



IDL Konsis

Installing the Application

23/03/2022

Content

1.	About this document.....	3
2.	Preliminary remarks	5
3.	Architecture of IDL Konsis	5
3.1.	Configuration scenarios	6
3.2.	Client connection	7
3.3.	Interfaces	10
4.	Preparation and planning for installation	11
4.1.	Recommended installation procedure (for new installation).....	11
4.2.	Preparation when using Microsoft SQL database server.....	11
4.3.	Preparation when using the Oracle database server.....	12
5.	Installing the Application.....	13
5.1.	New installation of the application and installing the source database.....	13
5.2.	Updating the application	14
6.	Reassigning public rights for views to a new role if required	15
7.	Configuring the Application Server	16
7.1.	General settings	17
7.2.	Network settings.....	18
7.3.	Database driver	19
7.4.	Configuring the database.....	20
7.5.	SSL certificates and KeyStore	23
8.	IDL Konsis – client installation.....	31
9.	Launching the IDL Konsis application.....	34
9.1.	Launch via the IDL Portal	34
9.2.	Launch with IDL LAUNCHER	36
9.3.	Installed client – launch with installed start icon	38
10.	The login dialog box in IDL Konsis	39
	Host and port	39

Proxy settings.....	39
Username and password	39
11. User authentication.....	40
12. Notes on virtualisation	44
13. Documentation	45
14. IDL support	46

1. About this document

Changes to this document

The information contained in this document is subject to change. “insightsoftware Deutschland GmbH” assumes no warranty in this respect.

“insightsoftware Deutschland GmbH” has exercised all due care to ensure that the information published in this document is accurate and assumes no warranty, no legal responsibility, or any liability for the use of this information. No liability shall attach to Insightsoftware Deutschland GmbH for any losses attributable to a malfunction of programs, etc., including for the breach of patent rights or other third-party rights arising as a result.

Copyright

Copyright © 1992-2022 “insightsoftware Deutschland GmbH”. All rights reserved.

No part of this document may be reproduced, transferred, stored in a data retrieval system, or translated into another language without the prior consent of “insightsoftware Deutschland GmbH”.

This documentation is protected both by copyright laws and international copyright provisions and also by laws that protect intellectual property.

Intellectual property rights

IDL® is a registered trademark. Microsoft Windows is a registered trademark of the Microsoft Corporation. SAP®, SAP R/3®, SAP Business Information Warehouse® and SAP NetWeaver® are registered trademarks of SAP AG, Walldorf, Germany. All other trademarks referred to in this documentation are trademarks belonging to the respective holders.

Limitation of liability

The information set out in this document may not be modified without prior notice and does not constitute an obligation. “insightsoftware Deutschland GmbH” or its suppliers will not under any circumstances be held liable for any specific, incidental, indirect or consequential losses (including, without limitation, lost profits, interruption of ongoing business operations, loss of business information or any other monetary loss) up to the maximum amount permitted by law. In particular “insightsoftware Deutschland GmbH” will not assume any liability where the documentation is used defectively or improperly or if no precautions have been taken to avoid potential damage.

2. Preliminary remarks

This manual is aimed at IT administrators and explains all of the steps that need to be performed to install IDL Konsis. After you have read the manual, you will be able to install IDL Konsis. If any questions are not answered in the manual, please contact IDL Support. You can find the contact details in the final chapter [IDL Support](#).

3. Architecture of IDL Konsis

Starting with the 2014 release, IDL Konsis was supplied with the new Jetty-based¹ Application Server, which communicates using the HTTPS protocol. The Application Server handles all communication with the IDL Konsis database, meaning that the IDL Konsis client only sends its requests to the IDL Application Server, which retrieves the data from the database and returns it to the client as a bundle. Further, the new IDL Application Server also provides web services that enable, for instance, current user sessions to be monitored. The Application Server runs in 64-bit mode. New functionality requires that software components for the Application Server and the client software are strictly separated from one another. As a result, the client software always needs to be launched in addition to the server software. IDL Konsis essentially consists of the following three components:

¹ Jetty is a servlet container and a web server that requires a Java Runtime Environment. With its simple architecture and small size, it can be easily integrated into applications such as IDL Konsis.

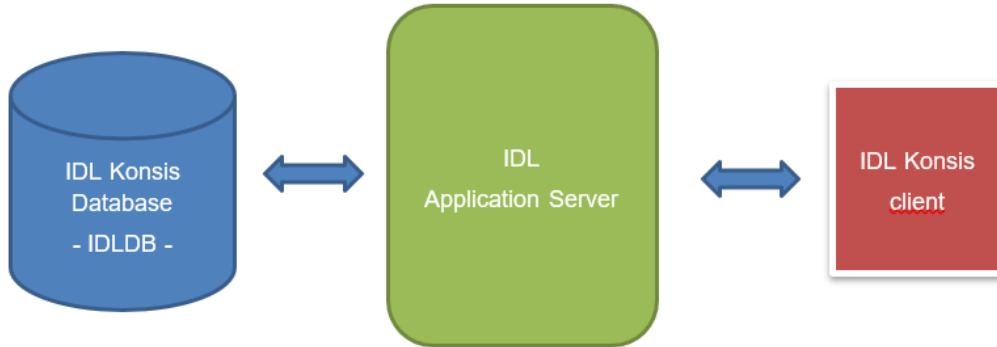


Figure 1 Database architecture – Application Server – client

The Application Server can provide multiple database connections to different IDL Konsis databases. However, the release level of the IDL Konsis database must be consistent with the release of the Application Server.

3.1. Configuration scenarios

The Application Server is a service that is often installed on a separate computer – usually a dedicated server with a Windows Server operating system. The database or the database management system may also be located on this server or also on a separate database server.

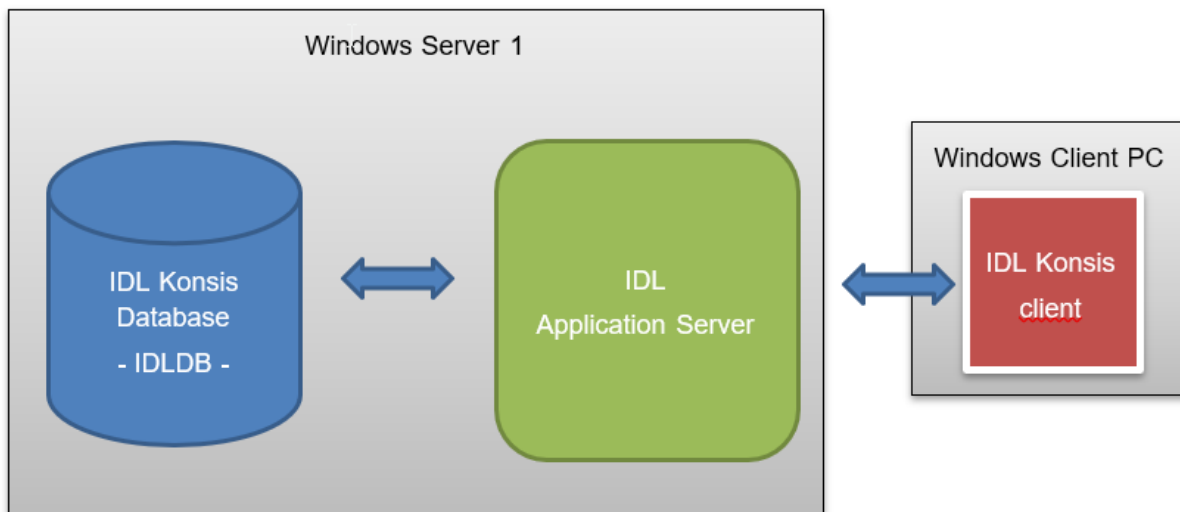


Figure 2 Database and Application Server on the same server

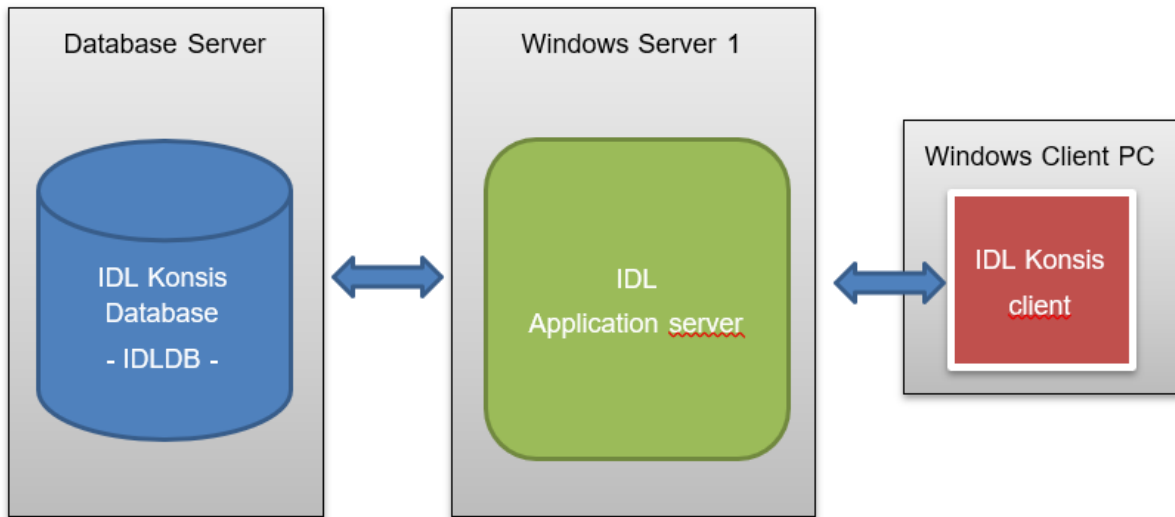


Figure 3 Database and Application Server on separate servers

Because the client only communicates with the Application Server using the HTTPS protocol and the Application Server in turn communicates with the IDL Konsis database through a secure channel, the database driver only needs to be installed on the server with the Application Server.

If a Microsoft SQL server is used as the database system, these drivers are preinstalled on the server with a Windows Server operating system.

3.2. Client connection

Two basic types of client connection are possible: either the installed IDL Konsis client is used to launch IDL Konsis, or the application is automatically downloaded and launched using the automated IDL LAUNCHER process.

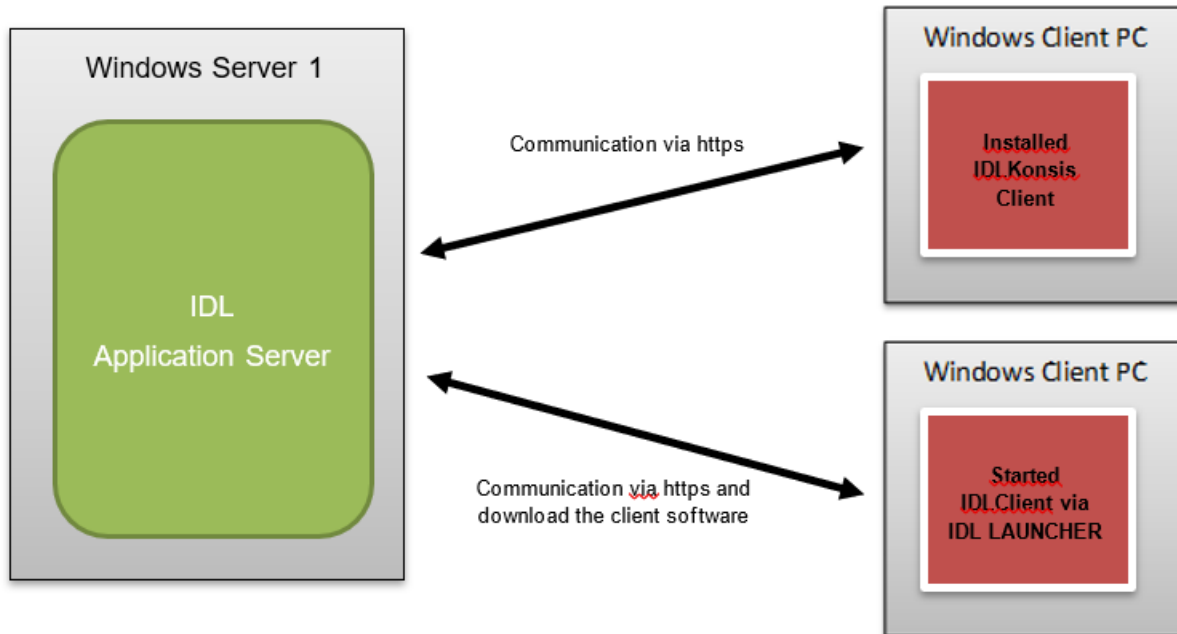


Figure 4 Application Server and client

The client software essentially a pure Java application that requires a Java Runtime Environment (JRE). This is included in the delivery. The two client types differ in terms of how the client and the JRE are installed.

