

Quick Start Guide

HP ArcSight Logger™ 5.3 - Downloadable Version

August 24, 2012



Quick Start Guide

HP ArcSight Logger™ 5.3 - Downloadable Version

Copyright © 2012 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.

This document is confidential.

Revision History

Date	Product Version	Description
08/24/2012	5.3	Updated for Logger 5.3.
12/09/2011	5.2	Updated for Logger 5.2.
05/31/11	5.1	Updated for Logger 5.1.
11/10/10	5.0 Patch 2	Removed Patch 1 upgrade info, as that info is now in the release notes. This guide is specific to fresh installs only.
10/12/10	5.0	Included information about installing 5.0 Patch 1.
09/17/10	5.0	First version of the guide for Logger software.

Document template version: 1.0.5

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

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	9
Before You Install	9
Supported Platforms and Browsers	9
Downloading the Installation Package	10
How Licensing Works	10
Installing and Configuring Logger	11
Prerequisites for Installation	11
Installation Modes	11
Installing Logger	12
Connecting to Logger for the first time	18
Starting and Stopping Logger	19
Uninstalling Logger	21
Chapter 3: Receiving Events and Logs	23
Enabling the Preconfigured Receivers	23
Configuring New Receivers	25
Sending Structured Data to Logger	25
Configuring a SmartConnector to Send Events to Logger	25
Chapter 4: Overview of the Logger User Interface	27
Navigating the User Interface	27
Help	28
Options	28
Logout	28
Summary	29
Dashboards	29

Chapter 5: Searching for Events	31
Example Queries	31
Syntax of a Query	31
Building a Query	32
Run a Query	33
Query Building Tools	33
Exporting Search Results	34
Saving Queries for Later Use	34
System Filters (Predefined Filters)	35
Tuning Search Performance	35
Chapter 6: Alerts	37
Types of Alerts	37
Configuring Alerts	38
Chapter 7: Other Logger Features	39
Reports	39
Scheduling Tasks	39
Archiving Events	39
Access Control on Logger Users	40
Chapter 8: Example Queries	41

About this Guide

This guide enables you to download, install, and use the downloadable version of HP ArcSight Logger™ in 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 install and start using Logger quickly. If you need an in-depth understanding of Logger or any of its features, refer to the online Help available with the product or the HP ArcSight Logger Administrator's Guide.

Chapter 1

Overview

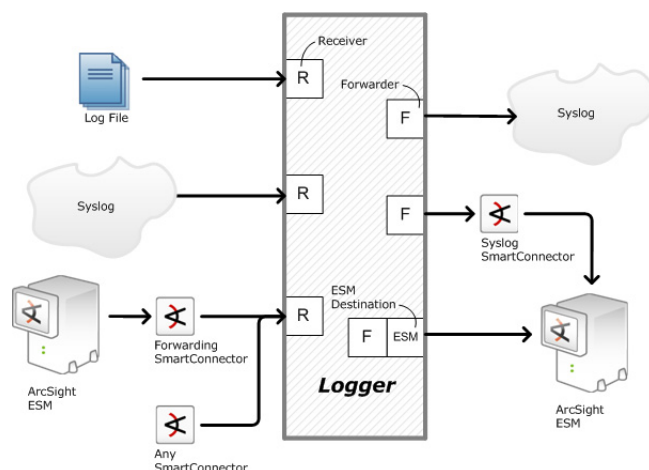
HP ArcSight Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events;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

Logger is available in two form factors: an appliance and software. The appliance-based solution is a hardened, dedicated, enterprise-class system that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. The software solution can be installed on a supported platform or a VM image of a supported platform of your choice. Both form factors offer identical features and require a valid license file to install and configure.

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 HP ArcSight SmartConnectors, syslog messages, and log files directly from a device. 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 command event format (CEF).



Logger can forward received events to ArcSight ESM Manager or a syslog server.

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 to 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

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. For example, unsuccessful login attempts, the number of events by source, SSH authentications on UNIX servers, special privileges assigned to new logon on Windows, and so on. As a result, you don't need to define queries to search for commonly searched events. Additionally, you can 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 HP ArcSight Logger Administrator's Guide. Information about how to use predefined filters is included in "[System Filters \(Predefined Filters\)](#)" on page 35.

Chapter 2

Installing and Configuring

Before You Install

Ensure the following before you begin installing Logger:

- You are installing Logger on a supported platform.
- You have received a license file in an e-mail from HP. This license is required to complete the installation. This file is automatically sent to you when you download the Logger installation package.

Supported Platforms and Browsers

You can install the software Logger on a platform with the following specifications. For a detailed capacity planning guide, see the Capacity Planning for Software Version of Logger document that is available for download from the Protect 724 Community at <https://protect724.arcsight.com>.

A VM installation of the operating systems listed in the table below is supported. HP strongly recommends allocating 4 GB RAM per VM instance. Additionally, the sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.

Specification	Details
Certified Operating Systems	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL), version 6.1, 64-bit• Oracle Enterprise Linux (OEL) 5.5, 64-bit• CentOS, version 6.1, 64-bit
Other Supported Operating Systems	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL), version 5.5, 64-bit
Browsers	<p>Refer to the Release Notes for up-to-date information on supported browsers for your version.</p> <p>An Adobe Flash Player plug-in is required on these browsers for some of the features, such as Histogram and charts, to work.</p>

Specification	Details
CPU, Memory, Disk Space	<p>For the Downloadable Version</p> <ul style="list-style-type: none"> • CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4 - 12 GB (12 GB is recommended) • Disk Space: 10 GB (minimum) <p>For the Enterprise Version</p> <ul style="list-style-type: none"> • CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12 - 24 GB (24 GB is recommended) • Disk Space: 65 GB (minimum) <p>NOTES:</p> <ul style="list-style-type: none"> • The disk space needs to be on the partition where you will install the Logger software. • Using NFS as primary storage for events on the software Logger is not recommended. • The system on which you are installing the software Logger must not have more than two CPUs.
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install the software Logger.

