



HP ArcSight Trial Logger

Software Version: 6.1

Quick Start Guide

August 31, 2015



Copyright © 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	http://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
08/31/2015	6.1	Updated for Logger 6.1 release.
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	5
Chapter 1: Overview	7
How Logger Works	7
Logger for Security, Compliance, and IT Operations	8
Chapter 2: Installing and Configuring Logger	11
Before You Install	11
Trial License	11
How Licensing Works	11
Viewing Your License	12
Prerequisites for Installation	12
Increasing the User Process Limit	13
Installing the Trial Logger	13
Installing Trial Logger on a Linux System	14
Installing Trial Logger for VMware VM	16
Preparing the Virtual Machine	17
Installing the Trial Logger on the Virtual Machine	18
Connecting to Logger	20
Initial Logger Configuration	22
Starting and Stopping Logger	22
Uninstalling Logger	23
Chapter 3: Receiving Events and Logs	25
Enabling the Preconfigured Receivers	25
Configuring New Receivers	27
Sending Structured Data to Logger	27
Configuring a SmartConnector to Send Events to Logger	28
Chapter 4: Overview of the Logger User Interface	29
Navigating the User Interface	29
Take Me To	29
Server Clock, Current User, and Options Dropdown	30
The Options Page	30

Logout	30
Summary	31
Dashboards	31
Chapter 5: Searching for Events	33
Example Queries	33
Syntax of a Query	33
Building a Query	34
Run a Query	35
Query Building Tools	35
Exporting Search Results	37
Saving Queries for Later Use	37
System Filters (Predefined Filters)	37
Tuning Search Performance	38
Chapter 6: Alerts	39
Types of Alerts	39
Configuring Alerts	40
Chapter 7: Other Logger Features	41
Scheduling Tasks	41
Archiving Events	41
Access Control on Logger Users	41
Enriching Data Through Static Correlation	41
Web Services	42
Chapter 8: Example Queries	43

About this Guide

This guide enables you to download, install, and start using the trial version of ArcSight Logger in a matter of minutes. You do not require any prior knowledge of Logger to use the product or to understand information in this document; however, you should be familiar with the log management concept.

The goal of this guide is to enable you to start using Trial Logger quickly. For an in-depth discussion of Logger, or any of its features, refer to the online Help available with the product or to the ArcSight Logger Administrator's Guide.

Chapter 1

Overview

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

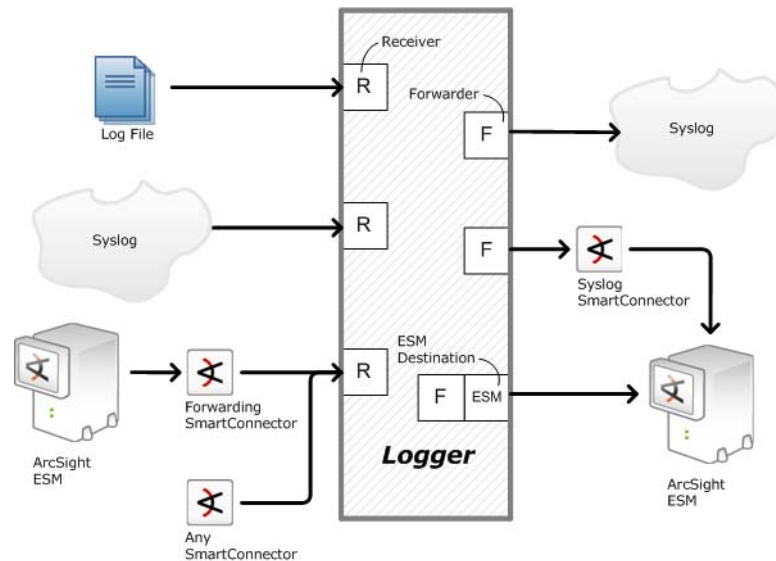


The features available on Logger vary by version and license. Certain Logger features mentioned in this guide are not available in the trial version. These are indicated by *italic* font.

The trial version of Logger is available in two form factors, as software and as a virtualized image. The form factors offer identical features. Trial Logger can be installed on a supported Linux platform of your choice. Trial Logger for VMware VM includes the Trial Logger installation files and a preinstalled operating system to enable quick deployment on an ESXi server.

How Logger Works

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



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

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

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

** The trial version of Logger differs from the Enterprise version of Logger in that it does not include Forwarding Connectors, the Reporting feature, support for Peering, or remote management via ArcSight Management Center. To take advantage of these features, purchase and install an Enterprise version of Logger.*

Logger for Security, Compliance, and IT Operations

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

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

addition, *Logger also contains predefined reports for common security and device monitoring use cases.*

For a complete list of predefined content filters *and predefined reports*, refer to the ArcSight Logger Administrator's Guide. Information about how to use predefined filters is included in ["System Filters \(Predefined Filters\)" on page 37](#).

