

Quick Start Guide

ArcSight Logger™ 5.1 - Downloadable Version

May 31, 2011



Quick Start Guide ArcSight Logger™ 5.1 - Downloadable Version

Copyright © 2010-2011 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
05/31/11	version 5.1	Updated for Logger v5.1.
11/10/10	version 5.x	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	version 5.0	Included information about installing v5.0 Patch 1.
09/17/10	version 5.0	First version of the guide for Logger software.

Document template version: 1.0.5

ArcSight Customer Support

Phone	1-877-900-ARST (North America)
E-mail	loggersupport@arcsight.com
Protect 724 Community	https://protect724.arcsight.com
Documentation	https://arcsight.subscribenet.com

Contents

About this Guide	v
Chapter 1: Overview	1
How Logger Works	1
Logger for Security, Compliance, and IT Operations	2
Next Steps	2
Chapter 2: Installing and Configuring	3
Before You Install	3
Supported Platforms and Browsers	3
Downloading the Software	4
How Licensing Works on the Software Logger	4
Installing and Configuring the Software	5
Prerequisites for Installation	5
Installation Modes	6
Installation Steps	6
Using the GUI Mode to Install Software Logger	6
Connecting to the Software Logger User Interface	14
Starting and Stopping Logger	14
Uninstalling the Logger Software	16
Applying a New License on the Software Version of Logger	16
Enabling or Disabling Logger as a System Service	17
Best Practices for the Minimal Install	18
Next Steps	18
Chapter 3: Overview of the Logger User Interface	19
Connecting to the Logger User Interface	19
Browser Requirements	20
Navigating the User Interface	20
Help	20
Options	21
Logout	21

Chapter 4: Receiving Events and Logs	23
Receiver Name and Type	23
Receiver Parameters	24
Configuring a Syslog Receiver for Receiving Events on Logger	24
Sending CEF Events to Logger	25
Chapter 5: Searching for Events	27
Example Queries	27
Syntax of a Query	27
Building a Query	28
Run a Query	29
Query Building Tools	29
Exporting Search Results	30
Saving Queries for Later Use	31
System Filters (Predefined Filters)	31
Tuning Search Performance	32
Chapter 6: Alerts	33
Types of Alerts	33
Configuring Alerts	34
Chapter 7: Other Logger Features	35
Reports	35
Scheduling Tasks	35
Archiving Events	35
Access Control on Logger Users	36
Chapter 8: Example Queries	37

About this Guide

This guide enables you to download, install, and use the software version of 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.

Chapter 1

Overview

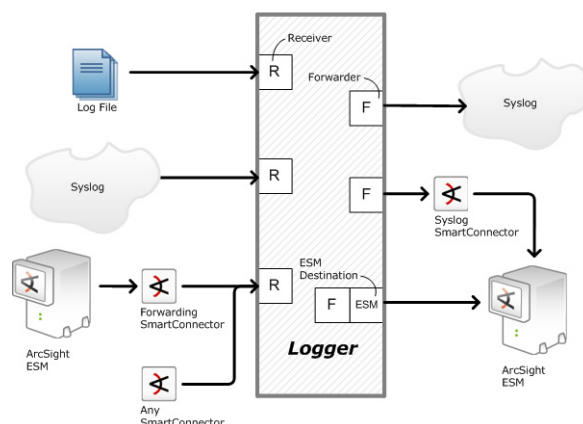
Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events; supports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



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 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
- Generate reports of events of interest
- 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, see the Logger Administrator's Guide. Information about how to use predefined filters is included in ["System Filters \(Predefined Filters\)" on page 31](#).

Next Steps

Install and configure the Logger software using information in the next section, ["Installing and Configuring" on page 3](#).

Chapter 2

Installing and Configuring

Before You Install

Ensure the following before you begin installing the Logger software:

- You are installing the software on a supported platform. See [“Supported Platforms and Browsers” on page 3](#) for more information.
- You have received a license file in an email from ArcSight. This license is required to complete the installation. This file is automatically sent to you when you download the software.

Supported Platforms and Browsers

You can install the software version of Logger on a platform with the following specifications.

A VM installation of the operating systems listed in the table below is supported. ArcSight 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 5.4 and 5.5, 64-bit• Oracle Enterprise Linux (OEL) 5.4, 64-bit• CentOS, versions 5.4 and 5.5, 64-bit
Other Supported Operating Systems	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL), version 4.x, 64-bit• Oracle Enterprise Linux (OEL) 5.5, 64-bit• CentOS, version 4.x, 64-bit

Specification	Details
CPU, Memory, Disk Space	<p>For Small Deployments <i>(Only for ArcSight Logger—Downloadable Version)</i></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 Medium to Large Deployments</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: 120 - 400 GB (400 GB is recommended) <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 version of Logger is not recommended. The system on which you are installing the software version of Logger must not have more than two CPUs.
Browsers	<ul style="list-style-type: none"> Internet Explorer: Versions 7 and 8 Firefox: Versions 3.5 and 3.6 <p>An Adobe Flash Player plug-in is required on these browsers for some of the features, such as Histogram and charts, to work. Additionally, make sure that the SSLv3 or TLSv1 option is enabled to access the software Logger user interface.</p>
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install the software version of Logger.

Downloading the Software

The software for Logger is available for download from the ArcSight Customer Support web site at <http://www.arcsight.com/products/products-logger/>.

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



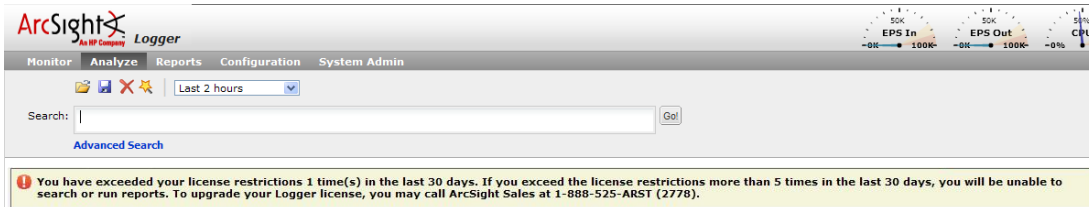
You must use the Installation Wizard as described in "Installation Steps" on [page 6](#) to install software Logger. Using the console mode for installing software Logger is not supported.

