

# Quick Start Guide

---

Logger for VMware VM

ArcSight Logger 5.3 SP1

June 28, 2013



Copyright © 2013 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>

## Contact Information

---

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

---

## Revision History

---

Date	Product Version	Description
06/28/2013	5.3 SP1	Revision for Logger 5.3 SP1.
05/01/2013	5.3 SP1	First version of the guide for Logger on VMware.

---

# Contents

---

<b>About this Guide .....</b>	<b>5</b>
<b>Chapter 1: Overview .....</b>	<b>7</b>
How Logger Works .....	7
Logger for Security, Compliance, and IT Operations .....	8
<b>Chapter 2: Installing and Configuring Logger .....</b>	<b>9</b>
Before You Install .....	9
Downloading the Installation Package .....	9
How Licensing Works .....	9
Trial License .....	10
Viewing your license .....	10
Installing Logger .....	10
Importing the Virtual Machine .....	10
Installing Software Logger on the Virtual Machine .....	11
Connecting to Logger .....	14
Initial Logger Configuration .....	15
Starting and Stopping Logger .....	15
Uninstalling Logger .....	16
<b>Chapter 3: Receiving Events and Logs .....</b>	<b>17</b>
Enabling the Preconfigured Receivers .....	17
Configuring New Receivers .....	19
Sending Structured Data to Logger .....	19
Configuring a SmartConnector to Send Events to Logger .....	19
<b>Chapter 4: Overview of the Logger User Interface .....</b>	<b>21</b>
Navigating the User Interface .....	21
Help .....	22
Options .....	22
Logout .....	22
Summary .....	22
Dashboards .....	23

<b>Chapter 5: Searching for Events .....</b>	<b>25</b>
Example Queries .....	25
Syntax of a Query .....	25
Building a Query .....	26
Run a Query .....	27
Query Building Tools .....	27
Exporting Search Results .....	29
Saving Queries for Later Use .....	29
System Filters (Predefined Filters) .....	29
Tuning Search Performance .....	30
<b>Chapter 6: Alerts .....</b>	<b>31</b>
Types of Alerts .....	31
Configuring Alerts .....	32
<b>Chapter 7: Other Logger Features .....</b>	<b>33</b>
Reports .....	33
Scheduling Tasks .....	33
Archiving Events .....	33
Access Control on Logger Users .....	34
<b>Chapter 8: Example Queries .....</b>	<b>35</b>

# About this Guide

---

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

The goal of this guide is to enable you to start using 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 ArcSight Logger Administrator's Guide.



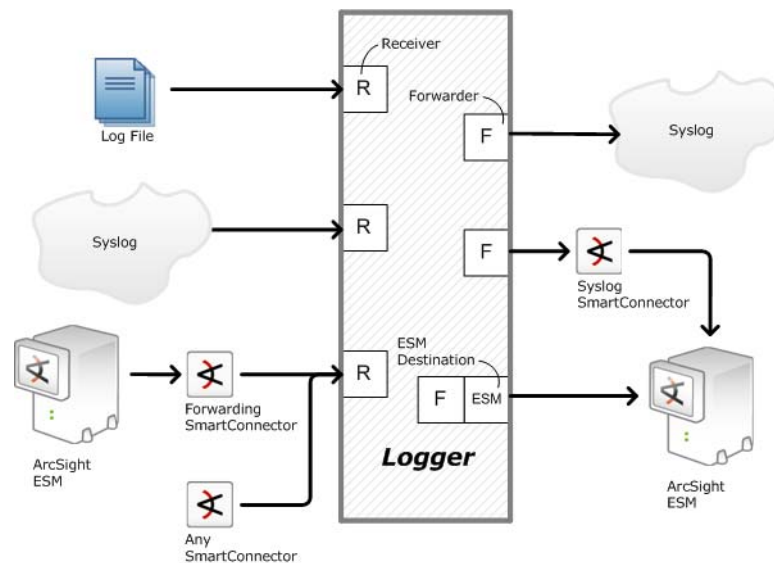
## Chapter 1 Overview

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

Logger is available in three form factors, as an appliance, as software, and as a virtualized image. The form factors offer identical features. Logger for VMware VM includes the software Logger installation files and a preinstalled operating system to enable quick deployment on an ESXi server.

