Table of Contents

Welcome…

… to the official help section of **Password Safe by MATESO**. The following compendium aims to support our existing customers, as well as all interested parties in getting started with the **version 8** of Password Safe. As usual, our existing customers benefit from active software support and free access to the upgrade for the new version 8. If you require further information, don’t hesitate to contact us via the usual channels.

[redacted]

PASSWORD SAFE

[redacted]

If you are still unsure as to which plan best suits your requirements, please use our Description of the editions.

> One important reason why our products never stop evolving is the constant feedback we receive from our customers – with their wishes and suggestions motivating us daily to constantly improve our products to meet our customers’ needs. It is only with your direct feedback that we can also continue to update these help pages to meet your requirements.

We are very pleased that you have decided to use Password Safe version 8, and we hope for a mutually beneficial collaboration. Have fun browsing!

The Password Safe Team

- Why Password Safe?
- “What is new in version 8?”:#was-gibt-es-neues-in-der-version-8
- Achieving your goal with the right edition

Why Password Safe?

Users depend on passwords …

… now more than ever. They are indispensable in the day-to-day business worldwide. They are used constantly and everywhere, and they need to be professionally managed. They should be safe, and should have at least 12 characters, including uppercase and lowercase as well as special characters. In the best case, a separate access password should be used for each account. It should be changed regularly at short intervals. It is hard enough to meet this challenge in private settings. In a large corporate environment, you wouldn’t be able to adequately manage this task without the use of a professional password management tool.

User-defined scalability…

… of the Password Safe makes it suitable for use in SMEs, large companies, and global corporations. The flexibility required for this task was a driving factor behind our decision to provide a new software version, which would meet the ever-changing requirements of modern and safety-conscious companies, instead of developing the previous version. In Version 8, Password Safe is the perfect software solution for companies that wish to effectively manage security-relevant data such as passwords, documents, or certificates at the highest encryption level. In the meantime, over 10,000 business customers rely on MATESO, the market leader for professional password management in Germany, Austria, and Switzerland.

gotcha
Kirsche42
440044
Jupiter
sunrise
Blumi68
Internet_21
SALSA_LALA
abracadabra
bigfoot
apollo_13
FRITZI
MYNETWORK
HAPPY-POTTER
footrott
alpha_omega
Enter Password
schatzi
Stern94
skimaus78
yello
megan_6
4444
Steffile
Wolf13
Bärchen_53
Oma_1908
Lilli_1
admin_13
ANGELINA
DR.HOUSE_1
hobbit99
03_06_70
vertraulich
vertraulich

What is new in version 8?

Version history

The latest patch notes are always available via the following link:#changelogs.

One important reason why our products never stop evolving …

… is the constant feedback we receive from our customers. On the one hand, their compliments validate our approach; on the other, their wishes and suggestions motivate us daily to further develop our products. We would like to thank you for your feedback, and to provide you with the following features in Password Safe Version 8:

- Completely revised, intuitive operating concept
- Freely configurable dashboards for daily overview
- Newly developed SSO engine for logging on to applications and websites
- New modern add-ons for browsers
- Native RDP and SSH integration
- Advanced tag system for the optimal classification of your data
- Customizable search filters including full-text search
- Significant performance improvement thanks to the newly developed stateless multi-tier architecture
- End-to-end encryption (E2EE)
- Administration of privileged accounts including password reset and password discovery
- Maximum encryption via synchronous and asynchronous procedures
- Two-factor authentication
- Rights down to the record level, including temporary releases
- Extensive reporting for audits
- And much more

Authorization administration as the basis

Authorization administration based on roles and organisational structures is one of the central topics in Password Safe Version 8. The aim is to have a role concept that would reproduce the hierarchies within a company properly and completely. By means of synchronization with the Active Directory, the existing structures can be imported and adapted as required. Both user information and group membership are thus imported directly from the Microsoft directory service. Optionally, end-to-end encryption (E2EE) can prevent private user keys from being transmitted to the server, which could be a weak point, at least in theory.

The sophisticated authorization concept ensures that each user group or department always has access to the passwords to which they are also entitled. The requirements of hierarchically nested user structures in large companies and corporations are taken into account. This is ensured by wizards, permission pre-sets, and intuitively designed methods of inheritance.

Privileged password management

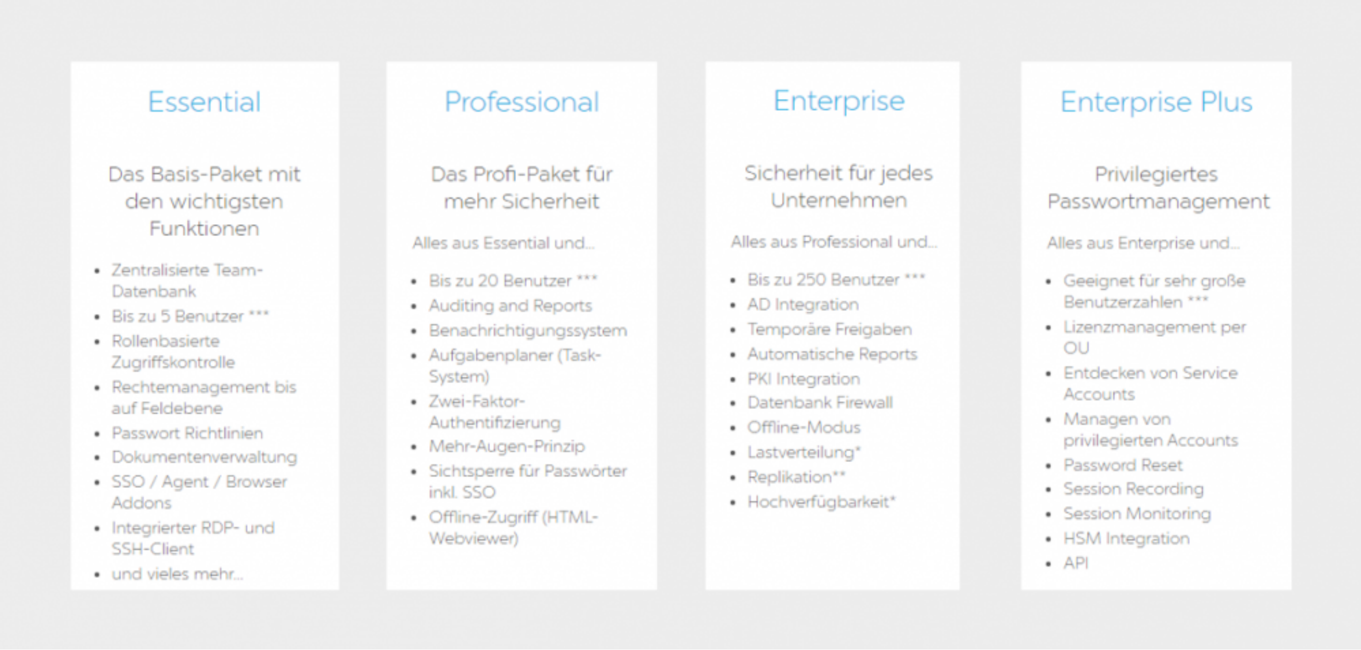
Service accounts and administrative access with far-reaching authorizations are always the key vulnerability points within companies, and have often been a gateway for attackers and manipulations. Maintenance and administration of existing, historical accounts are difficult due to their number. With Password Discovery & Reset, MATESO now provides two tools to protect these usual attack targets. Password Discovery creates a list of accounts, which are registered directly within Password Safe, by scanning the existing network structures. These accesses can then be automatically reset by means of password reset for service accounts, Active Directory access points, or Windows and MSSQL users at freely definable time periods.

SSO, logging and reporting

Single Sign On (SSO) is an integral part of corporate software configurations. With the help of the newly designed SSO agent, automatic login to websites is intuitive and easy to perform. Connections via RDP or SSH can also be automated without any problems. A special feature of Password Safe is that passwords for these access points can always be hidden from users by means of password masking. Security-critical applications, in particular, can be additionally secured by the double-check principle of the sealing system. Obviously, traceability of changes through logs and history is always possible. Documents can also be maintained in the database and archived by the integrated version management for logging and eventual restoration. Password Safe v8 also provides a granularly definable tool for security audits with the fully automated reporting system.

Achieving your goal with the right edition

Available plans



Essential

Das Basis-Paket mit den wichtigsten Funktionen

- Zentralisierte Team-Datenbank
- Bis zu 5 Benutzer ***
- Rollenbasierte Zugriffskontrolle
- Rechtemanagement bis auf Feldebene
- Passwort Richtlinien
- Dokumentenverwaltung
- SSO / Agent / Browser Addons
- Integrierter RDP- und SSH-Client
- und vieles mehr...

Professional

Das Profi-Paket für mehr Sicherheit

Alles aus Essential und...

- Bis zu 20 Benutzer ***
- Auditing and Reports
- Benachrichtigungssystem
- Aufgabenplaner (Task-System)
- Zwei-Faktor-Authentifizierung
- Mehr-Augen-Prinzip
- Sichtsperre für Passwörter inkl. SSO
- Offline-Zugriff (HTML-Webviewer)

Enterprise

Sicherheit für jedes Unternehmen

Alles aus Professional und...

- Bis zu 250 Benutzer ***
- AD Integration
- Temporäre Freigaben
- Automatische Reports
- PKI Integration
- Datenbank Firewall
- Offline-Modus
- Lastverteilung*
- Replikation**
- Hochverfügbarkeit*

Enterprise Plus

Privilegiertes Passwortmanagement

Alles aus Enterprise und...

- Geeignet für sehr große Benutzerzahlen ***
- Lizenzmanagement per OU
- Entdecken von Service Accounts
- Managen von privilegierten Accounts
- Password Reset
- Session Recording
- Session Monitoring
- HSM Integration
- API

Essential

The Essential Edition will give you an introduction to the world of professional password management. Please note that the purchase of this edition always includes precisely 5 users. The Essential Edition can only be purchased from the webshop:https://www.cleverbridge.com/611/uurl-1jneqb8gfb.

Professional

The Professional Edition is designed for small and medium-sized teams up to 20 people. In addition to the basic functionality included in the Essential, you can view passwords, single sign on agents, and reporting and auditing.

Enterprise

The Enterprise Edition is intended for larger teams and company-wide roll-outs with a maximum of 250 users. The features of the Professional Edition are supplemented by Active Directory Integration, temporary releases as well as the possibility to include a second factor in the registration.

Enterprise Plus

The Enterprise Plus version is designed for an unlimited number of users. It includes an API, as well as Auto Discovery and Password Reset, which are the essential features for large corporations.

If you require further information about the editions and their prices or you are interested in acquiring a test licence, please contact us directly via the “official homepage”:https://www.passwordsafe.de/kaufen/.

Licence model

How does licensing work?

Licensing in Password Safe is always carried out based on the number of users. The named user model means that every user receives their own licence accordingly. The following basic conditions apply:

- The extent to which Password Safe is used is irrelevant. Every user requires their own licence.
- The use of light licences is (currently) not possible
- Even the sole use of the SSO agent requires possession of a full licence

Modules from version 7

In contrast to version 7, there are no longer any modules. Adapting the licensing per computer using modules was still possible in the previous version (No Client Licensing module). This is no longer necessary. All licensing processes are covered by the above-mentioned licensing model.

Security

IT security is changing with the times

It is a declared goal that Germany’s digital infrastructures should be among the safest in the world. The **IT Security Act**, which came into force in July 2015, is intended to form a blueprint for this purpose, and to ensure the leading position of Germany in the fight against digital threats. The Federal Office for Information Security (BSI), which is also responsible for the **ISO 27001 Certification based on the IT Baseline Protection Catalogues**, has been setting the course for this. At the European level, too, the potential danger is taken into account by the * Directive on Network and Information Security (NIS) *, the counterpart to the German IT security law. Through the EU-wide strengthening of resistance to risks from the Internet, such criminal energies should be further restricted.

Hazards and risks

This is to be assessed as a reaction to a hazard, which could not be more concrete: The Federal Office of Criminal Investigation has estimated the number of digital attacks on German companies at 300,000 a day. According to the Federal Office for the Protection of the Constitution, the federal networks are targeted over a million times a year by hackers with financial interest, by politically motivated “hacktivists” and, of course, by secret services. The BKA has been warning on the internet for years, both in the private sector and in the company environment. Acquired thieves in the form of security-critical corporate interiors are regularly subject to blackmail.

Vulnerability of passwords

Due to the rapid digital revolution, more and more focus is being placed on the topic of password security in particular. Passwords, which were still relatively safe 5 years ago, have to be put to the test again due to technical progress. Only randomly selected passwords with a corresponding number of digits can really defuse this problem. It is also important to ensure that these passwords are changed at predefined intervals.

The solutions of the MATESO Password Safe

The safest passwords are still those that can be completely hidden from the users. **Automatic entries** allow users to work efficiently without knowing their passwords. By means of the most advanced methods of the **Password Reset**, these access codes can also be reset automatically at intervals that can be as short as required. There are also safety mechanisms which link access to systems to a release by those users with the required permissions, according to the **double-check principle**. All these routines are backed up by **highly complex encryption methods**. Regular penetration tests ensure that the software is specifically tested by independent experts for weaknesses in architecture as well as the correct use of state-of-the-art cryptographic technologies. Conclusion: Human misconduct in the handling of passwords must be reduced to a minimum by technically enforced specifications and workflows. Christian Strobel, COO of MATESO GmbH:

> Whether SMEs, global corporations or government agencies: If the risk of data gaps and IT terrorism are to be minimized in the future, the discussion of the subject matter is inevitable. On the other hand, the use of a professional password management software is no alternative.

- Used encryption algorithms
- External penetration tests
- IT security made in Germany

Used encryption algorithms

Encryption algorithms

Safety has always been one of the most basic considerations when designing software. All other requirements were assessed according to how safe they were. Parallel to the development phase, the theoretical concepts of external security companies were examined in terms of feasibility, as well as compliance with IT security standards. Prototypes have been ultimately developed on the basis of these findings, which form the blueprint for the current Password Safe version 8. The following encryption techniques and algorithms are currently in use:

- AES 256
- PBKDF2 with 100,000 iterations for the formation of user hashes
- PBKDF2 with 1000 iterations for the hashes of the passwords within the database
- RSA 4096 for private and public key methods

Applied cryptographic procedures

The container encryption of the passwords is based on the aforementioned algorithms. Each container has its own randomly generated salt. Each password, user, and role has its own key pair. When releases are granted for users and roles, the passwords within the database are hierarchically encrypted. Password Safe also uses the following cryptographic methods to achieve maximum security:

- To integrate an AD, you can choose between an end-to-end encryption (E2EE – the safest mode) and the Master Key
- The server key is protected using the hardware security module (HSM) via PKCS#11
- Brute force protection for logging in by means of automatic blocking of the requesting client
- Certificate protection when using applications
- Certificate request for client/server connection You may use your own certificate authority (CA) as an option.
- Latest version of the Secure Sockets Layer (SSL)
- Passwords are only encrypted and transported to the client when they have been explicitly requested in advance. More…

! Only secrets are encrypted. Metadata is not encrypted to ensure search speed. Secrets are usually passwords. However, the customer can decide what kind of data they are. Note that Secrets cannot be searched for.

Security hardware components we have tested:

HSM:

- SafeNet Luna SA – HSM with network connection
- SafeNet Luna PCI-E – Embedded-HSM

Two-factor authentication:

- SafeNet eToken Pass
- RSA SecureID 700
- Google authenticator

External penetration tests

Penetration tests by SySS GmbH

For over 15 years, SySS GmbH has been focusing on software penetration testing (pentests), as well as maintaining the maximum security of IT infrastructures in companies of any industry and size. The security specialists from Tubingen now serve over 20 of the DAX30 corporations across the industry. State institutions (Ministry of the Interior, German Armed Forces, Deutsche Flugsicherung (German air navigation services organisation), …) also rely on the expertise of SySS GmbH. Professional cooperation with the market leader in several iterations has set the course for closing and continuously avoiding potential security loopholes.

Pentest of version 8.3.0

Due to the huge increase in the functional scope since the last pentest, version 8.3.0 was subjected to a new test. The text was passed with flying colours.

Components of the pentest

Amongst other things, the following scenarios were tested during the test:

- Simulation of client-side attacks of different types
- Intensive source code review
- Qualitative assessment of all cryptographic methods

Test conditions

SySS GmbH had full access to the source code and to the database server at all times to ensure complete and granular execution of the tests.

Summary of the test

SySS
THE PENTEST EXPERTS.

Certified Product
Approved Security
VALID – 11.2018

Sebastian Schreiber, the Managing Director of SySS GmbH, attested to the successfully conducted test. Here is an excerpt:

> During the course of the security test, it was not possible for SySS GmbH to access protected password information and documents from third party users of the Password Safe 8 software application using unauthorised measures, neither from the perspective of a user with login data nor from the perspective of an external attacker without login data. In the view of SySS GmbH, the processes used for authentication, authorisation and encryption provide effective protection for the sensitive data saved within the application.

> According to the findings from SySS GmbH, an attacker (…) is not able to directly access login passwords in plain text or unencrypted RSA key material about users.

> The fact that access to the private RSA key in plain text is only possible after prior entry of the correct password and that this authentication information is thus introduced to the Password Safe application externally by one person as part of the user login process was considered very positive by SySS GmbH. Even in the event of various different weaknesses, an attacker is not immediately able as a result to access encrypted data such as passwords or documents.

> In terms of the encryption process used in the system, SySS GmbH could not identify any weaknesses as part of the completed security test.

Overall, SySS GmbH rates the security level of the tested software version of the Password Safe 8 application as “very good”.

IT security made in Germany

The TeleTrusT initiative

MATESO GmbH, with the product “Password Safe and Repository”, is a member of the TeleTrusT Initiative “IT-Security made in Germany”. The quality label has its roots in the co-operation between the German Federal Ministry of the Interior (BMI), the German Federal Ministry for Economic Affairs and Energy (BMWi), and representatives of the German IT security industry. This co-operation has been pushed forward since 2005.

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

The quality label certifies the following characteristics of the MATESO Password Safe version 8:

- The company headquarters are in Germany
- The company offers trusted IT security solutions
- The products offered include no hidden access points
- The company’s IT security research and development takes place in Germany
- The company undertakes to meet the requirements of the German data protection law

Getting started

Getting started

We recommend that you follow these ten steps when installing Password Safe version 8. We strongly recommend that you carefully record all configuration information, such as set passwords and similar data. If you find gaps in the Help section during the installation, do not hesitate to send us a short feedback. We will be happy to add any missing information and make it available to you and other Password Safe users.

1. Microsoft SQL system requirements

We use Microsoft SQL Server as the database management system due to its high-performance data access, widespread use and extensive backup options.
Follow this link for information on MSSQL system requirements

2. Application server system requirements

Particular attention should be paid to the subsections “Required users” :#systemanforderungen-serverand Rights for PowerShell scripts.
Follow this link for information on system requirements for the application server

3. Client system requirements

The requirements for the client environment have been specified separately.
Follow this link for information on client system requirements

4. Installing AdminClient

All required parameters are defined with the help of a wizard when installing the Password Safe AdminClient.
Follow this link for information on how to install the AdminClient

5. Basic configuration of Password Safe

When the AdminClient is opened for the first time, the Password Safe basic configuration starts. This guides the user through the basic configuration with the help of a wizard.
Follow this link for information on Password Safe basic configuration

6. Authentication on the AdminClient

After completing the basic configuration, you can authenticate directly to the AdminClient.

> The default password for the AdminClient is “admin”

7. Setup wizard

The setup wizard includes allocating a new password for the Password Safe AdminClient, integrating the license, and configuring the database and SMTP settings.
Click here for the setup wizard

8. Creating databases

The MSSQL databases can, of course, also be created and managed directly via our AdminClient.
Follow this link for information on how to create databases

9. Installing the client

The client’s installation, which is also accompanied by a wizard, is the first step to allow users to work with Password Safe.

Follow this link for information on how to install the client

10. Creating database profiles

The number of databases is not licensed. In theory, any number of databases is thus possible. To keep an overview, it is recommended to create profiles that contain all the parameters required for successful logon to a database.

Follow this link for information on how to create database profiles

Architecture and system requirements

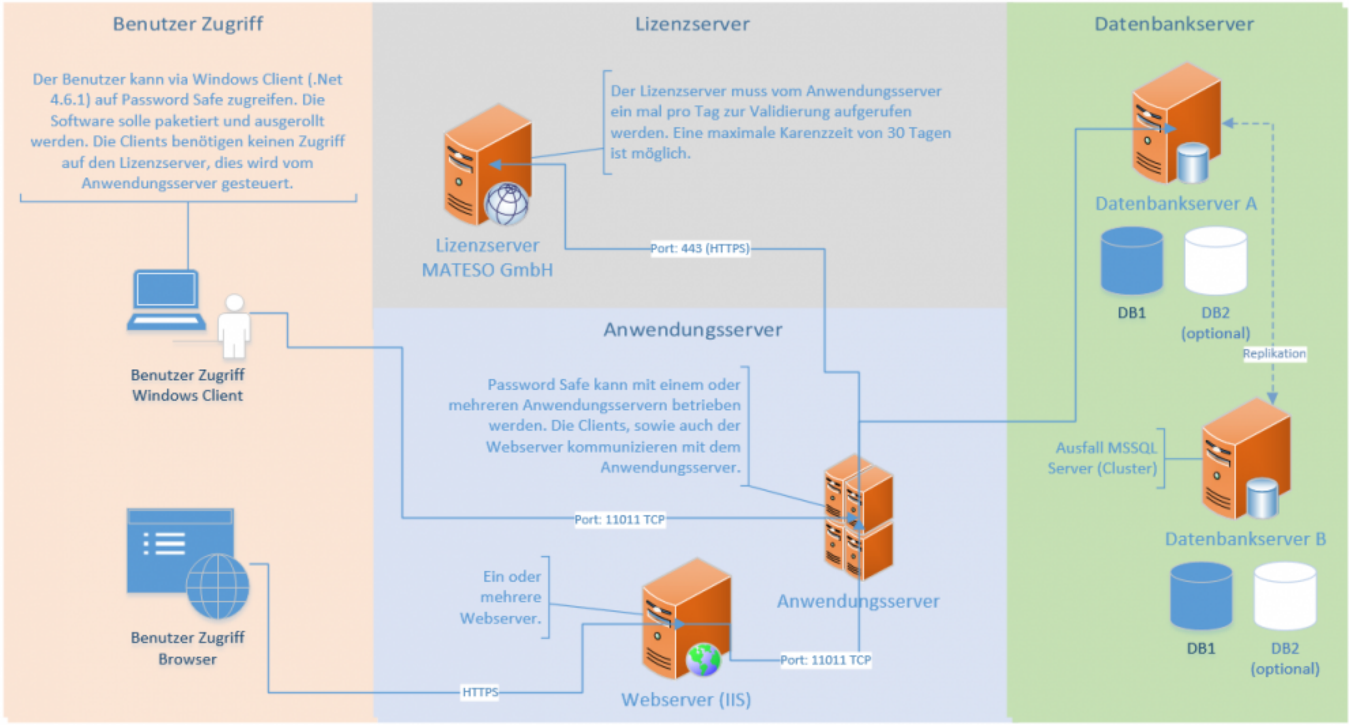
Multi-tier architecture

The structure of Password Safe v8 is based on the principle of **multi-tier architecture**. This multi-layered design of the individual software components provides the basis for a well thought-out and ground-breaking security concept. The three separately acting layers can each be scaled as needed. As a result, Password Safe v8 can also be used efficiently in companies with very large number of users and **sites around the world**. If the **“end-to-end” encryption** is used, data can be encrypted or decrypted also on the clients. This ensures that unencrypted passwords will never exist on the database server or the application server. The “private and public key method” ensures that the private key is always only available to the user. The application server only knows the value of the public key and is thus unable to see the value of the password.

Password Safe version 8 can be set up on small to global system landscapes. Any number of clients, application servers and database servers can be connected within the multi-tier architecture. The use of a fail-safe cluster is recommended for databases in a production system. Microsoft SQL Server can replicate the data to a different data centre, e.g. via WAN. We also recommend providing a separate Windows server in each case.

System landscape

The following overview presents a classic Password Safe **system landscape**. Version 8 allows use of several database servers across all sites. These are then synchronized with one another using Microsoft standard applications. Any number of application servers can be made available for the client connection. This ensures load distribution, and allows work without significant latency. This technology offers enormous performance advantages, particularly in the case of installations that are spread across worldwide locations.



Der Benutzer kann via Windows Client (.Net 4.6.1) auf Password Safe zugreifen. Die Software solle paketiert und ausgerollt werden. Die Clients benötigen keinen Zugriff auf den Lizenzserver, dies wird vom Anwendungsserver gesteuert.

Der Lizenzserver muss vom Anwendungsserver ein mal pro Tag zur Validierung aufgerufen werden. Eine maximale Karenzzeit von 30 Tagen ist möglich.

Password Safe kann mit einem oder mehreren Anwendungsservern betrieben werden. Die Clients, sowie auch der Webserver kommunizieren mit dem Anwendungsserver.

Ein oder mehrere Webserver.

Client (presentation layer)

The client layer handles the representation of all data and functions, which are provided by the application server.

Application server (business logic)

The application server is entirely responsible for the control of the business logic. This server only ever delivers the data for which the corresponding permissions are available. The multi-tier architecture described at the beginning allows the use of several application servers and ensures efficient load distribution.

Database server (data storage)

Password Safe version 8 uses Microsoft SQL Server to store data due to its widespread use, and its ability to ensure high-performance access even in large and geographically scattered environments. Smaller installations may also use the free SQL Express version.

At least three servers are thus recommended:

- Database server (MSSQL)
- Application server (Password Safe services)
- Web server (IIS)

! For databases in a production system, we recommend using a fail-safe cluster. Microsoft SQL Server can replicate the data to a different data centre, e.g via WAN. We also recommend providing a Windows server for each function. Separating the systems makes it easier to expand and scale the system landscape at a later point in time. However, it is not absolutely necessary to separate the systems. Accordingly, all of the components can also be installed on one server in the case of smaller installations.

MSSQL System Requirements

Required hardware

We recommend that you install the database on a separate MSSQL database cluster to ensure enhanced fail-safe operation. The database should also be mirrored to another data centre at a different location. We recommend the following to ensure smooth operation:

- Min. Windows Server 2012 R2
- Recommended Windows Server 2016
- At least 4 x CPU
- Min. 16 GB RAM
- Min. 100 GB hard disk space
- Installed and licensed Microsoft MSSQL Server 2012 or later (from Express)

The application server requires the following port to be enabled:

- Port 1433 TCP for communication with the application server

A comparison of the different MSSQL server editions can be found under the following link:
SQL Server Editions
The capacity limits for the specific editions are also listed here.

Required databases

At least two databases are created during installation:

1. The configuration database, which contains all settings for the application servers
2. The main database, which holds all information about users and records

Requirements

The two databases can be created and managed directly via the admin console. However, some **requirements** must be met on the MSSQL server for this purpose:

User

A specific SQL user should be used for the Password Safe V8 databases. The server admin (SA) may be used but is not absolutely necessary. The user thus requires the following rights:

- **dbCreator**: If the databases are created via the server, the user must have the **dbCreator** permission
- **dbOwner**: If the databases are created manually on the MSSQL server, and are only managed by the server, **dbOwner** rights are sufficient
- In any case, the user must have **read rights for the master database**

Databases

An MSSQL database is required for each Password Safe database. Multiple databases can be run on one SQL instance. As Password Safe V8 enables the clean separation of all data via the authorization concept, a single MSSQL database is sufficient for most applications.

> ! The databases must have the collation **Latin1_General_CI_AS**. If the SQL Server uses a different collation, Password Safe cannot create the database correctly. In this case, the database must be created manually on the server side with the correct collation, and this must then be linked to the AdminClient.

Click here to return to the “Getting started” section

Server system requirements

Required hardware and software

The business logic is managed by the application server. The load is determined by both the number of users and also the number of server requests. To ensure optimal operation, we recommend that the following hardware resources are made available:

- At least Windows Server 2012 R2 (current patch level is mandatory!)
- Recommended Windows Server 2016
- At least 4 x CPU
- Min. 8 GB RAM
- Min. 40 GB hard disk space
- Current .net library (current minimum requirement is version 4.6.2)
- Firewall release
- Windows Management Framework 4.0 must be installed! (Windows update KB2819745)

The application server requires that the following ports are enabled:

- Port 443 HTTPS to connect to the MATESO license server
- Port 11011 TCP for communication with the clients or the Web server IIS
- Port 11014 TCP for the backup service
- Port 11018 TCP (incoming) for the Realtime API
- Port 1433 TCP for communication with the SQL server

Windows Server 2012 R2 requires the latest patch level (SSL3, TLS)

If you are connected outside a local network (such as via VPN), you should ensure that the MTU is configured to 1500 bytes (1472 bytes + 28 bytes for the header). Otherwise, the packets to be transmitted are fragmented, which can lead to a significant loss of performance.

Web server (IIS)

Several web servers can be configured for web access, but at least one is required to use the web access. In the first iteration of version 8, access via WebClient is not yet equipped with all functions. We recommend the following to ensure optimal operation:

- At least Windows Server 2012 R2 (current patch level is mandatory!)
- Recommended Windows Server 2016
- At least 4 x CPU
- Min. 8 GB RAM
- Min. 40 GB hard disk space
- Current .net library (current minimum requirement is version 4.6.1)
- SSL certificate
- If necessary, configure firewall access after access (http, or https)

Required users

A user via which the Password Safe server can log in to the SQL server is required for configuration. A user who can execute the Password Safe services is also required. The various configurations are briefly explained here.

Service user

The service user runs the Password Safe server service. The following can be configured here:

- **AD user:** It is specified in the format **Domain\username** along with its associated password
- ***Local user:** It is specified in the format **.\user name** along with its associated password
- **Local system account:** It can be activated via a checkbox

> ! The service user creates the databases. Certificates are generated in the meantime. Therefore, the **service user** must be a **local administrator** or a **domain administrator**, otherwise it would have no rights to save data in the certificate store.

Backup service user

In principle, the backup service is run by the service user. In expert mode, however, it may be another user. A backup service user has the same requirements as a service user.

User for the SQL configuration instance

The user for the SQL configuration instance logs on to the SQL server to create the Password Safe databases. You can use an AD user or a local SQL user for this purpose. The following options are available:

- **Service user:** If the checkbox is activated, the stored service user is used. Please note that this can only be configured via the checkbox. It is not possible to manually set up the service user again.

- **SQL user:** An SQL user may also be used. It is saved on the SQL server according to the configuration.

> ✻ If the Password Safe server is to be used to create databases, the user needs dbCreator rights. Alternatively, the databases can be created directly by the SQL server. The Password Safe server will manage them. In this case, dbOwner rights are sufficient.

Configuration examples

Variant 1:
A service user is created in the AD. It will be added as a service user, which can start both the Password Safe server service and the backup service. This user requires rights to start services. This user is then used for the SQL configuration instance (by activating the check box).

Variant 2:
A local user is used as a service user. Specify a local SQL user, secured with a password, as a user for the SQL configuration instance. This could be the default sa user, for example.

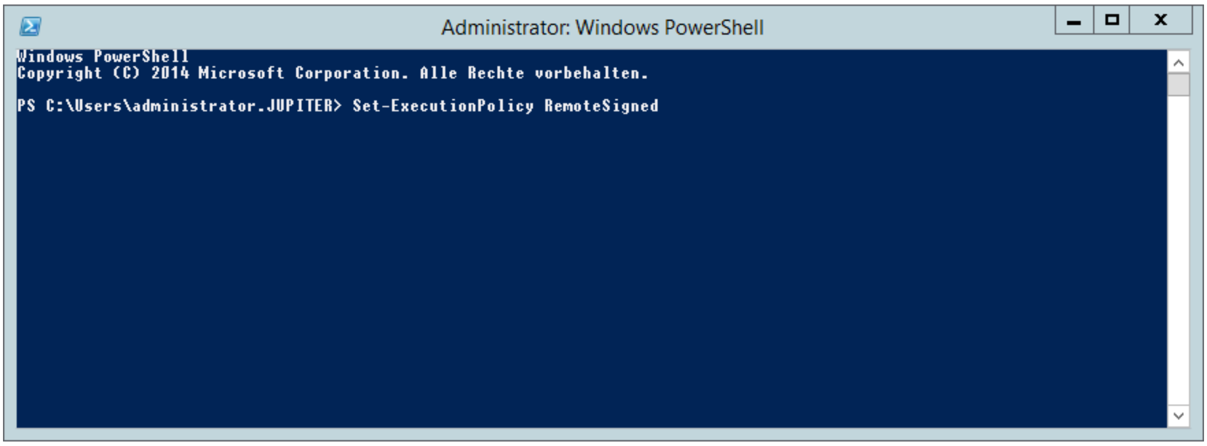
> ! It is not possible to combine local system and service users for the SQL configuration instance!

Rights for Windows PowerShell

In Password Safe V8, Windows PowerShell scripts are used in several places. These are required, for example, to use the certificate-protected server key or to create the server certificate. Password Reset also uses this functionality. It is therefore absolutely necessary that the Windows security policy allows PowerShell scripts to be executed. You can set this up and check manually as follows:

> ! Windows Management Framework 4.0 must be installed! (Windows update KB2819745)

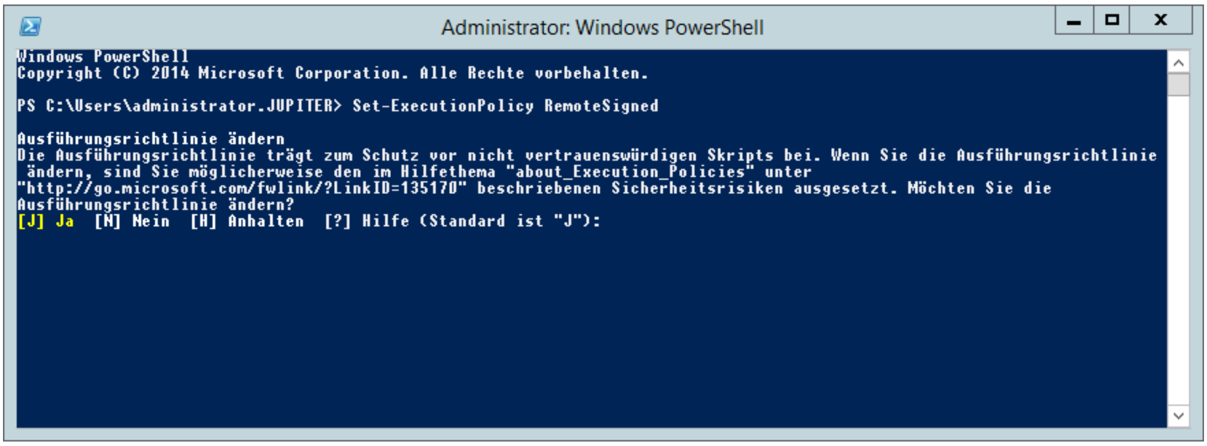
Open the PowerShell console. Enter **Set-ExecutionPolicy RemoteSigned** and confirm.



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\administrator.JUPITER> Set-ExecutionPolicy RemoteSigned
```

The change to the policy is confirmed in the next step.

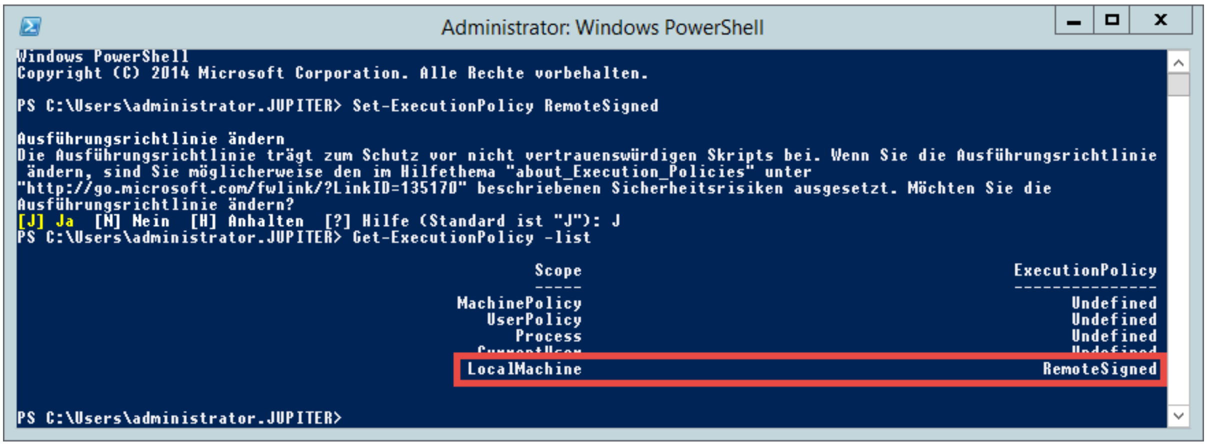


```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\administrator.JUPITER> Set-ExecutionPolicy RemoteSigned

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die Ausführungsrichtlinie
 ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"http://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die
Ausführungsrichtlinie ändern?
[J] Ja  [N] Nein  [H] Anhalten  [?] Hilfe (Standard ist "J"):
```

The changed policy can be queried via **Get-ExecutionPolicy -list**.



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\administrator.JUPITER> Set-ExecutionPolicy RemoteSigned

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die Ausführungsrichtlinie
 ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"http://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die
Ausführungsrichtlinie ändern?
[J] Ja  [N] Nein  [H] Anhalten  [?] Hilfe (Standard ist "J"): J
PS C:\Users\administrator.JUPITER> Get-ExecutionPolicy -list

                                                      Scope                                             ExecutionPolicy
                                                      -----                                             ---------------
                                              MachinePolicy                                                   Undefined
                                                 UserPolicy                                                   Undefined
                                                    Process                                                   Undefined
                                                CurrentUser                                                   Undefined
                                               LocalMachine                                                RemoteSigned


PS C:\Users\administrator.JUPITER>
```

Click here to return to the Getting Started section

Client system requirements

Required hardware

The performance is only dependent on the client to a small extent. The user's settings are imported directly from the MSSQL database. We recommend the following to ensure smooth operation:

- Microsoft Windows version 7 (latest patch level)
- At least 2 x CPU
- Min. 2 GB RAM
- Min. 40 GB hard disk space
- Current .net framework (current minimum requirement is version 4.6.2)
- If RDP connections are to be established, it is necessary to have installed RDP 8.1 at least

The clients require that the following ports are enabled:

- Port 11011 TCP for communication with the application server
- Port 52120 TCP with the addon

> ✻ We recommend packaging the client and installing it on the respective PC's. We provide an MSI installer package for that purpose.

> ✻ The clients can run on all current Windows versions, from Windows 7 to Windows 10

Use in terminal server operation

The client can also be operated on a Windows Terminal Server. For the automatic sign-on, the SSO Agent must be installed as a service on the terminal server.

Click here to return to the "Getting started" section

System requirements for the WebClient

In principle, the Password Safe WebClient can be installed on all current web servers. For this purpose, a corresponding SSL certificate is required for the https connection. The WebClient should ideally have the same version as the Password Safe server.

As every web server is individually installed and configured, detailed knowledge of the system being used is required. Our partners would be pleased to carry out the installation via consulting.

Supported web servers

The Password Safe WebClient has been successfully tested on the following systems:

IIS

- from **Version 7**
- **URL Rewrite** module
- **Application Request Routing** module

Apache

- from **Version 2.4**
- **mod_rewrite** module
- **mod_proxy** module
- **mod_ssl** module
- **mod_proxy_http** module

nginx

- From **Version 1.13**

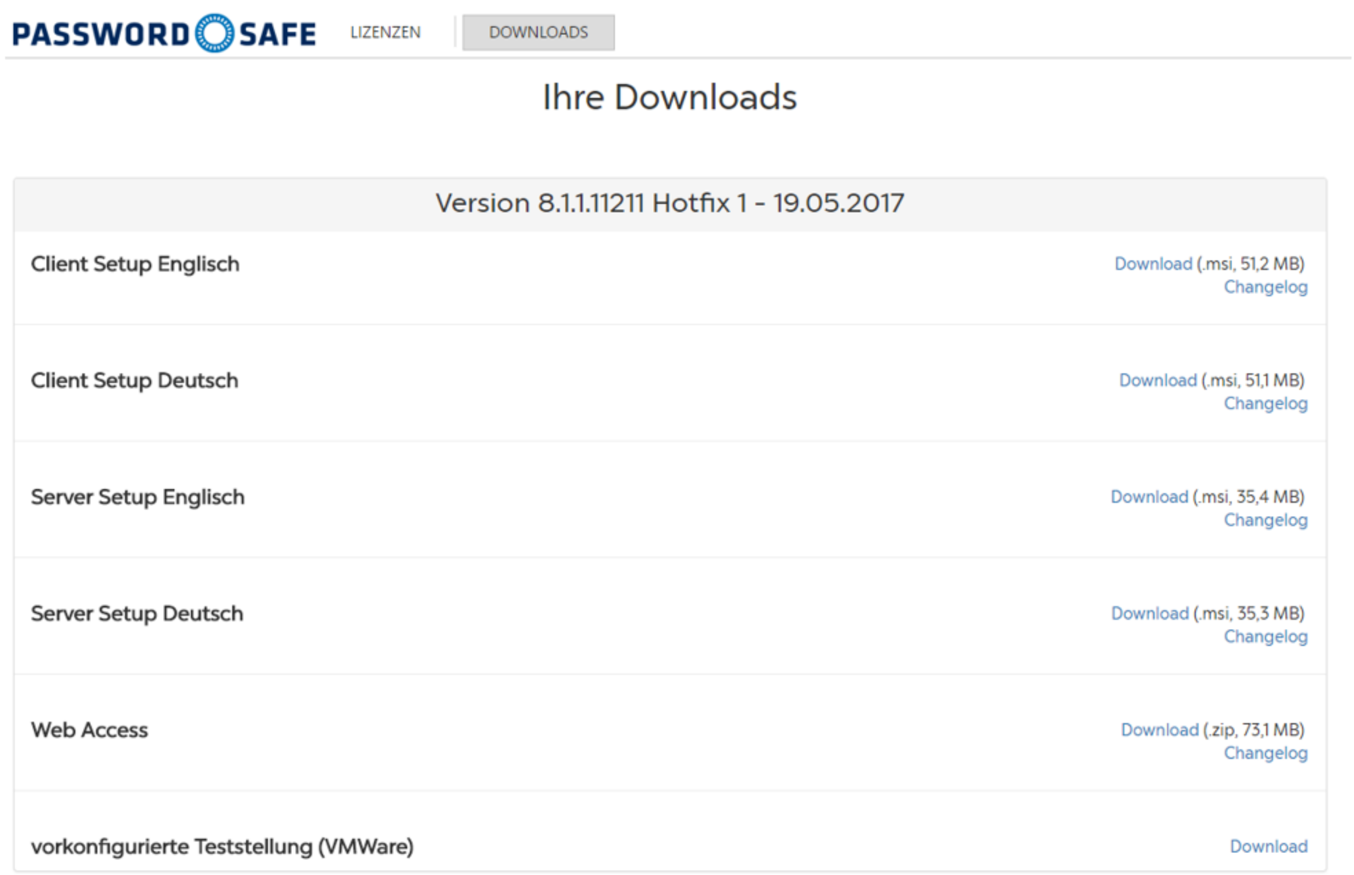
As already mentioned, the Password Safe WebClient can be operated on all standard web servers. Due to possible side effects, proper functionality cannot be guaranteed on all available web servers. In cases of doubt, the functionality of the WebClient should thus be tested in advance.

! The connection between the browser and the web server must be protected by an SSL certificate. It is strongly recommended that you purchase a certificate for this purpose from a service provider e.g.: Thawte. If you have not purchased an official certificate, please ensure that your certificate is sufficiently trusted. Otherwise, the certificate will be displayed in red and shown as insecure in the browser.

Installation

Installation files

The installation files are directly available via our portal provided for this purpose: https://license.passwordsafe.de/kis



Ihre Downloads

Version 8.1.1.11211 Hotfix 1 - 19.05.2017	
Client Setup Englisch	Download (.msi, 51,2 MB) Changelog
Client Setup Deutsch	Download (.msi, 51,1 MB) Changelog
Server Setup Englisch	Download (.msi, 35,4 MB) Changelog
Server Setup Deutsch	Download (.msi, 35,3 MB) Changelog
Web Access	Download (.zip, 73,1 MB) Changelog
vorkonfigurierte Teststellung (VMWare)	Download

You will receive the access data with the delivery of the licence. If you are interested in acquiring a test licence, please use the form designed for this purpose: https://www.passwordsafe.de/testen/testlizenz.

✻ In contrast to version 7, no certificates are delivered. Your certificate is stored on our licence server and can be called up using the access data you receive.

Conceptual design before installation

Password Safe is designed to represent the existing hierarchies in a company in the form of differentiated and precisely definable permission structures. The better you can understand these hierarchical structures, the easier it will be to implement the software. Errors in the analysis phase thus often lead to subsequent errors, which can only be corrected with a great deal of effort. It is therefore indispensable to devote the necessary attention to the conceptual design. Well-thought-out and strictly planned projects profit greatly from a thoroughly comprehended project plan, both during implementation and during ongoing operations.

Documentation parallel to the installation

! Documentation is an important part of the installation. Ensure that the systems and access points used are fully covered. When changing responsibilities or modifying the architecture, you will benefit significantly from a reference work in the form of a complete Password Safe documentation.

Definition of responsibilities

We recommend that you designate a person responsible for Password Safe, as well as a representative, and train these persons adequately. In case of larger installations, it is likely that the responsibility must be borne by several people. You must specify which persons (groups) will have access to the various functionalities within Password Safe:

- Management of organisational structures and roles
- Creation and maintenance of forms and applications
- Configuration of the settings and rights, as well as masking of modules
- Definition of authorizations and definition of rights templates
- Developing an access model:
  - To what extent and by whom are the databases supported?
  - Is a separation of administrative activities necessary?

"If necessary, our experienced support team will be glad to assist you." Mailto: support@passwordsafe.de

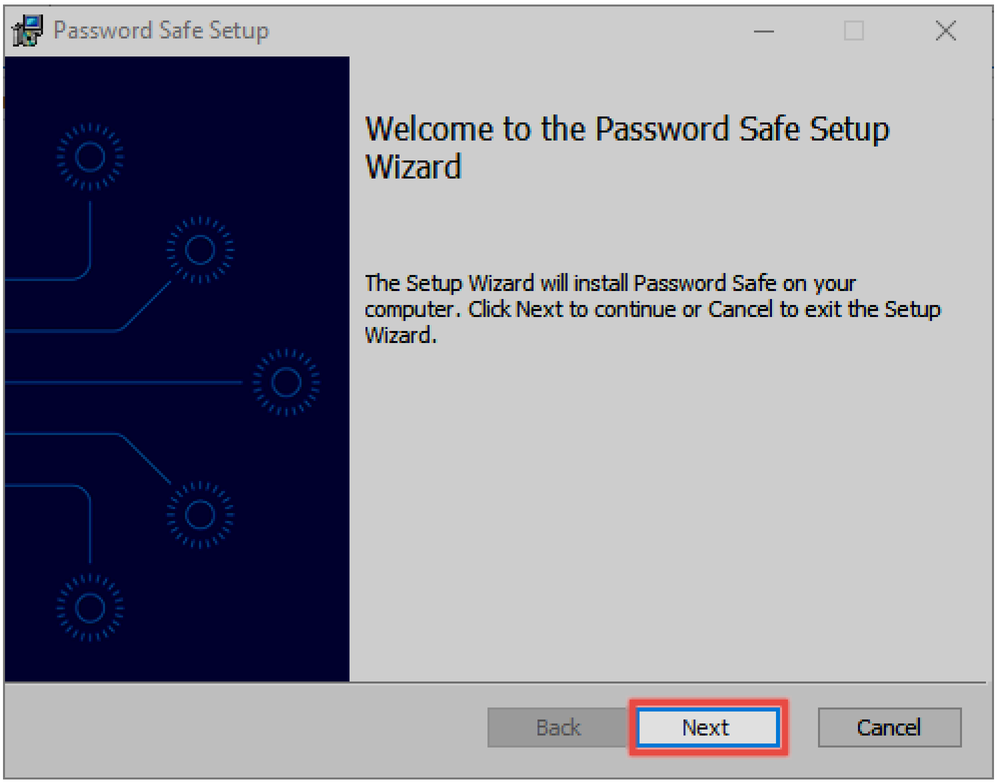
- Installation of AdminClient
- "Installation of client":#installation-client
- "Installation of WebAccess":#404

Installation AdminClient

Video guide

Guide

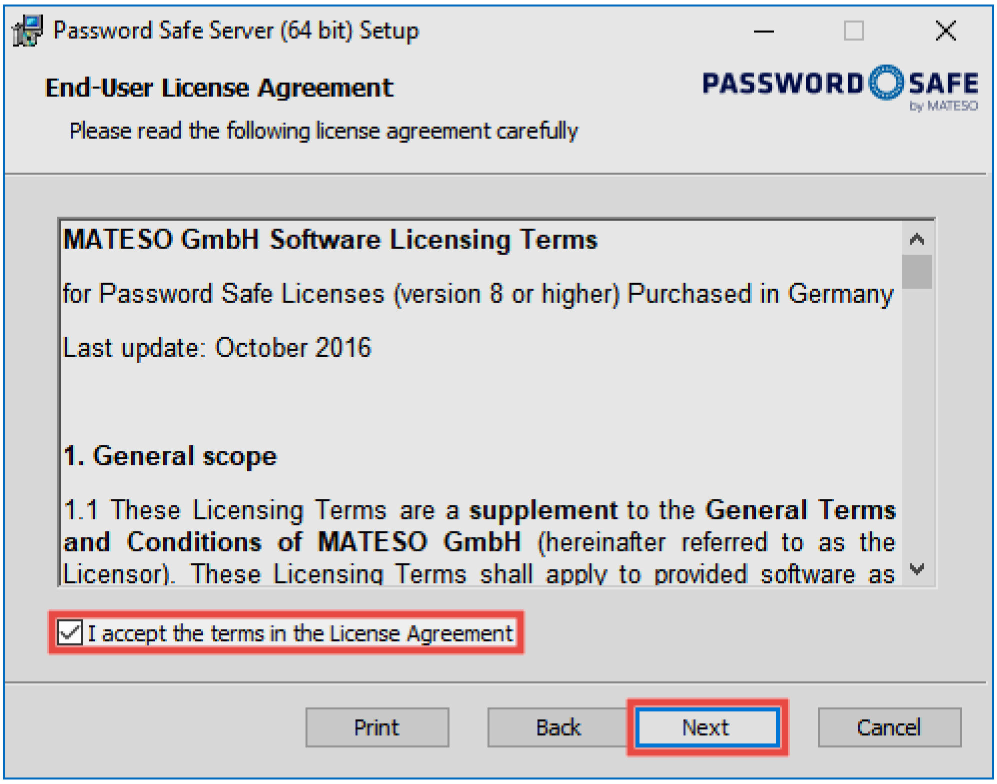
The “MSI installation files”:#installation-und-dokumentation and the associated “Server system requirements”:#systemanforderungen-server can be found in the corresponding sections. The following step-by-step guide will accompany you through the wizards.


Password Safe Setup

Welcome to the Password Safe Setup Wizard

The Setup Wizard will install Password Safe on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

You are firstly required to read and accept the license terms. These can also be printed.



Password Safe Server (64 bit) Setup

End-User License Agreement

Please read the following license agreement carefully

MATESO GmbH Software Licensing Terms

for Password Safe Licenses (version 8 or higher) Purchased in Germany

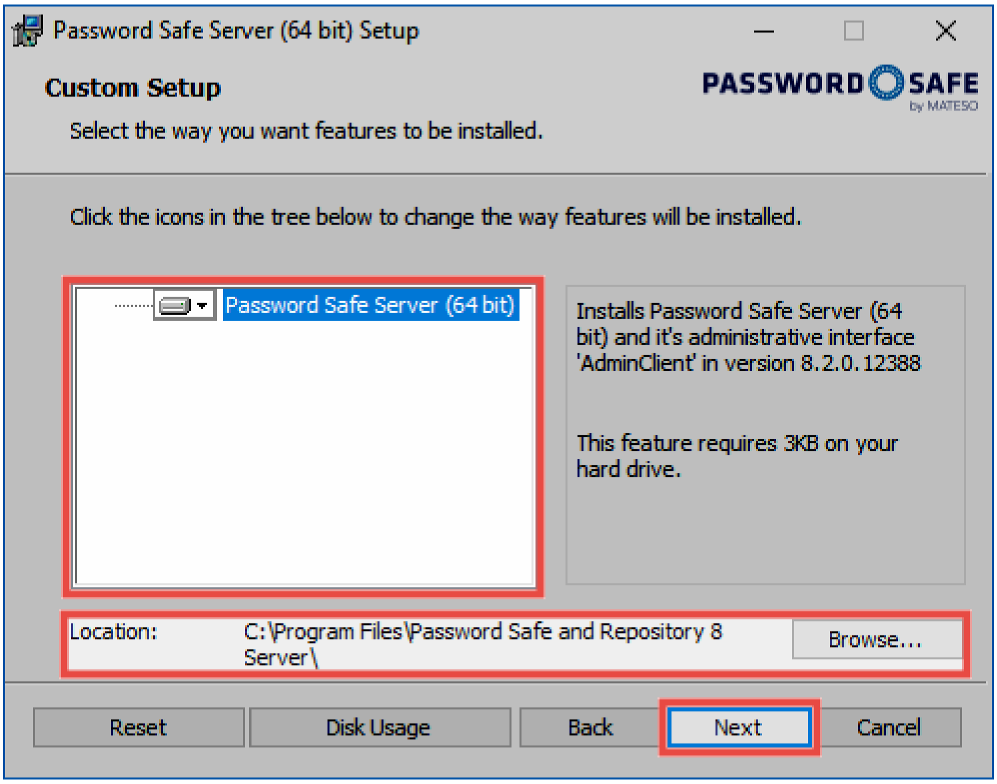
Last update: October 2016

1. General scope

1.1 These Licensing Terms are a **supplement** to the **General Terms and Conditions of MATESO GmbH** (hereinafter referred to as the Licensor). These Licensing Terms shall apply to provided software as

☑ I accept the terms in the License Agreement

The next step is to define the location. As a rule, the suggested location can be retained.



Password Safe Server (64 bit) Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

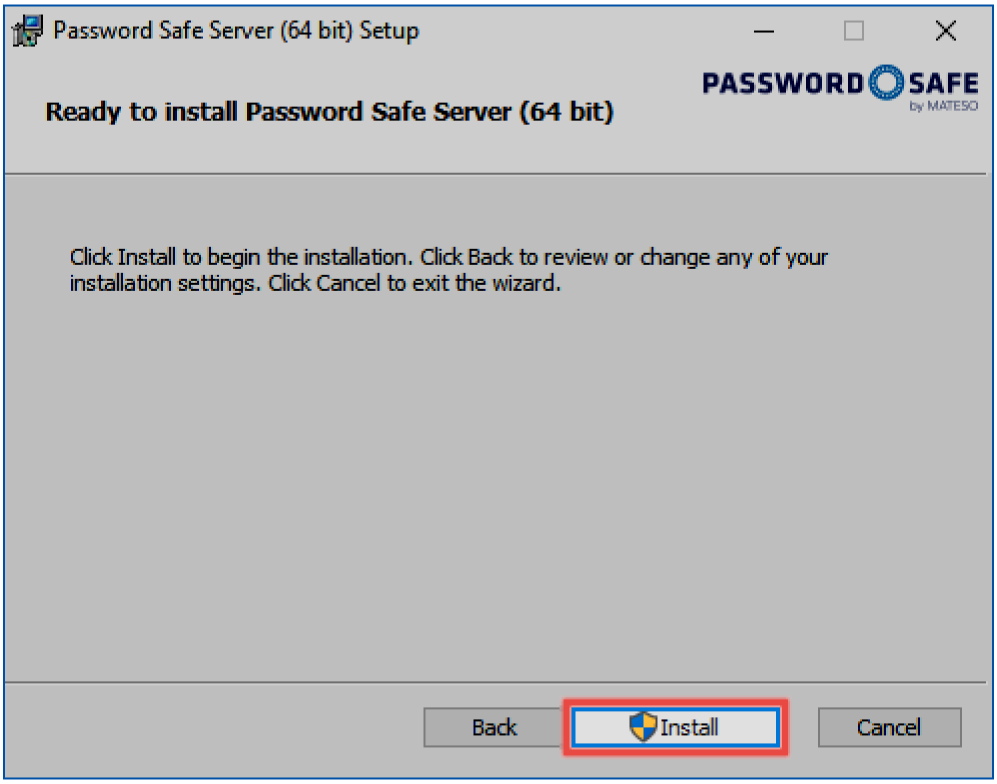
Password Safe Server (64 bit)

Installs Password Safe Server (64 bit) and it's administrative interface 'AdminClient' in version 8.2.0.12388

This feature requires 3KB on your hard drive.

Location: C:\Program Files\Password Safe and Repository 8 Server\

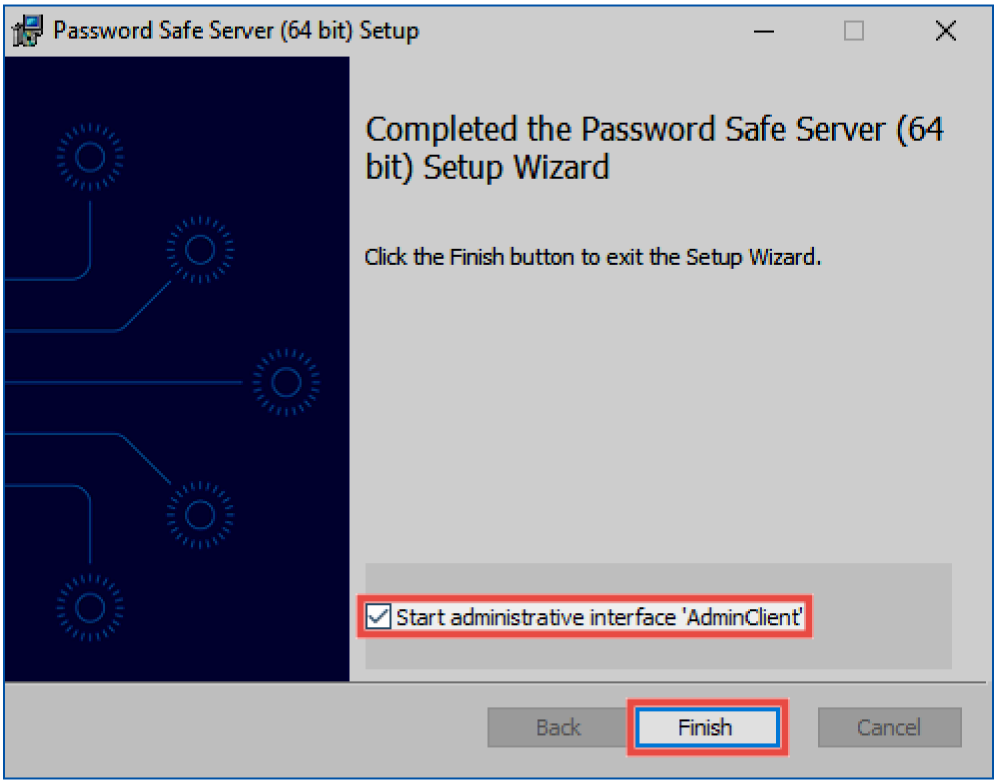
The next step is starting the installation.



Ready to install Password Safe Server (64 bit)

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

The last step closes the setup and opens (if desired) the server.



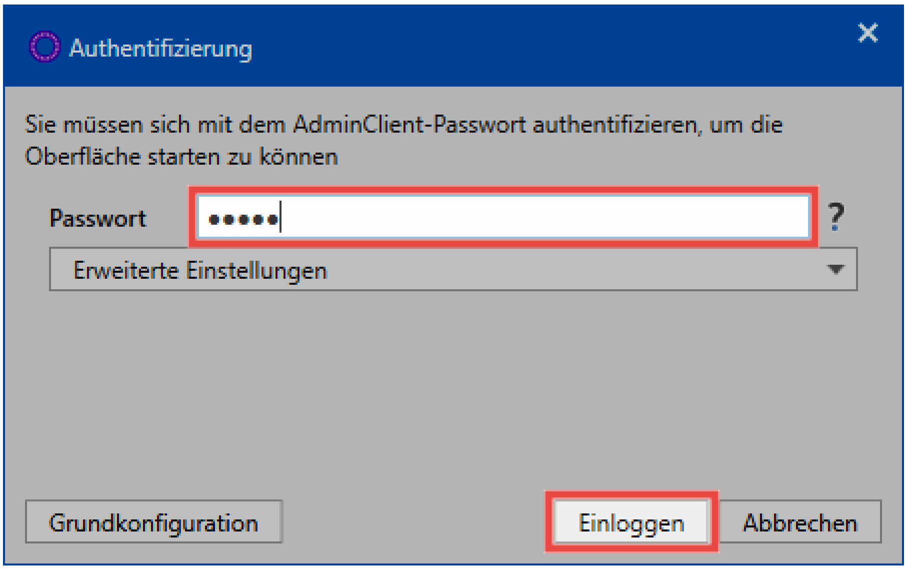
Completed the Password Safe Server (64 bit) Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Start administrative interface 'AdminClient'

Authentication

After the installation, you can login directly to the AdminClient.



Sie müssen sich mit dem AdminClient-Passwort authentifizieren, um die Oberfläche starten zu können

Passwort •••••

The initial password for the first login is “admin”. It should be changed directly after the logon.

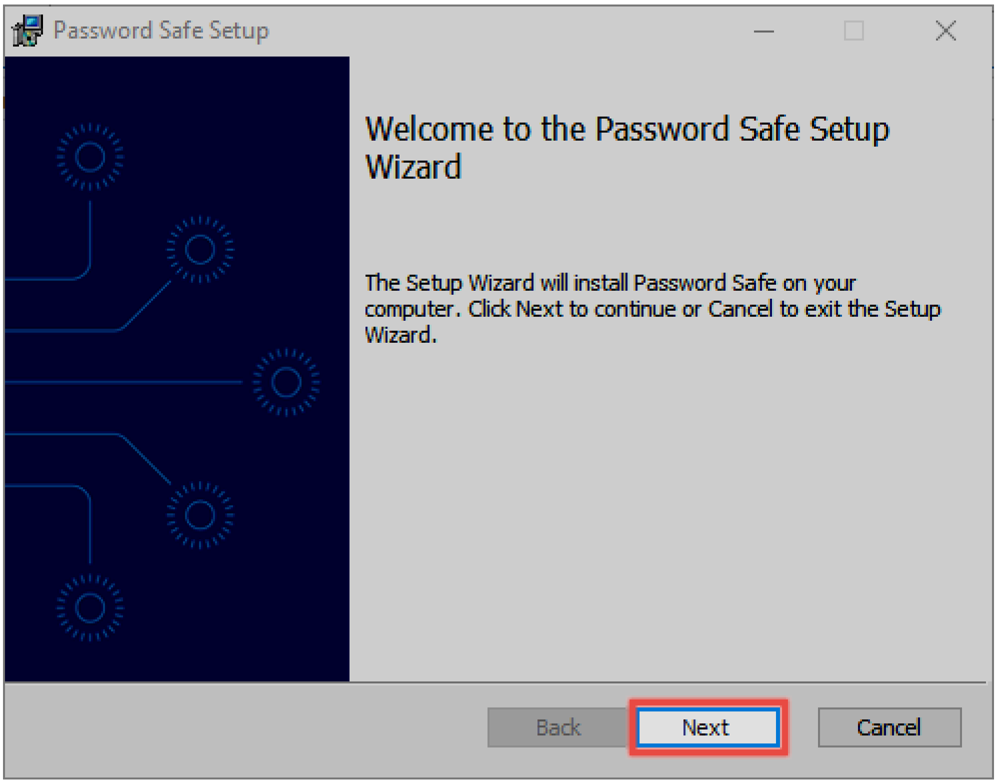
Click here to return to the “Getting started” section

Installation Client

Video guide

Guide

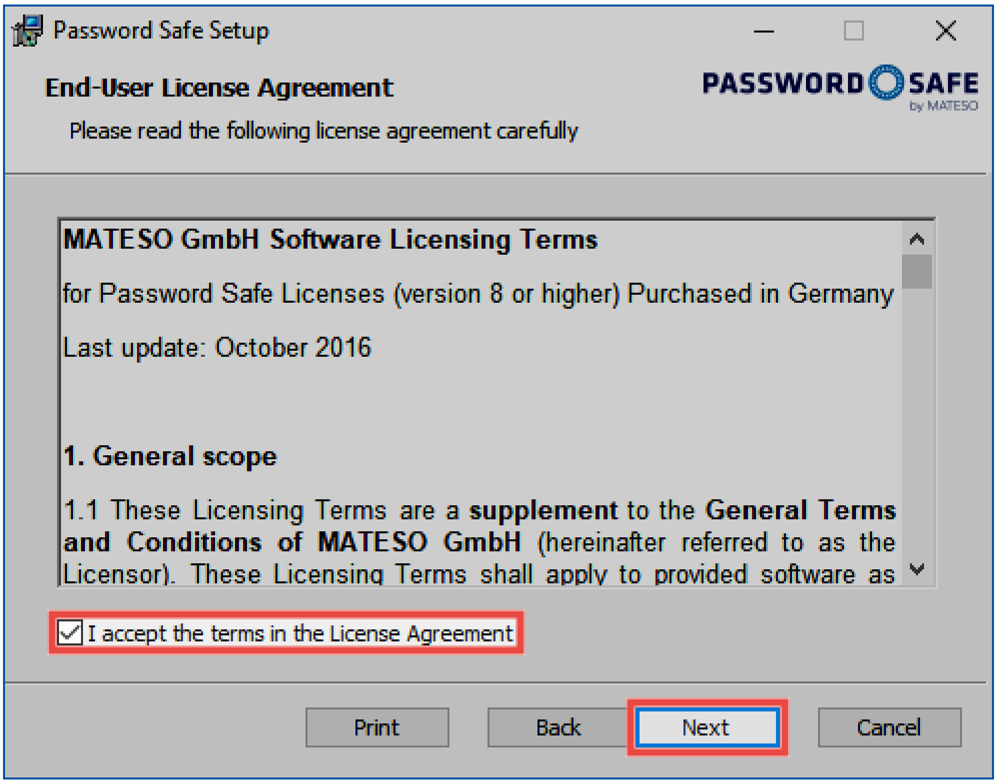
The “MSI installation files”:#installation-und-dokumentation and the associated “Client system requirements”:#systemanforderungen-client can be found in the corresponding sections. The following step-by-step guide will accompany you through the wizards.



Welcome to the Password Safe Setup Wizard

The Setup Wizard will install Password Safe on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

You are firstly required to read and accept the license terms. These can also be printed.



End-User License Agreement

Please read the following license agreement carefully

MATESO GmbH Software Licensing Terms

for Password Safe Licenses (version 8 or higher) Purchased in Germany

Last update: October 2016

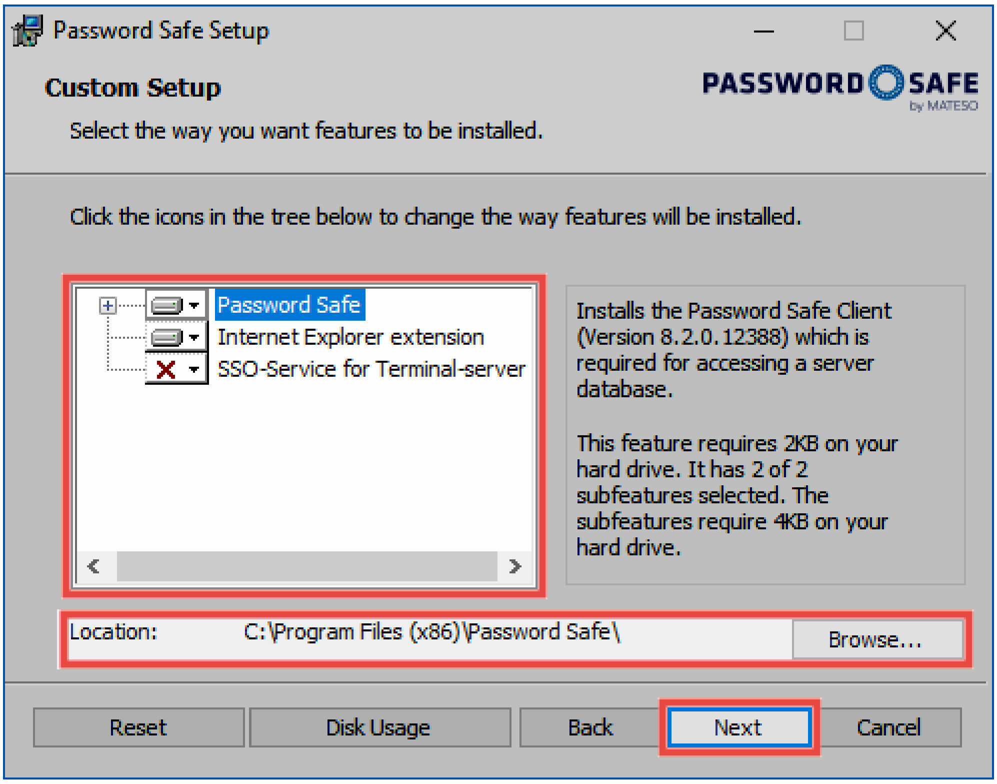
1. General scope

1.1 These Licensing Terms are a **supplement** to the **General Terms and Conditions of MATESO GmbH** (hereinafter referred to as the Licensor). These Licensing Terms shall apply to provided software as

☑ I accept the terms in the License Agreement

The next step is to define the location of the client. You can also define here whether additional components should be installed.

- **Password Safe and Repository 8** installs the client
- **Internet Explorer extension** is required to automatically transfer access data to Internet Explorer
- **SSO service for terminal server** allows automatic sign-on in the terminal server mode



Password Safe Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- Password Safe
- Internet Explorer extension
- SSO-Service for Terminal-server

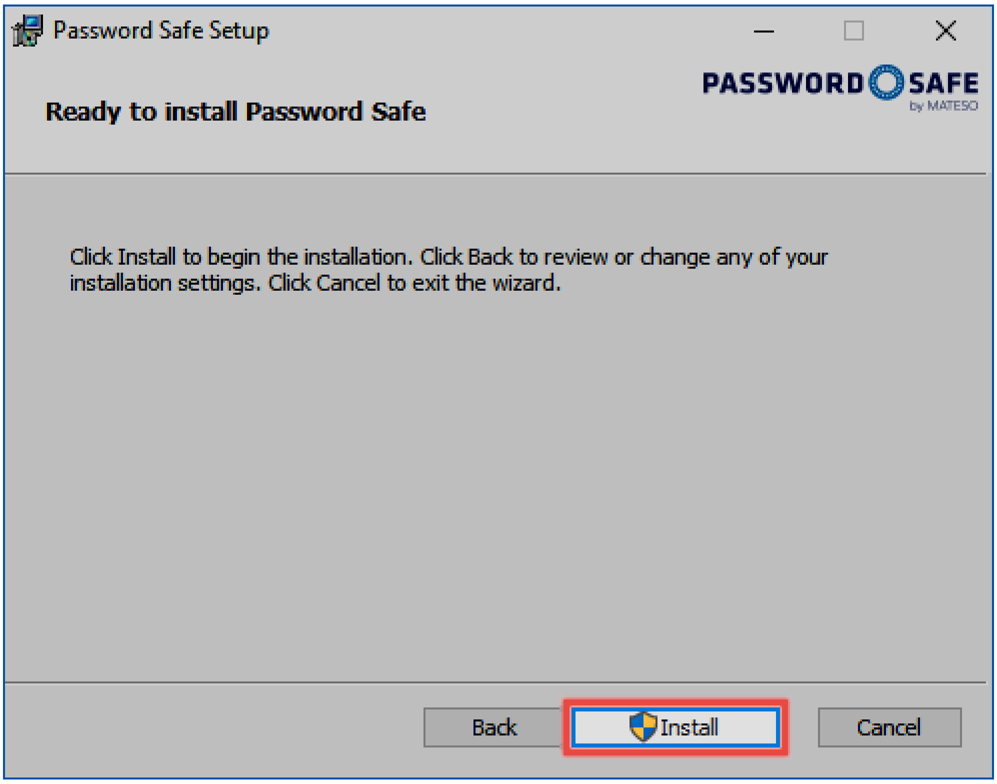
Installs the Password Safe Client (Version 8.2.0.12388) which is required for accessing a server database.

This feature requires 2KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 4KB on your hard drive.

Location: C:\Program Files (x86)\Password Safe\

! Please install the SSO service only if the terminal server operation is devised!

The actual installation starts in the next step.

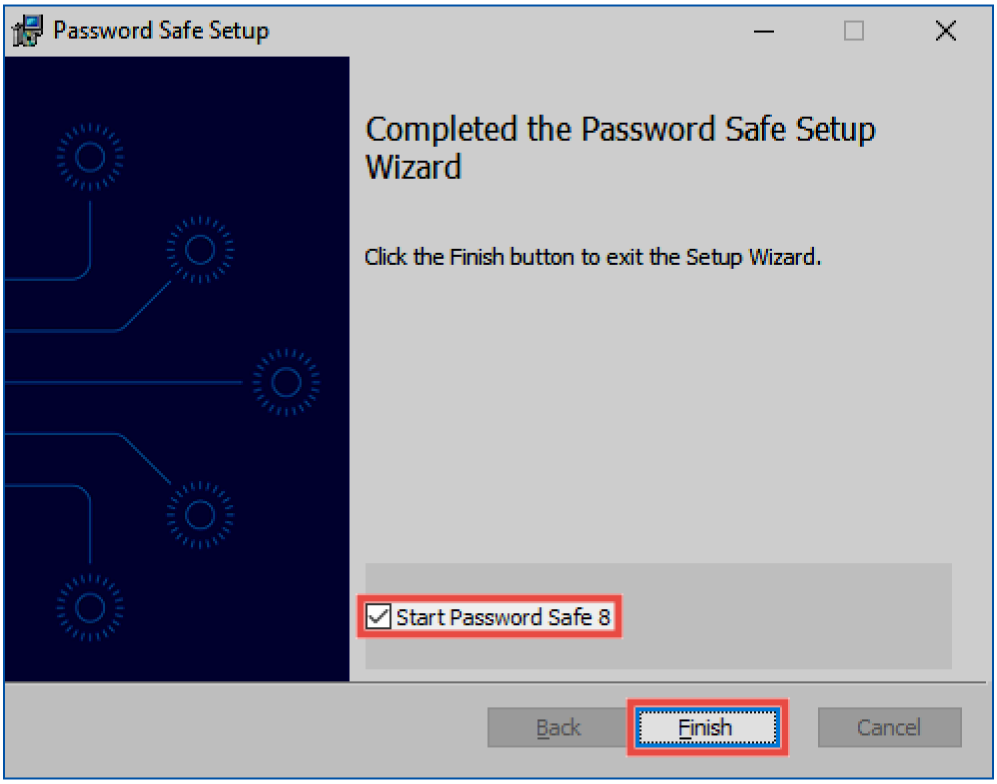


Password Safe Setup

Ready to install Password Safe

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

The last step finishes the setup and opens the client.



Password Safe Setup

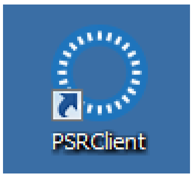
Completed the Password Safe Setup Wizard

Click the Finish button to exit the Setup Wizard.

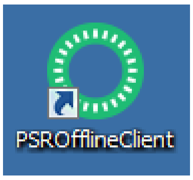
☑ Start Password Safe 8

Installed applications

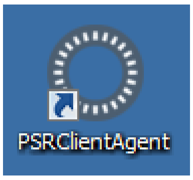
There are always several applications installed.



This is the regular client.



The Offline Client allows access to the data without connection to server.



The SSO Agent is the link between the browser add-ons and the database. It allows automatic login without opening the Client and runs in the background.

Integrating a database

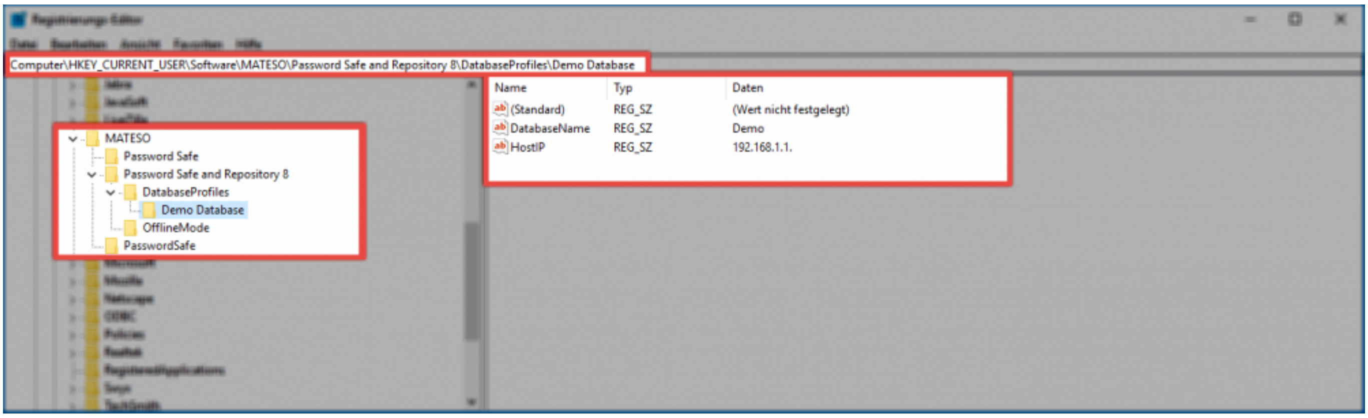
For connection to the database, the creation of a database profile is obligatory. The following information is required:

- **Profile name:** The name of the profile. This will be displayed on the client in the future
- **IP address:** The IP address of the Password Safe V8 server is stored here
- **Database name:** Specifies the name of the database

Distributing database profiles via the registry

Of course, there is also an option to distribute database profiles. The profiles are specified via a corresponding registry entry. At the next program start, they are transferred to Password Safe and saved within the configuration file. The following registry entry is created: **HKEY_CURRENT_USER\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles**. A new key with the name of the database is created here. The key must have the following entries:

HostIP: Server IP address
DatabaseName: Name of the database
LastUserName: The field for the user name can be specified here



Computer\HKEY_CURRENT_USER\Software\MATESO\Password Safe and Repository 8\DatabaseProfiles\Demo Database

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
DatabaseName	REG_SZ	Demo
HostIP	REG_SZ	192.168.1.1.

✻ If the corresponding registry entry is set and no related database profile exists, the profile will be created at the next start-up. Profiles created in this way cannot be edited or deleted on the client.

Click here to return to the “Getting started” section

Installation with parameters

What is installation with parameters?

The installation of the Password Safe client can also be optionally run on the command line. This method also requires the transfer of parameters. These can be combined with one another. In this case, the individual parameters are separated from one another by a blank space. The parameters listed in the following section enable you to adapt the type of client installation.

Running on the command line with parameters

Run the installation via the command line: **MSI-FILE.msi [PARAMETER]**

Parameter

- **INSTALL_IE_EXTENSION="0"**: The extension for Internet Explorer is not installed. In the list of the components to be installed in the setup, a check mark has not been set but this can be set again by the user
- **SSO_START_VIA_REGISTRY="0"**: Deactivates launching the SSO Agent in Windows autostart
- **INSTALL_SSO_AGENT="0"**: Deactivates the installation of the SSO Agent. In the list of the components to be installed in the setup, a check mark has not been set but this can be set again by the user
- **INSTALL_OFFLINE_CLIENT="0"**: Deactivates the installation of the offline client. In the list of the components to be installed in the setup, a check mark has not been set but this can be set again by the user

Installation of the WebClient

! This section exclusively deals with the first installation. The steps described here must **not** be carried out for an update.

For the installation of the WebClient, a WebClient module has been provided in the AdminClient.

Preparations for installation

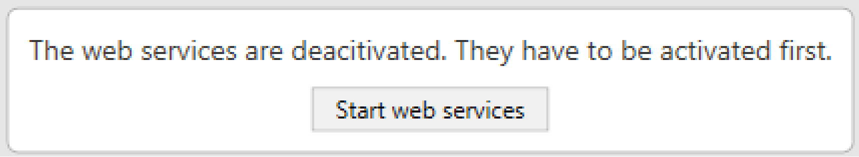
To carry out the installation of the WebClient without any further complications, the following preparations should be carried out:

System requirements

It should first be ensured that all of the “system requirements”:#systemanforderungen-webclient have been met.

Web service

When calling up the **WebClient** module in **AdminClient** for the first time, the web service firstly needs to be started.



The web services are deacitivated. They have to be activated first.

The Password Safe Server will restart as a result. The configuration interface is then displayed in the **WebClient** module.

SSL certificate

When starting the web service, the certificate selected in the basic configuration for use with the web services will be configured and connected to port 11016. This is the connection certificate for communication between the web server and the Password Safe server.

✻ In the background, the certificate is integrated into the operating system for use with the configured port (11016 TCP) with **netsh http add sslcert**. To uninstall, the connection is amended with **netsh http delete sslcert**.

Firewall

The port 11016 TCP must have been enabled for incoming communication.

Databases

All databases that are to be used on the **WebClient** need to be approved for this purpose. It is sufficient to double click on the corresponding database. The option **Activate access via WebClient** can now be selected.

Installation

The WebClient is generated by the AdminClient and made available in a ZIP archive. Depending on the web server used, the ZIP archive is created accordingly. The installation also differs depending on the relevant web server. Irrespective of the web server used, the following information firstly needs to be entered:

Target file
The folder where the ZIP archive containing the WebClient should be saved is entered here.

> ✻ If it is being installed on an IIS web server, a file with the name “config.bat”:#installation-webclient will be created in the ZIP archive, which then integrates the WebClient onto the web server.

> ! The **installation directory** for the AdminClient may **not** be used here.

Server IP
The IP address for the Password Safe server is displayed here for purely informative purposes.

> ✻ It should be checked whether the IP address is correct because otherwise the WebClient will not be able to establish any connection. If the IP address is not correct, it needs to be changed in the basic configuration for the AdminClient.

Web server host address
The IP address or the host name of the web server needs to be entered.

Port
The port that is used to communicate with the WebClient is entered here.

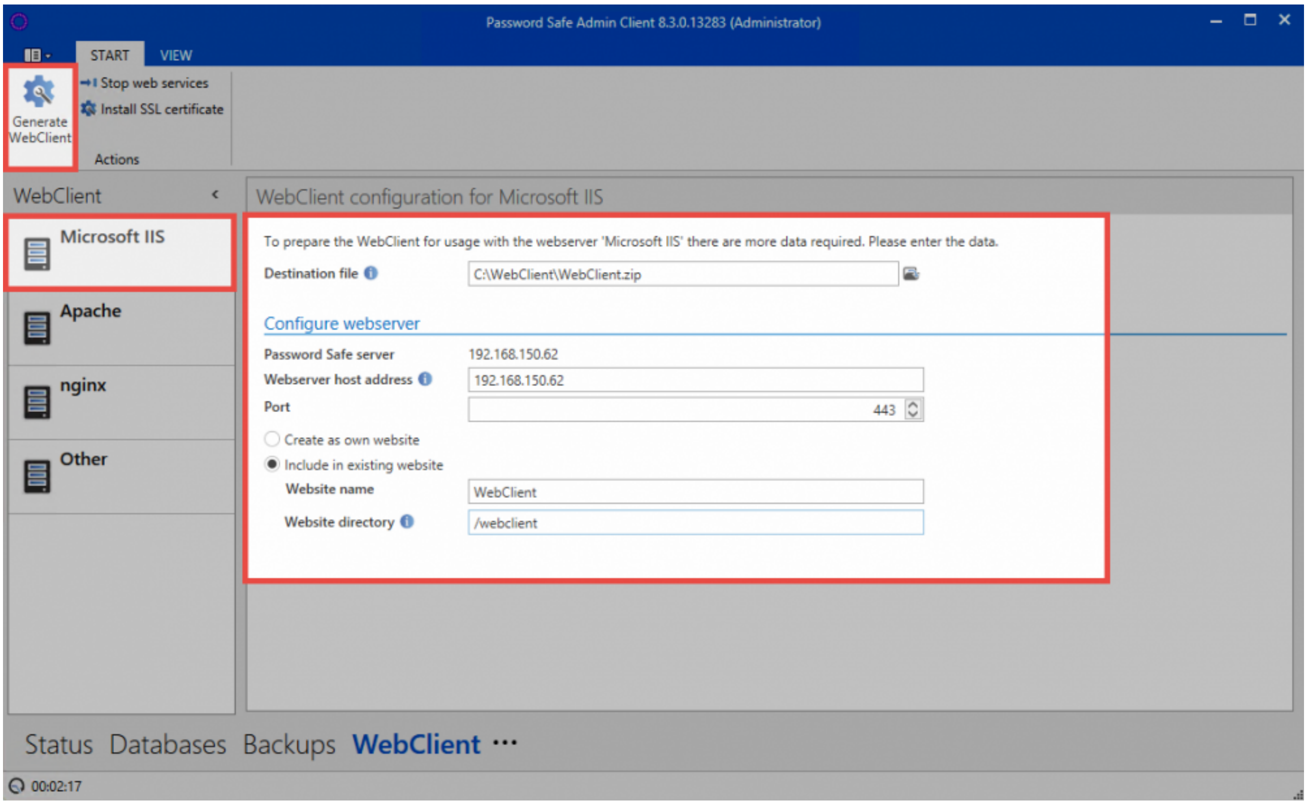
All of the subsequent steps or the required tasks will be explained below for each specific web server.

Microsoft IIS

If the **WebClient** is being operated on a Microsoft IIS web server, there are two methods for integrating it into the system:

Create as its own website
For this option, a website with the name “WebClient” will be directly created on the IIS by config.bat. The WebClient will be operated here from the standard directory C:\inetpub\wwwroot.

Integrate in existing website
requires there to be an existing website. Therefore, a website needs to be firstly created on the IIS web sever. The **name of the website** then needs to be entered in the AdminClient. It is also necessary to enter the folder from which the WebClient should be operated under *website directory”. The format here is “/webclient”



WebClient configuration for Microsoft IIS

To prepare the WebClient for usage with the webserver 'Microsoft IIS' there are more data required. Please enter the data.

Destination file: C:\WebClient\WebClient.zip

Configure webserver

Password Safe server: 192.168.150.62

Webserver host address: 192.168.150.62

Port: 443

○ Create as own website

● Include in existing website

Website name: WebClient

Website directory: /webclient

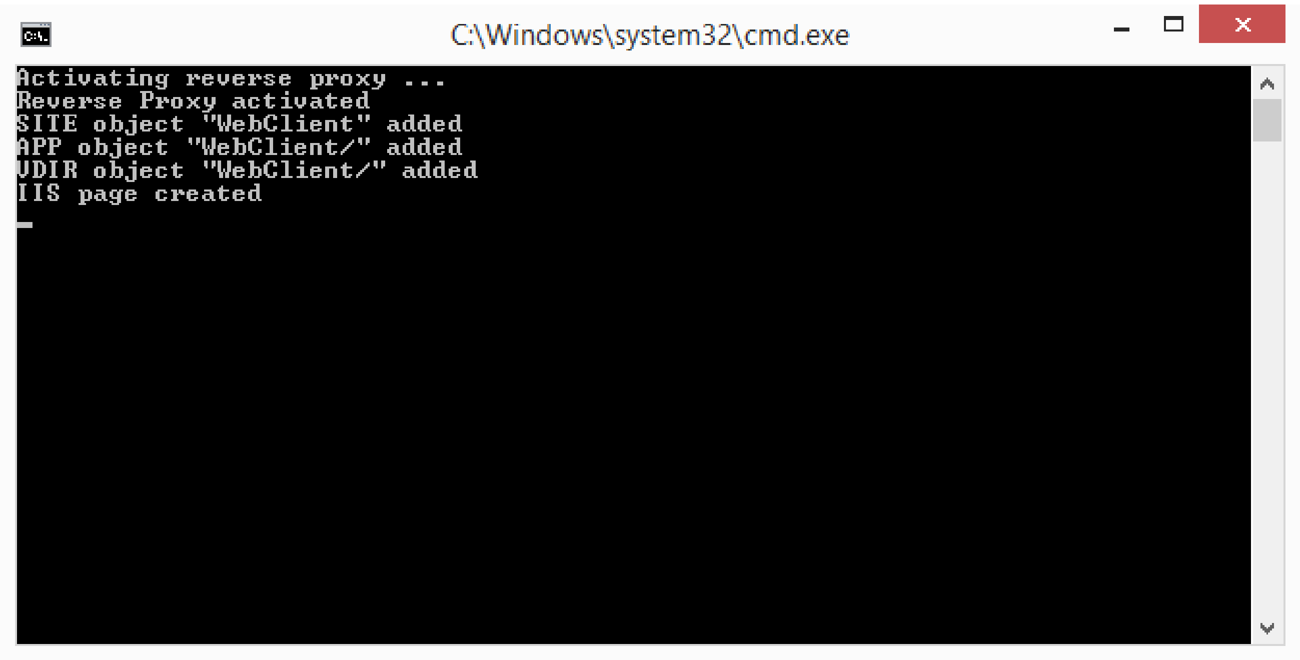
Once all of the settings have been entered, the WebClient can be created via the corresponding button in the ribbon. When the ZIP archive containing the WebClient has been created, it is copied to the previously defined directory (C:\inetpub\wwwroot as standard) and unzipped there to create a new directory.

Config.bat

The file **config.bat** can be found in the newly created **WebClient** directory and now needs to be executed when logged on as the administrator. This will integrate the WebClient into the IIS web server.

> If the system requirements have not been met, you will be informed that the **URL Rewrite** and/or **Application Request Routing** modules need to be installed. In this case, follow the instructions on the wizard that will then immediately open. Afterwards, **config.bat** needs to be executed again.

If the website has been correctly created, this will be correspondingly indicated by the notification **IIS page created**.

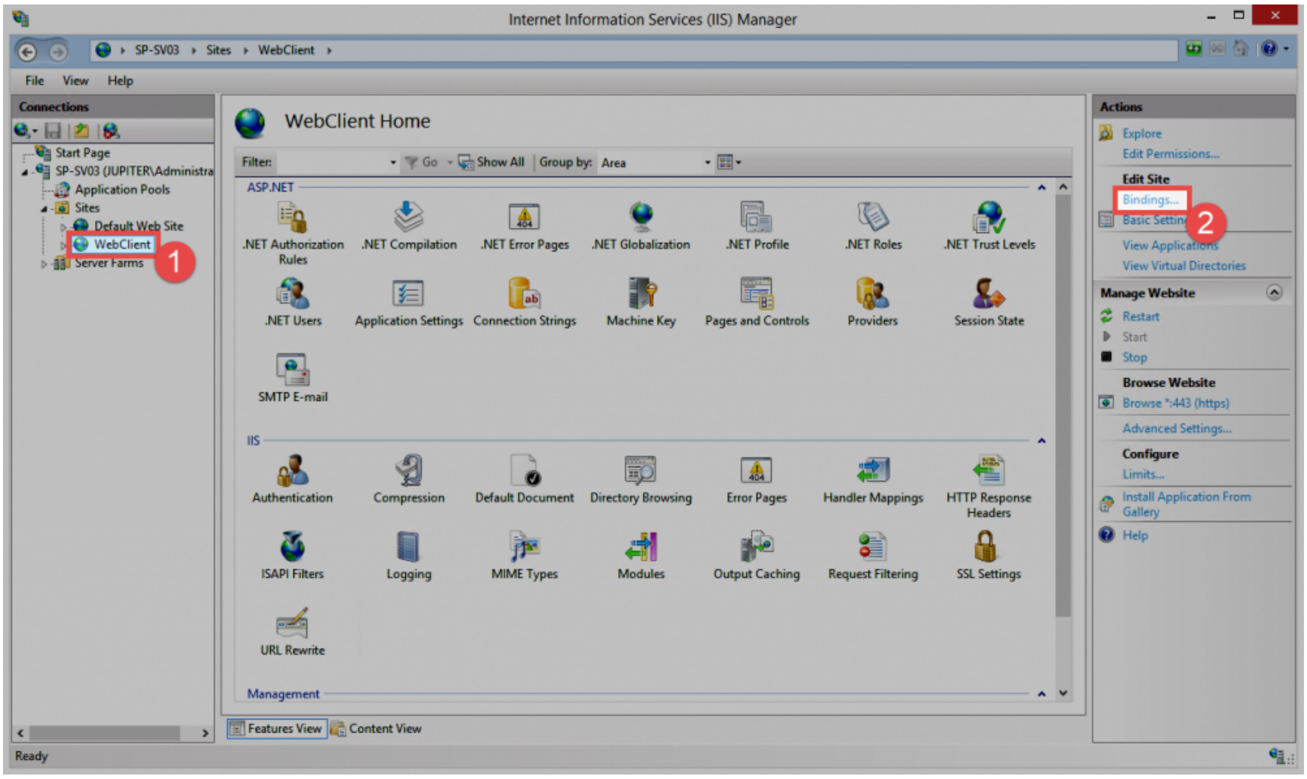


```
Activating reverse proxy ...
Reverse Proxy activated
SITE object "WebClient" added
APP object "WebClient/" added
VDIR object "WebClient/" added
IIS page created
```

> **!** Following a successful installation, it is imperative that **config.bat** is deleted! The **config.bat** file should also not be used for an “update”:#updates!

Certificate

The certificate then needs to be saved. Select the newly created website on the IIS web server. The bindings can now be opened on the far right.



Select the **https** entry and open it for editing. The **SSL certificate** is then selected here.

The WebClient is now ready to use and can be directly started. Further information can be found at the end of this section under “Calling up the WebClient”:#installation-webclient.

In addition, the Password Safe certificate needs to be exported from the Password Safe Server and imported onto the ISS under **local computer > trusted root certificate location -> certificates**. Further information can be found in the section Certificates.

Apache

In order to integrate the WebClient onto an Apache server, it is first necessary to enter all of the relevant settings:

Document directory

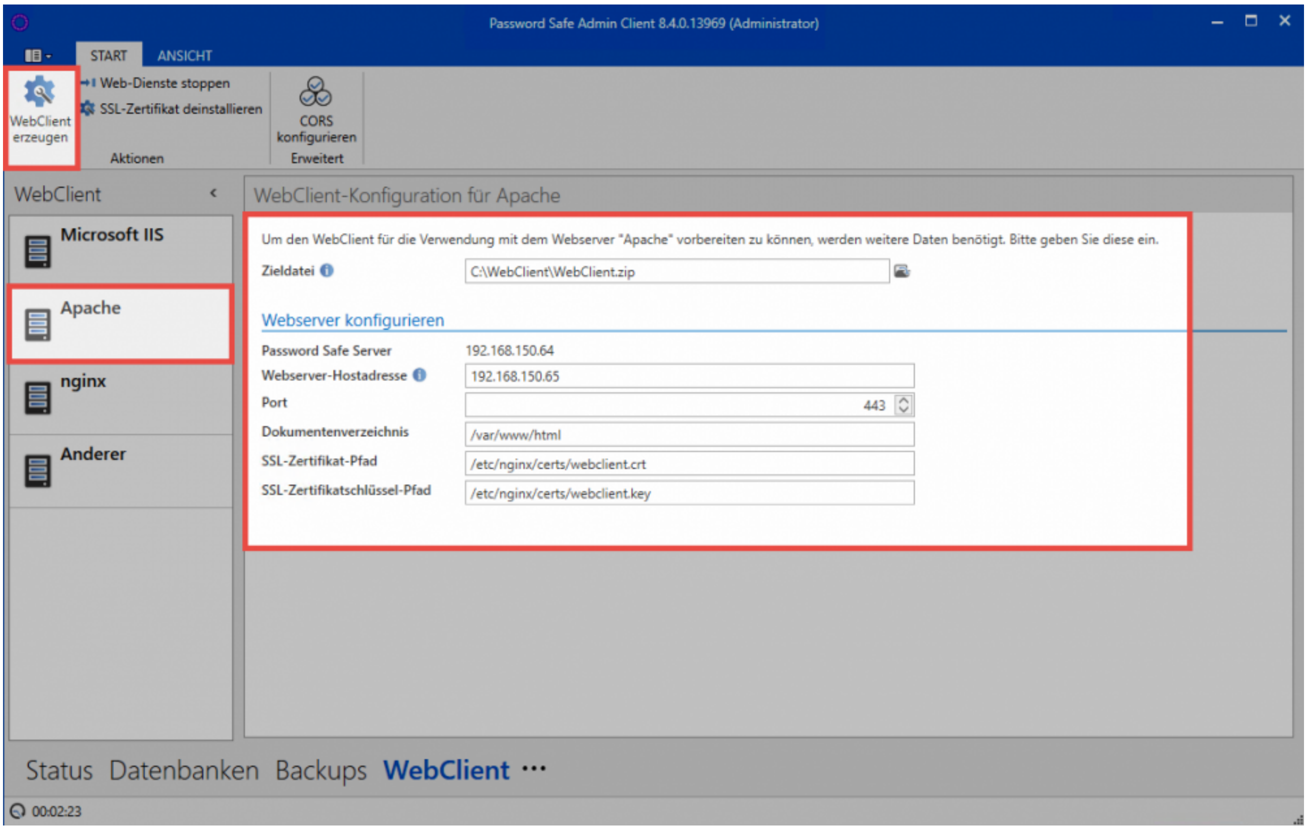
The folder from which the WebClient should be operated is entered here.
The default folder is **/var/www/html**

SSL certificate path

It is necessary to enter the directory in which the certificate will be saved here.

SSL certificate key path

Finally, it is necessary to enter where the certificate key is located here.



WebClient-Konfiguration für Apache

Um den WebClient für die Verwendung mit dem Webserver "Apache" vorbereiten zu können, werden weitere Daten benötigt. Bitte geben Sie diese ein.

Zieldatei: C:\WebClient\WebClient.zip

Webserver konfigurieren

Password Safe Server: 192.168.150.64

Webserver-Hostadresse: 192.168.150.65

Port: 443

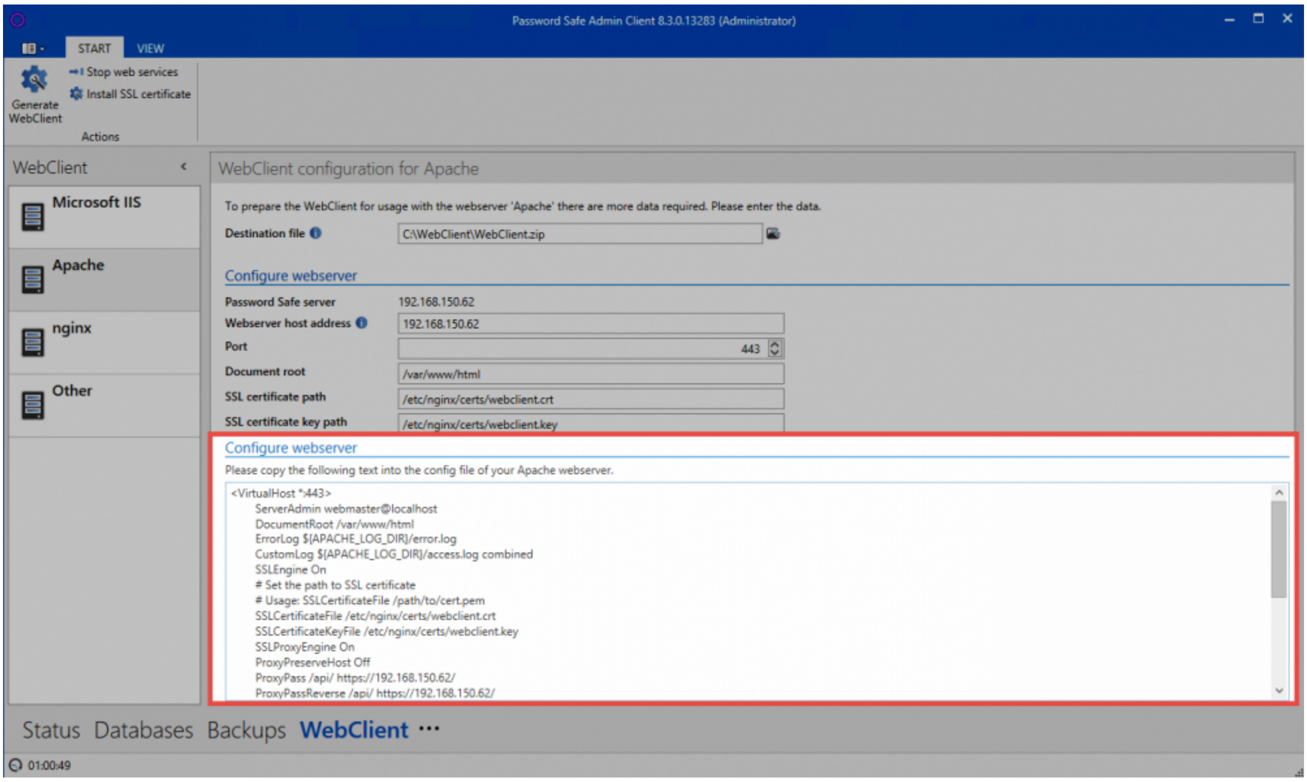
Dokumentenverzeichnis: /var/www/html

SSL-Zertifikat-Pfad: /etc/nginx/certs/webclient.crt

SSL-Zertifikatschlüssel-Pfad: /etc/nginx/certs/webclient.key

Once all of the settings have been entered, the WebClient can be created via the button in the ribbon. The folder in which the ZIP file is located will then open automatically. The archive is now unzipped and the contents copied to the document directory on the web server.

The configuration for the Apache server has now also been created and can be viewed on the AdminClient.



WebClient configuration for Apache

To prepare the WebClient for usage with the webserver 'Apache' there are more data required. Please enter the data.

Destination file: C:\WebClient\WebClient.zip

Configure webserver

Password Safe server: 192.168.150.62
Webserver host address: 192.168.150.62
Port: 443
Document root: /var/www/html
SSL certificate path: /etc/nginx/certs/webclient.crt
SSL certificate key path: /etc/nginx/certs/webclient.key

Configure webserver

Please copy the following text into the config file of your Apache webserver.

```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine On
        # Set the path to SSL certificate
        # Usage: SSLCertificateFile /path/to/cert.pem
        SSLCertificateFile /etc/nginx/certs/webclient.crt
        SSLCertificateKeyFile /etc/nginx/certs/webclient.key
        SSLProxyEngine On
        ProxyPreserveHost Off
        ProxyPass /api/ https://192.168.150.62/
        ProxyPassReverse /api/ https://192.168.150.62/
```

The configuration can be selected using CTRL+A and copied. It is then directly integrated onto the Apache server.

> ✻ The configuration of the Apache server is always individual. Therefore, it is only possible to roughly describe the process for a standard installation.

Standard configuration

The file **/etc/apache2/sites-available/default-ssl.conf** is (for example “nano”) opened. Everything between `<IfModule mod_ssl.c>` and `</IfModule mod_ssl.c>` is now deleted and replaced by the configuration from the server. Apache is subsequently restarted via **systemctl reload apache**.

The WebClient is now ready to use and can be directly started. Further information can be found at the end of this section under “Calling up the WebClient”:#installation-webclient.

nginx

In order to integrate the WebClient onto an nginx server, it is first necessary to enter all of the relevant settings:

Document directory

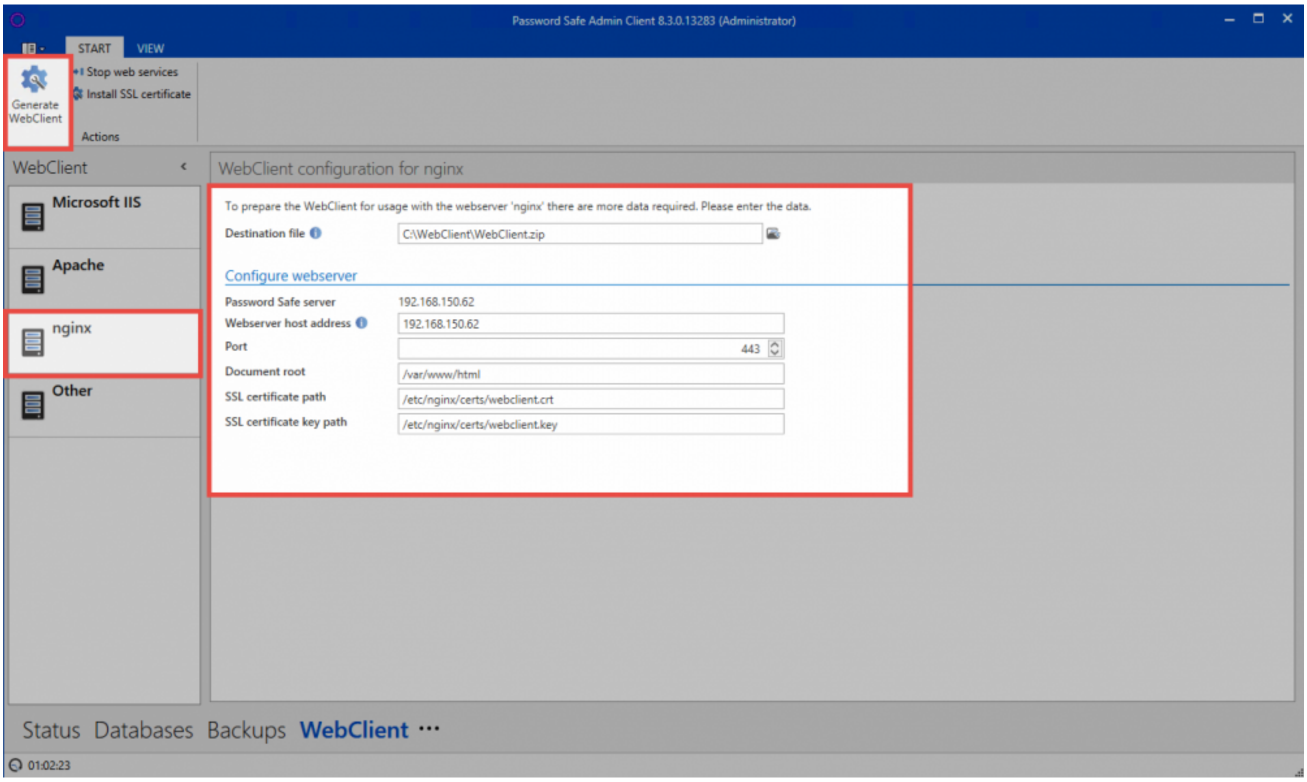
The folder from which the WebClient should be operated is entered here.
The default folder is **/var/www/html**

SSL certificate path

It is necessary to enter the directory in which the certificate will be saved here.
The standard path here is **/etc/nginx/certs/webclient.crt**

SSL certificate key path

Finally, it is necessary to enter where the certificate key is located here.
The default setting is **/etc/nginx/certs/webclient.key**



WebClient configuration for nginx

To prepare the WebClient for usage with the webserver 'nginx' there are more data required. Please enter the data.

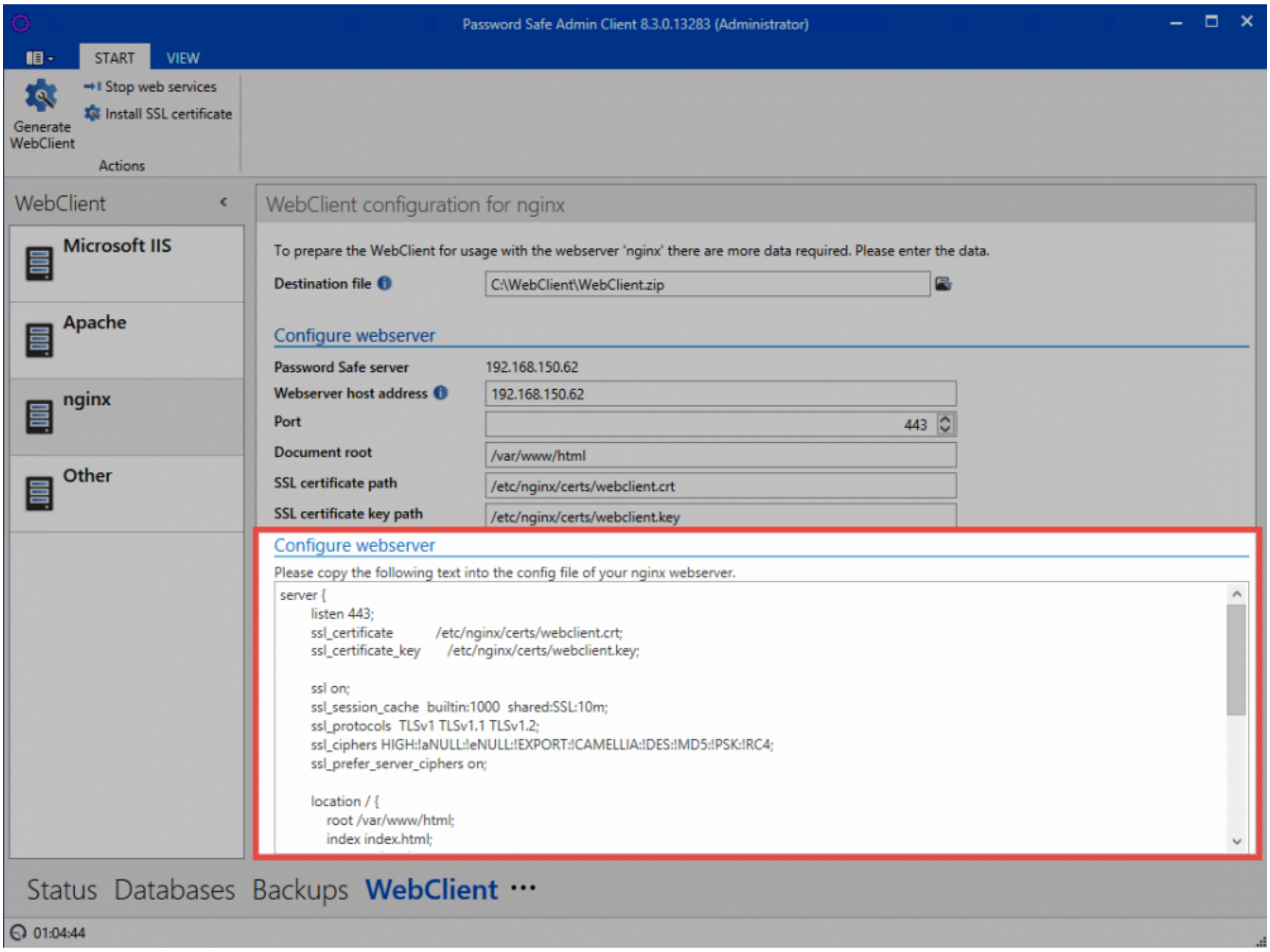
Destination file: C:\WebClient\WebClient.zip

Configure webserver

Password Safe server: 192.168.150.62
Webserver host address: 192.168.150.62
Port: 443
Document root: /var/www/html
SSL certificate path: /etc/nginx/certs/webclient.crt
SSL certificate key path: /etc/nginx/certs/webclient.key

Once all of the settings have been entered, the WebClient can be created via the button in the ribbon. The folder in which the ZIP file is located will then immediately open. The archive is unzipped and its contents are copied to the document directory on the web server.

The configuration for the nginx server was also created together with the ZIP file. This can be directly viewed on the AdminClient.



WebClient configuration for nginx

To prepare the WebClient for usage with the webserver 'nginx' there are more data required. Please enter the data.

Destination file: C:\WebClient\WebClient.zip

Configure webserver

Password Safe server: 192.168.150.62
Webserver host address: 192.168.150.62
Port: 443
Document root: /var/www/html
SSL certificate path: /etc/nginx/certs/webclient.crt
SSL certificate key path: /etc/nginx/certs/webclient.key

Configure webserver

Please copy the following text into the config file of your nginx webserver.

```
server {
        listen 443;
        ssl_certificate         /etc/nginx/certs/webclient.crt;
        ssl_certificate_key       /etc/nginx/certs/webclient.key;

        ssl on;
        ssl_session_cache  builtin:1000  shared:SSL:10m;
        ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
        ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
        ssl_prefer_server_ciphers on;

        location / {
            root /var/www/html;
            index index.html;
```

The configuration then still needs to be integrated onto the nginx server. It can be directly copied on the AdminClient for this purpose.

> Every web server configuration is individual. Therefore, it is only possible to outline the normal process for a standard installation.

Standard configuration

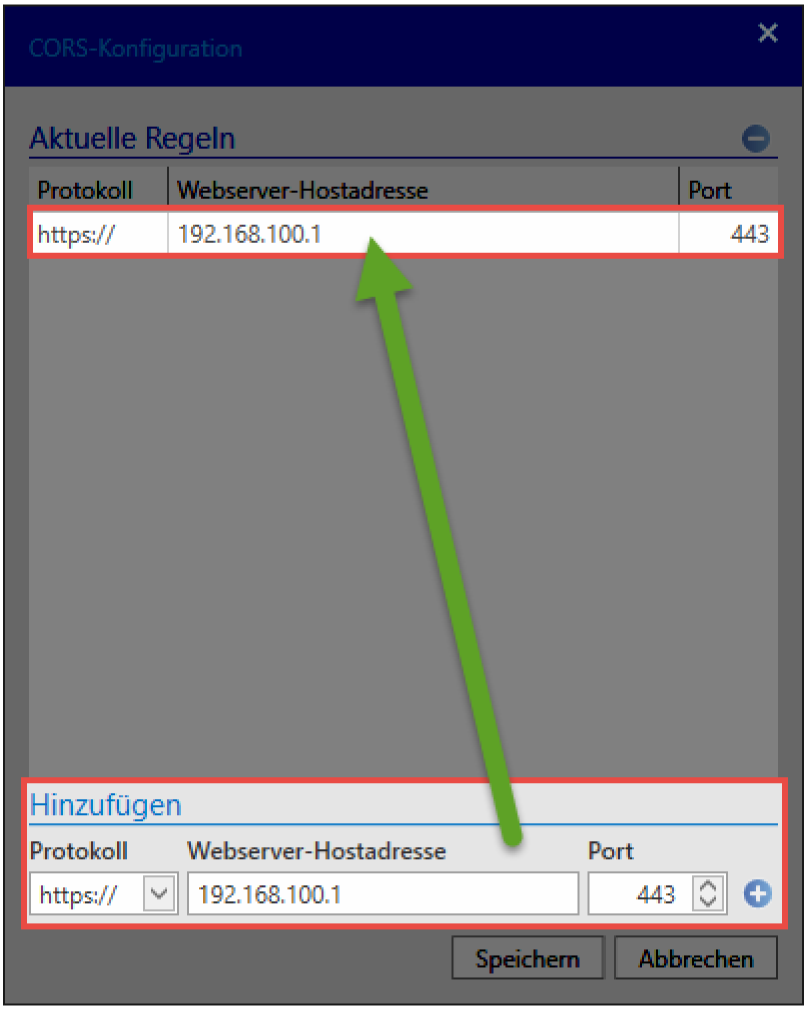
The file **/etc/nginx/sites-available/default** is firstly opened. For example via “nano”. Now search for the entry `server { }`. The configuration for the AdminClient is then added. Finally, the web server is restarted using the command **systemctl restart nginx**.

The WebClient is now ready to use and can be directly started.

CORS configuration

A button for the so-called **CORS configuration** can be found on the ribbon. It is essential that this configuration is carried out before the WebClient can be used. A list of the permitted CORS domains will be saved as a result. Requests received via the WebClient can then be checked against this list. The request will only be successfully carried out if the origin header for a request is available in the permitted domains.

In order to add a domain, simply enter it at the bottom of the dialogue. Clicking on ⊕ will add the entry to the list at the top.



Protokoll	Webserver-Hostadresse	Port
https://	192.168.100.1	443

Protokoll: https://
Webserver-Hostadresse: 192.168.100.1
Port: 443

✻ In general, it is sufficient to add the IP address which was also saved as the **Web server host address**.

Calling up the WebClient

The process for calling up the WebClient is dependent on the configuration of the web server:

WebClient in **root directory** -> **https://hostname**
WebClient in a **subdirectory** -> **https://hostname/pfad-zum-unterverzeichnis**
Port is not set to 443 -> **https://hostname:port/pfad-zum-unterverzeichnis**

Updates

Reasons for regular updates

Our development team is constantly working on the further development of the software. This does not only involve fixing any problems but also primarily the development of new features to adapt the software as best as possible to the requirements of our customers. Therefore, it is recommended that you regularly install the updates. Only in this way can you benefit from these further developments.

The documentation always refers to the latest version available. If Password Safe deviates from the documentation (e.g. in appearance or also its functional scope), it makes sense to firstly update to the latest version.

> ✻ The update check on the server or the client can be used to search for available updates. The update check on the client must firstly be released for users in the settings. We recommend leaving the update check deactivated for normal users because otherwise these users could independently attempt to install updates. As a new client cannot connect to an old server, this will mean that the user is no longer able to log in.

Requirements

Some requirements should be checked or established before an update.

Check the software maintenance package

The right to install updates is acquired with the software maintenance package. It is important to note that you are permitted to install all updates as long as the software maintenance package is still active. If the software maintenance package has expired, you are only permitted to use those versions that were released during the term of the software maintenance package. Therefore, you should check whether the software maintenance package is still active before an update. This can be easily checked on the AdminClient under “License settings”:#lizenzeinstellungen.

Creating a backup

An update always involves making a profound change to the existing software. A corresponding “backup”:#backupverwaltung should thus be created directly before the update to ensure that no data is lost if a serious problem arises.

Checking compatibility

An attempt is always made to design the AdminClient so that it is backwards compatible. Unfortunately this is not always possible. Therefore, you should always check which client version the AdminClient is compatible with before an update. The “version history”:#changelogs for the relevant version will provide this information.

> ! If the password for logging in to the AdminClient on the database has been saved, it is essential that it is noted down or temporarily saved elsewhere before an update!

Latest installation files

The installation files can be downloaded from the customer information system:
https://license.passwordsafe.de/kis
Please simply use the access data that we sent to you by email to log in.

Update

Updating the AdminClient

The AdminClient is simply installed on top of the existing installation.

> ✻ If the service has not been ended in advance, the installation wizard will give you the opportunity to do so. If the service is still not ended at this stage, the computer will then need to be restarted. It is thus recommended that the Password Safe services are ended before the update.

Further information on the installation wizard can be found in the section “Installation of the AdminClient”:#installation-server.

Patch level update for the databases

The databases are usually deactivated after updating the AdminClient because they do not yet have the corresponding patch level. This should be immediately checked. After logging in to the AdminClient, the module “Databases” is immediately visible. If the databases have been deactivated, you can reactivate them directly in the ribbon via the corresponding button. The patch level will be updated during this process.

Updating the client

The updates for the client are also simply installed over the existing installation. Further information can be found in the section Installation of the client. Naturally, the update can also be carried out using the installation parameters.

Updating the WebClient

The application server must firstly be updated. A new “WebClient”:#installation-webclient is then created according to the instructions for the web server being used. The document directory on the web server should now be completely emptied. The WebClient is then unzipped and copied to the document directory on the corresponding web server.

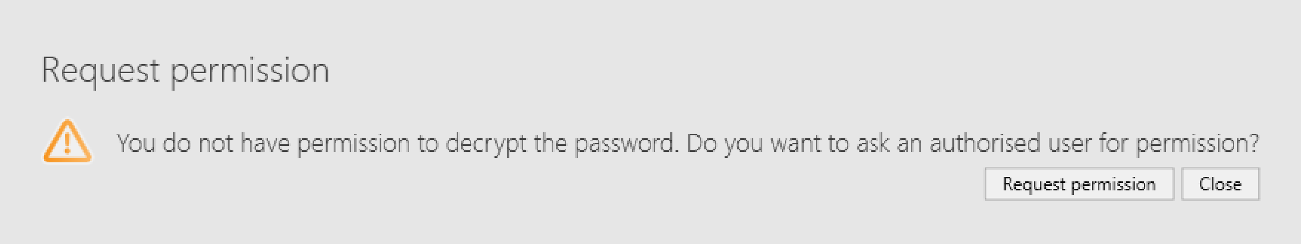
! If the WebClient is being operated on an IIS web server, a new **config.bat** is generated for creating the new version. This must not be executed if the WebClient has already been installed and it must be deleted without fail after a successful update.

When updating to version 8.4.0.14576, it is essential that the **CORS configuration** is carried out. This version also changes the port on the server side from 443 TCP to 11016 TCP. The standard SSL port will be available for use by the WebServer as a result. If a port other than 443 was previously used (because the web server and Password Safe server are running on one machine), this can now be used again. It will be automatically configured when you run the new WebClient.

Settlement right key

Problem Description

In the version 8.3.0.13378 passwords which cannot be decrypted for other users could be created. In this case, individual users or even all users do not have the necessary legal key. If a user wants to reveal an affected password, the following message is displayed:



Request permission

You do not have permission to decrypt the password. Do you want to ask an authorised user for permission?

Bugfix

The bug was fixed with the version 8.3.0.14422 Hotfix 1. If an older version is in use, it is important to update to the latest version 8.4.0.14576.

Review and settlement of records

When updating to version 8.4.0.14576, the AdminClient is checked for affected data records.

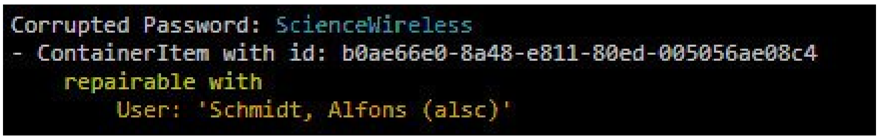
Review via the AdminClient

The results of the query show which passwords can be fixed by which user. (In this example, the entries are highlighted in color).

Blue = password name
Yellow = Repairable / Irreparable
Orange = users / roles who can fix the password

Reparable records

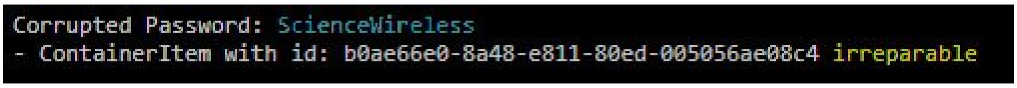
Passwords in which users / roles with entitlement right and right key exist:



```
Corrupted Password: ScienceWireless
- ContainerItem with id: b0ae66e0-8a48-e811-80ed-005056ae08c4
    repairable with
        User: 'Schmidt, Alfons (alsc)'
```

Irreparable records

Passwords in which users / roles without a legal key or with a legal key but without an authorization right exist:

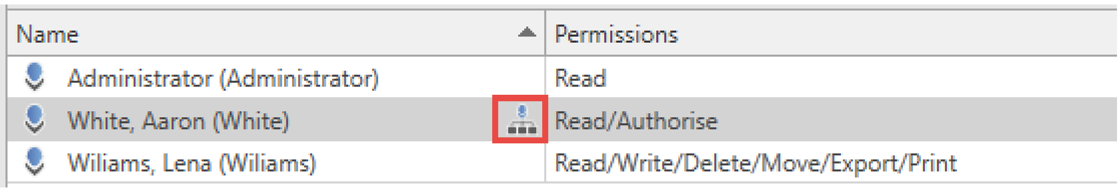


```
Corrupted Password: ScienceWireless
- ContainerItem with id: b0ae66e0-8a48-e811-80ed-005056ae08c4 irreparable
```

Settlement of reparable records

Damaged passwords are corrected automatically with the users / roles specified under ‘repairable with’ when logging on to the client or WebClient.

The right key can be checked using the form field permissions of password fields. If at least one user has the right key, the password can be fixed. In the following example, only the user ‘white’ has the right key and thus only this user can discover and correct the password.



Name	Permissions
Administrator (Administrator)	Read
White, Aaron (White)	Read/Authorise
Wiliams, Lena (Wiliams)	Read/Write/Delete/Move/Export/Print

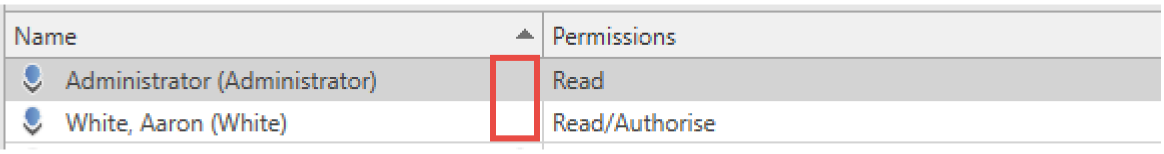
When logging on to the database via the client, a cleanup task is started automatically. This task always runs with the logged in user. In this case – as far as it is possible with the user – all affected passwords are corrected. Thus, when all users have logged in once, all affected passwords should be adjusted.

Irreparable records (not repairable)

Irreparable passwords cannot be corrected automatically. Nevertheless, it may happen that passwords marked as irreparably can be corrected manually.

First case

In the first case, no user / role has the right key on the password. Thus, no user can decrypt or correct the password.

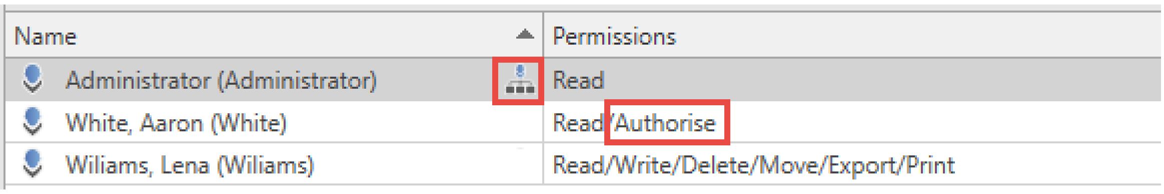


Name	Permissions
Administrator (Administrator)	Read
White, Aaron (White)	Read/Authorise

The affected passwords have to be recreated. For the security, a new database with an older backup can be included. From this database, the affected passwords / data can be taken over into the current database again.

Second case

In the second case, there are users / roles who have the right key but not the right to claim. As far as the number of irreparable passwords is limited, these can be used to check the form field permissions manually.



Name	Permissions
Administrator (Administrator)	Read
White, Aaron (White)	Read/Authorise
Wiliams, Lena (Wiliams)	Read/Write/Delete/Move/Export/Print

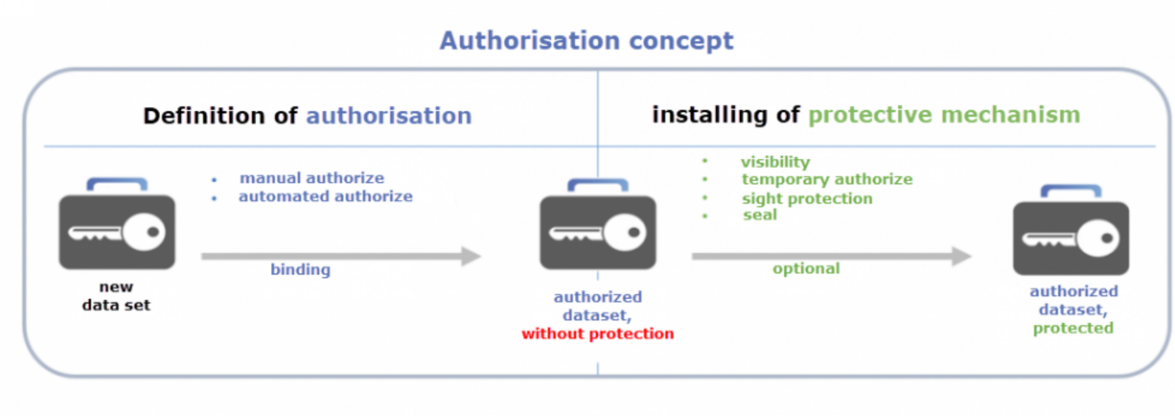
For the passwords concerned, the user with the legal key must be given the right of authorization temporarily to correct. If the corresponding user has the entitlement right, he can reset the legal key, either automatically when logging in or manually when saving the authorizations.

Authorization concept and protective mechanisms

What is the authorization concept?

The strength of Password Safe version 8 lies in the fact that it provides the right solution to all conceivable demands placed on it with regards to authorization management. In order to keep the manual work to a minimum, handling several users at once via roles is a tried-and-tested method. The setting of the permissions for these roles can either be completed manually or automatically. There are a number of variants for both options, which are explained in detail in the following sections.

Alongside the definition of manual and automatic setting of permissions, the (optional) setting of protective mechanisms forms part of the authorization concept. The protective mechanisms are thus downstream of the permissions. The interrelationships between all of these elements are illustrated in the following diagram.



✻ Applying some form of permissions is obligatory. Applying a protective mechanism is optional.

✻ The configuration of visibility is de facto a technical part of the permissions process. However, this mechanism has a “protective character” and is thus listed under protective mechanisms.

Before the manual and automatic setting of permissions and the possible protective mechanisms are covered in the next section, it is still necessary to explain the basic mechanics of the authorization concept here. These three cornerstones are irrevocable and always impact permissions of every type.

The three cornerstones of the authorization concept

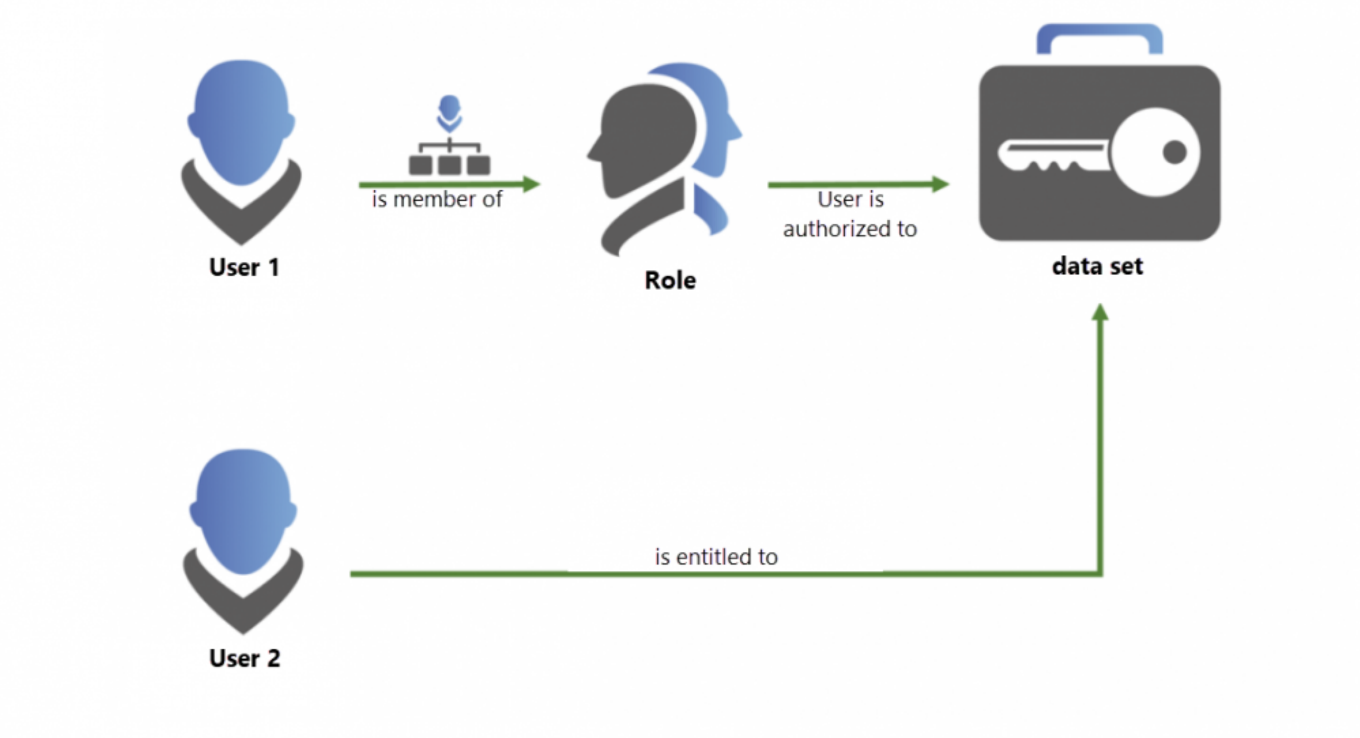
The reproduction of company-specific authorization structures can vary greatly in terms of effort. However, small working groups as well as international corporations are generally subject to the same rules with regard to administration in Password Safe. The basic concept is based on only a few rules which always apply without exception. Despite the innumerable individual adjustment screws, these basic rules can be summarized in three essential steps.

1. Permissions only for users or roles

If the authorization for a data record is to be defined, there are basically only two possibilities:

1. Authorization for a **user**
2. Authorization for a **role**

A role is technically nothing more than a summary of multiple users with the same permissions. It is, of course, a good idea to manage these roles in accordance with your company's activities. The role "Administrators" can therefore be provided with more extensive authorizations than, for example, the role "Sales Assistance". This role-based inheritance allows the organization to maintain the overview in a larger corporate structure as well as a simple procedure when adding new employees. Instead of having to entitle him individually, this is simply added to his role.

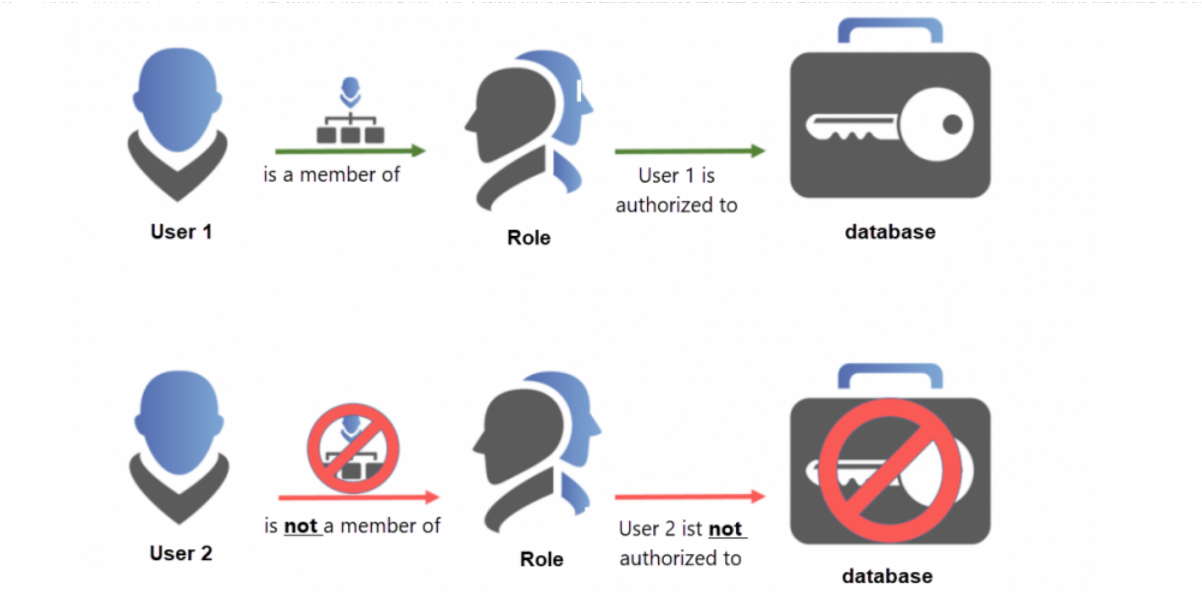


It is obvious to proceed with the organization of accesses using the concept of roles as a basis and only to grant rights individually to employees in exceptional cases. The unplanned absence of personnel must also be taken into account in such concepts. Working with roles defuses such risks significantly.

Permissions are always granted to only one user or role!

2. Membership in roles

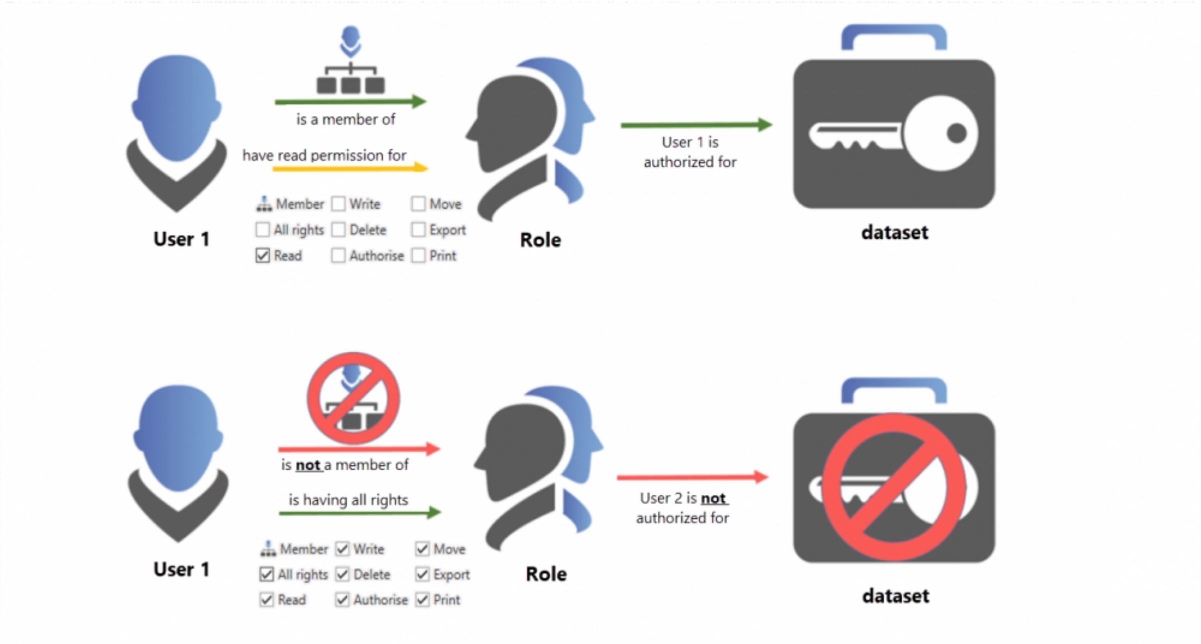
The key point is membership in a role. If an employee can use the authorizations according to the roles assigned to him, * he must be a member of the role *. Only members see the records that have been authorized for the role.



A small technical digression into the nature of the encryption can be very helpful with the basic understanding. Each role has a key pair. The first key is used to encrypt data. Access to this information is only possible with the second key. The membership in a role is equivalent to this second key.

3. Membership vs. permissions for roles

The admin user in Password Safe must pay particular attention to the interplay between users and roles. This dynamics is crucial for understanding the concept of authorization, in order to ensure maximum software adaptability to any corporate structure. The following diagram illustrates this with an example of two users.



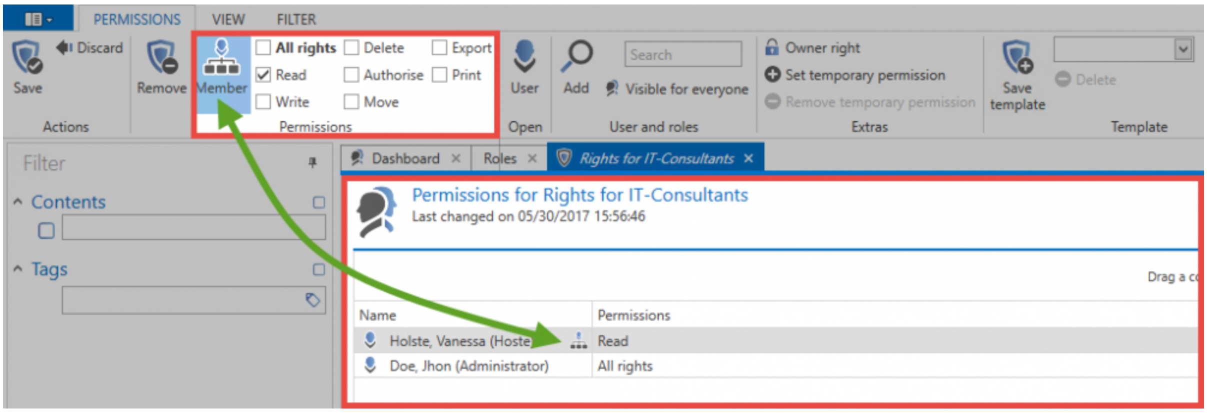
- **User 1** is a member of the role, and is therefore authorised for all records that are assigned to the role. However, it has only “read rights” for the role itself. This means, it can see the role, but cannot “Edit, move, or delete” it.
- **User 2** has all rights for the role. It can add additional users to the role by means of “authorise”. The crucial point, however, is that it is not a member of the role. It cannot, therefore, see any records for which the role is authorized.

In practice, the first user would be a classic user that is assigned, for example, to the Sales role by the administrators, and can view the records accordingly. The second user could be one of those administrators. This user has extensive rights for the role. It can edit it, and add users to it. However, it cannot see any data that is assigned to sales. It lacks membership in the role.

As a member of a role, it must have at least the “read” right for the role!

Specific example and configuration

Similar to the previous section (Membership vs. rights to roles)., the configuration of a role will be illustrated using two users. The configuration is performed in the Client Module Roles. By double-clicking on the role “IT-Consultants” in the list view, you can open their detailed view.

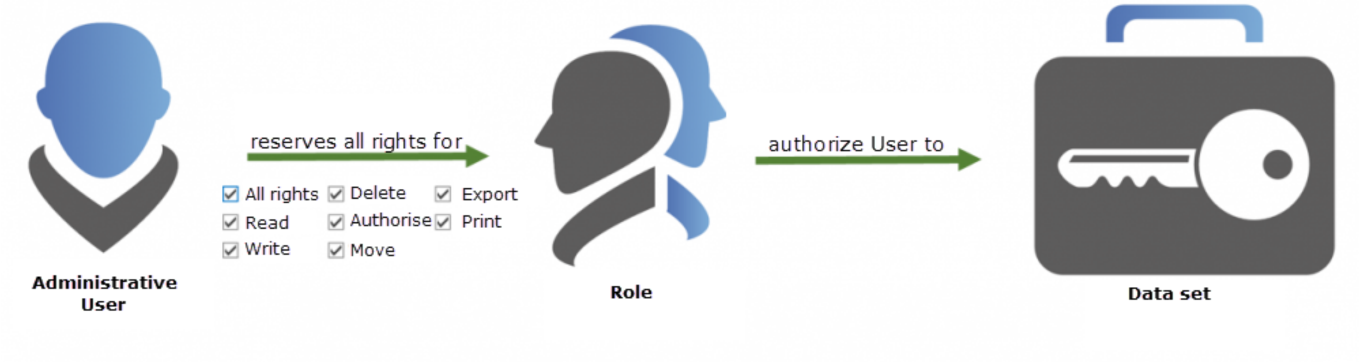


☐ All rights ☐ Delete ☐ Export
☑ Read ☐ Authorise ☐ Print
☐ Write ☐ Move

Permissions for Rights for IT-Consultants
Last changed on 05/30/2017 15:56:46

Name	Permissions
Holste, Vanessa (Hoste)	Read
Doe, Jhon (Administrator)	All rights

- The user “Holste” is a member of the role and can, therefore, access those records for which the role has permissions. He has the obligatory read right for the role, which is the basic requirement in order to be a member of the role. Which exact rights it has to the data record is not defined within the role! This is set out in the following section.
- The user “Administrator” has all rights to the role, but is not a member! Thus, it cannot see any records that are authorized for the role. However, it has all rights to the role and can therefore print, assign other users to the role, and delete them.



This example clearly shows the advantages of the concept. The complete separation of administrative users from regular users brings significant advantages. Of course, one does not necessarily exclude the other. An administrator can, of course, have full access to the role and also be a member in it! The boundaries between the two often overlap, and can be freely defined in Password Safe.

Manual setting of permissions

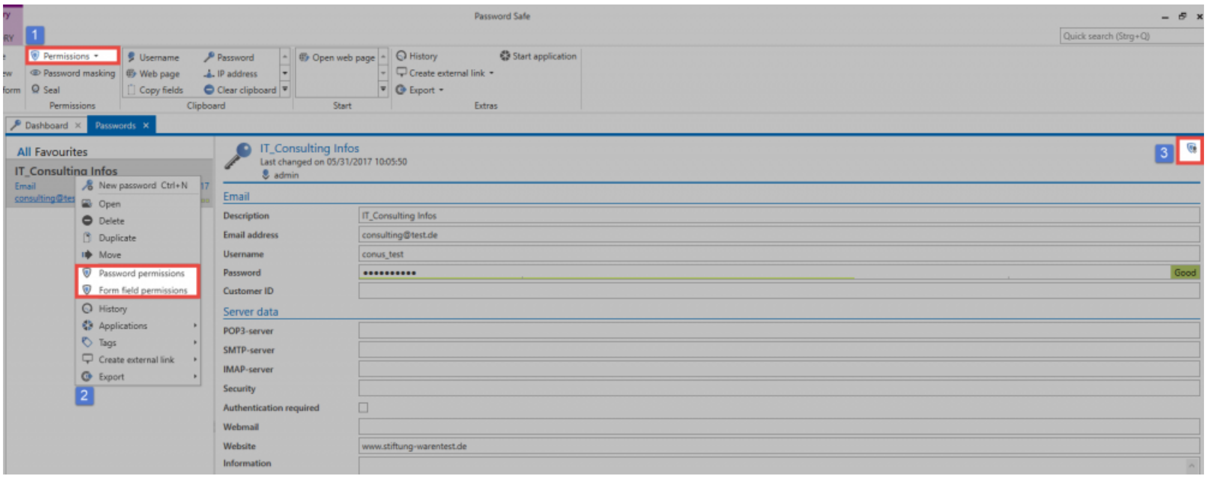
What is the manual setting of permissions for records?

In contrast to the automatic setting of permissions, the manual approach does not utilise any automatic processes. This method of setting permissions is thus carried out separately for every record – this process is thus not as recommended for newly created data. If you want to work effectively in the long term, the automatic setting of permissions for records should be used for creating passwords. However, the manual setting of permissions is generally used when editing already existing records.

Adding additional users with permissions

In the previous section, it was clarified that permissions for records are granted either directly to one user or to several users grouped in a role. With this knowledge, the permissions can as such be set manually for a record. In the Passwords client module, you can access the permissions in the list view of a record in three different ways:

1. Icon in the ribbon
2. Context menu of a data record (right-click)
3. Icon at the right edge of the reading pane



IT_Consulting Infos
Last changed on 05/31/2017 10:05:50
admin

Email

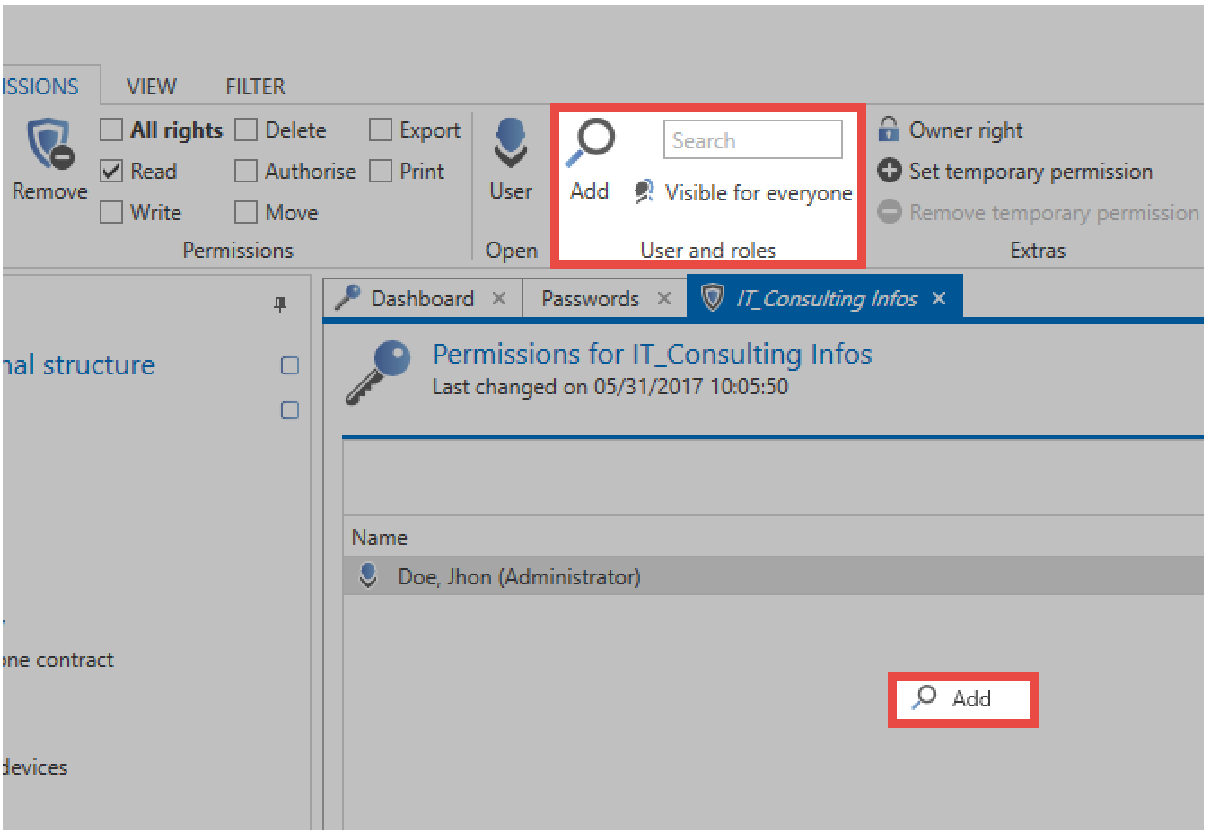
Description: IT_Consulting Infos
Email address: consulting@test.de
Username: conus_test
Password: ••••••••••
Customer ID:

Server data

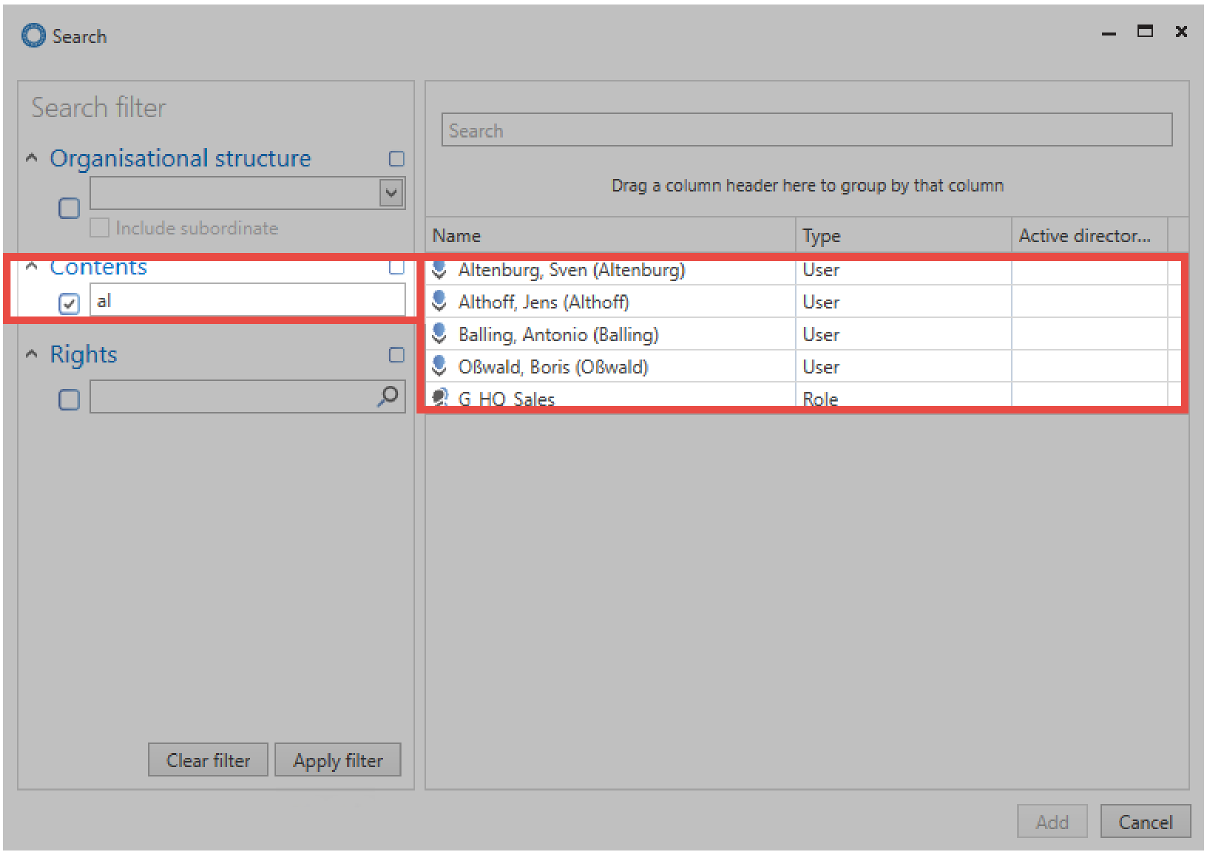
POP3-server:
SMTP-server:
IMAP-server:
Security:
Authentication required: □
Webmail:
Website: www.stiftung-warentest.de
Information:

The icon on the right of the reading pane reveals “mouseover” the information whether the record is personal or public. In case of personal data records, the user that is logged on is the only one who has permissions!

The author is created with all rights for the record. As described in the Authorization Concept, you can now add both roles and users. You can go to the search filter by right clicking on the tab or using the corresponding icon in the ribbon. The filter helps you to quickly find those users who should be granted permissions for the record in just a few steps.



The search filter opens in a separate tab. The filter can be configured as usual. The search is similar to the search in the list view.



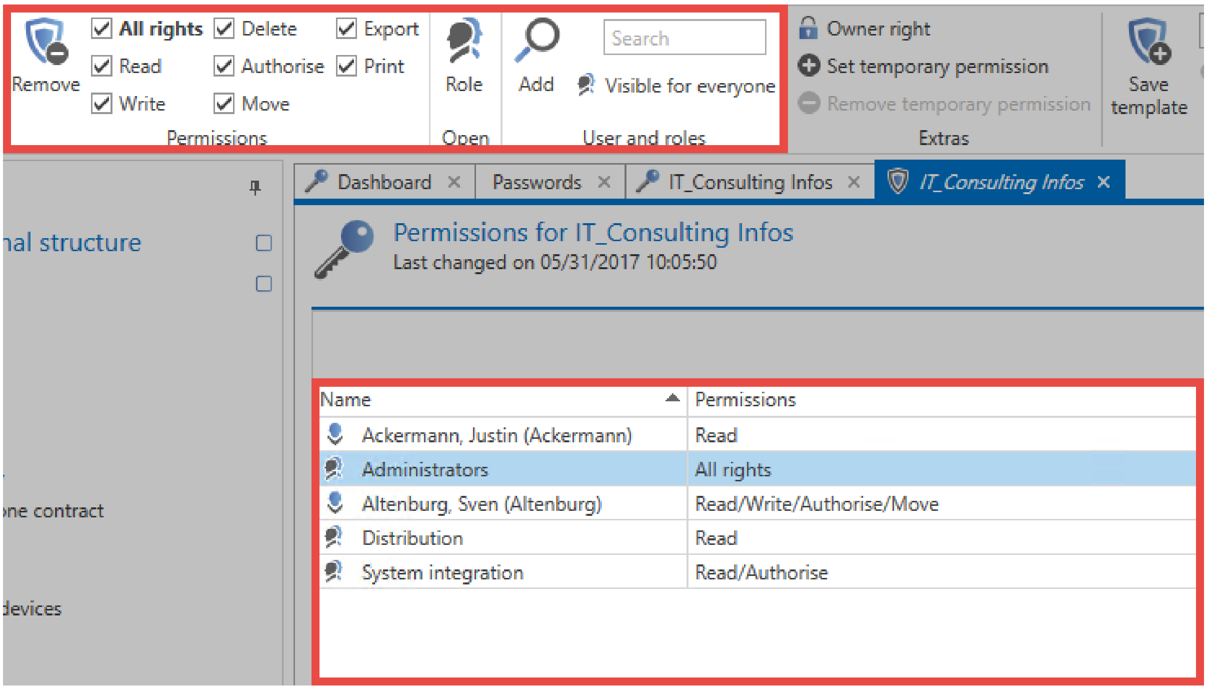
Contents
☑ al

Name	Type	Active director...
Altenburg, Sven (Altenburg)	User	
Althoff, Jens (Althoff)	User	
Balling, Antonio (Balling)	User	
Oßwald, Boris (Oßwald)	User	
G_HQ_Sales	Role	

The **multiple selection** is also enabled. It allows to add several users via the Windows standard Ctrl/ Shift + left mouse button.

Setting and removing permissions

By default, all added users or roles receive only the “Read” right on the record. It can be extended as required. You can add users as well as administrative roles using the available tools. The right “Read” right at the beginning is sufficient to view the fields of the data record and to use the password. Write permission allows you to edit a data record. * The right “Authorize” is necessary to authorize other users to the record *. This is also used as a basis for the configuration of the seal.



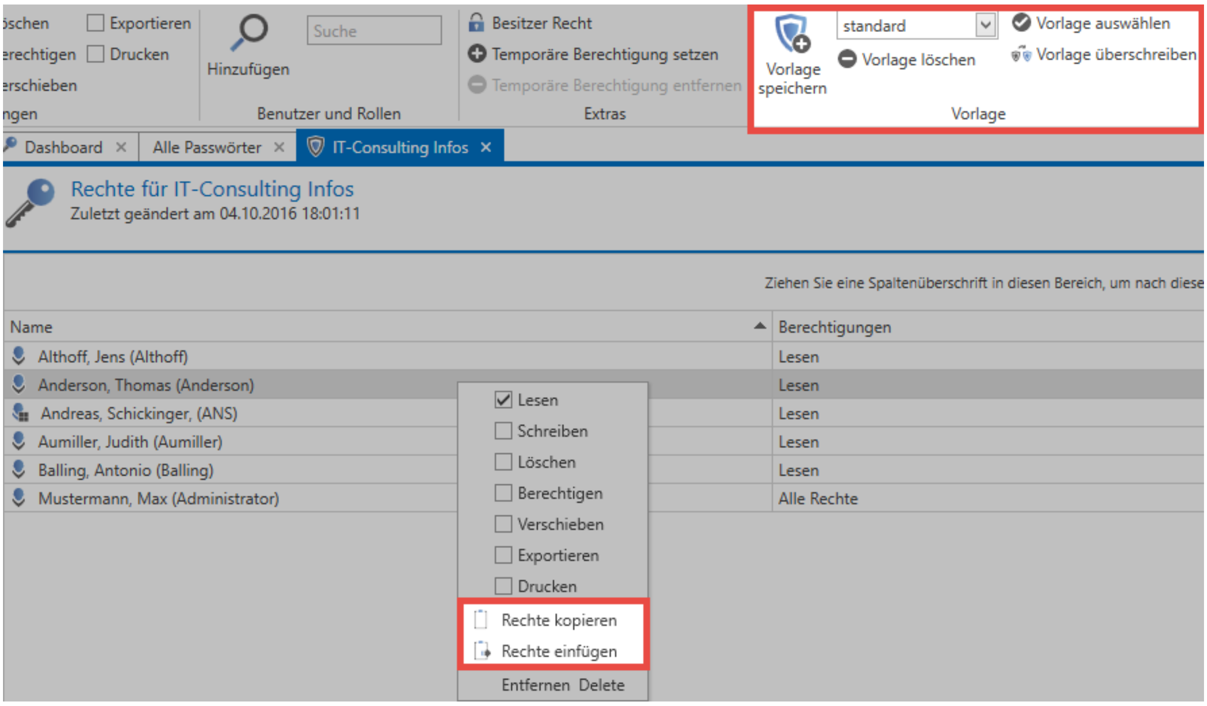
Permissions for IT_Consulting Infos

Last changed on 05/31/2017 10:05:50

Name	Permissions
Ackermann, Justin (Ackermann)	Read
Administrators	All rights
Altenburg, Sven (Altenburg)	Read/Write/Authorise/Move
Distribution	Read
System integration	Read/Authorise

Transferring rights

A simple right-click on a user can be used to copy and transfer rights configurations of users or roles to others in the context menu. In this context, the use of rights templates is also very practical. In the “Template” area of the ribbon, you can save configured permissions, including all users, and reuse them for other records.



