ELO server – Installation and operation

Installation

Table of contents

Getting started

Introduction

This documentation is intended for use by people with a system administrator role and contains important information that they must follow during installation and for administrating the system. Detailed information on using the software can be found in the respective ELO client manuals. There are also areas in ELO that should not be fully accessible to everybody due to security considerations, e .g. server configuration, passwords, document paths, and system security settings. These subjects are covered in detail in this documentation, but are only briefly covered in the documentation for each of the clients.

> **Please note**
>
> Some of the paths in this documentation contain placeholders. You should replace these with the values you require for your installation. The placeholder <ELO> stands for the ELO installation folder.

Operating system

The following installation guide is based (in most sections) on the Microsoft Windows operating system. Although there are some differences when installing on a Linux operating system, the procedure is basically the same.

> **Please note**
>
> ELO server installation is not currently supported for the Solaris operating system.

Differences in the installation processes between operating systems are noted in these instructions when they occur.

Quick start

The following steps are required for a quick ELO server installation.

Step	Explanation
1. Create password lists and checklists	Because of the large number of accounts, we recommend that you keep password lists. Checklists help you to maintain a overview and serve as proof of performance.
2. Set up accounts	You should set up the following accounts in advance: - Database service account - ELO Server Engine/Apache Tomcat service account
3. Install SQL Server	Microsoft SQL Server or PostgreSQL
4. Run ELO Server Setup	Download ELO Server Setup and execute it on desired server computer.

Preparations

Introduction

Before the actual installation of the ELO server, you need to take some preliminary steps. For example, you need to set up important accounts and install a database.

An installation checklist can help you with this.

Installation checklist

Before you install ELO, create a checklist of information required by the system to function. Keep this information secure. You may not need all of the information listed below for your installation, but you should use it as a general guide.

Accounts

Windows accounts: (name and password)

- Database service
- ELO Server Engine/Apache Tomcat

Database accounts:

- Database administrator account
- ELO database account (default: elodb)

ELO accounts:

- Administrator account
- Service account (default: ELO Service)

Apache Tomcat accounts:

- Administrator account (manager-gui)
- Script account (manager-script)

> **Information**
>
> Depending on your configuration, there may be any number of Windows accounts used to run any number of Apache Tomcat servers. Make sure the account names and passwords for all of these accounts are recorded somewhere. One Windows service account may be used to run any number of Apache Tomcats to keep administration simple.

Database

- Computer name
-

Type (MS SQL/Oracle/DB2/PostgreSQL)
- Port
- Storage location
- Miscellaneous: Instance name, authentication mode, database name/schema, etc.

> **Please note**
>
> When using IMB DB2, the database parameter `extended_row_sz` has to be set to `ENABLE` manually.

Apache Tomcat

- Computer name (name for ELOenterprise)
- Apache Tomcat service
- Ports
- Version

> **Information**
>
> The default server configuration for ELO ECM Suite installs four Apache Tomcat instances. Your specific configuration may be different depending on your specific requirements. Record information for each Apache Tomcat server in use here.

Windows Service account

By default, the ELO server components use the local system account. For security reasons, it is recommended to run both Apache Tomcat and the database services on a domain account with limited privileges for production systems. We recommend that you create Active Directory domain service accounts for these accounts.

Please note

The account used for this is also required for the following directories/files:

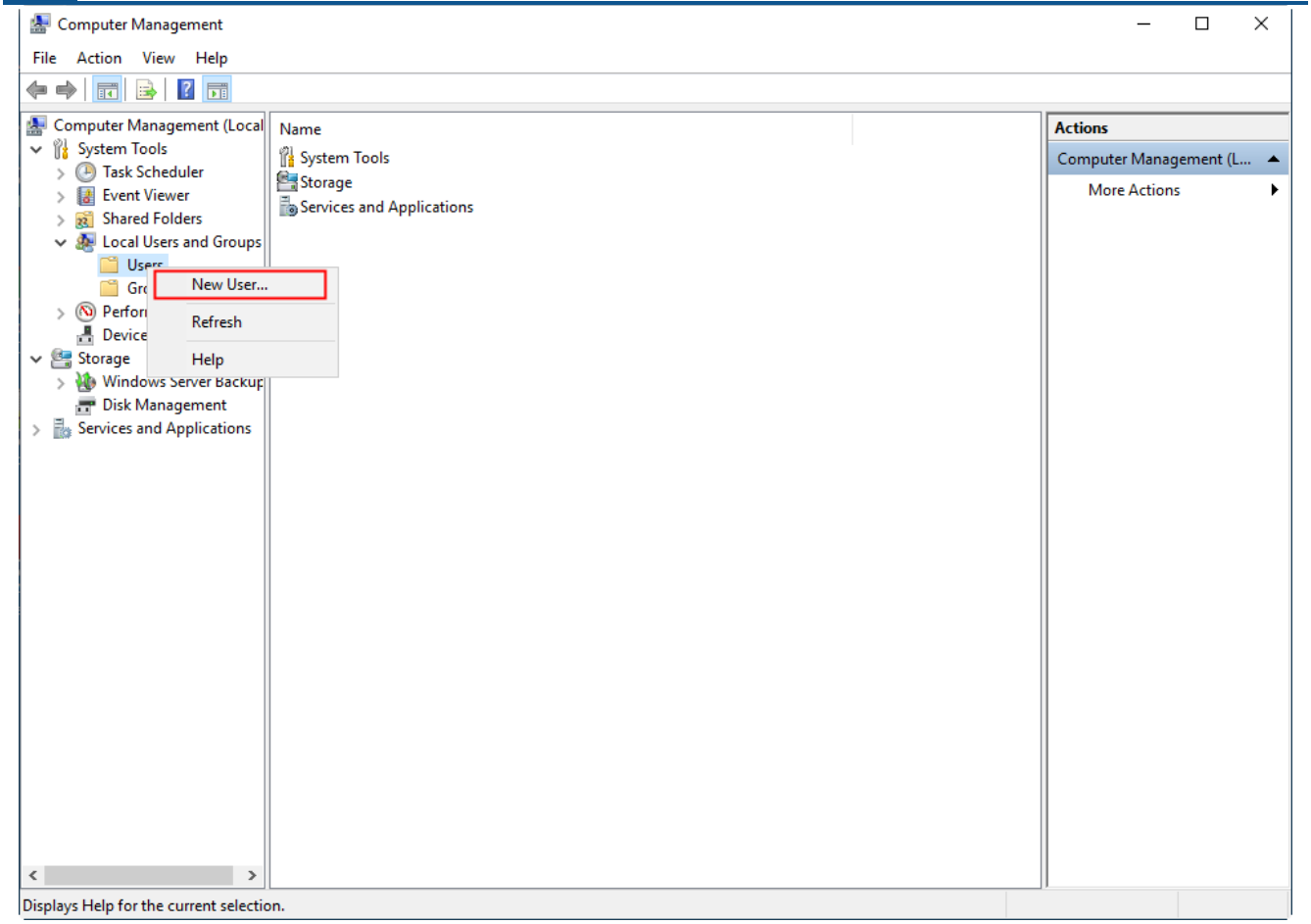
- Folder *lib*: For each Apache Tomcat server. Stored under: `<ELO>\servers\<server name>-1\lib`, for example.
- Folder *webapps*: Stored under `<ELO>\prog\webapps`
- File *jmxremote.password*: Stored under `<ELO>\config\serversetup2\jmxremote.password`

The ELO Server Setup sets the permissions for the account in the appropriate directories. The permissions are passed on to all child entries.

Make sure that the account you are using has the necessary permissions to access directories/files.

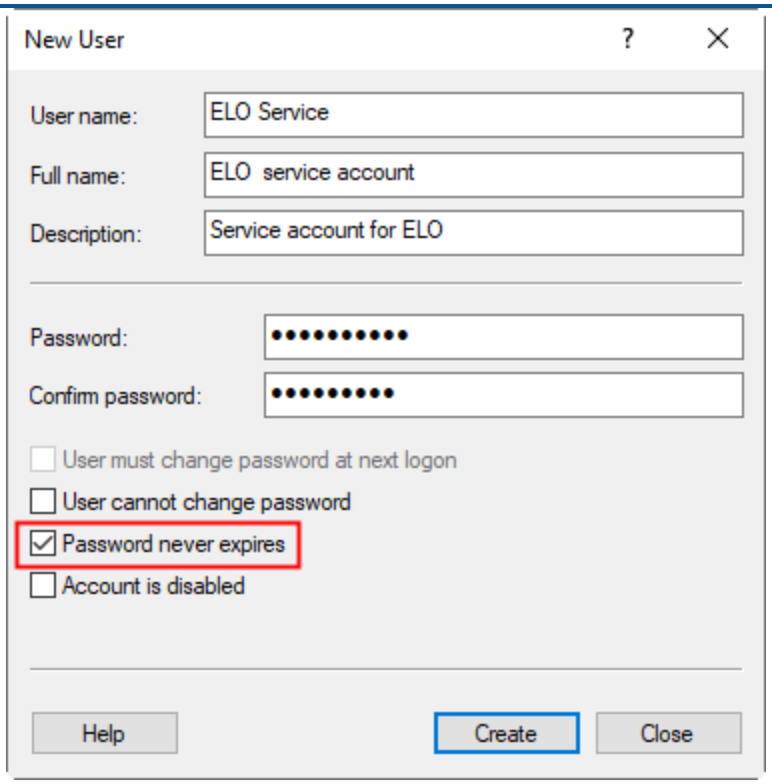
Create 'ELO Service' account

To create the *ELO Service* account, open the *Active Directory Users and Computers* window and select a domain node and folder in which you want to create it. This account should not be assigned to any groups other than *Domain Users*. This prevents the account from being unintentionally granted rights that the account does not need or should not have. It is especially important that the *ELO Service* account is not assigned to any of the administrator groups.



1. Open the content menu of the required folder.

2. In the context menu, select *New User*.



The *New User* dialog box opens.

3. Enter a name for the account (*ELO Service* in this example) and a password.
4. Clear the option *User must change password at next logon*.
5. Enable *Password never expires*.
6. Select *Create* to create the account.

> **Important**
>
> If the option *User must change password at next logon* is selected for a service account, you must log on with that account manually and change the account password before it can be used. Otherwise, services associated with that account will not start.

This closes the dialog box.

7. Open the Group Policy Management Editor and assign the account the *Log on as a service* right.

Microsoft SQL Server

A database must be up and running before the ELO server components can be installed. ELOprofessional and ELOenterprise support Microsoft SQL Server, PostgreSQL, IBM DB2, and Oracle database products. See the separate System requirements documentation for more information on the supported versions of each product. The following instructions detail how to set up Microsoft SQL Server for use with ELO.

> **Please note**
>
> Please ensure that your computer has enough free storage space before starting the installation. Microsoft SQL Server requires at least 6 GB free disk space.

If any of these components need to be updated, the setup routine will automatically download and install the required components. Please see the Microsoft website for more details on the system requirements.

Account

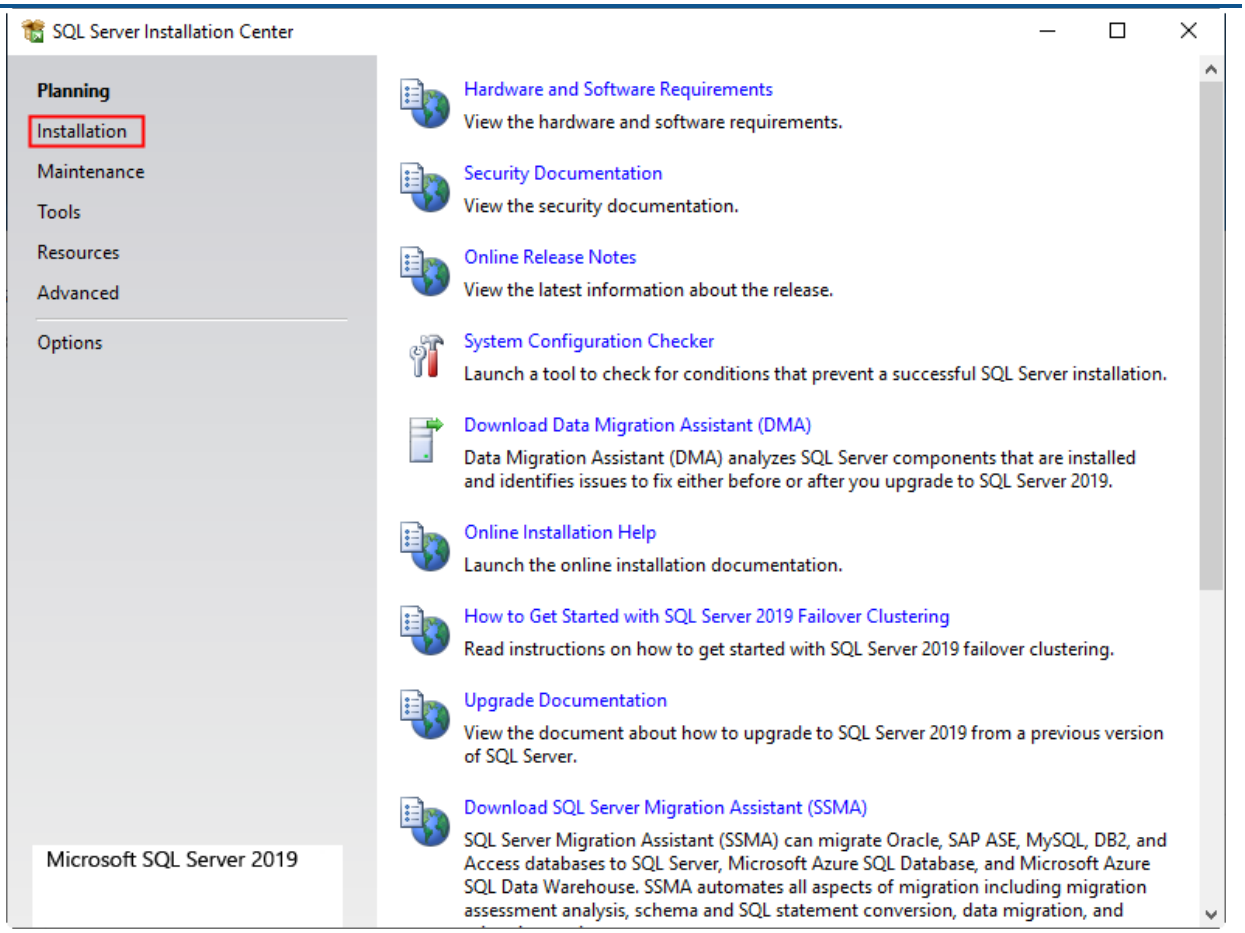
Before installing Microsoft SQL Server, create a service account on the domain, e. g. *SERVICESQL*. You can also create the service account within a group designed for it, e. g. *GRPSQLADMINS*. You must give this account the *Log on as a service* Windows right.

Server RAM

It is recommended to assign the SQL Server approximately 20 percent more RAM than the largest ELO database in order to ensure maximum performance as well as for future updates.

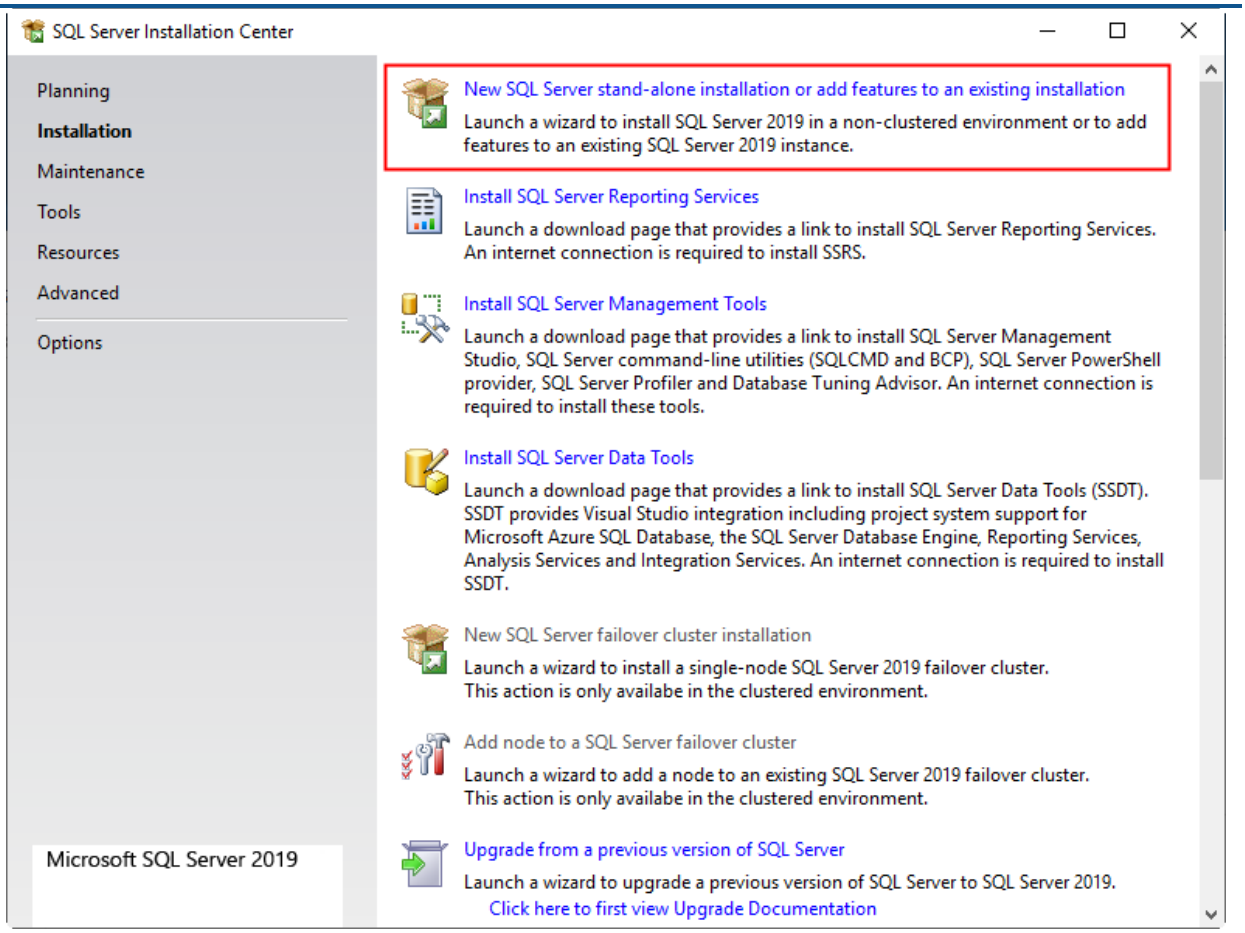
Installation of Microsoft SQL Server

1. Run the Microsoft SQL Server setup.



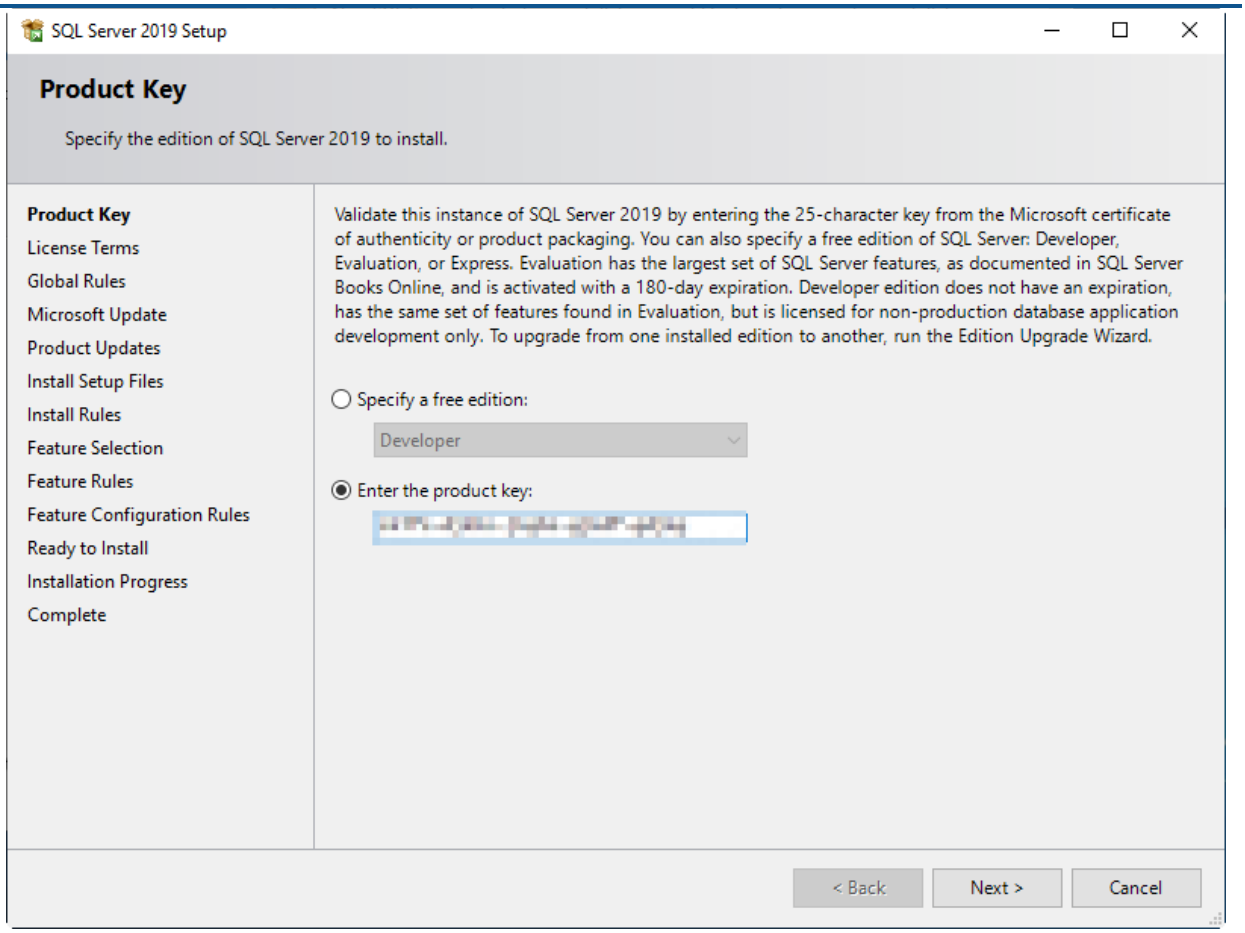
The SQL Server Installation Center opens.

2. Select *Installation* in the left navigation pane to select the required installation type.



The *Installation* tab appears.

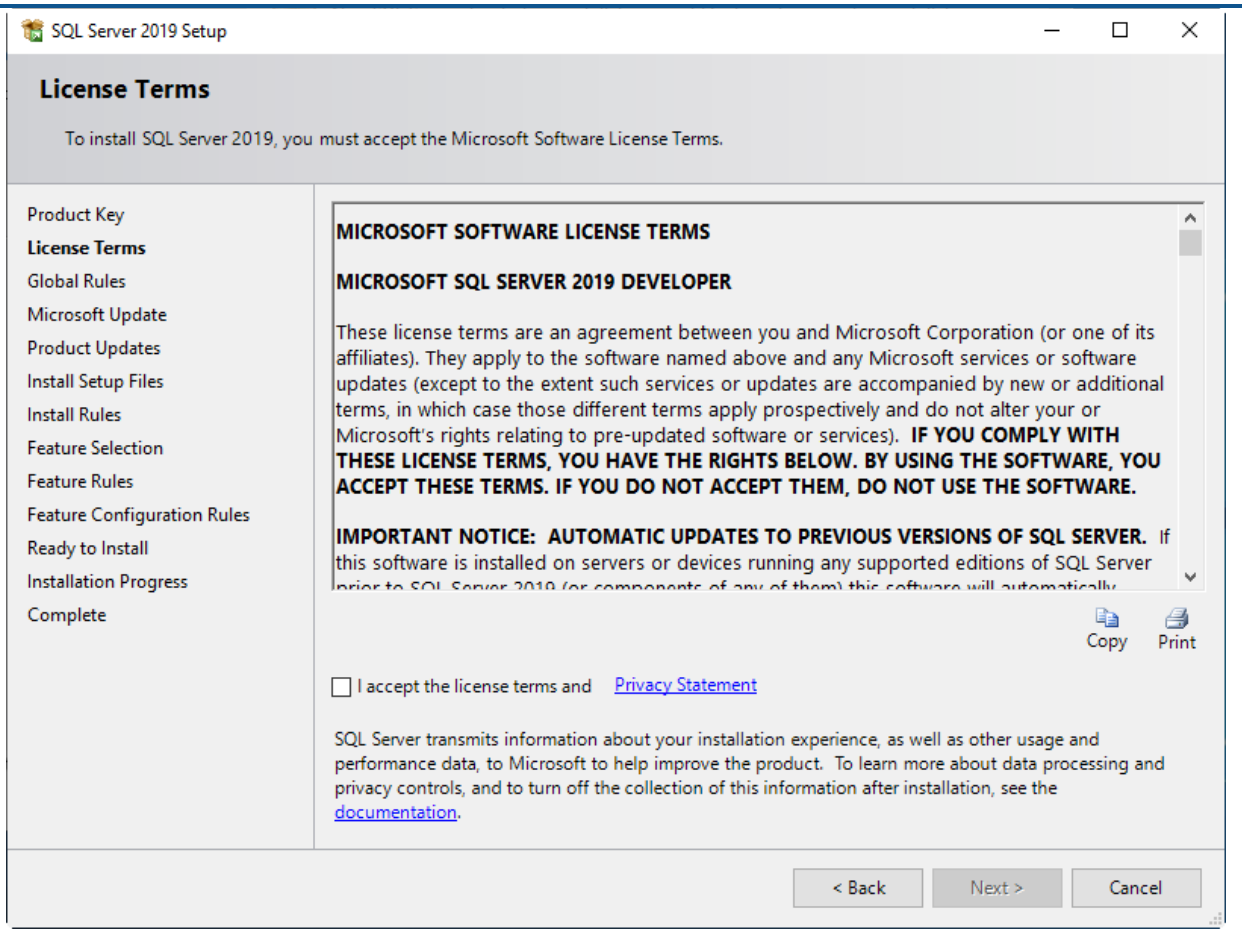
1. Now select *New SQL Server stand-alone installation or add features to an existing installation*.



The *Product Key* screen opens.

2. Enter the license key in the *Enter the product key* field.

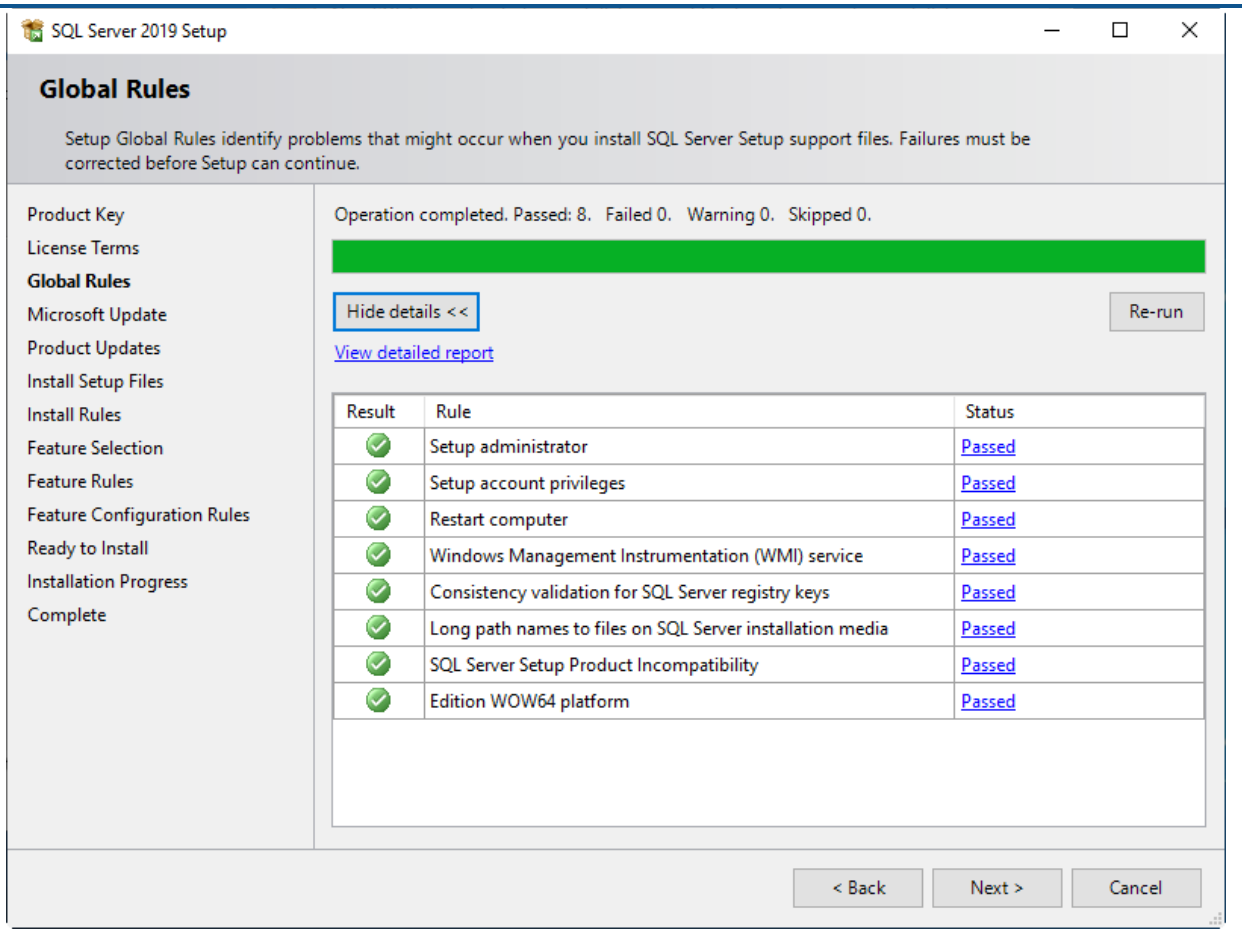
3. Select *Next*.



The *License Terms* screen opens.

4. Confirm the license terms by selecting the *I accept the license terms and Privacy Statement* check box.

5. Select *Next*.

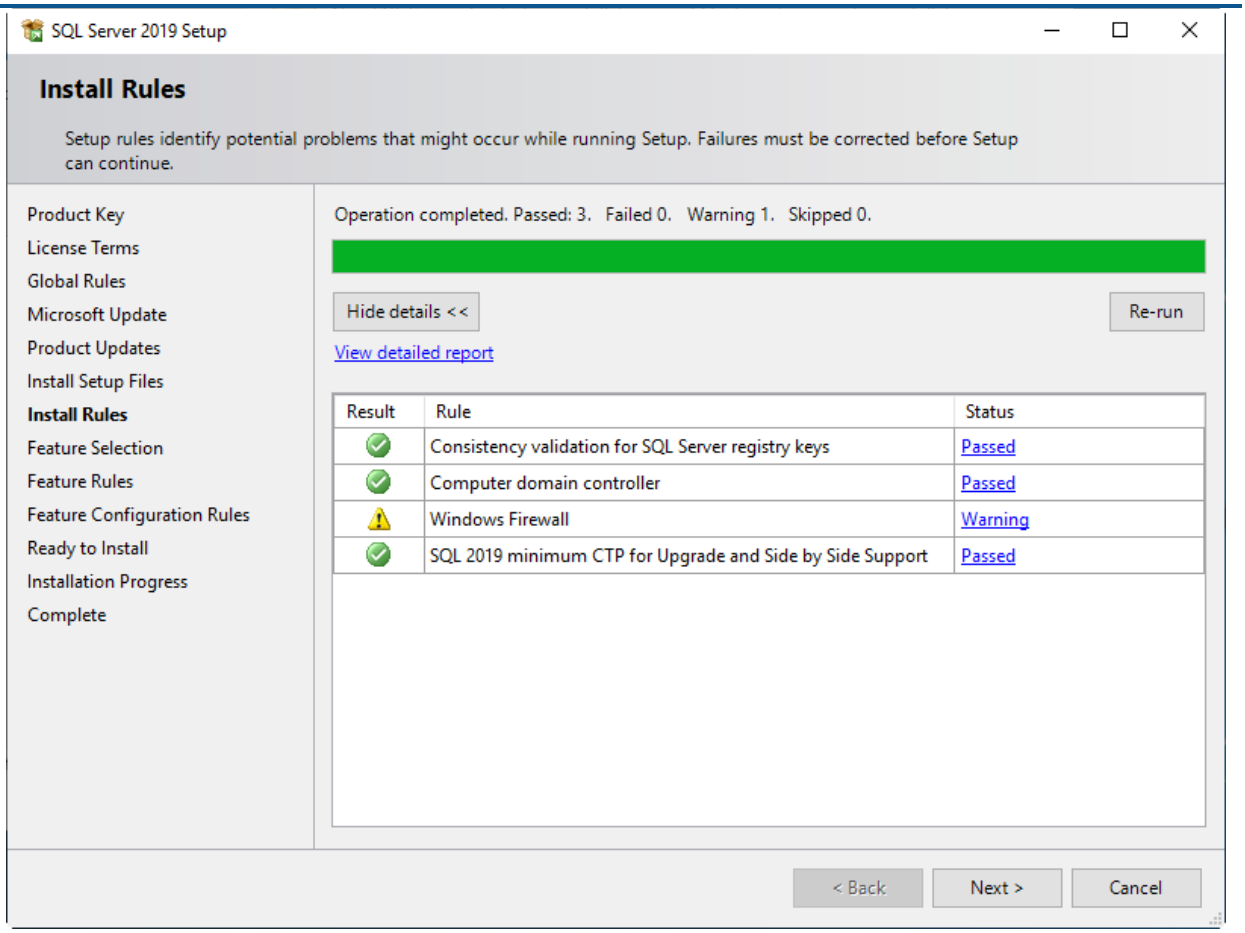


The *Global Rules* screen opens. The installer first checks whether all conditions are met for installing SQL Server. If any errors are detected, they must be corrected before proceeding with the installation.

6. When the check completes successfully, select *Next*.

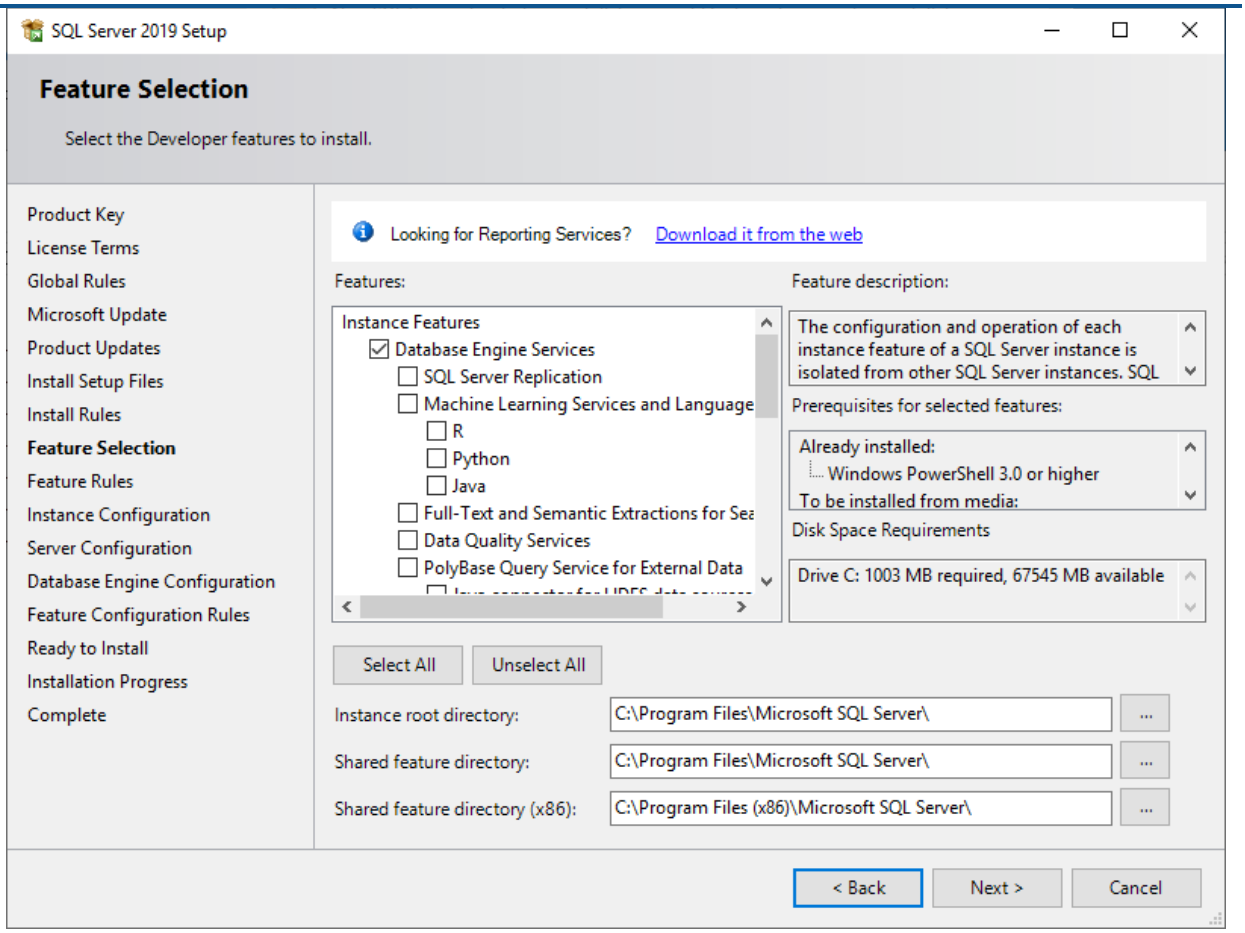
   Optional: SQL Server Setup may ask you whether you want to use Windows updates.

   If you enable the option, SQL Server Setup searches for updates and installs them.



The *Install Rules* screen opens. If you see a warning about the Microsoft Windows Firewall, you can ignore it.

7. Select *Next*.



The *Feature Selection* screen appears. You can modify the installation paths and select individual components.

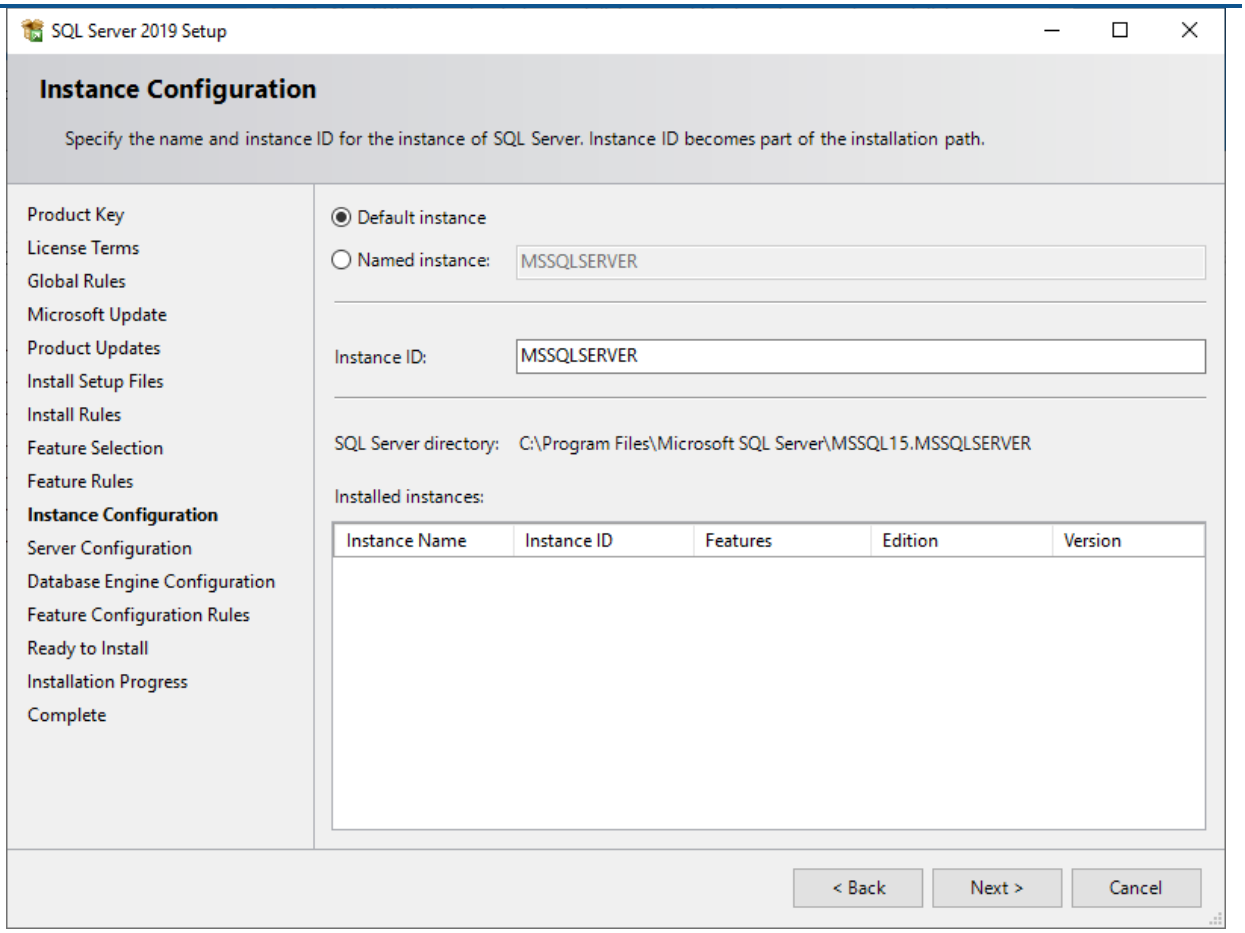
8. Enable the component *Database Engine Services*.

   Optional: Enable other components as required.

> **Information**
>
> You *must* install Microsoft SQL Server Management Studio after completing the setup. To do this, you need to download the corresponding package from the Internet. You *can* install additional components such as *Analysis Services* or Reporting Services in the same way.

9. Select *Next*.

   The installer checks whether the rules for the selected components are in passed status.



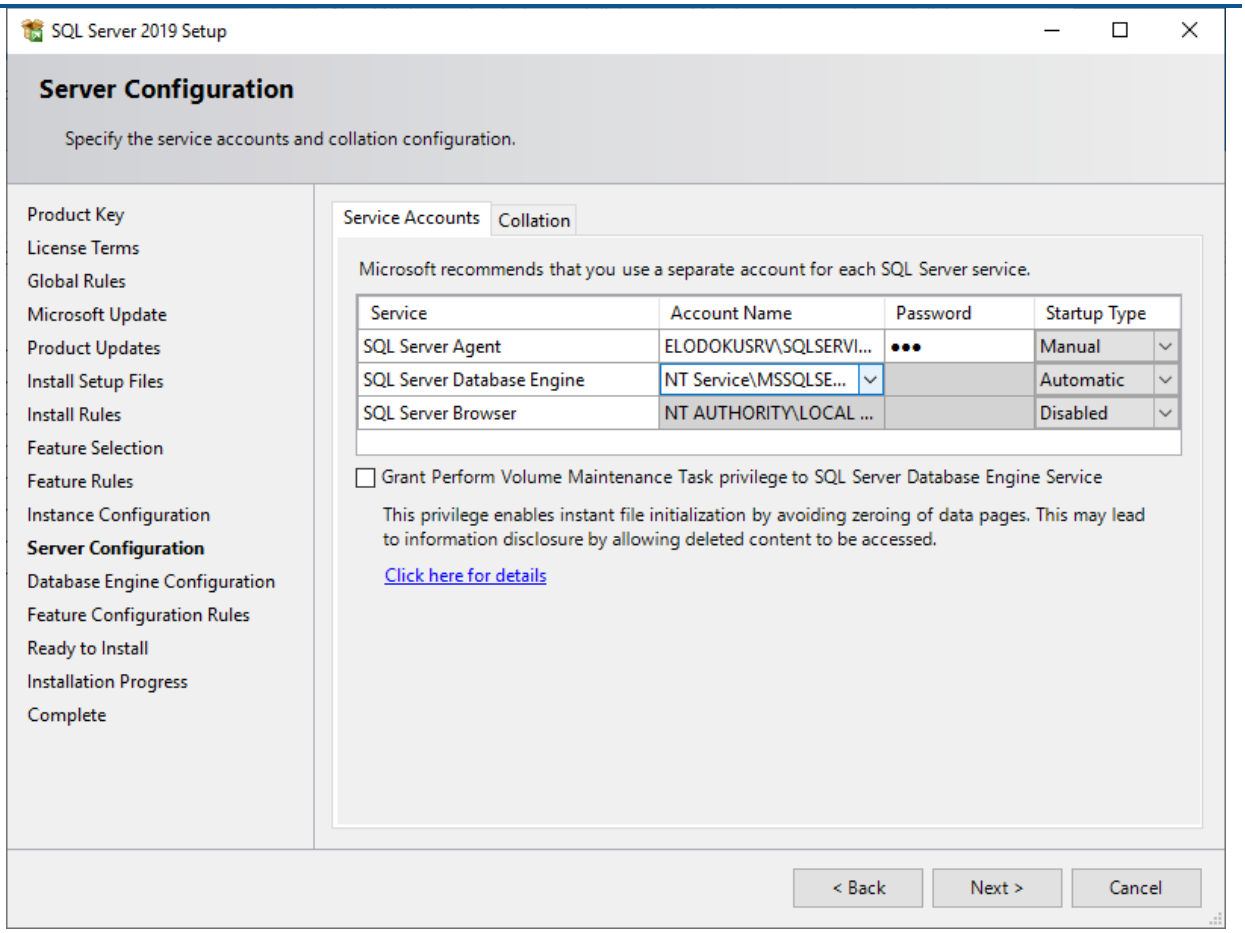
The *Instance Configuration* screen opens.

> **Please note**
>
> Before configuring SQL Server, it is recommended to create a separate account in Windows for running the SQL Server service. Instructions for doing this can be found at the beginning of the chapter under Account.

10. Select the option *Default instance*.

    Alternative: Select the *Named instance* option and enter the name of the instance and the instance ID.

11. Select *Next*.



The *Server Configuration* screen opens.

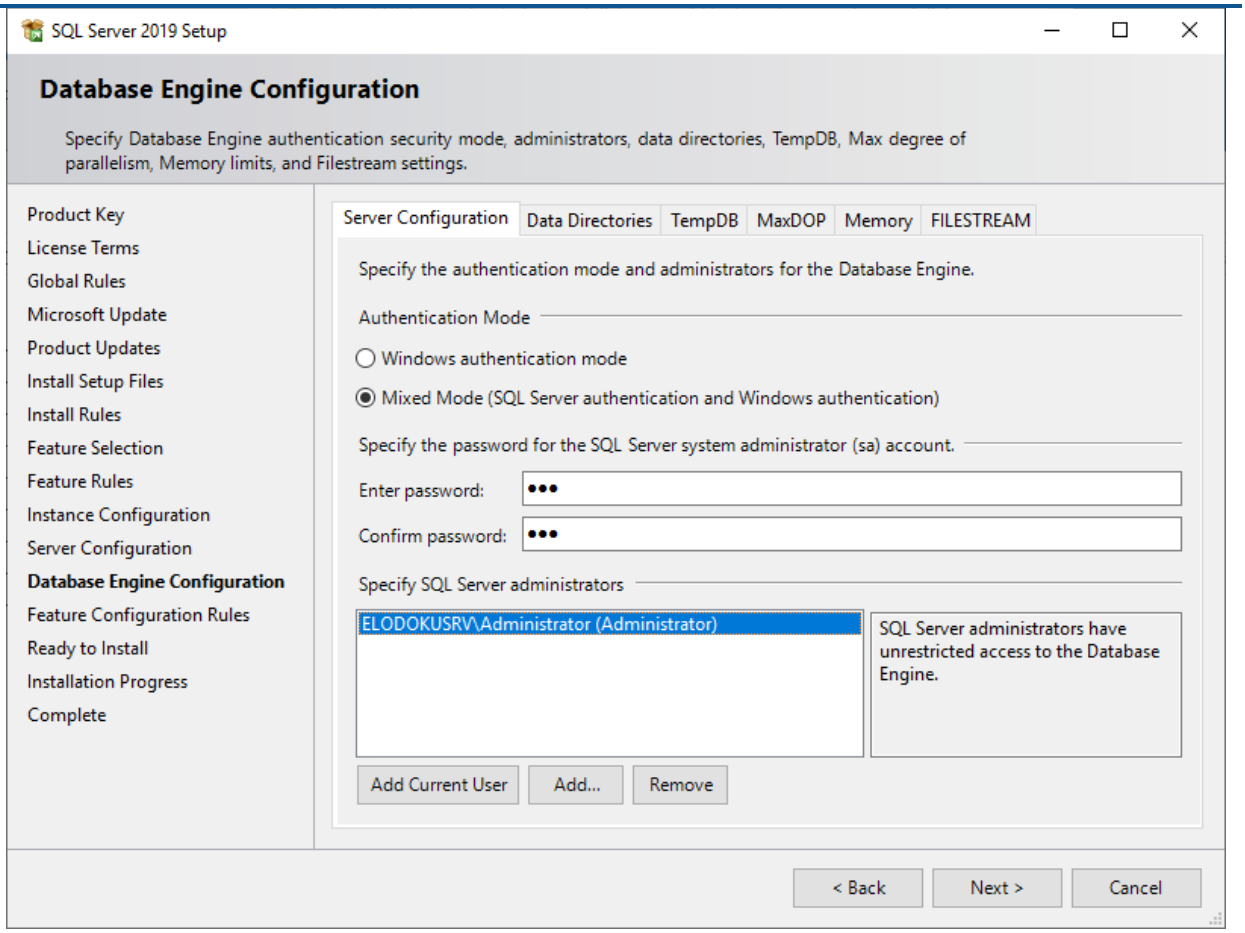
> **Please note**
>
> The most important entry is the *SQL Server Agent*. Assign the Active Directory SQL service account (e. g. SQLSERVICE) to this account here. It is easier to do so during installation. However, the end of this chapter provides some notes on how to do this after the installation.
>
> In the drop-down menu under *Startup Type*, select *Automatic*.

12. Enter the account names and passwords for the services required by SQL Server.

    On the *Collation* tab, you can change the collation settings for the database. These settings control the types of data used by the database and how they are sorted.

> **Please note**
>
> Keep the default setting case insensitive (CI) on the *Collation* tab. Changing these settings after you install SQL Server may require significant time and effort.

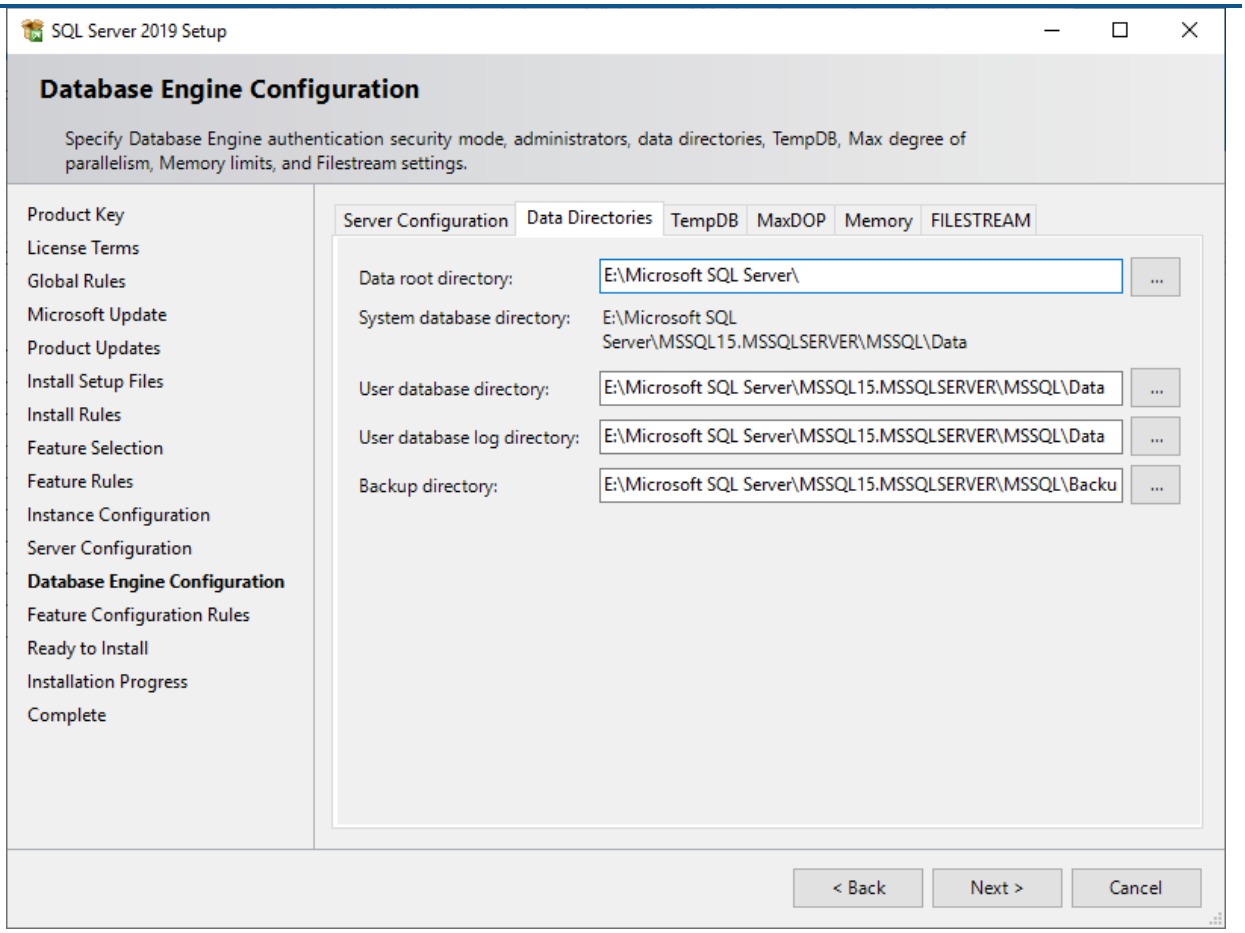
13. Select *Next*.



