



Data Migration Between Loggers

Summary	1
The Data Migration Process	1
Supported Migration Paths	2
Prerequisites for Migration	3
Non-SAN Appliance Migration	4
Migrating Event Archive Settings Separately	11
SAN to Non-SAN Appliance Event Archive Settings Migration	17
After the Migration	22
Troubleshooting	23

The information in this technical note applies to ArcSight Logger 6.1 (L7491) and the Logger Data Migration Utility 6.1 (D1086).

Summary

Event data on a Logger can be migrated from a Logger Appliance to another Logger Appliance of equal or higher capacity or to a Software Logger installed on a supported operating system. Event Archives can be migrated from a SAN Logger appliance to a Non-SAN Logger Appliance or a Software Logger. Migrating from a Software Logger to another Logger of any type is not supported. For a list of supported migration paths, see [“Supported Migration Paths” on page 2](#).

Data migration between Loggers might be required for these cases:

- 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.

This document describes the data migration process.

The Data Migration Process

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 a step-by-step manner in [“Migrating Data—Step-by-Step Instructions” on page 5](#).

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, HP 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 [“Non-SAN Appliance Migration” on page 4](#). 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. HP ArcSight **does not** recommend using a wide area network (WAN) link for the migration. HP 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.



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

Migration Path	From	Version	To	Version
Appliance to Appliance	Lx400	6.1	Lx500	6.1
Appliance to Software	Lx400 Lx500	6.1	Software Logger	6.1
SAN Appliance to Non-SAN Appliance*	L7400-SAN	6.1	Lx500	6.1
SAN Appliance to Software*	L7400-SAN L7500-SAN	6.1	Software Logger	6.1
* Archive migration only				

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 Logger Administrator's Guide. • 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 the supported Logger version (6.1) for migration.</p> <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>Notes:</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 storage volume on the target Logger during the data migration process. If any pre-allocated space exists on the target, it is overwritten.
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>Note: If the mount point is not set up on the target Logger before data migration begins, the process will fail.</p>
Event Archive	If an event archive is loaded on the source Logger, make sure it is unloaded before you begin the data migration process.
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>

Non-SAN Appliance Migration

If the source is a Non-SAN Logger appliance, you can migrate event data in live storage, archived event data, and some Logger configuration data to another Logger of a supported type.

Only the following data is migrated:

- 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 11](#) 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 11](#) for how to handle data that is not migrated.

- Parser definitions
- Receivers
- Retention information
- Source type information
- Storage groups
- Superindexing information

No other data is migrated.



Note

Do not simply use the configuration backup and restore feature to migrate data that is not migrated to the target Logger. See [“Migrating Event Archive Settings Separately” on page 11](#) for how to handle data that is not migrated.

Examples of data that is not migrated include:

- 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

Migrating Data—Step-by-Step Instructions

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



Be sure to start the target Logger script before the source Logger script, as described in [Step 13 on page 7](#) and [Step 16 on page 7](#); otherwise, the data migration process will not proceed as expected.

If data migration fails at any point, refer to [“Troubleshooting” on page 23](#).

	On the Source Logger...	On the Target Logger...
1	Make sure that the source and target Loggers meet the requirements listed in the “Prerequisites for Migration” on page 3 section before proceeding further.	
2	Reboot the Source Logger.	
3	Copy <code>datamigration-6.1-D1086.tar.gz</code> to <code>/opt/arcsight/logger</code> . This is the Logger home directory, referred to by the Data Migration utility as <code>ARCSIGHT_HOME</code> .	Copy <code>datamigration-6.1-D1086.tar.gz</code> to the following directory: On Logger Appliances: <code>/opt/arcsight/logger</code> On Software Loggers, this varies based on the directory Logger was installed into. The default is: <code>/opt/current/arcsight/logger</code> This is the Logger home directory, referred to by the Data Migration utility as <code>ARCSIGHT_HOME</code> .
4	SSH to the Logger and log in as user <code>“root”</code> .	SSH to the Logger and log in as user <code>“root”</code> .