Rechte für IT-Consulting Infos

Zuletzt geändert am 04.10.2016 18:01:11

Name	Berechtigungen
Althoff, Jens (Althoff)	Lesen
Anderson, Thomas (Anderson)	Lesen
Andreas, Schickinger, (ANS)	Lesen
Aumiller, Judith (Aumiller)	Lesen
Balling, Antonio (Balling)	Lesen
Mustermann, Max (Administrator)	Alle Rechte

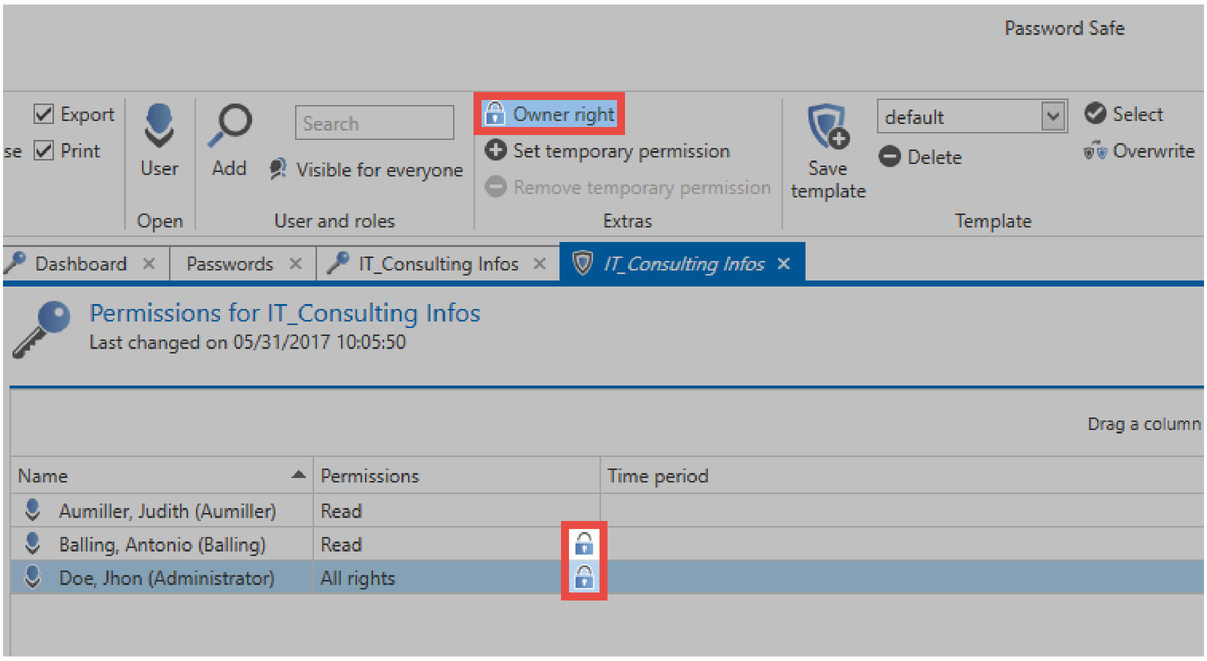
The transfer of rights and their reuse can be an important building block to create and maintain entitlement integrity. This method cannot rule out misconfigurations, but it will minimize the risk significantly. Of course, the correct configuration of these templates is a prerequisite.

The add right

The “add right” holds a special position in the authorization concept. This right controls whether a user/ role is permitted e.g. to create a new record within an organisational structure. Consequently, this right can only be set in the organisational structure module. More…

Owner right

The owner right may be made available to each user. These rights are more of **a guarantee**. Once assigned, there is no way to remove users or roles with the owner right from the permissions for a record. Only the user or the role itself can do that.



Permissions for IT_Consulting Infos
Last changed on 05/31/2017 10:05:50

Name	Permissions	Time period
Aumiller, Judith (Aumiller)	Read	
Balling, Antonio (Balling)	Read 🔒	
Doe, Jhon (Administrator)	All rights 🔒	

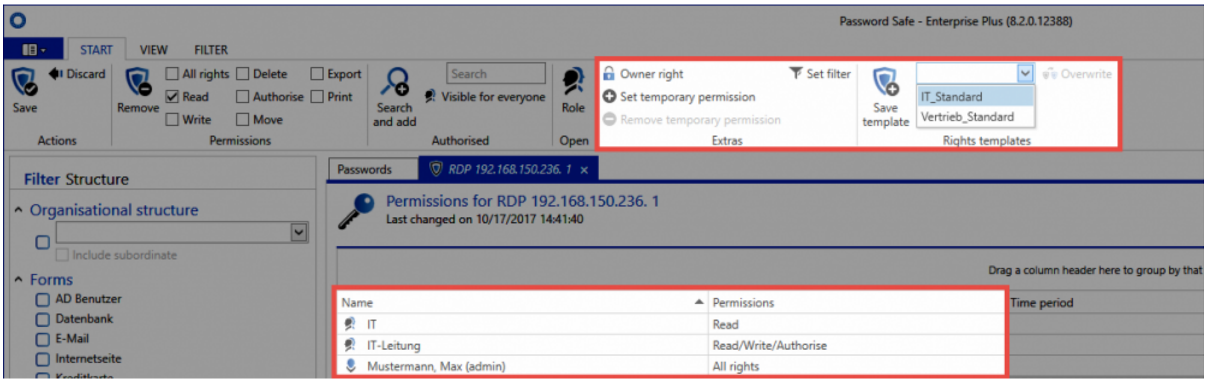
The owner right thus prevents other users who have the “Authorise” right from removing any users from the record.

! The owner right does not protect a record from being deleted. Any user who has deletion permission can delete the record!

Using rights templates

Using rights templates

Once they have been configured, permissions can be constantly reused. The functionality *Saving permissions as a template” in the ribbon is used for this purpose. The templates are globally available and can also be used for other records.



Permissions for RDP 192.168.150.236. 1
Last changed on 10/17/2017 14:41:40

Name	Permissions	Time period
IT	Read	
IT-Leitung	Read/Write/Authorise	
Mustermann, Max (admin)	All rights	

When saving templates, always select a name that will also allow it to be safely differentiated from other templates if you have a large number of rights templates.

Nevertheless, the use of rights templates merely reduces the amount of work and still envisages the manual setting of rights. Automatic process for the issuing of rights also exist in Password Safe and will be covered in the section Predefining rights and also under Inheritance from organisational structures.

Multiple editing of permissions

What is involved in the multiple editing of permissions?

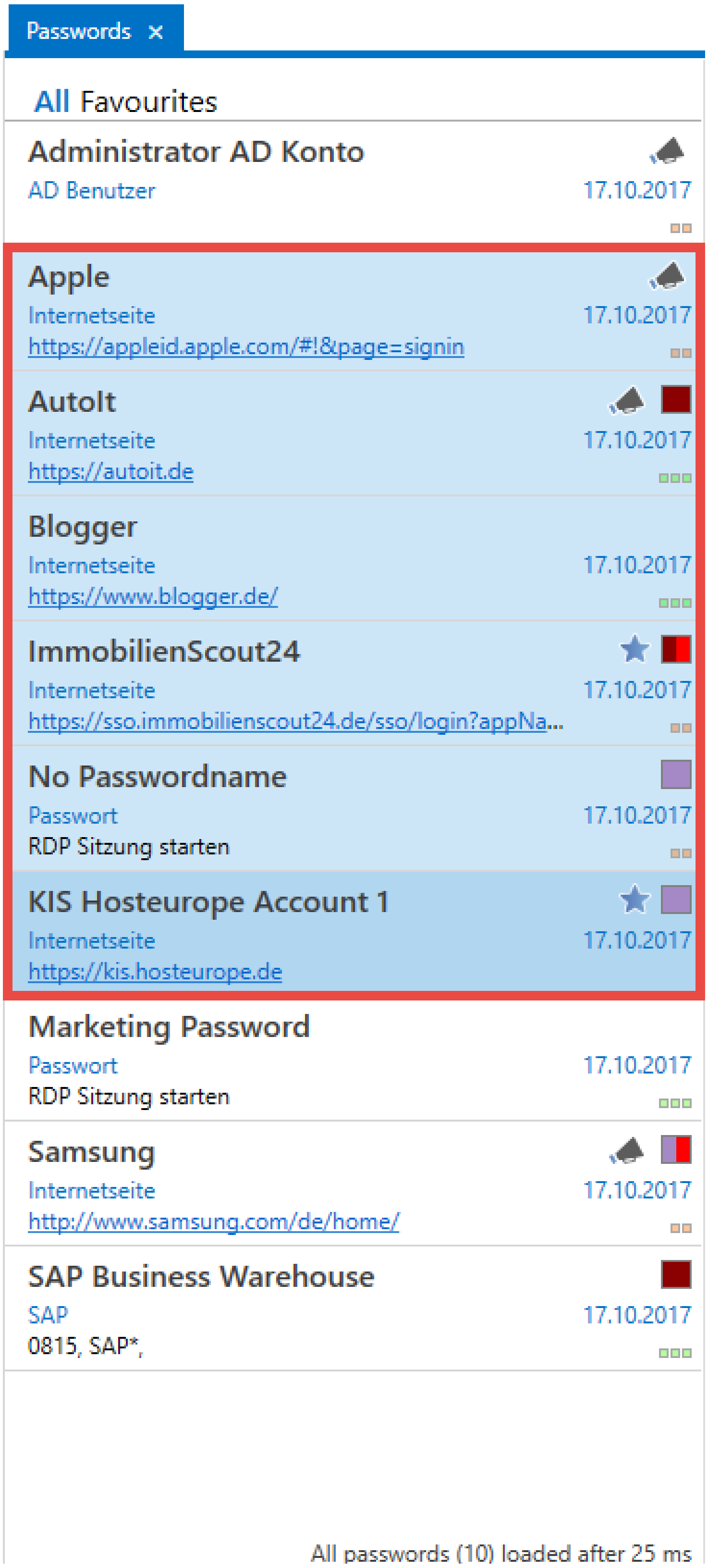
As part of the manual modification of permissions, it is also possible to edit multiple records at the same time. Various mechanisms can be used here to select the records to be edited. This could involve selecting the records in list view or also using the filter as part of the multiple editing function. Both scenarios are described below.

Multiple editing via list view

Individual rights can be supplemented or removed via **Multiple editing within list view**. The existing rights will **not be overwritten** here.

Selecting the records

In "list view ":#listenansicht, Shift or Ctrl + mouse click can be used to select multiple records. Permissions can also be granted for these records at the same time via the selection. The marked records are displayed in a different colour to usual. 6 records are marked in the following image.



Passwords ×

All Favourites

Administrator AD Konto
AD Benutzer 17.10.2017

Apple
Internetseite 17.10.2017
https://appleid.apple.com/#!&page=signin

AutoIt
Internetseite 17.10.2017
https://autoit.de

Blogger
Internetseite 17.10.2017
https://www.blogger.de/

ImmobilienScout24 ★
Internetseite 17.10.2017
https://sso.immobilienscout24.de/sso/login?appNa...

No Passwordname
Passwort 17.10.2017
RDP Sitzung starten

KIS Hosteurope Account 1 ★
Internetseite 17.10.2017
https://kis.hosteurope.de

Marketing Password
Passwort 17.10.2017
RDP Sitzung starten

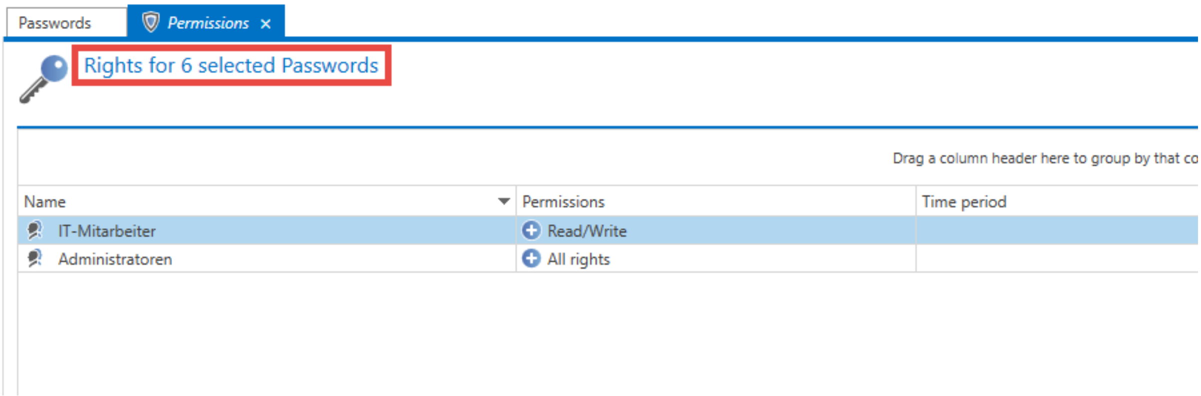
Samsung
Internetseite 17.10.2017
http://www.samsung.com/de/home/

SAP Business Warehouse
SAP 17.10.2017
0815, SAP*,

All passwords (10) loaded after 25 ms

Dialogue for configuring the rights

A new tab will be opened in the ribbon above the **Permissions** button in which the rights to be granted can be configured. The tab will display the number of records that will be affected by the defined changes.



Rights for 6 selected Passwords

Drag a column header here to group by that co

Name	Permissions	Time period
IT-Mitarbeiter	⊕ Read/Write	
Administratoren	⊕ All rights	

> As the already granted rights for the selected records may differ, it is not possible to display the rights here.

Adding rights

To add a right, a user or role is selected first in the ribbon under **Search and add** or **Search**. The permissions are then selected as usual in the ribbon. The ⊕ symbol indicates that right will be added. In the following example, Mr. Steiner receives read rights to all selected records. In contrast, Mr. Brewery receives all rights.

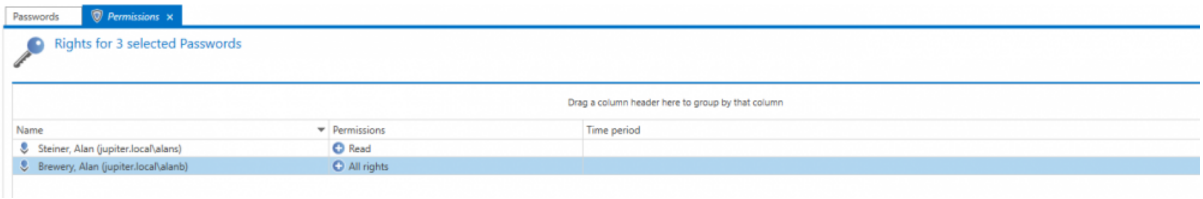
Reducing rights / removing users and roles from the permissions

If you want to remove rights, it is also necessary to firstly add the user or the desired role to be edited. Clicking on **Reduce rights** now means that rights will be removed. This is indicated by the ⊖ symbol. The rights to be removed are then selected.

> If the **read** right is to be removed for a user or role, the user will be completely removed from the permissions.

Examples

In the following example, Mr. Steiner receives read rights to all selected records. In contrast, Mr. Brewery receives all rights:

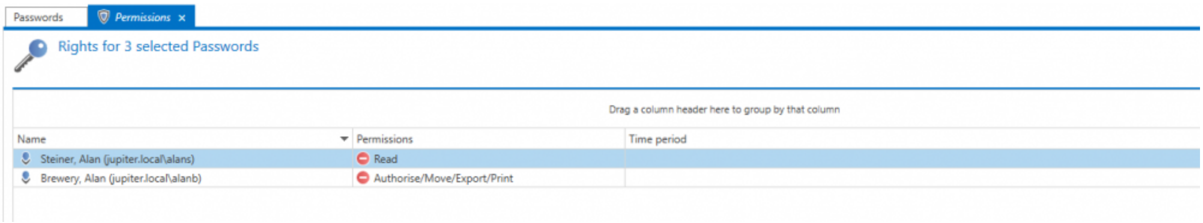


Rights for 3 selected Passwords

Drag a column header here to group by that column

Name	Permissions	Time period
Steiner, Alan (jupiter.local\alans)	⊕ Read	
Brewery, Alan (jupiter.local\alanb)	⊕ All rights	

The read right will be removed here for Mr. Steiner. As removing the read right means that no other rights exist for the record, Mr. Steiner is completely removed from the permissions. The authorize, move, export and print rights are being removed from Mr. Brewery. Assuming that he previously had all rights, he will then have read, write and delete rights remaining:



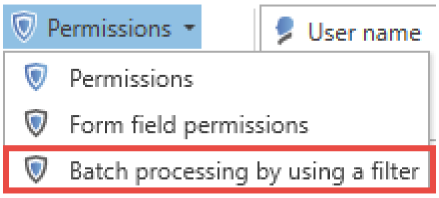
Rights for 3 selected Passwords

Drag a column header here to group by that column

Name	Permissions	Time period
Steiner, Alan (jupiter.local\alans)	⊖ Read	
Brewery, Alan (jupiter.local\alanb)	⊖ Authorise/Move/Export/Print	

Batch processing using a filter

In some cases it is necessary to edit the permissions for a very large number of records. On the one hand, a maximum limit of 1000 records exists and on the other had, handling a very large number of records via list view is not always the best solution. The **Batch processing using a filter** mode has been developed for this purpose. This is directly initiated via the ribbon.

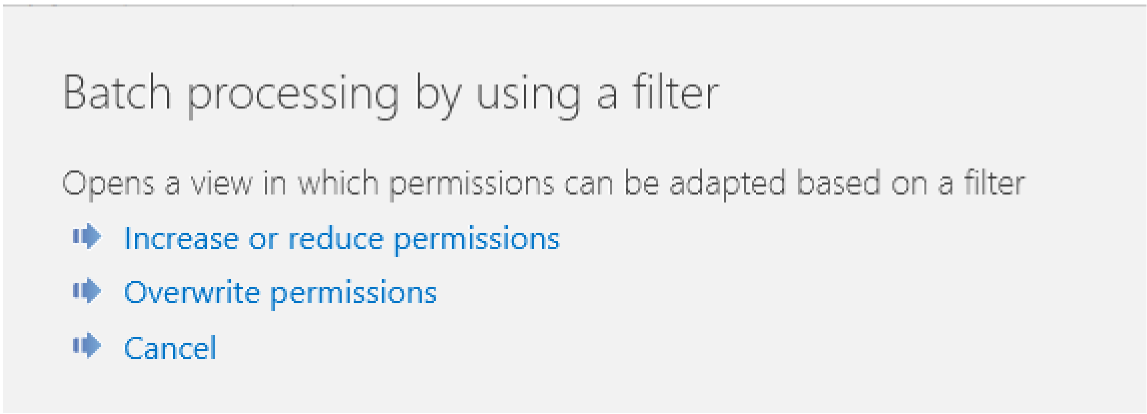


In the subsequent dialogue, you define whether you want to expand, reduce or completely overwrite existing permissions. If you select **expand or reduce** at this stage, the same logic as for **editing via list view** is used. No rights will thus be overwritten.

In the option **overwrite permissions**, the existing rights are firstly removed and then replaced by the newly defined rights.

! It is important to proceed with great caution when overwriting rights because this function can quickly lead to a large number of records becoming unusable.

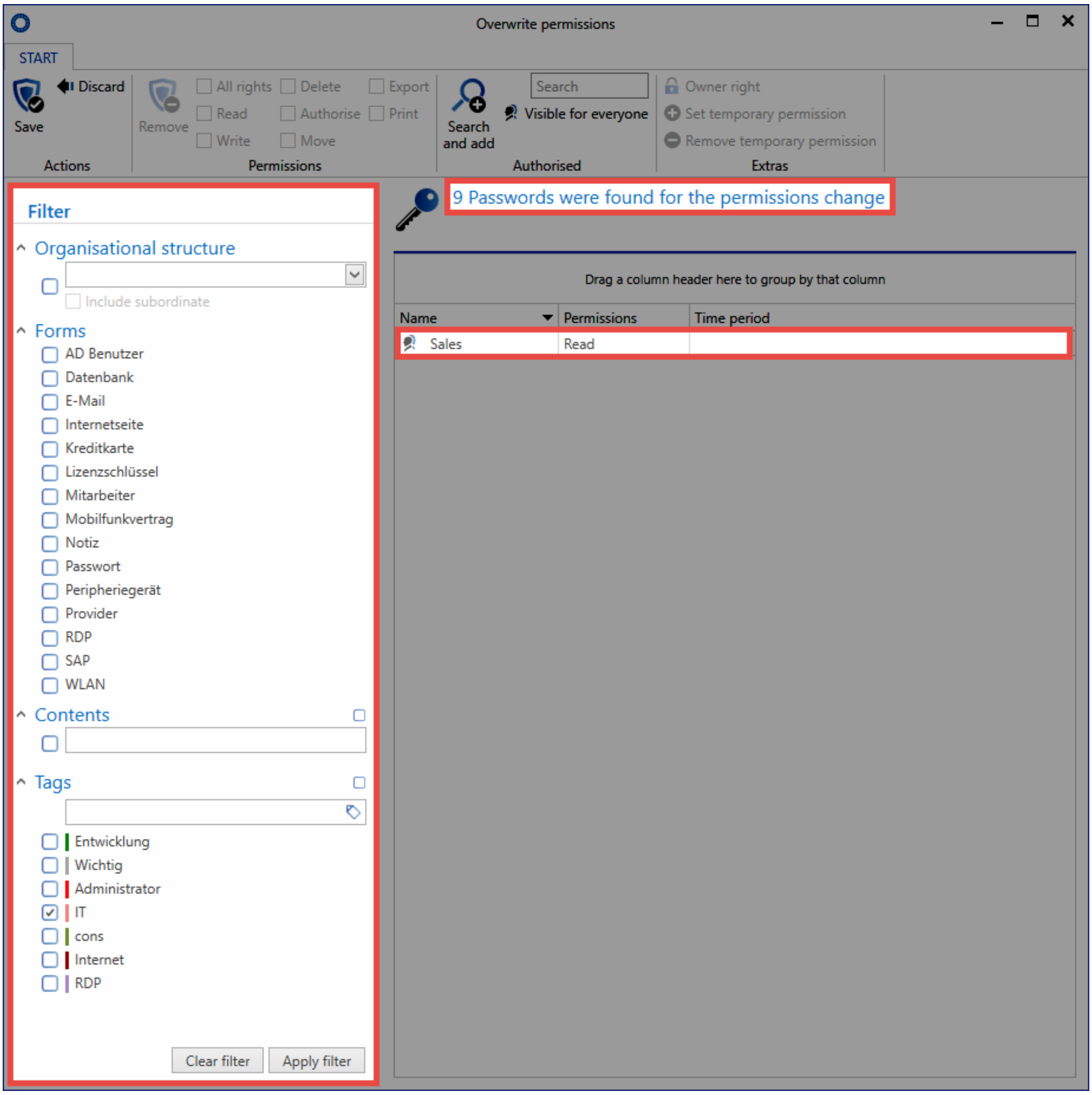
✻ This mode is inactive by default and must firstly be activated using the right **Can carry out batch processing of permissions using a filter**.



Batch processing by using a filter

Opens a view in which permissions can be adapted based on a filter

The filter itself defines the selection criteria for the records to be edited. The currently configured filter will be used as default. The records that will be affected by the changes are also not displayed in this view. Only the number of records is displayed. In the following example, 9 passwords are being edited to give the role “Sales” the read right.



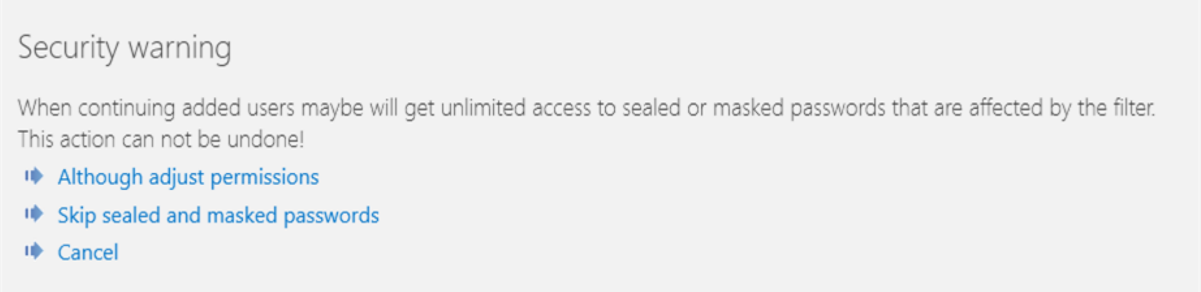
Tags: ☑ IT

9 Passwords were found for the permissions change

Name	Permissions	Time period
Sales	Read	

Seals and password masking

Sealed or masked records cannot be edited using batch processing. If these types of password are selected, a dialogue will be displayed when carrying out batch processing to inquire how these records should be handled.

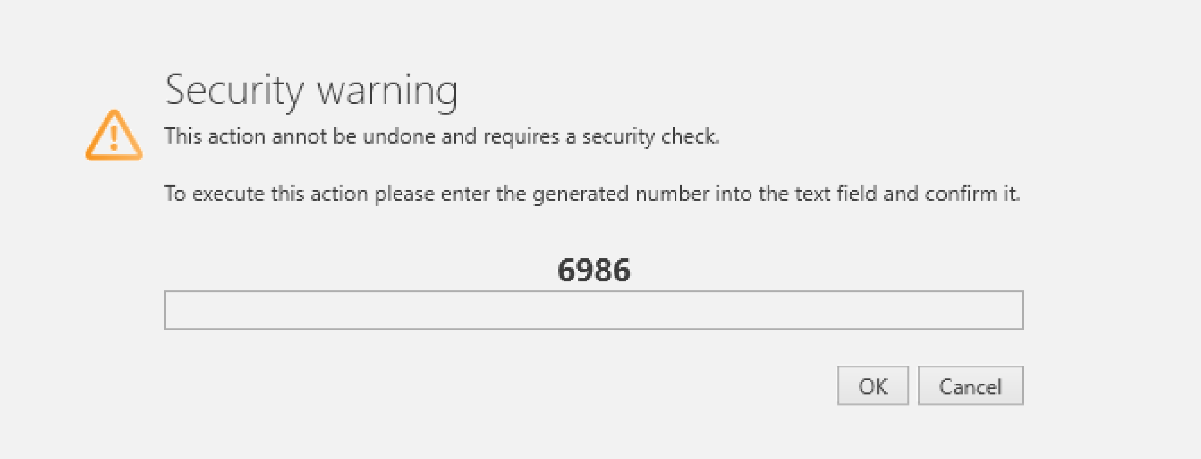


Security warning

When continuing added users maybe will get unlimited access to sealed or masked passwords that are affected by the filter. This action can not be undone!

- Although adjust permissions
- Skip sealed and masked passwords
- Cancel

It is possible to select whether the affected records are skipped or whether the seal or password masking should be removed. If the **remove** option is selected, the process needs to be confirmed again by entering a PIN.



Security warning

This action annot be undone and requires a security check.

To execute this action please enter the generated number into the text field and confirm it.

6986

! The removal of seals and password masking cannot be reversed!

Depending on the number of records, editing records may take a long time. This process is carried out in the background for this reason. A hint will indicate that the permissions process has been completed.

Automated setting of permissions

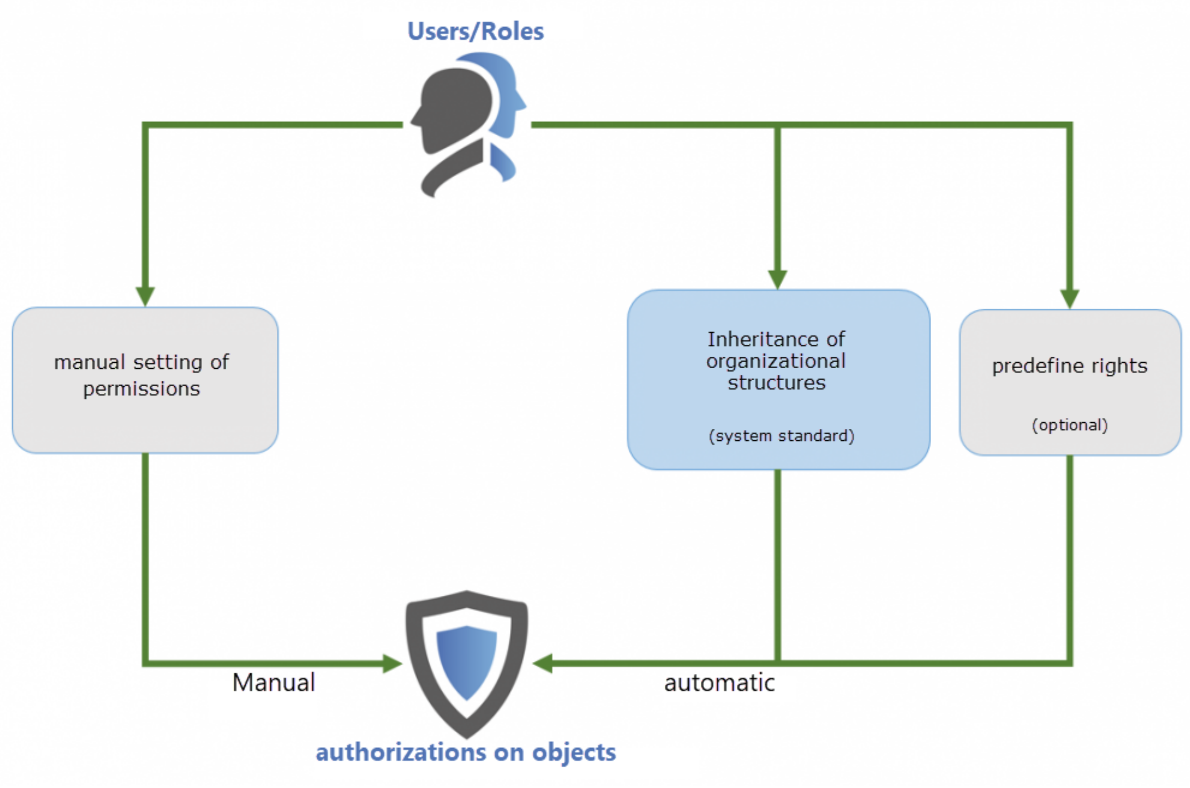
Reusing permissions

Password Safe generally differentiates between multiple methods for setting permissions:

1. Manual setting of permissions
2. Inheritance of permissions within organisational structures
3. Using predefined rights

- In the manual setting of permissions, the desired permissions are directly configured for each record. Automatic processes and inheritance are **not** used in this case.
- Both the use of predefined rights and also the inheritance from organisational structures are based on the **automated reuse** of already granted permissions according to previously defined rules.

The following diagram deals with the question: **How do users or roles receive the intended permissions?**

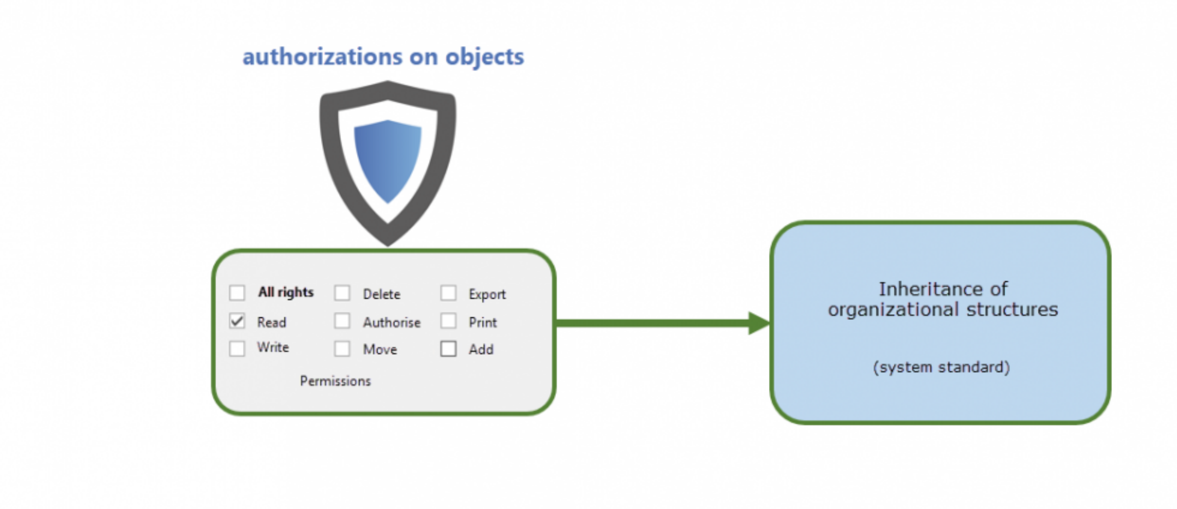

Users/Roles
manual setting of permissions
Inheritance of organizational structures
(system standard)
predefine rights
(optional)
Manual
automatic
authorizations on objects

Inheritance from organisational structures is defined by **default** in the system. This can be configured in the settings. The relevant setting is “Inherit permissions for new objects (without rights template)”. “Further info…”:#vererbung-aus-organisationsstrukturen

Inheritance from organisational structures

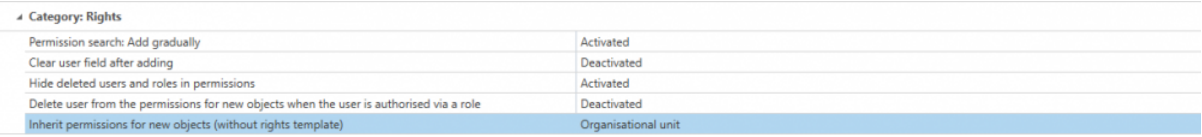
Organisational structures as a basis

The aim of organisational structures is collect together and reflect the hierarchies and dependencies amongst employees that exist in a company. Permissions are granted to these structures as usual via the ribbon. Further information on this subject can be found in the section “Permissions for organisational structures”. As a specific authorization concept is generally used within organisational structures, this is also used as the basis for further permissions. This form of inheritance is technically equivalent to granting rights based on **affiliations to a folder**. When creating a new record, the record receives the permissions in accordance with the defined permissions for the organisational unit.



Relevant user settings

Whether this form of inheritance should be applied is defined via the settings in the ribbon. The relevant setting is “Inherit permissions for new objects (without rights template)”.



Category: Rights	
Permission search: Add gradually	Activated
Clear user field after adding	Deactivated
Hide deleted users and roles in permissions	Activated
Delete user from the permissions for new objects when the user is authorised via a role	Deactivated
Inherit permissions for new objects (without rights template)	Organisational unit

Possible values

- **Off**: Permissions from OUs are not inherited
- **Organisational unit**: When creating new objects, permissions are set in accordance with the defined rights for the target organisational unit.

- **Organisational unit and user**: As well as inheriting permissions for organisation units, the configured permissions for the user are now also inherited when creating private records.

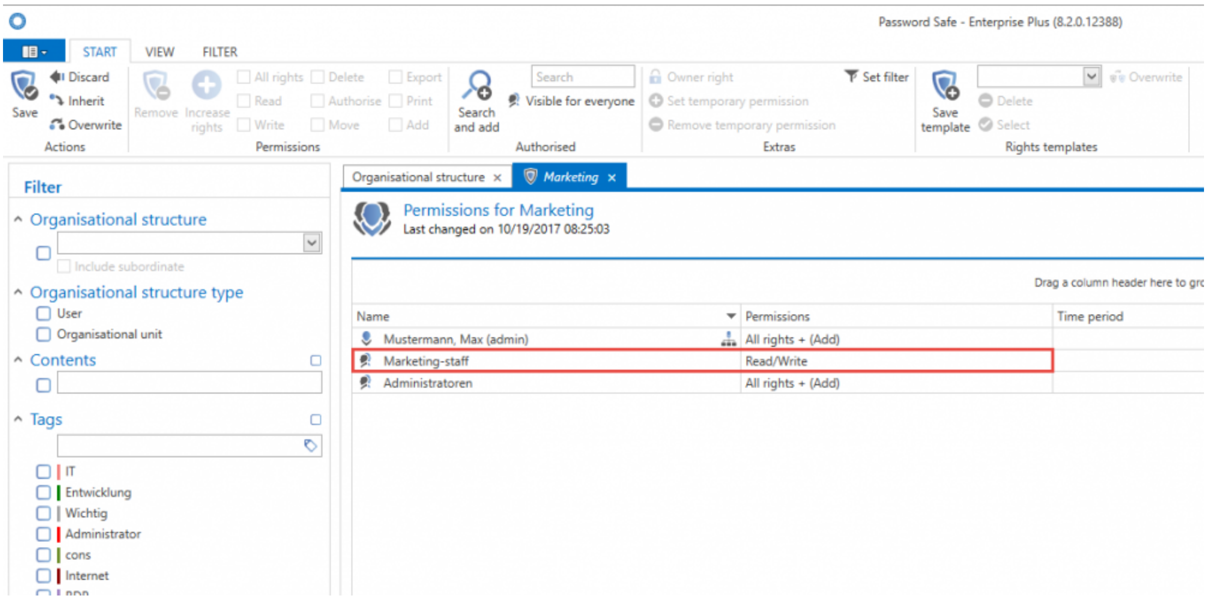
> If inheritance for the users is also activated, the creation of private records is in itself no longer possible. When creating new records to be saved in the organisational unit for the logged-in user, the permissions for the record are now granted in accordance with the permissions for the user.

> ! If a predefined right exists, this will always overwrite inherited permissions from organisational structures

Example case

This example shows the creation of a new record in the organisational structure “marketing”. It is defined in the settings for the stated organisational structure that permissions should be inherited by new objects in accordance with the organisational structure.

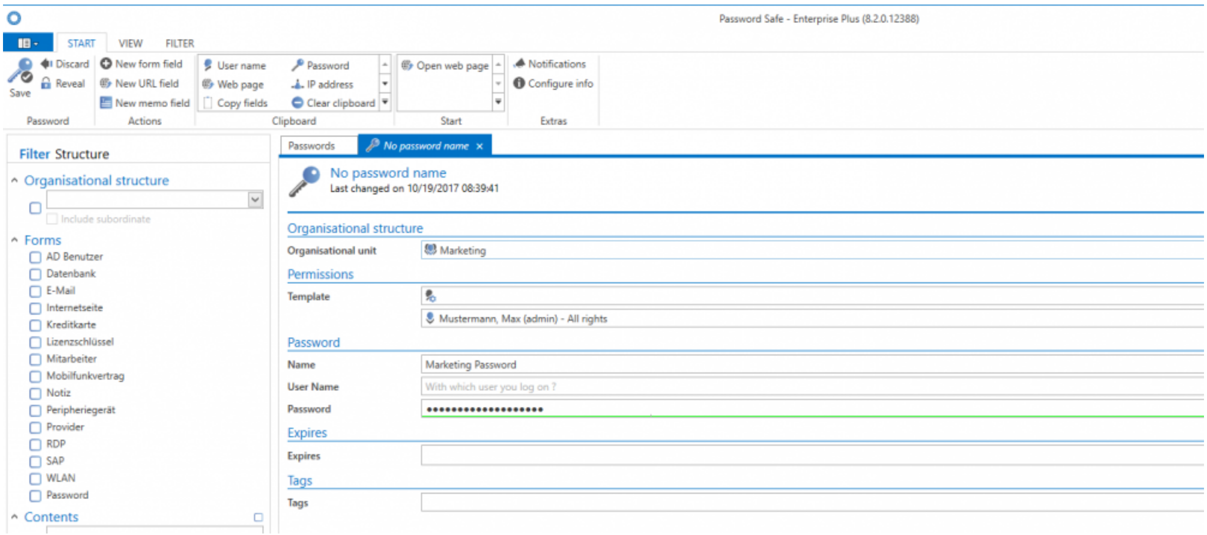
The permissions for the organisational unit “marketing” are shown below:



Permissions for Marketing
Last changed on 10/19/2017 08:25:03

Name	Permissions	Time period
Mustermann, Max (admin)	All rights + (Add)	
Marketing-staff	Read/Write	
Administratoren	All rights + (Add)	

A new password is now created in the organisational unit “marketing”.



No password name
Last changed on 10/19/2017 08:39:41

Organisational structure

Organisational unit: Marketing

Permissions

Template:
Mustermann, Max (admin) - All rights

Password

Name: Marketing Password

User Name: With which user you log on ?

Password: •••••••••••••••••••

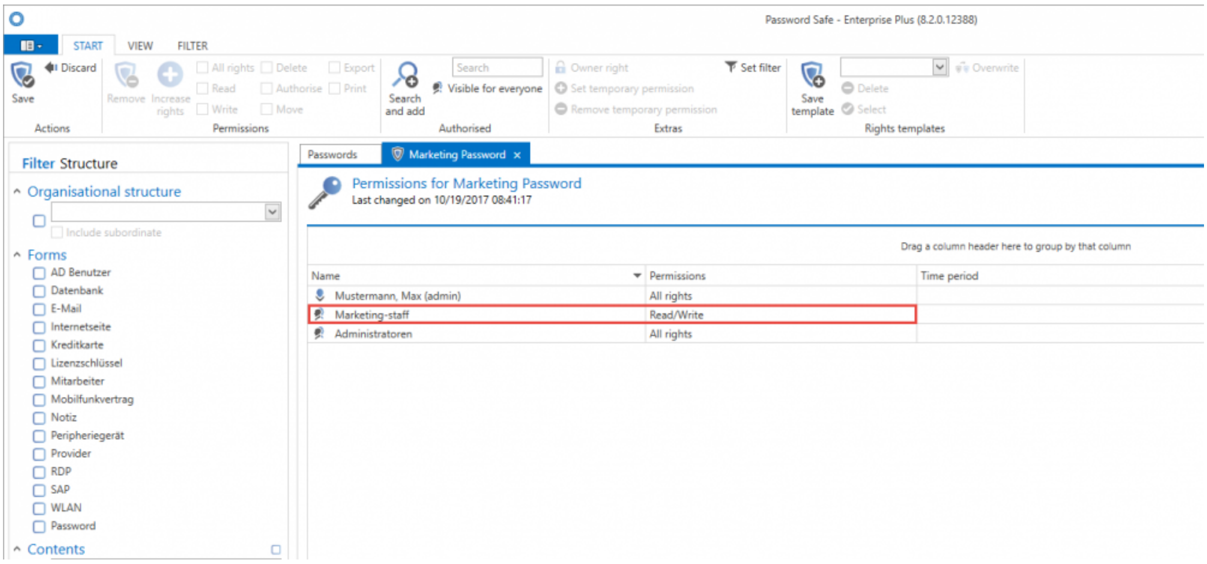
Expires

Expires:

Tags

Tags:

It is important that **no** preset is defined for this organisational unit. The permissions for the record just created are now shown.



Permissions for Marketing Password
Last changed on 10/19/2017 08:41:17

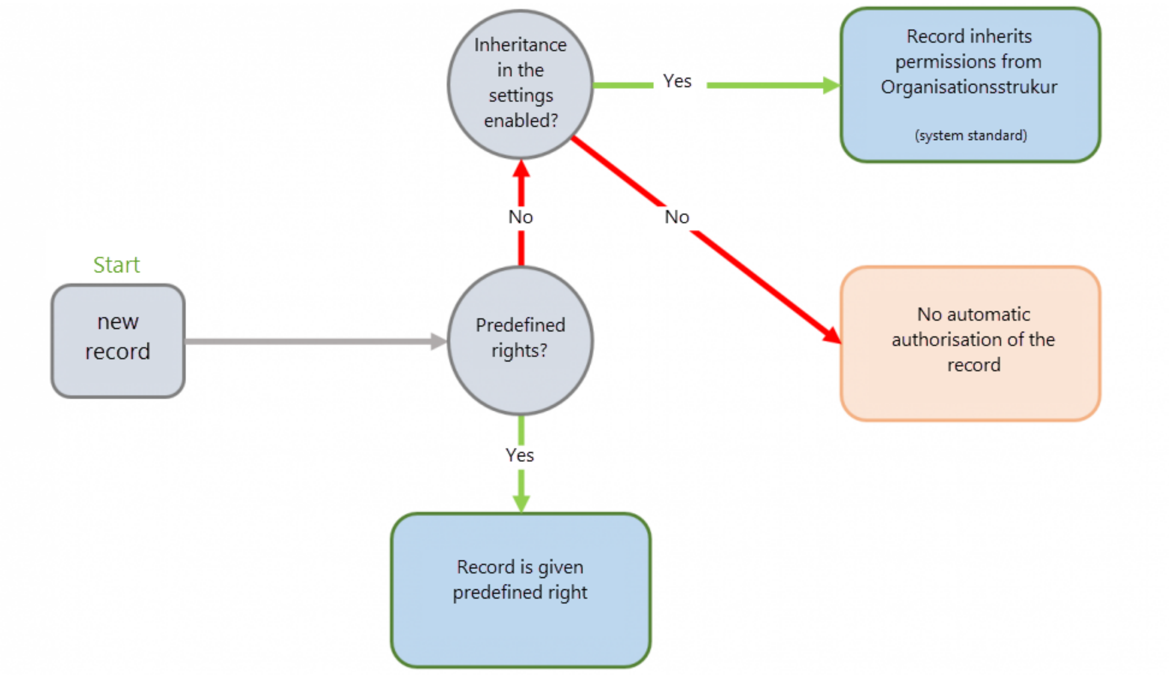
Name	Permissions	Time period
Mustermann, Max (admin)	All rights	
Marketing-staff	Read/Write	
Administratoren	All rights	

Conclusion

The permissions for the “storage location” are simply used when creating new objects. Two conditions apply here:

1. The value “organisational unit” must be selected in the settings for the inheritance of permissions
2. There must be no predefined right for the affected organisational structure

This process is illustrated in the following diagram:


Start
new record
Predefined rights?
No
Inheritance in the settings enabled?
Yes
Record inherits permissions from Organisationsstrukur
(system standard)
No
No automatic authorisation of the record
Yes
Record is given predefined right

Predefining rights

What are predefined rights?

Setting permissions for records can naturally be carried out separately for every record. Although this method enables you to very closely control every intended permission structure, it is not really efficient. On the one hand, there is too much configuration work involved, while on the other hand, there is a danger that people who should also receive permissions to access data are forgotten. In addition, there is the fact that many users should not even have the right to set permissions. “Predefining rights” is a suitable method to simplify the issuing of permissions and reduce error rates by using automated processes. This page covers the configuration of predefined rights, please also refer to the sections Working with predefined rights and their Scope of validity.

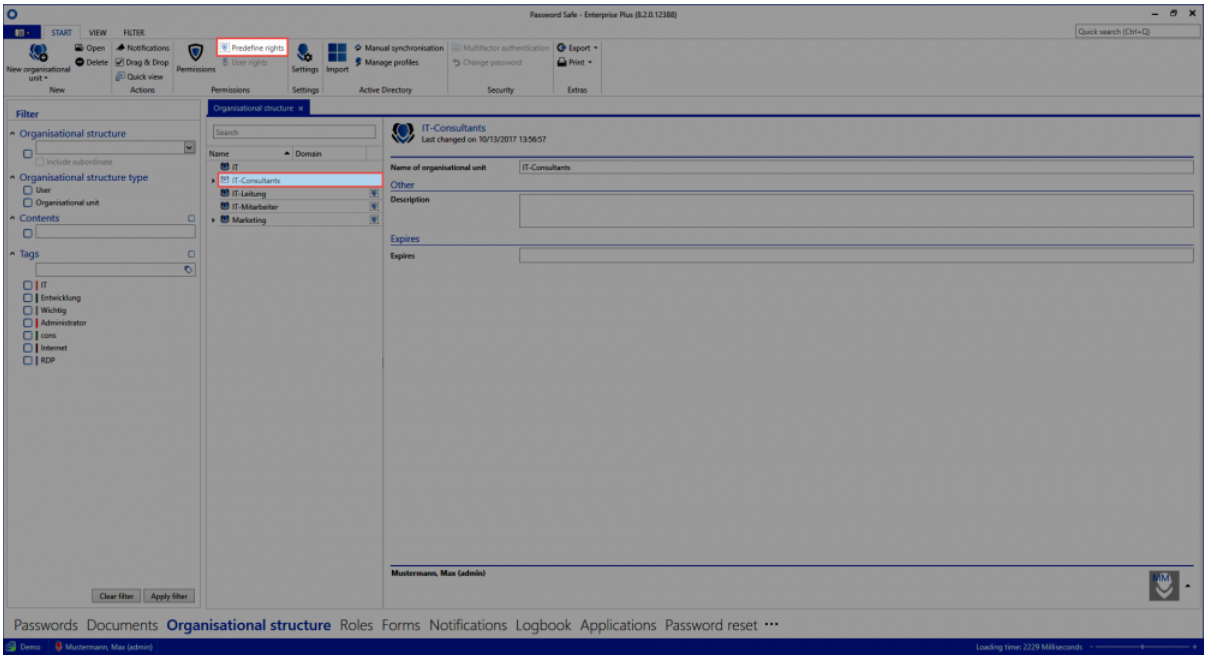
Organisational structures as a basis

Organisational structures can be very useful in many areas in Password Safe. In this example, they provide the basic framework for the automated granting of rights. In the broadest sense, these organisational structures should always be entered in accordance with existing departments in a company. The following example specifically focuses on an IT department. The following 3 hierarchies (roles) have been defined within this IT department:

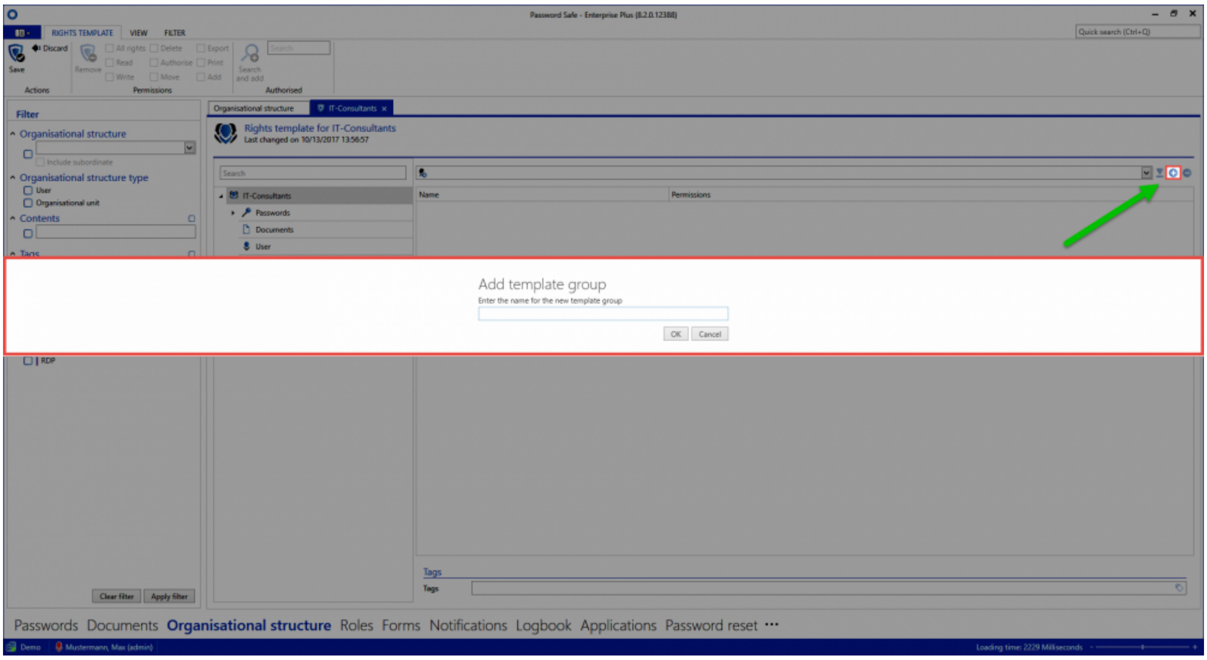
- **IT employee**
- **IT manager**
- **Administrator**

Predefining rights

In general, a more senior, managerial employee is granted more extensive rights than those granted to a trainee. This hierarchy and the associated permission structures can be predefined. In the organisational structure module, we now select those OUs (departments) for which rights should be predefined and select *predefine rights” in the ribbon.


Password Safe - Enterprise Plus (8.2.0.12388)
START
VIEW
FILTER
Predefine rights
User rights
Organisational structure
Filter
IT-Consultants
Last changed on 10/13/2017 13:56:57
Name of organisational unit
IT-Consultants
Other
Description
Expires
IT
IT-Consultants
IT-Leitung
IT-Mitarbeiter
Marketing
Passwords Documents Organisational structure Roles Forms Notifications Logbook Applications Password reset ···

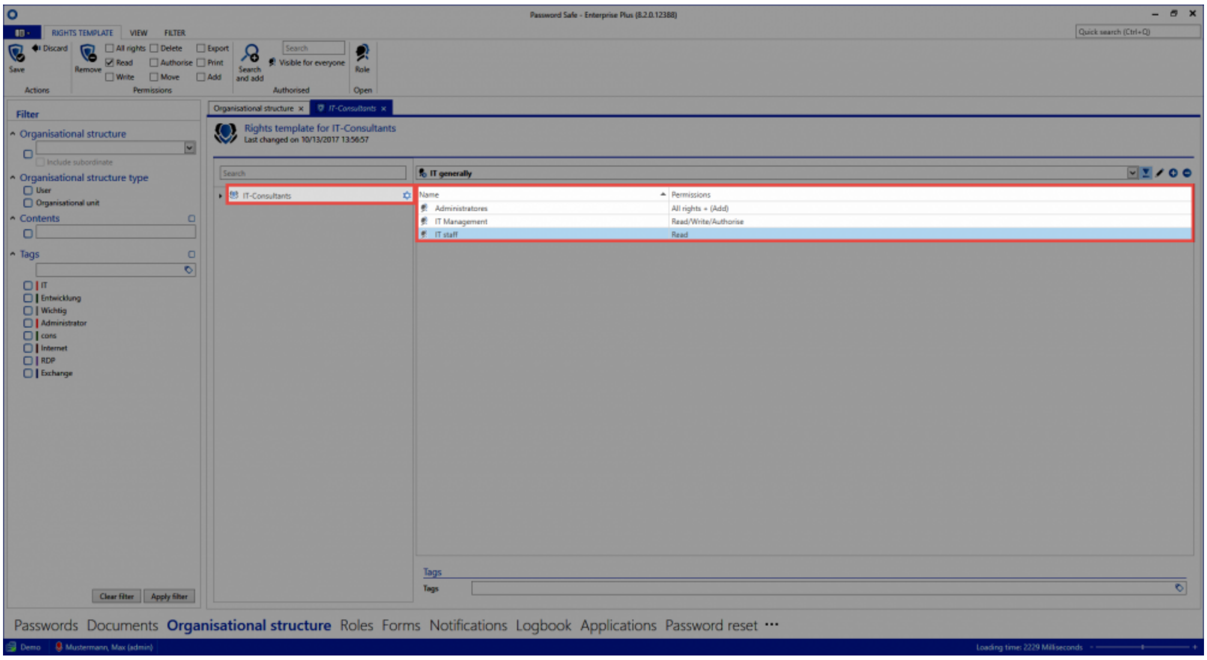
- **Creating the first template group:** A modal window will appear after clicking on the icon for adding a new template group (green arrow) in which a meaningful name for the template group should be entered.


Password Safe - Enterprise Plus (8.2.0.12388)
RIGHTS TEMPLATE
VIEW
FILTER
Save
Discard
Organisational structure
IT-Consultants
Rights template for IT-Consultants
Last changed on 10/13/2017 13:56:57
IT-Consultants
Passwords
Documents
User
Name
Permissions
OK
Cancel
Passwords Documents Organisational structure Roles Forms Notifications Logbook Applications Password reset ···

Add template group

Enter the name for the new template group

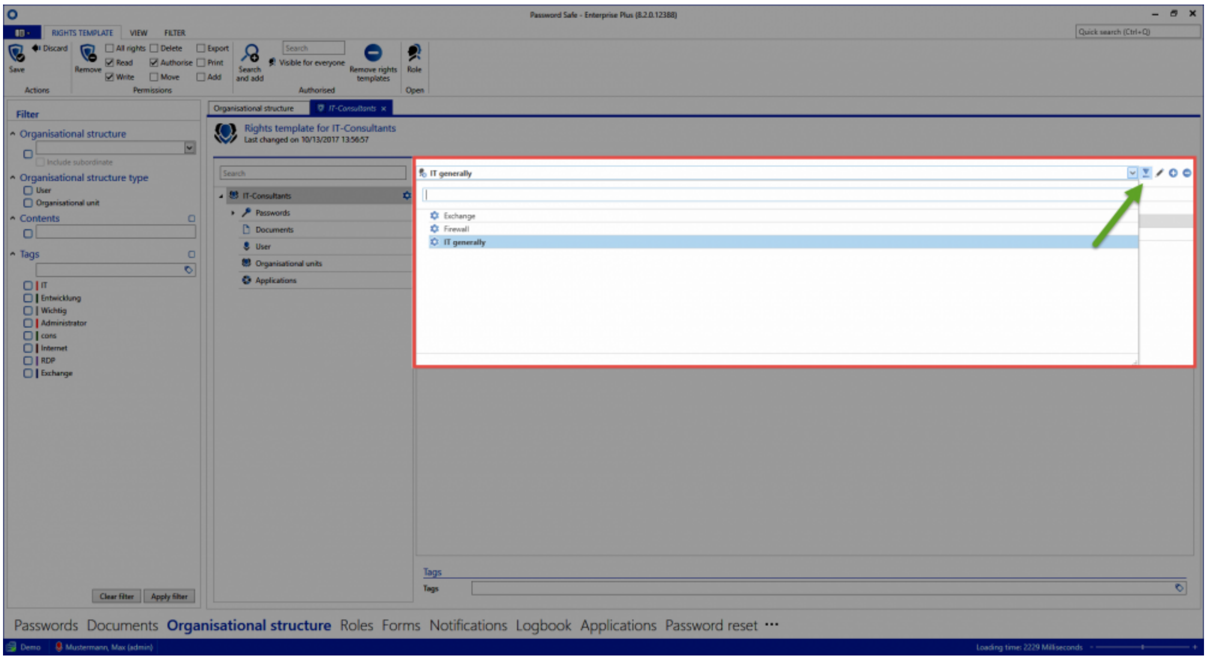
Roles and users can now be added to this template both via the ribbon and also via the context menu (right mouse click). This was already completed in the next step. The role **IT employee** only has read rights, the **IT manager** also has write rights and the capability of managing permissions. **Administrators** possess all available rights. Configuration of the rights structures is explained in the appropriate section.



Name	Permissions
Administratores	All rights + (Add)
IT Management	Read/Write/Authorise
IT staff	Read

Adding other template groups

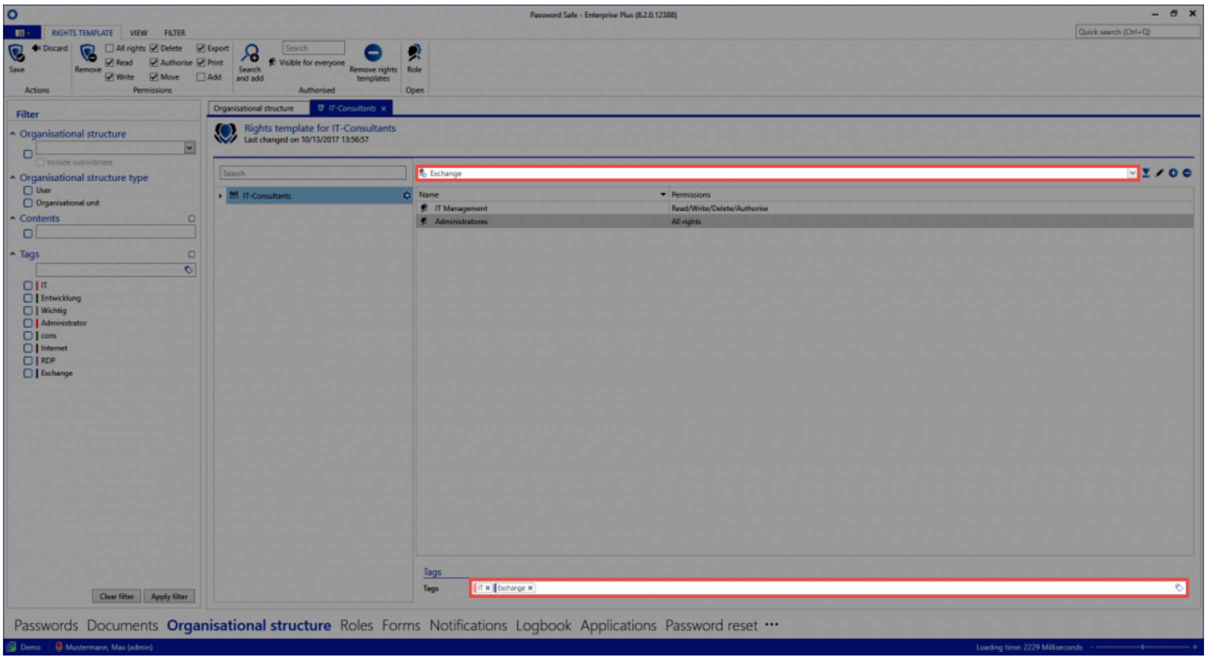
It is also possible to configure several different rights templates within one department. This may be necessary e.g. if there are several areas of competency within one department which should each receive different permissions. Alongside the **IT general** area, the template groups **Exchange** and **Firewall** have also been defined below.



A **default template group** can be defined directly next to the drop-down menu for selecting the template group (green arrow). This is always preconfigured when you select “IT” as the OU to save records.

Issuing tags for predefining rights

In the same way that permissions are defined within rights templates, it is also possible to automatically set **tags**. Their configuration is carried out in the same way as issuing tags for records.



Rights template for IT-Consultants
Last changed on 10/13/2017 13:56:57

Exchange

Name	Permissions
IT Management	Read/Write/Delete/Authorise
Administratores	All rights

Tags: IT, Exchange

This process ensures that a special tag is automatically issued when using a certain template group. Example cases can be found in the relevant section.

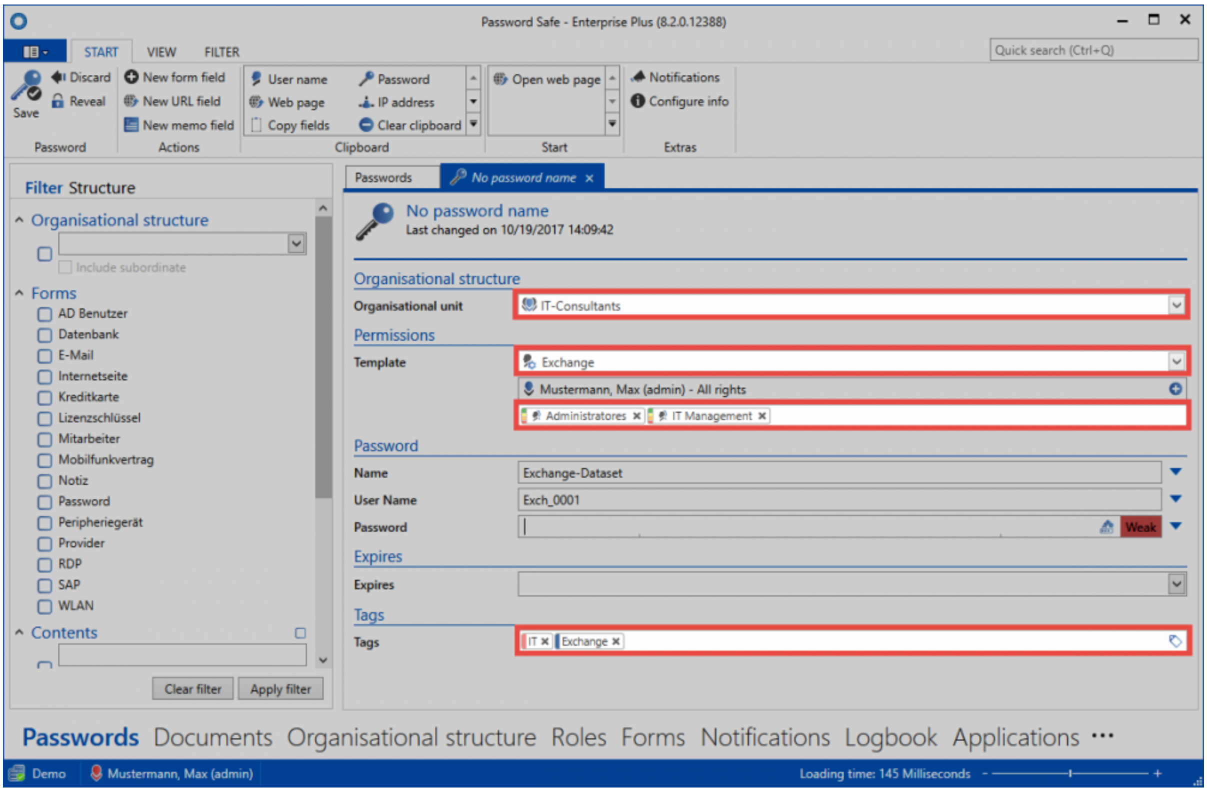
Working with predefined rights

Using predefined rights when creating passwords

After you have preconfigured the rights, you can then use them to create new records. Proceed here as follows:

- Select the password module
- “New password” via the ribbon
- Select a form

In the next window to appear, the organisational unit “IT” and the template group “Exchange” are selected.



Password Safe - Enterprise Plus (8.2.0.12388)

No password name
Last changed on 10/19/2017 14:09:42

Organisational structure
Organisational unit: IT-Consultants

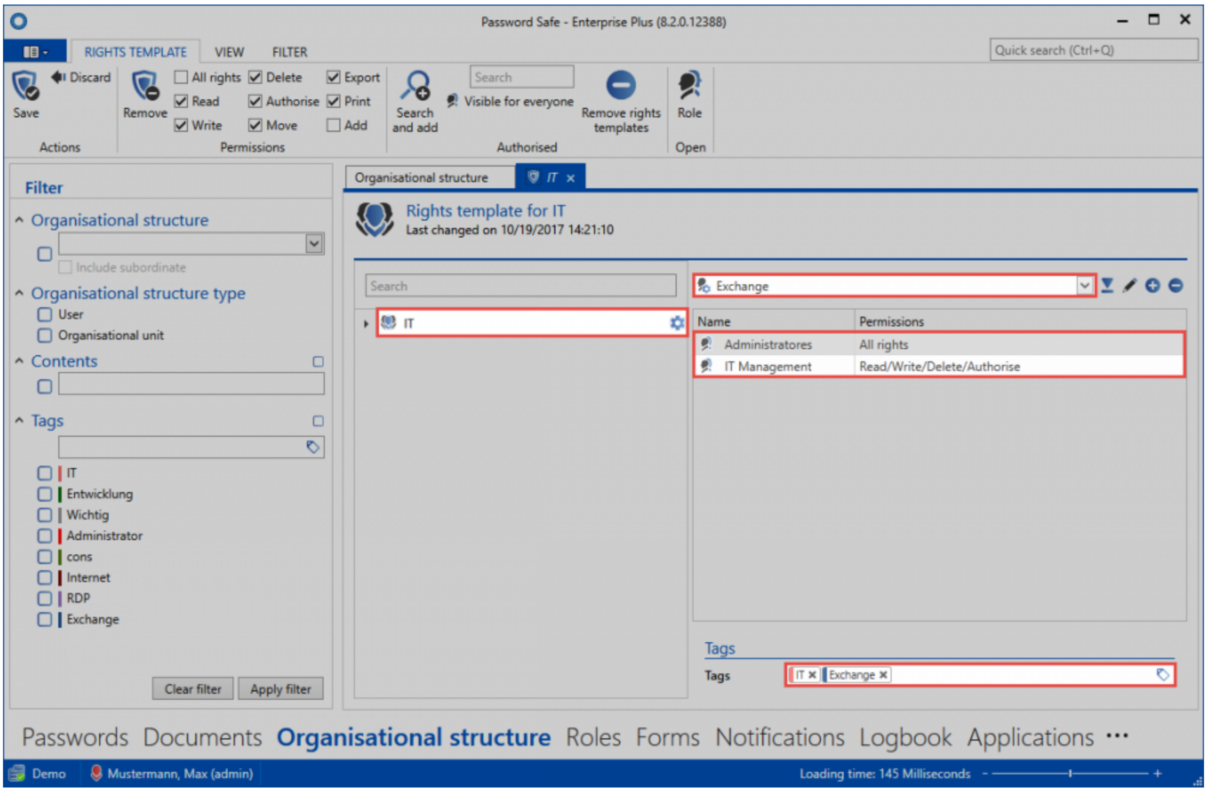
Permissions
Template: Exchange
Mustermann, Max (admin) - All rights
Administratores, IT Management

Password
Name: Exchange-Dataset
User Name: Exch_0001
Password: Weak

Expires
Expires:

Tags
Tags: IT, Exchange

Here is the underlying rights template as a comparison:



Name	Permissions
Administratores	All rights
IT Management	Read/Write/Delete/Authorise

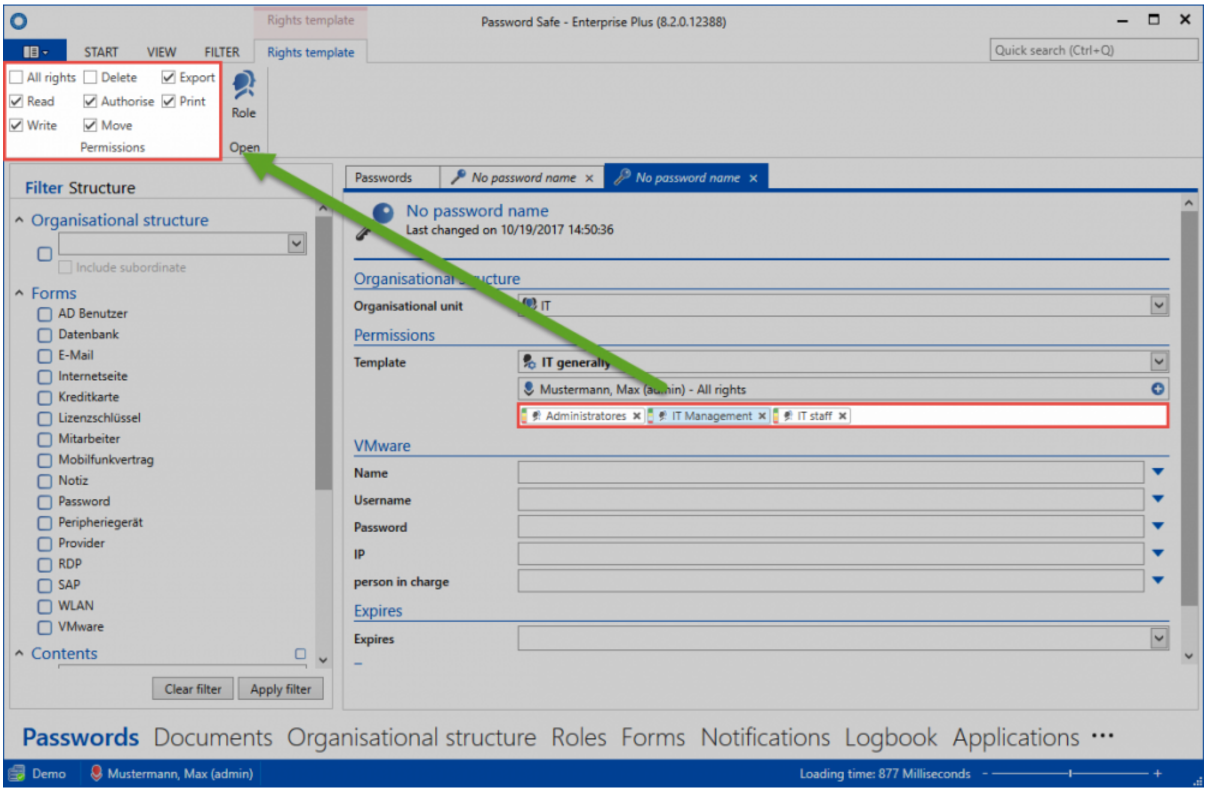
The relationship between them is obvious. It can be immediately seen that by selecting the organisational unit “IT” based on the rights configured in the rights template, permissions are granted for the roles “IT management” and also “Administrators”. **The underlying tags “IT” and “Exchange” are also set**.

Preview of the permissions to be set

When using rights templates, the permissions to be granted can be very quickly classified via a **colour table**. The actual permissions can also be viewed as usual via the ribbon. The following colour key is used with the associated permissions:

Colour	Permission
Green	Read
Yellow	Write
Orange	Delete
Red	Authorize

Other rights also exist that are, however, not separately indicated by a colour. The overview in the ribbon can be used to see whether the “move”, “export” and “print” rights are set or not. The permissions for the selected role/user are always displayed – in this case for the role “IT management”.



☐ All rights ☐ Delete ☑ Export
☑ Read ☑ Authorise ☑ Print
☑ Write ☑ Move

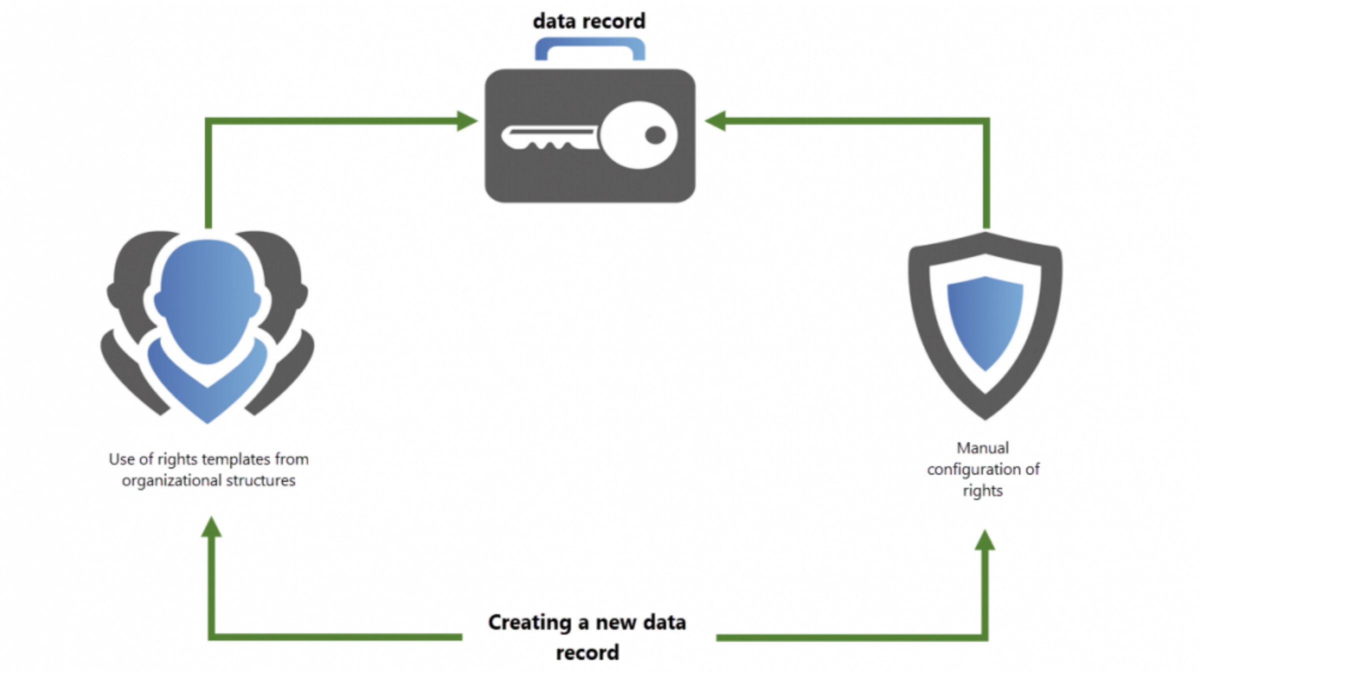
No password name
Last changed on 10/19/2017 14:50:36

Organisational structure
Organisational unit: IT

Permissions
Template: IT generally
Mustermann, Max (admin) - All rights
Administratores ×, IT Management ×, IT staff ×

Conclusion

The manual setting of permissions enables the configuration of rights for both existing and also new records. The option of predefining rights represents a very efficient alternative. Instead of having to separately grant permissions for every record, a “preset” is defined once for each organisational structure. Once this has been done, it is sufficient in future to merely select the organisational structure when creating a record. The permissions are then set automatically. This process is particularly advantageous for those users who should not set their permissions themselves.

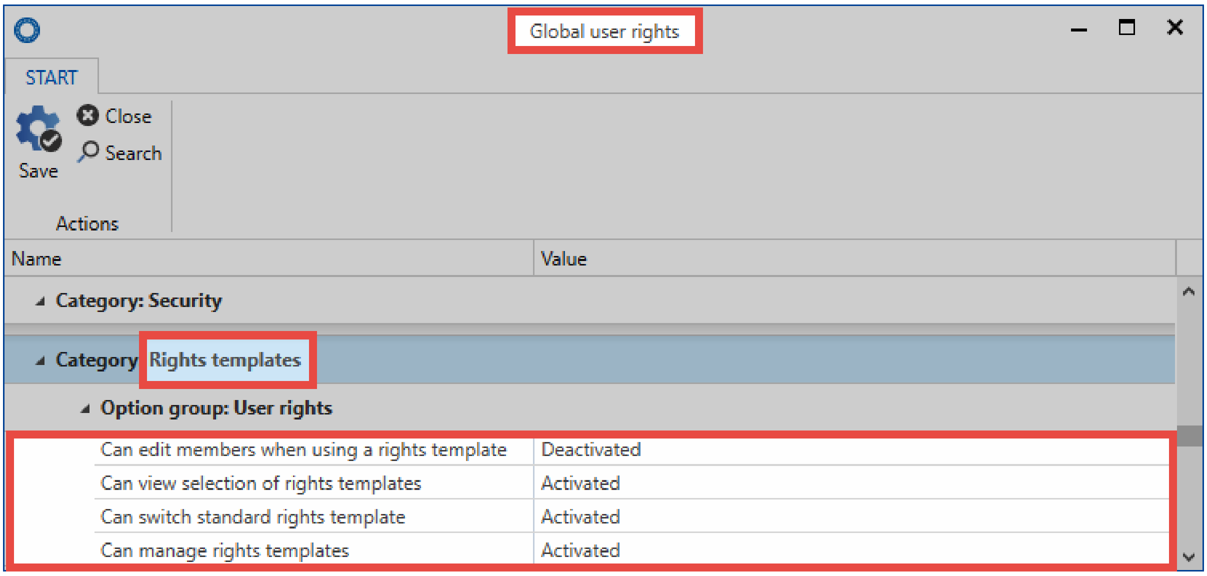

data record
Use of rights templates from organizational structures
Manual configuration of rights
Creating a new data record

! The configuration of permissions can be carried out manually or automatically as described. If you want to change previously set permissions later, this has to be done manually. Retrospectively defining rights is not possible.

Relevant user rights

User rights for predefined rights

The user rights section provides all of the basic information required for handling user rights . Nevertheless, the four user rights related to “predefining rights” are explained below.



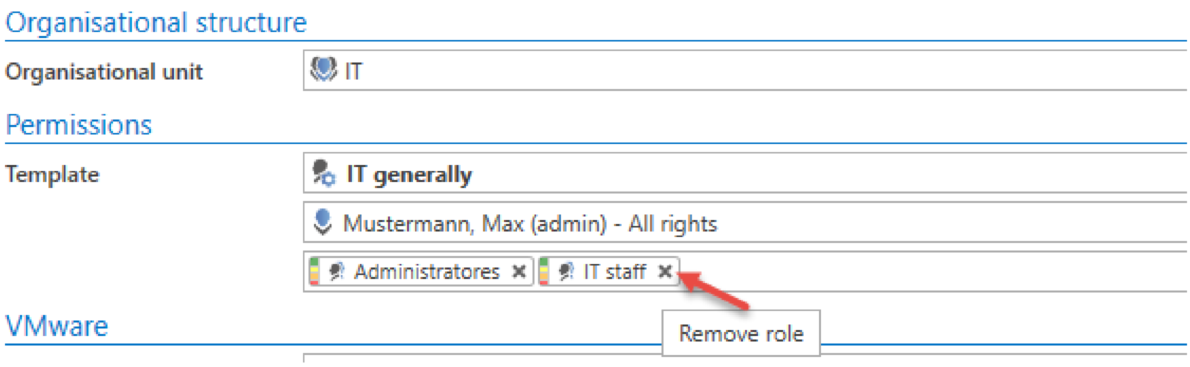
Name	Value
Can edit members when using a rights template	Deactivated
Can view selection of rights templates	Activated
Can switch standard rights template	Activated
Can manage rights templates	Activated

- **Can switch default rights templates:** When selecting the rights template, a diverse range of rights template groups can be selected. To be able to select a different template to the default template, the right “Can switch default rights templates” is required. If this right has not been granted, you are forced to use the default template.

- **Can manage rights templates:** If the user has the right to manage rights templates, they can open the management function for the rights template via the button “predefine rights”. To receive full rights to manage the rights templates for an organisational unit, the rights “read” and “authorize” are required for the corresponding organisational unit.

- **Can view selection of rights templates:** This right controls whether the rights template selection function is displayed or not when creating new records. If this right has not been granted, the user is thus not able to see for which roles and users the user rights are being defined.

- **Can remove members from rights templates:** Roles defined within the rights templates cannot be removed without this right. If this right has not been granted, the roles defined in the templates are always authorized for records in this organisational structure. If the user right is activated: The user can delete the roles via the “x” icon:



Organisational structure

Organisational unit: IT

Permissions

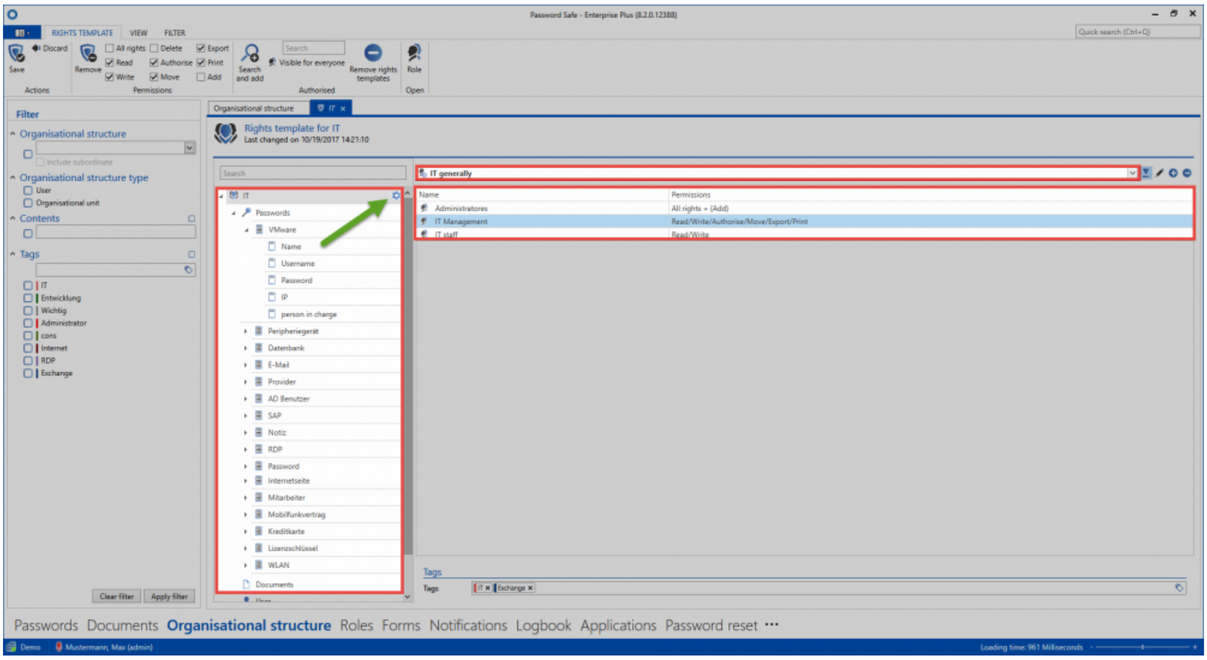
Template: **IT generally**

Mustermann, Max (admin) - All rights

VMware

Scope of validity for predefined rights

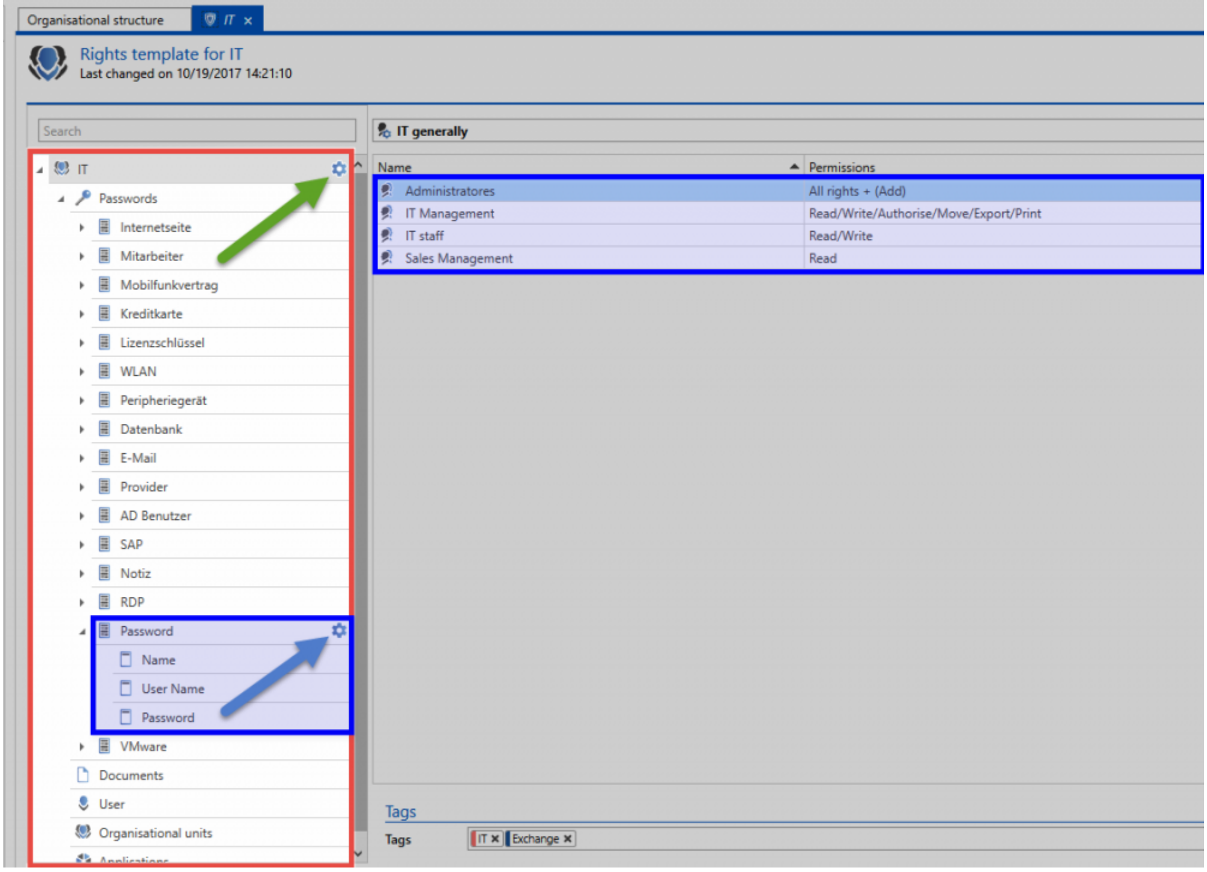
In general, all of the predefined rights for an organisational structure are applied to all underlying objects. These objects could be passwords, forms, form fields documents, users, applications or also other nested organisational structures in the hierarchy. In the following example, the rights template **IT general** has been defined for the organisational unit **IT**.



Name	Permissions
Administratores	All rights + (Add)
IT Management	Read/Write/Authorise/Move/Export/Print
IT staff	Read/Write

If this type of "preset" has been defined, the corresponding icon is displayed at the corresponding level (= green arrow). As no other icons exist below this level, this means that the preset is valid for all underlying objects.

The following example shows how a preset can be defined for when the "password" form is used that not only grants the existing permissions to the roles but also provides the sales manager with read rights.



Rights template for IT
Last changed on 10/19/2017 14:21:10

IT generally

Name	Permissions
Administratores	All rights + (Add)
IT Management	Read/Write/Authorise/Move/Export/Print
IT staff	Read/Write
Sales Management	Read

As can be seen, the preset “IT general” is valid for all objects. An exception here is the “password” form because a unique preset has been defined for this form (blue arrow). As a result, all records created using the “password” form receive permissions as defined in this preset (incl. the sales manager).

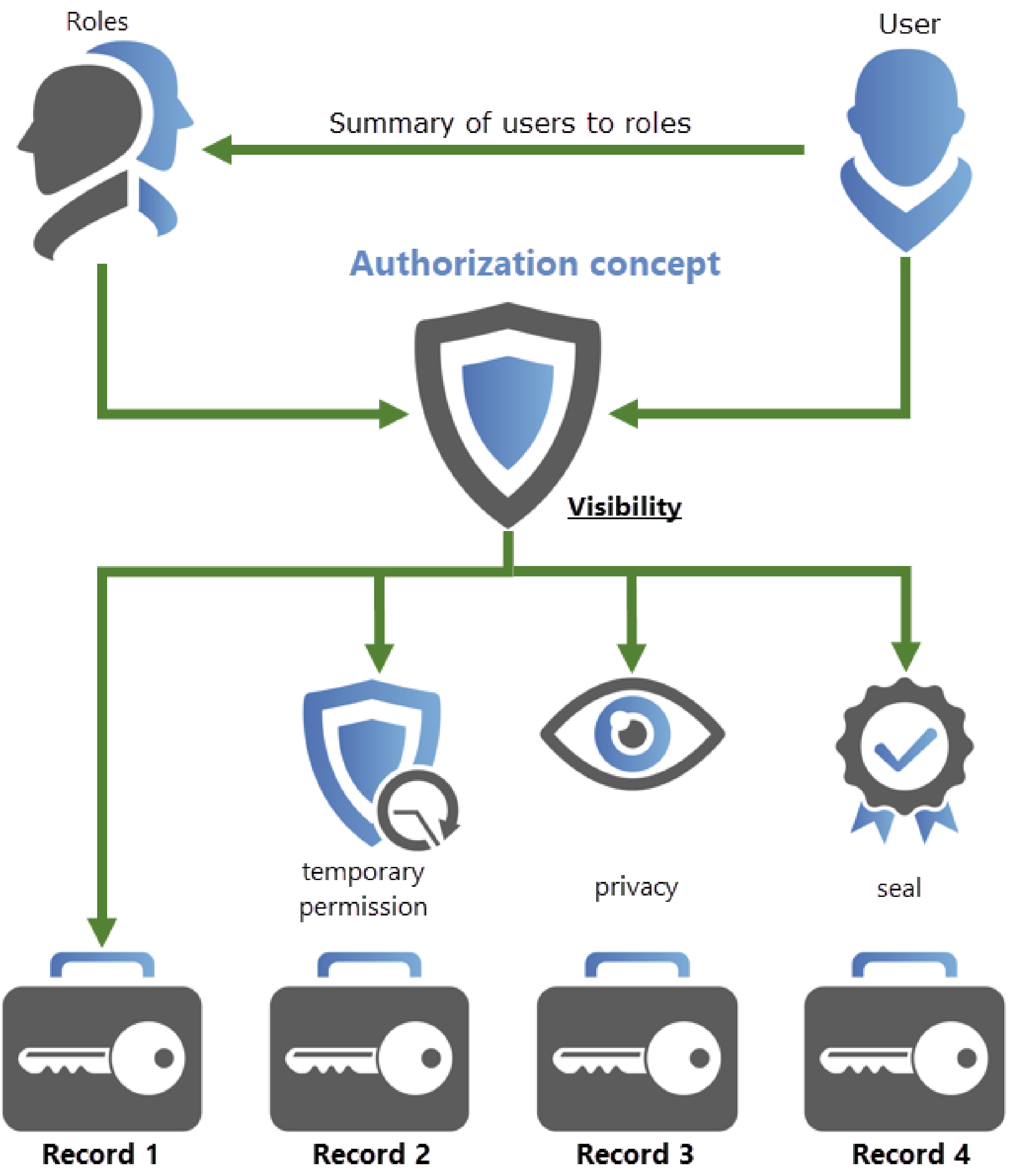
Protective mechanisms

What are protective mechanisms?

The primary goal of Password Safe is to ensure data security at all times. The **authorization concept** is naturally the most important component when it comes to granting users the intended level of permissions for accessing data. Specifically, this makes it possible to make certain information only available to selected employees. Nevertheless, it is still necessary to have protective mechanisms above and beyond the authorization concept in order to handle complex requirements.

- Visibility is not separately configured but is instead directly controlled via the authorization concept (read right). Nevertheless, it represents an important component within the existing protective mechanisms and is why a separate section has been dedicated to this subject.
- By configuring temporary permissions, it is possible to grant users or roles temporary access to data.
- Password masking enables access to the system without having to reveal the passwords of users. The value of the password remains constantly hidden.
- To link the release of highly sensitive access data to a double-check principle, it is possible to use “seals”:#siegel. The configuration of users or roles with the permissions to issue a release is possible down to a granular level and is always adaptable to individual requirements.

The following diagram shows a summary of how the existing protective mechanisms are integrated into the authorization concept.



In the interplay of the authorization concept with the protective mechanisms, almost all conceivable scenarios can be depicted. It is worth mentioning again that the authorization concept is already a very effective tool, with limited visibility of passwords and data records. This concept is present everywhere in Password Safe, and will be explained in more detail below.

Visibility as a basic requirement

It should always be noted that **visibility** is always a basic requirement for applying further protective mechanisms. A record that is completely hidden from a user (= no read right) can naturally not be given any further protective mechanisms.

✻ The visibility of a record is always the basic requirement for applying further protective mechanisms

Combining multiple protective mechanisms

In principle, there are a diverse range of possibilities for combining the above-mentioned protective mechanisms. Temporary access to a “masked” record is possible just as having a “masked” record which is additionally secured by a double-check principle is also possible. **Nevertheless, it should be noted that temporary permissions in combination with seals always pose a risk**. If releasing a seal requires approval from a person who only possesses or possessed temporary permissions or will only possess them in future, this could naturally conflict with the configured release criteria.

! The combination of seals and temporary permissions is not recommended if the user with permissions to issue a release has only been given temporary permissions.

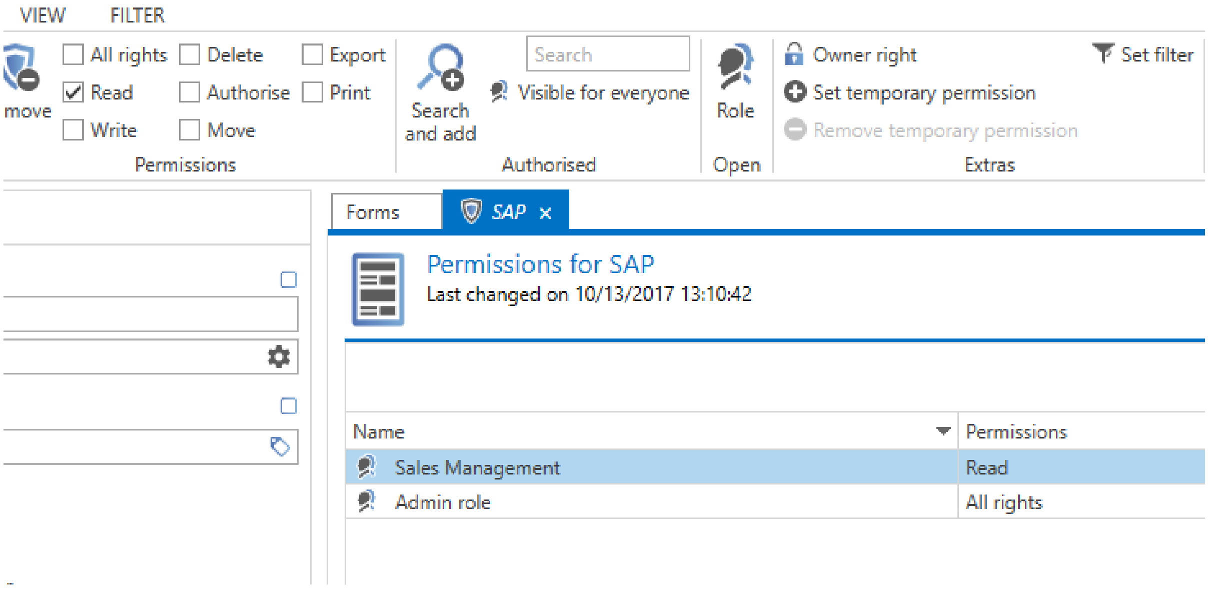
Visibility

Visibility of data

The use of a filter is generally the gateway to displaying existing records. Nevertheless, this aspect of the visibility of the records is closely interwoven with the existing permissions structure. Naturally, a user can always only see those records for which they have at least a read right. This doctrine should always be taken into consideration when handling records. Tags are not subject to any permissions and can thus always be used as filter criteria. Nevertheless, the delivered results will only contain those records for which the user themselves actually has permissions. A good example here is the tag “personal record”. Every user can mark their own record as personal – yet each user will naturally only be able to find their own personal records.

Creating independently working environments

The possibility of separately defining the visibility of individual objects is one of the special features within the Password Safe authorization concept. Irrespective of whether handling records, documents, organisational structures, roles or forms: it is always possible to define whether a user or a role possesses a read right to the object or not. The permissions for each of these objects can be defined separately via the ribbon in the permissions dialogue. This approach enables the creation of independently existing departments within a database. The permissions structure for the SAP form can be seen below. It shows that only the sales manager and the administrators are currently permitted to create new records of type SAP.



Permissions for SAP
Last changed on 10/13/2017 13:10:42

Name	Permissions
Sales Management	Read
Admin role	All rights

In general, each department can independently use forms, create passwords and manage hierarchies in this way. Especially in very sensitive areas of a company, this type of compartmentalisation is often required and also desired.

An **alternative** also supported by Password Safe is for each department to set up their own MSSQL database. However, this physical separation requires considerably more administration work than the above-mentioned separation of data based on permissions and visibility.

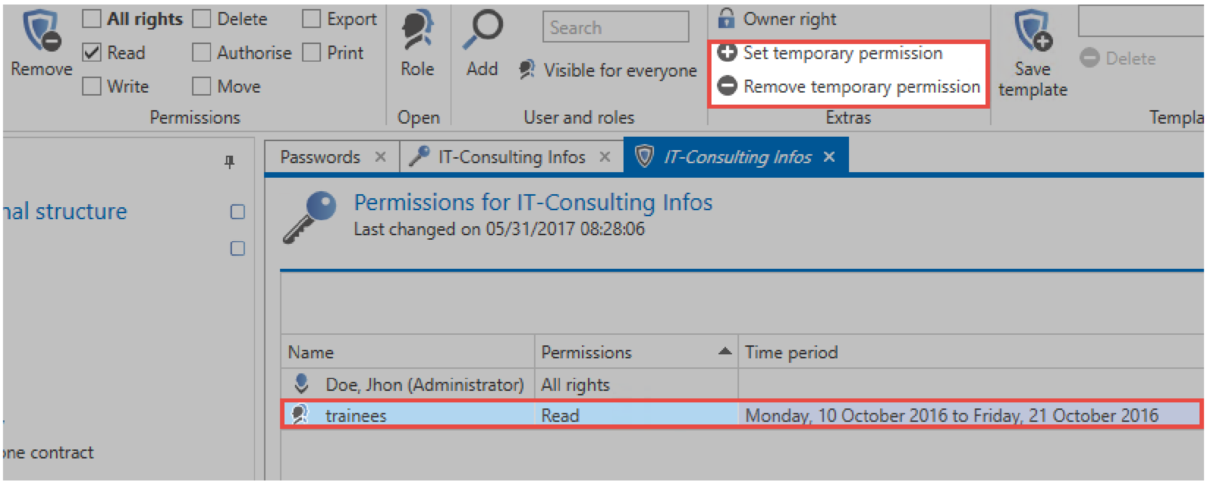
Temporary permissions

What are temporary permissions?

So far, we have covered permissions that were valid for an unlimited period. However, a release can also be granted in advance with a time restriction. Examples are users who stay in the company for a limited time, such as interns or student trainees.

Configuration

When configuring the permissions for records, you can specify a temporary release for each role. The start date as well as the end date is selected here. You can start the configuration using the **Extras** area in the ribbon.



Permissions for IT-Consulting Infos
Last changed on 05/31/2017 08:28:06

Name	Permissions	Time period
Doe, Jhon (Administrator)	All rights	
trainees	Read	Monday, 10 October 2016 to Friday, 21 October 2016

In this example, the role “trainees” was granted to a data set for two weeks of reading permission.

Colour scheme

The colours in the “time period” column provide information on the current status of the granted permissions:

- **Brown:** The temporary permission is configured but is still inactive. The selected time period is still in the future.
- **Green:** The temporary permission is active
- **Red:** The time period for the temporary permissions has already expired and is thus in the past

> Temporary permissions can also be assigned to multiple roles and users at the same time. You can select multiple users and roles as usual with Ctrl/Shift + left mouse button!

Special features of the authorization system

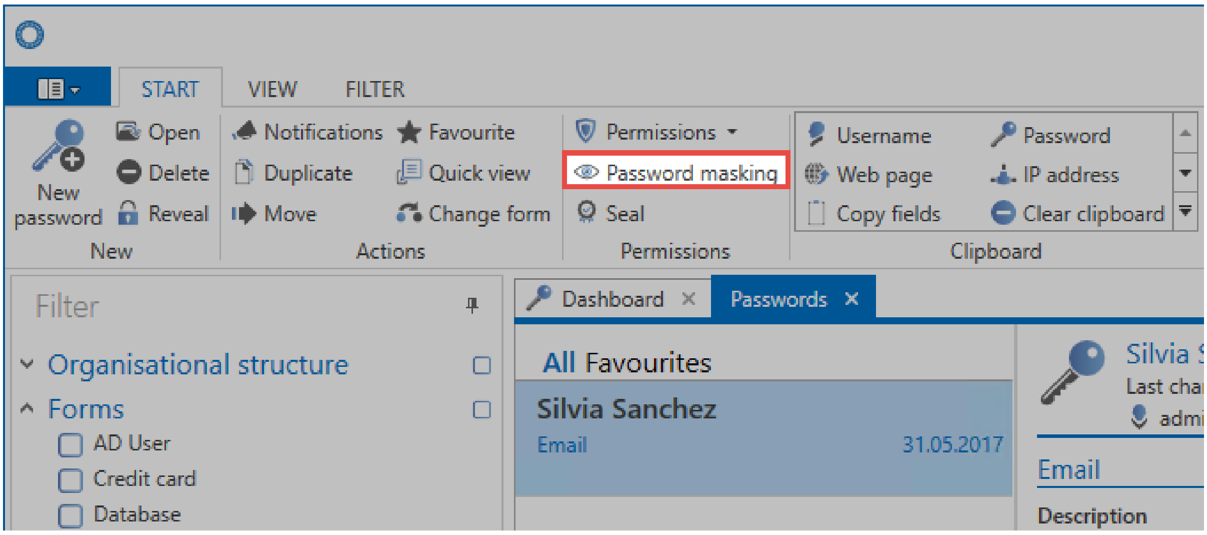
Due to their very nature, temporary permissions leave lots of potential for incorrect configurations. Conceivable constellations include a situation when the only user with all rights only has temporary permissions. When these permissions expire, there is no longer any user with full permissions. To prevent this happening, users with temporary permissions are handled differently.

! There must always be one user who has the “authorize” right to a record, who does not only have temporary permissions.

Password masking

What is password masking?

The safest passwords are those that you do not know. Password masking follows this approach. It prevents the password from being shown, while allowing the use of the automatic sign-on. You can apply it via the button of the same name in the ribbon.



Required permissions

Analogous to the seal configuration, the **Authorise** permission on the data set is required to be able to install or remove the masking. Users use have the **authorize** right for a record can continue to use the record without limitations after applying password masking. Password masking thus only applies to users without the stated right.

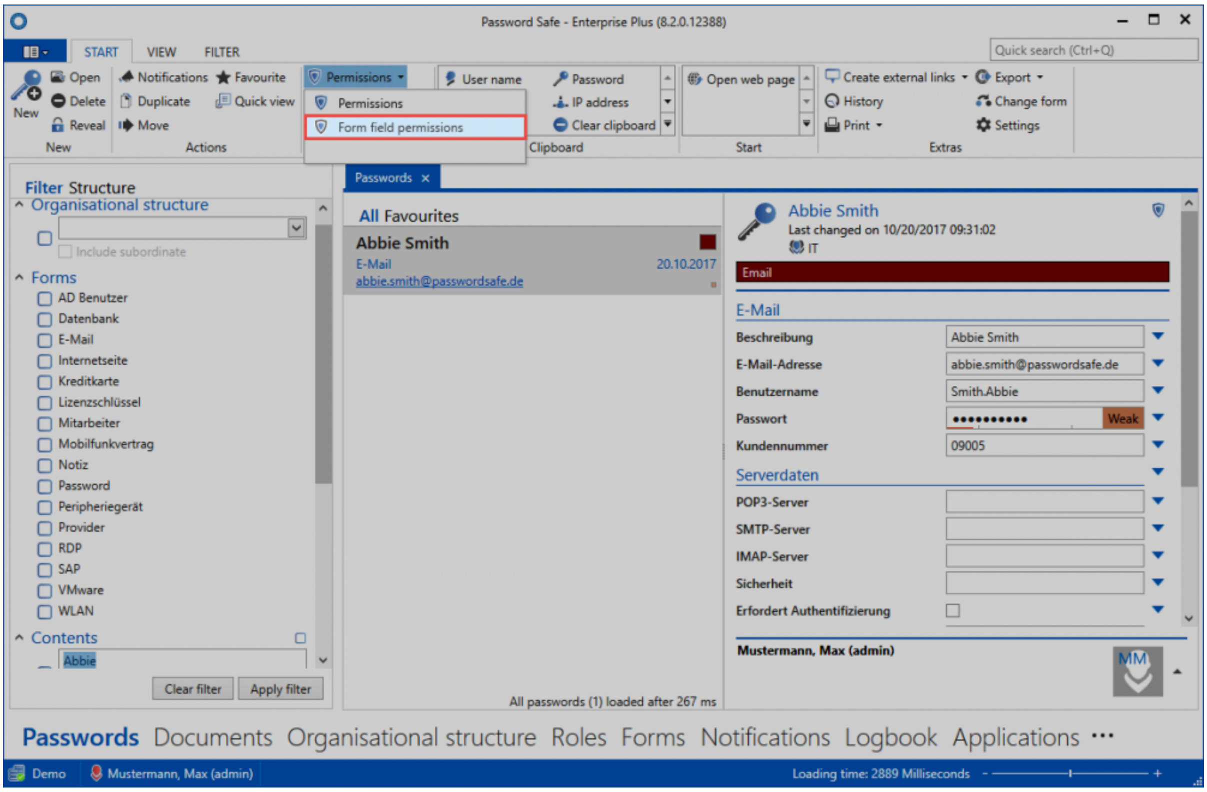
Password masking can only be applied to records with an existing password!

Applying password masking

The icon in the ribbon allows users with the required permissions to apply password masking following a confirmation prompt. By default, the privacy is for all those who have at least reading permission, but not the right * entitled *.

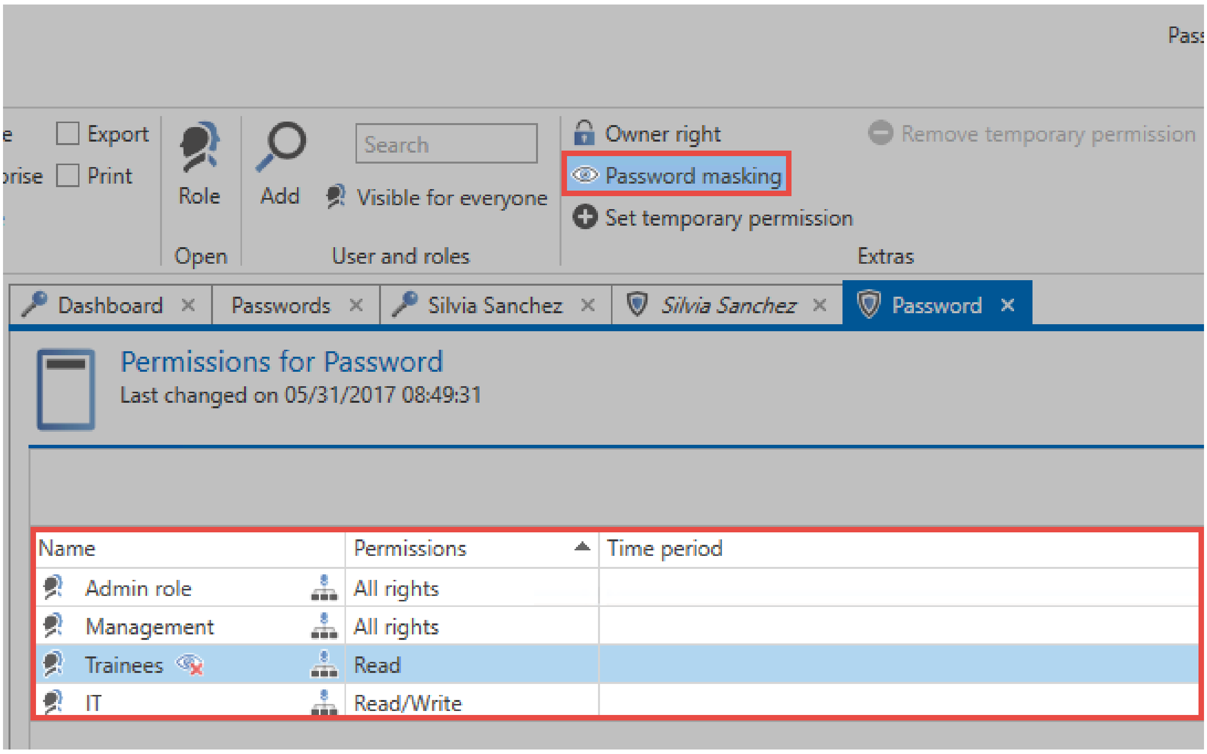
Password masking via form field permissions

As an alternative, you can also apply password masking via the form field permissions. In the detailed view of a record, there is a separate button in the ribbon for that purpose. Ensure that the password field is highlighted.



Beschreibung	Abbie Smith
E-Mail-Adresse	abbie.smith@passwordsafe.de
Benutzername	Smith.Abbie
Passwort	•••••••••• Weak
Kundennummer	09005
POP3-Server	
SMTP-Server	
IMAP-Server	
Sicherheit	
Erfordert Authentifizierung	☐

The special feature when setting or editing masking via the form field permissions is that you can individually select users to whom masking will be applied. In the following example, masking has been specified only for the role of “trainees”, although the “IT” role does not have the **Authorize** right either. In addition to the name of the role or the user, the icon symbolizes the fact that visa protection applies to trainees.



Permissions for Password

Last changed on 05/31/2017 08:49:31

Name	Permissions	Time period
Admin role	All rights	
Management	All rights	
Trainees	Read	
IT	Read/Write	

Use the icon in the ribbon to apply password masking to all users who have read permission on the record, but not the **Authorize** right. If you wish to specify more precisely for which users the password masking should be applied, this is also possible via the **form field permissions**.

Seals

What are seals?

Passwords are selectively made available to the different user groups by means of the authorization concept. Nevertheless, there are many scenarios in which the ability to view and use a record should be linked to a release issued in advance. In this context, the seal is an effective protective mechanism. This double-check principle protects passwords by securing them with granular release mechanisms. If you want to see a password, this must be requested and released. The release can also be temporary.

Required permissions

The user must have the **“Authorize”** right for the data record to create seals. It also needs read access to all users and roles, which are contained in the seal. The exact configuration of password masking and permissions for records is described in detail in the Authorization concept section.

What exactly is sealed?

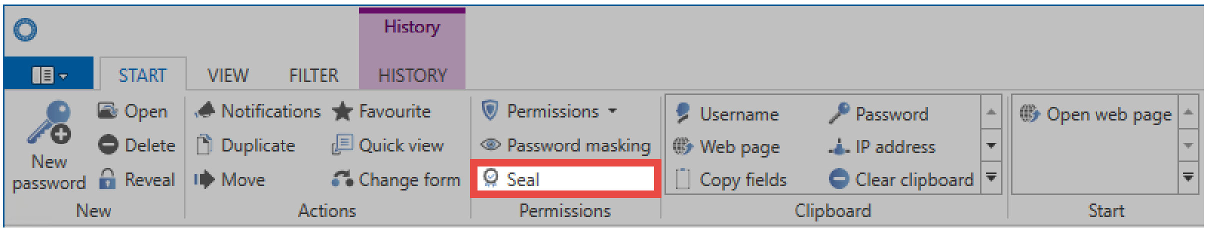
Even with sealed data sets, not all fields are sealed. This s the case only with the passwords that need to be protected. Technically speaking, the password itself is not sealed. It is the right to see a password field that is protected by a seal. This allows for the most sensitive configurations, in which one group can use the password without restrictions, but the same password is sealed for the other user group. The wizard assists users in applying seals, as well as in future maintenance thereof.

! The complete data set is never sealed! Only the right to view a password is protected by a seal.

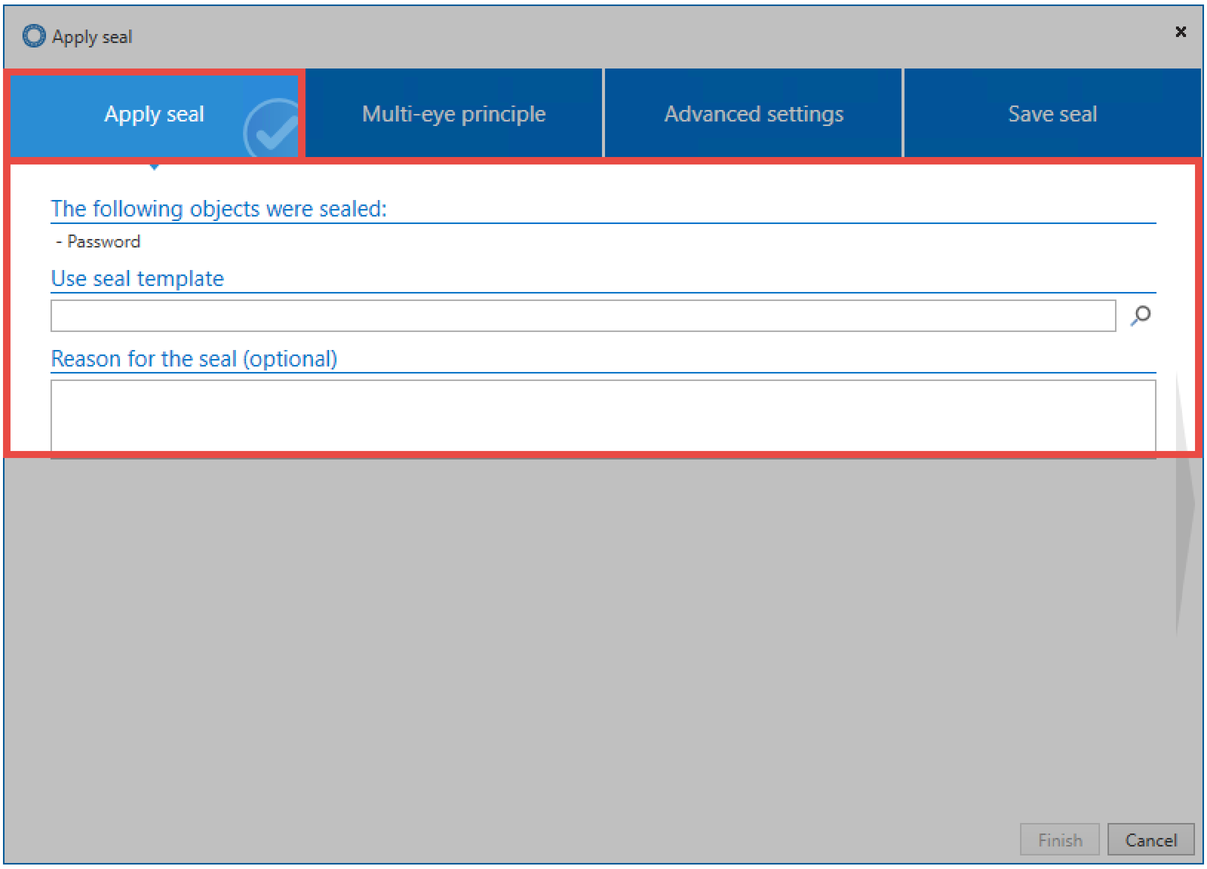
! Only records that are protected with a password can be sealed!

Seal wizard

All seal configurations are performed in the wizard. Both the application of new seals as well as the processing and erasing are possible here. The current state of a seal can also be viewed in an overview, which is also reached via the button in the ribbon. When the seal assistant is opened via the ribbon, the assistant appears in the case of unsealed data sets, which runs in * four steps * through the configuration of the seal.



1. Apply seal



The following objects were sealed:

- Password

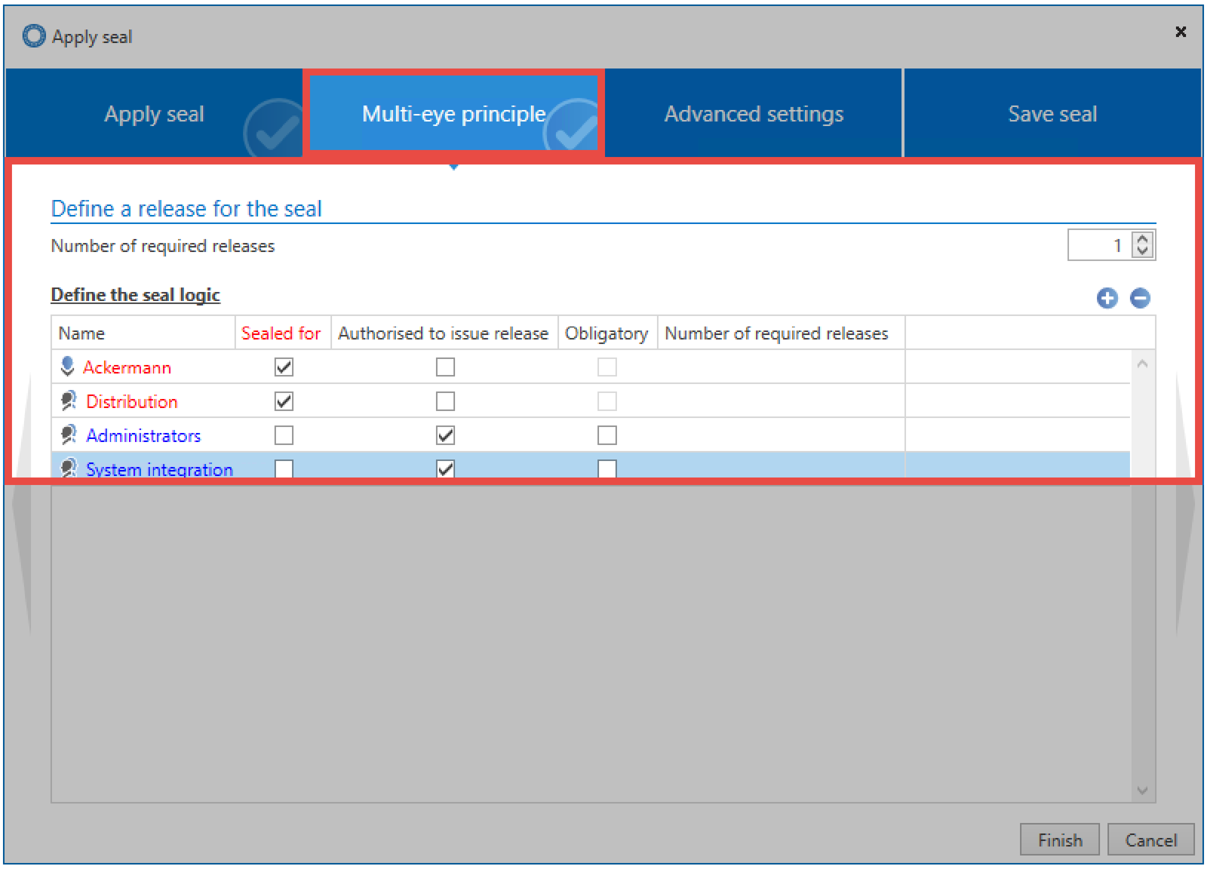
Use seal template

Reason for the seal (optional)

All objects that are sealed are displayed at the beginning. Depending on the data record, this can be one object, or several. It is also possible to use existing seal templates. Optionally, you can enter a reason for each seal.

2. Double-check principle

The seal logic is the most basic element of this protective mechanism. Here, you define for which users or roles the record should be sealed or released in the future. All those for whom the record is to be sealed are displayed in red, while all users with the required permissions to issue a release are displayed in blue.



Define a release for the seal

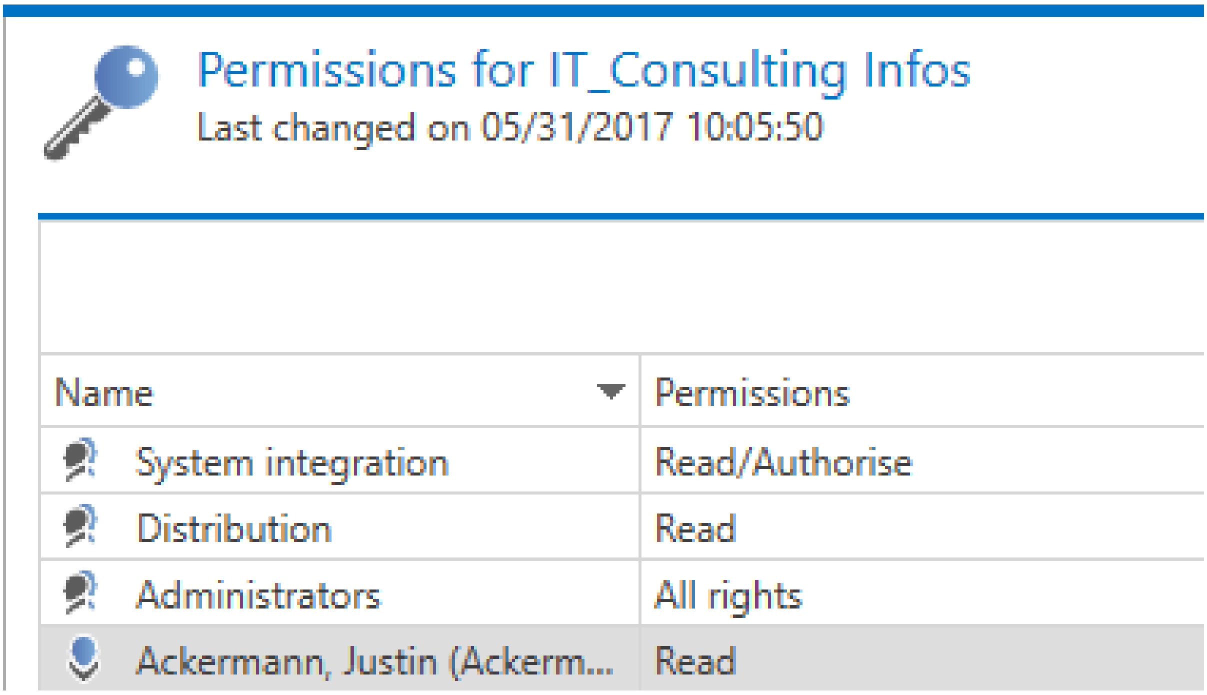
Number of required releases: 1

Define the seal logic

Name	Sealed for	Authorised to issue release	Obligatory	Number of required releases
Ackermann	☑	□	□	
Distribution	☑	□	□	
Administrators	□	☑	□	
System integration	□	☑	□	

All users and roles for which the data set is not sealed and which are not authorized for release are displayed in green. These can use the data record independently of the seal.

To avoid having to perform any configuration manually, roles and users are copied directly from the authorizations of the data record. Compare with the **“permissions”** for the record (can be viewed via the ribbon).



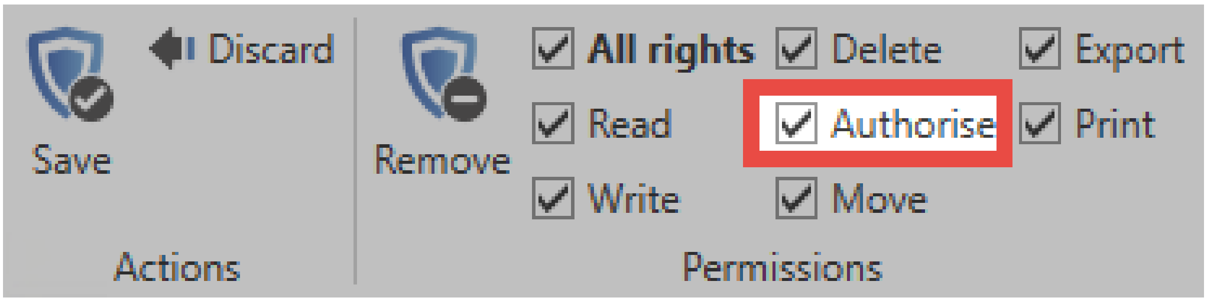
Permissions for IT_Consulting Infos
Last changed on 05/31/2017 10:05:50

Name	Permissions
System integration	Read/Authorise
Distribution	Read
Administrators	All rights
Ackermann, Justin (Ackerm...	Read

The relationships are obvious. As a rule, supervisors should issue the releases for their employees. Therefore, the checkbox also follows the existing authorizations. The following **scheme** is used:

> All users and roles that have the “Authorize” right to the record are **“authorised to issue a release for the seal by default”**. All users and roles that do not have the “Authorize” right to the record are copied directly into the **“Sealed for”** column.

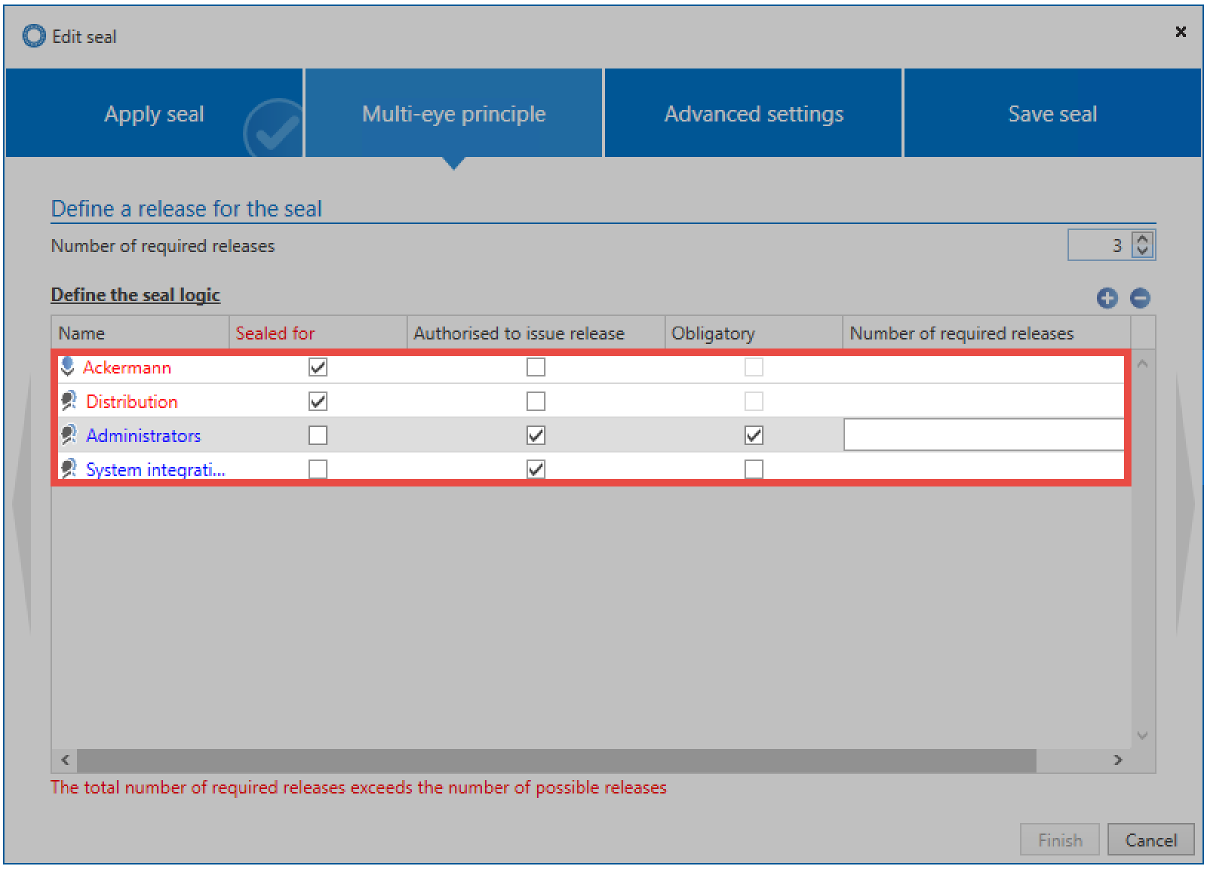
Here is a closer look at the permissions of the role * Administrators * on the record:



☑ **All rights** ☑ Delete ☑ Export
☑ Read ☑ Authorise ☑ Print
☑ Write ☑ Move

Adjusting the seal logic

Although standard authorizations are used as a basis for the sealing concept, these can, of course, be adapted. The number of releases generally required is just as configurable as the required number of releases from a role. In the following example, the seal has been extended so that a total of three release authorizations are required in order to release the seal **(double-check principle)**. The role of the administrators has been marked in the mandatory column. This means that it must grant at least one release In summary: A total of three releases must be made, whereby the group of administrators must grant at least one release.



Define a release for the seal

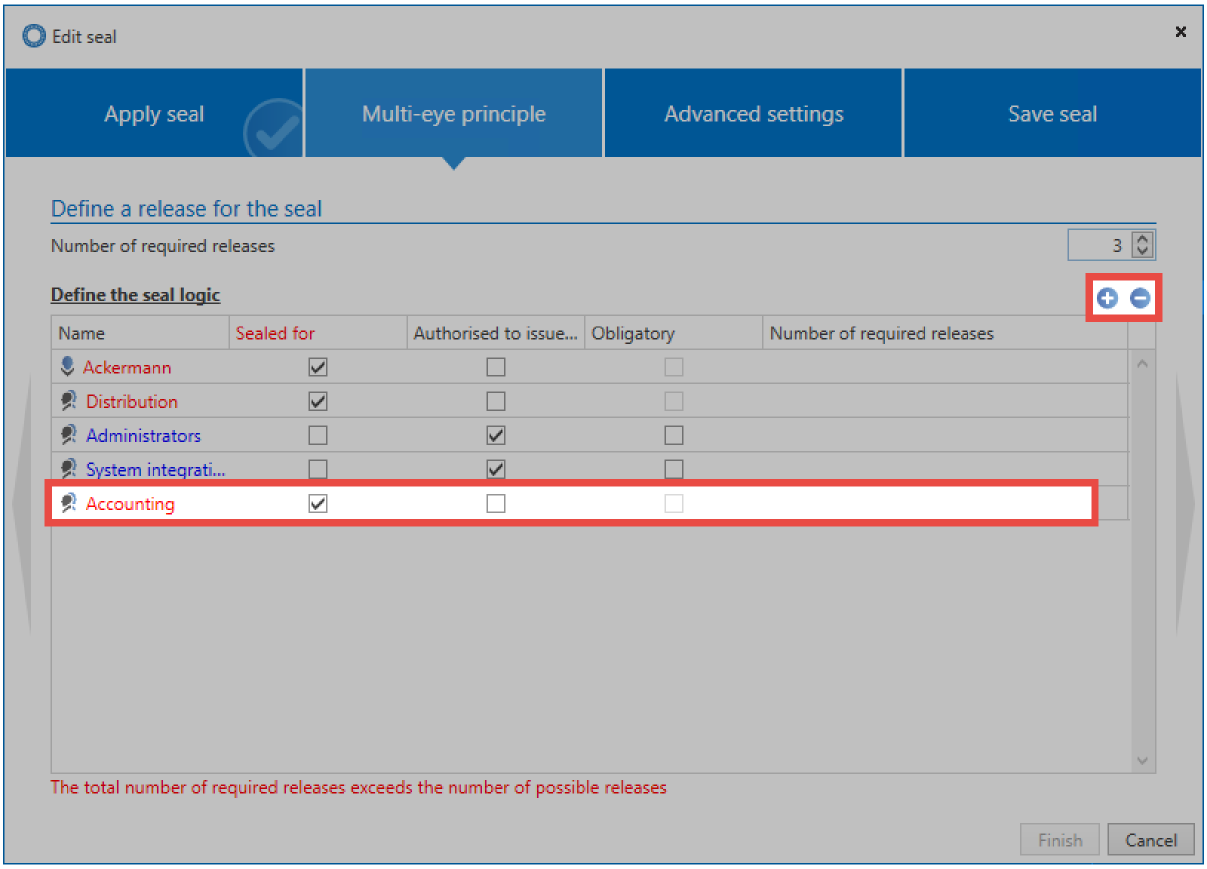
Number of required releases 3

Define the seal logic

Name	Sealed for	Authorised to issue release	Obligatory	Number of required releases
Ackermann	☑	□	□	
Distribution	☑	□	□	
Administrators	□	☑	☑	
System integrati...	□	☑	□	

The total number of required releases exceeds the number of possible releases

In order to be not only dependent on existing authorizations on the data set, other users can also be added to the seal. The role accounting under “sealed for” has been added below.



Define a release for the seal

Number of required releases: 3

Define the seal logic

Name	Sealed for	Authorised to issue...	Obligatory	Number of required releases
Ackermann	☑	☐	☐	
Distribution	☑	☐	☐	
Administrators	☐	☑	☐	
System integrati...	☐	☑	☐	
Accounting	☑	☐	☐	

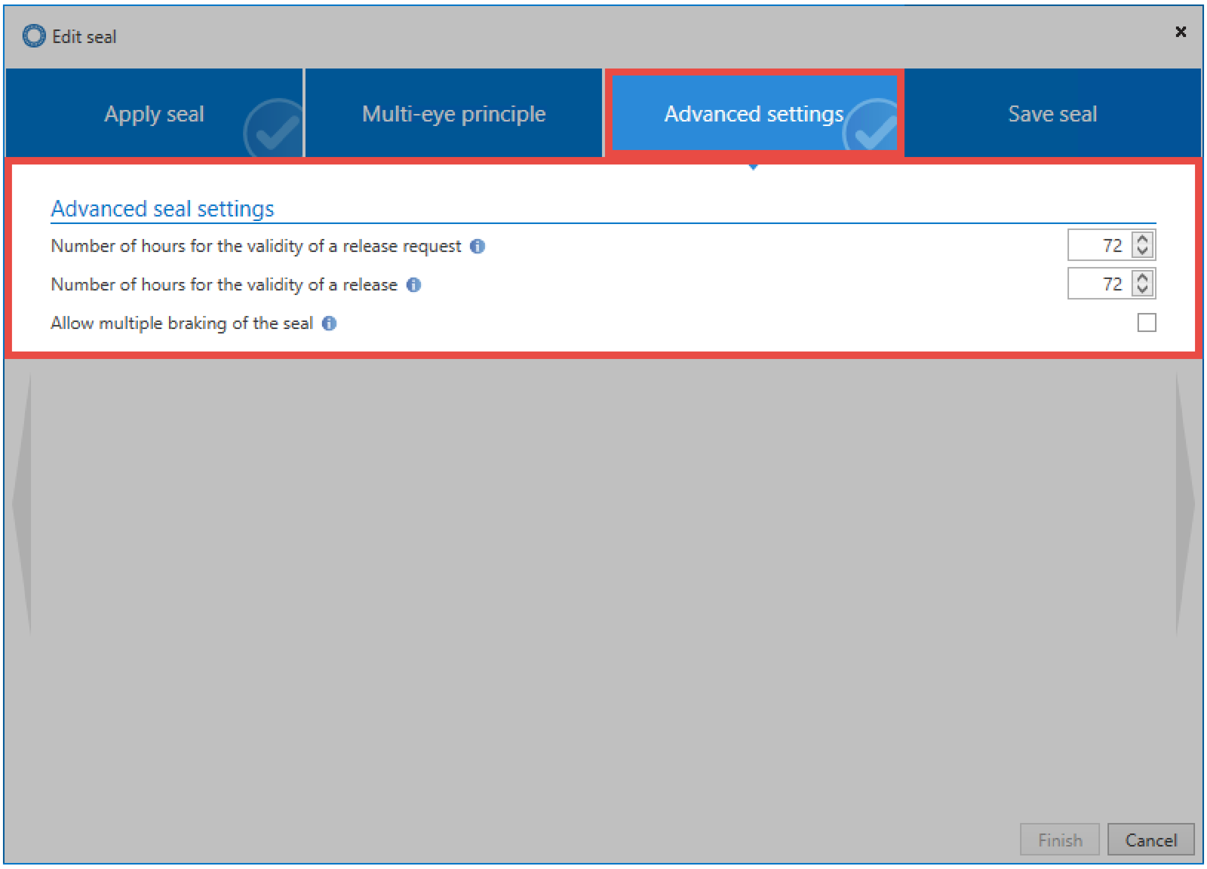
The total number of required releases exceeds the number of possible releases

When a role or a user is added to a seal, these users also receive permissions on the record according to the authorization granted in the seal. A role that is added under “Sealed for” receives the “Read” right on the record. When you add authorization permissions, these will henceforth include the “Read, Write, Delete, and Authorize” rights.

All the roles that were once added to the seal can no longer be removed via the seal logic. This is only possible directly via the authorizations of the data record!

3. Advanced settings

Advanced seal settings allow you to adjust the double-check principle. Both the time validity of a release request as well as a granted release can be configured. Multiple break defines whether after the breaking of a seal by a user, other users may still break it.



Advanced seal settings

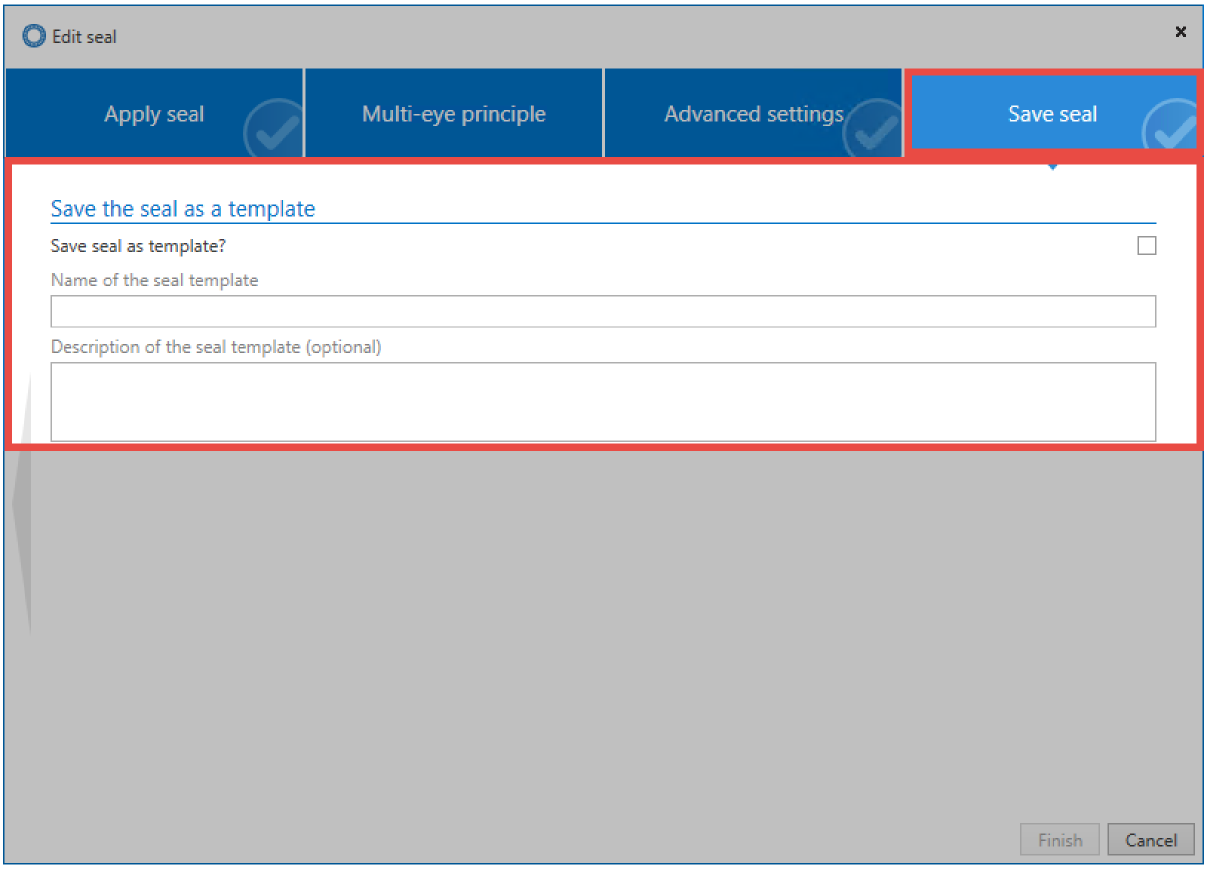
Number of hours for the validity of a release request: 72

Number of hours for the validity of a release: 72

Allow multiple braking of the seal: □

4. Saving the seal

Before closing the wizard, it is possible to save the configuration for later use in the form of a template. Seal templates can be optionally provided with a description for the purpose of overview.



Save the seal as a template

Save seal as template? □

Name of the seal template

Description of the seal template (optional)

Summary

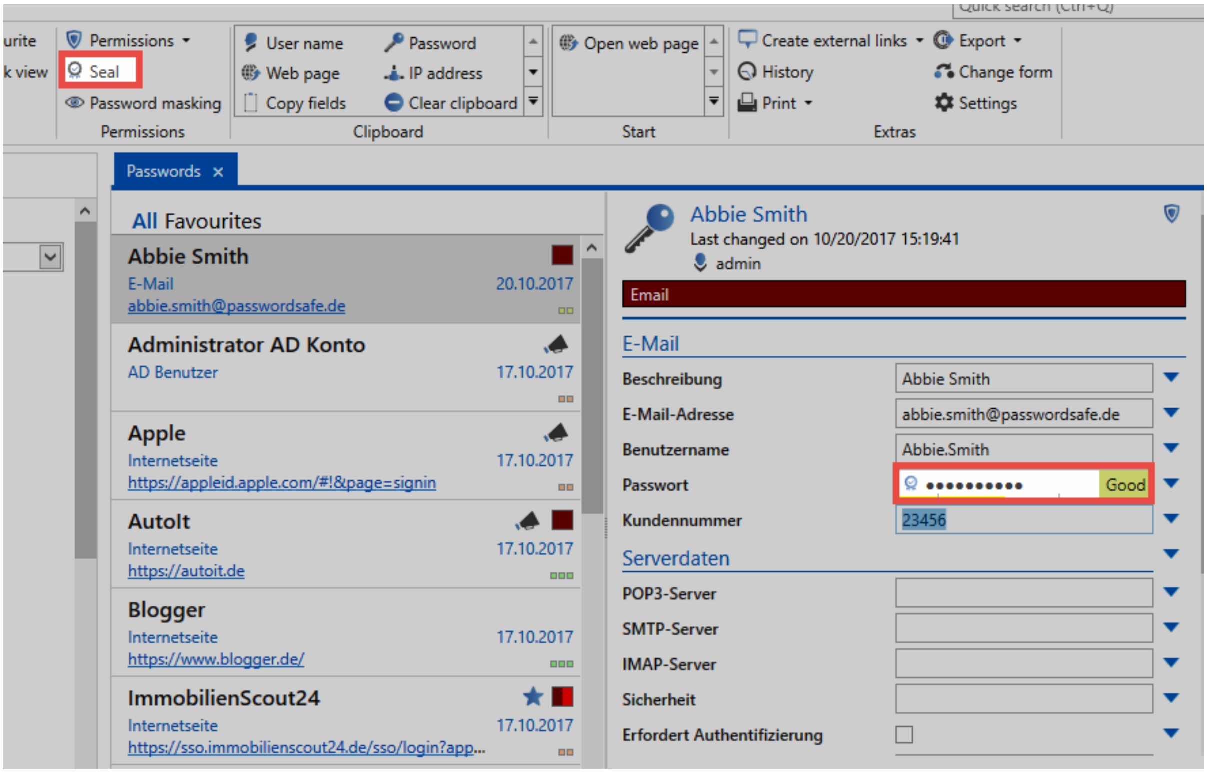
The rights already present on the data set form the basis for any complex seal configurations. It is thus freely definable which users have to go through a release mechanism before accessing the password. The roles, which may be granted, are freely definable. An always accessible seal overview allows all authorized persons to view the current state of the seals. The section on the release mechanism describes in detail the individual steps, from the initial release request to the final release.

- Seal overview
- Release mechanism

Seal overview

What is seal overview?

Users with the required permissions to issue the releases receive access to the current state of the existing seals at any time via the seal overview. The overview is accessible via the ribbon as well as via the icon in the password field of the reading pane.



Abbie Smith
E-Mail 20.10.2017
abbie.smith@passwordsafe.de

Administrator AD Konto
AD Benutzer 17.10.2017

Apple
Internetseite 17.10.2017
https://appleid.apple.com/#!&page=signin

AutoIt
Internetseite 17.10.2017
https://autoit.de

Blogger
Internetseite 17.10.2017
https://www.blogger.de/

ImmobilienScout24
Internetseite 17.10.2017
https://sso.immobilienscout24.de/sso/login?app...

Abbie Smith
Last changed on 10/20/2017 15:19:41
admin
Email

E-Mail

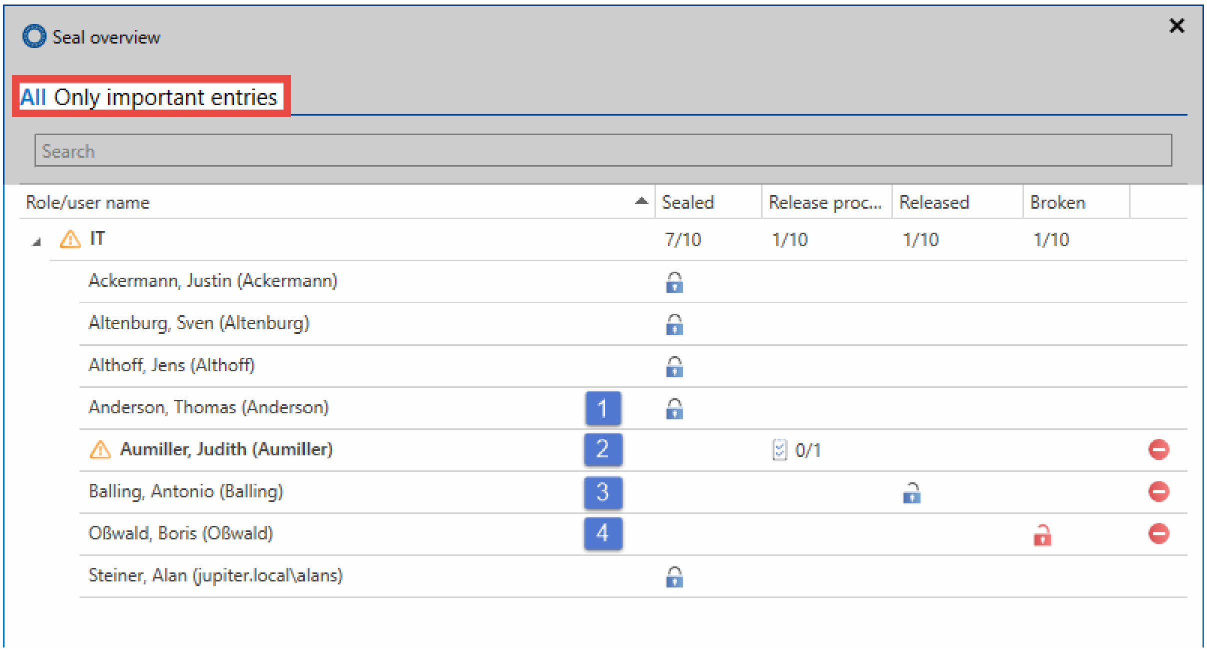
Beschreibung	Abbie Smith
E-Mail-Adresse	abbie.smith@passwordsafe.de
Benutzername	Abbie.Smith
Passwort	●●●●●●●●●● Good
Kundennummer	23456

Serverdaten

POP3-Server	
SMTP-Server	
IMAP-Server	
Sicherheit	
Erfordert Authentifizierung	□

The four states of a seal

In principle, the seal overview provides an overview of all users who have access to the sealed data set. This is, of course, also the case when they receive the seal on the membership of a role. Functions for editing and deleting existing seals are also available. In addition, the current state of the seal is displayed in the form of a release matrix. There are a total of * four states *, in which a seal can be found:



Seal overview

All Only important entries

Search

Role/user name	Sealed	Release proc...	Released	Broken	
⚠ IT	7/10	1/10	1/10	1/10	
Ackermann, Justin (Ackermann)	🔒				
Altenburg, Sven (Altenburg)	🔒				
Althoff, Jens (Althoff)	🔒				
Anderson, Thomas (Anderson)	🔒				
⚠ **Aumiller, Judith (Aumiller)**		0/1			⊖
Balling, Antonio (Balling)			🔓		⊖
Oßwald, Boris (Oßwald)				🔓	⊖
Steiner, Alan (jupiter.local\alans)	🔒				

1. Sealed

If a data record for a user * is sealed *, the user is prevented from seeing the password by the seal. This also corresponds to the condition when a seal has been newly installed. By resetting a request via the icon at the right edge of the screen, current requests from individual users are also returned to the “sealed” state.

2. Release process

If a user has requested a release, it is in the **release process**. This status is highlighted by a corresponding icon next to the user name, since a possible release can be actively granted by the authorized user. After these so-called * important entries * can also be filtered in the headline of the seal overview in the same named rider. The maximum duration of an release request can be configured in the advanced seal settings. If the deadline has elapsed without sufficient releases being made, the request is deleted and the state “sealed” is restored.

3. Released

If a release is granted, a seal is approved as * released *. The maximum duration of a granted release can be limited in the advanced seal settings. The user then has, for example, 24 hours to accept the release and break the seal.

4. Broken

The actual * seal breach * is obtained by acquiring knowledge of the release and by actively breaking the seal after a security query. Viewing the password is irrelevant. Once broken seals can be manually reset by the icon to the right of the broken seal column. The state “Sealed” is restored.

! It makes no logical sense to re-seal already visible passwords. The user was able to view the password. Therefore, it is not monitorable whether the password has been saved, for example, by screenshot. In such cases, a new password is the only way to guarantee 100% password security!

Release mechanism

What is the release mechanism?

A sealed password will not be released until the number of approvals required in the seal has been granted. Releases can be granted by anyone who has been defined as having the required permissions to issue the release in the seal. The mechanism describes the complete process from the first release request to the final grant of the release and the breaking of the seal.

Users and roles in the release mechanism

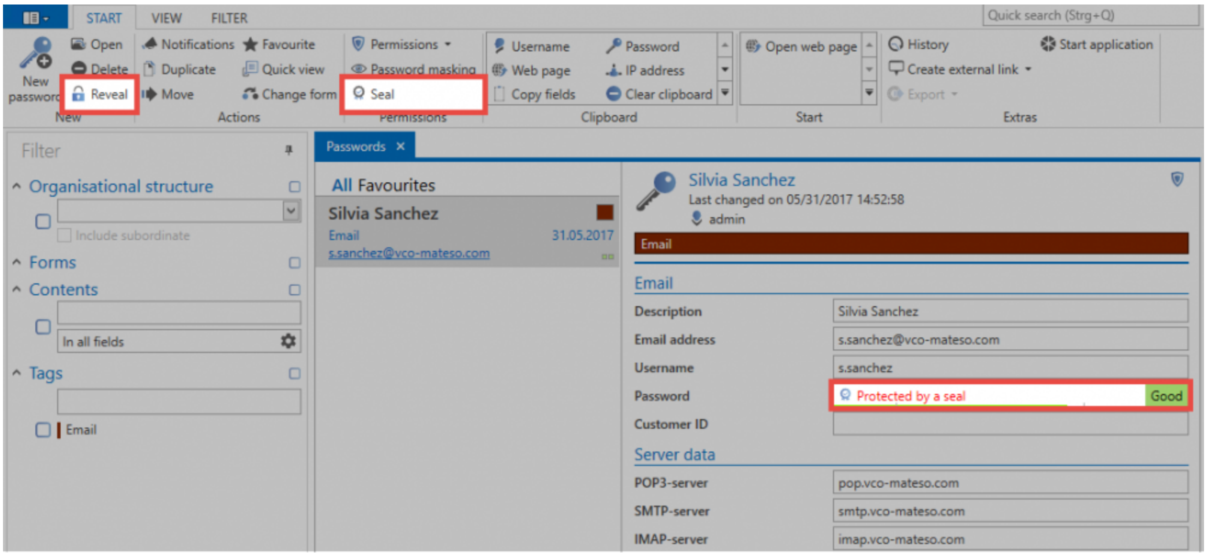
As noted in the previous sections, seals always restrict the right of a user to view a specific password. Even if the configuration is usually done at the level of the role, each user is naturally responsible for his own request when carrying out the release. Even if a seal is defined for a role, technically separate seals are created for each individual member of the role.

Requests or releases are only valid for the respective user!

! If a user is a member of several roles of a seal, the “stronger” right is always applied. Release rights have a priority over read rights

1. Requesting a release

In order to release a seal for sealed passwords, this must be requested from the user with the required permissions to issue the release. Within the Password Safe client, this can be done via the buttons **Reveal** and **Seal** in the ribbon, as well as via the **Icon in the password field** of the data record in the reading pane.



Silvia Sanchez
Email 31.05.2017
s.sanchez@vco-mateso.com

Silvia Sanchez
Last changed on 05/31/2017 14:52:58
admin

Email

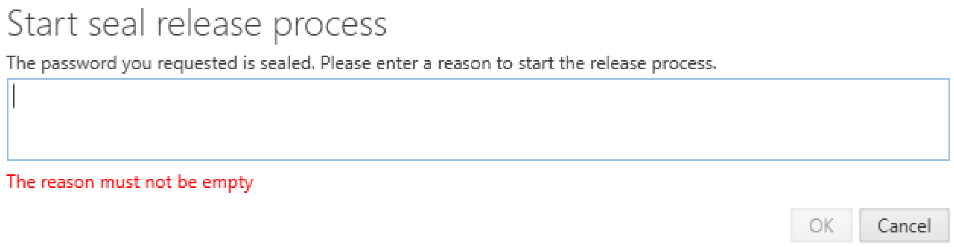
Email

Description	Silvia Sanchez
Email address	s.sanchez@vco-mateso.com
Username	s.sanchez
Password	Protected by a seal Good
Customer ID	

Server data

POP3-server	pop.vco-mateso.com
SMTP-server	smtp.vco-mateso.com
IMAP-server	imap.vco-mateso.com

A modal window opens, which can be used to request the seal. The reason for the entry will be displayed to the users with the required permissions to issue the release.



Start seal release process

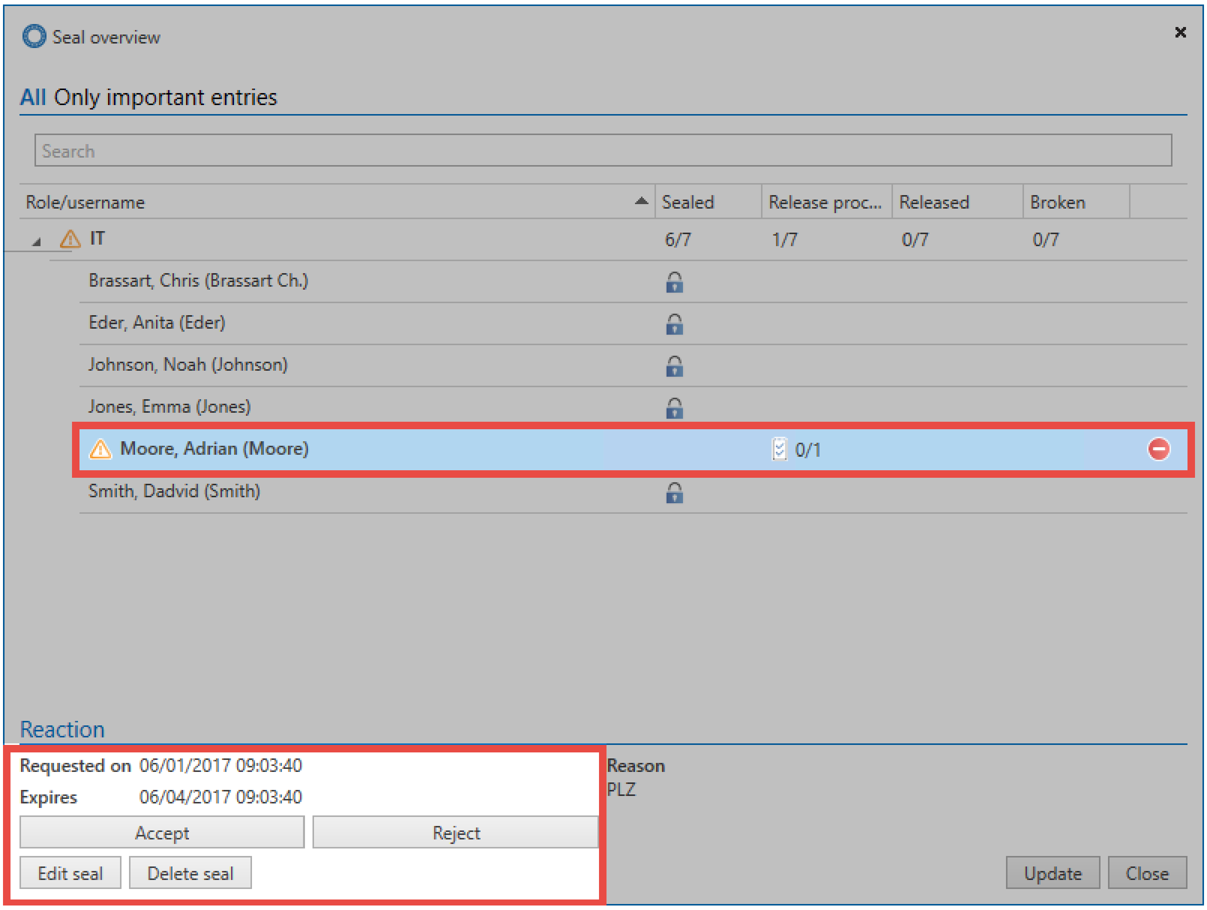
The password you requested is sealed. Please enter a reason to start the release process.

The reason must not be empty

All user with the required permissions to issue the release will be notified that the user has requested the seal. This can be viewed via the module Notifications, as well as in the Seal overview.

2. Granting a release

The seal overview can be opened via the seal symbol in the ribbon directly from the mentioned notification. It is indicated by the corresponding icon that there is a need for action. All relevant data for a release are illustrated within the seal overview. The reason given in the release is also evident.



Seal overview

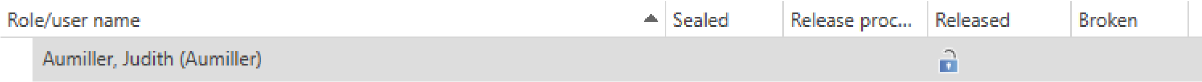
Role/username	Sealed	Release proc...	Released	Broken
IT	6/7	1/7	0/7	0/7
Brassart, Chris (Brassart Ch.)	🔒			
Eder, Anita (Eder)	🔒			
Johnson, Noah (Johnson)	🔒			
Jones, Emma (Jones)	🔒			
Moore, Adrian (Moore)		0/1		
Smith, Dadvid (Smith)	🔒			

Reaction

Requested on 06/01/2017 09:03:40
Expires 06/04/2017 09:03:40

Reason
PLZ

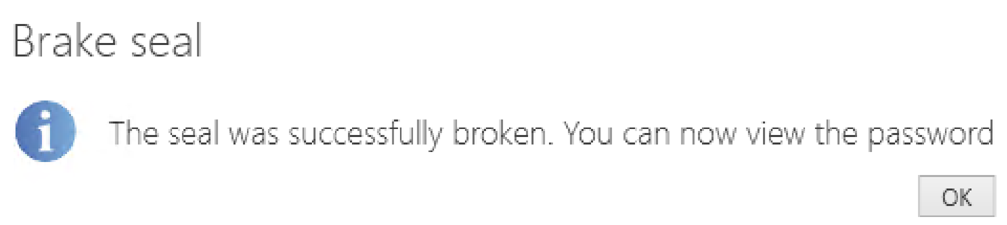
If the release is granted, the Inquirer Im * Module Notifications * will be informed. You can also open the seal directly from the ribbon and see the now released state.



Role/user name	Sealed	Release proc...	Released	Broken
Aumiller, Judith (Aumiller)			🔓	

3. Breaking the seal

As soon as the requesting user has received the number of the required releases, he will be informed via the notifications as usual. The seal can now be broken. From this point on, the user will be able to see the password.



