Crypt-o Manual

Version 3.4

Table of Contents

1. About Crypt-o

Crypt-o password manager will help you to organize and store securely any kind of valuable information, such as logins, passwords, lists of customers or employees, access codes, credit card numbers, PIN codes, files, etc.

Crypt-o is a true Client/Server solution for creating custom databases, which is designed for use in enterprise networks. The data is reliably stored in Firebird SQL Server database and is encrypted using AES encryption algorithm with 256-bit key. Crypt-o client applications access the Crypt-o Server using secure TLS connection.

If needed, Crypt-o Server can be connected from any location over the Internet, LAN or WAN link.

A flexible system of user account permissions allows to control users access to whole program, databases, folders or even individual records. Crypt-o can authenticate user accounts in Windows domain.

Every user action is logged to the Audit log. Privileged users can keep an eye on the program's usage.

Crypt-o can autofill web pages, registration forms, logon windows, etc. This feature is compatible with Chrome, Firefox, Edge, Internet Explorer and majority of usual Windows applications.

Crypt-o possesses user friendly interface, which can be easily adjusted to your likes.

2. Features

Features of Crypt-o password manager:

Exceptionally high security level

- Client/Server architecture with TLS encryption of network traffic;
- additional protection against man-in-the-middle hacker attacks;
- data is encrypted using AES encryption algorithm with 256-bit key;
- all user actions are logged to the Audit log;
- user permissions are validated by Crypt-o Server during every client request;
- automatic disconnection of inactive client connections;
- no unencrypted temporary files ever created;
- memory blocks are cleared when no longer needed;
- built-in password generator;

Multi-user environment support

- the hundreds of remote client connections can be handled simultaneously;
- support for remote client connections via slow network links like WAN or the Internet;
- ability to create user and group accounts with desired permissions;
- Windows domain authentication support;
- LDAP directory authentication support;
- multi-factor authentication support;
- ability to create multiple databases;
- user permissions can be set for databases, folders or even individual records;
- easy deployment via Group Policy;

Secure custom data storage

- data is reliably stored in an encrypted database, which is handled by Firebird SQL Server Embedded;
- database and folder fields can be fully customized. It is possible to add/modify/remove fields for individual folder or entire database;
- Files can be attached to database records;
- export and import to/from CSV and TXT files;
- printing and ability to create custom print templates;
- backup servers to improve data availability;
- API to access data via scripting;

Other features

- autofill & form filler functionality. Currently it works in Chrome, Firefox, Edge, Internet Explorer and most of ordinary Windows applications;
- a portable version of Crypt-o can be installed to a removable device such as USB flash drive and used to access databases when offline;
- offline access to your data;
- Web interface;
- backup and restoring of databases;
- multilingual user interface;
- program can be minimized or closed to the system tray;
- handy and easy adjustable user interface;
- the program can be installed on any computer running the following operating systems: Windows 11, Windows 10, Windows Server 2019, Windows Server 2016, Windows 8.1/8, Windows Server 2012/R2, Windows 7, Windows Vista, Windows Server 2008/R2, Windows Server 2003, Windows XP.

3. License agreement

SOFTWARE LICENSE AGREEMENT

You should carefully read the following terms and conditions before using the software.

LICENSE AGREEMENT

This is the End User License Agreement (the "AGREEMENT") is a legal agreement between you ("LICENSEE"), the end-user, and Soft-o, the manufacturer and the copyright owner, for the use of the "**Crypt-o**" software product ("SOFTWARE").

By using this Software or storing this program on a computer drive (or other media), you are agreeing to be bound by the terms of this Agreement. If you do not agree with the terms of this Agreement, please remove this Software from your system.

This Software is not Freeware. However, you may install an Evaluation Version of this Software to test and evaluate the application during the Trial Period. If the program meets your requirements, and you wish to continue using the Software, after the Trial Period has ended, you have to purchase the Registered Version. If you do not want to continue using Software after the Trial Period, please remove this Software from your system.

You accept responsibility for any network usage costs or any other costs, incurred by using this Software.

TRIAL PERIOD

There is a free 30-day Trial Period for this Software.

EVALUATION VERSION

The Evaluation Version allows you to test and evaluate characteristics, features, and quality of this Software. You can also test the compatibility of the Software with your hardware and your operating system. The Evaluation Version may have some restricted features or limitations. Using this Software after the Trial Period without registration violates copyright laws and may result in severe civil and criminal penalties.

REGISTERED VERSION

The Registered Version has no restricted features or limitations.

LICENSE

The software is licensed on a per user basis. The license permits you to distribute the specified number of licensed copies of the Software entirely within your organization, solely for use by your employees. The software may be used by your employees worldwide. You may not give, transfer or sell licensed copies of the Software to your customer(s), or any third party, nor include such copies in, or with, products you sell. Subject to the number of copies licensed by your organization, users may access the software in any way that is convenient; for example, multiple users on a single machine, by accessing copies stored on local hard disks, or copies stored on network servers. The license is not a concurrent-use license. A license for the Software entitles your organization to duplicate the software as necessary for distribution within your organization to the specified number of users, in accordance with the Agreement.

SINGLE OFFICE SITE LICENSE

A single office site license authorizes you to install and use the product to any number of computers within a single site. You are entitled to upgrade to any future version of the software free of charge.

WORLDWIDE SITE LICENSE

A worldwide site license authorizes you to install and use the product to any number of computers belonging to your organization - no matter where they are located. You are entitled to upgrade to any future version of the software free of charge.

REGISTRATION KEY

The Registration Key may come as an unlock code, password, algorithm, or a service file. The Evaluation Version becomes Registered after the Registration Key has been applied. The Registration Key can be obtained directly from Soft-o or from its authorized dealer or representative only. You can only use the Registration Key that you own or have permissions to use, as an employee or member of a licensed group. You must not publicize or distribute the Registration Key (or a part of it) without the permission of Soft-o.

UPDATES

The Software is updated in major releases (e.g. 1.0, 2.0, 3.0), minor releases (e.g. 1.1, 1.2, 1.3) and patches (e.g. 1.0.15, 1.0.16, 1.0.17). Major releases involve significant changes in functionality and are released when such changes have been made for any reason. Minor releases include bug fixes and smaller functionality changes. Patches include bug fixes of urgent or high priority and are released as soon as the bugs can be corrected.

UPGRADES

If you had registered the Software, you are granted the right to receive (download) and install all the Minor Updates to the version initially installed free of charge. Installation of a Major Update may or may not require an upgrade fee, which is at sole discretion of the Copyright Owners.
Installation of the Minor Update does not require repeating the registration procedure, as the registration data will be inherited from the previous installation. Installation of a Major Update will or will not require new registration.

DISTRIBUTION

The Evaluation Version of this Software may be distributed freely through on-line services, bulletin boards, or other forms of electronic media, as long as the files are distributed in their entirety. Computer Magazines/Archives are authorized to distribute the Evaluation Version on any Cover Disk or CD-ROM without an individual permission. Please inform us via e-mail (info@soft-o.com) each time you distribute the evaluation copy.

RESTRICTIONS

YOU MAY NOT ALTER THIS SOFTWARE IN ANY WAY, INCLUDING CHANGING OR REMOVING ANY MESSAGES OR WINDOWS. YOU MAY NOT DECOMPILE, REVERSE ENGINEER, DISASSEMBLE OR OTHERWISE REDUCE THIS SOFTWARE TO A HUMAN PERCEIVABLE FORM. YOU MAY NOT MODIFY, RENT OR RESELL THIS SOFTWARE FOR PROFIT, OR CREATE ANY DERIVATIVE WORKS, BASED UPON THIS SOFTWARE. PUBLICATION OR DISTRIBUTING OF THE REGISTRATION KEY OR SOME OF ITS PART IS STRICTLY PROHIBITED!

DISCLAIMER

THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND SUITABILITY FOR A PARTICULAR PURPOSE. THE PERSON USING THE SOFTWARE BEARS ALL RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE. Soft-o WILL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES DUE TO LOSS OF DATA OR ANY OTHER REASON, EVEN IF Soft-o OR AN AGENT OF Soft-o HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL Soft-o BE LIABLE FOR COSTS OF ANY DAMAGES, EXCEEDING THE PRICE PAID FOR THE SOFTWARE LICENSE, REGARDLESS OF THE FORM OF THE CLAIM. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE, UNDERSTOOD IT, AND AGREED TO BE BOUND BY ITS TERMS.

4. Acknowledgements

We wish to thank the following people for their help in developing Crypt-o:

David Barton for DCPCrypt library;
Firebird development team for Firebird SQL Server;
OpenSSL Software Foundation for OpenSSL lbrary;
Jordan Russell for Inno Setup;
Lukas Gebauer for Synapse library.

Enetic IT Department for the Spanish translation;
Julien Després for the French translation;
Oliver Hirsch for the German translation;
Gašper Cas – Geniusnet d.o.o. for the Slovenian translation;
ICT Teamwork for the Dutch translation;
Enrico Francot for the Italian translation;
Nikola Smiljakovic for the Serbian translation;
Michael Jørgensen for the Danish translation;
Patrick Kvaksrud for the Norwegian translation;
Evgenii Frolov for the Greek translation;
Kristaps Lacis for the Latvian translation.

5. Quick Start

This topic briefly overviews the main commands. It is made to help you get started with Crypt-o password manager quickly. This topic is recommended for reading to both newbies and advanced users.

Creating user accounts

For the purpose of distinction of the access privileges to Crypt-o Server, the specific databases or objects of a database, it is necessary to create user accounts. To manage user accounts, choose **Tools > Administrative tools** from the menu. Then click on the **User management** link in the **Administrative tools** panel.

Creating databases and folders with required fields structure

Do not use the sample database for storing your data. Once the program is installed, please create a new database for your data.
Create a folders structure for storing your data. Create a required field structure and list columns to be displayed for each folder. The field structure can be copied from the sample database. To have that done, simply copy a folder to your database and delete the demo records from it.

Importing data to the program

Once your database and folders structure are created, you can import your data, if you have them stored in a text file with delimiters or in the **.csv** format (Excel can save data to **.csv** files). First, select the folder to import the data to, and then select the **Database > Import...** item on the menu.
Also you can import a Crypt-o database including all advanced features like images, file attachments, user accounts, object permissions.

Configuring and using form auto-fill

The program allows entering data to forms automatically and filling out forms on demand. Hotkeys, browser or system tray menu items can be used to call the auto-fill manually.

All forms that are "known" to the program will be filled out automatically. To have the "unknown" form filled automatically in the future, you will need to enter the required data manually for the first time and save the data to the program by selecting the **Save form data to Crypt-o** item on the browser's popup menu (or by selecting the same item in the program's tray menu) or press the hotkey **Alt+Win+S**.

By default, Crypt-o will ask whether you want to save the form data you have entered to the database once you click on the Submit button. For more information on configuring the automatic form filling, please read the Integration :: Form filling topic.

If the database already has a record with the data that you want to enter in the current form, you can call the auto-fill by selecting the **Fill out form using Crypt-o** item on the browser's popup menu (or by selecting the same item in the program's tray menu) or press the hotkey **Alt+Win+L**. From now on, the form will be filled out automatically, since the program will remember which record in the database it has to use for the current form.

For more information on filling out forms, please read the Form fill out and form data saving topic.

6. Working with Crypt-o

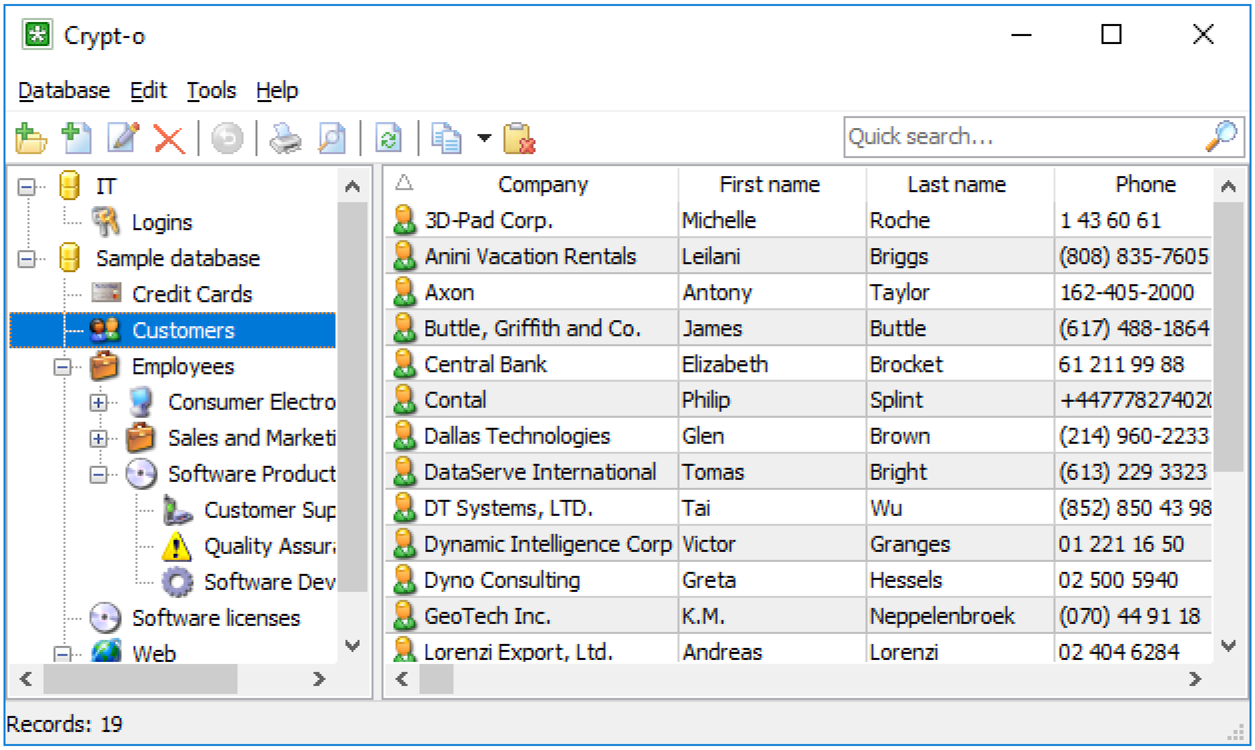
- Quick Start
- Working with databases
- Working with data
- Form fill-out and form data saving
- User management
- Audit log
- Password generator
- Configuration of Crypt-o
- Frequently Asked Questions

6.1. Working with databases

Crypt-o allows you to create several databases for storing information. List of all available databases is displayed in the left part of the program's window.

> **NOTE:** If your user account does not have a permission to access some database, it will not be displayed in the list of databases.

- Creating a new database
- Deleting a database
- Importing data
- Exporting data
- Backuping data
- Restoring data from a backup file
- Portable/Offline databases



Company	First name	Last name	Phone
3D-Pad Corp.	Michelle	Roche	1 43 60 61
Anini Vacation Rentals	Leilani	Briggs	(808) 835-7605
Axon	Antony	Taylor	162-405-2000
Buttle, Griffith and Co.	James	Buttle	(617) 488-1864
Central Bank	Elizabeth	Brocket	61 211 99 88
Contal	Philip	Splint	+44777827402
Dallas Technologies	Glen	Brown	(214) 960-2233
DataServe International	Tomas	Bright	(613) 229 3323
DT Systems, LTD.	Tai	Wu	(852) 850 43 98
Dynamic Intelligence Corp	Victor	Granges	01 221 16 50
Dyno Consulting	Greta	Hessels	02 500 5940
GeoTech Inc.	K.M.	Neppelenbroek	(070) 44 91 18
Lorenzi Export, Ltd.	Andreas	Lorenzi	02 404 6284

Records: 19

The main window

6.1.1. Creating a new database

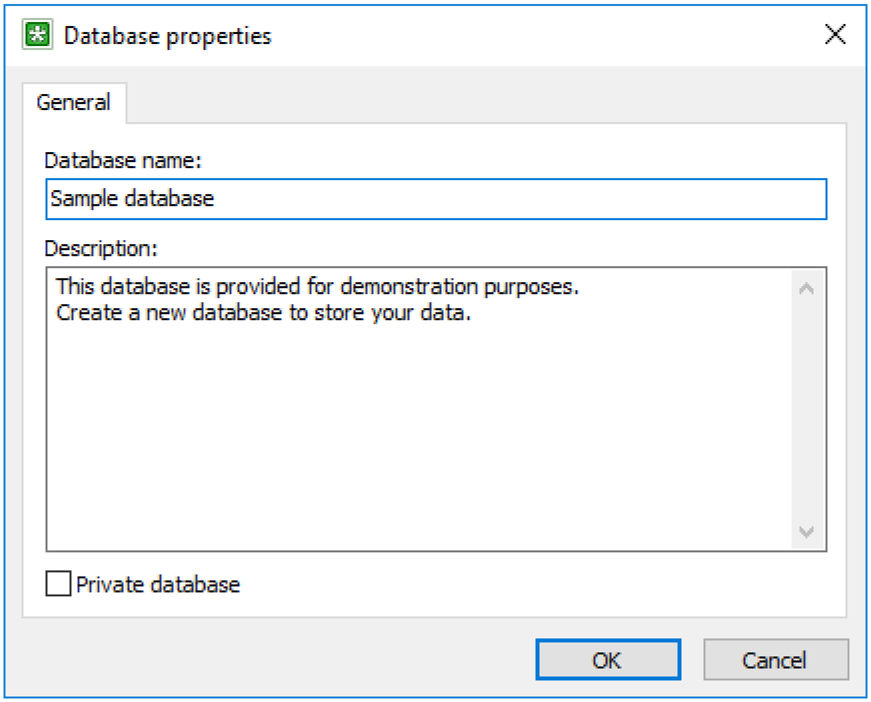
To create a new database choose **Database > Create database...** from the menu. The database properties window will appear. Enter a name for the new database and its description. Press **OK** to create the database.

☑ **Private database** - if this option is selected, the database will be private. Only the database owner will have full control over the database.

> **NOTE:** Even a system administrator is not able to access a private database without corresponding permission from the database owner. If a private database is abandoned (e.g. a user account of the database owner has been deleted), a system administrator can take ownership of this database by editing permissions in the User management.

> **NOTE:** Your user account must have a permission to create new databases.

Your user account will be set as the owner of the newly created database. A database owner is allowed to perform any operation in the database.



Database name: Sample database

Description:
This database is provided for demonstration purposes.
Create a new database to store your data.

□ Private database

The Database properties window

6.1.2. Deleting a database

To delete a database choose **Database > Delete database...** from the menu.

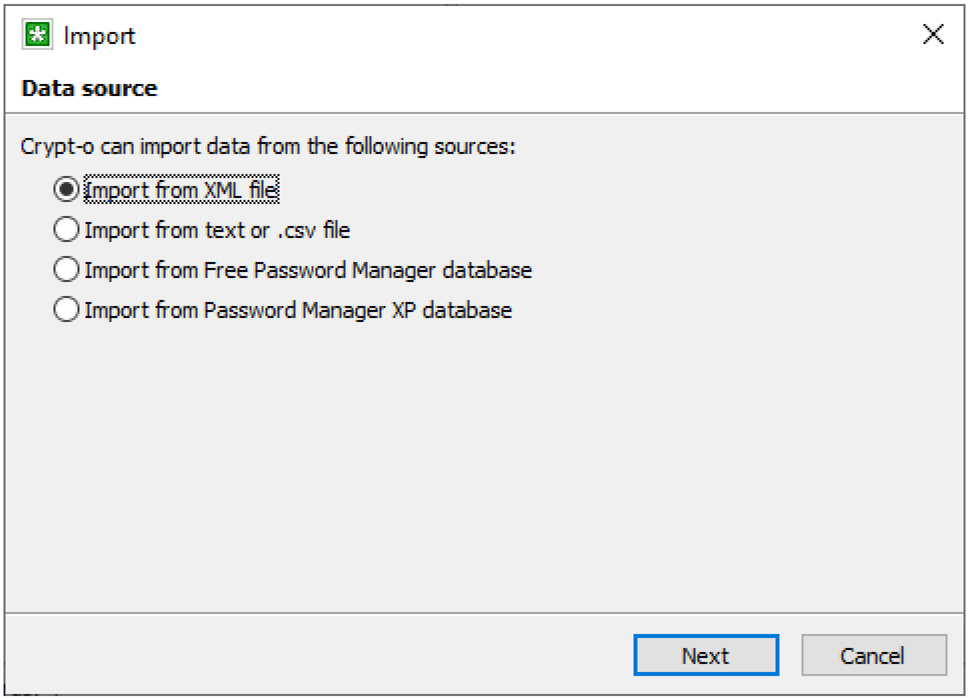
NOTE: Your user account must have a database owner privilege to delete the database.

⚠ **WARNING:** A database file is completely wiped from the file system during deletion. The only way to restore the database is to perform a full restore from a backup file.

6.1.3. Importing data

Crypt-o can import data from **XML files**, **text files** with delimiters and from **.csv files** (these ones can be created with Excel). Also Crypt-o can import Free Password Manager databases and Password Manager XP databases including all advanced features such as images, file attachments, user accounts, object permissions.

To start the Import Wizard choose **Database > Import** from the menu. On the first page of the Wizard, choose a data source to import data from.



Data source

Crypt-o can import data from the following sources:

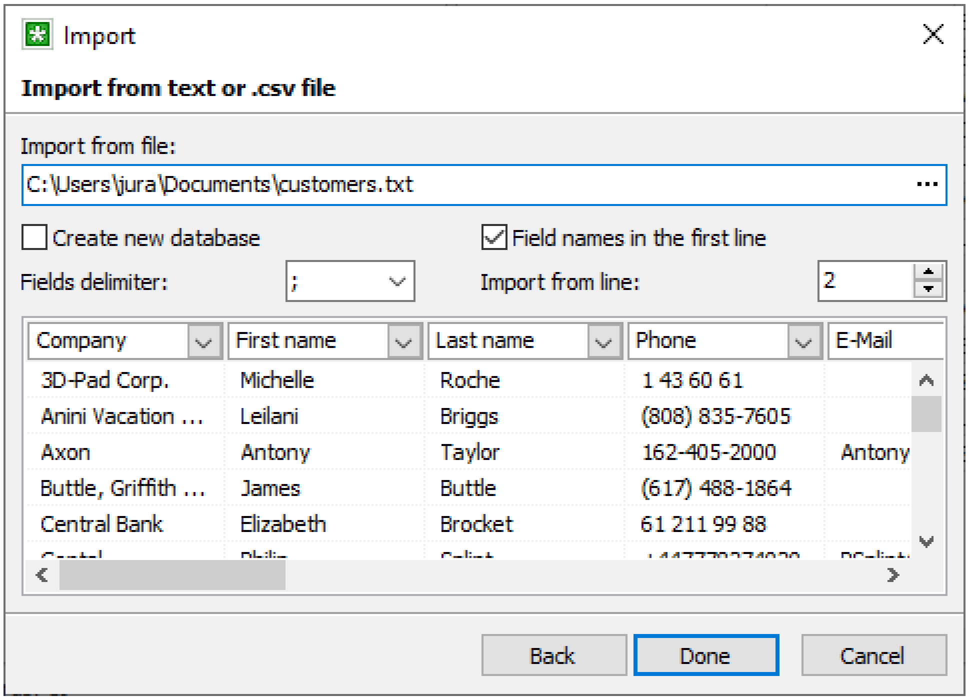
- ● Import from XML file
- ○ Import from text or .csv file
- ○ Import from Free Password Manager database
- ○ Import from Password Manager XP database

The import sources page

Importing from a text or .csv file

To perform the import, specify a text or .csv file to import data from. Then choose a proper **Fields delimiter** for that file, the line, from where data is to be imported, and the fields to store data into. Use the data preview to adjust the import parameters.
When the **Field names in the first line** option is selected Crypt-o will use data from the first line of the source file as field titles.
The data will be imported to the currently selected folder in the main window, unless you select the ☑ **Create new database** option. In that case a new database will be created and the data will be imported into that database.
When you are finished with the settings, click **Done** to start the import.

NOTE: It is possible to import data from a text file with predefined field names and the folder structure. To find out how the text file need to be formatted, just export to a text file some test database which contains several records and sub-folders with different fields structure. Don't forget to specify to export folder and field names in the export options.



Import

Import from text or .csv file

Import from file: C:\Users\jura\Documents\customers.txt

□ Create new database ☑ Field names in the first line

Fields delimiter: ;

Import from line: 2

Company	First name	Last name	Phone	E-Mail
3D-Pad Corp.	Michelle	Roche	1 43 60 61	
Anini Vacation ...	Leilani	Briggs	(808) 835-7605	
Axon	Antony	Taylor	162-405-2000	Antony
Buttle, Griffith ...	James	Buttle	(617) 488-1864	
Central Bank	Elizabeth	Brocket	61 211 99 88	

Text file import options

Importing from a XML file

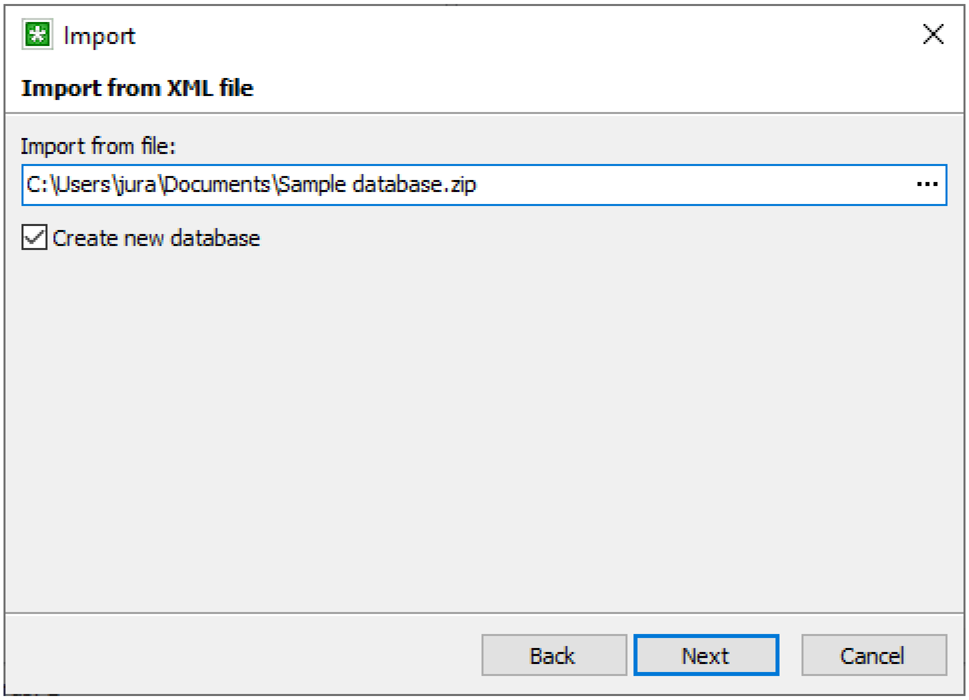
Crypt-o can import data from a specially formatted XML file or a ZIP archive containing a XML file. You can import complete database from a XML file - records, folders, permissions, images, file attachments, form filling information.

NOTE: To find out how the XML file need to be formatted, just export to a XML file some test database which contains several records and sub-folders with different fields structure.

To perform the import, specify a XML or ZIP file to import data from.

By default the ☑ **Create new database** option is selected and the data will be imported in a new database. Deselect this option to import data to the current folder.

Press **Next** to continue.



Import

Import from XML file

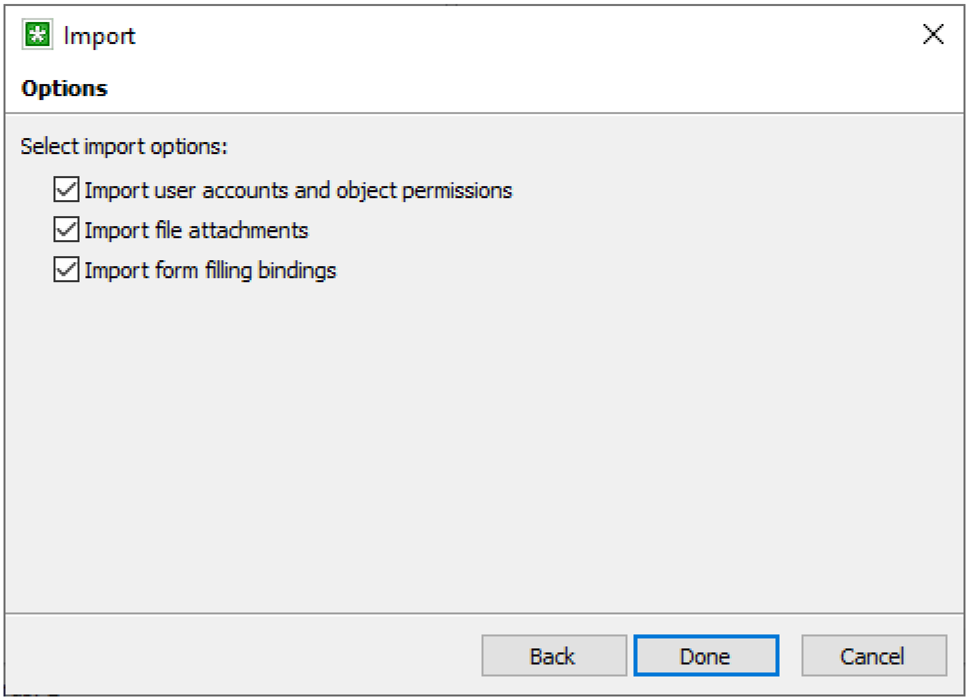
Import from file:

C:\Users\jura\Documents\Sample database.zip

☑ Create new database

XML file import options

Specify needed options on the import options page and press **Done** to start the import.



Import

Options

Select import options:

☑ Import user accounts and object permissions

☑ Import file attachments

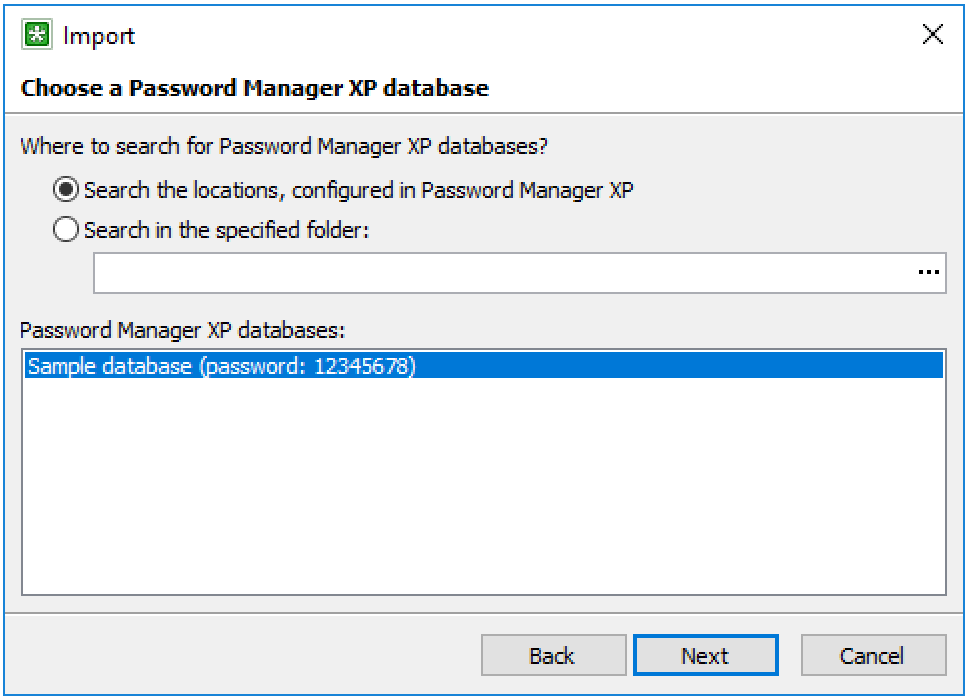
☑ Import form filling bindings

Import options

Importing a Free Password Manager or Password Manager XP database

NOTE: Only users with the **Create databases** privilege can import Free Password Manager or Password Manager XP databases.

Select a Free Password Manager or Password Manager XP database to import data from and click **Next**.



Import

Choose a Password Manager XP database

Where to search for Password Manager XP databases?

● Search the locations, configured in Password Manager XP

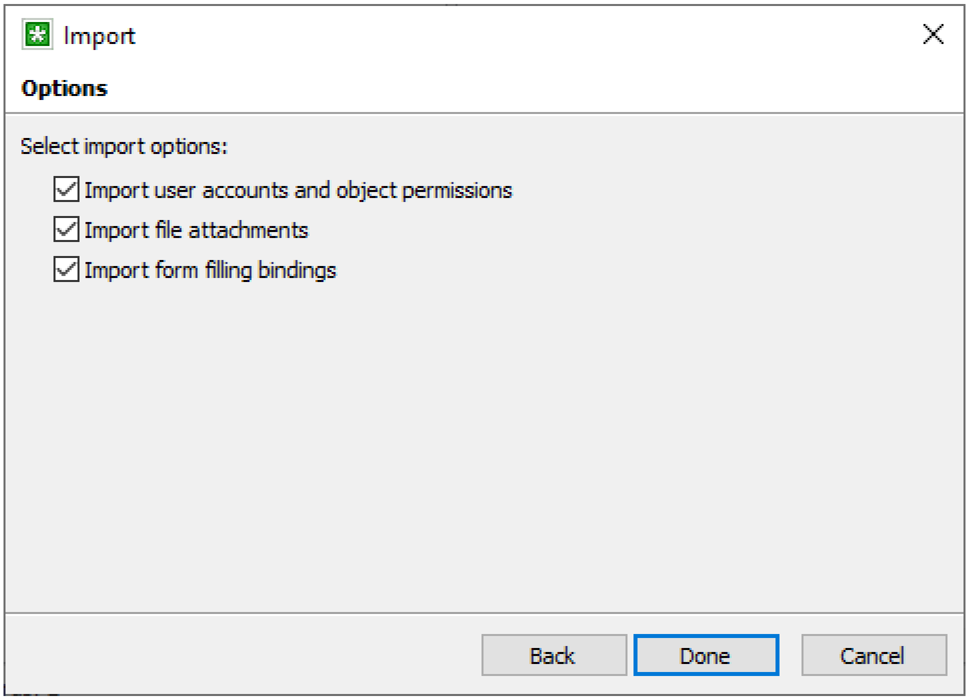
○ Search in the specified folder:

Password Manager XP databases:

Sample database (password: 12345678)

Import Password Manager XP database

On the next page specify a password to open the selected database and press **Next**. If the database has user accounts defined, you will be asked to enter a password for a built-in user with Administrator privileges.



Import

Options

Select import options:

☑ Import user accounts and object permissions

☑ Import file attachments

☑ Import form filling bindings

Import options

Specify needed options on the import options page and press **Done** to start the import.

6.1.4. Exporting data

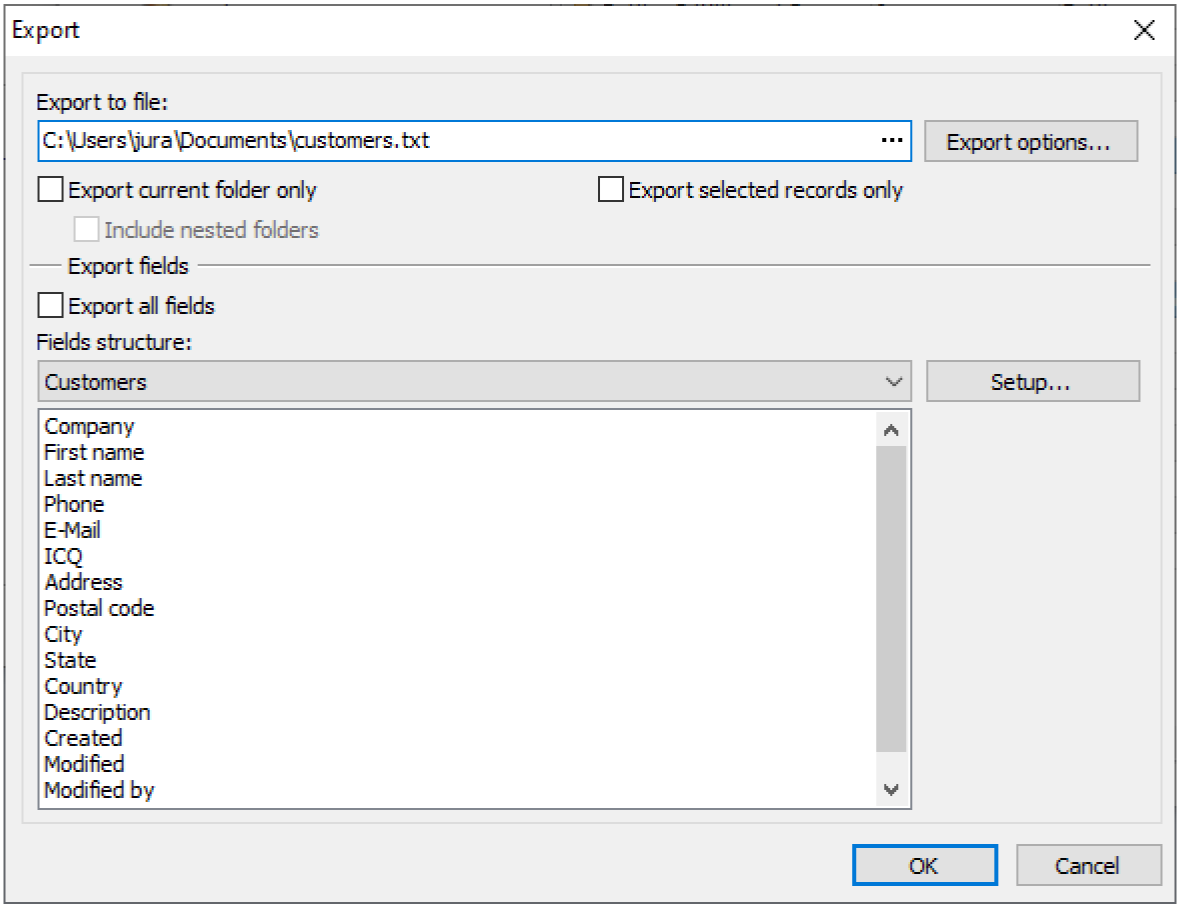
Crypt-o can export data to files of the following formats:

- XML file;
- XML file in a ZIP archive;
- Text file with delimiters;
- .csv file (can be opened by Excel);
- Rich text file (RTF);
- Excel file (Excel2003 or later);
- HTML file.

NOTE: The best way to export all data in a database is to use the **XML file (ZIP archive)** export file format. To perform the export, select a database, then select **Database > Export all...** in the menu and specify a file name of the output file.
All database data will be exported - records, folders, permissions, images, file attachments, form filling information.

NOTE: Only records with the **Print and Export** permission, granted for your user account, will be exported.

To export data to a file select **Database > Export...** in the menu. The export window will appear. Specify the target file and its type, export options and press **OK** to start the export.



Export to file: C:\Users\jura\Documents\customers.txt

□ Export current folder only □ Export selected records only

□ Include nested folders

Export fields

□ Export all fields

Fields structure: Customers

Company
First name
Last name
Phone
E-Mail
ICQ
Address
Postal code
City
State
Country
Description
Created
Modified
Modified by

The Export window

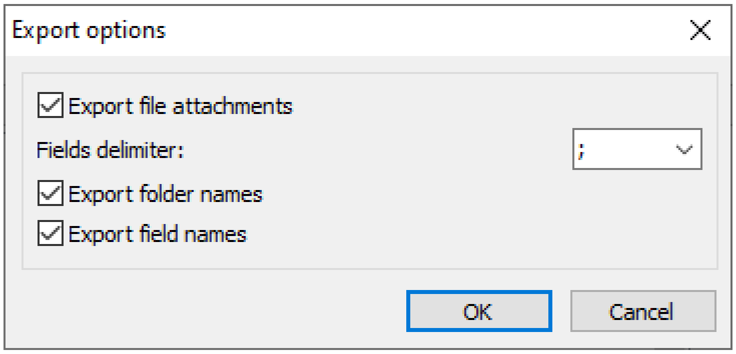
The following export options are available:

Option	Description

Export current folder only	If selected, only data from the currently selected folder will be exported.
Include nested folders	If selected, all nested folders of the currently selected folder will be also exported.
Selected records only	If selected, currently selected records will be exported only.
Export all fields	If selected, all data fields will be exported.
Fields structure	Displays which fields will be exported for every folder with different fields structure. To setup fields press the **Setup...** button.

To specify advanced export options for a chosen file format press the **Export options...** button.

The following advanced export options are available for text and .csv file formats:



☑ Export file attachments

Fields delimiter: ;

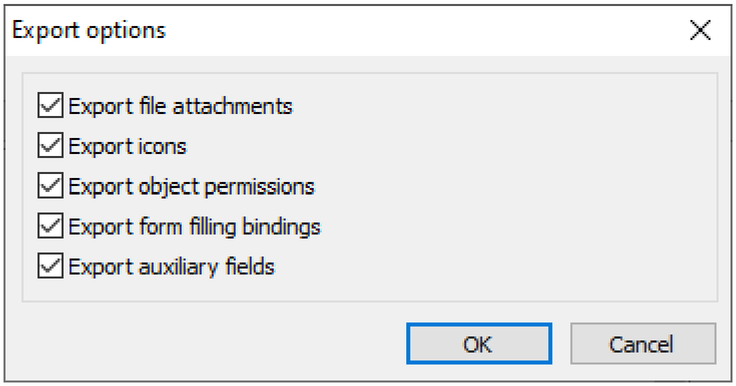
☑ Export folder names

☑ Export field names

Export options for text and .csv files

Option	Description
Export file attachments	If selected, file attachments will be exported and placed in the folder named **`<output_file_name>_files`**.
Fields delimiter	One or more character(s) are used to separate fields data.
Export folder names	If selected, the folder names will be exported.
Export field names	If selected, the field names will be exported.

The following advanced export options are available for XML file format:



☑ Export file attachments

☑ Export icons

☑ Export object permissions

☑ Export form filling bindings

☑ Export auxiliary fields

Export options for XML files

Option	Description
Export file attachments	If selected, file attachments will be exported and placed in the folder named **`<output_file_name>_files`**.

Export icons	If selected, custom icons images will be exported and placed in the folder named `<output_file_name>_files\icons`.
Export object permissions	If selected, users and object permissions will be exported.
Export form filling bindings	If selected, information needed to perform form filling will be exported.
Export auxiliary fields	If selected, the following auxiliary fields will be exported: Created, Modified, Modified by.