Downloading the Installation Package

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

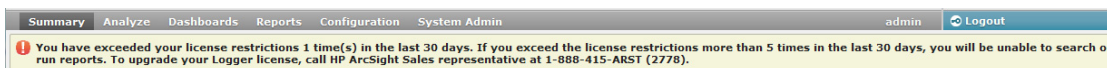
Once you have downloaded the package, you receive an e-mail from HP that contains the license file you will need to install Logger. A license file is uniquely generated for each download; therefore, you cannot use the same license file to install multiple instances of Logger.

How Licensing Works

A license for Logger defines the limits for the following:

- **Data limit:** A per day limit on the amount of incoming data. For example, 50 GB per day. The sum of the size of the original events is used to determine this value.
- **Storage limit:** The maximum storage for this Logger. For example 80 GB.

When a data limit violation occurs, the Search user interface displays a warning, as shown in the following figure.



For a detailed explanation of how licensing works, see the HP ArcSight Logger Administrator's Guide.

To confirm the specific limits that your license imposes, see the e-mail message with license-file attachment that you received from HP.

Installing and Configuring Logger

This section describes the prerequisites and the procedure for installing Logger.

Prerequisites for Installation

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

- You have a valid license file.
 - Make sure a non-root user account exists on the system on which you are installing Logger.
- You can be logged in as a root user or a non-root user on the system on which you are installing the software. Your installation options vary depending on which you choose.
- When you install as a root user, a non-root user account is still required.
 - When you install as a root user, 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.
 - If you are upgrading from a version prior to 5.1, you cannot change the previous install 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.
 - You must not have an instance of MySQL or PostgreSQL installed on the Linux machine on which you will install Logger. If instances of these exist on that machine, uninstall them before proceeding with the installation.
 - If you want to use the GUI mode of installation and will be installing Logger software over an SSH connection, 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 Linux machine.
 - Installation on 64-bit systems requires `glibc-2.12-1.25.el6.i686` and `nss-softokn-freebl-3.12.9-3.el6.i686`. Install these packages if the installation fails with the following error message, "Installation requirements not met. Pre-install check failed: 32-bit compatibility libraries not found."

Installation Modes

The 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.
- Console—In this mode, a command-line process steps you through the installation and configuration of software Logger.
- 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.

The Console and Silent installation modes are not discussed in this document. Please refer to the HP ArcSight Logger Administrator's Guide for the version you are installing.

Installing Logger

This section only describes the GUI mode of installation. The other two modes are discussed in the HP ArcSight Logger Administrator's Guide for the version you are installing.

Make sure the machine on which you will be installing the software Logger complies with the requirements listed in ["Supported Platforms and Browsers" on page 9](#) and the prerequisites listed in ["Prerequisites for Installation" on page 11](#) are met.

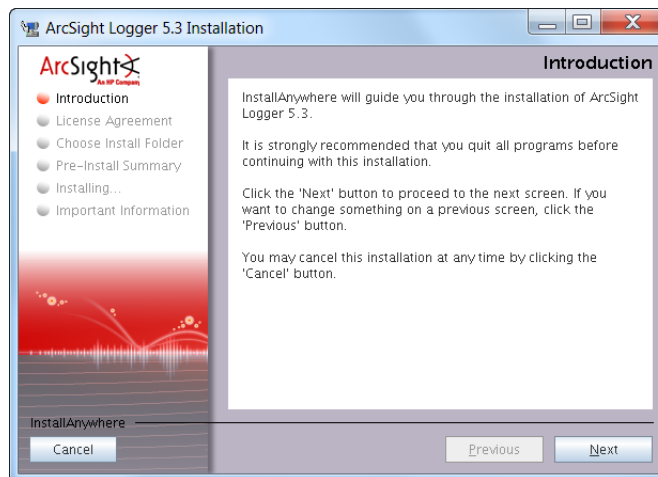
You can install software Logger as a root user or as a non-root user. See ["Prerequisites for Installation" on page 11](#) for details and restrictions.

To install the software Logger using the GUI mode:

