

Install Guide

for

Safran Risk v25.1.00

(Last update: March 3 2026)

Accuracy

Rest assured, every effort has been made to ensure the accuracy and completeness of this document. However, no warranty, expressed or implied, is made by Safran Software Solutions as to the accuracy of this publication and the features or the applicability of the techniques suggested.

Copyright Notice

The information provided in this manual is for informational purposes only. It may be changed without notice and does not represent a commitment to merchantability or fitness for a particular purpose by Safran Software Solutions. Safran Software Solutions provides the software described in this manual under a Safran License Agreement. The software may be used only by the terms of the license agreement. This software and its associated documentation are protected by copyright law. Unauthorized use, reproduction, or distribution of this software, including the use of AI tools to copy, reproduce, re-engineer, or train on any part of this software or documentation, is strictly prohibited and may result in severe civil and criminal penalties.

Safran is a registered trademark of Safran Software Solutions. Safran Project, Safran Details, Safran Details Developer, Safran Enterprise Developer, Safran Planner, Safran for the Microsoft Project Platform, Safran for Microsoft Project, Safran Web Access, Safran Project Viewer, Safran Risk, Safran Risk Manager, Safran Project Integration API, Safran Project ILAP Gateway API, Safran Project Data Reporting Utility, and Working Smarter are trademarks of Safran Software Solutions. All other brands and product names are trademarks, or registered trademarks are property of their respective holders. **Safran** is a registered trademark of Safran Software Solutions AS.

All other trademarks are property of their respective holders.

Introduction

The purpose of the *Safran Risk Install Guide* is to familiarise you with the process of installing Safran Risk and the structure of Safran Risk folders and file structure.

This guide is written to assist support personnel, application developers, and system integrators.

Contents

1.	Installation.....	5
1.1.	General.....	5
1.2.	Requirements.....	5
1.2.1.	Client configuration:	5
1.2.2.	Database server configuration.....	5
1.2.3.	Database User authentication	6
1.2.4.	External Communication	7
1.2.5.	Administrative privileges:	7
1.3.	Support for other Safran software products.....	7
1.4.	Installing Safran Risk with local database	7
1.5.	Installing Safran Risk – Using a MS SQL Server Database	13
1.6.	Silent Install and Uninstall.....	19
2.	Activation of Safran Risk.....	21
2.1.	Add a license key to activate Safran Risk.....	21
2.2.	Presetting the license key on a user’s machine.....	23
2.3.	Offline period.....	23
2.4.	Offline activation.....	23
3.	Administering a multi-user shared database	29
3.1.	Setting up the database.....	29
3.2.	Upgrading the database	33
3.3.	Microsoft Entra Authentication.....	34
3.3.1.	Via Entra user.....	34
3.3.2.	Via Alias user	35
3.3.3.	Via an App Registration	36
4.	Using the Safran System Administrator tool.....	43
4.1.	Starting Safran System Administration.....	43
4.2.	Safran System Administration Window	45
4.3.	Users and security.....	46
4.4.	Safran Users	47

4.5.	Safran User Groups.....	47
4.6.	User Access Object Type.....	48
4.6.1.	Window Access Restrictions	49
4.7.	Defining and maintaining users.....	50
4.7.1.	Adding a new Safran user	51
4.7.2.	Deleting a Safran user	52
4.7.3.	Create a New Safran User Group.....	52
4.7.4.	Adding a User to a Group.....	53
4.7.5.	Remove a User from a Group	54
4.7.6.	Object Ownership	55
4.7.7.	Transferring ownership.....	55
4.7.8.	Restricting Access to a Window.....	56
4.8.	Activate cleaning of invalid locks in the database.....	58
4.9.	Managing the license.....	58
4.10.	Managing the Safran Database.....	58
4.10.1.	Initiating a New Safran Database.....	59
4.10.2.	Upgrade an existing Safran Database to latest version	59
4.11.	Database Utilities	59
4.12.	Execute SQL Queries.....	59
4.13.	Run SQL Command files.....	61
4.14.	See all current Safran users (MS SQL Server only).....	64
4.15.	Update Database Statistics.....	64
4.16.	Rebuild Indexes	65
4.17.	Removing database duplicates.....	66
4.18.	Remove trailing blank characters	68
4.19.	Delete Log.....	69
5.	Troubleshooting.....	71
6.	Contact Safran Software Solutions AS.....	74

1. Installation

1.1. General

Safran Risk installation is a basic msi installation created with InstallShield. This guide performs a normal set up with the executable file but informs you were to pick up the clean msi-package.

1.2. Requirements

1.2.1. Client configuration:

	Recommended	Minimum
Operating systems	Windows 11 64bit	Windows 10 64bit
Processor	3Ghz or higher	2Ghz
Memory (RAM)	32GB	16GB
Free disk space after local installation	100GB	10GB
Microsoft .Net	8	8

- Microsoft OLE DB Driver for SQL Server (64bit) is required for connecting to a Microsoft SQL Database

The users' temp folder (C:\Users\\AppData\Roaming\Safran\temp) is extensively used by Safran Risk. The temp folder should be kept locally for best performance. (E.g. If you install Safran Risk in a terminal server environment, the temporary folder should be placed as near to the Safran Risk client as possible.)

1.2.2. Database server configuration

The following database management systems are now supported:

- MS SQL Server 2017, 2019 and 2022 (Compatibility level needs to be 140 or higher)

- MS SQL Server 2022 LocalDB(x64) (Included in installation package).
- Azure SQL (only using sql authentication)
- Azure SQL Managed Instance

On the database server, the performance will be influenced by processing speed and how much RAM is available for the database service. The rule of thumb here is you need more RAM and higher processing speeds if you have many users working on the same database at the same time. The same is true if there are many or large projects that carry a large amount of information. Available free space on the database is also important. We recommend that if you configure the database to expand if it is close to filled, make it expand by at least 20% at a time.

1.2.3. Database User authentication

Authentication to Safran Risk is achieved via database authentication. In other words each Safran Risk user must be associated with a database login.

These are the authentication methods that are supported for the different databases.

	SQL Server Authentication	Windows Authentication	Microsoft Entra Authenticaction
MS SQL Server 2017, 2019 and 2022	Yes	Yes	Yes
MS SQL Server 2022 LocalDB(x64)	Yes	Yes	No
Azure SQL	Yes	No	Yes
Azure SQL Managed Instance	Yes	Yes (if synced with Microsoft Entra)	Yes

If you're planning to use Azure SQL managed instance with Windows authentication, this is a good starting point:

<https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/winauth-azuread-setup?view=azuresql>

1.2.4. External Communication

Safran Risk needs to communicate with the database and the license server.

Database: The database will be a sql server database. If the database resides on a different machine from where Safran Risk is installed it's necessary to make sure that the communication ports are open. This is done by making sure that the MS Sql Server Port is open on the server. This port is normally 1433 but can be changed on the server side. The Safran Risk client supports TLS 1.2 for database communication.

License server: To allow Safran Risk to validate the license it need to access port 443 at api.licensing.safran.com.

This can be avoided by using offline activation. Remember that offline activation is much more cumbersome and should be avoided if at all possible.

1.2.5. Administrative privileges:

The installation must be done with Admin rights on the client computer.

1.3. Support for other Safran software products

If Safran Risk is sharing the database with Safran Project, you need to make sure that Safran Project is of the same version as Safran Risk, or at least uses the same version of the database as Safran Risk.

1.4. Installing Safran Risk with local database

Safran Risk uses InstallShield from Flexera Software for automatic software distribution and installation.

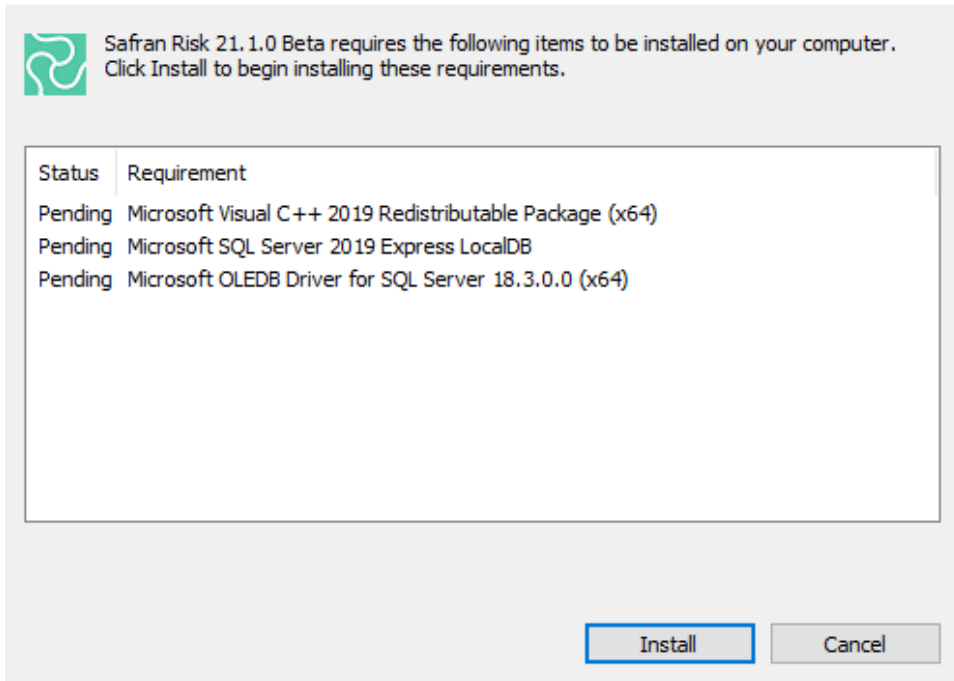
Follow these instructions if you are installing a copy of the Safran Risk software.

To install:

1. Open Windows Explorer and browse for the Safran installation files

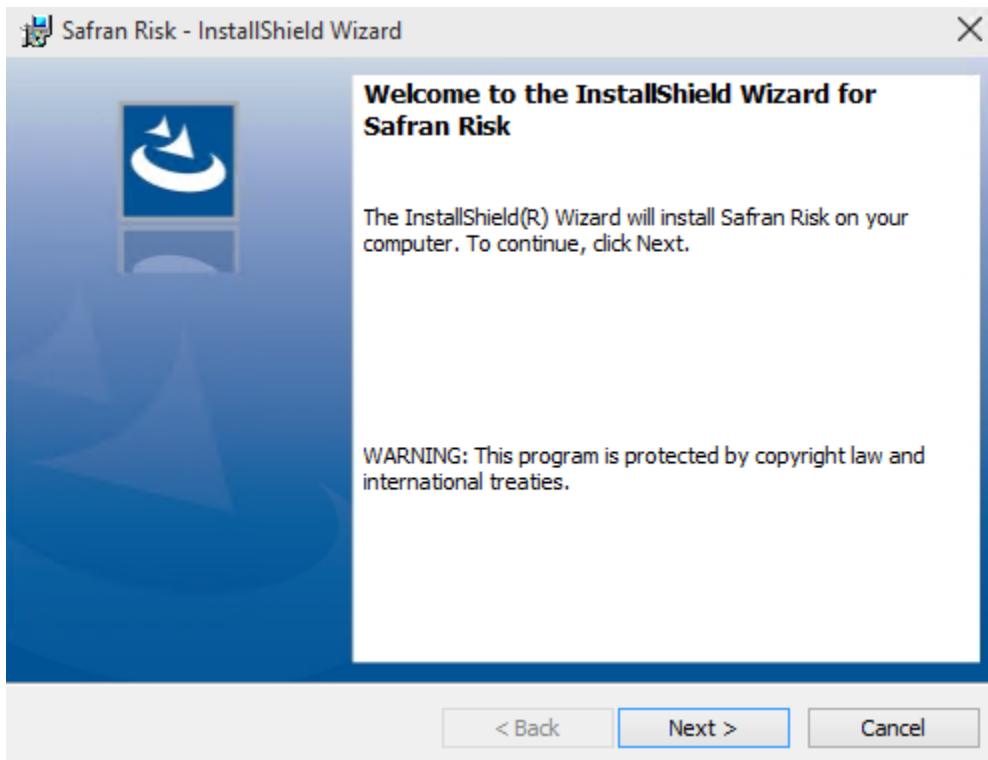
2. Run the installation file
3. The installation checks if you have Microsoft OLE DB Driver for SQL Server, Microsoft Visual C++ 2019 Redistributable Package and MS SQL Server 2022 Express LocalDB installed. If they are not click Install

Safran Risk 21.1.0 Beta - InstallShield Wizard

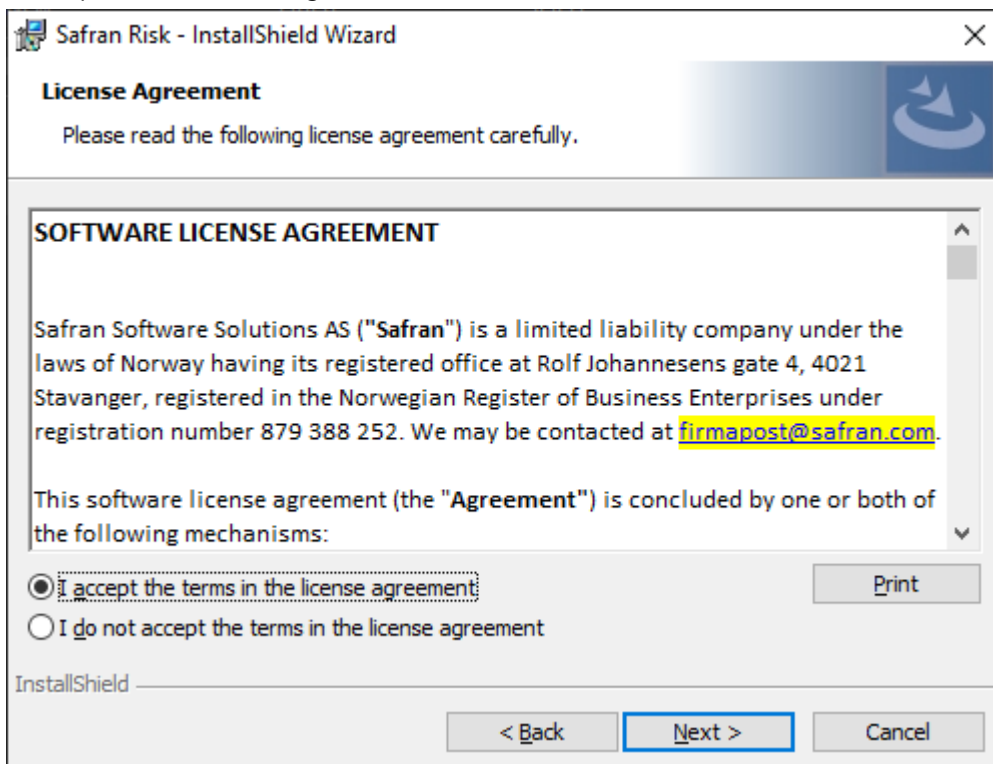


4. Click Next to start installing Safran Risk

NOTE: During the installation of SQL Server the machine may reboot itself before continuing the installation, this is a normal part of the SQL Server installation. The Safran Risk installation will continue within a short while of the machine being restarted.

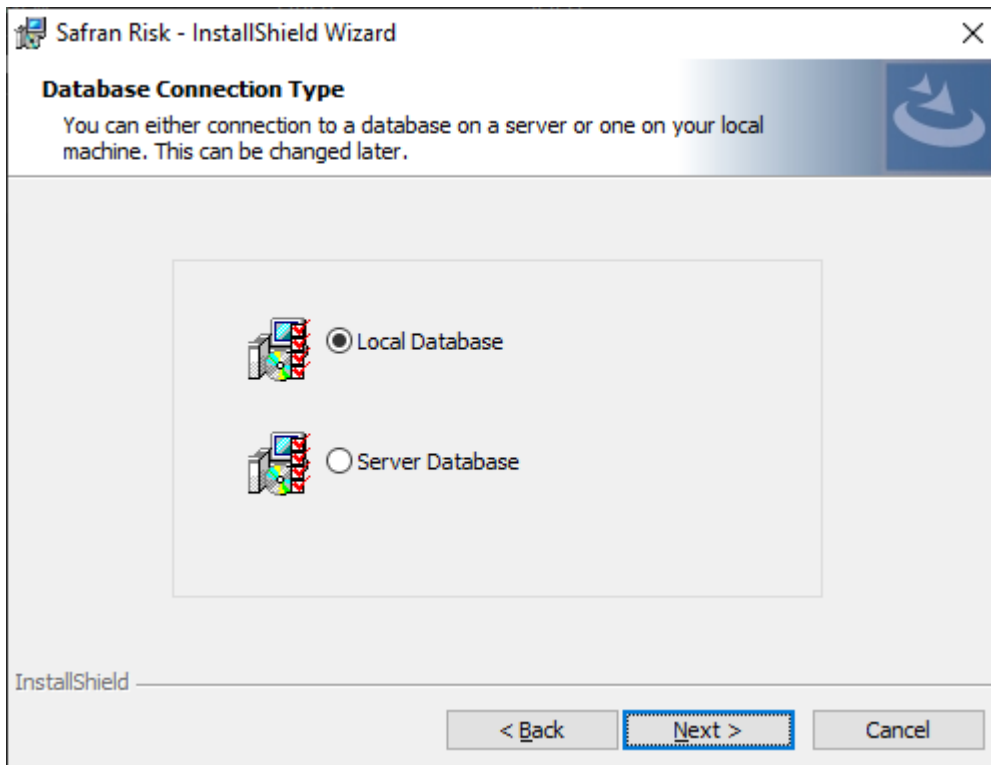


5. Accept the license agreement and click Next



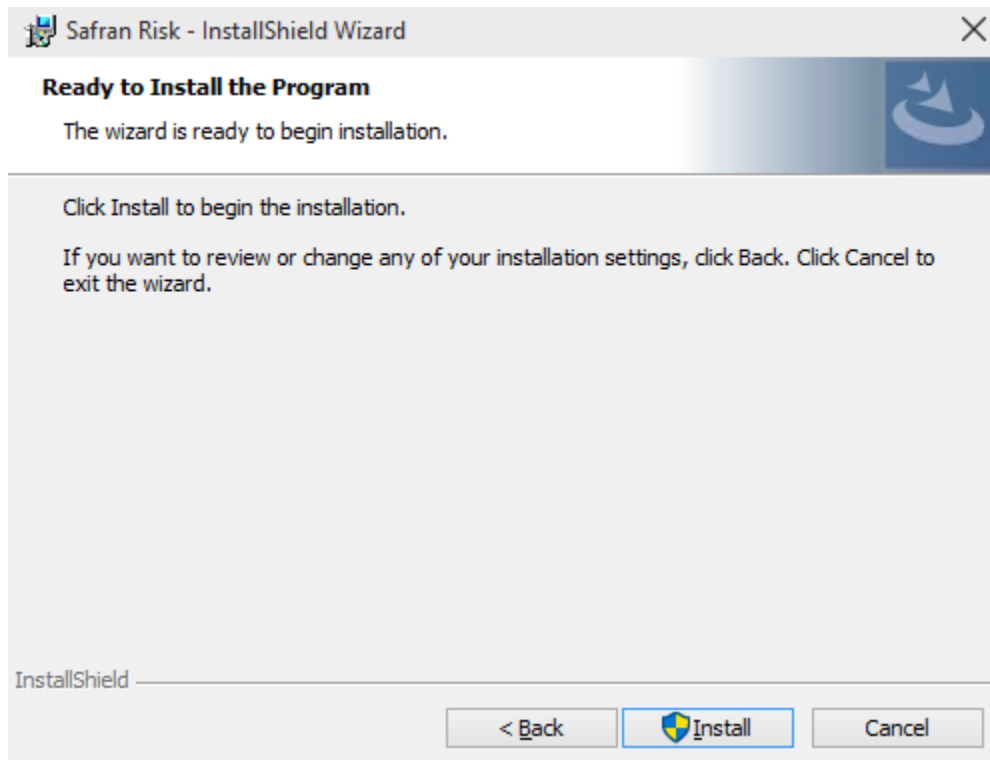
6. Choose if you want to use a Local Database (if not existing it will be created when Safran Risk is started for the first time), or if you want to connect to a

database on a sever (Server Database). Note that this connection can also be done later once Safran Risk has been installed. The setting chosen here will however be the default for the installation.

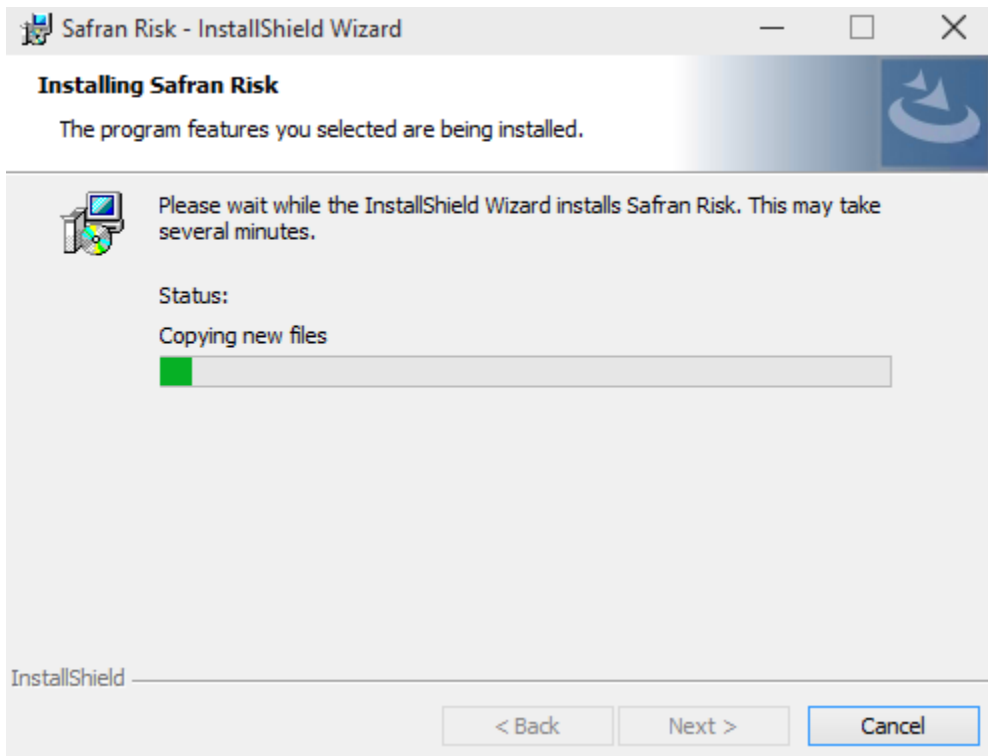


If you want to deploy Safran Risk with an msi package, you need to browse to "C:\Users\YOURACCOUNT\AppData\Local\Temp" In one of the folders with a cryptic numeric name, and todays date, you will find Safran Risk.msi file. Copy and paste this file to a location for further packaging.

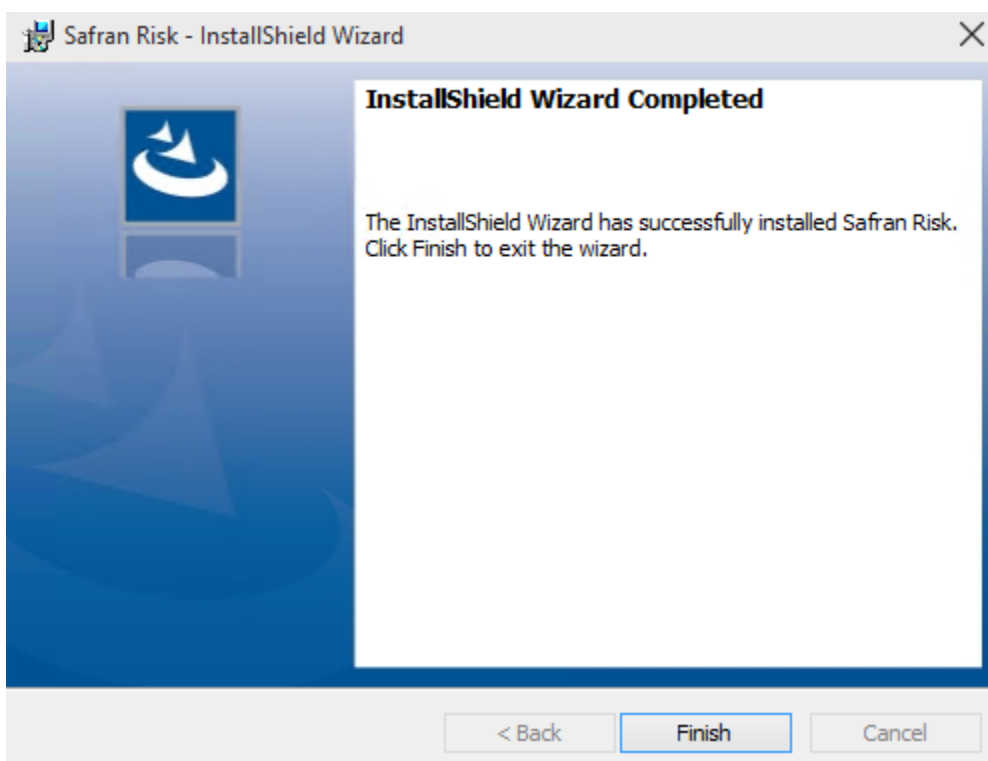
7. Click Install or follow instructions.