How Licensing Works on the Software Logger

A license for the software Logger defines the limits for the following:

- **Data limit:** A per day limit on the amount of incoming data. For example, 20 GB per day. The sum of the size of the original events is used to determine this value.
- **Aggregated storage limit:** A limit on the aggregated storage—the sum of storage used to store incoming events and the storage consumed due to retention—used on the 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 *Logger Administrator's Guide*. To learn about the specific limits that your license imposes, see the e-mail message with license-file attachment that you received from ArcSight.

Installing and Configuring the Software

Prerequisites for Installation

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

- You received a license file from ArcSight. The file is attached to an email that you received from ArcSight after downloading the Logger software. You will need this file for installation.
- You can be logged in as a root user or a non-root user on the system on which you are installing the software. When you install the software as a root user, you can select the port on which Logger listens for secure web connections. However, when you install it as a non-root user, Logger can only listen for connections on port 9000. You cannot configure the port to a different value. Additionally, you can configure Logger to start as a service when you install as a root user.

The ability to install as a root user is new in version 5.1; only non-root user installation was supported prior to this release. Therefore, if you are upgrading from a previous version of Logger 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. A non-root user account is still required to complete the Logger installation as a root user. Therefore, make sure a non-root user account exists on the system on which you are installing 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.
- Ensure that the umask setting in the `/etc/bashrc` file and your local `.bashrc` file has not been modified on the system which you are installing the Logger software. If this setting is modified, Logger might not function as expected.

If you want to use the GUI mode of installation (described in ["Installation Modes" on page 6](#)) 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 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. The installation using this mode is not discussed in this document. Please refer to *Logger v5.1 Administrator's Guide* for details.
- **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 installation using this mode is not discussed in this document. Please refer to *Logger v5.1 Administrator's Guide* for details.

Installation Steps

This section only describes the GUI mode of installation. The other two modes are discussed in the *Logger v5.1 Administrator's Guide*.

Using the GUI Mode to Install Software Logger



You can install software Logger as a root user or as a non-root user. See ["Prerequisites for Installation" on page 5](#) for details.

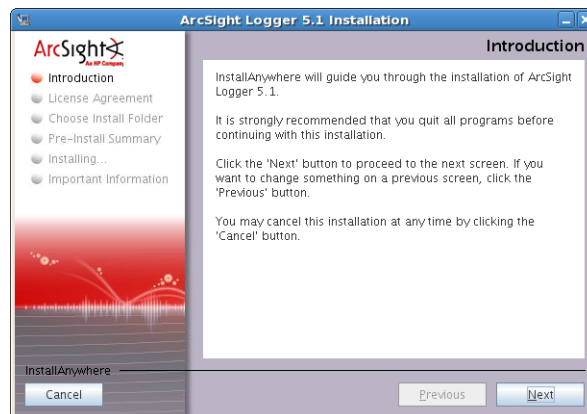
To install the software version of Logger using the GUI mode:

- 1 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 3](#) and the prerequisites listed in ["Prerequisites for Installation" on page 5](#) are met.
- 2 Run these commands from the directory where you copied the Logger software:

```
chmod +x ArcSight-logger-5.1.0.XXXX.0.bin
```

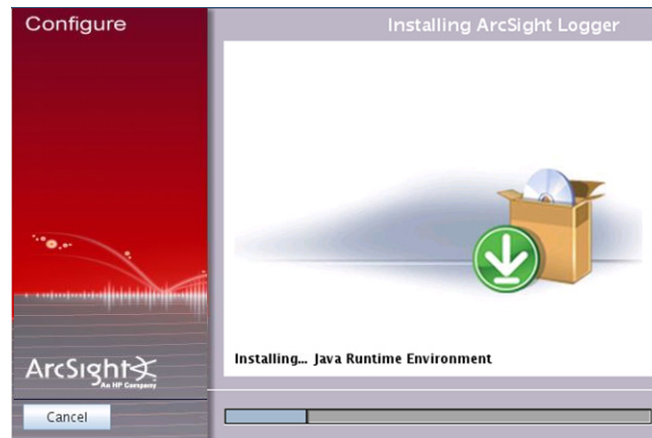
```
./ArcSight-logger-5.1.0.XXXX.0.bin
```

The installation wizard launches, as shown in the following figure. Click **Next**.



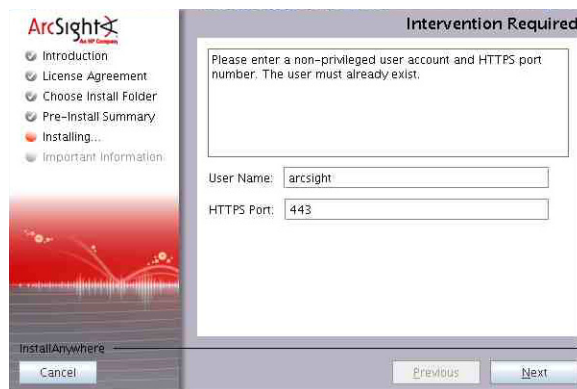
- 3 On the next screen, read through the License Agreement details. Click **I accept the terms of the License Agreement**. Then, click **Next**.

- 7 The Logger software begins to install, as shown in the following figure.

