Installation Guide

ArcSight Logger 6.0

September 23, 2014

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
09/23/2014	6.0	Correction for Logger 6.0 release.
09/11/2014	6.0	New guide for Logger 6.0 release.

Contents

About this Guide

This guide describes how to install and initialize the enterprise version of Logger. It includes information on how to initialize the Logger Appliance and how to install the Software Logger on Linux and on VMware VM. For information on installing Trial Loggers, refer to the Quick Start Guide for ArcSight Logger 6.0, which is available from the same location you download the Trial Logger installation file.

This guide includes information on the following subjects.

Chapter 1

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:

Storage Strategy

Logger events can be stored locally on any Logger, and remotely on Logger Appliance models that support Storage Area Network (SAN). The SAN should be available before you bring the Logger online.

A SAN can be used for storing events on both types of Loggers; however, only one LUN can be used for storing events. On Software Loggers, the LUN (Logical Unit Number) must be mapped to the `<install_dir>/data/` directory on the system on which the Logger software is installed.

The Logger Appliance can interact with Network Attached Storage (NAS) or with a Storage Area Network (SAN) using a SAN gateway. On Logger Appliance models that support a Storage Area Network (SAN), you need to use the SAN for storage. Using a Network File System (NFS) as primary storage for events on a Logger Appliance is not recommended.

On Software Loggers, you need to have at least the minimum disk space described in the Release Notes to store events. The disk space needs to be on the partition where the `<install_dir>` directory exists. Specifically, most of this space should be available for the `<install_dir>/data/logger` directory. Using a Network File System (NFS) as primary storage for events is not recommended for Software Loggers. However, you can use an NFS as secondary storage for archiving data.

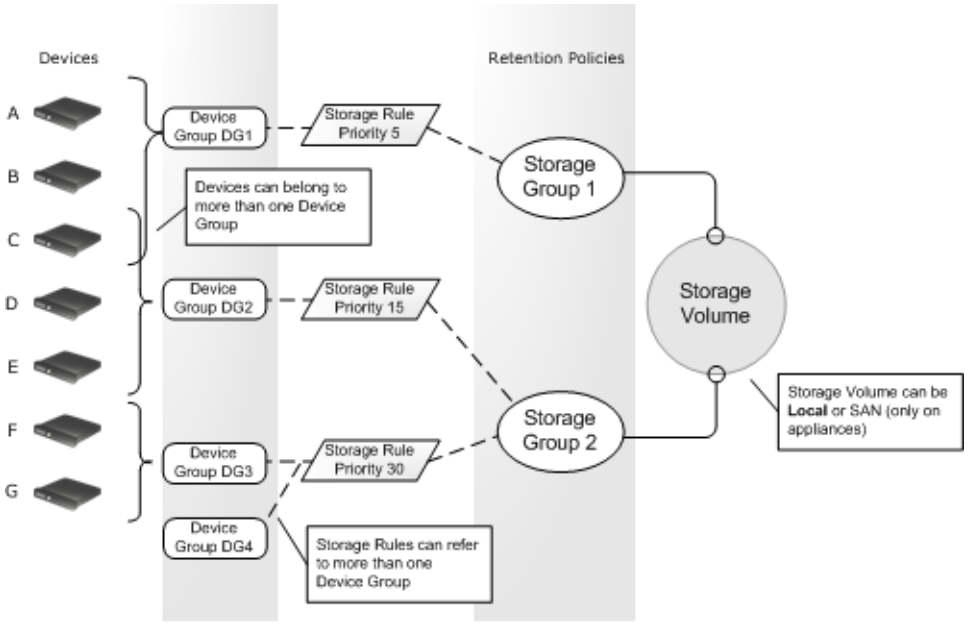
An NFS or a CIFS system can be used for archiving Logger data such as event archives, Saved Searches, exported filters and alerts, and configuration backup information on all Loggers. You can also configure the Logger to read event data or log files from a CIFS host.

The storage volume, either external or local, can be divided into multiple storage groups, each with a separate retention policy. Two storage groups are created when Logger is first configured. New storage groups can be added later, a storage group's size can be increased or decreased, and the retention policy defined for it can be changed. For more information on event storage, refer to the Logger Administrator's Guide.

Retention Policy

Logger supports several storage groups, each of which can have a different retention policy. Retention policy is specified in terms of number of days that events are stored, or overall maximum size (in GB). Events from specific IP addresses can be routed to particular storage groups, making it possible to store all router events, for example, to a storage group with short retention, and business-critical host events to another storage group with a longer retention. The Logger receipt time of an event is used to determine the starting time for its retention period.

Before installing and initializing Logger, you should have an idea of your various retention policy needs, both initially and over the life span of the Logger installation.



The previous figure illustrates the relationship between ArcSight components and retention policies.

- Devices, on the left, are grouped by device groups.
- Storage groups implement different retention policies on the storage volume.
- Storage rules, in the middle, create a mapping between device groups and storage groups.

In the example shown, Device C is a member of both Device Group 1 and Device Group 2. Storage rules are defined that send Device Group 1 events to Storage Group 1 and Device Group 2 events to Storage Group 2. There is no ambiguity, however, because each storage rule has a unique priority value, and the lower value has the higher priority. In the example, events from Device C are stored in Storage Group 1 because that storage rule has a priority of 5, which is lower than the other matching storage rule, which has a priority of 15.

An implicit storage rule, with lowest priority, maps all devices to the Default Storage Group.

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 49 and refer to the Logger Administrator's guide.

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

SAN

This section only applies to SAN-enabled appliance models.

If you are using a SAN as your primary storage for a Logger Appliance, the SAN must be set up before initializing the Logger.

By default, the HBA card on your SAN Logger has two ports. You can connect both of those ports to the same LUN for multipathing, or, alternatively, use one port for primary storage and the other for an additional LUN for event archival, configuration backup, and export. Logger can attach to only one LUN at a time for primary storage.

When you multipath a LUN, you create two different network paths to it from Logger. Doing so reduces the possibility of a single point of failure causing the LUN to become unavailable. Refer to the System Admin-Logger Appliance chapter of the Logger Administrator's Guide for detailed information about connecting the LUN and multipathing.

Storage Volume

Logger's storage volume varies by version, up to the maximum of 8 TB. The initialization process sets the storage volume. For Logger appliances, the storage volume is set to the maximum capacity for the model. For software Loggers, the storage volume is set to the maximum capacity specified in the license or the available disk space, whichever is smaller.

If Logger's maximum capacity is exceeded, events will begin to fall out of storage. For information on how to retain these events, refer to the Configuration chapter of the Logger Administrator's Guide.

After installing Logger, you can view the current limits on the **Configuration | Advanced > License Information** page. For instructions, refer to the Configuration chapter of the Logger Administrator's Guide. For more information about licenses, including how to upload a new one, refer to the System Admin-Logger Appliance or System Admin-Software Logger chapters of the Logger Administrator's Guide.

Storage volume can be extended after installation, but not reduced. For more information on increasing the storage volume, refer to the Configuration chapter of the Logger 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:

Table 1-1 Preconfigured Default Storage Group Settings

Attribute	Appliance Logger	Software Logger
Size	Storage Volume/2	Storage Volume/2
Retention Period	180 days	180 days

Table 1-2 Preconfigured Internal Storage Group Settings

Attribute	Appliance Logger	Software Logger
Size	5 GB	3 GB
Retention Period	365 days	365 days

Logger can have a maximum of six storage groups; therefore, you can create an additional four storage groups after your Logger has been initialized. 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. Refer to the Configuration chapter of the Logger Administrator's Guide for the details of adding and resizing storage groups, and changing their retention policies.

Indexed Fields and Full-text Indexing

Frequently used fields are indexed during initialization. You can add additional fields to the index, but once a field has been added, you cannot unindex it. Logger comes prepared for full-text indexing. Refer to the Search chapter of the Logger Administrator's Guide for more information.