8. Safran Risk installs.



9. When complete, click Finish



1.5. Installing Safran Risk – Using a MS SQL Server Database

Follow these instructions if you are installing a copy of the Safran Risk software when you want Safran Risk to use a Microsoft SQL Server Database.

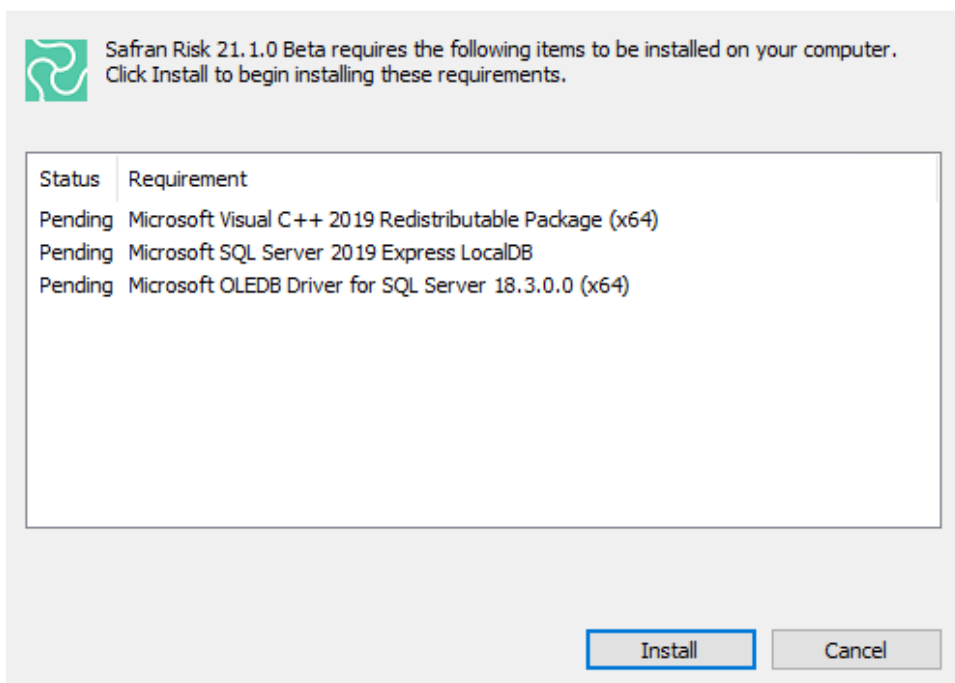
Pre-requisites:

1. An empty SQL Server database must be created for the installation to connect to

To install:

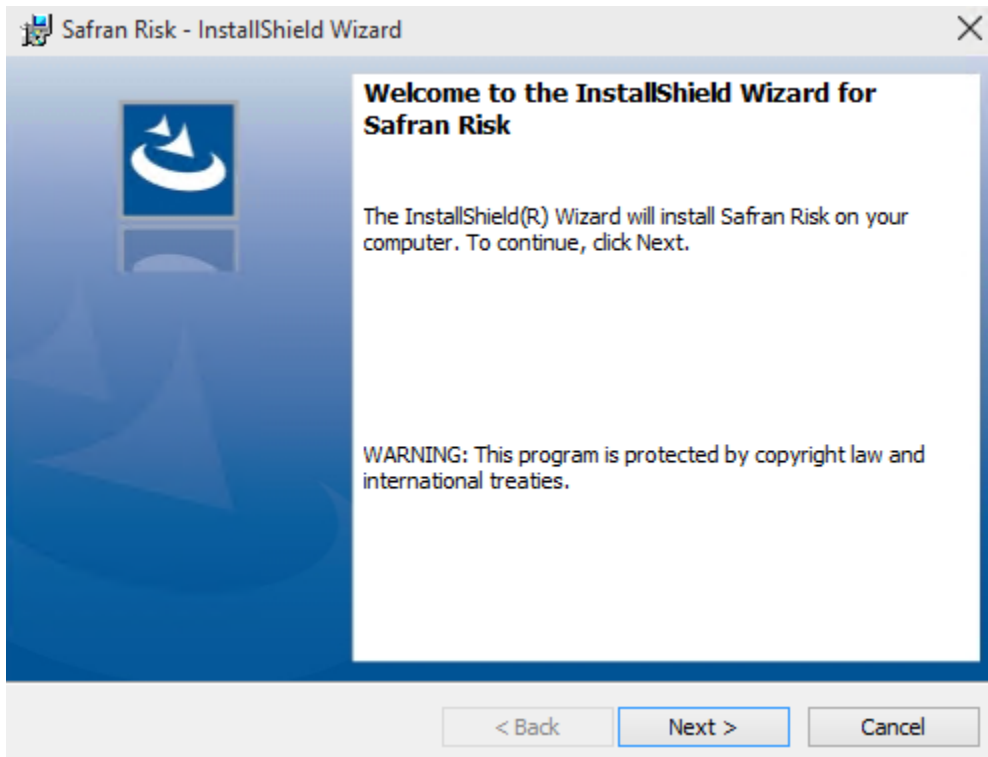
1. Open Windows Explorer and browse for the Safran installation files
2. Run the installation file
3. The installation checks if you have MS OLEDB Driver for SQL Server, MS Visual C++ 2019 Redistributable package and MS SQL 2022 Express LocalDB installed. If they are not click Install

Safran Risk 21.1.0 Beta - InstallShield Wizard

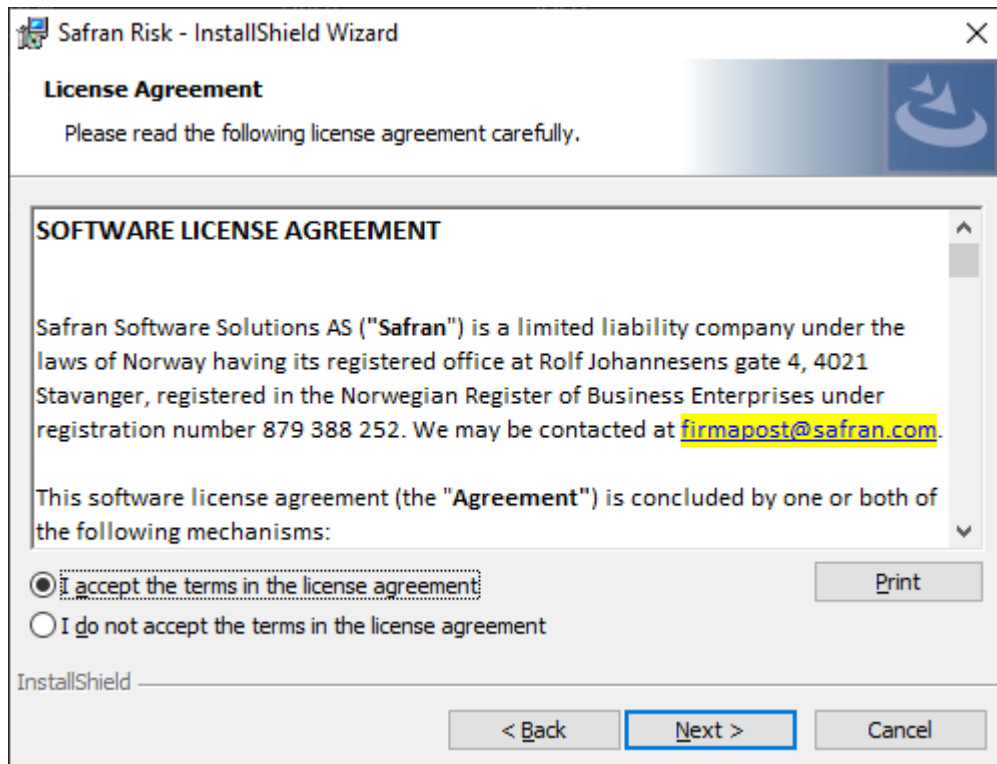


4. Click Next to start installing Safran Risk

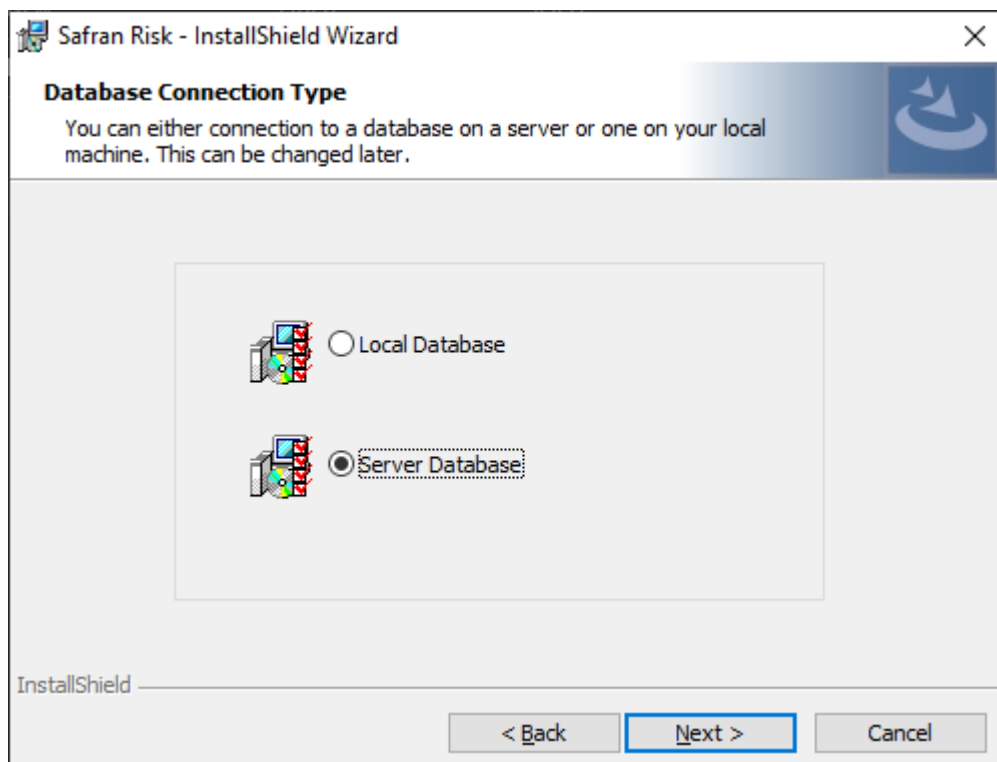
NOTE: During the installation of SQL Server the machine may reboot itself before continuing the installation, this is a normal part of the SQL Server installation. The Safran Risk installation will continue within a short while of the machine being restarted.



5. Accept the license agreement and click Next



6. Select Server Database.

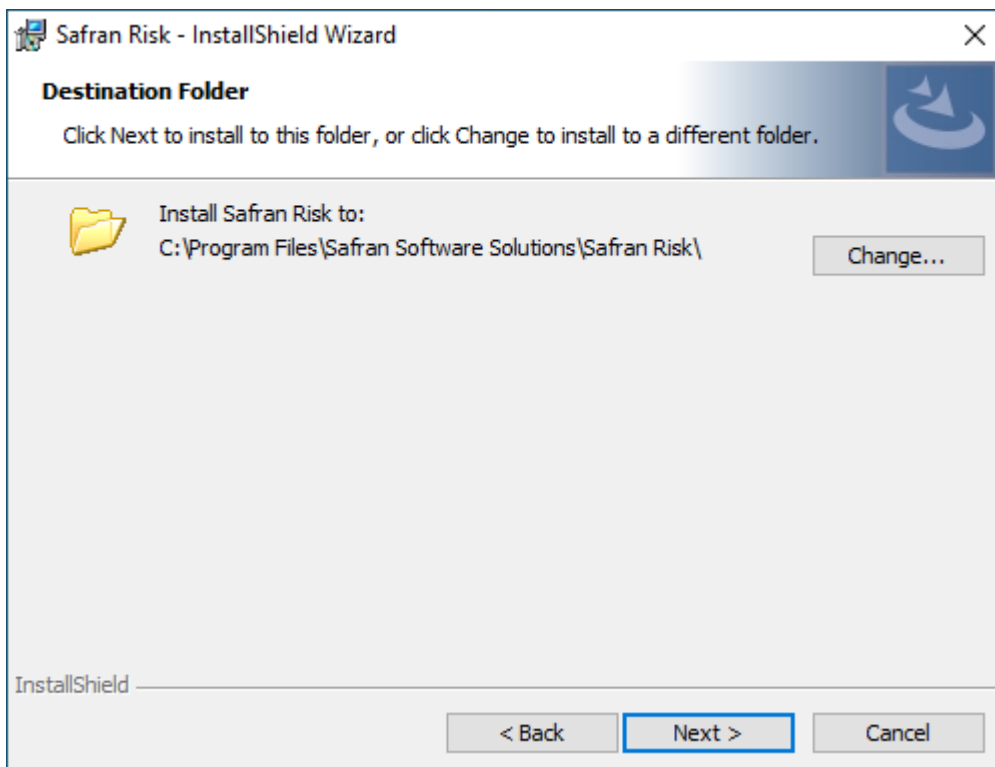


If you want to deploy Safran Risk with an msi package, you need to browse to

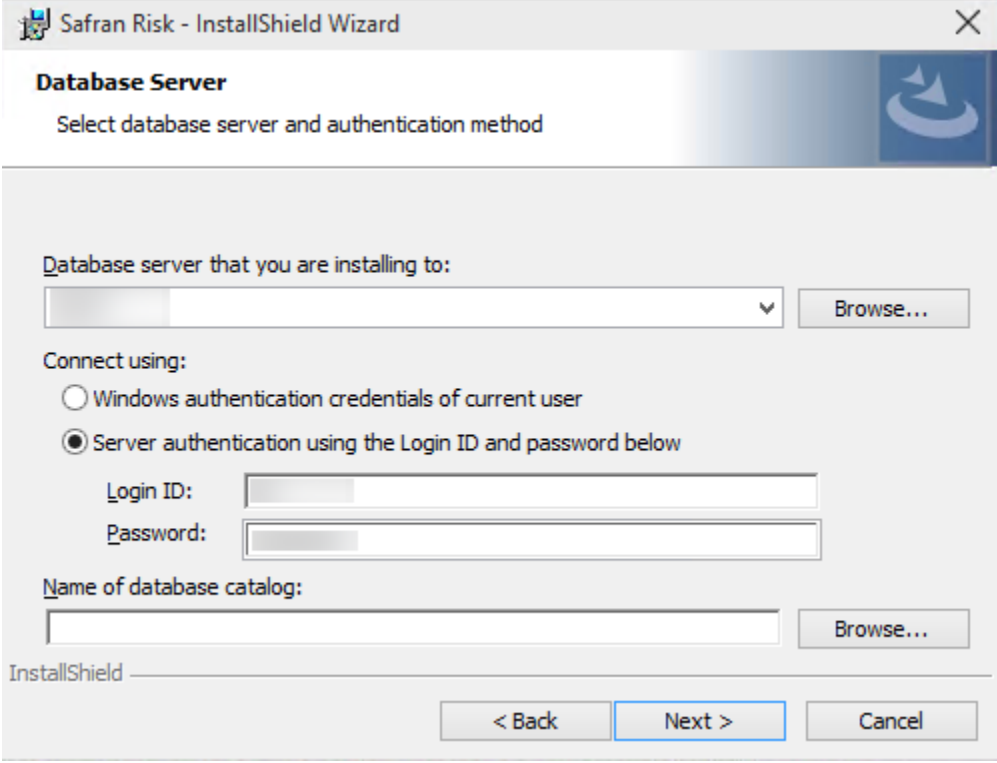
"C:\Users\YOURACCOUNT\AppData\Local\Temp"

In one of the folders with a cryptic numeric name, and today's date, you will find Safran Risk.msi file. Copy and paste this file to a location for further packaging.

7. Choose where to install Safran Risk, default is
C:\Program Files\Safran Software Solutions\Safran Risk\
Click Next.



8. Setup the connection to the database server, using the appropriate login details for the database you are going to use and click Next (Note: This must either be an existing empty database, or an existing Safran database of a compatible version)

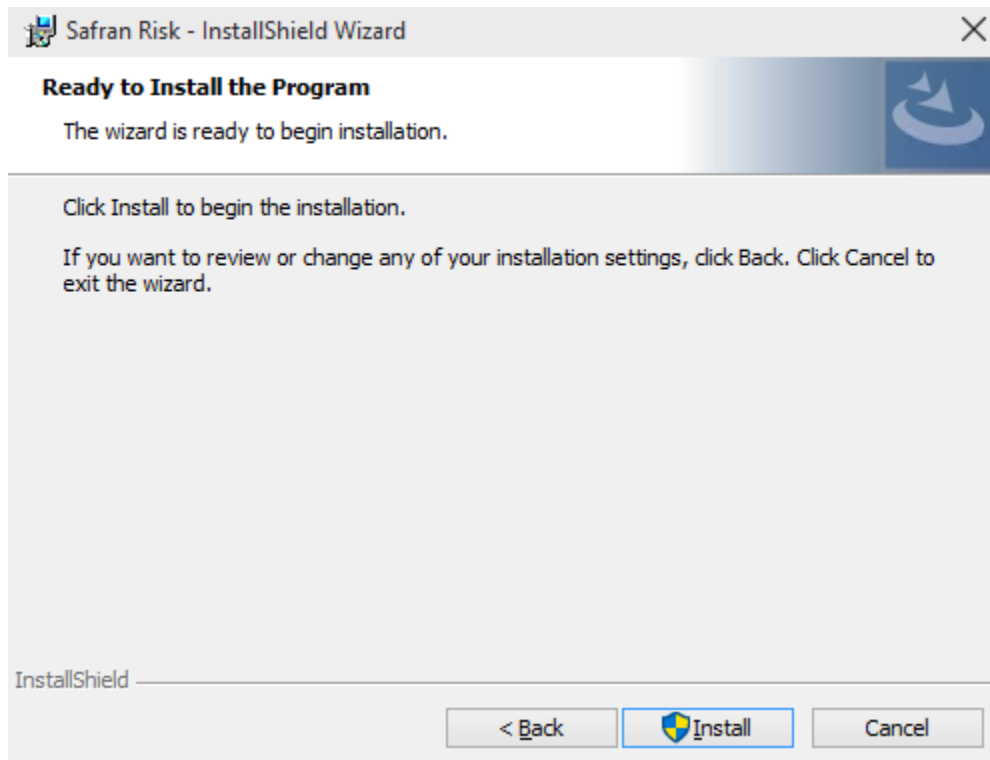


The screenshot shows the 'Database Server' step of the 'Safran Risk - InstallShield Wizard'. The title bar reads 'Safran Risk - InstallShield Wizard'. The main heading is 'Database Server' with the instruction 'Select database server and authentication method'. The dialog contains the following fields and controls:

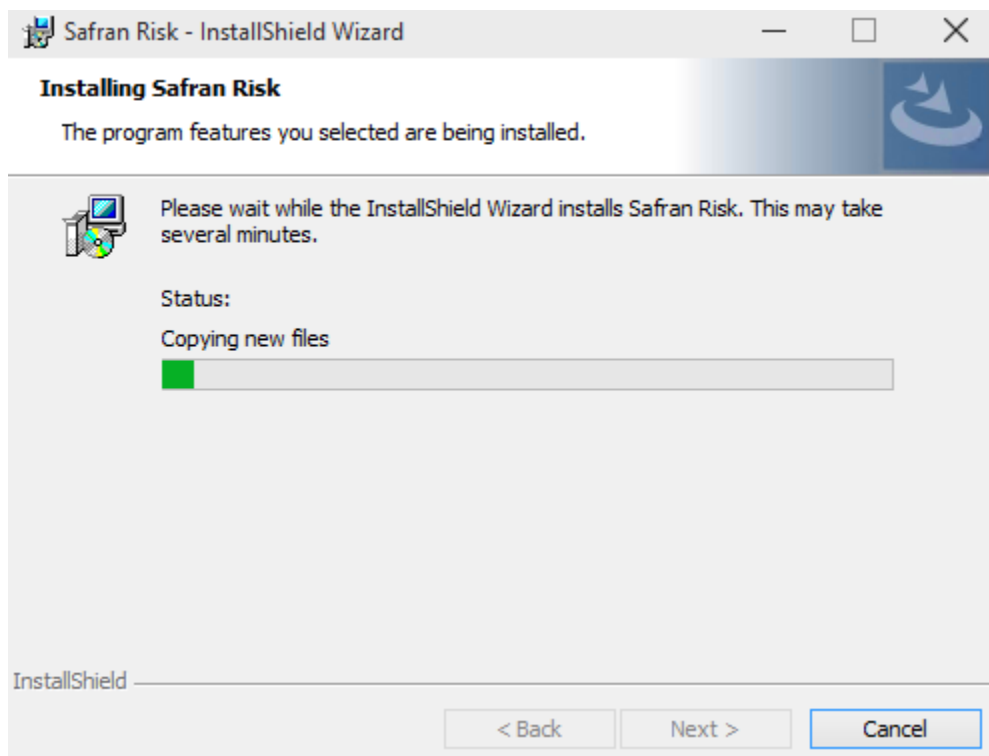
- 'Database server that you are installing to:' with a dropdown menu and a 'Browse...' button.
- 'Connect using:' with two radio buttons:
 - Windows authentication credentials of current user
 - Server authentication using the Login ID and password below
- 'Login ID:' and 'Password:' text boxes.
- 'Name of database catalog:' with a text box and a 'Browse...' button.
- At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Should you need to connect to an azure database using Microsoft Entra authentication this cannot be done in this dialog. You can however change the default login to Microsoft Entra authentication by changing the appsettings.json file after the install. The appsettings.json is located in the installation folder which is normally C:\Program Files\Safran Software Solutions\Safran Risk. For Microsoft Entra authentication the connection string should look like this: "Server=safraansqlserver.database.windows.net; Authentication=Active Directory Interactive; Database=SafranRisk"

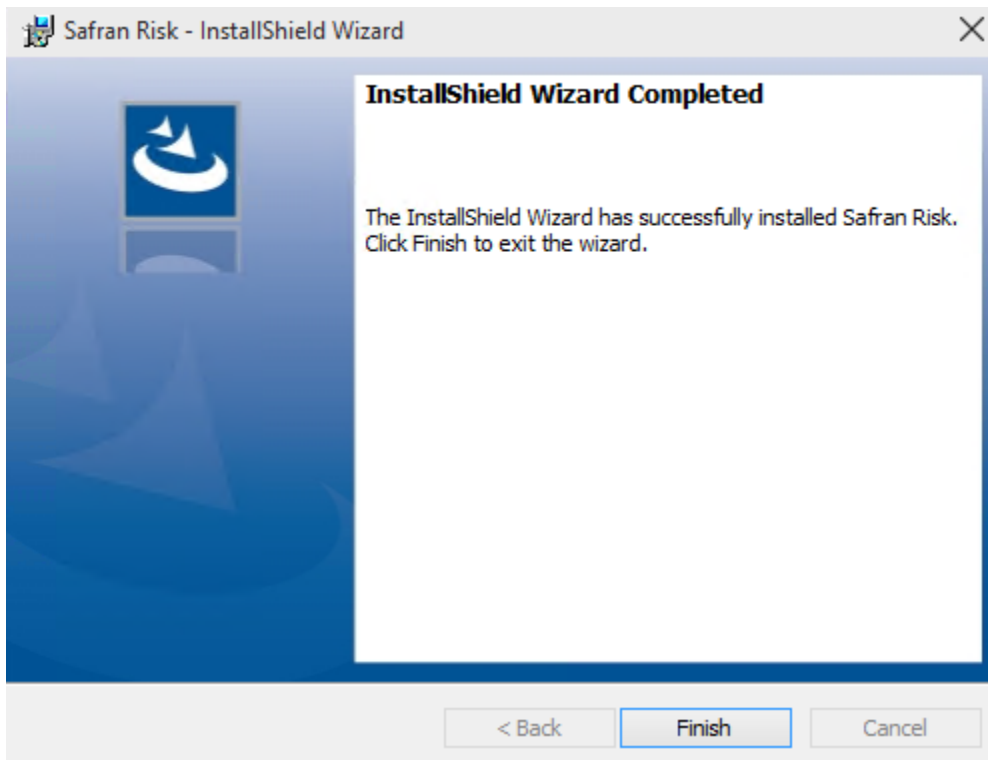
9. Click Install or follow instructions.



10. Safran Risk installs.



11. When complete, click Finish



1.6. Silent Install and Uninstall

It's possible to run the Safran Risk installation silently. This can be achieved by running the installer exe file with a couple of arguments.