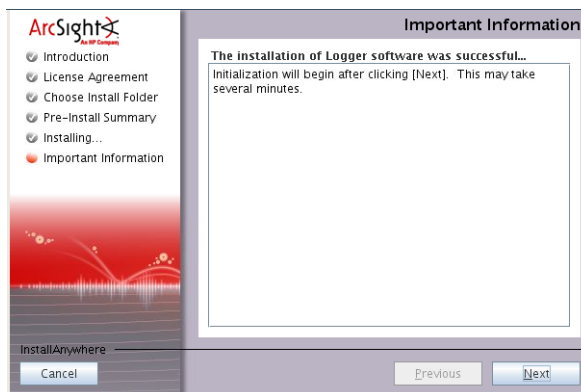


- 8 If you are logged in as a root user on the system on which you are installing Logger software, the following screen is displayed next. This screen enables you to specify a non-root user (that must exist on the system already) and configure a port on which Logger users will connect to it through the Logger UI. For example, you can enter 443, the standard HTTPS port, or any other that suits your needs. If any port except 443 is specified, your users will need to enter that port number in the URL they use to access the Logger UI.

Enter the user name of the non-root user and HTTPS port number, and click **Next**.



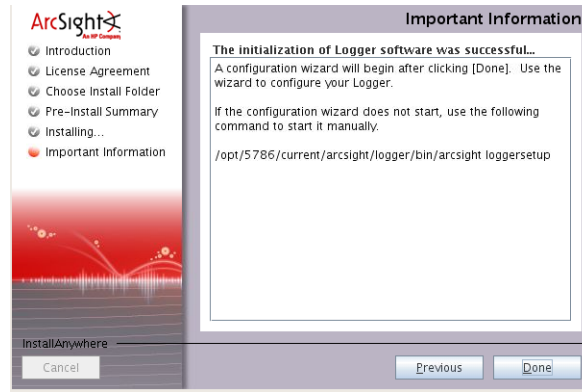
- 9 Once the software is installed, the following screen is displayed. Click **Next** to begin Logger initialization.




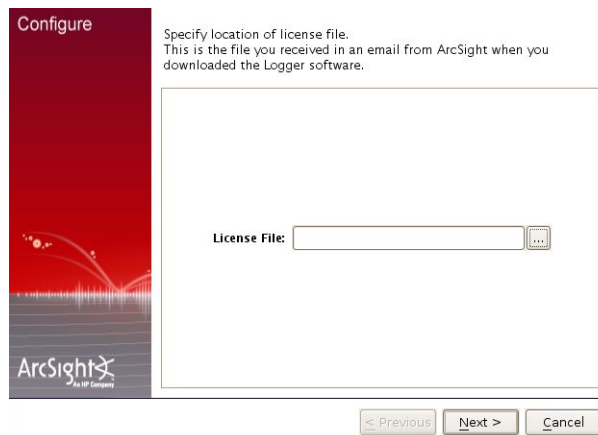
- 10** Once initialization is complete, the following screen is displayed. Click **Done** to launch the Logger Configuration wizard.

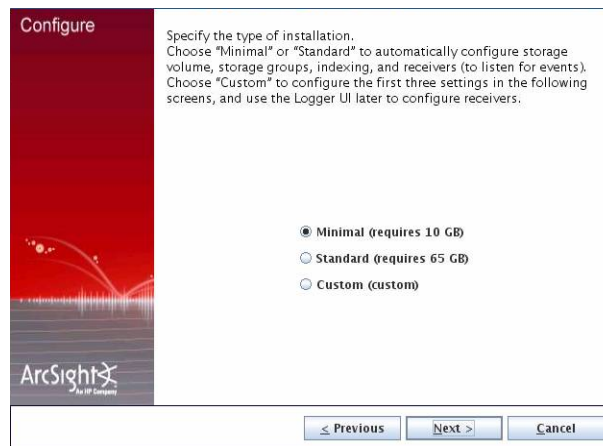
Note: The Configuration wizard launches automatically. However, if it does not, use this command to start it:

```
<install_dir>/current/arcsight/logger/bin/arcsight loggersetup
```



- 11** In the next screen, click the Browse () icon to locate the license file that you received from ArcSight. Click **Next**.



12 Select the type of installation.

You can select from these choices.

Setting	Minimal	Standard
Minimum Disk Space Required	10 GB	65 GB
Storage Volume	10 GB	65 GB
Storage Groups	2	6
Indexing	Full-text and field-based	Full-text and field-based
Receivers	2	2

- ◆ *Minimal or Standard*—If you choose either of these options, storage volume, storage groups, indexing, and receivers (to listen for events) are automatically configured for you during the installation process using the default values listed in the above table.

The following guidelines provide additional information for the above listed settings:

- *Storage Volume:* If needed, you can increase the storage volume size later if additional disk space is available.
- *Storage Groups:* Only two storage groups can be configured for the Minimal installation type. Once configured, the number of storage groups cannot be increased. Therefore, if you choose Minimal installation, ensure that two storage groups will be sufficient for your needs.
- *Indexing:* All recommended fields are included in the index and full-text indexing is enabled. A complete list of fields is available in the *Logger Administrator's Guide*.
- *Receivers:* A TCP and a UDP receiver is automatically configured and enabled. Make sure your events sources are configured to send events to these receivers on the ports that the configuration wizard displays after this step. You can add more receivers or modify the automatically configured ones later using the Logger user interface.
- ◆ *Custom*—If you choose this option, you need to configure indexing, storage groups, and the storage volume size, as described in the next step. For this type of installation, the receivers are configured using the Logger UI after the installation is complete.

13 If you selected "Custom":

- a** Enter the maximum size of the Storage Volume. Click **Next**.

The maximum size you enter can only be equal to or less than the aggregated storage size allowed by your license.

The screenshot shows the 'Configure' window with a red sidebar on the left containing the ArcSight logo. The main area is titled 'Specify size of Storage Volume.' and includes a descriptive paragraph: 'Storage Volume is where all event data is stored. You can increase the Storage Volume size after it has been created, but you cannot decrease it.' Below this is a text input field labeled 'Maximum Size (GB)' with the value '50' entered. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

- b** Add the storage groups to suit your needs. Click the Maximum Age (number of days to retain the event) and Maximum Size fields for each storage group you add and specify values. Click **Next**.

