Table of Contents

Upgrade RiskVision Server

RiskVision continually makes improvements to its RiskVision Server to enhance the user experience for its customers. To upgrade your setup to a newer version that is within the existing version of your RiskVision Server, RiskVision provides the following two types of software releases:

- Hot fix
- Service pack

Hot Fix

RiskVision considers hot fixes to be upgrades. A hot fix typically consists of one or more bug fixes targeted for specific customers, although some hot fixes are recommended for all customers. Installing a hot fix will upgrade your RiskVision Server to a higher version within the same major release.

Service Pack

A service pack is an enhancement of the RiskVision system for all users. These are released when new features are created, major changes in features are made, or issues from prior versions have been fixed. When installing a service pack on your RiskVision Server, perform the steps specified in the process map that suits your deployment scenario.

Minor Version Upgrade

The Minor Version Upgrade installer is part of the installation/upgrade packages and allows users to perform minor upgrades to required the third-party software. See the Minor Version Upgrade Installer section more information and a list of prerequisites.

Upgrade System Requirements

The following components must be installed to use RiskVision:

1. RiskVision Server:
    - Apache Web Server
    - Tomcat Application Server
    - MySQL or Oracle database

> If the Apache Web Server, Apache Tomcat, MySQL, and/or Java services are already installed on your system, but require a version upgrade, you may be able to use the Minor Version Upgrade installer to perform these upgrades. See the Minor Version Upgrade Installersection for more information and a list of prerequisites.

2. RiskVisionReport Server (JasperReports Server)

System Requirements

The following hardware requirements represent the **minimum** system requirements to install Resolver RiskVision™ V. 9.6. These specifications are for planning purposes only. To learn about the recommended hardware and software for your environment, contact Resolver Support.

Hardware	Minimum
Total number of CPU cores	8
Memory	16 GB
Disk Space	At least 100 GB of free disk space

> Resolver recommends increasing the RAM of the National Vulnerability Database Connector by at least 500 MB to accomodate the CPE Match Feed from RiskVision version 9.3 and higher.

Supported Third-Party Software

Product	Version
Operating System	Microsoft Windows Server® 2012 R2 Standard x64, Windows Server® 2016
Amazon Coretto (JDK)	1.8.0_275
Apache Tomcat	8.5.61
Apache Web Server	2.4.46
Apache OpenOffice	4.1.7
Jasper Reports Server	7.2
MySQL	5.7.32
Oracle	12.2.0.1
Web Browser	Microsoft Internet Explorer® 11, Microsoft Edge, Mozilla Firefox®, Google Chrome®
Adobe® Flash browser plug-in	Adobe® Flash Player, version 11 (optional)
Microsoft Visual C++	2013 x64 Redistributable - 12.0.30501, 2008 x64 Redistributable - 9.0.30729.6161 (Optional- to run Apache open office), C++ 2008 x86 Redistributable - 9.0.30729.6161, 2010 x86 Redistributable - 10.0.40219
Open SSL	1.0.2r

> Users who wish to use Tomcat version 8.5.35 or above must update their RiskVision software to version 9.3 or higher.

JasperReports Server 7.2 comes with the following technologies:

Product	Version
PostgreSQL	10.5
Apache Tomcat	8.5.34

Oracle JDK 8	1.8.0_201

Upgrade Prerequisites

Make sure all directories and folders are closed during the upgrade process.

If you are performing an in-place upgrade, open the `config/agiliance.properties` file and comment out the `com.agiliance.esapi.allowed.file.extensions` property. To comment it out placing a # character at the beginning of the line where the property exists and save it. After the upgrade is complete, you can uncomment the property.

RiskVision does not support Internet Explorer version 8 or Internet Explorer Compatibility mode, which causes the browser to run as if it was a version 8 browser.

If you are on RiskVision 7.5, 8.0, and 8.5x or 9.0 version, then you can directly upgrade to RiskVision 9.2. From there, users can upgrade to 9.3.

The below table shows the recommended upgrade paths depending on the current version of RiskVision:

FROM VERSION	TO VERSION
7.5	9.1 or 9.2 (recommended)
8.0	9.1 or 9.2 (recommended)
8.5 (all variations)	9.1 or 9.2 (recommended)
9.0	9.1 or 9.2 (recommended)
9.1	9.2 or 9.3
9.2	9.3 or 9.3.5
9.3	9.3.5 or 9.4
9.3.5	9.4 or 9.5
9.4	9.5 or 9.6
9.5	9.6
9.6	-

Important: If you are upgrading from the 7.5 release, verify in the **agiliance.properties** file that the `jasper.use.secure.connection=FALSE` property is not set. If it is, delete the property from the **agiliance.properties** file.

For more information on the UAC setting, see Configure the UAC Setting.

Identify the Appropriate Setup Wizard

To determine the appropriate wizard to use for upgrading your RiskVision Server, see Upgrade Process Map for Single Tier RiskVision Setup and Upgrade Process Map for N-tier RiskVision Setup to find the correct setup for your system. Before upgrading, make sure you have all the required permissions to edit the Server (%AGILIANCE_HOME%) folder. Perform the necessary steps shown in the version information.

If the Apache Web Server, Apache Tomcat, MySQL, and/or Java services are already installed on your system, but require a version upgrade, you may be able to use the Minor Version Upgrade installer to perform these upgrades. See the Minor Version Upgrade Installer section for more information and a list of prerequisites.

For further questions, contact Resolver Support.

Upgrade Procedure for Versions 9.0 & Later

The following describes the difference between the RiskVision Server Upgrade Setup installer in versions 9.0 and above, as compared to previous versions.

Change	Description
Upgrade Procedure	The following changes are specific to the Resolver RiskVision Server Upgrade Setup installer and upgrade procedure: • Before beginning the upgrade setup, stop all services, including Apache, Tomcat, and Job Manager, except the MySQL and JasperReport related services. • The look and feel of the upgrade installer is different.
Services	Services have been renamed as: • RiskVision Job Manager • RiskVision Apache • RiskVision Tomcat • RiskVision MySQL

Upgrade Process Map

The RiskVision Server Upgrade Setup provides a step-by-step process to install the upgrade, such as hotfixes and service packs, in the existing version of RiskVision Server. This section includes a map that will help you install an upgraded version of RiskVision Server.

Note: For the MySQL database upgrade, RiskVision strongly recommends that the Database Statistics Updater job be run on a weekly basis and during a period of low system activity, such as on the weekend.

For the MySQL database, upgrade the database server first to get the latest database schema changes, and then upgrade the application server and web server sequentially.

For the Oracle database, upgrade the application server first to get the latest database schema changes, and then upgrade the web server and database server sequentially.

Upgrade Process Map for a Single-Tier Setup

The RiskVision Server Upgrade Setup wizard is used to upgrade your RiskVision environment. Both MySQL and Oracle databases are supported in all RiskVision applications.

The following scenario demonstrates a single-tier RiskVision setup.

Scenario for single-tier:

Host	Apache Web Server, Tomcat Application Server, RiskVision Job Manager, Database (MySQL or Oracle), and RiskVision Report Server.

Upgrade steps for single-tier:

When	Map
7.0.x, 7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Download the new files required for upgrade, see Downloading New Files. Step 2: Back up the database. For a MySQL database, see Backing up the MySQL Database. If you're using an Oracle database, ask your database administrator to perform the back up. Step 3: Backing up the RiskVision Configuration Step 4: Preparing for an Upgrade Step 5: Running the Upgrade Installer for One Server Step 6: Customization Upgrade Note Step 7: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database Setting up the Oracle Database - perform this step if you are using an Oracle database

Upgrade Process Map for an N-Tier Setup

In an n-tier setup, RiskVision is distributed to multiple servers. To ensure a successful upgrade, select the most appropriate scenario in the the "*Deployment Scenarios*" section, then follow the instructions specific to that scenario.

Deployment Scenarios

Scenario for two-tier: Case A

Host A	Host B
Apache Web Server	RiskVision Report Server
RiskVision Tomcat Application Server	
Database (MySQL or Oracle)	

Upgrade steps for two-tier: Case A

When	Map
7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Download the new files required for upgrade. See Downloading New Files. Step 2: Oracle Database Upgrade. Ignore this step if you are using a MySQL database. Step 3: Back up the database. For MySQL, see Backing up the MySQL Database. If you're using an Oracle database, ask your database administrator to perform the back up. Step 4: Backing up the RiskVision Configuration. Step 5: Preparing for an Upgrade. Step 6: On Host A, run the RiskVision Upgrade Installer by selecting the **Web Server (Apache HTTP Server), Application Server (Apache Tomcat)** and **Database Server (MySQL or Oracle Database)** components. Step 7: On Host B, run the RiskVision Upgrade Installer, by selecting the **Report Server (TIBCO Jasper-Reports Server)** component. Step 8: Customization Upgrade Note. Step 9: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database. Setting up the Oracle Database - perform this step if you are using an Oracle database.

Scenario for two-tier: Case B

Host A	Host B
Apache Web Server	Database (MySQL or Oracle)
RiskVision Tomcat Application Server	
RiskVision Report Server	

Upgrade steps for two-tier: Case B

When	Map

When	Map
7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Downloading New Files. Step 2: Oracle Database Upgrade. Ignore this step if you are using a MySQL database. Step 3: Back up the database. For MySQL, see Backing up the MySQL Database. If you're using an Oracle database, ask your database administrator to perform the back up. Step 4: Backing up the RiskVision Configuration. Step 5: Preparing for an Upgrade. Step 6: On Host A, run the RiskVision Upgrade Installer by selecting the **Web Server (Apache HTTP Server)**, **Application Server (Apache Tomcat)** and **Report Server (TIBCO JasperReports Server)** components. Step 7: On Host B, run the RiskVision Upgrade Installer by selecting and **Database Server (MySQL or Oracle Database)** components. Step 8: Customization Upgrade Note. Step 9: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database. Setting up the Oracle Database - perform this step if you are using an Oracle database.

Scenario for three-tier: Case A

Host A	Host B	Host C
Apache Web Server RiskVision Tomcat Application Server	Database (MySQL or Oracle)	RiskVision Report Server

Upgrade steps for three-tier: Case A

When	Map
7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Downloading New Files. Step 2: Oracle Database Upgrade. Ignore this step if you are using a MySQL Database. Step 3: Back up the database. For a MySQL database, see Backing up the MySQL Database. If you are using an Oracle database, ask your database administrator to perform the back up. Step 4: Backing up the RiskVision Configuration. Step 5: Preparing for an Upgrade. Step 6: On Host A, run the RiskVision Upgrade Installer by selecting the **Web Server (Apache HTTP Server)**, and **Application Server (Apache Tomcat)**. Step 7: On Host B, run the RiskVision Upgrade Installer by selecting the **Database Server (MySQL or Oracle Database)** component. Step 8: On Host C, run the RiskVision Upgrade Installer by selecting the **Report Server (TIBCO Jasper-Reports Server)** component. Step 9: Customization Upgrade Note.

When	Map
	Step 10: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database. Setting up the Oracle Database - perform this step if you are using an Oracle database.

Scenario for three-tier: Case B

Host A	Host B	Host C
Apache Web Server	RiskVision Tomcat Application Server	Database (MySQL or Oracle) RiskVision Report Server

Upgrade steps for three-tier: Case B

When	Map
7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Downloading New Files. Step 2: Oracle Database Upgrade. Ignore this step if you are using a MySQL database. Step 3: Back up the database. For a MySQL database, see Backing up the MySQL Database. Ifyou are using an Oracle database, ask your database administrator to perform the back up. Step 4: Backing up the RiskVision Configuration. Step 5: Preparing for an Upgrade. Step 6: On Host B, run the RiskVision Upgrade Installer by selecting the **Application Server (Apache Tomcat)** component. Step 7: On Host A, run the RiskVision Upgrade Installer by selecting the **Web Server (Apache HTTP Server)** component. Step 8: Run the RiskVision installer, by selecting the **Report Server (TIBCO JasperReports Server)** and **Database Server (MySQL or Oracle)** component, on Host C. Step 9: Customization Upgrade Note. Step 10: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database. Setting up the Oracle Database - perform this step if you are using an Oracle database.

Scenario for four-tier:

Host A	Host B	Host C	Host D
Apache Web Server	RiskVision Tomcat Application Server	Database (MySQL or Oracle)	RiskVision Report Server

Upgrade steps for four-tier:

When	Map

When	Map
7.5.x, 8.0, 8.5x, 9.0 to 9.1	Step 1: Downloading New Files. Step 2: Oracle Database Upgrade. Ignore this step if you are using a MySQL database. Step 3: Back up the database. For a MySQL database, see Backing up the MySQL Database. Ifyou are using an Oracle database, ask your database administrator to perform the back up. Step 4: Backing up the RiskVision Configuration. Step 5: Preparing for an Upgrade. Step 6: On Host B, run the RiskVision Upgrade Installer by selecting the **Application Server (Apache Tomcat)** component. Step 7: On Host A, run the RiskVision Upgrade Installer by selecting the **Web Server (Apache HTTP Server)** component. Step 8: On Host C, run the RiskVision Upgrade Installer by selecting the Database Server (MySQL or Oracle Database) component. Step 9: On Host D, run the RiskVision Upgrade Installer by selecting the **Report Server (TIBCO Jasper- Reports Server)** component. Step 10: Customization Upgrade Note. Step 11: Replacing and Reverting the MySQL Configuration - perform this step if you are using a MySQL database. Setting up the Oracle Database - perform this step if you are using an Oracle database.

Upgrade Files

Obtain the following files from Resolver Support and place the new files, with the exception of the license and readme files, in a temporary directory, such as or `C:\AglInstall` `D:\AglInstall`.

> The **mysql-5.7.32-winx64.zip** and **mysql-connector-java-5.1.39.zip** files cannot be obtained from Resolver Support and must be obtained directly from MySQL.

Files required for all RiskVision Server upgrade scenarios:

File	MySQL	Oracle
riskvision.license	✓	✓
RiskVisionApplicationServerUpgrade.exe	✓	✓
jce_policy-8.zip	✓	✓
TIB_js-jrs_6.4.3_windows_x86_64.exe	✓	✓
mysql-5.7.32-winx64.zip	✓	✗
mysql-connector-java-5.1.39.zip	✓	✗
Riskvision-part1.zip	✓	✓
Riskvision-part2.zip	✓	✓
Riskvision-part3.zip	✓	✓
MinorVersionUpgradeInstaller.exe	✓	✓

The RiskVision Report Server can only be installed on a 64-bit version of the Windows operating system.

You will also need to download the jce_policy-8.zip file from Oracle.

Download MySQL Artifacts

Download the following files if your MySQL database server version is earlier than 5.7.32 and your MySQL connector version is earlier than 5.1.39.

Filename	URL
mysql-5.7.32-winx64.zip	https://downloads.mysql.com/archives/get/p/23/file/mysql-5.7.32-winx64.zip
mysql-connector-java-5.1.39.zip	https://downloads.mysql.com/archives/get/p/3/file/mysql-connector-java-5.1.39.zip

Oracle Database Upgrade

Your database must be Oracle version 12.2.0.1.

After completing the upgrade, ensure that the upgrade has not impact your database and you are able to use the current version of the RiskVision Server without any issues.

Back up the Database and RiskVision Configuration

Back up the following areas before beginning the upgrade process of the RiskVision applications.
If you are using an Oracle database, ask your database administrator to back up the data, and then see Backing up the RiskVision Configuration.

The Oracle database back up can be performed only with the Schema Owner account.

If you are using a MySQL database, you must perform the following steps.

- Back up the MySQL database
- Backing up the RiskVision Configuration
- Disable SSL encryption for MySQL

To exclude subfolders within the data folder from your backups use the property com.agiliance.admin.backup.ServerBackupManager.excludeDirectories where the subfolders are separated by a comma, such as "attachments", "reports" and "dashboards".

For example, if you want to exclude all 3 folders, you should use the following property value:
`com.agiliance.admin.backup.ServerBackupManager.excludeDirectories=attachments,reports,dashboards`

Back-up Your MySQL Database

Before backing up your MySQL database, make sure you have stopped all RiskVision services.

To back up your MySQL database:

1. Log in as the Administrator.
2. Open the command window in the RiskVision database server host.
3. Enter the following line in the command window (ensure that the information is all in one line):

   ```
   %AGILIANCE_HOME%\MySql\bin\mysqldump -uroot -p --databases agiliance --routines --triggers --add-drop-database --single-transaction --max_allowed_packet=32MB > snap.sql
   ```

   The above command will back up your data to the `.sql` file. Copy this file to the back-up directory.

Back up the RiskVision Configuration

To back up the RiskVision configuration, create a backup folder outside the folder `%AGILIANCE_HOME%` and copy the following files and directories to the backup directory.

`%AGILIANCE_HOME%\install`

`%AGILIANCE_HOME%\apache2`

`%AGILIANCE_HOME%\backup`

`%AGILIANCE_HOME%\config`

`%AGILIANCE_HOME%\data`

`%AGILIANCE_HOME%\java`

`%AGILIANCE_HOME%\Tomcat`

`%AGILIANCE_HOME%\MySql`

For the Oracle database, it is not required to back up the Schema User account, because the Schema User account can be reinitialized by following the steps mentioned in the Setting up the Oracle Database.

Using the above files, back up each host in the N-Tier RiskVision installation. This includes servers with Apache, Tomcat, and the database.

When performing an upgrade, the database dump and data files must be available. The data files reside in RiskVision's data folder, which by default resides in the folder `%AGILIANCE_HOME%\data`. If some of the data subfolders have been relocated using the file `agiliance.properties` in the config folder, make sure that these folders are available and accessible.

Disable SSL Encryption for your MySQL Database

This section is applicable only for the MySQL database if you have enabled SSL encryption for the MySQL database in version 6.5 SP1 and above. Unless you disable SSL encryption settings, the RiskVision Upgrade Setup will not upgrade to a newer version of RiskVision.

To disable SSL encryption:

1. Check to see if the my.ini file in the %AGILIANCE_HOME%\MySQL\config directory is backed up. If not, see Backing up the RiskVision Server Configuration for more details.
2. Go to the %AGILIANCE_HOME%\MySQL\config directory. Open the my.ini file by using a text editor, locate the Client and Server sections in the my.ini file, and comment the lines shown below in the respective sections.
   - Client Section
     - `ssl-ca="~/ca-cert.pem"`
     - `ssl-cert="~/client-cert.pem"`
     - `ssl-key="~/client-key.pem"`
     - `ssl-cipher=DHE-RSA-AES256-SHA`
   - Server Section
     - `ssl-ca="~/ca-cert.pem"`
     - `ssl-cert="~/server-cert.pem"`
     - `ssl-key="~/server-key.pem"`
     - `ssl-cipher=DHE-RSA-AES256-SHA`

   Where, "~" denotes certificate's directory.
3. Go to the directory `%AGILIANCE_HOME%\config`. Open the agiliance.properties file by using a text editor, comment the property `database.mysql.useSSL=true` and specify the database hostname in the file.
4. Connect to the MySQL database and run the following commands to disable the SSL encryption:

   ```
   GRANT USAGE ON agiliance.* TO 'agiliance'@' REQUIRE NONE;

   GRANT USAGE ON agiliance.* TO 'reportuser'@' REQUIRE NONE;

   FLUSH PRIVILEGES;
   ```

5. Restart the RiskVision Tomcat and RiskVision MySQL services to apply the latest changes.

Prepare for an Upgrade

On the host server, close all of the following:

- Services.msc (the Windows Services application);
- Web browsers (including RiskVision);
- MySQL sessions;
- Applications accessing log files; and
- Connectors and other utilities.

Before the upgrade process, stop all services except the MySQL service, then manually select the components in the upgrade installer.

If you have an Oracle database, uncomment the Schema Owner and comment the Schema User in the `agiliance.properties` file.

