Hewlett Packard
Enterprise

HPE Security ArcSight Logger

Software Version: 6.5

Installation and Configuration Guide

October 12, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/support-contact-information
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://community.saas.hpe.com/t5/ArcSight/ct-p/arcsight

Contents

About this Guide

This guide describes how to install and initialize version 6.5 of the ArcSight Data Platform (ADP) Logger and the standalone ArcSight Logger. It includes information on how to initialize the Logger Appliance and how to install the Software Logger on Linux and on VMware VM.

Note: Where there are no specific differences, all types of Logger are called *Logger* in this document. Where there are differences, the specific type of Logger is indicated.

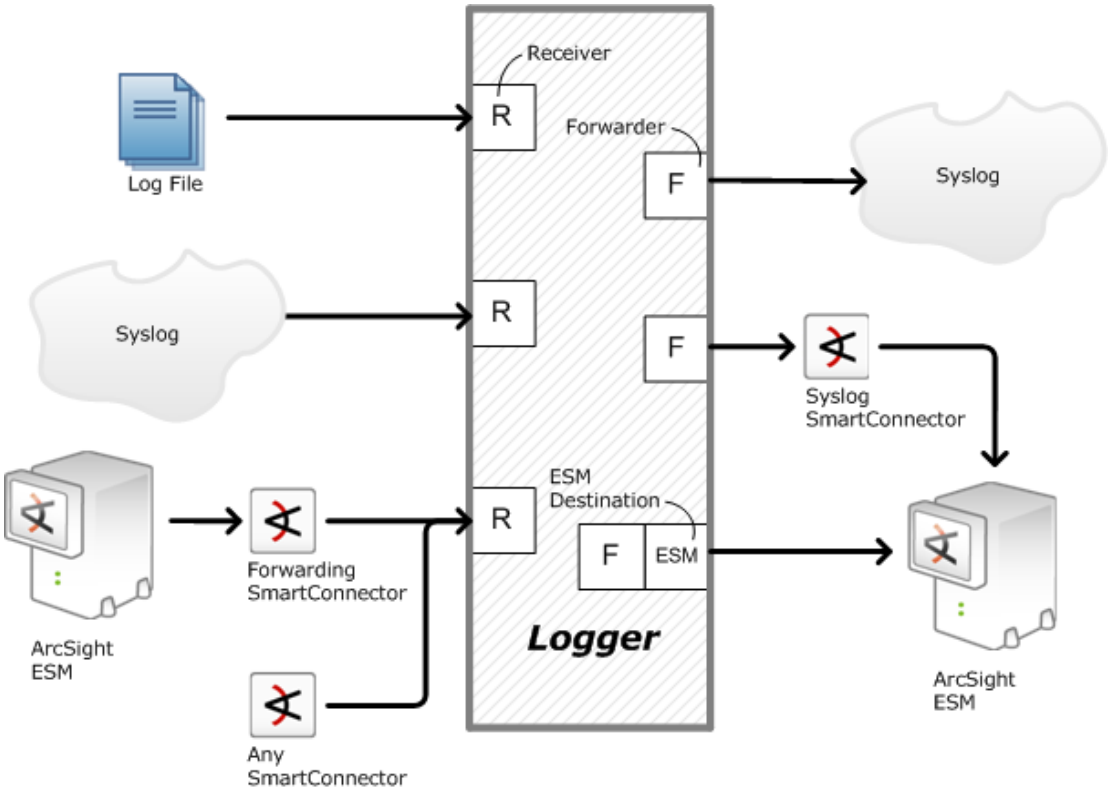
Chapter 1: Overview

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 log entry, such as a syslog message sent by a host, or a line appended to a log file. Logger receives and stores events; supports search, retrieval, and reporting; and can forward selected events for correlation and analysis to destinations such as a syslog server.

How Logger Works

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

SmartConnectors are the interface between Logger and devices on your network that generate events you want to store on Logger. SmartConnectors collect event data and normalize it into a Common Event Format (CEF). For more information about CEF, search for “ArcSight Common Event Format (CEF) Guide” in the ArcSight Product Documentation Community on Protect 724, and refer to "Implementing ArcSight 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. Alerts can notify you by e-mail, an SNMP trap, or a Syslog message.
- Establish dashboards that display events that match a specific query.
- Forward selected events to ArcSight ESM for correlation and analysis.
- Forward events to a syslog server.

Logger for Security, Compliance, and IT Operations

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

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

For a complete list of predefined content filters and predefined reports, refer to the ArcSight Logger Administrator's Guide. Information about how to use predefined filters is included in "System Filters (Predefined Filters)" on page 62.

Chapter 1: Deployment Planning

Before installing Logger, you should plan how you will store events and how long you need to retain them. Consider the information in the sections below when planning your deployment:

Getting the Latest Documentation

The latest version of the documentation for this release is available for download (in PDF format) from the ArcSight Product Documentation Community on Protect 724.

Help is available through the Logger user interface (UI) . To access the online help from any user-interface page, click the down-arrow by your user name and then select Help.

Trial Licenses

ArcSight Logger both come with a trial license that you can use for a 90 day evaluation period. After the evaluation period is over, you will not be able to access any Logger features until you apply a valid license.

The trial license gives you access to the following:

- All Logger features except Reporting.
- 5 GB per day ingested data volume. (Software Loggers only.)
- 90 GB Storage Volume.

Please upload your full license as soon as possible. To upload a new license, open **System Admin** in the menu bar, and then click **License & Update** in the **System** section. For instructions, refer the System Admin chapter of the Logger Administrator's guide.

Depending on whether your license entitles you to management by ArcMC, you can update the trial license with either a standalone license or an ADP license. (ADP Loggers are managed by ArcMC.) After you upload either license, the Reporting feature is enabled, and the licensed daily data volume and storage volume are increased to the capacity of the license.

The ingested daily data volume of your Logger is displayed on the Data Volume page under **Configuration | Advanced > Data Volume**. You can view your daily data limit and other license information in Logger under **Configuration | Advanced > License Information** and under **System Admin > System > License & Update**.

Initial Configuration

The installation and initialization process sets up your Logger with an initial configuration described in the sections below. You can do additional configuration on Logger to implement your retention policies. See "Configuring Logger" on page 43. For further information, refer to the Configuration chapter of the Logger Administrator's guide.

Logger's initial configuration is described in the sections below:

Storage Volume

Logger's storage volume varies by version, up to the maximum of 12 TB. The initialization process sets the storage volume. For Logger appliances, the storage volume is set to the maximum capacity for the model or to 12 TB, whichever is smaller. For software Loggers, the storage volume is set to the maximum capacity specified in the license or the available disk space, whichever is smaller.

Caution: If Logger's maximum capacity is exceeded, events will begin to fall out of storage. For information on how to retain these events, refer to the Configuration chapter of the Logger Administrator's Guide.

After installing Logger, you can view the current limits on the **Configuration > Advanced > License Information** page. For instructions, refer to the Configuration chapter of the Logger Administrator's Guide. For more information about licenses, including how to upload a new one, refer to the System Admin chapter of the Logger Administrator's Guide.

Storage volume can be extended after installation, but not reduced. For more information on increasing the storage volume, refer to the Configuration chapter of the Logger Administrator's Guide.

Storage Groups

Two storage groups, the Default Storage Group and the Internal Event Storage Group, are created automatically during Logger initialization.

These storage groups come preconfigured with the following settings:

Preconfigured Default Storage Group Settings

Attribute	Appliance Logger	Software Logger
Size	1/2 Storage volume capacity	1/2 Storage volume capacity
Retention Period	180 days	180 days

Preconfigured Internal Storage Group Settings

Attribute	Appliance Logger	Software Logger
Size	5 GB	3 GB
Retention Period	365 days	365 days

Logger can have a maximum of six storage groups; therefore, you can create an additional four storage groups after your Logger has been initialized. Each storage group can have different settings. You can change the retention policy and size for all storage groups, but you can only change the name of the user-defined storage groups. Refer to the Configuration chapter of the Logger Administrator's Guide for the details of adding and resizing storage groups, and changing their retention policies.

Search Indexes

Logger comes prepared for full-text searches, also frequently used fields are indexed during initialization. You can add additional fields to the index, but once a field has been added, you cannot unindex it. Refer to the Search chapter of the Logger Administrator's Guide for more information.

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. Before a receiver can receive data, the port it is listening on must be opened through the firewall. For more information, see "Firewall Rules" on the next page.

You can also change and delete receivers or disable and enable them as needed.

Tip: Be sure to update the firewall configuration whenever you add or remove a receiver.

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

- A UDP receiver: Enabled by default.

  The UDP receiver is on port 514/udp for Logger Appliances. If you are installing Software Logger as root, the UDP receiver is on port 514/udp. For non-root installs, it is on port 8514/udp. If this port is already occupied, the initialization process selects the next higher unoccupied port.
- A TCP receiver: Enabled by default.

  The TCP receiver is on port 515/tcp for Logger Appliances. If you are installing Software Logger as root, the TCP receiver is on port 515/tcp. For non-root installs, it is on port 8515/tcp. If this port is already occupied, the initialization process selects the next higher unoccupied port.
- A SmartMessage receiver: Enabled by default.

  To receive events from a SmartConnector, download the SmartConnector and set the **Receiver Name** to be "SmartMessage Receiver" when configuring the destination. The SmartMessage receiver listens on the same port as the User Interface, 443/tcp on Logger appliances, and typically 443/tcp on

Software Logger installed as root, and 9000/tcp on Software Logger installed as non-root. The Software Logger ports may vary.

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.

For Software Logger, 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`

  Note: The 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.

Auditing is disabled on some Logger Appliance models. Logger Appliances that have auditing enabled will have the same preconfigured receivers as Software Logger.

When auditing is disabled on the system where Logger is installed, 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`

For instructions on how to enable the preconfigured receivers, see "Receivers" on page 43. For more information about all Logger receivers, refer to the Configuration chapter of the Logger Administrator's Guide.

Firewall Rules

Before Logger can receive data, some ports must be opened through the firewall.

- For Software Logger, you are responsible for setting up the firewall. After you first install or Logger 6.5, you should configure the firewall to be open only for the ports required for your configuration.

  Caution: HPE ArcSight strongly recommends that you configure your firewall so that only the required ports are open.

- For the Logger Appliance, the firewall is preconfigured. HPE ArcSight provides a script you can use to update the firewall.