	On the Source Logger...	On the Target Logger...
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:</p> <pre>/opt/current/arcsight/logger</pre>
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_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> <p>Edit the /etc/hosts.allow file to add the following:</p> <pre>all: <sourceLoggerIPAddress></pre> <p>where <sourceLoggerIPAddress> is the IP address of the source Logger.</p> <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>

	On the Source Logger...	On the Target Logger...
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> <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>Note: 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 bin/scripts/dataMigrationSource.sh -force_checksum</pre> <p>Notes: Using the <code>-force_checksum</code> option can take significantly longer to migrate data. However, this command provides an additional check to ensure that each file has been reliably copied from the source to the target Logger.</p>	
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>Note: 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>	

On the Source Logger...	On the Target Logger...
<p>19 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>	
<p>20 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 configuration metadata and mappings) are migrated and any missing archives will be accessible if you restore them to their original location. 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 11 for more information. <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 page 8.</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 page 8.</p> <p>If you entered 'n', the utility asks you if you are sure you want to skip archive migration?</p> <p>Important: 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> <p>See "Migrating Event Archive Settings Separately" on page 11 for more information.</p> <p>If you entered 'n', the utility returns to the beginning of this step, or press Ctrl+C to exit the script.</p>	
<p>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.</p>	

On the Source Logger...	On the Target Logger...
<p>22 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>	
<p>23 If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <p>Important: Wait for the target Logger to complete before going on to the next step.</p> <p>Source:</p> <pre>source: Source box is done! source: Please make sure data migration has completed on the target logger before rebooting this logger.</pre> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, You can run the Archive Migration Utility, as described in "Migrating Event Archive Settings Separately" on page 11, after completing this step.</p>	<p>If the migration script completes successfully, the following messages are displayed on the source target Logger.</p> <p>Important: Wait for the target Logger to display this message before going on to the next step.</p> <p>Target:</p> <pre>target: Data migration successfully completed! target: Please reboot target box!</pre> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, You can run the Archive Migration Utility, as described in "Migrating Event Archive Settings Separately" on page 11, after completing this step.</p>
<p>24 Reboot the Logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, you can reboot/restart after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, for more information. If you are not going to migrate your archives immediately, reboot at this point.</p>	<p>Reboot the Logger Appliance/Restart the Software Logger.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, and are immediately migrating your archives, you can reboot/restart after you migrate the archives. See "Migrating Event Archive Settings Separately" on page 11, for more information. If you are not going to migrate your archives immediately, reboot/restart at this point.</p>
<p>25</p>	<p>Configure the target Logger to make it match the source Logger. See "Non-SAN Appliance Migration" on page 4 and "After the Migration" on page 22 for more information.</p> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11 for more information.</p>

	On the Source Logger...	On the Target Logger...
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 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, for more information.</p>
27	<p>After reboot, reset the <code>ARCSIGHT_HOME</code> environment variable, as described in Step 5 on page 6.</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 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, for more information.</p>	<p>After reboot, reset the <code>ARCSIGHT_HOME</code> environment variable, as described in Step 5 on page 6.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationOnTarget_rsh_cleanup.sh</pre> <p>Note: If you chose to skip archive migration (the third option) in Step 20 on page 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, 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 <code>dataMigrationLog.20150428_PDT130524.tar.gz</code> is created in the <code>ARCSIGHT_HOME</code> 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 <code>dataMigrationLog.20150428_PDT130524.tar.gz</code> is created in the <code>ARCSIGHT_HOME</code> 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>Notes:</p> <ul style="list-style-type: none"> This will delete the gzip of the log files created in Step 28 on page 10. To preserve this file, copy it to another location. If you chose to skip archive migration (the third option) in Step 20 on page 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, for more information. 	<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>Notes:</p> <ul style="list-style-type: none"> This will delete the gzip of the log files created in Step 28 on page 10. To preserve this file, copy it to another location. If you chose to skip archive migration (the third option) in Step 20 on page 8, this step can be performed after you migrate your archives. See "Migrating Event Archive Settings Separately" on page 11, 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.



