

RiskyProject Enterprise 7.2

Project Risk Management Software

Administrator's Guide



Intaver Institute Inc.

www.intaver.com

email: info@intaver.com

COPYRIGHT

Copyright © 2022 Intaver Institute. All rights reserved.

The information in this document is subject to change without notice. The software described in this document is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Intaver Institute.

RiskyProject™ and Event Chain Methodology™ are trademarks of Intaver Institute.

Microsoft® is a registered trademark of Microsoft Corporation. Windows®, and Project®, are registered trademarks of Microsoft Corporation.

All other names and trademarks are the property of their respective owners.

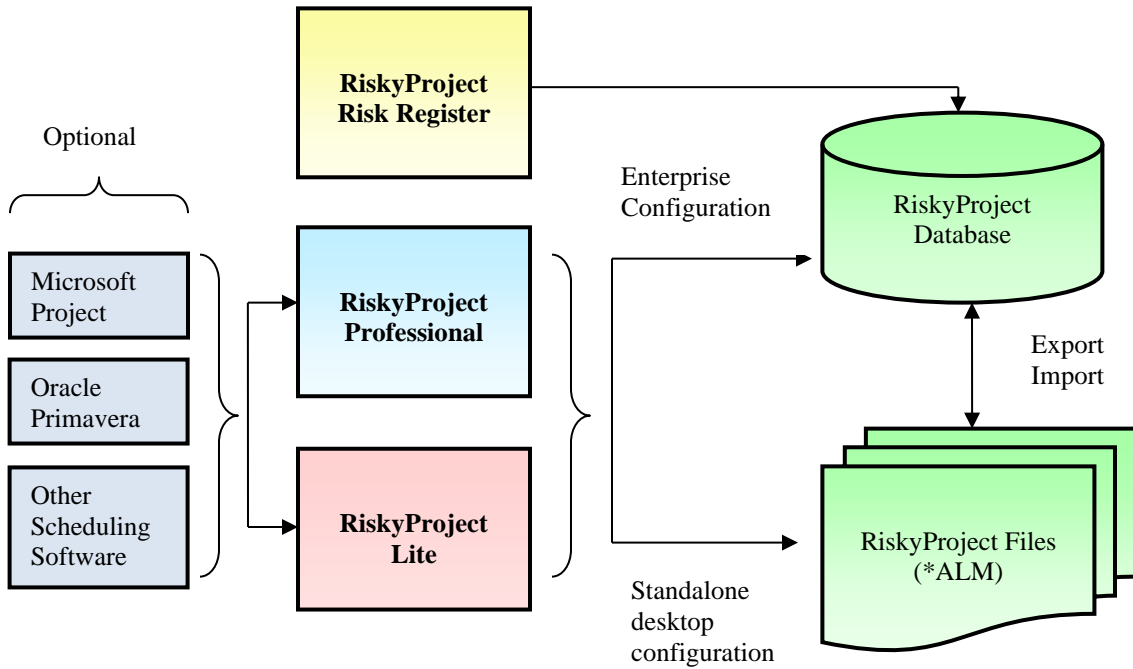
Contents

Chapter 1: Introduction to RiskyProject Enterprise	1
About RiskyProject Enterprise	2
What do I need to install RiskyProject Enterprise	3
Chapter 2: RiskyProject Enterprise Installation	5
RiskyProject and Windows Authentication Modes	6
Installing RiskyProject Professional	7
Configuring Access to a Remote Database	7
Installing Empty RiskyProject Database	8
Setting up connection to database	10
Enabling number of users, type of user licenses, and license duration	10
Defining Information about Administrator	11
Installing RiskyProject Sample Database	12
Configuring Access to Remove SQL Server Database	12
Chapter 3: RiskyProject Enterprise Configuration	17
About User Management	18
About Organizational Breakdown Structure	18
About Roles	18
About Creating and Modifying Users, Organizational Units and Security Groups	18
Switching Between Authentication Modes	21
About Project Permissions	22
About the Logon History	23
Updating RiskyProject Enterprise License	23
Switching Between Enterprise and Standalone Desktop Configurations	24
Connecting to a Different Database	25
Other RiskyProject Configuration Steps	26
Configuring Integration with Proteus Envision®	26
Notification Messages	27
Using Windows Task Scheduler for Sending Notification Messages	27

Chapter 1: Introduction to RiskyProject Enterprise

About RiskyProject Enterprise

RiskyProject is project risk management software. RiskyProject can be configured as standalone desktop software, which saves files to the set of files for each project, and enterprise software, which saves data in the database. As the same installation package is used for desktop and enterprise software, switching from one version to another is quick and easy. You can switch from one configuration to another two configurations using the RiskyProject user interface.



What do I need to install RiskyProject Enterprise

To install RiskyProject Enterprise you need to have:

1. RiskyProject Professional installation file: RiskyProjectSetup.msi
2. License file (RiskyProject.lic)

License file includes the following information:

- Number of users
- Type of users: **concurrent** or **named**. If users are concurrent, only a limited number of users can be logged on to the enterprise system at the same time. If users are named, only a limited number of user names can be entered into the system.
- Duration of the license.

By default (without license files), the number of users is 1 and license duration is 1 month.

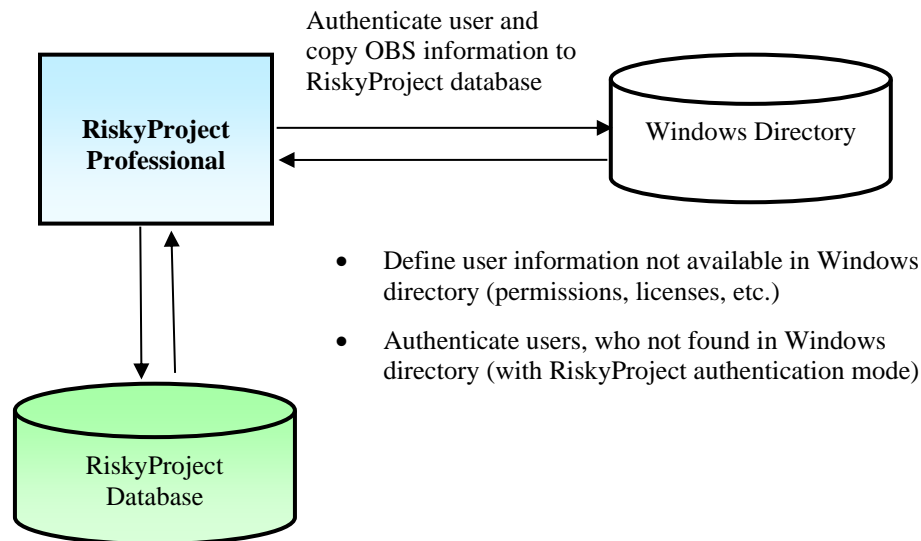
3. Access to the database. At a present moment, RiskyProject works only with SQL Server or SQL Server Express. RiskyProject supports SQL Server 2018 and later. SQL Server Express can be downloaded free of charge from the Microsoft web site.
4. RiskyProject Lite installation file (optional): RiskyProjectLiteSetup.msi
5. RiskyProject Risk Register installation file (optional): RiskyProjectRiskRegisterSetup.msi

Chapter 2: RiskyProject Enterprise Installation

RiskyProject and Windows Authentication Modes

Before installing RiskyProject you may need to decide, what authentication mode you will use. RiskyProject uses two authentication modes:

1. **RiskyProject authentication.** In this mode RiskyProject administrator needs to define Organizational Breakdown Structure (OBS) with all users in RiskyProject using User Management dialog. Administrator will define user information including names, emails and other contact information, permissions, roles. The administrator will assign RiskyProject license types for each user which include RiskyProject Professional, RiskyProject Lite, or RiskyProject Risk Register. In this mode all user information including passwords in encrypted form are saved in the RiskyProject database. This way of authentication is recommended if Windows directory is not accessible or if OBS used in RiskyProject is different than in the Windows directory. For example, if RiskyProject will have only a few users and Windows directory contains all users in the organization.
2. **Windows and RiskyProject authentication.** In this mode RiskyProject will authenticate the user against Windows Active directory. If the user has appropriate permissions, RiskyProject will read OBS to each time RiskyProject starts and save it in RiskyProject database. This OBS information will be used for RiskyProject operation. Users will not enter their passwords when logging onto RiskyProject. Since the Windows directory does not contain all information necessary for RiskyProject operation, the administrator needs to define user permissions, license types, and contact information and save this in the RiskyProject database. The administrator may add user that are not in Windows directory, to RiskyProject database. These users may need to enter their user names and passwords. Also, the administrator may remove certain users from RiskyProject OBS even if they are in the Windows directory. This method of authentication is recommended when many or all users in organization need to have an access to RiskyProject and organization has an extensive OBS.



