Table of Contents

System Overview

RiskVision runs an enterprise web application on an Apache Tomcat server. Users with different roles can set up and use RiskVision to perform IT-GRC tasks, such as:

- Creating users, teams, and roles;

- Defining and storing information about assets and entities;

- Setting up assessment programs and defining the process to evaluate compliance and risk;

- Evaluating vulnerabilities and controls; and

- Reporting on all aspects of an organization's risk and compliance status.

Users monitor and control RiskVision operations based on the roles and associated permissions assigned to them by their RiskVision administrator.
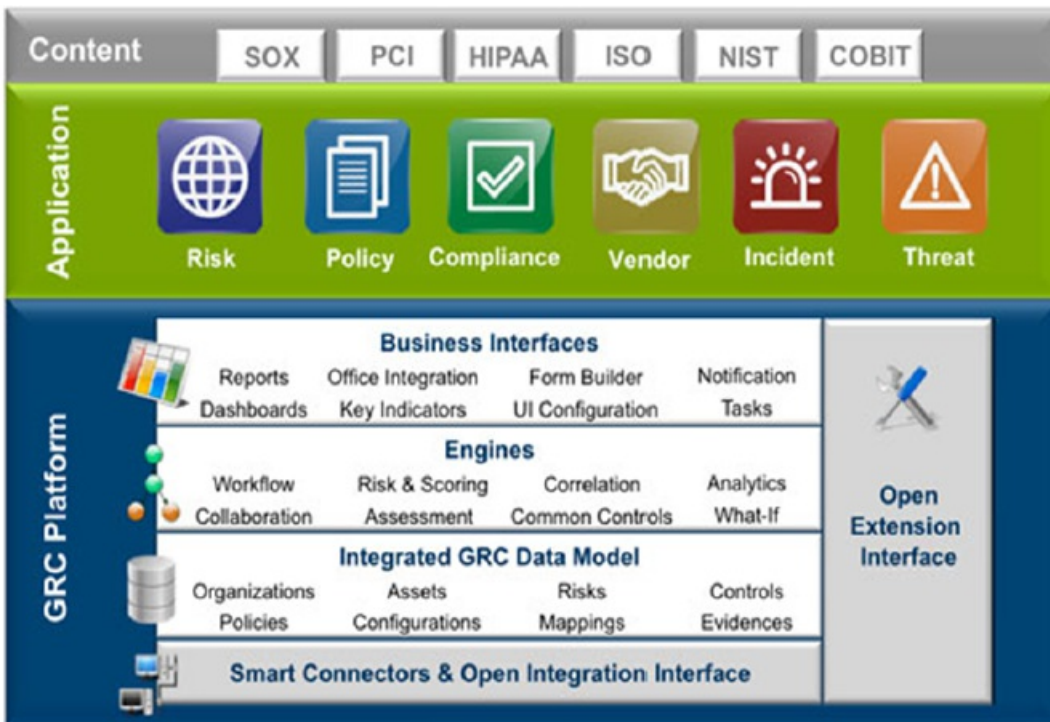
RiskVision System Architecture.

RiskVision stores all data, such as risk information and questionnaire responses, in a relational database.

Additional connectors installed and configured in your environment can extend the system's capability. For example, customers can use connectors to automatically evaluate and return control results, evaluate and send vulnerability information to RiskVision. Connectors can also be used to integrate with other third-party applications and systems that provide services such as security event detection, and vulnerability scanning and tracking.

To start using RiskVision, you must connect the RiskVision Server computer to a network that has TCP/IP connectivity. Depending on your requirements, installing RiskVision on the same network as the systems and computers you want to evaluate may provide additional monitoring, management, or reporting capabilities.

About RiskVision

RiskVision is comprised of several of separately-licensed applications that share a common user interface and underlying components. Depending on your license, the list at the top of your console may not include all of the applications shown here. The **Administration** link is used for managing users, connectors, and other configuration tasks across your installed applications.

The current application workspace is part of the URL. Users can bookmark specific RiskVision pages to start on any desired page within any particular application.

ICON	APPLICATION	DESCRIPTION
✅	Compliance Manager	Compliance Manager allows an organization to effectively manage and measure compliance programs across multiple regulations, standards, and frameworks. It automates the compliance process through general computer controls (GCC) and questionnaires. Evidence and control results can be automatically collected through connectors or questionnaire results from business users. Compliance Manager enables data classification, ownership configuration, compliance assessment, mitigation, and reporting. It supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI, and others. Compliance Manager improves process efficiency and integrity as well as data quality and reliability.
🌐	Enterprise Risk Manager	Enterprise Risk Manager is a comprehensive risk lifecycle management solution. Using Enterprise Risk Manager, a company can identify, assess, and mitigate risk with an appropriate risk treatment plan. Its flexible risk model supports both qualitative and quantitative methodologies, including calculation of inherent risk, current risk, and residual risk within the context of mitigating controls. This application features rich reports and dashboards, as well as easy to use risk assessment tools. It will help your organization understand and monitor its enterprise risk position by providing out-of-the box support for popular risk methodologies, such as COSO, AZ/NZS 4360 and ISO.
👁	Vendor Risk Manager	Vendor Risk Manager helps organizations audit and manage third-party risks, as mandated by regulations and standards, such as ISO 27001, PCI, and FISMA. This application classifies, assesses, and reports on third-party risk, based on the standard control framework from shared assessment programs, or an organization's custom control framework. Vendor Risk Manager provides a portal where vendors participate in assessments and the results are retrieved by an organization's risk analysts. Vendors are classified automatically into appropriate tiers and applicable controls are applied based on the vendor tier. Powerful delegated administration and automation features allow Vendor Risk Manager to scale to large numbers of vendors.
⚠	Threat and Vulnerability Manager	Threat and Vulnerability Manager allows organizations to consolidate their threat and vulnerability programs on a single platform. It integrates vulnerability and early warning data feeds from iDefense and National Vulnerability, and correlates these feeds with vulnerability scanner results to eliminate false positives and report incidents. Inferred scans are performed by correlating the vulnerability data feeds to a company's RiskVision asset database, which mitigates risks for assets not reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and remediated using the system's workflow for true closed-loop vulnerability management.
		Policy Manager manages enterprise policies on a single centralized platform. Organizations

	Policy Manager	can enforce policy and process standards across different locations, departments, and programs. Policy Manager supports simultaneous policy editing across multiple stakeholders using a rich WYSIWYG user interface. An organization can automate processes for policy authoring, reviewing and approval. Policy templates help enforce consistent formatting and structure. Policy Manager has a highly configurable workflow which allows your organization to enforce change control and maintain accountability. It supports policy awareness campaigns with policy distribution, attestation, and comprehension testing tools.
	Incident Manager	Incident Manager allows organizations to collect, classify, and manage multiple IT and non-IT incidents. It's a single collection point for all manually reported and automatically imported incidents. It imports incidents reported from most monitoring systems and scanners as well as Security Incident Management (SIM) solutions. All incidents, including business, operational, and environmental can be reported in the incident-reporting portal. Incidents are assessed based on a configurable workflow and automatically created and classified based on rules that are tracked throughout the incident's lifecycle. Incidents are tied to controls, policies, and risks to provide closed loop feedback for policy and control assessment and risk monitoring. Incidents are rated based on the criticality so that organizations can respond based on the impact to the business.

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 Installer section 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 |

Required Components

Below is a list of required server components. Each version of RiskVision has its own list of requirements that can be reviewed on its release page.

Apache Web Server

Apache Web Server is the web server that is most commonly used with RiskVision and RiskVision Report Server (JasperReports Server). The Apache Web Server is used to provide web pages requested by RiskVision client computers. Clients typically request and view web pages using web browser applications, such as Firefox, Internet Explorer or Chrome.

A URL points to the web server using its Fully Qualified Domain Name (FQDN) and a path to the required resource. For example, to view the homepage of the RiskVision Server, you will need to enter only the FQDN. The Apache web server will transfer web pages using the most common protocol called Hyper Text Transfer Protocol (HTTP).

Database Server

Installing the RiskVision Server requires either MySQL (5.7.26) database or an Oracle 12.2.0.1 database. The RiskVision Server Setup Installer wizard can install a MySQL database, provided the required artifacts are obtained from Resolver Support or from the MySQL website.

Deploying RiskVision to use an Oracle database requires setting up both an Oracle server and Oracle client, both of which must be version 12.2.0.1. To add the Oracle client to your deployment, download the Oracle database (12.2.01) from the Oracle website.

Tomcat Application Server

Tomcat Application Server provides RiskVision with services, such as security, data services, transaction support, and management of large distributed systems.

RiskVision Report Server

JasperReports Server is embedded within RiskVision and is used by all application modules. It provides a robust and flexible business intelligence engine for RiskVision data.

Microsoft Visual C++

RiskVision requires Microsoft Visual C++ version 2013 x64 Redistributable - 12.0.30501 in order to run. For versions 9.1 and up, this will be installed automatically as part of RiskVision. Customers wishing to install a version of RiskVision before 9.1 will need to have VC++ version 2013 x64 Redistributable - 12.0.30501 installed on their machine before attempting to install RiskVision.

Open SSL

The latest version of Open SSL is required to run RiskVision as of version 9.4 This will be automatically installed with versions 9.4 and up.

RiskVision Server-Side Connector

The Server-side connector is used for executing the sub-control checks against the data stored in the RiskVision database. Install the RiskVision Server-side connector on the same host as the RiskVision Server. The Server-side connector supports RiskVision system, version 5.0 and above.

RiskVision Connector Manager

The RiskVision Connector Manager acts as a decoupling agent between RiskVision Server and RiskVision Connector. The connector communicates with Connector Manager, and in turn the Connector Manager pushes the data into the database. The RiskVision Server will not be involved in this process. The Connector Manager reduces the load that older, non-web services connectors place on the RiskVision Server.

Jaspersoft Studio Professional Application

The TIBCO Jaspersoft Studio Professional application, from Jaspersoft Corporation, is an eclipse-based report designer for Jaspersoft reports. This application is an improved version of iReport Designer Professional application, that allows creation of reports from sources such as JDBC, TableModels, JavaBeans, XML, Hibernate, and Big Data in PDF, RTF, XML, XLS, CSV, HTML, XHTML, text, DOCX, and OpenOffice output formats. This is a standalone software application in that it must be installed separately by downloading the installer file from the FTP site or by obtaining the installer file from Resolver Support.

Jaspersoft Corporation has stopped providing updates to the iReport Designer Professional application and may retire it in the near future. We recommend migrating existing reports to Jaspersoft Studio Professional and uninstalling iReport Designer Professional.

See the System Requirements document for information on the latest software requirements.

Minimum Hardware Requirements

This section provides minimum hardware requirements to install the RiskVision platform. You can use virtual environment or physical server to install the RiskVision Server.

The table below lists the minimum hardware requirements:

Hardware	Minimum
Total number of CPU cores	8*
Memory	16 GB*
Disk	At least 100 GB* of free disk space with RAID 1, RAID 5, or RAID 10 as appropriate

UPS is recommended for power management.

By default, the maximum and minimum heap size for jasper-export is 1024M and 2048M. This can be updated whenever you see any out-of-memory exception while executing jasper export.

These requirements represent the **minimum** system requirements to install the RiskVision Server. The recommended requirements will vary according to each customer's use cases and will be provided by your solution architect. Factors that are important to consider include a large number of concurrent users, a sizable number of objects, and a high number of connectors importing a large volume of data.

MySQL and Tomcat require a special configuration to make use of additional memory. For example, running Java Virtual Machine applications such as Tomcat with the parameter -Xmx5120m establishes a maximum heap size of 5GB for Tomcat's use. Make sure to specify a maximum heap size that is well under the physical memory of the server. For information about changing the heap size, see Increasing Tomcat Heap Memory.

Configure the UAC Setting

UAC is a security feature of Windows Vista, Windows 7 and Windows 8 which helps prevent unauthorized changes to your computer. These changes can be initiated by applications, viruses or other users. User Account Control makes sure these changes are made only with approval from the administrator. If the changes are not approved by the administrator, they are not executed and Windows remains unchanged.

To configure UAC:

1. Click the **Start** button and type **UAC**.

2. Click **Change User Account Control Settings**.

3. Drag the slide bar to **Never notify** level, which is the lowest setting

4. Click **OK**.

Increase Tomcat Heap Memory

By default, the Tomcat heap memory is set to 3GB. If recommended by a Resolver Support or Services representative, you may follow these steps to increase the Tomcat heap memory:

1. Go to the `%AGILIANCE_HOME%\Tomcat\bin` directory and double-click the `tomcat8w.exe` file to launch the RiskVision Tomcat properties dialog.

2. Click the **Java** tab and enter a value, in megabyte as required, in the **maximum memory pool** field.

3. Click **Apply** and click **OK** to save and close the dialog.

4. Restart the RiskVision Tomcat service to apply the latest changes.

Operating Environment

- Ensure that no versions of Java™, MySQL™, Tomcat, or Apache have been installed on the target system.

- Any other web servers on the host (such as IIS) cannot run on ports 80 or 443.

- The installer sets the JAVA_HOME environment variable to the JRE bundled with the RiskVision.

Size & Scaling

As part of the pre-installation planning for your RiskVision deployment, Resolver Professional Services can work with you to determine appropriate sizing and scaling of the RiskVision Server to meet your present and future needs. Factors that contribute to resource requirements include the following:

- Number of managed/tracked entities: Computers, processes, applications, users, accounts, non-computer entities, and so on.

- Number of controls and associated subcontrols (automated control checks or manual questionnaire questions).

- Requirements for evidence collection and data retention requirements.

- Number and type of deployed connectors, integration with third parties for other capabilities such as incident tracking, event collection, and remediation.

- Number and type of dashboards and reports.

The successful deployment of your RiskVision Server requires an appropriate archive and backup strategy and tools. Based on your organization's current archive and backup policies and available tools, you may want to ask professional services for assistance.

Contact Resolver Support for more information.

Server Preparation & Hardening

Before or after installing RiskVision, we recommend that you also perform system and server hardening steps.

You may have your own procedures and methods for hardening servers and other requirements specified by your IT organization.

Harden Systems & Servers

- Operating system hardening; disabling or removing any unnecessary applications, closing unused ports, firewall, and system access.

- Remove all non-essential tools and utilities.

- Apply latest patches and upgrades.

- Activate all appropriate security features.

- Lock all ports except as listed in the following table.

- Enable or install firewall protection.

- Anti-Virus software; McAfee may require that the 'MySQL' directory and its sub-directories are excluded. For more information, refer to the McAfee knowledge base.

- Physical security: Install RiskVision solution in a secured location.

Open Ports

While deploying on multiple servers, certain ports must be open to specific servers. When RiskVision is deployed on a single server, open only the ports that are marked as "open to the world."

Server	Port	Open to
Apache	TCP/80	Open to the world (optional)
Apache	TCP/443	Open to the world
Tomcat	TCP/8009	Open to the Apache server*
JasperReports Server	TCP/8409	Open to the Apache server*
MySQL	TCP/3306	Open to the Tomcat server*
Oracle	TCP/1521	Open to the Tomcat server*

*Not applicable for single-server deployment.

Also, see Illustration of Ports in Multiple Server Configuration.

Download Files for Required Components

The table below lists the files you need to install the Resolver RiskVision with the MySQL and Oracle databases and the files required to install the RiskVision Server and the RiskVision Report Server.

File	MySQL	Oracle
riskvision.license	✅	✅
RiskVisionApplicationServerInstallation.exe	✅	✅
jce_policy-8.zip	✅	✅
mysql-5.7.26-win64.zip	✅	❌
mysql-connector-java-5.1.39.zip	✅	❌
Riskvision-part1.zip	✅	✅
Riskvision-part2.zip	✅	✅
Riskvision-part3.zip	✅	✅

Downloading Files for Optional Components

This section covers the list of files and URL location of the optional components.

The table below lists the files required for installing the optional components - RiskVision Connector Manager and Jaspersoft Studio Professional.

File	MySQL	Oracle
RiskVisionConnectorManagerInstallation.exe	✅	✅
TIB_js-jss_7.2_windows_x86_64.exe	✅	✅

To download files for optional components:

1. Navigate to the Submit a request page on the Resolver Support site to create a ticket to request the required installation files.

2. Once Resolver Support has provided the necessary files, copy/save the required files, as specified in the table above, to a local directory, such as `C:\AglTemp`. The path must not have any spaces (for example, `C:\Program Files\Temp` will not work). The installer expects all files to be in a single directory.

To download files if your MySQL database server version is earlier than 5.7.26 and MySQL connector version is earlier than 5.1.39, visit the URLs as specified in the table below:

Filename	URL
mysql-5.7.26-winx64.zip	https://downloads.mysql.com/archives/get/file/mysql-5.7.26-winx64.zip
mysql-connector-java-5.1.39.zip	http://downloads.mysql.com/archives/get/file/mysql-connector-java-5.1.39.zip

You also need to download jce_policy-8.zip file from **http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html**

To obtain files required to set up an Oracle Client, visit the following URL:

http://www.oracle.com/technetwork/database/windows/downloads/index.html

Use the RiskVision Installers

Use the following installers to deploy the RiskVision system.

Product	File	Description
RiskVision Server Setup	RiskVisionApplicatoinServerInstallation.exe	Installs the Apache Web Server, Tomcat Application Server, RiskVision Report Server, RiskVision Job Manager, and Apache OpenOffice
Jaspersoft Studio Professional 6.4.21 final Setup	TIB_js-jss_6.4.21_windows_x86_64.exe	Installs Jaspersoft Studio Professional. Deploy this application on the computer of a report developer. This is a standalone application.
RiskVision Connector Manager Setup	RiskVisionConnectorManagerInstallation.exe	Deploys the Connector Manager application.

Installation Topologies

The RiskVision system can be installed in many different topologies. This section illustrates the most common topologies that help you understand the installation procedure and to choose a topology relevant to your environment. You can distribute the components in any combination, however, recommends opting one of the following topologies for reasonable performance and scalability.

One-tier Topology

The following graphic represents the One-tier topology in which only one server is used for installing the RiskVision Server and its components.
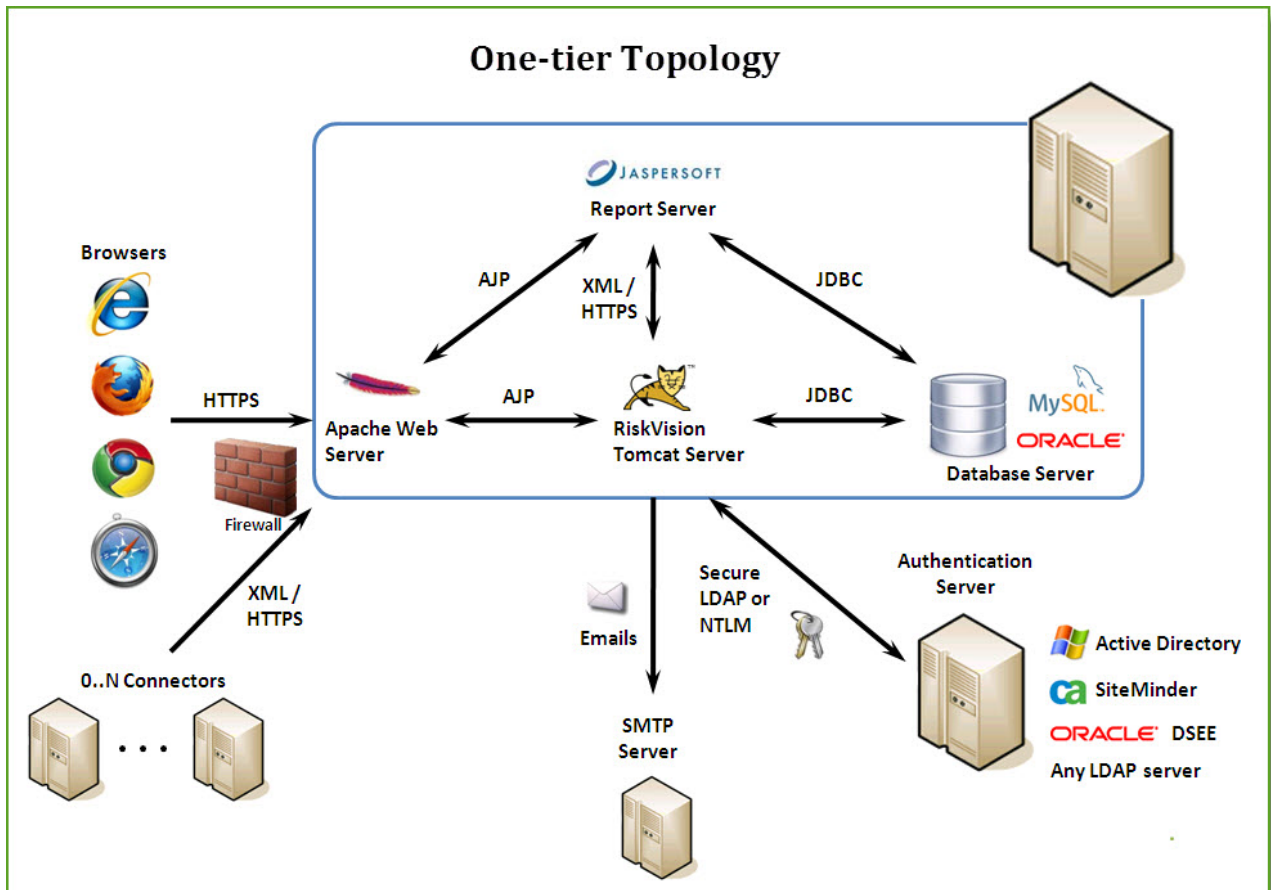
Three-tier Topology

The following graphic represents the Three-tier topology in which three servers are used for installing the RiskVision Server and its components.

Three-tier Topology
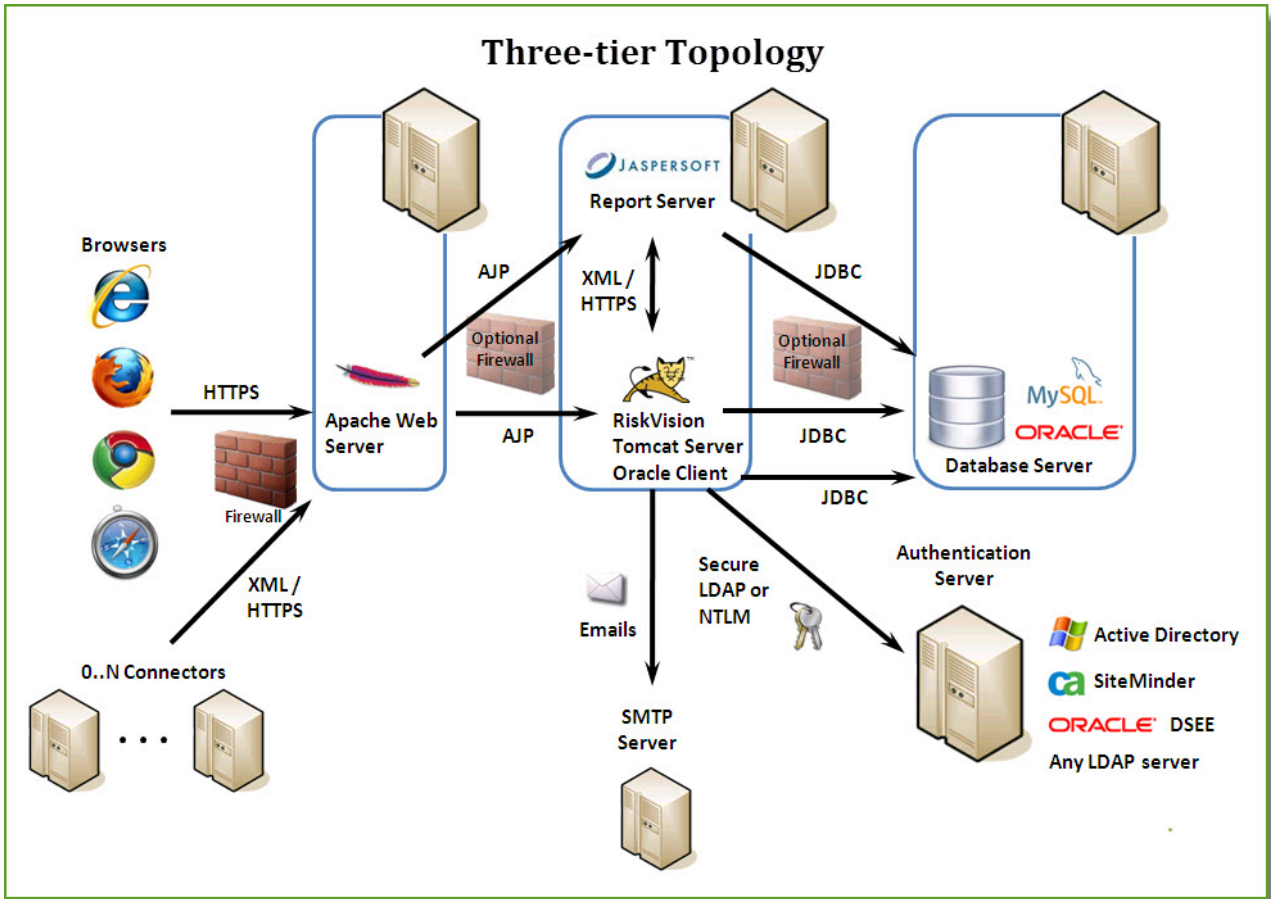
Large Scale Clustered Server Topology

The following graphic represents the large-scale clustered server topology in which four servers are used for installing the RiskVision Server and its components. Install one or more Connector Managers in your environment to achieve data processing at ultra-speed.

Large Scale Clustered Server Topology
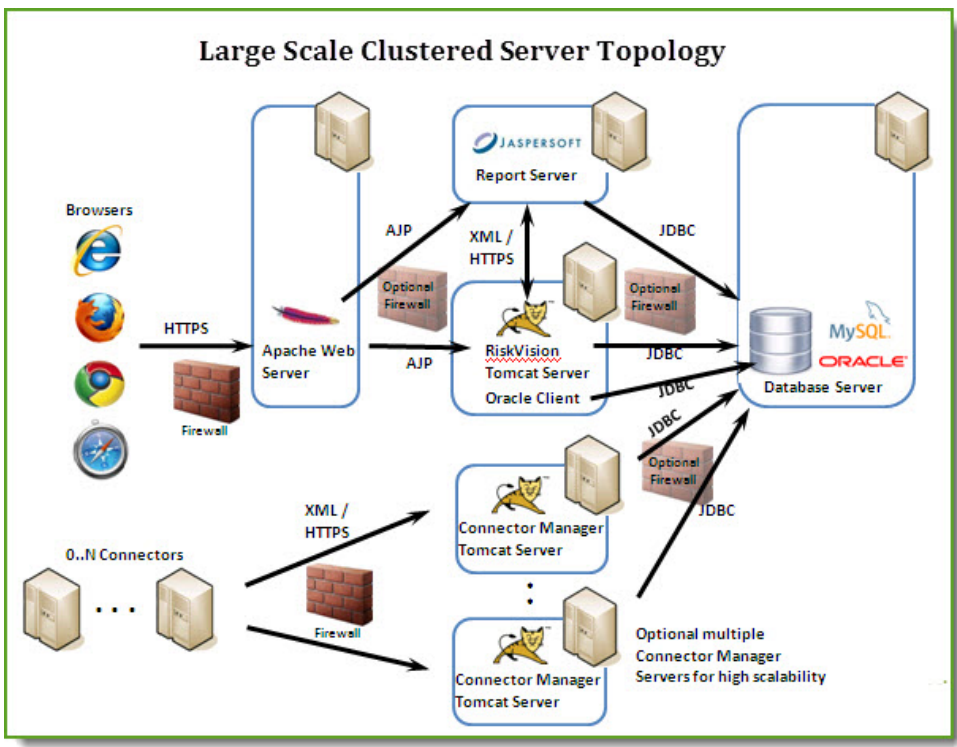
If you have to install the Server-side connector, you must install it on the RiskVision Tomcat application server host.

Ports in a Multiple Server Installation

The following graphic provides the use of ports in a multiple server installation.
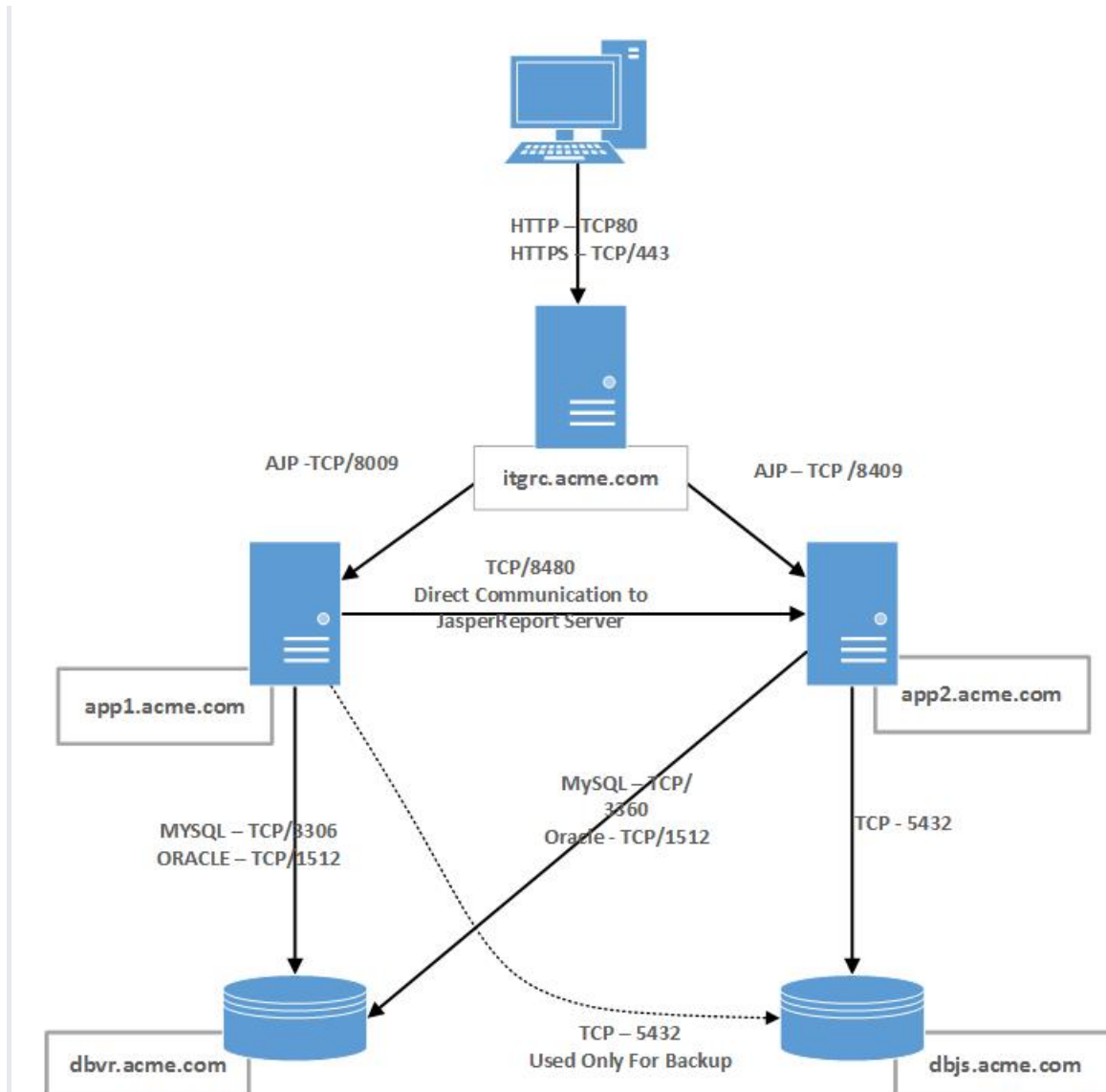
Open Ports

A multi-server installation allows you to open only certain ports between hosts for increased security. Browsers communicate with RiskVision Server components and JasperReports Server using the HTTPS protocol. If the port TCP/80 is open, any HTTP request on that port will be redirected to HTTPS on port TCP/443.

The following ports must be open on each host in a multi-server deployment.

Host	Server Process	Open Ports
itgrc.acme.com	Apache HTTPS server	TCP/80, TCP/443 to world
app1.acme.com	RiskVision Tomcat application server	TCP/8009 to itgrc.acme.com
app2.acme.com	JasperReports Server Tomcat application server	TCP/8409 to irgrc.acme.com TCP/8480 to app1.acme.com (used over HTTP) TCP/8480 to localhost
dbrv.acme.com	MySQL database server	TCP/3306 to app1.acme.com and app2.acme.com

	Oracle database server	TCP/1521 to app1.acme.com and app2.acme.com
dbjs.acme.com	PostgreSQL database	TCP/5432 to app1.acme.com and app2.acme.com

Note: If Apache and RiskVision Tomcat are on separate servers, any firewall between them needs to allow the RiskVision Tomcat server to connect to port TCP/443 of the Apache server. If this path is not open, there will be issues with Jasper reports embedded in the detail pane tabs.

Oracle Server

Use the following checklist when setting up Oracle Server 12.2.0.1 for use with RiskVision:

Note: A complete discussion regarding installing and operating Oracle is beyond the scope of this document.

To set up Oracle Server 12.2.0.1:

1. Qualified engineers must perform your Oracle hardware and software installation. Only the Oracle JVM Standard Database Component is required for use in Oracle database with RiskVision. A trained Database Administrator (DBA) should manage most of the Oracle installation process.

2. The database used for RiskVision must use the AL32UTF8 Unicode character set. RiskVision can share a database with other applications as long as the character set is correct.

3. Make sure that the Oracle database server port is open. It uses port 1521 by default.

4. The Oracle Server installer creates the **SYSTEM** user when the installation is complete; you must use the `SYSTEM` user to export the RiskVision schema to the Oracle directory.

5. Setup the following tablespaces. Note that data grows over time, so these sizes must be revisited on a regular basis. Or, you can enable the auto-extensible option for a datafile of a tablespace so that the size of the file is automatically increased when more space is needed in the database.

Name	Description	Suggested size
AGLDATA	Used for tables, data, and other objects	10 GB
AGLINDEX	Used for all indexes	10 GB
AGLTEMP	Used for temporary operations	20 GB*
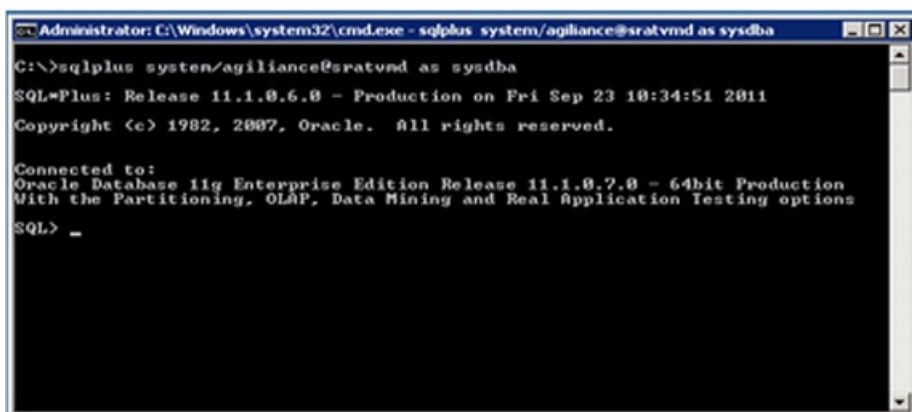
Ideally, you must have 3 tablespaces in parallel to each of the above. When there are more than 3 tablespaces, you need to re-map all indexes accordingly.

If you need to map the tablespaces with your own tablespaces, see Remapping RiskVision Tablespaces.