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, as described in a step-by-step manner in below.

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 8](#). 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.



Be sure to start the target Logger script before the source Logger script, as described in [Step 13 on page 14](#) and [Step 15 on page 14](#); otherwise, the archive migration process will not proceed as expected.

If archive migration fails at any point, refer to [“Troubleshooting” on page 23](#).

	On the Source Logger...	On the Target Logger...
1	Make sure that you have completed the data migration process to up to at least Step 23 on page 9 before starting archive migration.	
2	<p>Enable SSH access to the appliance if it is not already enabled.</p> <p>On the System Admin page, under System, click SSH. The SSH configuration page opens. Click Enable.</p>	<p>Enable SSH access to the target Logger if it 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>

On the Source Logger...	On the Target Logger...
<p>3 Copy <code>datamigration-6.1-D1086.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 10.</p>	<p>Copy <code>datamigration-6.1-D1086.tar.gz</code> to the following directory:</p> <p>On Logger Appliances: <code>/opt/arcsight/logger</code></p> <p>On Software Loggers, this varies based on the directory Logger was installed into. The default is: <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 10.</p>
<p>4 SSH to the Logger and log in as user "root".</p>	<p>SSH to the Logger and log in as user "root".</p>
<p>5 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=<LoggerInstallDirectory> /current/arcsight/logger</pre> <p>By default this is: <code>/opt/current/arcsight/logger</code></p> <p>Note: You can skip this step if you did not reset the <code>ARCSIGHT_HOME</code> environment variable, or run the cleanup script as described in Step 27 on page 10.</p>
<p>6 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>
<p>7 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 10.</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 10.</p>
<p>8 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>

	On the Source Logger...	On the Target Logger...
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 <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> <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 10.
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> <p>Notes:</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 10.

	On the Source Logger...	On the Target Logger...
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, 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>Note: 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> <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>	

On the Source Logger...	On the Target Logger...
<p>19 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 page 15.</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 page 15. If you entered 'n', the utility returns to the beginning of this step, or press Ctrl+C to exit the script.</p>	
<p>20 The utility prompts you to confirm the settings. Enter 'y' to proceed or 'n' to enter the settings again.</p>	
<p>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.</p>	
<p>22 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> <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/dataMigrationSourceArchiveOnly.out</code> and <code>user/logger/dataMigrationTargetArchiveOnly.out</code></p>	

	On the Source Logger...	On the Target Logger...
23	<p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <p>Important: Wait for the target Logger to complete before going on to the next step.</p> <p>Source:</p> <pre>source: Source box is done! source: Please make sure Archive Migration has completed on the target logger before rebooting this logger.</pre>	<p>If the migration script completes successfully, the following messages are displayed on the source target Logger.</p> <p>Important: Wait for the target Logger to display this message before going on to the next step.</p> <p>Target:</p> <pre>target: Archive Migration successfully completed! target: Please reboot target box!</pre>
24	Reboot the Logger.	Reboot the Logger Appliance/Restart the Software Logger.
25		<p>Note: Skip this step if you configured your Logger before performing the event archive migration, as described in Step 25 on page 9.</p> <p>Configure the target Logger to make it match the source Logger. See “Non-SAN Appliance Migration” on page 4 and “After the Migration” on page 22 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 ARCSIGHT_HOME environment variable, as described in Step 5 on page 12.</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 ARCSIGHT_HOME environment variable, as described in Step 5 on page 12.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationOnTarget_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.20150428_PDT130524.tar.gz</code> is created in the ARCSIGHT_HOME 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.20150428_PDT130524.tar.gz</code> is created in the ARCSIGHT_HOME directory.</p>
29	<p>Remove the original Data Migration utility files.</p> <p>To do so, enter this command:</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 page 16. To preserve this file, copy it to another location.</p>	<p>Remove the original Data Migration utility files.</p> <p>To do so, enter this command:</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 page 16. To preserve this file, copy it to another location.</p>

SAN to Non-SAN Appliance Event Archive Settings Migration

The SAN to Non-SAN Appliance Archive Migration Utility migrates the event archive settings only from a SAN Logger Appliance to a Non-SAN Logger Appliance.