Installing RiskyProject Professional

Use the RiskyProject Professional installation file (*RiskyProjectSetup.msi*) to install RiskyProject Enterprise.

Configuring Access to a Remote Database

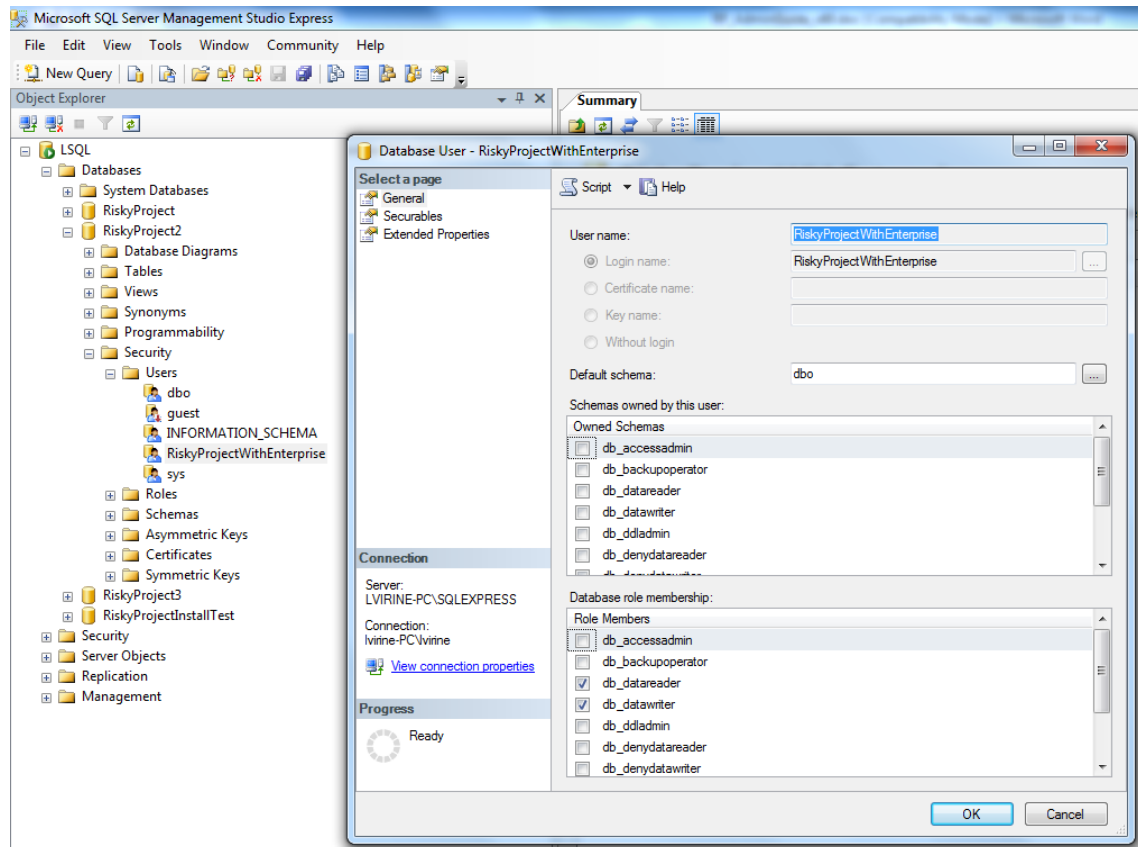
The RiskyProject database must be accessible by RiskyProject clients (RiskyProject Professional, RiskyProject Lite, or RiskyProject Risk Register), which are installed on computers on a network.

Firewall systems help prevent unauthorized access to computer resources. If a firewall is turned on but not correctly configured, attempts to connect to SQL Server might be blocked.

For more information regarding how to configure a firewall please visit:
<http://msdn.microsoft.com/en-ca/library/cc646023.aspx>.

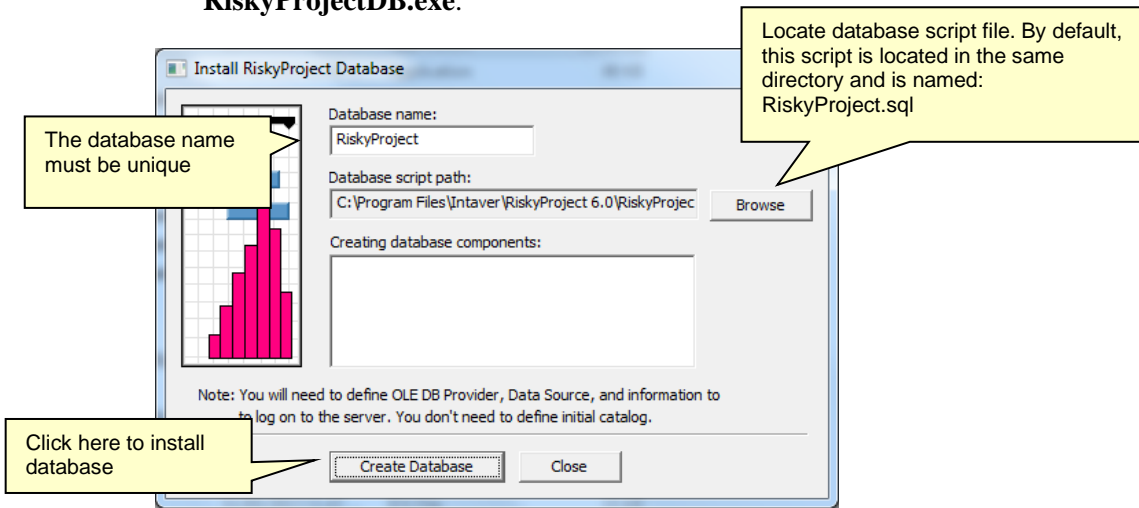
For each Windows user or group on your network that will be running RiskyProject Enterprise, you must use SQL Server Management Studio to create:

1. SQL Server Logins for all your users or groups
2. Once you have installed the RiskyProject Enterprise database, users in the RiskyProject Enterprise database with memberships in the db_datareader and db_datawriter roles.

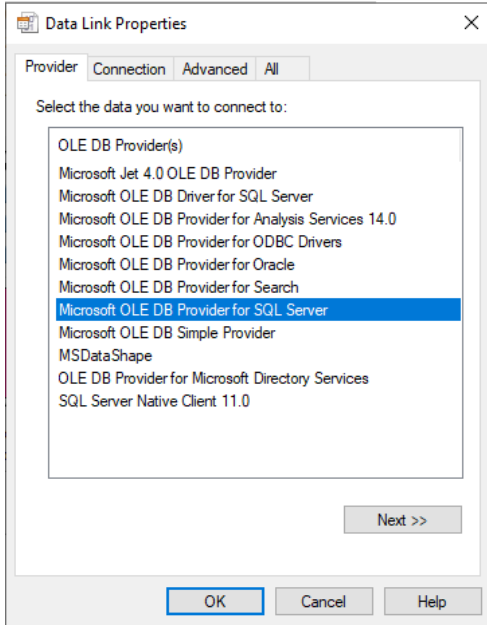


Installing Empty RiskyProject Database

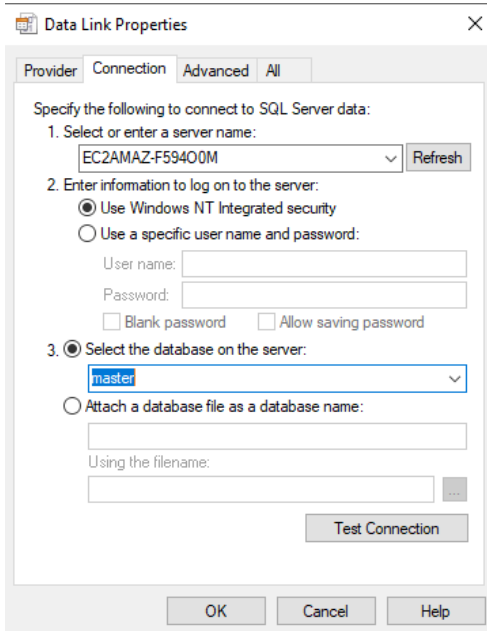
1. From RiskyProject directory (e.g. C:\Program Files\Intaver\RiskyProject 7.2) launch **RiskyProjectDB.exe**.