Allocate 400 MB for Redo Log Groups, but adjust based on performance testing. Some RiskVision operations require more log headroom than others. If the Redo Log appears to be a bottleneck, increase the allocation.

*20 GB is recommended to accommodate backups on the same host. Depending on the operating configuration, less disk space may be sufficient.

6. From the Windows command prompt, run the following command to verify the Oracle client-server connectivity: `Sqlplus system/agiliance@ as sysdba`

About Oracle Schema Accounts

The following Oracle Schema accounts are available for the installation and management of RiskVision Server on an Oracle database.

Oracle Schema Account	Description
Schema Owner	Accountable for the installation of RiskVision. Typically, the owner of all objects in the RiskVision database, and can therefore create, modify, and drop objects.
Schema User	Has access to the objects owner by the Schema Owner and is used in all database connection properties. You must use the Schema User to access the database as this user account allows you to manipulate data and create temporary tables and views. Therefore, this user acts as a secured layer and restricts unauthorized users from modifying schema objects.

Install RiskVision on a Single Server

You can install the RiskVision Server components on the single server. This kind of setup is appropriate for small-scale enterprises with a relatively small number of assets. RiskVision offers a third-party business intelligence tool called JasperReports Server that you can use for building sophisticated charts and dashboards.

We do not recommend running MySQL, Apache2, or Tomcat for programs other than RiskVision on the target system. If any conflicting servers are installed, stop them before beginning the RiskVision installation process. The **Help** icon shows the installation steps in the Installer wizard.

To install the RiskVision Server:

1. Disable User Account Control before you begin the installation if you're using Windows Server 2008 or 2012. You may re-enable this feature after installation if required

   a. Go to **Administrative Tools** > **Local Security Policy** > **Local Policies** > **Security Options**.

   b. Double-click **ser Account Control: Run all administrators in Admin Approval Mode**.

   c. Click the **Local Security Setting** tab.

   d. Click **Disabled**.

   e. Click **OK**.

   f. Reboot the host.

2. Double-click the `RiskVisionApplicationServerInstallation.exe` to open the **InstallShield** wizard.

3. Click **Next**.
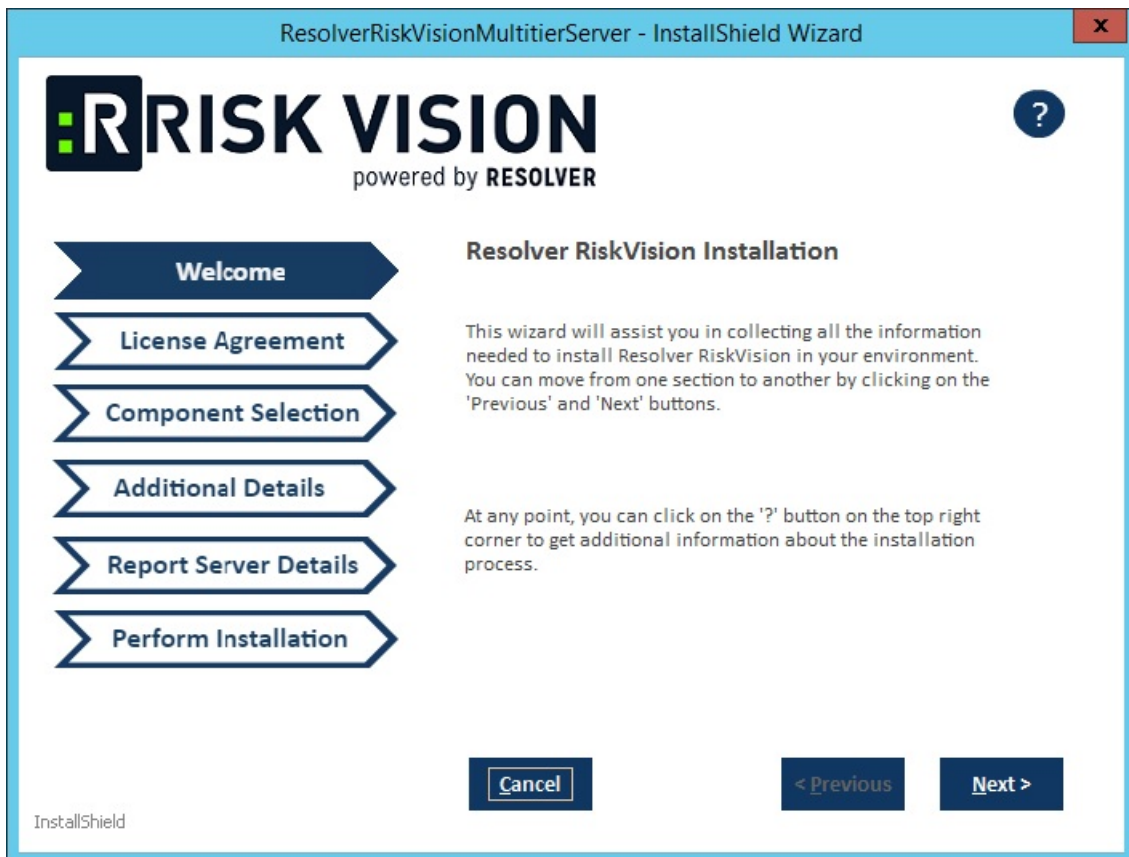
4. Click **I accept the terms of the license agreement**
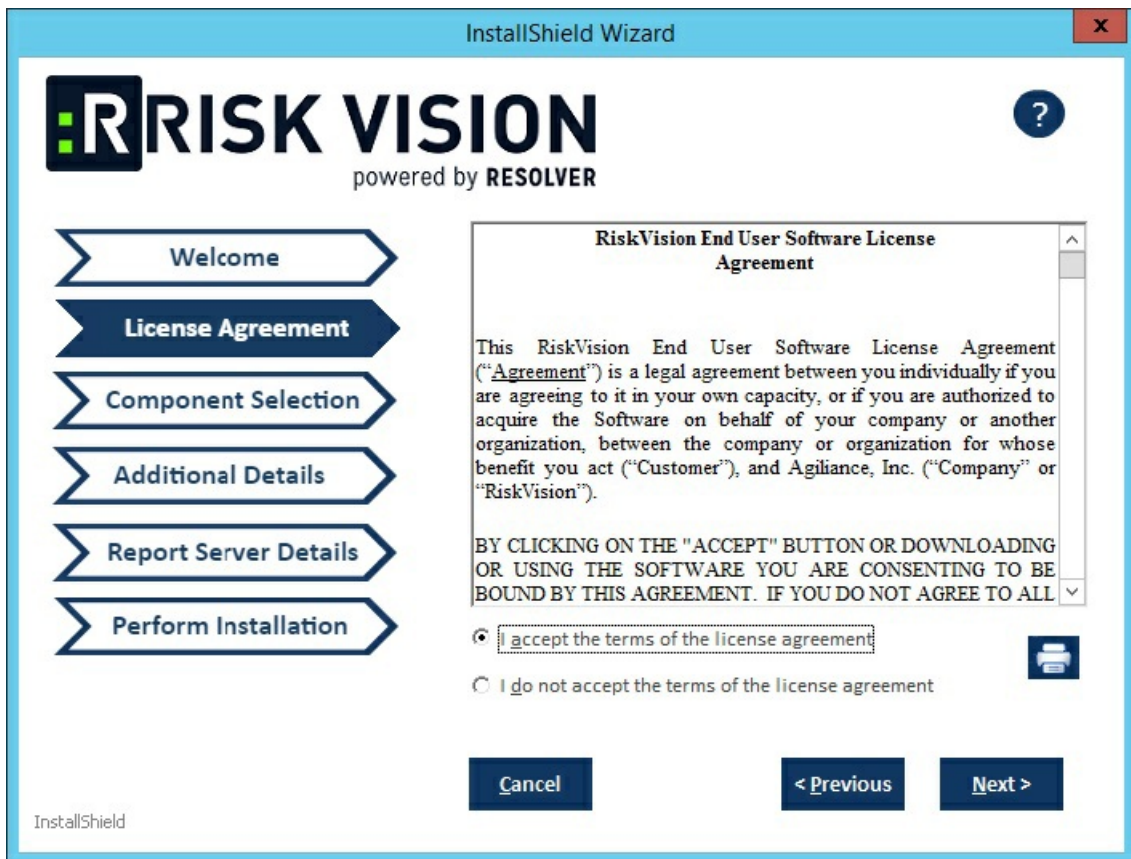
5. Click **Next**.

6. Click the **Web Server**, **Application Server**, **Database Server**, and **Report Server** checkboxes. This will install the Apache HTTP Server, Apache Tomcat application server, database server (MySQL), TIBCO Jasper Report Server and Apache open office. If you need to set up RiskVision Server using an Oracle database, see Oracle Database Pre-Installation.
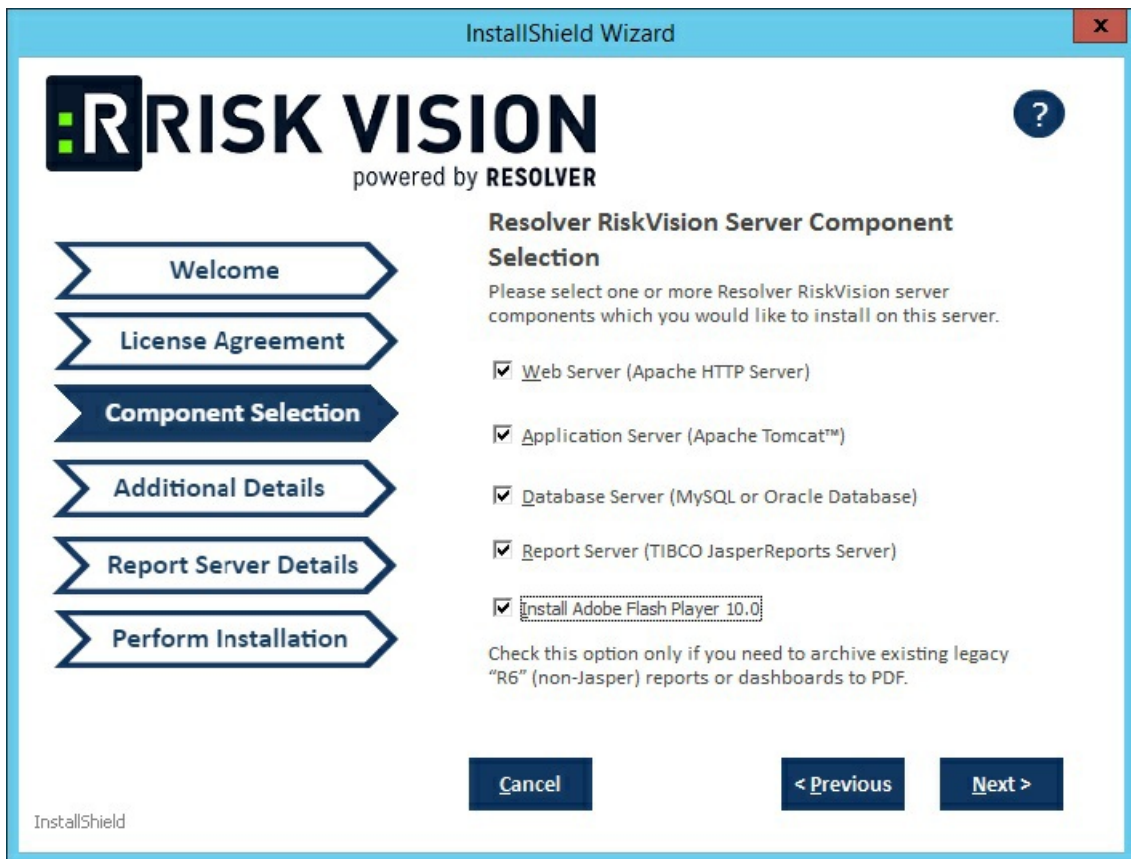
7. Click **Next**.

8. Select the **MySQL 5.7.24** or **Oracle 12.2.01** radio button to indicate the database type.
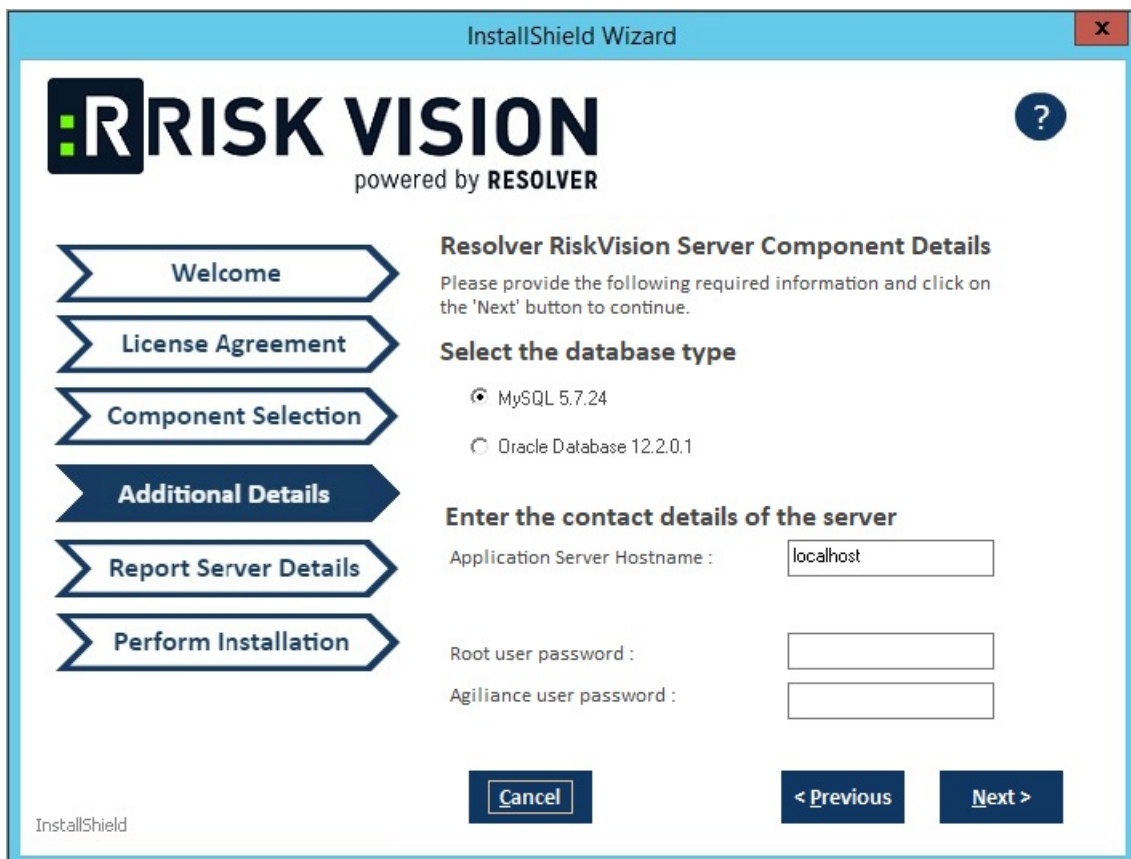
- **MySQL Database**:

    a. Click the **Root user password** field and enter a password for the root user.

    b. Click the **Agiliance user password** field and enter a password for the Agiliance user.

    c. Click **Next**. A warning message may appear if the required TCP ports are used by the server where you are currently running this installer. If the warning message appears, click **Cancel**, then click **Next** to stop the installation, or click **Ignore**, then click **Next** to continue.

    d. Click the **Application Server IPAddress** field and enter the location of the application server IP address.

    e. Click the **Application Server Hostname** field and enter the location of the application server hostname.

    f. Enter a password for the reportuser user in the **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field to ensure that the password you entered is correct. You will need to input the password again in the database.

    g. Enter the database port number, in the **Database Port** field.

- **Oracle Database:**

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

    b. Enter the application server IP address in the **Application Server IP Address** field.

    c. Click the **Application Server Hostname** field and enter the location of the application server hostname.

    d. Enter a password for the reportuser user in the **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field. You will need to input the password again in the database.

    e. Enter the database port number in the **Database Port** field.

    f. Enter the Oracle service name in the **Oracle Service Name** field.

    g. Click **Next** to open the **Perform Installation** page.
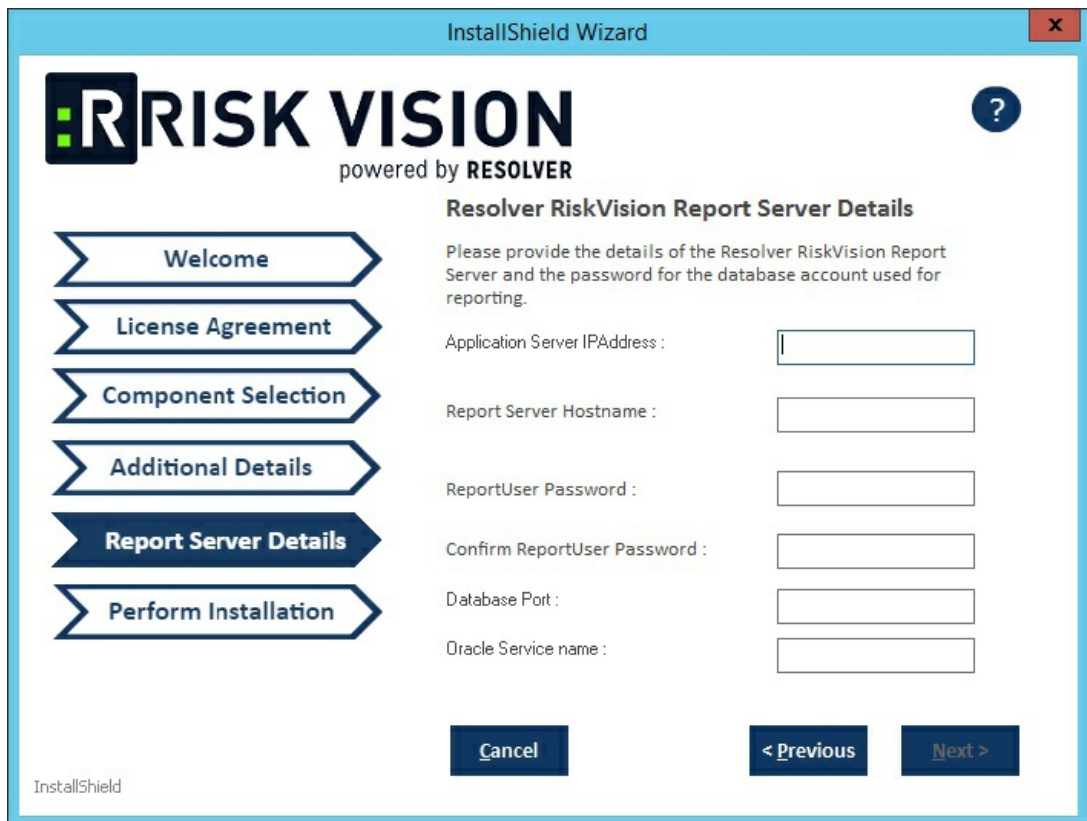
9. **Optional**: Click **Browse** to change the installation path. By default, components will be installed in the directory `C:\Server`. If you have changed the installation path, ensure you have at least 100 GB of free disk space for installing RiskVision Server and Report Server.
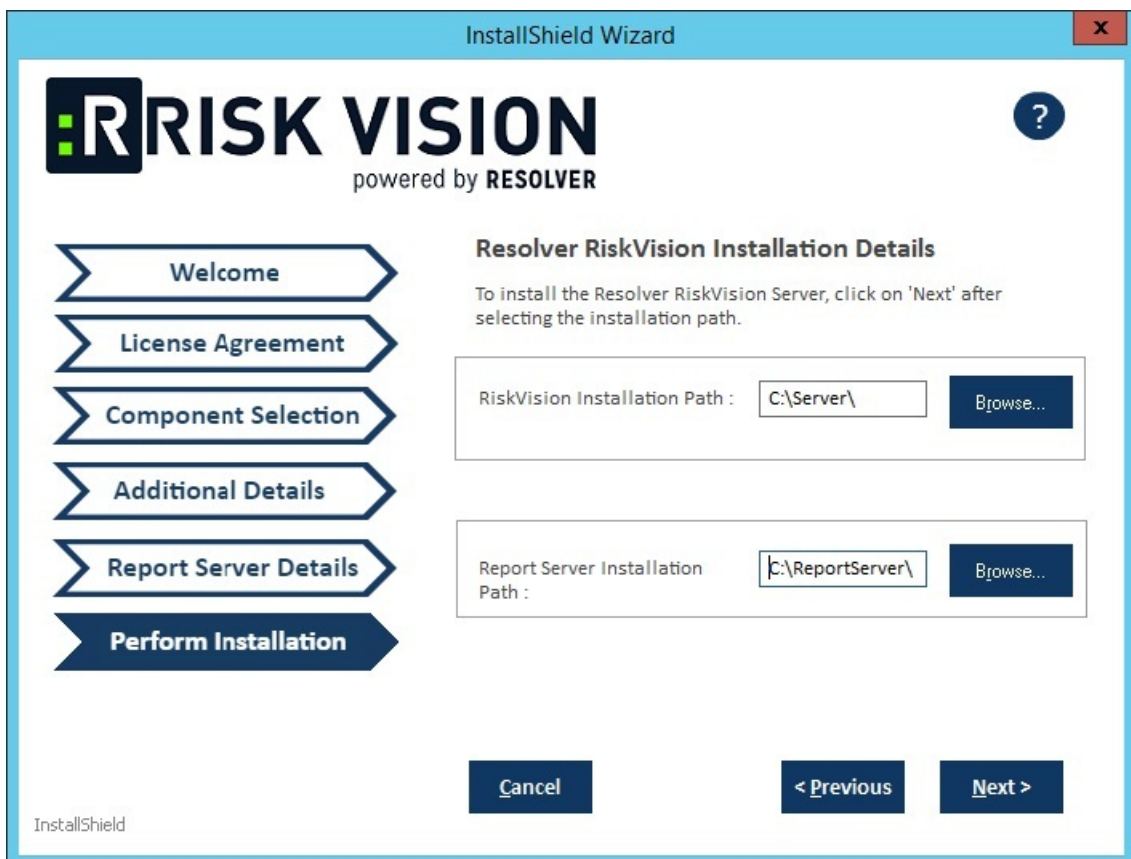
10. Click **Next** to open the **Begin Installation** wizard. If the server where you are currently running the installer does not meet the system and hardware requirements, the **Disclaimer** page will open. Continuing the installation without proper hardware could severely affect performance. Refer to the Minimum Hardware Requirements page for more information. To disregard the **Disclaimer** page, click **Accept**, then click **Next**.
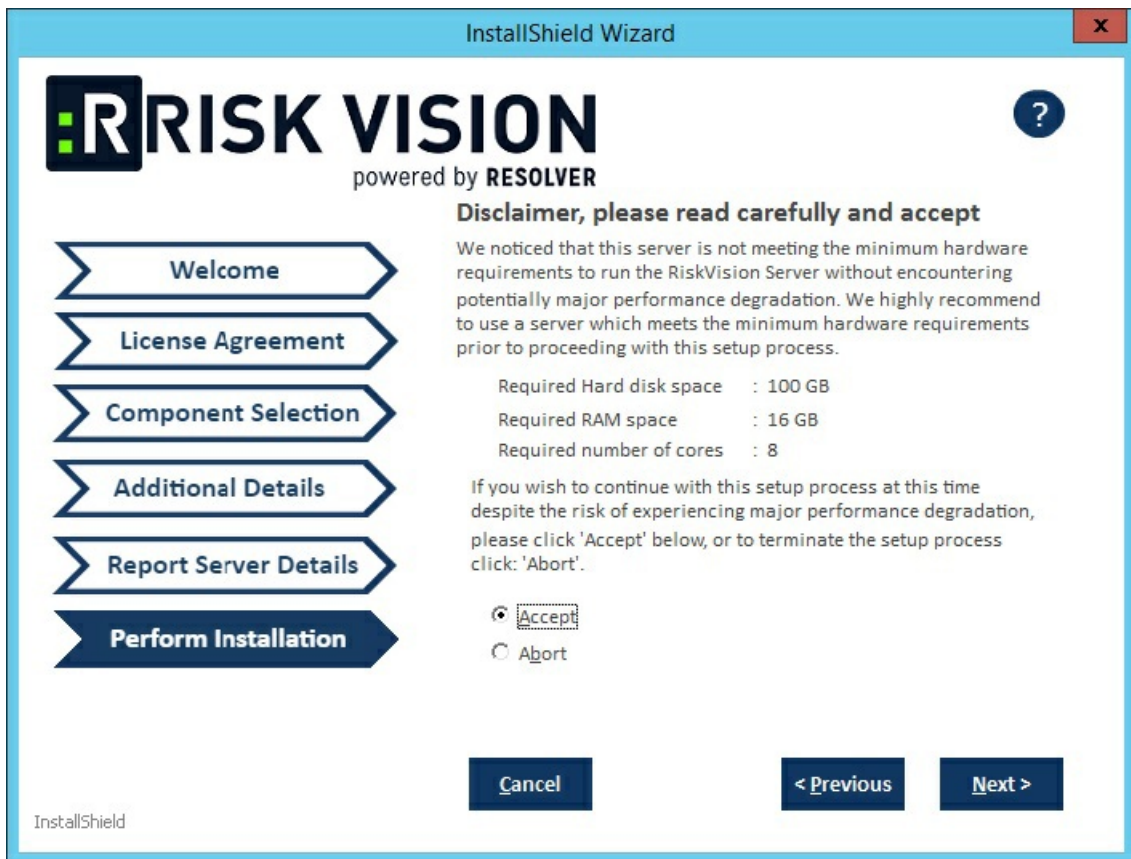
The installer sets the environment variable to `%AGILIANCE_HOME%` the product install path specified here. The default install directory is `C:\Server`. From this point forward, the install directory is referred to as `%AGILIANCE_HOME%`. The path `%AGILIANCE_HOME%` must not contain spaces.

11. Click **Next**.

12. Click **Install**.
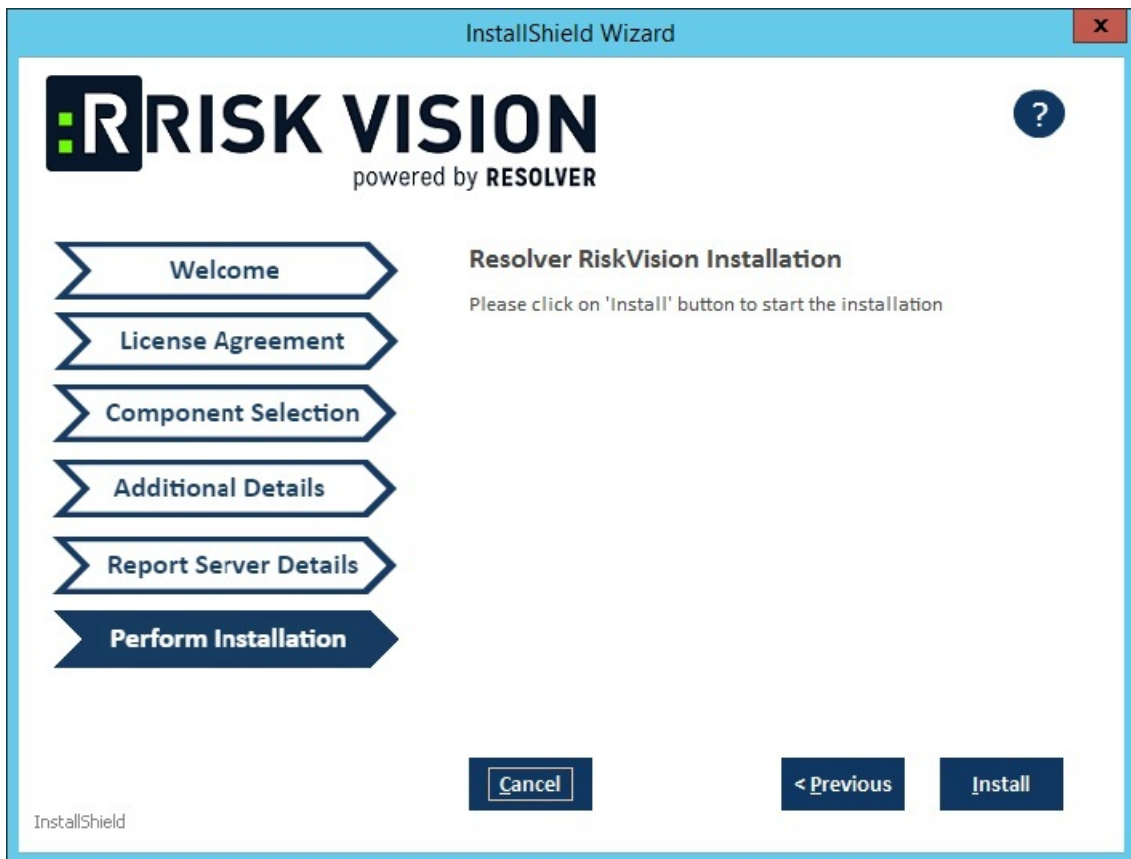
13. Review the path to your SSL Certificate File, SSL Certificate Key, and Resolver RiskVision License File.

14. Review the Release Notes for the post-installation steps, then check the **I confirm that I have read the above notes** checkbox.

15. Click **Finish**.
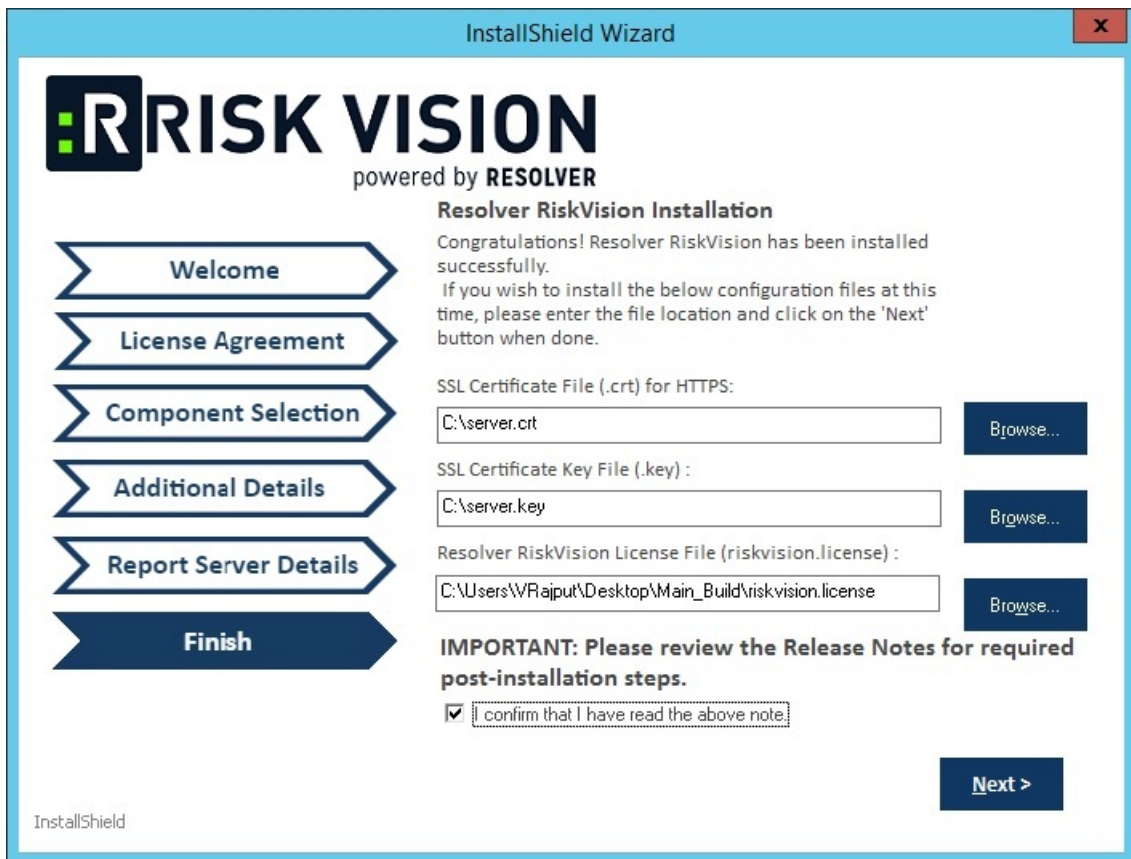
16. Click **Next**.

17. Click **Finish** to complete the installation if you are using a MySQL database. The application servers, MySQL database, web server, and report server are now installed. If you are setting up the RiskVision Server on an Oracle database, see Setting up Oracle Database.

> ⚠️ If a command window opens while the scripts are running, do not close it. The window will close by itself.

> ℹ️ If the installation fails, consult the installation log file(`Install.log`)in the folder where RiskVisionApplicationServerInstallation.exe was executed. This file captures the output and results of the installation scripts.

Install Riskvision Server on Multiple Servers

RiskVision Server components: Apache web server, Tomcat application server, RiskVision Reports server and database application can be installed on multiple servers. This kind of setup is appropriate for large-scale enterprises with high volume of assets. You prefer distributing the installation for spreading process load across multiple servers, for security reasons, to comply with company policy, or mainly to experience better performance. The RiskVision Server components that can be distributed include:

- Apache web server

- Tomcat application server

- Database server (MySQL or Oracle)

- JasperReports server (RiskVision Reports Server)

The procedure for installing the RiskVision Server components on multiple servers involves selecting the required component(s) in the RiskVision Server Setup installer. You use the RiskVision Server Setup installer to install the following RiskVision Server components: Apache web server, Tomcat application server, database (only MySQL), and JasperReports server application one in each sever.

Installation Sequence

In a distributed installation, the sequence in which you will install the components is significant to the successful installation. RiskVision recommends installing the components in the following sequence:

- Tomcat application server

- Apache web server

- Database server (if installing RiskVision Server to use Oracle database, set up the Oracle Server first)

- RiskVision Reports server

Install a MySQL Database

You can distribute the database component to host it on a separate server. Either of the following databases can be installed on different server:

- MySQL
- Oracle

If you intend to install your MySQL database on a separate server where no other components of RiskVision Server have been installed, you will need to complete some additional configuration.

To install a MySQL database on a separate server:

1. Copy the following files to the server where the MySQL database server will be installed.

   - riskvision.license;
   - RiskVisionApplicationServerInstallation.exe;
   - jce_policy-8.zip;
   - mysql-5.7.26-winx64.zip;
   - mysql-connector-java-5.1.39.zip;
   - Riskvision-part1.zip;
   - Riskvision-part2.zip; and
   - Riskvision-part3.zip.

2. Double-click the `RiskVisionApplicationServerInstallation.exe` file to launch the **RiskVision Server Setup** wizard.

3. Click **Next**.

4. Click **I accept the terms in the License Agreement**, then click **Next**.

5. Check the **Database Server(MySQL or Oracle Database)** checkbox.

The Component Selection section of the setup wizard.

6. Click **Next**.

5. In the **Additional Details** section:

44

a. Click **MySQL 5.7.26** to install the MySQL database.

b. Click the **Application Server hostname** field and enter the hostname or IP address of the server where the Tomcat application server is installed.

c. Click the **Root user password** field and enter a password for the root user.

d. Click the **Agiliance user password** field and enter a password for the Agiliance user.

The Additional Details section of the setup wizard.

6. Click **Next**. A warning message will appear if the required TCP ports are being used by the server where you are currently running this installer. If the warning message appears, click **Cancel**, then click **Next** to stop the installation. If you wish to continue, click **Ignore**, then click **Next**.