Chapter 2

Installing and Configuring Logger

This chapter explains what you need to know to install and start running Trial Logger on a LINUX system or on a VMware VM.

Before You Install

You need to have a server with supported operating system and storage available to install the Trial Logger. For more information about the platforms on which you can install and use Logger, refer to the Release Notes and Support Matrix for your version. These documents are available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.

You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 5.5. The VM image includes the Logger 6.1 Trial installer on a 64-bit CentOS 7.1 configured with 12 GB RAM and four physical (and eight logical) cores.

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

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

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

Trial License

Trial Logger includes a built-in trial license that you can use for a limited period of time for test and evaluation purposes. To use Logger after the trial period is over or to access Logger's full feature set, you must purchase and install the Enterprise version. Contact your HP ArcSight sales representative for details.



The Trial Logger cannot be migrated or upgraded to an Enterprise version of Logger. Be sure to use an Enterprise version of when deploying Logger on a production system.

How Licensing Works

The license for Logger defines its Daily Data limit—a per day limit on the amount of incoming data. For example, the limit might be 5 GB per day. The sum of the sizes of the events is used to determine this value.

When a data limit violation occurs, the Search user interface displays a warning. For a detailed explanation of how licensing works, refer to the Logger Administrator's Guide.

Viewing Your License

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

Prerequisites for Installation

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

- Verify that you have the correct installation file, as described in [“Before You Install” on page 11](#).
- Increase the user process limit, as described in [“Increasing the User Process Limit” on page 13](#).
- 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. If you are installing Logger on VMware VM, 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. If you are installing Logger on VMware VM, 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.

Additional prerequisites for installing trial Logger on VMWare VM only:

- Boot up the operating system on the VM, log in, set the timezone, and do any other necessary configuration before proceeding with the installation.



The VM has the default root password “arcsight”. A non-root user, arcsight, with no password is also included. For security reasons and so that you can SCP and SSH to your machine, change the root password and add a password for the arcsight user as soon as possible.

- 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.

Additional prerequisite for installing Trial Logger on a native Linux system only:

- Ensure that you are installing Logger on a supported platform. Refer to the Release Notes and Support Matrix for this information. These documents are available for download from the ArcSight Product Documentation community at <https://protect724.hp.com>.
- You must have an X Window System server installed to use the GUI mode of installation. If you will be installing the Trial 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.

Increasing the User Process Limit

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

To increase the default user process limit:

- 1 Open the file `/etc/security/limits.d/<NN>-nproc.conf`. (<NN> is 90 for RHEL or CentOS 6.6 and 20 for RHEL and CentOS 7.1.)
 - ◆ If you do not already have a `/etc/security/limits.d/<NN>-nproc.conf` file, create one (and the `limits.d` directory, if necessary).
 - ◆ If the file already exists, delete all entries in the file.
- 2 Add the following lines:

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



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
```

Installing the Trial Logger

This section describes the prerequisites and the procedure for installing Trial Logger. Installing the Trial Logger software on either platform requires the same basic steps.

However, if you are installing Logger on a virtual machine, you will need to prepare the virtual machine before installing Logger on it.

Overview of steps to install Trial Logger:

- 1 Confirm that you meet the prerequisites for installation as described in [“Prerequisites for Installation” on page 12](#).
- 2 Install the Logger software using the appropriate instructions for your platform.
 - ◆ To install Trial Logger on a native Linux system, follow the steps in [“Installing Trial Logger on a Linux System” on page 14](#).
 - ◆ To install Trial Logger on VMware VM, follow the steps in [“Installing Trial Logger for VMware VM” on page 16](#).

After you finish installing the Logger software, you can connect to Logger as described in [“Connecting to Logger” on page 20](#).

Installing Trial Logger on a Linux System

This section describes the procedure for installing Trial Logger on a native Linux system. For instructions on how to install Trial Logger on a VMware VM, see [“Installing Trial Logger for VMware VM” on page 16](#).

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 12](#) are met.

Preinstallation steps:

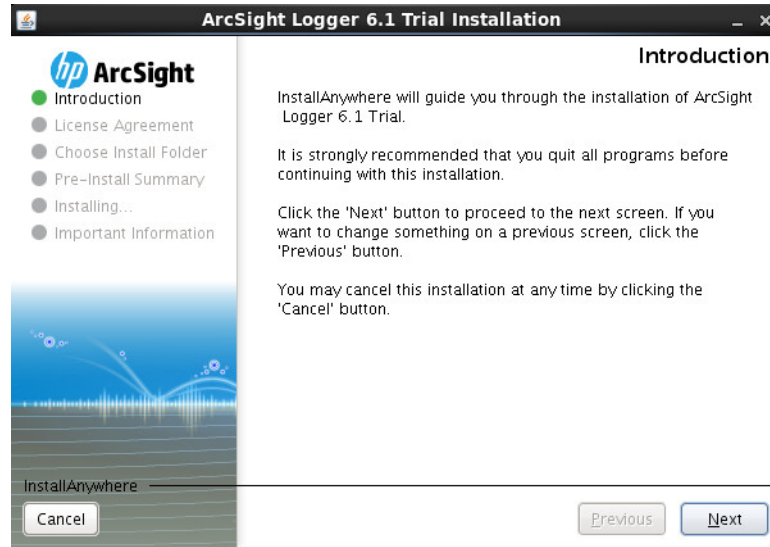
- Before you install, you must increase the user process limit on the OS, as described in [“Increasing the User Process Limit” on page 13](#).
- You can verify that you have the correct installation file, as described in [“Before You Install” on page 11](#).

You can install Logger as a root user or as a non-root user. See [“Prerequisites for Installation” on page 12](#) for details and restrictions.

To install the Logger software:

- 1 Run these commands from the `/opt/arcsight/installers` directory:

```
chmod +x ArcSight-logger-6.1.0.XXXX.0.trial.bin
./ArcSight-logger-6.1.0.XXXX.0.trial.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.



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 **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 for trial Logger 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 Review the pre-install summary and then click **Install**.

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

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

Field	Notes
Non-root user name	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 <code>arcsight_logger</code> , 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 can still do so later. For instructions on how to enable Logger to start as a service after installation, see "System Settings" on page 449 .

- 10 Select the locale of this installation and click **Next**.

- 11 Click **Next** to initialize Logger components.

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

- 12 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.

- 13 Make a note of the URL and then click **Done** to exit the installer.

You can use the URL you noted during the installation to connect to Logger and start configuring it to receive events. See ["Connecting to Logger" on page 20](#).

Installing Trial Logger for VMware VM

This section describes the procedure for installing Trial Logger for VMware VM. For instructions on how to install Trial Logger on a native Linux system, see ["Installing Trial Logger on a Linux System" on page 14](#).

Installing Trial Logger for VMware VM requires two basic steps:

- ["Preparing the Virtual Machine" on page 17](#)
- ["Installing the Trial Logger on the Virtual Machine" on page 18](#).

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 package (Logger6.1_Trial_LXXXX_QXXXX.ova) that you downloaded previously. Click **Open** and then click **Next**.
- 4 The OVF Template Details panel displays product information and 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 pre-existing hard disk on the VM 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 8 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. For security reasons and so that you can SCP and SSH to your machine, change the root password and add a password for the arcsight user as soon as possible.

Installing the Trial Logger on the Virtual Machine

Make sure the VM image is configured to comply with the requirements listed in the Release Notes for your version and that the prerequisites listed in ["Prerequisites for Installation" on page 12](#) 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 13](#).
- You can verify that you have the correct installation file, as described in ["Before You Install" on page 11](#).

You can install Logger as root or as a non-root user. See ["Prerequisites for Installation" on page 12](#) for details and restrictions.



You must install into the /opt/arcsight/logger directory.

To install the Logger software:

