:

   Use the URL configured during Logger installation to connect to Logger through a supported browser.

   For Software Logger or Logger Appliance L8000: `https://<hostname or IP address>:<configured_port>`

   For Logger Appliance L7700: `https://<hostname or IP address>`

   where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

2. Scroll down to the bottom of the screen to review and accept the EULA. After you accept, the Login screen is displayed.

3. Log in:

   When the Login dialog is displayed, enter your user name and password, and click **Login**.

   Use the following default credentials if you are connecting for the first time:

   **Username:** admin
   **Password:** password

> **Note:** After logging in for the first time with the default user name and password, you will be prompted to change the password. Follow the prompts to enter and verify the new password.

For more information, see ArcSight Logger 7.3  Administrator’s Guide.

Once you have successfully logged in, proceed to the section, "Initializing the Logger Appliance L7700" below.

## Initializing the Logger Appliance L7700

> ✓ This topic applies to the L7700 Logger Appliance models only.

After you accept the EULA and log in for the first time, the  **Logger Configuration** screen is displayed. On this screen, you can upload the license file and configure the initial settings for your Logger Appliance. Once you complete that configuration, your Logger Appliance will be ready for use.

> **Note:** The initialization of a Logger Appliance can only be changed by restoring Logger to its initial factory settings.

Logger comes with a trial license valid only for 90 days. This license provides limited functionality. For full access, you must upload your EPS or GB per day license as Standalone or Managed by ArcMC. See "Trial Licenses" on page 10 for more information.

If you do not have a license, see "Acquiring a License for a Logger" on page 10.

### To initialize the Logger Appliance:

1. Upload a full license when you first connect or use trial license and upload the license later.
    - If you have a license, apply it now. To apply the license, go to **Logger Configuration >Select License File to Upload** and navigate to specify the path and file name of the license for the Logger Appliance, and click **Upload License**.
    - After the upload, the License pane displays updated license status information.
2. Select a **Locale** for this Logger Appliance from the **System Locale Setting** drop-down list.

   The locale setting ensures that the user interface displays information such as date, time, numbers, and messages in the format and language appropriate for the selected country. Once configured, this setting cannot be changed.

3. Confirm the “Current Time Zone” and the “Current Time” settings are correct for your environment.

   To update the time settings, check **Change Time Zone** and **Change Date/Time** under **Date/Time Settings**.

4. Click **Save**.

   The Logger initialization process begins. Once the initialization is complete, the system reboots. After completing the install and initialization, see "Configuring Logger" on page 60 for additional information to enable the pre-configured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy.

## Using the Logger Appliance Command Line Interface

> ✓ This topic applies to the L7700 Logger Appliance models only.

The Logger appliance CLI enables you to start and stop the appliance as well as issue commands for the Logger application.

Use one of the following methods to connect to the appliance Command Line Interface (CLI):

- For appliance version L7700: Log into Micro Focus ProLiant Integrated Lights-Out (iLO) and launch the remote console feature. For more information, see "Setting Up the L7700 Appliance for Remote Access" on page 19.
- Connect a keyboard and monitor to the ports on the rear panel of the appliance.
- Connect a terminal to the serial port on the appliance using a null modem cable with DB-9 connector.

  The serial port expects a standard VT100-compatible terminal: **9600 bps**, **8-bits**, **no parity**, **1 stop bit** (**8N1**), **no flow control**.
- Once you are connected to the CLI, a Login prompt displays.

The following commands are available at the CLI prompt:

| Category | Command | Description |
|---|---|---|
| **System Commands** | | |
| | exit | Logout |
| | halt | Stop and power down the Logger Appliance |
| | help | Opens the command line interface help |
| | reboot | Reboot the Logger Appliance |

| Category | Command | Description |
|---|---|---|
| **Administrative Commands** | | |
| | show admin | Show the default administrator user's name |
| **Authentication Commands** | | |
| | reset authentication | Revert the authentication mechanism to the default, local authentication. This can be useful if a different authentication mechanism such as CAC, LDAP or Radius had been configured and is somehow no longer working. |
| **Configuration Commands** | | |
| | show config | Show host name, IP address, DNS, and default gateway for the Logger |
| **Date Commands** | | |
| | show date | Show the date and time currently configured on the Logger |
| | set date | Set the date and time on Logger<br>The date/time format is `yyyyMMddhhmmss`<br>Example date: `20101219081533` |
| **Default Gateway Commands** | | |
| | set defaultgw <IP> [nic] | Set the default gateway for one or all network interfaces |
| | show defaultgw [nic] | Display the default gateway for all or the specified network interface |
| **DNS Commands** | | |
| | show dns | Show the currently configured DNS servers on the Logger |
| | set dns <sd> <ns><br>set dns <sd1>,<sd2> <ns1> <ns2> | Set DNS name server(s)<br>sd=search domain, ns = name server<br>You can add up to three name servers and six search domains<br>**Note:** When using multiple search domains, separate them with a comma, but no space. When using multiple name servers, separate them with a space but no comma. |
| **Hostname Commands** | | |
| | show hostname | Show the currently configured hostname on the Logger |
| | set hostname <host> | Set Logger's host name |

| Category | Command | Description |
|---|---|---|
| **IP Commands** | | |
| | show ip [nic] | Show the IP addresses of all or the specified network interface |
| | set ip <nic> <IP> [/prefix] [netmask] | Set Logger’s IP address for a specific network interface |
| **NTP Commands** | | |
| | set ntp <ntp server> <ntp server> <ntp server> ... | Sets the NTP server addresses. This entry over writes the current NTP server setting<br>You can specify as many NTP servers as you like. If you specify multiple NTP servers, they are each checked in turn. The time given by the first server to respond is used.<br>Example:<br>`logger> set ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org` |
| | show ntp | Show the current NTP server setting.<br>Example:<br>`logger> show ntp`<br>`ntp.arcsight.com time.nist.gov 0.rhel.pool.org` |
| **Password Commands** | | |
| | set password | Set the password the current user’s account |
| **Process Commands** | | |
| | restart process | Restart a process |
| | start process | Start a process |
| | status process | Show process status |
| | stop process | Stop a process |
| **SSL Certificate Commands** | | |
| | show sslcert | Show the currently loaded SSL certificate on Logger |
| | reset sslcert | Creates and installs a new self-signed certificate with the original default information, then restarts the HTTPS server. |
| | diag sslcert | Display the SSL session information |

# Chapter 3: Setting Up a Logger Appliance L8000

This section describes how to rack mount your Logger Appliance, and to configure an IP address and initial settings for it. You do not need to run an installer when setting up your appliance; the Logger software comes pre-installed on it. These basic steps enable you to start using your Logger Appliance.

For information on how to install Software Logger on Linux, see "Installing Software Logger on Linux" on page 31. For information about installing Software Logger on VMware VM, see, "Installing Software Logger on VMware" on page 50.

## Encryption of SEDs

The L8000 Logger Appliances support FIPS enabled self-encrypting disks (SEDs). Because the data contained in these SED drives would be accessible to third parties if the drive was stolen, you have the option to add data protection against the loss or theft of the disks. This protection consists of setting up passphrase-access-only.

The SEDs ship without the passphrase, allowing you to chose your own. To set up a passphrase, first follow the steps to establish a security key.

The chosen passphrase can then be applied to pre-existing virtual disks by following the steps in Secure a pre-existing virtual disk.

To change or disable a security key, please follow the specific procedures listed under this section.

## Installing the Logger Appliance L8000

### Before you Begin:

- Redeem your license key by following the instructions in the documents you received when purchasing. Redeeming this key gets you the license that you need to access Logger functionality. For more information, see "Acquiring a License for a Logger" on page 10.

### To install the appliance:

1. Unpack the appliance and its accompanying accessories.

   > **Note:** Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.
3. Make the rear panel connections.
4. Power on the appliance.

## Connecting to the Logger Appliance L8000

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the Release Notes for details on Logger 7.3 browser support.

Logger's publicly-accessible ports must be allowed through any firewall rules. Firewall rules are pre-configured on the Logger Appliance. See "Firewall Rules" on page 14 for more information.

- 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.

  > **Note:** The ports listed here are the default ports. Your Logger may use different ports.

- JavaScript and cookies must be enabled.

### To connect and Log in for the first time:

1. Connect to Logger:

   Use the URL configured during Logger installation to connect to Logger through a supported browser.

   For Software Logger or Logger Appliance L8000: `https://<hostname or IP address>:<configured_port>`

   For Logger Appliance L7700: `https://<hostname or IP address>`

   where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

2. Log into the appliance with your root user and password.

3. The Micro Focus EULA will be presented, and it can be navigated using the spacebar key to display one page after the other. Enter q after the last page to exit the EULA screen, and enter y when asked:

    ```
     Are you sure you  want to quit? (y)
    ```

4. The final EULA prompt is:

    ```
    Do you accept the Micro Focus license presented to you? (y/n)
    ```

    You must enter y to accept the terms.

5. Next, the Red Hat license will be presented, and it can be navigated using the spacebar key to display one page after the other. Enter q after the last page to exit the license screen, and enter y when asked:

    ```
     Are you sure you  want to quit? (y)
    ```

6. The final license prompt is:

    ```
    Do you accept the Red Hat license presented to you? (y/n)
    ```

    You must enter y to accept the terms.

7. Having accepted both licenses, you will receive the following prompt:

    ```
    Congratulations, you accepted the license agreements.  The system will now
    start up.
    ```

# Configuring an IP Address for the Logger Appliance L8000

> The Logger Appliance L8000 is built on an Software Logger platform. The end user and their IT team are ultimately responsible for its network administration.

If a DHCP server is available in your environment, the L8000 appliance is configured to use DHCP by default. Otherwise, you may need to configure a static IP to the L8000 appliance, and these initial steps can be used for guidance:

1. Find the configuration file of the active network port in the /etc/sysconfig/network-scripts/ directory.

    Run the following command to identify the configuration file for the active network port:

    ```
    ip a | grep "state UP" | awk '{print "/etc/sysconfig/network-
    scripts/ifcfg-"$2}' | tr -d ":"
    ```

    Output Example:

    ```
    /etc/sysconfig/network-scripts/ifcfg-eno12399np0
    ```

If you do not get a response for the above command, make sure that a live network cable has been attached to the appliance, and then repeat the command.

> ✓ Create a backup copy of the selected files prior to any modification.

2. Please modify the following lines in the file identified in the previous step (you can use an editor of your choice for the changes):

| Original line | Modified line | |
|---|---|---|
| BOOTPROTO=dhcp | `BOOTPROTO=static` | |
| ONBOOT=no (if yes, leave as is) | `ONBOOT=yes` | |

3. Add the following lines to the end of the file:

```
IPADDR=<ip_address>
```

```
NETMASK=<subnet_mask>
```

```
GATEWAY=<gateway_address>
```

Where:

`<ip_address>` is the static IP you're assigning to the L8000 appliance

`<subnet_mask>` is the subnet mask of the IP

`<gateway_address>` is the gateway address of the IP

The values above must be assigned according to your own specifications, the following is just an example to show the format of the data:

```
IPADDR=192.168.1.10
```

```
NETMASK=255.255.255.0
```

```
GATEWAY=192.168.1.1
```

4. Save the file with the changes.
5. Restart the networking service with the following command:

```
systemctl restart NetworkManager
```

Once these steps are applied, the L8000 appliance should have the static IP configured.