Receivers

The default installation includes several receivers. To start receiving events, you can direct your event sources to the default receivers. After initialization, you can create additional receivers to listen for events. You can also change and delete receivers or disable and enable them as needed.

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 for Logger Appliances. If you are installing Software Logger as root, the UDP receiver is on port 514. For non-root installs, it is on port 8514. If this port is already occupied, the initialization process selects the next higher unoccupied port. This port should be allowed through any firewall rules you have configured.
- A TCP receiver: Enabled by default. The TCP receiver is on port 515 for Logger Appliances. If you are installing Software Logger as root, the TCP receiver is on port 515. For non-root installs, it is on port 8515. If this port is already occupied, the

initialization process selects the next higher unoccupied port. This port should be allowed through any firewall rules you have configured.

- 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.

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.

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`

The folder follower receiver for the `/var/log/audit/audit.log` is only created if the folder `/var/log/audit/` already exists on your system at installation time.

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

When auditing is disabled on the system where Logger is installed, the preconfigured 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 preconfigured receivers, see "Receivers" on page 49.

For more information about receivers in general, refer to the Configuration chapter of the Logger Administrator's Guide.

Chapter 2

Initializing a Logger Appliance

This chapter describes how to configure the initial settings for your Logger Appliance. It assumes that you have already rack mounted and configured an IP address for your appliance, as described in Getting Started with the ArcSight Logger Appliance, included in the shipment with your Logger Appliance.

You do not need to run an installer when setting up your appliance; the Logger software comes preinstalled 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 21. For information about installing Software Logger on VMware VM, see, "Installing Software Logger on VMware" on page 37. For information about installing Trial Logger on Linux or on VMware VM, refer to the Trial Logger Quick Start guide.

Acquiring a License for the Logger Appliance

Starting with Logger 5.5, licenses for all Logger types are based on Daily Data (the amount of data that comes into Logger per day). The Daily Data value is monitored and enforced on software Loggers; however, currently, this value is not enforced on Logger appliances. Logger uses the sum of the sizes of the events received each day to determine this value.

For software Loggers, you can increase your Daily Data limit by purchasing a higher ingestion rate in increments of 5 GB/day. While you can purchase a higher ingestion rate for software Loggers, Logger appliances come preset with the maximum ingestion capacity of the model. Therefore, the ingestion capacity of Logger appliances cannot be upgraded.

A valid license file is required on the Logger Appliance before you can access its functionality. If you have not obtained a license yet, follow instructions in "Hewlett-Packard Entitlement Certificate" document included in the shipment with your Logger Appliance to

redeem your license key. If you do not have that document, contact customer support at http://support.openview.hp.com.

If you have multiple Loggers, you will need a separate license file for each of them.

After initializing Logger, you can view the specific details of the current license on the License Information and License & Update pages (**Configuration | Advanced > License Information and System Administration | System > License & Update**). For more information, refer to the Configuration and System Admin-Logger Appliance chapters of the Logger Administrator's Guide.

Logging In and Accepting the License Agreement

The Logger user interface (UI) is a web browser application using Secure Sockets Layer (SSL) encryption. Users must log in and be authenticated before they can access the Logger UI.

Logger 6.0 supports access through the following browsers:

- **Firefox:** Version ESR 31
- **Internet Explorer:** Versions 10 and 11
- **Chrome**: Latest version
- **Safari:** version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at http://www.adobe.com/products/flashplayer.html

JavaScript and cookies must be enabled.

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

For root installs, access to the port 443 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.

For non-root installs, access to port 9000 must be allowed, plus the ports for any protocol that the Logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.

The ports listed here are the default ports. Your Logger may use different ports.

The first time you connect to the appliance through a browser, the End User License Agreement (EULA) is displayed. Before you can log in and initialize the appliance, you must review and accept the EULA.

To accept the EULA and log in:

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

```
https://<hostname or IP address> for the Logger Appliance>
```

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

The **END USER LICENSE AGREEMENT** is displayed.

2 Review and accept the EULA. After you accept, the Login screen is displayed.

3 Enter your user name and password, and click Login. Use the following default credentials if you are connecting for the first time or have not yet changed the default credentials:

Username: admin
Password: password

4 Once you have successfully logged in, proceed to the section, "Initializing the Logger Appliance" on page 15.

Caution For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time. Refer to the appropriate System Administration chapter of the Logger Administrator's Guide for instructions.

For more information about the log in screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator's Guide.

Initializing the Logger Appliance

After you accept the EULA and log in for the first time, the Logger Configuration screen is displayed. On this screen, you must 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.

The initialization of a Logger Appliance can only be changed by performing a factory reset. Refer to the Logger Administrator's Guide for more information.

To initialize the Logger Appliance:

1. On the **Logger Configuration** screen, under **Select License File to Upload**, navigate to or specify the path and filename of the license for the Logger Appliance, and click **Upload License**. If you do not have a license, see "Acquiring a License for the Logger Appliance" on page 13.

   After the upload, the License pane displays updated license status information.

2. Under **System Locale Setting**, select a **Locale** for this Logger Appliance from the 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. Under **Date/Time Settings**, ensure that the "Current Time Zone" and the "Current Time" settings are correct for your environment.

   Click **Change Time Zone** and **Change Date/Time**, respectively, to update the time settings. For more information, refer to the System Admin-Logger Appliance chapter of the Logger Administrator's Guide.

4. Save your changes.

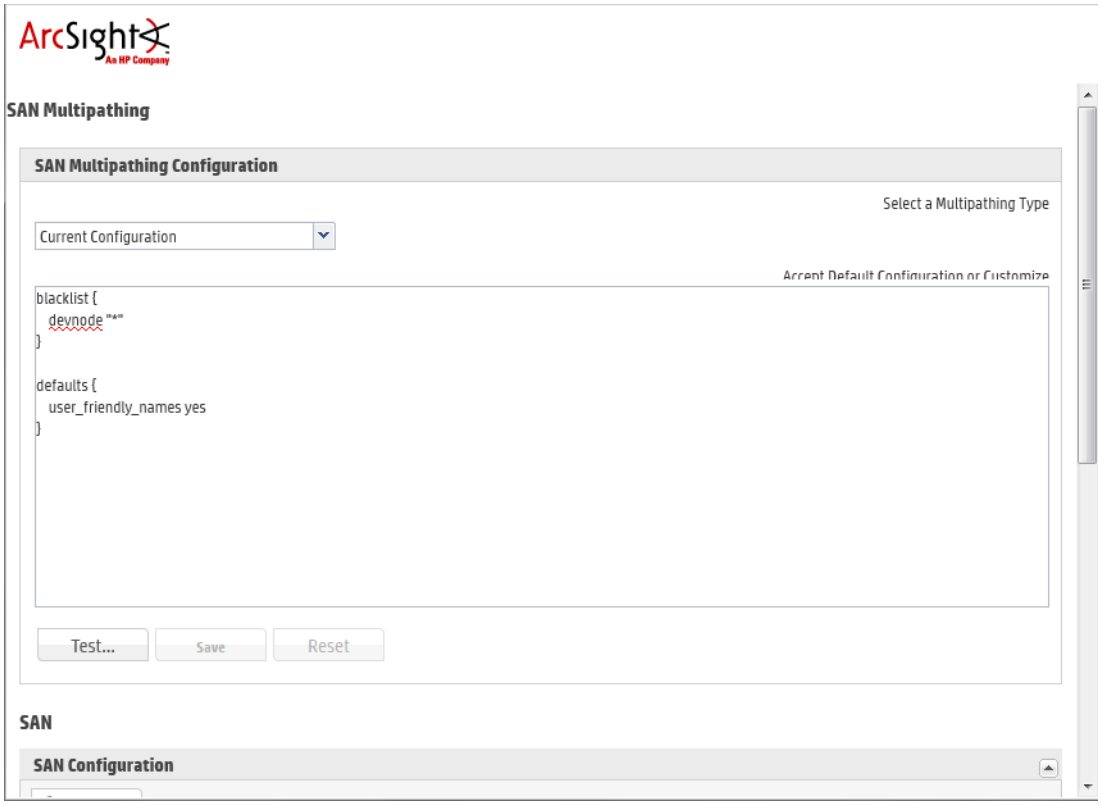
   - For non-SAN models, click **Save**.