- 1 Run these commands from the /opt/arcsight/installers directory:

```
chmod +x ArcSight-logger-6.1.0.XXXX.0.trial.bin
./ArcSight-logger-6.1.0.XXXX.0.trial.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 6.1 Trial.
```

```
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 6.1 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 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.

- 10 **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. 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.

Field	Notes
Choose if you want to run Logger as a system service.	<p>Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone.</p> <p>Select this option to create a service called <code>arcsight_logger</code>, and enable it to run at levels 2, 3, 4, and 5.</p> <p>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.</p>

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

12 Press Enter to initialize Logger components.

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

13 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.

14 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 20](#).

Connecting to Logger

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

Logger 6.1 supports access through the following browsers:

- IE 10, IE 11
- FF ESR 39
- Chrome (current)
- Safari 8.x (on OS X 10.9)

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

- For root installs, allow access to port 443 as well as 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, allow access to port 9000 as well as 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.



Note

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

JavaScript and cookies must be enabled.

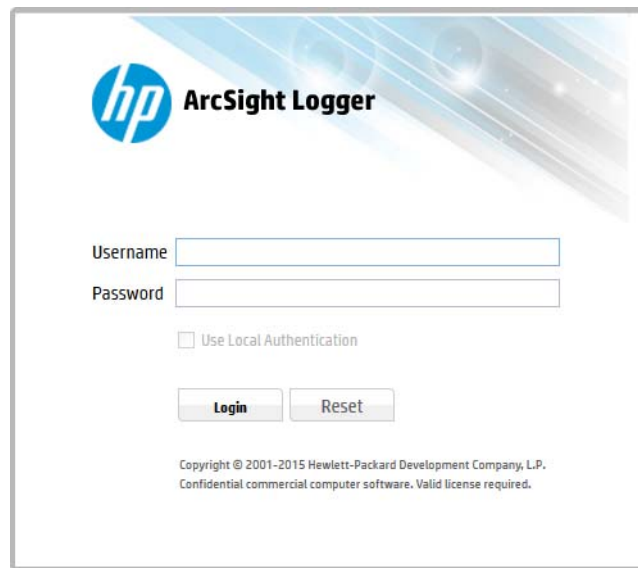
To connect and log into Logger:

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

`https://<hostname or IP address>:<configured_port>`

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.

- 2 The first time you connect on a Logger appliance, the END USER LICENSE AGREEMENT is displayed. Scroll down to the bottom of the screen to review and accept the EULA. After you accept, the Login screen is displayed.
- 3 Once you connect, the following Login screen is displayed.



- 4 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 log-in screen and connecting to Logger, refer to the ArcSight Logger Administrator's Guide.



Note

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

Refer to the ArcSight Logger Administrator's Guide instructions.

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 ["Enabling the Preconfigured Receivers" on page 25](#) for information on how to set up your Logger to start receiving events.

Initial Logger Configuration

The Logger initialization sets up the following default configuration. For details about the listed components, refer to the ArcSight Logger Administrator's Guide.

Component	Default Configuration
Storage Volume	7 GB (available for data storage)
Storage Groups	Two: A Default Storage Group and an Internal Storage Group
Indexing	Full-text and field-based indexing enabled
Receivers	Six total: One of each TCP, UDP, and SmartMessage type; and three Folder Follower receivers

Starting and Stopping 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
<code>loggerd start</code>	Start all processes listed under the System and Process sections in the figure above. Use this command to launch Logger.
<code>loggerd stop</code>	Stop processes listed under the Process section only. Use this command when you want to leave <code>loggerd</code> running but all other processes stopped.

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

Uninstalling Logger

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

Before uninstalling Logger, stop the Logger processes by using the `loggerd stop` command, as described in [“Starting and Stopping Software Logger” on page 35](#). To uninstall the Logger software, enter this command in the installation directory:

```
./UninstallerData/Uninstall_ArcSight_Logger_6.1_trial
```

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

Chapter 3

Receiving Events and Logs

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

Logger can also receive events from ArcSight SmartConnectors that collect event data from sources on your network. A subset of ArcSight SmartConnectors is supported for Trial Logger and available for download from the same location from which you downloaded Logger. The Configuration Guides for the supported SmartConnectors are included and available at the same web site. To learn more about ArcSight SmartConnectors, visit <http://www8.hp.com/us/en/software-solutions/enterprise-security.html>.

Enabling the Preconfigured 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. 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. 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.

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`



A 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.

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.

Add Data









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.


Receivers

Add

Once you enable the Apache URL Access Error Log receiver, Logger will start storing entries from the `<install_dir>/userdata/logs/apache/http_error_log` file.


Logger can also store entries from the messages and audit.log files in the `/var/log/*` folders. Before enabling the receivers for these files, consult the Logger Administrators guide for details.

Name	Type	IP Address	Port	
Apache URL Access Error Log	Folder Follower Receiver			
Audit Log	Folder Follower Receiver			
Var Log Messages	Folder Follower Receiver			
SmartMessage Receiver	SmartMessage Receiver			
TCP Receiver	TCP Receiver	All	8515	
UDP Receiver	UDP Receiver	All	8514	

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.

Once you enable the receivers, you should see events coming into your system from those logs. For more information about receivers, refer to the ArcSight Logger Administrator's Guide.

Configuring New Receivers

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

You can configure the following types of receiver for Logger:

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



- The SCP, SFTP, and FTP file transfer receivers depend on the FTP (File Transfer Protocol) SCP (Secure Copy Protocol) and SFTP (SSH file transfer protocol) clients installed on your system.
- The SCP and SFTP protocols on Logger appliances are not FIPS compliant.

- **SmartMessage Receiver:** SmartMessage receivers listen for encrypted messages from ArcSight SmartConnectors. To start using the preinstalled receiver, you must configure a SmartConnector to send events to it. For instructions, see [“Configuring a SmartConnector to Send Events to Logger” on page 28](#).

Sending Structured Data to Logger

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

Logger can receive structured data in the form of normalized CEF events from ArcSight SmartConnectors, as shown in the illustration in [“How Logger Works” on page 7](#).

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>.

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.



Refer to the documentation that came with your SmartConnector for instructions.

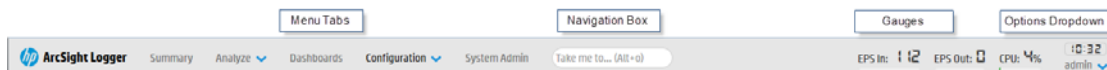
- 2 Specify the required parameters. Enter the Logger hostname or IP address and the name of the SmartMessage receiver. These settings must match the receiver in Logger that listen for events from this connector.
 - ◆ To use the preconfigured receiver, specify "SmartMessage Receiver" as the **Receiver 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.

Overview of the Logger User Interface

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

Navigating the User Interface

As shown in the following figure, a navigation and information band runs across the top of every page in the user interface.

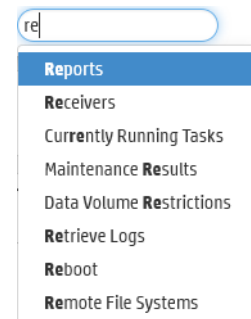


Gauges at the top of the screen provide an indication of the throughput and CPU usage information available in more detail on the Monitor Dashboard (["Dashboards" on page 31](#)). You can change the range of the gauges on the Options page. The name of the currently logged-in user is shown below the statistics. The menu list in the upper right includes links for Help, Options, and Logout.

Take Me To

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

You can access the Take me to... navigation box by clicking in it or by using the Alt+o, Alt+p, or Ctrl+Shift +o hot keys. As you type, a list of features that match drops down. Click an item in the list or press enter to go to the specified feature.



Note

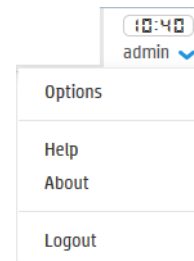
You can open the help for your current UI page, by typing `help` in the **Take me to...** search box.

Server Clock, Current User, and Options Dropdown

The server clock is shown to the right of the gauges, along with the currently logged-in user's name and the options dropdown.

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

Click the down-arrow by the user name to access the Options, Help, About, and Logout links.



The Options Page

The Options page, shown in the following figure, allows you to set the range on the EPS In and EPS Out gauges. If the event rate exceeds the specified maximum, the range is automatically increased.

From here, you can **Upload a logo (.png file)** and replace the ArcSight Logger logo with your custom logo. The logo must be in .png format. The recommended size is 150 X 30 px and the maximum file size is 1MB.

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

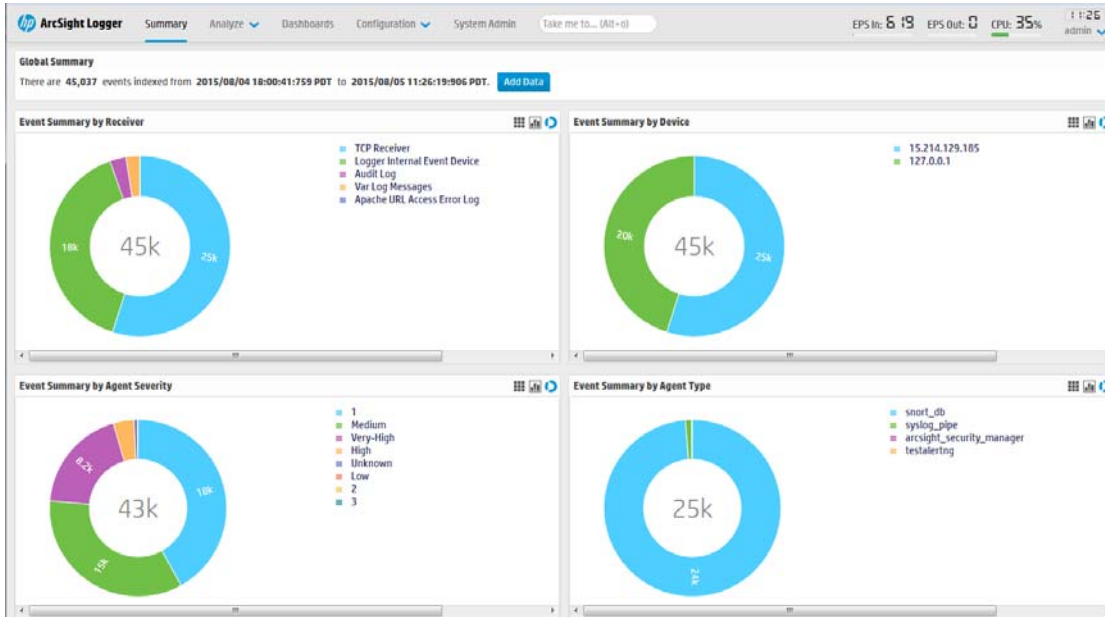
Logout

Click the Logout link on any page to return to the Login screen. Logging out is good security practice, to eliminate the chance of unauthorized use of an unattended Logger session.

Logger automatically logs you out after a user-configurable length of time (15 minutes by default). To change this length of time, refer to the ArcSight Logger Administrator's Guide.

Summary

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



Dashboards

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

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

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

Chapter 5

Searching for Events

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

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

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

Example Queries

Simple Queries:

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

Complex Query:

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

Syntax of a Query

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

keyword expression

field-based expression | search operator expression

- A keyword: a word expressed in plain English; for example, warning, failed, login, and so on.

- A field-based expression: searching for values in the fields of an event. This includes searches for uncommon values in specific fields.

Examples:

```
name="failed login"
message!="failed login"
sourceAddress=192.0.2.0
```

A complete list of fields is available in the ArcSight Logger Administrator's Guide, along with a list of the fields have been indexed and the fields that have been super indexed for faster searches.

- A search operator expression: an expression that uses search operators to refine the data that matches the expressions specified by the keyword and the field-based expression.

Search operators: The following search operators are available in Logger 6.1: `cef`, `chart`, `dedup`, `eval`, `extract`, `fields`, `head`, `keys`, `rare`, `regex`, `rename`, `replace`, `rex`, `sort`, `tail`, `top`, `transaction`, and `where`.

Extraction operator: The `rex` search operator is useful for syslog events (raw or unstructured data) or if you want to extract information from a specific point in an event, such as the 15th character in an event.

Example:

To extract an IP address from the following event

```
[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP
Warning: Can't connect to 10.4.31.4:11211
```

and assign it to a field called "IP_Address", use the following rex expression:

```
| rex "(?<IPAddress>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
```

Implied field extraction operator: You can specify the event fields directly in queries, as shown in the examples below.

To display search results of the count of unique values device addresses in a chart form:

```
failed | chart _count by deviceAddress
```

To display search results of the most common values for the `deviceAddress` field in table form. That is, the values are listed in order from the highest number of matches to the lowest.

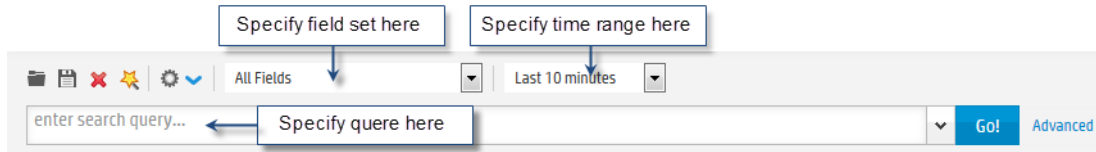
```
failed | top deviceAddress
```

For detailed usage and examples of the search expressions, refer to the ArcSight Logger Administrator's Guide.

Building a Query

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

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



In addition, you can also include constraints that limit the search to specific device groups and storage groups. For more information about specifying constraints, refer to the ArcSight Logger Administrator's Guide.

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

Run a Query

To run a query:

- 1 Click **Analyze > Search**.
- 2 Specify the query expression in the Search text box.
- 3 Select the time range and (optionally) the field set.
- 4 Click **Go**.



If you receive a syntax error when running a query, ensure that the syntax of the query follows the requirements specified in the "Syntax Reference for Query Expression" section of the ArcSight Logger Administrator's Guide.

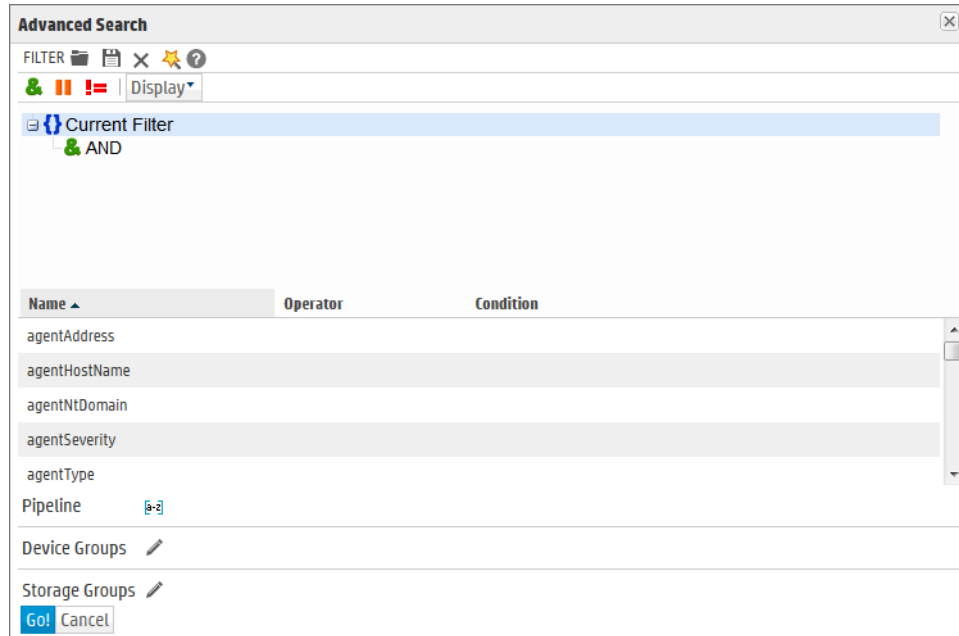
Query Building Tools

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

■ Search Builder

The Search Builder tool, as shown in the following figure, is a Boolean-logic conditions editor that enables you to build search queries quickly and accurately. The tool provides a visual representation of the conditions you are including in a query. You can specify keywords, field-based conditions, and regular expressions using this tool. In addition, the tool enables you to specify search constraints such as device groups and storage groups.

Click **Advanced Search** below the Search text box to access this tool. For information about how to use this tool, refer to the ArcSight Logger Administrator's Guide.



■ Regex Helper

Creating a regular expression for the `rex` extraction operator can be complex and error prone. The Regex Helper tool enables you to create regular expressions to use with the `rex` pipeline operator to extract fields of interest from an event. This tool not only simplifies the task of creating regular expressions for the `rex` operator but also makes it efficient and error free. For details about this tool, refer to the ArcSight Logger Administrator's Guide.

