Upgrading ArcSight™ Express to v4.5 SP2

Document Status

This technical note describes the steps required to upgrade the software components on ArcSight Express from v4.5 SP1 or v4.5 SP1 Patch 2 to v4.5 SP2.

If you are upgrading from an older version of ESM, you are required to upgrade to all the interim versions one at a time, before you upgrade to v4.5 SP2.

For example, if you are upgrading from v4.5 GA to v4.5 SP2, you will be required to first upgrade your v4.5 GA installation to v4.5 SP1 before upgrading to v4.5 SP2. See the *Upgrading ArcSight Express from v4.5 GA to v4.5 SP1* document for details on upgrading to v4.5 SP1. After you have upgraded to v4.5 SP1, use this guide to upgrade to v4.5 SP2.

Summary

This document covers the following topics:

On M7100 Appliance When Upgrading From v4.5 SP1 Patch 2 (build 6043)

For instructions on how to check your ArcSight Express Appliance build number, follow Step 1 on page 2.

When upgrading from ESM 4.5 SP1 Patch 2 to ESM 4.5 SP2, you need to follow these steps in order to avoid receiving a dbcheck error:

1. Open a shell window and go to the Database's `<ARCSIGHT_HOME>/bin/scripts` directory.
2. Run the `dos2unix dbcheck.sh` command.

Upgrading to v4.5 SP2

To upgrade the components on your ArcSight Express Appliance:

1. Make sure to get the build number on your ArcSight Express Appliance and make a note of it. In future if you need to contact ArcSight Customer Support, you need to have your build number handy.

   To check the software build number on your ArcSight Express appliance, run the following from a command prompt:

   ```
   rpm -q arcsight-express-manager
   ```

   If you see the following output:

   ```
   arcsight-express-manager-4.5-M5793
   ```

   then you are on v4.5 GA version of ArcSight Express. You will need to first upgrade to v4.5 SP1 before proceeding any further.

2. Download the self-extracting upgrade file, `aeupdate-4.5.2.xxxx.x.pl` and optionally its checksum file, `aeupdate-4.5.2.xxxx.x.pl.md5`, from the ArcSight Customer Support web site. The xxxx in the file name stands for the build number.

3. If you downloaded the file(s) to a system other than the ArcSight Express appliance that you want to upgrade, move the file(s) over to the ArcSight Express appliance using the `scp` command. For example, from your local machine where the file(s) are located, run:

   ```
   scp aeupdate-4.5.2.xxxx.x.pl root@<hostname>.<domain>:/root
   ```

4. You can perform the rest of the steps either directly on the ArcSight Express machine or remotely using `ssh`. To use `ssh`, open a shell window by running:

   ```
   ssh root@<hostname>.<domain>
   ```

   Using an `ssh -X` session to upgrade ArcSight Express causes errors.

   Instead of using `ssh -X` to upgrade ArcSight Express, run the upgrade in a simple `ssh` connection to the appliance.

5. Verify the integrity of the update file you have downloaded just to make sure that it was not truncated or corrupted during the download. Run:

   ```
   md5sum -c aeupdate-4.5.2.xxxx.x.pl.md5
   ```

6. Run the self-extracting upgrade file:

   ```
   perl aeupdate-4.5.2.xxxx.x.pl
   ```

   The upgrade is done in silent mode and transfers configurations, upgrades the schema, upgrades the content, and generates upgrade report for the Manager upgrade.

   - Before the upgrade process begins, the existing software components will be backed up into the following location:
     - `/opt/arcsight/db.preUpgradeBackup`
     - `/opt/arcsight/manager.preUpgradeBackup`

- /opt/arcsight/web.preUpgradeBackup

Keep in mind that if you do multiple upgrades, the preUpgradeBackup files get overwritten each time you do an upgrade. For example, if you are on v4.5 GA and upgrade to v4.5 SP1, these backup files get created for the v4.5 GA installation. But if you further upgrade from v4.5 SP1 to v4.5 SP2, the v4.5 GA backup files get overwritten with the v4.5 SP1 backup files. Consequetly, will not be able to rollback to v4.5 GA version because you would have lost those backup files.