ArcSight recommends that you create the maximum allowed of four additional Storage Groups (in addition to the two that preexist—Default Storage Group and the Internal Storage Group) at this stage even if you do not need all of them because you cannot add storage groups later, although you can decrease or increase the size of a Storage Group at any time. Additionally, if you will not use all storage groups, keep the size of the spare groups to a minimum to optimize space for storage groups that you will use.

The screenshot shows the 'Configure' window with a red sidebar on the left containing the ArcSight logo. The main area is titled 'Specify Storage Groups and their retention policies.' and includes two bullet points: 'Once created, a storage group cannot be deleted, however its size can be changed.' and 'A Default Storage Group and an Internal Event Storage Group must always exist on Logger and are created automatically.' Below this is a table with three columns: 'Storage Group Name', 'Maximum Age (Days)', and 'Maximum Size (GB)'. The table lists six storage groups: Default Storage Group, Internal Event Storage ..., Long retention 1, Long retention 2, Short retention 1, and Short retention 2. Below the table are 'Add' and 'Remove' buttons. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

Storage Group Name	Maximum Age (Days)	Maximum Size (GB)
Default Storage Group	180	15
Internal Event Storage ...	365	5
Long retention 1	365	8
Long retention 2	365	8
Short retention 1	30	5
Short retention 2	30	5

- c** If you want to enable full-text indexing, click "Enable full text index".

Tip: ArcSight strongly recommends that you enable indexing because indexing significantly improves search and reporting performance. When you add fields to the index, search queries yield significantly faster results.

Select the fields you want to index. You can drag and drop fields from the left column (Indexable Fields) to the right column (Selected Fields). You can also click

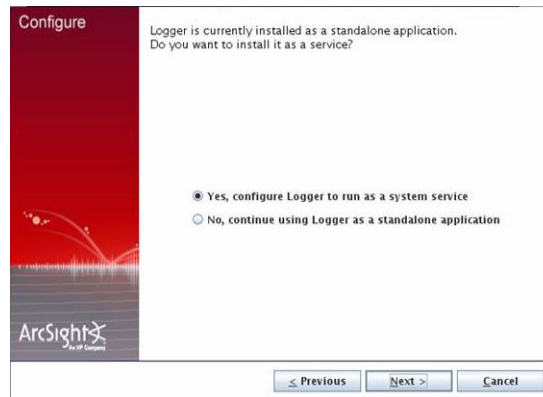
"Select Recommended Fields" to select the ArcSight recommended fields with one click and then drag them to the right column. Click **Next**.

14 Select the Locale for your Logger, as shown in the following figure. Click **Next**.

15 If you are logged in as a root user on the system on which you are installing Logger software, the following screen enables you to configure software Logger to run as a system service. By default, software Logger runs as a standalone application, which you need to launch manually after each system reboot.

When you install software Logger as a root user, a service called `arcsight_logger` can be configured created and enabled at run levels 2, 3, 4, and 5. Additionally, a few libraries are added using `ldconfig`. For a complete list of those libraries, see

`/etc/ld.so.conf.d/arcsight_logger.conf` and
`<install_dir>/current/arcsight/install/ldconfig.out.`

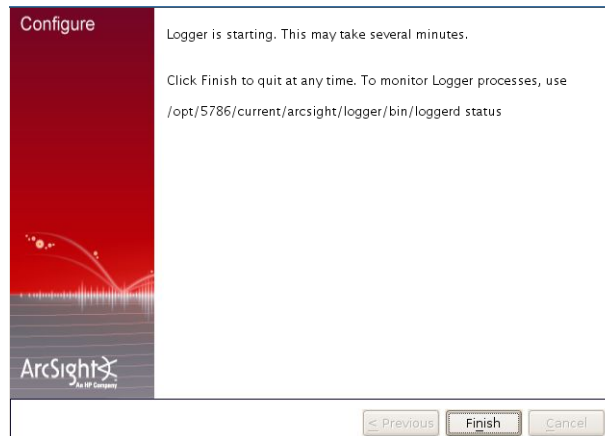


16 You have installed Logger. Click **Start Logger Now**.

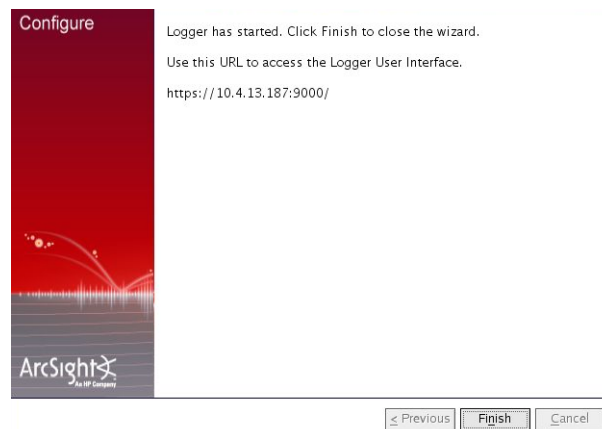
OR click **Start Logger later** and click **Finish**.

If you selected to start Logger later, you need to read the [“Starting and Stopping Logger” on page 14](#) information to understand how to start Logger later.

17 If you selected “Start Logger Now”, the following screen is displayed.



You can click **Finish** to exit the wizard. Logger continues to start service and processes in the background. Once Logger service and processes have started up, the following screen is displayed.



Follow the instructions on the above screen or use instructions in ["Connecting to the Software Logger User Interface" on page 14](#) to connect to the Logger.

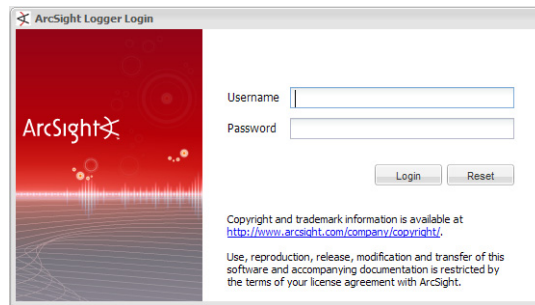
Connecting to the Software Logger User Interface

Because the software Logger user interface uses SSL, make sure you connect to it using this URL:

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

where `hostname` or `IP address` is of the system on which you installed Logger software.