6.1.5. Backuping data

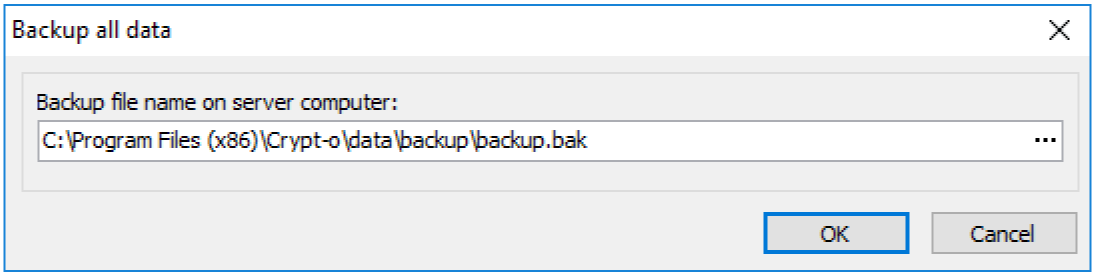
Crypt-o can create backups of all your data stored in all Crypt-o databases. Data backups can be made automatically or manually.

By default Crypt-o is configured to perform the following automatic backup tasks:

Task	Description
Daily backup	Creates backup copies every day at 1:00AM and keeps the last 7 backup files..
Weekly backup	Creates backup copies every week on Monday at 1:00AM and keeps the last 4 backup files.
Monthly backup	Creates backup copies every first day of month at 1:00AM and keeps the last 6 backup files.

By default, backup files, created by automatic backup tasks, are stored in the **backup** folder inside the program's data folder on a computer where Crypt-o Server is running. By default it is the **"C:\Program Files (x86)\Crypt-o\data\backup"** folder.

Manual backups can be made only by users with the **System administrator** privilege. To create a backup choose **Tools > Administrative tools** from the menu. Then click on the **Backup...** link in the **Administrative tools** panel. The backup window will appear. Specify a backup file name on the Crypt-o Server computer and press **OK** to start the backup.



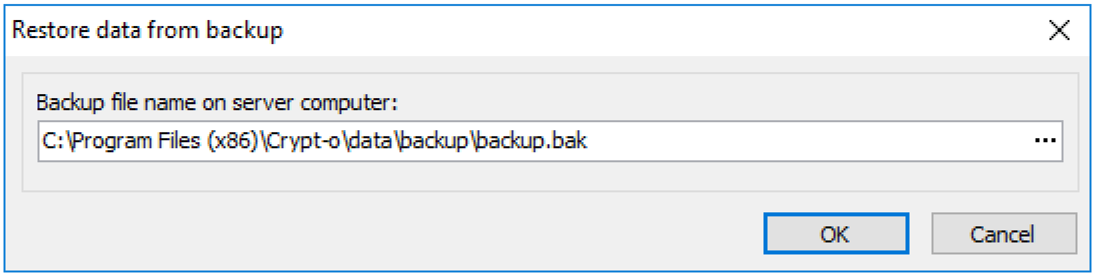
C:\Program Files (x86)\Crypt-o\data\backup\backup.bak

The Backup data window

6.1.6. Restoring data from a backup file

Only users with the **System administrator** privilege can restore data from a backup file. To do the restore, choose **Tools > Administrative tools** from the menu. Then click on the **Restore...** link in the **Administrative tools** panel. The restore data window will appear. Specify a backup file name on the Crypt-o Server computer and press **OK** to start the restore.

> **NOTE:** By default backup files are located in the **`backup`** sub-folder in the data folder of Crypt-o Server. The default location of backup files is **`C:\Program Files (x86)\Crypt-o\data\backup`**.



Restore data from backup

Backup file name on server computer:

C:\Program Files (x86)\Crypt-o\data\backup\backup.bak

The Restore data window

Restoring from a backup file using the command line

This method should be used, if it is not possible to log on to Crypt-o and perform the restore using the GUI method, described above.

- Stop the Crypt-o Server service.
- Open the command prompt as an Administrator on the server computer and execute the following command:
  `"C:\Program Files (x86)\Crypt-o\server.exe" -a -restore:"<backup_file_name>"`
    * Change the path to the `server.exe` file according to your installation.
    * Replace the `<backup_file_name>` parameter by a full path to an actual backup file.
- Start the Crypt-o Server service to start using the restored database.

6.1.7. Portable/Offline databases

Crypt-o offers you the following options to access databases when offline:

- **Offline access** to your databases using the currently installed Crypt-o Client application.
  Configure the offline access in the Crypt-o Client options.

- **Portable version** of Crypt-o installed to a removable device such as a USB flash drive.

It is possible to create a portable version of Crypt-o with offline copies of your databases. The portable version of Crypt-o can be installed to a removable device such as a USB flash drive. You can plug the device to any Windows computer, run Crypt-o directly from the device and access your databases.

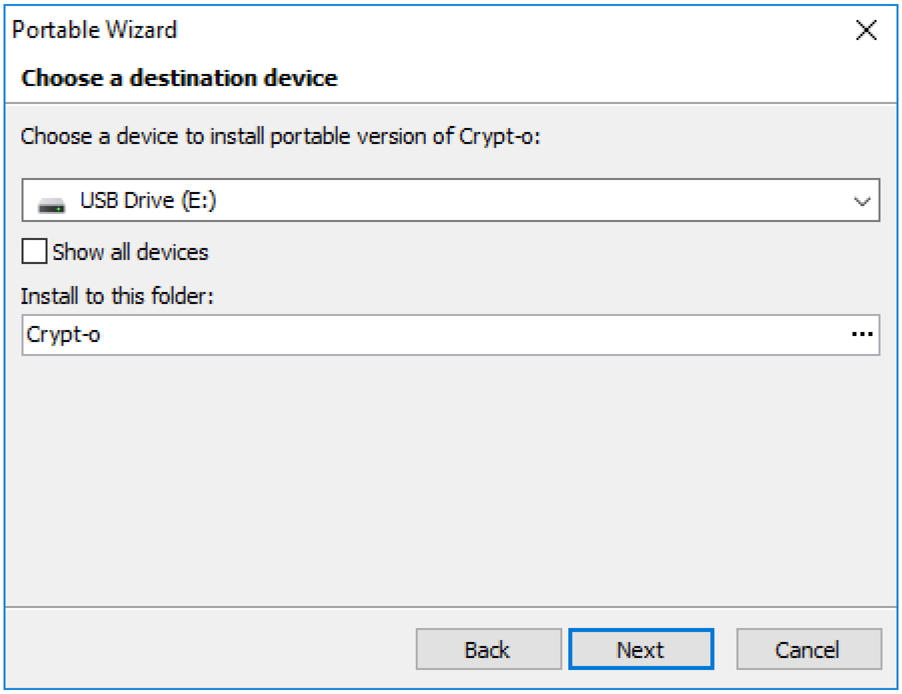
To create a portable version of Crypt-o choose **Tools > Create portable version** from the menu. The **Portable Wizard** will appear.

NOTE: Your user account must have the **Portable mode** permission for a database in order to create a portable version of this database.

NOTE: By default only records with the **Print and Export** permission, granted to your user account, will be available in a portable database. You can adjust this behavior using the **Take into account "Print and export" permission for portable version** system option on the Security page.

NOTE: You can configure expiration parameters for a portable version in the System options on the Security page.

Click **Next** to navigate to the next page.



Portable Wizard

Choose a destination device

Choose a device to install portable version of Crypt-o:

USB Drive (E:)

□ Show all devices

Install to this folder:

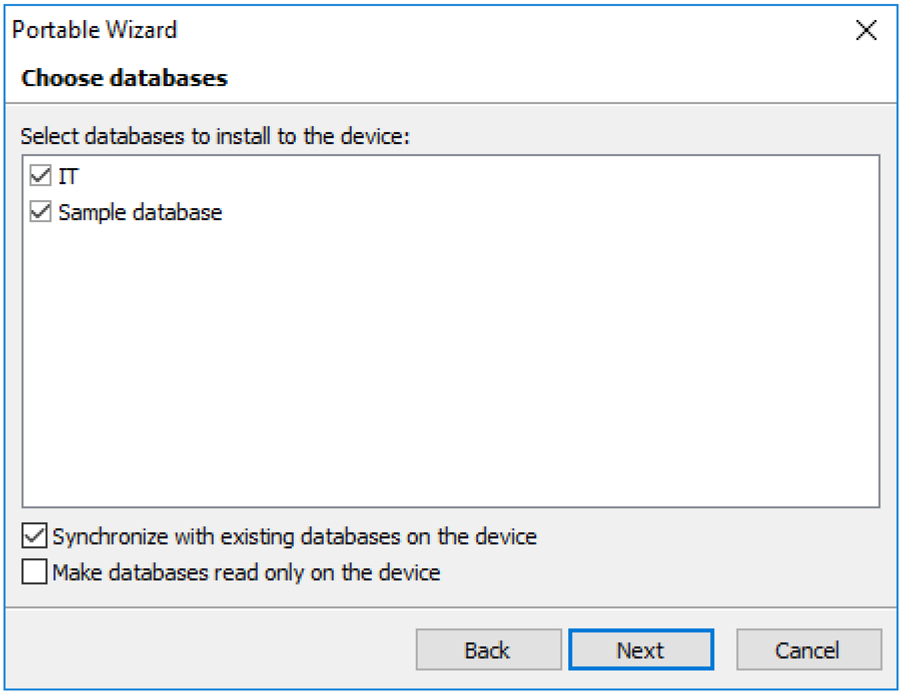
Crypt-o

Portable Wizard

Choose a destination device for installation of the portable version.

- ☑ **Show all devices** - when this option is selected, the program will display all devices available for the installation of the program, not only removable ones.
- **Install to this folder** - the destination folder on the device.

Click **Next** to navigate to the next page.



Portable Wizard

Choose databases

Select databases to install to the device:

☑ IT

☑ Sample database

☑ Synchronize with existing databases on the device

□ Make databases read only on the device

Portable Wizard

Choose databases to install with the portable version of Crypt-o.

- ☑ **Synchronize with existing databases on the device** - when this option is selected, the program will synchronize all changes, made in the existing portable database on the device, to the main server database.
- ☑ **Make databases read only on the device** - when this option is selected, all portable databases on the device will be marked as read only. Data modifications will not be allowed.

Click **Next** to start the installation.

After successful installation, the device will contain Crypt-o executable files and chosen databases. To access your data, run `Crypt-o.exe` file on the device and log on using your user name and password.

Quick portable version

To quickly create a portable version of Crypt-o choose **Tools > Quick portable version** from the menu or press **F9** . The silent installation, using the last used parameters, will be performed.

Limitations of a portable version

- Printing is disabled by default. Use the **Allow printing in portable version** option in the Crypt-o System options to enable it if needed.
- Fields customization is not possible.
- Creation of new databases is not possible.

6.1.8. Repairing databases

Crypt-o databases can be corrupted due to many factors such as power failure, OS failure, hardware failure, etc. Not always there is a fresh backup copy to fix the database corruption by restoring the backup.
Crypt-o has a built-in function to perform the database integrity check and repair. Though it may not work for severe database corruptions.

If you are able to log on to Crypt-o you can rebuild a database to ensure it contain no errors. To perform the rebuild, select a database and click **Database - Rebuild...** in the menu.

If it is not possible to log on to Crypt-o, you need access to the computer where Crypt-o Server is running.
To perform the database check and repair do the following on the server computer:

- Stop the Crypt-o Server service.
- Open the command prompt as an Administrator on the server computer and execute the following command:
  `"C:\Program Files (x86)\Crypt-o\server.exe" -a -checkdb"`
  * Change the path to the `server.exe` file according to your installation.
- You will see a message that the database check will be performed at the server start.
- Start the Crypt-o Server service.

After that, when you log on to Crypt-o and access databases they will be checked for errors. If there are errors, the repair will be performed.

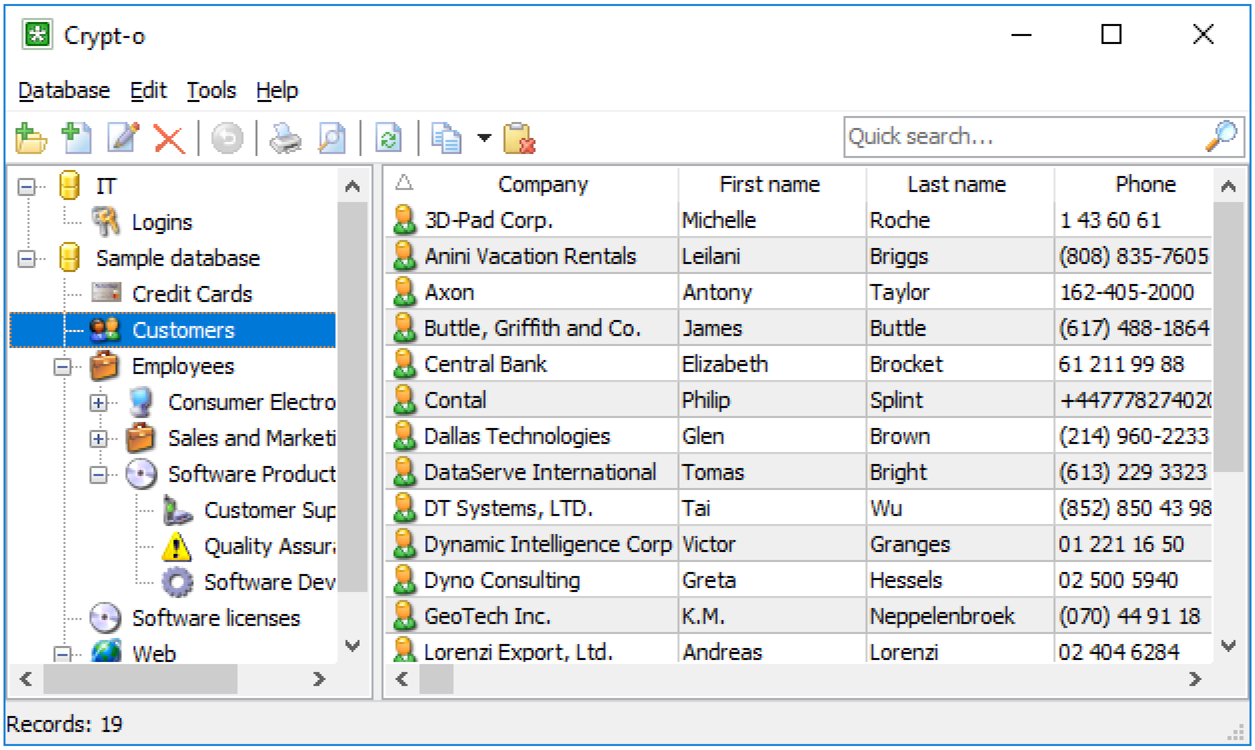
📝 **NOTE:** You can omit the database integrity check and force the database repair by specifying the **`-checkdb:repair`** command line switch instead of the **`-checkdb`** switch.

6.2. Working with data

The Crypt-o main window is divided by two parts. Databases and folders tree is displayed in the left part of the main window. A records list of the currently selected folder is displayed in the right part of the main window.
To create a new folder click on the **New folder** button on the toolbar or choose **Edit > New folder** from the menu.
To edit a folder name, select the folder and press **F2** key.
To edit folder properties, select the folder and choose **Edit > Properties...** from the menu.
To delete a folder, select it and press **Del** key or click on **Delete** button on the toolbar.
You can revert the last modifications by using the Undo function. To undo press **Ctrl+Z** keys or choose **Edit > Undo** in the menu.

> **NOTE:** You can use "**Ctrl +**" and "**Ctrl -**" keys to recursively expand and collapse sub-folders of the currently selected folder.

- Customizing the fields' structure
- Creating and editing records
- Selecting several records
- Deleting records
- Copying and moving records
- Copying protected fields to the clipboard
- Working with files
- Adding custom icons
- Setting up columns' appearance
- Printing
- Object permissions



Company	First name	Last name	Phone
3D-Pad Corp.	Michelle	Roche	1 43 60 61
Anini Vacation Rentals	Leilani	Briggs	(808) 835-7605
Axon	Antony	Taylor	162-405-2000
Buttle, Griffith and Co.	James	Buttle	(617) 488-1864
Central Bank	Elizabeth	Brocket	61 211 99 88
Contal	Philip	Splint	+44777827402
Dallas Technologies	Glen	Brown	(214) 960-2233
DataServe International	Tomas	Bright	(613) 229 3323
DT Systems, LTD.	Tai	Wu	(852) 850 43 98
Dynamic Intelligence Corp	Victor	Granges	01 221 16 50
Dyno Consulting	Greta	Hessels	02 500 5940
GeoTech Inc.	K.M.	Neppelenbroek	(070) 44 91 18
Lorenzi Export, Ltd.	Andreas	Lorenzi	02 404 6284

Records: 19

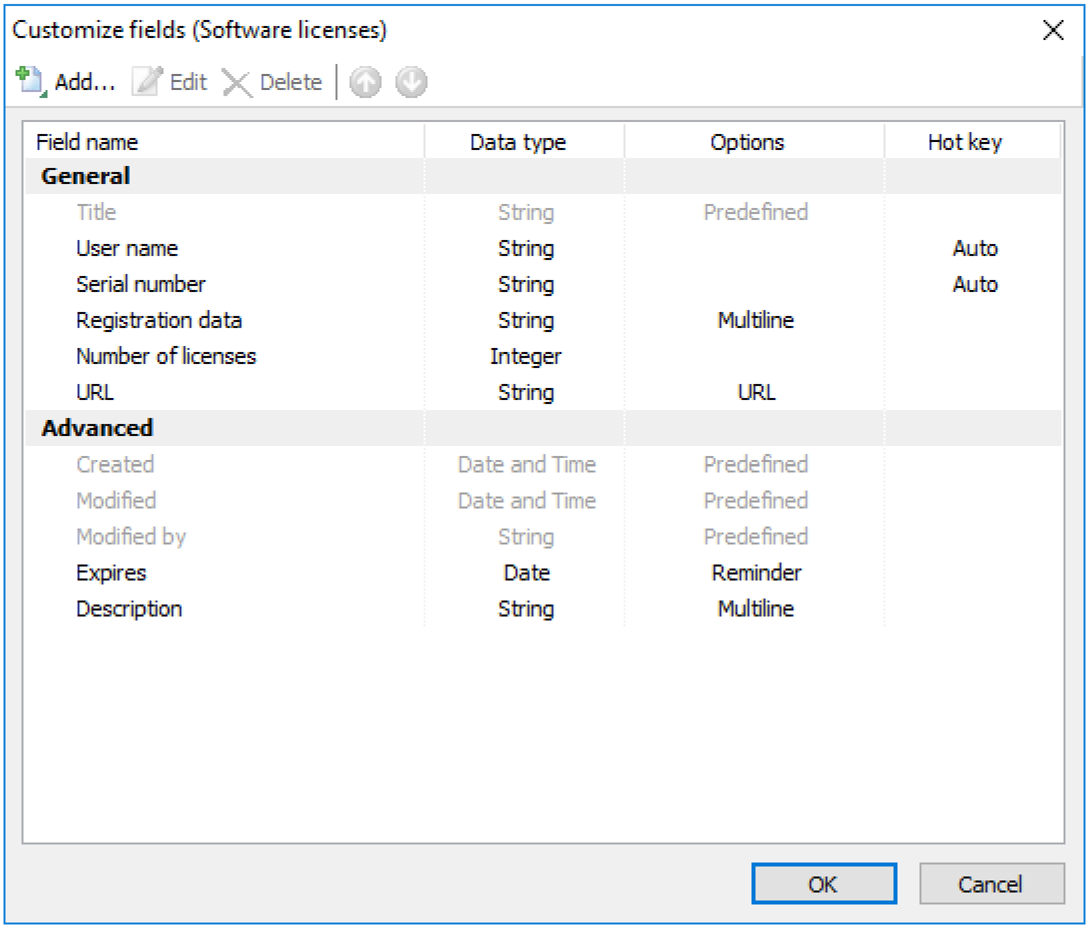
The main window

6.2.1. Customizing the fields' structure

You can customize the data fields' structure in the database for each folder or a group of folders, at your own discretion. Which means that you can create the folders for storing various data types, such as: credit cards, notes, passwords, contacts, software support e t.c. The fields' list is unlimited. The fields may be of various types and may be arranged in the editing window in the required way and on the specified tabs. At any time, you can modify the fields' naming and the arrangement order with no data loss.

To adjust the fields' structure, highlight the required folder and select the **Edit > Customize fields...** menu item. If the folder inherits its structure from a parent folder, a confirmation window appears. Press **Yes** to create an independent fields' structure for this folder and all of its subfolders; press **No** to edit the structure of the parent folder.

When you're done, a fields' structure editing window appears.



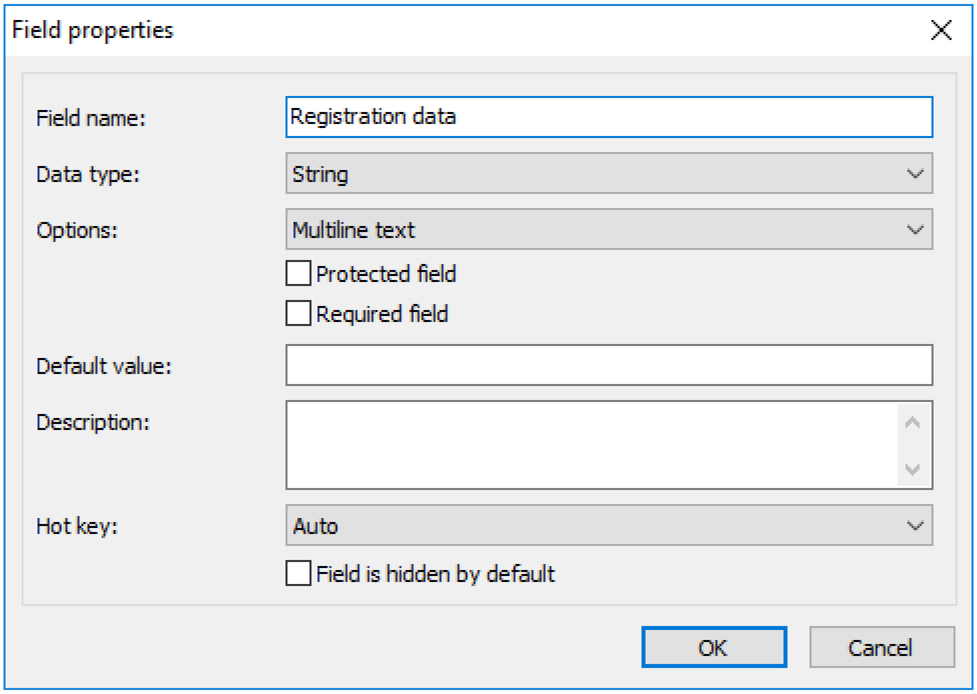
Field name	Data type	Options	Hot key
General			
Title	String	Predefined	
User name	String		Auto
Serial number	String		Auto
Registration data	String	Multiline	
Number of licenses	Integer		
URL	String	URL	
Advanced			
Created	Date and Time	Predefined	
Modified	Date and Time	Predefined	
Modified by	String	Predefined	
Expires	Date	Reminder	
Description	String	Multiline	

The customize fields window

The fields list is divided by sections, which are marked as bold. Each section constitutes a tab in the records editing and creating window. The tabs are arranged in the same order, as the sections in the list.
There also are a few mandatory fields, which cannot be removed, such as: **Title**, **Created**, **Modified**, **Modified by**.
The fields and sections can be moved using **Move up** and **Move down** buttons. The title field can not be move and is always placed first.

The following fields' structure editing actions are available:

- **Add...** - add a field or a section;
- **Edit...** - edit a field or a section;
- **Delete** - delete a field or a section;
- **Move up** - move a field or a section one position up;
- **Move down** - move a field or a section one position down.



Field name: Registration data
Data type: String
Options: Multiline text
□ Protected field
□ Required field
Default value:
Description:
Hot key: Auto
□ Field is hidden by default

The field properties window

Each field has the following parameters:

- **Field name** - a field's title, which is displayed in the records editing window and in the table's title;
- **Data type** - a field's data type: **String**, **Integer**, **Float**, **Date**, **Date and Time** or **Checkbox**;
- **Options** - an option for a field of **String** or **Date** data type.

  The following options are available for **String**-type fields:
  Regular string - a simple string field;
  Multiline text - multiple lines of text can be entered into this field;
  Clickable URL - a special field with clickable link to its contents;
  Predefined values - only predefined values can be selected;
  OTP generator - this field will provide you generated OTP (One-time Password) codes.

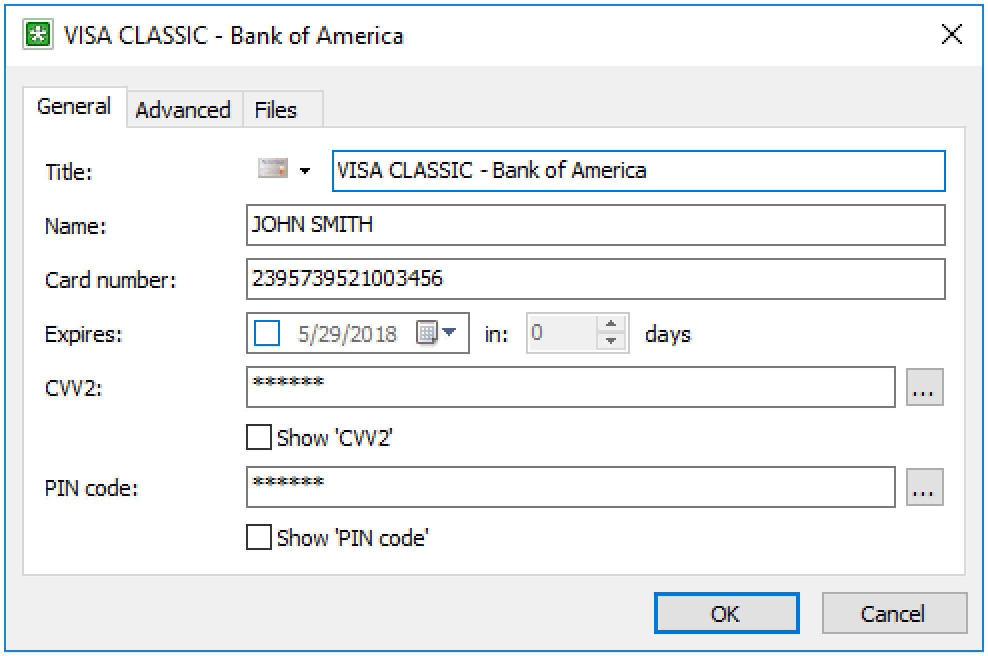
  The following options are available for **Date**-type fields:
  Regular date value - a simple date field;
  Reminder - a special date field. It allows you to specify future dates when Crypt-o will remind you of records that require attention.
  By default Crypt-o shows active reminders when you log on. Choose **Database - View reminders** in the main menu to view active reminders at any time. Also you can configure email notifications about active reminders in databases or specific folders.

- **Protected field** - data of this field will be hidden by default. To view the data it is needed to open the edit window for a record and click on a checkbox to show the field contents. When data of a protected field is viewed, Crypt-o writes the **View protected** event to the Audit log.
- **Required field** - a field requires a value to be entered;
- **Default value** - a default value for a field. The field is automatically populated with this value when a new record is created. The following macros can be used in a default value: `%DATETIME%`, `%DATE%`, `%TIME%`.
- **Description** - an optional description of a field;
- **Hot key** - a hot key (shortcut) to copy the field value to the clipboard;
- **Field is hidden by default** - if this option is selected, the field is not displayed by default in Crypt-o Client application and Web interface.

6.2.2. Creating and editing records

To create a new record press the **New record** button on the toolbar or choose **Edit > New record...** from the menu. To edit a record double click on it or press the **Edit record** button on the toolbar or choose **Edit > Edit record...** from the menu.

The record properties window will appear.



VISA CLASSIC - Bank of America

Title: VISA CLASSIC - Bank of America

Name: JOHN SMITH

Card number: 2395739521003456

Expires: □ 5/29/2018 in: 0 days

CVV2: *******

□ Show 'CVV2'

PIN code: *******

□ Show 'PIN code'

The record properties window

Enter the data in the corresponding fields at your discretion. See the Customizing the fields' structure topic to find out how to setup fields for entering data of different types.

Data of protected fields is hidden, unless you click on a checkbox to show the field contents. When data of a protected field is viewed, Crypt-o writes the **View protected** event to the Audit log.

Password generator can be used for generating strong passwords. In order to do so press the button to the right of the protected field's edit box.

Fields of type **URL** can be used to store links to the following objects:

- Web page address (`https://www.soft-o.com`).
- E-Mail address (`mailto:support@soft-o.com`).
- Local folder or file (`C:\Program Files` or `C:\Documents\Price.txt`).
- Remote folder or file (`\\Sever\Share` or `\\Sever\Share\readme.txt`).
- Executable file with command line parameters (`notepad.exe c:\readme.txt`). It is needed to specify the **.exe** extension for an executable file.
- Other records and folders in Crypt-o (`?d=<database_id>&f=<folder_id>&r=<record_id>`). Use the **Edit - Paste** shortcut menu to create shortcut records.

You can include field values of the current record in a URL-type field using the following notation: **`%%Field name%%`**
For example, you enter the following in a URL-type field:

```
mstsc.exe /v:%%Server name%% /u:%%User name%% /p:%%Password%%
```

When you click to that field, the Terminal Services client will be launched and values, specified in the **Server name**, **User name** and **Password** fields, will be used to automatically connect and log on to a remote server.

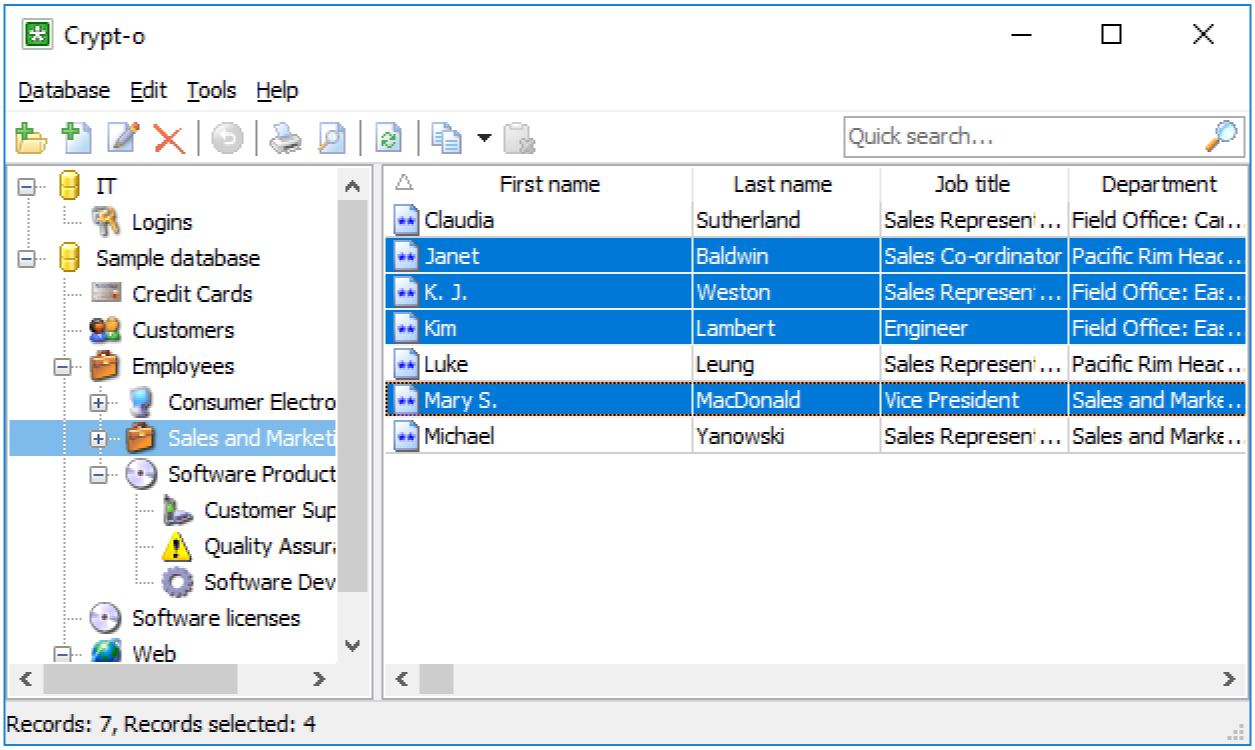
Fields of type **OTP generator** can be used to store and access **TOTP** codes generators which can be used to perform Multi-factor authentication in external services.
Press the **Configure OTP generator** tool button next to the OTP field to open the OTP configuration window.

You can set an image to appear on the records list for each record. At your discretion, you can assign images for records from the collection provided by the program or add your own images. See Adding custom icons topic for more information.

You can also attach files to a record by clicking on the **Files** page. See Working with files topic for more information.
Finally press **OK** to save the record.

6.2.3. Selecting several records

Sometimes it is needed to delete/move/copy several records at the same time. To select several records hold down **Ctrl** key and select records with mouse. To select a range of records click on the first record, hold down **Shift** key and click at the last record of the range. When the records are selected you can do the required operation.



First name	Last name	Job title	Department
Claudia	Sutherland	Sales Represen'...	Field Office: Ca...
Janet	Baldwin	Sales Co-ordinator	Pacific Rim Heac...
K. J.	Weston	Sales Represen'...	Field Office: Ea:...
Kim	Lambert	Engineer	Field Office: Ea:...
Luke	Leung	Sales Represen'...	Pacific Rim Heac...
Mary S.	MacDonald	Vice President	Sales and Marke...
Michael	Yanowski	Sales Represen'...	Sales and Marke...

Records: 7, Records selected: 4

Selected records

6.2.4. Deleting records

First of all, select records to be deleted in the records list. To delete the selected records press the **Delete** button on the toolbar or select **Edit > Delete** from the menu. Confirm the operation in the popup window.

6.2.5. Copying and moving records

First of all, select records to be copied or moved in the records list.

Moving records

To move selected records, drag and drop the them to a target folder.
Also you can choose **Edit > Cut** from the menu or press the **Ctrl+X** key combination to cut the records. Then open a target folder and choose **Edit > Paste** from the menu or press the **Ctrl+V** key combination to paste the records.

Copying records

To copy selected records, drag and drop the them to a target folder while holding the **Ctrl** key.
Also you can choose **Edit > Copy** from the menu or press the **Ctrl+C** key combination to copy the records. Then open a target folder and choose **Edit > Paste** from the menu or press the **Ctrl+V** key combination to paste the records.

Creating shortcuts to records or folders

You can create a shortcut record which points to other record or folder.
To do that select a record or folder and choose **Edit > Copy** from the menu or press the **Ctrl+C** key combination. Then open a target folder and choose **Edit > Paste shortcut** from the menu. The shortcut record will be created. The first record's field of type URL will contain the shortcut link to the source object.

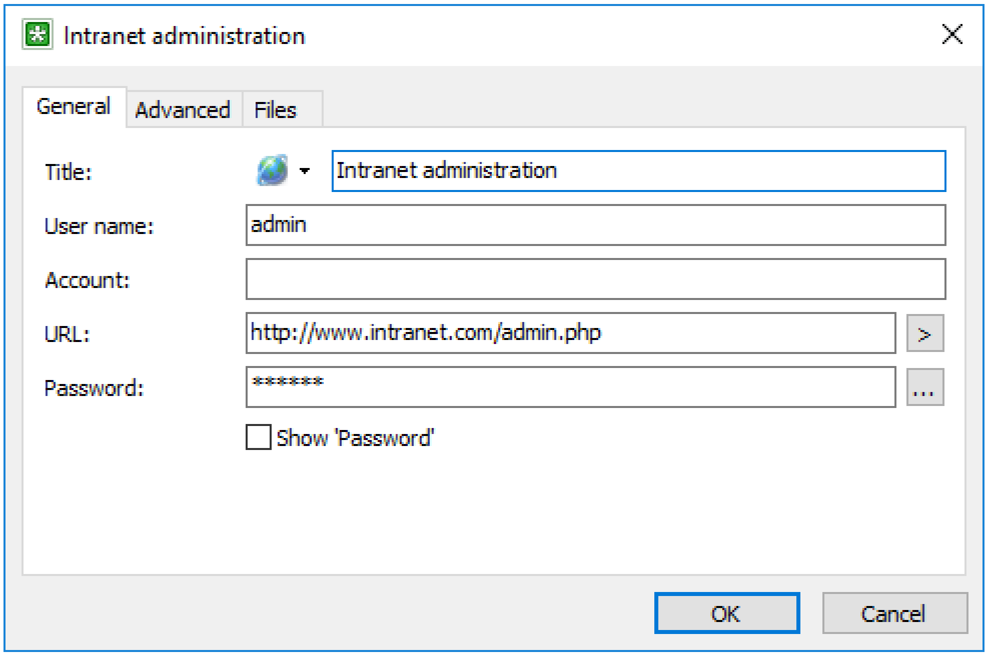
6.2.6. Cloning records

To create a new record based on an existing one, select the original record and then select **Edit > Clone record...** from the menu. The new record window will appear; data from the selected record will be pasted to the new record form automatically.

6.2.7. Copying protected fields to the clipboard

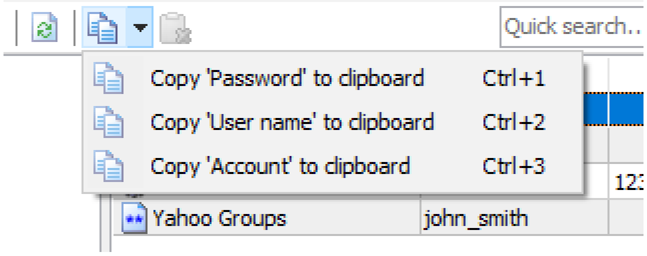
If you want to copy data of a protected field of the selected record to the clipboard, press the **Copy 'X' to clipboard** button on the toolbar or press **Ctrl+1** shortcut or select the corresponding item from the popup menu. The data then can be pasted from the clipboard to any application, but only once. Contents of the next non-protected field of the same record are copied to the clipboard also. Thus, the protected data is pasted at the first paste, and the non-protected - at subsequent paste. After that these data become unavailable to paste. Also the data will be unavailable to paste if not pasted within 1 minute. Once you need to paste it again you'll have to repeat the procedure (copy data to the clipboard). When program quits you won't be able to paste the data any more.

For example there is the following record:



Title: Intranet administration
User name: admin
Account:
URL: http://www.intranet.com/admin.php
Password: *******
☐ Show 'Password'

And the following options to copy to the clipboard are available:

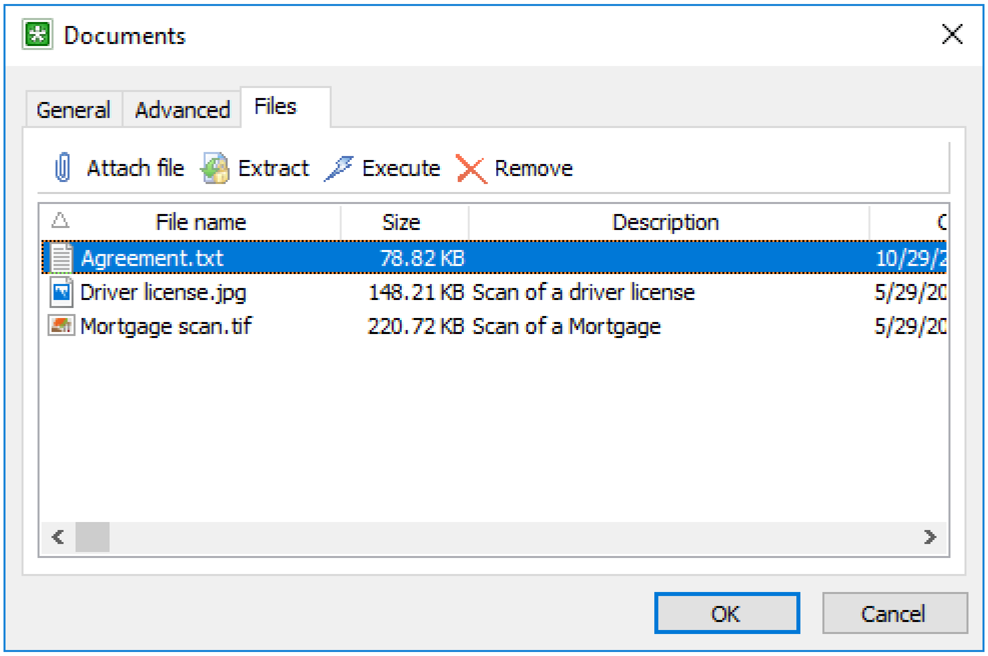

Quick search..
Copy 'Password' to clipboard Ctrl+1
Copy 'User name' to clipboard Ctrl+2
Copy 'Account' to clipboard Ctrl+3
123
Yahoo Groups
john_smith

When you choose the **Copy 'Password' to clipboard** item, you will be able to paste the password to some password input field in other application and immediately after that to paste the user name to some other input field. When you choose the **Copy 'User name' to clipboard** item, you will be able to paste the user name and immediately after that to paste the password.

NOTE: It is possible to turn off the secure clipboard copy using the Crypt-o Client options on the Security page.

6.2.8. Working with files

To securely store files you can attach them to records.



File name	Size	Description	C
Agreement.txt	78.82 KB		10/29/2
Driver license.jpg	148.21 KB	Scan of a driver license	5/29/20
Mortgage scan.tif	220.72 KB	Scan of a Mortgage	5/29/20

The Files page

Attaching files

To attach a new file, select the record to add the file to and then open it for editing. In the window that appears, open the **Files** tab and then click on the **Attach file** button. Next, select the file to be attached and then click on the **Open** button. Also you can use drag and drop to attach files.

Extracting files

To extract a file, select the record to extract the file from and then open it for editing. In the window that appears, open the **Files** tab, then select the file to be extracted (or select several files by holding the **Ctrl** key down) and then click on the **Extract** button. Next, select the folder where the files are to be saved and then click **OK**.
Another way to extract files is right-clicking on a record or folder and using the popup menu's **Extract files...** item. Also you can use drag and drop to extract files.

Executing files

To execute/open a file, select the record to extract the file from and then open it for editing. In the window that appears, open the **Files** tab, then select the file to be executed and then click on the **Execute** button. The file will be extracted to the temporary folder and executed/opened. Crypt-o will wipe the extracted file from the file system when you close the file.

