

Quick Start Guide

ArcSight Logger 5.3 SP1
for Hyper-V

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>

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

This document is confidential.

Contact Information

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

Revision History

Date	Product Version	Description
06/28/2013	5.3 SP1	Revision for Logger 5.3 SP1.
02/27/2013	5.3 SP1	Updated for Logger 5.3 SP1, including trial license information.
08/24/2012	5.3	First version of the guide for Hyper-V installation.

Contents

About this Guide	5
Chapter 1: Overview	7
How Logger Works	7
Logger for Security, Compliance, and IT Operations	8
Chapter 2: Installing and Configuring Logger	9
Before You Install	9
Supported Platforms and Browsers	9
Downloading the Installation Package	9
How Licensing Works	9
Trial License	10
Viewing your license	10
Installing and Configuring Logger	10
Prerequisites for Installation	10
Installing Logger	10
Install and Configure Hyper-V on Windows Server 2008 R2	11
Create a Logger Virtual Machine	12
Configure the Logger Virtual Machine	14
Initialize the Logger Virtual Machine	15
Connecting to Logger	19
Initial Logger Configuration	20
Adding Connectors After Logger Initialization	20
Modifying Connector Settings	21
Uninstalling Logger	22
Chapter 3: Receiving Events and Logs	23
Enabling the Preconfigured Receivers	23
Configuring New Receivers	24
Sending Structured Data to Logger	25
Configuring a SmartConnector to Send Events to Logger	25
Chapter 4: Overview of the Logger User Interface	27
Navigating the User Interface	27

Help	28
Options	28
Logout	28
Summary	29
Dashboards	29
Chapter 5: Searching for Events	31
Example Queries	31
Syntax of a Query	31
Building a Query	32
Run a Query	33
Query Building Tools	33
Exporting Search Results	35
Saving Queries for Later Use	35
System Filters (Predefined Filters)	35
Tuning Search Performance	36
Chapter 6: Alerts	37
Types of Alerts	37
Configuring Alerts	38
Chapter 7: Other Logger Features	39
Reports	39
Scheduling Tasks	39
Archiving Events	39
Access Control on Logger Users	40
Chapter 8: Example Queries	41

About this Guide

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

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

Chapter 1

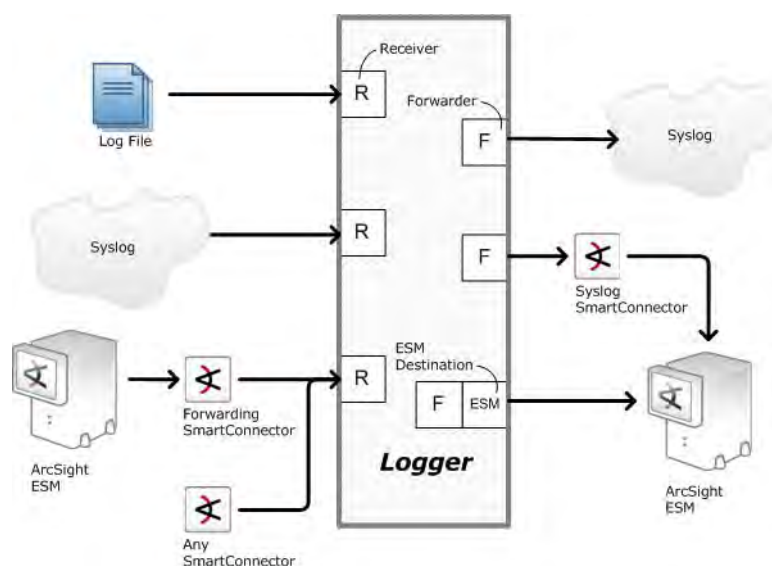
Overview

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 the the same features. Logger for Hyper-V is an image of the Logger appliance that you can deploy on a Windows 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 don't need to define queries to search for commonly searched events. Additionally, you can copy the predefined content filters and modify them to suit your needs, thus saving time and effort required to start writing queries from scratch.

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

For a complete list of predefined content filters and predefined reports, refer to the ArcSight Logger Administrator's Guide Information about how to use predefined filters is included in ["System Filters \(Predefined Filters\)" on page 35](#).

Installing and Configuring Logger

Before You Install

Ensure that you are installing Logger on a supported platform.

Supported Platforms and Browsers

You can install Logger on a Windows Server 2008 R2. The server must have an instance of Hyper-V, with the following specifications, installed.

CPU: 1 Intel Xeon Quad Core or equivalent (4 processors)

Memory: 12 GB (for trial version); 18 GB (for a production-level system; up to 12 GB physically allocated)

Disk Space: 40 GB (for Logger software) and at least 8 GB (for data)

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.

For optimal performance, make sure no other virtual machines or other applications exist on the Windows server on which you install the Hyper-V Logger.

Downloading the Installation Package

The Logger installation package 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:



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. The sum of the sizes of the original events is used to determine this value.

- **Retention period:** Number of days for which you can retain events on Logger, for example, 8 days.
- **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 and Configuring Logger

This section describes the prerequisites and the procedure for installing Logger on a Hyper-V instance.

Prerequisites for Installation

Make sure that you have downloaded the Logger installation package (.vhd file) for Hyper-V.

