

# **Migrating ESM Resources From Oracle to CORR-Engine**

---

ESM 5.0 SP2 or ESM 5.2  
to ESM 6.0c

October 15, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

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

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

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

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

## Contact Information

---

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

---

## Revision History

---

<b>Date</b>	<b>Product Version</b>	<b>Description</b>
10/15/2013	ESM with CORR-Engine 6.0c	Describes how to migrate ESM Resources from ESM 5.0 SP2 or ESM 5.2 to ESM 6.0c

---

# Contents

---

**Migrating ESM Resources**  
**From Oracle to CORR-Engine ..... 7**

    Migrating the Resources ..... 7

    What Gets Migrated ..... 7

    Migration Paths ..... 8

    The Log Files ..... 8

    Excluding Resources from Being Migrated ..... 8

    Before Running the Migration Tool ..... 8

        Case Customization ..... 10

    Running the Tool ..... 10

    Resource Migration in a Hierarchical Setup ..... 12

    Troubleshooting ..... 13

    Post Migration Issues ..... 13

    Uninstalling the Tool ..... 14



# Migrating ESM Resources From Oracle to CORR-Engine

---

This document tells you how to migrate the ESM resources from your legacy systems, such as ESM 5.0 SP2 or ESM 5.2 to ESM 6.0c.

The goal of this migration is to help you migrate your content from the Oracle database to CORR-Engine.

## Migrating the Resources

To upgrade your legacy Oracle-based ESM 5.x, follow these two steps in the order listed below:

- 1 Install ESM 6.0c on a machine other than your ESM 5.x machine. Refer to the 6.0c ESM Installation and Configuration Guide for instructions on installing ESM 6.0c.
- 2 Migrate your resources from an existing (legacy) ESM 5.x installation to the **freshly installed ESM 6.0c** on which the resources have not been altered or added.

**Important!** Any resources that are changed or added after installation along with their associations with any events will be wiped out while migrating the resources. This document will assist you in this step.

## What Gets Migrated

Consider the following before you migrate:

- Migration of content is only supported to a **freshly** installed ESM 6.0c installation.
- The following will **not** be migrated:
  - ◆ Event data
  - ◆ Case event data
  - ◆ Trend data - Trend tables are not migrated as part of data migration tool as these tables can have large amount of data. Trend tables are recreated on the system when the trend runs first time based on the schedule. Wait for the first scheduled run of a trend before running a query on the trend.
  - ◆ Domain fields - fields will migrate, but actions on the data won't work because the Domains feature is not supported on the CORR-Engine. Rule actions won't fire on domain fields and channels with domain fields will not have values.

## Migration Paths

The following table outlines the migration paths from the source version to the destination.

**Table 1** Migration Paths

Source	Destination
ESM 5.0 SP2 Patch 3 or higher	ESM 6.0c
ESM 5.2 Patch 1 or higher	ESM 6.0c

## The Log Files

The migration tool creates the `ResourceMigration.log` file, which logs the actual schema and data transfer process. The file is located in

`/opt/arcsight/resourcemigration/logs/ResourceMigration.log`.



The `ResourceMigration.log` file is overwritten each time you run the migration tool.

The upgrade process which is run from the ArcSight Manager's bin directory (in [Step 13 on page 12](#)) creates two log files, `server.upgrade.log` and `server.upgrade.std.log` which are located in `/opt/arcsight/manager/logs/upgrade`.

These logs are also helpful for troubleshooting should you run into issues while running the tool.

## Excluding Resources from Being Migrated



MySQL 5.1 supports 1024 partitions. If a table you are migrating has more than 1024 partitions, the migration will fail and you will receive an error informing you that too many partitions were defined. To resolve this issue, exclude tables that have over 1024 partitions by adding the table name to the `SqlQueryPattern.xml` file located in `/opt/arcsight/resourcemigration/config` directory.