Installed IDL Konsis client

The installed client includes the full functional scope of the client for IDL Konsis. This is installed on the client via a Windows installer, usually in the x86 program path.

The following components are installed:

- IDL Konsis
- IDL Xlink
- Interface components (kcusap.exe, rstart.exe) for legacy systems such as SAP, Navision etc.
- Java Runtime Environment (compatible with the release)

As the client software is versioned via the installer mechanism, only one release may be installed at a time. Different versions of parallel clients are not possible on the user computer.

A database driver is no longer required on the client computer.

Calling the application via IDL LAUNCHER

The key difference to the installed client is that the client software is downloaded on to the client computer via the IDL LAUNCHER mechanism. This requires an IDL LAUNCHER to be installed on the client computer.

When launching the client, the user first uses their browser (IE, Firefox, Edge etc.) to connect to the IDL Application Server launch page. The IDL LAUNCHER mechanism automatically downloads the client software in the form of JAR files.

The client software is not installed in the program directory but is placed in the user's profile on the client computer. IDL Konsis is automatically launched once the software has been successfully downloaded. The software is not downloaded anew each time, but rather the IDL LAUNCHER mechanism checks whether a current version already exists. The client software is only downloaded when the client software on the server is newer than the client software in the user's profile. This is always the case when IDL Konsis has been updated on the server.

Advantages:

- Guarantees that the client software on the client is always up to date.
- The client does not require installation of the software and administrative rights.
- Multiple versions may run in parallel (e.g. test and live environment).

Disadvantages:

- Cannot be used if interface processes for legacy systems are in use, e.g. via the IDL Importer (rstart.exe) or the old SAP interface (kcusap.exe).

Area of use: The call via IDL LAUNCHER is a good option for users who access IDL Konsis from other locations, for whom the installation of the IDL Konsis client is more difficult and who do not launch any interface processes.

3.3. Interfaces

Special features of the old SAP interface (kcusap.exe)

The configuration file “kcusap.ini” required for SAP access was usually located centrally in the system folder on the server. In these cases, the configuration file can be stored, for instance, in a system directory (in parallel to the export/import/batch paths).

Special features of the interface for legacy systems / SAP via the IDL Importer

In most cases, the interface via the IDL Importer still requires access to a release on the Application Server. The IDL Importer generates log files and a temporary interface file that needs to be read by the IDL Konsis client. This release should be set up so that it only contains the files and directories relevant for the IDL Importer. Similarly, the configuration file “kcusap.ini” required for SAP access must be placed in a different directory. It is recommended that the configuration file is placed in a system directory in the ###approved directory for the IDL Importer files. The path to the configuration file must be managed in the options.

4. Preparation and planning for installation

You will obtain the licence file required for a new installation via our sales team. The current hardware and software requirements can be found on the Insightsoftware customer portal at <https://help.insightsoftware.com/s/?language=en>

4.1. Recommended installation procedure (for new installation)

- Install the database server (if existing solution is not being used)
- Create the IDL Konsis database
- When using an Oracle database, the Oracle database client for the IDL Application Server is also installed
- Install the source database
- Install IDL KONSIS (Server Installation)
- Configure, install, and launch the IDL Application Server
- Install any existing fix pack
- Install the IDL Konsis client
- Reassign “public” rights for views to a new role as required
- Call the IDL Konsis application
- Login to IDL Konsis, first setup of user “idladmin” in the “voradmin” module
- Set up additional users

4.2. Preparation when using Microsoft SQL database server

When using Microsoft’s SQL database server, please refer to the corresponding documentation from Microsoft. Please note:

- Microsoft suggests using Windows NT authentication for login. Switch to mixed mode here. Mixed mode activates both Windows authentication as well as SQL server authentication.
- The selected collation should be “Latin1_General_CI_AS”. Other collation methods may cause errors when logging on or accessing the tables/views.
- If possible, the IDL Konsis database should not be located on the system partition.

Creating the database

Create a new database using Microsoft SQL Management Studio (SSMS). We recommend “**idldb**” for the name of the database.

Database users

IDL Konsis requires the following technical database users who need to be set up for access to the IDL Konsis database: **“idldb”**; **“idlwps”**, **“idlapp”**, **“idladmin”**. These database users must be created with SQL-authentication. All technical database users should similarly be configured so that they use the IDL Konsis database (usually idldb) as the default database. It is still recommended that complex passwords are used for all users. System-related restrictions apply to special characters in the password for the technical database user **“idlapp”** (ASCII code < 128). The following characters are permitted: a-z A-Z 0-9 ä ö ü Ä Ö Ü _ . * - + : # ! ? % { } | @ [] ; = “ & \$ / ()

- **idldb**: This is required for updating the IDL Konsis database. The user needs database owner rights (DBO) in the IDL Konsis database.
- **idlwps**: Required as an interface user for the DataMart and reporting. Because this database user also needs to create tables in the IDL Konsis database, this user must similarly have database owner rights (DBO).
- **idlapp**: This user is used by the Application Server service to access the IDL Konsis database(s). The user **“idlapp”** does not require any further permissions.
- **idladmin**: This user is used for administrative tasks within IDL Konsis. Initial setup and creation of users within IDL Konsis are performed via this user. The user **“idladmin”** does not require any further permissions.

User mapping of the technical database users

The technical database users must be mapped to the IDL Konsis database in the user mapping. The default schema in the user mapping for the IDL Konsis database is always **“idldb”**. All database users are automatically assigned the **“public”** database role.

4.3. Preparation when using the Oracle database server

Please use the Oracle documentation provided for installing the Oracle Database server and the Oracle Database client. Once unpacked, this can be found in the following directory of the current software package under **“Konsis\Doku\Installation\ENG”**.

- Oracle_12cR1_Installation_deu.pdf
- Oracle_12cR2_Installation_deu.pdf
- Oracle_19cR3_Installation_deu.pdf

Important:

- The IDL.Application Server must **not** be installed on a server on which a 64-bit Oracle database server is also running.
- It must be ensured that an Oracle client is installed on the IDL Application Server:
 - If no IDL Designer is being used, a TCP/IP driver is recommended. In this case, a 32-bit Oracle DB client installed on the IDL Application Server is sufficient.
 - If the IDL Designer is used in addition to IDL Konsis, a native database driver is deployed on the IDL Application Server. In this case, IDL Konsis also requires a 64-bit database client in addition to the 32-bit database client. If this is the case, the OLE DB provider must not be installed with the 64-bit database client.
- As a rule, “tnsnames.ora” is present on the Oracle client and contains the entry for the IDL Konsis database. Alternatively, a TNS_ADMIN environmental variable can be defined that points to the directory that is on the network as a ###release and contains the “tnsnames.ora”.

Please use tnsping for a command-line check of whether the IDL Konsis database can be reached. Please contact your Oracle administrator if you have further questions.

5. Installing the Application

Starting from the 2016 release, IDL KONSIS requires the installation of a dedicated Application Server service. The client communicates with the Application Server service via HTTPS. The clients can also access the Application Server service via a proxy. Part of the functionality of the Application Server service can also be accessed using a browser, for instance, the launch page of the IDL Konsis Application Server, the download of the client setup and the launcher. In addition, this page provides an option for monitoring the IDL Konsis Application Server. The network connection requirements are set out in our document on hardware and software requirements.

5.1. New installation of the application and installing the source database

To complete a new installation, the licence file (licence.xml) must be available. This file can be obtained from our Sales team.

To install IDL Konsis, open the “\Konsis\install” directory on the installation medium, and from there launch the application “install.exe”. First, select the language in which the installer will communicate with you. Select the language and confirm with the [OK] button. Information will now be requested. Once a selection has been made, the [Next] button can be used to jump to the next page. Return to the previous page if you have entered something incorrectly by pressing the [Back] button.

- **Product information input:** Here you can choose between a server installation or a server installation with start icon.
- **Select maintenance type:** New Installation or update of an existing system. The latter only works if an IDL KONSIS installation is already present.
- **Installation path:** The Windows Program Files directory is suggested.
- **Specify licence file:** Select the file “licence.xml” here.
- **Overview of installation parameters**

The installation is launched using the [**Install**] button.

Note: We recommend installing with start icons. In this case, icons to launch IDL Konsis and the Application Server configuration program will be created.

Note on installing the source database

The source database can be installed from release version 2021 update 1 and above in the installation setup. Select the “Create source database” option. During the further course of the setup, the database system (MSSQL or Oracle), the name of the database, username and password will be requested. The database user “**idldb**” must always be used both to set up the source database and to update the IDL Konsis database as this user has the necessary permissions. When creating the source database, the tables and views are created first. The metadata is then populated and finally the foreign keys are created.

5.2. Updating the application

The database and programs can be updated separately from one another (e.g. with different responsibilities). However, it should be noted here that this should not be done too far apart, as IDL Konsis can only be used if the database and program versions match. Open the directory “\Konsis\install” on the installation medium, and from there launch the application “install.exe”.

First, select the language in which the installer will communicate with you. Select the language and confirm with the [**OK**] button. Information will now be requested. Once a selection has been made, the [**Next**] button can be used to jump to the next page. Return to the previous page using the [**Back**] button.

- **Product information input:** Here, too, you can choose between a server installation or a server installation with start icon.
- **Installation type:** New Installation or update of an existing system.
- **Installation path:** Where is the IDL KONSIS application located? The path to the root directory for IDL KONSIS is sufficient here.
- **Update database:** If marked, the database will be updated.
- **Update program:** If marked, the program will be updated.
- **Heed the warning regarding the database backup!**
- **Select database system:** *Microsoft*® SQL Server or Oracle.
- **Parameters for the database update:** For Oracle, it is sufficient to enter the database name in the “Database” field.

When using Microsoft SQL Server with an IDL Konsis database, the following syntax applies for updating the database. `<hostname>[\named instance] .<databasename>`

Please enter the username “**idldb**” in the “**Username**” field, and the password that you have set for the user “**idldb**” in the “**Password**” field. The installation is launched using the [Install] button.

6. Reassigning public rights for views to a new role if required

The “public” role is a standard role in database usage and is used by both Oracle and *Microsoft*® SQL Server. However, the “public” role can affect the security policies of a company or a data centre. For that reason, capability has been created to enable the mapping of the “public” role to be changed to a different role of your choice in the views. To change this mapping, please contact IDL support. We will provide you with support or send you an instruction manual at your request. When using Oracle, SQL scripts are provided to give a new role permission for the views.