2. Select the database provider such as Microsoft OLE DB Provider for SQL Server:



3. Specify data link properties. In *Select the database or server* don't select anything or select master



Click **OK**. RiskyProject database will be created.

Setting up connection to database

1. Launch RiskyProject Professional, RiskyProject Lite, or RiskyProject Risk Register
2. Select **Enterprise Client (requires database)**
3. Configure database connection: follow the same steps you use to connect to the database as you did in step 3. In *Enter the initial catalog to use* select the database you just created.
4. Select if you would like to use **Windows and RiskyProject Authentication** (Active directory). Alternatively, you can use RiskyProject Authentication. If you use Windows Authentication, you may define a Domain Name for Active directory.

Enabling number of users, type of user licenses, and license duration

Number of users, type of user licenses (concurrent or named users) and license duration come from the license file, such as RiskyProject.lic. If this file is not available, default number of users will be 1, license duration will be 30 days.

- If you use concurrent user type, RiskyProject will control how many users can logon to the database at the same time.
- If you use named user type, RiskyProject will control how many user names can be available.

You may switch type of users, number of users, and license duration at any time. To do so, you must request a new RiskyProject license file (RiskyProject.lic).

These information will be populated from the license file

Select license file which is supplied by Intaver Institute

Defining Information about Administrator

If you use RiskyProject authentication method you need to define Administrator's information. It is a first user information which will define all other users. Administrator will have full permissions to all RiskyProject data.

After you define the Administrator's information, you need to define password for administrator. Passwords can be recovered via email. Therefore it is important to define the correct email of Administrator in User Profile dialog and configure email access in Notification manager (see *Notification Messages* in the *RiskyProject Enterprise User Guide* for more information).

If user name or password for administrator are lost, email is not configured, and other administrators are not defined, the only way to recover administrative access to RiskyProject would be to delete all content of RP_Users table in the database.

Installing RiskyProject Sample Database

RiskyProject comes with a sample database, which includes sample data. The sample database will help you to learn how to use RiskyProject. To install the sample database:

1. Download the script called **RiskyProjectSampleDB.sql** from <https://intaver.com/products/riskyproject-enterprise> and save it in the temporary folder.
2. Start **RiskyProjectDB.exe** from the RiskyProject directory.
3. Click Browse and select the script called **RiskyProjectSampleDB.sql**
4. Configure access to the database by following the steps outlined in “*Step 3: Install Empty RiskyProject Database*”
5. Set up database connection by following the steps outlined in “*Step 4: Setup connection to database*”. Administrator's user name is **Admin**, password is **Admin** (case sensitive).



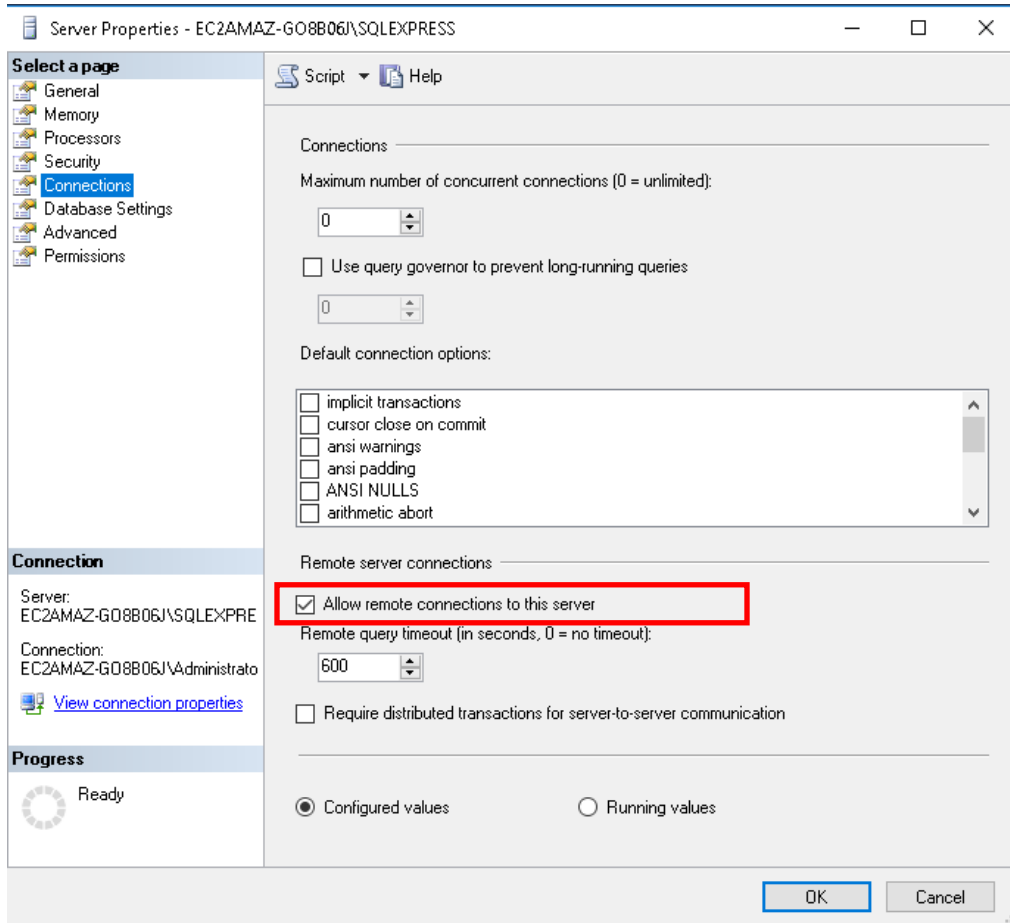
You can also execute the same script using Microsoft SQL Server Management Studio.

Configuring Access to Remove SQL Server Database

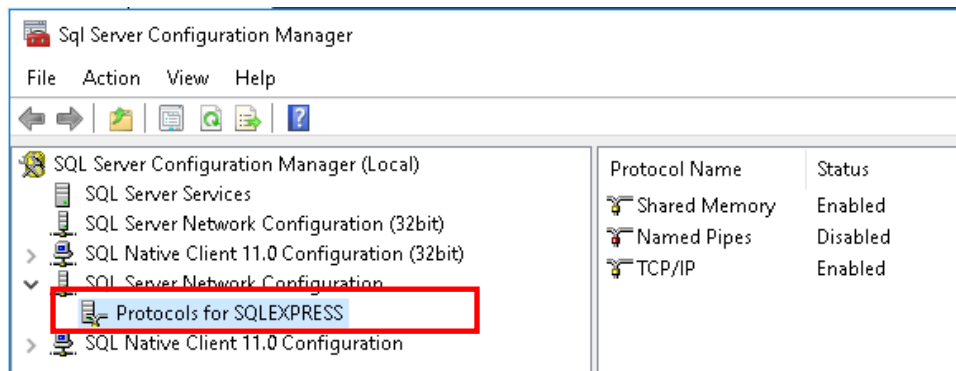
This section explains how to configure remote access on a SQL Server instance and connect to a remote SQL Server instance with RiskyProject client