### How Logger Works

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



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).

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. These include unsuccessful login attempts, the number of events by source, SSH authentications on UNIX servers, and special privileges assigned to new Windows logons. As a result, you do not 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 ArcSight Logger Administrator's Guide. Information about how to use predefined filters is included in ["System Filters \(Predefined Filters\)" on page 29](#).



# Installing and Configuring Logger

## Before You Install

You can deploy the Logger virtual machine (VM) on a VMware ESXi server, version 4.1 or 5.1. The VM image includes the Logger 5.3 SP1 installer on a 64-bit CentOS 6.2 configured with 12 GB of physical memory and 8 CPU.

Once Logger is installed, you can access the Logger user interface using any of these Web browsers:

- Internet Explorer: Versions 8 and 9
- Firefox: Versions 12 and 13

An Adobe Flash Player plug-in is required on these browsers for some of the features, such as histogram and charts, to work.

## Downloading the Installation Package

The Logger for VMware VM installation package (Logger5.3SP1\_QXXXX.ova) is available for download from the HP Software Depot at <http://software.hp.com>.

## How Licensing Works

A license for Logger defines the limits for the following:

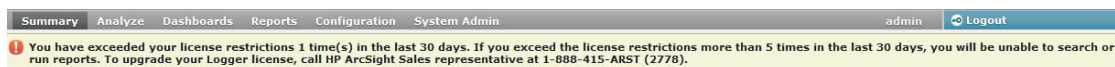


Note

These are example values. The specific limits imposed by your license may differ. See “[Viewing your license](#)” on page 10 for information on how to view your Logger’s current license.

- **Data limit:** A limit on the amount of incoming data per day, for example, 20 GB per day. This value is determined by the sum of the sizes of the original events.
- **Storage limit:** The maximum storage for this Logger, for example, 800 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, refer to the Logger Administrator’s Guide.

## Trial License

Logger includes a built in trial license that you can use for a limited period of time for test and evaluation purposes.

To continue using Logger after the trial period is over, you must purchase the Enterprise version. Contact your HP ArcSight sales representative for details.



Be sure to use the enterprise version when deploying Logger on a production system.

---

## Viewing your license

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

# Installing Logger

Before you can install the Logger software, you must import and configure the VM.

## Importing the Virtual Machine

This section guides you through the steps of importing and configuring the VM. As part of the operating system configuration process, you will need to create a second hard disk before installing Logger. Once the second hard disk is attached and system is powered on, the startup scripts attach the second hard disk and format it with an XFS partition. This partition will be used for storing the Logger data.

### To import the virtual machine:

- 1 Open the vSphere client and connect to the ESXi server.
- 2 On the vSphere client, open the File menu and select **Deploy OVF Template...**
- 3 On the Source panel, browse to select the Logger installation file (Logger5.3SP1\_QXXXX.ova) that you downloaded previously, and click **Open**.
- 4 The OVF Template Details panel displays product information. Click **Next**.
- 5 On the Name and Location panel, enter a name for the virtual machine and click **Next**.
- 6 On the Disk Format panel select **Thick Provision Lazy Zeroed** and click **Next**.
- 7 The Ready to complete panel displays options you selected. Click **Finish** to confirm your selections and deploy the virtual machine.

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

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

**To add a second hard disk:**

- 1 Select the new VM from the ESXi server's list and make sure it is powered off.
- 2 Right-click the VM to open the dropdown menu, and then select **Edit Settings**.
- 3 The Virtual Machine Properties dialog box opens. Click **Add...**
- 4 The Device Type panel displays a list of devices you can add.
- 5 Select **Hard Disk** and click **Next**.
- 6 The Select a Disk panel displays the type of disks you can use. Select **Create a new virtual disk** and click **Next**.
- 7 The Create a Disk Panel displays virtual disk size and provisioning options.



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

- 8 Select **Thick Provision Lazy Zeroed** and click **Next**.

The Advanced Options panel displays other options. Keep the default Virtual device Node and click **Next**.

- 9 The Ready to complete panel displays options you selected. Click **Finish** to confirm your selections and add the hard disk.

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

- 10 Click **OK**.

The new VM has been created. The VM has the default root password "arcsight". A non-root user, arcsight, with no password is also included. Change the root password as soon as possible.