The simplest way to do this is:

SafranRisk22.1.1.exe /s /v"/qn"

This will install Safran Risk silently using the default settings i.e. with a Local Database.

To install with the Server Database option you can use the following command line:

SafranRisk22.1.1.exe /s /v"/qn RBGROUP=SDB "

The following properties can be set using a similar command line syntax.

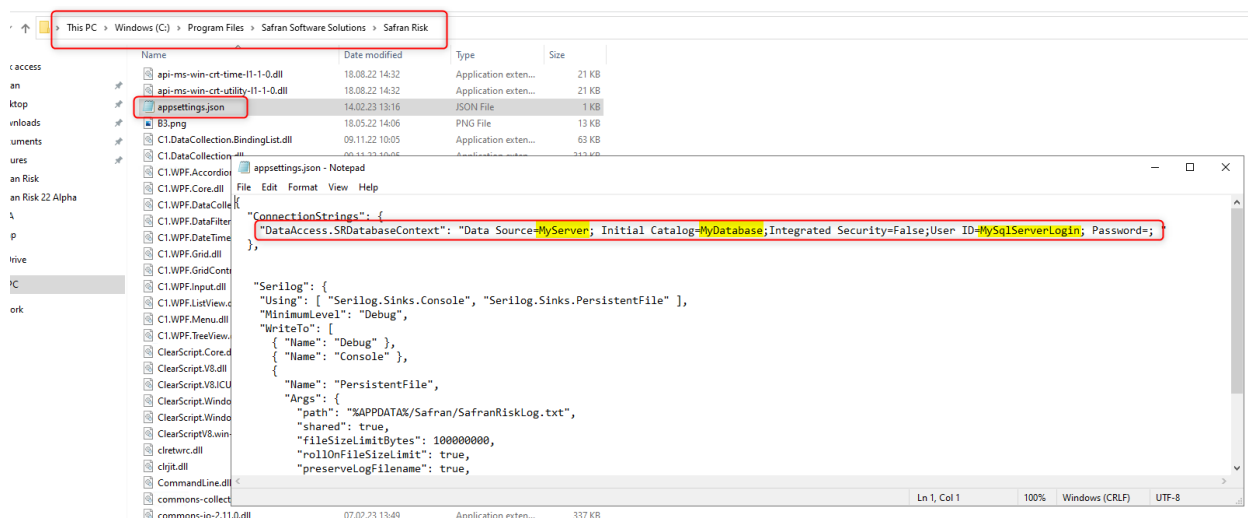
Property	Values
RBGROUP	PDB: Local database SDB: Server Database
IS_SQLSERVER_SERVER	The name of the server

IS_SQLSERVER_AUTHENTICATION	0: Windows Authentication 1: Sql Server Authentication
IS_SQLSERVER_USERNAME	User name for sql server authentication
IS_SQLSERVER_DATABASE	The name of the database catalog

As an example this command line will install Safran Risk with a default database Login to a server database using Sql Server Authentication.

```
SafranRisk22.1.1.exe /s /v"/qn RBGROUP=SDB IS_SQLSERVER_SERVER=MyServer
IS_SQLSERVER_AUTHENTICATION=1 IS_SQLSERVER_USERNAME=MySqlServerLogin
IS_SQLSERVER_DATABASE=MyDatabase"
```

After this install has been run the appsettings.json file in the Safran Risk install directory should have a database connection string looking like this:



Uninstall is achieved with the /x parameter, which can also be used in conjunction with the silent parameters:

```
SafranRisk22.1.1.exe /x /s /v"/qn"
```

2. Activation of Safran Risk

The first time you start Safran Risk you will see a dialog like this:

A screenshot of a Windows-style dialog box titled "Safran". The dialog has a light blue header with the Safran logo and the text "Welcome as a Safran User! Please tell us who you are." Below the header are five text input fields labeled "First Name", "Last Name", "Company", "Email", and "Phone". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Here you are prompted to enter the information that will help the Safran support in case you have any issues in the future. Only the email is a mandatory field. Safran does not strictly require you to enter a valid email, but doing so can be helpful for the Support team.

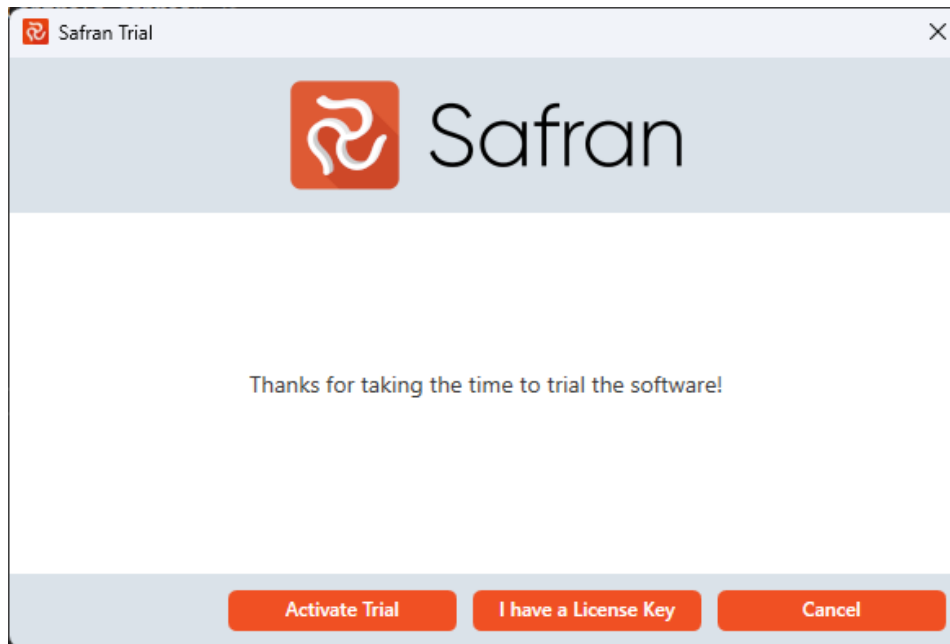
In order to run Safran Risk you need to have a license key. When starting Safran Risk for the first time you get prompted if you want to enter a license key or if you want to continue trial. If you choose to trial Safran Risk you are allowed to do so for 30 days. (The trial version is a full version that includes the cost module) After the trial period ends you need to activate the product with a license key if you want to continue using it.

The license key has a limit to the number of users that can use it. If you purchase Safran Risk for x users you will get one code that x users can use to activate Safran Risk. In other words, normally all the users in an organization will be using the same license key. It is allowed for a user to activate the application on up to two machines.

2.1. Add a license key to activate Safran Risk

1. Start Safran Risk

2. Click "I have a license key".



3. Enter License key and click OK



4. Safran Risk is activating

2.2. Presetting the license key on a user's machine

If you're an administrator that wants to for example deploy Safran Risk by some form of virtualization you might want to "pre-install" the license key. This can be done by adding a file called "RiskLicense.txt" to the folder "C:\Users\

2.3. Offline period

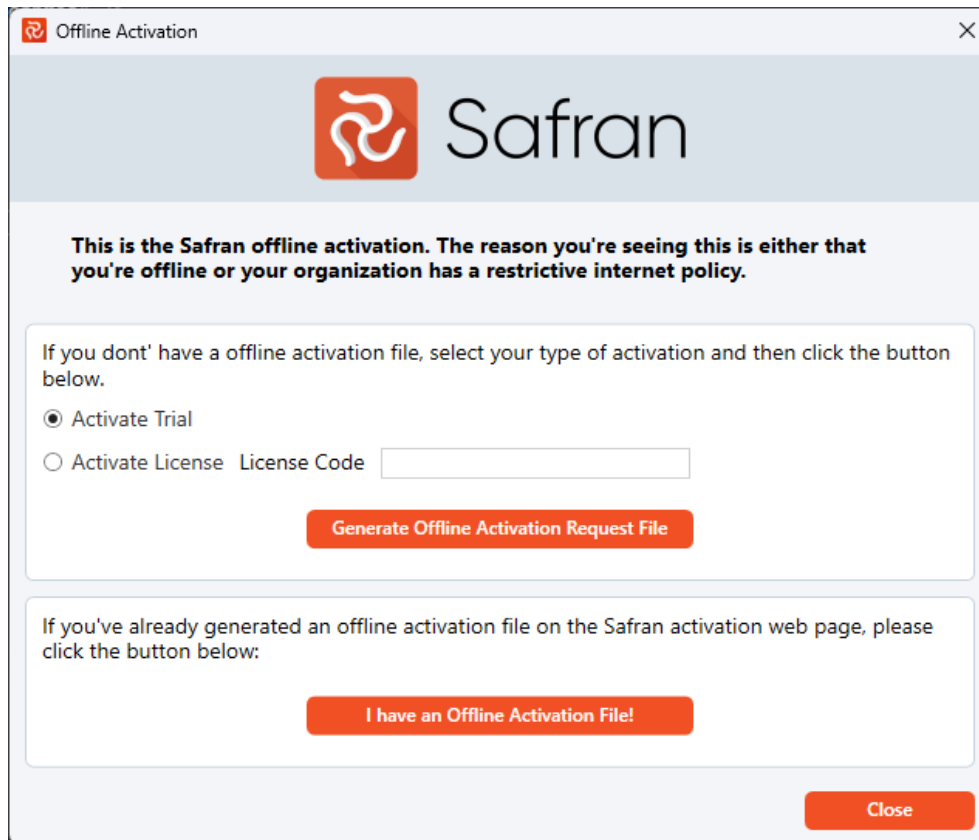
If for any reason a user loses the connection to the internet, the software will continue working for 30 days counting from the last successful connection to the license server. After this period the user needs to reconnect to the internet to continue using the software.

2.4. Offline activation

For users who work in a locked down environment where no connection to the internet is available Safran Risk allows for offline activation.

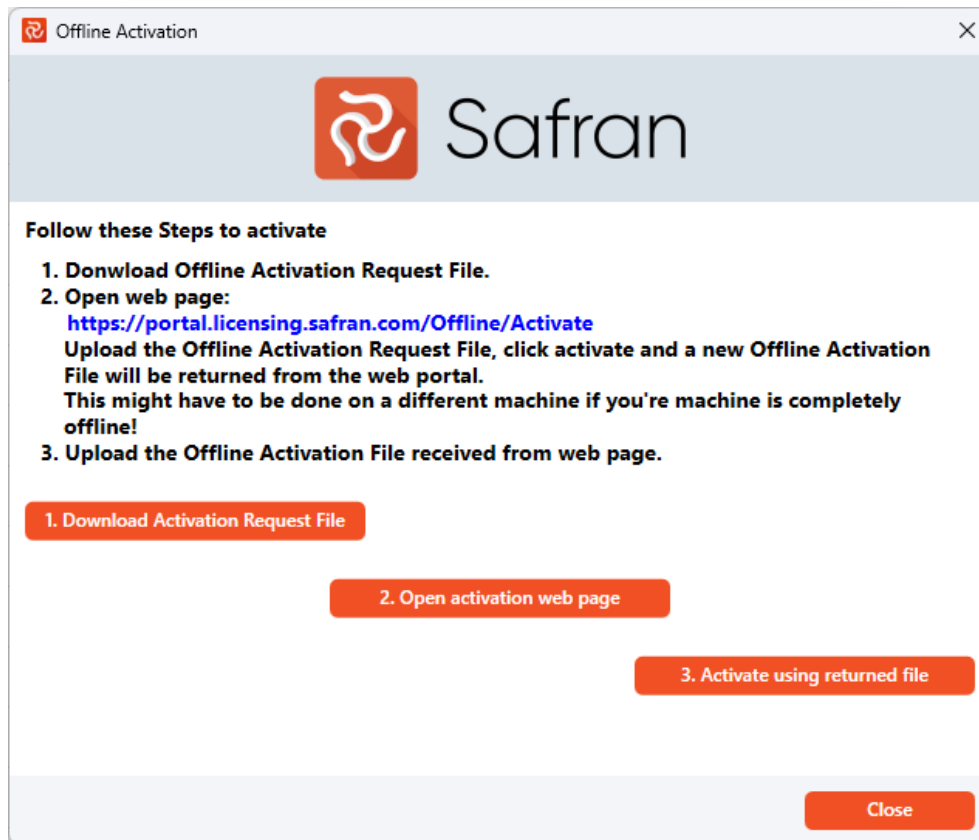
1. Start Safran Risk
2. Choose "Activate License" and enter the License key.

3. Click "Generate Offline Activation Request File". This will generate a file.

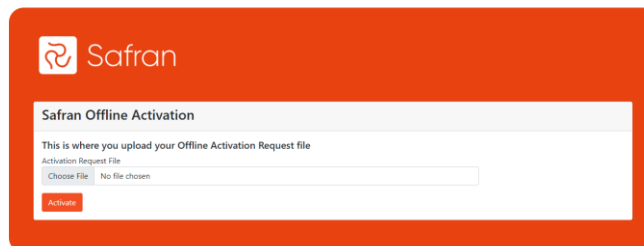


4. Open the activation web page and upload the "Offline Activation Request File". If you're really offline, copy the file to, for example, a USB Drive and go to a computer that has an internet connection.
If you do have an internet connection on your machine you can open the web

page by clicking button number 2.

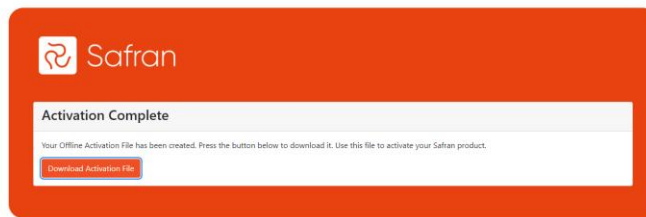


5. The webpage should look like this:

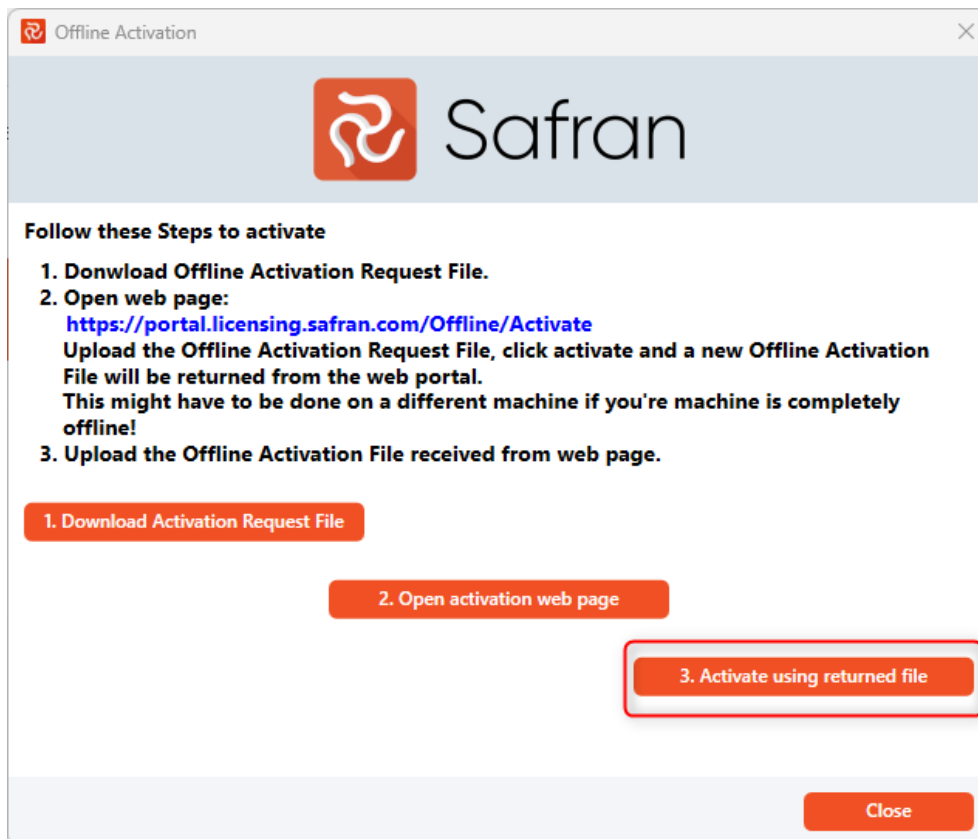


6. Upload the file and click "Activate"

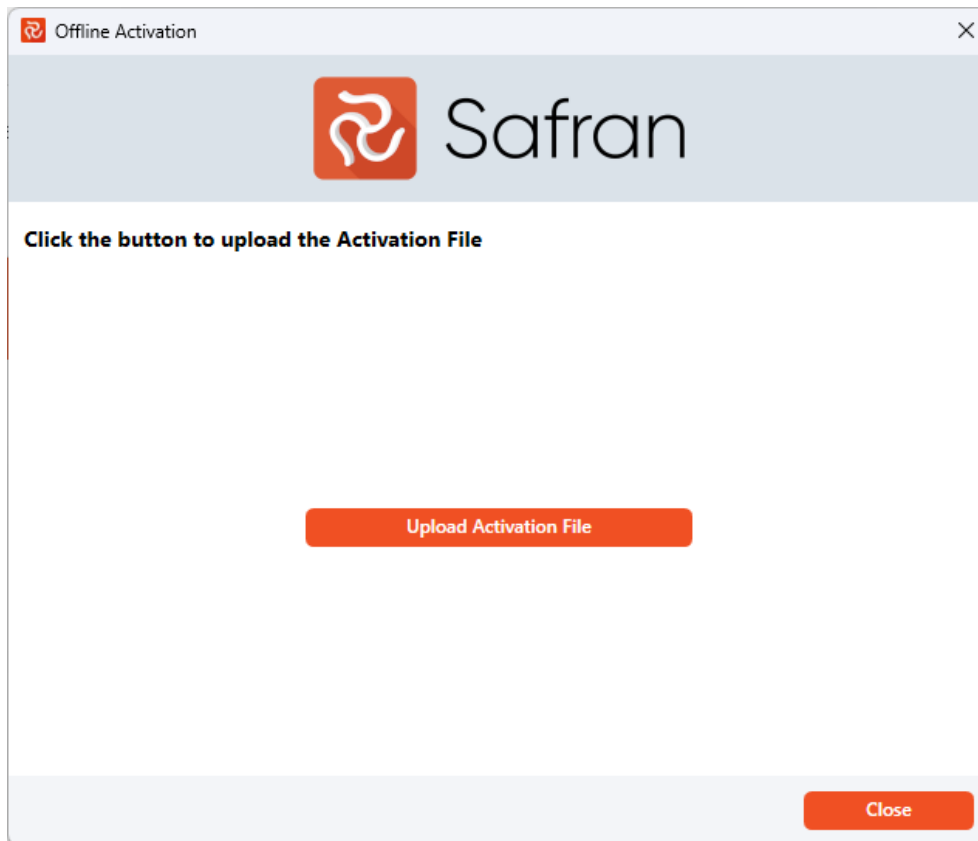
7. If the file was valid the page will return a new file to download like in the screen below.



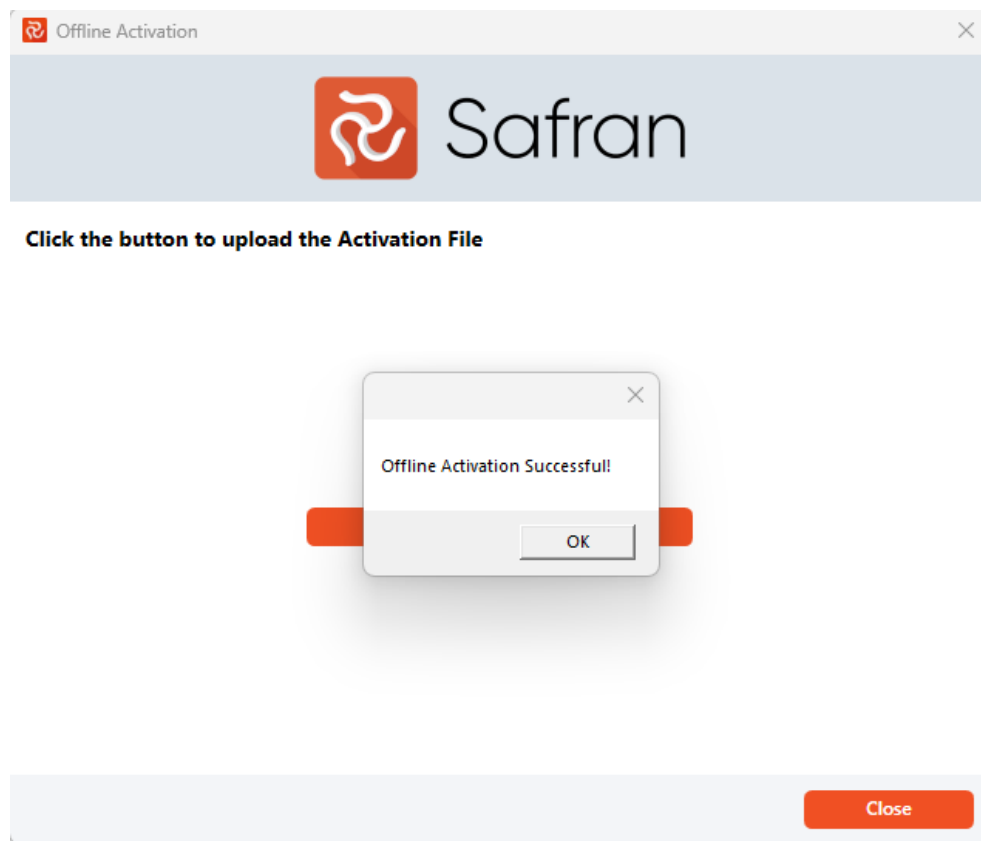
8. Click "Download Activation File" and go back to the Safran activation screen. If you're on a different computer, you can copy the file to a memory stick and take it back to the computer where Safran Risk has been installed.
9. Click "3. Activate using returned file"



10. Upload the activation file that you downloaded from the web page by clicking "Upload Activation File".



11. Safran Risk is now activated!



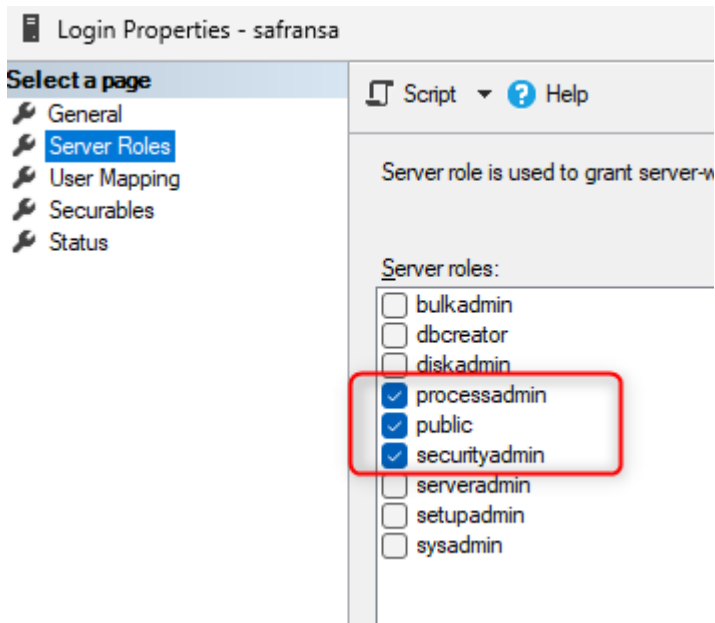
12. Click the Close button and Safran should now start.

