



# Netwrix Password Secure – Manual – Mobile App

1.19 — Last update: Oct 13, 2022

MATESO GmbH

# Table of Contents

- Welcome..... 1
- Security..... 2
- Establishment..... 3
  - Installing the App ..... 4
  - Linking the database ..... 5
  - Biometric login ..... 6
  - Automatic entry ..... 7
- Tabs ..... 8
- Synchronization ..... 9
- Passwords ..... 10
- Automatic registration iOS ..... 12
- Automatic registration Android ..... 14
- Settings..... 16

# Welcome...

---

... to the official help for the **Netwrix Password Secure App**. With the new apps you have the perfect complement to **Netwrix Password Secure App** Version 8, whether you are already a **Netwrix Password Secure** customer or have no previous knowledge:

This help guides you safely through the operation.

## Screenshot

## The Netwrix Password Secure App – Secure passwords. Mobile and simple!

You can expect a highly professional and intuitive app, for **iOS**

All functions of the **Netwrix Password Secure Apps** are integrated into a **convenient interface**. This allows users to find their way around quickly and easily.

**Instant access:** After a quick synchronisation, your personal passwords are available directly in the **Netwrix Password Secure App**.

Thanks to its simple and intuitive operation, you do not need any training or configuration for the **Netwrix Password Secure App** and can start right away!

## Security on mobile devices

Whether you work with a smartphone or tablet, you will benefit from the highest possible security on all **iOS** devices. All your passwords are not only available on your mobile device but can also be automatically transferred to websites. So you can use highly complex and therefore secure passwords and don't have to remember them anymore. **Netwrix Password Secure Apps** thus combine **security and convenience**.

## All data always available!

The automated synchronization in the background ensures that you always have the latest data on your mobile devices. The use of a local database ensures that you can access your passwords even if you are not connected to the network.



Do you have any questions, requests or suggestions about the **Netwrix Password Secure Apps** or this help?  
Then [write us](#) simply!

We are pleased that you trust **Netwrix Password Secure** to protect your company. And we hope you enjoy discovering the **Netwrix Password Secure Apps**!

Your **Netwrix Password Secure Team**

# Security

---

## Your safety is our effort

Security is a top priority at **Netwrix Password Secure** – from the very conception stage it sets the course for all further developments. Of course, attention was also paid to security in the development of the **Netwrix Password Secure Apps** and the latest technologies have been used. The following encryption techniques and algorithms are currently in use:

### Global

- AES 256 / RSA 4096 encrypted
- PBKDF2 with up to 100,000 iterations
- End to end encrypted (like all **Netwrix Password Secure** clients)
- No direct connection to the **Netwrix Password Secure** server necessary. Connection via web server.
- MDM (Mobile Device Management) support
- Passwords can also be used offline if access to the server is not possible
- Fast incremental data synchronization
- Simple connection between the **Netwrix Password Secure Apps** and the server via QR Code
- Easy navigation between private and shared passwords
- Automatic comparison of the data by means of real-time updating
- Two-factor authentication
- Comparison with several databases possible
- Expiry date of the databases to ensure automatic deletion
- Server and app side security settings. Who may use the app and to what extent?

### iOS

- Full support of FaceID and TouchID for passwordless login to the **Netwrix Password Secure App**
- Support of Password AutoFill. Passwords are automatically filled in other apps and Safari. (No copy/paste or typing)

# Establishment

---

## Requirements

The Password Safe Mobile apps synchronize automatically with an existing **Netwrix Password Secure** database. The interface used for this is the **WebClients**. This must therefore be installed. The database must also be released for use with mobile devices on the **AdminClient**.

## Setup and configuration

The setup and initial configuration of the **Netwrix Password Secure Apps** is explained in the following chapters:

- Installing the App
- Linking the database
- Biometric login
- Automatic entry

# Installing the App

---

The **Netwrix Password Secure App** is installed as usual via the **Apple Store** or **Google Playstore**. The apps can be found under the following links:



## Requirements

**iOS:** at least version 10.14

**Android:** at least version 8.0

**WebClient:** Since the app connects via the WebClient, it must be [installed](#)

**Port:** The connection is made via https port 443, which must be enabled on the server side

**User rights:** The users need the right [Can synchronize with mobile devices](#)

# Linking the database

---

First, an existing database must be connected to the **Netwrix Password Secure App** in order to finally synchronize the data. During the connection an **encrypted** database is created on the mobile device which makes the data available even without a network connection.

There are two ways to create a link.

## Manual linking

If the database is to be connected manually, the dialog for creating the link is first called up in the upper right-hand corner using the +. The address of the **WebClient** is then entered here and confirmed by clicking on **Connect**.

### Screenshot

In the next step, all databases that are available are displayed. With one click the desired one is selected.

### Screenshot

Finally, the login with username and password takes place. In addition, a meaningful name can be assigned.