## Installing Software Logger on the Virtual Machine

Before installing software Logger:

- Boot up the operating system on the VM, set the timezone, and do any other necessary configuration before proceeding with the installation.
- Change the root password of the VM.
- By default, the network setting for the VM image is configured to use DHCP. HP ArcSight recommends that you change the setting to static. The hostname must be resolvable, either by the DNS server or by settings in `/etc/hosts`.
- 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.
- SELinux and SSH are enabled on the OS, but the firewall is disabled. Enable a firewall and add your firewall policy to allow or deny devices to ensure proper access to Logger as soon as possible.
- If you have acquired a license file for your Logger, SCP it to the VM before you begin the installation. Make a note of the file name and location; you will need them during the installation process.
- Decide whether to install Logger while logged into the VM as root or as arcsight, the non-root user.

- ◆ If you install as root, you can choose whether to configure Logger to start as a service and you can select the port on which Logger listens for secure web connections.
- ◆ If you install as “arcsight”, the non-root user, Logger can only listen for connections on port 9000. You cannot configure the port to a different value.



Note

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

---

### To Install Logger:

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

```
./ArcSight-logger-5.3.1.XXXX.0.bin
```

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

```
Introduction
```

```
-----
```

```
InstallAnywhere will guide you through the installation of  
ArcSight Logger 5.3 SP1.
```

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

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

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

```
PRESS <ENTER> TO CONTINUE:
```

- 3 The next several screens display the end user license agreement. Installation and use of Logger 5.3 SP1 requires acceptance of the license agreement. Press Enter to display each part of the license agreement, until you reach the following prompt:

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

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

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



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.

---

- 5 If Logger is currently running on this machine, a message is displayed. Type Y and press Enter to stop all current Logger processes and proceed with the installation, or type quit and press Enter to exit the installer.

```
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 The Choose Install Folder screen is displayed. Type the following path and then press Enter:

```
/opt/arcsight/logger
```



You must install Logger in this location. Do not select the default or specify a different location.

- 7 Type `y` and press Enter to confirm the installation location.
- 8 If there is not enough space to install the software, a message is displayed. Type `quit` and press Enter to exit the installer and reconfigure your VM.
- 9 If Logger is already installed at the location you specify, a message is displayed. Type `quit` and press Enter to exit the installer and uninstall the previous version.

- 10 Indicate the type of license that you want to use.

- ◆ To evaluate Logger using the trial license, type `1` and press Enter.  
If you start with a trial license, you can upload the license file for the Enterprise Logger later. You do not need to upload a license to use the trial Logger.
- ◆ To use a license file, type `2` and press Enter. Then type the absolute path to the license file and then press Enter.

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

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

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

Field	Notes
User Name	Use the non-root user "arcsight" that comes preconfigured on your VM image.
HTTPS Port	The port number to use when accessing the Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI.
Choose if you want to run Logger as a system service.	Type <code>1</code> and press Enter to configure Logger as a service, or type <code>2</code> and press Enter to configure Logger as standalone. Select this option to create a service called <code>arcsight_logger</code> , and enable it to run at levels 2, 3, 4, and 5. If you do not enable Logger to start as service during the installation process, you still do so later. For instructions on how to enable Logger to start as a service, see the Logger Administrator's Guide.

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

- 14 Press Enter to initialize Logger components.

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

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

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

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

Now that you are done installing and initializing your Logger, you can use that URL to log in and start configuring Logger to receive events.

## Connecting to Logger

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

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

where the hostname or IP address is the system on which the Logger software is installed, and configured\_port is the port set up during the Logger installation, if applicable. (A port is not required if the installation was done as the root user.)

Once you connect, the following Login screen is displayed.

- 2 Enter your user name and password, and click Login. Use the following default credentials:

Username: admin  
Password: password



For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time. Refer to the Logger Administrator's guide for instructions.

---

## Initial Logger Configuration

During the Logger initialization process, Logger is given the following default configuration. For more details about the listed components, see the ArcSight Logger Administrator's Guide.

Component	Default Configuration
Storage Volume	6 GB (available for data storage)
Storage Groups	Two—A Default Storage Group and an Internal Storage Group
Indexing	Full-text and field-based indexing enabled
Receivers	Six total: One of each TCP, UDP, and SmartMessage type; and three Folder Follower receivers

## Starting and Stopping Logger

The `loggerd` command enables you to start or stop the Logger software running on your machine. In addition, the command includes a number of subcommands that you can use to control other processes that run as part of the Logger software. If your Logger is installed to run as a system service, 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	Load	CPU Usage	Memory Usage	Data Collected
mutsum05-107.arcsight.com	running	[0.75] [0.66] [0.58]	14.8%us 3.6%sy 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.

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% (218336 kB)
connector	running	15m	0.0%	0.0% (568 kB)
insp	running	15m	0.0%	0.3% (19892 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
<code>loggerd start</code>	Start all processes listed under the System and Process sections in the figure above. Use this command to launch Logger.
<code>loggerd stop</code>	Stop processes listed under the Process section only. Use this command when you want to leave <code>loggerd</code> running but all other processes stopped.
<code>loggerd restart</code>	<p>This command restarts processes listed under the Process section only.</p> <p><b>Note:</b> When the <code>loggerd restart</code> command is used to restart Logger, the status message for the "aps" process displays this message:</p> <p>Process 'aps' Execution failed.</p> <p>After a few seconds, the message changes to:</p> <p>Process 'aps' running.</p>
<code>loggerd status</code>	Display the 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 &lt;process_name&gt;</code>	Start the named process. For example, <code>loggerd start apache</code>
<code>loggerd stop &lt;process_name&gt;</code>	Stop the named process. For example, <code>loggerd stop apache</code>
<code>loggerd restart &lt;process_name&gt;</code>	Restart the named process. For example, <code>loggerd restart apache</code>