Configuring remote access on a SQL Server instance

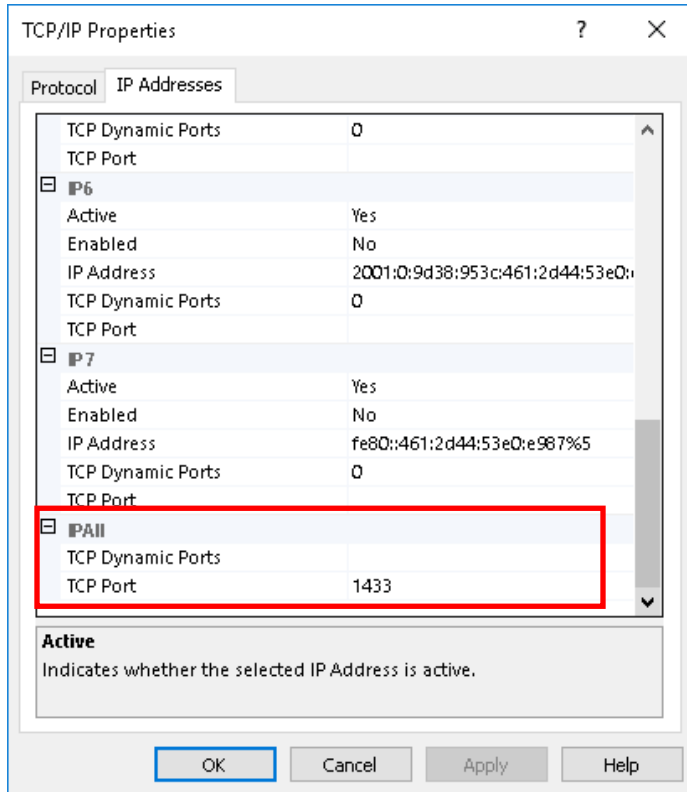
1. On the server Start Microsoft SQL Server Management Studio
2. Right click on the server and select the Properties option.
3. In the Server Properties dialog under the Connections tab check the Allow remote connections to this server option:



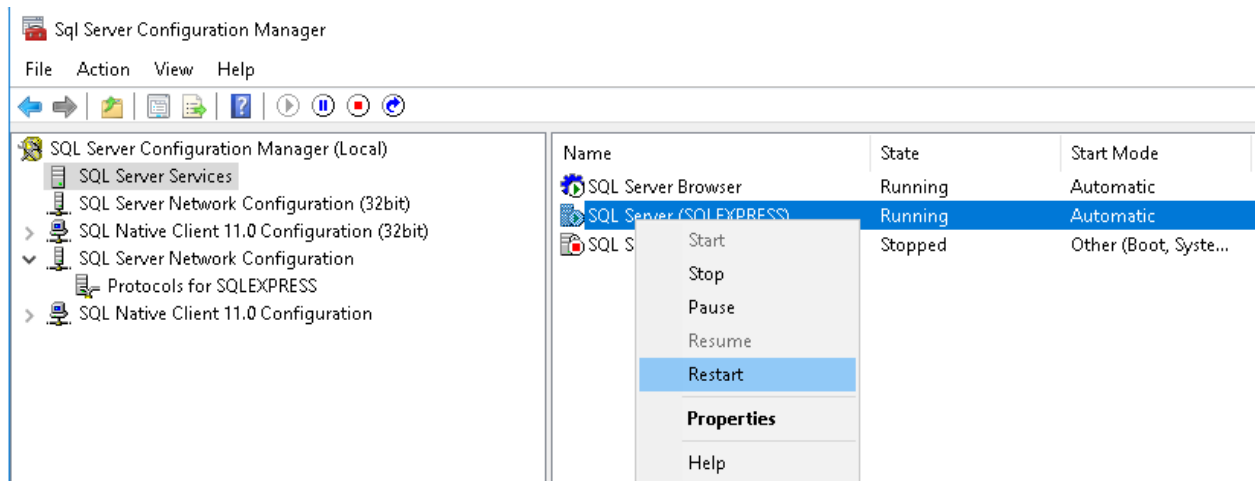
4. Go to Start->Programs->Microsoft SQL Server... ->Configuration Tools and select the SQL Server Configuration Manager
5. Under the SQL Server Network Configuration select Protocols for <your server name>:



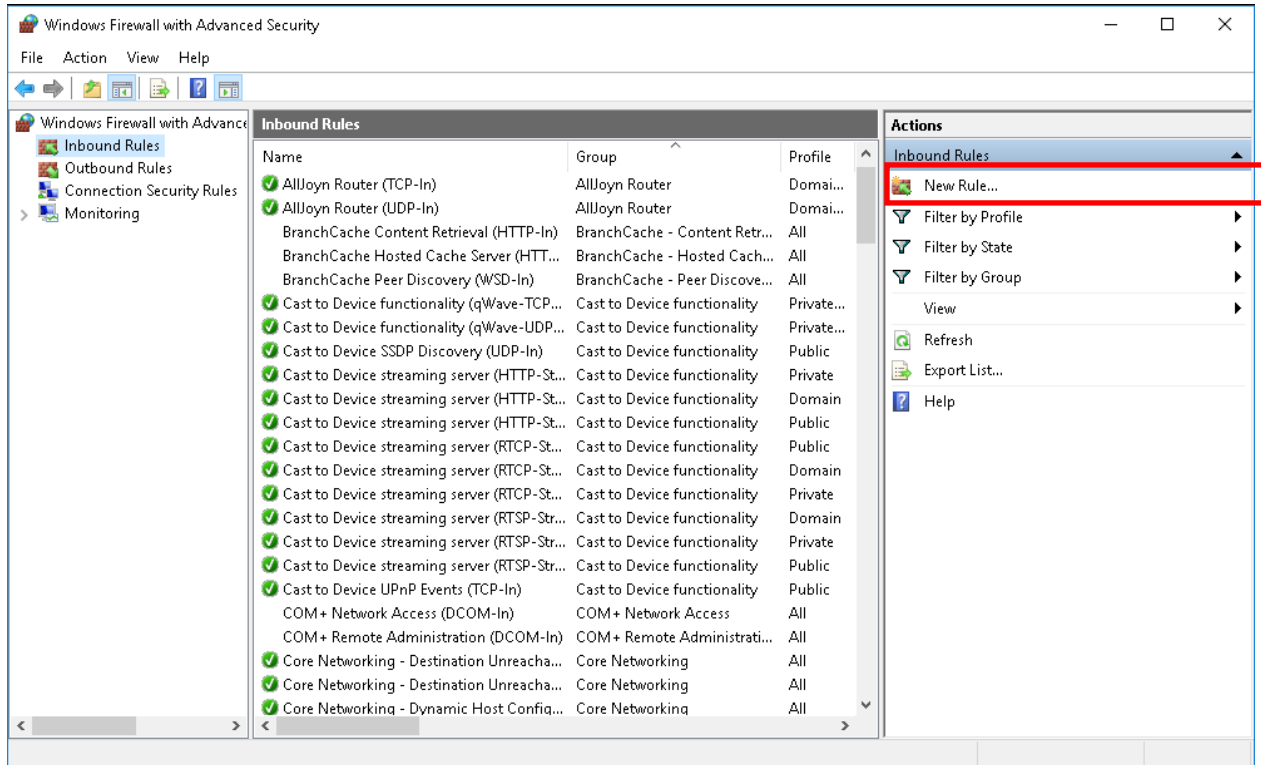
Make sure that TCP/IP protocol is enabled and right click on TCP/IP and select the Properties option. In the TCP/IP Properties dialog select the IP Addresses tab and scroll down to IPAll. If the TCP Dynamic Ports dialog box contains 0, which indicates that the Database Engine is listening on dynamic ports, delete the 0 and set the TCP Dynamic Ports to blank and TCP Port to 1433. Port 1433 is the default instance that SQL Server uses:



- When you click the OK button you will be prompted with a message to restart the service. In the left pane of SQL Server Configuration Manager click SQL Server Services, right-click SQL Server<instance_name>, and click Restart:



- You also need to configure a Windows Firewall for Database Engine Access. To add a firewall exception for the 1433 port go to Programs -> Administrative Tools select the Windows Firewall with Advanced Security option.
- In the Windows Firewall with Advanced Security dialog click on the Inbound Rules option and select the New Rule command:



9. In the New Inbound Rule wizard select the Port option and click Next
10. In the Protocols and Ports window specify the protocols and ports to which a rule applies. Select the TCP option, in the Specific local ports text box enter the 1433 port, and click Next.
11. In the Action window select the Allow the connection to specify the action to be taken when a connection matches the conditions specified in the rule.
12. Specify the profiles for which the rule applies in the Profile window, and click Next. You can now see the created rule in the list of inbound rules.
13. If you are using Amazon Web Services, you also need to open port 1433 in Security group. For virtual machine with RiskyProject client, define port 1433 as part of Outbound rules.