### Screenshot

## Linking via QR-Code

The fastest way to create the link is to use a QR-Code. To do this, you first log on to the client. In the backstage under **account** you will find the corresponding QR Code:

### Screenshot

Then click on the button for the QR-Code in the app. In the following dialog only the QR-Code is photographed from the monitor. In the background, the mobile database is now created directly and linked to the database on the server. In the next step you can give the database profile a meaningful name and log in directly:

### Screenshot

# Biometric login

---

Depending on the operating system used (iOS or Android), the logon to the app can also be carried out via biometric factors such as fingerprint or face recognition. Directly at the first login the app suggests (depending on the type of smartphone) the use of Touch ID or fingerprint or Face ID or facial recognition. Here, a click on **Yes** is sufficient to log on to the database using the respective biometric feature in the future.

## Screenshot



# Automatic entry

The most important convenience feature of **Netwrix Password Secure Apps** is probably the automatic entry, i.e. the possibility of having access data entered directly into the input mask. The automatic entry must first be set up or configured.

## Setting up automatic registration under iOS

In the **Settings**, first select the item **Passwords & Accounts** and then select **Auto Fill**. As soon as **Autofill** is activated, all possibilities for filling in login windows are offered. Here you then select **Netwrix Password Secure**.

### Screenshot



We recommend to deactivate the **Keyring (iOS)** and possibly other offered apps to avoid misunderstandings in usage.

## Setting up automatic registration under Android

In the **Settings** the item **AutoFill service** <sup>1</sup> is called up. Here, **Netwrix Password Secure** is then simply selected by clicking on it.

### Screenshot

Finally, in the **Settings** the **Operational aids** <sup>1</sup> are selected. Here the **Netwrix Password Secure** is then activated among the **downloaded services**.

### Screenshot



We recommend to use **Netwrix Password Secure** only for the automatic registration and to deactivate all other apps here. This prevents possible misunderstandings in the operation.

<sup>1</sup> Depending on the smartphone or tablet used, the function may have a different name.

# Tabs

---

## Structure of the tab

Once you have successfully logged in, you will find yourself in the view that contains all the user's passwords.

### Screenshot

The following possibilities are offered here:

#### Action menu

With a click on **Screenshot** the action menu is opened.

### Screenshot

The following actions are offered:

- **Open settings** (further information can be found in the chapter "Settings": [Link](#))
- **Close tab** (the option is only offered if you are in an organizational units tab. The default ones are excluded)
- **Log out** (you are logged out of the database)
- **Cancel** (closes the action menu and you are back in the tab view)

## Tabs

Below the passwords there is a bar to manage tabs.

### Screenshot

By clicking on the plus sign it is possible to add more tabs.

### Screenshot

These tabs are organizational units which the user can see. The tabs **"All passwords "** and **"Personal "** are stored by default.

# Synchronization

---

Extremely important is the matching of data between mobile database and server database. Generally speaking, there is no need to worry about synchronization, because the data is automatically synchronized in the background.

## Synchronization logic

First of all, it is important to note that the synchronization is configured in the [Settings](#). A prerequisite for successful synchronization is that the configured connection is available. This is done via the https port 443, which must be opened on the server side. If the prerequisites are met, the following triggers for synchronization will occur:

- A registration at the app takes place
- Wiping down in the app
- The synchronization is started in the app's settings
- a record is changed in one of the two databases

## Which data status is synchronized?

In **Netwrix Password Secure** every field in a record has a time stamp. During synchronization, these time stamps are checked, and the newer field is written to the other database.

### Example:

Assuming that the field "Username" is changed in the FullClient and the field "Password" in the app, you have different data states on both devices. After a synchronization you will get the changed username and the new password on both devices.

## Settings for synchronization

The configuration is described in the chapter **Settings**

# Passwords

---

In principle, there are two types of passwords. **Global** and **personal passwords**.

## Global passwords

Global passwords are passwords that are assigned to an organizational unit. These passwords are usually used by more than one user.

### Screenshot

### Requirements

Before new global passwords can be created, the following requirements must be met:

- User right **can create new passwords**
- **Add right** to the corresponding organizational unit

## Personal passwords

Personal passwords are passwords to which only the creating user is authorized.

### Screenshot

### Requirement

The following user rights are required to create personal passwords:

- **Can create new passwords**
- **Can create personal records**

## Creating passwords

When creating a new data set, it is important to be clear whether this is a personal or a global password, because according to this criterion you select the corresponding tab and click on the **+**, which is located in the upper right corner.

### Screenshot

Then select the required **form**.

### Screenshot

As soon as you have filled in all relevant information of the selected form, a click on **Save** is sufficient to create the password.

## Screenshot

# Editing passwords

To edit a password, click on the corresponding password and select the pen icon.

## Screenshot

As soon as you click the pencil icon again in the new window, in the so-called readonly view, there is the possibility to edit all existing fields.

## Screenshot

## Screenshot

# Delete

Passwords can currently only be deleted via the Full or WebClient.

# Tags

Tags can be added or removed both when creating a new password and when editing a password.