- The aeupdate-4.5.2.xxxx.x.pl file extracts itself into a subdirectory within /opt/updates directory and automatically upgrades the existing RPMs.
- The following log files for the upgrade are placed in the /opt/updates directory:
  - *.res - shows the result of the operation, such as success, error, or reboot
  - *.log - records the details of the upgrade process

  where * stands for the name of the self-extracting perl file.
- Before the components get upgraded, a check is performed on the database of your previous installation to make sure that it is ready for the upgrade and the logs for this check are placed in the /opt/arcsight/db.preUpgradeBackup/ directory.
- The system tables are exported as arcsight.dmp and placed in the /opt/arcsight/db.preUpgradeBackup directory.
- The logs for the dbcheck can be found in /opt/arcsight/db.preUpgradeBackup/logs/dbcheck directory. The ResourceCountV4.0.htm file contains the names of all resources. However, the names of new resources do not appear in the file.

To confirm that the upgrade succeeded

You can check the upgrade summary report and logs to find out if the Manager upgraded successfully. The upgrade summary report is applicable to the Manager only.

To make sure that your upgrade completed, run:

```
rpm -qa | grep arcsight | sort
```

You should see the following packages listed where xxxx stands for the build number:

```
arcsight-3ware-cli-x.xx.xx.xxxraidx-x
arcsight-connector-4.7.6.xxxx.x-x
arcsight-express-db-4.5.2-Mxxxx
arcsight-express-manager-4.5.2-Mxxxx
arcsight-express-web-4.5.2-Mxxxx
arcsight-logos-x.x-x
arcsight-megaraid-cli-x.xx.xx-x
arcsight-oracle-10.2.0.4-Mxxxx.x
** arcsight-oracle-cpuxxxxxx-xxxxx.xxxxxxx.x-Mxxxx.x
arcsight-platform-setup-x.x-xxxxxxxx_xxxx
```

The x in these package names represents a number in the package's version number.

** Depending on the number of Oracle CPUs that are installed on your system, you may see multiple oracle cpu packages, one package per CPU installed.

An incomplete or aborted upgrade will show some of the packages with the upgraded version number, but others will have the original (pre-upgrade) version number-- depending upon which component the upgrade stopped at.

You have upgraded to ArcSight Express v4.5 SP2.

Make sure that you have obtained the new license file from ArcSight Customer Support and updated your appliance with it.

Make sure to upgrade your existing Console. See "Upgrading the Console" on page 7.

Rolling Back to the Previous Version

- If you run into issues when upgrading and are on an Arcsight Express version prior to build 4.5.1.6044.2, ArcSight recommends that you contact ArcSight Customer Support **before** you roll back your upgraded version using the procedure in this section.
- When you do an upgrade, an `arcsight.dmp` file (containing your base ESM installation) gets created in the `/opt/arcsight/db.preUpgradeBackup` directory. If for any reason, you have to roll back to your original installation after or while doing an upgrade, we recommend that you first copy the `arcsight.dmp` file to a secure location. This will allow you to restore your original data if needed. Keep in mind that the `arcsight.dmp` file gets overwritten with any subsequent upgrades.

If you encounter a problem when installing this patch you can roll back the software to the base installation which existed on your ArcSight Express appliance before you started installing the patch. You can roll back only the Database, Manager, and Web.

Should the patch installation fail, file an ArcSight Customer Support ticket and provide the installation logs. You have the option to manually repair the incomplete patch installation with the help of ArcSight Support, or you can roll back to the previous version.

To rollback to the previous version of the software:

1. Make sure you are logged in as user "root".
2. Stop ArcSight Manager if it is running:

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

3. Stop ArcSight Web if it is running:

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

4. Delete the ArcSight Express components by running:

   ```
   rpm -e --nodeps arcsight-express-web-4.5.2-xxxx
   ```

   ```
   rpm -e --nodeps arcsight-express-manager-4.5.2-xxxx
   ```

```
rpm -e --nodeps arcsight-express-db-4.5.2-xxxx
```

where `x` stands for a digit in the build number.

The above commands delete the ArcSight Express files. You may see warning(s) similar to this:

```
warning: /opt/arcsight/manager/jre/lib/security/cacerts saved
as /opt/arcsight/manager/jre/lib/security/cacerts.rpmsave
```

Note that if the upgrade failed before it completes, you will receive an error message that one or more of the packages is not installed.