     The Logger initialization process begins. Once the initialization is complete, the system reboots.

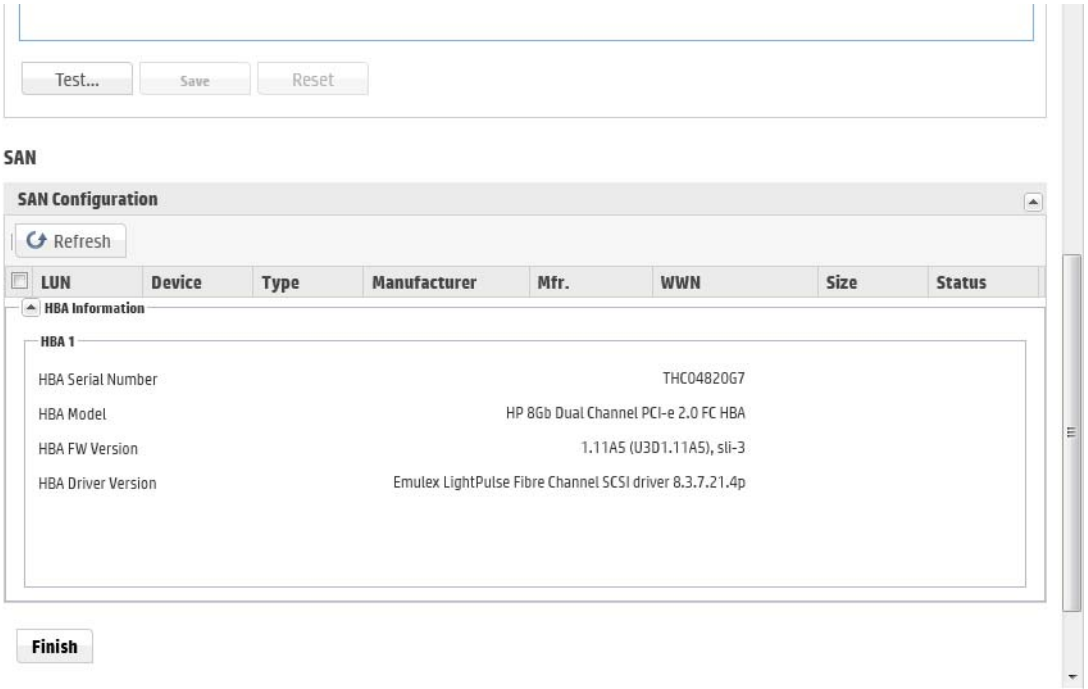
     Now that you are done installing and initializing your Logger, go to the section, "Configuring Logger" on page 49 for information on how to set up your Logger to start receiving events.

   - For **SAN models,** click **Save and Configure SAN**. Refer to the System Admin-Logger Appliance chapter of the Logger Administrator's Guide for more information about connecting LUN and multipathing.
   - The SAN Multipathing Configuration screen is displayed. This screen has two panes.

     The upper pane, SAN Multipathing Configuration, displays multipathing information.



The lower pane, SAN Configuration, displays the currently attached or connected LUN or LUNs.



5 If you plan to use a single path, proceed to Step 7 on page 18.

6 If you plan to multipath, follow these steps to configure multipathing on Logger.

Note

If your SAN environment is set up to use multipathing, you must configure multipathing on the Logger.

a Scroll up to the SAN Multipathing pane and select a type from the **Select a Multipathing Type** drop-down list.

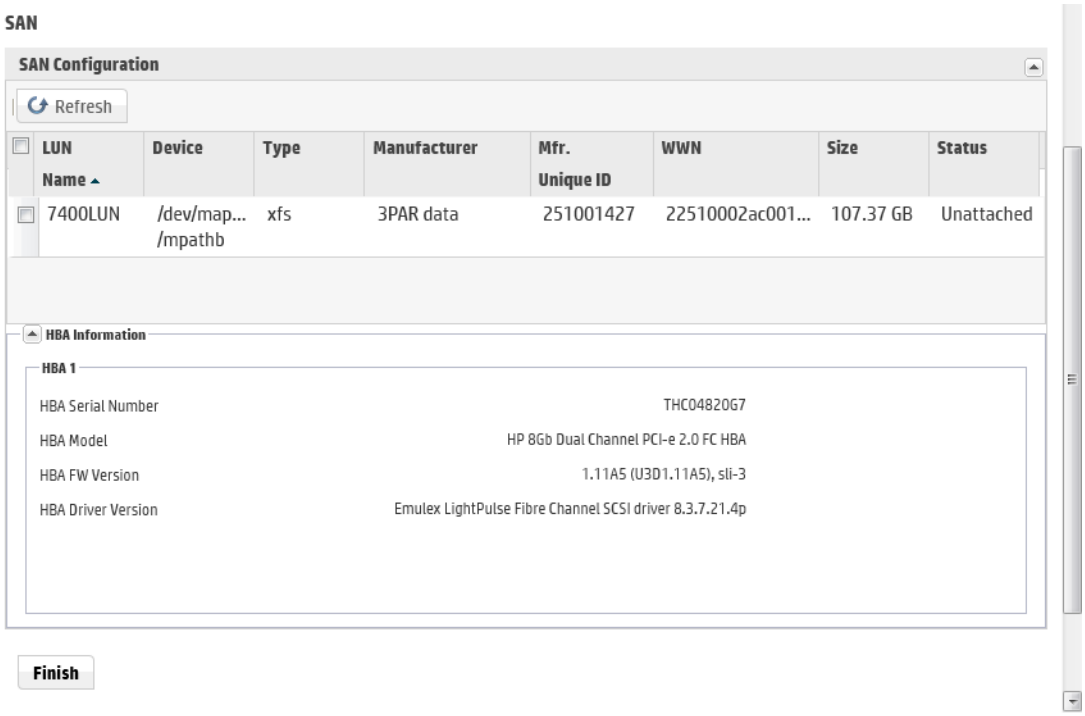
b Click **Test** to review your configuration. You cannot change the configuration once it has been saved. Be sure to review it carefully.

c The test screen displays the routes that are currently recognized and will be multipathed if you save. When you are done reviewing the configuration, click **Close**.

d You can accept the default configuration or customize it. Once you are satisfied with the configuration, click **Save**, and then click **OK**.

e Click **Refresh** from the top left of the SAN Configuration pane.

The multipathed device is displayed on the SAN Configuration pane.



7 Select the device's checkbox in the SAN Configuration pane. The **Attach** button is displayed.

Note

Storage volume can be extended but the size of a LUN cannot be changed after it has been attached to the Logger.

For more information, refer to the Configuration chapter of the Logger Administrator's Guide.

8 Click **Attach** from the top left of the SAN Configuration pane.

If no LUNs are available to attach, consult your SAN administrator to have storage allocated for the Logger.

9 Enter a mount name for the selected LUN and click **OK**. The LUNs Attachment Status will change to “Attached” when the LUN is ready for use.

10 Click **Finish**.

The Logger initialization process begins. Once the initialization is complete, the system reboots.

When you configure multipath SAN connectivity to the appliance, you must also make sure that the multipathd service is configured to start on boot.

11 Now that you are done installing and initializing your Logger, you can connect, log in, and start configuring your Logger to receive events. Go to the section, “Configuring Logger” on page 49 for information on how to set up your Logger to start receiving events.