Editing files description

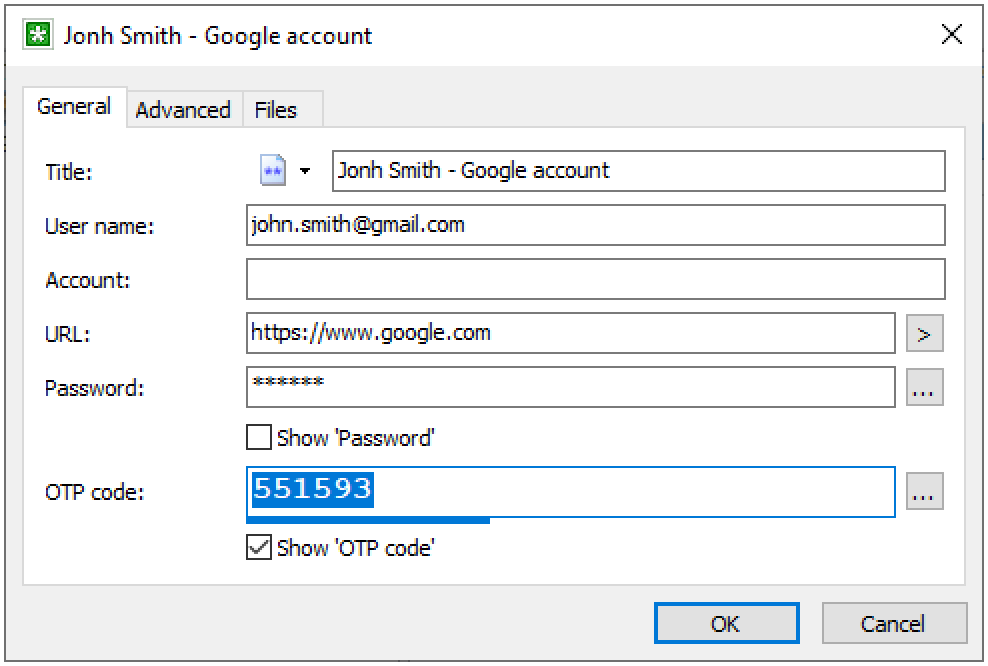
To edit a file description, select a file and press the **F2** key to the description show edit box. Press **Enter** to finish editing.

Removing files

To remove file, select the required record and open it for editing. In the window that appears, open the **Files** tab, select the file you need (or select several files by holding the **Ctrl** key down) and then click on the **Remove** button. Then confirm the removal by clicking on the **Yes** button in the confirmation window.

6.2.9. Generate OTP codes

Crypt-o allows you to store OTP code generators to be used by multiple users to perform Multi-factor authentication in external services.



Title: Jonh Smith - Google account

User name: john.smith@gmail.com

Account:

URL: https://www.google.com

Password: ******

☐ Show 'Password'

OTP code: 551593

☑ Show 'OTP code'

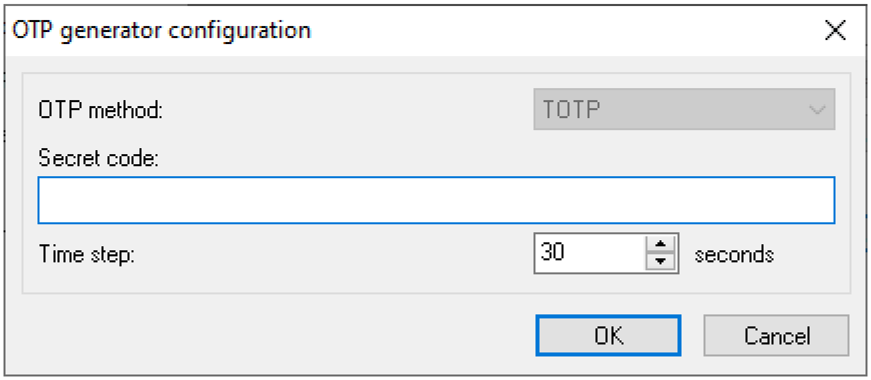
TOTP code generator

Crypt-o can generate TOTP codes.

To create an OTP code generator first you need to add a new **String** data filed of type **OTP generator** to a folder.

Then you can create records in this folder which will contain OTP code generators.

Press the **Configure OTP generator** tool button next to the OTP field in the record properties window to open the configuration window.



OTP method: TOTP

Secret code:

Time step: 30 seconds

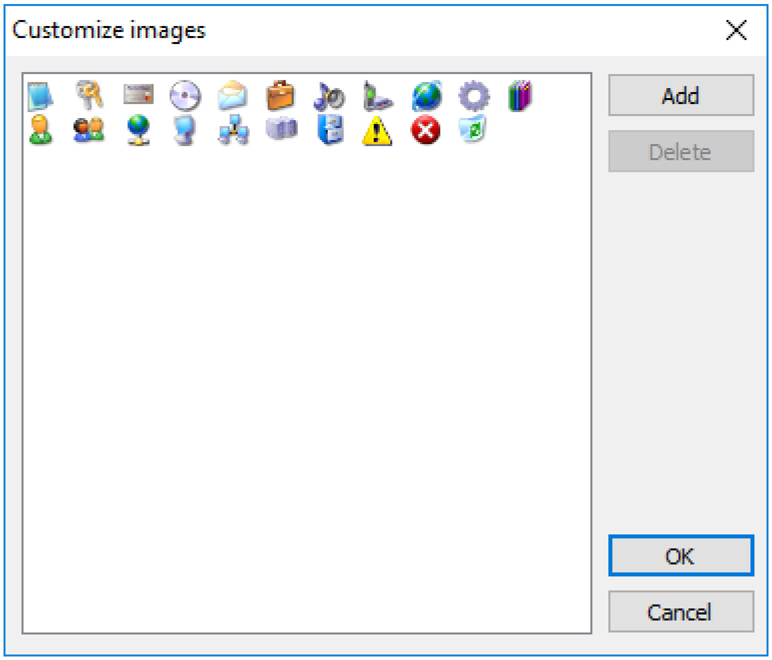
The OTP generator configuration window

Type the Base32 or Hex encoded **Secret code** and optionally change the **Time step**.

Press **OK** when done.

6.2.10. Adding custom icons

Crypt-o allows adding custom icon images for records and folders. Open a record or folder for editing. In the window that appears, click on the image selection combo box and then click on the **Customize...** button. That will open the **Customize images** window.

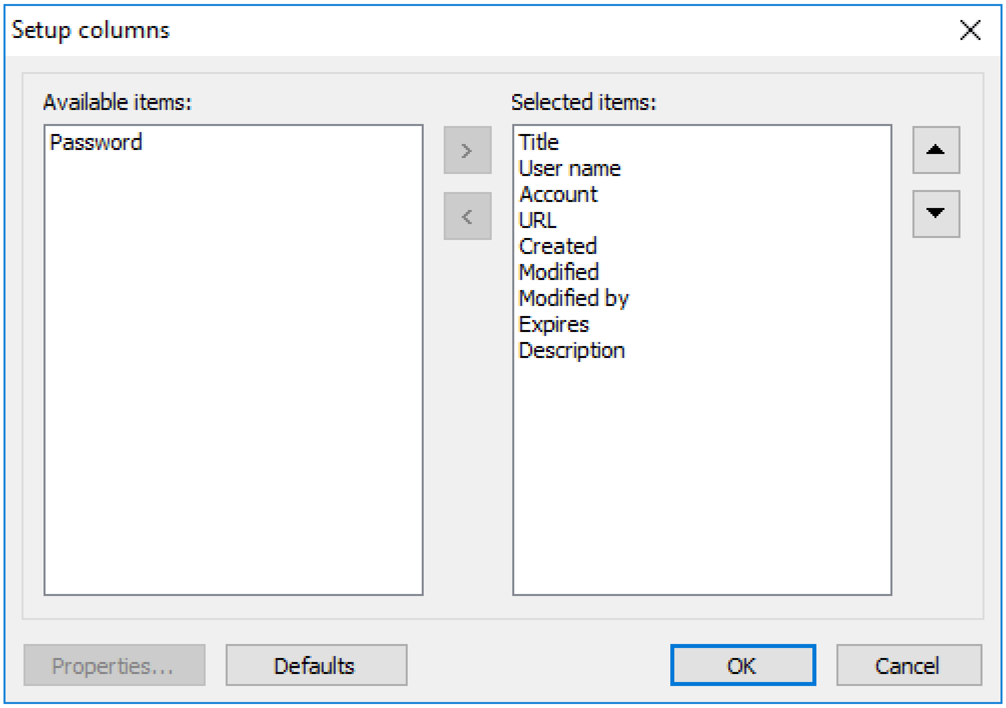


The Customize images window

In this window, you can add new custom images from image files, remove images, and copy images from other Crypt-o databases. The program supports the following image formats: ***.png**, ***.ico**, ***.bmp**. All images will be resized to 16x16 pixels; therefore, it is better to have the original images prepared in the 16x16 pixels format.

6.2.11. Setting up columns' appearance

Each folder in the program can have its own list of columns and the order how they are to appear on the list. To customize that, select **Tools > Setup columns...** from the menu. In the window that appears, set the columns to be displayed and the order they are to follow by using the **Up** and **Down** buttons. Click on the **Properties...** button to change the selected column's title, width and other properties. Click on the **Defaults** button to restore the default order and properties of the columns.



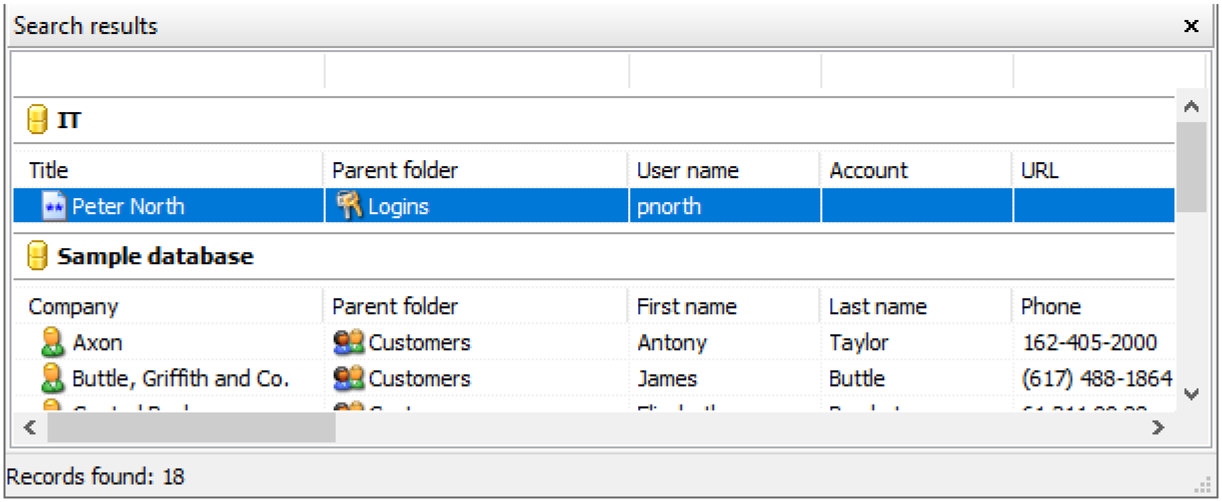
Available items:
Password

Selected items:
Title
User name
Account
URL
Created
Modified
Modified by
Expires
Description

The Setup columns window

6.2.12. Search

Crypt-o allows you to easily search data stored in databases.



Search results

IT

Title	Parent folder	User name	Account	URL
Peter North	Logins	pnorth		

Sample database

Company	Parent folder	First name	Last name	Phone
Axon	Customers	Antony	Taylor	162-405-2000
Buttle, Griffith and Co.	Customers	James	Buttle	(617) 488-1864

Records found: 18

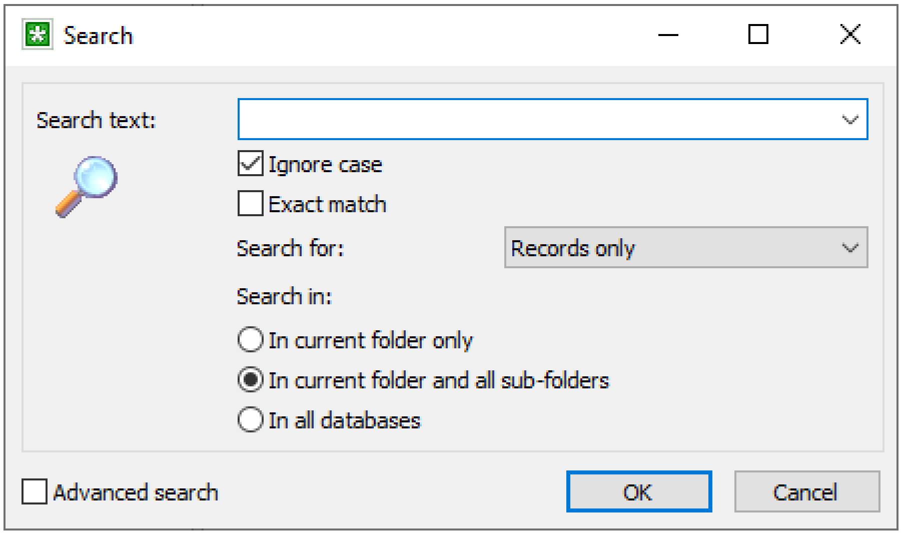
The Search results pane

Quick search

To quickly find records containing some text in the current folder and all sub-folders click the **Quick search** box in the top-right corner of the main window. Type a text and press Enter.

Search

To find records or folders and specify additional parameters choose **Database > Search...** in the main menu or press **Ctrl+F**.



Search

Search text:

☑ Ignore case

□ Exact match

Search for: Records only

Search in:

○ In current folder only

● In current folder and all sub-folders

○ In all databases

□ Advanced search

The Search window

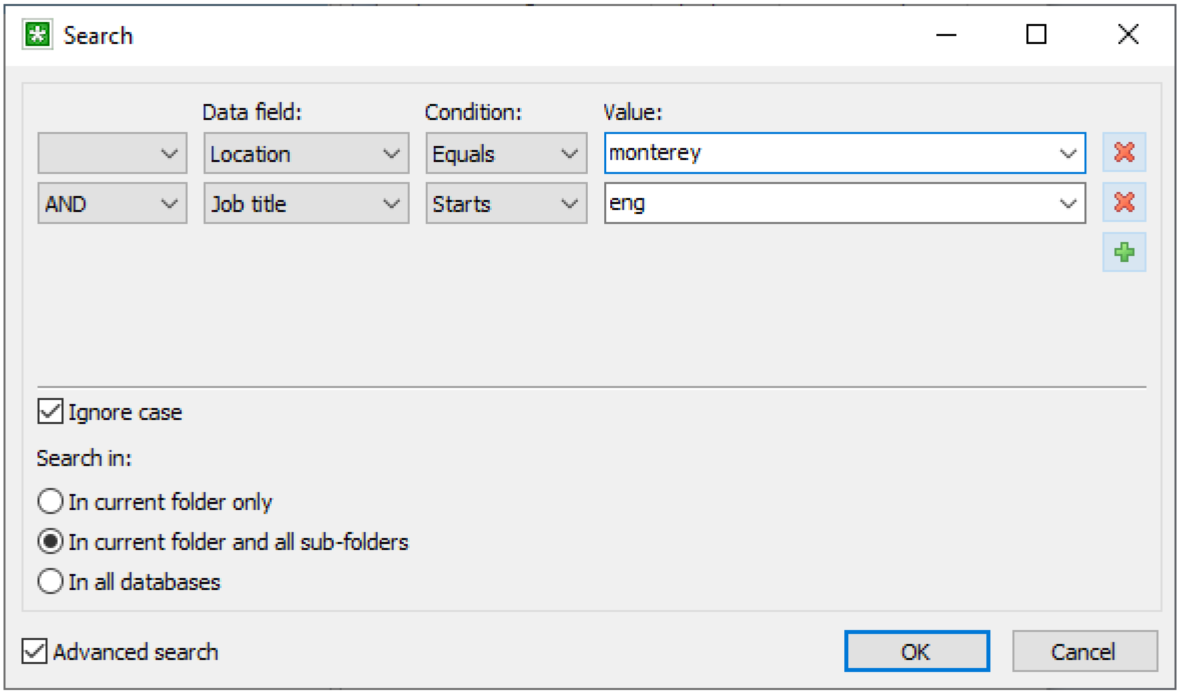
In the Search window you can specify the following parameters:

Search text - a text to be searched in records or folders.
☑ **Ignore case** - when this option is selected, the text will be searched ignoring difference between upper and

lower case letters.
☑ **Exact match** - when this option is selected, the whole contents of data fields is compared with the search text. Otherwise partial comparison is performed.
Search for - specifies which data object need to be searched and included in the search results: **Records only**, **Folders only**, **Records and folders**.
Search in - specifies the search scope: **In current folder only**, **In current folder and all sub-folders**, **In all databases**.

Advanced search

Using Advanced search you can construct and perform complex search queries.
To use Advanced search open the Search window by choosing **Database > Search...** in the main menu or by pressing **Ctrl+F**. Then enable the ☑ **Advanced search** option.



	Data field:	Condition:	Value:
	Location	Equals	monterey
AND	Job title	Starts	eng

☑ Ignore case

Search in:

○ In current folder only
● In current folder and all sub-folders
○ In all databases

☑ Advanced search

The Advanced search window

An advanced search query consists of several condition rows joined by logical operators.
To add a new query row press the **Add row** button.
To delete a query row press the **Delete row** button.

There are parameters of a query row:

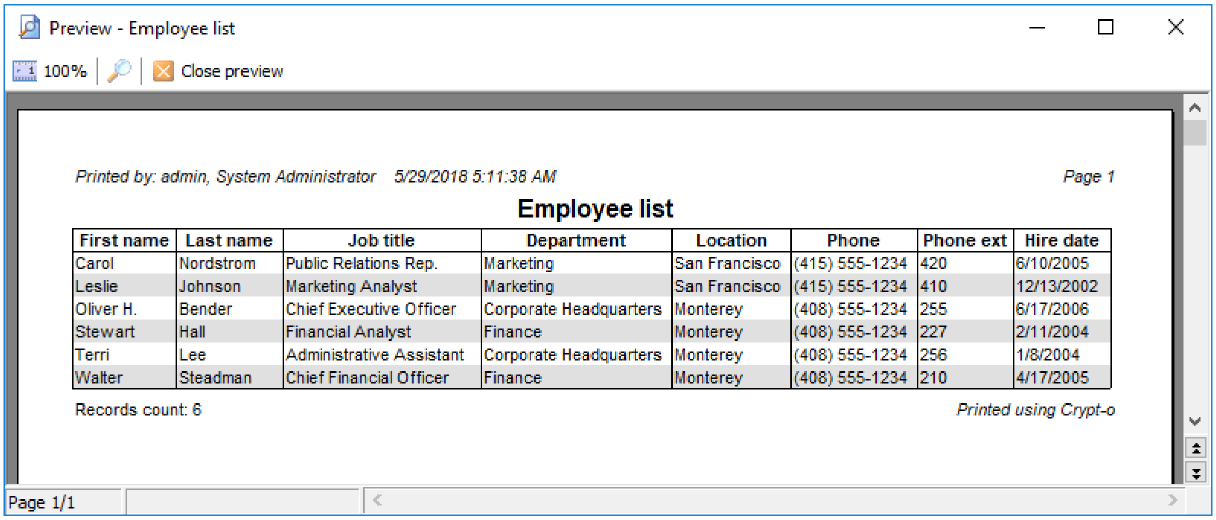
Logical operator:
NOT - reverses the condition of the row;
AND - this row and the previous row must all meet theirs conditions;
OR - either the condition of this row or the condition the previous row must be met.
Data field - a data field to be used in this query row.
Condition - a condition to be applied to values stored in the **Data field** and to the specified **Value**:
Equals - a value of the data field must be equal to the specified value;
Not equals - a value of the data field must be not equal to the specified value;
> - a value of the data field must be greater than the specified value;
>= - a value of the data field must be greater or equal than the specified value;
< - a value of the data field must be less than the specified value;
<= - a value of the data field must be less or equal than the specified value;
Contains - a value of the data field must contain the specified value;
Starts - a value of the data field must start with the specified value;
Ends - a value of the data field must end with the specified value;

6.2.13. Printing

Crypt-o allows you to print your data. You can either print data stored in the current folder or print all data stored in a database. You can create your own print templates with desired report name, columns to be printed, their titles, width, length, sequence, format and other parameters. Page orientation (portrait or landscape) and margins can be specified as well.

Printing data from a folder

To print data from a folder, select it and press the **Print** button on the toolbar. To see how the data will look like when printed out, press the **Print preview** button on the toolbar.



Printed by: admin, System Administrator 5/29/2018 5:11:38 AM *Page 1*

Employee list

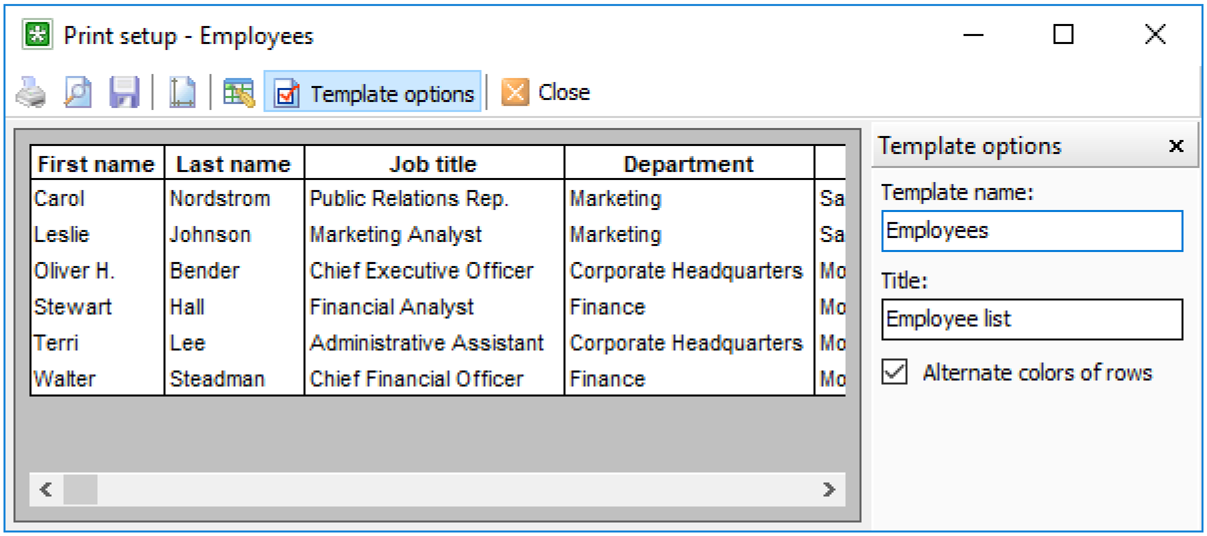
First name	Last name	Job title	Department	Location	Phone	Phone ext	Hire date
Carol	Nordstrom	Public Relations Rep.	Marketing	San Francisco	(415) 555-1234	420	6/10/2005
Leslie	Johnson	Marketing Analyst	Marketing	San Francisco	(415) 555-1234	410	12/13/2002
Oliver H.	Bender	Chief Executive Officer	Corporate Headquarters	Monterey	(408) 555-1234	255	6/17/2006
Stewart	Hall	Financial Analyst	Finance	Monterey	(408) 555-1234	227	2/11/2004
Terri	Lee	Administrative Assistant	Corporate Headquarters	Monterey	(408) 555-1234	256	1/8/2004
Walter	Steadman	Chief Financial Officer	Finance	Monterey	(408) 555-1234	210	4/17/2005

Records count: 6 *Printed using Crypt-o*

The print preview window

Configuring printed data appearance

To configure columns to be printed, their order and width and other parameters choose **Database > Print setup...** from the menu. The print setup window for the last used print template will appear.



First name	Last name	Job title	Department	
Carol	Nordstrom	Public Relations Rep.	Marketing	Sa
Leslie	Johnson	Marketing Analyst	Marketing	Sa
Oliver H.	Bender	Chief Executive Officer	Corporate Headquarters	Mo
Stewart	Hall	Financial Analyst	Finance	Mo
Terri	Lee	Administrative Assistant	Corporate Headquarters	Mo
Walter	Steadman	Chief Financial Officer	Finance	Mo

Template options ×

Template name: Employees

Title: Employee list

☑ Alternate colors of rows

The print template setup window

Use the mouse to change columns width and drag columns to change their order.
Press the **Columns setup** button on the toolbar to change columns' visibility, order, title, width and alignment.
Press the **Template options** button on the toolbar to change a title of the template.
Press the **Page setup** button on the toolbar to change page orientation and margins.

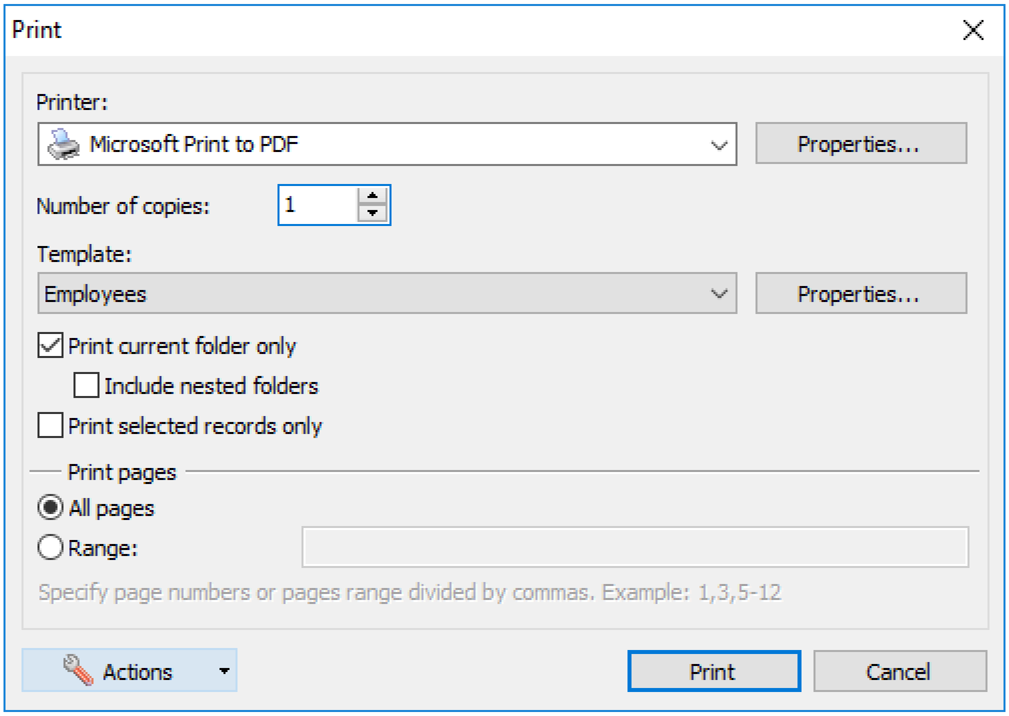
Use the **Print preview** button to see how your report will look like.

Printing the entire database

To print the entire database, choose **Database > Print...** from the menu. The print parameters window will appear. Deselect the ☑ **Print current folder only** option, choose the print template and printing parameters. Then, press **Print** to start printing.

Press the **Action** button to access additional commands:

- **Print Preview** to see how your report will look like.
- **Manage templates** to create/modify/delete print templates.
- **Save to file** to save the report in one of the following file formats:
  - Rich text file (RTF);
  - Excel file (Excel2003 or later);
  - HTML file.



Print

Printer: Microsoft Print to PDF

Number of copies: 1

Template: Employees

☑ Print current folder only

□ Include nested folders

□ Print selected records only

Print pages

● All pages

○ Range:

Specify page numbers or pages range divided by commas. Example: 1,3,5-12

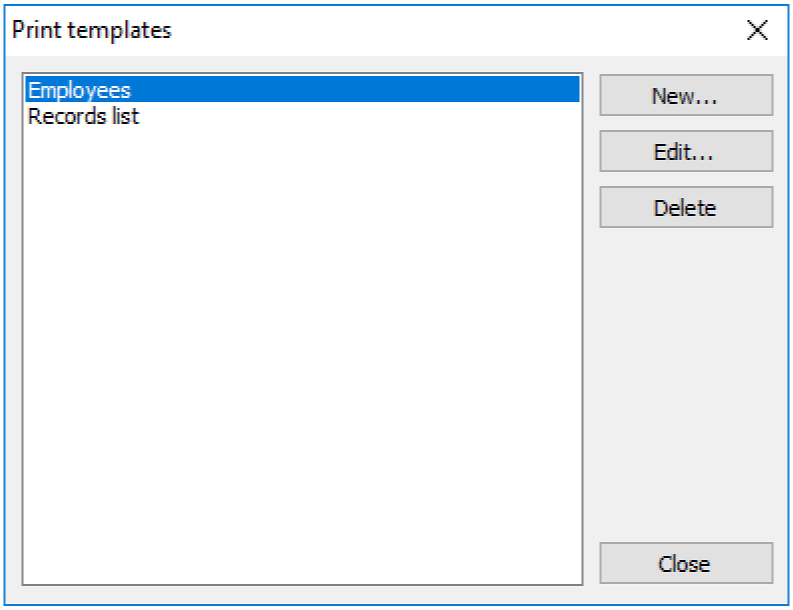
The print parameters window

Printing selected records only

To print selected records only, choose **Database > Print...** from the menu. The print parameters window will appear. Select the ☑ **Print selected records only** option, choose the print template and printing parameters. Then, press **Print** to start printing.

Managing print templates

To manage print templates, select **Database > Print...** from the menu and press the **Templates...** button. The window that appears will let you create, edit or delete print templates. To create a new template, press **New...** button and then setup template options, like the template name, columns to be printed and their parameters, etc.



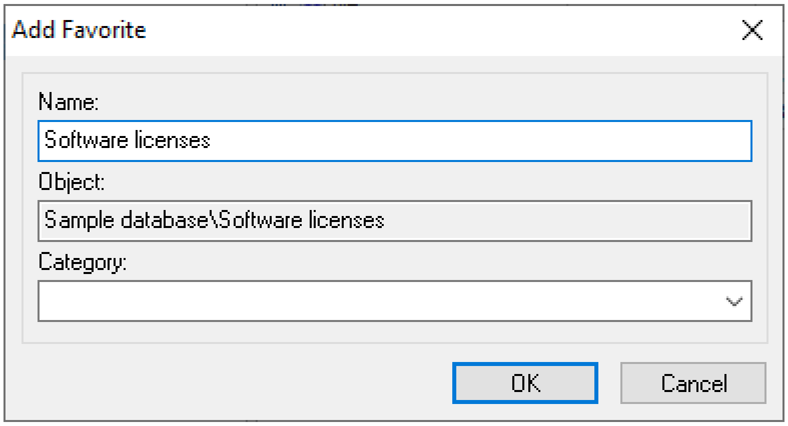
The print templates window

6.2.14. Favorites

You can add a shortcut for frequently used records or folders to the **Favorites** menu for further quick access.

NOTE: You can also create shortcut records in the database.

To add a currently selected record or folder to Favorites, select **Favorites - Add to Favorites...** in the menu.


Add Favorite

Name: Software licenses

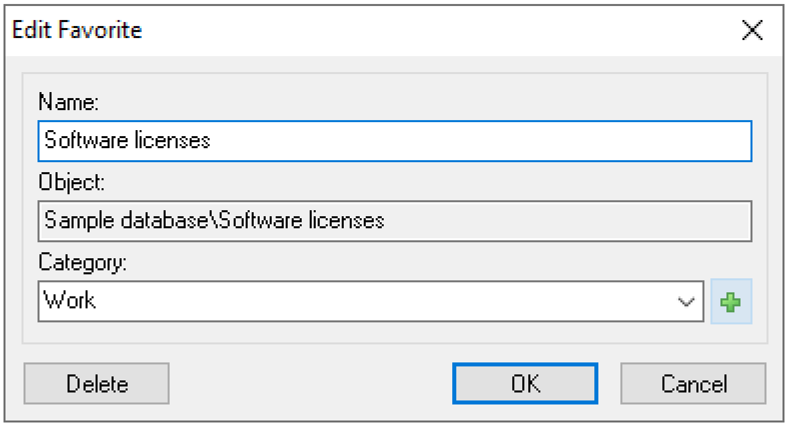
Object: Sample database\Software licenses

Category:

The Add Favorite window

Specify the entry's name and optional **Category** and press **OK**.

To edit or delete a Favorite entry you need to navigate to it first. Then select **Favorites - Edit Favorite...** in the menu.


Edit Favorite

Name: Software licenses

Object: Sample database\Software licenses

Category: Work

The Edit Favorite window

Press the **Delete** button to delete the entry.

If a category is already assigned for the entry, you can perform the following operations in the **Category** field:

- choose other existing category from the list;
- add a new category by pressing the **Add category** tool button and entering a new category name;
- rename the current category by typing a new category name.

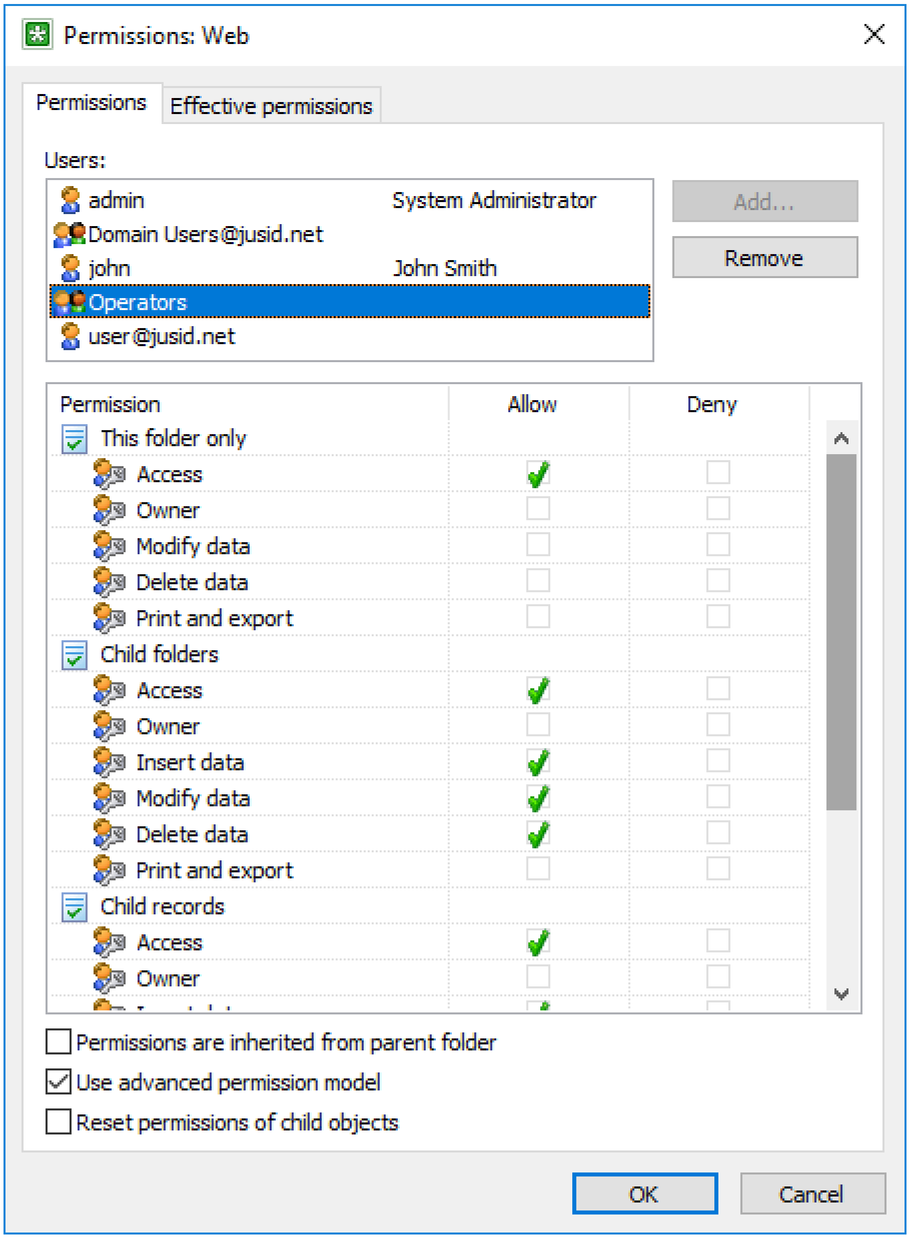
Press **OK** to finish editing.

6.2.15. Object permissions

Crypt-o allows you to set custom permissions for folders or even individual records.

> **NOTE:** Your user account must be an object owner to be able to edit the object's permissions.

To edit an object's permissions select the object and choose **Edit > Permissions...** from the menu.



Users:

admin	System Administrator
Domain Users@jusid.net	
john	John Smith
Operators	
user@jusid.net	

Permission	Allow	Deny
This folder only		
Access	✓	☐
Owner	☐	☐
Modify data	☐	☐
Delete data	☐	☐
Print and export	☐	☐
Child folders		
Access	✓	☐
Owner	☐	☐
Insert data	✓	☐
Modify data	✓	☐
Delete data	✓	☐
Print and export	☐	☐
Child records		
Access	✓	☐
Owner	☐	☐

☐ Permissions are inherited from parent folder

☑ Use advanced permission model

☐ Reset permissions of child objects

The object permissions window

The users list contains accounts for which permissions are configured for the object. Press the **Add...** button to add new users to the list and **Remove** to delete.
To allow or deny a permission for an account, choose the account in the list and then select the according checkbox (**Allow** or **Deny**) for the permission. The list of available permissions is documented in the User management topic

> **NOTE: Deny** permission takes precedence over **Allow** permission when permissions of groups are applied. Use **Deny** only if it is absolutely necessary.

> **NOTE:** If you delete an account from the list, the object will become completely unavailable to this account - the folders will be invisible and all of the records' data will be displayed as the asterisks ("*" symbols).

NOTE: It is needed to grant the database **Access** permission for a user account in order to be able to configure the account's permissions for child folders or records.

Inheritance of permissions

When you create a new folder or record, its permissions are fully inherited from a parent folder. To control inheritance use the ☑ **Permissions are inherited from parent folder** checkbox.

When permissions are **inherited**:

- When permissions of the object's parents are changed, it affects permissions of the object.
- An allow/deny state of inherited permissions is displayed as gray icons.
- If **Allow** is inherited for a permission, you can change it to **Deny**. If **Deny** is inherited, it is not possible to change it.
- You cannot delete inherited user accounts from the list. You can only change its permissions.

When permissions are **not inherited**:

- When permissions of the object's parents are changed, it does not affect permissions of the object.
- You have full control over who can access the object and which permission are set.

For a folder set the ☑ **Reset permissions of child objects** checkbox to reset the permissions for all of the child objects and set full inheritance of permissions from this folder.

Advanced permissions

There are two permissions models available in Crypt-o for data objects - Basic and Advanced.
The model controls how the following permissions are applied: **Access, Owner, Insert data, Modify data, Delete, Print and export**.

Basic model (default):

- These permissions are always applied to the object and all child objects.

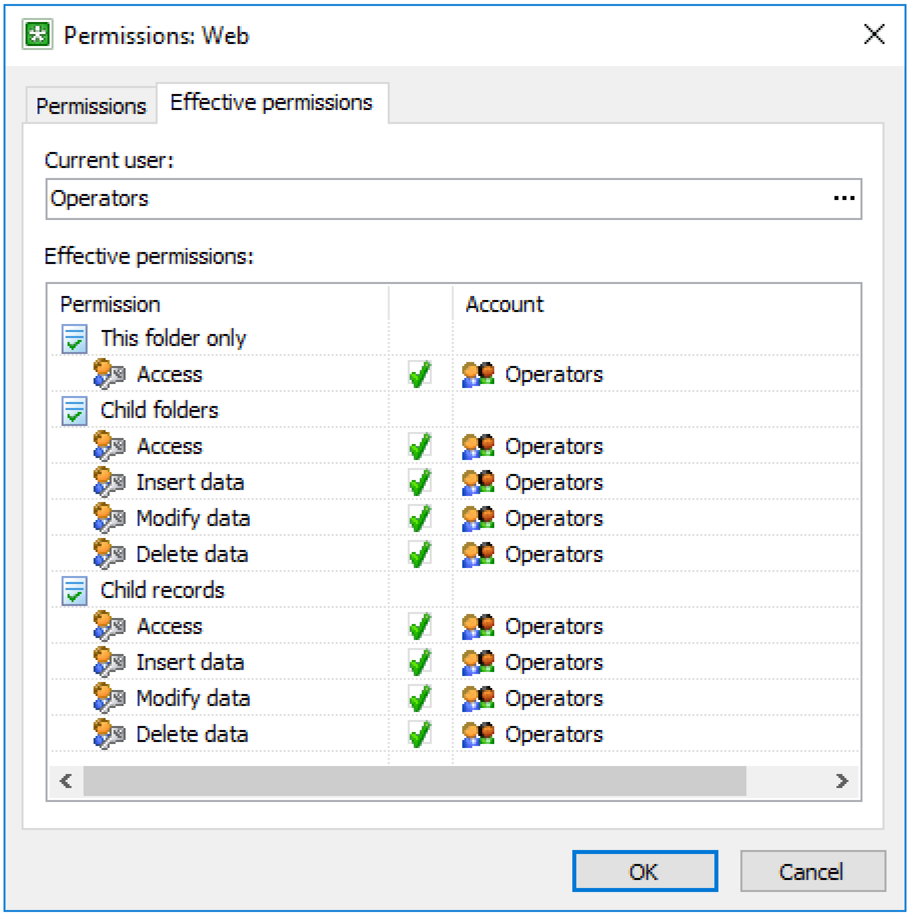
Advanced model:

- These permissions can be separately applied to: **This folder only**, **Child folders**, **Child records**.

To set the mode use the ☑ **Use advanced permission model** checkbox.

Effective permissions

To view effective permissions for a user account open the **Effective permissions** page.
By default, the effective permissions of the current user account is displayed. If you are the object's owner you can choose other user account by pressing the browse button.