When choosing whether to perform this migration, you should be aware of the following:

- Only event archive settings (archive configuration metadata and mappings) are migrated. **Nothing else is migrated.**
- Data in live storage is **not** migrated. Any data that you want to migrate from a SAN to a Non-SAN appliance must be archived.
- Logger configuration data is **not** migrated. After the migration, you will need to configure the target Logger manually.
- After the archive migration is complete, you will be able to see and access your event archives from your new Logger's UI, provided they exist in the expected locations.



Event data is archived without indexes. Searches on the restored archives will be slow unless you index the archives. You can index a daily archive after it has been stored, but this process can take some time.

Examples of data that is NOT migrated include:

- Alerts
- Archived events



The archives themselves are not moved. They stay in their original locations, but you will be able to access them from the target Logger because the event archive settings are migrated.

- Configuration Backup settings
- Custom schema fields
- Dashboards
- Device Groups
- Devices
- ESM Destinations
- Event data in live storage
- Filters, including system filters, user-defined filters, and PCI/SOX package filters
- Forwarders
- Global Summary data
- Indexing information
- Lookup files
- Parser definitions
- Peer configuration
- Receivers
- Reports (including published reports)
- Retention information

- Saved searches
- Scheduled jobs
- Source Type information
- Storage Groups
- Storage Rules
- Superindexing information

Migrating SAN to Non-SAN Loggers—Step-by-Step Instructions

The SAN to Non-SAN Appliance Archive Migration Utility consists of two scripts, one for the source Logger and the other one for the target s. The scripts need to be run in parallel on the source and target Loggers, as described in a step-by-step manner in below.

Perform these steps to migrate event archive settings from a SAN Logger Appliance to Non-SAN Logger Appliance.



Be sure to start the target Logger script before the source Logger script, as described in [Step 13 on page 14](#) and [Step 15 on page 14](#); otherwise, the archive migration process will not proceed as expected.

If archive migration fails at any point, refer to [“Troubleshooting” on page 23](#).

	On the Source Logger...	On the Target Logger...
1	Make sure that the source and target Loggers meet the requirements listed in the “Prerequisites for Migration” on page 3 section before proceeding further.	
2	Enable SSH access to the appliance if it is not already enabled. On the System Admin page, under System, click SSH . The SSH configuration page opens. Click Enable .	Enable SSH access to the target Logger if it is not already enabled. On the System Admin page, under System, click SSH . The SSH configuration page opens. Click Enable .
3	Copy <code>datamigration-6.1-D1086.tar.gz</code> to <code>/opt/arcsight/logger</code> . This is the Logger home directory, referred to by the Archive Migration utility as <code>ARCSIGHT_HOME</code> .	Copy <code>datamigration-6.1-D1086.tar.gz</code> to the following directory: On Logger Appliances: <code>/opt/arcsight/logger</code>
4	SSH to the Logger and log in as user “root”.	SSH to the Logger and log in as user “root”.
5	Set the <code>ARCSIGHT_HOME</code> environment variable, using the following command: <code>export ARCSIGHT_HOME=/opt/arcsight/logger</code>	Set the <code>ARCSIGHT_HOME</code> environment variable, using the following command: <code>export ARCSIGHT_HOME=/opt/arcsight/logger</code>
6	Enter this command to navigate to the Logger home directory: <code>cd \$ARCSIGHT_HOME</code>	Enter this command to navigate to the Logger home directory: <code>cd \$ARCSIGHT_HOME</code>
7	Enter this command to extract the compressed files: <code>tar xzvf datamigration*.tar.gz</code>	Enter this command to extract the compressed files: <code>tar xzvf datamigration*.tar.gz</code>