Tip: Be sure to update the firewall configuration whenever you add or remove any service that requires an open port for incoming traffic, such as a receivers or SNMP polling.

Refer to the System Admin chapter of the Logger Administrator's Guide for a list of default ports and other information.

Chapter 2: Setting Up a Logger Appliance

This chapter describes how to rack mount your Logger appliance, and to configure an IP address and initial settings for it. You do not need to run an installer when setting up your appliance; the Logger software comes pre-installed on it. These basic steps enable you to start using your Logger Appliance:

For information on how to install Software Logger on Linux, see "Installing Software Logger on Linux" on page 24. For information about installing Software Logger on VMware VM, see, "Installing Software Logger on VMware" on page 42.

Running Logger on Encrypted Appliances

Logger can be run on encrypted hardware to help you to meet compliance regulations and privacy challenges by securing your sensitive data at rest.

You can encrypt your L7600 Logger Appliance by using HPE Secure Encryption, available from the Server Management Software > HPE Secure Encryption web page. For instructions, refer to the HPE Secure Encryption Installation and User Guide, available in PDF and CHM formats through the Technical Support / Manuals link on that page.

L7600 Logger Appliances are encryption capable. They come pre-installed with everything necessary for you to encrypt them using HPE Secure Encryption. The length of time encryption takes depends on the amount of data on the server being encrypted. In our testing, an L7600 Logger Appliance with 7.5 TB of stored data took about 72 hours to encrypt. You can continue using Logger while the encryption runs. You may notice some performance degradation after encrypting your existing Logger appliance.

Caution: After encryption, you cannot restore your Logger to its previously unencrypted state.

Installing the Logger Appliance

Before you Begin:

- Redeem your license key by following the instructions in the enclosed “License Entitlement Certificate” document. Redeeming this key gets you the license that you need to access Logger functionality. For more information, see "Acquiring a License for the Logger Appliance" on page 18.
- Apply for an account on Protect 724 (https://www.protect724.hpe.com), the ArcSight user community. You will need this account to access product documentation and other community-based resources.

To install the appliance:

1. Unpack the appliance and its accompanying accessories.

   Note: Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.
3. Make the rear panel connections.
4. Power on the appliance.

Configuring an IP Address for the Appliance

The appliance ships with the default IP address 192.168.35.35 (subnet mask 255.255.255.0) on eno1. To begin setting up your appliance, follow the steps below to configure a new IP address on the Logger Appliance command line interface (CLI).

To run a command in the Logger CLI, type it at the prompt and press Enter. For more information on the command line interface, see "Using the Logger Appliance Command Line Interface" on page 20 or enter `help` at the prompt for a list of available commands.

Note: You can configure your appliance with and IPv4 address, an IPv6 address or both.

To set up a new IP address:

1. Use one of the following methods to connect to the Logger (not the operating system) CLI:
   - Log into HPE ProLiant Integrated Lights-Out (iLO) and launch the remote console feature. For more information, see "Setting Up the Appliance for Remote Access" on the next page.
   - Connect a keyboard and monitor to the ports on the rear panel of the appliance.
   - Connect a terminal to the serial port on the appliance using a null modem cable with DB-9 connector. The serial port expects a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control.

     Once you are connected to the CLI, a log in prompt is displayed.

2. Enter the following default credentials to log in as the administrator:

   ```
   Login: admin
   Password: password
   ```

3. Configure an IPv6 address either by providing static IPv4 address or choosing auto (SLAAC) configuration.
   - For Static IPv4 configuration use following command format:
     `set ipv4 eno1 <ip>/<prefix>`

Example: `set ipv4 eno1 192.0.2.5/24`

- For Auto IPv4 configuration user following command format:
  `set ipv4 eno1 <ip> <subnetmask>`
  Example: `set ipv4 eno1 192.0.2.5 255.255.255.0`

4. Enter `set defaultgw <ip>`, replacing `<ip>` with your default gateway IP address.
5. Enter `set hostname <domain>.<company.com>`, replacing `<domain>.<company.com>` with the fully-qualified domain name (FQDN) of the desired host.
6. 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`

   Tip: 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.

7. 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`

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

Setting Up the Appliance for Remote Access

All ArcSight appliances are equipped with an HPE ProLiant Integrated Lights-Out (iLO) Advanced remote management card. HPE strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you (and Customer Support, with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and power control.

Follow the directions in the HPE ProLiant Integrated Lights-Out User Guide to set up your appliance for remote access. The guide is available at http://www8.hp.com/us/en/products/servers/ilo/index.html.

Note: The L7600 models require you to obtain and enter a license key. The iLO license is preinstalled, but you should obtain and keep your iLO license key and documentation for potential future use. This license key can be used with any replacement appliance.

Instructions for obtaining the license key are included on your License Entitlement Certificate. Once you have obtained the license key, log into iLO, and then go to **Administration > Licensing** to enter it.

Acquiring a License for the Logger Appliance

A valid license file must be applied to the Logger Appliance before you can access some Logger functionality. For information and restrictions, see "Trial Licenses" on page 10. To acquire the license, follow instructions in the "Entitlement Certificate" document included in the shipment with your Logger Appliance to redeem your license key. If you do not have that document, contact customer support at https://softwaresupport.hpe.com.

Note: If you have multiple Loggers, you may need a separate license file for each of them, depending on your purchase order.

After initializing Logger, you can view the specific details of the current license on the License Information and License & Update pages (**Configuration > Advanced > License Information** and **System Admin > System > License & Update**). For more information, refer to the Configuration and System Admin chapters of the Logger Administrator's Guide.

Connecting to the Logger Appliance

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.5 browser support.

Logger's publicly-accessible ports must be allowed through any firewall rules. For Software Logger, you are responsible for setting up the firewall. Firewall rules are preconfigured on the Logger Appliance. See "Firewall Rules" on page 13 for more information.

- For root installs, allow access to port `443/tcp` as well as the ports for any protocol that the logger receivers need, such as port `514/udp` for the UDP receiver and port `515/tcp` for the TCP receiver.
- For non-root installs, allow access to port `9000/tcp` as well as the ports for any protocol that the Logger receivers need, such as port `8514/udp` for the UDP receiver and port `8515/tcp` for the TCP receiver.

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

JavaScript and cookies must be enabled.

To connect and Log in for the first time:

1. Connect to Logger:

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

   For Software Logger: `https://<hostname or IP address>:<configured_port>`

For Logger Appliance: `https://<hostname or IP address>`

where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

2. The **END USER LICENSE AGREEMENT** is displayed. Scroll down to the bottom of the screen to review and accept the EULA. After you accept, the Login screen is displayed.
3. Log in:

   When the Login dialog is displayed, enter your user name and password, and click **Login**.

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

   Username: admin
   Password: password

   > **Note:** After logging in for the first time with the default user name and password, you will be prompted to change the password. Follow the prompts to enter and verify the new password.

   For more information about the Login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator's Guide.

Once you have successfully logged in, proceed to the section, "Initializing the Logger Appliance" below.

Initializing the Logger Appliance

After you accept the EULA and log in for the first time, the **Logger Configuration** screen is displayed. On this screen, you can upload the license file and configure the initial settings for your Logger Appliance. Once you complete that configuration, your Logger Appliance will be ready for use.

> **Note:** The initialization of a Logger Appliance can only be changed by restoring Logger to its initial factory settings. Refer to the Logger Administrator's Guide for more information.

Logger comes with a trial license that is good for 90 days. This license provides limited functionality. You must upload your full ArcSight Data Platform Logger or standalone ArcSight Logger license access the full functionality. See "Trial Licenses" on page 10 for more information.

If you do not have a license, see "Acquiring a License for the Logger Appliance" on the previous page.

To initialize the Logger Appliance:

1. You can upload a full license when you first connect or use trial license for now and upload the license later.
   - If you have a license, you can apply it now.

     To apply the license, on the **Logger Configuration** screen, under **Select License File to Upload**, navigate to or specify the path and file name of the license for the Logger Appliance, and click **Upload License**.

After the upload, the License pane displays updated license status information.

- If you do not to apply a license now, be sure to apply before the trial license expires.

2. Under **System Locale Setting**, select a **Locale** for this Logger Appliance from the drop-down list.

   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, this setting cannot be changed.

3. Under **Date/Time Settings**, ensure that the “Current Time Zone” and the “Current Time” settings are correct for your environment.

   Click **Change Time Zone** and **Change Date/Time**, respectively, to update the time settings. For more information, refer to the System Admin chapter of the Logger Administrator’s Guide.

4. Click **Save**.

   The Logger initialization process begins. Once the initialization is complete, the system reboots. Now that you are done installing and initializing your Logger, go to the "Configuring Logger" chapter of the Logger Installation Guide for information on how to set up your Logger to start receiving events.

Now that you are finished installing and initializing your Logger, you can enable the preconfigured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy. See "Configuring Logger" on page 43 and refer to the Configuration chapter of the Logger Administrator's Guide for information on how to set up your Logger to start receiving events.

For more information about the login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator’s Guide.

Using the Logger Appliance Command Line Interface

The Logger appliance CLI enables you to start and stop the appliance as well as issue commands for the Logger application.

Use one of the following methods to connect to the appliance Command Line Interface (CLI):

- Log into HPE ProLiant Integrated Lights-Out (iLO) and launch the remote console feature. For more information, see "Setting Up the Appliance for Remote Access" on page 17.
- Connect a keyboard and monitor to the ports on the rear panel of the appliance.
- Connect a terminal to the serial port on the appliance using a null modem cable with DB-9 connector.

  The serial port expects a standard VT100-compatible terminal: **9600 bps**, **8-bits**, **no parity**, **1 stop bit** (**8N1**), **no flow control**.
- Once you are connected to the CLI, a Login prompt displays.