When migrating your resources from Oracle to CORR-Engine, there may be some tables in your Oracle database that you may not want to transfer. You can configure the tool to exclude such tables. The `<pattern>` tag in the

`/opt/arcsight/resourcemigration/config/SqlQueryPattern.xml` file defines which tables get migrated. Should you need to modify this tag to either include additional tables or exclude tables that are already included, the migration tool provides means to exclude an Oracle table during transfer. For details, contact HP by sending an email to [arst - resourcemigrationtool@hp.com](mailto:arst - resourcemigrationtool@hp.com) before you do so.

## Before Running the Migration Tool

**Important!** Keep in mind that both source (ESM using Oracle) and destination (ESM using CORR- Engine) must be installed in the same mode (FIPS mode or default mode) and they must use the same authentication parameters (Password Based or SSL, etc.).

Have the source and destination environments ready by following the steps below.

**Source machine (where Oracle is installed):**

- ◆ Shut down the Manager and ArcSight Web.

**On Unix machines:**

Run the following command to stop ArcSight Web:

```
/etc/init.d/arcsight_web stop
```

Run the following command while logged in as the **superuser** in order to stop the ArcSight Manager:

```
/etc/init.d/arcsight_manager stop
```

**On Windows:**

When not running as a service, press Ctrl-C in the command window where the ArcSight Manager or ArcSight Web is running.

- ◆ **Important!** Make sure that Oracle is up and running.
- ◆ Edit the `<ORACLE_HOME>/network/admin/sqlnet.ora` file to add your destination machine's IP address to the `TCP.INVITED_NODES` field.
- ◆ Restart the TNS listener by running the following command on Unix machines:

```
/etc/init.d/tnslister restart
```

On Windows, you must stop and then start the TNS Listener service.

- ◆ Some tables are dynamically created (for instance Active List, Session List and Trends). The column names for such tables depend on input from you. Make sure that your tablename in Oracle do not contain any special characters. Special characters are not permitted for table names in MySQL, because table names are mapped to actual file names in the operating system. So any character (or even character sequence) that is not permitted in the operating system's file system can not be used in a table name.
- ◆ Make sure archived report definitions are not saved in the database. If reports are saved in the database, download the BLOB files for them to the system file, and then remove them from database before you run the resource migration.
- ◆ Make sure that you have the location of the Firefox browser listed in your path environment variable.
- ◆ The size of BLOB/CLOB objects such as reports, or configuration files or any other BLOB/CLOB files saved in database, must not exceed 125 MB. Should they exceed 125 MB, they must be downloaded on your machine and removed from the database before you begin the migration process. To see the size of such objects:
  - i Find all the tables in 'arcsight' schema.
  - ii Select all the tables that have blob columns.
  - iii Find the length of each blob column in each table.

Refer to the Oracle documents for details on the above steps.

**Destination machine (ESM 6.0c):**

- ◆ Your machine must have at least 500 MB of free space.
- ◆ Make sure that the Oracle database on the source system is accessible.
- ◆ If you have a very large number of resources, the default 6 GB of heap size on the Manager may not be sufficient to handle the load. To work around this issue, set `ARCSIGHT_JVM_OPTIONS` environment variable to the desired heap size before you run the migration tool. For instance,

```
ARCSIGHT_JVM_OPTIONS="-Xms4096m -Xmx8192m".
```

- ◆ Your destination machine should have a **freshly installed** ESM 6.0c, where no live events have been processed or other resources created. All data on the destination system will be overwritten by the resource migration. In other words, all resources created before migration will be lost.
- ◆ If you have large Active Lists and Session Lists (entries in millions) that need to be migrated, you must add the following properties in `/opt/arcsight/manager/config/server.properties` on the **destination** machine in order to avoid data loss:

```
sessionlist.max_capacity=<max_entry_in_SessionList>
```

```
activelist.max_capacity=<max_entry_in_ActiveList>
```

- ◆ Shut down the ArcSight Manager and ArcSight Web.

## Case Customization

If you have done any case customizations on the source ESM system, contact HP by sending an email to [arst - resourcemigrationtool@hp.com](mailto:arst-resourcemigrationtool@hp.com) before proceeding with the resource migration.