The *Database Engine Configuration* screen opens.

14. Under *Authentication Mode*, select the *Mixed Mode* option.

15. Enter the SQL server administrator account (sa) as well as the corresponding password.



16. On the *Data Directories* tab, change the location of the database files.

    For production environments, you should think carefully about where these directories are stored.

    > **Please note**
    >
    > Never store the database files on the `C:\` drive.
    >
    > In addition, you should never store the installation files straight after the drive letter but always in a child folder.

    The *Data root directory* field is where you specify the root directory for the database files.

    The *User database directory* path contains the MDF files that make up the actual databases. This directory must exist on the same server as the SQL Server software.

    The *User database log directory* path contains the LDF files, i.e. the transaction log files. You should store this directory on a high-performance drive.

    You can enter UNC paths to the *Backup directory* field. You should store backups on a separate drive on the network.

17.

The *TempDB* tab is where you manage the temporary directories and the corresponding log directory.

Swap files are temporarily stored in this directory. The initial size of this directory should be limited to roughly 20 percent of the size of the largest database. Every time a new SQL Server instance is started, the temporary directory is reset to its initial size.

> **Please note**
>
> Never store the temporary database files on the `C:\` drive.

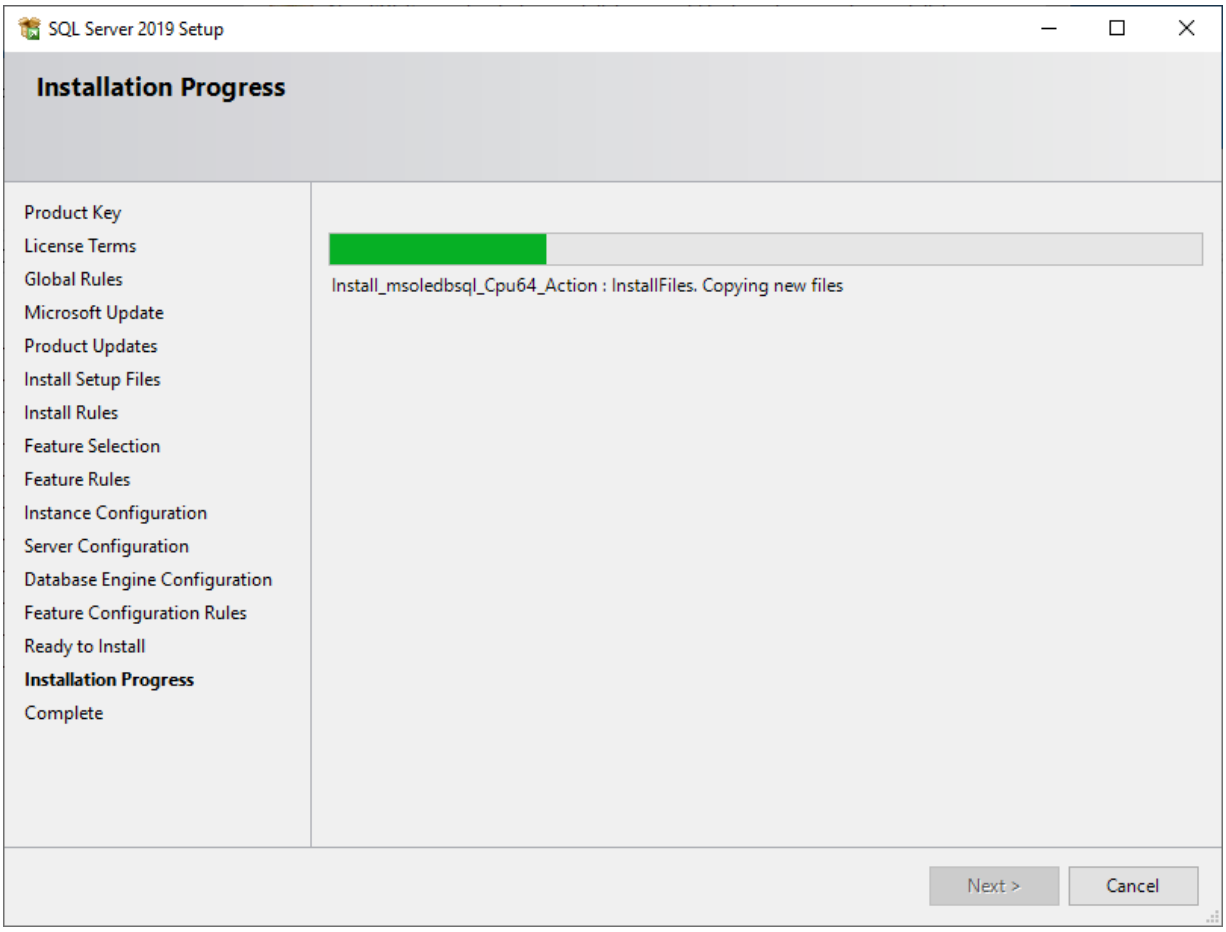
The *temporary database log directory* should be created in the same way as the user database log directory.

Optional: You can enable *FILESTREAM* on the FILESTREAM tab. Consult the Microsoft documentation for more information on this topic.

18. Select *Next*.

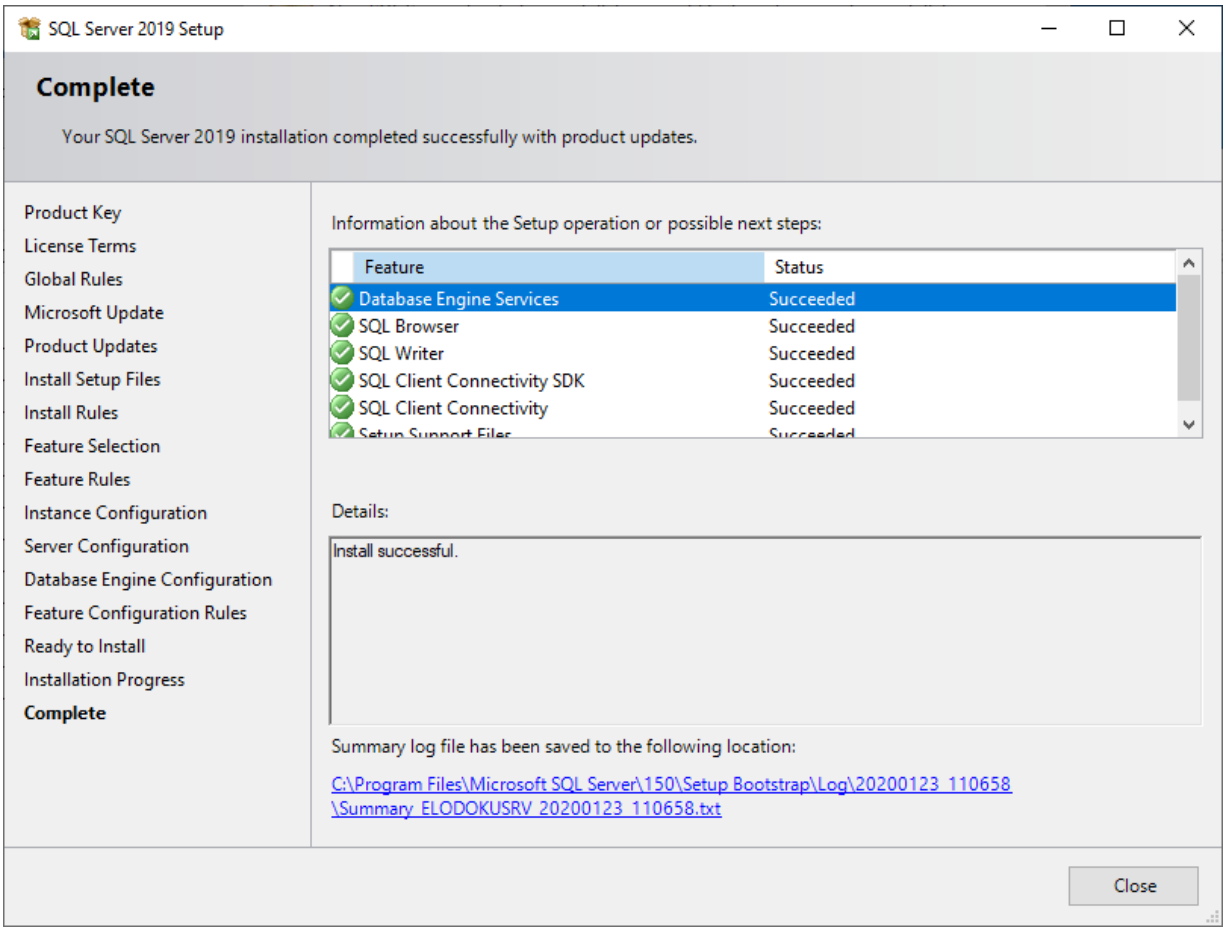
    The *Ready to Install* screen opens. You see a summary of the selected settings.

19. Check the settings and select *Install*.



The *Installation Progress* screen opens. This is where you see the installation progress.

20. After installation is completed, select *Next*.



The *Complete* screen opens. This is where you see that the installation was completed.

21. Select *Close* to finish the installation.

> **Information**
>
> It is recommended to download and install any available updates or service packs immediately after installation if the updates were not installed automatically during installation.
>
> Next, install Microsoft SQL Server Management Studio.

elodb account

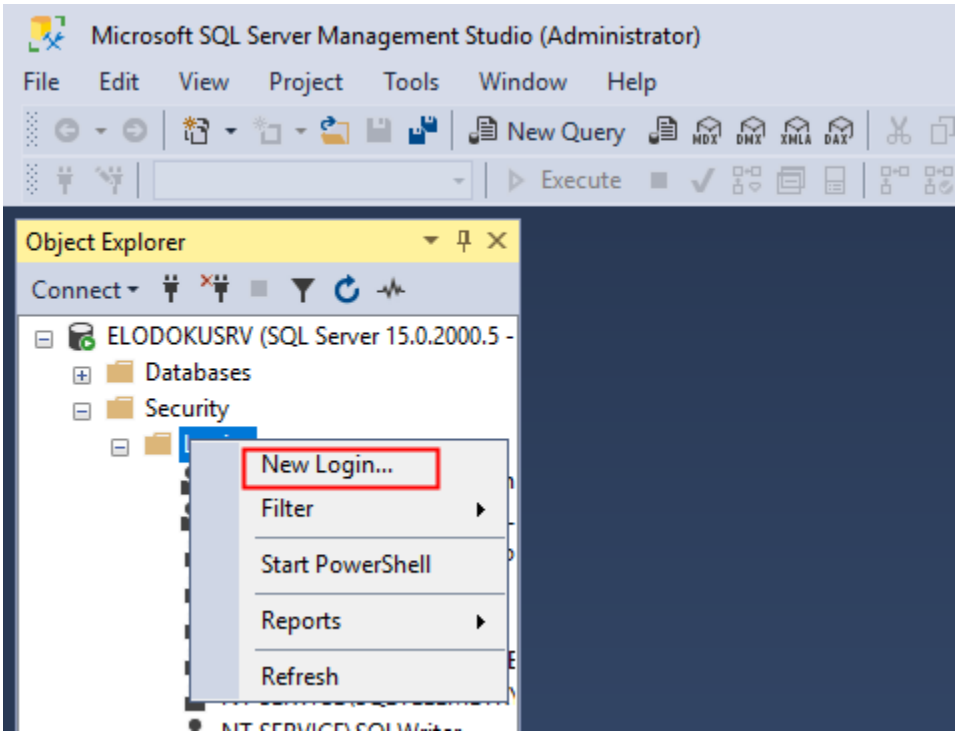
After installing Microsoft SQL Server and Microsoft SQL Server Management Studio, you can create a database account that ELO uses to manage repositories.

1. Start Microsoft SQL Server Management Studio and log on.

Please note

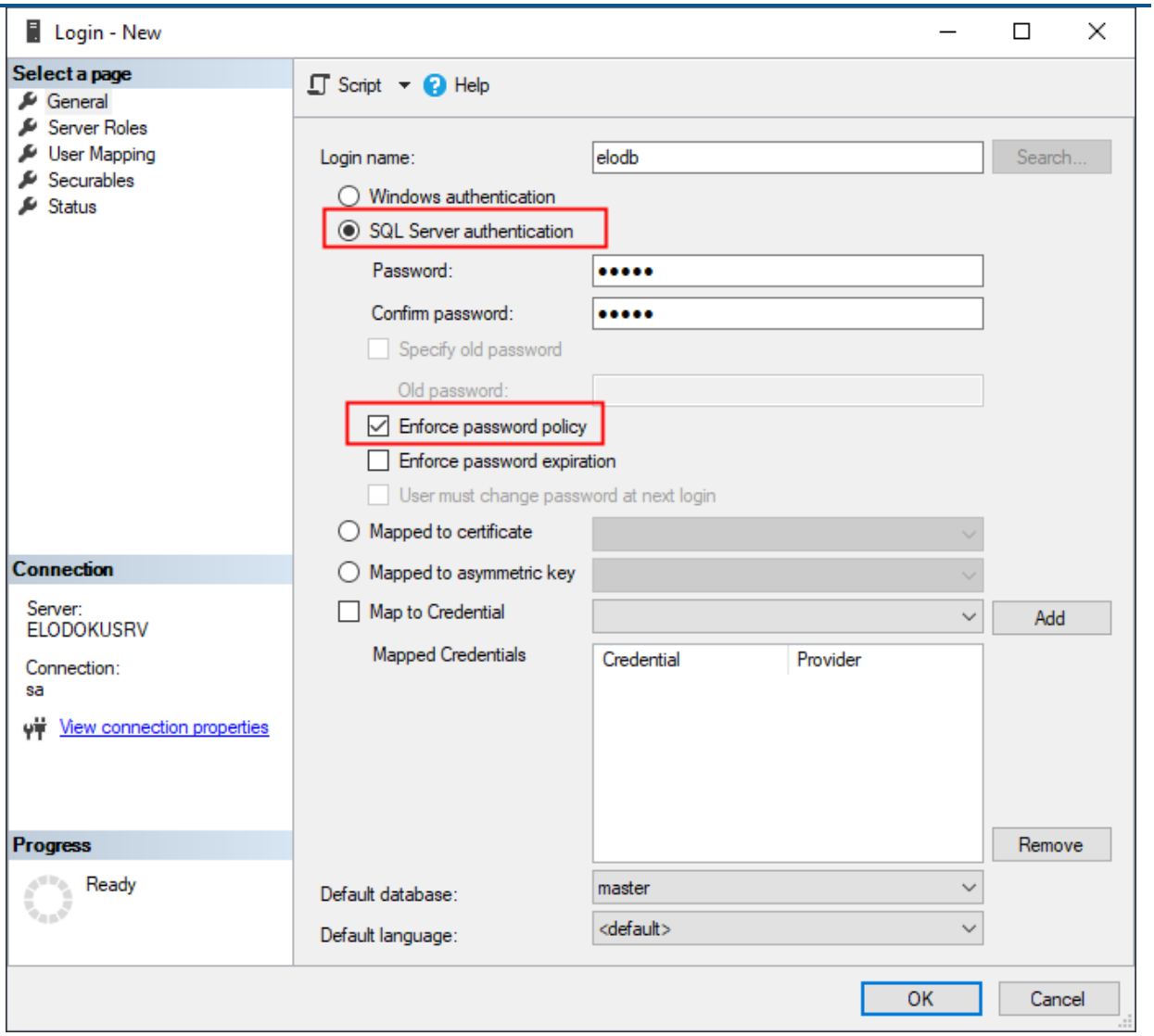
This step is required in the ELO ECM Suite. You can use the database administrator account (sa) as the ELO database account, but this is not recommended in production environments for security reasons.

2. In the Object Explorer, navigate to *Databases* > *Logins*.



3. Open the context menu.

4. Select the *New Login* menu item.



A window opens in which you can create a new database account.

5. Configure the account with the following settings:

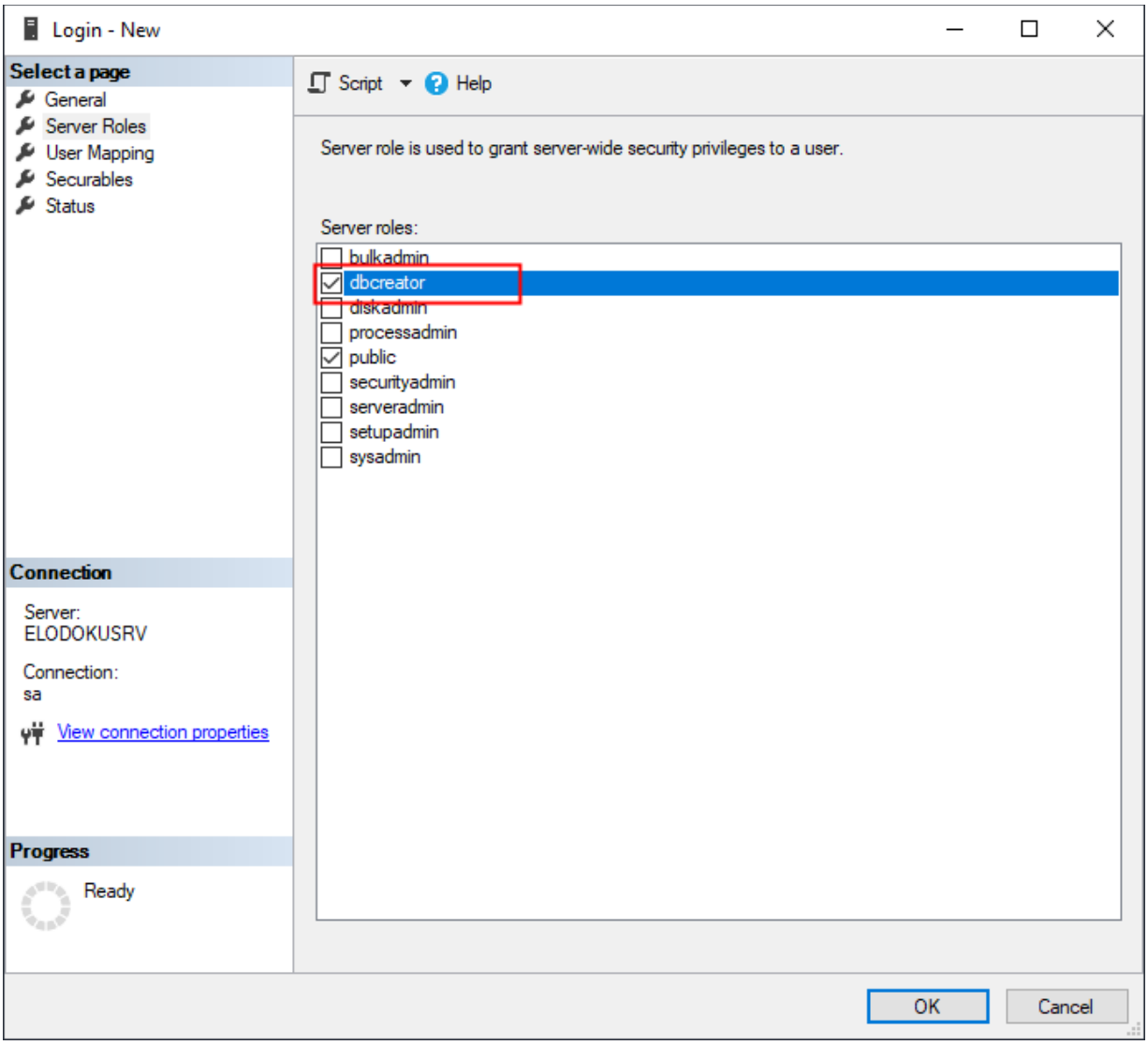
   - Login name: elodb

     > **Information**
     >
     > The database account does not need to be named `elodb`. If you choose a different name for the database user here, make sure you change the names when installing the ELO server.

   - SQL Server authentication: Enabled
   - Password: Assign a secure password
   - Enforce password policy: Enabled (recommended)
   -

Enforce password expiration: Disabled

Optional: You may select *Enforce password policy* if you wish to apply the computer's password rules to the database account.



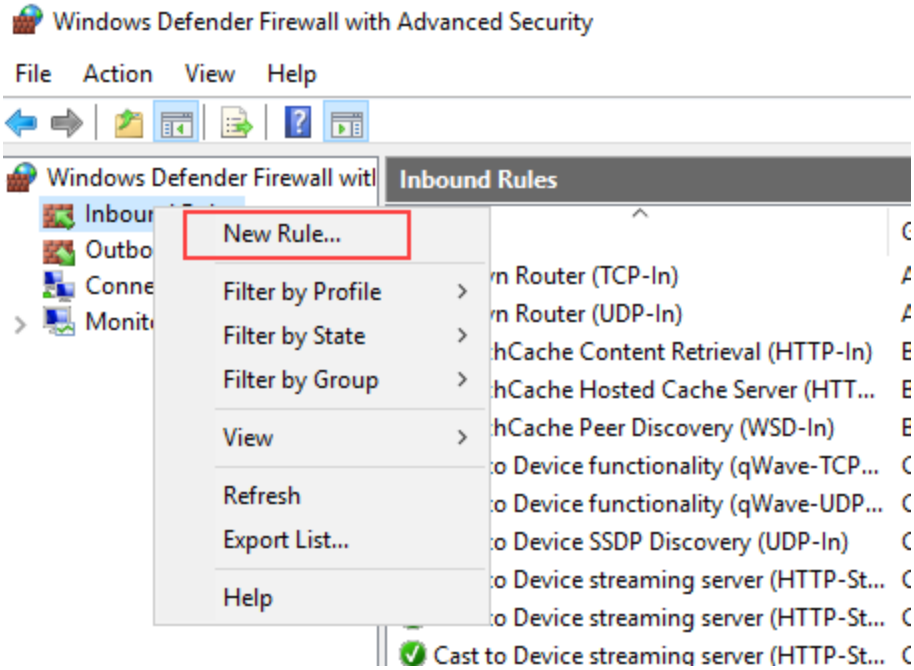
6. Switch to the *Server Roles* screen and select the *dbcreator* check box.
7. Select *OK* to create the database account *elodb*.
8. Close Microsoft SQL Management Studio to begin installing the ELO server components.

Open port

The port for the Microsoft SQL database is not automatically opened during the installation of the database. After installation, create a corresponding inbound rule for the Microsoft firewall.

1. Open Windows Firewall with Advanced Security.
2. Select the *Inbound Rules* menu item.
3.

Open the context menu of the *Inbound Rules* menu item.



4. Select *New Rule*

   The dialog box for creating inbound rules opens.

5. Select the type *Port*.
6. Select *Next*.
7. Enter the port of the SQL database in the *Specific local ports* field.
8. Select *Next*.

   The *Allow the connection* option must be enabled.

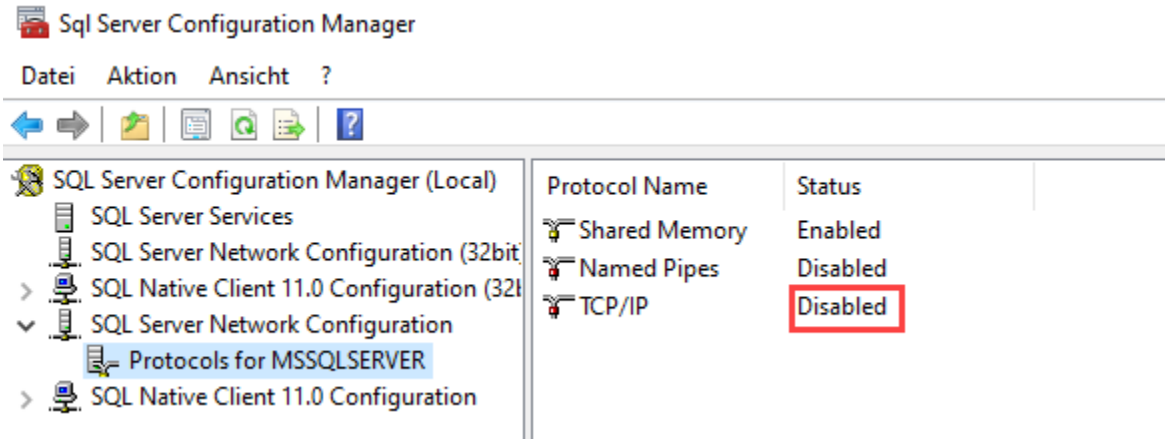
9. Select *Next*.

   The *Profiles* screen opens.

10. Select the required setting for your network.
11. Select *Next*.
12. Enter a name for the rule in the *Name* field.
13. Select *Finish*.

The port is now open.

Enable TCP/IP



With the default settings, TCP/IP is disabled.

You need to enable TCP/IP using the *SQL Server Configuration Manager* tool.

1. Press the keyboard shortcut WINDOWS+R.

   The *Run* dialog box opens.

2. Enter the following command in the *Open* field:

   ```
   SQLServerManager<Version>.msc
   ```

   > **Information**
   >
   > You will find the version of the tool that matches your Microsoft SQL version at docs.microsoft.com.

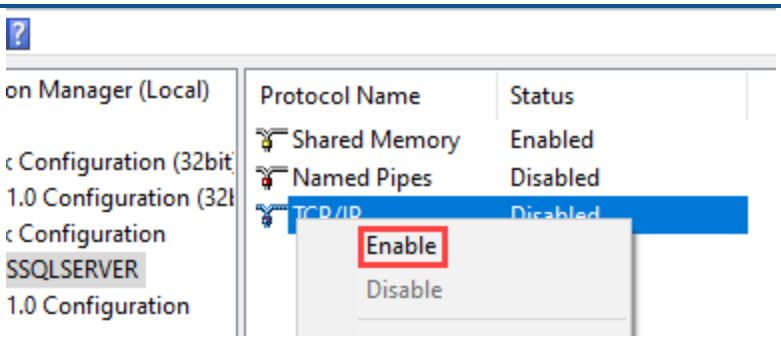
3. Execute the command.

   SQL Server Configuration Manager starts.

4. Select *SQL Server Network Configuration*.

5. Select *Protocols for <Instance name>*.

   You will see a list of protocols and their status.



6. Open the context menu of the *TCP/IP* entry.
7. Select *Enable*

TCP/IP is now enabled.

SQL Server Agent

When you install Microsoft SQL Server, the Microsoft SQL Server Agent is disabled by default. This is a Windows service that performs administrative tasks.

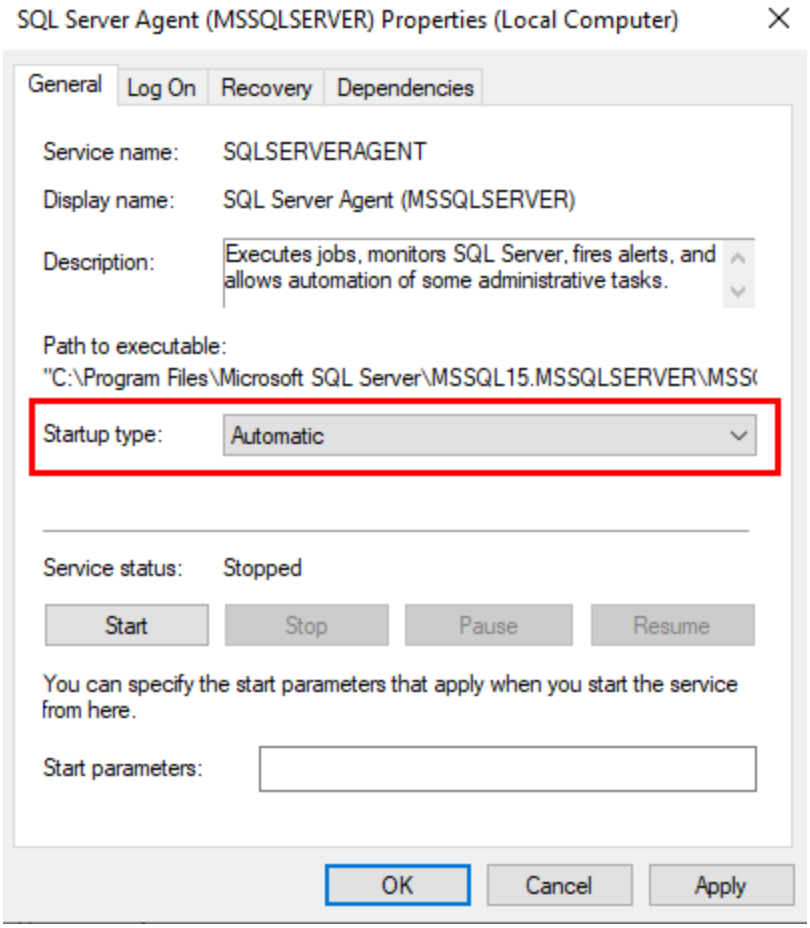
When you are installing Microsoft SQL Server, you can set the SQL Server Agent *Startup Type* to *Automatic*.

If you did not enable the service during the installation, you must enable it later so that maintenance tasks are automatically executed with Microsoft SQL Server.

1. To enable the agent, press the keyboard shortcut WINDOWS+R.

   The *Run* dialog box opens.
2. Enter "services.msc" in the *Open* field.
3. Select *OK*.

   The *Services* dialog box opens.
4. Open the context menu of the *SQL Server Agent* entry.
5. In the context menu, select *Properties*.



The *SQL Server Agent Properties* dialog box opens.

6. In the drop-down menu under *Startup type*, select the *Automatic* entry.
7. Select *Start*.
8. Open Microsoft SQL Server Management Studio and check the status of the SQL Server Agent in the Object Explorer.

If it is running, you can move on to set up administrative tasks.

Database performance

Reduce fragmentation

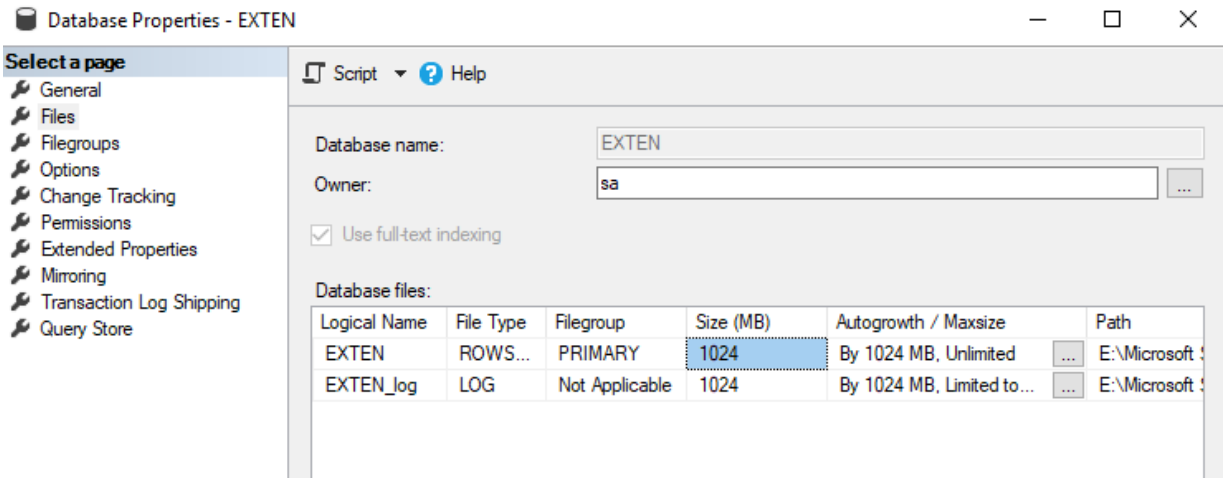
When ELO is installed, it uses the default values in Microsoft SQL Server for initial size and growth rates. These values can lead to fragmentation and reduced performance over time in production environments.

1. Log on to Microsoft SQL Management Studio with the database administrator account.
2. Navigate to *Object Explorer > Databases*.
3. Check the values for each repository:

a) Open the context menu for a repository.

b) In the context menu, select *Properties*.

c) In the database properties, navigate to the *Files* screen.



There is no formula for calculating database sizes and growth rates that are ideal for all scenarios, but it is recommended to use the following as rules of thumb:

1. Set the initial size for the database (repository name) to 50 percent of the total anticipated database size in two years.
2. Set the initial size for the database log (repository name and *_log*) to ten percent of the total anticipated database size in two years.
3. Set the autogrowth rate for the database to 25 percent of the initial database size.
4. Set the autogrowth rate for the database log to 25 percent of the initial log size.

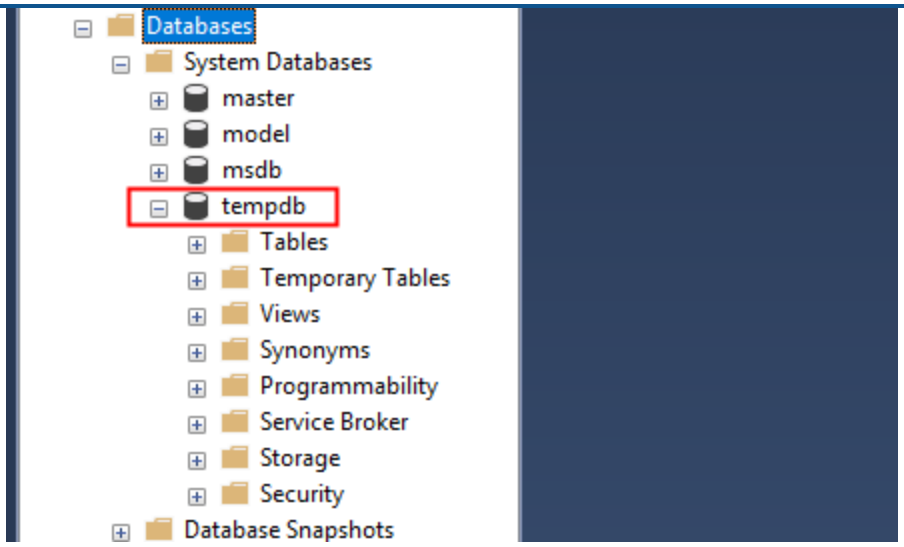
For example, if you anticipate the ELO database to take up 20 GB in two years, use the following settings:

-	**Size (MB)**	**Autogrowth**
Database	10240 MB	By 2560 MB
DB log	2048 MB	512 MB

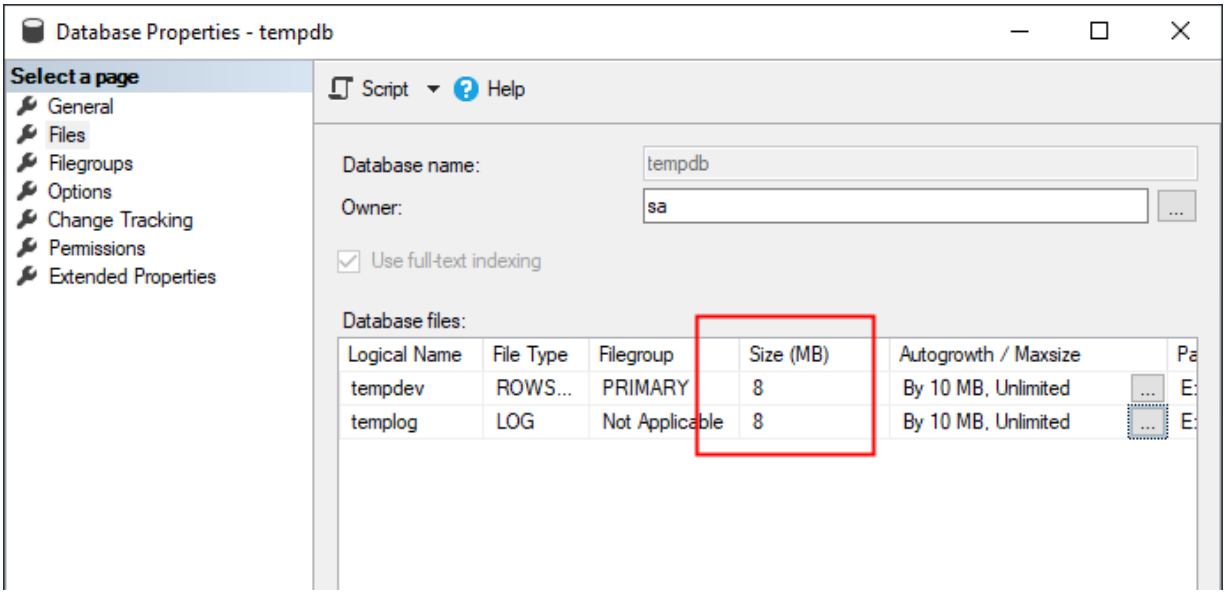
Adjustments to the tempdb database

The default values of the tempdb database in Microsoft SQL Server do not ensure optimal performance since they specify an initial size of only a few MB for the database and log files. Change this to a value about 20 percent of the largest ELO database.

1. Log on to Microsoft SQL Management Studio with the database administrator account.



2. Navigate to *Object Explorer > Databases > System Databases > tempdb*.
3. Open the context menu of the *tempdb* database.
4. In the context menu, select *Properties*.
5. Navigate to the *Files* screen.
6. Change the *Size* values for *tempdev* and *templog*.



   Change the values so that *tempdb* is about 20 percent of the largest ELO database and templog is about a tenth of that.

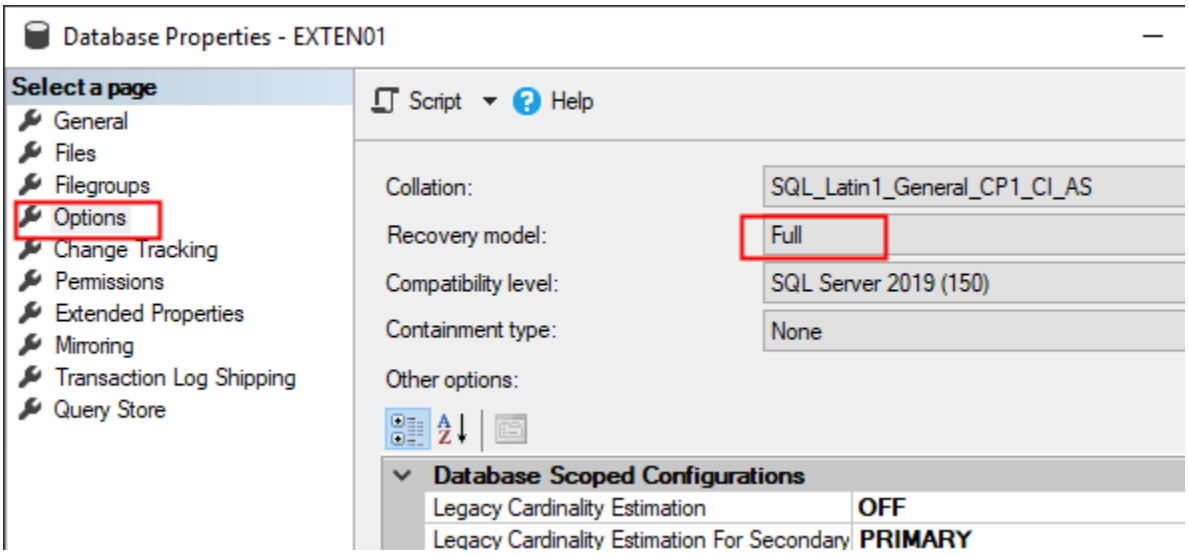
7. To apply the changes, select *OK*.

Recovery models

Once you have installed a database, you need to set up a maintenance and backup plan. The following sections describe how to set them up.

1. Log on to Microsoft SQL Management Studio with the database administrator account.
2. Navigate to *Object Explorer* > *Databases* > *<Repository name>*.
3. Open the context menu of the respective database.
4. In the context menu, select the *Properties* > *Options* item.

   Microsoft SQL Server supports three different recovery models: *Simple*, *Bulk-logged*, and *Full*. *Full* is the default mode for new ELO databases. It is usually best to keep this model because it allows for complete, differential, and transaction log backups.



5. Select the menu item *Full* in the *Recovery model* drop-down menu before you create a backup and maintenance plan.

Maintenance plans

First of all, you need to develop a concept for what the maintenance plan needs to achieve.

It is recommended to use the following plan as a minimum for a production database:

- Full daily backup of Microsoft SQL system databases
- Full daily backup of all user databases
- Periodic transaction backup of all databases running with the *Full* recovery model.

The transaction log backups should occur much more frequently than the full database backups. The more often the transaction log file is backed up, the smaller each log is, enabling you to recover the database to its state at the time of failure.

For this reason, it is recommended to back up transaction logs every 30 minutes or more.

Old backup files should always be deleted to avoid wasting space on your server. Set the options in the maintenance plan to delete the backup files after a few days.

Transaction logs, since they are created more often than full backups, can be deleted every few days or weekly.

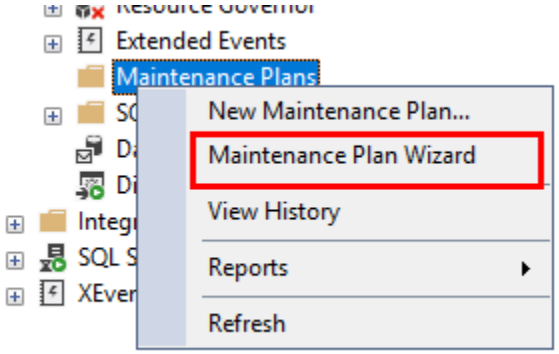
Maintenance plan for full backup and cleanup

The steps below describe how to set up a full daily backup of all databases, along with a *Maintenance Cleanup Task* for backups more than a few days old.

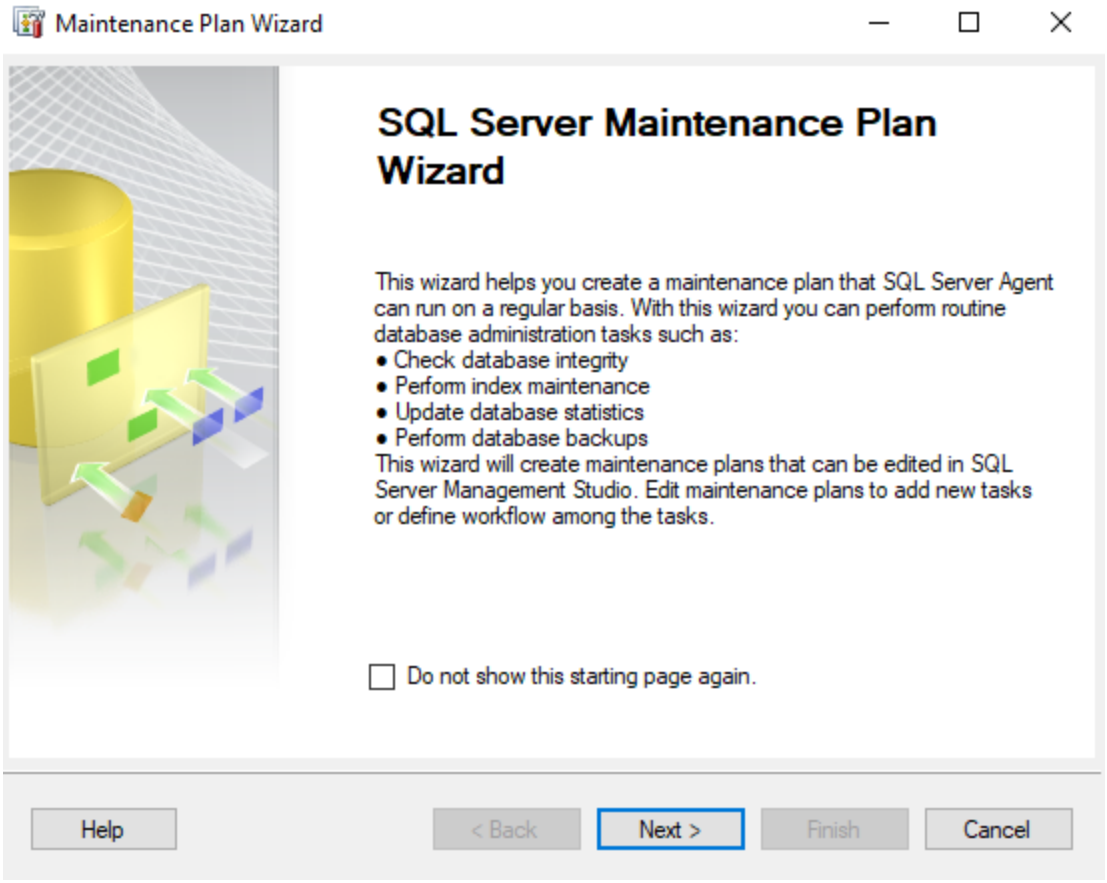
The examples of additional maintenance plans are created based on the same method.

Basic settings

1. In the Object Explorer, navigate to *Management > Maintenance Plans*.

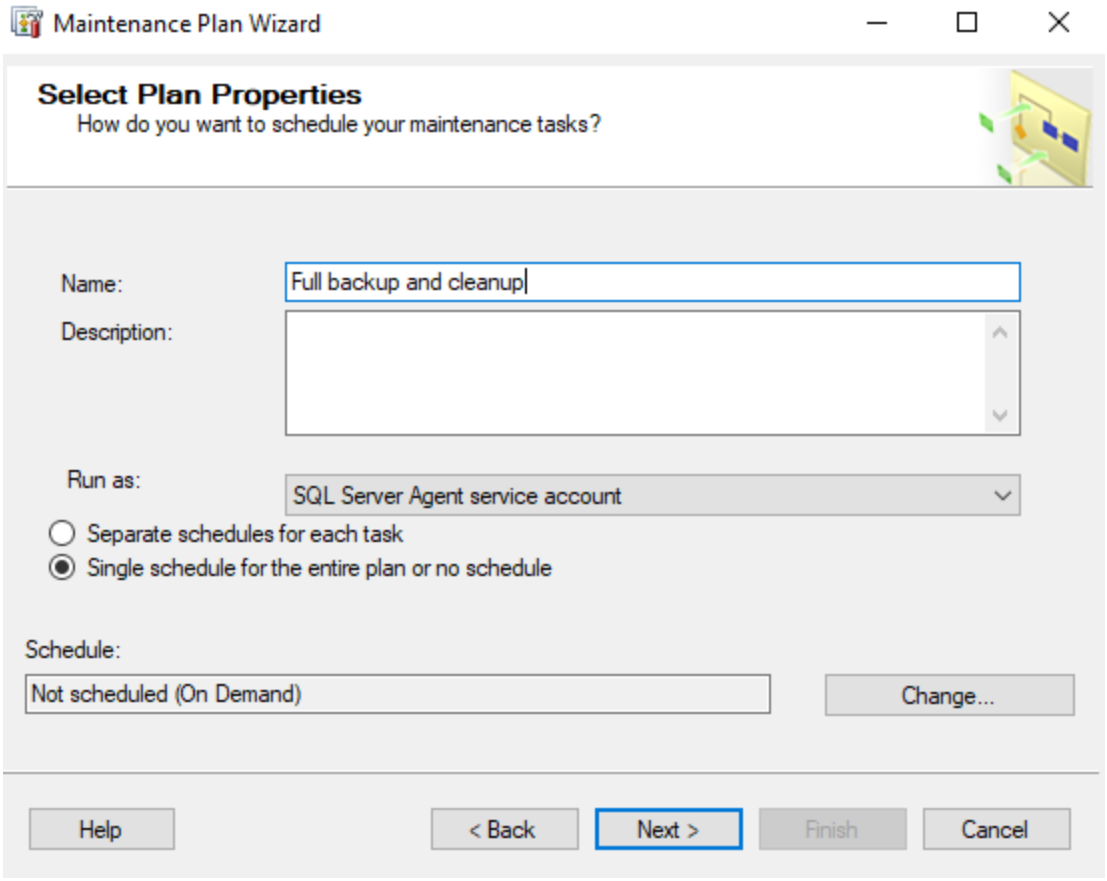


2. Open the content menu of the *Maintenance Plans* folder.
3. Select *Maintenance Plan Wizard*.



The *Maintenance Plan Wizard* dialog box opens.

4. Select *Next*.



The *Select Plan Properties* screen opens.

5. Complete the following fields as follows:

   Name: Enter a name in the *Name* field.

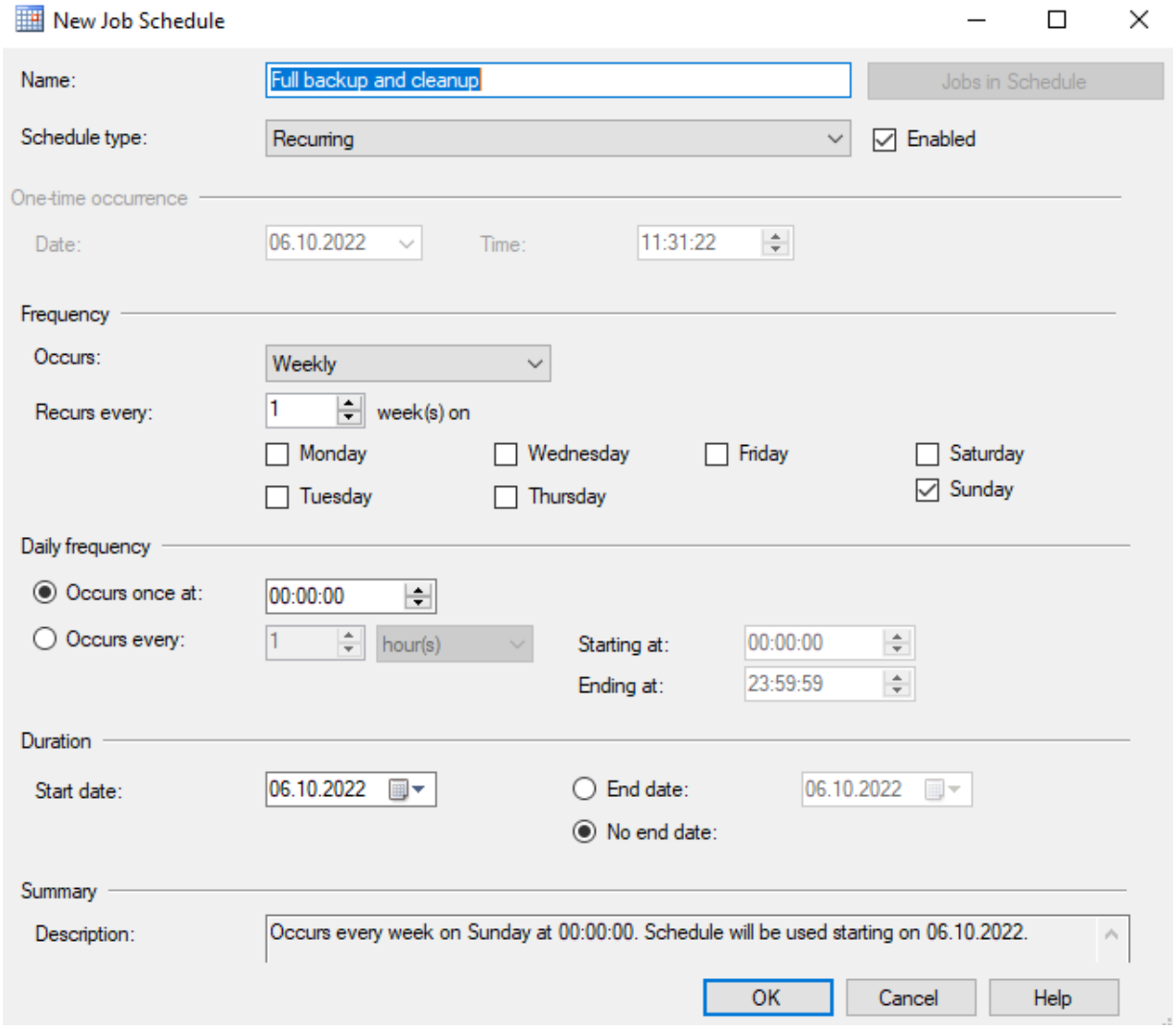
   Description: You can enter a description of the plan in the *Description* field.

   Run as: SQL Server Agent service account

   The basic settings of the maintenance plan are now complete. Now you need to define a schedule.

Schedule

1. Enable the *Single schedule for the entire plan or no schedule* option.
2. Under *Schedule*, select *Change*.



The *New Job Schedule* dialog box opens.

3. Edit the schedule according to the project requirements. The following settings are used in this example:

   Occurs: Daily

   Occurs once at: 02:00:00

   > **Information**
   >
   > Select a time when users are not expected to be using the server. Though users can continue to access ELO and the database while the backup is running, there will be an impact on performance.

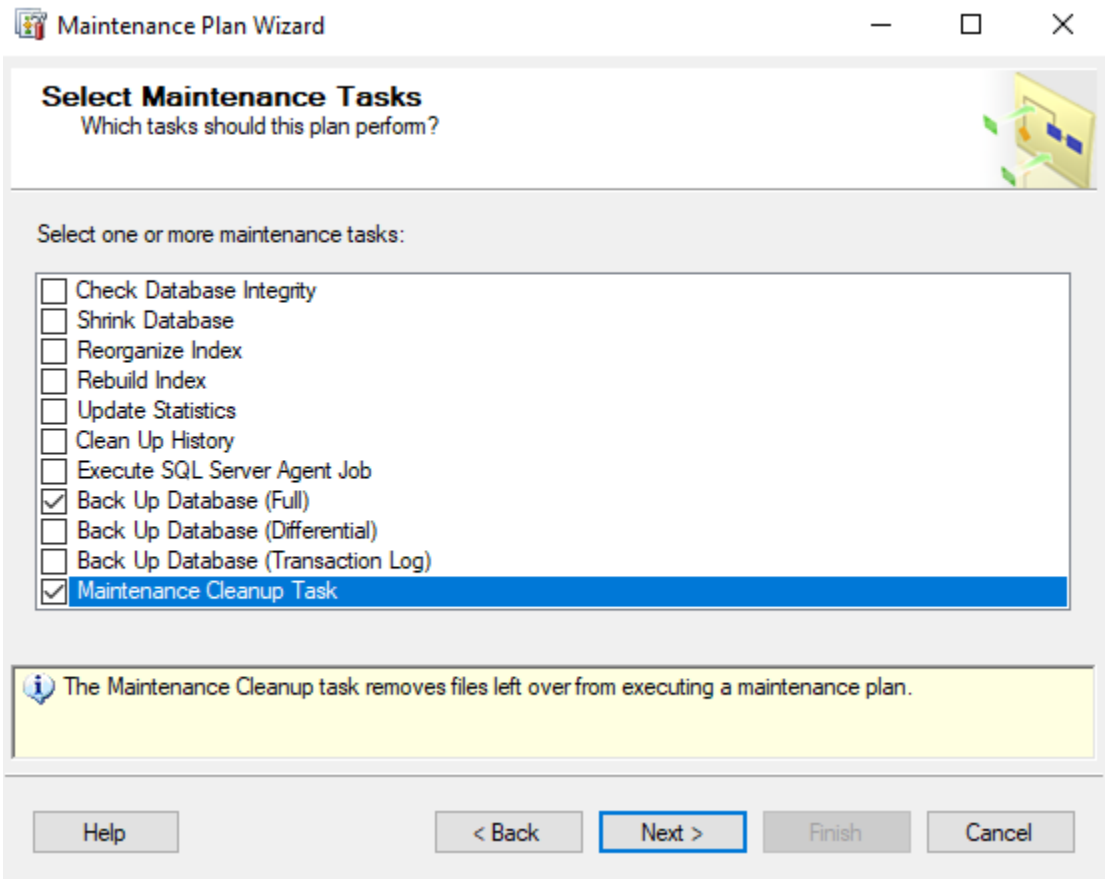
   For all other settings, we have used the default program settings.