The following commands are available at the CLI prompt:

Category	Command	Description
System Commands		
	exit	Logout
	halt	Stop and power down the Logger Appliance
	help	Opens the command line interface help
	reboot	Reboot the Logger Appliance
Administrative Commands		
	show admin	Show the default administrator user's name
Authentication Commands		
	reset authentication	Revert the authentication mechanism to the default, local authentication. This can be useful if a different authentication mechanism such as CAC, LDAP or Radius had been configured and is somehow no longer working.
Configuration Commands		
	show config	Show host name, IP address, DNS, and default gateway for the Logger
Date Commands		
	show date	Show the date and time currently configured on the Logger
	set date	Set the date and time on Logger The date/time format is yyyyMMddhhmmss Example date: 20101219081533
Default Gateway Commands		
	set defaultgw <IP> [nic]	Set the default gateway for one or all network interfaces
	show defaultgw [nic]	Display the default gateway for all or the specified network interface
DNS Commands		
	show dns	Show the currently configured DNS servers on the Logger
	set dns <sd> <ns> set dns <sd1>,<sd2> <ns1> <ns2>	Set DNS name server(s) sd=search domain, ns = name server You can add up to three name servers and six search domains

Category	Command	Description
		Note: 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.
Hostname Commands		
	show hostname	Show the currently configured hostname on the Logger
	set hostname <host>	Set Logger's host name
IP Commands		
	show ip [nic]	Show the IP addresses of all or the specified network interface
	set ip <nic> <IP> [/prefix] [netmask]	Set Logger's IP address for a specific network interface
NTP Commands		
	set ntp <ntp server> <ntp server> <ntp server> ...	Sets the NTP server addresses. This entry over writes the current NTP server setting You can specify as many NTP servers as you like. If you specify multiple NTP servers, they are each checked in turn. The time given by the first server to respond is used. Example: `logger> set ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
	show ntp	Show the current NTP server setting. Example: `logger> show ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
Password Commands		
	set password	Set the password the current user's account
Process Commands		
	restart process	Restart a process
	start process	Start a process
	status process	Show process status
	stop process	Stop a process

Category	Command	Description
SSL Certificate Commands		
	show sslcert	Show the currently loaded SSL certificate on Logger
	reset sslcert	Creates and installs a new self-signed certificate with the original default information, then restarts the HTTPS server.
	diag sslcert	Display the SSL session information
Status Commands		
	show status	Show the Logger configuration

Chapter 3: Installing Software Logger on Linux

You can install Software Logger on a Linux system or on a VMware virtual machine (VM). This chapter explains what you need to know to install and start running Software Logger on a Linux system. It includes information on the following topics:

For information about installing Software Logger on a VMware VM, see, "Installing Software Logger on VMware" on page 42. For initialization information about the Logger Appliance, see "Setting Up a Logger Appliance" on page 15.

Before You Begin

You need to have a server with supported operating system and storage available to install the Software Logger. For information about the platforms on which you can install and use Logger, refer to the Release Notes and ArcSight Data Platform Support Matrix for your version. These documents are available for download from the ArcSight Product Documentation Community on Protect 724.

Downloading the Installation Package

The installation package is available for download from the HPE Software Depot at https://h20392.www2.hpe.com/portal/swdepot/index.do.

Verifying the Downloaded Installation Software

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

Visit the following site for information and instructions:

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

How Licensing Works in Software Logger

Logger comes with a trial license that is good for 90 days. This license provides limited functionality. You must upload your full ArcSight Data Platform Logger or standalone ArcSight Logger license access the full functionality. See "Trial Licenses" on page 10 for more information.

If you do not have a license file, see "Acquiring a License for Software Logger" on page 26. Depending on your purchase order, you need a separate license file for each instance of Software Logger. A license file is uniquely generated for each Logger download.

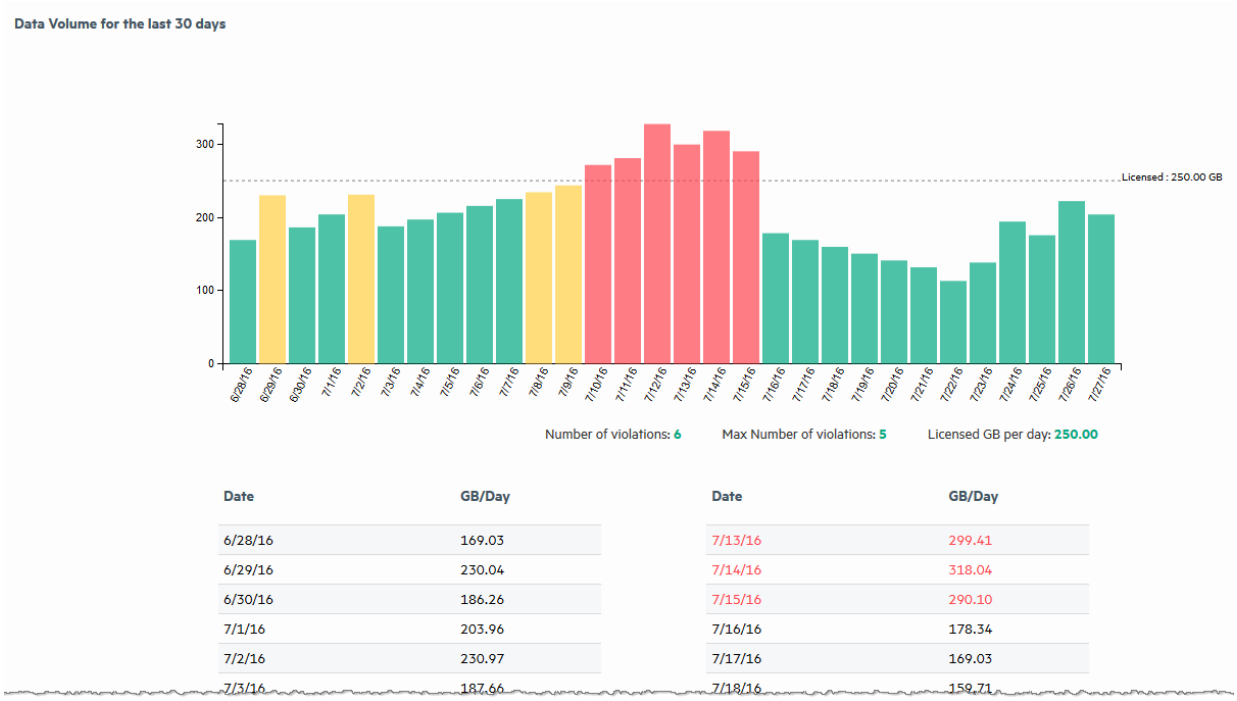
The type of license you have affects how the data volume restriction function works and what is displayed on the Data Volume page.

- For ADP Loggers, ArcMC manages the license restrictions. Refer to the ArcMC Administrator's Guide for more information.
- For standalone ArcSight Loggers, the data volume restriction function manages the license restrictions.

The data volume restriction function adds the sum of the sizes of the events received on a given day to compute the ingested daily data volume (the amount of data that comes into Logger per day). Logger compares that value against the daily data limit in the license. If this limit is exceeded, Logger continues to collect and store events, so that no events are lost. However, if the daily data limit is exceeded on more than five days in a 30-day sliding window, all search-related features are disabled. You will not be able to forward, search, or run reports on the collected events until the 30-day sliding window contains five or less data limit violations.

For example, you install the Logger software on January 1 with an ingested daily data limit of 20 GB and start collecting events. Your Logger receives more than 20 GB of event data on these dates: January 5th, 13th, 18th, 19th, and 20th. Because there are five violations so far, you can forward, search, and report on the stored event data on January 21st. However, if there is another violation on January 30th, you cannot forward, search, or report on January 31st because the number of violations has exceeded the maximum allowed. (A search run on January 31st fails and the user interface displays a warning.) If there are no additional ingested daily data violations from January 31st to February 4th, the ability to forward, search, and report resumes on February 5th because the January 5th violation is now outside of the 30-day window.

The Data Volume page (**Configuration > Advanced > Data Volume**) lists the data stored on your Software Logger on day-by-day basis in the last 30 days. It also indicates the days on which data limits were exceeded, as shown in the following figure.



Date	GB/Day	Date	GB/Day
6/28/16	169.03	7/13/16	299.41
6/29/16	230.04	7/14/16	318.04
6/30/16	186.26	7/15/16	290.10
7/1/16	203.96	7/16/16	178.34
7/2/16	230.97	7/17/16	169.03
7/3/16	187.66	7/18/16	159.71

When a data limit violation occurs, the Search user interface displays a warning. If you exceed the daily data limit frequently, you should consider purchasing a license that suits your needs. Contact your HPE ArcSight sales representative to purchase a new license. Once you obtain the new license, follow the instructions in the ArcSight Logger Administrator's Guide to apply it on your Logger.

Acquiring a License for Software Logger

Software Logger requires a license file for installation. To acquire the license, follow the instructions in the Electronic Delivery Receipt you receive from HPE in an email after you place the order. If you do not have that document, contact customer support at https://softwaresupport.hpe.com.

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

Prerequisites for Installation

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

- Ensure that you are installing Logger on a supported platform. Refer to the Release Notes and ArcSight Data Platform Support Matrix for this information. These documents are available for download from the ArcSight Product Documentation Community on Protect 724.
- If you are installing on RHEL 7.X, edit the `logind.conf` file as described in "Editing the logind Configuration File for RHEL 7.X" on page 29.

- Increase the user process limit on your Operating System, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on the next page.
- Make sure that you have the latest supported tzdata rpm, tzdata2017b, installed on your OS **before** installing Logger.
- Before deploying in a production environment, get valid license file. If you do not have a license file, see "Acquiring a License for Software Logger" on the previous page. You may need a separate license file for each instance of Logger. A license file is uniquely generated for each download.
- A non-root user account must exist on the system on which you are installing Logger, or the installer will ask you to provide one. Even if you install as root, a non-root user account is still required. The userid and its primary groupid should be the same for this account. The UID for the non-root user should be 1500 and the GID should be 750. For example, to create the non-root user, run these commands as `root`:

  ```
  groupadd –g 750 arcsight
  useradd –m –g arcsight –u 1500 arcsight
  ```

  These commands create a non-root user named `arcsight` that will work with a Logger software installation.
- Decide whether to install Logger while logged in as root or as a non-root user. Your installation options vary depending on which user you choose.

  Tip: If you are installing as a non-root user, the user must have privileges to write to the installation directory and its sub-directories. For example, for the non-root user arcsight, use the command `chown -R arcsight:arcsight /opt/arcsight`.

  a. If you install as root, you can choose to configure Logger to start as a service and select the port on which Logger listens for secure web connections.

  b. If you install as the non-root user, Logger can only listen for connections on port 9000/tcp. You cannot configure the port to a different value.