# Setting Up the L8000 Appliance for Remote Access

All ArcSight L8000 appliances are equipped with an `iDRAC Service Module (iSM)` for remote access. Micro Focus strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you or Customer Support (with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and power control.

## Changing the iDRAC password on your L8000 Appliance

L8000 Appliance boxes come with a tag that contains the iDRAC password. This is a unique password, which will be required the first time iDRAC is accessed. The appliance then will prompt for a new password to be chosen. For security reasons, Micro Focus recommends to change this password as soon as possible.

To set up your appliance for remote access, follow the instructions in the EMC iDRAC Service Module.

# Software Logger and Logger Appliance L8000 Command Line Options

**This topic applies to Software Loggers and L8000 Logger Appliances**

The loggerd command enables you to start or stop these types of Loggers. In addition, the command includes a number of subcommands that you can use to control other processes that run as part of the Logger.

> **Note:** If your Logger is installed to run as a system service, you can use your operating system's service command to start, stop, or check the status of a process on Logger. The default service name is arcsight_logger.

- For a Software :

  ```
  <install_dir>/current/arcsight/logger/bin/loggerd
  {start|stop|restart|status|quit}
  ```

  ```
  <install_dir>/current/arcsight/logger/bin/loggerd {start <process_name> |
  stop <process_name> | restart <process_name>}
  ```

- For a  Appliance L8000:

  ```
  /opt/softlogger/current/arcsight/logger/bin/loggerd
  {start|stop|restart|status|quit}
  ```

  ```
  /opt/softlogger/current/arcsight/logger/bin/loggerd {start <process_name>
  | stop <process_name> | restart <process_name>}
  ```

To view the processes that can be started, stopped, or restarted with loggerd, click **System Admin** from the top-level menu bar. Then, under **System**, pick **Process Status.** The processes are listed on the right under **Processes.**

The following table describes the subcommands available with `loggerd` and their purpose.

| Command | Purpose |
|---|---|
| `loggerd start` | Start all processes listed under the System and Process sections. Use this command to launch Logger. |
| `loggerd stop` | Stop processes listed under the Process section only. Use this command when you want to leave loggerd running but all other processes stopped.<br>**Important:**Micro Focus recommends that you do not stop the **servers** process. To shut down Logger, use the `loggerd stop` or `quit` commands.<br>Never stop the Logger**servers** process while events are still coming in, this can cause data loss. If you must stop the **servers** process, be sure to stop the **receivers** process first, then stop the **servers** process. |
| `loggerd restart` | This command restarts processes listed under the Process section only.<br>**Note:** When the `loggerd restart` command is used to restart Logger, the status message for the “aps” process displays this message:<br>`Process ‘aps’ Execution failed.`<br>After a few seconds, the message changes to:<br>`Process ‘aps’ running.` |
| `loggerd status` | Display the status of all processes. |
| `loggerd quit` | Stops all processes listed under the System and Process sections. Use this command to stop Logger. |
| `loggerd start <process_name>` | Start the named process. For example, `loggerd start apache` |
| `loggerd stop <process_name>` | Stop the named process. For example, `loggerd stop apache` |
| `loggerd restart <process_name>` | Restart the named process. For example, `loggerd restart apache` |

You can also start and stop and view the status of Logger processes from the **System Admin > System > Process Status** page.

# Chapter 4: Installing Software Logger on Linux

You can install Software Logger on a Linux system or on a VMware virtual machine (VM). This chapter explains what you need to know to install and start running Software Logger on a Linux system. It includes information on the following topics:

For information about installing Software Logger on a VMware VM, see, "Installing Software Logger on VMware" on page 50. For initialization information about the Logger Appliance, see "Setting Up a Logger Appliance L7700" on page 16.

## Before You Begin

You need to have a server with supported operating system and storage available to install the Software Logger. Refer to the Release Notes for details on the Logger 7.3 release. For information about the platforms on which you can install and use Logger, refer to the Release Notes.

> If the machine you plan to install Logger on is still on the `RHEL 7.9` OS, please review the Red Hat documentation to perform an upgrade to `RHEL 8.x`. This will ensure that your machine has the latest security fixes, and can continue supporting future Logger upgrades.

### Downloading the Installation Package

The installation package is available for download from the Logger 7.3 Software Depot at Micro Focus Entitlement Page.

### Verifying the Downloaded Installation Software

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

## How Licensing Works in Software Logger

Logger comes with a limited functionality trial license that is valid for only 90 days. To access the full functionality, upload your EPS or GB per day license as standalone ArcSight Logger or Managed by ArcMC. See "Trial Licenses" on page 10 for more information.

If you do not have a license file, see "Acquiring a License for a Logger" on page 10. You need a separate license file for each instance of Software Logger. A license file is uniquely generated for each Logger download.

The type of license you have affects how the license usage restriction function works and what is displayed on the **License Usage** page.

- For managed by ArcMC Loggers, ArcSight Management Center manages the license (EPS or GB per day) restrictions. Refer to the ArcSight Management Center Administrator’s Guide for more information.
- For standalone ArcSight Loggers, the license usage restriction function manages the license (EPS or GB per day) restrictions.

The license usage restriction function adds the sum of the sizes of the events received on a given day to compute the amount of data that comes into Logger per day. Logger compares that value against the daily data limit in the license. If this limit is exceeded, Logger continues to collect and store events, so that no events are lost. For GB per day license, if the daily data limit is exceeded on more than five days in a 30-day sliding window, all search-related features are disabled. You will not be able to forward, search, or run reports on the collected events until the 30-day sliding window contains five or less data limit violations. For EPS, there is no over the limit restrictions for the 45 days displayed on the graph.

The license usage page (**Configuration > Advanced > License Usage**) lists the data stored on your Software Logger on day-by-day basis in the last 45 days for EPS (30 days for GB per day). It also indicates the days on which data limits were exceeded. For more information, see the **Configuration** chapter of the ArcSight Logger 7.3  Administrator’s Guide.

If you're interested in Logger pay-per-use licensing options, please visit:

https://www.microfocus.com/documentation/arcsight/mssp/

## Prerequisites for Installation

Make sure these prerequisites are met before you install the Logger software:

- To retrieve logs correctly and prevent rotation, Software Logger requires 2 Linux OS pre-installed packages (zip and unzip). If these are unavailable, use the following commands to install:

  ```
  yum install - unzip
  ```

  ```
  yum install -y fontconfig \ dejavu-sans-fonts
  ```

- If you are installing on RHEL 7.X, edit the `logind.conf` file as described in "Editing the logind Configuration File for RHEL 7.X" on page 36.

- Before installing or upgrading Logger, you must modify four TCP properties of the OS environment as described in "Configuring TCP keepalive parameters for Linux OS" on page 36.
- Before installing or upgrading Logger, you must add the `rng-tools` package and enable the `rngd.service` as described in "Install package rng-tools" on page 37.
- Before installing or upgrading to Logger 7.3 (and when upgrading from RHEL 7.X to RHEL 8.4), you must connect through SSH to the Logger console to validate the presence of the packages in the following table. Use the command in the **Verification command** column for each package.

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

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

| Package | Verification command | Installation command |
|---|---|---|
| libnsl | `rpm -qa \| grep libnsl` | `yum install libnsl` |
| compat-openssl10 | `rpm -qa \| grep compat-openssl10` | `yum install compat-openssl10` |
| ncurses-compat-libs | `rpm -qa \| grep ncurses-compat-libs` | `yum install ncurses-compat-libs` |
| Optional: tzdata. The Logger installer will show the version required, and having an older version will generate a **User Intervention Required** prompt. However, choosing NO to keep the current version will not affect the installation process. Therefore, executing the commands below is optional. | | |
| tzdata | `rpm -qa \| grep tzdata` | `yum install tzdata` |

- Increase the user process limit on your Operating System, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on page 35.
- Before deploying in a production environment, get valid license file. If you do not have a license file, see "Acquiring a License for a Logger" on page 10. You may need a separate license file for each instance of Logger. A license file is uniquely generated for each download.
- A non-root user account must exist on the system on which you are installing Logger, or the installer will ask you to provide one. Even if you install as root, a non-root user account is still required. The userid and its primary groupid 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. Make sure to assign a password for this user.

- Decide whether to install Logger while logged in as root or as a non-root user. Your installation options vary depending on which user you choose.

  **Tip:** If you are installing as a non-root user, the user must have privileges to write to the installation directory and its sub-directories. For example, for the non-root user arcsight, use the command:

  ```
  chown -R arcsight:arcsight /opt/arcsight
  ```

  a. If you install as root, you can choose to configure Logger to start as a service and select the port on which Logger listens for secure web connections.

  b. If you install as the non-root user, Logger can only listen for connections on port 9000/tcp. You cannot configure the port to a different value.

     **Note:** The user must have privileges to write to the installation directory and its sub-directories, for example:

     ```
     chown -R arcsight:arcsight /opt/arcsight
     ```

  c. When upgrading, you cannot change a previous non-root installation to a root-user installation. You will need to use the previously configured port 9000/tcp for accessing Software Logger.

- Install into an empty folder. If you have uninstalled Logger previously, and are installing into the same location, be sure to remove any files that the uninstaller left in place.
- The hostname of the machine on which you are installing Logger cannot be “localhost.” If it is, change the hostname before proceeding with the installation.
- You must not have an instance of MySQL installed on the machine on which you install Logger. If an instance of MySQL exists on that machine, uninstall it before installing Logger.
- If you are installing/uninstalling Logger in console mode with a non-root user, you must unset the DISPLAY environment variable by executing the following command `unset DISPLAY`.
  - If you will be installing Logger over an SSH connection and want to use the GUI mode of installation, make sure that you have enabled X window forwarding using the -X option so that you can view the screens of the installation wizard.
  - If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the machine onto which you want to install Logger.

## Increasing the User Process Limit and the Maximum Number of Open Files

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

### To increase the default user process limit:

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

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

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

2. Add the following lines:

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

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

3. Log out and log back in again.
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
```

After you have increased the user process limit and met the other pre-requisites, you are ready to install Logger.

## Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7x, 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. Find the RemoveIPC line. RemoveIPC should be active and set to no.

   Remove the # if it is there, and = change the `yes` to `no` if appropriate. 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
   ```

After you have modified this setting and met the other prerequisites, you are ready to install Logger.

