



Hewlett Packard
Enterprise

HPE ArcSight Logger

Software Version: 6.2

Data Migration Guide

February 22, 2016

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 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

© Copyright 2016 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Support

Contact Information

Phone	A list of phone numbers is available on the HPE ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Data Migration Between Loggers	4
Summary	4
The Data Migration Process	5
Supported Migration Paths	6
Prerequisites for Migration	7
Migrating Data Between Loggers	9
What is Migrated from a Logger Appliance	9
Migrating Data—Step-by-Step Instructions	10
Migrating Event Archive Settings Separately	20
Migrating the Event Archive Settings—Step-by-Step Instructions	20
After the Migration	29
Troubleshooting	30
Send Documentation Feedback	31

Data Migration Between Loggers

This document explains how to migrate data and event archive settings between supported HPE Security ArcSight Loggers. The information in this guide applies to ArcSight Logger 6.2 (6.2 xxxx) and the Logger Data Migration Utility 6.2 (DM6.2-D1090).

Summary

Data migration between Loggers may occasionally be required for situations like these:

- You want to move data to a Logger with higher storage capacity.
- You want to move data from an old Logger model to a current model.
- You want to move data from a Logger Appliance to a Software Logger.

Event data on an Logger Appliance can be migrated to the following devices:

- Another Logger Appliance of equal or higher capacity.
- A Software Logger installed on a supported operating system.

This capability applies to both storage-area network (SAN) and non-SAN Loggers.

Note: Migrating from a Software Logger to another Logger of any type is not supported. For a list of supported migration paths, see ["Migrating Data Between Loggers" on page 9](#).

The Data Migration Process

HPE Security ArcSight offers a data migration utility for migrating data between two Loggers. The utility consists of two scripts, one for the source Logger and the other one for the target Logger. The scripts need to be run in parallel on the source and target Loggers, as described in ["Migrating Data—Step-by-Step Instructions" on page 10](#).

Both the source and the target Logger must be up and running for data migration to work. You cannot use the data migration process to migrate data from a non-functional, down Logger, or for migrating data from Logger's local storage to NFS storage.

The utility copies data from the source to the target Logger. Therefore, data on the source Logger is preserved after a successful migration. The target Logger should not have any data on it before migration.

The existing configuration and event data on a target Logger is overwritten by this utility. If there is any existing data on a target Logger appliance, HPE Security ArcSight recommends that you restore the appliance to its original factory settings before beginning the migration.

The data migration stops all Logger processes except for the Logger and the PostgreSQL servers. Therefore, neither Logger can receive events during this phase; however, SSH access to both Loggers is still available.

Scheduled tasks on the source Logger do not run either, but the tasks resume as scheduled on the source after the migration is complete. (Scheduled task information is not migrated over to the target Logger, as described in ["Migrating Data Between Loggers" on page 9](#). Therefore, scheduled tasks will not run on the target Logger until explicitly configured after the migration.)

Supported Migration Paths

You can migrate data between Loggers over a high-speed local area network (LAN) connection that can provide at least 1 Gbps dedicated network bandwidth. Network speed and traffic will affect data migration speed. HPE Security ArcSight **does not** recommend using a wide area network (WAN) link for the migration. ArcSight strongly recommends using a cross-over cable between Logger Appliances to eliminate network latency delays.

Migration times vary and may take from 5 to 18 hours or more. The time required to migrate data depends on the connectivity between the two Loggers, the amount of data migrated, the event data size, the form factors between which the migration takes place, and the options chosen during migration.

The paths in the table below are supported for data migration between two Loggers.

Note: Data migration tools and services for older versions of Logger may be available through Professional Services engagement.