Single-Tier Server Upgrade

This section provides instructions for upgrading a single-server RiskVision installation where Tomcat Application Server, Apache Web Server, Database and Report Server are installed on the same server. The RiskVision Server Upgrade Set-up installer only needs to be run once on the host server. This section also provides the upgrade instructions specific to this single-tier installations.

To upgrade a single-server installation:

1. Copy the download files to the host server. See Downloading New Files for more information.
2. Ensure that you have local administrator privileges on Windows Server 2008 or Windows Server 2012, User Account Control (UAC) is disabled, and all RiskVision services, such as MySQL, are running.
3. Click **Next**.
4. Double-click the RiskVisionApplicationServerUpgrade.exe file to launch the **RiskVisionMulti-TierUpgradeInslater-InstallShield** wizard.
5. Click **Next**.
6. Click the **I accept the terms in the license agreement** radio button.
7. Click **Next**.
8. Check the **Web Server (Apache HTTP Server)**, **Application Server (Apache Tomcat)**, **Database Server (MySQL or Oracle Database)**, and **Report Server (TIBCO JasperReportServer)** checkboxes.
9. Click **Next**. If you select MySQL database, you will see the following window:

   Enter the root password of the MySQL database in the **Password** field and click **Validate**. Enter the default RiskVision user password in the **Password** field and click **Validate**.

   Click **Next** to open the **Report Server Details** wizard page.

10. Select the database type, either **MySQL** or **Oracle**.
    - **MySQL database**:
      a. Click the **Application Server IP Address** field and enter the IP address of the RiskVision Server in which the application server is running.
      b. Click the **Application Server Host Name** field and enter the hostname of the RiskVision Server in which the application server is running.
      c. Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **ReportUser Confirm Password** field. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
      d. Enter the hostname of the database in the **Database HostName** field.
      e. Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
      f. Enter the database port in the **Database Port** field.
      g. Enter the PostgreSQL admin password in the **PostgreSQL Admin Password** field. Enter the same password in the **Confirm PostgreSQL Admin Password** field.
    - **Oracle database**:
      a. Enter the IP address of the RiskVision Server in which the application server is running in the **Application Server IP Address** field.
      b. Enter the hostname of the RiskVision Server in which the application server is running in the **Application Server Host Name** field.
      c. Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **Confirm ReportUser Password** field. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
      d. Enter the hostname of the database in the **Database HostName** field.
      e. Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
      f. Enter the database port in the **Database Port** field.

g. Enter the Oracle Service name, in the **Oracle Service name** field.

h. Enter the PostgreSQL Admin password in the **PostgreSQL Admin Password** field. Enter the same password in the **Confirm PostgreSQL Admin Password** field.

11. Click **Next**.

12. Enter **localhost** as the hostname if the RiskVision is deployed on the server where you are currently running this upgrade installer.

13. If your server does not meet the system and hardware requirements, the **System Requirement** wizard page will open. Continuing without meeting the system requirements could adversely affect performance. Consult the Minimum Hardware Requirements. To continue click **Accept**.

14. Click **Install**.

15. Review the Release Notes, then check the **I confirm that I have read the above notes** checkbox. Click **Finish**.

At this point, the upgrade process is complete. Depending on the size of your data, the upgrade may take four to five hours, but this is only an estimate.

A log of the upgrade process is written to the temporary directory where the upgrade installer is triggered.

Two-Tier Server Upgrade

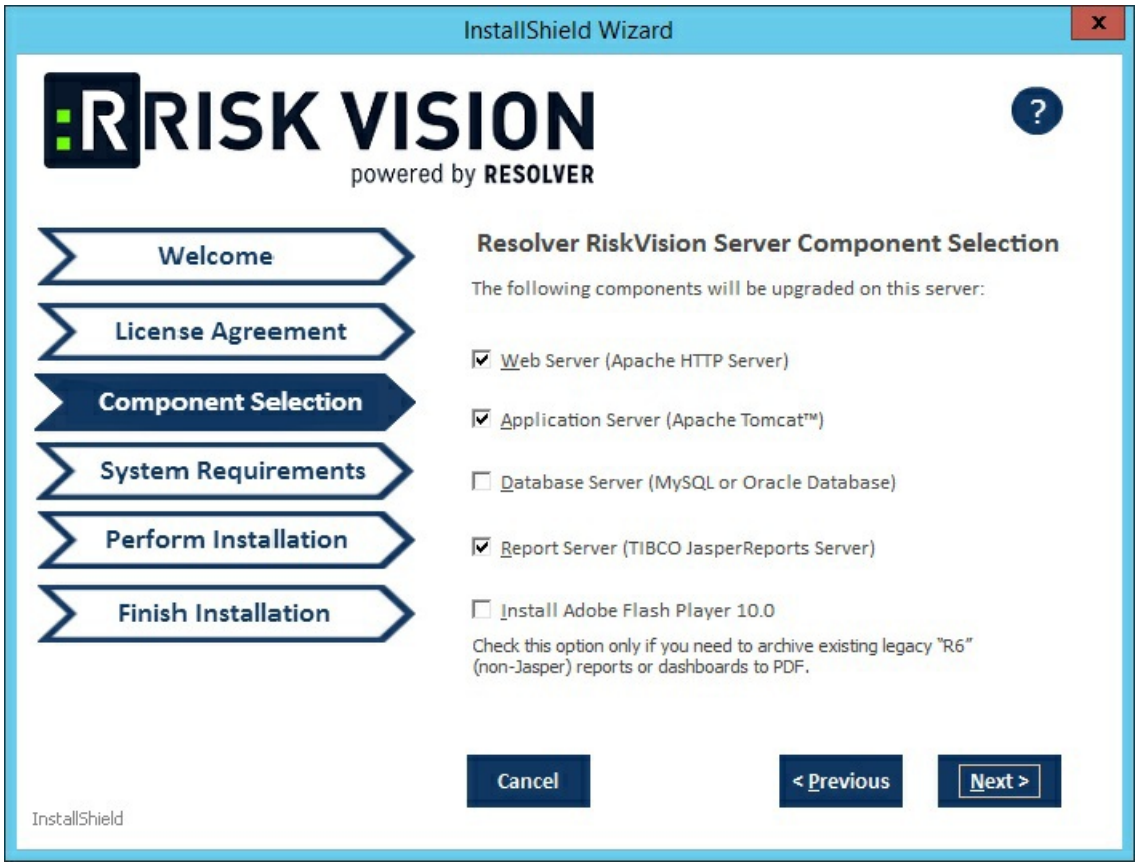
This section provides instructions for upgrading a two-tiered deployment where RiskVision Tomcat Application Server, Apache Web Server, and the Report Server are installed on one server and the database is installed on another. The RiskVision Upgrade Installer is run on the application server. This section also provides the upgrade instructions specific to a two-tiered installation.

To upgrade the deployment:

1. Copy the following files to the servers where the database server, Tomcat Application Server, Apache Web Server, and RiskVision Job Manager are installed.

File	MySQL	Oracle
riskvision.license	✓	✓
RiskVisionApplicationServerUpgrade.exe	✓	✓
jce_policy-8.zip	✓	✓
TIB_js-jrs_6.4.3_windows_x86_64.exe	✓	✓
mysql-5.7.22-winx64.zip	✓	✗
mysql-connector-java-5.1.39.zip	✓	✗
Riskvision-part1.zip	✓	✓
Riskvision-part2.zip	✓	✓
Riskvision-part3.zip	✓	✓

2. Run the upgrade installer on both servers, one after another. Double-click `RiskVisionApplicationServerUpgrade.exe`.
3. Click **Next**.
4. Check the **I accept the terms in the License Agreement** checkbox. Click **Next**.
5. Check the **Web Server (Apache HTTP Server)**, **Application Server (Apache Tomcat)**, and **Report Server (TIBCO JasperReport Server)** checkboxes.



6. Click **Next**.

7. If the MySQL database is selected the **Component Selection** page modifies and appears as shown below:

   Enter the root password of the MySQL database in the **Password** field and click the **Validate** button, to validate the entered password to connect to the MySQL database Enter the default RiskVision user password in the **Password** field and click the **Validate** button, to validate the entered password to connect to the MySQL database.

   Click **Next** to continue.

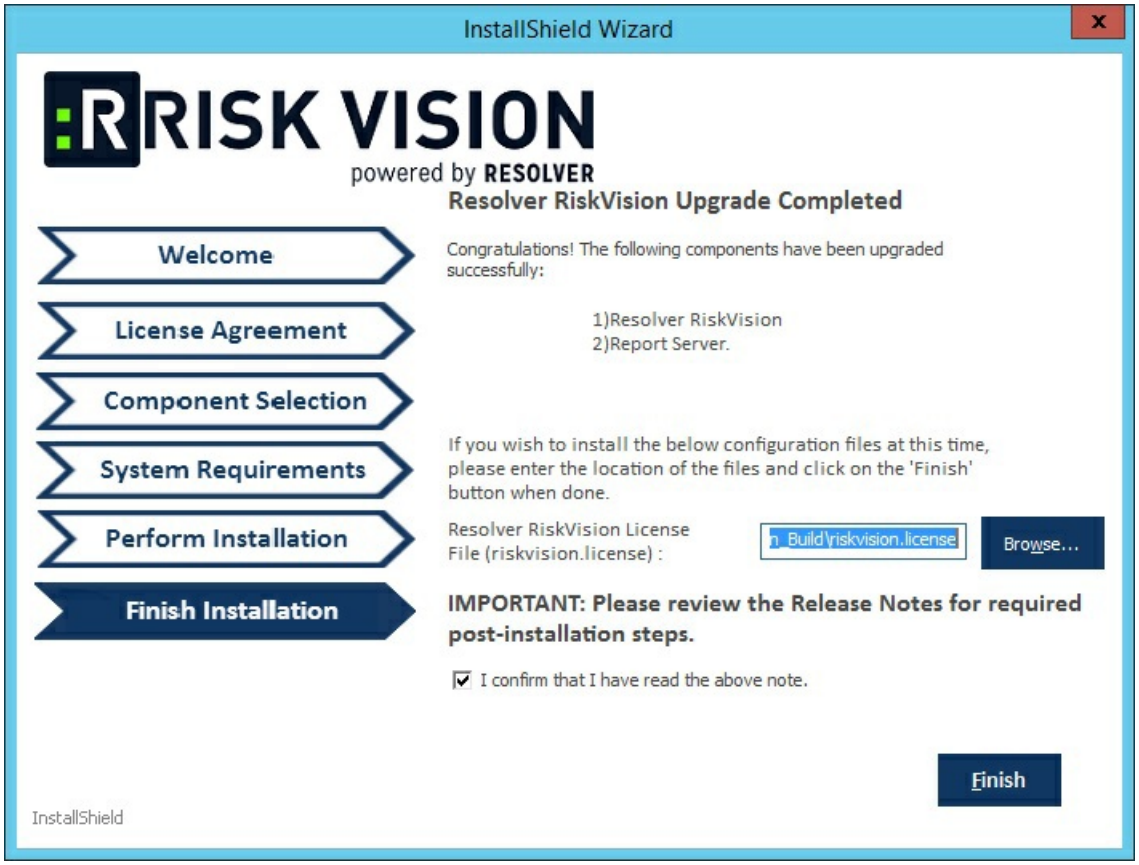
8. Select the database type, either **MySQL** or **Oracle**.

   - **MySQL database**:
     - Enter the IP address of the RiskVision Server in which the application server is running in the **Application Server IP Address** field.
     - Enter the hostname of the RiskVision Server in which the application server is running in the **Application Server Host Name** field.
     - Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **ReportUser Confirm Password** field. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
     - Enter the hostname of the database in the **Database HostName** field.
     - Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
     - Enter the database port in the **Database Port** field.
     - Enter the PostgreSQL admin password in the **PostgreSQL Admin Password** field.
     - Enter the same password in the **Confirm PostgreSQL Admin Password** field to ensure that the password entered is correct.
   - **Oracle database**:
     - Enter the IP address of the RiskVision Server in which the application server is running in the **Application Server IP Address**

field.

- Enter the hostname of the RiskVision Server in which the application server is running in the **Application Server Host Name** field.
- Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **ReportUser Confirm Password**. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
- Enter the hostname of the database in the **Database HostName** field.
- Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
- Enter the database port in the **Database Port** field.
- Enter the Oracle Service name, in the **Oracle Service name** field.
- Enter the PostgreSQL admin password in the **PostgreSQL Admin Password** field. Enter the same password in the **Confirm PostgreSQL Admin Password**.

9. If your server does not meet the system and hardware requirements, the **System Requirement** wizard page will open. Continuing without meeting the system requirements could adversely affect performance. Consult the Minimum Hardware Requirements. To continue click **Accept**.
10. Click **Install**.
11. Review the Release Notes, then check the **I confirm that I have read the above notes** checkbox.
12. Click **Finish**.



.

Three-Tier Server Upgrade

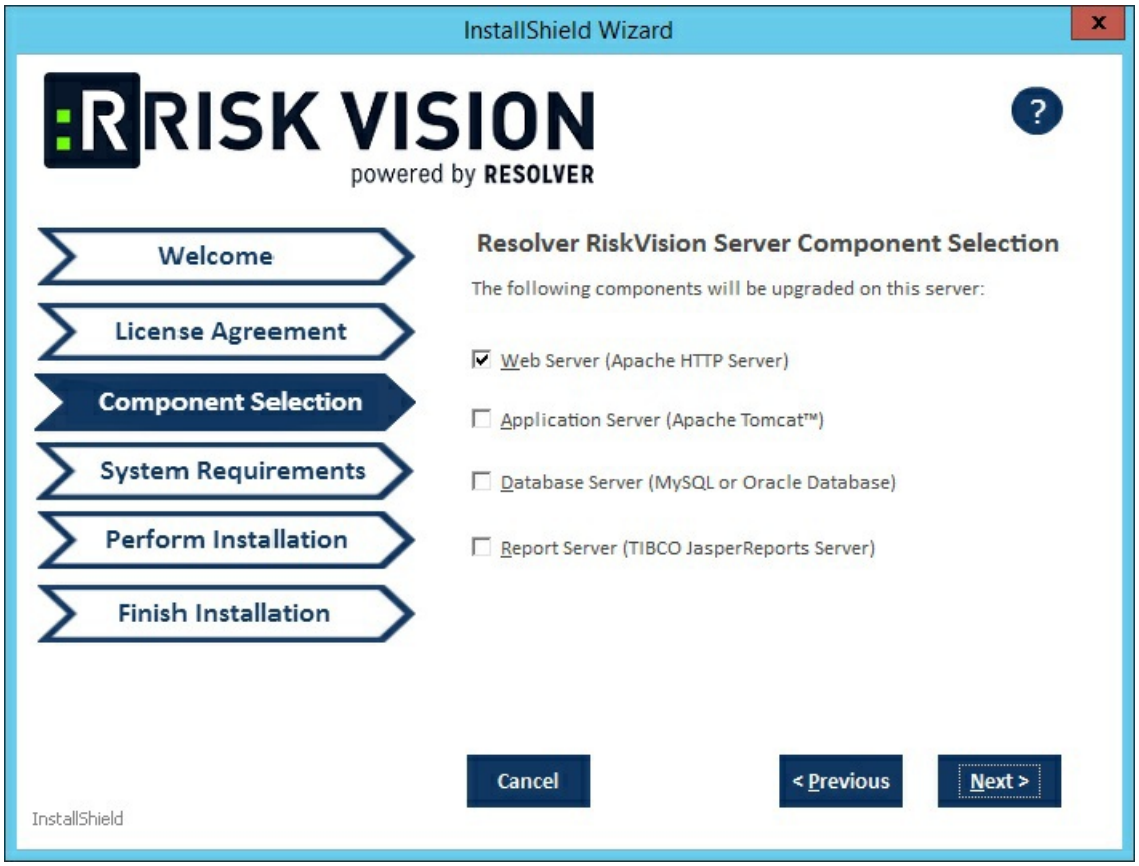
This section provides instructions to upgrade your deployment when the RiskVision Tomcat Application Server, Apache Web Server, and database are distributed on three servers. The upgrade process emphasizes the step(s) with specific options to select for each component when running the installer to upgrade each component. **The RiskVisionApplicationServerUpgrade.exe installer must be run three times, one time on each server.** Further, this section provides upgrade instructions specific to the three-tier: Case B and four-tier scenarios.

To upgrade the deployment:

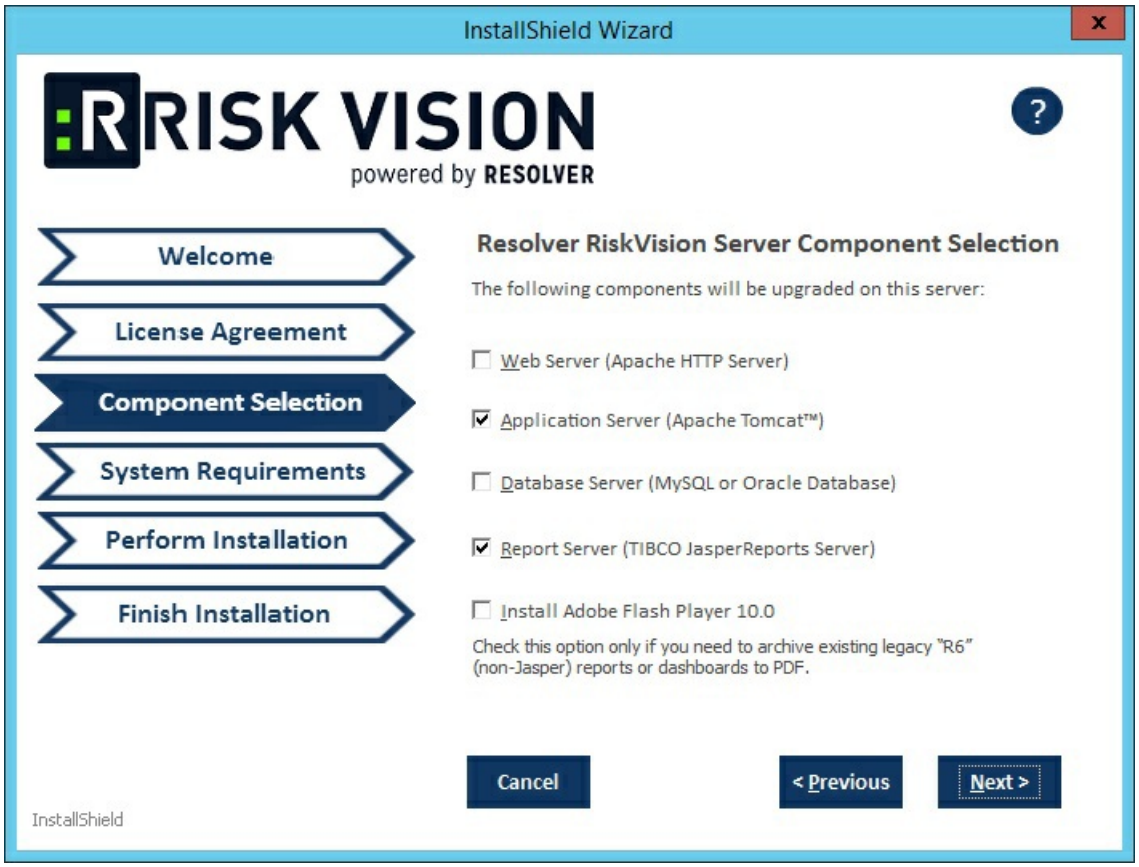
1. Copy the following files to the servers where database server, Apache Web Server, Tomcat Application Server and RiskVision Job Manager are installed.