3. Administrating a multi-user shared database

3.1. Setting up the database

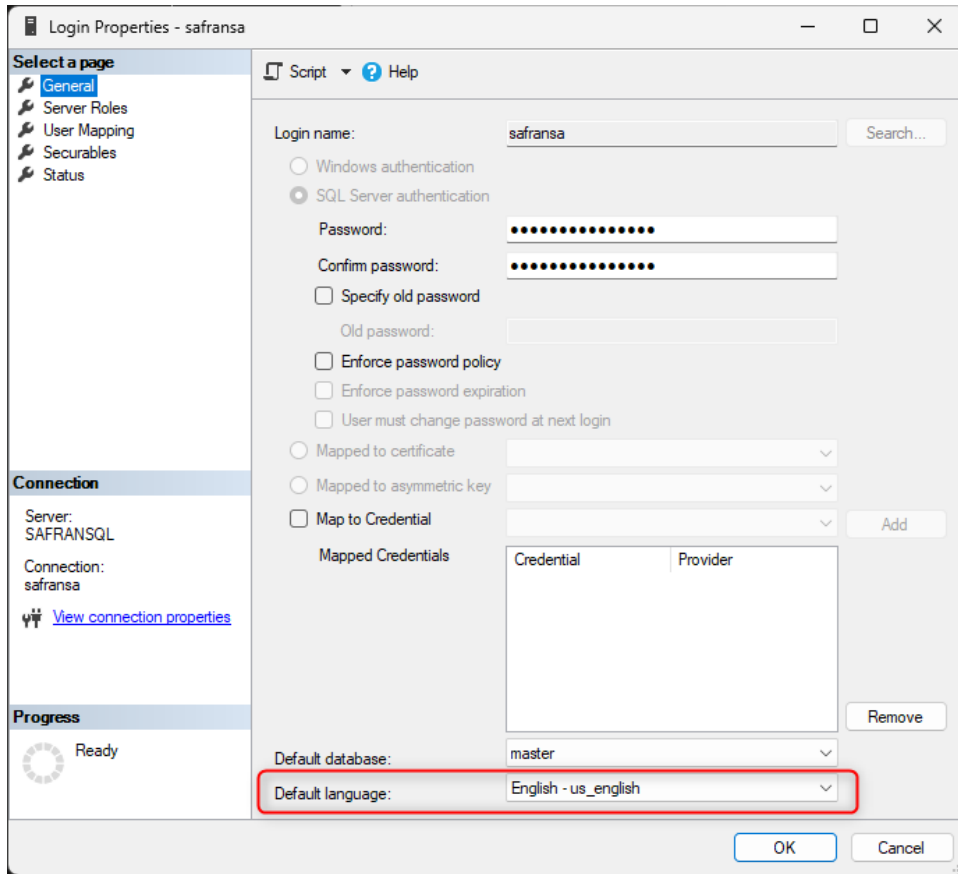
These are the main steps for setting up a shared database.

1. Create a sql server login user called safransa. Make sure the safransa login has the server roles processadmin and securityadmin.

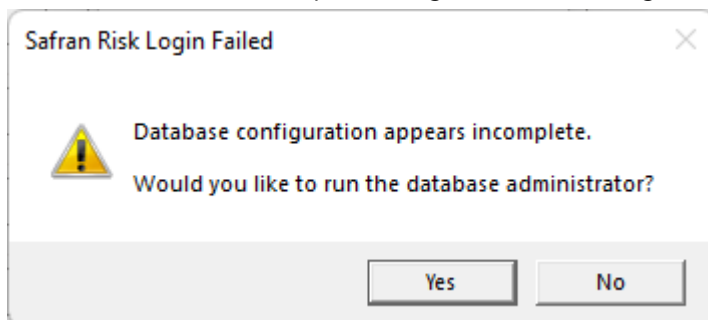


Also make sure that the default language of the safransa login is set to "English - us_english". If this is set to another language some of the database scripts

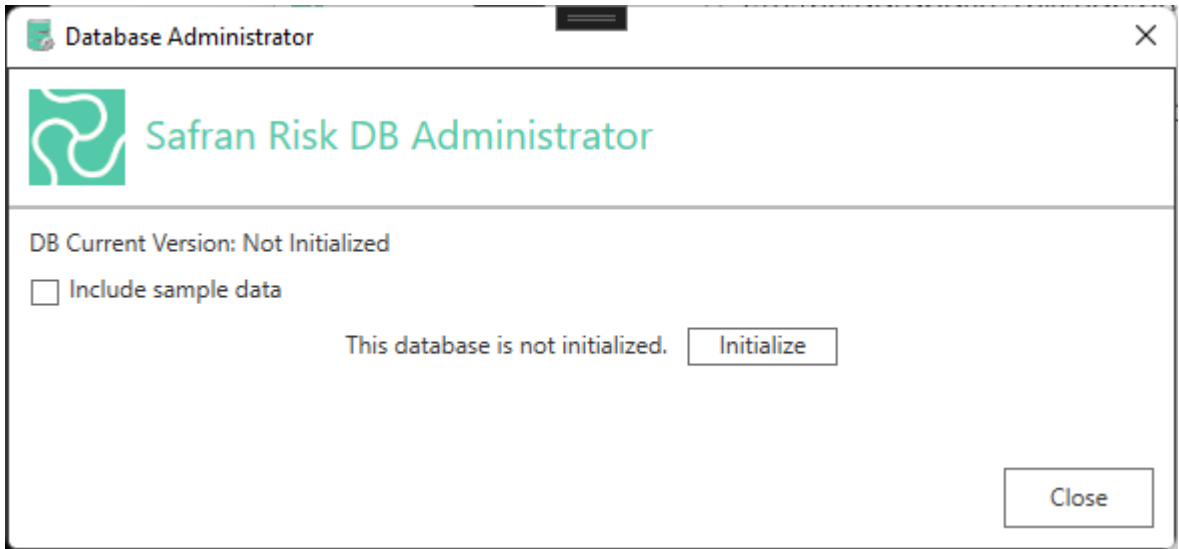
may fail.



2. Create an empty database and make sure that safransa is the db owner. Creating a database owner with a different name will still let you create the database but not all features in the Safran Sys Admin tool will be available (see next chapter). Make sure the collation of the new database is set to Latin_1_General_CI_AS or Danish_Norwegian_CI_AS.
3. Start Safran Risk and direct it to the database. (If the database wasn't selected during install this can be done after Safran Risk has started by clicking Change Database on the home tab).
When you direct Safran Risk to an empty database and you have logged in as the database owner you will get this message:



Answering Yes here will take you to the simple database administrator window:



Here you can create a new Safran Risk database. You have an option to include Sample Data. This means that there will be some layouts and projects in the database the first time you access it.

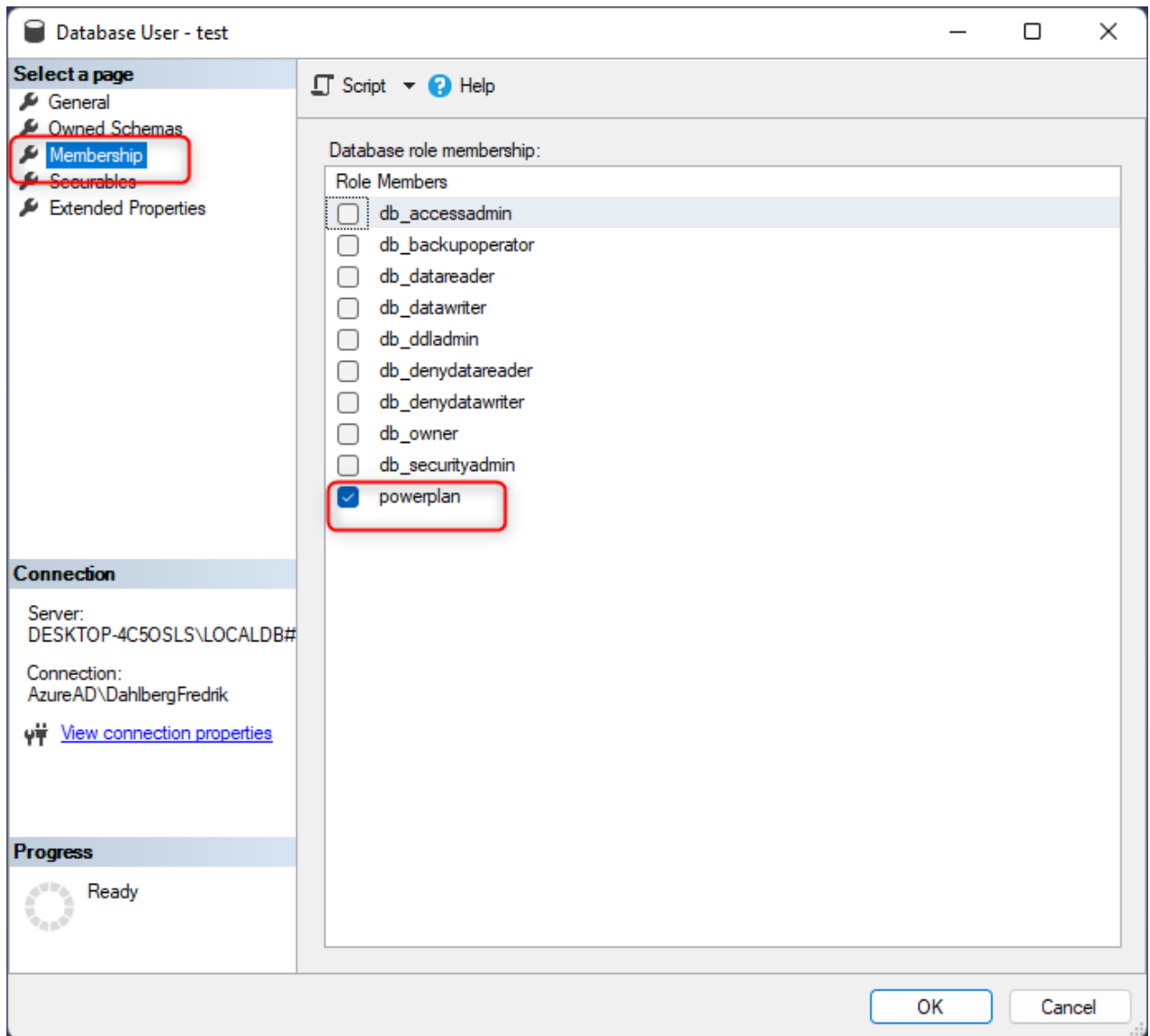
Clicking Initialize will run all the database scripts that creates the database. This can take a couple of minutes.

Once this is done your database is ready to be used.

4. (If setting up an Azure Sql Server Database with Microsoft Entra authentication see 3.3)

Add users to the database. Access to Safran Risk is controlled by access to the database. In other words, to have access to Safran Risk the user needs to have access to the database.

When you add users to the database they will need the role "powerplan". This is a role added by Safran. It's necessary to be a member of this role for all users that are not database owners.



Safran Risk supports both Sql Server Authentication and Windows Authentication.

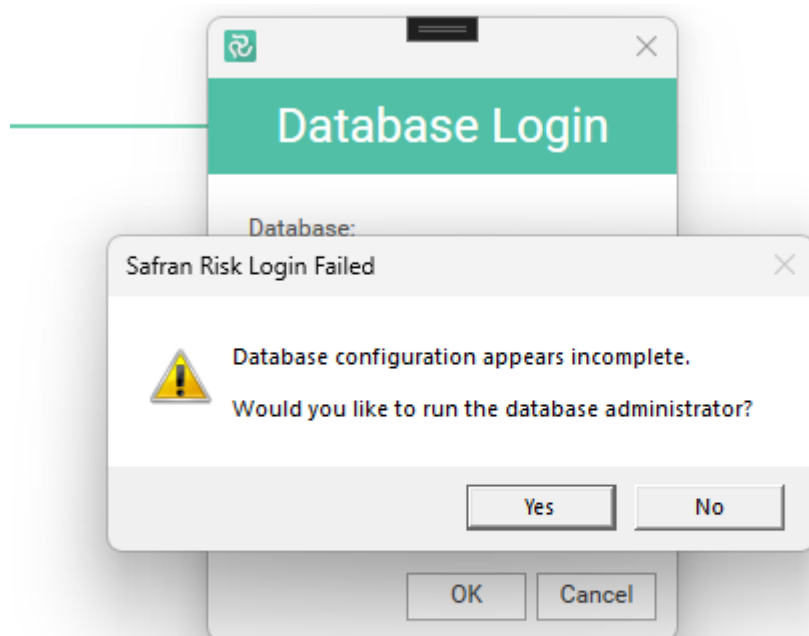
5. Your database is now ready for use! In order to do more advanced administration of the user's permissions, see the next chapter.
6. As an additional, but not mandatory step, it is strongly recommended to activate cleaning of invalid locks. This is described in section 4.8

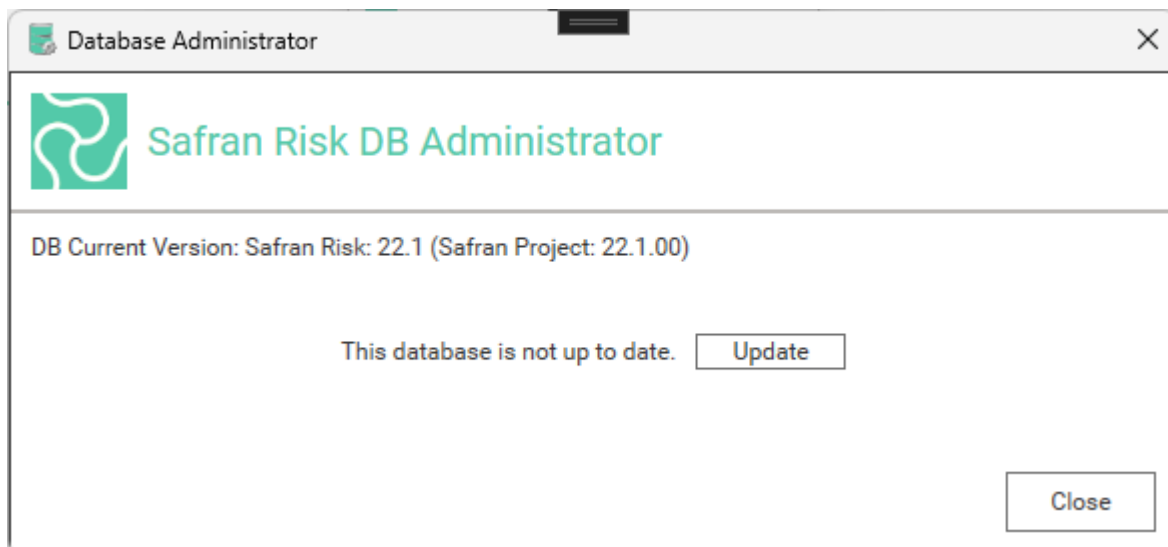
3.2. Upgrading the database

The database upgrade scripts are part of the Safran Risk application. To upgrade the database you should run Safran Risk and log in with the safransa user. This will give you a dialog from where you can upgrade the database. Note that you should not use the Safran System Administrator tool to upgrade Safran Risk. The upgrade functionality here should only be used for a pure Safran Project database.

NOTE: You should **ONLY** use the safransa user when upgrading the database. It's possible to run the upgrade with another user that is db owner but this will have unwanted consequences.

When you log in to a database that needs to be upgraded using the safransa user you will see the following dialogs:





Clicking update will upgrade your database to the version of the installed Safran Risk application.

3.3. Microsoft Entra Authentication

Safran Risk supports Microsoft Entra authentication. Access can either be given directly to the Entra user, via an Alias user or via an App registration. For most cases we would recommend access directly to the Entra user.

3.3.1. Via Entra user

In this set up you give the Entra users direct access to the database. You can also add them to an Entra group and give that group access to the database.

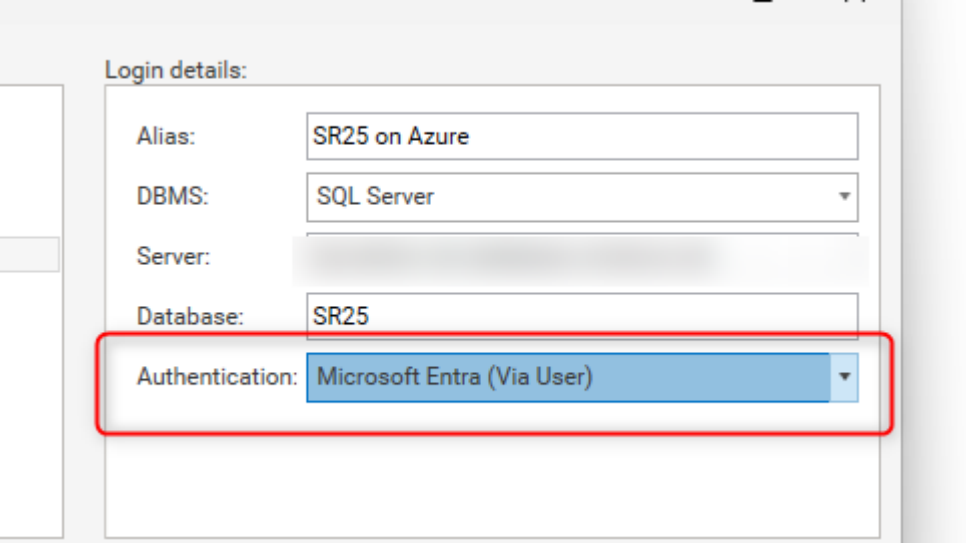
The users should only need to be given the role powerplan.

To give a user access to a database you can run these commands:

```
CREATE USER [user@company.com] FROM EXTERNAL PROVIDER;
```

```
ALTER ROLE powerplan ADD MEMBER [user@company.com];
```

When the users log in via Safran Risk they should use this authentication:



Login details:

Alias: SR25 on Azure

DBMS: SQL Server

Server: [blurred]

Database: SR25

Authentication: Microsoft Entra (Via User)

3.3.2. Via Alias user

In this set up an alias user is used for all the database transactions. The Entra user will only be used to get access to the alias user.

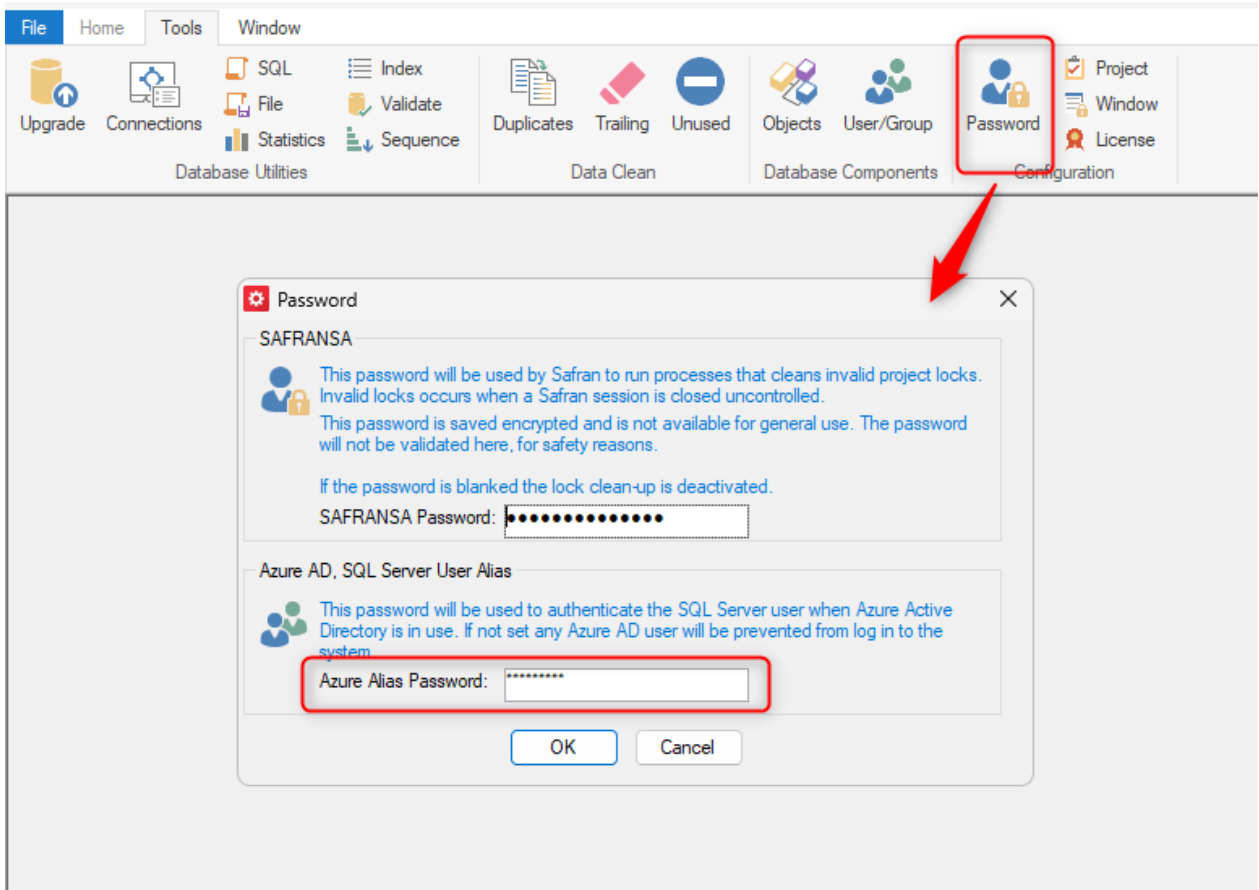
These are the steps for setting up an alias user:

1. Run the following command on the master database:
`CREATE LOGIN [SAFRANSQLUSERALIAS] WITH PASSWORD='<password>';`
Make a note of the password you used. The name of the alias user cannot be changed!
2. On the database that you're setting up run the following commands:

```
CREATE USER [SAFRANSQLUSERALIAS] FOR LOGIN [SAFRANSQLUSERALIAS];  
ALTER ROLE [powerplan] ADD MEMBER [SAFRANSQLUSERALIAS]
```

This will give the alias user access to the database.

3. The last step needs to be done after the database tables have been created. To do this start up the Safran Admin tool, log in to the database. In the admin tool click on Password and insert the password of the alias user. Click ok. It will now be possible for Safran Risk to use the alias user when a user logs in using Microsoft Entra.



Once the alias user has been set up you can give Microsoft Entra users access to the database. These users should only be in the role “public” and not “powerplan”.

3.3.3. Via an App Registration

One way to allow the Safran Risk users to access data in azure (without assigning users directly to the database) is to use an app registration.

The goal is to enable Safran Risk to authenticate securely to Azure AD using a certificate that you control.

Follow the steps below to set up this form of database access.

Create an app registration in Azure

1. Go to Azure Portal
2. Navigate to Entra **App registrations**
3. Click **New registration**

4. Enter a name (e.g.,SafranRiskApp)
5. Choose **Accounts in this organizational directory only**
6. Click **Register**

Generate a Client Authentication Certificate

Use PowerShell to generate a self-signed certificate:

```
$cert = New-SelfSignedCertificate `
  -Subject "CN=SafranRisk" `
  -KeySpec Signature `
  -KeyExportPolicy Exportable `
  -KeyUsage DigitalSignature `
  -Type Custom `
  -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2") `
  -CertStoreLocation "Cert:\CurrentUser\My"

Export-Certificate `
  -Cert $cert `
  -FilePath "C:\Temp\SafranRisk.cer"

Export-PfxCertificate `
  -Cert $cert `
  -FilePath "C:\Temp\SafranRisk.pfx" `
  -Password (ConvertTo-SecureString -String "StrongPassword123" -Force -AsPlainText)
```

This creates a certificate with the correct usage for Azure AD authentication and installs it in your Windows Certificate Store.

The first Export-Certificate bit creates a Public Certificate in the form of a .cer file. This will be uploaded to the Azure App registration.

The second export creates a certificate with a private key. This is used to install the certificate on all the machines of the users.

Upload the Public Certificate to Azure AD

1. Go to your App Registration
2. Navigate to 'Certificates & secrets'

3. Click 'Upload certificate'
4. Select the .cer file you exported
5. Click 'Add'

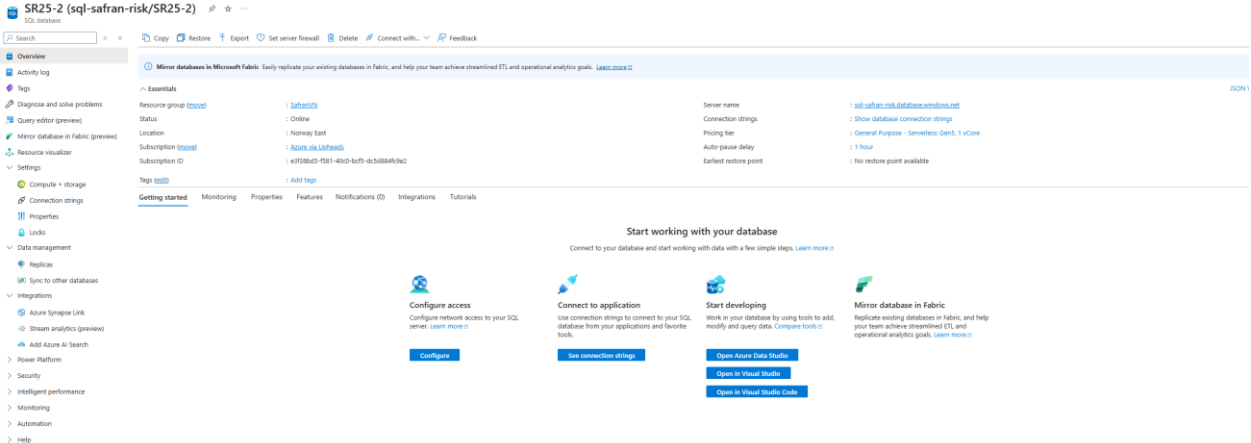
Assign API Permissions to App Registration

In the App Registration:

1. Go to 'API permissions'
2. Click 'Add a permission'
3. Choose 'APIs my organization uses'
4. Search for 'Azure SQL Database'
5. Select 'Application permissions' (e.g., user_impersonation or .default)
6. Click 'Add permissions'
7. Click 'Grant admin consent' (if required)

Create a database and populate it using the Safran Risk scripts

Create an azure database. Choose a size that is suitable.