Migration Path	Source / From	Version	Target / To	Version
Appliance to Appliance	Lx400	6.1	L7600	6.2
	Lx500	6.2	L7600	6.2
Appliance to Software	Lx400	6.1	Software Logger	6.2
	Lx500	6.2	Software Logger	6.2
SAN Appliance to Non-SAN Appliance	L7400-SAN	6.1	L7600	6.2
	L7500-SAN	6.2	L7600	6.2
SAN Appliance to Software	L7400-SAN	6.1	Software Logger	6.2
	L7500-SAN	6.2	Software Logger	6.2

Prerequisites for Migration

Ensure that the following prerequisites are met before beginning the data migration process.

Area	Prerequisite
Target Logger	<ul style="list-style-type: none">• Must be of equal or higher capacity than the source Logger.• Must be either a brand-new Logger with only the configuration described in this section or, for Logger Appliances, an existing Logger that has been restored to its original factory settings. For details about restoring a Logger to its factory settings, see the <i>Logger Administrator's Guide</i>.• The storage volume on the target Logger must be at least as large as the storage volume of the Source Logger. After installing the target Logger software and before migrating the data, ensure that the storage volume is at least as large as that on the source Logger.• If the target Logger is a Software Logger, the non-root user's UID and GID must be 1500 and 750, respectively, to match the UID and GID of the same user on the source Logger.• If the target Logger is a Software Logger, it must have been installed as user "root".
Logger Version	<p>Both Loggers must be running a supported Logger version for migration:</p> <ul style="list-style-type: none">• The source Logger must be running Logger version 6.1 or 6.2.• The target Logger must be running Logger version 6.2. <p>Note: Upgrade your appliance to the appropriate version before the migration.</p>
Time settings	Time settings (timestamp and time zone) must be identical on both Loggers.
Storage Groups	<p>The target Logger can be configured with either the default storage groups or any additional ones.</p> <p>Caution:</p> <ul style="list-style-type: none">• The target Logger's storage group configuration is overwritten with the source Logger's information. Therefore, after the migration, only the storage groups that existed on the source Logger will be available on the target.• A 100% pre-allocation of space is performed automatically on the

Area	Prerequisite
	<p>storage volume on the target Logger during the data migration process. If any pre-allocated space exists on the target, it is overwritten.</p>
NFS/CIFS Mount Name	<p>The remote mount points on the source and target Loggers must match. That is, the same number of mounts, with the same name, hostname, and path for each mount must exist on the source and target Loggers.</p> <p>When setting the mount point on Logger Appliance targets, use Logger's System Admin interface. For Software Logger targets, set the mount points manually as appropriate for your operating system.</p> <p>Caution: If the mount point is not set up on the target Logger before data migration begins, the process will fail.</p>
Event Archive	<p>If an event archive is loaded on the source Logger, make sure it is unloaded before you begin the data migration process.</p>
Archive Settings	<p>If you archive events to an NFS or CIFS server, make sure the mount point is configured on the target Logger, and the server is up and reachable from the target Logger.</p> <p>When setting the mount point on Logger Appliance targets, use Logger's System Admin interface. For Software Logger targets, set the mount points manually as appropriate for your operating system.</p>

Migrating Data Between Loggers

If the source is a Logger Appliance (SAN or non-SAN), you can migrate event data in live storage, archived event data, and some Logger configuration data to another Logger of a supported type.

What is Migrated from a Logger Appliance

The following table lists all the event and configuration data that can be migrated from a Logger appliance using the Data Migration script. For examples of data types that are not migrated, see ["Data That is Not Migrated from Logger Appliance" on the next page](#).

Data Migrated from Logger Appliance

- Custom schema fields
- Devices
- Event archive settings (archive configuration metadata and mappings)

Caution: If you skip archive migration during the data migration process, your archive configuration metadata and mappings will not be migrated. After the migration, you will not be able to access any of your archives until you migrate your archives. See ["Migrating Event Archive Settings Separately" on page 20](#) for more information.

- Event data and its metadata
- Global summary data (**Summary** menu option)

Note: Global Summary Persistence was disabled in Logger 5.3 SP1, however, any existing global summary data will still be migrated.