Once you use the URL specified above, the following Login screen is displayed.



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

Username: `admin`
Password: `password`



Note

Change the credentials as soon as possible after connecting to your Logger for the first time.

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.

```
<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>]
```

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

The screenshot shows the 'Process Status' window. It has a 'Refresh Status' button and two main sections: 'System section' and 'Processes section'. The 'System section' displays system-wide metrics. The 'Processes section' lists individual processes with their status, uptime, CPU usage, and memory usage. The 'apache' process is highlighted in the list.

System					
System	Status	Log	CPU Usage	Memory Usage	Data Collected
mutsumt55-1277.arsight.com	running		[0.75] [0.60] [0.50]	14.8%us 3.6%kay 1.2%wa	26.2% [1603580 KB] 09/10/2010 14:26:30

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

Processes					
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	29344				
Status	running				
Uptime	14m				
aps	running	14m	0.2%	3.5%	[219336 KB]
connector	running	15m	0.0%	0.0%	[568 KB]
inasp	running	15m	0.0%	0.3%	[18952 KB]
mysqld	running	15m	0.0%	0.3%	[20520 KB]
postgresql	running	15m	0.0%	0.1%	[8192 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%	[108256 KB]

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 the Logger process running but all other processes stopped.
<code>loggerd restart</code>	This command restarts processes listed under the Process section only.
<code>loggerd status</code>	Display the current 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 the Logger Software



Note

If you will be uninstalling 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 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 version of Logger, enter this command in the directory where you installed the software version of Logger:

```
./UninstallerData/Uninstall_Arcsight_Logger_5.1
```

The uninstall wizard is launched. Click **Uninstall** to start uninstalling Logger.

Applying a New License on the Software Version of Logger

To apply a license on the software version of Logger:


- 1 Save the license file you receive from ArcSight on a computer from which you access the Logger user interface through a browser.

- 2 Run this command:

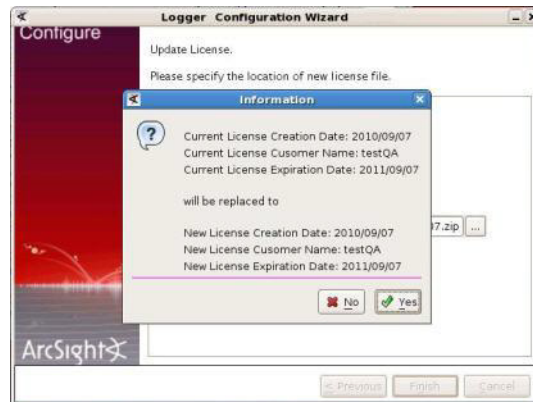
```
<install_dir>/current/arcsight/logger/bin/arcsight loggersetup
```

The following Update License screen is displayed. If you are logged in as a root user, the following screen also provides an option to enable or disable Logger from starting as a system service. For more information about configuring Logger to start as a system service, see ["Enabling or Disabling Logger as a System Service" on page 17](#).



- 3 Click the Browse () icon to locate the license file that you received from ArcSight. Click **OK**.

- 4 Click **Finish**. A message on the screen confirms that the license was applied, as shown in the following figure.



- 5 Restart the Logger service and related processes after applying the license. Use this command to restart the service and processes:

```
<install_dir>/current/arcsight/logger/bin/loggerd restart
```

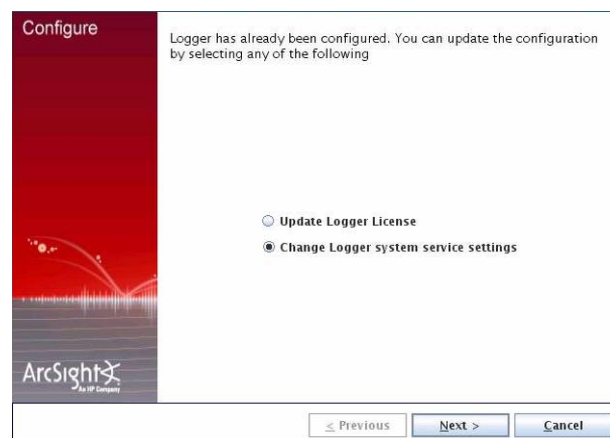
Enabling or Disabling Logger as a System Service

If you want to disable Logger from starting as a system service, or if you want to enable it to start as a system service after it has been installed, follow these steps.

- 1 Make sure you are logged in as a root user on the system on which Logger is installed.
- 2 Run this command:

```
<install_dir>/current/arcsight/logger/bin/arcsight loggersetup
```

The following screen is displayed.



- 3 Select **Change Logger system service settings** and click **Next**.
- 4 If Logger is currently installed as a service, the next screen provides you the option to disable it. Conversely, if Logger is currently installed as a standalone application, you can configure it to run as a service. Click **Finish** and reboot the Logger for changes to take effect.

Best Practices for the Minimal Install

In general, you should use the “Minimal” install for evaluation purposes or if you do not have a server with 65 GB of storage space available, which is the storage space required for a “Standard” install. To truly experience the power of Logger, ArcSight recommends installing software Logger using the “Standard” or “Custom” installation type. Doing so creates a storage system infrastructure on Logger that can handle large data storage needs, such as published reports, large amount of exported data, event archives, and so on.

However, if you must install Logger using the “Minimal” installation type, remember that Logger does not manage disk space availability for published reports, exported data, or event archives. You must ensure that there is sufficient disk space available for these functions. A Logger installed using the “Minimal” installation type can quickly run out of space if you publish a large number (or large) reports, export a large amount of data, or archive events for a long period.

Next Steps

Go to the next section, [“Overview of the Logger User Interface” on page 19](#) for instructions on connecting to the Logger for the first time.