Current user: Operators

Effective permissions:

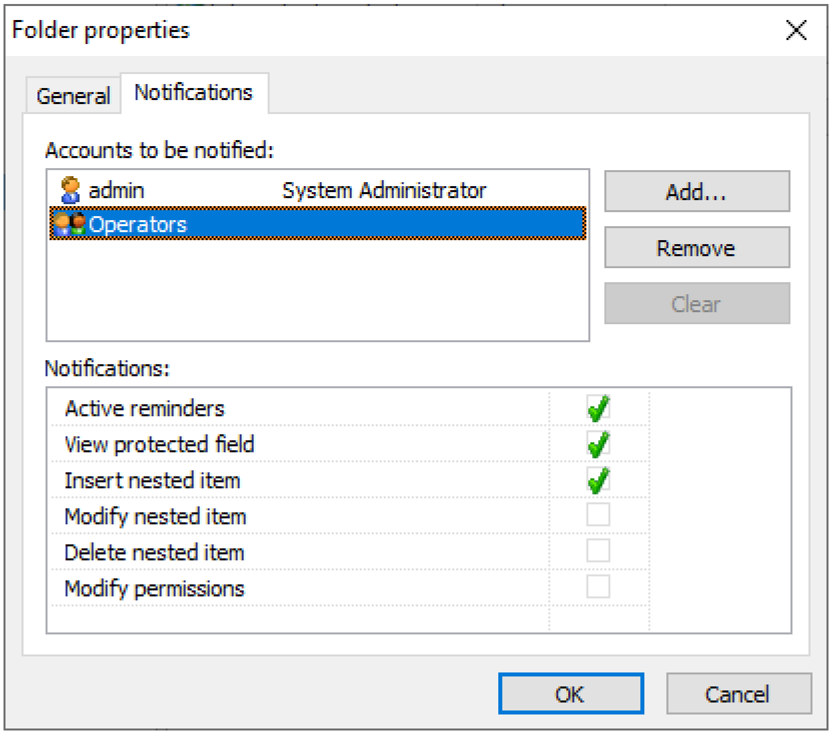
Permission		Account
This folder only		
Access	✓	Operators
Child folders		
Access	✓	Operators
Insert data	✓	Operators
Modify data	✓	Operators
Delete data	✓	Operators
Child records		
Access	✓	Operators
Insert data	✓	Operators
Modify data	✓	Operators
Delete data	✓	Operators

Effective permissions

6.2.16. Object notifiactions

Crypt-o allows you to configure email notifications about various events related to records and folders.
Notifications are configured for a database/folder and apply to all nested records and sub-folders.
To edit notifications select a folder or a database and choose **Edit > Properties...** in the menu. Then open the **Notifications** tab.

NOTE: Your user account must be an object's owner to be able to edit the notifications.



Accounts to be notified:

admin System Administrator
Operators

Notifications:

Active reminders	☑
View protected field	☑
Insert nested item	☑
Modify nested item	□
Delete nested item	□
Modify permissions	□

The object notifications window

Accounts to be notified - specify which accounts will receive notifications. Press the **Add...** button to add an account. Use **Remove** to remove the selected account from the list. When the **Clear** button is clicked all user accounts added for this object will be removed.
Notifications - specify which notification will be sent to the selected account.

The following notifications are available:

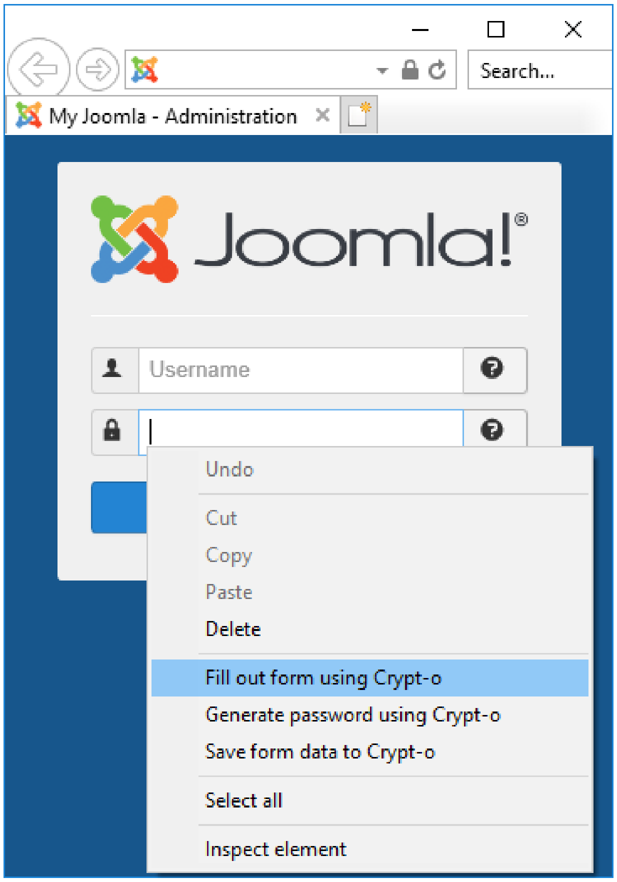
Notification	Description
Active reminders	This notification is sent once per day when there are nested records with active (expired) reminder-type fields.
View protected field	This notification is sent when contents of a protected field has been viewed a nested record.
Insert nested item	This notification is sent when a new nested record or folder has been added.
Modify nested item	This notification is sent when a nested record or folder has been modified.
Delete nested item	This notification is sent when a nested record or folder has been deleted.
Modify permissions	This notification is sent when permissions for a nested record or folder has been modified.

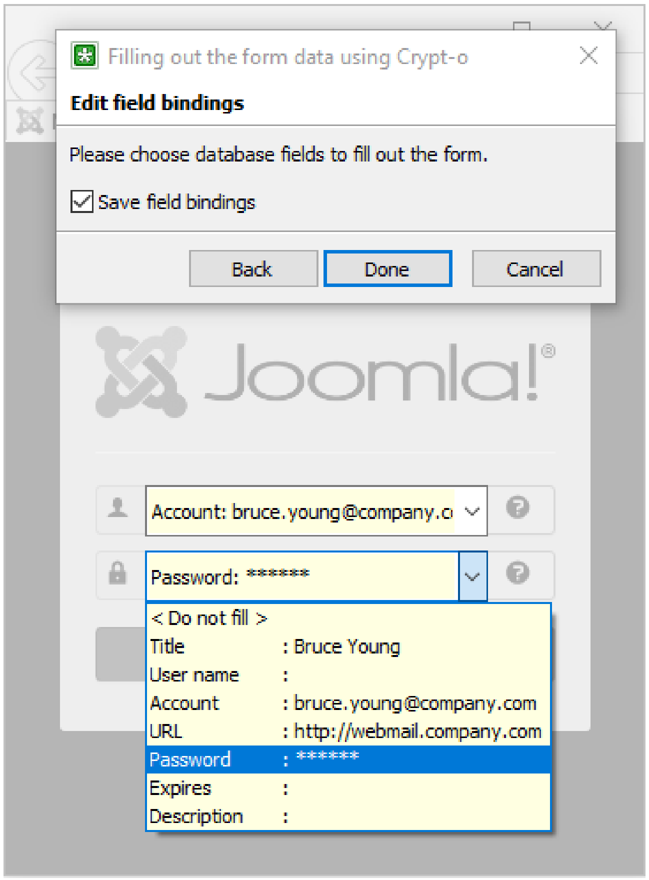
6.3. Form fill out and form data saving

Crypt-o can be used for automatic fill out of various forms. For example, for the automatic login and password input at various websites, filling out your personal data, when creating an account e.t.c. Besides the websites, the data may be entered into most of the regular Windows applications.

All forms the program "knows" about will be filled out automatically. To enable the auto-filling, make sure the browser you are using is supported by Crypt-o, and the integration with that browser is enabled in the program's settings on the Integration :: Browsers page. The auto-filling options can be set on the Integration :: Form filling page in the program's settings.

Forms that are not "known" to the program can be filled manually, by pressing the hotkeys, browser's popup menu or the menu on the program's tray icon. After that, the program will "remember" how to fill that form and will fill it automatically in the future.


Search...
My Joomla - Administration
Joomla!
Username
Undo
Cut
Copy
Paste
Delete
Fill out form using Crypt-o
Generate password using Crypt-o
Save form data to Crypt-o
Select all
Inspect element



Filling out the form data using Crypt-o

Edit field bindings

Please choose database fields to fill out the form.

☑ Save field bindings

Account: bruce.young@company.c

Password: ******

< Do not fill >

Title	: Bruce Young
User name	:
Account	: bruce.young@company.com
URL	: http://webmail.company.com
Password	: ******
Expires	:
Description	:

Working with forms

Crypt-o offers two operations for working with the forms: **Fill out form** and **Save form data**. These operations can be called in the following ways:

1. Using the menu, which appears at right-clicking on the Crypt-o icon in system tray area of the task bar.
2. Using browser's popup menu, which opens up by right-clicking on web pages' data entry fields. Items are added to Crypt-o's pop-up menu if the integration with the browser is enabled in the program's settings on the Integration :: Browsers page.
3. By default, Crypt-o will ask whether you want to save data entered in the form to database when the submit button is clicked on. See Integration :: Form filling topic for more information.
4. Using the hotkeys. By default, for **Fill form**, press **Alt+Win+L** key combination and for **Save form data**, press **Alt+Win+S**. The hotkeys may be reassigned at Integration :: Hot keys page of the program settings. Moreover, there exists a parameter, which permits the hotkeys even if Crypt-o is not currently running.

Saving form data into a database

First of all, create the folders with the fields' structure, sufficient for storing data for various forms in the database. Right after that you can create the data records and enter data manually into the database.

Database records can also be created and populated with the data of the current form, using **Save form data** function (it is called by using the **Alt+Win+S** hotkey or via program's tray icon menu or via browser popup menu).

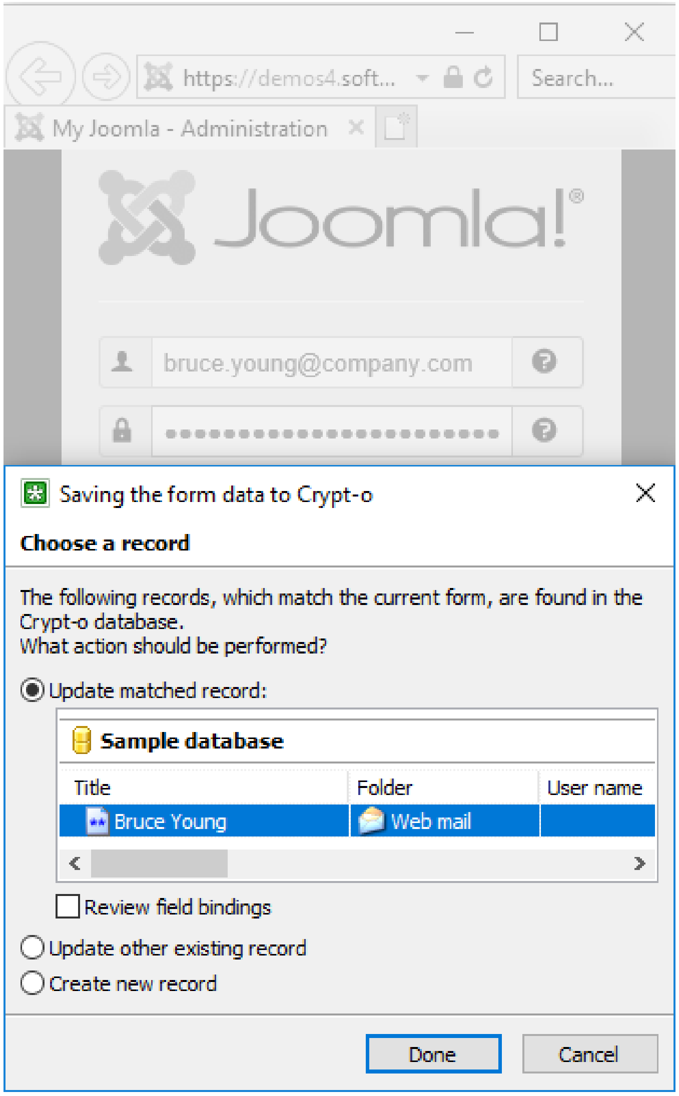
If Crypt-o "knows" about this form, the corresponding record in the database will be updated silently (database password can be prompted if the database is currently closed).

> **NOTE:** To save form data to another record or to edit field bindings of a record linked to this form, press and hold down the **Shift** and select the **Save form data** item on your browser's popup menu or in the program's tray icon menu.

If the current form is "unknown" to the program or **Shift** key was holded down, the form will be shaded and a Crypt-o window will appear, where you will need to do the following:

1. Open the database, which the form data will be saved to.
2. If Crypt-o "knows" about this form, you will be offered the applicable records for saving form data.
   a) Select a record and press **Done** to save the form data into this record.
   b) Select the ☑ **Review field bindings** parameter and press **Next** to review whether the form fields correspond to the record fields.
3. If the program did not find any records, suitable for this form, you have to select a folder, which the new records will be created in, or select an existing record to overwrite its data with form's data.
4. Indicate the accordance of the form fields with the record fields in the database, using yellow comboboxes, located above the form fields.
5. Press the **Done** button.
6. A record adding/editing window will appear, where the entry fields will be populated with the form data. Press **OK** to save the data.

After that, the program will remember, which record in the database is to be used for this form. And if the form auto-filling is enabled in the program's settings on the Integration :: Form filling page, the form will be filled out automatically the next time it is opened.



Saving the form data to Crypt-o

Choose a record

The following records, which match the current form, are found in the Crypt-o database.
What action should be performed?

● Update matched record:

Sample database

Title	Folder	User name
Bruce Young	Web mail	

☐ Review field bindings

○ Update other existing record

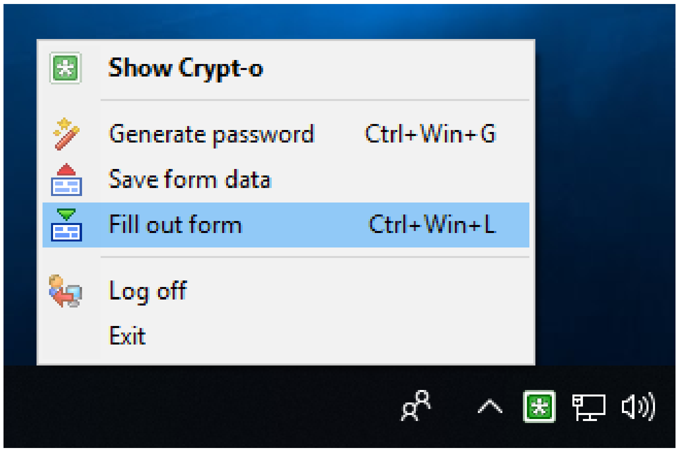
○ Create new record

Calling form fill out manually

To fill out a current form, perform the **Fill out form** operation (called by using the **Alt+Win+L** hotkey or via the tray icon menu or via browser popup menu).

If Crypt-o "knows" about this form, it will be filled out immediately (user logon prompt can appear if needed).

NOTE: To fill a form with data from another record or edit field bindings of a record linked to this form, press and hold down the **Shift** and select the **Fill out form** on your browser's popup menu or in the program's tray icon menu.



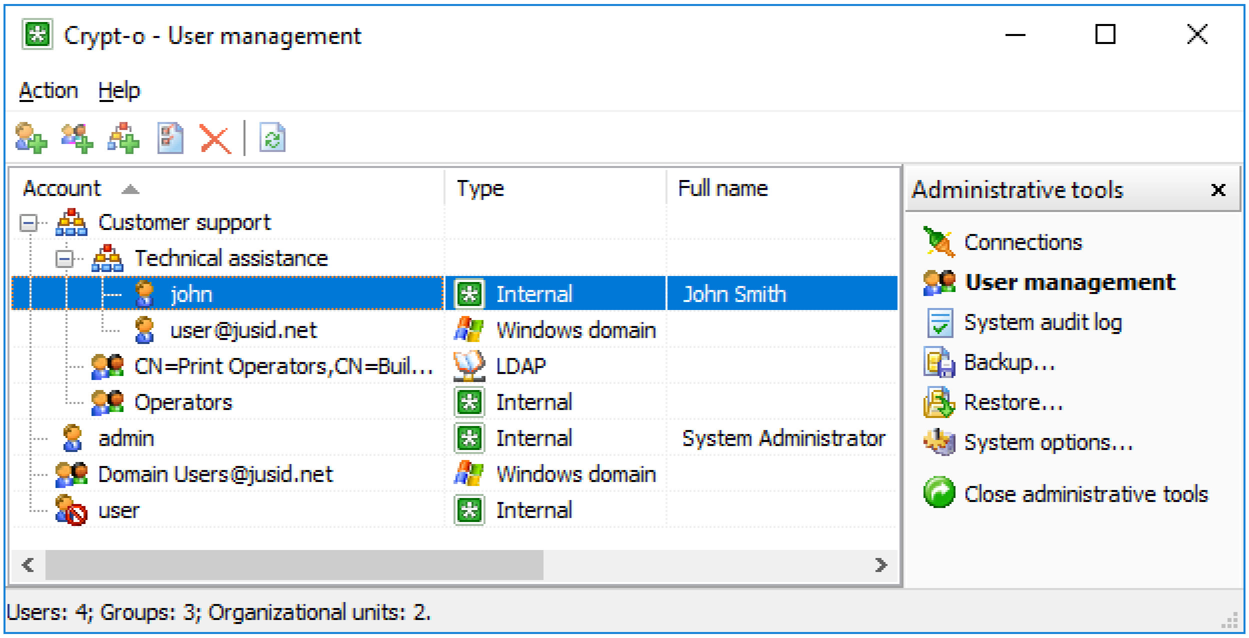
If the current form is "unknown" to the program or **Shift** key was held down, the form will be shaded and Crypt-o window will appear, where you will need to do the following:

1. Open the database, which the form data will be taken from.
2. If Crypt-o "knows" about this form, you will be offered the applicable records for filling out the form.
   a) Select a record and press **Done** to fill out the form.
   b) Select the ☑ **Review field bindings** parameter and press **Next** to review whether the form fields correspond to the record fields.
3. If the program did not find any records, suitable for this form, you have to select a proper record.
4. Indicate the accordance of the form fields with the record fields in the database, using yellow comboboxes, located above the form fields.
5. Press the **Done** button to fill out the form.

6.4. User management

Crypt-o allows to define user accounts and assign needed permissions to them. User and group accounts from a Windows domain or LDAP directory can be used as well. In that case, user credentials will be checked using Windows domain or LDAP authentication.
To manage user accounts, choose **Tools > Administrative tools** from the menu. Then click on the **User management** link in the **Administrative tools** panel.

> **NOTE:** Only users with the **System administrator** or **User management** permissions can manage user accounts.



Account	Type	Full name
Customer support		
Technical assistance		
john	Internal	John Smith
user@jusid.net	Windows domain	
CN=Print Operators,CN=Buil...	LDAP	
Operators	Internal	
admin	Internal	System Administrator
Domain Users@jusid.net	Windows domain	
user	Internal	

Users: 4; Groups: 3; Organizational units: 2.

The User management window

The following account types are available:

Account type	Description
User	An account which represents a single user.
Group	A container account which can include other accounts as its members. Permissions assigned for a group are applied to all its members recursively.
Organizational Unit	A container account which is used to organize your accounts list as a hierarchy tree. Permissions assigned for an Organizational Unit are applied to all its members recursively.
Backup server account	A special user account which is used by %PROGNAME% backup servers.

To add a new user account choose **Action > New user...** from the menu.
To add a new group account choose **Action > New group...** from the menu.
To add a new Organizational Unit choose **Action > New Organizational Unit...** from the menu.
To add a new account for a backup server choose **Action > New backup server account...** from the menu.
To edit a user or group account select it in the list and choose **Action > Properties...** from the menu.
To delete a user or group account select it in the list and choose **Action > Delete** from the menu.

You can change some options for multiple user accounts at once. To do that select the accounts in the list and choose one of the following menu items:

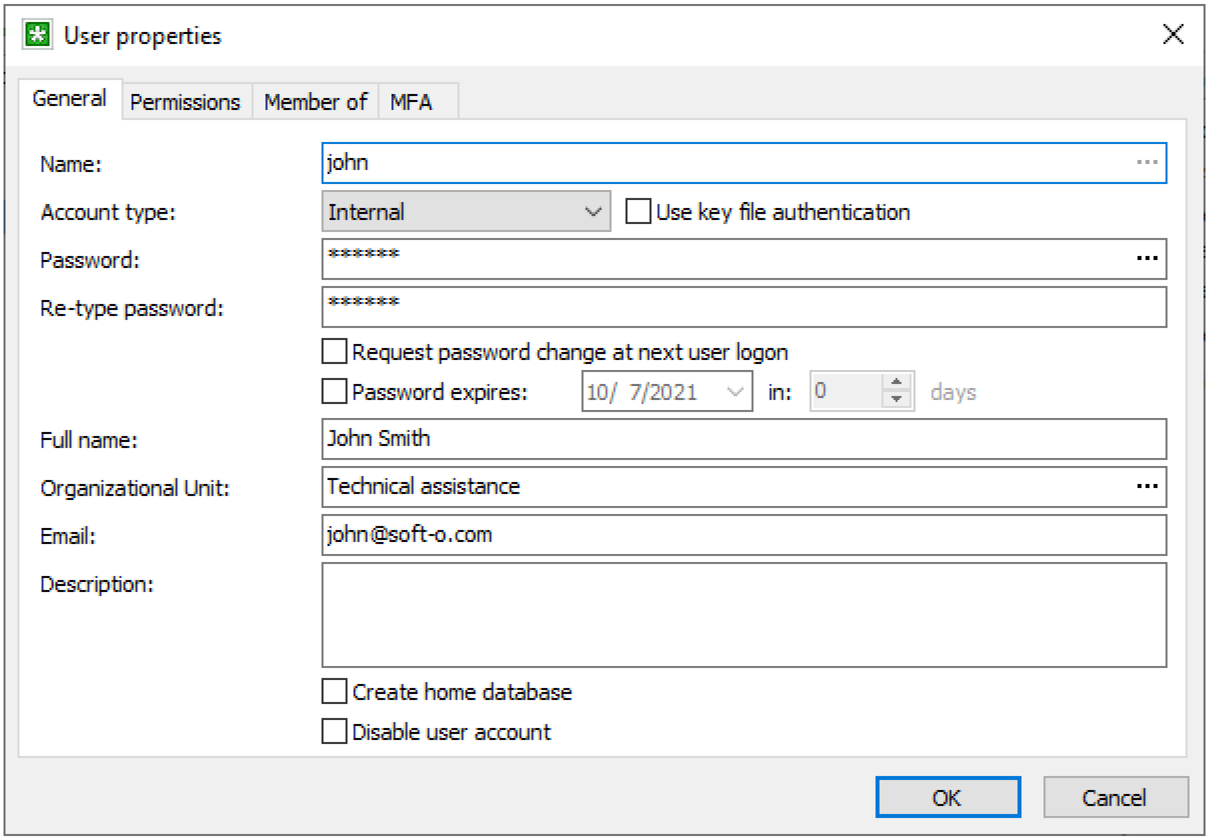
Action > Request password change
Action > Cancel password change request

Action > Enable user account
Action > Disable user account

> **NOTE:** If you select a group or OU account and choose to change an option such way, the option will be applied to all member user accounts of the group.

> **NOTE:** When you use external user accounts (Windows domain, LDAP) in Crypt-o, it may happen that some user accounts have been deleted in Active Directory or LDAP directory with time.
> To find out which user accounts have become invalid, choose **Action > View > Invalid accounts** in the menu.

User properties :: General page



Name: john
Account type: Internal ☐ Use key file authentication
Password: *******
Re-type password: *******
☐ Request password change at next user logon
☐ Password expires: 10/ 7/2021 in: 0 days
Full name: John Smith
Organizational Unit: Technical assistance
Email: john@soft-o.com
Description:
☐ Create home database
☐ Disable user account

General page

- **Name** - a name of the user account.
- **Account type** - a type of the user account. Possible values:
  - **Internal** - internal Crypt-o user account. You need to specify a password for the user account or use key file authentication.
  - **Windows domain** - Windows domain authentication will be used to check the user account password. Enter a user account name of Windows domain in the `UserName@Domain` form. To select a user account from the list, click the **...** button at the right of the **Name** input field.
  - **LDAP** - LDAP directory authentication will be used to check the user account password. Enter a distinguished name of the LDAP user account or click click the **...** button at the right of the **Name** input field to browse LDAP directory. You need to configure available LDAP servers in the System options on the LDAP page.
- ☑ **Use key file authentication** - if selected, the user will be authenticated using a key file. You will be prompted to to save a key file for this user, when this option is turned on. You need to pass this key file to the user. Only Crypt-o user accounts can use the key file authentication. You can create a new key file for a user by choosing **Action > Create new key file...** from the menu in the users list window.

NOTE: By default, a user must store a key file on a removable device, in order to be able to log on using the key file. You can control this behavior in the Crypt-o system options.

WARNING: Store key files on removable devices, such as USB flash drives, for security reasons. Unplug the device with your key file, when you finished working with Crypt-o.

- **Password** - the user account password.
- **Retype password** - verification of the password.
- ☑ **Request password change at the next user logon** - if selected, the user will be prompted to enter a new password at the next logon.
- ☑ **Password expires** - you can specify an expiration date for the password of the user account. When the password is expired, the user is forced to change the password.

  NOTE: See the Security page in the System options for more settings related to password expiration.

- **Full name** - optional full name of the user.
- **Organizational Unit** - optionally select an Organizational Unit for this account.
- **Email** - optional email address. It is used to send notifications about various events.
- **Description** - optional description of the user.
- ☑ **Create home database** - if selected, a home database will be automatically created for the user. The user will be the owner of his home database, but the database can not be deleted by the user. By default other users have no access to the home database, even administrators. The user may allow access to his home database for other users if necessary.

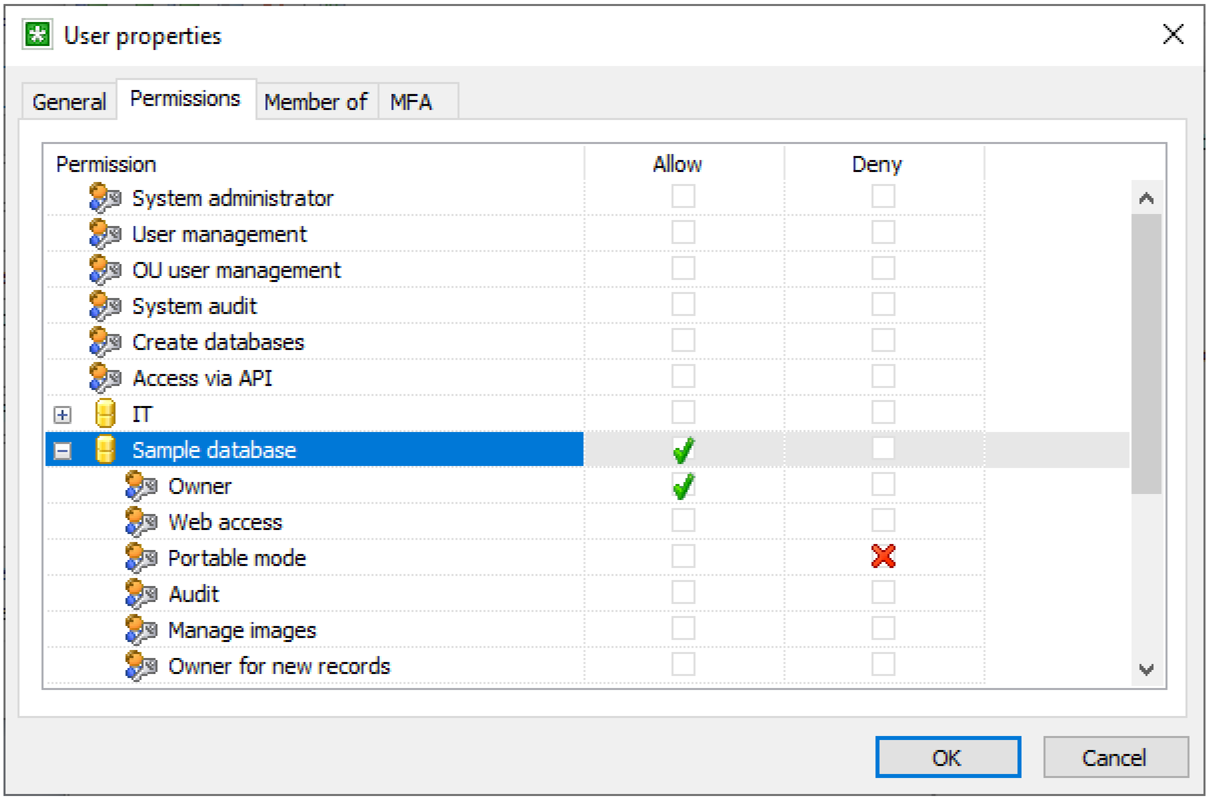
  NOTE: If the **Create home database** option is enabled for a group, home databases will be created for all members of the group.

  NOTE: By default, Web access is disabled for new home databases. You can enable it in the Crypt-o system options.

- ☑ **Disable user account** - the user account is disabled and the user logon will fail.

User properties :: Permissions page

On that page you can assign permissions for a user account. Set a mark on the **Allow** column for a permission to enable this permissions for the user. Set a mark on the **Deny** column for a permission to disable this permissions for the user. **Deny** permission takes precedence over **Allow** permission.



Permission	Allow	Deny
System administrator	□	□
User management	□	□
OU user management	□	□
System audit	□	□
Create databases	□	□
Access via API	□	□
⊞ IT	□	□
⊟ Sample database	✓	□
Owner	✓	□
Web access	□	□
Portable mode	□	☒
Audit	□	□
Manage images	□	□
Owner for new records	□	□

Permissions page

The following system permissions are available:

Permission	Description
System administrator	A user can do everything.
User management	A user can manage user accounts and assign permissions. The following restrictions apply: • It is not allowed to create or modify accounts with the **System administrator** permission. • It is not allowed to change a password for accounts which have access to private or home databases. • It is not allowed to modify a name and options of accounts which have access to private or home databases. • It is not allowed to delete accounts which have access to private databases.
OU user management	A user can manage user accounts only within the user's organizational unit (OU), including nested organizational units. The OU user manager can can add, modify, delete user accounts within his OU, add OU users to OU groups. But individual permissions for OU groups can be set only by other users with higher privileges (**User management** or **System administrator**). The following restrictions apply: • All restrictions which apply to the **User management** permission. • When changing group membership for an account both the account and the group account must belong to the OU. • It is not allowed to change system permissions for accounts. • It is not allowed to change database permissions for accounts unless the user is the database owner. • It is not allowed to delete an account or change its password if the account has

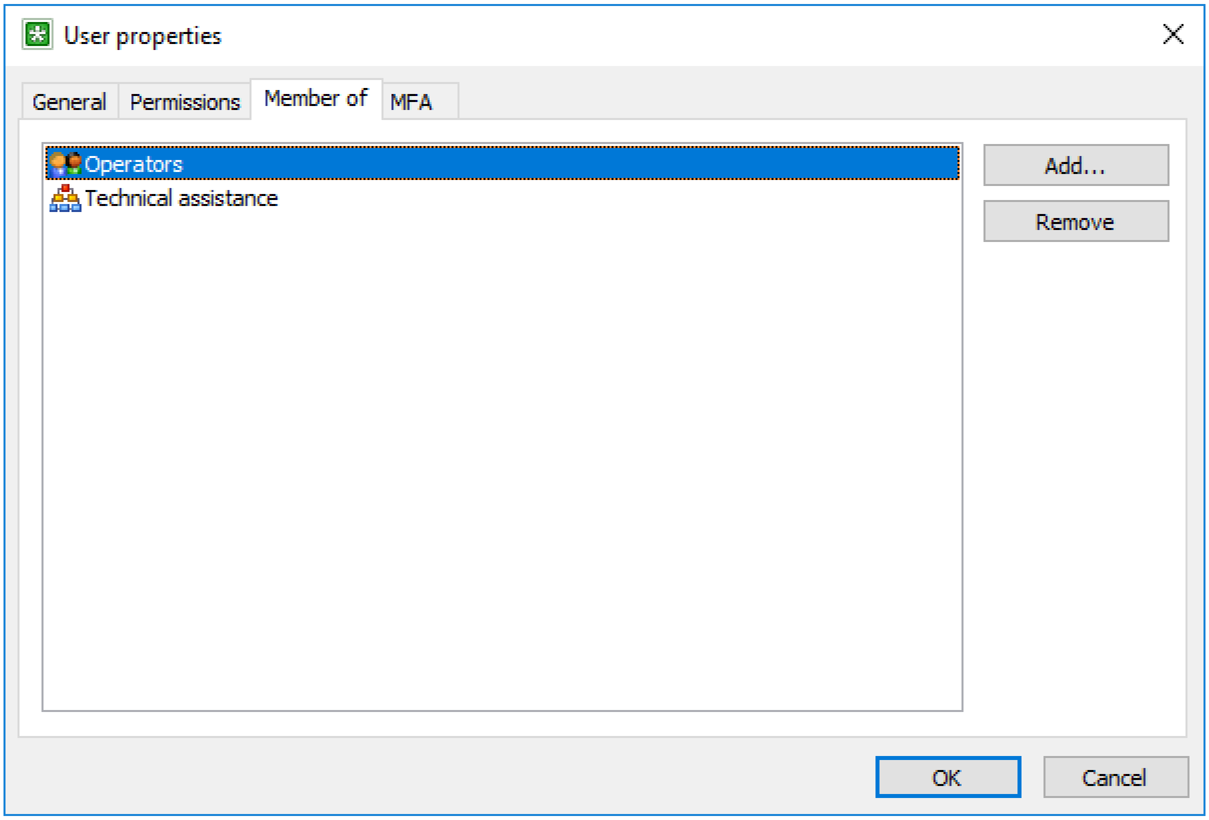
	system permissions set or the account is the member of groups outside the OU.
System audit	A user can view the System audit log.
Create databases	A user can create new databases.
Access via API	A user account can be used to access Crypt-o via API.

The following object permissions are available:

Permission	Description
Owner	A user can do everything with an object.
Web access	This permission applies to databases only. A user can access a database via Web interface.
Portable mode	This permission applies to databases only. A user can create a portable/offline version of a database.
Audit	This permission applies to databases only. A user can view a database audit log.
Manage images	This permission applies to databases only. A user can add/modify/delete images, which are used as icons for folders and records.
Owner for new records	This permission applies to databases only. When a user creates a new record, the user becomes an owner of this record.
Insert data	A user can create new records and new sub-folders.
Modify data	A user can edit records and edit folders.
Delete data	A user can delete records and delete folders.
Manage attachments	A user can add or remove file attachments.
Extract attachments	A user can execute or extract file attachments.
View protected fields	A user can view data in protected fields. If a user does not have this permission, he is not able to view data in protected fields. But if the user has the **Form filling** permission, he is allowed to fill out forms with data of the protected fields.
Print and export	A user can print and export data.
Form filling	A user can use the form filling feature.

User properties :: Member of page

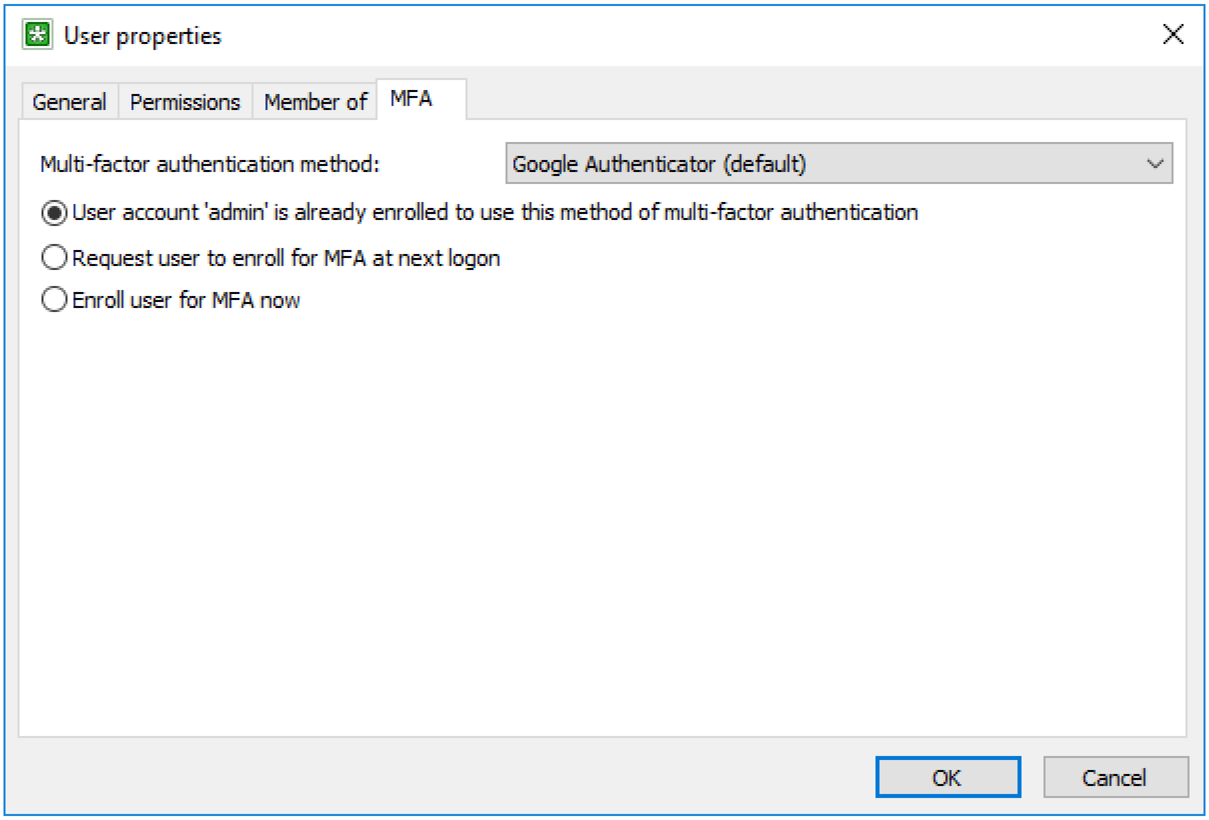
On that page you can specify group membership for a user account.



Member of page

User properties :: MFA

On that page you can control multi-factor authentication (MFA) for a user account.



Multi-factor authentication method: Google Authenticator (default)

● User account 'admin' is already enrolled to use this method of multi-factor authentication

○ Request user to enroll for MFA at next logon

○ Enroll user for MFA now

MFA page

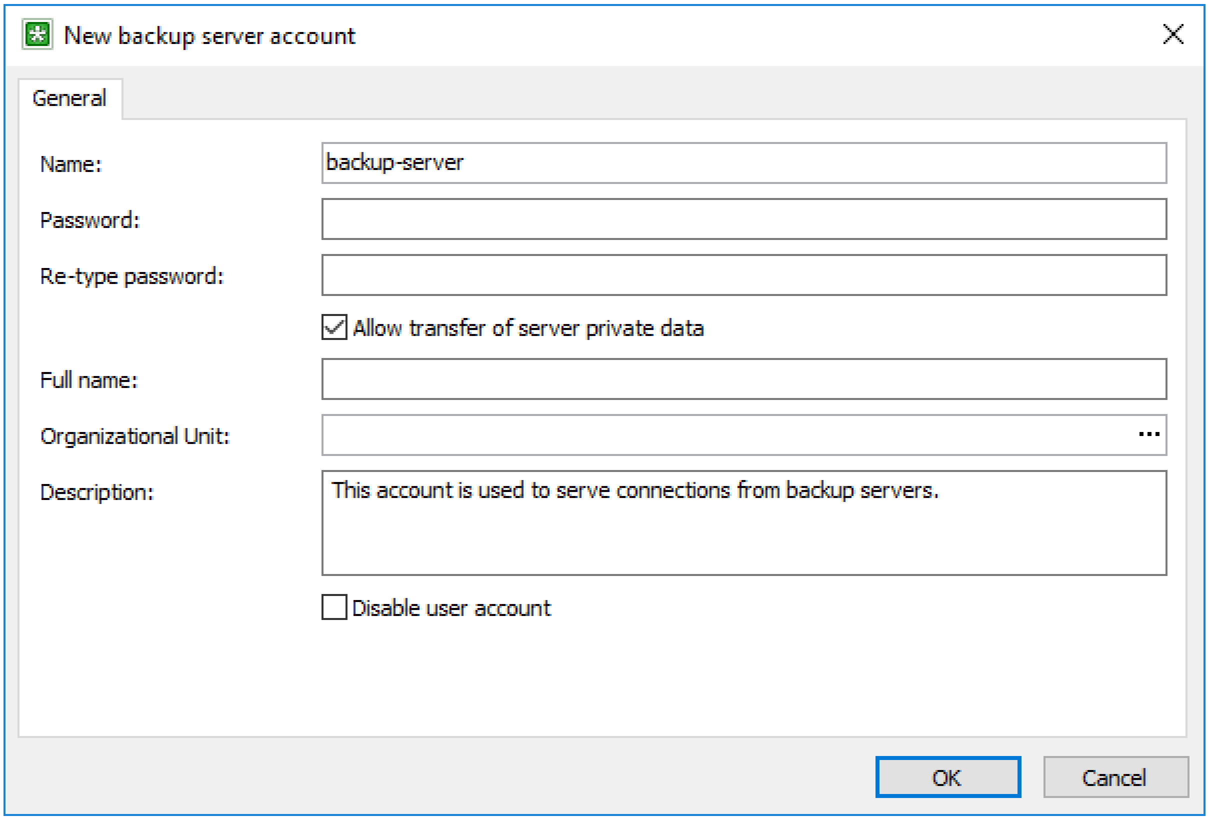
By default multi-factor authentication is disabled and this page is not available for a user account. To enable MFA use the Multi-factor authentication page in the Crypt-o system options.
Initially all user accounts use the default MFA method specified in the system options. If needed you can set a different MFA method for specific user accounts.
At user logon Crypt-o requests a user to enroll for MFA if it is not done yet.

If a TOTP/HOTP authentication method is used, a **User manager** or **System administrator** can select the following options:

- **Request user to enroll for MFA at next logon** - when this option is selected Crypt-o will request the user to enroll for MFA at next logon.
- **Enroll user for MFA now** - when this option is selected the user enrollment will start after pressing **OK**.

Specialized user account for backup servers

When you set up a backup server, you need to create a specialized user account on the primary server. This user account is used by a backup server to connect to the primary server. It is needed to allow transfer of the primary server's private data (TLS certificates and keys, licenses) to perform proper initialization of a backup server. The initialization is made only once during setup of a backup server.
To add a new account for a backup server choose **Action > New backup server account...** from the menu.



Name: backup-server

Password:

Re-type password:

☑ Allow transfer of server private data

Full name:

Organizational Unit: ...

Description: This account is used to serve connections from backup servers.

☐ Disable user account

Adding a user account for a backup server

- **Name** - a name of the user account.
- ☑ **Allow transfer of server private data** - when this option is selected, backup servers will be able to obtain private data of the main server, such as TLS certificates and keys, registration data, etc.

  > ⚠ **WARNING:** This option is needed only for initialization of a backup server. Turn off this option immediately after initialization of a backup server.