- Indexing information
- Lookup files

Note: A known issue with data migration prevents lookup files from being properly migrated if the path to the data migration file on the target Logger is different from the one on the source Logger. See ["Migrating Event Archive Settings Separately" on page 20](#) for how to handle data that is not migrated.

- Parser definitions
- Receivers
- Retention information
- Source type information

- Storage groups
- Superindexing information

Data That is Not Migrated from Logger Appliance

- Alerts
- All scheduled jobs
- Archived events
- Configuration backup settings
- Dashboards
- Device groups
- ESM destinations
- Filters, including system filters, user-defined filters, and PCI/SOX package filters
- Forwarders
- Peer configuration
- Reports (including published reports)
- Saved searches
- Storage rules

Caution: Do not use the configuration backup and restore feature in an attempt to move data that is not migrated to the target Logger. See ["Migrating Event Archive Settings Separately" on page 20](#) for how to handle data that is not migrated.

Migrating Data—Step-by-Step Instructions

Perform these steps to migrate data from one Logger to another.

Note: Be sure to start the **target** Logger script before the **source** Logger script, as described in [Step 13 on page 13](#) and [Step 16 on page 13](#); otherwise, the data migration process will not proceed as expected.

If data migration fails at any point, refer to ["Troubleshooting" on page 30](#).

	On the Source Logger...	On the Target Logger...
1	Make sure that the source and target Loggers meet the requirements listed in "Prerequisites for Migration" on page 7 before proceeding further.	
2	Reboot the Source Logger.	

	On the Source Logger...	On the Target Logger...
3	<p>Copy datamigration-6.2-D1092.tar.gz to: /opt/arcsight/logger.</p> <p>This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.</p>	<p>Copy datamigration-6.2-D1092.tar.gz to the following directory:</p> <p>On Logger Appliances: /opt/arcsight/logger</p> <p>On Software Loggers, use the directory path where Logger was installed. The default is: /opt/current/arcsight/logger</p> <p>This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.</p>
4	SSH to the Logger and log in as user “root.”	SSH to the Logger and log in as user “root.”
5	<p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre>	<p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME=<LoggerInstallDirectory>/current/arcsight/logger</pre> <p>By default this is: /opt/current/arcsight/logger</p>
6	<p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre>	<p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre>
7	<p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre>	<p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre>
8	<p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationSource</pre>	<p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationTarget</pre>

	On the Source Logger...	On the Target Logger...
	<code>_rsh_setup.sh</code>	<code>_rsh_setup.sh</code>
9		<p>The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location.</p> <p>If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory.</p> <p>After you enter the directory, the script prompts you to confirm the location you entered. Enter 'y' to confirm or 'n' to re-enter the location.</p>
10		You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not.
11		<p>Edit the <code>/etc/hosts.deny</code> file to add the following information:</p> <pre>in.rlogind: all in.rshd: all</pre> <p>Edit the <code>/etc/hosts.allow</code> file to add the following:</p> <pre>all: <sourceLoggerIPAddress></pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p> <div> <p>Note: When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached.</p> </div>
12		<p>Edit the <code>/etc/hosts.equiv</code> and <code>/root/.rhosts</code> files to add the following information:</p> <pre><sourceLoggerIPAddress> root</pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p>

	On the Source Logger...	On the Target Logger...
		<p>Note: When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached.</p>
13		<p>Enter this command to run the Data Migration utility:</p> <pre>bin/scripts/dataMigrationTarget.sh</pre> <p>Tip: Press Ctrl+C to exit the script at any time.</p>
14		<p>On software Logger, you may be asked if the non-root user is “arcsight.” If so, enter ‘y’. If not, enter the non-root user name used when installing Logger.</p> <p>After you enter the user name, the script prompts you to confirm it. Enter ‘y’ to confirm or ‘n’ to re-enter the user name.</p>
15		<p>A message telling you to run the data migration script on the source Logger is displayed.</p>
16	<p>Enter one of the following commands to run the Data Migration utility:</p> <pre>bin/scripts/dataMigrationSource.sh</pre> <pre>bin/scripts/dataMigrationSource.sh -force_checksum</pre> <p>Tip: Using the -force_checksum option can take significantly longer to migrate data. However, this command provides an additional check to ensure that each file has been reliably copied</p>	