7. In the **Report Server Details** section:

a. Enter the report server hostname in the **Report Server Hostname** field**.**

b. Enter a password for the report user in the **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field.

c. Enter the database port number, in the **Database Port** field.
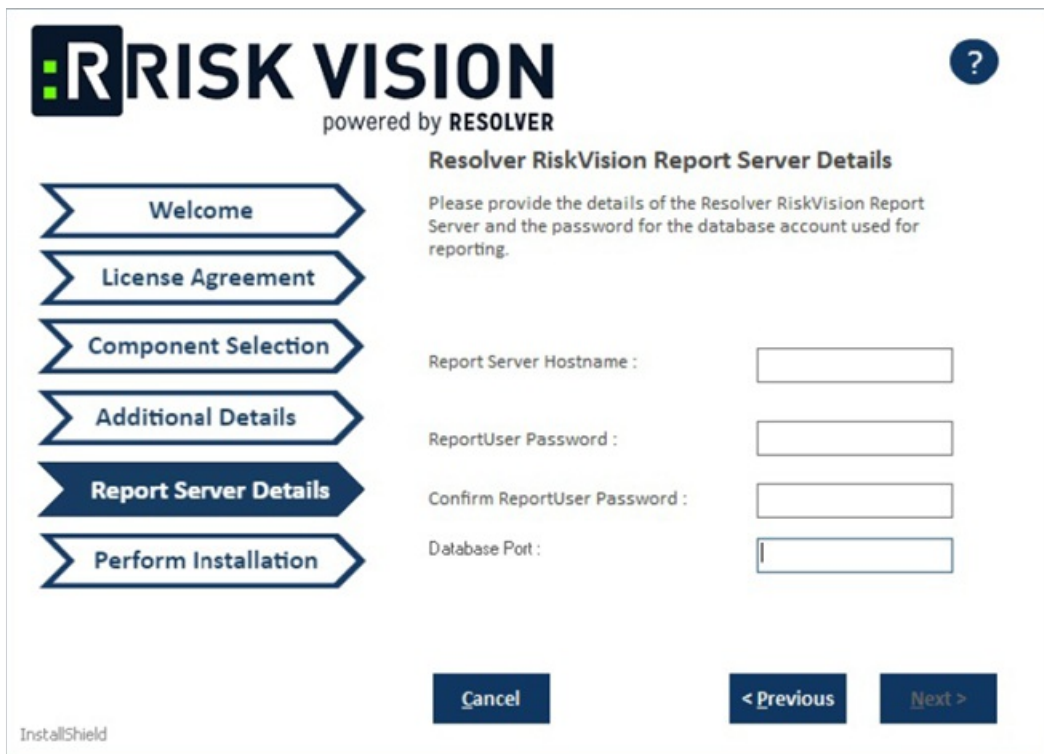
The Report Server Details section of the setup wizard.

8. Click **Next** to open the **Begin Installation wizard**. If the server where you are currently running the installer does not meet the system and hardware requirements, the **Disclaimer** page will open. Continuing the installation without proper hardware could severely affect performance. Refer to the Minimum Hardware Requirements page for more information. To disregard the **Disclaimer** page, click **Accept**, then click **Next**.

9. **Optional**: Click **Browse** to change the installation path. By default, the MySQL database is installed on `C:\Server\` . Ensure you have enough disk space if you change the installation path.

10. Click **Install** to begin installing the MySQL database. Allow sufficient time for the setup to complete the installation. When installation is complete, the **Finish** page will appear.

11. Review the Release Notes for required post-installation steps, then check the **I confirm that I have read the above notes**checkbox.

12. Click **Next**.

The Finish section of the setup wizard.

13. Click **Finish** to exit the installation wizard.
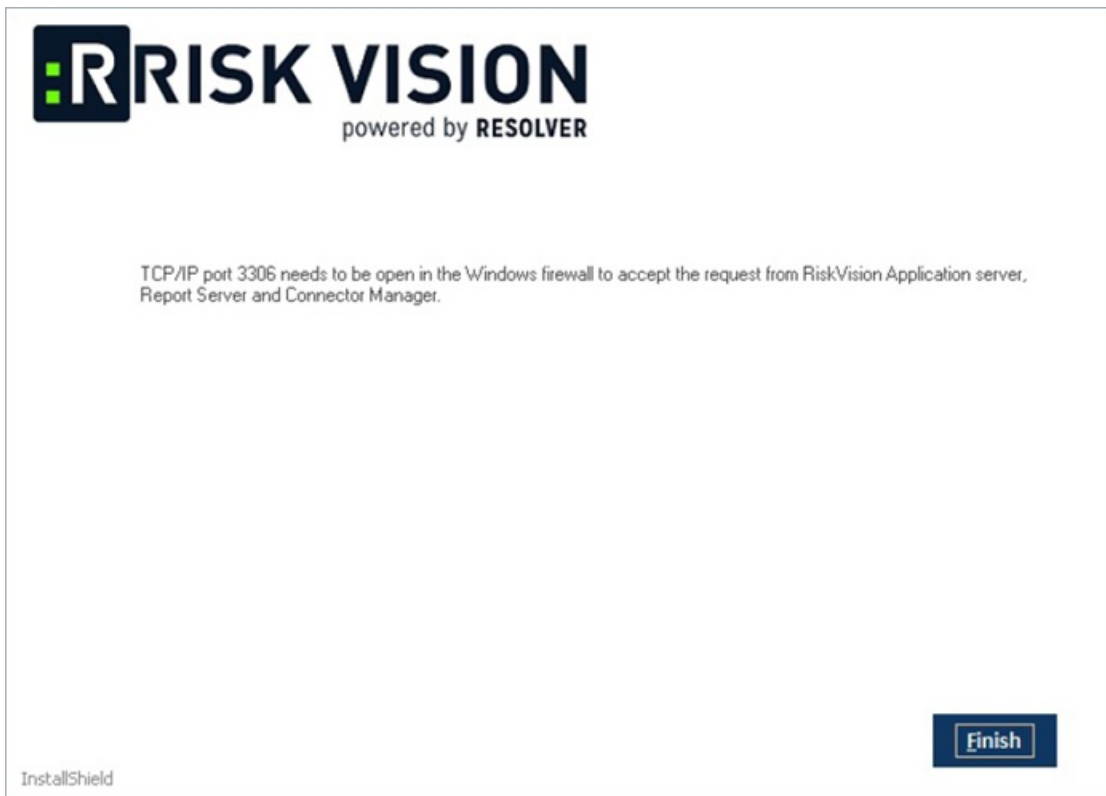
The completion screen of the setup wizard.

Install an Oracle Database

You don't need to run the RiskVision Server Setup Installer on the server where your Oracle database is installed, because you will specify the IP address or hostname of the Oracle server while installing the Tomcat application server. For instructions on setting up the Oracle database, see Setting up Oracle Database.

Install the Application Server

If you want to install the application server on its own server, you will need to perform some additional configuration.

To install the application server on its own server:

1. Copy the following files to the server where the application server will be installed:

File	MySQL	Oracle
riskvision.license	✅	✅
RiskVisionApplicationServerInstallation.exe	✅	✅
jce_policy-8.zip	✅	✅
Riskvision-part1.zip	✅	✅
Riskvision-part2.zip	✅	✅
Riskvision-part3.zip	✅	✅

2. Double-click the `RiskVisionApplicationServerInstallation.exe` file to launch the **Resolver RiskVision MultitierServer Setup** wizard.

3. Click **Next**.

4. Check the **I accept the terms in the License Agreement** checkbox, then click **Next**.

5. Check the **Application Server (Apache Tomcat** ᵀᴹ**)** checkbox. This will install the application server only.
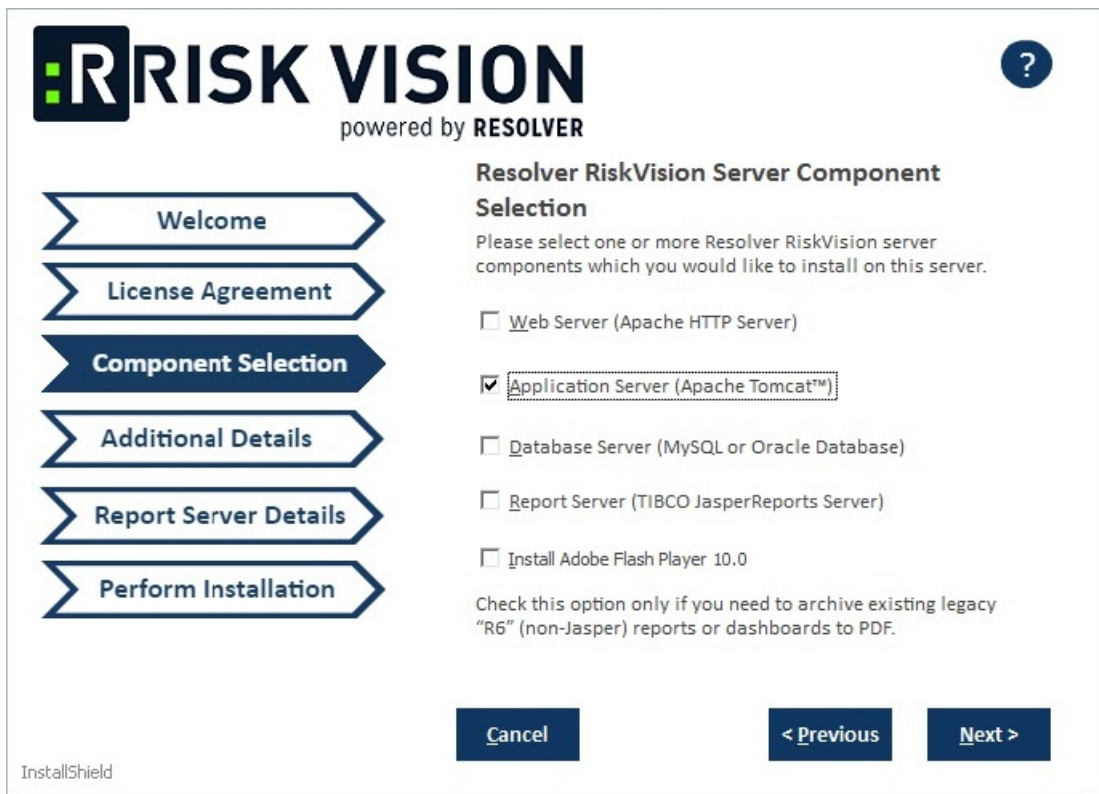
The Component Selection section of the setup wizard.

6. Click **Next**.

7. Select one of the following options:

   - **MySQL Database**:

     a. Click the **MySQL 5.7.26** radio button to install the MySQL database.

     b. Enter a password for the root user in the **Root user password** field.

     c. Enter a password for the Agiliance user in the **RiskVision user password** field.

     d. Enter the host name or IP address of the server in which the Tomcat application server will be installed in the **Database Server hostname** field.

The Additional Details section of the setup wizard.

- **Oracle Database**:

  a. Click the **Oracle Database 12.2.01** radio button.

  b. Enter a password for the root user in the **Database Server Hostname** field.

  c. Click **Next**. A warning message may appear if the required TCP ports are used by the server where you are running the installer. If the warning message appears, click **Cancel**, then click **Next** to stop the installation.

8. Click the **Report Server Hostname** field and enter the report server hostname.

9. Complete one of the options below:

  - **MySQL database**:

    a. Enter a password for the report user in the **Report user password** field and reenter the same password in the **Confirm ReportUser Password** field.

    b. Click the **Database Port** field and enter the database port number.

The Report Server Details section for the MySQL database.

- **Oracle Database**:

    a. Click the Report Server Hostname field and enter the report server hostname.

    b. Enter a password for the report user in the **ReportUser password** field and reenter the same password in the **Confirm ReportUser Password**.

    c. Enter the database port number in the **Database Port** field.

    d. Enter the Oracle service name in the **Oracle Service Name** field.

    e. Click **Next**.

The Report Server Details section for the Oracle Database.

10. **Optional**: Click **Browse** to change the installation path. By default, the MySQL database is installed on `C:\Server\` . Ensure you have enough disk space if you change the installation path.

11. Click **Next** to open the **Begin Installation wizard**. If the server where you are currently running the installer does not meet the system and hardware requirements, the **Disclaimer** page will open. Continuing the installation without proper hardware could severely affect performance. Refer to the Minimum Hardware Requirements page for more information. To disregard the **Disclaimer** page, click **Accept**, then click **Next**.

12. Click **Install** to begin installing the application server. Allow sufficient time for the setup to complete the installation. When installation is complete, the RiskVision installer will display the riskvision.license path.

The Finish section of the setup wizard.

13. Review the Release Notes for required post-installation steps then check the **I confirm that I have read the above notes** checkbox.

14. Click **Next**. Click **Finish** to complete the installation.
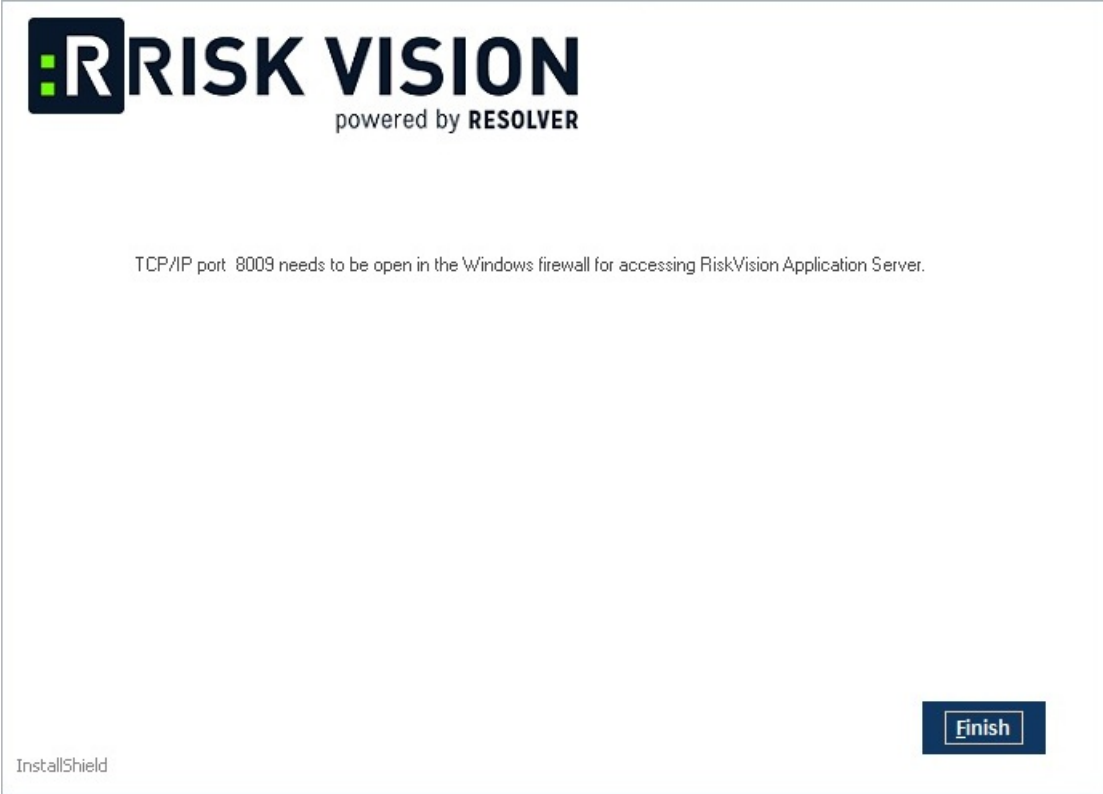
The completion screen of the setup wizard.

Install the Web Server

If you intend to install the Apache web server on its own server, you will need to do some additional configuration.

To install the web server on its own server:

1. Copy the following files to the server where Apache web server will be installed:

File	MySQL	Oracle
riskvision.license	✓	✓
RiskVisionApplicationServerInstallation.exe	✓	✓
jce_policy-8.zip	✓	✓
Riskvision-part1.zip	✓	✓
Riskvision-part2.zip	✓	✓
Riskvision-part3.zip	✓	✓

2. Double-click the `RiskVisionApplicationServerInstallation.exe` file to launch the **Resolver RiskVision Multitier Server Setup wizard**. Click **Next**.

3. Check the **I accept the terms in the license agreement** checkbox, then click **Next**.

4. Check the **Web Server (Apache HTTP Server)** checkbox.
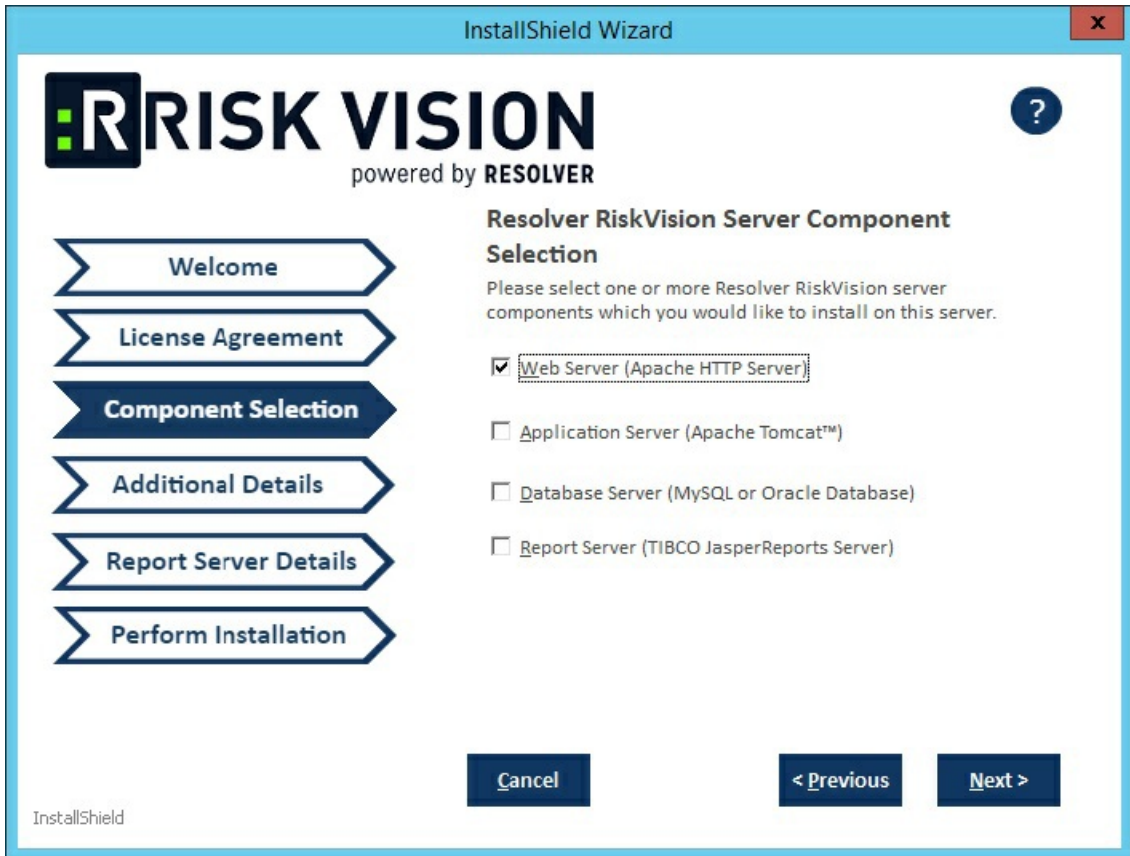
5. Click **Next**.

6. Click the **Application Server Hostname** field and enter the hostname of the server where the Tomcat Application Server is installed.
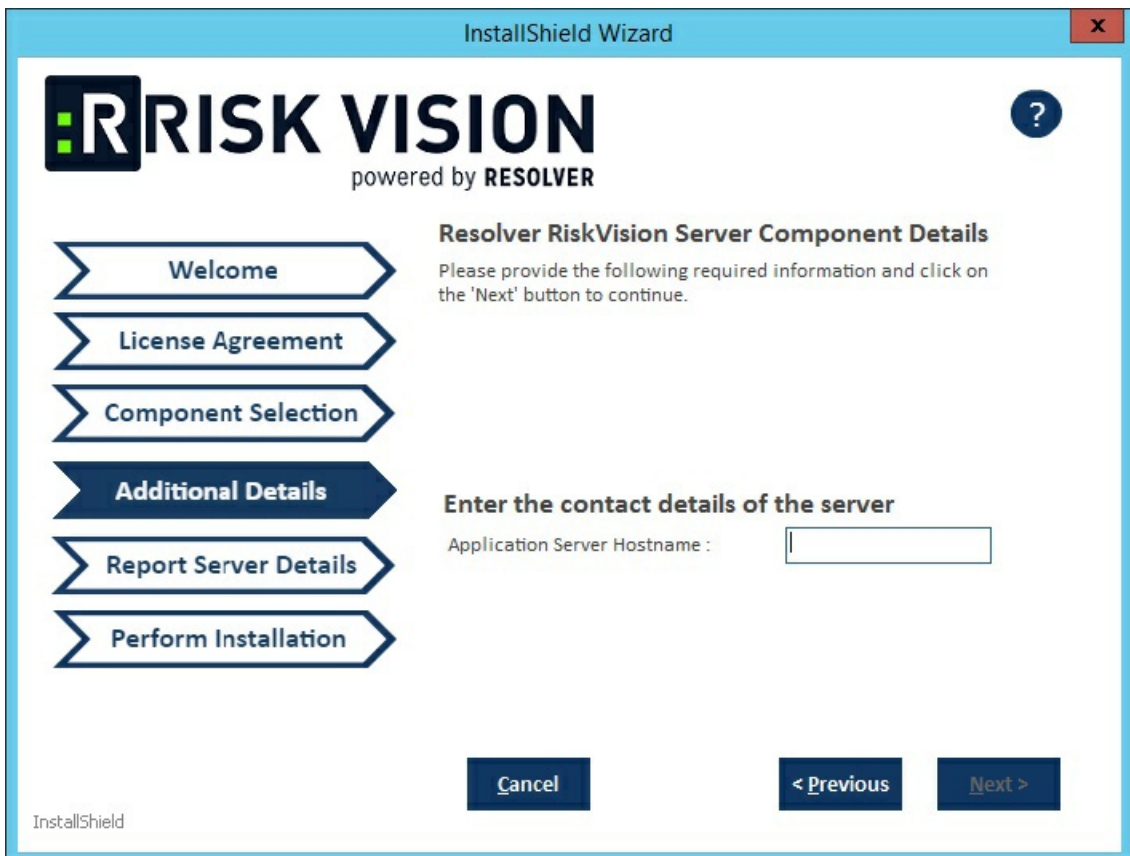
7. Click **Next**.

8. Click the **Report Server Hostname** field and enter the report server hostname.

9. Enter a password for the user `report` in **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field to ensure that the password you entered is correct. Memorize the password, because you will need to input the password again in the database.
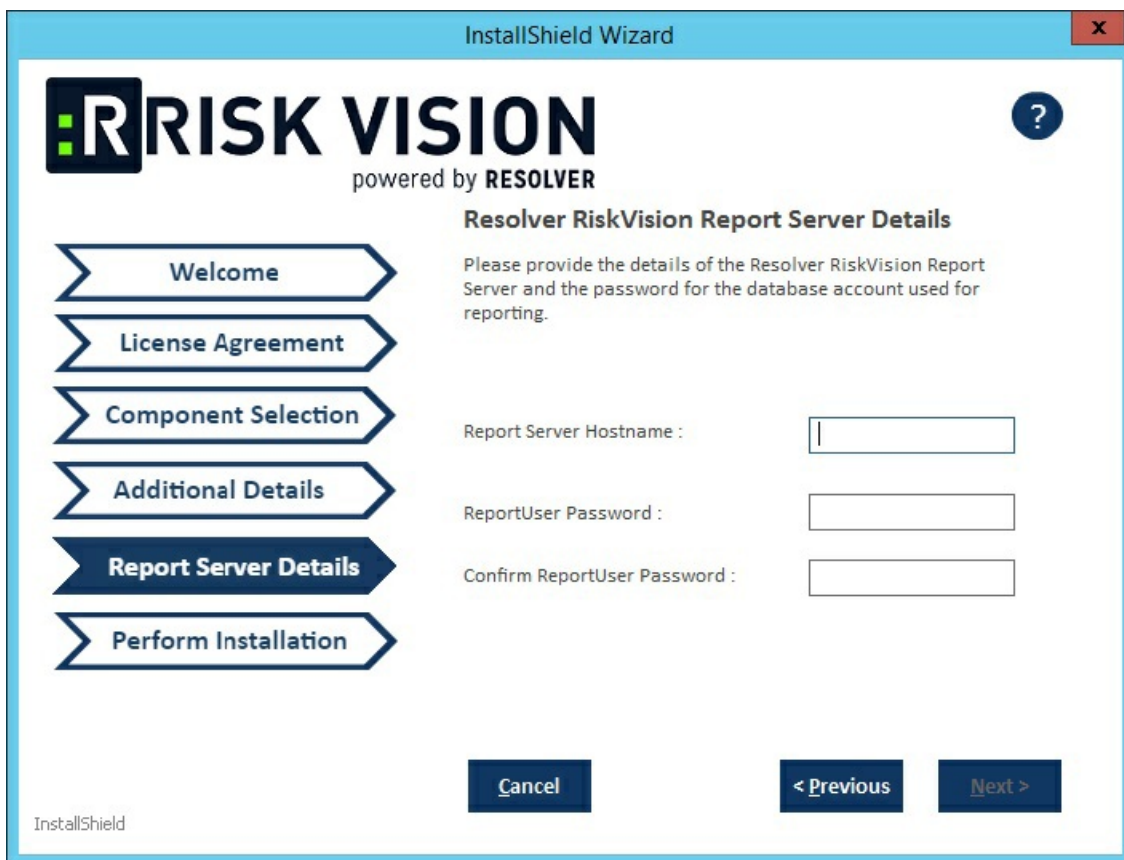
Click **Next** to continue.

10. The **Perform Installation** page appears. By default, the web server will be installed in the directory `C:\Server\` . The disk space requirements will show how much disk space is needed to install the product in your system. To change the installation path, click **Browse** and select the required path. Be sure to check the disk space if you have changed the installation path.

    Click **Next** to continue.

8. The **Perform Installation** page modifies and the **Disclaimer** page appears, if the server where you are currently running the installer does not meet the system and hardware requirements, else you will be directed to the Begin Installation wizard page.

    At this point, you must decide whether to continue the installation without meeting the minimum hardware requirements or to cancel the installation. Continuing the installation without proper hardware might severely degrade the performance of deployments, whether running a production phase or a testing phase. Stop the installation and glance through the minimum hardware requirements in the wizard page or refer to the Minimum Hardware Requirements section to give the best of RiskVision software to your users.

    Click **Accept** to continue the installation and click **Next** to continue.

9. The **Perform Installation** page modifies, click **Install**. The setup now starts installing the Web Server. Allow sufficient time for the setup to complete the installation.

10. The **Finish** page appears, when the setup completes the installation, the RiskVision installer displays the path where the SSL Certificate files and SSL Certificate Key is saved.

11. You need to review the Release Notes for the post-installation steps for the successful RiskVision application setup and then select the **I confirm that I have read the above notes** check box, then the **Next** button will be enabled.
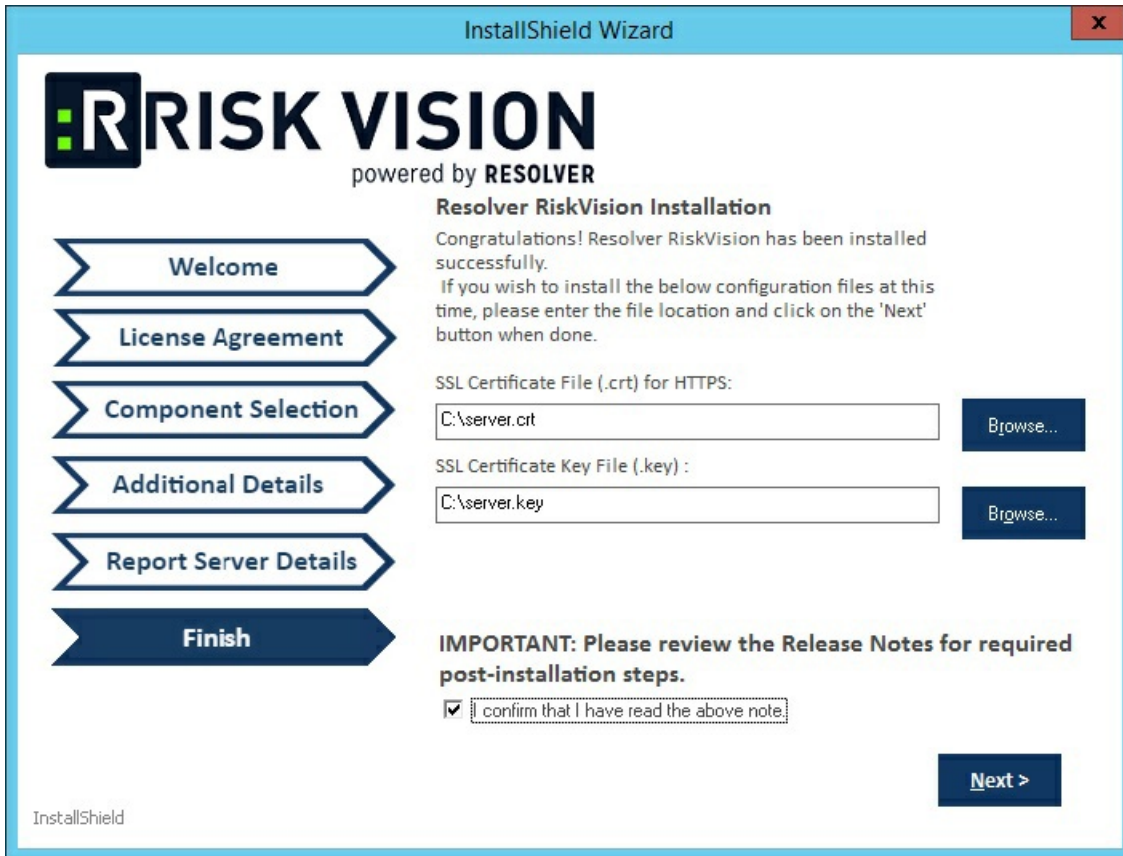
Click **Next** button to continue.

The **Finish** window appears, click **Finish** button to exit the installation wizard. This completes the web server installation.

Install the RiskVision Report Server

If you want to install the JasperReports Server on its own server, you will need to complete some additional configurations.

To install the JasperReports Server on its own server:

1. Copy the following files to the server where JasperReports Server will be installed.

File	MySQL	Oracle
riskvision.license	✅	✅
RiskVisionApplicationServerInstallation.exe	✅	✅
TIB_js-jrs_7.2_windows_x86_64.exe	✅	✅
jce_policy-8.zip	✅	✅
Riskvision-part1.zip	✅	✅
Riskvision-part2.zip	✅	✅
Riskvision-part3.zip	✅	✅

2. Double-click the `RiskVisionApplicationServerInstallation.exe` file to launch the **RiskVision Server Setup** wizard.

3. Click **Next**.

4. Click **I accept the terms in the License Agreement**, then click **Next**.

5. Check the **Report Server (TIBCO JasperReport Server)** checkbox.

The Component Selection section of the setup wizard.

6. Click **Next**.

7. Select one of the following options:

   - **MySQL database**:

     a. Click the **MySQL 5.7.26** radio button to install the MySQL database.

     b. Click the **Application Server Hostname** field and enter the hostname or IP address of the server where the Tomcat application server is installed.

     c. Click the **Database Server Hostname** field and enter the location where the database server is installed.
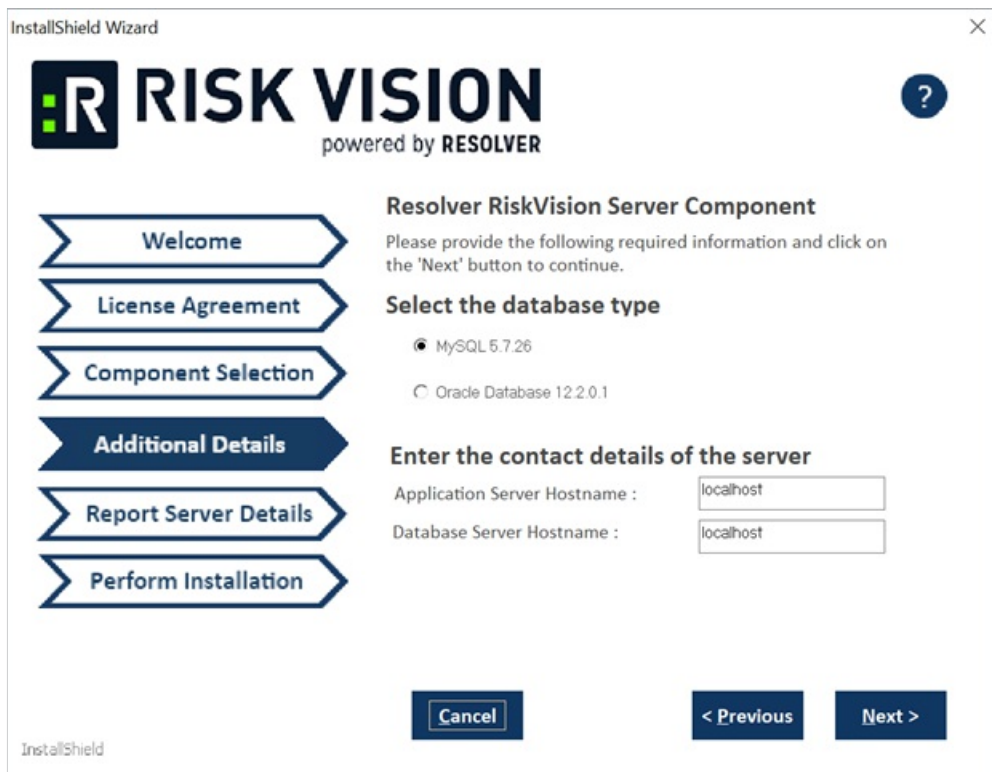
     d. Click **Next**.

The Additional Details section of the setup wizard.

- **Oracle Database:**

  a. Click the **Oracle Database 12.2.01** radio button.

  b. Click the **Application Server Hostname** field and enter the hostname or IP address of the server where the Tomcat server is installed.

  c. Click the **Database Server Hostname** field and enter the hostname or IP address of the server where the database server is installed.

  d. Click **Next**.

8. Complete one of the options below:

   - **MySQL database:**

     a. Click the **Application Server IP Address** field and enter the location of the application server IP address.

     b. Click the **Report Server Hostname** field then enter the location of the report server hostname.

     c. Enter a password for the report user in the **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field. You will need to input the password again in the database.

     d. In the **Database Port** field, enter the database port number.

The Report Server Details section for the MySQL database.

- **Oracle Database:**

    a. Enter the application server IP address in the **Application Server IP Address** field.

    b. Click the **Report Server Hostname** field and enter the location of the report server host name.

    c. Enter a password for the report user in the **ReportUser Password** field and reenter the same password in the **Confirm ReportUser Password** field. You will need to input the password again in the database.

    d. Enter the database port number in the **Database Port** field.

    e. Enter the Oracle service name in the **Oracle Service Name** field.

The Report Server Details section for the Oracle Database.

9. Click **Next** to open the **Begin Installation wizard**. If the server where you are currently running the installer does not meet the system and hardware requirements, the **Disclaimer** page will open. Continuing the installation without proper hardware could severely affect performance. Refer to the Minimum Hardware Requirements page for more information. To disregard the **Disclaimer** page, click **Accept**, then click **Next**.

10. **Optional**: Click **Browse** to change the installation path. By default, the MySQL database is installed on `C:\Server\` . Ensure you have enough disk space if you change the installation path.

11. Click **Install** to begin installing the Report Server. Allow sufficient time for the setup to complete the installation. When installation is complete, the **Finish** page will appear.