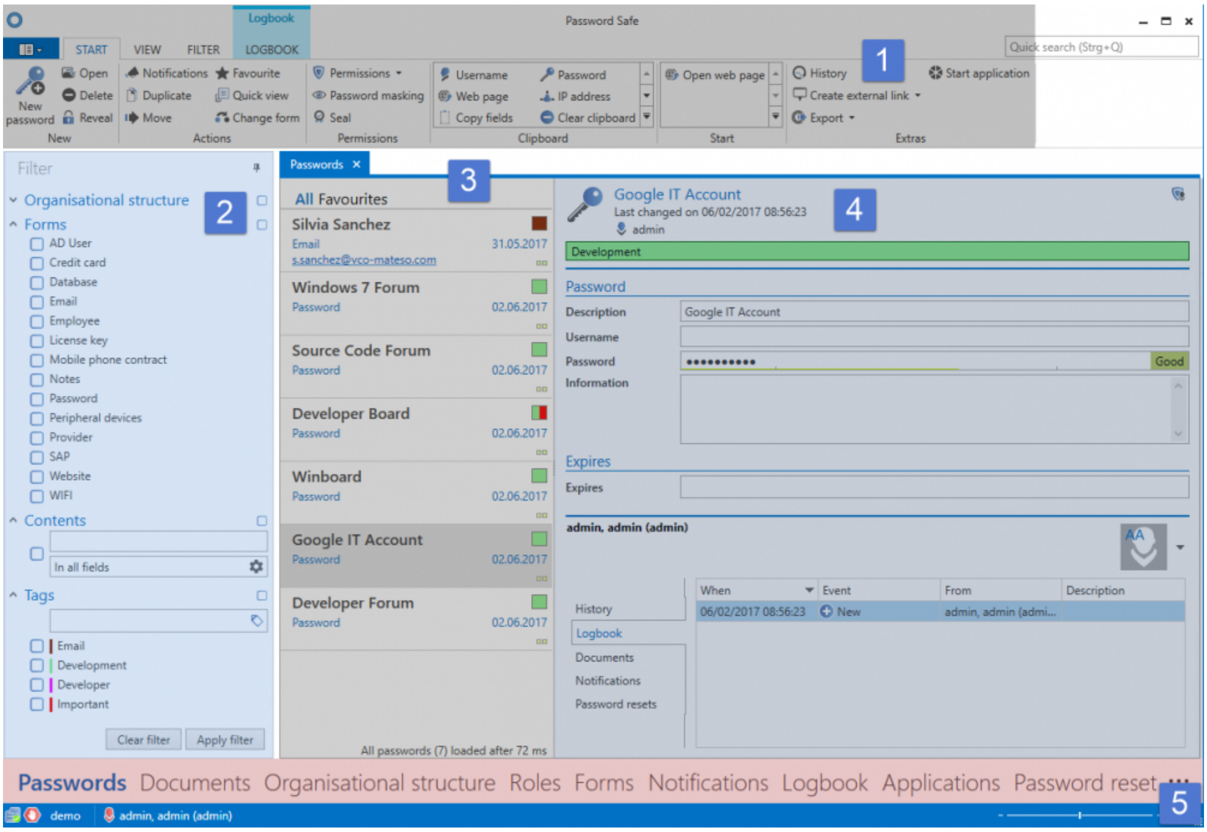
Brake seal

The seal was successfully broken. You can now view the password

Operation and setup

Client structure

The modular structure of the client ensure that the required functionalities are always in the same place. Although the module selection gives access to the various areas of Password Safe, the control elements always remain at the positions specified for this purpose. This intuitive operating concept ensures efficient work and a minimum of training time.



Description: Google IT Account
Username:
Password: ●●●●●●●●●● Good
Information:
Expires:
admin, admin (admin)

When	Event	From	Description
06/02/2017 08:56:23	New	admin, admin (admi...	

1. Ribbon

2. Filter

3. List view

4. Reading pane

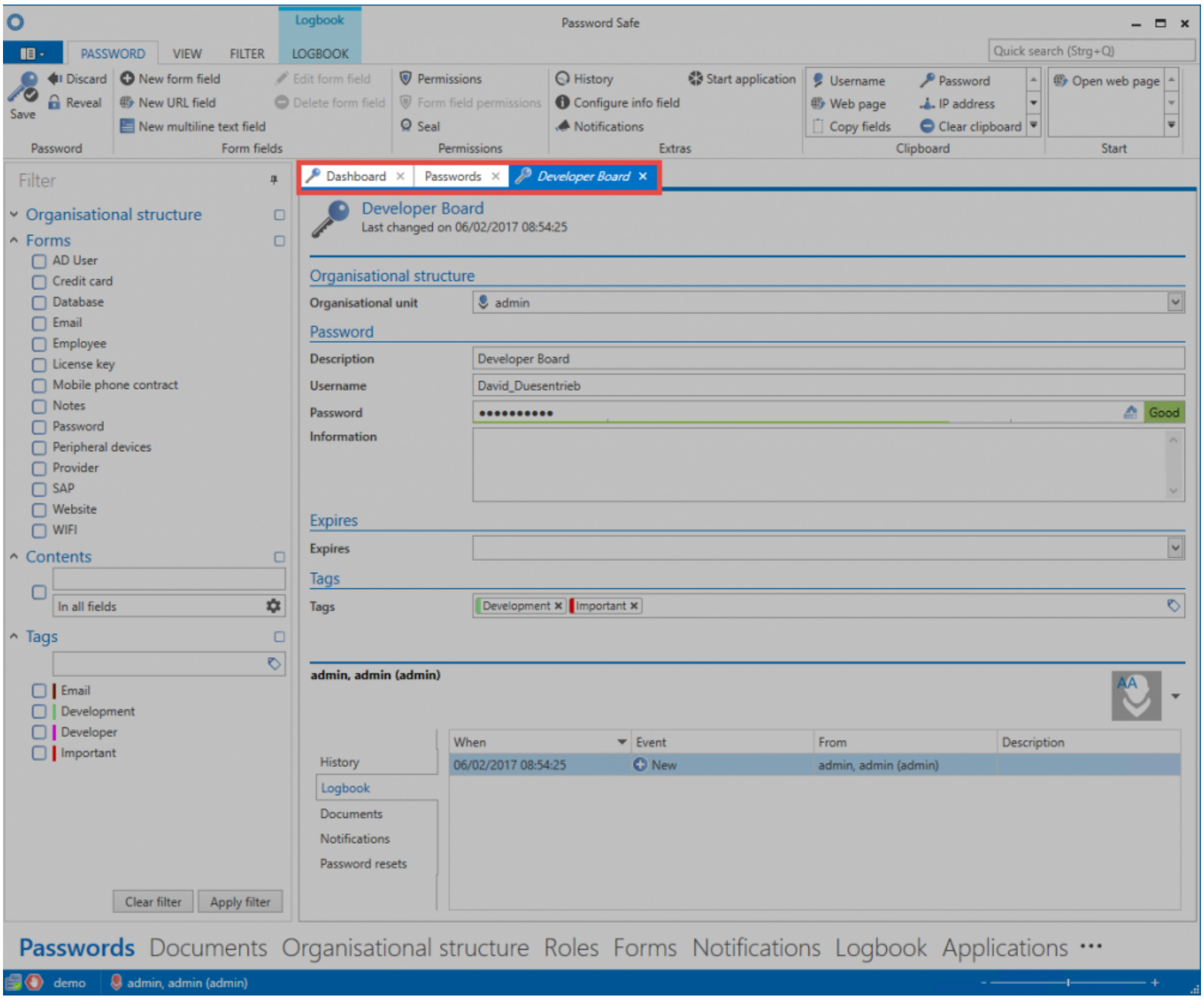
5. Tags

6. Search

7. Dashboard and widgets

TABs

Tabs offer yet another option within the Password Safe to present related information in a separate area. This tab navigation enables you to display, quickly access and switch between relevant information. The results for a filter with specific criteria can thus be retained without the original result being overwritten when a new filter is applied. In parallel, detailed information about records can also be found in their own tabs. It is of course possible to adjust the order of the tabs via drag & drop according to your individual requirements.



Developer Board
Last changed on 06/02/2017 08:54:25

Organisational structure

Organisational unit: admin

Password

Description: Developer Board

Username: David_Duesentrieb

Password: •••••••••• Good

Information:

Expires

Expires:

Tags

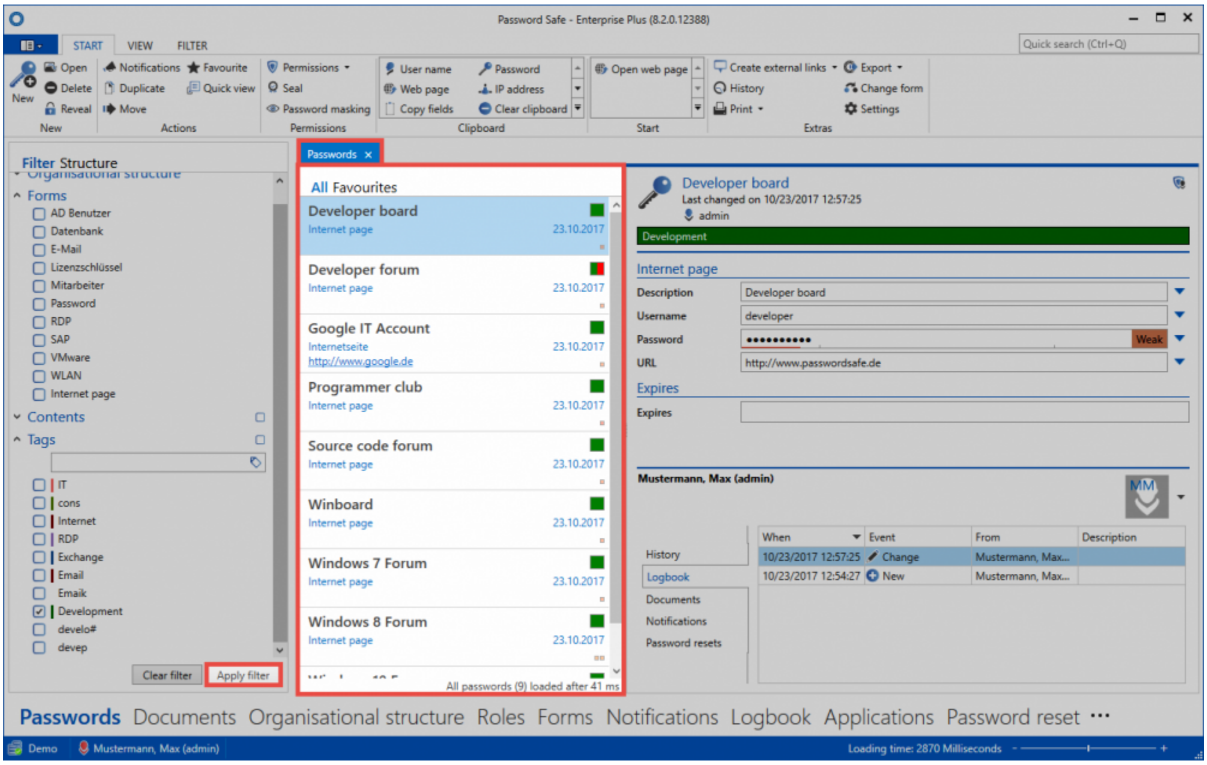
Tags: Development ✕ Important ✕

admin, admin (admin)

When	Event	From	Description
06/02/2017 08:54:25	New	admin, admin (admin)	

Standard tab

Depending on the active module, the **All passwords** tab will be renamed to the corresponding module by default. (All documents, all forms, etc.)

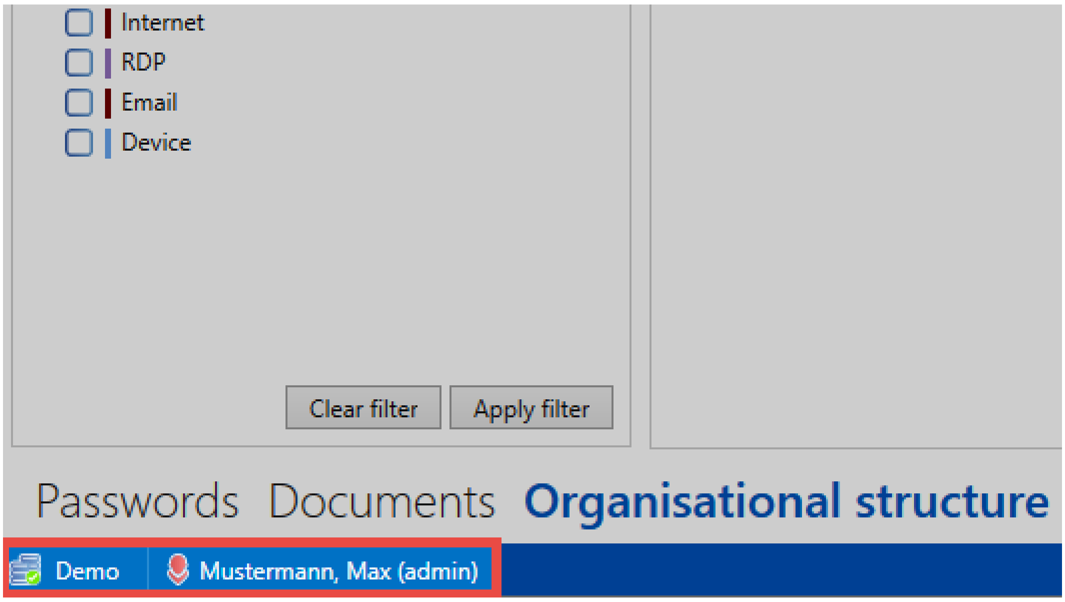


Although the name suggests that all records in the database are displayed, the records displayed in list view correspond to the criteria that have been defined in the filter. The tab closes and can be restored by reusing the filter.

Client footer information

Independently of the module chosen, various information is displayed in the footer area of the client. The icons are also provided with a meaningful mouse-over text, which provides additional information.

- Connection to database
- Feedback in case connection is insecure
- Last name, first name (user name) of the logged-in user

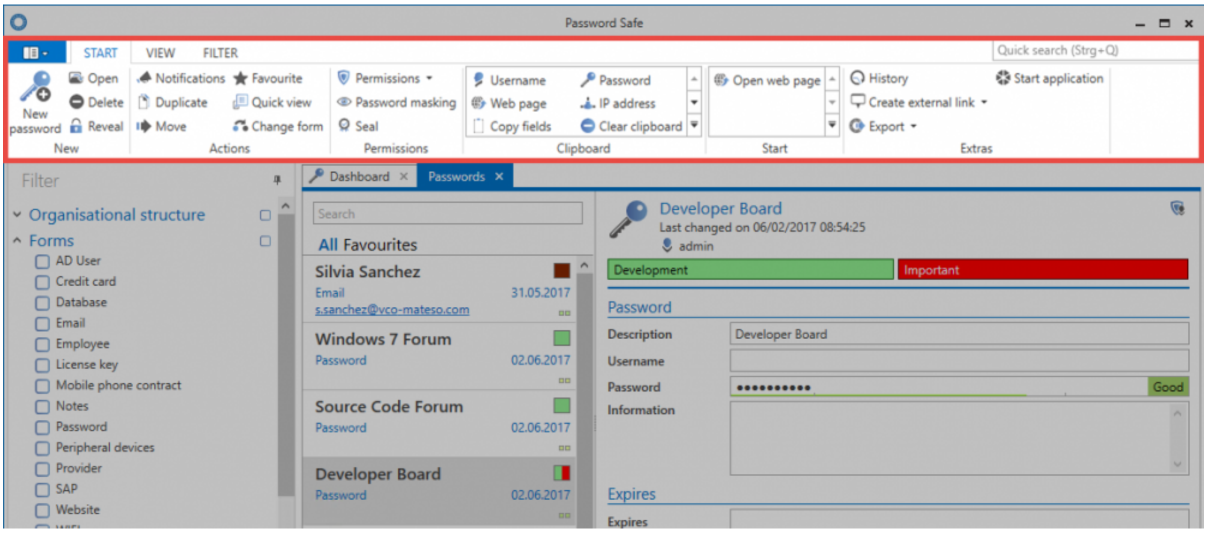


- Ribbon
- Filter
- List view
- Reading pane
- Tags
- Search
- Dashboard and widgets
- “Shortcut key”:#tastaturk-rzel

Ribbon

What is the ribbon?

The ribbon is the central control element of Password Safe Version 8. It is available in all modules. Password Safe is almost always operated via the ribbon in the header area of the PSR client.



Silvia Sanchez
Email 31.05.2017
s.sanchez@vco-mateso.com

Windows 7 Forum
Password 02.06.2017

Source Code Forum
Password 02.06.2017

Developer Board
Password 02.06.2017

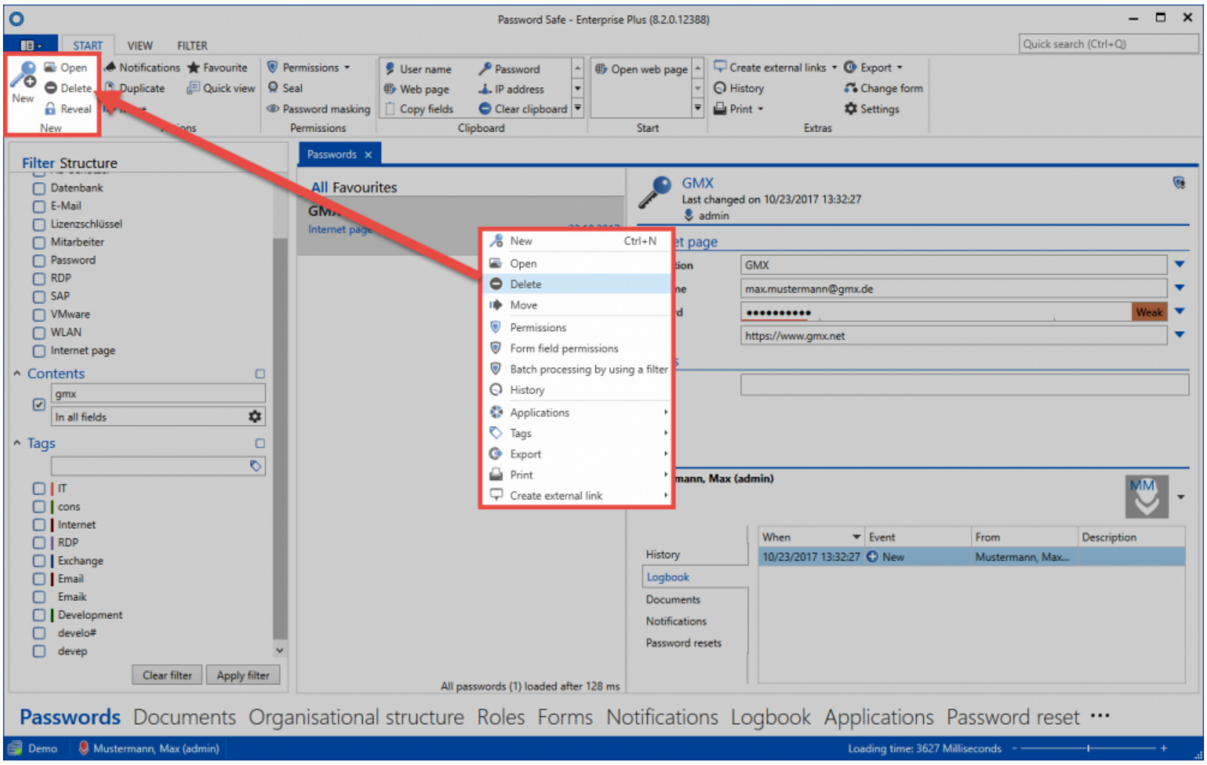
Developer Board
Last changed on 06/02/2017 08:54:25
admin

Development | Important

Password
Description: Developer Board
Username:
Password: ••••••••••• Good
Information:

Expires
Expires

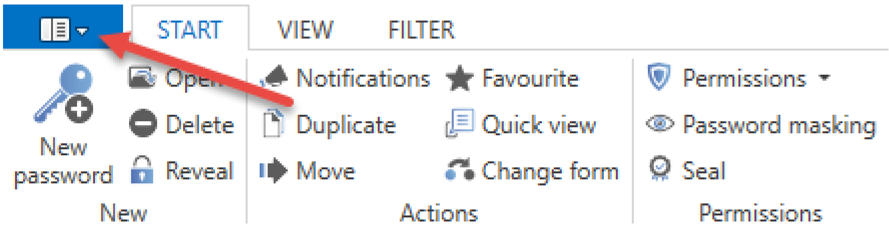
The features available within the ribbon are dynamic, and are based on the currently available actions. Various actions can be performed, depending on which object is selected. The module selected also affects the features that are available in the ribbon. Of course, the most important actions can also be controlled via the context menu (right mouse button).



This mainly affects the very often used features such as opening, deleting or assigning tags. However, a complete listing of the possible actions is always only possible directly in the ribbon. This ensures that the context menu can be kept lean.

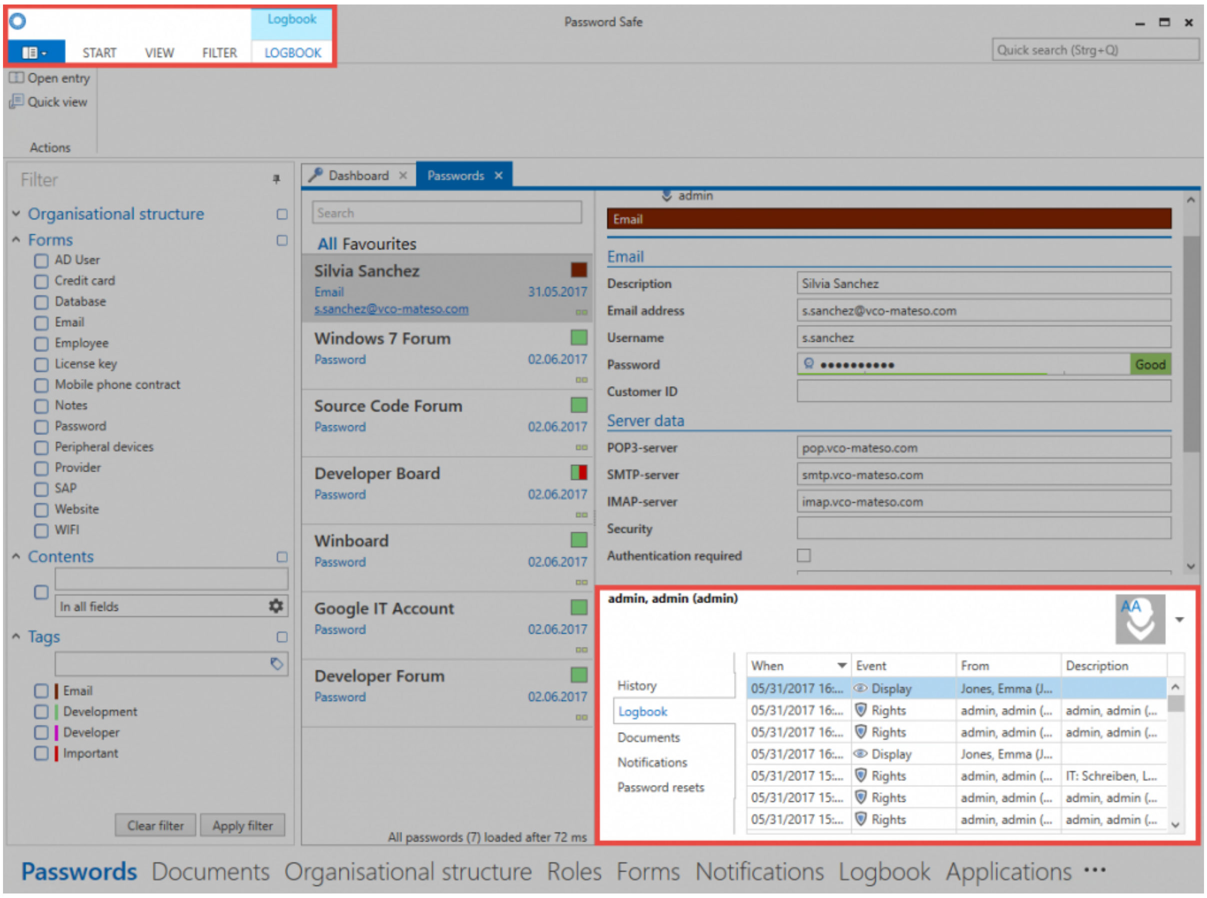
Access to the client main menu (backstage)

The button at the top left of the ribbon provides access to the client settings:



Ribbon tabs

There are tabs in the header area of the ribbon that summarize all available operations. By default, module-independent * Start, View, and Filter * is available. If the footer of the reading pane is opened **(1)**, further tabs will be visible in the ribbon **(2)**. These contain, according to the selection made in the footer, other possible actions.



Silvia Sanchez
Email 31.05.2017
s.sanchez@vco-mateso.com

Windows 7 Forum
Password 02.06.2017

Source Code Forum
Password 02.06.2017

Developer Board
Password 02.06.2017

Winboard
Password 02.06.2017

Google IT Account
Password 02.06.2017

Developer Forum
Password 02.06.2017

All passwords (7) loaded after 72 ms

Email

Description	Silvia Sanchez
Email address	s.sanchez@vco-mateso.com
Username	s.sanchez
Password	•••••••••• Good
Customer ID	

Server data

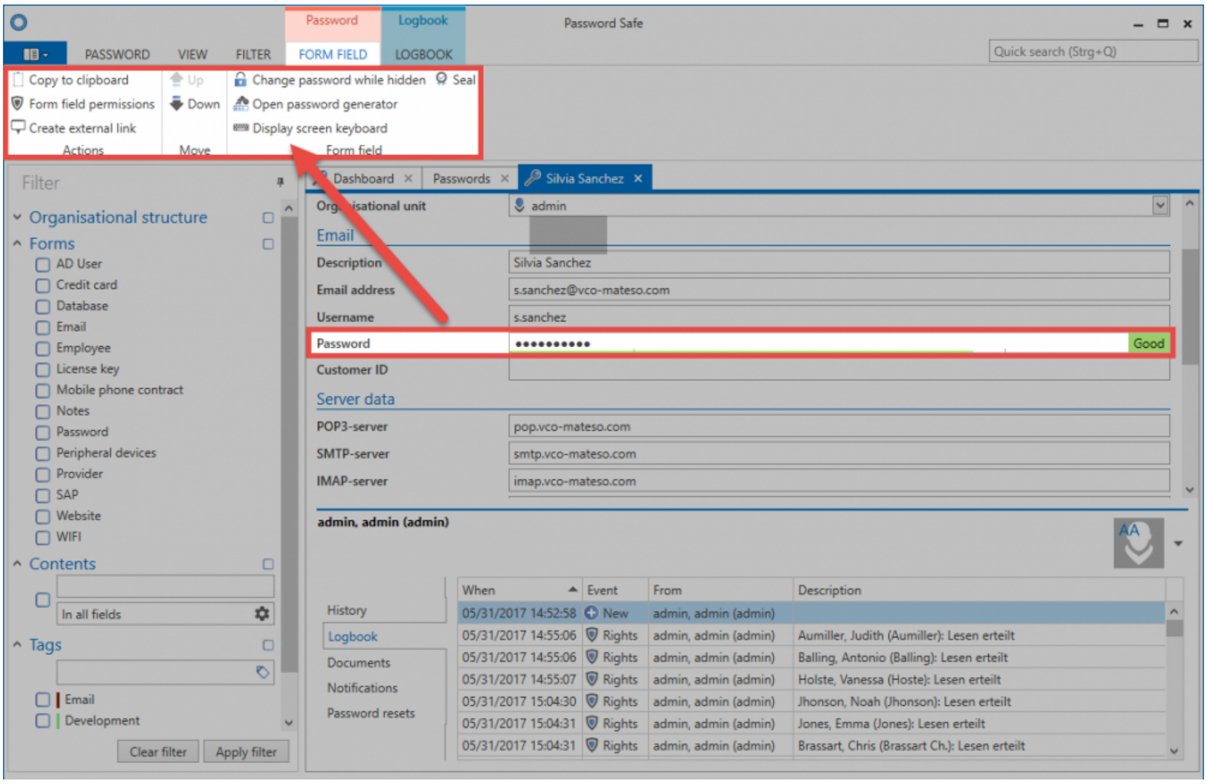
POP3-server	pop.vco-mateso.com
SMTP-server	smtp.vco-mateso.com
IMAP-server	imap.vco-mateso.com
Security	
Authentication required	□

admin, admin (admin)

When	Event	From	Description
05/31/2017 16:...	Display	Jones, Emma (J...	
05/31/2017 16:...	Rights	admin, admin (...	admin, admin (...
05/31/2017 16:...	Rights	admin, admin (...	admin, admin (...
05/31/2017 16:...	Display	Jones, Emma (J...	
05/31/2017 15:...	Rights	admin, admin (...	IT: Schreiben, L...
05/31/2017 15:...	Rights	admin, admin (...	admin, admin (...
05/31/2017 15:...	Rights	admin, admin (...	admin, admin (...

Content tabs

Double-clicking on an object in the List view opens a new tab with its detailed view. Depending on which form field you have selected, the corresponding content tab opens in the ribbon.



Organisational unit: admin

Email

Description	Silvia Sanchez
Email address	s.sanchez@vco-mateso.com
Username	s.sanchez
Password	•••••••••• Good
Customer ID	

Server data

POP3-server	pop.vco-mateso.com
SMTP-server	smtp.vco-mateso.com
IMAP-server	imap.vco-mateso.com

admin, admin (admin)

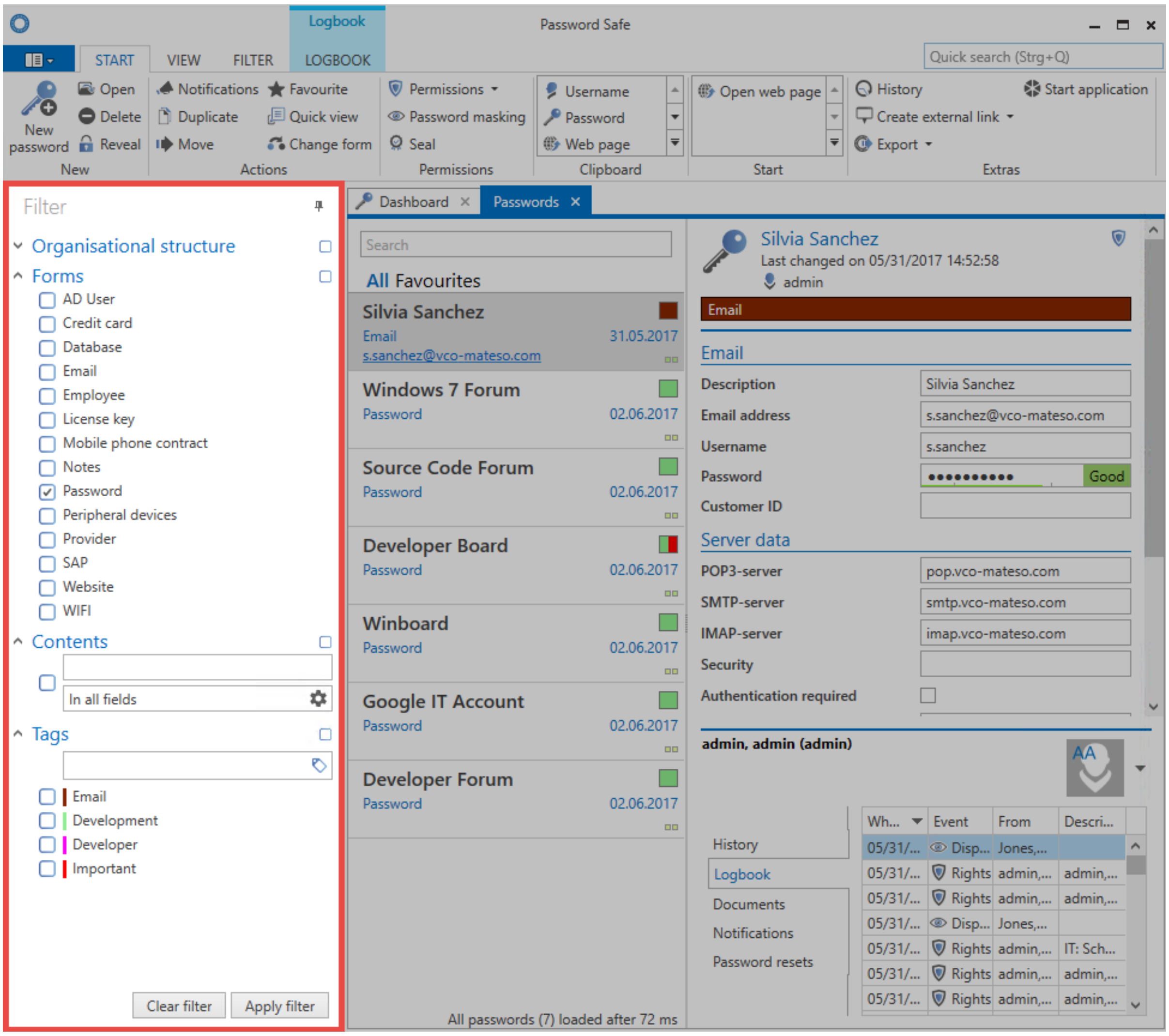
When	Event	From	Description
05/31/2017 14:52:58	New	admin, admin (admin)	
05/31/2017 14:55:06	Rights	admin, admin (admin)	Aumiller, Judith (Aumiller): Lesen erteilt
05/31/2017 14:55:06	Rights	admin, admin (admin)	Balling, Antonio (Balling): Lesen erteilt
05/31/2017 14:55:07	Rights	admin, admin (admin)	Holste, Vanessa (Hoste): Lesen erteilt
05/31/2017 15:04:30	Rights	admin, admin (admin)	Jhonson, Noah (Jhonson): Lesen erteilt
05/31/2017 15:04:31	Rights	admin, admin (admin)	Jones, Emma (Jones): Lesen erteilt
05/31/2017 15:04:31	Rights	admin, admin (admin)	Brassart, Chris (Brassart Ch.): Lesen erteilt

Depending on the selected form field, further actions are offered in the Content tab. In the Password field, this is, for example, calling the password generator or the screen keyboard, or the possibility to copy it to the clipboard.

Filter

What is a filter?

The freely configurable filters of the PSR client provide all methods for easy retrieval of stored data. The filter criteria are always adapted according to the module in which you are currently located. When you select one or several search criteria, and click on “Apply filter”, the results will be displayed in the list view. If necessary, this process can be repeated as desired and further restrictions can be added.



Silvia Sanchez	Email	31.05.2017
s.sanchez@vco-mateso.com		
Windows 7 Forum	Password	02.06.2017
Source Code Forum	Password	02.06.2017
Developer Board	Password	02.06.2017
Winboard	Password	02.06.2017
Google IT Account	Password	02.06.2017
Developer Forum	Password	02.06.2017

All passwords (7) loaded after 72 ms

Silvia Sanchez
Last changed on 05/31/2017 14:52:58
admin

Email

Email

Description	Silvia Sanchez
Email address	s.sanchez@vco-mateso.com
Username	s.sanchez
Password	●●●●●●●●●●● Good
Customer ID	

Server data

POP3-server	pop.vco-mateso.com
SMTP-server	smtp.vco-mateso.com
IMAP-server	imap.vco-mateso.com
Security	
Authentication required	□

admin, admin (admin)

Wh...	Event	From	Descri...
05/31/...	Disp...	Jones,...	
05/31/...	Rights	admin,...	admin,...
05/31/...	Rights	admin,...	admin,...
05/31/...	Disp...	Jones,...	
05/31/...	Rights	admin,...	IT: Sch...
05/31/...	Rights	admin,...	admin,...
05/31/...	Rights	admin,...	admin,...

Who is allowed to use the filter?

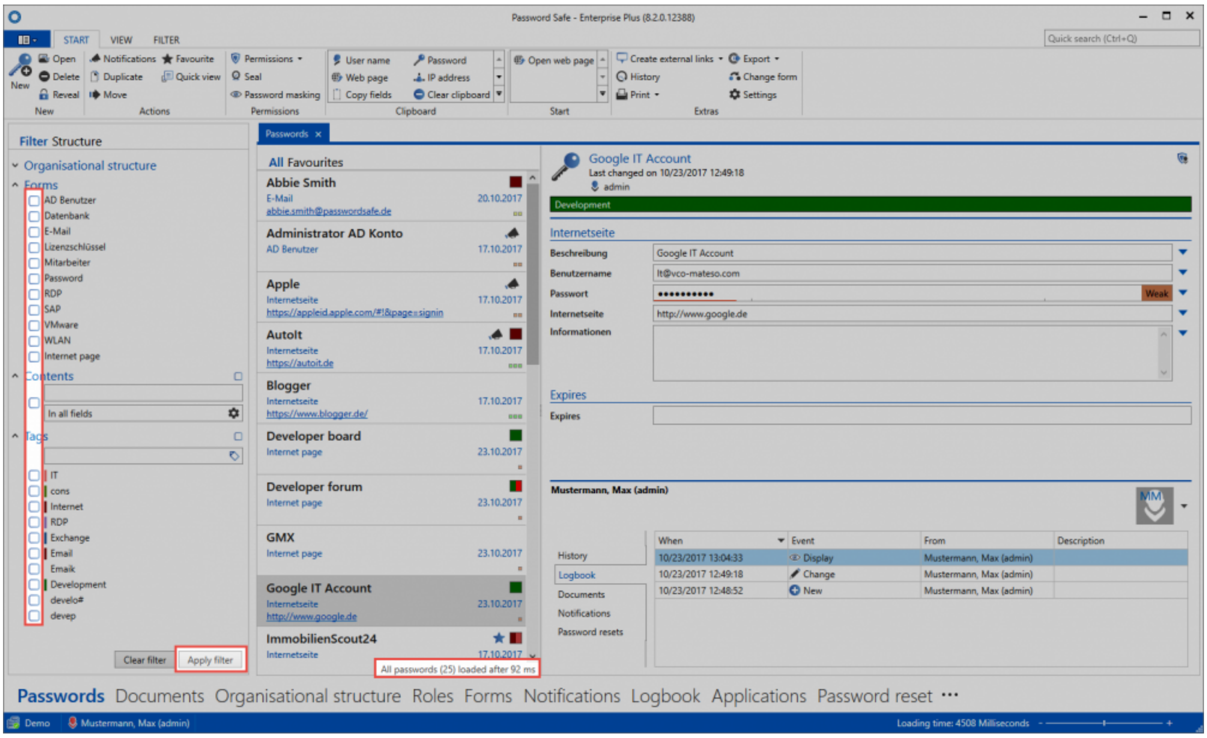
The filter is an indispensable working tool because of the possibility to restrict existing results according to individual requirements. Consequently, all users can use the filter. It is, of course, possible to place restrictions for filter criteria. This means that the possible filter criteria can be restricted for individual employees by means of permissions. For example, an employee could filter for the form **password** only if it had read permission for that form.

> ! There are no authorizations for tags. That means, any employee can use any tags. The display order in the filter is determined by the frequency of use. This handling is not safety-critical, since tags do not grant any permissions. They are merely a supportive measure for filtering.

Application example

Filter without criteria

By selecting the required criteria and applying the filter using the button of the same name, the set of all the records corresponding to the criteria is displayed in the list view. If you used the filter **without criteria**, you would obtain a list of all data records to which you are entitled in general.



Abbie Smith – E-Mail – abbie.smith@passwordsafe.de – 20.10.2017
Administrator AD Konto – AD Benutzer – 17.10.2017
Apple – Internetseite – https://appleid.apple.com/#!&page=signin – 17.10.2017
AutoIt – Internetseite – https://autoit.de – 17.10.2017
Blogger – Internetseite – https://www.blogger.de/ – 17.10.2017
Developer board – Internet page – 23.10.2017
Developer forum – Internet page – 23.10.2017
GMX – Internet page – 23.10.2017
Google IT Account – Internetseite – http://www.google.de – 23.10.2017
ImmobilienScout24 – Internetseite – 17.10.2017

All passwords (25) loaded after 92 ms

Google IT Account
Last changed on 10/23/2017 12:49:18
admin
Development

Internetseite
Beschreibung: Google IT Account
Benutzername: lt@vco-mateso.com
Passwort: ●●●●●●●●●●● Weak
Internetseite: http://www.google.de
Informationen:

Expires
Expires:

Mustermann, Max (admin)

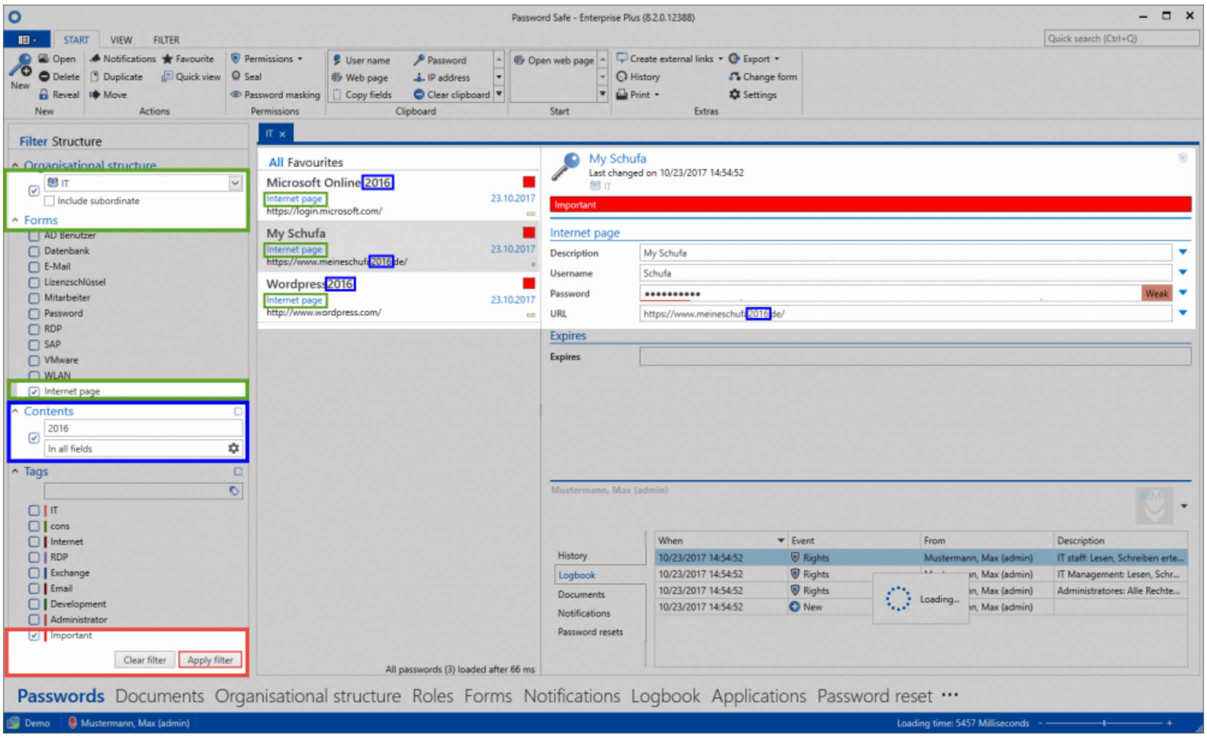
History
Logbook
Documents
Notifications
Password resets

When	Event	From	Description
10/23/2017 13:04:33	Display	Mustermann, Max (admin)	
10/23/2017 12:49:18	Change	Mustermann, Max (admin)	
10/23/2017 12:48:52	New	Mustermann, Max (admin)	

As you can see, 133 records are not really manageable. In most situations you will need to reduce the number of records by adding filters.

Adding filter criteria

The filter **organization** can be applied directly to the authorizations to restrict the number of records according to the authorizations granted. In this case, the logged-on user holds rights for various areas. However, it would like to see only those records which are assigned to the **Own passwords** area within the organisational structure. In addition, there should be further restrictions, which could be formulated as in the following sentence: “Deliver all records from my own passwords that were created with the form **password** and which contain the expression **2016** and the tag **Administrator**.



Filter Structure

Organisational structure
☑ IT
☐ Include subordinate

Forms
☐ AD Benutzer
☐ Datenbank
☐ E-Mail
☐ Lizenzschlüssel
☐ Mitarbeiter
☐ Password
☐ RDP
☐ SAP
☐ VMware
☐ WLAN
☑ Internet page

Contents
☑ 2016
In all fields

Tags
☐ IT
☐ cons
☐ Internet
☐ RDP
☐ Exchange
☐ Email
☐ Development
☐ Administrator
☑ Important

Clear filter | Apply filter

All Favourites

Microsoft Online 2016 Internet page https://login.microsoft.com/	23.10.2017
My Schufa Internet page https://www.meineschufa2016de/	23.10.2017
Wordpress 2016 Internet page http://www.wordpress.com/	23.10.2017

All passwords (3) loaded after 66 ms

My Schufa
Last changed on 10/23/2017 14:54:52
IT
Important

Internet page
Description: My Schufa
Username: Schufa
Password: •••••••••• Weak
URL: https://www.meineschufa2016de/

Expires
Expires:

Mustermann, Max (admin)

History
Logbook
Documents
Notifications
Password resets

When	Event	From	Description
10/23/2017 14:54:52	Rights	Mustermann, Max (admin)	IT staff: Lesen, Schreiben erte...
10/23/2017 14:54:52	Rights	...n, Max (admin)	IT Management: Lesen, Schr...
10/23/2017 14:54:52	Rights	...n, Max (admin)	Administratores: Alle Rechte...
10/23/2017 14:54:52	New	...n, Max (admin)	

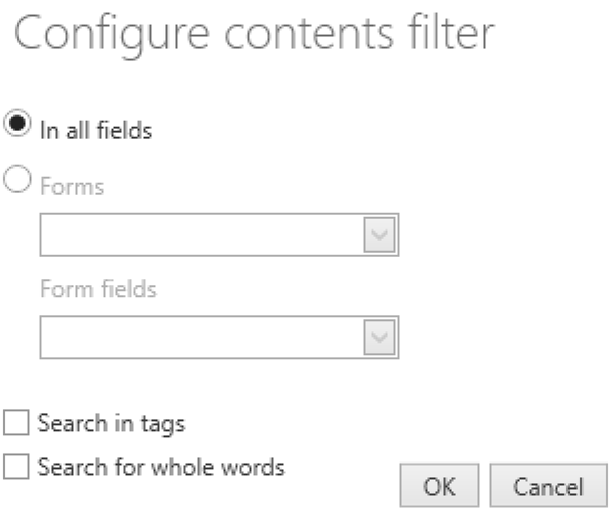
Loading...

As can be seen, the filter delivers the desired results. The extent to which the filter criteria match the three remaining data sets is assigned in colour.

> ! When filtering with several criteria, such as forms, content and tags, all filter criteria must be complied with. It is therefore a logical “AND operation”. Other possible operation types are described in detail in the Advanced Filter Settings.

Content filter

The term * 2016 * is part of the description in the * My Schufa * record, part of the description of * Wordpress 2016 * and Microsoft Online 2016 **. Since the search *“in all fields”** is activated in the content filter, all three records are included in the results, and are displayed in the list view. You can also configure the content filter to search for expressions in a specific field. The icon next to the expression **“in all fields”** opens the content filter configuration in a modal window. As you can see it was configured that the content filter should only have the form * password *, and only the form field * Internet address * should be considered:



Configure contents filter

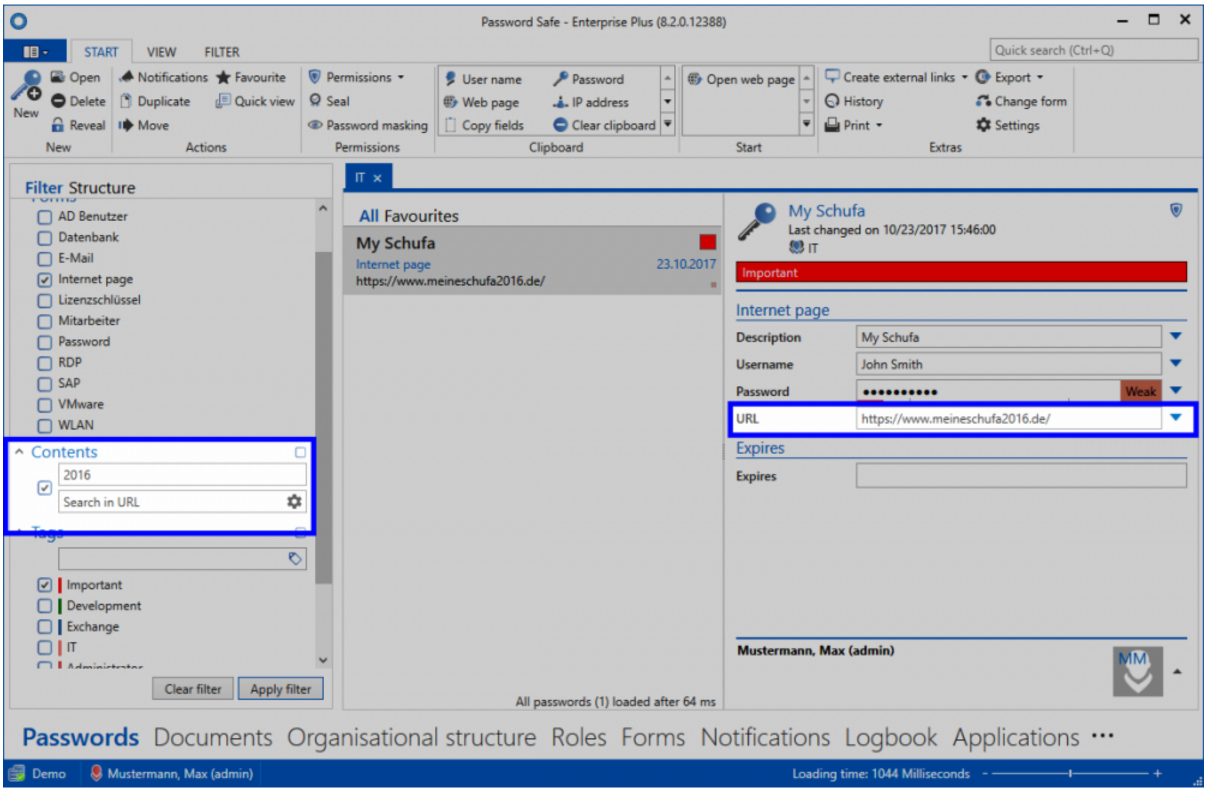
● In all fields

○ Forms

Form fields

□ Search in tags

□ Search for whole words



Password Safe - Enterprise Plus (8.2.0.12388)

Filter Structure

Forms
- □ AD Benutzer
- □ Datenbank
- □ E-Mail
- ☑ Internet page
- □ Lizenzschlüssel
- □ Mitarbeiter
- □ Password
- □ RDP
- □ SAP
- □ VMware
- □ WLAN

Contents
- ☑ 2016
- Search in URL

Tags
- ☑ Important
- □ Development
- □ Exchange
- □ IT
- □ Administrator

All Favourites

My Schufa
Internet page 23.10.2017
https://www.meineschufa2016.de/

All passwords (1) loaded after 64 ms

My Schufa
Last changed on 10/23/2017 15:46:00
IT

Important

Internet page

Description	My Schufa
Username	John Smith
Password	•••••••••• Weak
URL	https://www.meineschufa2016.de/

Expires

Expires

Mustermann, Max (admin)

Demo Mustermann, Max (admin) Loading time: 1044 Milliseconds

It is very easy to abstract, because of the present example, that the filter can be adapted to your personal requirements. It is thus the most important tool to be able to retrieve data once stored in the database.

> ! The effectiveness of the filter is closely linked to data integrity. Only when data is kept clean, efficient operation with the filter is ensured. It is important that employees are trained in the correct handling of the filter tool as well as when creating the data records.

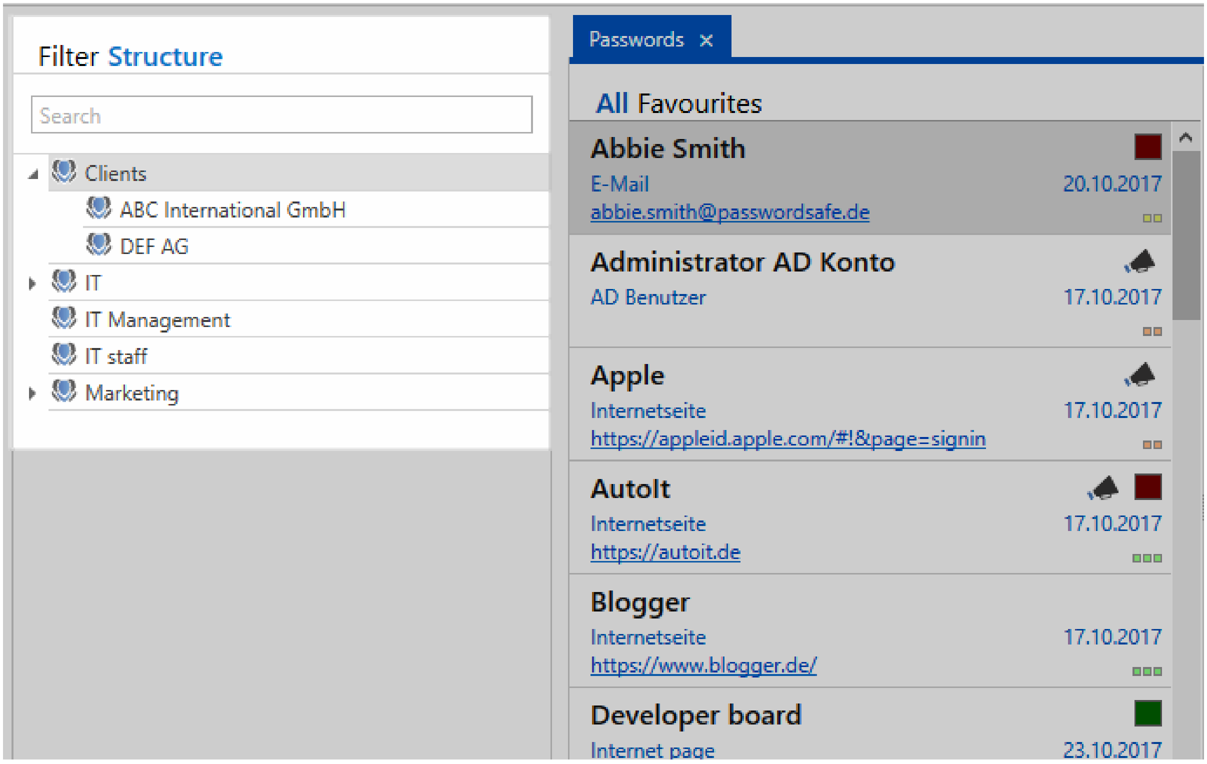
Workshops show the best success rate in this context. If you require further information, “contact us“mailto: sales@passwordsafe.de.

Display mode

What display modes exist?

In addition to the already described filter, it is possible to switch to structure view. This alternative view enables you to filter solely on the basis of the organisational structure. Although this type of filtering is also possible in standard filter view, you are able to directly see the complete organisational structure in structure view.

> As there are no longer any folders in Password Safe version 8, the structure view can not mirror all of the functionalities of the folder view in version 7. However, the structure view has been modelled on the folder view to make the changeover from the previous version easier.



Abbie Smith
E-Mail 20.10.2017
abbie.smith@passwordsafe.de

Administrator AD Konto
AD Benutzer 17.10.2017

Apple
Internetseite 17.10.2017
https://appleid.apple.com/#!&page=signin

AutoIt
Internetseite 17.10.2017
https://autoit.de

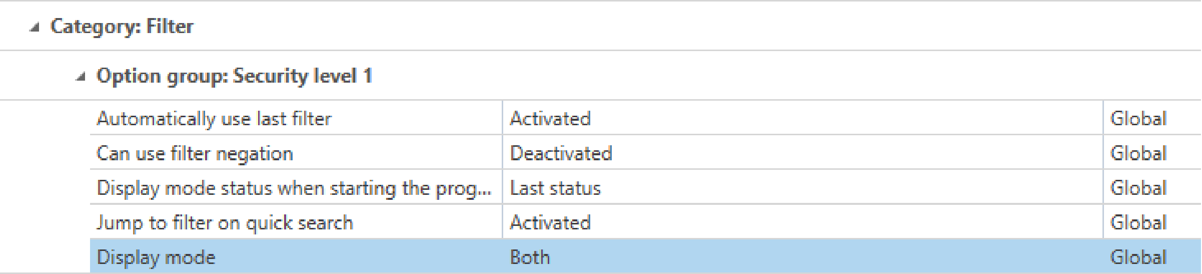
Blogger
Internetseite 17.10.2017
https://www.blogger.de/

Developer board
Internet page 23.10.2017

As you can see, only the organisational structure is visible in this view. This view is the ideal choice for users who want to work in a highly structural-based manner.

Relevant options

There are three relevant settings associated with the display mode:



◢ Category: Filter

◢ Option group: Security level 1

Automatically use last filter	Activated	Global
Can use filter negation	Deactivated	Global
Display mode status when starting the prog...	Last status	Global
Jump to filter on quick search	Activated	Global
Display mode	Both	Global

- **Display mode**: It is possible to define whether the standard filter, structure filter or both are displayed. If the last option is selected, you can switch between both views.
- **Jump to filter on quick search**: If you are using structure view, it is possible to define whether the system should automatically jump to the standard filter if you click the quick search (top right in the client)
- **Display mode status when starting the program**: This setting defines which display mode is displayed as default when starting the program.

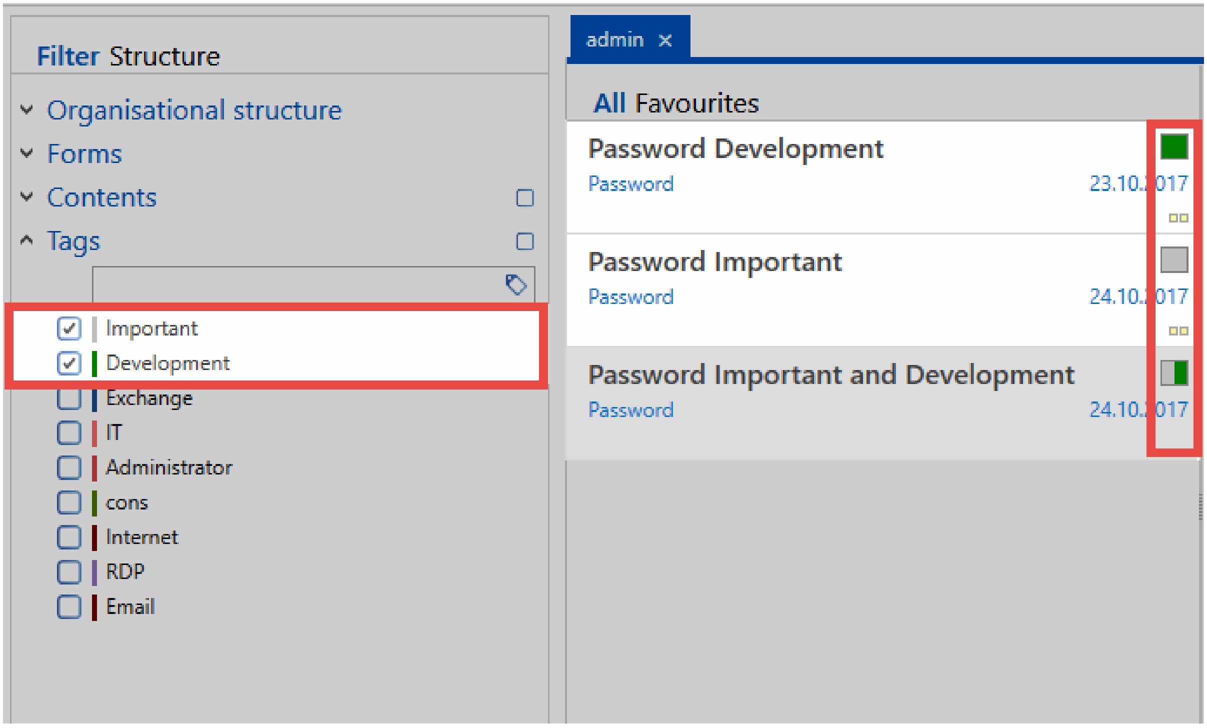
Advanced filter settings

Linking filters

The two options, with which filter criteria can be linked, are easy to explain using the example of tags. The following options are available:

1. Logical “Or operator”

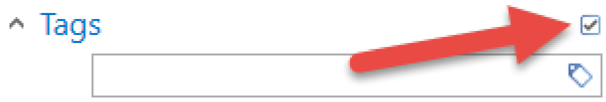
By default, the filter is active in this mode. In the following example, you want to find all records with at least one of the tags **“Important”** or **“Development”**. This also means that records can either have one of the tags, or both.

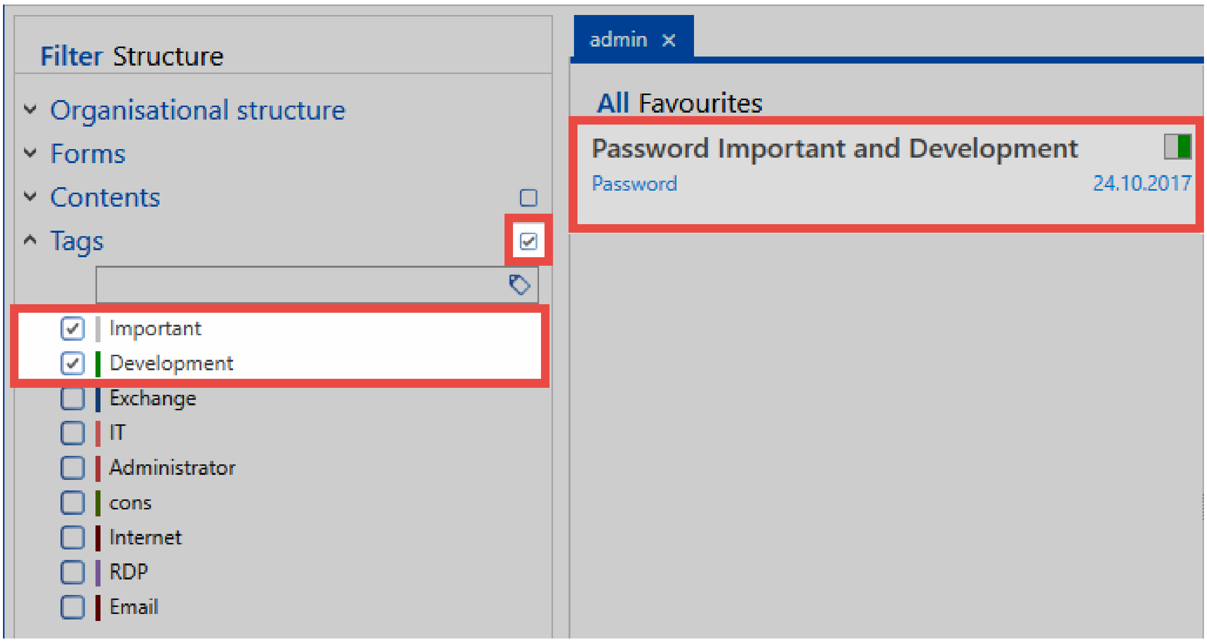


Due to the colour coding of the tags in the data records, it can be seen that the first two data records have one of the tags, while the third one has both tags. However, all three are included in the results. **At least one filter criterion must be met**.

2. Logical “And operator”

This mode is activated directly by the checkbox in the filter. Each filter criterion has its own checkbox.

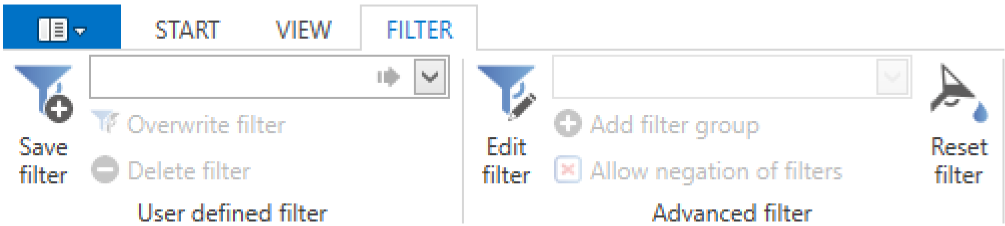




In contrast to the "OR link", the "AND link" must fulfil both criteria. Accordingly, in the present example, only the records that have both the tag **"important"** and the tag **"development"** are listed with the results.

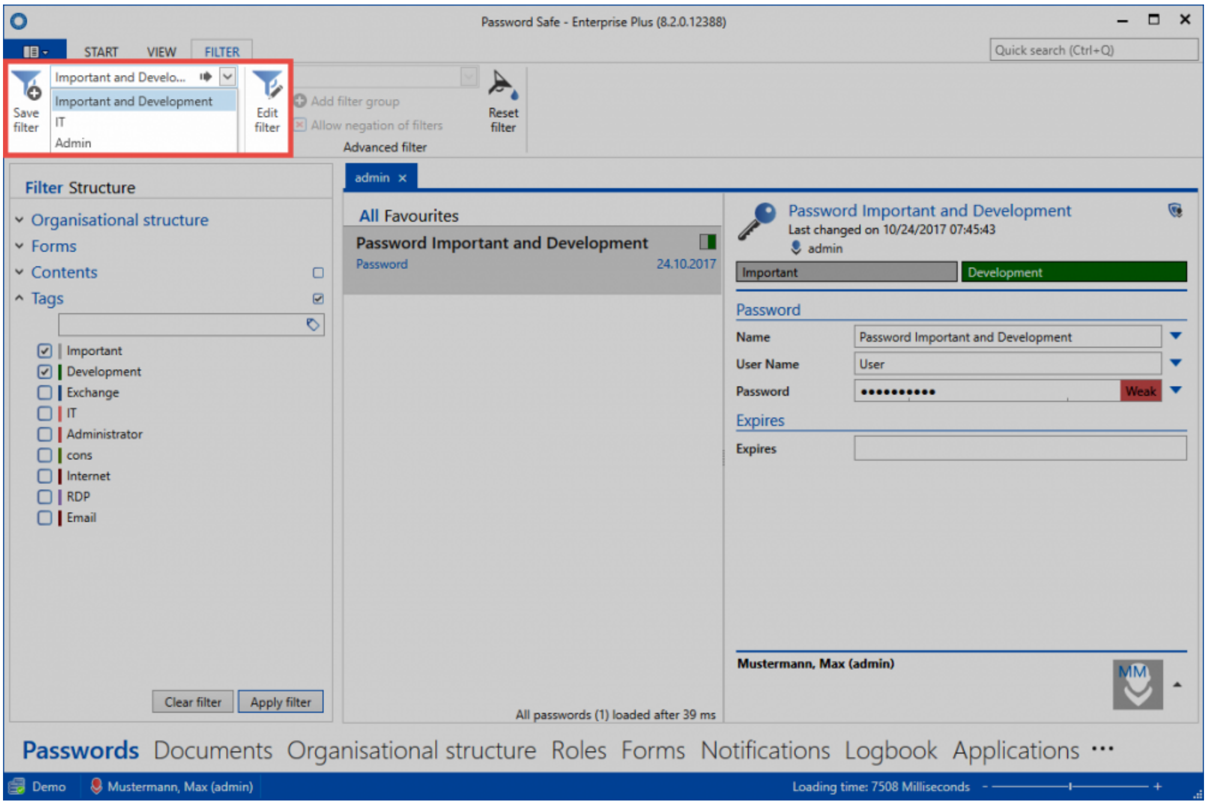
Filter tab in the ribbon

The filter management can also be found in the ribbon. Here, for example, you can expand the currently configured filter criteria, save the filter, or simply clear all currently applied filters.



Saving, editing, and deleting filters

In many cases, it is recommended to store defined filters. In this way, it is possible to make efficient use of filter results from previous searches. The button "**Save filter**" prompts you directly to assign a meaningful name for this filter. The filter is saved according to the criteria currently configured in the filter. This filter is now listed in the selection menu and can now be selected. Note that a selected filter selection is immediately applied to the filter but is not automatically executed. The filter must be used for this purpose. Both the button in the ribbon, so also the counterpart in the filter, lead to the same result here.

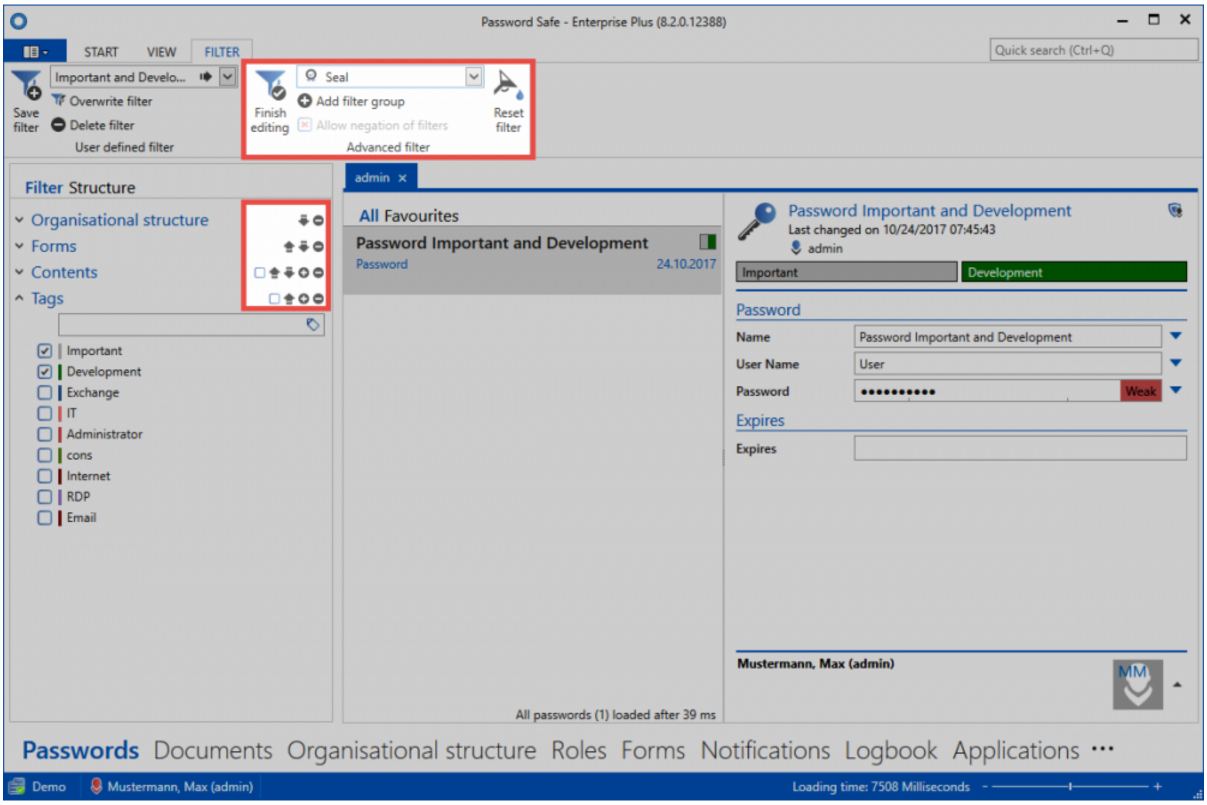


Deleting and overwriting existing filters is identical in the procedure. The filter, which has been marked in the selection field, is always deleted. If an existing filter is to be overwritten, the name of the filter is retained and is overwritten with the filter criteria currently configured in the filter.

———————————

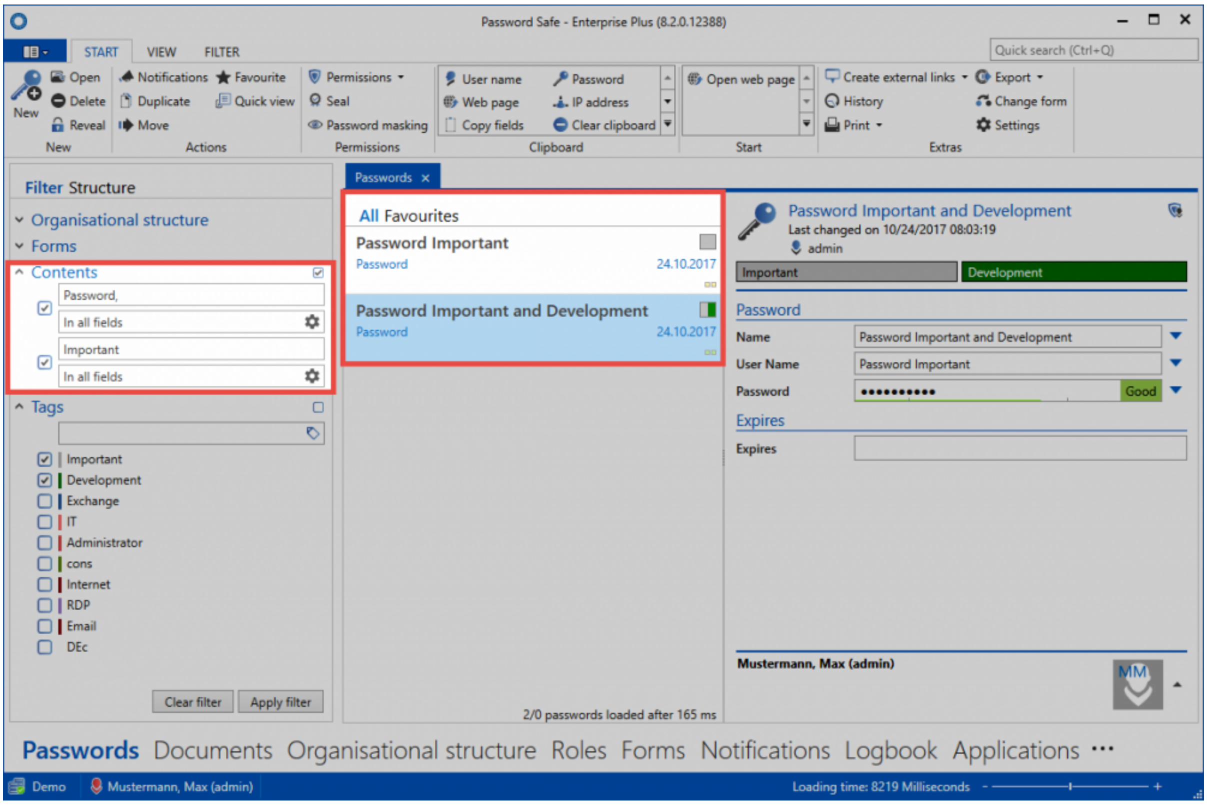
Advanced filter

In the “Extended filter” category you can adjust the filter as desired, eg by adding or removing filter groups. Clicking on **“Edit filter”** activates the processing mode. You can terminate it with **“Finish editing”**.



New filter groups can now be added via the selection field. For this purpose, the desired filter type is selected (in the example, the filter group is the seal). The process is completed by **“adding a filter group”**. Newly added filter groups are always placed at the very bottom of the filter.

In **Edit mode**, the filter view changes, in addition to the possible actions in the ribbon. Use the arrow buttons to adjust the order of the filter groups. The icons “Plus” and “Minus” can be used to create additional instances of existing filter groups or to remove existing ones. In the following example, a content filter was added and all other filter groups removed.

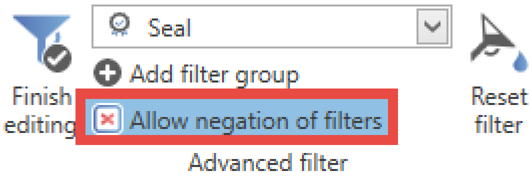


Name: Password Important and Development
User Name: Password Important
Password: •••••••••• Good
Expires:

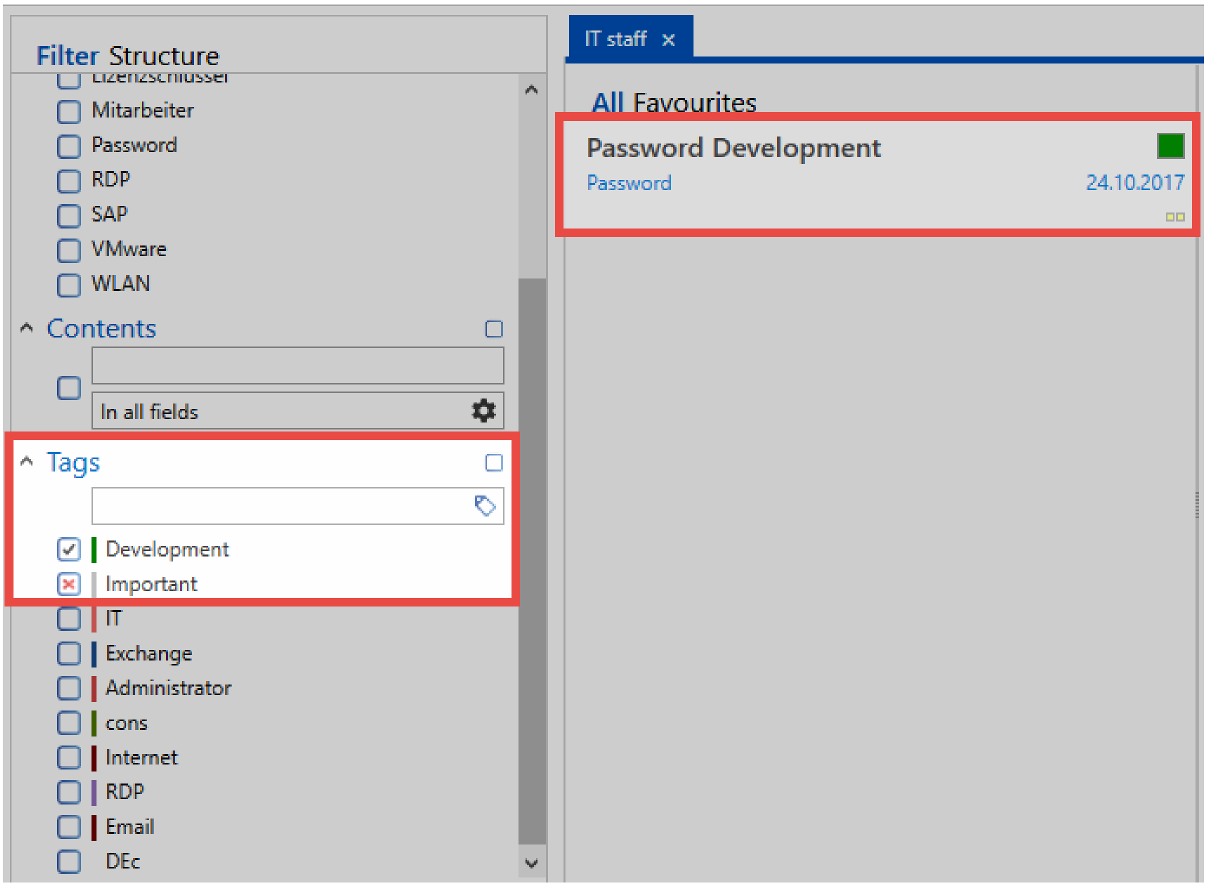
In this example, only the content filter is used – in two instances! * The “And” link will now display all records that contain both the word “password” and the phrase “important”. *

Negation of filters

In Edit mode, there is also the possibility to negate criteria.



It is thus possible to refine very precisely filter results even further. This becomes more and more important when there are a large number of records in the database and the resulting amount of data is still unmanageable despite the fact that filters has been appropriately defined.



Negations are defined directly in the checkbox of an element within a filter group. Without negations, you can only search e.g. for a tag. Negations make the following queries possible:

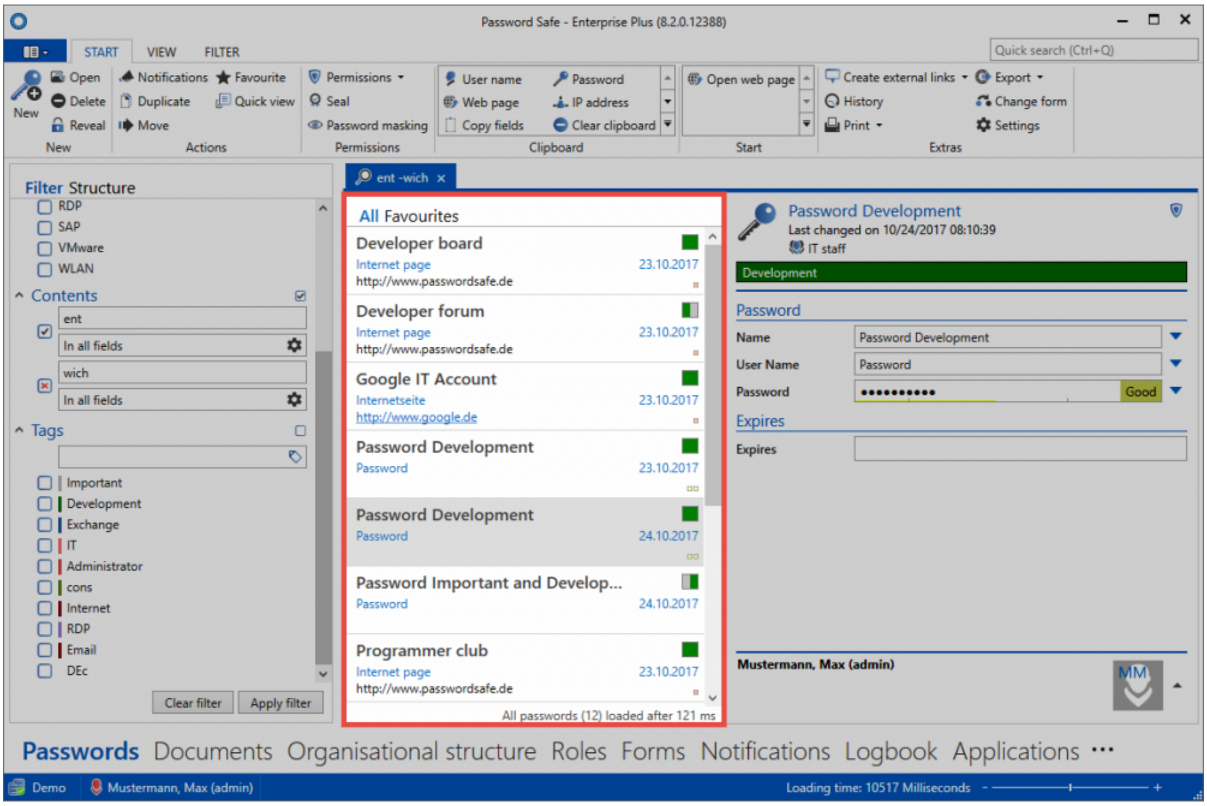
“Deliver all records that have the tag “development” but are not tagged with “important”!”

> ! In order to effectively use negations, it is important that “and links” are always enabled. Otherwise operations with negations cannot be modelled mathematically.

List view

What is the list view?

The list view is located centrally in the Password Safe client, and is a key element of daily work. There are also list views in Windows operating systems. If you click on a folder in Windows Explorer, the contents of the folder are displayed in a list view. The same is true in Password Safe version 8. However, instead of folders, the content of the list view is defined by the currently applied filter. * This always means that the list view is the result of a filtered filter *. For the currently marked record in list view, all existing form fields are output to the reading pane. With the two tabs "All" and "Favourites, the filter results can be further restricted.



Filter: ☐ RDP ☐ SAP ☐ VMware ☐ WLAN; Contents ☑ ent – In all fields; ☒ wich – In all fields; Tags: ☐ Important ☐ Development ☐ Exchange ☐ IT ☐ Administrator ☐ cons ☐ Internet ☐ RDP ☐ Email ☐ DEc

Developer board – Internet page – http://www.passwordsafe.de – 23.10.2017
Developer forum – Internet page – http://www.passwordsafe.de – 23.10.2017
Google IT Account – Internetseite – http://www.google.de – 23.10.2017
Password Development – Password – 23.10.2017
Password Development – Password – 24.10.2017
Password Important and Develop... – Password – 24.10.2017
Programmer club – Internet page – http://www.passwordsafe.de – 23.10.2017
All passwords (12) loaded after 121 ms

Password Development
Last changed on 10/24/2017 08:10:39
IT staff
Development
Password
Name: Password Development
User Name: Password
Password: •••••••••• Good
Expires
Expires:
Mustermann, Max (admin)

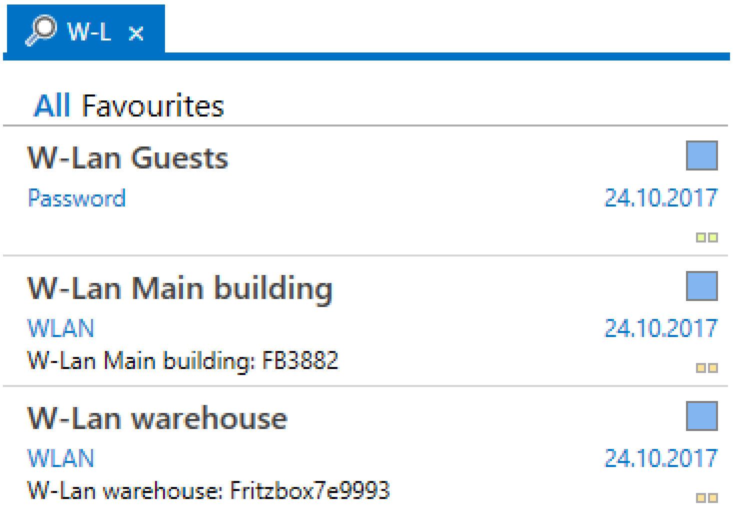
Demo | Mustermann, Max (admin) | Loading time: 10517 Milliseconds

At the bottom of the list view, the number of loaded records and the time required for this are shown.

> For more than 100 list elements, only the first 100 records are displayed by default. This is to prevent excessive database queries where the results are unmanageable. In this case, it makes sense to further refine the filter criteria. By pressing the "All" button in the header of the list view, you can still manually switch to the complete list.

Searching in list view

Through the search field, the results found by the filter can be further refined as required. After you have entered the search term, the results are automatically limited to those records which correspond to the criteria (after about half a second). The search used for the search is highlighted in yellow.



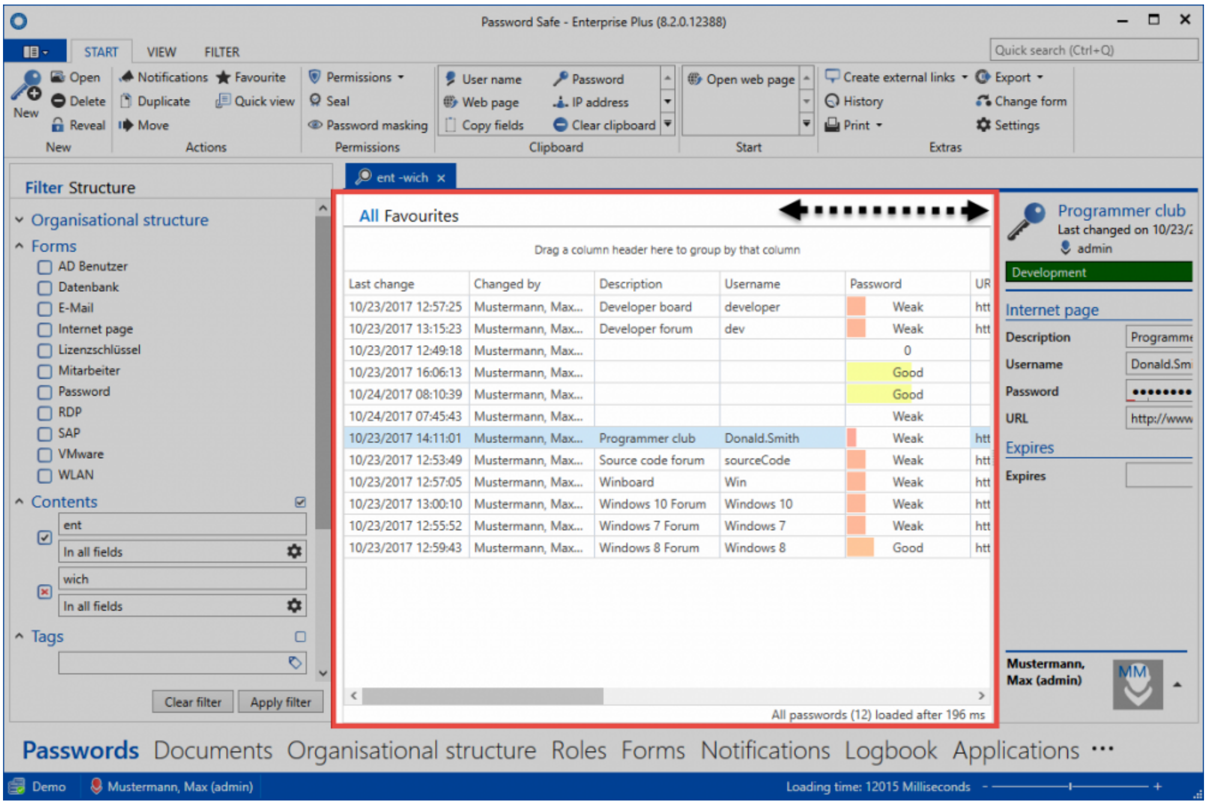
W-Lan Guests
Password 24.10.2017

W-Lan Main building
WLAN 24.10.2017
W-Lan Main building: FB3882

W-Lan warehouse
WLAN 24.10.2017
W-Lan warehouse: Fritzbox7e9993

Detailed list view

The default view displays only limited information about the records. However, the width of the list view is flexible and can be adjusted by mouse. At a certain point, the view automatically changes to the detailed list view, similar to the procedure in Microsoft Outlook. All form fields are displayed



Forms:
- □ AD Benutzer
- □ Datenbank
- □ E-Mail
- □ Internet page
- □ Lizenzschlüssel
- □ Mitarbeiter
- □ Password
- □ RDP
- □ SAP
- □ VMware
- □ WLAN

Contents:
- ☑ ent — In all fields
- ☒ wich — In all fields

All Favourites

Drag a column header here to group by that column

Last change	Changed by	Description	Username	Password	UR
10/23/2017 12:57:25	Mustermann, Max...	Developer board	developer	Weak	htt
10/23/2017 13:15:23	Mustermann, Max...	Developer forum	dev	Weak	htt
10/23/2017 12:49:18	Mustermann, Max...			0	
10/23/2017 16:06:13	Mustermann, Max...			Good	
10/24/2017 08:10:39	Mustermann, Max...			Good	
10/24/2017 07:45:43	Mustermann, Max...			Weak	
10/23/2017 14:11:01	Mustermann, Max...	Programmer club	Donald.Smith	Weak	htt
10/23/2017 12:53:49	Mustermann, Max...	Source code forum	sourceCode	Weak	htt
10/23/2017 12:57:05	Mustermann, Max...	Winboard	Win	Weak	htt
10/23/2017 13:00:10	Mustermann, Max...	Windows 10 Forum	Windows 10	Weak	htt
10/23/2017 12:55:52	Mustermann, Max...	Windows 7 Forum	Windows 7	Weak	htt
10/23/2017 12:59:43	Mustermann, Max...	Windows 8 Forum	Windows 8	Good	htt

All passwords (12) loaded after 196 ms

Programmer club
Last changed on 10/23/2
admin
Development

Internet page

Description	Programme
Username	Donald.Smi
Password	•••••••••
URL	http://www

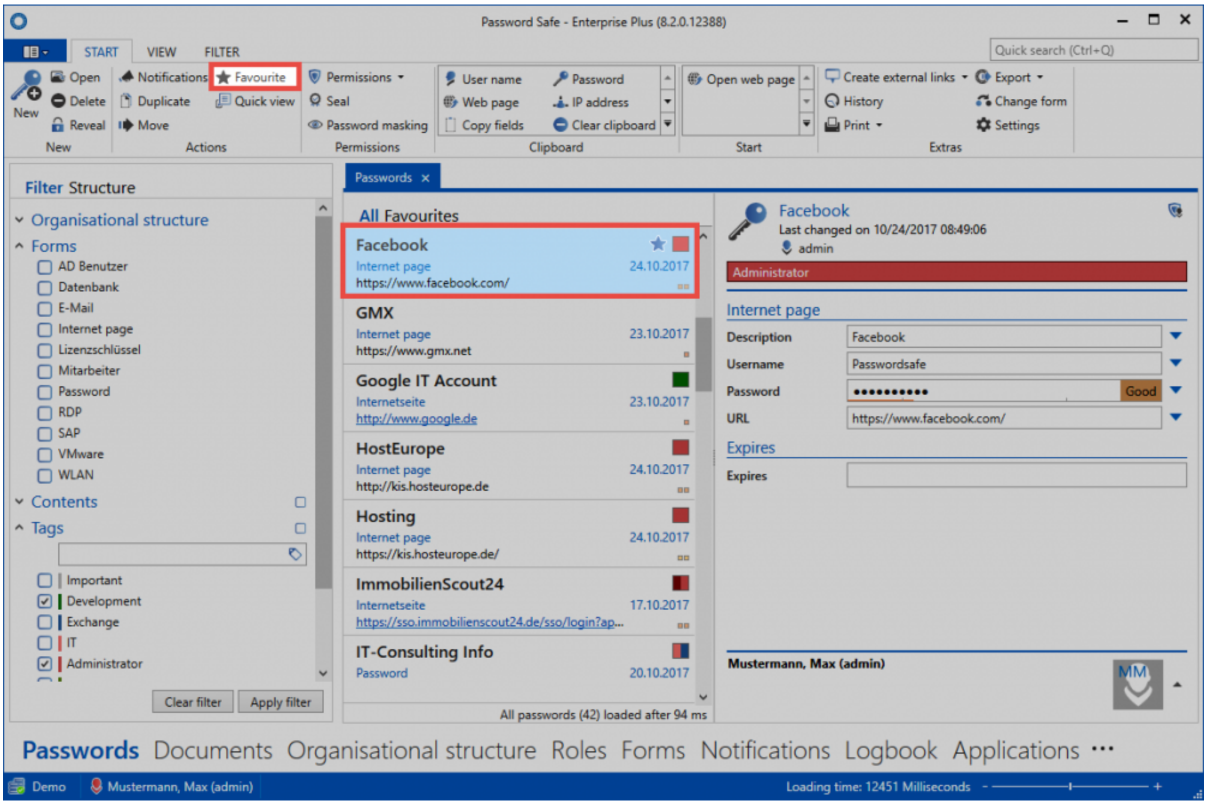
Expires

Expires	

Mustermann, Max (admin)

Favourites

Regularly used records can be marked as favourites. This process is carried out directly in the ribbon. A record marked as a favourite is indicated with a star in list view.



Forms:
- ☐ AD Benutzer
- ☐ Datenbank
- ☐ E-Mail
- ☐ Internet page
- ☐ Lizenzschlüssel
- ☐ Mitarbeiter
- ☐ Password
- ☐ RDP
- ☐ SAP
- ☐ VMware
- ☐ WLAN

Tags:
- ☐ Important
- ☑ Development
- ☐ Exchange
- ☐ IT
- ☑ Administrator

All Favourites

Facebook	Internet page	24.10.2017
	https://www.facebook.com/	
GMX	Internet page	23.10.2017
	https://www.gmx.net	
Google IT Account	Internetseite	23.10.2017
	http://www.google.de	
HostEurope	Internet page	24.10.2017
	http://kis.hosteurope.de	
Hosting	Internet page	24.10.2017
	https://kis.hosteurope.de/	
ImmobilienScout24	Internetseite	17.10.2017
	https://sso.immobilienscout24.de/sso/login?ap...	
IT-Consulting Info	Password	20.10.2017

All passwords (42) loaded after 94 ms

Facebook
Last changed on 10/24/2017 08:49:06
admin
Administrator

Internet page

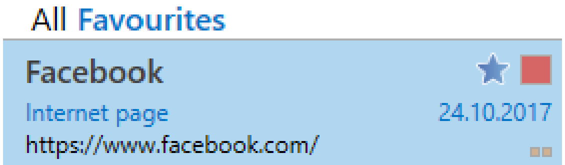
Description	Facebook
Username	Passwordsafe
Password	●●●●●●●●●● Good
URL	https://www.facebook.com/

Expires

Expires	

Mustermann, Max (admin)

You can filter for favourites directly in the list view. For this purpose, simply switch to the **“Favourites”** tab.

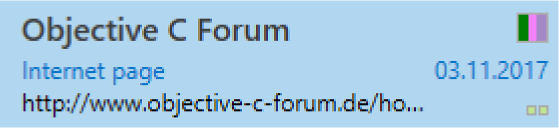


All Favourites

Facebook
Internet page 24.10.2017
https://www.facebook.com/

Other symbols

Every record displayed in list view has multiple icons on the right. These give feedback in colour about both the password quality and the tags used. Mouseover tooltips provide more precise details.

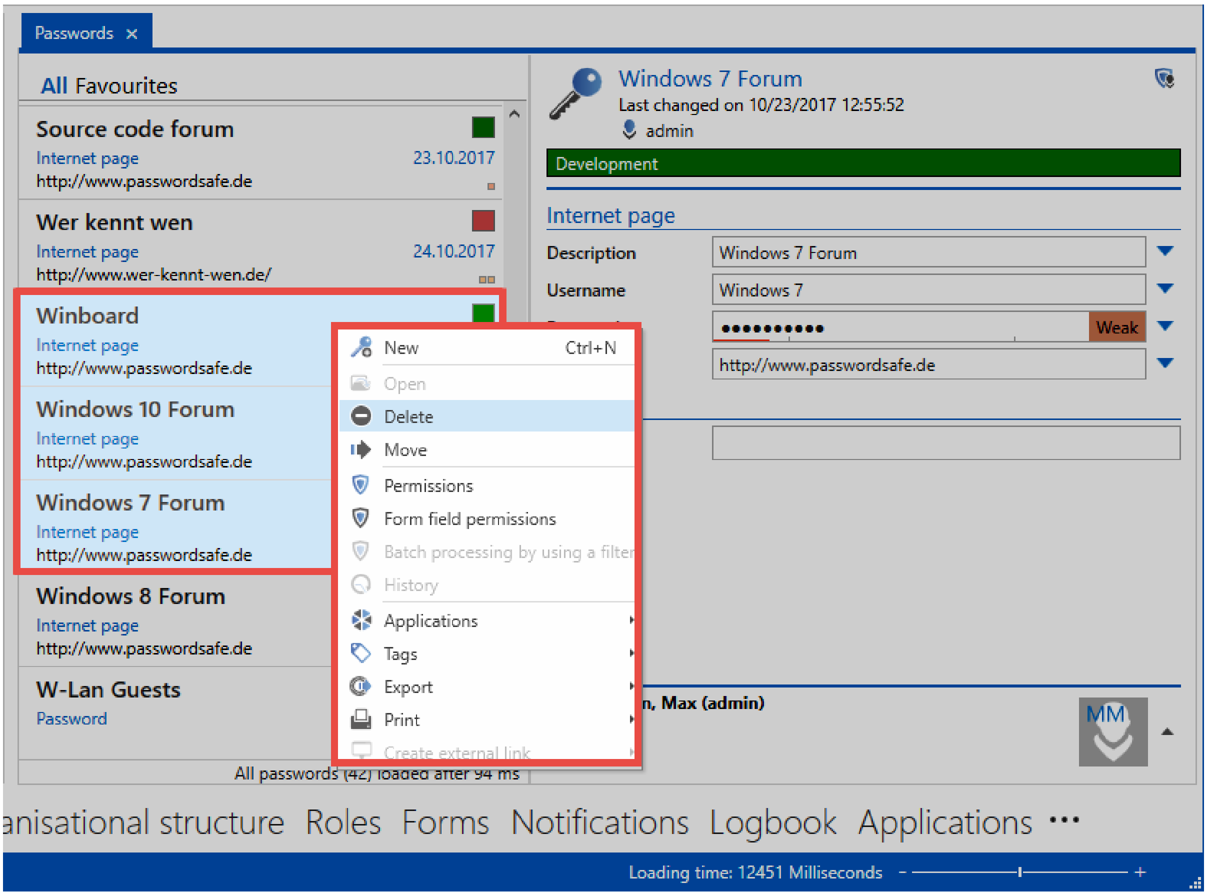


Objective C Forum
Internet page 03.11.2017
http://www.objective-c-forum.de/ho...

> The information visible underneath the password name is taken from the info field for the associated form and will be explained separately

Working with records

All records that correspond to the filter criteria are now displayed in list view. These can now be opened, edited, or deleted via the ribbon. Many functions are also available directly from the context menu. You can do this by right-clicking the record. Multiple selection is also possible. To do this, simply highlight the desired objects by holding down the Ctrl key.



Passwords ×

All Favourites

Source code forum
Internet page 23.10.2017
http://www.passwordsafe.de

Wer kennt wen
Internet page 24.10.2017
http://www.wer-kennt-wen.de/

Winboard
Internet page
http://www.passwordsafe.de

Windows 10 Forum
Internet page
http://www.passwordsafe.de

Windows 7 Forum
Internet page
http://www.passwordsafe.de

Windows 8 Forum
Internet page
http://www.passwordsafe.de

W-Lan Guests
Password

All passwords (42) loaded after 94 ms

Windows 7 Forum
Last changed on 10/23/2017 12:55:52
admin

Development

Internet page

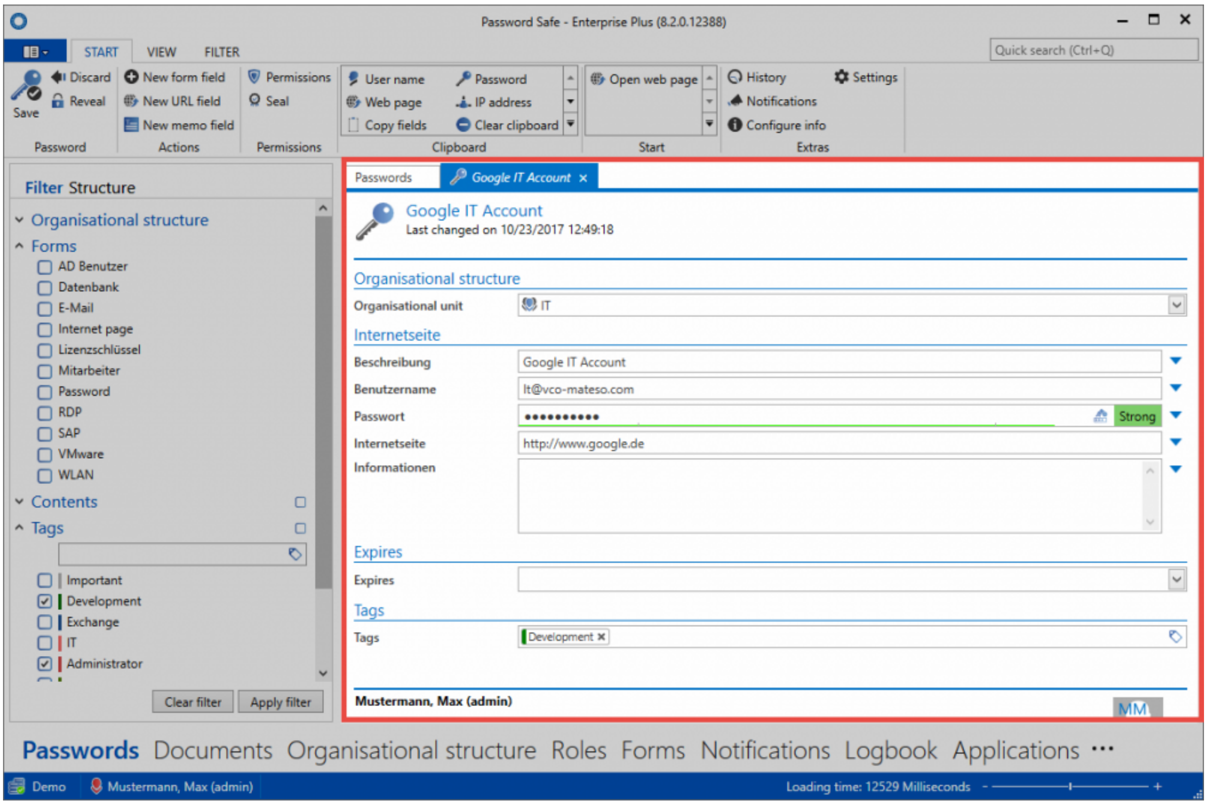
Description: Windows 7 Forum
Username: Windows 7
●●●●●●●●●● Weak
http://www.passwordsafe.de

n, Max (admin)

Loading time: 12451 Milliseconds

Opening and editing data sets

By double-clicking, as with the context menu (right mouse button), all records can be opened from the list view in a separate tab. Only in this view can you make changes. This detail view opens in a separate tab, the list view is completely hidden.



Google IT Account
Last changed on 10/23/2017 12:49:18

Organisational structure

Organisational unit: IT

Internetseite

Beschreibung: Google IT Account

Benutzername: It@vco-mateso.com

Passwort: •••••••••• Strong

Internetseite: http://www.google.de

Informationen:

Expires

Expires:

Tags

Tags: Development

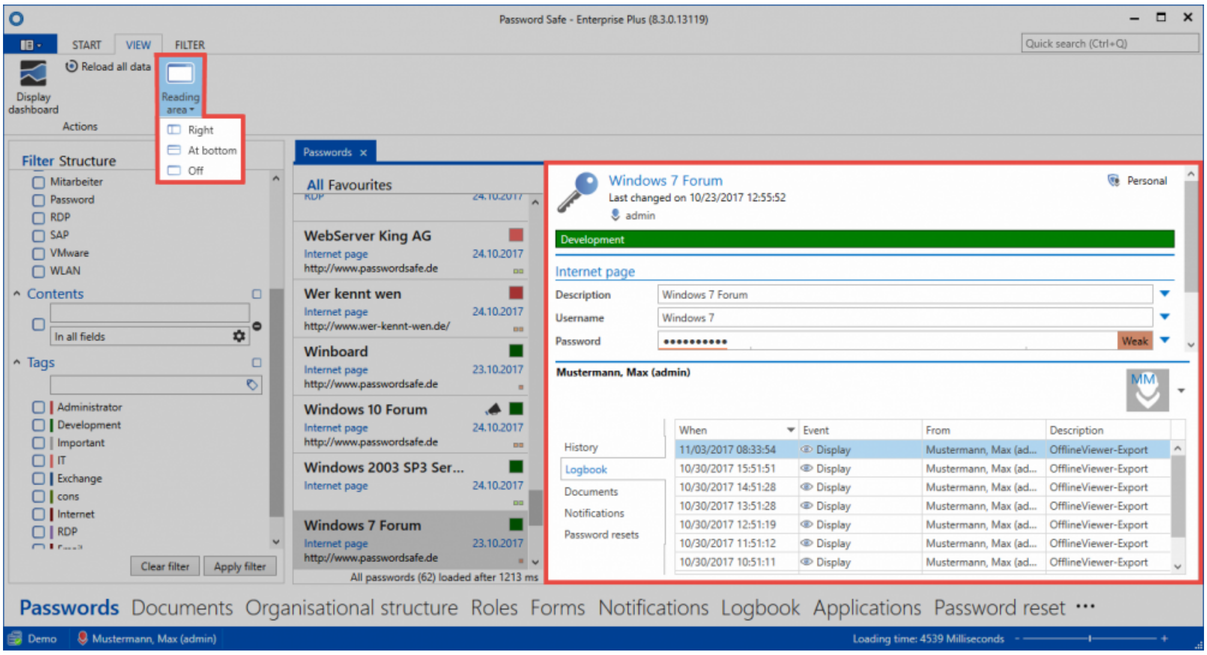
Mustermann, Max (admin)

✻ Working with data records depends of course on the type of the data record. Whether passwords, documents or organisational structures: The handling is partly very different. For more information, please refer to the respective sections on the individual "modules".:#psr-client

Reading pane

What is the reading pane?

The reading pane on the right side of the client always corresponds to the detailed view of the selected record in the list view and can be completely deactivated via the ribbon. In addition, you can configure here the arrangement of the reading pane – either on the right, or underneath thelist view.



Windows 7 Forum
Last changed on 10/23/2017 12:55:52
admin

Description: Windows 7 Forum
Username: Windows 7
Password: •••••••••• Weak

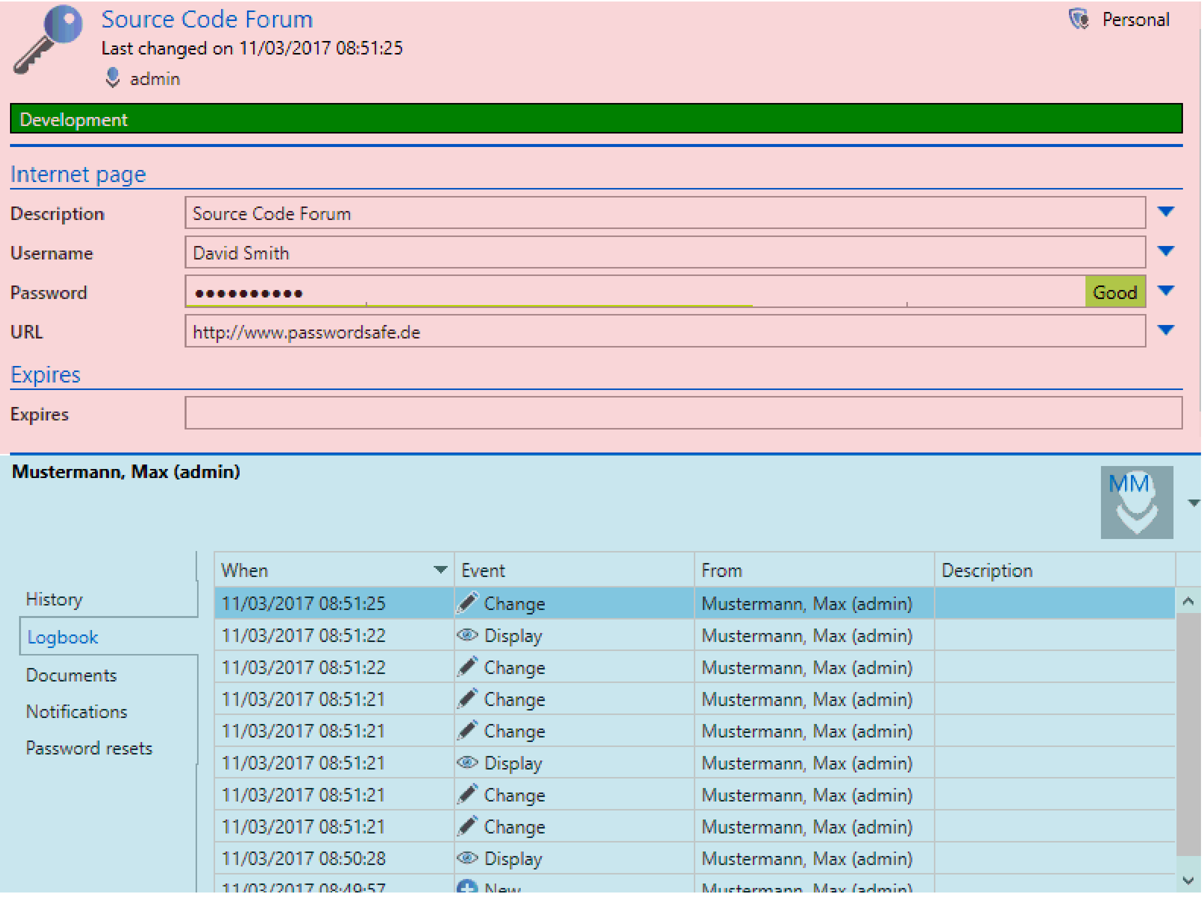
Mustermann, Max (admin)

When	Event	From	Description
11/03/2017 08:33:54	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 15:51:51	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 14:51:28	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 13:51:28	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 12:51:19	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 11:51:12	Display	Mustermann, Max (ad...	OfflineViewer-Export
10/30/2017 10:51:11	Display	Mustermann, Max (ad...	OfflineViewer-Export

Structure of the reading pane

The reading pane is divided into two areas:

1. **Details area**
2. **Footer area**



Source Code Forum
Last changed on 11/03/2017 08:51:25
admin

Internet page

Description: Source Code Forum
Username: David Smith
Password: ●●●●●●●●●● Good
URL: http://www.passwordsafe.de

Expires

Expires:

Mustermann, Max (admin)

When	Event	From	Description
11/03/2017 08:51:25	Change	Mustermann, Max (admin)	
11/03/2017 08:51:22	Display	Mustermann, Max (admin)	
11/03/2017 08:51:22	Change	Mustermann, Max (admin)	
11/03/2017 08:51:21	Change	Mustermann, Max (admin)	
11/03/2017 08:51:21	Change	Mustermann, Max (admin)	
11/03/2017 08:51:21	Display	Mustermann, Max (admin)	
11/03/2017 08:51:21	Change	Mustermann, Max (admin)	
11/03/2017 08:51:21	Change	Mustermann, Max (admin)	
11/03/2017 08:50:28	Display	Mustermann, Max (admin)	
11/03/2017 08:49:57	New	Mustermann, Max (admin)	

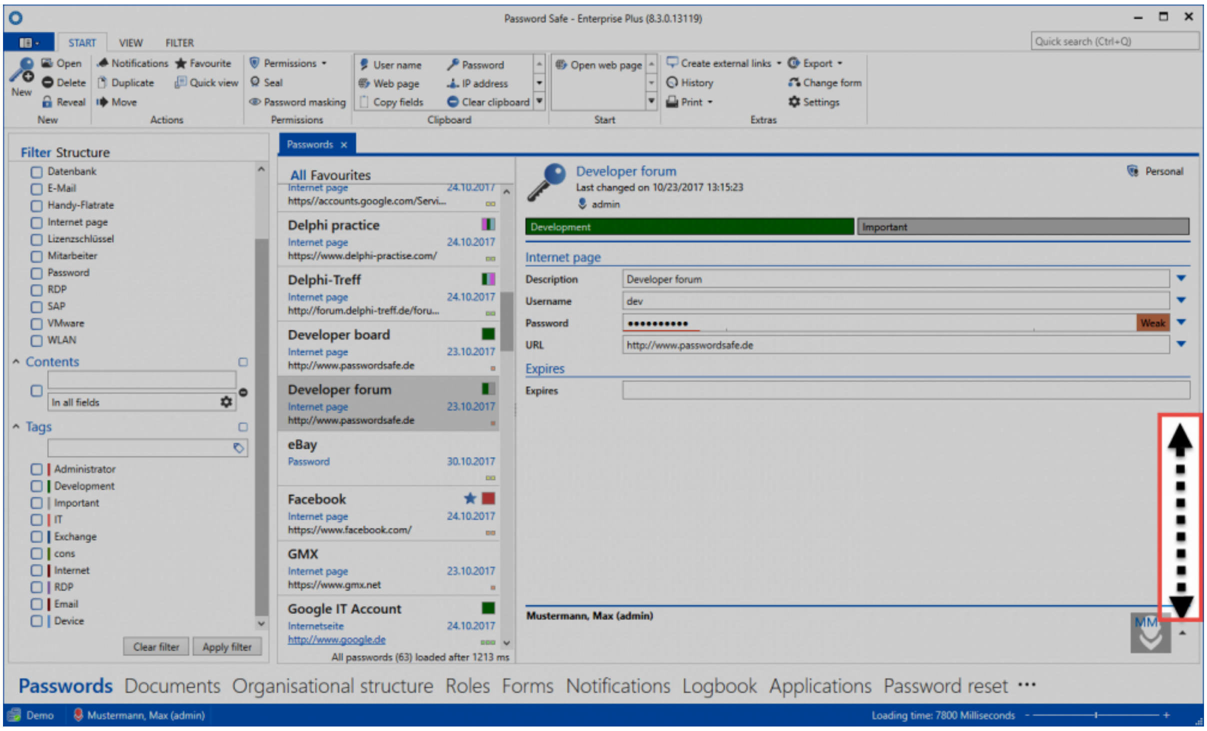
1. Details area

Depending on which record you have selected in “list view”:#listenansicht, the corresponding fields are displayed here. In the header, the assigned “tags”:#tags, as well as the “organisational structures”:#organisationsstrukturen are displayed.

! It should be noted that the details area cannot be used for editing records! Although it displays all of the data, editing is only possible if the record has been opened.

2. Footer area

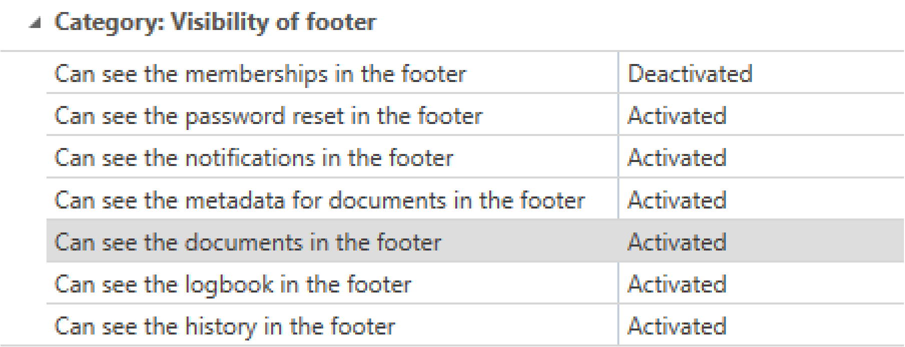
In the footer area of the reading pane, it is possible to display various information for the currently selected record. The button can be activated via the button provided. It is hidden by default.


Password Safe - Enterprise Plus (8.3.0.13119)
START VIEW FILTER
Quick search (Ctrl+Q)
New Open Delete Reveal Notifications Duplicate Move Favourite Quick view Actions
Permissions Seal Password masking Permissions
User name Web page Copy fields Password IP address Clear clipboard Clipboard
Open web page Start
Create external links History Print Export Change form Settings Extras
Filter Structure
Datenbank
E-Mail
Handy-Flatrate
Internet page
Lizenzschlüssel
Mitarbeiter
Password
RDP
SAP
VMware
WLAN
Contents
In all fields
Tags
Administrator
Development
Important
IT
Exchange
cons
Internet
RDP
Email
Device
Clear filter Apply filter
Passwords
All Favourites
Internet page https://accounts.google.com/Servi... 24.10.2017
Delphi practice Internet page 24.10.2017 https://www.delphi-practise.com/
Delphi-Treff Internet page 24.10.2017 http://forum.delphi-treff.de/foru...
Developer board Internet page 23.10.2017 http://www.passwordsafe.de
Developer forum Internet page 23.10.2017 http://www.passwordsafe.de
eBay Password 30.10.2017
Facebook Internet page 24.10.2017 https://www.facebook.com/
GMX Internet page 23.10.2017 https://www.gmx.net
Google IT Account Internetseite 24.10.2017 http://www.google.de
All passwords (63) loaded after 1213 ms
Developer forum
Last changed on 10/23/2017 13:15:23
admin
Personal
Development Important
Internet page
Weak
Expires
Mustermann, Max (admin)
MM
Passwords Documents Organisational structure Roles Forms Notifications Logbook Applications Password reset ···
Demo Mustermann, Max (admin) Loading time: 7800 Milliseconds

Description: Developer forum
Username: dev
Password: ••••••••••
URL: http://www.passwordsafe.de
Expires:

The logbook, linked documents, history, notifications and password resets can be accessed separately here via the tabs. The individual elements can be viewed with a double-click, as well as by using the quick view (space bar). Double clicking always opens a separate tab, the quick view merely opens a modal window.

Visibility of the individual tabs within the footer section is secured via separate "user rights":#globale-benutzerrechte:



◢ Category: Visibility of footer

Can see the memberships in the footer	Deactivated
Can see the password reset in the footer	Activated
Can see the notifications in the footer	Activated
Can see the metadata for documents in the footer	Activated
Can see the documents in the footer	Activated
Can see the logbook in the footer	Activated
Can see the history in the footer	Activated

The same options can also be found in the settings. A tab is only displayed if it has been activated both in the rights and also in the settings. This makes it possible to specify (for example via the administrator) whether a user is permitted to view the tab or not. The user can then define themselves which tabs they want to be displayed.

Tags

What are tags?

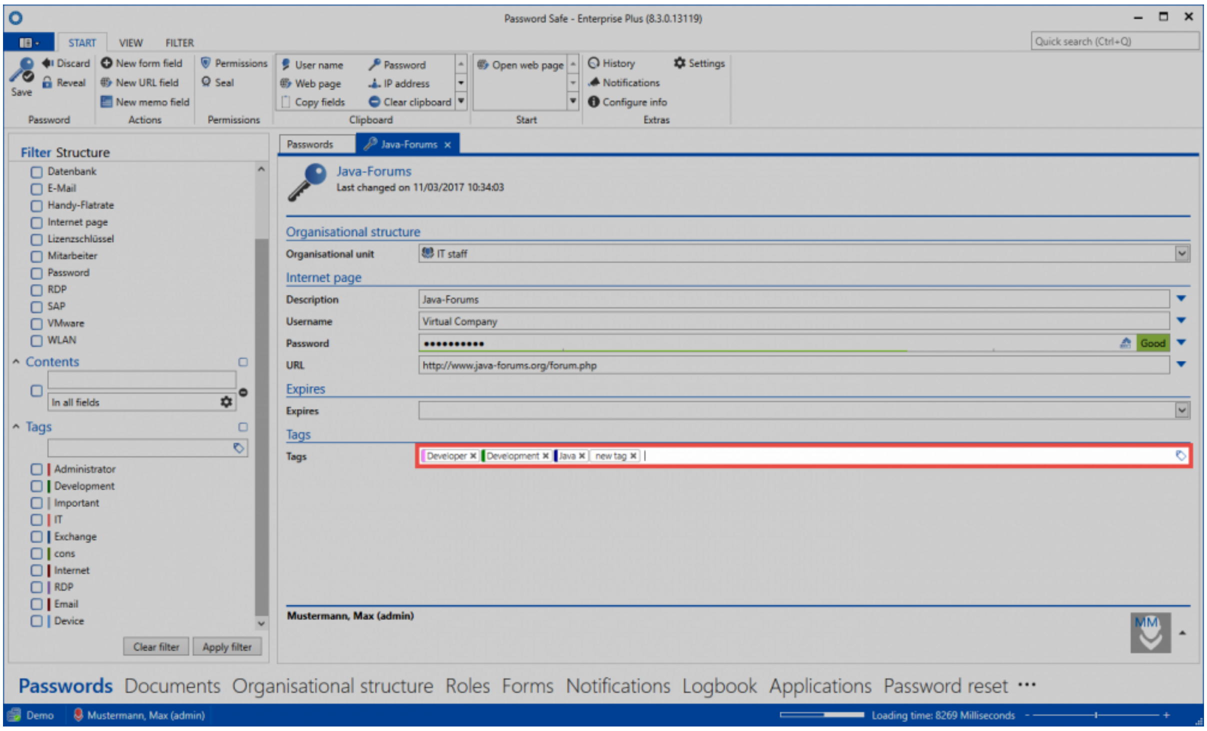
The tag system is ubiquitous in Password Safe. It can be used to classify and describe almost every object. An object can have several such tags. These are always displayed in the header area of the data record. Optionally, tags can be provided with colours or a description. They determine the aesthetics of Password Safe, and are optically a great help, in order not to loose the overview even in case of large amounts of data.

Tags have no permissions. Any user can use any tag!

Adding tags to records

! The right **“Can add new tags”** is required to create new tags. This right is one of the user rights.

Tags can be directly added when creating new records and also when editing records. The procedure is the same. In Edit mode, the tags are always at the bottom.



Java-Forums
Last changed on 11/03/2017 10:34:03

Organisational structure
Organisational unit: IT staff

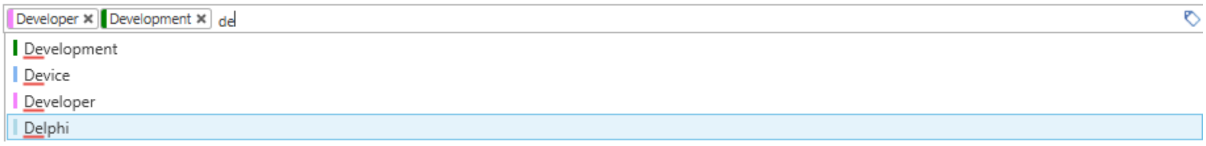
Internet page
Description: Java-Forums
Username: Virtual Company
Password: •••••••••• Good
URL: http://www.java-forums.org/forum.php

Expires
Expires:

Tags
Tags: Developer × Development × Java × new tag ×

Mustermann, Max (admin)

The operation is intuitive. From the third entered letter, existing tags are searched for full text. If the desired tag has been found, it can be added. Both the navigation with mouse, thus also with keyboard, is possible. If a new tag is to be created, this can be done directly with “Return”.

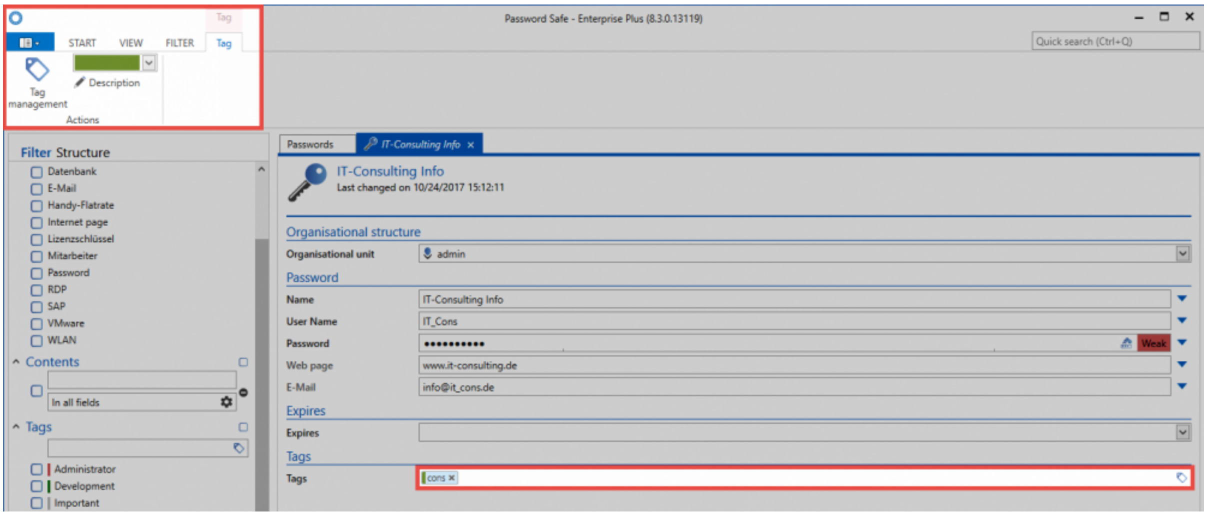


Developer × Development × de

- Development
- Device
- Developer
- Delphi

Tags in the ribbon

If you edit a record and mark an existing or new tag, a corresponding content tab appears in the ribbon. Here, the tag manager can be opened as well as the colour and description of the tag can be adapted directly.



IT-Consulting Info
Last changed on 10/24/2017 15:12:11

Organisational structure

Organisational unit: admin

Password

Name: IT-Consulting Info

User Name: IT_Cons

Password: •••••••••• Weak

Web page: www.it-consulting.de

E-Mail: info@it_cons.de

Expires

Expires:

Tags

Tags: cons ×

Management of tags

A separate section is available under Extras in the client for the tag manager. This is explained in a special section.

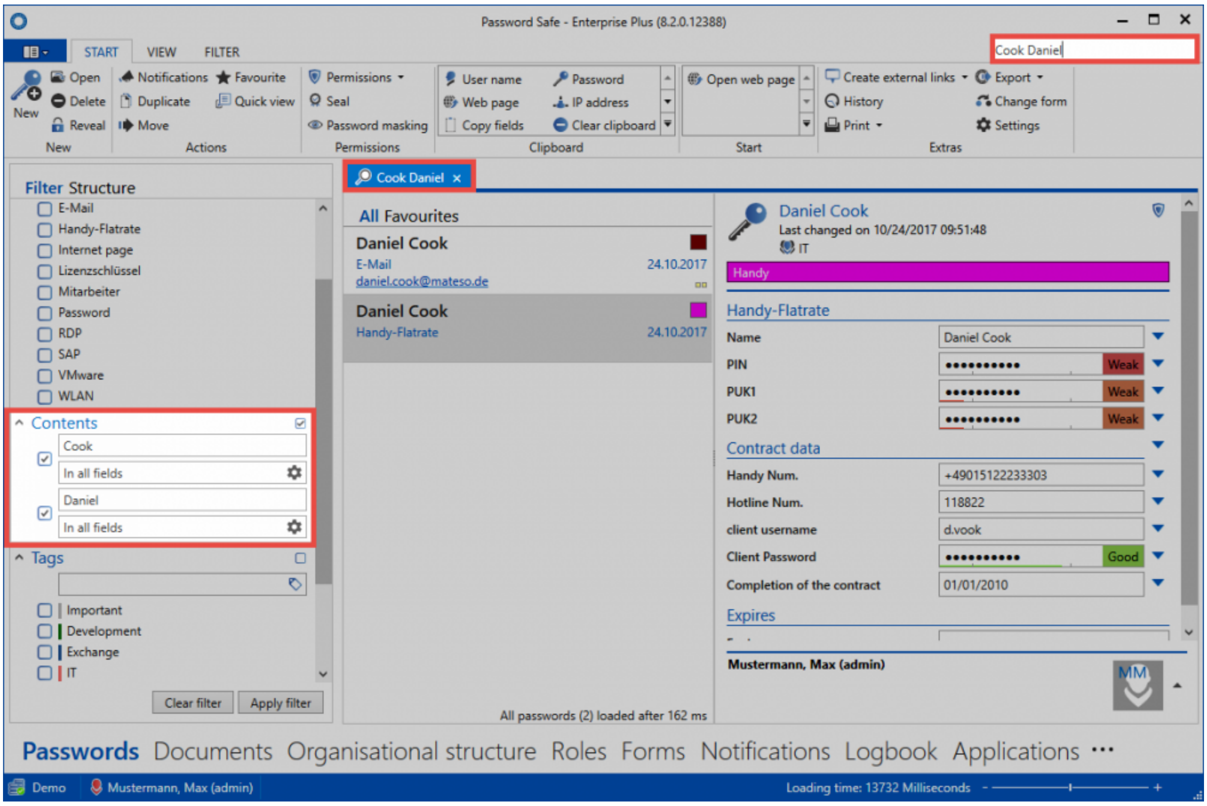
Search

What is search?

With the help of the search, it is possible to find data stored in the database efficiently according to selected criteria. Basically, there are 2 search modes:

1. Quick search

In the upper right section of the ribbon, there is a search field, which scans the module that is currently open. This is a full-text search that scans all fields and tags except the password field.



Search field: Cook Daniel

Contents:
☑ Cook — In all fields
☑ Daniel — In all fields

All Favourites

Daniel Cook — E-Mail — daniel.cook@mateso.de — 24.10.2017

Daniel Cook — Handy-Flatrate — 24.10.2017

All passwords (2) loaded after 162 ms

Daniel Cook
Last changed on 10/24/2017 09:51:48
IT

Handy

Handy-Flatrate

Name	Daniel Cook
PIN	•••••••••• Weak
PUK1	•••••••••• Weak
PUK2	•••••••••• Weak

Contract data

Handy Num.	+49015122233303
Hotline Num.	118822
client username	d.vook
Client Password	•••••••••• Good
Completion of the contract	01/01/2010

Expires

Mustermann, Max (admin)

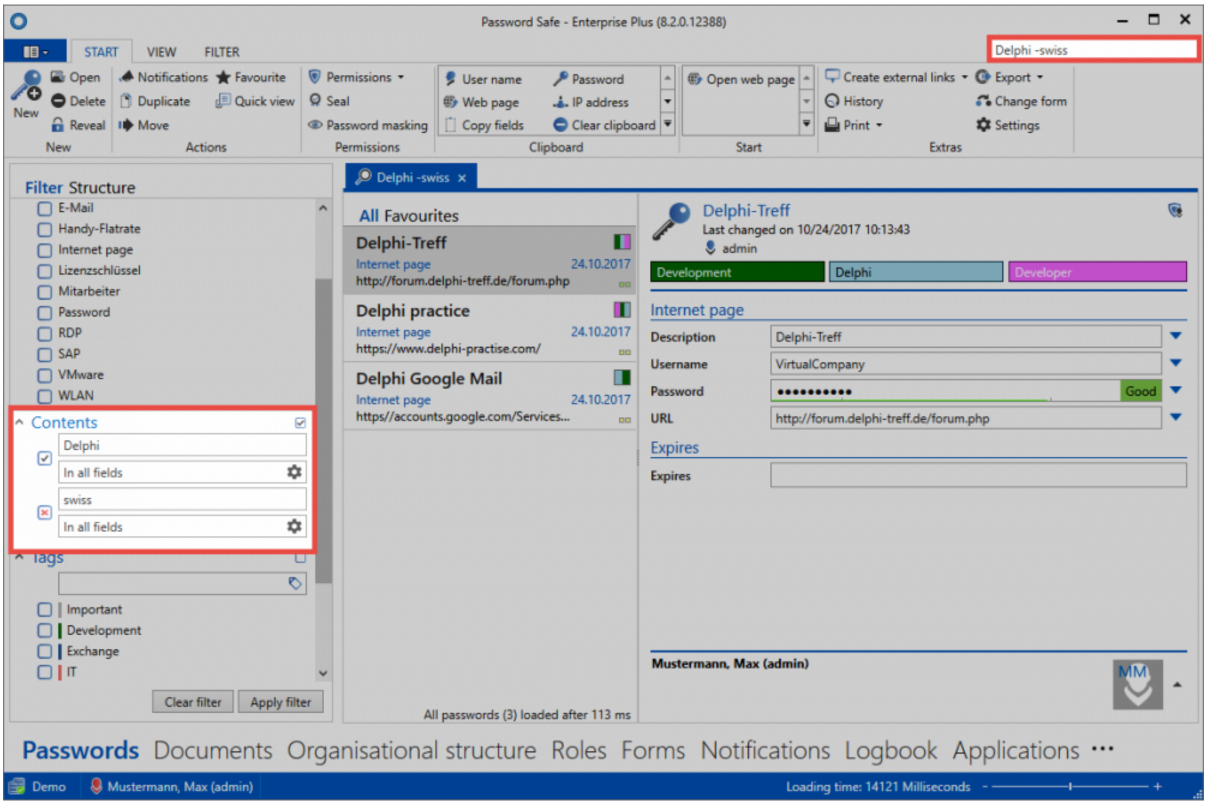
Loading time: 13732 Milliseconds

The fast search is closely linked to the filter, because search queries are converted directly into one or several content filters. You can also separate search terms using spaces, for example, **Cook Daniel**. Note that this search creates two separate content filters, +which are logically linked with “and” +. This means that both words must occur in the data record. The sequence is irrelevant. If the ordering needs to be taken into account, the search term must be enclosed in quotation marks: **“Cook Daniel”**. The search is not case sensitive. No distinction is made between upper and lower case.

You can access quick search directly via * Ctrl + Q*!

Negations in the quick search

Negations restrict the results to such an extent that certain criteria may not be met. The following example searches for all records that contain the expression * Delphi **, but not the expression * swiss *. The notation, which must be entered in the quick search, is: *Delphi -swiss**



Password Safe - Enterprise Plus (8.2.0.12388)

Quick search: Delphi -swiss

Filter Structure

Contents: Delphi – In all fields (☑); swiss – In all fields (☒)

Tab: Delphi -swiss

All Favourites

- Delphi-Treff – Internet page – 24.10.2017 – http://forum.delphi-treff.de/forum.php
- Delphi practice – Internet page – 24.10.2017 – https://www.delphi-practise.com/
- Delphi Google Mail – Internet page – 24.10.2017 – https//accounts.google.com/Services...

All passwords (3) loaded after 113 ms

Delphi-Treff

Last changed on 10/24/2017 10:13:43

admin

Development | Delphi | Developer

Internet page

Description	Delphi-Treff
Username	VirtualCompany
Password	•••••••••• Good
URL	http://forum.delphi-treff.de/forum.php

Expires

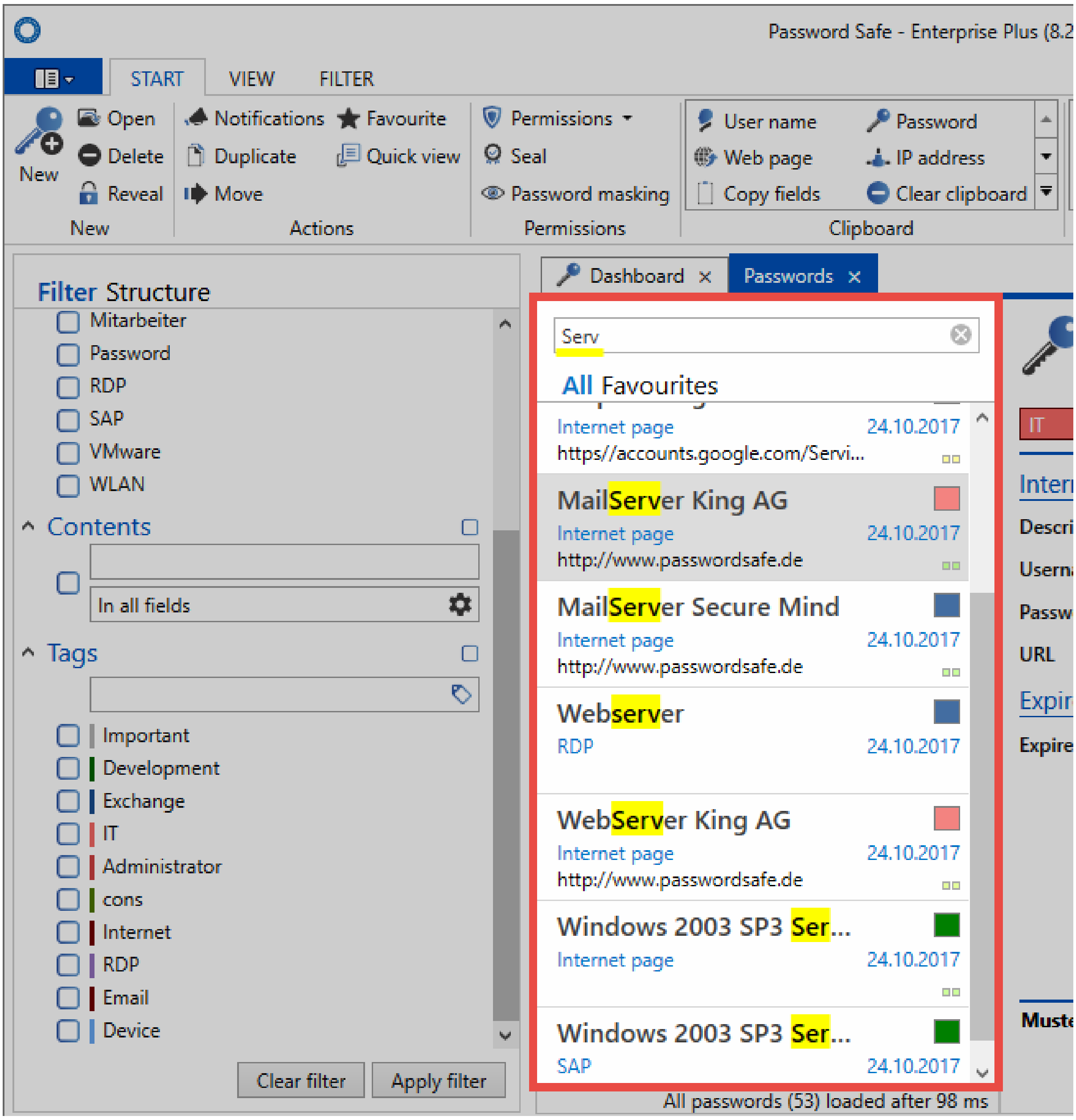
Expires	

Mustermann, Max (admin)

Demo | Mustermann, Max (admin) | Loading time: 14121 Milliseconds

2. List search

With the list search in the header of the list view, the results of the filter can be searched further. This type of search is available in almost every list. Scans only the currently filtered results. Password fields are not searched. The search is live, so the result is further refined with every additional character that is entered. Automatic “highlighting” takes place in yellow colour.



A direct database query is performed when the filter is executed. The list search only searches within the query already made.

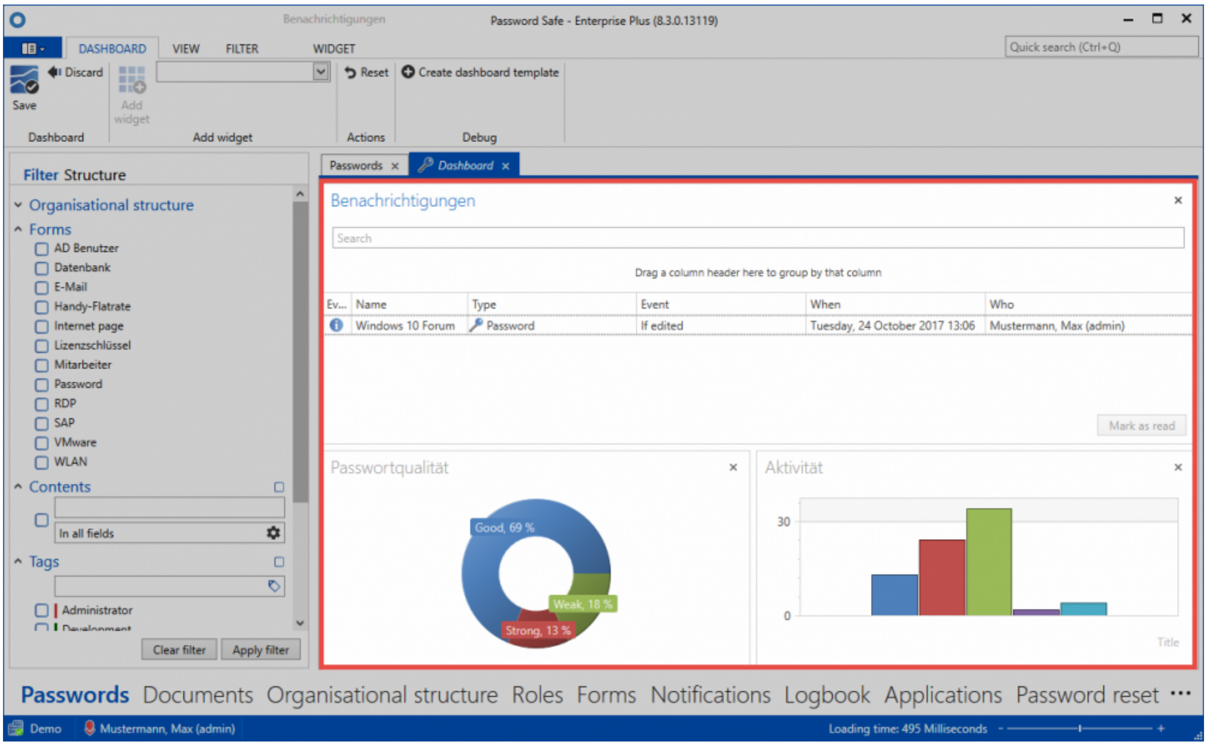
The list search is hidden by default and can be activated with "**Ctrl + F**"

Dashboard and widgets

! The dashboard is deactivated by default for performance reasons. In the global settings, the option **“Display dashboard on startup”** can be selected.

What are dashboards and widgets?

In case of large installations, the amount of information provided by Password Safe may seem overwhelming. Dashboards expand the existing filter possibilities by an arbitrarily customizable info area, which visually prepares important events or facts.



Ev...	Name	Type	Event	When	Who
ⓘ	Windows 10 Forum	Password	If edited	Tuesday, 24 October 2017 13:06	Mustermann, Max (admin)

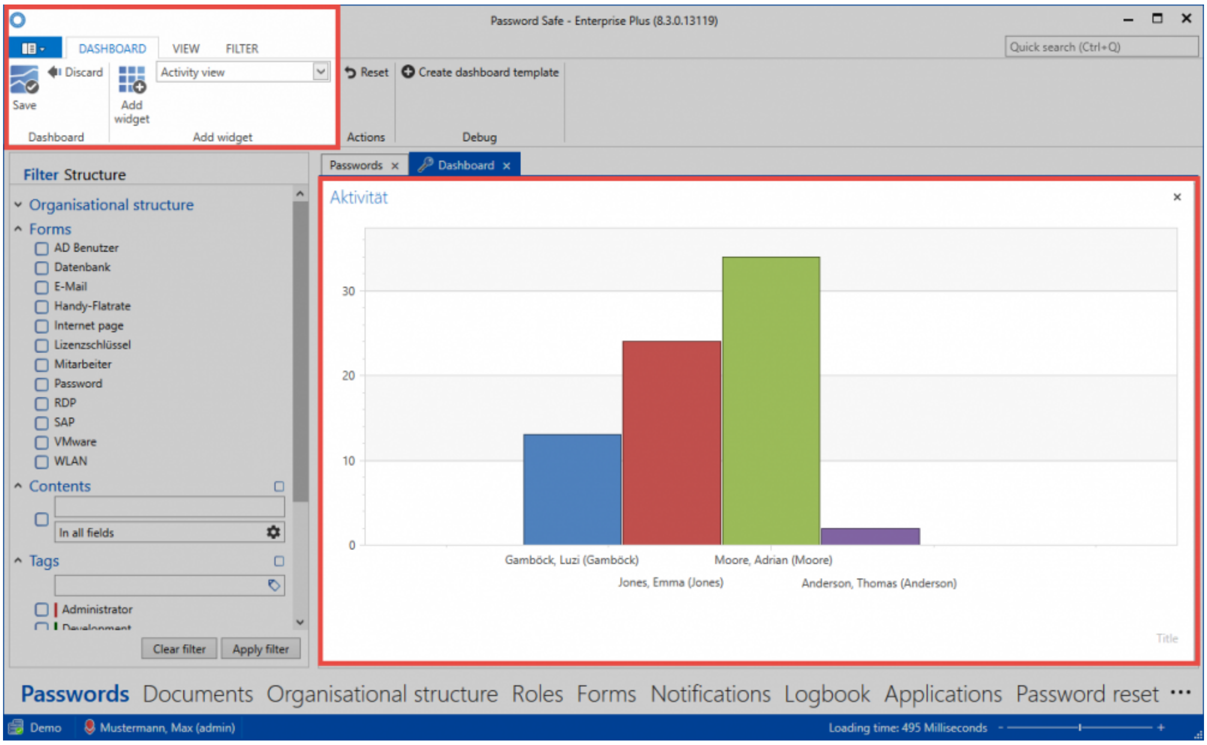
Dashboards are available in almost all client modules. A separate dashboard can be set for each module. **Widgets** correspond to the individual modules of the dashboard. There are various widgets, which can be individually defined and can be configured separately. In the above example, three widgets are enabled and provide information about current notifications, password quality, and user activity. The * maximum number of possible widgets * is managed in the user settings.

You can close the dashboard using the button in the tab. You can open it again via **View > Show dashboard** in the ribbon.

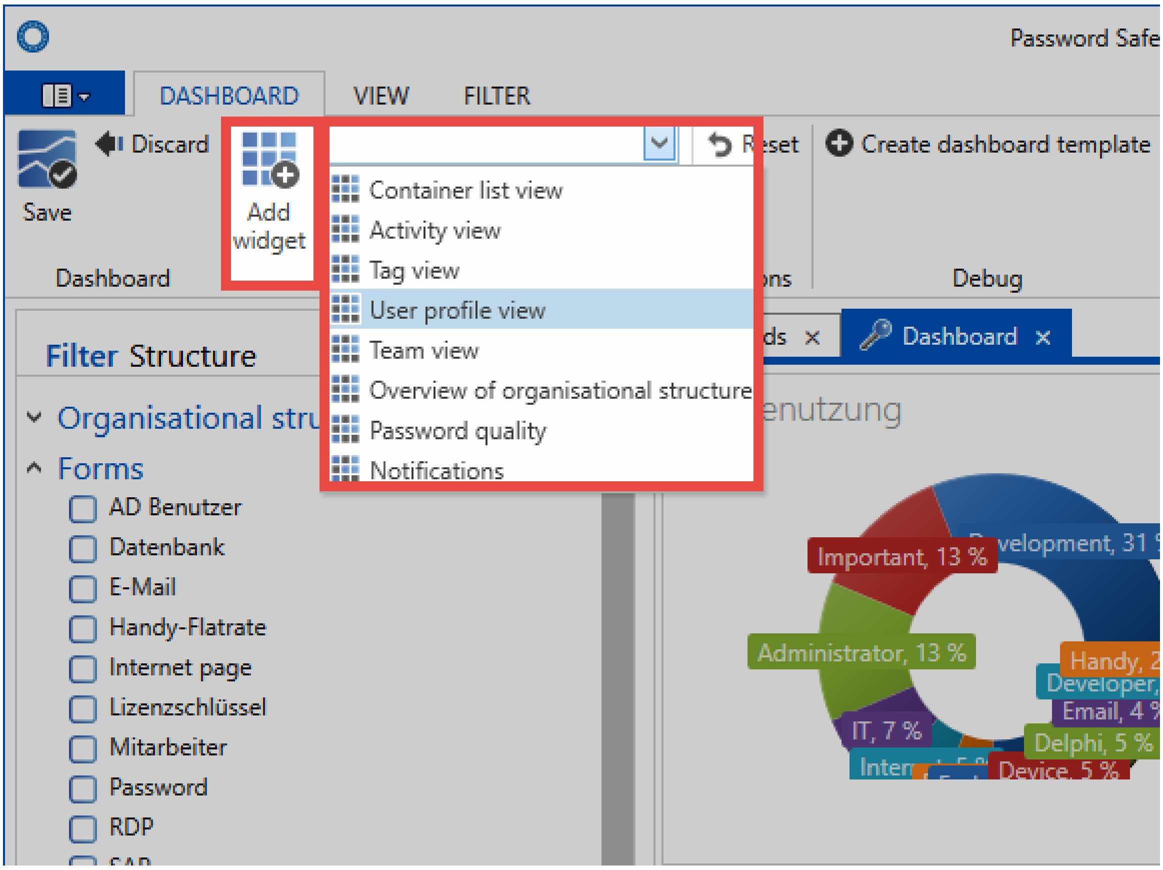
The display of the dashboard is basically uncritical since the user can only see the data on which he is also entitled.

Adding and removing widgets

If the dashboard tab is enabled, you can enable the dashboard editing mode via the ribbon. Adding and editing widgets is only possible in this mode.

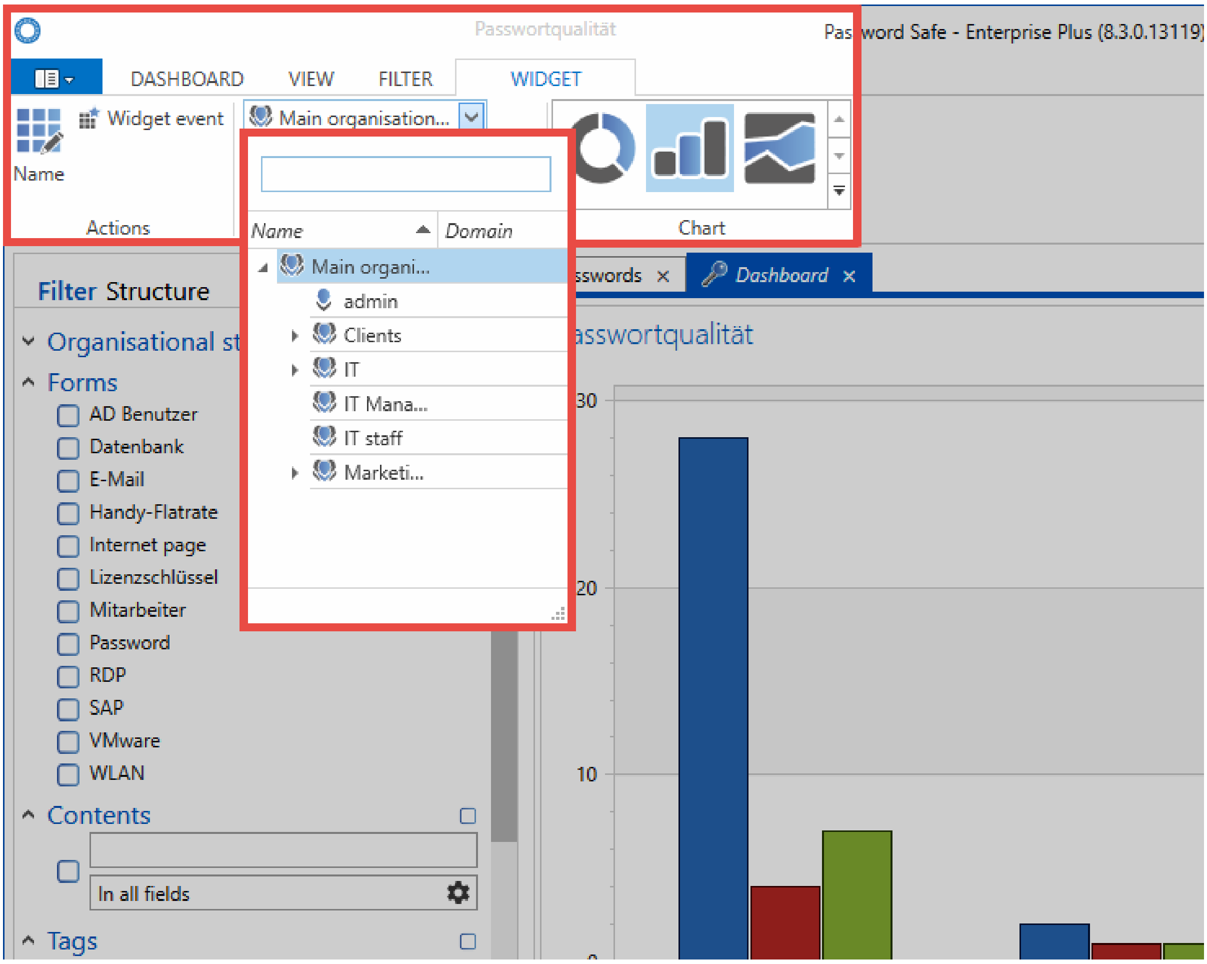


Use the drop-down menu to select the widget to be added * (1) **. Then add the widget to the dashboard using the corresponding button in the ribbon *(2)**. The maximum number of widgets that can be added can be configured in the user settings. In editing mode, any widget can be directly removed in the dashboard via the button on the upper right edge. The processing mode is ended by saving via the ribbon.



Customizing widgets

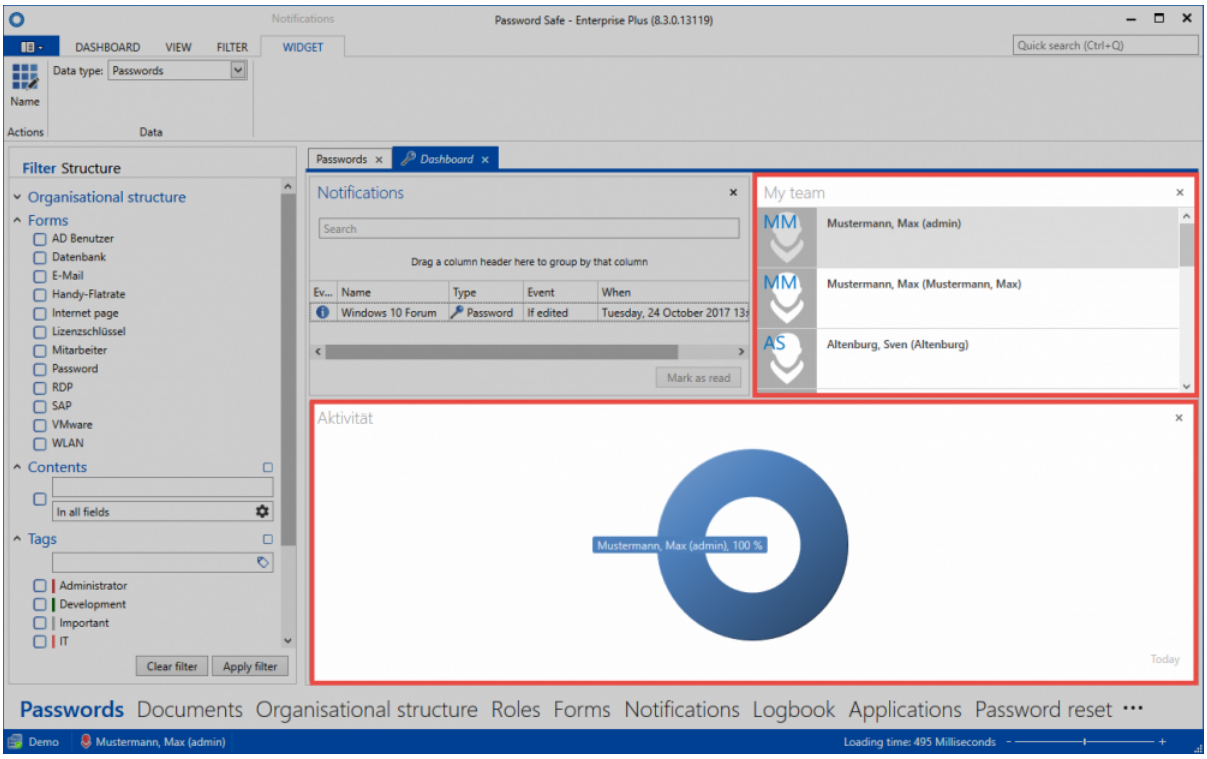
In the editing mode, you can customize each widget separately. To do this, select the widget and switch to the * widget content tab * in the ribbon.



Separate variables can be customized for each widget. This example shows how often users have had passwords displayed. Naturally, the variables are distinct for each widget since other information could be relevant.

Widget event

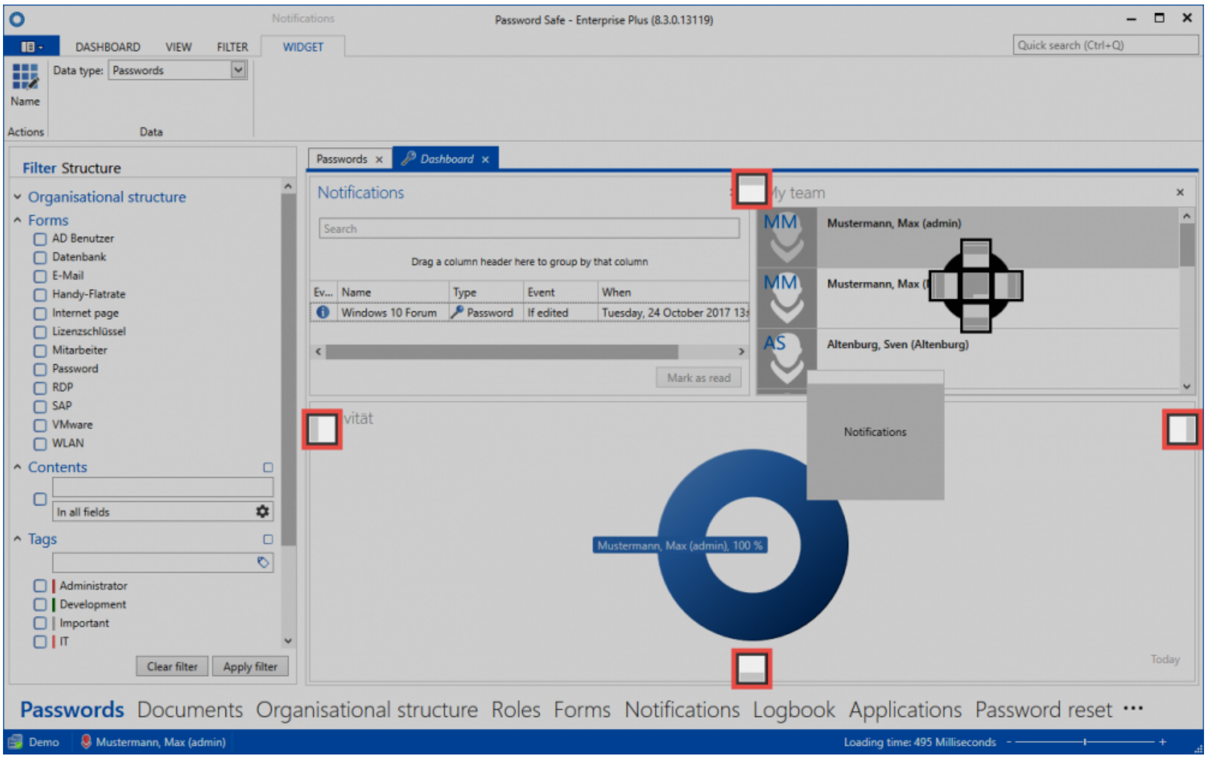
You can select the **Widget Event** option in the ribbon. This activates the interaction of the widgets. In the following example, this feature was enabled for the Activity widget. As a result, the dashboard not only displays all activities, but also filters them according to the user selected in the **Team List** widget. It therefore concerns all activities of the user “Moore”. These are filtered “live” and displayed in real-time.