	On the Source Logger...	On the Target Logger...
	from the source to the target Logger.	
17	<p>The utility prompts you to confirm the ARCSIGHT_HOME location. Enter 'y' to confirm or 'n' to re-enter the location.</p> <p>The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>Tip: Press Ctrl+C to exit the script at any time.</p>	
18	<p>The utility prompts you to enter the IP address of the target Logger.</p> <p>After you enter the IP address, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the IP address.</p>	
19	<p>The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'n', the utility prompts you to enter the ARCSIGHT_HOME of the target machine. (The utility assumes the ARCSIGHT_HOME for Logger Appliances.)</p> <p>After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.</p>	
20	<p>The utility prompts you to consider how you want to handle archive migration:</p> <ol style="list-style-type: none"> 1. Default archive migration: The data migration script fails and exits if the archive check fails. If the scripts exits because the archive check failed, restore the missing archives and run the script again. 2. Ignore archive check: Data migration continues even if the archive check fails. Event archive settings (Archive 	

	On the Source Logger...	On the Target Logger...
	<p>configuration metadata and mappings) are migrated and any missing archives will be accessible if you restore them to their original location.</p> <p>3. Skip archive migration: No archive configuration metadata is migrated. You will not be able to access any of your archives until after you run the Archive Migration Utility. See "Migrating Event Archive Settings Separately" on page 20 for more information.</p> <p>The utility then asks if you would like to migrate your archives only after the archive check passes. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'y', proceed to Step 21 on the next page.</p> <p>If you entered 'n', the utility asks you if you would like to migrate the archive configuration metadata even if some archives are missing. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'y', proceed to Step 21 on the next page.</p> <p>If you entered 'n', the utility asks you if you are sure you want to skip archive migration?</p> <div data-bbox="316 1451 841 1635"> <p>Caution: If you confirm this option, you will NOT be able to access ANY of your archives after the migration until after you run the Archive Migration Utility.</p> </div> <p>See "Migrating Event Archive Settings Separately" on page 20 for more information.</p> <p>If you entered 'n', the utility returns to the beginning of this step, or press Ctrl+C to</p>	

	On the Source Logger...	On the Target Logger...
	exit the script.	
21	The utility prompts you to confirm the location of the source and target Loggers' data directories. Enter 'y' to confirm or 'n' to exit the without migrating the data.	
22	<p>The data migration utility starts to migrate the data.</p> <p>During the migration process, the utility checks if there is sufficient space on the source Logger to perform the dump. If sufficient space is not found, a message indicating the amount of space required is displayed and the utility exits on both Loggers, the source and target. You must free up the indicated amount of space before restarting the utility.</p> <p>Note: When you restart the utility, make sure that you start it on the target Logger first, and then the source Logger.</p> <p>You can check the progress of the migration in <code>user/logger/dataMigrationSource.out</code> and <code>user/logger/dataMigrationTarget.out</code>.</p>	
23	<p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <p>Caution: Wait for the target Logger to complete and display this message before going on to the next step.</p> <p>source: Source box is done! source: Please make sure data migration has completed on the target logger before rebooting this logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, You can run the Archive Migration Utility, as described in "Migrating Event Archive Settings Separately" on page 20, after completing this step.</p>	<p>If the migration script completes successfully, the following messages are displayed on the source target Logger.</p> <p>Caution: Wait for the target Logger to complete and display this message before going on to the next step.</p> <p>target: Data migration successfully completed! target: Please reboot target box!</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, You can run the Archive Migration Utility, as described in "Migrating Event Archive Settings Separately" on page 20, after completing this step.</p>