  > ✎ **NOTE:** For security reasons, this option is turned off automatically after 15 minutes.

- **Password** - the user account password.
- **Retype password** - verification of the password.
- **Full name** - optional full name of the user.
- **Description** - optional description of the user.
- ☑ **Disable user account** - the user account is disabled and the user logon will fail.

6.5. Audit log

Crypt-o writes the following events into the **Audit log** for each database:

- Insert
- Update
- Delete
- View protected
- Export
- Print
- Extract file
- Form fill

The following events are written to the **System audit log**:

- Log on
- Log off
- Backup
- Restore

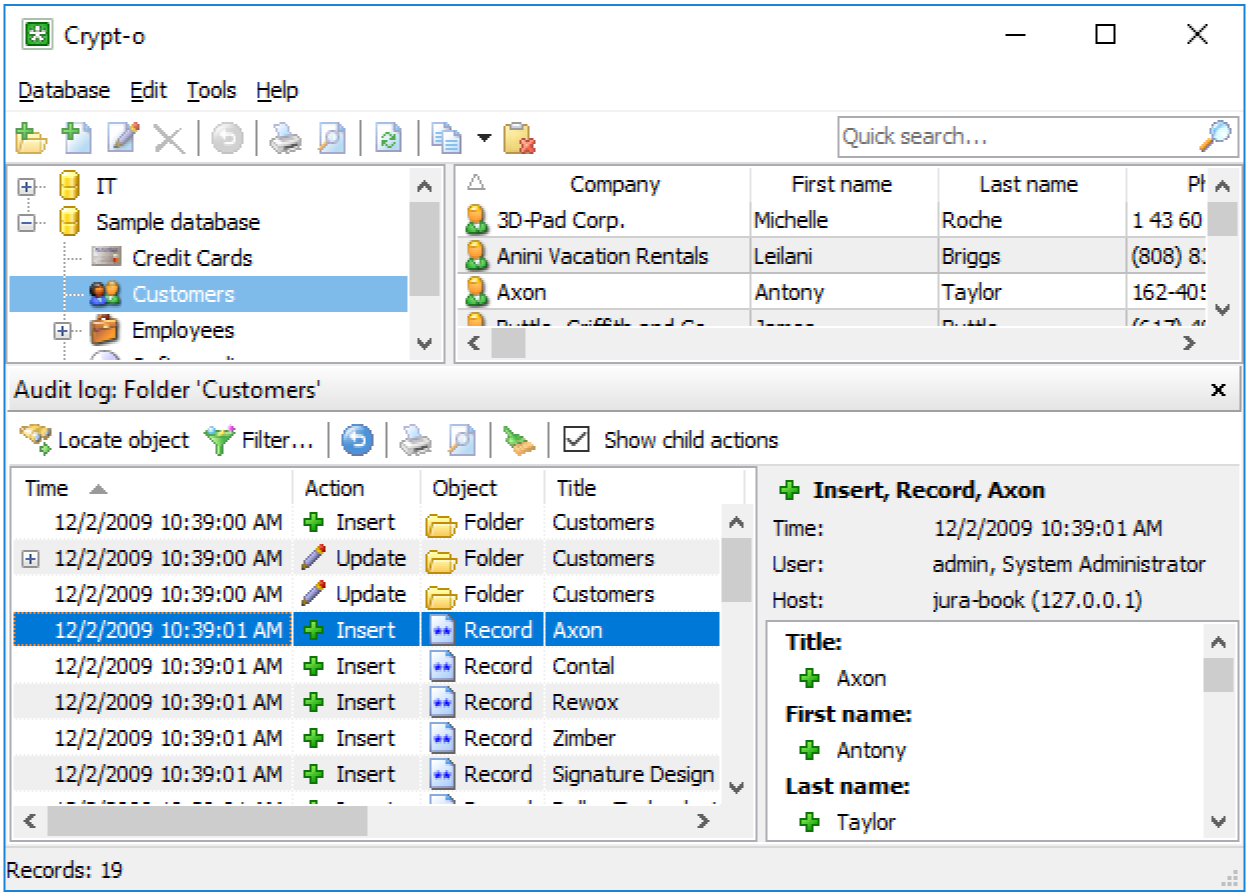
Audit log

To view the audit log for a record, folder or database, select a needed object and choose **Tools > Audit log** from the menu.

NOTE: If your user account does not have the **Owner** or **Audit** permissions for an object, only **Insert, Update, Delete** events will be shown in the audit log for that object.

To view the audit log for an entire database, select **Database > Database audit log...** from the menu.

NOTE: Your user account must have the **Owner** or **Audit** permissions for a database in order to view the database audit log.



Company	First name	Last name	Pl
3D-Pad Corp.	Michelle	Roche	1 43 60
Anini Vacation Rentals	Leilani	Briggs	(808) 8:
Axon	Antony	Taylor	162-405

Time	Action	Object	Title
12/2/2009 10:39:00 AM	Insert	Folder	Customers
12/2/2009 10:39:00 AM	Update	Folder	Customers
12/2/2009 10:39:00 AM	Update	Folder	Customers
12/2/2009 10:39:01 AM	Insert	Record	Axon
12/2/2009 10:39:01 AM	Insert	Record	Contal
12/2/2009 10:39:01 AM	Insert	Record	Rewox
12/2/2009 10:39:01 AM	Insert	Record	Zimber
12/2/2009 10:39:01 AM	Insert	Record	Signature Design

Insert, Record, Axon

Time: 12/2/2009 10:39:01 AM

User: admin, System Administrator

Host: jura-book (127.0.0.1)

Title:

Axon

First name:

Antony

Last name:

Taylor

Records: 19

The audit log

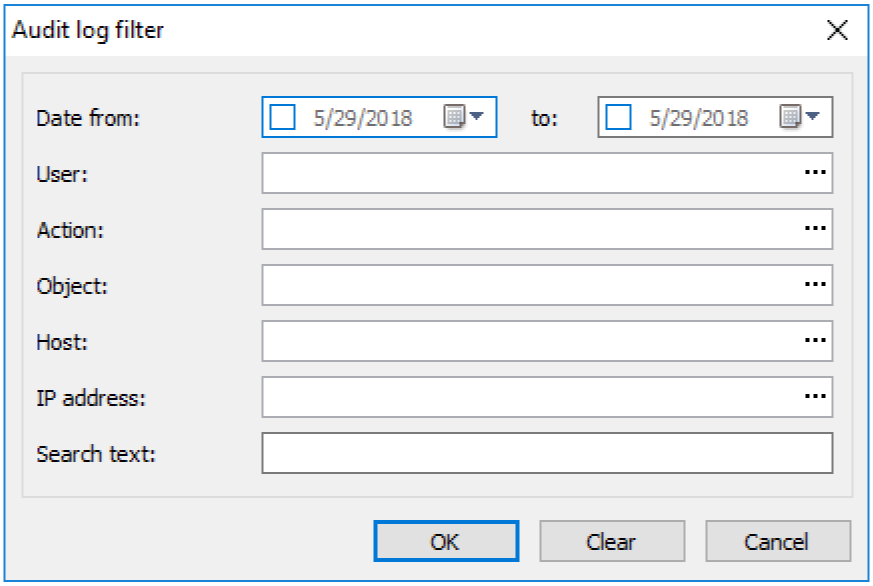
Click on an event in the list to view the event details in the right part of the audit log window.
Click the **Locate object** button to locate the object related to the currently selected event.
Click the **Revert changes** button to revert the selected changes.
By default, when viewing the Audit log for folders, actions for child objects is also displayed. To control this, use the **Show child actions** option.
To open the new Audit log view for the selected object in the current Audit log view, choose **Tools > Audit log** in the main menu.
Click the **Clean up Audit log** button to delete unneeded entries in the Audit log. Only System administrator can perform this operation.

Click the **Print** button to print records of the audit log. To adjust columns width or hide a column, choose **Database > Print setup...** in the main menu.

To export the audit log to a file click the **Print** button. Then press the **Action** button in the **Print** windows to access additional commands.
Choose **Save to file** to save the audit log in one of the following file formats:

- Rich text file (RTF);
- Excel file (Excel2003 or later);
- HTML file.

Click the **Filter...** button to specify filter options for the audit log. The audit log filter window will appear.



Date from: □ 5/29/2018 to: □ 5/29/2018

The audit log filter window

You can specify the following filtering parameters:

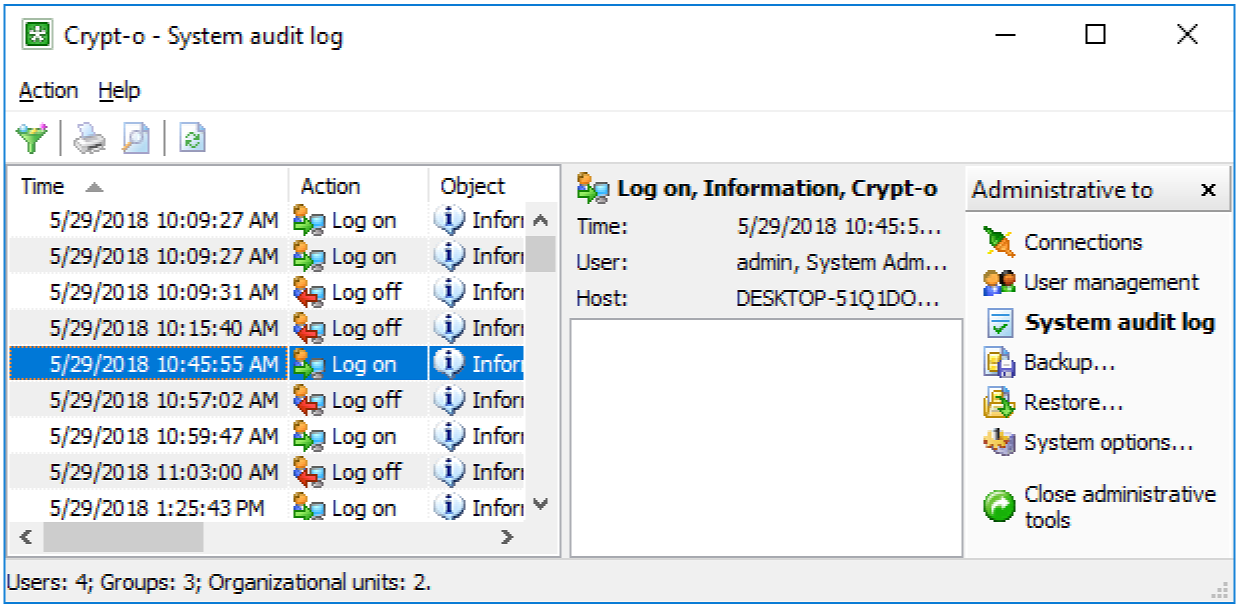
- **Date from** - display events beginning with this date;
- **Date to** - display events ending by this date;
- **User** - display events for this user;
- **Action** - display events of this type;
- **Object** - display events for this object type;
- **Host** - display events for this host;
- **IP address** - display events for this IP address;
- **Search text** - display events containing the specified text.

Once the necessary filter parameters are set, click **OK**.

System audit log

To view the System audit log, choose **Tools > Administrative tools** from the menu. Then click on the **System audit log** link in the **Administrative tools** panel.

NOTE: Your user account must have the **System administrator** or **System audit** permissions in order to view the system audit log.



Time	Action	Object
5/29/2018 10:09:27 AM	Log on	Infor
5/29/2018 10:09:27 AM	Log on	Infor
5/29/2018 10:09:31 AM	Log off	Infor
5/29/2018 10:15:40 AM	Log off	Infor
5/29/2018 10:45:55 AM	Log on	Infor
5/29/2018 10:57:02 AM	Log off	Infor
5/29/2018 10:59:47 AM	Log on	Infor
5/29/2018 11:03:00 AM	Log off	Infor
5/29/2018 1:25:43 PM	Log on	Infor

Log on, Information, Crypt-o

Time:	5/29/2018 10:45:5...
User:	admin, System Adm...
Host:	DESKTOP-51Q1DO...

Users: 4; Groups: 3; Organizational units: 2.

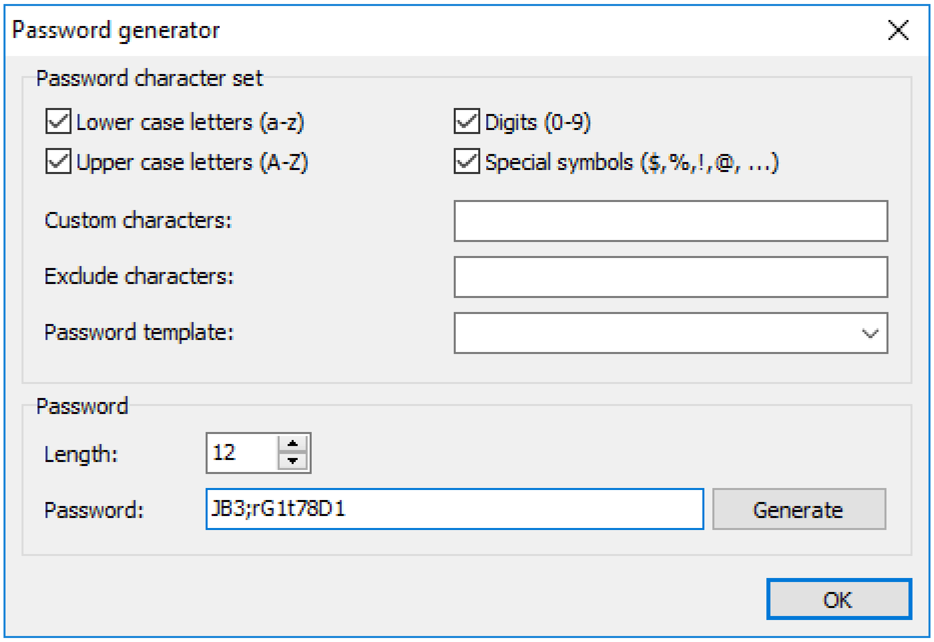
The system audit log

6.6. Password generator

Crypt-o allows you to generate secure random passwords.
The random password generator has the following options:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Lower case letters (a-z)</td><td>Lower case letters **a-z** will be used for password generation.</td></tr>
<tr><td>Upper case letters (A-Z)</td><td>Upper case letters **A-Z** will be used for password generation.</td></tr>
<tr><td>Digits (0-9)</td><td>Digits **0-9** will be used for password generation.</td></tr>
<tr><td>Special symbols ($,%,!,@, ...)</td><td>Special symbols **~ ! @ $ % ^ & * ( ) - + | = / : ; [ ] < > , .** will be used for password generation.</td></tr>
<tr><td>Custom characters</td><td>User defined characters will be used for password generation. Enter needed characters in this input field.</td></tr>
<tr><td>Exclude characters</td><td>The specified characters will be excluded from password generation. Enter needed characters in this input field.</td></tr>
<tr><td>Password template</td><td>It is possible to define a template for password generation. If the template is specified, a password will be generated according to this template.

The following characters can be used in a template:
<table>
<tr><td>**a**</td><td>a random lower case letter will be placed in this position;</td></tr>
<tr><td>**A**</td><td>a random upper case letter will be placed in this position;</td></tr>
<tr><td>**9**</td><td>a random digit will be placed in this position;</td></tr>
<tr><td>**$**</td><td>a random special character will be placed in this position;</td></tr>
<tr><td>**C**</td><td>one of the user defined characters, specified in the **Custom characters** input field, will be placed in this position;</td></tr>
<tr><td>**"**</td><td>a quoted text will be placed in the resulting password as is.</td></tr>
</table>
</td></tr>
<tr><td>Length</td><td>A desired length of a password.</td></tr>
</table>



Password generator

Password character set

☑ Lower case letters (a-z)
☑ Digits (0-9)
☑ Upper case letters (A-Z)
☑ Special symbols ($,%,!,@, ...)

Custom characters:

Exclude characters:

Password template:

Password

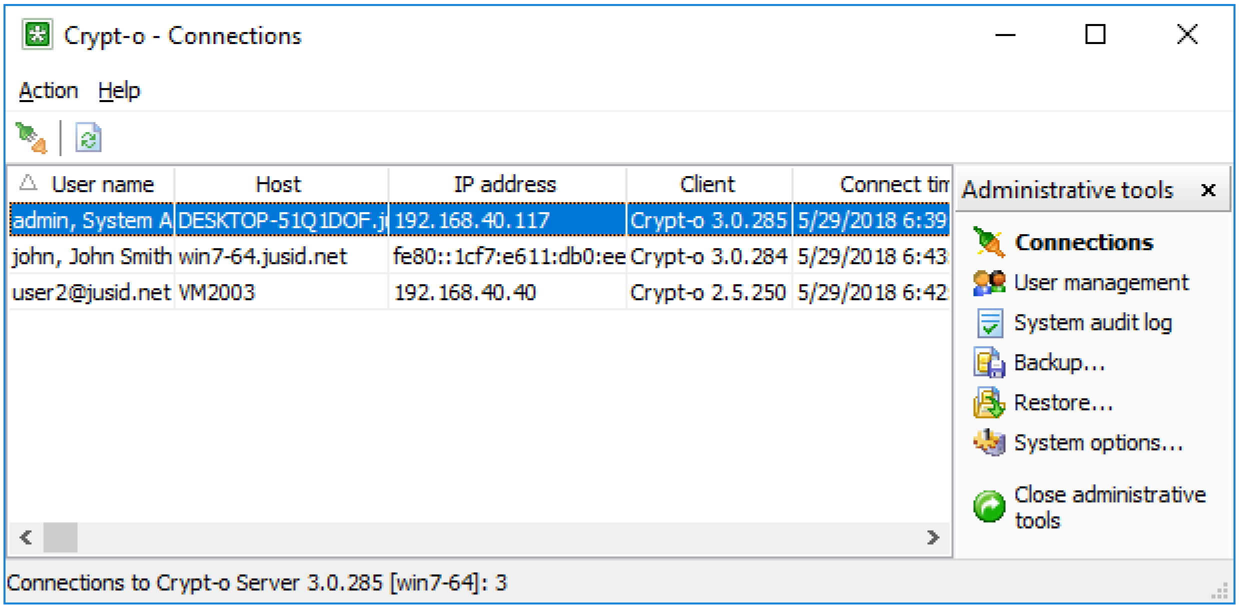
Length: 12

Password: JB3;rG1t78D1

The password generator

6.7. Managing client connections

Users with the **System administrator** permission can view and manage active client connections to Crypt-o Server. To do that, choose **Tools > Administrative tools** from the menu. Then click on the **Connections** link in the **Administrative tools** panel.



User name	Host	IP address	Client	Connect tim
admin, System A	DESKTOP-51Q1DOF.j	192.168.40.117	Crypt-o 3.0.285	5/29/2018 6:39
john, John Smith	win7-64.jusid.net	fe80::1cf7:e611:db0:ee	Crypt-o 3.0.284	5/29/2018 6:43
user2@jusid.net	VM2003	192.168.40.40	Crypt-o 2.5.250	5/29/2018 6:42

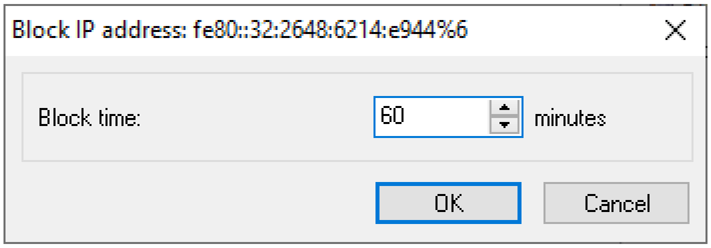
Connections to Crypt-o Server 3.0.285 [win7-64]: 3

The Connections window

You will see all currently active client connections to Crypt-o Server.
To disconnect the selected client connection choose **Action > Disconnect** from the menu.

Blocking IP addresses

You can block all Crypt-o Client connections from an IP address for a certain period of time. To do that select a connection in the list and choose **Action > Block IP address...** in the menu. Then specify a time interval for the block and press **OK**.



Block time: 60 minutes

The Block IP address window

NOTE: Crypt-o Server blocks an IP address automatically for 6 hours if there was 20 failed log on attempts from this IP address.

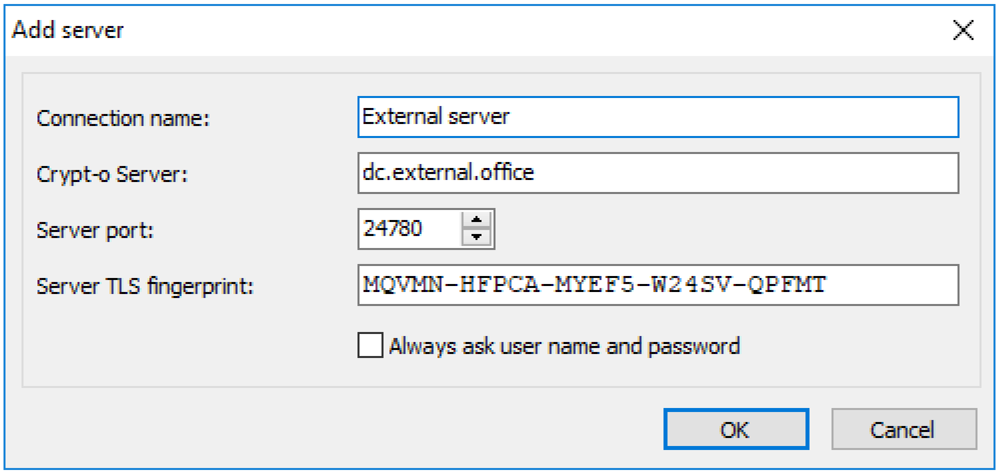
NOTE: All IP address blocks are removed when Crypt-o Server is restarted.

Unblocking IP addresses

To view the list of currently blocked IP addresses choose **Action > View > Blocked IP addresses** in the menu.
To unblock an IP address select its entry in the list and choose **Action > Unblock IP address** in the menu.

6.8. Additional Crypt-o Servers

Crypt-o Client can be configured to work with multiple independent Crypt-o Servers. By default Crypt-o Client connects to a single Crypt-o Server and its available databases are displayed in the left pane of the application's main window. To add a new additional Crypt-o Server, select **Tools > Additional servers > Add server...** in the main menu. The following window will appear:



Add server

Connection name: External server

Crypt-o Server: dc.external.office

Server port: 24780

Server TLS fingerprint: MQVMN-HFPCA-MYEF5-W24SV-QPFMT

□ Always ask user name and password

Adding additional server

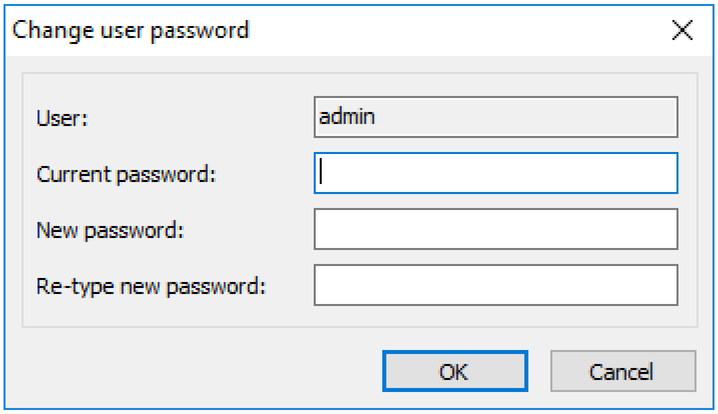
- **Connection name** - a user friendly name of this server connection. It will be displayed in the left pane of the main window.
- **Crypt-o Server** - a host name or an IP address of a computer where the Crypt-o Server is running.
- **Server port** - a TCP port number, which is used by the Crypt-o Server. By default it is `24780`.
- **Server TLS fingerprint** - an TLS fingerprint of the Crypt-o Server. This TLS fingerprint is used to verify the server TLS certificate and protects against man-in-the-middle hacker attacks.
- **Always ask user name and password** - when this option is enabled you will be asked for a user name and password every time you connect to this server. Otherwise the user name and password will be saved at the main server and then used for the automatic connection to this server.

> **NOTE:** Since the user name and password are saved in the encrypted database of the main server, it is safe to use this option.

Press **OK** to add the server. You will be asked for a user name and password to connect to the server. After successful connection the server will be added to the tree in the left pane of the application's main window.

6.9. Change password

To change a password of the currently logged on user, select Tools - Change password... in the main menu. Then you need to type the current password and the new password. Press **OK** to confirm the change.



User: admin

Change password window

7. Configuration of Crypt-o

- Crypt-o Client options
- Crypt-o system options
- Group Policy Administrative Template

7.1. Crypt-o Client options

To access Crypt-o Client options choose **Tools > Options...** from the menu. Crypt-o Client options include the following pages:

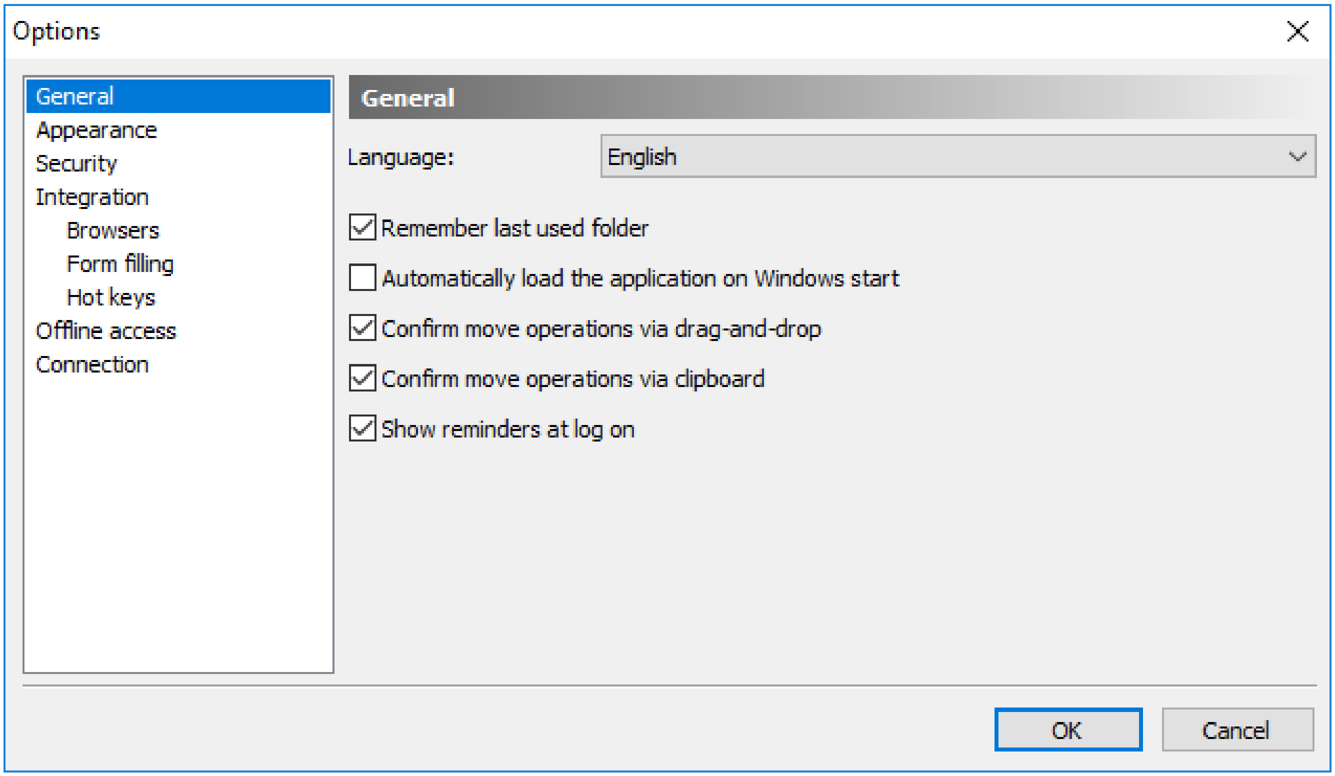
- General
- Appearance
- Security
- Integration :: Hot keys
- Integration :: Browsers
- Integration :: Form filling
- Offline access
- Connection

7.1.1. General

- **Language** - user interface language.

> **NOTE:** We offer **10 FREE licenses of Crypt-o**, if you translate Crypt-o user interface to a language, which is not available yet. See the list of languages.

- ☑ **Remember last used folder** - when this option is selected, the currently selected folder is remembered on a user log off. The remembered folder is automatically selected on the next user logon.
- ☑ **Automatically load the application on Windows start** - when this option is selected, Crypt-o will be loaded on Windows start and minimized to the system tray.
- ☑ **Confirm move operations via drag-and-drop** - when this option is selected, Crypt-o will prompt you to confirm moving of records or folders using drag-and-drop by the mouse.
- ☑ **Confirm move operations via clipboard** - when this option is selected, Crypt-o will prompt you to confirm moving of records or folders using the clipboard.
- ☑ **Show reminders at log on** - when this option is selected, **Crypt-o will show all expired records at user log on.**



Language: English

☑ Remember last used folder

□ Automatically load the application on Windows start

☑ Confirm move operations via drag-and-drop

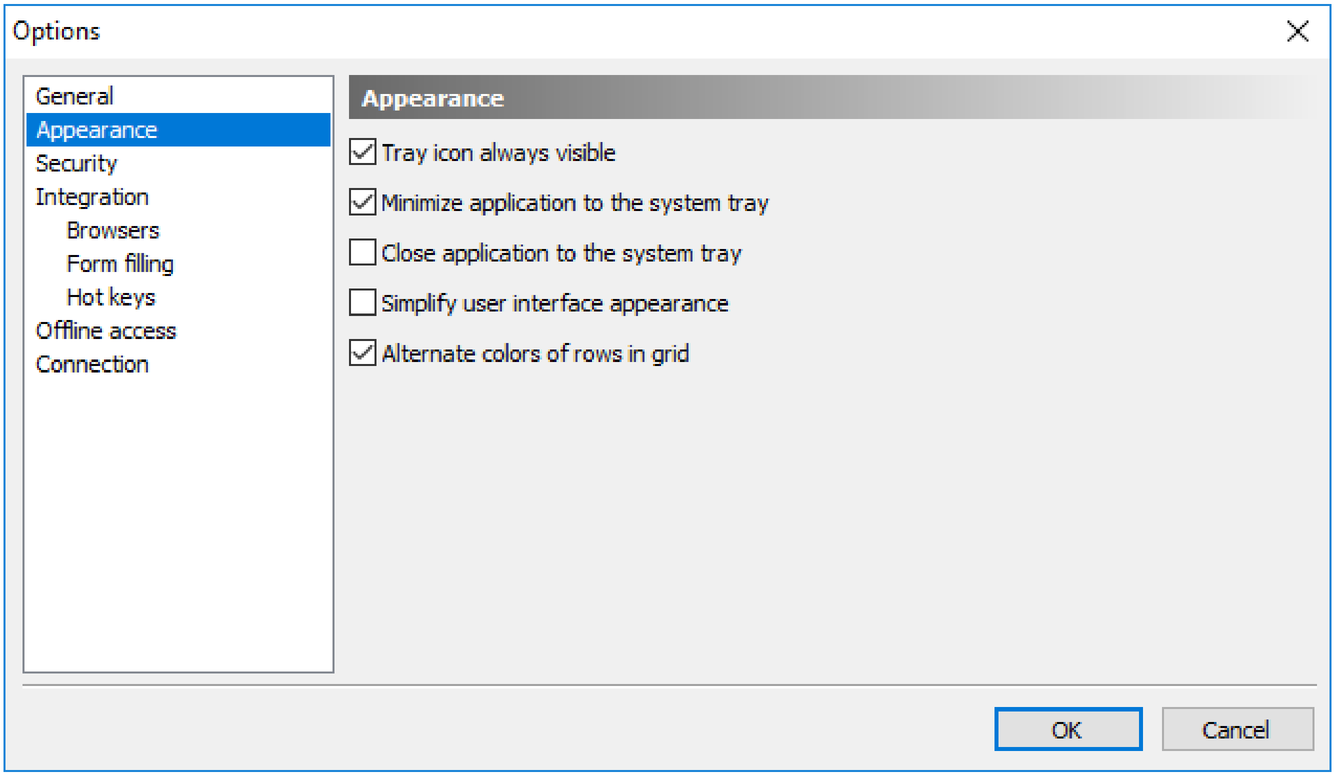
☑ Confirm move operations via clipboard

☑ Show reminders at log on

General options

7.1.2. Appearance

- ☑ **Tray icon always visible** - if selected, the Crypt-o icon will be always shown in the system tray.
- ☑ **Minimize application to the system tray** - this option allows to minimize the application to the system tray. Crypt-o button will not be shown in the system taskbar when the program will be minimized.
- ☑ **Close application to the system tray** - when this option is selected, the application will be minimized to the system tray when you press the close button. To quit the application you need to choose **Database > Exit** from the main menu or choose **Exit** from the program's tray icon menu.
- ☑ **Simplify user interface appearance** - when this option is selected a simple startup screen will be shown. It is useful to simplify the startup screen when working in a terminal session.
- ☑ **Alternate colors of rows in grid** - when this option is selected, even and odd rows in the records list will be drawn using slightly different background colors.



Appearance

☑ Tray icon always visible

☑ Minimize application to the system tray

☐ Close application to the system tray

☐ Simplify user interface appearance

☑ Alternate colors of rows in grid

Appearance options

7.1.3. Security

- ☑ **Log off when the application is inactive** - this option forces automatic log off of the current user on expiry of the given time interval. When the program stays inactive for this period of time, an automatic log off will be performed.

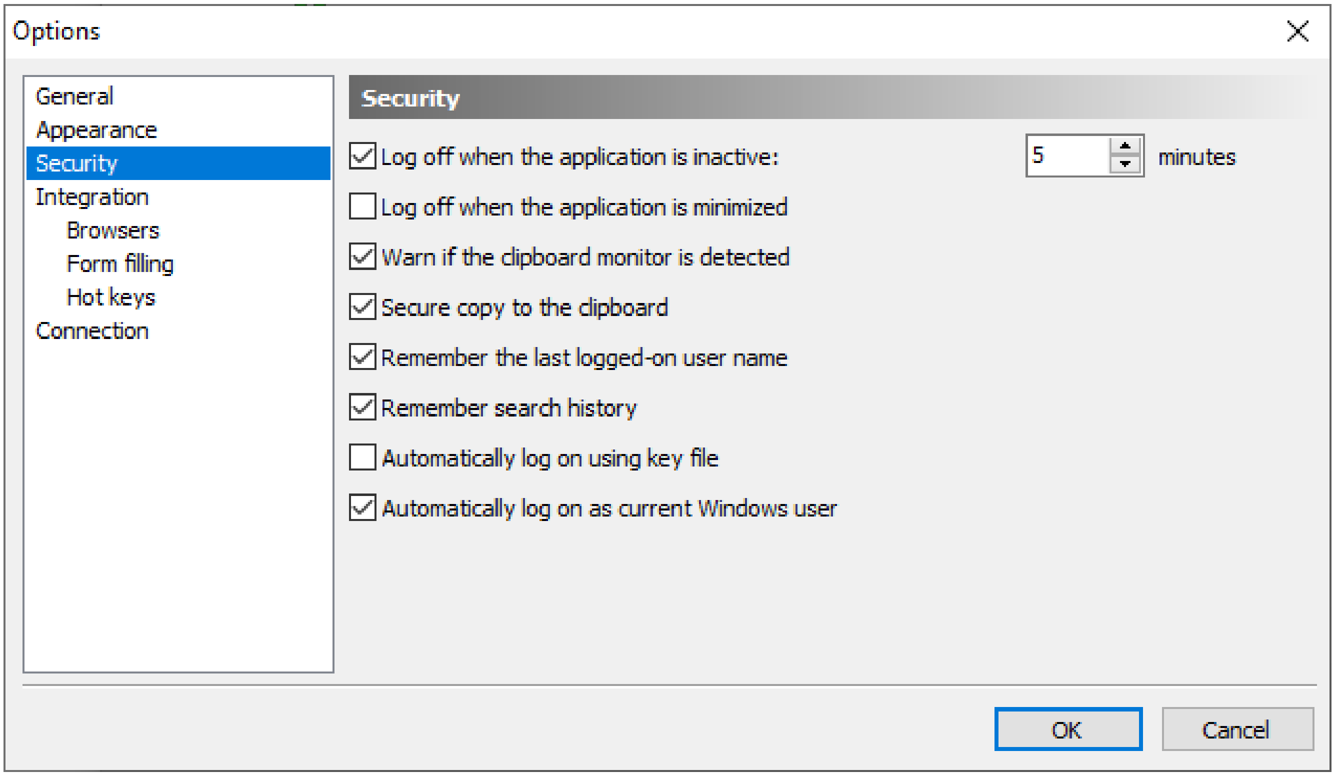
  NOTE: There is also the global inactivity timeout option, which is in effect for all clients. See the **Disconnect a client when inactive** option on the Security page in the Crypt-o system options.

- ☑ **Log off when the application is minimized** - when this option is selected, the current user will be logged off when Crypt-o will be minimized.
- ☑ **Warn if clipboard monitor was detected** - if some application is monitoring the clipboard contents, Crypt-o will warn you.
- ☑ **Secure copy to the clipboard** - when this option is selected, a special secure clipboard operations are performed when you choose to copy a field to the clipboard. See Copying protected fields to the clipboard for more details. When this option is deselected, the regular copy to the clipboard will be used.
- ☑ **Remember the last logged-on user name** - when this option is selected, the name of the last user logged on to Crypt-o will be selected by default next time the program is run.
- ☑ **Remember search history** - when this option is selected, Crypt-o will save 20 recent search queries.
- ☑ **Automatically log on using key file** - when this option is selected, Crypt-o will try to perform automatic log on using a user name and a key file, that were used for the last log on.

  WARNING: Store key files on removable devices, such a USB flash drives, for security reasons. Unplug the device with your key file, when you have finished working with Crypt-o.

- ☑ **Automatically log as current Windows user** - when this option is selected, Crypt-o will try to perform automatic log on of the current Windows user.

  NOTE: This option is available only if automatic log on of the current Windows user is enabled for Crypt-o Client on the Security page in the Crypt-o system options.



Options

Security

☑ Log off when the application is inactive: 5 minutes

☐ Log off when the application is minimized

☑ Warn if the clipboard monitor is detected

☑ Secure copy to the clipboard

☑ Remember the last logged-on user name

☑ Remember search history

☐ Automatically log on using key file

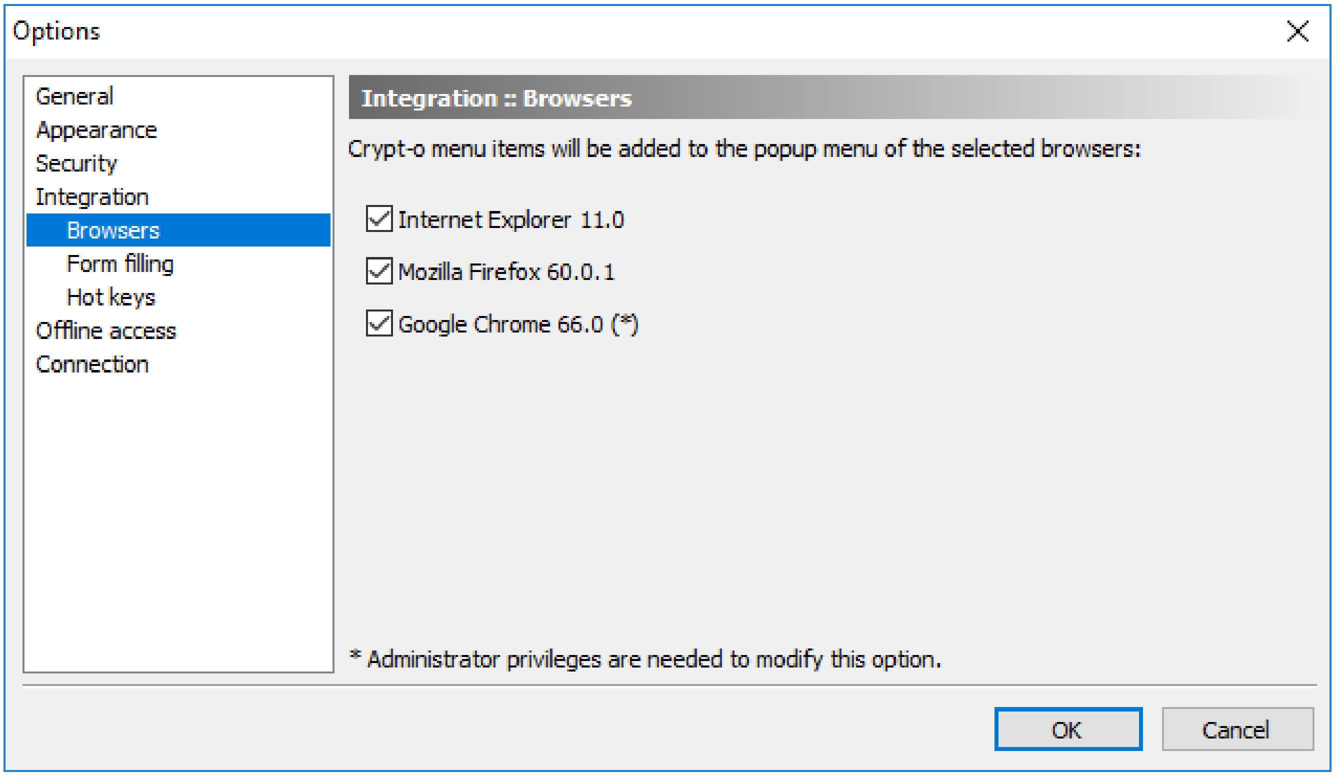
☑ Automatically log on as current Windows user

Security options

7.1.4. Integration :: Browsers

This page lists all internet browsers that has been found in your system. Crypt-o can add menu items to the browser's popup menu to easily use form data filling and saving functions. Also browser integration allow the automatic form filling function in a browser.

NOTE: Popup menu integration is not needed to use form data filling and saving in a browser. You can use hot keys or Crypt-o tray icon menu to do these tasks.



Crypt-o menu items will be added to the popup menu of the selected browsers:

☑ Internet Explorer 11.0

☑ Mozilla Firefox 60.0.1

☑ Google Chrome 66.0 (*)

* Administrator privileges are needed to modify this option.

