Upgrading ArcSight™ Express to v5.0 Patch 1

Document Status

This technical note describes the steps required to upgrade the software components on ArcSight Express from v4.5 SP2 Patch 2 or v4.5 SP3 to v5.0 Patch 1.

- If you are upgrading from an older version of ESM, you are required to upgrade to v4.5 SP2 Patch 2 or v4.5 SP3 before upgrading to v5.0 Patch 1.
- If you are on v4.5 SP2, make sure that you have the v4.5 SP2 Patch 2 installed before upgrading to v5.0 Patch 1.
- You will not be able to do two consecutive upgrades on the same day. For example, upgrading from v4.5 SP2 to v4.5 SP3, then upgrading to v5.0 Patch 1 cannot be done on the same day.

  After doing one upgrade, wait until the execution of the next scheduled Partition Manager job before doing the next upgrade. This allows Partition Manager to create a new partition which allows the system to be recognized as upgraded to an intermediate version. Execution of the Partition Manager scheduled job can be ensured by letting the Manager from the first upgrade run for a day (24 hours). Do the next upgrade after a day.
- Although the upgrade program does not prevent you from doing so, upgrading directly from v4.5 SP1 Patch 2 to v5.0 Patch 1 is not supported. If you are on v4.5 SP1 Patch 2 and would like to upgrade to v5.0 Patch 1, make sure you first upgrade to v4.5 SP2 Patch 2 before upgrading to v5.0 Patch 1.

Summary

This document covers the following topics:

Upgrading to v5.0 Patch 1

Verify that you have enough space (approximately 2 GB) available before you begin to install the patch.

To upgrade the components on your ArcSight Express Appliance:

1 **Important**: Obtain and note the build number on your ArcSight Express Appliance and make a note of it. In future if you need to contact ArcSight Customer Support or rollback this upgrade, 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:

   For v4.5 SP2 Patch 2:

   ```
   arcsight-express-manager-4.5-2.M6100
   ```

   then you are on v4.5 SP2 Patch 2 version of ArcSight Express. You will need to follow the upgrade path outlined in the caution on page 1 before proceeding any further.

   For v4.5 SP3:

   ```
   arcsight-express-manager-4.5-3.M6126
   ```

   then you are on v4.5 SP3 version of ArcSight Express. You will need to follow the upgrade path outlined in the caution on page 1 before proceeding any further.

2 Download the self-extracting upgrade file, `aeupdate-5.0.0.xxxx.1.pl` 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-5.0.0.xxxx.1.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:

   a Open a browser and go to the ArcSight Download Center.

   b Click 'Estimated Times and Details' link in the box from which you downloaded your executable file.

   c In the Download Details window, verify the MD5 Signature.

6 We recommend that you copy the following file to a secure location before installing the patch.

/opt/arcsight/db.preUpgradeBackup/arcsight.dmp

Any previous upgrade would have created an arcsight.dmp file (containing your base ESM installation) in the /opt/arcsight/db.preUpgradeBackup directory. If, for any reason, you have to roll back to your previous installation after or during an upgrade, ArcSight recommends that you first copy the arcsight.dmp file to a secure location. This allows you to restore your original content, if needed.

The arcsight.dmp file is overwritten with all subsequent upgrades.

7 Run the self-extracting upgrade file:

```
perl aeupdate-5.0.0.xxxx.1.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

If you do multiple upgrades, the preUpgradeBackup files get overwritten each time you do an upgrade. For example, if you are on v4.5 SP2 and upgrade to v4.5 SP3, backup files get created for the v4.5 SP2 installation. But if you further upgrade from v4.5 SP3 to v5.0 Patch 1, the v4.5 SP2backup files get overwritten with the v4.5 SP3 backup files and you lose the backup files for v4.5 SP2. Consequently, you will not be able to rollback to v4.5 SP2 version because you would have lost its backup files.

- The aeupdate-5.0.0.xxxx.1.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/logs/dbcheck 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/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.
- Make sure to copy any Case customizations from the *.preUpgradeBackup folders that you may have made to the Manager and Web's <ARCSIGHT_HOME>\i18n\common\label_strings.properties and <ARCSIGHT_HOME>\i18n\common\resource_strings.properties files

from the backup of your previous installation. When you install the patch, configuration files are not merged from your previous installation.

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:

```
arcsight-3ware-cli-x.xx.xx.xxxraidx-x
arcsight-connector-5.0.2.xxxx.x-x
arcsight-deltarpm-x.x-x
arcsight-express-db-5.0-Mxxxx
arcsight-express-manager-5.0-Mxxxx
arcsight-express-web-5.0-Mxxxx
arcsight-logos-x.x-x
arcsight-megaraid-cli-x.xx.xx-x
arcsight-oracle-10.2.0.4-Mxxxx.0
arcsight-oracle-cpuxxxxxx-xxxxx.xxxxxxx.x-Mxxxx.x
arcsight-oracle-cpuxxxxxx-xxxxx.xxxxxxx.x-Mxxxx.x
arcsight-oracle-cpuxxxxxx-xxxxx.xxxxxxx.x-Mxxxx.x
arcsight-platform-setup-x.x-xxxxxxxx_xxxx
arcsight-smartmontools-x.xx-x
```

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 where the component upgrade halted.

You have upgraded to ArcSight Express v5.0 Patch 1.

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.

Handling Upgrade Failures

The ArcSight Express upgrade involves upgrading the event schema to v5.0. Your upgrade process could fail either before the event schema upgrade takes place or it could happen either during or after the event schema upgrade has completed. If your upgrade fails before the event schema upgrade, then ArcSight Customer Support can help you roll back to the previous version of ESM that was on your machine before you started the upgrade. If the upgrade fails after the event schema has been upgraded, you will not be able to roll back to the previous version. Therefore, if you run into issues when upgrading, regardless

of when the upgrade failed, ArcSight recommends that you contact ArcSight Customer Support to help you decide on the next course of action. File an ArcSight Customer Support ticket and provide the installation logs.

Upgrading the Console

To upgrade the Console to v5.0 Patch 1, you must first upgrade the Console to v5.0 GA, then apply the v5.0 GA Patch 1.

Upgrading the Console to v5.0 GA

Your 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 v5.0 GA 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/SP3 that is different from where the existing Console is installed.

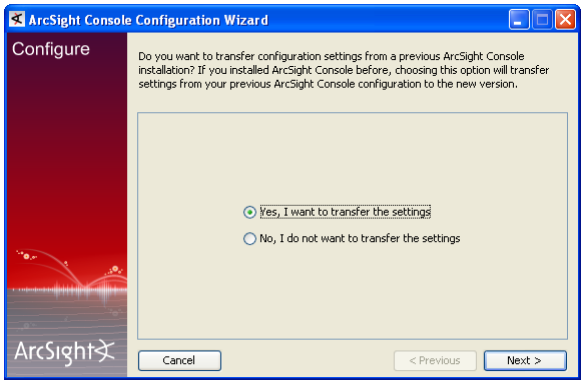
Do NOT install v5.0 GA Console in the same location as the existing Console.

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.

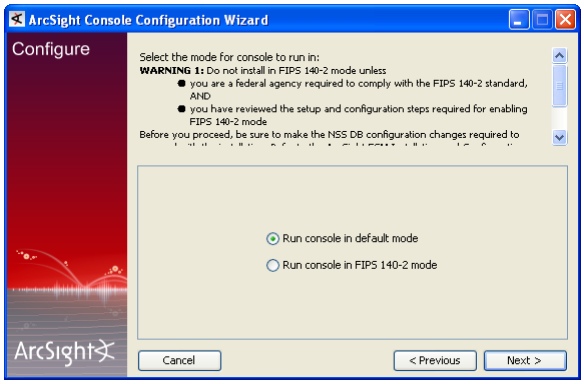


6 You will be prompted to enter the location of your previous Console installation:

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* 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 v5.0.

10 After you have upgraded a Console to v5.0 Patch 1, if no event viewers appear initially in the Console, select the `All Active Channels/ArcSight System/Core/Live` channel to view real-time events.

Applying the v5.0 Patch 1

Refer to the *ArcSight ESM Release Notes* for instructions on how to apply v5.0 Patch 1.

Last Updated: 10/20/10
Keywords: upgrade, database, manager, web