4. Select *OK*.

The *New Job Schedule* dialog box closes.

5. In the *Maintenance Plan Wizard* dialog box, select *Next*.

Select tasks

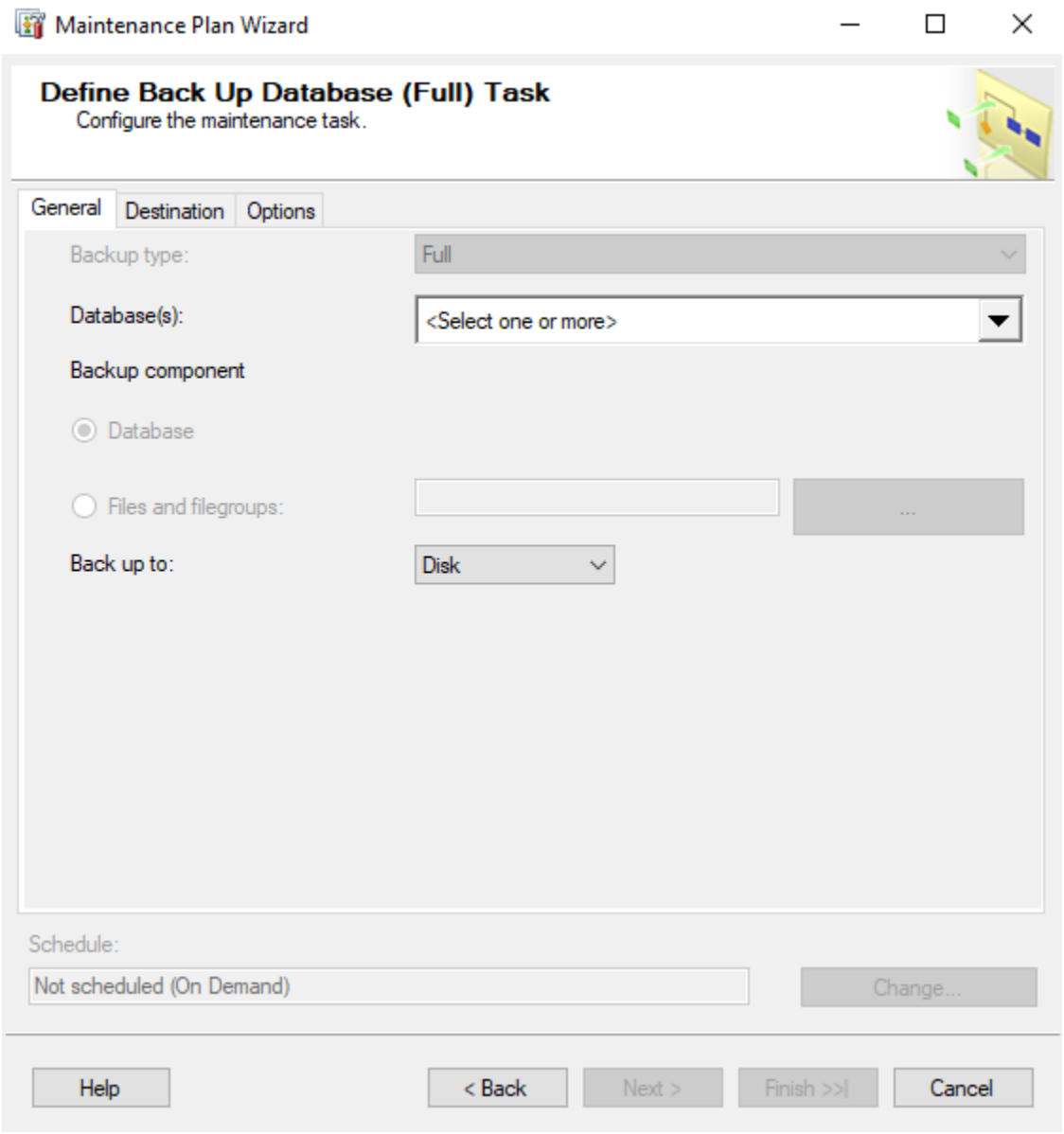


The *Select Maintenance Tasks* screen opens.

1. Enable the check boxes of the following tasks:
   - Back Up Database (Full)
   - Maintenance Cleanup Task
2. Select *Next*.

   The *Select Maintenance Task Order* screen opens.
3. Check the order and correct if necessary.
4. Select *Next*.

Backup task



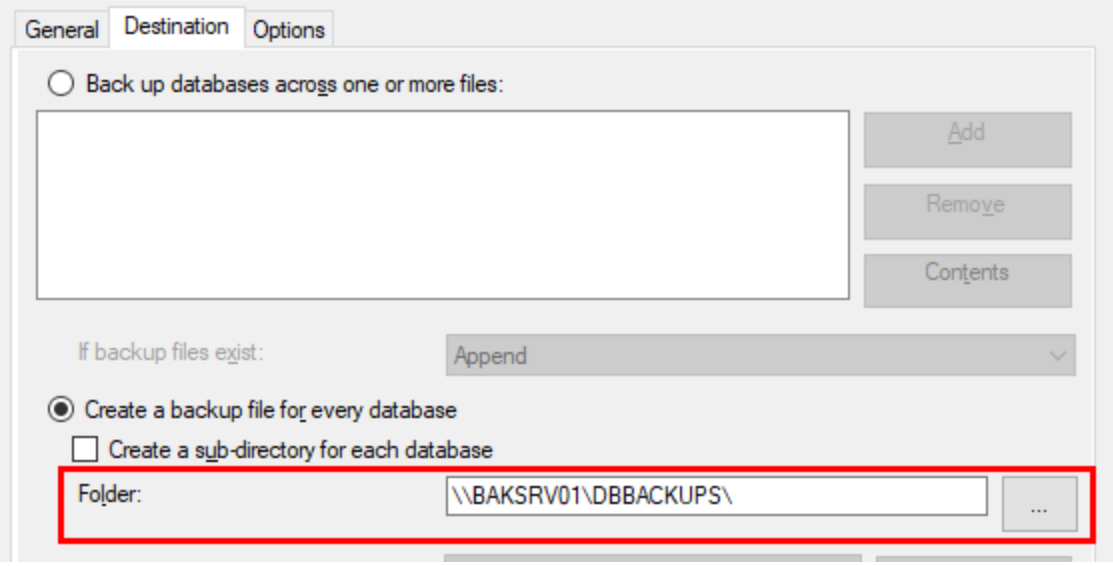
The *Define Back Up Database (Full) Task* screen opens. The *General* tab is open.

1. In the *Database(s)* drop-down menu, select the *All databases* option.

   > **Information**
   >
   > To reduce the amount of work involved, it is recommended to select *All databases* for backup. This also ensures that new databases and ELO repositories will be backed up automatically, even if they did not exist at the time you created the task.

2. In the *Back up to* drop-down menu, select the *Disk* menu item.

3. Switch to the *Destination* tab.



4. In the *Folder* field, specify where you want the backups to be stored. You can also enter UNC network paths here.

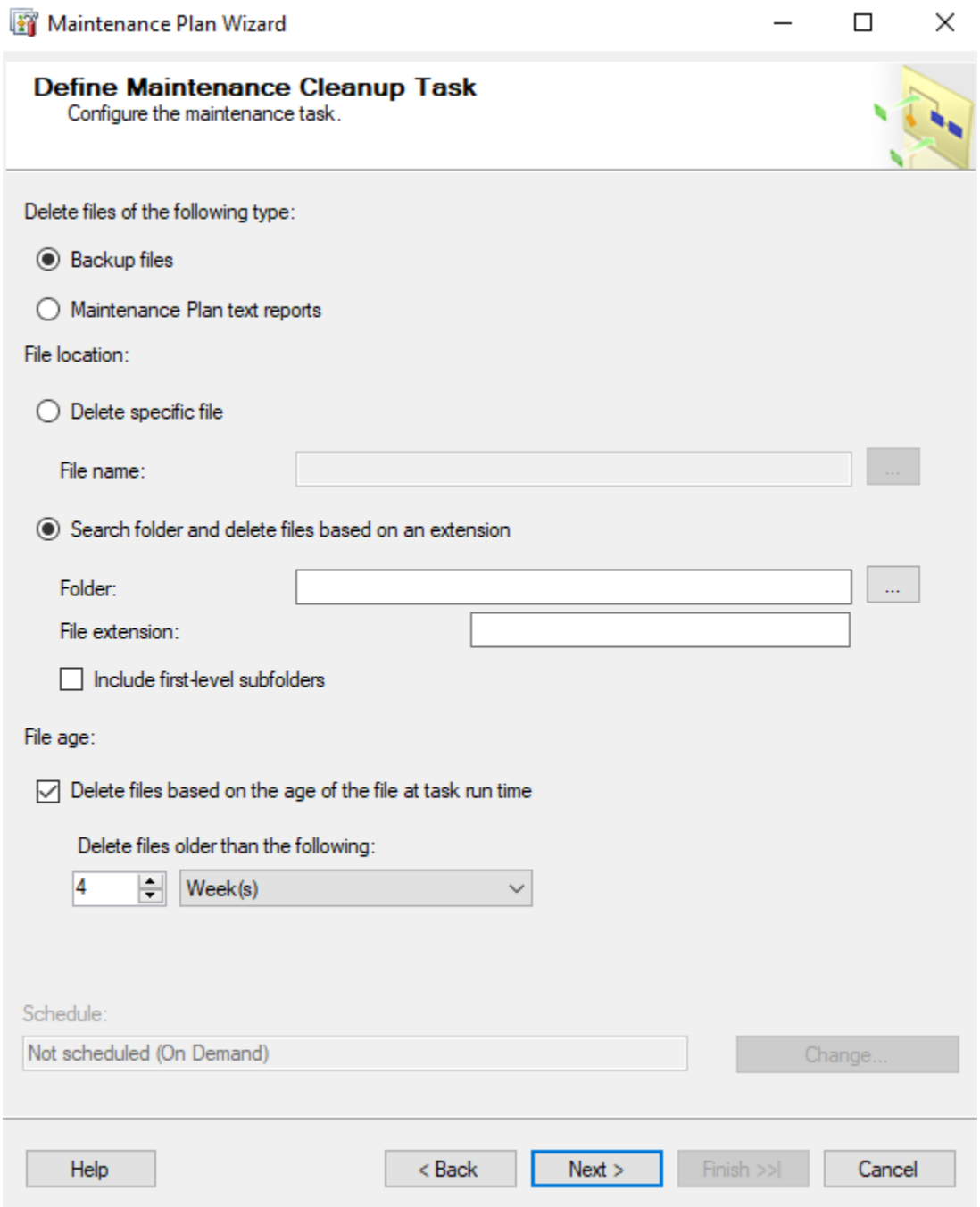
> **Important**
>
> Do not store backup files on the same computer or physical drive as the SQL Server. Saving database backups on the same computer as the database server only provides minimal protection against failures.

> **Please note**
>
> Make sure that the *SQL Server Agent* account has sufficient permissions to create and delete files on the selected path.

For all other settings, we have used the default program settings.

5. Select *Next*.

Cleanup task



The *Define Maintenance Cleanup Task* screen opens.

1. The following settings are used in this example:

   Delete files of the following type: Backup files

   File location: Not enabled

   Search folder and delete files based on extension: Enabled

Folder: Path to the backup files as specified for the *Back Up Database (Full)* task.

File extension: File extension of the backup files. In this case, the file extension *bak* was defined for *Back Up Database (Full)*.

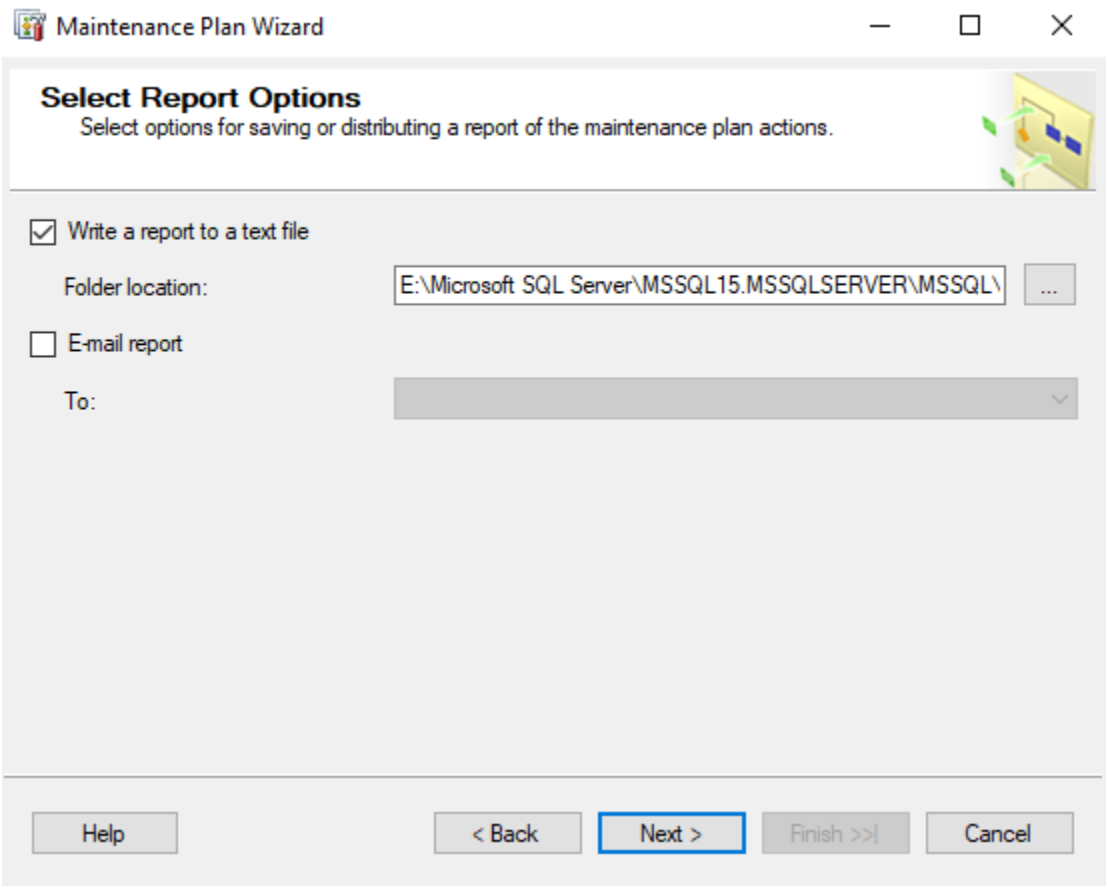
Include first-level subfolders: Enabled

Delete files based on the age of the file at task run time: Enabled

Delete files older than the following: 4 days

2. Select *Next*.

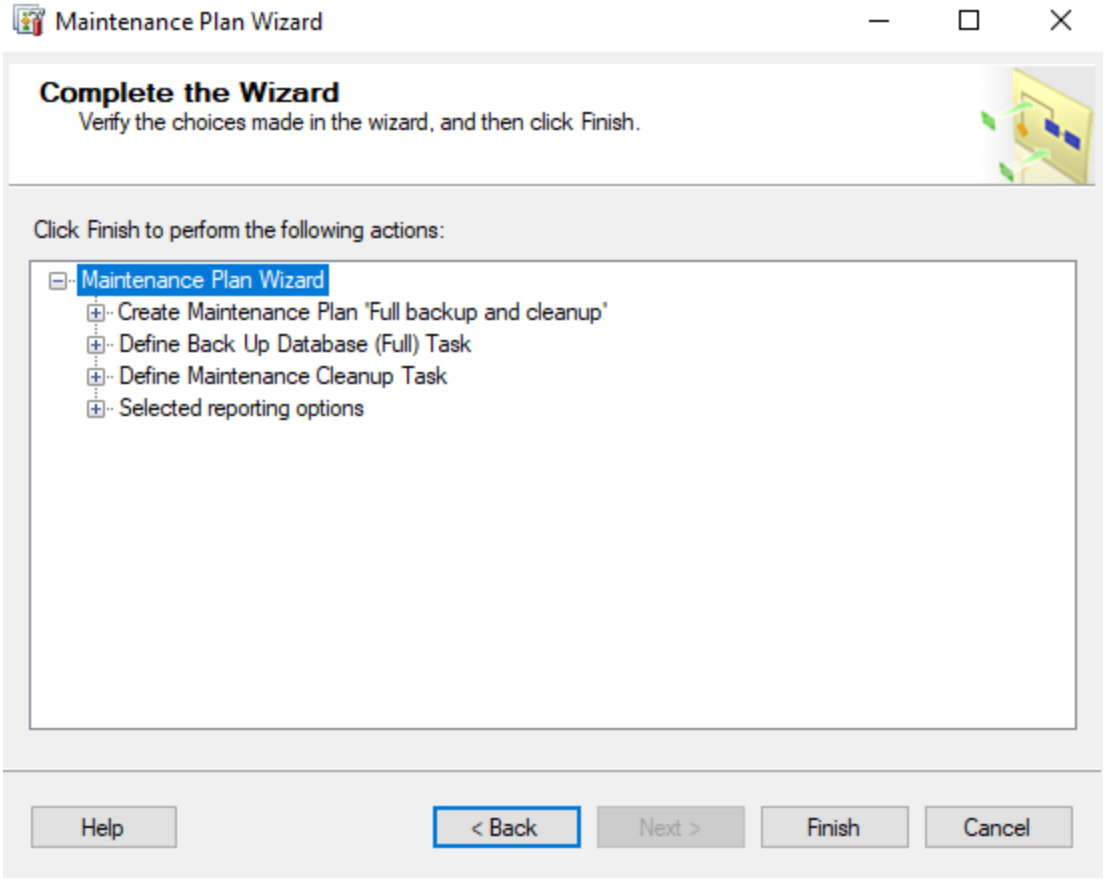
Final steps



The *Select Report Options* screen opens.

Optional: Change the report settings if you need to.

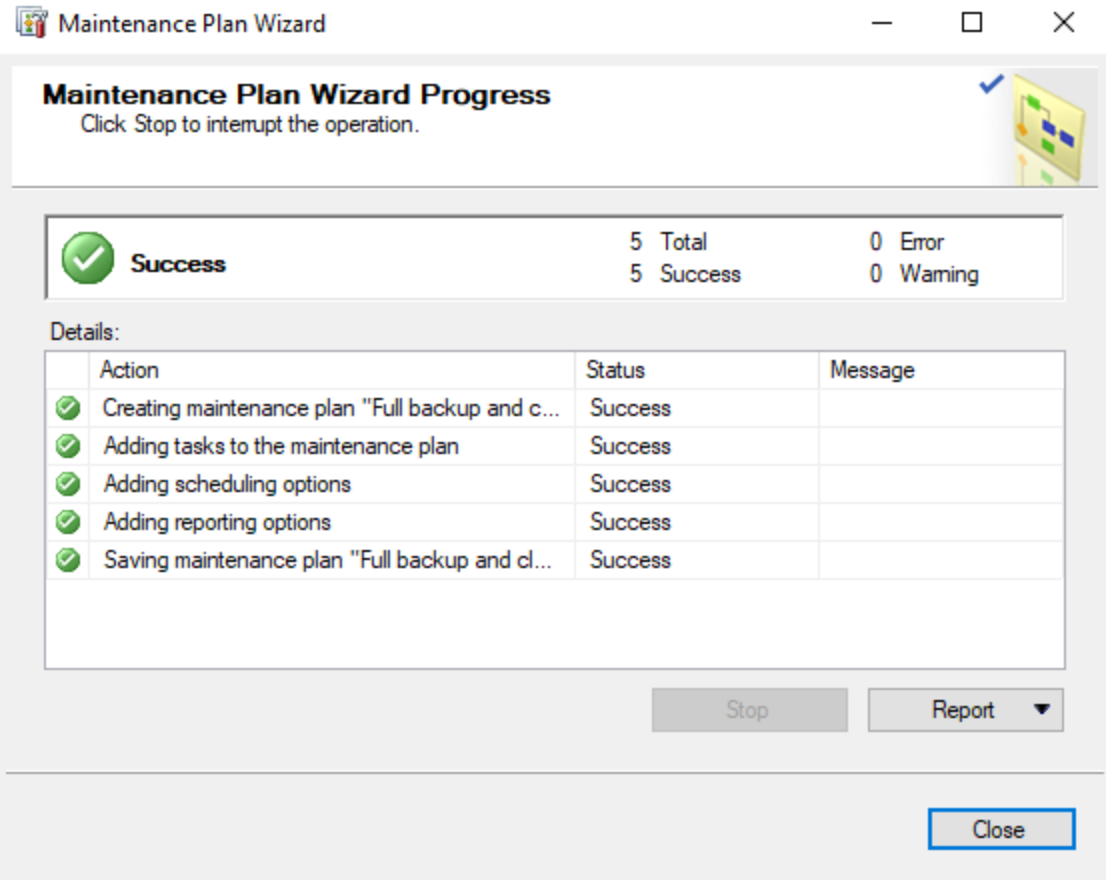
1. Select *Next*.



The *Complete the Wizard* screen opens. You will see an overview of the plan you created.

2. Check the settings.

3. Select *Finish*.



The *Maintenance Plan Wizard Progress* screen opens. The plan is successfully completed.

4. Once the wizard is finished, select *Close*.

   This closes the dialog box.

> **Please note**
>
> It is recommended to additionally copy periodic backups to a long-term storage medium (e. g. tape backup) in somewhat longer intervals. This can be performed by the Windows Scheduler, the SQL Server Agent, or another backup solution.

Transaction log backup

Now create a backup plan for the transaction logs. You can edit an existing plan or create a new one. This document describes how to create a separate plan.

Information

Transaction logs contain a journaled sequential record of all operations in the database which can be used to fill in the gaps between full backups. It is important to note that these logs are crucial to restoring the database in case of failure, in contrast to other types of logs used to solve errors, analyze performance, etc.

1. Create a new maintenance plan as described above under Basic settings.
2. Enable the *Single schedule for the entire plan or no schedule* option.
3. Under *Schedule*, select *Change*.

   The *New Job Schedule* dialog box opens.
4. Edit the schedule according to the project requirements. The following settings are used in this example:

   Occurs: Daily

   Occurs every: 30 minutes(s)

   Information

   Change the schedule so that the backup runs every 15-30 minutes (depending on your requirements).

   For all other settings, we have used the default program settings.
5. Select *OK*.

   The *New Job Schedule* dialog box closes.
6. Select *Next*.

   The *Select Maintenance Tasks* screen opens.
7. Enable the check boxes of the following tasks:
   - Back Up Database (Transaction Log)
   - Maintenance Cleanup Task
8. Select *Next*.

   The *Select Maintenance Task Order* screen opens.
9. Select *Next*.

   The *Define Back Up Database (Transaction Log) Task* screen opens. The *General* tab is open.
10. In the *Database(s)* drop-down menu, select the *All databases* option.
11.

In the *Back up to* drop-down menu, select the *Disk* menu item.

12. Switch to the *Destination* tab.
13. In the *Folder* field, specify where you want the backups to be stored. You can also enter UNC network paths here.

    Important

    Do not store backup files on the same computer or physical drive as the SQL Server. Saving database backups on the same computer as the database server only provides minimal protection against failures.

    Please note

    Make sure that the SQL Server Agent account has sufficient permissions to create and delete files on the selected path.

    For all other settings, we have used the default program settings.

14. Select *Next*.

    The *Define Maintenance Cleanup Task* screen opens.

15. Define the cleanup tasks as described above under Cleanup task.

    Please note

    With a transaction log cleanup task, you normally need to specify the *trn* file extension. Change the file extension accordingly if you have used a different file extension.

16. Follow the steps described above under Final steps.

    The maintenance plan is successfully completed.

Database optimization

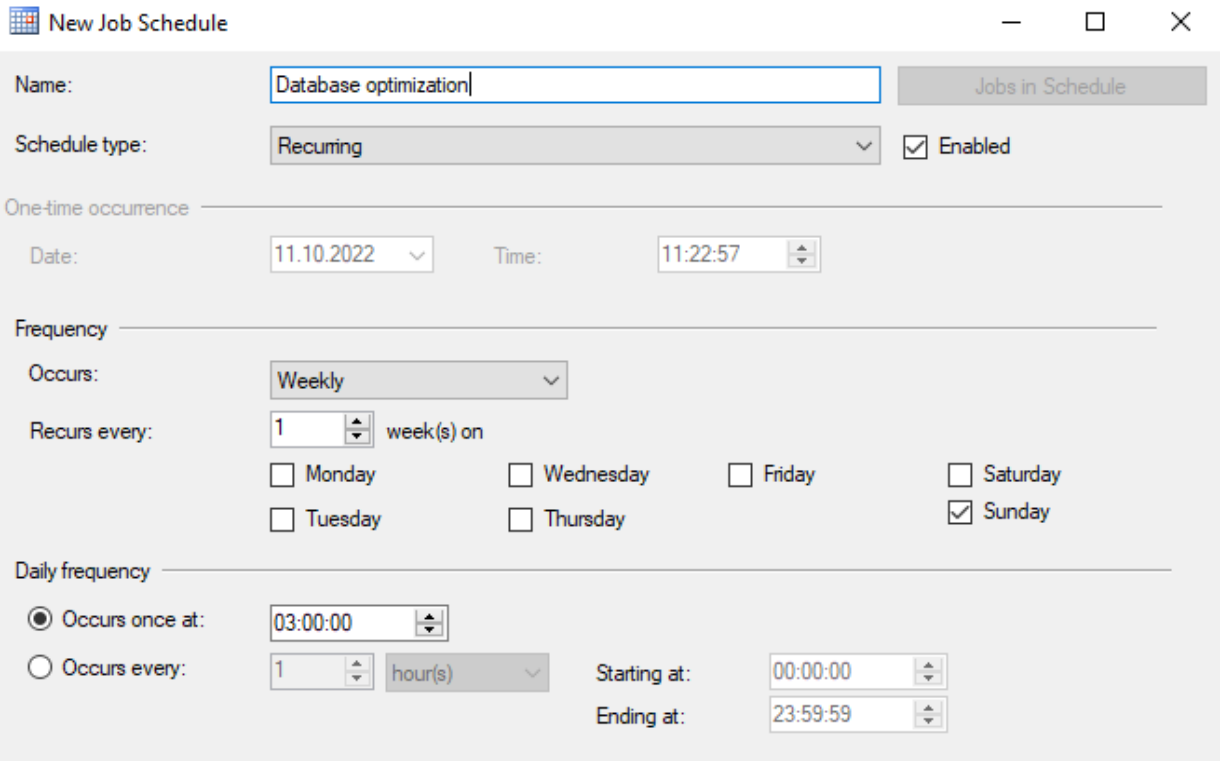
In addition to database backups, the database should be regularly optimized and checked to ensure that it functions properly. The following section describes how to set up this task.

1. Create a new maintenance plan as described above under Basic settings.
2. Enable the *Single schedule for the entire plan or no schedule* option.
3. Under *Schedule*, select *Change*.

   The *New Job Schedule* dialog box opens.

4.

Edit the schedule according to the project requirements. The following settings are used in this example:



Occurs: Weekly

Occurs once at: 03:00:00

> **Information**
>
> This plan will have a significant impact on database performance, and depending on the options you select, may mean that the database will be unavailable for some time. Set the the task to run once a week and select the time when database utilization is lowest.

For all other settings, we have used the default program settings.

5. Select *OK*.

   The *New Job Schedule* dialog box closes.

6. Select *Next*.

   The *Select Maintenance Tasks* screen opens.

7. Enable the check boxes of the following tasks:

   - Check Database Integrity Task
   - Rebuild Index Task
   -

History Cleanup Task

Please note

The ELO server cannot access the database while the *Rebuild Index Task* is running. ELO is not available at all during this maintenance task. However, it is important to maintain the database indexes regularly to ensure long-term performance.

However, this task can also result in timeouts on the ELO server and other errors. If this occurs, stop the ELO Application Server (Apache Tomcat) service while this maintenance task is running. It is possible that ELO needs to be available during maintenance time. The *Sort results in tempdb* and *Keep index online* options in SQL Server Enterprise Edition allow the server to continue running. However, please note that this process still has a significant impact on database performance.

Another alternative to the *Rebuild Index Task* is to use the *Reorganize Index Task* followed by an *Update Statistics Task*. Although this does not increase performance to the same extent as rebuilding the index, it does allow you to extend the time between complete rebuilds of the index.

1. Select *Next*.

   The *Select Maintenance Task Order* screen opens.

2. Check the order and correct if necessary.

3. Select *Next*.

Check Database Integrity Task

The *Define Database Check Integrity Task* screen opens.

Information

The *Check Database Integrity* task checks the health of the database pages by comparing the written blocks on the hard drive to the database tables. If an error is detected, it will be logged by this task.

1. In the *Databases* drop-down menu, select the *All databases* menu item.

2. Select *Next*.

Rebuild Index Task

The *Define Rebuild Index Task* screen opens.

Information

This task creates indexes along with the ELO databases in order to optimize search times in the database. Note that many different searches are performed on the SQL Server, and not just those performed by the user.

This task deletes the existing indexes and then recreates them. This essentially reduces fragmentation and disk I/O operations, optimizing search times afterwards. In addition, the *Rebuild Index Task* generates database statistics for later performance analysis.

It is recommended to perform the *Rebuild Index Task* at least once a week. If database performance decreases rapidly as the week commences, consider performing the task more often.

1. In the *Databases* drop-down menu, select the *All user databases* menu item.
2. Select the option *Default free space per page*.

   Optional: If you need to run the task during normal server operations, enable the options *Sort results in tempdb* and *Keep index online*.

   Information

   These options are only available for Microsoft SQL Enterprise.

3. Under *Scan type*, select the *Detailed* option.

   Please note

   The *Detailed* method takes more time than the other methods.

   For all other settings, use the default program settings.

4. Select *Next*.

History Cleanup Task

The *Define History Cleanup Task* screen opens.

Information

The *History Cleanup Task* deletes historical data after a defined time period. If you do not delete this data, the maintenance plan histories may take a very long time to load.

With the default settings, the *History Cleanup Task* deletes data that is older than four weeks. This applies to the backup and restore history, the SQL Server Agent job history, and the maintenance plan history.

1. Edit the settings if required.

You do not need to change the default settings in most cases.

2. Select *Next*.
3. Follow the steps described above under Final steps.

   The maintenance plan is successfully completed.

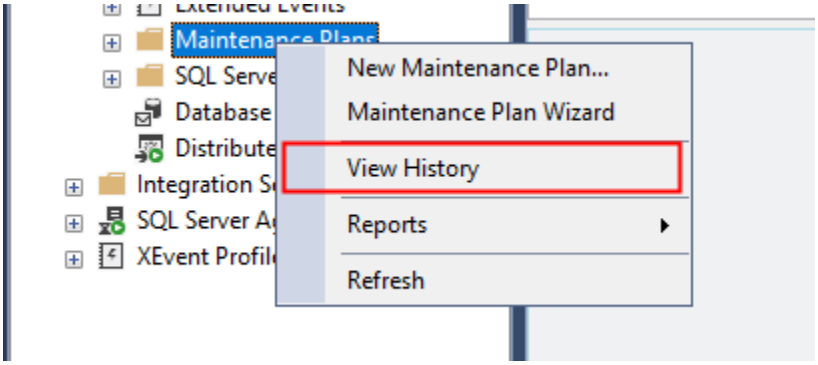
Optional: Reorganize Index Task

The *Reorganize Index Task* is another way to optimize the database. It is recommended to run this task every night or, e. g. every few nights. It is also useful to run the *Update Statistics Task* within the same maintenance plan following this.

A good way to check whether you need to reorganize the index on a frequent basis is to check the database statistics regularly. If the database is highly fragmented (e.g. over 30%) after you run the *Rebuild Index Task*, the *Reorganize Index Task* can significantly improve performance.

Please note that reorganizing the indexes has a noticeable impact on database performance and may take longer to complete than if you rebuild the index.

Maintenance plan reports



To view the history of a maintenance plan, follow these steps:

1. In the Object Explorer, navigate to the *Maintenance Plans* folder.
2. Open the context menu.
3. Select *View History* from the context menu.

General logs

You can view logs for SQL Server processes in the Object Explorer.

1. Navigate to *SQL Server Agent > Error Logs*.
2. Open the *Error Logs* folder.
3. Select one of the log files.
4.

Open the context menu.

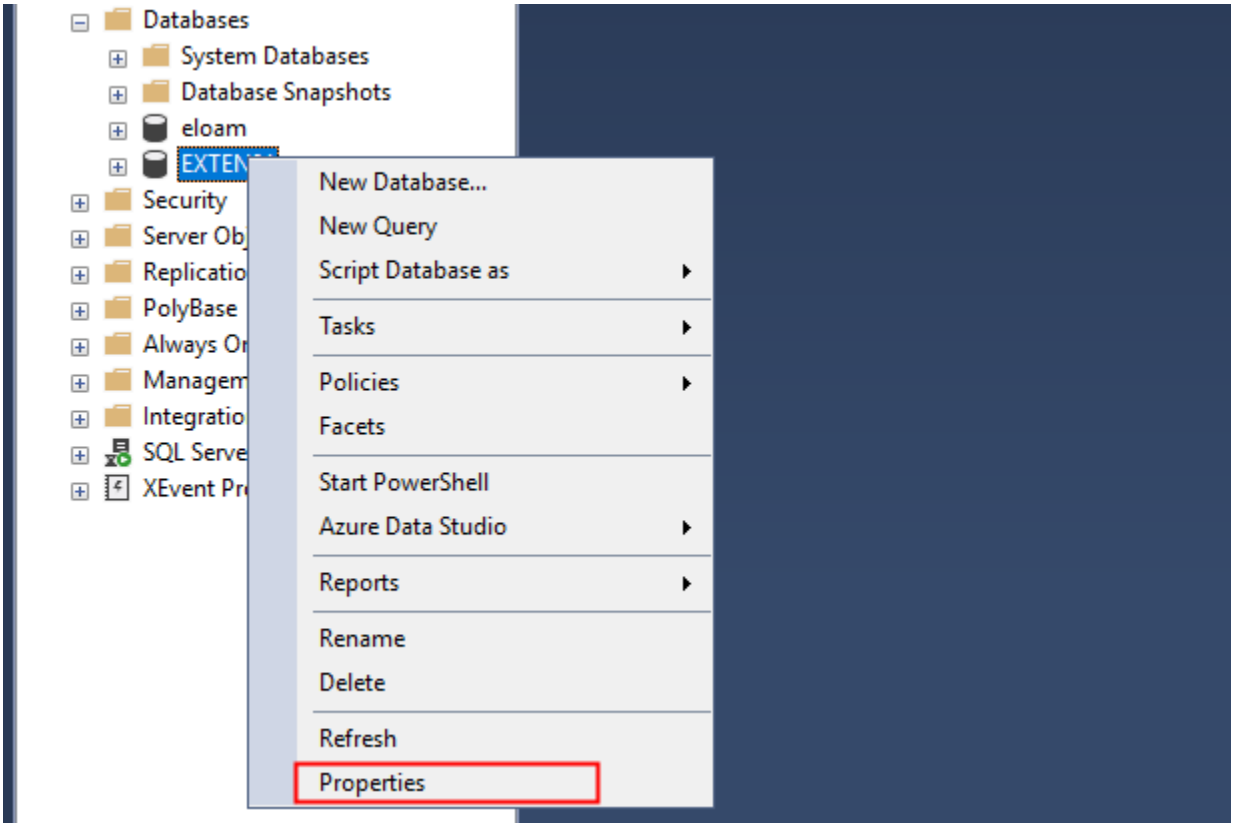
5. Select the *View Agent log* menu item.

The *Log File Viewer* dialog box opens.

The log files store information, errors, and warnings. The logs are also saved as text files in the SQL Server installation directory.

Troubleshooting: Creating maintenance plans later

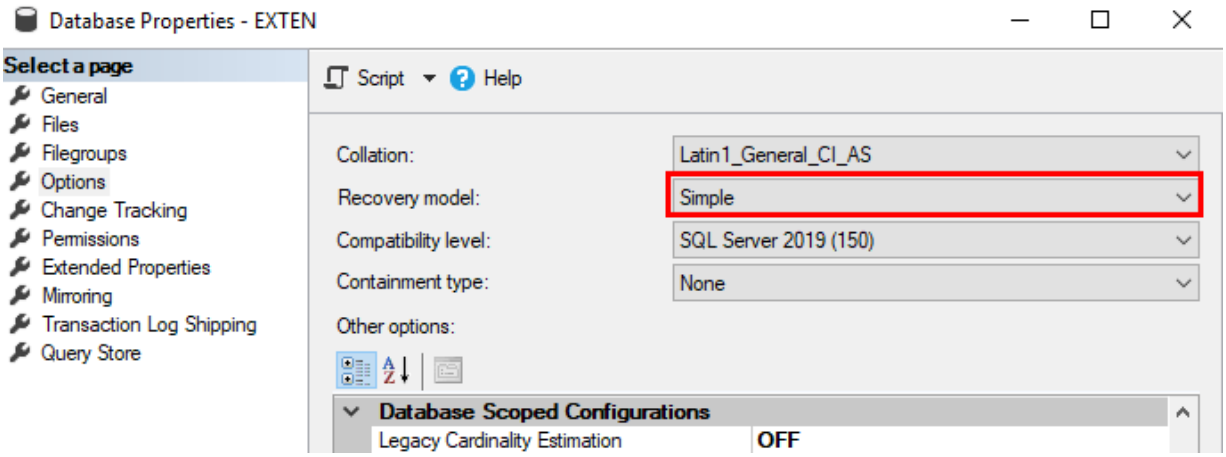
If you did not set up maintenance plans when you first installed Microsoft SQL Server and the ELO server, you can create them later. However, the standard method described above will take a long time to complete unless you shrink the transaction log first. The following sections explain how to do this.



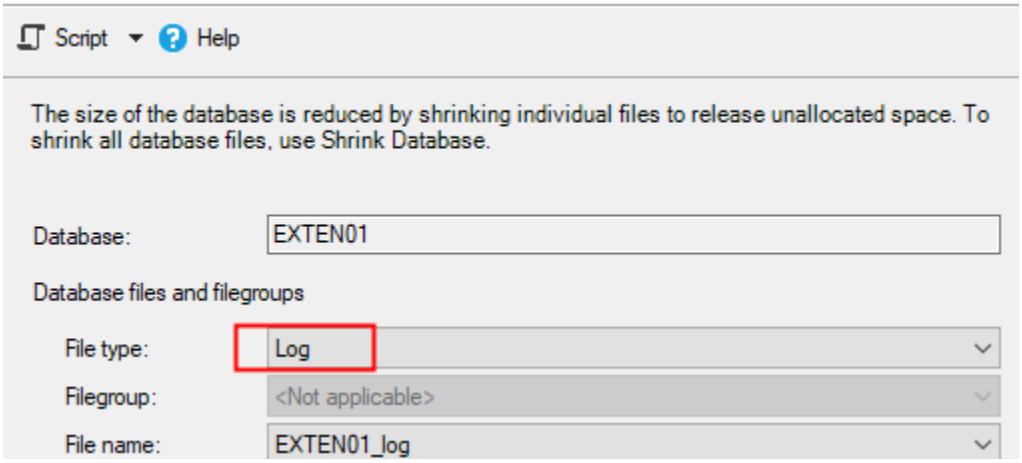
1. Before setting up the maintenance plans, navigate to the *Databases* folder.

2. Open the context menu of the required database.

3. In the context menu, select the *Properties* menu item.



4. Navigate to the *Options* screen.
5. Select *Simple* for the *Recovery model*.
6. Click *OK* to close the dialog box.
7. Open the context menu of the selected database.
8. In the context menu, select *Tasks* > *Shrink* > *File*.

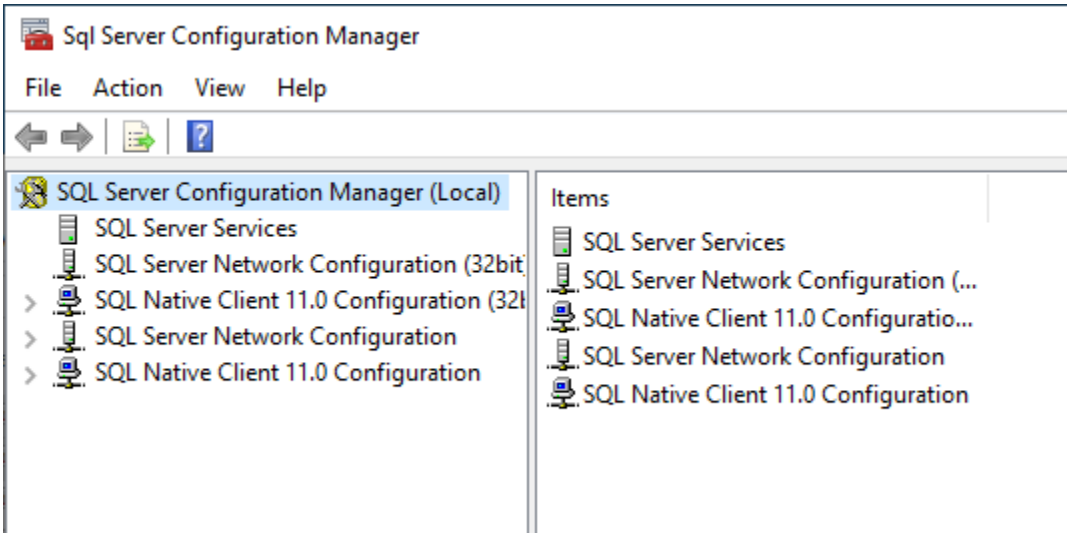


   The *Shrink File* dialog box opens.

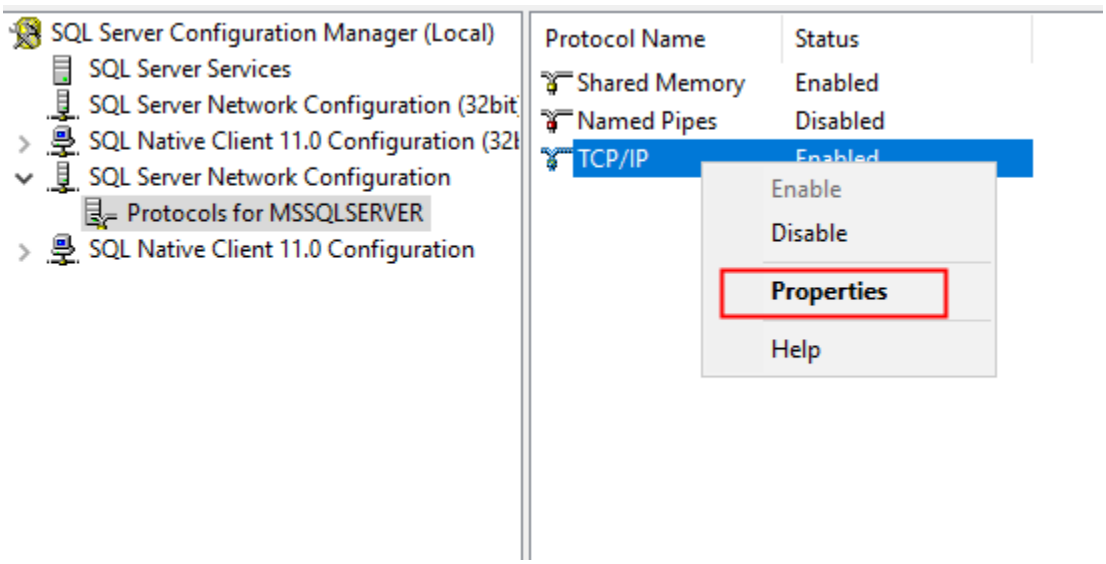
9. In the *File type* drop-down menu, change the file type to *Log*.
10. Select *OK* to shrink the files.
11. Repeat this for all ELO databases.
12. Change the recovery model back to *Full*.
13. Now create database backup and maintenance tasks as described above.

Instances

In some cases, you may need ELO to connect to a non-standard instance of Microsoft SQL Server. As it is only possible to configure the computer name and port in the ELO server configuration, you need to configure some SQL Server instances to listen to specific ports.

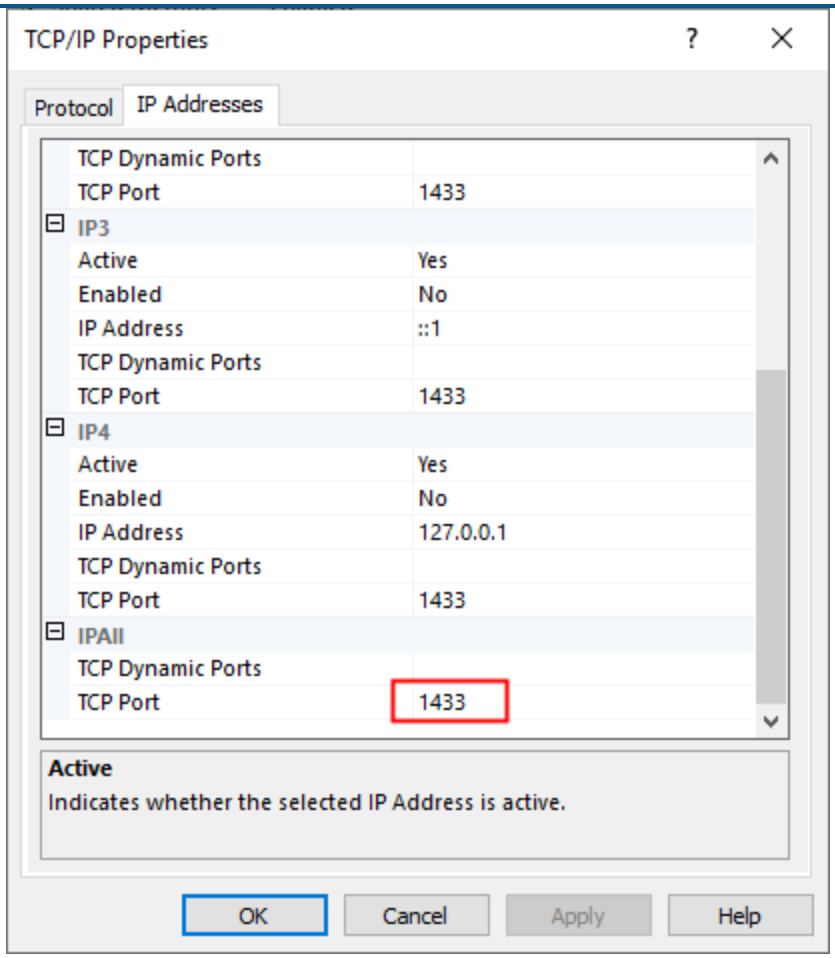


1. Open SQL Server Configuration Manager.
2. Navigate to *SQL Server Network Configuration*.
3. Select *Protocols for <Instance name>*.



4. Open the context menu of the *TCP/IP* entry.
5. In the context menu, select *Properties*.

   The *TCP/IP Properties* dialog box opens.



6. Switch to the *IP Addresses* tab.
7. Under *IPAll*, enter the desired port in the TCP Port field.
8. Select *OK* to save the configuration.
9. Close the SQL Server Configuration Manager.
10. Restart the Microsoft SQL Server Service to apply the change.

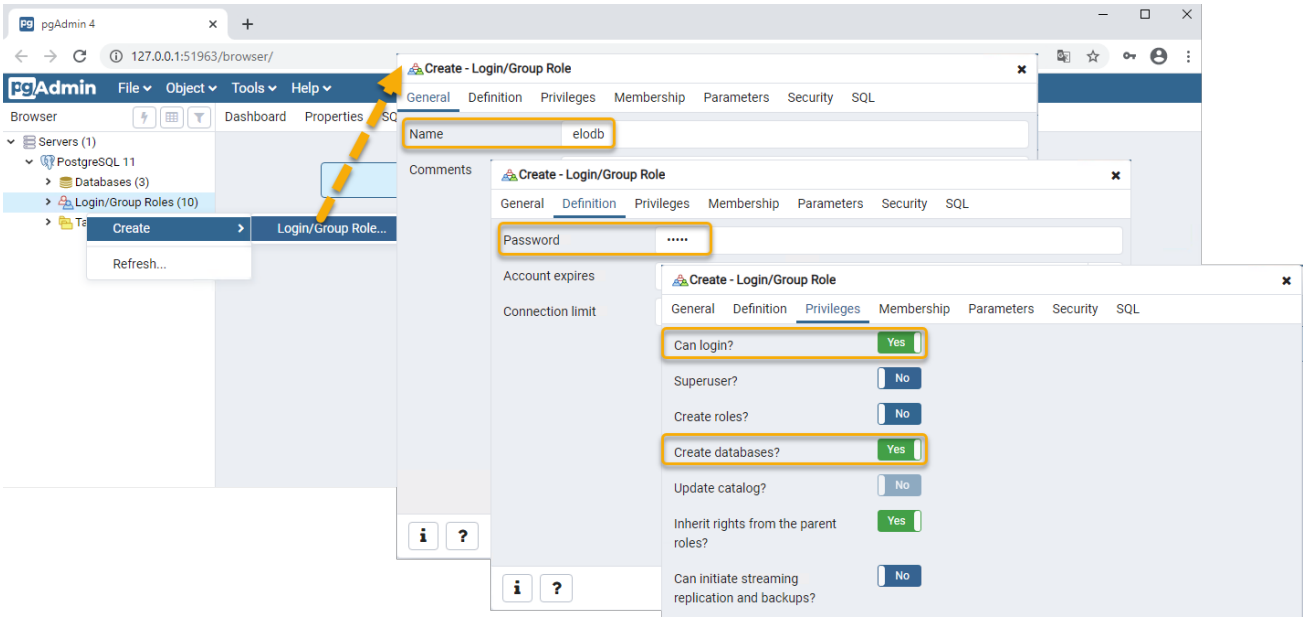
Enter this port during installation of the ELO server to connect directly to this SQL Server instance.

PostgreSQL Server

A PostgreSQL server can be used as an alternative to Microsoft SQL Server. A full description of the installation is not provided in this documentation.

Creating a logon for the PostgreSQL Server

To use SQL authentication, we have to set up a logon for the ELO installation. The account name and password combinations are managed within SQL Server.



Set up the login in the PostgreSQL Server as follows:

> **Please note**
>
> *UTF-8* encoding must be selected for PostgreSQL databases.

1. Start SQL Management Studio *pgAdmin 4* and connect to the PostgreSQL 9.5 (localhost:5432) database server.
2. Open the content menu of the *Login/Group Roles* folder.
3. Select *Create*.
4. Select *Login/Group Role*.

   The *Create* dialog box opens.
5. On the *General* tab, enter the logon name *elodb* in the corresponding field in the *Name* dialog box.
6. On the *Definition* tab, enter the password for the *elodb* account in the corresponding field.
7.

Switch to the *Privileges* tab.

This tab lists all possible roles that can be assigned to the new login.

8. Assign the necessary roles to the account.

   Installing ELO requires the following server roles:

   - Can login?
   - Create databases?

9. Select *OK*.

Oracle SQL Server

Requirements

A fully installed version of Oracle SQL Server version 11g or 12c is required for a successful ELO installation. A new option for Oracle Database 12c allows a container database to hold multiple pluggable databases. This new architecture means that you have to pay attention to specific things before and during the installation. These variations are shown in information boxes.

- Database character set: The Unicode character set *AL32UTF8* is recommended. For compatibility reasons, the 8-bit Microsoft Windows character sets are still supported (for Western Europe, this is *WE8MSWIN1252*).
- National character set (for nvarchar2 columns): the default character set (*AL16UTF16*) must be used.

Unicode (*nvarchar2*) columns are standard in ELO version 9. The content of the database definition file *elodb8uni.txt* is used by the ELO Server Setup for new installations. If an older ELO version without Unicode columns is updated, it is recommended to convert the columns into Unicode before any ELO 9 applications are started. An ELO tool and a guide are available for converting the columns.

If the ELO server applications are already installed and the database character set is converted to *AL32UTF8*, the Unicode column must be converted first (nvarchar2 columns must exist). An ELO tool and a guide are available for converting the columns.

The character set *WE8ISO8859P1* and the Microsoft driver for Oracle were recommended for Oracle 8i (this version is no longer supported by ELO).