  Note: The user must have privileges to write to the installation directory and its sub-directories, for example, `chown –R arcsight /opt/arcsight`.

  c. When upgrading, you cannot change a previous non-root installation to a root-user installation. You will need to use the previously configured port 9000/tcp for accessing Software Logger.
- Install into an empty folder. If you have uninstalled Logger previously, and are installing into the same location, be sure to remove any files that the uninstaller left in place.
- The hostname of the machine on which you are installing Logger cannot be “localhost.” If it is, change the hostname before proceeding with the installation.
- You must not have an instance of MySQL installed on the machine on which you install Logger. If an instance of MySQL exists on that machine, uninstall it before installing Logger.
- If you are installing/ uninstalling Logger in console mode with a non-root user, you must unset the DISPLAY environment variable by executing the following command `unset DISPLAY`.

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

Increasing the User Process Limit and the Maximum Number of Open Files

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

To increase the default user process limit:

1. Open the file `/etc/security/limits.d/<NN>-nproc.conf`.
   (`<NN>` is 90 for RHEL or CentOS 6.X and 20 for RHEL and CentOS 7.X.)
   - If you do not already have a `/etc/security/limits.d/<NN>-nproc.conf file,` create one (and the `limits.d` directory, if necessary).
   - If the file already exists, delete all entries in the file.
2. Add the following lines:

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

   Caution: Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system run-time errors.
3. Log out and log back in again.
4. Run the following command to verify the new settings: `ulimit -a`
5. Verify that the output shows the following values for “open files” and “max user processes”:

   ```
   open files 65536
   max user processes 10240
   ```

After you have increased the user process limit and met the other prerequisites, you are ready to install Logger.

Editing the logind Configuration File for RHEL 7.X

Before installing or upgrading Logger on Red Hat Enterprise Linux (RHEL) 7.1 or 7.2, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the logind.conf file for RHEL 7.X:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the RemoveIPC line. RemoveIPC should be active and set to no.

   Remove the # if it is there, and =change the `yes` to no if appropriate. The correct entry is:

   ```
   RemoveIPC=no
   ```
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect:

   ```
   systemctl restart systemd-logind.service
   ```

After you have modified this setting and met the other prerequisites, you are ready to install Logger.

Installation

Software Logger can be installed in three ways:

- GUI mode: A wizard steps you through the installation and configuration of Software Logger. You must have an X-Windows server installed on your OS to use GUI mode.
- Console mode: A command-line process steps you through the installation and configuration of Software Logger.

  Tip: If you are installing remotely and bandwidth is an issue, console mode may allow you to install Logger more quickly.
- Silent mode: You provide the input required for installation and configuration through a file. Therefore, you do not need to interact with the installer to complete the installation and configuration on each server. However, before you can use this mode, you must run the installation and configuration using one of the other modes to record the input in a file.

Using GUI Mode to Install Software Logger

Make sure the machine on which you will be installing Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 26 are met.

Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on page 28, and for RHEL 7.X only, modify the `logind.conf` file, as described in "Editing the logind Configuration File for RHEL 7.X" on the previous page.

You can verify that you have the correct installation file, as described in "Verifying the Downloaded Installation Software" on page 24.

You can install Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 26 for details and restrictions.

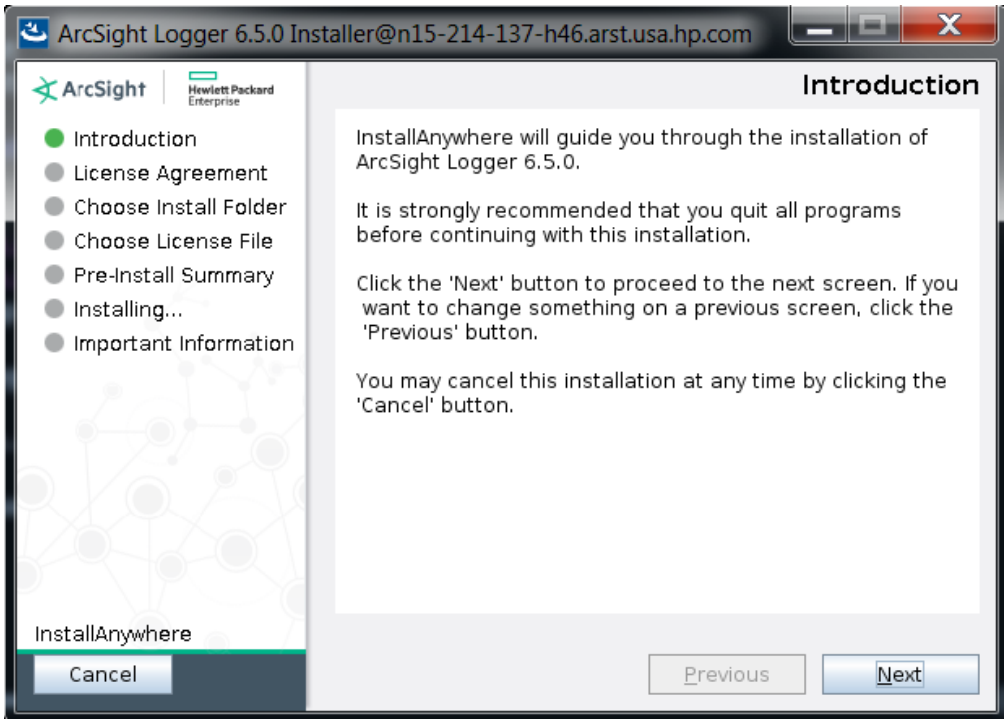
Note: If you will be installing the Software Logger over an SSH connection and want to use the GUI mode of installation, make sure that you have enabled X window forwarding using the `-X` option so that you can view the screens of the installation wizard. If you will be using PuTTY, you will also need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

To install the Logger software:

1. Run these commands from the directory where you copied the Logger installation file:

   ```
   chmod u+x ArcSight-logger-6.5.XXXX.0.bin
   ./ArcSight-logger-6.5.0.XXXX.0.bin
   ```

2. The installation wizard launches. Click **Next**.



You can click **Cancel** to exit the installer at any point during the installation process.

Caution: Do not use the Ctrl+C to close the installer. If you use Ctrl+C to exit the installer and then uninstall Logger, uninstallation may delete your `/tmp` directory.

3. The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the "I accept the terms of the License Agreement" button.
4. Select **I accept the terms of the License Agreement** and click **Next**.
5. The installer checks that installation prerequisites are met:
   - Operating system check—the installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS.

     Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

   - Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

   Example

   An Intervention Required message displays, informing you that a parameter needs to be changed from `yes` to `no` in the `etc/logind.conf` file. The message tells you what needs to be done. In this example, quit the installer, and follow the instructions in "Editing the logind Configuration File for RHEL 7.X" on page 29. When the file has been modified and saved, enter the installation command again.

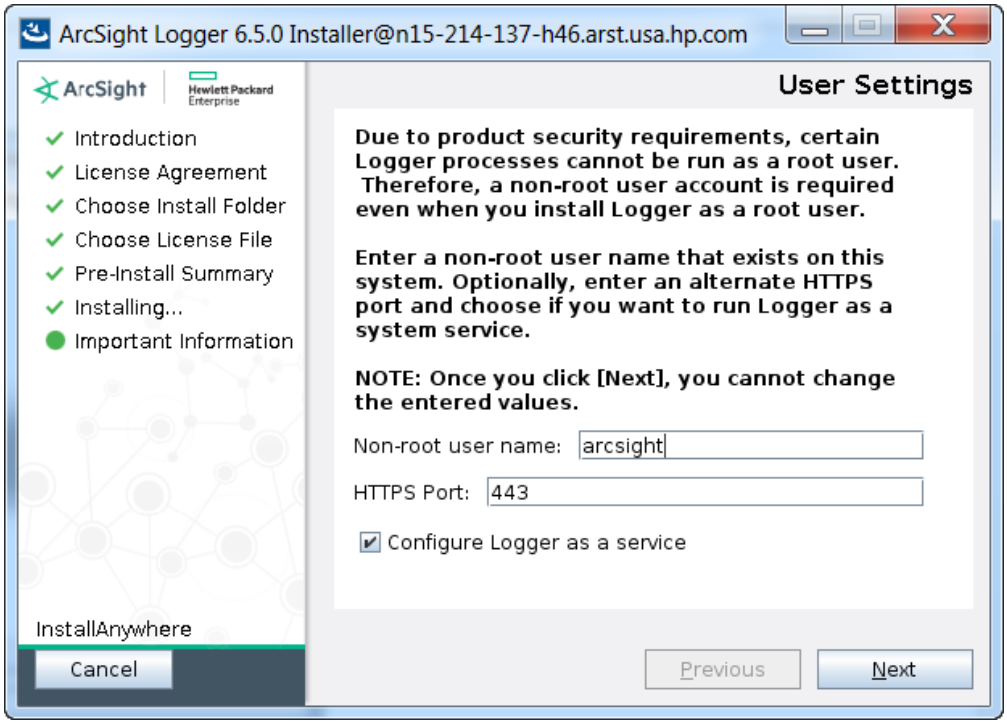
   Once all the checks are complete, the Choose Install Folder screen is displayed.
6. Navigate to or specify the location where you want to install Logger.

   The default installation path is `/opt`. You can install into this location or another location of your choice.
7. Click **Next** to install into the selected location.
   - If there is not enough space to install the software at the location you specified, a message is displayed. To proceed with the installation, specify a different location or make sufficient space available at the location you specified. Click **Previous** to specify another location or **Quit** to exit the installer.
   - If Logger is already installed at the location you specified, a message is displayed. Click **Upgrade** to continue or **Previous** to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.
8. Review the pre-install summary and then click **Install**.

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

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

Field	Notes
Non-root user name	If this user does not already exist on the system, you are prompted to supply one.
HTTPS port	The port number to use when accessing the Logger UI. You can keep the default HTTPS port (443/tcp) or enter any other port that suits your needs. If you specify any port except 443/tcp, users will need to enter that port number in the URL they use to access the Logger UI.
Configure Logger as a service	Indicate whether to configure Logger to run as a service. Select this option to create a service called `arcsight_logger`, and enable it to run at levels 2, 3, 4, and 5. If you do not enable Logger to start as service during the installation process, you can still do so later. For instructions on how to enable Logger to start as a service after installation, see "Using Software Logger Command Line Options" on page 39.



10. Select the locale of this installation and click **Next**.
11. Specify the path and file name of the license file and click **Next**.

Note: If you do not provide a license file, Logger installs a 90-day trial license that has significant restrictions. See "Trial Licenses" on page 10.