- 1 Run these commands from the directory where you copied the Logger software:

```
chmod +x ArcSight-logger-5.3.0.XXXX.0.bin
./ArcSight-logger-5.3.0.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.



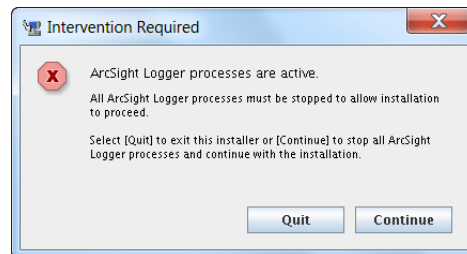
Caution

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.

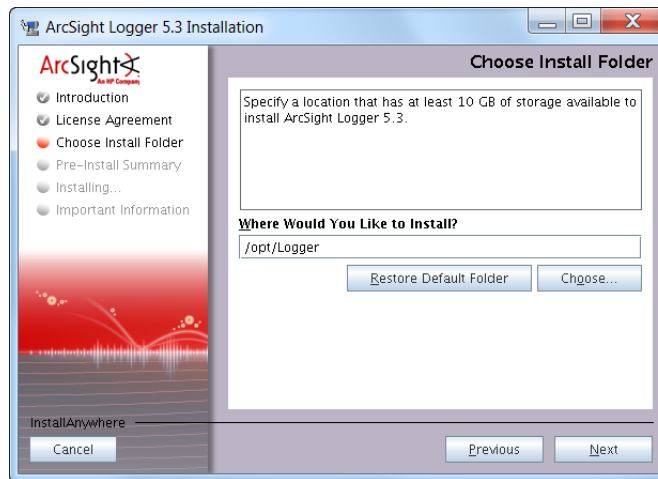


- 4 Select **I accept the terms of the License Agreement** and click **Next**.
- 5 If Logger is currently running on this machine, an Intervention Required message is displayed. Click **Continue** to stop all current Logger processes and proceed with the installation, or click or **Quit** to exit the installer.



The installer stops the running Logger processes and checks for other installation prerequisites. A message is displayed asking you to wait. 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. By default, the /opt directory is specified.

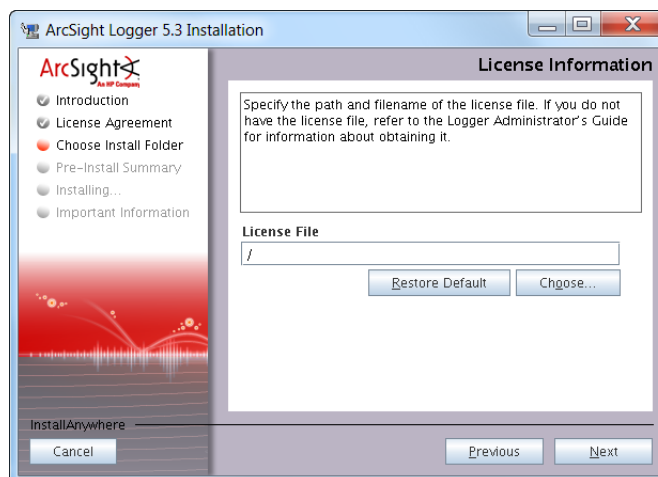


Note

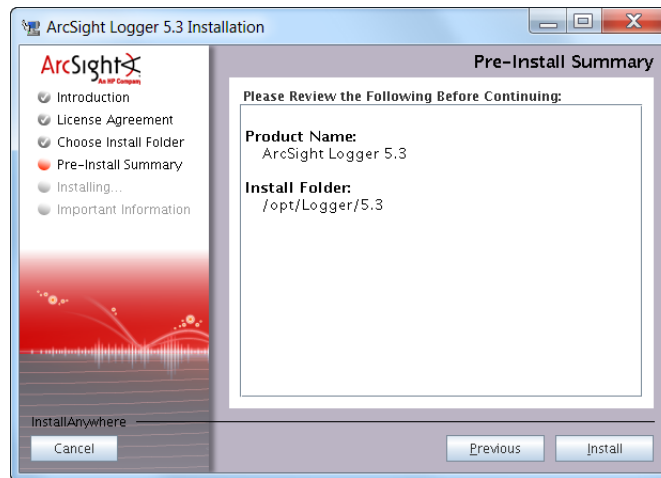
The user you are installing with must have access to the parent directory of the install directory. Otherwise, users will not be able to connect to the Logger UI and will see the following error message when they try to connect:

```
"Error 403 Forbidden. You don't have permission to access / on
this server"
```

- 7 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 **Back** to specify another location or **Quit** to exit the installer.
- 8 If Logger is already installed at the location you specify, a message is displayed. Click **Upgrade** to continue or **Back** to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.
- 9 Navigate to or specify the path and filename of the license file for this software Logger, and click **Next**.



10 Review the pre-install summary and click **Install**.



11 Installation may take a few minutes. Please wait.



Once installation is complete, the next screen is displayed.

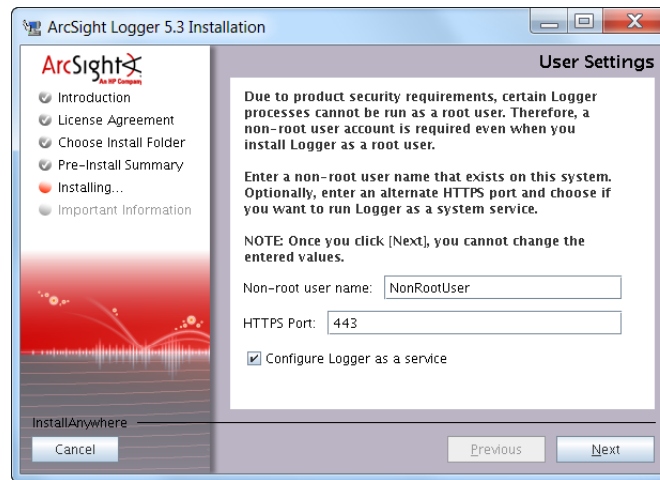
12 If you are logged in as a root user on the system on which you are installing Logger software, in the next screen you need to:

- ◆ Specify a non-root user. (This user must already exist on the system.)
- ◆ Configure a HTTPS port number for your users to access the Logger UI.

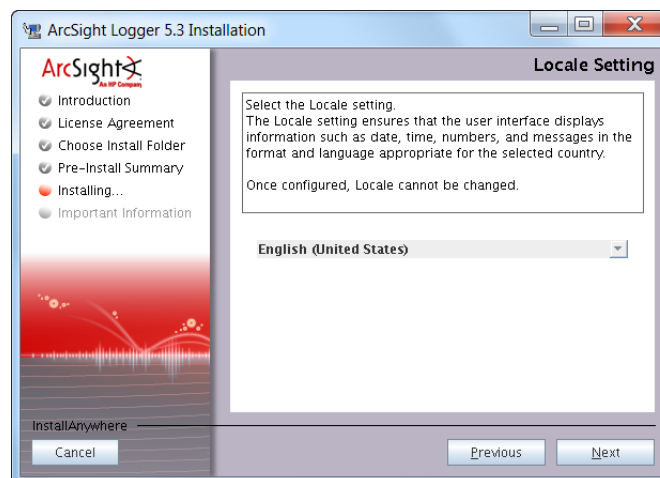
You can use the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, your users will need to enter that port number in the URL they use to access the Logger UI.

Specify whether to configure Logger to run as a service. If you select this option, the initialization will create a service called `arcsight_logger`, and enable it to run at levels 2, 3, 4, and 5.

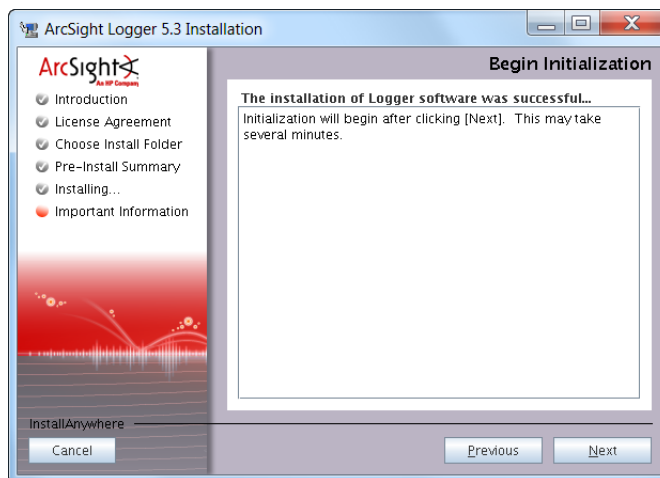
- ◆ Click **Next**.



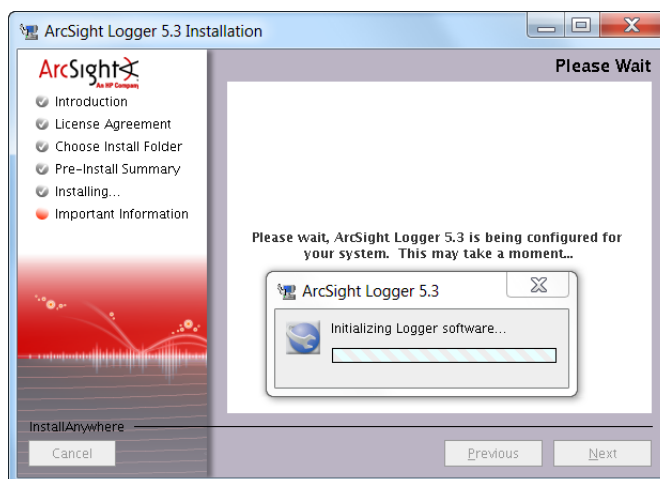
- 13 Select the locale of this installation and click **Next**.



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

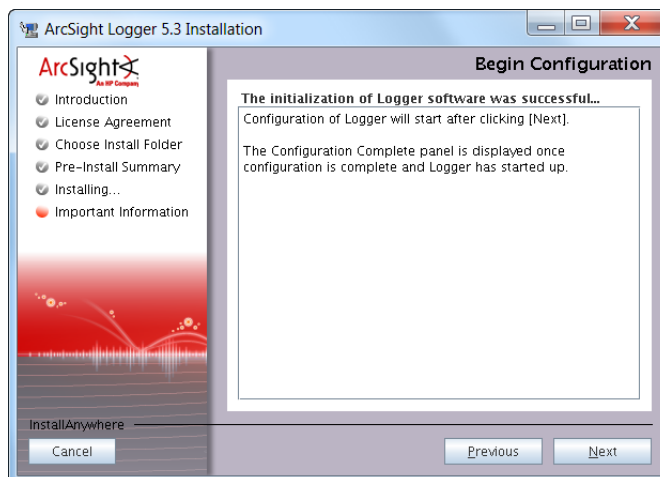


Initialization may take a few minutes. Please wait.

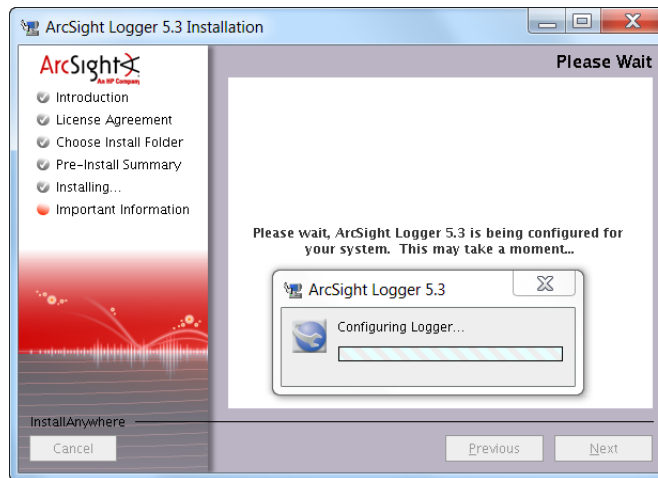


Once initialization is complete, the next screen is displayed.

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

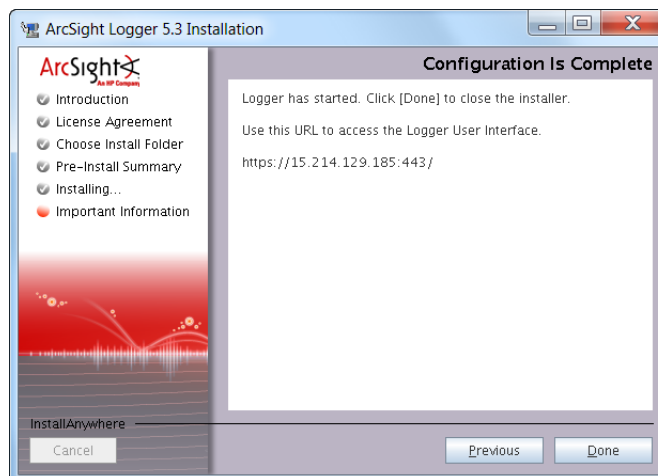


Configuration may take a few minutes. Please wait.



Once configuration is complete, Logger starts up and the next screen is displayed.

- 16** Click **Done** to exit the installer.



- 17** Now that you are done installing and initializing your Logger, connect to it by following the instructions in "Connecting to Logger for the first time" on page 18.

Connecting to Logger for the first time

Logger works with most browsers, including Firefox and Internet Explorer. JavaScript and cookies must be enabled. An Adobe Flash Player plug-in is required for Internet Explorer browsers that access the Logger user interface. 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>.

The Logger user interface is a web browser application using Secure Sockets Layer (SSL) encryption. Users must be authenticated with a name and password before they can use the interface. Refer to the Release Notes document to find out the browsers and their versions supported for this release.

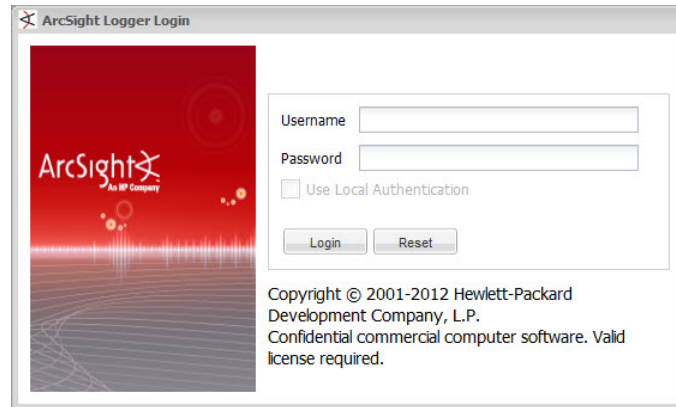
To connect and log into Logger:

- 1 Use the following URL 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 specified during the Logger installation.

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:

- 3 Username: `admin`
 Password: `password`

For more information about the log in screen and connecting to Logger, refer to the HP 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 *HP 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 23](#) for information on how to set up your Logger to start receiving events.

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, use the `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>}

/etc/init.d/service arcsight_logger {start | stop | status}
```