Installing Logger

The process of installing Logger on a Windows Server 2008 R2 includes these steps:

- 1 ["Install and Configure Hyper-V on Windows Server 2008 R2" on page 11](#), if it does not already exist.
- 2 ["Create a Logger Virtual Machine" on page 12](#).
- 3 ["Configure the Logger Virtual Machine" on page 14](#).
- 4 ["Initialize the Logger Virtual Machine" on page 15](#).

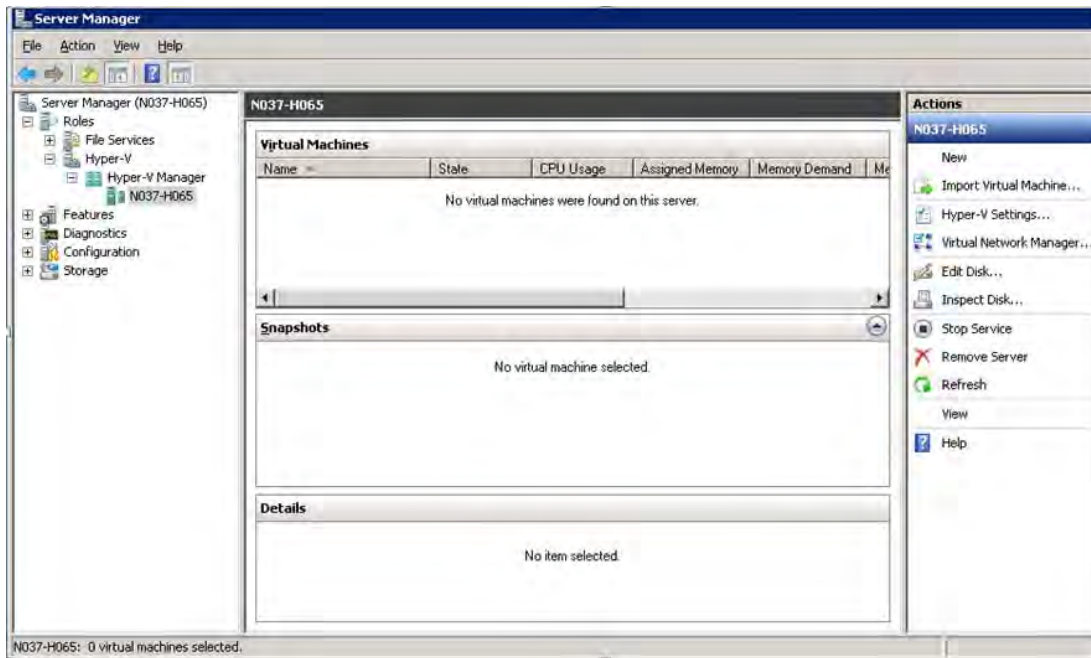
Install and Configure Hyper-V on Windows Server 2008 R2

This section guides you about installing Hyper-V on Windows Server 2008 R2 and configuring it for network access. A brand new Hyper-V role does not have any network settings configured and you will need to configure them. **If you have Hyper-V installed already, skip this section.**

To install and configure Hyper-V:

- 1 On your Windows Server 2008 R2 server, use the Server Manager to install the Hyper-V role:
 - a Click the **Roles** option under the Server Manager menu.
 - b Select **Hyper-V** from the list of roles you can install.
 - c Step through the wizard to complete the Hyper-V role installation.
 - d Reboot the server when the wizard prompts you to do so.

The Server Manager now includes a Hyper-V role, and a Hyper-V Manager with a hostname that is same as the hostname of your Windows Server 2008 R2 machine, as shown in the following example.



- 2 Configure network settings for Hyper-V:
 - a Ensure that the hostname of the Hyper-V Manager you added is selected in Server Manager.
 - b Click **Virtual Network Manager** from the Actions panel on the right side.
 - c Click **New virtual network**.
 - d Ignore the currently selected type of virtual network, and click **Add**.
 - e Enter information for these settings on the New Virtual Network screen:
 - Name—A meaningful name for the virtual network you are creating, for example, Logger Network Access.

- Notes—A description for the virtual network.
 - Connection Type—Select **External** and click the **Allow management operating system to share this network adapter** setting to select it.
 - Click the “More about managing virtual network” link to review information about configuring the network.
- f** Click **OK**.

A warning message indicates that your network connectivity will be briefly disrupted. If you are connected through a remote desktop session, you might also be disconnected from it.

Create a Logger Virtual Machine

This section guides you through the steps of creating a virtual machine for Logger that includes creating two hard drives—one for storing the Logger software and the other one for storing data that Logger will receive.

To create a Logger virtual machine:

- 1** Ensure that the hostname of the Hyper-V Manager you added is selected in Server Manager.
- 2** Click **New** > **Virtual Machine** from the Actions panel on the right side.
- 3** Follow the New Virtual Machine Wizard. Use the following recommended values for settings in this wizard:
 - ◆ Specify Name and Location—Specify a name for the virtual machine, for example, Logger Virtual Machine. If you want to store the virtual machine in a different directory location than the one shown on your screen, click “Store the virtual machine in a different location” and specify it in the Location field.
 - ◆ Assign Memory—HP recommends allocating at least 12 GB of memory for trial versions and 18 GB for production-level systems.
 - ◆ Configure Networking—Select the name you specified earlier for the virtual network you created, for example, Logger Network Access.
 - ◆ Connect Virtual Hard Disk—Select **Attach a virtual hard disk later**.
 - ◆ Completing the New Virtual Machine Wizard—Verify all the settings and click **Finish**.
- 4** (Optional, but recommended) Follow these steps to convert the .vhd file to fixed size. Doing so converts the dynamically expandable .vhd file to a fixed size disk, and can improve runtime performance, since the disk does not need to be grown on-the-fly.
 - a** Select the virtual machine you just created.
 - b** Select **Edit Disk** from the Actions panel on the right side.
 - c** Click **Browse** on the “Locate Virtual Hard Disk” screen to specify the location of the .vhd file that you downloaded before starting the installation process. Click **Next**.
 - d** Select **Convert** on the Choose Action screen. Click **Next**.
 - e** Enter a new file name or **Browse** to a new file to which the contents of the original .vhd file will be copied, for example, 2012-07-31_L750MB-V_L6647.fixedsize.vhd.
 - f** Click **Finish**.

- g Verify the new file name and other related information and click **Finish**.



The process of disk conversion takes a few minutes.

- 5 Ensure that the virtual machine you just created is selected.
- 6 Click **Settings** under the menu options for your virtual machine name in the Actions panel on the right side.
- The Settings for <Your Virtual Machine Name> page is displayed.
- 7 Select **Processor** from the Hardware menu in the left panel, and click the **Number of logical processors** drop-down to increase the number to 4. Click **Apply**.
- For optimal Logger performance, at least four processors should be assigned to the virtual machine.
- 8 Select **Network Adapter** from the Hardware menu in the left panel, and select the virtual network you have added for Logger, for example, Logger Network Access.
- 9 Follow these steps to add two hard drives to IDE Controller 0—one for storing the Logger software and the other one for storing data that Logger will receive:

- a Click **IDE Controller 0** from the Hardware menu in the left panel, select **Hard Drive** (from the right side), and click **Add**.
- b In the next screen, click **Browse** to locate the directory where the Logger installation package (.vhd file that you downloaded from the HP Customer Support web site or the fixed disk to which you converted the originally downloaded .vhd file) is stored. Click **OK**.

This step creates the first hard drive of the size specified by the .vhd file (40 GB).

- c Click **IDE Controller 0** again to add the second hard drive. This time, the Location field (on the right side) will display "1 (in use)". Select **Hard Drive** (from the right side) and click **Add**.
- d Either select **Physical hard disk** to specify a physical hard disk, or click **New** to launch the New Virtual Hard Disk Wizard. Use the following recommended values for settings in this wizard:
- Choose Disk Type—Fixed size.
 - Specify Name and Location—Specify a meaningful name for the disk, for example, Logger Data Disk.vhd. Also, specify the location of the virtual disk file.
 - Configure Disk—Select **Create a new blank virtual hard disk**, and specify at least **8 GB** in the Size field.
 - Completing the New Virtual Hard Disk Wizard—Verify all the settings and click **Finish**.

You have finished creating a virtual machine with two hard drives attached to the first IDE interface on your Windows Server 2008 R2.

- e Configure the Automatic Stop Action for the virtual machine to "Turn off the virtual machine" when the physical server on which it is configured shuts down. To do so, configure the management settings under the Management section in the left panel.

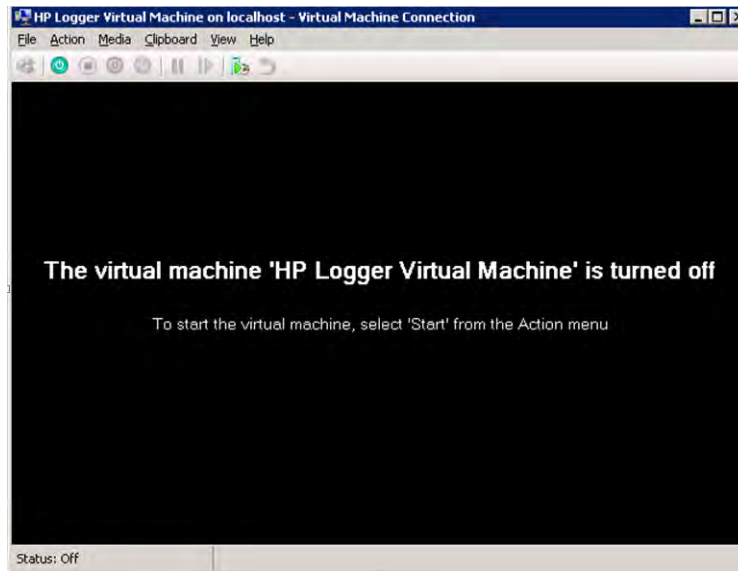
Configure the Logger Virtual Machine

Once you have created a Logger virtual machine, you need to configure the network settings valid for your environment—IP address, default gateway, NTP server, and so on.

To configure network setting on the Logger virtual machine:

- 1 Double click the hostname of the Hyper-V Manager in Server Manager.

The console window for the Logger virtual machine is displayed.



- 2 Click the Power button () to activate the virtual machine.