The two character sets of the database can be displayed with this SQL command:

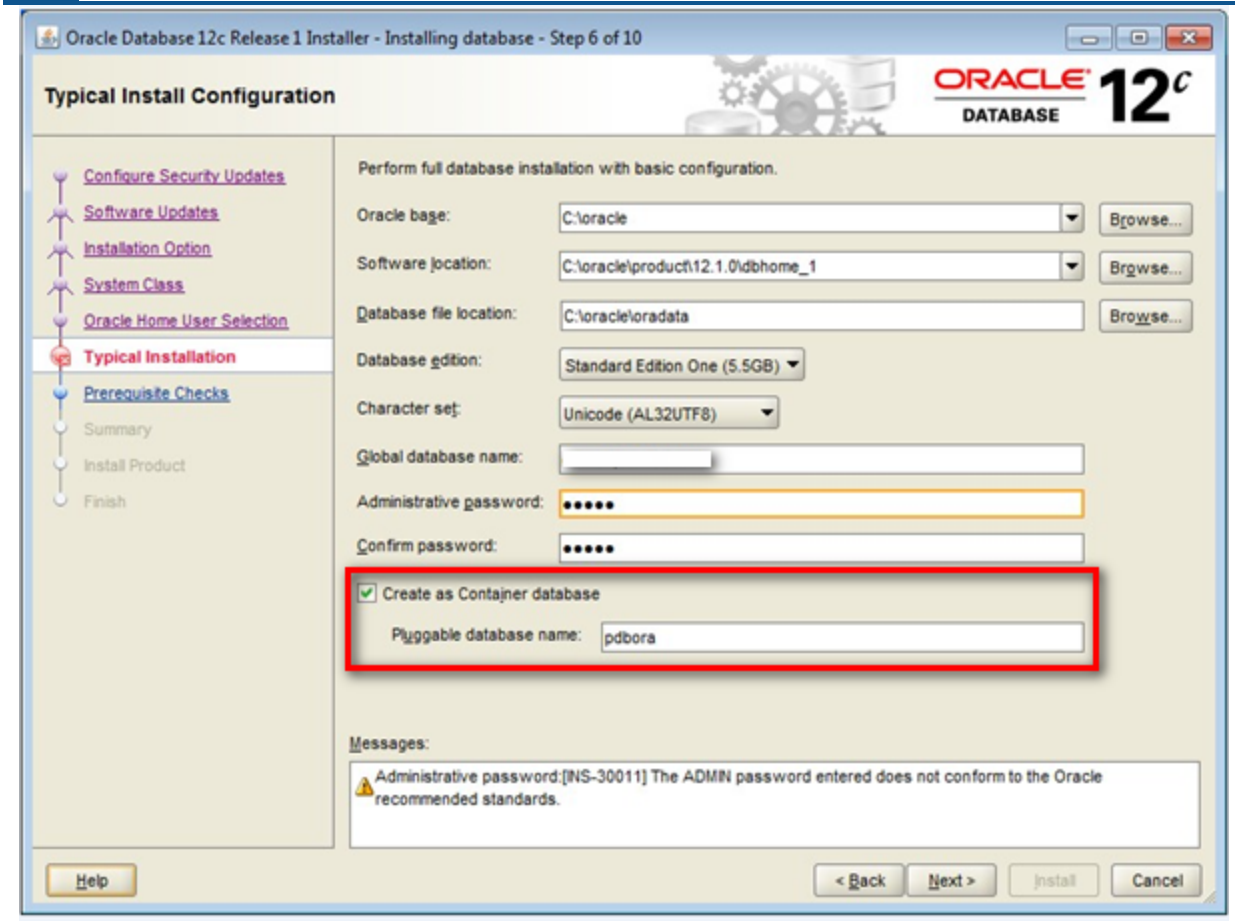
```
SELECT * FROM NLS_DATABASE_PARAMETERS.
```

More information about character sets can be found in the Oracle Database Globalization Support Guide.

Oracle 12c

The option to “Create as Container database” must be set during the database installation.

> **Information**
>
> The following sections refer to an installation with Oracle 12c Release 1.

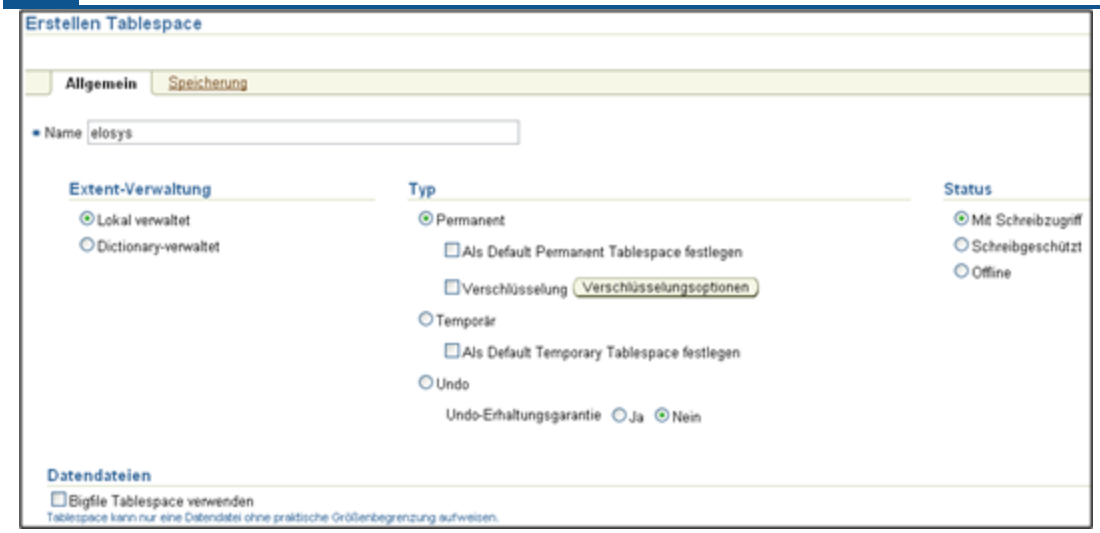


The pluggable database is named *pdbora* in the example here. In the following, the container database is named *ora12c*.

This option must be selected due to the naming convention for common users in Oracle 12c: The name must begin with C## or c##, which causes some problems for servlets. For this reason, ELO must be installed with a local account in a pluggable database (PDB).

Tablespace configuration

When creating a new repository, the ELO Server Setup program requires the correct tablespace. Either the storage area for the tables or for the indices is required. Normally, the two tablespaces should have the names ELOSYS and ELOLOG, although you may use other names if necessary. Existing tablespaces can also be used or shared, although this is not recommended because it makes database administration more difficult. This means that data from different applications would also be integrated.



You can configure the tablespaces in Oracle Enterprise Manager, for example.

Note that when configuring the repository, several tables with initial sizes of between 1 and 10 MB are created. An empty test repository requires approximately 100 MB disk space. This should be taken into consideration when creating the tablespaces.

As a rule, when a number of smaller repositories are created, ELOSYS should have a minimum capacity of 4 GB and ELOLOG a minimum of 2 GB.

If the option to automatically increase the memory capacity is not enabled, the system administrator should regularly check the available memory capacity. If the tablespace is full, ELO cannot perform filing actions or add entries to the report.

In Oracle 12c, the tablespaces can easily be created with “sqlplus.exe”:

```
Enter user name: sys as sysdba


Enter password:

SQL> alter pluggable database all open;
Pluggable database altered.

SQL> alter session set container = pdbora;
Session altered.

SQL> CREATE TABLESPACE elosys DATAFILE
'C:\oracle\oradata\ora12c\pdbora\ELOSYS.dbf' SIZE 2000M
Default Storage (Initial 120K Next 120k minextents 2
maxextents 10000 pctincrease 0) ;
Tablespace created.

SQL> CREATE TABLESPACE elolog DATAFILE
```

```
'C:\oracle\oradata\ora12c\pdbora\ELOLOG.dbf' SIZE 2000M Default Storage
(Initial 120K Next 120k minextents 2 maxextents 10000 pctincrease 0) ;
Tablespace created.
```

Create ELO accounts

Creating an account with Oracle Enterprise Manager

An ELO account must be created for all ELO clients. This can be done with the Oracle Enterprise Manager. The usual name for this account is *elodb*. This account provides access for all ELO clients, although the password is encoded with a 128-bit key and is not known by the normal ELO account.

ELOSYS is recommended as the tablespace for the account.

Rights for account "elodb"

The following rights are required for the *elodb* account:

- ALTER ANY SEQUENCE
- ALTER ANY TABLE
- ALTER ANY TRIGGER
- ALTER USER
- CREATE ANY INDEX
- CREATE ANY PROCEDURE
- CREATE ANY SEQUENCE
- CREATE ANY TABLE
- CREATE ANY TRIGGER
- CREATE ANY VIEW
- CREATE USER
- CREATE ROLE
-

CREATE SESSION
- DELETE ANY TABLE
- EXECUTE ANY PROCEDURE
- GRANT ANY PRIVILEGE
- INSERT ANY TABLE
- SELECT ANY SEQUENCE
- SELECT ANY TABLE
- UPDATE ANY TABLE

ELO Server Setup

The ELO Server Setup program requires an existing account with the role DBA. This can be either the *elodb* account, which must be temporarily assigned the additional role, or better another Oracle account that has been assigned this role (e.g. *elodbadmin*).

Due to security considerations, the *elodb* account must not be assigned the role of DBA when it is used as a part of the operating system.

The ELO Server Setup program creates the following Oracle accounts:

- One for each ELO Access Manager
- One for each repository

The account names correspond to the names of the repositories or ELO Access Manager. For example, if you create a repository named *Repo1*, an Oracle account is created with the name *Repo1*. An account for a repository or ELO Access Manager contains all of the tables for a repository or ELO Access Manager. These accounts are used by the corresponding ELO Access Manager and ELO Indexserver.

In Oracle 12c databases, an account with the DBA role can also be created by "sqlplus.exe":

```
Enter user name: sys as sysdba
Enter password:

SQL> alter pluggable database all open;
Pluggable database altered.

SQL> alter session set container = pdbora;
Session altered.

SQL> CREATE USER elodbadmin IDENTIFIED BY <password> DEFAULT TABLESPACE
ELOSYS TEMPORARY TABLESPACE temp;
User created.

SQL> grant dba to elodbadmin;
Grant succeeded.
```

```
SQL> grant create session to elodbadmin;
Grant succeeded.
```

To complete the preliminary work for Oracle 12c, two additional steps have to be performed.

First, the following two files must be updated. Remember that the placeholders in pointy brackets (<) must be replaced with your own values.

tnsnames.ora:

Default content:

```
# tnsnames.ora Network Configuration File:
C:\oracle\product\12.1.0\dbhome_1\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

ORACLR_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
    (CONNECT_DATA =
      (SID = CLRExtProc)
      (PRESENTATION = RO)
    )
)
```

The updated file looks like this:

```
# tnsnames.ora Network Configuration File:
C:\oracle\product\12.1.0\dbhome_1\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.
ORA12C =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = <HOST)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ora12c.<domain)
    )
  )

PDBORA =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = <HOST)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
```

```
      (SERVICE_NAME = pdbora.<domain)
    )
  )
ORACLR_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
    (CONNECT_DATA =
      (SID = CLRExtProc)
      (PRESENTATION = RO)
    )
)
```

listener.ora:

Default content:

```
# listener.ora Network Configuration File:
C:\oracle\product\12.1.0\dbhome_1\network\admin\listener.ora
# Generated by Oracle configuration tools.

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = CLRExtProc)
      (ORACLE_HOME = C:\oracle\product\12.1.0\dbhome_1)
      (PROGRAM = extproc)
      (ENVS =
"EXTPROC_DLLS=ONLY:C:\oracle\product\12.1.0\dbhome_1\bin\oraclr12.dll")
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
      (ADDRESS = (PROTOCOL = TCP) (HOST = <HOST)(PORT = 1521))
    )
  )
```

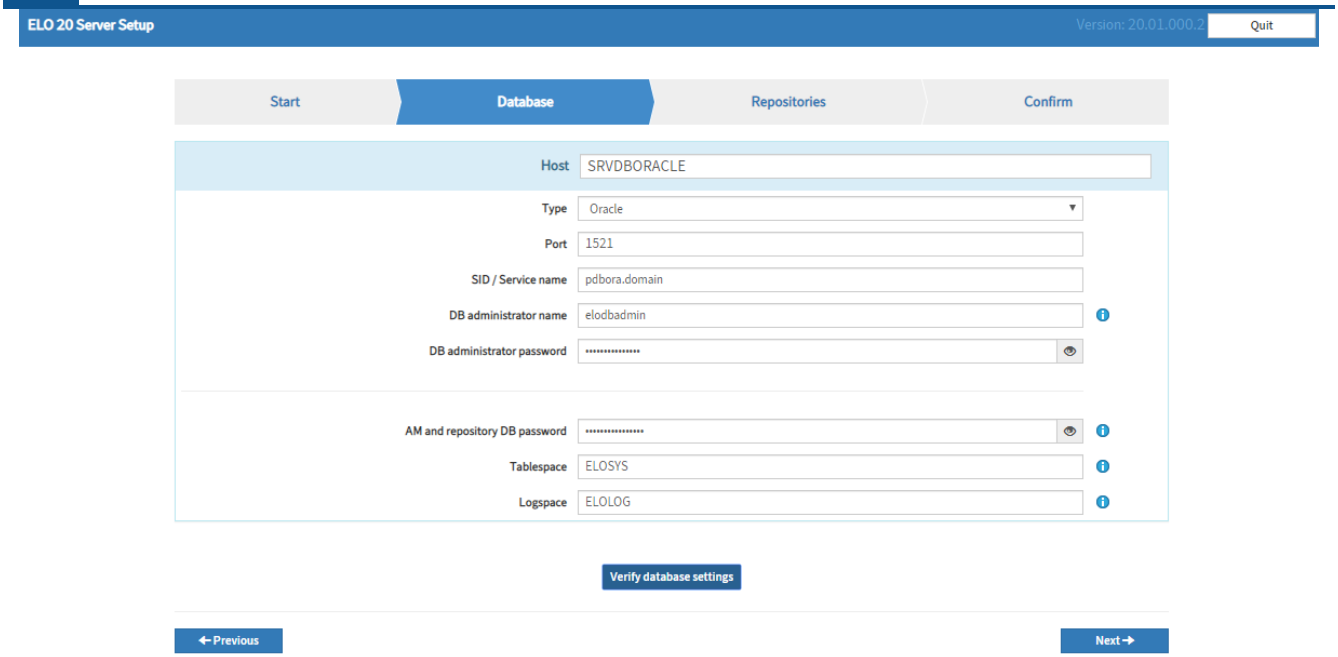
The updated file looks like this:

```
# listener.ora Network Configuration File:
C:\oracle\product\12.1.0\dbhome_1\network\admin\listener.ora
```

```
# Generated by Oracle configuration tools.

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = CLRExtProc)
      (ORACLE_HOME = C:\oracle\product\12.1.0\dbhome_1)
      (PROGRAM = extproc)
      (ENVS =
"EXTPROC_DLLS=ONLY:C:\oracle\product\12.1.0\dbhome_1\bin\oraclr12.dll")
    )
    (SID_DESC=
      (GLOBAL_DBNAME=ora12c)
      (SID_NAME= ora12c)
    )
    (SID_DESC=
      (GLOBAL_DBNAME=pdbora)
      (SID_NAME=pdbora)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
      (ADDRESS = (PROTOCOL = TCP) (HOST = <HOST)(PORT = 1521))
    )
  )
```

The installation can then be performed. Notice that in the ELO Server Setup dialog box for entering the database parameters, you must provide the name of the pluggable database with the domain:

Host	Oracle server host name
Port	TNS port for client connections
SID/Service name	PDB name with domain
DB administrator name	DBA account for the PDB
DB administrator password	DBA account password for the PDB
AM and repository DB password	The setup will create the ELO Access Manager and repository DB accounts with this password.



Substitute for the DBA role

In some cases, the DBA role is not available.

If this is the case, the Oracle account *elodbadmin* can be created with all the rights assigned to the *elodb* account.

Passwords

In Oracle 11, passwords expire after 180 days. We recommend changing this. If the password expiration is not changed before running the ELO installation, all created database accounts should be checked. This check can be performed in Oracle Enterprise Manager.

Notes

Case-sensitive search

When using Microsoft SQL Server, the search process for a standard installation is not case sensitive, meaning that it does not matter whether a string contains upper or lower case letters. This is useful, since a case-sensitive search will fail if letters are capitalized improperly; for example, if you search with "test", a document named "Test" will not be returned. Unfortunately, Oracle SQL Server offers only a case-sensitive search and as such is not ideal. For this reason, certain functionalities have been integrated in ELO to reduce the impact of the case-sensitive search.

Searching in the short name and extra text causes a full table scan to occur. Here, ELO can carry out the search with a "where upper(…" clause without any adverse effects on performance.

The method described above will not work when searching the metadata. This is because SQL Server efficiently accesses the field contents using an index. For this reason, the contents of the

metadata are stored twice on the Oracle server, once under *okeydata* in the original text format, and once under *okeyudata* in upper case form. Search requests from ELO are addressed to the *okeyudata* column to ensure a rapid response to the request. The display is then carried out from the *okeydata* column, using the text in the original format.

All table, index, and column names within ELO are generally written in lower case to prevent conflicts.

Searching in the sticky notes always uses a full table scan. Therefore, this can also be carried out using a "where upper(..." query.

ELO Business Solutions on an Oracle database

Some ELO Business Solutions (ELO Knowledge and others) require you to change an Oracle database setting so that you can run them: `MAX_STRING_SIZE=EXTENDED`

Background

Some ELO Business Solutions require you to change an Oracle database parameter so that you can run them. This applies in particular to ELO Knowledge. ELO Invoice is not affected.

In an Oracle database, the NVARCHAR2 data type is limited to 2000 characters by default. The OBJDESC column in the OBJECTS table has this data type. This field corresponds to the extra text of an ELO object ("sord").

The ELO Business Solutions store the solution-specific button definitions (action definitions) in JSON format in this field. ELO Knowledge also stores post texts in this field. This means that buttons are not always displayed due to the length restriction and posts cannot be saved in full.

To fix this problem, we can increase the maximum length of the NVARCHAR2 type in the Oracle database and widen the OBJEKTE.OBJDESC column. This solution is available starting with Oracle database version 12c.

The database administrator is responsible for making changes to the database. The solution to the problem is based on this blog entry:

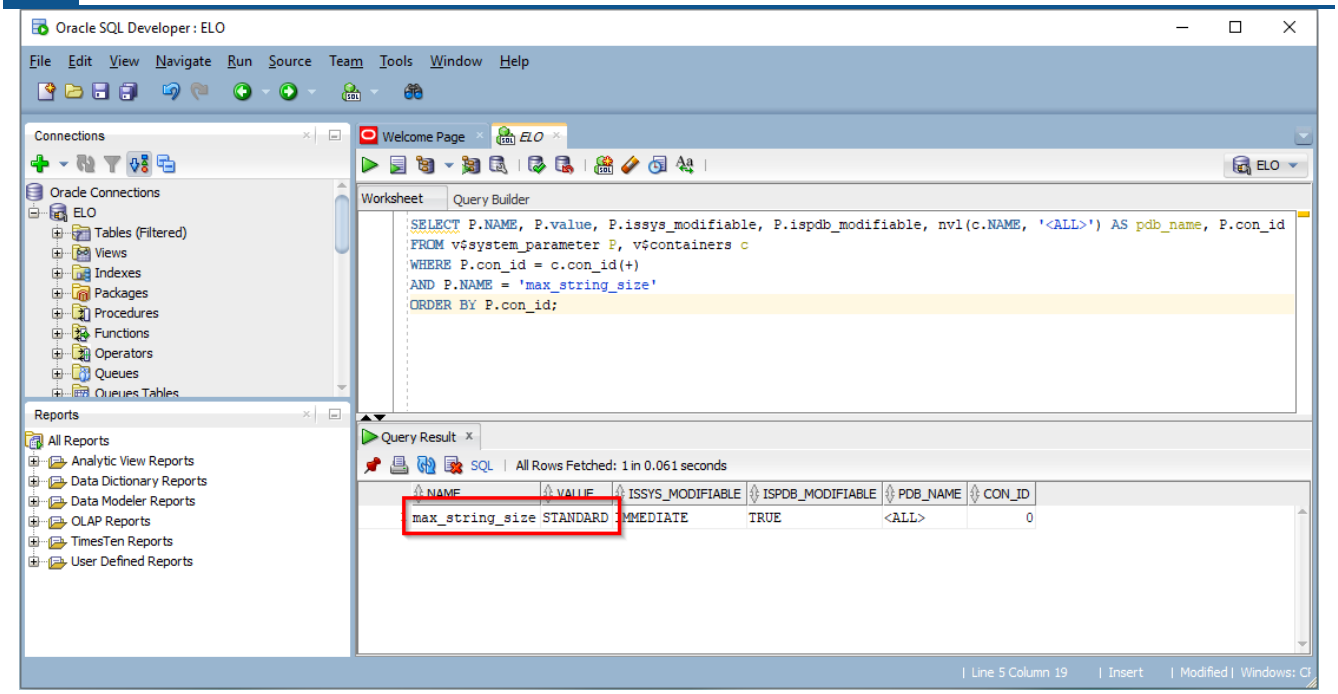
https://www.carajandb.com/en/blog/2014/extended-data-types-with-varchar2-32767-en/

Implementation

This section describes how to implement the changes.

Changing the MAX_STRING_SIZE setting

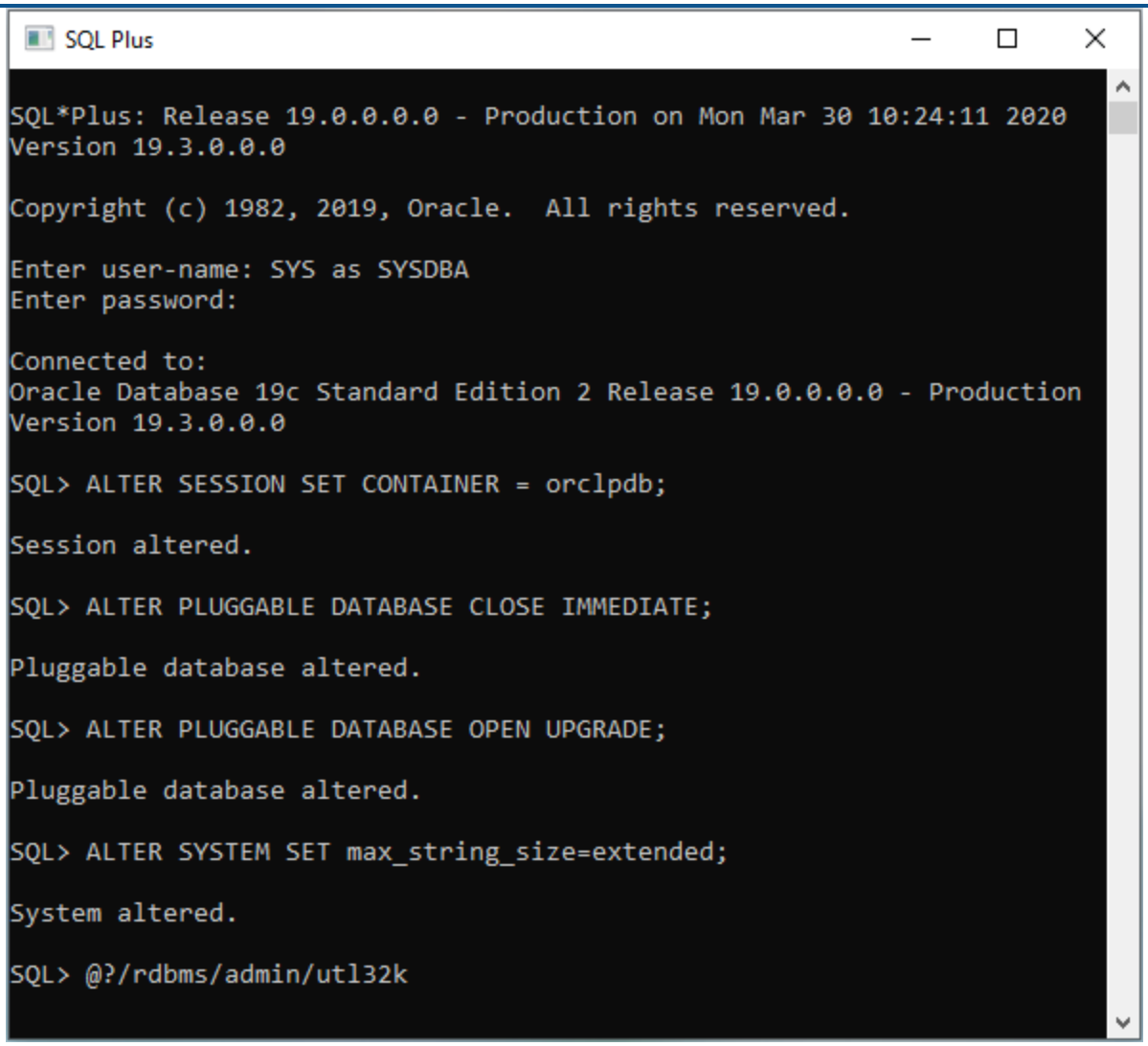
This example describes how to implement the change on a multitenant database.



1. First, call the current value of the `MAX_STRING_SIZE` parameter in Oracle SQL Developer.

   The corresponding query is:

```
SELECT P.NAME, P.value, P.issys_modifiable, P.ispdb_modifiable,
        nvl(c.NAME, '<ALL>') AS pdb_name, P.con_id
FROM v$system_parameter P, v$containers c
WHERE P.con_id = c.con_id(+)
AND P.NAME = 'max_string_size'
ORDER BY P.con_id;
```



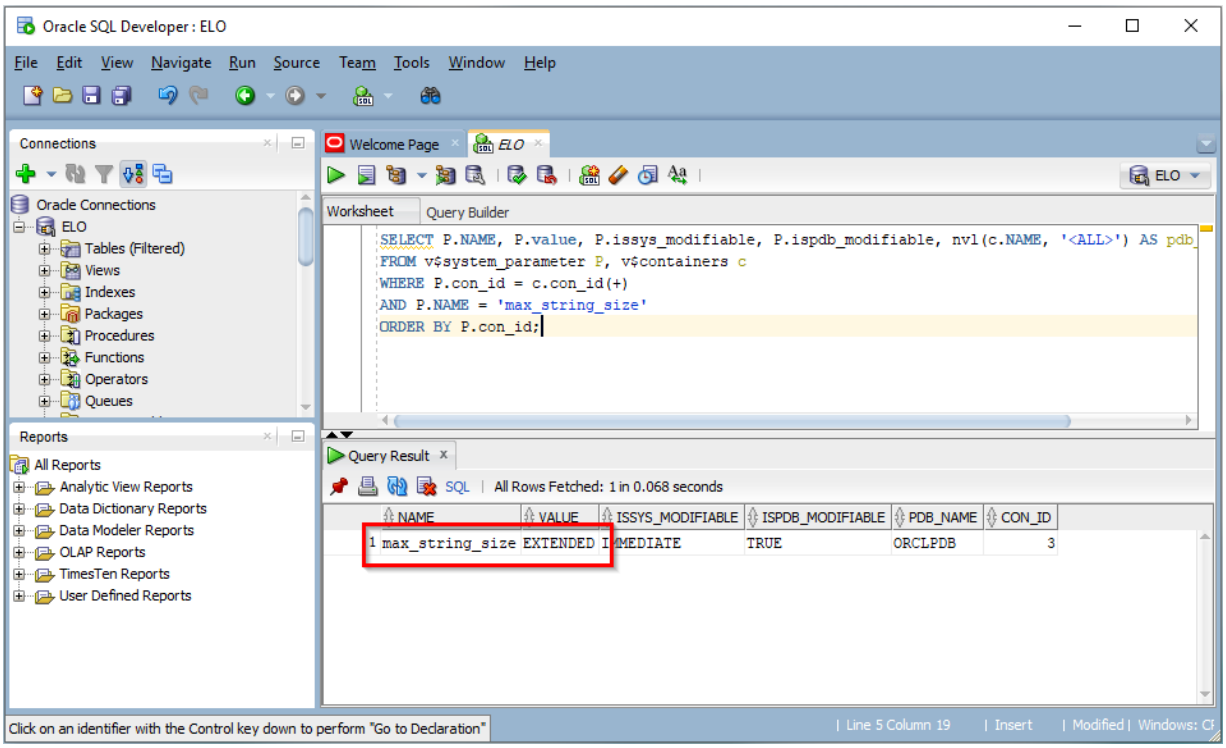
2. Use SQL Plus to change the value of the `MAX_STRING_SIZE` parameter to `EXTENDED`.

> **Please note**
>
> This step cannot be reversed.

The following commands are issued to change the parameter:

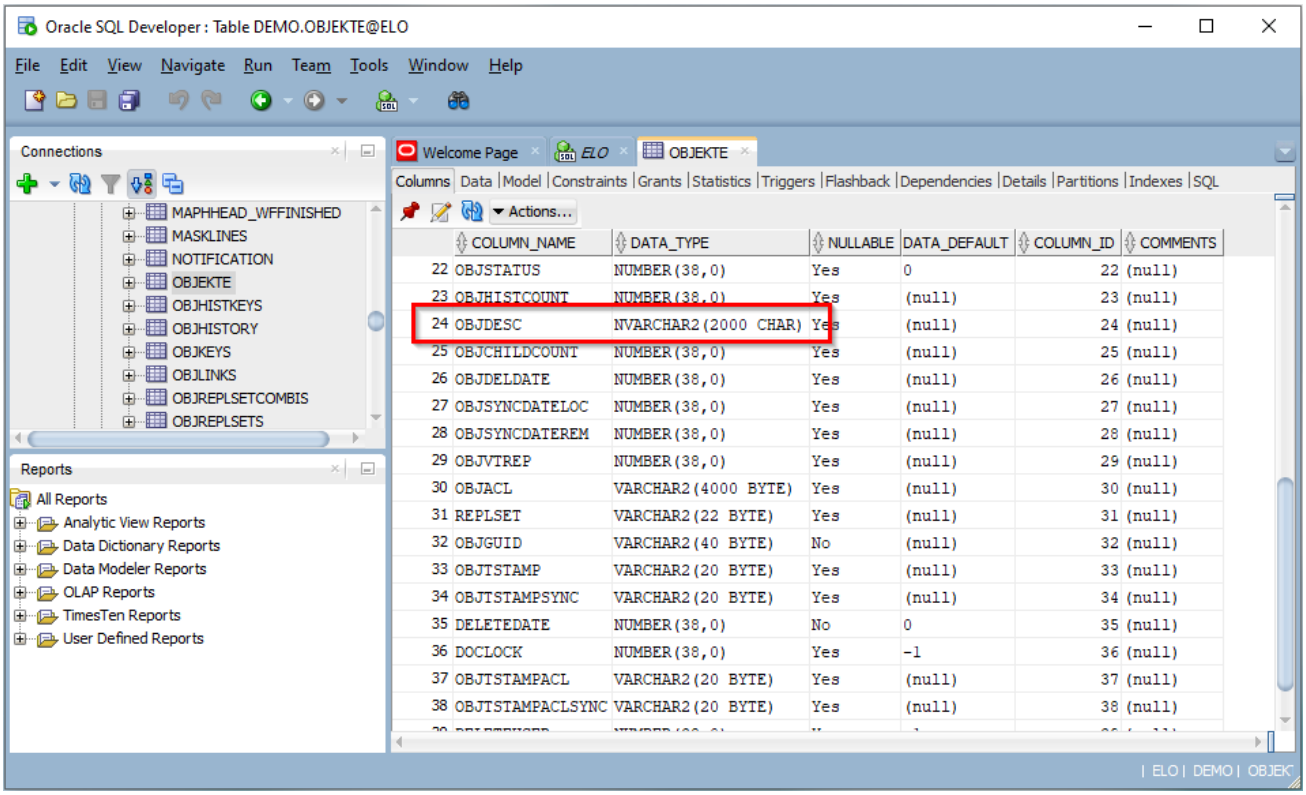
```
ALTER SESSION SET CONTAINER = orclpdb;

ALTER PLUGGABLE DATABASE CLOSE IMMEDIATE;

ALTER PLUGGABLE DATABASE OPEN UPGRADE;

ALTER SYSTEM SET max_string_size=extended;

@?/rdbms/admin/utl32k
```

```
ALTER PLUGGABLE DATABASE CLOSE;

ALTER PLUGGABLE DATABASE OPEN;
```

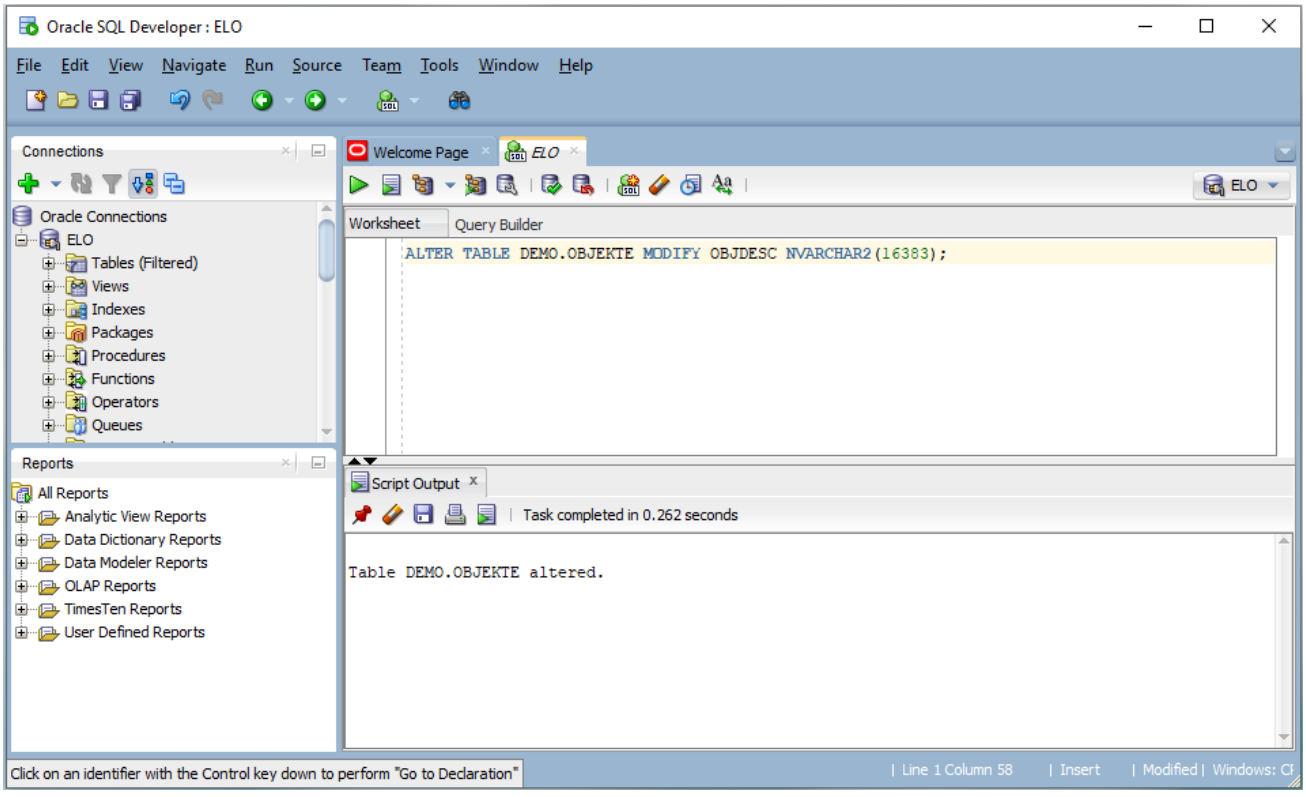


3. Check the change to the parameter in Oracle SQL Developer.

Widen OBJEKTE.OBJDESC column



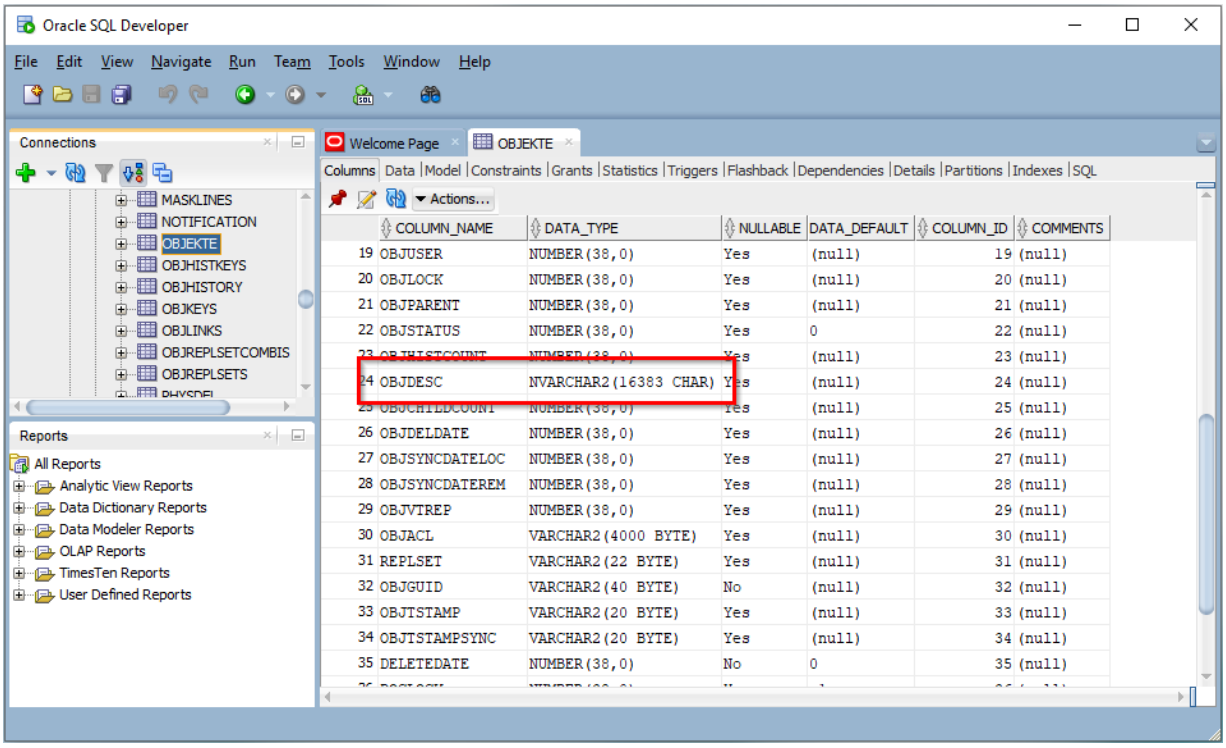
The *OBJEKTE.OBJDESC* column has a width of 2000 characters by default.



1.

Change the column width in Oracle SQL Developer with the following command:

```
ALTER TABLE DEMO.OBJEKTE MODIFY OBJDESC NVARCHAR2(16383);
```



You can now see the changed column size in Oracle SQL Developer.

2. Restart all ELO server components.

   After a restart, you can install the ELO Business Solutions as required.

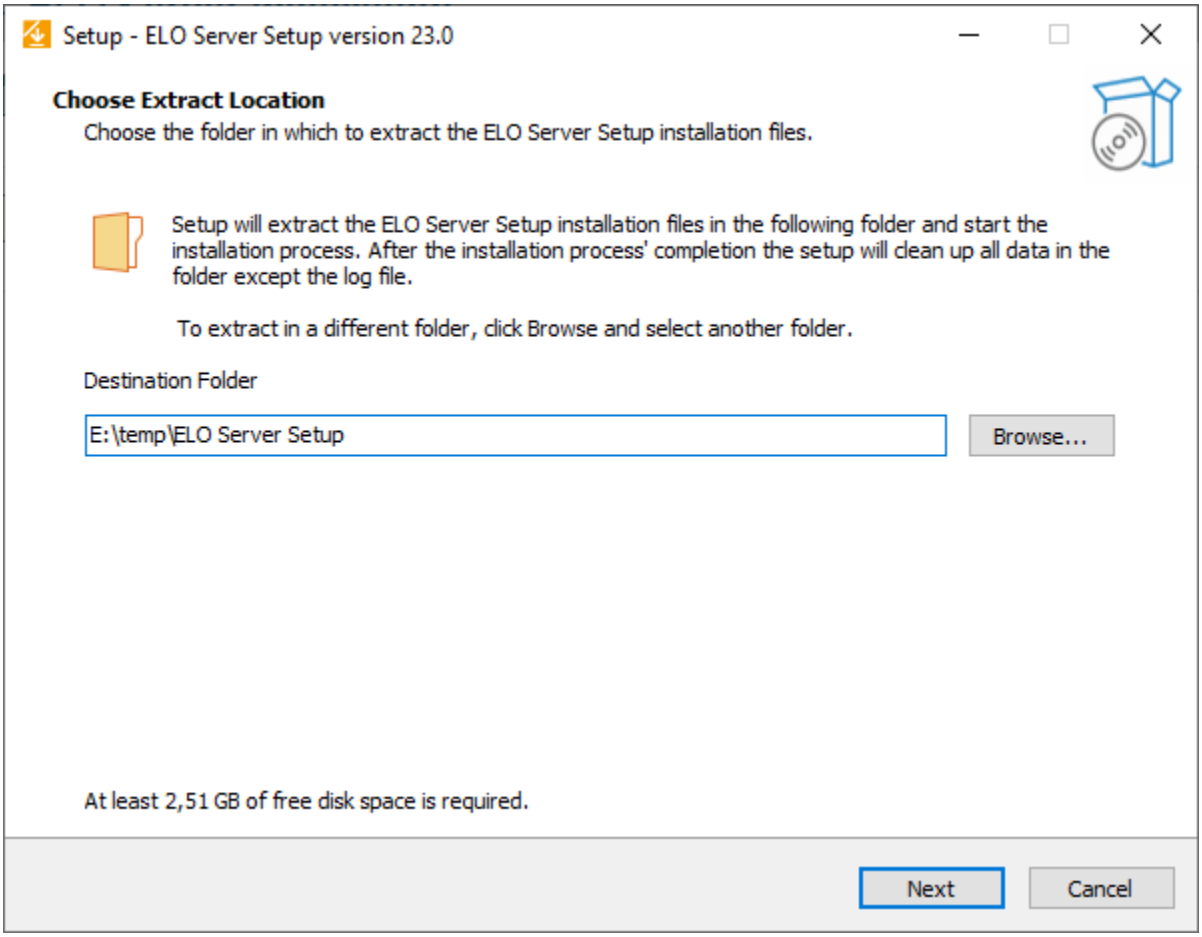
ELO Server Setup

Introduction

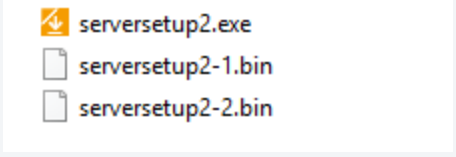
This chapter describes how to install the ELO server. Differences between ELOprofessional and ELOenterprise are explained where applicable.

> **Information**
>
> If you are installing ELOenterprise, it is possible to install various server modules to different computers. See the Distributed installation of ELOenterprise section of this documentation for details on this feature.

1. Run the ELO Server Setup.



> **Information**

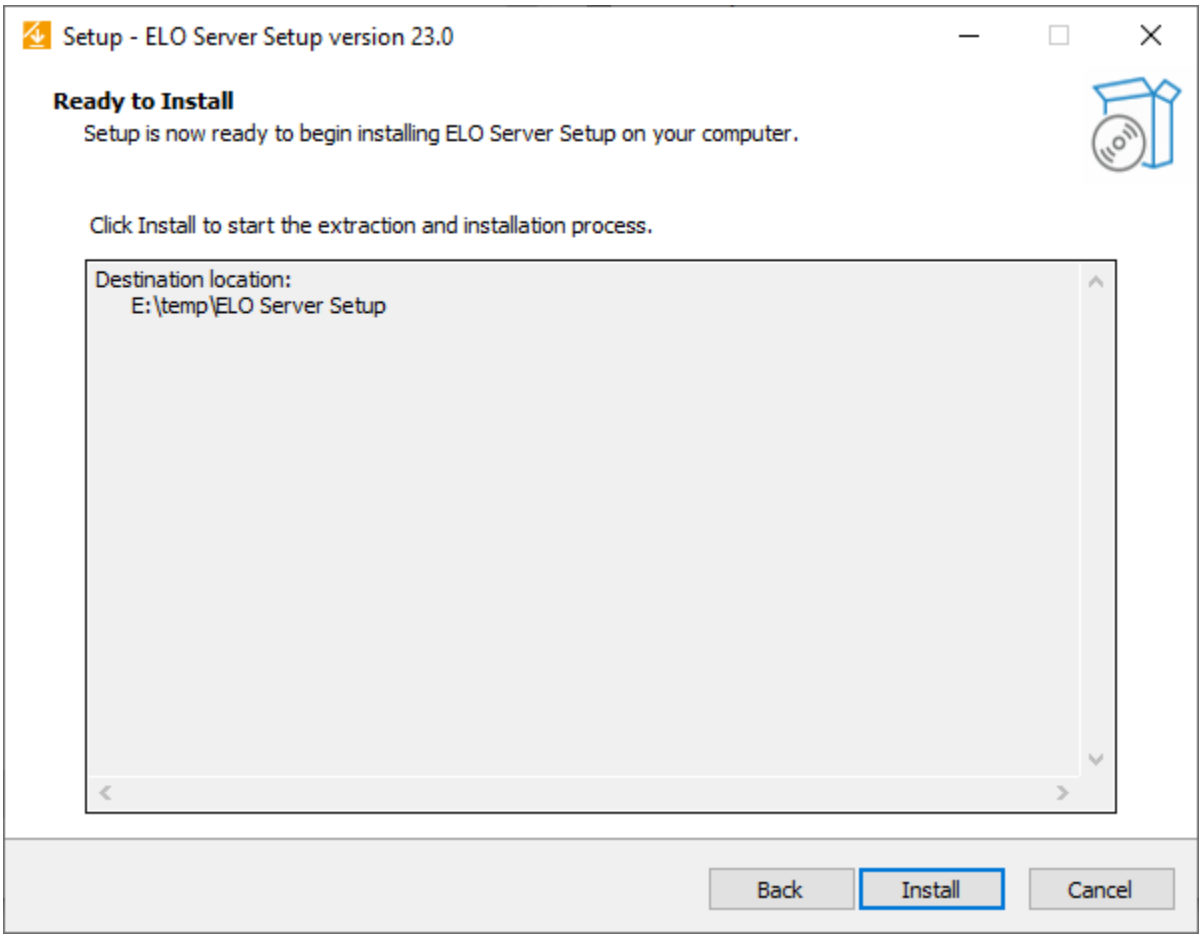


If you are using the setup as a single download, make sure that you have copied all setup files to the target system. Under Windows, three files are required starting with ELO 21.1 (*serversetup2.exe*, *serversetup2-1.bin* and *serversetup2-2.bin*).

2. Choose the folder you want to extract the installation files to.

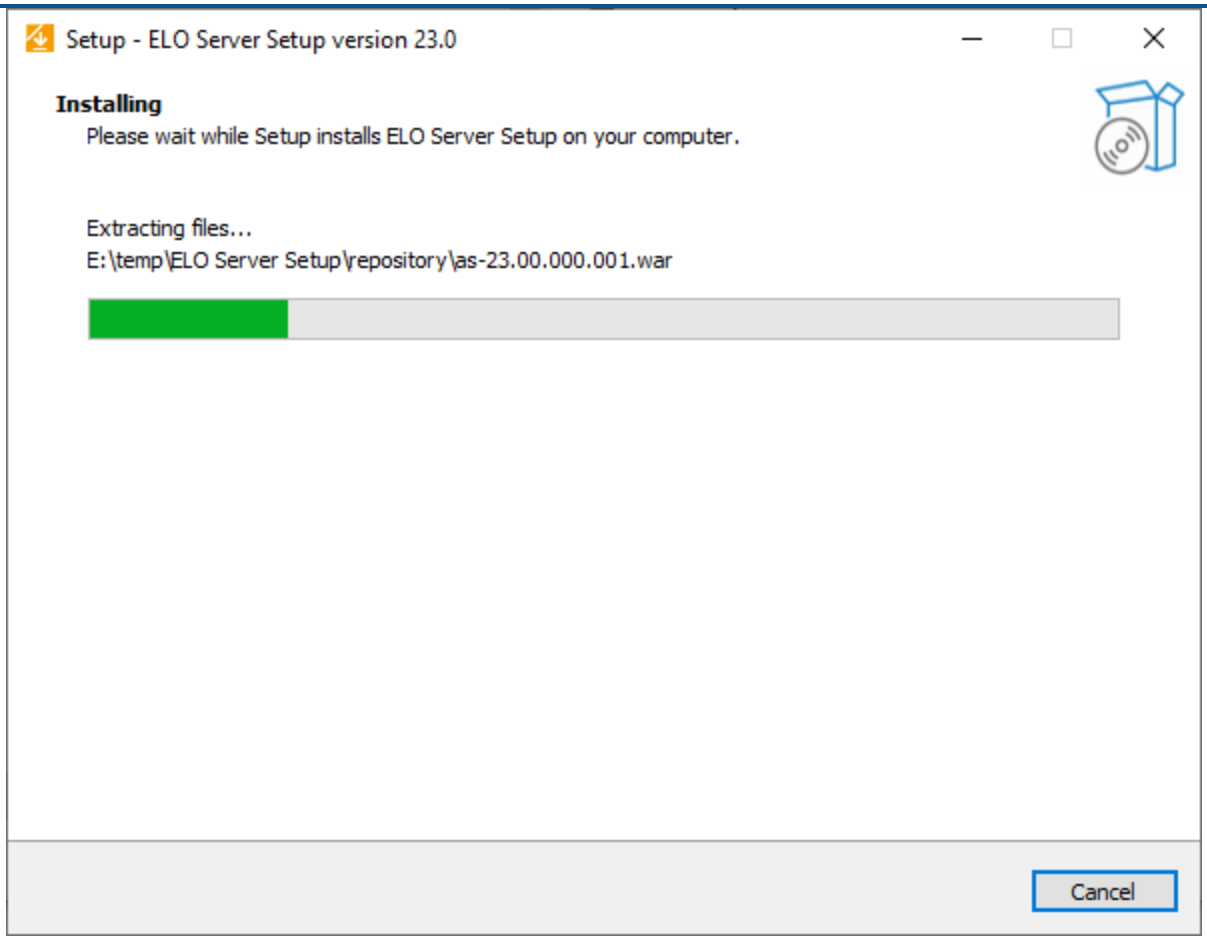
Information

Nothing will actually be installed at this point. The installation files are only temporarily stored here until the ELO server components are set up and installed. When the ELO Server Setup closes, the temporary files are deleted from the drive.

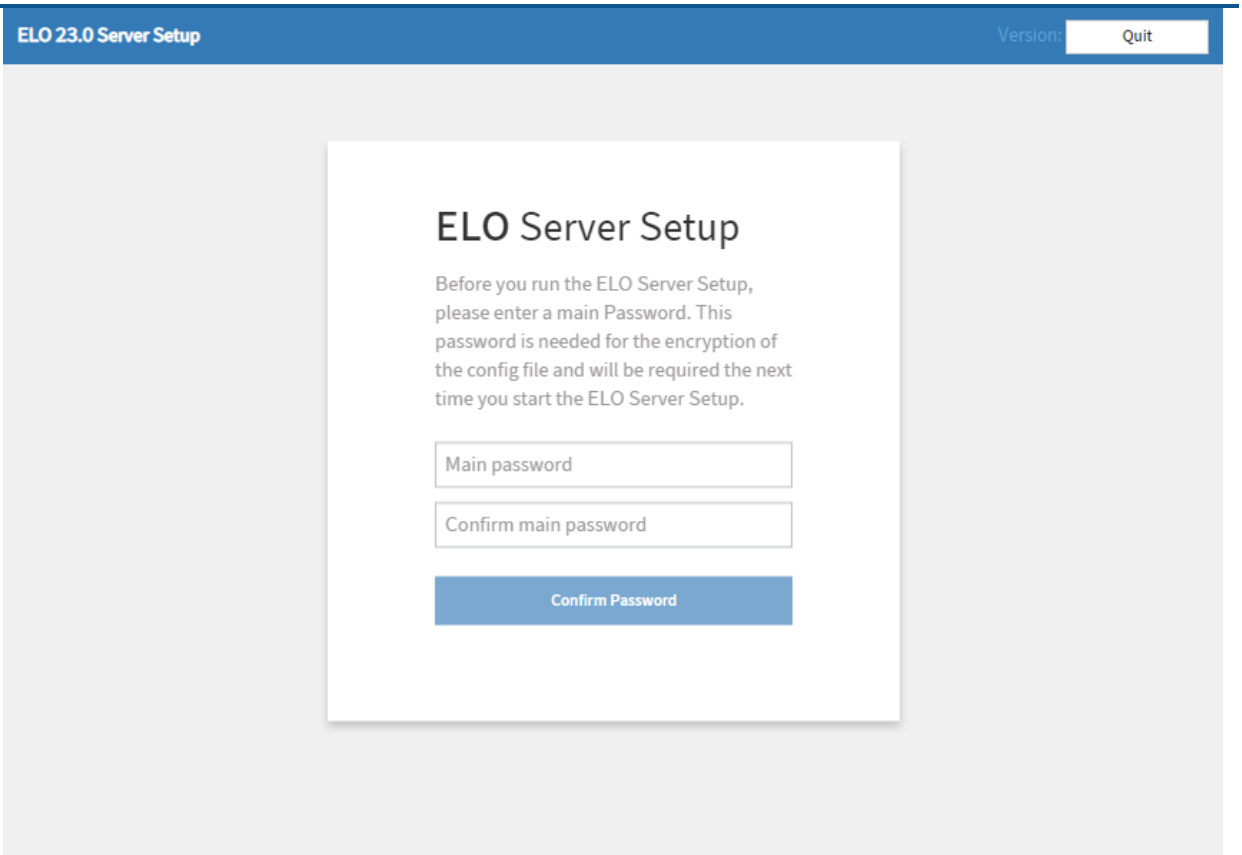


The *Ready to Install* screen opens.

3. Confirm with *Install*.



Wait a few minutes while the package contents extract.



When the process is complete, your default browser will open. You will be asked to set a *main password* for the ELO Server Setup.

4. Set a main password for the ELO Server Setup.

> **Important**
>
> In the following installation process, the *elosetup.conf file* is encrypted. The key is the main password.
>
> If you lose the main password, you will no longer be able to decrypt and edit the *elosetup.conf* file. All saved data will be lost.
>
> To learn how to decrypt the files, refer to the documentation Decrypting the setup configuration.