The following screen shot lists the processes that can be started, stopped, or restarted with loggerd.

Process Status

Refresh Status

System section Processes section

System	Status	Log	CPU Usage	Memory Usage	Data Collected
mutsumt55122 / arcsight.com	running		[0.75] [0.66] [0.58]	14.8%us 3.6%sy 1.2%wa	28.2% [1603580 KB]

NOTE: This Start/Stop buttons are for diagnostic purposes. Please use them with care.

Process	Status	Uptime	CPU Usage	Memory Usage
apache	running	14m	0.0%	0.1% [7400 KB]
Children		14		
CPU Percent		0.0%		
CPU Percent Total		0.0%		
Data Collected		09/10/2010 14:26:34		
Memory Kilobytes		7400		
Memory Kilobytes Total		72464		
Memory Percent		0.1%		
Memory Percent Total		1.1%		
Monitoring Status		monitored		
Parent PID		1		
PID		20244		
Status		running		
Uptime		14m		
aps	running	14m	0.2%	3.5% [219336 KB]
connector	running	15m	0.0%	0.0% [560 KB]
inasp	running	15m	0.0%	0.3% [16992 KB]
mysqld	running	15m	0.0%	0.3% [20520 KB]
postgresql	running	15m	0.0%	0.1% [9192 KB]
processors	running	14m	0.0%	0.9% [56452 KB]
receivers	running	13m	0.0%	0.5% [34232 KB]
reportengine	running	14m	0.0%	3.0% [188256 KB]

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 current 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

Command	Purpose
<code>loggerd restart</code> <code><process_name></code>	Restart the named process. For example, <code>loggerd restart apache</code>

Uninstalling Logger

If you will be uninstalling Logger software over an SSH connection in 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 software Logger, enter this command in the directory where you installed the software Logger:

```
./UninstallerData/Uninstall_ArcSight_Logger_5.3
```

The uninstall wizard is launched. Click **Uninstall** 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 are supported 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 HP ArcSight SmartConnectors, visit <http://www.arcsight.com>.

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. The UDP Receiver is on port 514 for Logger appliances. For software Logger, if you are installing 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.
- A TCP receiver—Enabled by default. The TCP receiver is on port 515 for Logger appliances. For software Logger, if you are installing 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.
- 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.

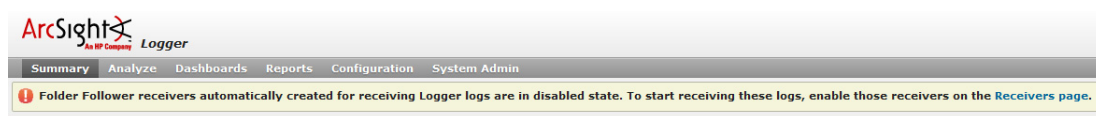
The preconfigured folder follower receivers include:

- Var Log Messages—`/var/log/messages`
- Audit Log—`/var/log/audit/audit.log`
- Apache URL Access Error Log—`<install_directory>/current/local/apache/logs/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, Logger will display a banner like the one below, telling you about the disabled receivers.



Click the link in the banner to open the Receivers page.

Receivers
Source Types
Parsers

Add

Logger can receive its HTTP error logs from the `<install_dir>/current/local/apache/logs/http_error_log` file when the automatically created Folder Follower receiver for the file is enabled.

Additionally, Logger can receive logs from the `messages` and `audit.log` files in the `/var/log/*` folders. Before enabling the receivers for these files, consult the [Logger Administrator's Guide](#) for additional details.

Name	Type	IP Address	Port			
Apache URL Access Error Log	Folder Follower Receiver					
Audit Log	Folder Follower Receiver					
SmartMessage Receiver	SmartMessage Receiver					
TCP Receiver	TCP Receiver	All	515			
UDP Receiver	UDP Receiver	All	514			
Var Log Messages	Folder Follower Receiver					

Before enabling the receivers, make `/var/log/audit/audit.log` and `/var/log/messages` readable by the non-root user you install with or specify 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 Click **Configuration** or **Configuration > Settings** from the top-level menu bar.
- 2 Click **Event Input** (left panel) > **Receivers** tab (right panel).
- 3 Click the disabled icon () at the end of the 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 HP 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 preinstalled UDP receiver is enable 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 preinstalled TCP receiver is enable 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 preinstalled 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 25](#).