Type	Protocol	Port Range	Destination	Description
MS SQL	TCP	1433	0.0.0.0/0	
MS SQL	TCP	1433	:::0	

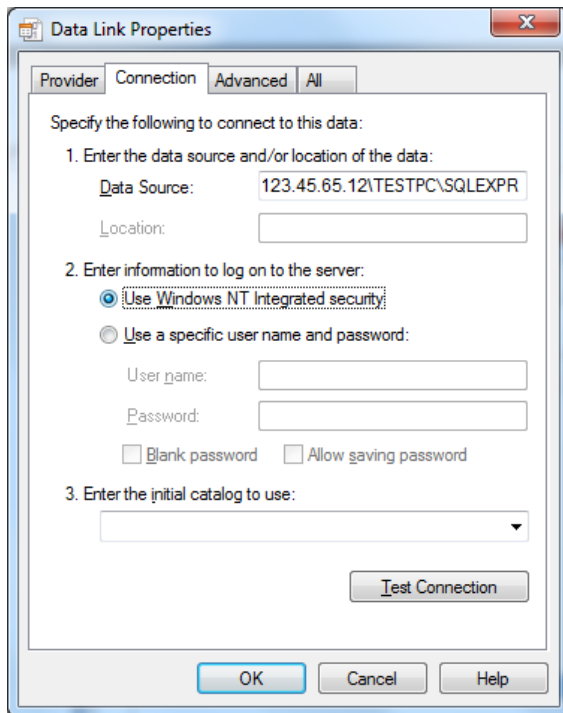
14. For virtual machine with SQL Server database, define port 1433 as part of Inbound rules.

Description **Inbound** Outbound Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
MS SQL	TCP	1433	0.0.0.0/0
MS SQL	TCP	1433	:::0
RDP	TCP	3389	0.0.0.0/0
RDP	TCP	3389	:::0

15. RiskyProject connection to remote database is similar to connection to locally installed database. However in Data Lost Properties dialog, Connection tab, you need to define IP address of remote computer before the name of the instance.



Chapter 3: RiskyProject Enterprise Configuration

About User Management

In RiskyProject Enterprise, user management is based on users, roles, and permissions. Each individual who accesses the system, should be assigned user logon credentials which are defined in the User Administration panel. Users can be assigned one of three roles: Administrator, Manager, or User.

RiskyProject Enterprise licensing defines the:

- Number of named or concurrent users
- The number of each Professional, Lite, and Risk Register modules that are included with the system.

About Organizational Breakdown Structure

In RiskyProject Enterprise, you can define an Organizational Breakdown Structure (OBS). The OBS includes a hierarchical system of **Organizational Units** and **Security Groups**. Security groups are used to define permissions for groups of users. A hierarchy of organizational units should repeat the actual organizational structure and include information about the location and managers of organizational units. This information is used for properties of projects, risks, and issues, as well as for risk notification. Users may belong to multiple organizational units or security groups.

About Roles

RiskyProject Enterprise has 3 defined roles that can be assigned to users: Administrator, Manager, and User.

Administrator: has full access to RiskyProject, including managing permissions.

Manager: may have full access to RiskyProject except managing users and updating user permissions. The manager's permissions can be limited by an administrator.

User: cannot manage users, modify portfolio settings, or delete projects. In addition, an administrator can limit a user's permissions.

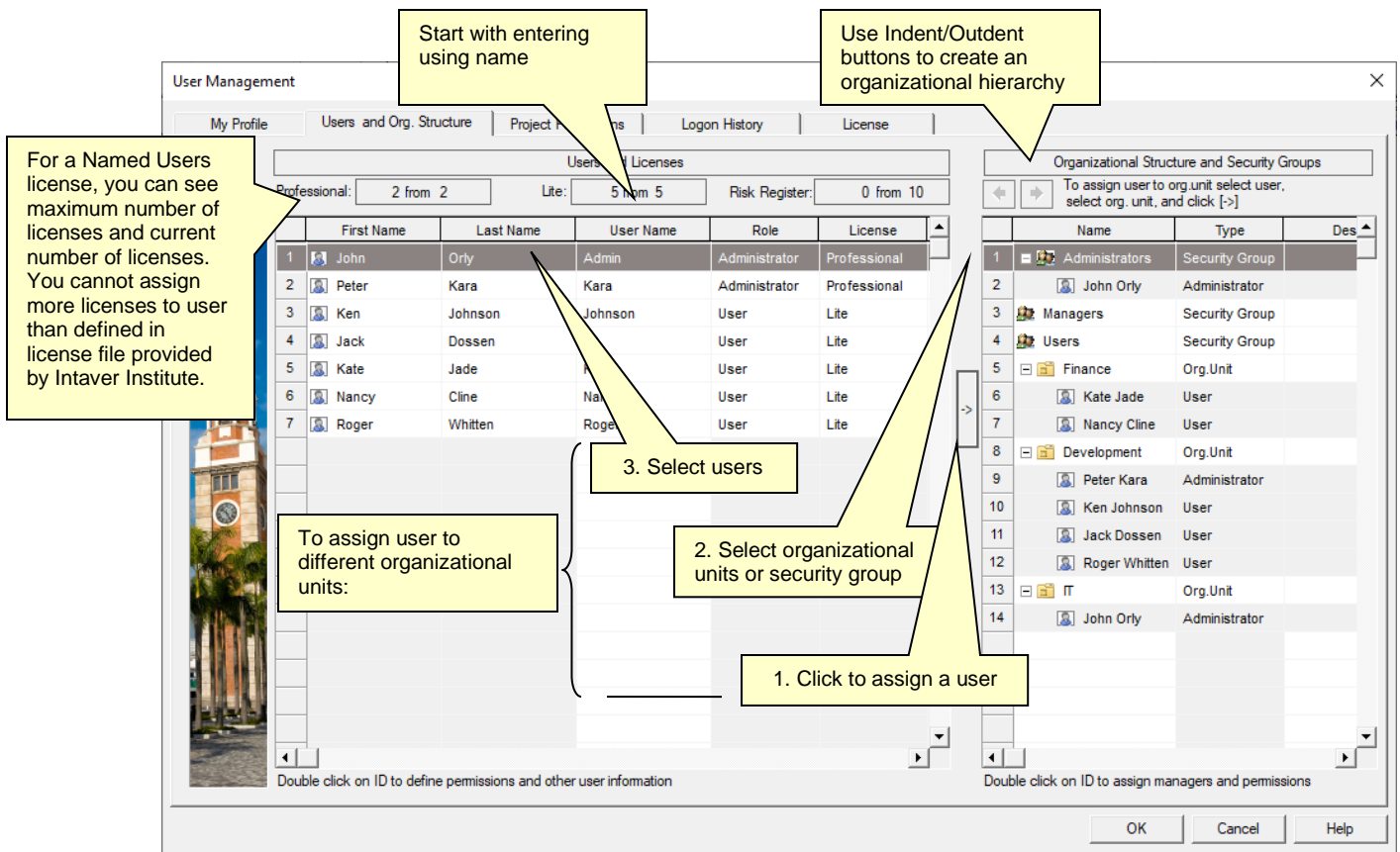
About Creating and Modifying Users, Organizational Units and Security Groups

Create a New User

Once you have created the Administrator role, you can create a new user.

To create a new user:

1. Click the **Users and Org Structure** tab.
2. In the **User Name** column, click in an empty row and type in the user name.
3. In the **Role** column, Select a role for the user from the drop-down list.
4. Select a RiskyProject module type for the user. Modules are RiskyProject Professional, Lite, and Risk Register. The logon will be denied if the assigned module does not correspond with actual software installed on user computer.



5. Right-click on the user and choose **User Profile**. The User Profile dialog box opens.
6. Add user information as required.
7. In the **Permissions** group, select the permissions that you want to grant to the user.
8. Click **OK** to save the user profile.

Create the Organizational Structure

You can define organizational units and security groups in the right pane of **Users and Org Structure** tab. Three security groups: Administrators, Managers, and Users are created by default.

To create an organizational structure:

1. Type organizational unit or security group name in right pane.
2. Designate it as an Organizational Unit or Security Group by selecting **Org. Unit** or **Security Group** in Type column on the **Organizational Structure and Security Groups** pane.
3. Use the **Indent/Outdent** buttons to create the organizational hierarchy.
4. Assign users to organizational unit or security group by:
 - a. selecting users,
 - b. selecting an organizational unit or security group, and
 - c. clicking the [->] button to assign users.
5. Right-click on the organizational unit and select **Properties**. Enter the managers, description and location of the organizational unit. If you use the Windows and RiskyProject

Authentication method, this information will be obtained from Windows and will be read-only.