## Running the Tool

The Migration Tool must be run on the **destination** machine.

- 1 Log in as user "arcsight" on your destination system that has ESM 6.0c installed on it.
- 2 Stop ArcSight Web by running:

```
/sbin/service arcsight_services stop arcsight_web
```

- 3 Stop the ArcSight Manager by running:

```
/sbin/service arcsight_services stop manager
```

- 4 Download the following file on your destination machine:

```
ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin
```

where x.x.x stands for the migration tool version number.

- 5 Run the following file from the location where you placed it. It can be run in GUI mode or console mode. If you do not have X Windows installed, it automatically runs in console mode.

```
./ArcSight-ResourceMigration-x.x.x.<build_number>.0-Linux.bin
```

- 6 Follow the prompts on the screens.
- 7 After the installation completes, open the `/opt/arcsight/resourcemigration/config/Config.databases.properties` file.
- 8 Edit the properties as follows and save the file:



You only need to change the credentials to the source and destination systems and source database instance name if it is other than "arcsight". Accept the default values for the remaining properties.

---



```

sourceServerName=<IP address or hostname of the machine that has
Oracle on it>

sourceSchema=<Oracle database instance name>

sourcePortNumber=1521

sourceUserName=<"oracle" user's username (usually "arcsight")>
*sourcePassword=

* Delete the default text in the file and leave this property blank.

targetServerName=127.0.0.1

```



Do not change the IP for the `targetServerName` field. By default, it is set to 127.0.0.1.

```

targetSchema=arcsight

targetPortNumber=3306

targetUserName=arcsight

**targetPassword=

** Delete the default text in the file and leave this property blank.

validation=Yes

transferData=Yes

preSql=Yes

postSql=Yes

disableKeys=Yes

parallel=Yes

maxLobSize=125 MB<max size of record in any table in MySQL
database>

skipDDLSpecialChars=Yes

useFreeMemOnly=Yes

```

**9 Verify that Logger, MySQL and postgresql are up by running:**

```
/sbin/service arcsight_services status all
```

If they are not running, be sure to start them.

To start the postgresql, run:

```
/sbin/service arcsight_services start postgresql
```

To start MySQL, run:

```
/sbin/service arcsight_services start mysqld
```

To start Logger, run:

```
/sbin/service arcsight_services start logger
```

**10** If running, stop the following components:

## ◆ ArcSight Web

```
/sbin/service arcsight_services stop arcsight_web
```

## ◆ ArcSight Manager

```
/sbin/service arcsight_services stop manager
```

**Important!**

If you run the migration from a remote system connected to the appliance, have X-Windows running on your remote system and use `ssh -X` to run the migration.

---

**11** Run the Resource Migration tool:**a** The tool checks to make sure that the version of the database schema on your source machine is listed in the

`/opt/arcsight/resourcemigration/config/Version.properties` file. It compares only the major, minor, and service pack version of the version number. For example, if the version number is 5.2.0.6584.0, it will compare only 5.2.0 and ignore the rest. If it is not already listed, add your database schema version to the `Version.properties` file and save it. For example, if `Version.properties` looks as follows, add your version below 5.2.0:

```
5.0.2
```

```
5.2.0
```

**b** From the `bin` directory of the Resource Migration tool (by default `/opt/arcsight/resourcemigration/bin`), run the following:

```
./arcsight_resourcemigration.sh
```

**12** Check the `ResourceMigration.log` file. If you find any errors in the file, resolve them first before proceeding further. If you are unable to fix the issue, contact HP for help with it by sending an email to [arst - resourcemigrationtool@hp.com](mailto:arst - resourcemigrationtool@hp.com). Then, follow [Step 11 on page 12](#) again.**13** Verify that upgrade was successful by checking both the Upgrade Wizard's report located in `/opt/arcsight/manager/upgrade/out/<date-time>/summary.html` and the wizard's log in `/opt/arcsight/manager/logs/upgrade`.**14** Start the Manager by running:

```
/sbin/service arcsight_services start manager
```

**15** Start ArcSight Web by running:

```
/sbin/service arcsight_services start arcsight_web
```

## Resource Migration in a Hierarchical Setup

A hierarchical setup is where data from one or more source ArcSight Managers is forwarded to a central, destination ArcSight Manager.