12. Review the Release Notes for required post-installation steps, then check the **I confirm that I have read the above notes**checkbox.

13. Click **Next**.

The Finish section of the setup wizard.

14. Click **Finish** to exit the installation wizard.
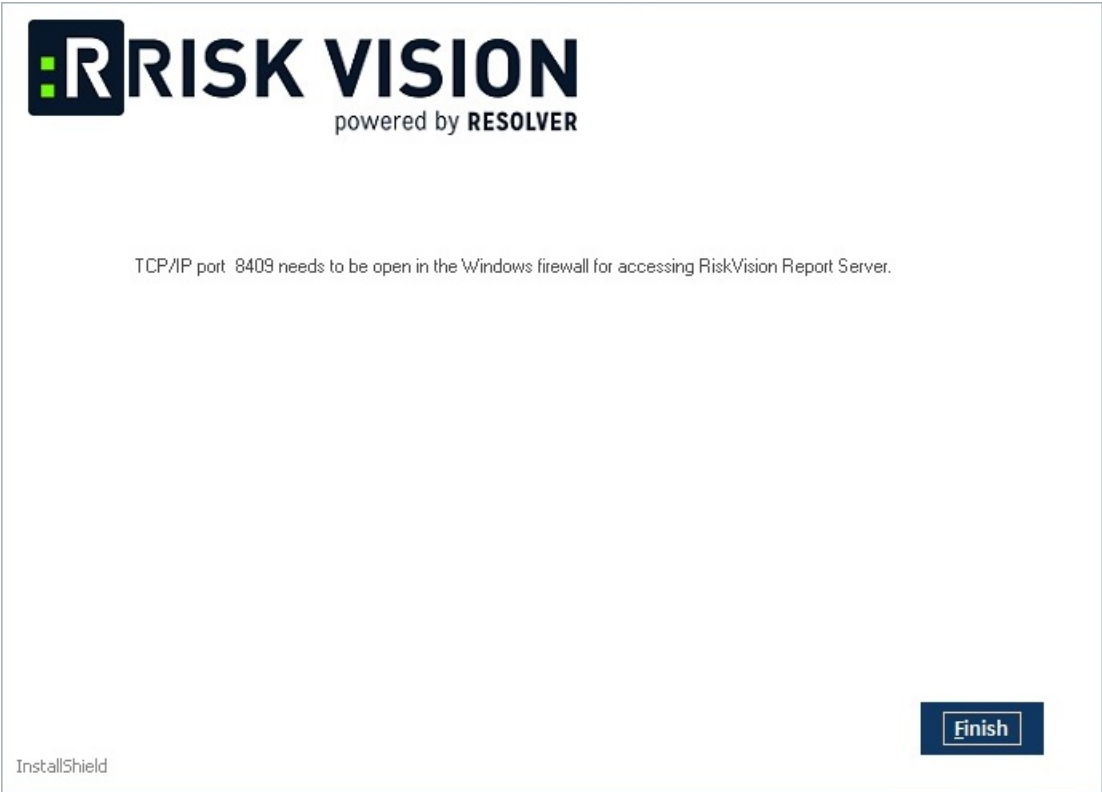
The completion screen of the setup wizard.

Set up an Oracle Database Server

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 have to 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.

MySQL Post-Installation Script

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 `agl_master.sql` are in this folder.

3. Execute the following command to load the scripts and make sure that 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`

Register Apache OpenOffice

Importing Microsoft Word documents as policy documents requires third-party OpenOffice software. This software is included in the RiskVision Server Setup installer, but the registration process requires some additional configuration. On the Windows 2008, 2012, 2016, and 2019 servers, OpenOffice uses the RiskVision Tomcat service that is running with the LocalSystem account.

Register OpenOffice with the LocalSystem account, but human users are not allowed to log in as LocalSystem. The following steps will temporarily impersonate LocalSystem in order to register OpenOffice as this user so that the RiskVision Server can call the OpenOffice API in the future without permission problems.

To register OpenOffice on Windows 2008, 2012, 2016, and 2019 Server:

1. Log in to the Windows 2008, 2012, 2016, and 2019 server where RiskVision Tomcat Application Server has been installed.

   a. Log in on the server as a user with Administrator privileges and open a command window; or

   b. Open a remote desktop session command window on the server. On your machine, open a command window and enter:*mstsc/admin*

   Enter your credentials for the remote desktop session. A command window opens when the connection is made.

2. Download PsTools from **http://technet.microsoft.com/en-us/sysinternals/bb896649**. Extract PsTools to the **%AGILIANCE_HOME\Install** directory.

3. In the **%AGILIANCE_HOME%\install\pstools** directory, open a command window running under the Local System account with one of the following commands, depending on your version of Tomcat:

   - For Tomcat versions prior to 8.5.53: `psexec -i -s cmd.exe`

   - For Tomcat version 8.5.53 and above: `psexec -d -i -u "NT Authority\Local Service" cmd.exe`

4. Click **Agree** to open a new command window. In this window, move to the**%AGILIANCE_HOME%\OpenOffice\program** directory and run `soffice.exe`

5. This OpenOffice program will prompt for user registration. Because you appear to be LocalSystem rather than an ordinary user, (using Tomcat running as LocalSystem) will be the registered owner of the OpenOffice installation. Enter your registration information, complete the process, and exit.

6. Close all open command prompt windows.

7. Set the following property in the config\agiliance.properties file :

   `com.agiliance.word.OpenOffice.program=`

   For example, if **%AGILIANCE_HOME%** is **C:\Server**:

   `com.agiliance.word.OpenOffice.program=C:/Server/OpenOffice/program`

8. Restart the RiskVision Tomcat service to show the latest changes.

> ⚠ **Failure to register OpenOffice will result in a runtime error while importing the Word documents.**

To register OpenOffice on Windows 2003 Server:

1. Open a remote desktop session command window on the RiskVision Server. On your machine, open a command prompt window and enter : `mstsc/admin`

   Enter your credentials for the remote desktop session. A command window opens while the connection is made.

2. Create a temporary service, which by default will run as LocalSystem. At the command line, enter: `sc create testsvc binpath= "cmd /K start" type= own type= interact`

3. Start the service: `sc start testsvc`

   The error--[SC] StartService FAILED 1053-- is expected. A new command window, running as LocalSystem, will open.

4. Switch to the new, LocalSystem, command window. Change the directory to the OpenOffice folder under Program Files. Run the command: `soffice.exe` .

   This OpenOffice program will prompt for user registration. Because you appear to be LocalSystem rather than an ordinary user, (using Tomcat running as LocalSystem) will be the registered owner of the OpenOffice installation. Enter your registration information, complete the process, and exit.

   > ⚠️ Failure to register OpenOffice will result in a runtime error when importing Word documents.

5. Close the LocalSystem command window. In the original command window, remove the temporary service by entering: `sc delete testsvc`

6. Set the following property in the **config\agiliance.properties** file:

   `com.agiliance.word.OpenOffice.program=`

7. Restart the RiskVision Tomcat service to apply the latest changes.

Start & Stop RiskVision Server Components

The RiskVision Server Setup installer sets up the processes as services automatically. If you have installed RiskVision on multiple servers, services will be available on their respective servers.

The following table provides a listing and description of these process names:

Service name	Description
RiskVision Job Manager	RiskVision Server web application process
RiskVision Apache	Apache Web Server
RiskVision Tomcat	Apache Application Server
RiskVision MySQL	MySQL relational database (RDBMS) (not applicable if you are using Oracle)

You can stop and restart individual services if needed, such as when making configuration changes or troubleshooting.

The Tomcat Application server may take some time to restart, due to system jobs. To reduce startup time, use the following property in the `agiliance.properties` file to stop system jobs from running until after the server has restarted.

To start, restart, or stop a service:

1. Go to **Start** > **Control Panel** > **Administrative Tools**.

2. Click **Services**.

3. Right-click a service and select **Start**, **Restart**, or **Stop**, in the context menu.

Log in for the First Time

This section explains how to log in using the system administrator account. A system administrator can only access server and application configuration settings, such as the email and LDAP connector settings, the application URL, logs, and Content.

System administrators manage the accounts of other system administrators only. Accounts created by the system administrator are internal accounts with the privileges required to modify other system administrator accounts, the server settings, and Content.

To log into RiskVision as the system administrator:

1. Open a browser and enter your host name. For example: https://RiskVisionHostname

   Where *RiskVisionHostname* is the hostname or IP address for the RiskVision Server

2. Accept the security certificate to open the **Login** page.

   By default, RiskVision Server uses a self-signed certificate for SSL authentication between web browsers and RiskVision. Depending on your browser, you may see a message such as, "Web site certified by an unknown authority." Accept the certificate permanently or temporarily to avoid seeing these types of messages in future sessions or accessing the new web pages.

3. Enter the default administrator account credentials: username is `administrator` and password is `compliance.`

   When logging in for the first time, the administrator does not get to log in using a domain name. If you are planning to set up multiple LDAPs, the administrator has to configure an LDAP Server to allow the users to authenticate based on their domain. For more information on how to set up an LDAP, see Configuring an External Authentication Server.

   The default system administrator account manages the server configuration and locked content, such as licensed Risk and Control Content packs**.**

4. Click **Log In**.

5. Click **Accept**.

6. You must change the default password the first time you log in.

   > [i]   The system administrator can add system administrator accounts only. Use the
   > Administrator account to create other kinds of the user accounts.

7. Go to **Administration** > **Server Administration**.

8. Click **Commands**

9. Click **Recreate** in the **Search** section. This will build your search indexes for improved search capability.

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. (Optional) Verify the success of the import by running the following command:

   `>` `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. But, if you need to connect the JasperReports Server over HTTP, you must make the following changes to the `agiliance.properties` file, available in the `%AGILIANCE_HOME%\config` directory:

- Enable the property `jasper.use.secure.connection=false`

- Enable the `jasper.admin.port=8480` property

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

There are times when users run Jaspersoft reports within RiskVision, such as when using the RiskVision Contextual Reporting feature and when running a Jasper report attached to a RiskVision tab. The communication of the available Jasper reports to the RiskVision UI relies on 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 and `jasper.api.SSLcertificate.validation=true` install an SSL certificate. The default value of the property is false.

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

Access JasperReports Server in Resolver RiskVision

JasperReports Server can be accessed in two ways: using the RiskVision system and in a standalone mode.

Accessing the JasperReports Server From Within the RiskVision Application

To access the JasperReports Server from within the RiskVision application:

1. Log in to the RiskVision application.

2. On the **Analytics** menu, click **Analytics and Reporting**. The JasperReports Server application is launched.
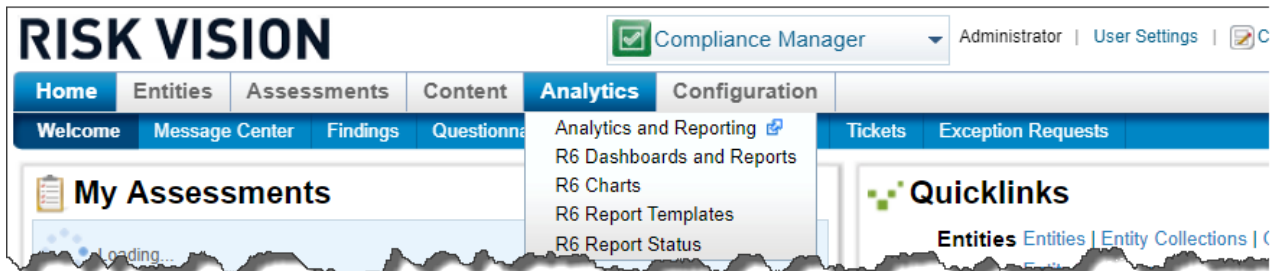
If problems arise accessing the JasperReports Server, see the Troubleshooting JasperReports Server Installation.

Launch JasperReports Server in Standalone Mode

Although the JasperReports Server application can be accessed through the RiskVision application, you can also launch the JasperReports Server application in standalone mode from the localhost in which the JasperReports Server is installed. This can be the preferred method by administrators to administer the JasperReports Server application. Essentially, you will need to connect to the JasperReports Server in standalone mode for the purpose of creating a user account that will be used to establish a connection between the JasperReports Server and Jaspersoft Studio Professional applications.

To launch JasperReports Server in a standalone mode from local host:

1. From the JasperReports Server installed system, open a browser and enter the following URL:

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

   Where is the JasperReports Server name and is the default port number '8480,' which is utilized by the JasperReports Server for communication.

2. When the login page is displayed, 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.

Set up the Encryption Compatibility between RiskVision Server and Jasper Reports Server

With object Id encryption in 7.5 and later, you might experience compatibility issues between RiskVision Server and JasperReports Server. The cases where you will encounter the compatibility issues, include the following:

- When clicking on a link in a Jaspersoft report to drill down to a view of specific object in the RiskVision, the parameters in the link need to be encrypted.

- When inserting a Jasper report such as custom tab of a detailed view of an object. The ID of that object is sent to the JasperReports Server in the encrypted format when the report is displayed.

To avoid the compatibility issues, the agiliance.keystore file in RiskVision Server and JasperReports Server needs to be identical. The steps to accomplish the encryption compatibility are given below:

1. In the RiskVision Tomcat application server host, go to the `%AGILIANCE_HOME%\config` directory, and copy the `agiliance.keystore file.`

2. Place the `agiliance.keystore` file in the `%JASPER_HOME%\Agiliance` directory.

3. Restart the jasperreportsTomcat service to apply the changes.

If you encounter hyperlink errors in Jaspersoft reports, please obtain the Resolving Hyperlink Errors in Jaspersoft Reports technical note from RiskVision Customer Support for detailed instructions on resolving hyperlink errors. Check whether the error that you have encountered is available in the Example Hyperlink Error Scenarios section and try resolving the errors. If all your attempts to resolve the errors have been failed, please contact Resolver Support.

Troubleshoot the JasperReports Server Installation

The following is a list of common problems that may arise while installing the JasperReports Server. JasperReports server does not support IE 8 or IE Compatibility mode.

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

The Analytics and Reporting submenu allows you to launch JasperReports Server. If its missing from the **Analytics** menu:

1. Go to the `%AGILIANCE_HOME%\apache2\conf\extra\` directory location, open the `workers.properties` file using a text editor, 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. Restart the RiskVision Apache and RiskVision Tomcat services if you made any changes to the agiliance.properties file.

Problem II: The Jasper RiskVision Analytics server is currently unavailable

Launch JasperReports Server from the Analytics menu. If you see the message "the Jasper RiskVision Analytics server is currently unavailable," verify the JasperReports Server installed directory in the following order:
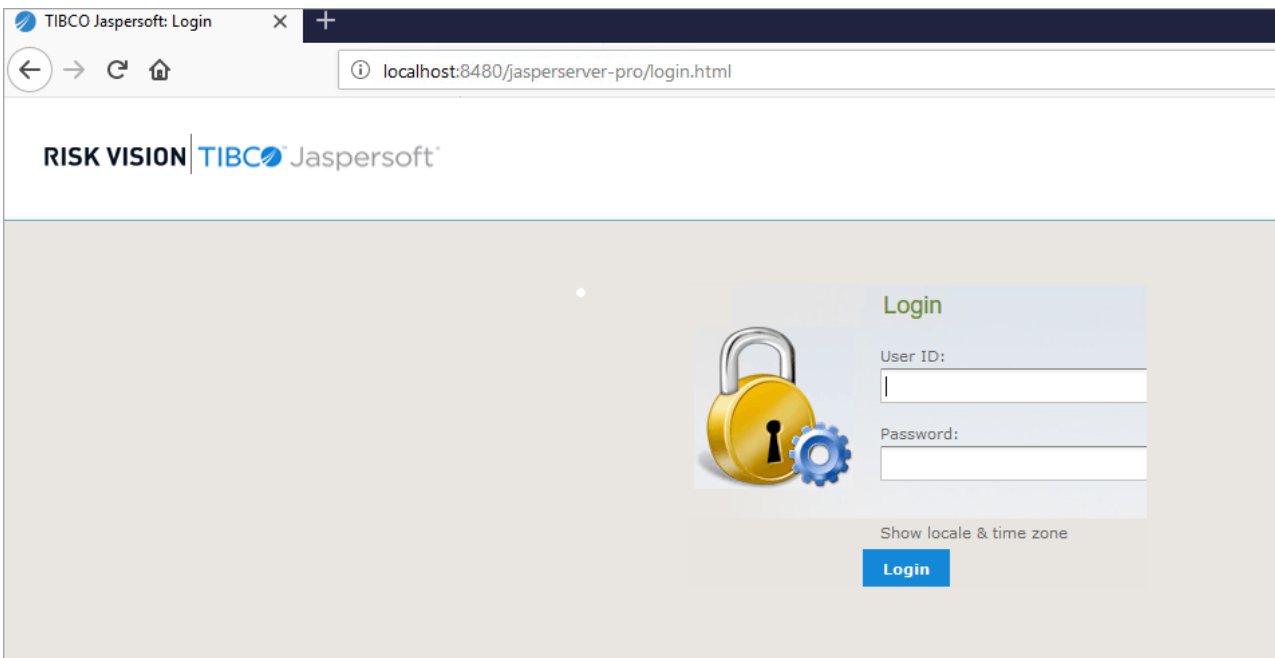
1. Launch the JasperReports Server in a standalone mode:
   - Ensure Jaspersoft services jasperreportsPostgreSQL and jasperreportsTomcat are running.

   - Go to:

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

Where the is the IP address of the JasperReports Server.

- Enter the **User ID** sysadmin and **Password** agiliance in the JasperReports Server Login page.

- If the JasperReports Server homepage appears: See
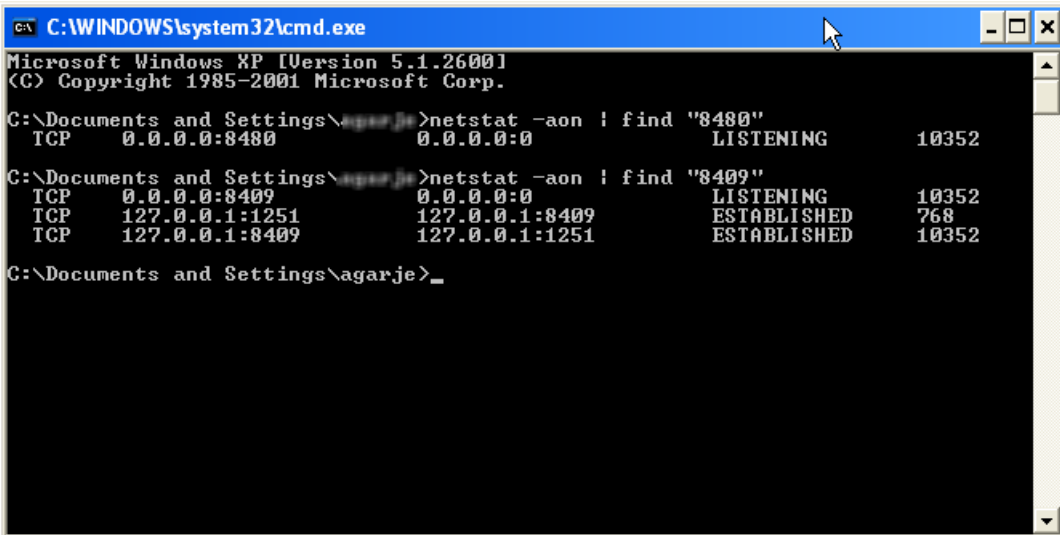
2. If you see the error message "Unable to launch the JasperReports Server": JasperReports Server is not installed properly.

3. Go to the `<%JASPER_HOME%>\Agiliance\scripts` directory to ensure Jaspersoft services is working.

4. Open the `initdb.log` file 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.

5. If there are no errors in the file `initdb.log` , stop Jaspersoft services, go to the following directories, back up the log files, and then delete all the log files:

   `%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 Windows Command prompt to verify whether the ports '8480' and '8409' are listening.

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


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

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

7. 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%\Agiliance\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%\Agiliance\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

8. If there are missing files or inappropriate file contents, copy the file from the source directory to the target directory.

9. Restart the Jaspersoft services if changes were made. The changes are applied to the JasperReports Server installation directory and JasperReports Server should launch.

10. 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:

   - **MySQL**:

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

   - **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 Setup

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

To verify the JasperReports Server installation:

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

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

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 into RiskVision and launch the JasperReports Server.

4. If the problem persists, go to the `%AGILIANCE_HOME%\config` directory, open the `agiliance.properties` file 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 the RiskVision Connector Manager

Install the Connector Manager on the Application Server, or on a Windows server that is reachable by both the legacy connector, the RiskVision Tomcat Server host, and the database host.

To install the RiskVision Connector Manager:

1. Copy the following files to the server that will host the RiskVision Connector Manager.

File	MySQL	Oracle
riskvision.license	✔	✔
RiskVisionConnectorManagerInstallation.exe	✔	✔
mysql-connector-java-5.1.39.zip	✔	✘

2. Double-click the RiskVisionConnectorManagerInstallation.exe file to launch the **Resolver Connector Manager Setup** wizard.
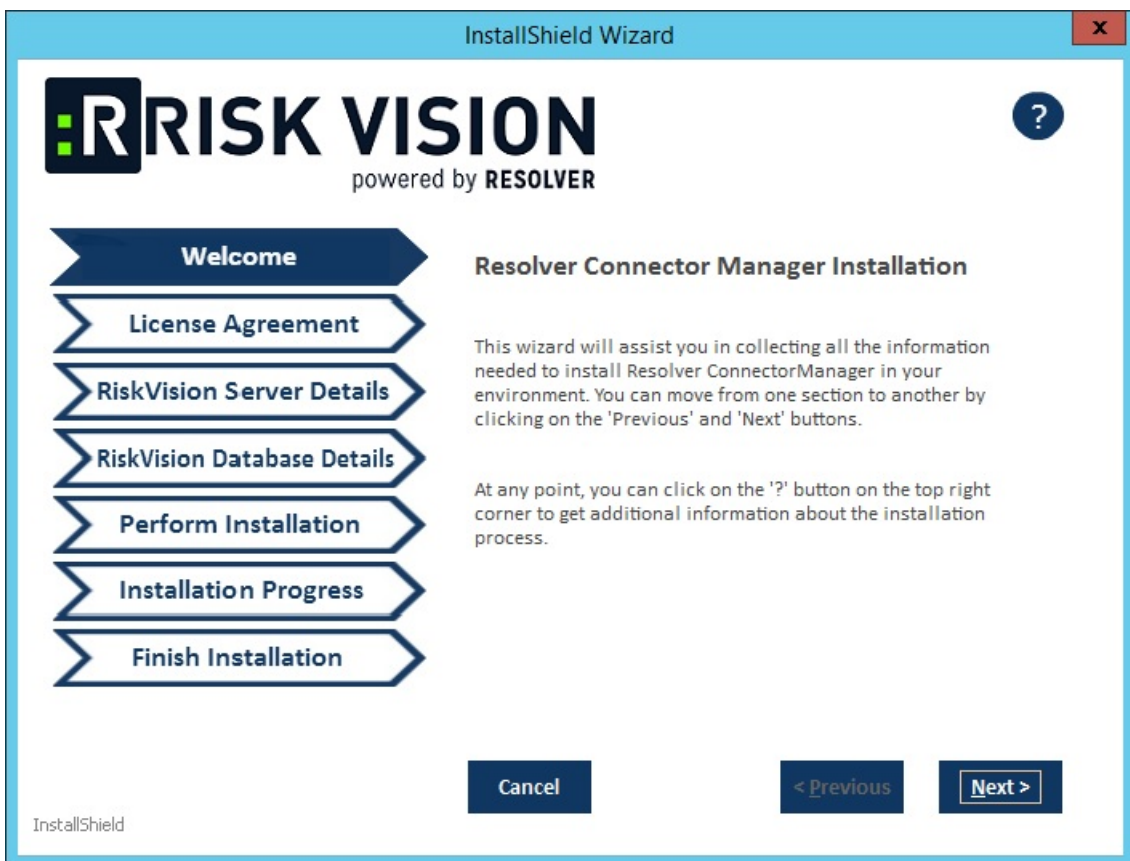
In the **Welcome** wizard page, Click **Next** to continue.

3. The **License Agreement** wizard page appears. Select **I accept the terms in the License Agreement**.
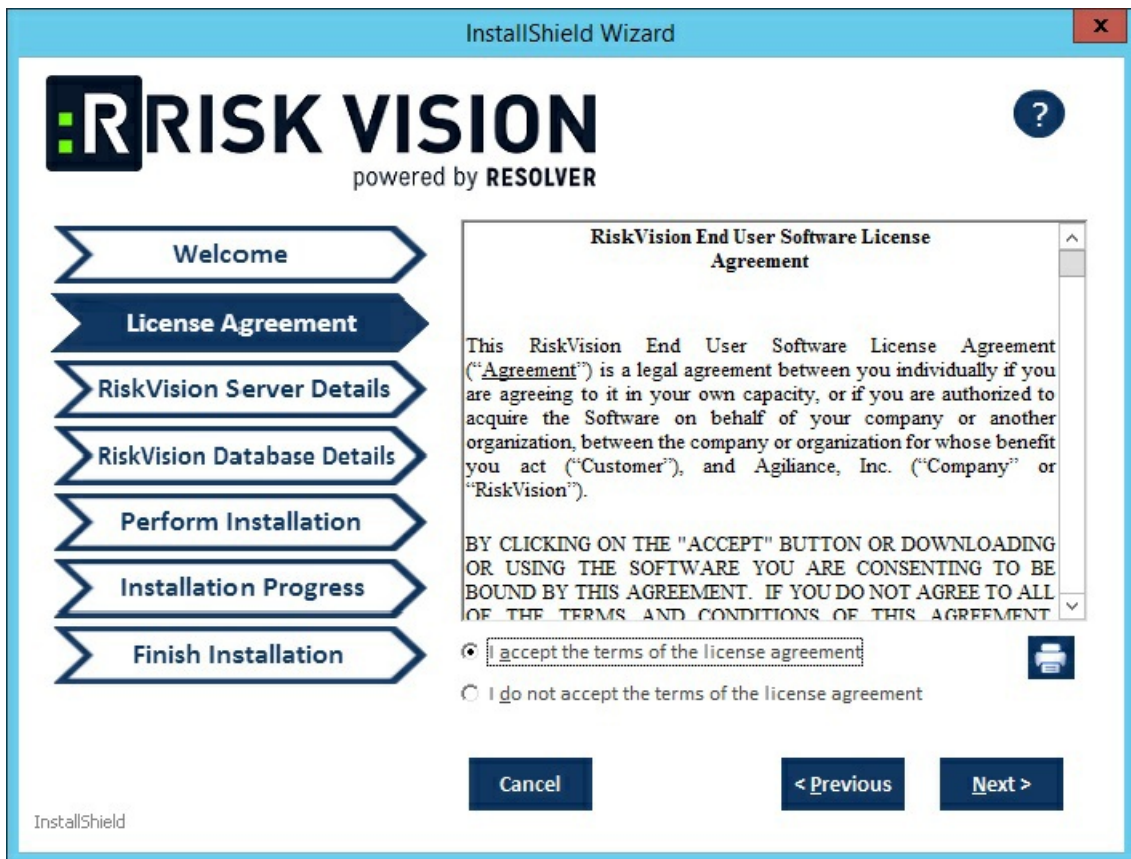
Click **Next** to continue.

4. The **RiskVision Server Details** wizard page appears.

Enter the server hostname in the **RiskVision Server Hostname** text box and then select the Database.

For MySQL, this wizard page contains the options as shown below:
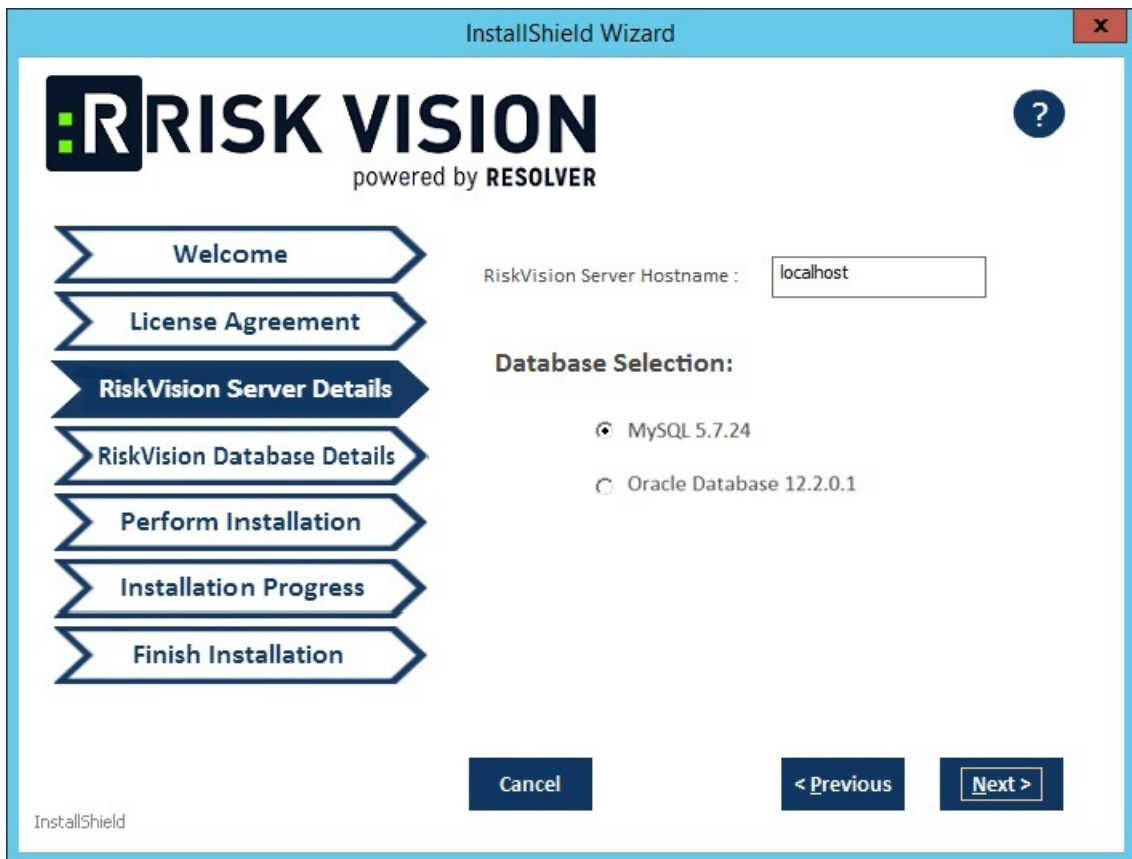
5. Click **Next** to continue.

6. The **RiskVision Database Details** wizard appears, enter the following fields, which appear based on the database type selected.

   For the MySQL instance, this wizard page contains the options as shown below:

Field	Description
Database Username	The database user.
Database Password	The database password for the user.
Database Confirm Password	Enter the same password one more time to ensure that the password entered is correct.
Database Hostname	The fully qualified domain hostname of RiskVision database (MySQL or Oracle). Enter `localhost` if the RiskVision database is on the server where you are currently running this installer.
Database Port	The port number of MySQL or Oracle.
Database Service Name	(Required only for Oracle). The service name by which the RiskVision Connector Manager can connect to the Oracle database instance.

7. Click **Next** to continue.

8. The **Perform Installation** wizard page appears.
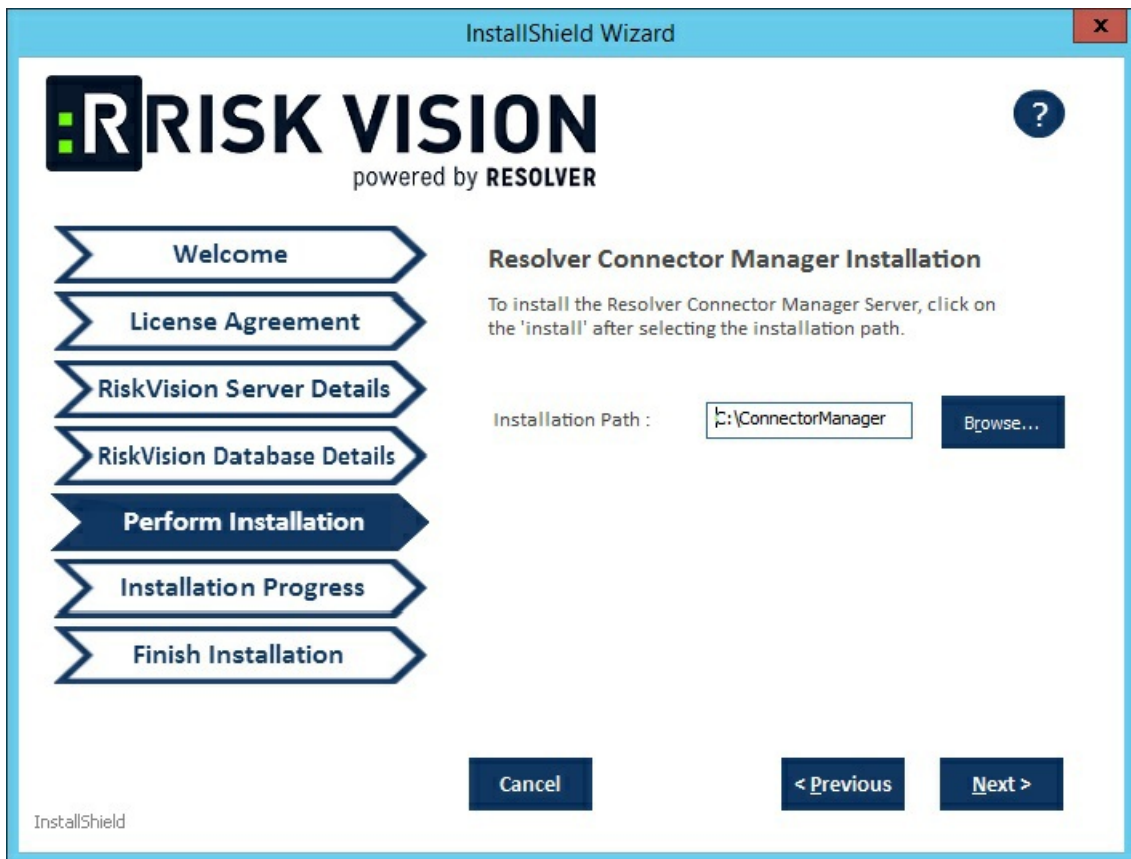
By default, the RiskVision Connector Manager is installed in the directory `C:\ConnectorManager\` path. The installer sets the environment variable to `%AGILIANCE_HOME%` the product installation path specified here. Click **Browse** and select the path to install the RiskVision Connector Manager in a different directory.