Notes

- Changes of this nature represent a modification of the database itself. Make sure that you have backed up the database beforehand. This will enable you to restore the database in the event of an error.
- Each update that involves changes to the database will reset the role back to “**public**”, This is why it is necessary to perform the relevant steps again to modify the role after each update.
- Alongside the technical users `idlapp`, `idladm`, `idlwps`, all other SQL-authenticated and NT-authenticated (SSO) database users also need to be connected to the new database role.

7. Configuring the Application Server

Once IDL Konsis is successfully installed, you will be asked if the configuration program for the Application Server should be launched. We recommend performing the configuration right away. However, the configuration can also be performed or modified at a later time. The Application Server must be correctly configured for the client to successfully communicate with the server. The following sections describe the individual pages of the configuration program. Once the configuration program “configure.exe” is launched, a launch page will first appear on which you can select a language.



Figure 5 Configurator for language selection

Select the language in which you wish to perform the configuration here.

7.1. General settings

IDL Konsis Configuration

Common Configuration

1. Common Configuration 2. Network configuration 3. Database Driver 4. Database Configuration 5. SSL-Certificate-KeyStore	Hosts (e.g. Host1, Host2)	<input type="text" value="idl-server.insightsoftware.com"/>	<input checked="" type="checkbox"/> Bind service to all network interfaces
	Default-Port	<input type="text" value="81"/>	
	SSL-Ports (e.g. Port1, Port2)	<input type="text" value="444"/>	
	Stop-Port	<input type="text" value="7853"/>	
	Memory (MB)	<input type="text" value="8192"/>	Please uninstall service and install service again!
	IDL Launcher Host (optional)	<input type="text"/>	
	Financial-Reporting-Host (optional)	<input type="text"/>	
	Portal-Url (optional)	<input type="text"/>	<input checked="" type="checkbox"/> disable statistics
	Service-Name	<input type="text" value="IDLAppServer"/>	Delete Service Not installed
	Service-Displayname	<input type="text" value="IDL Application Server"/>	Delete Service Not installed
Client Inactivity Timeout	<input type="text"/>	minutes	

back next Finish

Figure 6 Configuration of general settings

- **Hosts:** This is where the name of the server is specified under which this service can be reached. This is generally just a single server name, but several server names may be specified separated by commas. The hostname or FQDN (fully-qualified domain name) is accepted.
- **Bind service to all network interfaces:** Servers may have multiple network adapters. Marking this option this will bind the service to all network adapters.
- **Default port:** Port for the HTTP protocol (default: 81).
- **SSL ports:** Port(s) for the HTTPS protocol (default: 444). Multiple entries must be separated using commas. This port/these ports are used for the client/server connection.
- **Stop port:** Port for stopping the Application Server (only used internally).
- **Memory (MB):** Specify the maximum required memory of the Application Server here. This amount of memory will be used jointly by all clients. This value should be based on the circumstances of your physical or virtual machine.
- **LAUNCHER host (optional):** This only needs to be specified if the client is **not** intended to be rolled out by the Application Server itself via LAUNCHER.

- **Financial reporting host (optional):** This field is not currently in use
- **Portal URL (optional):** If ad-hoc and web reporting are to be used, the URL of the IDL portal can be configured here.
- **Service name:** The service name of the Application Server is entered here.
- **Displayed service name:** A meaningful displayed service name can be entered here. Spaces are also permitted in names. The default is “IDL Application Server”.
- **Client inactivity timeout:** Disconnection after inactivity in min.

Note: By default, port 80 is used for HTTP and port 443 for HTTPS. However, past experience has shown that port 80 is frequently occupied by the reporting service of Microsoft’s SQL Server. Port 443 may also be occupied by other applications (e.g. Internet Information Server). Because the Application Server service can only be bound to free ports, ports 81 and 444 in the configuration program have been preset.

7.2. Network settings

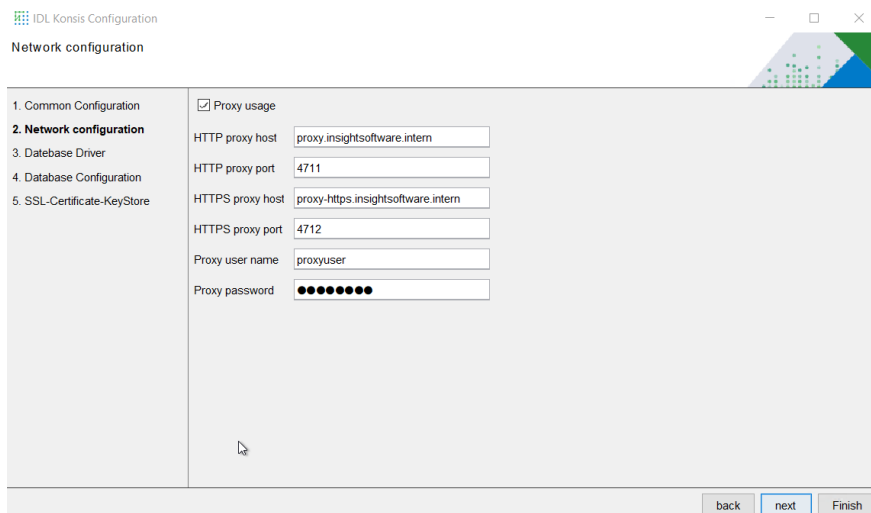


Figure 7 Configuration of network settings

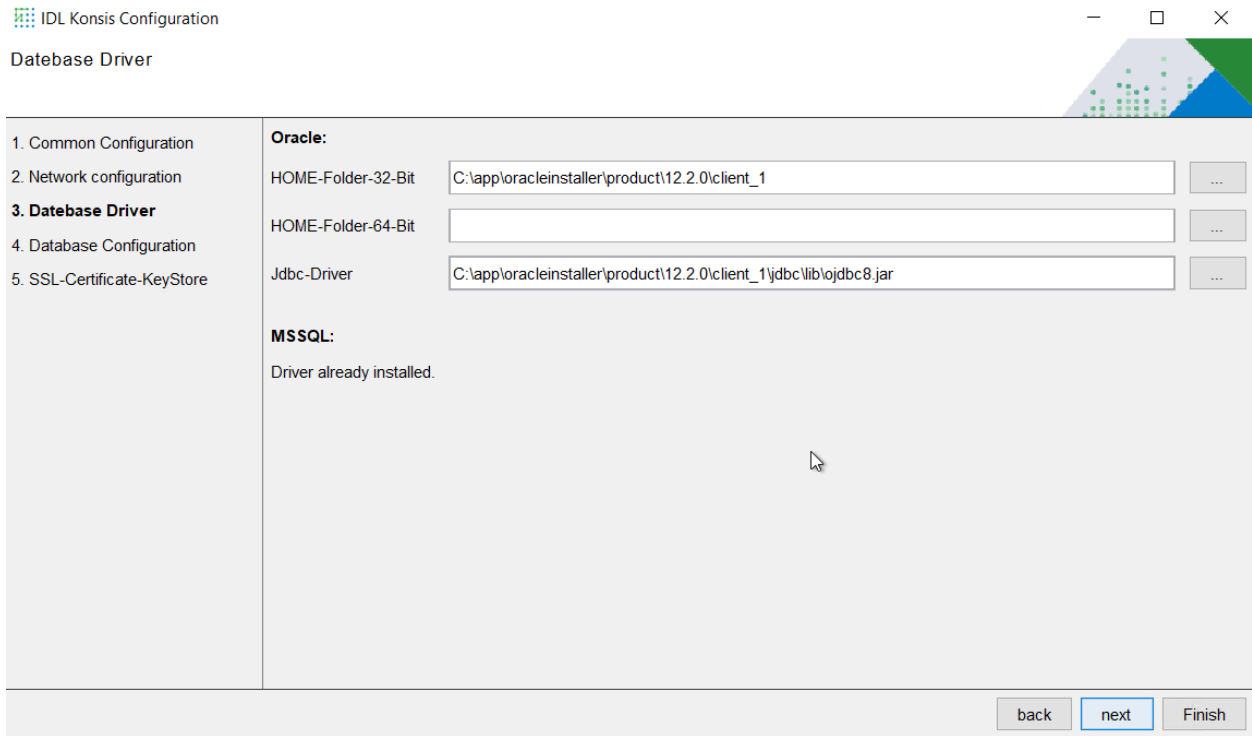
To load the exchange rates of the ECB Bank directly to IDL.KONSIS, a connection to the following URL of the ECB Bank is required:

<https://www.ecb.europa.eu/stats/eurofxref/eurofxref-hist.xml>

If a proxy configuration is required to access this URL, the requisite proxy parameters can be input via the network settings.

To access the input fields, the ###“Proxy-Verwendung” option must be checked.

7.3. Database driver



IDL Konsis Configuration

Database Driver

1. Common Configuration
2. Network configuration
3. Database Driver
4. Database Configuration
5. SSL-Certificate-KeyStore

Oracle:

HOME-Folder-32-Bit ...

HOME-Folder-64-Bit ...

Jdbc-Driver ...

MSSQL:

Driver already installed.

back next Finish

Figure 8 Configuration of database drivers

If Microsoft SQL Server is being used, the drivers are already present in the operating system.

- **HOME directory 32-bit:** Path to Oracle’s native 32-bit driver.
- **HOME directory 64-bit:** Path to Oracle’s native 64-bit driver.
- **JDBC driver:** Path to Oracle’s JDBC driver.

7.4. Configuring the database

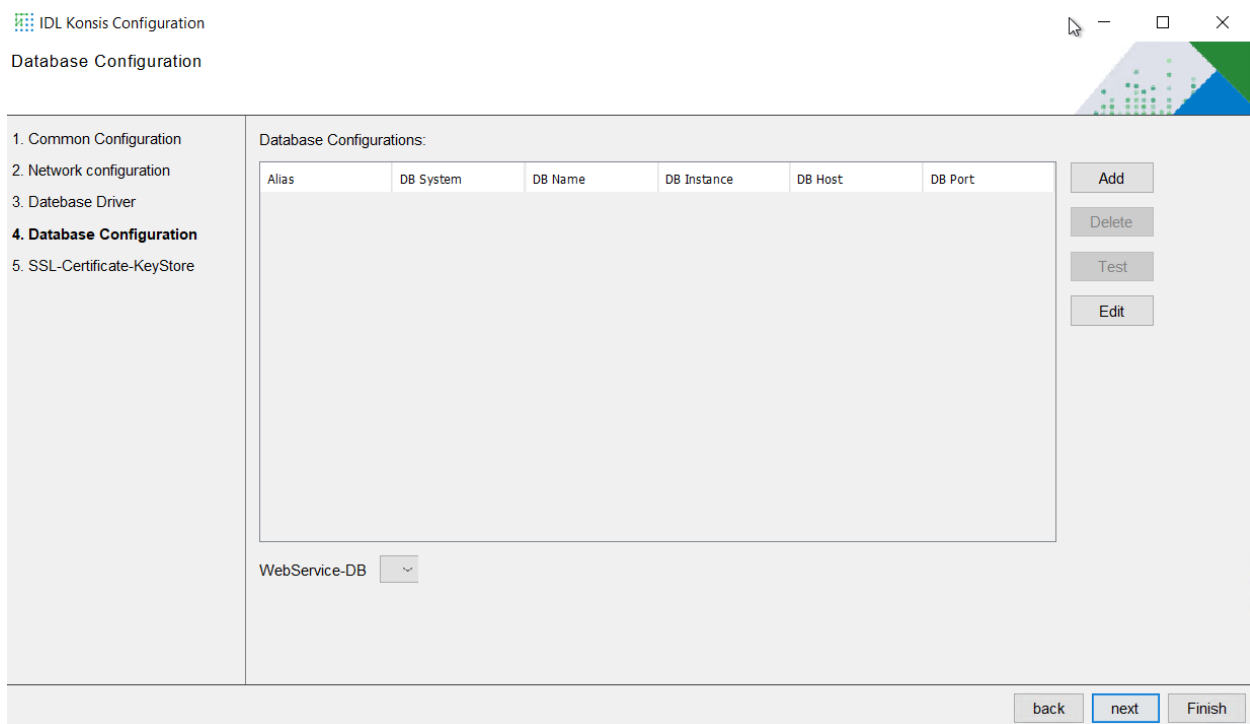


Figure 9 Database configuration

This is where the databases to be used by the Application Server service are set up. The client addresses the database by their aliases.