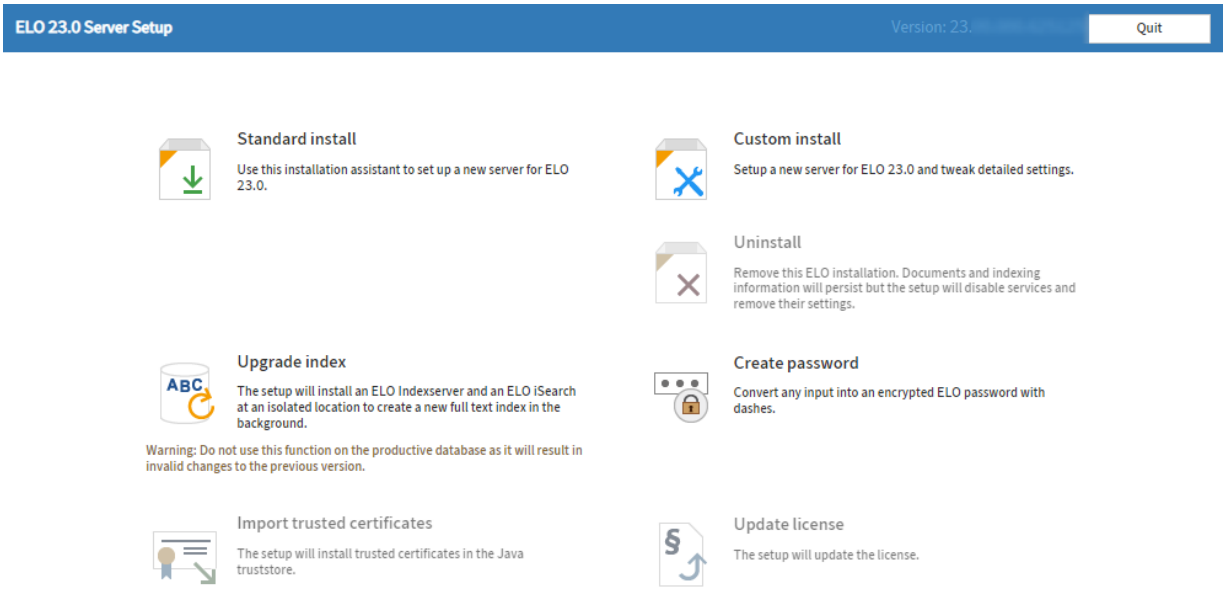
> **Information**
>
> The main password is requested every time you run the ELO Server Setup.

The second password field is initially red because the password has not yet been confirmed.

5. Enter the password again in the second field.

If you entered the password correctly, the field turns green.

6. Select *Confirm Password*.



The ELO Server Setup menu appears.

At this point, you can install or upgrade the ELO server, or quit the installer either by selecting *Quit* or by closing the window.

> **Please note**
>
> If an Apache Tomcat server is already installed on this computer, some Apache Tomcat configurations can run into problems installing ELO server components. This can occur even if the Apache Tomcat is uninstalled first (if some parts of the previous installation were not completely uninstalled). If this occurs, remove the previous Apache Tomcat services and delete the Apache Tomcat files on the hard drive, then attempt installation again.

Standard Install: To install ELOprofessional or ELOenterprise with default settings, select *Standard Install*. Refer to the section Standard Install for more information.

Custom Install: Select *Custom Install* if you want to make advanced settings before installation. Refer to the section Custom Install for more information.

Information

The *Upgrade* option is no longer available. If your ELO installation is version 9 or older, you will need to do the update in multiple steps.

For more information, refer to the Update documentation.

Uninstall: To uninstall an ELO server, select *Uninstall*. Data and indexes will not be deleted.

Upgrade index: To create a full text index in the background, select *Upgrade Index*. This option installs an additional ELO Indexserver and ELO iSearch module on a separate path.

Create password: To generate an encrypted password, select *Create password*.

Import trusted certificates: To upload certificates for server encryption, select *Import trusted certificates*. The certificates are loaded into a certificate store.

Update license: To update the license file only, select *Update license*.

Standard Install

This section describes the installation using the *Standard Install* mode.

The following buttons are on almost every tab:

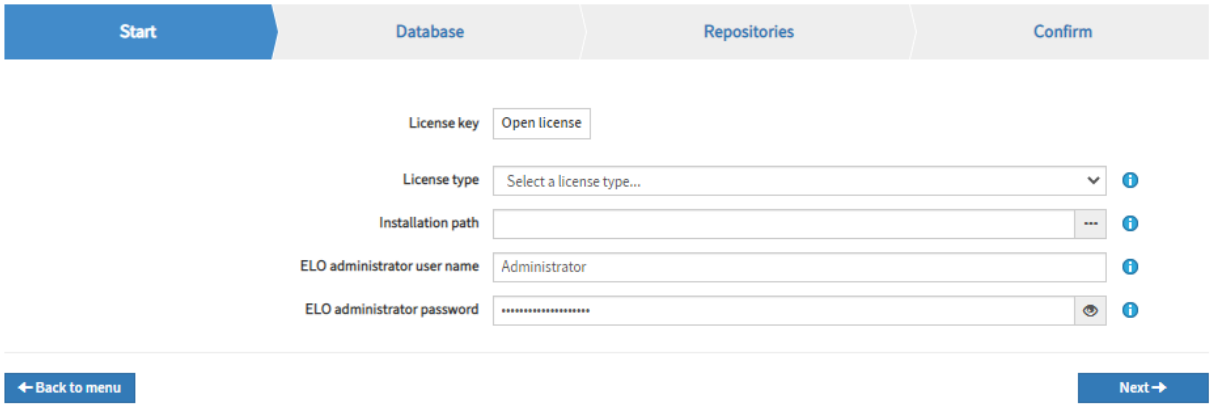
Previous: Select *Previous* to go back to the previous tab.

Quit: Select *Quit* if you wish to close the installer.

Next: Select *Next* to continue on to the next tab of the installer.

> **Please note**
>
> The standard installation mode installs four Apache Tomcat instances and requires several free ports on the server. See the *Default server configuration* section in the *ELO server and modules* chapter for details on required ports.

'Start' tab



After you have selected the installation mode, the *Start* tab opens.

License key: Select *Open license* and select a valid license file.

> **Please note**
>
> In this installation mode, all server modules will be installed to the current computer regardless of whether you enter an ELOenterprise or ELOprofessional key. If you want to run a distributed installation, return to the menu and choose *Custom Install*.

License Type: In the *License Type* drop-down menu, select the type of system you want to install (production system, test system, or development system).

Installation path: Enter the path where you want to install the ELO server. Select the *(...)* button to open a dialog box for selecting a folder.

ELO administrator user name: This is the name for the default ELO administrator account (with the fixed ID `0`). *Administrator* is selected by default.

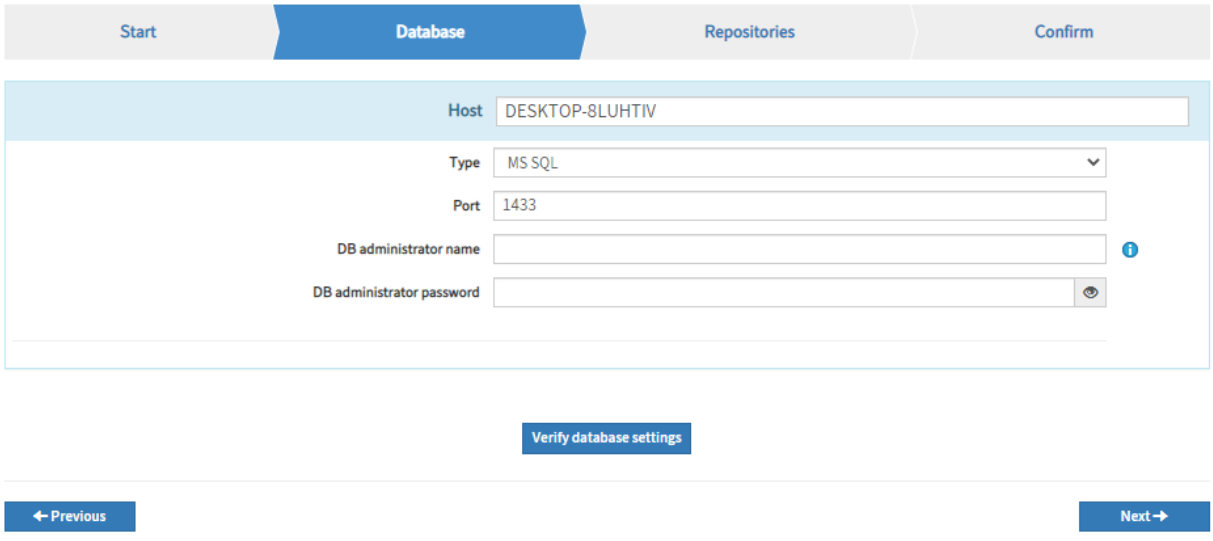
> **Please note**
>
> In earlier versions of ELO, a different name was assigned for the ELO administrator account according to the respective language. If you wish to use an administrator with a country-specific name (e.g. *administrateur*), you must change it here.

ELO administrator password: A random password is generated for the ELO administrator account by default. You may change this password before installation. Select the button with the *eye* icon on the right to view the password.

> **Information**
>
> Earlier versions of ELO used the same password for the administrator account and the *ELO Service* account during installation. Since ELO 10, you can create separate passwords for these accounts. If you want to edit the *ELO Service* account name or password, use *Custom install* mode.

Back to menu: To return to the menu, select *Back to menu*.

'Database' tab



Host: Enter the computer name or IP address of the SQL Server. The local computer name is entered in this field by default.

Type: Select the database system used from the list. Additional information is required if you select *Oracle* or (IBM) *DB2*.

Port: Enter the port used to communicate with SQL Server. The standard port for each database type is entered in this field by default (e. g. 5432 for PostgreSQL, 50000 for IBM DB2, etc.).

SID/Service name: This field only appears for Oracle databases. Enter the SID that uniquely identifies your Oracle database instance here.

DB administrator name: Enter the name of the ELO database here. For example, the account *elodb*.

> **Please note**
>
> The method used to set up the ELO database account varies depending on the database software used (default *elodb*). Refer to the following sections for more information:
>
> - Microsoft SQL Server > elodb account
> - PostgreSQL Server > Create a logon for PostgreSQL Server
> - Oracle SQL Server > Creating the ELO accounts

DB administrator password: Enter the current password for the ELO database account. The password is hidden by default. Select the button with the *eye* icon on the right to view the password.

Instance: This field only appears for IBM DB2 databases. Enter the name of the instance in this field.

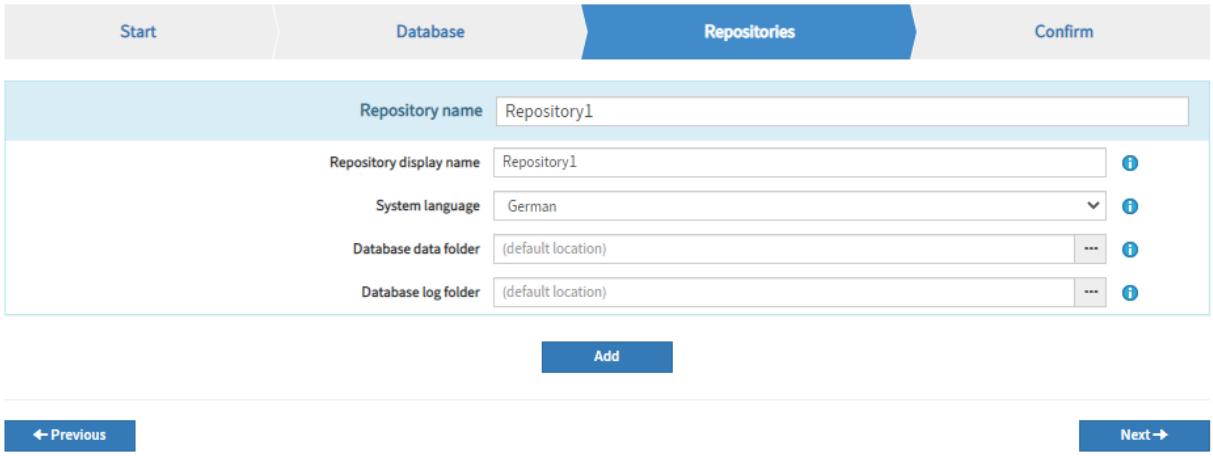
AM and Repository DB Password: This field only appears for Oracle databases. A password is assigned to the ELO Access Manager and repository tables during installation, and you can view and change it here. The password is generated randomly and hidden by default. Select the button with the *eye* icon to view the password.

Tablespace: This field only appears for Oracle databases. Enter the tablespace to be used during installation of ELO. ELOSYS is entered in the field by default.

Logspace: This field only appears for Oracle databases. Enter the logspace to be used during installation of ELO. ELOLOG is entered in the field by default.

Verify database settings: *Verify database settings* allows you to check whether you can connect to the SQL database with the current database settings.

'Repositories' tab



Repository name: Enter a name for the repository in the field here. The name affects the connection to the ELO Indexserver, ELO Web Client, and other ELO modules, as well as the names of various directories and other settings.

Repository display name: You can specify a display name that differs from the repository name if required. The display name is shown at the top folder level in the client, for example, and is also the name of the tile for the *Repository* work area.

You can also change the display name in the ELO Administration Console.

System language: Select the repository language from this drop-down list. English is selected by default. This setting affects the following names:

- The name of the "Everyone" group
- The names of ELO font colors
- The names of ELO projects and activities
- The name of the system key
- The names of ELO metadata forms

Data folder: In the *Data folder* field, you can specify a database base path that differs from the default one. For Oracle, enter the name of the SYS tablespace.

Log folder: In the *Log folder* field, you can specify a database log path that differs from the default one. For Oracle, enter the name of the LOG tablespace.

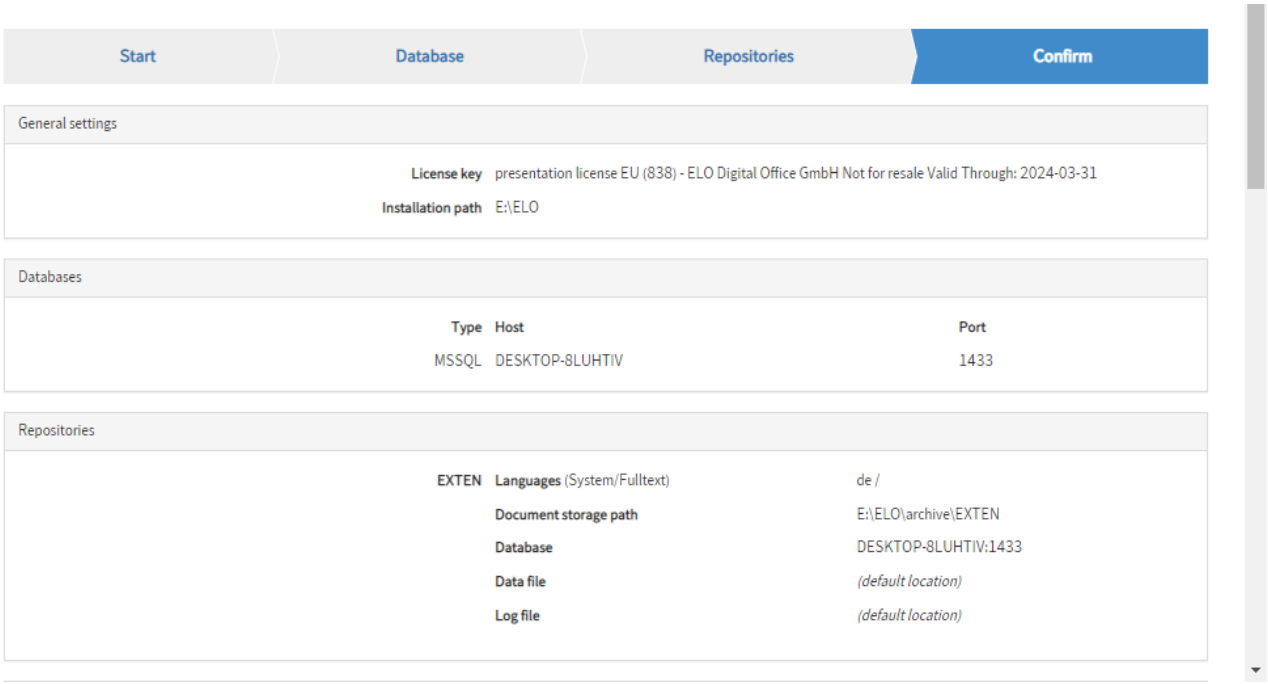
Add: Select *Add* to create additional repositories during installation. You must create at least one repository to complete the installation.

Remove: To remove a repository, select *Remove*.

Please note

For the *Remove* button to appear, there must be at least two repositories. There must always be at least one repository left.

'Confirm' tab



This tab contains the settings for the ELO server after installation. If any errors are found during installation, they are displayed in red in a table at the top of this screen.

Review the settings shown here and make sure they are correct before proceeding.

User names and passwords

The *User names and passwords* table at the bottom of this tab shows the accounts that will be created when ELO is installed.

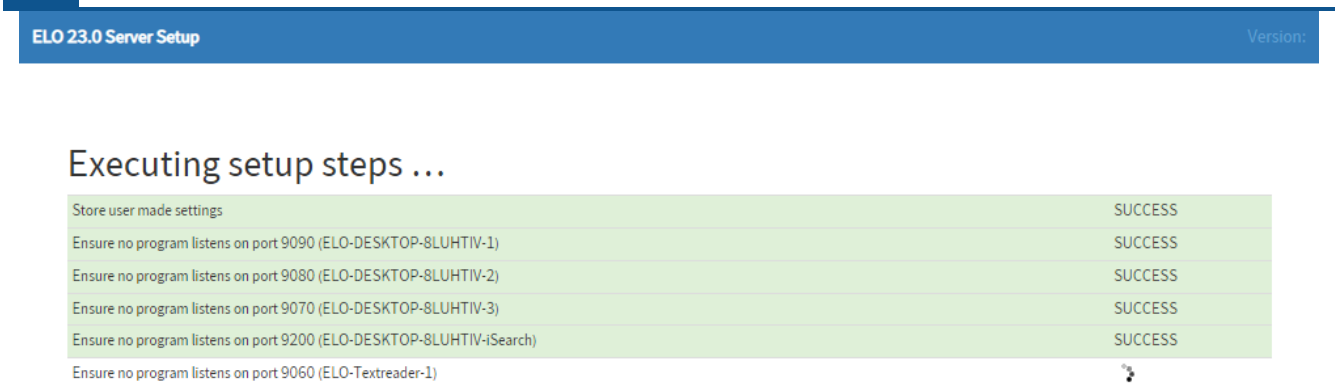
Show passwords: *Show passwords* enables you to see and check all passwords. In this mode, you can also print the passwords using the *Print* function (see below).

Important

Make sure that you make a note of the *ELO Service* password and *Apache Tomcat Administrator* password. These are generated automatically during setup.

Print: Use the *Print* button to print the page for your records.

Install: Select *Install* to install the ELO server.



The installation switches to the next screen, which shows the progress of the individual installation steps and any errors.

Finish: When the *Finish* button appears at the bottom of the screen, the installation is complete. Select *Finish* and close the window.

A detailed log of the installation progress is stored in the server setup directory in *serversetup2.log*. Keep this file for your records. It may be required for support requests in the future.

> **Important**
>
> Make sure that this file is kept in a secure location. As it is a detailed log of the installation process, it lists all passwords used (or created) in the installation in plain text.

The *Default server configuration* section provides basic information about the server you just installed. After reviewing it, go to the *Server-side adjustments following installation* section to see if there are any follow-up steps you still need to complete.

Custom Install

This section describes the installation using the *Custom Install* mode.

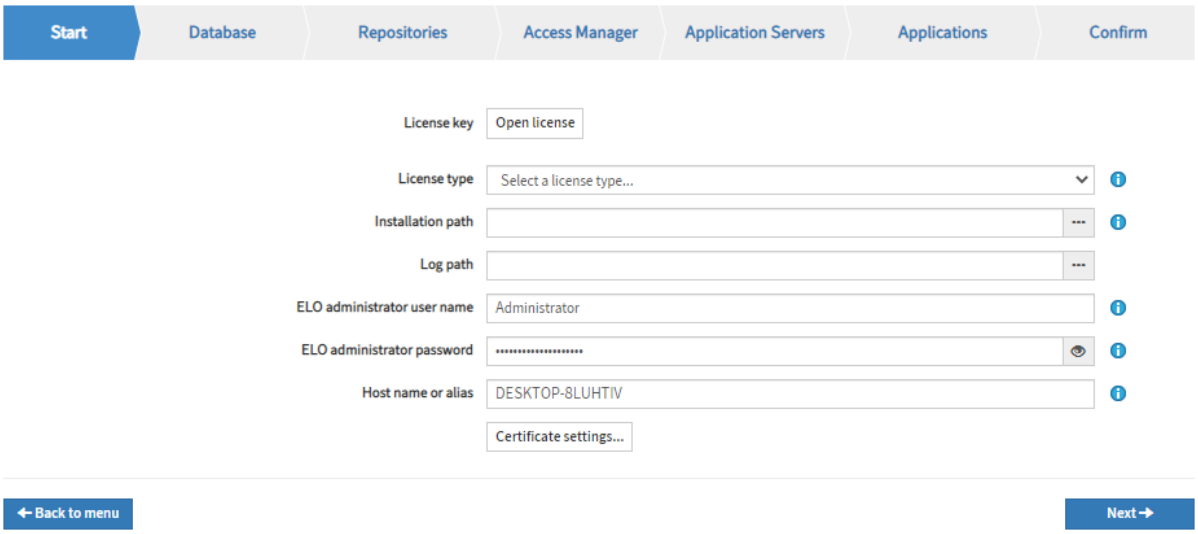
The following buttons are on almost every tab:

Previous: Select *Previous* to go back to the previous tab.

Quit: Select *Quit* if you wish to close the installer.

Next: Select *Next* to continue on to the next tab of the installer.

'Start' tab



After you have selected the installation mode, the *Start* tab opens.

License key: Select *Open license* and select a valid license file.

License Type: In the *License Type* drop-down menu, select the type of system you want to install (production system, test system, or development system).

Installation path: Enter the path where you want to install the ELO server. Select the *(...)* button to open a dialog box for selecting a folder.

ELO administrator user name: This is the name for the default ELO administrator account (with the fixed ID `0`). *Administrator* is selected by default.

Please note

In earlier versions of ELO, a different name was assigned for the ELO administrator account according to the respective language. If you wish to use an administrator with a country-specific name (e.g. *administrateur*), you must change it here.

ELO administrator password: A random password is generated for the ELO administrator account by default. You may change this password before installation. Select the button with the *eye* icon to view the password.

Information

Earlier versions of ELO used the same password for the administrator account and the *ELO Service* account during installation. Since ELO 10, you can change the name and passwords for all these accounts in the *Custom Install* mode.

Host name or alias: Enter the host name or an alias to the *Host name or alias* field.

Certificate settings: *Certificate settings* opens a dialog box where you can load and manage SSL certificates.

Information

The *Host name or alias* field and the *Certificate settings* button only apply for ELOprofessional installations. They disappear as soon as you upload an ELOenterprise license file. You will find the corresponding settings on the *Servers* tab.

- Generate self signed certificates: If the option *Generate self signed certificates* is set to *ON*, the ELO Server Setup generates a certificate for encryption.

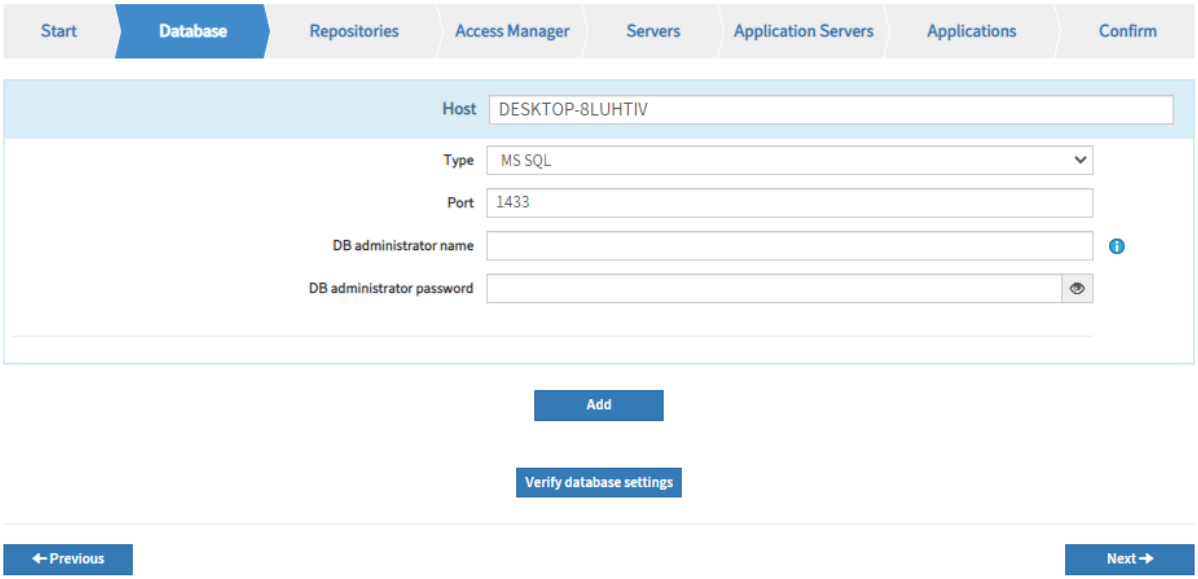
Information

After installation, you will find the certificate file *rootca.pem* under the path `<installation directory>\data\serversetup2`.

You need to import the *rootca.pem* file to the client computers so that they can connect to the server.

Back to menu: To return to the menu, select *Back to menu*.

'Database' tab



Host: Enter the computer name or IP address of the SQL Server. The local computer name is entered in this field by default.

Type: Select the database system used from the list. Additional information is required if you select *Oracle* or (IBM) *DB2*.

Port: Enter the port used to communicate with SQL Server. The standard port for each database type is entered in this field by default (e. g. 5432 for PostgreSQL, 50000 for IBM DB2, etc.).

SID/Service name: This field only appears for Oracle databases. Enter the SID that uniquely identifies your Oracle database instance here.

DB administrator name: Enter the name of the ELO database here. For example, the account *elodb*.

> **Please note**
>
> The method used to set up the ELO database account varies depending on the database software used (default *elodb*). Refer to the following sections for more information:
>
> - Microsoft SQL Server > elodb account
> - PostgreSQL Server > Create a logon for PostgreSQL Server
> - Oracle SQL Server > Creating the ELO accounts

DB administrator password: Enter the current password for the ELO database account. The password is hidden by default. Select the button with the *eye* icon on the right to view the password.

Instance: This field only appears for IBM DB2 databases. Enter the name of the instance in this field.

AM and Repository DB Password: This field only appears for Oracle databases. A password is assigned to the ELO Access Manager and repository tables during installation, and you can view and change it here. The password is generated randomly and hidden by default. Select the button with the *eye* icon to view the password.

Tablespace: This field only appears for Oracle databases. Enter the tablespace to be used during installation of ELO. ELOSYS is entered in the field by default.

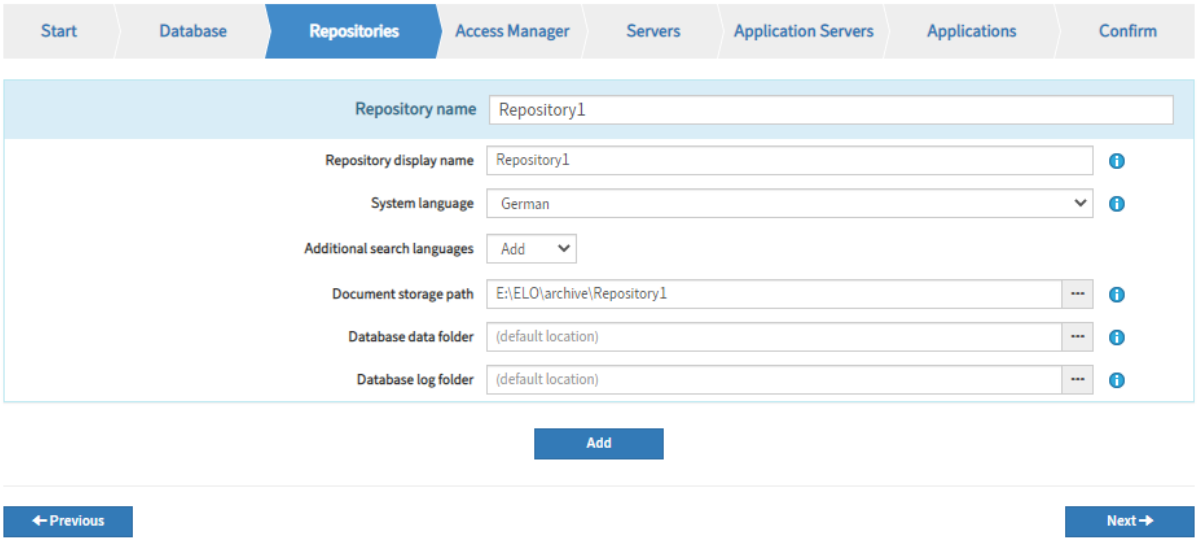
Logspace: This field only appears for Oracle databases. Enter the logspace to be used during installation of ELO. ELOLOG is entered in the field by default.

Add: Use the *Add* button to create additional database connections.

Remove: To remove a database connection, select *Remove*.

Verify database settings: *Verify database settings* allows you to check whether you can connect to the SQL database with the current database settings.

'Repositories' tab



Repository name: Enter a name for the repository in the field here. The name affects the connection to the ELO Indexserver, ELO Web Client, and other ELO modules, as well as the names of various directories and other settings.

Repository display name: You can specify a display name that differs from the repository name if required. The display name is shown at the top folder level in the client, for example, and is also the name of the tile for the *Repository* work area.

You can also change the display name in the ELO Administration Console.

System language: Select the repository language from this drop-down list. English is selected by default. This setting affects the following names:

- The name of the "Everyone" group
- The names of ELO font colors
- The names of ELO projects and activities
- The name of the system key
- The names of ELO metadata forms

Additional search languages: This setting affects the thesauruses imported into ELO iSearch. If you have users that need to use a different language than the system language, you can select them here.

Document storage path: Files in the repository are stored in a document path. Two of these paths are created the first time you install a repository. The default document paths are:

```
<ELO>\archive\<repository name>\basis
<ELO>\archive\<repository name>\elosys
```

You can optionally enter a custom document path here. For example, you may wish to store documents on an MD5 storage device or on a separate, fast network storage device.

This path replaces the string of directories before `\basis` and `\elosys`.

Select *Add* to create additional repositories during installation. Select the button with the X icon to the right of the repository to remove it from the installation. You must install at least one repository to complete the installation.

Data folder: In the *Data folder* field, you can specify a database base path that differs from the default one. For Oracle, enter the name of the SYS tablespace.

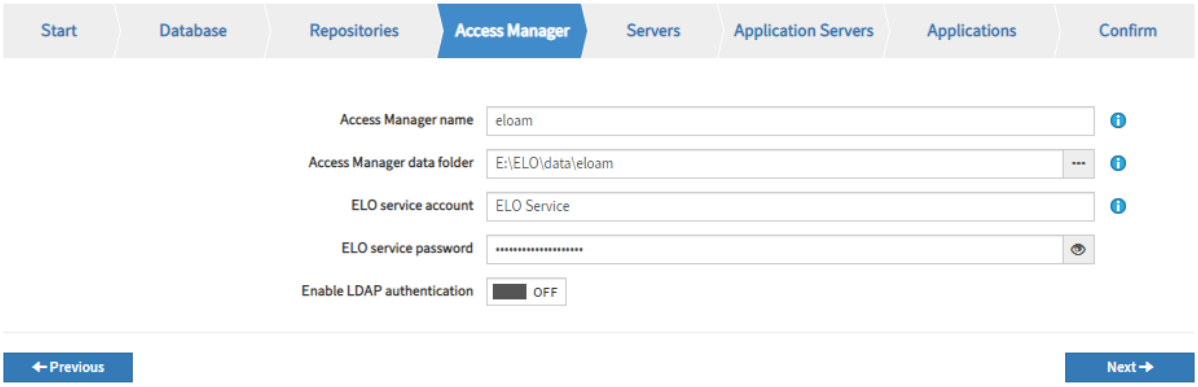
Log folder: In the *Log folder* field, you can specify a database log path that differs from the default one. For Oracle, enter the name of the LOG tablespace.

Add: Select *Add* to create additional repositories during installation. You must create at least one repository to complete the installation.

Remove: To remove a repository, select *Remove*.

> **Please note**
>
> For the *Remove* button to appear, there must be at least two repositories. There must always be at least one repository left.

'Access Manager' tab



Enter the ELO Access Manager and LDAP/Active Directory settings in this tab. You can also define settings for the ELO Service account here.

Access Manager name: Enter a name for the ELO Access Manager in this field. The ELO Access Manager controls permissions to all repositories and information within them that are associated with the ELO Access Manager.

The entry in this field applies for the name of the Access Manager database (which is given exactly the name specified here) and the name of the Access Manager server module (`am-<name>`.

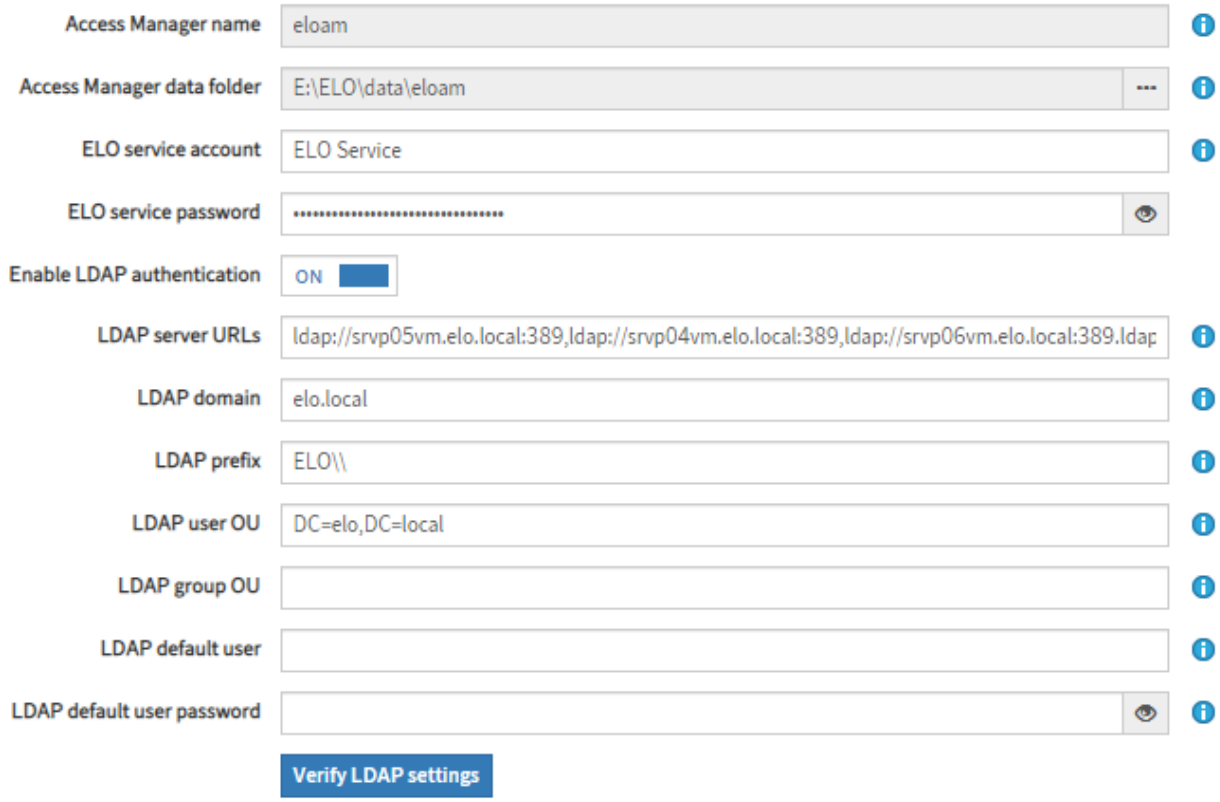
ELO Service account: ELO creates a service account during installation to manage internal processes. By default, this is the *ELO Service* account. You can use another name, e .g. if the service user on your domain account is named differently.

ELO Service password: The ELO Server Setup selects a random password for the *ELO Service* account by default. You can keep this password or enter a different one.

Enable LDAP authentication: Select *OFF* if you want to import accounts from an LDAP directory during installation. Once this option is enabled, the fields below can be edited.

It is possible to enter LDAP settings after installation as well. See the *ELO LDAP* documentation for more information on using single sign-on (SSO) in ELO.

If you do not select the *Enable LDAP authentication* option, you can ignore all other settings on the tab and select *Next*.



LDAP Server URLs: Enter the URL(s) for the LDAP server(s) here.

> **Please note**
>
> At the time of initial installation, LDAPS cannot exist in the Java keystore.
>
> It is not possible to perform an initial installation with an LDAPS URL.
>
> Use an LDAP URL.

LDAP Domain: Enter the domain name which the ELO server is running on. If your company uses multiple domains, select the one which accounts are selected from.

LDAP Prefix: The domain prefix is required if multiple domains are configured and the sAMAccountName is saved as the Windows account for the ELO account. There must be a separator character at the end of the domain prefix. This separates the prefix from the account name. Ideally, you should use a double backslash.

Information

If you are using SSO, the domain prefix must match the NetBIOS domain name. You will find the corresponding domain prefix for SSO in the *USERDOMAIN* environment variable on the client computer. For SSO with domain prefix, you need to set the option *"ntlm.domainUserFormat"* in the ELO Indexserver `config.xml` file.

LDAP user OU: This is where you enter the DN for searching for accounts.

LDAP Group OU: This is where you enter the DN for searching for groups.

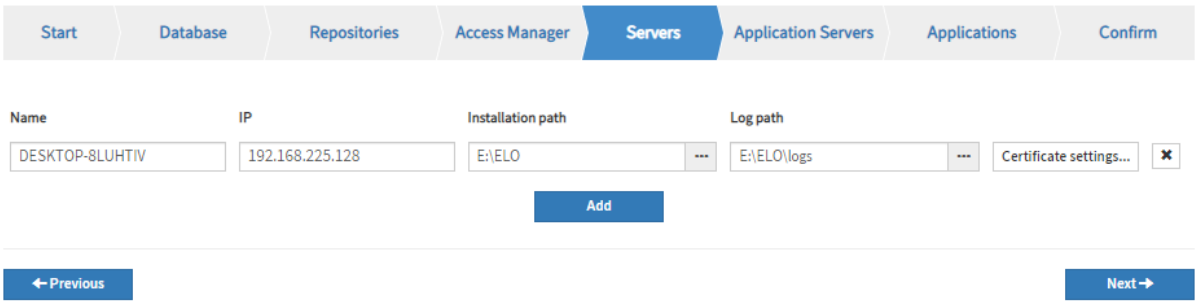
LDAP Default User: SSO requires a technical account to search LDAP for the account name transferred by the SSO mechanism (usually sAMAccountName). The account must also have sufficient permissions to read the account attributes and group memberships.

The account is used for authentication against the LDAP server. As it bears no relation to the ELO user manager, it does not have to be an ELO account.

LDAP Default User Password: In the *LDAP Default User Password* field, enter the unencrypted password for the LDAP default user account. The ELO Indexserver stores the password encrypted on restart.

Verify LDAP settings: Enter a name and password of a valid domain account in order to test the LDAP settings. These configuration settings are optional. Select *Verify LDAP settings* to check the LDAP settings entered above.

'Servers' tab



This tab will only be displayed if you have entered a valid ELOenterprise license file.

On the *Servers* tab, enter all computers that you want to run ELOenterprise server applications on. This refers to all applications that require an Apache Tomcat to run and are installed with the ELO Server Setup: ELO Indexserver, ELO iSearch (Elasticsearch), and so on.

Up to ELO ECM Suite 9, the ELOenterprise server setup had to be run every time a separate server application was installed. Since ELO ECM Suite 10, the ELO Server Setup only needs to be run once per server.

If you are running the ELO Server Setup for the first time, enter the configuration data for all computers that you want to run server applications on. During installation, the ELO Server Setup creates a configuration that makes it easier to install the other servers.

Name: Enter the name of a computer that ELOenterprise server applications will be running on. The current computer's name is entered in the first field by default.

IP: Enter the IP address of the computer running ELOenterprise server applications. The current computer's IP address is entered in the first field by default.

> **Information**
>
> See the *Distributed installation of ELOenterprise* section for information on installing ELO server components to multiple servers. The server name and IP address are required to correctly assign different server applications to different computers.

Installation path: Select the path on each computer where you want the ELO server components to be installed. The path specified on the *Repositories* tab is entered in this field by default.

Log path: Select the path where you want to store the log files for the ELO server components installed to each computer. By default, ELO selects the `logs` directory within the installation path.

> **Information**
>
> Log files within this path are also stored within a folder named after the corresponding ELO Server Engine, e. g.: `C:\ELOprofessional\logs\ELO-Server1\ix-Repository.txt`

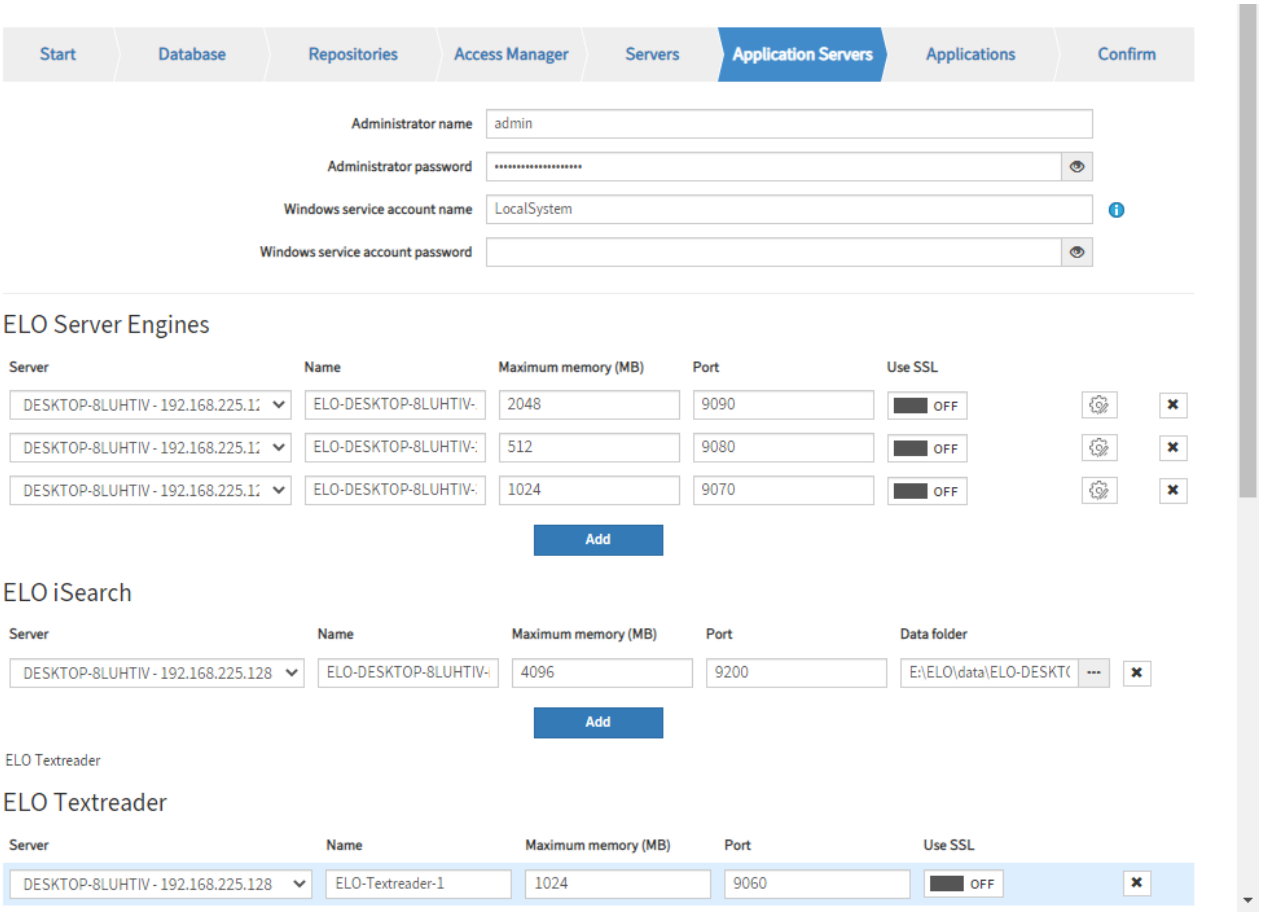
Certificate settings: *Certificate settings* opens a dialog box where you can load and manage SSL certificates for the respective server.

- Generate self signed certificates: If the option *Generate self signed certificates* is set to *ON*, the ELO Server Setup generates a certificate for encryption.

  > **Information**
  >
  > After installation, you will find the certificate file *rootca.pem* under the path `<installation directory>\data\serversetup2`.
  >
  > You need to import the *rootca.pem* file to the client computers so that they can connect to the server.

Add: To create additional fields for other ELO servers, select *Add*. Select the button with the X icon to the right of a field to remove a server from the list.

'Application Servers' tab



The *Application Servers* tab is where you define the number and basic configuration of Apache Tomcat application servers used with ELO. If you are installing ELOenterprise, do not switch to this tab until you have added all servers on the *Servers* tab.

Administrator name: Enter the name for the Apache Tomcat administrator account. *admin* is entered here by default. This account is assigned the Apache Tomcat roles *manager-gui* and *admin-gui*. This setting is applied to all Apache Tomcats installed with the ELO Server Setup.

Administrator password: Enter the password for the Apache Tomcat administrator account. The password is generated randomly by the ELO Server Setup. This setting is applied to all Apache Tomcats installed with the ELO Server Setup.

Windows service account name: The ELO Server Engines require a Windows account to run. The local system account is selected by default, but it is recommended to use a domain account for this purpose as described previously.

If you enter a domain account in this field, you must enter the account name in the format: `DOMAIN\user`.

Please note

The account entered into *Windows service account name* is also required for the following directories/files:

- Folder *lib*: For each Apache Tomcat server. Stored under: `<ELO>\servers\<server name>-1\lib`, for example.
- Folder *webapps*: Stored under `<ELO>\prog\webapps`
- File *jmxremote.password*: Stored under `<ELO>\config\serversetup2\jmxremote.password`

The ELO Server Setup sets the permissions for the account in the appropriate directories. The permissions are passed on to all child entries.

Make sure that the account you are using has the necessary permissions to access directories/files.

Windows service account password: If you entered a domain account in the field above this one, enter the corresponding password here. If you are keeping the local system account, leave the field blank..

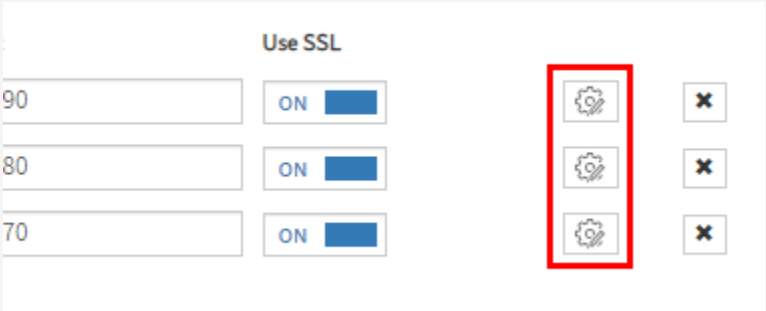
The rest of the page is divided into areas for *ELO Server Engines* (most ELO server applications) and *ELO iSearch*.

ELO Server Engines

By default, the ELO Server Setup installs different ELO components to multiple Apache Tomcat servers to maximize stability and performance. You may reduce the number of Apache Tomcats to a minimum of one or a maximum of one Apache Tomcat server per web application (see *Applications* tab).

Select *Add* to install other ELO Server Engine instances.

Information



For the Apache Tomcat servers, you can specify additional startup options for the JVM on the *Application Servers* tab via a button (gear icon).

Example:

```
-Dhttps.proxyHost=127.0.0.1
-Dhttps.proxyPort=8080
```

Use one line for each setting.

ELO iSearch

ELO uses Elasticsearch technology for the full text search (ELO iSearch), which is integrated in the ELO Indexserver. Older versions of ELO iSearch use the modules ELOis and ELOsx. These modules are not integrated in the ELO Indexserver. See the *ELO iSearch* documentation for more details on how to configure ELO iSearch for your environment.

By default, ELO iSearch is installed to a single additional Apache Tomcat instance.

Please note

As of ELO 21.2, the ELO iSearch port (default: 9200) is secured with TLS/SSL.

You may get a certificate warning the first time you open it in a browser.

Depending on the browser and operating system, you must import the certificate into the certificate store of the browser or operating system.

For example, if you are using Microsoft Edge or Google Chrome on Microsoft Windows, load the *keystore.jks* file from `<ELO>\config\elastic\<ELO iSearch server>\certificates` into the Windows certificate store.

If you are using Mozilla Firefox, add the certificate to the Mozilla Firefox certificate store by ignoring the certificate warning message.

ELO Textreader

ELO Textreader (gen. 2) has been used since ELO 21.4.

It is installed on a separate Apache Tomcat server from ELOix by default

ELO Textreader (gen. 2) replaces the previous ELO Textreader (ELOtr), ELO Preview Converter (ELOpreview), and ELO OCR Service (ELOocr).

Please note

If you are working on a system with multiple installations (e.g. for multiple clients), make sure that the values in the *Name* and *Port* fields are different from those of the other ELO Textreaders.

For more information, refer to the *ELO Textreader (gen. 2)* documentation.

ELO XC

ELO XC is a Windows service that enables you to transfer data from an Exchange server to an ELO repository.

You can add an ELO XC server via the ELO Server Setup if required. Under *ELO XC*, select *Add*.

> **Please note**
>
> You must have a working SSL connection to use ELO XC.

For more information, refer to the *ELO XC* documentation.

ELO Flows worker

ELO Flows presents a new customization platform for ELO.

You can add an ELO Flows worker via the ELO Server Setup if required. Under *ELO Flows Worker*, select *Add*.

> **Please note**
>
> If you are working on a system with multiple installations (e.g. for multiple clients), make sure that the values in the *Name* and *Port* fields are different from those of the other ELO Flows workers.

> **Please note**
>
> If you want to use ELO Spaces, you have to install ELO Flows, as ELO Flows transmits a host of information.

For more information, refer to the *ELO Flows* documentation.

ELO Bot for Microsoft Teams

The ELO Bot is an app that integrates with Microsoft Teams.

You can add a service for ELO Bot for Microsoft Teams via the ELO Server Setup if required. Under *ELO Bot for Microsoft Teams*, select *Add*.

For more information, refer to the *ELO Bot for Microsoft Teams* documentation.

ELO Azure Administration

ELO Azure Administration is an additional service for managing app registrations for Microsoft Azure. Installing the service adds a corresponding area to the ELO Administration Console.

> **Please note**
>
> An app has to be registered in Microsoft Azure and a Microsoft Azure account with administrator rights has to be used to connect to Microsoft Azure.

For more information, refer to the *ELO Azure Administration* documentation.

Settings

You can apply different settings depending on the server/service used. These settings are briefly explained in the following section.

Server: This drop-down menu will only be displayed if you are installing ELOenterprise. The menu only contains one option by default, unless you have added servers on the *Servers* tab. Select a server to install an ELO Server Engine to that computer.

> **Information**
>
> See the *Distributed installation of ELOenterprise* section for tips on installing ELO to multiple computers.

Name: Enter a name for each Apache Tomcat server/service here. ELO provides a standard name that does not usually need to be changed.

The name selected here is used in the following places:

- The name of the service during installation
- The Apache Tomcat directory (`<ELO program directory>\server\<name>`)
- The URLs of the Application Manager page and web application-related sites (e. g. application status pages)

Maximum memory (MB): Select the amount of RAM that each Apache Tomcat/service is allowed to request from the operating system. The memory allocated by default should be sufficient for new ELO repositories. See the *Default server configuration* section in the *ELO server and modules* chapter for more information about memory requirements.

> **Information**
>
> The maximum memory allocated here is assigned under the *Initial memory pool* and *Maximum memory pool* settings for each Apache Tomcat.

Please note

It is recommended to keep the default value of 4096 MB memory assigned to ELO iSearch.

Less memory can affect performance. Experience has shown that going above 4 GB RAM can result in problems.

Port: Select the HTTP connection port that the corresponding Apache Tomcat service will use. You must enter a multiple of 10 here (a number ending with 0).

See the *Default server configuration* section in the chapter *ELO server and modules* for more information about using ports.

If you do not specify a port ending in 0 here, a corresponding error is displayed on the *Confirm* tab.

Information

If you keep the default settings, the Indexserver address will be `http://<server name>:9090/ix-<repository name>/ix`. The client applications use this URL to access the ELO server.

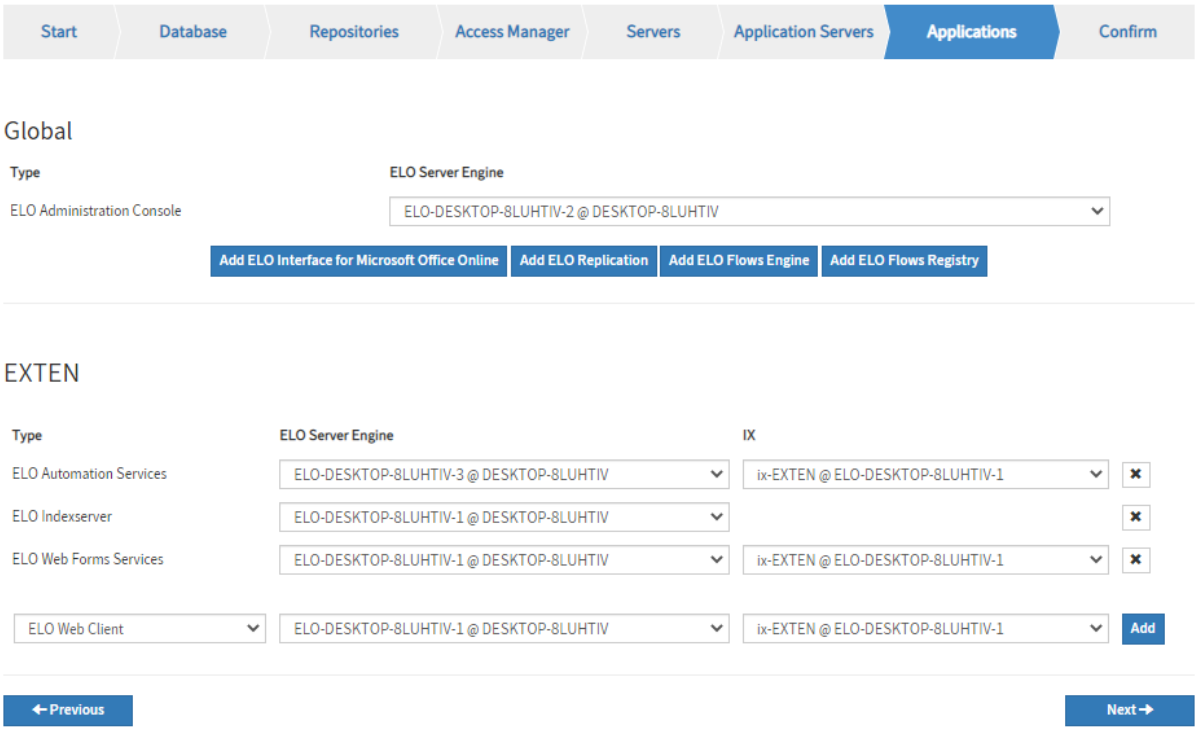
Information

You can check whether a port is open on your computer by entering `netstat -aon | find "<port>"` in the Windows command line. Replace `<port>` with the port number you are currently testing.