	On the Source Logger...	On the Target Logger...
24	<p>Reboot the Logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, you can reboot/restart after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 20, for more information. If you are not going to migrate your archives immediately, reboot at this point.</p>	<p>Reboot the Logger Appliance or restart the Software Logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, and are immediately migrating your archives, you can reboot/restart after you migrate the archives. See "Migrating Event Archive Settings Separately" on page 20, for more information. If you are not going to migrate your archives immediately, reboot/restart at this point.</p>
25		<p>Configure the target Logger to make it match the source Logger. See "Migrating Data Between Loggers" on page 9 and "After the Migration" on page 29 for more information.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 20 for more information.</p>
26		<p>Edit the <code>/etc/hosts.equiv</code> and <code>/root/.rhosts</code> files to remove the following information:</p> <pre><sourceLoggerIPAddress> root</pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 20 for more information.</p>

	On the Source Logger...	On the Target Logger...
		Separately" on page 20 , for more information.
27	<p>After reboot, reset the ARCSIGHT_HOME environment variable, as described in Step 5 on page 11.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationSource_rsh_cleanup.sh</pre> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 20, for more information.</p>	<p>After reboot, reset the ARCSIGHT_HOME environment variable, as described in Step 5 on page 11.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationTarget_rsh_cleanup.sh</pre> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 20, for more information.</p>
28	<p>Create a gzip file of log files created during the data migration process.</p> <p>To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> <p>A file such as dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory.</p>	<p>Create a gzip file of log files created during the data migration process.</p> <p>To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> <p>A file such as dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory.</p>
29	<p>Remove the original data migration utility files. To do so, enter this command:</p> <pre>rm -f \$ARCSIGHT_HOME/datamigration*.tar.gz</pre> <p>Note:</p> <ul style="list-style-type: none"> This will delete the gzip of the log files created in Step 28 above. To preserve this file, copy it to another 	<p>Remove the original data migration utility files. To do so, enter this command:</p> <pre>rm -f \$ARCSIGHT_HOME/datamigration*.tar.gz</pre> <p>Note:</p> <ul style="list-style-type: none"> This will delete the gzip of the log files created in Step 28 above. To preserve this file, copy it to another

	On the Source Logger...	On the Target Logger...
	<p>location.</p> <ul style="list-style-type: none">• If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on the next page, for more information.	<p>location.</p> <ul style="list-style-type: none">• If you chose to skip archive migration (the third option) in Step 20 on page 14, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on the next page, for more information.

Migrating Event Archive Settings Separately

The event archive settings consist of the archive configuration metadata and mappings. If you chose to skip archive migration during data migration, the data that tells Logger how to find the event archives was not migrated. Therefore, when you look at your Event Archive list in Logger, the archives will not be displayed.

The Archive Migration Utility migrates these event archive settings. After archive migration is complete, you will be able to see and access your event archives from your Logger UI, provided they exist in the expected locations.

Note: The archives themselves are not moved. They stay in their original locations, but you will be able to access them from the target Logger.

The archive mapping migration process is very similar to the data migration process and has the same requirements. Like the Data Migration Utility, the Archive Migration Utility consists of two scripts, one for the source Logger and the other one for the target Logger. The scripts need to be run in parallel on the source and target Loggers.

Migrating the Event Archive Settings— Step-by-Step Instructions

Migrating your event archives separately is only required if you chose to skip archive migration (the third option in [Step 20 on page 14](#).) If you chose the first or second option and migrated your archives, do not run these scripts.

Perform these steps to migrate event archive settings from one Logger to another.

Note: Be sure to start the **target** Logger script before the **source** Logger script, as described in [Step 13 on page 23](#) and [Step 15 on page 24](#); otherwise, the archive migration process will not proceed as expected.

If archive migration fails at any point, refer to ["Troubleshooting" on page 30](#).