## Configuring TCP keepalive parameters for Linux OS

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

1. Edit the system file and press Shift + G:

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

2. Add and modify the following timeout properties and their recommended values:

   - `net.ipv4.tcp_fin_timeout = 30`
   - `net.ipv4.tcp_keepalive_time = 60`
   - `net.ipv4.tcp_keepalive_intvl = 2`
   - `net.ipv4.tcp_keepalive_probes = 2`

3. Exit and save:

   ```
   (wq!)
   ```

4. Apply the changes by running the command:

   ```
   sysctl -p
   ```

## Install package rng-tools

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

Make sure to follow the steps below:

1. Install the package by running the following command:

   ```
   yum install -y rng-tools
   ```

2. To see the status of the `rngd.service` after an install, run:

   ```
   systemctl status rngd
   ```

3. Run the commands to start or enable the service:

   ```
   systemctl start rngd.service
   ```

   ```
    systemctl enable rngd.service
   ```

# Installation

Software Logger can be installed in three ways:

- GUI mode: A wizard steps you through the installation and configuration of Software Logger. You must have an X-Windows server installed on your OS to use GUI mode.
- Console mode: A command-line process steps you through the installation and configuration of Software Logger.

  > **Tip:** Console mode may allow you to install Logger more quickly if you encounter bandwidth issues while installing remotely.

- Silent mode: You provide the input required for installation and configuration through a file. Therefore, you do not need to interact with the installer to complete the installation and configuration on each server. However, before you can use this mode, you must run the installation and configuration using one of the other modes to record the input in a file.

## Using GUI Mode to Install Software Logger

Make sure the machine on which you will be installing Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for

Installation" on page 32 are met.

Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on page 35, and for RHEL 7.X only, modify the `logind.conf` file, as described in "Editing the logind Configuration File for RHEL 7.X" on page 36.

You can verify that you have the correct installation file, as described in "Before You Begin" on page 31.

You can install Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 32 for details and restrictions.

> **Note:** If you will be installing the Software Logger using the GUI mode of installation with SSH connection, enable the X window forwarding using the `-X` option to view the screens of the installation wizard. If you will be using PuTTY, an X client is required on the machine from which you are connecting to the machine onto which you want to install Logger.

### To install the Logger software:

1. Run these commands from the directory where you copied the Logger installation file:

   ```
   chmod u+x ArcSight-logger-7.3.L8455.0.bin
   ```

   ```
   ./ArcSight-logger-7.3.L8455.0.bin
   ```

2. The installation wizard launches. Click **Next**.

   You can click **Cancel** to exit the installer at any point during the installation process.

   > **Caution:** Do not use the Ctrl+C to exit the installer and uninstall, uninstallation may delete your `/tmp` directory.

3. The License Agreement screen is displayed. Scroll to the bottom to review the agreement and enable the “I accept the terms of the License Agreement” button.
4. Select **I accept the terms of the License Agreement** and click **Next**.
5. The installer checks that installation prerequisites are met:
   - Operating system check—the installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS.

     > **Note:** Micro Focus ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the Release Notes for a list of supported operating system platforms.

- Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

Once all the checks are complete, the **Choose Install Folder** screen is displayed.

**Example**

An Intervention Required message displays, informing you that a parameter needs to be changed from `yes` to no in the `etc/logind.conf` file. The message tells you what needs to be done. In this example, quit the installer, and follow the instructions in "Editing the logind Configuration File for RHEL 7.X" on page 36. When the file has been modified and saved, enter the installation command again.

6. Navigate to or specify the location where you want to install Logger.

   The default installation path is `/opt` but you can install in another location of your choice.

7. Click **Next** to install into the selected location.

   - If there is insufficient space at the location you specified, a message is displayed. Make sufficient space available or specify a different location by clicking **Previous**. Otherwise, click **Quit** to exit the installer.
   - If Logger is already installed at the location you specified, a message is displayed. Click **Upgrade** to continue or **Previous** to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

8. Review the pre-install summary and then click **Install**.

   Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

9. If you are logged in as root, the following prompts are displayed. Fill in the fields and click **Next**.

| Field | Notes |
|---|---|
| Non-root user name | If this user does not already exist on the system, you are prompted to supply one. |
| HTTPS port | The port number to use when accessing the Logger UI.<br>You can keep the default HTTPS port (443/tcp) or enter any other port that suits your needs. If you specify any port except 443/tcp, users will need to enter that port number in the URL they use to access the Logger UI. |
| Configure Logger as a service | Indicate whether to configure Logger to run as a service.<br>Select this option to create a service called `arcsight_logger,` and enable it to run at levels 2, 3, 4, and 5. |

| Field | Notes |
|---|---|
| | If you do not enable Logger to start as service during the installation process, you can still do so later. For instructions on how to enable Logger to start as a service after installation, see "Software Logger and Logger Appliance L8000 Command Line Options" on page 47. |

10. Select the locale of this installation and click **Next**.
11. Specify the path and file name of the license file and click **Next**. The initialization screen is displayed.

    > **Note:** If you do not provide a license file, Logger installs a 90-day trial license with significant limitations. See "Trial Licenses" on page 10.

12. Click **Next** again to Initialize Logger components. Initialization may take a few minutes. Once initialization is complete, the configuration screen is displayed.
13. Click **Next** to allow Logger to configure storage groups and storage volume. Configuration may take a few minutes.

    Once it appears the **Configuration is Complete** window, Logger starts and the Logger user interface is displayed.
14. Make a note of the URL and then click **Done** to exit the installer.

Now that you are done installing and initializing your Logger, you can use the URL you noted during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on page 46.

## Using Console Mode to Install Software Logger

Make sure the machine on which you will be installing Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 32 are met.

Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on page 35, and for RHEL 7.X only, modify the `logind.conf` file, as described in "Editing the logind Configuration File for RHEL 7.X" on page 36.

You can verify that you have the correct installation file, as described in "Before You Begin" on page 31.

You can install Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 32 for details and restrictions.

### To install the Logger software:

1. Run these commands from the directory where you copied the Logger installation file:

   ```
   chmod u+x ArcSight-logger-7.3.L8455.0.bin
   ```

   ```
   ./ArcSight-logger-7.3.L8455.0.bin -i console
   ```

2. The installation wizard launches in command-line mode. Press **Enter** to continue.

   ```
   ==========================================================================
   Introduction
   InstallAnywhere will guide you through the installation of ArcSight Logger
   7.3.
   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 next several screens display the end user license agreement. Press **Enter** to display each part of the license agreement, until you reach the following prompt:

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

4. Type Y and press **Enter** to accept the terms of the License Agreement.

   You can type `quit` and press **Enter** to exit the installer at any point during the installation process.

5. The installer checks that installation prerequisites are met:

   - Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS.

     > **Note:** Micro Focus ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the Release Notes for a list of supported operating system platforms.

   - Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

**Example**

If Logger is running on this machine, an Intervention Required message displays:

```
========================================================================
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:
```

In this case, you would enter 1 (or hit **Enter**) to stop Logger processes, or 2 to quit the installer.

Once all checks complete, the installation continues, and the Choose Install Folder screen is displayed.

6. From the Choose Install Folder screen, type the installation path for Logger and then press **Enter**.

   The default installation path is `/opt`. You can install into this location or another location of your choice.

7. Type Y and press **Enter** to confirm the installation location.

   - If there is not enough space to install the software at the location you specified, a message is displayed. To proceed with the installation, specify a different location or make sufficient space available at the location you specified. Type `quit` and press **Enter** to exit the installer.

   - If Logger is already installed at the location you specify, a message is displayed. Enter 2 to continue with the upgrade and 1 to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

8. Review the pre-install summary and press **Enter** to install Logger.

   Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

9. If you are logged in as root, the following prompts are displayed. Type your response and press **Enter** after each.

| Field | Notes |
|---|---|
| User Name | If this user does not already exist on the system, you are prompted to supply one.<br>✓ **Tip:** When installing Logger on VMWare VM, use the non-root user `arcsight` that comes preconfigured on your system. |
| HTTPS Port | The port number to use when accessing the Logger UI.<br>You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI. |
| Choose if you want to run Logger as a system service. | Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone.<br>Select this option to create a service called `arcsight_logger`, and enable it to run at levels 2, 3, 4, and 5.<br>If you do not enable Logger to start as service during the installation process, you still do so later. For instructions on how to enable Logger to start as a service after installation, refer to the ArcSight Logger 7.3  Administrator's Guide. |

10. Type the number for your desired locale, and press **Enter:**
    - 1 for English
    - 2 for Japanese
    - 3 for Simplified Chinese
    - 4 for Traditional Chinese
11. Type the absolute the path to the license file and click **Next**.

    > **Note:** If you do not provide a license file, Logger installs a 90-day trial license that has significant restrictions. See "Acquiring a License for a Logger" on page 10.

    The initialization screen is displayed.
12. Press **Enter** again to initialize Logger components.

    Initialization may take a few minutes. Please wait. Once initialization is complete, the configuration screen is displayed.
13. Click **Next** to configure storage groups and storage volume and restart Logger

    Configuration may take a few minutes. Please wait.

    Once configuration is complete, Logger starts up and the next screen is displays the URL you should use to connect to Logger.
14. Make a note of the URL and then press **Enter** to exit the installer.

Now that you are finished installing and initializing your Logger, you can use the URL you noted during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on page 46.

## Using Silent Mode to Install Software Logger

Before you install Software Logger in silent mode, you need to create the properties file required for the silent mode installation. Once you have generated the file, you can use it for silent mode installations.

### Licenses for Silent Mode Installations

As for any Logger installation, each silent mode installation requires a unique license file. You must obtain licenses as described in "Acquiring a License for a Logger" on page 10 and place them on the machines on which you will be installing Logger in silent mode, or ensure that the location where the licenses are placed is accessible from those machines.

### Generating the Silent Install Properties File

**To generate a properties file for future silent installations:**

1. Log in to the machine on which you will install Software Logger to generate an installation properties file.

   If you want the silent mode installations to be done as root user, log in as `root`. Otherwise, log in as a non-root user.

2. Run these commands:

   ```
   chmod u+x ArcSight-logger-7.3.L8455.0.bin
   ```

   ```
   ./ArcSight-logger-7.3.L8455.0.bin -r <path_for_generated_file>
   ```

   The `<path_for_generated_file>` is the directory location where the generated properties file called `installer.properties` should be placed. You cannot specify or change this name.

3. Install Logger in GUI mode. See "Using GUI Mode to Install Software Logger" on page 37.

4. Once the installation completes, navigate to the directory location you specified for the `installer.properties` file earlier. Then go to "Installing Software Logger in Silent Mode" on the next page.

   The following is an example of a generated `installer.properties` file.

   ```
   # Wed Aug 14 18:27:49 PDT 2016
   # Replay feature output
   # ---------------------
   # This file was built by the Replay feature of InstallAnywhere.
   # It contains variables that were set by Panels, Consoles or Custom Code.
   ```

```
#Choose Install Folder
#---------------------
USER_INSTALL_DIR=/opt/Logger
```