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. For more information about CEF, see the HP ArcSight Logger Administrator's Guide.

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

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** If you are using the Downloadable Version of Software Logger, refer to the documentation that came with your Smart Connector for instructions.

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 a 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.

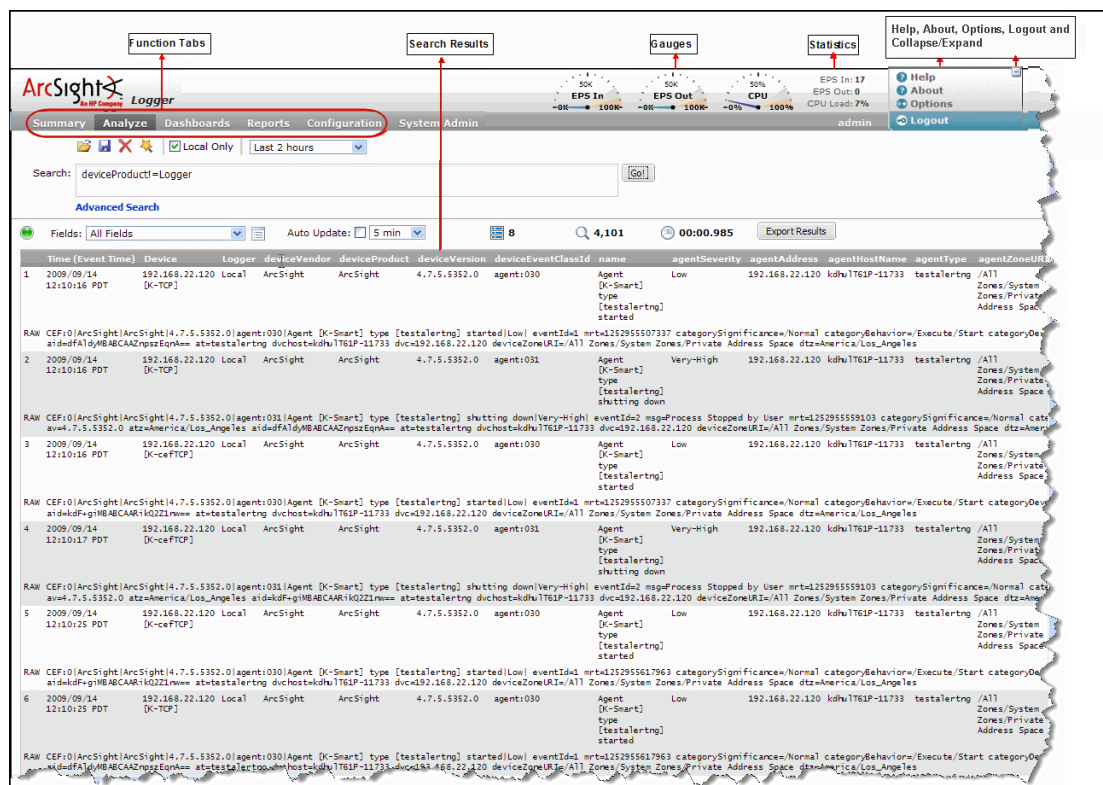
For more information about the Common Event Format (CEF), refer to Implementing ArcSight CEF on <https://protect724.arcsight.com/docs/DOC-2611>.



Overview of the Logger User Interface

This section provides a high-level view of the Logger User Interface, with an emphasis on the Search user interface. For more information and for user interface options not discussed in this section, refer to the HP 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 29). The range of the gauges can be changed on the Options page. The current logged-in user's name is shown below the statistics. The gauge and logo bar can be collapsed to allow more room on the screen for search results and reports. Click the  icon to collapse the bar, and the  icon to expand it.

The menu list in the upper right includes links for Help, Options, and Logout.

Help

Clicking the Help link on any page displays online help for the current page. In addition, Search Helper, a search-specific utility is available that provides search history, search operator history, examples, suggested next operators, and list of fields and operators.

Options

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.

Additionally, the default start page (home page) for all users and specific start pages for individual users can be set on the Options page. These pages indicate which user interface page is displayed after a user logs in.

Options

System

EPS input rate gauge max 100K

EPS output rate gauge max 100K

Default start page for all users Dashboards

Personal

Default start page for admin Use default for all users

Save Cancel

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 HP 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.

Summary Analyze Dashboards Reports Configuration System Admin admin Logout

Global Summary

There are 3,727,905 events indexed from 2011/10/26 13:38:32 to 2011/11/06 06:55:13.

The tables lists all of the data loaded into the Logger since started.

Receivers

Page 1 of 2 | Displaying 1 - 10 of 12

Receiver	Count	Most Recent
tcp2	751,127	2011/11/02 09:06:43
tcp6	608,918	2011/11/02 10:30:56
Logger Internal Event Device	608,825	2011/11/06 06:55:13
tcp5	597,436	2011/11/02 10:37:22
tcp4	494,087	2011/11/02 08:12:15
tcp1	263,758	2011/11/02 09:06:43
tcp7	185,593	2011/10/28 11:18:02
tcp3	82,815	2011/11/02 09:01:48
udp1	71,370	2011/11/03 10:04:48
tcp8	63,846	2011/11/02 10:35:52

Devices

Page 1 of 1 | Displaying 1 - 5 of 5

Device	Count	Most Recent
192.168.35.16	3,047,241	2011/11/02 10:37:22
127.0.0.1	608,825	2011/11/06 06:55:13
192.168.37.21	71,263	2011/11/03 10:04:48
192.168.35.6	556	2011/11/02 09:06:43
10.4.10.196	20	2011/10/26 13:55:13

Agent Severities

Page 1 of 1 | Displaying 1 - 6 of 6

Agent Severity	Count	Most Recent
1	68,402,531	2011/11/06 06:55:13
3	1,049,961	2011/11/06 06:31:11
2	508,768	2011/11/03 10:04:47
Medium	126,872	2011/11/02 10:30:13
5	52,835	2011/11/03 10:16:00
Low	20,290	2011/11/02 10:30:13

Agent Types

Page 1 of 1 | Displaying 1 - 1 of 1

Agent Type	Count	Most Recent
checkpointfirewall_ad_opsec	1,595	2011/11/02 10:30:13

Dashboards

Dashboards are an all-in-one view of the Logger information of interest to you. 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 for status at-a-glance.