File	MySQL	Oracle
riskvision.license	✓	✓
RiskVisionApplicationServerUpgrade.exe	✓	✓
jce_policy-8.zip	✓	✓
TIB_js-jrs_6.4.3_windows_x86_64.exe	✓	✓
mysql-5.7.24-winx64.zip	✓	✗
mysql-connector-java-5.1.39.zip	✓	✗
Riskvision-part1.zip	✓	✓
Riskvision-part2.zip	✓	✓
Riskvision-part3.zip	✓	✓

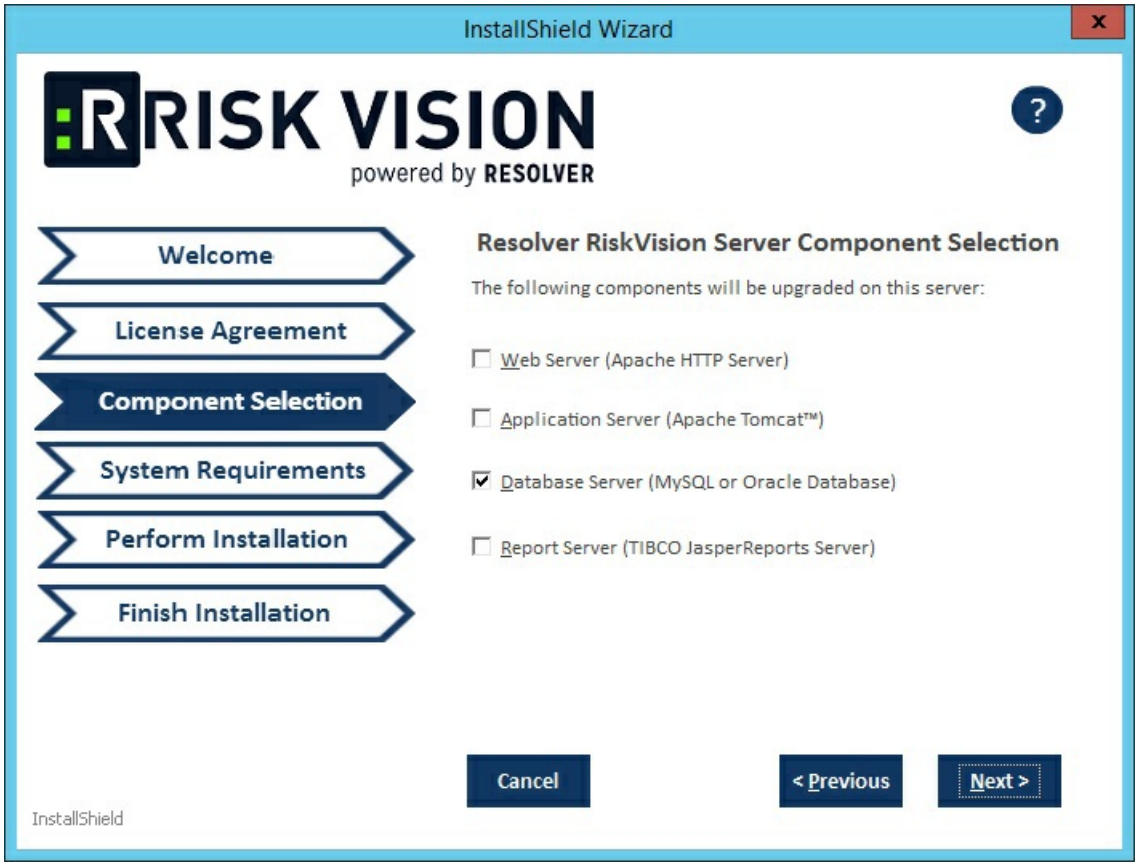
2. Run the upgrade installer on each server one after another. Double-click `RiskVisionApplicationServerUpgrade.exe`.
3. Click **Next**.
4. Check the **I accept the terms in the License Agreement** checkbox.
5. Click **Next**.
6. When running the upgrade installer on the web server system, check the **Web Server(Apache HTTP Server)** checkbox.



When running the upgrade installer on Tomcat application server system and Report server, check the**Application Server (Apache Tomcat)** and **Report Server (TIBCO JasperReport Server)** checkboxes.



When running the upgrade installer on the web server system, check the **Database Server(MySQL or Oracle Database)** checkbox.

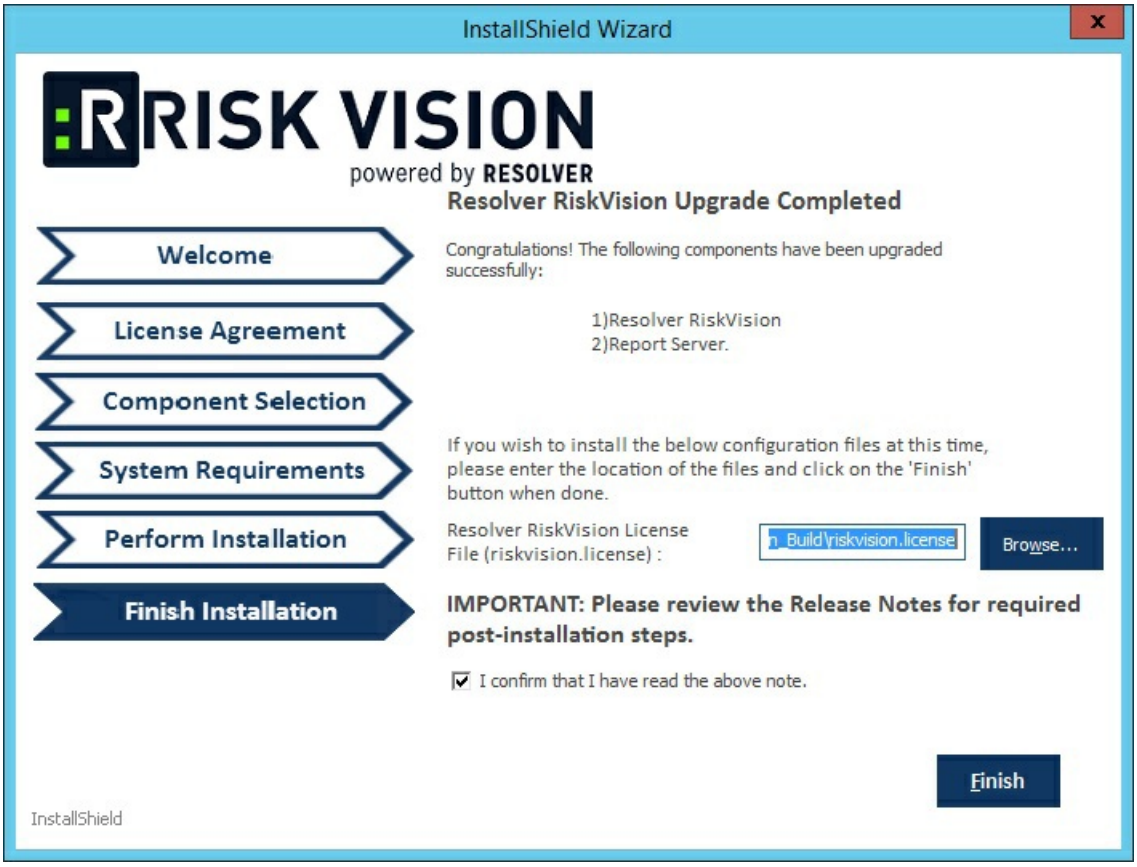


7. Click **Next**.
8. Select the database type, either **MySQL or Oracle**.
    - **MySQL database**:
        a. Click the **Application Server IP Address** field and enter the IP address of the RiskVision Server in which the application server is running.
        b. Click the **Application Server Host Name** field and enter the hostname of the RiskVision Server in which the application server is running.
        c. Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **ReportUser Confirm Password** field. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
        d. Enter the hostname of the database in the **Database HostName** field.
        e. Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
        f. Enter the database port in the **Database Port** field.
        g. Enter the PostgreSQL admin password in the **PostgreSQL Admin Password** field. Enter the same password in the **Confirm PostgreSQL Admin Password** field.
    - **Oracle database**:
        a. Enter the IP address of the RiskVision Server in which the application server is running in the **Application Server IP Address** field.
        b. Enter the hostname of the RiskVision Server in which the application server is running in the **Application Server Host Name** field.
        c. Enter the database reportuser password in the **ReportUser Password** field. Enter the same password in the **Confirm ReportUser Password** field. Memorize this password as you will need it when you set up the RiskVision Report Server, whether for a new installation or an upgrade.
        d. Enter the hostname of the database in the **Database HostName** field.
        e. Enter the fully qualified domain name of the RiskVision Report Server in the **Report Server HostName** field.
        f. Enter the database port in the **Database Port** field.
        g. Enter the Oracle Service name, in the **Oracle Service name** field.

h. Enter the PostgreSQL Admin password in the **PostgreSQL Admin Password** field. Enter the same password in the **Confirm PostgreSQL Admin Password** field.

9. Click **Next**.
10. If your server does not meet the system and hardware requirements, the **System Requirement** wizard page will open. Continuing without meeting the system requirements could adversely affect performance. Consult the Minimum Hardware Requirements. Click **Accept** to continue the installation or click **Abort** to cancel. If you click **Accept** followed by **Next**, you will be directed to the **Begin Installation** wizard page. If you click **Abort** followed by **Next**, you will be prompted to click **Finish** so that you can stop the installation.
11. Click **Install** to begin the installation.
12. Review the Release Notes, then check the **I confirm that I have read the above notes** checkbox.
13. Click **Finish**

At this point, the upgrade process is complete.



Upgrade RiskVision Connector Manager

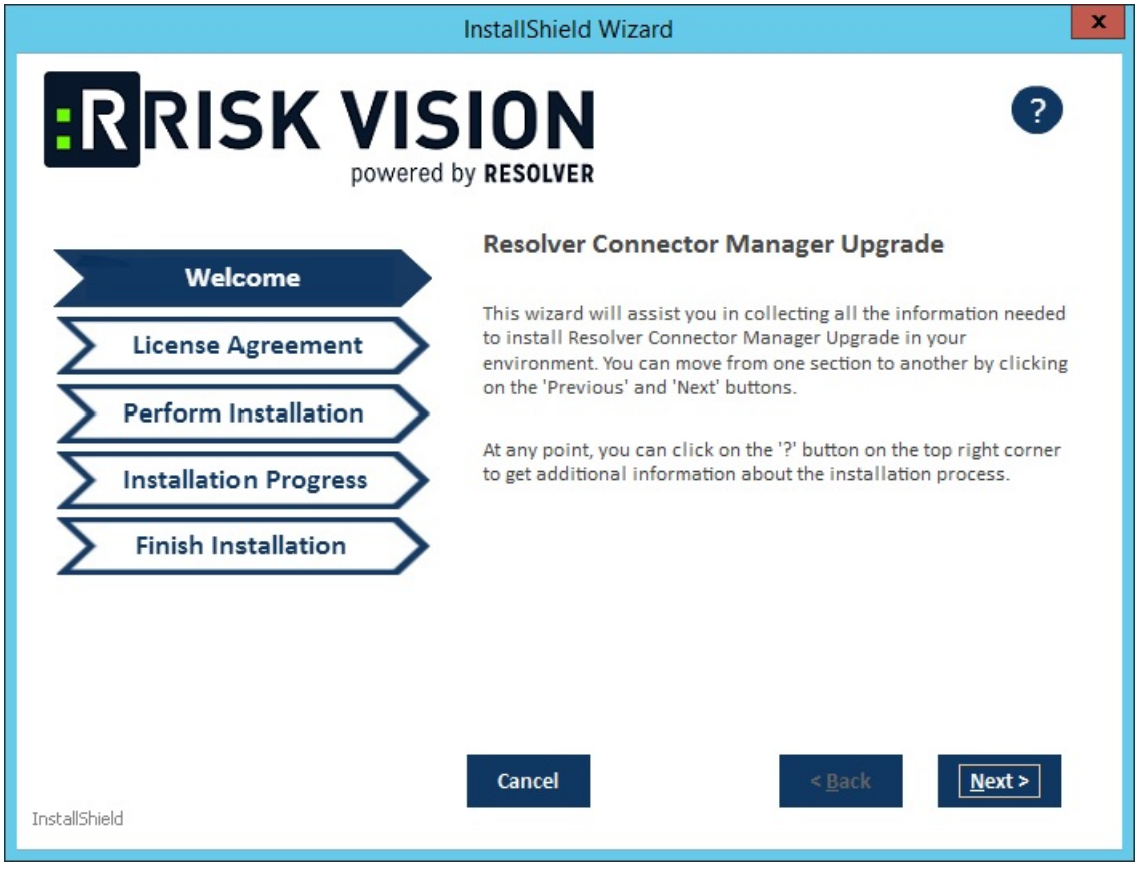
You can upgrade your RiskVision Connector Manager by obtaining the latest installer file from Resolver Support.

To upgrade RiskVision Connector Manager:

1. Copy the following files to the RiskVision Connector Manager server.

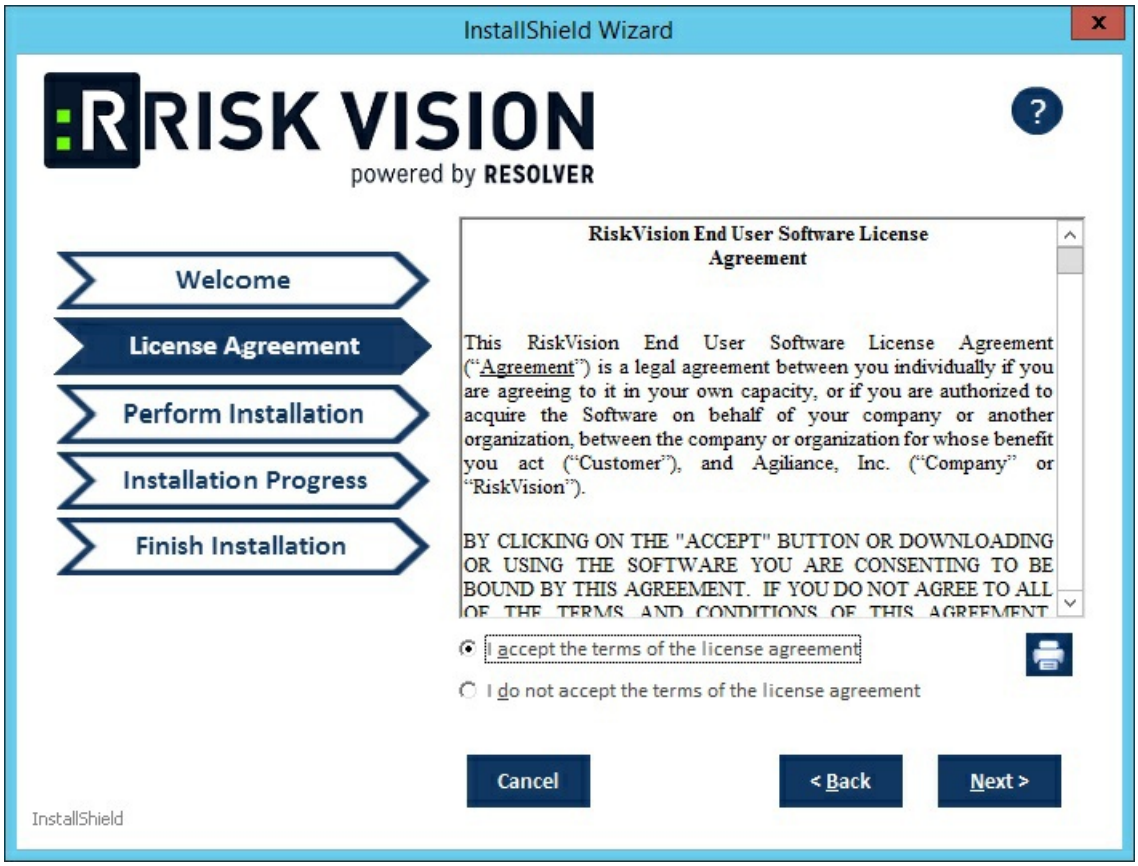
File	MySQL	Oracle
riskvision.license	✓	✓
RiskVisionConnectorManagerUpgrade.exe	✓	✓
mysql -connector-java-5.1.39.zip	✓	✗

2. Double-click the RiskVisionConnectorManagerUpgrade.exe file.

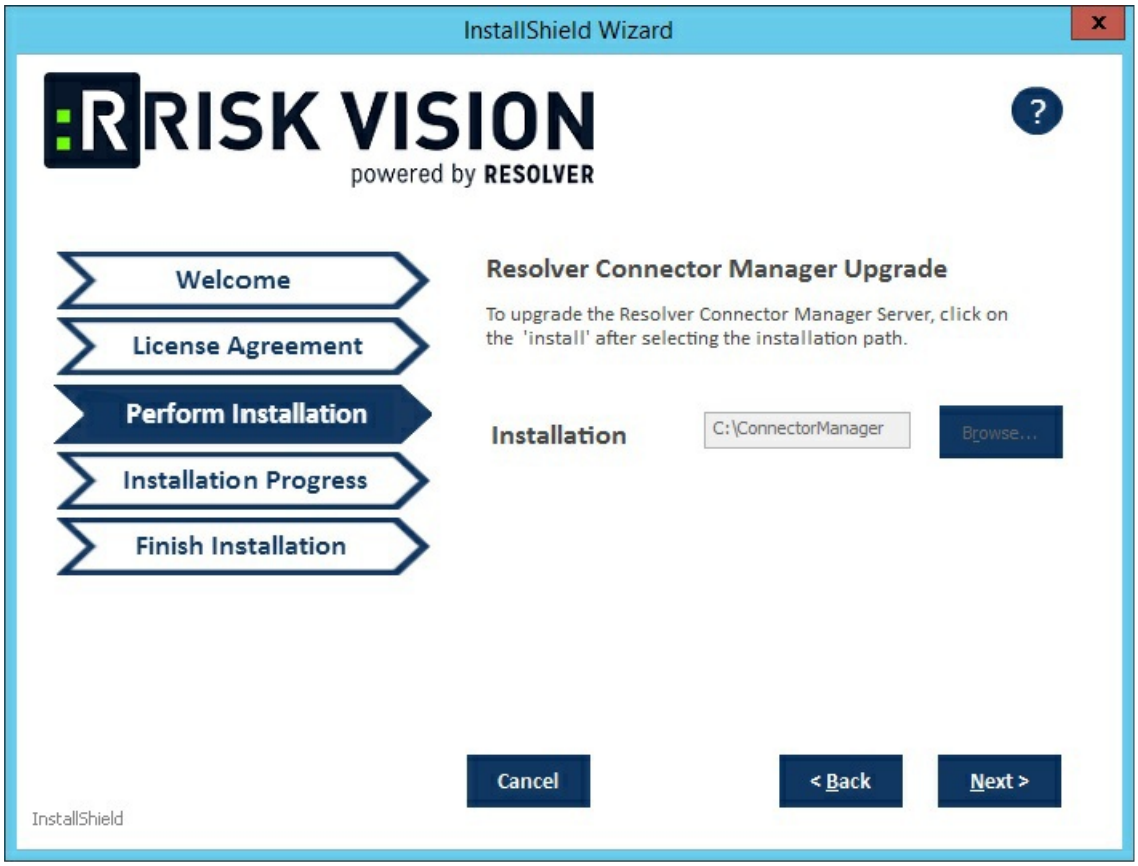


3. Click **Next**.

4. Check the **I accept the terms in the License Agreement** checkbox.

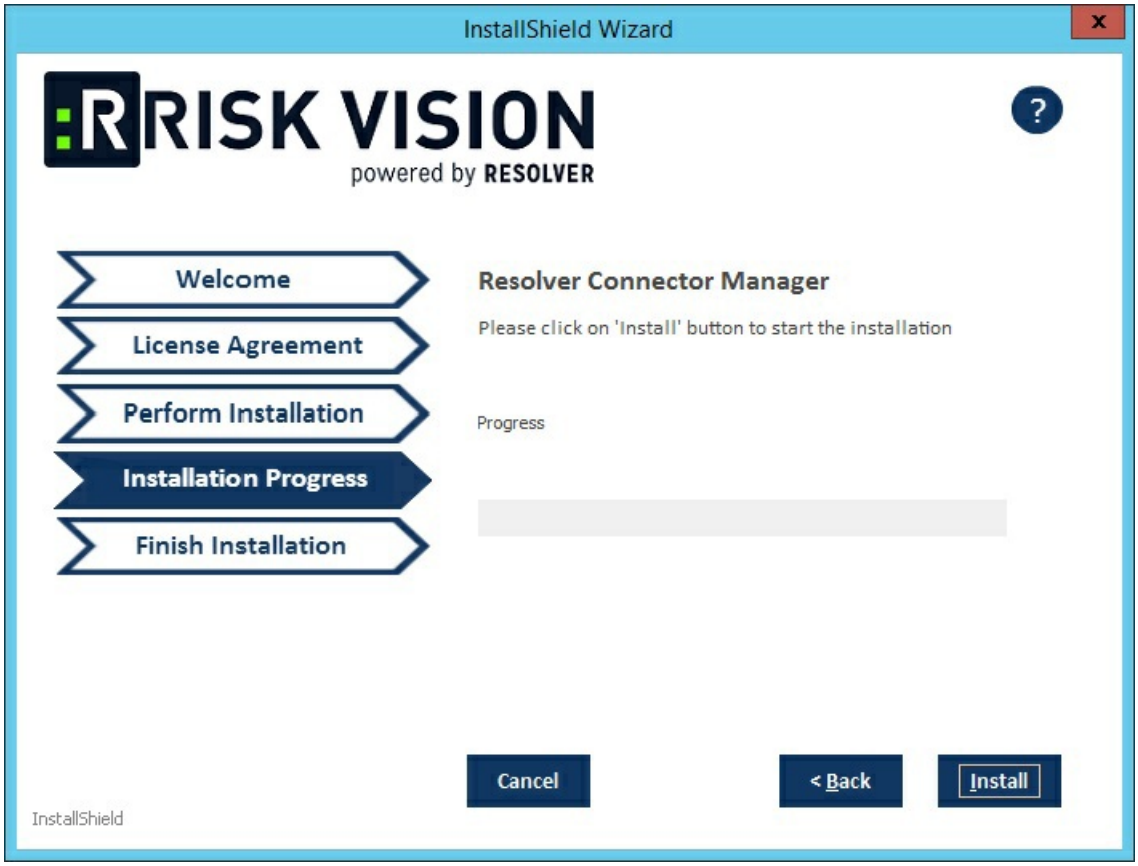


5. Click **Next**.
6. **Optional**: Click **Browse** to change the installation destination. By default, RiskVision Connector Manager is installed in the `C:\ConnectorManager\` directory. The installer sets the environment variable `%AGILIANCE_HOME%` to the product installation path specified here.