The screenshot shows the Azure portal interface for a Microsoft SQL Database. The top navigation bar includes 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Query editor (preview)', 'Minor database in Fabric (preview)', 'Resource visualizer', and 'Settings'. The main content area is titled 'SR25-2 (sql-safran-risk/SR25-2)' and shows the following details:

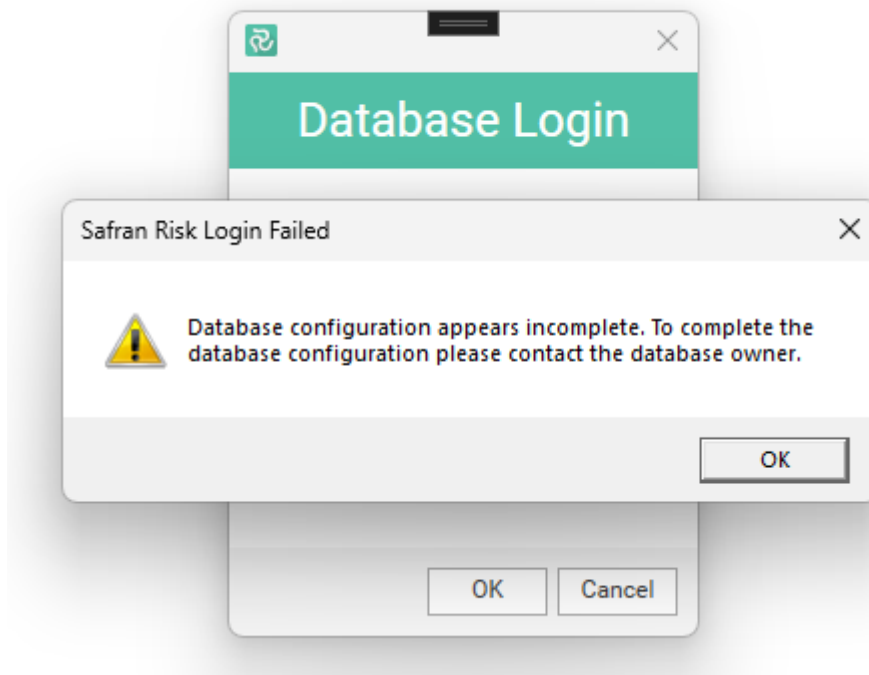
- Resource group: safran(r)
- Status: Online
- Location: Norway East
- Subscription ID: e1f538d3-75d1-4b3d-b67b-8c388a4c9e2
- Server name: sql-safran-risk.database.windows.net
- Connection strings: Show database connection strings
- Pricing tier: General Purpose - Serverless Gen1, 1 vCore
- Auto-pause delay: 1 hour
- Earliest restore point: No restore point available

Below the settings, there is a 'Start working with your database' section with the following cards:

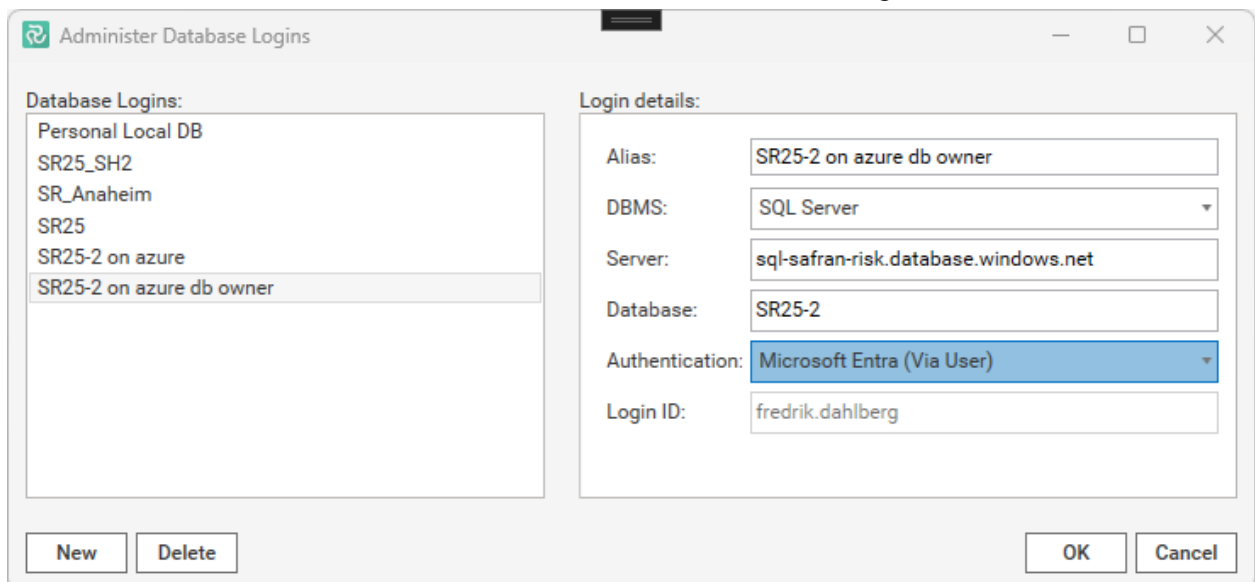
- Configure access:** Configure network access to your SQL server. [Learn more >](#)
- Connect to application:** Use connection strings to connect to your SQL database from your applications and favorite tools. [See connection strings](#)
- Start developing:** Work in your database by using tools to add, modify and query data. [Compare tools >](#)
- Mirror database in Fabric:** Replicate existing databases in Fabric, and help your team achieve streamlined ETL and operational analytics goals. [Learn more >](#)

To populate the database with tables and procedures you need to run Safran Risk and point it to the database.

When running Safran Risk against an empty database you might get this message:



It's necessary to be a db owner in order to build the database. We don't recommend that all the users connect to the database as db owner. Therefore, it's better to log in as the actual db owner when building the database. You can do this by setting authentication method to "Microsoft Entra (Via User)" and log in as the db owner.

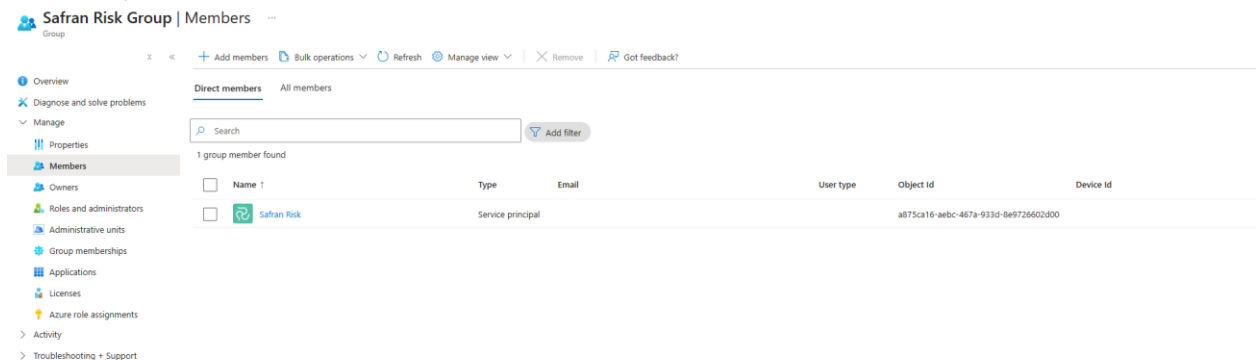


The database should now be built.

Give the app registration access to the database

Now you need to give the app access to the database.

The preferred way of doing this is to create an Entra group and add the app as a member to that group:



Now you can create a db user from the group by running the following sql command (either in azure portal or for example in SSMS):

```
CREATE USER [<Group Name>] FROM EXTERNAL PROVIDER;
```

Give the group some permissions:

```
ALTER ROLE powerplan ADD MEMBER [<Group Name>];
```

For azure we need to give the powerplan some more permissions:

```
GRANT VIEW DATABASE STATE TO powerplan
```

Set up the end-users' machines

On each end-user machine the following needs to be done:

Install Safran Risk

Safran Risk needs to be installed either via the installer provided by Safran or your own version of it. If you have your own installer you might be able to include the next steps as part of that.

Install Certificate

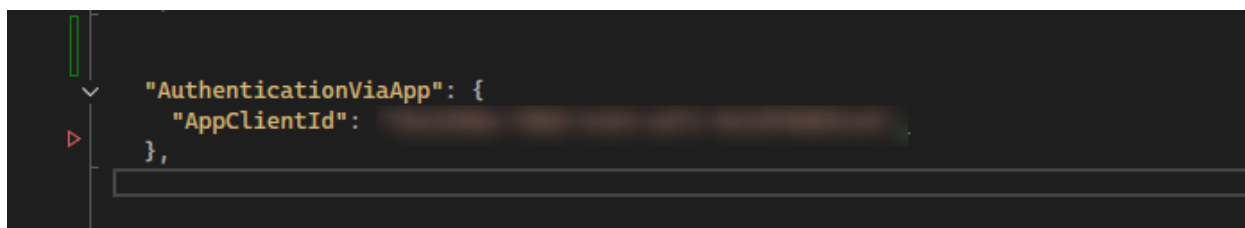
The pfx file that was generated in step 2 will be used to install the certificate on the user's machine.

Here's one way to install it from powershell:

```
$certPath = "C:\Path\To\SafranRisk.pfx"
$certPassword = ConvertTo-SecureString -String "StrongPassword123" -Force -
AsPlainText
Import-PfxCertificate `
  -FilePath $certPath `
  -CertStoreLocation "Cert:\CurrentUser\My" `
  -Password $certPassword
```

Add client id to appsettings.json to allow Safran Risk to connect via the azure app registration

For Safran Risk to connect as the app you need to add one value to the appsettings.json file. It's located in the Safran Risk installation folder.

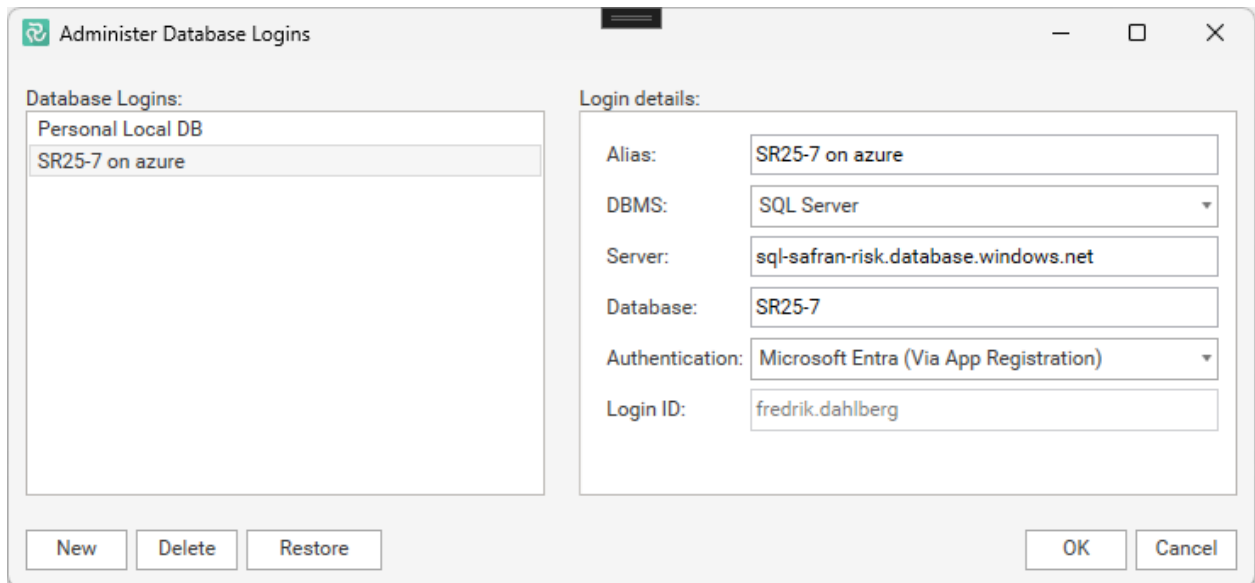


AppClientId: The client id of the app registration

This value needs to be in the appsettings.json on every users machine. The appsettings.json file resides in the install directory of Safran Risk.

The users in your organization should now be able to access the database via Safran Risk as long as the appsettings.json is set up correctly and the certificate is installed.

To login they need to add a Database Login that looks like this:



Note that the Authentication is set to “Microsoft Entra (Via App registration)”.

4. Using the Safran System Administrator tool

The Safran System Administration application (Sysadm) is used to maintain your Safran application and database. To be able to use Sysadm, a database and at least one user with database administrator privileges is needed, this user should be named safransa. Creating databases is normally among the tasks that the IS department like to consider their domain. Therefore, we recommend that you contact your IS department and work closely with them. When you are ready to install Safran Risk you should follow the steps described in the previous chapters.

If you are running a Safran Risk Personal edition with MS SQL Local DB, the database file is part of the installation. It is already configured with a DBA user, and the Sysadm application can be utilized after installing the software.

Note that this tool is used both by Safran Project and Safran Risk users. Some parts of the tool will only be relevant for Safran Project users.

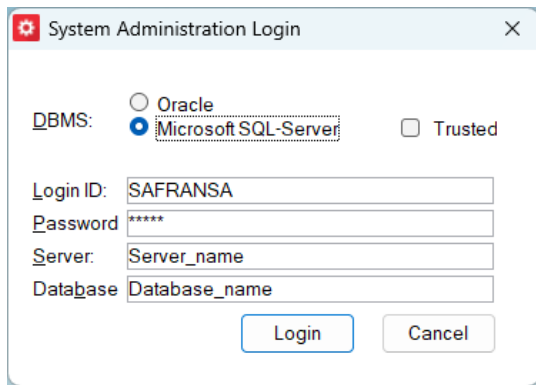
4.1. Starting Safran System Administration

Depending on your installation there are three ways to start the Safran System Administration tool.

Using an Icon. For convenient access, a windows capability allows a short-cut icon to be added to your desktop.

Using the windows Start Menu. Another windows capability that is available for initiating programs is the Start Menu.

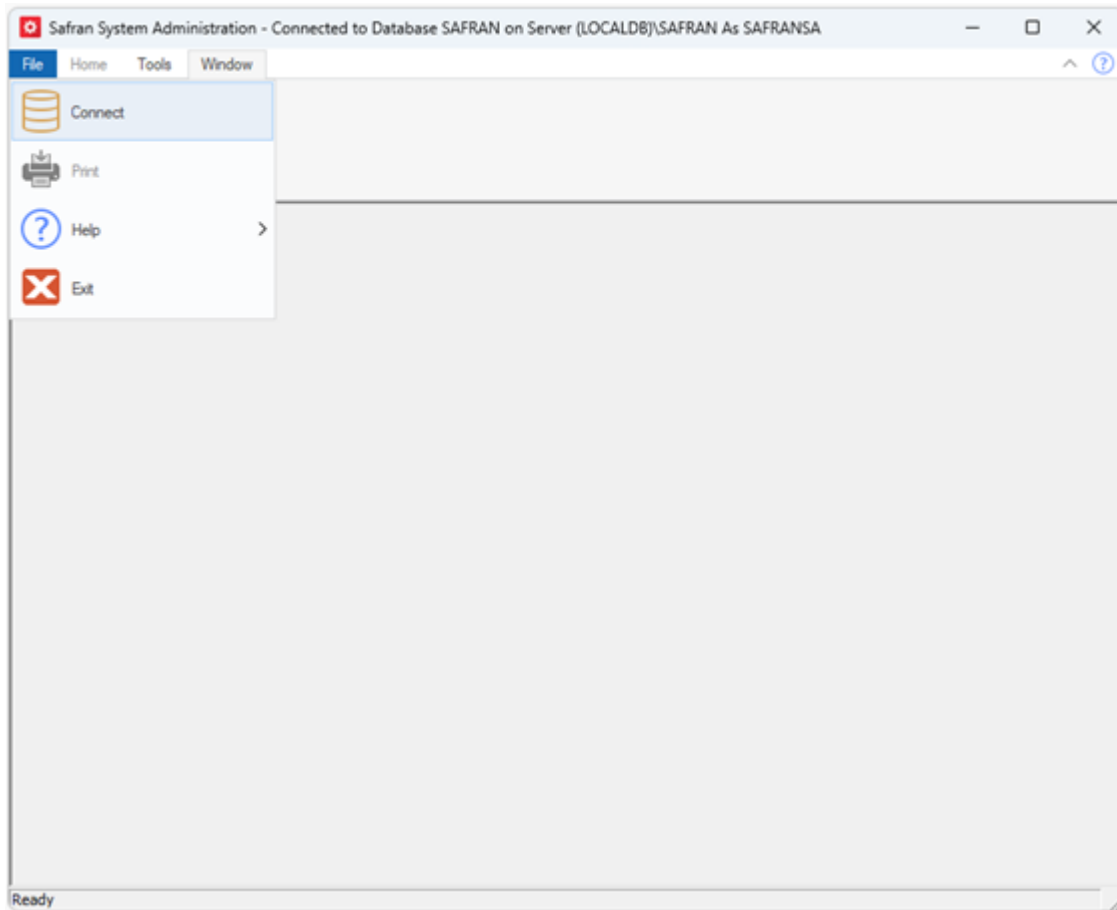
Choose the program file (.EXE) from the appropriate install directory window in your windows explorer. It will be located here: "C:\Program Files\Safran Software Solutions\Safran Risk\Project\safransa.exe"



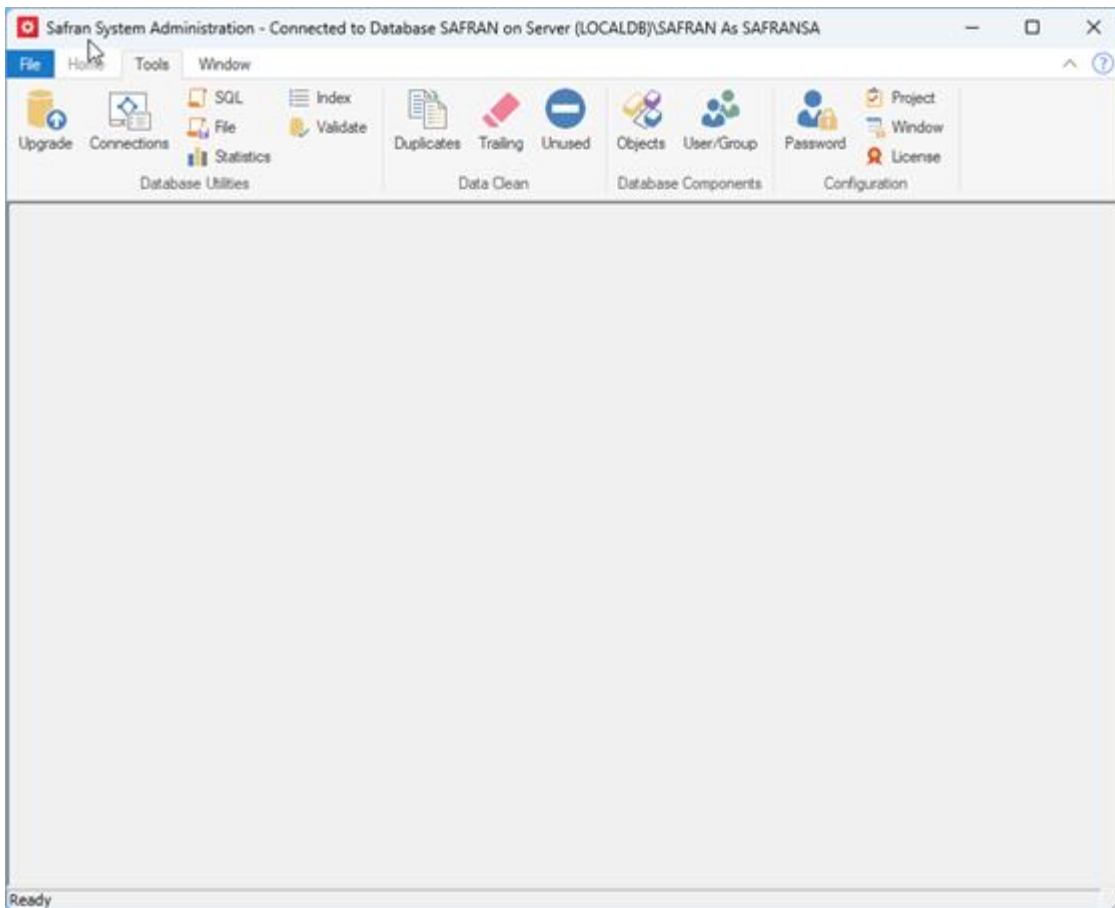
To login, Select DBMS system (should be Microsoft SQL-Server for Safran Risk users), enter your Log in ID and Password, and server and/or database name. The system administration login and password should be provided by your IS department. If you do not know this information you should check with your IS department.

If you are using Safran Personal, you can connect to the local database by using trusted connection and the servername (localdb)/Safran and database name: SafranRisk.

4.2. Safran System Administration Window



Choose Connect from the File menu to connect to different databases.



The Tools menu lets you add and modify users and user groups, work with database tables, views, procedures and more, create database profiles, you can restrict access on certain Safran windows for regular users, define Enterprise fields to be used for this database, set network defaults and view license key information and maintain your license. NB The license part is not relevant for Safran Risk users! This is only relevant for Safran Project.

For details on these functions please see the relevant chapters in this guide.

4.3. Users and security

Safran provides two mechanisms for protecting against unauthorized access:

- User name and password – to prevent “outsiders” accessing your project data
- Access permissions – to control the actions authorized users can perform on the objects in your Safran implementation.

4.4. Safran Users

Control over who can access Safran is mainly kept by creating users who can be granted or denied access to Projects, Project Groups, Calendars, Userfield sets, Resource sets, Symbol sets, Rule sets, Rate sets, and Profile sets. The users are kept in the table "users" with columns "login_name" and "full_name."

Each Safran user must also be a database user. To create a Safran user, the user should be made in the database first. All Safran users should be members of at least one database group. When a Safran database is initiated, a default group is initiated, and this group is granted "all" privilege to all the tables and "execute" privilege to stored procedures. Initially, all Safran project users should be assigned to this group.

Suppose the technical system administrator wants to differentiate the database privilege between different groups of users. In that case, a new group may be added through the Safran interface, and some users can be moved from the default group to this new group. The system administrator must then keep track of which users belong to which database group and grant and revoke privileges accordingly.

4.5. Safran User Groups

Safran users can be organised into user groups to simplify access control.

Note: User groups, as defined in Safran, are different from DBMS Groups, which are part of the database management system. User groups in Safran are used to organize users for access control purposes.

A user can be a member of several groups.

Information about groups is kept in two tables: One table, "user_groups," keeps the definition of the groups, with columns "group_id," a numeric identification for the group, and "name," to keep a descriptive name for the group; another table "group_members" with the column "group_id" and "login_name," keeps track of which user is member of which groups.

When a Safran database is initiated, the default group "public" is created, with group_id=1. All new users are given membership in this group.

4.6. User Access Object Type

There are two tables for access control: "user_access", with the columns "login" (user), "object_id", "object_type" and "access_level" (From 1(Read) to 4 (Exclusive)); and "group_access" with "group_id", "object_id", "object_type" and "access_level".

Access for the different objects is controlled from inside Safran Risk.

Code	Safran Object	Access Levels
N	Project	1=read,2=test,3=update,4=exclusive
S	Sub-Project	1=read,2=test,3=update,4=exclusive
R	Resource set	1=read,2=update
P	Profile set	1=read,2=update
C	Calendar	1=read,2=update
U	Userfield set	1=read,2=update
W	Window	1=read,2=update
A	Rule set	1=read,2=update
B	Symbol set	1=read,2=update
G	Project Group	1=read,2=test,3=update,4=exclusive
L	Global Sets	1=read,2=update
O	Rate Sets	1=read,2=update

4.6.1. Window Access Restrictions

Whereas access must be set explicitly on a standard object for a user to be able to access them, windows are, by default, accessible for all users. This window must be added to the list of windows with limited access to restrict user access to a window. If a window has restrictions, only users granted access can open it. Setting Window access restrictions is done from Tools -> Window

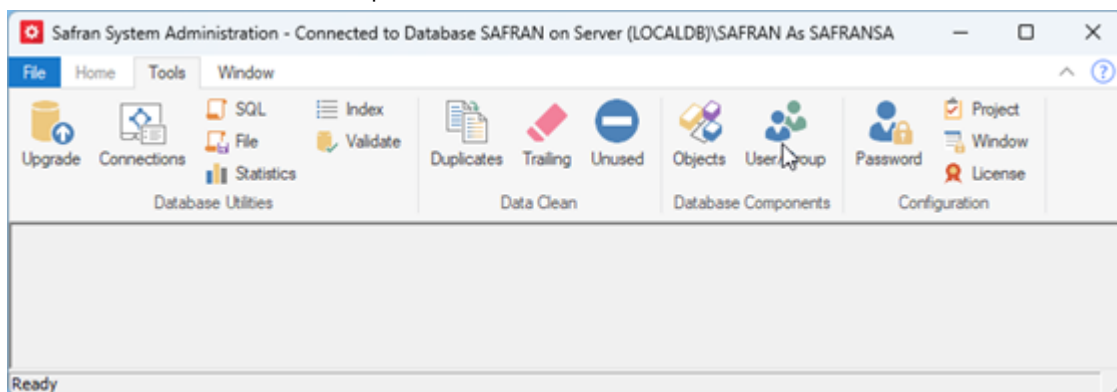
4.7. Defining and maintaining users

As a key function of Safran System Administration, the creation and maintenance of Safran users is of utmost importance. Every user accessing Safran Project or Safran Planner must be defined as a valid Safran user, underscoring the crucial role of system administrators in managing user access.