The initialization screen is displayed.

12. Click **Next** again to Initialize Logger components. Initialization may take a few minutes. Please wait. Once initialization is complete, the configuration screen is displayed.
13. Click **Next** to allow Logger to configure storage groups and storage volume. Configuration may take a few minutes. Please wait.

    Once configuration is complete, Logger starts and the Configuration is Complete window displays the Logger user interface URL.
14. Make a note of the URL and then click **Done** to exit the installer.

Now that you are done installing and initializing your Logger, you can use the URL you noted during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on page 38.

Using Console Mode to Install Software Logger

Make sure the machine on which you will be installing Logger complies with the specifications listed the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 26 are met.

Before you install, you must increase the user process limit on the OS, as described in "Increasing the User Process Limit and the Maximum Number of Open Files" on page 28, and for RHEL 7.X only, modify the `logind.conf` file, as described in "Editing the logind Configuration File for RHEL 7.X" on page 29.

You can verify that you have the correct installation file, as described in "Verifying the Downloaded Installation Software" on page 24.

You can install Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 26 for details and restrictions.

To install the Logger software:

1. Run these commands from the directory where you copied the Logger installation file:

   ```
   chmod u+x ArcSight-logger-6.5.XXXX.0.bin
   ./ArcSight-logger-6.5.XXXX.0.bin -i console
   ```
2. The installation wizard launches in command-line mode. Press **Enter** to continue.

   ```
   ===============================================================================

   Introduction
   ------------

   InstallAnywhere will guide you through the installation of ArcSight Logger
   6.5.

   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. Press **Enter** to display each part of the license agreement, until you reach the following prompt:

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

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

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

5. The installer checks that installation prerequisites are met:
   - Operating system check—The installer checks to see if your device is running a supported operating system. If you are not, a message displays, but it does not prevent you from installing Logger software. This happens because some update scenarios start with an earlier OS.

     Note: HPE ArcSight strongly recommends that you upgrade to a supported OS before installing. Refer to the ArcSight Data Platform Support Matrix for a list of supported operating system platforms.

   - Installation prerequisite check—If a check fails, Logger displays a message. You will need to fix the issue before proceeding.

   Example

   If Logger is running on this machine, an Intervention Required message displays:

```
================================================================================

Intervention Required

---------------------

ArcSight Logger processes are active.

All ArcSight Logger processes must be stopped to allow installation to
proceed.

Type 'Quit' to exit this installer or 'Continue' to stop all ArcSight
Logger processes and continue with the installation.

->1- Continue

  2- Quit

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
```

   In this case, you would enter 1 (or hit **Enter**) to stop Logger processes, or 2 to quit the installer.

Once all checks complete, the installation continues, and the Choose Install Folder screen is displayed.

6. From the Choose Install Folder screen, type the installation path for Logger and then press **Enter**.

   The default installation path is `/opt`. You can install into this location or another location of your choice.

7. Type Y and press **Enter** to confirm the installation location.
   - If there is not enough space to install the software at the location you specified, a message is displayed. To proceed with the installation, specify a different location or make sufficient space available at the location you specified. Type `quit` and press **Enter** to exit the installer.
   - If Logger is already installed at the location you specify, a message is displayed. Enter 2 to continue with the upgrade and 1 to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

8. 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.

9. If you are logged in as root, the following prompts are displayed. Type your response and press **Enter** after each.

Field	Notes
User Name	If this user does not already exist on the system, you are prompted to supply one. **Tip:** When installing Logger on VMWare VM, use the non-root user `arcsight` that comes preconfigured on your system.
HTTPS Port	The port number to use when accessing the Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the Logger UI.
Choose if you want to run Logger as a system service.	Type 1 and press Enter to configure Logger as a service, or type 2 and press Enter to configure Logger as standalone. Select this option to create a service called `arcsight_logger`, 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 after installation, refer to the Logger Administrator's Guide.

10. Type the number for your desired locale, and press **Enter:**
    - 1 for English
    - 2 for Japanese
    - 3 for Simplified Chinese
    - 4 for Traditional Chinese

11. Type the absolute the path to the license file and click **Next**.

    Note: If you do not provide a license file, Logger installs a 90-day trial license that has significant restrictions. See "Acquiring a License for the Logger Appliance" on page 18.

    The initialization screen is displayed.

12. Press **Enter** again to initialize Logger components.

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

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

    Configuration may take a few minutes. Please wait.

    Once configuration is complete, Logger starts up and the next screen is displays the URL you should use to connect to Logger.

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

Now that you are finished installing and initializing your Logger, you can use the URL you noted during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" on page 38.

Using Silent Mode to Install Software Logger

Before you install Software Logger in silent mode, you need to create the properties file required for the silent mode installation. Once you have generated the file, you can use it for silent mode installations.

Licenses for Silent Mode Installations

As for any Logger installation, each silent mode installation requires a unique license file. You must obtain licenses as described in "Acquiring a License for Software Logger" on page 26 and place them on the machines on which you will be installing Logger in silent mode, or ensure that the location where the licenses are placed is accessible from those machines.

Generating the Silent Install Properties File

To generate a properties file for future silent installations:

1. Log in to the machine on which you can install Software Logger to generate an installation properties file.

   If you want the silent mode installations to be done as root user, log in as `root`. Otherwise, log in as a non-root user.

2. Run these commands:

   ```
   chmod u+x ArcSight-logger-6.5.0.XXXX.0.bin
   ./ArcSight-logger-6.5.XXXX.0.bin -r <path_for_generated_file>
   ```

where <path_for_generated_file> is the location of the directory where the generated properties file should be placed. The generated properties file is called `installer.properties`. You cannot specify or change this name.

3. Install Logger in GUI mode. See "Using GUI Mode to Install Software Logger" on page 29.
4. Once the installation completes, navigate to the directory location you specified for the `installer.properties` file earlier. Then go to "Installing Software Logger in Silent Mode" below.

   The following is an example of a generated `installer.properties` file.

```
# Wed Aug 14 18:27:49 PDT 2016
# Replay feature output
# --------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=/opt/Logger

#License Information
#-------------------
LICENSE_LOCATION=/home/user/arcsight.lic
```

Installing Software Logger in Silent Mode

Make sure the machine on which you will be installing the Software Logger complies with the platform requirements listed in the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 26 are met.

If you are installing as `root`, make sure that non-root user account that you entered when generating the silent mode properties file exists on the machines on which you are using the silent installer to install Logger.

To install the Software Logger using the Silent mode:

1. Copy the silent mode properties file you generated previously to the same location where you have copied the Logger software on the new system.
2. Edit the `LICENSE_LOCATION` property in the silent mode properties file to include the location of license file for this instance of installation. (A unique license file is required for each instance of installation.)

   Or

   Set the `LICENSE_LOCATION` property to point to a file, such as `logger_license.zip`. Then, for each instance of the silent mode installation, copy the relevant license file to the location and

rename it to `logger_license.zip`. Doing so will avoid the need to update the combined properties file for each installation.

3. Run these commands from the directory where you copied the Logger software:

```
chmod u+x ArcSight-logger-6.5.XXXX.0.bin
./ArcSight-logger-6.5.XXXX.0.bin -i SILENT -f <path to
installer.properties>
```

The rest of the installation and configuration proceed silently, without requiring any input from you.

After the installation and initialization completes, you can use the URL created during the installation to connect to Logger. For instructions and information, see "Connecting to Software Logger" below.

Connecting to Software Logger

The Logger user interface (UI) is a password-protected web browser application that uses an encrypted HTTPS connection. Refer to the ADP Support Matrix document available on the Protect 724 site for details on Logger 6.5 browser support.

Logger's publicly-accessible ports must be allowed through any firewall rules. For Software Logger, you are responsible for setting up the firewall. Firewall rules are preconfigured on the Logger Appliance. See "Firewall Rules" on page 13 for more information.

- For root installs, allow access to port `443/tcp` as well as the ports for any protocol that the logger receivers need, such as port `514/udp` for the UDP receiver and port `515/tcp` for the TCP receiver.
- For non-root installs, allow access to port `9000/tcp` as well as the ports for any protocol that the Logger receivers need, such as port `8514/udp` for the UDP receiver and port `8515/tcp` for the TCP receiver.

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

JavaScript and cookies must be enabled.

To connect to Logger:

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

For Software Logger: `https://<hostname or IP address>:<configured_port>`

For Logger Appliance: `https://<hostname or IP address>`

where the hostname or IP address is that of the system on which the Logger software is installed, and configured_port is the port set up during the Logger installation, if applicable.

After you connect, the Login screen is displayed.

To log in:

When the Login dialog is displayed, enter your user name and password, and click **Login**.

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

Username: admin
Password: password

Note: After logging in for the first time with the default user name and password, you will be prompted to change the password. Follow the prompts to enter and verify the new password.

For more information about the Login screen and connecting to Logger, refer to the User Interface and Dashboards chapter of the Logger Administrator's Guide.

Once you have logged in successfully, you can enable the preconfigured receivers and configure devices, device groups, and storage groups necessary to implement your retention policy. See "Configuring Logger" on page 43 and refer to the Configuration chapter of the Logger Administrator's Guide for information on how to set up your Logger to start receiving events.

Using Software Logger Command Line Options

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.

Note: If your Logger is installed to run as a system service, you can use your operating system's `service` command to start, stop, or check the status of a process on Logger.