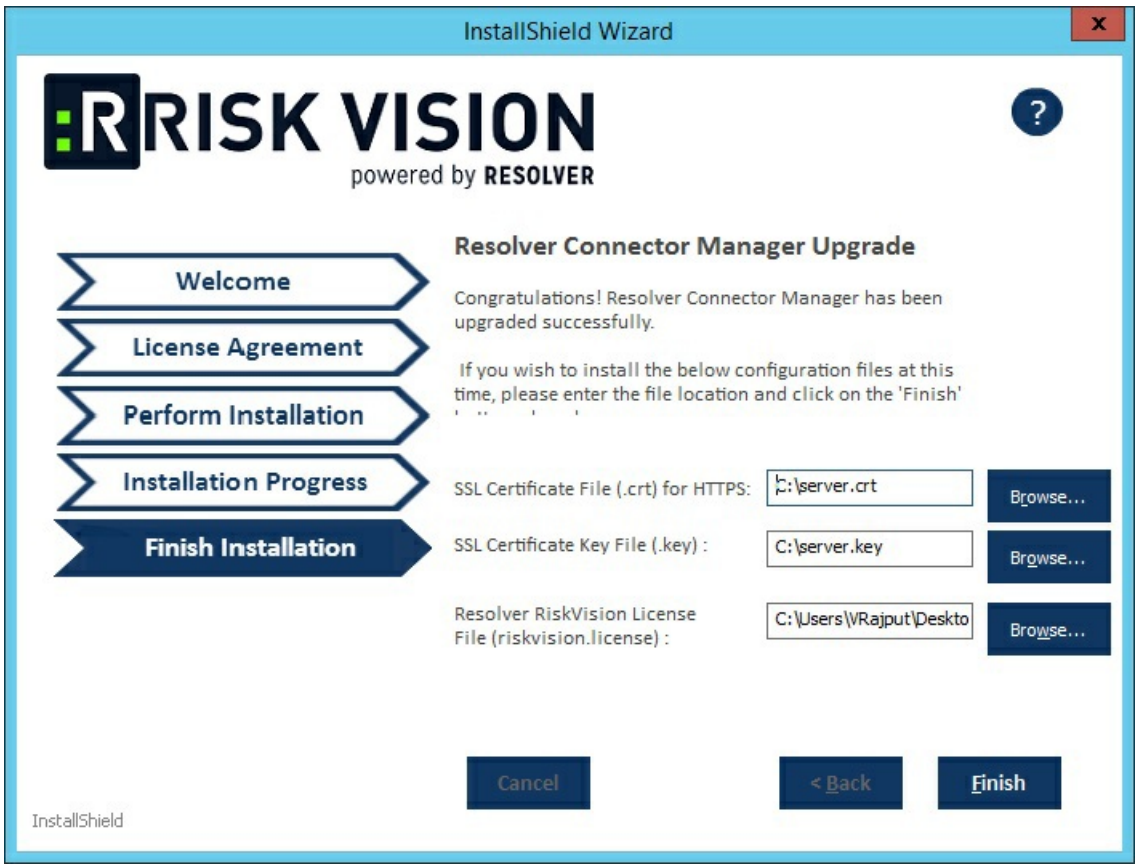
The Perform Installation wizard page.

5. Click **Next**.



6. The **Installation Progress** wizard page appears. Click **Install** to begin the upgrade process.

7. The **Finish Installation** wizard appears, click **Finish** to exit the wizard.



At this point, the RiskVision Connector Manager upgrade process is complete.

After the upgrade, the Resolver Connector Manager works on port 9443 make sure that all the connectors connect to the Resolver Connector Manager using the port 9443.

MySQL Post-Installation Scripts

To run the MySQL post-installation scripts:

1. Using command line, go to the folder where scripts are installed.
    - Example: `cd C:\Server\MySQL_PI`
2. Ensure that all the files included in `agl_master.sql` are in this folder.
3. Execute the following command. This will load the scripts and make sure that the MySQL executable is set in the path correctly so that it can be accessed from anywhere:
    - `.mysql -h[hostname] -u[username] -p [databasename] < agl_master.sql`
    - Example: `mysql -hlocalhost -uagiliance -p agiliance < agl_master.sql`

Oracle Post-Installation Scripts

After completing the installation of the Application Server and Web Server, you will need to set up the Oracle Database Server. The steps mentioned in this section must be performed on the Oracle Server host and the Application Server host.

To set up an Oracle database server:

1. Provide all of the scripts in the `%AGILIANCE_HOME%\Oracle` directory on the application server to the Oracle database administrator.
2. Open your Oracle Server host.
3. Open the command window and navigate to the ~\Database\Oracle directory. Run the following command:

   ```
   sqlplus system@ @agl_master.sql
   ```

4. Enter the Schema Owner name, Report User password, Schema User name, and Schema User password that appear in the command window upon executing the command above. If you don't own the responsibility of managing the Oracle Server, ask your organization's Oracle database administrator to run the command mentioned above.
5. Open your application server host.
6. Go to the `%AGILIANCE_HOME%\config` directory, then open the agiliance.properties file using a text editor.
7. Ensure the following properties are available for the Schema User and Schema owner:

   ```
   database.oracle.schema= database.
   oracle.username.encrypted=SchemaUserinEncryptedStringdata- base.oracle.
   password.encrypted=SchemaUserPasswordinEncryptedString
   ```

   Uncomment the Schema User and comment the Schema Owner. Save the file.
8. Restart the Tomcat service.

During the upgrade, the database points to the schema owner, so the SCHEMA_USER needs to be commented.

When setting up the Oracle Database you need to make a note of the below points:

1. Schema Owner name cannot be blank.
2. Schema Owner name cannot be SYS or SYSTEM.
3. Schema Owner name is valid i.e. Schema owner exists.
4. Report User password cannot be blank.
5. Schema User name cannot be blank.
6. Schema User name cannot be same as Schema Owner.
7. Schema User name cannot be SYS or SYSTEM.
8. Schema User password cannot be blank.
9. Schema User is not already connected.
10. Report User is not already connected.

UI Customization Upgrade Notes

You can customize RiskVision either by using the `ConfigureUI` option in the application UI (recommended) or manually in the `UICustomization.xml` file.

- Step 1:

  UI changes done in the `ConfigureUI` feature are saved in the database. During the RiskVision upgrade, the changes are automatically handled by the upgrade code (installer). The customizations can be verified after the application is upgraded successfully.

- Step 2:

  UI customization file changes are done in the `UICustomization.xml` for customizations that cannot be accomplished through `ConfigureUI`. The `UICustomization.xml` file is available in the `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` directory. To implement any changes in the `UICustomization.xml` file, you must copy the `UICustomization.xml` file to `%AGILIANCE_HOME%\config` directory and implement the customization.

  If there are differences between the UICustomization.xml file in the backed up `%AGILIANCE_HOME%\config` directory and the `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` directory after upgrading your RiskVision server (note: changes will result from new features and other UI changes) perform the below following steps:

To implement UI Customization in the UICustomization.xml file:

1. Copy the `UICustomization.xml` file from `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` to `%AGILIANCE_HOME%\config.`
2. Copy the changed XML blocks from the backed up `%AGILIANCE_HOME%\config` directory to the new `%AGILIANCE_HOME%\config` directory.
3. Save the `UICustomization.xml` file.

UIWorkspace Upgrade Notes

After upgrading RiskVision, you can keep the Jasper reports/dashboard submenu by manually customizing the `UIWorkspace.xml` file. By default, this file is located in the `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` directory. To implement any changes in the `UIWorkspace.xml` file, you will need to copy the `UIWorkspace.xml` file to the `%AGILIANCE_HOME%\config` directory and implement the customization. If there are differences between the `UIWorkspace.xml` file in the backed up `%AGILIANCE_HOME%\config` directory and the `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` directory after your upgrade (note: changes will result from new features and other UI changes) make the following changes.

To add the Jasper reports/dashboard submenu:

1. Copy the `UIWorkspace.xml` file from `%AGILIANCE_HOME%\Tomcat\webapps\spc\classes` to `%AGILIANCE_HOME%\config`
2. Copy the changed XML blocks from the backed up `%AGILIANCE_HOME%\config` to the current `%AGILIANCE_HOME%\config` file.
3. Save the `UIWorkspace.xml` file.

Add the Jasper Server Report Folder to the Tree Node

After upgrading RiskVision , you can maintain access to the Jasper Server Report folder in the RiskVision application tree node by manually configuring the `AddonTreenodeForJasperReport.xml` file.

To add the Jasper Server Report Folder to the RiskVision tree node:

1. Copy the changed XML blocks from the backed up `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` to the current `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes`
2. Save the `AddonTreenodeForJasperReport.xml` file.

Troubleshoot Upgrade Failures

This section discusses upgrade failure cases.

Case I:

If the upgrade has failed:

Check the `Upgrade.log` file in the temporary directory where the upgrade installer is triggered, and the `%AGILIANCE_HOME%\toolbox\bin\upgradedb.log` file for more details about the causes for error(s).

If the upgrade cannot be completed:

A command prompt window will open to run the rollback process. To rollback to your pre-upgrade state, use your backup files.

1. Click 'y,' when prompted.
    - **MySQL** – The rollback will be performed seamlessly without any manual intervention.
    - **Oracle** – Once the rollback is complete, the database administrator must manually restore the database to the previous state.

Case II:

If the RiskVision Server upgrade has failed on an Oracle database due to the omission of the System User connection, and the `upgradedb.log` file does not show any errors, the database has stopped abruptly. To resolve this error, you must run the `oracle_jasper_manual.bat` and `upgradedatabaseschema` scripts.

To restore all reportuser grants:

1. Open command prompt and navigate to the `%AGILIANCE_HOME%\install\` directory.
2. Enter `oracle_jasper_manual.bat` on the command line and press **Enter**.
3. Follow the instructions that appear on the command line to successfully execute the script.

To restore the database to its original state:

1. Open command prompt window and navigate to the `%AGILIANCE_HOME%\install\toolbox\bin\` directory.
2. Enter `upgradedatabaseschema.cmd` on the command line and press **Enter** to successfully execute the script.

Case III

There have been cases in which the RiskVision Server upgrade appears to have worked successfully, but Tomcat displays the following error:

****
The server is expecting the database version [Expected Version No.]. But the current database version is [Current Version No.]
***05-07 00:49:11.385|I|localhost-startStop-1|57089024|?|VersionCheckUtil - See the Administrator's Guide for instructions on how to upgrade the database.**

In this case, the problem is that there is not enough memory being allocated to Tomcat on the user's environment and the memory space must be increased.

To increase the memory space:

1. Close all RiskVision and Tomcat services.
2. Navigate to the **C:\Server\install\toolbox\bin** folder.
3. Open the **ajava.cmd** file.
4. Increase the `spaceSize` using the following code:

```
echo this is 64 bit JVM
"%JAVA%" -Xms1024M -Xmx4096M -XX:MaxMetaspaceSize=512m -Djava.util.Arrays.useLegacyMergeSort=true %*
) else (
echo this is not 64 bit JVM
"%JAVA%" -Xms256M -Xmx1536M -XX:MaxMetaspaceSize=512m -Djava.util.Arrays.useLegacyMergeSort=true %* )
-Xmx4096M, -Xmx1536M by 8 or 6 times
```

5. Restart RiskVision.

6. Run the **upgradedatabaseschema.cmd** file in the **C:\Server\install\toolbox\bin** folder.

Change the Database Account Passwords

This section explains how to lock down the database and change the default passwords in MySQL. You must change the corresponding settings in the application, as explained in the Configuring Database on the RiskVision Application section.

To change a MySQL root account password:

1. Navigate to `%AGILIANCE_HOME%\MySQL\bin` and open Command Prompt from that window.

2. Enter the command:

```
mysql -uroot -p default_password -Dmysql.
```

3. Change the root password using the following command:

```
SET PASSWORD FOR 'root'@'localhost'= PASSWORD ('newpass');
```

```
FLUSH PRIVILEGES;
```

4. Try logging in from mysql with the root and new password.

5. Run grants:

    1. grant all on *.* to 'root'@'' identified by 'NEW PASSWORD' with grant option;

    2. flush privileges;

Special characters like " ' " and " / " cannot be used in the password.

To change the Oracle Schema Accounts:

Your Oracle database administrator must change the password for the Schema Owner and Schema User accounts by executing the ALTER USER commands. After the passwords are changed, you must replace the changed password in all database connection properties.

- `ALTER user IDENTIFIED BY`

The Application server

This section describes the application properties required for connecting to a MySQL or Oracle database.

To update the passwords used by the application:

1. Encrypt the root password with `encrypt.cmd.`
    - Open command prompt and navigate to the `Server\install\toolbox\bin` directory.
    - Run the following command: `encrypt.cmd`
2. Copy the encrypted password.
3. Open the `%AGILIANCE_HOME%\config\agiliance.properties` file and set the below properties:

    For a MySQL database:

    `database.mysql.admin.username.encrypted=EncryptedString`

    `database.mysql.admin.password.encrypted=EncryptedString`

    For an Oracle database:

    `database.oracle.username.encrypted=`

    `database.oracle.password.encrypted=`

4. Save the `agiliance.properties` file.
5. Restart the RiskVision Tomcat.

To change the MySQL agiliance application passwords:

MySQL Database:

1. Navigate to `%AGILIANCE_HOME%\MySQL\bin` and open command prompt from that window.
2. Enter the following command:

   ```
   mysql -uroot -p default_password -Dmysql.
   ```

3. Change the agiliance password using the following command:

   ```
   SET PASSWORD FOR 'agiliance'@'localhost'= PASSWORD ('newpass');
   ```

   ```
   FLUSH PRIVILEGES;
   ```

4. Try logging in from MySQL with the new agiliance password.
5. Run grants:
   - grant all on *.* to 'agiliance'@'' identified by 'NEW PASSWORD' with grant option;
   - flush privileges;

Oracle Database:

- `ALTER user IDENTIFIED BY`

On the Application server:

1. Encrypt the agiliance password with encrypt.cmd:
   1. Open command prompt and navigate to the `Server\install\toolbox\bin` directory.
   2. Run the following command: `encrypt.cmd`
2. Copy the encrypted password.
3. Open the `%AGILIANCE_HOME%\config\agiliance.properties` file and set the following properties:

   For the MySQL database:

   ```
   database.mysql.username.encrypted=EncryptedString
   database.mysql.password.encrypted=EncryptedString
   ```

   For the ORACLE database:

   ```
   database.oracle.username.encrypted=
   database.oracle.password.encrypted=
   ```

4. Save the `agiliance.properties file.`
5. Restart the RiskVision Tomcat.

Install an SSL Certificate on the JasperReports Server

JasperReports Server includes a self-signed Secure Sockets Layer (SSL) certificate to ensure a safe, secure, and reliable connection. You can access the JasperReports Server using web services over HTTPS or HTTP.

Note: Since you can set up Jaspersoft reports or dashboards in the RiskVision user interface, you must also be able to access the JasperReports Server repository from the RiskVision application.

To install a third-party SSL certificate:

1. Copy the server.crt file to the `%Agiliance_HOME%\apache2\conf directory.`
2. Navigate to the working directory with the following command:

   `> cd %JAVA_HOME%/ jre /bin`

3. Run the following command to import the SSL certificate:

   `> keytool -import -alias server. crt - keystore ../lib/security/ cacerts -file %Agiliance_HOME%\apache2\conf\server.crt`

4. When the commands are successfully executed, enter the default password: changeit.
5. **Optional**: Run the following command the check that the certificate was imported successfully:

   `> keytool -list - keystore ..\lib\security\cacerts -alias server.crt`

Once the certificate is installed, HTTPS is used for communication between the JasperReports Server and the RiskVision Server. To connect to the JasperReports Server over HTTP, you must make the following changes to the `agiliance.properties` file, available in the `%AGILIANCE_HOME%\config` directory:

1. Enable the `jasper.use.secure.connection=false` property.
2. Enable the `jasper.admin.port=8480` property.

Also, change the `riskvision.host.ipaddress=` property to the `agiliance.properties` file available in the `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF` directory.

Jaspersoft reports sometimes need to be run in RiskVision, such as when using the RiskVision Contextual Reporting feature or running a Jasper report attached to a RiskVision tab. Jasper reports communicate with the RiskVision UI using a REST API.

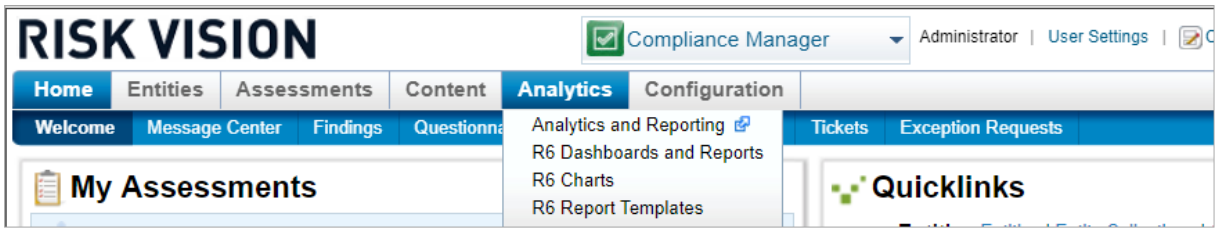
The REST web service fetches the list of reports from the JasperReports Server to RiskVision when the user selects the Analytics report picker. By default, the REST web service uses a secure connection but does not validate the SSL certificate. If you want to force the Jasper REST web services to use an HTTPS connection, then you can set the property `jasper.api.SSLcertificate.validation=true` and install an SSL certificate. The default value of the property is false.