For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time. Refer to the appropriate System Administration chapter of the Logger Administrator’s Guide for instructions.

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

Setting Up the Logger Appliance for Remote Access

HP strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you (and customer support, with your permission and assistance) can remotely access your appliance's console for troubleshooting, maintenance, and power control.

All ArcSight appliances are equipped with an HP ProLiant Integrated Lights-Out (iLO) Advanced remote management card. The Lx500 models require you to obtain and enter a license key. Instructions for obtaining the license key are included on your License Entitlement Certificate. Once you have obtained the license key, log into iLO, and then go to **Administration > Licensing** to enter it.

Follow the directions in the HP ProLiant Integrated Lights-Out User Guide to set up your appliance for remote access. The guide is available at http://www.hp.com/go/iLO.

Chapter 3

Installing Software Logger on Linux

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 Linux system. It includes information on the following topics:

For information about installing Software Logger on VMware VM, see, "Installing Software Logger on VMware" on page 37. For initialization information about the Logger Appliance, see "Initializing a Logger Appliance" on page 13. For information about installing Trial Logger on Linux or on VMware VM, refer to the Trial Logger Quick Start guide.

Before You Begin

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

Downloading the Installation Package

The installation package is available for download from the HP Software Depot at http://software.hp.com.

Verifying the Downloaded Installation Software

HP provides code signing to enable you to verify that the software you have received is indeed from HP and has not been manipulated in any way by a third party. To do this, the software has been signed with a digital private key only held by HP.

Access the following link to download HP's public certificate:

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

This site also provides the step-by-step instructions for how to import HP's public certificate and verify the signature file.

How Licensing Works in Software Logger

Starting with Logger 5.5, licenses for all Logger types are based on Daily Data (the amount of data that comes into Logger per day). The Daily Data value is monitored and enforced on Software Loggers; however, currently, this value is not enforced on Logger appliances. Logger uses the sum of the sizes of the events received each day to determine this value.

For Software Loggers, you can increase your Daily Data limit by purchasing a higher ingestion rate in increments of 5 GB/day. While you can purchase a higher ingestion rate for Software Loggers, Logger appliances come preset with the maximum ingestion capacity of the model. Therefore, the ingestion capacity of Logger appliances cannot be upgraded.

See "Acquiring a License for a Software Logger" on page 23 for information about licensing your Software Logger.

If you are using ArcSight Connectors to send events to the Software Logger, make sure you are running connector version 5.1.3.5870.0 or later on your connectors to ensure that event size is accurately accounted on the Logger.

Even if this limit is exceeded, the Logger continues to collect and store events; therefore, no events are lost. However, if the limit is exceeded on more than five days in a 30-day sliding window, all features involving search are disabled.

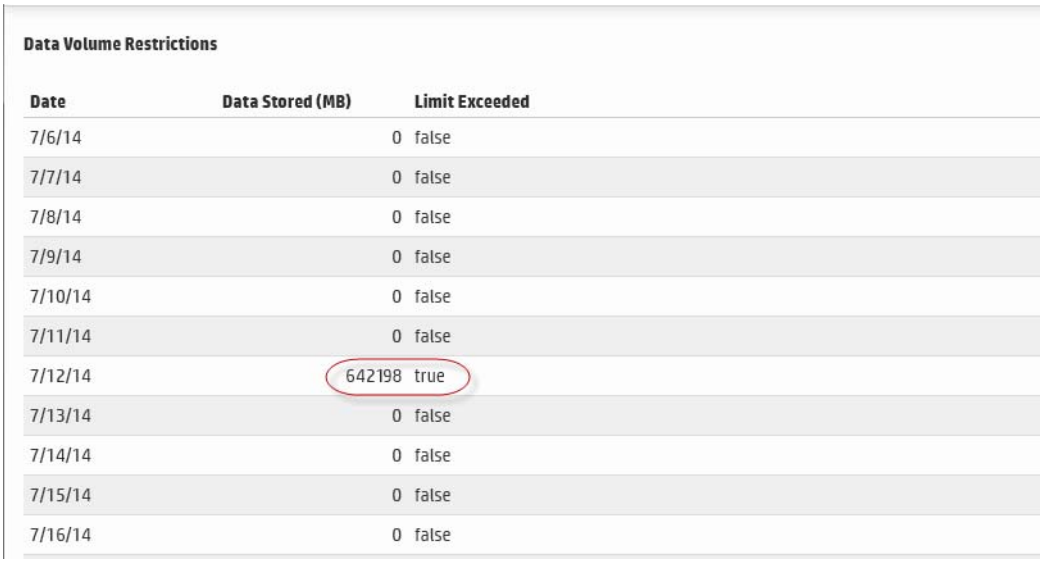
The disabled search features include forwarders as well as all searching and reporting functionality.

If this limit is exceeded six or more times (any six days or more days) in a given 30-day period, you cannot forward, search, or run reports on the collected events until the 30-day sliding window contains five or less data limit violations.

For example, you install the Logger software on January 1 with a data storage limit of 20 GB and start collecting events. Your Logger receives more than 20 GB of event data on these dates: January 5th, 13th, 18th, 19th, and 20th. Because there are five violations so far, you can forward, search, and report on the stored event data on January 21st. However, if there is another violation on January 30th, you cannot forward, search, or report on January 31st because the number of violations has exceeded the maximum allowed. (A search run on January 31st fails and the user interface displays a warning.) If there are no additional data storage-limit violations from January 31st to February 4th, the ability to forward, search, and report resumes on February 5th because the January 5th violation is now outside of the 30-day window.

The Data Volume Restrictions page (**Configuration | Advanced > Data Volume Restrictions**) lists the data stored on your Software Logger on day-by-day basis in the last

30 days. It also indicates the days on which data limits were exceeded, as shown in the following figure.



Data Volume Restrictions

Date	Data Stored (MB)	Limit Exceeded
7/6/14	0	false
7/7/14	0	false
7/8/14	0	false
7/9/14	0	false
7/10/14	0	false
7/11/14	0	false
7/12/14	642198	true
7/13/14	0	false
7/14/14	0	false
7/15/14	0	false
7/16/14	0	false

When a data limit violation occurs, the Search user interface displays a warning. If you exceed the daily data limit frequently, you should consider purchasing a license that suits your needs. Contact your HP ArcSight sales representative to purchase a new license. Once you obtain the new license, follow the instructions in the ArcSight Logger Administrator's Guide to apply it on your Logger.

Acquiring a License for a Software Logger

For Software Loggers, starting with Logger 5.5, you can increase your daily data limit by purchasing a higher ingestion rate in increments of 5 GB/day.

While you can purchase a higher ingestion rate for Software Logger, the Logger Appliance comes preset with the maximum ingestion capacity of the model.

The Software Logger requires a license file for installation. To acquire the license, follow the instructions in the Electronic Delivery Receipt you receive from HP in an email after you place the order.

After installing Logger, you can view the specific details of the current license on the License Information and License & Update pages (**Configuration | Advanced > License Information and System Administration | System > License & Update**). For more information, refer to the Configuration and System Admin-Software Logger chapters of the Logger Administrator's Guide.

Prerequisites for Installation

Make sure these prerequisites are met before you install Software Logger:

- Before deploying in a production environment, get valid license file. If you do not have a license file, see "Acquiring a License for a Software Logger" on page 23.

- You need a separate license file for each instance of Software Logger. A license file is uniquely generated for each Enterprise Version download.
- 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.
  - A non-root user account must exist on the system on which you are installing Logger.
  - When you install as root, a non-root user account is still required.
  - When 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.
  - When you install as a non-root user, Logger can only listen for connections on port 9000. You cannot configure the port to a different value.
  - When upgrading, you cannot change the previous installation to a root-user installation. You will need to use the previously configured port 9000 for accessing Software Logger.
- 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.
- 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.
- 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 will be installing the Software 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.
- Increase the user process limit, as described in “Increasing the User Process Limit” on page 24.
- Verify that you have the correct installation file, as described in “Verifying the Downloaded Installation Software” on page 21.