	On the Source Logger...	On the Target Logger...
1	Make sure that you have completed the data migration process to up to at least "Migrating Data—Step-by-Step Instructions" on page 10 before starting archive migration.	
2	Enable SSH access to the appliance if it is not	Enable SSH access to the target Logger if it

	On the Source Logger...	On the Target Logger...
	<p>already enabled.</p> <p>On the System Admin page, under System, click SSH. The SSH configuration page opens. Click Enable.</p>	<p>is not already enabled.</p> <p>On Logger appliances: On the System Admin page, under System, click SSH. The SSH configuration page opens. Click Enable.</p> <p>On Software Loggers: Ensure that SSH access to the system on which Logger is installed is available.</p>
3	<p>Copy <code>datamigration-6.2-D1092.tar.gz</code> to: <code>/opt/arcsight/logger</code>.</p> <p>This is the Logger home directory, referred to by the Archive Migration utility as <code>ARCSIGHT_HOME</code>.</p> <p>Note: You can skip this step if you did not remove the Data Migration files as described in Step 29 on page 18.</p>	<p>Copy <code>datamigration-6.2-D1092.tar.gz</code></p> <p>On Logger Appliances:</p> <p>to <code>/opt/arcsight/logger</code>.</p> <p>On Software Loggers, use the directory path where Logger was installed. The default is:</p> <p><code>/opt/current/arcsight/logger</code></p> <p>This is the Logger home directory, referred to by the Archive Migration utility as <code>ARCSIGHT_HOME</code>.</p> <p>Note: You can skip this step if you did not remove the Data Migration files as described in Step 29 on page 18.</p>
4	SSH to the Logger and log in as user “root.”	SSH to the Logger and log in as user “root.”
5	<p>Set the <code>ARCSIGHT_HOME</code> environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre>	<p>Set the <code>ARCSIGHT_HOME</code> environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME=<Logger_install_directory>/current/arcsight/logger</pre> <p>By default this is:</p>

	On the Source Logger...	On the Target Logger...
		<p>/opt/current/arcsight/Logger</p> <p>You can skip this step if you did not reset the ARCSIGHT_HOME environment variable, or run the cleanup script as described in Step 27 on page 18.</p>
6	<p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre>	<p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre>
7	<p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> <p>Note: You can skip this step if you did not run the cleanup script as described in Step 27 on page 18.</p>	<p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> <p>Note: You can skip this step if you did not run the cleanup script as described in Step 27 on page 18.</p>
8	<p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationSource_rsh_setup.sh</pre>	<p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationTarget_rsh_setup.sh</pre>
9		<p>The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location.</p> <p>If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory.</p> <p>After you enter the directory, the script prompts you to confirm the location you entered. Enter 'y' to confirm or 'n' to re-enter the location.</p>
10		<p>You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not.</p>
11		<p>Edit the /etc/hosts.deny file to add the following information:</p> <pre>in.rlogind: all in.rshd: all</pre>

	On the Source Logger...	On the Target Logger...
		<p>Edit the <code>/etc/hosts.allow</code> file to add the following:</p> <pre>all: <sourceLoggerIPAddress></pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p> <div> <p>Note:</p> <ul style="list-style-type: none"> When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached. You can skip this step if you did not edit the files as described in Step 26 on page 17. </div>
12		<p>Edit the <code>/etc/hosts.equiv</code> and <code>/root/.rhosts</code> files to add the following information:</p> <pre><sourceLoggerIPAddress> root</pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p> <div> <p>Note:</p> <ul style="list-style-type: none"> When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached. You can skip this step if you did not edit the files as described in Step 26 on page 17. </div>
13		<p>Enter this command to run the Archive Migration utility:</p> <pre>bin/scripts/dataMigrationTarget_Archive_Only.sh</pre> <p>On software Logger targets, you may be asked if the non-root user is “arcsight”. If so,</p>