```
#License Information
#-------------------
LICENSE_LOCATION=/home/user/arcsight.lic
```

## Installing Software Logger in Silent Mode

Make sure the machine on which you will be installing the Software Logger complies with the platform requirements listed in the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 32 are met.

If you are installing as root, make sure the non-root user account you entered in previous steps exists on the machines on which you are using the silent installer to install Logger.

### To install the Software Logger using the Silent mode:

1. Copy the silent mode properties file previously generated to the same location you have copied the Logger software.
2. Edit the LICENSE_LOCATION property in the properties file to include the location of license file (a unique license file is required for each instance of installation).

   Or

   Set the LICENSE_LOCATION property to point to a file, such as logger_license.zip. Then, for each instance of the silent mode installation, copy the relevant license file to the location and rename it to logger_license.zip. Doing so will avoid the need to update the combined properties file for each installation.
3. Run these commands from the directory where you copied the Logger software:

   ```
   chmod u+x ArcSight-logger-7.3.L8455.0.bin
   ```

   ```
   ./ArcSight-logger-7.3.L8455.0.bin -i SILENT -f <path to
   installer.properties>
   ```

The rest of the installation and configuration proceed silently, without requiring any input from you.

After the installation and initialization completes, you can use the URL created during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on the next page.

# Connecting to Software Logger

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the Release Notes for details on Logger 7.3 browser support.

Logger's publicly-accessible ports must be allowed through any firewall rules. For Software Logger, you are responsible for setting up the firewall. Firewall rules are preconfigured on the Logger Appliance. See "Firewall Rules" on page 14 for more information.

- 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.

- JavaScript and cookies must be enabled.

### To connect to Logger:

Use the URL configured during Logger installation to connect to Logger through a supported browser.

For Software Logger or Logger Appliance L8000: `https://<hostname or IP address>:<configured_port>`

For Logger Appliance L7700: `https://<hostname or IP address>`

where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

After you connect, the Login screen is displayed.

### To log in:

When the Login dialog is displayed, enter your user name and password, and click **Login**.

Use the following default credentials if you are connecting for the first time:

```
Username: admin
Password: password
```

> **Note:** After logging in for the first time with the default user name and password, you will be prompted to change the password. Follow the prompts to enter and verify the new password.

For more information about the Login screen and connecting to Logger and receive events, refer to the ArcSight Logger 7.3  Administrator's Guide.

# Software Logger and Logger Appliance L8000 Command Line Options

**This topic applies to Software Loggers and L8000 Logger Appliances**

The `loggerd` command enables you to start or stop these types of Loggers. In addition, the command includes a number of subcommands that you can use to control other processes that run as part of the Logger.

> **Note:** If your Logger is installed to run as a system service, you can use your operating system's `service` command to start, stop, or check the status of a process on Logger. The default service name is `arcsight_logger`.

- For a Software :

  ```
  <install_dir>/current/arcsight/logger/bin/loggerd
  {start|stop|restart|status|quit}
  ```

  ```
  <install_dir>/current/arcsight/logger/bin/loggerd {start <process_name> |
  stop <process_name> | restart <process_name>}
  ```

- For a  Appliance L8000:

  ```
  /opt/softlogger/current/arcsight/logger/bin/loggerd
  {start|stop|restart|status|quit}
  ```

  ```
  /opt/softlogger/current/arcsight/logger/bin/loggerd {start <process_name>
  | stop <process_name> | restart <process_name>}
  ```

To view the processes that can be started, stopped, or restarted with `loggerd`, click **System Admin** from the top-level menu bar. Then, under **System**, pick **Process Status.** The processes are listed on the right under **Processes.**

The following table describes the subcommands available with `loggerd` and their purpose.

| Command | Purpose |
|---|---|
| `loggerd start` | Start all processes listed under the System and Process sections. Use this command to launch Logger. |
| `loggerd stop` | Stop processes listed under the Process section only. Use this command when you want to leave loggerd running but all other processes stopped.<br>**Important:**Micro Focus recommends that you do not stop the **servers** process. To shut down Logger, use the `loggerd stop` or `quit` commands.<br>Never stop the Logger**servers** process while events are still coming in, this can cause data loss. If you must stop the **servers** process, be sure to stop the **receivers** process first, then stop the **servers** process. |
| `loggerd restart` | This command restarts processes listed under the Process section only.<br>**Note:** When the `loggerd restart` command is used to restart Logger, the status message for the “aps” process displays this message:<br>`Process ‘aps’ Execution failed.`<br>After a few seconds, the message changes to:<br>`Process ‘aps’ running.` |
| `loggerd status` | Display the status of all processes. |
| `loggerd quit` | Stops all processes listed under the System and Process sections. Use this command to stop Logger. |
| `loggerd start <process_name>` | Start the named process. For example, `loggerd start apache` |
| `loggerd stop <process_name>` | Stop the named process. For example, `loggerd stop apache` |
| `loggerd restart <process_name>` | Restart the named process. For example, `loggerd restart apache` |

You can also start and stop and view the status of Logger processes from the **System Admin > System > Process Status** page.

# Uninstalling Logger

If you will be uninstalling the Software Logger over an SSH connection and want to use GUI mode, make sure that you have enabled X window forwarding using the `-X` option, so that you can view the screens of the uninstall wizard. If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the Linux machine.

Before uninstalling Logger, stop the Logger processes by using the `loggerd stop` command, as described in Software Logger and Logger Appliance L8000 Command Line Options

### To uninstall the Logger software:

1. Enter this command in the installation directory:

   ```
   ./UninstallerData/Uninstall_ArcSight_Logger_7.3.0
   ```

   The uninstall wizard launches.

2. Click **Uninstall** or press **Enter** to start uninstalling Logger.

# Chapter 5: Installing Software Logger on VMware

You can install Software Logger on a Linux system or on a VMware VM. This chapter explains what you need to know to install and start running Software Logger on a VMware VM.

For information on how to install Software Logger on Linux, see Installing Software Logger on Linux. For initialization information about the Logger Appliance, see Setting Up a Logger Appliance L7700.

## Before You Begin

You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5 or greater. The VM image includes the Logger 7.3 installer on 64-bit CentOS 7.9 operating system, configured with 16 GB RAM and four physical (and eight logical) cores. Refer to the Release Notes for details on the Logger 7.3 release. For more information on the release, refer to the Release Notes.

**Important**: The VM image on 32-bit is no longer supported.

### Downloading the Installation Package

The installation package for the latest version of Logger does not include an OVA file, instead take the OVA file Logger 7_2_L8372_Q1001.ova available for download from the Micro Focus Software Depot. Upgrade to Logger 7.3 by following the instructions from "Installing Software Logger on Linux" on page 31

**Note:** OVA is not available for Logger 7.3. For more information on how to install Logger on VMware, see "Installing Logger on the Virtual Machine" on page 53

### Verifying the Downloaded Installation Software

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

## How Licensing Works in Software Logger

Logger comes with a limited functionality trial license that is valid for only 90 days. To access the full functionality, upload your EPS or GB per day license as Standalone Logger or Managed by ArcMC. See "Trial Licenses" on page 10 for more information.

If you do not have a license file, see "Acquiring a License for a Logger" on page 10. Depending on your purchase order, you need a separate license file for each instance of Software Logger. A license file is uniquely generated for each Logger download.

The type of license you have affects how the license usage restriction function works and what is displayed on the **License Usage** page.

- For Loggers managed by ArcMC, ArcSight Management Center manages the license (EPS or GB per day) restrictions. Refer to the ArcSight Management Center Administrator’s Guide for more information.
- For standalone ArcSight Loggers, the license usage restriction function manages the license (EPS or GB per day) restrictions.

The license usage restriction function adds the sum of the sizes of the events received on a given day to compute the amount of data that comes into Logger per day. Logger compares that value against the daily data limit in the license. If this limit is exceeded, Logger continues to collect and store events, so that no events are lost. For GB per day license, if the daily data limit is exceeded on more than five days in a 30-day sliding window, all search-related features are disabled. You will not be able to forward, search, or run reports on the collected events until the 30-day sliding window contains five or less data limit violations. For EPS, there is no over the limit restrictions for the 45 days displayed on the graph.

The license usage page (**Configuration > Advanced > License Usage**) lists the data stored on your Software Logger on day-by-day basis in the last 45 days for EPS ( 30 days for GB per day). It also indicates the days on which data limits were exceeded. For more information, see chapter 5 of ArcSight Logger 7.3  Administrator’s Guide.

Once you obtain the new license, follow the instructions in the ArcSight Logger 7.3 Administrator’s Guide to apply it on your Logger.

## Prerequisites for Installation

The VM has the default root password `arcsight`. A non-root user, `arcsight`, with no password, is also included. This user is required for installation.

**Caution:** For security reasons and so that you can SCP or SSH to your machine, change the root password and add a password for the arcsight user as soon as possible.

Make sure these prerequisites are met before you install the Logger software on the VM:

- Boot up the operating system on the VM, log in, set the timezone, and do any other necessary configuration before proceeding with the installation.
- Configure the network on the VM as appropriate for your environment. The hostname must be resolvable, either by the DNS server or by settings in `/etc/hosts`.
- Ensure the `/etc/systemd/logind.conf parameter RemoveIPC` is set to `RemoveIPC=no`, see "Editing the logind Configuration File for RHEL 7.X" on page 36
- SELinux and SSH are enabled on the OS, but the firewall is disabled. To ensure proper access to Logger, enable a firewall and add your firewall policy to allow or deny devices as soon as possible. For more information, see "Firewall Rules" on page 14.
- Before deploying in a production environment, get a valid license file. If you do not have a license file, see "How Licensing Works in Software Logger" on the previous page. You may need a separate license file for each instance of Logger. A license file is uniquely generated for each download.
- SCP the license to the VM and make a note of the file name and location; you will need them during the installation process.
- Decide whether to install Logger while logged in as root or as the preconfigured non-root user, arcsight. Your installation options vary depending on which user you choose.
  a. If you install as root, you can choose to configure Logger to start as a service and select the port on which Logger listens for secure web connections.
  b. If you install as the non-root user, Logger can only listen for connections on port 9000/tcp. You cannot configure the port to a different value.

     **Note:** The user must have privileges to write to the installation directory and its sub-directories, for example:

     ```
     chown -R arcsight:arcsight /opt/arcsight
     ```

  c. When upgrading, you cannot change a previous non-root installation to a root-user installation. You will need to use the previously configured port 9000/tcp for accessing Software Logger.
- Install into an empty folder. If you have uninstalled Logger previously, be sure to remove any files that the uninstaller left in place.
- The hostname of the machine on which you are installing Logger cannot be “localhost.” If it is, change the hostname before proceeding with the installation.

- You must not have an instance of MySQL installed on the machine on which you install Logger. If an instance of MySQL exists on that machine, uninstall it before installing Logger.

## Installing Logger on the Virtual Machine

Make sure the machine on which you will be installing Software Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 51 are met.

### Preinstallation:

You can verify that you have the correct installation file, as described in "Before You Begin" on page 50.

You can install Logger as a root user or as the non-root user, arcsight. See "Prerequisites for Installation" on page 51 for details and restrictions.

**Note:** You must install Logger in the `/opt/arcsight/logger` directory.

### To install the Logger software:

1. Run these commands from the directory where you copied the Logger installation file:

```
chmod u+x ArcSight-logger-7.3.8455.0.bin
```

```
./ArcSight-logger-7.3.8455.0.bin -i console
```

2. The installation wizard launches in command-line mode. Press **Enter** to continue.