You must use a fully qualified server name while using the secure connection to display the reports based on user's permissions.

Access Jasper Reports Server from Within RiskVision

To access JasperReports Server from within RiskVision:

1. Log into RiskVision.
2. Click the **Analytics** menu > **Analytics and Reporting** to launch the JasperReports Server.



The Analytics menu.

If you have any problems accessing the JasperReports Server, see Troubleshooting the JasperReports Server Installation.

Launch JasperReports Server in Standalone Mode

Although JasperReports Server can be accessed through the RiskVision UI, you can also launch it in standalone mode from the local host in which the JasperReports Server is installed. This is generally the preferred method for administering the application. To use JasperReports Server in standalone mode, you must create a user that will help establish a connection between JasperReports Server and Jaspersoft Studio Professional.

To launch JasperReports Server in a standalone mode from the localhost:

1. Open a browser on your JasperReports Server and enter the following URL: `http://:/jasperserver-pro/login.html`

   where is the JasperReports Server name and is the default, port 8480, which is used by JasperReports Server for communication.

2. Enter the following credentials:
   Username: `sysadmin`
   Password: `agiliance`

Change the Default Port Number

Change the default port number by downloading the following files from the JasperReports Server:

- server.xml
- agiliance.properties

server.xml

Go to the `%JASPER_HOME%\apache-tomcat\conf` directory, open the `server.xml` file by using a text editor, locate the following element and then change the port number:

agiliance.properties

Go to the `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF` directory, open the `agiliance.properties` file by using a text editor and then change the port number in the following property:

`jasper.admin.port=`

You can also login to the JasperReports Server using the port 8480 from the RiskVision Server host over HTTP using the properties as described in the "Installing the Secure Sockets Layer (SSL) Certificate on JasperReports Server" section.

To start or stop services:

1. Go to **Start > All Programs > Report Server > Start or Stop Services**

2. Do one of the following:

- To start services, click **Start Service**.
- To stop services, click **Stop Service**.

3. When you perform either of the actions, one or more command windows appear, indicating that the services are being started or stopped. The command window(s) will close automatically when the services are started or stopped.

To start, restart, or stop a specific service:

1. Go to **Start > Control Panel > Administrative Tools**, and then double-click **Services**. The Services window is displayed.

2. Right-click a service and select the appropriate action: **Start, Restart, Stop** in the context menu.

Schedule Reports in JasperReports Server

Version 9.1 & Later

This section describes how to setup the scheduler available in JasperReports Server in version 9.1 and later For version 9.0 and older, see the **Version 9.0** section below. These settings will allow you to email multiple recipients when a scheduled report is complete.

To set up the JasperReports Scheduler:

1. Stop the Jasper server.
2. Go to the `%JASPER_HOME%/apache-tomcat/webapps/jasperserver-pro/WEB-INF` directory.
3. Open the `js.quartz` properties file using a text editor and specify the following properties:

   `report.scheduler.mail.sender.username=`
   `report.scheduler.mail.sender.password=`
   `report.scheduler.mail.sender.from=`
   `report.scheduler.mail.sender.protocol=smtp`
   `report.scheduler.mail.sender.port=587`
   `report.scheduler.mail.smtp.starttls.enable=true`
   `report.scheduler.mail.smtp.auth=true`
4. Add the following properties in the `applicationcontext.xml` file:
   `property name="javaMailProperties">`

   `true`
   `true`
   `true`

5. Add the following properties to the `applicationcontetx-report-scheduling.xml` file:
   `property name="javaMailProperties">`

   `true`
   `true`
   `true`

6. Restart the server.
7. Add Schedule information(follow steps above) for any report and verify email.

Version 9.0

1. Stop the JasperReports Server service.

2. Go to the `%JASPER_HOME%/apache-tomcat/webapps/jasperserver-pro/WEB-INF` directory, open the `js.quartz` properties file by using a text editor, and specify the following properties:

`report.scheduler.mail.sender.host=`

`report.scheduler.mail.sender.username=`

`report.scheduler.mail.sender.password=`

`report.scheduler.mail.sender.from=`

Where **host** is the computer name containing the mail server, **username** is the name of the user in the mail server that JasperReports Server will use, **password** is mail user's password, and **from** is the email address that appears in the From field of email notifications.

3. When you finish configuring the properties, restart the JasperReports Server service to show the latest changes.

Troubleshoot the JasperReports Server Installation

Here is a list of common problems that may arise while installing the JasperReports Server. Find the problem that most closely matches the situation that is occurring. Then, follow the steps to fix the problem.

Jasper Report server does not support the IE 8 and IE Compatibility mode.

Problem I: Analytics and Reporting submenu item not visible on the Analytics menu

If the **Analytics and Reporting** sub-menu item is not visible on the **Analytics** menu to launch the JasperReports Server, perform the following steps:

1. Go to the `%AGILIANCE_HOME%\apache2\conf\extra\` directory location, open the `workers.properties` file using a text editor, and then verify whether the following properties are correct:

   `worker.jasper_tomcat.port=8409`

   `worker.jasper_tomcat.host=`, where is the fully qualified hostname of the system on which the JasperReports Server is installed.

   `worker.jasper_tomcat.type=ajp13`

2. Go to the `%AGILIANCE_HOME%\config` directory, open the `agiliance.properties` file using a text editor, and then verify whether the following properties are available:

   `jasper.hostname= or`

   `jasper.database.host= or`

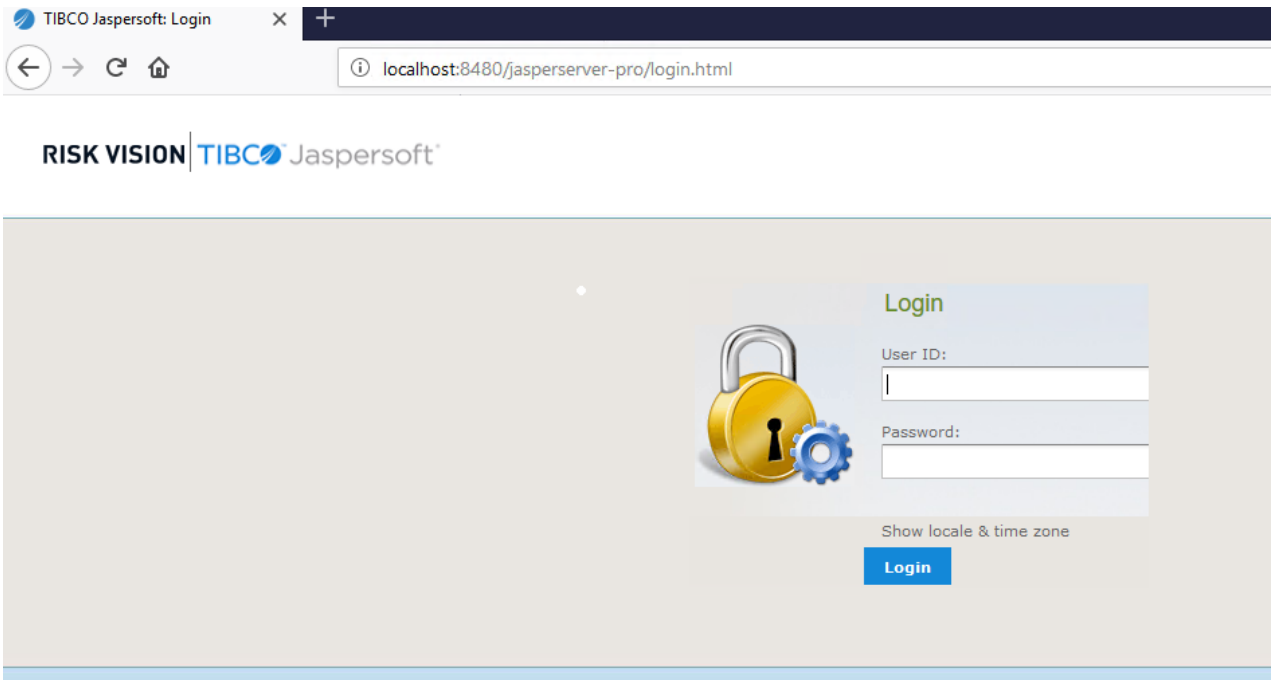
   `jasper.database.port=5432`

3. If you make any changes to the agiliance.properties file, restart the RiskVision Apache and RiskVision Tomcat services.

   Once the services have been restarted to show the latest changes, view the**Analytics and Reporting** submenu in the **Analytics** menu.

Problem II: The Jasper RiskVision Analytics server is currently unavailable

When JasperReports Server is accessed from the Analytics menu, the message "the Jasper RiskVision Analytics server is currently unavailable" is displayed. To fix this problem, evaluate the JasperReports Server installed directory in the following order:



1. Perform the following steps to verify whether you are able to launch the JasperReports Server in a standalone mode:
   - Ensure Jaspersoft services jasperreportsPostgreSQL and jasperreportsTomcat are running.

- Go to:

  `http://:8480/jasperserver-pro/login.html`

  Where the is the IP address of the system on which the JasperReports Server is installed.

- The JasperReports Server Login page appears. Enter the sysadmin as User ID and agiliance as Password. If the JasperReports Server homepage appears, see Verifying the JasperReports Server Installation on the RiskVision Server Setup. Otherwise, continue with the steps below:

2. If you see the error message "Unable to launch the JasperReports Server," the JasperReports Server is not installed properly. To ensure Jaspersoft services is working, go to the directory `<%JASPER_HOME%>\Agiliance\scripts`. Open the file `initdb.log` by using a text editor. If there are errors in the `initdb.log`, PostgreSQL database is not properly installed. Follow the installation instructions and re-install the JasperReports Server. If there are no errors in the file `initdb.log`, continue the investigation:

3. Stop the Jaspersoft services, go to the following directories, back up the log files, and then delete all the log files. The default location of the log files is here:

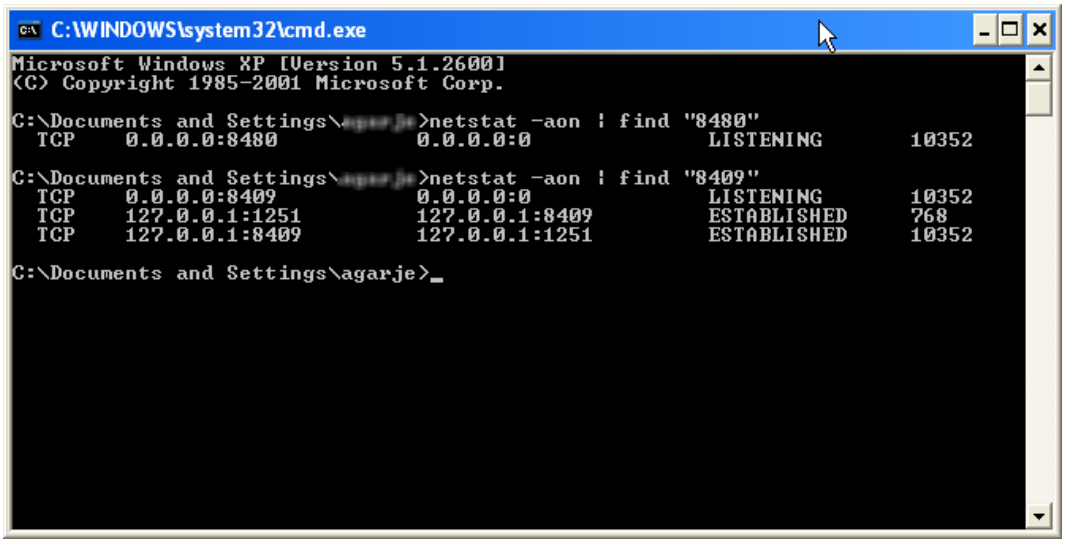
   `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\logs`

   `%JASPER_HOME%\apache-tomcat\logs`

4. After all the log files are deleted, start Jaspersoft services.

5. Run the following commands using the Windows Command prompt to verify whether the ports '8480' and '8409' are listening.

   ```
   > netstat -aon | find "8480"
   > netstat -aon | find "8409"
   ```



6. If both ports are listening, go to **step 1** and verify if you are able to launch the JasperReports Server.

7. If the problem still persists, check the log files for any errors.

8. If JasperReports Server does not launch, the RiskVision Report Server installer failed to copy the file contents or skipped copying files from the source directory to the target directory. Compare the directory, files, and contents to see if they match the listed source directory and the target directory columns.

Source Directory	Target Directory
%JASPER_HOME%\Agiliance\cfg\tomcat\server.xml	%JASPER_HOME%\apache-tomcat\conf\server.xml
%JASPER_HOME%\Agiliance\cfg\jasper-web-inf*.-jar	%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\lib
%JASPER_HOME%\A-giliance\cfg\license\jasperserver.license	%JASPER_HOME%\jasperserver.license
%JASPER_HOME%\Agiliance\lib*.jar	%JASPER_HOME%\apache-tomcat\lib*.jar
%JASPER_HOME%\Agiliance\lib*.jar	%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\lib*.jar
%JASPER_HOME%\A-giliance\cfg\postgres\postgres-changes.sql	%JASPER_HOME%\postgresql\bin\postgres-changes.sql

Source Directory	Target Directory
%JASPER_HOME%\scripts\installer\grant-priv-js-postgres8.sql	%JASPER_HOME%\postgresql\bin\grant-priv-js-post-gres8.sql
%JASPER_HOME%\Agiliance\cfg\buildomatic\build_conf\default\js.jdbc.properties	%JASPER_HOME%\buildomatic\build_con-f\default\js.jdbc.properties

9. If there are missing files or inappropriate file contents, copy the file from the source directory to the target directory.
10. Restart the Jaspersoft services if changes were made. The changes are applied to the JasperReports Server installation directory and JasperReports Server should launch.
11. If the problem still exists after copying all the artifacts to the target directory, go to the directory `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF` . Open the `agiliance.properties` file by using a text editor, and then verify if the following properties are correct:

For MySQL

```
database.type=mysql
database.mysql.driver=com.mysql.jdbc.Driver
database.mysql.url=jdbc:mysql://:3306/
riskvision.app.url=
jasper.admin.port=8480
```

For Oracle

```
database.type=Oracle
database.oracle.driver=oracle.jdbc.OracleDriver
database.oracle.url=jdbc:oracle:thin:@:1521/agl
riskvision.app.url=
jasper.admin.port=8480
```

By default, the property is set to 8480. If you have changed the port number, specify the correct port number.

If your investigation still does not resolve the problem, contact Resolver Support and provide the appropriate log files.

Verify the JasperReports Server Installation on the RiskVision Server

If you are able to launch the JasperReports Server in a standalone mode, perform these steps to verify the JasperReports Server installation on the RiskVision Server setup.

If there any errors in the log files, restart the services: RiskVision Tomcat and RiskVision Apache.

1. Go to the `%Agiliance_HOME%\apache2\logs` directory to check the log files for errors.

   If there are errors in the log files, re-start the services: RiskVision Tomcat and RiskVision Apache.

2. Go to the `%AGILIANCE_HOME%\apache2\conf\extra`, open the `worker.properties` file using a text editor, and verify whether the following properties are set correctly:

   worker.jasper_tomcat.port=8409

   worker.jasper_tomcat.host=

   Where is the fully qualified hostname of the system on which the JasperReports Server is installed.

3. Log in to RiskVision application and launch the JasperReports Server. The JasperReports Server home page must appear.

4. If the problem still exists, go to the directory `%AGILIANCE_HOME%\config`, open the file `agiliance.properties` using a text editor, and ensure that the properties related to the JasperReports Server are set correctly.

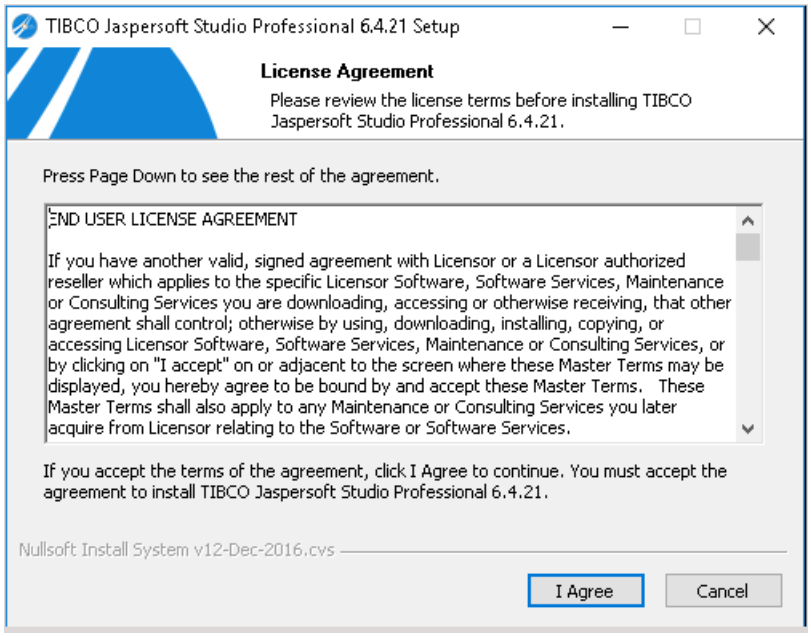
If verification fails to resolve the problem, contact Resolver Support with the appropriate log files.

Install TIBCO Jaspersoft Studio Professional 6.4.2.1

This section describes the procedural steps to install the Jaspersoft Studio Professional application.

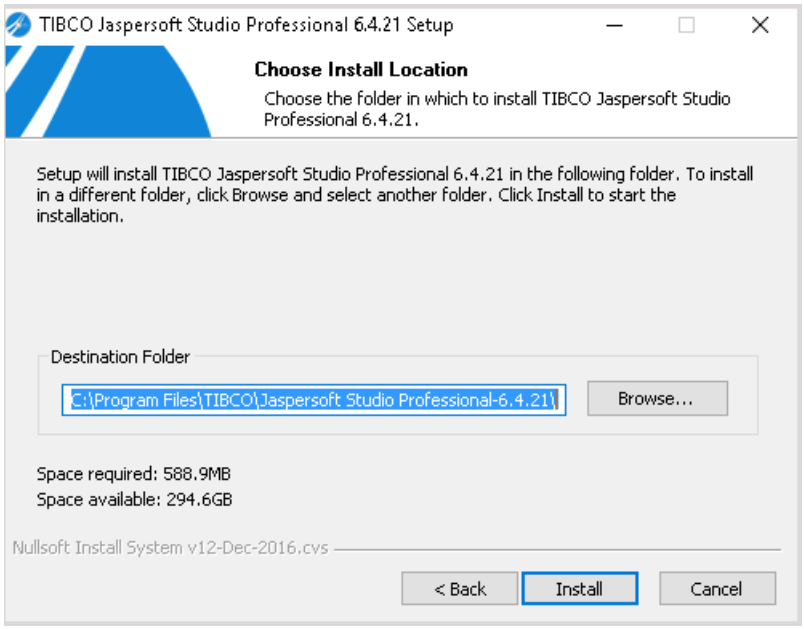
To install TIBCO Jaspersoft Studio Professional:

1. Double-click the TIB_js-jss_6.4.2.1_windows_x86_64.exe file to launch the Jaspersoft Studio Professional 6.4.2.1 Setup wizard.
2. The License Agreement wizard appears.