Increasing the User Process Limit

Before installing or upgrading to Logger 6.0, you must increase this default limit while logged in as user *root*. This ensures that the system has adequate processing capacity.

To increase the default user process limit:

1. If you do not already have a file `/etc/security/limits.d/90-nproc.conf`, 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
```

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 runtime errors.

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

```
ulimit -a
```

5. Verify that the output shows the following values for Open files and Max user processes:
   - open files 65536
   - max user processes 10240

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

Installing Logger

Software Logger can be installed in the following three modes:

- GUI: In this mode, a wizard steps you through the installation and configuration of Software Logger. For instructions, see "Using the GUI Mode to Install Software Logger" on page 25.
- Console: In this mode, a command-line process steps you through the installation and configuration of Software Logger. For instructions, see "Using the Console Mode to Install Software Logger" on page 28.
- Silent: In this 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. 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. For instructions, see "Using the Silent Mode to Install Software Logger" on page 30.

Using the GUI Mode to Install Software Logger

Make sure the machine on which you will be installing Trial Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 23 are met.

Preinstallation steps:

- Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit" on page 24.

- You can verify that you have the correct installation file, as described in “Verifying the Downloaded Installation Software” on page 21.

You can install Logger as a root user or as a non-root user. See “Prerequisites for Installation” on page 23 for details and restrictions.

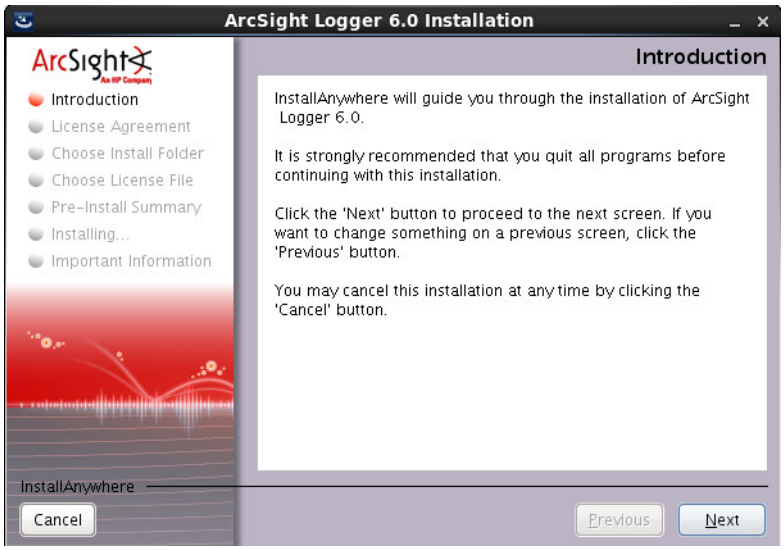
To install the Logger software:

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

```
chmod +x ArcSight-logger-6.0.0.XXXX.0.bin

./ArcSight-logger-6.0.0.XXXX.0.bin
```

2. The installation wizard launches, as shown in the following figure. 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 close the installer. If you use Ctrl+C to exit the installer and then uninstall Logger, uninstallation may delete your /tmp directory.

3. The License Agreement screen is displayed. Scroll to the bottom of the license agreement 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. If a check fails, it displays a message. You will need to fix the issue before proceeding. For example, if Logger is currently running on this machine, an Intervention Required message is displayed. In that case, click **Continue** to stop all current Logger processes and proceed with the installation, or click or **Quit** to exit the installer. Once all Logger processes are stopped and the checks complete, the next screen is displayed.
6. Navigate to or specify the location where you want to install Logger.

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

The user you are installing with must have access to the parent directory of the install directory. Otherwise, users will not be able to connect to the Logger UI and will see the following error message when they try to connect, "`Error 403 Forbidden. You don't have permission to access / on this server`".

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

- If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Click **Previous** to specify another location or **Quit** to exit the installer.
- If Logger is already installed at the location you specify, 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 Click **Choose** and navigate to or type the path and filename of the license file for this Logger. Click **Next**.

9 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.

10 **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	This user must already exist on the system.
HTTPS port	The port number to use when accessing the Logger UI. 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.
Configure Logger as a service	Indicate whether to configure Logger to run as a service. Select this option to create a service called `arcsight_logger`, and enable it to run at levels 2, 3, 4, and 5. 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, see "System Settings" on page 447.

11 Select the locale of this installation and click **Next**.

12 Click **Next** to initialize Logger components.

Initialization may take a few minutes. Please wait. Once initialization is complete, the next 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 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 Logger" on page 32.

Using the Console Mode to Install Software Logger

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 23 are met.

You can install Software Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 23 for details and restrictions.

To install the Logger software:

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

```
chmod +x ArcSight-logger-6.0.0.XXXX.0.bin

./ArcSight-logger-6.0.0.XXXX.0.bin -i console
```

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

```
Introduction
------------

InstallAnywhere will guide you through the installation of
ArcSight Logger 6.0.

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

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

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

PRESS <ENTER> TO CONTINUE:
```

3 The next several screens display the end user license agreement. Installation and use of Logger 6.0 requires acceptance of the 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. If a check fails, it displays a message. You will need to fix the issue before proceeding. For example, if Logger is currently running on this machine, an Intervention Required message is displayed. In

that case, type `Y` and press enter to stop all current Logger processes and proceed with the installation, or type `quit` and press Enter to exit the installer. Once all checks complete, the next screen is displayed.

6 The Choose Install Folder screen is displayed. 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.

The user you are installing with must have access to the parent directory of the install directory. Otherwise, users will not be able to connect to the Logger UI and will see the following error message when they try to connect, "`Error 403 Forbidden. You don't have permission to access / on this server`".

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

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

9 If Logger is already installed at the location you specify, a message is displayed. Type `quit` and press Enter to exit the installer or type `back` and press Enter to specify another location and uninstall the previous version. Click **Upgrade** to continue or **Previous** to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

10 Type the absolute path to the license file and then press Enter.

11 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.

12 **If you are logged in as root,** the following prompts will be displayed. Type responses and press Enter after each.

Field	Notes
User Name	This non-root user must already exist on the system.
HTTPS Port	The port number to use when accessing the Logger UI. 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. Select this option to create a service called arcsight_logger, and enable it to run at levels 2, 3, 4, and 5. 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 Logger Administrator's Guide.

13 Type the number that describes the desired locale, and pressed Enter.

14 Press Enter to initialize Logger components.

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

15 Press Enter to configure storage groups and storage volume and restart Logger automatically.

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.

16 Make a note of the URL and then press Enter 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 Logger" on page 32.

Using the 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.

About 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 Software Logger" on page 23 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 to be used for future silent installations:

1 Log in to the machine on which you can 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 +x ArcSight-logger-6.0.0.XXXX.0.bin

./ArcSight-logger-6.0.0.XXXX.0.bin -r <directory_location>
```

where `<directory_location>` is the location of the directory where the generated properties file will be placed.

The properties file is called `installer.properties`. You cannot specify or change this name.

3 Install Logger in GUI mode, as described in "Using the GUI Mode to Install Software Logger" on page 25.

4 Once the installation completes, navigate to the directory location you specified for the `installer.properties` file earlier.