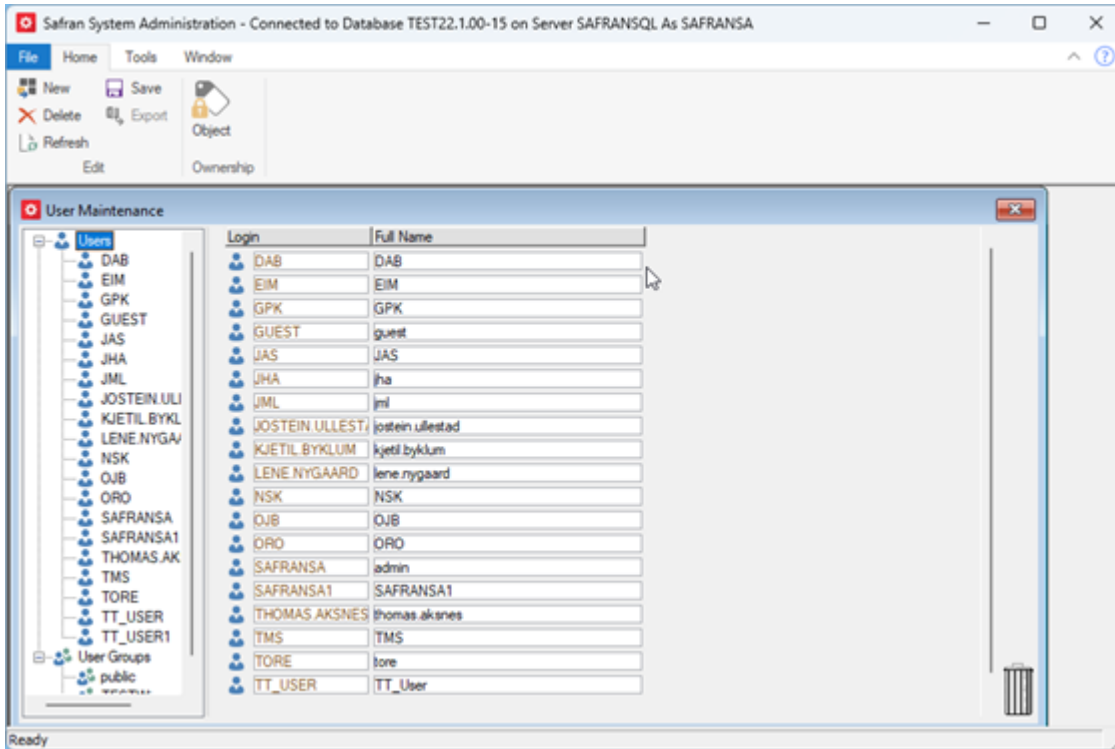
The User Maintenance option allows you to:

- Create users
- Create user groups
- Delete users
- Delete user groups
- Change/modify the user's full name
- Transfer ownership

Select Tools -> User/Group from the menu.



The User Maintenance window is a two-paned window with a hierarchic out-line style window on the left and a list of users, groups, and user details on the right.



If you, in the left pane, select "users," the right pane displays a list of all defined users with login ID and full name.

If you, in the left pane, click on the "Users" icon and select an individual user, the right pane displays the login ID and the full name together with any group membership of that particular user.

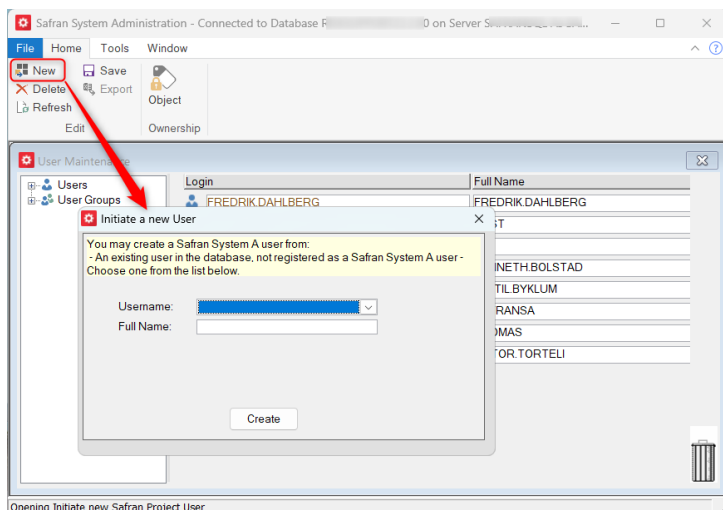
Selecting user groups in the left pane window displays a list of defined user groups in the right pane.

Selecting a user group in the left pane displays group memberships in the right pane.

4.7.1. Adding a new Safran user

NOTE: In Oracle, the system administrator must create a database user. In Microsoft SQL-Server a database login must be created before a database user is created. A database login can only be created by a database system administrator. Be sure that these are in place before creating corresponding Safran Users, as it is not possible to create a Safran User without a corresponding database user.

With the user/group maintenance window open, select the New button from the Home tab. The "Initiate new Safran user"-window will appear:



Now you can select a name from the username drop down, which contains users in the database that currently are not registered as Safran users. Choosing a user may also populate the "full name" field, enabling you to choose next.

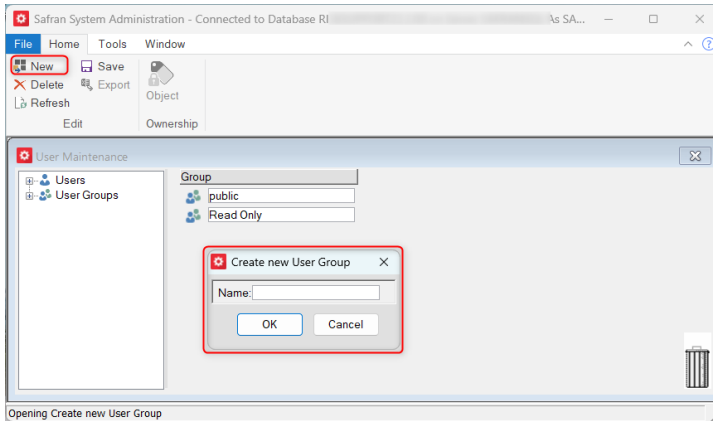
4.7.2. Deleting a Safran user

In the user/group maintenance window, select the user. Choose "Delete" on the Home tab menu (you may also drag and drop the user to the bin). You should now be prompted to confirm deletion of the user.

NOTE: Before deleting or removing a user from your Safran database, please read the "object Ownership" section carefully. Deleting users also removes his or hers filters, layouts and report specifications

4.7.3. Create a New Safran User Group

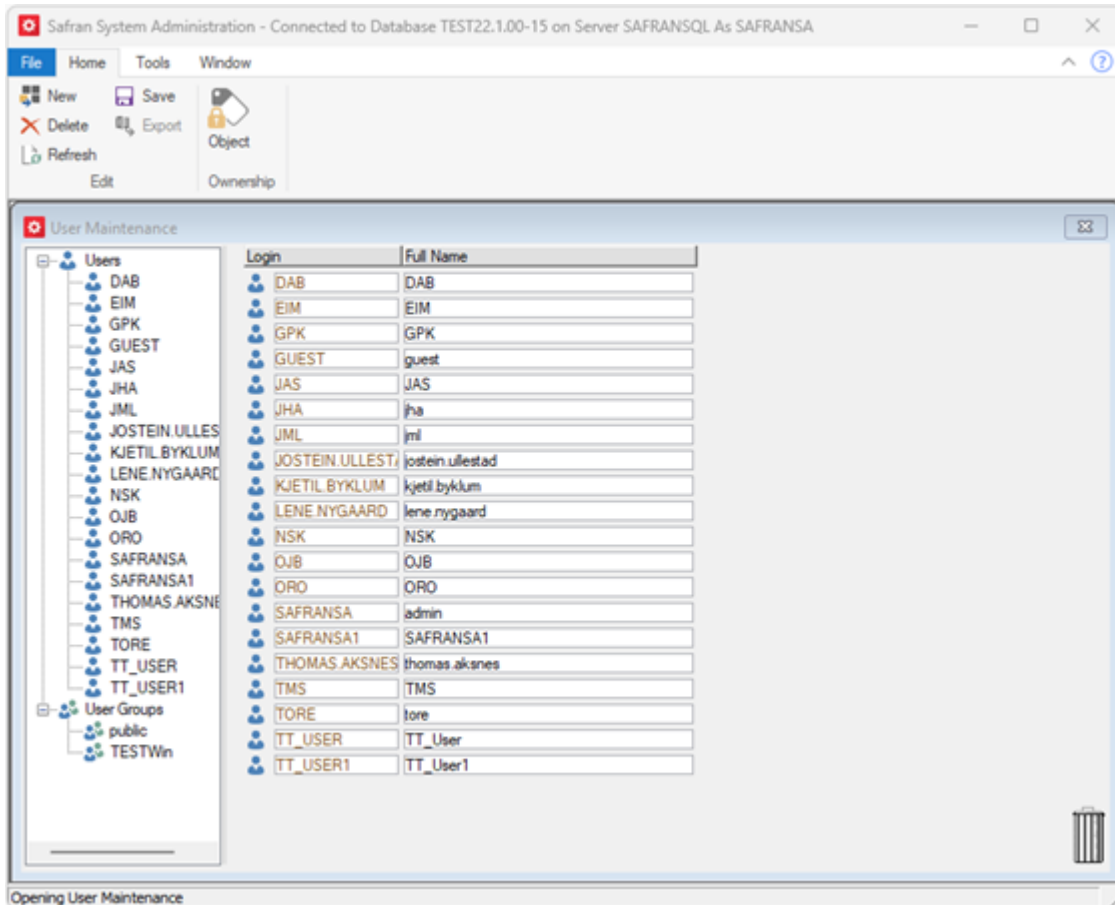
In the user/group maintenance window, select "User Groups" in the outline pane, and then "New" in the Home tab section. The "Create new Group" - window will open:



You should now enter the new group's name. Having done that you click "OK", and the new group is created and ready to accept members.

4.7.4. Adding a User to a Group

Set focus on "User" in the left-hand section of the user maintenance window. You will now get a list of all the users in the right-hand area. Drag the user name from the right-hand section to the appropriate group in the left-hand section to add the user to the selected group.



4.7.5. Remove a User from a Group

Select the user in the left-hand section of the user maintenance window. The right-hand section of the window displays the group memberships for that particular user. Find the group membership you want to remove and drag it to the recycle bin in the lower right-hand corner to remove the group membership.

OR:

Select the group in the left-hand section of the user maintenance window. You will now get a list of all the users belonging to the group in the right-hand area of the window. Drag the user to the recycle bin to remove the user from the group.

NOTE: You cannot remove a user from the "Public" group!

4.7.6. Object Ownership

By default, the user creating any of the Safran objects (projects, symbol sets, resource sets, rule sets, userfield sets, calendar sets, profile sets and user saved report specifications and filters) is defined as the Owner of the objects.

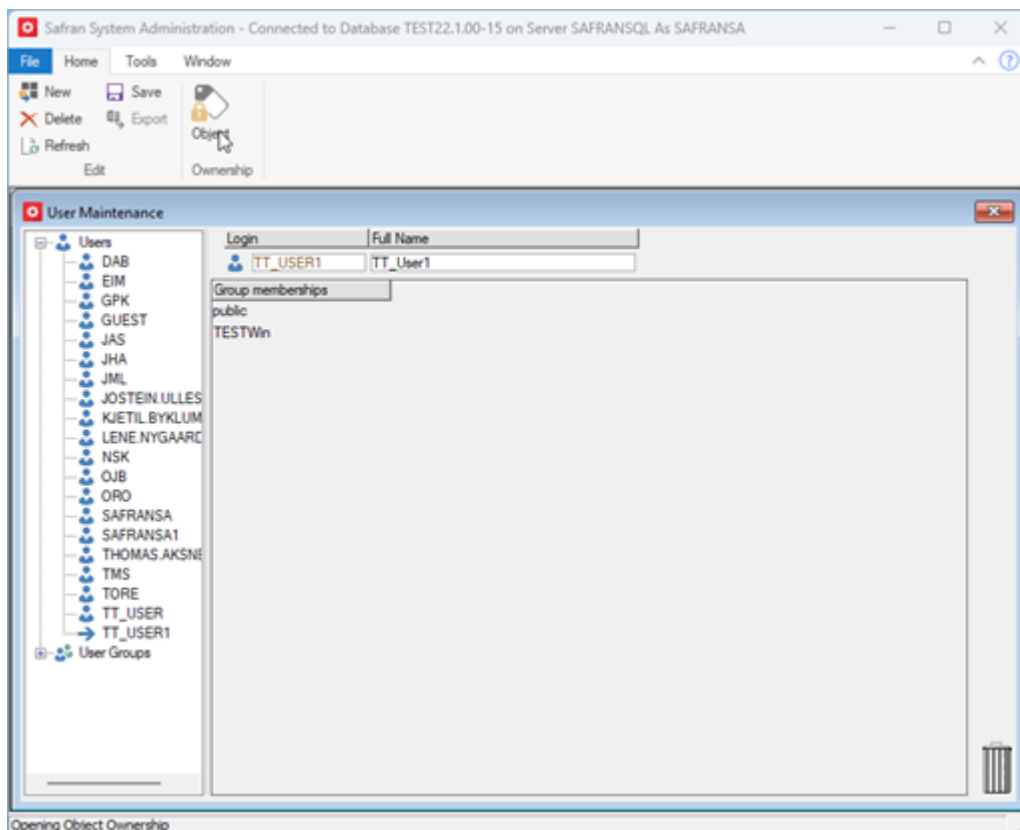
For all objects other than filters and report specifications the owner assigns user access to these objects. All users may use filters or report specifications created by any user, but they are not allowed to modify or alter any of these.

When you remove a user from the system, the object owner is no longer valid. The system administrator may change Ownership from one user to another on all objects.

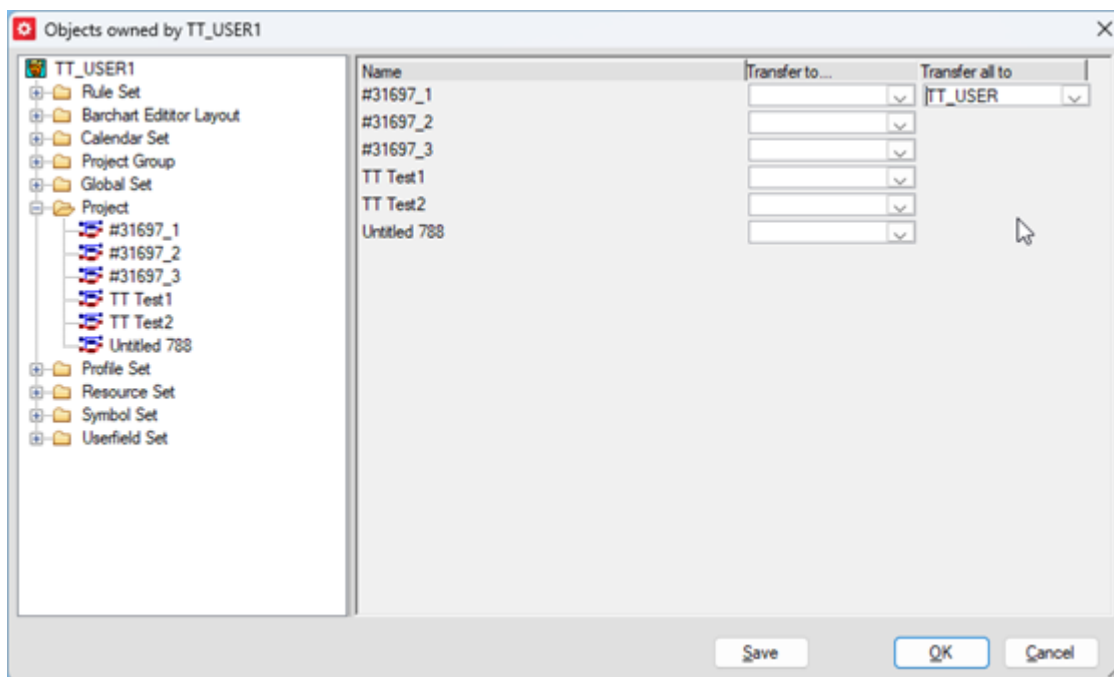
Removing a user also removes his or hers filters, layouts and report specifications as these are “private”. However, if a user’s report specifications or filters should be available to other users, you should transfer ownership to a new user.

4.7.7. Transferring ownership

Transfer object ownerships before removing a user from the system, select Tools>Users/Groups. In the Home tab, select the Object button. You will now see the full list of all objects defined by and owned by the selected user.



To transfer ownership, select the object type and the object(s) you want to transfer or choose transfer all objects, then select the user to receive the ownership from the drop-down list. Click "save" to finalise the transfer.

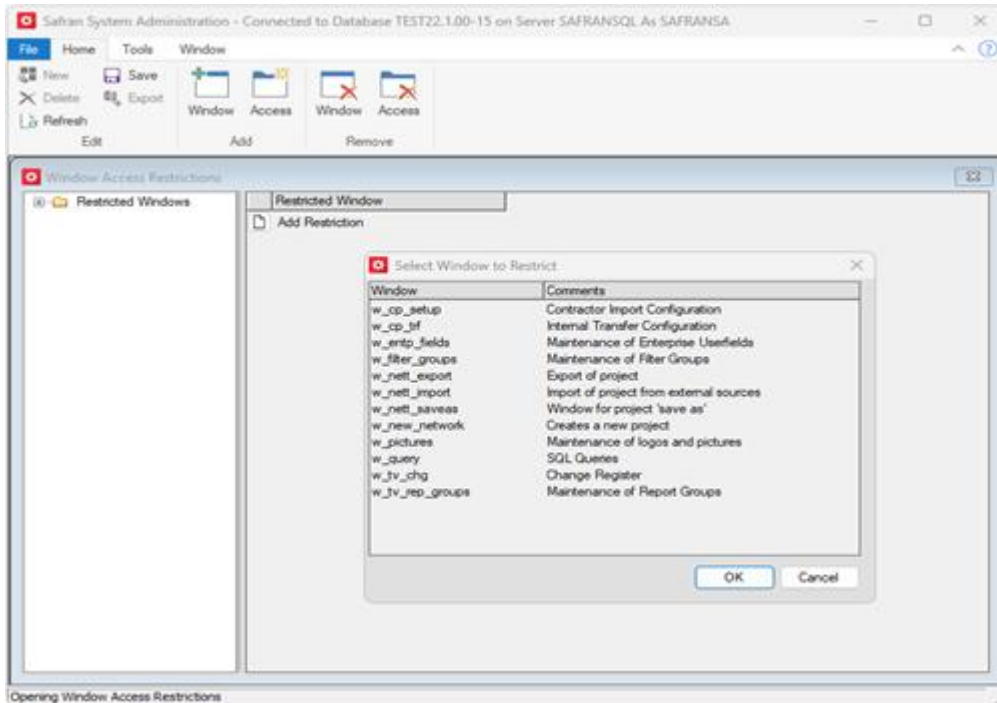


4.7.8. Restricting Access to a Window

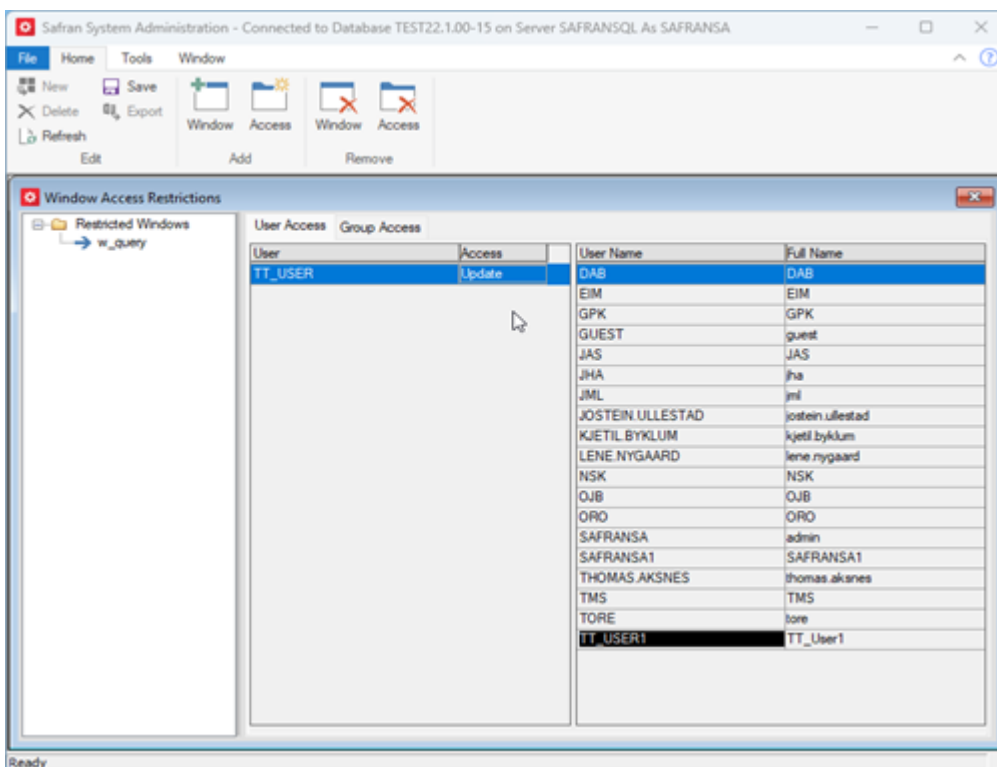
You may want to restrict access from some of the areas or features of Safran, allowing only some of the users to e.g. update project information, update calendars, run the initial Baseline, have Access to the SQL window etc. To do that, you restrict access to the relevant window.

From the menu, choose "Tools -> Window." The window for window access control opens. In the left pane of this window, there is a tree view with "Restricted Windows" on top, exploding to show the names of all windows with access restrictions implemented.

Click "Add restriction" to add a new restriction. This opens the "Select window to restrict" window. Select which window to restrict and click ok.



The window restriction will, by default, apply to all users connected to the database. You can tweak this in the "Window access restriction" window. You can create deviations from the window restriction by adding and providing individual users or group access.

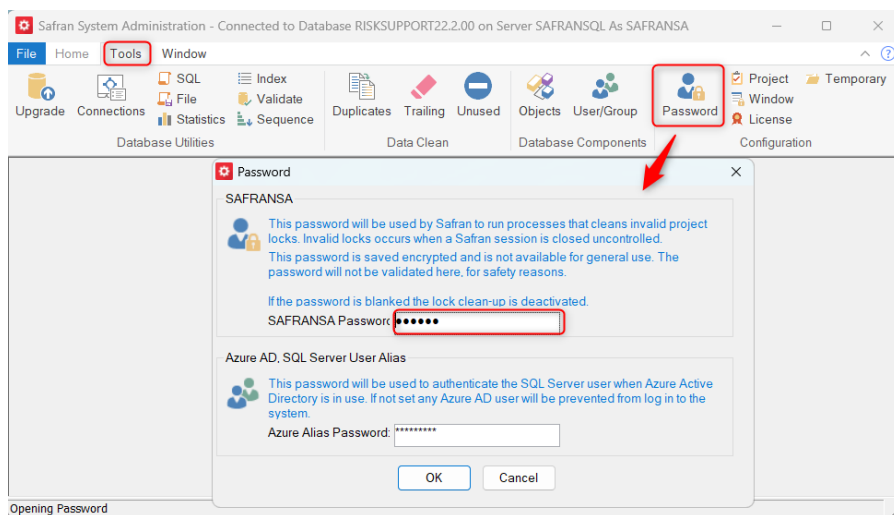


4.8. Activate cleaning of invalid locks in the database

Sometimes data in the database can remain locked, due to an unexpected end of some process accessing the database.

In order to allow Safran to clean up these locks automatically, follow this process.

1. If using Sql Server (not azure) make sure that the safransa user is granted "View Server State". This can be done using a tool like Sql Server Management Studio.
2. Start Safran System Administrator. (See section 4.1)
3. Click on Tools Password...