```
==========================================================================
Introduction
------------
InstallAnywhere will guide you through the installation of ArcSight Logger
7.3.
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 next several screens display the end user license agreement. Press **Enter** to display each part of the license agreement, until you reach the following prompt:

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

4. Type Y and press **Enter** to accept the terms of the License Agreement.

   You can type `quit` and press **Enter** to exit the installer at any point during the installation process.

5. The installer checks that installation prerequisites are met:

   - Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS.

     > **Note:** Micro Focus ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the Release Notes for a list of supported operating system .platforms.

   - Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

   **Example**

   If Logger is running on this machine, an Intervention Required message displays:

   ```
   ========================================================================
   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:
   ```

   In this case, you would enter 1 (or hit **Enter**) to stop Logger processes, or 2 to quit the installer.

   Once all checks complete, the installation continues, and the Choose Install Folder screen is displayed.

6. From the Choose Install Folder screen, type the installation path for Logger and then press **Enter**.

   The default installation path is `/opt`. The installation path on the VM image is `/opt/arcsight/logger`. You must use this location. Do not specify a different location.

7. Type Y and press **Enter** to confirm the installation location.

   - If there is not enough space at the location you specified, a message is displayed. Make sufficient space available or specify a different location by typing `quit`.

Otherwise, press **Enter** to exit the installer.

- If Logger is already installed at the location you specify, a message is displayed. Enter 2 to continue with the upgrade and 1 to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

8. Review the pre-install summary and press **Enter** to install Logger.

   Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

9. If you are logged in as root, the following prompts are displayed. Type your response and press **Enter** after each.

| Field | Notes |
|---|---|
| User Name | If this user does not already exist on the system, you are prompted to supply one.<br>**Tip:** When installing Logger on VMWare VM, use the non-root user `arcsight` that comes preconfigured on your system. |
| HTTPS Port | The port number to use when accessing the Logger UI.<br>You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI. |
| Choose if you want to run Logger as a system service. | Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone.<br>Select this option to create a service called `arcsight_logger`, and enable it to run at levels 2, 3, 4, and 5.<br>If you do not enable Logger to start as service during the installation process, you still do so later. For instructions on how to enable Logger to start as a service after installation, refer to the ArcSight Logger 7.3  Administrator's Guide. |

10. Type the number for your desired locale, and press **Enter:**

    - 1 for English
    - 2 for Japanese
    - 3 for Simplified Chinese
    - 4 for Traditional Chinese

11. Type the absolute the path to the license file and click **Next**. The initialization screen is displayed.

    **Note:** If you do not provide a license file, Logger installs a 90-day trial license that has significant restrictions. See "Acquiring a License for a Logger" on page 10.

12. Press **Enter** again to initialize Logger components. Initialization may take a few minutes. Once initialization is complete, the configuration screen is displayed.

13. Click **Next** to configure storage groups and storage volume and restart Logger

    Configuration may take a few minutes. Once configuration is complete, Logger starts up and the next screen displays the URL you should use to connect to Logger.

14. Make a note of the URL and then press **Enter** to exit the installer.

Now that you are finished installing and initializing your Logger, you can use the URL you noted during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on page 46.

# Connecting to Software Logger

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the Release Notes for details on Logger 7.3 browser support.

Logger's publicly-accessible ports must be allowed through any firewall rules. For Software Logger, you are responsible for setting up the firewall. Firewall rules are pre-configured on the Logger Appliance. See "Firewall Rules" on page 14 for more information.

- For root installs, allow access to port `443/tcp` (or the https port configured during the install) 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. If new ports are configured, make sure to include them in the firewall rules.

JavaScript and cookies must be enabled.

### Connecting to Logger:

Use the URL configured during Logger installation to connect to Logger through a supported browser.

For Software Logger or Logger Appliance L8000: `https://<hostname or IP address>:<configured_port>`

For Logger Appliance L7700: `https://<hostname or IP address>`

where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

### Logging into Logger

When the Login dialog is displayed, enter your user name and password, and click **Login**.

Use the following default credentials if you are connecting for the first time:

**Username:** admin
**Password:** password

**Note:** After logging in for the first time with the default user name and password, you will be prompted to change the password. Follow the prompts to enter and verify the new password.

For more information about the Login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the ArcSight Logger 7.3  Administrator’s Guide.

Once you have logged in successfully, you can enable the pre-configured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy. See "Configuring Logger" on page 60 and refer to the **Configuration** chapter of ArcSight Logger 7.3  Administrator’s Guide.

## Using Software Logger Command Line Options

The `loggerd` command enables you to start or stop the Logger software running on your machine. In addition, the command includes a number of subcommands that you can use to control other processes that run as part of the Logger software.

**Note:** If your Logger is installed to run as a system service, you can use your operating system’s `service` command to start, stop, or check the status of a process on Logger.

```
<install_dir>/current/arcsight/logger/bin/loggerd
{start|stop|restart|status|quit}<install_dir>
```

```
/current/arcsight/logger/bin/loggerd {start <process_name> | stop <process_
name> | restart <process_name>}
```

To view the processes that can be started, stopped, or restarted with `loggerd`, click **System Admin** from the top-level menu bar. Then, under **System**, pick **Process Status**. The processes are listed on the right under **Processes.**

The following table describes the subcommands available with `loggerd` and their purpose.

| Command | Purpose |
|---|---|
| `loggerd start` | Start all processes listed under the System and Process sections in the figure above. Use this command to launch Logger. |
| `loggerd stop` | Stop processes listed under the Process section only. Use this command when you want to leave `loggerd` running but all other processes stopped. |
| `loggerd restart` | This command restarts processes listed under the Process section only.<br>**Note:** When the `loggerd restart` command is used to restart Logger, the status message for the “aps” process displays this message:<br>Process ‘aps’ Execution failed<br>After a few seconds, the message changes to:<br>Process ‘aps’ running |
| `loggerd status` | Display the status of all processes. |
| `loggerd quit` | Stops all processes listed under the System and Process sections in the figure above. Use this command to stop Logger. |
| `loggerd start <process_name>` | Start the named process. For example, `loggerd start apache`. |
| `loggerd stop <process_name>` | Stop the named process. For example, `loggerd stop apache`. |
| `loggerd restart <process_name>` | Restart the named process. For example, `loggerd restart apache` |

You can also start and stop and view the status of Logger processes from the **System Admin > System > Process Status** page. Refer to the ArcSight Logger 7.3  Administrator’s Guide or online help for more information.

# Uninstalling Logger

To uninstall the Logger software, simply delete the VM. Alternatively, you can uninstall the software Logger from the VM.

If you will be uninstalling the Software Logger over an SSH connection and want to use GUI mode, make sure that you have enabled X window forwarding using the `-X` option, so that you can view the screens of the uninstall wizard. If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the Linux machine.

Before uninstalling Logger, stop and then quit the Logger processes by using the `loggerd stop` and `loggerd quit` commands, as described in Software Logger and Logger Appliance L8000 Command Line Options

### To uninstall the Logger software:

1. Enter this command in the installation directory:

   ```
   ./UninstallerData/Uninstall_ArcSight_Logger_7.3
   ```

   The uninstall wizard launches.

2. Click **Uninstall** or press **Enter** to start uninstalling Logger.

# Chapter 6: Configuring Logger

This chapter includes basic deployment and configuration information on the following topics. It is applicable to all Logger types. If you have installed multiple Loggers, you must connect to each and configure it separately or use ArcSight Management Center to make bulk configuration changes.

For more information on directly configuring and administering your Logger, refer to the ArcSight Logger 7.3  Administrator's Guide. For more information on configuring and administering your Logger using ArcSight Management Center, refer to the ArcSight Management Center Administrator's Guide . For more information on setting Connectors, refer to the documentation for each Connector.

## Receiving Events and Logs

Logger comes preconfigured with several receivers that are ready to receive events and log files directly from devices and systems on your network, such as syslog servers, NFS, CIFS, or SAN systems.

> **Note:** In order to retrieve logs correctly and prevent rotation, Software Logger requires 2 Linux OS pre-installed packages: zip and unzip.

Logger can also receive events from ArcSight SmartConnectors that collect event data from sources on your network. A subset of ArcSight SmartConnectors is supported for Trial Logger and available for download from the same location from which you downloaded Logger. The Configuration Guides for the supported SmartConnectors are included and available at the same web site. To learn more about ArcSight SmartConnectors, visit Installation and User Guide for SmartConnectors.

### Receivers

Now that you have finished installing Logger, you can set up receivers to listen for events. Logger comes preconfigured with several receivers that are ready to receive events and log files directly from devices and systems on your network, such as syslog servers, NFS, CIFS, or SAN systems. You can use the preconfigured receivers or add your own. Receivers can be disabled and re-enabled later. You can add, change, and delete them as needed.

The preconfigured receivers include a TCP receiver, a UDP Receiver, and a SmartMessage receiver already enabled and ready to receive events. Logger also comes preconfigured with folder follower receivers for Logger's Apache Access Error Log, the system Messages Log, and the system Messages Audit Log (if auditing is enabled on your Linux OS).

To receive data, a receiver's ports must be allowed through any firewall rules. See "Firewall Rules" on page 14 for more information. You must enable these receivers in order to use them. See "Enabling the Preconfigured Folder Follower Receivers" below for instructions.

The preconfigured receivers are described more detail in "Receivers" on page 13. For further information on receivers, refer to the Configuration chapter of the ArcSight Logger 7.3 Administrator’s Guide.

Logger can also receive events from ArcSight SmartConnectors that collect event data from sources on your network. To learn more about ArcSight SmartConnectors, visit Micro Focus Documentation.

## Enabling the Preconfigured Folder Follower Receivers

The preconfigured receivers are described more detail in "Receivers" on page 13. For further information on receivers, refer to the **Configuration** chapter of the ArcSight Logger 7.3 Administrator’s Guide.

When you first log in by using the URL you configured, the preconfigured folder follower receivers are disabled. Click **Add Data** under **Home** page to open the Receivers page and enable the receivers.

> ✓ **Tip:** Before enabling these receivers, you must make `/var/log/audit/audit.log` and `/var/log/messages` readable by the non-root user you installed with or specified during Logger installation.

To enable a receiver, click the disabled icon (⊘) at the end of the row.

Alternately, you can navigate to the Receivers page from the menu to enable the receivers.

### To open the Receivers page from the menu and enable a receiver:

1. Open the **Configuration > Data** menu and click **Receivers**.
2. Identify the receiver you want to enable, and click the disabled icon ( ⊘) at the end of that row.