9. Click **Next** to continue.

10. The **Installation Progress** wizard page appears. Click **Install** to begin the installation process.
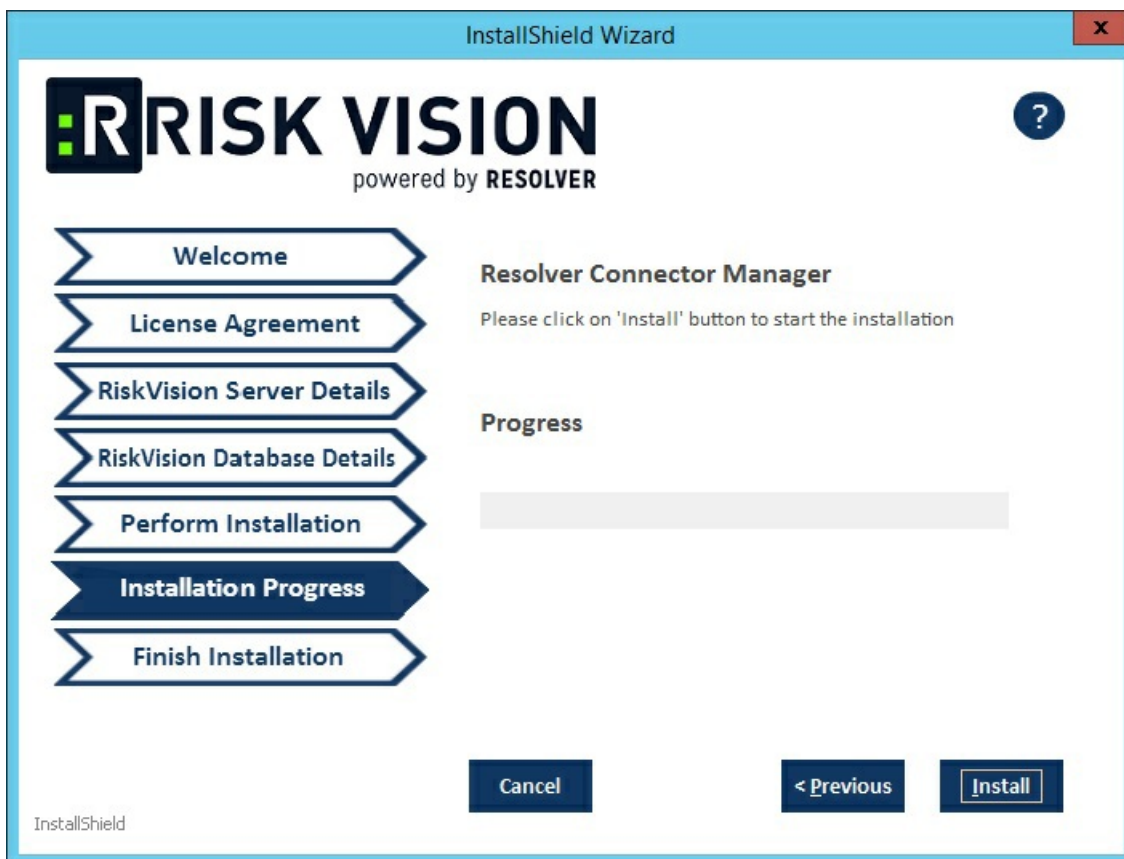
During the Connector Manager installation process, the setup wizard opens one or more command windows; do not close the windows. Allow sufficient time for the setup to automatically close the command windows and to conclude the installation successfully.

11. The **Finish Installation** wizard appears after the setup concludes successfully, click **Finish** to exit the wizard.

Post-Install Configurations

This section explains how to set up the Connector Manager to use with the RiskVision Server.

After installing the Connector Manager, the property `com.agiliance.agent.isIndependentAgent=true.` gets automatically added to the file `%ConnectorManager_HOME%\config\agiliance.properties`. To make the RiskVision Server and the RiskVision Connector Manager work, perform the following steps:

`com.agiliance.agent.useIndependentAgent=true`

`com.agiliance.agent.isIndependentAgent=false`

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

1. In the RiskVision Tomcat Application Server host, go to the `%AGILIANCE_HOME%\config` directory, open `agiliance.properties` file using a text editor, and add the following properties:
   `com.agiliance.agent.useIndependentAgent=true`

   `com.agiliance.agent.isIndependentAgent=false`

2. Restart the RiskVision Tomcat service to apply the latest changes.

3. If you using a MySQL database, run the following MySQL commands to connect the Connector Manager.

The RiskVision Connector Manager works on port 9443 make sure that all the connectors connect to the RiskVision Connector Manager using port 9443. All the stand-alone connectors, except the Email Connector and Authentication Connector, must point to the RiskVision Connector Manager.

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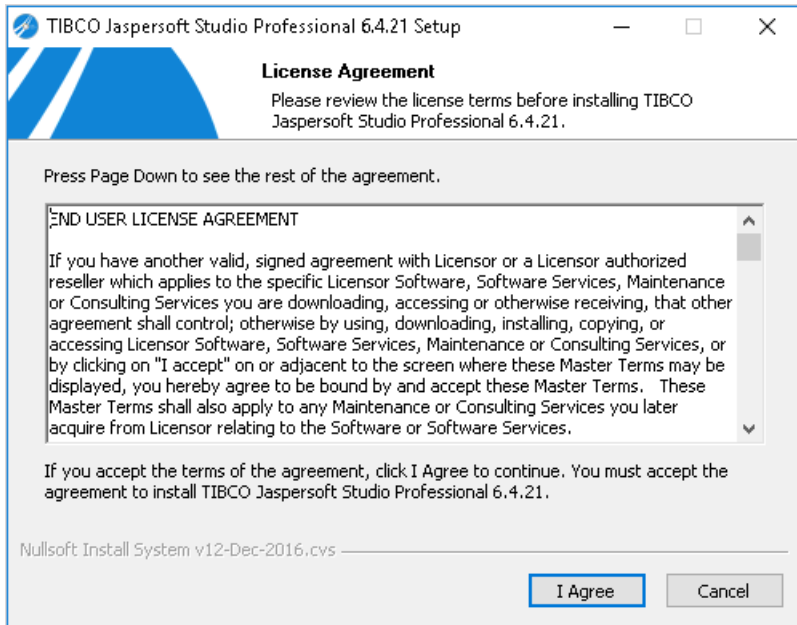
Click **I Agree** to accept the license agreement and to continue.

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.
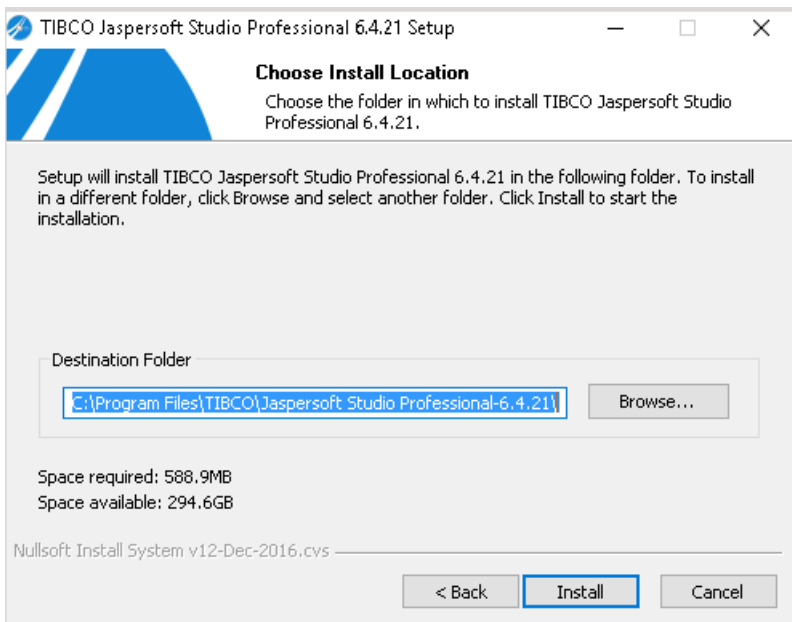
Click **Install** to start installation.

4. The set up now prepares the settings required by the installation scripts based on your previous selection.
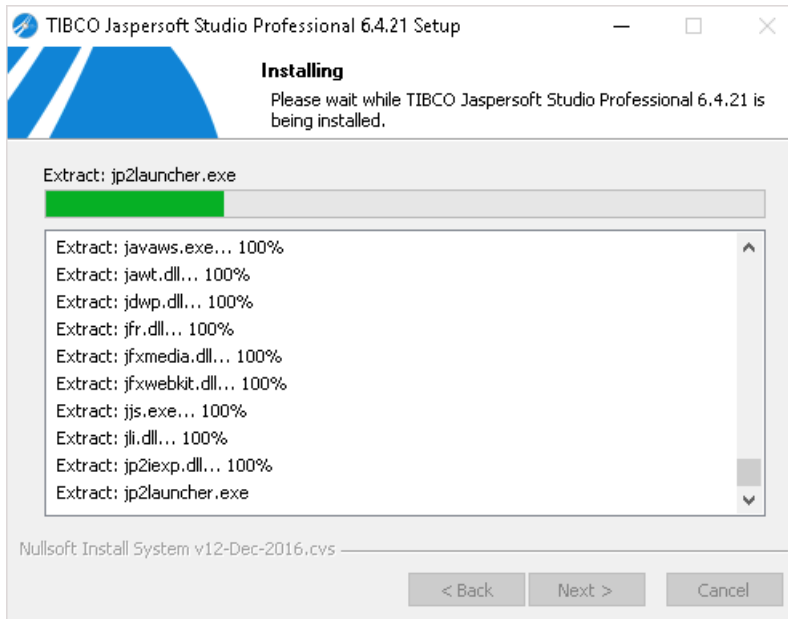
5. After the installation is complete, click **Finish** to exit the wizard and to launch the TIBCO Jaspersoft Studio Professional application.

6. Perform the following additional tasks to complete the TIBCO Jaspersoft Studio Professional installation:
   - Set up a Jaspersoft Studio License. See Installing the Jaspersoft Studio Professional License.

   - Set up a connection to the RiskVision database and JasperReports Server repository. See Setting up Jaspersoft Studio Professional.

.

Install the Jaspersoft Studio Professional License

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

To install the license:

1. Obtain the `jasperserver.license` file from the JasperReports Server installation directory. The default location is `%JASPER_HOME%\.` 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**,then click **License Manager**.
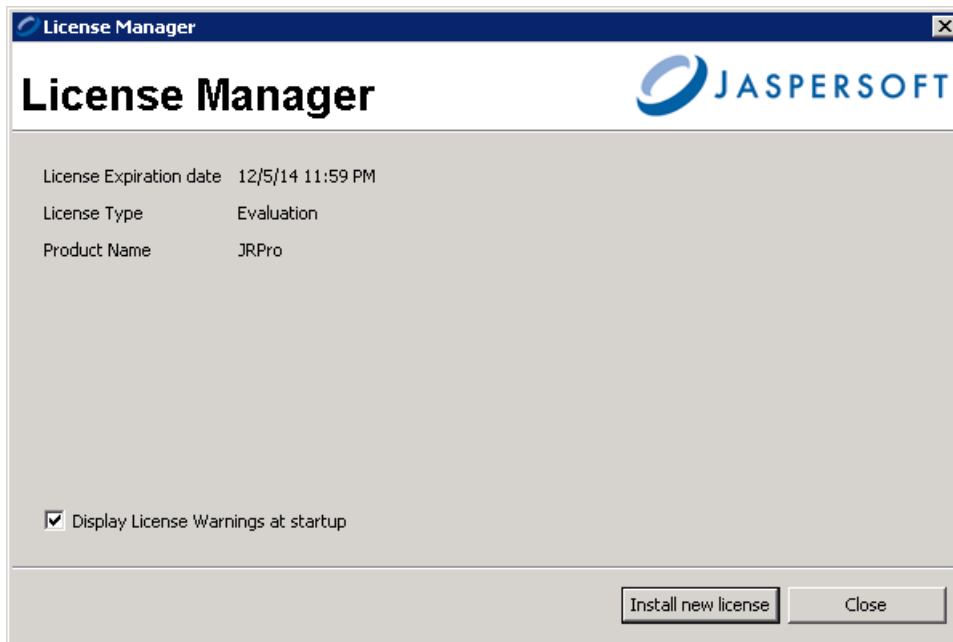
The License Manager dialog.

4. Click **Install new license**.

5. Select the `jasperserver.license` file from the appropriate location, then click **Open**.

6. Click **OK**, then click **Close**.

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 Jaspersoft Studio Professional.

2. Click the **File** menu > **New** > **Data Adapter**.

3. Select the parent folder. The data adapter settings, by default, are saved in the NEW_DATAADAPTER file. Rename the file, if required.
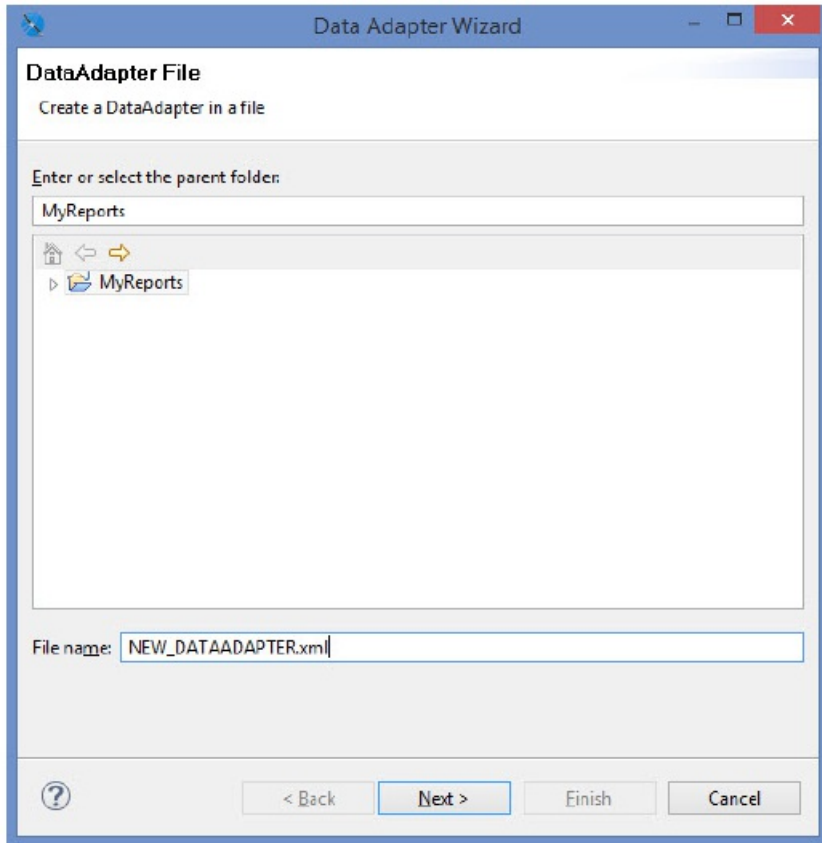
The Data Adapter File wizard page.

4. Click **Next**.

5. The **Data Adapters** wizard page appears. Click **Database JDBC Connection**.
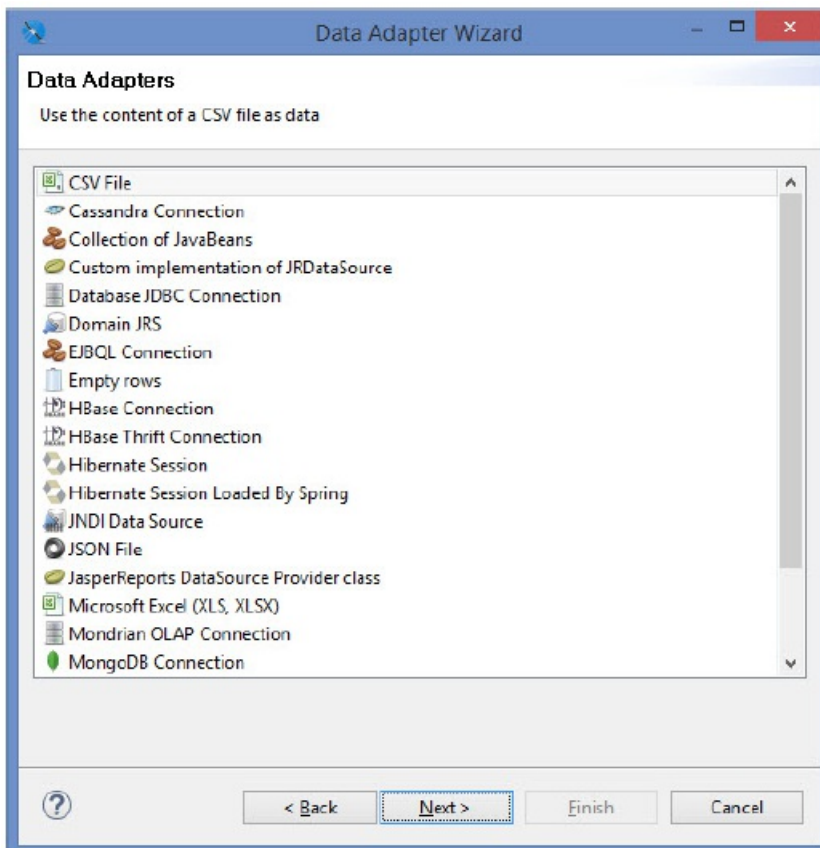
6. Click **Next**.

7. Enter the 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 selec **t 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
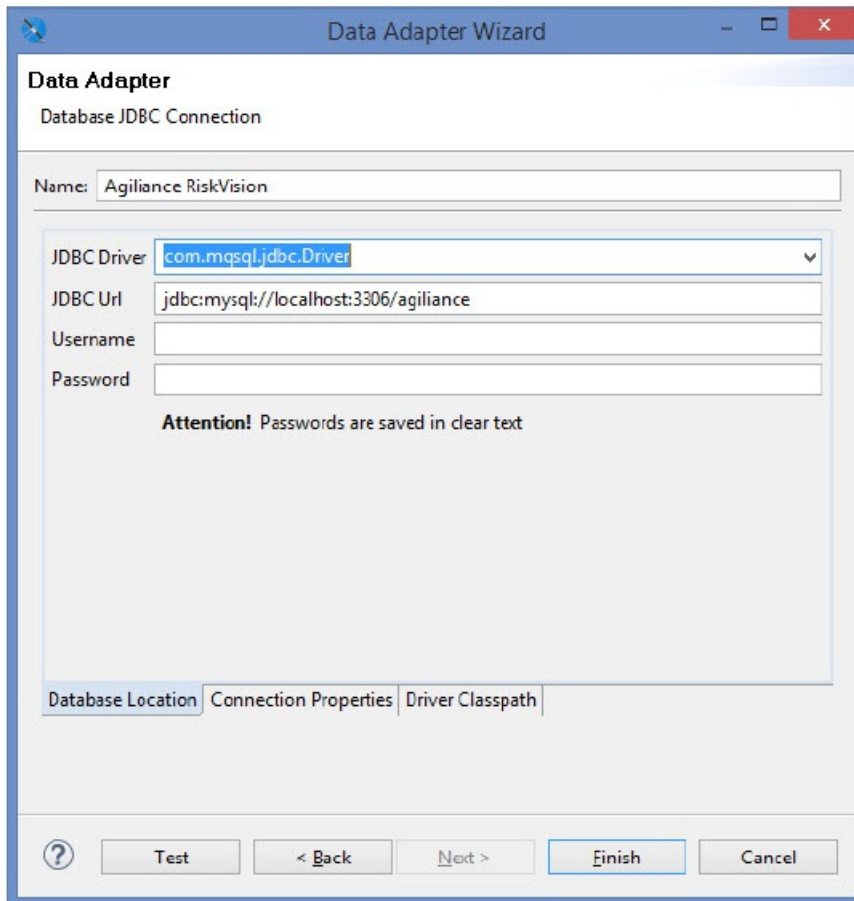
The Database Location tab.

8. Click the **Driver Classpath** tab. Click **Add**. Select the jar file for the database from the appropriate directory, then click **Open**. The JDBC Driver jars file for the MySQL and Oracle databases are:

   MySQL. mysql-connector-java-5.1.39-bin.jar
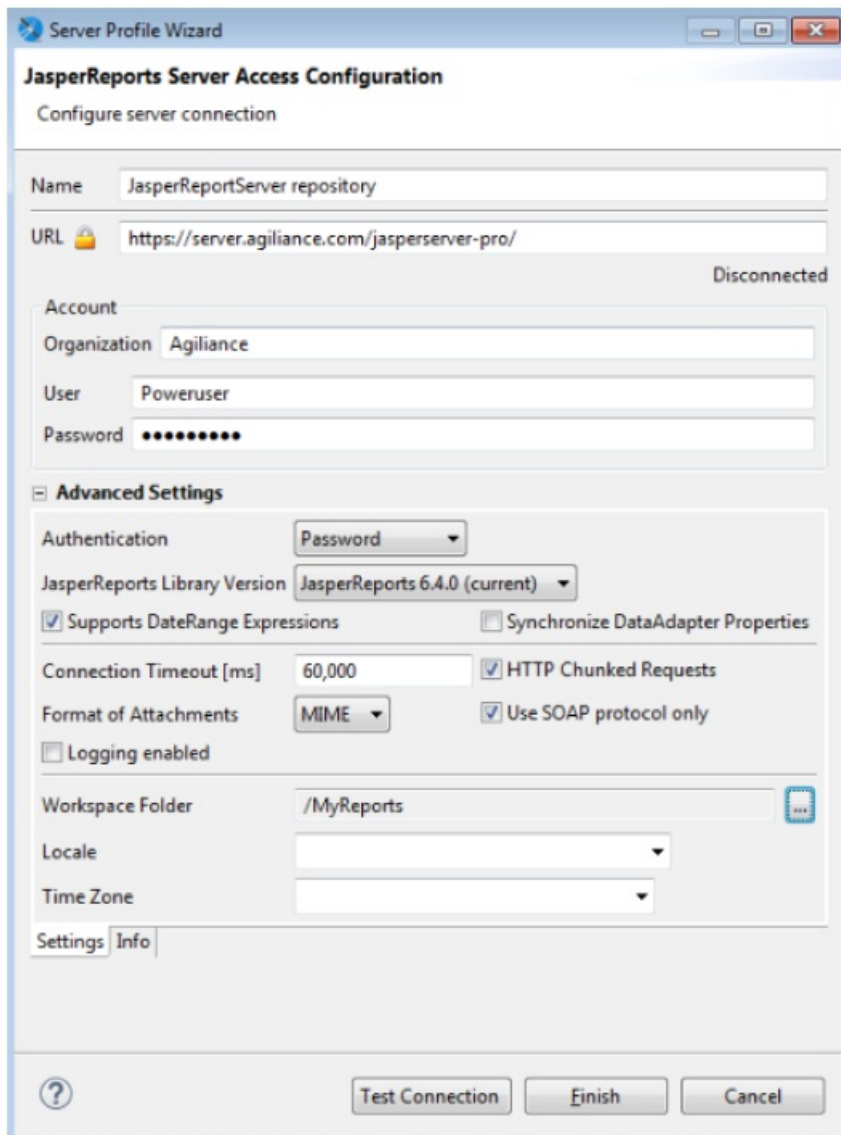
   Oracle. ojdbc6.jar

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

10. Click **Finish** to save the connection and exit the **Data Adapter Wizard**.

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.

Manage JasperReports Server using Command Prompt

By default, a user with administrative privileges that installs the JasperReports Server is allowed to manage tasks in the JasperReports Server from the Windows Command Prompt. If more users need access to the JasperReports Server host to manage their individual tasks from the Windows Command Prompt, you will need to copy the keystore files (.jrsks and .jrsksp) into the users' work environment.

*Note: **These steps are only required up for RiskVision Version 8.5 and older** Before starting, take a backup of the .jrsks and .jrsksp files and delete them from the user directories. You will also need to backup these files before upgrading to 9.0.*

Copy the Keystore Files:

1. Log in to the JasperReports Server host with the user account that you have used to install the JasperReports Server, go to the C:\Users\ directory, and then copy the .jrsks and .jrsksp files.

2. Switch the user account on the JasperReports Server, go to the C:\Users directory, and then paste the .jrsks and .jrsksp files.

   Where is the user account with administrative privileges on the JasperReports Server host.

   Similarly, copy the keystore files into each user's work environment that need to perform tasks from the Windows Command Prompt.

Secure the Jaspersoft Installation

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

JasperReports Server

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

- `rvJasperUser` - This user is created for the tenant, which is used for the web services by the RiskVision system. Ensure that you do not delete the internal user 'rvJasperUser.' Because when the `rvJasperUser` user is deleted, the web services connectivity from the RiskVision system to the JasperReports Server is lost.

- However, you can change the password of `rvJasperUser` user 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 of 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 and then change the password.

Uninstall the RiskVision Server

Before uninstalling the RiskVision application and database, uninstall the connectors.

The uninstall process does not remove backup files, configuration files, or connectors. If you do not need to keep the backup files, configuration file customizations, uploaded data, reports, dashboards or logs, delete the installation folder.

To uninstall the RiskVision Server:

1. On the Microsoft Windows **Start** menu, select **Programs** > **RiskVision Server** > **Uninstall RiskVision**. The RiskVision Uninstallation wizard appears. Click **Next** to continue.
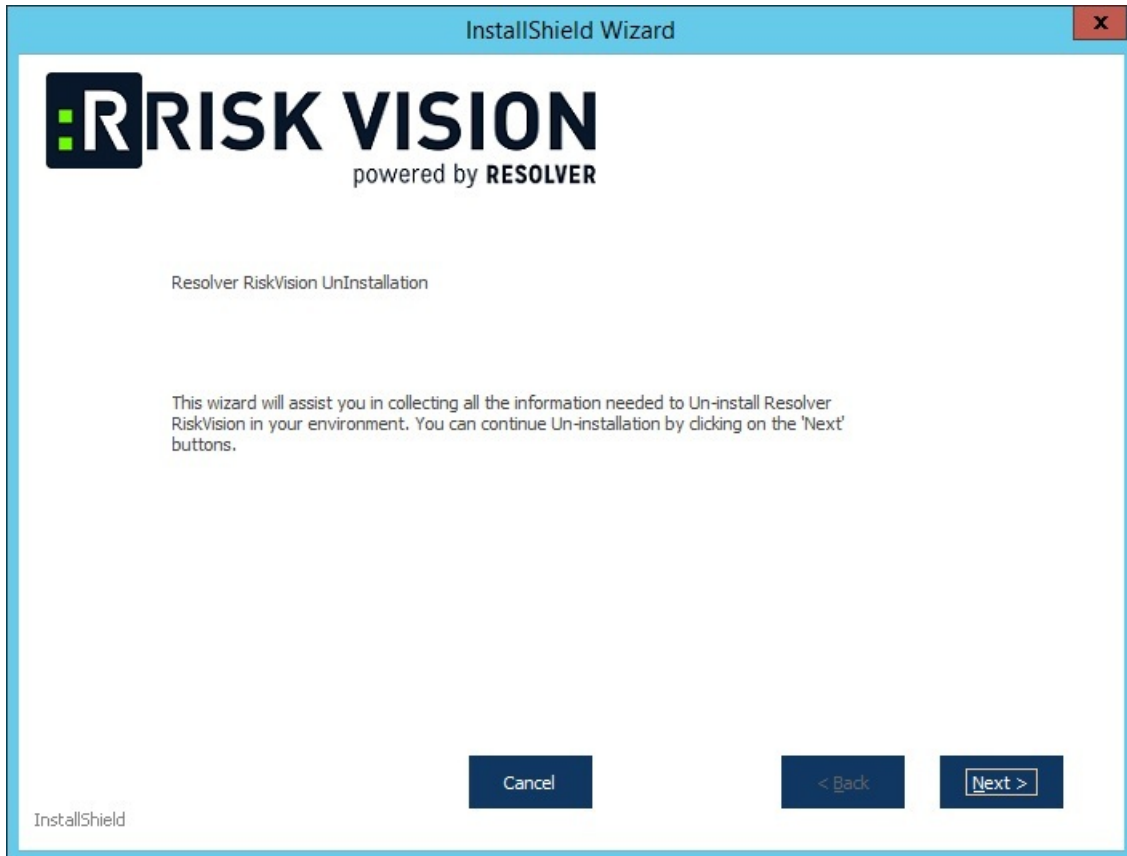
2. The **RiskVision Uninstallation** wizard modifies, select the **Uninstall Database Server** option to delete the data. Click **Next** to continue.
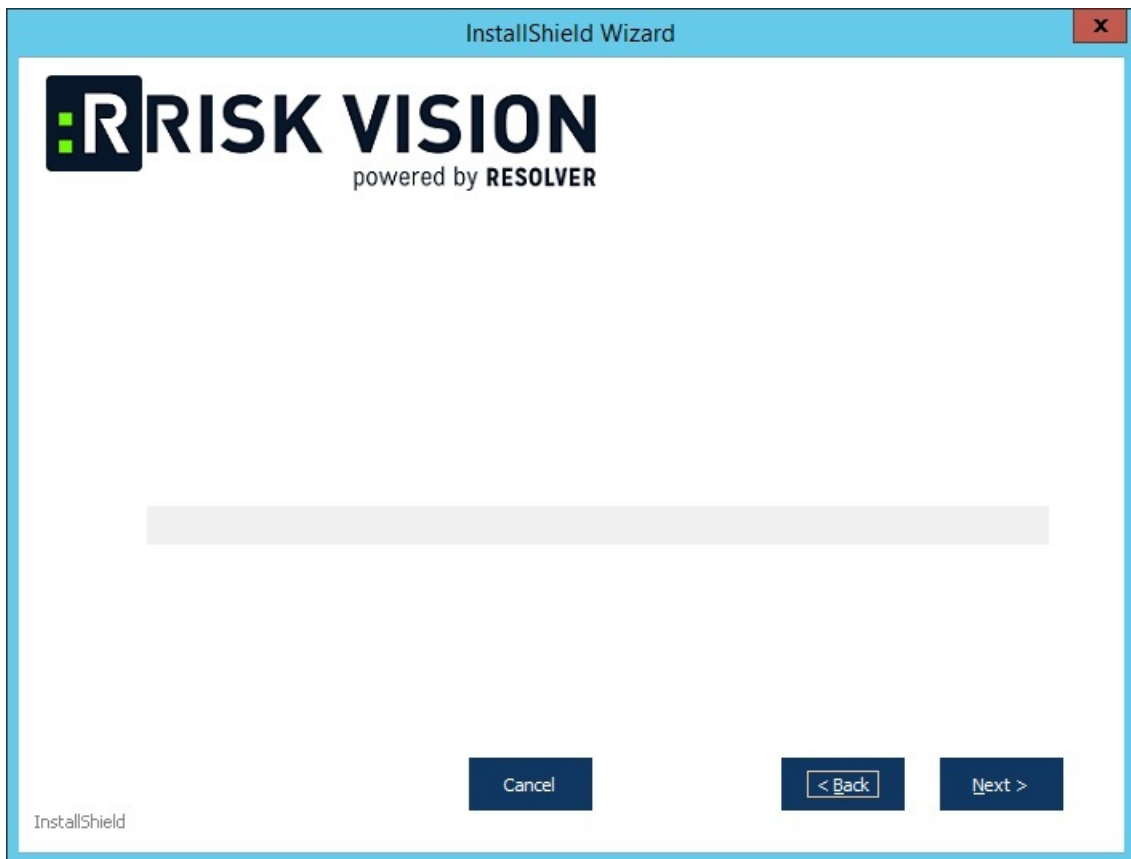
3. Click **Uninstall** option, then the uninstallation of RiskVision starts.

4. Once the RiskVision uninstallation is done, click **Finish** button, the **RiskVision Uninstallation** wizard closes.

Selecting from available options will complete uninstalling the RiskVision Server.

Uninstall the RiskVision Connector Manager

Before uninstalling the RiskVision Connector Manager, uninstall the connectors and RiskVision Server.

The uninstall process does not remove backup files, configuration file customizations, or connectors. To remove these items, delete the installation folder.