```
<install_dir>/current/arcsight/logger/bin/loggerd
{start|stop|restart|status|quit}<install_dir>
```

```
/current/arcsight/logger/bin/loggerd {start <process_name> | stop <process_
name> | restart <process_name>}
```

To view the processes that can be started, stopped, or restarted with `loggerd`, click **System Admin** from the top-level menu bar. Then, under **System**, pick **Process Status**. The processes are listed on the right under **Processes.**

The following table describes the subcommands available with `loggerd` and their purpose.

Command	Purpose
`loggerd start`	Start all processes listed under the System and Process sections in the figure above. Use this command to launch Logger.
`loggerd stop`	Stop processes listed under the Process section only. Use this command when you want to leave `loggerd` running but all other processes stopped.

`loggerd restart`	This command restarts processes listed under the Process section only.
	Note: When the `loggerd restart` command is used to restart Logger, the status message for the "aps" process displays this message:
	`Process 'aps' Execution failed`
	After a few seconds, the message changes to:
	`Process 'aps' running`

`loggerd status`	Display the status of all processes.
`loggerd quit`	Stops all processes listed under the System and Process sections in the figure above. Use this command to stop Logger.
`loggerd start <process_name>`	Start the named process. For example, `loggerd start apache`.
`loggerd stop <process_name>`	Stop the named process. For example, `loggerd stop apache`.
`loggerd restart <process_name>`	Restart the named process. For example, `loggerd restart apache`

You can also start and stop and view the status of Logger processes from the **System Admin > System > Process Status** page. Refer to the Logger Administrator's guide or online help for more information.

Uninstalling Logger

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

Before uninstalling Logger, stop the Logger processes by using the `loggerd stop` command, as described in "Connecting to Software Logger" on page 38.

To uninstall the Logger software:

1. Enter this command in the installation directory:

   ```
   ./UninstallerData/Uninstall_ArcSight_Logger_6.5
   ```

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

Chapter 4: Installing Software Logger on VMware

Logger 6.5 virtual machine (VM) is not available as a fresh installation.

To install Logger 6.5, first deploy Logger 6.4 virtual machine (VM) (see Logger's Installation and Configuration Guide 6.4) and upgrade to Logger 6.5 by following the instructions in Logger 6.5 Release Notes.

For information on how to install Software Logger on Linux, see Installing Software Logger on Linux. For initialization information about the Logger Appliance, see "Setting Up a Logger Appliance" on page 15.

Chapter 5: Configuring Logger

This chapter includes basic deployment and configuration information on the following topics. It is applicable to all Logger types. If you have installed multiple Loggers, you must connect to each and configure it separately or use ArcSight Management Center to make bulk configuration changes.

For more information on directly configuring and administering your Logger, refer to the Logger Administrator's Guide. For more information on configuring and administering your Logger using ArcMC, refer to the ArcSight Management Center Administrator's Guide. For more information on setting Connectors, refer to the documentation for each Connector.

Receiving Events and Logs

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

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

Receivers

Now that you have finished installing Logger, you can set up receivers to listen for events. 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. You can use the preconfigured receivers or add your own. Receivers can be disabled and re-enabled later. You can add, change, and delete them as needed.

The preconfigured receivers include a TCP receiver, a UDP Receiver, and a SmartMessage receiver already enabled and ready to receive events. Logger also comes preconfigured with folder follower receivers for Logger's Apache Access Error Log, the system Messages Log, and the system Messages Audit Log (if auditing is enabled on your Linux OS).

To receive data, a receiver's ports must be allowed through any firewall rules. See "Firewall Rules" on page 13 for more information. You must enable these receivers in order to use them. See "Enabling the Preconfigured Folder Follower Receivers" on the next page for instructions.

The preconfigured receivers are described more detail in "Receivers" on page 12. For further information on receivers, refer to the Configuration chapter of the Logger Administrator's Guide.

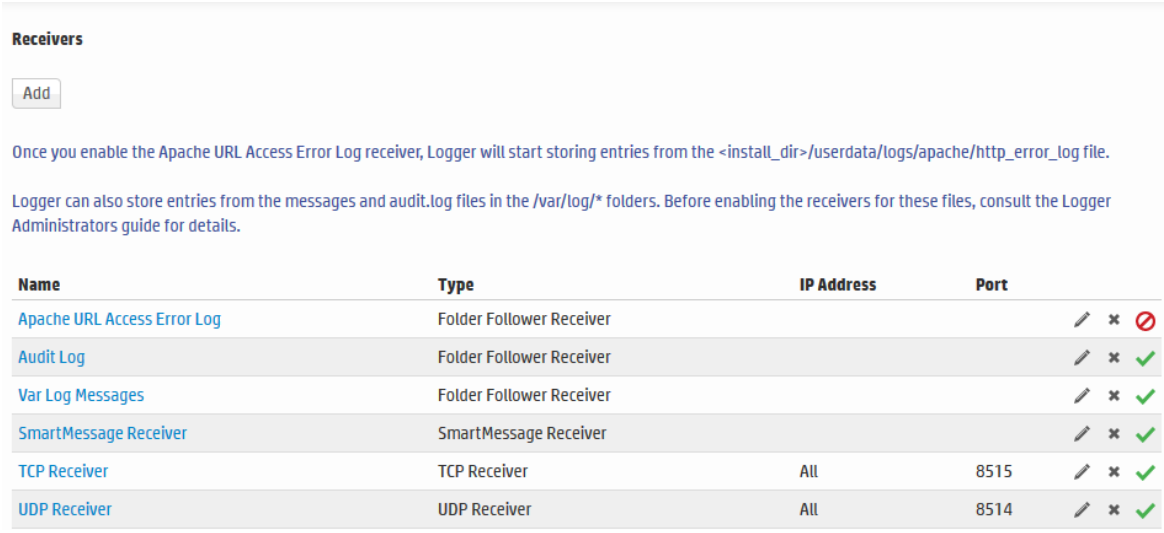
Logger can also receive events from ArcSight SmartConnectors that collect event data from sources on your network. To learn more about ArcSight SmartConnectors, visit https://www.hpe.com/us/en/solutions/security.html.

Enabling the Preconfigured Folder Follower Receivers

The preconfigured receivers are described more detail in "Receivers" on page 12. For further information on receivers, refer to the Configuration chapter of the Logger Administrator's Guide.

When you first log in by using the URL you configured, the preconfigured folder follower receivers are disabled. The Home page displays an Add Data button. Click **Add Data** (Add Data) to open the Receivers page and enable the receivers.

Tip: Before enabling these receivers, you must make `/var/log/audit/audit.log` and `/var/log/messages` readable by the non-root user you installed with or specified during Logger installation.



To enable a receiver, click the disabled icon ( ) at the end of the row.

Alternately, you can navigate to the Receivers page from the menu to enable the receivers.

To open the Receivers page from the menu and enable a receiver:

1. Open the **Configuration > Data** menu and click **Receivers**.
2. Identify the receiver you want to enable, and click the disabled icon ( ) at the end of that row.

For information on how to use the preconfigured SmartMessage receiver, see "Using SmartConnectors to Collect Events" on page 46.

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 Secure Copy Protocol (SCP), Secure file transfer protocol (SFTP), or File Transfer Protocol (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.

  Caution: The SCP and SFTP protocols on Logger appliances are not FIPS compliant.

  Note: The SCP, SFTP, and FTP file transfer receivers depend on the FTP, SCP, and SFTP clients installed on your system.

- **SmartMessage Receiver**: SmartMessage receivers listen for encrypted messages from ArcSight SmartConnectors. To start using the pre-installed receiver, you must configure a SmartConnector to send events to it. For instructions, see "Configuring a SmartConnector to Send Events to Logger" on the next page.

Sending Structured Data to Logger

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

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

For more information about the Common Event Format (CEF), refer to Implementing ArcSight CEF. For a downloadable a copy of this guide, search for “ArcSight Common Event Format (CEF) Guide” in the ArcSight Product Documentation Community on Protect 724.

Using SmartConnectors to Collect Events

Similar to ArcSight Manager, Logger leverages the ArcSight SmartConnectors to collect events. SmartConnectors can read security events from heterogeneous devices on a network (such as firewalls and servers) and filter events of interest (and optionally aggregate them) and send them to a Logger receiver. Logger can receive structured data in the form of normalized Common Event Format (CEF) events from the SmartConnectors.

This section gives basic information on each of these topics. For details, refer to the documentation for that Connector and the SmartConnector User's Guide, available for download from the ArcSight Product Documentation Community on Protect 724.

SmartMessage

SmartMessage is an HPE ArcSight technology that provides an efficient secure channel for Common Event Format (CEF) events between ArcSight SmartConnectors and Logger.

SmartMessage provides an end-to-end encrypted secure channel using Transport Layer Security (TLS). One end is an ArcSight SmartConnector, receiving events from the many devices supported by ArcSight SmartConnectors. The other end is a SmartMessage receiver on Logger.

Note: The SmartMessage secure channel uses TLS protocol to send encrypted events to Logger. This is similar to, but different from, the encrypted binary protocol used between SmartConnectors and ArcSight Manager.

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.

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

2. Specify the required parameters. Enter the Logger hostname or IP address and the name of the SmartMessage receiver. These settings must match the receiver in Logger that listen for events from this connector.
   - To use the preconfigured receiver, specify "SmartMessage Receiver" as the **Receiver Name**.
   - To use SmartMessage to communicate between an ArcSight SmartConnector and a Logger Appliance, configure the SmartConnector to use port 443/tcp.
   - To communicate between an ArcSight SmartConnector and Software Logger, configure the SmartConnector to use the port configured for the Software Logger.
   - For unencrypted CEF syslog, enter the Logger hostname or IP address, the desired port, and choose UDP or TCP output.

Configuring SmartConnectors to Send Events to Both Logger and an ArcSight Manager

You can configure a SmartConnector to send CEF syslog output to Logger and send events to an ArcSight Manager at the same time.

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 ArcSight Product Documentation Community on Protect 724.

1. Install the SmartConnector normally. Register the SmartConnector with a running ArcSight Manager and test that the SmartConnector is up and running.
2. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
3. Select **I want to add/remove/modify ArcSight Manager destinations**, then choose **Add new destination**.
4. Choose Logger and specify the requested parameters. Restart the SmartConnector for changes to take effect.

Configuring SmartConnectors for Failover Destinations

SmartConnectors can be configured to send events to a secondary failover destination when a primary connection fails.

To configure a failover destination, follow these steps:

1. Configure the SmartConnector for the primary Logger as described above. The transport must be raw TCP in order to detect the transmission errors that trigger failover.

2. Edit the `agent.properties` file in the directory `$ARCSIGHT_HOME/current/user/agent`, where `$ARCSIGHT_HOME` is the root directory where the SmartConnector component was installed.