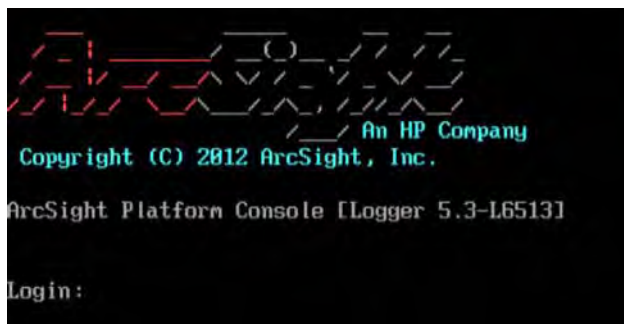
Although it takes some time to boot the virtual machine, use these troubleshooting tips if the virtual machine does not start:

- ◆ Ensure that virtualization is enabled in the BIOS.
- ◆ Disable hyperthreading

For more information about these settings, see the Windows Server 2008 R2 documentation.

- 3 Once the Logger console is displayed, enter the following default credentials to log in as the administrator:

Login: admin
Password: password



- 4 Configure a **static** IP address for the Logger that is valid for your environment using one of the following commands:
 - ◆ `set ip eth0 <ip>/<prefix>`
(Example: `set ip eth0 192.0.2.12/24`)
 - ◆ `set ip eth0 <ip> <subnetmask>`
(Example: `set ip eth0 192.0.2.12 255.255.255.0`)
- 5 Enter `set defaultgw <ip>`, replacing `<ip>` with your default gateway IP address.
- 6 Enter `set hostname <logger>`, replacing `<logger>` with the fully-qualified domain name (FQDN) of the desired host.
- 7 Enter `set dns <search_domain1>,<search_domain2> <nameserver1> <nameserver2>`, replacing each `<search_domainN>` with a search domain, and each `<nameserverN>` with the IP address of a name server. (Example: `set dns domain1.company.com,domain2.company.com 192.0.2.1 192.0.2.2`)



When using multiple search domains, separate them with a comma but no space. When using multiple name servers separate them with a space but no comma.

- 8 Enter `set ntp <ntp_server1> <ntp_server2> <ntp_server3>` replacing `<ntp_serverN>` with the NTP server you want to use to set the time. (Example: `set ntp time.nist.gov`)



Although configuring an NTP server is optional, it is strongly recommended because precise time stamping of events is critical for accurate and reliable log management on Logger.

- 9 Enter `show config` to review the configuration settings you entered in previous steps. If needed, change the settings.

You are ready to connect to your Logger interface.

Initialize the Logger Virtual Machine

A one-time configuration is required on Logger when it is freshly installed. This process is also referred as Logger initialization. During this process, you will configure settings such as timezone and locale. Additionally, you will have the option to configure three ArcSight Connectors that can collect events from the following Microsoft databases. These connectors are included in the Logger installation package for Hyper-V.

- Microsoft Audit Collection System
- Microsoft System Center Operations Manager
- Microsoft System Center Operations Manager 2005 and 2007



If your session times out or you close the browser before you have completed the connector configuration, you will not be able to restart the connector configuration wizard described in the following procedure. Instead, connect to the Logger UI as described in [“Connecting to Logger” on page 19](#) and go to **Configuration > Event Input > Connectors** to configure the connectors.

To initialize the Logger virtual machine:

- 1 From a supported Web browser, connect to the Logger using this URL:

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

where `hostname or IP address` is the one you configured in ["Configure the Logger Virtual Machine" on page 14](#).

- 2 You are directed to the End User License Agreement. Before you can proceed further, you must review and accept the license agreement.

Scroll down to the bottom of the screen to review the license. Mark the **I accept the terms of the License Agreement** checkbox and click **Accept**. The Login screen is displayed.

- 3 At the Login screen, use the following default credentials to log in as the administrator:

Username: admin

Password: password



Change the credentials as soon as possible after connecting to your Logger for the first time. See the ArcSight Logger Administrator's Guide for information on changing your password.

The Logger Configuration screen is displayed. This screen enables you to configure the settings to initialize your Logger.



Logger Configuration

Logger Configuration

Welcome to Logger!
Configure the following settings for Logger initialization.

License

Select License File to Upload

License Status

System Date/Time 01/08/2013 16:45:57
Model L750MB-V
License status Trial license.

System Locale Setting

The Locale setting ensures that the user interface displays information such as date, time, numbers, and messages in the format and language appropriate for the selected country.

Locale

Date/Time Settings

Current Time Zone

Current Time

- 4 Logger comes with a built-in trial license. You can upload a license file now or evaluate Logger by using the trial license.

- ◆ Click **Browse** to navigate to the license file for your Logger or enter the path and filename, and click **Upload License**.

If the license file is uploaded successfully, the License Status section (below the Upload License button) indicates that status.

- ◆ If you do not upload a license file, Logger uses the trial license. If you start with a trial license, you can upgrade to use a license file later.

- 5 In the System Locale Setting section, click the **Locale** drop-down list to select the Locale setting for this Logger.

The Locale setting ensures that the user interface displays information such as date, time, numbers, and messages in the format and language appropriate for the selected country. Once configured, the Locale setting cannot be changed.

- 6 In the Date/Time Settings section, click **Change Time Zone** and **Change Date/Time**, respectively, to update the time zone and date/time settings for your environment.

- 7 Click **Save**.

The Logger configuration begins. See [“Initial Logger Configuration” on page 20](#) for information about the default configuration on Logger.

Once the configuration is complete, Logger reboots automatically. The reboot process takes a few minutes. Do not refresh the browser page from which you are connected to Logger during this time. Doing so might result in an HTTP “404 Error”.