To uninstall the RiskVision Connector Manager:

1. Open the Microsoft Windows Start Menu. Click **Programs** > **Connector Manager** > **Uninstall** to open the **ConnectorManagerUninstaller-InstallShield** wizard appears.
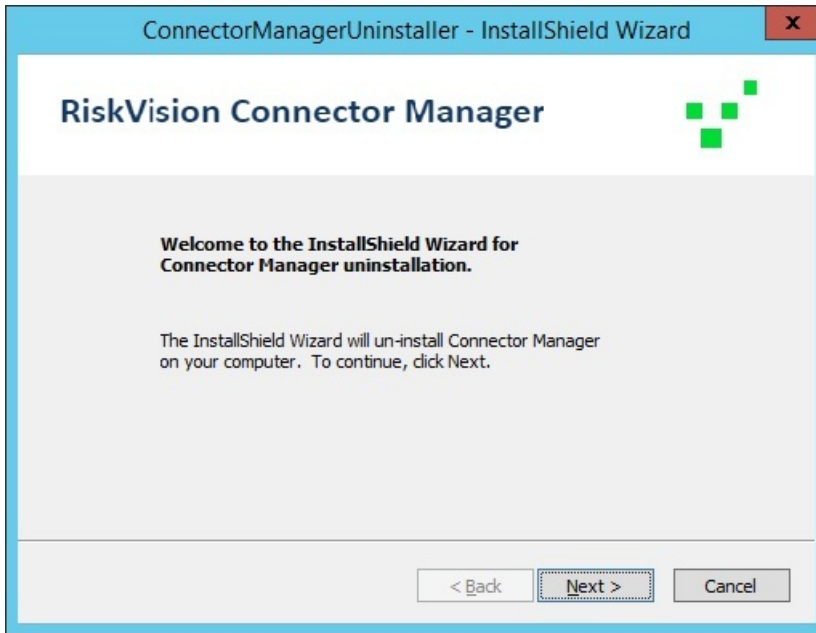
2. Click **Next**, then click **Uninstall**.
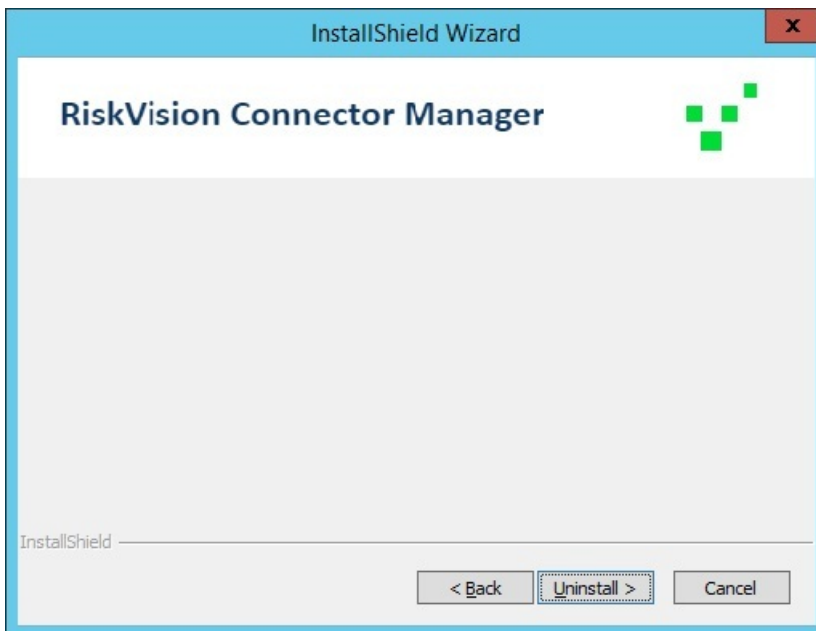
3. Click the **Finish** button to exit the wizard
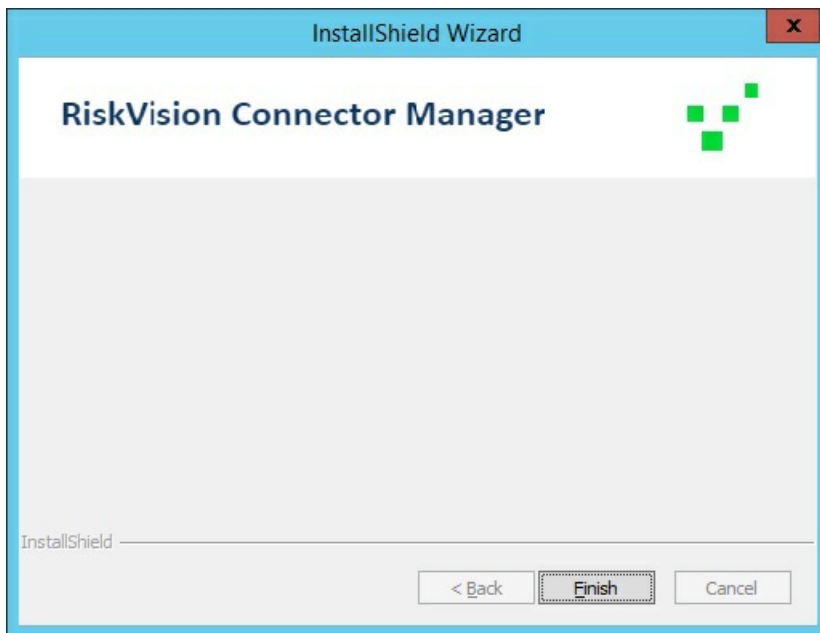
Uninstall Jaspersoft Studio Professional

To uninstall TIBCO Jaspersoft Studio Professional:

1. Go to **Start > TIBCO > Jaspersoft Studio Professional-6.4.2.1.final** and click **uninst**.

2. Click **Yes**.
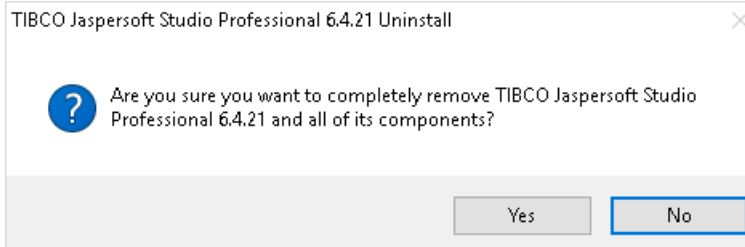
3. Allow sufficient time for uninstallation. If you close the window, the process will be canceled.
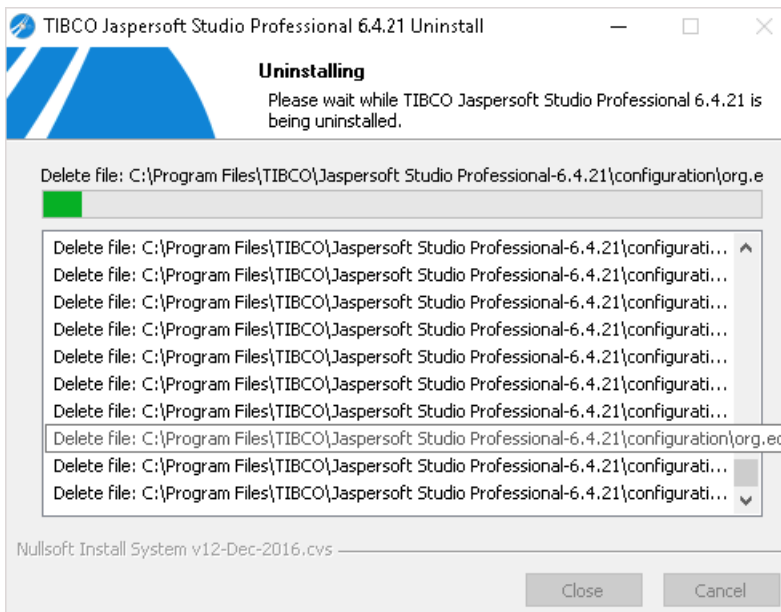
4. Click **OK** to exit the dialog.
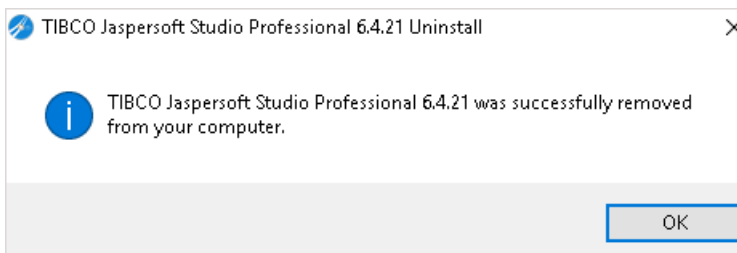
Leftover Files and Folders

The uninstallation process leaves behind certain files and folders. The leftover files and folders from the removal of different software components are listed in the table below:

Software	Files/Folders
RiskVision Server	During the RiskVision Server Uninstallation: If the uninstall DB option is selected, the leftover folder is: %Agiliance_HOME%\Uninstall If the uninstall DB folder option is not selected, the leftover folders are: %Agiliance_HOME%\Apache24 %Agiliance_HOME%\apache-tomcat-8.5.35 %Agiliance_HOME%\backup %Agiliance_HOME%\data %Agiliance_HOME%\MySQL %Agiliance_HOME%\mysql-5.7.24-winx64 %Agiliance_HOME%\OpenOffice %Agiliance_HOME%\Uninstall
RiskVision Report Server	%JASPER_HOME%\ %JASPER_HOME%\java %JASPER_HOME%\postgresql %JASPER_HOME%\rolbackBackupDirectory

Uninstall RiskVision Report Server

To uninstall the RiskVision Report Server:

1. Go to **Start > RiskVision Report Server**.

2. Click **Uninstall Report Server**.

3. Click **Yes**.
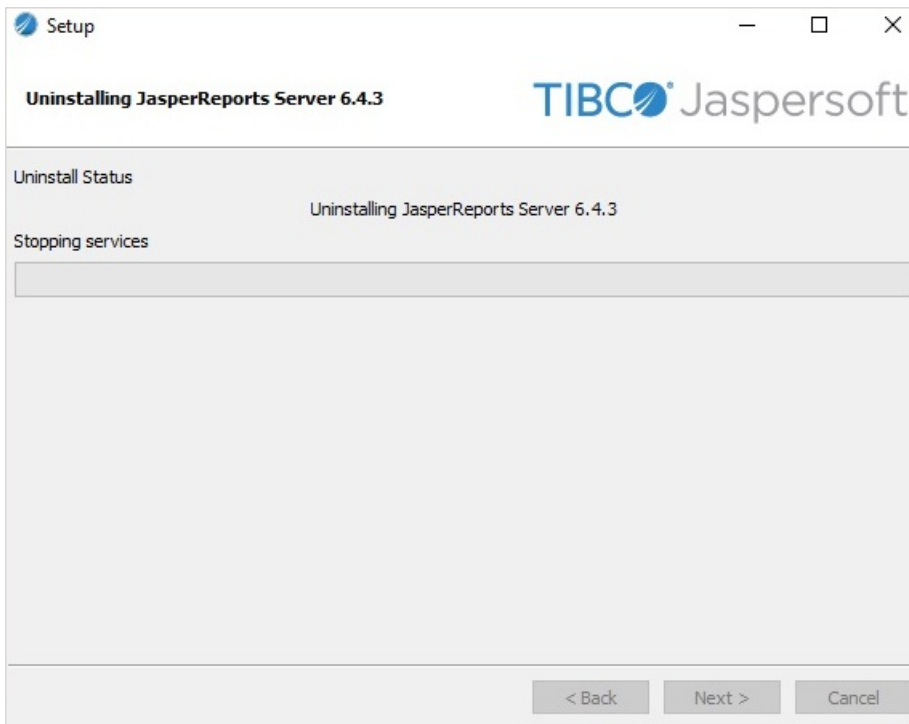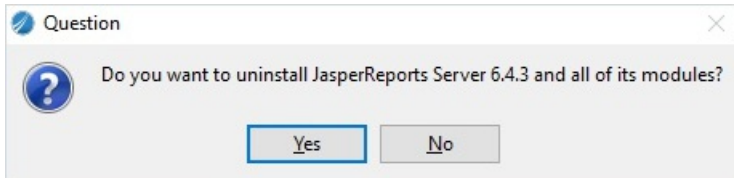
4. Click **No**.
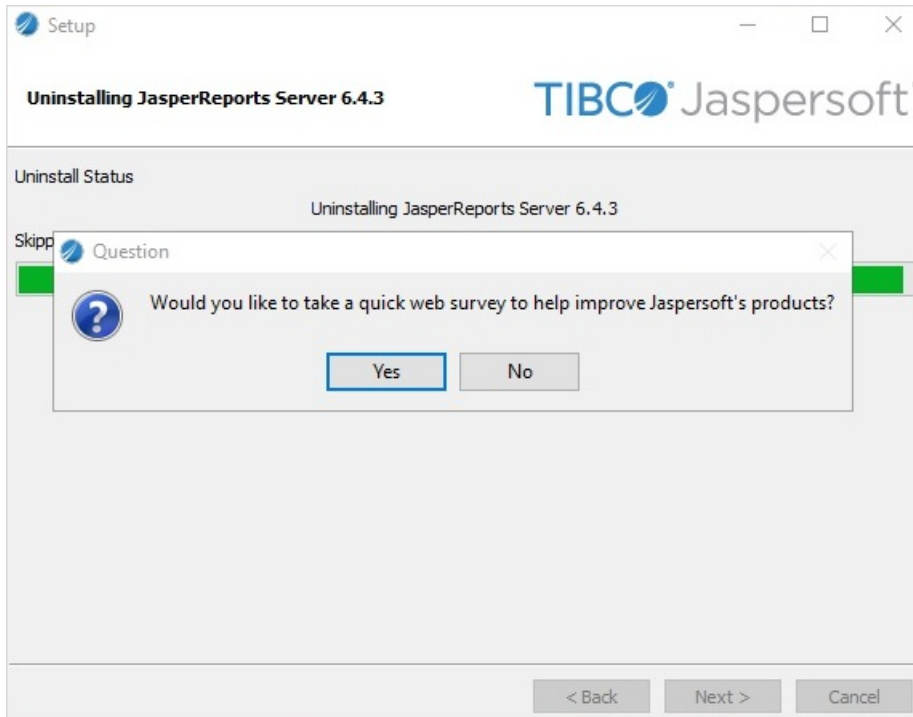
5. Click **OK**.
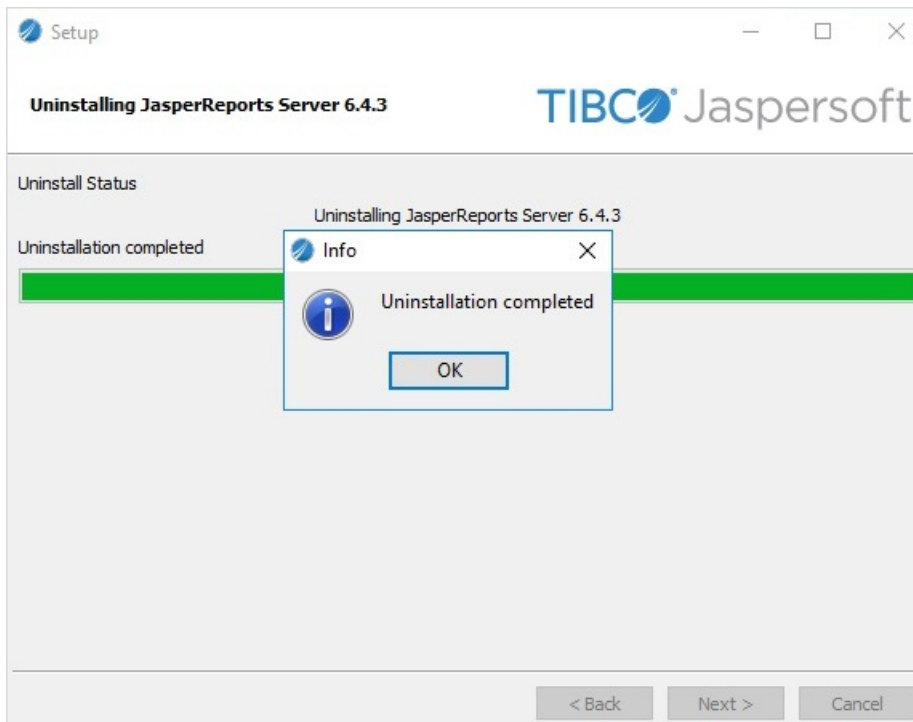
Modify Default Properties

The RiskVision uses a number of different server property and XML configuration files to set parameters and customize operations of the Console, and the database.

On the computer where the is installed, default properties and configuration settings are specified in the files `agiliance.default.system.properties` and `agiliance.default.application.properties` located in the directory:

`%Agiliance_HOME%\Tomcat\webapps\spc\WEB-INF\classes`

Do not modify files in the directory `WEB-INF\classes` ; changes will be overwritten without warning.

Add properties that you want to override to the file `config\agiliance.properties` . This file must contain only overrides, but not default values for properties that do not need to be overridden. Copying blocks of properties from the default files and leaving them unmodified in `config\agiliance.properties` may impact performance.

To override the default settings:

1. Edit the file: `%AGILIANCE_HOME%\config\agiliance.properties`

2. Add the property that you want to override.

3. Reload the configuration file

   - Log in using a system administrator account.

   - Go to **Administration** > **Server Administration** > Commands.

   - In the **Configuration** section, click **Reload**.

The change is applied.

Keep the file `agiliance.properties` as small as possible and only include overridden properties. This improves performance and upgrades easier in the future.

Set Up the Apache Web Server with Signed Certificates

If you are using a signed certificate for setting up Apache web server, you must perform the following tasks.

During the **.csr** file generation, provide the Apache web server public hostname, organization details, and the passphrase if the **.key** file is generated with the passphrase.

```
%AGILIANCE_HOME%\apache2\conf
```

To generate the .key file:

Apache supports either passphrase or **SSLFIPS ON**, but not both at the same time.

1. Download OpenSSL from **https://slproweb.com/products/Win32OpenSSL.html**.

2. Run the downloaded **.exe** file and follow the installation instruction to complete the OpenSSL installation.

3. After successful installation of OpenSSL, perform the following steps:

   > *[i]* If you are restricted from being able to modify your environment variables while using the command prompt, then navigate to the **%OpenSSL_INSTALL_LOCATION%\bin** folder to execute **openssl.exe** from the command line.

   a. Set the **Environment Variable** `OPENSSL_CONF`

   b. Add **OpenSSL** to the **PATH Variable**.

   c. To generate the **.key** and **.csr** files, run the commands below:

   ```
   openssl genrsa -out server.key 2048
   ```

   ```
   openssl genrsa –des3 -out server.key 2048
   ```

   ```
   openssl req -new -key server.key -out server.csr
   ```

To generate a certificate signing request:

Refer to How to Create Private Key, CSR and Certificates with OpenSSL for Apache.

The signed certificates and generated **.key** file should be placed in the **C:\Server\apache2\conf** folder.

If the .key file is generated with the passphrase:

1. Navigate to the **%AGILIANCE_HOME%\apache2\conf** folder and open the **passphrase.bat** file using a text editor.

2. Enter the passphrase and save the file.

3. Navigate to the **%AGILIANCE_HOME%\apache2\conf\extra** folder and open the **httpd-ssl.conf** file and change the **SSLFIPS ON** to **SSLFIPS OFF**.

4. Restart the Apache Service.

To change the passphrase:

1. Rename **server.key** to **server.key.org**.

2. Run the command: `openssl rsa –des3 -in server.key.org -out server.key`

3. Provide the new passphrase.

4. Navigate to the **%AGILIANCE_HOME%\apache2\conf\extra** folder and enter the new passphrase in the **passphrase.bat** file.

5. Restart the Apache Service.

To remove the passphrase:

1. Rename **server.key** to **server.key.org**.

2. Run the command: `openssl rsa -in server.key.org -out server.key`

3. Restart the Apache Service.

Change 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 the MySQL root account passwords:

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 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 for connecting to the MySQL or Oracle database.

To update the passwords used by the application:

1. Encrypt the root password with `encrypt.cmd.`
    - Open the command prompt and navigate to the directory `Server\install\toolbox\bin` .
    - 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 and `%AGILIANCE_HOME%\MySQL\bin` open the command prompt from that window.

2. In command prompt manually enter the 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 agiliance and new 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 the 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 %AGILIANCE_HOME%\config\agiliance.properties file and set the below mentioned 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.

Change the Password for JasperReports Server

RiskVision is using four different accounts to facilitate the tight integration with JasperReports Server. We recommend changing the default passwords for each of these accounts. The three accounts are as follows:

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 need to be changed in the below servers:

- MySQL database or Oracle database
- Application server
- Report server

For the MySQL database:

1. Navigate to `%AGILIANCE_HOME%\MySQL\bin` and open the 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 below command on the:

   ```
   > 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 the Oracle database:

`ALTER user IDENTIFIED BY`

For the Application Server:

1. Encrypt the reportuser password with encrypt.cmd.

2. Open command prompt and navigate to the `%AGILIANCE_HOME%\install\toolbox\bin` directory.

3. Run the command: `encrypt.cmd`

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. In file `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF\agiliance.properties` ,

   - Set the password for property

     For the MySQL database
     `database.mysql.password.encrypted=EncryptedString`
     For the Oracle database
     `database.oracle.password.encrypted =SchemaUserPasswordinEncryptedString`

   - Restart the ReportServer

2. 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

3. Log in with sysadmin credentials (username as sysadmin and password as agiliance)

4. On the View menu, click Repository

5. Expand the Public folder, select Data Sources, and edit the RiskVision JDBC data source.

6. Enter the new reportuser password

7. Test connection

8. Click Save

9. Restart the jasperreportsTomcat service.

Change the Password for the rvJasperUser

1. Go to the JasperReports Server host and access the URL by using a browser

2. http://localhost:8480/jasperserver-pro/login.html

   The JasperReports Server login page is displayed.

3. Go to **Manage** > **Users**

4. Select is `rvJasperUser` user

5. Click Edit

6. Change the password. The password is changed successfully.

If the unencrypted password is used to set the property, perform the steps below:

1. Open the `%AGILIANCE_HOME%\config\agiliance.properties` file by 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.

If the encrypted password is used to set the property, perform the following steps:

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 Password for the Sysadmin User

1. Go to the JasperReports Server host and access the URL by using a browser

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

   The JasperReports Server login page is displayed

2. Go to **Manage** > **Users**
3. Select **sysadmin user**
4. Click **Edit**
5. Change the password.

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 the command prompt, navigate to the `%JASPER_HOME%\buildomatic` directory, and run the command `js-ant refresh-config.`

7. On, the Report Server, replace `external.jdbc.password` value 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. On the Application Server, perform the following:

   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 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.`

1. In the `default_master.properites` file set the value of RiskVision Reportuser Password to dbPassword property (dbPassword is for the PostgreSQL database but for a workaround to generate RiskVision password we can use the dbPassword temporarily)

2. Set `encrypt=true`

3. Set `propsToEncrypt=dbPassword` ,sysPassword

4. In command line go to `%JASPER_HOME%\buildomatic`

5. Run `js-ant refresh-config`

6. Step 5 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 dbPassword with the PostgreSQL database password

9. Change `encrypt.done=true` to `encrypt=true`

10. Run step 4 and 5 again to fix the PostgreSQL password.

Keystore Password Encryption for Jasper Report Server

RiskVision provides a default encryption key. You can change it into a unique encryption key by following the below steps.

To enable keystore password encryption for the JasperReports Server and Connector Manager:

Copy the agiliance.keystore file from RiskVision server side to the following locations:

1. %JASPER_HOME%\Agiliance

2. %JASPER_HOME%\Agiliance\config

3. %ConnectorManager_Home%\ConnectorManager\config

Encryption

To encrypt using a keystore based password, you will have to set the `PBEPassword.disableKeyStoreBasedPwd=false` in the agiliance.properties file. **encrypt.cmd** is a command line utility for encrypting strings such as those in properties files.

To use a keystore based password:

Set the following property as false `PBEPassword.disableKeyStoreBasedPwd=false` in the agiliance.properties file in the following locations:

1. %AGILAINCE_HOME%\config if run from RiskVision side.

2. %JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF and copy this agiliance.properties file in %JASPER_HOME%\Agiliance\config.

3. %ConnectorManager_Home%\ConnectorManager\config, if run from connector side.

> [i] The PBEPassword.disableKeyStoreBasedPwd is only needed for encryption. However it's good practice to have all the properties files in synchronization for PBEPassword.disableKeyStoreBasedPwd, even if you don't encrypt from that location.

Decryption

The code automatically detects what type of password was used in encryption, either hardcoded or keystore based. You do not need to set `PBEPassword.disableKeyStoreBasedPwd` for decryption. Nonetheless, you should keep the property the same across all locations to avoid confusion and accidental errors, such as accidentally runing encrypt.cmd with the wrong setting.

Configure Email Accounts to Send Notifications

The default email configuration sends notifications to a local SMTP service for email distribution. With default email configuration, all notifications are sent out using one email address. You can add multiple email configurations to send out notifications from more than one email account. You might do this for users tasked with the administration of RiskVision objects, such as assessments, findings, incidents, and tickets so that stakeholders can directly reach out to those users. Once you configure multiple email configurations, the email addresses are available for selection in the **Sender Email Account** field of email templates to send out notifications using different email addresses. If no sender account is selected in the email template, the notifications are sent out using the default email configuration.

To set up the email configuration:

1. In the **RiskVision Administration** application, go to **Administration** > **Notifications**, and click the **Configuration** tab. The default notification sender account is displayed.
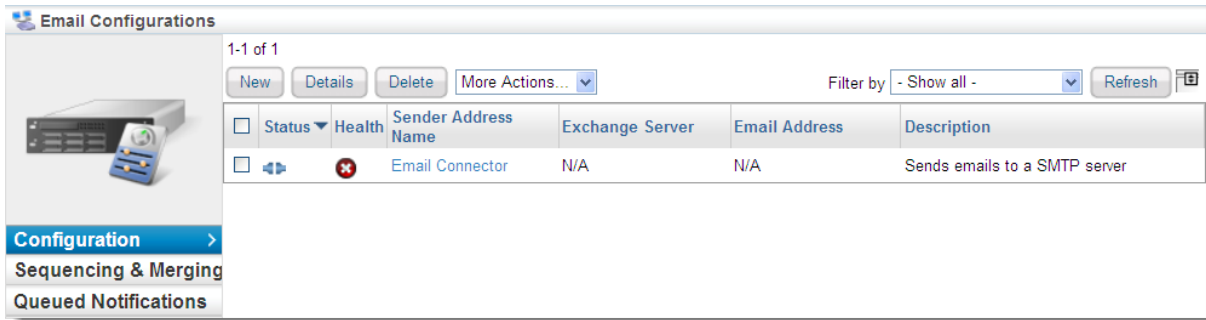
2. Select the default notification sender account to open the sender account or click **New** to add a sender account.

3. Enter the following fields to update the configuration:

   ○ **Sender Address Name.** Enter the sender's name using which you will want to send the email notifications.

- **Description**. Any additional information to help understand the use of exchange server.

- **Host Name**. Enter the fully qualified Domain Name of the SMTP host.

- **IP address**. Enter the IP address of the SMTP host

- **Secure transport**. Choose Yes or No.

- **Port**. Enter the SMTP listening port (default value is 25).

- **Login** (if required). Enter the username for SMTP service if the service requires authentication. By default, the email configuration uses the Login ID entered here to send out notifications.

- **Password** (if required). Enter the password if the SMTP service requires authentication.

- **Confirm password**. Enter the password again for confirmation.

- **Sender email** (optional). Enter an email address using which you will want to send the email notifications rather than using the Login ID.

- **Return email** (optional). Enter the email address where you want to receive email replies.

4. To test the configuration, enter a valid email Id in the Email address field, and click **Send test email**. If the configuration entered is correct, you will receive an email notification.

5. Click **OK** to save and exit the dialog.

Configure an External Authentication Server

In addition to using the built-in application authentication mechanism, you can configure a local LDAP directory service for authentication. When using LDAP, the Console prompts users to enter their credentials. Once the user is authenticated by LDAP (that is, the credentials are validated by the underlying LDAP directory service), RiskVision retrieves the corresponding user's attributes and permissions based on the mapping roles stored in the database. RiskVision can map the User ID, first name, last name, email, and LDAP group from the Identify Provider.

In multi-tenant deployments, only the SysAdmin user can configure the Authentication Server. The Administrator or the SysAdmin user can manage the Authentication Server in a single-tenant deployment.
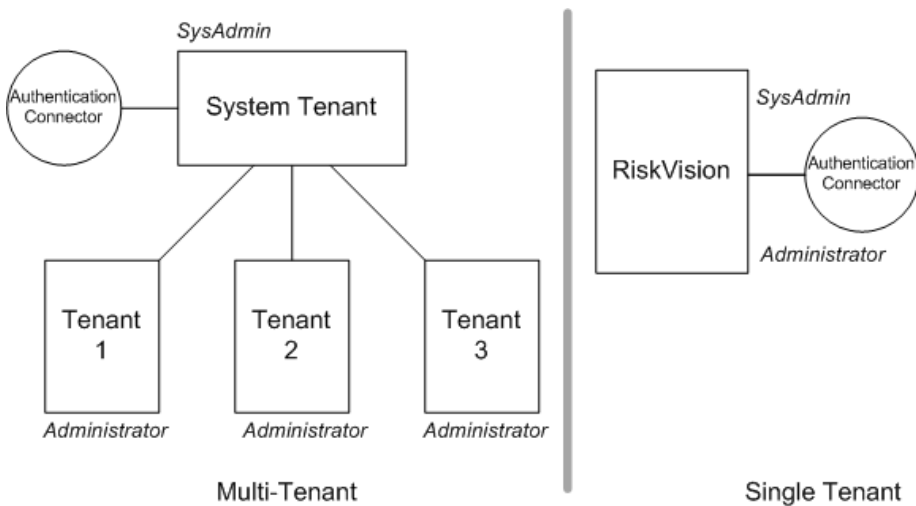
Providing LDAP authentication to RiskVision requires installing the following:

- A supported LDAP Directory service such as Active Directory (AD) or Sun Directory Server.

- Creating and configuring an LDAP Server.

- Optionally, if LDAP users will be imported into the RiskVision database, login names defined for LDAP users that you want to grant access to the RiskVision solution.

Support and Professional Services can assist you in exploring options and setting up LDAP authentication when installing the RiskVision Server at your site. You can configure the attributes for each LDAP Server to provide a separate user role. For more information, see "Configuring Attribute Mappings" and "Configuring External User Authorization" in *Administrators Guide*.

To set up the LDAP or Active Directory service connection

1. Log in as sysadmin or administrator. (Note: In multi-tenant deployments, only the 'sysadmin' user in the system tenant space can configure the authentication connector.)In the Administration application, go to Administration > External Authentication. The LDAP Servers page is displayed.

2. A default Authentication Connector is available for you to set up an LDAP service. You can also create a new LDAP service by clicking **New**. When you click new, the **LDAP Server Configuration** dialog is displayed.

3. Enter the following configuration information:

   - Name: Enter the LDAP name.

   - Description: Provide information explaining the purpose to set up an LDAP.

   - Protocol: Select the connection type (such as LDAP or Secure LDAP) if requested.

   - Host name: Enter the host name or the IP address.

   - IP address: Enter the IP address.

   - Port: Enter the connection port, the default is 389 (LDAP) or 636 (Secure LDAP).

   - Domain: Specify the domain name. Display domain name for users to select while logging in to RiskVision.

   - Base DN: Enter the base distinguished name such as `dc=,dc=com`.

   - Uid key: Enter the name of the field that specifies the unique user identifier, For example, uid for standard LDAPs or sAMAccountName for the AD.

   - Default domain(If you have multiple domains).

4. Enter the connection and search details.

   - Login: Optional, enter the account information that the application must use to authenticate users against the LDAP service. The account requires at least read access to the DN and search base.

   - Password: Optional, enter the account password.

   - Confirm password: Verifies if you have entered the correct password.

   - Search base: Use for large directories to prevent timeouts, this field is combined with the base DN; for example, enter OU=Security

   - Search filter: Limit the scope of the search to certain objects, for example, to search the only user in the AD, enter ObjectClass=User.

5. Click **OK**.

6. Enter the credentials for a user in the LDAP other than the LDAP account and click**Test**. The authentication success or failure message is displayed.

Use NTLM for Authentication

To use NTLM for user authentication, configure the LDAP Authentication Connector. Add the following properties to the `config\agiliance.properties` file on the RiskVision Server. Create the properties file if it does not exist.

Property	Description
authentication.processing.filter=ntlmAuthenticationProcessingFilter	The default value is AuthenticationProcessingFilter. The values are case-sensitive. This property is used to make sure that all requests are from authenticated sessions.
ntlm.default.domain=	Specify one property or the other. The system can find the controller for a given domain name.
authentication.allow.ntlm=true	Set this property to true to provide a Login with Windows credentials link to the RiskVision login page.

To use NTLM authentication, add the RiskVision Server to your browser(s) as a trusted NTLM server host. The procedure for each of the supported browsers is different.

Microsoft Internet Explorer

Go to **Tools** > **Internet Options**. Click the **Security** tab, then click **Local Intranet**, and then click the **Sites** button. Click **Advanced** in the Local Intranet dialog. Add the RiskVision Server URL (for example, `https://server.agiliance.com`) to the zone.

Mozilla Firefox

Enter "about:config" in the address bar. Find the configuration: network.automatic-ntlm-auth.trusted-uris. Edit the configuration to add RiskVision Server URL (for example, https://server.agiliance.com).

Set up Kerberos Authentication Without Encryption

The Kerberos v5 authentication protocol ensures that a service accessed over the network is secure and safe, and it provides exceptional performance over NT LAN Manager (NTLM). To use Kerberos authentication, set up a Lightweight Directory Access Protocol (LDAP) server and then see Configuring Kerberos Authentication.

Configure Kerberos Authentication

To enable Kerberos authentication in RiskVision, the Windows administrator and RiskVision administrator must perform the following:

- Generating the Service Principal Name (SPN) and Keytab file

- Configure the Tomcat for Kerberos Single Sign-On (SSO)

- Configure Browsers for Kerberos Authentication

Generate the Service Principal Name (SPN) and Keytab File

To set up the SPN and generate the keytab file, perform the following steps:

1. Log on to the active directory that uses the Kerberos Key Distribution Center (KDC).

2. For the user account in active directory, set the account to as "Password never expires" and "This account supports
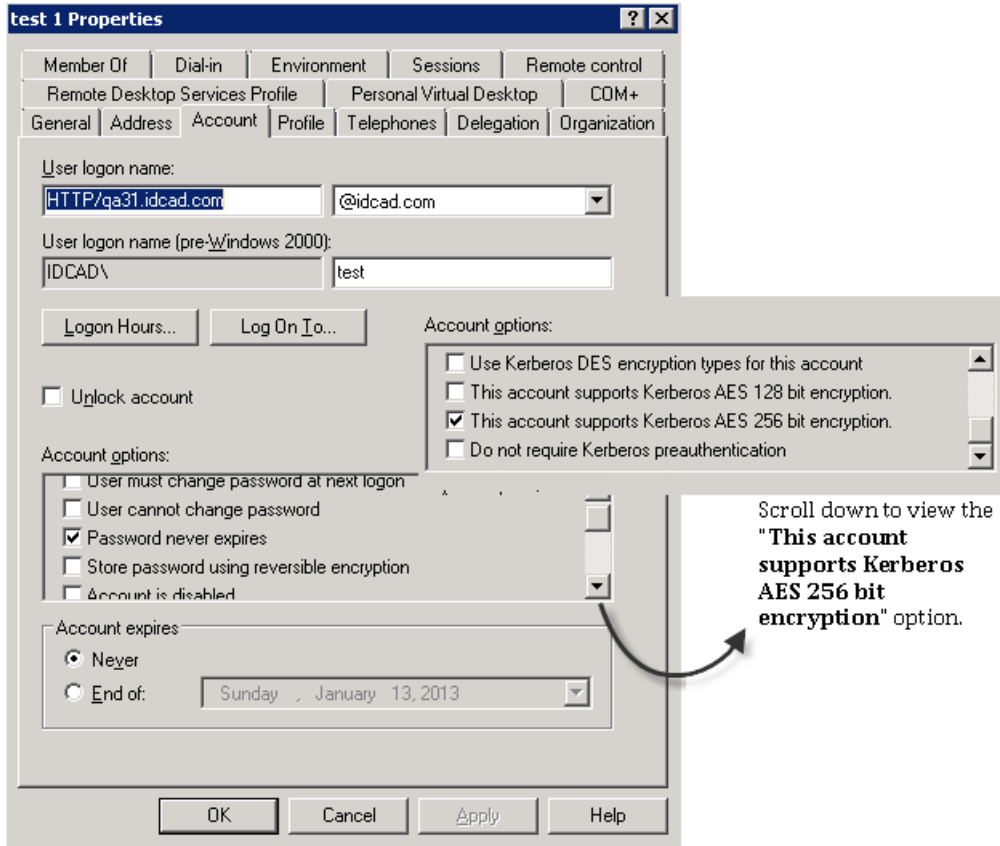
3. Open the Windows Command prompt and run the following command to generate a keytab for the user account.

```
ktpass -princ HTTP/[FQDN_LOWERCASE]@[DOMAIN_UPPERCASE] -mapuser [USERNAME] @ [DOMAIN_NAME] -pass
[PASSWORD] -ptype KRB5_NT_PRINCIPAL -kvno 0 -crypto AES256-SHA1 -out [OUTPUT-FILENAME].keytab
```

Note: Execute this command in the Active Directory server

Here FQDN is the RiskVision Web Server Hostname

4. After the keytab file is generated, open the Windows Command Prompt, and run the following command to verify whether the SPN is registered for the hostname that a user will need for logging into RiskVision.