For information on how to use the pre-configured SmartMessage receiver, see "Using SmartConnectors to Collect Events" on page 63.

## Configuring New Receivers

In addition to the out-of-box receivers, you can configure other receivers to meet your needs. Receiver types include UDP, TCP, SmartMessage, and three types of file follower, File Transfer, File Receiver, and Folder Follower Receiver.

You can configure the following types of receiver for Logger:

- **UDP Receiver**: UDP receivers listen for User Datagram Protocol messages on the port you specify. The pre-installed UDP receiver is enabled by default.
- **CEF UDP Receiver**: UDP receivers that receive events in Common Event Format.
- **TCP Receiver**: TCP receivers listen for Transmission Control Protocol messages on the port you specify. The pre-installed TCP receiver is enabled by default.
- **CEF TCP Receiver**: TCP receivers that receive events in Common Event Format.
- **File Receiver**: Depending on the type of Logger, file receivers read log files from a local file system, Network File System (NFS), Common Internet File System (CIFS), or Storage Area Network (SAN). File receivers read single or multi-line log files. They provide a snapshot of a log file at a single point in time.
- **Folder Follower Receiver:** Folder follower receivers actively read the log files in a specified directory as they are updated. If the source directory contains different types of log files, you can create a receiver for each type of file that you want to monitor. To start using the pre-installed folder follower receivers you must enable them.
- **File Transfer**: File Transfer receivers read remote log files using Secure Copy Protocol (SCP), Secure file transfer protocol (SFTP), or File Transfer Protocol (FTP) protocol. These receivers can read single- or multi-line log files. You can schedule the receiver to read a file or batch of files periodically.

  **Caution:** The SCP and SFTP protocols on L7700 Logger appliances are not FIPS compliant.

  **Note:** The SCP, SFTP, and FTP file transfer receivers depend on the FTP, SCP, and SFTP clients installed on your system.

- **SmartMessage Receiver**: SmartMessage receivers listen for encrypted messages from ArcSight SmartConnectors. To start using the pre-installed receiver, you must configure a SmartConnector to send events to it. For instructions, see "Configuring a SmartConnector to Send Events to Logger" on the next page.

## Sending Structured Data to Logger

Although Logger is message-agnostic, it can do more with messages that adhere to the Common Event Format (CEF), an industry standard for the interoperability of event- or log-generating devices. Events in Common Event Format (CEF) have more columns defined, making the data more useful.

Logger can receive structured data in the form of normalized CEF events from ArcSight SmartConnectors, as shown in the illustration in "How Logger Works" on page 8.

## Using SmartConnectors to Collect Events

Similar to ArcSight Manager, Logger leverages the ArcSight SmartConnectors to collect events. SmartConnectors can read security events from heterogeneous devices on a network (such as firewalls and servers) and filter events of interest (and optionally aggregate them) and send them to a Logger receiver. Logger can receive structured data in the form of normalized Common Event Format (CEF) events from the SmartConnectors.

This section gives basic information on each of these topics. For details, refer to the documentation for that Connector and the SmartConnector User's Guide, available at the Micro Focus Security Community.

### SmartMessage

SmartMessage is an Micro Focus ArcSight technology that provides an efficient secure channel for Common Event Format (CEF) events between ArcSight SmartConnectors and Logger.

SmartMessage provides an end-to-end encrypted secure channel using Transport Layer Security (TLS). One end is an ArcSight SmartConnector, receiving events from the many devices supported by ArcSight SmartConnectors. The other end is a SmartMessage receiver on Logger.

> **Note:** The SmartMessage secure channel uses TLS protocol to send encrypted events to Logger. This is similar to, but different from, the encrypted binary protocol used between SmartConnectors and ArcSight Manager.

### Configuring a SmartConnector to Send Events to Logger

Logger comes pre-configured with a SmartMessage Receiver. To receive events from a SmartConnector, you must configure the SmartConnector as described below. You can also create new SmartMessage receivers and configure the SmartConnectors with these newly created receivers. When configuring a SmartConnector, be sure to specify the correct receiver name.

**To configure a SmartConnector to send events to Logger:**

1. Install the SmartConnector component using the SmartConnector User’s Guide as a reference. Specify Logger as the destination instead of ArcSight ESM or a CEF file.

   > **Note:** Refer to the documentation that came with your SmartConnector for instructions.

2. Specify the required parameters. Enter the Logger hostname or IP address and the name of the SmartMessage receiver. These settings must match the receiver in Logger that listen for events from this connector.
   - To use the pre-configured receiver, specify “SmartMessage Receiver” as the **Receiver Name**.
   - To use SmartMessage to communicate between an ArcSight SmartConnector and a Logger Appliance L7700, configure the SmartConnector to use port 443/tcp.
   - To communicate between an ArcSight SmartConnector and Software Logger or a Logger Appliance L8000, configure the SmartConnector to use the port configured for the Software Logger.
   - For unencrypted CEF syslog, enter the Logger hostname or IP address, the desired port, and choose UDP or TCP output.

## Configuring SmartConnectors to Send Events to Both Logger and an ArcSight Manager

You can configure a SmartConnector to send CEF syslog output to Logger and send events to an ArcSight Manager at the same time.

1. Install the SmartConnector normally. Register the SmartConnector with a running ArcSight Manager and test that the SmartConnector is up and running.
2. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
3. Select **I want to add/remove/modify ArcSight Manager destinations**, then choose **Add new destination**.
4. Choose Logger and specify the requested parameters. Restart the SmartConnector for changes to take effect.

## Configuring SmartConnectors for Failover Destinations

SmartConnectors can be configured to send events to a secondary failover destination when a primary connection fails.

### To configure a failover destination, follow these steps:

1. Configure the SmartConnector for the primary Logger as described above. The transport must be raw TCP in order to detect the transmission errors that trigger failover.
2. Edit the `agent.properties` file in the directory `$ARCSIGHT_HOME/current/user/agent`, where `$ARCSIGHT_HOME` is the root directory where the SmartConnector component was

installed.

a. Add this property:

```
transport.types=http,file,cefsyslog
```

b. Delete this property:

```
transport.default.type
```

3. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
4. Choose **I want to add/remove/modify** and, with the primary Logger selected, choose **Modify**. Then select **Add failover destination**.
5. Enter information for the secondary Logger.
6. Restart the SmartConnector for the changes to take effect.
7. For more information about installing and configuring ArcSight SmartConnectors, refer to the ArcSight SmartConnector User's Guide, or specific SmartConnector Configuration Guides, available from the Micro Focus Community.

## Downloading SmartConnectors

Contact your Micro Focus ArcSight sales representative or customer support for the location to download the supported SmartConnectors. To learn more about ArcSight SmartConnectors, visit Micro Focus Documentation.

# Devices

Logger begins storing events when an enabled receiver receives data or, in the case of a file receiver, when the files become available. Using a process called autodiscovery, Logger automatically creates resources called devices to keep track of source IP addresses and uses DNS to map them to hostnames. Eventually, a device is created for each device from which Logger received events.

You can also create devices preemptively, by entering the IP addresses or hostnames of data sources that you expect to be sending events to Logger. You might do this if you do not want to wait for autodiscovery, or if you want to control the initial naming of each device. Discovered devices are named for their host, or if the DNS lookup fails, for their IP address, and their receiver. For information about creating devices, see the ArcSight Logger 7.3  Administrator’s Guide.

# Device Groups

Device groups are containers or logical groupings for devices, in the same way folders (or directories) contain files. They are a name for a group of devices. A given device can be a member of several device groups. Each device group can be associated with particular storage group, which would assign a retention policy.

You can change and delete device groups freely as your needs change. Setting up device groups initially is not critical; incoming events that are not assigned to a device group are automatically sent to the Default Storage Group. For the details of setting up device groups, see the ArcSight Logger 7.3  Administrator’s Guide.

# Storage Rules

Events are stored in the Default Storage Group unless otherwise specified. Storage rules are a way to direct events from certain device groups to certain storage groups. You can use them to implement additional retention policies.

If you want to implement multiple retention policies, you can create storage rules that associate the specific device groups with the storage groups that implement the desired retention policy.

For example, you could create one device group for each retention policy. However, for more control, you could associate device groups with storage groups and storage rules and use them to categorize events.

Storage rules are evaluated in order of priority; the first matching rule determines where the event is sent. This approach means that a single device can belong to several device groups without ambiguity about which storage group it will end up in.

For more information, see ArcSight Logger 7.3  Administrator’s Guide.

# Roles

Tuning role(s) (Reports, Search, Forwarding, and Receiver, Storing Support per Search Roles) guarantees better performance in your daily activities. You can (un)check any role as needed. Still, you can access any unchecked role and perform any activity with the minimum required memory.

For more information, see ArcSight Logger 7.3  Administrator’s Guide.

# Sending Events from ArcSight ESM to Logger

The ArcSight Forwarding SmartConnector can read events from an ArcSight Manager and forward them to Logger as CEF-formatted syslog messages.

> **Note:** The Forwarding SmartConnector is a separate installable file, named similar to these:
>
> `ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.exe`
>
> `ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.bin`
>
> Use build 4810 or later for compatibility with Logger.

### To configure the ArcSight Forwarding SmartConnector to send events to Logger:

1. Install the SmartConnector component normally, but cancel the installation when the SmartConnector Wizard asks whether the target Manager uses a demo certificate.

   When the first screen of the SmartConnector Configuration Wizard appears, asking about a demo certificate, click **Cancel**.
2. Confirm that you want to exit, then click **Done** to dismiss the Install Wizard. This will install the SmartConnector, but leave it un-configured.
3. Create a file called **agent.properties** in the directory `$ARCSIGHT_HOME/current/user/agent`, where `$ARCSIGHT_HOME` is the root directory where the SmartConnector component was installed. This file should contain a single line:

   ```
   transport.default.type=cefsyslog
   ```
4. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
5. Specify the required parameters for CEF output. Enter the desired port for UDP or TCP output. These settings will need to match the receiver you create in Logger to listen for events from ArcSight ESM.

   | Parameter | Description |
   |---|---|
   | IP/Host | IP or host name of the Logger |
   | Port | 514 or another port that matches the receiver |
   | Protocol | UDP or Raw TCP |
   | ArcSight Source Manager Host Name | IP or host name of the source ArcSight Manager |
   | ArcSight Source Manager Port | 8443 (default) |

| Parameter | Description |
|---|---|
| ArcSight Source Manager User Name | A user account on the source Manager with sufficient privileges to read events |
| ArcSight Source Manager Password | Password for the specified Manager user account |
| SmartConnector Name | A name for the ESM to Logger connector (visible in the Manager) |
| SmartConnector Location | Notation of where this connector is installed |
| Device Location | Notation of where the source Manager is installed |
| Comment | Optional comments |

To configure the Forwarding SmartConnector to send CEF output to Logger and send events to another ArcSight Manager at the same time, see "Configuring SmartConnectors to Send Events to Both Logger and an ArcSight Manager" on page 64.