   a. Add this property: `transport.types=http,file,cefsyslog`
   b. Delete this property: `transport.default.type`
3. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
4. Choose **I want to add/remove/modify** and, with the primary Logger selected, choose **Modify**. Then select **Add failover destination**.
5. Enter information for the secondary Logger.
6. Restart the SmartConnector for the changes to take effect.
7. For more information about installing and configuring ArcSight SmartConnectors, refer to the ArcSight SmartConnector User's Guide, or specific SmartConnector Configuration Guides, available from the ArcSight Product Documentation Community on Protect 724.

Downloading SmartConnectors

Contact your HPE ArcSight sales representative or customer support for the location to download the supported SmartConnectors. To learn more about ArcSight SmartConnectors, visit https://www.hpe.com/us/en/solutions/security.html.

Devices

Logger begins storing events when an enabled receiver receives data or, in the case of a file receivers, when the files become available. Using a process called autodiscovery, Logger automatically creates resources called devices to keep track of source IP addresses and uses DNS to map them to hostnames. Eventually, a device is created for each device from which Logger received events.

You can also create devices preemptively, by entering the IP addresses or hostnames of data sources that you expect to be sending events to Logger. You might do this if you do not want to wait for autodiscovery, or if you want to control the initial naming of each device. Discovered devices are named for their host, or if the DNS lookup fails, for their IP address, and their receiver. For information about creating devices, refer to the Configuration chapter of the Logger Administrator's Guide.

Device Groups

Device groups are containers or logical groupings for devices, in the same way folders (or directories) contain files. They are a name for a group of devices. A given device can be a member of several device groups. Each device group can be associated with particular storage group, which would assign a retention policy.

You can change and delete device groups freely as your needs change. Setting up device groups initially is not critical; incoming events that are not assigned to a device group are automatically sent to the Default Storage Group. For the details of setting up device groups, refer to the Configuration chapter of the Logger Administrator's Guide.

Storage Rules

Events are stored in the Default Storage Group unless otherwise specified. Storage rules are a way to direct events from certain device groups to certain storage groups. You can use them to implement additional retention policies.

If you created additional storage groups, and want to send events to them, you can do that with storage rules. If you choose not to create storage rules, events from all devices will be sent to the Default Storage Group and use its specified retention policy.

If you want to implement multiple retention policies, you can create storage rules that associate the specific device groups with the storage groups that implement the desired retention policy.

For example, you could create one device group for each retention policy. However, for more control, you could associate device groups with storage groups and storage rules and use them to categorize events. For example, you could search for events that match a certain pattern and which belong to a particular device group, and send them to a particular storage group for retention based on event category.

Storage rules are evaluated in order of priority; the first matching rule determines to which storage group an event is sent. This approach means that a single device can belong to several device groups without ambiguity about which storage group it will end up in.

Refer to the Configuration chapter of the Logger Administrator's Guide for more information on storage rules.

Sending Events from ArcSight ESM to Logger

The ArcSight Forwarding SmartConnector can read events from an ArcSight Manager and forward them to Logger as CEF-formatted syslog messages.

Note: The Forwarding SmartConnector is a separate installable file, named similar to these:

`ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.exe`

`ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.bin`

Use build 4810 or later for compatibility with Logger.

To configure the ArcSight Forwarding SmartConnector to send events to Logger:

1. Install the SmartConnector component normally, but cancel the installation when the SmartConnector Wizard asks whether the target Manager uses a demo certificate.

   When the first screen of the SmartConnector Configuration Wizard appears, asking about a demo certificate, click **Cancel**.
2. Confirm that you want to exit, then click **Done** to dismiss the Install Wizard. This will install the SmartConnector, but leave it un-configured.
3. Create a file called **agent.properties** in the directory `$ARCSIGHT_HOME/current/user/agent`, where `$ARCSIGHT_HOME` is the root directory where the SmartConnector component was installed. This file should contain a single line:

   ```
   transport.default.type=cefsyslog
   ```
4. Start the SmartConnector configuration program again using the `$ARCSIGHT_HOME/current/bin/runagentsetup` script (or `arcsight agentsetup -w`).
5. Specify the required parameters for CEF output. Enter the desired port for UDP or TCP output. These settings will need to match the receiver you create in Logger to listen for events from ArcSight ESM.

Parameter	Description
IP/Host	IP or host name of the Logger
Port	514 or another port that matches the receiver
Protocol	UDP or Raw TCP
ArcSight Source Manager Host Name	IP or host name of the source ArcSight Manager
ArcSight Source Manager Port	8443 (default)
ArcSight Source Manager User Name	A user account on the source Manager with sufficient privileges to read events
ArcSight Source Manager Password	Password for the specified Manager user account
SmartConnector Name	A name for the ESM to Logger connector (visible in the Manager)
SmartConnector Location	Notation of where this connector is installed
Device Location	Notation of where the source Manager is installed
Comment	Optional comments

To configure the Forwarding SmartConnector to send CEF output to Logger and send events to another ArcSight Manager at the same time, see "Configuring SmartConnectors to Send Events to Both Logger and an ArcSight Manager" on page 47.

For more information about the Common Event Format (CEF), refer to Implementing ArcSight CEF. For a downloadable copy of this guide, search for “ArcSight Common Event Format (CEF) Guide” in the ArcSight Product Documentation Community on Protect 724.

Chapter 6: Alerts

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

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

Types of Alerts

Logger provides two types of alerts:

- Real time alerts
- Saved Search Alerts

The following table compares the two types of alerts.

Real Time Alerts	**Saved Search Alerts**
No limit on the number of alerts that can be defined. A maximum of 25 alerts can be enabled at any time.	Any number of alerts can be defined. All defined alerts are enabled and effective; however, a maximum of 50 alerts can run concurrently.
No limit on the number of configured e-mail destinations; however, you can only set one SNMP, one Syslog, 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.
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**.
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.
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.	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

Real Time Alerts	Saved Search Alerts
	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: `5/11/2016 10:38:04` End Time: `5/12/2016 10:38:04` And, the number of matches and threshold are the following: Match Count: 5 Threshold: `3600` An alert will trigger if five or more events occur in one hour anytime between May 11th, 2016 10:38:04 a.m. and May 12th, 2016 10:38:04 a.m.

Configuring Alerts

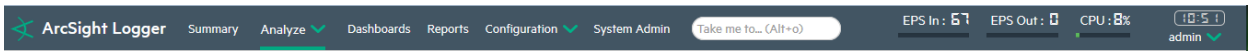
Refer to the ArcSight Logger Administrator's Guide for detailed instructions on how to create both types of alerts.

Chapter 7: 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

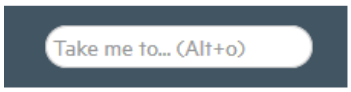
A navigation and information band runs across the top of every page in the user interface. It contains menu tabs, a quick navigation field, events gauges, system clock, and a menu including Options, Help, About, and Logout.

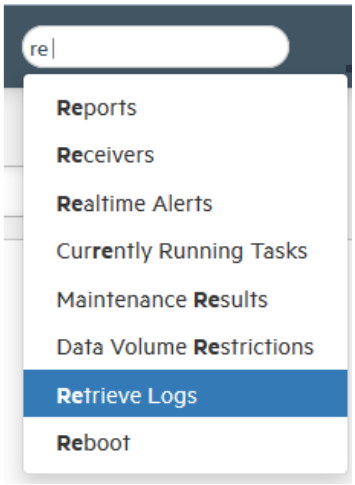


Bar gauges at the top of the screen provide an indication of the throughput and CPU usage information available in more detail on the Monitor Dashboard ("Dashboards" on page 56). You can change the range of the bar gauges on the Options page. The name of the logged-in user is shown below the clock, to the right of the gauges.

Take Me To

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





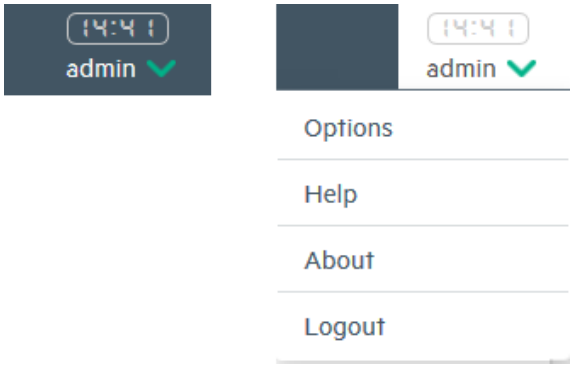
You can access the Take me to... navigation box by clicking in it or by using the Alt+o, Alt+p, or Ctrl+Shift +o hot keys. As you type, a list of features that match drops down. Click an item in the list or press enter to go to the specified feature.

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

Server Clock, Current User, and Options Dropdown

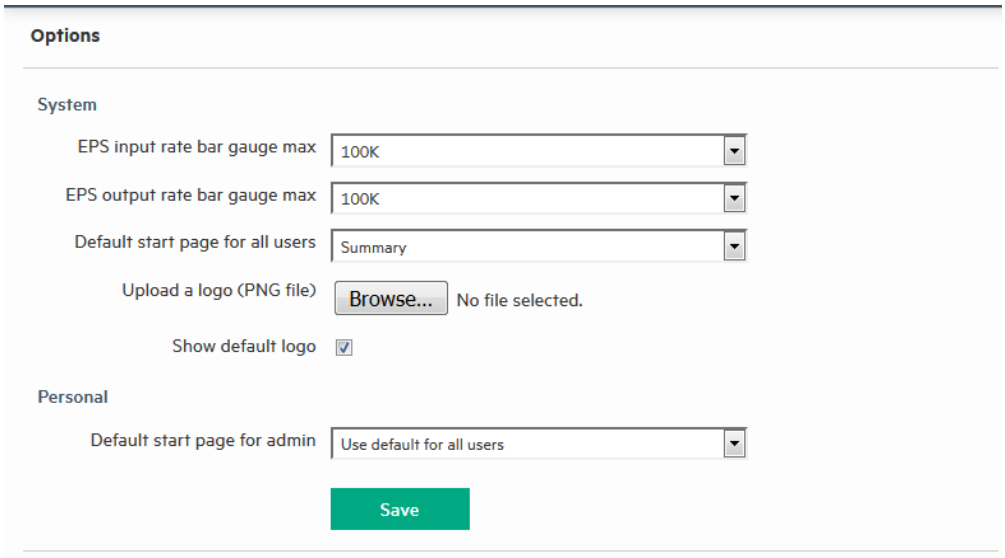
The server clock is shown to the right of the bar gauges, along with the currently logged-in user's name and the options dropdown.

The server clock displays the Logger server's system time. This may be different from the user's local time. Click the down-arrow by the user name to access the Options, Help, About, and Logout links.



The Options Page

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



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

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

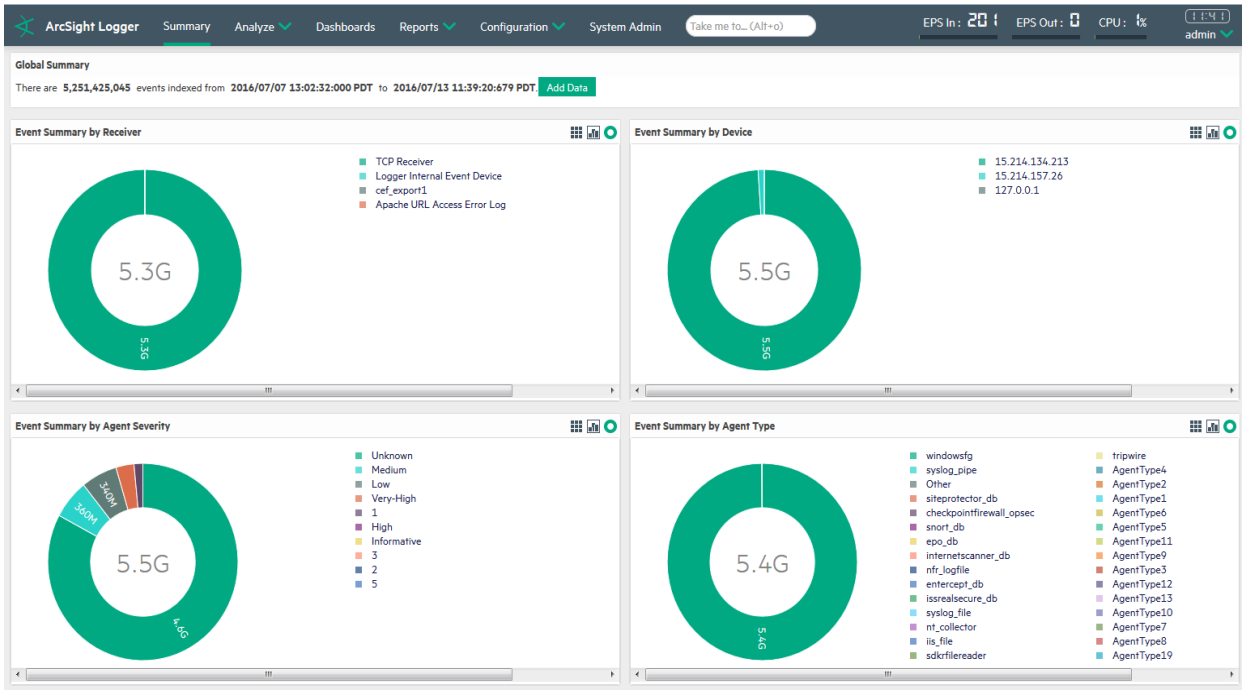
Logout

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

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

Summary

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



Dashboards

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

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

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

Chapter 8: Searching for Events

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

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

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

Example Queries

Simple query examples:

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

Complex query example:

```
_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 types of expressions:

Query Element	Description

Keyword expression	A keyword: a word expressed in plain text; for example:
	`warning`
	`failed`
	`login`

Query Element	Description

Field-based expression	A field-based expression: searching for values in the fields of an event. This includes searches for uncommon values in specific fields; for example:
	`name="failed login"`
	`message!="failed login"`
	`sourceAddress=192.0.2.0`

Search operator expression	A search operator expression: an expression that uses search operators to refine the data that matches the expressions specified by the keyword and the field-based expression. The following search operators are available in Logger 6.5: `cef, chart, dedup, eval, extract, fields, head, keys, rare, regex, rename, replace, rex, sort, tail, top, transaction, where`

Extraction operator expression	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.
	For 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; for example:.
	To display search results of the count of unique values device addresses in a chart form:
	`failed | chart _count by deviceAddress`
	To display search results of the most common values for the `deviceAddress` field in table form. That is, the values are listed in order from the highest number of matches to the lowest.
	`failed | top deviceAddress`

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

Building a Query

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

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

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

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

Run a Query

To run a query:

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

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

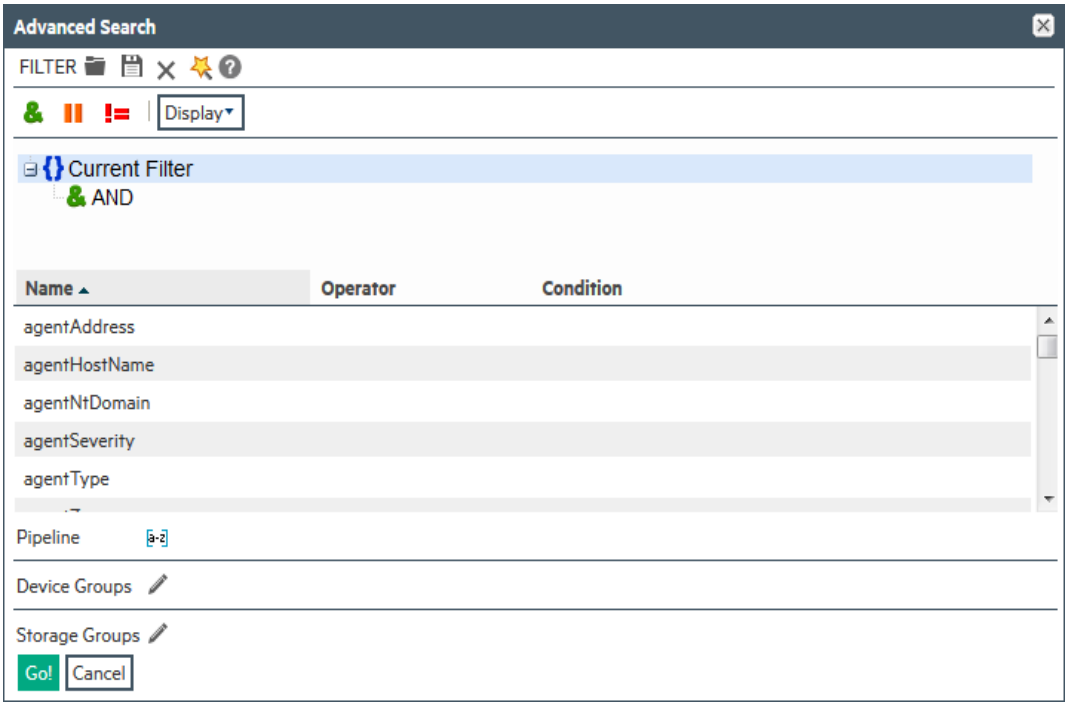
Query Building Tools

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

- Search Builder

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

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



- Regex Helper

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

- Search Helper

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

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

Exporting Search Results

You can export search results in these formats:

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

To export search results:

1. Run a search query.
2. Click **Export Results**. ()

Saving Queries for Later Use

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

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

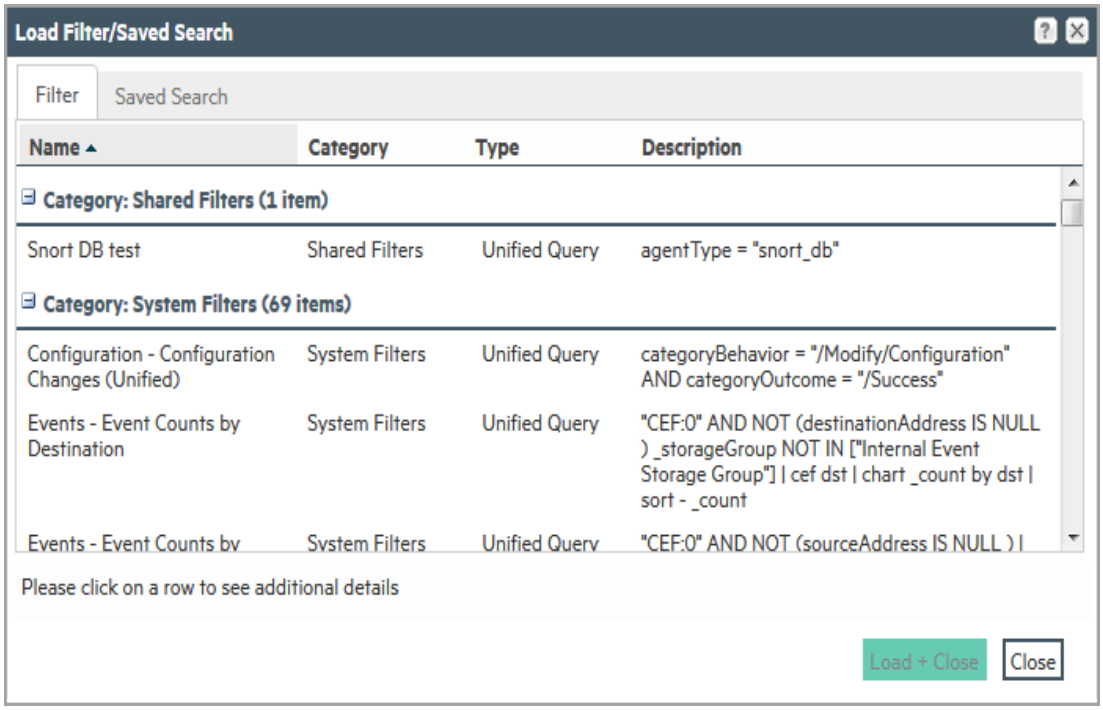
  For more information about saving queries and using them again, refer to the ArcSight Logger Administrator's Guide.

System Filters (Predefined Filters)

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

To use a system filter:

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



3. Click **Load+Close**.

Tuning Search Performance

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

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

- Take advantage of super indexes where possible, for the fastest search results. Refer to the ArcSight Logger Administrator's Guide for more information on how to search super-indexed fields.
- The amount of time it takes to search depends on the size of the data set that must be searched, the complexity of the query, and whether the search is distributed across peers. To limit the data set, ensure that time range you specify does not result in a query that needs to scan multimillions of events.
- Limiting search to specific storage groups or peers typically results in better search performance than when the storage groups or peers are not specified.
- Reduce the load on the system when your query needs to run, for example, scheduled jobs, running multiple reports, or large number of incoming events.

Tip: 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, HPE strongly recommends that you index fields that you will be using in search and report queries. Refer to the ArcSightLogger Administrator's Guide for more information on indexing fields.

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.

Tip: To form a `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>[^ ]*)" | 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>[^ ]*)" | chart _
  count by CustomUser
  ```

Other Logger Features

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

Scheduling Tasks

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

Archiving Events

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

Access Control on Logger Users

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

Enriching Data Through Static Correlation

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

Web Services

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

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation and Configuration Guide (Logger 6.5)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!