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

```
# Fri May 11 18:27:49 PDT 2012
# 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/53

#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 23 are met.

If you are installing as root, make sure that non-root user account that you entered when generating the silent mode properties file 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 you generated previously to the same location where you have copied the Logger software.
2. Edit the LICENSE_LOCATION property in the silent mode properties file to include the location of license file for this instance of installation. (A unique license file is required for each instance of installation.)

   OR

   Set the LICENSE_LOCATION property to point to a file, such as software_logger_license.zip. Then, for each instance of the silent mode installation, copy the relevant license file to the location and rename it to software_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 +x ArcSight-logger-6.0.0.XXXX.0.bin

   ./ArcSight-logger-6.0.XXXX.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 Logger" on page 32.

Connecting to Logger

The Logger user interface (UI) is a web browser application using Secure Sockets Layer (SSL) encryption. Users must log in and be authenticated before they can access the Logger UI.

Logger 6.0 supports access through the following browsers:

- **Firefox:** Version ESR 31
- **Internet Explorer:** Versions 10 and 11
- **Chrome**: Latest version
- **Safari:** version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at http://www.adobe.com/products/flashplayer.html

JavaScript and cookies must be enabled.

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

For root installs, access to the port 443 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.

For non-root installs, access to port 9000 must be allowed, plus the ports for any protocol that the Logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.

The ports listed here are the default ports. Your Logger may use different ports.

To connect and log into Logger:

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

```
https://<hostname or IP address>:<configured_port> for the
Software Logger
```

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

Once you connect, the following Login screen is displayed.

2 Enter your user name and password, and click Login. Use the following default credentials if you are connecting for the first time or have not yet changed the default credentials:

Username: admin
Password: password

For more information about the login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator's Guide.

For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time.

Once you have logged in successfully, you can enable the preconfigured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy. Go to the section, "Configuring Logger" on page 49 for information on how to set up your Logger to start receiving events.

Starting and Stopping Software Logger

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.

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.
	Note: When the `loggerd restart` command is used to restart Logger, the status message for the "aps" process displays this message:
	`Process 'aps' Execution failed.`
	After a few seconds, the message changes to:
	`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 Logger Administrator's guide for more information.

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.

To uninstall the Logger software, enter this command in the installation directory:

```
./UninstallerData/Uninstall_ArcSight_Logger_6.0
```

The uninstall wizard launches. Click **Uninstall** or press Enter to start uninstalling Logger.

Chapter 4

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. It includes information on the following topics:

For information on how to install Software Logger on Linux, see "Installing Software Logger on Linux" on page 21. For initialization information about the Logger Appliance, see "Initializing a Logger Appliance" on page 13. For information about installing Trial Logger on Linux or on VMware VM, refer to the Trial Logger Quick Start guide.

Before You Begin

You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger 6.0 installer on a 64-bit CentOS 6.5 configured with 12 GB RAM and four physical (and eight logical) cores.

Downloading the Installation Package

The Logger installation package (Logger6.0_Ent_LXXXX_QXXXX.ova) is available for download from the HP Software Depot at http://software.hp.com.

Verifying the Downloaded Installation Software

HP provides code signing to enable you to verify that the software you have received is indeed from HP and has not been manipulated in any way by a third party. To do this, the software has been signed with a digital private key only held by HP.

Access the following link to download HP's public certificate:

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

This site also provides the step-by-step instructions for how to import HP's public certificate and verify the signature file.

How Licensing Works in Software Logger

Starting with Logger 5.5, licenses for all Logger types are based on Daily Data (the amount of data that comes into Logger per day). The Daily Data value is monitored and enforced on Software Loggers; however, currently, this value is not enforced on Logger appliances. Logger uses the sum of the sizes of the events received each day to determine this value.

For Software Loggers, you can increase your Daily Data limit by purchasing a higher ingestion rate in increments of 5 GB/day. While you can purchase a higher ingestion rate for Software Loggers, Logger appliances come preset with the maximum ingestion capacity of the model. Therefore, the ingestion capacity of Logger appliances cannot be upgraded.

See "Acquiring a License for a Software Logger" on page 39 for information about licensing your Software Logger.

If you are using ArcSight Connectors to send events to the Software Logger, make sure you are running connector version 5.1.3.5870.0 or later on your connectors to ensure that event size is accurately accounted on the Logger.

Even if this limit is exceeded, the Logger continues to collect and store events; therefore, no events are lost. However, if the limit is exceeded on more than five days in a 30-day sliding window, all features involving search are disabled.

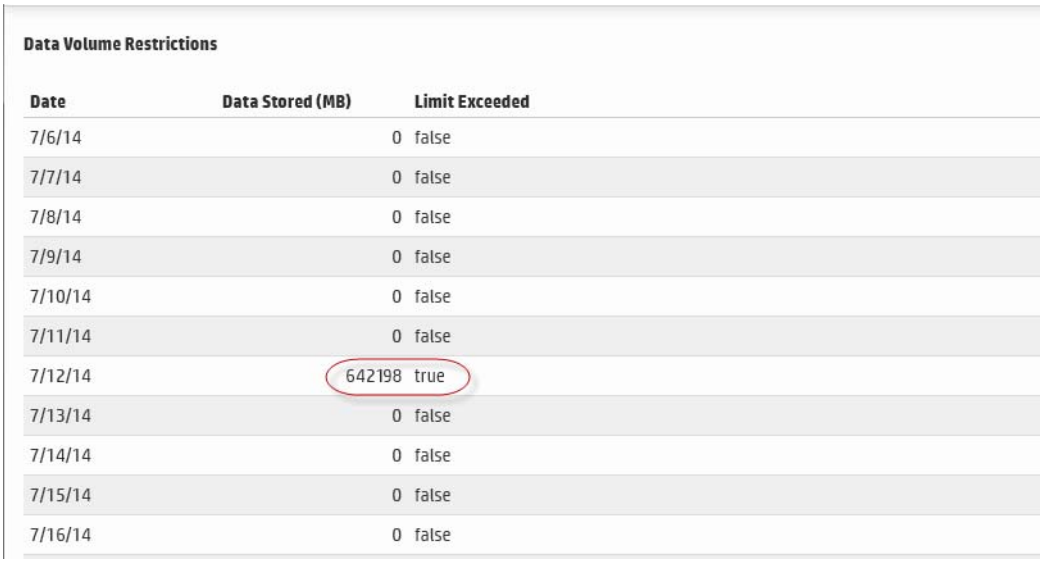
The disabled search features include forwarders as well as all searching and reporting functionality.

If this limit is exceeded six or more times (any six days or more days) in a given 30-day period, you cannot forward, search, or run reports on the collected events until the 30-day sliding window contains five or less data limit violations.

For example, you install the Logger software on January 1 with a data storage limit of 20 GB and start collecting events. Your Logger receives more than 20 GB of event data on these dates: January 5th, 13th, 18th, 19th, and 20th. Because there are five violations so far, you can forward, search, and report on the stored event data on January 21st. However, if there is another violation on January 30th, you cannot forward, search, or report on January 31st because the number of violations has exceeded the maximum allowed. (A search run on January 31st fails and the user interface displays a warning.) If there are no additional data storage-limit violations from January 31st to February 4th, the ability to forward, search, and report resumes on February 5th because the January 5th violation is now outside of the 30-day window.

The Data Volume Restrictions page (**Configuration | Advanced > Data Volume Restrictions**) lists the data stored on your Software Logger on day-by-day basis in the last

30 days. It also indicates the days on which data limits were exceeded, as shown in the following figure.



Data Volume Restrictions

Date	Data Stored (MB)	Limit Exceeded
7/6/14	0	false
7/7/14	0	false
7/8/14	0	false
7/9/14	0	false
7/10/14	0	false
7/11/14	0	false
7/12/14	642198	true
7/13/14	0	false
7/14/14	0	false
7/15/14	0	false
7/16/14	0	false

When a data limit violation occurs, the Search user interface displays a warning. If you exceed the daily data limit frequently, you should consider purchasing a license that suits your needs. Contact your HP ArcSight sales representative to purchase a new license. Once you obtain the new license, follow the instructions in the ArcSight Logger Administrator's Guide to apply it on your Logger.

Acquiring a License for a Software Logger

For Software Loggers, starting with Logger 5.5, you can increase your daily data limit by purchasing a higher ingestion rate in increments of 5 GB/day.

While you can purchase a higher ingestion rate for Software Logger, the Logger Appliance comes preset with the maximum ingestion capacity of the model.

The Software Logger requires a license file for installation. To acquire the license, follow the instructions in the Electronic Delivery Receipt you receive from HP in an email after you place the order.

After installing Logger, you can view the specific details of the current license on the License Information and License & Update pages (**Configuration | Advanced > License Information and System Administration |System > License & Update**). For more information, refer to the Configuration and System Admin-Software Logger chapters of the Logger Administrator's Guide.

Preparing the Virtual Machine

Before you can install the Logger software, you must import and configure the VM. This section guides you through the steps of importing and configuring the VM. As part of the operating system configuration process, you will need to create a second hard disk before installing Logger. After you add the second hard disk and power the system back on, the

startup scripts attach the second hard disk and format it with an XFS partition. This partition will be used for storing the Logger data.

To import the virtual machine:

1. Open the vSphere client and connect to the ESXi server.
2. On the vSphere client, open the File menu and select **Deploy OVF Template...**. and click **Next**.
3. On the Source panel, browse to select the Logger installation file (Logger6.0_Ent_LXXXX_QXXXX.ova) that you downloaded previously. Click **Open** and then click **Next.**
4. The OVF Template Details panel displays product information. Click **Next**.
5. On the Name and Location panel, enter a name for the virtual machine and click **Next**.
6. If there is more than one destination storage location available, select where to store the virtual machine. Click **Next**.
7. On the Disk Format panel select **Thick Provision Lazy Zeroed** and click **Next**.
8. The Ready to complete panel displays options you selected. Click **Finish** to confirm your selections and deploy the virtual machine.

   A progress bar displays the deployment progress. When the deployment is complete, the VM you created is displayed in the ESXi server's list.

The existing hard disk is for the Logger software. You must create another virtual hard disk to store Logger data.

To add a second hard disk:

1. Select the new VM from the ESXi server's list and make sure it is powered off.
2. Right-click the VM to open the dropdown menu, and then select **Edit Settings**.
3. The Virtual Machine Properties dialog box opens. Click **Add...**.

   The Device Type panel displays a list of devices you can add.
4. Select **Hard Disk** and click **Next**.
5. The Select a Disk panel displays the type of disks you can use. Select **Create a new virtual disk** and click **Next**.
6. The Create a Disk Panel displays virtual disk size and provisioning options.
   - Set the **Disk Size**.

   Be sure to set the Disk Size as large as possible. You cannot expand the hard disk once created. The minimum size is 40 GB. The maximum size is 2 TB.

   - Select **Thick Provision Lazy Zeroed**.
   - Click **Next**.
7. The Advanced Options panel displays other options. Keep the default Virtual device Node and click **Next**.
8. The Ready to complete panel displays options you selected. Click **Finish** to confirm your selections and add the hard disk.

Once created, the new hard disk is displayed in the Hardware list.

9 Click **OK** and Power on the new VM. The second hard disk is attached.

The VM has the default root password “arcsight”. A non-root user, arcsight, with no password is also included. Be sure to change the root password as soon as possible.

Prerequisites for Installation

Before installing Logger on the VM, make sure that the following prerequisites are met:

- 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.
  - A non-root user, arcsight, with no password, comes preconfigured on your VM image.
  - When you install as root, a non-root user account is still required. Use the non-root user, arcsight, which comes preconfigured on your VM image.
  - When 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.
  - When you install as arcsight, the non-root user, Logger can only listen for connections on port 9000. You cannot configure the port to a different value.
- 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.
- 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.
- 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.
- Before deploying in a production environment, get valid license file. If you do not have a license file, see “Acquiring a License for a Software Logger” on page 39.
- You need a separate license file for each instance of Software Logger. A license file is uniquely generated for each Enterprise Version download.
- Boot up the operating system on the VM, log in, set the time zone, and do any other necessary configuration before proceeding with the installation.
- Change the root password on the VM if you have not already done so.
- 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`.
- 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.
- If you have acquired a license file for your Logger, SCP it to the VM before you begin the installation. Make a note of the file name and location; you will need them during the installation process.
- Increase the user process limit, as described in “Increasing the User Process Limit” on page 42.
- Verify that you have the correct installation file, as described in “Verifying the Downloaded Installation Software” on page 37.

Increasing the User Process Limit

Before installing or upgrading to Logger 6.0, you must increase this default limit while logged in as user *root*. This ensures that the system has adequate processing capacity.

To increase the default user process limit:

1. If you do not already have a file `/etc/security/limits.d/90-nproc.conf`, 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
```