# Chapter 7: Alerts

You can configure your Logger to alert you by e-mail, an SNMP trap, or a Syslog message when a new event that matches a specific query is received or when a specified number of matches occur within a given time threshold.

You can also view the alerts through the **Alert** sub-menu under the Analyze tab. When an alert is triggered, Logger creates an alert event and sends a notification to the destinations you configured previously.

## Types of Alerts

Logger provides two types of alerts:

- Real time alerts
- Saved Search Alerts

The following table compares the two types of alerts.

| Real Time Alerts | Saved Search Alerts |
|---|---|
| No limit on the number of alerts that can be defined.<br>A maximum of 25 alerts can be enabled at any time. | Any number of alerts can be defined. All defined alerts are enabled and effective; however, a maximum of 50 alerts can run concurrently. |
| No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination. | No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination. |
| Alerts are triggered in real time. That is, when specified number of matches occurs within the specified threshold, an alert is **immediately** triggered. | These alerts are triggered at scheduled intervals. That is, when a specified number of matches occurs within the specified threshold, an alert is triggered **at the next scheduled time interval**. |
| Only regular expression queries can be specified for these alerts. | Queries for these alerts are defined using the flow-based search language that allows you to specify multiple search commands in a pipeline format, including regular expressions. Aggregation operators such as chart and top cannot be included in the search query. |
| To define a real time alert, you specify a query, match count, threshold, and one or more destinations.<br>A time range is not associated with the queries defined for these alerts. Therefore, whenever the specified number of matches occurs within the specified threshold, an alert is triggered. | To define a Saved Search Alert, you specify a Saved Search (which is a query with a time range), match count, threshold, and one or more destinations.<br>A time range (within which events should be searched) is specified for the query associated with these alerts. Therefore, specified number of matches within the |

| Real Time Alerts | Saved Search Alerts |
|---|---|
| | specified threshold (in minutes) must occur within the specified time range. You can also use dynamic time range (for example, `$Now-1d`, `$Now`, and so on).<br>For example, if a Saved Search query has these start and end times:<br>Start Time: `5/11/2016 10:38:04`<br>End Time: `5/12/2016 10:38:04`<br>And, the number of matches and threshold are the following:<br>Match Count: `5`<br>Threshold: `3600`<br>An alert will trigger if five or more events occur in one hour anytime between May 11th, 2016 10:38:04 a.m. and May 12th, 2016 10:38:04 a.m. |

## Configuring Alerts

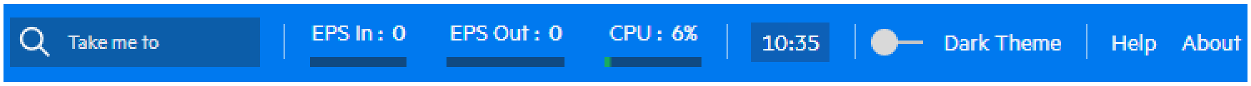
Refer to the ArcSight Logger 7.3  Administrator’s Guide for detailed instructions on how to create both types of alerts.

# Chapter 8: Overview of the Logger User Interface

This section provides a high-level view of the Logger User Interface, with an emphasis on the Search interface. For more information and for user interface options not discussed in this section, refer to the ArcSight Logger 7.3  Administrator's Guide.

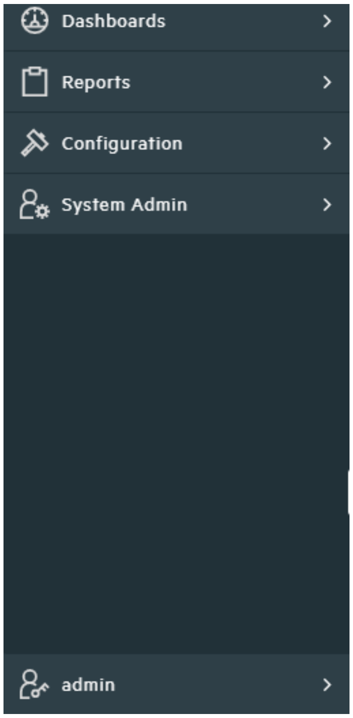
## Navigating the User Interface

An information band runs across the top of every page in the user interface. It contains a quick navigation field, events gauges, system clock, Help, and About.



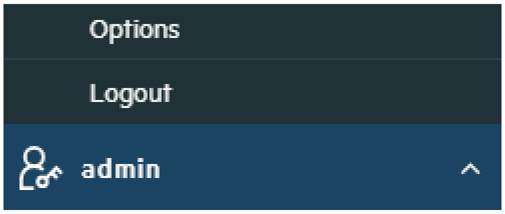
Bar gauges at the top of the screen provide an indication of the throughput and CPU usage information available in more detail on the Monitor Dashboard ("Dashboards" on page 74). You can change the range of the bar gauges on the Options page. The name of the logged-in user is shown below the clock, to the right of the gauges.

To access any Logger function, click the navigation bar located at left side of the page. You can also expand/ collapse the navigation bar by clicking the icon if needed.



## Current User and Logout

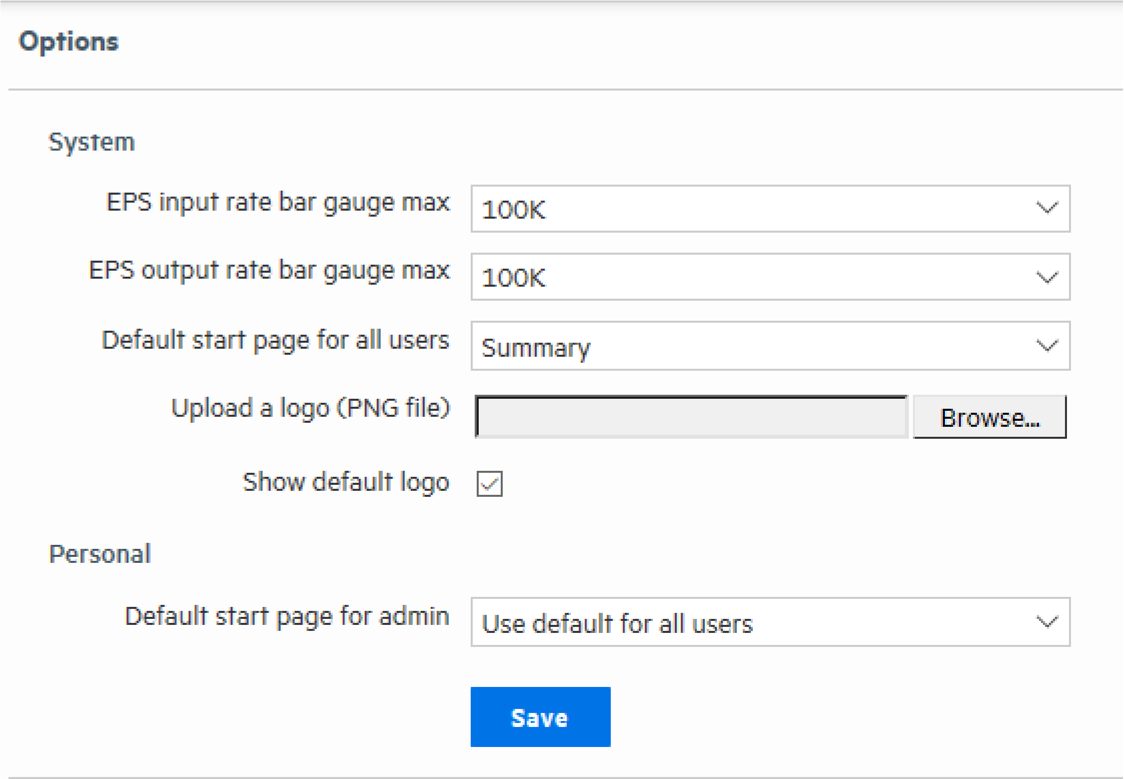
From the **navigation bar > admin** icon , click the Logout link.



Logging out is good security practice, to eliminate the chance of unauthorized use of an unattended Logger session. Logger automatically logs you out after a user-configurable length of time (15 minutes by default). For more information on how to update the logout time, see the ArcSight Logger 7.3  Administrator's Guide.

## Options Page

From the **navigation bar > admin** icon , click the Options link. The Options page allows to admin rights users to set the range on the EPS In and EPS Out bar gauges. If the event rate exceeds the specified maximum, the range is automatically increased.



Options

System

| | |
|---|---|
| EPS input rate bar gauge max | 100K |
| EPS output rate bar gauge max | 100K |
| Default start page for all users | Summary |
| Upload a logo (PNG file) | Browse... |
| Show default logo | ☑ |

Personal

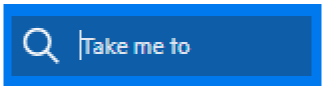
| | |
|---|---|
| Default start page for admin | Use default for all users |

From here, you can **Upload a logo (PNG file)** and replace the ArcSight Logger logo with your custom logo. The logo must be in .png format. The recommended size is 175 x 50 pixeles and the maximum file size is 1 MB.

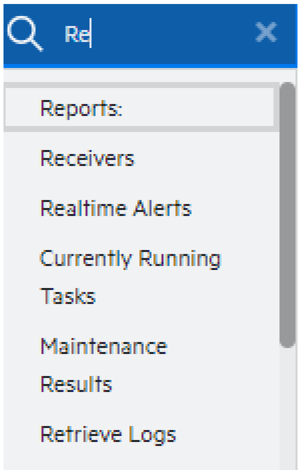
Additionally, you can set the default start page (home page) for all users and specific start pages for individual users here. The start page is the user interface page Logger displays when a user logs in.

## Take Me To and Server Clock

To the right of the menu tabs, the **Take me to...** navigation box provides a quick and easy way to navigate to any location in the user interface (UI). The Take me to... feature enables you to navigate to any Logger feature simply by starting to type the feature's name.



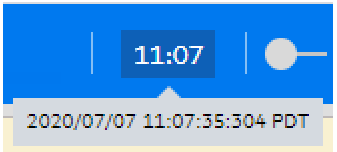
You can access the **Take me to...** navigation box by clicking it or pressing the `Alt+o`, `Alt+p`, or `Ctrl+Shift +o` hot keys. In the navigation box, type a word to display a list menu of matching results. To select a particular option, use the arrow keys and then press enter.



**Note:** You can also open the online help for your current UI page by typing `help` in the **Take me to...**search box.