- **New:** Creates a new database alias.
- **Delete:** Deletes a database alias.
- **Test:** Access to the marked database can be tested here.
- **Modify:** “Modify” has two functions.
 - An entry can be modified without modifying the alias.
 - Or, if the alias name for the database has been changed, a new database alias with the details of the selected database configuration can be created.
- **WebService DB:** If a database is selected here, authentication is performed via this database by default if no specific database (syntax: <user@dbAlias>) is entered on login to the web services.

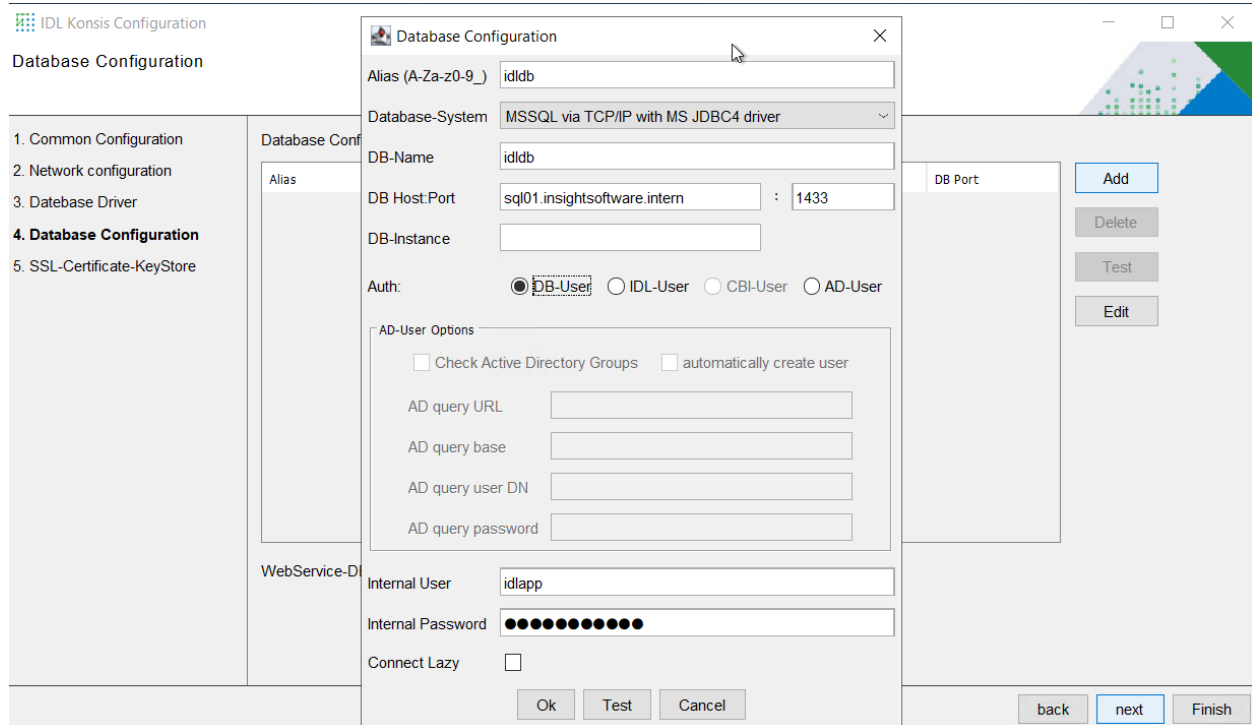


Figure 10 Database configuration for creating an alias

- **Alias:** The alias name for the database. This is sent to the client or selected in the client for use.
- **Database system:** The driver for the database system to be used. The following drivers may be selected:
 - **MSSQL via named pipes:** Requires the user to have write permissions on the server on which Microsoft SQL Server is being hosted.
 - **Oracle via TCP/IP:** The Oracle client must be installed on the server on which the Application Server service is also running. See also [Creating the Oracle database](#)
 - **MSSQL via TCP/IP using MS-JDBC4 driver:** Default for communication with MS SQL Server.
 - **Oracle via native client:** This driver requires Oracle's 32- or 64-bit client to be also installed.
 - **MSSQL via TCP/IP:** Legacy method to bind to an MS SQL Server database.
- **DB name:** The name of the database is entered here.
- **DB host:Port:** The hostname on which the database server is installed. The default port for Microsoft SQL Server is 1433, while for an Oracle Database server it is 1521. If different ports are used, these must be entered.
 - **DB instance:** If more than one instance of Microsoft SQL Server is installed on a server, they are recognised as different instances. The first instance, which is unnamed, is usually the

default instance. In this case, the “###DB instance” field can remain empty. Other installed Microsoft SQL Servers on the same server are then isolated by means of “named instances”. If the IDL.KONSIS database is in a named instance, the name of this instance must be entered into the “###DB instance” field. The “Port” field may be left empty as the port of the associated instance is determined dynamically. However, this requires the SQL Server browser service to be running. However, if a port is specified then the associated port must be used as an instance in this case.

- **Auth:** The Application Server service offers several authentication options.
 - **DB user:** This authentication method uses either **Single Sign-On (SSO)** or **SQL authentication**. Single Sign-On involves the use of the authentication on the client PC. SQL authentication involves the management of login information in the database system.
 - **IDL user:** With this login method, the users and the associated passwords are managed exclusively within the IDL KONSIS application.
 - **AD user:** A login method via the integrated Windows login within a Windows domain. However, this requires the IDL Konsis client and the IDL Application Server to be in the same domain. As such, this process deviates from the SSO with the DB user as described above because there the IDL Konsis client and the database server need to be located within the same domain. The AD-USER method still provides the option to check on login whether the user is allocated to specific groups in the Active Directory. This option is activated via the “###Check Active Directory groups” checkbox. In addition, users can be automatically created in IDL Konsis via a domain group. When creating the new user in IDL Konsis, the surname, the first name and the email address may be queried from the Active Directory.

The query from the Active Directory is performed via the LDAP interface with the inputs:

1. query URL incl. port, e.g.: “ldap://server.idl.eu:389”
2. Query base, e.g. : “ou=groups”
3. Query user DN, DN of AD user with query permission, e.g. :
“CN=aduser,OU=ServiceUser,OU=IDL_User,DC=idl,DC=de”
4. Password of query user

If configured, the alias configuration test checks whether such an LDAP query is possible accordingly.

- **Internal user:** To connect to the database, the Application Server always uses an internal user, which must be specified here. This is usually specified via the database user “idlapp”.
- **Internal password:** The password of the internal user.

- **Lazy connection:** If enabled, the connection to the database is only established if there is a client access attempt. If disabled, the connection to the database will already have been established when the Application Server is launched as a service.

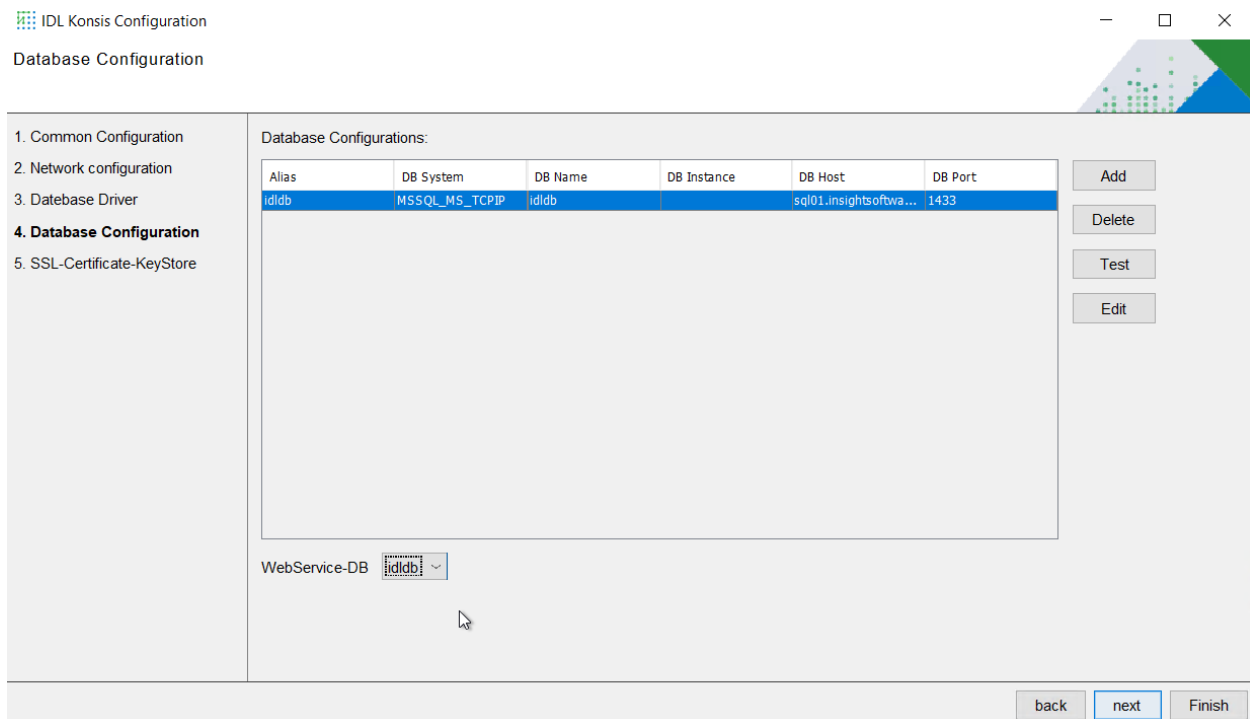


Figure 10-2 Database

7.5. SSL certificates and KeyStore

To communicate with the clients, the Application Server service uses the HTTPS protocol, which both enables the connection to be encrypted and the authenticity of the server to be verified. To allow the clients to verify the authenticity of the Application Server, it requires a certificate. This certificate must contain the correct hostname and should be signed by a certificate authority. This certificate is stored in an encrypted certificate store file, which contains the certificate and the private key.

Certificates can also exist as certificate chains, which means that multiple certificate authorities have validated a certificate. There are two ways to achieve this: The certificates of all certificate authorities can either be included in a single certificate, or they can be distributed across multiple individual certificates. The configuration program of the Application Server can

currently only handle certificate chains that are present in a single certificate. For certificate chains consisting of multiple individual certificates, appropriate tools (such as KeyStore Explorer) must be used to create a single certificate store file.

The process is such that a self-signed certificate is usually first issued before then being validated by a certificate authority and then imported using the Application Server's configuration program.

It is also possible to have a key pair, including the certificate, created directly by a certificate authority, in which case the private key will be supplied along with the certificate, and both will be imported together using the Application Server's configuration program.

Creating a self-signed certificate

Note: Please note that a self-signed certificate is not trusted, which means that the browser will output a warning or even outright reject the certificate. If a warning is issued, the user can also have a self-signed certificate trusted (for them).