Browsers integration options

Supported web browsers:

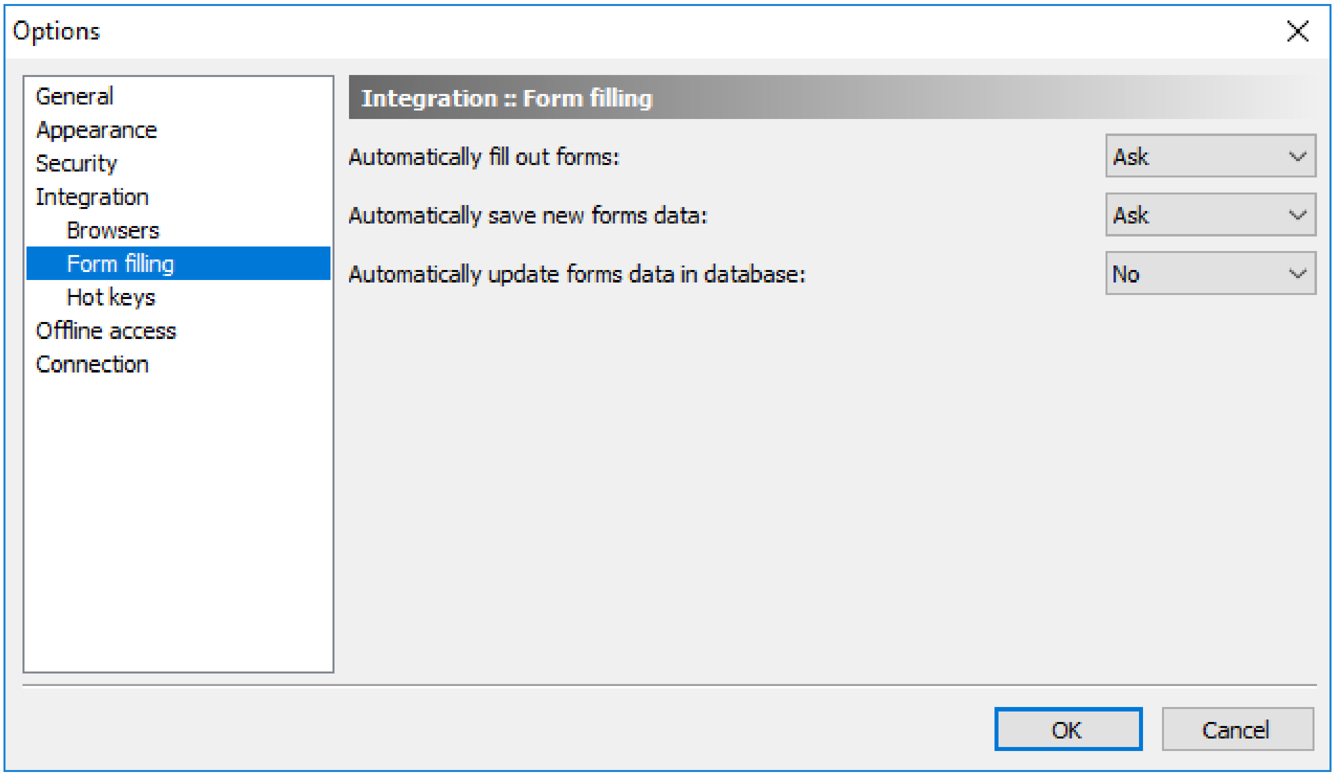
- **Google Chrome** version 49 or later;
- **Microsoft Edge** version 79 or later;
- **Mozilla Firefox** version 52 or later;
- **Microsoft Internet Explorer** version 11.

NOTE: If you accidentally removed the Crypt-o extension in Chrome or Edge, you can re-install it by visiting this page:
https://chrome.google.com/webstore/detail/crypt-o/dcmakiijmdfgijnoamfmbojjmcijfcbl

7.1.5. Integration :: Form filling

This page contains the list of settings that configure form fill parameters:

Automatically fill out forms	This parameter can accept the following values: **Yes** - forms will be filled with data automatically if a match with a record in Crypt-o's database is found. **No** - forms will not be filled with data automatically. **Ask** - user will be asked whether a form is to be filled automatically.
Automatically save new forms data	This parameter can accept the following values: **Yes** - forms filled manually once will be saved automatically in Crypt-o's database. **No** - forms will not be saved in database automatically. **Ask** - a user will be asked whether a form filled manually once is to be saved to database.
Automatically update forms data in database	This parameter can accept the following values: **Yes** - data changes in forms will be automatically updated in Crypt-o's database. **No** - data changes in forms will not be updated automatically. **Ask** - when data in the form is changed, user will be asked whether the changes are to be saved in the database.



Automatically fill out forms: Ask

Automatically save new forms data: Ask

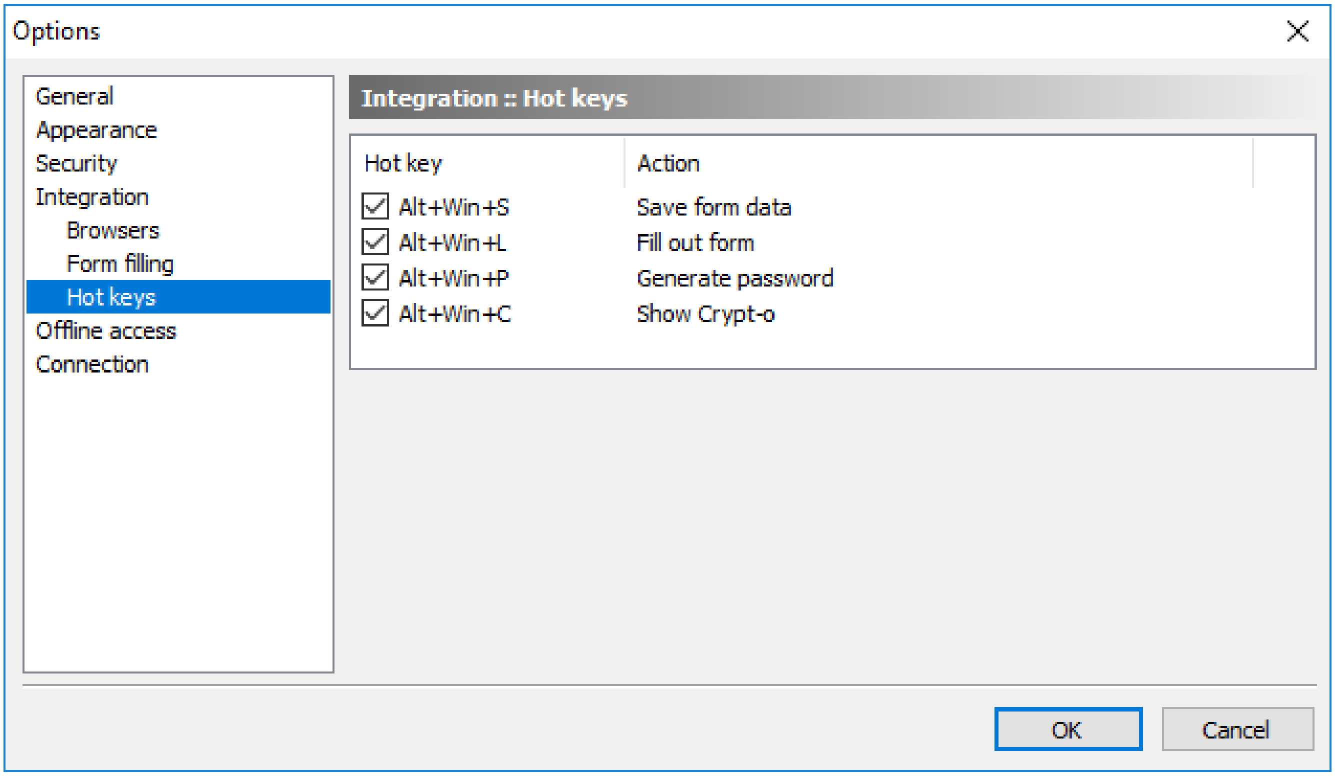
Automatically update forms data in database: No

Form filling options

NOTE: If you do not use the program for long time, it will log off you automatically when the inactivity timeout is reached.

7.1.6. Integration :: Hot keys

This page lists currently assigned hot keys. To modify a hot key double click on its entry.



Hot key	Action
☑ Alt+Win+S	Save form data
☑ Alt+Win+L	Fill out form
☑ Alt+Win+P	Generate password
☑ Alt+Win+C	Show Crypt-o

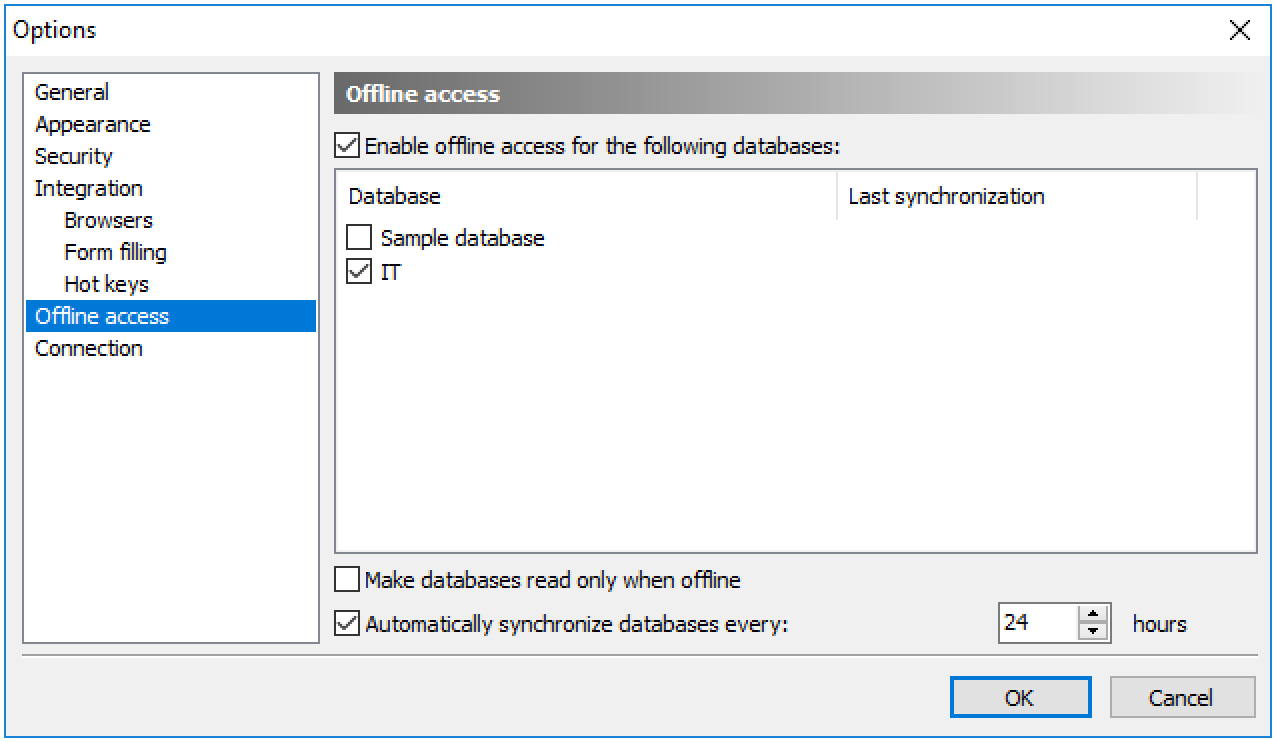
Hot keys options

7.1.7. Offline access

This page lists options to control offline access to databases.
When offline access is enabled, Crypt-o Client automatically switches to the offline mode when a connection to the main server is not possible. You can work with your databases while offline and make changes to the data if needed. Next time you log on to Crypt-o and the connection to the main server is available again, all your changes made in the offline mode will be synchronized with the main server automatically. To force update of the offline data, choose **Tools > Update offline data** in the main menu or simply press **Ctrl+F9**.

- ☑ **Enable offline access for the following databases** - enable this option to allow offline access to the selected databases.
- ☑ **Make databases read only when offline** - when this option is enabled, databases will be read only when accessed offline.
- ☑ **Automatically synchronize databases** - when this option is enabled, the offline databases will be automatically updated with the up to date data from the server. The synchronization is performed in the background. An icon in the status bar is displayed during synchronization.

NOTE: You can also create a portable version of Crypt-o at a USB flash drive.



☑ Enable offline access for the following databases:

Database	Last synchronization
□ Sample database	
☑ IT	

□ Make databases read only when offline

☑ Automatically synchronize databases every: 24 hours

Offline access options

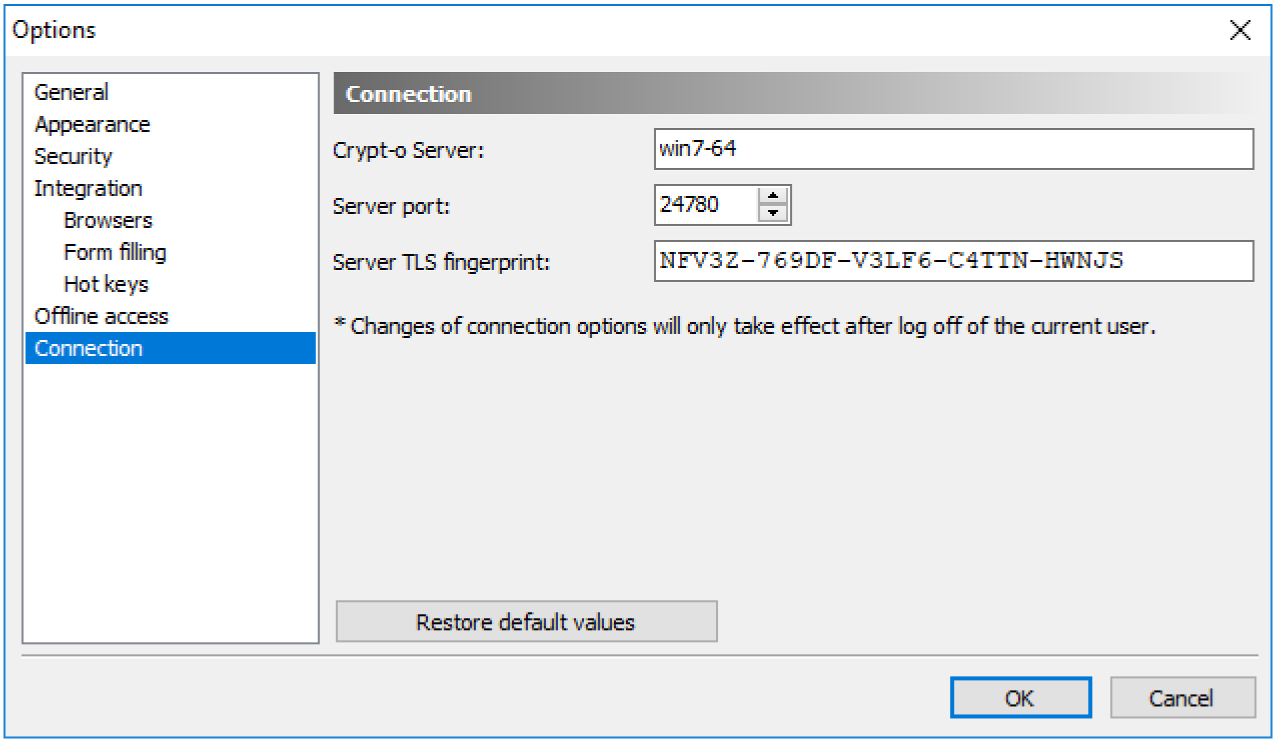
Limitations of the offline mode

- Printing is disabled by default. Use the **Allow printing in portable version** option in the Crypt-o System options to enable it if needed.
- Fields customization is not possible.
- Creation of new databases is not possible.

7.1.8. Connection

This page lists Crypt-o Client connection options.

- **Crypt-o Server** - a host name or an IP address of a computer where the Crypt-o Server is running. You can specify reserve Crypt-o Servers delimited by semicolon.
- **Server port** - a TCP port number, which is used by the Crypt-o Server. By default it is `24780`.
- **Server TLS fingerprint** - an TLS fingerprint of the Crypt-o Server. This TLS fingerprint is used to verify the server TLS certificate and protects against man-in-the-middle hacker attacks.



Crypt-o Server: win7-64

Server port: 24780

Server TLS fingerprint: NFV3Z-769DF-V3LF6-C4TTN-HWNJS

* Changes of connection options will only take effect after log off of the current user.

Connection options

NOTE: You can configure connections to additional Crypt-o Servers if needed.

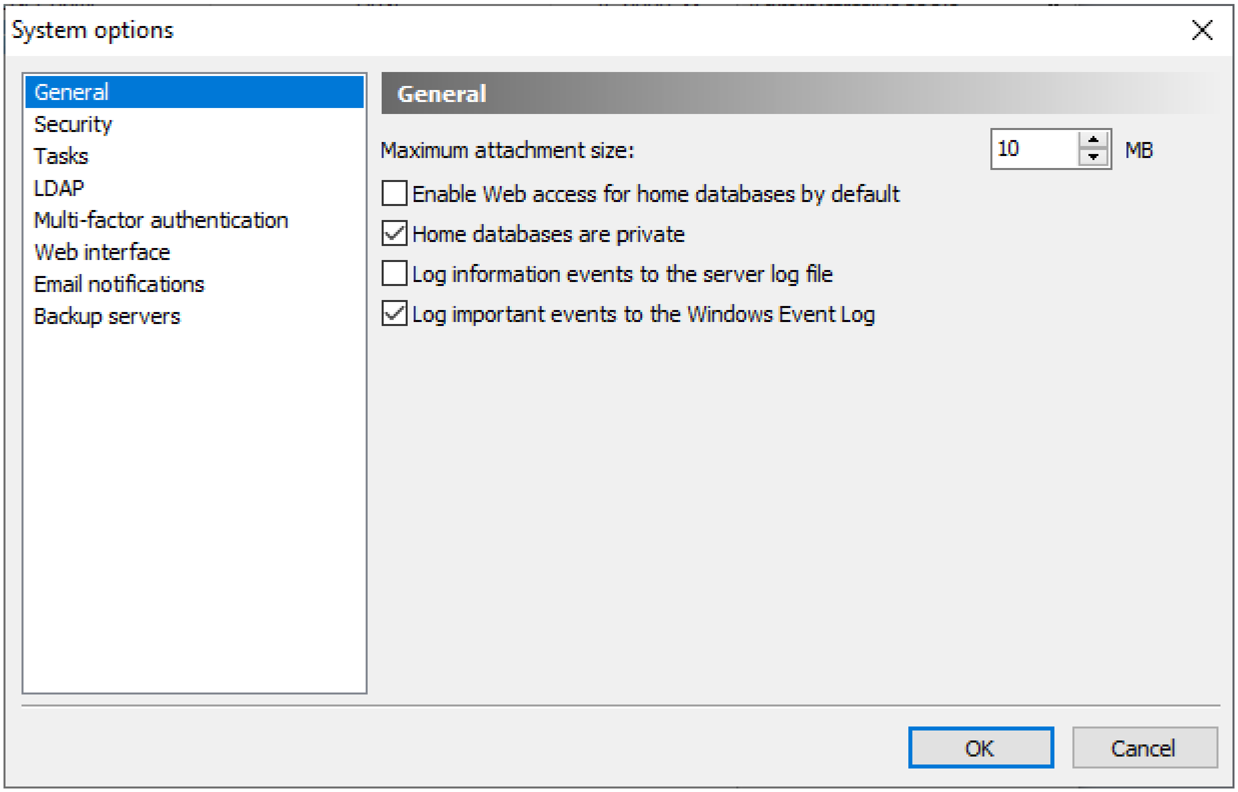
7.2. Crypt-o system options

Only users with the **System administrator** permission can configure Crypt-o system options. To access Crypt-o system options, choose **Tools > Administrative tools** from the menu. Then click on the **System options...** link in the **Administrative tools** panel. Crypt-o system options include the following pages:

- General
- Security
- Tasks
- LDAP
- Multi-factor authentication
- Web interface
- Email notifications
- Backup servers

7.2.1. General

Maximum attachment size - specifies the maximum size of a file attachment. This option applies for all users and databases.
☑ **Enable Web access for home databases by default** - when this option is selected, users will be able to access their home databases via the Web interface. This option applies only for new user accounts.
☑ **Home databases are private** - when this option is selected, new home databases for users are created marked as private.
☑ **Log information events to the server log file** - when this option is selected, information events will be recorded to the `server.log` file located in the data folder of Crypt-o Server.
☑ **Log important events to the Windows Event log** - when this option is selected, important events (errors and warnings) will be recorded to the Windows Event log.



Maximum attachment size: 10 MB
☐ Enable Web access for home databases by default
☑ Home databases are private
☐ Log information events to the server log file
☑ Log important events to the Windows Event Log

System general options

7.2.2. Security

☑ **Require strong passwords for user accounts** - when this option is selected, passwords for user accounts must conform to the following rules:

- minimum password length is 8 characters;
- a password must contain mixed case letters, digits and special symbols.

If this option is not selected, any password longer than 4 characters can be used for user accounts.

⚠ **WARNING:** Do not use weak passwords for user accounts.

☑ **Require strong passwords for Windows and LDAP user accounts** - when this option is selected, passwords for Windows and LDAP user accounts must conform to the rules, described above.

☑ **Key file must be located on removable device** - when this option is selected, users must store their key files on a removable devices. If a key file is not located on a removable device, user log on will fail.

☑ **Disconnect a client when inactive** - this option forces automatic disconnection of inactive client connections on expiry of the given time interval.

☑ **Lock user accounts after failed login attempts** - when this option is selected, Crypt-o will lock user accounts after specified number of failed login attempts.

📝 **NOTE:** Administrator user accounts will not be locked to prevent misuse of this function.

☑ **Prevent users from using previous passwords** - when this option is selected, Crypt-o will keep history of passwords for each user account and prevent users from using passwords found in the history.

Number of passwords in history - specify how many passwords must be kept in the history of used passwords for each user account.

☑ **User account password expiration time** - specify the expiration time for new user passwords in days.

Allow automatic log on as current Windows user in:

☑ **Crypt-o client application** - when this option is selected the Crypt-o Client application is allowed to perform automatic log on of the current Windows user.

📝 **NOTE:** For fully automatic log on of the current Windows user in Crypt-o Client it is also needed to enable the **Automatically log as current Windows user** option on the Security page in the Crypt-o Client options.

☑ **Web interface** - when this option is selected Crypt-o Web interface will send a request to a browser to perform automatic authentication of the current Windows user.

📝 **NOTE:** It is needed to specially configure a web browser to enable automatic SPNEGO/NTLM authentication.

☑ **Portable version expires in X days** - when this option is selected, all portable versions of Crypt-o, created by users, will run only within a specified number of days.

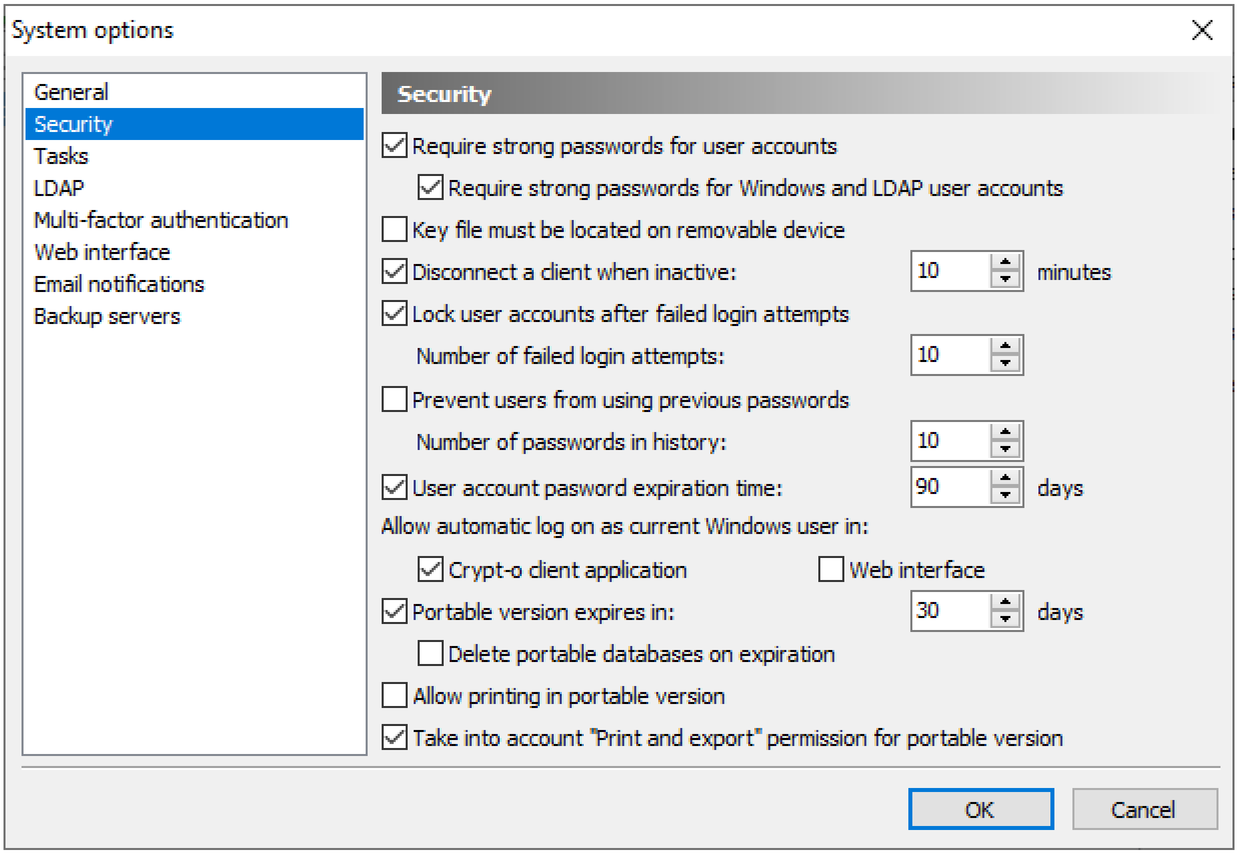
☑ **Delete portable databases on expiration** - when this option is selected, any portable version of Crypt-o will try to delete its portable databases, if the program was launched after its expiration.

⚠ **WARNING:** Use this option on your own risk, since it may lead to loss of all changes, made to portable databases.

☑ **Allow printing in portable version** - when this option is selected, it is possible to print data when running a portable version of Crypt-o.

☑ **Take into account "Print and export" permission for portable version** - when this option is selected (default state), only records with the **Print and Export** permission for a current user will be available in a portable version of a database. If this option is not selected, all records regardless of the **Print and Export** permissions will be available in a portable database.

📝 **NOTE:** A user must have the **Portable mode** permission for a database in order to create a portable version of the database.



System options

Security

☑ Require strong passwords for user accounts

☑ Require strong passwords for Windows and LDAP user accounts

□ Key file must be located on removable device

☑ Disconnect a client when inactive: 10 minutes

☑ Lock user accounts after failed login attempts

Number of failed login attempts: 10

□ Prevent users from using previous passwords

Number of passwords in history: 10

☑ User account pasword expiration time: 90 days

Allow automatic log on as current Windows user in:

☑ Crypt-o client application □ Web interface

☑ Portable version expires in: 30 days

□ Delete portable databases on expiration

□ Allow printing in portable version

☑ Take into account "Print and export" permission for portable version

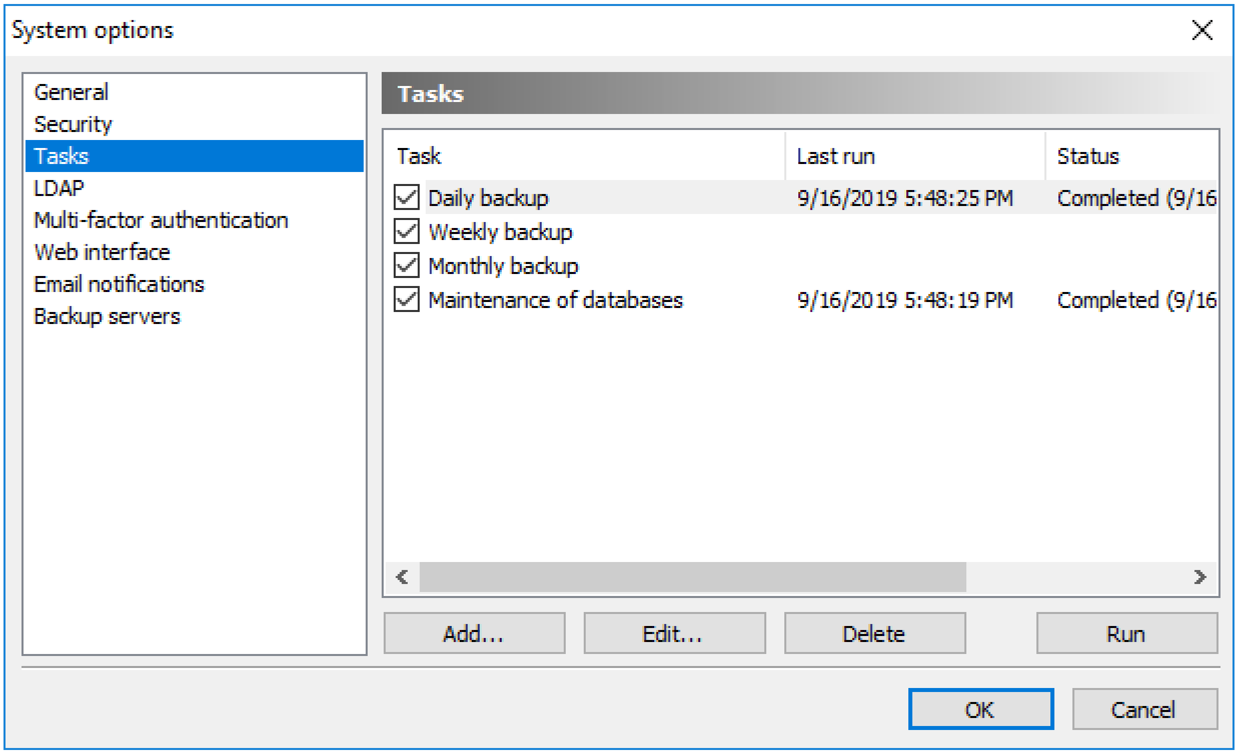
System security options

7.2.3. Tasks

This page lists all automatic tasks. Crypt-o Server executes the tasks in background.

The following tasks are available:

- **Database backup** - this task perform full backup of Crypt-o databases. It is possible to create several backup tasks.
- **Database maintenance** - this task performs maintenance of databases (cleanup, index updates, etc). Only single instance of this task is present.

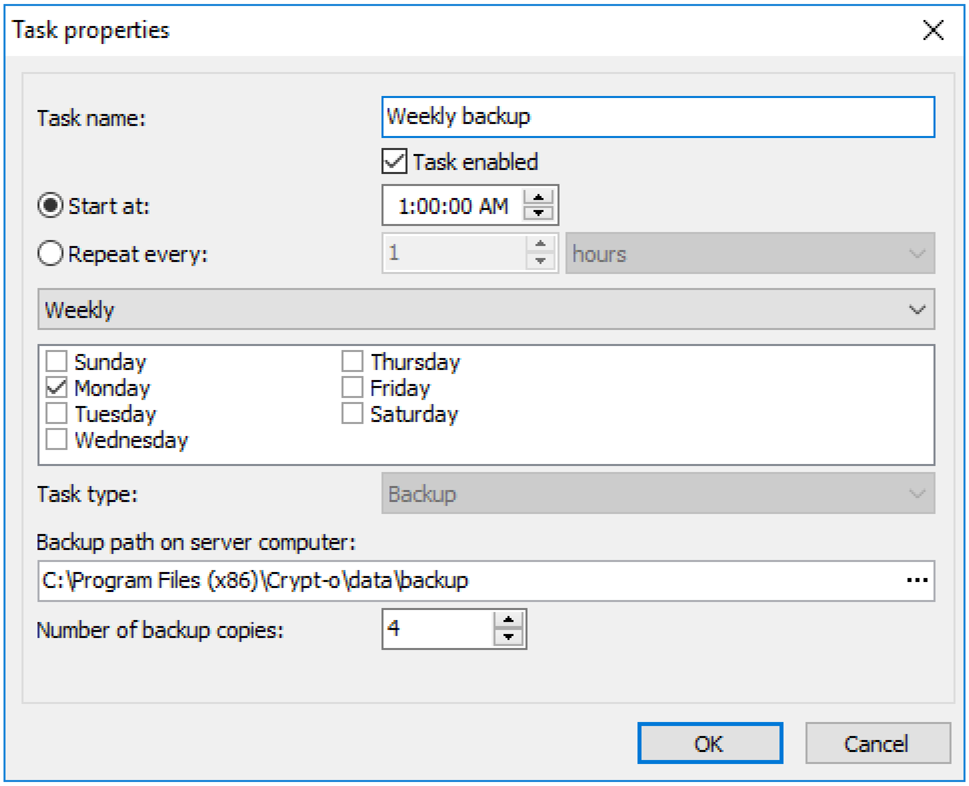


Task	Last run	Status
☑ Daily backup	9/16/2019 5:48:25 PM	Completed (9/16
☑ Weekly backup		
☑ Monthly backup		
☑ Maintenance of databases	9/16/2019 5:48:19 PM	Completed (9/16

System tasks

Click the **Add...** button to add a new task.
Click the **Edit...** button to edit the selected task parameters.
Click the **Delete** button to delete the selected task.
Click the **Run** button to run the selected task.

To enable/disable a task click on a checkbox on the left of the task's name.



Task properties

Task name: Weekly backup

☑ Task enabled

● Start at: 1:00:00 AM

○ Repeat every: 1 hours

Weekly

□ Sunday	□ Thursday
☑ Monday	□ Friday
□ Tuesday	□ Saturday
□ Wednesday	

Task type: Backup

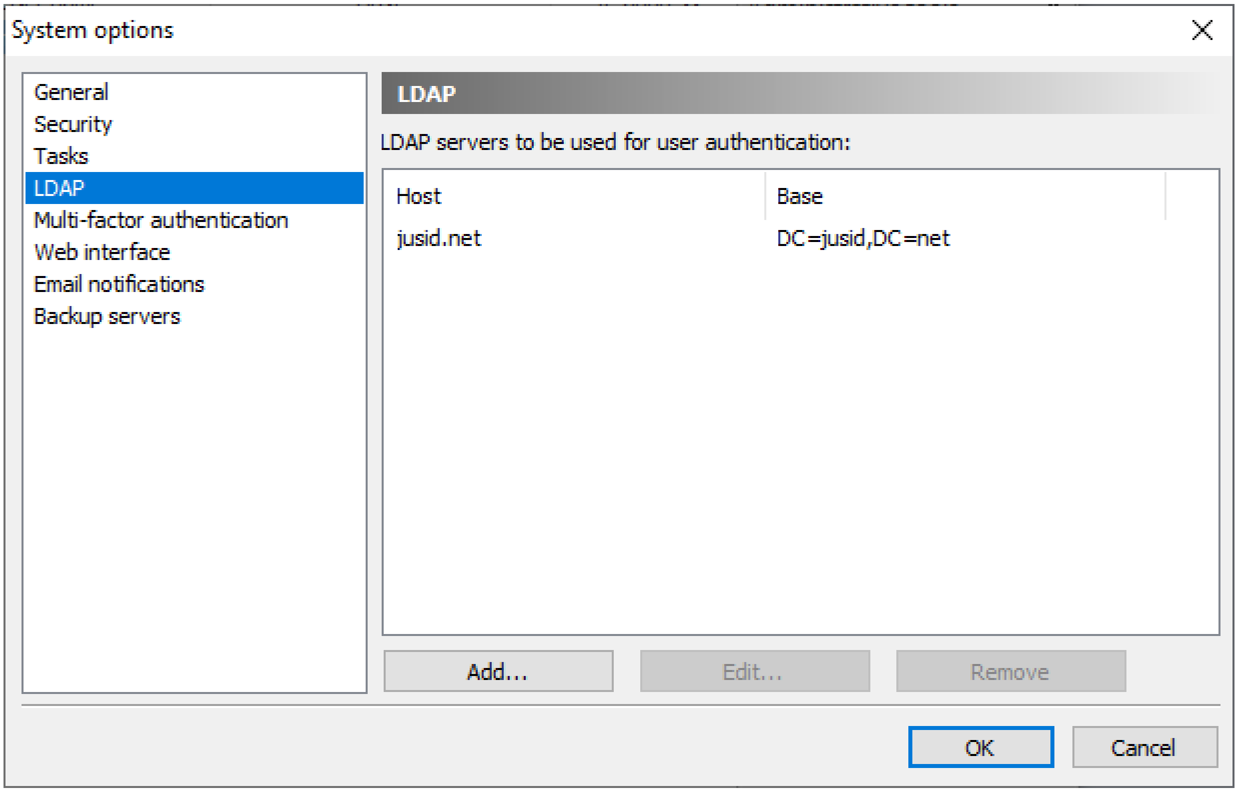
Backup path on server computer:
C:\Program Files (x86)\Crypt-o\data\backup

Number of backup copies: 4

The task properties window

7.2.4. LDAP

Crypt-o can use a LDAP server to authenticate user accounts.
This page lists all registered LDAP servers to be used for user authentication.

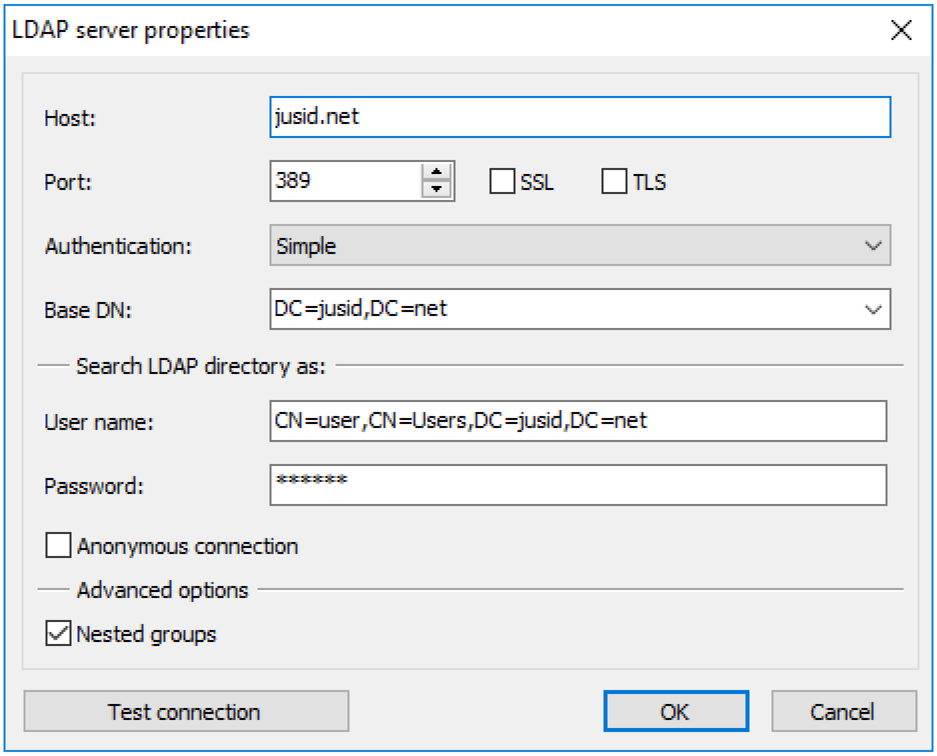


LDAP servers to be used for user authentication:

Host	Base
jusid.net	DC=jusid,DC=net

LDAP servers configuration

Click the **Add...** button to add a new LDAP server.
Click the **Edit...** button to edit parameters of the selected LDAP server.
Click the **Remove** button to delete the selected server from the list.



LDAP server properties

Host: jusid.net

Port: 389 □ SSL □ TLS

Authentication: Simple

Base DN: DC=jusid,DC=net

Search LDAP directory as:

User name: CN=user,CN=Users,DC=jusid,DC=net

Password: *******

□ Anonymous connection

Advanced options

☑ Nested groups

LDAP server properties

Host - specify a host name or IP address of the computer where the LDAP server is running.
Port - TCP/IP port of the LDAP server.

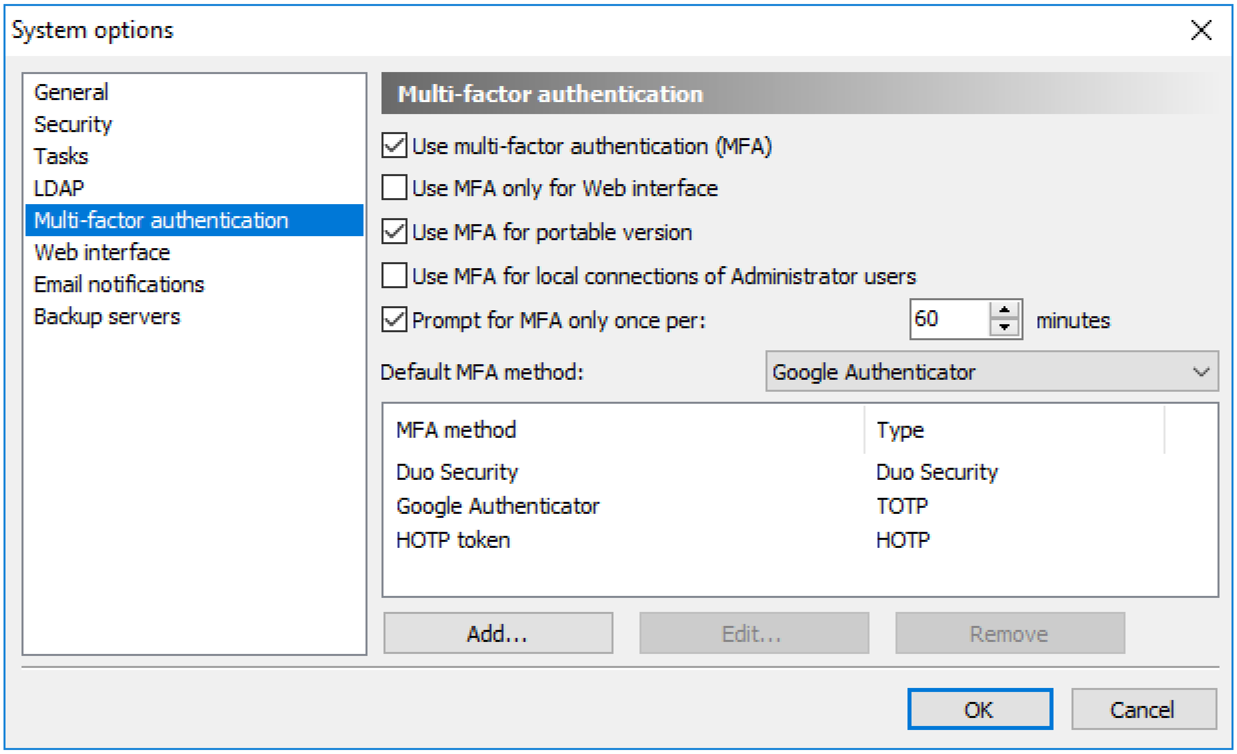
NOTE: If you, for some reason, connect Active Directory, use port **3268** instead of the default port 389. It will improve performance. But it is recommended to use the native Windows authentication support in Crypt-o to authenticate users of a Windows domain.