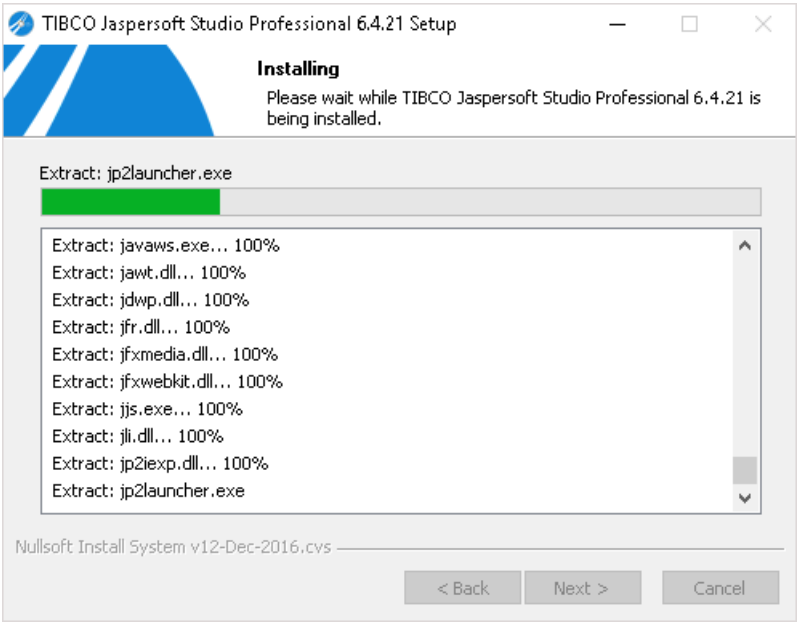
Click **I Agree** to accept the license agreement and to continue.

3. The **Choose Install Location** wizard page appears. By default, Jaspersoft Studio Professional is installed in the `C:\Program Files\TIBCO\Jaspersoft Studio Professional-6.4.2.1.final\` directory. The installer sets the environment variable `%JaspersoftStudio_HOME%` to the product installation path specified here. Observe that the installation folder meets the minimum space criteria. Click **Browse** if the installation folder does not have sufficient space or if you wish to install the Jaspersoft Studio Professional in another directory.



Click **Install** to start installation.

4. The set up now prepares the settings required by the installation scripts based on your previous selection.



5. After the installation is complete, click **Finish** to exit the wizard and to launch the TIBCO Jaspersoft Studio Professional application.

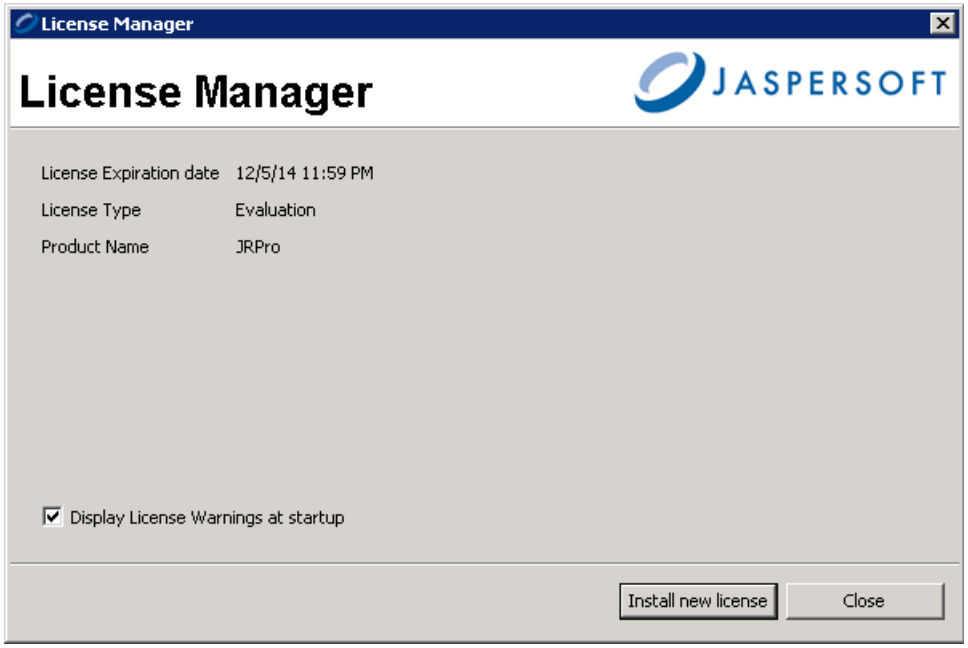
This completes the TIBCO Jaspersoft Studio Professional installation.

Install the Jaspersoft Studio Professional License

After completing the installation of Jaspersoft Studio Professional application, you will need to install the Jaspersoft Studio Professional application license.

To install the license:

1. Obtain the `jasperserver.license` file from the JasperReports Server installed directory: `%JASPER_HOME%\` and place it in a temporary folder if you have installed the Jaspersoft Studio Professional application on a host other than the JasperReports Server.
2. Go to **Start** > **All Programs** > **TIBCO** > **Jaspersoft Studio Professional** to launch the Jaspersoft Studio Professional application.
3. Go to **Help** and click **License Manager**. The **License Manager** dialog appears.



4. Click **Install new license**, choose the `jasperserver.license` file from the appropriate location, and then click **Open**. The **License Manager** information dialog with the following message is displayed: "The License file has been installed," click **OK**, and then click **Close** on the **License Manager** dialog box.

To set up a connection to the RiskVision database and JasperReports Server repository, see Setting up Jaspersoft Studio Professional.

Set up Jaspersoft Studio Professional

Prerequisites to setting up Jaspersoft Studio Professional:

- Installation of Tibco Jaspersoft Studio Professional 6.4.2.1; and
- Installation of the Jaspersoft Studio Professional License.

Before using Jaspersoft Studio Professional to create or design reports, you must perform the following tasks:

1. Create the database connection.
2. Create the JasperReports Server Repository connection.
3. Install an SSL certificate on the Jaspersoft Studio Professional application host.

Perform the above steps for every installation of Jaspersoft Studio Professional.

Creating a User in JasperReports Server

To create a user on your JasperReports Server, set up the connection between Jaspersoft Studio Professional and the JasperReports Server.

To create a user on the JasperReports Server:

1. Open a browser and enter the following URL to launch the JasperReports Server in standalone mode.

   `http://:8480/jasperserver-pro/login.html`

   When the Jaspersoft login page appears, enter User ID **sysadmin** and Password **agiliance**.

2. Go to **Manage > Users**, then click **Add User**.
3. Enter the user information in the following fields: **User name**, **User ID**, **Email**, **Password**, and **Confirm Password**. Click **Add User to**.
4. Click **Edit** and scroll down to view the **Roles Available** section.
5. Click the **ROLE_POWERUSER** role.
6. Click **>>** to move the role into the **Role Assigned** section, then click **Save.**

Database Configuration

You must establish communication between Jaspersoft Studio Professional and the RiskVision database if they are not installed on the same host server.

MySQL database:

Run the following MySQL command to provide access to the database server. By default, both the user name and password are "agiliance".

*> grant all on *.* to 'agiliance'@'' identified by 'agiliance' with grant option;*

*> grant all on *.* to 'root'@'' identified by 'agiliance' with grant option;*

> flush privileges;

Oracle database:

1. Install and configure the Oracle Client version 12.2.0.1 then go to the `%ORACLE_HOME%\app\network\admin directory` to open the `tnsnames.ora` file using a text editor.
2. Locate the database name used by the RiskVision Server and change the host to point the Oracle server.

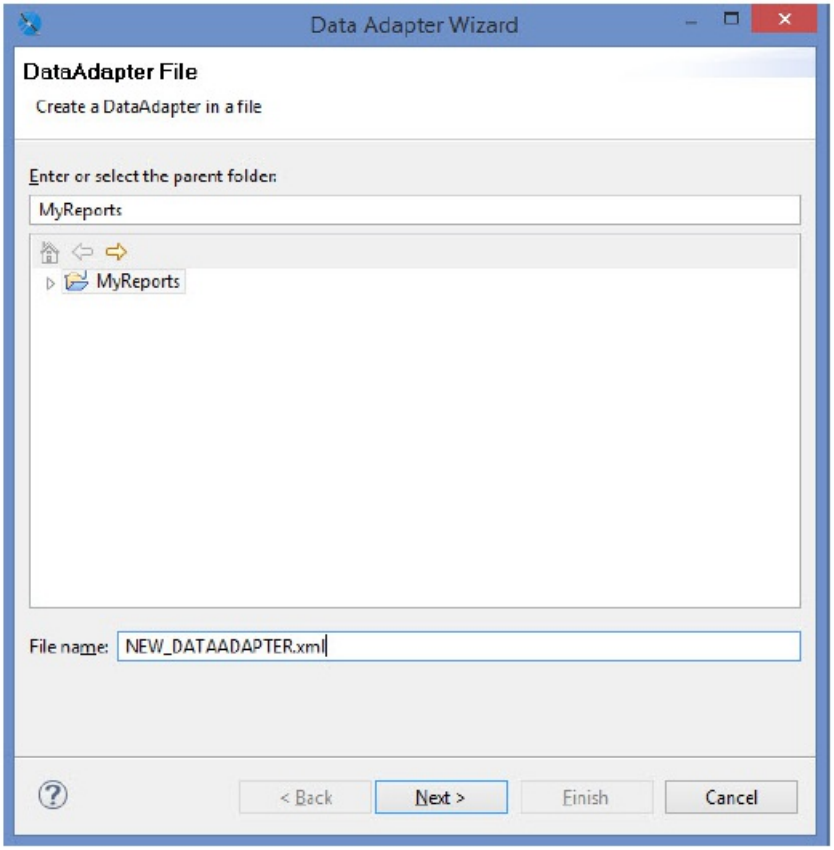
To create a database connection and jasperreports server repository connection, see:

- Creating the Database Connection.

- Creating the JasperReports Server Repository Connection.

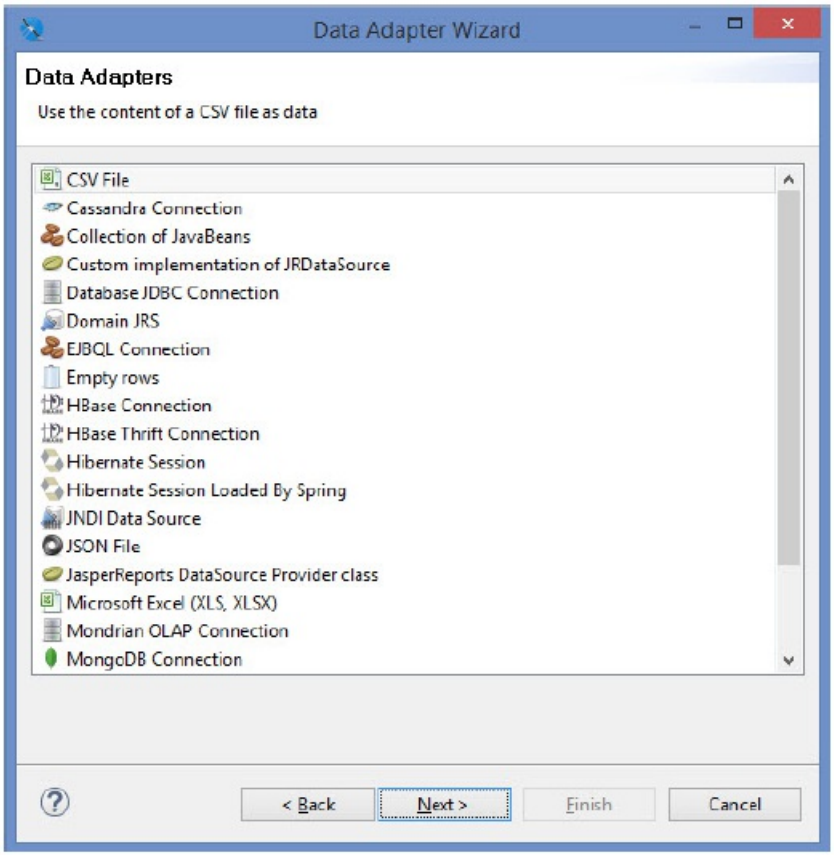
Create the Database Connection

1. Start the Jaspersoft Studio Professional application.
2. On the **File** menu, click **New > Data Adapter**.
3. The **Data Adapter Wizard** displays the **DataAdapter File** wizard page.Select the parent folder. The data adapter settings, by default, are saved in the NEW_DATAADAPTER file. Rename the file if required.



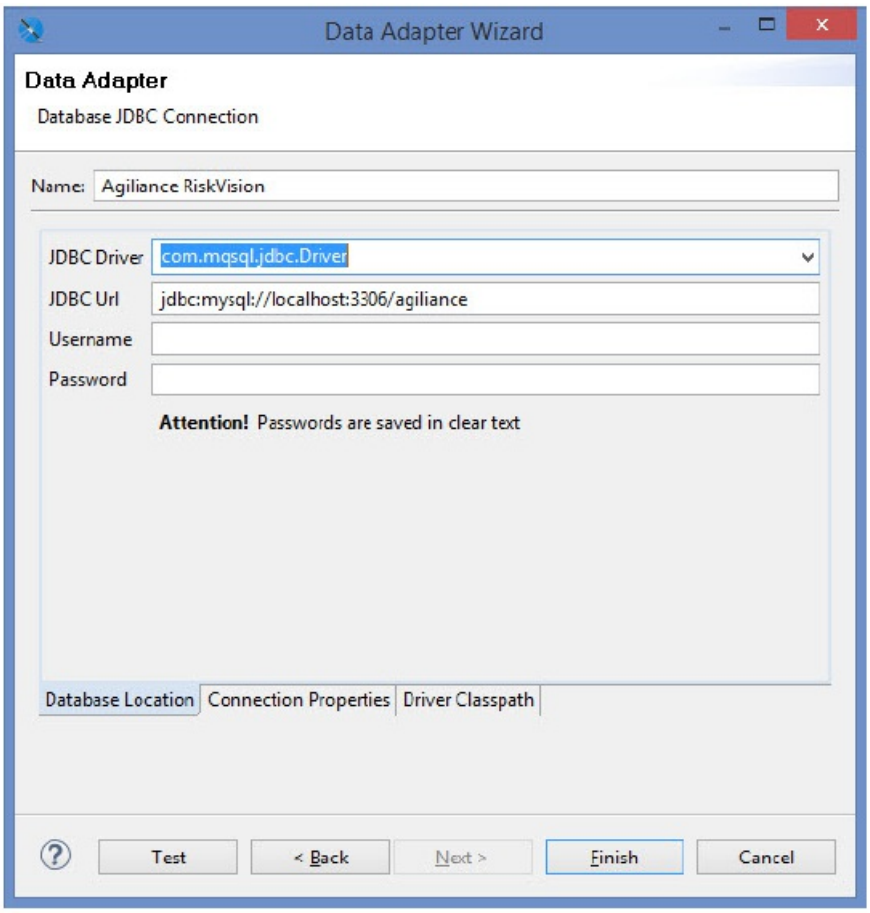
Click **Next** to continue

4. The **Data Adapters** wizard page appears. Select **Database JDBC Connection**.



Click **Next** to continue.

5. The **Database Adapter** wizard page displays the **Database Location** tab. Enter Name, JDBC Driver, JDBC URL, Username, and Password. If your database is MySQL, you must select **com.mysql.jdbc.Driver** in the JDBC Driver drop-down list. If your database is Oracle, you must select **oracle.jdbc.driver.OracleDriver** in the JDBC Driver drop-down list. The JDBC URL pattern for MySQL and Oracle databases is given below:
MySQL. jdbc:mysql://localhost:3306/agiliance
Oracle. jdbc:oracle:thin:@localhost:1521/agl



6. On the Database Adapter wizard page, click the Driver Classpath tab. Click Add and select the jar file for the database from the appropriate directory, and click Open. The JDBC Driver jars file for the MySQL and Oracle databases are given below:

   MySQL. mysql-connector-java-5.1.39-bin.jar

   Oracle. ojdbc6.jar

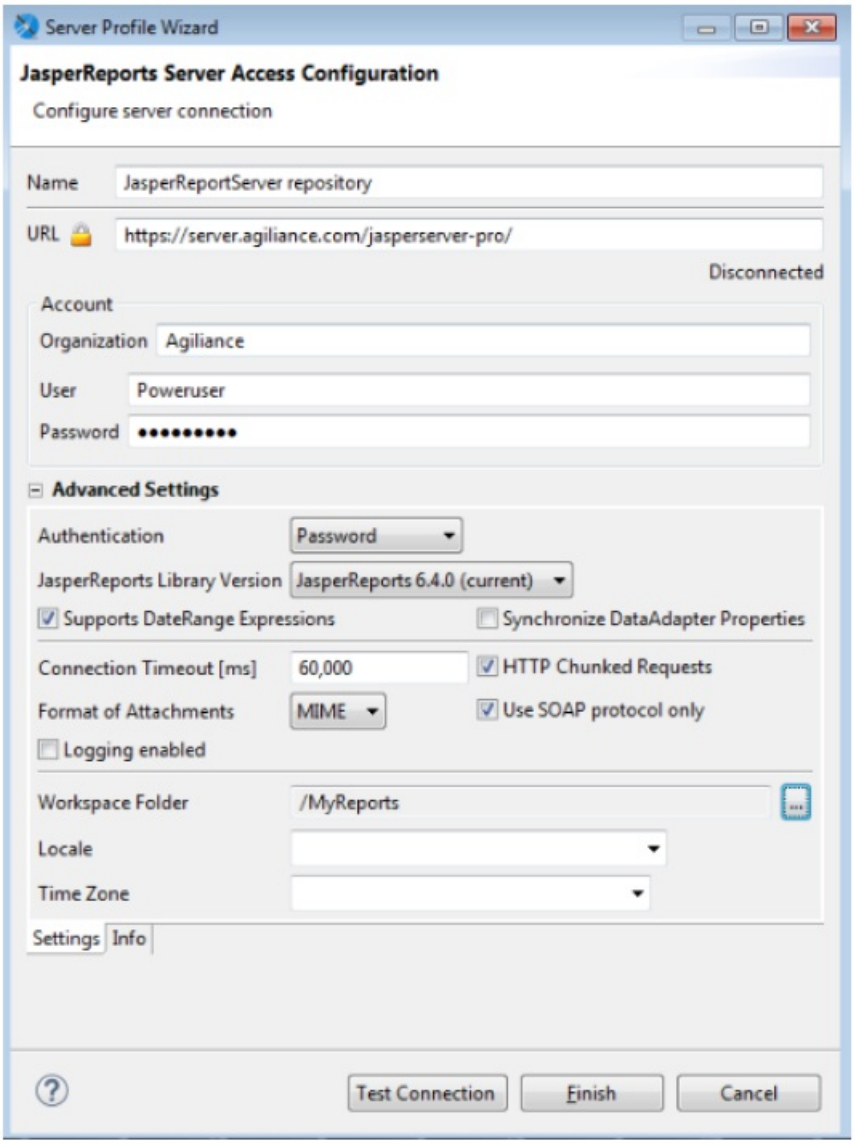
   7. Click **Test** to verify the connection.

   8. Click **Finish** to save the connection and to exit the **Data Adapter Wizard**. The database connection is created

Create the JasperReports Server Repository Connection

To create the JasperReports Server Repository connection:

1. Create a user in the Jaspersoft Report Server application. For information about creating a user in the JasperReports Server application, see Creating a User in JasperReports Server.
2. On the **Window** menu, click **New Window**.
3. The **Repository Explorer** appears at the left-hand side within the Jaspersoft Studio Professional application. Click the  icon to create the JasperReports Server connection.
4. The **Server Profile Wizard** appears. Enter the JasperReports Server information as follows: Name, URL, and in the Account section, enter the Organization, User, and Password. The User and Password are the user credentials of the JasperReports Server user that you have created in the section, Creating a User in JasperReports Server.