	On the Source Logger...	On the Target Logger...
8	Enter this command to run the setup script: bin/scripts/dataMigrationSource_rsh_setup.sh	Enter this command to run the setup script: bin/scripts/dataMigrationTarget_rsh_setup.sh
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 /etc/hosts.deny file to add the following information:</p> <pre>in.rlogind: all in.rshd: all</pre> <p>Edit the /etc/hosts.allow file to add the following:</p> <pre>all: <sourceLoggerIPAddress></pre> <p>where <sourceLoggerIPAddress> is the IP address of the source Logger.</p> <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>
12		<p>Edit the /etc/hosts.equiv and /root/.rhosts files to add the following information:</p> <pre><sourceLoggerIPAddress> root</pre> <p>where <sourceLoggerIPAddress> is the IP address of the source Logger.</p> <p>Notes: When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached.</p>

	On the Source Logger...	On the Target Logger...
13		<p>Enter this command to run the San to Non-SAN Archive Migration utility:</p> <pre>bin/scripts/dataMigrationTarget_Archive_Only_SANToNonSAN.sh</pre> <p>The utility asks you to confirm that you are migrating archive metadata only from a SAN Logger to a non-SAN Logger. Enter 'y' if so. Enter 'n' if not.</p> <p>Next, the utility warns you that to migrate archived metadata from a SAN Logger appliance to a non-SAN Logger, all data on the Target Logger needs to be erased before migrating. Enter 'y' to erase any data on the target Logger and proceed with the data migration. Enter 'n' to exit the data migration script and leave the data on the target logger unaffected.</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 San to Non-SAN Archive Migration utility:</p> <pre>bin/scripts/dataMigrationSource_Archive_Only_SANToNonSAN.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>Note: 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 confirm that you are migrating archive metadata only from a SAN Logger appliance to a non-SAN Logger. 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>	

	On the Source Logger...	On the Target Logger...
19	<p>The utility 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 page 21.</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 page 21. If you entered 'n', the utility returns to the beginning of this step, or press Ctrl+C to exit the script.</p>	
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> <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_Archive_Only_SANToNonSAN.out</code> and <code>user/logger/dataMigrationTargetArchive_Only_SANToNonSAN.out</code></p>	
23	<p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <p>Important: Wait for the target Logger to complete before going on to the next step.</p> <p>Source:</p> <pre>source: Source box is done! source: Please make sure Archive Migration has completed on the target logger before rebooting this logger.</pre>	<p>If the migration script completes successfully, the following messages are displayed on the source target Logger.</p> <p>Important: Wait for the target Logger to display this message before going on to the next step.</p> <p>Target:</p> <pre>target: Archive Migration successfully completed! target: Please reboot target box!</pre>
24	Reboot the Logger.	Reboot the Logger Appliance.
25		Configure the target Logger to make it match the source Logger. See "SAN to Non-SAN Appliance Event Archive Settings Migration" on page 17 and "After the Migration" on page 22 for more information.

	On the Source Logger...	On the Target Logger...
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 18.</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 18.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationOnTarget_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.20150428_PDT130524.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.20150428_PDT130524.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> <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 page 22. To preserve this file, copy it to another location.</p>	<p>Remove the original Data Migration utility files.</p> <p>To do so, enter this command:</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 page 22. 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 ["Non-SAN Appliance Migration" on page 4](#)) on the target Logger or ["SAN to Non-SAN Appliance Event Archive Settings Migration" on page 17](#):
 - 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 content from the Source Logger and import it into the Target Logger.
 - For Non-SAN to Non-SAN Data Migration, you can export alerts* and filters from the source Logger and Import them on the target Logger.
 - For SAN to Non-SAN, you can export Alerts*, Filters, Dashboards, Fieldsets, Parsers**, Saved Searches, and Source Types.



* You may need to add destination information to imported Alerts.

** If an extra parser is created, you can delete it.

- 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 ArcSight Customer Support upon request.
 - 4** If lookup files were not migrated properly, delete the look-up files on the target Logger, and upload those files the 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 7](#), the archive migration scripts from [Step 13 on page 14](#) or the SAN to Non-SAN archive migration scripts from [Step 13 on page 20](#). 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, 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.

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

Copyright © 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

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

September 15, 2015