5 Delete the remaining files under `/opt/arcsight/db`, `/opt/arcsight/manager`, `/opt/arcsight/web` (for example, the log files, `.config` file(s), and other dynamically created files):

```
cd /opt/arcsight/

rm -rf web manager db
```

6 Restore the backed up v4.5.x versions (previously installed) of each component (Database, Manager, Web):

```
cd /opt/arcsight/

mv web.preUpgradeBackup web.preUpgradeBackup.01

mv manager.preUpgradeBackup manager.preUpgradeBackup.01

mv db.preUpgradeBackup db.preUpgradeBackup.01

cp -prd web.preUpgradeBackup.01 web

cp -prd manager.preUpgradeBackup.01 manager

cp -prd db.preUpgradeBackup.01 db
```

7 Check whether you need to download and extract the 4.5.x update bundle:

```
cd /opt/updates/aeupdate-4.5.1.xxxx.x/RPMS
```

where x stands for a number in the version number of your previously installed bundle.

If the directory exists, then you do not need to do the download and extraction. Go to Step 10.

8 Download the v4.5 service pack update bundle, `aeupdate-4.5.1.xxxx.x.pl`, relevant to your previous installation, from ArcSight Support download website. For example, if you were on v4.5 SP1 build 6044, then you should download the file `aeupdate-4.5.1.6044.2.pl`

9 Extract the contents of this file by running the following command (be sure to include the '-n' option at the end:

```
perl aeupdate-4.5.1.xxxx.x.pl -n
```

This will create the `/opt/updates/aeupdate-4.5.1.xxxx.x/RPMS` directory.

10 Go to the RPMS directory:

```
cd /opt/updates/aeupdate-4.5.1.xxxx.x/RPMS

mkdir /root/rpms.451
```

```
cp arcsight-express-*.rpm  /root/rpms.451

cd /root/rpms.451
```

11 Synchronize the RPM database with the fileset that is currently on your local disk from the directory where you downloaded it. (In the example above, it would be cd /root/rpms.451/). If all your components are in the same directory, run:

```
rpm -i --justdb --nodeps --noscripts --notriggers *.rpm
```

If you had copied your RPM files in multiple locations, you will have to run the command for each component individually from their respective locations (relevant to the version you want to roll back to) as follows:

Database:

```
rpm -i --justdb --nodeps --noscripts --notriggers
arcsight-express-db-4.5.1-xxxx.x86_64.rpm
```

Manager:

```
rpm -i --justdb --nodeps --noscripts --notriggers
arcsight-express-manager-4.5.1-xxxx.x86_64.rpm
```

Web:

```
rpm -i --justdb --nodeps --noscripts --notriggers
arcsight-express-web-4.5.1-xxxx.x86_64.rpm
```

12 Reimport `arcsight.dmp` file from `/opt/arcsight/db` directory. This is required in order to revert your schema to its original pre-upgrade version. To import the arcsight.dmp file, run this command from your ArcSight Database's `ARCSIGHT_HOME/bin` directory:

```
arcsight import_system_tables <export_username>
<import_username> <import_password> <TNS_name> <dump_file_path>
```

13 Start the Manager:

```
/etc/init.d/arcsight_manager start
```

14 Start the Web:

```
/etc/init.d/arcsight_web start
```

15 Make sure to move or rename the `/opt/updates` directory.

Rolling back a Platform Package

Run this command to list all the packages:

```
rpm -qa | grep arcsight | sort
```

The following packages are platform packages which are related to the ArcSight Express Appliance itself:

```
arcsight-3ware-cli-x.xx.xx.xxxraidx-x
arcsight-deltarpm-x.x-x
arcsight-logos-x.x-x
arcsight-megaraid-cli-x.xx.xx-x
arcsight-platform-setup-x.x-xxxxxxxx_xxxx
```

The x in these package names represents a number in the package's version number.

If any of the above packages shows two entries such as the `arcsight-platform-setup` package in the following example:

```
arcsight-3ware-cli-2.00.03.015raid6-1
...
arcsight-platform-setup-1.2-20081120_1136
arcsight-platform-setup-1.2-20090227_1501
```

it is an indication that the package did not get upgraded.

To roll back a platform package, contact ArcSight Customer Support for help.