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 runtime errors.

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

```
ulimit -a
```

5. Verify that the output shows the following values for Open files and Max user processes:
   - open files 65536
   - max user processes 10240

After you have increased the user process limit and met the other prerequisites, you are ready to install 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 41 are met.

Preinstallation steps:

- Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit" on page 42.
- You can verify that you have the correct installation file, as described in "Verifying the Downloaded Installation Software" on page 37.

You can install Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 41 for details and restrictions.

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

To install the Logger software:

1. Run this command from the `/opt/arcsight/installers` directory:

   ```
   ./ArcSight-logger-6.0.0.XXXX.0.bin
   ```

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

   ```
   Introduction
   ------------

   InstallAnywhere will guide you through the installation of
   ArcSight Logger 6.0.

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

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

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

   PRESS <ENTER> TO CONTINUE:
   ```

3. The next several screens display the end user license agreement. Installation and use of Logger 6.0 requires acceptance of the 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. If a check fails, it displays a message. You will need to fix the issue before proceeding. For example, if Logger is currently running on this machine, an Intervention Required message is displayed. In that case, type `Y` and press enter to stop all current Logger processes and proceed with the installation, or type `quit` and press Enter to exit the installer. Once all checks complete, the next screen is displayed.

6. The Choose Install Folder screen is displayed. Type the installation path for Logger and then press Enter.

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

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

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

9. Type the absolute path to the license file and then press Enter.

10. 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.

11 **If you are logged in as root,** the following prompts will be displayed. Type responses and press Enter after each.

Field	Notes
User Name	Use the non-root user "`arcsight`" that comes preconfigured on your VM image.
HTTPS Port	The port number to use when accessing the Logger UI. 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. Select this option to create a service called arcsight_logger, and enable it to run at levels 2, 3, 4, and 5. 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 Logger Administrator's Guide.

12 Type the number that describes the desired locale, and pressed Enter.

13 Press Enter to initialize Logger components.

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

14 Press Enter to configure storage groups and storage volume and restart Logger automatically.

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.

15 Make a note of the URL and then press Enter 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 Logger" on page 44.

Connecting to Logger

The Logger user interface (UI) is a web browser application using Secure Sockets Layer (SSL) encryption. Users must log in and be authenticated before they can access the Logger UI.

Logger 6.0 supports access through the following browsers:

- **Firefox:** Version ESR 31
- **Internet Explorer:** Versions 10 and 11
- **Chrome**: Latest version
- **Safari:** version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at http://www.adobe.com/products/flashplayer.html

JavaScript and cookies must be enabled.

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

For root installs, access to the port 443 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.

For non-root installs, access to port 9000 must be allowed, plus the ports for any protocol that the Logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.

The ports listed here are the default ports. Your Logger may use different ports.

To connect and log into Logger:

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

```
https://<hostname or IP address>:<configured_port> for the
Software Logger
```

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

Once you connect, the following Login screen is displayed.

2 Enter your user name and password, and click Login. Use the following default credentials if you are connecting for the first time or have not yet changed the default credentials:

Username: admin
Password: password

For more information about the login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator's Guide.