Data folder: This field is only displayed for ELO iSearch server engines. Select the directory you want the ELO iSearch server to store data in.

Use SSL: To use an SSL connection for the respective server service, set the option *Use SSL* to *ON*.

'Applications' tab



This tab is where you define the ELO server modules to be installed and the ELO Server Engine and repositories they will be assigned to. The default configuration installs all ELO web applications and assigns them to servers to ensure maximum performance and stability.

> **Important**
>
> Changing the assignment of ELO server modules may affect system performance and functionality. Due to the same-origin policy, some ELO applications need to run on the same server so that they can communicate with each other. As a rule:
>
> The ELO Web Client and the ELO Indexserver must be installed to the same ELO Server Engine. If you have created forms in ELOwf that trigger direct call rules in ELOas, both applications must be installed to the same ELO Server Engine. It is possible to use different ELO Server Engines for these applications if a proxy is set up for them. The *Web Client Internet Access* documentation describes how to accomplish this. If this type of configuration error occurs, error messages directly resulting from it will not be written to the logs!

Global

The *Global* area is where you select the ELO applications that are shared by all repositories.

Add ELO Integration for Microsoft Office Online: Select *Add ELO Integration for Microsoft Office Online* to add the ELO Interface for Microsoft Office Online (ELOimo) interface. The interface enables users to connect a Microsoft Office Online Server to the ELO system.

> **Please note**
>
> To use ELOimo, you need a Microsoft Office Online Server. It cannot connect to Microsoft Office 365.

For more information, refer to the *ELO Interface for Microsoft Office Online* documentation.*

Add ELO Replication: Select *Add ELO Replication* to add the *ELO Replication* module. ELO Replication compares entries between multiple repositories. The relevant repositories can be installed at different locations.

For more information, refer to the *ELO Replication* documentation.

Add ELO Flows Engine: Select *Add ELO Flows Engine* to add the *ELO Flows Engine* module. This module is required for ELO Flows.

> **Please note**
>
> You need an ELO Flows worker. On the *Applications Servers* page, check whether you have set up a corresponding service.

> **Please note**
>
> If you want to use ELO Spaces, you have to install ELO Flows, as ELO Flows transmits a host of information.

For more information, refer to the *ELO Flows* documentation.

Add ELO Flows Registry: Select *Add ELO Flows Registry* to add the *ELO Flows Registry* module. This module is required for ELO Flows.

> **Please note**
>
> You need an ELO Flows worker. On the *Applications Servers* page, check whether you have set up a corresponding service.

Please note

If you want to use ELO Spaces, you have to install ELO Flows, as ELO Flows transmits a host of information.

For more information, refer to the *ELO Flows* documentation.

[Repository]

All other areas on this tab are named after the repositories you are installing. The ELO server applications assigned to each repository are listed within that area.

Type: The name of the ELO application is shown here.

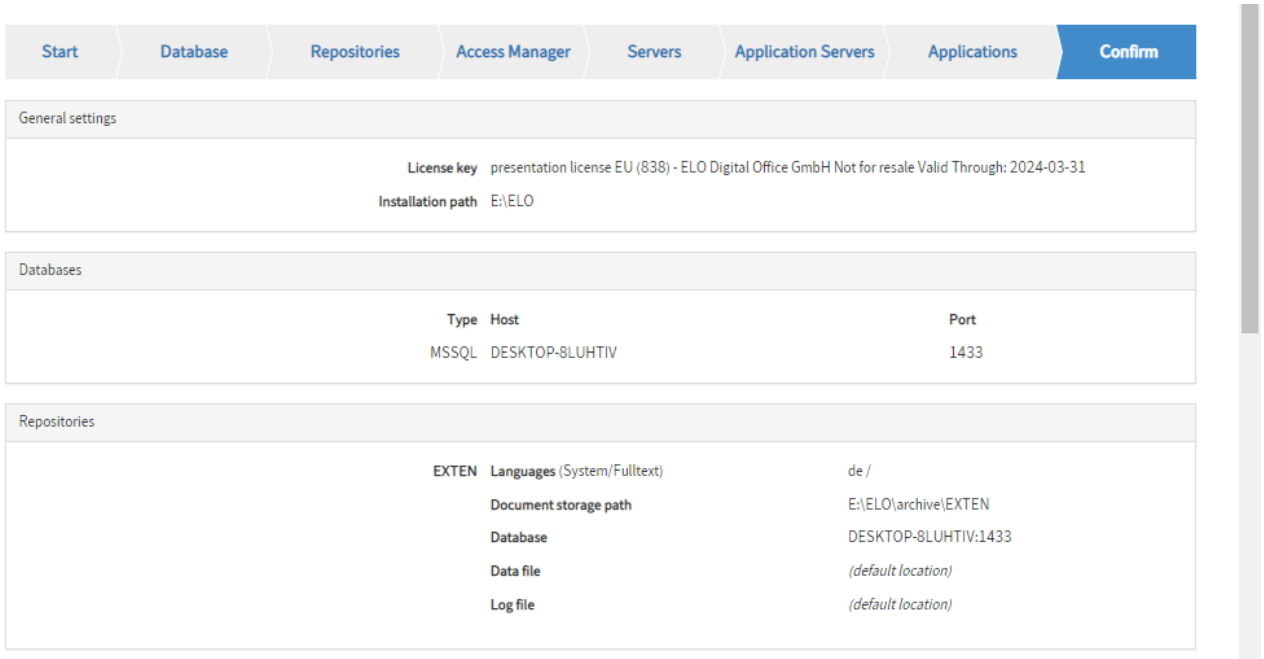
ELO Server Engine: Select an ELO Server Engine from the drop-down menu. These servers are defined on the *Application Servers* tab.

IX: Most of the ELO server applications must communicate with a single ELO Indexserver in order to work. Select the ELO Indexserver you want these applications to communicate with from the drop-down menu. By default, one ELO Indexserver is installed per repository.

Add: Use the last line to add server applications. Select the application from the drop-down menu and select *Add*.

Select the button with the X icon to the right of an application to remove it from the list.

'Confirm' tab



This tab contains the settings for the ELO server after installation. If any errors are found during installation, they are displayed in red in a table at the top of this screen.

Review the settings shown here and make sure they are correct before proceeding.

User names and passwords

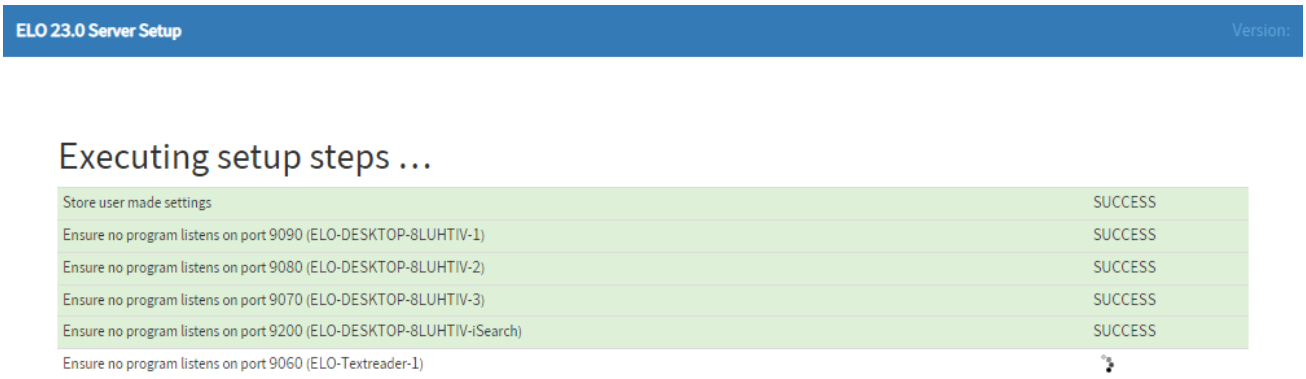
The *User names and passwords* table at the bottom of this tab shows the accounts that will be created when ELO is installed.

Show passwords: *Show passwords* enables you to see and check all passwords. In this mode, you can also print the passwords using the *Print* function (see below).

> **Important**
>
> Make sure that you make a note of the *ELO Service* password and *Apache Tomcat Administrator* password. These are automatically generated by the ELO Server Setup if not configured otherwise.

Print: Use the *Print* button to print the page for your records.

Install: Select *Install* to install the ELO server.



The installation switches to the next screen, which shows the progress of the individual installation steps and any errors.

Finish: When the *Finish* button appears at the bottom of the screen, the installation is complete. Select *Finish* and close the window.

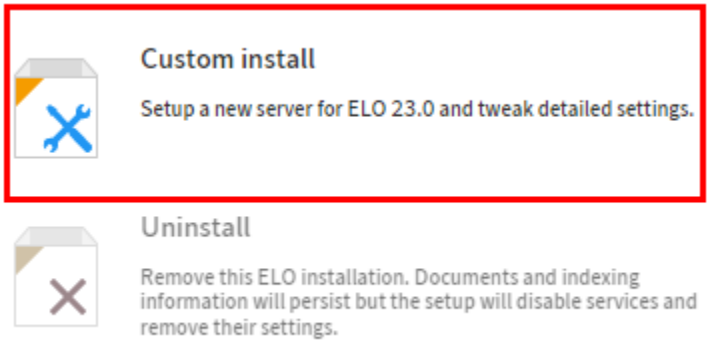
A detailed log of the installation progress is stored in the server setup directory in *serversetup2.log*. Keep this file for your records. It may be required for support requests in the future.

> **Important**
>
> Make sure that this file is kept in a secure location. As it is a detailed log of the installation process, it lists all passwords used (or created) in the installation in plain text.

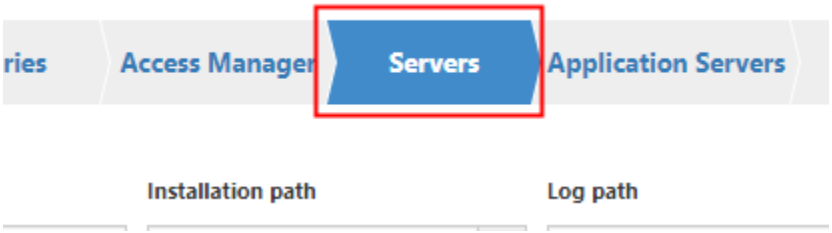
Distributed installation of ELOenterprise

One of the defining features of ELOenterprise is its ability to install server modules to any number of different computers (multi-tenant capability). This section describes how to implement this functionality.

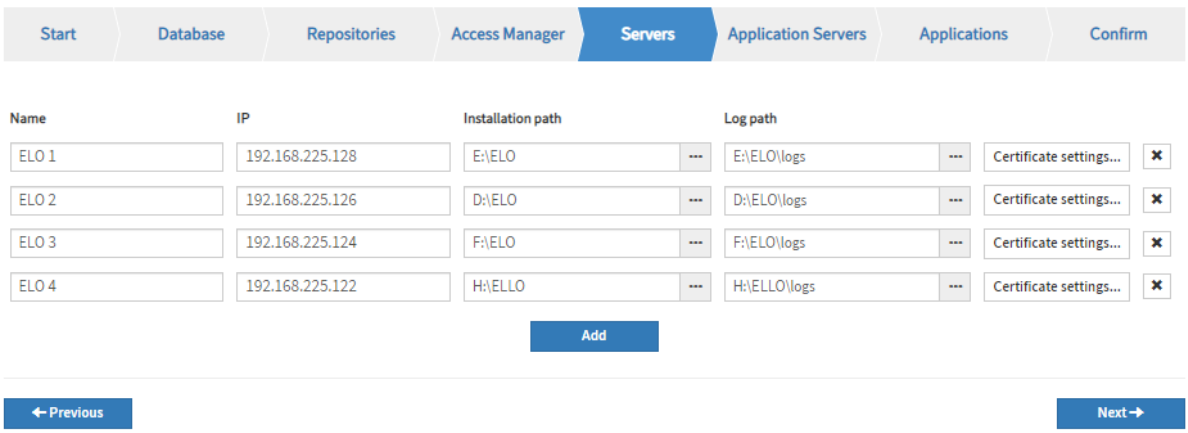
If you are installing all ELOenterprise modules on the same computer, you may skip this section. Otherwise, proceed as follows:



1. On the first screen of the ELO Server Setup, select the option *Custom Install*.

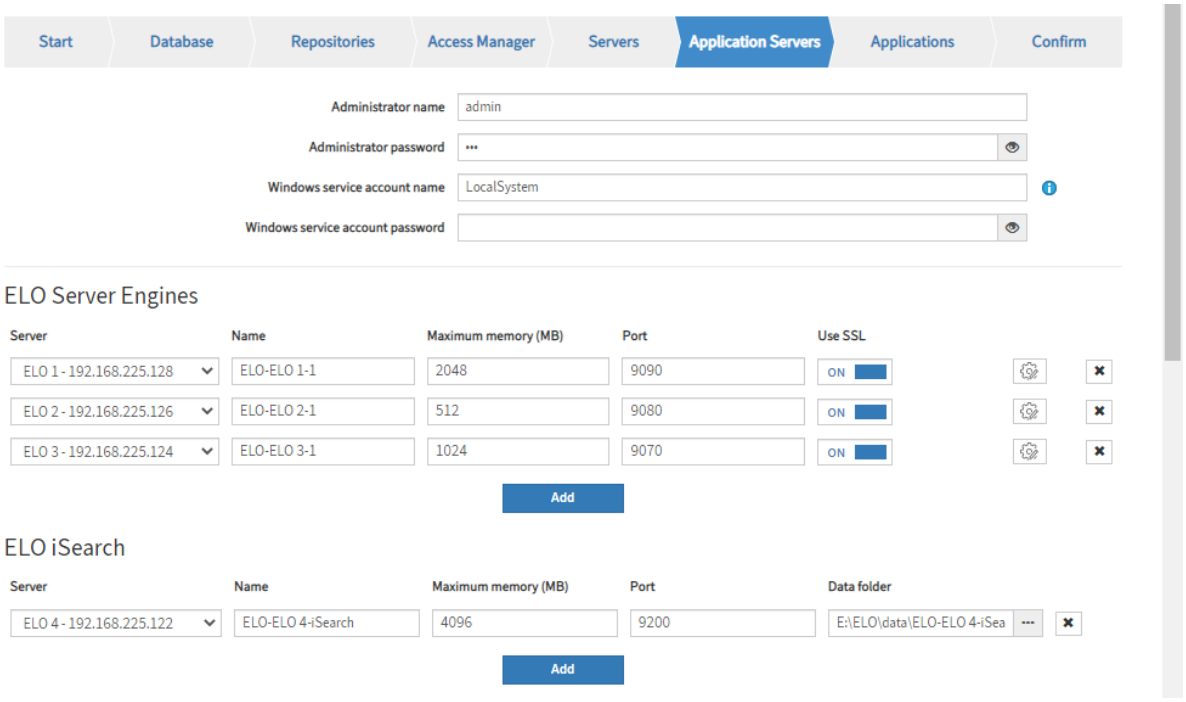


2. Upload a valid license file for ELOenterprise on the *Start* tab. You now have access to the *Servers* tab.

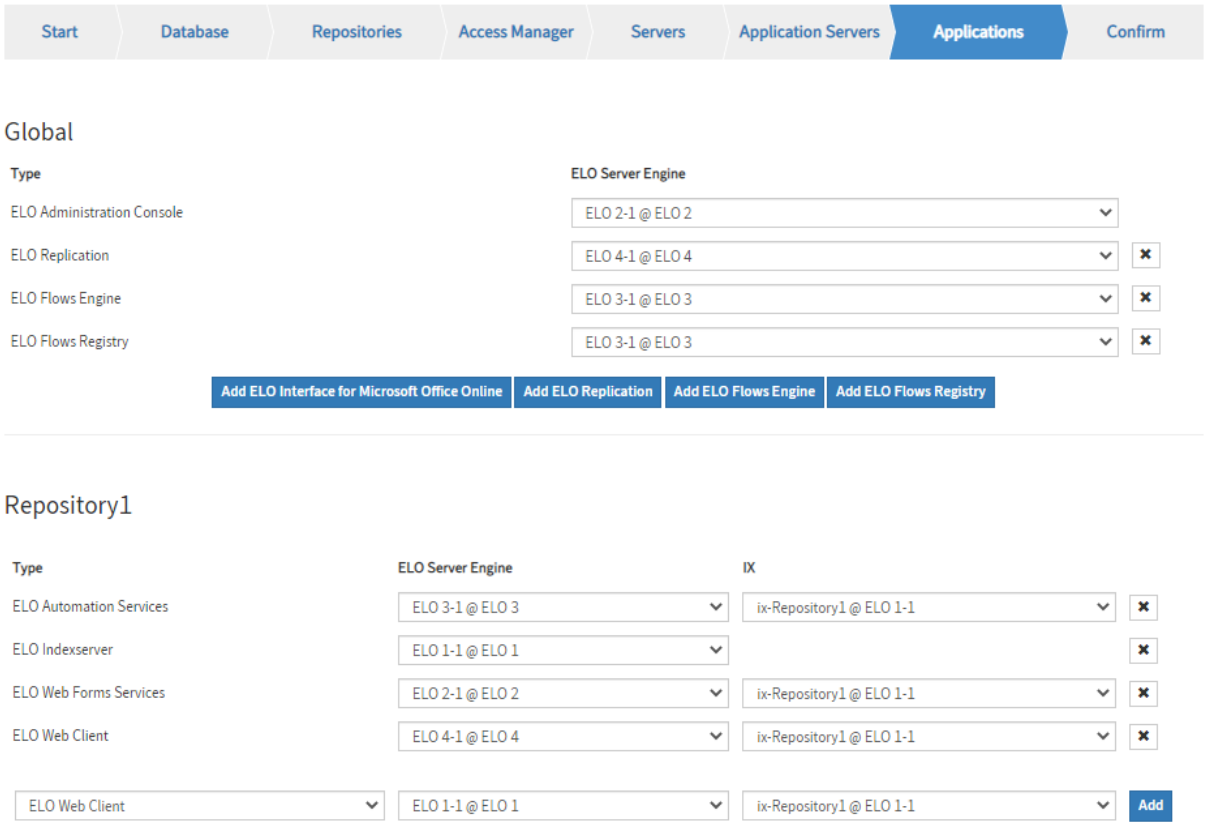


3.

Enter all the required information on the *Repositories*, *Database*, and *Access Manager* tabs. On the *Servers* tab, enter the computer name, IP address, and other data for all computers that ELO components will be installed on.



4. On the *Application Servers* tab, select the computers in the *Server* column that you defined in the previous step.



5. On the *Applications* screen, assign the ELO server modules in the same way as described previously. There are now different computers listed under *ELO Server Engine*.

6. Proceed with the installation. When installation is complete, open a Windows Explorer window and navigate to the following location:

   `C:\Users\<user name>\`

   Replace `<user name>` with the name of the account you are using on the computer.

   This directory contains a hidden file named `.elosetup.conf`. If you do not see it, enable the option to display hidden files in that folder.

   This file is your setup configuration.

   > **Please note**
   >
   > The ELO Server Setup encrypts the file *.elosetup.conf*. It can only be accessed with the main password.

7. Copy `.elosetup.conf` to the corresponding directory on all other computers you are installing ELO server components on.

8.

After you have copied the configuration to the other computers, run the ELO Server Setup on each of these computers. You should not need to enter any configuration settings on these additional servers. After reviewing the settings, install ELO there.

Advanced

Introduction

The installation of the ELO applications is designed to be flexible. ELOenterprise can be installed all on one computer, on a number of virtual computers, or on different physical servers. The simplified setup program for ELOprofessional must be installed to a single computer, but it can also have the database to a separate system for load balancing. To keep this manual as simple as possible, we have not covered all possible configurations. If a custom installation scenario is required, the *config.xml* file for each of the ELO web applications can be adapted to such requirements. However, this requires detailed knowledge of the ELO ECM Suite along with a thorough understanding of the Apache Tomcat Application Server and the structure of the configuration files.

The following sections deal with advanced topics relating to the ELO server.

For example, some sections provide information about useful customizations after the installation.

You will also get information about additional installation types.

Finally, potential issues that may occur during installation are explained.

Server-side adjustments following installation

The following few sections describe some adjustments that may be needed to optimize your ELO server after installing the basic components.

Database connections

Previous versions of ELO allowed you to adjust the number of database connections established by the ELO Access Manager and ELO Document Manager during installation. The default value is currently `50`.

As a rule of thumb, you should set the number of simultaneous database connections for ELOam and ELOdm to between 1 and 3 % of the numbers of users expected to be using ELO at the same time. Note that any value less than three will significantly impact ELO's performance. Increasing the number of database connections will also result in increased static RAM usage, so this setting may need to be adjusted to find the setting that guarantees optimum performance.

> **Information**
>
> The default configuration is therefore sufficient for installations with up to 1600-5000 simultaneous ELO accounts.

You can adjust the number of database connections in the `config.xml` file of each of these modules. These are stored here:

<ELO>\config\<application name>\<server name>\config.xml

Replace `<ELO>`, `<application name>` and `<server name>` with the correct values for your environment.

Textreader/OCR settings

There are several optional settings for the ELO Textreader and OCR that you may need to adjust after installation.

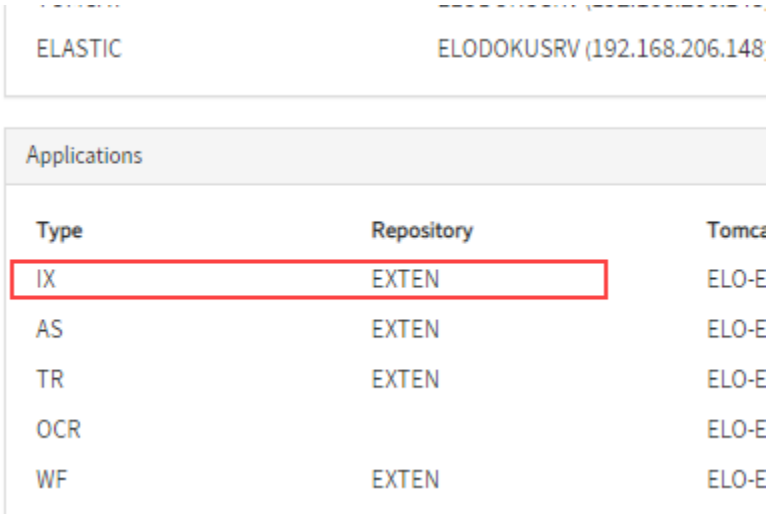
For more information, refer to the *ELO Textreader (gen. 2)* documentation.

Enable external links

The *Create external link* function shares documents in an ELO repository with persons who do not have an ELO account. When the ELO server is first installed, however, these external links only work with computers that are on the same network or domain as the ELO server. To share ELO documents with all computers with an Internet connection, proceed as follows.

1. Assign a fixed IP address to the computer that the ELO server is running on. To access this IP from outside the network, you may need to make additional configuration settings on the network controller or in the firewall. These settings are not described here.

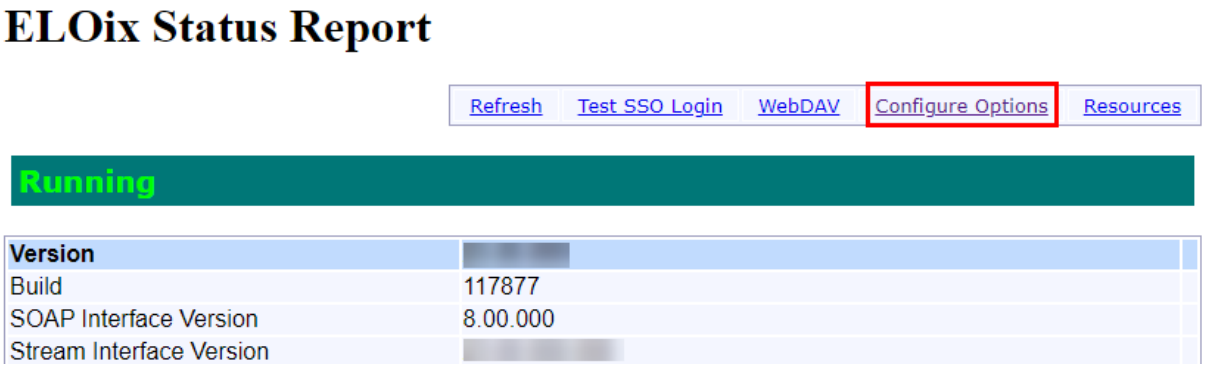
2. Open the ELO Server Manager and select the *ELO Indexserver* entry to open its status page.



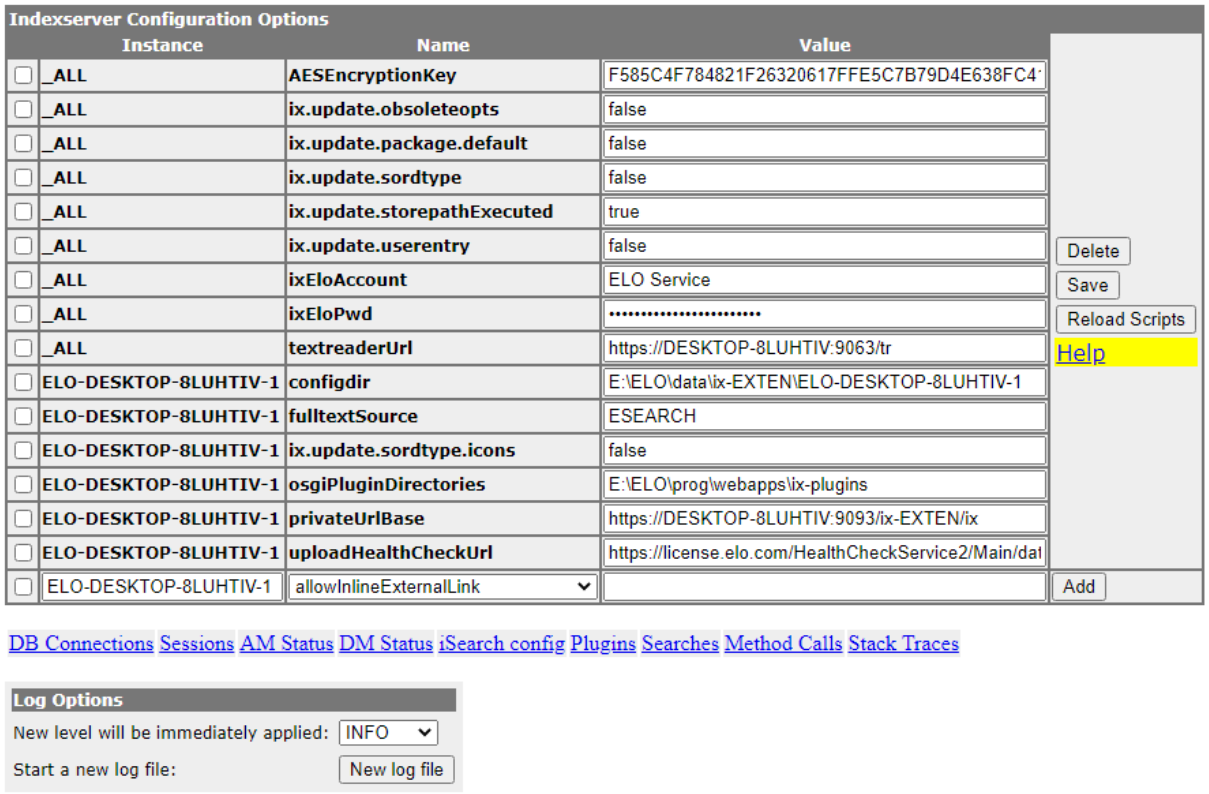
3. Select the *ELO Indexserver* entry to open its status page.

4. Select *Login*.

5. Log on to the ELO Application Server with the administrator account.



6. The ELO Indexserver status page opens in a new tab. Select *Configure Options*.



The *Indexserver Configuration Options* page is displayed.

7. Select the Indexserver option *publicUrlBase* from the drop-down menu at the bottom of the table.

8. Enter the ELO Indexserver URL as follows:

   `http(s)://<fixed server IP>:<port>/ix-<repository name>/ix`

9. Select *Add*.

The setting is applied to the table.

10. Select *Save* and then *Reload Scripts* to save the change and apply it to the server.

    The *Create external link* function now takes users to the correct document.

Important

Exposing a computer to the Internet requires elevated security settings to protect your network from intrusions. Please ensure that the required security measures are in effect before enabling the *Create external link* function.

The value for *publicUrlBase* can also be changed to a website if your network rules have been set to redirect requests to the ELO Indexserver and/or port.

Example of a corresponding external link:

```
https://www.exten.com/extdl?cmd=readdoc1&downloadid=(8F3C3338-748A-DB9C-D2EE-B71A86D67875)&
```

Enabling SSL in the server setup

This documentation explains how you can use X.509 certificates to encrypt HTTP connections in the ELO Server Setup.

The first part of the documentation describes how to generate the certificates required for HTTPS communication. After that, you will learn what settings you need to make in the ELO Server Setup in order to enable HTTPS. The next part describes how you can verify that encryption is working. Finally, you will learn what settings you need to make in the client.

> **Please note**
>
> If you are installing on Microsoft Azure with PostgreSQL, SSL must be configured separately. The ELO Server Setup only works in this context without an existing SSL PostgreSQL JDBC connection.

X.509 certificates

X.509 certificates are required for enabling encrypted HTTP communication between the ELO Java Client and the ELO Indexserver as well as between the ELO server components. These can either be issued by a certificate authority or you can issue your own.

You will need at least:

- Server certificate
- Private key for the server certificate
- Root certificate used to sign the server certificate

The following sections go into detail on each of the above.

Server certificate

The server certificate must be encoded as PEM (file extensions *crt*, *cer*, or *pem*). Certificates stored in any other format or that are placed in a certificate store (e. g. PKCS #12 or Java keystore) cannot be processed.

You can convert CRT/CER or DER certificates to PEM format with OpenSSL.

The certificate must have the *Subject Alternative Name* extension as well as at least one *DNS name* that is associated with the computer on the ELO network requesting the certificate. You can also add *DNS names* to the certificate that do not share the same computer name.

Private key

The same conditions apply for the server certificate's private key, i.e. it must be encoded as PEM; certificates in a certificate store cannot be processed. The file extension for private keys is usually *key*.

Root certificate

The root certificate is used to sign the server certificate. If you want to issue your own root certificate, the format specifications described above (DER or PEM) apply.

You can normally download root certificates from a certificate authority.

Certificate chain

The certificate chain traces the path of a certificate back to the root certificate. There are two situations in which the chain consists of more than the root certificate and the server certificate.

Firstly, some certificate authorities use intermediate certificates to sign third-party certificates. These intermediate certificates are signed with your own root certificate.

Secondly, it is also possible to obtain a *signing certificate* that enables you to sign your own certificates.

In both cases, it is necessary to have all the intermediate certificates required to verify the server certificate all the way to the root certificate.

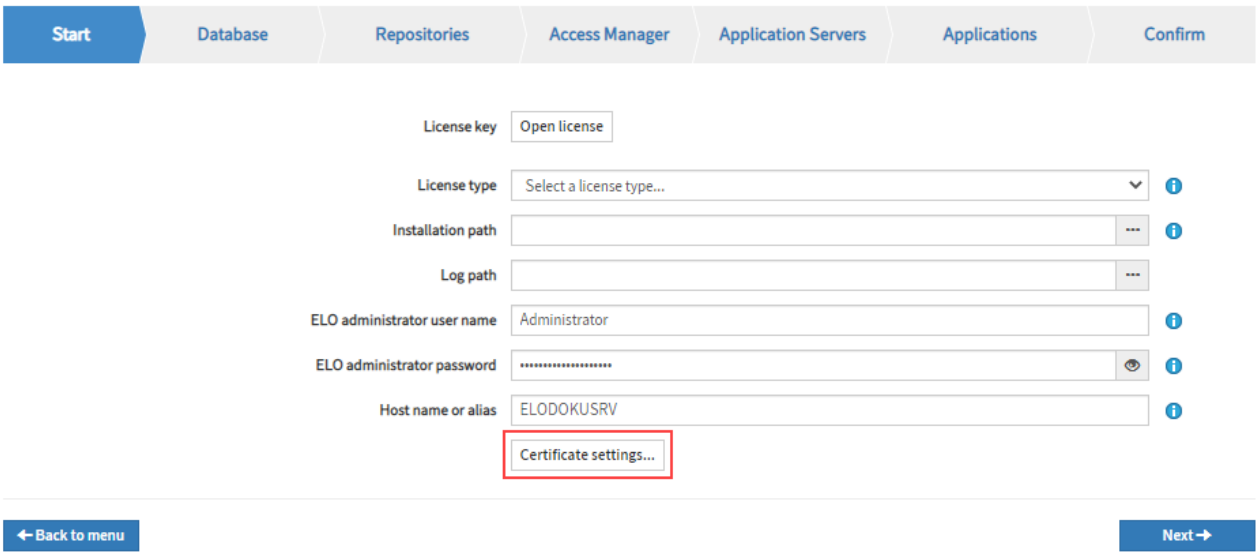
Settings in the ELO Server Setup

Two steps are required to enable HTTPS in the ELO Server Setup. First of all, you need to load the certificate chain and the server certificate's private key to the setup. After this, you need to enable SSL for each application server that you want run encrypted HTTP connections on.

The method for enabling SSL in ELOprofessional and ELOenterprise is identical, but the methods for loading certificates are different.

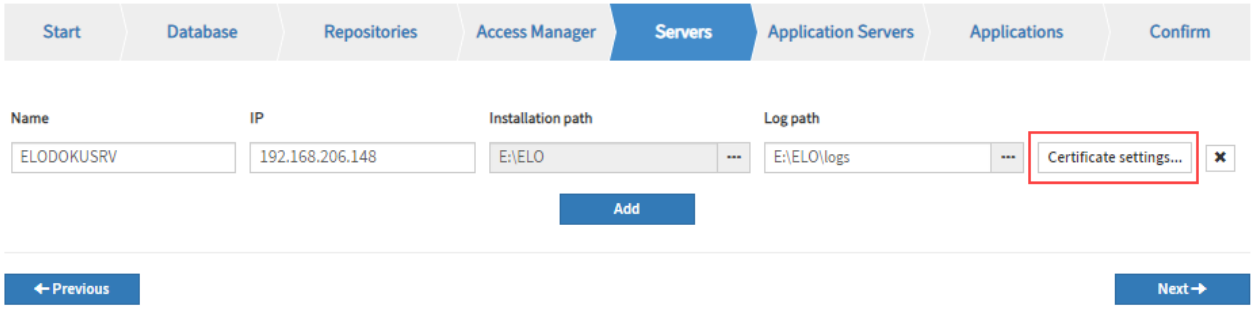
Loading certificates in ELOprofessional

In ELOprofessional, the buttons for loading certificates are located on the *Repositories* page:



Loading certificates in ELOenterprise

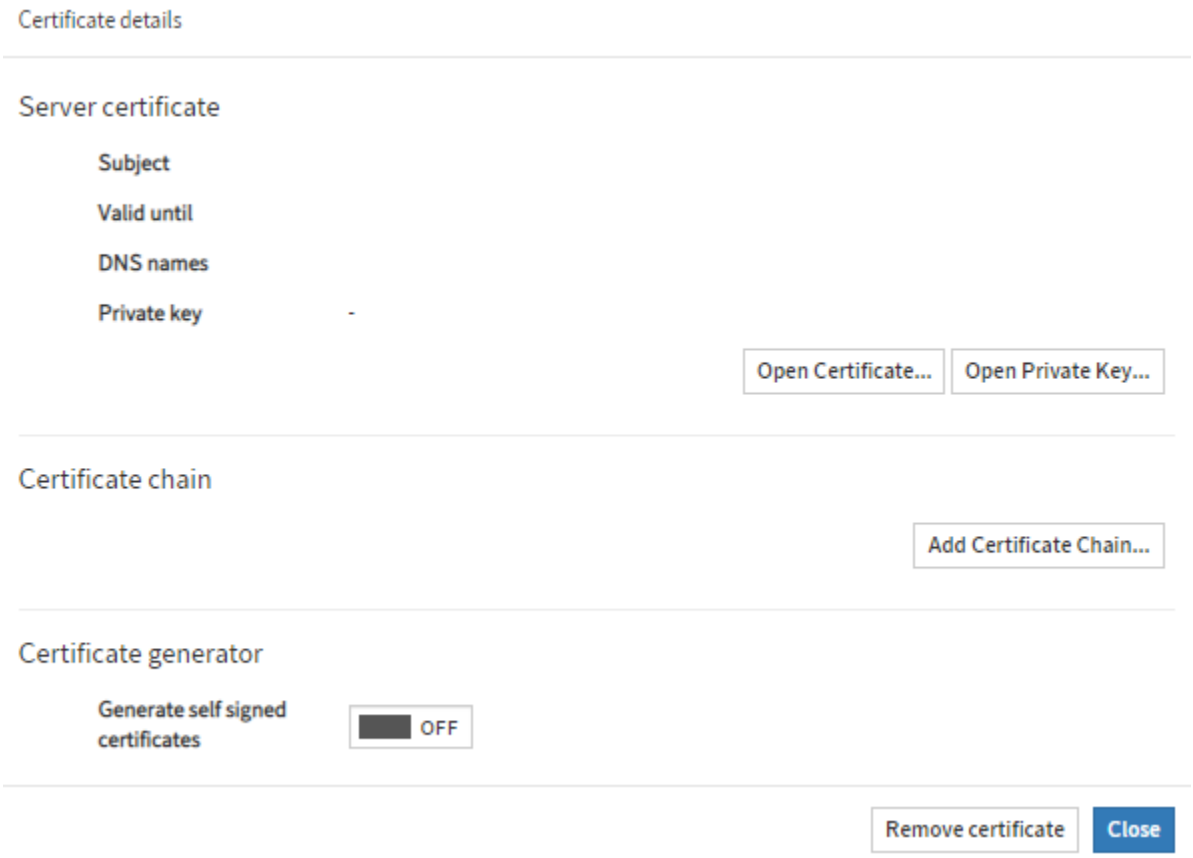
In ELOenterprise, the button for loading certificates are located on the *Servers* page:



You need to upload the certificates for each server that you want to enable encrypted HTTP traffic on. This also applies if you intend to use the same certificate for multiple servers.

Loading certificates

Several steps are required in the dialog box for loading certificates:



Open Certificate: This opens a dialog box for selecting a file for the server certificate. Once you have opened the correct file, the server setup loads and reads the certificate. If successful, the corresponding certificate values will have been entered in *Subject*, *Valid until*, and *DNS Names*.

Open Private Key: This opens a dialog box for selecting a file for the server certificate's private key. Once you have selected the correct file, the server setup loads and reads the private key. If successful, the value for *Private Key* will be set to *Ok*.

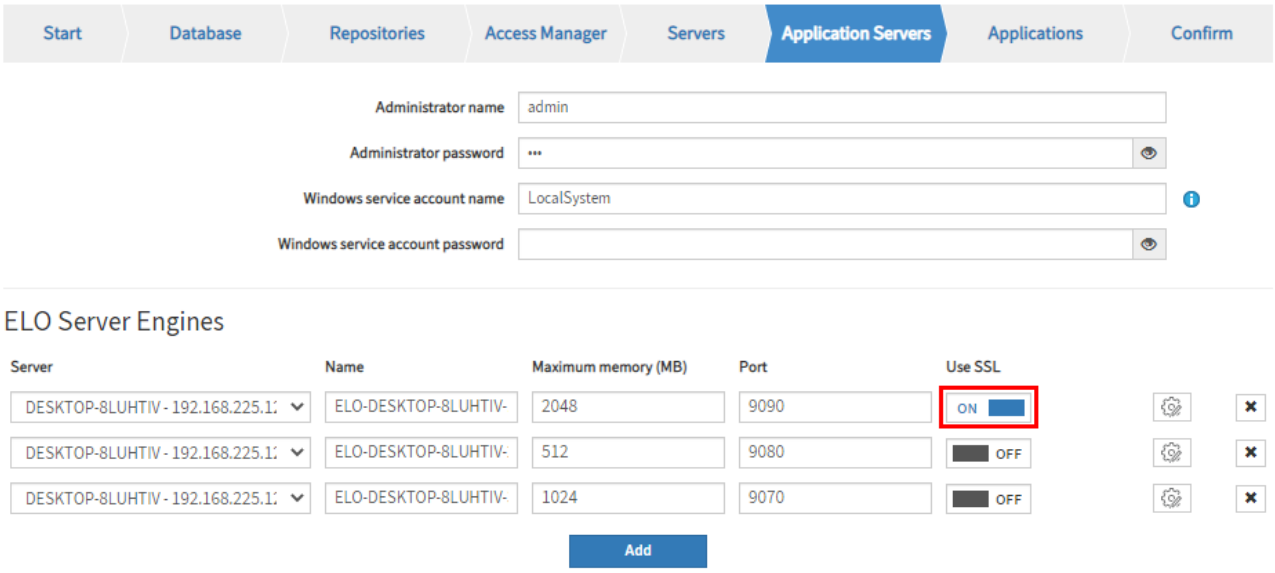
Add Certificate Chain: This also opens a dialog box for selecting a file. This button is used to load each certificate in the certificate chain, including the root certificate, to the setup.

Generate self signed certificates: If the option *Generate self signed certificates* is enabled, the ELO Server Setup automatically generates a self-signed certificate. This certificate can be used to encrypt the ELO server.

> **Please note**
>
> Since the certificate is self-signed, you have to import the certificate into the certificate stores of the server and client systems afterwards.
>
> After installation, you will find the certificate file *rootca.pem* under the path `<installation directory>\data\serversetup2`.
>
> You need to import the *rootca.pem* file to the client computers so that they can connect to the server.
>
> Alternative: Alternatively, you can export the certificate from the Apache Tomcat keystore.
>
> Use a tool such as Portecle for this.
>
> You will find the password for the keystore in the *server.xml* file under:
>
> *<ELO>\servers\<Server>\conf*

Enabling SSL in the Application Server

You can specify which application server you want to use for the encrypted connection. Set the *Use SSL* button on the *Application Servers* page to *On*.



This setting can only be found in the *ELO Server Engines* section. Since version 10.2 of *ELO iSearch*, communication between the ELO iSearch node and the ELO Indexserver is automatically encrypted. The required certificates are automatically generated by the setup during installation.

Firewall

The ELO Server Setup creates a firewall rule that enables the following ports by default:

- 9204
- 9203
- 9200
- 9093
- 9090
- 9083
- 9080
- 9073
- 9070
- 9063
- 9060
- 9043
- 9040
- 9033
- 9030
- 9000

To increase server security, we recommend removing the ports for connection without SSL (9200, 9090, 9080, 9070, 9060, 9040, and 9030) from the firewall rule if SSL authentication is enabled.

Please note

The rule has to be updated every time the ELO Server Setup is run.

Function test

The HTTPS port is automatically generated from the HTTP port+3. One way to check whether encryption is working is to open the ELO Indexserver status page in your browser. The URL could look like this:

```
https://eloserver:9093/ix-repository1/
```

If you see the status page, encryption is working.

Setting in modules and clients

ELO iSearch

As of ELO 21.2, the ELO iSearch port (default: 9200) is secured with TLS/SSL.

You may get a certificate warning the first time you open it in a browser.

Depending on the browser and operating system, you must import the certificate into the certificate store of the browser or operating system.

For example, if you are using Microsoft Edge or Google Chrome on Microsoft Windows, load the *keystore.jks* file from `<ELO>\config\elastic\<ELO iSearch server>\certificates` into the Windows certificate store.

If you are using Mozilla Firefox, add the certificate to the Mozilla Firefox certificate store by ignoring the certificate warning message.

ELO Java Client

You need to modify the URL for the repository profiles in the ELO Java Client so that they refer to the encrypted endpoint of the ELO Indexserver:

```
https://<server>:9093/ix-<repository>/ix
```

Windows

In Windows systems, you need to store self-signed root certificates in the certificate store with the MMC.

Linux

In Linux systems, self-signed root certificates must be imported into Java's truststore.

```
<java>\bin\keytool -import -alias <alias> -keystore <java>\jre\lib\security\cacerts -file c
```

ELO Web Client

The settings for the ELO Web Client are automatically configured in the ELO Server Setup. These can be found at:

```
https://<server>:9093/web-<repository>/
```

Installation in Linux

This chapter briefly describes the installation and operation of an ELO server in Unix-based operating systems.

> **Please note**
>
> This chapter goes into less detail on server administration than the chapter on a Windows-based system. You must have sufficient experience to run a Linux server.

systemd

systemd must be installed to run the ELO ECM Suite server setup.

SQL

An SQL Server must be installed before installing the ELO server.

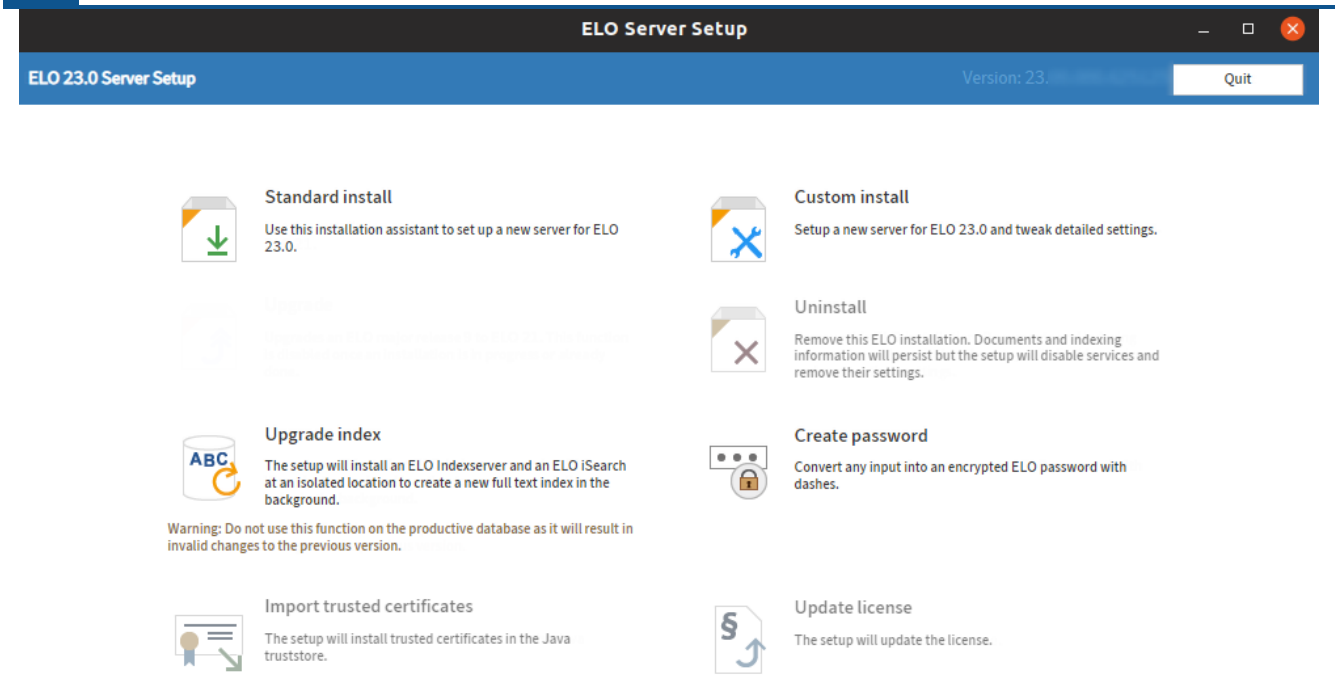
ELO server

Copy the ELO Server Setup file to your server and open a terminal window. Navigate to the location of the ELO Server Setup and run the following commands:

```
chmod +x serversetup2-<version>.sh
sh ./serversetup2-<version>.sh
```

Replace `<version>` with the version number of the setup files you downloaded.

The setup program will start automatically. All processes are logged in the open console window. A browser window opens with the installation menu:



From here, the installation process is similar to the ELO Server Setup in Windows. For information on the various installation options and requirements, refer to the chapters Standard Install, Custom Install, and Distributed installation of ELOenterprise.

Directory rights

After a standard installation, Apache Tomcat runs as a service under the system account and has full access to all local directories. There are several disadvantages to using this account. First, in the event of a security breach in Apache Tomcat, an attacker would gain complete access to all local files. Second, the system account would have restricted access to networked resources like file servers. The Apache Tomcat installation chapter describes the procedure for creating a separate account for Apache Tomcat in Windows. The section below describes how to create this account in Linux and Solaris.

Linux

In Linux, Apache Tomcat should be given its own account with restricted access rights instead of running under the *root* account. Linux generally includes Apache Tomcat and configures it with the appropriate access rights.

When using Solaris, it may be necessary to create a start script under `/etc/init.d` which sets the account for Apache Tomcat. It is also necessary to set an appropriate owner for the Apache Tomcat directory.

The ELOenterprise installation is performed using the *root* account and the ownership of file and repository directories (including child directories and files) is normally set during the installation of an application. If this is not done, certain applications like the ELO Access Manager will be unable to write or create files due to insufficient access rights. This means that the configuration must be carried out manually. This applies to the following directories:

- Data directory (default value: ELOenterprise/data)
- Repository directory (default value: ELOenterprise/archive)

When installing to Linux, the setup program informs you at the end of the installation process about the ownership of the directories if they have not been correctly configured. This is the data directory for the ELO Access Manager, ELO Indexserver, and ELO XML Importer, and the repository directory for the ELO Document Manager.

Example

In SUSE, the name of the Apache Tomcat account is *tomcat* (see file `/etc/init.d/tomcat`). There is also a group with the same name. Within the ELOenterprise directory, the commands are as follows:

- For the data directory: `chown -R tomcat:tomcat data`
- For the repository directory: `chown -R tomcat:tomcat archive`

Unattended installation

This document describes how to perform an unattended ELOprofessional or ELOenterprise server installation based on a configuration file. It also describes the available installation options.

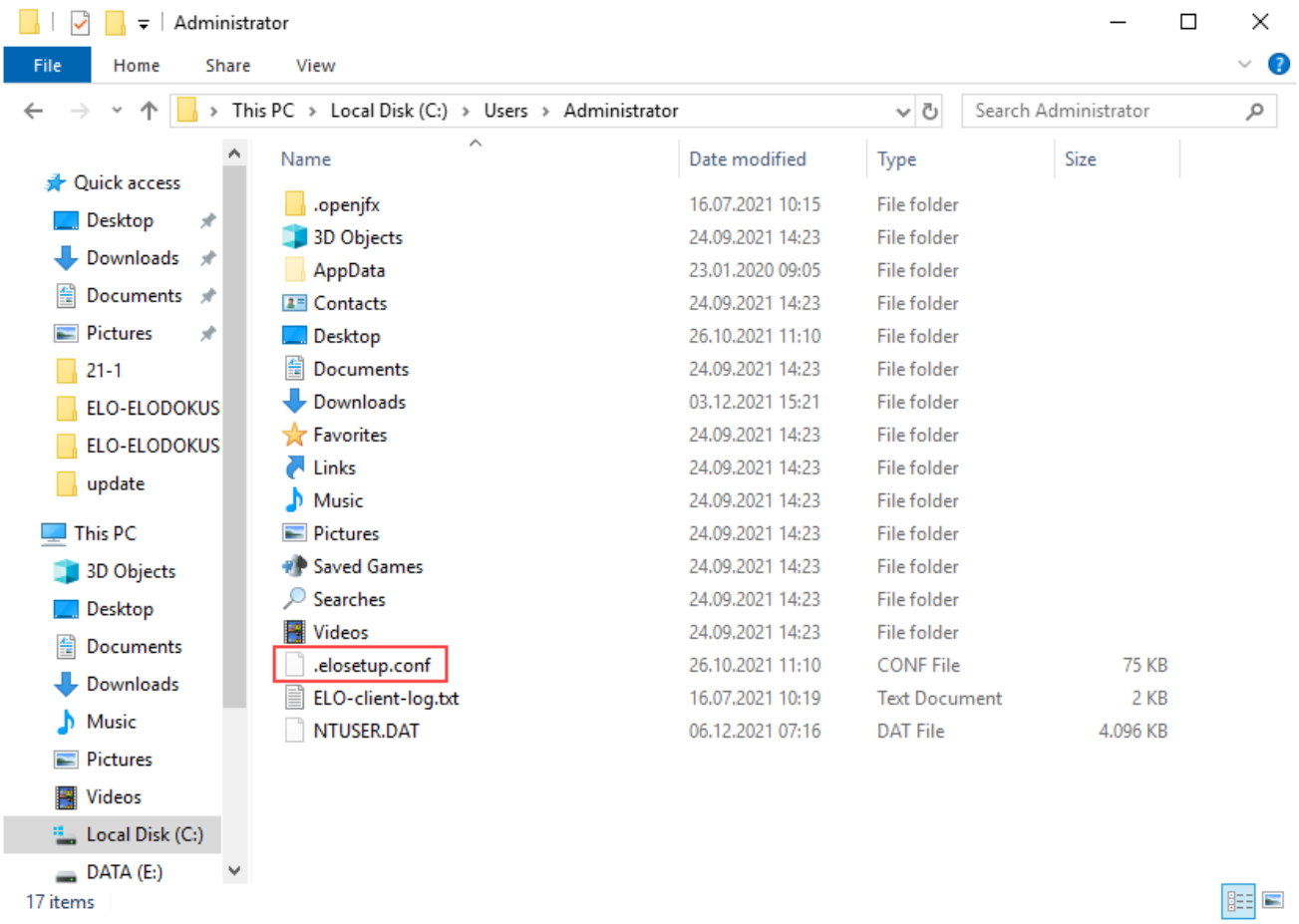
> **Information**
>
> The information provided here only applies to ELO server versions 10.1 and later.