	On the Source Logger...	On the Target Logger...
		<p>enter 'y'. If not, enter the non-root user name that was used when installing Logger.</p> <p>After you enter the user name, the script prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the user name.</p>
14		<p>A message telling you to run the data migration script on the source Logger is displayed.</p> <p>Note: Press Ctrl+C to exit the script at any time.</p>
15	<p>Enter this command to run the Archive Migration utility:</p> <pre>bin/scripts/dataMigrationSource_Archive_Only.sh</pre>	
16	<p>The utility prompts you to confirm the ARCSIGHT_HOME location. Enter 'y' to confirm or 'n' to re-enter the location.</p> <p>The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>Tip: Press Ctrl+C to exit the script at any time.</p>	
17	<p>The utility prompts you to enter the IP address of the target Logger.</p> <p>After you enter the IP address, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the IP address.</p>	
18	<p>The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'n', the utility prompts you to enter the ARCSIGHT_HOME of the target machine. (The utility assumes the ARCSIGHT_HOME for Logger Appliances.)</p>	

	On the Source Logger...	On the Target Logger...
	After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.	
19	<p>If you migrated the archive event settings when performing the Data Migration You cannot run this script, and the script will display the following warning: "You did not choose to skip archive migration last time, thus You cannot migrate archive separately."</p> <p>Otherwise, the utility prompts you to consider how you want to handle archive migration:</p> <ol style="list-style-type: none"> 1. Default archive migration: The Archive Migration script fails and exits if the archive check fails. If the scripts exits because the archive check failed, restore the missing archives and run the script again. 2. Ignore archive check: Archive Migration continues even if the archive check fails. Event archive settings (archive configuration metadata and mappings) are migrated and any missing archives will be accessible if you restore them to their original location. <p>The utility then asks if you would like to migrate your archives only after the archive check passes. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'y', proceed to Step 20 on the next page.</p> <p>If you entered 'n', the utility asks you if you would like to migrate the archive configuration metadata even if some archives are missing? Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'y', proceed to Step 20 on the</p>	

	On the Source Logger...	On the Target Logger...
	next page . If you entered 'n', the utility returns to the beginning of this step, or press Ctrl+C to exit the script.	
20	The utility prompts you to confirm the settings. Enter 'y' to proceed or 'n' to enter the settings again.	
21	The utility asks if you want to migrate the event archive settings now. Enter 'y' to confirm or 'n' to exit the without migrating the event archive settings.	
22	<p>The Archive Migration utility starts to migrate the settings.</p> <p>During the migration process, the utility checks if there is sufficient space on the source Logger to perform the dump. If sufficient space is not found, a message indicating the amount of space required is displayed and the utility exits on both Loggers, the source and target. You must free up the indicated amount of space before restarting the utility.</p> <div> <p>Note: When you restart the utility, make sure that you start it on the target Logger first and then the source Logger.</p> </div> <p>You can check the progress of the migration in user/Logger/dataMigrationSourceArchiveOnly.out and user/Logger/dataMigrationTargetArchiveOnly.out</p>	
23	<p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <div> <p>Caution: Wait for the target Logger to complete and display this message before going on to the next step.</p> </div> <p>source: Source box is done! source: Please make sure Archive Migration has completed on the target logger before rebooting this logger.</p>	<p>If the migration script completes successfully, the following messages are displayed on the source target Logger.</p> <div> <p>Caution: Wait for the target Logger to complete and display this message before going on to the next step.</p> </div> <p>target: Archive Migration successfully completed! target: Please reboot target box!</p>
24	Reboot the Logger.	Reboot the Logger Appliance or restart the Software Logger.