■ Search Helper

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


- ◆ **Search History:** Displays the recently run queries on Logger, thus enabling you to select and reuse previously run queries without typing them again.
- ◆ **Search Operator History:** Displays the fields used previously with the search operator you have typed in the Search text box.
- ◆ **Examples:** Lists examples relevant to the latest query operator you have typed in the Search text box.
- ◆ **Suggested Next Operators:** List of operators that generally follow the currently typed query. For example, if you type `logger |`, the operators that often follow are `rex`, `extract`, or `regex`.
- ◆ **Help:** Provides context-sensitive help for the last-listed operator in the query you have typed in the Search text box.
- ◆ **List of Fields and Operators:** Depending on the query you have typed in the Search text box, a complete list of fields that possibly match the field name you are typing or a list of operators that are available on Logger is displayed.

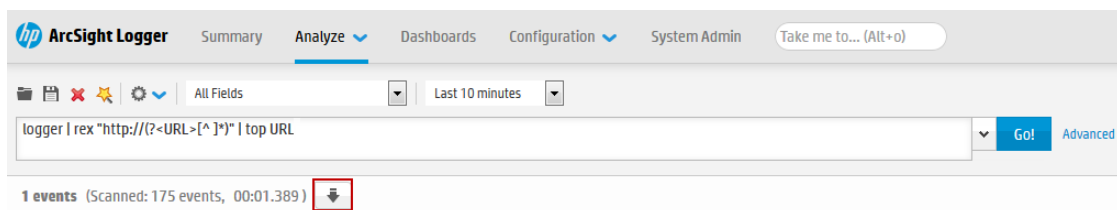
Exporting Search Results

You can export search results in these formats:

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

To export search results:

- 1 Run a search query.
- 2 Click **Export Results**. 



Saving Queries for Later Use

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

- Saved filter: Save the query expression, but not the time range or field set information.
- Saved search: Save the query expression and the time range.

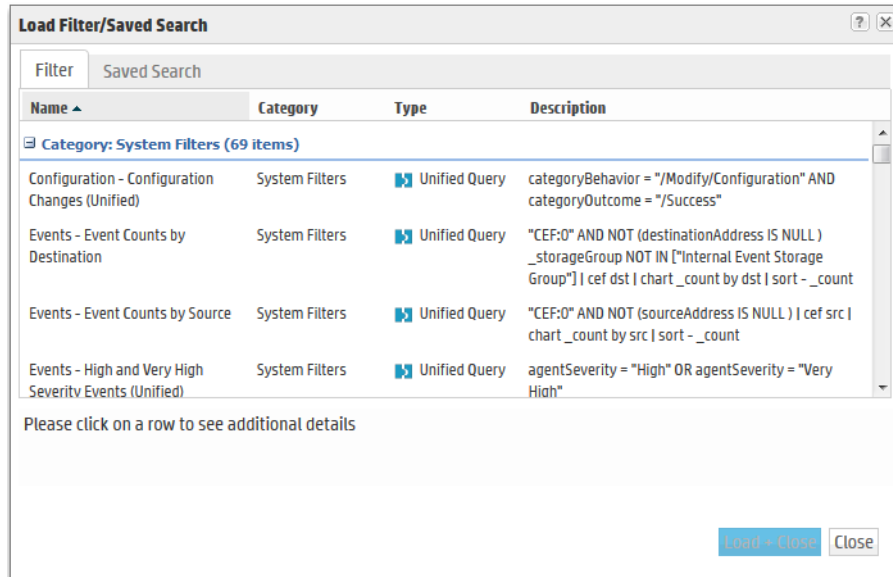
For more information about saving queries and using them again, refer to the ArcSight Logger Administrator's Guide.

System Filters (Predefined Filters)

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

To use a system filter:

- 1 Click **Analyze > Search**.
- 2 Click the Load a Saved Filter icon () to view a list of all system filters.



- 3 Click **Load + Close**.

Tuning Search Performance

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

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

- Take advantage of super indexes where possible, for the fastest search results. Refer to the ArcSight Logger Administrator's Guide for more information on how to search super-indexed fields.
- The amount of time it takes to search depends on the size of the data set that must be searched through, the complexity of the query, and whether the search is distributed across peers. To limit the data set, ensure that time range you specify does not result in a query that needs to scan multi-millions of events.
- Limiting search to specific storage groups or peers typically results in better search performance than when the storage groups or peers are not specified.
- Reduce other load on the system when your query needs to run, such as scheduled jobs, multiple reports being run, or large number of incoming events.
- Full-text indexing and Field-based indexing for a recommended set of fields are automatically enabled at Logger initialization time. In addition to these fields, HP strongly recommends that you index fields that you will be using in search and report queries. Refer to the ArcSight Logger Administrator's Guide for more information on indexing fields.

Chapter 6

Alerts

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

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

Types of Alerts

Logger provides two types of alerts:

- Real time alerts
- Saved Search Alerts

The following table compares the two types of alerts.

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

Real Time Alerts	Saved Search Alerts