Ev...	Name	Type	Event	When
●	Windows 10 Forum	Password	If edited	Tuesday, 24 October 2017 13:

Arranging widgets

In the edit mode, the layout of the widgets is user-defined. Drag & drop allows you to place a widget in the corresponding position on the dashboard (left, right, top, or bottom).



Ev...	Name	Type	Event	When
●	Windows 10 Forum	Password	If edited	Tuesday, 24 October 2017 13:

Keyboard shortcuts

Functionality

Some actions can be executed very efficiently using keyboard shortcuts. These are configured in the section of the same name within the “global user settings”:#globale-einstellungen.

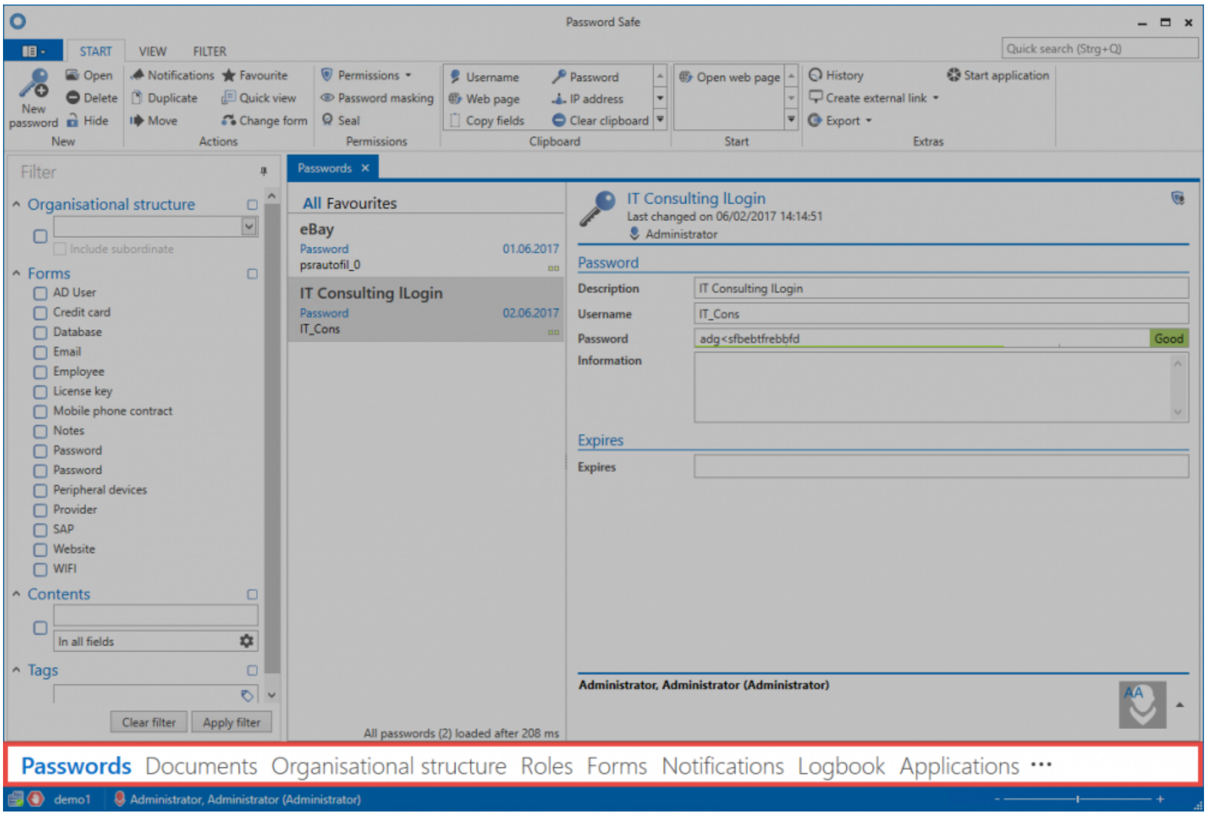
The following keyboard shortcuts are available:

- **CTRL+ ALT + U** transfers the user name from the selected record to the active window
- **CTRL+ ALT + S** starts a script that firstly transfers the user name from the selected record to the active window. The shortcut will then execute a TAB jump and transfer the password.
- **CTRL+ ALT + P** enters the selected password into the active window or field
- **CTRL+ ALT + R** firstly transfers the user name from the selected record to the active window via the enter key. The shortcut will then execute a TAB jump and transfer the password.

Client Module

What are modules?

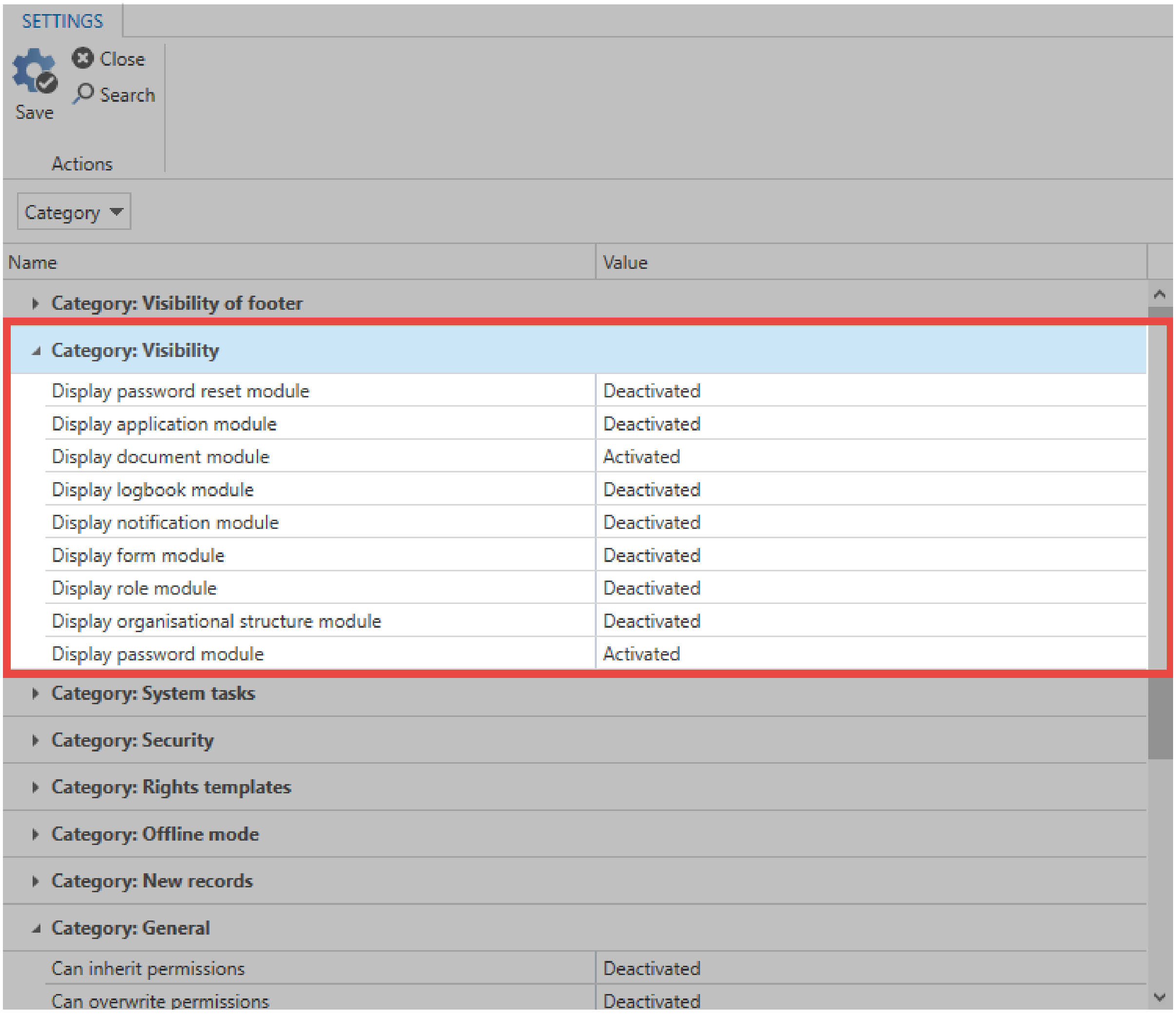
Password Safe can be customized according to the needs of the users. This requirement can be applied by the user, and can also be applied by administrative users. This means that everyone gets only those functionalities that are necessary for his special work. The amount of features required by an administrator differs significantly from those of a normal user. The **modular structure** of Password Safe supports this approach by showing only those specific areas that should actually be used by the respective user.



Description: IT Consulting ILogin
Username: IT_Cons
Password: adg<sfbebtfrebbfd Good
Information:

Visibility of modules

The modules are the gateway to the various features of version 8. Similarly to the features, not all modules have to be made available to all user layers. The **Visibility of modules** can be defined individually within the user rights.

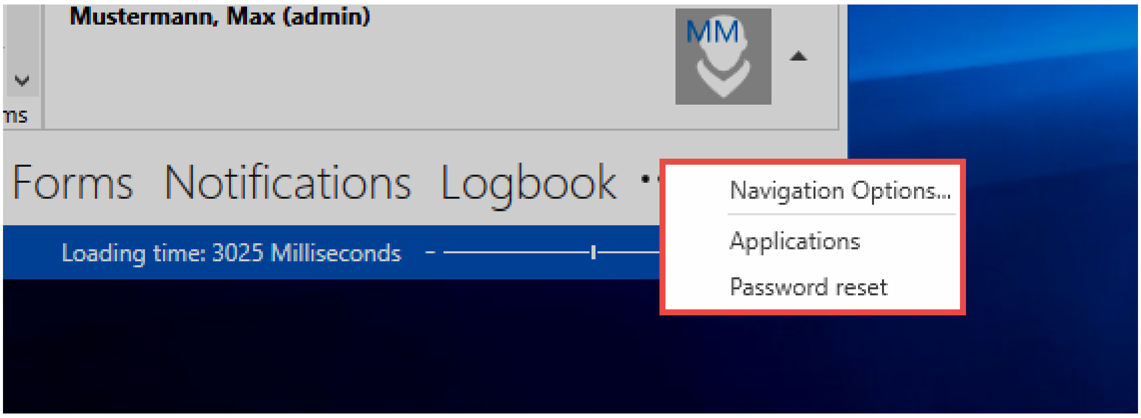


Name	Value
Category: Visibility of footer	
Category: Visibility	
Display password reset module	Deactivated
Display application module	Deactivated
Display document module	Activated
Display logbook module	Deactivated
Display notification module	Deactivated
Display form module	Deactivated
Display role module	Deactivated
Display organisational structure module	Deactivated
Display password module	Activated
Category: System tasks	
Category: Security	
Category: Rights templates	
Category: Offline mode	
Category: New records	
Category: General	
Can inherit permissions	Deactivated
Can overwrite permissions	Deactivated

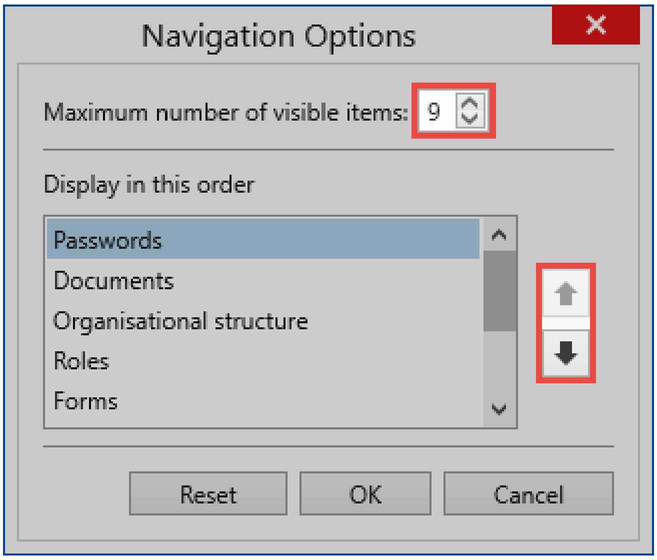
✻ The visibility of modules can always be adapted to the needs of individual user groups

Sorting modules

You can access the “Navigation options” via the three dots found at the bottom right end of the module displayed in the client. You can also find those modules displayed there that you have permissions to see in accordance with the visibility settings explained previously but which are hidden e.g. due to the scaling of the size of the client (Application and Password Reset in the example).



The navigation options enable you to define the maximum number of visible elements and also how they are sorted.

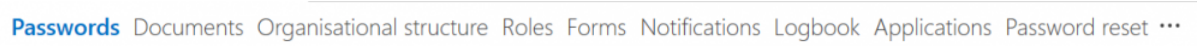


✻ The previously described visibility of the modules is a basic requirement for viewing and sorting them in the navigation options

Passwords

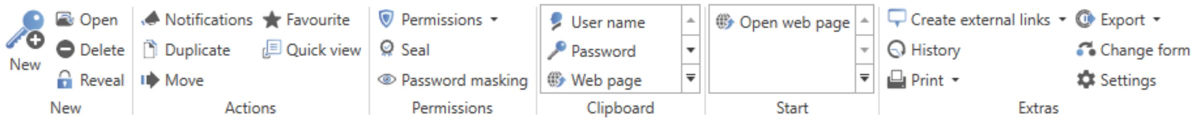
What are passwords?

In Password Safe v8, the data record with the passwords contained therein represents the central data object. The Passwords module provides both central administrators and end users with the central access to the daily handling of these sensitive and safe data. Freely definable search filters in combination with colour-highlighted tag markings on records enable very focussed work. Various approaches can be used to help apply the desired permissions to objects. Furthermore, the ergonomic structure of the module helps all users to use Password Safe in an efficient and targeted manner. The configuration of **visibility** is explained in a similar way to the other modules in one place.



Module-specific ribbon functions

A great strength of the ribbon is that it offers access to all possible actions relevant to the situation at all times. Especially within the “Passwords” module, the ribbon plays a key role due to the numerous module-specific functions. General information on the subject of the ribbon is available in the relevant section. The module-specific ribbon functions will be described below.

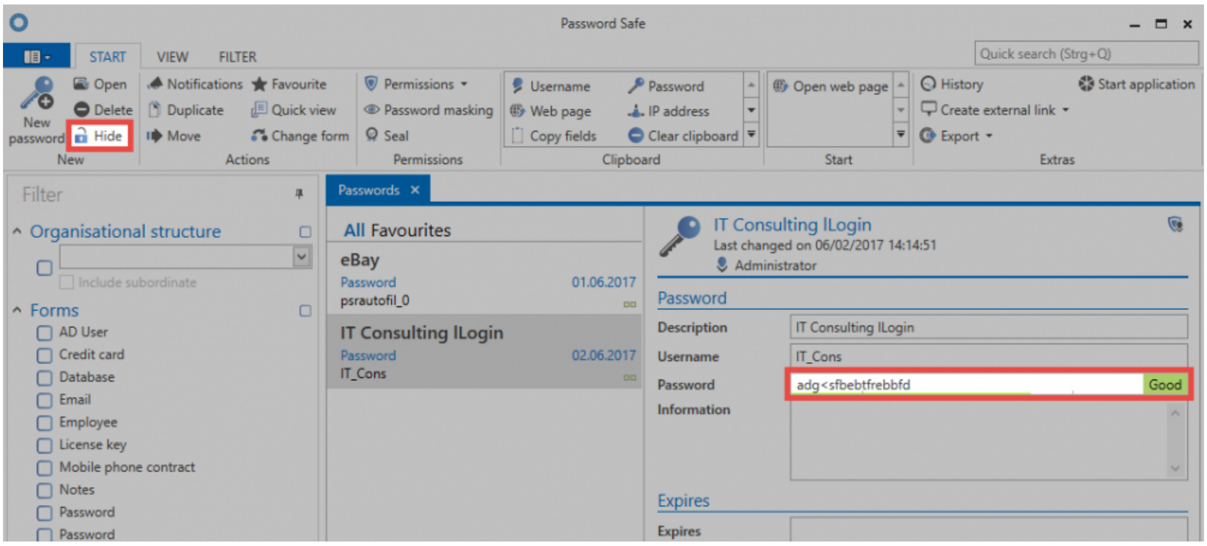


New

- “New password” New passwords can be added via both this icon in the ribbon and also via the context menu that is accessed using the right mouse button. In addition, the keyboard shortcut for this function is “Ctrl + N”. The next step is to select a suitable form.

! The user right **Can add new passwords** is required!

- **Open**: Opens the object marked in list view and provides further information about the record in the reading pane
- **Delete** Deletes the object marked in list view. A log file entry is created. (see Logbook)
- **Reveal**: The function **Reveal** can be used for all records that have a password field. Here, the passwords in the reading pane are revealed and are visible. In the example, this is revealed, and can be hidden again with the * Hide * button.



eBay
Password 01.06.2017
psrautofil_0

IT Consulting ILogin
Password 02.06.2017
IT_Cons

IT Consulting ILogin
Last changed on 06/02/2017 14:14:51
Administrator

Password

Description	IT Consulting ILogin
Username	IT_Cons
Password	adg<sfbebtfrebbfd Good
Information	

Expires

Expires	

Actions

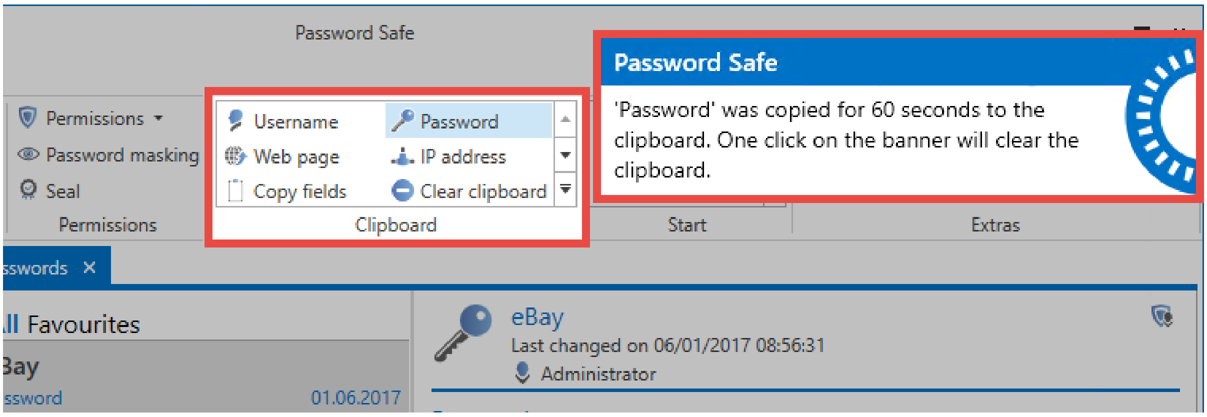
- **Notifications**: Defining notifications enables a constant flow of information about any type of change to records. The issuing of notifications is carried out in the module designed for this purpose.
- **Duplicate**: Duplicating records produces an exact copy of the record marked in list view. This applies to all saved information and also defined permissions.
- **Move**: Moves the record marked in list view to another organisational structure. More…
- **Favourite**: The selected record is marked as a favourite. It is possible to switch between all records and favourites at any time above the list view.
- **Quick view**: A modal window opens for the selected record for 15 seconds and displays all available information **including the value of the password**.
- **Change form**: It is possible to change the form used for individual records. “Mapping” of the previous form fields can be directly carried out in the modal window that opens.

Permissions

- **Permissions**: The drop-down menu can be used to set both password permissions and also form field permissions. This method only allows the manual setting of permissions for data. (see Authorization concept)
- **Password masking**: Masking passwords that need to be protected from unauthorized users is an important feature of the security concept in Password Safe. The functionality of this mechanism is described in a separate section.
- **Seal**: The double-check principle in Password Safe is also covered in its own section.

Clipboard

The clipboard is a key element in the ribbon. This only exists in the “Passwords” module. **Clicking on the desired form field of a record in the ribbon** will copy it to the clipboard.



Password Safe

'Password' was copied for 60 seconds to the clipboard. One click on the banner will clear the clipboard.

Last changed on 06/01/2017 08:56:31

The message in the style of the “Balloon Tips” in Windows shows that the password has now been saved in the clipboard for 300 seconds. (Note: the time until the clipboard is cleared is 60 seconds by default. In the present case, this has been adjusted via the user settings.)

Start

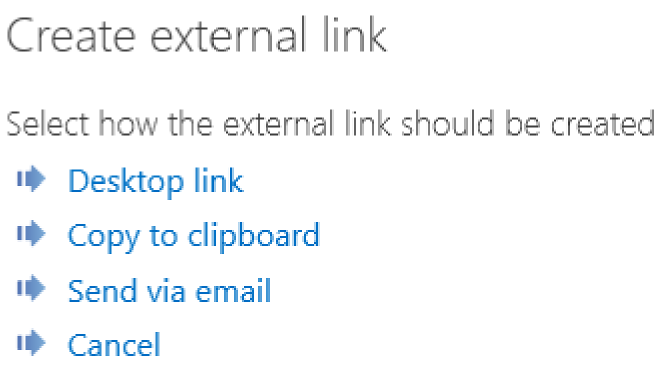
Conveniently working with passwords is only possible via the efficient usage of automated accesses via RDP, SSH, general Windows applications or websites. This makes it possible to dispense with (unsecure) entries via copy & paste.

- **Open web page**: If a URL is saved in the record, this menu option can be used to directly open it
- **Applications**: If applications have been linked to records, they can be directly opened via the “start menu”

Extras

- **History**: This icon opens the history of those records selected in list view in a new tab. Due to the comprehensive recording of historical versions of passwords, it is now possible to compare several versions with one another. Further information on this subject is available in a separate section.

- **Create external link**: This option makes it possible to create an external link for the record marked in list view. A number of different options can be selected:



Create external link

Select how the external link should be created

- Desktop link
- Copy to clipboard
- Send via email
- Cancel

- **Start application**: In contrast to the option for starting linked applications, this icon can be used to also directly start non-linked applications using the log-in information from the record marked in list view.

- “Export”: It is possible to export both all the selected records and also the data defined by the filter to a .csv file. More…

Creating new passwords

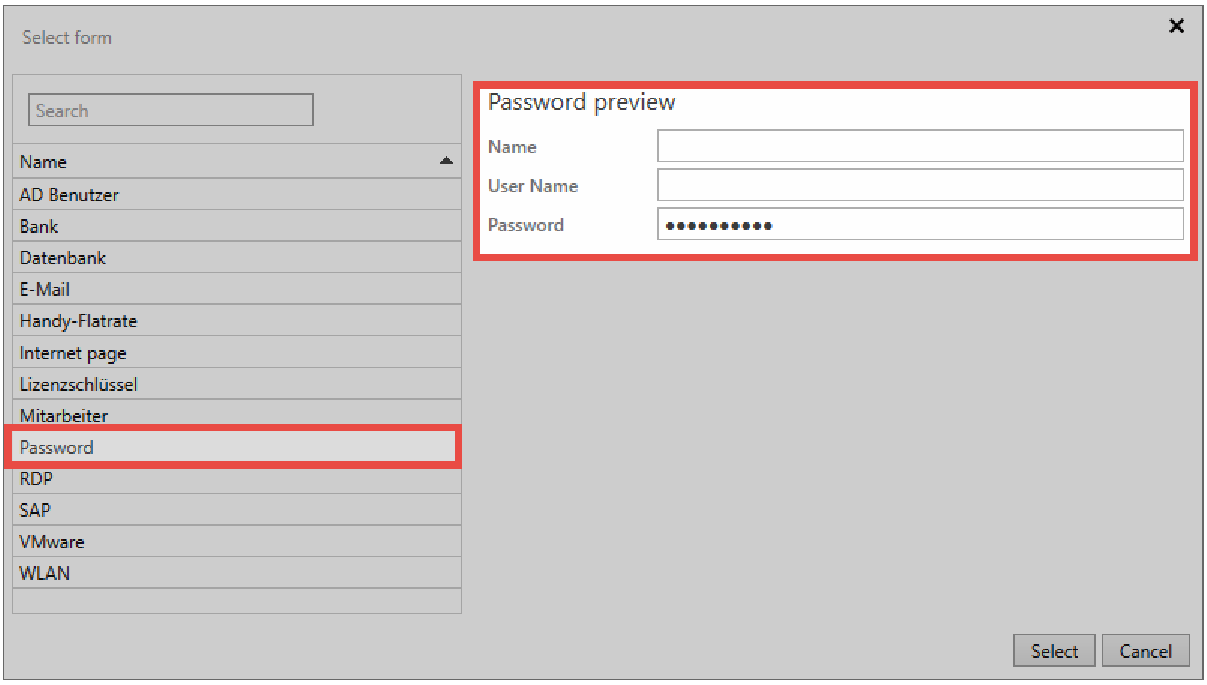
What does creating new passwords/records mean?

Saving a record/password stores information in the MSSQL database. This process is started in the "Passwords module for the client":#psr-client. It is accessed either via the icon in the ribbon, using the keyboard shortcut "CTRL + N" or via the context menu that is accessed using the right mouse button in list view. The next step is to select a suitable form that will open in a modal window.

> ! The right **Can add new passwords** and the ability to view the **password module** are required

Selecting a form

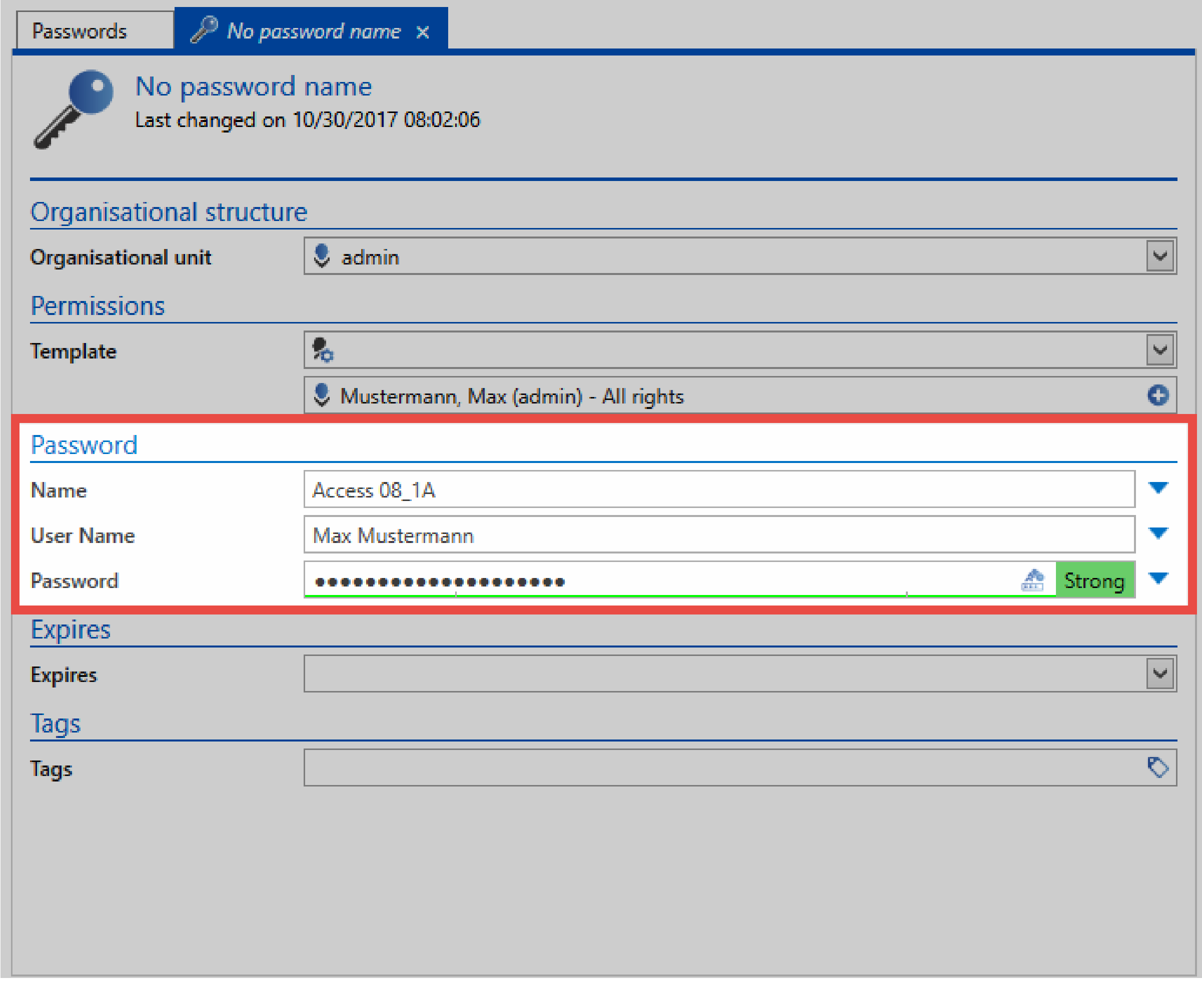
When creating a new record, it is possible to select from all the forms for which the logged-in user has the required permissions. To make the selection process as easy as possible, a preview of the form fields included in the form is shown on the right hand side.



In this example, you can see that the "Password" form marked on the left contains three form fields "Name", "User name" and "Password". Forms thus act as **templates** according to which their information is saved. (Management of the forms including issuing permissions and editing existing forms is covered in a separate section)

Entering data

The window for creating a new record always open in a separate tab. As can be seen below, the corresponding form fields for the previously selected form can now be filled. Password fields deserve special mention here because they can be handled differently based on password rules. The record can be saved via the ribbon when all fields have been filled.



No password name
Last changed on 10/30/2017 08:02:06

Organisational structure
Organisational unit: admin

Permissions
Template:
Mustermann, Max (admin) - All rights

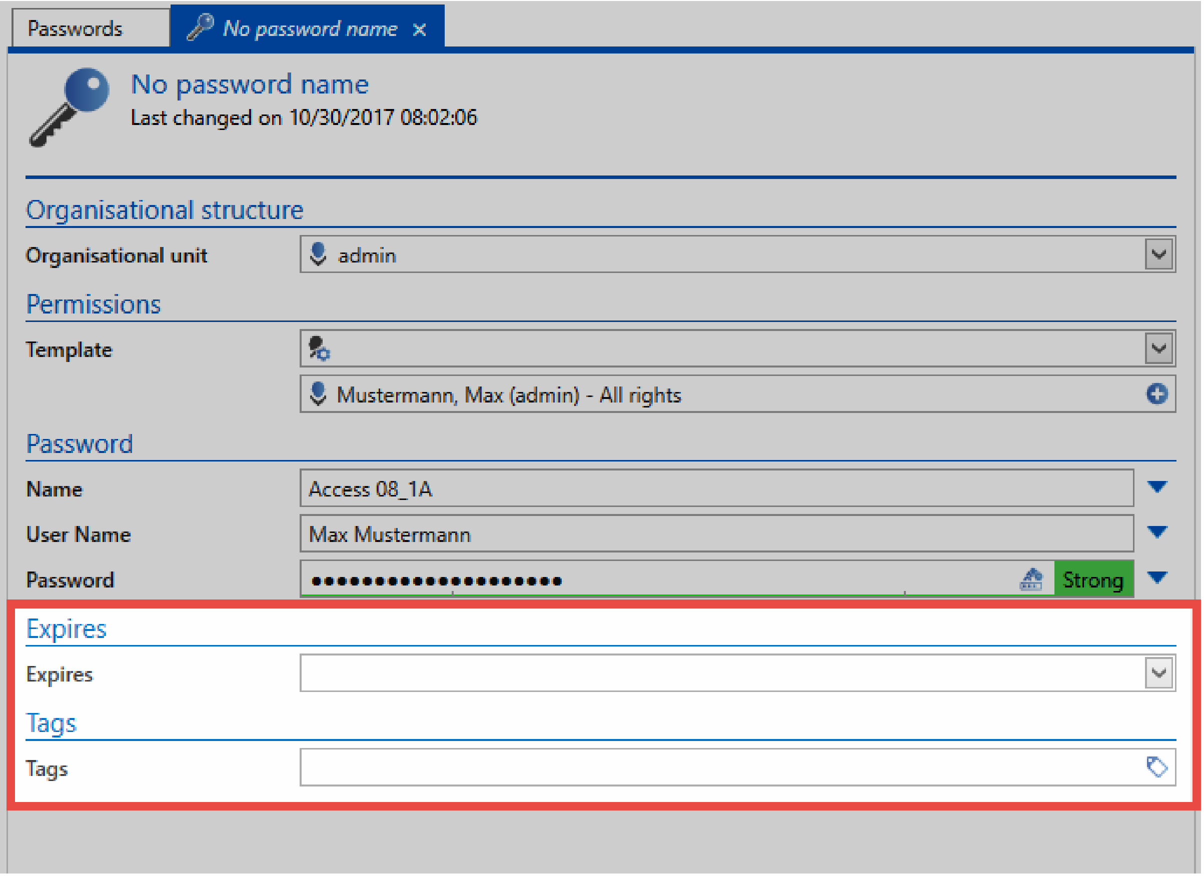
Password
Name: Access 08_1A
User Name: Max Mustermann
Password: ●●●●●●●●●●●●●●●●●●●● Strong

Expires
Expires:

Tags
Tags:

Validity and tags

Irrespective of the selected form, it is always possible to define the validity and tags for a record. Both values are optional.



No password name
Last changed on 10/30/2017 08:02:06

Organisational structure

Organisational unit: admin

Permissions

Template:
Mustermann, Max (admin) - All rights

Password

Name: Access 08_1A
User Name: Max Mustermann
Password: ●●●●●●●●●●●●●●●●●●●● Strong

Expires

Expires:

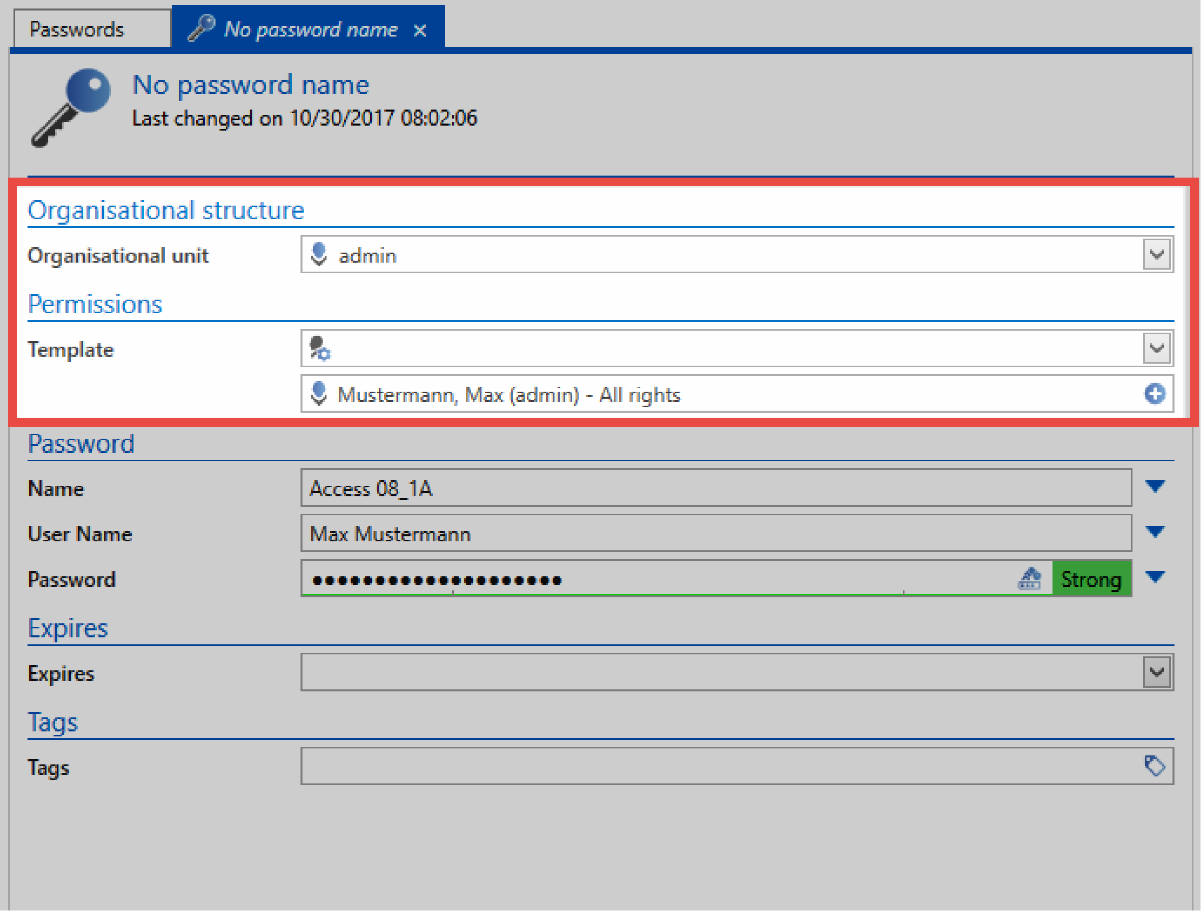
Tags

Tags:

- The **validity** defines an end date until which the record is valid. This information can be evaluated e.g. in the logbook or in reports. It is thus possible to create a list of all expired passwords for a user or an authorized entity. However, it is not possible to limit the usability of expired passwords for security reasons.
- **Tags** are freely definable properties of records that can be used as search criteria. This also allows thematically linked information to be grouped together. More...

Setting permissions for new records

In principle, there are various approaches for setting permissions for newly created records. All of them have already been described in the Authorization concept section. It is important to note here that **manual setting of permissions is only possible after saving** a record. Automatic permissions are set before the record is saved. In this context, the selection of the organisational structure and the permissions for a record are important aspects.



No password name
Last changed on 10/30/2017 08:02:06

Organisational structure

Organisational unit	admin

Permissions

Template	
	Mustermann, Max (admin) - All rights

Password

Name	Access 08_1A
User Name	Max Mustermann
Password	•••••••••••••••••••• Strong

Expires

Expires	

Tags

Tags	

- **Manual setting of permissions**: If you want to manually set permissions for the record, select the organisational structure in which the record should be saved. After saving the record, the permissions can be manually amended via the permissions tab in the ribbon. If you only want to create a personal record for which no other user will receive permissions, simply select your own organisational structure and conclude the process with “save” via the ribbon.

✻ If any kind of automatic permissions have been activated for the selected OU, this will always be prioritised.

! Even when creating private records, inheritance of permissions based on the logged-in user can also be activated as an option. This option is described in a “separate section”:#vererbung-aus-organisationsstrukturen.

✻ The user right **Allow sharing of personal passwords** can be used to define that personal passwords cannot be released to other users.

- **Automatic setting of permissions**: Automatic setting of permissions is carried out before the record is saved. Irrespective of whether predefined rights or rights inheritance is being used, the configuration is always carried out in the organisational structure or permissions area. Saving the record thus completes the process for creating the password including the issuing of permissions.

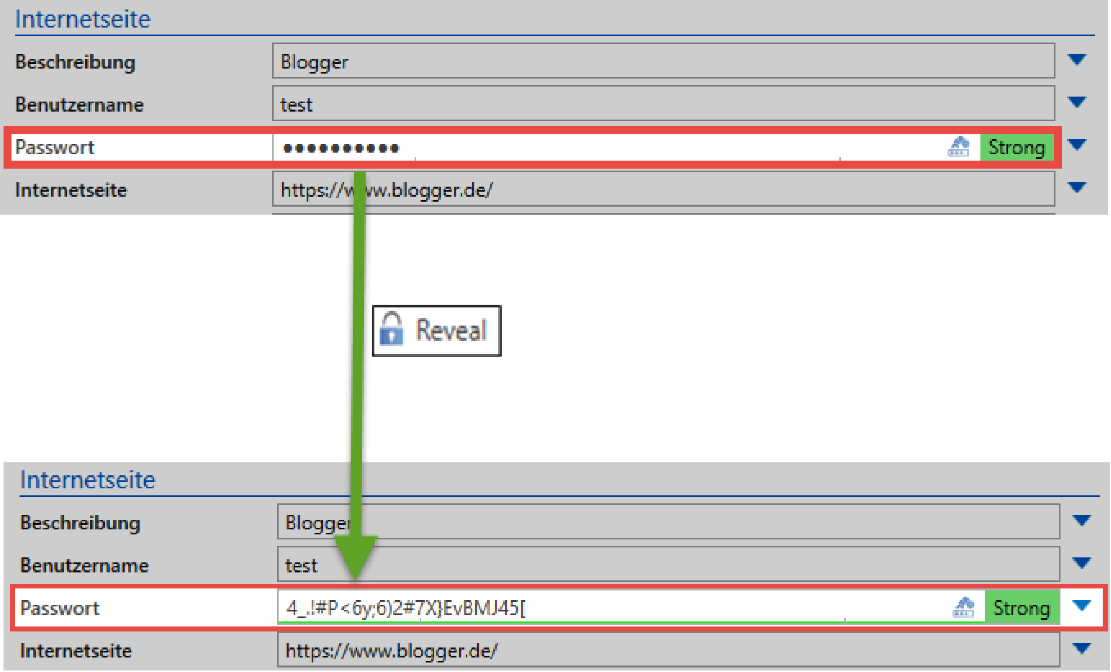
Revealing passwords

What is involved in revealing passwords?

Not all information is encrypted by the MSSQL database in Password Safe for performance reasons. Only the password itself (=secret) is encrypted with the help of the used encryption algorithms and is then saved in the MSSQL database. As access to the MSSQL server is otherwise secured via access permissions, this process enables the **maximum possible working speed** with a **unchanged high level of security** through the use of **sophisticated, cryptographic methods**. Revealing passwords describes the mechanism by which a password is made visible to the user in the client. This process for dealing with passwords very precisely reflects the importance of data security in Password Safe – and this process will thus be described in detail below.

Example case

The record “Blogger” has been saved in the database and is visible to the logged-in user. It can thus be deduced that the user has at least a read right for the record. As can be gathered from the authorization concept, the user thus also generally has a read right to the password itself. This means the user can view the value of the password using the “reveal” function.



Internetseite

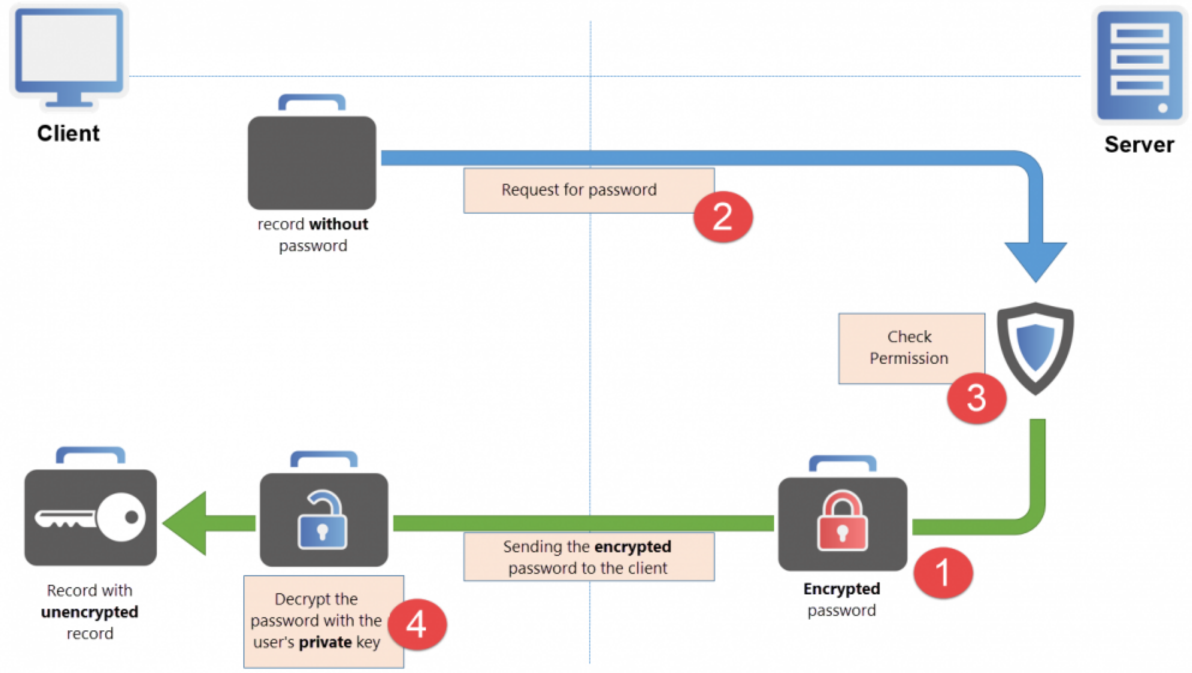
Beschreibung	Blogger
Benutzername	test
Passwort	●●●●●●●●●● Strong
Internetseite	https://www.blogger.de/

Internetseite

Beschreibung	Blogger
Benutzername	test
Passwort	4_.!#P<6y;6)2#7X}EvBMJ45[Strong
Internetseite	https://www.blogger.de/

Revealing passwords – diagram

In this context, it is important to note that the word “reveal” does not really accurately describe this process. It creates the **incorrect** impression that the client already has the password and only needs to reveal it. However, the processes running in the background until the password are revealed are much more complex and will thus be described below.


Client
Server
record **without** password
Request for password
2
Check Permission
3
Record with **unencrypted** record
Decrypt the password with the user's **private** key
4
Sending the **encrypted** password to the client
Encrypted password
1

1. Saving the password on the server

Even though you would assume the opposite, at the start a masked password (******) is neither available on the client nor the server in plain text! The password is stored as part of the MSSQL database in a hybrid encrypted state via the two methods **AES 256** and **RSA 4096**. Accordingly, it is not currently possible either on the server or the client to view the password. If you mark a record, the password is not available at all on the client and is encrypted on the server before it is revealed.

2. The encrypted password is requested

Pressing the “reveal”- button triggers the process for requesting the password. A request is sent to the server to apply for the encrypted password to be released. The server itself does not possess the required key (private key) to decrypt the password. Therefore, it can only deliver the **encrypted value**.

3. Checking the permissions

Whether the request sent in step 2 is approved is defined in the authorization concept. Once the request has been received, the server checks whether the user possess the required rights. It also checks the possible existence of other security mechanisms such as a seal or password masking. If the necessary requirements for releasing the password have been met, the server now sends the **encrypted**

password. In the same step, a **log file entry** is saved that documents the user’s access to the password.

4. Decrypting the password on the client

The user now has the encrypted password which has been delivered by the server. The user himself possesses the **private key** required for decrypting the password and can now view the actual password.

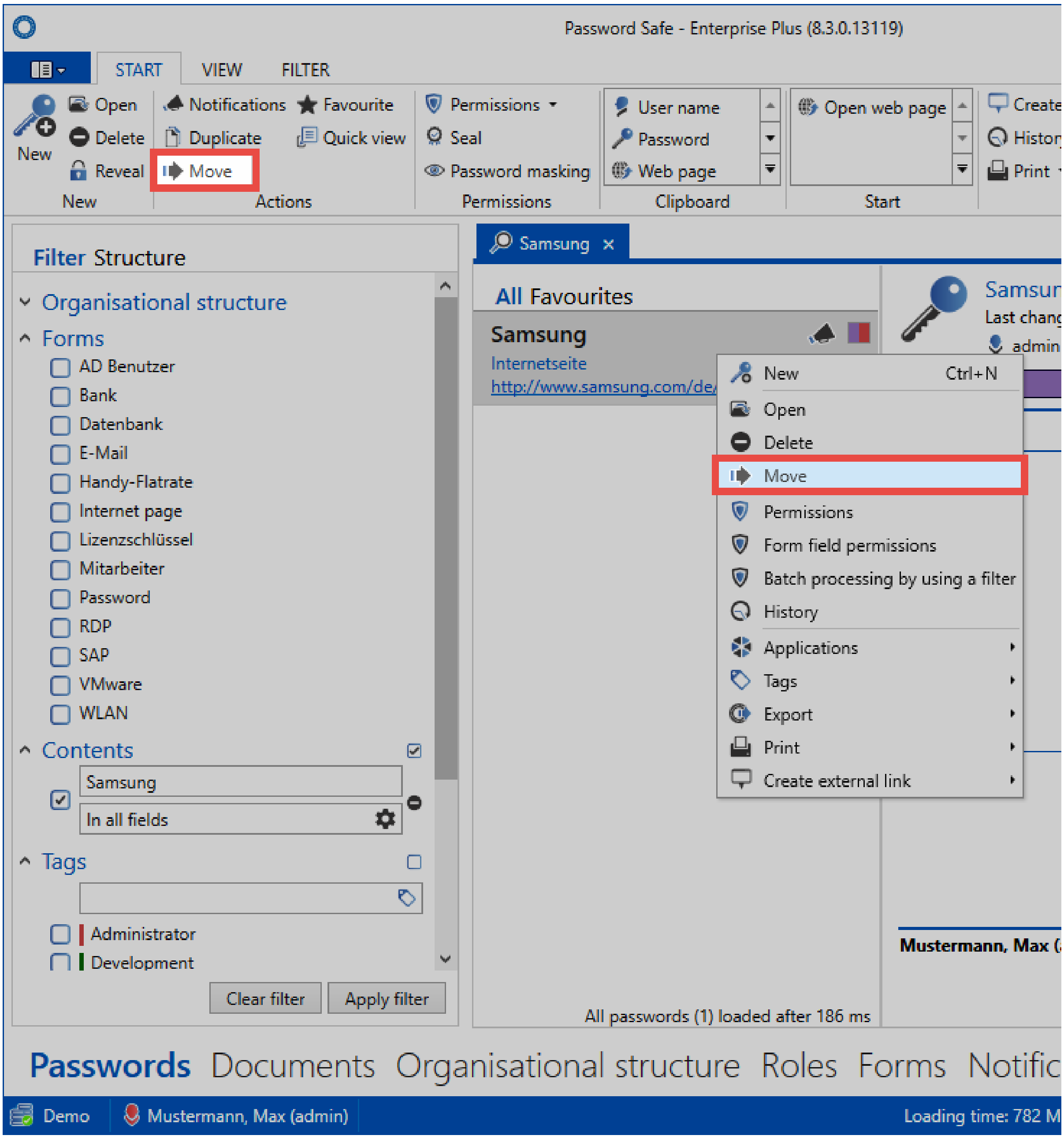
Moving passwords

What happens when records are moved?

Data can be moved within Password Safe to another organisational structure. This does not necessarily have to be linked to a change in permissions (the effects are described separately below). Moving records without changing the permissions mainly has effects on the filtering or search functions for records.

How do you move a record?

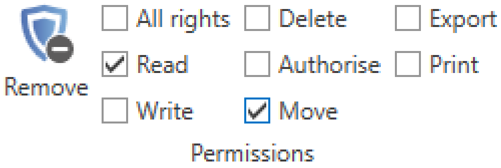
The (marked) records are moved either via the ribbon or via the context menu that is accessed using the right mouse button.



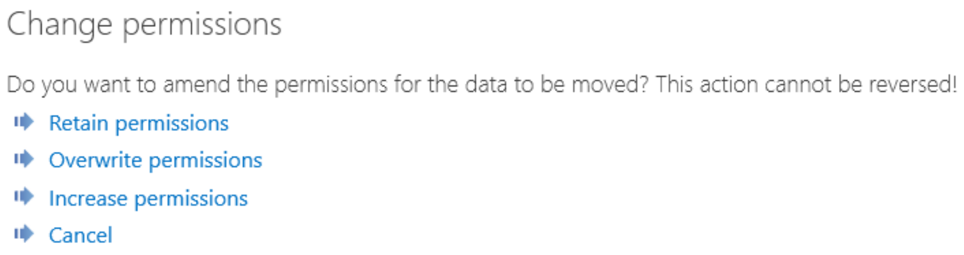
Multiple records can also be marked and moved. The selected permissions are then valid for all records in this case.

Required permissions

No special user rights/settings are required in order to move records. The “move” right for the record is the only deciding factor.



Effects on existing permissions



Change permissions

Do you want to amend the permissions for the data to be moved? This action cannot be reversed!

- **Retain permissions**: The permissions for the record are not changed by moving it and are retained
- **Overwrite permissions**: The permissions for the record are overwritten by the target OU
- **Extend permissions**: The existing permissions are extended to include the permissions for the target OU

! From a technical perspective, all rights will be removed from the record when overwriting the permissions. The permissions will then be applied to the record in accordance with the **rights template** or **inheritance from organisational structures**. It is important to note here that it is theoretically possible to remove your own rights to the record! The rights change will only be carried out if at least one user retains the right to issue permissions as a result. Otherwise, the rights change will be cancelled with a corresponding message.

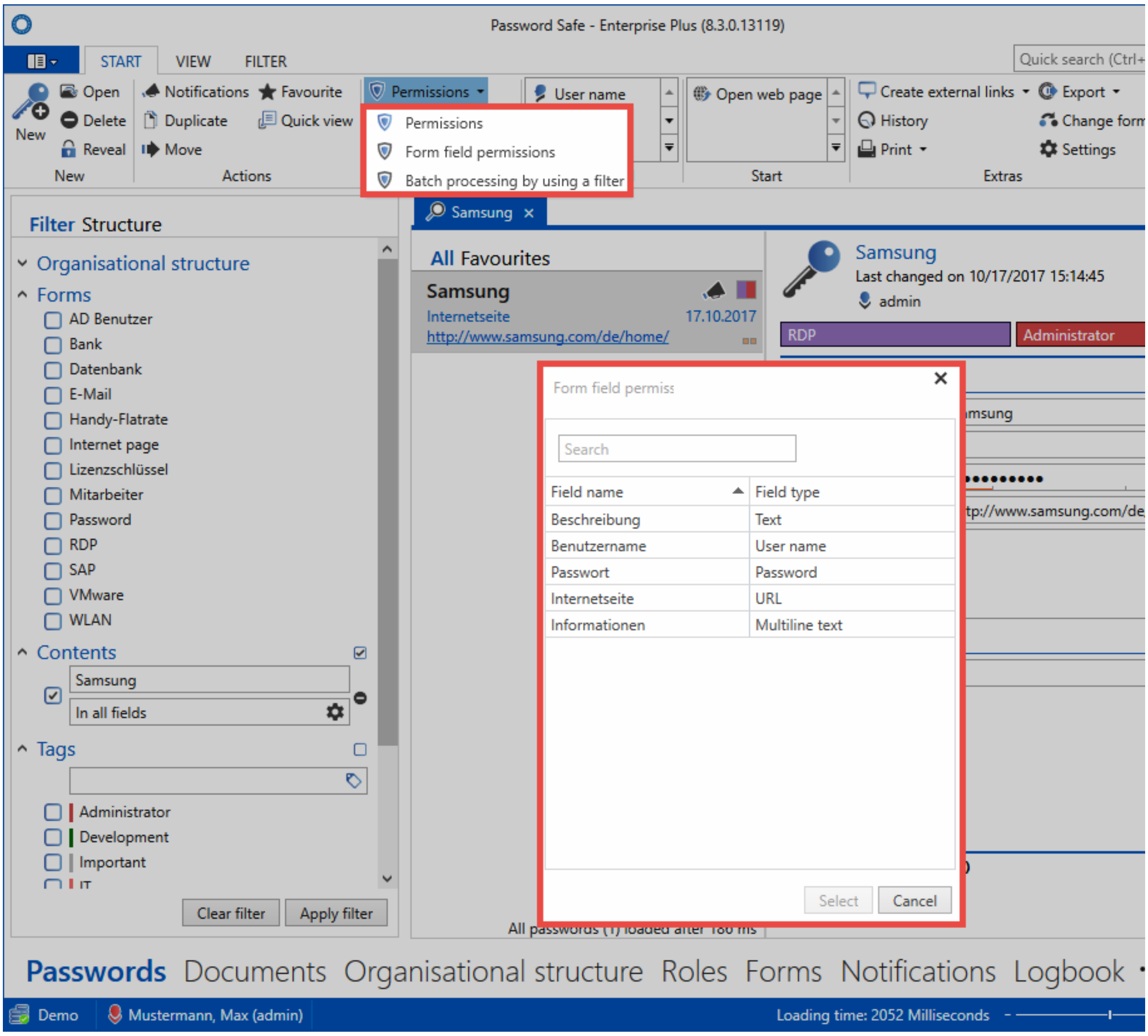
Form field permissions

What are form field permissions?

The authorization concept describes that separate permissions can be set for each object. These objects could be records, forms or users. Password Safe goes one step further in this context. Every single form field for a record can also be granted with separate permissions. It is thus possible to grant different permissions for the password field of a record than are set for the other fields.

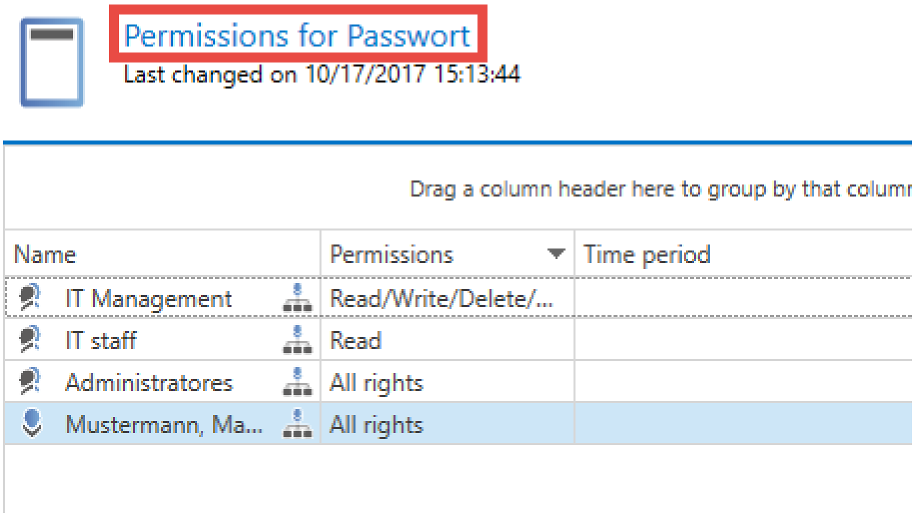
Configuration

The associated form field permissions for the marked record can be opened via the ribbon using the drop-down menu under "Permissions".



Field name	Field type
Beschreibung	Text
Benutzername	User name
Passwort	Password
Internetseite	URL
Informationen	Multiline text

The window that opens allows you to select the relevant form field for which you want to grant permissions. The following example focuses on the password field.



Permissions for Passwort
Last changed on 10/17/2017 15:13:44

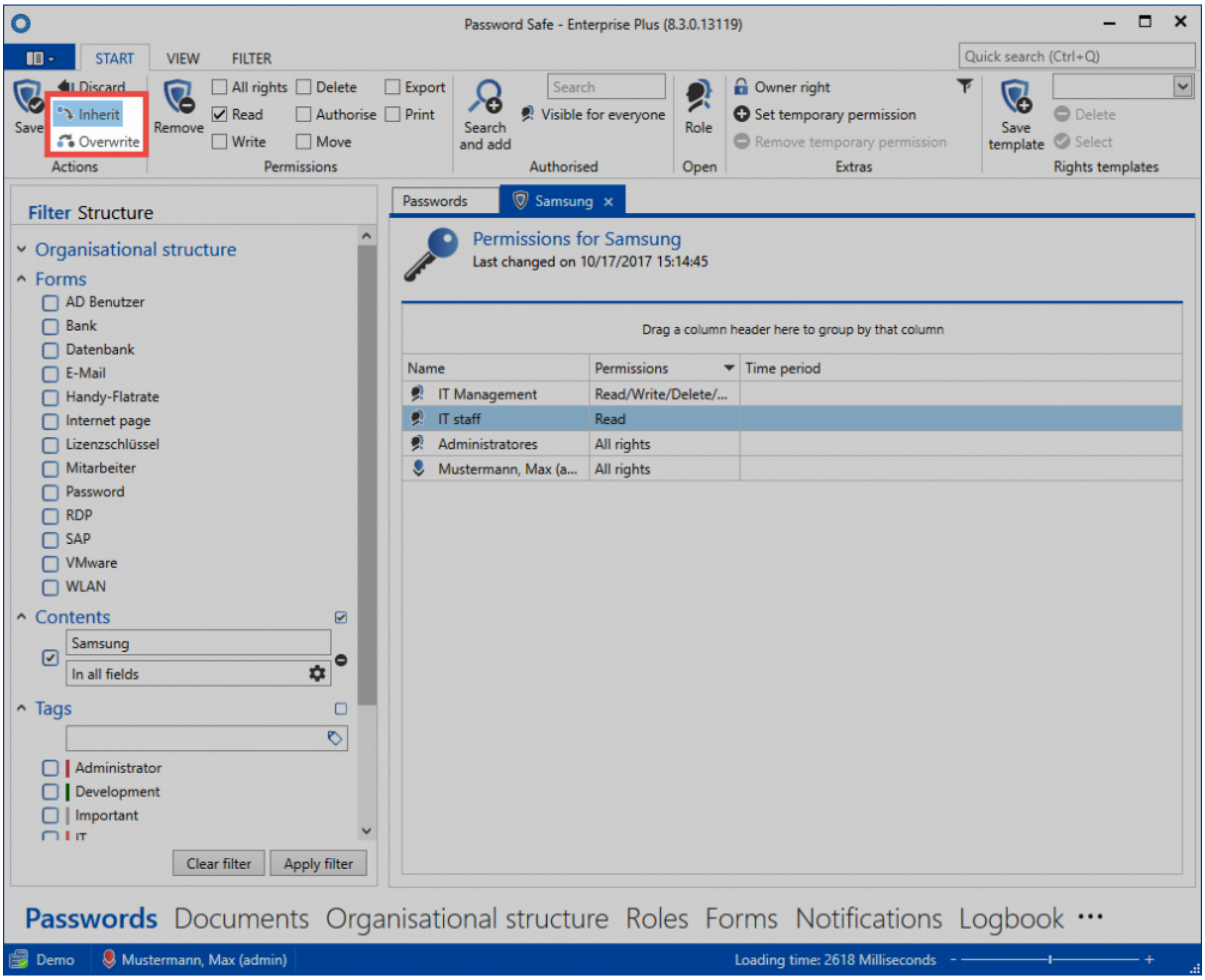
Drag a column header here to group by that columr

Name	Permissions	Time period
IT Management	Read/Write/Delete/...	
IT staff	Read	
Administratores	All rights	
Mustermann, Ma...	All rights	

The permissions configured here now exclusively apply to the password field. The other form fields remain unaffected.

Inheritance of permissions within records

Changes to the permissions for a record are automatically inherited by all form fields by default. If you open the permissions for a record via the ribbon, the configured rights are then valid for all form fields. This mechanism can be switched on and off using the two buttons “Inherit” and “Overwrite” in the ribbon.



☐ All rights ☐ Delete ☐ Export
☑ Read ☐ Authorise ☐ Print
☐ Write ☐ Move

☑ Contents: Samsung
In all fields

Permissions for Samsung
Last changed on 10/17/2017 15:14:45

Name	Permissions	Time period
IT Management	Read/Write/Delete/...	
IT staff	Read	
Administratores	All rights	
Mustermann, Max (a...	All rights	

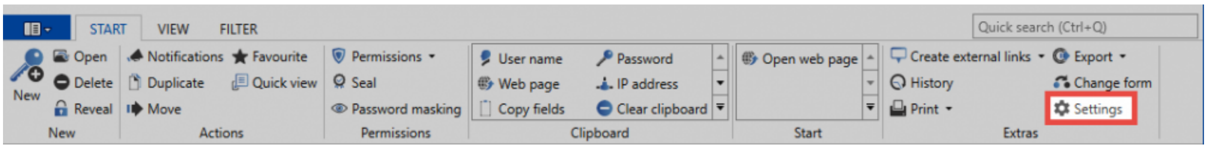
! The visibility of these icons can be controlled via the user rights **Can overwrite permissions** and **Can inherit permissions**.

In this way, you have the option of deciding that changes to the permissions for a record are not automatically inherited by all available underlying form fields. It is only necessary to remove the tick from the “Inherit” field.

Password settings

What are password settings?

The password settings can be used to define a diverse range of options. These can be found in the ribbon in the subsection “Extras”. The settings open up in a new tab.



Category: Browser

- **Default browser**: This option can be used to define a default browser for every record separately. You can select from all browsers that have been registered as a browser in Windows.

Category: SSO

- **Browser add-ons: Exact domain check**: This setting defines whether the domain for displaying the record should be subjected to an exact domain check or not. Further information on this subject can be found under Add-ons.

- **Browser add-ons**: Automatically fill login masks: This setting defines whether the login masks are automatically filled when logging in via SSO. This is the case when the user is located on a login page. If the record for this page has been saved, the login mask will be filled if this option has been activated. Otherwise, this step needs to be carried out manually via the add-on. If multiple records have been saved for this page, the user must complete this step manually via the add-on in both cases.

- **Browser add-ons**: Automatically send login masks: If this option has been activated, the login button is automatically pressed after filling in the login information.

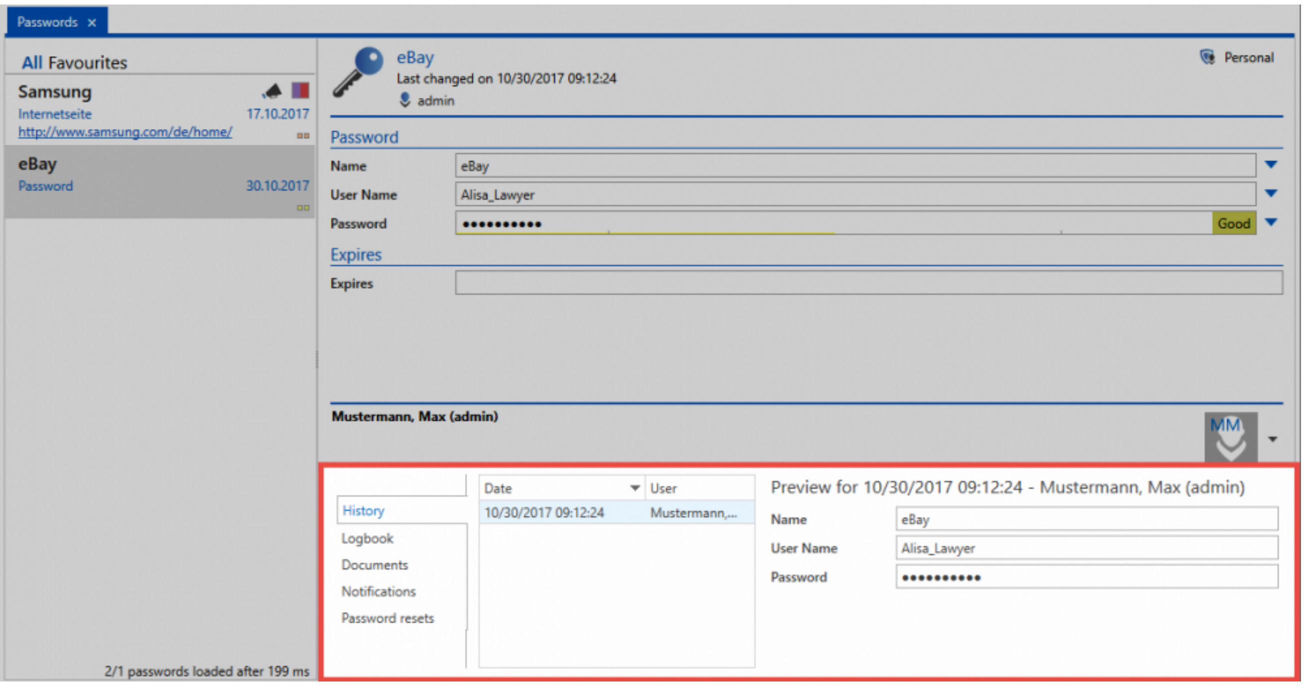
History

What is the history?

Alongside saving passwords and keeping them safe, the ability to trace changes to records also has great relevance. The history maintains a seamless account of the versions for all form fields in a record. Every change to records is separately recorded, saved and can thus also be restored. In addition, it is always possible to compare historical values with the current version. The history is thus an indispensable component of every security concept.

The history in the reading pane

The optional footer area can be used to already display the history when in the reading pane. All of the historical entries are listed and sorted in chronological order.



Samsung
Internetseite 17.10.2017
http://www.samsung.com/de/home/

eBay
Password 30.10.2017

eBay
Last changed on 10/30/2017 09:12:24
admin
Personal

Password
Name: eBay
User Name: Alisa_Lawyer
Password: •••••••••• Good

Expires
Expires:

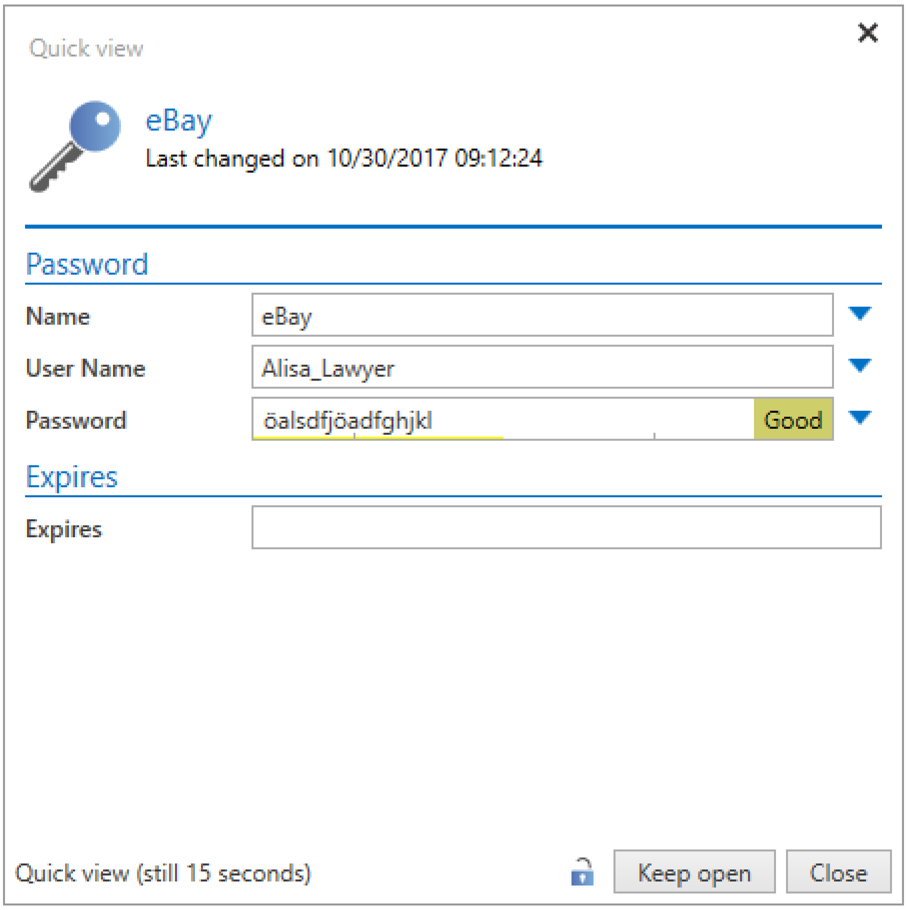
Mustermann, Max (admin)

Date	User
10/30/2017 09:12:24	Mustermann,...

Preview for 10/30/2017 09:12:24 - Mustermann, Max (admin)
Name: eBay
User Name: Alisa_Lawyer
Password: ••••••••••

2/1 passwords loaded after 199 ms

The different versions are displayed one below the other on the left. The info for each respective version can then be seen alongside on the right. A quick view can be displayed via the **History** in the ribbon or via a double click.



Quick view

eBay

Last changed on 10/30/2017 09:12:24

Password

Name: eBay

User Name: Alisa_Lawyer

Password: öalsdfjöadfghjkl Good

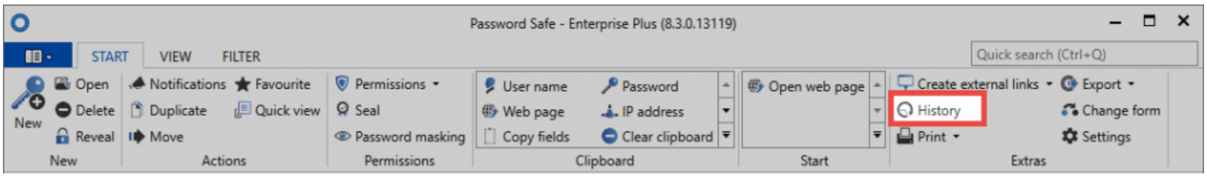
Expires

Expires:

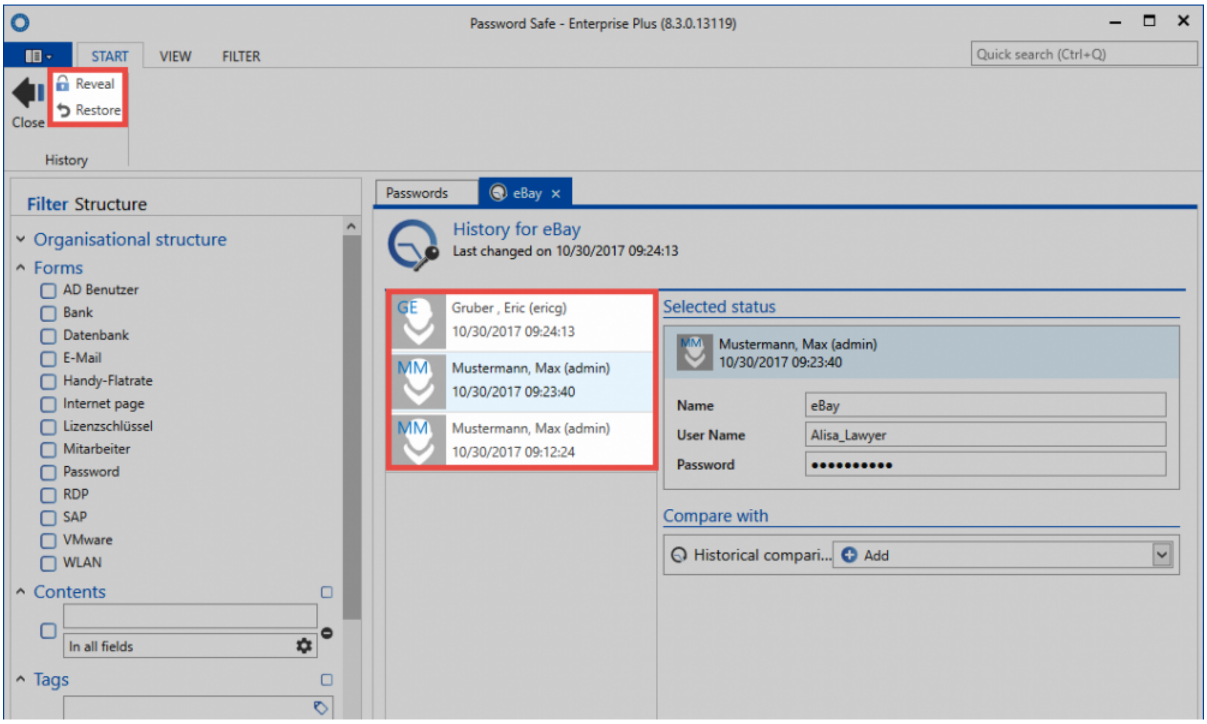
Quick view (still 15 seconds)

Detailed history in the Extras

The detailed history for the record marked in list view can be called up in the Start/Extras tab.



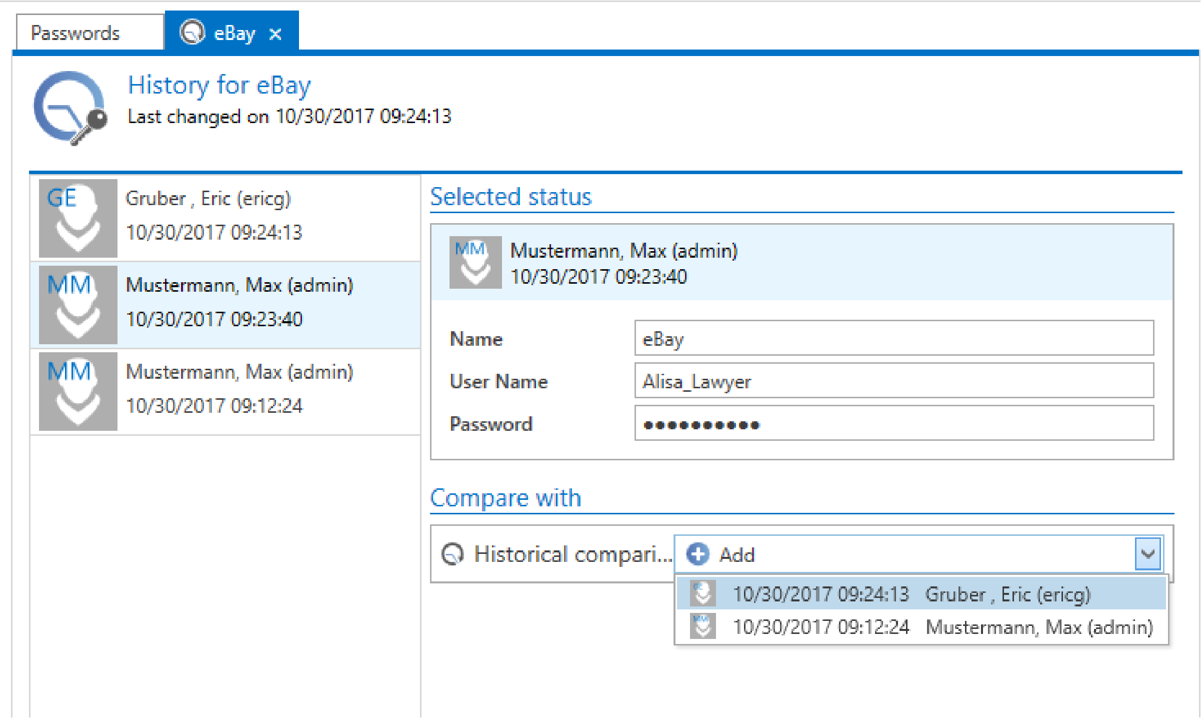
The history for the marked record opens in a separate tab. In list view, all of the available versions with the date and time of their last change are sorted in chronological order.



Name: eBay
User Name: Alisa_Lawyer
Password: ••••••••••

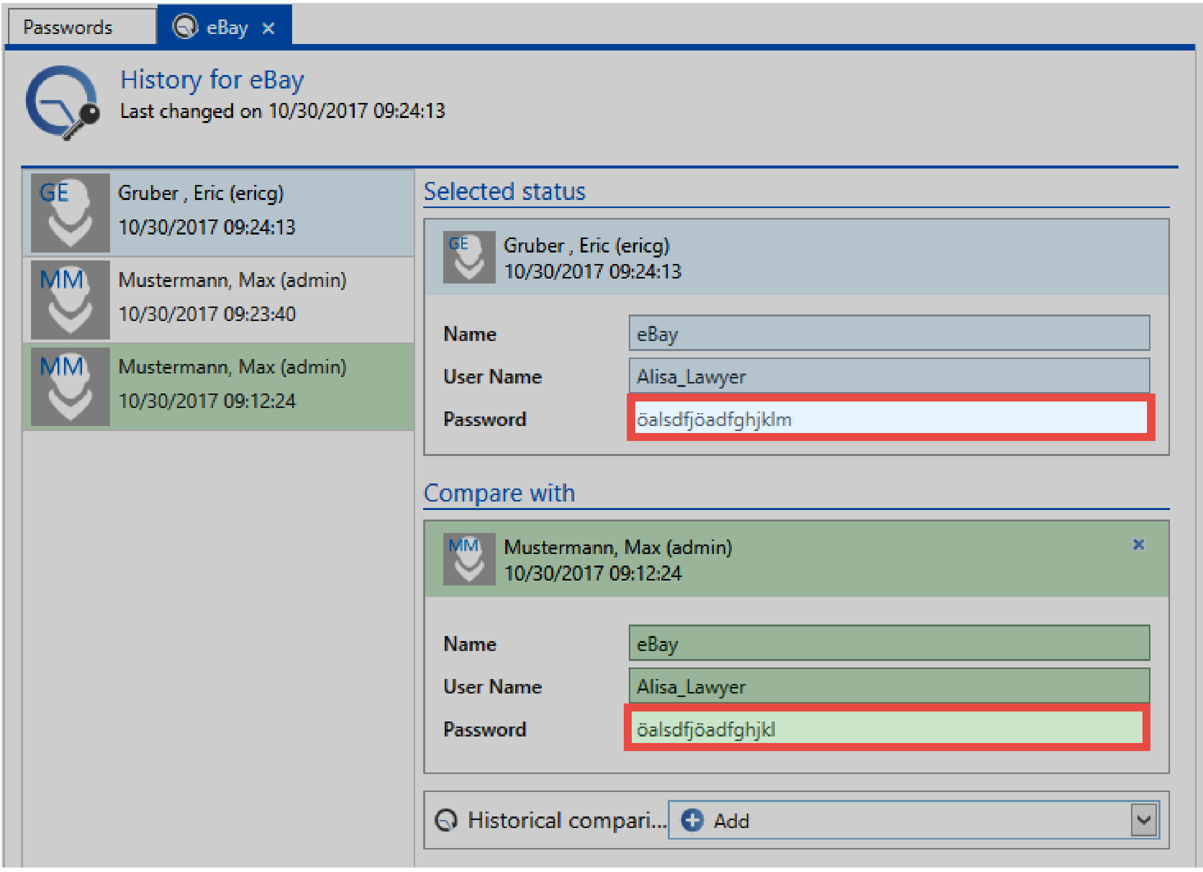
Comparison of versions

At least two versions need to be selected in order to carry out a comparison. In list view, mark the first version and then add another version via the “Add” button on the right of the reading pane to compare with the first one.


Passwords
eBay
History for eBay
Last changed on 10/30/2017 09:24:13
Gruber , Eric (ericg) 10/30/2017 09:24:13
Mustermann, Max (admin) 10/30/2017 09:23:40
Mustermann, Max (admin) 10/30/2017 09:12:24
Selected status
Mustermann, Max (admin) 10/30/2017 09:23:40
Compare with
Historical compari...
Add
10/30/2017 09:24:13 Gruber , Eric (ericg)
10/30/2017 09:12:24 Mustermann, Max (admin)

Name: eBay
User Name: Alisa_Lawyer
Password: ••••••••••

If deviations exist between the two versions, these will be highlighted in colour.



Selected status

Gruber , Eric (ericg)
10/30/2017 09:24:13

Name	eBay
User Name	Alisa_Lawyer
Password	öalsdfjöadfghjklm

Compare with

Mustermann, Max (admin)
10/30/2017 09:12:24

Name	eBay
User Name	Alisa_Lawyer
Password	öalsdfjöadfghjkl

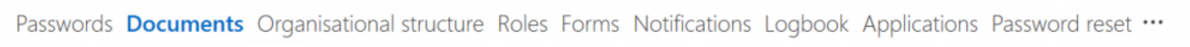
Restoring versions

A selected status can be restored via the ribbon. The current state is overwritten and added to the history

Documents

What are documents?

Security-critical data does not necessarily need to be in the form of passwords. To enable the uniform and secure storage of data other than passwords, Password Safe version 8 offers effective tools for the professional handling of sensitive documents and files. The ability to share documents with others according to their permissions gives you access to the current status of a document and helps avoid redundancies. The documents module is complemented by a sophisticated version management system, which records all versions of a document that were saved in the past and thus enables you to revert back to historical versions. The configuration of **visibility** is explained in a similar way to the other modules in one place..

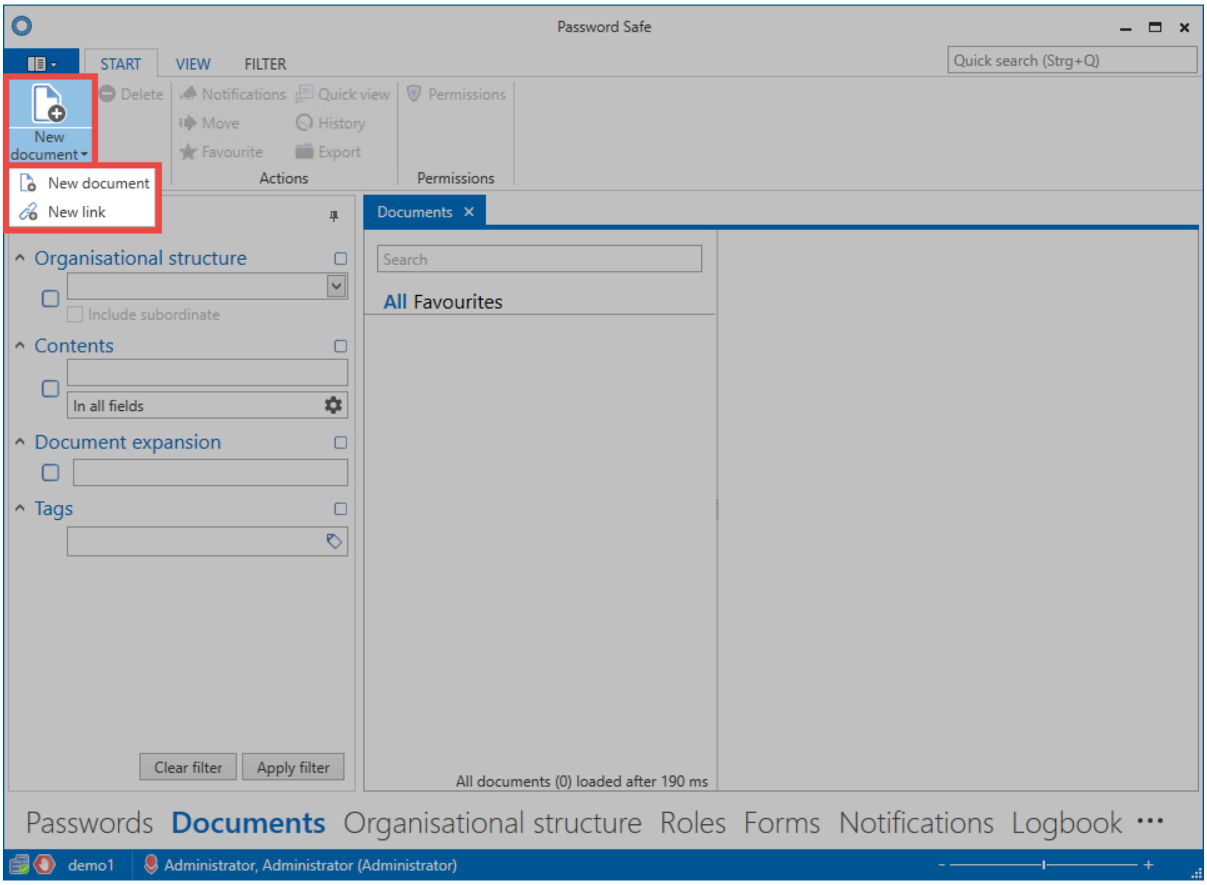

Passwords **Documents** Organisational structure Roles Forms Notifications Logbook Applications Password reset ···

! The right **Can add new documents** is required

Adding documents

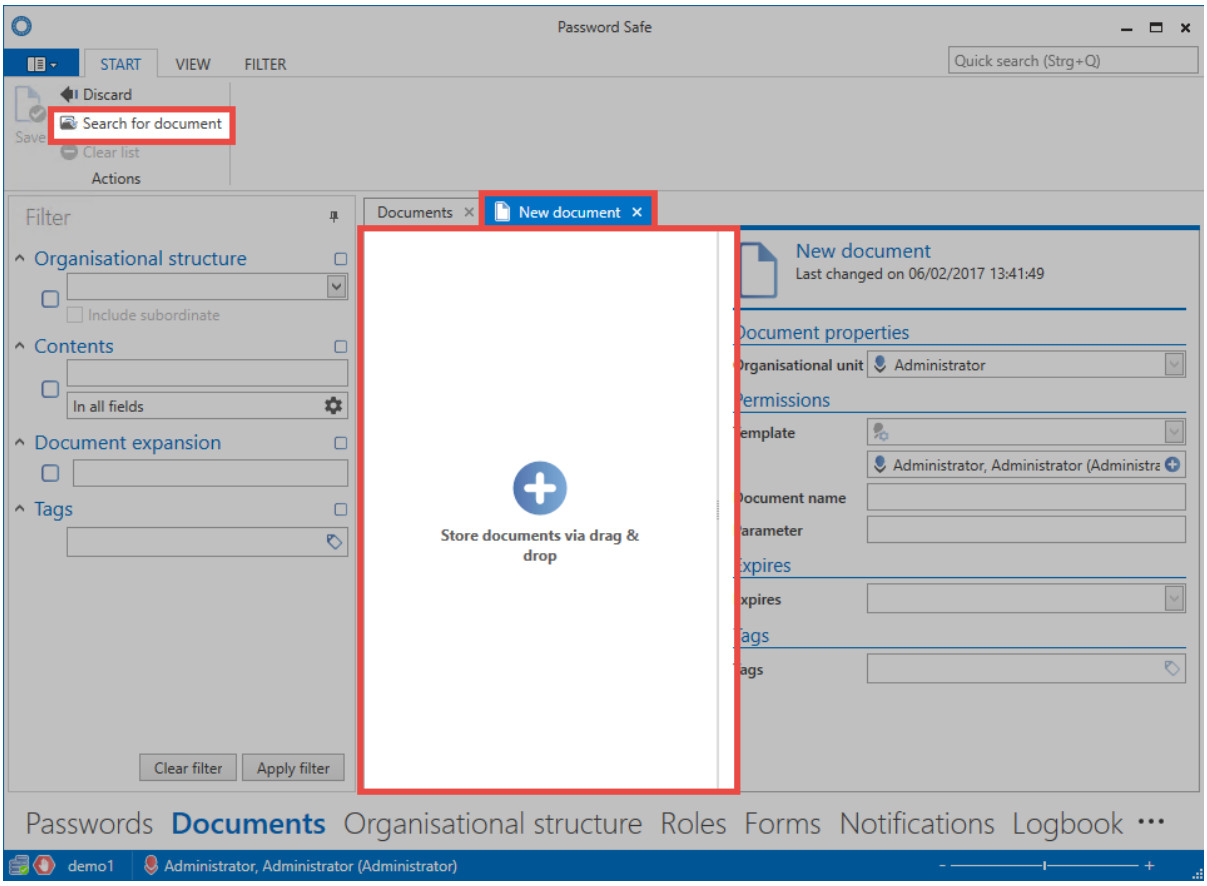
There are two ways to manage documents and files in Password Safe v8:

1. **Creating a link:** In this case, only a file that is located locally or on a network drive will be linked. The file itself is not stored in the database. Neither version management nor the traceability of changes in the history are possible.
2. **Storing the document in the database:** The file becomes part of the encrypted database. It is saved within the database and can be made available selectively to employees for further processing in the future based on their permissions.



Document selection

When selecting the file to be uploaded, you can either browse your file system via the Explorer view or add objects by drag & drop. The latter gives you the possibility to directly import several documents in one step.



New document
Last changed on 06/02/2017 13:41:49

Organisational unit: Administrator

Template: Administrator, Administrator (Administra

Document name:

Parameter:

Expires:

Tags:

Versioning

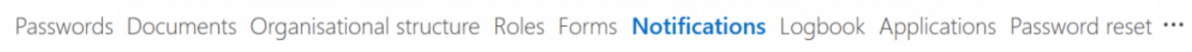
The heart of each document management system is the ability to capture and archive changes to documents or files. All versions of a document can be compared with each other and historical versions can be restored if necessary. Password Safe provides this functionality via the history in the ribbon, as well as in the footer area for the detailed view of a document. This can be used in the same way as the password history. The interplay between the document-specific event logbook and the history provides a complete list of all information that is relevant to the handling of sensitive data. Version management can be used to restore any historical versions of a document.

The file size for a **linked document** can only be updated if the document was opened using Password Safe.

Notifications

What are notifications?

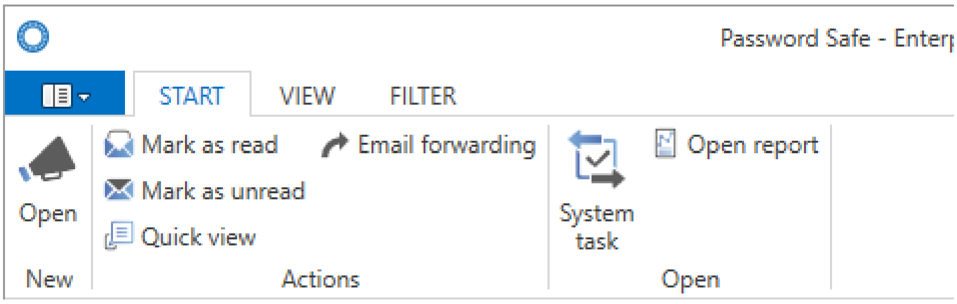
With the notification system, you are always up-to-date on all events that you consider important. Almost all modules allow users to configure when to receive notifications. All configured messages are only created for the currently registered Password Safe user. It is not possible to create a notification for another user. Each user can and should define himself which passwords, which triggers as well as changes are important and informative for him. The configuration of **visibility** is explained in a similar way to the other modules in one place.



The reading pane is deactivated in this module by default. It can be activated in the "Display" tab in the ribbon.

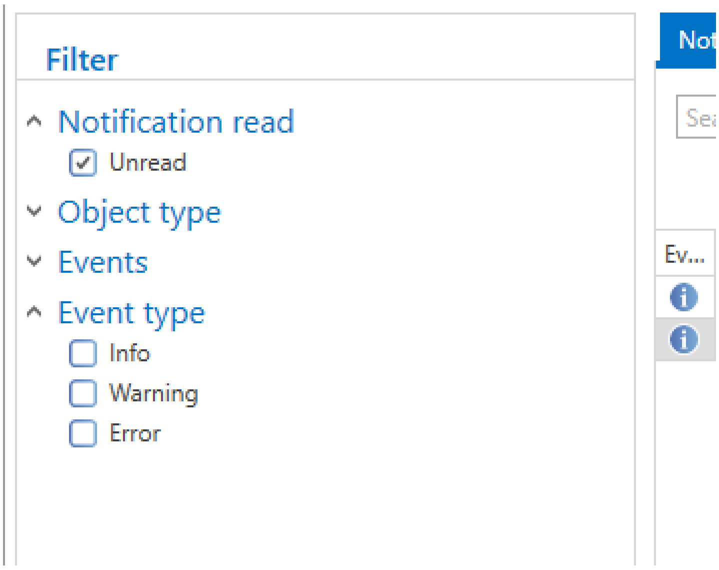
Module-specific ribbon functions

There are also some ribbon functionalities that are exclusively available for the notification module. In particular, the function **Forward important notifications to email addresses** enables administrators and users to maintain control and transparency independent of the location.



Mark notifications as read

The two buttons on the ribbon enable you to mark notifications as read/unread. The filter criterion available in this context (see following screenshot) enables, in particular, fast sorting according to current and also historical notifications.



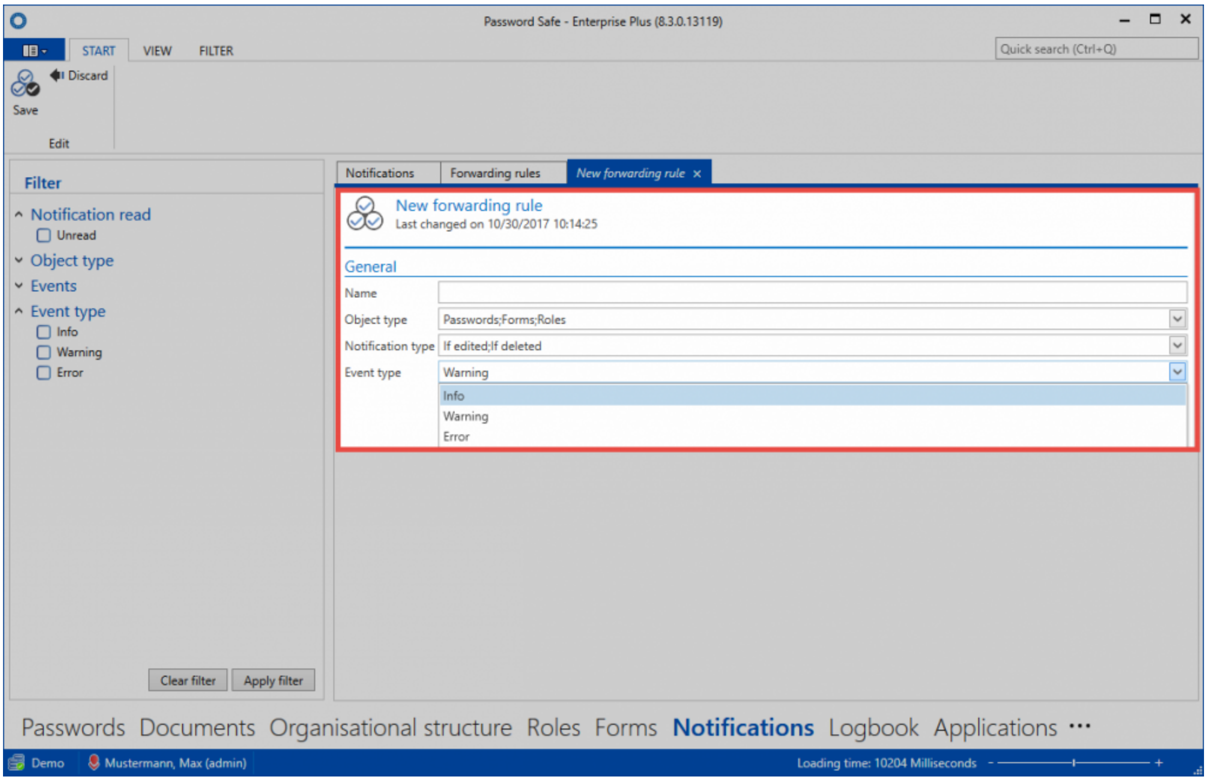
Filter

- Notification read
  - ☑ Unread
- Object type
- Events
- Event type
  - □ Info
  - □ Warning
  - □ Error

It is possible to mark the notifications as read/unread via the ribbon and also via the context menu that is accessed using the right mouse button. If the corresponding setting has been activated, opening a notification will also mean that it is marked as read.

Email forwarding

Various forwarding rules can be defined via the ribbon. A rule defines when a notification should be forwarded to email.



New forwarding rule
Last changed on 10/30/2017 10:14:25

General

Name	
Object type	Passwords;Forms;Roles
Notification type	If edited;If deleted
Event type	Warning

Info
Warning
Error

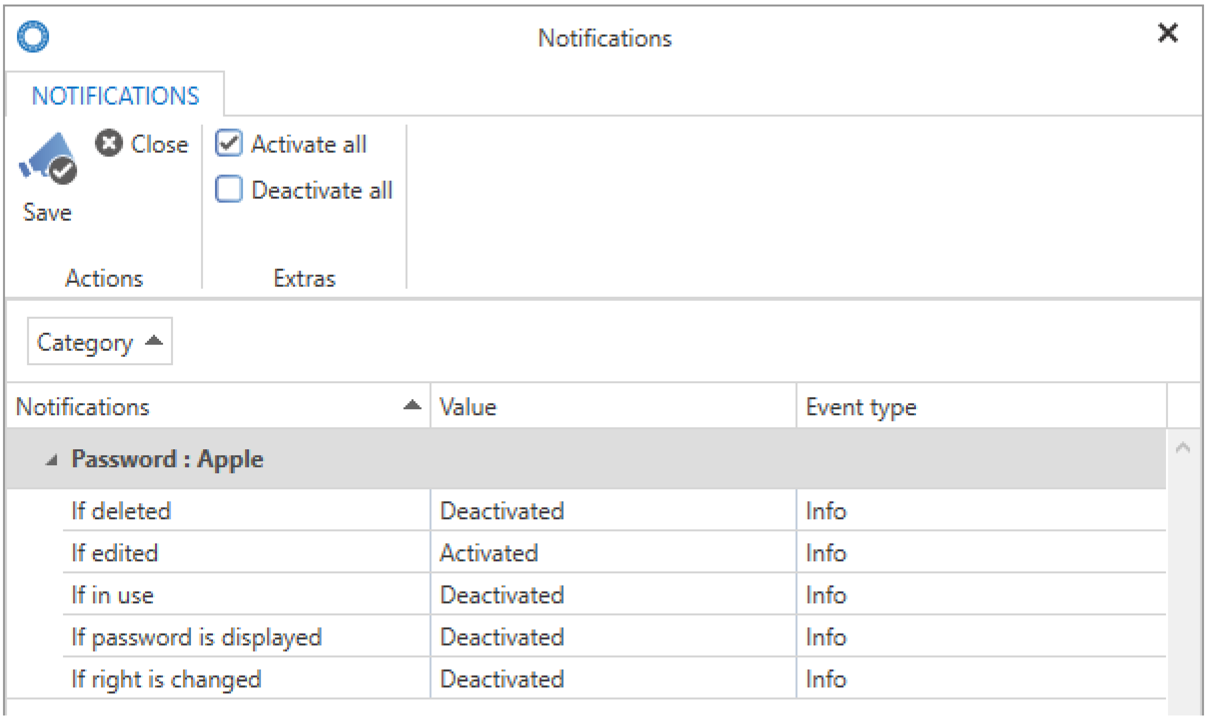
In this example, all notifications that match the stated object type (passwords, forms, roles) and notification type (when edited, when deleted) are forwarded. In addition, it is also possible to filter according to the notification type (=Event type).

> ✻ The prerequisite for the forwarding of notifications is that an email address has been saved for the logged-in user under account in the main menu

Opens the record that is the subject of the notification in a separate tab

Manual configuration of notifications

Irrespective of the selected module, permissions can be configured manually for objects. The following dialogue can be opened via the ribbon in the “Actions” tab:



Notifications ▲	Value	Event type
Password : Apple		
If deleted	Deactivated	Info
If edited	Activated	Info
If in use	Deactivated	Info
If password is displayed	Deactivated	Info
If right is changed	Deactivated	Info

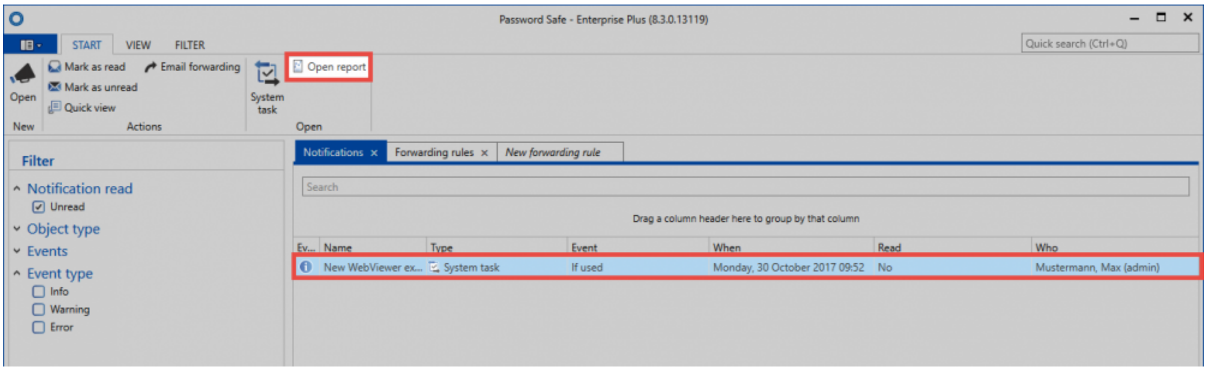
- **Notification**: Definition for the trigger
- **Value**: Defines whether a notification should be created for the previously defined trigger. In the example for the “Apple” record, this only occurs when the record is edited.
- **Event type**: The event type for the generated notifications can be either “Info”, “Warning” or “Error”. This information can also be used e.g. as an additional filter criterion.

In contrast to previous editions, it is best to configure the notifications manually. This ensures that a notification is really only triggered for relevant events.

Other triggers for notifications

As well as manually configurable notifications, there are other triggers in Password Safe which will result in notifications.

- **Seal**: Requests to release sealed records are handled via the notification system
- **System tasks**: If reports are automatically created via the system tasks, these are also made available in the form of a notification. If this type of notification is selected, it can be directly opened via the corresponding button that appears on the ribbon.



Ev...	Name	Type	Event	When	Read	Who
ⓘ	New WebViewer ex...	System task	If used	Monday, 30 October 2017 09:52	No	Mustermann, Max (admin)

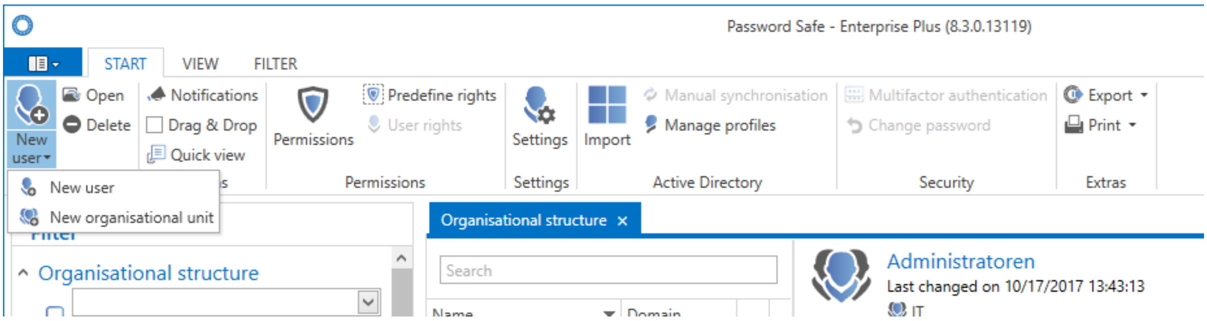
Organisational structure

What are organisational structures?

The storage of passwords or documents ultimately always takes place according to defined organisational structures. The module enables arbitrarily complex structures to be defined, which later form the basis for the systematic storage of data. It is often possible to define them on the basis of already existing organigrams for the company or the department. Of course, it is also possible to use other criteria, such as the function / activity performed, as the basis for creating hierarchies. It is always up to the customer themselves to decide which structure is most useful for the purpose of the application. The configuration of **visibility** is explained in a similar way to the other modules in one place.

Module-specific ribbon functions

The operation of the ribbon differs fundamentally in a couple of aspects to how it works in other modules. The following section will focus on only those elements of the ribbon that differ. The remaining actions have already be explained for the password module.

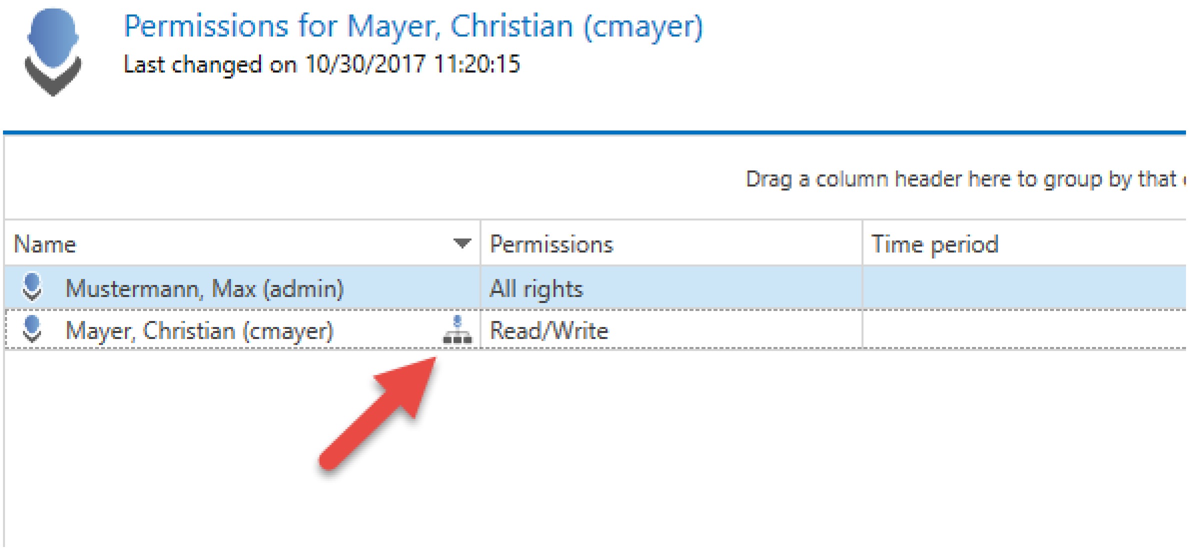


- **New organisational unit/user**: New organisational units or new users can be added via the ribbon, the keyboard shortcut “CTRL + N” or also the context menu that is accessed using the right mouse button. Due to its complexity, there is a separate section for this function: New organisational structures / new user
- **Drag & Drop**: If this option has been activated, it is possible to move users or organisational units in list view via drag & drop
- **Permissions**: The configuration of permissions within the organisational structure is important both for the administration of the structure and also as the basis for the permissions in accordance with inheritance from organisational structures. The benefits of **“predefining rights”** are explained in a separate section.

- **Settings**: The settings can be configured for both users and also organisational units. More information on user settings…
- **Active Directory**: The connection to Active Directory (available from the Enterprise Edition upwards) is explained in a dedicated section
- **Multifactor authentication**: Additional security during login is provided through positive authentication based on another factor. More on this subject…
- **Reset password**: Administrators can reset the passwords with which users log in to Password Safe to a defined value. Naturally, this is only possible if the connection to Active Directory is configured via end-to-end encryption. In the alternative Master Key mode, the authentication is linked to the correct entry of the AD password.

✻ To reset a user password, membership for the user is a prerequisite.

The example below shows the configuration of a user where only the user themselves is a member.



Permissions for Mayer, Christian (cmayer)

Last changed on 10/30/2017 11:20:15

Drag a column header here to group by that

Name	Permissions	Time period
Mustermann, Max (admin)	All rights	
Mayer, Christian (cmayer)	Read/Write	

This configuration means that the user password cannot be reset by administrators. The disadvantage is that if the password is lost there is no technical solution for “resetting” the password in the system.

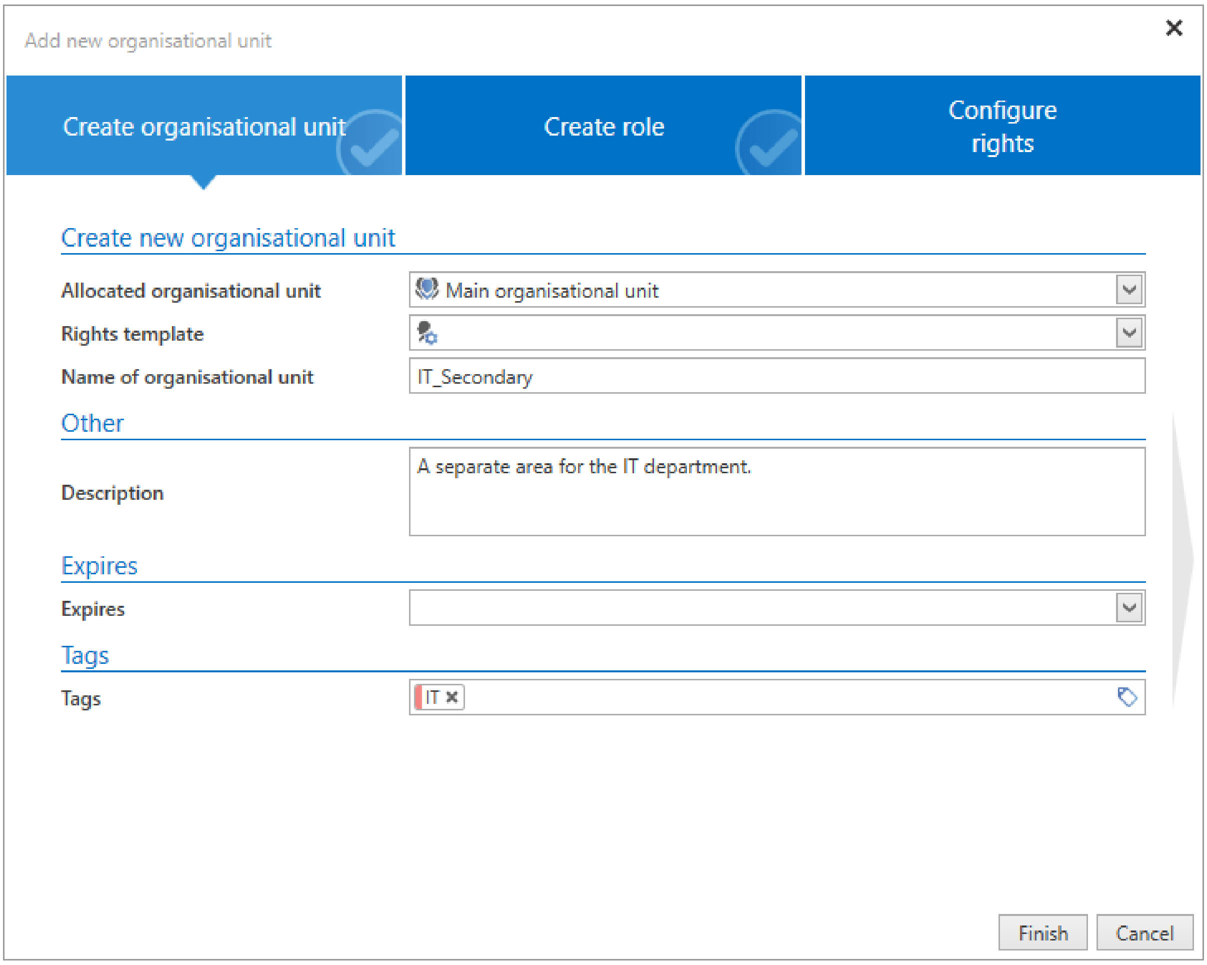
! It is*not* recommended to configure the permissions so that only the user themselves has membership. No other interventions can be made if the password is then lost.

Adding local organisational units

! The right **Can add new organisational units** and the ability to view the *organisational units module” are required

Both users and also organisational units themselves can be added as usual via the ribbon (alternatively via Ctrl + N or via the context menu). These processes are supported by various wizards. The example below shows the creation of a new organisational unit:

Create organisational unit



Create new organisational unit

Allocated organisational unit: Main organisational unit

Rights template:

Name of organisational unit: IT_Secondary

Other

Description: A separate area for the IT department.

Expires

Expires:

Tags

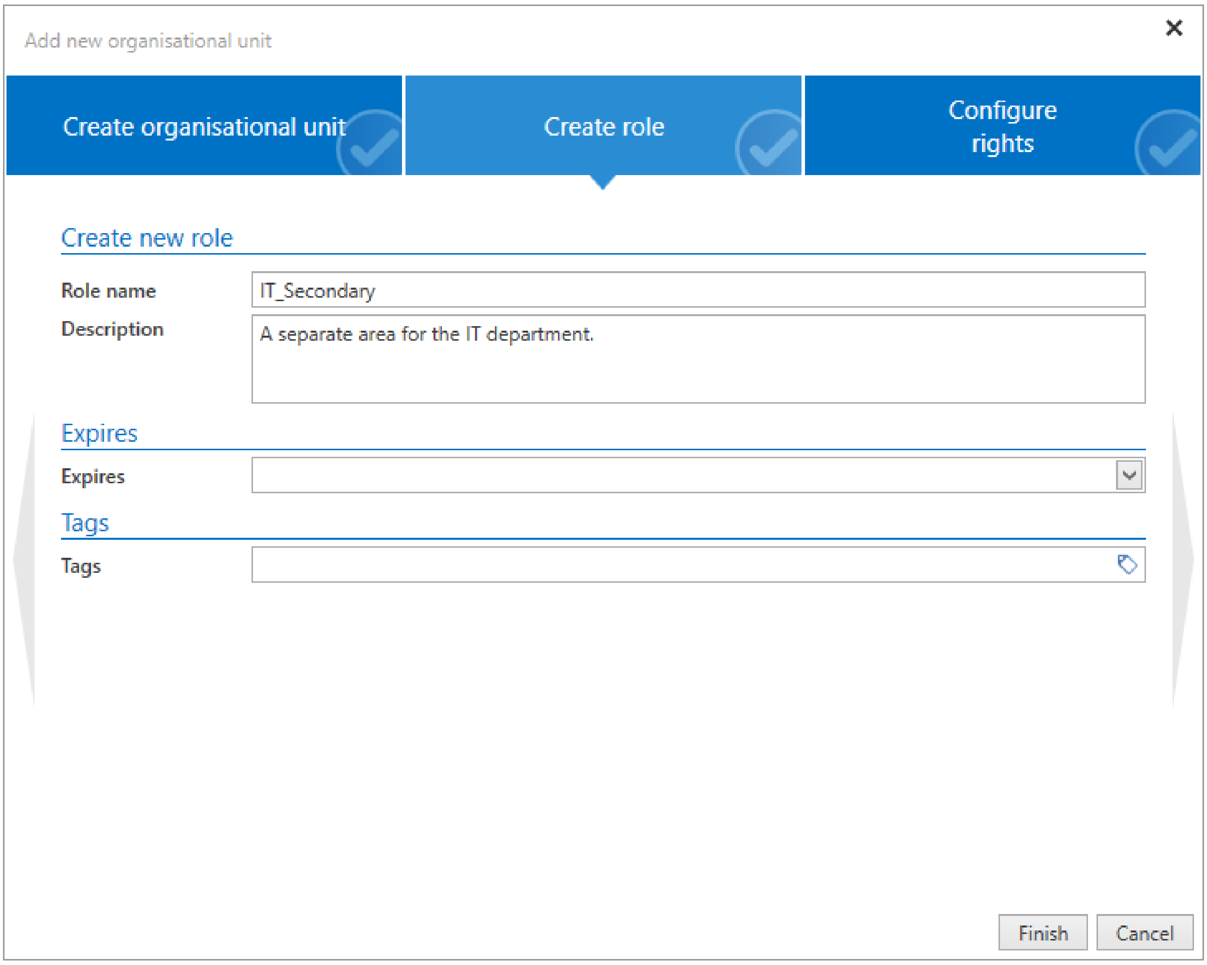
Tags: IT

- **Allocated organisational unit**: If its defined here as the **main organisational unit**, the new object is not allocated to an existing organisational unit

- **Rights template group**: If an already existing organisational unit was selected under “allocated organisational unit”, you can select one of the existing rights template groups here

> The organisational unit marked in list view will be used as a default. This applies to the fields “allocated organisational unit” and also “rights template”.

Create role



Create new role

Role name: IT_Secondary

Description: A separate area for the IT department.

Expires

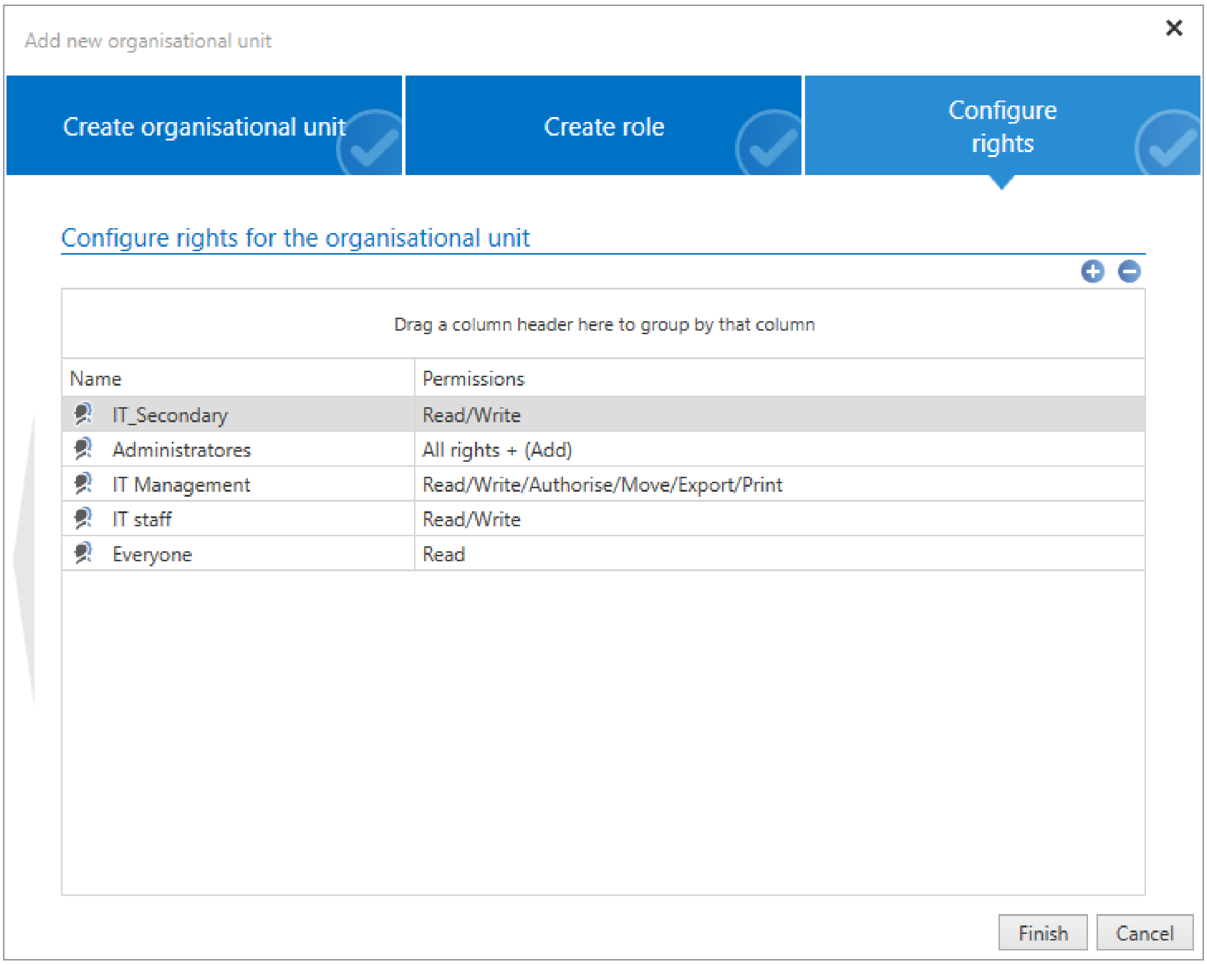
Expires:

Tags

Tags:

When creating a new organisational unit, the second tab in the wizard enables you to directly create a new role. This role will not only be created but also given “read” rights to the newly created organisational unit.

Configuring rights


Add new organisational unit
Create organisational unit
Create role
Configure rights
Configure rights for the organisational unit
Drag a column header here to group by that column
Finish
Cancel

Name	Permissions
IT_Secondary	Read/Write
Administratores	All rights + (Add)
IT Management	Read/Write/Authorise/Move/Export/Print
IT staff	Read/Write
Everyone	Read

The third tab of the wizard allows you to define the permissions for the newly created organisational unit. If an allocated organisational unit or a rights template group was defined in the first tab, the new organisational unit will inherit its permissions. Here, these permissions can be adapted if desired.

Managing users

How are users managed in Password Safe?

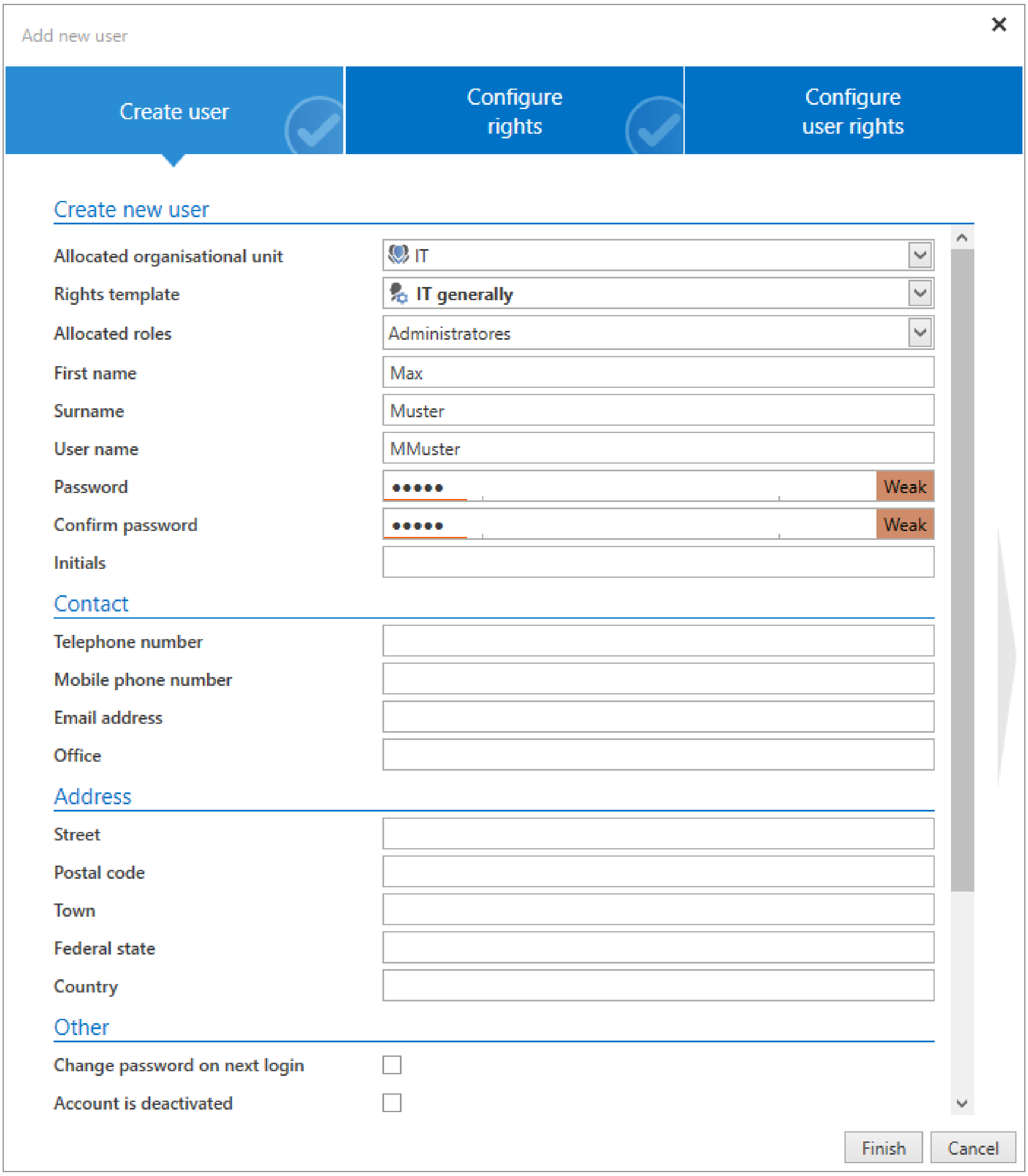
The way in which users are managed is highly dependent on whether Active Directory is connected or not. In Master Key mode, Active Directory remains the leading system. Accordingly, users are then managed on AD. If Password Safe is the leading system e.g. in end-to-end mode, users are managed in the organisational structures module. More details are provided in the relevant sections. More…

Adding local users

! The right **Can add new users** and the ability to view the **organisational units module** are required

In general, new users are added in the same way as creating a local organisational unit. Therefore, only the differences will be covered below.

Creating users



Create new user

Allocated organisational unit	IT
Rights template	IT generally
Allocated roles	Administratores
First name	Max
Surname	Muster
User name	MMuster
Password	●●●●● Weak
Confirm password	●●●●● Weak
Initials	

Contact

Telephone number	
Mobile phone number	
Email address	
Office	

Address

Street	
Postal code	
Town	
Federal state	
Country	

Other

Change password on next login	□
Account is deactivated	□

- **Allocated roles**: New users can be directly allocated one or more roles when they are created
- **Change password on next login**: The user will be prompted to change their user password on the next login (obligatory)
- **Account is deactivated**: The user is created with the status “deactivated”. The account is thus not useable. The write rights for a user can be set/removed with this option. In editing mode, the account can also be deactivated during ongoing operation.
- **Restricted user**: Controlling entities exist in many companies that are only tasked with checking the integrity and hierarchies of various pieces of information with one another but are not required

to productively work with the information themselves. This could be a data protection officer or also an administrator in some cases. This would be the case if an administrator was responsible for issuing permissions to other people but should not be able to view the data themselves. The property **restricted user** is used to limit the visibility of the password field. It thus deals with purely administrative users or controlling entities.

Restricted users cannot view any passwords

Configuring rights

The second tab of the wizard allows you to define the permissions for the newly created user. If an allocated organisational unit or a rights template group was defined in the first tab, the new user will inherit its permissions. Here, these permissions can be adapted if desired.

Configuring user rights

Users always receive their user rights via a role, which is either user-specific or global (see user rights). If no role is defined in the first tab “Create user”, the third tab will thus contain globally defined user rights.

Importing users

Importing from Active Directory can be carried out in two ways that are described in a separate section.

User passwords / logging in to client

User passwords

Depending on the type of user, they will either be allocated their password in Password Safe or the login will be carried out using access data for the domain. How the user logs in also differs according to the type of user.

Differences between users and passwords

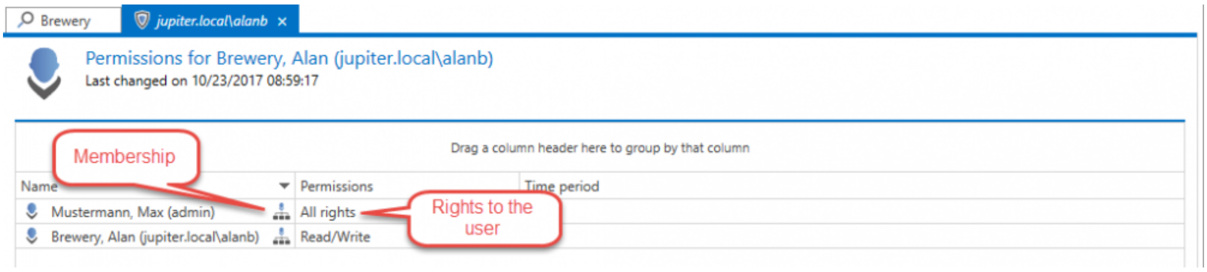
- **Local users**
  Local users are those users that were directly created in Password Safe. These users must be directly assigned a password when they are created. If local users are migrated from older versions, they receive a randomly generated password that is sent to them via email.

- **AD users in end-to-end mode**
  These users must also be assigned a password in Password Safe. A new password will also be issued via email for these users in the case of a possible migration.

- **AD users in Master Key mode**
  These users log in directly with access data for the domain. It is thus not necessary to assign them a password. As these users directly authenticate themselves via Active Directory, the currently saved password in Active Directory is thus always valid. These users can still directly log in using the existing password even after a migration

Required rights

Various rights are required in order to issue or change user passwords. One prerequisite is the user right **Can display organisational structure module**. **Read** and **write** rights for the user are also required. Finally, membership of the user is required. Normally, the user themselves and the user who created or imported the user have the right to change their password.



Permissions for Brewery, Alan (jupiter.local\alanb)
Last changed on 10/23/2017 08:59:17

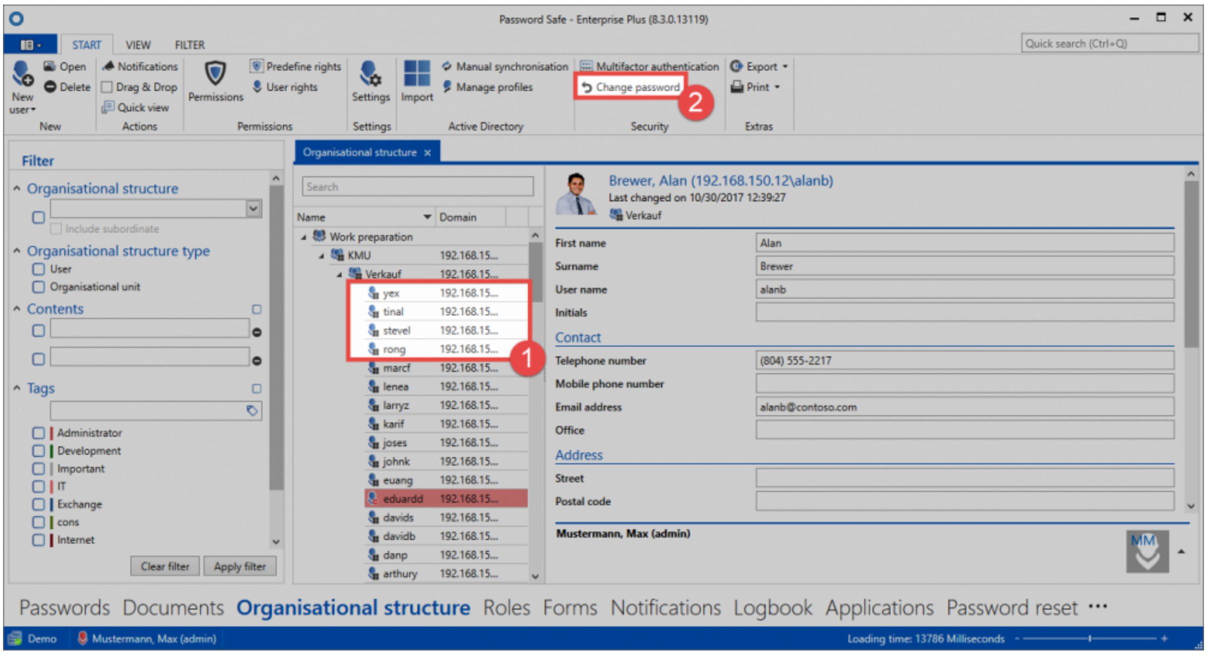
Drag a column header here to group by that column

Name	Permissions	Time period
Mustermann, Max (admin)	All rights	
Brewery, Alan (jupiter.local\alanb)	Read/Write	

Assigning and changing passwords

As already explained, local users are directly assigned their initial password when the user is created. The situation is different for users that are imported in end-to-end mode. They do not possess a password directly after the import and can thus not log in. It is thus necessary to assign passwords after the import.

The passwords can be directly assigned or changed via the ribbon. Naturally, it is also possible to select multiple users if e.g. several imported users should be assigned the same password.

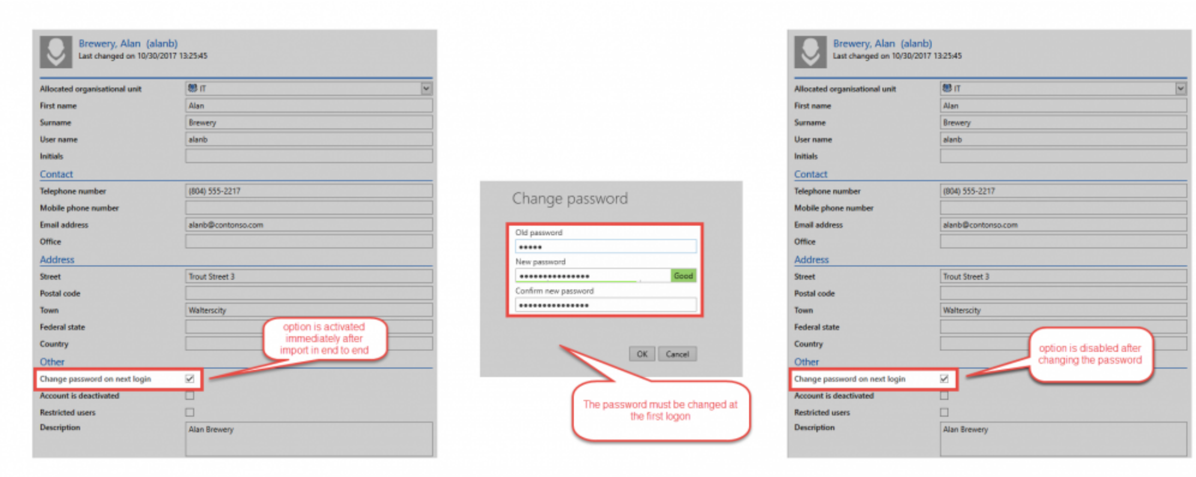


Brewer, Alan (192.168.150.12\alanb)
Last changed on 10/30/2017 12:39:27
Verkauf

First name	Alan
Surname	Brewer
User name	alanb
Initials	
Telephone number	(804) 555-2217
Mobile phone number	
Email address	alanb@contoso.com
Office	

Change password on next login

Even if several users receive the same initial password, it is sensible to force them to change it to an individual password. There is a corresponding option for this purpose. In the case of **local users**, this can be activated during the creation of the user. In the case of **users in end-to-end mode**, this option is directly activated during import for security reasons. This option is automatically deactivated after the user has successfully logged in and changed the password.



Brewery, Alan (alanb)
Last changed on 10/30/2017 13:25:45

Allocated organisational unit	IT
First name	Alan
Surname	Brewery
User name	alanb
Initials	
Contact	
Telephone number	(804) 555-2217
Mobile phone number	
Email address	alanb@contonso.com
Office	
Address	
Street	Trout Street 3
Postal code	
Town	Walterscity
Federal state	
Country	
Other	
Change password on next login	☑
Account is deactivated	□
Restricted users	□
Description	Alan Brewery

option is activated immediately after import in end to end

Change password

Old password: •••••

New password: ••••••••••••••• Good

Confirm new password: •••••••••••••••

The password must be changed at the first logon

option is disabled after changing the password

Security of passwords

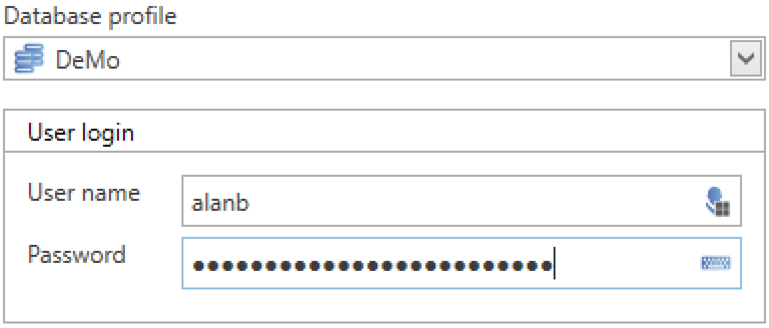
To guarantee that passwords are sufficiently strong, it is recommended that corresponding “password rules”:#passwortrichtlinien are created. It is especially important to ensure here that user names are excluded. The password rule then still needs to be defined as a “user password rule”:#administration.

Logging in to the database

The process for logging into the database differs depending on the type of user.

Local user

Local users simply log in using their user name and the assigned password.



Database profile: DeMo

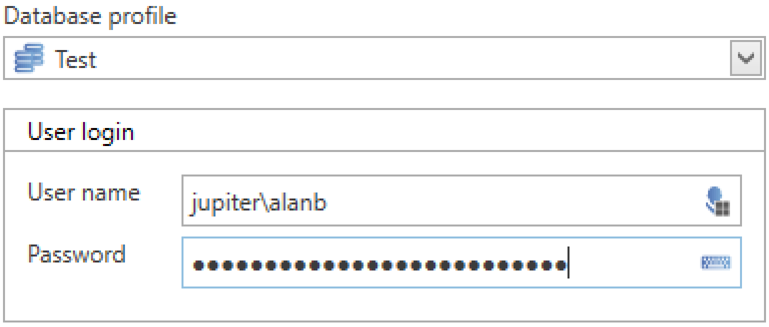
User login

User name: alanb

Password: •••••••••••••••••••••••••

AD user

If only one domain has been configured, the users from AD can also log in with their user name and password the same as local users. If multiple domains have been configured or there is a local user with the same name, the name of the domain must be entered in front of the user name:



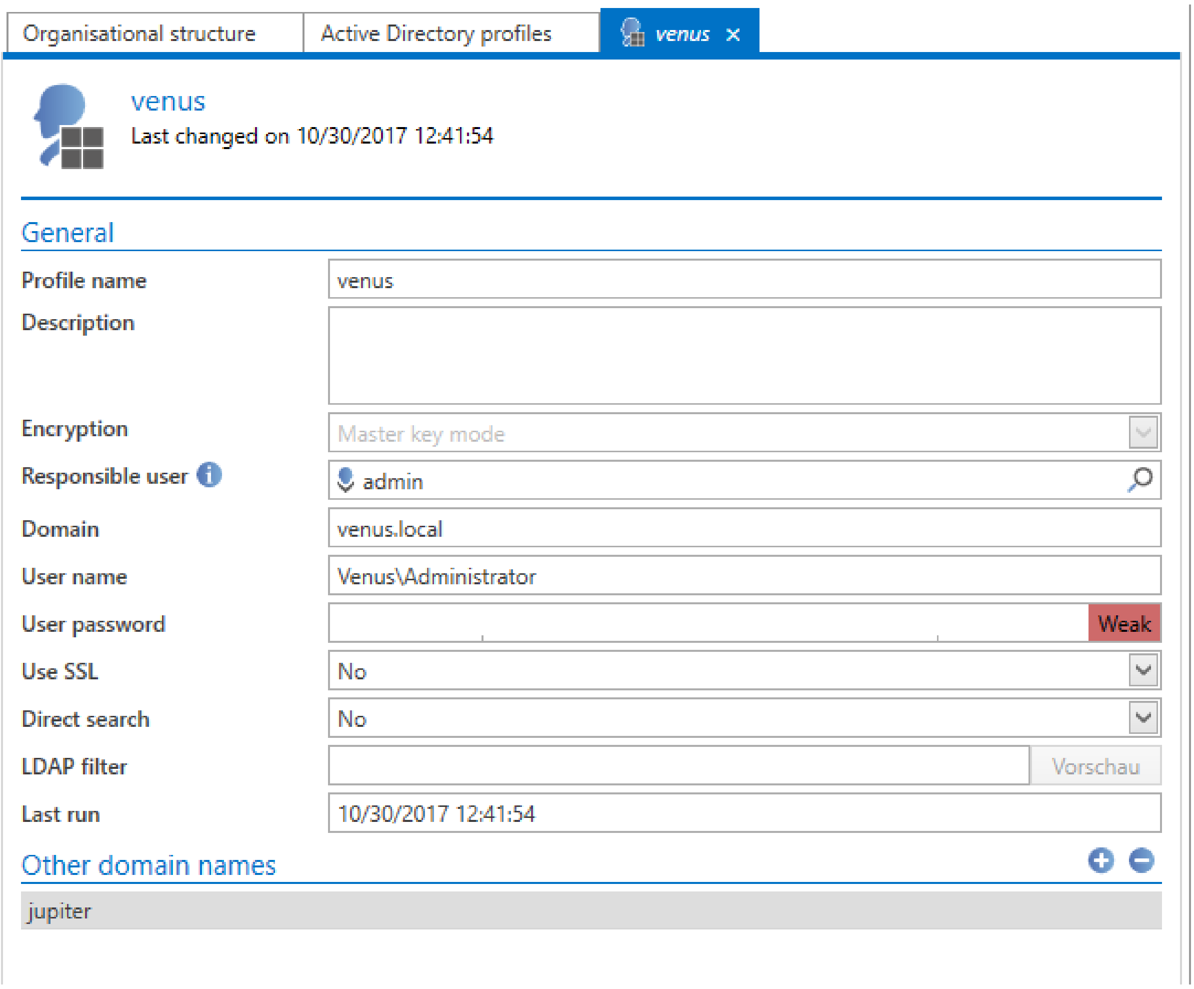
Database profile: Test

User login

User name: jupiter\alanb

Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●

The name of the domain must be entered as it is configured in the AD profile under **Domains**. The option **Other domain names** can be used to save other forms of the domain name.



venus
Last changed on 10/30/2017 12:41:54

General

Profile name	venus
Description	
Encryption	Master key mode
Responsible user	admin
Domain	venus.local
User name	Venus\Administrator
User password	Weak
Use SSL	No
Direct search	No
LDAP filter	Vorschau
Last run	10/30/2017 12:41:54

Other domain names

jupiter

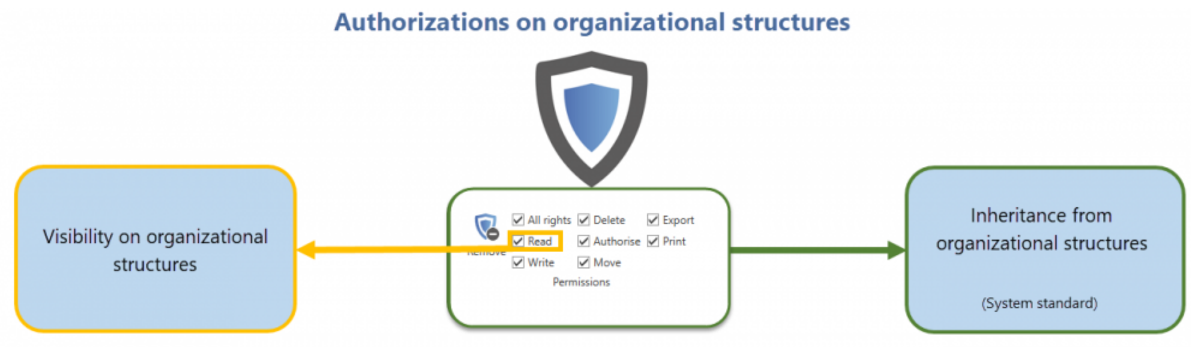
Permissions for organisational structures

Relevance

These permissions primarily define which users/roles have what form of permissions for organisational structures. In addition, there are **two mechanisms** that directly build on the permissions for organisational structures.

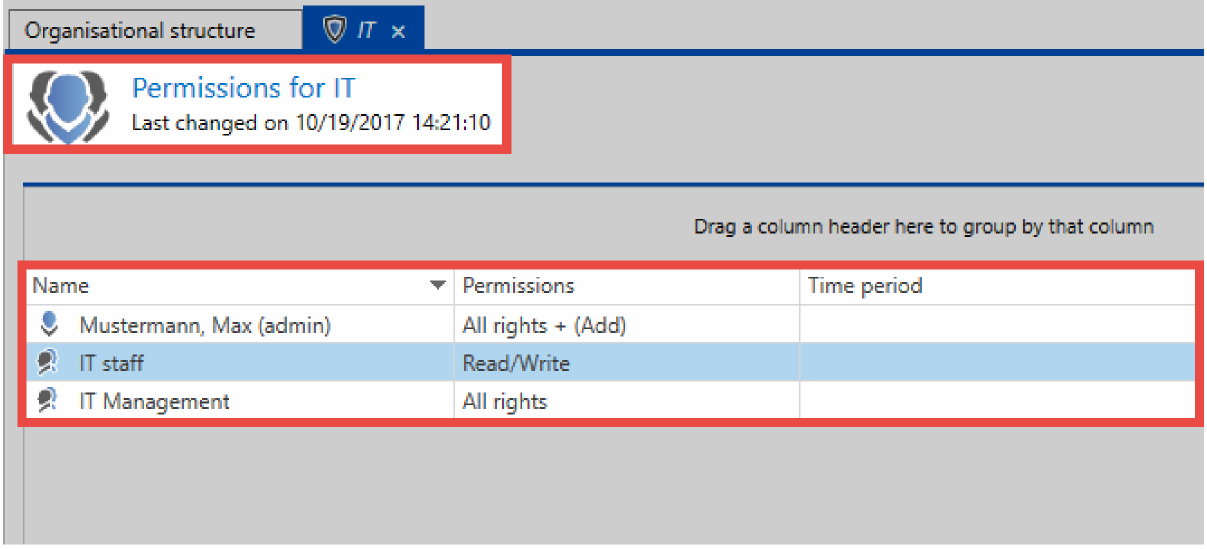
1. **Limiting visibility**: It was already explained in the section on visibility that selectively withholding information is a very effective “protective mechanism”:#schutzmechanismen. Configuration of the visibility is carried out directly when issuing permissions to organisational structures.
2. **Inheriting permissions for records**: Inheritance from organisational structures is defined as a system standard. This means that there is **no** difference between the permissions for an organisational structure and the permissions for data that is stored in these organisational structures.

The way in which permissions for organisational structures are designed thus effects the subsequent work with Password Safe in many ways. The following diagram describes the above-mentioned interfaces.


Authorizations on organizational structures
Visibility on organizational structures
All rights
Delete
Export
Read
Authorise
Print
Write
Move
Permissions
Inheritance from organizational structures
(System standard)

Permissions for organisational structures

The visibility and also inheritance mechanisms are not considered below. This section exclusively deals with permissions for the actual organisational structure. It deals with which users and roles have what form of permissions for a given organisational structure. Permissions for organisational structures can be defined via the ribbon or also the context menu that is accessed using the right mouse button. A permissions tab appears:



Permissions for IT

Last changed on 10/19/2017 14:21:10

Drag a column header here to group by that column

Name	Permissions	Time period
Mustermann, Max (admin)	All rights + (Add)	
IT staff	Read/Write	
IT Management	All rights	

The basic mechanisms for setting permissions is described in detail in the Authorization concept.

It is important that the permissions displayed here are interpreted correctly! The example above shows the permissions for the "organisational structure IT". The user Max Muster possesses all rights to the organisational structure IT and can thus edit, delete and also grant permissions for this structure.

The add right

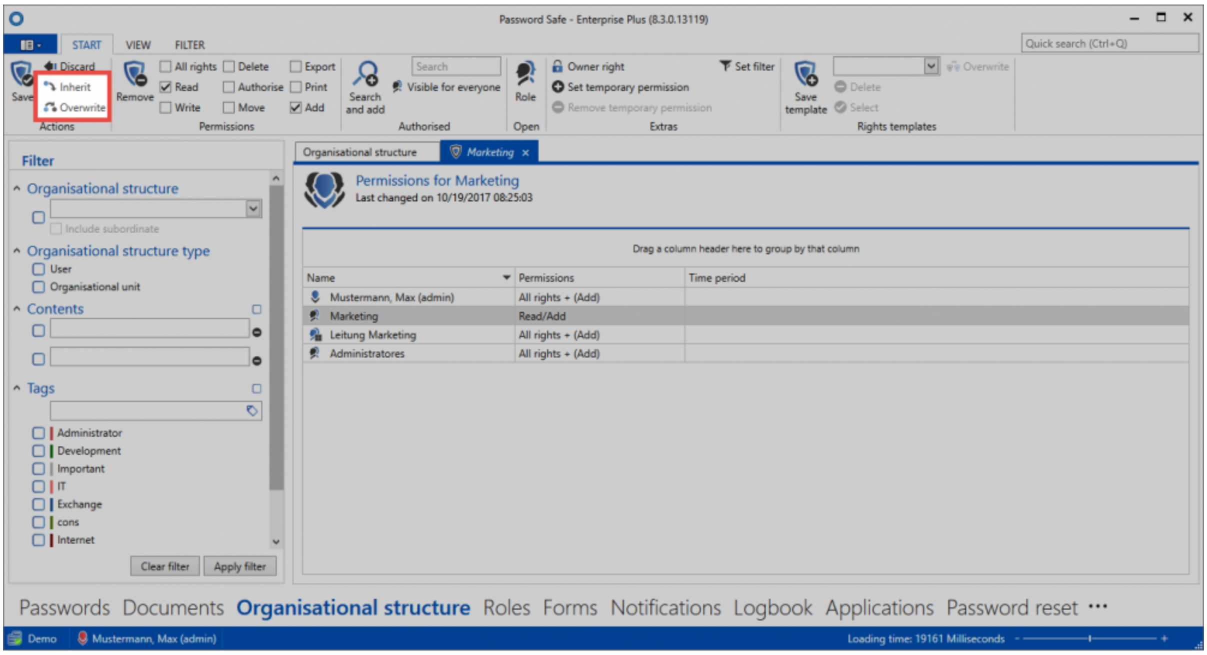
The "add" right holds a special position amongst the available rights because it does not refer to the organisational unit itself but rather to data that will be created within it. In general, it is fair to say that to add objects in an organisational unit requires the add right. If a user wants to add a new record to an organisational unit, the user requires the above-mentioned right. In the example above, only the administrator has the required permissions for adding new records. Even the IT manager – who possess all other rights to the organisational structure "IT" – does not have the right to add records.

! The add right merely describes the right to create objects in an organisational unit.

Inheriting permissions

What is inherited in organisational structures?

If you open the permissions for an organisational structure, the currently configured permissions will be visible. In the following example, there are a total of four roles with varying permissions for the organisational structure.



Permissions for Marketing

Last changed on 10/19/2017 08:25:03

Name	Permissions	Time period
Mustermann, Max (admin)	All rights + (Add)	
Marketing	Read/Add	
Leitung Marketing	All rights + (Add)	
Administratores	All rights + (Add)	

The two highlighted options are now available on the ribbon.

- **Inherit**: This means that all of the configurations defined in the current permissions mask are inherited by underlying organisational structures when it is saved. The permissions are added to existing ones
- **Overwrite**: This means that all of the configurations defined are applied to underlying organisational structures when it is saved. The previous permissions are lost.

Both mechanisms are protected by a confirmation prompt. If both “inherit” and also “overwrite” are selected, “overwrite” is considered the overriding function.

! Both mechanisms are not protected by user rights. The **authorize** right for the organisational structure is required to activate the inheritance or overwrite functions.

Active Directory link

What are active directory profiles?

The connection to Active Directory (AD) is established via so-called AD profiles. These profiles contain all of the information relevant for establishing a connection to AD and enable imports/synchronization of users, organisational units or roles. To connect to various different ADs, it is naturally also possible to create multiple AD profiles.

Two import modes in comparison

When importing from Active Directory, Password Safe distinguishes between two modes, which differ significantly and are explained in separate sections.

- End-to-end encryption
- Master Key mode

In principle, the two variants differ by the presence of the encryption mentioned above. In the solution with active end-to-end encryption **(E2EE)**, the process may be less convenient (see table) but there is a huge benefit in terms of security. In Master Key mode, a master key is created on the server that has full permissions for all users, organisational units and roles. This represents an additional attack vector, which does not exist in end-to-end mode. In return, however, in Master Key mode, users can be updated via synchronization with the Active Directory. Memberships of organisational units and roles are also imported. In the more secure end-to-end mode, this synchronization of the changes must be carried out manually.

> ✻ It is technically possible to create several profiles with different modes. However, this is not recommended for the sake of clarity.

	End-to-end mode	Master Key mode
End-to-end encryption	+	-
Importing user information	+	+
Importing assigned roles	-	+
Importing roles to organisational units	-	+
Synchronizing user information	-	+
Synchronizing assigned roles	-	+
Synchronizing roles with organisational units	-	+

User can be edited in Password Safe	+	-
Organization unit can be edited in Password Safe	+	-
Roles can be edited in Password Safe	+	-
Password can be edited in Password Safe	+	-
Login with domain password	-	+
Password Safe is the leading system	+	-
Active Directory is the leading system	-	+

As can be seen **E2EE offers the highest level of security**. The aim is merely to import users, organisational units and roles. Those must be administered and configured in Password Safe. In contrast, a connection in **Master Key mode offers the highest level of convenience**. It imports not only users, organisational units and roles but also their links and assignments. Synchronization with Active Directory is possible – **The AD is used as the leading system**.

Users, groups and roles

When importing or synchronizing from Active Directory, users are also added as users in Password Safe. Password Safe also uses the organisational units as such.

In order for Password Safe to be quickly integrated into the given infrastructure, roles can also be directly imported from the Active Directory. Namely Active Directory Groups are used to password-safe roles.

> Groups in groups Memberships, which may be present in the Active Directory, will not be displayed within password safe. Both groups are imported as roles, but independent and not linked in any way.

> If Master Key mode has been selected for the Active Directory profile, the AD is the leading system. In this mode, roles that have been imported cannot be changed locally in Password Safe.

- “End-to-end encryption”:#import-mit-profil-mit-e2ee
- Master Key mode

End-to-end encryption

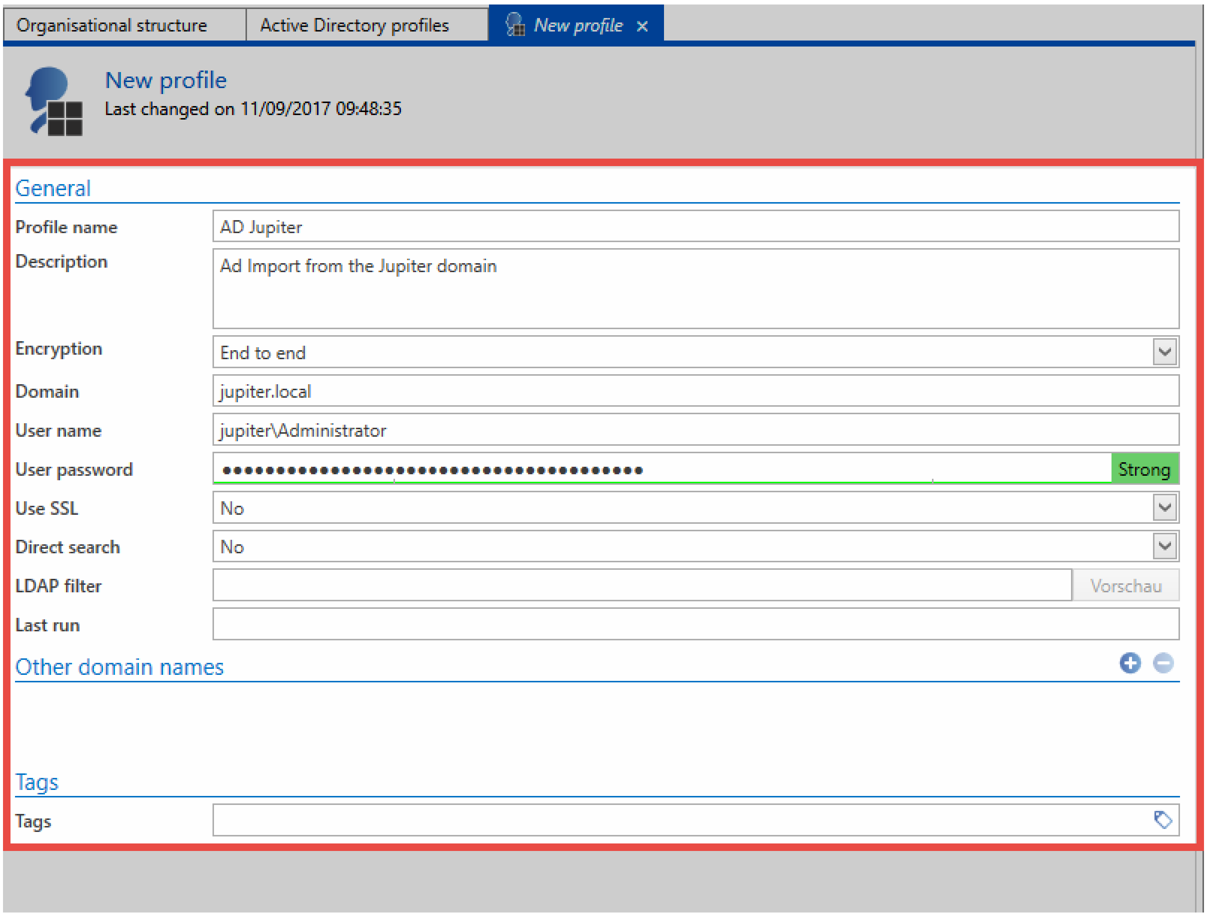
Maximum encryption

The Active Directory profile with active end-to-end encryption currently offers **maximum security**. Only users, organisational units and roles are imported. The permissions and the hierarchical relationship between the individual objects needs to be separately configured in Password Safe. The advantage offered by end-to-end encryption is that Active Directory is “defused” as a possible insecure gateway. In Master Key mode, users who control Active Directory receive de facto complete access to all passwords because resetting a Windows user name enables users to log in under another person’s name. Active Directory is thus the leading system. *Using an active E2EE connection, users require their own password for Password Safe. There is thus no access to users’ data via Active Directory.

Creating profiles

! The right **Can add new Active Directory profiles** and the ability to view the **organisational units module** or the “roles module” are required.

The process for creating a new profile is started via the icon “manage profile” on the ribbon.



New profile
Last changed on 11/09/2017 09:48:35

General

Profile name	AD Jupiter
Description	Ad Import from the Jupiter domain
Encryption	End to end
Domain	jupiter.local
User name	jupiter\Administrator
User password	••••••••••••••••••••••••••••••••••••••• Strong
Use SSL	No
Direct search	No
LDAP filter	
Last run	

Other domain names

Tags

Tags	

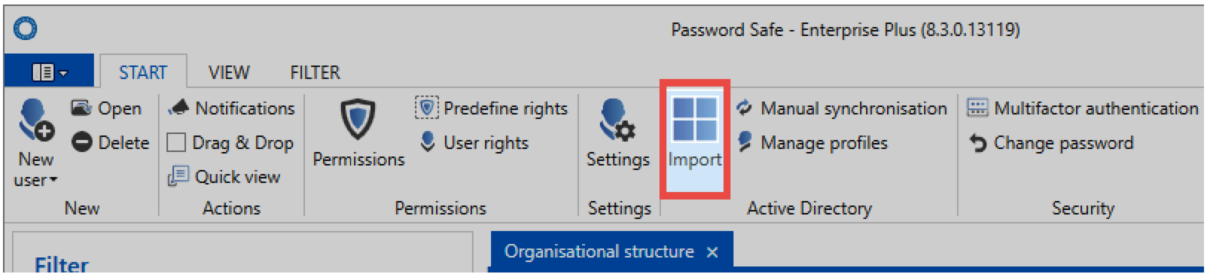
✻ “End-to-end” needs to be set* in the “Encryption” field

A *user is required to access the AD. The user should be formatted as follows: Domain\user. It must have access to the AD.