SSL - Enable SSL connection to the LDAP server.
TLS - Enable TLS connection to the LDAP server.
Authentication - LDAP server authentication type. Possible values - Simple, GSS, GSS SASL.
Base DN - a base distinguished name for the LDAP directory search.
User name - a distinguished name of a user account to be used for the LDAP directory search.
Password - a password of the user account specified in the **User name** box.
Anonymous connection - use the anonymous connection to the LDAP server. For security reasons anonymous connections are disabled for most LDAP servers.
Nested groups - when this option is enabled, Crypt-o will try to recursively find all parent groups for a LDAP user account during the log on. It may slow down the log on process in some cases. If you turn off this option, only immediate groups for a user account will be retrieved from the LDAP server.

Test connection - press this button to test entered connection parameters of the LDAP server.

7.2.5. Multi-factor authentication

You can enable Multi-factor authentication (MFA) to additionally secure user accounts in Crypt-o. Use this page to configure MFA.



Multi-factor authentication

☑ Use multi-factor authentication (MFA)

□ Use MFA only for Web interface

☑ Use MFA for portable version

□ Use MFA for local connections of Administrator users

☑ Prompt for MFA only once per: 60 minutes

Default MFA method: Google Authenticator

MFA method	Type
Duo Security	Duo Security
Google Authenticator	TOTP
HOTP token	HOTP

Configuration of Multi-factor authentication

Crypt-o supports the following MFA types:

- **TOTP** - Time-based One-Time Password algorithm;
- **HOTP** - HMAC-based One-Time Password algorithm;
- **Duo Security**.

The following options are available:

☑ **Use multi-factor authentication (MFA)** - to start using MFA select this option.

☑ **Use MFA only for Web interface** - when this option is selected MFA will be used only when connecting Crypt-o Server via the Web interface. When running Crypt-o Client application, MFA will not be used.

☑ **Use MFA for portable version** - when this option is selected MFA will be also used when running a portable/offline version of Crypt-o.

☑ **Use MFA for local connections of Administrator users** - when this option is selected MFA will be also used when a user with the **System administrator** permission connects to Crypt-o Server using the localhost/loopback interface. This option is not selected by default to allow System administrators to bypass MFA using a local server connection if something went wrong.

☑ **Prompt for MFA only once per** - when this option is selected, Crypt-o will prompt a user to perform MFA only once per the specified time interval.

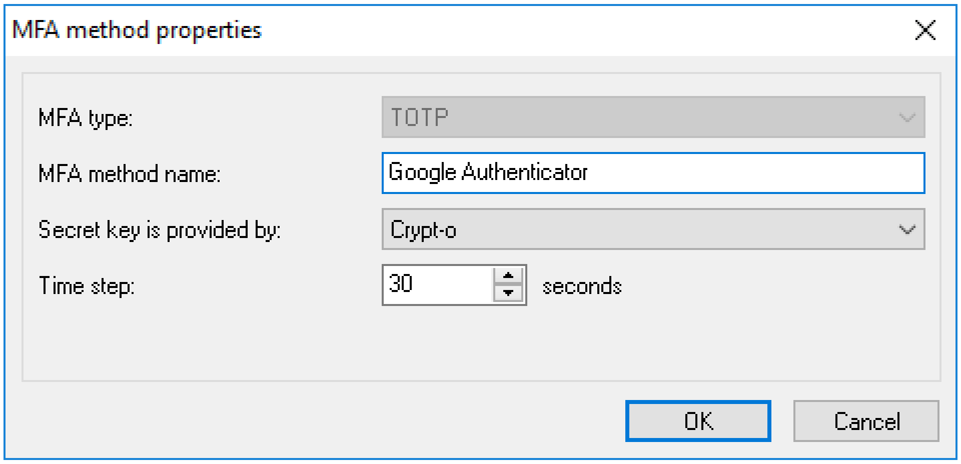
Default MFA method - use this option to select what MFA method will be used by default for all user accounts. If needed you can set an MFA method individually for each user account.

All configured MFA methods are displayed in the list.
Press the **Add...** button to add a new MFA method.
To edit an MFA method select it in the list and press **Edit...**
To delete an MFA method select it in the list and press **Remove**.

NOTE: If you lost administrator access to Crypt-o due to inability to pass the MFA, you can restore access using the following method:

- Use a text editor to open the `server.ini` file in the data folder of Crypt-o Server.
- Find the `UseMFALocalAdmin` parameter in the `[Options]` section and delete it if it exists.
- Save the changes to `server.ini`.
- Restart the Crypt-o Server service.
- Run Crypt-o Client on the computer where Crypt-o Server is running.
- Click **Options...** on the logon prompt.
- Type `localhost` as the **Crypt-o Server** parameter.
- Press **OK** and log on as a user with the **System administrator** permission.

TOTP



MFA type: TOTP

MFA method name: Google Authenticator

Secret key is provided by: Crypt-o

Time step: 30 seconds

TOTP method properties

Time-based One-Time Password algorithm (TOTP) is widely used for Multi-factor authentication. TOTP codes can be generated by a specialized device (token) or by an application running on your phone or tablet.One of the popular free OTP applications is **Google Authenticator**.

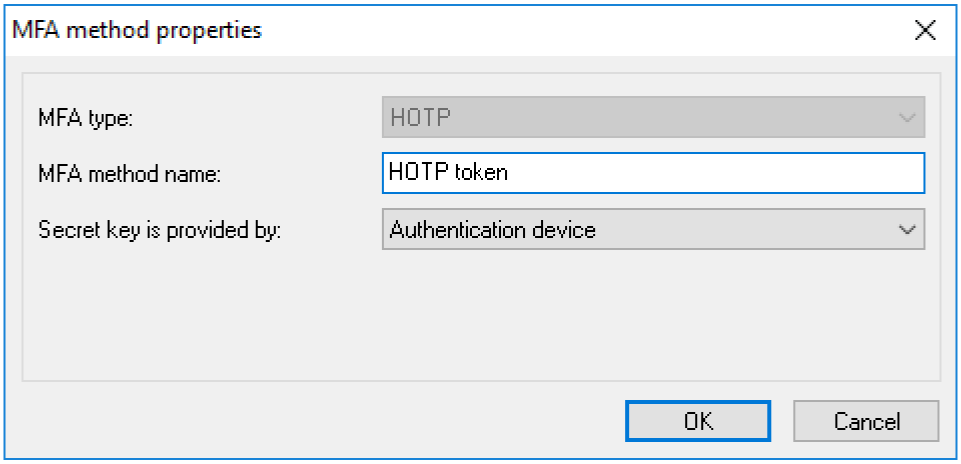
The following TOTP options are available:

MFA type - set it to TOTP.
MFA method name - set a user-friendly display name of this authentication method. It is recommended to use a real device/token name, since it will be presented to users of Crypt-o during MFA processing.
Secret key is provided by - choose which party provides a secret key. This depends of an authentication device you are going to use.

> **Crypt-o** - if this option is selected, Crypt-o will generate a secret key during enrollment of new MFA user. The secret code (in form of a QR-code or text) must be passed to the authentication device to complete the enrollment. Use this option if you are going to use an OTP application such as **Google Authenticator**.
> **Authentication device** - if this option is selected, Crypt-o will request the device's secret key during enrollment of new MFA user. Usually OTP tokens contain pre-generated keys - choose this option in such case.
> **Crypt-o or Authentication device** - if this option is selected, Crypt-o will allow to choose which party provides the secret key during enrollment of new MFA user.

Time step - a time interval to generate distinct TOTP codes. 30 seconds is the default value for most TOTP implementations.

HOTP



MFA method properties

MFA type: HOTP

MFA method name: HOTP token

Secret key is provided by: Authentication device

HOTP method properties

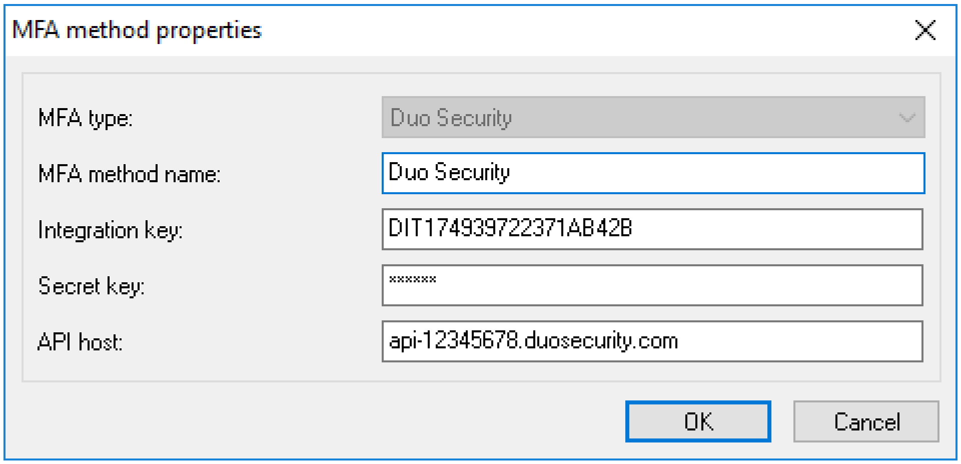
HMAC-based One-Time Password algorithm (HOTP) is widely used for Multi-factor authentication. HOTP codes can be generated by a specialized device (token) or by an application running on your phone or tablet.One of the popular free OTP applications is **Google Authenticator**.

The following HOTP options are available:

MFA type - set it to HOTP.
MFA method name - set a user-friendly display name of this authentication method. It is recommended to use a real device/token name, since it will be presented to users of Crypt-o during MFA processing.
Secret key is provided by - choose which party provides a secret key. This depends of an authentication device you are going to use.

> **Crypt-o** - if this option is selected, Crypt-o will generate a secret key during enrollment of new MFA user. The secret code (in form of a QR-code or text) must be passed to the authentication device to complete the enrollment. Use this option if you are going to use an OTP application such as **Google Authenticator**.
> **Authentication device** - if this option is selected, Crypt-o will request the device's secret key during enrollment of new MFA user. Usually OTP tokens contain pre-generated keys - choose this option in such case.
> **Crypt-o or Authentication device** - if this option is selected, Crypt-o will allow to choose which party provides the secret key during enrollment of new MFA user.

Duo Security



MFA method properties

MFA type: Duo Security

MFA method name: Duo Security

Integration key: DIT174939722371AB42B

Secret key: ******

API host: api-12345678.duosecurity.com

Duo Security method properties

Duo Security is a popular provider of Multi-factor authentication.

In order to use the Duo Security method in Crypt-o, you need:

- Sign up for a Duo account.
- Log in to the Duo Admin Panel and navigate to Applications.
- Click **Protect an Application** and locate `Auth API` or `Web SDK` in the applications list. Click Protect this Application to get your **Integration key**, **Secret key**, and **API host**.

The following options are available for Duo Security:

MFA type - set it to Duo Security.
MFA method name - set a user-friendly display name of this authentication method.
Integration key - copy the integration key from the Application page in the Duo Admin Panel.
Secret key - copy the secret key from the Application page in the Duo Admin Panel.
API host - copy the API host name from the Application page in the Duo Admin Panel.

7.2.6. Web interface

This page is used to configure Crypt-o Web interface.

NOTE: Crypt-o Web interface can be accessed via a secure **HTTPS** connection only. A TLS certificate is needed in order the Web interface to work.

It is recommended to obtain a TLS certificate from a trusted certificate provider. Then assign this certificate to Crypt-o Web interface. In such case, Web browsers will be able to verify the certificate and provide safe access to Crypt-o.

Also it is possible to create and use a untrusted self-signed certificate for Crypt-o Web interface. But it is not recommended, because Web browsers will not be able to verify such certificates.

NOTE: Users can be restricted from accessing certain databases via Web interface using the **Web access** permission.

☑ **Enable Web interface** - when this option is selected the Crypt-o Web interface will be available.
Web interface port - TCP port number for the Web interface.

NOTE: Enter the following URL in your browser to access Crypt-o: https://host.domain.com:24781

`host.domain.com` - is a full DNS name of a computer, where Crypt-o Server is running.
`24781` - a Web interface port.

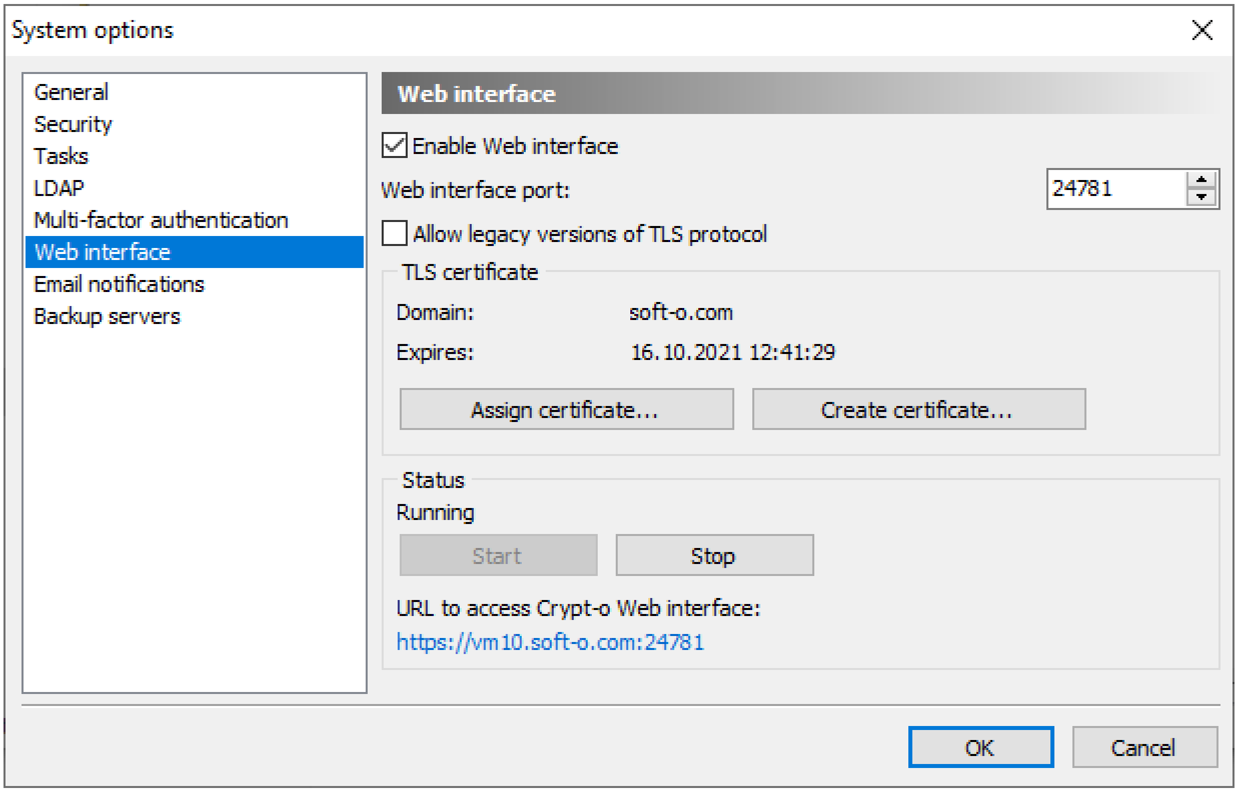
IMPORTANT: Do not use an IP address or short host name in a URL to access Crypt-o Web interface. **Always use a full DNS name of the host**, where Crypt-o Server is running.
Browsers do not store session cookies when an IP address or short host name is used in a URL. In such case, Crypt-o Web interface will direct you to the logon page, when any link is clicked.

☑ **Allow legacy versions of TLS protocol** - when this option is selected, Crypt-o Web interface can be accessed using legacy versions of the TLS protocol (TLS v1, v1.1).

WARNING: TLS v1 and v1.1 protocols are deprecated. Enable these protocols at your own risk only if you need to support access to Crypt-o Web interface using old web browsers.

Assign certificate... - use this button to assign an existing TLS certificate for Crypt-o Web interface. You can purchase an TLS certificate from many providers.
Create certificate... - use this button to create an untrusted self-signed certificate for Crypt-o Web interface.

The current state of Crypt-o Web interface is displayed in the **Status** box. You can start and stop Web interface using the corresponding buttons.



Web interface

☑ Enable Web interface

Web interface port: 24781

□ Allow legacy versions of TLS protocol

TLS certificate

Domain: soft-o.com

Expires: 16.10.2021 12:41:29

Status

Running

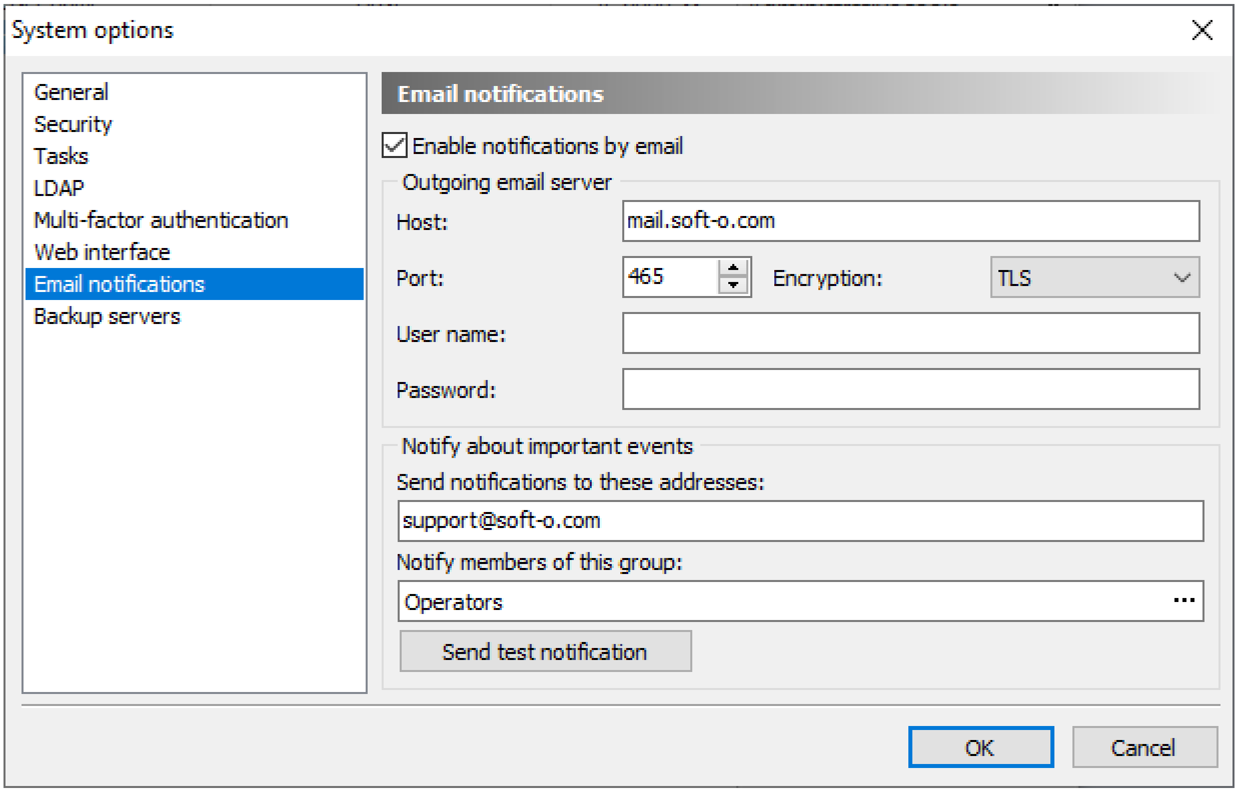
URL to access Crypt-o Web interface:

https://vm10.soft-o.com:24781

Web interface options

7.2.7. Email notifications

You can enable notifications by email about various events in Crypt-o.



☑ Enable notifications by email

Outgoing email server

Host: mail.soft-o.com

Port: 465 Encryption: TLS

User name:

Password:

Notify about important events

Send notifications to these addresses:

support@soft-o.com

Notify members of this group:

Operators

Configuration of email notifications

☑ **Enable notifications by email** - to start receiving notifications by email select this option.

Outgoing email server - parameters of an SMTP email server to be used to send notifications.
Host - a host name or IP address where the email server is running;
Port - a TCP port of the server;
Encryption - encryption mode of connections to the server;
User name and **Password** - optional credentials to perform authentication on the server.

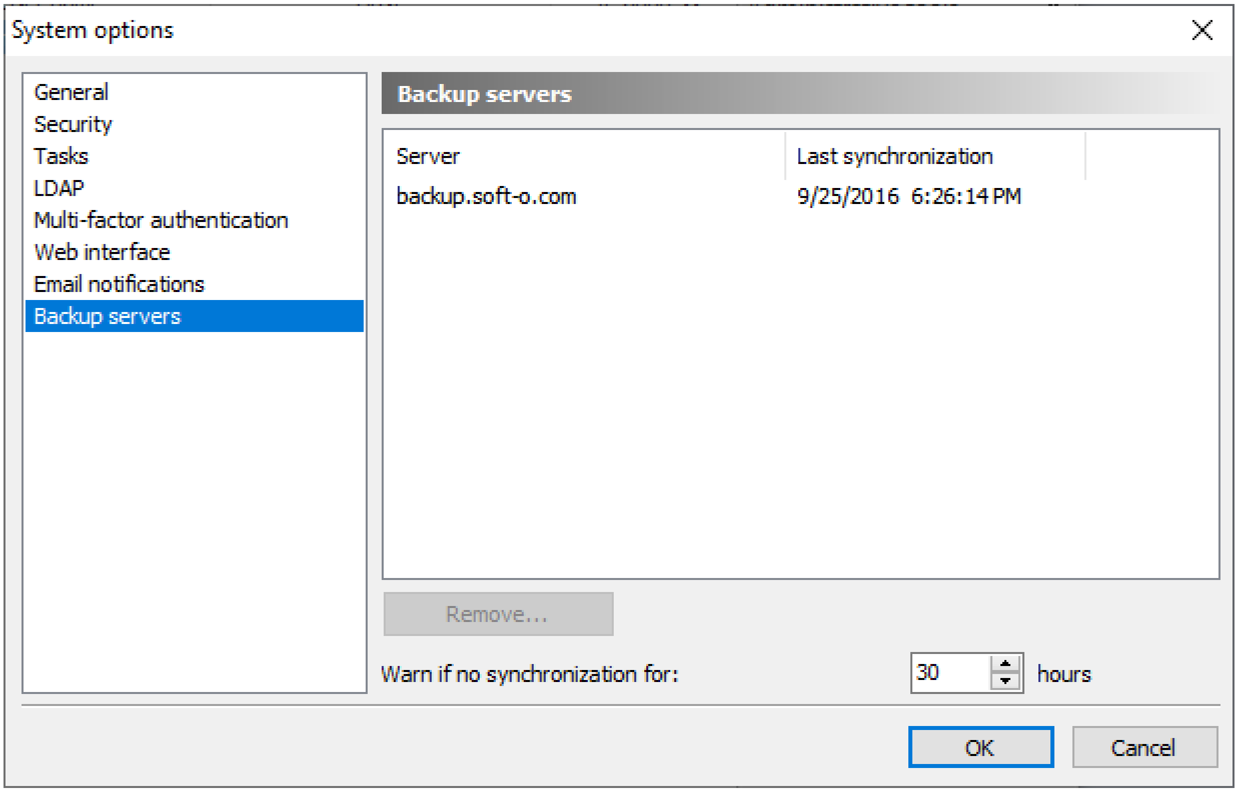
Notify about important events - this section specifies recipients for important events (errors and warnings) which occurs while Crypt-o Server is running.
Send notifications to these addresses - the colon-delimited list of email addresses which will receive notifications. At least one address is required.
Notify members of the following group - optionally specify a group which members will receive notifications if **Email** is specified for a member user account.

Press **Send test notification** to send a notification to the specified recipients to ensure the parameters are correct.

NOTE: You can enable additional object notifications related to records and folders.

7.2.8. Backup servers

This page lists all registered backup servers and date of the last data synchronization.



Server	Last synchronization
backup.soft-o.com	9/25/2016 6:26:14 PM

Warn if no synchronization for: 30 hours

Backup servers status

When you no longer need a backup server, use the **Remove...** button to remove it from the list.

Warn if no synchronization for - Crypt-o issue a warning when a Backup server has not performed synchronization within the specified time in hours.

NOTE: Your can configure email notifications to receive warnings related to synchronization.

7.3. Group Policy Administrative Template

Using the Crypt-o Group Policy Administrative Template, you can set different Crypt-o settings for all users within a Windows domain.

The Crypt-o Administrative Template file `Crypt-o.adm` can be found in the Crypt-o Server installation folder in the `Policy` sub-folder. The Crypt-o Administrative Template in the **ADMX** format can be found in the `Policy\admx` sub-folder.

To install the **ADM** template, open **Group Policy Editor** for your domain and add the Crypt-o Administrative Template file `Crypt-o.adm` to the **User configuration** section.

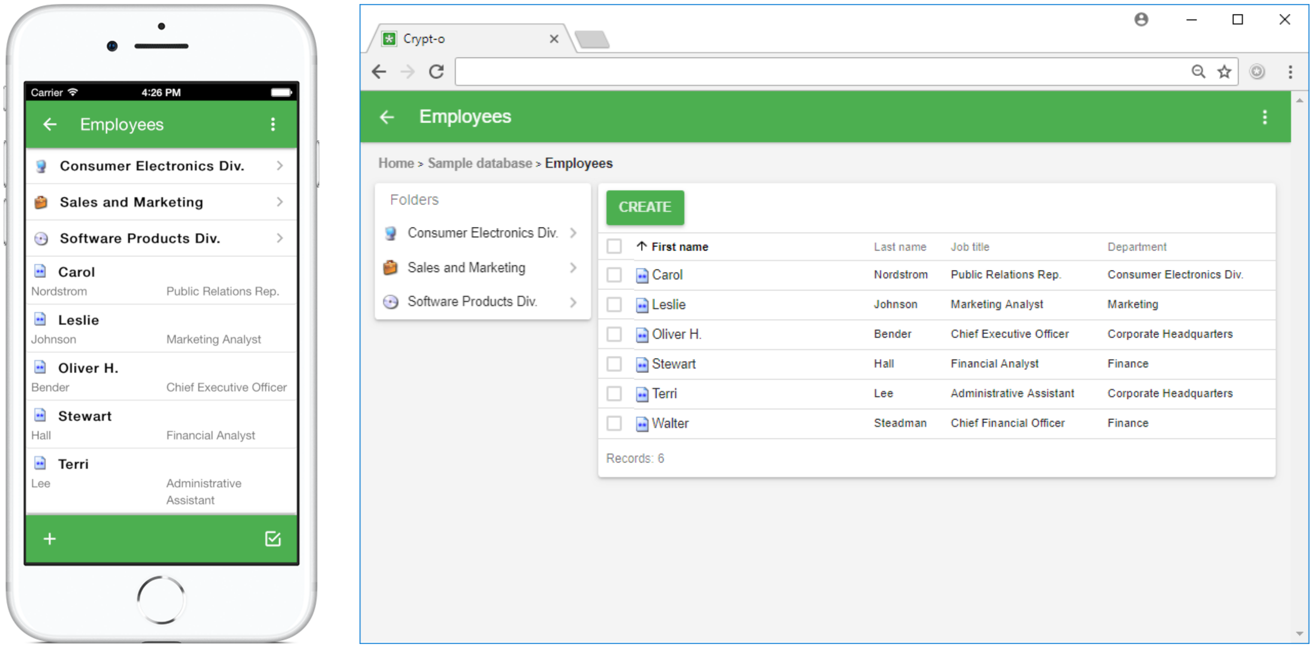
To install the **ADMX** template, copy the `Crypt-o.admx` file and the `en-us` folder to the Central Store of your domain. Then use the Group Policy tools to setup the settings.

The description of each option can be found in **Group Policy Editor** on the **Explain** page.

8. Web interface

Crypt-o provides a Web interface to allow users access Crypt-o on various desktop and mobile systems using a Web browser.
By default Crypt-o Web interface is turned off. To enable and configure Crypt-o Web interface, open the Crypt-o system options on the Web interface page.

Crypt-o Web interface is essentially a cross-platform Web application. To run it as the application you need to open the Web interface in Chrome or Safari and add a link to the Home screen/Desktop. When you click/tap the link, Crypt-o will run as the web application.



↑ First name	Last name	Job title	Department
Carol	Nordstrom	Public Relations Rep.	Consumer Electronics Div.
Leslie	Johnson	Marketing Analyst	Marketing
Oliver H.	Bender	Chief Executive Officer	Corporate Headquarters
Stewart	Hall	Financial Analyst	Finance
Terri	Lee	Administrative Assistant	Corporate Headquarters
Walter	Steadman	Chief Financial Officer	Finance

Records: 6

Crypt-o Web interface running on iPhone as Web application and on a desktop in a browser

Customization

It is possible to customize the Web interface for your needs.

First create a **`user`** sub-folder in the **`web`** folder inside the installation folder of Crypt-o Server.

- To add a custom styling, create the **`user.css`** file in the **`user`** folder. Then add your custom CSS rules to this file.
- To add a custom logo to the main page, put the **`clogo.png`** file to the **`user`** folder.
- To replace a standard image, put the image file with the same name as the standard image to the **`user`** folder.

If you do the customization using this approach, it will be preserved during updates of Crypt-o.

URL query parameters

The following URL query parameters can be used in Crypt-o Web interface:

Parameter	Description
`folder=<path>`	Use this parameter to specify a full path to a folder to be opened. Specify a database name as the first element of the path. Use **`\`** as the path delimiter. Example: **`https:\\host.domain.com:24781?folder=Sample database\Employees\Sales and Marketing`**
`record=<title>`	Use this parameter to specify a title of a record to be opened. You need to

Parameter	Description
	provide the `folder` parameter in order to specify a folder where the record is located. Example: `https:\\host.domain.com:24781?folder=Sample database\Employees\Sales and Marketing&record=Luke`

Compatibility

Crypt-o Web interface should properly work in any modern HTML5-capable web browser.

The following Web browsers were tested:

Desktop systems

- Internet Explorer 9+
- Edge
- Firefox 52+
- Chrome 49+
- Opera 15+
- Safari

Mobile systems

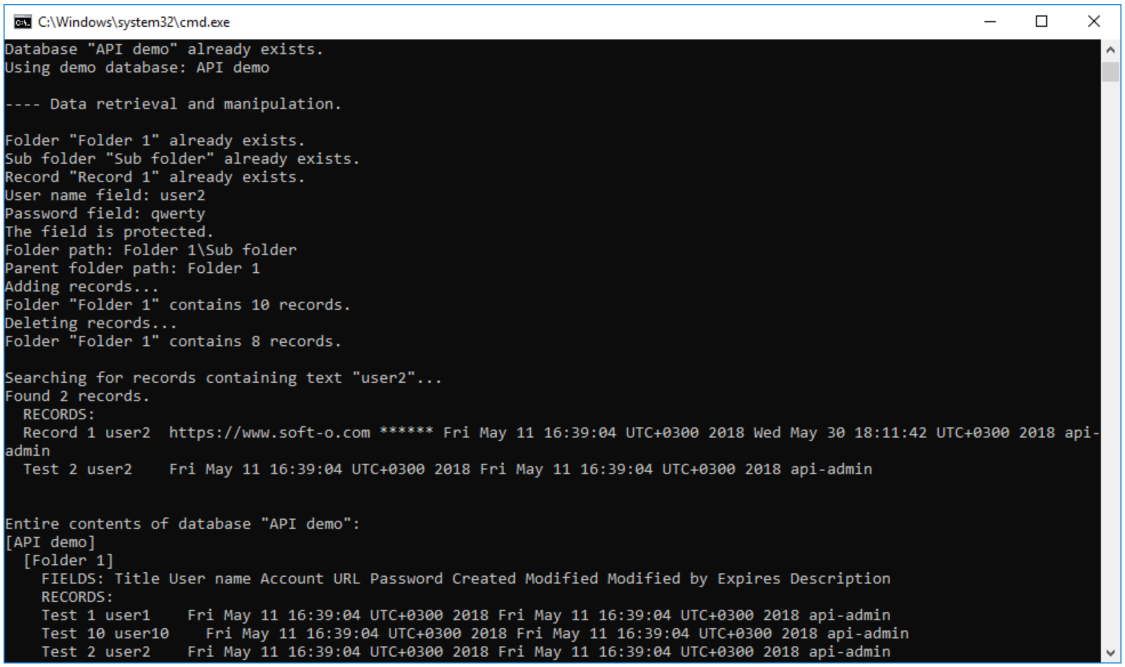
- Mobile Safari on iOS 7.1+ (iPhone/iPad)
- Default web browser on Android 2.3+
- Mobile Chrome 49+ on Android and iOS

9. Crypt-o API

Starting from Crypt-o 3.0 it is possible to use Crypt-o COM API to access and manipulate Crypt-o data via scripting. Crypt-o COM API is language independent. Use your preferred scripting language and engine (**JavaScript**, **PowerShell**, **VBScript**, etc) to access the API.

To use the API you need to install its support files on your computer using the Crypt-o Setup.

Then read the dedicated Crypt-o COM API documentation **`Crypt-o COM API.chm`** to learn how to use the API.



```
Database "API demo" already exists.
Using demo database: API demo

---- Data retrieval and manipulation.

Folder "Folder 1" already exists.
Sub folder "Sub folder" already exists.
Record "Record 1" already exists.
User name field: user2
Password field: qwerty
The field is protected.
Folder path: Folder 1\Sub folder
Parent folder path: Folder 1
Adding records...
Folder "Folder 1" contains 10 records.
Deleting records...
Folder "Folder 1" contains 8 records.

Searching for records containing text "user2"...
Found 2 records.
  RECORDS:
  Record 1 user2  https://www.soft-o.com ****** Fri May 11 16:39:04 UTC+0300 2018 Wed May 30 18:11:42 UTC+0300 2018 api-
admin
  Test 2 user2    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin


Entire contents of database "API demo":
[API demo]
  [Folder 1]
    FIELDS: Title User name Account URL Password Created Modified Modified by Expires Description
    RECORDS:
    Test 1 user1    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
    Test 10 user10    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
    Test 2 user2    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
```

Crypt-o COM API demo

10. Crypt-o Client command line parameters

The following command line parameters can be used with Crypt-o Client:

Parameter	Description
`/user:<user_name>`	A user name to be used for automatic log on.
`/password:<user_password>`	A password for the user, specified by the **`user`** parameter. If the password is not specified, you will be prompted to type it. ⚠ **WARNING:** It is very dangerous to specify passwords in a command line. **Use this parameter at your own risk!**
`/folder:<folder_path>`	A full path to a folder to be automatically selected. The path should be in the following format: `database_name\folder1\folder2`
`/min`	Start the client application minimized to the system tray.

Examples:

```
client.exe /user:"John Smith" /folder:"My database\Finance\Staff"
```

Crypt-o Client will ask a password for user **`John Smith`**. The **`"Finance\Staff"`** folder in database **`"My database"`** will be activated after successful logon.

11. Crypt-o installation

Crypt-o can be installed on any computer running the following operating systems:
Windows 11, Windows 10, Windows Server 2019, Windows Server 2016, Windows 8.1/8, Windows Server 2012/R2, Windows 7, Windows Vista, Windows Server 2008/R2, Windows Server 2003, Windows XP.

Crypt-o has a Client/Server architecture. Thus, you need to install the Crypt-o Server component on some computer. Usually it is one of the server computers in your network. All Crypt-o databases are stored on the server. To access the data, install Crypt-o Clients on needed workstations in your network.

Installation of Crypt-o Server

Run the setup package.

On the **Select Components** page choose **Full installation**.

On the **Crypt-o Server role** page choose a role for this instance of Crypt-o Server.

- **Primary server** - the main server will be installed. There can be only one primary server.
- **Backup server** - additional backup server will be installed. It is allowed to install several backup servers.

On the **Data path** page choose a location where Crypt-o data files will be stored.

📝 **NOTE:** This location is private to this server and must not be available from a network.

On the **Administrator password** page, enter a password for the System administrator user account `admin`. You will be able to log on to Crypt-o using `admin` user name and the specified password.

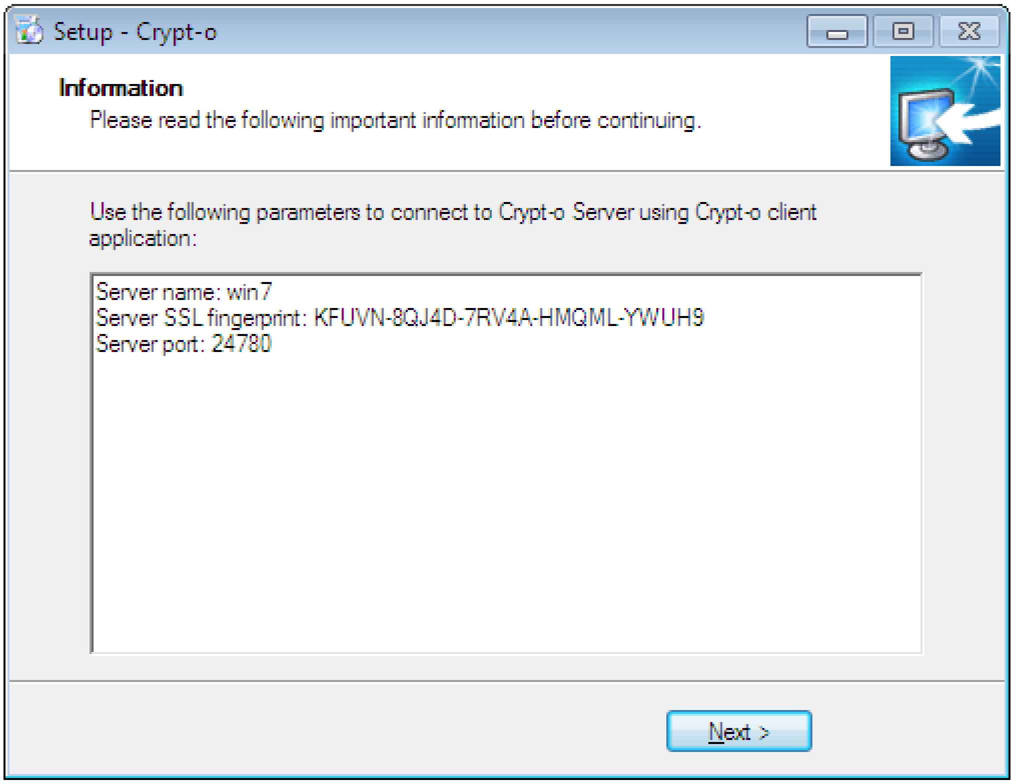
📝 **NOTE:** The password must be at least 8 characters in length and contain mixed case letters, digits and special symbols.

On the **Crypt-o Server access** page, specify a TCP port number for Crypt-o Server. This port will be used to accept secure TLS connections from Crypt-o clients. By default, Crypt-o Server uses TCP port `24780`.

📝 **NOTE:** Configure a firewall on the computer running Crypt-o Server to allow incoming connections to this TCP port.

When the installation will be finished, the **Information** page will appear. This page lists all parameters needed by Crypt-o Clients to connect to Crypt-o Server.

📝 **NOTE:** Save these parameters for later use during Crypt-o Client installations.


Setup - Crypt-o
Information
Please read the following important information before continuing.
Next >

Use the following parameters to connect to Crypt-o Server using Crypt-o client application:

```
Server name: win7
Server SSL fingerprint: KFUVN-8QJ4D-7RV4A-HMQML-YWUH9
Server port: 24780
```

Crypt-o Server connection parameters

Installation of Crypt-o Client

To learn how to automatically install Crypt-o Clients see Deployment topic.
To manually install Crypt-o Client run the setup package.

On the **Select Components** page choose **Client modules only**.

On the **Connection to Crypt-o Server** page, specify a computer name or IP address, where Crypt-o Server is running. Also provide the TLS fingerprint and TCP port of Crypt-o Server.

Read the Quick Start topic for further information how to use Crypt-o.

11.1. Deployment

The easiest way to deploy Crypt-o is to use **Software installation** service of your Windows domain's **Group Policy.** Use Crypt-o setup packaged as **.msi** for that purpose. To fully automate the deployment, you need to install the Crypt-o Group Policy Administrative Template and configure Crypt-o Server connection parameters.

Other way of the deployment is to run an unattended Crypt-o installation on workstations. To do that use command line parameters of the setup program.

11.2. Upgrade

To upgrade an existing installation of Crypt-o to the latest version do the following:

- Download the latest Crypt-o Setup package using this link: https://www.soft-o.com/products/crypt-o/download.html

- Run the Crypt-o Setup package on a computer where Crypt-o Server is running. The setup will update the existing installation automatically. Crypt-o Server can accept connections from older versions of Crypt-o Clients. See the **Upgrade** section in Release notes for the latest version of Crypt-o for details regarding what older versions of the Client are supported by the Server.

- To update Crypt-o Clients run the Setup package on client computers. The setup will update the existing installation automatically. Run the setup either manually or automate its deployment using Group Policy or other tools.

NOTE: It is not needed to uninstall an existing version of Crypt-o before the upgrade. The setup package will update the existing installation automatically.

Upgrading your licenses

Crypt-o licenses are valid for a given major version (1.x, 2.x, 3.x, etc). Therefore it is not needed to purchase a new licenses when you upgrade to a new minor version of Crypt-o of the same major version as your licenses. E.g. if you own licenses for Crypt-o 3.x you can upgrade from version 3.0 to version 3.1 and your licenses remain valid.

If you own Crypt-o licenses of an older major version (e.g. 1.x or 2.x), you are eligible for upgrade to the current major version at 50% discount of the full price.

NOTE: When you install a newer major version of Crypt-o over your existing installation of an older major version, the new version will be fully functional for 30 days. So you can test all new features and have time to purchase upgrade licenses while using the new version.

To purchase upgrade licenses do the following:

- Install the latest version of Crypt-o on the server computer over your existing installation of an older major version of Crypt-o;
- Run the client application;
- Log on as a user with administrator privileges;
- Select the **Help - About...** in the menu to open the About window;
- Follow the upgrade link in the About window.

Restoring a previous version of Crypt-o

Sometimes it is needed to restore a previous version of Crypt-o - the upgrade has not gone smoothly or there are bugs in the new version.

Please follow these steps to perform the downgrade:

- Run a setup package of an older version of Crypt-o on a computer where Crypt-o Server is running.