## Screenshot

It is also possible to create a completely new tag.

This is possible by searching for a tag that does not already exist in the **tag selection** in the search field.

You are then offered the option of creating this non-existent tag.

## Screenshot

# Automatic registration iOS

---

The most important convenience feature of the **Netwrix Password Secure App** is probably the automatic entry. This function transfers the access data from the **Netwrix Password Secure App** to the corresponding login masks. Automatic entry works both on websites which are called up via the browser and in other apps.

## Requirements

In order to ensure automatic registration, a few conditions must be met. First, the **automatic entry** must be set up in the **settings**. If the iOS keychain is not needed, it should be deactivated. This will make handling a little easier. Finally, of course, a database connection must exist and access to passwords must be possible.

## Entry

The **automatic entry** always occurs when a login mask is found. No matter if it is located in an app or on a website. With some login masks the process of **automatic entry** starts automatically. With other masks you have to type once into the first field. The **automatic entry** itself can be divided into three different scenarios.

### Dialog

Depending on the configuration and scenario, the dialog for entry can have different characteristics:

#### Screenshot

- First, one or more passwords are displayed which match the current page or app. These can be selected and entered with one click.
- It is also possible to open the dialog to select a password. If no password is found, this dialog will be displayed directly.
- Finally, the iOS keychain can be opened. If this function is not needed, it can be **deactivated**. The corresponding option is then no longer offered.

### No password found

If no password is found that matches the app or the website you are visiting, the desired password must first be selected.

#### Screenshot

### Only one password found

If there is a data record which contains exactly the URL which is called, the corresponding password can be suggested. A simple click on the password is then sufficient to forward the data to the website or app.

#### Screenshot

## Several passwords found

If several suitable passwords are found in the database, the desired one must be selected.

### Screenshot



Depending on the current status, it may be necessary to authenticate with the app before selecting or confirming the password to be entered. The database must then be unlocked using the password, the Touch ID or the Face ID.

# Automatic registration Android

---

During automatic entry, the access data is transferred from the **Netwrix Password Secure App** directly to the login screens. This works both for web pages in the browser and for other apps.

## Requirements

For automatic entry, the service must be activated in the **Operational aids<sup>1</sup>** and **Show via other apps<sup>1</sup>**. Password Safe must be activated.

## Entry

The login data is entered as soon as the app finds a corresponding mask on a website or in an app. With some masks the process starts automatically, with others you have to type in the first field.

**There are two possible scenarios.**

- The **Netwrix Password Secure App** displays all the matching passwords. The user selects the desired password and the app enters it.
- Selection of a password in the Password Safe app. This dialog opens automatically if no password is found.

### Screenshot

#### No password found

If no password is found that matches the app or the website you are visiting, the desired password must first be selected.

### Screenshot

#### Only one password found

If there is a data record which contains exactly the URL which is called, the corresponding password can be suggested. A simple click on the password is then sufficient to forward the data to the website or app.

### Screenshot

#### Multiple passwords found

If several suitable passwords are found in the database, the desired one must be selected.

### Screenshot



Depending on the current status, it may be necessary to authenticate with the app before selecting or confirming the password that has to be entered. The database must then be unlocked using the password or the Touch ID.



<sup>1</sup> Depending on the smartphone or tablet used, the function may have a different name.

# Settings

---

As soon as you are logged in to the **Netwrix Password Secure App**, you can call up the **Settings** using the three dots at the top left of the screen. These will be explained briefly here.

## Screenshot

## General

### Hide personal tab

In some use cases, personal passwords are not required on the mobile device. If this is the case, you can hide the tab with the personal passwords.

### Show all passwords in search tab

If this option is deactivated, a search always refers only to the currently open tab. This can be useful if there are several data records in the database which have the same name and can only be distinguished by their affiliation to an organizational unit.

## Security

### Touch ID / Face ID

Here the login via Face ID or Touch ID can be activated and deactivated.

### Automatic Logout

The automatic logout from the app can be activated and configured here.

## Synchronization

### Automatic Synchronization

Here you configure how to synchronize with the main database. The following options are available:

- **Any type of connection:** If a connection exists, synchronization is performed. No matter whether it is a WLAN connection or a connection via the mobile phone network.
- **WLAN connection only:** Synchronization only takes place if a connection via WLAN exists
- **Deactivated:** It is not synchronized



Costs may be incurred for synchronization via the mobile phone network!

### Synchronize now

Starts the synchronization. This can be started at any time, even outside the settings, by simply wiping

down. Further information can also be found in the chapter **Synchronisation**.

### **Correct Sync error**

This menu item first checks for errors that have occurred during synchronization. If there are such errors, you get the possibility to repair them or to overwrite them with the current state of the server database.

## **Logging**

### **Logging**

Logging can be activated or deactivated here.

### **Display log file**

If logging is active, the log file can be displayed here.

### **Delete log file**

Logs that are no longer required can be deleted here.