- The relevant **user password** (domain password) is required for the user mentioned above
- The connection can be established using **SSL** if required by the AD
- **Direct search** is recommended for very large domain trees. The representation of the tree structure is omitted, elements can only be found and selected via the search.
- The **filter** can be used to directly specify an AD path as an entry point via an LDAP query

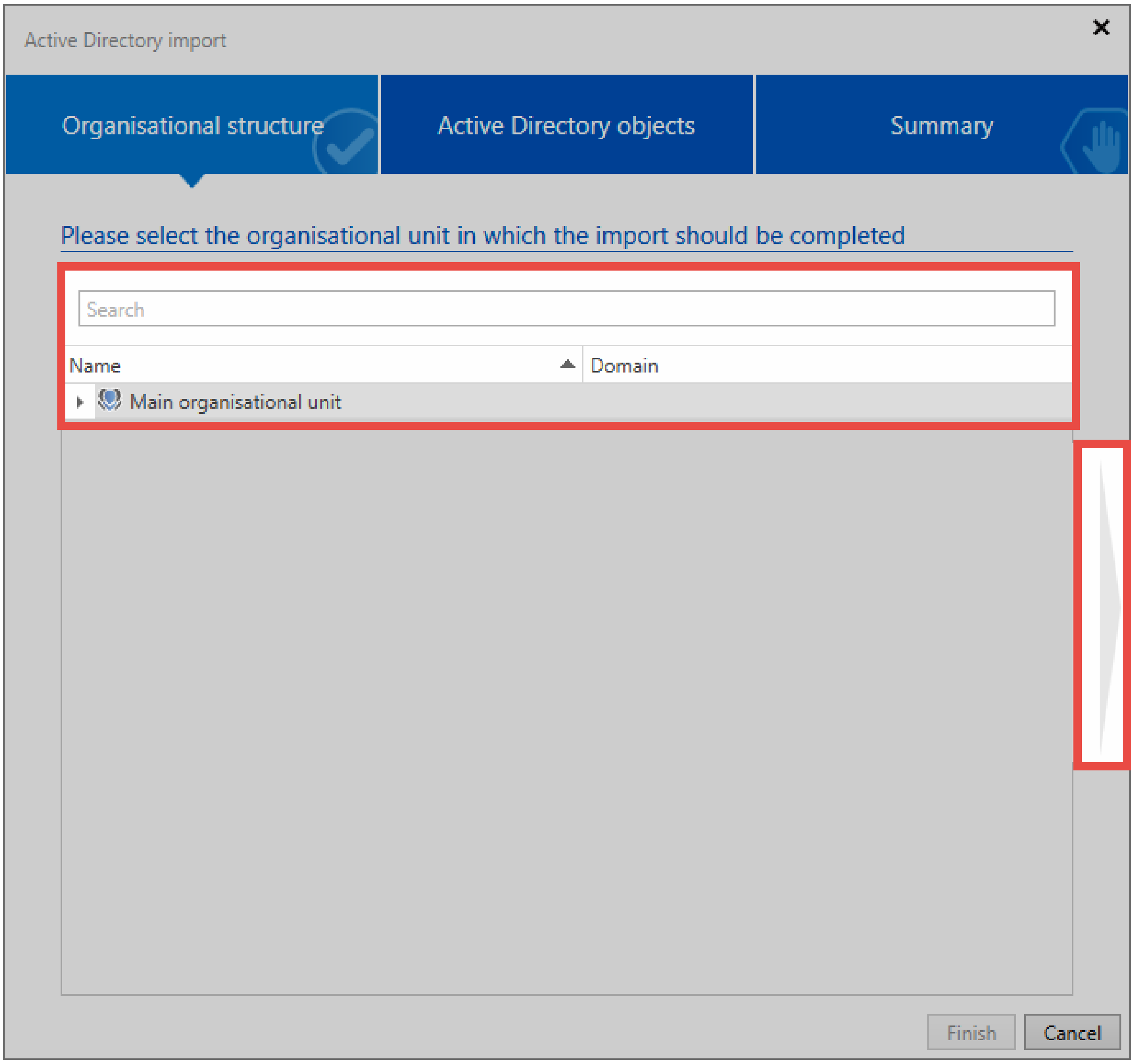
Import

The import is started directly in the ribbon. A wizard guides the user through the entire operation.



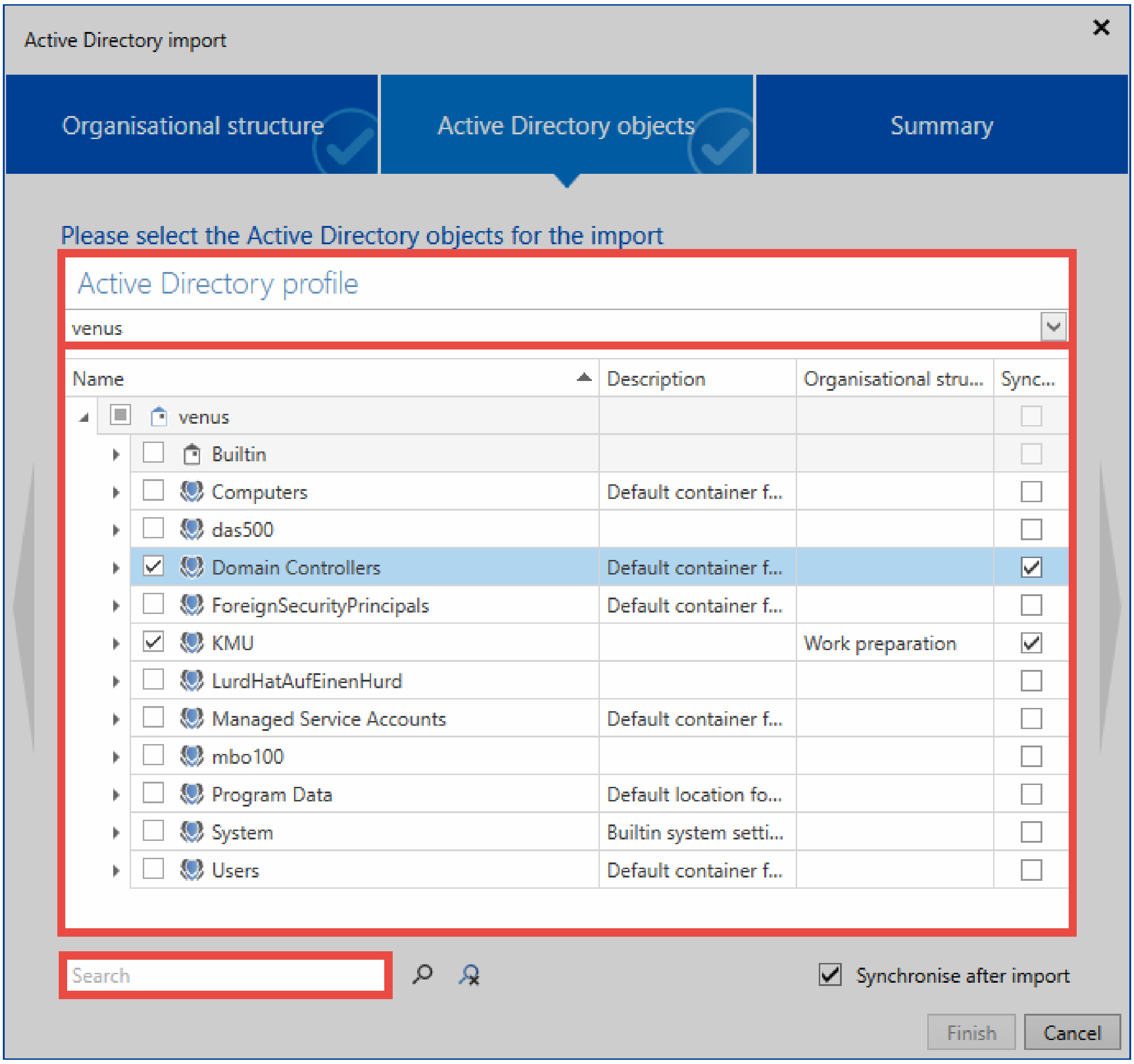
Organisational structure

First, an organisational unit is selected for the import. If there are no organisational units in the database yet, as in this example, the data is imported into the **main organisational unit**.



Active Directory objects

In the next step, select the relevant profile that should be used for the import. Then, select the organisational units and/or users for the import. A search is available for this purpose.



Active Directory import

Please select the Active Directory objects for the import

Active Directory profile

venus

Name	Description	Organisational stru...	Sync...
▣ venus			☐
☐ Builtin			☐
☐ Computers	Default container f...		☐
☐ das500			☐
☑ Domain Controllers	Default container f...		☑
☐ ForeignSecurityPrincipals	Default container f...		☐
☑ KMU		Work preparation	☑
☐ LurdHatAufEinenHurd			☐
☐ Managed Service Accounts	Default container f...		☐
☐ mbo100			☐
☐ Program Data	Default location fo...		☐
☐ System	Builtin system setti...		☐
☐ Users	Default container f...		☐

Search

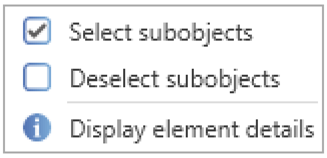
☑ Synchronise after import

It can be seen that the organisational units **Jupiter** and **Contoso** contain items to be imported. The organisational units themselves will not be imported. The check next to the group **Accounting** indicates that the group itself will be imported along with some of its sub-elements.

There are different symbols which indicate the elements to be imported.

☑ The element itself and all possible sub-elements will be imported
■ The element itself and some of its sub-elements will be imported
▣ The element will not be imported; however, it contains elements that will be imported

A context menu that is accessed using the right mouse button is available within the list that provides helpful functions for selecting the individual elements.

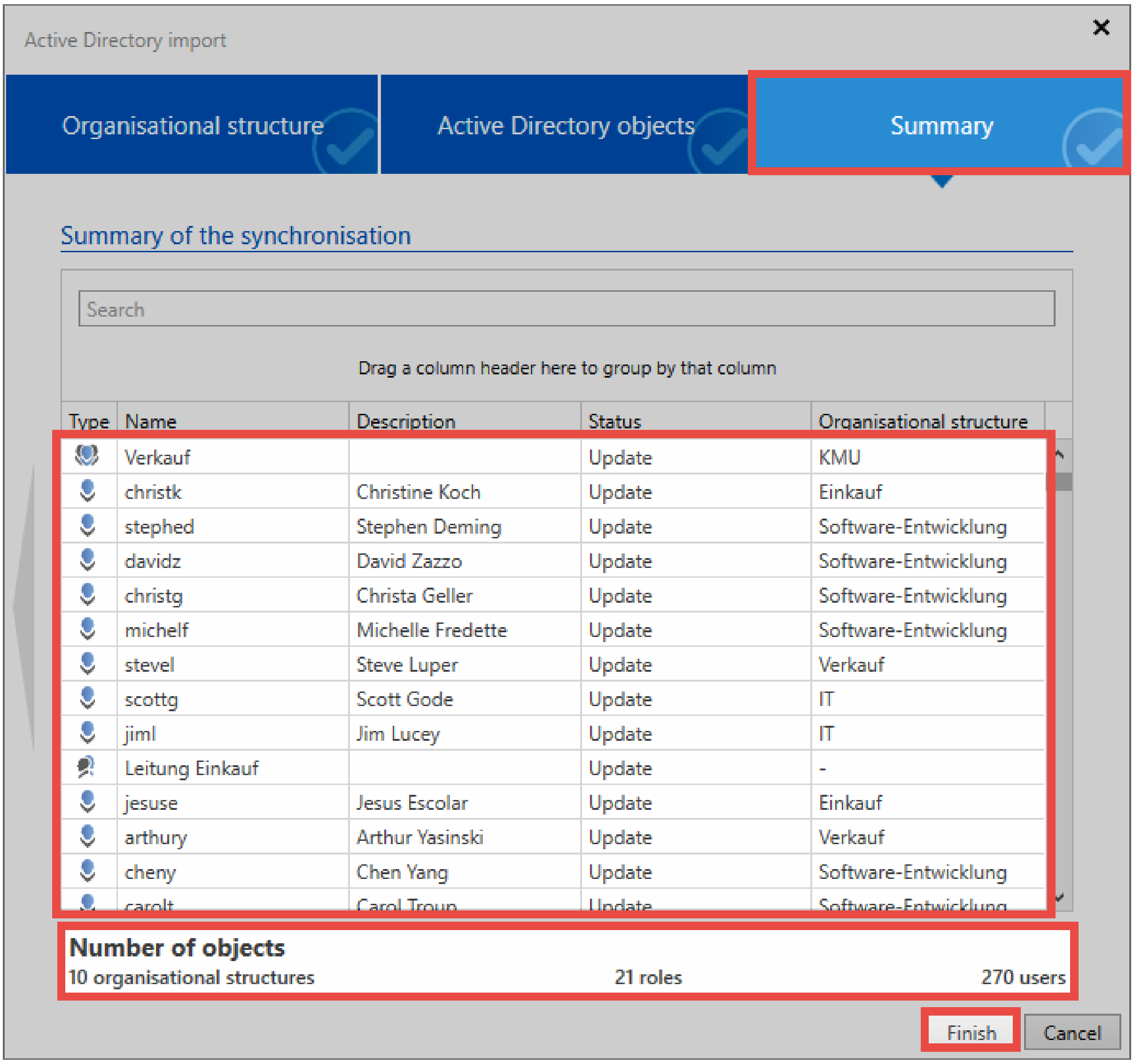


- **Select sub-objects** selects all sub-objects that are located **directly** below the current object
- **Deselect sub-objects** removes tags from all sub-objects that are located **directly** below the current object
- **Reset all items** removes all previously set tags
- **Display element details** lists all information that is available for the current element

> If individual users, organisational units, or roles cannot be selected for import, they have already been imported via another profile

Summary

The last page summarises which objects will be edited and in what form. It specifies the names of the elements along with their descriptions. The **Status** column specifies whether the object is added, updated, or disabled. The last column specifies the organisational unit into which the element is imported. The number of objects is added together at the bottom.



Summary of the synchronisation

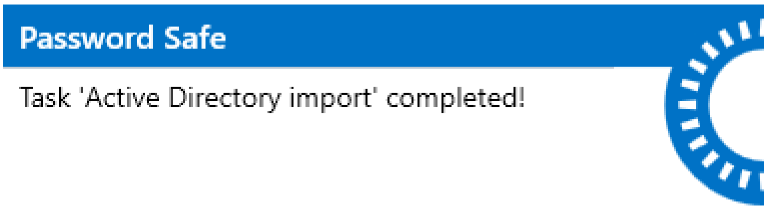
Type	Name	Description	Status	Organisational structure
	Verkauf		Update	KMU
	christk	Christine Koch	Update	Einkauf
	stephed	Stephen Deming	Update	Software-Entwicklung
	davidz	David Zazzo	Update	Software-Entwicklung
	christg	Christa Geller	Update	Software-Entwicklung
	michelf	Michelle Fredette	Update	Software-Entwicklung
	stevel	Steve Luper	Update	Verkauf
	scottg	Scott Gode	Update	IT
	jiml	Jim Lucey	Update	IT
	Leitung Einkauf		Update	-
	jesuse	Jesus Escolar	Update	Einkauf
	arthury	Arthur Yasinski	Update	Verkauf
	cheny	Chen Yang	Update	Software-Entwicklung
	carolt	Carol Troup	Update	Software-Entwicklung

Number of objects
10 organisational structures 21 roles 270 users

✱ Depending on the amount of data, it may take several minutes to create the summary.

Importing

The import itself is carried out by the server in the background. The individual elements then appear in the list one by one. This may take some time, depending on the amount of import data. If the import is terminated, you will receive a confirmation.



Password Safe

Task 'Active Directory import' completed!

✻ As end-to-end encryption is retained in this mode, the server does not receive a key to match already imported users with the AD. There is thus no synchronization with the AD. Similarly, no memberships can be imported. After the import, users must be manually assigned to the appropriate organisational units and roles.

Imported users and organisational units

In end-to-end mode, the imported users behave like local users. The users can/must be edited manually in Password Safe. The affiliations to organisational units and/or roles must be adapted manually.

Rights

The rights will be issued as follows during the import or synchronisation.

New objects

	User	Groups	Roles
Are rights inherited from the OU?	If no preset has been saved	If no preset has been saved	No
Are rights applied from a preset?	If a preset has been saved	If a preset has been saved	No
Is the “Add” right issued?	No	Yes	No
Who receives the rights key?	Imported users and all with the “Authorize” right	All	Imported roles and all with the “Authorize” right

Changed objects

	User	Groups	Roles
Are rights inherited from the OU?	No	No	No
Are rights applied from a preset?	No	No	No
Is the “Add” right issued?	No	No	No
Who receives the rights key?	Nobody	None	None

✻ In end-to-end mode, **no role affiliations** are issued during the import or synchronisation.

Login to Password Safe

Users that are imported in this mode **cannot** log in with the domain password. Instead, the user name is stored as a password when importing. This can be changed by administrators or users at the first login.

Master Key mode

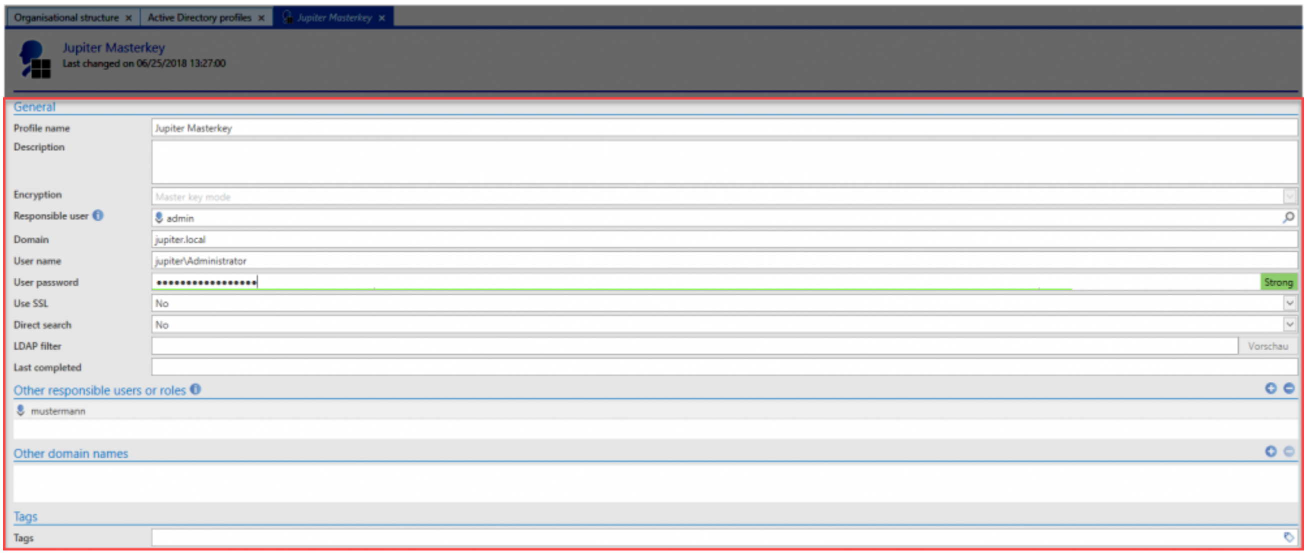
Maximum convenience

In contrast to end-to-end mode, which places the main focus on security, Master Key mode provides the maximum level of convenience. It not only imports users, organisational units and roles but also their links and affiliations. It can be synchronized to update the information and affiliations. **In this scenario, Active Directory is used as a leading system**.

Creating profiles

! The right **Can add new Active Directory profiles** and the ability to view the **organisational units module** or the **roles module** are required

Profile management is started via the icon of the same name on the ribbon.



Jupiter Masterkey
Last changed on 06/25/2018 13:27:00

General

Profile name	Jupiter Masterkey
Description	
Encryption	Master key mode
Responsible user	admin
Domain	jupiter.local
User name	jupiter\Administrator
User password	••••••••••••••••• Strong
Use SSL	No
Direct search	No
LDAP filter	
Last completed	

Other responsible users or roles

mustermann

Other domain names

Tags

Tags	

The following information must be provided in the profile:

- **Profile name**
- An optional **description**
- Master Key mode is selected for the **encryption**

In the case of already created profiles, the encryption can no longer be changed

- The **domain** field is used to define which domain is to be read. The value entered here will also be used for authentication if no alternative spellings have been saved under **Other domain names**.
- A local **user** (for example, the administrator) or an already imported user must be specified. The data will be imported under that user's name.

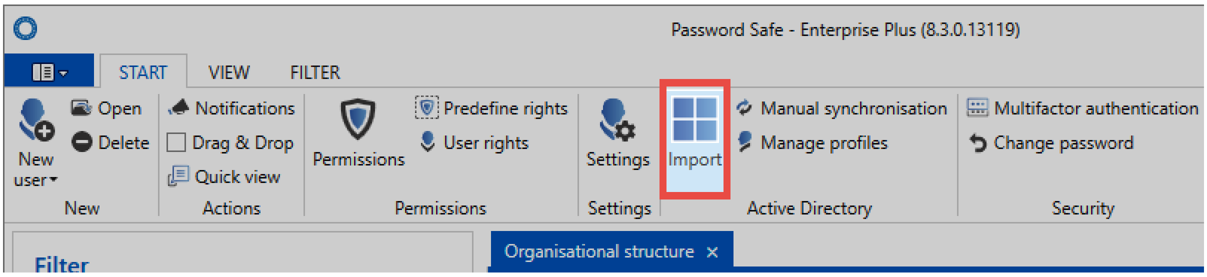
A *user is required to access the AD. The user should be formatted as follows: Domain\User. It must have access to the AD.

- Corresponding **user password** (domain password) for the user
- The connection can be established using **SSL** if required by the AD
- **Direct search** is recommended for very large domain trees. The tree structure is omitted, elements can then only be found and selected via the search.
- The **filter** can be used to directly specify an AD path as an entry point via an LDAP query.
- **Other responsible users or roles** can be used to define who is permitted to carry out the synchronisation with the AD.
- The option **Other domain names** can be used to save alternative spellings of the login domain. These must correspond to the spelling entered in the login window. For example, if a connection is being established to the domain **jupiter.local** or an IP address, the login can only be carried out with **jupiter\user** if **jupiter** has been saved here.

! The master key is added in the form of a certificate. It is **essential to back up** the generated certificate! If the database is being moved to another server, the certificate also needs to be transferred! Further information can be found in the section Certificates.

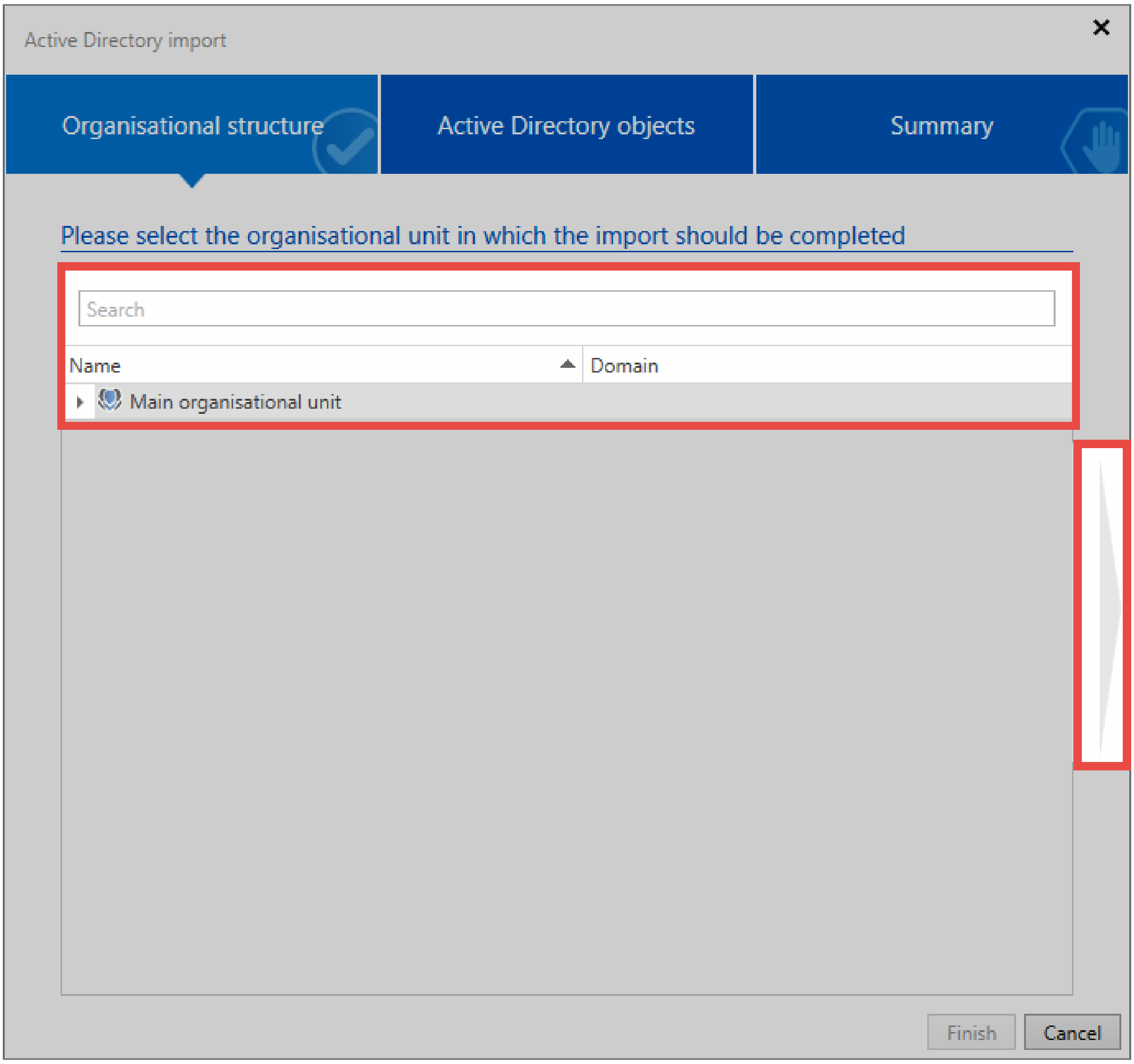
Import

You can start the import directly in the ribbon. A wizard guides the user through the entire operation.



Organisational structure

First, an organisational unit is selected for the import. If there are no organisational units in the database yet, as in this example, the data is imported into the **main organisational unit**.

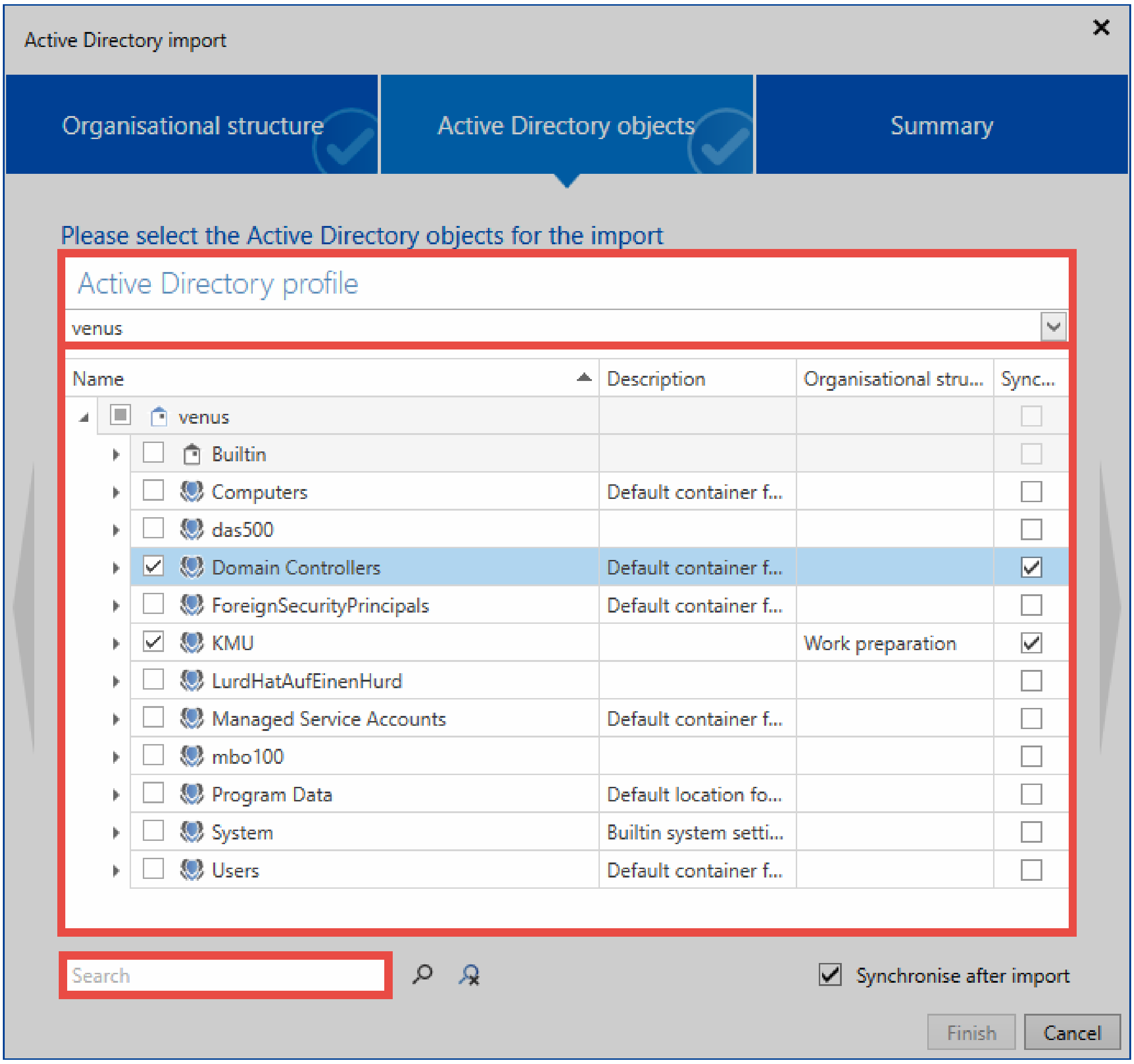


Please select the organisational unit in which the import should be completed

Main organisational unit

Active Directory objects

In the next step, select the profile you will use to import the data. Then, select organisational units and/or users for the import. A search is available for this purpose.



Active Directory import

Please select the Active Directory objects for the import

Active Directory profile

venus

Name	Description	Organisational stru...	Sync...
▣ venus			□
□ Builtin			□
□ Computers	Default container f...		□
□ das500			□
☑ Domain Controllers	Default container f...		☑
□ ForeignSecurityPrincipals	Default container f...		□
☑ KMU		Work preparation	☑
□ LurdHatAufEinenHurd			□
□ Managed Service Accounts	Default container f...		□
□ mbo100			□
□ Program Data	Default location fo...		□
□ System	Builtin system setti...		□
□ Users	Default container f...		□

Search

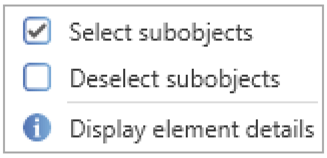
☑ Synchronise after import

As you can see, the organisational units **Jupiter** and **Contoso** contain items to be imported. The organisational units themselves will not be imported. The group **1099 Contractor** is imported including all sub-elements. The check next to the group **Accounting** indicates that the group itself will be imported along with some of its sub-elements. The hooks in the last column ensure that the elements are observed in future synchronization sequences.

There are different symbols which indicate the elements to be imported.

☑ The element itself and all possible sub-elements will be imported
■ The element itself and some of its sub-elements will be imported
▣ The element will not be imported; however, it contains elements that will be imported

Right-clicking in the list will launch a context menu. It provides helpful functions for the selection of the individual elements.



There are different symbols which indicate the elements to be imported.

☑ The element itself and all possible sub-elements will be imported
■ The element itself and some of its sub-elements will be imported
▨ The element will not be imported; however, it contains elements that will be imported

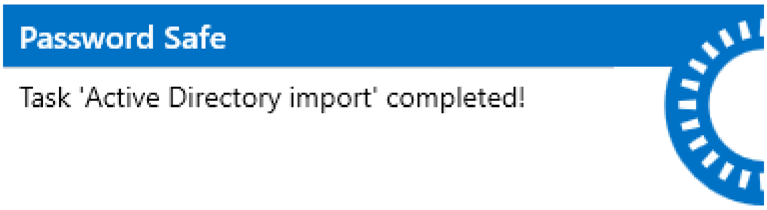
> If individual users cannot be selected for import, they have already been imported via an end-to-end encrypted profile.

Summary

The last page summarises which objects will be edited and in what form. It specifies the names of the elements along with their descriptions. The **Status** column specifies whether the object is added, updated, or disabled. The last column specifies the organisational unit into which the element is imported. The number of objects can be seen at the bottom.

Importing

The server imports data in the background. The individual elements then appear in the list one by one. This may take some time, depending on the amount of import data. If the import was terminated, this is symbolized by a hint.



Password Safe

Task 'Active Directory import' completed!

Imported users and organisational units

The users and organisational units imported in Master Key mode cannot be edited in Password Safe. Therefore, any changes must be made in AD and synchronized. **AD thus becomes the leading system**. Affiliations to organisational units or roles are also synchronized and must be set in the AD. In organisational units or roles created in Password Safe, the users can be included directly in Password Safe.

Rights

The rights will be issued as follows during the import or synchronisation.

New objects

	User	Groups	Roles
Are rights inherited from the OU?	If no preset has been saved	If no preset has been saved	No
Are rights applied from a preset?	If a preset has been saved	If a preset has been saved	No
Is the “Add” right issued?	No	Yes	No
Who receives the rights key?	Imported users and all with the “Authorize” right	All	All with the “Authorize” right

Changed objects

	User	Groups	Roles
Are rights inherited from the OU?	If no preset has been saved	No	No
Are rights applied from a preset?	If a preset has been saved	No	No
Is the “Add” right issued?	No	No	No
Who receives the rights key?	All with the “Authorize” right	None	All with the “Authorize” right

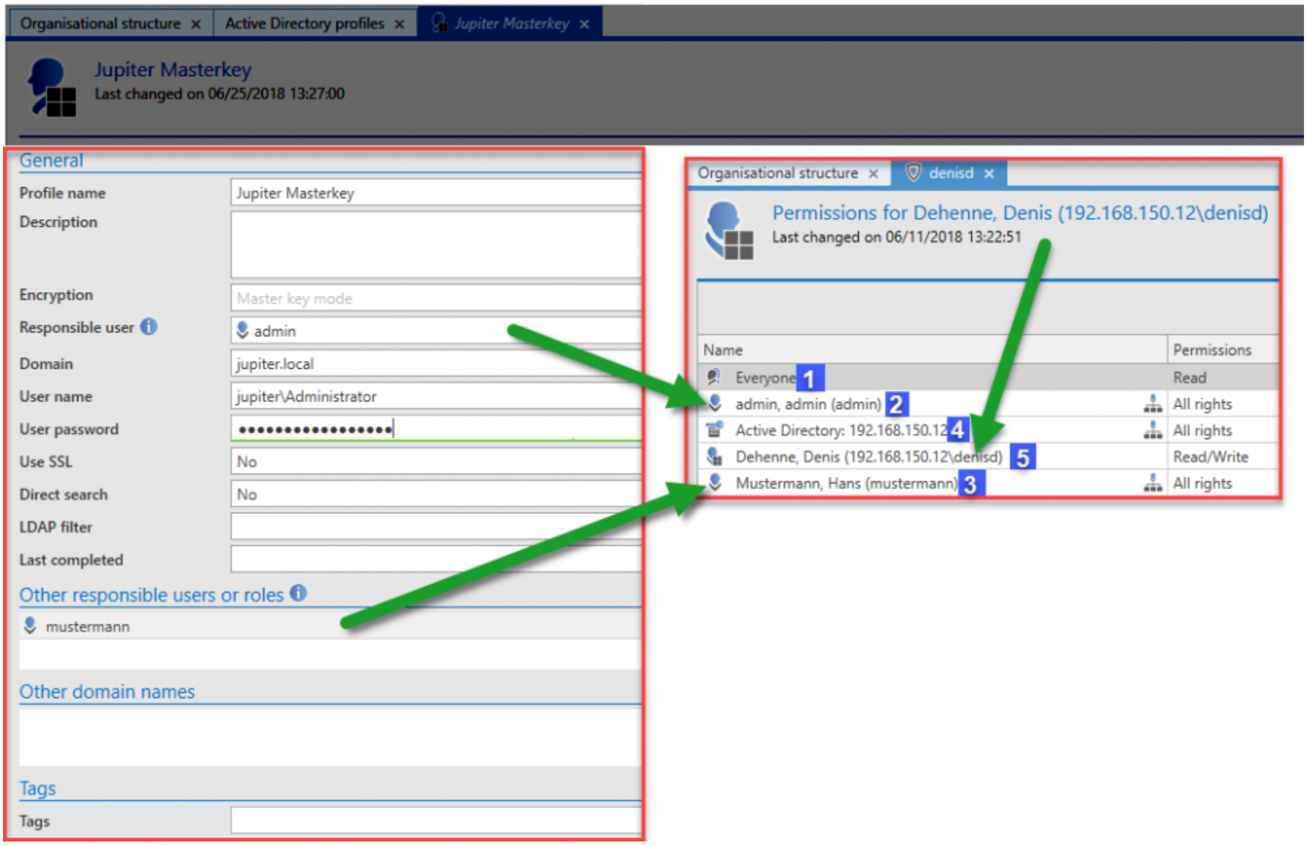
✻ If a user is imported, he will be given those roles that he also had in AD insofar as these roles already exist in Password Safe or have also been imported.

Login to Password Safe

Users who are imported using this mode can log in with the domain password. Please note that no domain needs to be specified when logging in. Of course, the login can also be supplemented with multifactor authentication.

Permissions to imported objects

The rights to be issued to imported users are explained using the following example:



Organisational structure ×
Active Directory profiles ×
Jupiter Masterkey ×

Jupiter Masterkey

Last changed on 06/25/2018 13:27:00

General

Profile name	Jupiter Masterkey
Description	
Encryption	Master key mode
Responsible user	admin
Domain	jupiter.local
User name	jupiter\Administrator
User password	•••••••••••••••••
Use SSL	No
Direct search	No
LDAP filter	
Last completed	

Other responsible users or roles

mustermann

Other domain names

Tags

Tags	

Organisational structure ×
denisd ×

Permissions for Dehenne, Denis (192.168.150.12\denisd)

Last changed on 06/11/2018 13:22:51

Name	Permissions
Everyone 1	Read
admin, admin (admin) 2	All rights
Active Directory: 192.168.150.12 4	All rights
Dehenne, Denis (192.168.150.12\denisd) 5	Read/Write
Mustermann, Hans (mustermann) 3	All rights

1. In Master Key mode, **all** users will be issued with the **read** right.
2. The **responsible user** will be issued with all rights and the key. This ensures that he can also synchronise or change the user in the future
3. **Other responsible users** are issued with the same rights as the **responsible user**
4. The **Master Key** for the **Active Directory** profile will also be issued with all rights and the key because it will be used for the synchronisation
5. Finally, users will be issued with the rights for themselves

> All users and roles issued with **rights** to the imported object also receive its rights key.

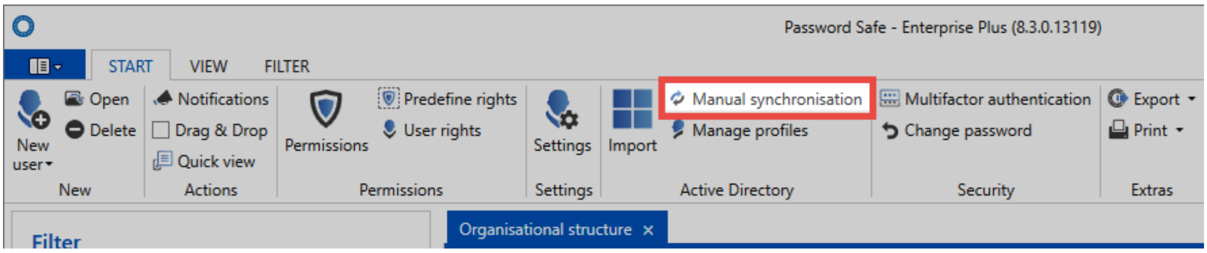
Synchronization

During synchronization, all relevant information for users, organisational units and roles (names, email, etc.) is updated. Changed affiliations for organisational units and roles are adjusted. Likewise, users are activated or deactivated according to the settings in the AD. New users and correspondingly defined roles are imported.

> If the hook was not set in the **Synchronization** column when a user is imported, no changes are made.

Manual synchronization

The synchronization can be started manually at any time via the corresponding button in the ribbon.



Select the required profile and start the synchronization. As is the case with the initial import, the synchronization runs in the background. A hint indicates that the process has been completed.

Synchronization via system tasks

The synchronization can also be carried out automatically. This is made possible as part of the system tasks.

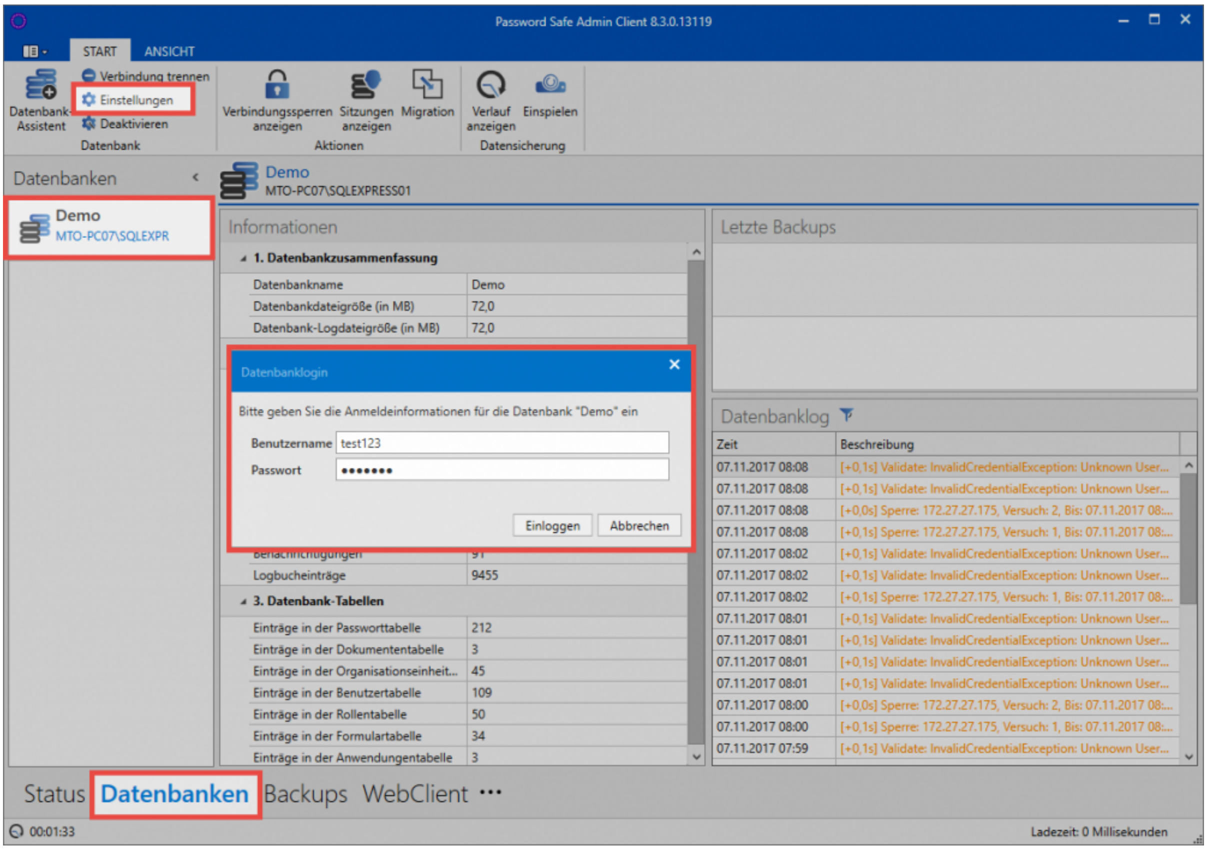
Multifactor authentication

What is multifactor authentication?

By means of multifactor authentication, you can save the login – in addition to the password – with a further factor. Setting up a multifactor authentication can be done by either the administrator or the user.

Requirements

To use multifactor authentication on a database, it must firstly have been activated on the AdminClient. In the database module, open the settings for the selected database via the ribbon.



1. Datenbankzusammenfassung

Datenbankname	Demo
Datenbankdateigröße (in MB)	72,0
Datenbank-Logdateigröße (in MB)	72,0
Benachrichtigungen	91
Logbucheinträge	9455

3. Datenbank-Tabellen

Einträge in der Passworttabelle	212
Einträge in der Dokumententabelle	3
Einträge in der Organisationseinheit...	45
Einträge in der Benutzertabelle	109
Einträge in der Rollentabelle	50
Einträge in der Formulartabelle	34
Einträge in der Anwendungentabelle	3

Datenbanklogin

Bitte geben Sie die Anmeldeinformationen für die Datenbank "Demo" ein

Benutzername: test123

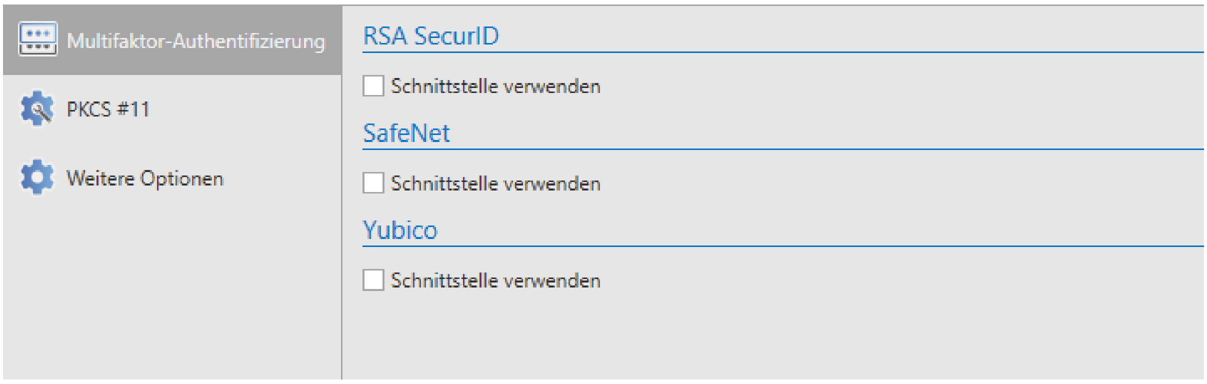
Passwort: •••••••

Einloggen | Abbrechen

Datenbanklog

Zeit	Beschreibung
07.11.2017 08:08	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:08	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:08	[+0,0s] Sperre: 172.27.27.175, Versuch: 2, Bis: 07.11.2017 08:...
07.11.2017 08:08	[+0,1s] Sperre: 172.27.27.175, Versuch: 1, Bis: 07.11.2017 08:...
07.11.2017 08:02	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:02	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:02	[+0,1s] Sperre: 172.27.27.175, Versuch: 1, Bis: 07.11.2017 08:...
07.11.2017 08:01	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:01	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:01	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:01	[+0,1s] Validate: InvalidCredentialException: Unknown User...
07.11.2017 08:00	[+0,0s] Sperre: 172.27.27.175, Versuch: 2, Bis: 07.11.2017 08:...
07.11.2017 08:00	[+0,1s] Sperre: 172.27.27.175, Versuch: 1, Bis: 07.11.2017 08:...
07.11.2017 07:59	[+0,1s] Validate: InvalidCredentialException: Unknown User...

It is possible to separately define in the settings whether it is permitted to use each interface on the database.



RSA SecurID

□ Schnittstelle verwenden

SafeNet

□ Schnittstelle verwenden

Yubico

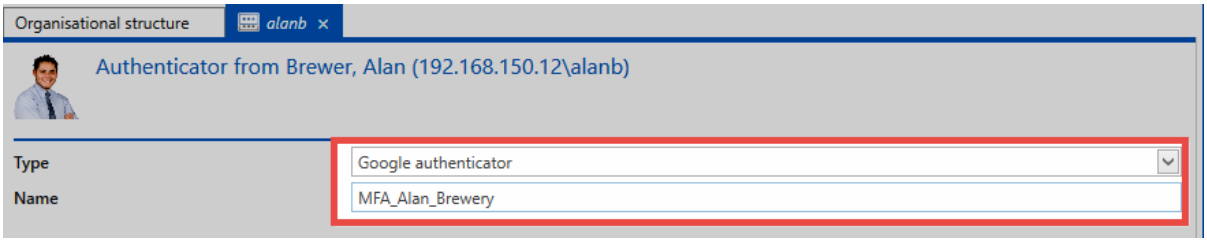
□ Schnittstelle verwenden

Other settings

In the user settings, it is also possible to define the “Length of validity of a multifactor authentication token” in minutes.

Configuration of multifactor authentication

In the organisational structure module, you select the user and the interface “Multifactor authentication” in the ribbon.



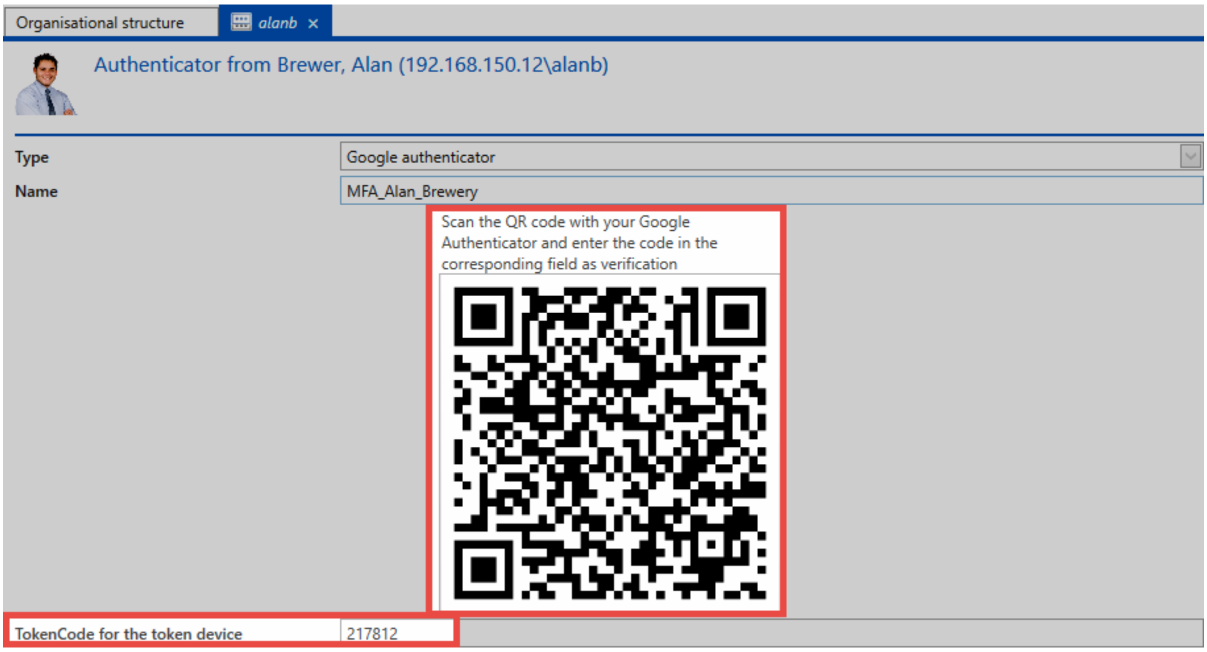
Authenticator from Brewer, Alan (192.168.150.12\alanb)

Type	Google authenticator
Name	MFA_Alan_Brewery

The desired type of authentication is selected and given a title. This name is also displayed to the user when logging in. The subsequent process differs depending on the desired authentication type.

Google authenticator

The prerequisite for this is that the relevant app has been started on a smartphone. After the name has been assigned for the authentication, you generate a new secret via the corresponding button. A QR code is displayed, which must be scanned using the Google Authenticator app on a smartphone.



Authenticator from Brewer, Alan (192.168.150.12\alanb)

Type	Google authenticator
Name	MFA_Alan_Brewery

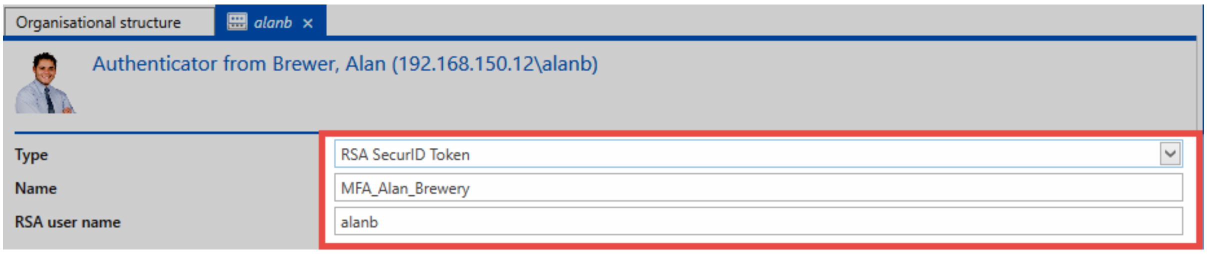
Scan the QR code with your Google Authenticator and enter the code in the corresponding field as verification

TokenCode for the token device	217812

Once the Google Authenticator app has detected the QR code, it will return a 6-digit PIN. You must then enter it in the appropriate field. Finally, click on **Create** in the ribbon.

RSA SecurID Token

To set up multifactor authentication using RSA SecurID, simply enter the RSA user name and click **Create** directly in the ribbon.



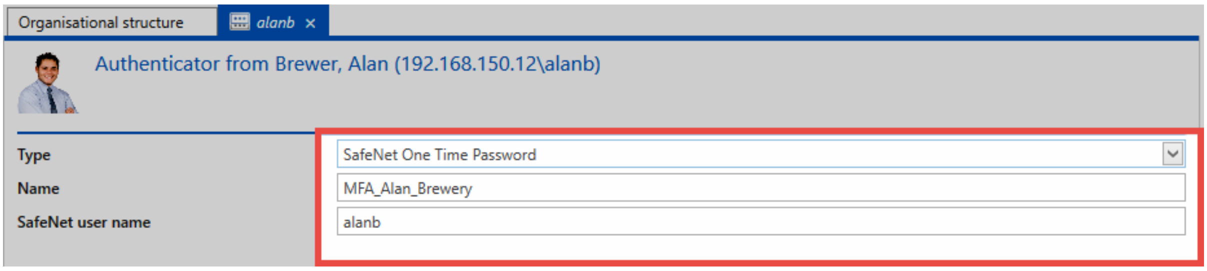
Authenticator from Brewer, Alan (192.168.150.12\alanb)

Type	RSA SecurID Token
Name	MFA_Alan_Brewery
RSA user name	alanb

The prerequisite for the use of RSA SecurID token is that the access data has been stored in the Database settings on the AdminClient.

SafeNet One-Time-Password

Multifactor authentication using SafeNet One-Time Password is set up using the SafeNet user name.



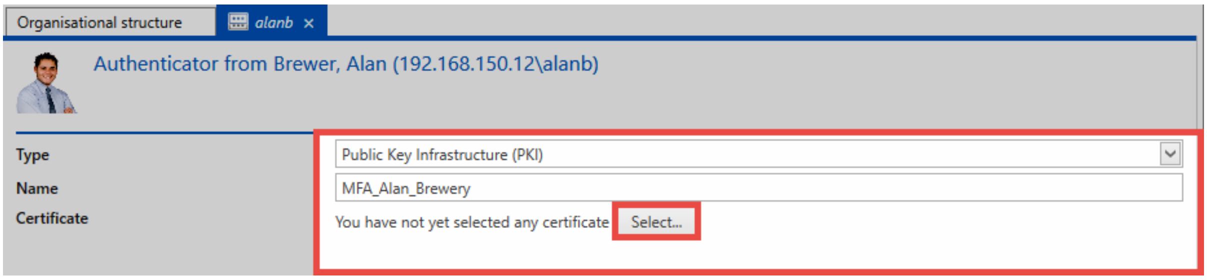
Authenticator from Brewer, Alan (192.168.150.12\alanb)

Type	SafeNet One Time Password
Name	MFA_Alan_Brewery
SafeNet user name	alanb

✻ The prerequisite for the use of SafeNet One-Time Password Token is that the access data has been stored on the AdminClient in Database settings.

Public key infrastructure

For PKI setup, the **Select** button is used to open the menu for selecting the desired certificate. All eligible certificates are displayed.



Authenticator from Brewer, Alan (192.168.150.12\alanb)

Type	Public Key Infrastructure (PKI)
Name	MFA_Alan_Brewery
Certificate	You have not yet selected any certificate

Now just select the desired certificate from the list to confirm the process.

Yubico One Time Password

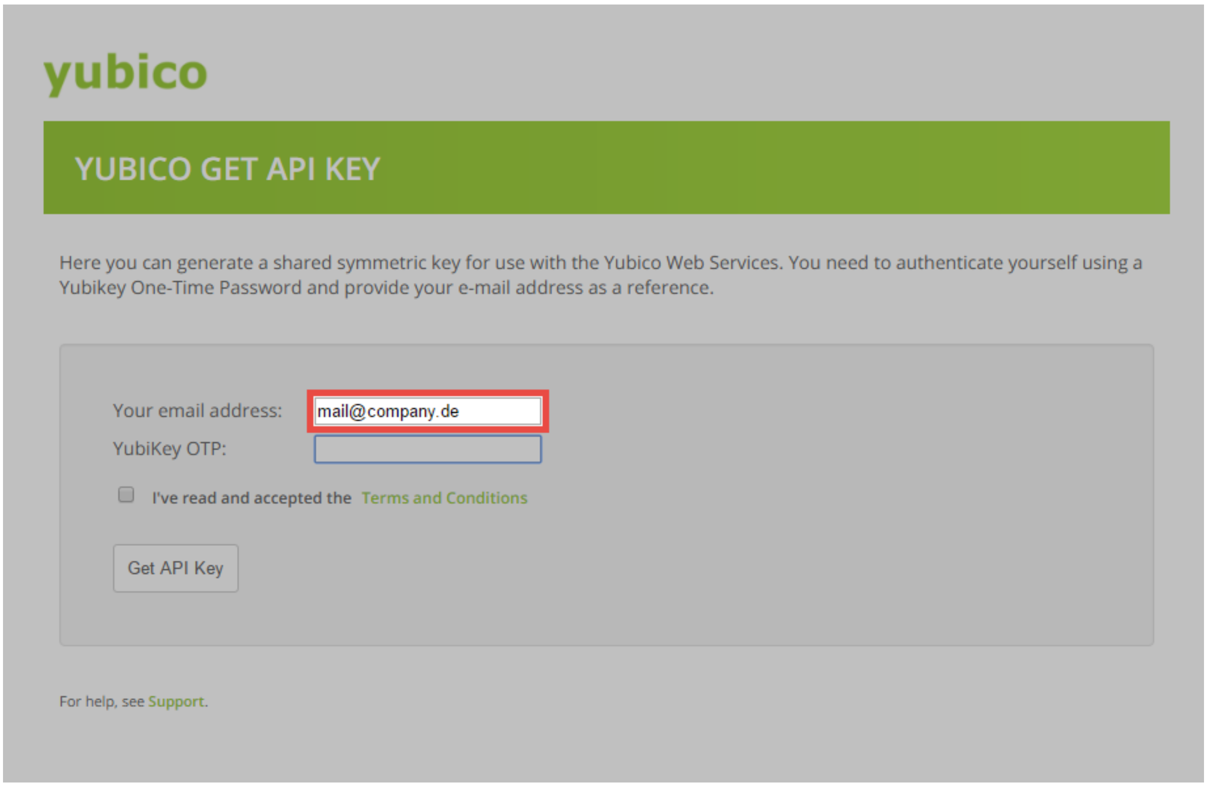
The configuration of multifactor authentication using Yubico One Time Password is described in a separate section.

Yubico / Yubikey

Setting up multifactor authentication

Requesting the Yubico API key

An API key must be requested for configuration. For this purpose, use the following link and enter an e-mail address: https://upgrade.yubico.com/getapikey/



YUBICO GET API KEY

Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

Your email address: mail@company.de

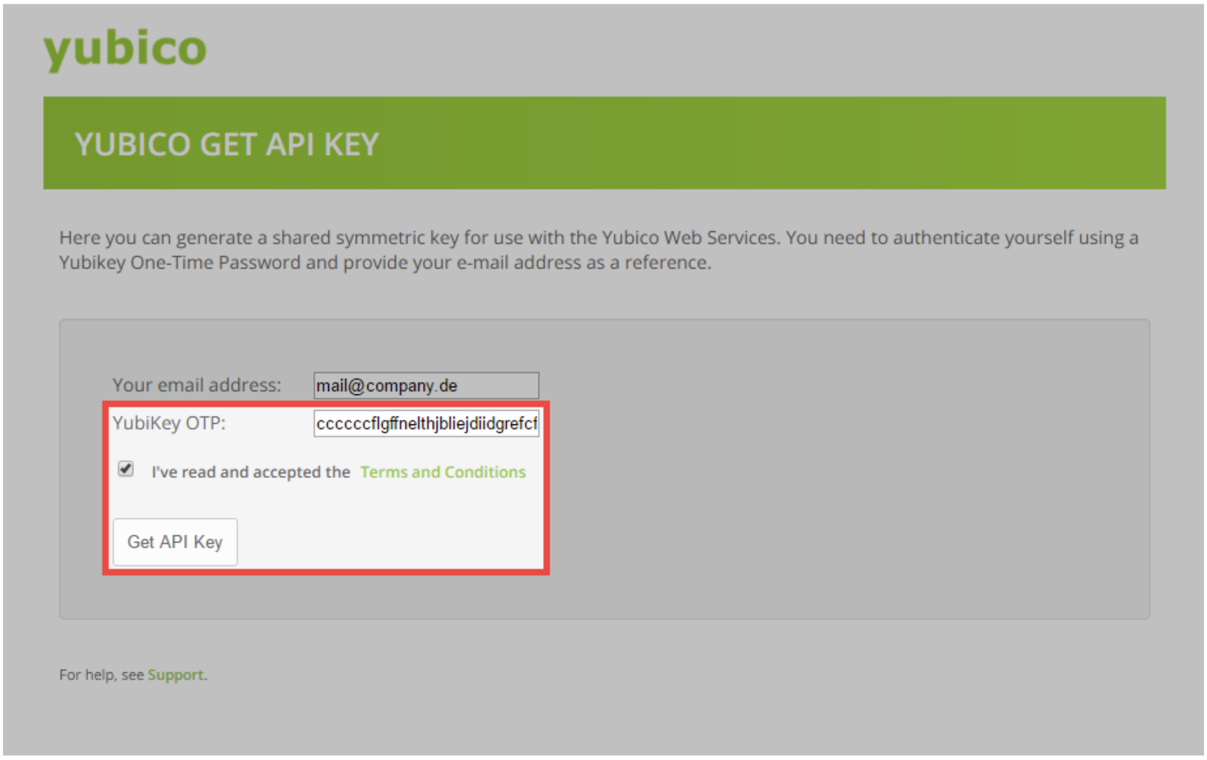
YubiKey OTP:

□ I've read and accepted the Terms and Conditions

For help, see Support.

Yubikey will then generate a **One Time Password**. The Yubikey used must only be touched in the right place.

The **One Time Password** is entered directly into the corresponding field.



YUBICO GET API KEY

Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

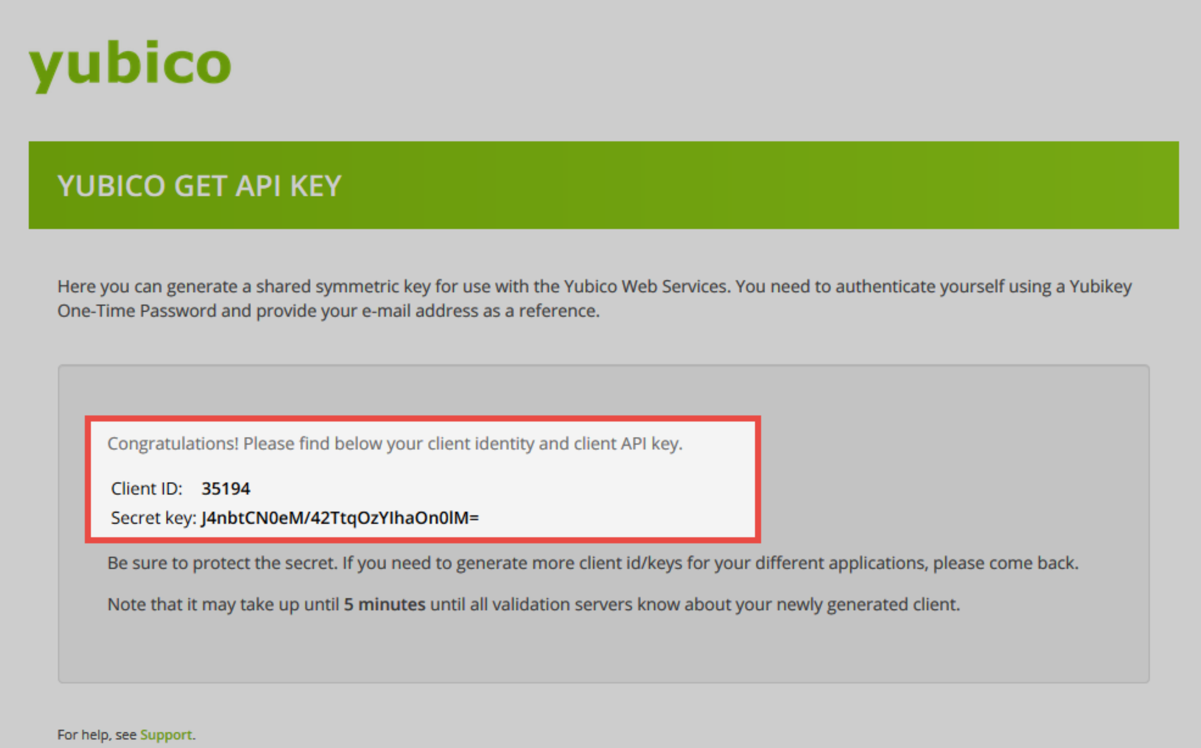
Your email address: mail@company.de

YubiKey OTP: ccccccflgffnelthjbliejdiidgrefcf

☑ I've read and accepted the Terms and Conditions

For help, see Support.

Once the general terms and conditions have been approved, the API Key can be requested.



YUBICO GET API KEY

Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

Congratulations! Please find below your client identity and client API key.

Client ID: **35194**
Secret key: **J4nbtCN0eM/42TtqOzYIhaOn0lM=**

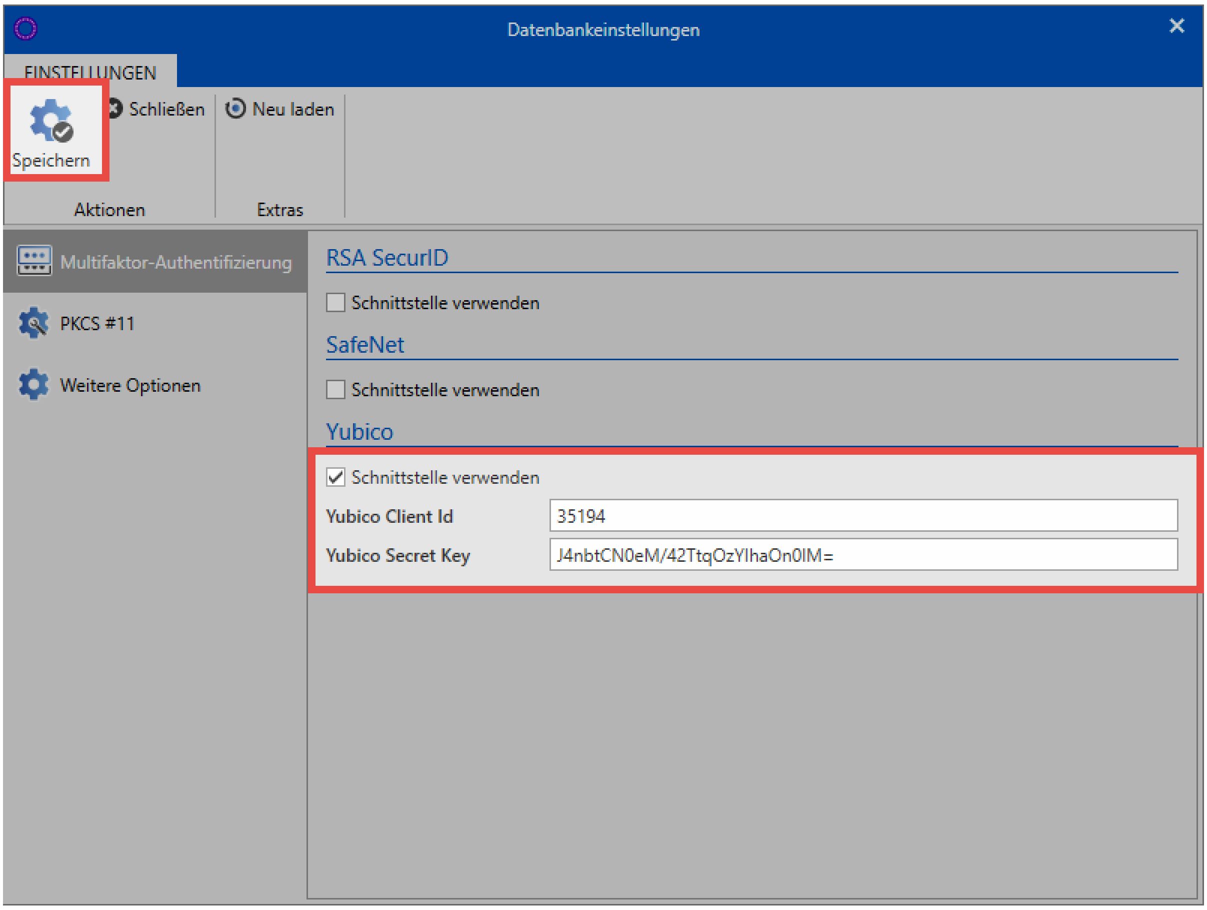
Be sure to protect the secret. If you need to generate more client id/keys for your different applications, please come back.

Note that it may take up until **5 minutes** until all validation servers know about your newly generated client.

For help, see Support.

Configuring the Yubikey API

The actual setting up of the multifactor authentication is carried out on the AdminClient in the * Database * module. First select the required data base; then open the “Features” in the ribbon.
The * Yubico Client ID * and the * Yubico Secret Key * must then be entered and saved.



Datenbankeinstellungen

EINSTELLUNGEN

RSA SecurID

□ Schnittstelle verwenden

SafeNet

□ Schnittstelle verwenden

Yubico

☑ Schnittstelle verwenden

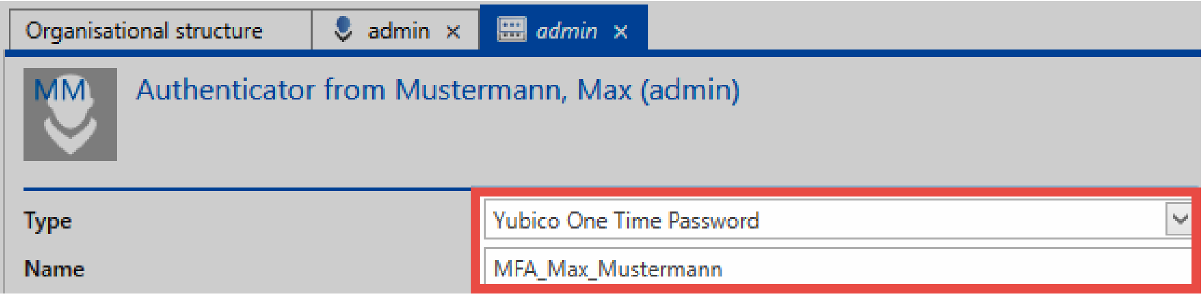
Yubico Client Id: 35194

Yubico Secret Key: J4nbtCN0eM/42TtqOzYlhaOn0IM=

The interface is now ready and can be used.

Configuring multifactor authentication for users

Multifactor authentication can be configured in the Password Safe client. It can be done by the user themselves in **Backstage** in the Account menu. It is also possible for the configuration to be applied to other users in the module organisational units. The procedure is identical in both cases. In order to configure the Yubikey, simply select **Yubico One Time Password** and enter the name for the multifactor authentication.



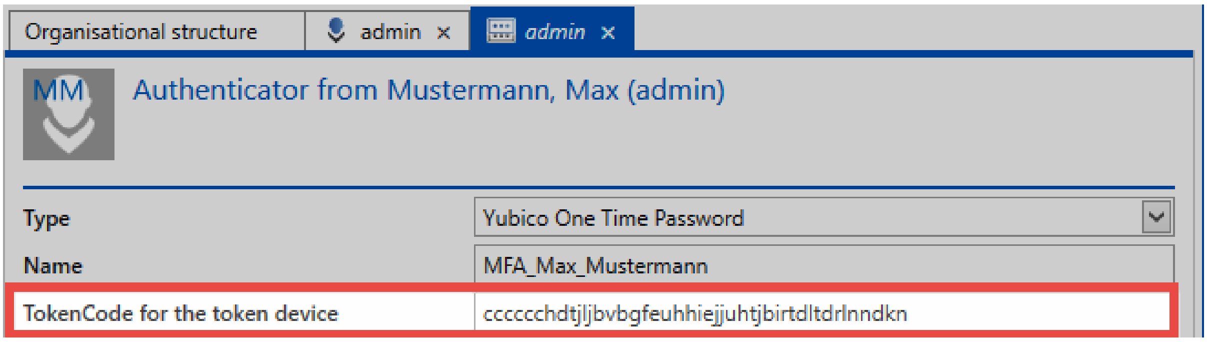
Authenticator from Mustermann, Max (admin)

Type: Yubico One Time Password

Name: MFA_Max_Mustermann

And then click on save. Now click in the field for the token and create a token using the Yubikey. For **Yubikey NEO**, you only need to touch the touch panel. The same applies to **Yubikey Nano**.

The token is entered directly into the corresponding field. The multifactor authentication is configured once you've clicked on save.

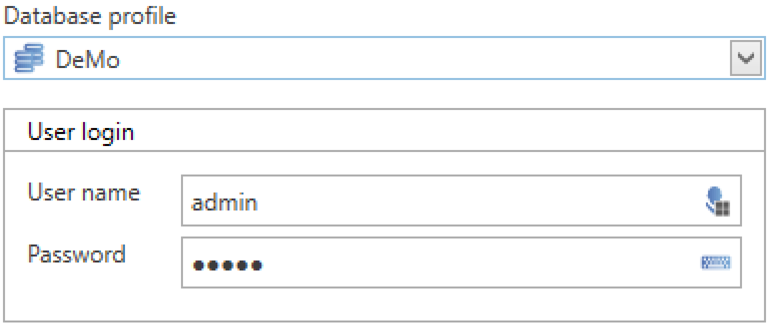


Authenticator from Mustermann, Max (admin)

Type	Yubico One Time Password
Name	MFA_Max_Mustermann
TokenCode for the token device	cccccchdtjljbvbgfeuhhiejjuhtjbirtdltdrlnndkn

Logging in with the Yubikey

To login with Multifactor Authentication, the database is first selected and then * User Name * and * Password * are entered and confirmed.

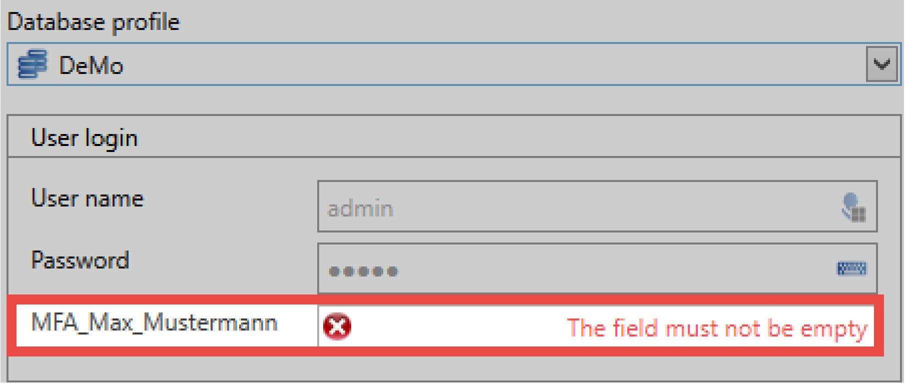


Database profile: DeMo

User login

User name	admin
Password	●●●●●

After the first password authentication, another field for the **One Time Password** is displayed.



Database profile

DeMo

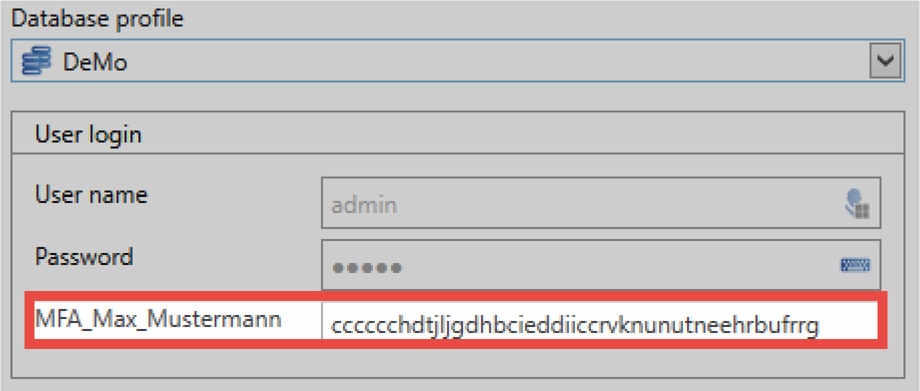
User login

User name admin

Password ●●●●●

MFA_Max_Mustermann The field must not be empty

Click on the field to highlight it, and enter the **One Time Password** by touching the Yubikeys.



Database profile

DeMo

User login

User name admin

Password ●●●●●

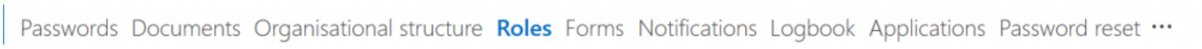
MFA_Max_Mustermann ccccchdtjljgdhbcieddiiccrvknunutneehrbufrrg

The user is now logged on.

Roles

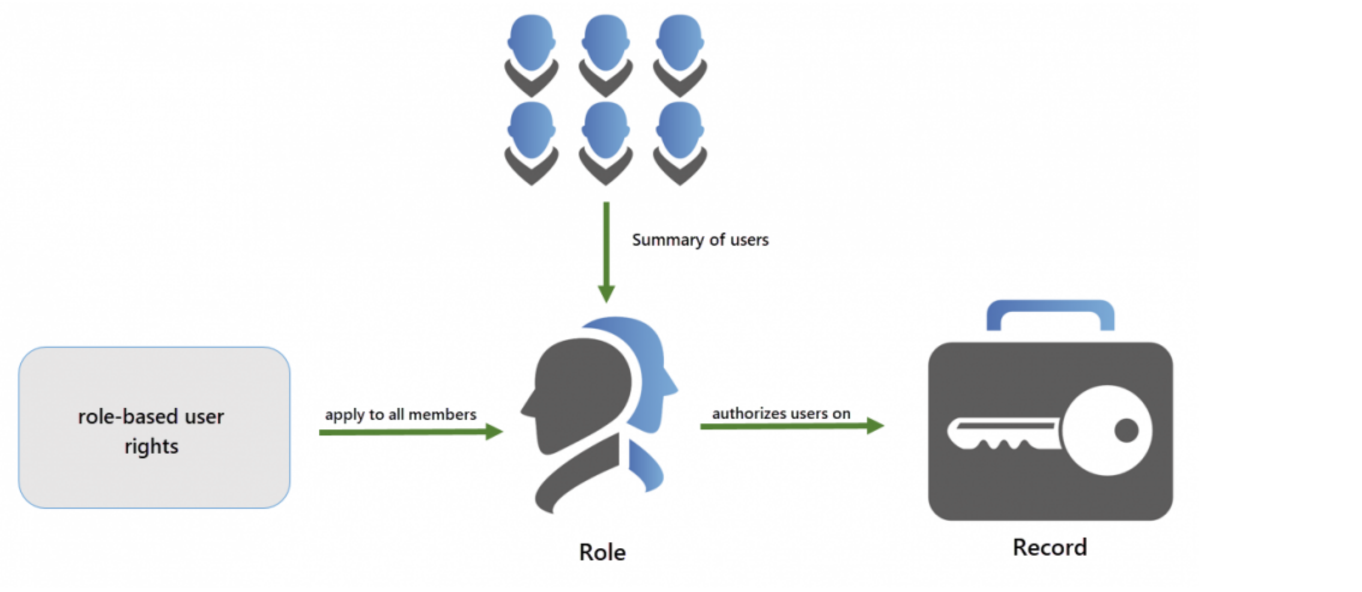
What are roles?

Each employee in a company is ultimately a member of a department and / or part of a particular function level. These departments or groups are mapped within Password Safe using the role concept. The authorizations can therefore be configured and inherited in a role-based manner. The “Roles” module should only be made available to administrators. Accordingly, it is recommended to limit the visibility of the role management. It is also possible to delegate the management of departments or separate areas completely to third parties via the role concept. The authorization concept ensures that users are only granted access to those roles to which they are entitled. The configuration of **visibility** is explained in a similar way to the other modules in one place.



Roles in focus

The configuration of roles is the basis for the authorization concept. Of course, the permissions for data could also be set at user level. However, the use of roles can dramatically reduce the administrative burden, and it helps to keep an overview. In addition to the authorizations for data, user rights are also mapped in the best case via roles.

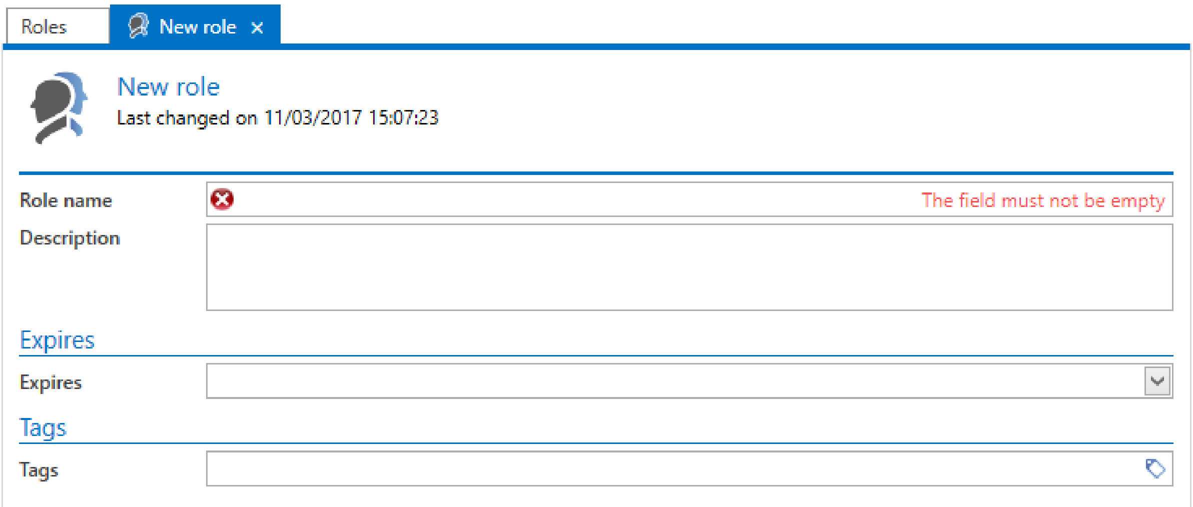


As you can see, roles are the central objects within Password Safe. They form the indispensable bridge between users and authorizations of any kind.

Creating and granting permissions for new roles

! The right **Can add new roles** and the ability to view the **roles module** are required

If you are in the “roles” module, the process for creating new roles is the same as for creating new records. Roles can be created via the ribbon and also via the context menu that is accessed using the right mouse button.



New role
Last changed on 11/03/2017 15:07:23

Role name: The field must not be empty
Description:

Expires
Expires:

Tags
Tags:

All information connected with the roles and the authorization concept is explained in a separate section.

Planning phase

Just like with the organisational structures, you should also familiarize yourself with the intended role concepts in advance. The mapping of the structures present in a company is the starting point for the success of Password Safe. You should design the roles in Password Safe only once a detailed design has been drawn up, and all the requirements of all project participants have been met.

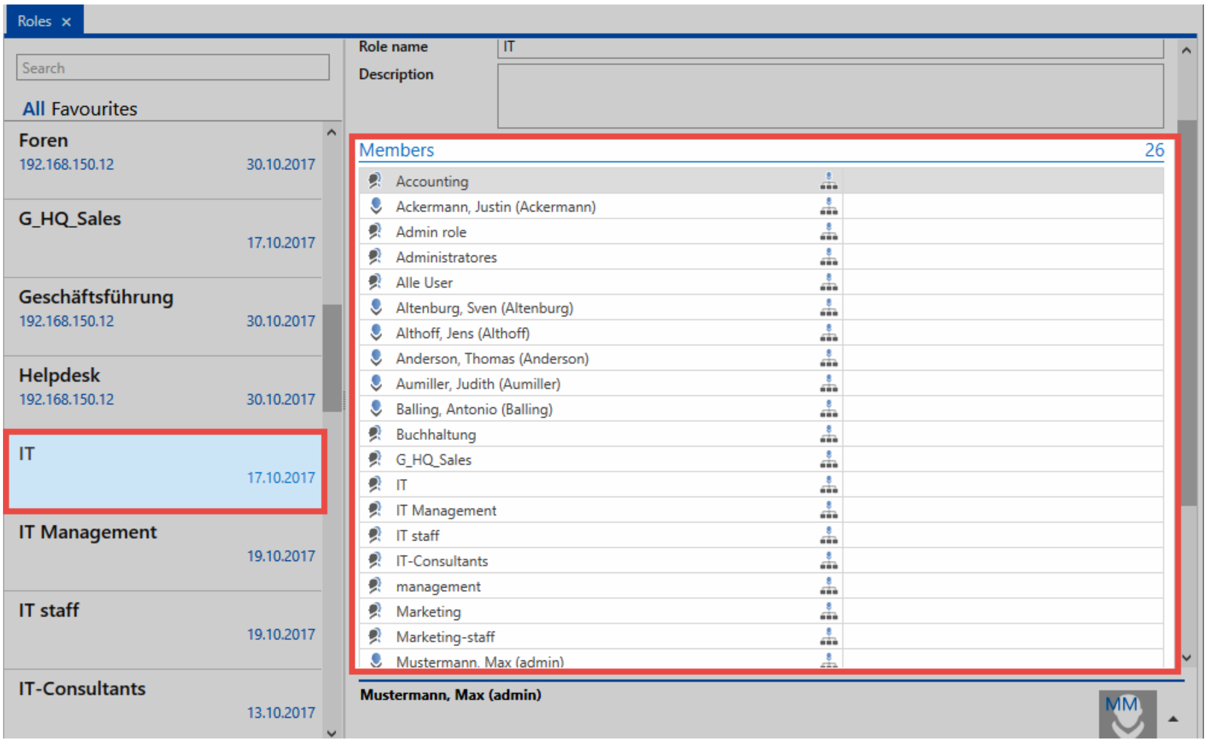
Why are there no groups?

Password Safe enforces the avoidance of unnecessary structures through the role concept. A group-in-group nesting is not supported – and is not necessary at all. The resultant increase in performance as well as increased overview promotes efficiency and effectiveness. The elegant interplay of organisational structures, roles, and granular filter options can cover all customer-specific scenarios.

✻ This architecture makes nesting of roles obsolete.

Overview of members for a role

As well as being able to view the members in the permissions dialogue, a list of all **members** for a role is already made available in the reading pane. All of the other users with permissions but without membership of the role are not taken into account.



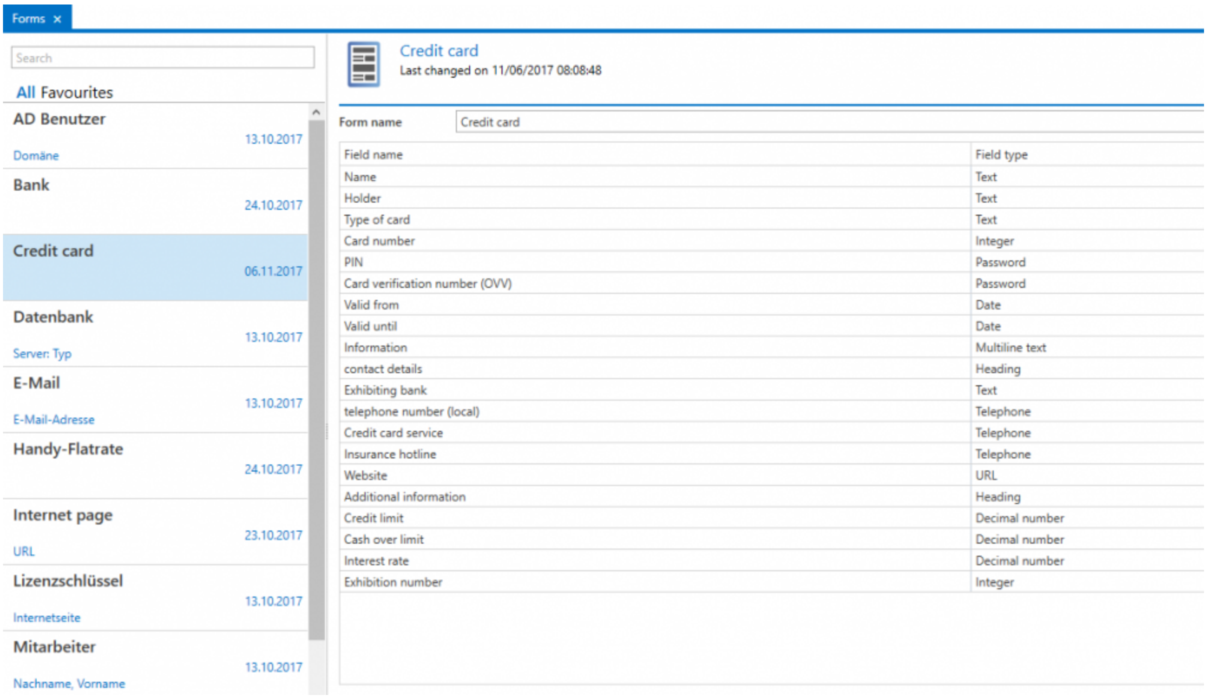
Forms

What are forms?

When creating a new data record, it is indispensable to always query all relevant data for the intended application. In this context, **Forms** represent templates for the information to be stored. The manageability of existing forms primarily ensures the completeness of the data to be stored. Nevertheless, their use as an effective filter criterion is not to be ignored! Forms have a lasting impact on working with Password Safe v8 and must be managed and maintained with the necessary care by the administration. The configuration of **visibility** is explained in a similar way to the other modules in one place.

Standard forms

Password Safe is supplied with a series of standard forms – these should generally cover all standard requirements. Naturally, it is still possible to adapt the standard forms to your individual requirements.



AD Benutzer 13.10.2017 Domäne
Bank 24.10.2017
Credit card 06.11.2017
Datenbank 13.10.2017 Server: Typ
E-Mail 13.10.2017 E-Mail-Adresse
Handy-Flatrate 24.10.2017
Internet page 23.10.2017 URL
Lizenzschlüssel 13.10.2017 Internetseite
Mitarbeiter 13.10.2017 Nachname, Vorname

Credit card
Last changed on 11/06/2017 08:08:48

Form name: Credit card

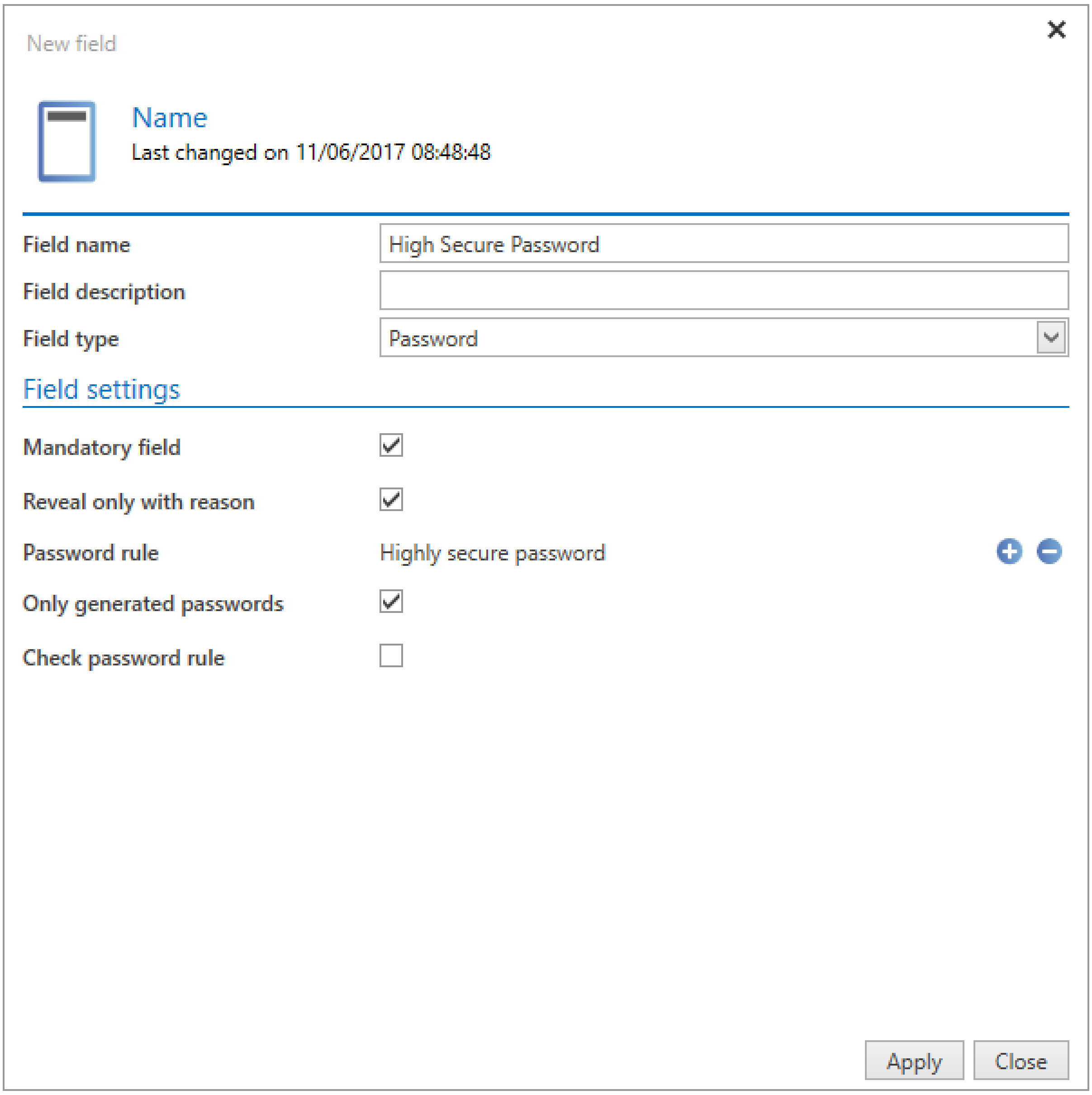
Field name	Field type
Name	Text
Holder	Text
Type of card	Text
Card number	Integer
PIN	Password
Card verification number (OVV)	Password
Valid from	Date
Valid until	Date
Information	Multiline text
contact details	Heading
Exhibiting bank	Text
telephone number (local)	Telephone
Credit card service	Telephone
Insurance hotline	Telephone
Website	URL
Additional information	Heading
Credit limit	Decimal number
Cash over limit	Decimal number
Interest rate	Decimal number
Exhibition number	Integer

The associated preview for the form selected in list view appears in the reading pane. Both the field name and also the field type are visible.

Creating new forms

! The right **Can add new forms** and the ability to view the **forms module** are required

The wizard for creating new forms can be started via the ribbon, the keyboard shortcut “Ctrl + N” or also the context menu that is accessed using the right mouse button. The same mechanisms can now be used to create new form fields within the wizard. Depending on the selected field type, other options are available in the **field settings** section. This will be clearly explained below using the example of the field type “Password”. The sequence in which form fields are requested when creating new records corresponds to the sequence within the form. This can be adapted using the relevant buttons in the ribbon.



Name
Last changed on 11/06/2017 08:48:48

Field name	High Secure Password
Field description	
Field type	Password

Field settings

Mandatory field	☑
Reveal only with reason	☑
Password rule	Highly secure password
Only generated passwords	☑
Check password rule	□

The following field settings thus appear for the field type “Password”: “Mandatory field, Reveal only with reason, Only generated passwords and Password rule”. These can now be defined as desired. (**Note:** It is possible to select password rules within the field settings, they are defined as part of the options in the main menu)

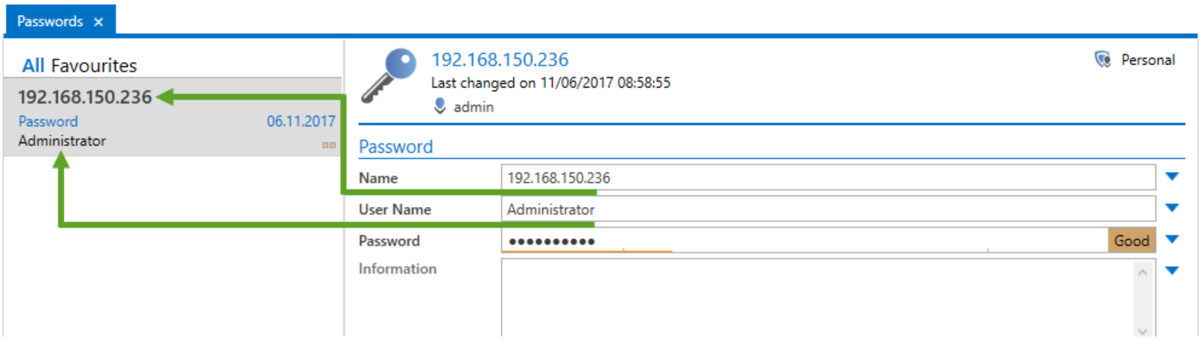
! If a form has been created, it can then be selected for use when creating new records. The prerequisite is that the logged-in user has at least read rights to the form.

Permissions for forms

In the same way as for other objects (records, roles, documents,…), permissions can also be granted for forms. On the one hand, this ensures that not everyone can edit existing forms, while on the other hand, this makes it possible to make forms available to selective groups. This ensures that clarity is maintained and that users are not confronted with information that is irrelevant to them. The form “Credit cards” may be relevant within the accounting department but administrators do not generally need to use it.

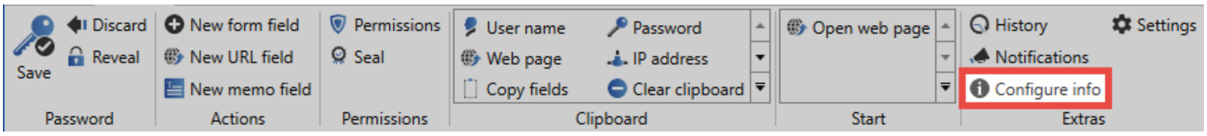
Configuring the info field

Every record displays other information underneath the obligatory name of the record in list view. In the following example, the user name is also displayed in addition to the name of the password. The name of the form is displayed in between in a blue font.

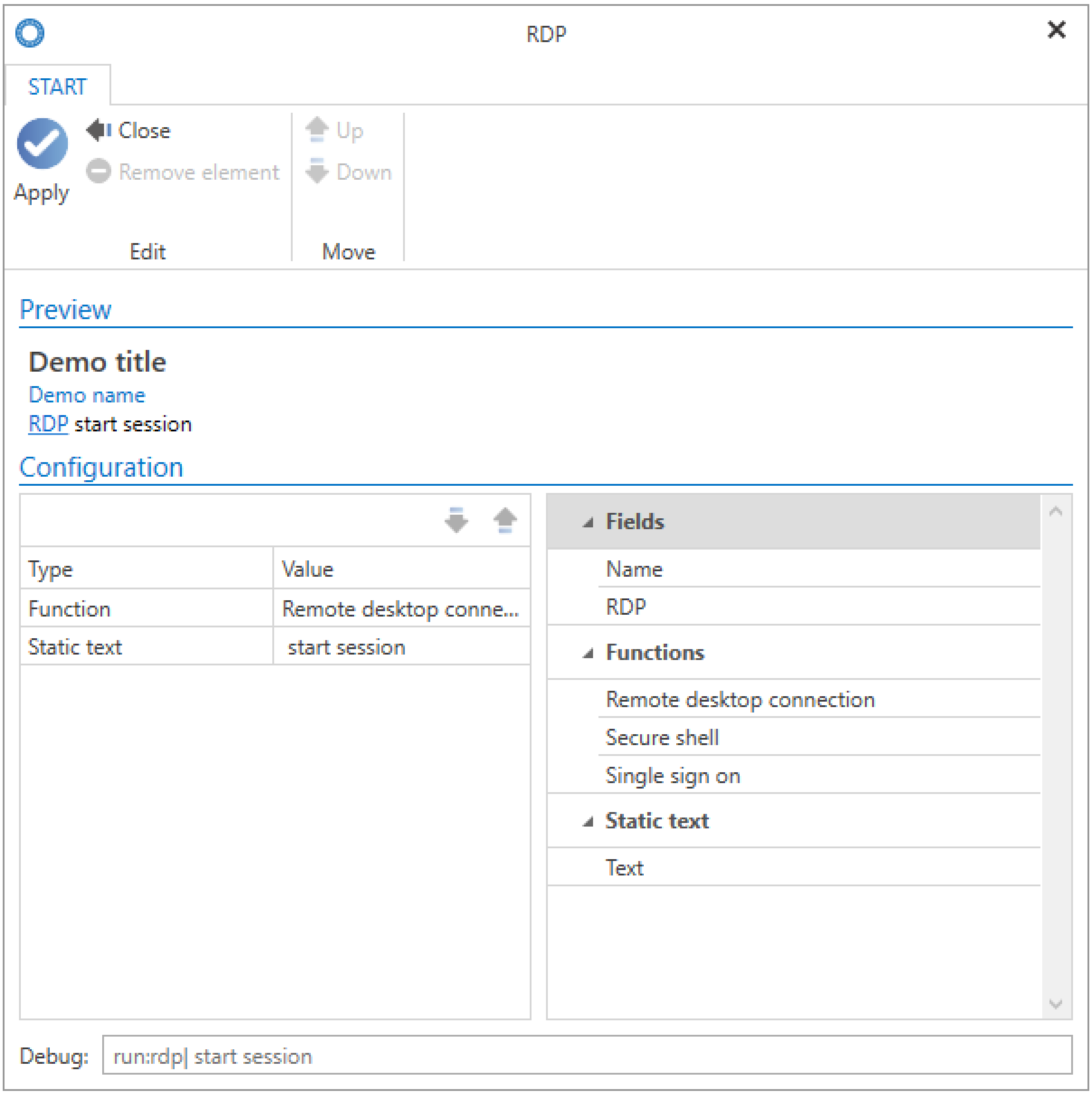


Name	192.168.150.236
User Name	Administrator
Password	●●●●●●●●●●

The name of the record (192.168.150.236) and the form (password) cannot be adjusted – these are always displayed. The user (Administrator) that is still saved for the record is currently displayed. This can be configured in the info field for the form. It is thus possible to separately define for each form what information for a record can be directly seen in list view. In the form module, the info field is configured by opening the form to be edited in editing mode by double clicking on it and then pressing the *Configure info field” button in the ribbon.



This will open a separate tab that enables you to design the info section via drag & drop. The fields that are available on the right can be “dragged” onto the configuration window on the left. In the following example, “Start RDP session” will be made visible in the info section, whereby only the word “RDP” is assigned a function – namely to start the RDP manager. A preview is shown in the top section.

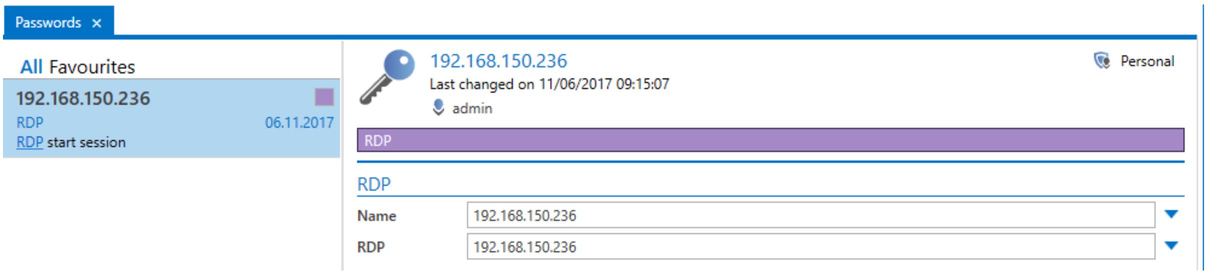


Demo title
Demo name
RDP start session

Type	Value
Function	Remote desktop conne...
Static text	start session

Debug: run:rdp| start session

The info field for the form is now updated. It is now possible to start the RDP session directly in the RDP session.



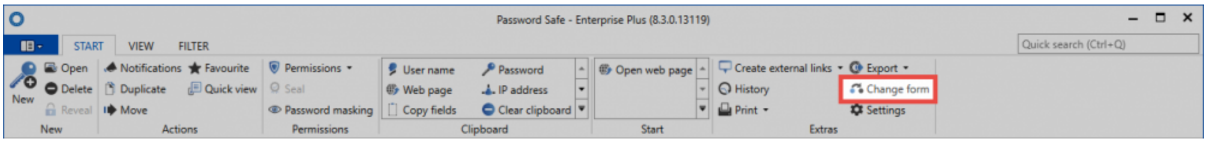
Name 192.168.150.236

RDP 192.168.150.236

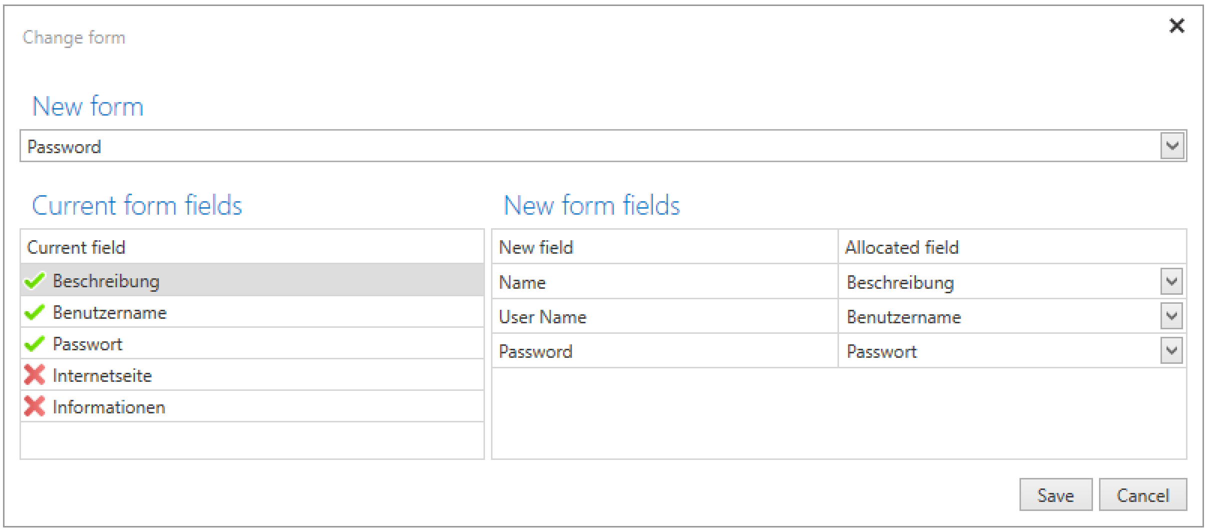
Change form

Changing forms

It is necessary in some cases to change the form for a record. In these cases, this is mostly to consolidate existing data or to adapt the form to match changes in the data structure. These functionalities are available under “Extras/Settings” in the ribbon.



In the following screenshot, you can see the dialogue for “mapping” the form fields from the previously used form to the new form. In this example, a record that previously belonged to the “Website” form is being “mapped” to the “Password” form (right).



Change form

New form

Password

Current form fields

Current field
✓ Beschreibung
✓ Benutzername
✓ Passwort
✗ Internetseite
✗ Informationen

New form fields

New field	Allocated field
Name	Beschreibung
User Name	Benutzername
Password	Passwort

The drop-down menu allows you to select the target form. The comparison of current and new form fields is shown in the lower section.

- Fields **marked in green** have already been assigned to the new form
- Fields **marked in red** indicate fields that have not been assigned

! Please note that information could be lost during this process! In the example, this applies to the fields “Website” and “Information”.

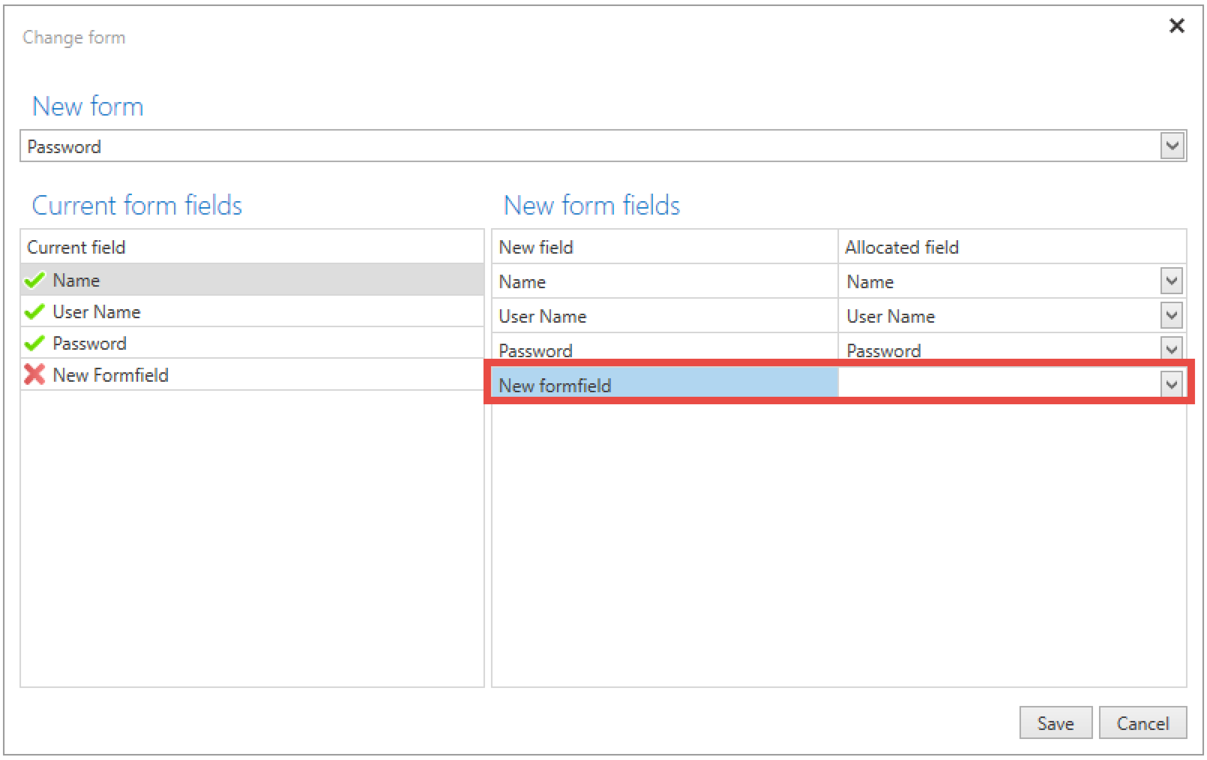
! The user right *Can change form for a password” is required

The effects of changes to forms on existing records

In general, changes to forms do not effect existing records. This means that a record that was created with a certain form will not itself be changed after this form has been adapted/changed. It remains in its original state. However, there are methods by which changes to forms could be adopted by existing records. There are two possibilities in this context:

Change form

If you press the “Change form” button (as mentioned in the previous section), the already existing form will be used by default. If this form has been changed in the meantime, the new form field will be directly shown and adopted after it is saved.



Change form

New form

Password

Current form fields

Current field
✓ Name
✓ User Name
✓ Password
✗ New Formfield

New form fields

New field	Allocated field
Name	Name
User Name	User Name
Password	Password
New formfield	

Apply form changes to passwords

The setting “Apply form changes to passwords” makes it possible to force the change to the form to be adopted. This becomes effective when editing the record! It is immaterial here whether changes are being made to the record. Simply re-editing and saving the record will cause the adjustment to the form.

The following permissions/configuration must exist:

- The user that wants to make the change requires the read right to the form
- The read right to the record is required (as well as to the associated form field)
- Sealed and masked records remain unaffected

Conclusion

A common feature of both variants is that adjustments to forms cannot be automatically triggered. Already existing records are thus not automatically adjusted. The adjustment thus needs to be carried out manually. In the first case, the manual step is to use the function “Change form”. In the second case, it is sufficient to simply edit and save the record.

Logbook

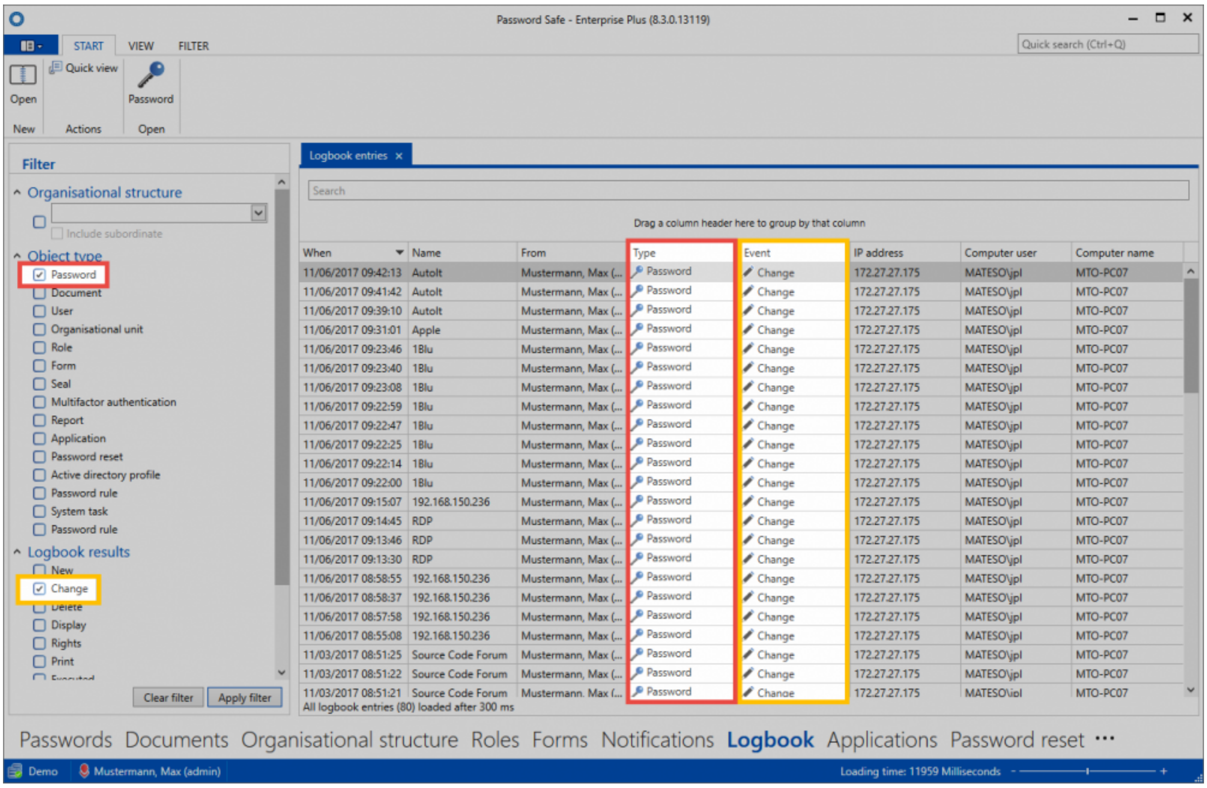
What is the logbook?

Password Safe logs all user interactions. These entries can be viewed and filtered via the module of the same name. In this way, it is possible in a central location to find out at any time which user has made exactly what changes. This module is (theoretically) classified as uncritical since the employee only has access to those logbook entries to which he is actually entitled. [The configuration of **visibility** is explained in a similar way to the other modules in one place.]

Passwords Documents Organisational structure Roles Forms Notifications Logbook Applications Password reset ···

Use of the filter in the logbook

As is the case in all other modules, you can also use the filter in the logbook to limit the number of displayed elements based on the defined criteria. In the following example, the user is searching for logbook entries relating to the object type “Password” that also match the event criteria “Change”. In short: The entries are being filtered based on changes to passwords.


Password Safe - Enterprise Plus (8.3.0.13119)
START
VIEW
FILTER
Quick search (Ctrl+Q)
Open
Quick view
Password
New
Actions
Open
Logbook entries ×
Search
Drag a column header here to group by that column
Clear filter
Apply filter
Passwords Documents Organisational structure Roles Forms Notifications Logbook Applications Password reset ···
Demo
Mustermann, Max (admin)
Loading time: 11959 Milliseconds

Filter

Organisational structure

□ Include subordinate

Object type

☑ Password
□ Document
□ User
□ Organisational unit
□ Role
□ Form
□ Seal
□ Multifactor authentication
□ Report
□ Application
□ Password reset
□ Active directory profile
□ Password rule
□ System task
□ Password rule

Logbook results

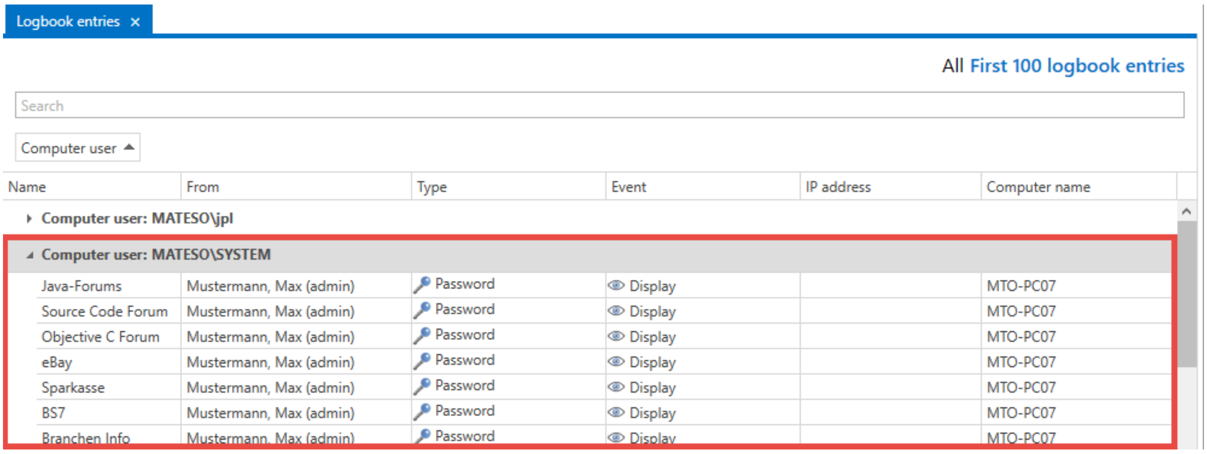
□ New
☑ Change
□ Delete
□ Display
□ Rights
□ Print
□ Executed

When	Name	From	Type	Event	IP address	Computer user	Computer name
11/06/2017 09:42:13	AutoIt	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:41:42	AutoIt	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:39:10	AutoIt	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:31:01	Apple	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:23:46	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:23:40	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:23:08	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:22:59	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:22:47	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:22:25	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:22:14	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:22:00	1Blu	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:15:07	192.168.150.236	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:14:45	RDP	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:13:46	RDP	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 09:13:30	RDP	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 08:58:55	192.168.150.236	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 08:58:37	192.168.150.236	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 08:57:58	192.168.150.236	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/06/2017 08:55:08	192.168.150.236	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/03/2017 08:51:25	Source Code Forum	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/03/2017 08:51:22	Source Code Forum	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07
11/03/2017 08:51:21	Source Code Forum	Mustermann, Max (...	Password	Change	172.27.27.175	MATESO\jpl	MTO-PC07

All logbook entries (80) loaded after 300 ms

Grouping in the logbook

The resulting list can also be grouped together by dragging and dropping column headers. The following shows the entries being grouped together based on the column “Computer user”. The filtered results correspond to all changes to passwords carried out by the computer user “administrator”.



Name	From	Type	Event	IP address	Computer name
▸ Computer user: MATESO\jpl					
◢ Computer user: MATESO\SYSTEM					
Java-Forums	Mustermann, Max (admin)	Password	Display		MTO-PC07
Source Code Forum	Mustermann, Max (admin)	Password	Display		MTO-PC07
Objective C Forum	Mustermann, Max (admin)	Password	Display		MTO-PC07
eBay	Mustermann, Max (admin)	Password	Display		MTO-PC07
Sparkasse	Mustermann, Max (admin)	Password	Display		MTO-PC07
BS7	Mustermann, Max (admin)	Password	Display		MTO-PC07
Branchen Info	Mustermann, Max (admin)	Password	Display		MTO-PC07

Revision-safe archiving

In Password Safe, an uncompromising method is used when handling the logbook. Every change of state is recorded and saved in the MSSQL database. There are no plans to allow triggers for logbook entries to be selectively defined. Revision-safe archiving and thus the audit-proof traceability of changes can only be guaranteed using this approach.

Transferring to a Syslog server

If desired, the logbook can also be completely transferred to a Syslog server. Further information can be found in the section **Syslog**.

Applications

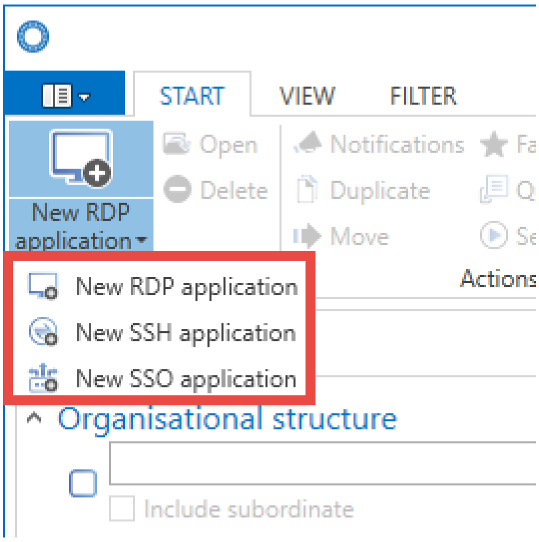
What are applications?

Applications can be used to configure automated logins to various systems. Especially when combined with various protective mechanisms, the company thus benefits in terms of security because complex passwords are automated and entered in the login masks in concealed form for the user. Various types are available, such as Remote Desktop (RDP), Secure Shell (SSH), general applications (SSO) and the web. The Single Sign On Engine offers countless configuration options to enable automatic logon to almost any kind of software. The configuration of **visibility** is explained in a similar way to the other modules in one place.

Automatic logins to websites are covered by the SSO agent.

The three types of applications

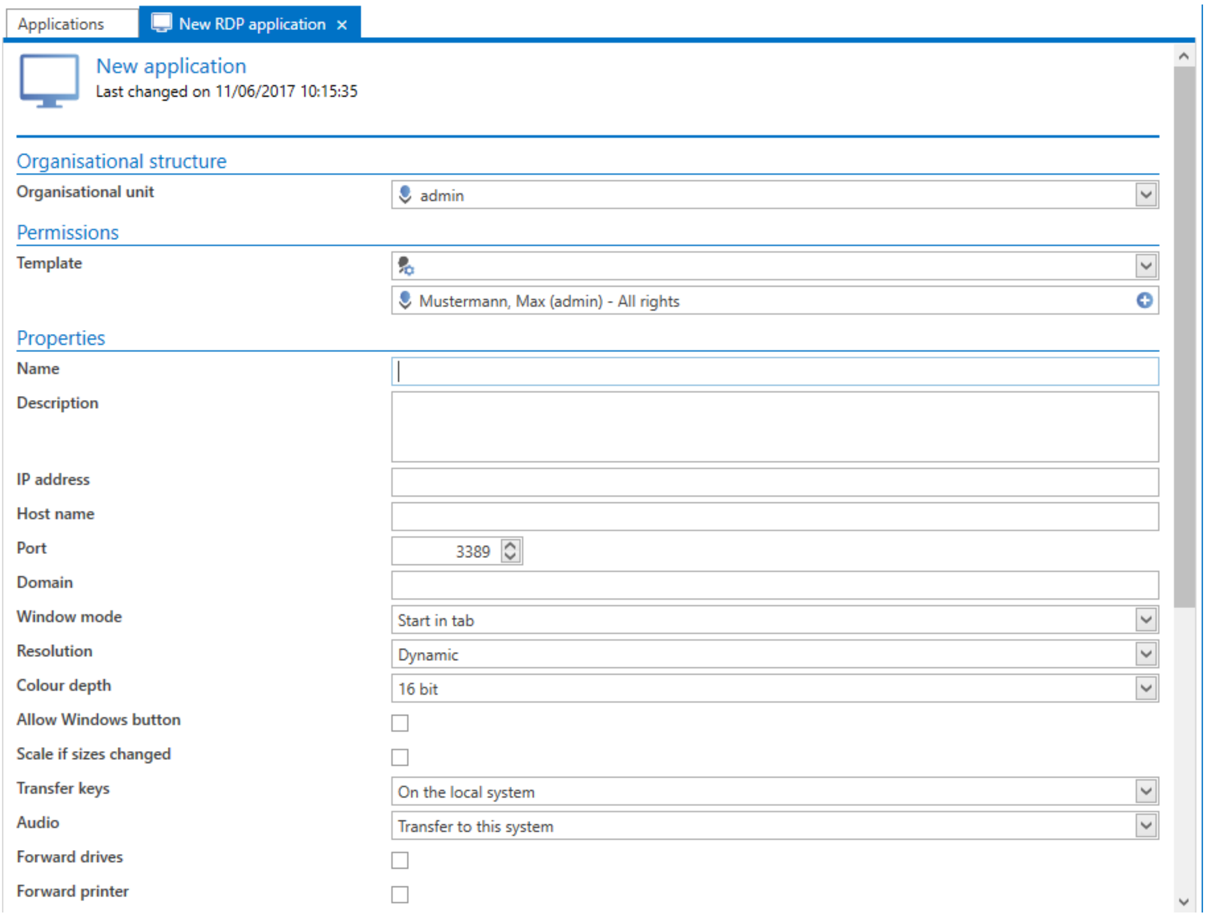
Password Safe differentiates between three different types of applications.



In terms of how they are handled, **RDP and SSH** applications can be covered together. Both types of application can be (optionally) “embedded” in Password Safe. The relevant session then opens in its own tab in the reading pane. All other forms of automatic logins are summarised in the **SSO applications** category. Precisely how these logins are created and used is covered in the next section. They include all forms of Windows login masks and also applications for websites. In contrast to RDP and SSH applications, they cannot be started embedded in Password Safe but are instead opened as usual in their own window. These SSO applications need to be defined once in advance. In Password Safe, this is also described as learning the applications. In contrast, RDP and SSH can be both completely defined and also started within Password Safe.

RDP and SSH

A new RDP/SSH application can be created via the ribbon or also the context menu that is accessed using the right mouse button. A corresponding form opens in each case where the variables for a connection can be defined.



New application
Last changed on 11/06/2017 10:15:35

Organisational structure

Organisational unit	admin

Permissions

Template	
	Mustermann, Max (admin) - All rights

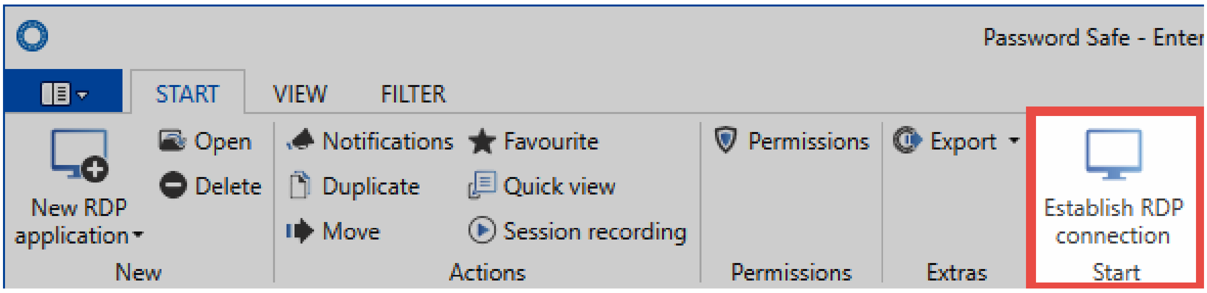
Properties

Name	
Description	
IP address	
Host name	
Port	3389
Domain	
Window mode	Start in tab
Resolution	Dynamic
Colour depth	16 bit
Allow Windows button	□
Scale if sizes changed	□
Transfer keys	On the local system
Audio	Transfer to this system
Forward drives	□
Forward printer	□

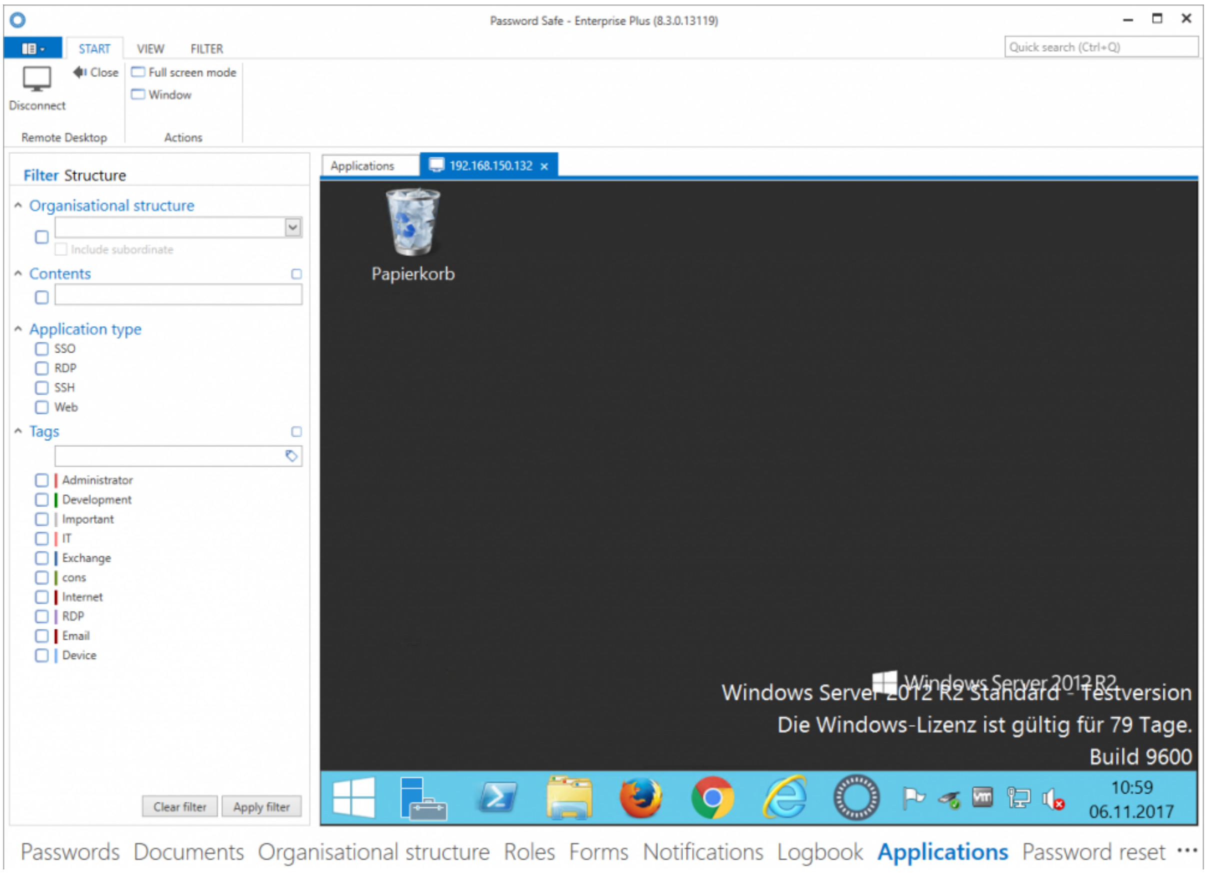
These variables also correspond precisely to those (using the example of RDP here) that can be configured when creating an RDP connection via “mstsc”. Whether the connections should be started in a tab, full screen mode or in a window can be defined in the field **“Window mode”**.

Working with RDP and SSH applications

If you have created e.g. an RDP connection, this can now also be directly started via the ribbon. The connection to the desired session can be established via the icon **Establish RDP connection**.

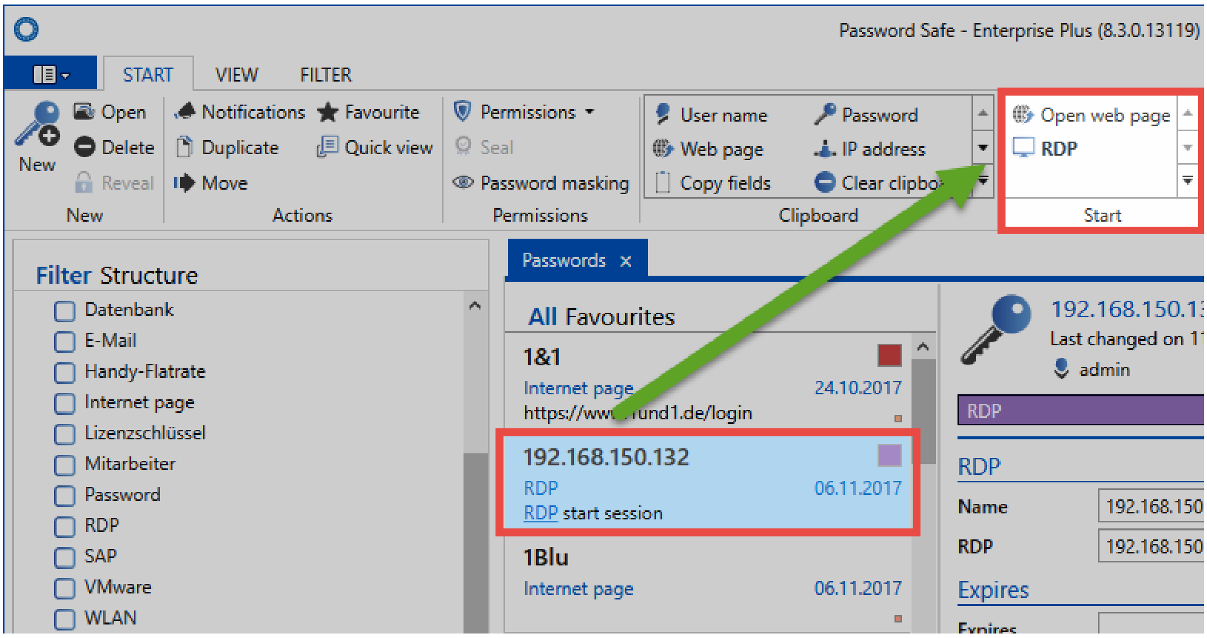


Password Safe now attempts to log in to the target system with the information available. Data that are not saved in the form will be directly requested when opening the session. It is thus also possible to only enter the IP address and/or the password after starting the Password Safe application. If all data has been retrieved, the RDP session will open in a tab – if so defined (Window mode field in the application):

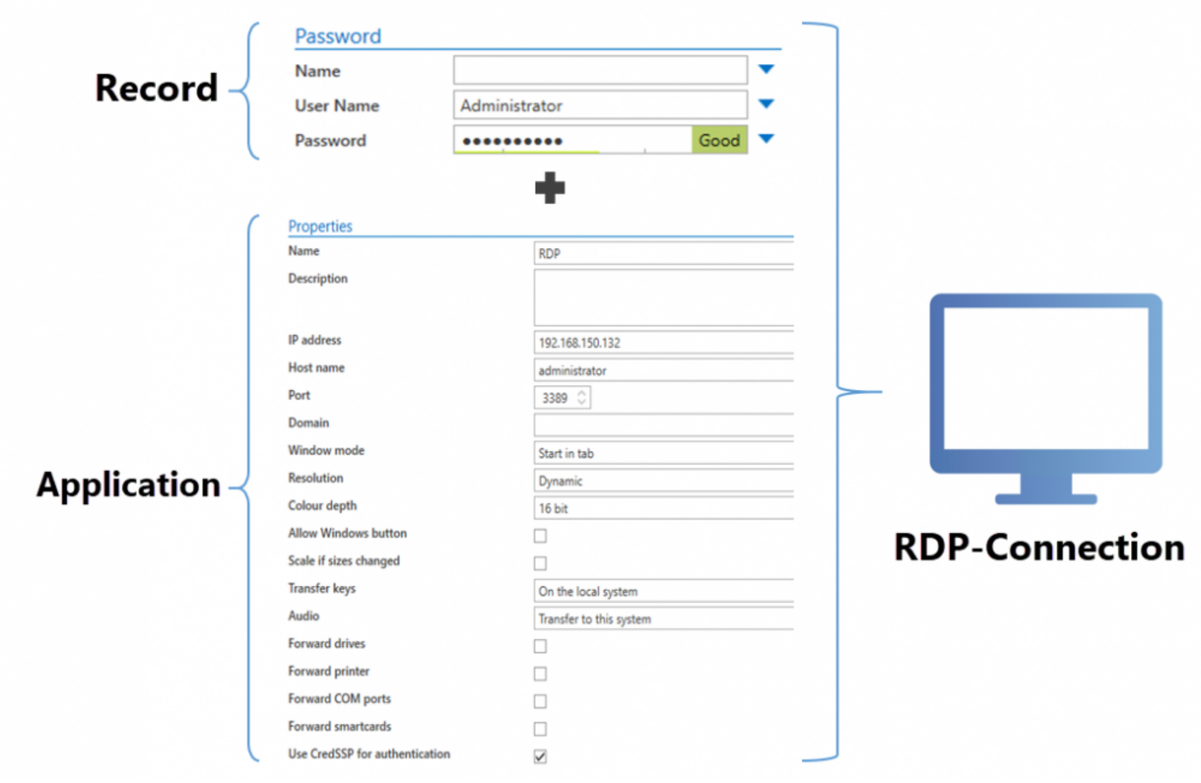


Linking records and applications

The application defines the requirements for the desired connection and also optionally for the target system. By linking records with applications, the complete login process can be automated. If the record now also supplies the user name and password, all of the information required for the login is available. Applications and records are linked via the “Start” tab in the ribbon. If this link to a record is established, a 1-click login to the target system is possible.



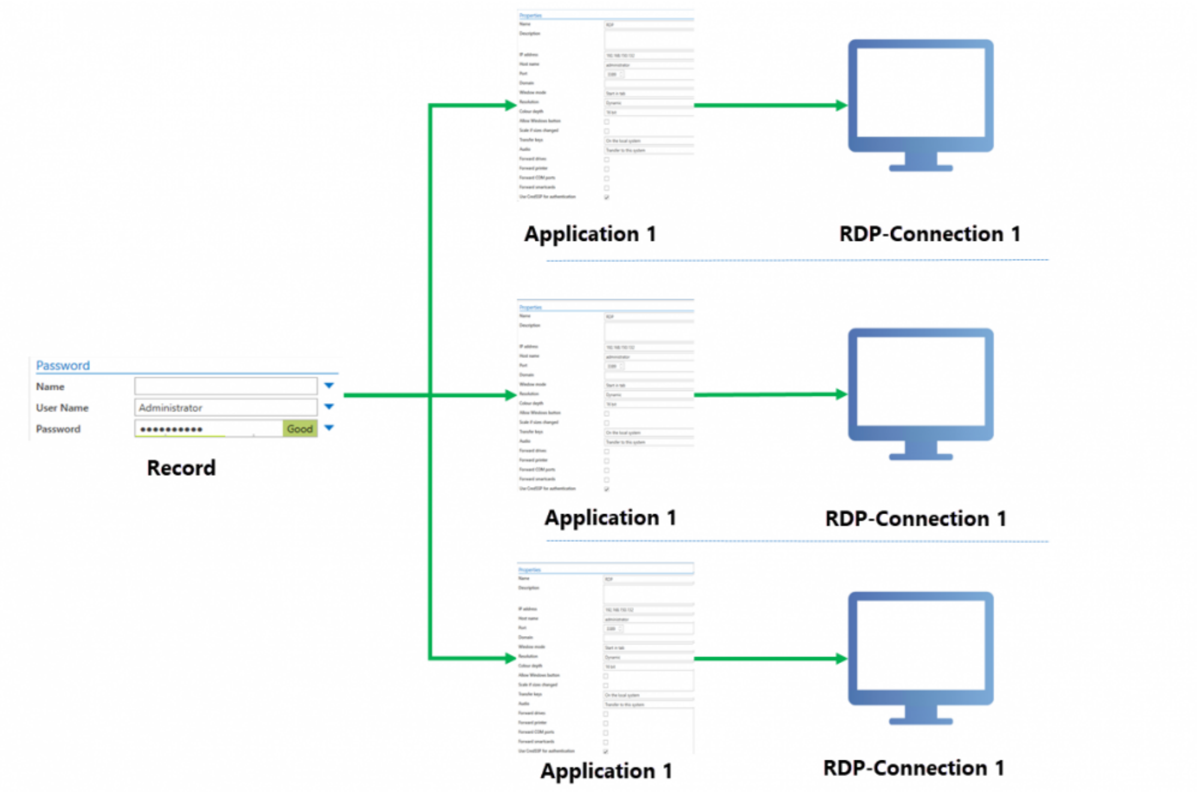
The following example illustrates this process using an RDP connection:



Name:
User Name: Administrator
Password: ●●●●●●●●●●● Good

Name: RDP
Description:
IP address: 192.168.150.132
Host name: administrator
Port: 3389
Domain:
Window mode: Start in tab
Resolution: Dynamic
Colour depth: 16 bit
Allow Windows button: □
Scale if sizes changed: □
Transfer keys: On the local system
Audio: Transfer to this system
Forward drives: □
Forward printer: □
Forward COM ports: □
Forward smartcards: □
Use CredSSP for authentication: ☑

A record can also be linked to multiple target systems in this manner. The user name and record are supplied by the record, while all other information necessary for the login is supplied by the different applications. In the following example, a record (user name and password) is linked to multiple access points.



This is generally a very common scenario. Nevertheless, it should be noted that accessing multiple servers with one single password is questionable from a security standpoint. It is generally recommended that a unique password is issued for every server/access point.

It is possible to leave the **IP address** field empty in the application. If an **IP address** field exists in the linked record then this address will be used. If there is also no IP address in the record, a popup window will appear in which the desired IP address can be entered manually.

Learning the applications

Which applications need to be learned?

As already indicated in the previous section, RDP and SSH applications are completely embedded in Password Safe. These applications thus do not need to be specially learned. All other applications in Windows need to be learned once.

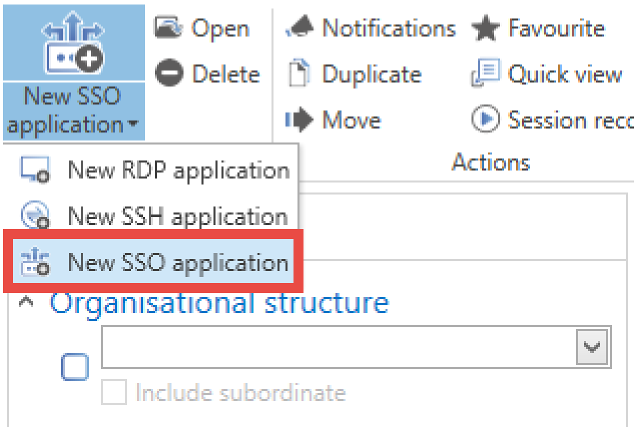
What does learning mean?

The record contains the user name and password. Learning involves defining the steps required. The result is equivalent to a script that defines where precisely the login data should be entered. In Password Safe, the completed instructions themselves are also known as an “application”.

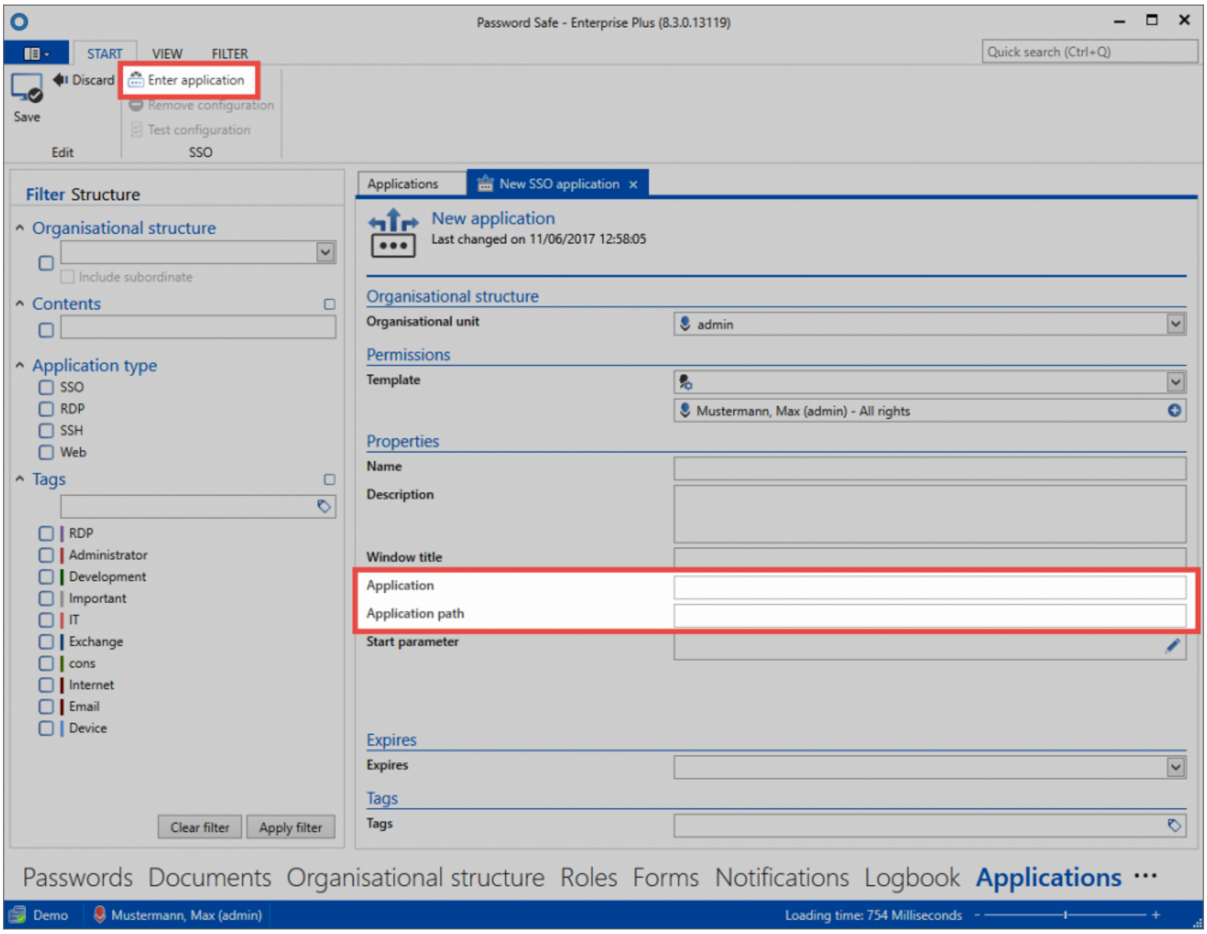
Configuration

! The user right “Can add new applications” is required for creating applications

First, a new SSO application is created via the ribbon.



Various properties for the application can now be defined in the tab that opens. The fields **Window title**, **Application** and **Application path** are not manually filled. This is done via the **Create application** button in the ribbon:



New application
Last changed on 11/06/2017 12:58:05

Organisational structure
Organisational unit: admin

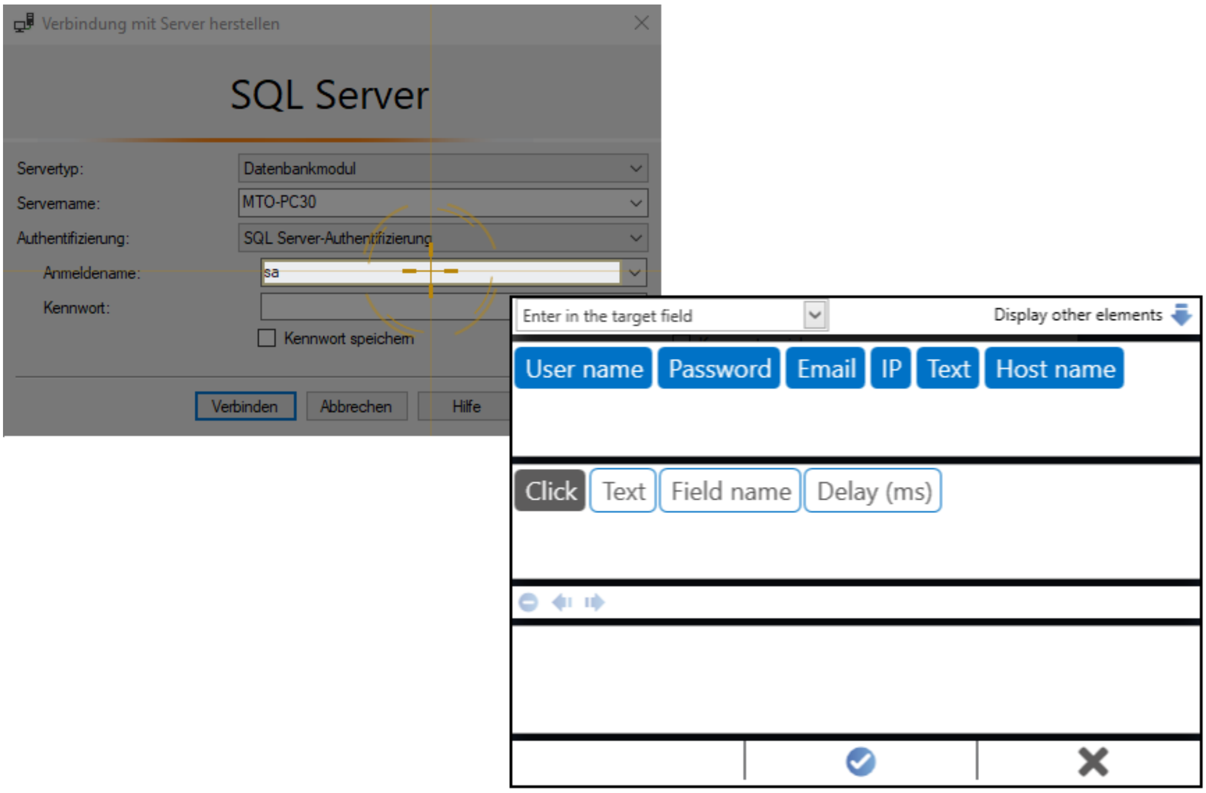
Permissions
Template:
Mustermann, Max (admin) - All rights

Properties
Name:
Description:
Window title:
Application:
Application path:
Start parameter:

Expires
Expires:

Tags
Tags:

A crosshair cursor now appears. It enables the actual “mapping” or assignment of the target fields. You can see the field assignment for the user name below using a login to an SQL server as an example. All of the other fields that should be automatically entered are assigned in the same way. The process is always the same. You select the field that needs to be automatically filled and then decide which information should be used to fill it.



Verbindung mit Server herstellen

SQL Server

Servertyp: Datenbankmodul

Servername: MTO-PC30

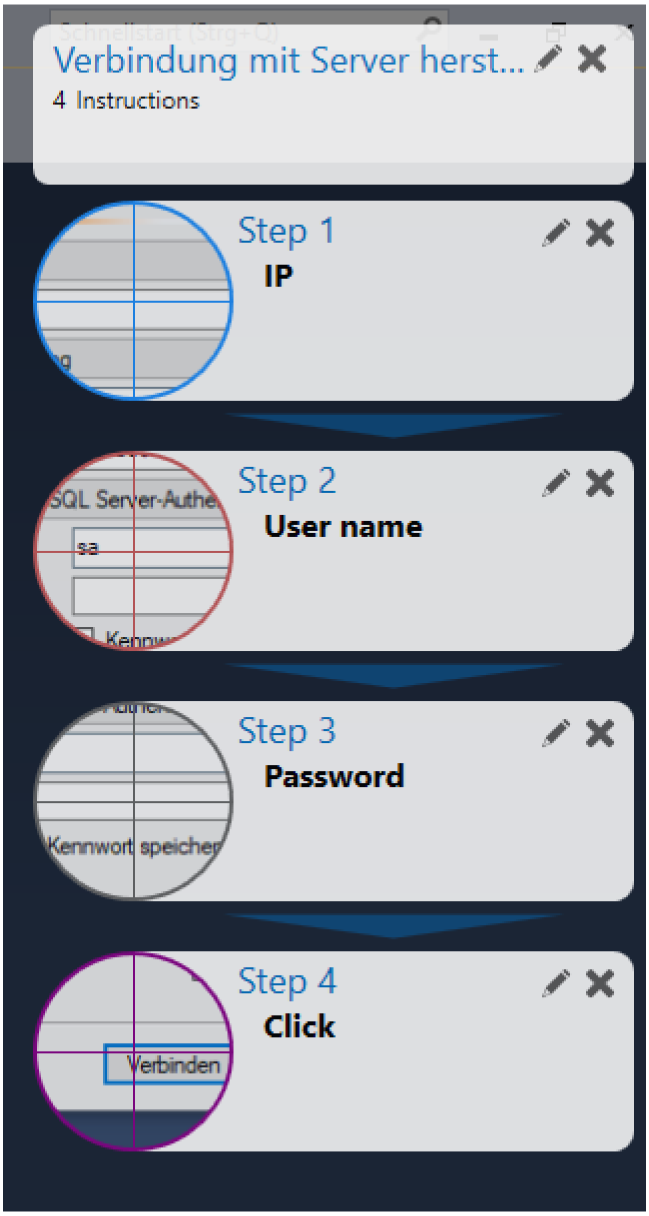
Authentifizierung: SQL Server-Authentifizierung

Anmeldename: sa

Kennwort:

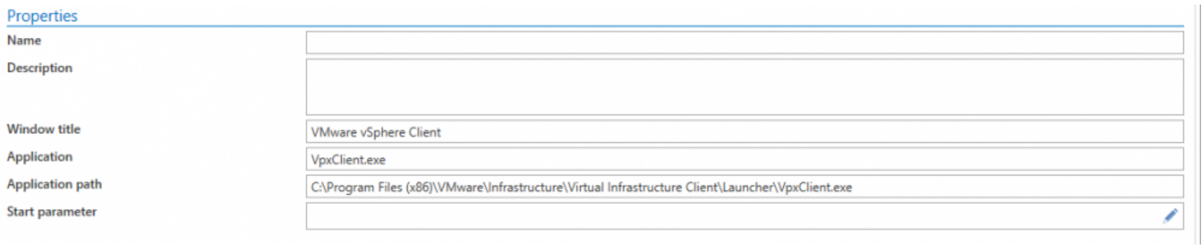
□ Kennwort speichern

In parallel to the previous step, all of the already assigned fields will be displayed on the right edge of the screen. In this example, the VMware vSphere Client has a total of 4 assigned fields: IP, user name, password and clicking the button to subsequently confirm the login.



Graphical recognition:
The graphical recognition function provides additional protection. It can be used to define other factors for the SSO. An area is defined that then serves as the output for the comparison (e.g. for login masks with an image). In order to activate the graphical recognition function, click on the eye at the top right after assigning the fields! The area that will serve as the output point is then marked.

Once you have assigned all of the fields, you can exit the application process using the enter button. The fields “Window title”, “Application” and “Application path” mentioned at the beginning are now automatically filled.



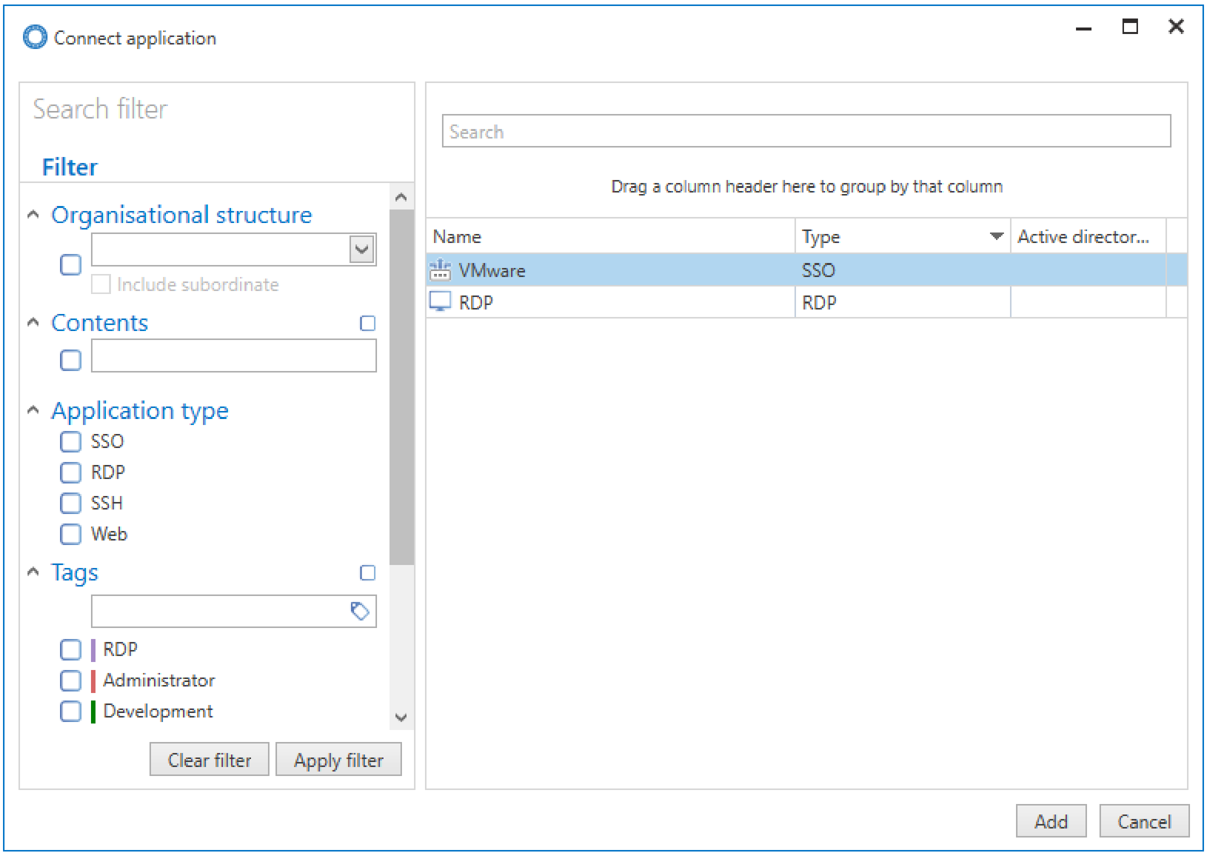
Properties

Name	
Description	
Window title	VMware vSphere Client
Application	VpxClient.exe
Application path	C:\Program Files (x86)\VMware\Infrastructure\Virtual Infrastructure Client\Launcher\VpxClient.exe
Start parameter	

As you can see, the .exe file is directly referenced. If the application is saved to the same storage location for all users, it can then also be accessed by all other users.