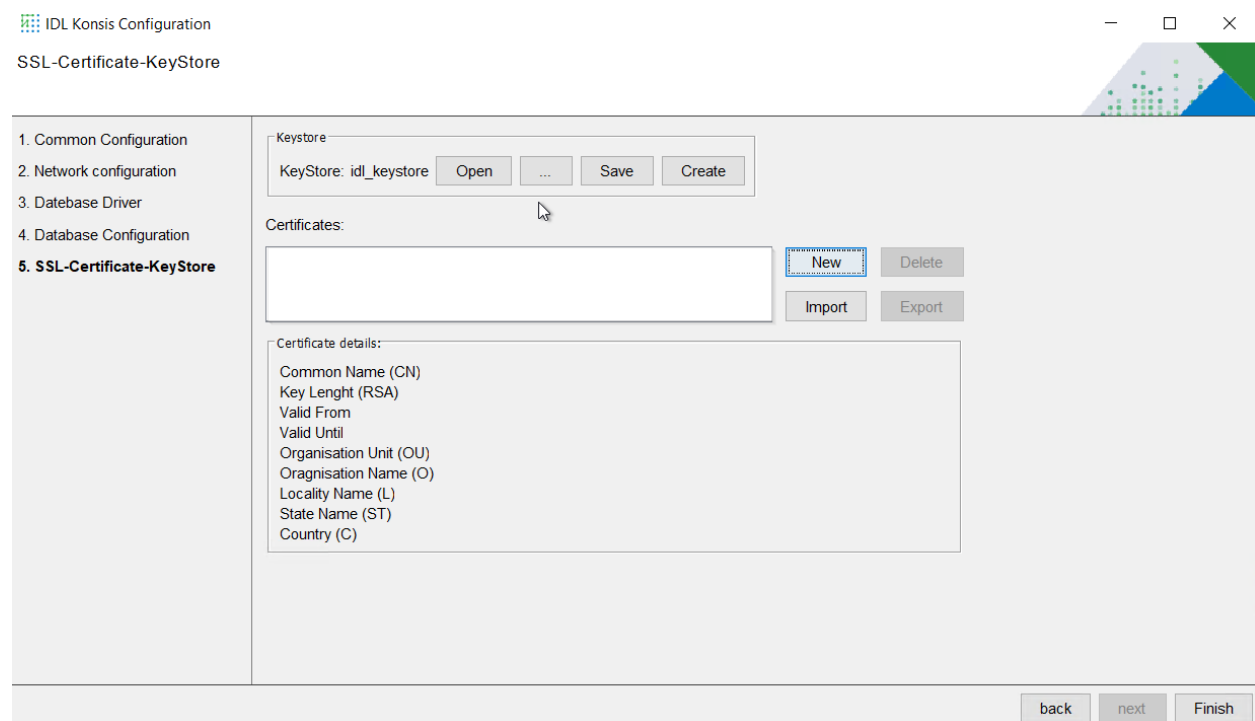


Figure 11 SSL certificate configuration

Following the new installation, it is initially necessary to create a certificate store file (KeyStore) for the cryptographic key and certificates.

To do this, press the **[Create]** button.

- **Open:** Opens the KeyStore with the name specified in the text “KeyStore:” before the **[Open]** button.
- **...** : Opens a dialog box to load a previously created KeyStore.
- **Save:** Saves a KeyStore.
- **Create:** Creates a new KeyStore.

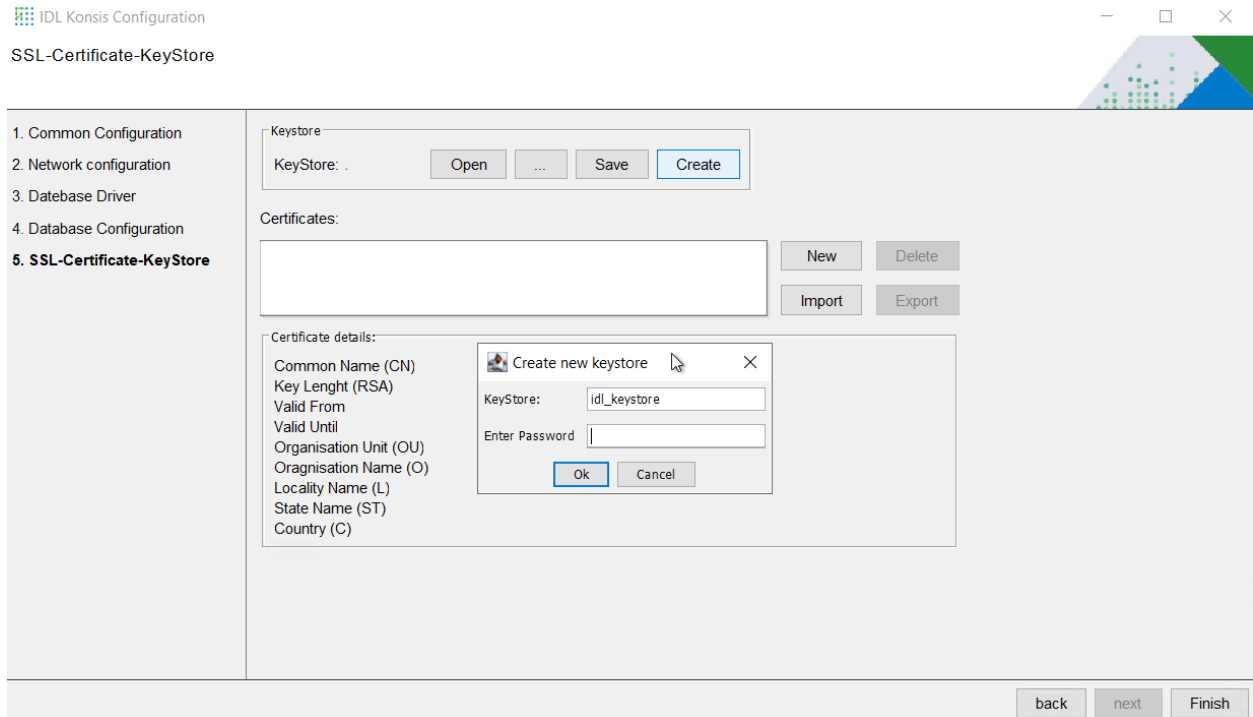


Figure 12 KeyStore configuration

In the window that now opens, you can enter a new name for the KeyStore. By default, this is “**idl_keystore**”. The second field is used to set the KeyStore password. Now confirm the entries with the **[OK]** button.

Now the previously deactivated buttons are enabled.

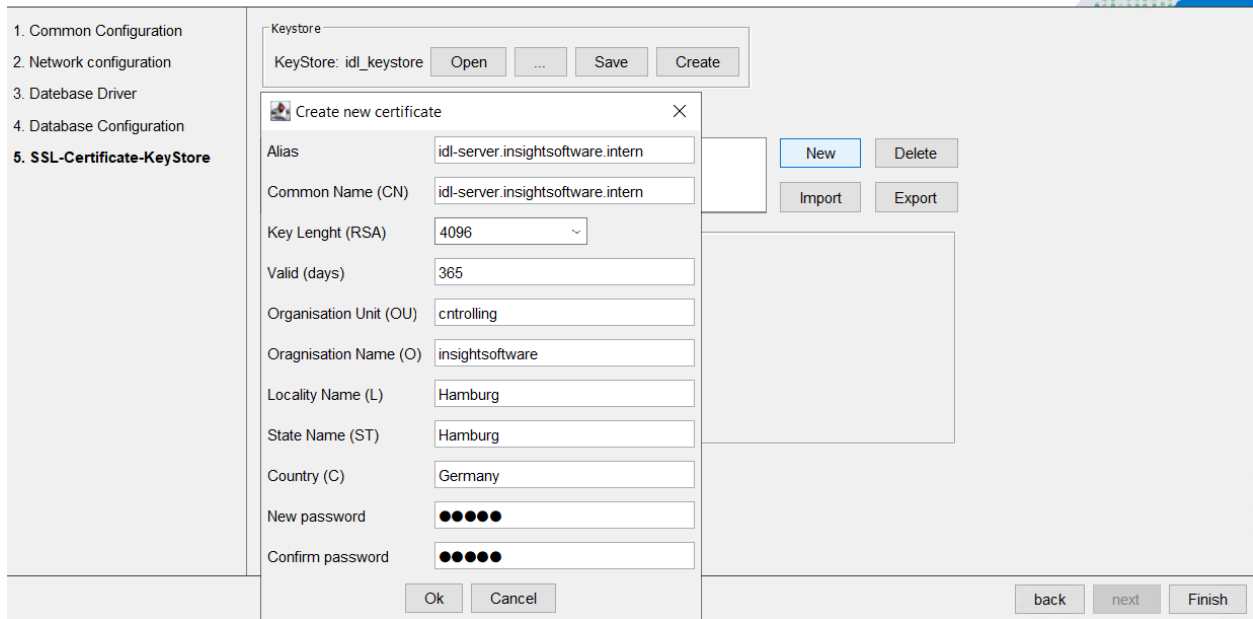
The buttons on the right have the following meanings:

- **New:** Create new self-signed certificate.
- **Delete:** Delete the certificate and private key.
- **Import:** Import a certificate, replace a certificate or apply a trusted certificate.
- **Export:** Export a certificate.

Pressing the [**New**] button will open a window. The following fields in the window have the following meanings:

- **Host (CN):** The name of the host to be certified (Common Name). This must match the content of the field “Hosts” on the “General settings” page. Otherwise, there will be no communication between a client and the Application Server.
- **Key length (RSA):** Defines the length of the key to be generated. 2048-bit and 4096-bit lengths are available. RSA is a cryptographic method and is not only used in certification. The use of key lengths shorter than 2048 bits is not recommended for security reasons.
- **Validity (days):** Period of validity of the certificate from the current date. Once the certificate expires, the certificate must be renewed.
- **Organisational unit (OU):** Defines the division within the company for which the certificate is to be issued.
- **Organisation (O):** Name of the company.
- **Location (L):** Physical place of business.
- **State (ST):** Federal state.
- **Country (C):** Country.
- **Certificate password:** Enter the password to protect the private key.
- **Repeat password:** Repeat password.

The input fields “Organisational unit”, “Organisation”, “Location”, “State” and “Country” are not validated by the configuration program, but only by a signing certificate authority.



The screenshot shows the 'SSL-Certificate-KeyStore' configuration window. On the left, a navigation pane lists five steps: 1. Common Configuration, 2. Network configuration, 3. Database Driver, 4. Database Configuration, and 5. SSL-Certificate-KeyStore (which is selected). The main area displays a 'Keystore' section with 'KeyStore: idl_keystore' and buttons for 'Open', '...', 'Save', and 'Create'. A 'Create new certificate' dialog box is open in the foreground, containing the following fields and values:

- Alias: idl-server.insightsoftware.intern
- Common Name (CN): idl-server.insightsoftware.intern
- Key Length (RSA): 4096
- Valid (days): 365
- Organisation Unit (OU): cntrolling
- Organisation Name (O): insightsoftware
- Locality Name (L): Hamburg
- State Name (ST): Hamburg
- Country (C): Germany
- New password: [masked]
- Confirm password: [masked]

Buttons for 'New', 'Delete', 'Import', and 'Export' are visible on the right side of the dialog. At the bottom of the dialog are 'Ok' and 'Cancel' buttons. The main window has 'back', 'next', and 'Finish' buttons at the bottom right.

Figure 13 New certificate creation

Once all the input fields have been completed, the certificate now needs to be generated. To do this, press the **[OK]** button.