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 HP 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. For example, unsuccessful login attempts, the number of events by source, SSH authentications. Additionally, you might want to include matching events in a report, or forward them 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
192.0.2.120
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 or field-based expression | search operator
expression
```

- A keyword—a word expressed in plain English; for example, `failed`, `login`, and so on.
- A field-based expression—searching for fields of an event.

Examples:

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

A complete list of fields is available in the HP ArcSight Logger Administrator's Guide.

- A search operator expression—an expression that uses search operators such `chart`, `head`, `tail`, `top`, `rare`, and so on to refine the data that matches the expressions specified by the keyword and the field-based expression.

Search operators—The following is a list of all the search operators:

```
chart, eval, fields, head, rare, regex, sort, tail, top, where
```

Extraction operators—The following two are special operators that are used to extract fields from matching events. The search operators act on these extracted fields, as shown in the examples below.

```
cef, rex
```

For detailed usage and examples of the above listed operators, refer to the HP ArcSight Logger Administrator's Guide.

Examples:

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

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

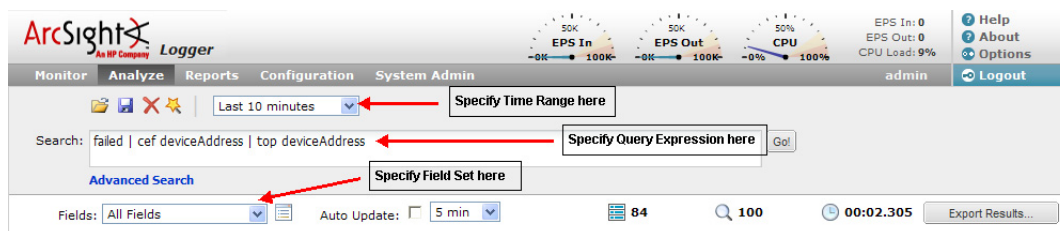
Displays search results in a tabular form of the most common values for the `deviceAddress` field. That is, the values are listed from the highest count value to the lowest.