	On the Source Logger...	On the Target Logger...
25		<p>Skip this step if you configured your Logger before performing the event archive migration, as described in Step 25 on page 17.</p> <p>Configure the target Logger to make it match the source Logger. See "Migrating Data Between Loggers" on page 9 and "After the Migration" on page 29 for more information.</p>
26		<p>Edit the <code>/etc/hosts.equiv</code> and <code>/root/.rhosts</code> files to remove the following information:</p> <pre>sourceLoggerIPAddress> root</pre> <p>where <code><sourceLoggerIPAddress></code> is the IP address of the source Logger.</p>
27	<p>After reboot, reset the <code>ARCSIGHT_HOME</code> environment variable, as described in Step 5 on page 21.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationSource_rsh_cleanup.sh</pre>	<p>After reboot, reset the <code>ARCSIGHT_HOME</code> environment variable, as described in Step 5 on page 21.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationTarget_rsh_cleanup.sh</pre>
28	<p>Create a gzip file of log files created during the migration process.</p> <p>To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> <p>A file such as <code>dataMigrationLog.2016-01-11PST164827.tar.gz</code> is created in the <code>ARCSIGHT_HOME</code> directory.</p>	<p>Create a gzip file of log files created during the migration process.</p> <p>To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> <p>A file such as <code>dataMigrationLog.2016-01-11PST164827.tar.gz</code> is created in the <code>ARCSIGHT_HOME</code> directory.</p>
29	<p>Remove the original Data Migration utility files.</p> <p>To do so, enter this command:</p>	<p>Remove the original Data Migration utility files.</p> <p>To do so, enter this command:</p>

	On the Source Logger...	On the Target Logger...
	<pre>rm -f \$ARCSIGHT_ HOME/datamigration*.tar.gz</pre> <p>Note: This will delete the gzip of the log files created in Step 28 on the previous page. To preserve this file, copy it to another location.</p>	<pre>rm -f \$ARCSIGHT_ HOME/datamigration*.tar.gz</pre> <p>Note: This will delete the gzip of the log files created in Step 28 on the previous page. To preserve this file, copy it to another location.</p>

After the Migration

Once data migration has completed successfully, do the following:

1. If file receivers were configured on the source Logger, add appropriate NFS mounts for them on the target Logger and configure the receivers to use those mount points. The NFS mount points need to be the same as the one on the source Logger.

When setting the mount point on Logger Appliance targets, use Logger's System Admin interface. For Software Logger targets, set the mount points manually as appropriate for your operating system.

2. Create data and perform configuration that is not migrated (as listed in ["Migrating Data Between Loggers" on page 9](#)) on the target Logger:
 - a. Use the Configuration Backup and Restore feature, described in Logger Administrator's Guide, to back up **only the report content** from the source Logger and restore it to the target Logger. (To back up only the report content, select **Report Content only** from the Backup Content field.)
 - b. Use the Content Import/Export capability of Logger, described in Logger Administrator's Guide, to export alerts and filters from the Source Logger and import it into the Target Logger.

Note: You may need to add destination information to imported alerts.

- c. Manually re-create all other data.
3. If the source Logger had Compliance Insight Packages for PCI, SOX, or IT Governance deployed, reload those packages to the target Logger. If the SOX filters on your source Logger were loaded using the `soxfilters-1188.enc` file, the file is available from HPE ArcSight Customer Support upon request.
 4. If look-up files were not migrated properly, delete the look-up files on the target Logger, and upload those files that are on the source Logger.

Troubleshooting

- If the data migration utility fails during the migration process, press **Ctrl+C** to terminate the utility on both (source and target) Loggers. Once you have exited, re-run the data migration scripts from [Step 13 on page 13](#), and the archive migration scripts from [Step 13 on page 23](#).

Note: When re-running the utility, make sure you start the target Logger script before the source Logger script.

- If the migration process is interrupted, the operation restarts from the beginning when the script is re-run on the source and target Loggers.
- If the data migration process fails with an error message similar to the following message:

```
source: event archive checking failed!
```

ensure that the remote mount points (that match the source Logger's mount points) are set up on the target Logger, or consider selecting a different Archive Migration option.

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 Data Migration Guide (Logger 6.2)

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!