Upgrading ArcSight™ Express v4.5 GA to v4.5 SP1

Document Status

The information in this note applies to ArcSight Express v4.5 SP1.

Summary

This technical note describes the steps required to upgrade the software components on ArcSight Express from v4.5 GA to v4.5 SP1.

Upgrading from v4.5 GA to v4.5 SP1

> **!** 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.

To upgrade the components on your ArcSight Express Appliance:

1. Download the self-extracting upgrade file, `aeupdate-4.5.1.xxxx.x.pl` and optionally its checksum file, `aeupdate-4.5.1.xxxx.x.pl.md5`, from the ArcSight Customer Support web site. The xxxx in the file name stands for the build number.
2. 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-4.5.1.xxxx.x.pl root@<hostname>.<domain>:/root
   ```

3. 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>
   ```

4. 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-4.5.1.xxxx.x.pl.md5
   ```

5. Run this script from your shell prompt. This is needed to update the `/etc/sysctl.conf` file with shared memory, semaphore, and file settings needed for running Oracle:

```
source /opt/arcsight/db/installer/oracle10g/unix/bin/
CheckLinuxPrerequisites.sh
```

6 To run the self-extracting upgrade file:

```
perl aeupdate-4.5.1.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`
- The `aeupdate-4.5.1.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 v4.5 GA database 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-4.7.1.xxxx.x-x
arcsight-express-db-4.5.1-Mxxxx
arcsight-express-manager-4.5.1-Mxxxx
arcsight-express-web-4.5.1-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.

> 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 SP1.

> 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 5.

Rolling 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 current (newly installed) ArcSight Express components:

   ```
   rpm -e --nodeps <componentName>
   ```

   Specifically,

   ```
   rpm -e --nodeps arcsight-express-web-4.5.1

   rpm -e --nodeps arcsight-express-manager-4.5.1

   rpm -e --nodeps arcsight-express-db-4.5.1
   ```

   to delete the newly installed ArcSight Express files. You will see output similar to this:

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

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 GA versions 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.4.5.0.5793.0

cp -prd manager.preUpgradeBackup.01 manager.4.5.0.5793.0

cp -prd db.preUpgradeBackup.01 db.4.5.0.5793.0

cd /opt/arcsight/

ln -s /opt/arcsight/web.4.5.0.5793.0 web

ln -s /opt/arcsight/manager.4.5.0.5793.0 manager

ln -s /opt/arcsight/db.4.5.0.5793.0 db
```

7. Download the v4.5 GA versions of RPMs from the Customer Support website into your own, separate directory. For example, /root/rpms.45.ga.

8. Synchronize the RPM database with the fileset that is currently on the disk from the directory where you downloaded it. (In the example above, it would be cd /root/rpms.45.ga/):

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

9. Import the system dump from `/opt/arcsight/db.preUpgradeBackup/arcsight.dmp:`

   Make sure to use the absolute path to the file when importing it. You will receive an error message if you use a relative path.

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

10. Start the Manager:

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

11. Start the Web server:

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

12. Before you attempt another upgrade, make sure to either rename or delete the `/opt/updates` directory.

In case the upgrade fails, please file an ArcSight Customer Support ticket and provide the upgrade logs. You have the option to manually repair the incomplete upgrade with the help of ArcSight Support, or you can revert back to the previous version.

Rolling back a Platform Package

Run the following 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-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 four 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 would be an indication that the package did not get upgraded.

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

Upgrading the Console

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 SP1 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 SP1 that is different from where the existing Console is installed.

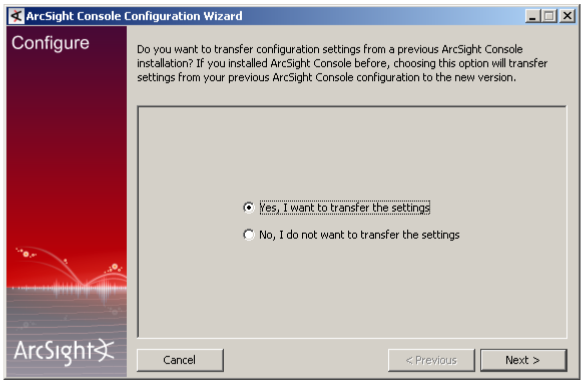
   > Do NOT install v4.5 SP1 Console in the same location as the existing Console.
   >
   > Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

   - **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.



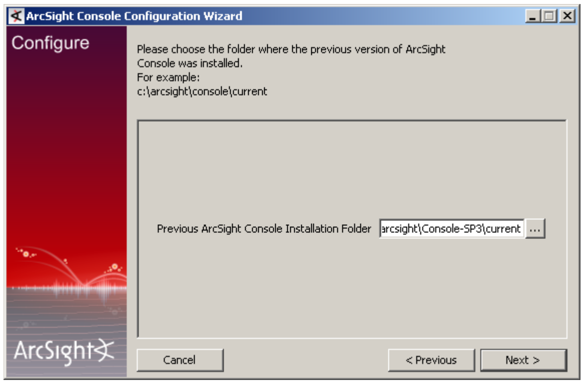
Do you want to transfer configuration settings from a previous ArcSight Console installation? If you installed ArcSight Console before, choosing this option will transfer settings from your previous ArcSight Console configuration to the new version.

● Yes, I want to transfer the settings

○ No, I do not want to transfer the settings

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

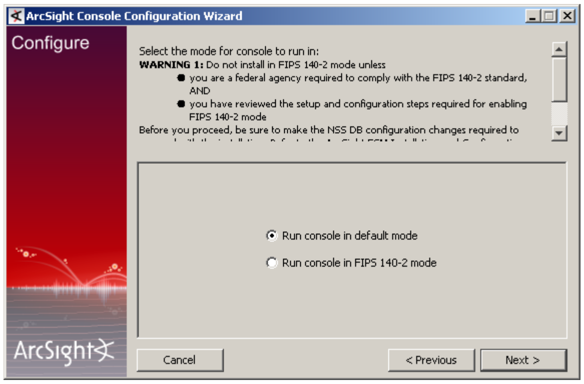
Make sure that you point to the `current` directory of the previous Console installation. For example, C:\arcsight\console\current.



Please choose the folder where the previous version of ArcSight Console was installed.
For example:
c:\arcsight\console\current

Previous ArcSight Console Installation Folder: arcsight\Console-SP3\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**:



Select the mode for console to run in:
WARNING 1: Do not install in FIPS 140-2 mode unless
- you are a federal agency required to comply with the FIPS 140-2 standard, AND
- you have reviewed the setup and configuration steps required for enabling FIPS 140-2 mode

Before you proceed, be sure to make the NSS DB configuration changes required to

● Run console in default mode

○ Run console in FIPS 140-2 mode

8 See the *ArcSight ESM Installation and Configuration Guide, v4.5 SP1* 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 SP1, 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: 04/20/09
Keywords: upgrade, database, manager, web

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

This document is ArcSight Confidential.

This technical note contains confidential information proprietary to ArcSight, Inc. Any party accepting this document agrees to hold its contents confidential, except for the purposes for which it was intended.