For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time.

Once you have logged in successfully, you can enable the preconfigured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy. Go to the section, "Configuring Logger" on page 49 for information on how to set up your Logger to start receiving events.

Starting and Stopping Software Logger

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.

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.

Command	Purpose

`loggerd restart`	This command restarts processes listed under the Process section only.
	Note: When the `loggerd restart` command is used to restart Logger, the status message for the "aps" process displays this message:
	`Process 'aps' Execution failed.`
	After a few seconds, the message changes to:
	`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 process from the **System Admin > System > Process Status** page. Refer to the Logger Administrator's guide for more information.

Uninstalling Logger

To uninstall the Logger software, simply delete the VM. Alternatively, enter this command in the installation directory:

```
./UninstallerData/Uninstall_ArcSight_Logger_6.0
```

The uninstall wizard launches. Click **Uninstall** or press Enter to start uninstalling Logger.

Chapter 5

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

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). You must enable these receivers in order to use them. See "Enabling the Preconfigured Folder Follower Receivers" on page 50 for instructions.

The preconfigured receivers are described more detail in "Receivers" on page 10. For further information on receivers, refer to the Configuration chapter of the Logger Administrator's Guide.

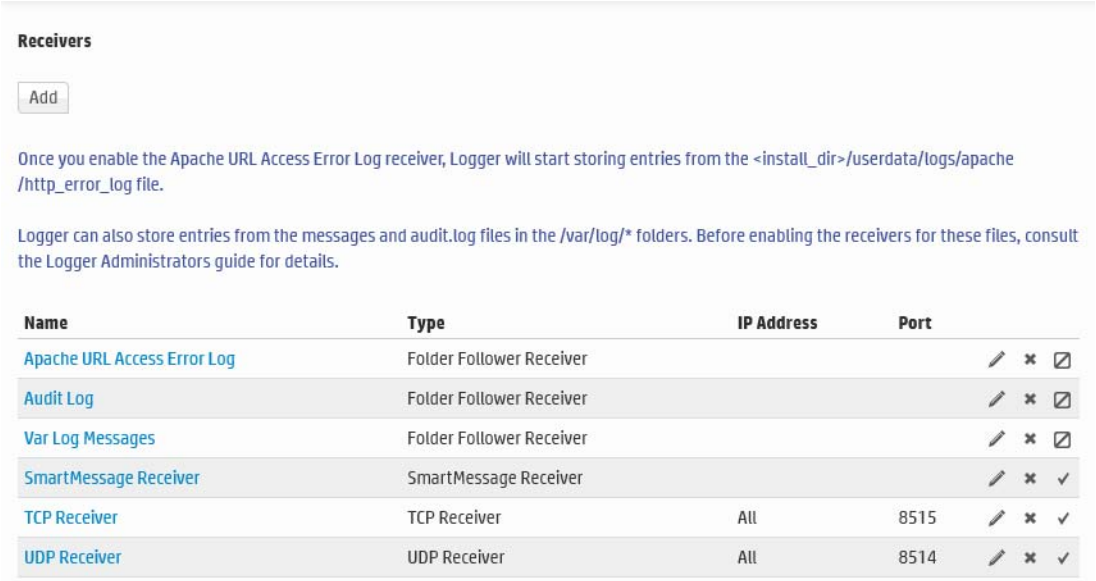
Logger can also receive events from ArcSight SmartConnectors that collect event data from sources on your network. To learn more about ArcSight SmartConnectors, visit http://www8.hp.com/us/en/software-solutions/enterprise-security.html.

Enabling the Preconfigured Folder Follower Receivers

The preconfigured receivers are described more detail in "Receivers" on page 10. For further information on receivers, refer to the Configuration chapter of the Logger Administrator's Guide.

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

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 preconfigured SmartMessage receiver, see "Using SmartConnectors to Collect Events" on page 51.

Devices

Logger begins storing events when an enabled receiver receives data or, in the case of a file receivers, 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, refer to the Configuration chapter of the Logger 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, refer to the Configuration chapter of the Logger 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 created additional storage groups, and want to send events to them, you can do that with storage rules. If you choose not to create storage rules, events from all devices will be sent to the Default Storage Group and use its specified retention policy.

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. For example, you could search for events that match a certain pattern and which belong to a particular device group, and send them to a particular storage group for retention based on event category.

Storage rules are evaluated in order of priority; the first matching rule determines to which storage group an 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.

Refer to the Configuration chapter of the Logger Administrator's Guide for more information on storage rules.

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.

SmartMessage

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

SmartMessage and FIPS require SmartConnector 4.7.5 or later. If you do not have the current build, download the latest from the HP ArcSight web site.

Older SmartConnectors will work with Logger, but may not support SmartMessage or FIPS.

SmartMessage provides an end-to-end encrypted secure channel using secure sockets layer (SSL). 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.

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

Downloading SmartConnectors

For Logger Appliance and the Enterprise Version of Software Logger, contact your HP ArcSight sales representative or customer support for the location to download SmartConnectors.

A restricted set of ArcSight SmartConnectors are supported and available For the Trial Version of Software Logger. You can download these SmartConnectors from the same location from which you downloaded Logger. The configuration guides for the supported SmartConnectors are available at the same web site. To learn more about ArcSight SmartConnectors, visit http://www8.hp.com/us/en/software-solutions/enterprise-security.html.

Configuring a SmartConnector to Send Events to Logger

Logger comes pre-configured with a SmartMessage Receiver. To use it 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.
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 preconfigured receiver, specify "SmartMessage Receiver" as the **Receiver Name**.
   - To use SmartMessage to communicate between an ArcSight SmartConnector and a Logger Appliance, configure the SmartConnector to use port 443.
   - To communicate between an ArcSight SmartConnector and Software Logger, configure the SmartConnector to use the port configured for the Software Logger.
   - For un-encrypted 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.

For more information about the Common Event Format (CEF), refer to Implementing ArcSight CEF. For a downloadable a copy of this guide, search for "ArcSight Common Event Format (CEF) Guide" on the Protect 724 Community at https://protect724.hp.com.

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. Add this property:

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

   Delete the `transport.default.type` property.

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 Protect 724 Community at https://protect724.hp.com.

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 this:

`ArcSight-4.x.x.<build>.x-SuperConnector-<platform>.exe`

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.

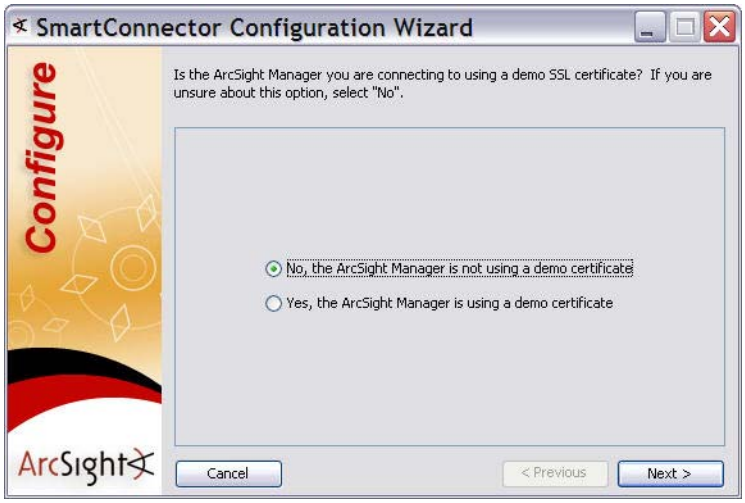


Figure 5-1 SmartConnector Configuration Wizard

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)
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 53.

For more information about the Common Event Format (CEF), refer to Implementing ArcSight CEF. For a downloadable a copy of this guide, search for “ArcSight Common Event Format (CEF) Guide” in the ArcSight Product Documentation community at https://protect724.hp.com.

Index