<p>To define a real time alert, you specify a query, match count, threshold, and one or more destinations.</p> <p>A time range is not associated with the queries defined for these alerts. Therefore, whenever the specified number of matches occurs within the specified threshold, an alert is triggered.</p>	<p>To define a Saved Search Alert, you specify a Saved Search (which is a query with a time range), match count, threshold, and one or more destinations.</p> <p>A time range (within which events should be searched) is specified for the query associated with these alerts. Therefore, specified number of matches within the specified threshold (in minutes) must occur within the specified time range. You can also use dynamic time range (for example, \$Now-1d, \$Now, and so on).</p> <p>For example, if a Saved Search query has these start and end times:</p> <p>Start Time: 5/11/2010 10:38:04</p> <p>End Time: 5/12/2010 10:38:04</p> <p>And, the number of matches and threshold are the following:</p> <p>Match Count: 5</p> <p>Threshold: 3600</p> <p>Then, 5 events should occur in one hour anytime between May 11th, 2010 10:38:04 a.m. and May 12th, 2010 10:38:04 for this alert to be triggered.</p>

Configuring Alerts

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

Other Logger Features

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

Scheduling Tasks

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

Archiving Events

Event Archives let you save the events for any day in the past, not including the current day. The archive location can be a local directory or a mount point that you have already established on the system on which Logger software is installed. You can also schedule a daily archive of the events. Index information is not included in event archives. However, you can index an archive after it has been added. This will enable searches on archived events to be as fast as searches in live storage.

Access Control on Logger Users

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

Enriching Data Through Static Correlation

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

Web Services

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

Chapter 8

Example Queries

This section provides a few example queries that you can use on Logger. These queries assume that your Logger is receiving and storing events. You can also modify these queries to suit your needs.



To form rex expression, use the Regex Helper tool available on your Logger. For details about the Regex Helper tool, refer to the ArcSight Logger Administrator's Guide.

Extract the IP address from any event that contains the word “failed” and show the top IP addresses:

```
failed | rex "(?<src_ip>[^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]" |  
top <src_ip>
```

Extract the network ID from an IP address:

The IP address is captured by the first rex expression and the network ID (assuming the first three bytes of the IP address represent it) to which the IP address belongs is extracted from the captured IP address:

```
error | rex "(?<src_ip>[^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]" |  
rex field=src_ip "(?<net_id>\d{1,3}\.\d{1,3}\.\d{1,3})"
```

Extract all URLs from events and generate a chart of the URL counts, excluding blank URLs:

```
http | rex "http://(?<customURL>[^\s]*)" | where customURL is not  
null | chart _count by customURL | sort - _count
```

Extract the first word after the word “user” (one space after the word) or “user=”:

The word “user” is case-insensitive in this case and must be preceded by a space character. That is, words such as “ruser” and “suser” should not be matched.

```
user | rex "\s[u|U][s|S][e|E][r|R][\s|=](?<CustomUser>[^\s]*)" |  
chart _count by CustomUser
```