```
setspn -l
```

133

```
Administrator: Command Prompt                                              _ □ ×

C:\Users\Administrator>setspn -l test
Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com:

C:\Users\Administrator>ktpass /out http-ro.keytab /mapuser test@idcad.com /pass
welcome@123 -ptype KRB5_NT_PRINCIPAL -kvno 0 /crypto AES256-SHA1 /princ HTTP/qa3
1.idcad.com@IDCAD.COM
Targeting domain controller: dev163.idcad.com
Using legacy password setting method
Successfully mapped HTTP/qa31.idcad.com to test.
Key created.
Output keytab to http-ro.keytab:
Keytab version: 0x502
keysize 80 HTTP/qa31.idcad.com@IDCAD.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype
 0x12 (AES256-SHA1) keylength 32 (0x40fe9350731009b1d714281be8f441cd3d08ab37f079
6a3064733cfec4321cdd)

C:\Users\Administrator>setspn -l test
Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com:
        HTTP/qa31.idcad.com

C:\Users\Administrator>_
```

5. Copy the keytab file to a directory in the RiskVision Application Server to enable the Kerberos Authentication.

Configure the Tomcat for Kerberos Single Sign-On

The following provides instructions for configuring the following files for the RiskVision Tomcat Application Server:

- applicationContext-kerberos.xml
- agiliance.default.application.properties

applicationContext-kerberos.xml

To configure the applicationContext-kerberos.xml file:

1. Go to %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF directory and open the applicationContext-kerberos.xml file using a text editor.

2. Uncomment all lines in-between start Kerberos configuration and end Kerberos configuration.

3. By default, Kerberos debugging is enabled. To disable debugging, set the following property to false:

   class="org.springframework.security.extensions.kerberos.GlobalSunJaasKerberosConfig">

agiliance.default. application.properties

To configure the agiliance.default.application.properties file:

1. Go to %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes directory and open the agilaince.default.application.properties file using a text editor.

2. Specify the Service Principal Name that was configured on the Active Directory for the RiskVision hostname. Only one SPN is allowed per domain and only one SPN is required for a hostname.

   `serviceprincipal=@`

3. Specify the location of .keytab file in RiskVision Server, which was generated in the active directory.

   `keytab.file=file:`

   Any changes to SPN or .keytab file requires restarting the RiskVision Tomcat service.

4. Specify the RiskVision Web Server hostname, provided during the .generation of .keytab file in the following property:

   `kerberos.host=`

   Note: Make sure that `RiskVisionWebServer_Hostname` is in lowercase

   Using the property above helps LDAP users to access the RiskVision application using Kerberos SSO.

5. Set the following property to true. Add the property if it does not exist.

   `authentication.allow.kerberos=true`

6. Specify the hostname of RiskVision Web Server, to allow vendors and internal users to access RiskVision application using credentials.

   `virtual.host=`

7. Use the following property to specify the number of attempts a user can make while logging into RiskVision. A user is disabled after all the attempts are exhausted.
   `password.disableAfterNFailedLogin=`
   By default, the value is '0', which signifies that the policy is not enforced.

8. Restart the RiskVision Tomcat to show the latest changes.

RiskVision strongly recommends copying the properties above to the `%AGILIANCE_HOME%\-config\agiliance.properties` file to ensure that Kerberos configuration is intact even after upgrading the RiskVisionServer.

Configure Browsers for Kerberos Authentication

By default, you will not be authenticated by Kerberos if you are using Mozilla® Firefox or Microsoft® Internet Explorer browser to access RiskVision Server. To allow a browser to support Kerberos AES 256 bit encryption, you must configure the settings specific to each browser type.

Mozilla Firefox

Perform the following steps to configure Mozilla Firefox browser, version 11.0:

1. Open the Firefox browser and enter "about:config" in the address bar. A warning message is displayed. Click **I'll be careful, I promise!** to accept the warning and continue.

2. Enter the string "negotiate" in the Search bar to search properties containing the string "negotiate." Double-click or right-click these properties, then click **Toggle** to set them to false.
   - `network.negotiate-auth.delegation-uris`
   - `network.negotiate-auth.trusted-uris`

3. Double-click each of the following properties to specify the URL of RiskVision Server.

   - `network.negotiate-auth.delegation-` `uris`

   - `network.negotiate-auth.trusted-` `uris`

4. Enter the string "ntlm" in the Search bar to search properties containing the string "ntlm". Double-click the `network.automatic-ntlm-auth.allow-proxies` property to set the value to "false."

5. Restart the browser to apply the configuration changes.

6. **Microsoft Internet Explorer**

   Perform the following steps to configure Internet Explorer browser versions 6.x, 7.x, 8.x, and 9.x. This configuration works perfectly well when the Internet Client accesses the RiskVision from a different machine other than RiskVision Server.

   1. Open the Internet Explorer browser and click **Tools** > **Internet Options**.

      1. Click the **Advanced** tab, under Security options, check the box next to "Enable Windows Integrated Authentication."

      2. Click the **Security** tab, select the **Intranet sites** icon, click **Sites** and then click **Advanced**. Enter the RiskVision URL in the Add this website to the zone field and click **Add** to apply security settings to the RiskVision URL, click **Close** and then click **OK**.

   2. Click **Apply** and then click **OK** to save the settings.

   3. Restart the browser to apply the configuration changes.

Enable Kerberos Debugging

Enable the Kerberos debugging by setting the following property to true:

```
class="org.springframework.security.extensions.kerberos.GlobalSunJaasKerberosConfig">
```

Troubleshoot Kerberos

The following will help you troubleshoot common issues with Kerberos authentication.

Common issues with Kerberos authentication:

1. Clock skew too great while getting initial credentials error.

   Solution: The Active directory and the RiskVision Server must not be more than 5 minutes apart. The clocks on both servers have to be in sync.

2. Defective token detected (Mechanism level: GSSHeader did not find the right tag)

   Solution: This can happen if the browser cannot negotiate the request with the Kerberos Distribution Center or the Active Directory.

   For Mozilla Firefox:

   Setup the following environment variables:

   - NSPR_LOG_FILE = c:/moz.log
   - NSPR_LOG_MODULES = negotiateauth:5

   Verify the Firefox configurations. Restart Firefox and check logs under C:/moz.log. If Firebug is enabled, check the header details. If the response is ":401 UnAuthorized," most likely, the issue is with the keytab files.

3. Cannot load keytab files on RiskVision Server startup

   Solution: The keytab files are loaded during startup. If the version number (kvno) is incorrect, the keytab will not be loaded. The best approach to generate the keytab files on the Active Directory is by using the ktpass command. The ktab command is known to cause issues due to the kvno number.

4. Server not found in Kerberos database

   Solution: This happens if the same SPN is mapped to multiple accounts or hostnames on the Active Directory. Unregister the SPN for other accounts on the Active Directory server by running the following command:

   setspn -D service/name hostname

5. Error 400 Bad Request

   Solution: If user has many groups in Active Directory then request size might be more for Kerberos Authentication which can lead to 400 Bad Request. In order to resolve this issue please perform below changes:

   1. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra`
   2. Open `httpd-ssl.conf` using text editor and add below directive under

   LimitRequestFieldSize 16380The default value for LimitRequestFieldSize is 8190, as per our requirement the size can be increase.

6. Error 413 - Request Entity Too Large

   Solution: When users encounters the error 413, then we need to perform below changes in Apache Web Server.

   1. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra`
   2. Open httpd-ssl.conf using text editor and add below directive under `LimitRequestBody 0`
   3. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra,` in the `workers.properties` file add: `worker.agl_tomcat.max_packet_size=65536`
   4. Restart Apache Service
   5. Go to < `%AGILIANCE_HOME%>\Tomcat\conf` , in `server.xml` file add the packetsize `packetSize="65536"`
      Example:

      ```
      enableLookups="false"
      protocol="AJP/1.3"
      packetSize="65536"
      connectionTimeout="900000"
      backlog="200"
      ```

```
maxThreads="300"
debug="0"
URIEncoding="UTF-8"/>
```

6. `Restart Tomcat Service`

`If error still exists then we need to increase packet size.`

Set Up Kerberos Version 5 to Use AES 256 Bit Encryption

From version 6.5 SP1 HF1 onwards, you can set up the Kerberos version 5 to use Advanced Encryption Standard (AES) 256 bit encryption in order to enhance the Kerberos v5 authentication usability.

You must set up the Kerberos AES 256 bit encryption only if the target systems use the following operating systems:

Supported Operating System	RiskVision Client	RiskVision Server	Kerberos Key Distribution Center (KDC)
Windows 7	✅		
Windows 2008 or later		✅	
Windows 2008 R2 Server or later			✅

To enable Kerberos AES 256 bit encryption in RiskVision, the Windows administrator and RiskVision administrator must perform the following tasks:

1. Generate the Service Principal Name (SPN) and Keytab file

2. Configure the RiskVision Server to use Kerberos AES 256 bit encryption

3. Configure the browsers for Kerberos authentication

Generate the Service Principal Name (SPN) and Keytab File

To set up the SPN and generate the keytab file, perform the following steps:

1. Log into the active directory that uses the Kerberos Key Distribution Center (KDC).

2. Find the user account and check the **Password never expires** and **This account supports** checkboxes.
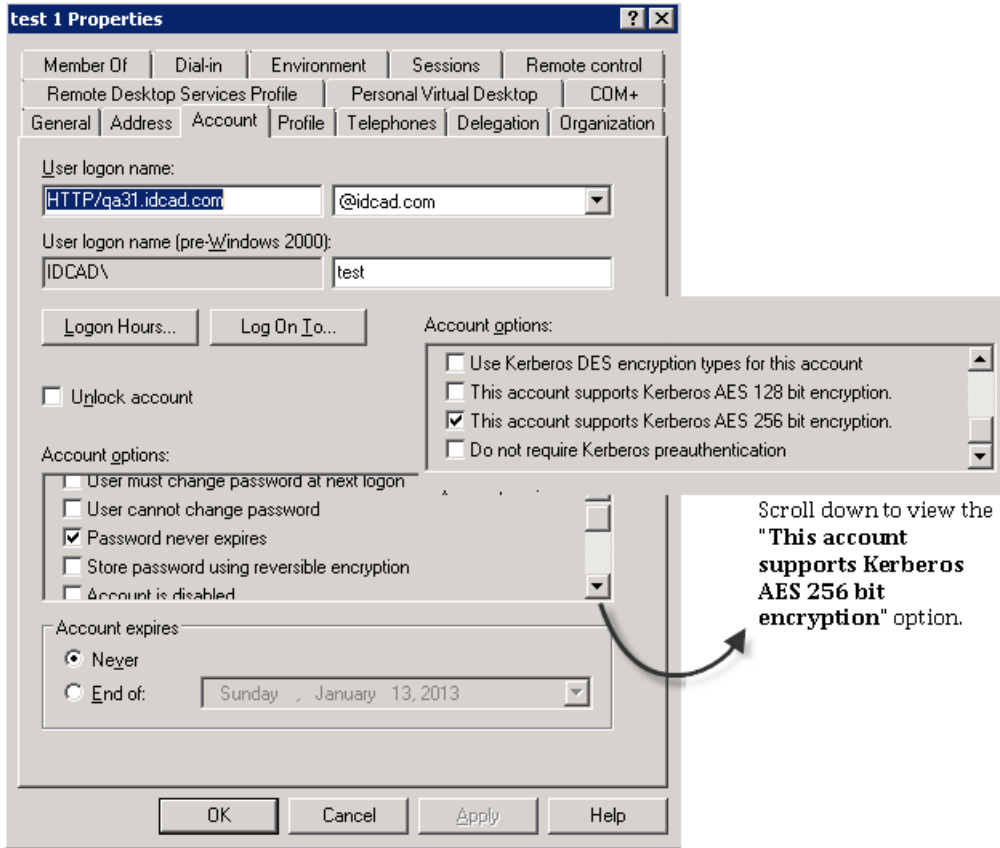
3. Open Windows Command prompt and run the following command to generate a keytab for the user account.

```
ktpass -princ HTTP/[FQDN_LOWERCASE]@[DOMAIN_UPPERCASE] -mapuser [USERNAME] @ [DOMAIN_NAME] -pass
[PASSWORD] -ptype KRB5_NT_PRINCIPAL -kvno 0 -crypto AES256-SHA1 -out [OUTPUT-FILENAME].keytab
```

Note: Execute this command in the Active Directory server

FQDN is the RiskVision Web Server Hostname

4. After the keytab file is generated, open Windows Command Prompt, and run the following command to verify whether the SPN is registered for the hostname that a user will need for logging into RiskVision.

```
setspn -l
```

141

```
Administrator: Command Prompt                                    _ □ ×
C:\Users\Administrator>setspn -l test
Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com:

C:\Users\Administrator>ktpass /out http-ro.keytab /mapuser test@idcad.com /pass
welcome@123 -ptype KRB5_NT_PRINCIPAL -kvno 0 /crypto AES256-SHA1 /princ HTTP/qa3
1.idcad.com@IDCAD.COM
Targeting domain controller: dev163.idcad.com
Using legacy password setting method
Successfully mapped HTTP/qa31.idcad.com to test.
Key created.
Output keytab to http-ro.keytab:
Keytab version: 0x502
keysize 80 HTTP/qa31.idcad.com@IDCAD.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype
 0x12 (AES256-SHA1) keylength 32 (0x40fe9350731009b1d714281be8f441cd3d08ab37f079
6a3064733cfec4321cdd)

C:\Users\Administrator>setspn -l test
Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com:
        HTTP/qa31.idcad.com

C:\Users\Administrator>_
```

5. Copy the keytab file to a directory in the RiskVision Application Server to enable the Kerberos Authentication.

Configure RiskVision Server to Use Kerberos AES 256 Bit Encryption

Configure the following files specific to the RiskVision Tomcat Application Server:

- applicationContext-kerberos.xml
- agiliance.default.application.properties

applicationContext-kerberos.xml

Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF` directory and open the `applicationContext-` `kerberos` `.` `xml` file by using a text editor and perform the following changes:

1. Uncomment all the lines in-between start Kerberos configuration and end Kerberos configuration.
2. By default, the Kerberos debugging is enabled. To disable the debugging, set the following property to false:

```
class="org.springframework.security.extensions.kerberos.GlobalSunJaasKerberosConfig">
```

agiliance.default. application.properties

Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory, open the **agilaince.default.application.properties** file by using a text editor and then perform the following changes:

`kerberos.host=`

Make sure that `RiskVisionWebServer_Hostname` is in lowercase.

Using the property above helps LDAP users to access the RiskVision application using Kerberos SSO.

`password.disableAfterNFailedLogin=`

By default, the value is '0', which signifies that the policy is not enforced.

1. **serviceprincipal**

   Specify the Service Principal Name that was configured on the Active Directory for the RiskVision hostname. Only one SPN is allowed per domain and only one SPN is required for a hostname.

   `serviceprincipal=@`

2. **keytab.file**

   Specify the location of .keytab file in RiskVision Server which was generated in the active directory.

   `keytab.file=file:`

   Any changes to SPN or .keytab file requires restarting the RiskVision Tomcat service.

3. Specify the RiskVision Web Server hostname, provided during the .generation of .keytab file in the following property:

4. Set the following property to true. Add the property if it does not exist.

   `authentication.allow.kerberos=true`

5. Specify another hostname of RiskVision Web Server, to allow vendors and internal users to access RiskVision application using credentials.

   `virtual.host=`

6. Use the following property to specify the number of attempts a user can make while logging into RiskVision. A user is disabled after all the attempts are exhausted.

After you finish configuring the settings, restart the RiskVision Tomcat to show the latest changes.

RiskVision strongly recommends copying the properties above to the

`%AGILIANCE_HOME%\config\agiliance.properties` file to ensure that Kerberos configuration is intact even after upgrading the RiskVision Server.

Configure Browsers for Kerberos Authentication

By default, you will not be authenticated by Kerberos if you are using Mozilla® Firefox or Microsoft® Internet Explorer browser to access RiskVision Server. To allow a browser to support Kerberos AES 256 bit encryption, you must configure the settings specific to each browser type.

Mozilla Firefox

To configure Mozilla Firefox version 11.0:

1. Open the Firefox browser and enter "about:config" in the address bar. A warning message is displayed. Click **I'll be careful, I promise!** to accept the warning and continue.

2. Enter the string "negotiate" in the Search bar to search properties containing the string "negotiate." The browser displays the following properties:
   - `network.negotiate-auth.delegation-uris`
   - `network.negotiate-auth.trusted-uris`
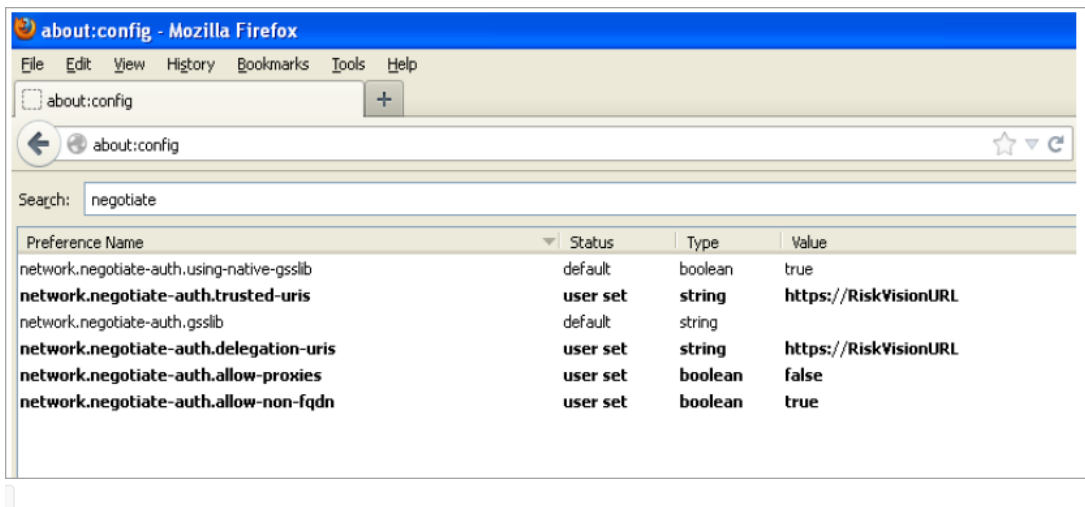
3. Double-click or right-click each property, then click Modify. Specify the RiskVision URL.

Microsoft Internet Explorer

See Microsoft Internet Explorer for instructions. For information on debugging and troubleshooting Kerberos AES 256 bit encryption, see Debugging and Troubleshooting.

Access RiskVision Server Using Kerberos Authentication

When Kerberos authentication is in-place, you can open a Firefox or Internet Explorer browser and enter the log in URL to gain implicit access to RiskVision application. After you log-out from the RiskVision application, credentials that relate to a different domain can be used explicitly to access RiskVision as a internal or external user. You can bookmark the login URL to use the **Login using your Windows account** link for future logins or any RiskVision page to go directly to a page to resume your work.

The **Login using your Windows account** link works only from the fully qualified domain name URL of RiskVision.

Retrieve Zombie Attachments

Files uploaded to RiskVision as evidence, documents stored in the Document Repository, or attachments on RiskVision objects like entities and tickets, will appear in 3 places:

- **User Interface:** You will see the document and its link within the UI where the file was uploaded.

- **RiskVision Database:** The file will have a record in the database that contains metadata such as the name and upload date. The file will also point to where it is stored on the RiskVision file system.

- **RiskVision's File System:** After being uploaded to RiskVision, the file is stored in the RiskVision server's data folder.

Files uploaded to RiskVision should always exist in each of the above 3 places. However, there are situations in which a file may be deleted through the UI and as a result be deleted from the database, but not from the file system. This would result in unneeded files residing in the file system. These files, referred to here as zombie attachments, can cause undue strain on the system by taking up memory and storage. In order to better maintain the system, RiskVision provides a way to identify and access the zombie attachments in the file system so they can be deleted.

Zombie database records may also exist. Zombie database records represent records in the database that don't have related files in the file system. There should not be any such records, and the zombie database report will provide proof that there are none. If such records exist, please contact Resolver Support.

The below steps will extract the zombie attachments as two separate .CSV reports: one for database zombies, and another for file system zombies. The database report contains the following columns:

- **Attachment ID:** The ID number of the attachment.

- **Path ID:** The ID of the file path for an object in the file system.

- **Owning Object ID:** The ID number of the object that the attachment is attached to.

- **File Name:** The file name of the attachment.

- **File Version:** The version number of the attachment.

- **Who Uploaded:** The RiskVision user name of the user who uploaded the attachment.

- **Content Type:** The type of file the attachment is.

The file system report contains the following columns:

- **Path ID:** The ID of the file path for an object in the file system.

- **Hash Filename:** The name of the attachment in the file system.

- **RiskVision Object Type:** The object type of the zombie attachment.

- **File Size (Kb):** The attachment's file size in kilobytes.

- **Last Modified:** The date and time that the attachment was last modified.

- **File Path:** The location of the attachment in the file system.

> The **RISKVISION_HOME\config\agiliance.properties** file contains a `com.agiliance.attachments.extractor.tool.encryptionCheck.excludedContentTypes` property to exclude certain file types from being extracted by the below steps. This property stores file types to be excluded as a comma-separated list and it excludes network paths and web links by default. Ensure that you check this property so the tool only extracts what you want it to.

To access zombie attachments:

1. Open the command prompt in administrator mode and navigate to the **RISKVISION_HOME\install\toolbox\bin**.

2. Run the `attachmentExtractionTool.cmd` command.

3. **Optional:** The following options can be used in the command line to modify how the zombie attachments are extracted:

   - **{f,-force-pre-process}:** Reloads the file system after changes have been made.

   - **{v,-verbose}:** Produces additional information on the files in the file path, including whether or not they are zombie attachments.

   - **{w,-show-object-types}:** Shows all the available RiskVision object types.

- {t,-object-types}: Extracts zombie attachments of the specified object type(s). The user must enter a comma separated list of RiskVision object types, a total list of which can be viewed by using the above **-w** command. For example, `attachmentExtractionTool.cmd -t ComputerSystem,OperatingSystem,Asset`. Entering no values will only extract entities of the **Application** object type. Entering `attachmentExtractionTool.cmd -t All` will extract all zombie attachments from the database and file system, regardless of object type. This command is useful for focusing on specific object types in a smaller report after running a full report of all zombie records.

- {y,-copy-zombie-attachments}: Copies the zombie attachments from the file system to the **RISKVISION_HOME\install\toolbox\bin\ZOMBIE_ATTACHMENTS\Copied_ZOMBIE_ATTACHMENTS** folder. If the user uses this command, the attachments will only be copied and will still remain in the file system. This command will not affect any attachments in the database.

- {o,-output-dir}: Creates a folder to store the extracted attachments. By default, the attachments will be saved to the **ZOMBIE_ATTACHMENTS** folder under the current directory.

- {h,-help}: Lists all the optional commands available in the `attachmentExtractionTool.cmd` command.

4. The file system and database zombie attachments will be extracted as two separate .CSV files under the **RISKVISION_HOME\install\toolbox\bin\ZOMBIE_ATTACHMENTS** folder.

List of Object Types

The following list shows all of the object types available to be used in RiskVision:

- Account
- Application
- Asset
- AuditProject – (note: this is a program)
- ComputerSystem
- Data
- Device
- Domain
- EntityCollection
- ExceptionRequest
- Financial
- Finding – (note: this is a data feed)
- Gap – (note: this is a finding)
- GapArchive – (note: this is an archived finding)
- GapObject – (note: this is an instance of a finding)
- GapObjectArchive – (note: this is an archived finding instance)
- Group
- Incident
- Intangible
- Location
- Network
- OrganizationalUnit
- Person
- Physical
- Questionnaire
- RAMatrix – (note: this is a risk definition)
- RAMitigation – (note: this is a response object)
- RAMitigationArchive – (note: this is an archived response)
- RAMitigationItem – (note: this is an instance of a response)
- RAProject – (note: this is an assessment object)
- RAUserInput – (note: this is an instance of a risk object or, in other words, a risk definition assigned to an assessment)
- RAUserInputArchive – (note: this is a risk instance archive)
- Ticket
- TicketArchive – (note: this is an archived ticket)
- TicketObjectArchive – (note: this is an archived instance of a ticket)
- Vendor

Customization and Advanced Configuration

There are a number of other configuration options and customizations that the RiskVision support and professional services personnel can assist you in setting up the RiskVision. The following list provides a summary of some of the more important RiskVision Server customizations that customers can tailor based on their own requirements:

- RiskVision Server configuration and optimization; certificates and Apache SSL/https setup

- Default virtual group setup

- Custom entity definition

- Some GUI customization

- Mapping the RiskVision server data folder to an external drive

- Run system jobs on a separate machine

The RiskVision Server uses a number of different server property and XML configuration files to set parameters and customize operations of the RiskVision Server and RiskVision solution. On the computer where the RiskVision Server is installed, there are two important directory locations where these files are stored:

`%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes`

This directory contains files that provide all default property and configuration settings.

`%AGILIANCE_HOME%\config`

This directory is used to optionally store files that overwrite default configuration settings.

`%AGILIANCE_HOME%` is the root location where the RiskVision Server is installed.

The properties file in the `%AGILIANCE_HOME%\config` directory overwrites values from the corresponding files in the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory. You only need to specify those properties where you want to overwrite default property settings. That way, you can easily change a few properties without having to specify the entire collection of properties in the overriding file. In these cases, you will create a properties file with only the changed properties and leave out the rest to default to their default values. Thus, the resulting effective properties used by are a combination of the two files.

Other key points about configuration:

1. The file names of the properties files in the two directories are different. For example, agiliance.properties in the `%AGILIANCE_HOME%\config` directory overrides agiliance.default property settings in the agiliance. default.application.properties and agiliance.default.system.properties files.

2. For XML configuration files, the file names in the two directories are similar. If a file with the similar name exists in `%AGILIANCE_HOME%\config`, it will be used to replace the corresponding default configuration file. So, it's important that the replacement configuration file contain all the settings of the original default file. You may want to backup the original default XML file and make changes to the copied file to override the settings in the default XML configuration files.

3. There are three XML configuration files--TextAttributes.xml, UICustomization.xml and SchedulerConfiguration.xml — that are exceptions to the processing rule described in item 2 above. For these three files, the entire contents of a new file do not replace the entire contents of the default configuration file, so you can simply include the elements that you want to override in a new XML configuration file. The only requirement is that you need to use complete XML path.

The following table lists the property and XML configuration files most commonly customized for specific RiskVision Server installations:

Filename	Description
agiliance.default.system.properties	RiskVision Server default configuration settings
agiliance.default.application.properties	RiskVision solution default configuration settings
chart.colors.defaults.properties	UI chart color customization
version.properties	Resolver version information
SchedulerConfiguration.xml	Configuration for jobs that must run on a regular schedule
Security.xml	ACL (access control list) customization (users, roles, permissions, etc.)
TargetSelectionObjects.xml	Customize the objects and fields that can be used to build the target selection criteria
TextAttributes.xml	Associates text tooltips with object attributes
UICustomization.xml	Field and detail tab display attributes and positioning

	Use the **Configure UI** facility to customize elements of the Console user interface.

Change the Date and Time Format

RiskVision allows you to change the date and time format, which appears on the detail pages of RiskVision objects. By default, RiskVision displays the date and time in the `YYYY-MM-DD format`. To change the date and time format to `MM:DD:YYYY`, add all the following properties in the `agiliance.properties file:`

- `ui.clientDateTimeFormat=MM-dd-yyyy HH:mm:ss`

- `ui.clientDateOnlyFormat=MM-dd-yyyy`

- `ui.clientTimeOnlyFormat=HH:mm`

These changes will be applied across the RiskVision application, but you cannot change the date and time format individually for each RiskVision object.

Set Time-Out Values for Report Execution

A time-out value is the maximum number of seconds that a report can continue to execute before it is stopped. A time-out value avoids long running queries that return large amounts of data and makes users wait until the grid is completely loaded. You can set time-out values for RiskVision reports and Jaspersoft reports.

RiskVision Report Execution Time-Out

In the RiskVision Server, by default, the time-out values are set to 3600000 Milliseconds in the following properties, available in the `agiliance.default.application.properties` file.

`com.agiliance.common.DatabaseConnectionManager.database.socket.timeout`

`com.agiliance.common.DatabaseConnectionManager.database.connection.timeout`

You can override the time-out values by adding the properties mentioned above to the `agiliance.properties` file.

Jaspersoft Report Execution Time-Out

In the JasperReports Server, by default, the Ad Hoc Query Timeout (seconds) field is set to 360 seconds. If you have to change the time-out value, please follow these steps:

1. Log into the JasperReports Server as system administrator.

2. On the **Manage** menu, click **Server Settings**.

3. Click **Ad Hoc Settings**, set the **Ad Hoc Query Timeout** (seconds) field, and click **Change**.

To set the time-out value in the .jrxml file definition, open the .jrxml file using a text editor, and add the following properties:

`net.sf.jasperreports.governor.timeout.enabled=true`

`net.sf.jasperreports.governor.timeout=`

Map the Data Folder to an External Drive

When you back up the RiskVision Server, the folders, such as reports, dashboards, and attachments, are copied to the directory `%AGILIANCE_HOME%\backup` where the server is installed. From version 6.5 SP1, you can map a universal naming convention path of an external drive to a folder present in the `%AGILIANCE_HOME%\data` directory.

This means you can configure the server to save folders directly in a separate system when evidence is added or when a chart or dashboard is archived. For example, you can configure the dashboards folder to an external drive, such as `\\RiskVision_server\\Data` to save all archived dashboards.

Prerequisites for Configuring the Data Folder

Obtain the name of the computer and the folder path(s) to which you want to map the dashboards, reports and attachments folders. Make sure that the RiskVision Server host has sufficient privileges to move the data folder contents to the external drive and to read the folder contents during the backup.

To configure the data folder:

1. Go to the directory `%AGILIANCE_HOME%\config` and open the `agiliance.properties` file using a text editor.

2. Add the following properties, then set each property to a new location other than the directory `%AGILIANCE_HOME%\backup` .

   ```
   save.folder.reports= <\\\\StorageServer\\RiskVision_server\\Data\\attachments>
    save.folder.dashboards=<\\\\StorageServer\\RiskVision_server\\Data\\attachments>
   save.folder.attachments=<\\\\StorageServer\\RiskVision_server\\Data\\attachments>
   ```

3. Where the computer `\\StorageServer` name and the name `RiskVision_server\\Data` of share to which reports, dashboards, and attachments folders are saved. Note that you can map each folder to a different external drive.

4. Restart the RiskVision Tomcat service to apply the latest changes.

The contents in reports, dashboards, and attachments folders will remain in the directory `%AGILIANCE_HOME%\data` , but those folders that are mapped to an external drive will start storing the data the moment you configure it. Once the Daily Server and Database Hot Backup job are run, the contents in the external mapped drive in the directory `%AGILIANCE_HOME%\` are backed up.

You must manually move the content within the previously archived folders to the newly-mapped drives so that your users can continue to access the content without any trouble.

Define a New Location for the Images Folder

Whenever a custom image is embedded in an object, such as a dashboard or policy, you may risk losing the custom images stored in the directory `%AGILIANCE_HOME%\Tomcat\webapps\spc\images` after upgrading RiskVision. To avoid this issue, we recommended changing the images folder location from `%AGILIANCE_HOME%\Tomcat\webapps\spc\images` to `%AGILIANCE_HOME%\config\images`.

To change the images folder location:

1. Go to the directory `%AGILIANCE_HOME%\config` and open the `agiliance.properties` file using a text editor.

2. Add the following property:
   `image.custom.folder=<%AGILIANCE_HOME%>\`

3. Specify a folder name to which you want to copy the images.

4. Restart the RiskVision Tomcat service.

Use the Location of the Images Folder

> ⚠️ Do not use this feature if your reports or dashboards need to be archived. Dashboards and reprots that are archived to PDF will not render images from the `<%AGILIANCE_HOME%\config\` directory. Use JasperReports Server instead.

You can copy custom images to the `%AGILIANCE_HOME%\config\images` directory to use this feature in the following scenarios:

1. A report author can use the `$DT.getCustomImageFromConfig` Dashboard Toolbox API call in the HTML layout template of a dashboard to render the image.

   For example, you can use the following code in the report's HTML layout template to render the image.

   `$DT.getCustomImageFromConfig("Logo.png", null, null, "From the config folder")`

2. An image embedded in any RiskVision object can be viewed by means of the following URL:

   `https:///spc/appbuilder/CustomImage.jsp?id=`

   Where is the fully qualified domain hostname, is the IP address of RiskVision Server, and is the file name of the image.

Run System Jobs on a Separate Machine

RiskVision uses system jobs to perform a variety of functions, including updating vulnerabilities, summarizing report data, and updating dynamic groups in program assessments. These jobs are scheduled to run automatically in the background on the server, or can be run manually. When dealing with large amounts of data, a particular job may cause services, such as Tomcat, to consume more memory and CPU. To avoid performance issues, you can run system jobs separately on a machine other than your RiskVision server using the RiskVision Job Manager.

When a scheduled job is triggered on the RiskVision server, the scheduler will verify which server the job should run on. When a job is scheduled to run on a separate machine, the RiskVision Server initiates a request to RiskVision Job Manager to run that particular job. The RiskVision Job Manager will process the request by triggering the job to execute on its scheduler. After the completion of job execution, data is saved back to the RiskVision Server.
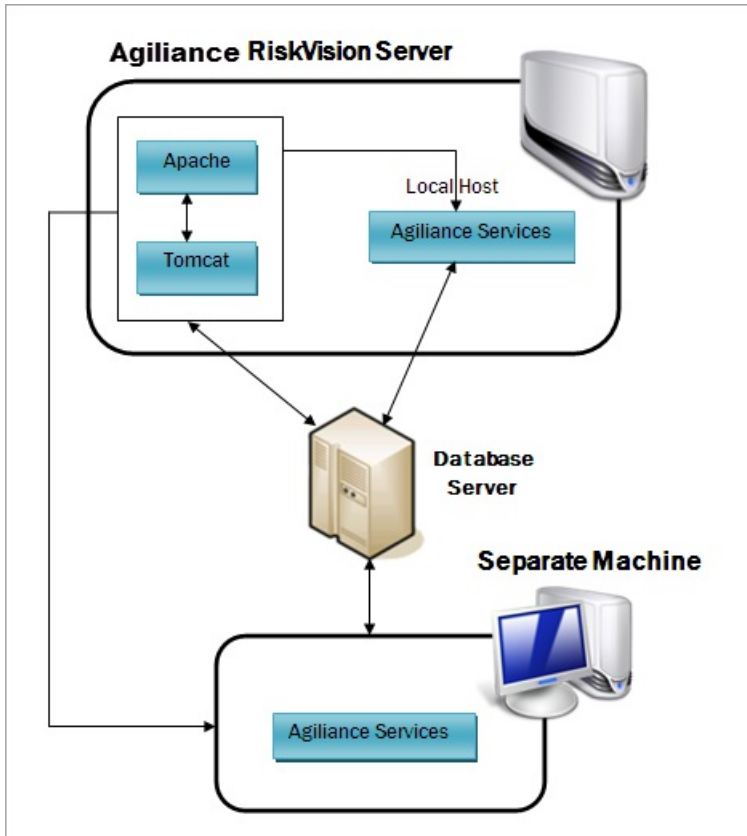
Running system jobs on a separate machine.

Configure RiskVision Server to Use a Separate Machine for Running System Jobs

To allow a machine to run system jobs:

1. Open your RiskVision server.

2. Run the following MySQL command from command prompt or MySQL shell. The username is agiliance and root and the default password is agiliance. Ignore this step if you're using an Oracle database.

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

2. Go to the following directory: `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` and open the SchedulerConfiguration.xml file. You must specify the IP address in the attribute to point the machine to where the system job can be run.

```
Builds report summary. daily
10.100.16.5
9080
1,0
false
false
```

3. Copy the `SchedulerConfiguration.xml` to the folder `%AGILIANCE_HOME%/config` .

Database Administration

Customization and Advanced Configuration describes RiskVision Server property and XML configuration files used to set parameters and customize operations of the RiskVision Server and Console. Specific system configuration required to perform tasks such as setting up and executing scheduled jobs for server and database backup can now be performed within the application.

Back Up Properties

When you back up RiskVision, a copy will be generated of:

- The contents of the RiskVision Server database;
- The contents of the configuration folder (%AGILIANCE_HOME%\config);
- The contents of the attachments folder;
- The contents of JasperReports Server database; and
- The contents of JasperReports Server repository.

Enable Backups

By default, the automatic daily backup job is enabled. To disable it, add the following line to the `%AGILIANCE_HOME%\config\agiliance.properties` file:

```
com.agiliance.admin.scheduler.BackupJob.Disable=true
```

By default, the automatic weekly backup job is also enabled. To disable it, add the following line to the `%AGILIANCE_HOME%\config\agiliance.properties` file:

```
com.agiliance.admin.scheduler.AttachmentBackupJob.Disabled=true
```

Backup Time

The default time set in the file `SchedulerConfiguration.xml` for the daily backup is 8 p.m. For the weekly back up, the default time set is 10 p.m. on Sunday. After setup, you can change the schedule on the **Administration** > **Scheduled Jobs** page.

Back Up the Destination Directory

The default destination directory for backups is `AGILIANCE%_HOME%\backup` .

To change the backup directory:

1. Add the following line to `%AGILIANCE_HOME%\config\agiliance.properties` file:

   `com.agiliance.admin.backup.BackupManager.BackupDestinationDirectory=`
   `FullPathnameToAnExistingDirectoryWithSufficientFreeSpace`

   The backup destination directory can be a mounted remote file system. If specified using the universal naming convention for Windows, each backslash (\) character in the path must be "escaped" by another backslash. That is, use two backslashes for each backslash in the path, such as:

   `\\\\fileserver1\\\\backup.`

2. For the MySQL incremental backup, change the directory path name in the following line of the `%AGILIANCE_HOME%\config\my.ini` file:

   `log-bin="%AGILIANCE_HOME%\MySQL\backup\"`

   You do not have to change the name "agiliance" in the line above.

Number of Saved Backups

By default, the maximum number of previous backups to keep in the directory `%AGILIANCE_HOME%\backup` is 7. Along with 7 previous backup files, you will also find the most recent back up in the file folder format. When the Daily Server and Database Hot Backup job is run, the preceding backup folder is compressed upon the new back up. To change the maximum number of backups to retain in the destination directory, add the following property to the `%AGILIANCE_HOME%\config\agiliance.properties` file:

`com.agiliance.admin.backup.BackupManager.MaxRetainedBackups=MaxNumberOfRetainedBackups`

Configure MySQL Backup Properties

Add the following line in the `%AGILIANCE_HOME%\config\agiliance.properties` file to override the parameters for `mysqldump` utility.