Then, read the section, [“Receiving Events and Logs” on page 23](#) for information on how to set up your Logger to start receiving events.

Overview of the Logger User Interface

The Logger user interface is a web browser application using Secure Sockets Layer (SSL) encryption. In addition to the system administration, configuration, search, and report functions, the user interface also enables you to monitor performance.

This section provides a high-level view of the Logger User Interface, with an emphasis on the Search user interface. For user interface options not discussed in this section, see the *Logger Administrator's Guide*.

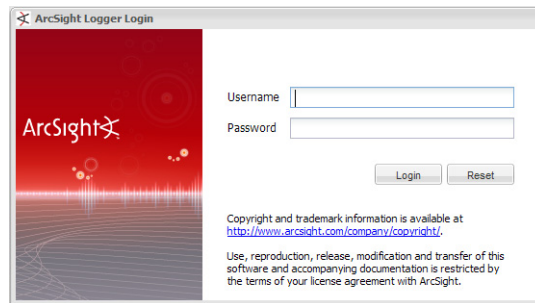
Connecting to the Logger User Interface

Because the software Logger user interface uses SSL, make sure you connect to it using this URL:

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

where `hostname` or `IP address` is of the system on which you installed Logger software.

Once you use the URL specified above, the following Login screen is displayed.



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

Username: `admin`
Password: `password`



Change the credentials as soon as possible after connecting to your Logger for the first time.

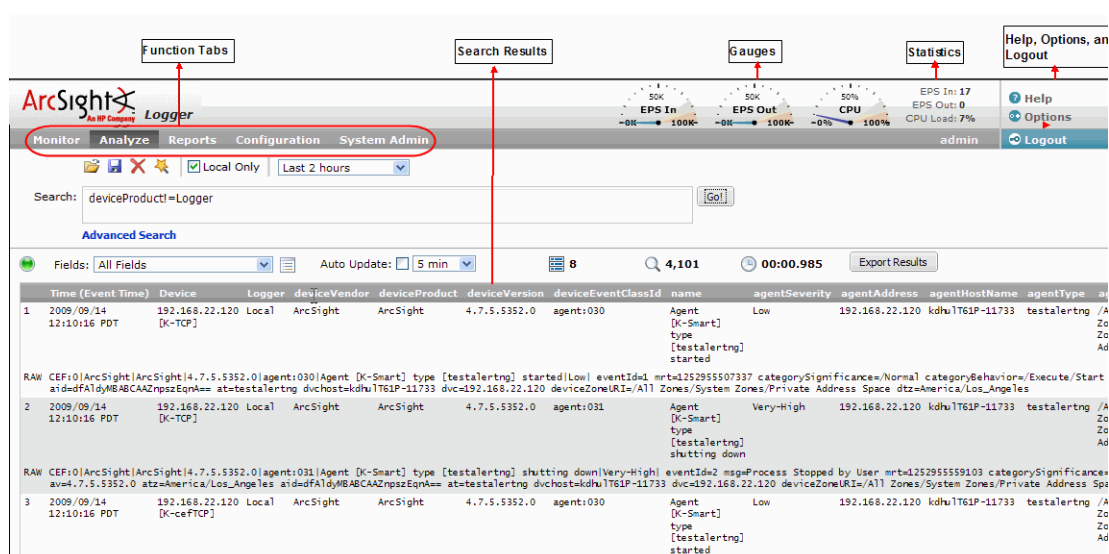
Browser Requirements

Logger works with most modern 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/>.

For the list of supported browser versions, see [“Supported Platforms and Browsers”](#) on page 3.

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 tab. The range of the gauges can be changed on the Options page. The current logged-in user's name is shown below the statistics.

A sub-menu pull down is available for all function tabs, as shown here for the Analyze tab.



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

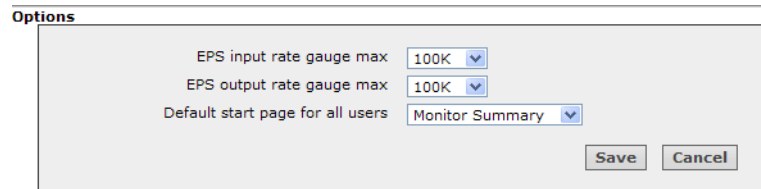
Help

Clicking the Help link on any page displays online help for the current page.

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.

The **Default start page for all users** can be set to Monitor Summary (the default), Reports Dashboard, or Analyze to configure which tab will be displayed after a user logs in.



The screenshot shows the 'Options' page with three configuration items:

- EPS input rate gauge max: 100K
- EPS output rate gauge max: 100K
- Default start page for all users: Monitor Summary

At the bottom right, there are 'Save' and 'Cancel' buttons.

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, see the *Logger Administrator's Guide*.

Chapter 4

Receiving Events and Logs

Before you can use Logger for searching and reporting on events, you must configure it to receive events and log files from sources 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). To learn more about ArcSight SmartConnectors, visit <http://www.arcsight.com>.

To enable Logger to receive events and log files, you need to configure Receivers. A Receiver on a Logger is associated with these properties:

- 1 A Receiver name and type
- 2 Type-specific Receiver Parameters

By default, two receivers—a TCP and a UDP receiver—are created for you automatically if you choose the minimal or standard installation type. You can create additional receivers to suit your needs.

Receiver Name and Type

Receiver name is a meaningful name that you assign to the Receiver. For example, `LoggerDev Syslog Server`.

Receiver type can be any of the following.