Setup configuration files

Starting with version 10, the ELO Server Setup creates setup configuration files during execution (*elosetup.conf* and *.elosetup.conf*) that automatically store all entries. When you run the server setup again, you do not have to re-enter the configuration details. When updating to a future version, the setup configuration files also store all information required to perform the update.

These setup configuration files can also be used to perform an unattended server installation or to roll out ELO servers to multiple computers. You can find the setup configuration files using the methods described below.

Windows




```
%HOMEPATH%\.elosetup.conf
```

> **Information**
>
> You must unhide hidden files in order to see this file in Windows Explorer.

Linux

```
${HOME}/.elosetup.conf
```

Alternative

Windows:

```
<installation path>\config\serversetup2\elosetup.conf
```

Linux:

```
<installation path>/config/serversetup2/elosetup.conf
```

Format

The *.elosetup.conf* file contains configuration data in JSON format:

```
"eloServiceUser": {
    "name": {
      "value": "ELO Service"
    },
    "password": {
      "value": "52-247-139-10-8-11-59-34"
    }
  },
```

Adjusting the configuration file

Before you perform an unattended installation, you need to edit the configuration file according to the requirements at hand.

Decrypt file

Starting with ELO 21.1, the ELO Server Setup encrypts the configuration files (*.elosetup.conf* or *elosetup.conf*).

To decrypt the files, refer to the documentation Decrypting the setup configuration.

Edit file

After you have decrypted the file, you can edit it.

> **Please note**
>
> Do not leave the copy permanently decrypted. Once you have completed the setup with the required changes, encrypt the file again with the ELO Server Setup.

This documentation does not describe all possible settings in the file or how to create it from scratch. It is best to run the ELO Server Setup once to create a sample configuration, then modify it for your needs.

When making adjustments to this file, please make sure that the used syntax is correct. Typos or other errors can cause unexpected behavior or, if the file cannot be interpreted by the ELO Server Setup, cause the setup to immediately close.

Potential error sources

The biggest source of potential problems is that the backslash \ character is interpreted as an escape character. If you need a literal backslash, such as in the ELO license key or in a path, you must enter one backslash. A network path will therefore require three backslashes.

Another potential source of problems is the text editor used to edit the configuration file. Use a text editor like Notepad or Notepad++. Do not use Microsoft Word or another similar word processor for this task.

In some cases, a path is entered at multiple places within the configuration file. Please make sure that if you change the path in one place, it is changed in exactly the same way elsewhere in the configuration.

Required adjustments

Parameters that must be changed for a custom installation file are:

```
hostInfo.hostList[.].name.value
hostInfo.hostList[.].ip.value
```

Passwords

Passwords can be entered directly to the configuration file in plaintext. However, passwords entered in this way to the file will not be encrypted during server installation. For this reason, it is recommended to enter the password via the ELO Server Setup. The ELO Server Setup encrypts all passwords entered in the setup interface (with the exception of the configuration in the *elasticsearch.yml* file for the ELO iSearch).

Alternatively, you can encrypt passwords after installation with the ELO Administration Console. Use the *Create password* menu item for this.

After editing

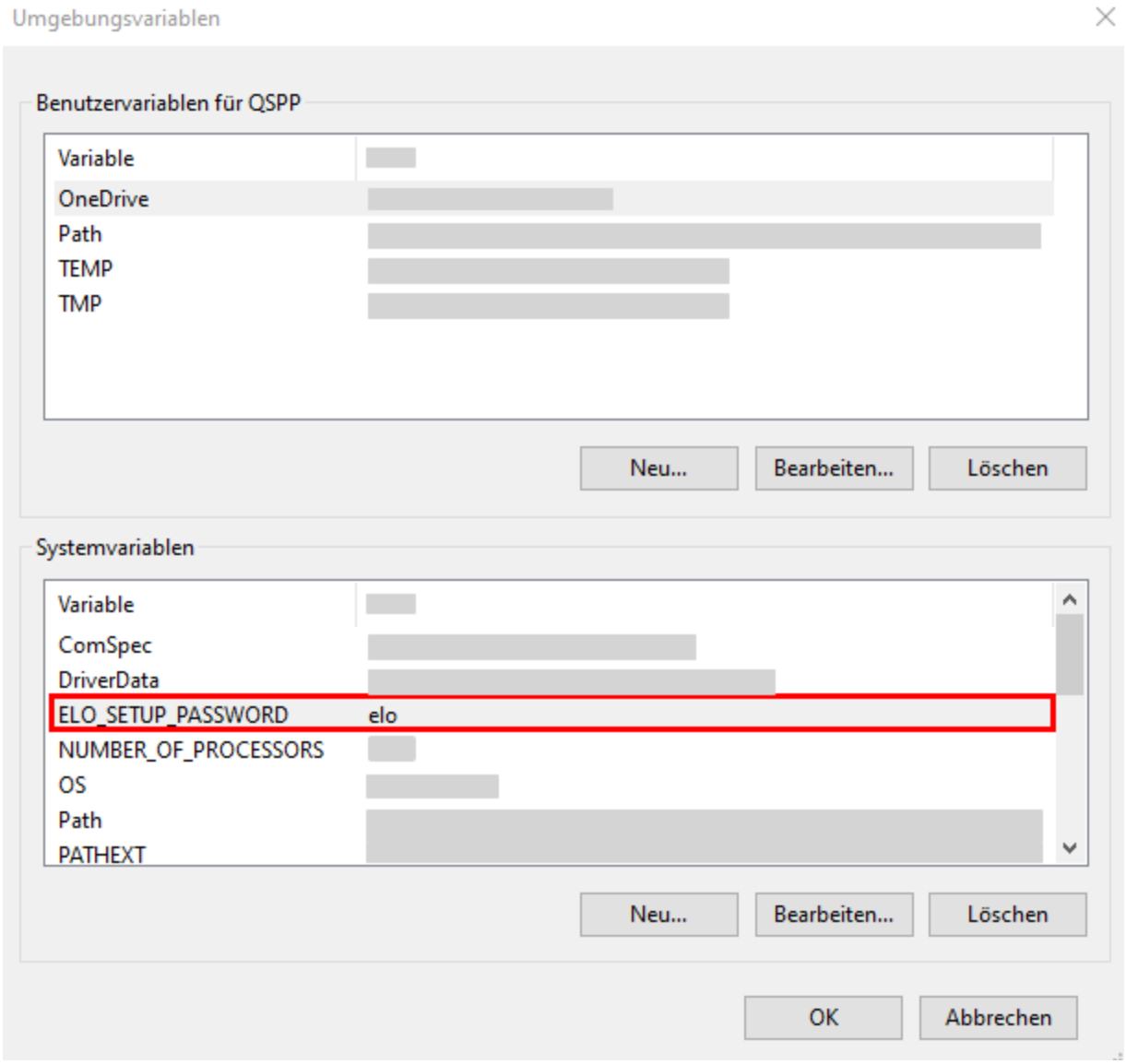
Once you have finished editing the file, you can use it for the ELO setup.

When performing the unattended installation, make sure that you specify the edited configuration file using the parameter `/f`.

This file will be encrypted when you run the ELO Server Setup. Read the following sections.

Store main password in 'ELO_SETUP_PASSWORD'

With the standard settings, because the *.elosetup.conf* and *elosetup.conf* configuration files are encrypted, you will need to enter the main password.



- Store the main password in the *ELO_SETUP_PASSWORD* environment variable to run the installation without a password request.

Command line parameters

The ELO Server Setup supports the following parameters: The syntax is as follows (the items in brackets are optional – if you use these parameters, enter them without brackets):

```
serversetup-version.exe [/S] /f=<configfile> [/D=<temppath>]
```

Windows

```
/S
```

Optional. Silent installation. The ELO server is installed while opening virtually no windows visible to the user.

```
/f=<configfile>
```

Specifying a configuration file triggers an unattended installation.

> **Please note**
>
> This path must be entered as an absolute path.

```
/D=<temppath>
```

Optional. Specify a temporary path to control where temporary installation files are extracted during installation. By default, this path is:

```
C:\temp\ELO Server Setup\
```

If this parameter is used, the argument must be entered as the last parameter in the command.

Linux

```
serversetup-version.sh –f <configfile>
```

Specifying a configuration file in `<configfile>` triggers an unattended installation.

Performing a minimal installation

The ELO Server Setup executable (serversetup-version.exe/.sh) consists mainly of a self-extracting executable. This means that when serversetup-version.exe is run on Windows or serversetup-version.sh is run on Linux, the files are initially extracted to a temporary directory, which contains the actual server installation script. The actual installation is then performed from the temporary directory.

If you want to skip this installation step, you can avoid it by copying the following directory to the target system:

```
<temppath>\ELO\prog\serversetup2
```

You can then perform the installation by running setup.bat or setup.sh along with the `-f` parameter as described above.

You also have to copy the following directory to the target system:

```
<temppath>\ELO\java
```

Only then does the installation folder contain the following folders and files:

- libs
- repository
- java
- setup.bat or setup.sh

Though this installation mode requires more work at the start, it provides significant opportunities for customization. For example, before installation you can remove modules from the *repository* directory that will not be needed on the target system.

Replace SSL certificate

Certificates have a limited lifetime and must be replaced when they expire.

With an unattended installation, you can set up a mechanism that automatically replaces SSL certificates.

Windows

Use the following command in Windows:

```
setup.bat -f <setup.conf> -a CERTIFICATE --certificate <certificate.pem> --privatekey <key.
```

Linux

Use the following command in Linux:

```
./setup.sh -f <setup.conf> -a CERTIFICATE --certificate <certificate.pem> --privatekey <key
```

Decrypting the setup configuration

The ELO Server Setup settings are stored in the *elosetup.conf* and *.elosetup.conf* files (also referred to here as *setup configuration files*). Since ELO 21.1, the ELO Server Setup encrypts these files.

The following steps show you how to decrypt the files. This can be useful if you need the files for a support incident or if you have to change something manually in the files.

Storage location

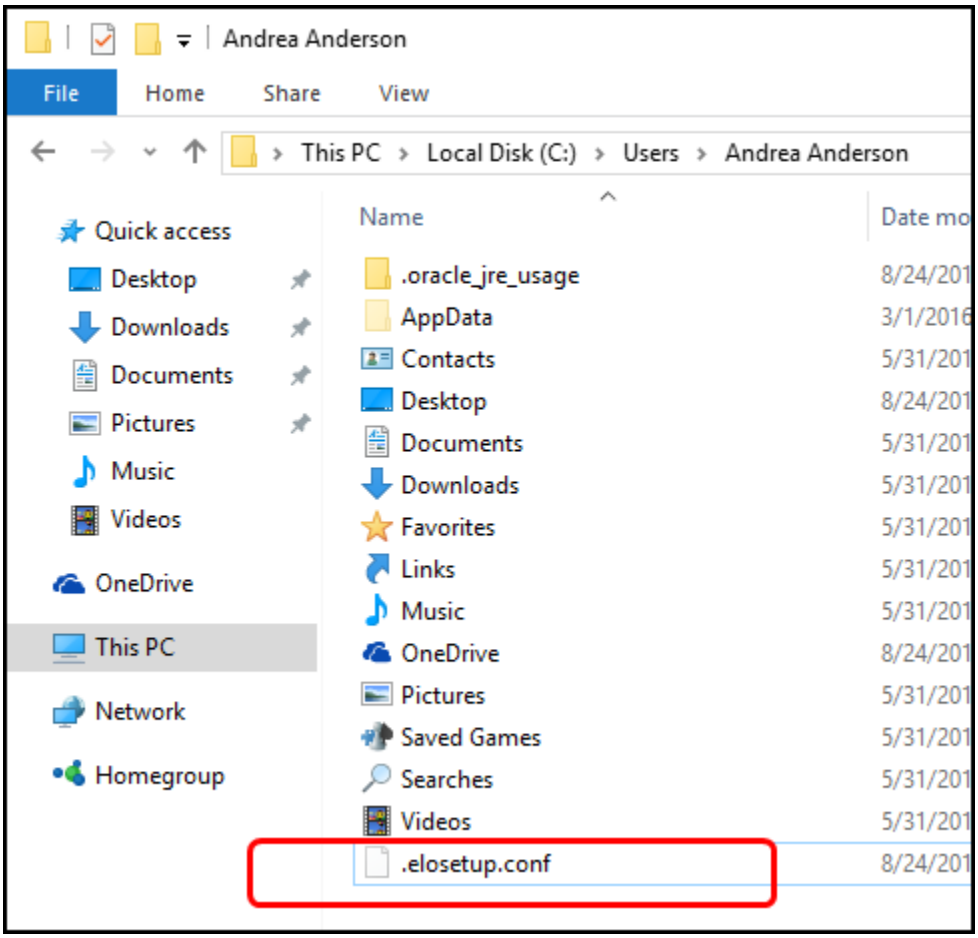
The files are stored under similar paths in Windows and Linux.

Windows

In Windows, the files are stored under the following paths:

> **Information**
>
> You must unhide hidden files in order to see this file in Windows Explorer.

.elosetup.conf




```
%HOMEPATH%\.elosetup.conf
```

elosetup.conf

```
<installation path>\config\serversetup2\elosetup.conf
```

Linux

In Linux, the files are stored under the following paths:

.elosetup.conf

```
${HOME}/.elosetup.conf
```

elosetup.conf

```
<installation path>/config/serversetup2/elosetup.conf
```

Decrypt

The decryption process differs depending on your system.

Windows

1. Navigate to the `<installation path>\prog\serversetup2\` directory on the ELO server.
2. Open the command line in this folder.
3. Use the following command:

   ```
   setup.bat -f <path\to\an\elosetup.conf> -a COPY -c decrypted.conf
   ```

   Example for elosetup.conf:

   ```
   setup.bat -f E:\ELO\config\serversetup2\elosetup.conf -a COPY -c decrypted.conf
   ```

   Example for .elosetup.conf:

   ```
   setup.bat -f C:\Users\Byte\.elosetup.conf -a COPY -c decrypted.conf
   ```

   > **Information**
   >
   > You can choose a target directory and a different target file name (here: *decrypted.conf*) if required.
   >
   > Example with a different path:
   >
   > ```
   > setup.bat -f E:\ELO\config\serversetup2\elosetup.conf -a COPY -c E:\config-file
   > ```
   >
   > If you don't select a target directory, the ELO Server Setup automatically uses the directory of the *setup.bat* file.

   After executing the command, the ELO Server Setup is started in the command line. This may take a few moments.

   You will be asked for the main password.

4. Enter the main password.
5.

Press the ENTER key to confirm.

The ELO Server Setup creates a decrypted copy of the configuration file.

Linux

1. Navigate to the ELO installation directory.
2. Open the terminal in this folder.
3. Use the following command:

```
./setup.sh -f <path/to/elosetup.conf> -a COPY -c decrypted.conf
```

Example:

```
./setup.sh -f /ELO/config/serversetup2/elosetup.conf -a COPY -c decrypted.conf
```

Alternative: Use the file *serversetup2.sh*:

```
./serversetup2.sh -f <path/to/elosetup.conf> -a COPY -c decrypted.conf
```

Example:

```
./serversetup2.sh -f /ELO/config/serversetup2/elosetup.conf -a COPY -c decrypted.conf
```

> **Information**
>
> You can choose a target directory and a different target file name (here: *decrypted.conf*) if required.
>
> Example with a different path:
>
> ```
> ./setup.sh -f /ELO/config/serversetup2/elosetup.conf -a COPY -c /config-files/m
> ```
>
> If you don't select a target directory, the ELO Server Setup automatically uses the directory of the executed setup file.

After executing the command, the ELO Server Setup is started in the terminal. This may take a few moments.

You will be asked for the main password.

4. Enter the main password.
5.

Press the ENTER key to confirm.

The ELO Server Setup creates a decrypted copy of the configuration file.

After decryption

After you have decrypted one of the files, you can use it for a support incident or edit it.

> **Please note**
>
> Do not leave the copy permanently decrypted. Delete decrypted copies as soon as you no longer need them.

Re-encrypt modified files

If you have made manual changes to any of the configuration files, follow these steps.

1. Navigate to the home directory of the person who most recently ran the setup.
2. Save the *.elosetup.conf* file.
3. Move the *.elosetup.conf* file to another directory.

   Alternative: Rename the file.
4. Copy the decrypted and modified setup configuration file to the home directory.
5. Rename the file to *.elosetup.conf*.
6. Run the ELO Server Setup.

   During the setup, you must re-enter the main password. The ELO Server Setup then encrypts the setup configuration files.
7. When the ELO Server Setup is complete, delete any copies of the decrypted setup configuration files that are no longer needed.

Managed Service Account (MSA)

Managed Service Accounts (MSA) are required in some environments to securely run service accounts.

If you want to run ELO with MSA, follow the steps below.

Setting up MSA

1. Start the *Active Directory module for Windows PowerShell* on the domain controller (DC) with administrator rights.

   > **Please note**
   >
   > The commands below refer to the environment used for this example. In this case, the host name of the ELO server is *VMQSPPSRV07*.
   >
   > Change the commands according to the respective installation.

2. Run the following PowerShell command:

   ```
   Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
   ```

3. Run the following PowerShell command:

   ```
   New-ADServiceAccount -Name ELOMSA -DNSHostName VMQSPPSRV07 -PrincipalsAllowedToRetriev
   ```

4. Run the following PowerShell command:

   ```
   Add-ADComputerServiceAccount -identity VMQSPPSRV07 -ServiceAccount ELOMSA
   ```

5. Run the following PowerShell command:

   ```
   Get-ADServiceAccount -Filter *
   ```

6. Switch to the ELO server.

   > **Information**
   >
   > In this example, the DC is also the ELO server.

7. On the ELO server, run the following PowerShell command in the Active Directory module for Windows PowerShell:

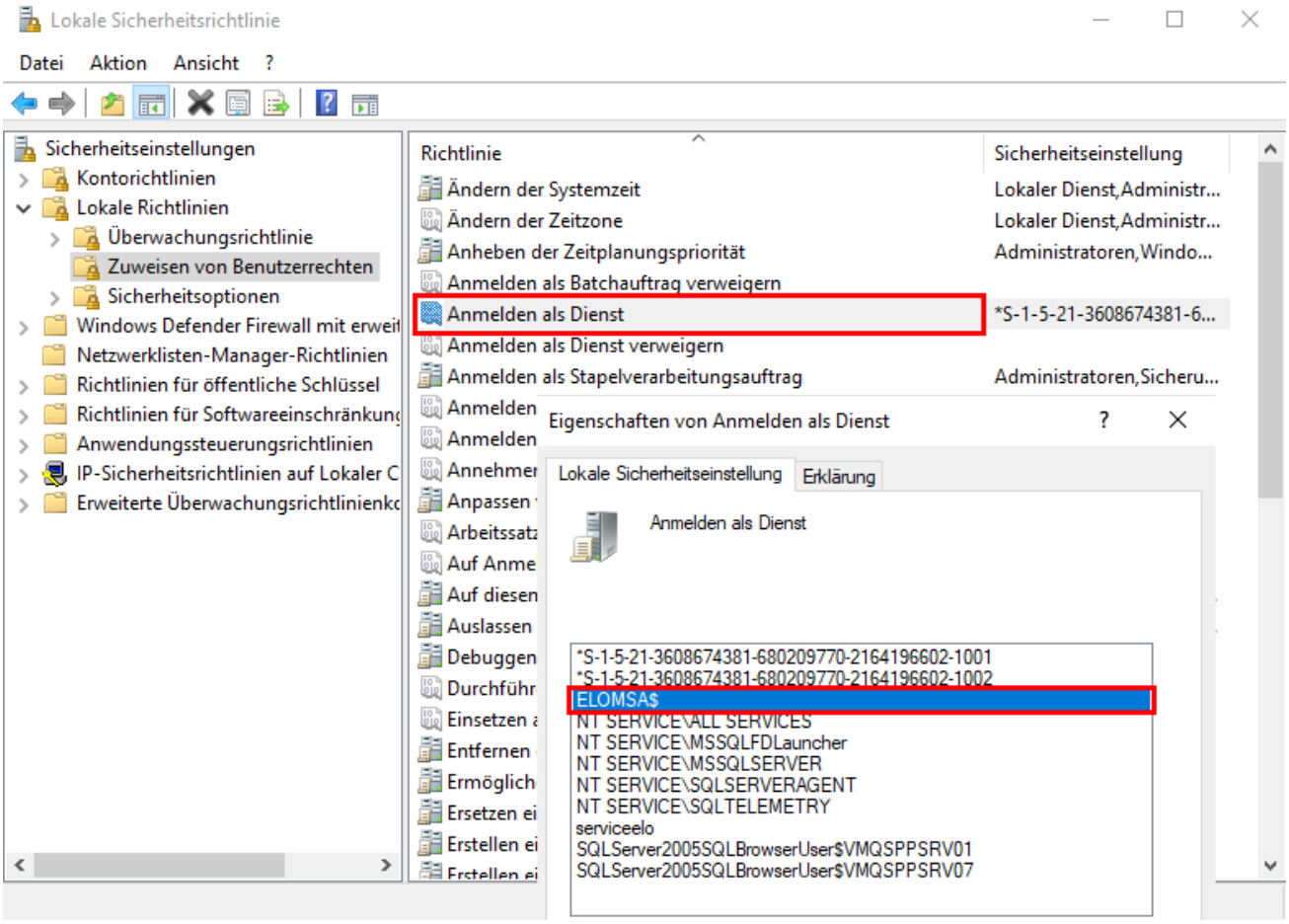
```
Install-ADServiceAccount -Identity ELOMSA
```

Information

If the Active Directory module for Windows PowerShell is not installed on the ELO server, you can install it with the following PowerShell command:

```
Add-WindowsFeature RSAT-AD-PowerShell
```

Log on as a service



Grant the MSA the *Log on as a service* permission.

Administrator rights

The *ELOMSA$* MSA does not have local administrator rights on the ELO server.

Installation with MSA

Currently, it is not possible to install ELO with an MSA or GSMA (Group managed service account).

First, install ELO with a domain account that is not an MSA or with the *LocalSystem* account.

Then you need to change the system to run with the MSA.

Switching to MSA post-installation

Switch the ELO services to run with a different account using the Microsoft Windows *Services* application.

Step-by-step instructions

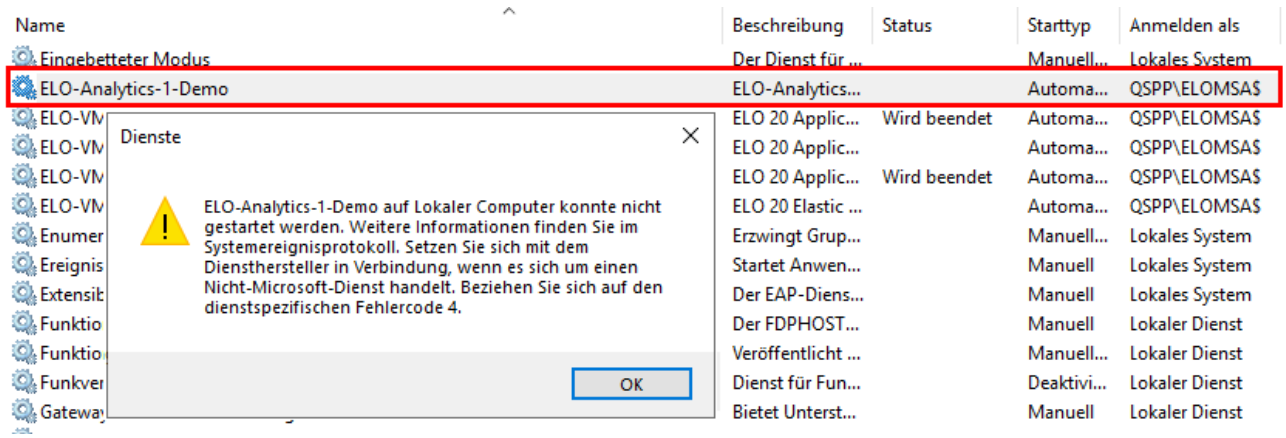
1. Open the *Services* application.
2. Open the context menu for the respective service.
3. Select *Properties*.
4. Select *Log on*.
5. Enable the *This account* option.
6. Enter the MSA.
7. Select *OK*.

Follow-up steps

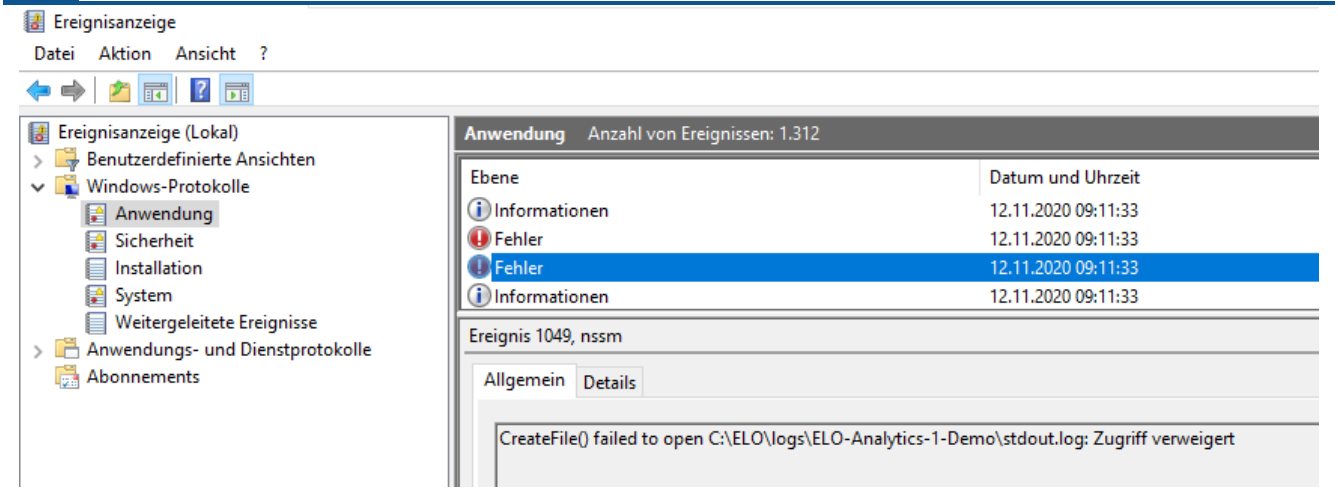
After you have completed the steps above, you need to make some additional changes.

Access to the ELO program directory

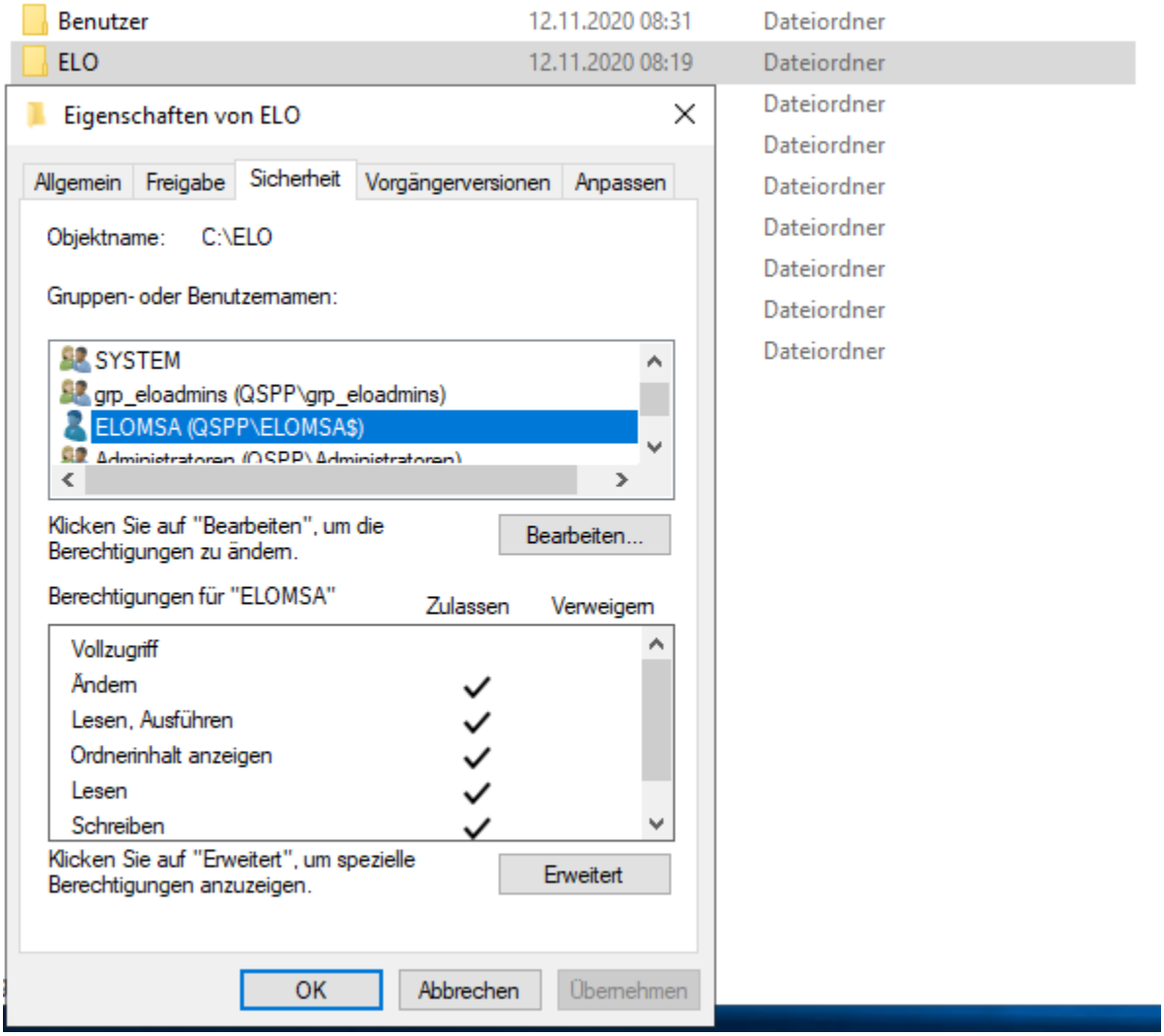
The MSA requires full access to the ELO program directory. Otherwise, errors will occur for some ELO applications (ELO Analytics, ELOwf and ELOsi).



In this example, ELO Analytics is not running.



The Windows Event Viewer displays a message indicating that there is no access to the ELO Analytics log directory.



- Give the *ELOMSA$* MSA write permissions to the ELO program directory.

'jmxremote.password' file

In addition, the MSA needs at least read permissions to the *jmxremote.password* file.

1. Grant the MSA at least read permissions to the *jmxremote.password* file.

   This file is in:

   ```
   <ELO>\config\serversetup2\
   ```

2. Additionally, enter the MSA as the owner of the *jmxremote.password* file.

   > **Information**
   >
   > You have to make this change for all services that have the parameter `-Dcom.sun.management.jmxremote.password.file` in the Java options.

ABBYY FineReader

To ensure that the ELO OCR Service or ELO OCR workers run correctly, follow the steps below.

Temp directory

1. Grant the MSA write permissions to the ABBYY FineReader temp directory so that the ELO OCR Service and ELO OCR workers will run correctly.

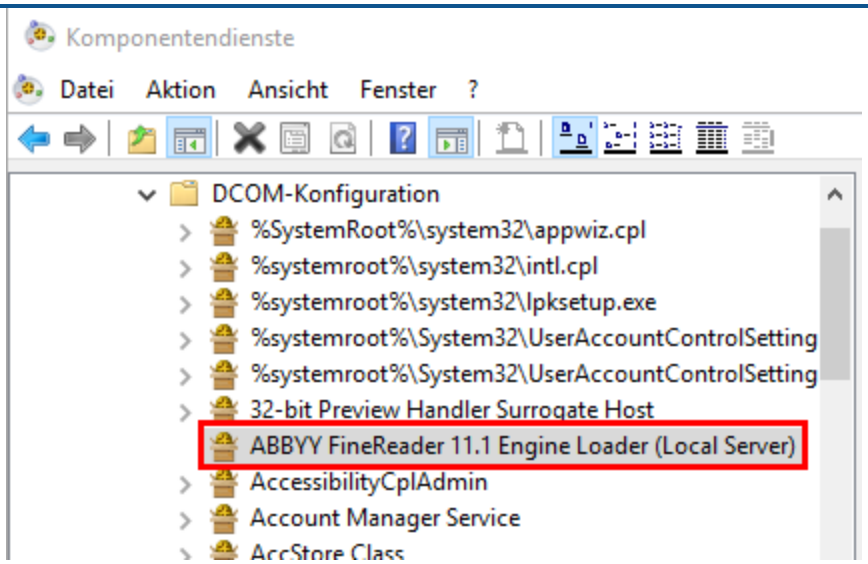
   Otherwise, you will get the following error message:

   ```
   08:50:07.194 [fr-obj-1] ERROR (FREngineActiveObject.java:1037) - Abbyy FineReaderEngi

   com.abbyy.FREngine.EngineException: Access to C:\Windows\TEMP\ABBYY FineReader Engine
   ```

Component services

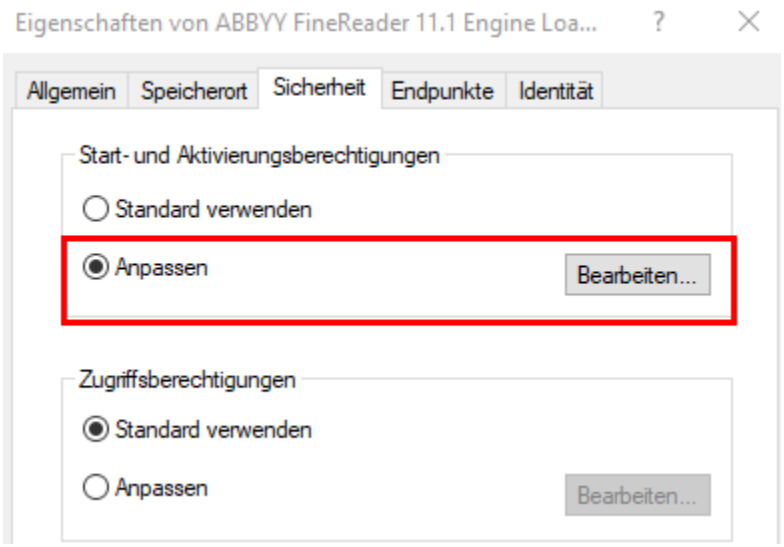
You also need to grant the MSA all permissions to *ABBYY FineReader 11 Engine Loader (Local Server)* under *Launch and Activation Permissions* in the *Microsoft Windows Component Services* application.

1. Open the *Component Services* application.
2. Navigate to the *DCOM Config* directory.



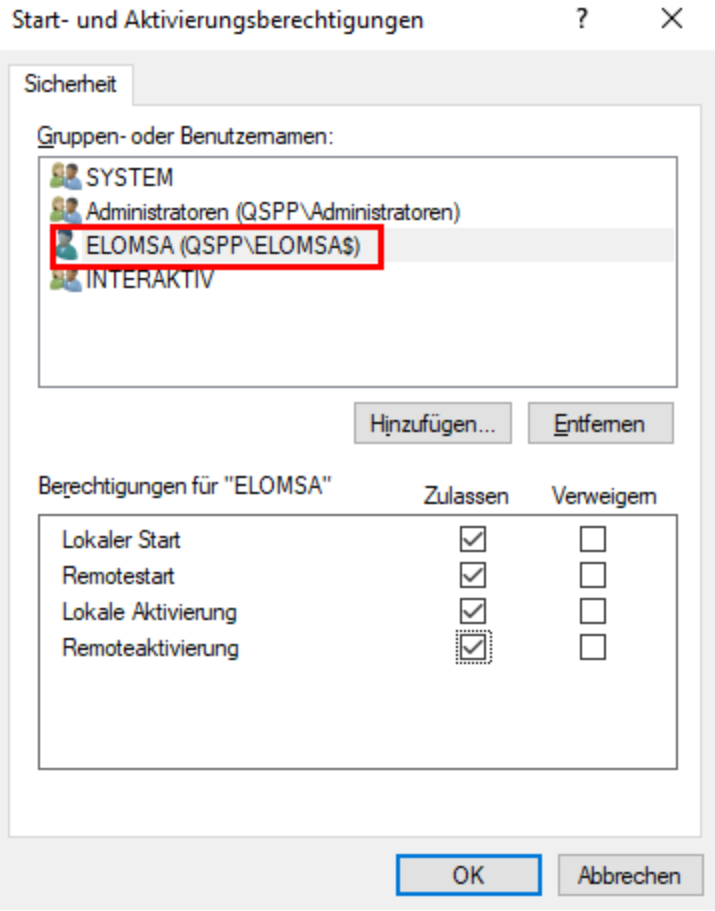
3. Open the context menu for the *ABBYY FineReader 11 Engine Loader (Local Server)* entry.
4. Select *Properties*.

   The *Properties of...* dialog box opens.
5. Select the *Security* tab.



6. Under *Launch and Activation Permissions*, enable the *Customize* option.
7. Select *Edit*.

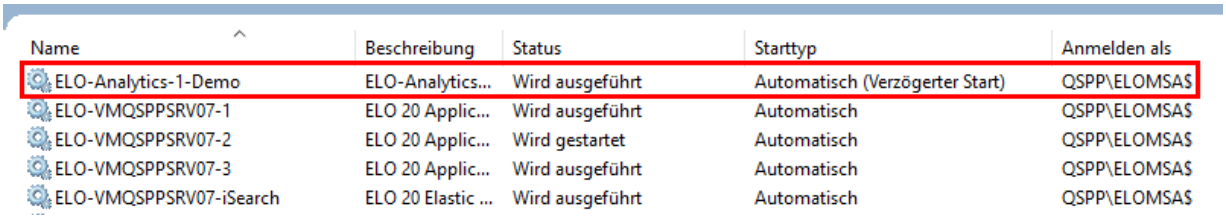
   The *Launch and Activation Permissions* dialog box opens.



8. Add the MSA will all permissions.
9. Click *OK* to close the *Launch and Activation Permissions* dialog box.
10. Click *OK* to close the *Properties of...* dialog box.

Final steps

1. Restart the ELO services.



The services should now run correctly again.

Potential installation issues

This section describes potential issues during initial installation or upgrades and how to resolve them.

Hot deployment not implemented

This issue can occur both during upgrade and initial installation. During installation, the following error message may occur:

```
Deploy Webapp [...] on [...] Hot deployment not implemented
```

This error occurs when an application is listening on the port that is configured for the ELO Application Server, such as when you update an ELO server but the old server has not been stopped in time.

Solution: Identify the application that is listening on the port in question (e.g. with `netstat -ano`).

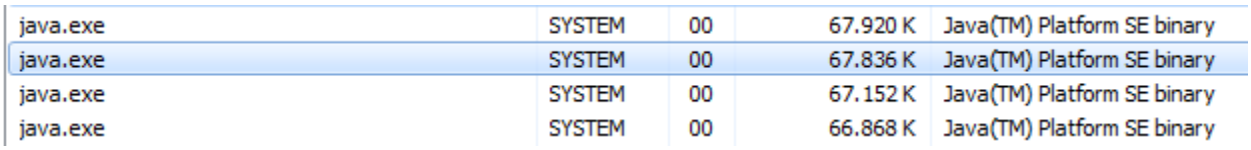
If necessary, end the process with Windows Task Manager.

Run the ELO Server Setup again. The application should now install correctly.

OCR update

This issue only occurs when updating an existing ELO system. In some cases, the ELO OCR worker processes do not shut down in time, which leads to an error in the ELO Server Setup.

In Windows Task Manager, you can see that the *java.exe_ processes all take up between 30 and 70 MB RAM.



java.exe	SYSTEM	00	67.920 K	Java(TM) Platform SE binary
java.exe	SYSTEM	00	67.836 K	Java(TM) Platform SE binary
java.exe	SYSTEM	00	67.152 K	Java(TM) Platform SE binary
java.exe	SYSTEM	00	66.868 K	Java(TM) Platform SE binary

You can also see that the ELO server `\webapps\ocr` directory was not completely deleted. This also prevents the updated WAR file from being deployed.

Solution: Stop the ELO Application Server that ELO OCR is running on.

Next, stop all of the OCR worker Java processes manually in the Task Manager.

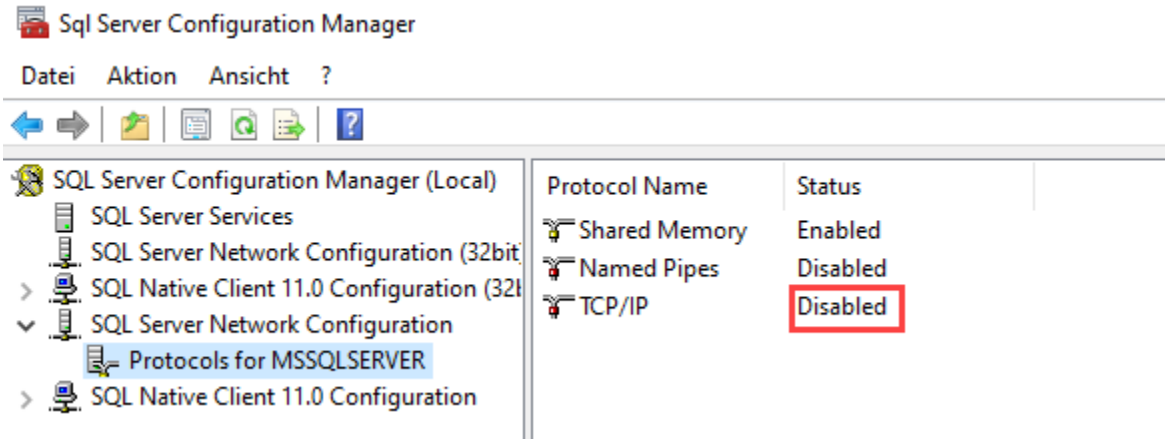
Now delete the `<ELO>\webapps\ocr` directory, replacing `<ELO>` with your ELO Application Server installation directory.

Finally, start the ELO Application Server again.

Problems connecting to the Microsoft SQL database

During installation, various problems can occur when connecting to the Microsoft SQL database. This section covers some of the issues.

TCP/IP not enabled



With the default settings, TCP/IP is disabled.

You need to enable TCP/IP using the *SQL Server Configuration Manager* tool.

For more information, refer to the section 'Enable TCP/IP' in the chapter 'Microsoft SQL Server'.

Database port blocked by firewall

With the default settings, the port for the Microsoft SQL database is blocked by a firewall.

Create an inbound rule for the corresponding port, such as described in the section 'Open port' in the chapter 'Microsoft SQL Server'.

'SQL Server Agent' service not started

With the default settings, the *SQL Browser Agent* service must be started manually.

Set the service startup type to *Automatic* as described under 'SQL Server Agent' in the chapter 'Microsoft SQL Server'.

Configuration files

In most cases, the *config.xml* file is configured with the appropriate values during the installation process and will not require manual changes.

Parameters in config.xml

In certain situations that require a custom installation, you need to change this file manually. The following list contains an overview of parameters for the files.

The configuration files for the ELO Administration Console, ELOwf, ELOas, and the ELO XML Importer are described in their respective manuals.

The parameters in the config files are structured according to the following convention:

```
<entry key="<name of parameter>"><value></entry>`
```

> **Information**
>
> Replace the two placeholders `<name of parameter>` and `<value>` without pointy brackets (<>). The pointy brackets are used here to mark the placeholders.

ELO Indexserver (ELOix, ELOam, ELOdm, and ELOft)

dbdriver: Java database driver (pure JDBC driver)

jdbcurl: Java database connection via JDBC

database: Database used. You should only set this parameter if you are using Microsoft SQL Server or a compatible database engine that allows you to switch between databases with the USE commands. If you do not enter anything here, the database must be included in jdbcurl (Oracle).

dbconnections: Number of database connections that are permanently in use (not for ELOix).

dbuser: Name of the database account. When using Oracle, the ELO Document Manager requires an individual database account for each repository.

dbpwd: Database account password. It is created in an encrypted form during installation (multiple numbers separated by a hyphen), but can be used in a non-encrypted form.

eloftoptgroup: Group number for the values in the database table *eloftopt*. This should not normally be changed (ELOft only).

proxyslot: Slot number (1-4) of the branch sharing the same ELOdm when proxy mode is used. "0" is for the main office (ELOdm only).

hideStatus: Can be set to `true` if you want to hide the detailed information on the status page of the ELO Indexserver.

ELO Textreader (ELOtr)

For information about configuring ELO Textreader (gen. 2), refer to the *ELO Textreader (gen. 2)* documentation.

Default configuration

To make the ELO installation process as easy as possible, the ELO Server Setup makes several settings automatically. This section provides information about the default configuration of the ELO server after installation. If you change any of these settings before installation, the installed ELO server will have a correspondingly different configuration.

Apache Tomcats

The standard installation mode installs four instances of Apache Tomcat for the different ELO server modules and the ELO iSearch module. The default settings on each Apache Tomcat are described below.

General settings

Several settings apply for all Apache Tomcats installed by the ELO Server Setup. The following is a list of the most important settings that apply for all Apache Tomcats:

- Tomcat administrator
- Name: admin (can be changed in custom installation mode)
- Roles: admin-gui, manager-gui

Custom settings

The different settings for each Apache Tomcat instance are as follows:

Tomcat 1: Named `ELO-<computer name>-1`. Contains ELO Indexserver (including ELO Access Manager and ELO Document Manager) and ELO Forms Services. Maximum memory 2048 MB, HTTP port 9090.

Tomcat 2: Named `ELO-<computer name>-2`. Contains the ELO Administration Console. Maximum memory 512 MB, HTTP port 9080.

Tomcat 3: Named `ELO-<computer name>-3`. Contains ELO Automation Services. Maximum memory 1024 MB, HTTP port 9070.

Tomcat 4: Name `ELO-Textreader-1`. Contains ELO Textreader (Gen. 2) with ELO OCR and ELO Preview Converter. Maximum memory 1024 MB, HTTP port 9060.

> **Information**
>
> All of the information listed above for Apache Tomcat 1-4 can be changed before you install custom installation mode.

Tomcat 5: Named `ELO iSearch`. Contains the ELO iSearch/Elasticsearch module. Maximum memory 4096 MB, HTTP port 9200.

Please note

ELO recommends keeping the default value for memory here. Experience has shown that assigning additional RAM here can result in various problems, while not appreciably increasing performance.

Ports used

The Apache Tomcat servers named above can use the following ports for communication. To check whether a port is currently in use, you can enter the following to the command line:

```
netstat -aon | find "<port>"
```

Replace `<port>` with the port number you are currently testing.

The ELO Server Setup automatically opens ports in the Windows firewall for communication with client applications. However, none of the ports named below should be used by other programs.

Information

The ports specified here are the values for a standard installation. They can vary depending on the configuration.

Tomcat 1

- 9090: HTTP
- 9091: JMX
- 9093: HTTPS/redirect (optional)
- 9094: AJP
- 9095: Shutdown
- 9096: Replication (optional)

Information

Use port 9090 to connect to the ELO server from client applications with standard settings (ELO Indexserver address).

Tomcat 2

- 9080: HTTP
- 9081: JMX
- 9083: HTTPS/redirect (optional)
- 9084: AJP
- 9085: Shutdown
- 9086: Replication (optional)

Tomcat 3

- 9070: HTTP
- 9071: JMX
- 9073: HTTPS/redirect (optional)
- 9074: AJP
- 9075: Shutdown
- 9076: Replication (optional)

Tomcat 4 (ELO Textreader)

- 9060: HTTP
- 9061: JMX
- 9063: HTTPS/redirect (optional)
- 9064: AJP
- 9065: Shutdown

Tomcat 5 (ELO iSearch)

- 9200: HTTP (REST)
- 9201: JMX
- 9204: TCP

> **Please note**
>
> Port 9204 is used for communication between the ELO Indexserver and the search module in the Indexserver options. This setting is applied automatically during setup.

ELO XC

- Port: Higher than 5000
- Default: 8010

ELO Flows worker

- Default port: 9000
- Default RAM: 1024

ELO Bot for Microsoft Teams

- Default port: 9040
- HTTPS: 9043

ELO Azure Administration

- Default port: 9030

ELO Smart Link for SAP® ERP

- 9050 or 9060: If installing on a separate Apache Tomcat, one of these ports should be used. Which one to use depends on whether another Apache Tomcat/module is already using one of the ports.

ELO Connectivity Pack for SAP® ERP

- 3300: RFC (port number increases by 1 for each instance)
- 3600: If using the SAP Message Server (port number increases by 1 for each instance; the start port may be different)

Standard storage locations

The following information will help you manage your ELO repository and shows you where important files related to your servers are installed.

In the following, your ELO installation directory (e. g. `C:\ELOprofessional`) is referred to as `<ELO>`.

Repository: The default storage path for repository documents is *<ELO>\Repository\<repository name>*. The two default storage paths, `basis` and `elosys`, are created here.

Configurations: Configuration files for the ELO web applications (`config.xml` and `logback.xml`) are stored in *<ELO>\config\<application name>\<server name>*.

Additional important configuration files are stored in the `servers` directory (see below).

Java: The ELO server stores a 64-bit version of OpenJDK in this directory. All Apache Tomcat servers installed by the ELO Server Setup use this version of Java.

ELO server modules: All ELO server modules (web applications/WAR files) are stored in `<ELO>\prog\webapps`. These files are extracted to directories on the corresponding Apache Tomcat server at startup.

Log files: The log files for the ELO web applications and ELO iSearch are stored in the directory *<ELO>\logs\<server name>*. Apache Tomcat-specific log files (`catalina.log, manager.log`, etc.) are stored under *<ELO>\servers\<server name>\logs*.

Servers: The Apache Tomcat servers and ELO iSearch are installed by default to *<ELO>\servers*.

Extracted WAR files: Extracted WAR files are stored for each ELO server module in *<ELO>/servers/<server name>/webapps*.

Log files

Various log files are written during the installation of ELO and later when using ELO applications such as the ELO Access Manager. These files are found in various locations depending upon whether ELOprofessional server or ELOenterprise is used. The information contained in these files is not only useful for troubleshooting, but also for analyzing the normal operation and status of ELO applications.

Apache Tomcat

The default location for the log files of the Apache Tomcat application manager is the `logs` directory within the ELO server installation directory. You can change this location by editing either the Apache Tomcat configuration files or the *logback.xml* file in each ELO module.

Only ELO iSearch uses the files *log4j2.properties* and *elasticsearch.yml* for the configuration.

stderr and stdout

There are two log files that store all messages received from Apache Tomcat. These are named according to the following convention:

```
<server instance>-stderr.<timestamp>.log

<server instance>-stdout.<timestamp>.log
```

They may also occasionally contain messages from ELO.

ELO components

Separate log files are written for each of the ELO applications.

as-*.log: This log file contains the log data for ELO Automation Services.

im-*.log: This log file contains the log data for the ELO XML Importer.

ix-*.log: This log file contains the log data for the ELO Indexserver.

tr-*.log: This log file contains the log data for the ELO Textreader.

wf-*.log: This log file contains the log data for ELO Web Forms Services.

serversetup2.log: This log file contains the log data for the installation process and is stored in the server installation directory.

logback

The *logback* library is used by web applications and controls the storage of data in the log files. Each log file has an individual configuration file, *logback.xml*. The format of the log data can be modified within this file.

The default location for these files is as follows:

```
<ELO>/config/<application name>-<repository name>/<server instance>/
```

You can also change the log level from *info* to *debug* here.

> **Information**
>
> Note that changing the logging level to *DEBUG* can reduce performance significantly and cause the log file to grow exponentially in size over time. You should store the log files in a part of the server where they cannot affect system performance, for example by taking up too much disk space.

New log files are started every day at midnight and the existing file is renamed with the appropriate date at the end of the name. These files can be deleted at any time. You do not usually need to make any adjustments to the configuration file or the log file.

Uninstall

This document describes how to uninstall web applications from the ELO server.

Basics

ELO web applications are the applications that run on an Apache Tomcat or ELO Application Server (referred to as *Tomcat* in the following). Web applications must be uninstalled manually. The web applications build on each other:

An Access Manager forms the basis (ELOam). One ELOam may manage several repositories. At least one Document Manager (ELOdm) is required for each of the repositories. Additional web applications may be installed for each repository, e. g. the ELO Indexserver (ELOix).

The fastest way is to remove all web applications, or an ELOam with all of its corresponding web applications at once. If only individual repositories are to be uninstalled, their entries must also be deleted on the ELOam.

Please note

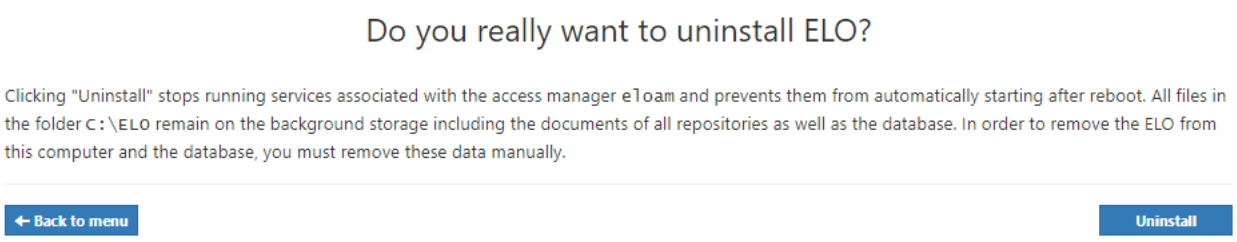
This document does not explain how to remove individual web applications. However, if you uninstall individual web applications, be aware that there may be dependencies with other applications.