### Server Clock

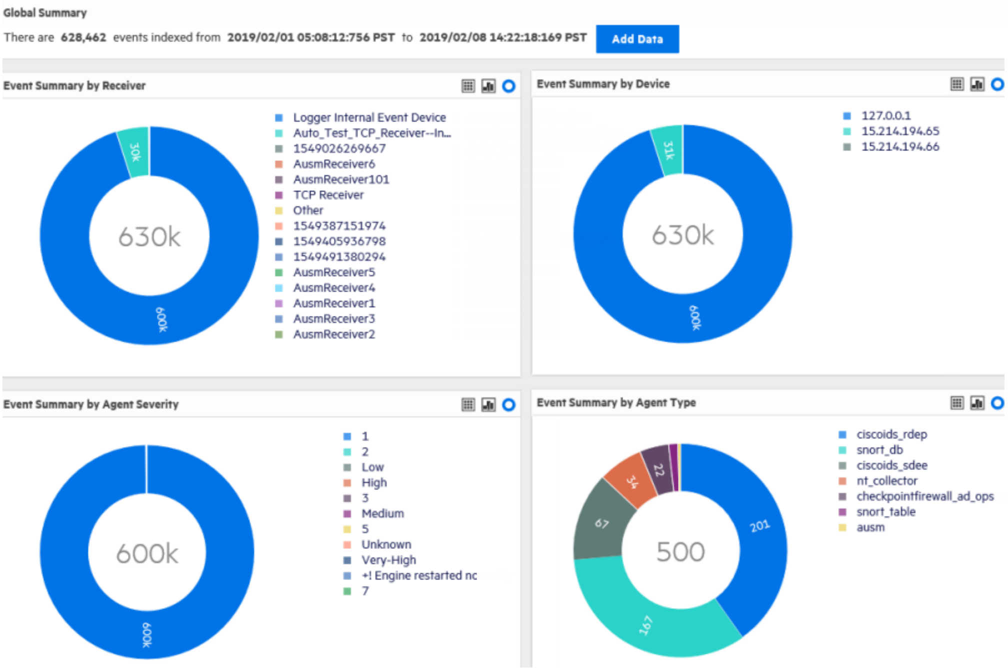
The server clock is shown to the right of the bar gauges, along with the dark theme, help and about.



The server clock displays the Logger server's system time. This may be different from the user's local time.

## Summary

The Summary page is a global dashboard that provides summarized event information about your Logger in one screen. It enables you to gauge incoming events activity and the status of indexing.



Global Summary

There are 628,462 events indexed from 2019/02/01 05:08:12:756 PST to 2019/02/08 14:22:18:169 PST

## Dashboards

Dashboards are an all-in-one view of the Logger information of interest. You can assemble various search queries that match events of interest to you, status of Logger components such as receivers, forwarders, storage, CPU, and disk, or a combination of both on a single dashboard.

Each Dashboard contains one or more panels of these types: Search Results and Monitor. The Search Results panels display events that match the query associated with the panel. The Monitor panels display the real-time and historical status of various Logger components such as receivers, forwarders, storage, CPU, and disk.

For more details about Dashboards, refer to the ArcSight Logger 7.3  Administrator’s Guide.

# Chapter 9: Searching for Events

Once Logger has stored events from heterogeneous sources on your network, you can search through those events for a wide array of uses such as unsuccessful login attempts, the number of events by source, SSH authentications. Additionally, you might want to include matching events in a report, or forward events to another system such as ArcSight ESM.

You need to create queries to search for events. Queries can be as simple as a term to match, such as “login” or an IP address; or they can be more complex, such as events that include multiple IP addresses, ports, and occurred between specific time ranges from devices that belong to a specific device group.

Searching through stored events is very simple and intuitive on Logger. It uses a flow-based search language that allows you to specify multiple search commands in a pipeline format. In addition, you can customize the display of search results, view search results as charts, and so on.

For detailed information of syntax and tools of queries, exporting and saving query results refer to the ArcSight Logger 7.3  Administrator’s Guide.

## Example Queries

Simple query examples:

- `error`
- `sourceAddress=192.0.2.0`
- `hostA.companyxyz.com`

Complex query example:

```
_storageGroup IN ["Default Storage Group"] _deviceGroup IN ["192.168.22.120
[TCPC]"] name="*[4924TestAlert]*" AND ("192.168.*" OR categoryBehavior
CONTAINS Stop) | REGEX=":\d31" | cef name deviceEventCategory | chart _count
by name
```

# Syntax of a Query

A Logger search query contains one or more of the following types of expressions:

<table>
<tr><th>Query Element</th><th>Description</th></tr>
<tr><td>Keyword expression</td><td>A keyword: a word expressed in plain text; for example:<br>warning<br>failed<br>login</td></tr>
<tr><td>Field-based expression</td><td>A field-based expression: searching for values in the fields of an event. This includes searches for uncommon values in specific fields; for example:<br>name="failed login"<br>message!="failed login"<br>sourceAddress=192.0.2.0</td></tr>
<tr><td>Search operator expression</td><td>A search operator expression: an expression that uses search operators to refine the data that matches the expressions specified by the keyword and the field-based expression.<br>The following search operators are available in Logger 7.3:<br>cef, chart, dedup, eval, extract, fields, head, keys, rare, regex, rename, replace, rex, sort, tail, top, transaction, where</td></tr>
<tr><td>Extraction operator expression</td><td>The rex search operator is useful for syslog events (raw or unstructured data) or if you want to extract information from a specific point in an event, such as the 15th character in an event.<br>For example, to extract an IP address from the following event:<br>[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP Warning: Can't connect to 10.4.31.4:11211<br>and assign it to a field called “IP_Address”, use the following rex expression:<br>| rex "(?<IPAddress>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"</td></tr>
<tr><td>Implied field extraction operator</td><td>You can specify the event fields directly in queries; for example:.<br>To display search results of the count of unique values device addresses in a chart form:<br>failed | chart _count by deviceAddress<br>To display search results of the most common values for the deviceAddress field in table form. That is, the values are listed in order from the highest number of matches to the lowest.<br>failed | top deviceAddress</td></tr>
</table>

# Building a Query

When you build a query, you must specify the following elements:

- **Query Expression**: the search conditions to use when selecting or rejecting an event.
- **Time range**: the time range within which to search.
- **Field Set**: the fields of an event to display for matching events; for example, you can select to display only the `deviceAddress` and `deviceReceiptTime` fields of matching events.

In addition, you can also include constraints that limit the search to specific device groups and storage groups.

- A Storage Group enables you to associate a retention policy with it. Therefore, by defining multiple storage groups, you can store events for different periods of time.
- A Device Group enables you to categorize devices of your choice into a group. You can associate a device group to a storage rule that defines in which storage group events from a specific device group are stored.

# Query Building Tools

Logger offers the following tools to assist you in building queries that are complex:

- Regex Helper

  Creating a regular expression for the `rex` extraction operator can be complex and error prone. The Regex Helper tool enables you to create regular expressions to use with the `rex` pipeline operator to extract fields of interest from an event. This tool not only simplifies the task of creating regular expressions for the `rex` operator but also makes it efficient and error free.
- Search Helper

  Search Helper is a search-specific utility that provides the following features:

  - **Search History**: Displays the recently run queries on Logger, thus enabling you to select and reuse previously run queries without typing them again.
  - **Search Operator History**: Displays the fields used previously with the search operator you have entered in the Search text box.
  - **Examples**: Lists examples relevant to the latest query operator you entered.
  - **Suggested Next Operators**: List of operators that generally follow the current query. For example, if you type `logger`, the operators that often follow are `rex`, `extract`, or `regex`.
  - **Help**: Provides context-sensitive help for the last-listed operator in your query.

- ○ **List of Fields and Operators**: Depending on the query you enter, Logger displays either a complete list of fields that possibly match the field name you are typing, or a list of available operators.

## Exporting Search Results

You can export search results in these formats:

- PDF: Useful in generating a quick report of the search results. The report includes a table of search results and any charts generated for the results. Both raw and CEF events can be included in the exported report.
- Comma-separated values (CSV) file: Useful for further analysis with other software applications. The report includes a table of search results. Charts cannot be included in this format.

## Saving Queries for Later Use

If you need to run the same query regularly, you can save it in several ways:

- Filter: Saves the query expression, but not the time range or field set information.
- Dashboard Panel: Saves dashboards using a search query that generates a chart.
- Search Result: Saves the results of a large search.
- Saved Search: Saves the query expression, the time range, and local only value.

## System Filters (Predefined Filters)

Your Logger ships with a number of predefined filters, also known as system filters. These filters define queries for commonly searched events such as unsuccessful login attempts or the number of events by source.

## Tuning Search Performance

Search performance depends on many factors and will vary from query to query. Some factors that can affect search performance are listed below.

To optimize search performance, ensure that you follow these recommendations:

- Take advantage of super indexes where possible, for the fastest search results. Refer to the ArcSight Logger 7.3  Administrator’s Guide for more information on how to search super-indexed fields.

- The amount of time it takes to search depends on the size of the data set that must be searched, the complexity of the query, and whether the search is distributed across peers. To limit the data set, ensure that time range you specify does not result in a query that needs to scan multimillions of events.
- Limiting search to specific storage groups or peers typically results in better search performance than when the storage groups or peers are not specified.
- If your receive syntax error when running a query, ensure that the syntax of the query follows the requirements specified in the **Syntax Reference for Query Expression** section of the ArcSight Logger 7.3  Administrator's Guide.
- Reduce the load on the system when your query needs to run, for example, scheduled jobs, running multiple reports, or large number of incoming events.

✓ **Tip:** Full-text indexing and Field-based indexing for a recommended set of fields are automatically enabled at Logger initialization time. In addition to these fields, Micro Focus strongly recommends that you index fields that you will be using in search and report queries.

# Chapter 10: Other Logger Features

In addition to the Logger features highlighted in this guide, Logger provides many other features. This section provides an overview of some of those features. For an in-depth understanding and how to use Logger, refer to the ArcSight Logger 7.3  Administrator’s Guide and ArcSight Logger Web Services API Guide.

## Scheduling Tasks

You can configure Logger to run jobs such as Configuration Backup, Event Archive, File Transfers, and Saved Searches on recurring basis.

## Archiving Events

Event Archives let you save the events for any day in the past, not including the current day. The archive location can be a local directory or a mount point that you have already established on the system on which Logger software is installed. You can also schedule a daily archive of the events. Archives are indexed at the creation; this will enable searches on archived events to be as fast as searches in live storage.

## Access Control on Logger Users

You can create users with different access privileges on Logger. For example, you create Joe with only Logger search privileges and give Jane Logger search and administration capabilities.

## Enriching Data Through Static Correlation

The Lookup feature enables you to augment data in Logger with data from an external file, and display this data in the Search results. This enables geo-tagging, asset tagging, user identification, and so on, through static correlation. For example, if you want the search results to include which country source IP addresses are located in, you can create a file listing the IP addresses and countries and then upload that file to Logger as a Lookup file. After that, you can use the `lookup` search operator to correlate the sourceAddress field in the events and the IP address column in the Lookup file, and display the country in the search results.

# Web Services

Logger includes SOAP and REST web services that you can use to integrate Logger functionality in your own applications. For example, you will be able to create programs that execute searches on stored Logger events or run Logger reports, and feed them back to your third-party system. Refer to the Logger Web Services API Guide. for more information on this feature.

# Publication Status

Released: May 31, 2023

Updated: Wednesday, March 20, 2024

# 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 ArcSight Logger Installation (Logger 7.3)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!