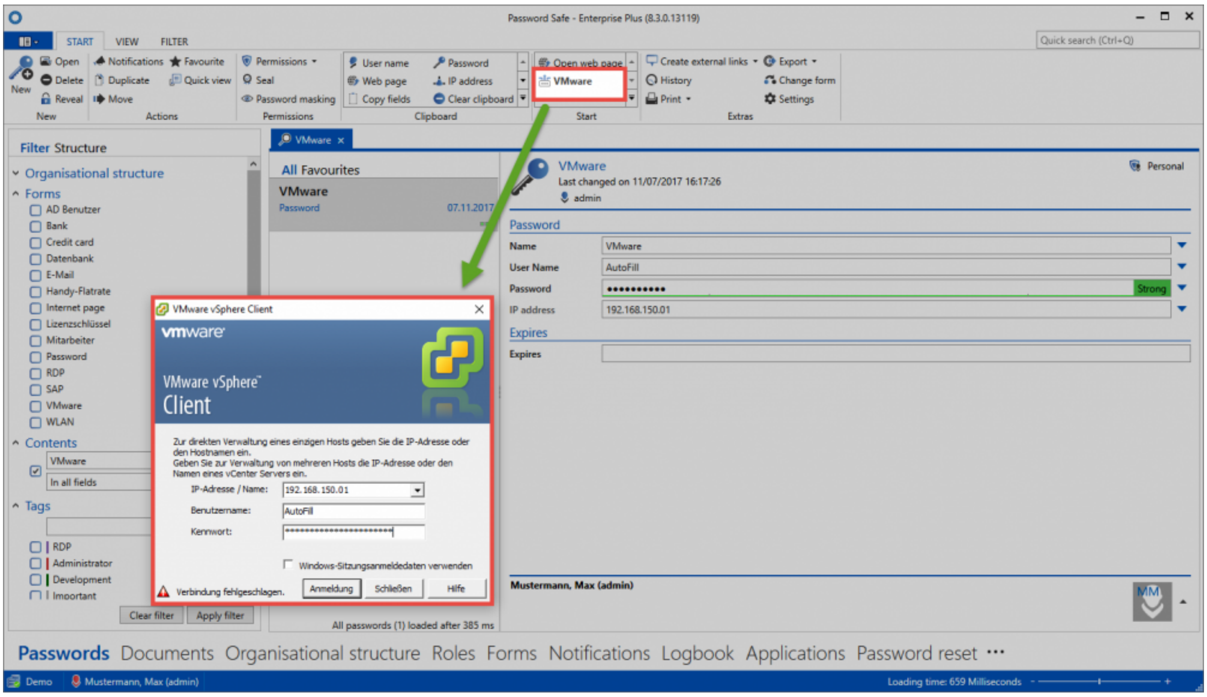
Linking records with applications

In the Passwords module, the newly created application can now be directly linked. To do this, mark the record to be linked and open the “Connect application” menu in the “Start” tab via the ribbon. This will open a list of all the available applications. It is now possible here to link to the previously created application “VMware”.



Name	Type	Active director...
VMware	SSO	
RDP	RDP	

When the link has been established, this application can then be directly started via the ribbon in future. Pressing the button directly opens the linked application.



VMware

Password 07.11.2017

All passwords (1) loaded after 385 ms

VMware
Last changed on 11/07/2017 16:17:26
admin

Personal

Password

Name	VMware
User Name	AutoFill
Password	•••••••••• Strong
IP address	192.168.150.01

Expires

Expires	

Mustermann, Max (admin)

Contents: ☑ VMware, In all fields

VMware vSphere Client

vmware

VMware vSphere™ Client

Zur direkten Verwaltung eines einzigen Hosts geben Sie die IP-Adresse oder den Hostnamen ein.
Geben Sie zur Verwaltung von mehreren Hosts die IP-Adresse oder den Namen eines vCenter Servers ein.

IP-Adresse / Name:	192.168.150.01
Benutzername:	AutoFill
Kennwort:	**********************

□ Windows-Sitzungsanmeldedaten verwenden

Verbindung fehlgeschlagen.

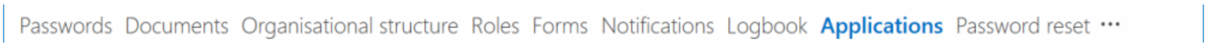
Anmeldung | Schließen | Hilfe

! With respect to permissions, applications are subject to the same rules as for passwords, roles or documents. It is thus possible to separately define which group of users is permitted to use each application.

Recording a session

What is session recording?

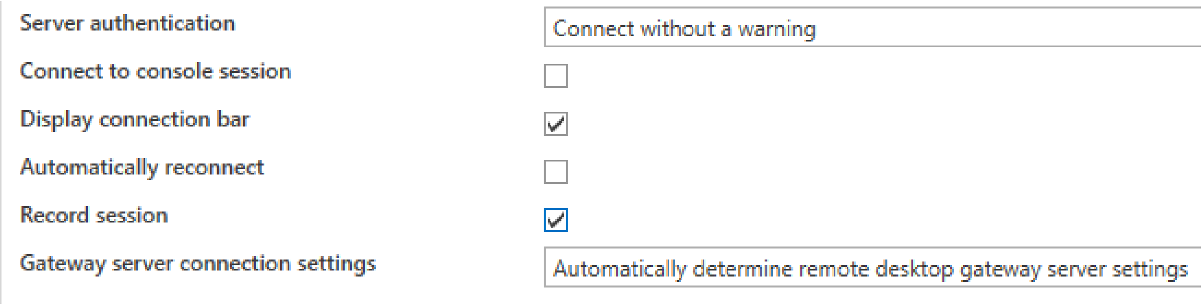
Session recording can be used to make a visual recording of RDP and SSH sessions. These recordings can then be subsequently viewed and evaluated. In this context, it is also possible to limit this functionality so that only the user themselves or an assigned person e.g. security officer can view and evaluate these recordings.



> Please note that session recording uses memory in the database. Although the way the recordings are saved is efficient in terms of resources, the required amount of memory varies greatly depending on the content. The more that is done during the recorded session, the higher the memory usage.

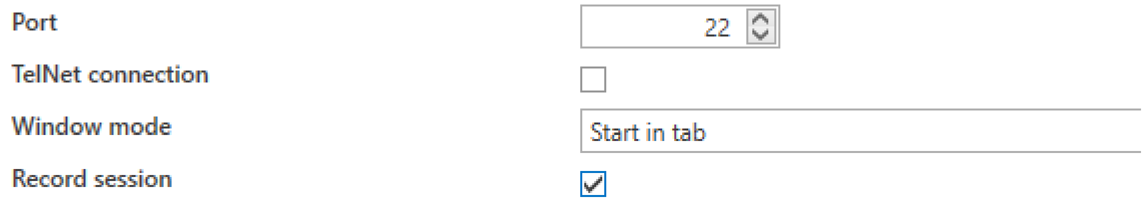
Session recording firstly needs to be activated for the relevant RDP or SSH application before it can take place.

RDP



Server authentication	Connect without a warning
Connect to console session	□
Display connection bar	☑
Automatically reconnect	□
Record session	☑
Gateway server connection settings	Automatically determine remote desktop gateway server settings

SSH



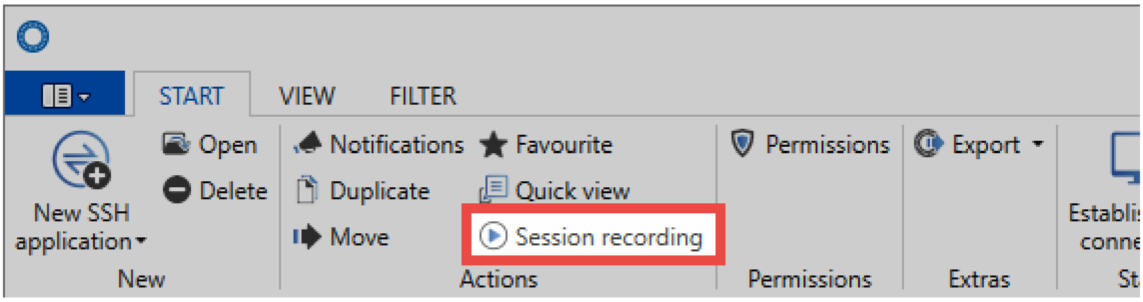
Port	22
TelNet connection	□
Window mode	Start in tab
Record session	☑

If the setting has been activated, the recording will start automatically the next time a connection is established.

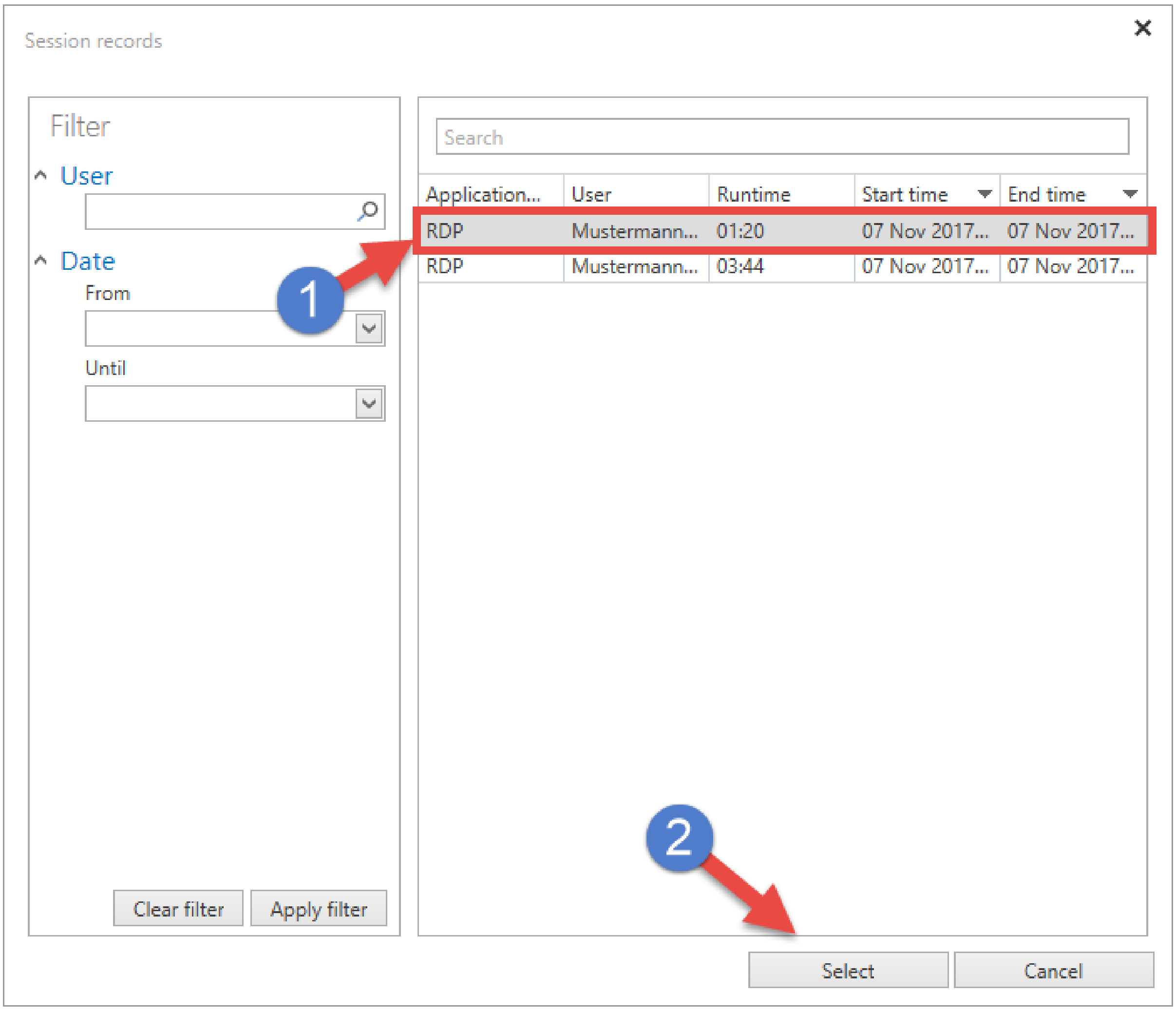
The recordings are already streamed to the server and into the database during the recording process. Therefore, no recordings are lost even if the connection is terminated. They are immediately saved until the connection is terminated or until the end of the session.

Viewing the session recordings

If recordings exist for an application, these can be called up and viewed in the Applications module.

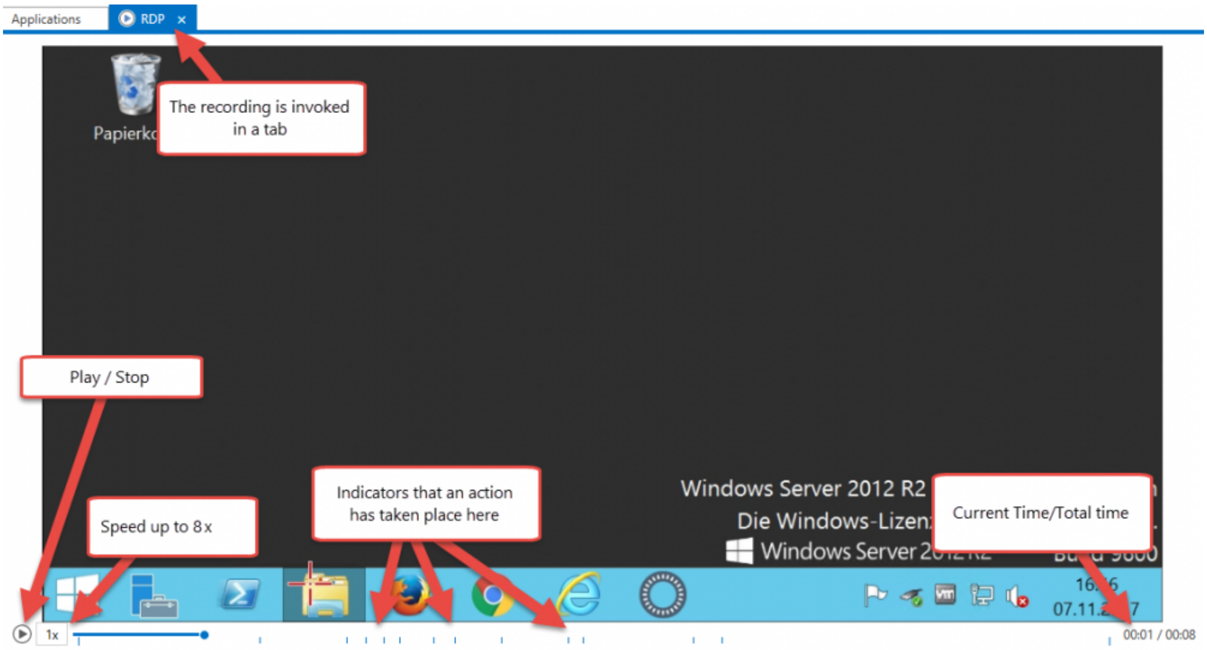


It is possible to search the session recordings using the filter as usual. It is also possible here to limit the search results based on the date and user. In the section on the right, it is also possible to further filter the searched list based on all column contents.



Application...	User	Runtime	Start time	End time
RDP	Mustermann...	01:20	07 Nov 2017...	07 Nov 2017...
RDP	Mustermann...	03:44	07 Nov 2017...	07 Nov 2017...

Once a session recording has been selected, a new tab will open in which you can view the recording. The function “Skip inactivity” can be activated via the ribbon so that a recording can be effectively and quickly viewed so as only to see the relevant actions.



When are indicators set?

- Mouse click
- Keyboard command

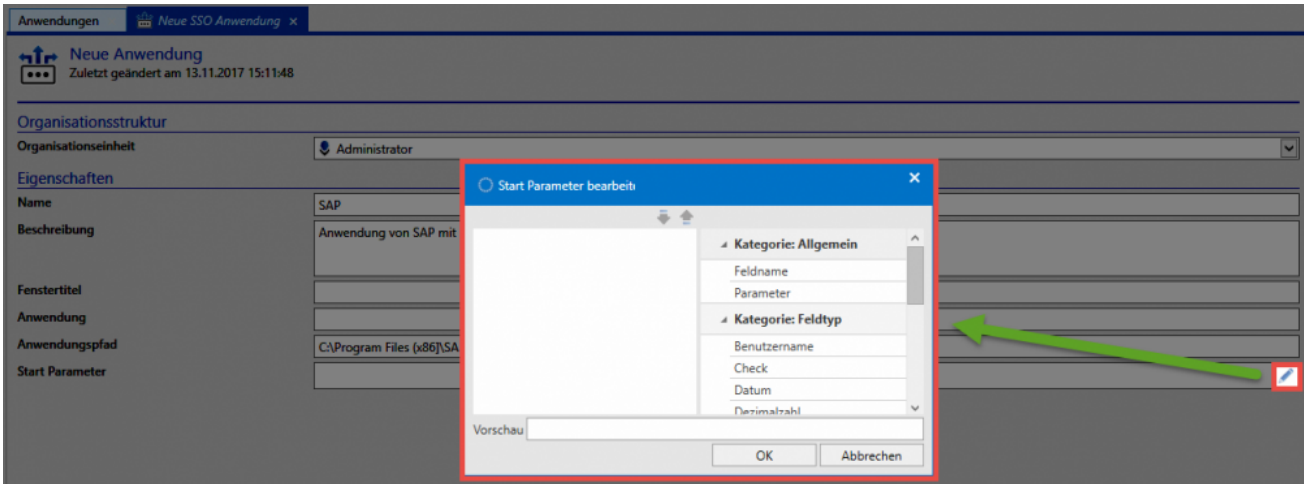
Start parameters

Start parameters for SSO applications

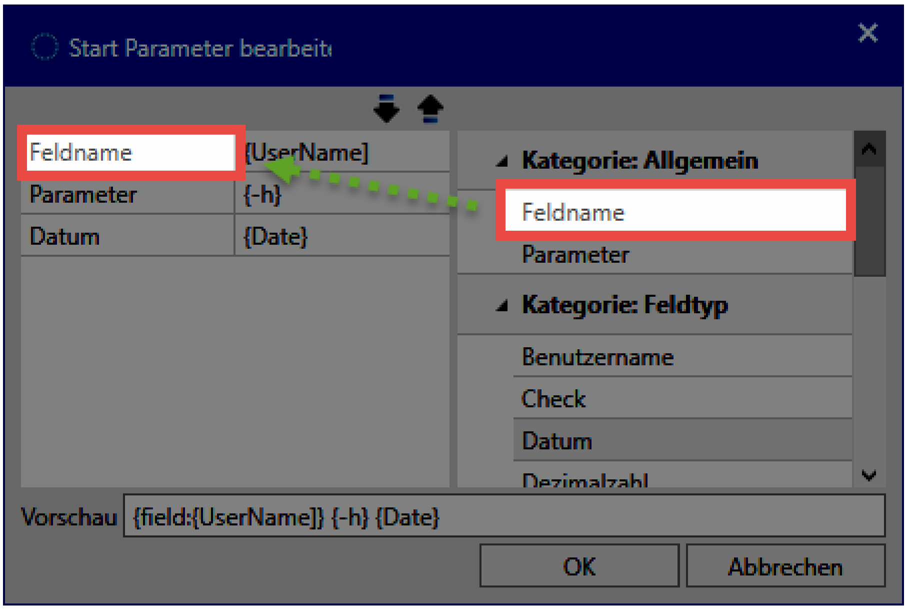
Start parameters can be defined when creating or editing an SSO application. These parameters are immediately transferred when starting the application. This is done, for example, to directly start the program with various basic settings. The corresponding parameters should be requested from the manufacturer of the software or taken from the documentation.

Configuration of the parameters

The parameters can be directly entered in the application in the corresponding field. Alternatively, a configuration window is also available for this purpose.



The required elements can be moved here from the right side to the left side by drag & drop.



Feldname	{UserName]
Parameter	{-h}
Datum	{Date}

Vorschau {field:{UserName]} {-h} {Date}

Different categories are available here:

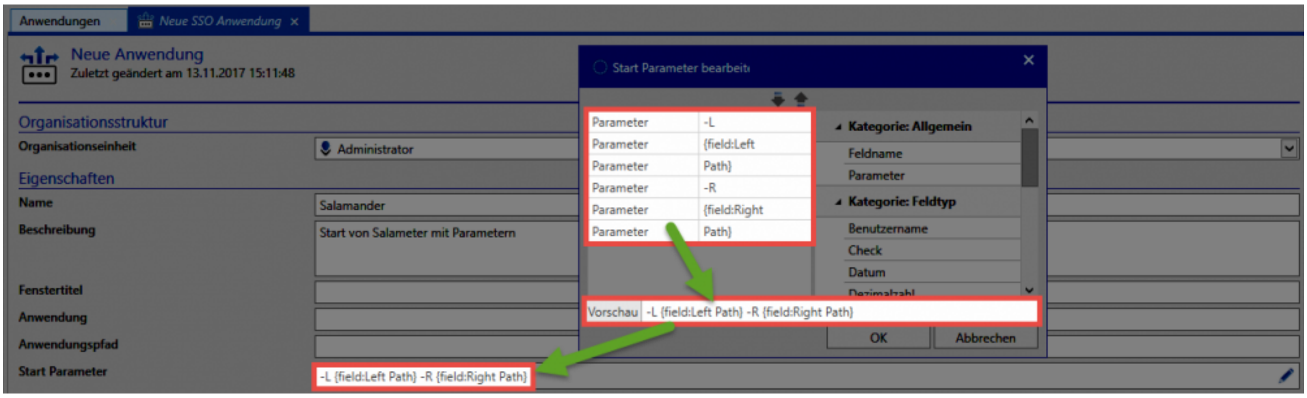
- In the **Parameter** category, only the parameter descriptions **Field name** or **Parameter** are available. These then need to be manually supplemented.
- The parameters in the **Field name** category can directly address the fields, meaning directly transfer the field names.

Example

In this example, the following start parameters have been defined for the Salamander application:

- -L (for folder path in the left column)
- -R (for folder path in the right column)

For both parameters, the password fields with the names “Left Path” and “Right Path” are then transferred in each case.



Zuletzt geändert am 13.11.2017 15:11:48

Organisationseinheit: Administrator

Name: Salamander

Beschreibung: Start von Salameter mit Parametern

Fenstertitel

Anwendung

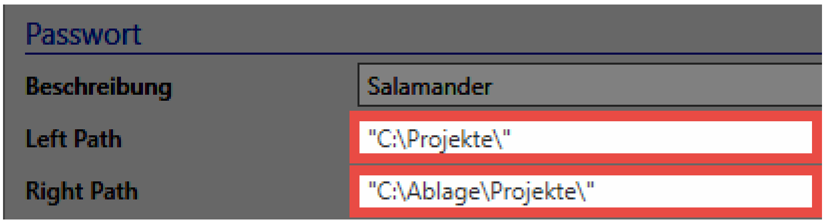
Anwendungspfad

Start Parameter: -L {field:Left Path} -R {field:Right Path}

Parameter	-L
Parameter	{field:Left
Parameter	Path}
Parameter	-R
Parameter	{field:Right
Parameter	Path}

Vorschau -L {field:Left Path} -R {field:Right Path}

The application is then linked with the following password:



Passwort

Beschreibung: Salamander

Left Path: "C:\Projekte\"

Right Path: "C:\Ablage\Projekte\"

When the Salamander application is started, the placeholder is replaced by the field names. Therefore, instead of

-L {field:Left Path} -R {field:Right Path}

the following start parameters are transferred:

-L "C:\Projekte\" -R "C:\Ablage\Projekte"

Placeholder for fields

Fields can be added via certain placeholders based on their type or their name. The easiest way to do this is using the configuration window described above.

Field type	Placeholder
Text	{Text}
Password	{Password}
Date	{Date}
Check	{Check}
URL	{Url}
Email	{Email}
Phone	{Phone}
List	{List}
Header	{Header}
Multiline text	{Memo}
Multiline password text	{PasswordMemo}
Integer	{Int}
Floating-point number	{Decimal}
User name	{UserName}
IP address	{Ip}

Enter field name	{field:name}

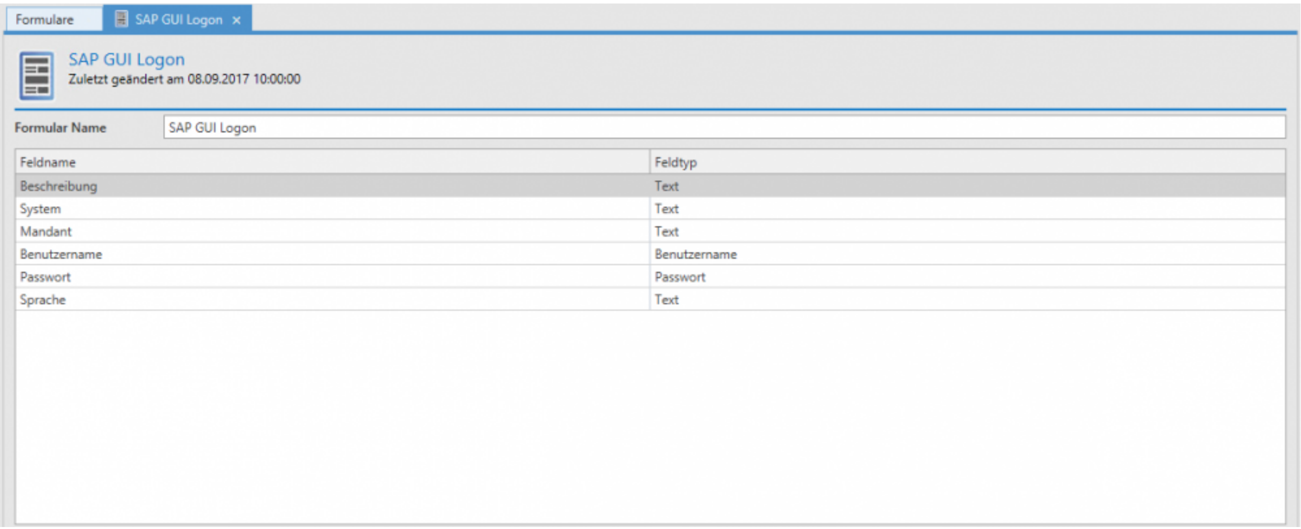
SAP GUI logon

Fundamental information

Logging into SAP can be achieved via “”:#startparameter. The prerequisite here is for the login process to be carried out via “SAPshortcuttextileRef:12094811745b4c70ed6613b:linkStartMarker:”.
All available parameters are listed under “”:https://wiki.scn.sap.com/wiki/display/NWTech/SAPshortcut.

Form

Firstly, a “form”:#formulare should be created with the required fields. This could look like this:



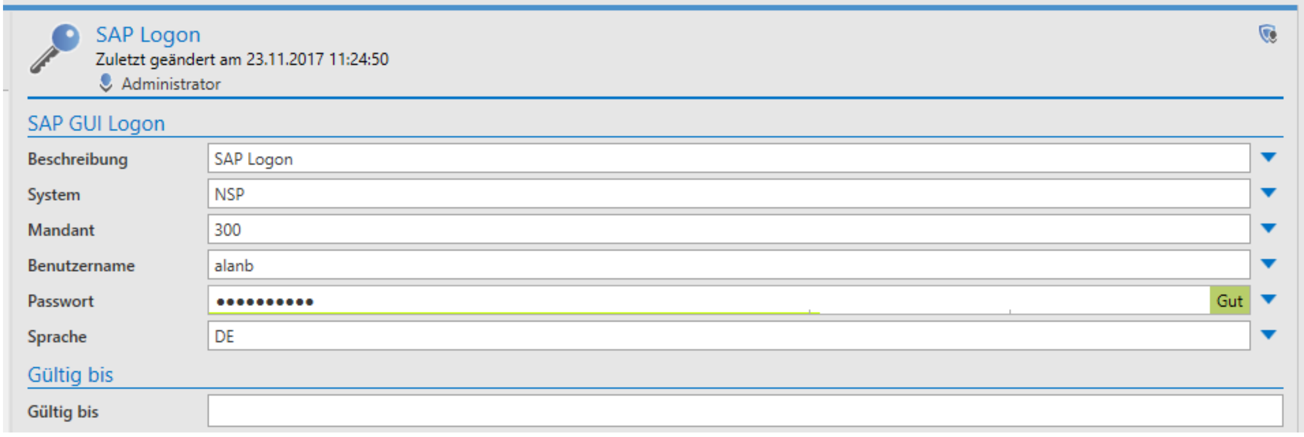
SAP GUI Logon
Zuletzt geändert am 08.09.2017 10:00:00

Formular Name: SAP GUI Logon

Feldname	Feldtyp
Beschreibung	Text
System	Text
Mandant	Text
Benutzername	Benutzername
Passwort	Passwort
Sprache	Text

Record

A corresponding record is then created via the form:



SAP Logon
Zuletzt geändert am 23.11.2017 11:24:50
Administrator

SAP GUI Logon

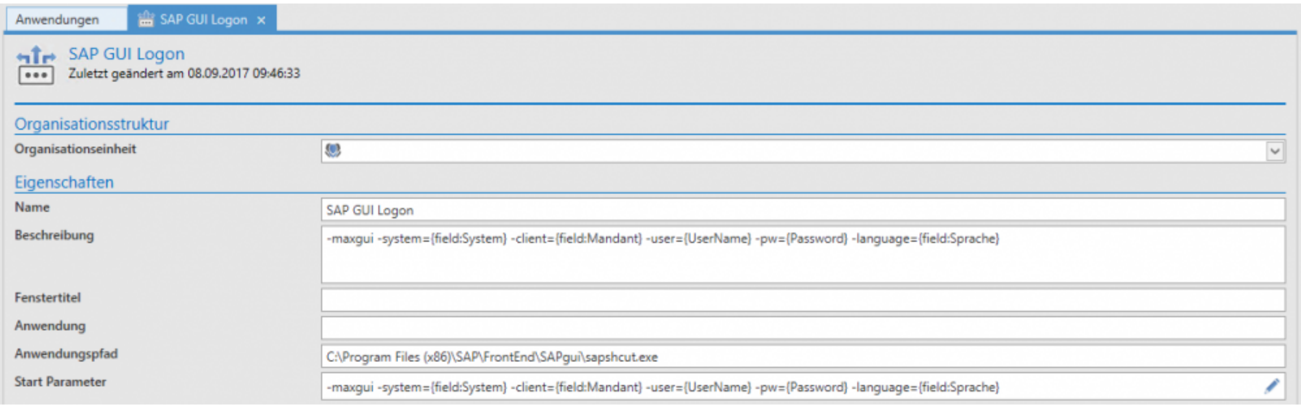
Beschreibung	SAP Logon
System	NSP
Mandant	300
Benutzername	alanb
Passwort	●●●●●●●●●● Gut
Sprache	DE

Gültig bis

Gültig bis	

Application

A corresponding SSO application now needs to be created.



SAP GUI Logon
Zuletzt geändert am 08.09.2017 09:46:33

Organisationsstruktur

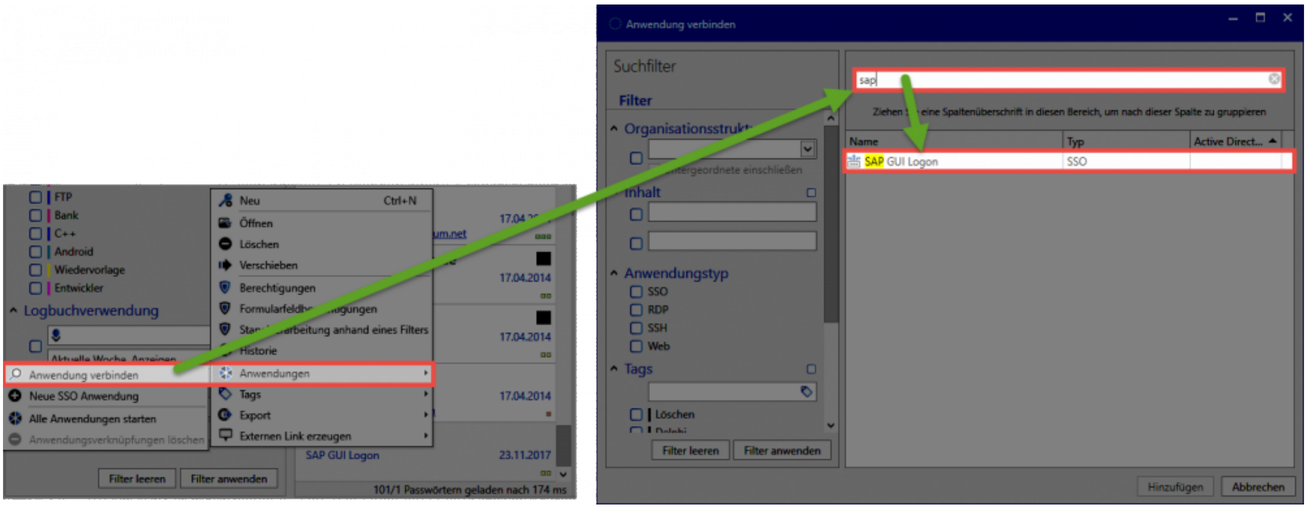
Organisationseinheit	

Eigenschaften

Name	SAP GUI Logon
Beschreibung	-maxgui -system={field:System} -client={field:Mandant} -user={UserName} -pw={Password} -language={field:Sprache}
Fenstertitel	
Anwendung	
Anwendungspfad	C:\Program Files (x86)\SAP\FrontEnd\SAPgui\sapshcut.exe
Start Parameter	-maxgui -system={field:System} -client={field:Mandant} -user={UserName} -pw={Password} -language={field:Sprache}

Link

The record now needs to be linked with the application. To do this, open the context menu by right clicking on the record. The previously created application can then be selected here via **Applications** and **Connect application**.



sap

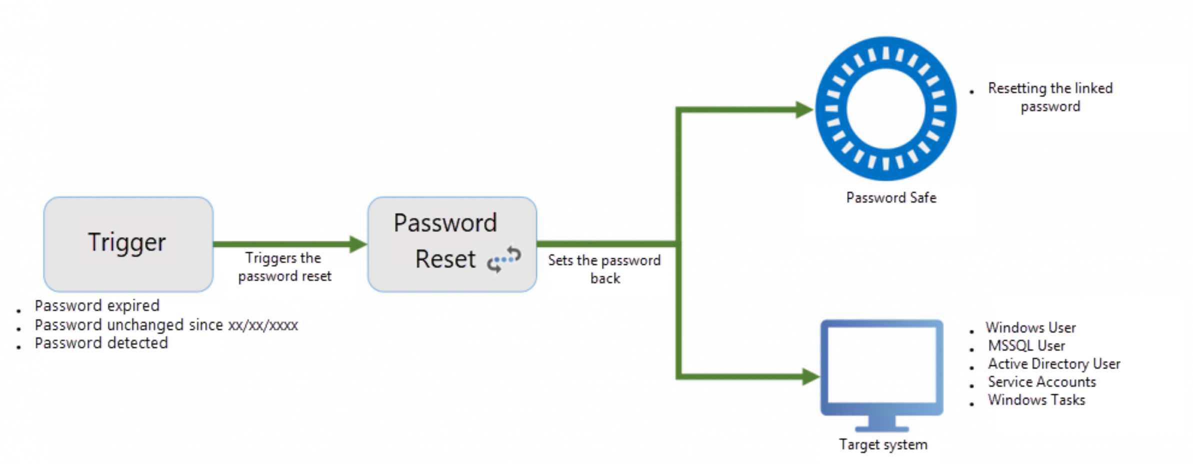
Name	Typ	Active Direct...
SAP GUI Logon	SSO	

The link is then displayed in the ribbon. Clicking on the link will now open SAP, whereby the parameters for logging in to the application are directly transferred.

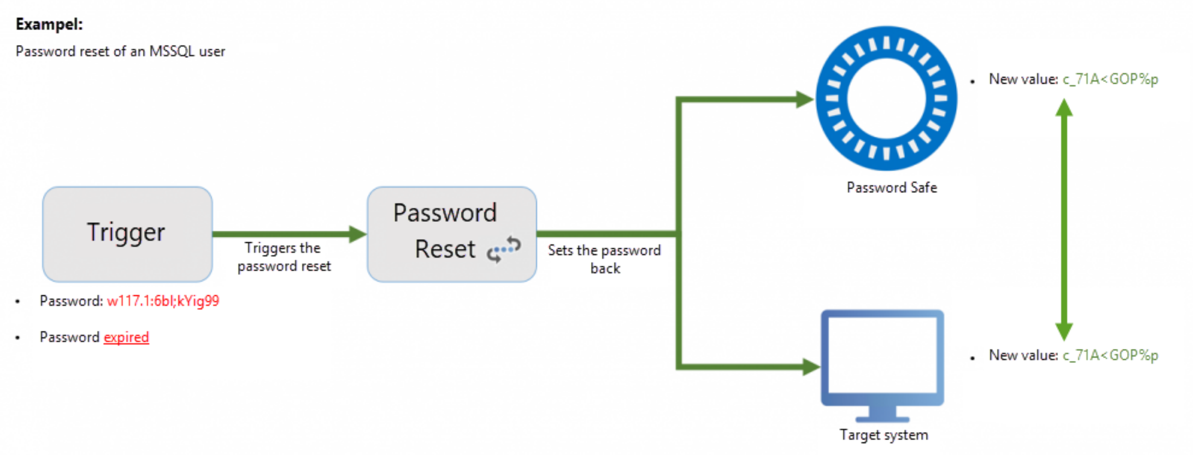
Password reset

What is Password Reset?

The safest passwords are those that no one knows. A Password Reset enables passwords to be reset to a new and unknown value according to freely definable triggers. A trigger could be a definable time interval or a certain action by the user. **The value of the password is changed in both Password Safe and also on the target system**.



This process will be explained below using a specific example. The password for the MSSQL user has expired. The Password Reset thus changes the password in Password Safe and also in the target system to a new value.



! Password Reset is an exclusive part of the **Enterprise Plus Edition**

! It is strongly recommended that Password Reset is configured * in combination with certified partners*. The desired simplification of work processes using the above-mentioned automated functions is accompanied by numerous risks.

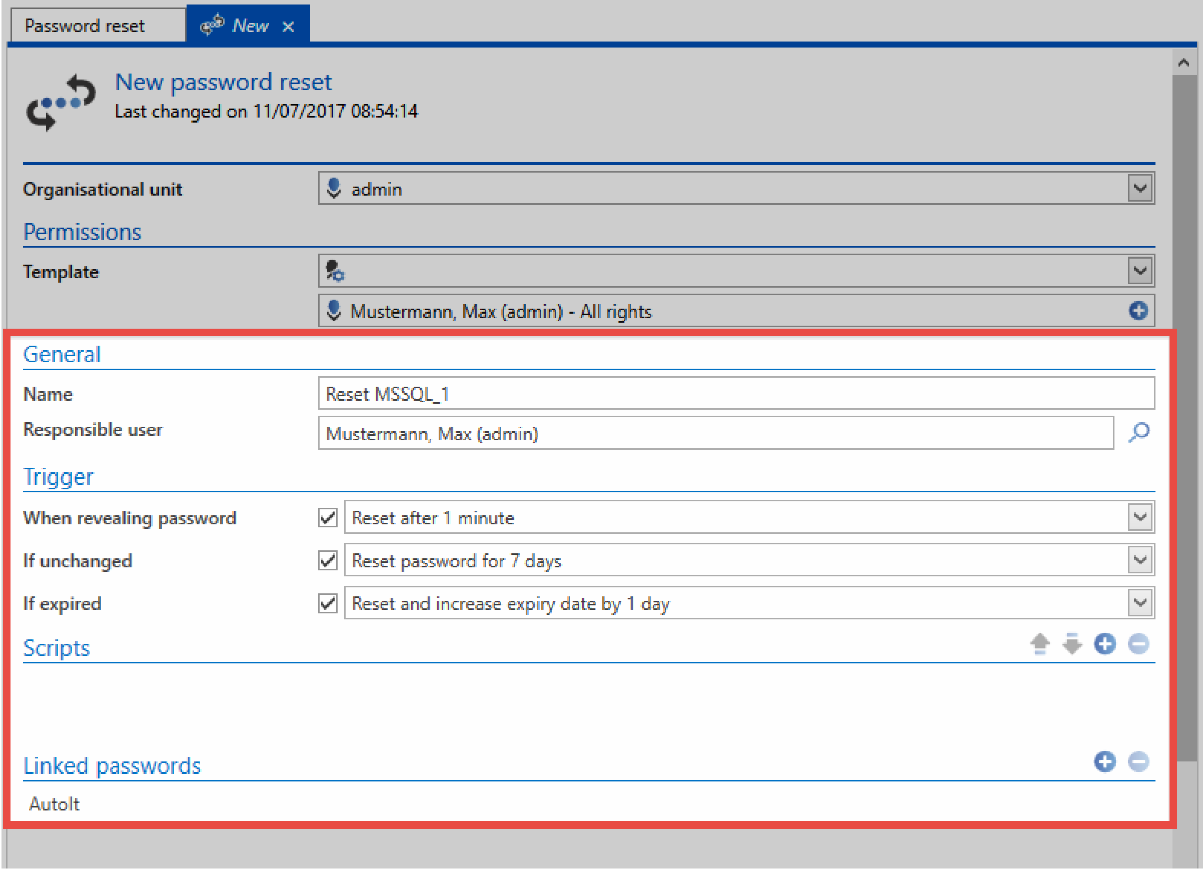
Creating a Password Reset

✻ The user rights “Display Password Reset module” and “Can add new Password Resets” are required.

New Password Resets can be directly added via the ribbon or the keyboard shortcut “Ctrl + N” in the Password Reset module. With regards to permission, a Password Reset behaves in precisely the same way as every other object. It can be managed to precisely define which users can view and use which Password Resets.

Configuration

The configuration of a new Password Reset comprises four steps. All of the necessary conditions and variables for the configuration are defined in the following areas: “General”, “Trigger”, “Scripts” and “Linked passwords”.



Last changed on 11/07/2017 08:54:14

Organisational unit: admin

Permissions

Template:

Mustermann, Max (admin) - All rights

General

Name: Reset MSSQL_1

Responsible user: Mustermann, Max (admin)

Trigger

When revealing password: ☑ Reset after 1 minute

If unchanged: ☑ Reset password for 7 days

If expired: ☑ Reset and increase expiry date by 1 day

Scripts

Linked passwords

AutoIt

General

- **Name**: Designation for the Password Reset
- **Responsible user**: All completed Password Resets are also recorded within Password Safe (logbook,…). To ensure these steps can be allocated to a user, a user who is registered in Password Safe is selected in the field “Responsible user”.

Trigger

Triggers describe the conditions that need to be fulfilled so that a Password Reset is carried out. There are a total of three possible triggers available:

- Reset the password x minutes after the password has been viewed
- Reset the password when it has not been changed for x days
- Reset the password when it has been expired for x days

At least one trigger must be activated so that the Password Reset is activated. Deactivating all triggers is equivalent to deactivating the Password Reset. All three triggers can be activated and deactivated independently of one another. Only one selection can be made in each of the three categories.

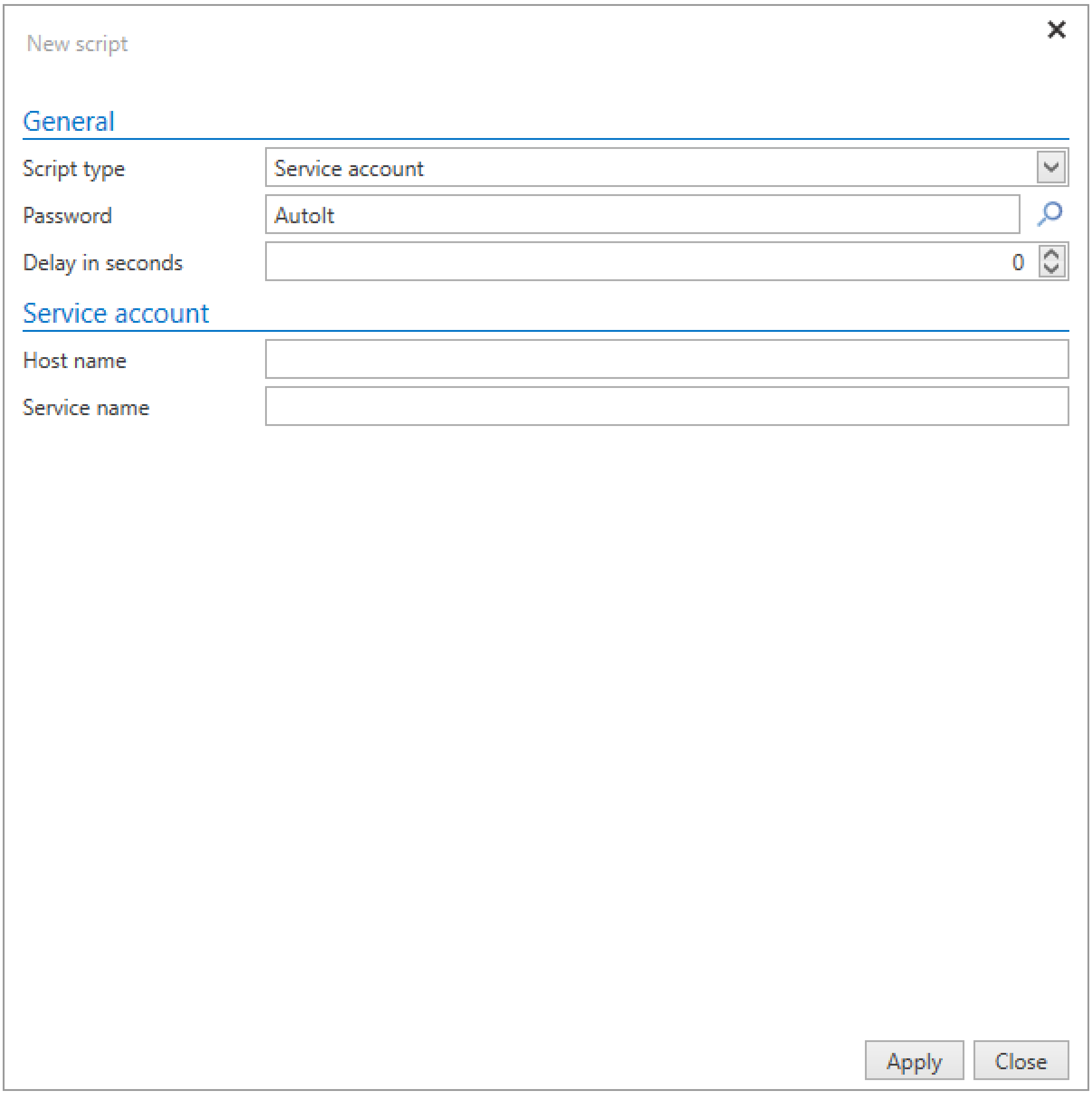
A separate system task within Password Safe checks every minute whether a trigger applies.

Scripts

The following systems can currently be automatically reset (script types).

- Windows user
- MSSQL user
- Active Directory user
- Service accounts
- Windows tasks

A new dialogue appears after the selection in which the type of system “to be reset” can be defined.



New script

General

Script type: Service account

Password: AutoIt

Delay in seconds: 0

Service account

Host name:

Service name:

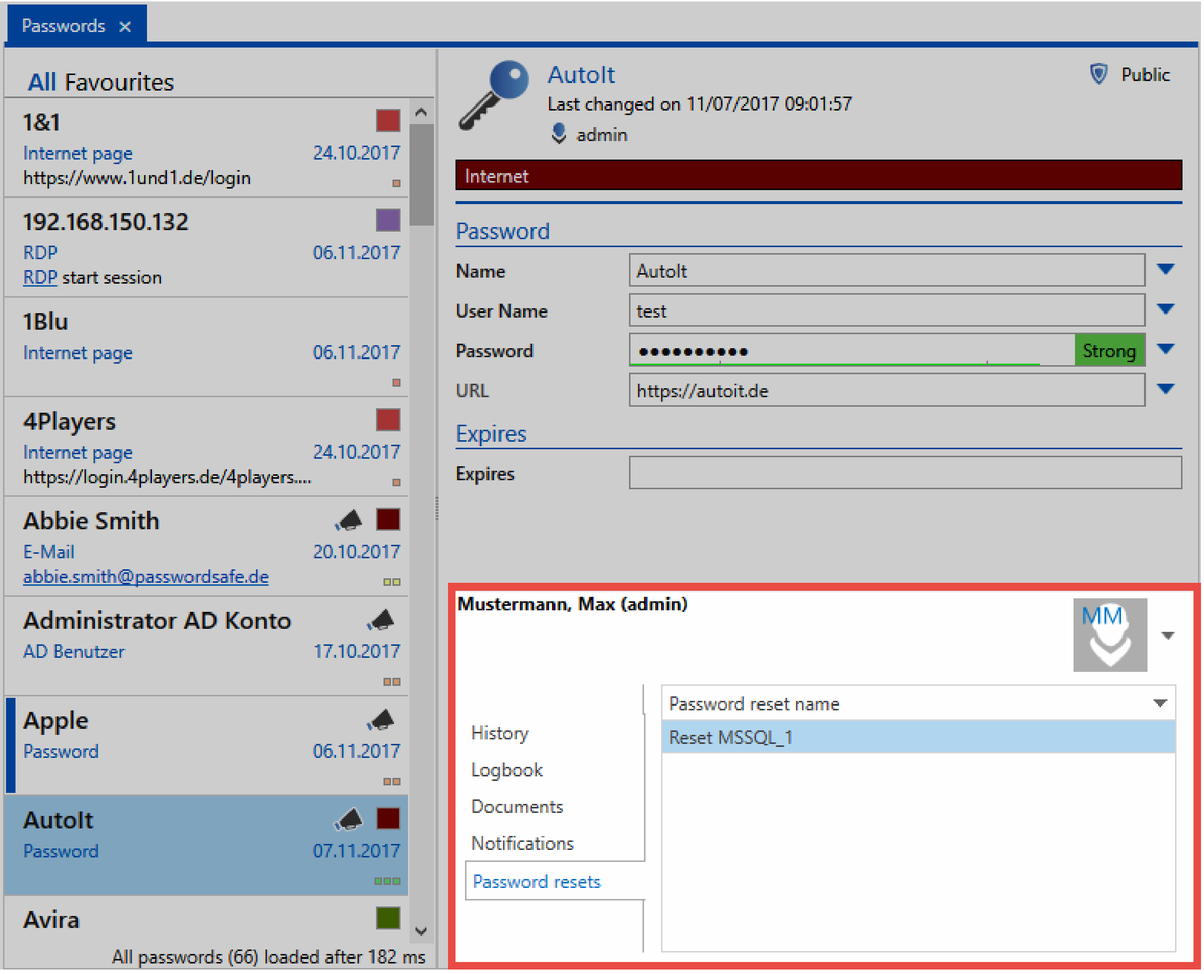
- **Script type**: You select here from the possible script types.
- **Password**: The credentials for the record that will ultimately carry out the Password Reset.

The required information is specifically requested in each case. For example, if the reset is for an MSSQL user, the MSSQL instance and the port used needs to be entered.

> ✻ It is not possible to create a Password Reset without an associated script.

Linked passwords

All records that should be reset with the Password Reset according to the selected trigger are listed under “Linked passwords”. It is possible to enter multiple objects. The linked Password Reset is also visible in the footer of the reading pane once it has been successfully configured.



Passwords ×
All Favourites
1&1
Internet page 24.10.2017
https://www.1und1.de/login
192.168.150.132
RDP 06.11.2017
RDP start session
1Blu
Internet page 06.11.2017
4Players
Internet page 24.10.2017
https://login.4players.de/4players....
Abbie Smith
E-Mail 20.10.2017
abbie.smith@passwordsafe.de
Administrator AD Konto
AD Benutzer 17.10.2017
Apple
Password 06.11.2017
AutoIt
Password 07.11.2017
Avira
All passwords (66) loaded after 182 ms
AutoIt
Last changed on 11/07/2017 09:01:57
admin
Public
Internet
Password
Name AutoIt
User Name test
Password ●●●●●●●●●● Strong
URL https://autoit.de
Expires
Expires
Mustermann, Max (admin)
MM
History
Logbook
Documents
Notifications
Password resets
Password reset name
Reset MSSQL_1

Discovery Service

The problem

Service accounts are used on most networks. These accounts are used, for example, to carry out certain services. It is not uncommon for **one and the same password** to be used here for multiple accounts. Manually changing these passwords is naturally extremely time consuming. Therefore, this process is often ignored for reasons of convenience.

The result is that the same outdated passwords are often used for many **security-critical access points**. This naturally represents a **severe security risk**. and leaves the door wide open for any attacker who gains access to just one of the passwords!

The solution

Using a combination of **Discovery Service** and **Password Reset**, **Password Safe** helps to resolve this problem by significantly increasing security on the network. The complete network can be scanned with the aid of **Discovery Service**. This process searches for both local user accounts and also Active Directory users. In addition, Password Resets are also established via which the passwords for the accounts discovered during the search can be reset.

Functionality

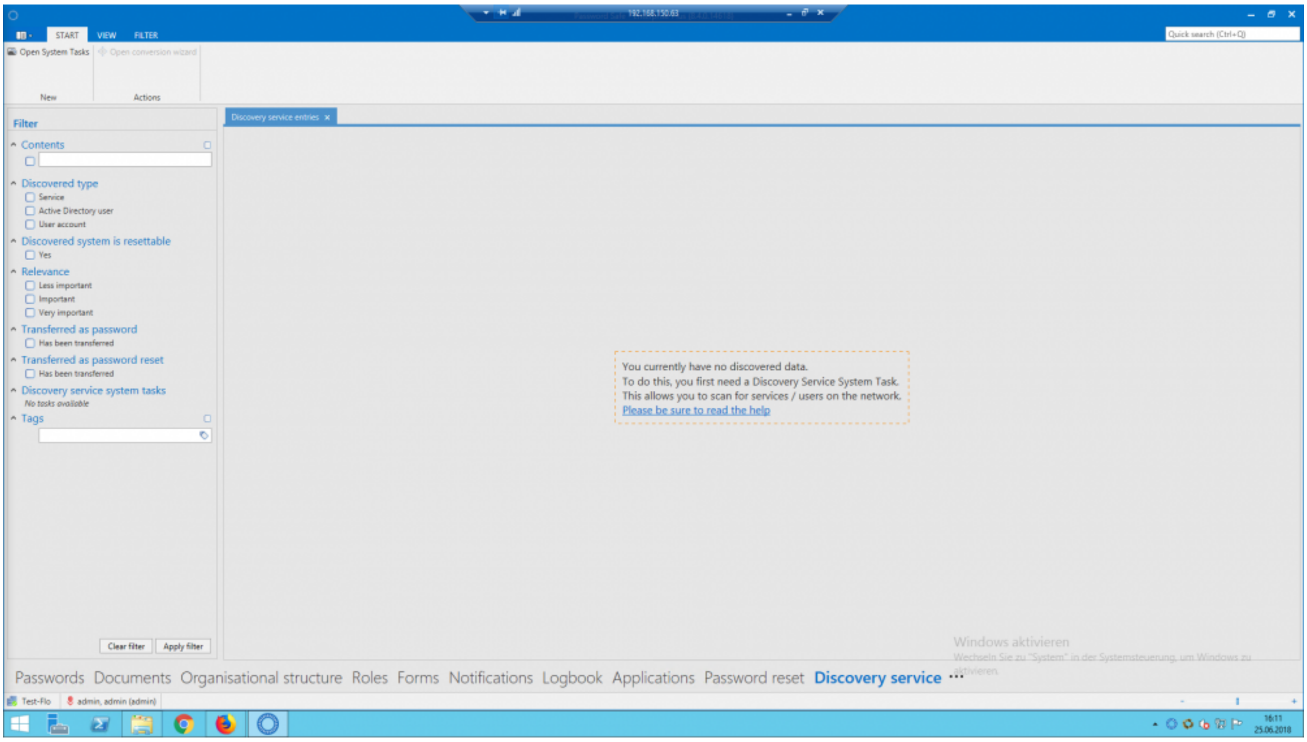
The **Discovery Service** process can be split into 3 logical steps:

1. A **Discovery Service Task** is added that searches for data on the network. This can be executed once or cyclically and runs in the background.
2. After the task has been executed successfully, the data discovered during the search is displayed in the **Discovery Service module** (e.g. Windows users, services, etc.).
3. **Passwords** or **Password Resets** can then be generated from the data discovered during the search.

Modules and requirements

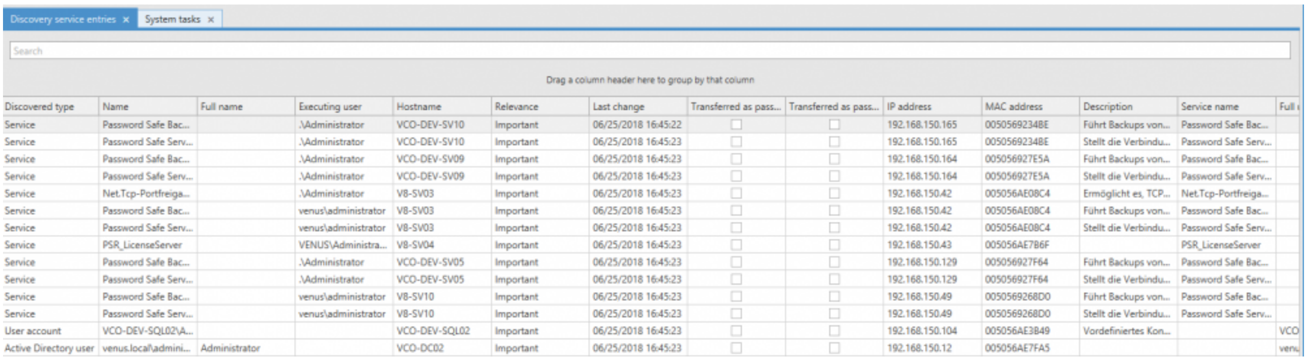
The Discovery Service module

When this module is opened in **Password Safe, there are no entries displayed in the *Discovery Service** module at the beginning. The entries need to be generated using a [System Task](#).



You currently have no discovered data.
To do this, you first need a Discovery Service System Task.
This allows you to scan for services / users on the network.
Please be sure to read the help

Once a **System Task** has been completed, the data discovered during the search is listed in a table:


Discovery service entries
System tasks
Search
Drag a column header here to group by that column

Discovered type	Name	Full name	Executing user	Hostname	Relevance	Last change	Transferred as pass...	Transferred as pass...	IP address	MAC address	Description	Service name	Full
Service	Password Safe Bac...		.\Administrator	VCO-DEV-SV10	Important	06/25/2018 16:45:22	□	□	192.168.150.165	005056923 4BE	Führt Backups von...	Password Safe Bac...	
Service	Password Safe Serv...		.\Administrator	VCO-DEV-SV10	Important	06/25/2018 16:45:23	□	□	192.168.150.165	0050569234BE	Stellt die Verbindu...	Password Safe Serv...	
Service	Password Safe Bac...		.\Administrator	VCO-DEV-SV09	Important	06/25/2018 16:45:23	□	□	192.168.150.164	005056927E5A	Führt Backups von...	Password Safe Bac...	
Service	Password Safe Serv...		.\Administrator	VCO-DEV-SV09	Important	06/25/2018 16:45:23	□	□	192.168.150.164	005056927E5A	Stellt die Verbindu...	Password Safe Serv...	
Service	Net.Tcp-Portfreiga...		.\Administrator	V8-SV03	Important	06/25/2018 16:45:23	□	□	192.168.150.42	005056AE08C4	Ermöglicht es, TCP...	Net.Tcp-Portfreiga...	
Service	Password Safe Bac...		venus\administrator	V8-SV03	Important	06/25/2018 16:45:23	□	□	192.168.150.42	005056AE08C4	Führt Backups von...	Password Safe Bac...	
Service	Password Safe Serv...		venus\administrator	V8-SV03	Important	06/25/2018 16:45:23	□	□	192.168.150.42	005056AE08C4	Stellt die Verbindu...	Password Safe Serv...	
Service	PSR_LicenseServer		VENUS\Administra...	V8-SV04	Important	06/25/2018 16:45:23	□	□	192.168.150.43	005056AE7B6F		PSR_LicenseServer	
Service	Password Safe Bac...		.\Administrator	VCO-DEV-SV05	Important	06/25/2018 16:45:23	□	□	192.168.150.129	005056927F64	Führt Backups von...	Password Safe Bac...	
Service	Password Safe Serv...		.\Administrator	VCO-DEV-SV05	Important	06/25/2018 16:45:23	□	□	192.168.150.129	005056927F64	Stellt die Verbindu...	Password Safe Serv...	
Service	Password Safe Bac...		venus\administrator	V8-SV10	Important	06/25/2018 16:45:23	□	□	192.168.150.49	0050569268D0	Führt Backups von...	Password Safe Bac...	
Service	Password Safe Serv...		venus\administrator	V8-SV10	Important	06/25/2018 16:45:23	□	□	192.168.150.49	0050569268D0	Stellt die Verbindu...	Password Safe Serv...	
User account	VCO-DEV-SQL02\A...			VCO-DEV-SQL02	Important	06/25/2018 16:45:23	□	□	192.168.150.104	005056AE3B49	Vordefiniertes Kon...		VCO
Active Directory user	venus.local\admini...	Administrator		VCO-DC02	Important	06/25/2018 16:45:23	□	□	192.168.150.12	005056AE7FA5			venu

The information can be grouped together using the column editor.

Requirements for the Discovery Service

One requirement for the **Discovery Service** is data about **Active Directory users, user accounts and service accounts.** A **Network Scan** is used to scan the network and collect this data. Before configuring the **Network Scan, a *password** needs to be issued that provides **access** to the corresponding **server/client** and **services on a network** for collecting the data. This user should also be a member of admin for the corresponding group of domains or you can use a domain administrator.

! A corresponding **password** with **rights** for the **domains** must exist before adding a **Network Scan**!

Password:

1. Required for the **authentication** process with the **Active Directory computer**
2. Required for the **authentication** process with the **WMI (Windows Management Instrumentation)** on the computer to be scanned

Requirements for the network infrastructure:

1. The computer to be scanned and AD controller must be accessible via the network
2. The service: “Windows Management Instrumentation” must have been started on the computer to be scanned (carried out by Windows as standard)
3. Help for starting the service: https://msdn.microsoft.com/de-de/library/aa826517(v=vs.85).aspx
4. The firewall must not block WMI requests (not blocked as standard)
5. Help for configuring the firewall: https://msdn.microsoft.com/de-de/library/aa822854(v=vs.85).aspx

Only **IPv4 addresses** can currently be scanned.

Open ports for the scan (necessary):

1. LDAP: Port 389(TCP,UDP)
2. RPC/WMI: Port 135(TCP)
3. (Windows Server 2008, Windows Vista and higher versions) – port 49152-65535 (TCP) or a static WMI port
4. (Windows 2000, Windows XP and Windows Server 2003) – port 1025-5000 (TCP) or a static WMI port

Computer name (Hostname):

1. IP address:
   Indicates the IP address for the element discovered during the scan – meaning where it was found (the IP address of the domain controller in the case of an Active Directory user)
2. Computer name and associated IP address:
   The computer name is first requested on the **DNS server** for the domain. The computer name returned by the server also contains the domain names as a postfix (e.g. Client01.domain.local).
   If there is no entry on the domain for the requested IP address, the computer name is determined via **NetBIOS** and the domain name is not displayed on the computer (e.g. Client01).
   In **Password Safe V8**, the **DNS request** is the preferred function for determining the computer name. If no result is delivered, a request via **NetBIOS** is made.

Configuration

Network Scan

A **Discovery Service Task** is used to add a new **Discovery Service** and is then correspondingly configured for a **Network Scan**. Depending on the configuration of the **Network Scan**, the following types are discovered:

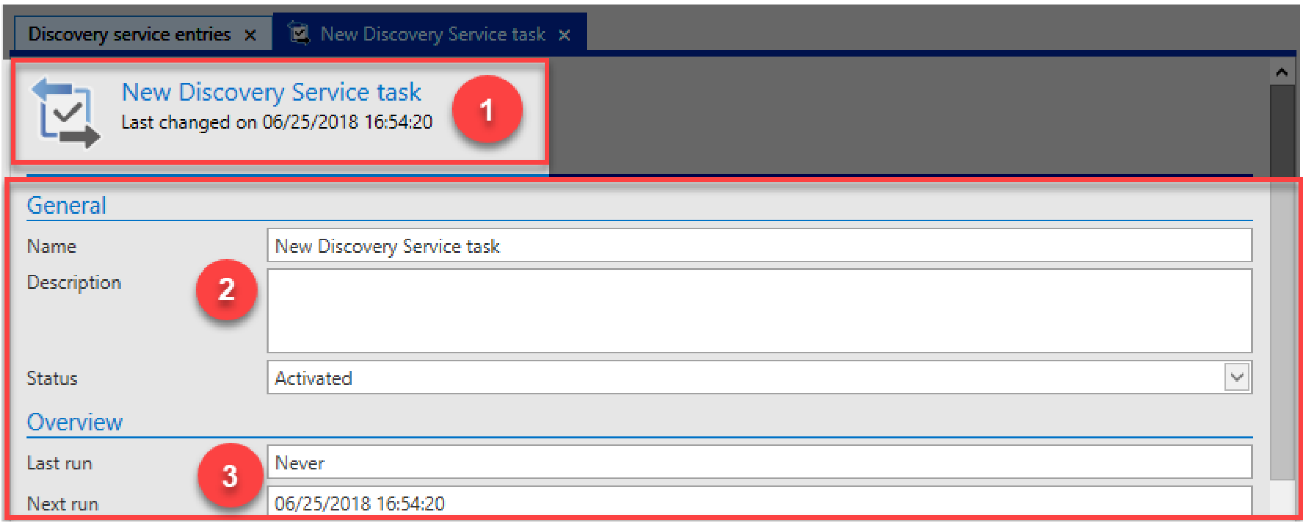
- Service accounts
- Active Directory users
- User accounts

Configuration of a Discovery Service Task

To collect data for the*Discovery Service*, the **Discovery Service Task** needs to be correspondingly configured for a **Network Scan**.

General and overview

The following image shows a newly added **Discovery Service Task**.



New Discovery Service task
Last changed on 06/25/2018 16:54:20

General

Name: New Discovery Service task
Description:
Status: Activated

Overview

Last run: Never
Next run: 06/25/2018 16:54:20

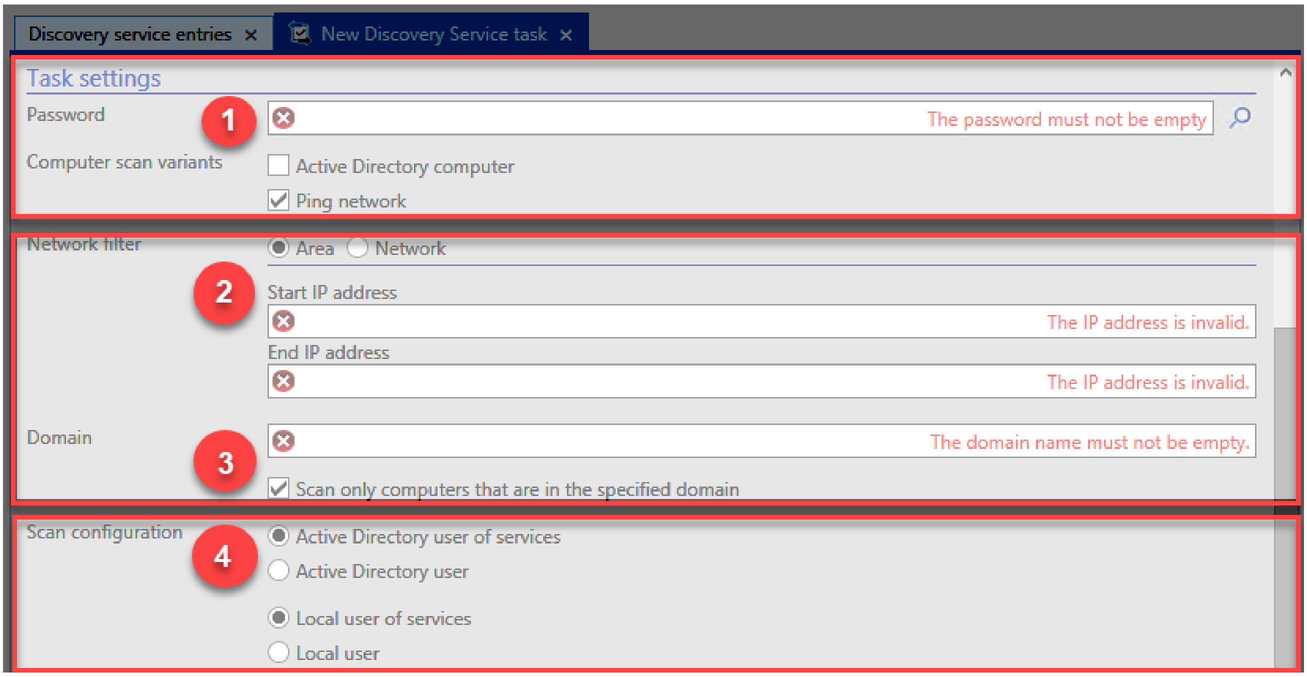
1. Shows information about the **Discovery Service Task**.
2. In the **General** section, the name of the **Discovery Service Task** is entered and a **Description** can also be added.
   The **Status** is always set to **Activated** by default but it can also be set to **Deactivated** in the configuration.

3. The **Overview** shows the activities of the **Discovery Service Task**:
   Last run: shows the date it was last run
   Next run: shows the date of the next run

Task settings

Password:
1. User name field: Type
2. Password field: Type
Multiple password field —> field 1. is used

This section is used for special entries for the **Discovery Service Task**. After it has been finished, the **Network Scan** scans the **network** according to these guidelines.



Task settings

Password: The password must not be empty

Computer scan variants: □ Active Directory computer ☑ Ping network

Network filter: ● Area ○ Network

Start IP address: The IP address is invalid.

End IP address: The IP address is invalid.

Domain: The domain name must not be empty.

☑ Scan only computers that are in the specified domain

Scan configuration: ● Active Directory user of services ○ Active Directory user ● Local user of services ○ Local user

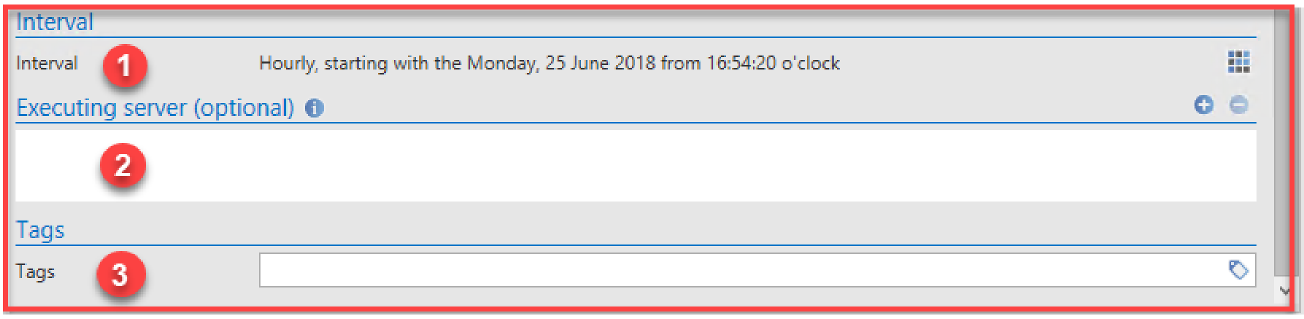
1. **Password** and **Computer scan variants:** The required password must already have been issued and it requires corresponding rights for the domain. This password has to be entered.
   Active Directory computer: Only those computers that are in Active Directory are scanned (there is also the option of using it individually or pinging the network)
   Ping network: A network filter for the configuration of the network is displayed
2. **Network filter**: This defines the network to be scanned either using an IP range or an IP network address.
   Range: The start IP address and end IP address for the range on the network are entered here.
   Network: The network address and corresponding subnet mask for the network are entered here.
3. **Domain:** The domain to be used for the **network scan** is entered here.
   In addition, you can select that only computers in the entered domain are scanned. A name resolution should work for this purpose.

4. **Scan configuration**:
   The Network Scan for the configuration of Active Directory is defined here. Select from either **Active Directory user of services** or **Active Directory user**.
   The second section defines the scan configuration for the local computer. Select from either **Local user of services** or * Local user*.

! The system executing the scan – on which the AdminClient is installed – is not scanned!

Interval / Executing server / Tags

This section is used to enter information about the start of the task and other additional information.



Interval

Interval: Hourly, starting with the Monday, 25 June 2018 from 16:54:20 o'clock

Executing server (optional)

Tags

Tags:

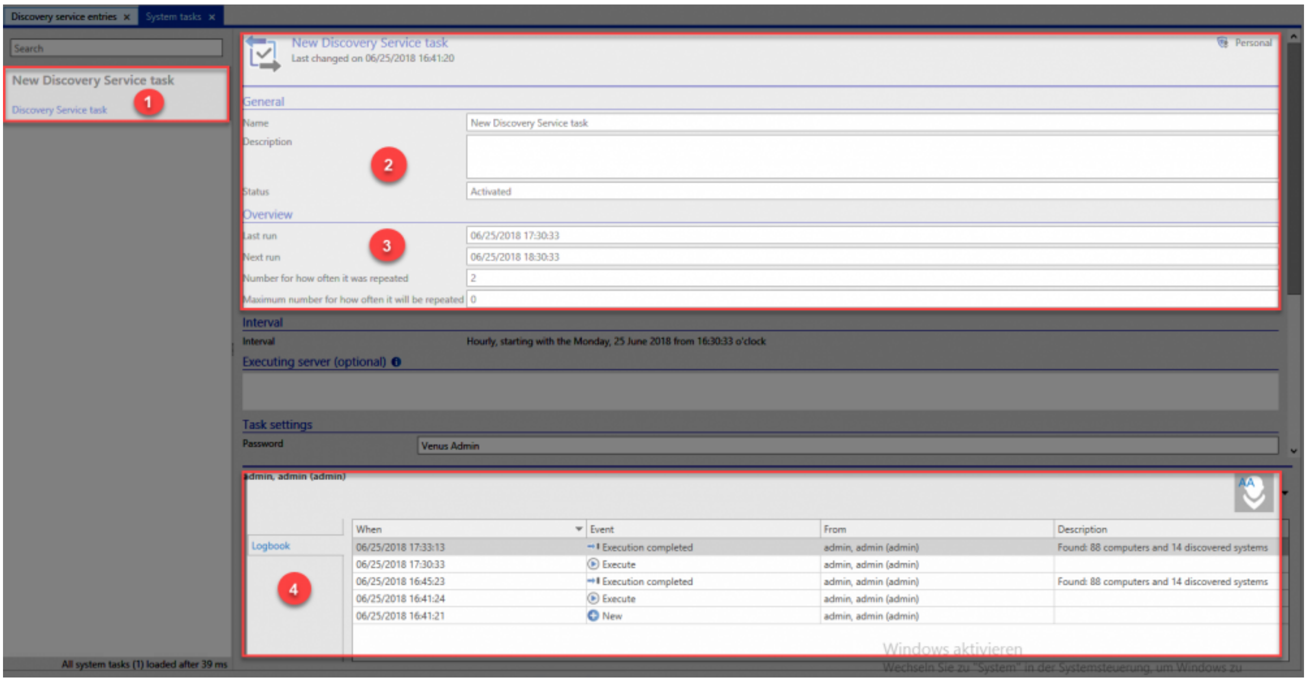
1. **Interval:** The interval at which the **Discovery Service Task** should be executed is defined here. The default setting is hourly, 1 year after adding the **Discovery Service Task**. The interval can be adjusted in minutes or set to be executed only once. It is also possible to enter an end date.
2. **Executing server (optional):** Servers with an **AdminClient** can be entered here that will be used to execute the **Discovery Service Task** if the main server crashes. The **Discovery Service Task** is then automatically taken over and executed by the accessible servers on the list. The list is searched from top to bottom to find an accessible server.
3. **Tags:** The use of tags is described in more detail in the section “tag manager”:#tags. A special tag can be entered here for the **Discovery Service Task**.

After the **Discovery Service Task** has been configured, a connection test is performed when the configuration is saved. It indicates whether the configuration is correct or faulty. Depending on the message, the **Discovery Service Task** may need to be amended.

! The **default setting** for the **Discovery Service Task** after it has been saved is **Activated**! It will **immediately actively scan** the network for data. This data is **read** but not amended!

Discovered entries

The entries for the **Discovery Service** are discovered using a **Discovery Service Task**. It can take some time for all the data on the systems for the entered IP network to be collected. This can be easily recognised by the **blue arrow** symbol on the **Discovery Service Task** and a corresponding message is also shown in the **General" display. Once the *Discovery Service Task** has been completed, the data will be shown in the **Discovery Service module**.


Discovery service entries ×
System tasks ×
Search
New Discovery Service task
Discovery Service task
1
2
3
4
Personal
All system tasks (1) loaded after 39 ms
Windows aktivieren
Wechseln Sie zu "System" in der Systemsteuerung, um Windows zu

New Discovery Service task
Last changed on 06/25/2018 16:41:20

General

Name: New Discovery Service task
Description:
Status: Activated

Overview

Last run: 06/25/2018 17:30:33
Next run: 06/25/2018 18:30:33
Number for how often it was repeated: 2
Maximum number for how often it will be repeated: 0

Interval

Interval: Hourly, starting with the Monday, 25 June 2018 from 16:30:33 o'clock

Executing server (optional)

Task settings

Password: Venus Admin

admin, admin (admin)

Logbook

When	Event	From	Description
06/25/2018 17:33:13	Execution completed	admin, admin (admin)	Found: 88 computers and 14 discovered systems
06/25/2018 17:30:33	Execute	admin, admin (admin)	
06/25/2018 16:45:23	Execution completed	admin, admin (admin)	Found: 88 computers and 14 discovered systems
06/25/2018 16:41:24	Execute	admin, admin (admin)	
06/25/2018 16:41:21	New	admin, admin (admin)	

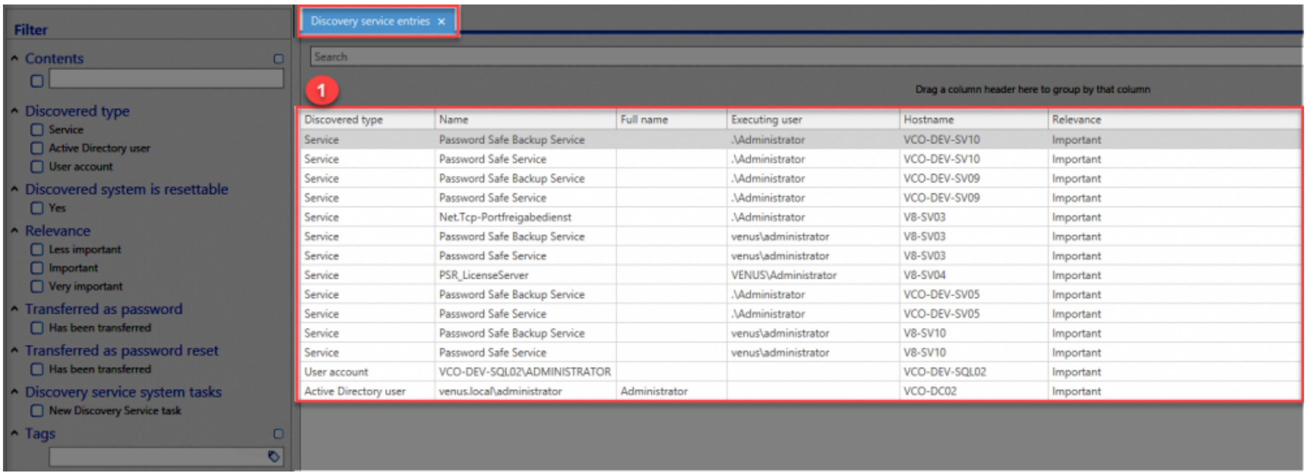
The **Discovery Service Task** needs to be carefully configured. The configurable sections are described below.

1. **Discovery Service Task**: Display of the status: this can be updated in the preview and logbook using the **F5 button**.
   Red hand: Deactivated
   Blue arrow: Activated and being executed
   Boxes: Corresponds to the assigned tag
2. **General:** The latest information about the **Discovery Service Task** is shown here. A **message** will be shown to indicate an active **Discovery Service Task**.
3. **Overview:** Current data for the **Discovery Service Task** about its progress and subsequent executions are shown here.
4. **Logbook:** The **logbook** can be found in the **footer** of the **Discovery Service Task**. The latest activities carried out by the **Discovery Service Task** are shown here.

The **data** is **not kept up-to-date while the task is being executed** and does not always show the latest status. Therefore, the data should be regularly **updated** using the **F5 button**!

Using the Discovery Service entries

The successful execution of a **Discovery Service Task** is a requirement for the **Discovery Service entries**. The discovered data is listed in table form in the **Discovery Service module** and can be correspondingly organised using the **Discovery Service System Task** filter.

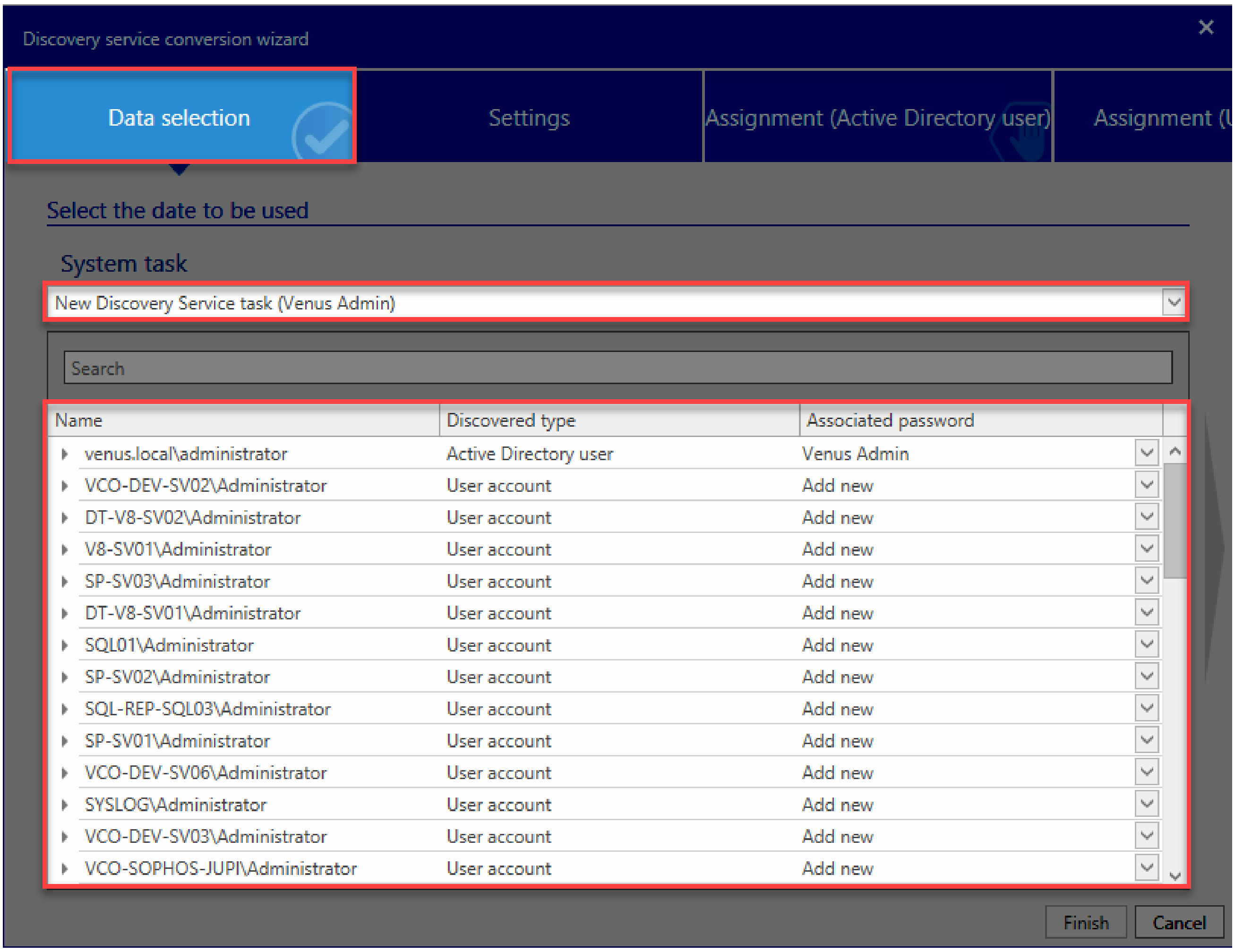

Filter
Contents
Discovered type
Service
Active Directory user
User account
Discovered system is resettable
Yes
Relevance
Less important
Important
Very important
Transferred as password
Has been transferred
Transferred as password reset
Has been transferred
Discovery service system tasks
New Discovery Service task
Tags
Discovery service entries ×
Search
1
Drag a column header here to group by that column

Discovered type	Name	Full name	Executing user	Hostname	Relevance
Service	Password Safe Backup Service		.\Administrator	VCO-DEV-SV10	Important
Service	Password Safe Service		.\Administrator	VCO-DEV-SV10	Important
Service	Password Safe Backup Service		.\Administrator	VCO-DEV-SV09	Important
Service	Password Safe Service		.\Administrator	VCO-DEV-SV09	Important
Service	Net.Tcp-Portfreigabedienst		.\Administrator	V8-SV03	Important
Service	Password Safe Backup Service		venus\administrator	V8-SV03	Important
Service	Password Safe Service		venus\administrator	V8-SV03	Important
Service	PSR_LicenseServer		VENUS\Administrator	V8-SV04	Important
Service	Password Safe Backup Service		.\Administrator	VCO-DEV-SV05	Important
Service	Password Safe Service		.\Administrator	VCO-DEV-SV05	Important
Service	Password Safe Backup Service		venus\administrator	V8-SV10	Important
Service	Password Safe Service		venus\administrator	V8-SV10	Important
User account	VCO-DEV-SQL02\ADMINISTRATOR			VCO-DEV-SQL02	Important
Active Directory user	venus.local\administrator	Administrator		VCO-DC02	Important

1. In this section, the **Discovery Service entries** that were discovered by the **Discovery Service Task** and selected for the **Conversion Wizard** are displayed.

Multiple selection of Discovery Service entries

If multiple entries are selected for a **Password Reset**, a corresponding number of **passwords** and **Password Resets** need to be added in the **Conversion Wizard**. Depending on the entries selected (service, Active Directory user, user account), it is necessary to carry out corresponding **assignments** in the **Conversion Wizard** for the **passwords**.



Discovery service conversion wizard
Data selection
Settings
Assignment (Active Directory user)
Assignment (U
Finish
Cancel

Select the date to be used

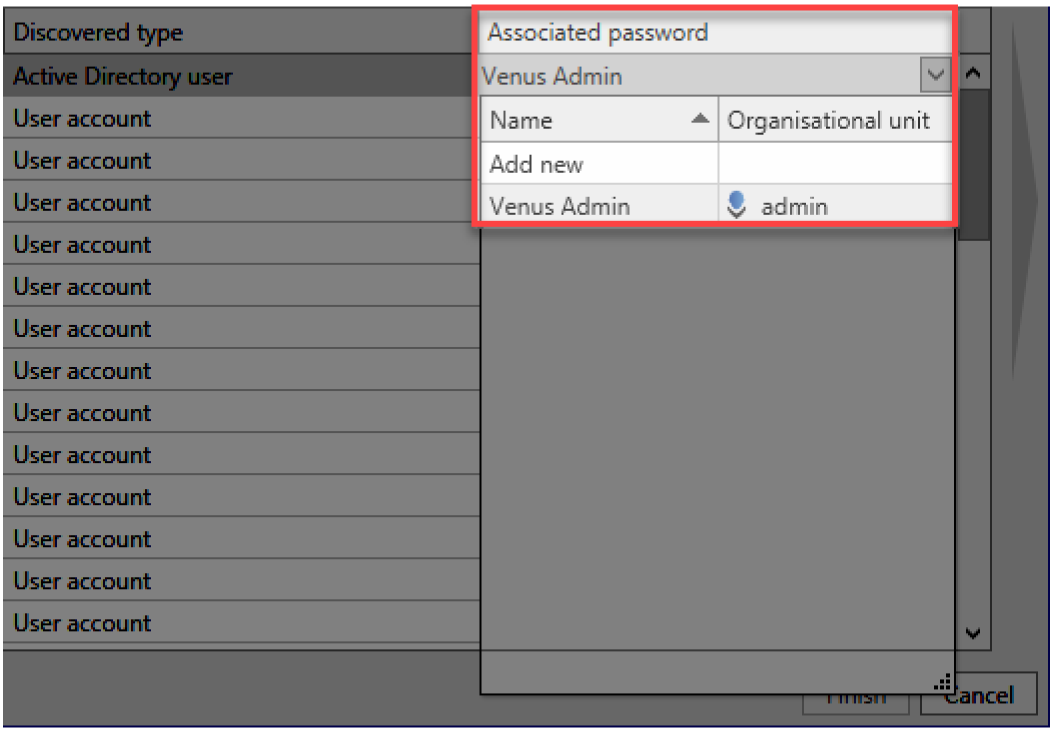
System task

New Discovery Service task (Venus Admin)

Search

Name	Discovered type	Associated password
venus.local\administrator	Active Directory user	Venus Admin
VCO-DEV-SV02\Administrator	User account	Add new
DT-V8-SV02\Administrator	User account	Add new
V8-SV01\Administrator	User account	Add new
SP-SV03\Administrator	User account	Add new
DT-V8-SV01\Administrator	User account	Add new
SQL01\Administrator	User account	Add new
SP-SV02\Administrator	User account	Add new
SQL-REP-SQL03\Administrator	User account	Add new
SP-SV01\Administrator	User account	Add new
VCO-DEV-SV06\Administrator	User account	Add new
SYSLOG\Administrator	User account	Add new
VCO-DEV-SV03\Administrator	User account	Add new
VCO-SOPHOS-JUPI\Administrator	User account	Add new

Every line must be connected to a **password** in the end. Therefore, it is necessary to carry out an assignment process in the **Conversion Wizard** for every entry.



Discovered type	Associated password
Active Directory user	Venus Admin
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	
User account	

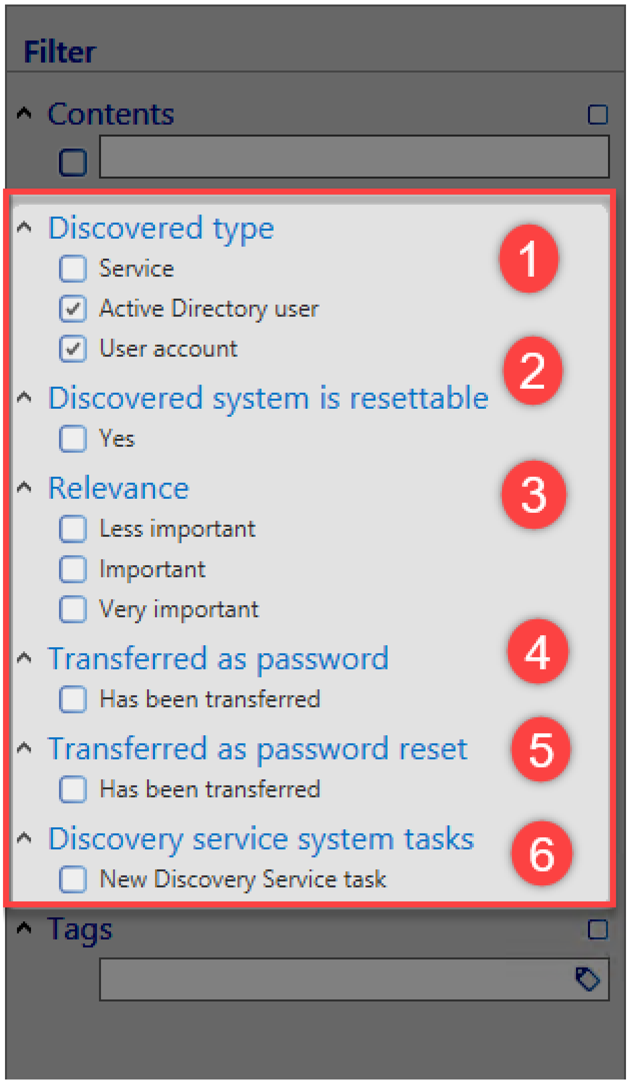
Name	Organisational unit
Add new	
Venus Admin	admin

For **Active Directory users**, it is possible to assign an existing **password**.

The subsequent process is carried out in the same way as when only one **Discovery Service entry** is selected.

Filter settings

A good filter is required for processing the discovered data. A **filter that has been adapted for this purpose** is available for processing the entries in the **Discovery Service module**. The options in the **filter** are described below:



Filter

Contents □

□

Discovered type
□ Service
☑ Active Directory user
☑ User account

Discovered system is resettable
□ Yes

Relevance
□ Less important
□ Important
□ Very important

Transferred as password
□ Has been transferred

Transferred as password reset
□ Has been transferred

Discovery service system tasks
□ New Discovery Service task

Tags □

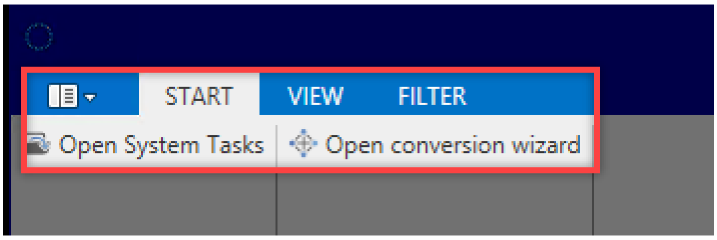
Description of the **filter with the special options for the Discovery Service entries:**

1. **Discovered type** The discovered entries can be filtered here according to their type.
2. **Discovered system is resettable:** Indicates whether a Password Reset can be created from the discovered data.
3. **Relevance:** Grading the importance of the discovered system.
   A high relevance means that multiple services have been discovered for an Active Directory user or user account.
   Less important: Exactly one service was found
   Important: Two to nine services were found
   Very important: 10 or more services were found
   If a Password Reset has already been created, the relevance is downgraded to less important.
4. **Transferred as password:** Indicates whether a password can be created via the Conversion Wizard
5. **Transferred as Password Reset:** Indicates whether a Password Reset can be created via the Conversion Wizard

6. **Discovery service system tasks:** The entries are filtered here based on the System Task.

Converting entries

An important element for the **Discovery Service** is the **Conversion Wizard**. It processes the discovered **entries** and then creates corresponding **passwords and Password Resets**.
The **Conversion Wizard** is started in the Start ribbon and it is also possible to switch here to the **System Tasks**.



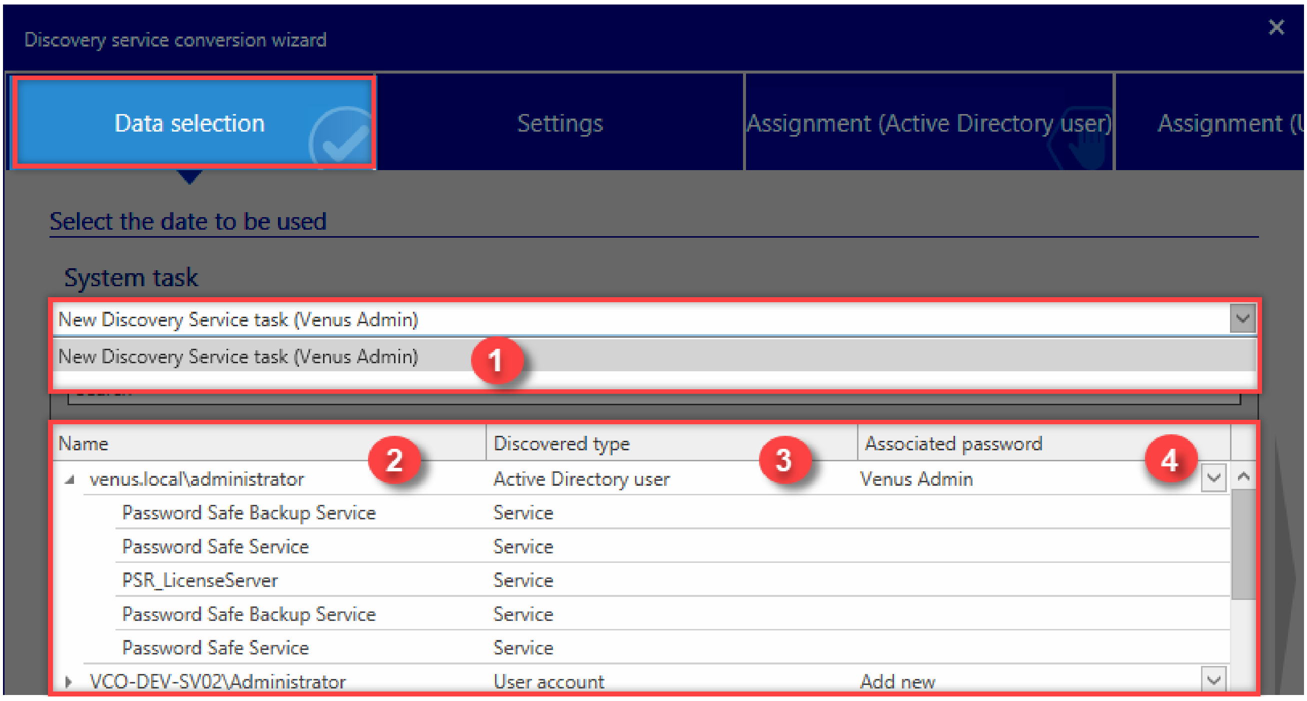
After the **Discovery Service Task** has been successfully executed, the entries are available in the **Discovery Service**. Further processing of the entries is then carried out using the **Conversion Wizard**.
For processing in the **Conversion Wizard**, the network is scanned for the following types:

1. Discovered type: Service
2. Discovered type: Active Directory user
3. Discovered type: User account

Only those **services are recorded** to which at least one **AD user** or **user account** can be assigned! Only **AD users** and **user accounts** to which **at least one service** can be assigned are recorded.

Execution

In the **Discovery Service** table, the user selects the entries for which he wants to add a **Password Reset** or **password**. The user then clicks on the **Conversion Wizard** and the **Discovery Service Cinversion Wizard** opens for further editing.


Discovery service conversion wizard
Data selection
Settings
Assignment (Active Directory user)
Assignment (U
1
2
3
4

Select the date to be used

System task

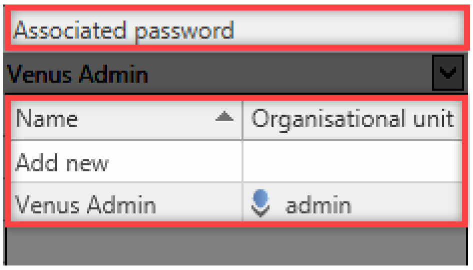
New Discovery Service task (Venus Admin)

Name	Discovered type	Associated password
venus.local\administrator	Active Directory user	Venus Admin
Password Safe Backup Service	Service	
Password Safe Service	Service	
PSR_LicenseServer	Service	
Password Safe Backup Service	Service	
Password Safe Service	Service	
VCO-DEV-SV02\Administrator	User account	Add new

1. A **Discovery Service Task** first needs to be selected. This determines the context in which the new data will be created (for a new **Password Reset**, the **password for the domain administrator** for the task will be used as the executing user. In addition, only those **Discovery Service Task entries** that are also discovered by the entered **Discovery Service Task** will be used for the conversion).
2. The discovered entries will be displayed in this column with the **services** for which the user has been entered.
3. This column shows the **discovered type** for the entry.
4. This column shows already existing passwords in Password Safe that match the discovered **Active Directory user** or **user account**. It is possible to select here which password can be used when creating a **Password Reset** (it is then used as the only password linked to the Password Reset). Alternatively, these passwords can also be newly created.

Logically, **every root node** corresponds to **one user** and all of its associated data (e.g. services). A **Password Reset** is created later for **every user** and its associated data.

The following image shows the options **add new password** or retain **existing password**.


Associated password

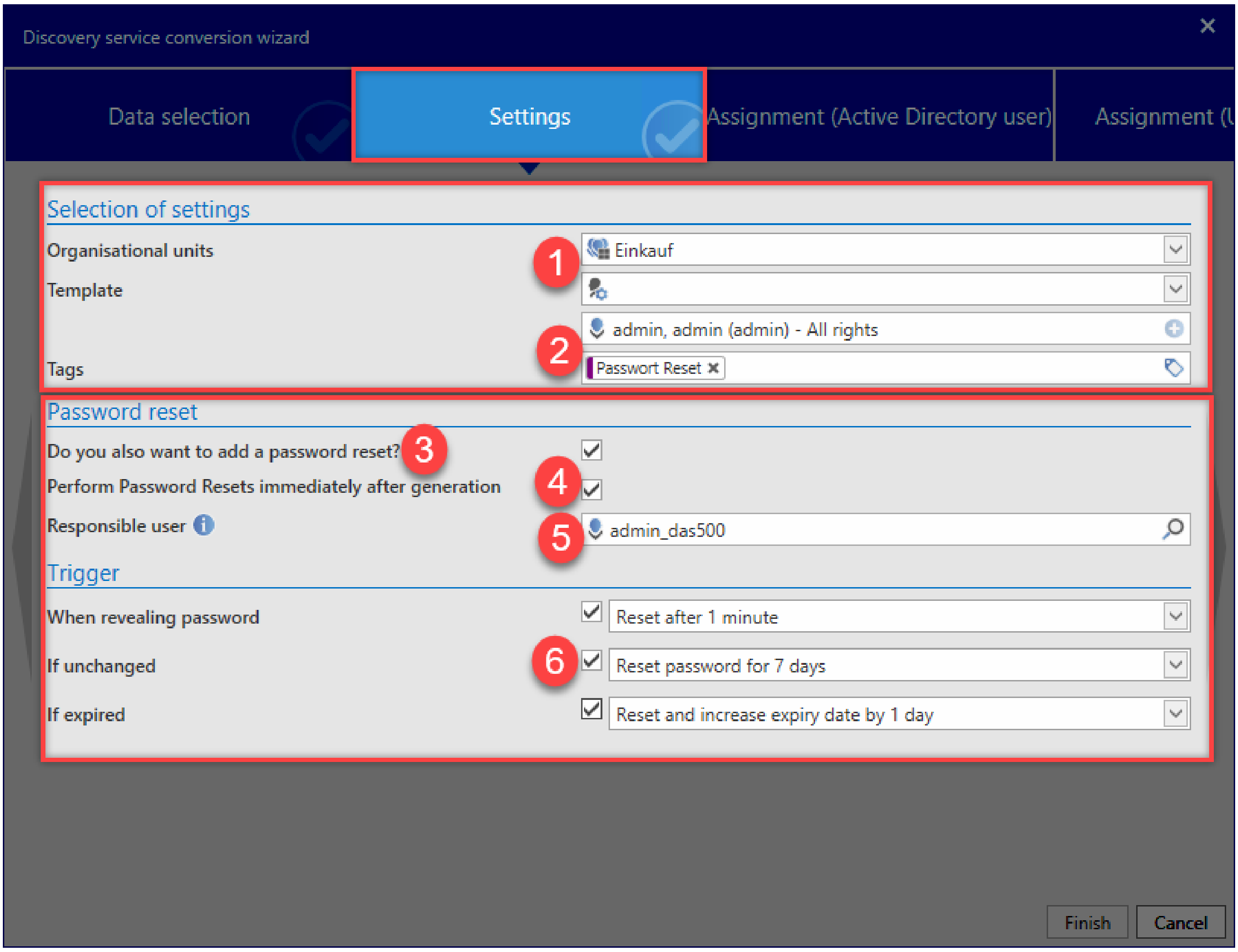
Venus Admin

Name	Organisational unit
Add new	
Venus Admin	admin

In addition, the **organisational unit** in which the existing password is located is displayed.

Settings

The **Password Reset** is configured in the **Settings** Ribbon.


Discovery service conversion wizard
Data selection
Settings
Assignment (Active Directory user)
Assignment (U
1
2
3
4
5
6
Finish
Cancel

Selection of settings

Organisational units: Einkauf

Template:

admin, admin (admin) - All rights

Tags: Passwort Reset

Password reset

Do you also want to add a password reset? ☑

Perform Password Resets immediately after generation ☑

Responsible user: admin_das500

Trigger

When revealing password ☑ Reset after 1 minute

If unchanged ☑ Reset password for 7 days

If expired ☑ Reset and increase expiry date by 1 day

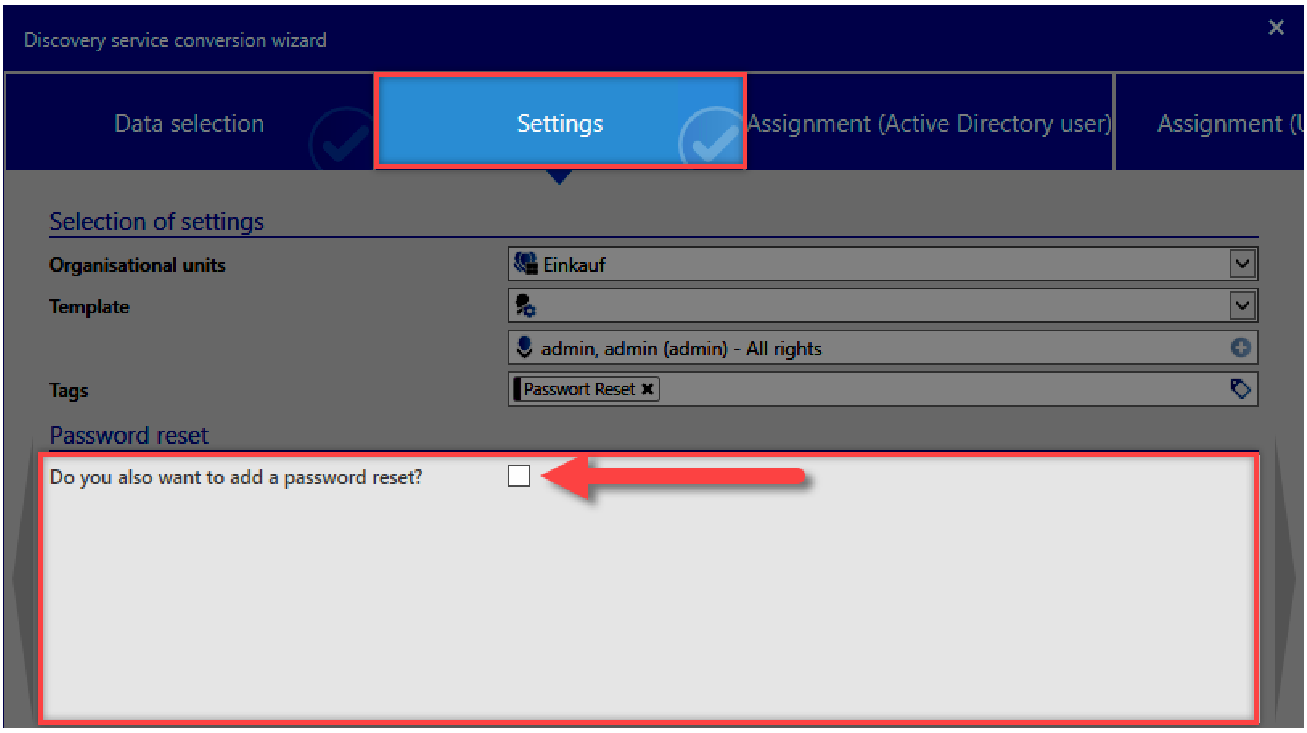
The **settings** will be described in more detail below:

1. The organisational unit in which the **Password Reset** should be created is entered here. In addition, a template for the rights inheritance can be entered here.
2. The **responsible user** for the **password** is entered here. A special **tag** can be set here.
3. Adding a **Password Reset**
   Option 1: **Do you also want to add a Password Reset?** Adds a* Password Reset* If **option 1** is not selected, the following options are not displayed.
4. Setting for executing a **Password Reset**
   Option 2: **(Execute Password Resets immediately after they are created)** means that the **Password Reset** will be executed as soon as you click on **Finish**.
5. The **responsible user for the Password Reset** is entered here.

6. Various **triggers for the Password Reset** can be selected here.

> ! After clicking on **Finish**, the **Password Resets** will be **immediately executed** and the **passwords changed!**. This also applies to **Windows passwords!**

If option 1: **Do you also want to add a Password Reset?** is not selected, *steps 4, 5 and 6 are not displayed for configuration.


Discovery service conversion wizard
×
Data selection
Settings
Assignment (Active Directory user)
Assignment (

Selection of settings

Organisational units: Einkauf

Template:

admin, admin (admin) - All rights

Tags: Passwort Reset ✖

Password reset

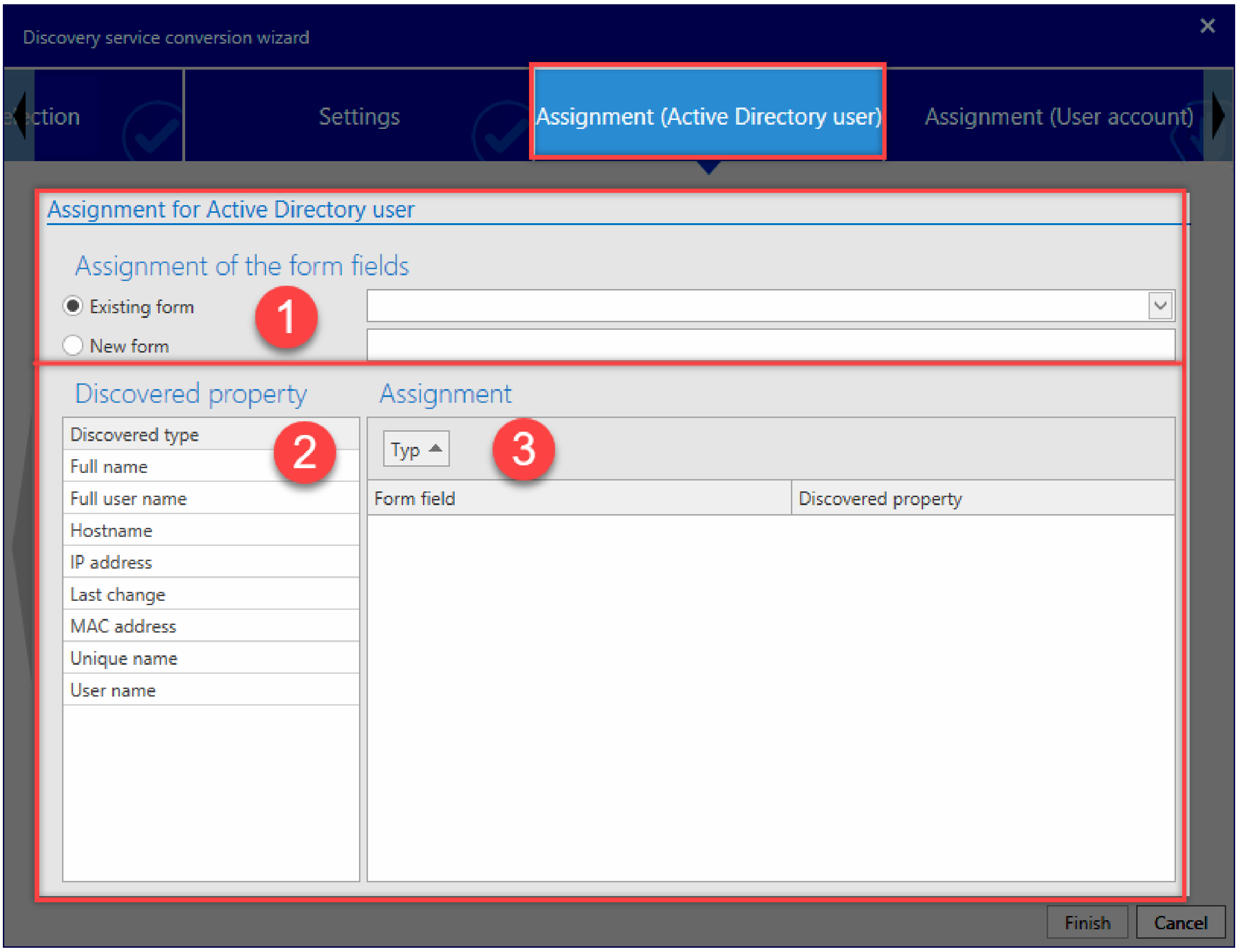
Do you also want to add a password reset? □

> ! After clicking on **Finish**, one or more **passwords will be created** but **no corresponding Password Resets will be created!**

Assignment (Active Directory user)

In the **Assignment (Active Directory user)** Ribbon, the discovered data for the **Discovery Service entries** is transferred to a password form.

The following images shows the **Assignment (Active Directory user)** Ribbon



Discovery service conversion wizard

Assignment for Active Directory user

Assignment of the form fields

● Existing form

○ New form

Discovered property

Discovered type
Full name
Full user name
Hostname
IP address
Last change
MAC address
Unique name
User name

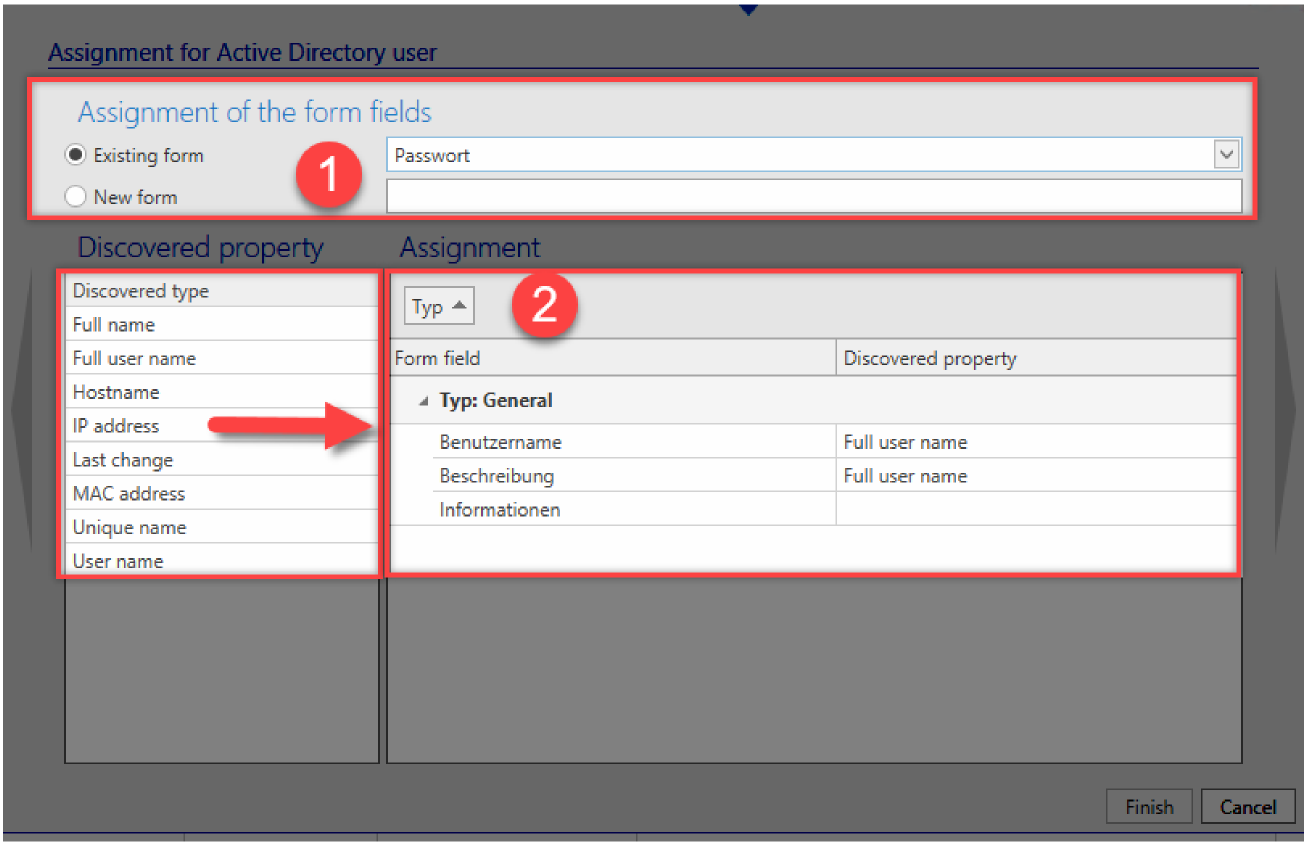
Assignment

Form field	Discovered property

Description

1. An **Existing form** can be selected or a **New form** with names can be added
2. The **discovered properties** are displayed here
3. The **properties** are *assigned to the form fields here

“Existing form” selected



Assignment for Active Directory user

Assignment of the form fields

● Existing form: Passwort

○ New form

Discovered property
Discovered type
Full name
Full user name
Hostname
IP address
Last change
MAC address
Unique name
User name

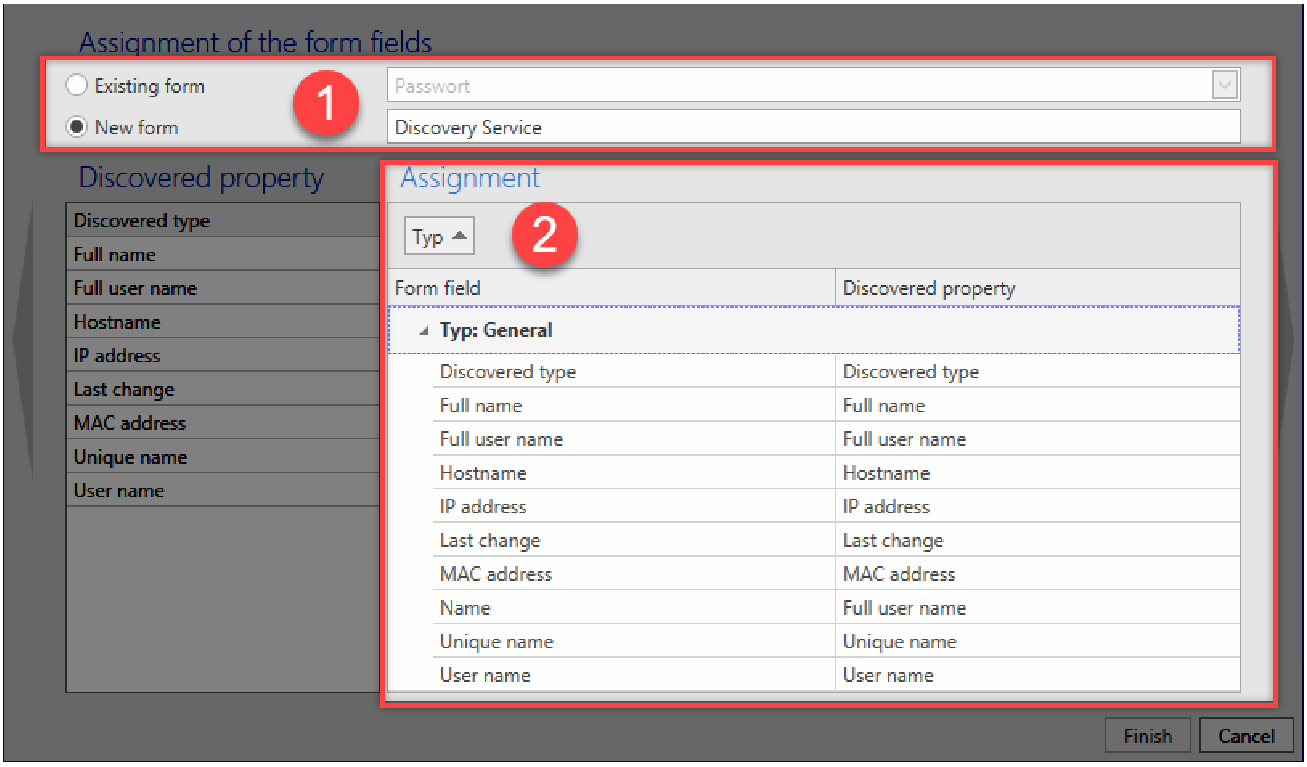
Assignment

Form field	Discovered property
Typ: General	
Benutzername	Full user name
Beschreibung	Full user name
Informationen	

Procedure:

1. An **Existing form** is selected here
2. The **assignment** to the fields is carried out here
   Important assignments are **Type: General** and **Type: Password Reset**. An amendment can be carried out here

“New form” selected



Assignment of the form fields

○ Existing form — Passwort

● New form — Discovery Service

Discovered property

- Discovered type
- Full name
- Full user name
- Hostname
- IP address
- Last change
- MAC address
- Unique name
- User name

Assignment

Typ ▲

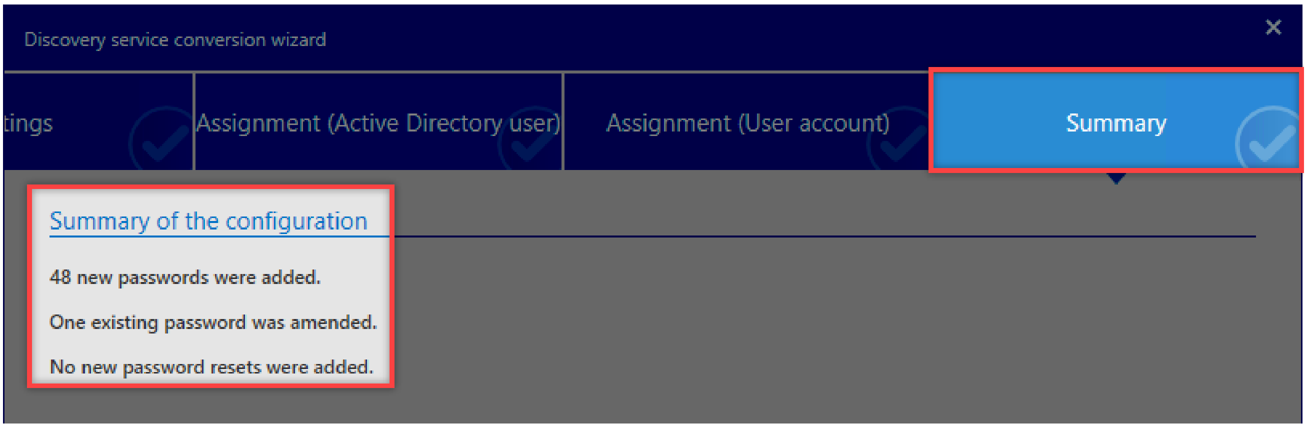
Form field	Discovered property
Typ: General	
Discovered type	Discovered type
Full name	Full name
Full user name	Full user name
Hostname	Hostname
IP address	IP address
Last change	Last change
MAC address	MAC address
Name	Full user name
Unique name	Unique name
User name	User name

Procedure:

1. A name for the **New form** needs to be entered here
2. The discovered entries are **automatically** assigned as standard
   Important assignments are **Type: General** and **Type: Password Reset**. An amendment can be carried out here

Summary

A brief overview of the actions that will be carried out with the added configuration is displayed in the **Summary** Ribbon. These actions will then be carried out if you click on **Finish**.



Discovery service conversion wizard

Summary of the configuration

48 new passwords were added.

One existing password was amended.

No new password resets were added.

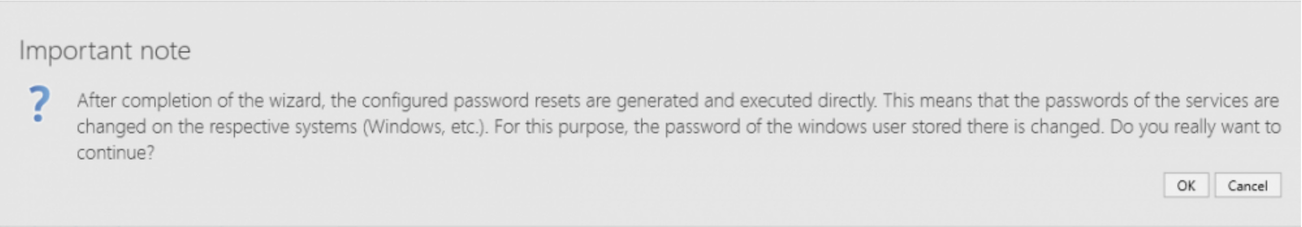
Confirmation prompt

An important aspect of **Password Safe V8** is the **security** of passwords on systems. In the **Discovery Service**, a **security measures** is thus triggered at the **last step** for creating **Password Resets**.
If the option **Execute Password Resets immediately after they are created** is used in the configuration, the **selected passwords** are immediately changed after clicking on **Finish**. If you are *not paying careful attention, this could have inconvenient consequences.

Security level 1:
An **Important note** is displayed in the **Summary** after clicking on **Finish**.

! **Please observe the note and read it through carefully!**

An **Overview** of which actions will be carried out is displayed for the user together with this **note**. The user can then still decide to **Cancel** the process.
If you click on **OK**, an **additional confirmation warning** will be displayed.



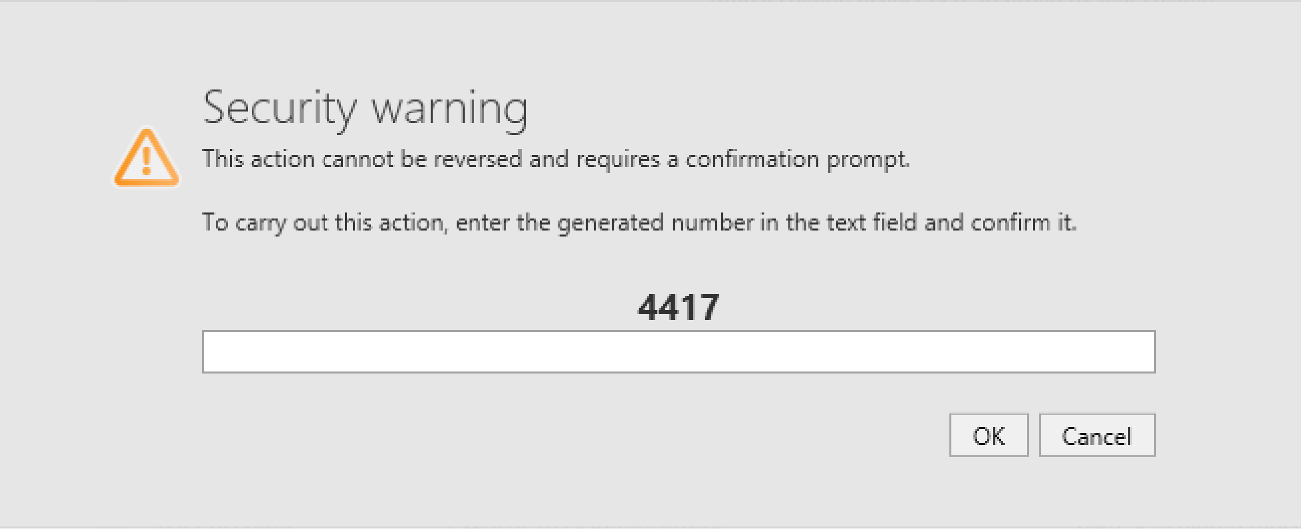
Important note

After completion of the wizard, the configured password resets are generated and executed directly. This means that the passwords of the services are changed on the respective systems (Windows, etc.). For this purpose, the password of the windows user stored there is changed. Do you really want to continue?

Security level 2:

Another **confirmation prompt** highlights that it is important to understand what you are about to do. It will no longer be possible to reverse the actions afterwards!

! **Last chance to cancel the execution!**



Security warning

This action cannot be reversed and requires a confirmation prompt.

To carry out this action, enter the generated number in the text field and confirm it.

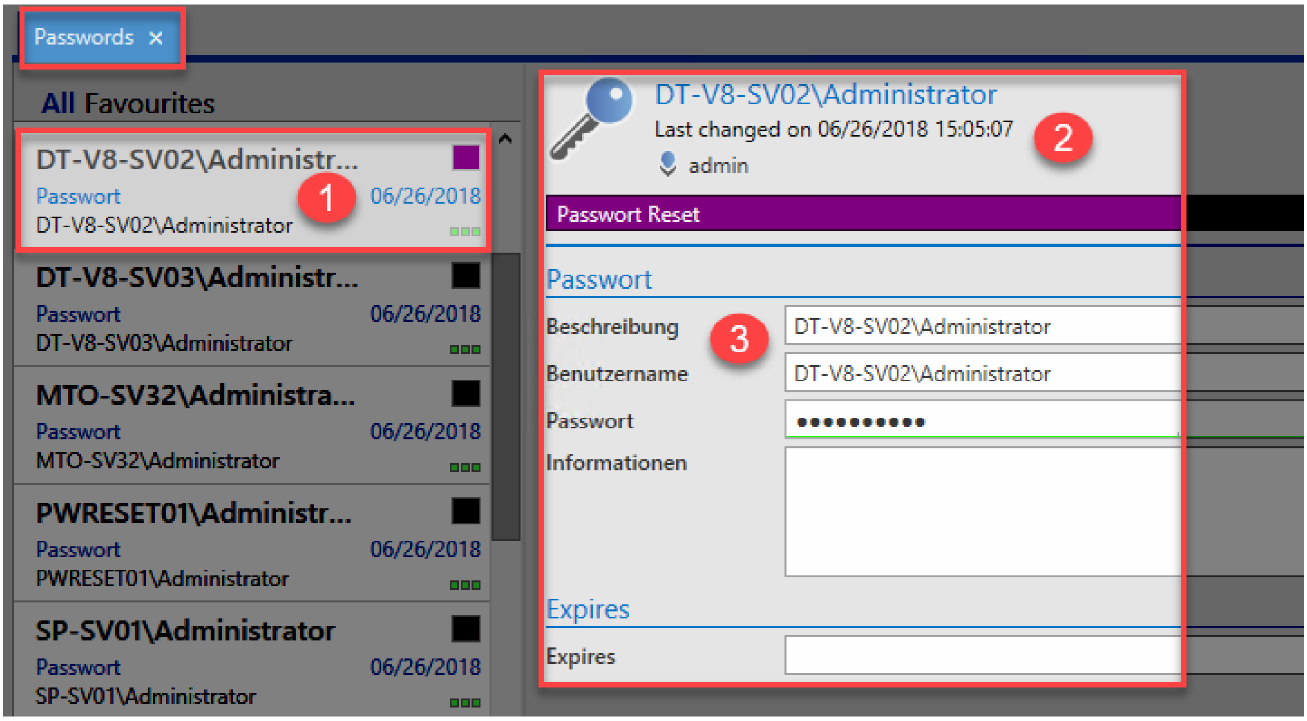
4417

After **entering the displayed number** and **confirming with OK**, the process is **executed immediately** and the **Password Resets** are carried out and the **associated passwords changed**.

Created passwords

After clicking on **Finish**, the **passwords** and the **Password Resets** (in accordance with the selected options) are created for the entries.
A **password** and a **Password Reset** are explained in the following example.

Password



DT-V8-SV02\Administr... Passwort 06/26/2018 DT-V8-SV02\Administrator

DT-V8-SV03\Administr... Passwort 06/26/2018 DT-V8-SV03\Administrator

MTO-SV32\Administra... Passwort 06/26/2018 MTO-SV32\Administrator

PWRESET01\Administr... Passwort 06/26/2018 PWRESET01\Administrator

SP-SV01\Administrator Passwort 06/26/2018 SP-SV01\Administrator

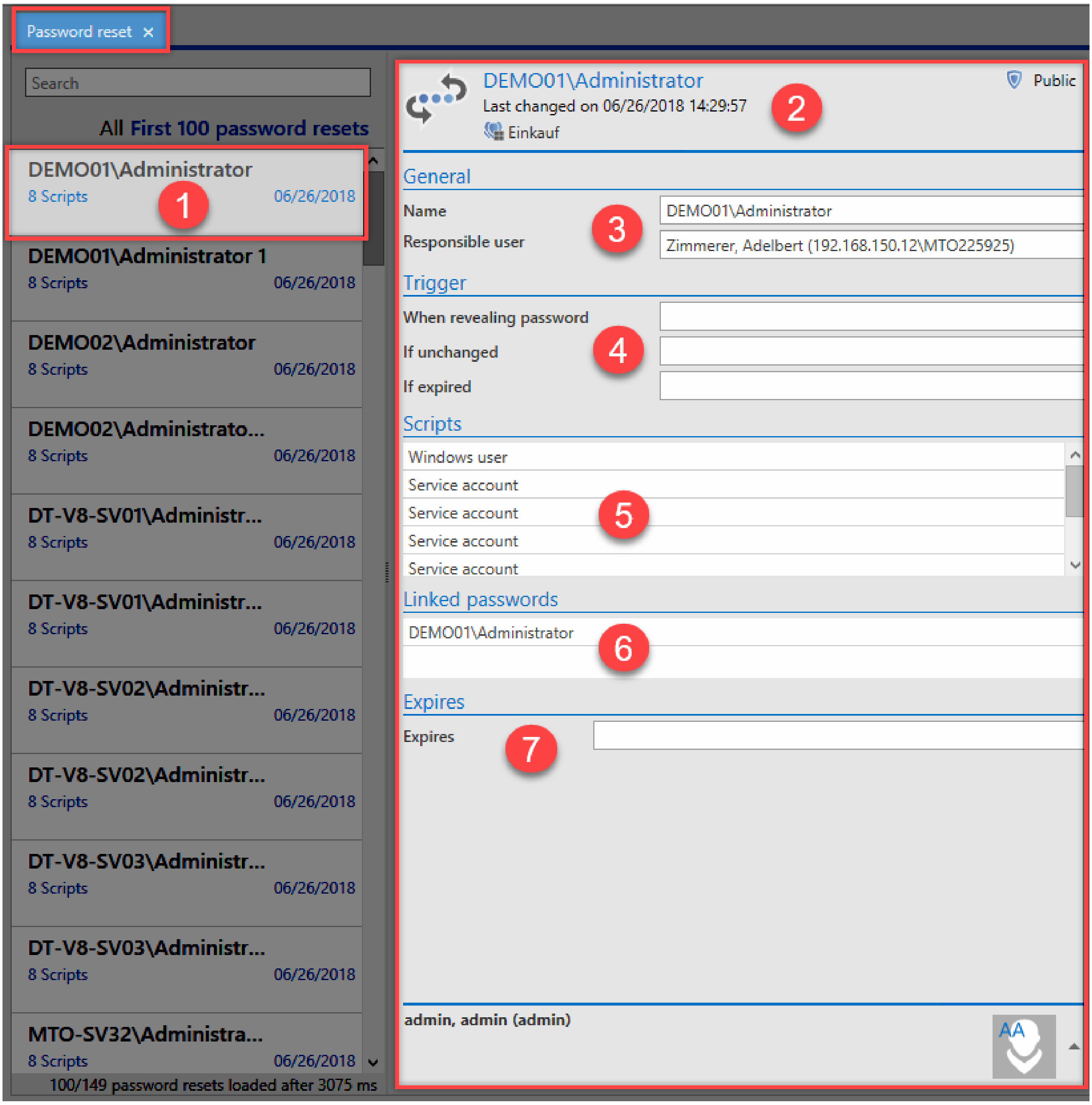
DT-V8-SV02\Administrator
Last changed on 06/26/2018 15:05:07
admin

Beschreibung: DT-V8-SV02\Administrator
Benutzername: DT-V8-SV02\Administrator
Passwort: ●●●●●●●●●●
Informationen:
Expires:

1. The name of the created password
2. General data about the password
3. Data about the password created from the form (existing or new)

Password Reset

Another password is created in the **Password Reset module** and is required for an associated Password Reset.



DEMO01\Administrator	8 Scripts	06/26/2018
DEMO01\Administrator 1	8 Scripts	06/26/2018
DEMO02\Administrator	8 Scripts	06/26/2018
DEMO02\Administrato...	8 Scripts	06/26/2018
DT-V8-SV01\Administr...	8 Scripts	06/26/2018
DT-V8-SV01\Administr...	8 Scripts	06/26/2018
DT-V8-SV02\Administr...	8 Scripts	06/26/2018
DT-V8-SV02\Administr...	8 Scripts	06/26/2018
DT-V8-SV03\Administr...	8 Scripts	06/26/2018
DT-V8-SV03\Administr...	8 Scripts	06/26/2018
MTO-SV32\Administra...	8 Scripts	06/26/2018

100/149 password resets loaded after 3075 ms

DEMO01\Administrator
Last changed on 06/26/2018 14:29:57
Einkauf

General

Name: DEMO01\Administrator
Responsible user: Zimmerer, Adelbert (192.168.150.12\MTO225925)

Trigger

When revealing password:
If unchanged:
If expired:

Scripts

Windows user
Service account
Service account
Service account
Service account

Linked passwords

DEMO01\Administrator

Expires

Expires:

admin, admin (admin)

Points 1-7 are described below:

1. The name of the Password Reset
2. Overview of the password
3. General
4. The data for the trigger are displayed here
5. The scripts for the passwords to be changed are displayed here
6. The associated password that will be reset using the Password Reset
7. The validity is shown here (if one has been entered)

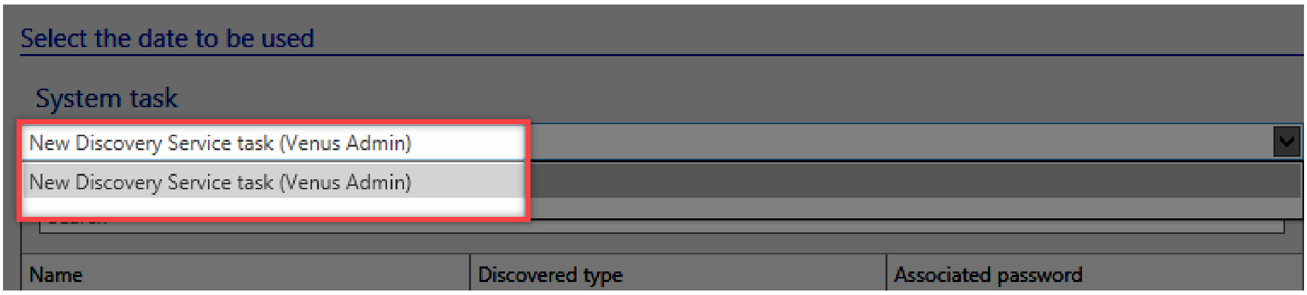
This data can then be used to create a **Password Reset** for the user for the discovered **Discovery Service entry**.
The **Password Reset** is activated via the corresponding trigger that has been set.

Deleting entries

After creating an automatic **Password Reset** via the **Conversion Wizard**, the data is no longer required and can be deleted. The discovered entries have a **link** to the relevant **Discovery Service Task** that was executed and can be found and displayed using the filter function.

Deletion process

The discovered data in the **Discovery Service** cannot simply be deleted and removed from the **Discovery Service entries**. As the entries have a **link to the Discovery Service Task**, it is necessary to delete the discovered entries via the **Discovery Service Task that was created**. If entries were discovered using a joint Discovery Service Task, it is not possible to simply delete them. This is the case if two different users have carried out a scan on the same area. If you delete one of the two **Discovery Service Task**, only the entries that had a single link to this **Discovery Service Task** will be deleted. The entries for the other **Discovery Service Task** will be retained and must be deleted via the associated **Discovery Service Task**.
You can find out which **Discovery Service Task** found a particular entry by selecting the entry via the **Conversion Wizard**.


Select the date to be used

System task

New Discovery Service task (Venus Admin)

New Discovery Service task (Venus Admin)

Name	Discovered type	Associated password

Deleting entries by changing the settings in the System Task

If the IP range for an existing **Discovery Service Task is changed and the *Discovery Service Task is then executed for this new IP range, the previously discovered entries from the previous executed *Discovery Service Task** will be deleted from the **Discovery Service**. If you want to carry out a **Discovery Service Task** for a different IP range, you should create a new **Discovery Service Task**. This will prevent any already discovered entries from being deleted. However, if the existing entries are no longer required, you can delete them by using the same **Discovery Service Task** with a different IP range.

1. Task B only scans the IP address: 192.168.150.1
2. Only the entries for the IP address 192.168.150.1 are discovered
3. Task A is changed and now scans the IP address:192.168.150.2
4. Result:

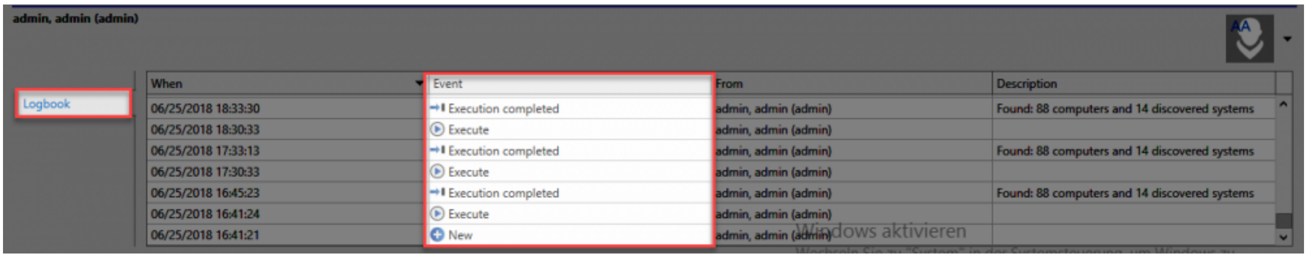
5. Only the entries from the IP address 192.168.150.2 are discovered
6. Entries for IP address 192.168.150.1 are deleted
7. Exception:
8. Task B scans the IP address: 192.168.150.1
9. The same entries for IP address 192.168.150.1 are discovered as for 1.
10. A new scan using Task A with a different IP address 192.168.150.2 will not delete the data from Task B

✻ The **Password Resets** and **passwords** created using the **Conversion Wizard** are not deleted when the **Discovery Service Tasks** are deleted.

Logbook

The **logbook in the footer** of the **Discovery Service Task** is extremely helpful for checking the **Discovery Service Task**. Information about the progress of the **Discovery Service Task** is displayed here. The data is displayed both in the **footer** and also in the **logbook module** (although in more detail here). To display the footer, the user requires the **user right**: #globale-einstellungen in the user settings in the **category: Footer area: Show logbook in the footer area (activated)**

Show in footer



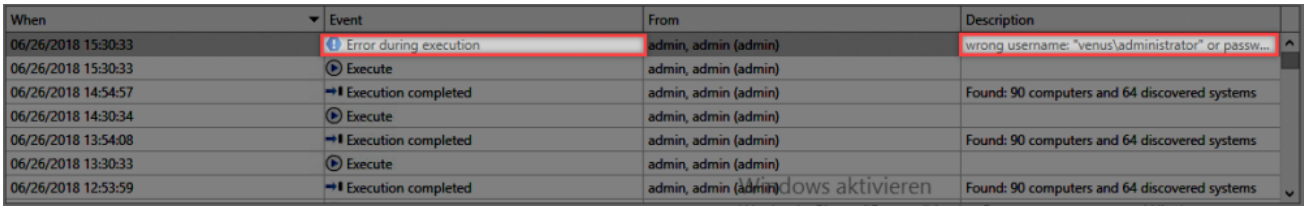
admin, admin (admin)

When	Event	From	Description
06/25/2018 18:33:30	Execution completed	admin, admin (admin)	Found: 88 computers and 14 discovered systems
06/25/2018 18:30:33	Execute	admin, admin (admin)	
06/25/2018 17:33:13	Execution completed	admin, admin (admin)	Found: 88 computers and 14 discovered systems
06/25/2018 17:30:33	Execute	admin, admin (admin)	
06/25/2018 16:45:23	Execution completed	admin, admin (admin)	Found: 88 computers and 14 discovered systems
06/25/2018 16:41:24	Execute	admin, admin (admin)	
06/25/2018 16:41:21	New	admin, admin (admin)	

The following **events** are displayed in the **logbook for the footer** and in the **logbook module**:

1. New
2. Change
3. Execute
4. Execution completed
5. Error during execution

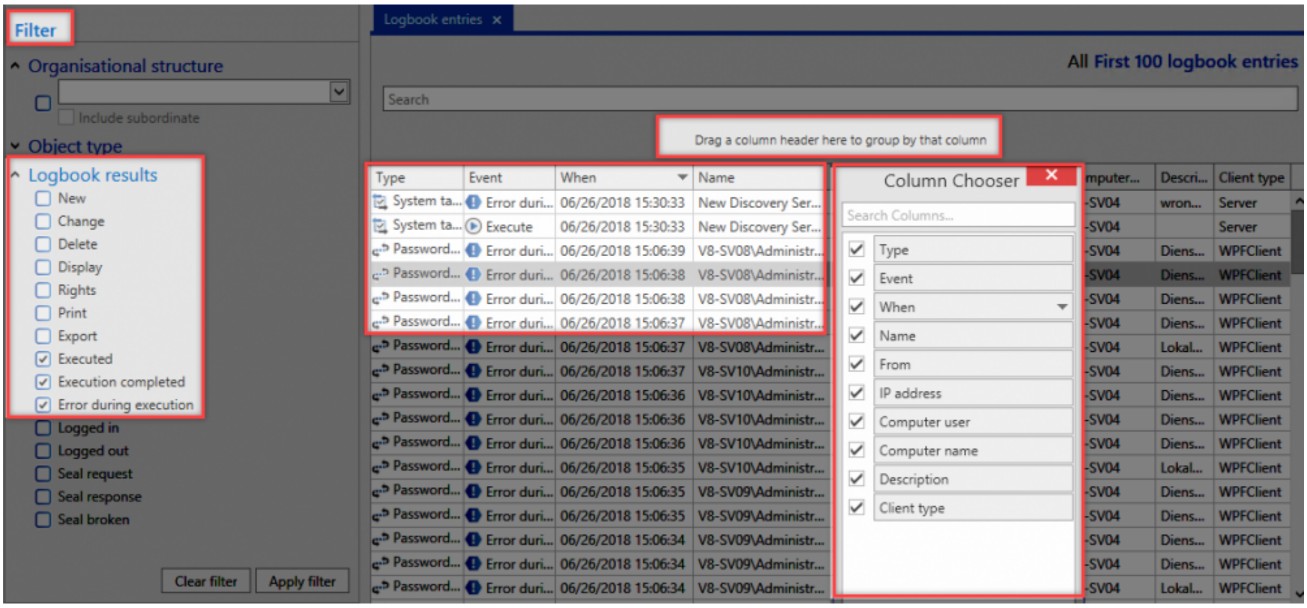
If an error occurs during the execution of the **Discovery Service Task**, this is also shown n the **logbook for the footer** with **additional information** about the error.



When	Event	From	Description
06/26/2018 15:30:33	Error during execution	admin, admin (admin)	wrong username: "venus\administrator" or passw...
06/26/2018 15:30:33	Execute	admin, admin (admin)	
06/26/2018 14:54:57	Execution completed	admin, admin (admin)	Found: 90 computers and 64 discovered systems
06/26/2018 14:30:34	Execute	admin, admin (admin)	
06/26/2018 13:54:08	Execution completed	admin, admin (admin)	Found: 90 computers and 64 discovered systems
06/26/2018 13:30:33	Execute	admin, admin (admin)	
06/26/2018 12:53:59	Execution completed	admin, admin (admin)	Found: 90 computers and 64 discovered systems

Display in the logbook

In general, the **logbook module** displays more detailed information about the **Discovery Service Task**. The “filter” can be used to select which data is displayed: #filter. The same **events** as for the footer for the **Discovery Service Task** are also used here.



Filter

Organisational structure

□

□ Include subordinate

Object type

Logbook results

□ New
□ Change
□ Delete
□ Display
□ Rights
□ Print
□ Export
☑ Executed
☑ Execution completed
☑ Error during execution
□ Logged in
□ Logged out
□ Seal request
□ Seal response
□ Seal broken

Clear filter | Apply filter

Logbook entries

All First 100 logbook entries

Search

Drag a column header here to group by that column

Type	Event	When	Name	mputer...	Descri...	Client type
System ta...	Error duri...	06/26/2018 15:30:33	New Discovery Ser...	-SV04	wron...	Server
System ta...	Execute	06/26/2018 15:30:33	New Discovery Ser...	-SV04		Server
Password...	Error duri...	06/26/2018 15:06:39	V8-SV08\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:38	V8-SV08\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:38	V8-SV08\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:37	V8-SV08\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:37	V8-SV08\Administr...	-SV04	Lokal...	WPFClient
Password...	Error duri...	06/26/2018 15:06:37	V8-SV10\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:36	V8-SV10\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:36	V8-SV10\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:36	V8-SV10\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:35	V8-SV10\Administr...	-SV04	Lokal...	WPFClient
Password...	Error duri...	06/26/2018 15:06:35	V8-SV09\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:35	V8-SV09\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:34	V8-SV09\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:34	V8-SV09\Administr...	-SV04	Diens...	WPFClient
Password...	Error duri...	06/26/2018 15:06:34	V8-SV09\Administr...	-SV04	Lokal...	WPFClient

Column Chooser

Search Columns...

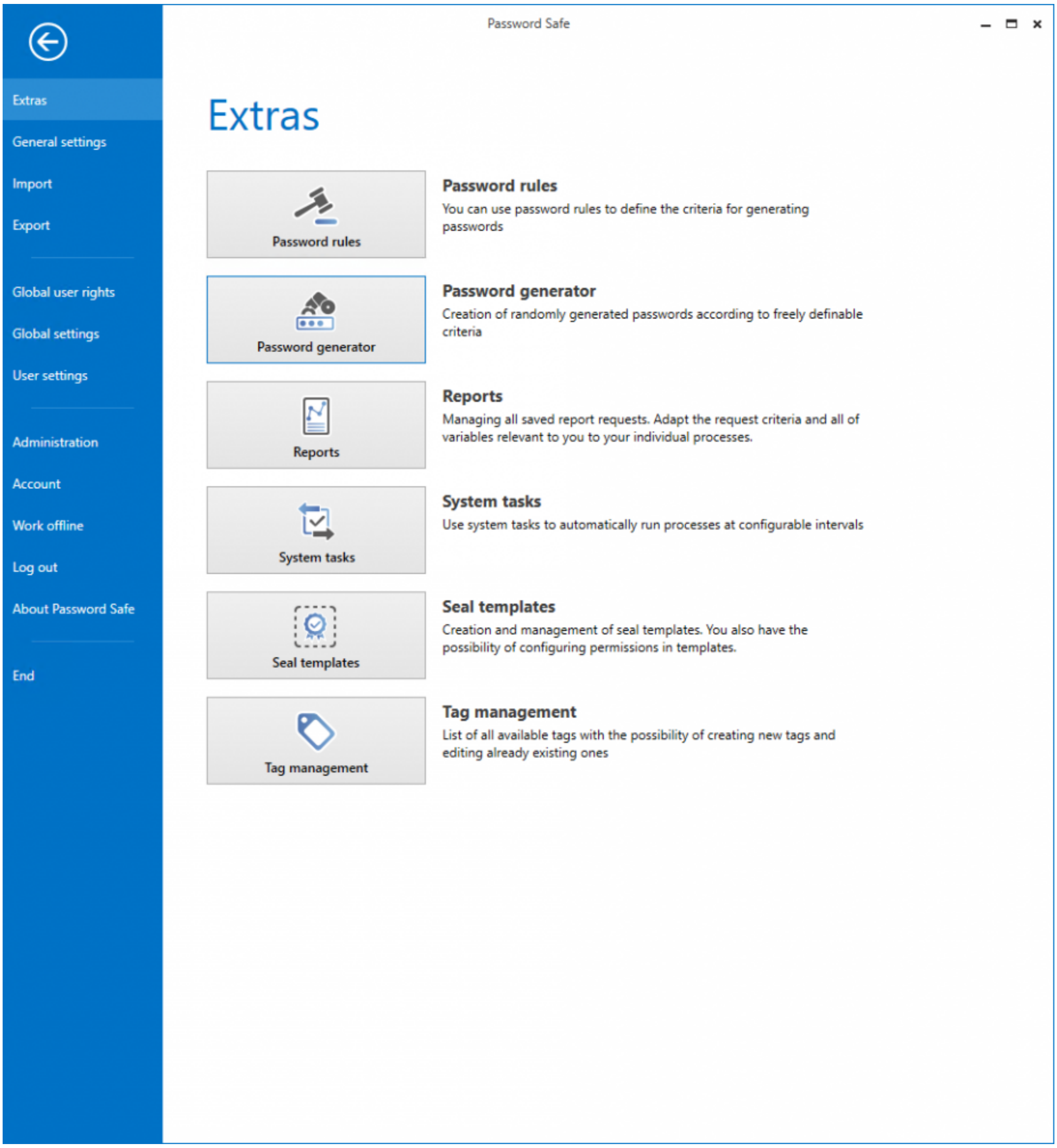
☑ Type
☑ Event
☑ When
☑ Name
☑ From
☑ IP address
☑ Computer user
☑ Computer name
☑ Description
☑ Client type

The column editor can be used to arrange and display the data in the table according to their importance.

Main menu

What is the Main menu/Backstage?

All settings that are not linked to a particular module are defined in the Backstage (main menu). This makes it easy to access the settings at any time and in any module.



Extras

Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

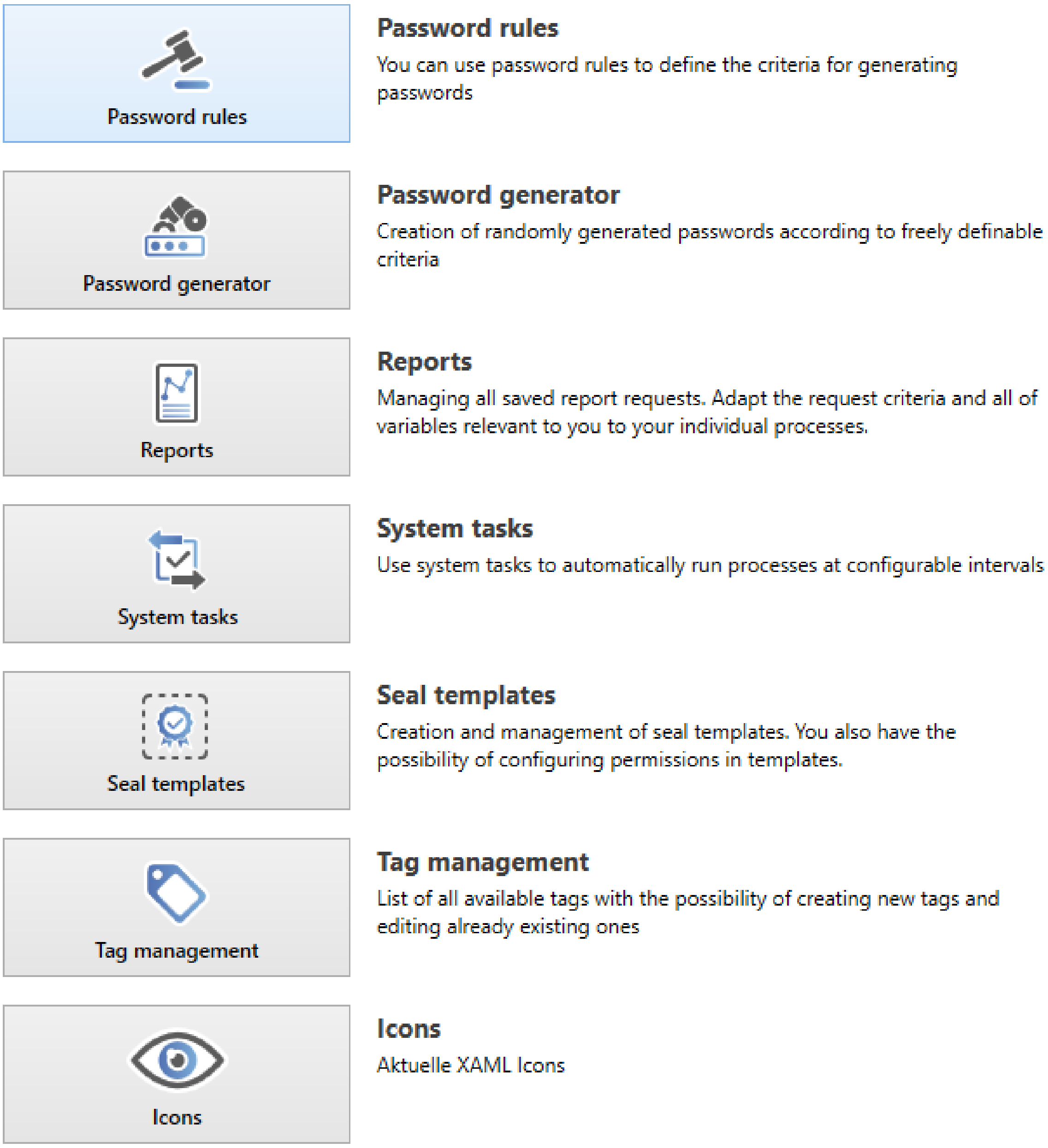
- Extras
- General settings

- Import
- Export
- User rights
- User settings
- Administration
- Account

Extras

What are Extras?

Password Safe provides a diverse range of supporting features that do not directly provide added value but mostly build on existing approaches and expand their functionalities. They are work-saving features that in total simplify the process of working with Password Safe.



Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons

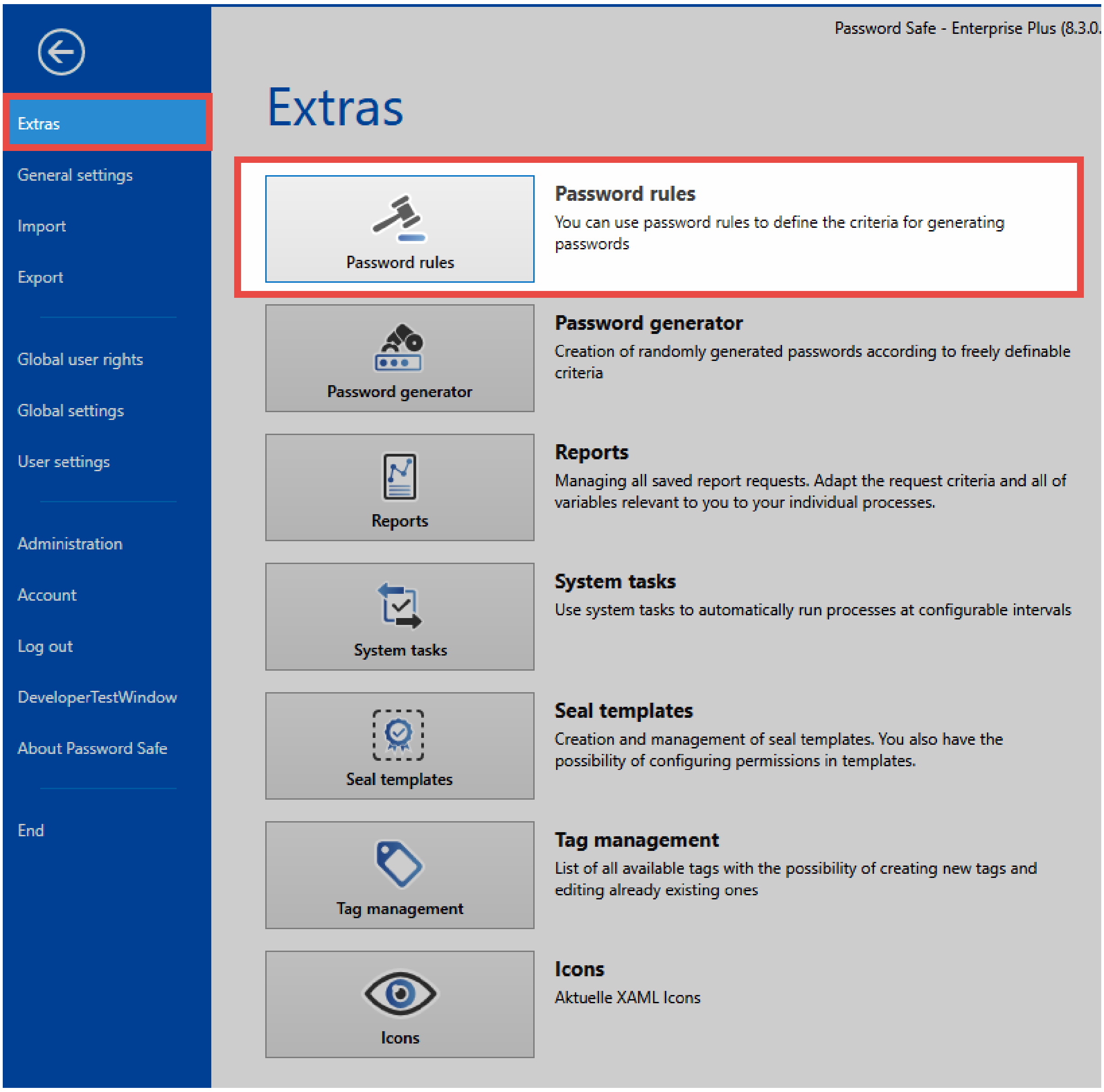
- Password rules
- Password generator

- Reports
- System tasks
- Seal templates
- Tag management

Password rules

What are password rules?