- Run Crypt-o Client on the server computer and try to log on. If you get a database structure error, you need to restore a backup file which was made automatically before upgrading the database structure.
  By default backup files are located in the **`backup`** sub-folder in the data folder of Crypt-o Server. The default location of backup files is **`C:\Program Files (x86)\Crypt-o\data\backup`**.
  Look for a recent backup file named **`db-vX.Y.Z-before-upgrade-DATE_TIME.bak`**. Since you can't log on to perform the restore using Crypt-o Client, you need to restore from a backup file using the command line.

- Downgrade client installations by running the setup package.

11.3. Setup program's command line parameters

Crypt-o setup program's command line parameters can be used for an unattended installation.
The following command line parameters are valid for the **.EXE** setup package. To pass parameters to the **.MSI** setup package you need to specify these parameters as the `CMDLINE` property. See the examples below for more information.

`/SILENT, /VERYSILENT`
Instructs Setup to be silent or very silent. When Setup is silent the wizard is not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed.

`/DIR="x:\dirname"`
Overrides the default directory name displayed on the **Select Destination Location** wizard page. A fully qualified pathname must be specified.

`/GROUP="folder name"`
Overrides the default folder name displayed on the **Select Start Menu Folder** wizard page.

`/TYPE=type name`
Overrides the default setup type. If the specified type exists and isn't a custom type, then any `/COMPONENTS` parameter will be ignored.
The following setup types can be used: `full`, `client`.
Default: `full`.

`/COMPONENTS="comma separated list of component names"`
Overrides the default component settings. Only the specified components will be selected; the rest will be deselected.
The following component names can be used: `Client`, `Server`, `API`, `Help`.

`/TASKS="comma separated list of task names"`
Specifies a list of tasks that should be initially selected. Only the specified tasks will be selected; the rest will be deselected.
The following task names can be used:

- `integration` - integrate Crypt-o Client with Internet browsers;
- `firewall` - add an exception for Crypt-o to the Windows Firewall;
- `desktopicon` - create a desktop icon;
- `quicklaunchicon` - create a quick launch icon;
- `iconscommon` - create program's shortcuts for all users;
- `iconsuser` - create program's shortcuts for the current user only.

Default: "`integration,firewall,desktopicon,iconscommon"`

`/SERVER=server name`
A host name or IP address of a computer where Crypt-o Server is running.

`/FINGERPRINT=server fingerprint`
An TLS fingerprint of Crypt-o Server.

`/PORT=port`
A TCP port number of Crypt-o Server. Default: `24780`.

`/NORESTART`
Instructs Setup not to reboot even if it's necessary.

Examples

How to silently install the Crypt-o client with desired connection parameters using the **.EXE** setup:

```
Crypt-o-Setup.exe /VERYSILENT /TYPE=client /SERVER=server.domain.com
```

```
/FINGERPRINT=AAAAA-BBBBB-CCCCC-DDDDD-EEEEE
```

How to do the same setup using the **.MSI** package:

```
msiexec /i Crypt-o-Setup.msi CMDLINE="/VERYSILENT /TYPE=client
/SERVER=server.domain.com /FINGERPRINT=AAAAA-BBBBB-CCCCC-DDDDD-EEEEE"
```

11.4. Moving Crypt-o Server

To move an existing Crypt-o Server to other computer follow these steps.

- Make sure you can access Crypt-o using a user account with administrator privileges and the **internal authentication** method.
- Uninstall Crypt-o on backup servers (if any).
- Install Crypt-o Server on the **new** computer.
- Stop the Crypt-o Server service on the **new** computer.
- Stop the Crypt-o Server service on the **old** computer.
- Copy contents of the Crypt-o data folder from the **old** computer to the **new** computer, replacing existing files.
- Start the Crypt-o Server service on the **new** computer.
- Log on to Crypt-o as an administrator, open Administrative tools, System options. Go to Tasks page, open each backup task and check if a backup folder is correct.
- Change connection parameters for all Crypt-o Client installations to use the host name of the **new** computer. The Crypt-o Server fingerprint will be the same, since you have moved all configuration.
- If needed, install and configure backup servers using the new Crypt-o Server as the primary server.
- Make sure the new Crypt-o Server works properly.
- Now you can permanently stop (or uninstall) Crypt-o Server on the **old** computer.

12. Backup Servers

To improve availability of Crypt-o Server, it is possible to set up additional backup servers. They will synchronize all data with the primary server on a specified schedule (by default once per day). When the primary server becomes unavailable, Crypt-o Clients will connect to backup servers automatically.

📝 **NOTE:** Backup servers do not allow data modifications and are used in emergency cases only.

Setting up a backup server

First, you need to create a new user account for a backup server on the main server. To do that, go to the User management window and choose **Action > New backup server account...** from the menu. The single user account can be used by several backup servers. Make sure that the **Allow transfer of server private data** is turned on for the user account prior to installing a new backup server.

Then run the Crypt-o Setup package on a computer, where the backup server will be running.

On the **Select Components** page choose **Full installation**.

On the **Crypt-o Server role** page choose the **Backup server** as a role for this instance of Crypt-o Server.

On the **Data path** page choose a location where Crypt-o data files will be stored.

📝 **NOTE:** This location is private to this server and must not be available from a network.

On the **Configuration of backup Crypt-o Server** page specify a computer name or IP address, where the primary Crypt-o Server is running, provide the TCP port and the TLS fingerprint of the primary Crypt-o Server. Also specify a user name and password of the specialized user account to be used to connect to the primary Crypt-o Server.

Complete the installation. The backup server will be installed and initialized.

To view status of backup servers open the Crypt-o system options on the Backup servers page.

13. Support and Registration

13.1. Registration

If you would like to order our products, you can do the registration **online** on the Internet by secure web site **ShareIt!** directly from the registration page. If you do not have access to the Internet, you can register via **phone**, **fax** or **postal mail**.

On purchase you receive:

- fully functional, unrestricted copy of Crypt-o;
- free and priority technical support by e-mail;
- free upgrades to all minor releases, until the next major release of the software.

For questions regarding Crypt-o purchase write to sales@soft-o.com.

📝 **NOTE:** We offer **10 FREE licenses of Crypt-o**, if you translate Crypt-o user interface to a language, which is not available yet. See the list of languages.

13.2. Unregistered version limitations

Crypt-o is distributed on a **Try Before You Buy** (shareware) basis. The evaluation (trial) version will work without any functionality limitations for **30 days** after the first install.

> **NOTE:** An unregistered version of Crypt-o will work in **read only mode** after end of the trial period.

If you like this program and decide to keep it, you will need to purchase a license. All functions will be available and limitations will be removed as soon as you register your copy of Crypt-o.

> **NOTE:** There is no need to reinstall the currently installed trial version of Crypt-o after you purchase a license. Just enter a registration code to register the program.

13.3. Technical support

You can send a message to our technical support team with your questions, bug reports or ideas. All errors found will be corrected as soon as possible.

Technical support for Crypt-o is provided via electronic mail solely.

Please provide us with the following information when contacting tech support:

- problem description along with the actions being taken before the problem occurred;
- Crypt-o version;
- your Windows version;
- your browser and its version.

14. Release notes

This page contains notes for Crypt-o releases.
You can also read the complete History of changes.

- Crypt-o 3.0
- Crypt-o 3.1
- Crypt-o 3.2
- Crypt-o 3.3
- Crypt-o 3.4

14.1. Crypt-o 3.0

Crypt-o 3.0 is a major release. This means existing licenses of Crypt-o need to be upgraded for use with Crypt-o 3.x.
If you already own a Crypt-o license and upgrade your existing installation of Crypt-o to version 3.0, you will get a 30 day trial of Crypt-o 3.0 with unrestricted functionality. Also you may wish to install Crypt-o 3.0 on a test server to evaluate the new version. You can register Crypt-o using your existing registration to get full 30 day trial.

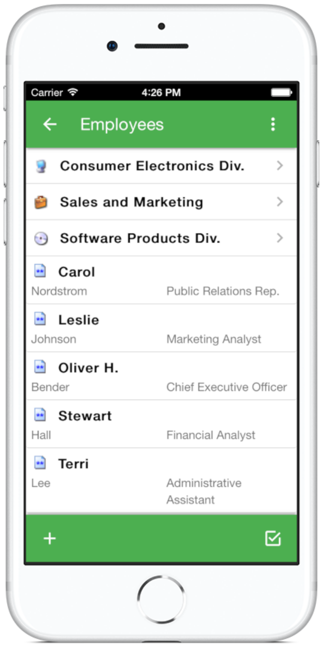
Users who already own a Crypt-o license are eligible for upgrade to version 3.x at 50% discount. To purchase an upgrade run the client application of Crypt-o 3.0, log on, select the **Help - About...** menu and follow the upgrade link in the About window.

Highlights of Crypt-o 3.0

Web interface

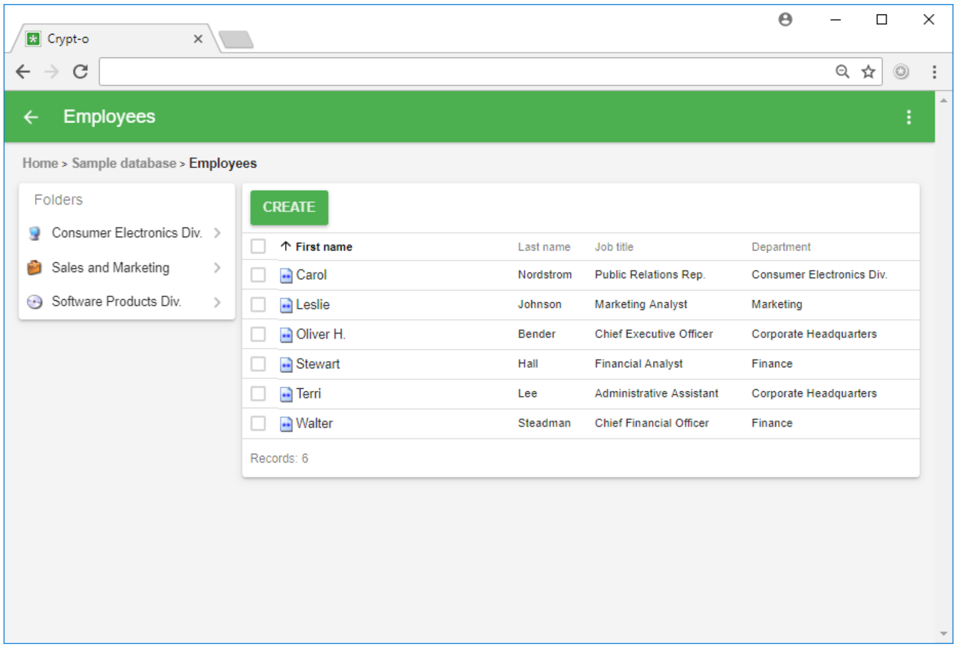
The Web interface has been reworked completely. It is essentially a cross-platform Web application now.
New functions:

- Records and folders can be copied and moved.
- Files can be attached to records.



Consumer Electronics Div.
Sales and Marketing
Software Products Div.

Carol Nordstrom	Public Relations Rep.
Leslie Johnson	Marketing Analyst
Oliver H. Bender	Chief Executive Officer
Stewart Hall	Financial Analyst
Terri Lee	Administrative Assistant



Home > Sample database > Employees

Folders
Consumer Electronics Div.
Sales and Marketing
Software Products Div.

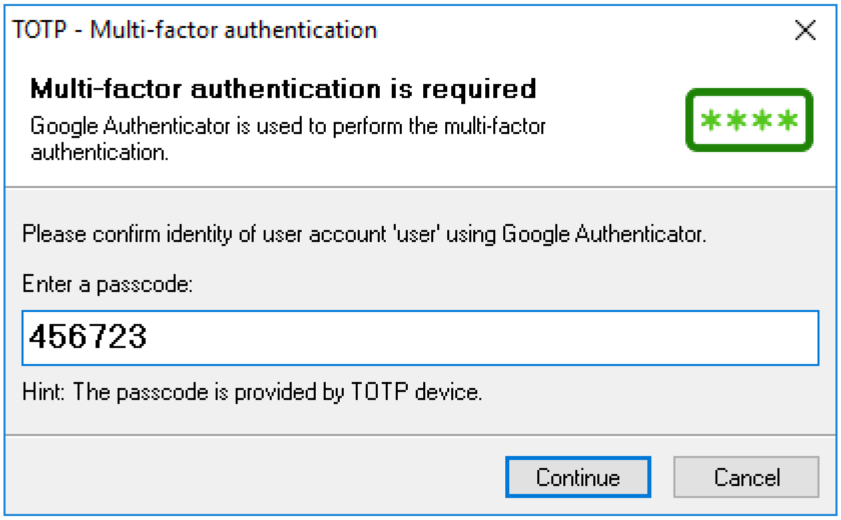
	First name	Last name	Job title	Department
□	Carol	Nordstrom	Public Relations Rep.	Consumer Electronics Div.
□	Leslie	Johnson	Marketing Analyst	Marketing
□	Oliver H.	Bender	Chief Executive Officer	Corporate Headquarters
□	Stewart	Hall	Financial Analyst	Finance
□	Terri	Lee	Administrative Assistant	Corporate Headquarters
□	Walter	Steadman	Chief Financial Officer	Finance

Records: 6

Multi-factor authentication

Crypt-o now supports Multi-factor authentication for user accounts.
The following MFA types are supported:

- TOTP - Time-based One-Time Password algorithm;
- HOTP - HMAC-based One-Time Password algorithm;
- Duo Security.



Multi-factor authentication is required

Google Authenticator is used to perform the multi-factor authentication.

Please confirm identity of user account 'user' using Google Authenticator.

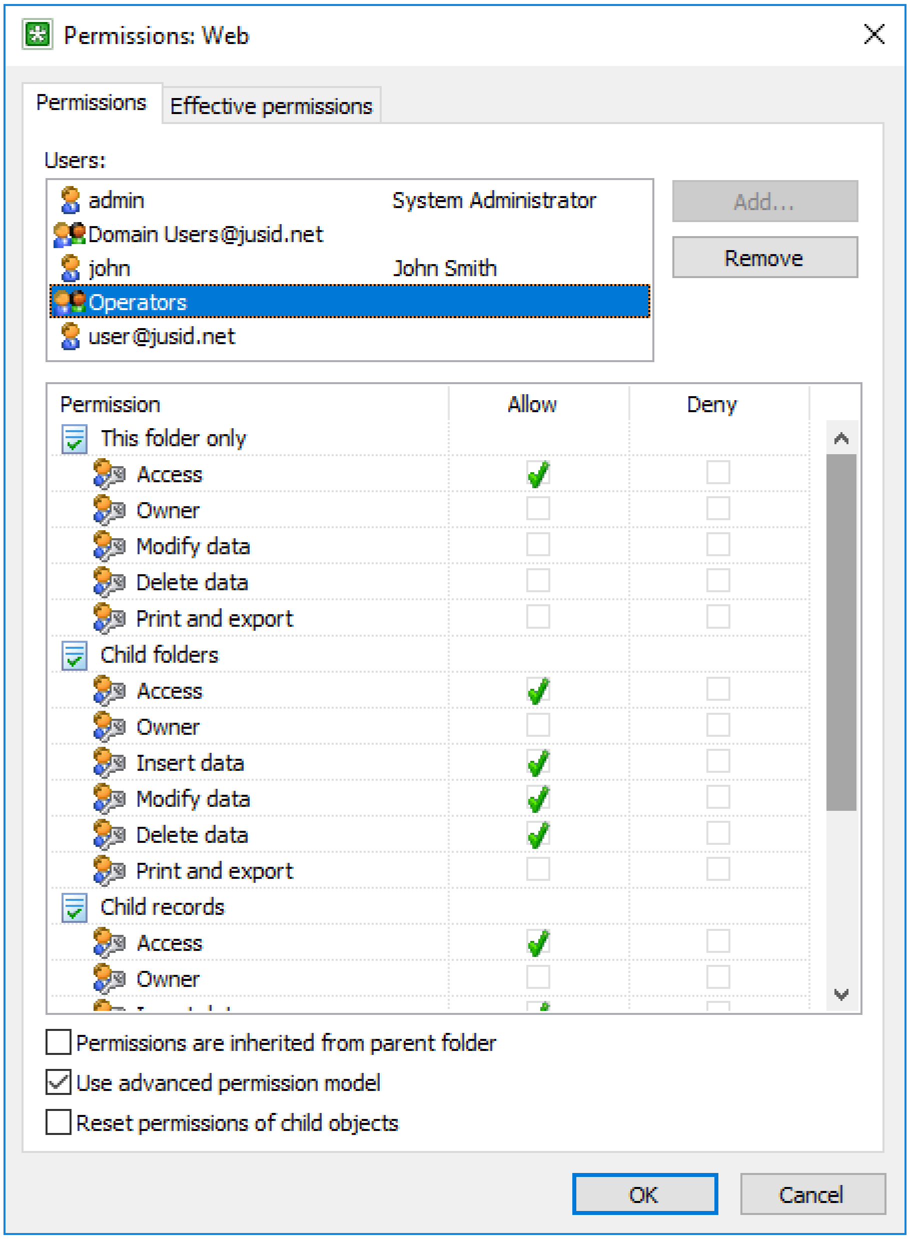
Enter a passcode: 456723

Hint: The passcode is provided by TOTP device.

Permissions

The object permissions system has been vastly improved.

- You can switch object permissions to the Advanced model. It allows permissions to be separately applied to: **This folder only**, **Child folders**, **Child records**.
- Object permissions can be adjusted without turning off inheritance.
- Object owners can select a user account to view its effective permissions for the object.
- New system permissions: **User management** and **Access via API**.
- It is prohibited to set Deny for the "Administrator" and "Database Owner" permissions. It will eliminate accidental loss of access to whole Crypt-o or individual databases.



Users:

admin	System Administrator
Domain Users@jusid.net	
john	John Smith
Operators	
user@jusid.net	

Permission	Allow	Deny
This folder only		
Access	✓	□
Owner	□	□
Modify data	□	□
Delete data	□	□
Print and export	□	□
Child folders		
Access	✓	□
Owner	□	□
Insert data	✓	□
Modify data	✓	□
Delete data	✓	□
Print and export	□	□
Child records		
Access	✓	□
Owner	□	□

□ Permissions are inherited from parent folder

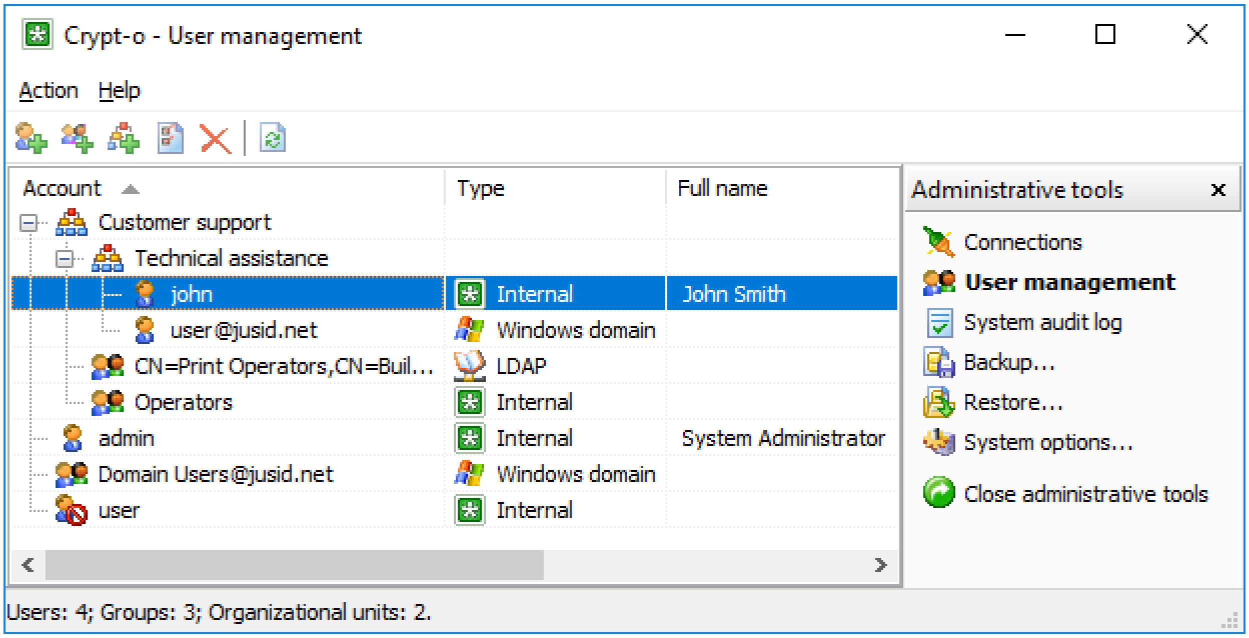
☑ Use advanced permission model

□ Reset permissions of child objects

Group accounts

There are also improvements to group accounts.

- New account type **Organizational unit** can be used to arrange user accounts as a tree.
- Group accounts can be added to other groups as members.

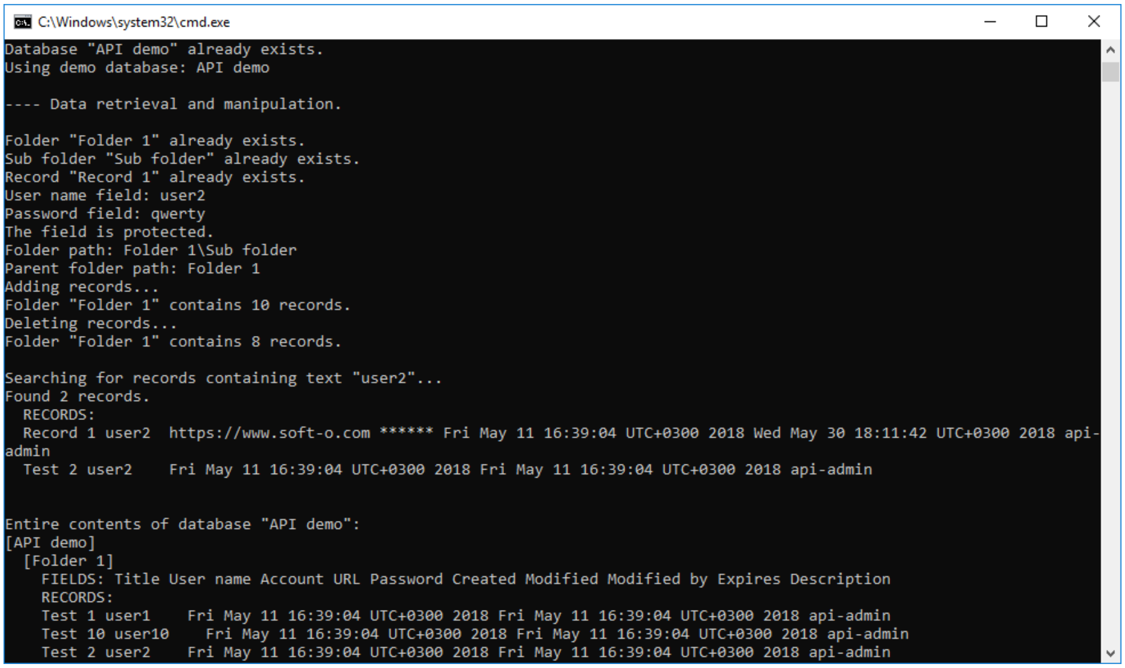


Account	Type	Full name
Customer support		
Technical assistance		
john	Internal	John Smith
user@jusid.net	Windows domain	
CN=Print Operators,CN=Buil...	LDAP	
Operators	Internal	
admin	Internal	System Administrator
Domain Users@jusid.net	Windows domain	
user	Internal	

Users: 4; Groups: 3; Organizational units: 2.

Crypt-o API

It is possible to use Crypt-o COM API to access and manipulate Crypt-o data via scripting.
Crypt-o COM API is language independent. Use your preferred scripting language and engine (**JavaScript**, **PowerShell**, **VBScript**, etc) to access the API.



```
Database "API demo" already exists.
Using demo database: API demo

---- Data retrieval and manipulation.

Folder "Folder 1" already exists.
Sub folder "Sub folder" already exists.
Record "Record 1" already exists.
User name field: user2
Password field: qwerty
The field is protected.
Folder path: Folder 1\Sub folder
Parent folder path: Folder 1
Adding records...
Folder "Folder 1" contains 10 records.
Deleting records...
Folder "Folder 1" contains 8 records.

Searching for records containing text "user2"...
Found 2 records.
  RECORDS:
  Record 1 user2  https://www.soft-o.com ****** Fri May 11 16:39:04 UTC+0300 2018 Wed May 30 18:11:42 UTC+0300 2018 api-
admin
  Test 2 user2    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin


Entire contents of database "API demo":
[API demo]
  [Folder 1]
    FIELDS: Title User name Account URL Password Created Modified Modified by Expires Description
    RECORDS:
    Test 1 user1    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
    Test 10 user10    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
    Test 2 user2    Fri May 11 16:39:04 UTC+0300 2018 Fri May 11 16:39:04 UTC+0300 2018 api-admin
```

Other improvements

- Option to search for folders.
- Option to turn off display of reminders at log on.
- PNG images can be used as custom icons.
- Changed global hot keys for form filling/saving, password generation and activation of Crypt-o. Old hot keys interfere with Windows 10 system hot keys.
- Crypt-o Server 3.0 can also accept connections from Crypt-o Clients of version 2.5.x.

Upgrade

Crypt-o 3.0 makes upgrades of an existing Crypt-o 2.5 installation easier than before. Crypt-o Server 3.0 can accept connections from Crypt-o Clients of version 2.5.x. It means you can upgrade Crypt-o Server to version 3.0 and existing Crypt-o 2.5 Clients will still work with the new Server. Then gradually upgrade all Clients to version 3.0.

See the Upgrade topic for details about upgrading.

14.2. Crypt-o 3.1

Crypt-o 3.1 is a minor release. If you have a license for Crypt-o 3.x you can upgrade to this version free of charge.

Users who already own a Crypt-o 1.x or 2.x license are eligible for upgrade to version 3.x at 50% discount. To purchase an upgrade run the client application of Crypt-o 3.1, log on, select the **Help - About...** menu and follow the upgrade link in the About window.

What's new in Crypt-o 3.1

- new: Email notifications about important events.
- new: Button to start a scheduled task right now.
- new: Information about scheduled tasks: last run time, current status.
- new: The System audit log includes messages from the log file of Crypt-o Server.
- new: Option to rebuild a database.
- new: Option to generate a password in the add user window.
- new: Email field for a user account.
- updated: Maintenance of databases is moved to a separate scheduled task.
- updated: Save column widths of the audit log list.
- updated: Vertical scroll bar in the edit record window when input fields do not fit the screen height.
- updated: Accept only TLS 1.2 connections from Crypt-o clients by Crypt-o Server.
- updated: Disabled TLS 1.0 for the Web interface.

Upgrade

Crypt-o Server 3.1 can accept connections from Crypt-o Clients of versions 2.5 - 3.1. It means you can upgrade Crypt-o Server to version 3.1 and existing Crypt-o 2.5 - 3.0 Clients will still work with the new Server. Then gradually upgrade all Clients to version 3.1.

See the Upgrade topic for details about upgrading.

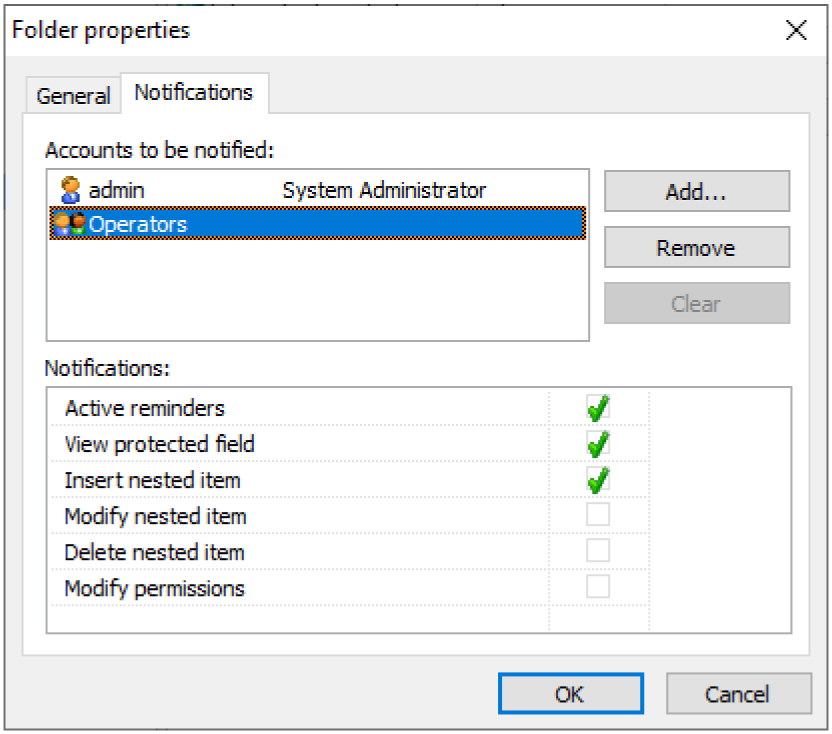
14.3. Crypt-o 3.2

Crypt-o 3.2 is a minor release. If you own licenses for Crypt-o 3.x you can upgrade to this version free of charge. Users who own Crypt-o 1.x or 2.x licenses are eligible for upgrade to version 3.x at 50% discount.

What's new in Crypt-o 3.2

Object notifications

- You can configure notifications about the following events related to records and folders: Active reminders, View protected field, Insert/Modify/Delete nested item, Modify permissions.



Accounts to be notified:

admin	System Administrator
Operators	

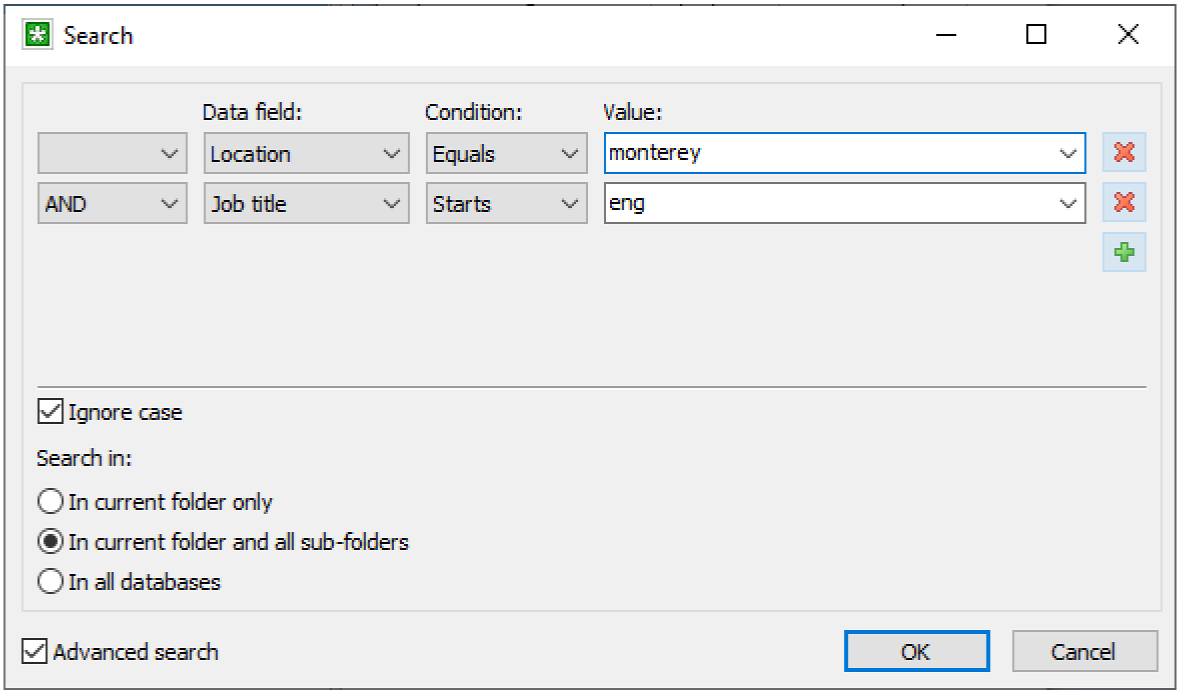
Notifications:

Active reminders	☑
View protected field	☑
Insert nested item	☑
Modify nested item	□
Delete nested item	□
Modify permissions	□

The object notifications window

Improved search

- Using Advanced search you can construct and perform complex search queries.
- In search results it is possible to edit and delete records, copy fields to the clipboard.
- Print and export of search results.
- Display a full path of a parent folder in search results.
- Clickable URLs in search results.



	Data field:	Condition:	Value:
	Location	Equals	monterey
AND	Job title	Starts	eng

☑ Ignore case

Search in:

○ In current folder only

● In current folder and all sub-folders

○ In all databases

☑ Advanced search

The Advanced search window

Other improvements

- Added support for the new Microsoft Edge browser.
- Added the Email column to the users list.
- The "Log important events to the Windows Event Log" system option. It is enabled by default.
- Additionally log the "Portable mode" event to the System audit log.
- Also cleanup the server.log file when cleanup of the System Audit log is requested.
- When the "Secure copy to the clipboard" option is not enabled, remove the copied data from the clipboard after 60 seconds.
- Improved processing speed of the `server.log` file.
- Monitor execution of background tasks on the server. A notification is sent when some task is running more than 3 hours.
- Improved database encryption to provide better security and speed.
- Reduced size of backup files and portable databases.
- Reduced database locking time during backup.
- Fixed a bug which caused the server to stop responding in some cases.
- Throw an error when a TCP port of the Server/Web interface is already in use.

Upgrade

Crypt-o Server 3.2 can accept connections from Crypt-o Clients of versions 2.5 - 3.2. It means you can upgrade Crypt-o Server to version 3.2 and existing Crypt-o 2.5 - 3.1 Clients will still work with the new Server. Then gradually upgrade all Clients to version 3.2.

See the Upgrade topic for details about upgrading.

14.4. Crypt-o 3.3

Crypt-o 3.3 is a minor release. If you own licenses for Crypt-o 3.x you can upgrade to this version free of charge. Users who own Crypt-o 1.x or 2.x licenses are eligible for upgrade to version 3.x at 50% discount.

What's new in Crypt-o 3.3

- Crypt-o can be configured to perform the automatic log on of the current Windows user in Crypt-o Client application and Web interface. See the **Allow automatic log on as current Windows user in** option on the Security page in Crypt-o system options.
- Added the new **OU user manager** system permission. A user with this permission can manage user accounts only within the user's organizational unit (OU), including nested organizational units. The OU user manager can can add, modify, delete user accounts within his OU, add OU users to OU groups. But individual permissions for OU groups can be set only by other users with higher privileges (**User management** or **System administrator**).
- Implemented the XML export and import of all data in a database. Now you can easily export a whole database to a single ZIP archive file which will contain a data XML file (records, folders, permissions, form filling information), images and file attachments. Such ZIP archive can be imported by Crypt-o in order to re-create the whole database.
- Added the **Member of** tab in the group properties window.
- Added an option to to request password change, disable, enable multiple user accounts at once.
- Added an option to extract all file attachments contained in a folder and its child folders.
- Added an option to view, block, unblock IP addresses in the Connections window.
- Display of progress information when a database integrity check or rebuilding is performed.
- Display of a database ID in the database properties window.
- Display of a progress bar during export.
- When exporting or printing, display a warning if some data can't be processed due to lack of permissions.
- Improved drag-n-drop of user accounts in User management.
- In the "IP address has been blocked" warning message include a user account name which has caused the blocking.
- Allow administrators to delete databases which are in the error state.
- Fixed the buttons layout of the file list in the Web interface.
- Fixed inability to turn off the "Remember the last logged-on user name" option in the Web interface.
- Fixed the default LDAP port.
- Fixed display of the wait mouse cursor.
- Fixed the default OU when adding a user account.
- Fixed resizing of the record properties window.
- Fixed the upgrade of database structure in some cases.

Important changes

Starting from Crypt-o 3.3.386, legacy TLS protocols (v1 and v1.1) are disabled by default for Crypt-o Web interface.

Upgrade

Crypt-o Server 3.3 can accept connections from Crypt-o Clients of versions 2.5 - 3.3. It means you can upgrade Crypt-o Server to version 3.3 and existing Crypt-o 2.5 - 3.2 Clients will still work with the new Server. Then gradually upgrade all Clients to version 3.3.

See the Upgrade topic for details about upgrading.

14.5. Crypt-o 3.4

Crypt-o 3.4 is a minor release. If you own licenses for Crypt-o 3.x you can upgrade to this version free of charge. Users who own Crypt-o 1.x or 2.x licenses are eligible for upgrade to version 3.x at 50% discount.

What's new in Crypt-o 3.4

- You can set an expiration date for passwords of user accounts.
- Added an option to prevent usage of previous password for user accounts.
- Added the Favorites menu in the Crypt-o client.
- You can create shortcut records which point to other records or folders.
- Added the Back and Forward navigation buttons.
- Added a new field option **OTP generator**, which allows you to store and use TOTP code generators for use in external services.
- You can copy to the clipboard a record with file attachments in Crypt-o and paste files in an external application.

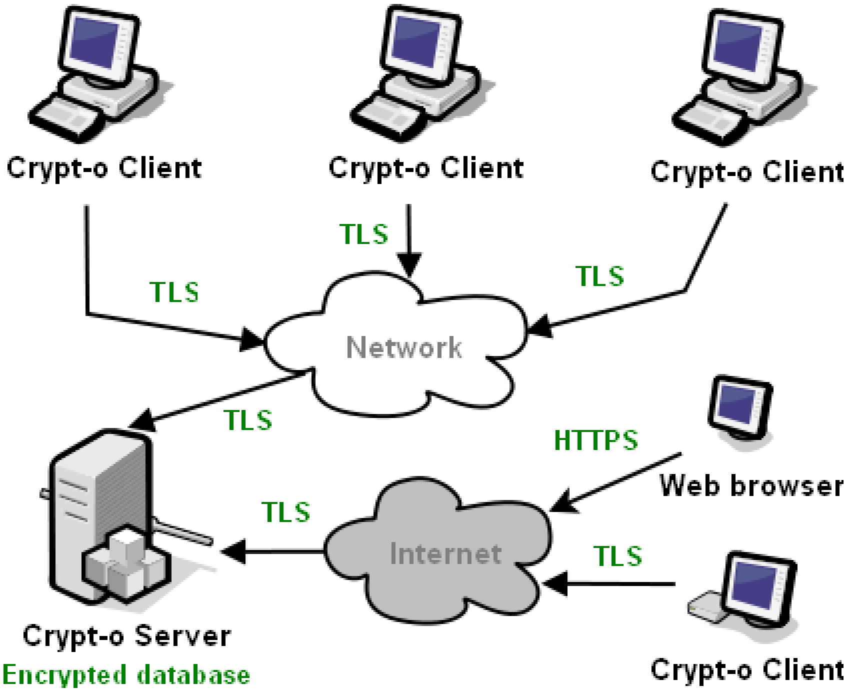
Upgrade

Crypt-o Server 3.4 can accept connections from Crypt-o Clients of versions 2.5 - 3.4. It means you can upgrade Crypt-o Server to version 3.4 and existing Crypt-o 2.5 - 3.3 Clients will still work with the new Server. Then gradually upgrade all Clients to version 3.4.

See the Upgrade topic for details about upgrading.

15. Crypt-o architecture

Crypt-o is a Client/Server application. The Crypt-o Server component accepts and serves secure TLS connections from Crypt-o Client applications. To verify the server identity the Crypt-o Client checks a fingerprint of the server's TLS certificate during connection. Such technique protects against man-in-the-middle hacker attacks.
Once a client connection has been established, the Crypt-o Client asks for a user name and password to log on to the server. Crypt-o Server supports both built-in user accounts and Windows domain user accounts for authentication.
After logon of a user, the Crypt-o Client allows the user to work with data stored on the server. User permissions are validated by Crypt-o Server during every client request. Thus, even a hacked version of the client will not be able to bypass permissions checks.



Crypt-o architecture

Crypt-o Server uses Firebird SQL Server Embedded to store all data. Firebird databases are encrypted using AES encryption algorithm with 256-bit key. During logon, a password of each user account is transformed using SHA-256 hash algorithm, applied several thousand times. After that the resulting hash is used to decrypt a key, used for decryption of the master database. Such approach guarantees data protection even if someone will get the physical database files from the server computer.

16. Localization

Crypt-o is available in the following languages:

- English;
- Danish;
- Dutch;
- French;
- German;
- Greek;
- Italian;
- Latvian;
- Norwegian;
- Russian;
- Serbian;
- Slovenian;
- Spanish;
- Ukrainian.

NOTE: You can translate Crypt-o user interface to a language, not listed here, in exchange for **10 licenses of Crypt-o**. Please send a message to support@soft-o.com, if you wish to make a translation.

17. FAQ

Q1: Why should I use Crypt-o?

A1: Crypt-o provides a centralized customizable database for securely storing any kind of information like employees or customers lists, logins, passwords, PIN codes, credit card numbers, access codes, files, etc. Allowed users can access the Crypt-o database from any networked computer.

Q2: When I open a web page in a browser, Crypt-o fills it automatically, but only the Password field is filled. How do I "teach" Crypt-o to fill out User Name field also?

A2: You need to edit field bindings for the record linked to this form. To do that, press and hold down the Shift key and then select the "Fill Form" item on your browser's popup menu or on the program's tray icon menu. Then select the "Review field bindings" option for the record and choose which form fields correspond with the record fields. Press "Done" to save new field bindings.

Q3: I have 2 accounts for a web site. But Crypt-o always fills login information automatically with the first account's credentials. Can Crypt-o ask me, data from which account should it use for filling the form?

A3: To fill a form with data from another record, press and hold down the Shift key and then select the "Fill Form" item on your browser's popup menu or on the program's tray icon menu. You will be able to choose the other record for your web site. From now on, you will be asked, which record is to be used for fill out the web site.

Q4: Is it possible to completely hide some folders for a user, while leave them visible to other users?

A4: Yes. To hide a folder for the user **John Smith**, open the Permissions window for the folder. Then delete **John Smith** from the list in the Permissions window. Click OK to apply the permissions. Now **John Smith** will not see the folder.

Q5: In what browsers Crypt-o can automatically fill-out forms?

A5: Google Chrome 49+, Microsoft Edge 79+, Mozilla Firefox 52+, Microsoft Internet Explorer 11.

Q6: Can you provide any information on migrating an existing Crypt-o database to a new server?

A6: Yes, see the Moving Crypt-o Server topic in the manual.