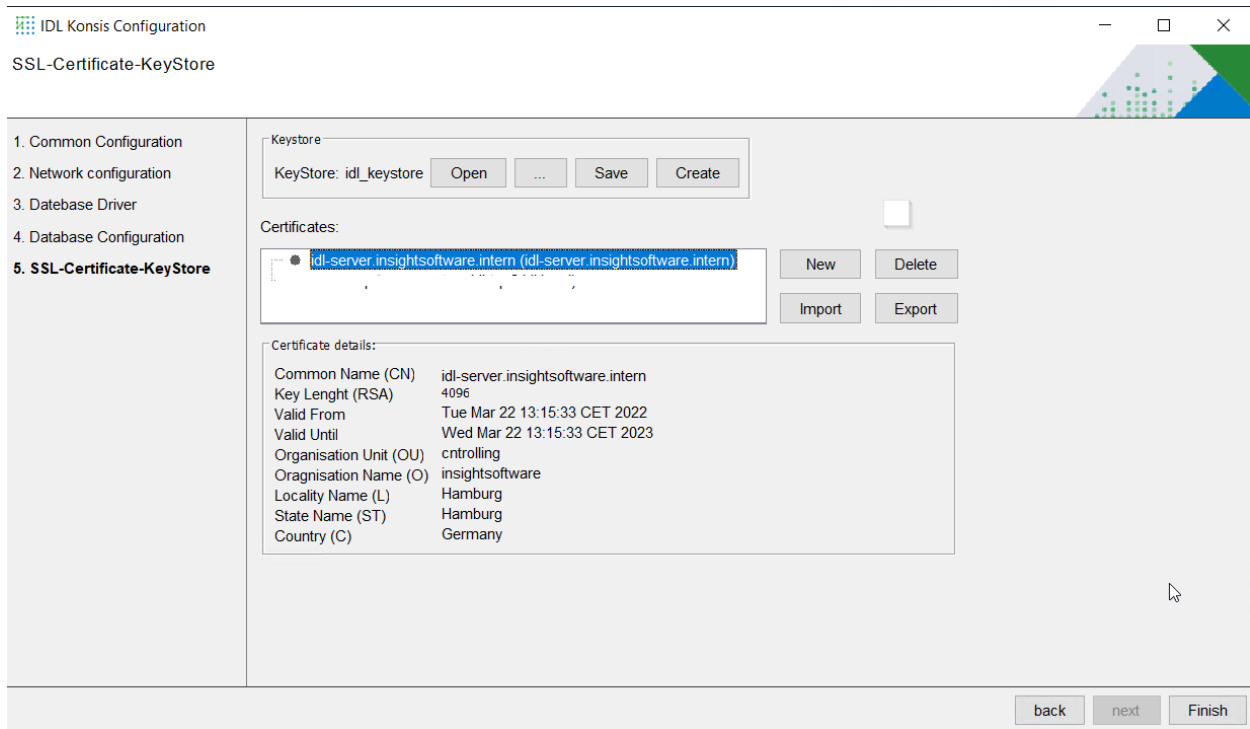


Figure 14 SSL certificate display

Once the certificate and the private key have been generated, the generated certificate can be viewed under “**Certificates**”. Clicking on the certificate will now display detailed information on the certificate under “**Certificate details:**”.

Trusted certificate

Trusted certificates can also be imported into IDL KONSIS. To do this, press the [**Import**] button.

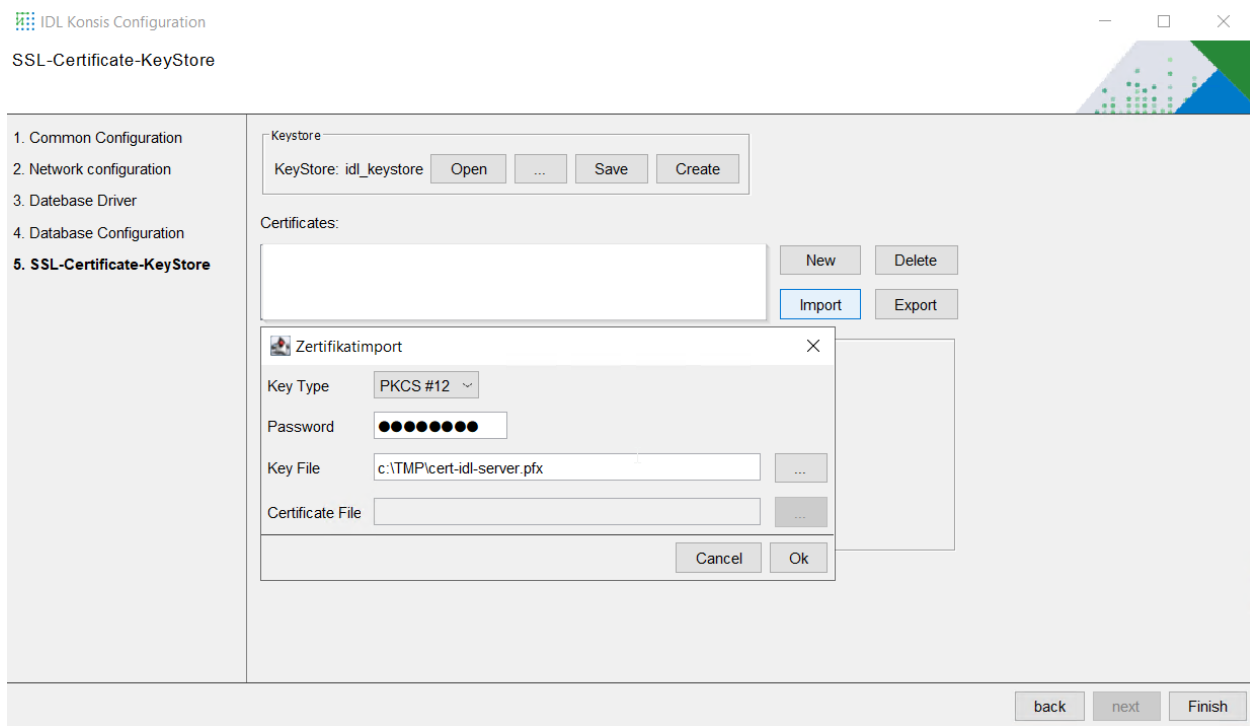


Figure 15 SSL certificate import

The window that then opens offers the following formats:

- **PKCS #12:** A format in which the private key and the certificate are stored with password protection. The certificate is part of the generated file.
- **PKCS #8:** This format stores private keys. There are two possible versions: encrypted and unencrypted. Ideally, the encrypted version should be used. The certificate is not part of the generated file.
- **MS PVK:** Microsoft's proprietary private key format.
- **OpenSSL:** Used if the certificate and private key are generated using the open-source tool OpenSSL.

Define three additional fields:

- **Password:** Password for the key file or certificate.
- **Key file:** File with the private key.
- **Certificate file:** File with the certificate.



Note: The handling of trusted certificates is not a trivial matter, which is why we recommend consulting experts from your certification authority if necessary.

Note: Because this represents changes to the domain, you should first consult your domain administrator beforehand.

8. IDL Konsis – client installation

The setup can also be downloaded from the homepage of the IDL Application Server. You can also find this on the server in the Web-Start\Client folder. It is also available as an MSI file to support automated installation with software roll-out tools.

When using a software roll-out tool, there are other additional parameters that can be used alongside the parameter set available with the “msiexec” application.

- **APPDIR:** Defines the directory in which the IDL Konsis client is installed
- **SHORTCUTDIR:** Defines a directory in which the shortcut is stored
- **PROP_HOST:** Specifies the FQDN on which the Application Server runs.
- **PROP_PORT:** Port via which the communication runs.

Sample call in the command line (cmd.exe):

```
msiexec /passive APPDIR="C:\Program Files (x86)\IDL\IDL KONSIS"  
SHORTCUTDIR="C:\ProgramData\Microsoft\Windows\Start Menu\Programs\IDL\IDL KONSIS"  
PROP_HOST=appserver.insightsoftware.com PROP_PORT=444 /i  
IDLKONSISFORECAST_Client.msi /L*v installationsprotokoll.log
```

Note:

Please note that the version of the client must match the version of the installed or updated Application Server. If a client is already installed on the client PC, it is replaced with the new version during installation. The client installation is performed by double-clicking the installation file “**IDLKONSISFORECAST_Client.exe**” or “**IDLKONSISFORECAST_Client.msi**”.

Continuing the installation:

- Select the installation language.
- Confirm the welcome page by clicking on “**Next**”.
- Leave the installation directory unchanged or select a new drive and/or directory. Then click on “**Next**”.
- Now press the [**Install**] button to start the installation.
- Inputs (modify program directory as need be, also add host and port###)
- Now click on the [**Finish**] button and the installation is complete.

Program directory of the installed client

The client program directory of the applications IDL.KONSIS and IDL.XLSLINK is located in the installation directory specified during the client installation.

Example: C:\Program Files (x86)\IDL\IDL.KONSIS.FORECAST.Client

The personal settings for working with IDL Konsis are stored on the client PC in a configuration file named "idlgui.ini". This file is created in the profile of the current user when launching IDL Konsis for the first time.

The certificate store is also located here.

Example: C:\Users\\AppData\Roaming\IDL\IDL.KONSIS.FORECAST.Client

The configuration file "idlgui.ini" is loaded each time the IDL Konsis client is launched. Launch settings such as the hostname and the port number of the Application Server are stored in the configuration file and can be modified there. The configuration file also contains user-specific settings. Many of these settings can be configured in the options of the opened IDL Konsis program. The application must be restarted after each change to the user-specific settings.

The installed start icons can be individually modified on the installed IDL Konsis client. The default start icons are located in the directory:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\IDL\IDL.KONSIS.FORECAST.Client

You can edit the properties of the start icons by right-clicking with the mouse and selecting "Properties". The following is an example of the start icon for IDL Konsis. The destination defined is:

"C:\Program Files (x86)\IDL\IDL.KONSIS.FORECAST.Client\jre\bin\javaw.exe" -Xmx1024m -jar konsis.jar /mode=h

Note -Xmx1024m = Maximum size of the Java storage allocation pool in megabytes.

The parameter /mode=h states that communication between the IDL Konsis client and the IDL Application Server is established with the https communication protocol. This parameter should not be deleted. Further parameters can be added.

Startup parameter	Value	Explanation

/suppresslogin		Do not display the login dialog (only with integrated Windows login)
/username=	<username>	User name (do not use with integrated Windows login)
/passwordchangeable		Display “###Enhanced” on login to change password
/hostname=	<host>	Hostname of the IDL Application Server
/port=	<port>	Port number of the IDL Application Server
/start=	<abbreviation>	Launches a specific Konsis application immediately after login
/textlocale=	de_DEU, en_ENG, fr_FRA	Preconfigure language for texts and menu language
/formatlocale=	de, en, fr, ...	Preconfigure language for formats
/i=	<path + ini-file>	Preconfigure an individual configuration file

Below you will find an example with multiple startup parameters being called:

```
"C:\Program Files (x86)\IDL\IDL.KONSIS.FORECAST.Client\jre\bin\javaw.exe" -Xmx1024m -jar konsis.jar /mode=h /supresslogin /username= /textLocale=en_ENG /formatlocale=en /debug
```

A configuration file with its own file name and storage location may also be stored as a call parameter.

Below is an example: "C:\Program Files (x86)\IDL\IDL.KONSIS.FORECAST.Client\jre\bin\javaw.exe" -Xmx1024m -jar konsis.jar /mode=h /i=%appdata%\IDL\IDL.KONSIS.FORECAST.Client\idlgui-produktivsystem.ini

Note on test and live system for IDL Konsis

When operating two or more systems, it makes sense to use IDL Konsis via a web browser with the IDL LAUNCHER. In this case the test system and live system may be different versions.

Alternatively, the installed client may be used. The precondition for the use of the installed IDL Konsis client, however, is that both the test and the live systems are the same version. Because the test system uses a different server address (host: port) than the live system, it is recommended that two different configuration files with different server addresses are used. To use a specific configuration file, use the startup parameter /i= in the call.