- Right-click on the security group and choose **Permissions**. Assign permissions to the group. The permissions will be applied to all users in the group. Administrators have full access to all functionalities.

Updating User Information

To update User information, double-click on user ID in the **Users and Org Structure** tab of the **User Management** dialog.

The screenshot shows the 'User Management' dialog box for a user named 'Kara'. The dialog is divided into several sections:

- Header:** Includes a 'Reset User Password' button and a 'License' dropdown menu set to 'Professional'. A callout points to the license dropdown: "Assign license type to the user from the pool of available licenses".
- Basic Information:** Fields for Display Name (Kara), First name (Jack), Last name (Karagan), and Initial. A callout points to the 'Reset User Password' button: "Click to create a temporary password for the user (RiskyProject authentication mode only)".
- Description:** Field containing 'Director, Information System'.
- Contact information:** Fields for Company (XYZ Corp), Address (760, 5th Ave), City (New York), State (New York), Postal Code (21044), Bus. Phone (212-304-4356), Home Phone (212-473-5493), and E-mail (kara@xyzcorp.com). A callout points to the E-mail field: "Temporary password will be used to this email. Also this email will be used for password recovery." A note above the Organizational Unit field says: "Assign user to organizational unit in 'Users and Org,Structure' tab of User Management Dialog".
- Emergency contact information:** Fields for First name, Last name, E-mail, and Bus. Phone. A callout points to this section: "Define user permissions".
- Permissions:** A section with checkboxes for:
 - Create risks/incidents*
 - Modify risks/incidents
 - Delete risks/incidents
 - Create mitigation/response plans
 - Modify mitigation/response plans
 - Delete mitigation/response plans
 - Create projects and update project hierarchy
 A note below the permissions section states: "* Select 'Create risks' to allow user to create risks at enterprise level of the hierarchy. Users can always create risks on project in which they have permissions."
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

If you use *RiskyProject authentication mode*, user profile includes option to generate a temporary password. If you click **Reset User Password**, a new temporary password for the user will be generated. When new user first logged on to RiskyProject, the temporary password will be required. After this the user will be prompted to change the password.

If your Administrator enters the user's email in User Profile Dialog and configures email notifications (see *Notification Messages of RiskyProject Enterprise User Guide* for more information), the temporary password will be sent to you automatically. If an e-mail is not defining or sending email is not configured, the Administrator can copy temporary password from the subsequent dialog and provide it to user by other means.

The passwords can be recovered via email if the user clicks on **Forgot Password** in Logon Dialog. Therefore it is important to define correct email and configure sending email.

If you use *Windows and RiskyProject authentication mode* the User Profile dialog will not have option to reset user passwords. In this mode, users are logged on based based on their Windows credentials.

Switching Between Authentication Modes

In RiskyProject you may have different user authentication using different modes. For example, user John will have Windows authentication and user Jack will have RiskyProject authentication. Authentication modes are defined in the **Users and Org. Structure** tab of **User Management** dialog box.

You can switch between two authentication methods using **License and Security** tab of **User Management** dialog.

- If you switch from Windows and RiskyProject authentication to RiskyProject authentication you must have at least one administrator with RiskyProject authentication. After the switch only users with RiskyProject authentication mode can log on to RiskyProject.
- If you switch from RiskyProject authentication to Windows and RiskyProject authentication, your organizational breakdown structure defined with RiskyProject authentication will be augmented with users, security groups, and organizational units from Windows directory.

In both cases, switching from one authentication mode to another, any previously defined organization structures and users will be preserved.

About Project Permissions

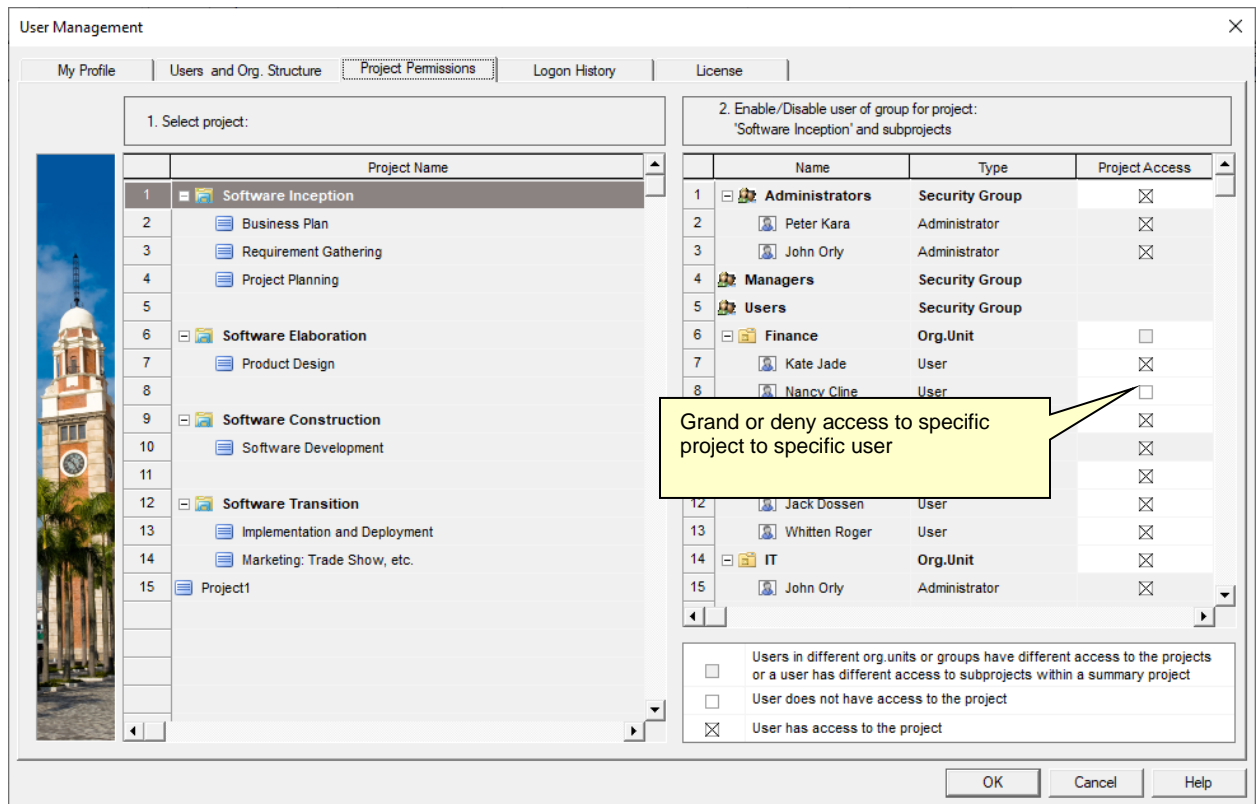
You can control access to projects using project permission. Project permissions either allow or deny users access to projects in your Portfolio. If you give access to a user (Manager or User), they will have complete access to the specified project(s) given the permissions they have been granted. User project permissions granted to a program (summary project) overwrite project permissions to all of its projects.

Adding Project Permissions to a user

You must be an administrator to add or modify project permissions.

To add project permissions to a user:

1. From the **File** menu, click **Users**. The **User Management** panel opens.
2. Click the **Project Permissions** tab.
3. In the **Project Name** pane on the left, select the project to which you want to provide or modify permissions. On the right is a table of organizational units and security groups.
4. From the list on the right, select the check box associated with the users or organizational units to which you want to grant permission to the selected project. You can deny user access by clearing the check boxes.
5. Click **OK** or switch to another tab.





- The project permission tab is not shown if the database does not have any projects. This may occur if you just created a database.
 - If you grant or deny permissions to certain users on a summary project, the permissions will be propagated down the project hierarchy to all sub-projects.
-

About the Logon History

The Logon History allows the Administrator to view the entire logon history of all the system users. The history includes:

- User Name
- Role
- Logon Time
- Log off Time
- Computer ID; computer ID is shown in RiskyProject About dialog (question mark at the right upper corner of RiskyProject window)
- License Type: RiskyProject Professional, Lite or Risk Register.
- Number of users currently logged on
- Number of rolling months that logon history will be kept.