```
failed | cef deviceAddress | top deviceAddress
```

Building a Query

When you build a query, the following elements need to be specified:

- Query Expression—search conditions that are used to select or reject an event.
- Time range—the time range within which events should be searched.
- Field Set—fields of an event that should be displayed 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 HP 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 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 *HP ArcSight Logger Administrator's Guide*.

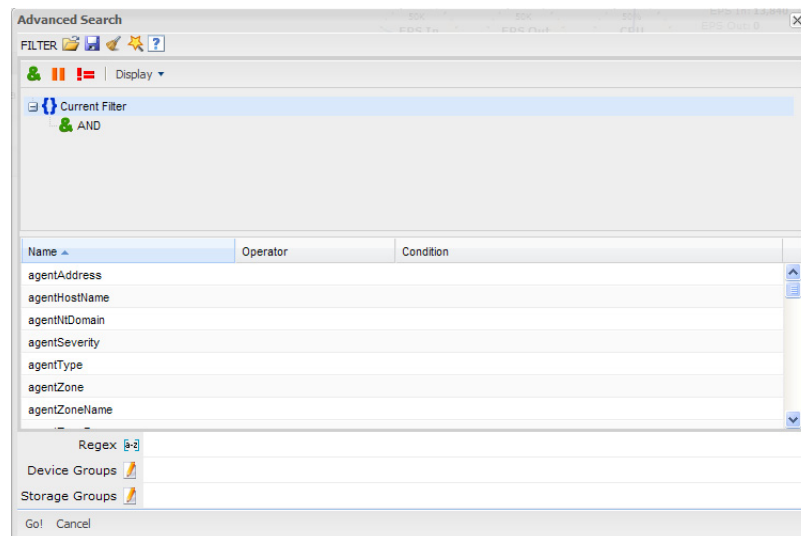
Query Building Tools

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 quickly and accurately build search queries. 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 HP ArcSight Logger Administrator's Guide.



■ Regex Helper

Creating regular expression for the rex extraction operator can be complex and error prone. The Regex Helper tool enables you to create regular expressions that can be

used 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 HP 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 that is currently 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 `cef`, `rex`, `extract`, or `regex`.
- ◆ Help—Provides context-sensitive help for the last-listed operator in the query that is currently typed in the Search text box.
- ◆ List of Fields and Operators—Depending on the current query 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.

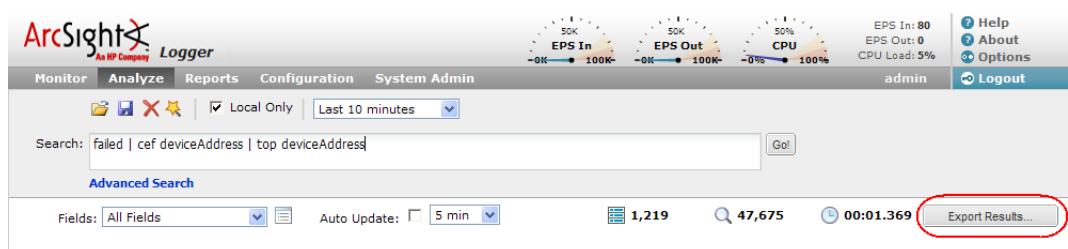
Exporting Search Results

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** in the top right-hand side of the search results screen.



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.

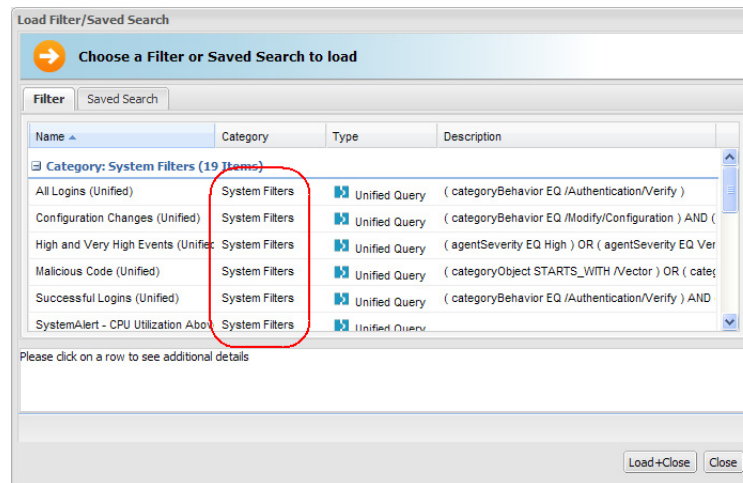
For more information about saving queries and using them again, refer to the HP ArcSight Logger Administrator's Guide.

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. For example, 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 impact search performance are listed below. To optimize search performance, ensure that you follow these recommendations:

- Enable full-text and field-based indexing. When events are indexed, Logger can quickly and efficiently search for relevant data.
- The amount of time it takes to search depends on the size of the data set that needs to 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 within which the events must be searched does not result in a query that needs to scan multi-millions of events. Additionally, limiting search to specific storage groups typically results in better search performance than when the storage groups are not specified.
- Reduce other load on the system when your query needs to run, such as scheduled jobs, large number of incoming events, multiple reports being run.

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 triggers, an alert event is logged on the Logger and a notification is sent through previously configured destinations.

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 are defined.	Any number of alerts can be defined. All defined alerts are enabled and effective, however, a maximum of 50 alerts can run concurrently.
A maximum of five alerts can be enabled at any time.	
No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination.	No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination.
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 occur within the specified threshold, an alert is immediately triggered.	These alerts are triggered at scheduled intervals. That is, when a specified number of matches occur within the specified threshold, an alert is triggered at the next scheduled time interval .

Real Time Alerts

To define a real time alert, you specify a query, match count, threshold, and one or more destinations.

A time range is not associated with the queries defined for these alerts. Therefore, whenever the specified number of matches occur within the specified threshold, an alert is triggered.

Saved Search Alerts

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.

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).

For example, if a Saved Search query has these start and end times:

Start Time: 5/11/2010 10:38:04

End Time: 5/12/2010 10:38:04

And, the number of matches and threshold are the following:

Match Count: 5

Threshold: 3600

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.

Configuring Alerts

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

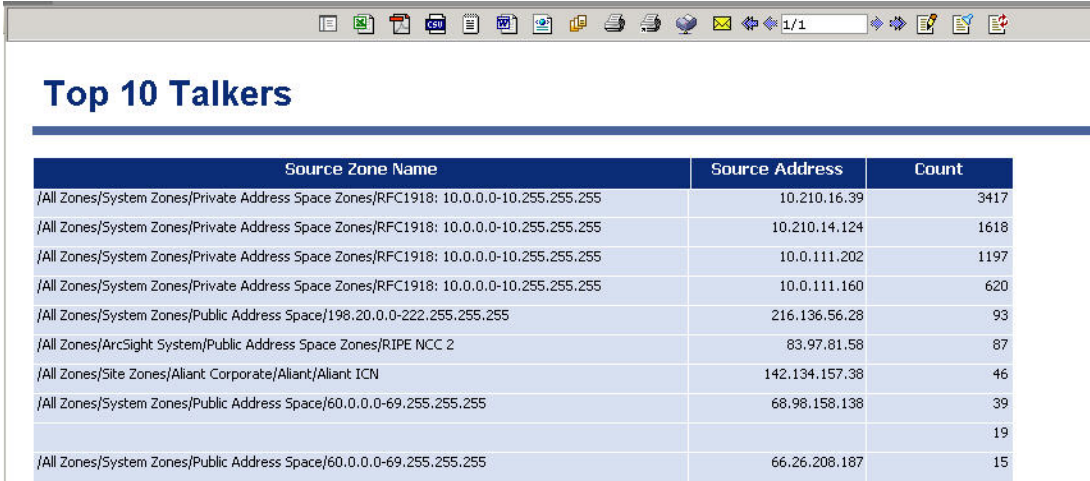
Chapter 7

Other Logger Features

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

Reports

Logger enables you to generate and export reports on events stored on your Logger. In addition to writing your own reports, you can use the predefined reports that exist on the Logger for common security and device monitoring use cases. The report output is displayed in the format—HTML, PDF, other—you choose. You can save the report output to a file or e-mail to other users.



The screenshot shows a web browser window displaying a report titled "Top 10 Talkers". The report is a table with three columns: "Source Zone Name", "Source Address", and "Count". The table lists the top 10 source zones based on the number of events (count). The data is as follows:

Source Zone Name	Source Address	Count
/All Zones/System Zones/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.210.16.39	3417
/All Zones/System Zones/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.210.14.124	1618
/All Zones/System Zones/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.0.111.202	1197
/All Zones/System Zones/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255	10.0.111.160	620
/All Zones/System Zones/Public Address Space/198.20.0.0-222.255.255.255	216.136.56.28	93
/All Zones/ArcSight System/Public Address Space Zones/RIPE NCC 2	83.97.81.58	87
/All Zones/Site Zones/Alliant Corporate/Alliant/Alliant ICN	142.134.157.38	46
/All Zones/System Zones/Public Address Space/60.0.0.0-69.255.255.255	68.98.158.138	39
		19
/All Zones/System Zones/Public Address Space/60.0.0.0-69.255.255.255	66.26.208.187	15

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.

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, while Jane has Logger search and reporting capabilities.

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 *HP 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
```