It is also possible to submit hostname and port as startup parameters. To do so, use the startup parameters /Hostname and /Port

Note on terminal server (multiuser systems)

The installation of the IDL Konsis client is recommended on terminal servers. Please note that when using terminal server farms, the IDL Konsis client needs to be installed or updated for each terminal server.

The update is performed via the setup file IDLKONSISFORECAST_Client.exe.

To be able to launch the IDL Konsis application for the first time, the user is advised to specify the server address (host: port) of the IDL Application Server on launch. You can also prepare the configuration file idlgui.ini by adding any corresponding modifications and copy this file to the users' profiles.

In addition, the trust store (idlcert) can be allocated to the users' user profiles. The certificates of the IDL Application Server are stored in this trust store.

9. Launching the IDL Konsis application

9.1. Launch via the IDL Portal

As the central starting point, the **IDL Portal** takes you directly to the IDL CPM Suite's world of products and solutions. Access to the IDL WPS² is required to access the IDL Portal via an Internet browser. In the address bar of your Internet browser, enter the address of the IDL WPS to call the IDL Portal. The hostname and the https port of the IDL WPS need to be input as the address (example: <https://idlserver.a.idl.de:443>).

² IDL WPS (IDL Workplace Server) is a server application and provides the backend services for IDL.DESIGNER, the IDL Portal, the Report Catalogue and the App Catalogue.

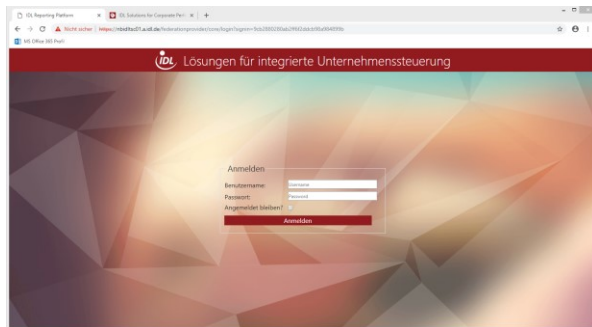


Figure 16 IDL Portal login

When the user logs into the IDL Portal, the Report Catalogue opens first. You can access the applications via the **App Launcher** (left-hand button in the menu bar at the top). From the Start Panel you can access the topics Consolidation, Planning, Reporting, Administration, Data Management, Report Catalogue, App Catalogue and Community. Clicking each tile opens further selection options. The App Catalogue enables you to download desktop or mobile apps. Administration enables users, licences and roles to be created and managed and the database connections to be configured.

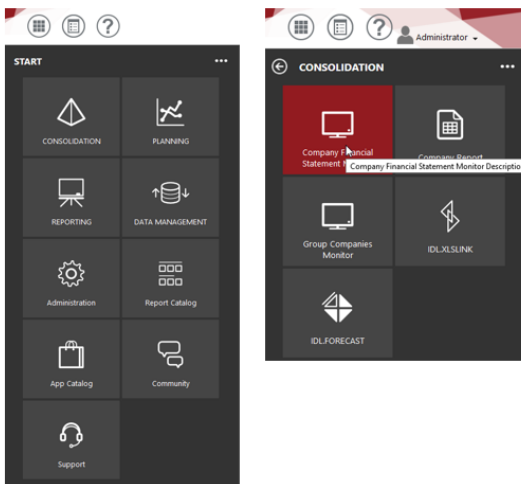


Figure 17 IDL Portal app launcher

Provided you have installed a IDL Konsis client, the following KONSIS modules can be called up directly from the CONSOLIDATION and PLANNING group:

CONSOLIDATION

- **Group Companies Monitor** (url: idlkonsisktkges://);
- **Company Report** (url: idlkonsisrep://)
- **Company Financial Statement Monitor** (url: idlkonsisea://);
- **IDL.XLSLINK** (url: idlconnector://)
- **IDL.FORECAST** (url: idlkonsisstart://)

PLANNING

- **Planning Monitor** (url: idlkonsispm://),
- **Plan Scenario** (url: idlforecastplan://)
- **Company Report** (url: idlkonsisrep://)
- **IDL.FORECAST** (url: idlkonsisstart://)

Clicking the three dots in the upper right-hand edge opens a widget panel. The “plus” icon here enables folders, weblinks, default groups and applications to be added. If the widget panel is open, applications can be edited and removed and tiles can be dragged and dropped to the start panel. Further widgets (including web links) can also be configured via self-created tiles.

9.2. Launch with IDL LAUNCHER

If you have installed IDL LAUNCHER, you can download and execute IDL Konsis via the browser. IDL LAUNCHER stores the IDL Konsis client application in the user’s profile. Subsequent startup processes are executed immediately because all necessary resources are already available in the user’s profile. On each launch, IDL LAUNCHER checks for newer IDL Konsis versions that are provided by the IDL Application Server. If newer versions are available, they are automatically downloaded and launched. Simply enter the address of the IDL Application Server in the address bar of your Internet browser to call the IDL Konsis launch page. The hostname and the https port of the IDL Application Server need to be input as the address.

https://<hostname>:<portnumber>

Example (https://idlserver.a.idl.de:444)

In the example, the hostname contains the full name (**fully qualified hostname**³).

On inputting the full address and confirming with enter, the launch page of the IDL Application Server opens. Your web browser may display a security warning that the connection is not trustworthy. In this case, ask your IT department whether a trustworthy certificate can be installed. If you want to trust the certificate, anyway, confirm this in your web browser. The launch page of the Application Server now opens.

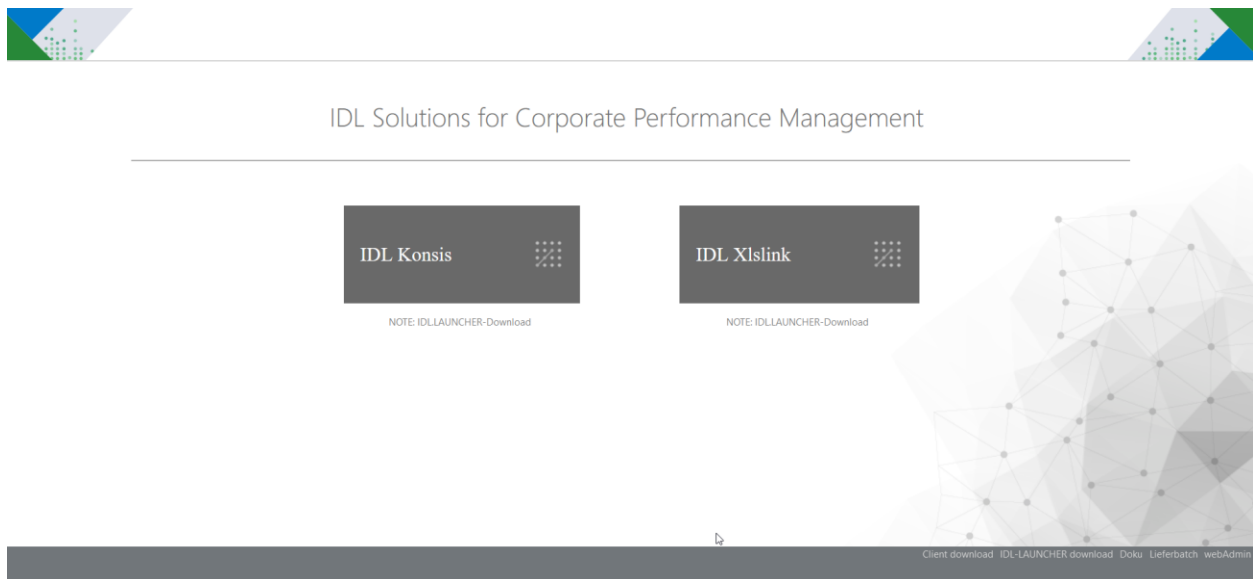


Figure 18 - Launch page of IDL Konsis Application Server

The two applications IDL Konsis and IDL Xlink are arranged as large, red tiles under the heading “**IDL Solutions for Corporate Performance Management**”. Both applications can be downloaded and executed by clicking the corresponding tile. First, launch IDL Konsis by clicking the tile. Because the communication protocol deployed is HTTPS, a security warning appears

³ A fully qualified hostname (**FQHN**) is a computer name that is presented either as a fully qualified name of a domain (**fully qualified domain name, FQDN**) or as an IP address. The FQHN uniquely refers to a specific computer.

with information about the security certificate deployed when launching the application. If you are not sure whether you can trust the certificate, ask your IT department. If you trust the security certificate, click “Yes” to confirm the dialog box. This downloads and subsequently executes IDL Konsis. Click “Allow” to launch the application. This security warning only appears on the first launch if you uncheck the option.

When launching IDL Konsis, you first see the login dialog box.

IDL LAUNCHER stores the entire IDL Konsis client application locally on your computer.

Example of program folder:

```
C:\Users\
```

9.3. Installed client – launch with installed start icon

Once the IDL Konsis client has been installed on your workstation, you will find the group “IDL” with the following start icons in the Windows start menu:

Launch the application with the start icon “IDL.KONSIS.FORECAST”!

You can also find the icons in the start menu in the Windows folder:

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\IDL\IDL.KONSIS.FORECAST.Client
```

When you launch IDL.KONSIS, the “###Login” dialog box appears.

When you log in for the first time, the field “Host: port” may not yet be populated with the correct data. You will be given the hostname and port number of the IDL Application Server by your IT application administrator who manages the application on the client and server side.

Enter the hostname and port using the following syntax:<hostname>:<portnumber>. When the host and port have been changed, confirm your input via the “Refresh” button.

You will be given your login information by your application administrator.

10. The login dialog box in IDL Konsis

Host and port

When launching the application via the installed icon, “Host: Port” appears in the login dialog box. You will be given your login information by your application administrator.

Enter the hostname and port using the following syntax:<hostname>:<portnumber>.

When the host and port have been changed, confirm your input via the “Refresh” button.

If the HTTPS connection has been made, a further dialog box with information about the security certificate that is installed on the IDL Application Server will be displayed on the first launch of the application if self-signed certificates or certificates issued in your company are used. If you trust the certificate, then confirm by clicking “OK”.

Proxy settings

A proxy server is a communication interface in computer networks. The proxy server transfers the client’s requests, such as the request to call up a website, to a server via its own address without the client and server having to be directly connected to one another. The two IDL Konsis and IDL Xlink clients can communicate with the IDL Application Server either directly or via a proxy server. Ask your IT service provider whether proxy settings are necessary on IDL Konsis.

To configure proxy settings, click the “Options” button in the IDL Konsis login dialog box. The Proxy settings for IDL Konsis can be set in the “Options” dialog box.

Enter the hostname and port number of the proxy server as need be and confirm your input by clicking “OK”. If the proxy server used in the company requires user authentication, you also need to enter your username and password. The proxy settings from the settings of the Microsoft Windows operating system that are stored in the Internet options may be used. In this case, check the “###Use system proxy settings” option and confirm by clicking “OK”.

Username and password

There are two basic options: one option is for users to leave the login dialog box username and password blank. The second option is for users to specify the username (known as the logon ID) and the associated password.

The username is stored in the application's configuration file and appears in the login dialog box on repeat login, although the password needs to be specified on each login because it is not stored. How you specifically log into IDL Konsis depends on the authentication method used by your company.

In the case of database authentication using integrated Windows authentication, you leave the username and password empty and simply confirm by clicking "OK".

In this case, authentication can also be performed without a dialog box. To enable this, your configuration file `idlgui.ini` needs to be edited using a text editor (for example, with Notepad). In `idlgui.ini`, set the entry `suppresslogin=true`.

Tip: Having successfully logged into IDL.KONSIS, you can select the "Info..." item in the menu bar via the question mark to open and edit the configuration file (`idlgui.ini`) with a text editor.

The enhanced setting in the IDL Konsis login dialog box can be used to reset the user password both in terms of database authentication and IDL-USER authentication. To be able to use this enhanced setting, you first need to open `idlgui.ini` with a text editor and edit the "General" section:

```
passwordChangeable=true
```

Next time the application is launched, the dialog box opens with the "Enhanced..." button.

To change the password, first enter the old password in the login dialog box, and then enter the new password in the enhanced window. Confirm this new password by re-entering it. Then confirm the login by clicking "OK" to execute the change of password.

11. User authentication

Two frequently used methods are the integrated Windows login and the IDL-USER authentication method.

With IDL-User authentication, an application administrator manages the user passwords. This administrator may amend the users' password policies, such as the complexity of the passwords, and can also reset passwords.

If database authentication without integrated Windows login takes place, a database administrator performs this task. If database authentication with integrated Windows login takes place, this additional administrative task is not required.

However, the management of the IDL Konsis users within the application remains the task of an application administrator for all authentication methods. This task is organised within the specialist department.

11.1. Authentication with integrated Windows login

Authentication with integrated Windows login means that a user, having logged into a Windows workstation once, can use all applications for which they are authorised without having to log in each time again with user name and password.

The principle of a single login is also referred to as single sign-on (SSO). Among other things, integrated Windows authentication provides methods for implementing password policies such as the complexity of secure passwords.

11.2. Authentication with IDL User mode

This requires a change to the authentication mode in the Application Server via the configuration program in the “**database configuration**” section, where the authentication mode must be set to “**IDL user**”.

The IDL USER mode stores all users and associated passwords as well as password policies within the IDL Konsis application. This means that both the users and their passwords can be managed in the individual USER application. In addition, there is an option to implement specific password policies for each individual user, for instance, to check the complexity when setting secure passwords or also the validity period of passwords that cause the mandatory expiry of the password from between 0 and 99 days.

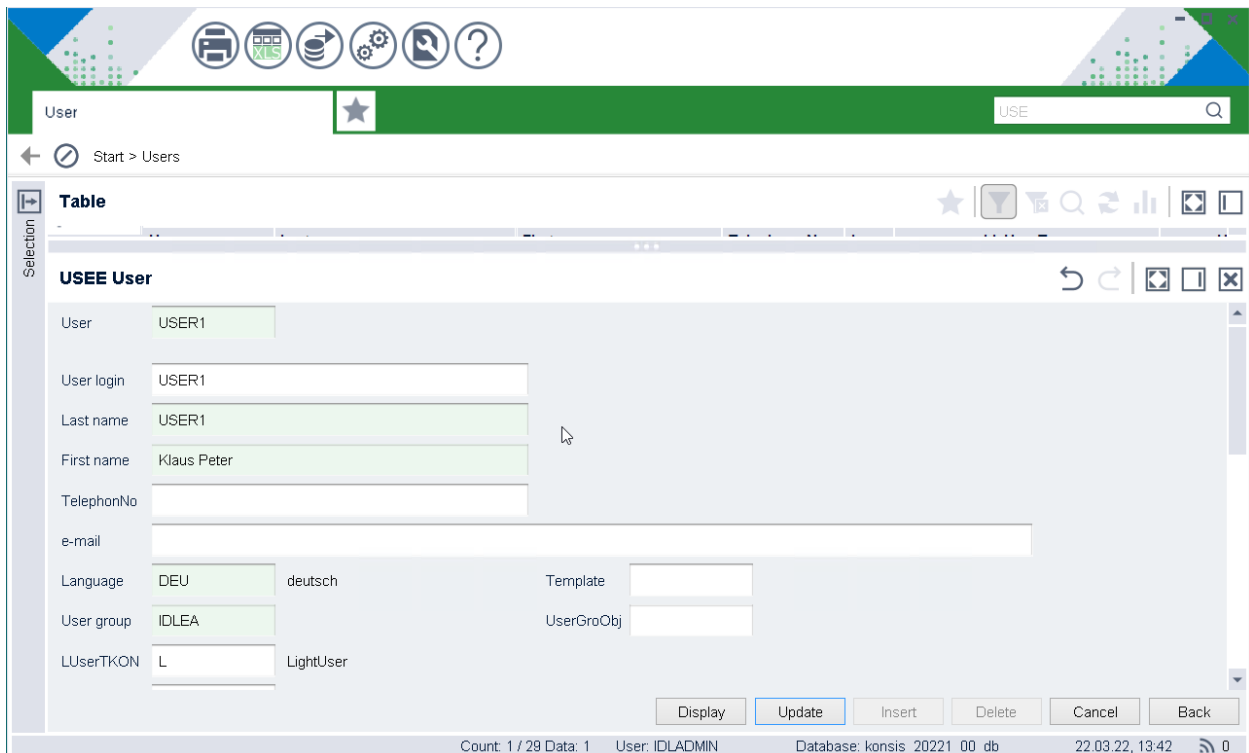
The passwords are stored in encrypted form in the IDL Konsis application and thus cannot be read by users. Permissions to amend the password policies and the permission to reset the passwords are the task of an application administrator as opposed to a database administrator. IDL User is a good option if a user wants to authenticate themselves on IDL Konsis outside the domain (external access) and integrated Windows authentication is not possible. Users who authenticate themselves on IDL Konsis with IDL USER mode need to enter their login information each time they log in.

Setting up users within IDL Konsis (IDL user authentication)

IDL Konsis has its own user management procedures. This entails management of users with a login name (login ID). In IDL USER authentication mode, passwords and password policies are also managed in the application.

From this point, the procedure is as follows:

- Launch IDL Konsis.
- Log into IDL Konsis as “idladmin” using the appropriate password. Make sure that you use the right database alias when selecting the database.
- Create the user, including the password, in the “USE” application.



The screenshot shows the 'USEE User' management interface. The form contains the following fields and values:

User	USER1
User login	USER1
Last name	USER1
First name	Klaus Peter
TelephonNo	
e-mail	
Language	DEU deutsch
Template	
User group	IDLEA
UserGroObj	
LUserTKON	L LightUser

At the bottom of the form, there are buttons for 'Display', 'Update', 'Insert', 'Delete', 'Cancel', and 'Back'. The status bar at the bottom indicates: 'Count: 1 / 29 Data: 1 User: IDLADMIN Database: konsis_20221_00_db 22.03.22, 13:42'.

Figure 18 User management (use)

The following fields warrant a closer look:

- **ÄndInterv (change interval)** – If this is “0”, no new password will be requested. The user will only be asked to change their default password once when logging on to IDL KONSIS for the first time. Values > 0 and < 99 represent the number of days that a password is valid for.

- **Pw-Reset (password reset)** – “A” must be selected here to enable a corresponding default password to be created, or if the user has forgotten the password that they set for themselves.
- **Pw-Länge (password length)** – If this field is empty, a password can have a maximum length of 16 characters. If this field is activated, the password must be at least 7 characters long and cannot exceed 16 characters in length.
- **Ident.Zei. (sequence of identical characters)** – If active, checks whether 4 identical characters have been used back-to-back.
- **Intervall (regularity)** – Expiry times
- **Seq.Alpha (alpha sequences)** – If active, sequences of characters such as “**abcdefg**” will not be accepted as passwords (checks for a length of 5 characters or more).
- **Seq.Num. (numerical sequences)** – If active, sequences of numerical characters such as “**12345**” will not be accepted as passwords (checks for a length of 3 characters or more).
- **Seq.Keyb. (keyboard sequences)** – If active, sequences of characters equivalent to keyboard layouts such as “qwertyu” will not be accepted as passwords (checks for a length of 5 characters or more).
- **>=1 Ziffer (one numerical character)** – At least one numerical character must be present in the password.
- **>=1 Sonder (one special character)** – At least one special character must be present in the password.
- **>=1 Kleinb (one lower-case character)** – At least one lower-case character must be present in the password.
- **>=1 Großb (one upper-case character)** – At least one upper-case character must be present in the password.

Note: Once the users have been created with their default passwords, all that is left to do is set the appropriate permissions that the users are to have in IDL KONSIS using the “**VORADMIN**” application.

12. Notes on virtualisation

Because the development of virtualisation is an ongoing process, here are some tips.

- **Citrix:** the user's profile must always be secure.
- Certain group policy objects (GPOs) may result in abnormal behaviour on IDL Konsis. This includes for example:
 - **Streaming user profiles:** This may still work on IDL Konsis but will result in an error on IDL Xlslink. This profile was developed by Citrix to enable faster logins and to download further profile data after login and during runtime.
 - **Application streaming:** Application streaming on a client PC with licence transfer during local runtime is not possible with IDL Konsis. There is no application streaming as of Citrix 7.x anymore. Citrix recommends Microsoft APP-V.
- **Microsoft RDP/RDS:** When publishing as a remote app, please ensure that the entry "Shell Working ###Directory: <path to load directory of IDL.KONSIS>" is present in the RDP/RDS file. If possible, please disable the multimedia functions when opening the app, and check the network connection specified in the app.
- **Microsoft APP-V:** Application streaming for temporary local user on a client PC is not possible with IDL Konsis.
- **Hyper-V:** This Microsoft solution presents no problem.

Please contact us regarding any other virtualisation solutions.

13. Documentation

Documentation is included in the downloaded installation package as well as the IDL Konsis installation directory of the server installation. This is in the directory “Doku” and is divided into the following subdirectories:

- **Excel:** contains documentation on the setup and operation of IDL. Xlslink.
- **Installation:** contains instructions for a new installation of IDL KONSIS including the underlying database.
- **Interfaces:** contains the documentation of the interfaces to upstream bookkeeping systems (Command Oxaion, DCW, Navision Axapta, SAP, SoftM, Schilling, Varial).
- **Release:** contains instructions on the installation of an IDL Konsis service pack as well as a description of the changes contained within this service pack.
- **Systech:** contains various technical system descriptions.

Further documentation, in particular the application documentation, is copied to the installation path on installation of IDL Konsis.

All documents can be called up with a web browser using the URL from your IDL Konsis server <https://<servername>:<portnumber>>. The bar at the bottom of this page contains a link labelled “Docu”.

14. IDL support

We're here for you – Please request professional support if you are intending to install, update, migrate or modify your software and/or systems.

The experienced product specialists from our IDL Support Team will provide the assistance you require. You can submit your support and service queries either by telephone, email or directly via the Customer portal.

Contact by telephone, week days from 8:00 a.m. to 5:00 p.m. (except on national statutory bank holidays in Germany):

- User questions and solutions **+49 4102-4785-10**
- Technical questions and services **+49 4102-4785-11**

Contact by email:

idsupport@insightsoftware.com

If you use this email address, a ticket for your query will be automatically generated. We will send you a confirmation of receipt with a ticket number. In the event of any queries or if you would like to submit any additional information about the ticket, please **always** use the reply function in your email program. This ensures that all information can be allocated to the ticket.

Contact via the customer portal:

<https://help.insightsoftware.com>

Log into the customer community to read knowledge articles, download installation software or to open a new ticket. Once logged in, you can also view your open tickets, add information or reopen closed tickets. If you do not have a login yet, please get in touch with us.

Remote support

With **IDL-QuickSupport** from TeamViewer, we can connect to your computer and provide rapid and efficient remote support. You can find IDL-QuickSupport on the customer portal. You do not need a login for the download. The software does not need to be installed. You simply execute the TeamViewerQS.exe file on your computer and let us know your TeamViewer ID and the generated password.

Your IDL Support Team