To access logon history:

1. From the **File** menu, click **Users**. The **User Management** panel opens.
2. Click the **Logon History** tab.

Delete all open sessions

As an administrator, you can remove logon sessions that are currently open from the list. This can be useful if the user “killed” the application without properly exiting it. If you use the concurrent user licensing model, it would limit the number of concurrent sessions and users may not be able to logon to RiskyProject.

To delete open sessions, click **Delete** all open sessions.

Set the number of months logon records are kept

Depending on the number of users you have, you may want to keep the history at a manageable size.

To set this period, type in the number of months in the months box and click **OK**.

Delete sessions from the list:

1. Select the sessions you want to delete.
2. Click the **Delete selected sessions** button.

Updating RiskyProject Enterprise License

You may update RiskyProject Enterprise license information:

- type of users (concurrent or named users)
- maximum number of users
- license duration

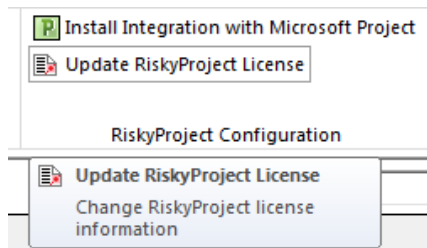
You would need to obtain a RiskyProject license file (RiskyProject.lic) from Intaver Institute Inc. Only an Administrator has to capacity to update license information.

To update RiskyProject Enterprise license information:

1. From the **File** menu, click **Users**. The **User Management** panel opens.
2. Click the **License and Security** tab.
3. Click on **Browse** and locate new RiskyProject.lic file.
4. Click **OK** or switch to another tab.

Switching Between Enterprise and Standalone Desktop Configurations

You may switch between Enterprise and Standalone desktop configurations of RiskyProject and vice versa at any moment. To do it use the **Update RiskyProject License** button on the Tools pane of the toolbar.



1. If you switch from **Enterprise** configuration to **standalone desktop** configuration you must have a license of RiskyProject standalone on your computer. If Enterprise configuration is saved in the database, the standalone license is saved in the Windows registry. You would need a license number, which is provided by Intaver Institute Inc.
2. If you switch from standalone desktop configuration to enterprise configuration, you need to define database connection properties in the manner described in *Chapter 2: RiskyProject Enterprise Installation*.
3. If you are in Enterprise mode, you may want to connect to a different database. Click on **Update RiskyProject License** and select **Enterprise: update database parameters**. You will be prompted to define database connection properties.



- You may switch from Enterprise configuration to standalone desktop configuration by clicking on Start regular desktop license (no database) with the RiskyProject Enterprise logon dialog.
- If the database connection is not available and your current configuration is Enterprise, you will be prompted to define database connection properties.
- Your database connection properties are saved in the system registry:
Computer\HKEY_CURRENT_USER\Software\Intaver\RiskyProject Pro x.x

If this registry entry is deleted or updated, you may be prompted to define database connection properties again.

Connecting to a Different Database

You may connect RiskyProject Enterprise to a different database. To do so:

1. Click on the **Update RiskyProject License** button on the Tools pane of the toolbar.
2. Select Enterprise: Update database parameters
3. Restart RiskyProject.
4. Define database connection properties in the manner described in *Chapter 2: RiskyProject Enterprise Installation*.

Other RiskyProject Configuration Steps

RiskyProject configuration consists of the following steps:

1. Configure users using File->Users...
2. Define enterprise options using Project->Options, such calendar options, calculation options, default risk options, and others
3. Format the Risk Matrix using **Risks->Format Risk Matrix** or right click on Risk Matrix and choose **Format Risk Matrix**.
4. Format the Risk Trend view: right click on **Risk Trend** chart and select **Format Risk Matrix**.
5. Define risk properties using Risks-> Define Risk Properties
6. Define risk categories using Risks-> Risk Categories
7. Customize reports using:
 - Risks ->Risk Report -> Customize...
 - Risks->Risk Dashboard->Dashboard Settings...
 - Report->Statistics Report->Customize...
 - Report->Task Report->Customize...
 - Report->Report: All Risks->Customize...
 - Report->Project Dashboard->Dashboard Settings...

All steps except for user configuration are described in the RiskyProject User Manual.

For enterprise configuration all these settings and options are saved in the database. These settings are common for all projects within a portfolio. The exception is Project Options. Project Options and portfolio options can be different. Once a project is created and imported, it is possible to define individual options for each project using Schedule->Options. However, the system administrator may deny users the ability to define options for individual projects using the settings on Project->Option.



Resources and calendars are defined on the project level and cannot be automatically shared within a portfolio.

Configuring Integration with Proteus Envision®

RiskyProject Enterprise is integrated with Proteus Envision by SNA Software. To configure integration with the Proteus Envision:

1. Go to **Projects** tab
2. Click on **Preferences**
3. Click on **Envision Database Connection Settings**
4. Define database connection properties in the manner described in *Chapter 2: RiskyProject Enterprise Installation*.

Notification Messages

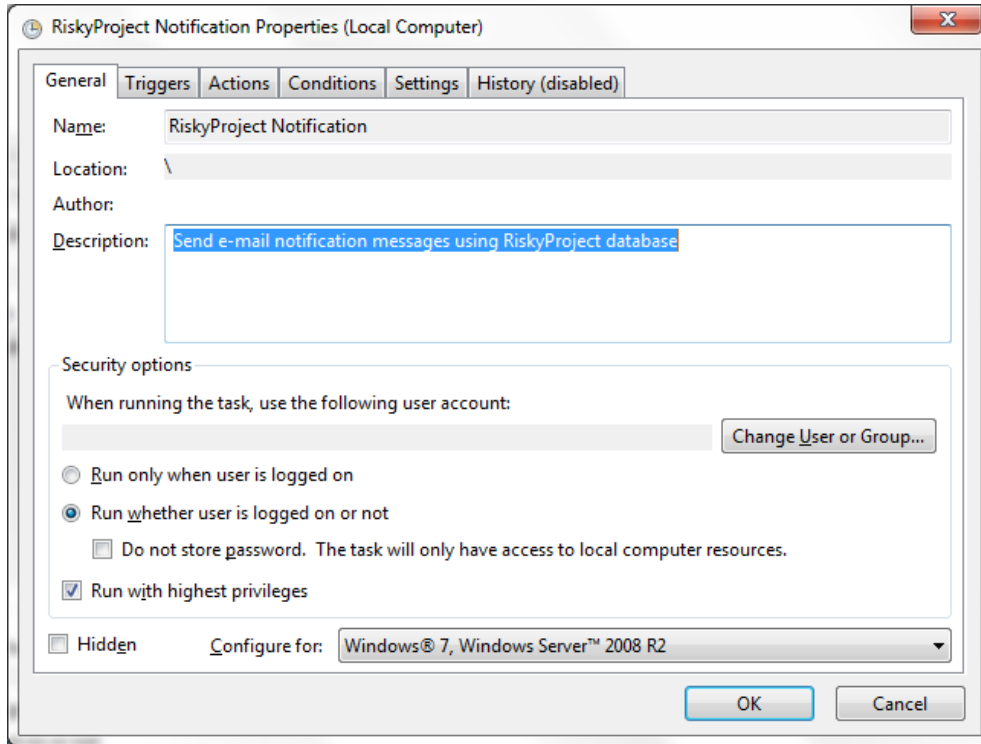
RiskyProject supports sending notification messages to its users via e-mail. RiskyProject can be executed using Windows Task Scheduler every 5 – 15 minutes without preventing user interface and send out notification e-mails. Notifications can be configured using Notification Manager. Notification Manager is accessible from **Tools -> Notification Manager** or from **File -> User Management -> License and Security Tab -> Notification Manager**. After notifications are configured, RiskyProject can read data from notification messages from the RiskyProject database and send them. For more information about notification please read *Notification Messages* in *RiskyProject Enterprise User Guide*.