Information

For live systems, we recommended that you back up the directories (Apache Tomcat directory, ELOprofessional or ELOenterprise directory) and the databases (Microsoft SQL Server) or database (Oracle and DB2) before uninstalling.

Uninstall the ELO server

The *Uninstall* option allows you to uninstall the ELO server.



In the next dialog box, you will be asked if you definitely want to uninstall the server. Select *Uninstall* to remove ELO.

If you uninstall ELO with this method, all services within the configuration of the ELO Access Manager are stopped and can only be restarted manually. No data will be deleted in the process.

Once the ELO server services are stopped, you can delete the associated installation directories, databases, services and other data associated with ELO.

High availability

Introduction

Cluster operation makes sense if you want to achieve high availability or load balancing. This document describes how you can configure ELOenterprise to operate in a cluster.

It addresses configuration of the ELO modules, and does not describe the configuration of third-party software, such as databases, HTTP proxies for load balancing, or failover managers required for cluster operation.

A load balancing cluster aims to distribute the workload of a service onto multiple computers in order to speed up response times. Clients can then be assigned specific services statically, which can also cause an unbalanced distribution of computing tasks. To counteract this, software is available for load balancing, e. g. Apache HTTPD with mod_proxy_balancer, which dynamically distributes queries to the available computers.

A high-availability cluster (HA cluster) is a link between at least two computers intended to increase the reliability of a service. Should a computer fail, the services it provides are migrated to other available computers. An HA cluster can also be combined with a load balancer, which is referred to as active/active clustering. In contrast, if a standby system is available in the background that steps in when the primary system fails, this is referred to as active/passive or failover clustering.

ELO Server Setup

The ELO Server Setup supports the installation of ELOenterprise for cluster systems. However, not all configurations are covered. The following document presents a few tricks as to how you can use the ELO Server Setup to realize the desired cluster configurations.

Configuration files

The ELO Server Setup uses two files for configuration, which are primarily identical in terms of content but are different semantically. The first file is stored to `%HOMEPATH%/.elosetup.conf` (or `${HOME}/.elosetup.conf`). Changes to the web interface are written to the first file as soon as you switch the tab in the ELO Server Setup. This file represents the target state of the ELO installation.

The other file is written to `<ELO>/config/serversetup2/elosetup.conf` just before installation is complete and represents the actual state of the ELO installation.

The file with the newer timestamp is considered the more current one. However, this only affects what is shown in the web interface. This property is useful when there are multiple people with administrative roles making changes via the setup, as the ELO Server Setup distributes changes made to the other people as soon as they start it.

Instance names

To differentiate between different instances within the same web application for a repository, they are named in their *config.xml*. This mechanism is necessary for ELO Access Manager, ELO Document Manager, and ELO Indexserver. These web applications have additional configuration parameters in the database that must differ depending on the instance.

One example is the *privateUrlBase* parameter for the ELO Indexserver. This parameter only has to be set to the URL the ELO Indexserver instance can be reached at so that other instances can connect in order to synchronize the cache e. g. of metadata forms.

The ELO Server Setup automatically configures the instance name for the web applications. The name of the ELO Application Server on which they were rolled out is used as the name. The ELO Server Setup makes sure these names are unique.

Setting up a cluster

This section explains how to set up clusters. There are the following types of clusters:

- Active/passive HA cluster
- Active/active HA cluster/load balancing cluster

Active/passive HA cluster

Logically, an active/passive HA cluster requires one active and one passive part. As the passive part only steps in if the active part fails, it is not necessary for the two parts to know of the other. Actually, the opposite is true. It is better for both parts to not know of the other. As it can be assumed that only one instance can be reached at runtime, attempting to synchronize the other, unavailable instance would always fail. It is better not to make the attempt at all.

To keep the instances unknown to one another, identical instance names should be used for an active/passive HA cluster, which requires identical installations on the active and passive system. However, because the ELO Server Setup requires unique instance names (names for the different ELO Application Servers), the ELO Server Setup must not know about the other installation either. This status can be achieved by configuring and installing the installation on the active system without the knowledge of the passive system. Next, you copy the `${HOME}/.elosetup.conf` from the active system to the passive system and then perform installation again in the same exact way.

> **Please note**
>
> If the host name of the passive system is different from that of the active system and you enter the name in the ELO Server Setup, the following applies:
>
> The web interface of the ELO Server Setup adjusts the names of the ELO Application Servers if they contained the previous host name. You will then have to set the name of the ELO Application Server back to the original value.

Active/active HA cluster/load balancing cluster

Compared with active/passive mode, ELO Indexserver or ELO iSearch must know about the other instance and communicate with it. On the first computer, using the ELO Server Setup, configure all involved components, including the components on the other computers that are part of the cluster. Afterwards, installation can be performed via the ELO Server Setup on the remaining computers by copying `<ELO>/config/serversetup2/elosetup.conf` from the first computer to %HOMEPATH%/.elosetup.conf (or. `${HOME}/.elosetup.conf`) on the remaining computers.

Information

The configuration file has to be copied from the installation directory, as only this file contains the certificates generated by the ELO Server Setup for encrypting communication between ELO Indexserver and ELO iSearch after initial installation.

ELO iSearch

If you have installed multiple instances of ELO iSearch for a cluster using the ELO Server Setup, these also automatically form their own cluster. For simple load balancing scenarios, the settings made by the ELO Server Setup should suffice. Should the requirements for system reliability increase, some configuration parameters should be adjusted as described in the following. You will find the corresponding configuration file under:

<ELO>/config/elastic/<service>/elasticsearch.yml

Master nodes and split-brain

To manage a cluster, all instances (nodes) in the ELO iSearch cluster determine a master node. A node can be set as the master node if its configuration file contains the value `master` under `node.roles`, which is the default setting.

If a communication error occurs in a cluster of two nodes between the two instances, but the two instances themselves are still capable of running, the result is referred to as a split-brain situation. Each of the two instances believes it is the master node and allows write operations on its index. However, this results in the data of the two instances diverging. This can cause data loss when restarting an instance, as it retrieves the data set from the other instance in its local cache. All write operations performed during this split-brain situation are lost.

Elasticsearch uses a *quorum-based* strategy to decide which of the available master nodes should be the new master node on start-up. The quorum is considered to be reached when at least `n` master nodes are available. The number `n` corresponds to the half of the available master nodes rounded down plus one (example for five available mater nodes: [5/2] + 1 = 3). The cluster is considered intact if at least `n` available master nodes can be reached. If a cluster is not intact, it is assigned the status *red*. An instance in a corrupt cluster no longer permits operations. If the cluster broke into two pieces, the part containing the majority of the master nodes would remain functional. The smaller cluster would no longer be intact.

This also means that a cluster with exactly two available master nodes will experience a split-brain situation. This is why a multi-node system should be made up of at least three available master nodes. The setting for the number of replicas must be adjusted to the number of nodes. For a cluster made up of three nodes, the number of replicas is already configured correctly with the value `1`.

Separate clusters on the same network

ELO supports installation of separate clusters on the same network. Although the setting `cluster.name: ELO` is set and identical for all installations, the Elasticsearch instances for separate installations are unable to find each other via the built-in auto-discovery mode as the Elasticsearch Search Guard plug-in only permits connections of instances with an identical root certificate.

System reliability and performance

Elasticsearch offers two main configuration parameters that can help improve performance and system reliability. The two following sections describe how you can improve performance by increasing the number of shards, as well as improve the reliability of a cluster by increasing the number of replicas. Depending on the scenario, the two settings may depend on each other.

Shards

Elasticsearch divides indices into a configurable number of parts, referred to as shards. Shards are the smallest unit of data that can be distributed to nodes in the cluster. To distribute queries to an index across several computers, it has to have been created with more than one shard or at least have a replica. Changing the number of shards in an index requires reindexing.

> **Information**
>
> Each index consists of at least one shard. Without manual intervention, adding a second Elasticsearch instance to the cluster causes cross-index searches to be distributed between the two instances.

In ELO, one index is created per metadata form. By default, each index consists of one shard. Creating one index per metadata form alone boosts cluster performance, as the indices are distributed to several nodes.

It also makes sense to split large indices into several shards. The advantage of this is that search queries are run in parallel on all shards. However, the number of search queries run in parallel within a node does not exceed the number of available CPUs.

As a result, the number of shards is based on the data contained. Elasticsearch recommends a shard size of 20 GB – 40 GB (See: www.elastic.co).

Too small of shards results in excessive communication between the shards, as the data has to be synchronized between them. Metadata forms containing an excessive amount of sords with full text should be split into multiple shards whenever possible.

The number of shards per metadata form can be set on the ELO iSearch configuration page, but changing this number requires all data to be reindexed.

Replicas

Replicas are like copies of an index. You can choose any value, including 0. One primary shard as well as the specified number of replica shards is created in the cluster for each shard. Primary shards and replica shards are always created on different nodes to be able to continue providing data in case of a failure. If a node fails, the primary shards that were previously allocated to this node are allocated to a different node. The replica shards are distributed to other nodes to ensure the best possible system reliability and performance. For orientation, you can assume that the number of replicas corresponds to the number of nodes that can fail without having a negative effect.

Another advantage of replica shards is parallel search queries: Elasticsearch distributes search queries to different primary shards and replica shards in order to balance the load of the search queries.

The health status of an index depends on what shard are available: If the primary shard is available, the status is "yellow". If all replica shards are also available, the status is "green".

The number of replica shards should be adjusted to the number of nodes in the cluster so that the shards can be distributed to several nodes in order to ensure system reliability. On the other hand, each replica requires just as much memory as the primary shard.

The default setting for the number of replicas is 1. In a cluster of more than one instance, each shard is replicated once, meaning it exists twice in total. Changing the number of replicas does not require reindexing.

To speed up reindexing in a cluster, you can set the number of replicas to 0 for the duration of reindexing and then increase it once reindexing is complete. If the number of replicas > 0, the data in both the primary shard and each replica shard is indexed at the same time. This means that analysis and conversion to Elasticsearch data takes place several times in parallel. If the number of replicas is set to 0, the data is only processed in one node during reindexing. Once the number of replicas is increased, the indexed primary shards are copied to the other nodes, which is generally much faster. Of course, system reliability cannot be guaranteed during reindexing.

The setting applies to an index and can be changed to 2 as in the following sample metadata form with ID 42 in the *demo* repository.

```
curl -X PUT "localhost:9200/demo¶42/_settings" -H 'Content-Type: application/json' -d'
{
    "index" : {
        "number_of_replicas" : 2
    }
}
'
```

If you want to change the setting for all indices, do not specify an index and use the URL the `localhost:9200/_settings`.

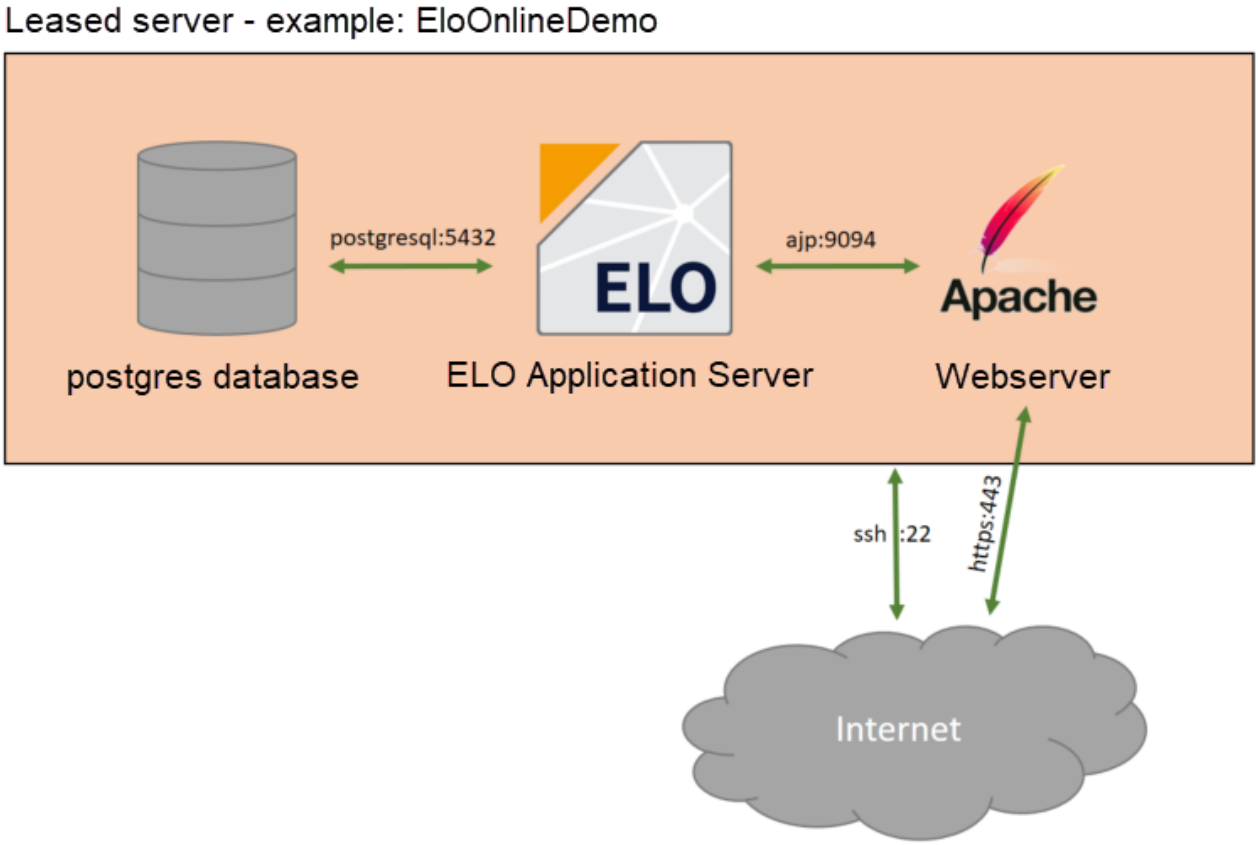
Failover cluster

In a failover cluster, the stand-by ELO iSearch system lacks current data from ongoing operation. In case of failover, ELO iSearch would find obsolete data or no data at all. This is why it is essential to save the ELO iSearch index on a high-availability network drive. In the ELO Server Setup, you can choose the path where ELO iSearch saves its index. You will find the setting in the ELO Server Setup under *Advanced Configuration > Application Servers* and the corresponding entry for the ELO iSearch *Data folder*.

Example installation – providing access to ELO via the web

Introduction

For maintenance purposes, the server should be accessible over SSH. In this example, we show how to configure the setup accordingly. We only want the ELO components to be accessible via a web server AJP proxy. The database can only be accessed locally.



We used the following hardware for this example:

- Virtual server
- 4 vCPUs
- 16 GB RAM
- 160 GB SSD

Experience has shown that virtual environments do not always deliver the specified performance. For this reason, we increased the hardware specifications of the rented server.

With a rented server, it is usually possible to directly select the OS used for installation. Due to its popularity, we chose Ubuntu (20.04 LTS). There are many online help forums for this OS, which makes it much easier to maintain.

To access the server, most servers offer a browser console, in our example a window with a *Bash*. In our case, SSH access was already enabled via *root*, giving us direct access with the shell client of our choice. However, the first step is also identical for a browser or administration console.

This documentation covers the following topics:

- Getting started
  - Account configuration
  - OS maintenance
  - Set the system locale
- Database server installation
  - Create the DB account
  - Modify the login rules
- ELO installation
  - Create required accounts and groups in OS
  - Install the ELO Server Setup
  - Run the ELO Server Setup
  - Access to the ELO Administration Console
- Reverse proxy web server installation
  - Before configuration
  - Web server configuration
  - Change firewall settings

Getting started

Account configuration

The first thing that needs to be done on a new system, whether Windows or Linux, is to install system updates.

Log on as "root". You will be given this data when you order the server. The basic provider configuration determines whether you can get access with a client of your choice or only with an administration console supplied by the provider. You generally need to use a *Bash*.

```
apt-get update
apt-get upgrade
```

Next, we need to block *remote SSH login* for the "root" account. To ensure that we don't disable access for ourselves, we create a new account beforehand and assign sufficient permissions:

```
adduser eloonlinedemo
```

We will be prompted to enter the password for this new account. Set a secure password.

> **Information**
>
> Depending on the shell or client you are using, some special characters may cause problems with the password; it is best not to be too creative here and instead use a simpler password with 20 or more characters.

```
New password: **********************************
Retype new password: **********************************
       Full Name []: elo
       Room Number []: online
       Work Phone []: demo
       Home Phone []: none
       Other []: none
```

To allow the new account to execute super user commands via `sudo`, we add this user to the sudo group.

```
usermod -aG sudo eloonlinedemo
```

Next, we need to allow the new account to log in to the server via SSH. If the SSH service is not installed on your server yet, you will need to do this beforehand. The following commands are required for this: `# sudo apt install openssh-server` and `# sudo ufw allow ssh`.

Edit the `ssh config` to add our new account:

```
vi /etc/ssh/sshd_config
```

Add the following line to the end of the configuration:

```
AllowUsers eloonlinedemo
```

Enter your chosen account name instead of "eloonlinedemo".

> **Information**
>
> Tip for using vim:
>
> | Command | Command mode |
> |---|---|
> | i | *Insert mode* or text |
> | ESC | Open *command mode* |
> | SHIFT + g | Jump to the end of the file |
> | ESC : wq ENTER | End text input and save and close the file (the lower case *: wq* stands for "write and quit"). |

We also need to modify the encryption methods and other parameters to meet the recommendations of the BSI. To do so, we need to add the following lines to the end of the configuration:

```
KeyAlgorithms diffie-hellman-group-exchange-sha256,
    ecdh-sha2-nistp521,ecdh-sha2-nistp384,
    ecdh-sha2-nistp256,diffie-hellman-group16-sha512
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha2-512,hmac-sha2-256
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,
    ecdsa-sha2-nistp521
```

The algorithms listed here are recommended by the BSI for use until 2028. By explicitly enabling them, all methods not configured here are blocked to ensure that insecure encryption methods are no longer used.

> **Information**
>
> Method with changed recommendations/other SSH services:

> Recommendations can of course change over time and the methods supported by a specific SSH service may also differ. To find out which ones are supported by your SSH service, or which methods the BSI currently recommends, check the OS documentation (here: Ubuntu):
>
> https://manpages.ubuntu.com/manpages/cosmic/en/man5/sshd_config.5.html
>
> The BSI Technical Guideline, currently TR02102:
>
> https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

Restart the SSH service.

```
systemctl restart sshd
```

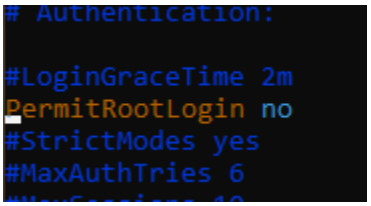
You can now test if the SSH login works for the new account. If you previously used a host administration console, you can now switch to the client of your choice. For this demo, we will use the Windows subsystem Ubuntu's Bash client.

```
ssh -l eloonlinedemo 111.222.333.444
```

(Replace the account name with your own, and the numeric sequence of your rental server IP.) To test the super user rights of our new account, we can disable the SSH login of the *root* account in the next step:

```
sudo vi /etc/ssh/sshd_config
```

Search for the line: `PermitRootLogin yes` and change it to `PermitRootLogin no`:



Save and close the file (ESC > : wq > ENTER). Restart the SSH service and check if you can still access via SSH with the *root* account. It should fail.

```
sudo systemctl restart sshd
```

OS maintenance

To keep the system up to date, set up automatic updates. Install the required packages:

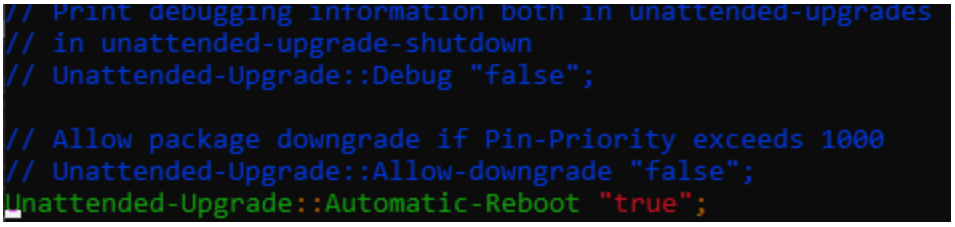
```
sudo apt-get install unattended-upgrades apt-listchanges
```

To configure them, edit the contents of the file *50unattended-upgrades* with the following command:

```
sudo vi /etc/apt/apt.conf.d/50unattended-upgrades
```

Optional: To enable automatic restart, add the following line:

```
Unattended-Upgrade::Automatic-Reboot "true";.
```



Not every image you get from your host has UFW enabled; in our example, this was automatically checked with:

```
sudo ufw status
# Status: inactive
```

We need to change this and enable the firewall as well as add it to the autostart sequence. To prevent all incoming connections from being rejected by the UFW firewall, we need to explicitly allow the legitimate incoming SSH connection:

```
sudo ufw allow ssh
```

The firewall can now be enabled.

```
sudo ufw enable
```

Make sure that access to the system remains the same and confirm the following request with y:

```
Command may disrupt existing SSH connections. Proceed with operation (y|n)?
```

If we now query the status, we see that only SSH traffic is allowed:

```
sudo ufw status
```

```
# Status: active

# To                         Action          From
# --                         ------          ----
# 22/tcp                     ALLOW     Anywhere
# 22/tcp (v6)                ALLOW     Anywhere (v6)
```

> **Information**
>
> To make the system even more secure, you can also configure it to allow only your public IP to establish SSH connections. You need to have a fixed IP for this to work.

Before we proceed with the next steps, we should check the system locale:

Set the system locale

```
locale

# LANG=en_US.UTF-8
…
```

To give you an example, if you wanted to install an ELO system in German, you need to change the locale to DE. You may be required to create the locale for the German language in UTF-8 first.

```
sudo locale-gen de_DE.UTF-8
```

You can check the result with the following command:

```
locale -a
```

Afterwards, you can reconfigure the language of `de_DE.UTF-8` using a simple tool.

```
sudo dpkg-reconfigure locales
```

You can check this result as well:

```
cat /etc/default/locale
```

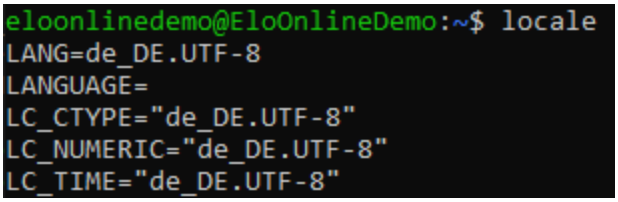
```
eloonlinedemo@EloOnlineDemo:~$ cat /etc/default/locale
LANG=de_DE.UTF-8
```

Restart the system.

```
sudo reboot
```

Once you have restarted, retrieve the locale again to check the result:

```
locale
```



Installing the database server

Now that the basic system is installed, we can move on to the requirements for the ELO installation. In addition to the various ELO server components, a database is required. In the next section, we will install a PostgreSQL server in a very basic way.

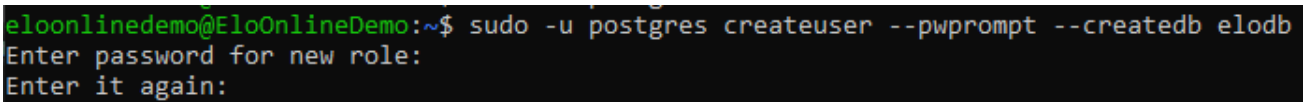
```
sudo apt-get update
sudo apt-get install -y postgresql
```

Once the server is installed, we will give it a very basic configuration. You can add more options here but we will only create and authorize an ELO account.

Create the database account

We create a new account in the PostgreSQL admin account "postgres" context:

```
sudo -u postgres createuser --pwprompt --createdb elodb
```



Modify the login rules

To allow the account "elodb" to authenticate with a password, the PostgreSQL server must be configured to allow password login:

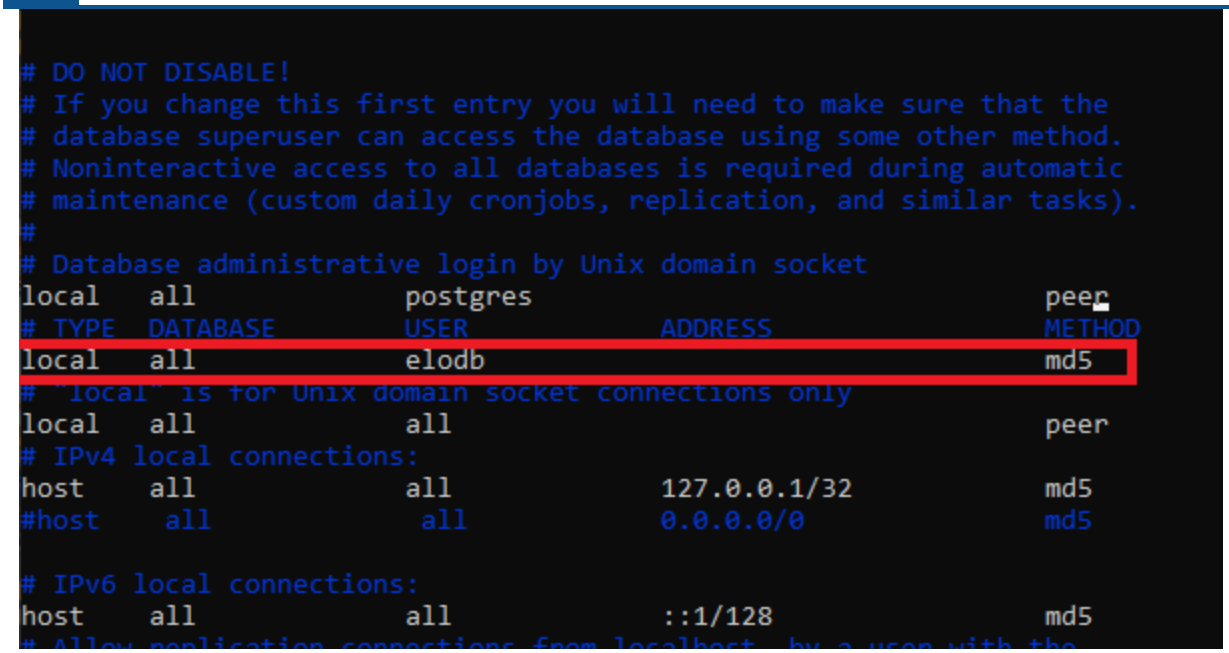
```
sudo vi /etc/postgresql/12/main/pg_hba.conf
```

Navigate to the line:

```
# TYPE  DATABASE  USER   ADDRESS  METHOD
```

Add the following line:

```
local   all       elodb           md5
```



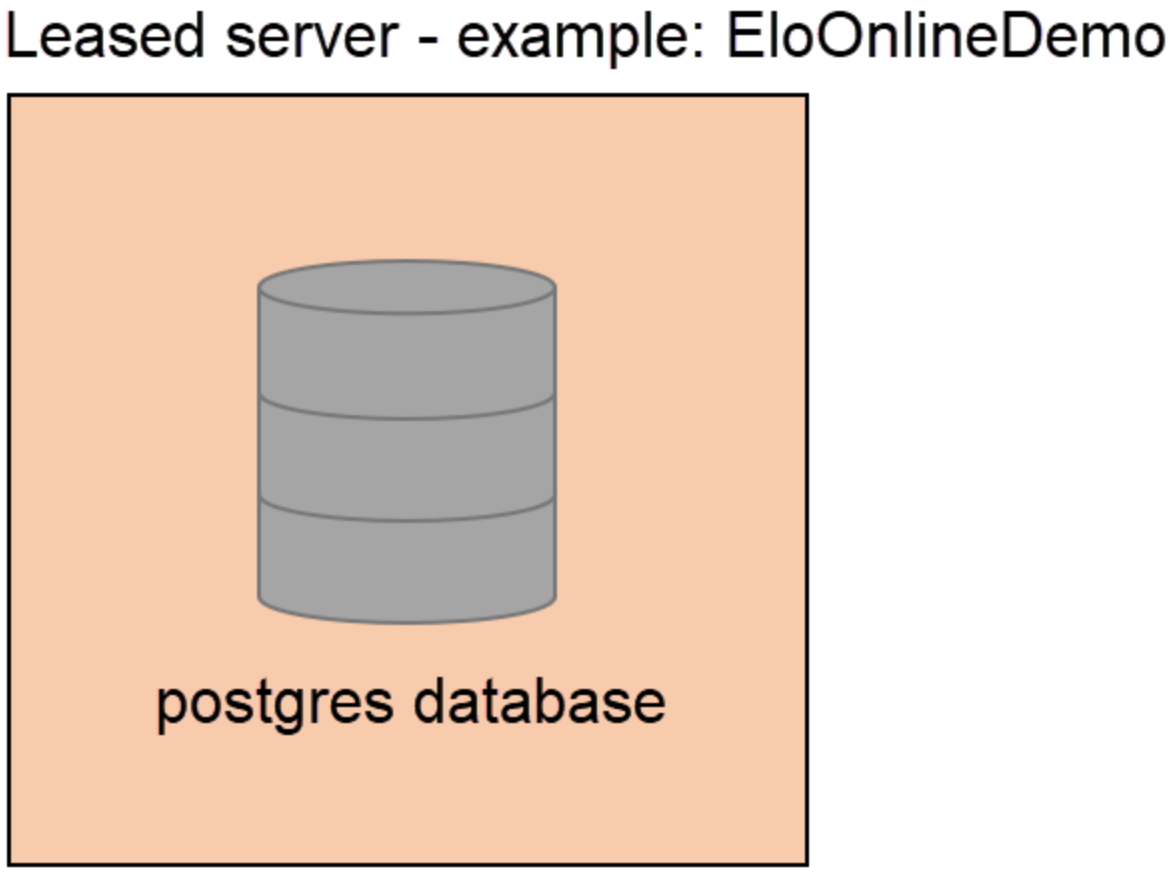
The account *elodb* can now authenticate on the server with a password but only from a local system. However, only from the local system. Check the login once with:

```
psql -h localhost -p 5432 -U elodb postgres
```

Close the psql interface with:

```
\q
```

The current setup now looks like this:



The PostgreSQL server can only be accessed locally.

We have now met the requirements for adding an ELO installation.

ELO installation

Create required accounts and groups in OS

The services that will run locally on the system for ELO require a service account. We will now create this service account and a corresponding group. The account name and group name will be "elo".

```
sudo useradd elo
sudo passwd elo
```

The account and group are now created. You can confirm this with `id elo`.

Install the ELO Server Setup

The next step is the ELO installation. The first thing you require is the ELO Server Setup for Linux. Download this on the usual channels and place it on the rented server, e.g. using SFTP.

> **Information**
>
> Tip for using SFTP: When enabling SSH access, access via SFTP is also enabled by default, so you can simply upload the setup with an FTP client of your choice to `sftp://<server IP>` if you do not want to download it using Bash.

The ELO Server Setup starts a web server on which you can perform the ELO installation; for security reasons this interface is only accessible via "localhost". We therefore need to establish a new SSH connection for the installation on our rented server that doesn't have a GUI. To do so, we redirect localhost: 7458 to port 7458 on the target server to enable us to access the ELO Server Setup with the browser from another computer that has a GUI.

We can terminate the existing SSH connection with `exit`. Afterwards, we can establish a new connection using the port redirect described above.

Run the ELO Server Setup

```
ssh -l <account name> -L 7458:localhost:7458 <destination IP of rented host>
```

> **Information**
>
> It is also possible to redirect the port with other clients, e.g. PuTTY.

We installed the ELO Server Setup via FTP client to the home directory of our demo account as shown here:

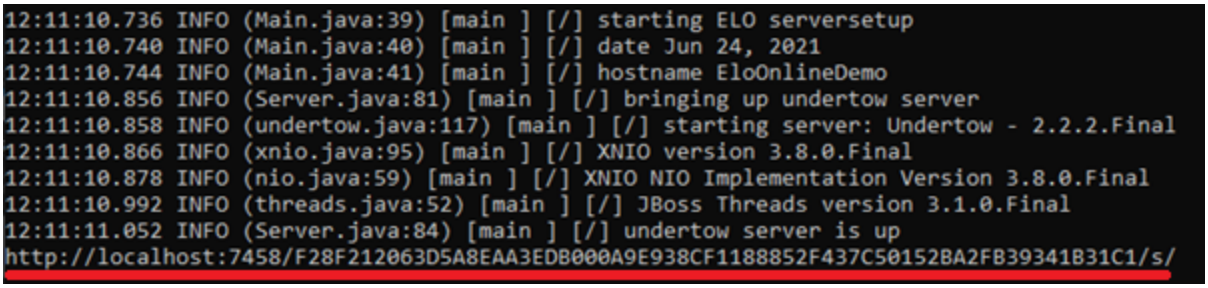
/home/eloonlinedemo/serversetup2.sh or */home/<account name>/serversetup2.sh*

Change the path as you go along if you stored it somewhere else in the file system.

We need elevated permissions to run the setup:

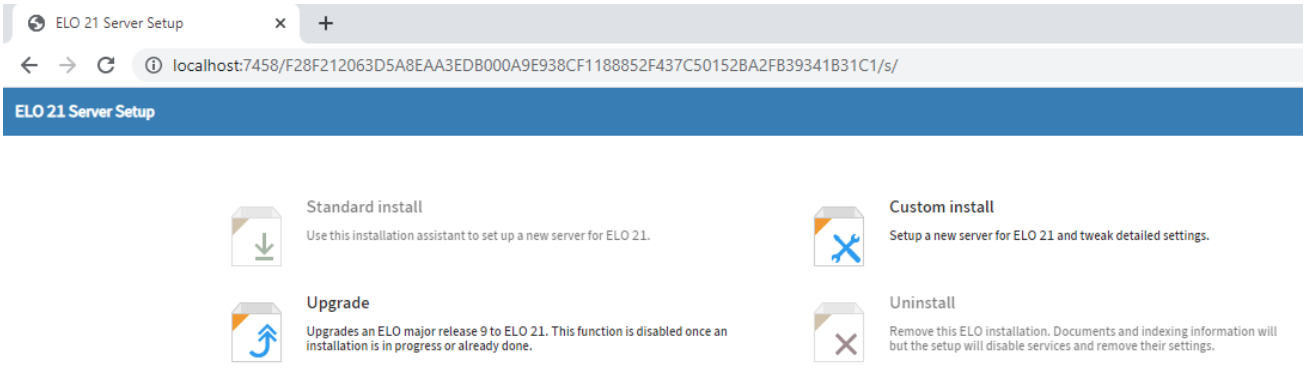
```
sudo sh ~/serversetup2.sh
```

The ELO Server Setup is now extracted and executed.



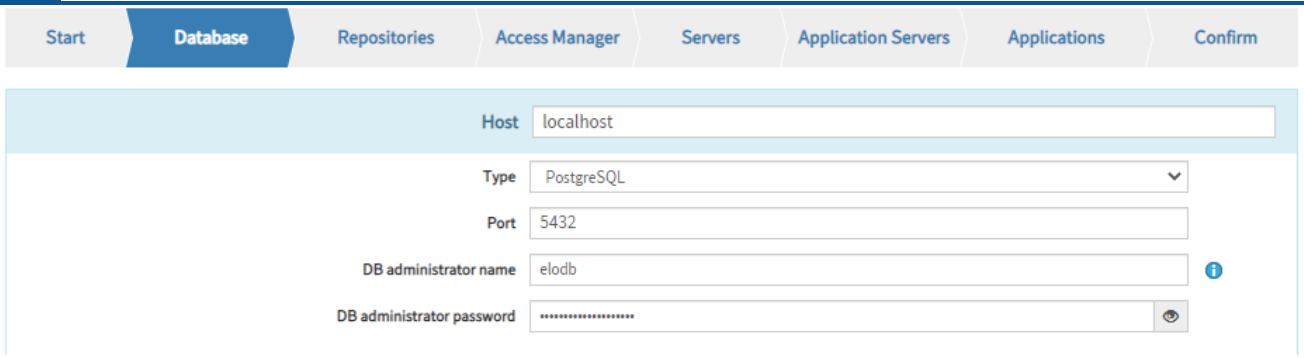
If the undertow server is available, a link is shown in Bash.

We can now open this in the browser on the computer that we established the SSH tunnel on.

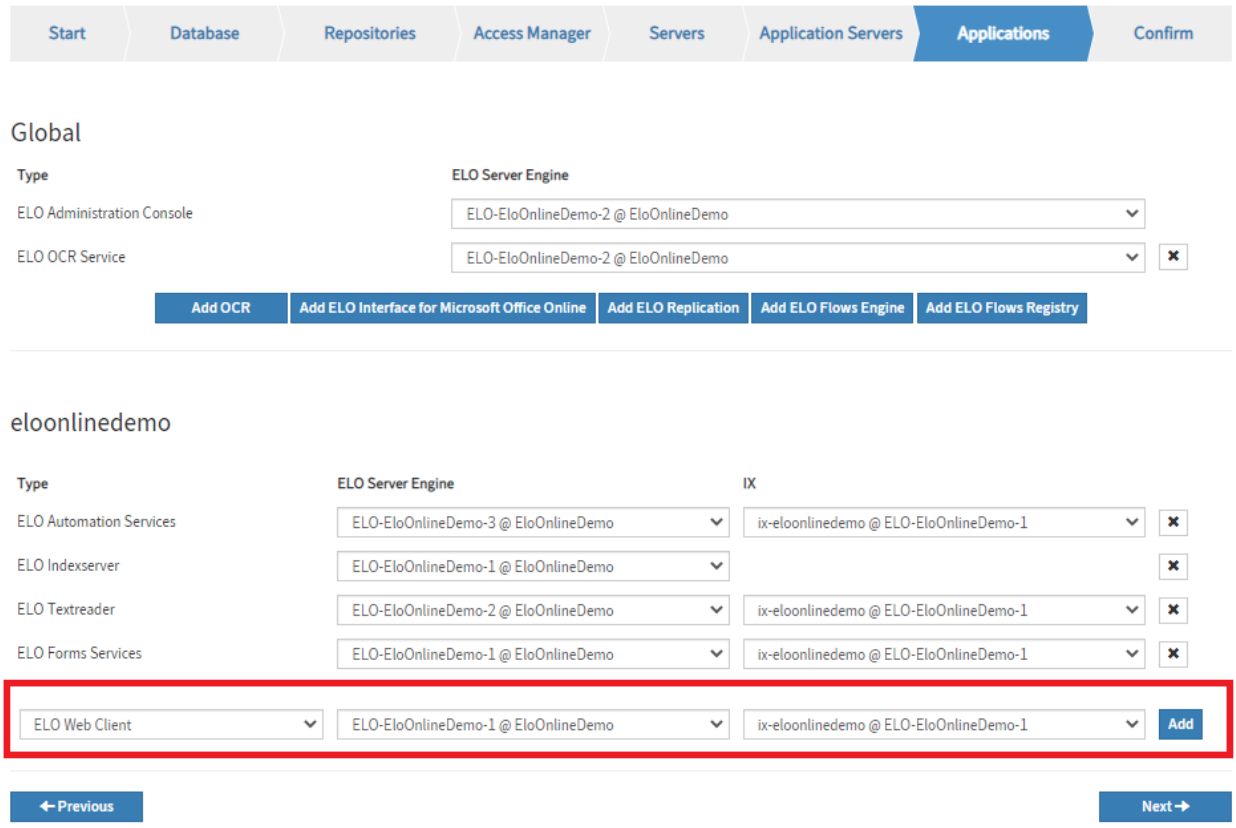


Information

As the firewall configuration does not allow remote access to port 7458, the connection is currently tunneled through SSH and routed through the shared port 22.

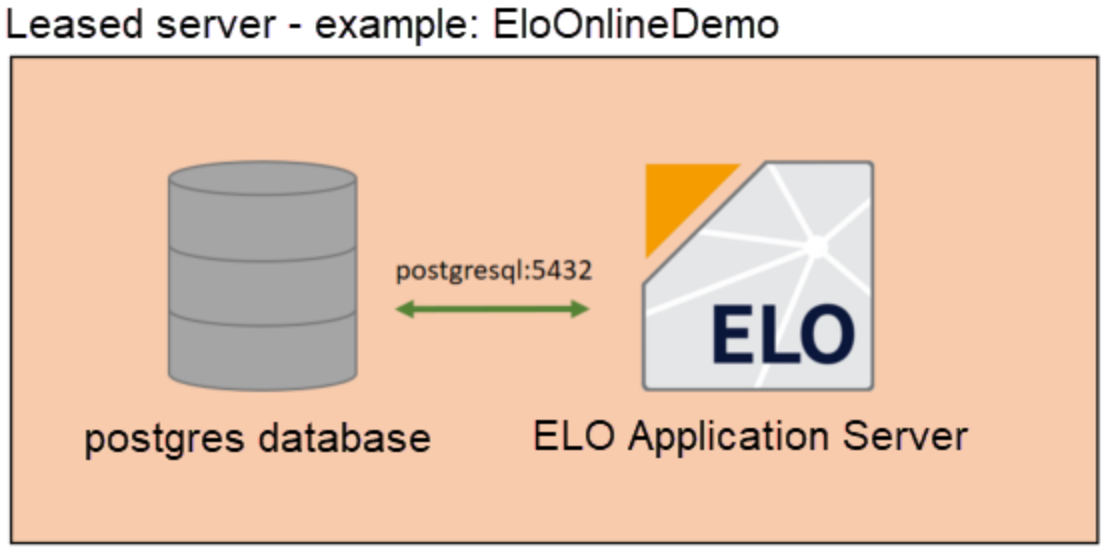


Select the option *Custom Install* and proceed with the ELO installation as usual.



Remember to add an ELO Web Client when you get to the *Applications*. (If you forget to do this, you can of course do it later by running the ELO Server Setup again.)

> **Information**
>
> Remember to check your records: You should make a note of all account names and passwords, preferably in encrypted form.



Access to the ELO Administration Console

Since the firewall only allows a connection through port 22, you cannot access the ELO Administration Console in this way. However, this is deliberately the case in order to ensure that only absolutely necessary components can be called. The port redirect used for the ELO Server Setup can also be used to access the ELO Administration Console. Only the port has to be changed:

```
ssh –l <account name> -L 9090:localhost:9090 <destination IP of rented host>
```

The URL for calling the ELO Administration Console would be as follows in the example:

```
http://localhost:9090/ix-eloonlinedemo/plugin/de.elo.ix.plugin.proxy/ac/registry/index.xhtm
```

> **Information**
>
> Later on in this documentation, we will configure the ELO Administration Console to be accessible via ELOix plug-in proxy.
>
> Use the tunnel solution described above if you need access to ELOas or other components that are not available by default with the ELOix plug-in proxy.

To allow access to the ELO server, i.e. ELO Indexserver and ELO Web Client, we now need to install and configure a web server. In this guide, we will use Apache2.

Install reverse proxy web server

This can be installed with the following command:

```
sudo apt-get install apache2
```

Afterwards, enable the proxy module and the AJP proxy module:

```
sudo a2enmod proxy
sudo a2enmod proxy_ajp
```

Now enable the SSL module:

```
sudo a2enmod ssl
```

Next, we need to store our certificate along with the CA certificate and private key on the server.

> **Information**
>
> You can use the SFTP upload function here, see the section Install the ELO Server Setup.

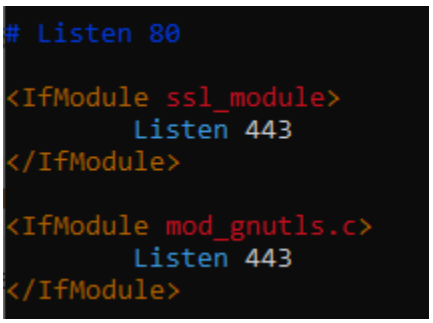
You will get the correct certificate format from each authority if you specify that you are using the Apache web server when you purchase it. If you still need to convert your certificate first, there are countless tutorials on the Internet.

Now that the web server is installed and the required modules are enabled, we can proceed with the configuration:

Disable listener on port 80:

```
sudo vi /etc/apache2/ports.conf
```

Just comment out the line `Listen 80`.



We don't require the default page. It can be disabled by simply deleting the link to it:

```
sudo rm /etc/apache2/sites-enabled/000-default.conf
```

In this guide, we use the default configuration file for SSL configuration. To enable this file (called site here), we link it to the *sites-enabled* folder:

```
sudo ln -s /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-enabled/
```

We make most of the settings in the configuration file we just linked to.

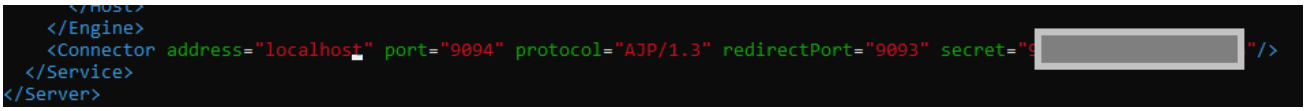
Before configuration

Before configuration, we need to gather some information:

- Path to the certificate in the example: /etc/ssl/eloonlinedemo/certificate.domain.com.crt
- Path to the private key in the example: /etc/ssl/private/key.domain.com.key
- Path to the CA certificate in the example: /etc/ssl/eloonlinedemo/root-certificate.domain.com.crt
- AJP port of the Apache Tomcat
- AJP secret of the Apache Tomcat

The last two items can be read from the server.xml of the Apache Tomcat hosting the ELO Indexserver. Open this file with:

```
sudo vi /ELO/servers/ELO-<name of repository>-1/conf/server.xml
```



The AJP port can be found under localhost:9094. The secret (in our case) is 9**********.

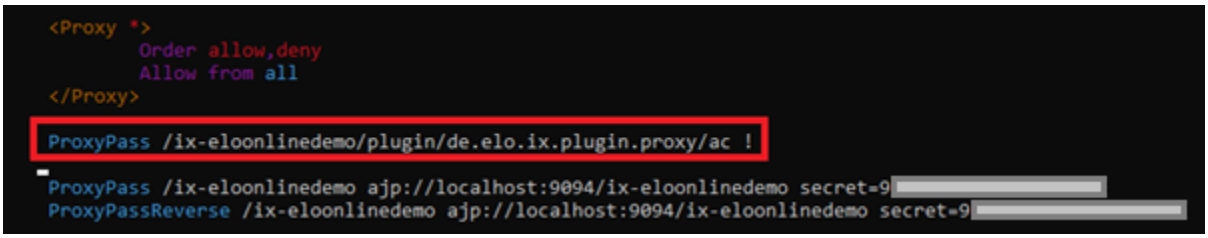
Once we have all the data we need, it can be stored in the Apache2 configuration.

```
sudo vi /etc/apache2/sites-available/default-ssl.conf
```

The result should look like this:

> **Information**
>
> Note that most of the options shown here are already in the configuration file and do not need to be added but only edited.

Web server configuration




```
ProxyPass /ix-eloonlinedemo/plugin/de.elo.ix.plugin.proxy/ac !
```

The line with the "!" at the end blocks a redirect via proxy instead of enabling it. This line can be added optionally to make the system more secure by further restricting access to the ELO Administration Console.

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/eloonlinedemo/Zertifikat.domain.com.crt
SSLCertificateKeyFile   /etc/ssl/private/Schluessel.domain.com.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#   Note: Inside SSLCACertificatePath you need hash symlinks
#                to point to the certificate files. Use the provided
#                Makefile to update the hash symlinks after changes.
SSLCACertificatePath /etc/ssl/eloonlinedemo
SSLCACertificateFile /etc/ssl/eloonlinedemo/Root-Zertifikat.domain.com.crt
```

> **Information**
>
> In this example, we use a version of Apache2 that supports a variety of SSL cipher suites. Some of these SSL cipher suites are classified as *not recommended* by the BSI.

> The following configuration snippet contains some cipher suites that are recommended for use until 2028 and beyond.

Configuring the cipher suites

We need to configure the cipher suites in the *ssl.conf* file of the associated module:

```
sudo vi /etc/apache2/mods-enabled/ssl.conf

SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:
    DHE-RSA-AES256-GCM-SHA384:
    DHE-RSA-AES256-CCM:
    ECDHE-RSA-AES128-GCM-SHA256:
    DHE-RSA-AES128-GCM-SHA256:
    DHE-RSA-AES128-CCM
SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
```

The web server must only allow *TLS 1.2* and *TLS 1.3*:

```
SSLProtocol -all +TLSv1.2 +TLSv1.3
```

```
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-CCM:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-CCM
SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384

# SSL server cipher order preference:
# Use server priorities for cipher algorithm choice.
# Clients may prefer lower grade encryption.  You should enable this
# option if you want to enforce stronger encryption, and can afford
# the CPU cost, and did not override SSLCipherSuite in a way that puts
# insecure ciphers first.
# Default: Off
SSLHonorCipherOrder on

#   The protocols to enable.
#   Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2
#   SSL v2  is no longer supported
#SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
SSLProtocol -all +TLSv1.2 +TLSv1.3
```

Switch Apache to run in *production mode*. This will prevent it from publishing specific version information about the web server and operating system.

To do this, edit the *apache2.conf* file and add two new lines if they do not already exist:

```
sudo vi /etc/apache2/apache2.conf

ServerTokens Prod
ServerSignature Off
```

We recommend a similar procedure for the *Apache Tomcat* ELO server. In this example, we use ELO 21.2, in which the corresponding option is enabled by default. If you are using a different version, you can check if the corresponding flag `showServerInfo="false"` is set by entering the following:

```
sudo grep -r 'showServerInfo="false"' /<ELO Install Dir>/
```

If the flag is missing, the configuration entry you need to set in *server.xml* could look like this:

```
sudo vi /ELO/servers/ELO-EloOnlineDemo-<X>/conf/server.xml
```

```
<Host appBase="webapps" autoDeploy="true" name="localhost" unpackWARs="true">
  <Valve className="org.apache.catalina.valves.AccessLogValve" directory="/ELO/logs/ELO-EloOnlineDemo-1" pattern="%h %l %u %t &quot;%r&quot; %s %b" prefix="localhost_access_log" suffix=".txt"/>
  <Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false" showServerInfo="false"/>
```

Now restart the Apache 2.

```
sudo systemctl restart apache2
```

Change firewall settings

To access the web server from the Internet, you still need to open the firewall for HTTPS traffic:

```
sudo ufw allow https
```

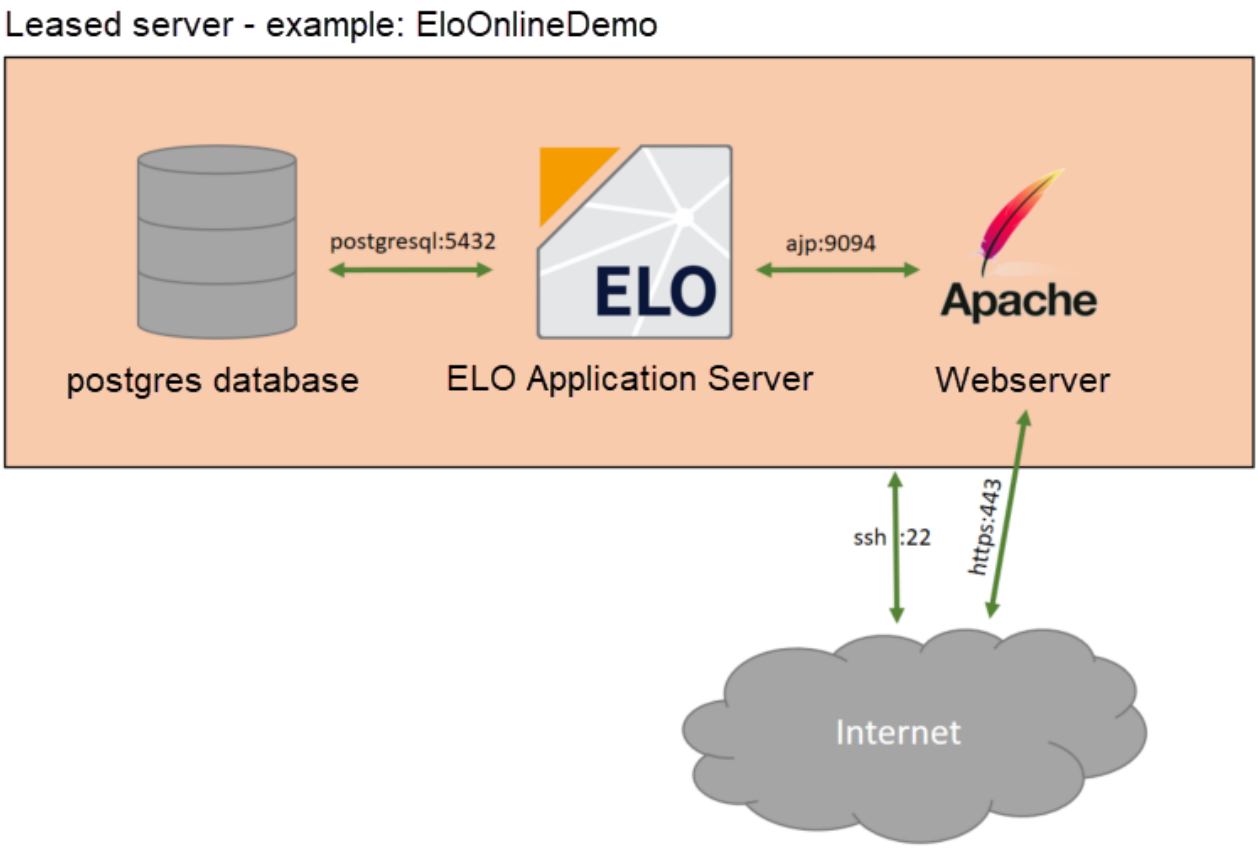
You should now be able to access the ELO Web Client:

```
https://<host IP>/ix-<name of repository>/plugin/de.elo.ix.plugin.proxy/web/
```

If required, also check whether you can access the ELO Administration Console:

```
https://<host IP>/ix-<name of repository>/plugin/de.elo.ix.plugin.proxy/ac/ui/login/index.x
```

If you have set the option shown above to block the ELO Administration Console, you should use the tunnel option via SSH described above and access the ELO Administration Console via port 9090.



Information

You can also check your own configuration using different online tools that are available. This allows you to get a rough idea of the security measures required for a *website SSL test* and an *SSH check*.