## Uninstalling Logger

To uninstall the software Logger, simply delete the VM. Alternatively, 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.

## Enabling the Preconfigured Receivers

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

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

- A UDP receiver—Enabled by default. If you are installing software Logger as root, the UDP receiver is on port 514. For non-root installs, it is on port 8514. If this port is already occupied, the initialization process selects the next higher unoccupied port. This port should be allowed through any firewall rules you have configured.
- A TCP receiver—Enabled by default. If you are installing software Logger as root, the TCP receiver is on port 515. For non-root installs, it is on port 8515. If this port is already occupied, the initialization process selects the next higher unoccupied port. This port should be allowed through any firewall rules you have configured.
- A SmartMessage receiver—Enabled by default. To receive events from a SmartConnector, download the SmartConnector and set the **Receiver Name** to be "SmartMessage Receiver" when configuring the destination.

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



Note

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

---

The preconfigured folder follower receivers include:

- Var Log Messages—`/var/log/messages`
- Audit Log—`/var/log/audit/audit.log`

- Apache URL Access Error Log—<install\_dir>/userdata/logs/apache/http\_error\_log



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

When you first log in by using the URL you configured, 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

Once you enable the Apache URL Access Error Log receiver, Logger will start storing entries from the <install\_dir>/userdata/logs/apache/http\_error\_log file.

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

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



Before enabling the receivers, you must make /var/log/audit/audit.log and /var/log/messages readable by the non-root user used during Logger installation.

#### To enable a receiver:

Click the disabled icon () at the end of the row. Once the receiver is enabled, the enabled icon () is displayed.

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 the receiver is enabled, the enabled icon () is displayed.

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

## Configuring New Receivers

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

You can configure the following types of receiver for Logger:

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



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

- **SmartMessage Receiver:** SmartMessage receivers listen for encrypted messages from ArcSight SmartConnectors.

## Sending Structured Data to Logger

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

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

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

## Configuring a SmartConnector to Send Events to Logger

Logger comes pre-configured with a SmartMessage Receiver. To use it to receive events from a SmartConnector, you must configure the SmartConnector as described below. You can also create new SmartMessage receivers and configure the SmartConnectors with

these newly created receivers. When configuring a SmartConnector, be sure to specify the correct receiver name.

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

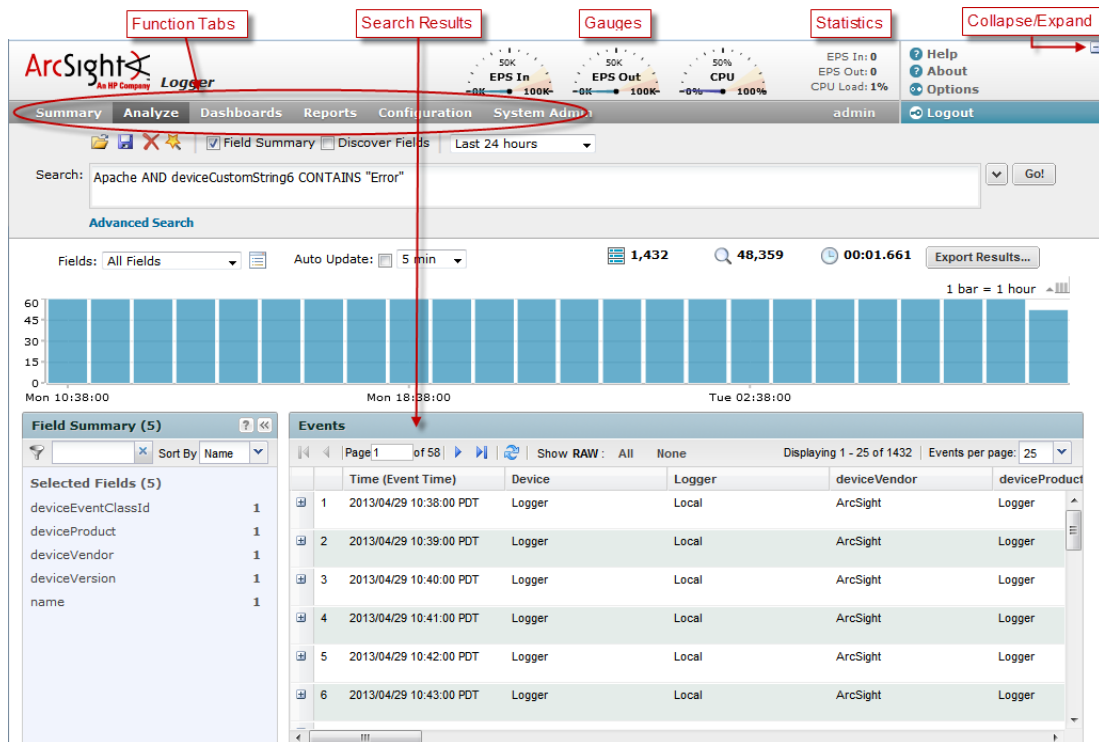
- 1** Install the SmartConnector component using the SmartConnector User's Guide as a reference. Specify Logger as the destination instead of ArcSight ESM or a CEF file.
- 2** Specify the required parameters. Enter the Logger hostname or IP address and the name of the SmartMessage receiver. These settings must match the receiver in Logger that listen for events from this connector.
  - ◆ To use the preconfigured receiver, specify "SmartMessage Receiver" as the **Receiver Name**.
  - ◆ To communicate between an ArcSight SmartConnector and software Logger, configure the SmartConnector to use the port configured for the software Logger.
  - ◆ For un-encrypted CEF syslog, enter the Logger hostname or IP address, the desired port, and choose UDP or TCP output.



# Overview of the Logger User Interface

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

## Navigating the User Interface

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



Gauges at the top of the screen provide an indication of the throughput and CPU usage information available in more detail on the Monitor Dashboard (["Dashboards" on page 23](#)). 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 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 ArcSight Logger Administrator's Guide.





## Chapter 5

# Searching for Events

---

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

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

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

**Example:**

To extract an IP address from the following event

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

and assign it to a field called "IP\_Address", use the following rex expression:

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

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

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

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

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