4. Type your safransa password and click ok.
5. Now you have activated the cleaning of invalid locks! Note that this will only work if your database owner is called safransa.

4.9. Managing the license

The parts related to licensing in the SysAdm tool are not relevant for Safran Risk!

4.10. Managing the Safran Database

This chapter contains information on how to initiate a new database for Safran, how to upgrade your Safran database to latest version and use the database utilities and

system objects features of Safran System Administration. For details on tables and table definitions please see the Safran System Guide – System tables and definitions.

4.10.1. Initiating a New Safran Database

For Safran Risk you should not use the SysAdm tool to create a new database. This will be done from Safran Risk!

4.10.2. Upgrade an existing Safran Database to latest version

For Safran Risk you should not use the SysAdm tool to upgrade a database. This will be done from Safran Risk!

4.11. Database Utilities

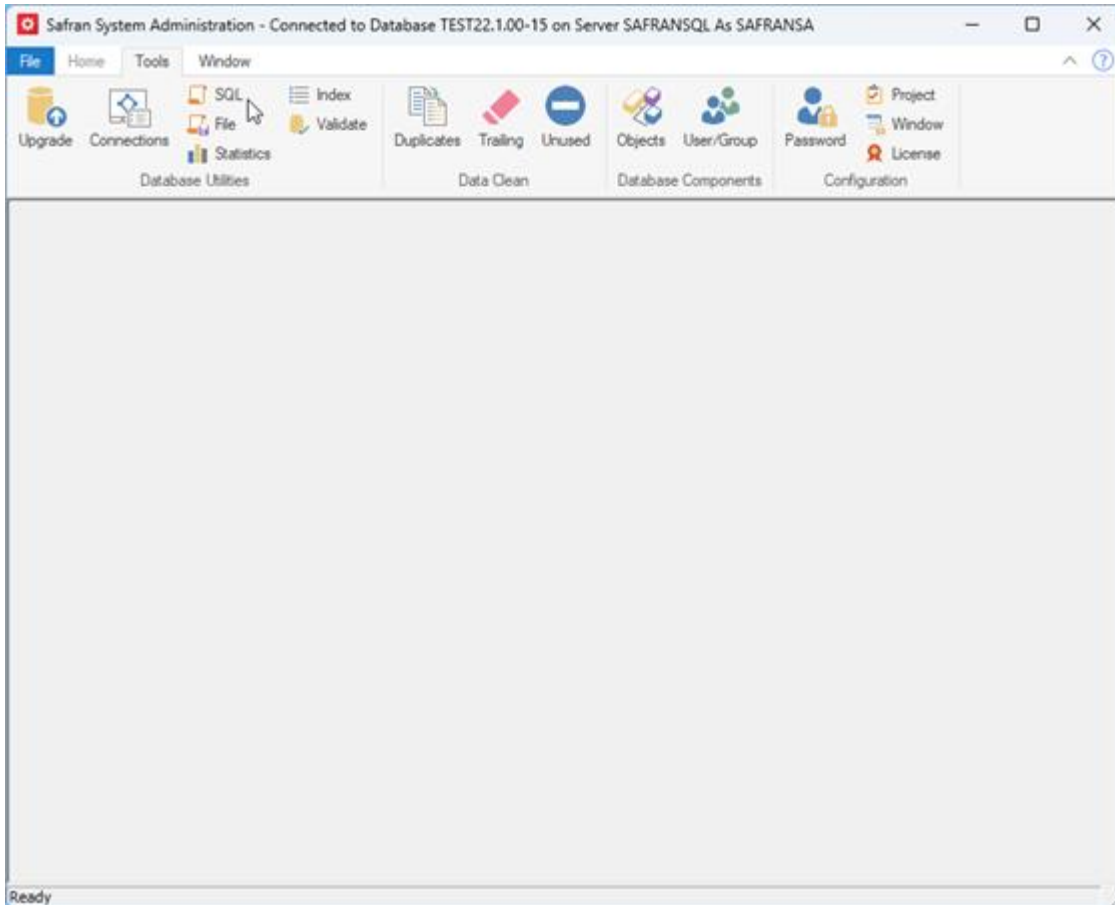
The database utilities of the database objects option allow you to:

- Execute SQL queries
- Run SQL command files and scripts
- Upgrade your Safran database (don't use for Safran Risk)
- See all current Safran users (MS SQL-Server only)
- Update Database Statistics (MS SQL-Server only)

4.12. Execute SQL Queries

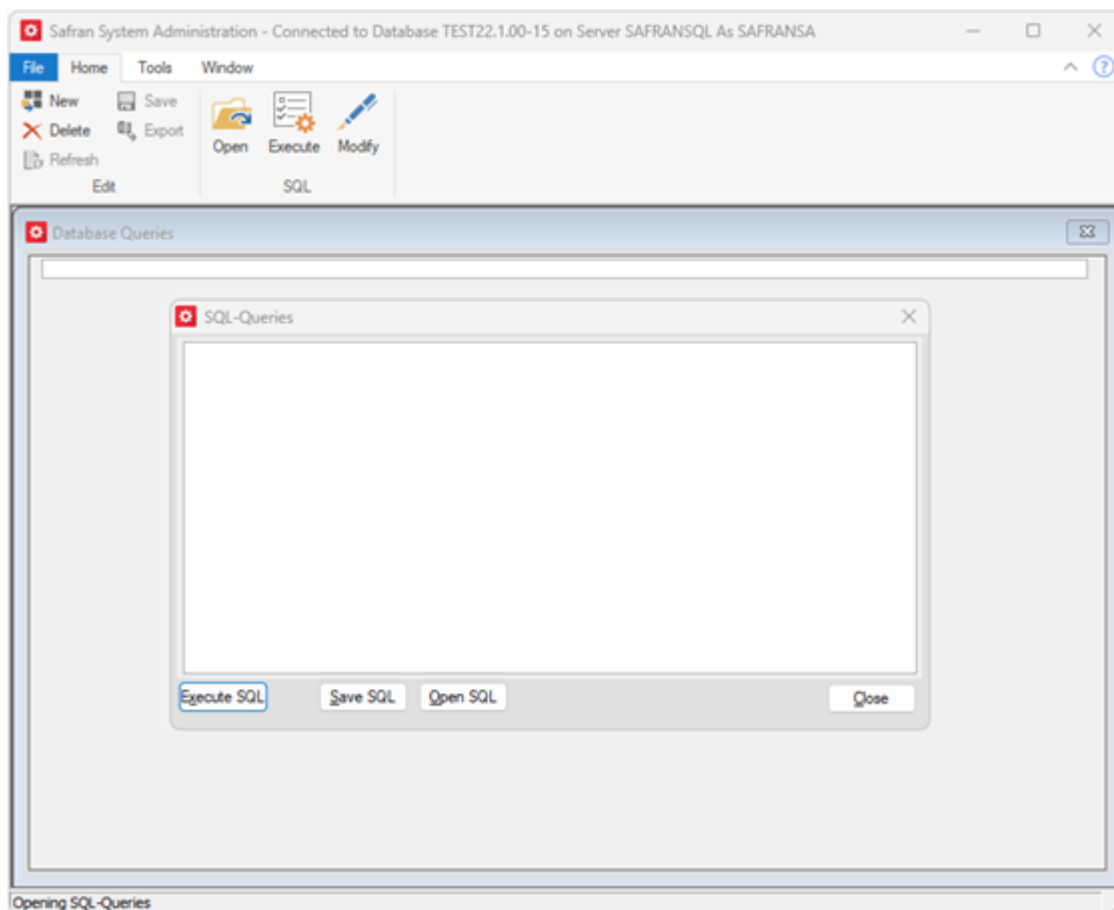
Warning: As a Safran Risk admin you shouldn't normally need this. Any mistake can result in the loss of data. If you feel that you need to use this, make sure you discuss with Safran Support First.

You can access the "Database queries" window from Tools -> SQL.



You may enter SQL commands here. You get a multiline input field if you double-click on the input line.

Note CAREFUL: commands entered here are executed and committed immediately when you click enter or the Execute button. Be careful what you ask for because you will get that! If you did something by mistake, you must either fix it manually or restore it from the database backup.



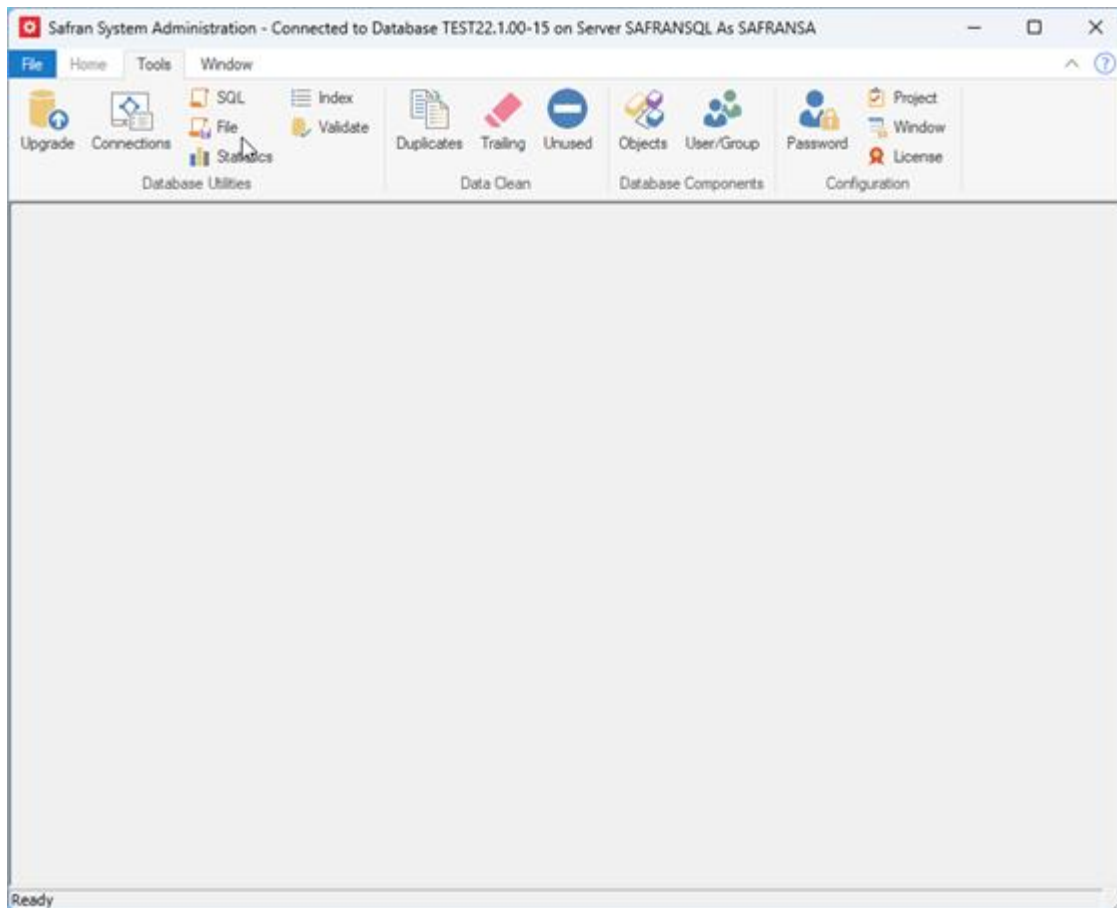
Running external applications using the Azure AD user will be limited, as the user only has read access to one table.

However, running the Safran Project "SQL Query" option still allows users to perform additional SQL queries as in previous versions.

4.13. Run SQL Command files

Warning: As a Safran Risk admin you shouldn't normally need this. Any mistake can result in the loss of data. If you feel that you need to use this, make sure you discuss with Safran Support First.

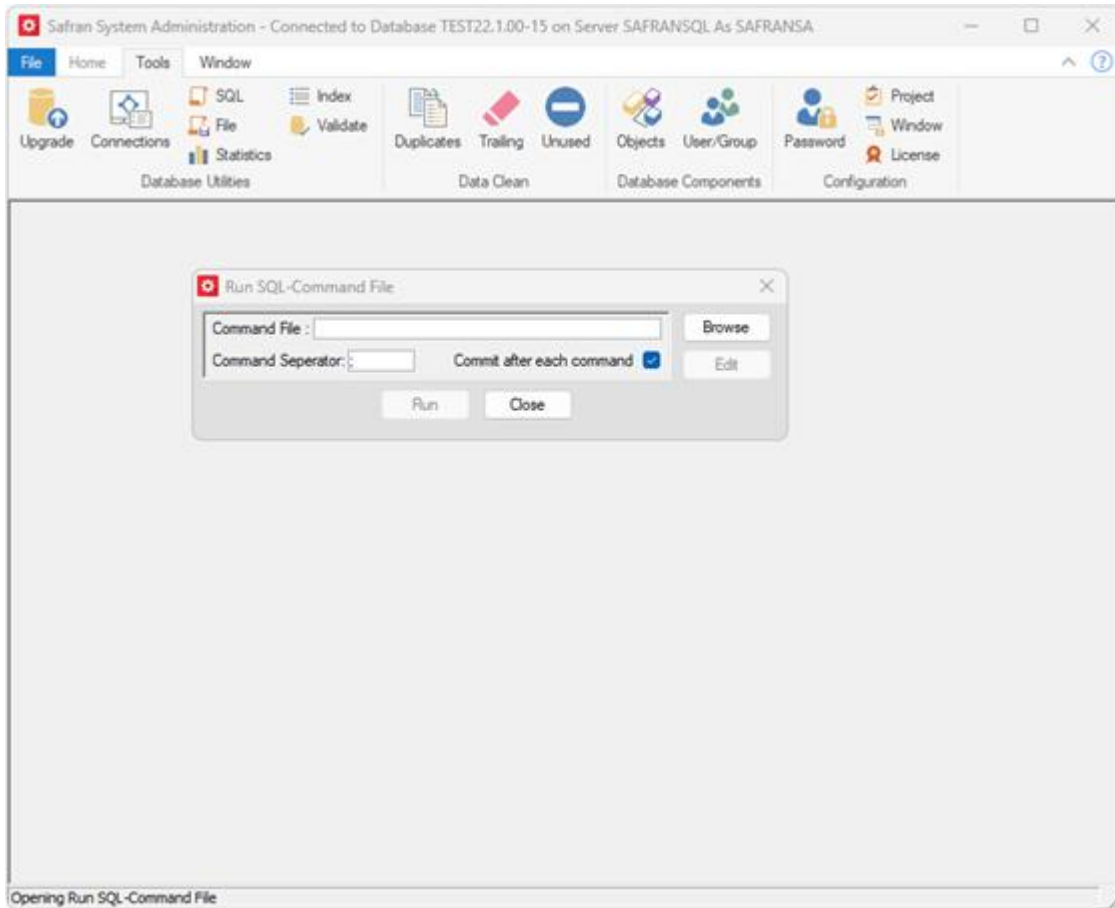
Access the "Run command file" window from Tools -> File.



You may browse and find the SQL command file you want to run.

You must also inform the system whether each command should be committed after execution (default) or all commits shall be done after execution of the document.

You must also specify the command delimiter used in the command file. The default is ";"



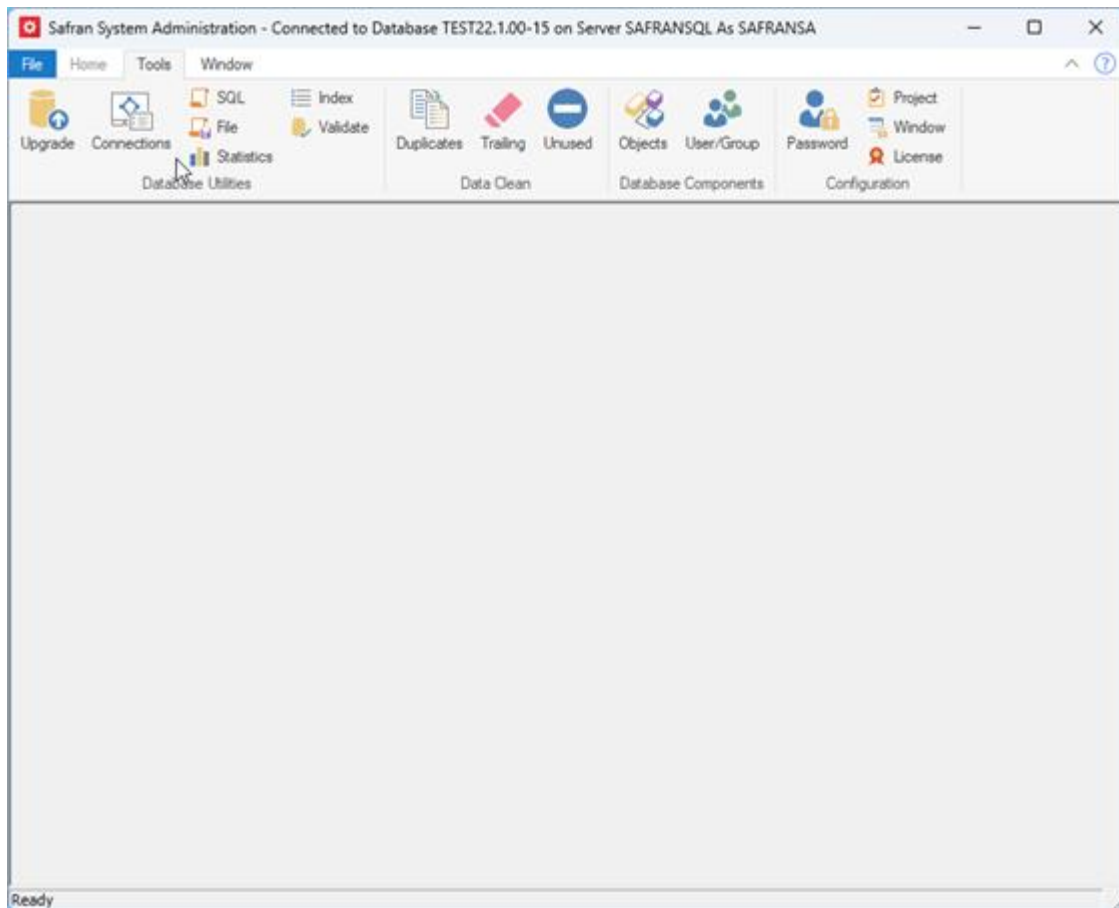
Click "Run" after finding the SQL command file you want to execute.

The system then executes the commands within the file, informing you of any (non-fatal) errors occurring during execution and giving you the options to continue or abort if errors occur.

When the operations are completed, the window gives you a message about the number of lines in the file.

4.14. See all current Safran users (MS SQL Server only)

You can see all active database connections by choosing Tools->Connections.



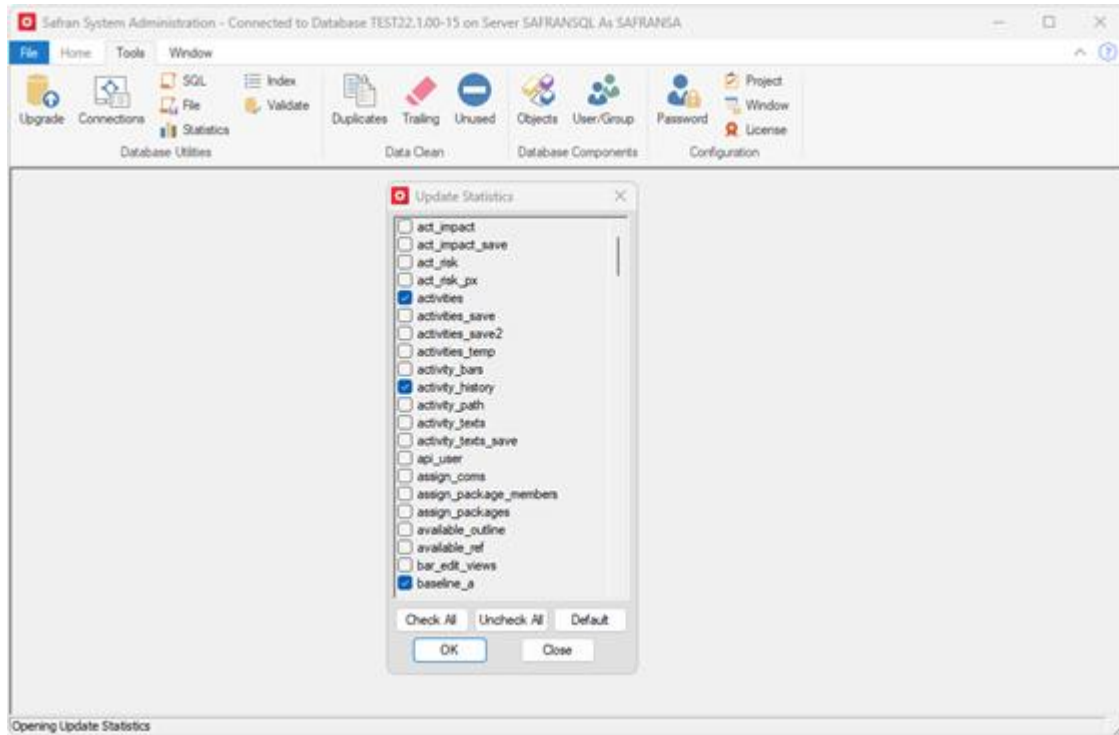
If you suspect that any Safran Project user hangs and that another process may cause this, you may select the "Show Blocked Processes Only"-option. This sets a filter on the users' list, showing only users waiting for a database lock to be released.

To identify the blocker, note the number under "Blocked by" and re-push the button (now renamed to "Show All Processes"). If the blocker is a Safran Project user, you can find him as a Process ID (If there are many users, pushing the "Process ID" header will sort the list on Process ID).

If the blocking process ID is not on the list, it does not belong to a Safran Project user.

4.15. Update Database Statistics

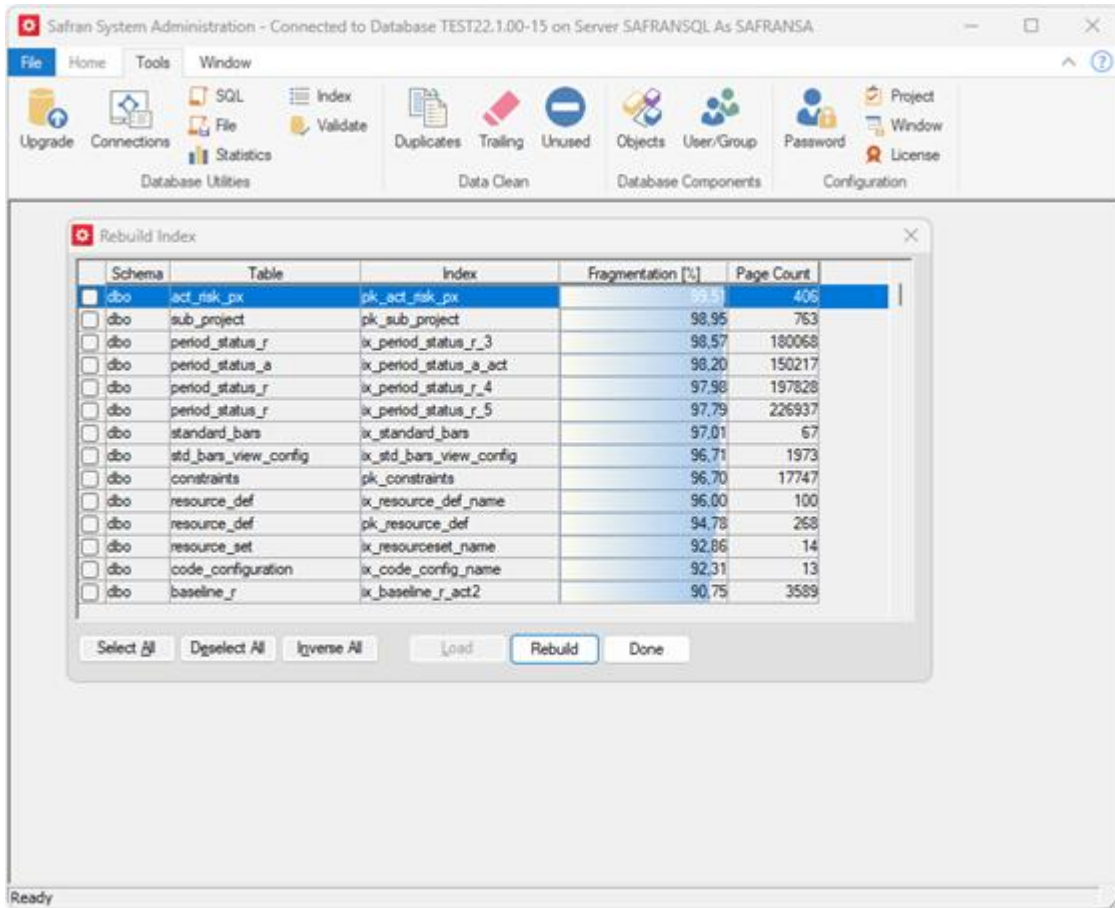
You may trigger an update of database statistics from Tools -> Statistics.