Note: You must install an SSL certificate to jaspersoft studio keystore. See Installing an SSL Certificate on the Jaspersoft Studio Professional Application Host.

Install an SSL certificate on the Jaspersoft Studio Professional Application Host

You must install Secure Sockets Layer (SSL) certificate on the Jaspersoft Studio Professional application host so that you can connect to the JasperReports Server with HTTPS in the URL.

To install SSL certificate:

1. Open command prompt and navigate to the `C:\Program Files\TIBCO\Jaspersoft Studio Professional-6.4.2.1\features\jre.win32.win32.x86_64.feature_1.8.0.u121\jre\bin` path.
2. Run the command `keytool.exe -import -alias server.crt -keystore " C:\Program Files\TIBCO\Jaspersoft Studio Professional-6.4.2.1\features\jre.win32.win32.x86_64.feature_1.8.0.u121\jre\lib\security"\cacerts -file \apache2\conf\server.crt`
3. When the command executes successfully, enter the default password `changeit`, you can now connect to the JasperReports Server over HTTPS protocol.
3. Restart Jaspersoft Studio Professional.

Secure Your Jaspersoft Installation

After installing JasperReports Server, please perform the following steps to secure the installation.

By default, two Jasper users are created internally when JasperReports Server is installed: `rvJasperUser` and `sysadmin`.

- **rvJasperUser**: This user is created for the tenant, which is used for RiskVision web services. Do not delete the internal user `rvJasperUser` because you will lose web services connectivity from RiskVision to the JasperReports Server.
    - You can change the `rvJasperUser's` password, or replace the internal user with another user. When you replace the `rvJasperUser` user, RiskVision recommends assigning only the `ROLE_USER` role to the newly-created user. To do so, configure the following properties in the `agiliance.properties` file on the RiskVision server:
    - `jasper.rvUserWebServiceUser=`
    - `jasper.rvUserWebServicePwd=`
- **sysadmin**: This is the root user for the JasperReports Server. By default, the password is `agiliance`. To secure the user account, log on to the JasperReports Server, then change the password.

Change the JasperReports Server Passwords

RiskVision uses four different accounts to facilitate a tight integration with JasperReports Server. We recommend changing the default passwords for each of these accounts. The accounts are:

1. **ReportUser**: Used to query data for reports.
2. **sysadmin**: Used to perform administrative actions on the JasperReports Server.
3. **rvJasperUser**: Used to query the JasperReports Server APIs from RiskVision and Jaspersoft Studio.
4. **PostgreSQL**: This account is the root account for PostgreSQL and is used to back up the JasperReports Server database.

Change the ReportUser Password

The ReportUser password must be changed on the following servers:

- MySQL database or Oracle database server;
- Application server; and
- Report server.

For a MySQL database:

1. Navigate to `%AGILIANCE_HOME%\MySQL\bin` and open command prompt from that window.
2. Enter the following command:

   ```
   mysql -u root -p
   ```

   Enter the root password (by default the root password is agiliance).

3. Check the connection for the reportuser by running the following query on the MySQL database:

   ```
   SELECT * FROM USER WHERE USER = 'reportuser';
   ```

4. Change the reportuser password using the following command:

   ```
   SET PASSWORD FOR 'reportuser'@'REPORT_SERVER_HOST'= PASSWORD ('newpassword');
   FLUSH PRIVILEGES;
   ```

   Enter the exit command to exit from the MySQL DB:
   `exit;`

5. Run the following command:

   ```
   > grant all on *.* to 'reportuser'@'' identified by 'reportuser' with grant option;
   > flush privileges;
   ```

   By default, the reportuser, username, and password is reportuser.

6. Try logging in from MySQL with the reportuser and new password.

For an Oracle database:

`ALTER user IDENTIFIED BY`

For the Application Server:

1. Open command prompt and navigate to the `%AGILIANCE_HOME%\install\toolbox\bin` directory.
2. Run the command: `encrypt.cmd` to encrypt the reportuser password.
2. Copy the encrypted password.
3. Open the `%AGILIANCE_HOME%\config\agiliance.properties` file and set the following property:
   `jasper.reportuser.password.encrypted=EncryptedString`
4. Restart the Application server.

For the Report Server:

1. Open the `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\agiliance.properties` file.
2. Set a password for property:

   For a MySQL database:
   `database.mysql.password.encrypted=EncryptedString`
   For an Oracle database:
   `database.oracle.password.encrypted =SchemaUserPasswordinEncryptedString`

3. Restart the ReportServer.

4. On the RiskVision Report Server host, open a web browser, enter the URL `http://:/jasperserver-pro/-login.html` that will allow you to log in to the RiskVision Report Server in a standalone mode.
5. Log in with sysadmin credentials (username as sysadmin and password as agiliance)
6. On the **View** menu, click **Repository**.
7. Expand the **Public** folder, then click **Data Sources**.
8. Edit the RiskVision JDBC data source.
9. Enter the new reportuser password.
10. Test the connection.
11. Click **Save**.
12. Restart the jasperreportsTomcat service.

Change the rvJasperUser Password

To change the rvJasperUser password:

1. Go to the JasperReports Server host and open http://localhost:8480/jasperserver-pro/login.html using a browser to open the JasperReports Server login page is displayed.
2. Go to **Manage** > **Users**
3. Click rvJasperUser.
4. Click Edit.
5. Change the password.

To use an unencrypted password to set the property:

1. Open the `%AGILIANCE_HOME%\config\agiliance.properties` file using a text editor.
2. Set the `jasper.rvUserWebServicePwd` property to the new password. The password can be read because it remains visible in the property.
3. Restart the RiskVision Tomcat service to apply the changes.

To use an encrypted password to set the property:

1. Open the command prompt and navigate to the `%AGILIANCE_HOME%\install\toolbox\bin` directory.
2. Enter the command: `encrypt.cmd .` This password must be confidential.
3. A new password is generated in the encrypted format.
4. Copy the encrypted password and paste the password in the `agiliance.properties` file.
5. Set the `jasper.rvUserWebServicePwdEncrypted` property to the password in encrypted form.
6. Restart the Application server Tomcat to apply the changes.

Change the Sysadmin Password

To change the password for the sysadmin user:

1. Go to the JasperReports Server host and access http://localhost:8480/jasperserver-pro/login.html using a browser.
2. Go to **Manage** > **Users.**
3. Click **sysadmin user**.
4. Click **Edit**.
5. Change the password.

Change the PostgreSQL Account Password

To change the password for the PostgreSQL account:

1. Open command prompt and navigate to the `%JASPER_HOME%\postgresql\bin` directory.
2. Run the following commands:
   ```
   psql -U postgres -d jasperserver
   alter user postgres with password '';
   ```
   The default password for the postgres user is `agiliance`.
3. Open command prompt again, making sure you select **Run as Administrator**.
4. Run the following commands:
   ```
   set PGPASSWORD=
   set ks= %JASPERREPORTS_HOME%\config_ks
   set ksp= %JASPERREPORTS_HOME%\config
   ```
5. If you have changed the Postgres database password, open the `%JASPER_HOME%\buildomatic\default_master.properties` file using a text editor and perform the following:
   - Enter the database password in the following property:

     `dbPassword=`

     The must be entered in clear text
   - Delete the following property:
     `encrypt.done=true property`
   - Add the following property:
     `encrypt=true`
6. Open command prompt, navigate to the `%JASPER_HOME%\buildomatic` directory, and run the command `js-ant refresh-config.`
7. Open the Report Server. Replace `external.jdbc.password` with the generated encrypted password from the `%JASPER_HOME%\buildomatic\default.master.properties` file to the `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\js.externalAuth.properties`
8. Restart the jasperreportsTomcat and jasperreportsPostgreSQL services to apply the changes.
9. Perform the following steps on the Application server:
   1. Encrypt the postgresSQL password using `%AGILAINCE_HOME%\install\toolbox\bin\encrypt.cmd`
   2. Copy the encrypted postgresSQL password, and open the `%AGILIANCE_HOME%\config\agiliance.properties` file and set the below mentioned properties:
      1. `jasper.database.password`
      2. `database.jasper.admin.password.encrypted`

      Note: These values are the encrypted password.
10. To copy the passwords from the Report server to Application server, perform the following:
    1. Go to the `%JASPER_HOME%\buildomatic\build_conf\default` directory and copy `js.jdbc.properties` password properties for postgresSQL metadata.
    2. Replace the copied properties onto `js.jdbc.properties` file in the `%AGILIANCE_HOME%\buildomatic\build_conf\default` directory.
    3. Restart the RiskVision Tomcat service to apply the changes successfully.

Generate a Ciphertext Password for the JNDI Datasource

This section describes the steps to manually generate a password and copy it to `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\META-INF\context.xml.`

To generate a ciphertext password:

1. Open the `default_master.properites` file.
2. Set the value of RiskVision Reportuser Password to the dbPassword property (dbPassword is for the PostgreSQL database but for a workaround to generate RiskVision password we can use the dbPassword temporarily)
3. Set `encrypt=true`
4. Set `propsToEncrypt=dbPassword` ,sysPassword
5. In command line go to `%JASPER_HOME%\buildomatic`
6. Run `js-ant refresh-config` This will replace the password value with the encrypted format.
7. Get the encrypted value of the dbPassword property and use that in the `context.xml`
8. Revert the value of the dbPassword with the PostgreSQL database password.
9. Change `encrypt.done=true` to `encrypt=true`
10. Run step 5 and 6 again to fix the PostgreSQL password.

Restore SSL Encryption for MySQL

The SSL encryption for MySQL must be disabled to upgrade the RiskVision Server. After upgrading the RiskVision Server components, restore the SSL encryption for MySQL.

To restore SSL encryption:

1. Go to the `%AGILIANCE_HOME%\MySQL\config` directory. Open the my.ini file by using a text editor. The upgrade process will overwrite the old my.ini file. Once the back up for the RiskVision configuration is complete, then changes must be completely backed up. For more information, see Backing up the RiskVision Configuration. Locate the Client and Server Sections in the `my.ini` file and uncomment the lines shown in the respective sections below.

- Client section

```
#ssl-ca="~/ca-cert.pem"
#ssl-cert="~/client-cert.pem"
#ssl-key="~/client-key.pem"
#ssl-cipher=DHE-RSA-AES256-SHA
```

- Server section

```
#ssl-ca="~/ca-cert.pem"
#ssl-cert="~/server-cert.pem"
#ssl-key="~/server-key.pem"
#ssl-cipher=DHE-RSA-AES256-SHA
```

Where "~" denotes certificate's directory

2. Go to the back up folder location where the old my.ini file resides. Open the file by using a text editor. Look for the custom settings that you made before upgrading the RiskVision Server. For example, you might have set the MySQL database port other than 3306. Carefully, incorporate all such settings from the old my.ini file into the new my.ini file.

   Apply the custom setting to the new my.ini file by manually editing the new `my.ini` file. Do not overwrite the new `my.ini` file with the old `my.ini` file.

3. Go to the `%AGILIANCE_HOME%\config` directory, open the agiliance.properties file by using a text editor, and perform the following changes:

- Set the property to: `database.mysql.url=jdbc:mysql://:/?verifyServerCertificate=true&useSSL=true&requireSSL=true`

  By default, the MySQL database port number is 3306.

- Uncomment the property: `#database.mysql.useSSL=true`

4. Connect to the MySQL database and run the following commands to enable the SSL encryption:

```
mysql > GRANT USAGE ON .* TO 'agliance'@'' REQUIRE SSL;
mysql > GRANT USAGE ON .* TO 'reportuser'@'' REQUIRE SSL;
mysql > FLUSH PRIVILEGES;
```

5. Restart the RiskVision Tomcat and RiskVision MySQL services to apply the latest changes.

Grant the 'reportuser' User the Permission to Access Views

This section is for customers using an Oracle database. If you experience issues creating or running the JasperReports Server application due to denied permissions or a missing table or view in the Oracle database, you must grant the **reportuser** user permission to access the required view to run the reports.

To grant the 'reportuser' user with the permission to access the views:

1. Open command prompt and navigate to the `%AGILIANCE_HOME%\RiskVision\Utils` directory.
2. To obtain the password in an encrypted format, enter the following command:

   `encrypt.cmd`

   A new password is generated and appears in an encrypted format.
3. Go to the `%AGILIANCE_HOME%\config` directory path, open the `agiliance.properties` file by using a text editor, and add the following properties:
   - `jasper.reportuser.name`
   - `jasper.reportuser.password.encrypted`
   - `database.oracle.admin.password.encrypted` (in encrypted format) (required, only if the Daily Server and Database Hot Backup job is accountable for backing up the Oracle database)
4. Open the command prompt, navigate to the directory `%AGILIANCE_HOME%\Install\Toolbox\bin`, and enter the `assign_jasper_permissions.cmd` command. The permissions are granted.

Replace and Revert Your MySQL Configuration

This section is applicable only to customers who are using a MySQL database and want to utilize the system memory of a host where their MySQL database is deployed to the fullest extent.

Replacing the MySQL Configuration

When you install or upgrade your RiskVision server, the installer will place the `my.ini` file in the `%AGILIANCE_HOME%\install` directory > **MySQL** folder. The Upgrade wizard also copies the `my-4CPU-8GB.ini` and `use_4CPU_8GB_mysql_ini.bat` files into the `%AGILIANCE_HOME%\install\mysql` directory. The `use_4CPU_8GB_mysql_ini.bat` file is used only if the MySQL database is deployed on the host with at least 8 GB of system memory to optimize the response time of the MySQL database.

To change the MySQL configuration on a host with at least 8 GB of system memory:

1. Ensure your RiskVision Server has been upgraded to the latest version. To upgrade, see the steps in Upgrade Process Map For Single Tier RiskVision Setup, or Upgrade Process Map For N-tier RiskVision Setup
2. Go to the `%AGILIANCE_HOME%\install\mysql` directory in the system that hosts the MySQL database.
3. Double-click the `use_4CPU_8GB_mysql_ini.bat` file to run the script. Allow sufficient time to run the script. After the script is complete, all the properties in the file `my.ini` are replaced with the properties specified in the `my-4CPU-8GB.ini` file.
4. Restart the RiskVision Tomcat service to apply the latest changes.

With the modified configuration `my.ini` file, RiskVision should load more quickly.

Revert to the Default MySQL Configuration

The file `use_default_mysql_ini.bat` provides the capability to revert the current running MySQL configuration to the default configuration. This script must be run if you want to revert changes either from the `my.ini` file or from running the `use_4CPU_8GB_mysql_ini.bat` script.

To revert the changes:

1. Go to the `%AGILIANCE_HOME%\install\mysql` directory in the system that hosts the MySQL database.
2. Double-click the `use_default_mysql_ini.bat` file to run the script. Allow sufficient time to run the script, and after the script is executed, the configuration will be reverted to the default state.
3. Restart the RiskVision Tomcat service to apply the latest changes.

Back up Your ReportServer Configurations

Configuring Daily Database and Database Hot Backup Jobs

> When upgrading a multi-tier setup, run the Daily Database and Hot Backup Job after any upgrade or installation, and check whether the Jasper repository and database backup is successful. If the Jasper repository backup and database backup fails, proceed with the following steps.

Once you have completed your upgrade or installation:

1. Navigate to the **js.jdbc.properties** properties file. The default location is:<%JASPER_HOME%>\buildomatic\build_conf\default directory
2. Copy the file.
3. Replace the **js.jdbc.properties** file with the copied file on the <%AGILIANCE_HOME%>\buildomatic\build_conf\default directory where the Application Server is installed.

   If you have a multi-tier setup, add your Jasper Server name to this line:

   metadata.jdbc.url= jdbc:postgresql://:5432/jasperserver

4. Retrieve the Jasper repository backup:
   a. Go to the **%Jasper_Home%\config** directory on the JasperReports Server host.
   b. Copy the **.jrsksp** file.
   c. On the RiskVision Tomcat host, paste the **.jrsksp** file into the desired backup folder.
   d. Go to **%Agiliance_Home%\buildomatic Edit js-export.bat.**
   e. Append the command **-Duser.home=**

      For example:

      If the file was placed on **C:\Server**:

      set JAVA_OPTS=%JAVA_OPTS% -Xms1024m -Xmx2048m -XX:PermSize=64m

      Would become:

      set JAVA_OPTS=%JAVA_OPTS% -Xms1024m -Xmx2048m -XX:PermSize=64m **-Duser.home=C:\Server**
5. On the JasperReports Server host, go to **%Jasper_Home%\config_ks.**
6. Copy the **.jrsks** file
7. In the RiskVision Tomcat host, create the same Jasper_Home path as above and paste the copied**config_ks** directory into the path.

   For example:

   If the **.jrsks** file is located at C:\ReportServer\ReportServer\config_ks, create the same directory in the RiskVision Application Server. Paste the **.jrsks** file into the directory.
8. Restart RiskVision and Jasper Services.
9. Access RiskVision and run the Daily Server Backup and Database Hot Backup jobs.

File Encryption

There are two types of files that RiskVision encrypts:

- Files that have been uploaded to RiskVision (e.g. questionnaire evidence, files added to the document repository, and attachments to entities, tickets, etc.); and
- Any reports archived using the R6 Reporting engine.

If the RiskVision Server is running any version that is 8.5 GA or higher, the above files will be automatically encrypted using AES 256 bit encryption. However, it is possible that some installations have disabled automatic encryption or chose to opt out during the upgrade. If this has happened, the server's encryption can be re-enabled.

Re-enabling automatic encryption will encrypt all files in the following folders:

- **%RISKVISION_HOME%\data\attachments**
- **%RISKVISION_HOME%\data\reports**
- **%RISKVISION_HOME%\data\dashboards**

Once automatic encryption has been re-enabled, all future files in the above folders will be encrypted. However, in order to encrypt existing files, the encryption utility to encrypt existing files must be run again. The below steps will show both how to re-enable automatic encryption and how to run the utility. If automatic encryption were to be disabled for any reason, all files in the above folders would lose their encryption.

These steps will only work for RiskVision version 9.5 or higher.

To re-enable automatic file encryption:

1. Navigate to **C:\Server\config**.
2. Open the **agiliance.properties** file.
3. Change the following properties as shown:
    - `Attachment.EncryptionEnabled=true`
    - `Attachment.newVersion=true`
4. Copy the **esapi** folder from **C:\AGILIANCE_HOME\Tomcat\webapps\spc\WEB-INF\classes** and paste it into **C:\AGILIANCE_HOME\install\toolbox\bin**.

To encrypt existing files:

1. Navigate to the **AGILIANCE_HOME\install\toolbox\bin** folder.
2. Run the following commands:
    - `encrypt_attachment_directory.cmd > attachment.log`
    - `encrypt_data_directory.cmd > data.log`

Re-import LDAP Certificate

Sometimes, after upgrading to RiskVision version 9.4 or above, users are unable to connect to the LDAP source, such as Active Directory, and receive the following error message:

Please check directory server configuration details for domain: qateam.local. javax.naming.CommunicationException: simple bind failed: [hostname]:636 [Root exception is javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

When this happens, re-importing the LDAP certificate will allow users to access Active Directory.

To re-import the LDAP certificate:

1. Open the command prompt and navigate to where the LDAP certificate was previously imported. By default it should be in the **%AGILIANCE_HOME%\apache2\conf\server.crt** folder.

2. Re-import and store the certificate in the **C:\SecureLDAP\keystore.cer** folder by running the following command all in one line:

    - `keytool -import -alias ldap1 -keystore %AGILIANCE_HOME%\Java\jre\lib\security\cacerts -trustcacerts -file C:\SecureLDAP\keystore.cer`

    > While importing the certificate, the system will prompt for keystore password. The default keystore password for cacerts is **changeit**.