```
failed | top deviceAddress
```

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

## Building a Query

When you build a query, 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.

The screenshot shows the ArcSight Logger web interface. At the top, there are system status gauges for EPS In, EPS Out, and CPU, along with a user menu (admin) and a Logout button. Below the navigation tabs (Summary, Analyze, Dashboards, Reports, Configuration, System Admin), there are checkboxes for 'Local Only', 'Field Summary', and 'Discover Fields'. A 'Custom time range' dropdown is set to 'Custom time range'. The search bar contains the query: 'logger | rex "http://(?<URL>[^\ ]\*)" | top URL'. Below the search bar, there are three boxes with red arrows pointing to them: 'Specify Field Set here' (pointing to the 'Fields' dropdown), 'Specify Query Expression here' (pointing to the search bar), and 'Specify Time Range here' (pointing to the 'Custom time range' dropdown). The 'Fields' dropdown is currently set to 'All Fields'. The 'Auto Update' is set to '5 min'. The search results show 311 items. There are also buttons for 'Export Results...' and 'Go!'.

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

A **storage group** enables you associate a retention policy with it. Therefore, by defining multiple storage groups, you can store events for different periods of time.

A **device group** enables you to categorize devices of your choice into a group. You can associate a device group to a storage rule that defines in which storage group events from a specific device group are stored.

## Run a Query

### To run a query:

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



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

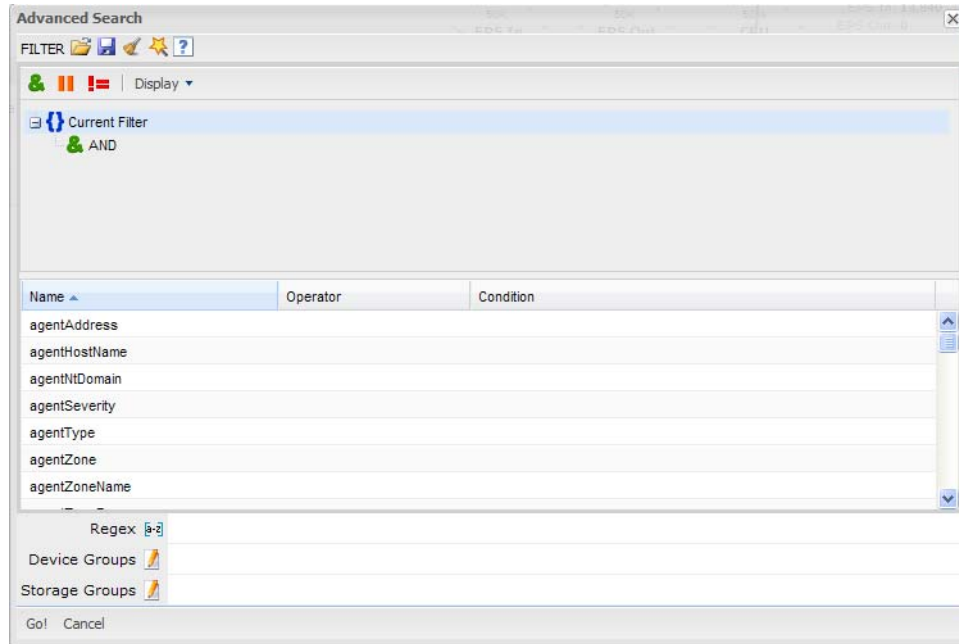
## Query Building Tools

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

### ■ Search Builder

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

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



#### ■ Regex Helper

Creating 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 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.

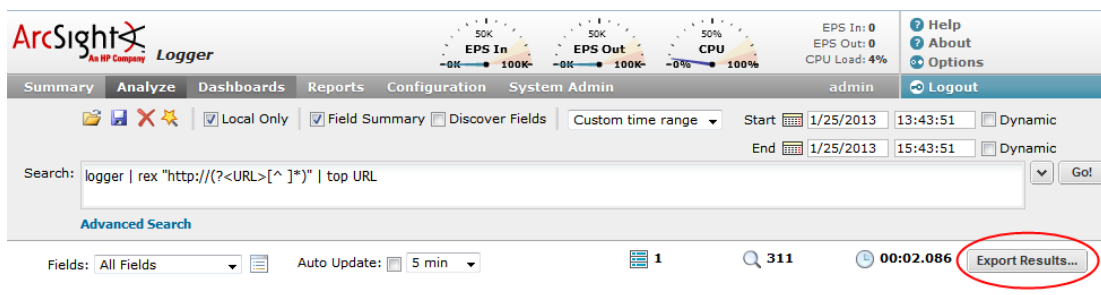
## Exporting Search Results

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.