Once Logger has finished rebooting, the following ArcSight connector selection screen is displayed, which enables you to choose the connectors you want to install for collecting events for your Hyper-V Logger.



- 8 HP recommends that you add the connectors for the database servers from which you want Logger to receive events at this point. However, if you do not want to configure connectors at this stage, click **Cancel**. You can configure connectors later using the Logger UI.

If your session times out, you close the browser before you have completed the connector configuration, or you clicked Cancel in this step to configure connectors later, you will not be able to restart the connector configuration wizard described in this procedure. Instead, connect to the Logger UI as described in [“Connecting to Logger” on page 19](#) and go to **Configuration > Event Input > Connectors** to configure the connectors.

- 9 To add connectors, repeat the following steps for each connector you want to add:
 - a Select the connector name and then click **Next**.

- b** Enter the following settings that the connector will use to establish communication with your database server.

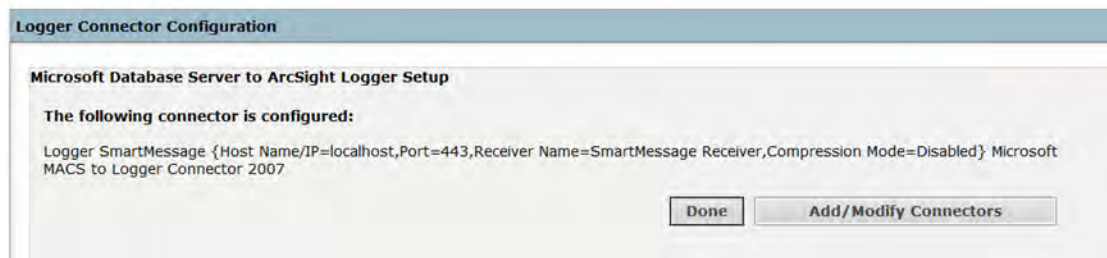
Setting	Description
Host/IP	Host name or IP address of the database server from which the connector will collect events
Port	Port number on which the connector will connect to the database server
Database	The name of the database for which the connector will collect events
User	Credential to use to authenticate to the database server from which the events will be collected Note: Because this connector is being installed on a non-Windows virtual machine, configure the Microsoft database from which it will collect events for Mixed Mode Authentication or SQL Server Authentication; integrated authentication on non-Windows operating systems is not supported.
Password	Password for the user name you specified above
Connector Name	A meaningful name to identify the connector
Smart Receiver	The name of the SmartMessage receiver that will receive events from the database server. This field is prepopulated with the value "SmartMessage Receiver".

- c** Click **Next**.

Once you see a message similar to the one in the following screen, the connector you selected has been configured.



System Configuration



- d** Click **Done** if you are done configuring all the connectors. OR
Click **Add/Modify Connectors** to add additional connectors.
- e** If you click Add/Modify Connectors, you are back at [Step 9 on page 17](#).

- f** If you click Done, the list of currently configured connectors is displayed, as shown in the following figure.

Microsoft Database Server to ArcSight Logger Setup

Click Add to add a connector, or use the Edit or Remove icons to edit or remove an existing connector.

Add

Name	Type	Host	Database		
Microsoft MACS to Logger Connector 2007	Microsoft Audit Collection System DB	HQENG-SQL2k5.arcsight.com	ACS2007		
Microsoft MOM to Logger Connector mom2007	Microsoft System Center Operations Manager 2005 and 2007 DB	HQENG-SQL2k.arcsight.com	MOM2007		

Done

Click **Done** again. The Logger configuration process begins. Once Logger has configured, the Logger Summary page is displayed. Your Logger is ready for use.

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

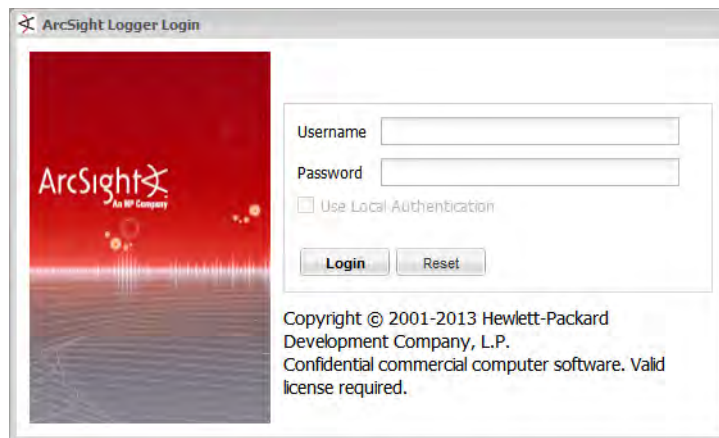
Connecting to Logger

Although the Logger initialization process connects you to the Logger interface automatically, if you need to re-establish connectivity, use this URL:

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

where hostname or IP address is the IP address configured for your Logger.

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



Use the following default credentials or the credentials you specified if you have already changed the 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—Default Storage Group and Internal Storage Group
Indexing	Enabled, full-text and field-based indexing
Receivers	Six total: One of each TCP, UDP, and SmartMessage type; and three Folder Follower receivers

Adding Connectors After Logger Initialization

During the Logger initialization process, you can install three ArcSight Connectors that can collect events from the following Microsoft databases.