```
com.agiliance.admin.backup.BackupManager.mysqldump.options=--single-transaction --add-drop-database --quick --compress --extended-insert --max-allowed-packet=32MB
```

(Enter the property name and value all on one line.)

Ignoring Database Tables During Backups

To specify the exclusion of certain tables from the normal backup process, include the following line in the agiliance.properties file:

```
com.agiliance.admin.backup.BackupManager.IgnoredTableNames=tableList
```

where is a comma-separated list of table names. By default, only the agl_auditlog table is specified in the `RiskVision.default.system.properties` file.

A MySQL dump file will be created for each ignored table when the database back up job runs for the first time. On subsequent back ups, new dump files will only be created for new tables specified in *tableList*, if you made changes to the list. These dump files must be imported into the database if the database is restored using a back up that does not contain these tables and their indexes.

Enable JasperReports Server Repository Backups

To enable scheduled backups of Jasper Repository and the PostgreSQL database:

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.

Back up the Destination Directory Files

Backup files are now named -YYYYMMDDhhmmss.zip, where the trailing characters in the filename are a timestamp of the backup date and time. This file normally contains the following backup and zip files:

- The RiskVision Server back up the file: server-YYYYMMDDhhmmss.zip.

- The MySQL dump file: mysqldump-YYYYMMDDhhmmss.sql.

- One or more MySQL binary log files (i.e., incremental backup files) generated between the MySQL dump file in the backup file and the one in the next backup file. These files are named -nnnnnn.

- The JasperReports Server database backup file: jasperdump-YYYYMMDDhhmmss.zip.

- The JasperReports Server repository dump file: jasperrepositorydump-YYYYMMDDhhmmss.zip.

- The index file for MySQL binary log files at the time of the backup.
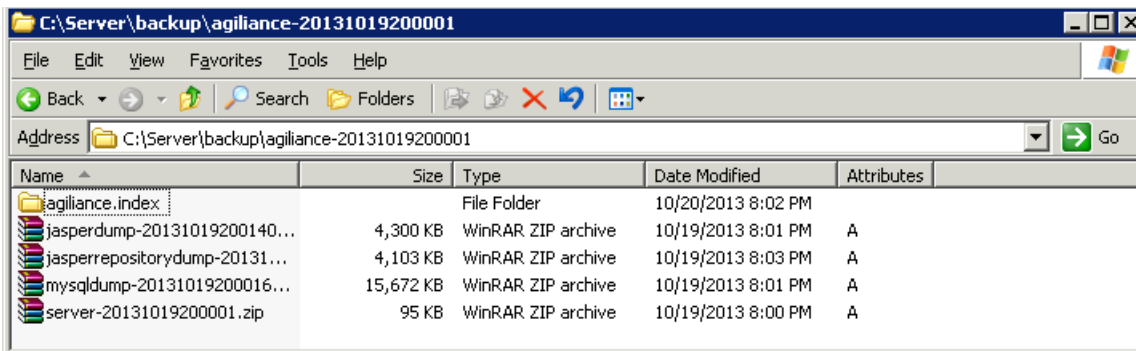
An example of RiskVision backup files.

Do not rename the files in the destination directory. Also, note that the timestamp of the MySQL dump file is later than that of the server back up file. Database back up files are password-protected (using the database root password at the time of the back up). They are not meant for end-user viewing or modification.

Encrypt Communication with MySQL Server

This section provides in-depth explanation required to enable the encryption for MySQL Data.

Enabling database encryption with MySQL consists of the following high-level steps, each of these steps has been discussed in their respective sections.

- Enabling SSL on the MySQL

- Creating Certificates

- Selecting the Cipher

- Enabling encryption between the MySQL and the various RiskVision components:
  - RiskVision Server

  - RiskVision Connector Manager

  - RiskVision Services

  - Server-side Connector

  - Web Services Server

  - SQL Connector

  - Jaspersoft Studio Professional

  - RiskVision Report Server

Configure MySQL

By default, MySQL traffic is neither compressed nor encrypted. To improve security, you can compress client/server traffic by using the --compress option while invoking the client programs. Another way to improve security is to set up an SSL connection between the RiskVision components that communicate with the MySQL.

Create New Certificates

To create new certificates:

1. Create a clean environment by deleting the junk files in the folders. You can create the directories as required.

2. Open command prompt, then enter `mkdir` to create a directory called `newcerts`.

   For example: `C:\>mkdir newcerts`

3. In command prompt, type `cd newcerts` The current working directory will be changed to newcerts.

4. Run the following commands:

```
openssl genrsa 2048 > ca-key.pem
```

```
openssl req -new -x509 -nodes -days 1000 -key ca-key.pem -out ca-cert.pem
```

```
openssl req -newkey rsa:2048 -days 1000 -nodes -keyout server-key.pem -out serverreqpem
```

```
openssl rsa -in server-key.pem -out server-key.pem
```

```
openssl x509 -req -in server-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -set_se
rial 01 -out server-cert.pem
```

```
openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client-key.pem -out clientreq.pem
```

```
openssl rsa -in client-key.pem -out client-key.pem
```

```
openssl x509 -req -in client-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -set_se
rial 01 -out client-cert.pem
```

5. Add the above generated files 4 (b), 4 (g)), and 4(h) to `my.ini` file for Client and 4 (g), 4 (d), and 4 (e) files for Server sections as mentioned below.

   The MySQL configuration file for Windows is `my.ini`.
   [Client]

   #SSL Client side files

```
ssl-ca="C:/newcerts/ca-cert.pem"
ssl-cert="C:/newcerts/client-cert.pem"
ssl-key="C:/newcerts/client-key.pem"
ssl-cipher=DHE-RSA-AES256-SHA
```

   [mysqld]

   # SSL Server side files

```
ssl-ca="C:/newcerts/ca-cert.pem"
ssl-cert="C:/newcerts/server-cert.pem"
ssl-key="C:/newcerts/server-key.pem"
ssl-cipher=DHE-RSA-AES256-SHA
```

6. Run the following commands in MySQL prompt:

```
GRANT USAGE ON agiliance.* TO 'agiliance''@'' REQUIRE SSL;
```

```
Example: GRANT USAGE ON agiliance.* TO 'agiliance'@'server_name' REQUIRE SSL;
```

```
FLUSH PRIVILEGES;
```

7. Restart the MySQL service and execute the query: show variables like 'have_%ssl%'

Variable Name	Value
have_openssl	YES
have_ssl	YES

MySQL is enabled for SSL connection.

8. Open a command prompt window an execute the following commands:

```
openssl pkcs12 -export -inkey client-key.pem -in client-cert.pem -out client.packet
```

```
%JAVA_HOME%\bin\keytool.exe -importkeystore -deststorepass  -destkeypass
 -destkeystore myKS.jks -srckeystore client.packet -srcstoretype PKCS12 -
srcstorepass  -alias 1
```

```
%JAVA_HOME%\bin\keytool.exe -importcert -alias mysqlCA -trustcacerts -file
ca-cert.pem -keystore myKS.jks
```

9. Create a folder `sslStore` under the `\config` directory .

10. Copy the `myKS.jks` file and paste it in the `\config\sslStore` folder.

11. For JDBC URL, when you enable SSL, append the following string:
    `verifyServerCertificate=true&useSSL=true&requireSSL=true`

12. By default, if you enter the server name as `localhost` , you may face errors. Instead, enter the actual host and/or server name which is referred in 6(a).

13. Refer to step 6 (b) and run the query.

For more information on properties, please refer to the `agiliance.properties` document.

Ciphers Overview

A cipher is an algorithm for performing encryption or decryption. The operation of a cipher usually depends on a piece of auxiliary information, called a key. Select a key before using a cipher to encrypt a message.

Cipher

To use a specific cipher, perform the following steps. It uses the `DHE-RSA-AES256-SHA` cipher as an example.

1. Open the `my.ini` file using a text editor.

2. Add the following line next to ssl-key line in Client and mysqld sections, then restart the MySQL service. `ssl` `-cipher=DHE-RSA-AES256-SHA`

3. By default, JRE 1.6 supports only 128-bit encryption. To use 256 bit, perform the following steps:
   - Download the zip file from: http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html.

     The zip file contains two jar files; local_policy.jar and US_export_policy.jar.

   - Rename or move the existing jar files and copy these files under `{JAVA_HOME}/jre/lib/security` directory. Make sure that these jar files are replaced if you are using a 256 bit encryption. For more information on properties, please refer to the agiliance.properties document.

4. Run the following MySQL client command to connect to the Server: `mysql` `-u -p --` `ssl` `-cipher=DHE-RSA-AES256-SHA`

Supported SSL Encryption

The following modules are supported for SSL encryption to and from the MySQL database:

- RiskVision Server
- RiskVision Connector Manager
- RiskVision Services
- Server-side Connector
- Web Services Server
- SQL Connector
- Jaspersoft Studio Professional
- RiskVision Report Server

RiskVision Server and Connector Manager

To allow RiskVision and the Connector Manager to communicate with an SSL encrypted database:

1. Set the following properties in the file `agiliance.properties` .

    o `database.mysql.url=jdbc:mysql://localhost:3306/?verifyServerCertificate=true`
    `&useSSL=true&requireSSL=true` (where localhost is database hostname)

    o `database.mysql.useSSL=true`

    o `database.mysql.keystore=config/sslStore/myKS.jks`

    o `database.mysql.keystoretype=JKS`

    o `database.mysql.keystore.password.encrypted=encrypted password`

    o `database.mysql.truststore=config/sslStore/myKS.jks`

    o `database.mysql.truststoretype=JKS`

    o `database.mysql.truststore.password.encrypted=06e2c4318c813af5h9kfxGjnv26pFS8qTm+zEQ==`

2. Restart the RiskVision Tomcat service.

Create an Encrypted Password

Perform the following steps to create the encrypted password.

To create an encrypted password:

1. Open Command Prompt.

2. Navigate to the folder `%AGILIANCE_HOME%>/Install/.toolbox/bin` .

3. Enter the command `encrypt.cmd` .

4. Observe that the encrypted password is generated to the ☐.

5. Copy the encrypted password and paste it for keystore and truststore passwords.

Server-Side Connector

Since the Server-Side connector will be installed on the same computer as the RiskVision Server, no additional configuration is required to configure JDBC encryption.

Web Services Server

Copy the java security files, paste the files into the web services server, then restart the server.

SQL Connector

No configuration changes are needed for SSL encryption.

RiskVision Report Server

Perform the following steps to configure SSL encryption.

Database

Execute the following query to enable reportuser to access SSL encrypted database:

- `GRANT USAGE ON` `agiliance` `.* TO '` `reportuser` `'@'' IDENTIFIED BY '' REQUIRE SSL;`

- `FLUSH PRIVILEGES`

RiskVision

1. Add the statements pointing to JKS files and keystore passwords in the agiliance.properties file.

2. Replace security jars under the security folder of jre\lib.

3. Restart RiskVision Job Manager, RiskVision Apache, and RiskVision Tomcat.

RiskVision Report Server

1. Add verify server certificate and use ssl properties to JDBC URL in \apache-tomcat\webapps\jasperserver-pro\WEB-INF\agiliance.properties file.

   Example: database.mysql.url=jdbc:mysql://:3306/?verifyServerCertificate=true&useSSL=true&requireSSL=true&useUnicode=true&characterEncoding=UTF-8&autoReconnect=true&autoReconnectForPools=true

2. Add the following statements pointing to JKS files and keystore passwords in the agiliance.properties file.

   The is where myKS.jks file is present. Make sure that you specify the complete path.

   Example:
   ```
   C:\sslStore\myKS.jks
   database.mysql.useSSL=truedatabase.mysql.keystore=/myKS.jks
   database.mysql.keystoretype=JKS
   ```
   `database.mysql.keystore.password.encrypted=encrypted password` (See Creating an Encrypted Password)
   `database.mysql.truststore=/myKS.jks`
   ```
   database.mysql.truststoretype=JKSc
   ```
   `database.mysql.truststore.password.encrypted=encrypted password`

3. Replace security jars, local_policy.jar and US_export_policy.jar under the %JASPER_HOME%\-java\jre\lib\security folder.

4. Open any browser and access the jasper server by using the URL : http://8480/jasperserverpro/login.html.
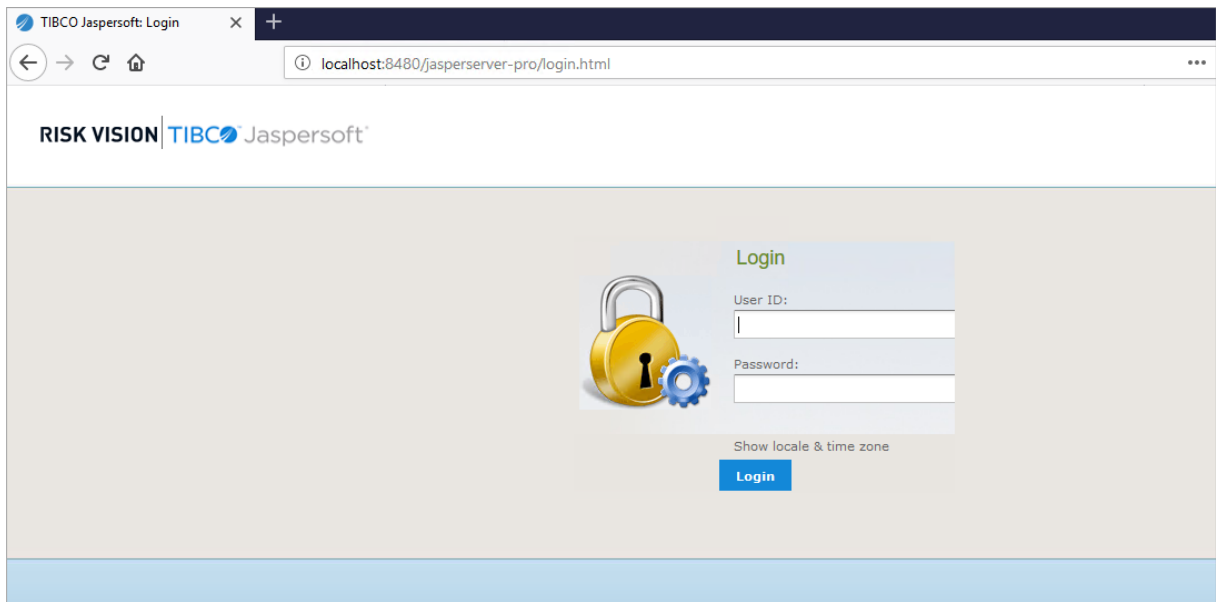
The JasperReport Server Login page.

5. Enter your **User ID** and **Password**, then click **Login**. The **JasperReports Server Home** page is displayed.
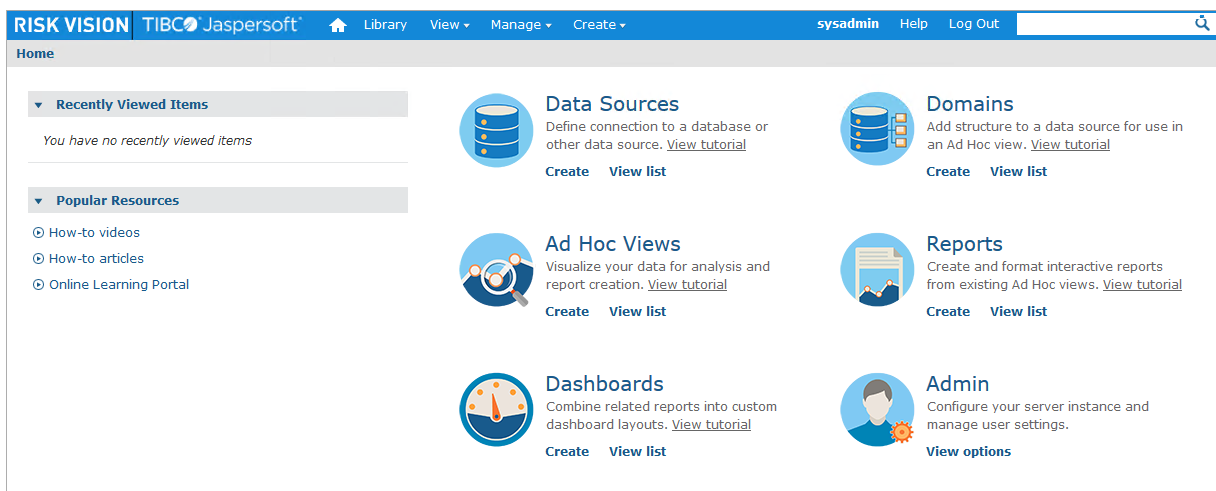
The JasperReports Server Home page.

6. Click **View** > **Repository**.
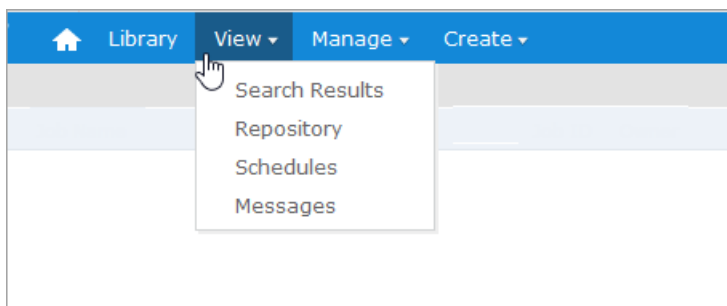
7. Expand **Public,** then click **Data Sources**. The **Data Source** appears in the **Repository** pane.
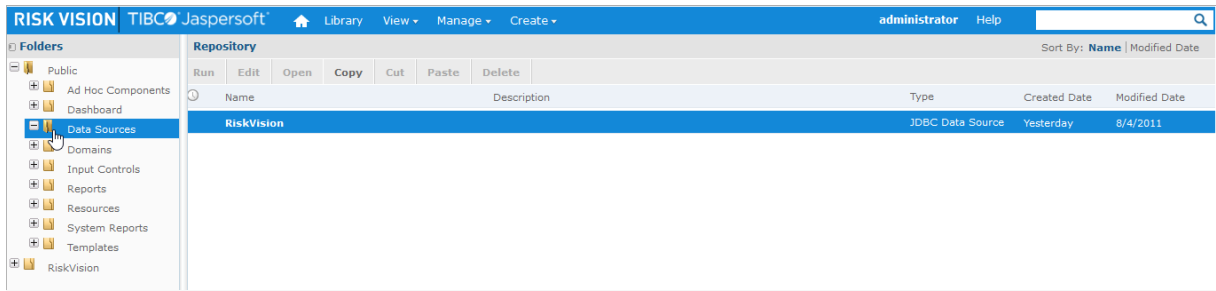
The Data Source in the Repository pane.

8. Click the data source, then click **Edit**.

The **Set Data Source Type and Properties** *page*

9. Append " `?verifyServerCertificate=true&RequireSSL=true&UseSSL=true` " to JDBC URL.

10. To validate the settings, click **Test Connection**. Based on the validation results, either proceed to step 11 or step 12.

Edit Data Source: RiskVision

Host (required):

localhost

Port (required):

3306

Database (required):

agiliance

URL (required):

jdbc:mysql://localhost:3306/agiliance?verifyServerCertificate=true&Requir

Hint: jdbc:postgresql://localhost:5432/mydb

User Name:

reportuser

Password:

••••••••••••••

Time Zone:

Use database setting

Hint: Do not change the time zone setting unless you know the database timestamp data is incorrect.

Test Connection ✅ Connection passed

Save **Cancel**

11. If the connection fails, verify the following steps:
    - Verify if the correct path for JKS file is specified.
    - Verify if you have executed the GRANT permissions with REQUIRED SSL.
    - Verify if the security jars have been replaced with the newly downloaded version.

12. Click **Submit**.

13. Restart the JasperpostgreSQL and JasperTomcat services:
    - Open the **Services** window.
    - Click the **jasperreportsPostgreSQL** service, then click **Restart**.
    - Click the **jasperreportsTomcat** service, then click **Restart**.

Remap RiskVision Tablespaces

If you need to name the Oracle tablespaces according to your organizational policy, the existing tablespaces in your Oracle database or the new ones that you would create must be allocated with sizes as suggested in step 5 of Oracle Server. When you are ready with tablespaces, perform the following steps:

1. Open the Windows command prompt, connect to the Oracle database, and navigate to the directory `%ORACLE_HOME%\admin\agl\dpdump` .

2. Execute the following command:

```
impdp system/agiliance@agl SCHEMAS=agiliance REMAP_SCHEMA=agiliance:target_schema
REMAP_TABLESPACE=AGLDATA:tablespace1 REMAP_TABLESPACE=AGLINDEX:tablespace2
REMAP_TABLESPACE=AGLTEMP:tablespace3 TABLE_EXISTS_ACTION=REPLACE DUMPFILE=AGLBASERELEASE.DMP NOLOGFILE=y;
```

Back up an Oracle Database

A database back up can be performed automatically using the Daily Server and Database Hot Back up system job or manually using a `expdp` command. Your database administrator should back up regularly to avoid problems when restoring the database. This section describes how to back up the Oracle database using a `expdp` command, roles required to perform a backup and the backup destination.

Manually Back up an Oracle Database

Users with appropriate role permissions can perform a database back up from Windows command prompt or SQL Plus using an `expdp` command.

1. Start SQL*Plus or any other tool that is available to run SQL commands.

2. Enter the following command and press **Enter**:

```
expdp system/@ schemas= directory=<%ORACLESERVER_HOME%> dumpfile=.dmp version=
```

3. Allow sufficient time for the backup process until the entire database is exported to an output file called dump file. When the command executes successfully, the dump file is archived to the following directory where the Oracle server is installed.

```
%ORACLESERVER_HOME%\admin\dpdump\.dmp
```

Assign a Role to Backup

To assign a role to a RiskVision schema user:

1. Start SQL*Plus or any other tool that is available to run SQL commands.

2. Connect the database, then execute the following grant command:

   `SQL>/@ as sysdba`

   `SQL>Grant exp_full_database to agl_owner`

   When you finish assigning the role, you can execute the `expdp` command to accomplish the backup job.

   Besides using the expdp command, you can also use the exp command to back up the Oracle database. Note that the exp command only supports a few datatypes that are available in Oracle Database 12c. Due to this limitation, we recommend using the expdp command instead.

`SQL>/@ as sysdba`

Oracle Backup Destination

When you run the Daily Server and Database Hot Backup system jobs, the procedure to track the backup file and folder vary slightly from the manual process.

To view the latest backup file name and the database location:

1. Go to the `%AGILIANCE_HOME%\backup` directory and open the `Oracle.backup` file.

   By default, this file retains the last 7 backups. The `lastBackup` property indicates the most recent backup folder.

2. Open the latest dump folder from the directory `%AGILIANCE_HOME%\backup`. Refer to the property `lastBackup` value and relate the value to the backup folder.

   The backup file is named using `-YYYYMMDDhhmmss.zip`, where the trailing characters in the filename are a timestamp of the backup date and time. This file normally contains the following back up and zip files:

   - The server backup file: `server-YYYYMMDDhhmmss.zip`

   - The Oracle dump file appears in the following form: `--backup-.dmp.log` For example, `oracle-scott-backup-6.dmp.log`.

3. Open the file `agiliance.log` using a text editor to view the database server location in which the backup file is present.

Skip the Oracle Database Backup

If your organization's security policies do not allow you to back up your RiskVision database, you can use the `com.agiliance.admin.backup.BackupManager.skipOracleBackup=true` property to skip the Oracle database backup and complete a RiskVision Server backup instead.

Oracle Schema Owner Privileges

Importing the **AGLBASERELEASE.DMP** file to set up the Oracle Server creates an Oracle schema owner with following default privileges. This will help you finalize the privileges for additional schema user that you might create to perform routine tasks.

Privilege	Description
ALTER USER QUOTA UNLIMITED ON agldata;	Sets unlimited quota on the `agldata` tablespace.
ALTER USER QUOTA UNLIMITED ON aglindex;	Sets unlimited quota on the `aglindex` tablespace.
GRANT CREATE SESSION TO ;	Allows connecting the database to create a user session.
GRANT CREATE TABLE TO ;	Allows creating tables in the database.
GRANT CREATE TRIGGER TO ;	Allows creating triggers in the database. The `aglt_alertrule_trg1` and `aglt_incidentdetail_trg1` are the two table level triggers in the RiskVision.
GRANT CREATE VIEW TO ;	Allows creating views in the database.
GRANT CREATE SEQUENCE TO ;	Allows creating sequences in the database. The `HIBERNATE_SEQUENCE` is the only sequence available in the database.
GRANT CREATE PROCEDURE TO ;	Allows creating procedures in the database.
GRANT CREATE TYPE TO ;	Allows creating types in the database. This privilege is required to create user-defined aggregate functions.
GRANT QUERY REWRITE TO ;	Enables with query rewrite. Oracle database offers an extremely powerful process called query rewrite to quickly answer a query using the materialized views. However, using query rewrite requires permissions to create materialized views and to enable the query rewrite.
GRANT READ, WRITE ON DIRECTORY TO ;	Assigns READ/WRITE permission on directories. For example, import and export schema on the data pump directory.

You may want to assign the SELECT ANY DICTIONARY privilege to Oracle Schema users. This provides additional debug options and allows users to query other schemas that are not relevant to their job function. However, users can to perform their jobs efficiently without the SELECT ANY DICTIONARY privilege, so provide only the necessary privileges to Oracle Schema users and to secure the database**.**

Reportuser Privileges

The **reportuser** user manages tasks related to the RiskVision Report Server in the Oracle database. This user has the following default privileges:

Privilege	Description
DROP USER CASCADE;	Allows dropping a user along with dependencies.
CREATE USER PROFILE default IDENTIFIED BY compliance DEFAULT TABLESPACE AGLDATA TEMPORARY TABLESPACE AGLTEMP ACCOUNT UNLOCK;	Allows creating a user on the `AGLDATA` tablespace with Unlock Account privilege.
GRANT CREATE SESSION TO;	Allows connecting the database to create a user session.
GRANT CREATE SYNONYM TO reportuser;	Allows creating a synonym in your own schema.
GRANT CREATE TRIGGER TO;	Allows creation of triggers. For example the trigger `agl_alterjssess_onlogon`.

Privileges for Reportuser in Oracle Database

The reportuser user manages tasks related to the RiskVision Report Server in Oracle database has the following default privileges:

Privilege	Description
DROP USER CASCADE;	Allows dropping a user along with dependencies.
CREATE USER PROFILE default IDENTIFIED BY compliance DEFAULT TABLESPACE AGLDATA TEMPORARY TABLESPACE AGLTEMP ACCOUNT UNLOCK;	Allows creating a user on AGLDATA tablespace with Unlock Account privilege
GRANT CREATE SESSION TO ;	Allows connecting the database to create a user session.
GRANT CREATE SYNONYM TO reportuser;	Allows creating a synonym in your own schema.
GRANT CREATE TRIGGER TO ;	Allows creation of triggers. For example the agl_alterjssess_onlogon trigger.

Manage a Tablespace in the Oracle Database

A datafile of a tablespace must be allocated with sufficient space on the disk so that RiskVision Server never halts when more space is needed in the database. While setting up tablespaces as required by the RiskVision Server, you can set the datafile size of a tablespace to extend the file size automatically to a specified maximum value. When you ran into the "*ORA-01654: unable to extend index*" error that has interrupted the RiskVision Server from operating, the error indicates that the auto-extensible option is not set for the datafile.

In order to resume the RiskVision Server and to avoid the occurrence of the error in future, perform the following steps:

1. Run the following query to check whether the auto-extensible option is enabled and free space in the datafile is available:

   ```
   SELECT de.file_id, df.file_name, df.AUTOEXTENSIBLE, df.bytes/1024/1024, SUM(de.bytes)/1024/1024
   FROM dba_extentions de, dba_data_files df
   WHERE de.file_id=df.file_id GROUP BY de.file_id,df.file_name, AUTOEXTENSIBLE, df.bytes/1024/1024;
   ```

   If the above query shows any free space, perform step 2, or else go to step 3.

2. When you notice any free space, run the following query to combine all the free space chunks into one large chunk.

   ```
   ALTER TABLESPACE aglindex COALESCE;
   ```

   Check whether you are able to operate the RiskVision Server as before.

3. If the problem still persists, run the following query to add a new datafile to the tablespace.

   ```
   ALTER TABLESPACE aglindex ADD DATAFILE '~/oradata/agl/datafile.dbf' AUTOEXTEND ON NEXT 500M MAXSIZE 20G;
   ```

   Adding a new datafile must resolve the problem.

4. If all your efforts to overcome the problem has failed even after you perform the steps above, run the following query to change the size of the existing datafile. Run this query only when you have reached the maximum number of datafiles allowed for a tablespace.

   ```
   ALTER DATABASE DATAFILE '<~/datafile.dbf>' RESIZE 10G;
   ```

   The sizes can be specified in the megabyte, gigabyte or terabyte. You must examine the free disk space before specifying the value for `NEXT` (a minimum size that a datafile must increment when it extends) and `MAXSIZE` (a maximum size that a datafile can automatically extend).

Restore the RiskVision Server

To restore the server to a specific point in time, get a copy of the backup file made closest to the time you want to restore and then unzip the file in the base RiskVision Server installation directory (denoted by in `%AGILIANCE_HOME%` the installation instructions).

Use a WinZip-compatible tool (e.g., WinZip, WinRAR, etc.) to extract the contents of the RiskVision Server back up file; the Windows built-in tool for Compressed (zipped) Folders and the unzip command in Cygwin will not work (because the back up files are created with a Java zip package that can create zip files larger than 2 GB).

Restore the RiskVision Database

Stop the RiskVision Tomcat service before you start restoring the database to the specific point in time when a database back up was made:

1. Go to the following back up directory: `%AGILIANCE_HOME%\backup`

   > `cd %AGILIANCE_HOME%\MySQL\bin`

2. Extract all the files and directories from the backup `-YYYYMMDDhhmmss.zip` file, including the database backup file, `mysqldump-YYYYMMDDhhmmss.sql`. Choose the backup file with a timestamp YYYYMMDDhhmmss that is closest to the time that you want to restore.

3. Open the command prompt and change the directory to the location as given in the following command:

4. Import the MySQL dump file with the following command:

   `mysql -u` `root` `-p` `rootpassword` --database < `%AGILIANCE_HOME%\backup\-YYYYMMDDhhmmss\mysqldump-YYYYMMDDhhmmss.sql`

   MySQL supports point-in-time recovery, which can be used to restore the database to a more specific point in time. However, this procedure is more complicated and must be performed only by an experienced the MySQL DBA.

   When you observe that a table is not created after completing the backup, run the following commands to ensure a full and smooth back up:

   ```
   mysql -uroot -prootpassword
   drop database agiliance;
   create database agiliance;
   exit;
   ```

   `mysql -uroot -prootpassword` `< mysqldump-` `YYYYMMDDhhmmss` `.sql`

5. If you have excluded tables from the normal back up process (see Ignoring Database Tables During Backup), run the following command:

   `mysql -uroot -p` `rootpassword` `<` `IgnoredTableName` `.sql`

   Repeat this command for each ignored table specified in tableList for the `IgnoredTableName` s parameter in the `agiliance.properties` file. The initial default configuration includes the agl_auditlog table in the list of settings `RiskVision.default.system.properties`.

6. Execute the MySQL post installation scripts.

   Note: When importing a database dump file from one server to another, you may encounter errors due to definer attributes remaining from the previous server. The post installation scripts will resolve this issue.

7. After the complete restoration of the database, start the RiskVision Tomcat service.

The default password for the MySQL root user is `agiliance`. Refer to the procedures described in Property and Configuration File Settings for more information on changing default MySQL usernames and passwords.

Restore the RiskVision Report Server

When the Daily Server and Database Hot Backup job is run, the RiskVision Report Server backup is created in the directory `%AGILIANCE_HOME%\backup` .

To restore the RiskVision Report Server:

> `cd %JASPER_HOME%\Postgresql\bin`

`pg_restore -c -h localhost -p 5432 -U postgres -d jasperserver -v %AGILIANCE_HOME%\backup\-YYYYMMDDhhmmss\jasperdump-YYYYMMDDhhmmss.sql`

Where -p and -v are optional parameters.

1. Obtain the file `jasperdump-YYYYMMDDhhmmss.zip` , extract the file and then save it in a temporary folder on the system in which the JasperReports Server is installed.

2. Open the command prompt and change the directory to the location given in the following command:

3. Import the dump file using the following command:

4. Enter the default password for `agiliance` the PostgreSQL database. The back up is restored successfully.

If you have changed the password for Postgres database then you need to set value for `database.jasper.admin.password.encrypted` . Use that value as the password to unzip `jasperdump-YYYYMMDDhhmmss.sql.zip` .

Appendix A: Database Recovery

The following instructions describe how to recover the RiskVision database to the point of a media failure:

1. Restore the database with the latest full backup file; the MySQL dump file mysqldump-YYYYMMDDhhmmss.sql contained in the server and database backup file -YYYYMMDDhhmmss.zip that has the latest timestamp YYYYMMDDhhmmss. See instructions in the Restoring the Database section.

2. Check in the MySQL dump file mysqldump-YYYYMMDDhhmmss.sql to find the value of MASTER_LOG_FILE. The value must be in the form of '.nnnnnn', where nnnnnn is a sequence number. This is the first incremental MySQL binary log file created after the backup was performed.

3. Go to the directory for the MySQL incremental backups (see the Backup Destination Directory section), run the mysqlbinlog and mysql commands to bring the database to the point when failure occurred.

   For example, if nnnnnn is 000100, and there are three binary log files newer than .000100, run this command:

   mysqlbinlog .000100 .000101 .000102 .000103 | mysql -uroot -p rootpassword

   When the command completes successfully, the database will be recovered to the previous point where the failure occurred.

Appendix B: Installation Log Files

This section discusses the log files of different components installed in your environment. Log files record almost everything - user operations, errors, and much 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

Create an SSL CA Certificate

Using SSL certificates boosts security and provides a more reliable connection while working in RiskVision. To create a certificate, follow the steps below:

To create an SSL CA certificate:

1. Download and install OpenSSL.

2. Create a bin folder, if required. (Will probably delete the last half of this sentence and replace it with "optional". Might also need to include steps on how to create a bin folder or link to instructions on how to.)

3. Create a file named `openssl.cfg` or similar. (How do we do this?)

4. Open Command Prompt and navigate to `Openssl_home\bin` (e.g., `c:\openssl\bin`). (This doesn't make sense to me. What context are we missing?)

5. Set `OPENSSL_CONF=c:\Openssl\bin\openssl.cfg` .

6. Run the following commands to generate a private key with a passphrase, entering the appropriate values for each prompt that appears:

   `>` `openssl req` `-x509` `-newkey rsa:4096` `-sha256` `-keyout server.key` `-passout pass:hello`

7. To create a CSR from the above generated key, run the following command: (is it command or commands?)

   `>` `openssl req -key server.key -new -out domain.csr`

   - Enter the passphrase generated in step 6 (e.g., hello).

   - Enter the appropriate values for each prompt.

8. Contact your CA (Certificate Authority) and request a new certificate generated from the CSR (Certificate Signing Request) created in step 7.

9. Place the newly created passphrase in `passphrase.bat` in the location:

   `'%RiskVision_Home%'\apache2\conf\extra`