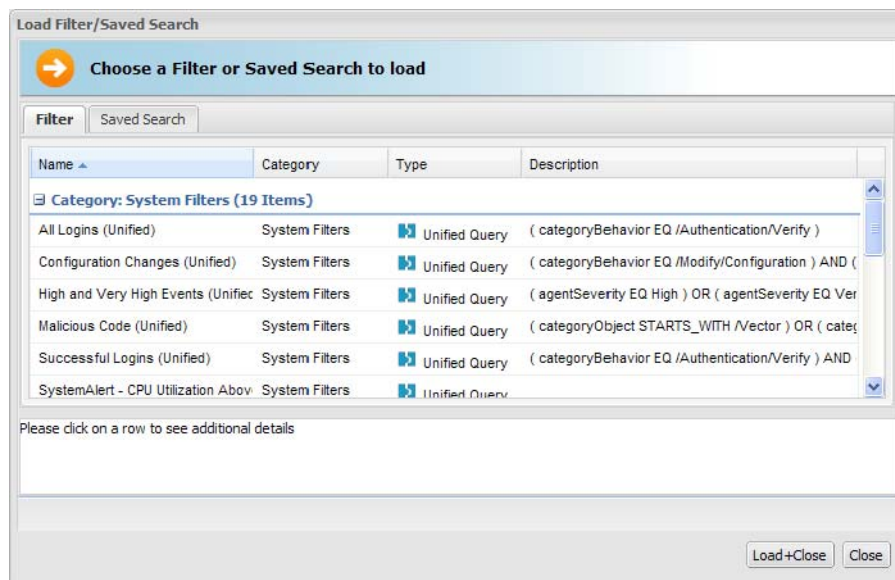
For more information about saving queries and using them again, refer to the ArcSight Logger Administrator's Guide.

## System Filters (Predefined Filters)

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

### To use a system filter:

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



- 3 Click **Load+Close**.

## Tuning Search Performance

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

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

- 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.

**Full-text indexing and Field-based indexing** for a recommended set of fields **are automatically enabled at Logger initialization time. In addition to these fields**, HP strongly recommends that you index fields that you will be using in search and report queries. Refer to the ArcSight Logger Administrator's Guide for more information on indexing fields.

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 can be defined. A maximum of <b>five</b> 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 occurs within the specified threshold, an alert is <b>immediately</b> triggered.	These alerts are triggered at scheduled intervals. That is, when a specified number of matches occurs within the specified threshold, an alert is triggered <b>at the next scheduled time interval</b> .

---

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



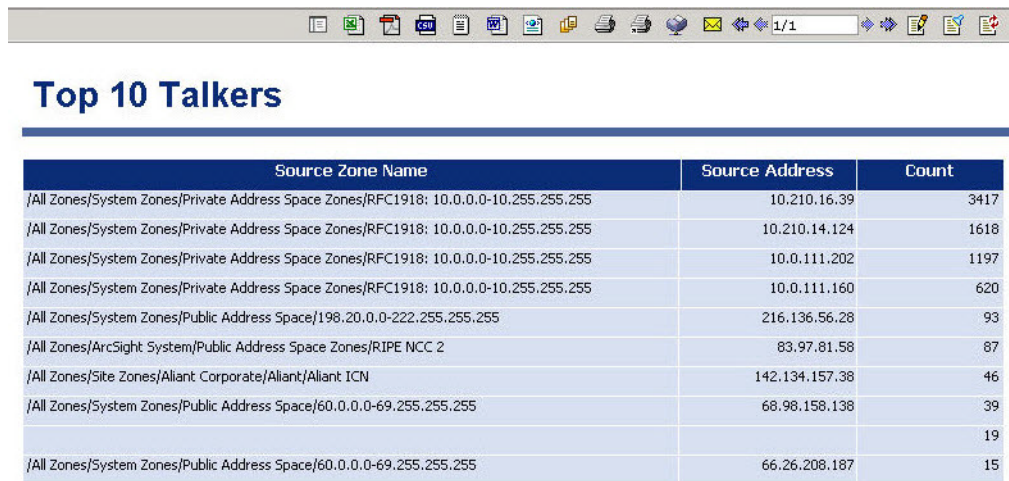
## Chapter 7

# Other Logger Features

In addition to the Logger features highlighted in this guide, Logger provides many other features. This section provides an overview of those features. For an in-depth understanding and how to use those features, refer to the 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-based interface with a toolbar at the top containing icons for file operations, navigation, and search. Below the toolbar, the title 'Top 10 Talkers' is displayed in a large, bold, blue font. Underneath the title 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/5ite Zones/Aliant Corporate/Aliant/Aliant 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 and give Jane 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 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
```