- Microsoft Audit Collection System
- Microsoft System Center Operations Manager
- Microsoft System Center Operations Manager 2005 and 2007

If you did not install all of these connectors at that time, you can do so by following instructions in this section after Logger has been initialized.

To add the Microsoft database connectors once Logger has been initialized:

- 1 Click **Configuration** from the top-level menu bar.
- 2 Click **Event Input** (left panel) > **Connectors** tab (right panel).
- 3 Click **Add**.
- 4 Select the connector you want to add, and click **Next**.
- 5 Enter the settings as described in [Step 9b on page 18](#).


Modifying Connector Settings

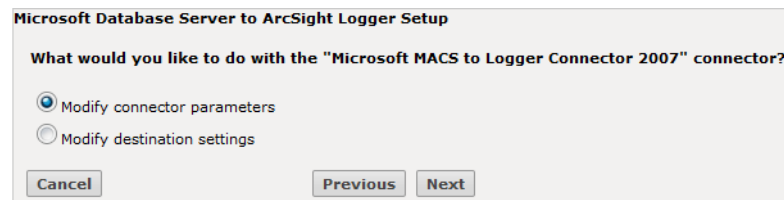
You can modify two types of settings on a connector:

- Connector parameters—Settings that the connector uses to communicate with the database server, such as hostname, user credentials, and so on.
- Connector destination settings—Settings that control various aspects of event collection and transmission to the connector destination (Logger, in this case), such as batching, time correction, and filtering. For more information, refer to the Destination Runtime Parameters appendix in the ArcSight Logger Administrator's Guide.

To modify connector settings:

- 1 Click **Configuration** from the top-level menu bar.
- 2 Click **Event Input** (left panel) > **Connectors** tab (right panel).

Click the  icon corresponding to the connector whose settings you want to modify. The following screen is displayed.



- 3 To modify connector parameters (as described earlier), select **Modify connector parameters**.

To modify connector destination parameters (as described earlier), select **Modify destination settings**.

Click **Next**.

- 4 If you selected Modify connector parameters, update the settings as described in [Step 9b on page 18](#). Click **Next**.

If you selected Modify destination settings, follow these steps to modify the settings:

- a Select the destination setting group to modify, such as Batching, Time Correction. Click **Next**.

For information about various destination settings, refer to the to the Destination Runtime Parameters appendix in the ArcSight Logger Administrator's Guide.

- b Configure the settings specific to the group you selected. Click **Next**.

- c Select **Edit more destination settings** to continue to configure additional destination settings. Go back to Step 5a. OR select **"Done with editing..."** if you are done.

Uninstalling Logger

If you need to uninstall Logger, delete the virtual machine you created and remove the associated .vhd files.

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.

The Hyper-V installation of Logger comes integrated with three connectors, which you configure during the installation process:

- Microsoft Audit Collection System
- Microsoft System Center Operations Manager
- Microsoft System Center Operations Manager 2005 and 2007

Once these connectors are configured, they start sending the events to the default SmartMessage receiver that is configured and enabled by default on your Logger.

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 on port 514. This port should be allowed through any firewall rules you have configured.
- A TCP receiver—Enabled by default on port 515. This port should be allowed through any firewall rules you have configured.
- A SmartMessage receiver—Enabled by default. To receive events from a SmartConnector, download the SmartConnector and set the **Receiver Name** to be “SmartMessage Receiver” when configuring the destination.

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



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

The preconfigured folder follower receivers include:

- Var Log Messages—/var/log/messages
- Apache URL Access Error Log—/opt/arcsight/userdata/logs/apache/http_error_log

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.



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 preinstalled 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 preinstalled 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 preinstalled 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. You configure the preinstalled receivers during the installation process.

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:

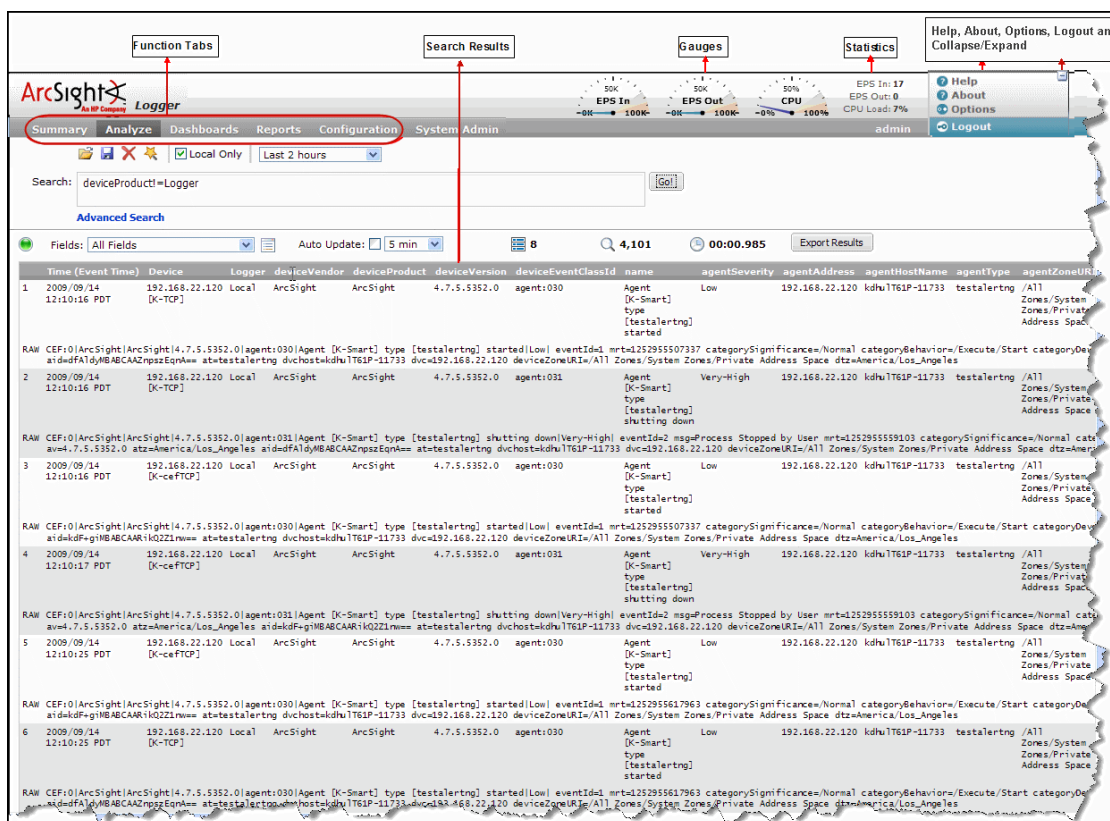
- 1** Install the SmartConnector component using the SmartConnector User's Guide as a reference. Specify Logger as the destination instead of ArcSight ESM or a CEF file.
- 2** Specify the required parameters. Enter the Logger hostname or IP address and the name of the SmartMessage receiver. These settings 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 use SmartMessage to communicate between an ArcSight SmartConnector and a Logger appliance, configure the SmartConnector to use port 443.
 - ◆ 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 29](#)). The range of the gauges can be changed on the Options page. The current logged-in user's name is shown below the statistics. The gauge and logo bar can be collapsed to allow more

room on the screen for search results and reports. Click the  icon to collapse the bar, and the  icon to expand it.

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

Help

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

Options

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

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

Options

System

EPS input rate gauge max

EPS output rate gauge max

Default start page for all users

Personal

Default start page for admin

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	283,758	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 all the search operators:

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

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

```
cef, rex
```

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

Examples:

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

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

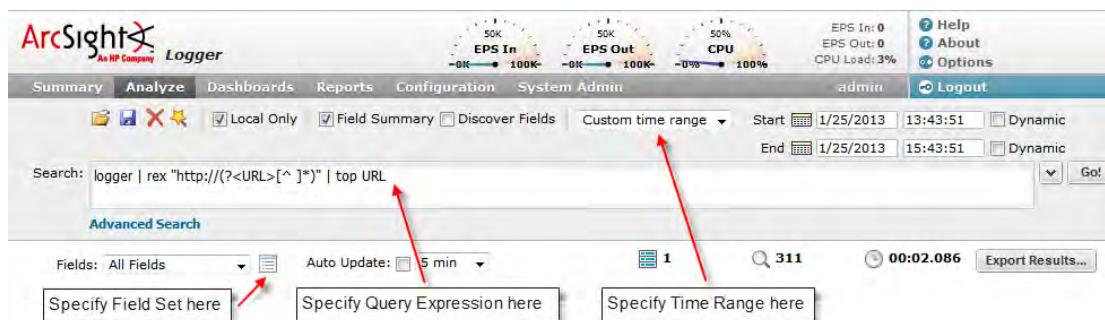
Displays search results in a tabular form of the most common values for the `deviceAddress` field. That is, the values are listed from the highest count value to the lowest.

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

Building a Query

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

- Query Expression—search conditions that are used to select or reject an event.
- Time range—the time range within which events should be searched.
- Field Set—fields of an event that should be displayed for matching events; for example, you can select to display only the `deviceAddress` and `deviceReceiptTime` fields of matching events.



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

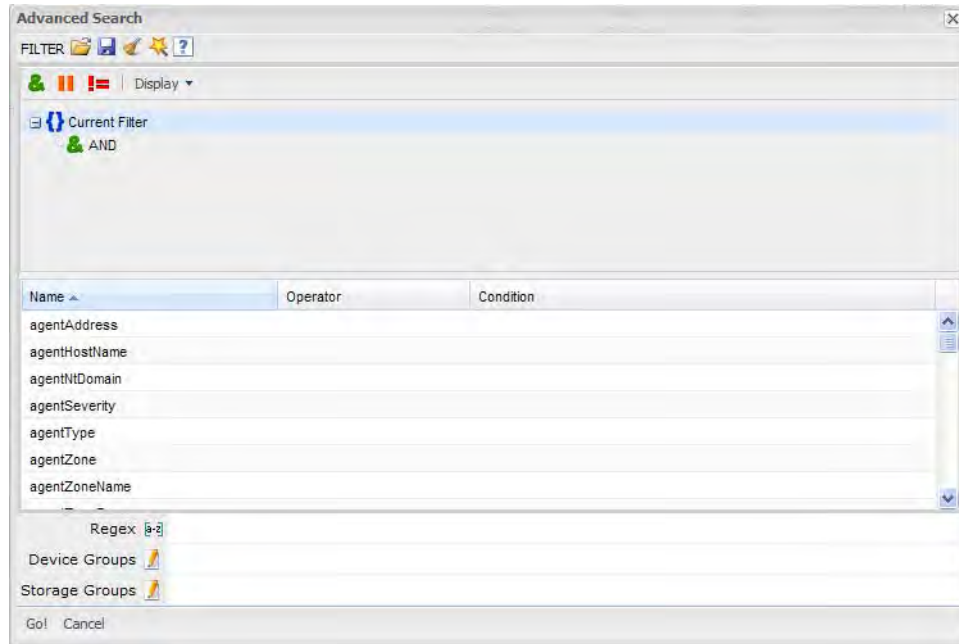
Query Building Tools

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.