To migrate resources in a hierarchical setup, you must first migrate the resources on the upper most level Managers one at a time. For each Manager, follow the directions in all the sections above. The next step is to migrate the resources on all ArcSight Managers at the

next-level down in the hierarchy until all Managers at each level of the hierarchy have been upgraded.

## Troubleshooting

Here are some tips for troubleshooting the following issues.

### ■ Errors when running the migration tool

If you run into errors when running the migration tool, the tool will terminate its execution. If you encountered the error while running the wizard, check the log file for the wizard, try to fix the issue if possible, then rerun the wizard.

If you encountered the error during the actual resource migration (after you run `./arcsight_resourcemigration.sh` command), you need to check the `ResourceMigration.log` file for the problem and try to fix the issue and rerun the `arcsight_resourcemigration.sh` command.

If you are unable to fix the issue, contact HP for help with it by sending an email to [arst-resourcemigrationtool@hp.com](mailto:arst-resourcemigrationtool@hp.com).

### ■ Error when running the content upgrade

The resource migration tool first migrates your resources and then upgrades the content.

Look for the line, "Data migration tool ends" in the `ResourceMigration.log` file which is an indication that your resources have been migrated successfully and that the content upgrade has begun. If you run into an error while upgrading your content, run the Content (Core and Foundation packages) upgrade (**while logged in as "arcsight" user**) from the Manager's `bin` directory (`/opt/arcsight/manager/bin`) on the destination machine to bring the schema and the standard content up to ESM 6.0c requirements:

```
./arcsight upgrade manager -m -i silent -f /dev/null
```

### ■ Trends-related error message

Immediately after resource migration, if you view the Trend, you will see the following error:

```
Persistence Exception. Unable to execute query.Table Trend***
doesn't exist.
```

This is because the trend data does not get migrated and there is no trend data available immediately after the resource migration. Once the trend runs, it will backfill data and this issue will automatically get resolved and trends will work normally.

### ■ Out of memory errors when migrating resources

This can happen when you have a very large number of resources and the default 6 GB of heap size is insufficient to handle the load. To work around this issue, set `ARCSIGHT_JVM_OPTIONS` environment variable to the desired heap size, then run the tool again. For instance,

```
ARCSIGHT_JVM_OPTIONS="-Xms4096m -Xmx8192m".
```

## Post Migration Issues

- After the resource migration completes, the latitude values for `ARC_LOCATION` get truncated and appear as a double value in MySQL. The in-memory value may not match the value in the database, especially if some of these values get stored in Active Lists and Session Lists.

- The Reference ID for a resource changes after the resource migration, so if any resource (for example, Filters) refers to another resource by its Reference ID, the referring resource needs to be manually updated to use the new Reference ID.
- Make sure to re-register your remotely installed connectors with the Manager.
- The Resource Validation report generated at the end of the upgrade process may have some invalid resources. As a workaround, run the resource validation script manually after the upgrade finishes:
  - a Run the resvalidate script the first time with '-persist true' (which is the default value if you do not explicitly state it) to validate and fix invalid resources. There is a chance that some invalid resources could be missed the first time.

```
arcsight resvalidate
```

- b So, run the resvalidate script a second time with '-persist false' to generate an accurate report:

```
arcsight resvalidate -persist false
```

In general, if you need to run the resource validation script at any point, be aware that you need to run it twice.

- Once you have completed resource migration, review the enabled Pattern Discovery schedules and disable or reduce any unneeded schedules. This will free system resources for yielding higher EPS.

## Uninstalling the Tool

To uninstall the tool, run the following command from

`/opt/arcsight/resourcemigration/UninstallerData` directory:

```
./Uninstall_ArcSight_Resource_Migration
```