It is generally recommended that passwords should consist of at least 12 different characters, be complex and be automatically created. Rules set guidelines that can be made binding for users – meaning that the use of passwords with a certain level of complexity is enforced. Existing rules can also be reused in other areas.



Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

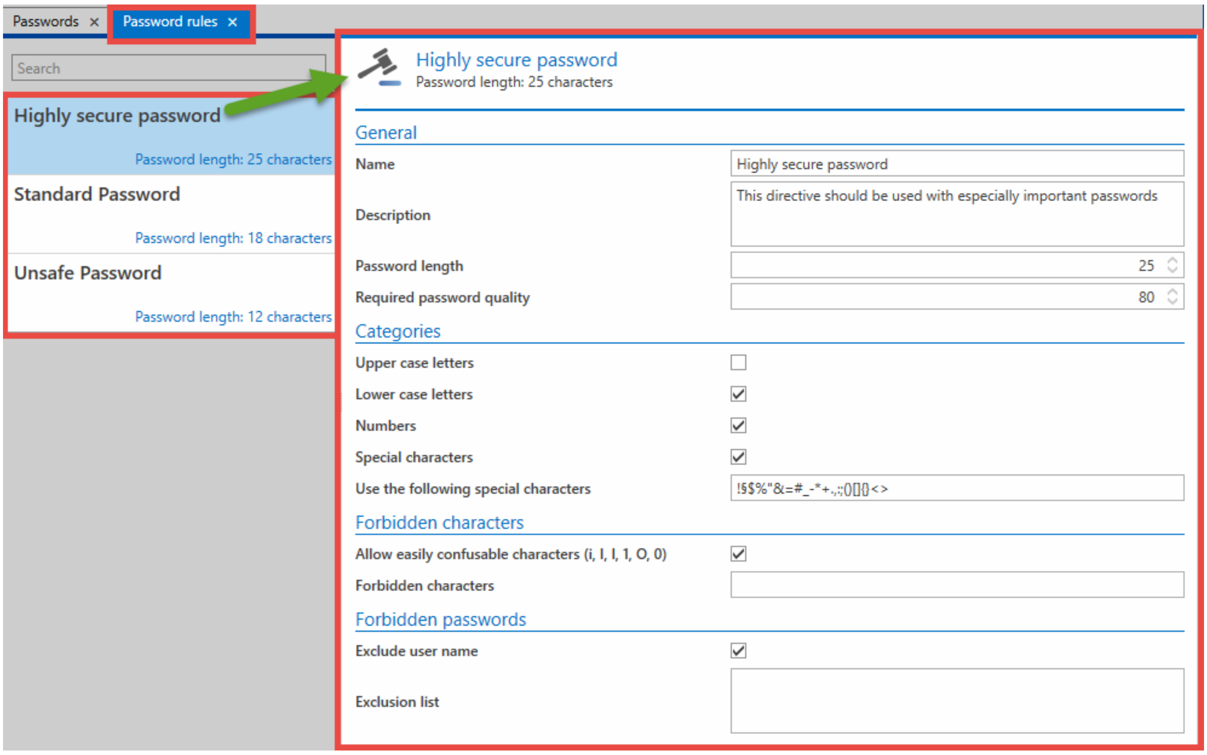
Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons

Managing password rules

If “Password rules” is selected under Main menu/Extras, the available password rules will appear in a separate tab in the currently active module.



Highly secure password
Password length: 25 characters

Standard Password
Password length: 18 characters

Unsafe Password
Password length: 12 characters

Highly secure password
Password length: 25 characters

General

Name	Highly secure password
Description	This directive should be used with especially important passwords
Password length	25
Required password quality	80

Categories

Upper case letters	□
Lower case letters	☑
Numbers	☑
Special characters	☑
Use the following special characters	!§$%"&=#_-*+.,:;()[]{}<>

Forbidden characters

Allow easily confusable characters (i, I, l, 1, O, 0)	☑
Forbidden characters	

Forbidden passwords

Exclude user name	☑
Exclusion list	

In this screenshot, a total of 3 password rules are shown. As the rule “Very secure password” has been selected in list view, the reading pane on the right displays the configuration for this rule:

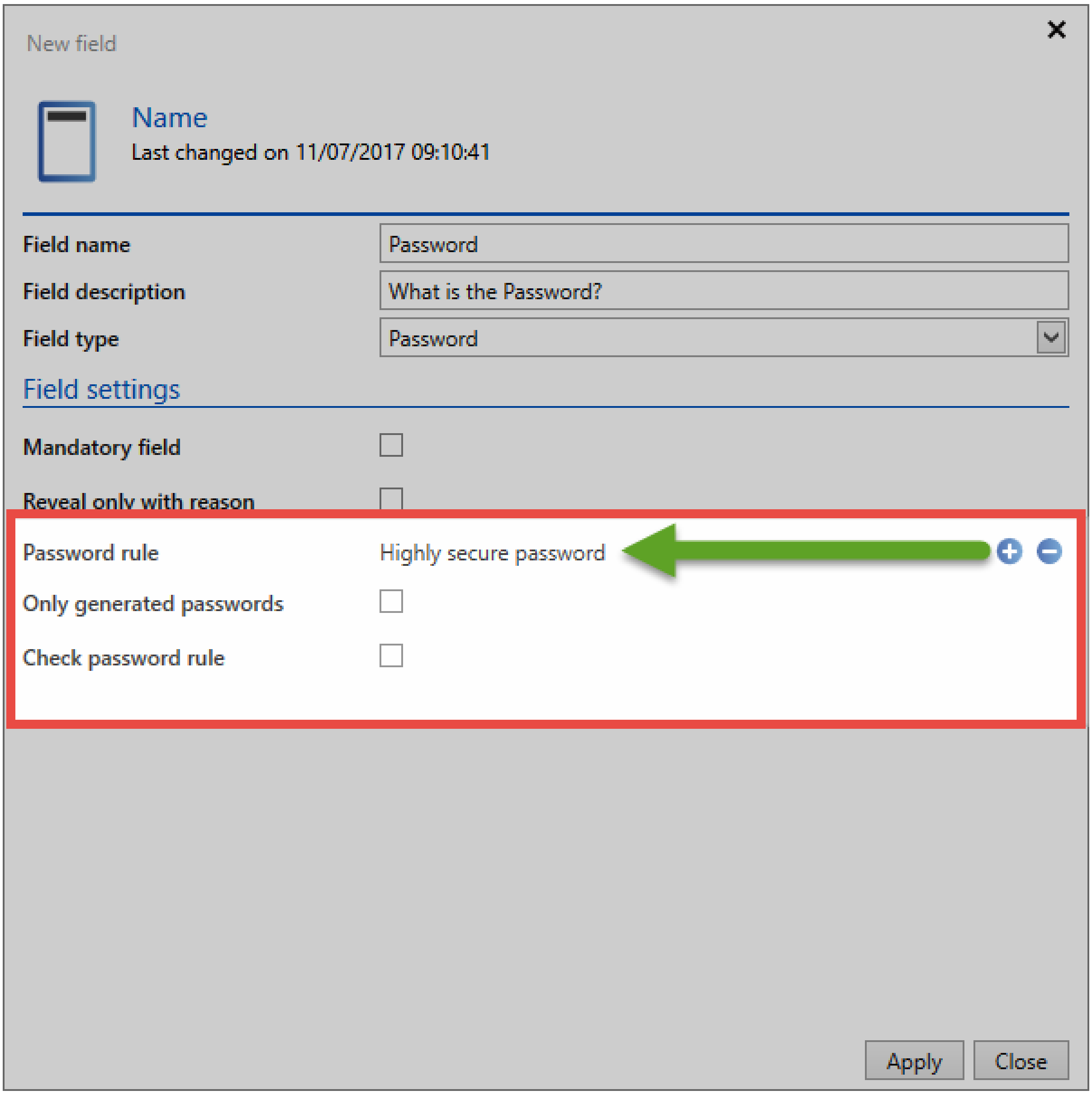
- **General**: The*Password length* of 25 is the minimum number of characters that a password needs to contain according to this rule. The required **Password quality** is an internal measure of security, which is calculated for this rule. This value always lies between 1 (very unsecure) and 100 (maximum security).
- **Categories**: A password can consist of a total of four categories. It is possible to define which of these categories to use and also how many of them to use.
- **Forbidden characters**: It is also possible to exclude some special characters. These characters need to be entered in the list without separators.
- **Forbidden passwords**: Some passwords and the user name can also be added to the list of forbidden passwords
- **Preview rules**: When new rules are created, an example password is generated that conforms to the configured rules. This is only the case for passwords with a minimum length of 3 characters!

Using password rules

Once password rules have been defined, they can be productively used in two different ways:

- Use within the password generator
- Default for the password field in a form:

When a password field is defined in a form, one of the defined password rules can be set as the default. This means that the default will always be used when a new password is created. In this way, it is possible to ensure that the required level of complexity is maintained for certain passwords.



New field

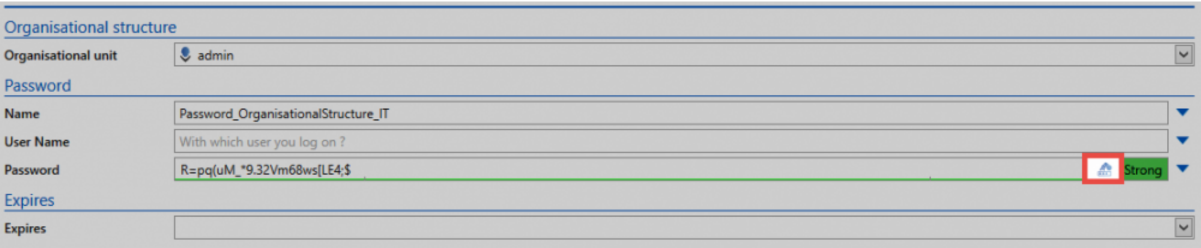
Name
Last changed on 11/07/2017 09:10:41

Field name: Password
Field description: What is the Password?
Field type: Password

Field settings

Mandatory field □
Reveal only with reason □
Password rule: Highly secure password
Only generated passwords □
Check password rule □

If one of these password rules is defined for a form, it is only possible to define a new random value for the password if a new password is created. The icon on the right hand side of the password field is used for this purpose.



Organisational structure

Organisational unit: admin

Password

Name: Password_OrganisationalStructure_IT

User Name: With which user you log on ?

Password: R=pq(uM_*9.32Vm68ws[LE4;$

Expires

Expires:

Defining standard rules for user passwords

If Master Key mode is not being used, users can change their passwords in Password Safe. The administrator can define the password strength required for these passwords by using standard password rules. More…

Visibility

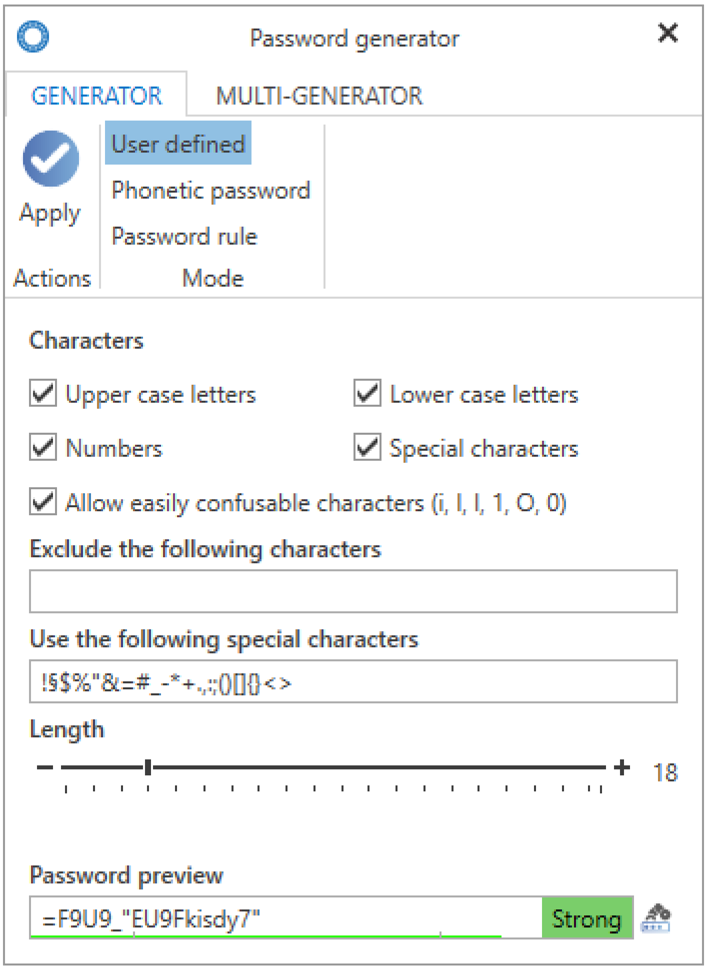
The password rules themselves are not subject to any permissions. All defined rules are therefore available to all users. The rules are managed from the Main menu.

Users can only manage the rules if they have the appropriate user right

Password generator

What is the password generator?

The complexity of passwords is generally determined by their randomness. In order to be able to rely 100% on the fact that the passwords are randomly generated, an algorithm for generating passwords is indispensable. The password generator performs this function and is completely integrated into the software.



Characters

☑ Upper case letters ☑ Lower case letters

☑ Numbers ☑ Special characters

☑ Allow easily confusable characters (i, I, l, 1, O, 0)

Exclude the following characters

Use the following special characters: !§$%"&=#_-*+.,:;()[]{}<>

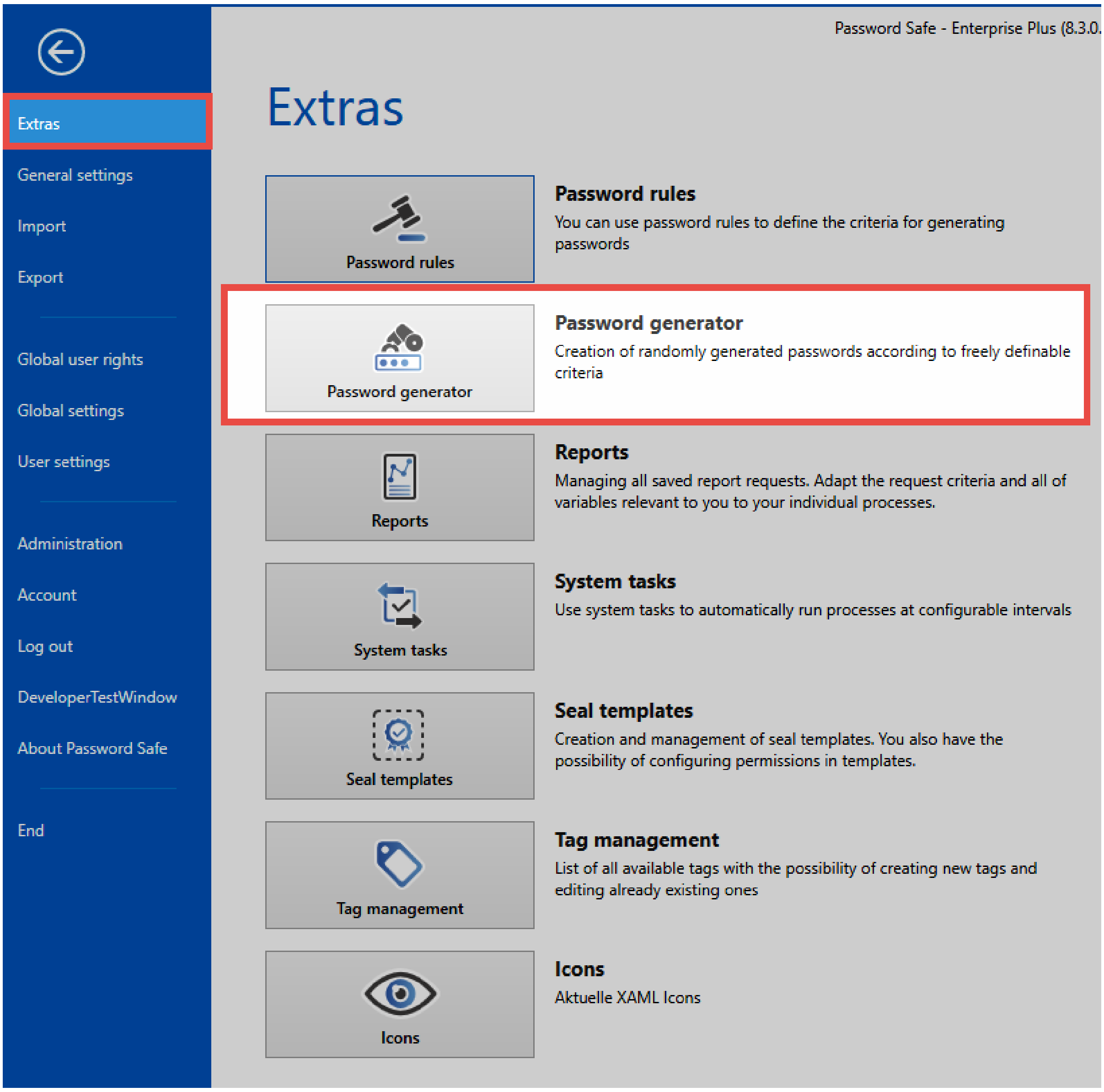
Length: 18

Password preview: =F9U9_"EU9Fkisdy7" Strong

Opening the password generator

The password generator can be opened in different ways:

- **Main menu/Extras/Password generator**: Here, the password generator is accessed directly. Passwords generated in the password generator can be copied to the clipboard.



Password Safe - Enterprise Plus (8.3.0.

Extras

Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons

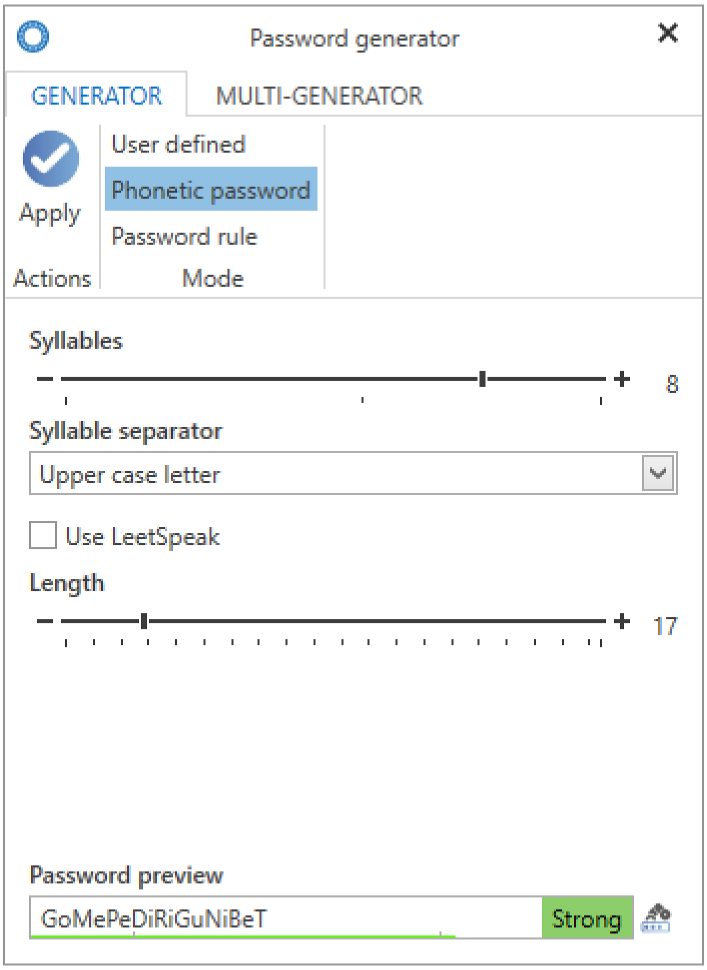
- **When creating new records**: Once the password field has been selected in the reading pane, the password generator can then be directly opened in the “Form field” tab via the ribbon. Passwords generated here can be directly entered into the password field for the new record using the “Adopt” button. Alternatively: The password generator can also be accessed on the right in the password field in the reading pane.

Functionality

The **Character** section is used to define the character groups that should form part of the password. This section can also be used to exclude (special) characters. Once the password length has been defined, a preview of a password that corresponds to the configured criteria is displayed on the bottom edge of the password generator. The “shuffle function” can be activated via the icon on the right next to the password preview. This will generate a new password in accordance with the defined criteria.

Phonetic passwords

This type of password can be recognised by the fact that it is relatively easy to remember (they are “readable”) but do not have any association to terms found in dictionaries. Only the number of syllables and the total length are defined in this case. Options that can be set are how the syllables are separated and whether to use LeetSpeak.



Syllables 8

Syllable separator: Upper case letter

□ Use LeetSpeak

Length 17

Password preview: GoMePeDiRiGuNiBeT

Password rule

Already defined password rules can be utilised for the automatic generation of new passwords

Multigenerator

The multigenerator makes it possible to automatically generate up to 200 passwords. The convention used for generating these passwords is always the previously defined default. This could be:

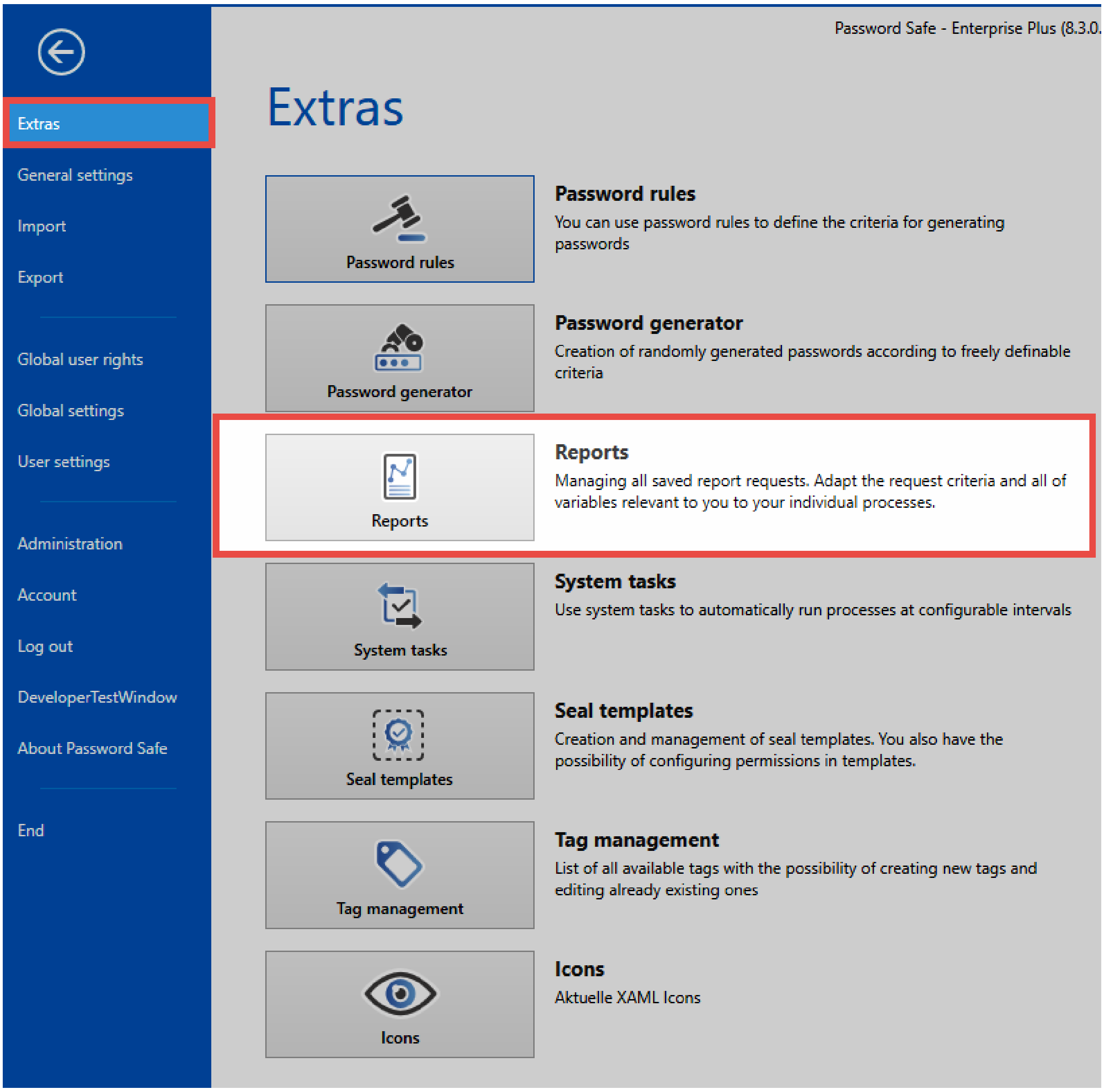
- User defined
- Phonetic passwords
- Password rules

The generated passwords are saved in a text file in the local user directory and can be opened immediately if desired.

Reports

What are reports?

Comprehensive reporting is an important component of the ongoing monitoring of processes in Password Safe. Similar to selectively configurable notifications, reports also contain information that can be selectively defined. The difference is mainly the trigger. Notifications are linked to an event, which acts as the trigger for the notification. In contrast, reports enable tabular lists of freely definable actions to be produced at any selected time – the trigger is thus the creation of a report. This process can also be automated via system tasks.



Password Safe - Enterprise Plus (8.3.0.

Extras

Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

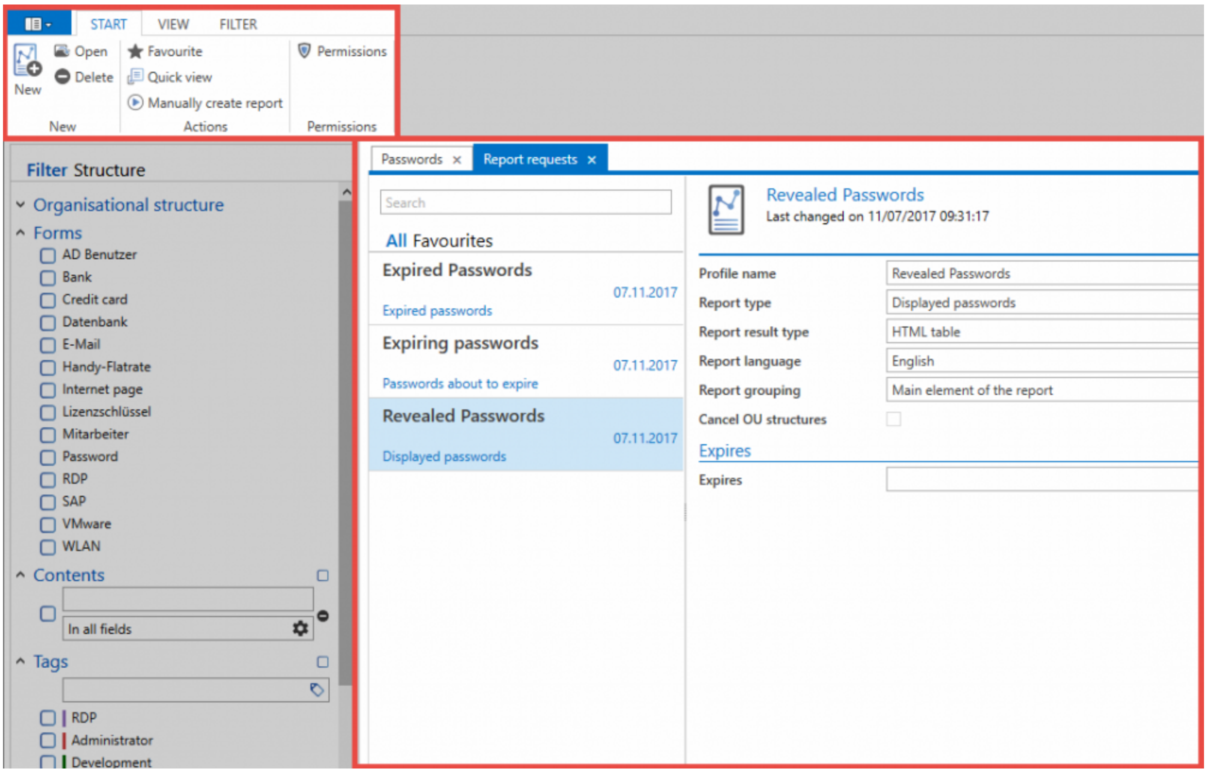
Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons

✻ Reports only ever contain information for which the user has the required permissions.

A separate tab for managing existing reports and creating new reports can be opened in the current module via the Main menu/Extras/Reports. The module in which the report is opened is irrelevant, the contents are always the same.



Expired Passwords 07.11.2017
Expired passwords

Expiring passwords 07.11.2017
Passwords about to expire

Revealed Passwords 07.11.2017
Displayed passwords

Revealed Passwords
Last changed on 11/07/2017 09:31:17

Profile name	Revealed Passwords
Report type	Displayed passwords
Report result type	HTML table
Report language	English
Report grouping	Main element of the report
Cancel OU structures	□

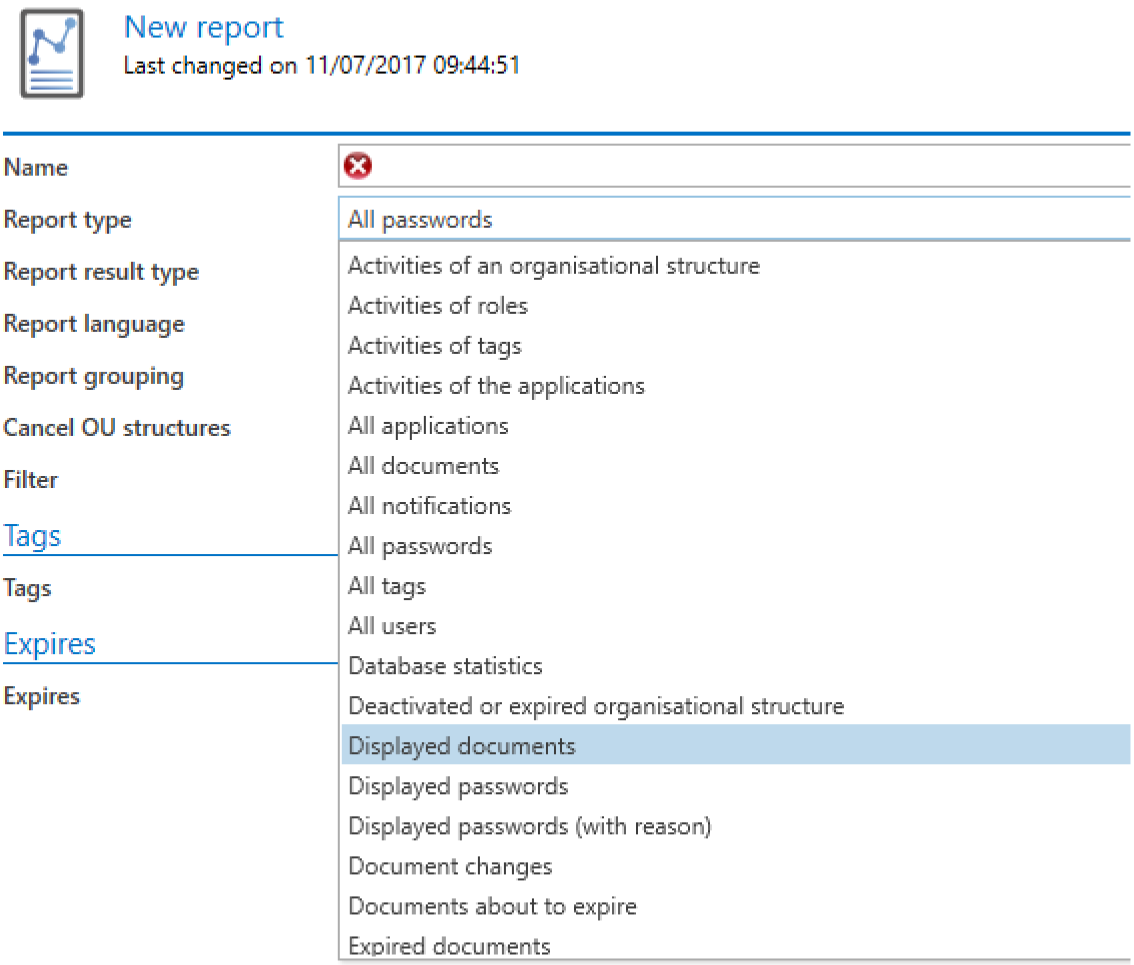
Expires

Expires	

The filter on the left has no relevance in relation to reports. Although reports can also be “tagged” in theory, filtering has no effect on the reports. In list view, there are currently three configured report requests shown.

Creating a report request

New report requests can be created in list view via the ribbon or also the context menu that is accessed using the right mouse button. The form for creating a new report request again opens in a separate tab. Alongside a diverse range of variables, the report type can be defined using a drop-down list. There are currently dozens of report types available.



New report
Last changed on 11/07/2017 09:44:51

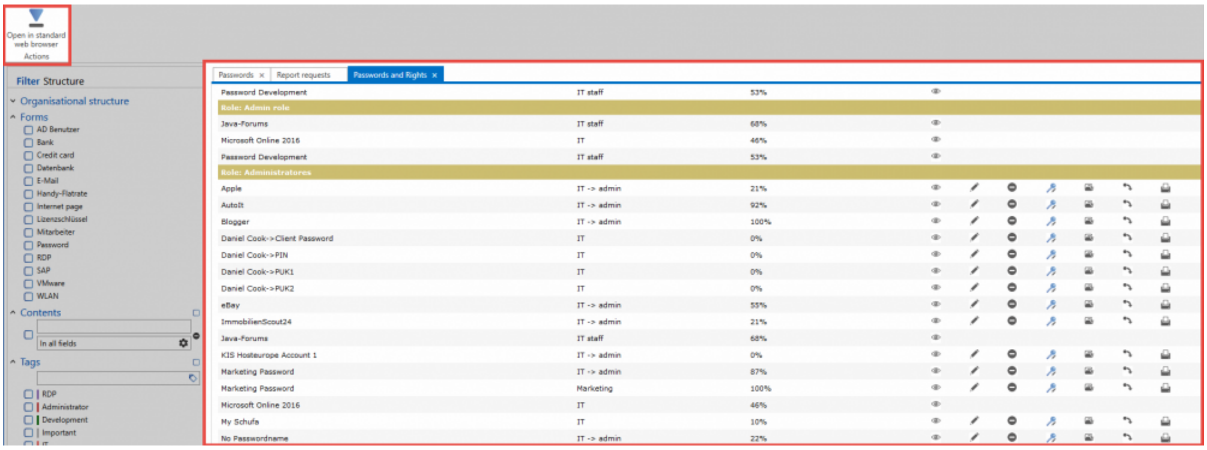
Name

Report type: All passwords

The filter can be used to define the scope of the report e.g. to focus on a certain OU or simply a selection of tags. Once saved, the report will now be shown in the list of report requests.

Manually create reports

You can now create a manual report via the ribbon. This will open in a separate tab and can be displayed in the default web browser if desired.



Password Development	IT staff	53%
Role: Admin role		
Java-Forums	IT staff	68%
Microsoft Online 2016	IT	46%
Password Development	IT staff	53%
Role: Administratores		
Apple	IT -> admin	21%
AutoIt	IT -> admin	92%
Blogger	IT -> admin	100%
Daniel Cook->Client Password	IT	0%
Daniel Cook->PIN	IT	0%
Daniel Cook->PUK1	IT	0%
Daniel Cook->PUK2	IT	0%
eBay	IT -> admin	55%
ImmobilienScout24	IT -> admin	21%
Java-Forums	IT staff	68%
KIS Hosteurope Account 1	IT -> admin	0%
Marketing Password	IT -> admin	87%
Marketing Password	Marketing	100%
Microsoft Online 2016	IT	46%
My Schufa	IT	10%
No Passwordname	IT -> admin	22%

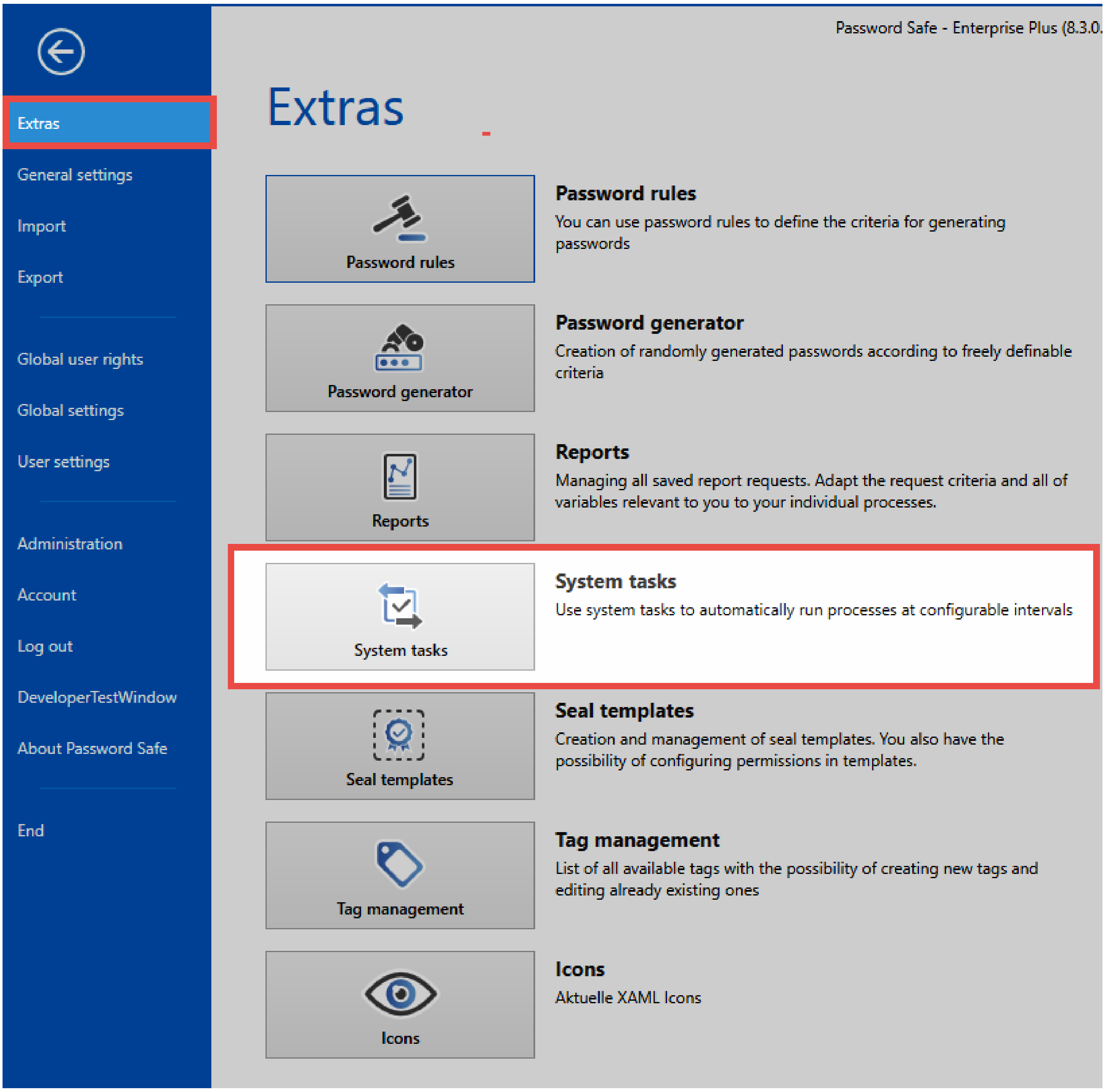
Automated sending of reports via system tasks

In general, reports are not manually created but are automatically sent to defined recipients. This is possible via system tasks, which can run processes of this nature at set times. More…

System tasks

What are system tasks?

Password Safe supports administrators and users by automating repetitive tasks. These are represented as system tasks. Predefined tasks can thus be carried out at freely defined intervals.



Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons

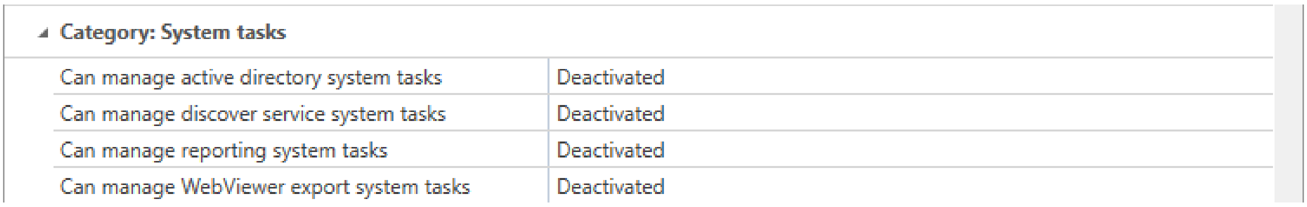
What can be automated?

There are currently four different work processes that can be automated using system tasks:

- **HTML WebViewer export**: Exports a freely definable selection of records in an AES-256 encrypted HTML file. The file is saved in the form of notifications.
- **Reports**: Automatically creates a report that is issued in the notifications. This requires a report request to be created in advance.
- **Network service scan**: Searches for service accounts on the network at defined cycles
- **Active Directory synchronization**: The comparison with Active Directory can also be automated via system tasks. This requires an Active Directory profile to be created in advance. It is important to note that only the **Master Key profile** can be automatically compared.

Requirements

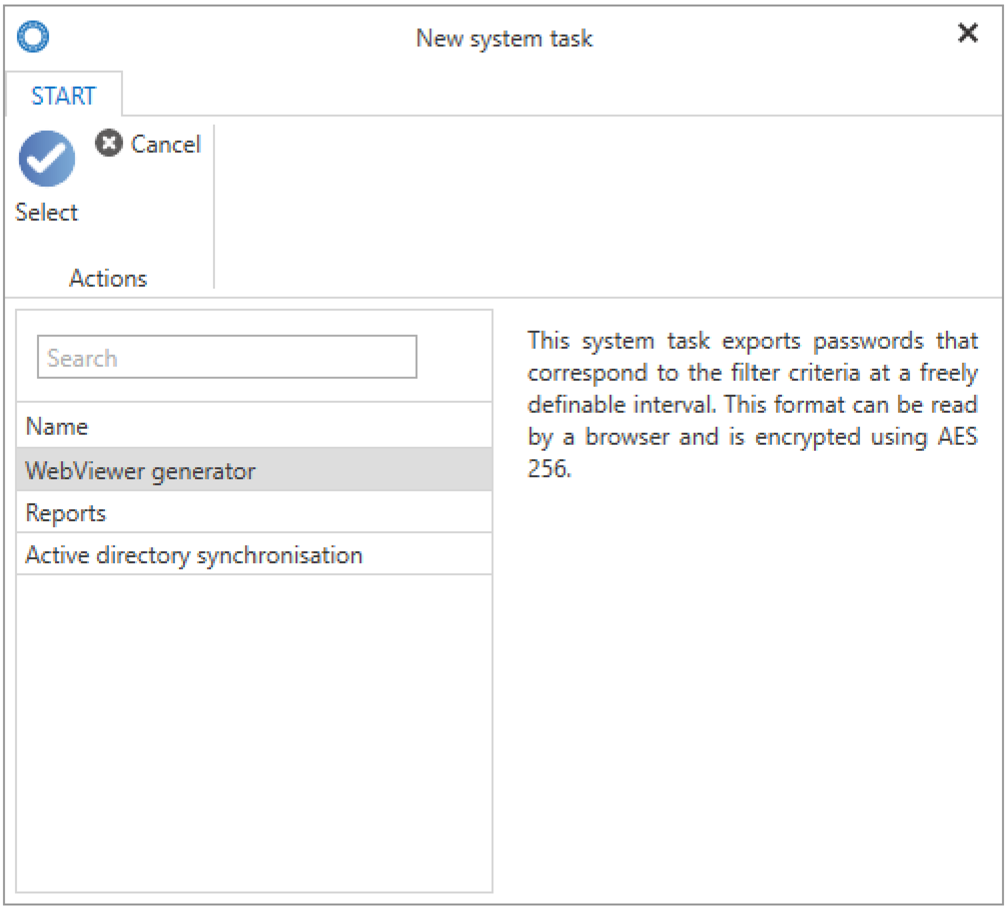
There is a separate user right for each of the four listed use cases:



Category: System tasks	
Can manage active directory system tasks	Deactivated
Can manage discover service system tasks	Deactivated
Can manage reporting system tasks	Deactivated
Can manage WebViewer export system tasks	Deactivated

Creating system tasks

System tasks can be initiated as usual via the ribbon or also the context menu that is accessed using the right mouse button. The desired process to be automated using system tasks is then selected from the four above-mentioned work processes.

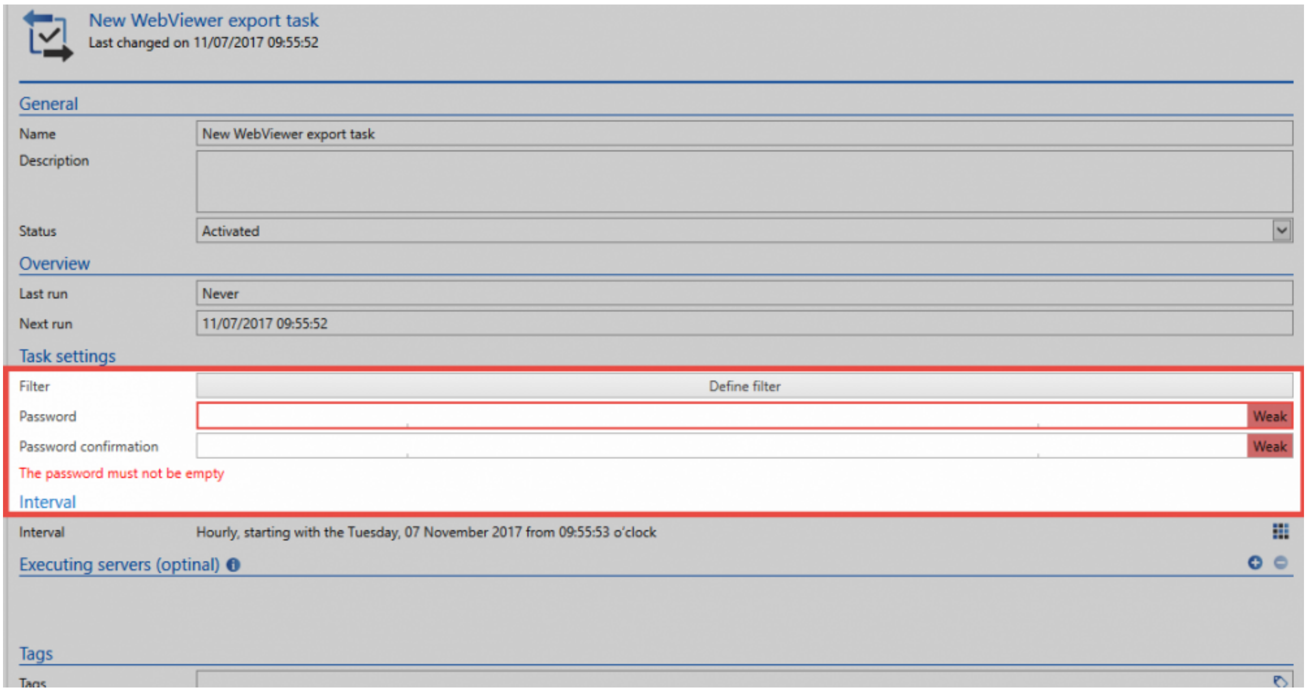


This system task exports passwords that correspond to the filter criteria at a freely definable interval. This format can be read by a browser and is encrypted using AES 256.

Naturally, the four work processes also share some similarities in their configuration.

- **Status**: The system task is normally activated and then starts immediately after it has been saved according to the defined intervals. If the system task is deactivated here, it is still saved but is not yet activated.
- **Next run**: This setting describes when the system task will be performed or when it was already performed for the first time (if this task was already created and is now being edited)
- **Interval**: The interval at which the system task should be executed is defined here. All increments between every minute and once only are possible. It is also possible to enter an end date.

The differences between the four work processes to be automated are described below. These differences are always part of the task settings within the system task form – the example here shows an HTML WebViewer export to be configured.



New WebViewer export task
Last changed on 11/07/2017 09:55:52

General

Name: New WebViewer export task
Description:
Status: Activated

Overview

Last run: Never
Next run: 11/07/2017 09:55:52

Task settings

Filter: Define filter
Password: Weak
Password confirmation: Weak
The password must not be empty

Interval

Interval: Hourly, starting with the Tuesday, 07 November 2017 from 09:55:53 o'clock

Executing servers (optinal)

Tags

Tags

WebViewer generator

- **Filter**: The passwords that should be exported are defined using a filter.
- **Password**: The HTML WebViewer creates an encrypted HTML file. The password is defined here and must then be confirmed.

Reports

- **Report request**: The report requests defined in Reports are available and can be selected here.

Discovery Service

- The **Discovery Service** scans the network and lists all of the services for which a service user has been saved. These can then be maintained using Password Safe. The information collected can then be directly transferred to the Password Reset for this purpose.

Active Directory synchronization

- *The Active Directory profile required for the synchronization is selected from those available.

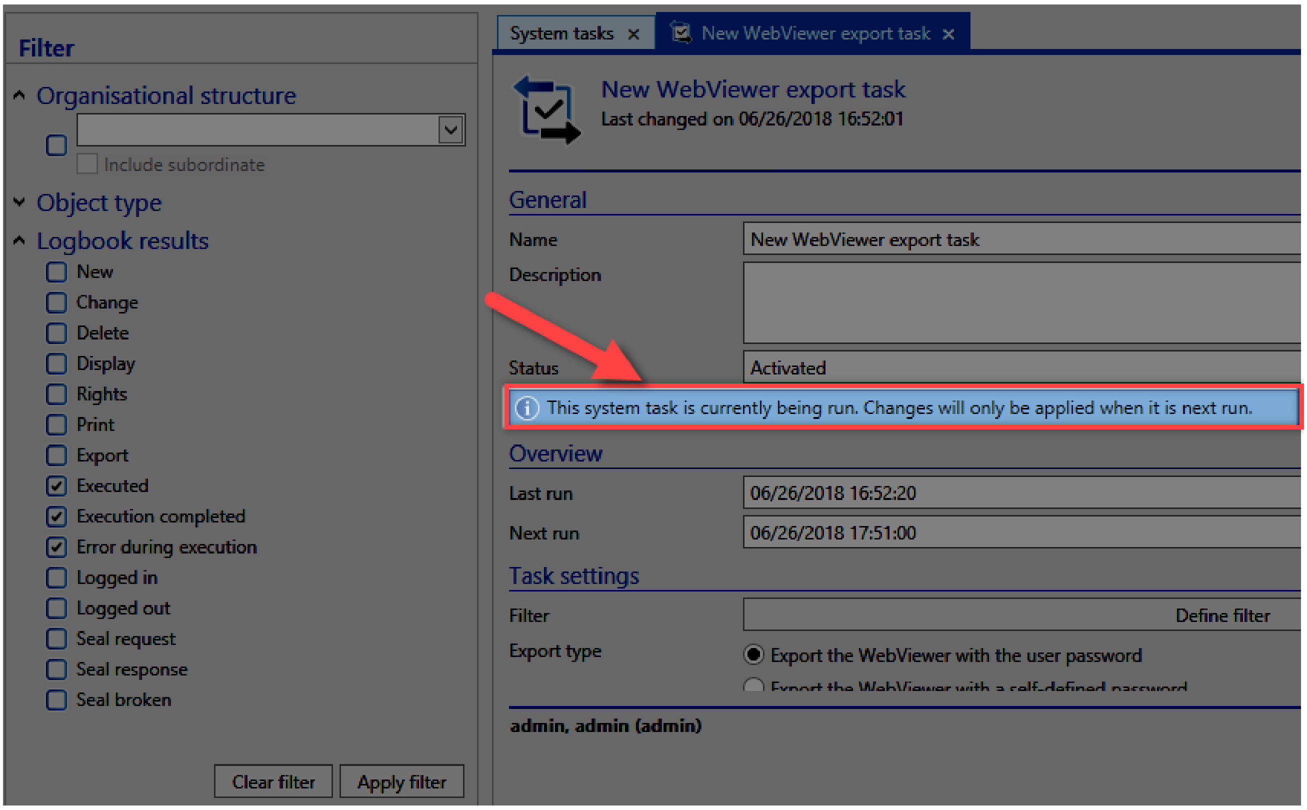
Emergency WebViewer export

- The Emergency WebViewer export creates an encrypted HTML file that contains all passwords. In an emergency, the data required to get the system up and running again can be accessed in this file.

> Tags could be defined for individual tasks – yet they have no relevance and can also not be used as filter criteria in the system tasks.

Status

A corresponding note will be displayed to indicate if a task is currently being executed.



Logbook results:
□ New
□ Change
□ Delete
□ Display
□ Rights
□ Print
□ Export
☑ Executed
☑ Execution completed
☑ Error during execution
□ Logged in
□ Logged out
□ Seal request
□ Seal response
□ Seal broken

New WebViewer export task
Last changed on 06/26/2018 16:52:01

Name: New WebViewer export task
Description:
Status: Activated

This system task is currently being run. Changes will only be applied when it is next run.

Last run: 06/26/2018 16:52:20
Next run: 06/26/2018 17:51:00

Filter:
Export type: ● Export the WebViewer with the user password
○ Export the WebViewer with a self-defined password

admin, admin (admin)

Emergency WebViewer

What is an Emergency WebViewer export?

Safeguarding data is essential and this should be carried out using backups. However, a backup is not sufficient in some cases e.g. if a backup cannot be directly restored due to a hardware problem. In these cases, **Password Safe** offers the backup feature **Emergency WebViewer Export**.

The **Emergency WebViewer Export** is based on an encrypted **HTML file** which can be decrypted using a corresponding **key**. Both files are required to view the passwords in a browser and form the core system of the backup mechanism.

Requirements

The Emergency WebViewer is included in the **Enterprise** and **Enterprise Plus** editions.

Creation of the file and key

The **Emergency WebViewer Export** is created in Password Safe as a **system task** and this task can be used to guarantee a **regular backup** of the records (passwords) by entering an **interval**. When setting up the system task, the user thus defines the cycle at which the **Emergency WebViewer.html file** is created on the AdminClient. The existing file is overwritten in each case by the latest version at the **defined interval**. The associated **key** is only created once at the beginning and needs to be saved. The current version of the **HTML file** can only be decrypted using this **key**.

> ! The key (PrivateKey.prvkey) and the file (Emergency WebViewer.html) must be saved onto a secure medium (USB stick, HDD, CD/DVD, …) and kept in a secure location!

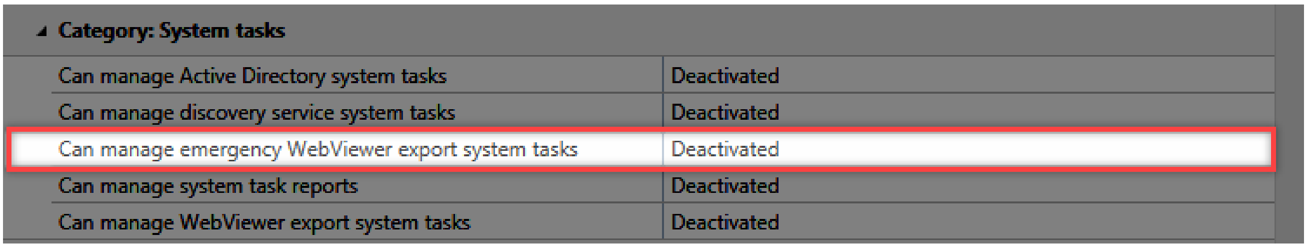
Data security

- Naturally, the HTML WebViewer file is encrypted
- The export of the file is protected using a corresponding user right
- The file can only be encrypted using the **PrivateKey.prvkey** file

> ! The **export right** for the passwords is not required for the **Emergency WebViewer Export!**

Required rights

The user requires the following right to create a **Emergency WebViewer Export system task**:



Category: System tasks	
Can manage Active Directory system tasks	Deactivated
Can manage discovery service system tasks	Deactivated
Can manage emergency WebViewer export system tasks	Deactivated
Can manage system task reports	Deactivated
Can manage WebViewer export system tasks	Deactivated

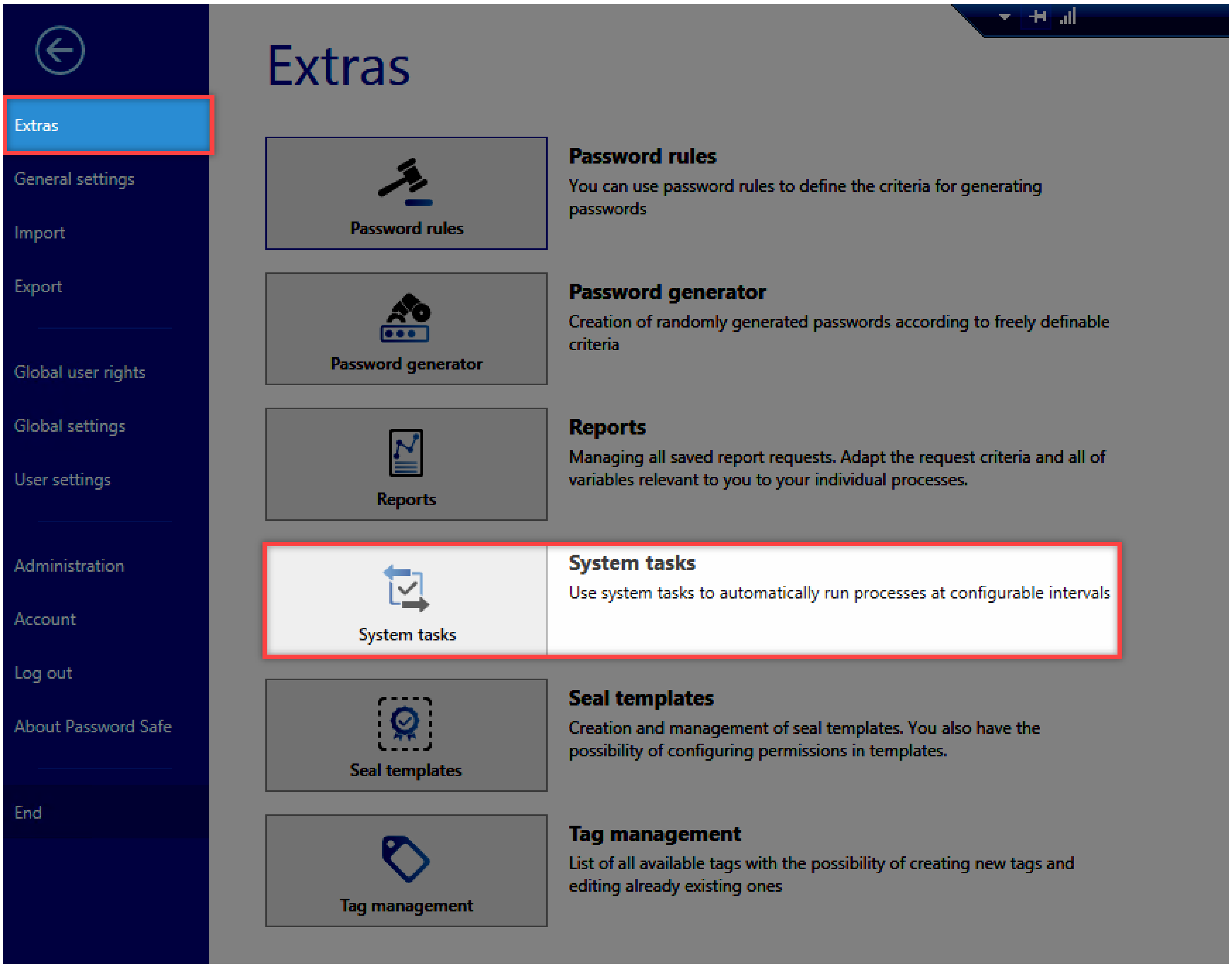
Emergency WebViewer.html and PrivateKey.prvkey

The*Emergency WebViewer Export* creates two associated files.

1. The file **Emergency WebViewer.html** is created on the computer executing the task
2. The associated key **PrivateKey.prvkey** is created on the client.

Calling up the Emergency WebViewer Export

The Emergency WebViewer Export is set up as a **system task**. It can be called up in the main menu under **Extras** -> **System Tasks**.



Extras

Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

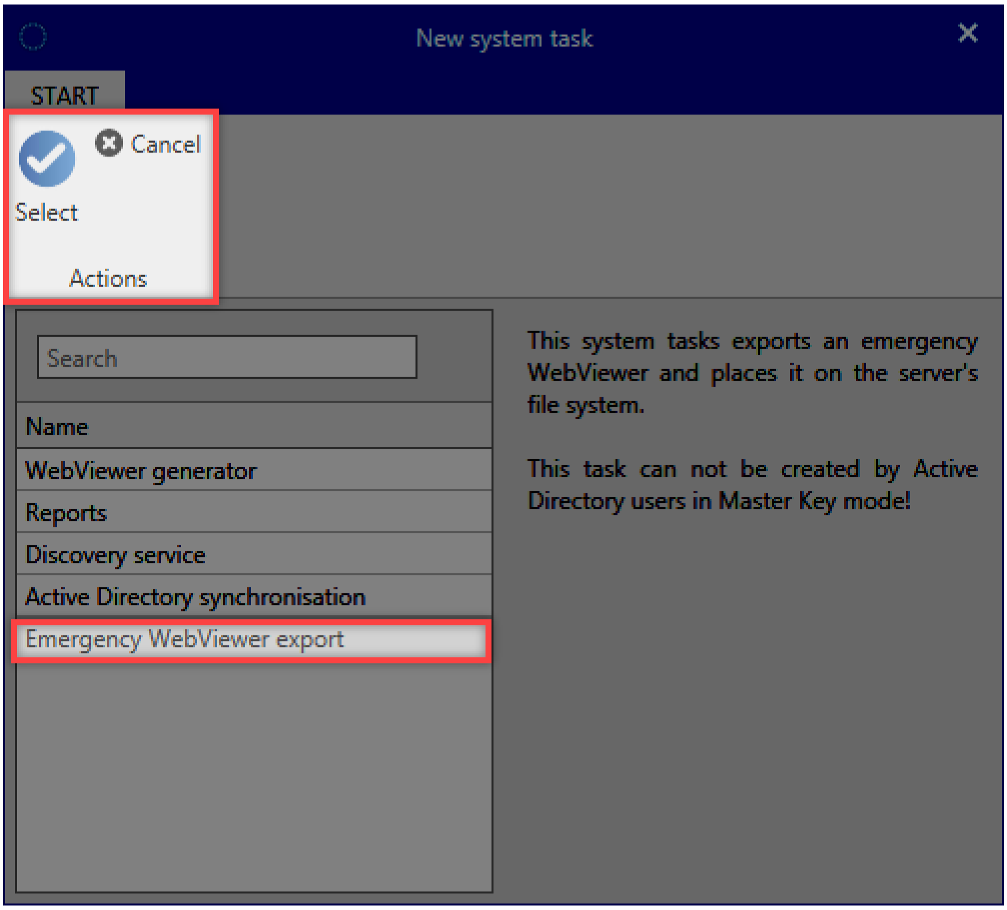
System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Creating a Emergency WebViewer Export file

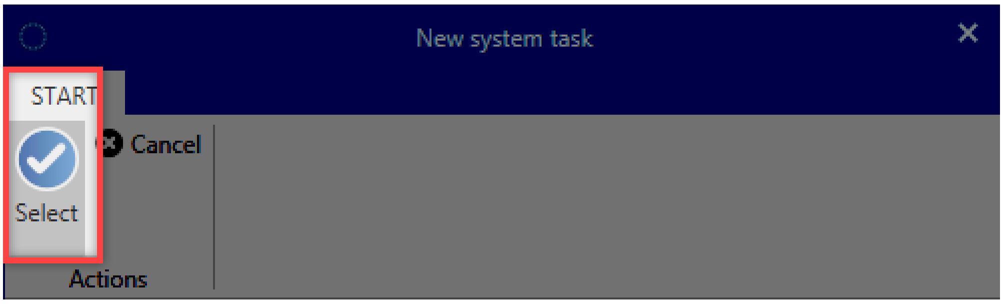
Clicking on **New** opens a new window and the **Emergency WebViewer Export** can be selected. The **configuration page** is then displayed.



This system tasks exports an emergency WebViewer and places it on the server's file system.

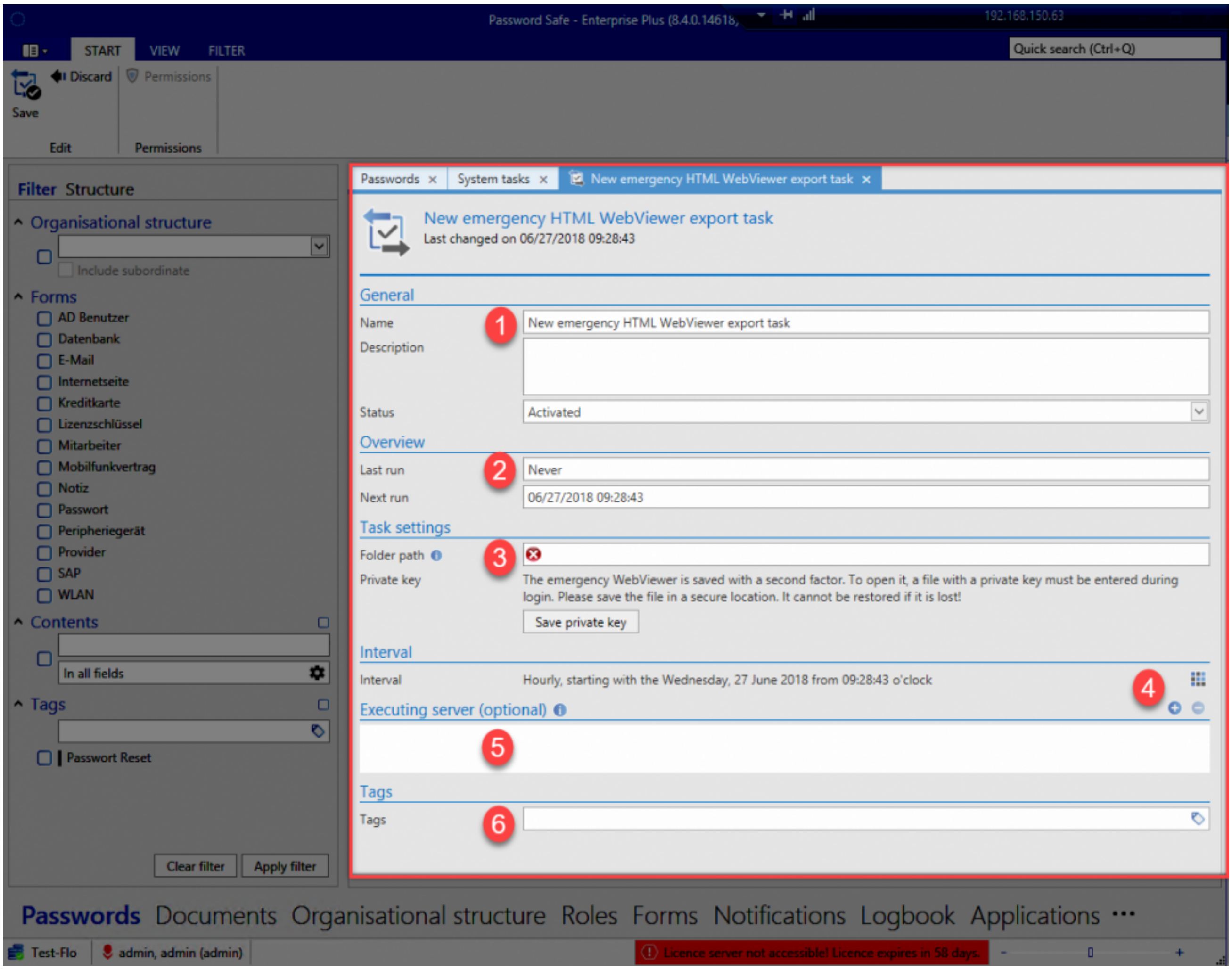
This task can not be created by Active Directory users in Master Key mode!

It is not possible to use the **Emergency WebViewer Export** with an **Active Directory user**.



Configuration page for the Emergency WebViewer Export task

A new tab is displayed: **New emergency HTML WebViewer export task** This now needs to be configured in accordance with the requirements.



New emergency HTML WebViewer export task

Last changed on 06/27/2018 09:28:43

Name: New emergency HTML WebViewer export task

Description:

Status: Activated

Last run: Never

Next run: 06/27/2018 09:28:43

Folder path:

Private key: The emergency WebViewer is saved with a second factor. To open it, a file with a private key must be entered during login. Please save the file in a secure location. It cannot be restored if it is lost!

Interval: Hourly, starting with the Wednesday, 27 June 2018 from 09:28:43 o'clock

Tags:

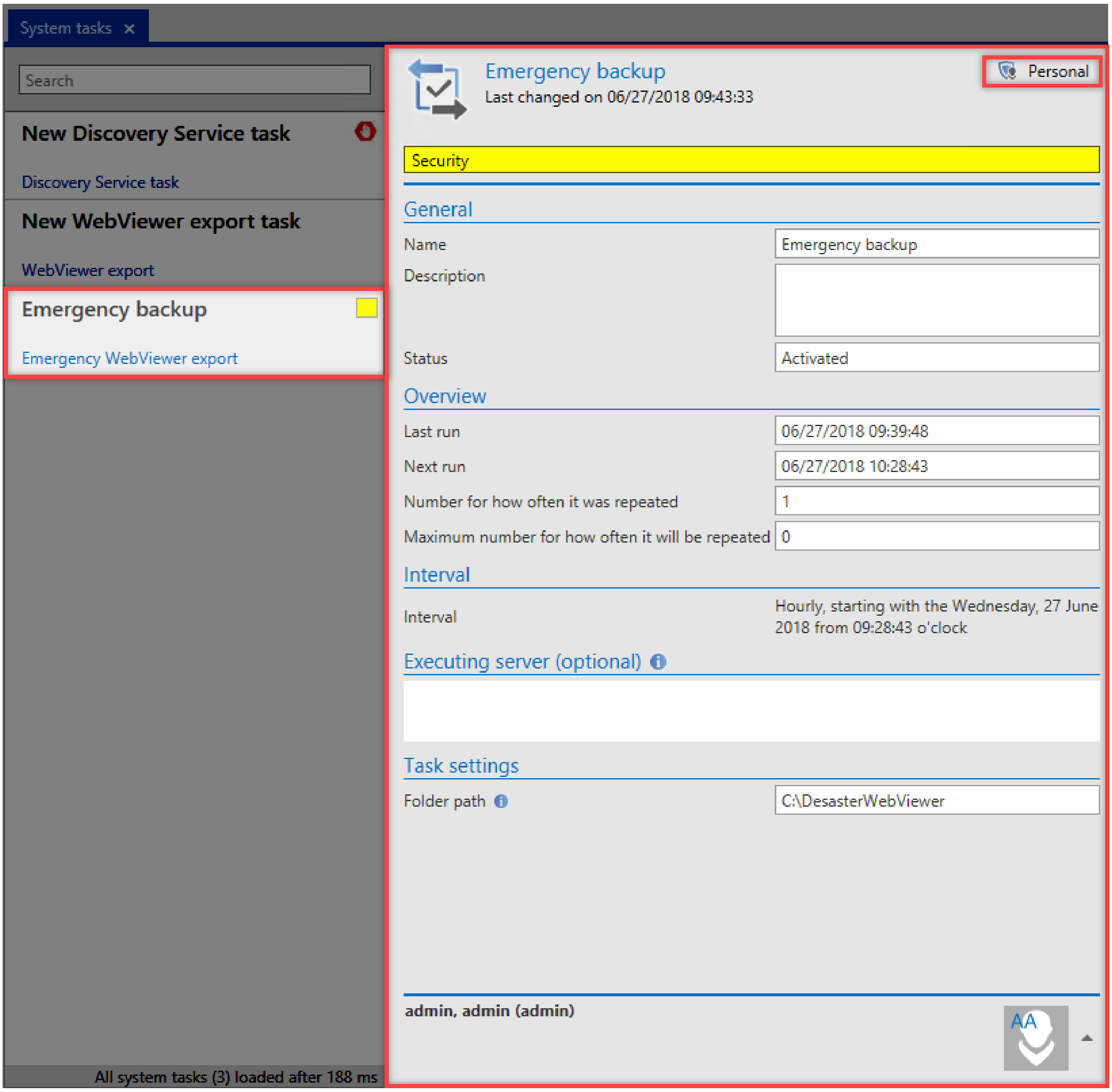
Licence server not accessible! Licence expires in 58 days.

1. **General**
   Name: Enter a unique name
   Description: Enter additional information
   Status: Execution: *Activated*/Deactivated
2. **Overview**
   Last run: Information display
   Next run: Information display
3. **Task settings**
   Folder path: Enter from the perspective of the server
   Private key: needs to be saved
4. **Interval**
   Setting for when the system task is executed
5. **Executing server (optional)**
   Address (IP) of the additional server
6. **Tags**
   Freely definable characteristics of records

! The private key for the Emergency WebViewer must be saved before the system task can be saved.

Displaying the Emergency WebViewer Export task

Once the configuration has been completed, the **system task** is displayed in the current module in the **System Tasks** tab. The user has the option of checking the data here.



New Discovery Service task
Discovery Service task

New WebViewer export task
WebViewer export

Emergency backup
Emergency WebViewer export

All system tasks (3) loaded after 188 ms

Emergency backup
Last changed on 06/27/2018 09:43:33

General

Name	Emergency backup
Description	
Status	Activated

Overview

Last run	06/27/2018 09:39:48
Next run	06/27/2018 10:28:43
Number for how often it was repeated	1
Maximum number for how often it will be repeated	0

Interval

Interval	Hourly, starting with the Wednesday, 27 June 2018 from 09:28:43 o'clock

Executing server (optional)

Task settings

Folder path	C:\DesasterWebViewer

admin, admin (admin)

Using the Emergency WebViewer.html file

After the **system task** has been successfully executed, **two files** will have been created for the password backup.

1. **Emergency WebViewer.html**
2. **PrivateKey.prvkey**

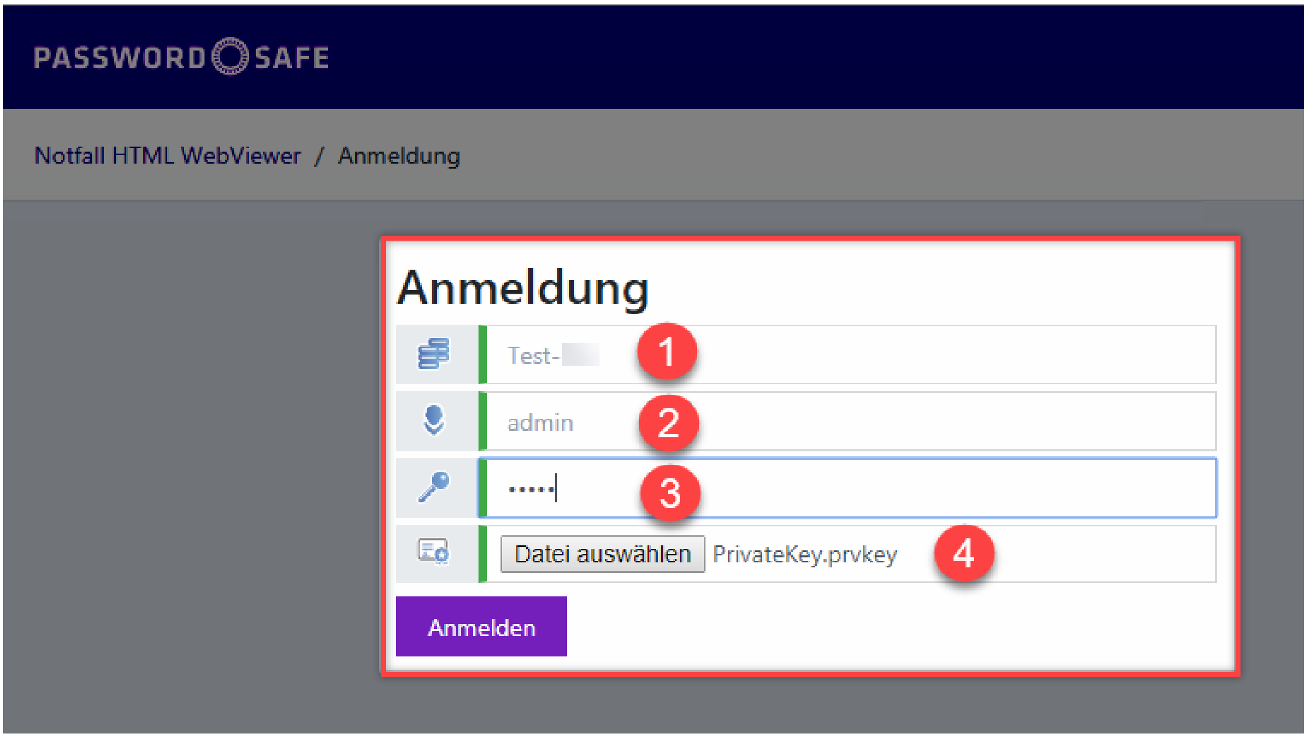
! The file **Emergency WebViewer.html** is **saved on the server** executing the task. The key **PrivateKey.prvkey** needs to be securely saved by the **user**!*

The **Emergency WebViewer Export** is used in the same way as the * WebViewer export.* The **passwords** are displayed in a current browser. The passwords are accessed in the **Emergency WebViewer Export** with the **user password** and the **key** saved for the user. The search function is used to select the **key (PrivateKey.prvkey)** and also to check its **validity**. If all data has been correctly entered, it is then possible to log in.

✻ The current user needs to log in using their password. If an incorrect password is entered, access is temporarily blocked.

Login data

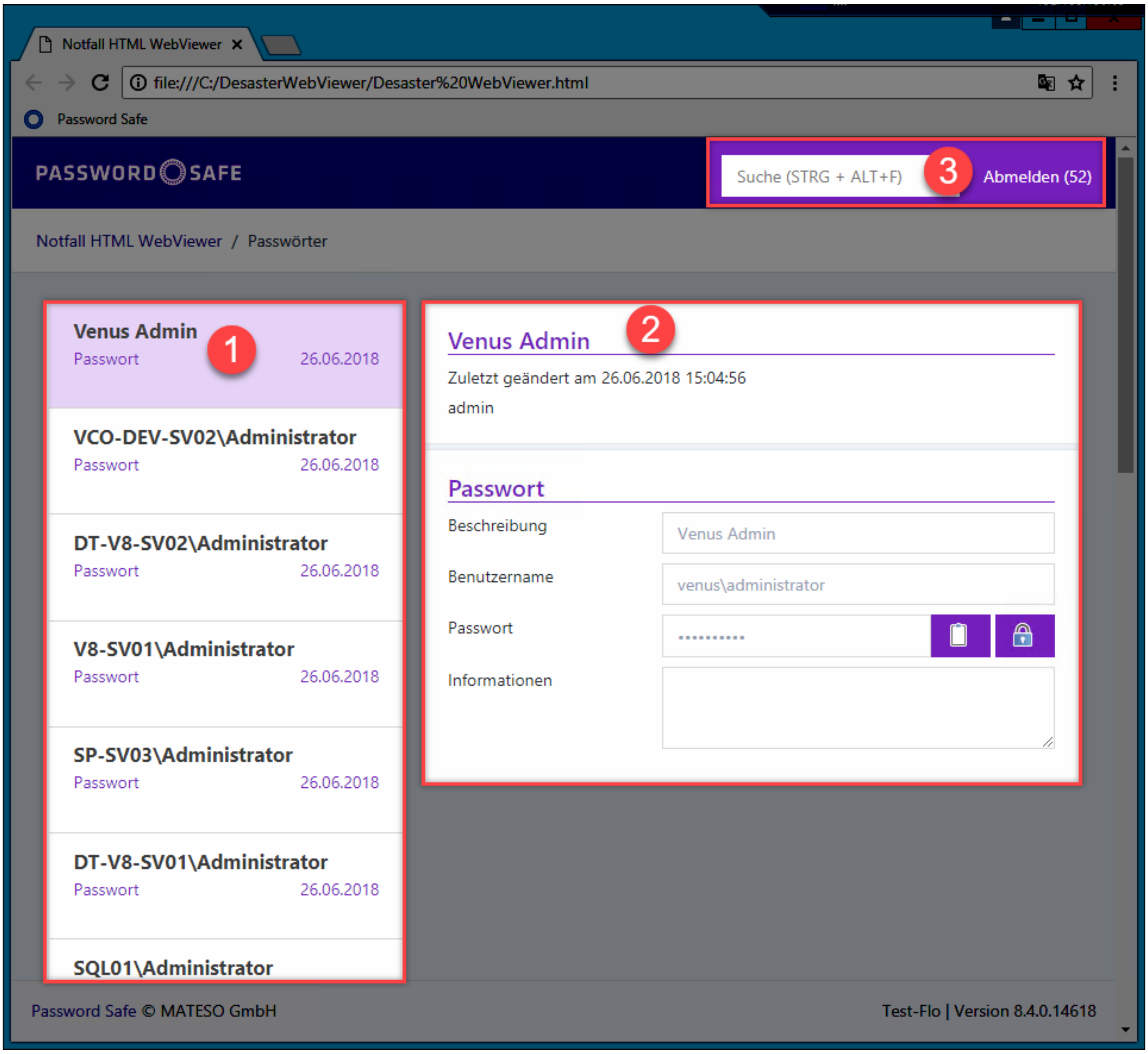
1. Database: Predefined
2. User: Predefined
3. Password : **User password (must be entered by the user)**
4. Key: **PrivateKey.prvkey**



Overview

After successfully logging in, the **overview page** for the **Emergency WebViewer Export** is displayed. This contains information about the saved **passwords** just like with the WebViewer export. The passwords are now available to the user.

Overview: Emergency HTML WebViewer / passwords



Notfall HTML WebViewer / Passwörter

Venus Admin
Passwort 26.06.2018

VCO-DEV-SV02\Administrator
Passwort 26.06.2018

DT-V8-SV02\Administrator
Passwort 26.06.2018

V8-SV01\Administrator
Passwort 26.06.2018

SP-SV03\Administrator
Passwort 26.06.2018

DT-V8-SV01\Administrator
Passwort 26.06.2018

SQL01\Administrator

Venus Admin

Zuletzt geändert am 26.06.2018 15:04:56
admin

Passwort

Beschreibung	Venus Admin
Benutzername	venus\administrator
Passwort	••••••••••
Informationen	

Password Safe © MATESO GmbH Test-Flo | Version 8.4.0.14618

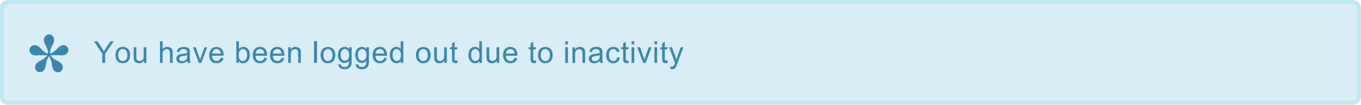
The following data is displayed in the overview:

Overview data:

1. Display of the currently available records
2. Detailed information on the selected record
3. Search, logout, timeout until logout
4. Copy password to clipboard
5. Reveal password

Security note

The existing **passwords** are now available to the user for further processing. The HTML page is closed by clicking on **Logout**.
If the user is **inactive** for **60 seconds**, he is automatically **logged out** and the **login** is displayed with additional information.



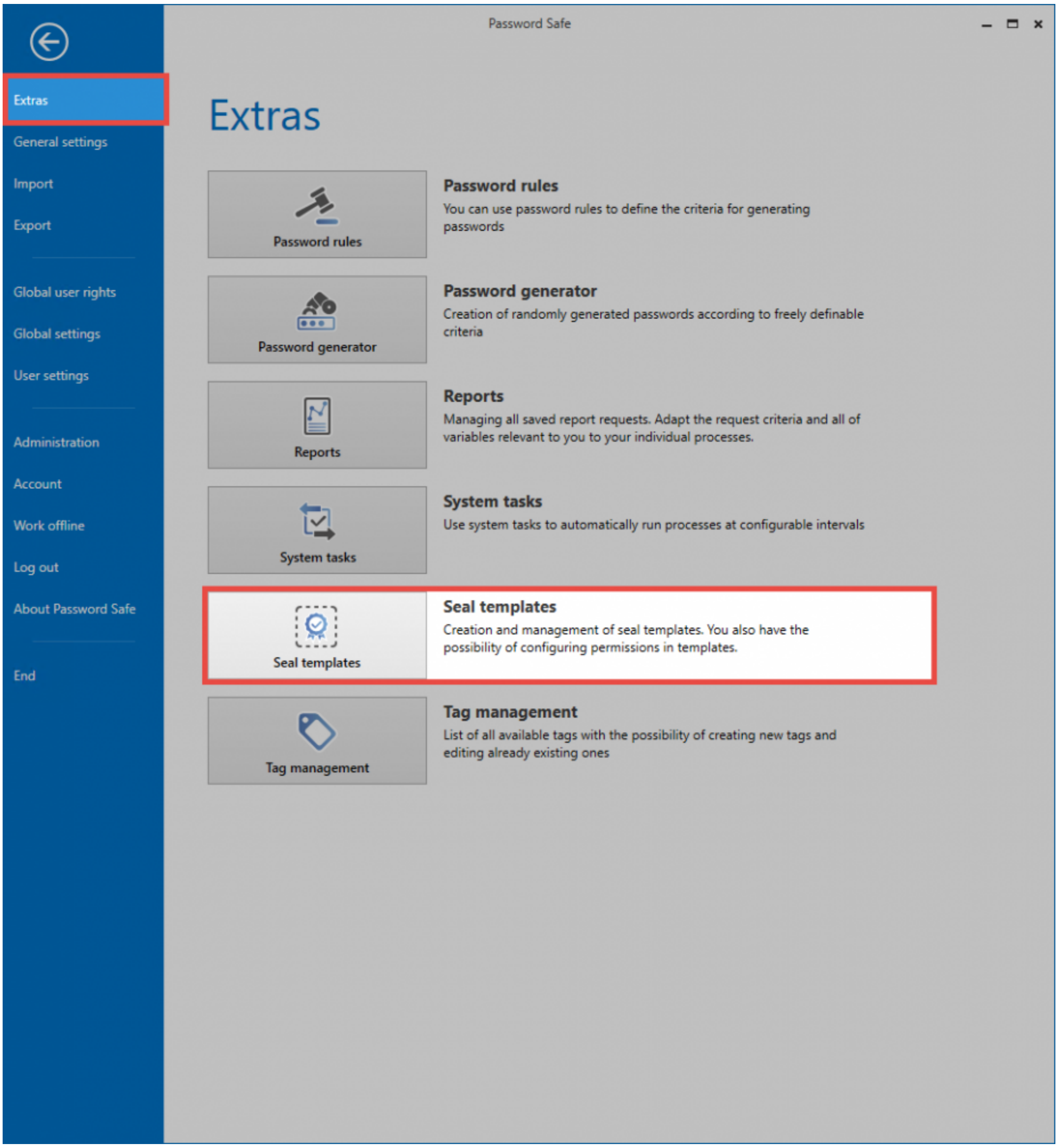
You have been logged out due to inactivity

The user can log in again using the **password** and **key** as described above. After successfully logging in, the **Emergency WebViewer Export overview** is displayed again.

Seal templates

What are the seal templates?

The configuration of seals must be well-thought-out and error-free. It is absolutely essential to save the once-invested effort in the form of seal templates. The automation of ever-recurring tasks will, in this context, extremely speed up the timing of the work. Once defined, templates can be attached to data records in a few simple steps. The adaptation of already created stencils is presented in the seal templates as clear and very fast.



Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

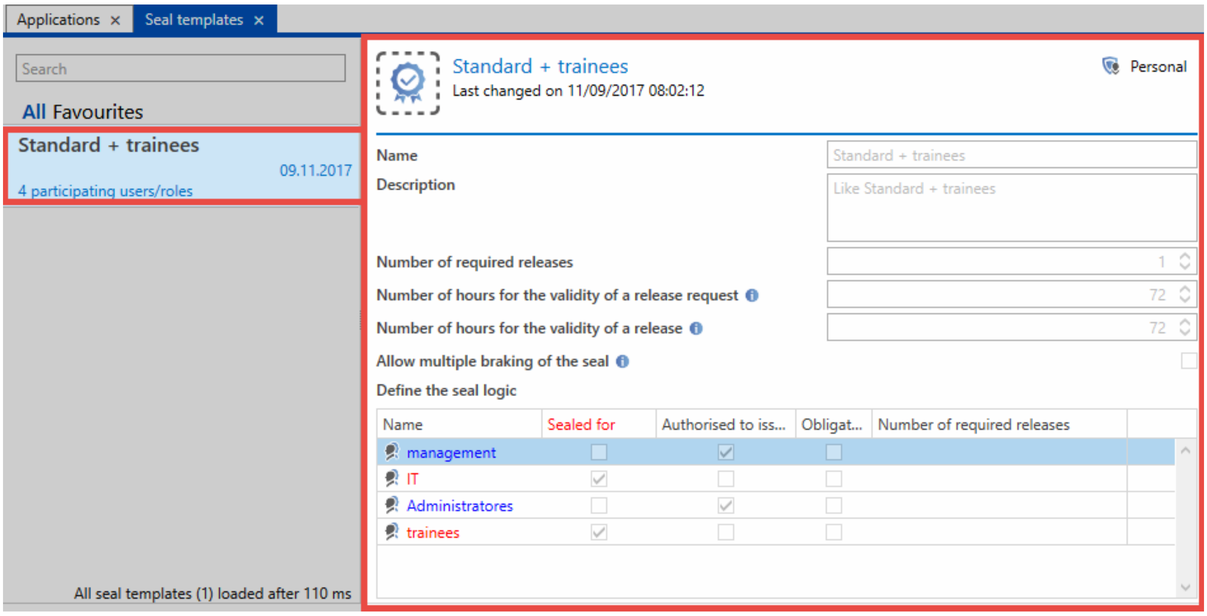
Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

✻ A separate tab opens in the active module in order to edit the default templates

Creating templates

! The right **Can manage seal templates** is required

When creating seals, the seal can be saved as a template using the wizard. All templates saved in this way are listed in the overview of the seal templates. Furthermore, it is possible to edit existing templates directly or create new ones via the button in the ribbon. This is done in the same way as the seal assistant.



Standard + trainees
09.11.2017
4 participating users/roles

All seal templates (1) loaded after 110 ms

Standard + trainees
Last changed on 11/09/2017 08:02:12
Personal

Name	Standard + trainees
Description	Like Standard + trainees
Number of required releases	1
Number of hours for the validity of a release request	72
Number of hours for the validity of a release	72
Allow multiple braking of the seal	☐

Define the seal logic

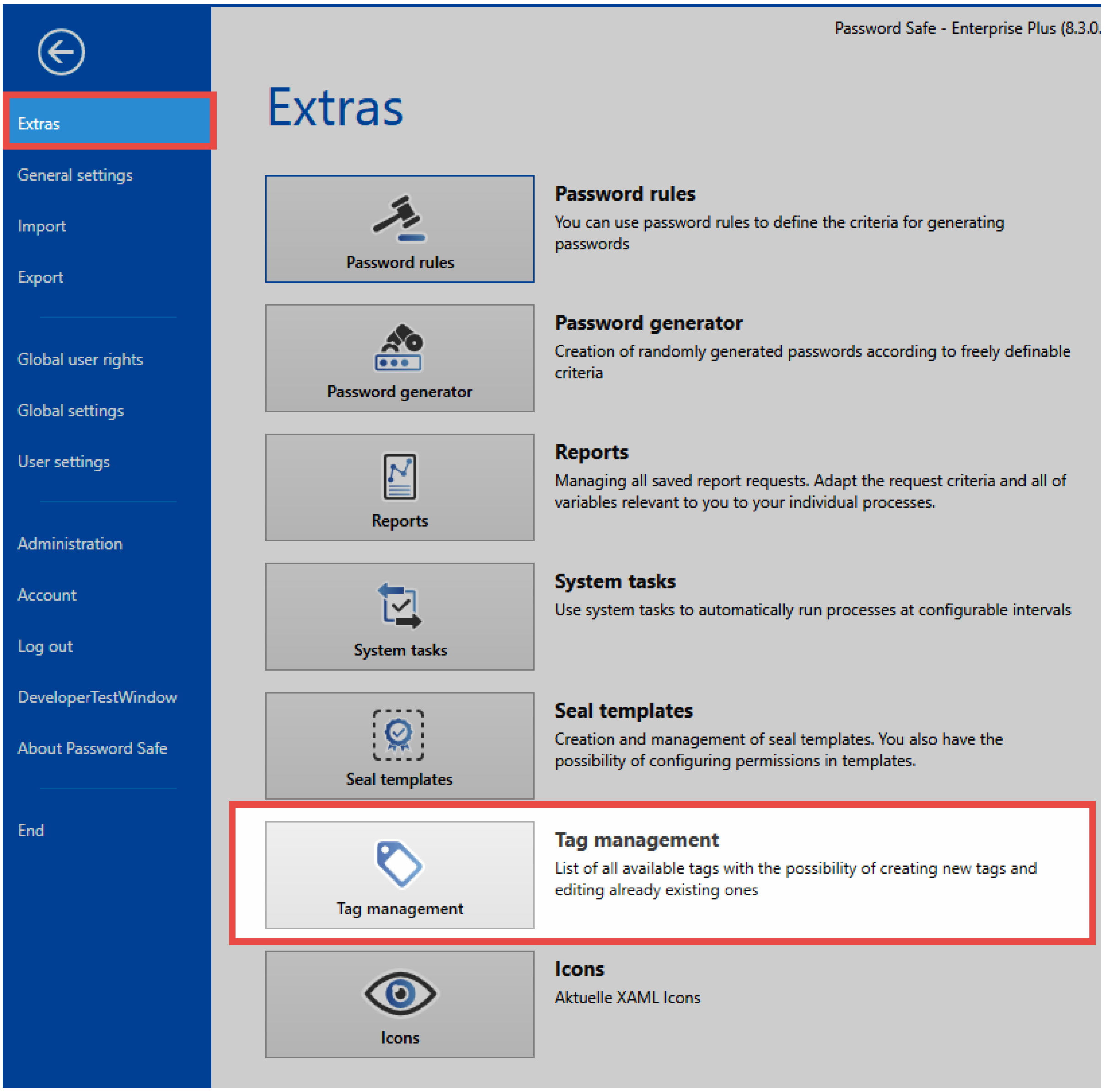
Name	Sealed for	Authorised to iss...	Obligat...	Number of required releases
management	☐	☑	☐	
IT	☑	☐	☐	
Administratores	☐	☑	☐	
trainees	☑	☐	☐	

Once templates have been added, they can be immediately used for the creation of new seals.

Tag manager

What is the tag manager?

All existing tags can be viewed, edited and deleted directly in the tag manager. This can be achieved via the filter, within the “Edit mode” of a data set as well as via the main menu under the group “Extras”.



Password Safe - Enterprise Plus (8.3.0.

Extras

Password rules
You can use password rules to define the criteria for generating passwords

Password generator
Creation of randomly generated passwords according to freely definable criteria

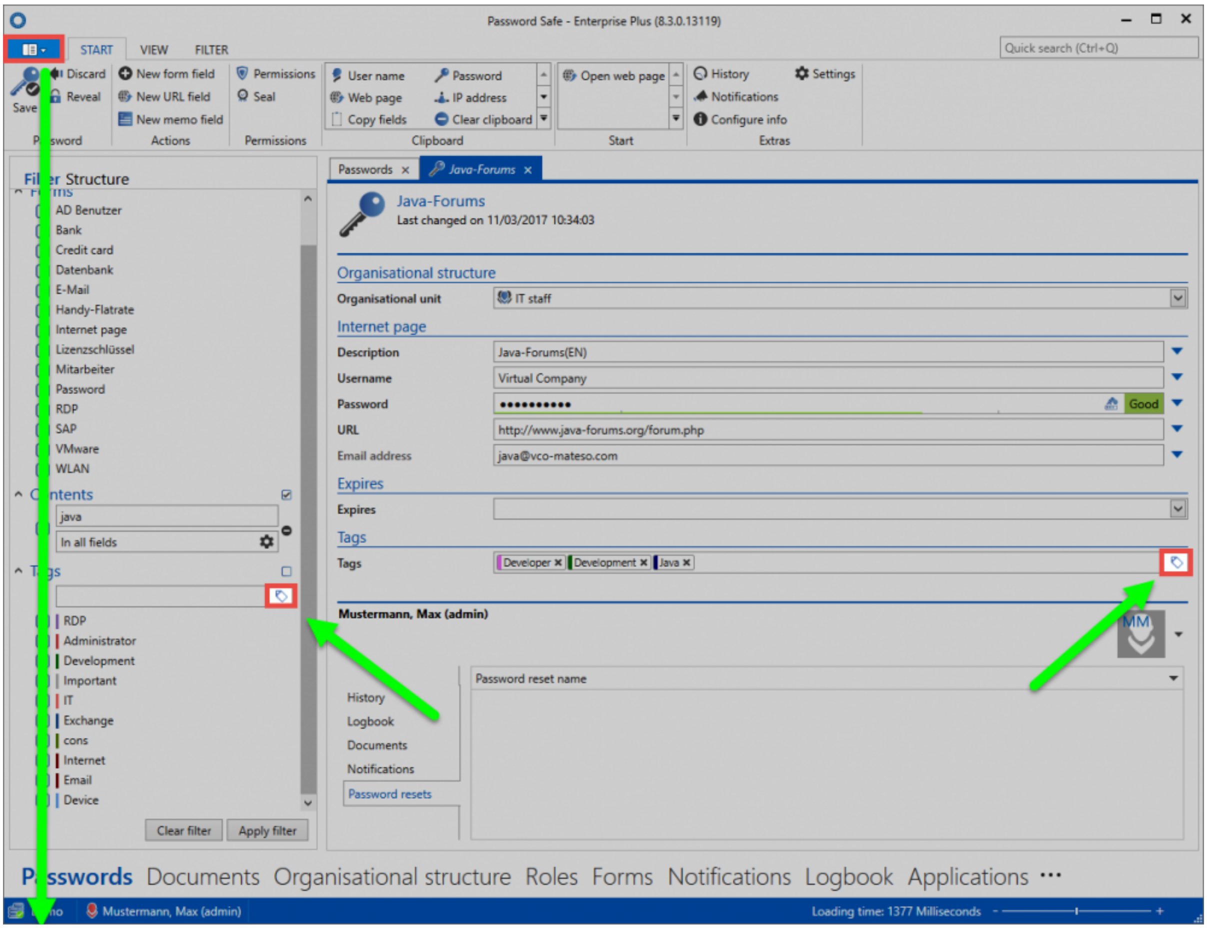
Reports
Managing all saved report requests. Adapt the request criteria and all of variables relevant to you to your individual processes.

System tasks
Use system tasks to automatically run processes at configurable intervals

Seal templates
Creation and management of seal templates. You also have the possibility of configuring permissions in templates.

Tag management
List of all available tags with the possibility of creating new tags and editing already existing ones

Icons
Aktuelle XAML Icons



Java-Forums
Last changed on 11/03/2017 10:34:03

Organisational structure

Organisational unit	IT staff

Internet page

Description	Java-Forums(EN)
Username	Virtual Company
Password	•••••••••• Good
URL	http://www.java-forums.org/forum.php
Email address	java@vco-mateso.com

Expires

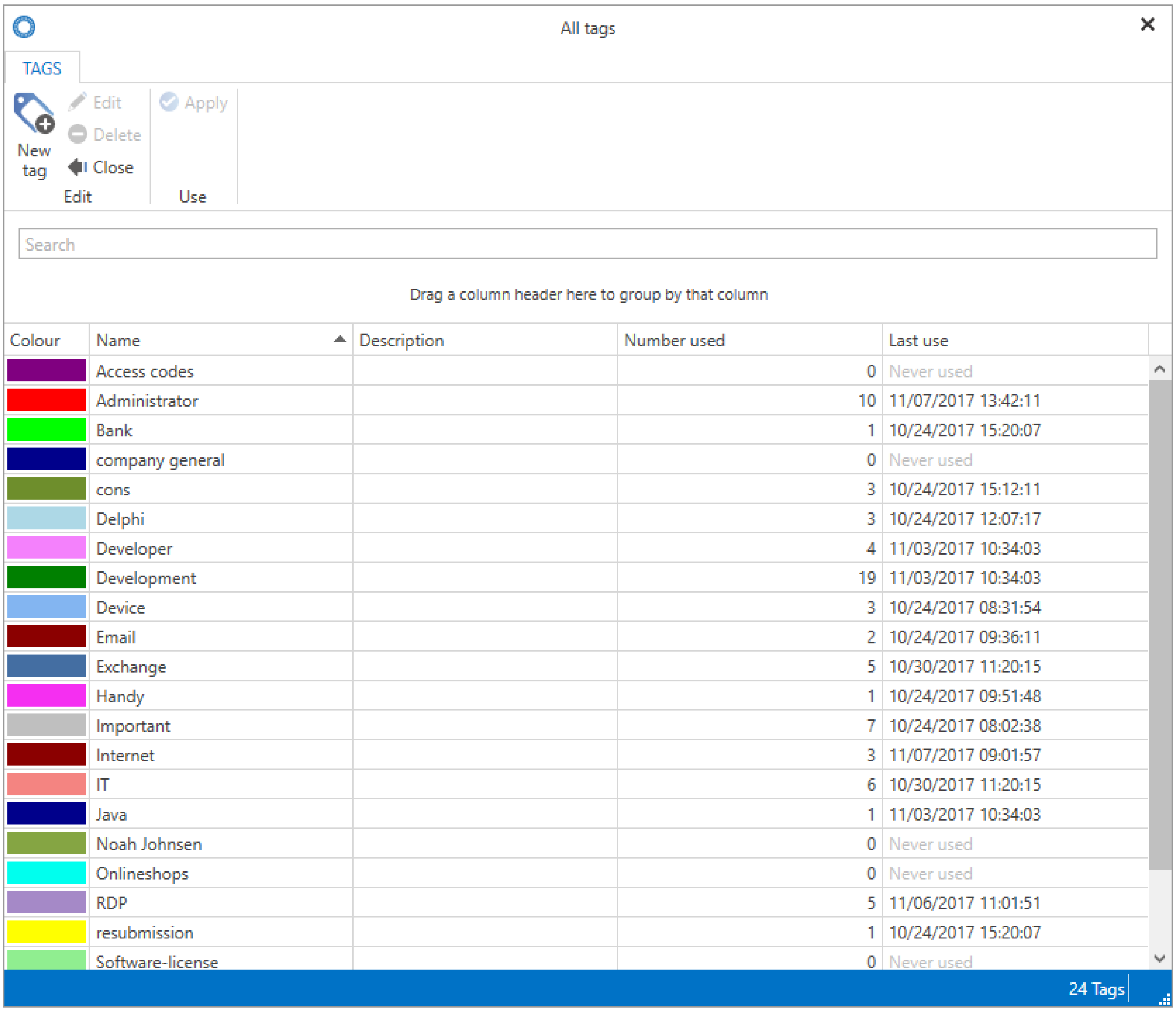
Expires	

Tags

Tags	Developer ✕ Development ✕ Java ✕

Mustermann, Max (admin)

The tag manager itself is a clearly structured tool with which you can view and edit all relevant information. The colours can also be assigned here. The “Number used” column indicates how often an object has been tagged with the tag. In this way, you can keep track of and remove tags that are no longer needed.



Colour	Name	Description	Number used	Last use
🟪	Access codes		0	Never used
🟥	Administrator		10	11/07/2017 13:42:11
🟩	Bank		1	10/24/2017 15:20:07
🟦	company general		0	Never used
🟩	cons		3	10/24/2017 15:12:11
🟦	Delphi		3	10/24/2017 12:07:17
🟪	Developer		4	11/03/2017 10:34:03
🟩	Development		19	11/03/2017 10:34:03
🟦	Device		3	10/24/2017 08:31:54
🟥	Email		2	10/24/2017 09:36:11
🟦	Exchange		5	10/30/2017 11:20:15
🟪	Handy		1	10/24/2017 09:51:48
⬜	Important		7	10/24/2017 08:02:38
🟥	Internet		3	11/07/2017 09:01:57
🟥	IT		6	10/30/2017 11:20:15
🟦	Java		1	11/03/2017 10:34:03
🟩	Noah Johnsen		0	Never used
🟦	Onlineshops		0	Never used
🟪	RDP		5	11/06/2017 11:01:51
🟨	resubmission		1	10/24/2017 15:20:07
🟩	Software-license		0	Never used

24 Tags

! The user right **tags** is required for managing tags. This right is one of the user rights.

! It is only possible to delete tags if there are no more data associated with them

General settings

What are general settings?

The **general settings** relate to users. Thus, each user can customize the software to their own needs. The following options can be configured:

Colour scheme

Various Windows colour schemes are available. The colour scheme **Colorful** provides e.g. different colours which make it easier to distinguish between the modules in the software. If the colour scheme is changed, the client must be restarted.

Language

The user can toggle between English and German. After changing the language, the client must be restarted.

Starting the application minimised in the notification area

You can start the client minimized if you wish to run Password Safe in the background. You will be able to access it through the notification area.

Minimise the application on closing

If this option has been activated, the Password Safe client will not end when the window is closed but will merely be minimised. It will continue to run in the background. It is then only possible to properly end Password Safe via the main menu.

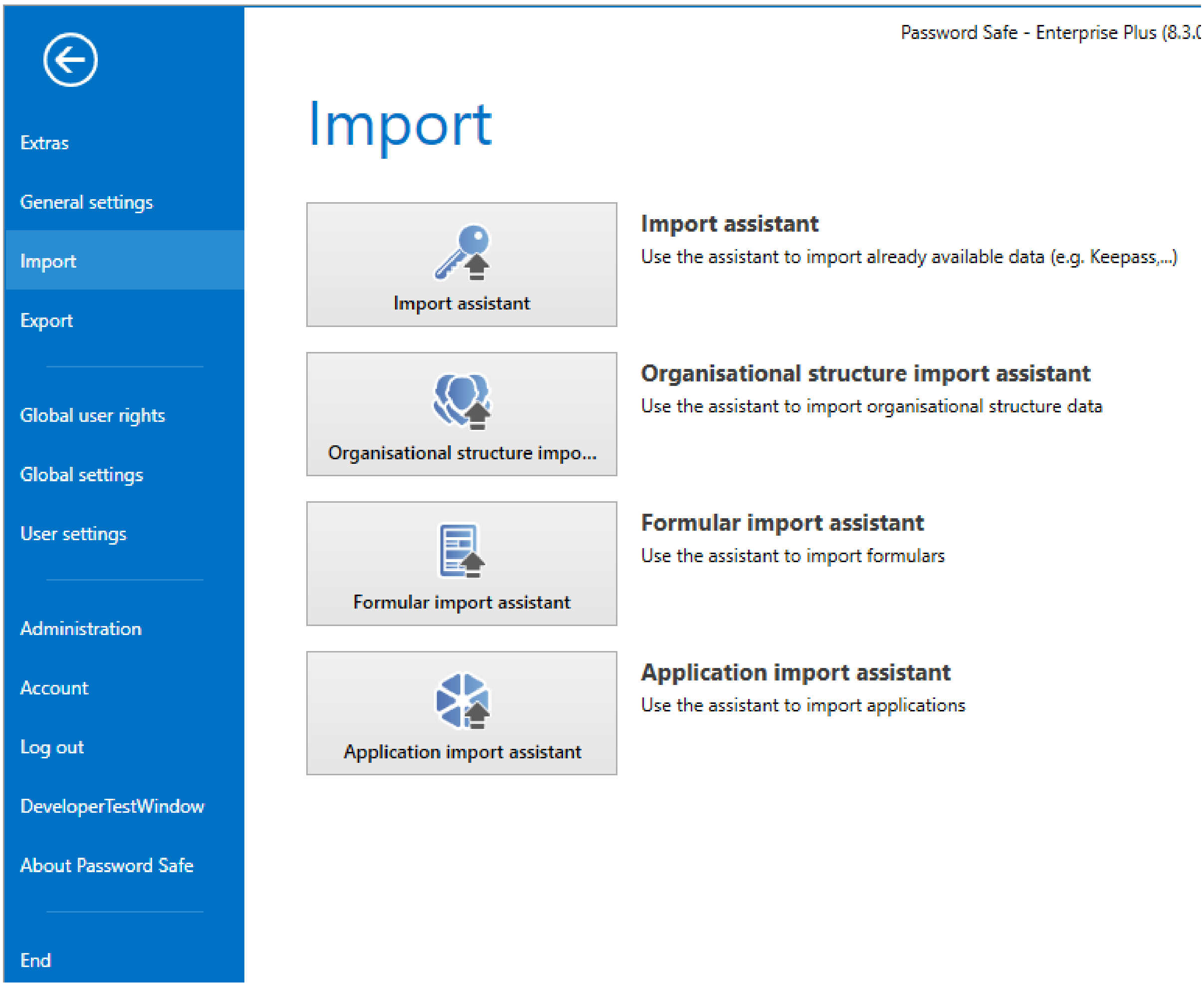
h4.Starting with Windows

Of course, you can start the Password Safe Client directly with Windows.

Import

What is an import?

If another password management tool was used before Password Safe, these data can be imported into Password Safe. The formats .csv and especially Keepass (.xml) are supported. Both variants can be set up in the import wizard, which is started via the Main menu/Import.



Import assistant
Use the assistant to import already available data (e.g. Keepass,...)

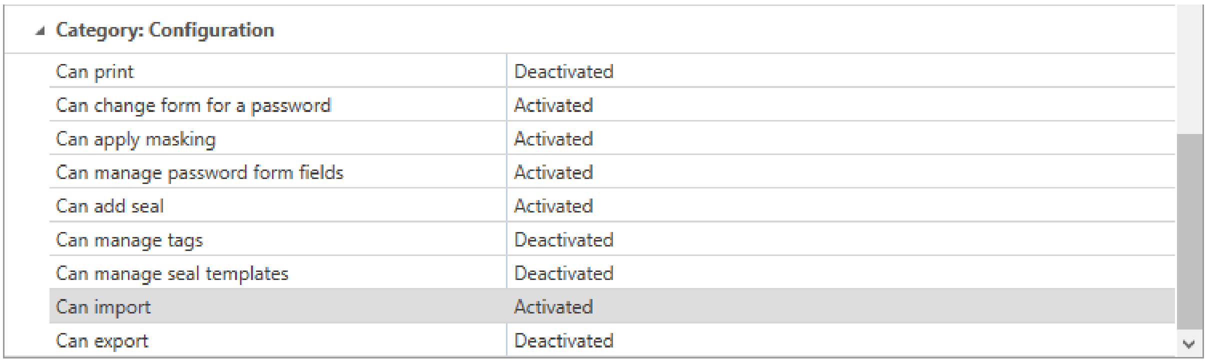
Organisational structure import assistant
Use the assistant to import organisational structure data

Formular import assistant
Use the assistant to import formulars

Application import assistant
Use the assistant to import applications

Requirements

Whether the user is permitted to import data is controlled by the corresponding user right.



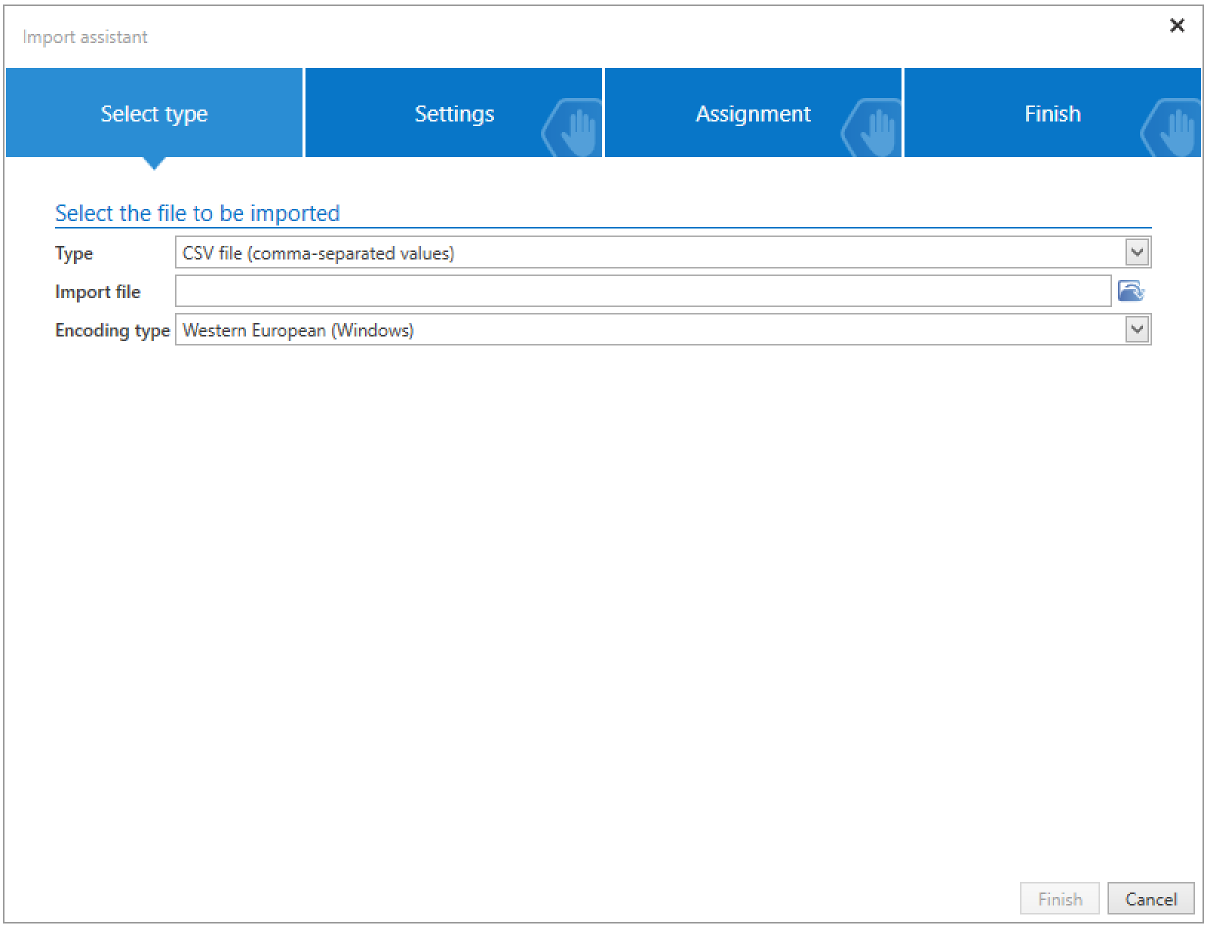
Category: Configuration

Can print	Deactivated
Can change form for a password	Activated
Can apply masking	Activated
Can manage password form fields	Activated
Can add seal	Activated
Can manage tags	Deactivated
Can manage seal templates	Deactivated
Can import	Activated
Can export	Deactivated

The import wizard

The wizard supports the import of data into Password Safe in four steps.

Select type



Select the file to be imported

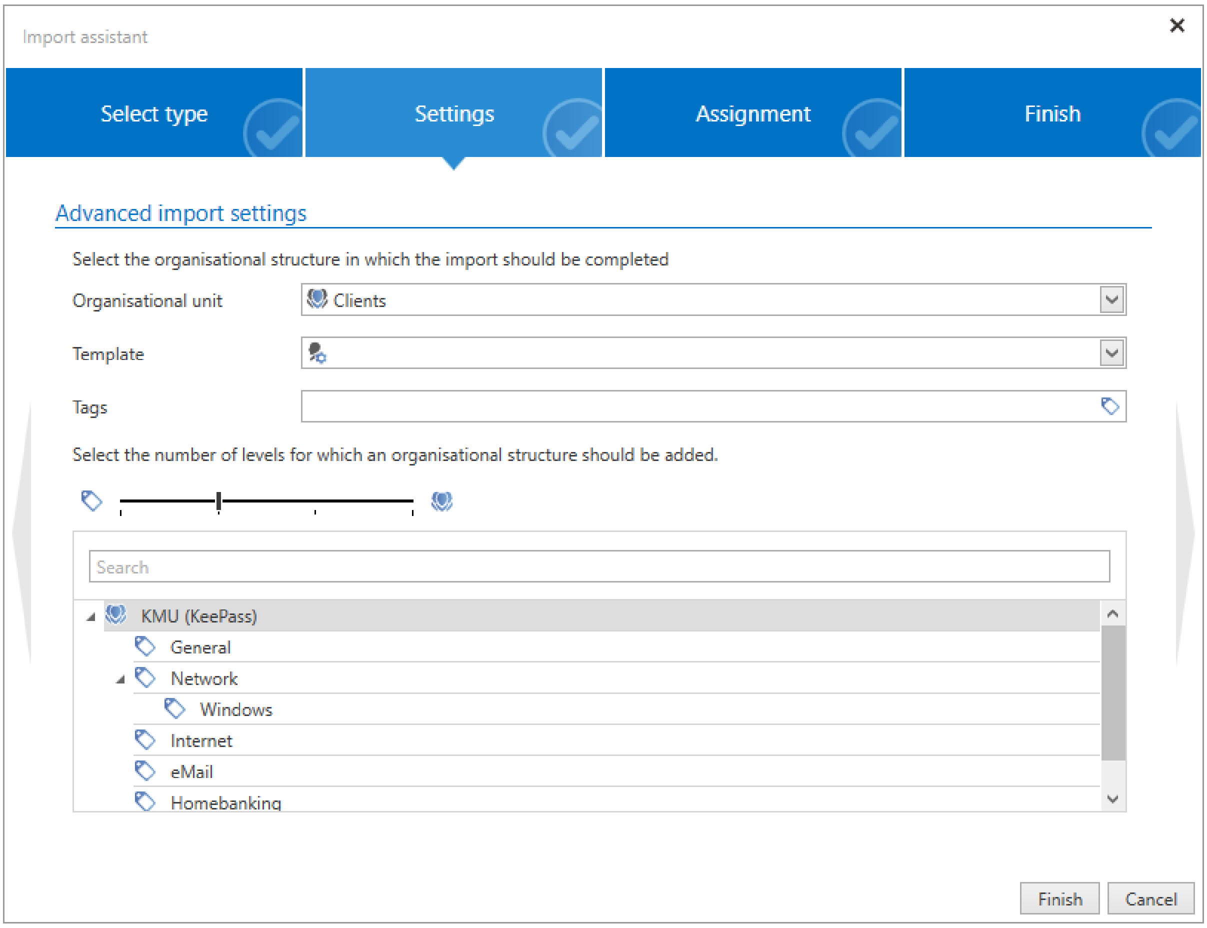
Type: CSV file (comma-separated values)

Import file:

Encoding type: Western European (Windows)

The first step is to define the file that is to be used for the import. It is only possible to proceed to the second step when the defined type corresponds to the stated file to be imported. The second step is the settings.

Settings



Import assistant

Advanced import settings

Select the organisational structure in which the import should be completed

Organisational unit: Clients

Template:

Tags:

Select the number of levels for which an organisational structure should be added.

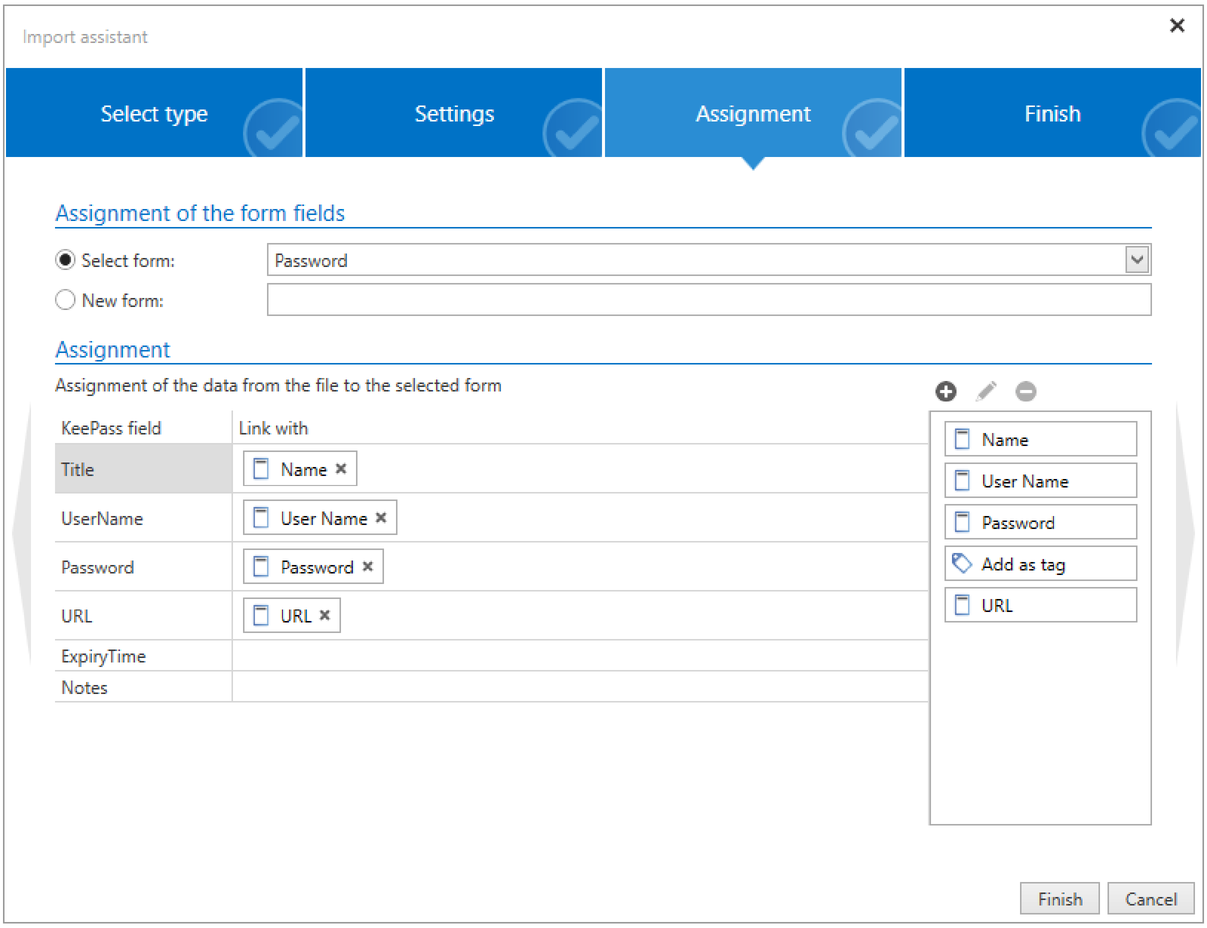
Search

- KMU (KeePass)
  - General
  - Network
    - Windows
  - Internet
  - eMail
  - Homebanking

1. The settings are used to firstly define the level in the hierarchy for saving the imported structure. As can be seen in the example, the import will take place in the main organisational unit. One of the existing organisational units can also be defined as a parent instance via the drop-down menu.
2. The slider defines whether the imported structures should be imported as an organisational unit or as a tag. If the slider is fully moved to the left, only tags are created. If it s moved to the right, all objects are imported as an organisational structure. In addition, every object can be configured separately via the context menu that is accessed using the right mouse button. It is also possible to ignore folders.

No folders exist in Password Safe. For this reason, it is necessary to define whether a folder is saved as an organisational structure or as a tag during the import. The same process is also used for the migration.

Assignment of the form fields



Assignment of the form fields

● Select form: Password

○ New form:

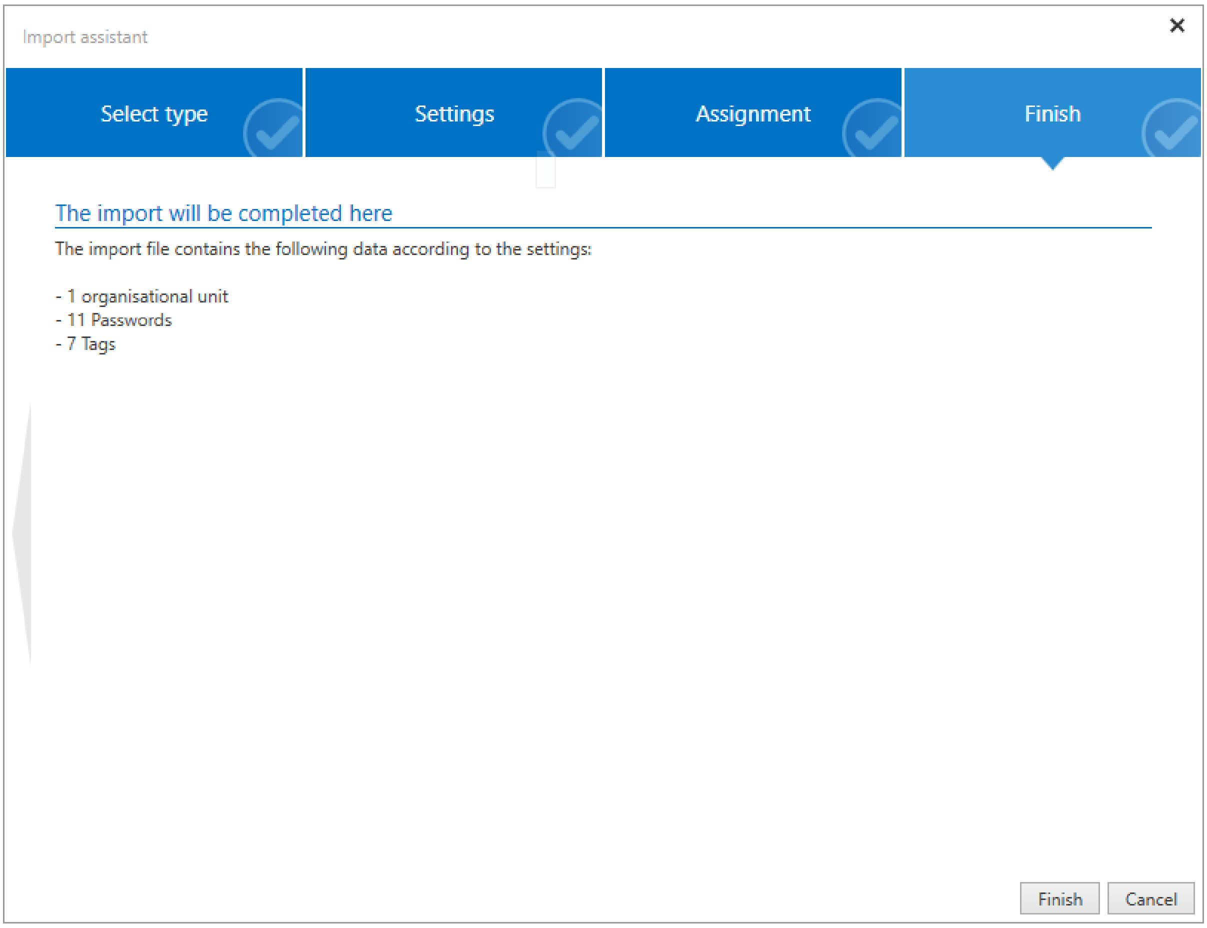
Assignment

Assignment of the data from the file to the selected form

KeePass field	Link with
Title	Name ✖
UserName	User Name ✖
Password	Password ✖
URL	URL ✖
ExpiryTime	
Notes	

The third step is to assign the forms from the file to be imported to already existing forms. As form fields may also have different names, the assignment process must be carried out manually via drag & drop. Depending on which form was selected on the top line, form fields from the list on the right can now be assigned to the form fields to be imported via drag & drop. It is also possible to create new forms.

Finish



The import will be completed here

The import file contains the following data according to the settings:

- 1 organisational unit
- 11 Passwords
- 7 Tags

In the final step, the configured settings are summarised as a list of the objects to be imported. The button “Finish” closes the wizard and starts the import.

Export

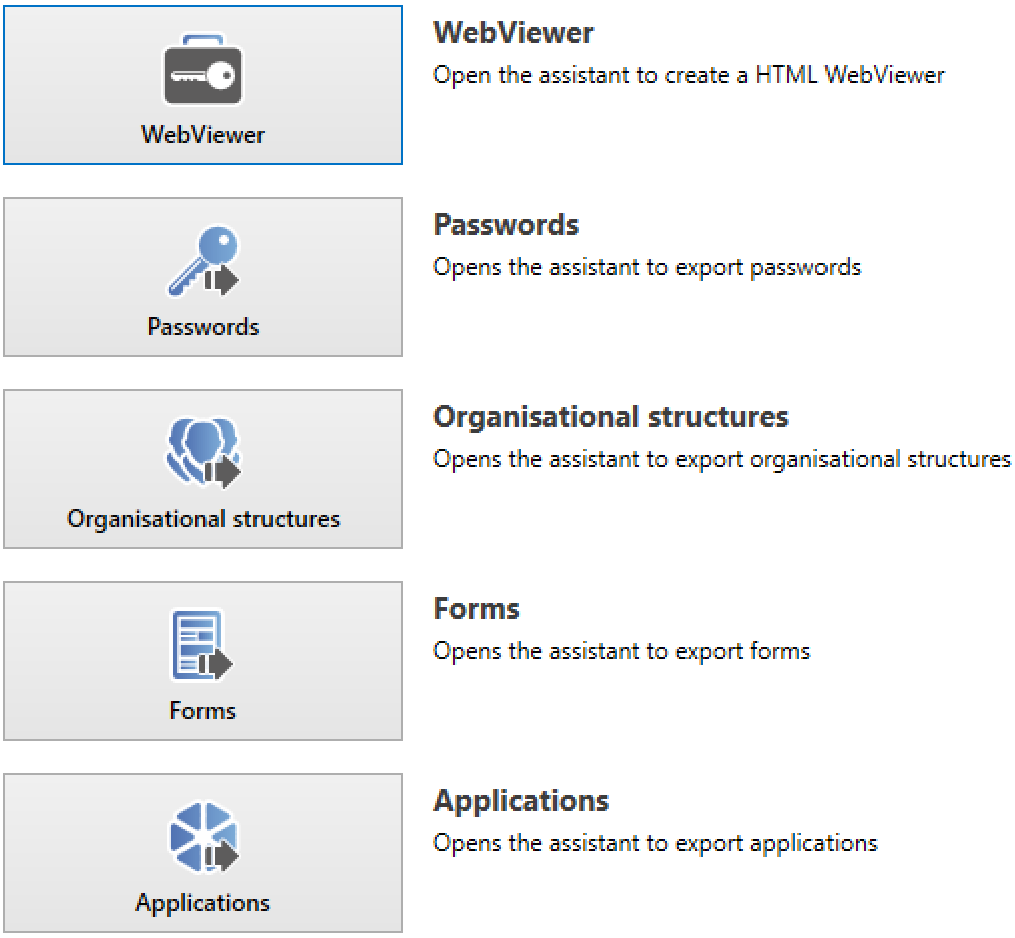
What is an export?

An export is used for extracting the data saved in the MSSQL database. Both selective (manual) and automated system tasks can extract information form Password Safe in this manner.

! Please note that extracting passwords is always associated with a weakening of the security concept. The informative value of the logbook will suffer when data is exported because the revision of this data will no longer be logged. This aspect needs to be taken into account particularly in conjunction with the Password Safe export wizard because the export result is not separately secured by a password.

The export function is accessed via the Main menu/Export. There are two fundamental types of export – the WebViewer export and the export wizard. However, the latter is divided into four subcategories.

Export



WebViewer

Open the assistant to create a HTML WebViewer

Passwords

Opens the assistant to export passwords

Organisational structures

Opens the assistant to export organisational structures

Forms

Opens the assistant to export forms

Applications

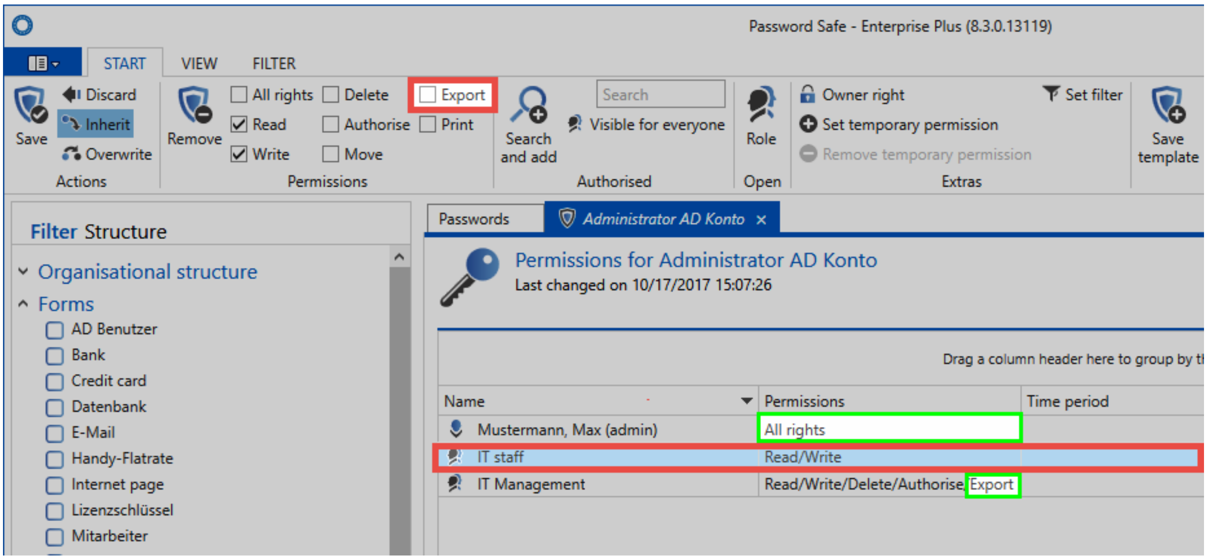
Opens the assistant to export applications

The WebViewer export creates a HTML file protected by a password. In contrast, the export wizard creates an open and unprotected .csv file.

Requirements

Permissions are used to define whether a record can be exported or not. Various protective mechanisms can be applied. Restrictions can be placed on either the record itself and also via user rights

- **The permissions for the record**: The permissions for the record define whether a record can be exported

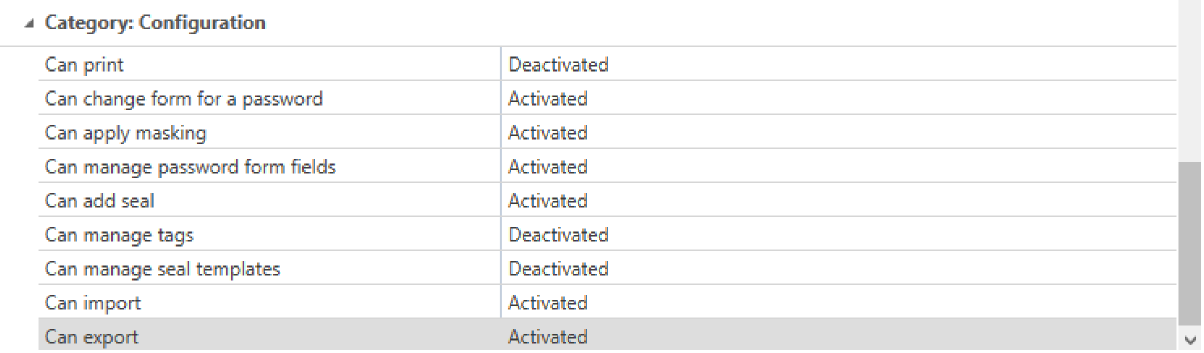


Permissions for Administrator AD Konto
Last changed on 10/17/2017 15:07:26

Name	Permissions	Time period
Mustermann, Max (admin)	All rights	
IT staff	Read/Write	
IT Management	Read/Write/Delete/Authorise/Export	

In this example, the marked role IT employee does not have the required permissions to export the record. In contrast, the IT manager does have the required permissions. In addition, the administrator possesses all rights, including the right to export.

- **The user right "Export"**: A user right is available in the "General" category that gives a user the right to export. If this right has not been granted, **no** form of export can generally be performed.



Category: Configuration

Can print	Deactivated
Can change form for a password	Activated
Can apply masking	Activated
Can manage password form fields	Activated
Can add seal	Activated
Can manage tags	Deactivated
Can manage seal templates	Deactivated
Can import	Activated
Can export	Activated

If a record is exported, this user right and also the corresponding permissions for the record must be set. The user right defines whether a user can **generally** export data, while the permissions for the record define **which** records can be exported.

HTML WebViewer export

What is a HTML WebViewer export?

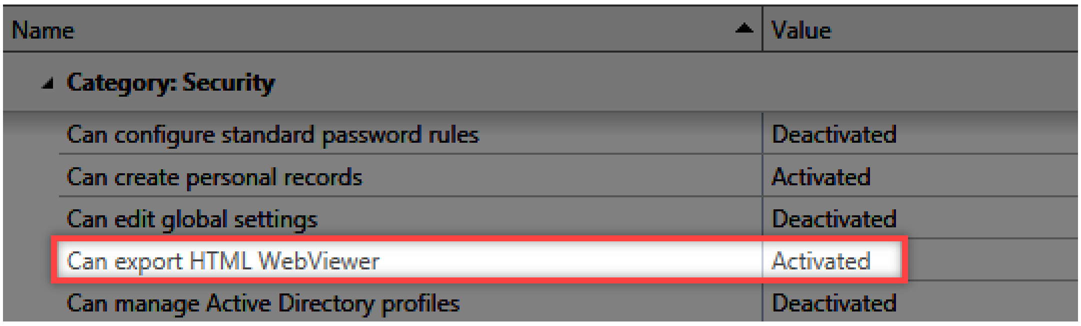
The * WebViewer * is an option in **Password Safe** for exporting **passwords** in an encrypted **HTML file**. The records are selected using the **filter function**. The passwords for which the user has the corresponding permissions are exported. They are displayed in a current browse that has **JavaScript activated**.

Data security

- Naturally, the HTML WebViewer file is encrypted
- The export itself is protected using a corresponding user right
- The user requires the **export right** for the passwords

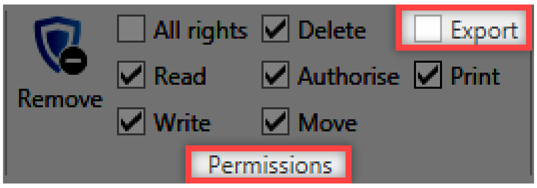
Required rights

The **export right for the WebViewer is configured via the *user rights**:



Name	Value
Category: Security	
Can configure standard password rules	Deactivated
Can create personal records	Activated
Can edit global settings	Deactivated
Can export HTML WebViewer	Activated
Can manage Active Directory profiles	Deactivated

The **export right** for the password is configured as normal via the ribbon:



Remove

□ All rights ☑ Delete □ Export

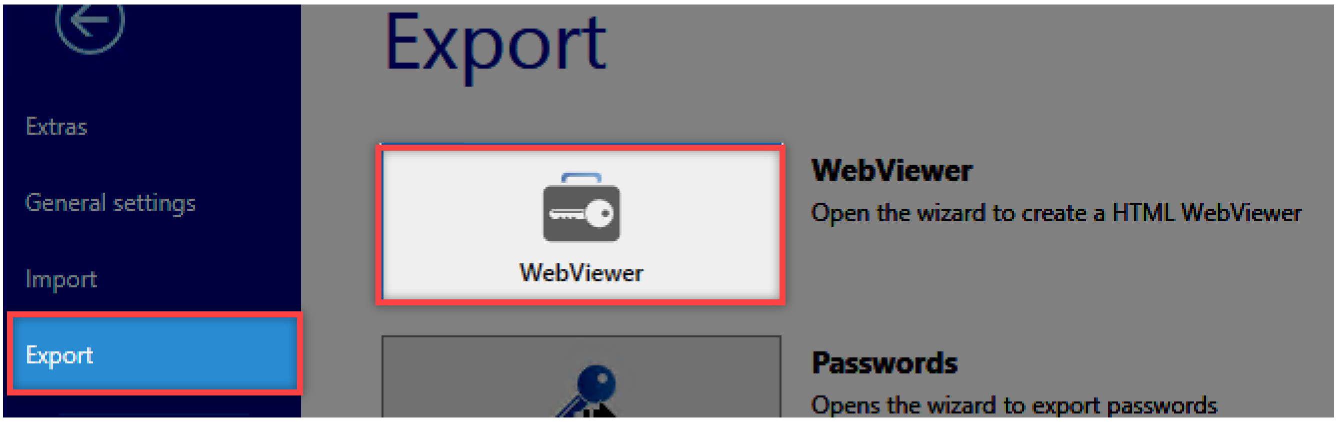
☑ Read ☑ Authorise ☑ Print

☑ Write ☑ Move

Permissions

Exporting a HTML file

The **HTML file** is created on the user*s client and started in the **Main menu** under **Export WebViewer**.


Export
Extras
General settings
Import
Export
WebViewer
WebViewer
Open the wizard to create a HTML WebViewer
Passwords
Opens the wizard to export passwords

The **HTML WebViewer Wizard** carries out the * WebViewer export*.

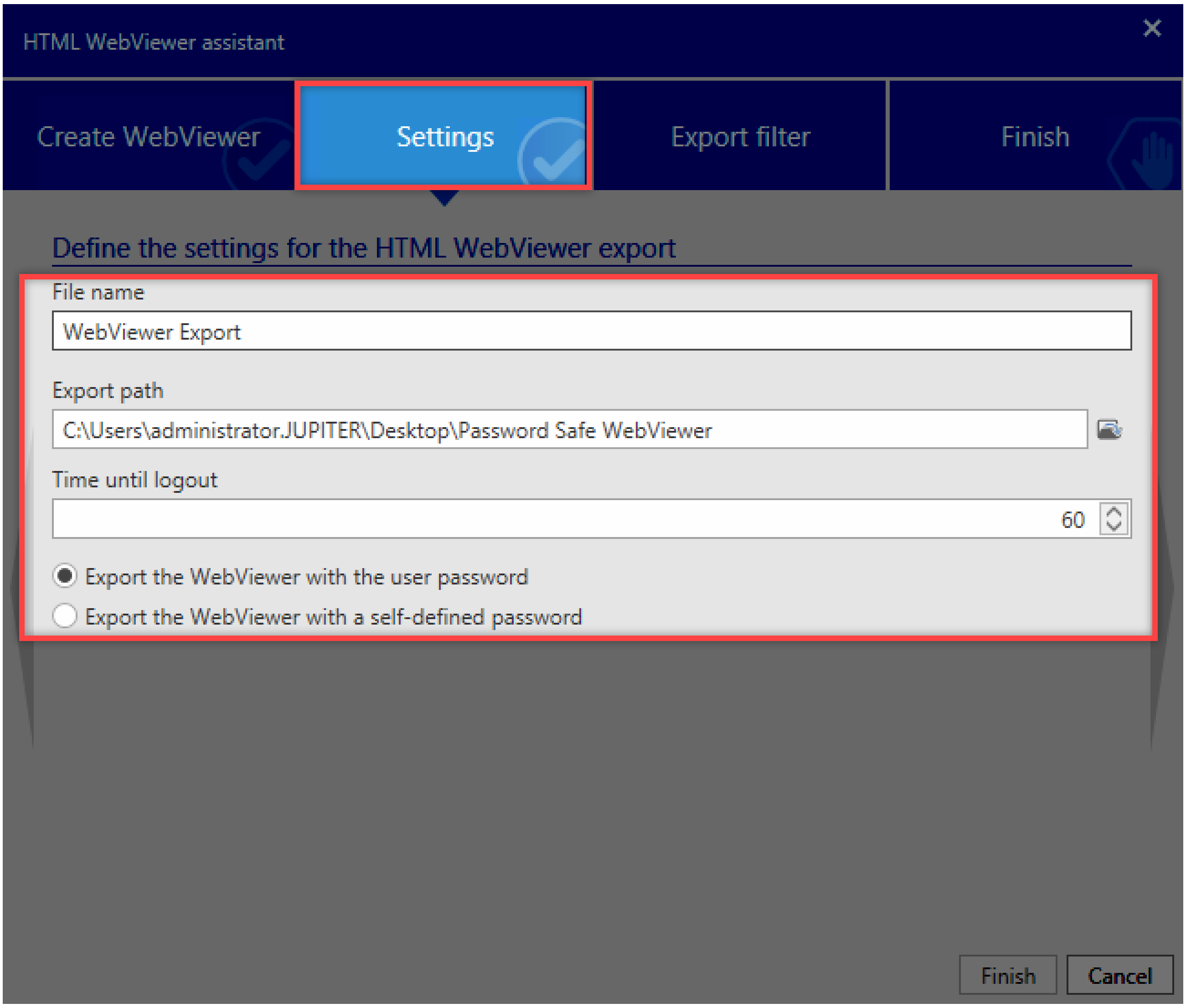
Create WebViewer

General information and notes about the export are displayed under **Create WebViewer**.

Settings

General information such as the **Name** and **Export path** for the **HTML file** can be entered here.

File name: Freely selectable name
Export path: Storage location for the file on the client
Time until logout: Time in seconds for which the window remains open without any activity
Standard value: 60 seconds, user can define the time
Export **WebViewer** with **user password** or new freely **definable password**: You can decide here whether to issue a new password for the export.



Define the settings for the HTML WebViewer export

File name: WebViewer Export

Export path: C:\Users\administrator.JUPITER\Desktop\Password Safe WebViewer

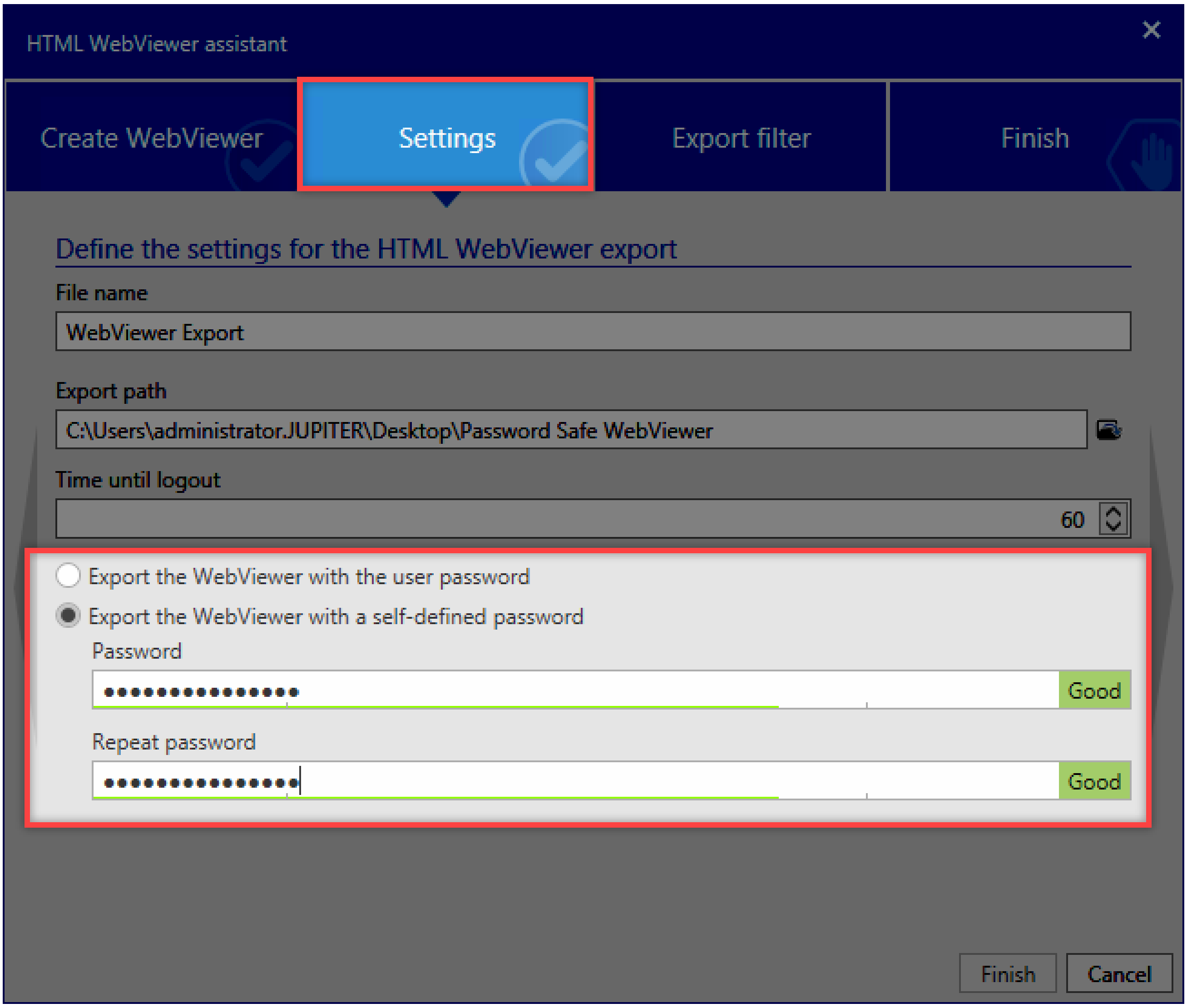
Time until logout: 60

● Export the WebViewer with the user password

○ Export the WebViewer with a self-defined password

WebViewer export with an Active Directory user

If an **Active Directory user** is carrying out the **WebViewer export**, a **password** needs to be explicitly entered.



Define the settings for the HTML WebViewer export

File name: WebViewer Export

Export path: C:\Users\administrator.JUPITER\Desktop\Password Safe WebViewer

Time until logout: 60

○ Export the WebViewer with the user password

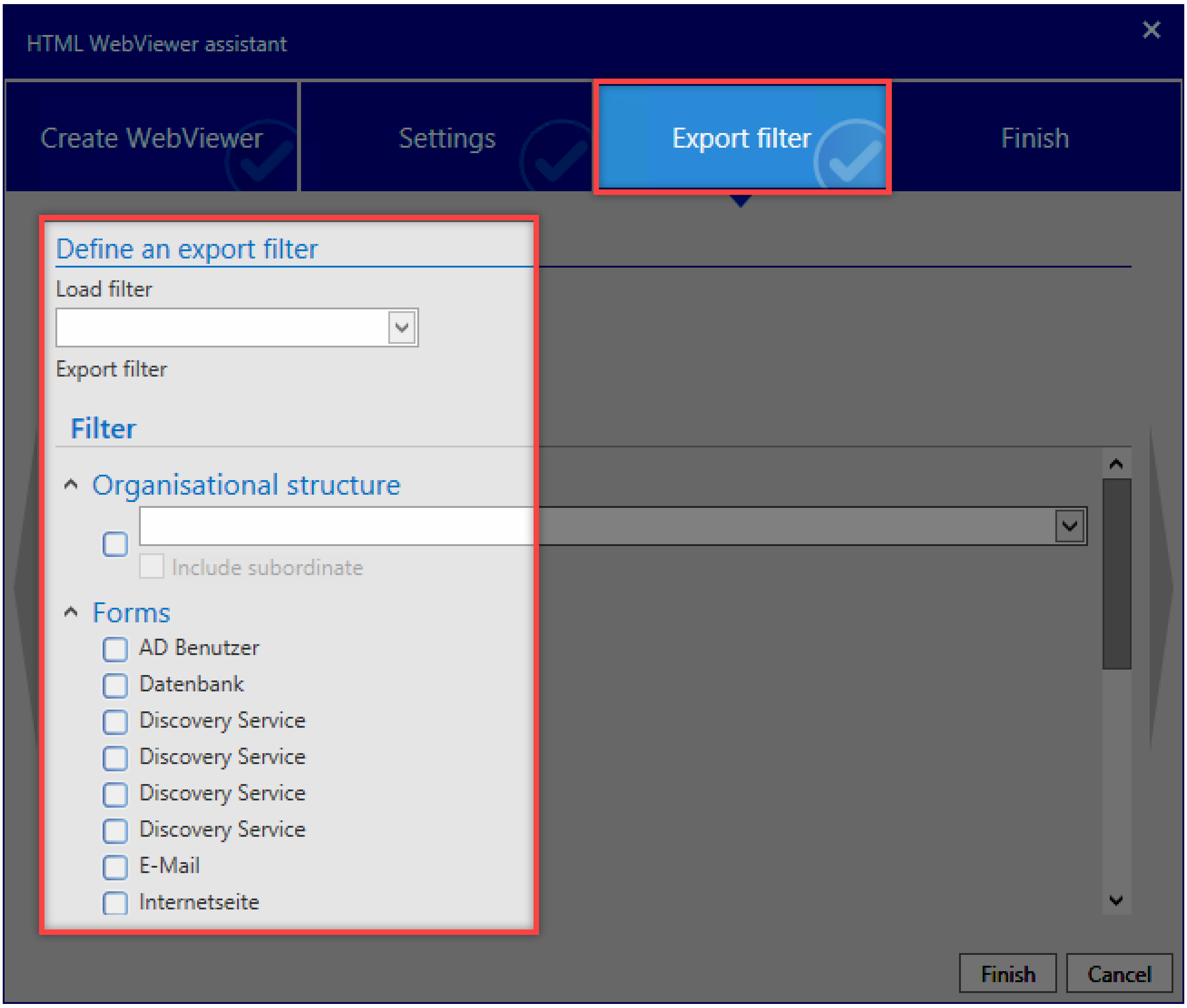
● Export the WebViewer with a self-defined password

Password: ••••••••••••••• Good

Repeat password: ••••••••••••••• Good

Export filter

The export filter works in the same way as the filters for the modules.



Define an export filter

Load filter

Export filter

Filter

Organisational structure

□

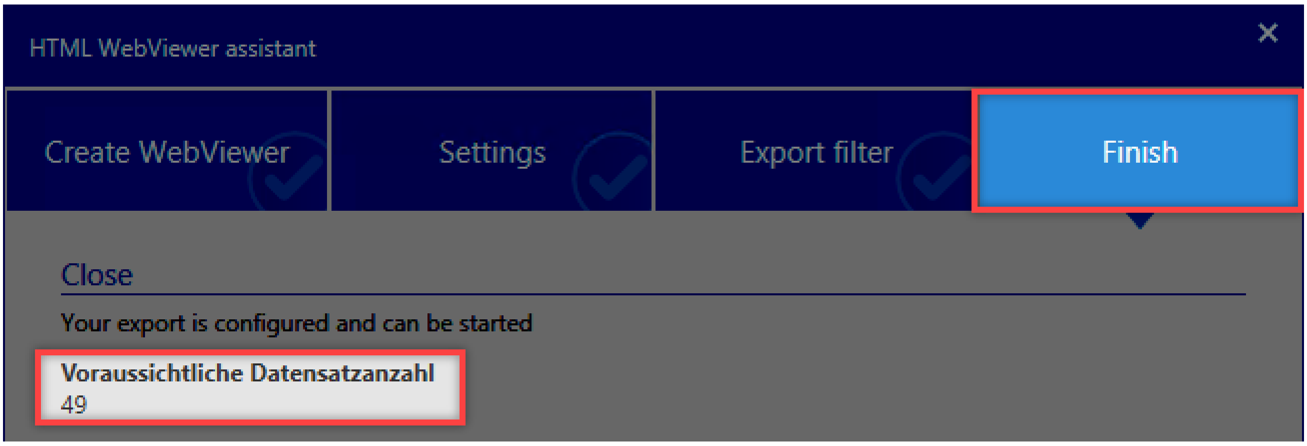
□ Include subordinate

Forms

□ AD Benutzer
□ Datenbank
□ Discovery Service
□ Discovery Service
□ Discovery Service
□ Discovery Service
□ E-Mail
□ Internetseite

Finish

The information about the exported passwords is displayed in the **Finish** ribbon. Clicking on the **Finish** button will then create the **HTML file** in the export path and close the window.

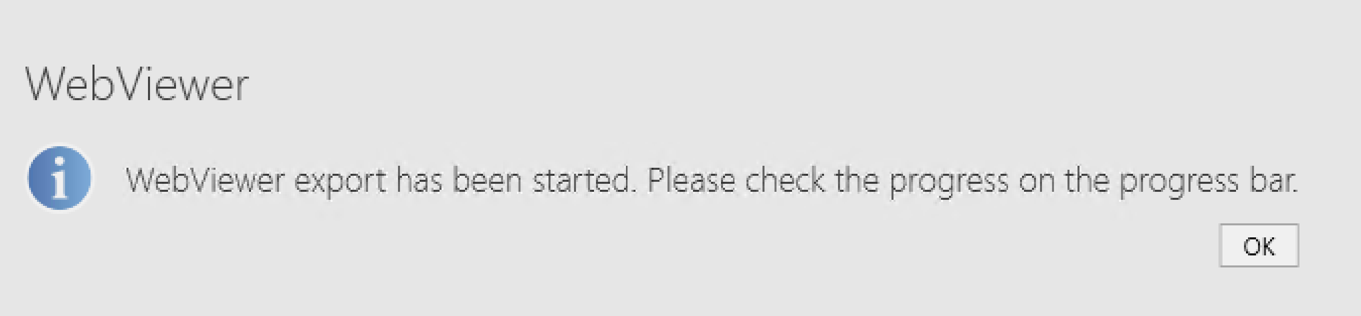


Close

Your export is configured and can be started

Voraussichtliche Datensatzanzahl
49

A subsequent note provides you with information about the export process.



WebViewer

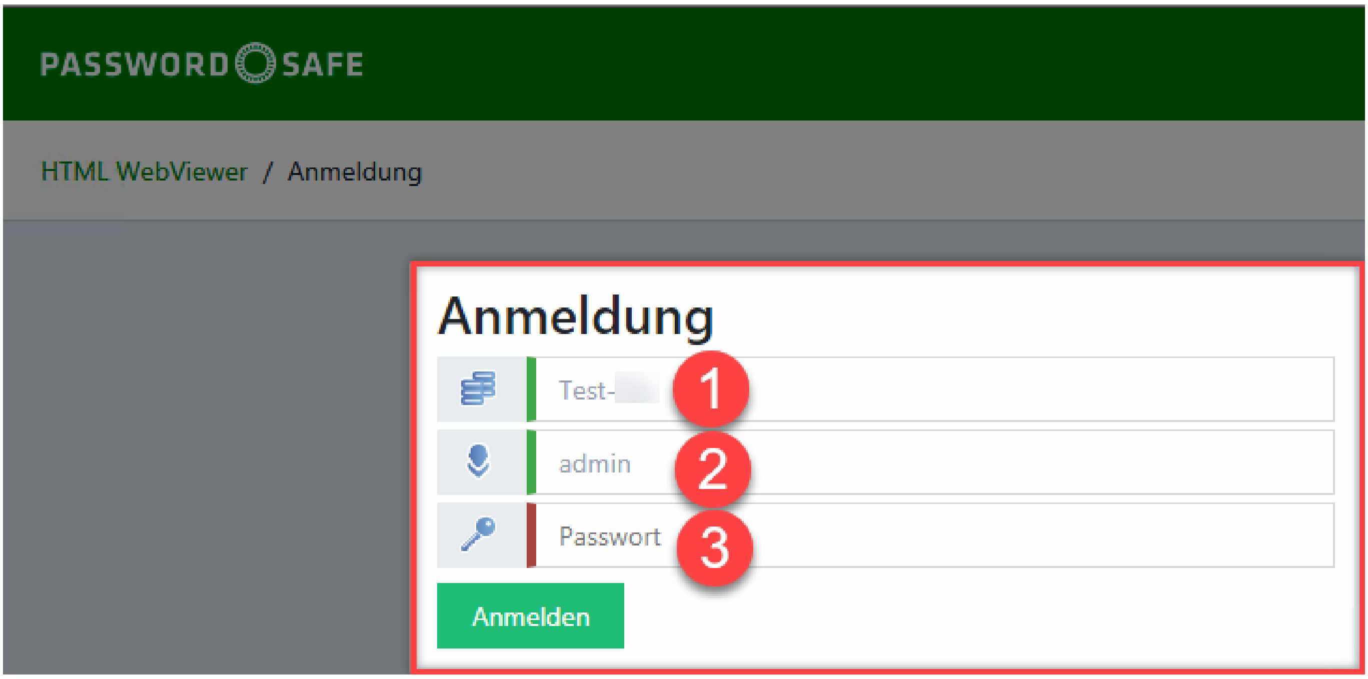
WebViewer export has been started. Please check the progress on the progress bar.

Using the HTML WebViewer file

The **HTML file** is created in the export path and can be copied to a mobile data medium (USB stick, external HDD, …). The **HTML file** can be opened in a standard browser and displays the **Password Safe – HTML WebViewer / Login** when started. The **database** and the **user name** are predefined. The user *password is used for the login.

! The login mask is blocked for a period of time if the password is incorrectly entered!