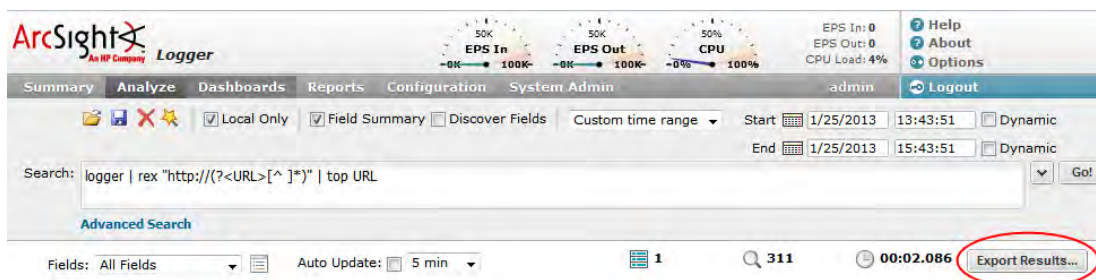
Exporting Search Results

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.

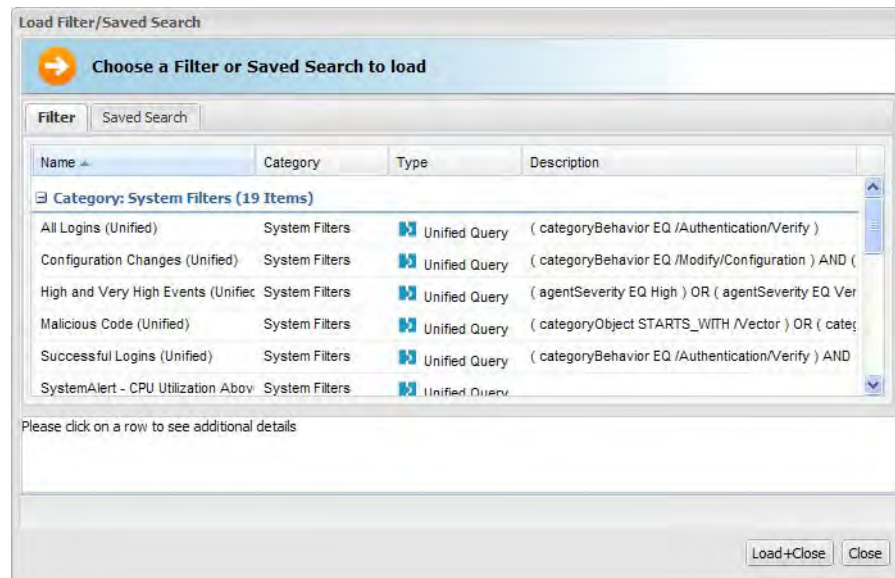
For more information about saving queries and using them again, refer to the ArcSight Logger Administrator's Guide.

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 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 occurs within the specified threshold, an alert is immediately triggered.	These alerts are triggered at scheduled intervals. That is, when a specified number of matches occurs within the specified threshold, an alert is triggered at the next scheduled time interval .

Real Time Alerts

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.

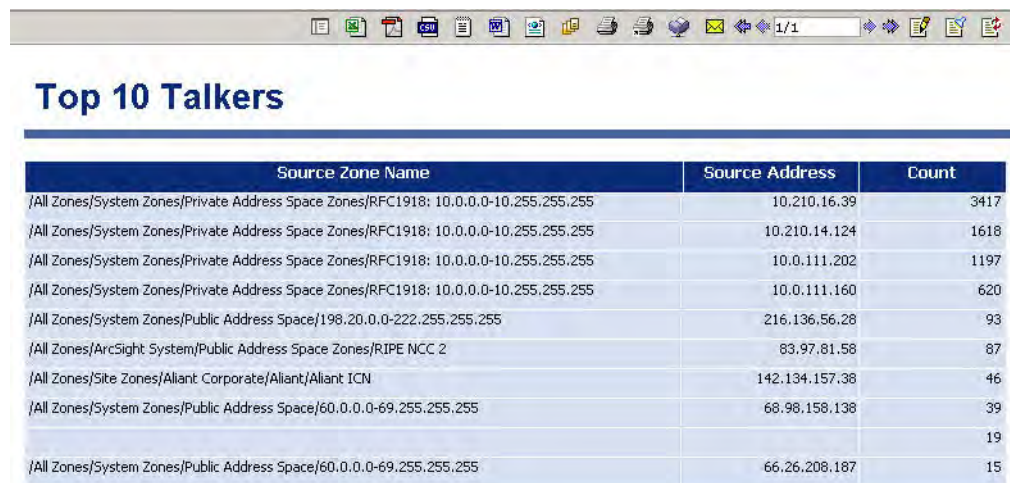
Chapter 7

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.



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 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
```