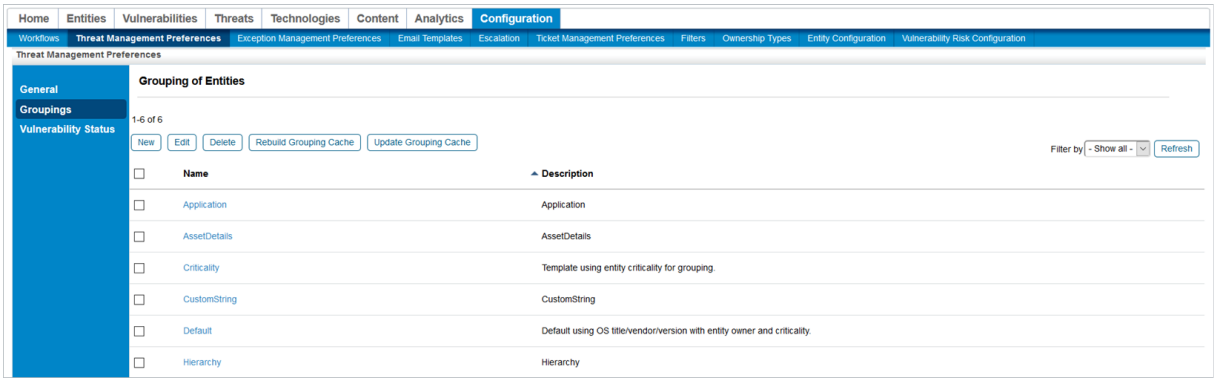
3. Restart the Tomcat server and check your LDAP connection again.

Fix the Risk Score Display

When upgrading to RiskVision 9.5 or higher, there might be an issue where the **Risk Score** column of a vulnerability's Affected Entities tab does not display with a decimal place. In order to display the risk scores properly, a RiskVision administrator must run the **Rebuild Grouping Cache** job be following the below steps:

To run the Rebuild Grouping Cache job:

1. Log on with an administrator account.
2. Open the **Threat and Vulnerability Manager** application.
3. Navigate to **Configuration** > **Threat Management Preferences**.
4. Navigate to the **Groupings** tab and click **Rebuild Grouping Cache**.



The Groupings tab.

In some cases, the Rebuild Grouping Cache job may not run correctly and the Vulnerability Risk score will display as N/A. If this happens, follow the below steps.

To resolve a failed Rebuild Grouping Cache job:

1. Execute the following queries in the database to get more details:
   - `Select * from agl_jobrun;`
   - `Select * from agl_db_log;`
2. Observe the results after executing the above queries. You should see the following text if the queries were executed successfully:
   - `ORA-0001:unique Containt(AGLDB.PK_AGL_ASSET_FACTOR_CUSTOMATTR) violated found in the agl_db_log`
3. Execute the below query to check for duplicate records in the custp, attributes table:
   - ```
     select object_id, attrib_level, count *
     from agl_customattributes group by object_id, attrib_level having count * > 1
     ```
4. If the above query returns any record, update the**object_id** to null.
5. Run the Rebuild Grouping Cache job.

If the above steps do not resolve the issue, contact Resolver Support.
     ```

Run NVD Tenant Tool

After upgrading to 9.6 of RiskVision, some users may see duplicate CPEs in their RiskVision environment. In order to resolve this issue, a new NVD Tenant tool must be run after upgrading to 9.6.

To run the NVD Tenant tool:

1. Stop the Tomcat service.
2. Open the Command Prompt as an administrator.
3. Naviagte to the **C:\Server\install\toolbox\bin** folder.
4. Execute the **migrate_NVD_tenant.cmd** tool.
5. **Optional**: Run the Post Installation scripts if you have an Oracle database.

View Technologies in 2.3 Format

One of the features of RiskVision version 9.6 is the ability to view a technology's CPE URI in a 2.3 format. However, this feature will not be enabled by default for existing CPEs. Users who have upgraded to version 9.6 from a previous version and using the VulnDB connector should request an updated Groovy file from services in order to properly display CPE 2.3 URIs. In addition, users should import the NVD CPE dictionary using NVD connector to view the existing CPE's in 2.3 version.

Minor Version Upgrade Installer Overview

The **Minor Version Upgrade** file is an installer that allows users to upgrade the following third-party software to the latest supported versions required to run the most recent version of RiskVision:

- Apache Tomcat
- Apache Web Server
- Oracle MySQL
- Java

> This installer only supports **minor** upgrades of the required third-party software. For example, upgrades from version 1.0.1 to 1.0.2 can be done via the installer, but 1.0 to 1.1 cannot.

Before upgrading, ensure all requirements in the Minor Version Upgrade Installer Prerequisites article are met. For instructions on running the installer, see Run the Minor Version Upgrade Installer article.

> RiskVision 9.2 can only run Apache Tomcat up to version 8.5.35. Users who wish to use Tomcat version 8.5.35 or above must update their RiskVision software to version 9.3.

Minor Version Upgrade Installer Prerequisites

Before the **MinorVersionUpgradeInstaller.exe** file can be run, the following prerequisites must be met:

- RiskVersion 9.2 or later is installed. If you're running this installer as part of a new installation, ensure the RiskVision installation is complete before upgrading the third-party software.
- The following third-party libraries have been previously downloaded and installed:
    - Apache Tomcat
    - Apache Web Server
    - Oracle MySQL
    - Java

    If one or more of these components are not on your machine at the time the Minor Version Upgrade installer is run, as may be the case with 4-tier setups, they will not will not appear in list of components eligible for upgrade. For more information or to obtain links for download, contact Resolver Support.

- The third-party software being updated requires only **minor** upgrades. For example, an upgrade from version 1.0.1 to 1.0.2 can be done via the installer, but 1.0 to 1.1 cannot.
- The user performing the upgrade has Administrator privileges on the system the installer is being run on.
- If you're upgrading Java or Apache Web Server, you must contact Resolver Support for further assistance.

Run the Minor Version Upgrade Installer

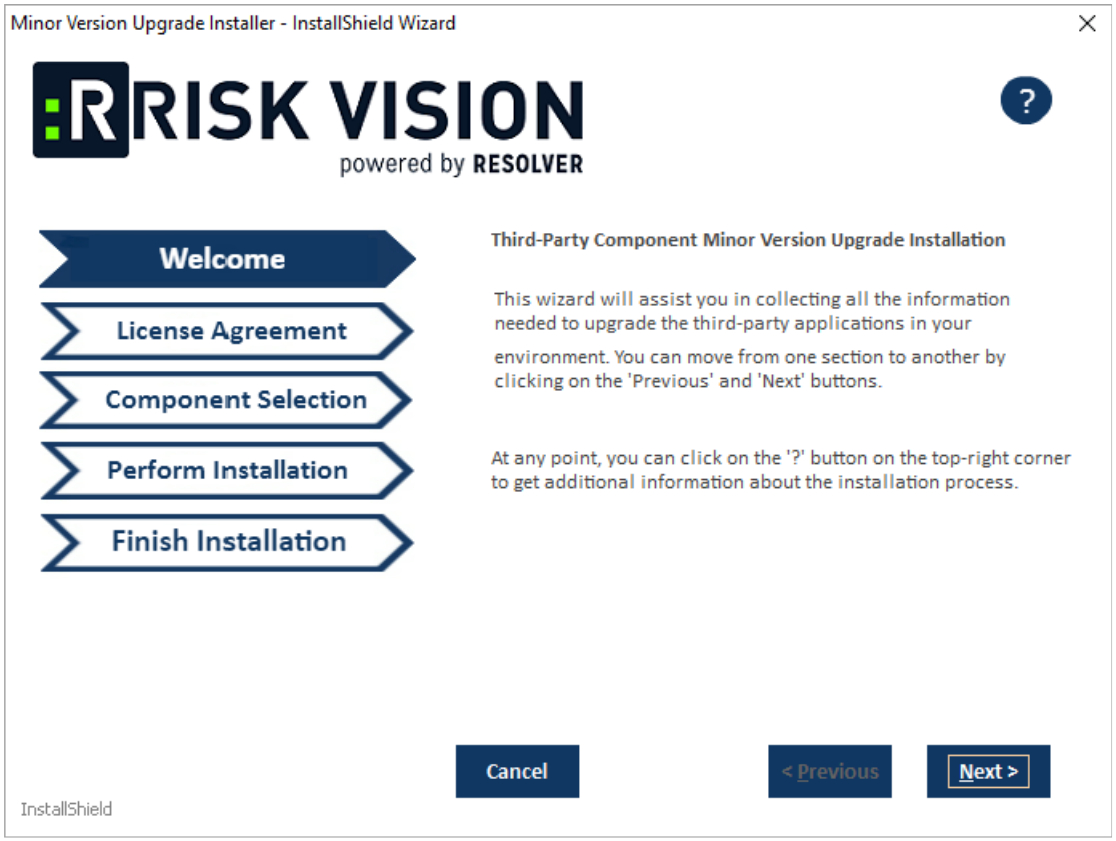
Important Notes

Before running the installer, note that:

- All the requirements in the Minor Version Upgrade Installer Prerequisites article must be met.
- Only minor upgrades of Apache Tomcat, Apache WebServer, Oracle MySQL, and Java can be performed through this installer.
- If you experience persistent errors in running the installer, contact Resolver Support for further assistance.

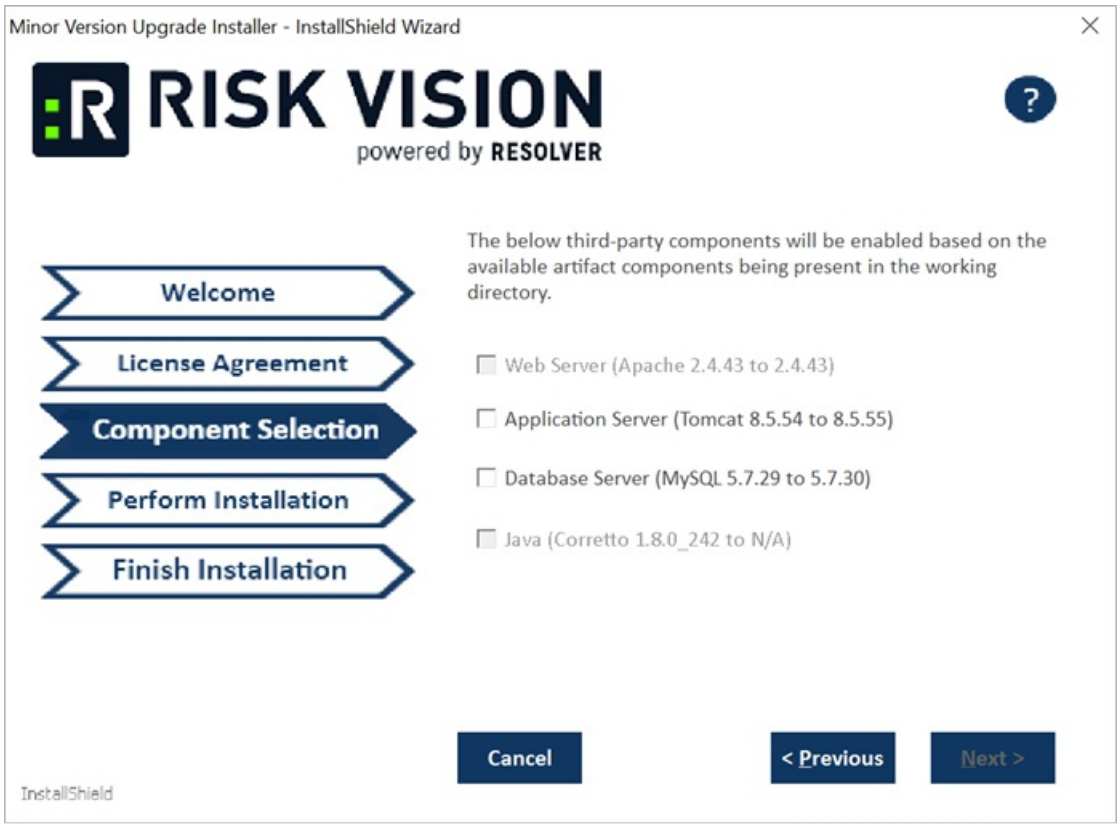
To run the Minor Version Upgrade installer:

1. Ensure that you have local administrator privileges on Windows Server 2008, Windows Server 2012, or Windows Server 2016 User Account Control (UAC) is disabled, and all RiskVision services, such as MySQL, are running.
2. Navigate to the folder where the installer is saved, ensuring the required third-party libraries are present in the same folder.
3. Right-click the **MinorUpgradeInstaller.exe** file, then click **Run as administrator**.
4. Enter your admin username and password in the **User account control** dialogue box, then click **Yes** to launch the installer.



The Welcome screen of the installer.

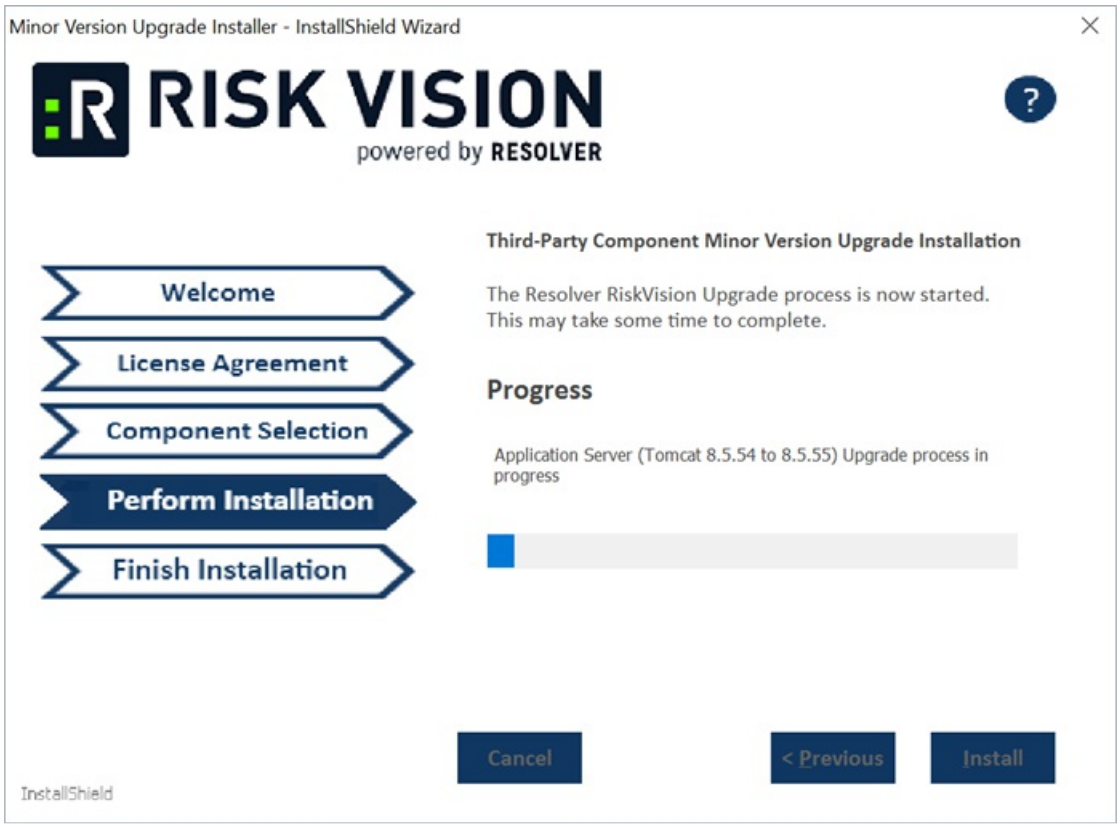
5. Click **Next** to view the **License Agreement** screen.
6. Review the license agreement, then select the **I accept the terms of the license agreement** radio button.
7. Click **Next** to view the **Component Selection** screen.
8. Select the checkboxes beside the components you wish to update.



The Component Selection screen.

If the services for one or more of the third-party components are not installed on the current server, those components will not be clickable on the **Component Selection** screen.

9. Click **Next** to begin the installation. To view the log file for installation statuses and any error messages, open the **MinorVersionUpgrade.txt** file in the installer directory.

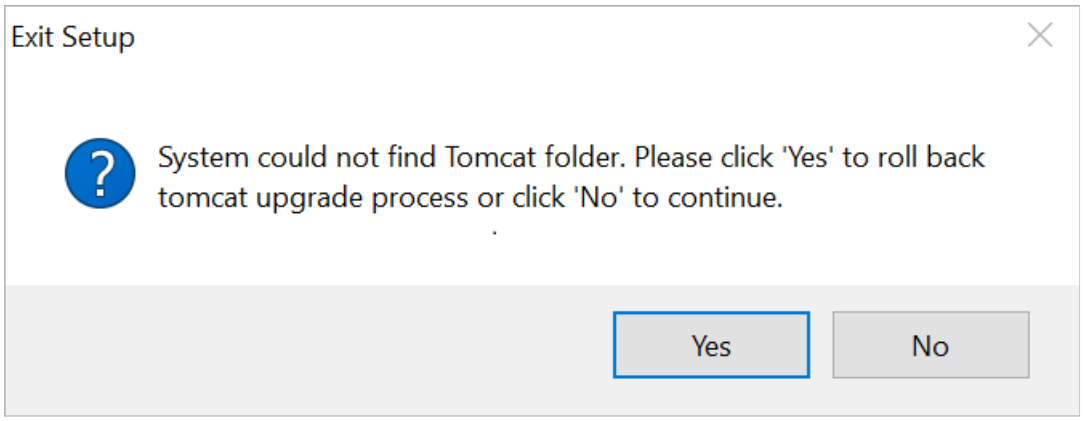


The Perform Installation screen.

10. Click **Finish** to close the installer once installation is complete.

The Finish Installation screen.

11. **Optional:** If the upgrade has failed for any reason, an error message similar to the below will display, depending on which component was unable to be upgraded. Click **Yes** to roll the specified component back to its previous version.



An example of an error message that appears in the event of upgrade failure.

Appendix B: Installation Log Files

This section discusses the log files for different components installed in your environment. Log files record almost everything - user operations, errors, and more - and are used by Technical Support as first-hand information to troubleshoot the reported problems. Therefore, it is important not to modify any of the log files. The default location of the log files for various components are mentioned in the table below:

Component	Directory	Log File
RiskVision Server (Application Server, Web Server, and Database Server (MySQL))	The folder where the installer is running.	install.log
	The folder where the upgrade is running	upgrade.log
	%AGILIANCE_HOME%\install\toolbox\bin	upgradedb.log
RiskVision Job Manager	%AGILIANCE_HOME%\Services\RC\logs	agiliance.log
		wrapper.log
RiskVision MySQL	%AGILIANCE_HOME%\MySQL\logs	agiliance.errors
RiskVision Apache	%AGILIANCE_HOME%\apache2\logs	access.log
		error.log
		https_access_yyyy_mm_dd.log
		https_error.log
		mod_jk.log
	%AGILIANCE_HOME%\backup_apache2\logs	rewrite.log
RiskVision Tomcat	%AGILIANCE_HOME%\Tomcat\logs	agiliance.log
		catalina.log
		commons-daemon.yyyy-mmdd.log
		hibernate.log
		host-manager.yyyy-mm-dd.log
		localhost.yyyy-mm-dd.log
		manager.yyyy-mm-dd.log
		pdperror.log
		tomcat8-stderr.yyyy-mm-dd.-log
		tomcat8-stdout.yyyy-mm-dd.-log
		error.log
JasperReports Server	%JASPER_HOME%\	installation.log
	%JASPER_HOME%\Agiliance\scripts\	install.log
		initdb.log
		output.log
JasperReports Server Tomcat	%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\logs	jasperserver.log
	%JASPER_HOME%\apache-tomcat\logs	jasperreportstomcatstderr_yyyymmdd.log
		jasperreportstomcatstdout_yyyymmdd.log
		commons-daemon.yyymmdd.log
RiskVision connectors	%AGILIANCE_HOME%\\logs	agiliance_.log