Receiver Type	Protocol	Common Use
UDP Receiver	UDP	Receiving syslog messages from Syslog servers
TCP Receiver	TCP	Receiving syslog messages from Syslog servers
CEF UDP Receiver	UDP in CEF	Systems such as ArcSight SmartConnectors that can forward events to Logger in Common Event Format (CEF)
CEF TCP Receiver	TCP in CEF	Systems such as ArcSight SmartConnectors that can forward events to Logger in Common Event Format (CEF)
File Transfer	SCP, SFTP, FTP	Reading remote log files from FTP, SFTP, or SCP servers
File Receiver	NFS, CIFS, SAN	Reading log files from NFS, CIFS, or SAN systems
SmartMessage	SSL	Receiving encrypted messages from ArcSight SmartConnectors

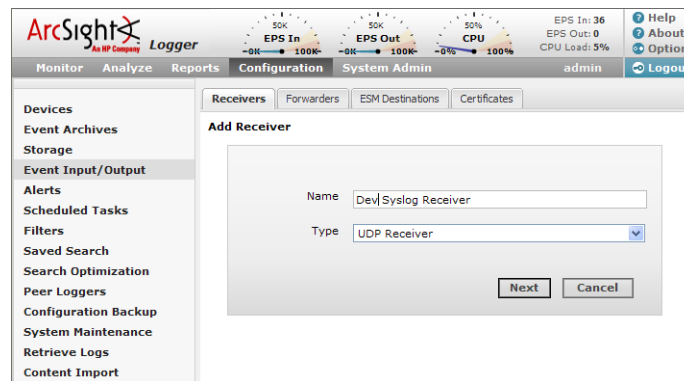
Receiver Parameters

A complete list of Receiver parameters is available in the *Logger Administrator's Guide*. This section highlights the parameters that you need to set up a UDP receiver to receive events from a syslog server on your network. This type of receiver is used for sending syslog events directly to the Logger. If you would like to create a receiver to capture events from an ArcSight SmartConnector, you need to setup a SmartMessage receiver. Refer to the *Logger Administrator's Guide* for information about setting up such a receiver.

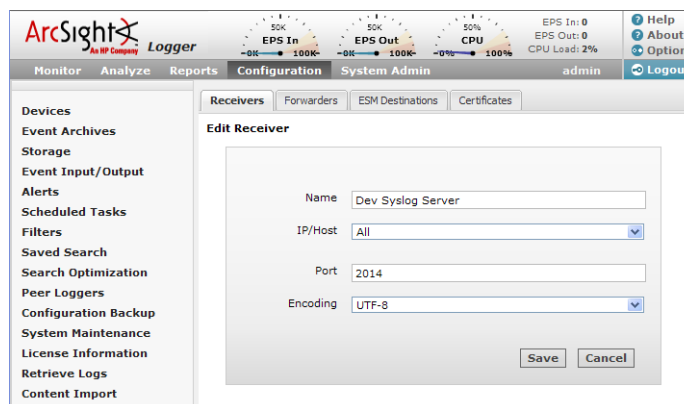
Configuring a Syslog Receiver for Receiving Events on Logger

To configure a Syslog Receiver to receive syslog events on Logger:

- 1 Click **Configuration** from the top-level menu bar.
- 2 Click **Event Input/Output** (left panel) > **Receivers** tab (right panel).
- 3 Click **Add**.



- 4 Enter a name for the new receiver in the Name field, as shown in the previous figure.
- 5 Select UDP Receiver from the Type field. Click **Next**.



- 6 In the IP/Host field, select the network connections of Logger on which the Receiver will listen for incoming events. Or select **All** to listen on all network connections.


Note: If localhost (127.0.0.1) appears in the list, it means that the Logger hostname has not been configured.

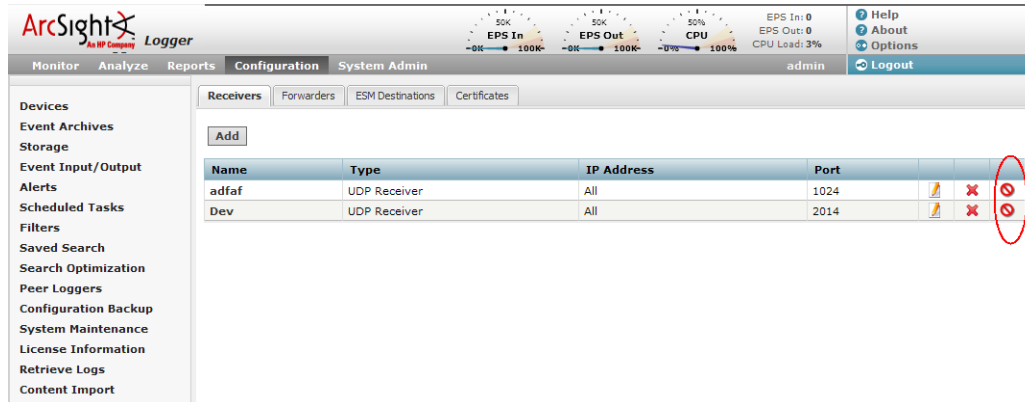
7 Enter a port number on which the Receiver will listen. **The port number needs to be greater than 1024 if you installed your software Logger as a non-root user. If you installed it as a root user, any available port can be used.**
Default: 8514.

8 Ensure that the Encoding field is set to suit your needs.

9 Click **Save**.

You have configured a syslog Receiver.

10 New receivers are initially disabled. Click the disabled icon () to enable the new receiver, as shown in the following figure.



Once a receiver is enabled, it starts listening for events on the port you selected when you configured it.

Sending CEF Events 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 *Logger Administrator's Guide*.

Logger can receive data in the form of normalized CEF events from ArcSight SmartConnectors, as shown in the illustration in the ["How Logger Works" on page 1](#) section. To set up such a configuration, download the software to install SmartConnectors and the accompanying documentation to understand in detail how to set up SmartConnectors to communicate with Logger. The SmartConnector software is available from the same web site from where you downloaded the Logger software.

Chapter 5

Searching for Events

When you need to analyze events matching a specific criteria, include them in a report, or forward them to another system such as ArcSight ESM, you will need to search for them on the Logger.