Upgrading the Console

You ArcSight Console should be installed on a machine other than the ArcSight Express. Make sure to perform the steps below on the machine on which you have ArcSight Console installed.

Perform the following steps to upgrade one of your ArcSight Console:

1. Stop ArcSight Console if it is running.
2. If you downloaded the v4.5 SP2 Console installation file to a different machine, transfer it to your Console machine.
3. Run the installation file.
4. Step through the Installation Wizard screens. Specifically, enter values as described below for the following Wizard screens:
   - **Choose Installation Folder**—Enter an `ARCSIGHT_HOME` path for v4.5 SP2 that is different from where the existing Console is installed.

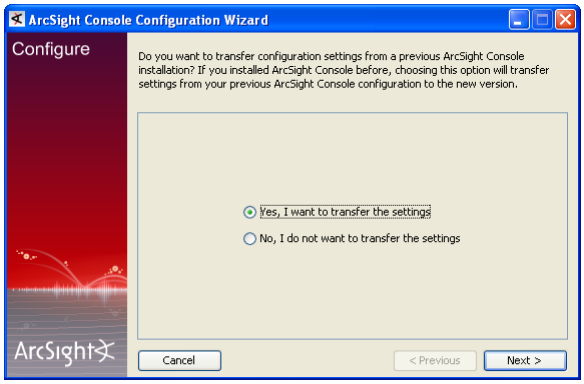
Do NOT install v4.5 SP2 Console in the same location as the existing Console.

Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

   - **Choose Shortcut Folder** (on Windows)**/Choose Link Folder** (on UNIX)—Specify or select where the ArcSight Console icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.
   - **Pre-Installation Summary—**Review the settings and click **Next**.

   After you have stepped through the Installation Wizard, it automatically starts the Configuration Wizard.
5. The Console installation program detects a previous installation and provides you an option to copy your existing settings to the new Console. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type.

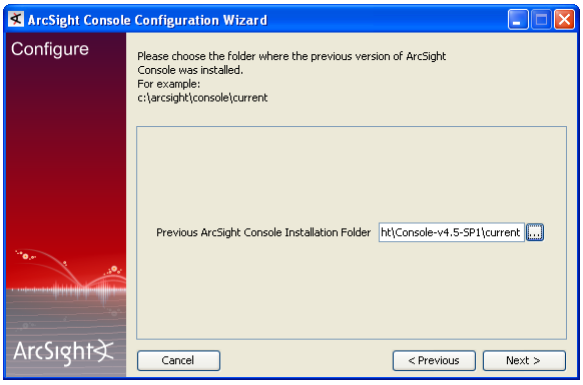
Copying existing settings is optional.



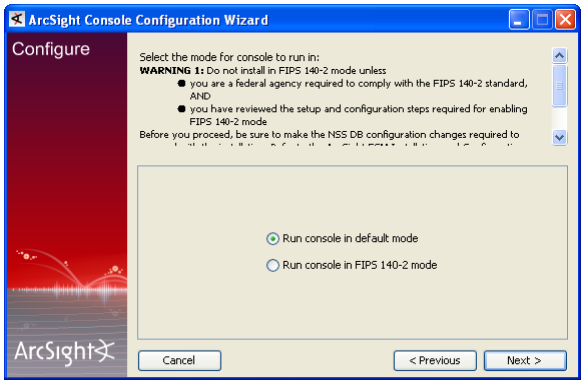
6 You will be prompted to enter the location of your previous Console installation:

Note

Make sure that you point to the `current` directory of the previous Console installation. For example, C:\arcsight\console\current.



7 Running Console in FIPS mode is not supported in this release. In the following screen, make sure that **Run console in default mode** is selected and click **Next**:



8 See the *ArcSight ESM Installation and Configuration Guide, v4.5 SP2* for details on the remaining screens for installing a Console using the installation wizard.

9 Start the ArcSight Console.

A What's new Quick Start screen is displayed automatically. This screen summarizes the new features in ESM v4.5.

10 After you have upgraded a Console to v4.5 SP2, if no event viewers appear initially in the Console, select the `All Active Channels/ArcSight System/Core/Live` channel to view real-time events.

Last Updated: 01/10/10
Keywords: upgrade, database, manager, web