Using Windows Task Scheduler for Sending Notification Messages

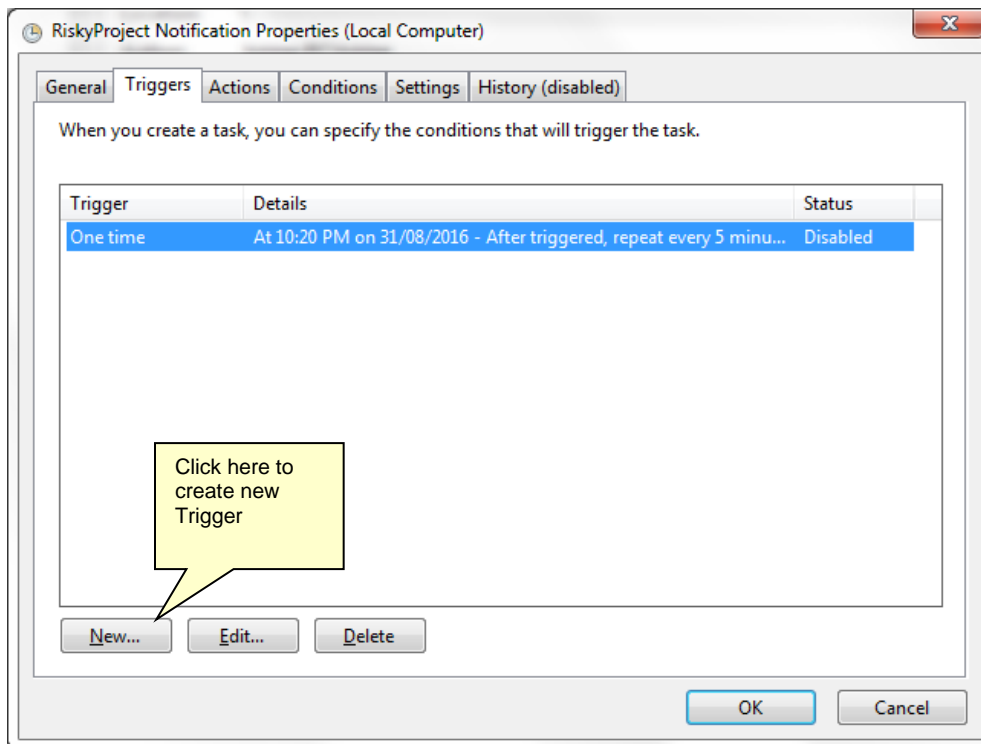
To execute RiskyProject using Windows Task Scheduler for notification messages it is recommended to install RiskyProject Professional, Lite, or Risk Register on the server. This installation can be done exactly the same way as on a client's computer. A dedicated user can be created to execute RiskyProject for notification messages. The user name and password for RiskyProject installed on the server will be encrypted and saved in the registry. When RiskyProject is executed by the Task Scheduler, no interface will be prevented and user name and password will not be asked.

To configure Task Scheduler for notification messages:

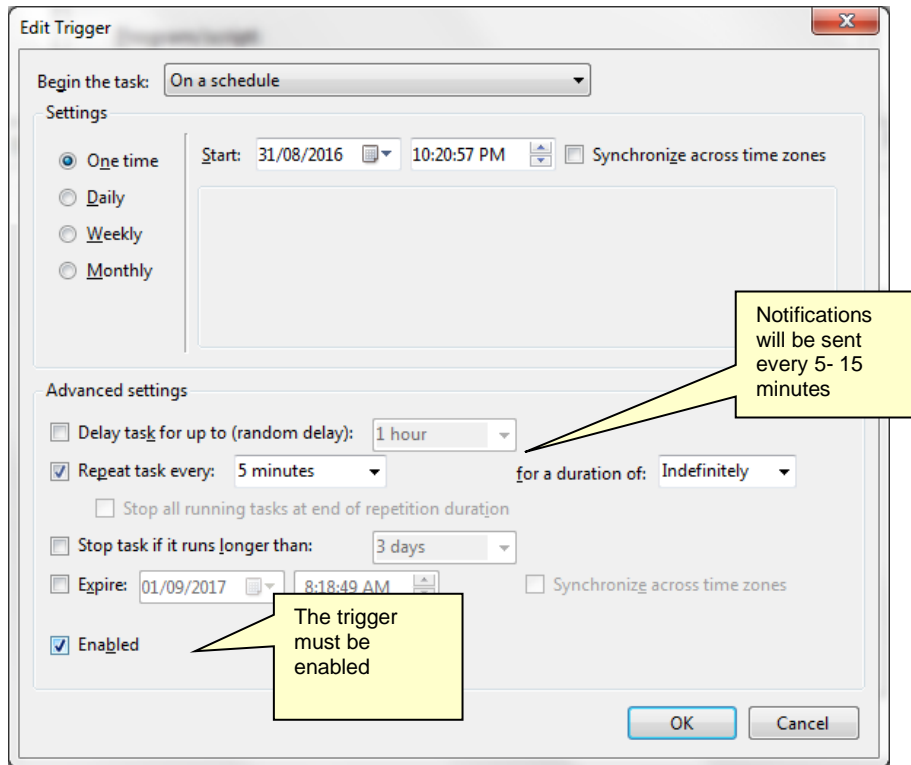
1. Start **Task Scheduler**. Task Scheduler can be found by clicking on the Windows Start button and typing "Task Scheduler" in the Search box.
2. Go to Console Tree (left pane) and click on **Task Scheduler Library**. If Console Tree is not displayed, use "Show/Hide Console Tree" button in toolbar to show Console Tree.
3. Right click on central pane, which includes a list of scheduled tasks. Select **Create New Task...** Properties dialog comes up.
4. Go to **General** tab. Enter task name, e.g. "RiskyProject Notification" and description, e.g. "Send e-mail notifications". We recommend checking RiskyProject Notification "Run whether user is logged on or not".



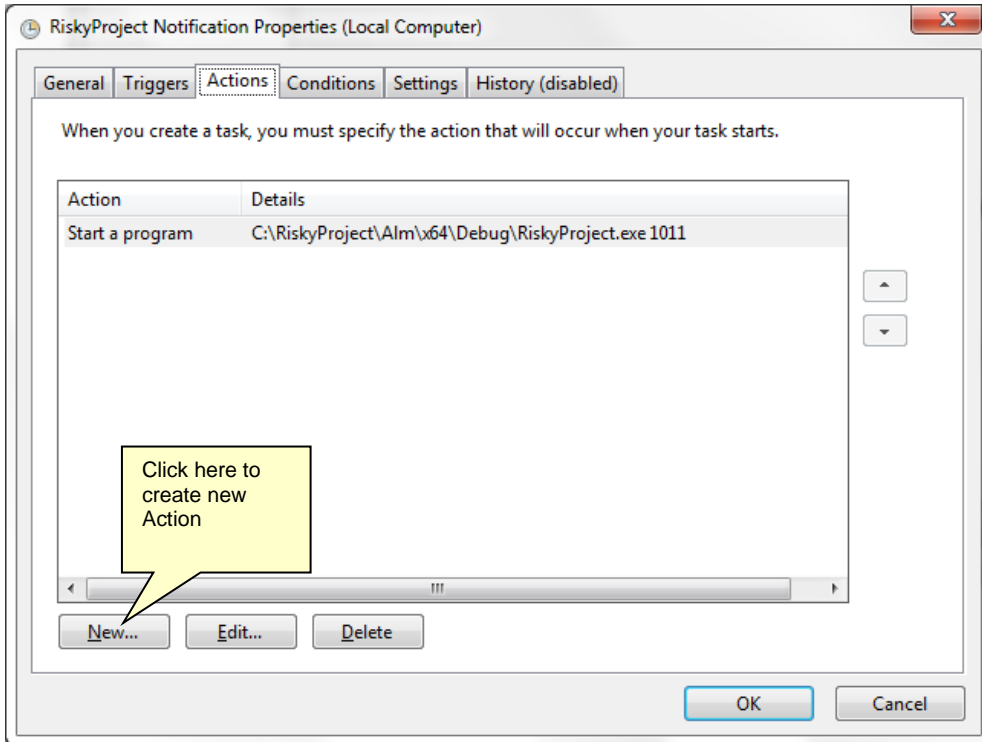
5. Go to **Triggers** tab and create a new trigger by clicking on the New button at the bottom of the dialog.



- In Edit Trigger dialog enter Trigger properties. The task may start at the current time and then be repeated every 5-15 minutes for the duration of "Indefinitely". To enable this trigger check the Enabled checkbox at the bottom of the dialog.



- Go to the Action tab and click on the New button at the bottom of the dialog. The Edit Action dialog will come up.



8. In the Edit Action dialog click Browse, click on Browse button and select RiskyProject.exe from your RiskyProject directory.
9. Enter argument 1011.