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 | 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 *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, see the *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
```

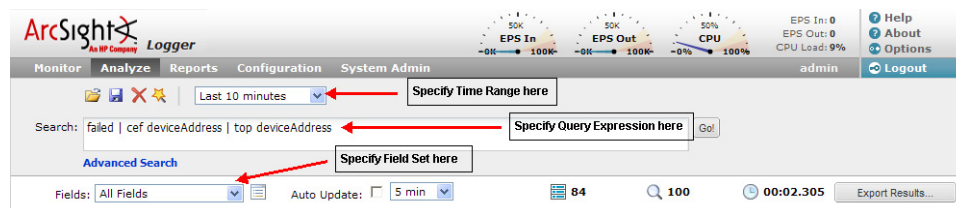
Displays search results in a tabular form of the most common values for the `deviceAddress` field. That is, the values are listed from the highest count value to the lowest.

```
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, see the *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 *Logger Administrator's Guide*.

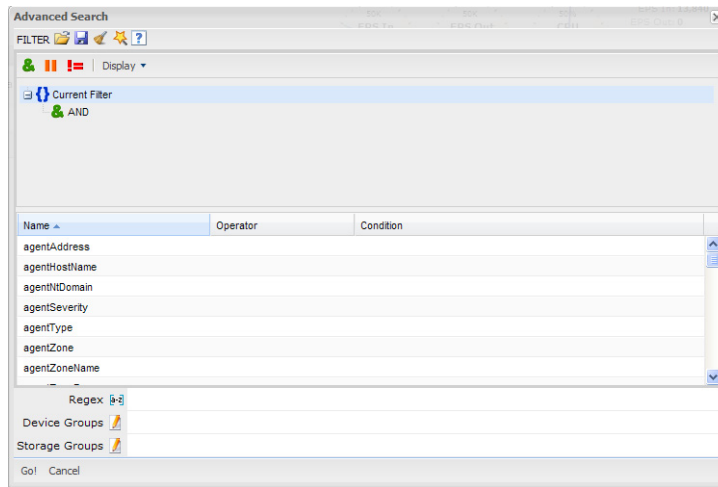
Query Building Tools

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, see the *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, see the *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

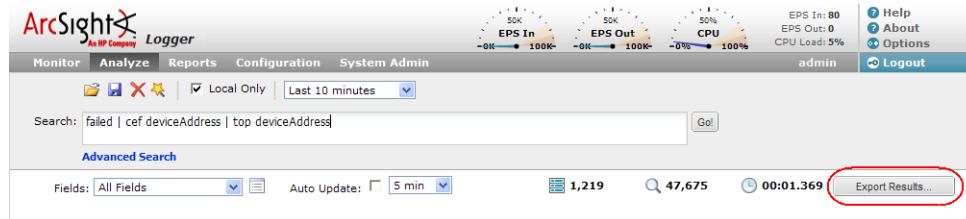
You can export search results in these formats:

- 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.

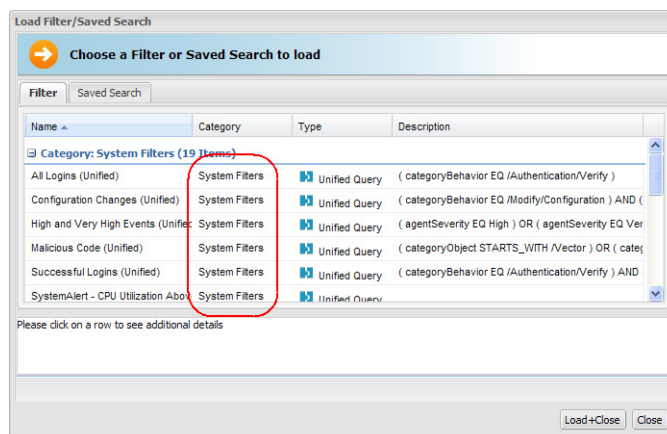
For more information about saving queries and using them again, see the *Logger Administrator's Guide*.

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. A maximum of five alerts can be enabled at any time.	Any number of alerts can be defined. All defined alerts are enabled and effective, however, a maximum of 50 alerts can run concurrently.
No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination.	No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, and one ESM destination.
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

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

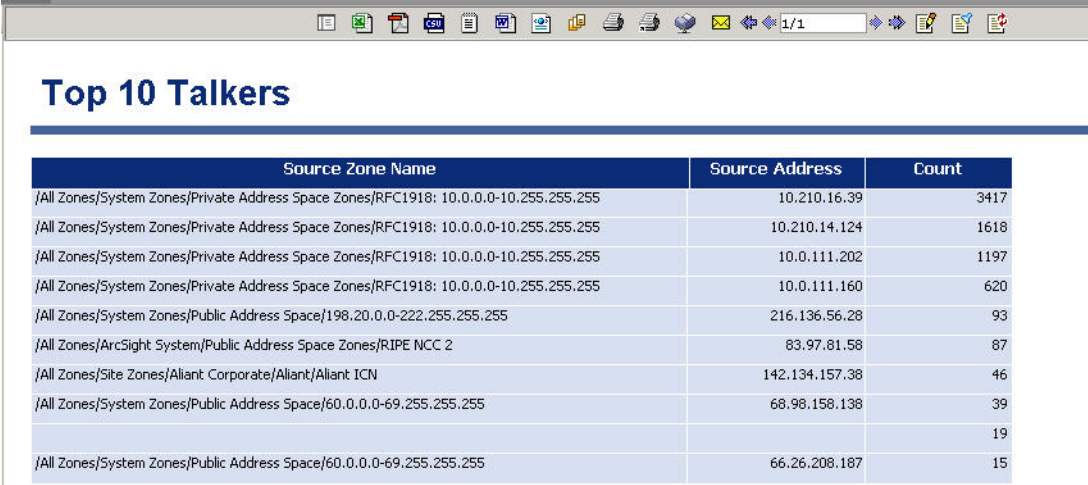
Chapter 7

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, see the *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 with a toolbar at the top. The main content area displays a report titled "Top 10 Talkers" in a blue header. Below the header is a table with three columns: "Source Zone Name", "Source Address", and "Count". The table lists the top 10 source zones based on event count.

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 your installed software 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, see the *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
```