Select the tables you want to update from the "Update statistics" window and click ok. (Remember that updating statistics can also be configured as a scheduled task by the DBA in the DBMS. This is our recommendation.)

4.16. Rebuild Indexes

You may trigger a rebuild of the database indexes from Tools -> Index.

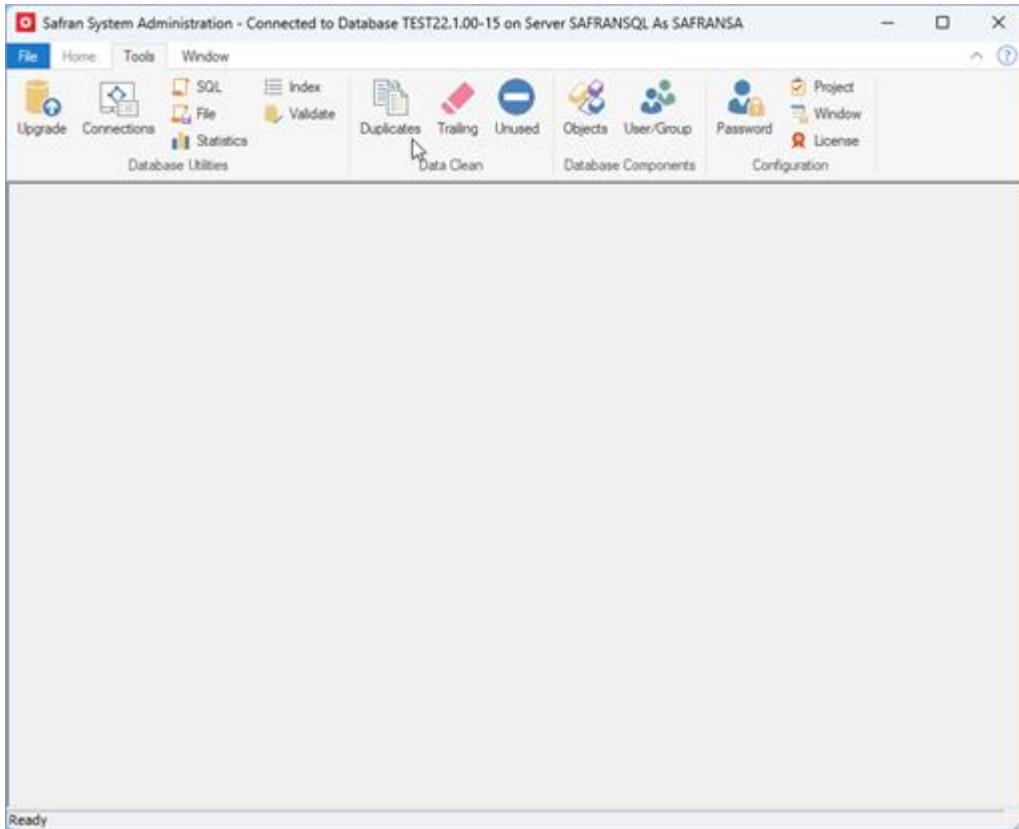


Click Load in the "Rebuild index" window. This will populate the window with information for all indexes.

You may select the indexes you want to rebuild and click "Rebuild" to start the process. (Remember that rebuilding indexes can also be configured as a scheduled task by the DBA in the DBMS. This is our recommendation.)

4.17. Removing database duplicates

The Safran System Administration tool can clean up duplicate objects from the database. This is done from Tools -> Duplicates. There is functionality to prevent duplicates from entering the database through Safran Project or Safran Planner. Still, it could happen if other systems are configured with access to the Safran database.



A window named "Remove duplicates" is displayed after clicking Tools -> Duplicates. This window lists the tables checked for duplicates; the column "Duplicates" tells you how many duplicate values there are in the different tables. You can clean this by clicking "Remove." The system will then add dup1 and dup2 endings to duplicate values to make each value different.

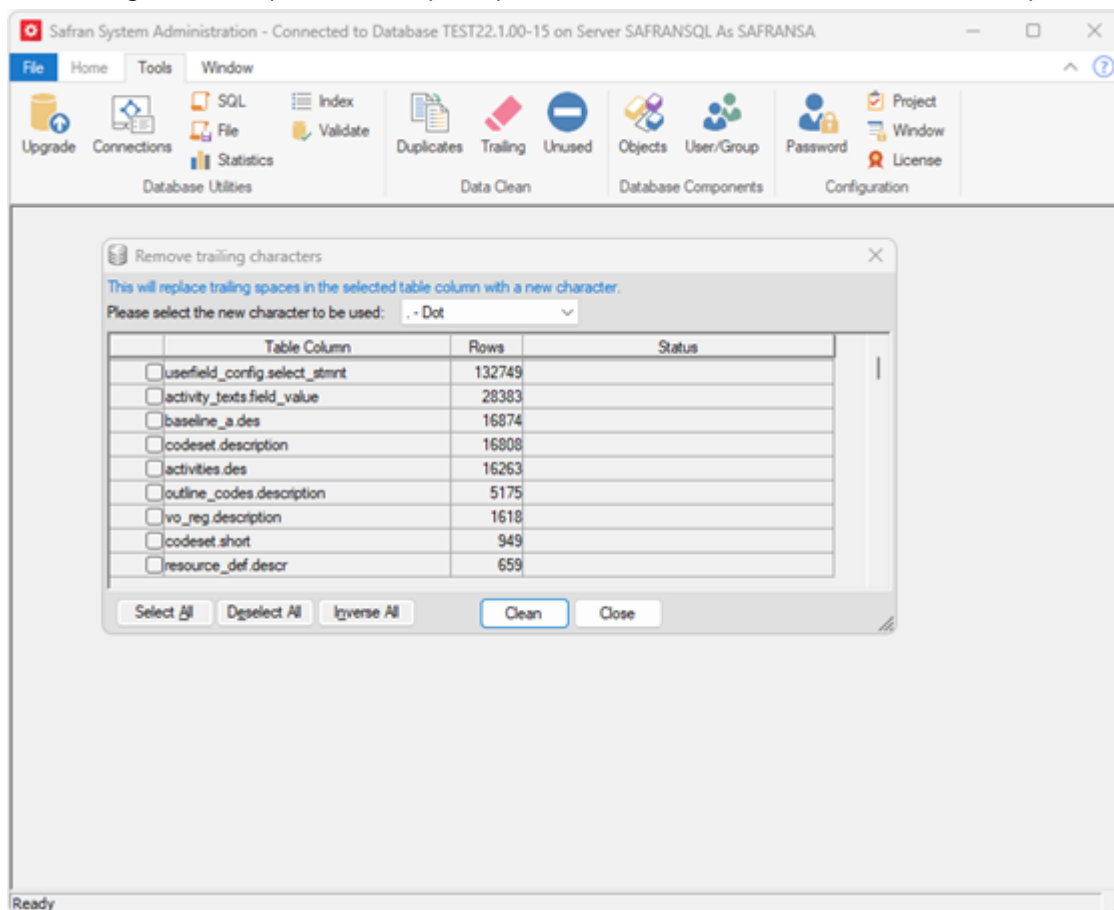
Table	Columns	Index	Rows	Duplicates	Status
filter_list	filter_name, owner, filterpk_filter_list		78	0	
pt_fonts	view_name, login_name, ix_pt_fonts		16663	0	
standard_bars	name, symbol_set	ix_name	21784	0	
window_defaults	net_id, login_name, windpk_window_defaults		6001	0	
resource_def	name, net_id	ix_resource_def_name	12388	0	
stdBarsViewConfig	style_id, symbol_set, viewix_stdBarsViewConfig		130586	46	
codeset	config_id, short, rfield_nr		1406201	0	
bar_edit_views	view_name, login_name, ix_beV_name		326	0	
edit_hist_views	view_name, login_name, ix_edit_hist_views		133	0	
rep_config	rep_name, user_name, six_rep_config_uni		568	0	
activities	an, net_id, rowid	ix_activities_an	1296843	0	

4.18. Remove trailing blank characters

The Safran System Administration tool can remove trailing blank/space characters from names in the database values. The empty/space character isn't deleted; you choose which character will replace the blank/space. This is done from Tools->Trailing.

Note: Use with Caution. This is something other than what you would usually do. Feel free to contact Safran Support for advice if you are unsure about this feature. There is no undo feature here, so remember to back up before performing this function.

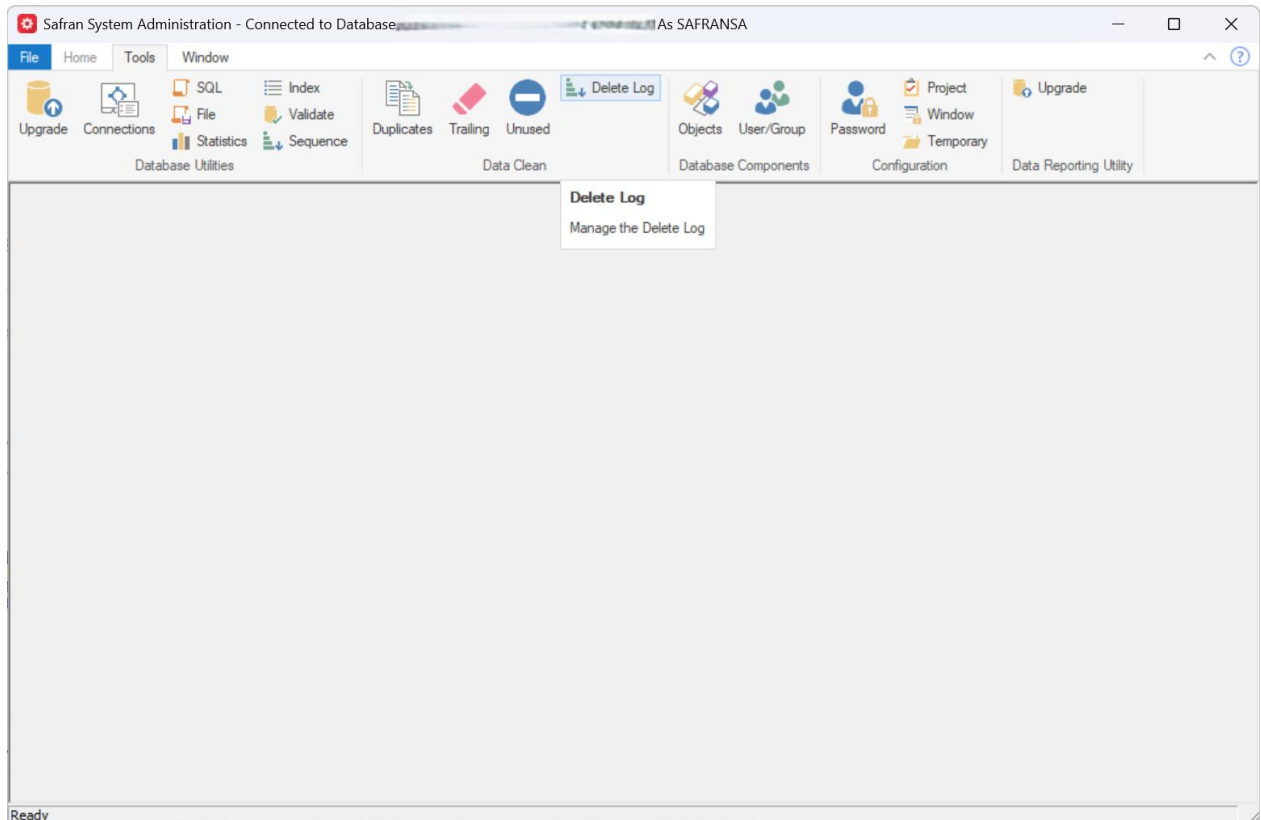
Restoring a backup is the only way to return if the function is mistakenly used.



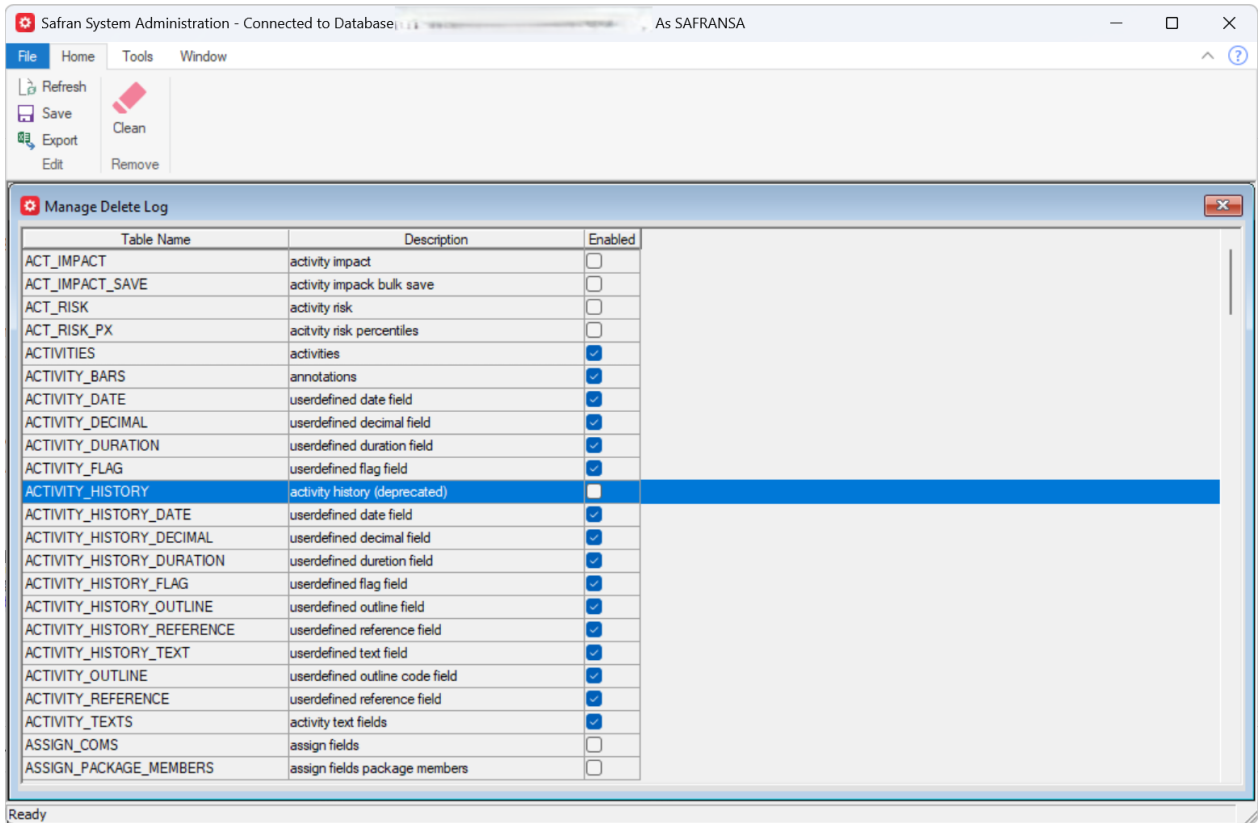
You need to select the replacement character from the drop-down list. Then, choose which tables you want to update before clicking clean. There is no undo feature here, so remember to back up before performing this function. Restoring a backup is the only way to return if the function was mistakenly used.

4.19. Delete Log

You may configure logging when a user deletes information in a database table using the Safran System Administration tool. This option is only available for system administrators.



A Manage Delete Log window will open when you click Delete Log from the Ribbon menu. The Manage Delete Log window lists the database tables and if they have the delete log enabled or not.



The system administrator can configure which database tables should be monitored using the enable switch. Click Save to save configuration updates if you have added or removed any database tables from monitoring. Clicking Export on the Ribbon menu enables an export of the delete log configuration to an Excel friendly format.

For those database tables that have delete log monitoring enabled, the information regarding the deletion of database table records are stored in the database.

There is also a remove option available from the Manage Delete Log window, this enables the configuration of how many days one would like to store information regarding deleted items. Older files will be deleted if they exceed the time limit configured.

5. Troubleshooting

Error message during installation of prerequisites.

In some rare instances you might see this error message during the installation of the prerequisites:

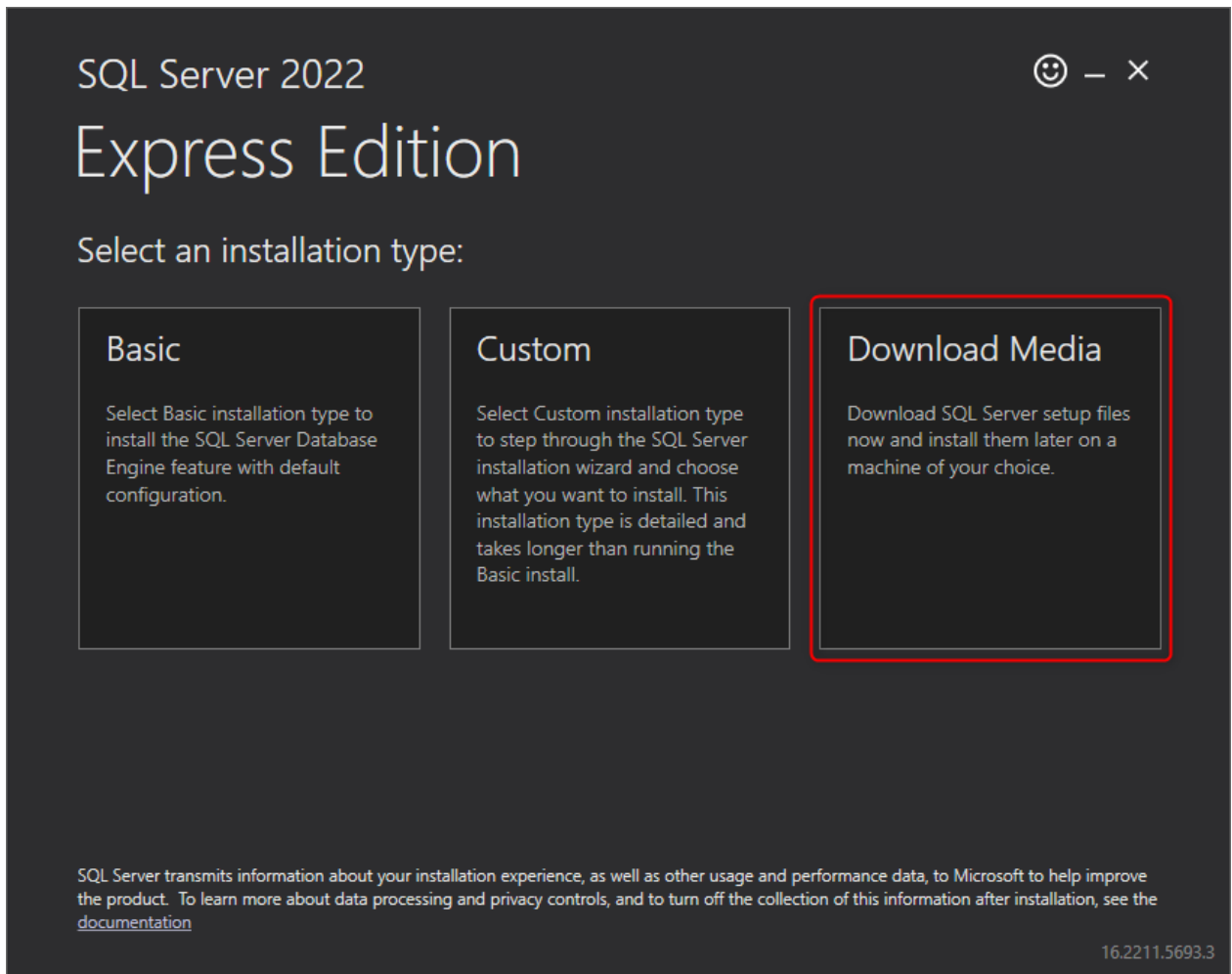


In these cases, it can help to install the prerequisites manually before installing Safran Risk.

The prerequisites and download links are:

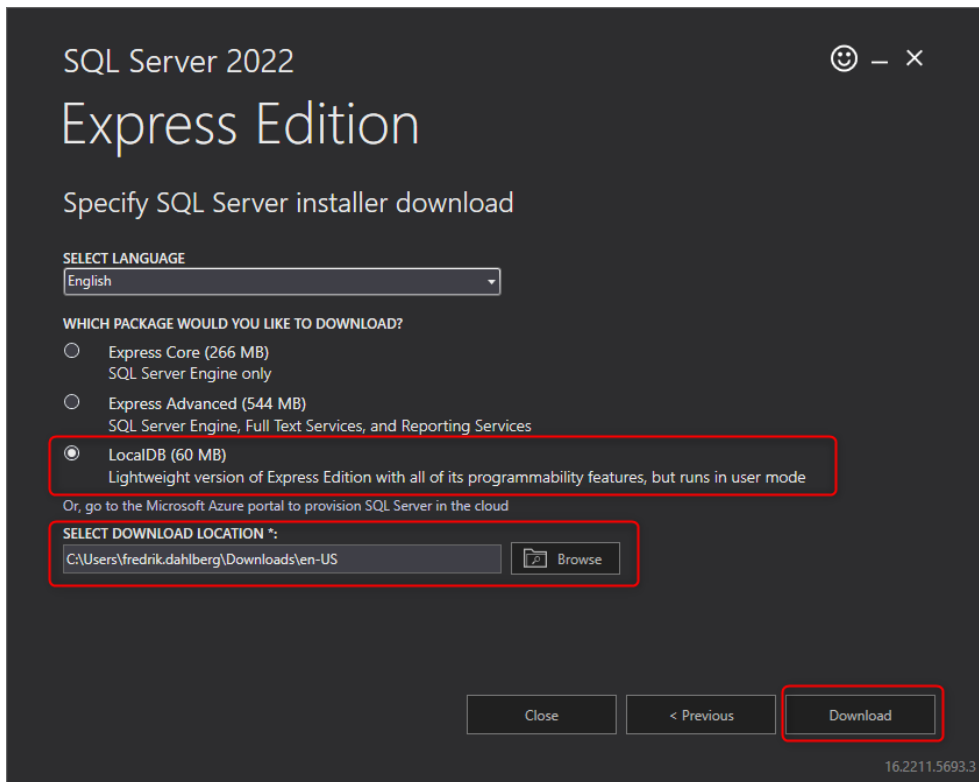
1. Microsoft OLE DB Driver for SQL Server
<https://go.microsoft.com/fwlink/?linkid=2117515>
2. Microsoft SQL Server 2022 LocalDB
<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/sql-server-express-localdb?view=sql-server-ver15>

When you run the installer choose "Download media"



then in the next screen select localdb, then location, and finally click download.

You will now have an msi file that you can run:



3. Microsoft Visual C++ 2015–2019 Redistributable (x64)

<https://download.visualstudio.microsoft.com/download/pr/3b070396-b7fb-4eee-aa8b->

[102a23c3e4f4/40EA2955391C9EAE3E35619C4C24B5AAF3D17AEAA6D09424EE9672AA9372AEED/VC_redist.x64.exe](https://download.visualstudio.microsoft.com/download/pr/3b070396-b7fb-4eee-aa8b-102a23c3e4f4/40EA2955391C9EAE3E35619C4C24B5AAF3D17AEAA6D09424EE9672AA9372AEED/VC_redist.x64.exe)

Download the three files (two msi and one .exe) and install them one by one. Then try to install Safran Risk again.

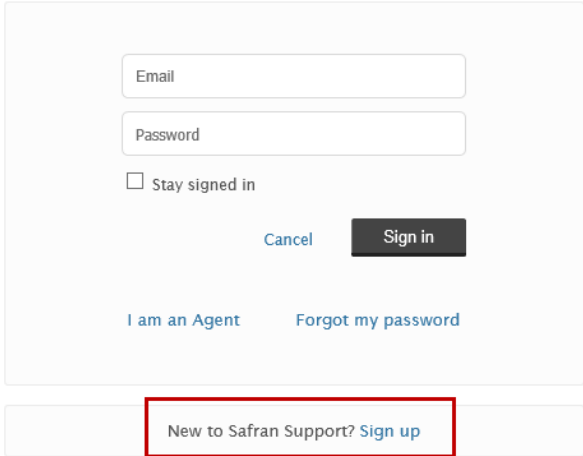
6. Contact Safran Software Solutions AS.

Submit a request online: <https://support.safran.com/>

When entering our support site, the first time you should choose Sign In. When on the Sign In page choose New to Safran Support. You will then become a registered Safran Support user with a username and password for future Sign In's to the site.



Sign in to Safran Support



Have you emailed us? [Get a password](#)

If you've communicated with our support staff through email previously, you're already registered.

You probably don't have a password yet, though.

Email address: support@safran.com

Telephone: +47 40 00 47 07