1. Database: Predefined
2. User: Predefined
3. Password: **Entered by the user**

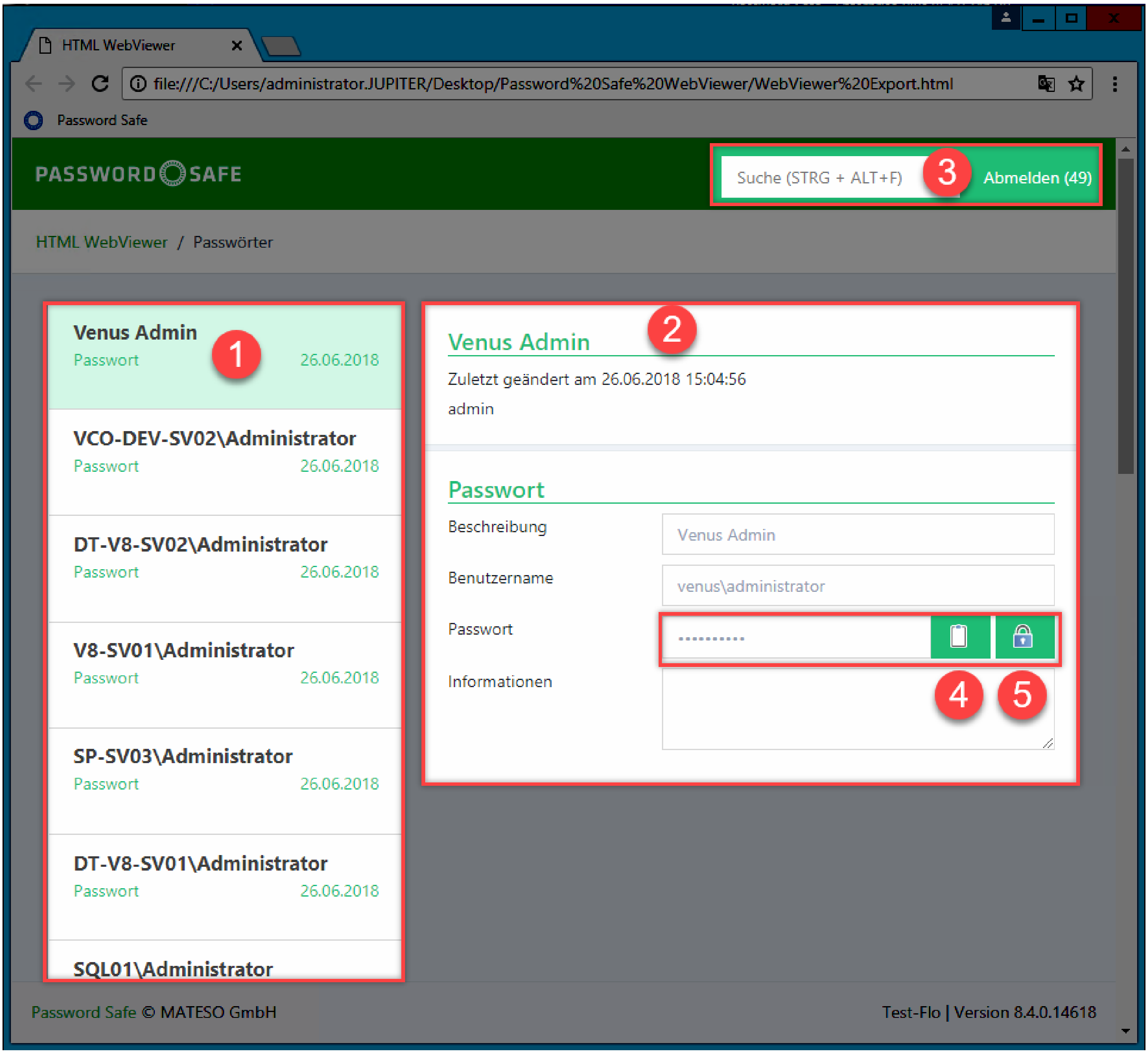


Overview

After logging in to **Password Safe**, the overview page for the *HTML- WebViewer * with the passwords is displayed.

> Use the password search function in the event of more than 20 passwords!

1. Display of the records (max. 20)
2. Detailed information on the selected record
3. Search, logout, timeout
4. Copy to clipboard
5. Reveal



Closing the HTML WebViewer overview

You can log out by clicking on **Logout**. In the event of a longer period of **inactivity, the user will be *automatically logged out after a set period of time has expired *(time until logout)**.

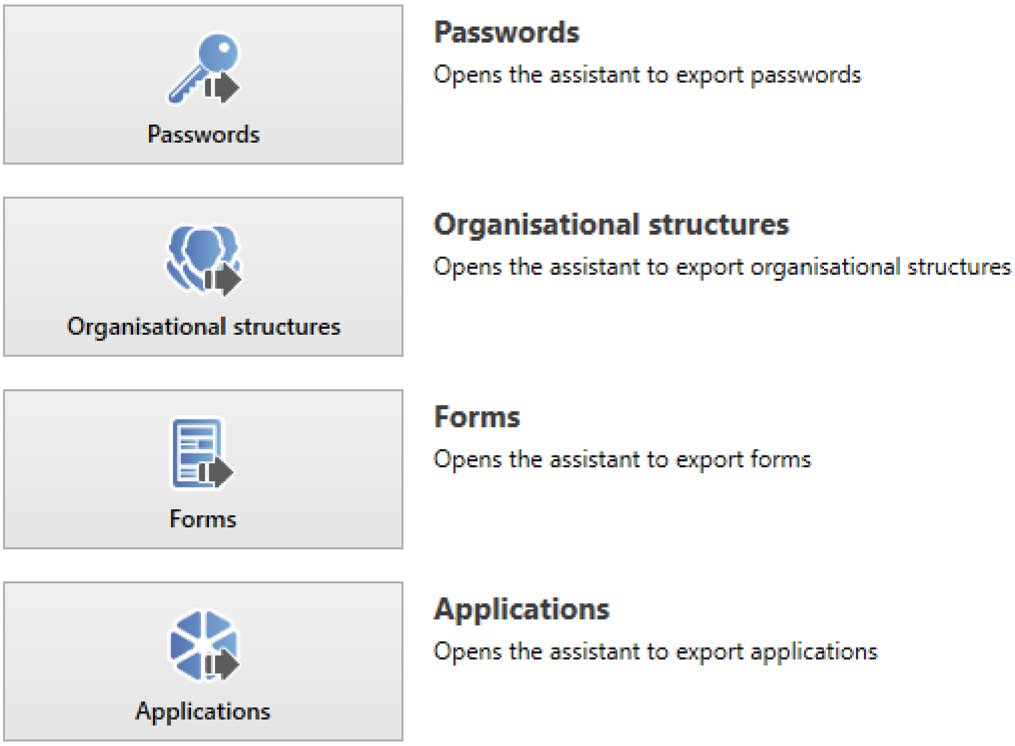
> ✻ You have been logged out due to inactivity.

The browser will then show the **Password Safe – HTML WebViewer / Login** again and also the reason for being logged out. It is possible to log in again.

Export wizard

What export wizards are there?

There are a total of four different export wizards.



Passwords
Opens the assistant to export passwords

Organisational structures
Opens the assistant to export organisational structures

Forms
Opens the assistant to export forms

Applications
Opens the assistant to export applications

The functionality of these wizards only differs based on the data to be exported. A distinction is made between passwords, organisational structures, forms and applications. **As all four wizards are handled in the same way, the following section will only describe the password export wizard**. The remaining three wizards function in the same way.

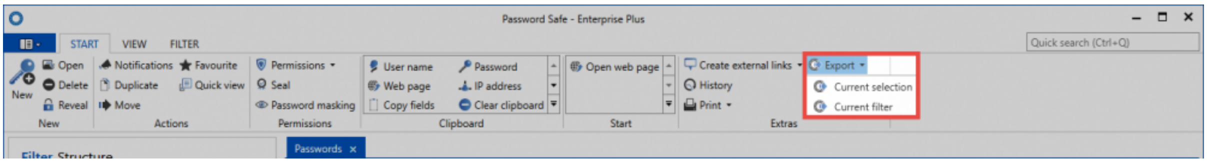
What is the password export wizard?

This wizard allows records to be exported in standard.csv format. In contrast to the WebViewer export, the resulting file is not protected by a password. It goes without saying that this feature must be used carefully.

Starting the password export wizard

The export wizard can be accessed in a variety of different ways:

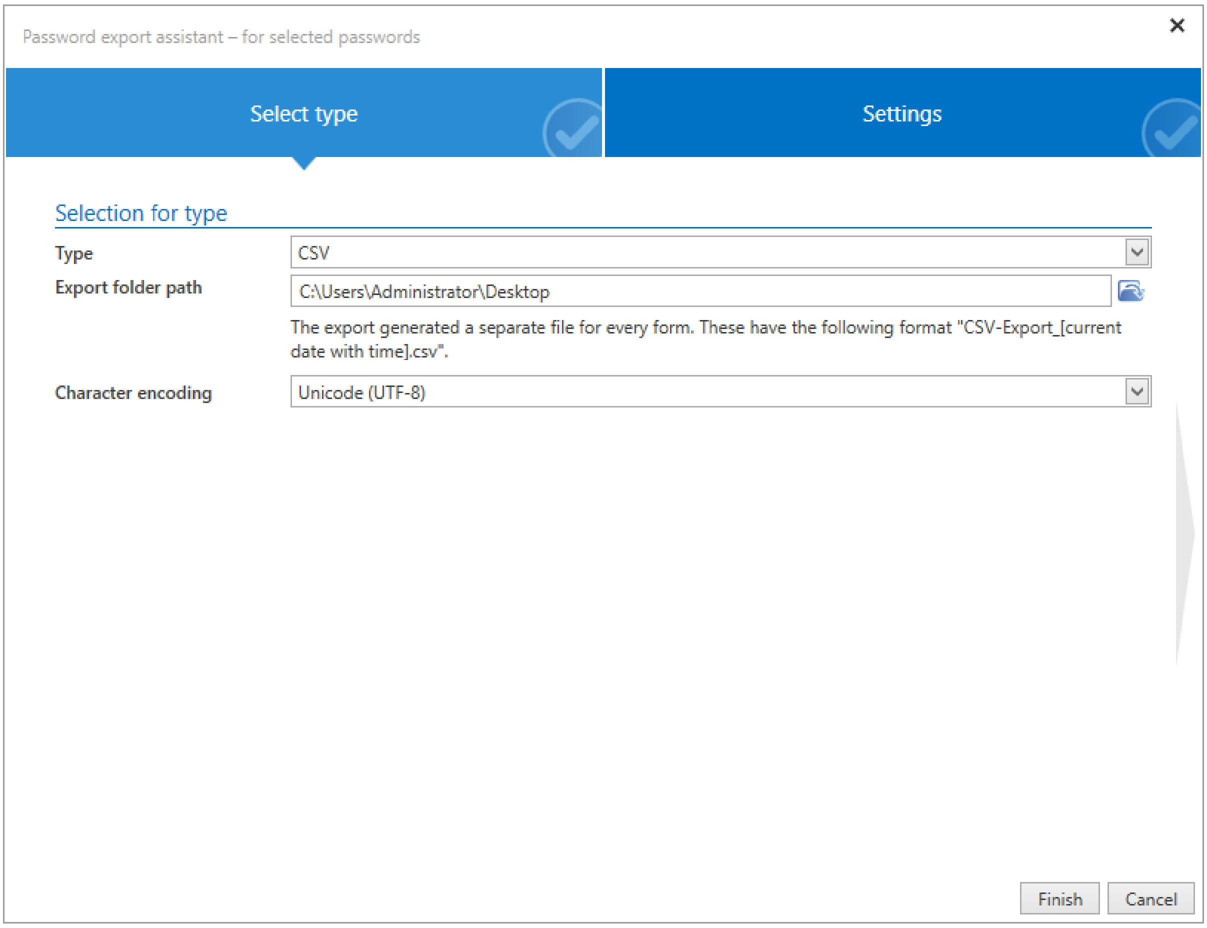
- **Starting via Main menu/Extras**: If the wizard is opened, the export will include all passwords for which the registered user has the required permissions. If the user is an administrator with permissions for all records, the export will include all passwords in the database.
- **Starting via the ribbon**: The export can also be started via the ribbon in the password module.



The password export wizard can be started via the ribbon in two ways. **Selected passwords** exports only those passwords marked in list view, whereby **Passwords based on the filter** uses the currently defined filter settings as the criteria.

The wizard

A diverse range of variables for the export and the storage location can be defined in the wizard. A corresponding preview is also provided.



Password export assistant – for selected passwords

Selection for type

Type	CSV
Export folder path	C:\Users\Administrator\Desktop
	The export generated a separate file for every form. These have the following format "CSV-Export_[current date with time].csv".
Character encoding	Unicode (UTF-8)

Once the wizard has been completed, the desired export is created and saved to the defined storage location.

! It is important to once again point out the sensitive nature of this export function that could have critical consequences from a security perspective. As the required permissions for this export are generally only granted to users/roles with higher positions in the hierarchy, this subject is even more relevant from a security perspective: It is possible to export all passwords for which a user has the required permissions. Administrators could thus (intentionally or unintentionally) cause more damage per se.

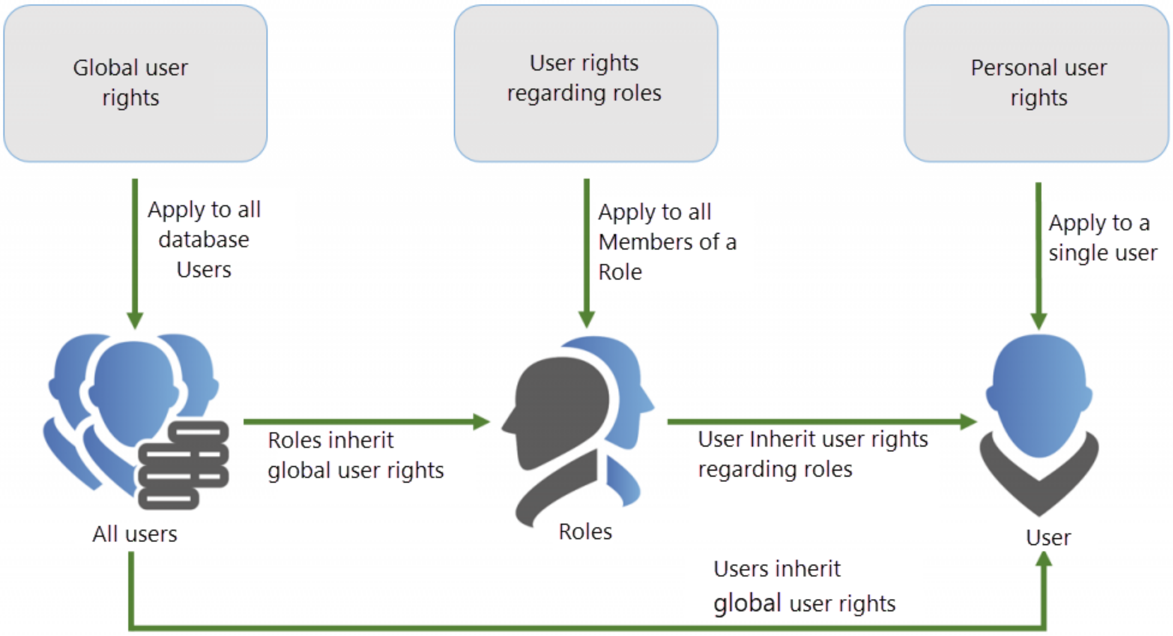
User rights

What are user rights?

In the user rights, access to functionalities is configured. Amongst tother things, this category includes both the visibility of individual modules, as well as the use of the import, export or management of rights templates functions. A complete listing is directly visible in the user rights.

Administration of user rights

Managing all user rights exclusively at the level of the user would be a time intensive process and thus require a disproportionate amount of care and maintenance. In the same way as with the authorization concept, an approach can be used in which several users are grouped together. Nevertheless, it must still be possible to additionally address the specific requirements of individual users. Some functionalities, on the other hand, should be available to all users. In order to do this, Password Safe offers a three-step concept.


Global user rights
User rights regarding roles
Personal user rights
Apply to all database Users
Apply to all Members of a Role
Apply to a single user
All users
Roles inherit global user rights
Roles
User Inherit user rights regarding roles
User
Users inherit global user rights

When it comes to user rights, the focus is always on the user. The user can receive user rights in one of the following three ways:

1. The **personal user right** only applies to a specific user. This is always configured via the organisational structure module.

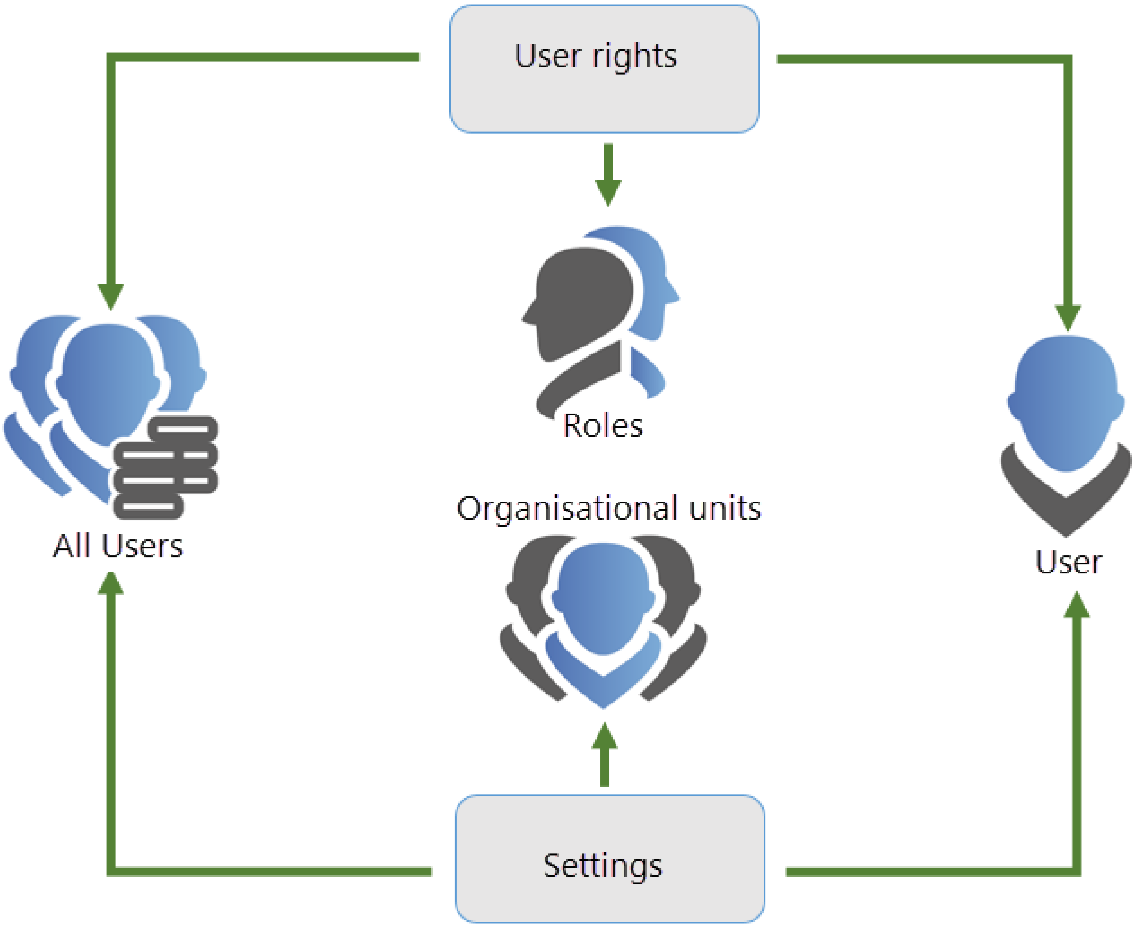
User rights to roles apply to all members of a role and are specified in the roles module

1. The **global user right** applies to all users of a database without exception. You can configure it in the client settings.

How a user receives a user right is irrelevant. The only important thing is that the user actually receives a required right in one of the three ways mentioned above. It is recommended that you link user rights to roles and, if necessary, supplement them with global user rights.

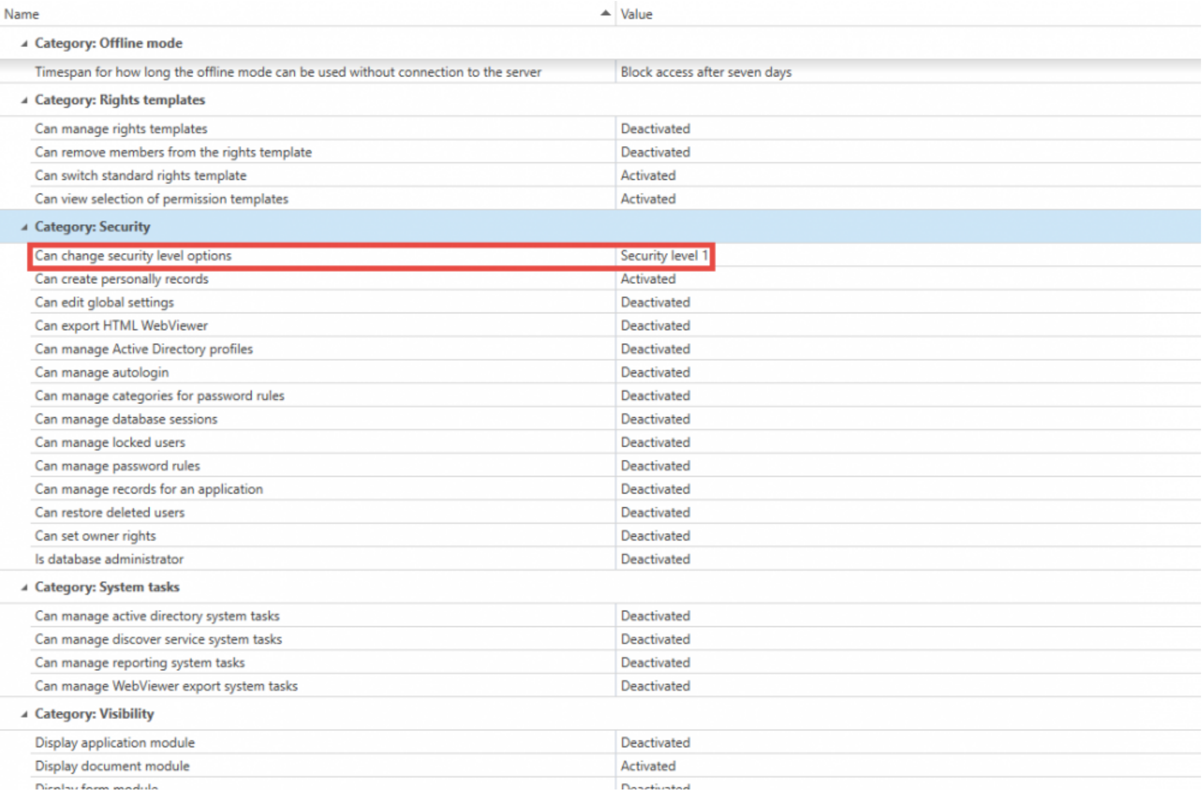
! In addition to personal and global user rights (as opposed to settings), user rights are assigned via roles and not via organisational units!

✻ Only those user rights that the current user possesses themselves can be issued. However, all rights can be removed.



Configuring the security level

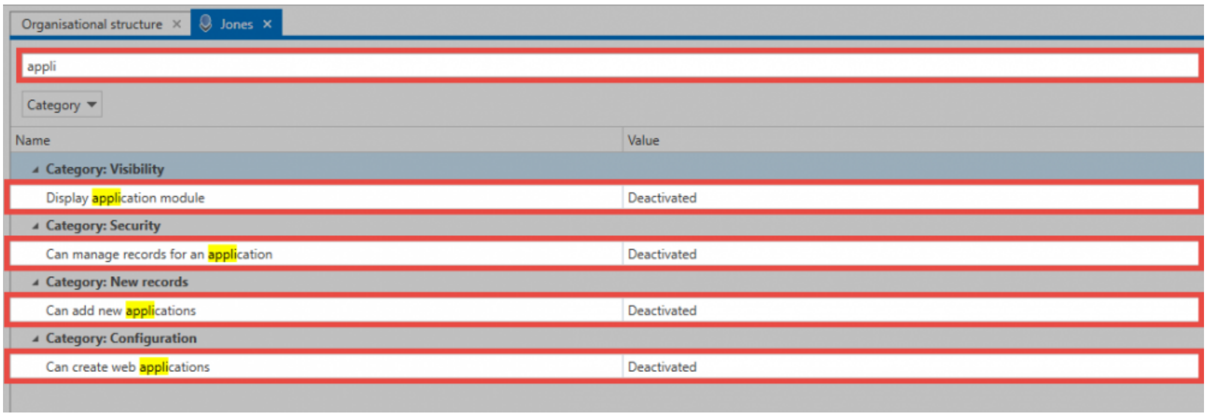
The **security level** is an essential element that is also specified in the user rights. This is the basis for the configuration of the user settings.



Name	Value
Category: Offline mode	
Timespan for how long the offline mode can be used without connection to the server	Block access after seven days
Category: Rights templates	
Can manage rights templates	Deactivated
Can remove members from the rights template	Deactivated
Can switch standard rights template	Activated
Can view selection of permission templates	Activated
Category: Security	
Can change security level options	Security level 1
Can create personally records	Activated
Can edit global settings	Deactivated
Can export HTML WebViewer	Deactivated
Can manage Active Directory profiles	Deactivated
Can manage autologin	Deactivated
Can manage categories for password rules	Deactivated
Can manage database sessions	Deactivated
Can manage locked users	Deactivated
Can manage password rules	Deactivated
Can manage records for an application	Deactivated
Can restore deleted users	Deactivated
Can set owner rights	Deactivated
Is database administrator	Deactivated
Category: System tasks	
Can manage active directory system tasks	Deactivated
Can manage discover service system tasks	Deactivated
Can manage reporting system tasks	Deactivated
Can manage WebViewer export system tasks	Deactivated
Category: Visibility	
Display application module	Deactivated
Display document module	Activated
Display form module	Deactivated

Searching within user rights

Due to the large number of possible configurations, the search function helps you to quickly find the desired configuration. This process is based as usual on the list search.



appli

Name	Value
Category: Visibility	
Display application module	Deactivated
Category: Security	
Can manage records for an application	Deactivated
Category: New records	
Can add new applications	Deactivated
Category: Configuration	
Can create web applications	Deactivated

Database administrator

Special attention should be given to the right **Is database administrator**. This right has the following effects:

- The user can also issue rights that he does not possess himself.
- The user can only have their rights removed by other database administrators.

- The user can unlock other users on the AdminClient.

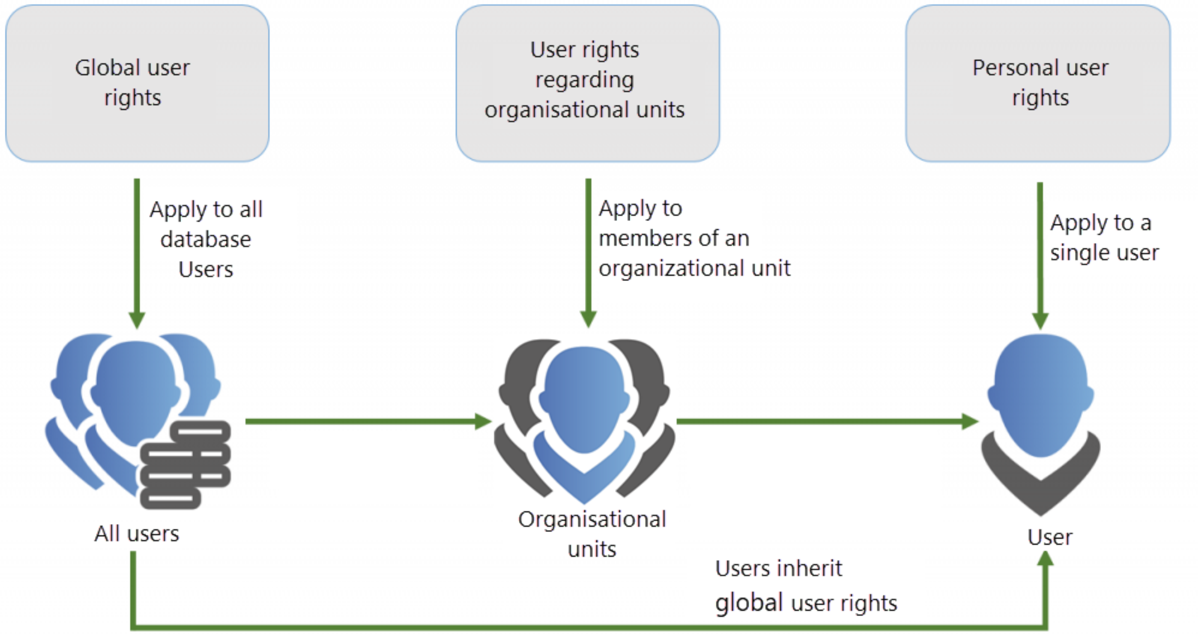
User settings

What are user settings?

There are many functions within Password Safe that can be adapted to the needs of users. It is also possible to define various parameters for optical representations. This can be inherited both at * user level *, * global * and * organisational units *. In addition, there is a security level concept, which categorizes the users into five layers. The administration of settings can thus be linked to the presence of the required security level.

Managing user settings

You can configure user settings similarly to user rights. Here too, there are a total of three possibilities with which a user can define his settings or be configured from another location. For the sake of easy manageability, it is again a good idea to configure the users not individually, but to provide several equal users with settings.

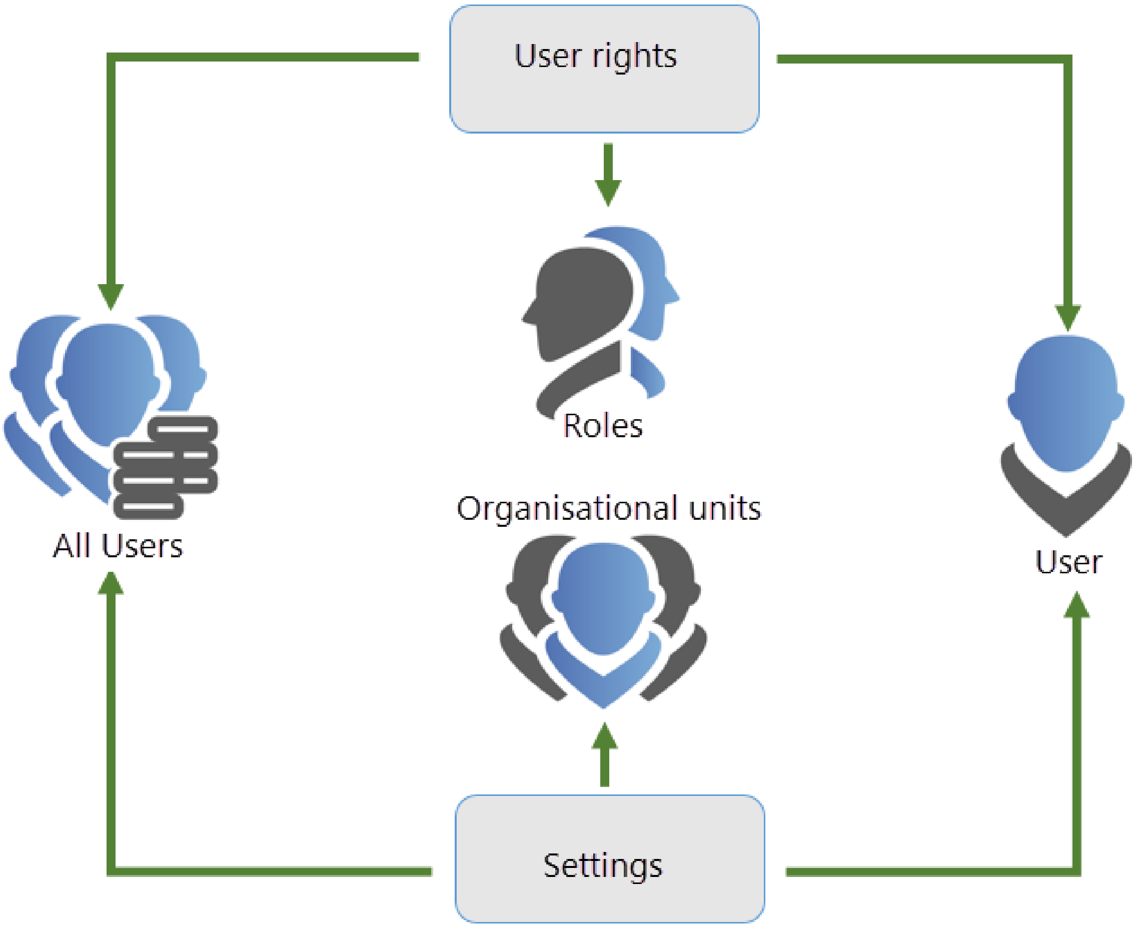

Global user rights
User rights regarding organisational units
Personal user rights
Apply to all database Users
Apply to members of an organizational unit
Apply to a single user
All users
Organisational units
User
Users inherit global user rights

The focus is always on the user, also when it comes to user rights. It can obtain its settings in one of the following three ways:

1. **Personal settings** only apply to a specific user. These are always configured via the organisational structure module.
2. **Settings for organisational structures** apply to all members of a role, and are specified in the organisational structure module

3. **Global settings** apply to all users of a database without exception. You can configure them in the client settings.

! In addition to personal and global settings (as opposed to authorizations), settings are not assigned via roles, but via organisational units!

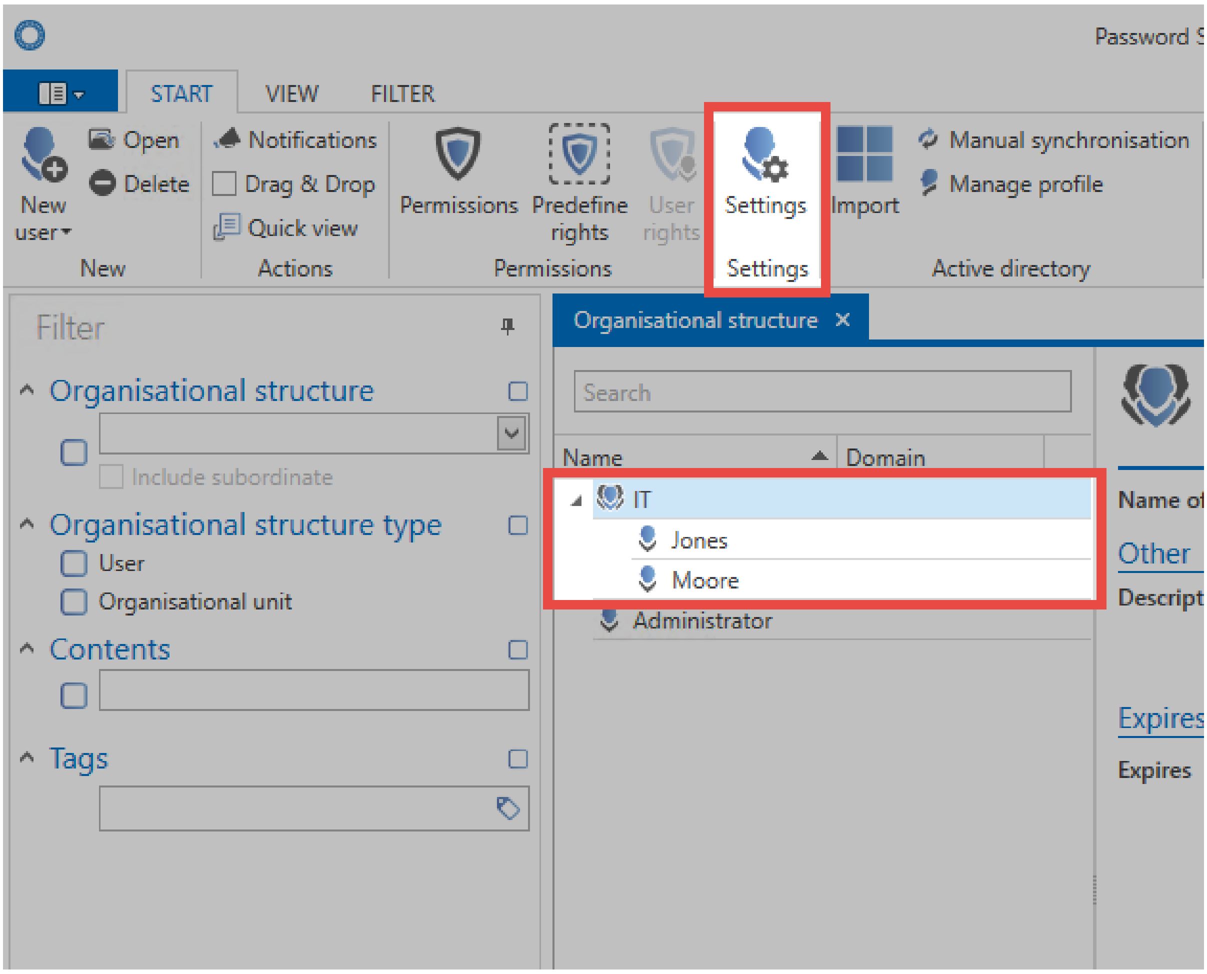


Inheritance of user settings

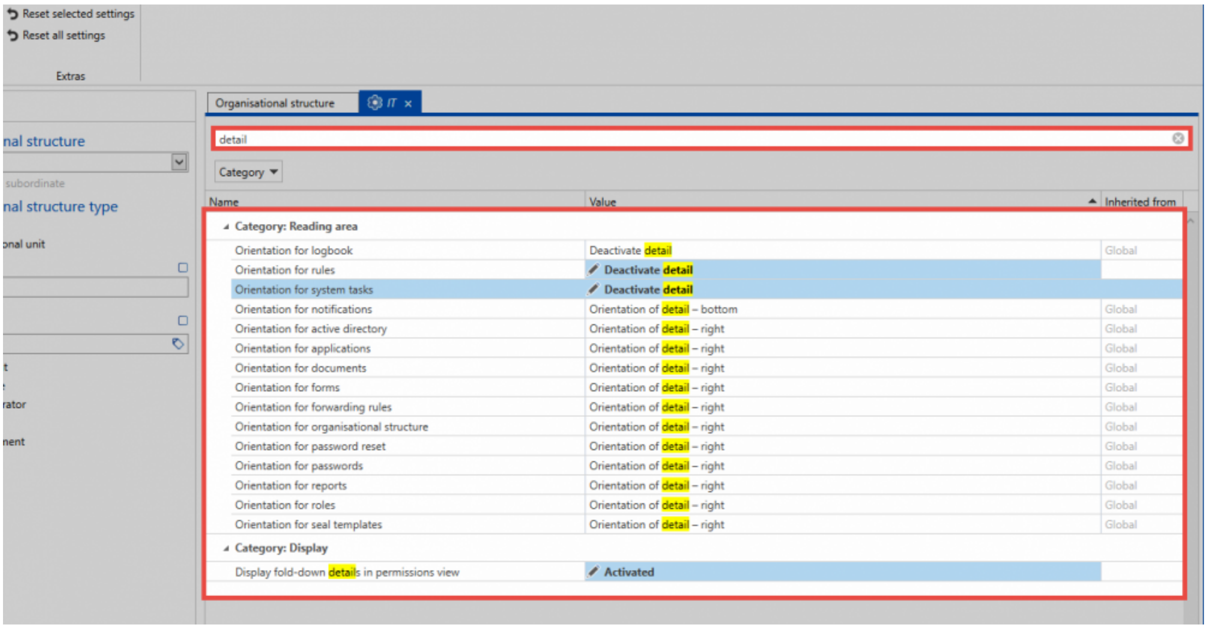
If you leave the personal settings on the outside, there are two ways to inherit settings:

1. Global inheritance
2. Inheritance on the basis of membership in organisational units (OU)

Global settings are configured as usual in the client settings. The organisational units are inherited via the organisational structure module. All users who are assigned to an organisational unit inherit all user settings for this OU. In the present case, the users “Jones” and “Moore” inherit all settings from the “IT” organisational unit:



The “Settings” button in the ribbon allows you to see the settings for both organisational units and users. The many setting options can be restricted by the known search mechanisms.



detail

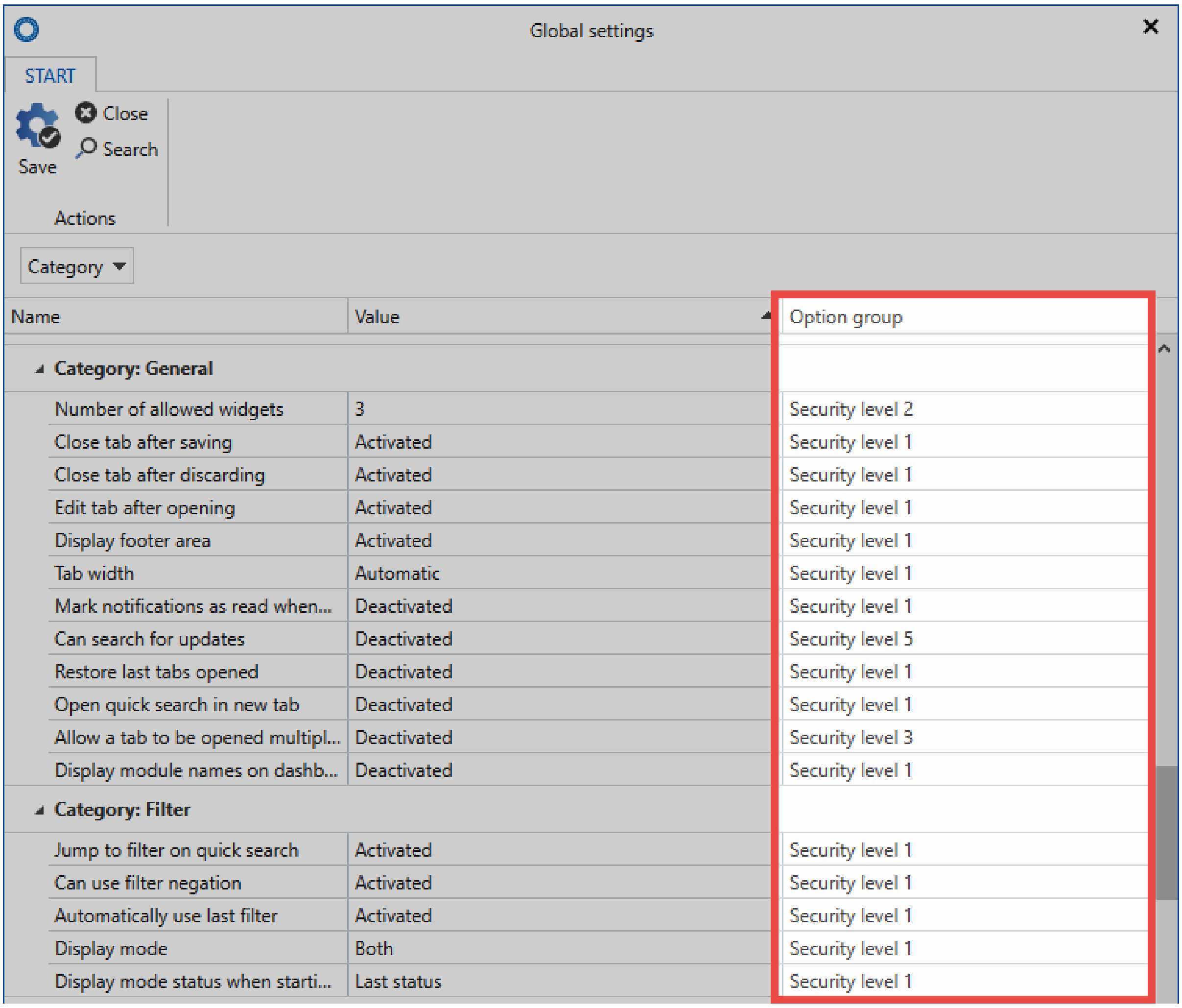
Name	Value	Inherited from
Category: Reading area		
Orientation for logbook	Deactivate detail	Global
Orientation for rules	Deactivate detail	
Orientation for system tasks	Deactivate detail	
Orientation for notifications	Orientation of detail – bottom	Global
Orientation for active directory	Orientation of detail – right	Global
Orientation for applications	Orientation of detail – right	Global
Orientation for documents	Orientation of detail – right	Global
Orientation for forms	Orientation of detail – right	Global
Orientation for forwarding rules	Orientation of detail – right	Global
Orientation for organisational structure	Orientation of detail – right	Global
Orientation for password reset	Orientation of detail – right	Global
Orientation for passwords	Orientation of detail – right	Global
Orientation for reports	Orientation of detail – right	Global
Orientation for roles	Orientation of detail – right	Global
Orientation for seal templates	Orientation of detail – right	Global
Category: Display		
Display fold-down details in permissions view	Activated	

The diagram shows the settings for the user “Jones”. The search has been filtered by the term “Detail”. The column **“Inherited from”** shows that some settings have been inherited globally, or by the organisational unit “IT”. The top two options have no value in the column. This is because this parameter has been defined at user level.

The inheritance for individual settings can be deactivated in the ribbon!

Security levels

Option groups were created in the global settings to ensure that users can control only those settings for which they hold permissions. Categorising security levels from 1 to 5 allows you to combine similar options and thus make them available to the users.



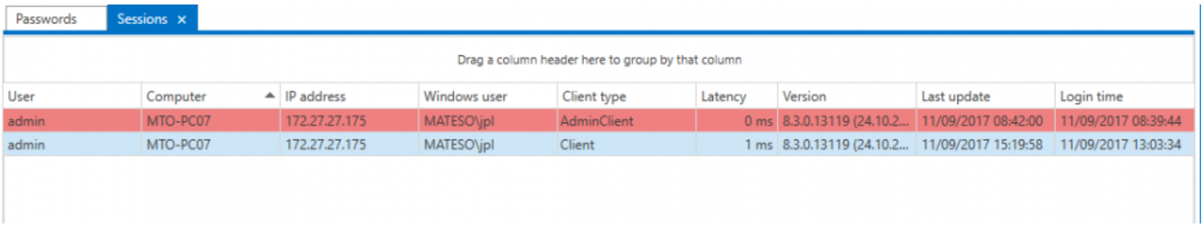
Name	Value	Option group
Category: General		
Number of allowed widgets	3	Security level 2
Close tab after saving	Activated	Security level 1
Close tab after discarding	Activated	Security level 1
Edit tab after opening	Activated	Security level 1
Display footer area	Activated	Security level 1
Tab width	Automatic	Security level 1
Mark notifications as read when...	Deactivated	Security level 1
Can search for updates	Deactivated	Security level 5
Restore last tabs opened	Deactivated	Security level 1
Open quick search in new tab	Deactivated	Security level 1
Allow a tab to be opened multipl...	Deactivated	Security level 3
Display module names on dashb...	Deactivated	Security level 1
Category: Filter		
Jump to filter on quick search	Activated	Security level 1
Can use filter negation	Activated	Security level 1
Automatically use last filter	Activated	Security level 1
Display mode	Both	Security level 1
Display mode status when starti...	Last status	Security level 1

The user rights define who has the required permissions to change which security levels. As with all rights, this is achieved either through global inheritance, the role, or as a right granted directly to the user.

Administration

Sessions

Via the menu item **Sessions**, all users connected to the database can be displayed. This page is purely informative in character and thus no configurations can be made here.



User	Computer	IP address	Windows user	Client type	Latency	Version	Last update	Login time
admin	MTO-PC07	172.27.27.175	MATESO\jpl	AdminClient	0 ms	8.3.0.13119 (24.10.2...	11/09/2017 08:42:00	11/09/2017 08:39:44
admin	MTO-PC07	172.27.27.175	MATESO\jpl	Client	1 ms	8.3.0.13119 (24.10.2...	11/09/2017 15:19:58	11/09/2017 13:03:34

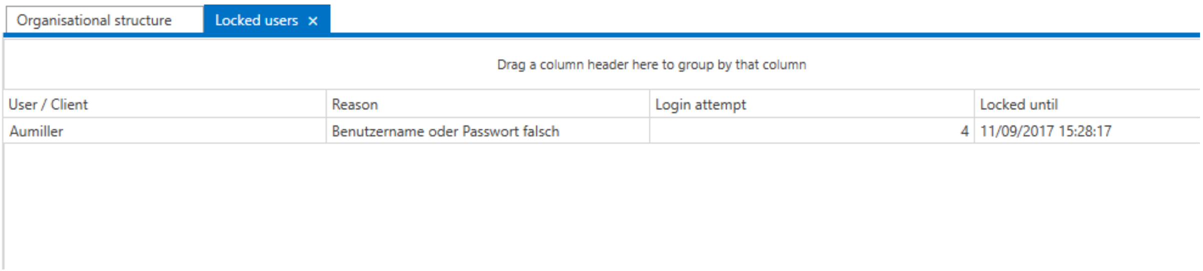
The session view starts in the currently active module in a separate tab.

Locked users

All currently locked users can also be retrieved. There are two scenarios here:

1. **User name correct, password incorrect**: The user name is displayed
2. **User name incorrect**: The client is displayed

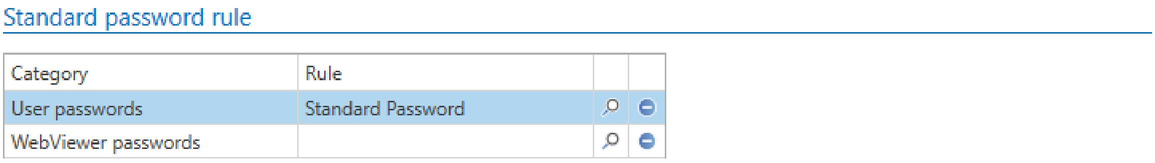
In addition, the number of attempted logins and the length of time that the user was locked in each case can be seen.



User / Client	Reason	Login attempt	Locked until
Aumiller	Benutzername oder Passwort falsch	4	11/09/2017 15:28:17

Default password rules

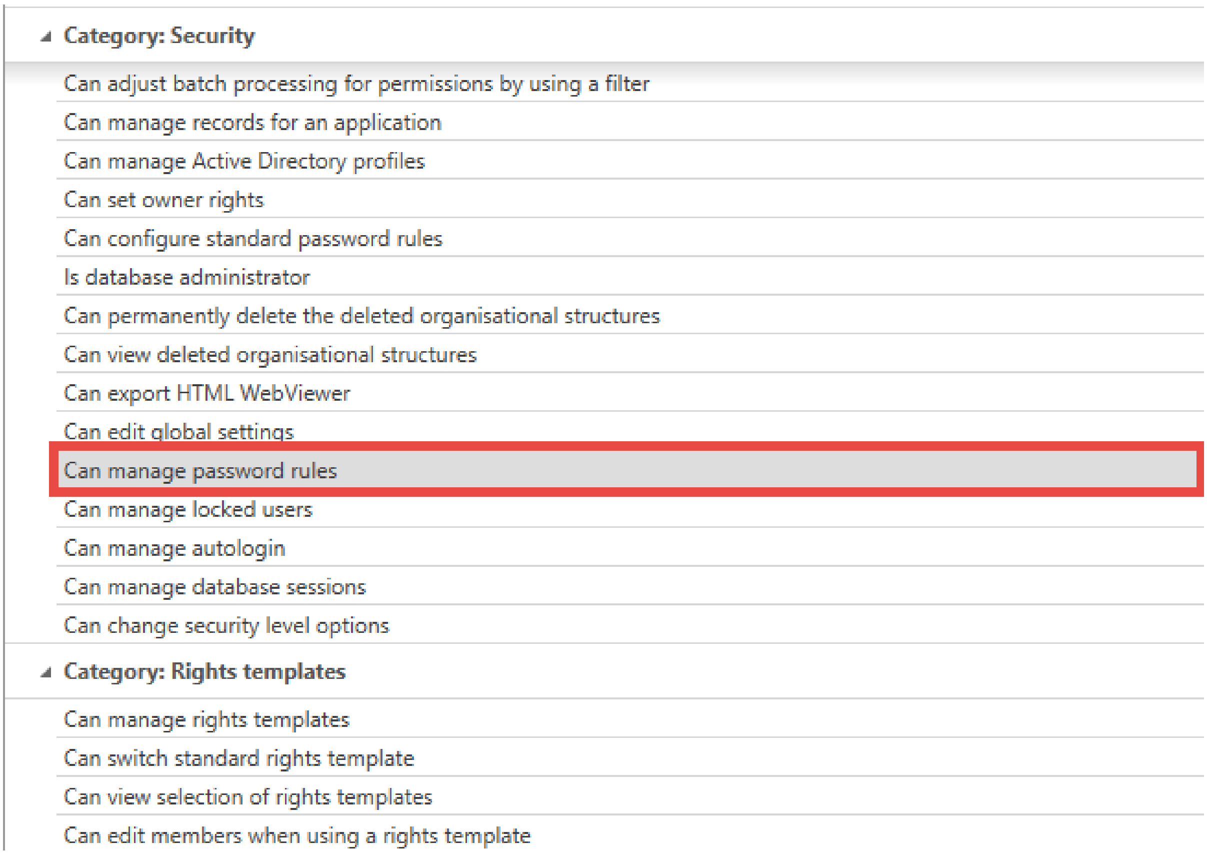
Password rules can be defined for both user passwords and also for WebViewer exports that then need to be fulfilled. In the following example, a user password must correspond to the “default password” rule in order to be valid.



Standard password rule

Category	Rule		
User passwords	Standard Password	⌕	⊖
WebViewer passwords		⌕	⊖

- Required user rights: In order to define the password rules for the above-mentioned passwords, the separate user right “Can manage categories for password rules” is required



◢ Category: Security

Can adjust batch processing for permissions by using a filter
Can manage records for an application
Can manage Active Directory profiles
Can set owner rights
Can configure standard password rules
Is database administrator
Can permanently delete the deleted organisational structures
Can view deleted organisational structures
Can export HTML WebViewer
Can edit global settings
Can manage password rules
Can manage locked users
Can manage autologin
Can manage database sessions
Can change security level options

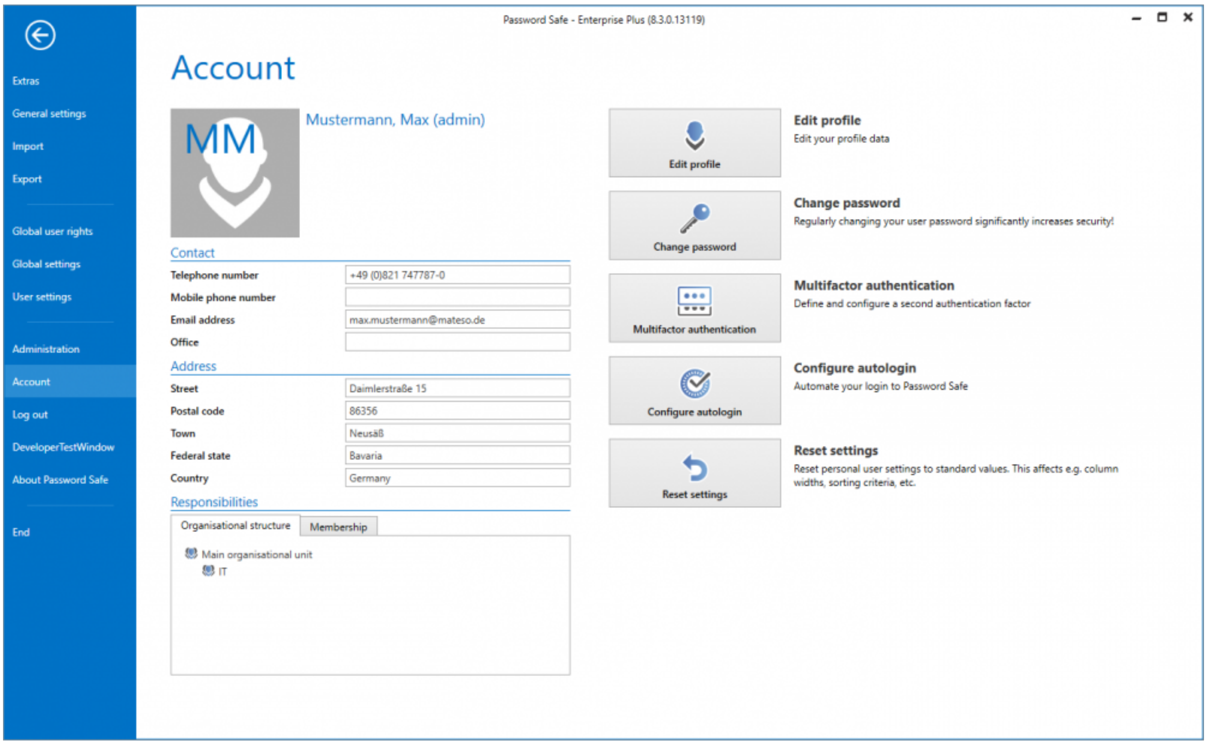
◢ Category: Rights templates

Can manage rights templates
Can switch standard rights template
Can view selection of rights templates
Can edit members when using a rights template

Account

What is an account?

Users can configure all user-specific information in their account. It should be noted that if the Master Key process is used, user data will always be taken from Active Directory – editing this information in Password Safe is thus not possible.



Password Safe - Enterprise Plus (8.3.0.13119)

Account

Mustermann, Max (admin)

Contact

Telephone number: +49 (0)821 747787-0
Mobile phone number:
Email address: max.mustermann@mateso.de
Office:

Address

Street: Daimlerstraße 15
Postal code: 86356
Town: Neusäß
Federal state: Bavaria
Country: Germany

Responsibilities

Organisational structure | Membership

Main organisational unit
IT

Edit profile
Edit your profile data

Change password
Regularly changing your user password significantly increases security!

Multifactor authentication
Define and configure a second authentication factor

Configure autologin
Automate your login to Password Safe

Reset settings
Reset personal user settings to standard values. This affects e.g. column widths, sorting criteria, etc.

Edit profile

All of the information in the contact and address sections can be defined under “Edit profile”. Some areas of the profile overlap with the **management of users**. This information is explained in a separate section.

> ✻ No changes can be made to users that were imported from AD using Master Key mode. In this case, all information will be imported from AD.

Editing user image

A new image can be added or the existing one replaced or deleted by clicking on the profile image.

No changes can be made to users that were imported from AD with the aid of Master Key mode. If an image has been saved in AD, it will be used here.

Change password

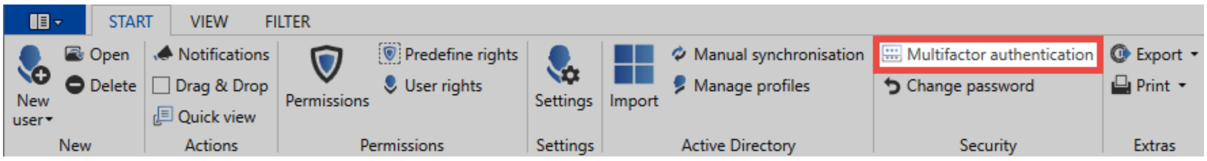
It is recommended that the user password is changed on a regular basis. If you want to use a new password, it is necessary to enter the existing password in advance. The strength of the password will be directly displayed.

Users who were imported from AD with the aid of Master Key mode log in with the domain password. Therefore, no password can be configured in this case.

The strength of the user password can be stipulated by administration through the issuing of password rules. More…

Multifactor authentication

Multifactor authentication provides additional protection through a second login authentication using a hardware token. The configuration is carried out via the ribbon in the “Security” section. More….



Configure autologin

This option can be used to automate the login to Password Safe. For setup, just enter the password twice and save it.

! The automatic registration is to be classified as a security criterion. It is important to note that all data can be accessed, for example, if you forget to lock the computer.

For security reasons, the autologin is only valid for 180 days and then needs to be subsequently renewed.

Reset settings

Clicking on this button resets all user-specific settings such as the column width, colour scheme, etc. to the default values.

Start offline synchronization

If you have made changes to the database and do not want to wait for the next automatic synchronization, an offline synchronization can also be started manually. The synchronization runs in the background and is indicated by a status bar in the footer as well as by the icon. More…

SSO Agent

What is the SSO agent?

The SSO Agent is responsible for the automatic entry of login data in applications. This enables logins without knowledge of the password, which can be a particularly valuable tool in combination with password masking. The authorization concept is used to define which users should receive access. However, the password remains hidden because it is entered by Password Safe.

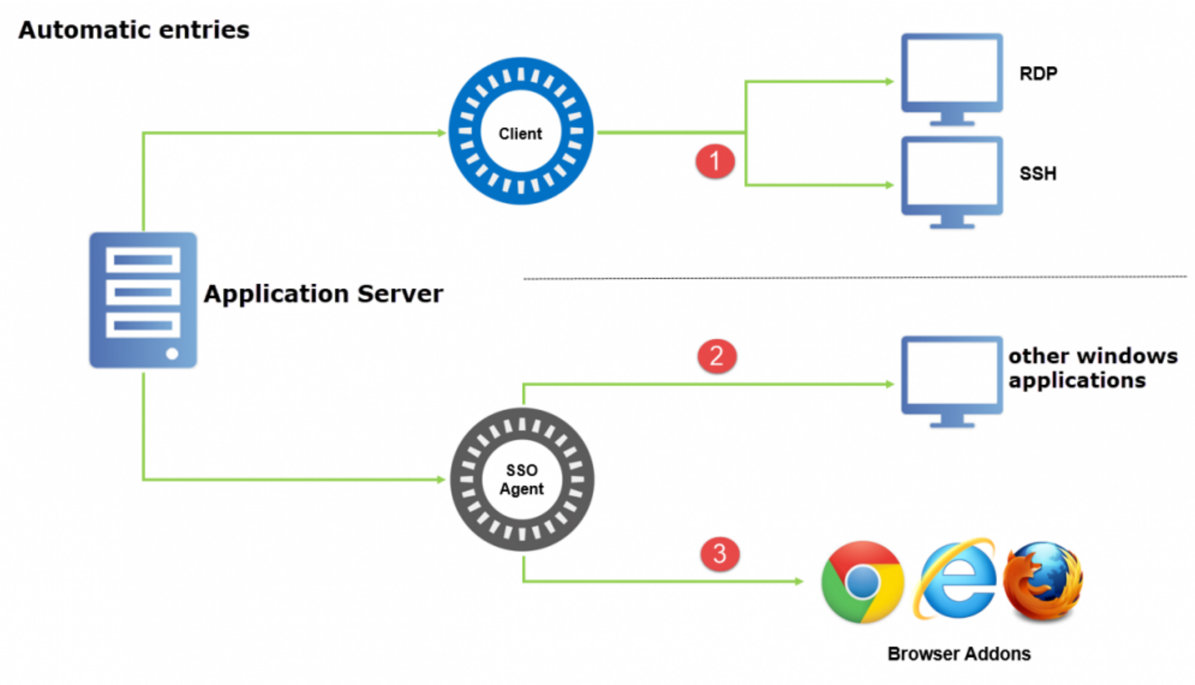
Requirements

The SSO agent is installed together with the Password Safe client and can then be used by users (assuming they have sufficient permissions). A separate installation is thus not necessary. A desktop link is created for both the client and also for the SSO agent.

> ! The right **Can create web applications** is required for creating new web applications

Functionality

The functionality of the SSO agent is illustrated in the following diagram.



RDP and SSH sessions(1) are not automatically started via the SSO agent. Applications are created for this purpose in the Password Safe client. The creation and use of these connections is explained in detail in the corresponding section.

Automatically starting all other types of connection is the task of the **SSO agent**. The following types of connections exist:

- **Entering login data in Windows applications**: Alongside the above-mentioned RDP and SSH sessions, other Windows applications can also be automated (2). A major difference is that the two above-mentioned connections are set up and “embedded” in a separate tab. Other applications, such as e.g. VMware, are directly started as usual (more…). In these cases, the SSO agent takes over the communication between the application server and the Windows applications.

- **Entering login data on websites**: Password Safe can automate the login process on websites. This means that the desired login is configured once via the add-on and can be efficiently used in future (in the same way that favourites are used). The SSO agent acts as an **interface** (3) here between the applications server and the available browser add-on (Google Chrome, Internet Explorer and Mozilla Firefox).

The agent can control multiple databases at the same time

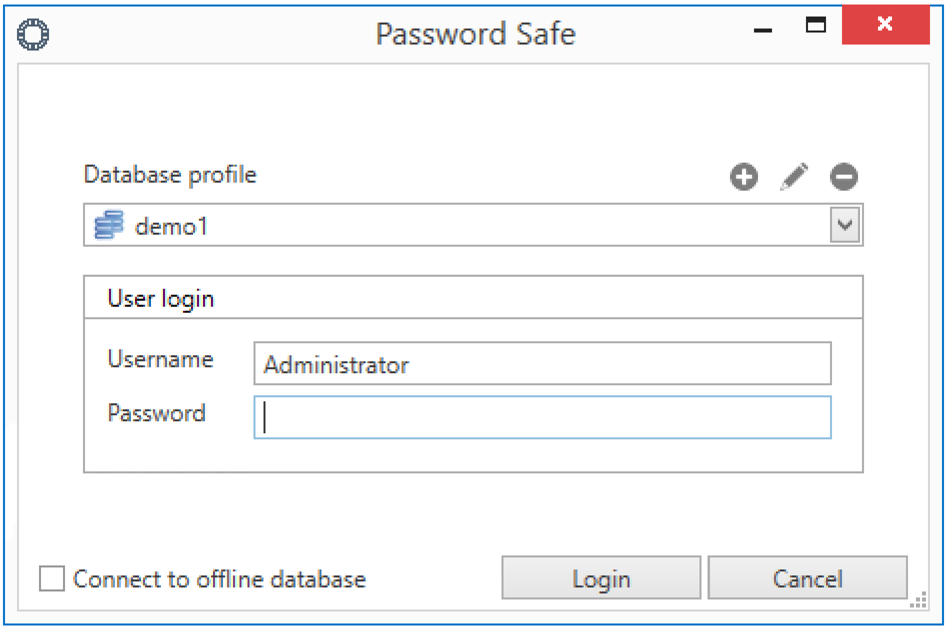
Conclusion

As the SSO agent is directly connected to the application server, login data can also be entered without the main client. Exceptions are the RDP and SSH connections. These are forced to remain part of the client. The SSO agent thus acts as a lean alternative for the use of the client with the two limitations mentioned. Naturally, all of the steps completed are still entered in the logbook and are always traceable.

Configuration

Starting the SSO agent

The SSO agent can be directly started via the desktop link that is automatically created when it is installed. The login data correspond to the normal user data for the client.



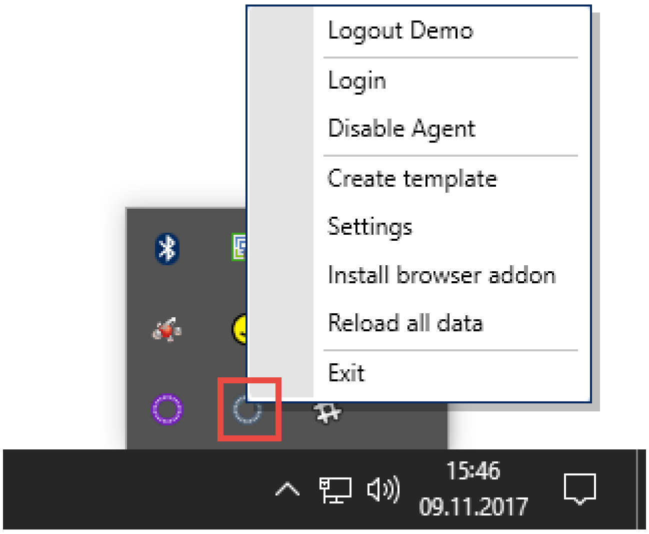
Username: Administrator

To log in, the desired database and the associated login data are firstly selected. The SSO agent makes all of the databases configured on the client available. It is also possible to create profiles as usual so that the connection data for certain databases can be used efficiently in the future.

The agent accesses the same configuration file as the client. All changes to profiles will thus also affect the client. New profiles can thus also be created via the SSO agent.

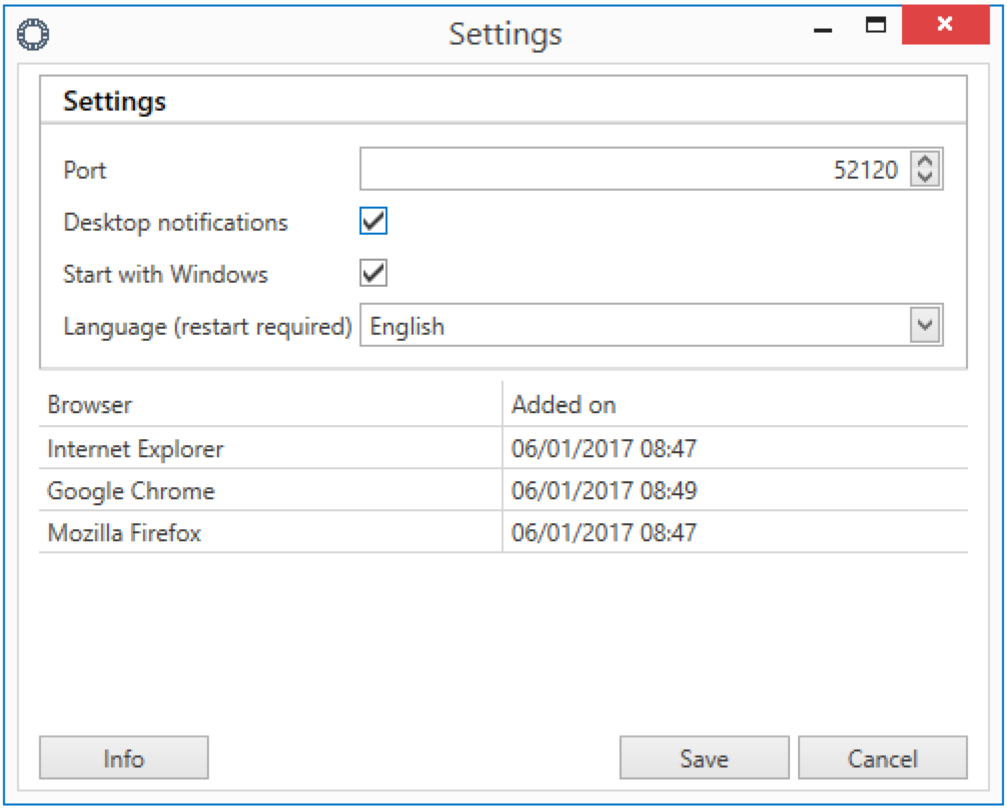
Context menu functionality

After successfully logging in, the SSO Agent firstly runs in the background. Right click on the icon in the system tray to open the context menu.



- **Disconnect**: Connect to database/disconnect from database. (All connections are shown for multiple databases)
- **Login** enables you to log into another database
- **Deactivate/activate agent** allows you the option of temporarily disabling automatic login
  A diverse range of variables can be defined via the **Settings**
- **Install browser add-on** starts the installation of the Google Chrome or Mozilla Firefox add-on.
- **Connect with add-on** enables the add-on and agent to be paired (only available in terminal server operation)

H4(#agent settings). Settings



Settings

Settings

Port: 52120

Desktop notifications: ☑

Start with Windows: ☑

Language (restart required): English

Browser	Added on
Internet Explorer	06/01/2017 08:47
Google Chrome	06/01/2017 08:49
Mozilla Firefox	06/01/2017 08:47

- The **port** for connection to the database does not usually need to be changed. If it is otherwise occupied, it can be newly defined here. If the port is changed here, it must also be changed in the add-on.
- In terminal server operation, a range of ports can be defined via **Terminal Server Ports** which the terminal server will use for the connection. In this case, the default is 1000. Adjustments are usually not necessary. In terminal server operation, the so-called **terminal server ID** can also be retrieved. This is a unique ID that correctly identifies the agent on the add-on. The ID must be specified in the add-on when making the first connection.
- The **desktop notifications** display various information, such as when data is entered
- **Start with Windows** includes the SSO Agent in the autostart menu
- The lower section shows which add-ons are currently linked to the SSO Agent

The SSO agent in terminal server operation

The SSO Agent firstly needs to be paired to the desired add-ons in order to start terminal server operation.

Requirements

Before pairing, ensure that the desired add-on is installed. The terminal server service must also be installed. This is installed together with the client.

Pairing

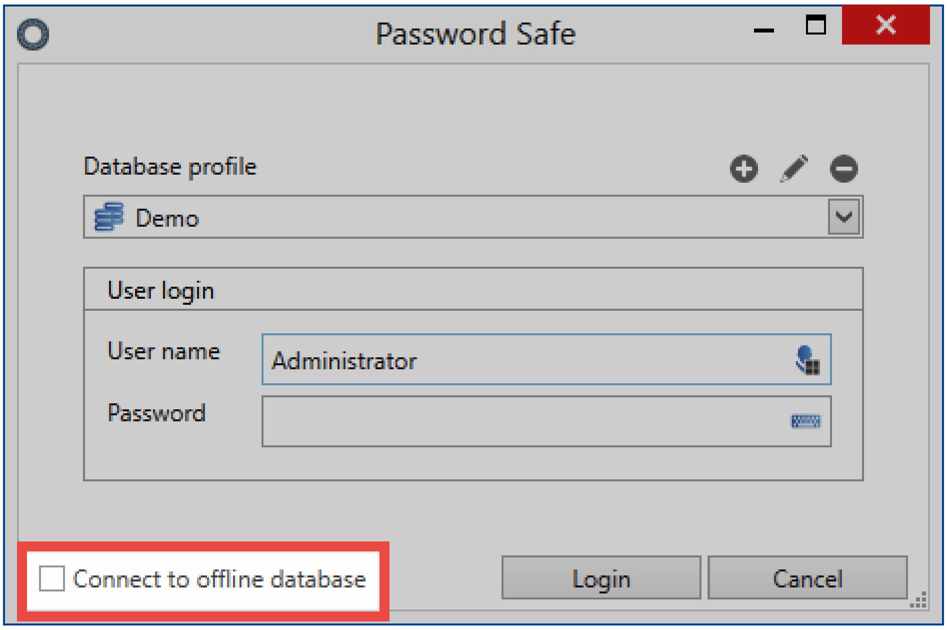
First, select the item **Connect to add-on** from the context menu in the agent. In the next window, select the desired browser. The browser will then open
and the settings for the add-on will be displayed. Usually, the terminal server ID has already been entered here. You just need to confirm it.

Changing the port

If it is necessary to change the port, you first need to log in to the **SSO agent**. The port can now be changed and saved in the **settings**. The **SSO agent** will then be ended. In order to accept the changes for the service, the Windows service **Password Safe V8 Terminal SSO Service** needs to be restarted. The **SSO agent** can now be restarted. The port will then also have been changed in the desired **browser add-on**.

Interplay with offline databases

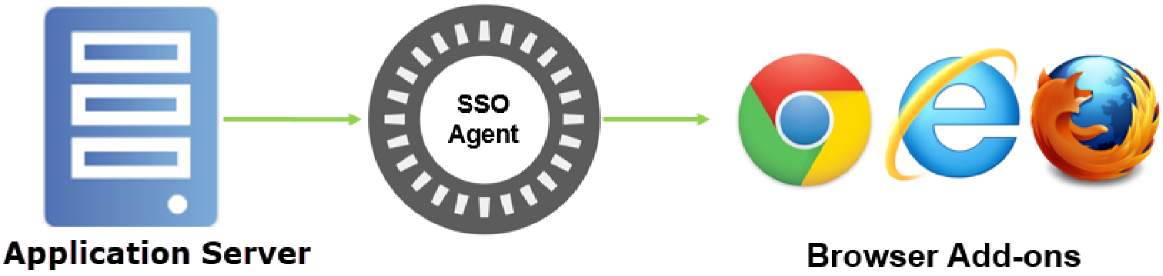
The SSO agent can also establish connections to offline databases. You can directly connect to the offline database, if one exists, at login. If there is no server connection, the connection to the offline database is directly suggested.



Add-ons

What are add-ons?

If you want to directly access the database from a browser, you need a browser add-on for the connection to the SSO agent. The agent is started via the icon in the system tray, whereby the add-on can be found in the menu section of the respective browser. Add-ons for Mozilla Firefox, Google Chrome and Microsoft Internet Explorer are currently available and they are responsible for automatically entering login data on websites.



✱ The login data is entered by (amongst other things) applications. The creation of these applications is explained in the following section.

Installation

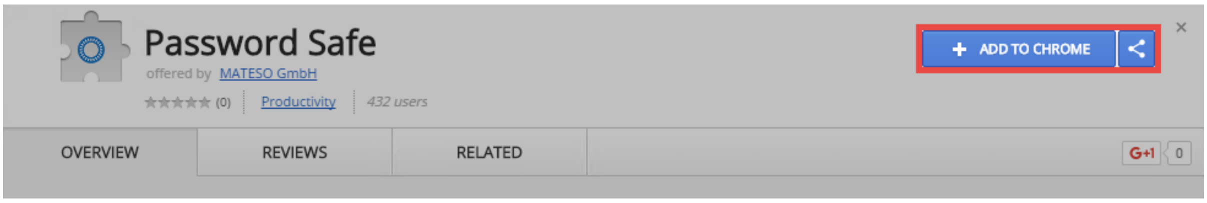
Browser add-ons for Google Chrome and Mozilla Firefox can be directly downloaded using the SSO Agent. Right-click on the icon to open the context menu. Click on **Install Browser Add-ons** to select the requested add-on. As the actual installation of the add-ons is different in each case, the installations will be described separately below:

Internet Explorer

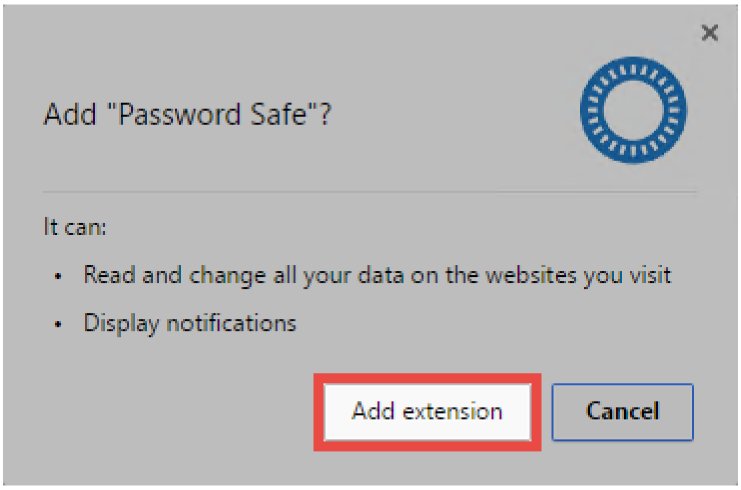
The Internet Explorer add-on can be directly installed together with the client. For this purpose, there is a corresponding option in the installer that is activated by default.

Google Chrome

The installation of the Google Chrome add-on is started using the SSO Agent. You will be directed to the Google Store, where you can start the installation by clicking on **Add**.



The add-on will now be installed and the icon added to the browser.


Add "Password Safe"?

It can:

- Read and change all your data on the websites you visit
- Display notifications

Firefox

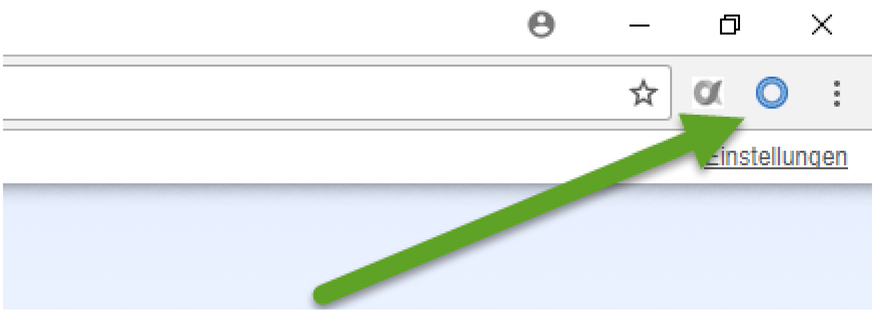
You can download the Firefox add-on via the following link:

Password Safe add-on for Firefox

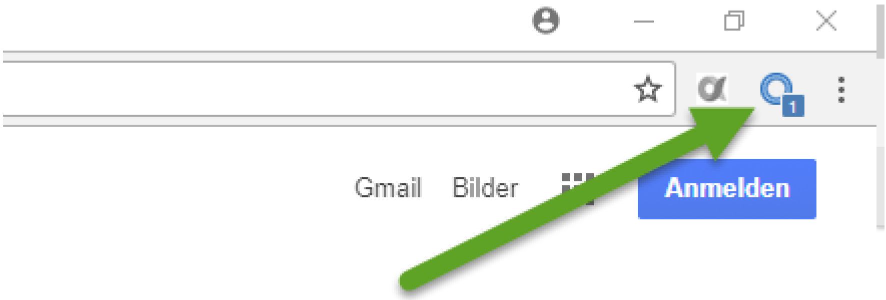
After the download, the add-on is simply dragged and dropped into the browser. After confirmation, it will be installed and an icon created in the menu bar.

Connection with the SSO agent

If the steps Installation of the add-on and Connection with the SSO agent have been carried out, the user can now open the desired browser. A window appears in which the security of the connection is confirmed. Pairing is performed with a simple click. The add-on is authorized to request data from the SSO Agent from this point onwards. A **new icon** will also be displayed in the desired browser from this point onwards:



If the icon is displayed as shown, it means that although the add-on has been installed, a connection has not yet been established with the SSO agent. Only **after logging into the agent** (via the icon in the system tray) will you receive a Windows notification about the successful login. If a connection to the agent has been established, the **number of available records for the current website** will be directly displayed on the icon.



A subscript “0” means that the add-on has successfully logged into the agent.

Settings

All settings that relate to the add-on are made centrally on the client. The user settings system can be used to enter settings globally per organisational unit or per user. The following options have a direct impact on the add-ons and can be found in the **SSO** category:

- **Browser add-ons: Automatically send login masks** ensures that the login is automatically completed after the access data has been entered. It is thus not necessary to click the relevant button manually
- About **browser add-ons: Automatically fill login masks** ensures that access data is entered without the need for any confirmation when a website is recognised.

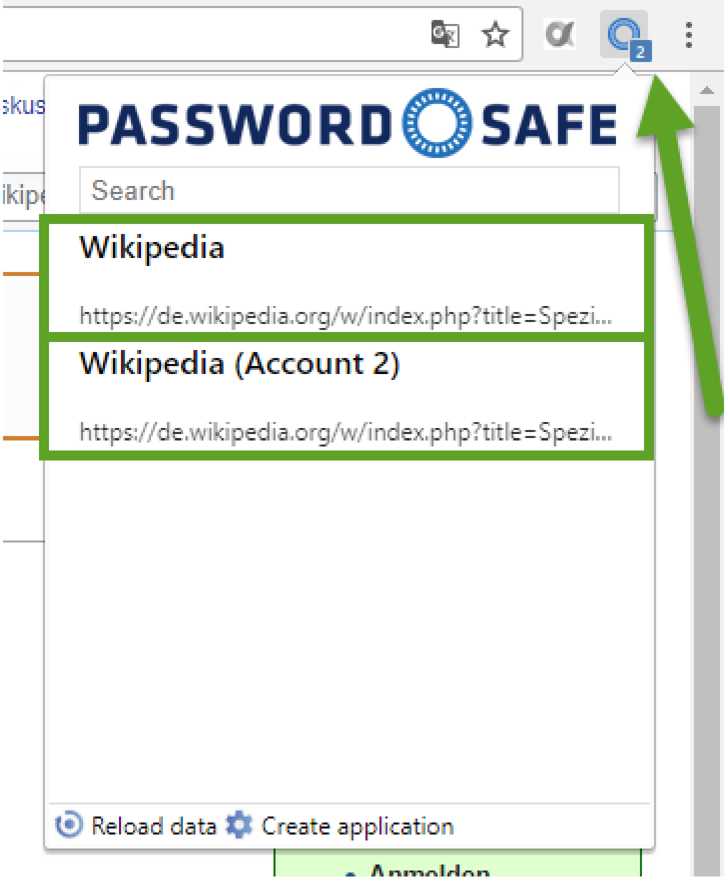
The **default browser** option also has an impact on the add-ons. This setting defines the browser in which the websites are opened from the client.

The above-mentioned settings can also be defined for each record. Further information can be found here: “

Working with add-ons

A record can only be used for entering data if it has a form field of type “URL”

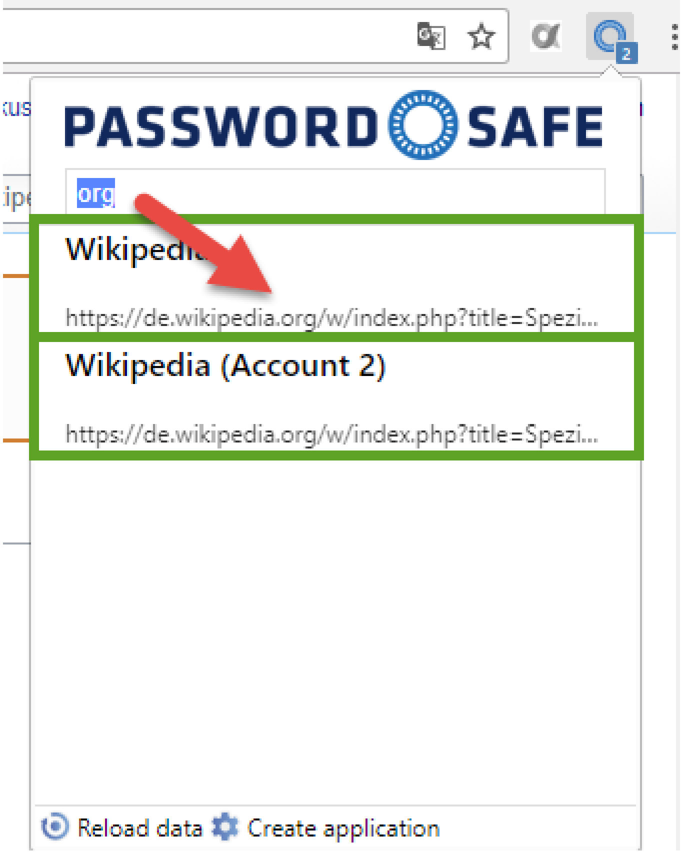
The subscript number mentioned in the previous section is, on the one hand, only available with active logins and, on the other hand, it already says a lot about the “Number of possible entries”. For example, if the number “2” is shown, you can directly select the account with which you want to log in.


PASSWORD SAFE
Search
Wikipedia
https://de.wikipedia.org/w/index.php?title=Spezi...
Wikipedia (Account 2)
https://de.wikipedia.org/w/index.php?title=Spezi...
Reload data
Create application
2

Previously, the prerequisite was that you had to manually navigate to the precise website via the browser that you actually wanted to use. This navigation can now also be handled by Password Safe – as described in the following section.

Searching and navigating

It is currently assumed that the user has to manually navigate to the website on which they want to automatically enter login data. This way of working is possible but is not convenient enough. The add-on can be used in a similar way to bookmarks. The search field can be used to search for the record in the database. The prerequisite is again that the record contains a URL.


PASSWORD SAFE
org
Wikipedia
https://de.wikipedia.org/w/index.php?title=Spezi...
Wikipedia (Account 2)
https://de.wikipedia.org/w/index.php?title=Spezi...
Reload data
Create application

In the screenshot, it can be seen that the URL as well as the name of the record (Wikipedia) are searched. The results for the search are displayed and can be selected using the arrow buttons or the mouse. The selected website will be opened in a separate tab.

Displayed passwords

Which passwords are displayed for a recognised website depends on how the record or records have been configured. It is possible to define for each password how granular the URL should be checked. Further information can be found in the section password settings.

The process will be explained using an **example**:

A unique password has been created for each of the following websites:

- www.passwordsafe.de
- help.passwordsafe.de
- license.passwordsafe.de

The **Exact domain check** is deactivated for all three passwords:
On **www.passwordsafe.de**, the passwords for the subdomains are also displayed in the add-on, i.e. **www.passwordsafe.de**, **help.passwordsafe.de** and **license.passwordsafe.de**

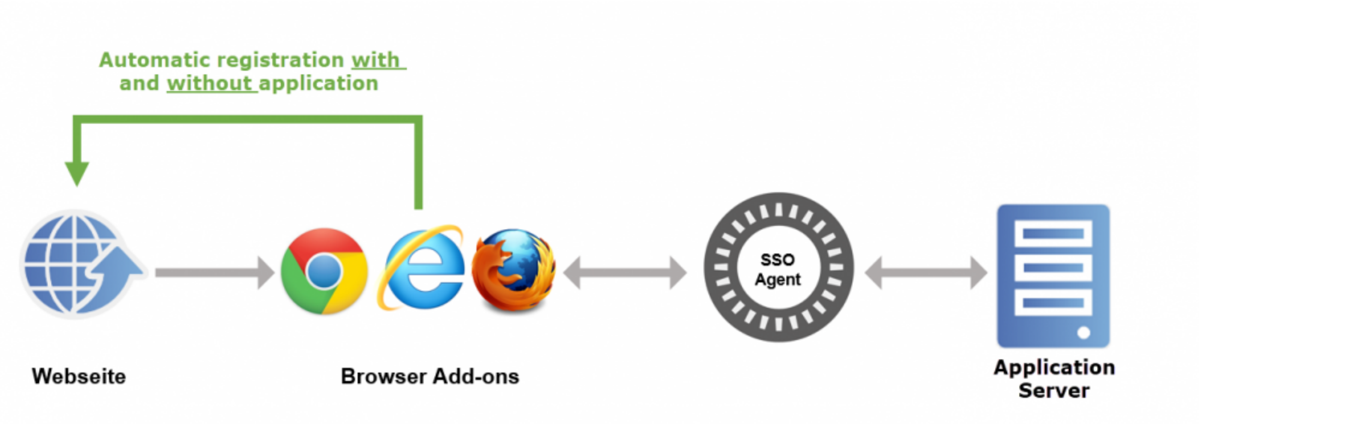
The **Exact domain check** is activated for all three passwords:
On **www.passwordsafe.de**, no passwords for the subdomains are displayed in the add-on. Only **www.passwordsafe.de** is displayed

The **Exact domain check** is activated for all passwords except for **license.passwordsafe.de**.
On **www.passwordsafe.de**, **www.passwordsafe.de** and **license.passwordsafe.de** are displayed in the add-on.

Applications

What are applications?

Data can be entered on many websites without further configuration. The website is scanned in order to find data entry fields in which the user name and password can then be entered. No further steps are thus necessary. For websites where data cannot be entered directly, it is necessary to create an application manually. These applications correspond to working guidelines that precisely define which information should be entered into which target field. The full script that describes the assignment is called an “application”.



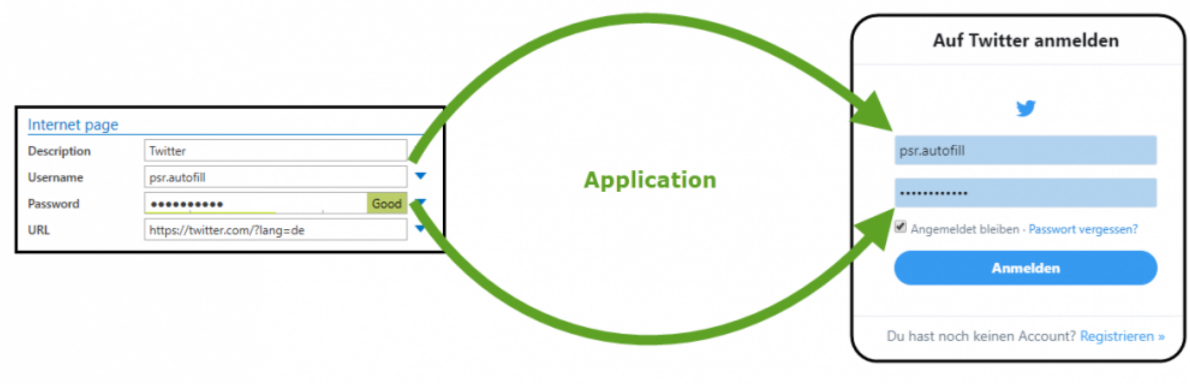
The diagram starts with the user navigating to a website. The application server is then checked (via the add-on and the SSO agent) to see whether a record has been saved for this website for which the currently registered user also has the required permissions. If this is the case, the information required for the login is sent to the browser add-on in encrypted form. The password is only decrypted in the add-on shortly before it is entered. There are two ways in which the information is entered: **Data entry without application** and **Data entry with application**.

Data entry without application

The data entry without application process is sufficient for most websites because the fields can be directly assigned (mapping). The system checks in the background whether a login mask has been found for any websites visited. The URL is now used to check if there are any records in the linked websites that would fit the page. It is only necessary for the hostname including the domain suffix, such as .de or .com, to match. If the registered user also has the required permissions for this record, the data will now be requested by the SSO agent. **Important: Up to this point, the add-on has no knowledge of passwords!**. The data are then entered. In this case, the user name is transmitted to the first user name field that can be found on the page. The password is also entered into the first password field found on the page. If automatic login has been activated in the settings, this is also carried out by clicking the login button.

Data entry with application

It is not possible to automatically recognise the fields that must be filled on some websites. An application needs to be created in these cases. If more than two fields need to be transferred, it is also necessary to create an application. In this context, “application” means instructions that are used to enter information into the fields. It thus assigns fields in the record to the associated fields on the website. This mapping process only needs to be configured once. The applications is responsible for entering data in the fields on the website from then on. In the following example, the data entry process is carried out from the client. Naturally, this is also possible via browser add-ons. The procedure remains the same.

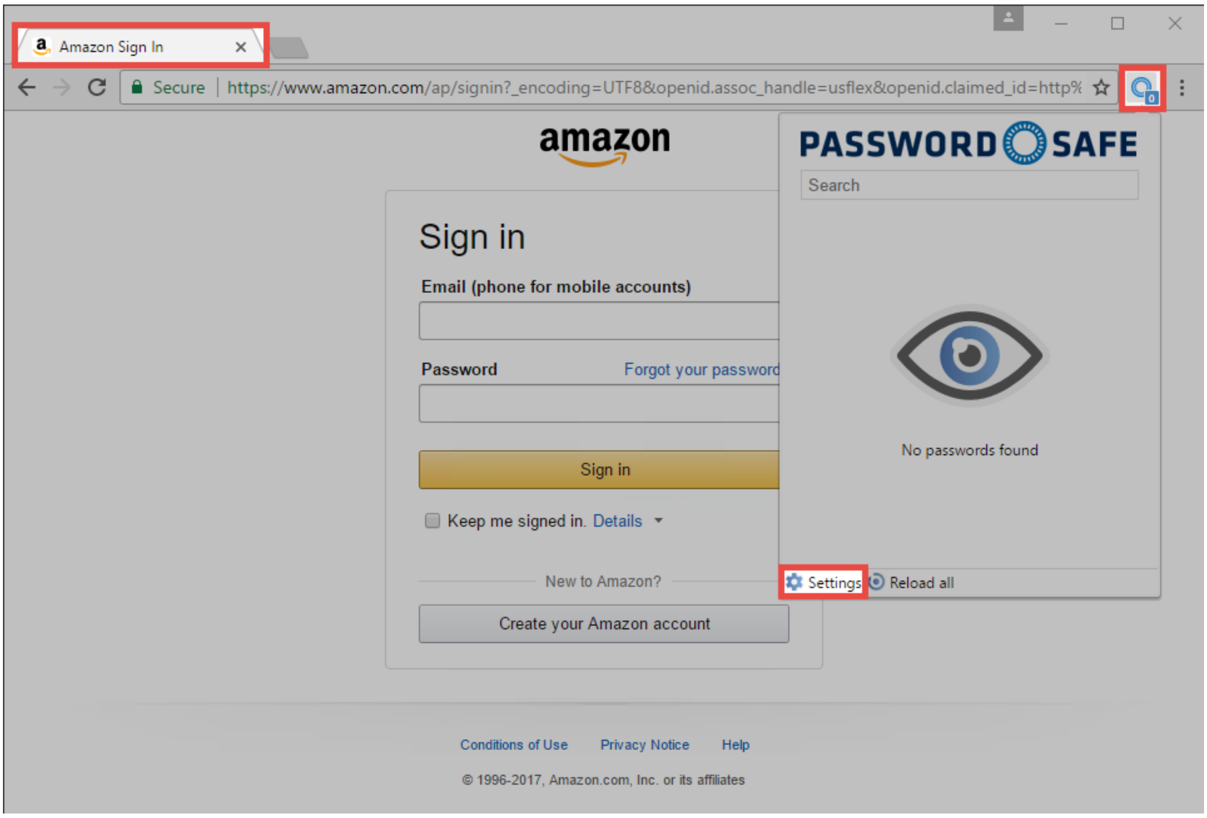


The URL is checked to see whether the record matches the web page. It is only necessary for the hostname including the domain suffix (“.de” or “.com”) to match.

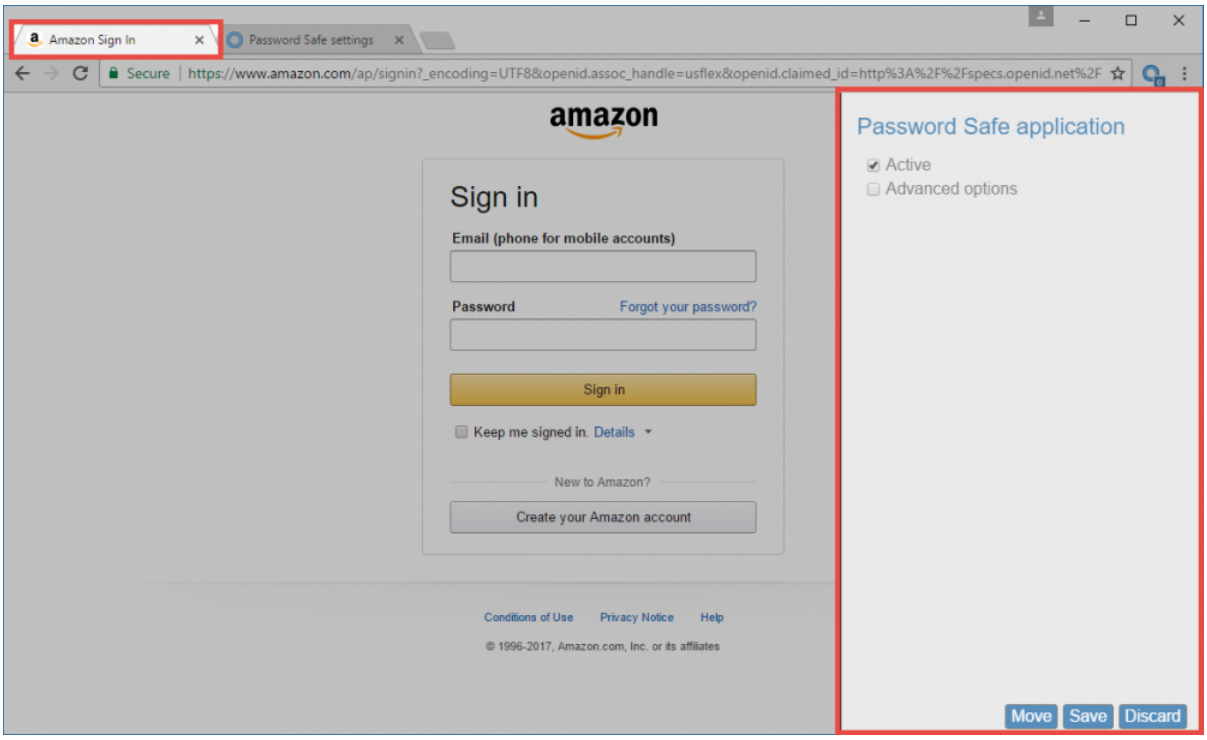
Creating applications

! The user right **Can add new web applications** is required in order to create applications

If the login mask on a website cannot be automatically completed, it is necessary to manually create an application. To create an application, the desired website is first called up. The add-on is then started via the relevant icon. The menu item “Create application* can be found here.


Amazon Sign In
Secure
https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex&openid.claimed_id=http%
amazon
Sign in
Email (phone for mobile accounts)
Password
Forgot your password
Sign in
Keep me signed in. Details
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2017, Amazon.com, Inc. or its affiliates
PASSWORD SAFE
Search
No passwords found
Settings
Reload all

A modal window now opens. The actual application is now created here.

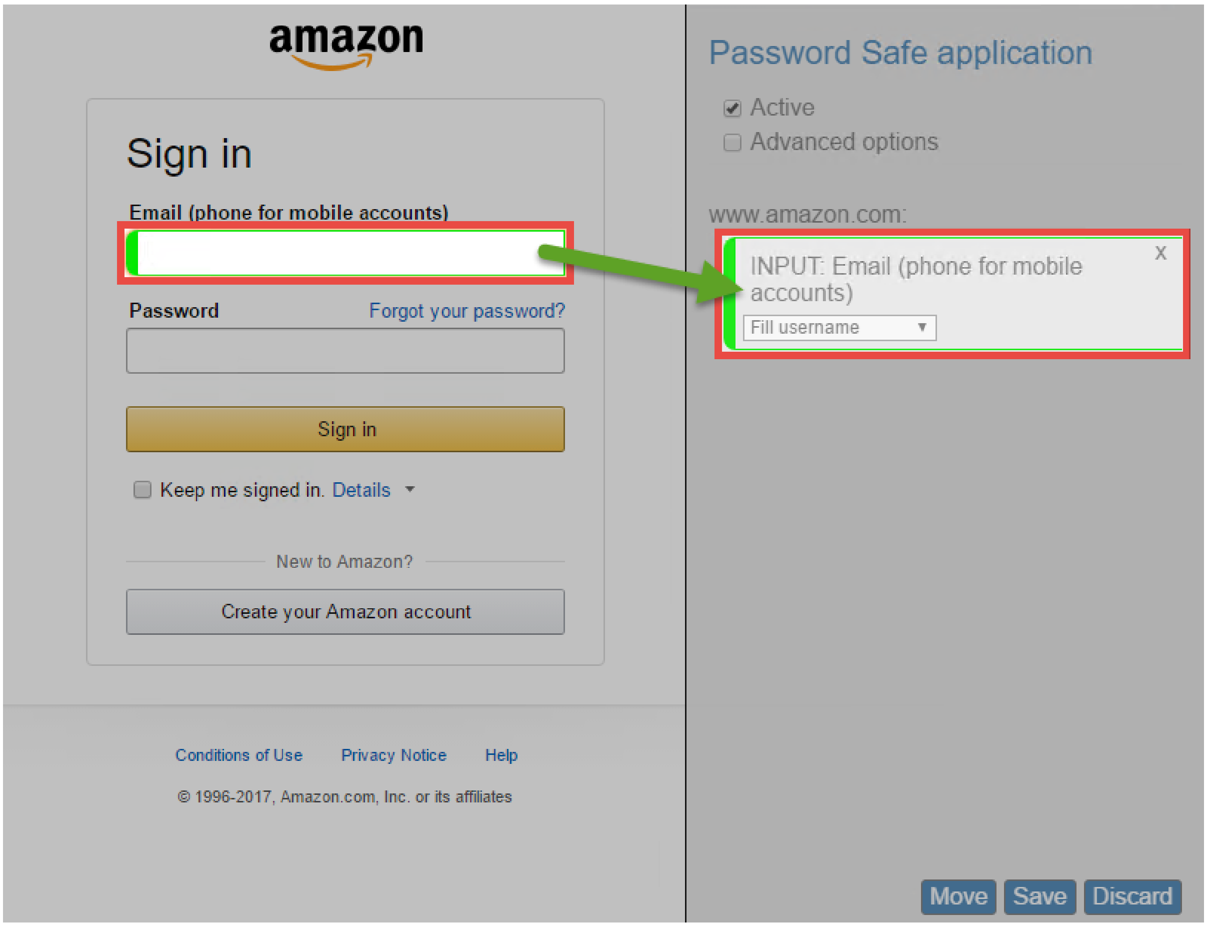

Amazon Sign In
Password Safe settings
Secure
https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%2F
amazon
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Sign in
Keep me signed in. Details
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2017, Amazon.com, Inc. or its affiliates
Password Safe application
☑ Active
□ Advanced options
Move
Save
Discard

The following options are available:

- The button *Capture fields” enables you to leave out the process for capturing fields

- **Advanced settings** allows you to define a delay separately for each field when entering the data. This is sensible when the process of entering the data would otherwise not run smoothly on sluggish websites.
- The **Move** setting can be used to change the position of the modal window if it covers the login window

To capture, click on the first field to be filled on the website. It will be directly added to the list in the modal window. For better identification, fields that belong together are marked in colour.



Password Safe application

☑ Active

□ Advanced options

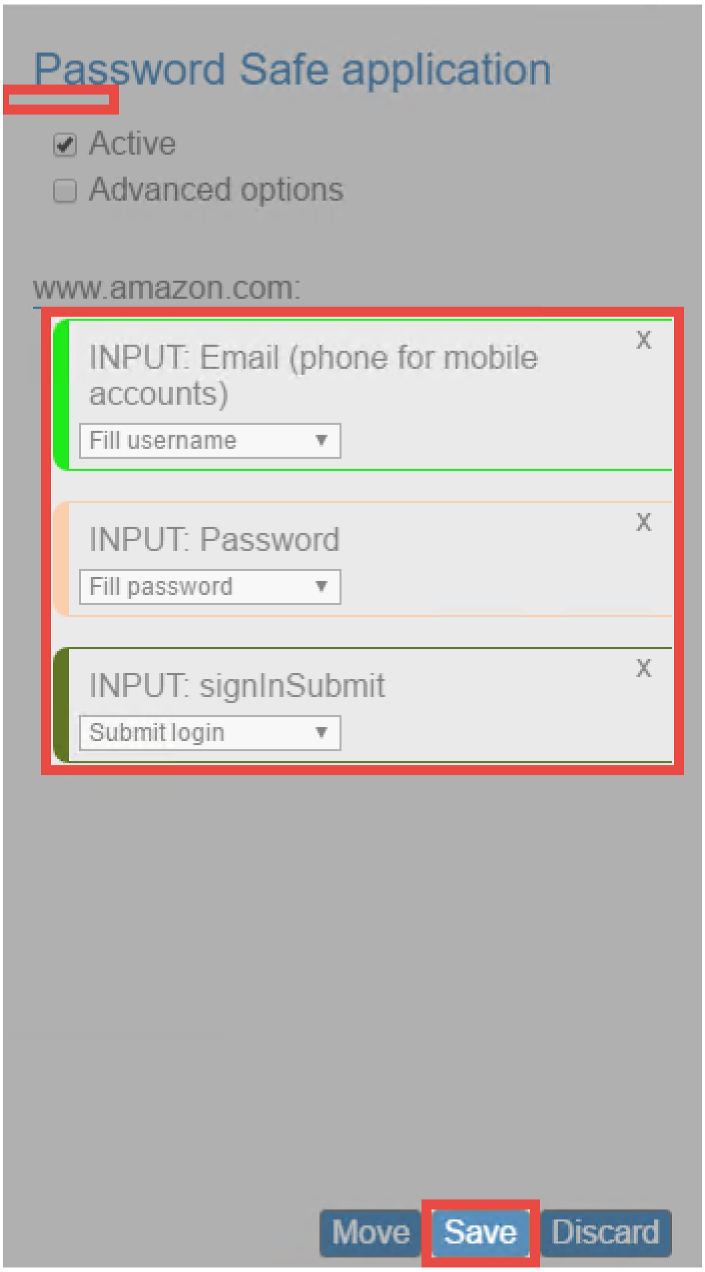
www.amazon.com:

INPUT: Email (phone for mobile accounts)

Fill username ▾

amazon
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Sign in
□ Keep me signed in. Details ▾
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2017, Amazon.com, Inc. or its affiliates
x
Move
Save
Discard

The field type (e.g. INPUT) and the field label are displayed in the field itself. In addition, an action is proposed which fits the field type, such as e.g. entering the user name. The action can naturally be adjusted if required. Once all fields have been captured, the system checks whether the actions are correct. Finally, the application can be saved.



Password Safe application

☑ Active

□ Advanced options

www.amazon.com:

INPUT: Email (phone for mobile accounts)
Fill username

INPUT: Password
Fill password

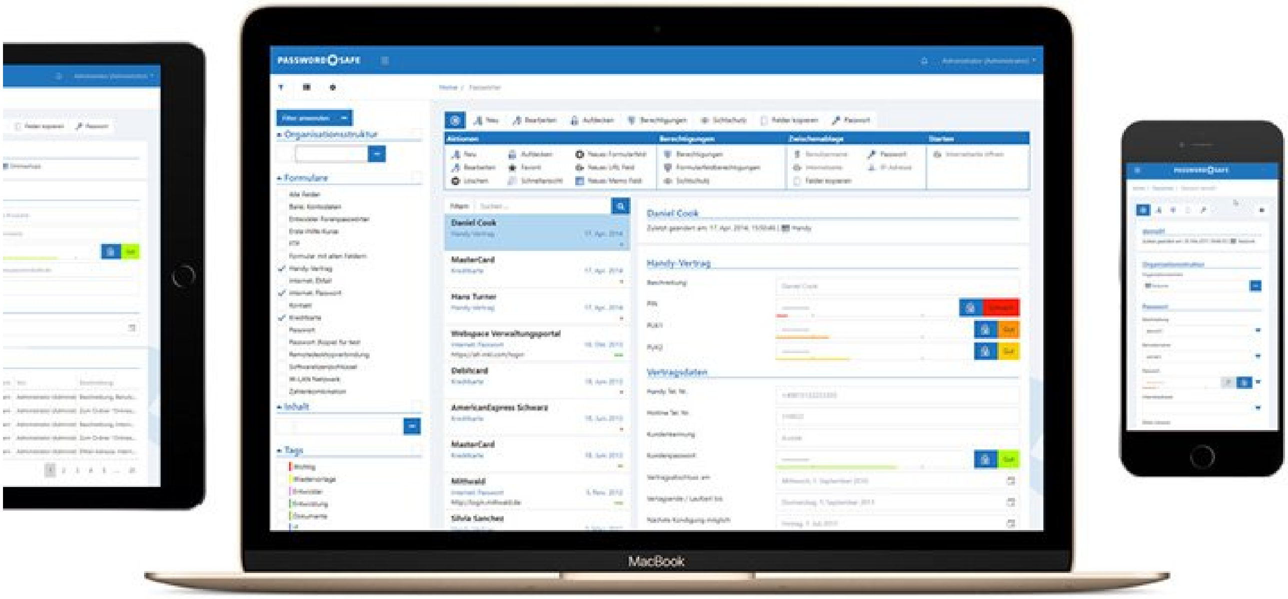
INPUT: signInSubmit
Submit login

The saved application is now available for the user and can be used via the add-on.

WebClient

What is the WebClient

The previous WebAccess function has been replaced by the **WebClient” in Password Safe version 8.3.0. The completely newly developed *WebClient** will act as the basis for the constant enhancement of the functional scope. The desired objective is to also provide the full functional scope of the client in the WebClient. The **WebClient** will thus be constantly enhanced.
All of the currently available functions can be viewed in the functional scope section.



Password Safe WebClient enables platform-independent access to the database via a browser. It is irrelevant whether you are using Microsoft Windows, macOS or Linux, it is only necessary for javascript to be supported. As the **Password Safe WebClient** has a responsive design, it can also be used on all mobile devices such as tablets and smartphones.

The **WebClient** is based both optically and also in its operation on the Password Safe client. As usual, users can only access the data for which they also have permissions. The installation is described in the section Installation of the WebClient .

Functional scope

The **WebClient** will act as the basis for a constant enhancement. The current functional scope will be explained at this point. For the purposes of clarity, the relevant modules will be described in their own subsections.

General functions

- Global settings and user settings
- Global user rights

Functions in the individual modules

- Password module
- Tag module

Password module

The following functions are currently available in the **password module**:

- Add
- Delete
- Edit
- Reveal password
- Quick search
- Add/edit form fields
- Apply tags
- Duplicate
- Move
- Quick view (automatically reveal passwords)
- Favourites
- Filter
- Structure filter
- Edit permissions/rights
- Form field permissions
- Change password while hidden
- Password generator with rules
- Copy to clipboard
- Open web page
- View logbook
- Display seal/masking
- German/English
- Change user password if “Change password on next login” is active
- Display notifications
- Keyboard navigation
    - ALT+Q: Quick search
    - ALT+N: New record
    - ALT+S: Save in edit/new view
    - ALT+DEL: Delete selected records
    - Up/down arrow in the list: Change selection
    - Right/left arrow in the list: Go to next/previous page
    - Enter: Open selected records
- Password masking
- Seals

Tag module

The **tag module** currently offers the following functions:

- Add
- Delete
- Edit

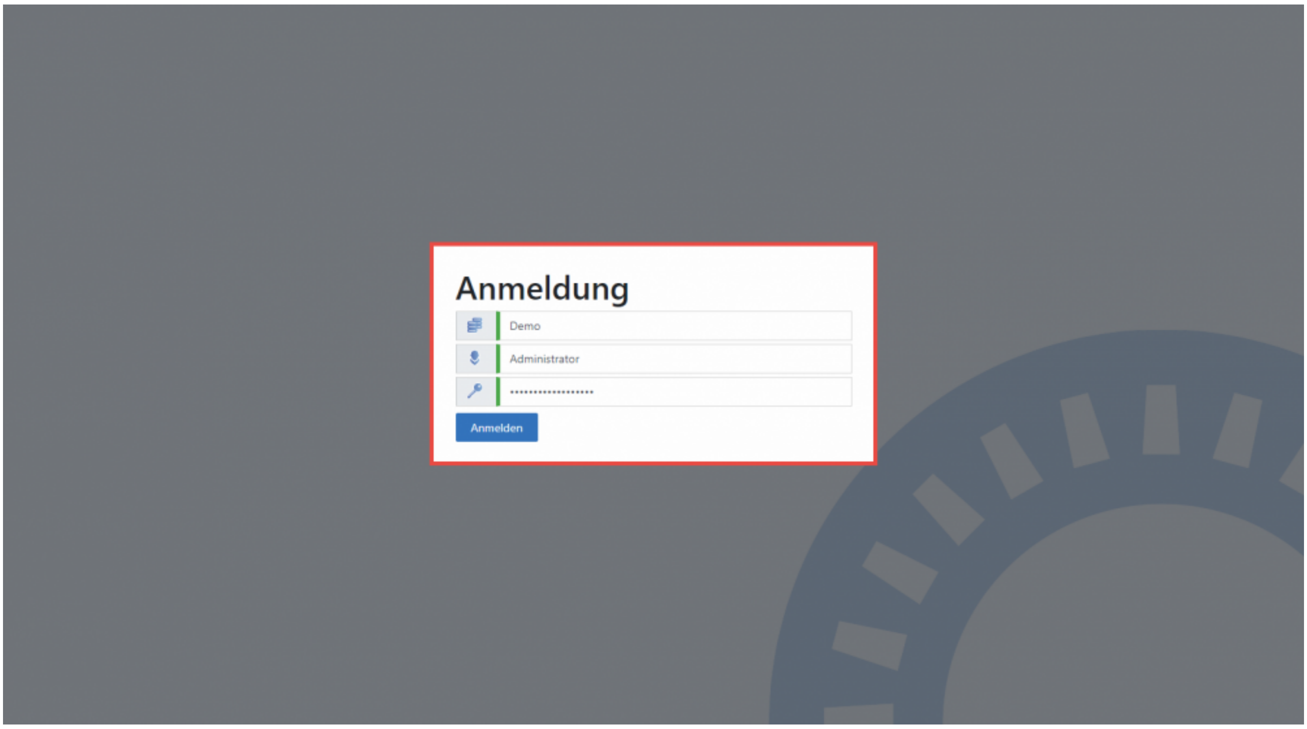
Operation

Operation of the WebClient has been based as far as possible on the operation of the Password Safe client. Nevertheless, there are some differences that need to be noted and they are described here.

Login

There is no database profile on the WebClient. All databases approved for the WebClient will be made available. The following information needs to be entered to log in:

Database name
User name
Password



Anmeldung

Demo

Administrator

••••••••••••••••••

After successfully logging in, the last database name used and the last registered user will be saved. You thus only need to enter the password for the next login.

Transferring login data via the URL

The **database name** and **user name** can be transferred directly via the URL. The following parameters are used here:

- **database** for transferring the database name

- **username** for transferring the user name

The parameters are simply attached to the URL for the WebClient and separated from one another with a **&**.

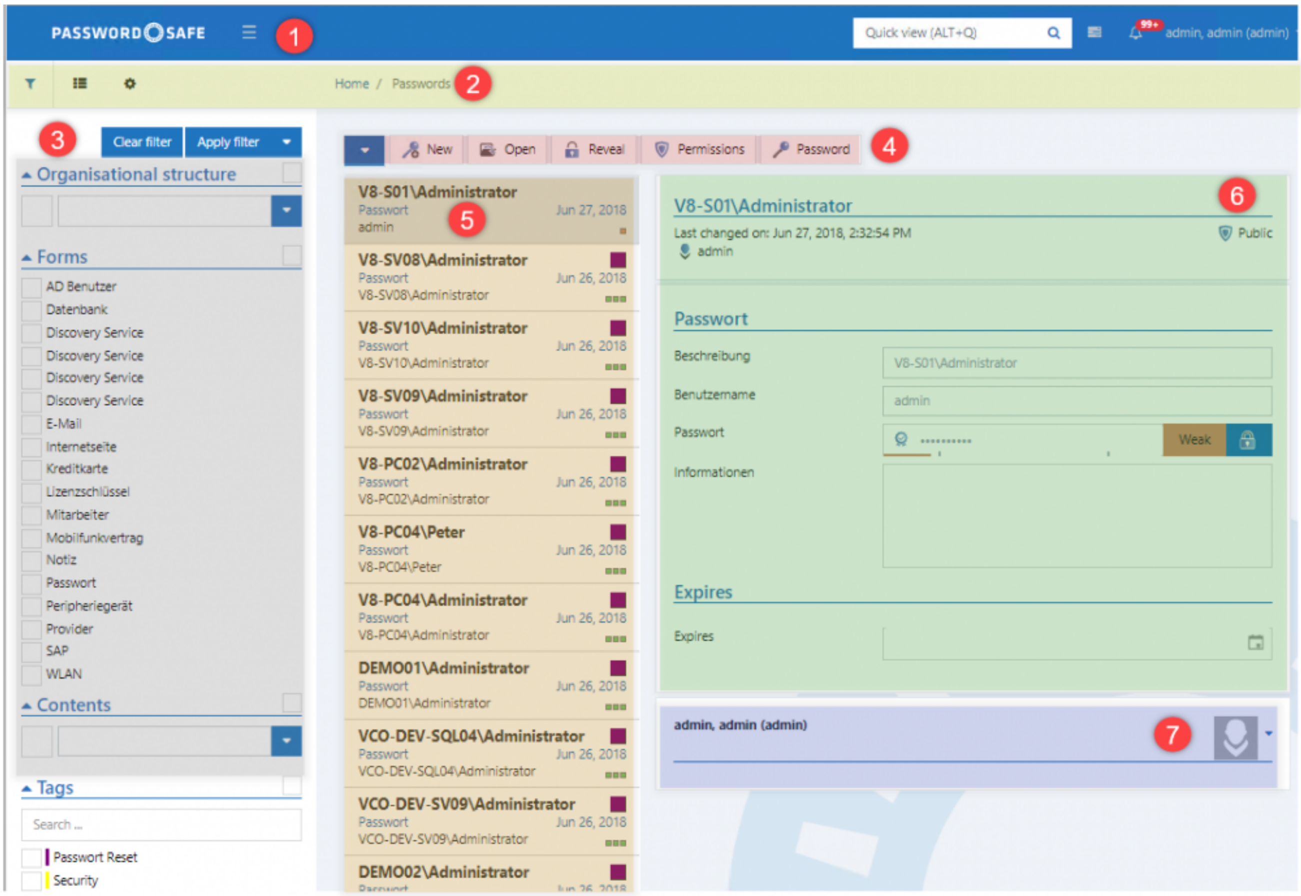
Example

You want to call up the WebClient under **https://psr_webclient.firma.com**. In the process, you want the login mask to be directly filled with the database **Passwords** and the user name **Anderson**. The following URL is then used: **https://psr_webclient.firma.com/authentication/login?database=Passwords&username=Anderson**

> It is possible to only transfer the database. The user name is not absolutely necessary.

Structure

The WebClient is split into a number of sections that are described below.



1. Header

The header provides access to some essential functions.

2. Navigation bar

It is possible to switch between module and filter view on the navigation bar.

3. Filter or structure area

As is also the case on the client, it is possible to select between filter and structure.

4. Menu bar

The ribbon on the client has been replaced by a menu bar on the WebClient.

5. List view

The records currently selected using the filter can be viewed in list view.

6. Reading pane

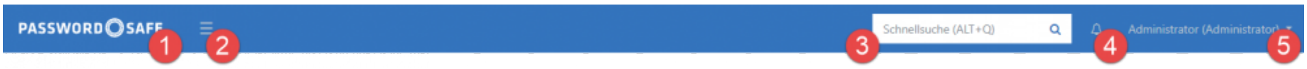
The reading pane shows you details about the relevantly selected element.

7. Footer

Various information about the record is displayed in the footer. For example, logbook entries or the history.

Header

The header provides the following functions.



1. Logo

The logo acts as a home button. It always takes you back to the standard view.

2. Display and hide filter

As is also the case on the client, the filter or structure area can be displayed and hidden.

3. Quick search

The quick search offers you the same functions as the quick search on the client. It searches in all fields of the complete database except the password field. The tags are still searched.

4. Notifications

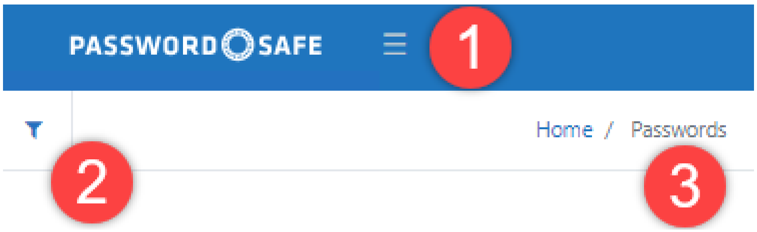
You will be informed here about incoming notifications. The notification can also be called up by clicking on it.

5. Account

The user who is currently logged in can be seen under account. You can log out by clicking on the account. It is also possible to call up the settings here.

Navigation bar

The navigation bar provides the following functions.



1. Filter

This function can be used to switch the view to the filter in the left section.

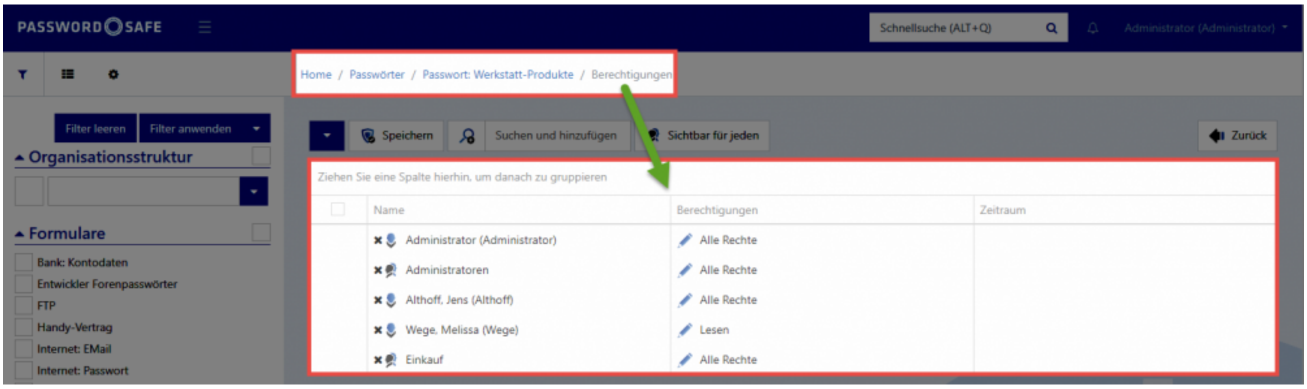
2. Structure

Switches from filter to structure.

3. Bread Crumbs

The so-called Bread Crumbs represent a secondary navigation function within the WebClient. They provide you with the possibility of returning to the originally selected element or quickly moving to different levels. The Bread Crumbs thus represent the logical path to the current position.

Example



Home / Passwörter / Passwort: Werkstatt-Produkte / Berechtigungen

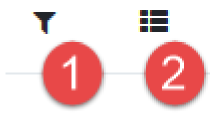
Ziehen Sie eine Spalte hierhin, um danach zu gruppieren

Name	Berechtigungen	Zeitraum
Administrator (Administrator)	Alle Rechte	
Administratoren	Alle Rechte	
Althoff, Jens (Althoff)	Alle Rechte	
Wege, Melissa (Wege)	Lesen	
Einkauf	Alle Rechte	

Select the passwords module on the start page, then the “Factory products” password and finally access its permissions. The first three levels are marked in blue and thus act as links. By clicking on **Passwords**, you will be taken back to the password module again. Clicking on **Password: Factory products** will return the user back to the password.

Filter or structure area

As is also the case on the client, it is possible to select between filter and structure. For this purpose, the following buttons are available on the “navigation bar”:#navigationsleiste:



1. Filter

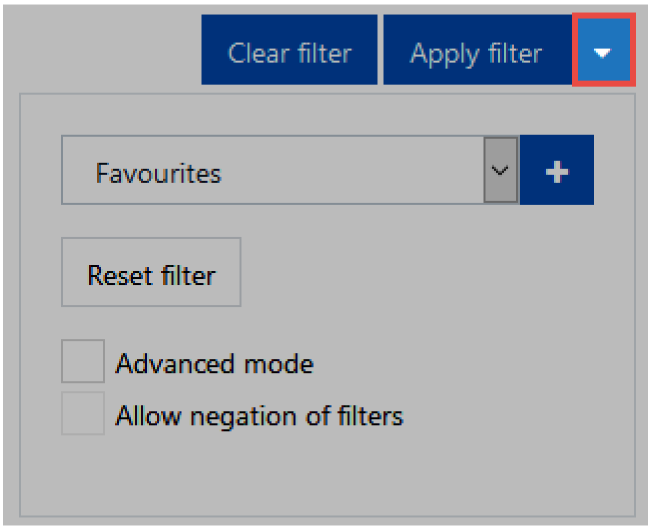
The filter on the WebClient is based on the “filter on the client:#filter. Therefore, only those characteristics specific to the WebClient will be described here.

Using the filter

Operation of the “WebClient filter” barely differs from the operation of the **client filter**. It is only necessary to note that the **Clear filter** and **Apply filter** buttons can be found above the filter. The configuration settings can also be found directly above the **WebClient filter**.

Configuring the filter

The configuration for the filter can be displayed via the following buttons:



New filter groups can be added using **Add filter groups** and the current filter can be reset using **Reset filter**. **Advanced mode** provides you with the possibility of deleting or moving individual filter groups. The **Allow negation of filters** option can also be selected.

2. Structure

The structure can be operated in precisely the same way as on the client.

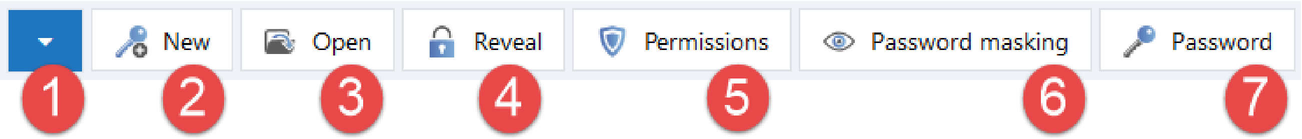
Menu

What is the menu?

The ribbon on the client has been replaced by a menu on the WebClient. The menu thus represents the central operating element on the WebClient. The functions available within the menu are dynamic and are based on the currently available actions. Different actions are possible depending on which view is currently being used.

Menu bar

The menu can take on two forms. In general, the **menu bar** containing the **most important functions** is displayed. It will be described here using the example of the password module.



1. Expand menu

The size of the menu can be maximised using this button

2. New

This option can be selected to call up the wizard for adding a new record.

3. Open

Displays the selected password and all of its details in the reading pane.

4. Reveal

Reveals the password.

5. Permissions

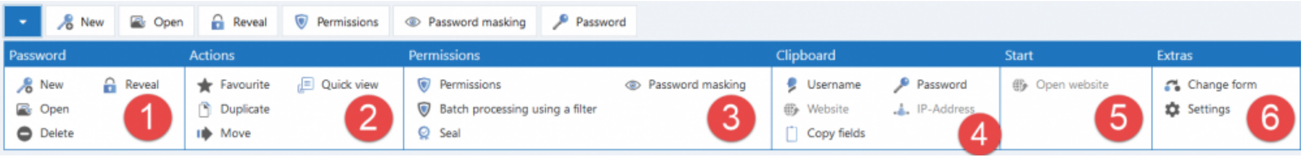
This button is used to configure the “rights”:#404 for the record.

6. Password

Copies the password to the clipboard

Advanced menu

If the menu – as described above – is maximised, **all functions** are then available. The functions on the menu bar are repeated here. The menu is divided into a number of sections. These correspond 1 to 1 to the sections of the ribbon on the client.



In our example, the menu looks like this:

1. Password

This section offers you more options for editing passwords. These include, for example, **Open** or also **Delete**.

2. Actions

The actions can be used, for example, to mark the password as a **Favourite** or also to **Duplicate** it.

3. Permissions

This section does not offer any additional functions than simply opening the permissions.

4. Clipboard

This section can be used to copy all available fields to the clipboard

5. Start

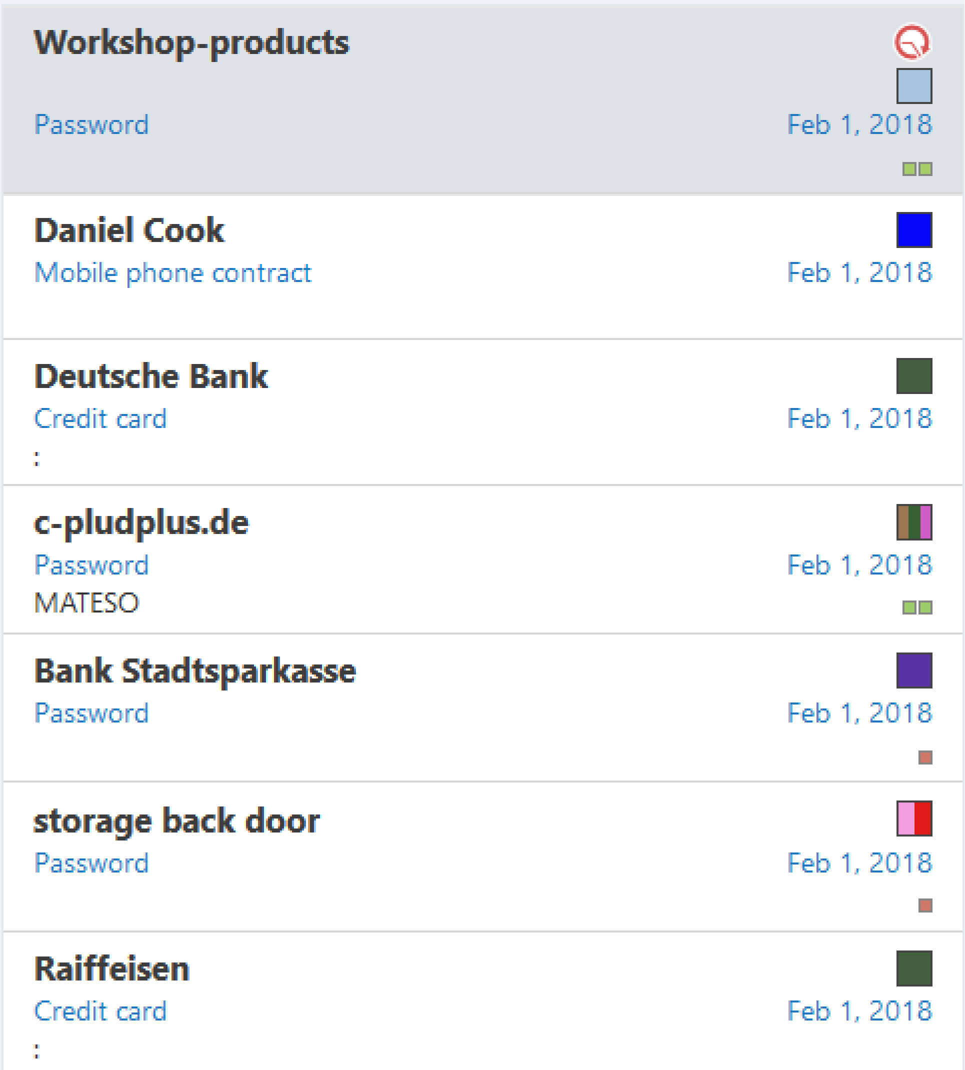
If you want to start a website, it is possible here.

As already described, the menu is dynamic and thus appears in a variety of different forms. However, the basic function is always the same: The menu bar contains the basis functions, while the advanced menu contains all functions.

List view

What is list view?

The central element of the navigation in the WebClient is list view, which clearly presents the filtered elements. As list view in the WebClient provides the same functions as list view in the client, we refer you at this point to the **list view** section.



Workshop-products
Password Feb 1, 2018

Daniel Cook
Mobile phone contract Feb 1, 2018

Deutsche Bank
Credit card Feb 1, 2018
:

c-pludplus.de
Password Feb 1, 2018
MATESO

Bank Stadtsparkasse
Password Feb 1, 2018

storage back door
Password Feb 1, 2018

Raiffeisen
Credit card Feb 1, 2018
:

Special features

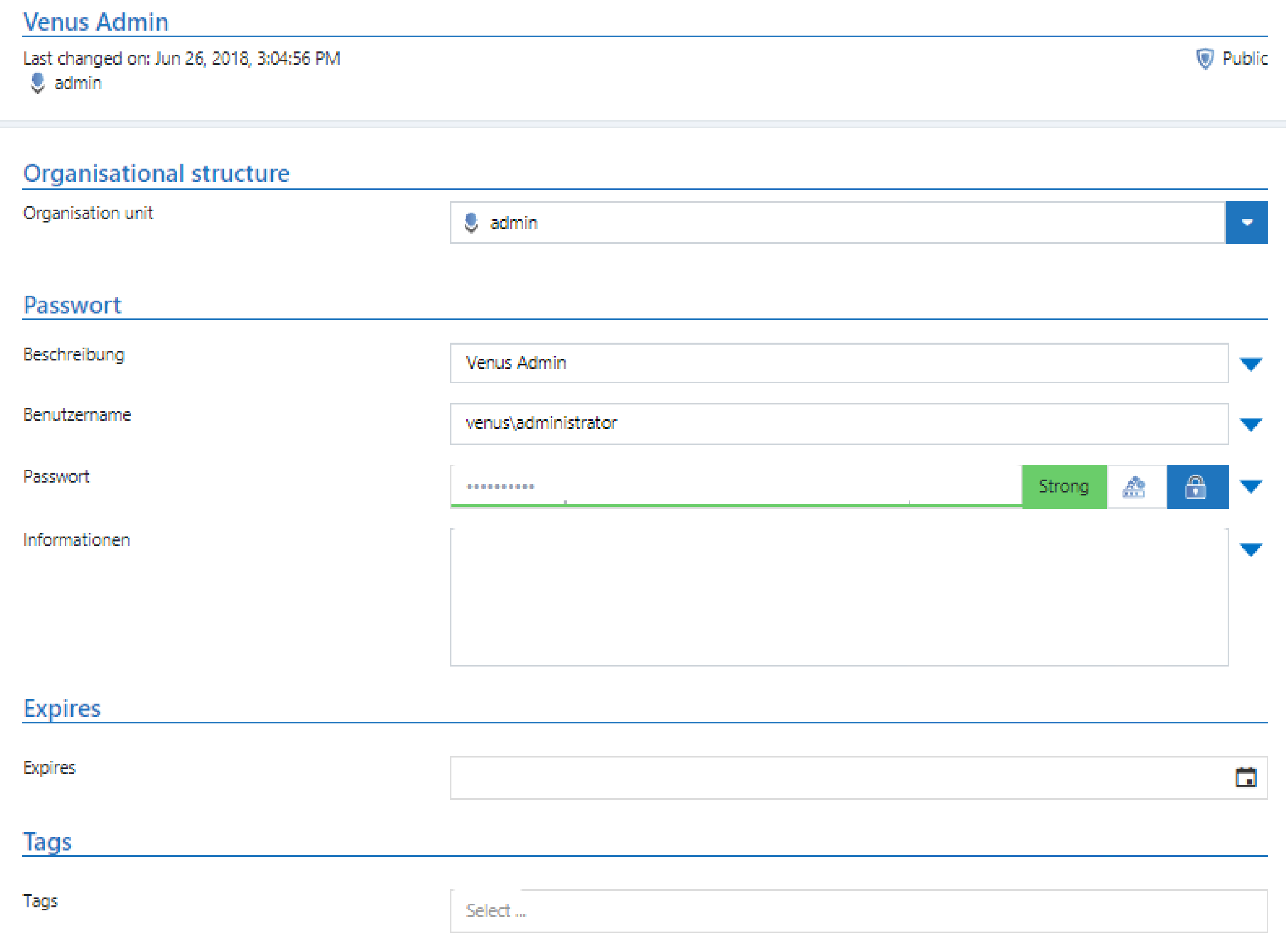
The list view differs from that on the client in the following areas:

- List view cannot be individually configured
- There are – as is usual in a browser – no context menus

Reading pane

What is the reading pane?

As with the list view, the reading pane on the WebClient is almost identical to that on the client. Therefore, we also refer you here to the corresponding reading pane section.



Venus Admin

Last changed on: Jun 26, 2018, 3:04:56 PM

admin

Public

Organisational structure

Organisation unit: admin

Passwort

Beschreibung: Venus Admin

Benutzername: venus\administrator

Passwort: •••••••••• Strong

Informationen:

Expires

Expires:

Tags

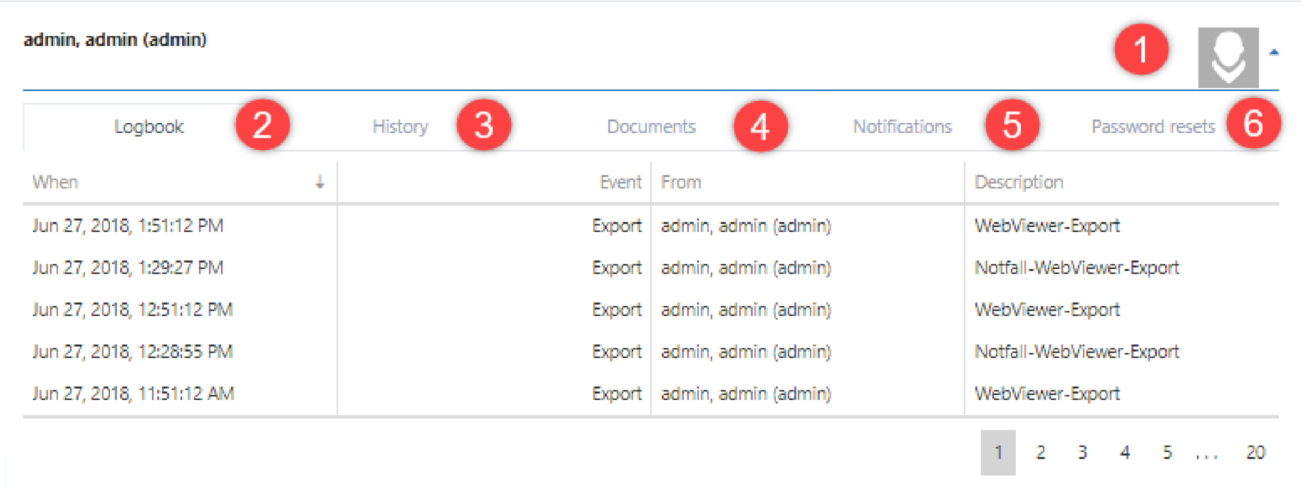
Tags: Select ...

Various information is displayed on the header – as is the case with the client. For example, the tags for the records or information on whether the record is public or private. Password masking is also symbolised here.

There are – as is usual in a browser – no context menus

Footer

The footer displays various different information about the currently selected record in multiple tabs. It can be activated or deactivated using the small arrow on the far right. The footer is hidden by default.



admin, admin (admin)

When	Event	From	Description
Jun 27, 2018, 1:51:12 PM	Export	admin, admin (admin)	WebViewer-Export
Jun 27, 2018, 1:29:27 PM	Export	admin, admin (admin)	Notfall-WebViewer-Export
Jun 27, 2018, 12:51:12 PM	Export	admin, admin (admin)	WebViewer-Export
Jun 27, 2018, 12:28:55 PM	Export	admin, admin (admin)	Notfall-WebViewer-Export
Jun 27, 2018, 11:51:12 AM	Export	admin, admin (admin)	WebViewer-Export

1. Notification area

The notification area shows who last had access to the record. The users are displayed using corresponding icons or their avatars. Clicking on the user will display their rights.

2. Logbook

You can view the last log entries about the record in the logbook tab.

3. History

The history can also be displayed via a corresponding tab.

4. Documents

The documents tab can be used to access all linked documents.

5. Notifications

This tab shows who has subscribed to receive notifications about the record.

6. Password Resets

The Password Resets that have been performed can also be listed.

Settings

The settings are called up via the navigation bar. The following options are available:

Language

You can select **German** or **English** here by simply clicking on them. The change is made immediately and does not require you to restart the browser.

Tags

The tag manager is called up here.

Settings

The following options can be managed via this menu item:

- Global user rights
- Global settings
- User settings

The management of these settings is based on the client. Further information can be found under global user rights and global settings.
The following settings are not available on the WebClient:

- Customizable window caption
- Permitted document extensions
- Clipboard gallery
- Category: Proxy

Authorization and protection mechanisms

Security and protection on the WebClient

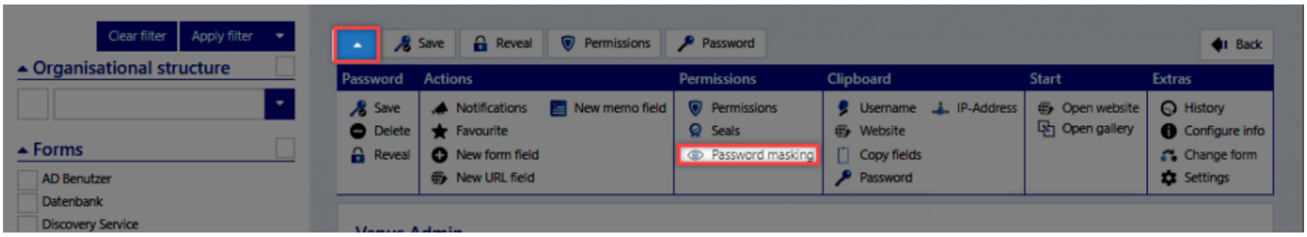
As with the client, the records can be protected on the WebClient with different mechanisms. The authorizations on records can also be managed in the WebClient. During the development of the WebClient, there was always taken care that the operation is identical to the operation of the client. Since the WebClient is based on HTML, it is unfortunately not possible to render the client 100% identical. Therefore, the operation may differ in details. These deviations should be clarified in this chapter.

Permissions and rights concept

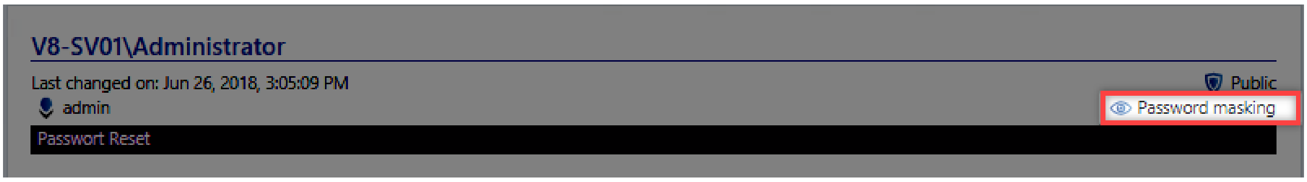
Protections

Password masking

The password masking follows the familiar logic of the client. Due to this function, reference should be made to the chapter of password masking.
There are marginal differences in the operation. The privacy protection is fixed or edited via a button in the extended menu.

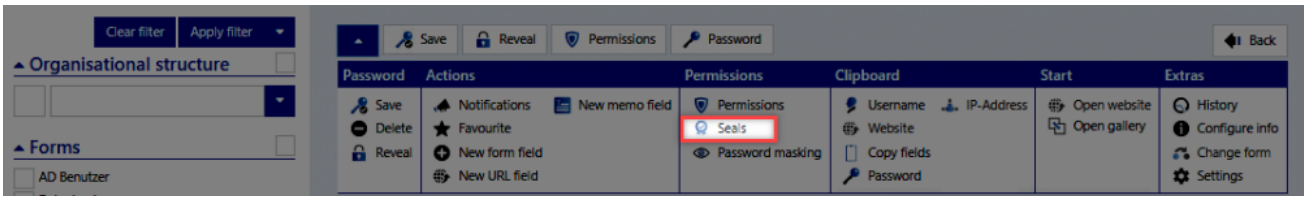


The corresponding button is only displayed if the logged in user has the sufficient rights.
If a record is provided with a privacy protection, this is shown in the header of the password.

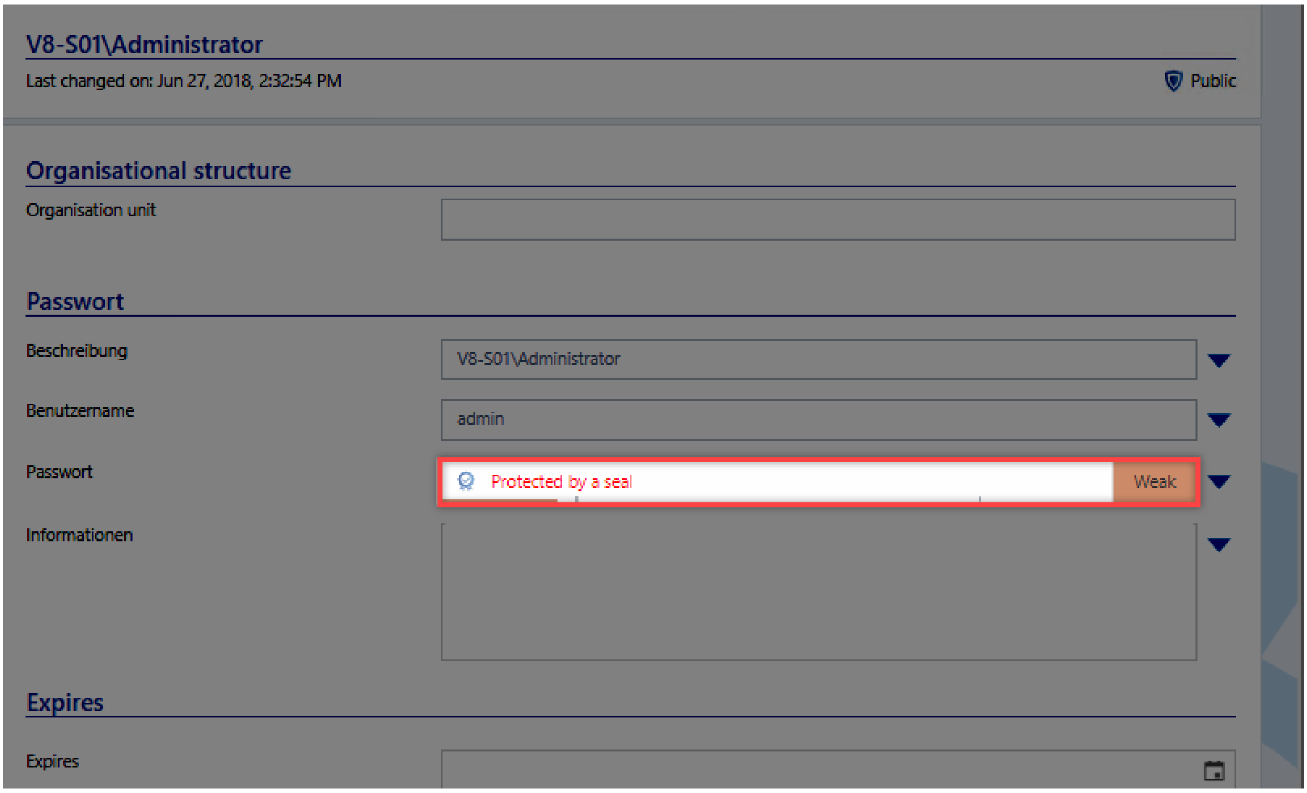


Seal

The seals also correspond in function to the known logic of the client. In the chapter seal further explanations can be found. The seals are configured in the extended menu via a button.



The button is only displayed for the users who have the rights to edit seals. If a record is sealed, this will be shown in the password field.

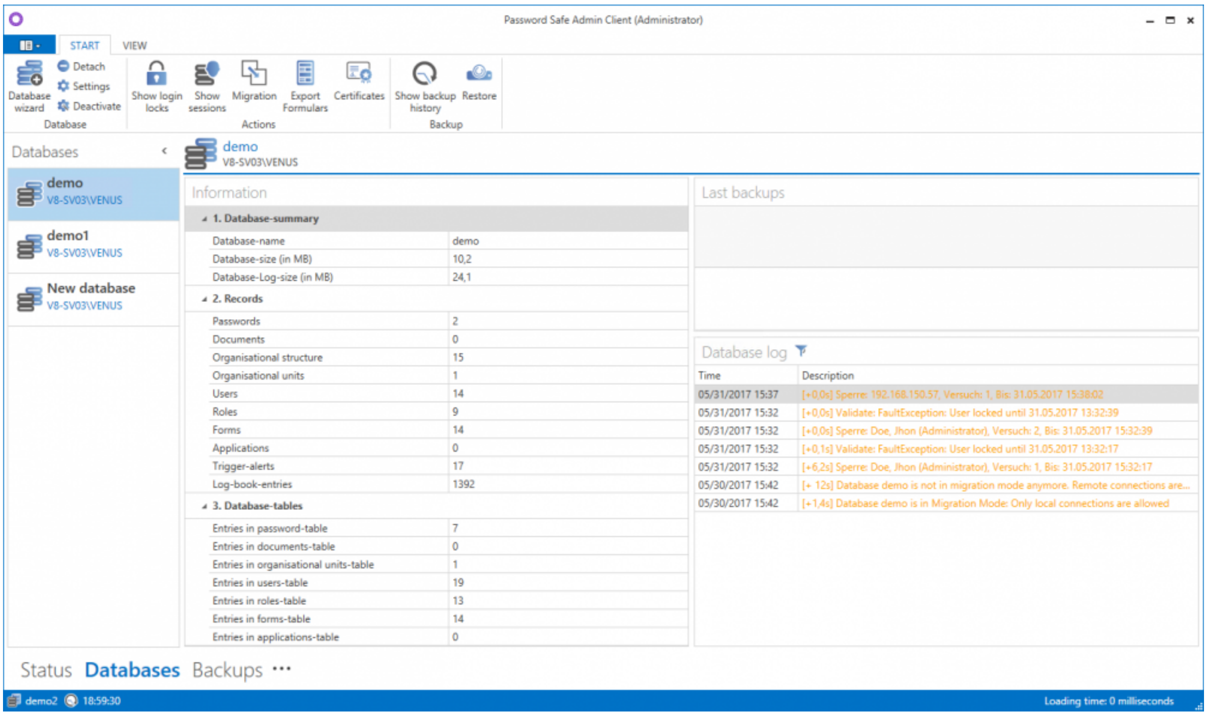


AdminClient

What is the AdminClient?

The AdminClient takes care of the central administration of the databases as well as the configuration of the backup profiles. In addition, it provides the very important interface to the Password Safe license server. Furthermore, it is used for the administration of globally defined settings, as well as the configuration of profiles for sending emails. Installing the AdminClient…

✻ The default password for the AdminClient is “admin”



1. Database-summary	
Database-name	demo
Database-size (in MB)	10,2
Database-Log-size (in MB)	24,1
2. Records	
Passwords	2
Documents	0
Organisational structure	15
Organisational units	1
Users	14
Roles	9
Forms	14
Applications	0
Trigger-alerts	17
Log-book-entries	1392
3. Database-tables	
Entries in password-table	7
Entries in documents-table	0
Entries in organisational units-table	1
Entries in users-table	19
Entries in roles-table	13
Entries in forms-table	14
Entries in applications-table	0

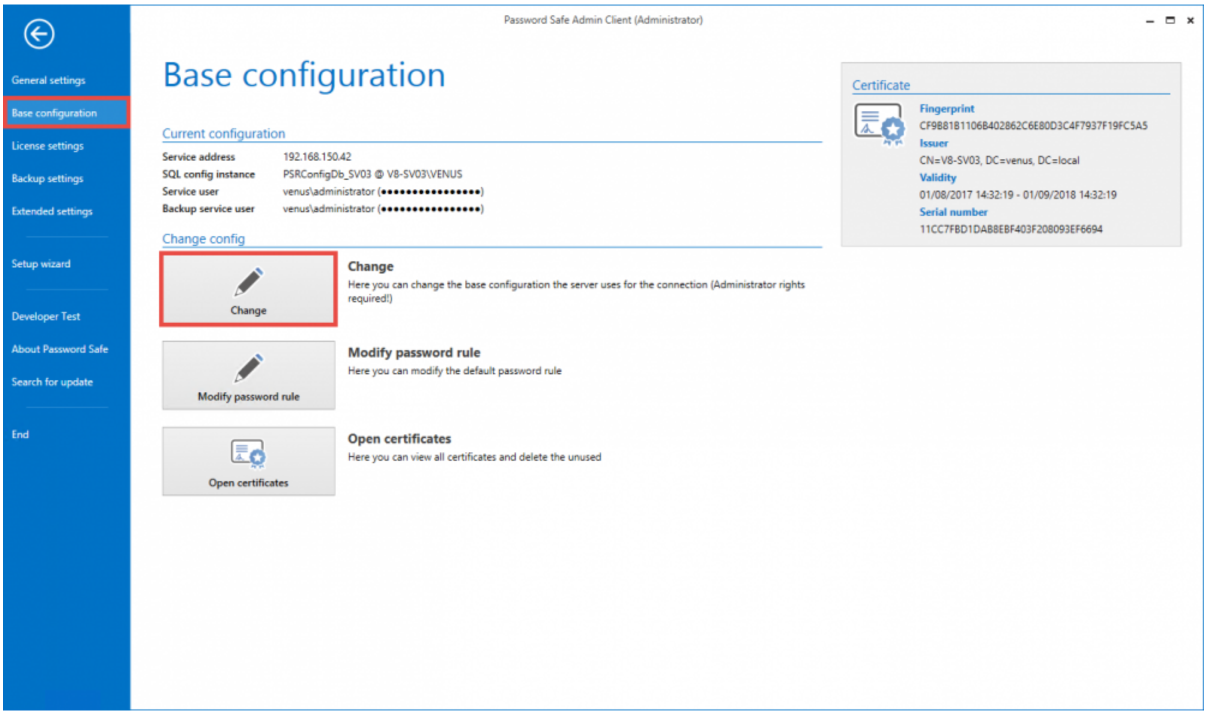
```
Time              Description
05/31/2017 15:37  [+0,0s] Sperre: 192.168.150.57, Versuch: 1, Bis: 31.05.2017 15:38:02
05/31/2017 15:32  [+0,0s] Validate: FaultException: User locked until 31.05.2017 13:32:39
05/31/2017 15:32  [+0,0s] Sperre: Doe, Jhon (Administrator), Versuch: 2, Bis: 31.05.2017 15:32:39
05/31/2017 15:32  [+0,1s] Validate: FaultException: User locked until 31.05.2017 13:32:17
05/31/2017 15:32  [+6,2s] Sperre: Doe, Jhon (Administrator), Versuch: 1, Bis: 31.05.2017 15:32:17
05/30/2017 15:42  [+ 12s] Database demo is not in migration mode anymore. Remote connections are...
05/30/2017 15:42  [+1,4s] Database demo is in Migration Mode: Only local connections are allowed
```

In this sense, the server service represents the interface between the client and the SQL server. The AdminClient is responsible for configuring the server service. It allows the central administration of the databases without having access to the SQL server. This is a huge advantage with regards to organization and authorizations.

Basic configuration

What is basic configuration?

The connection to the SQL server or databases is defined in the basic configuration. The basic configuration appears the first time the AdminClient is started and can be called up at any time in the basic configuration.



Base configuration

Current configuration

Service address	192.168.150.42
SQL config instance	PSRConfigDb_SV03 @ V8-SV03\VENUS
Service user	venus\administrator (●●●●●●●●●●●●●●●●)
Backup service user	venus\administrator (●●●●●●●●●●●●●●●●)

Change config

Change
Here you can change the base configuration the server uses for the connection (Administrator rights required!)

Modify password rule
Here you can modify the default password rule

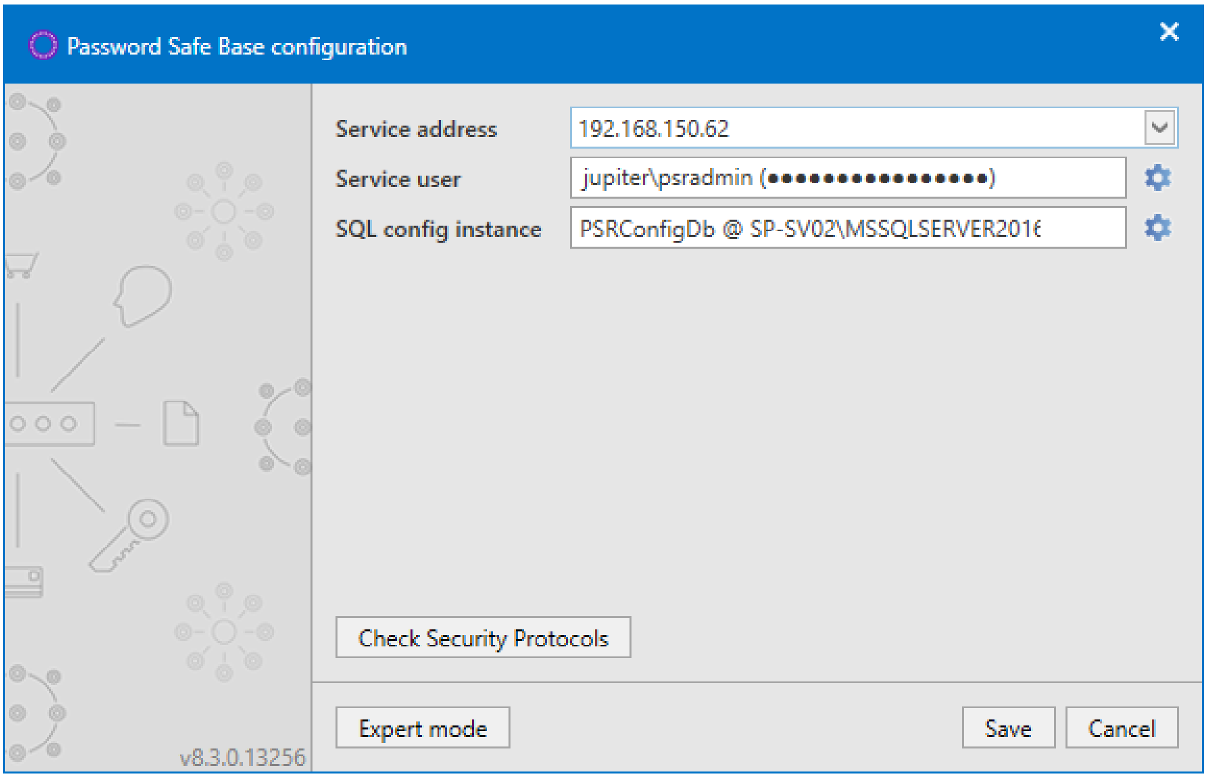
Open certificates
Here you can view all certificates and delete the unused

Certificate

Fingerprint
CF9B81B1106B402862C6E80D3C4F7937F19FC5A5
Issuer
CN=V8-SV03, DC=venus, DC=local
Validity
01/08/2017 14:32:19 - 01/09/2018 14:32:19
Serial number
11CC7FBD1DAB8EBF403F208093EF6694

The basic configuration

A special wizard is available to carry out the configuration:



Password Safe Base configuration

Service address: 192.168.150.62

Service user: jupiter\psradmin (●●●●●●●●●●●●●●●●)

SQL config instance: PSRConfigDb @ SP-SV02\MSSQLSERVER201€

Service address

The service address of the SQL server can be selected via the drop-down menu. It is mandatory to select the adapter via which the AdminClient can also access the SQL server.

The loopback address 127.0.0.1 should not be used here.

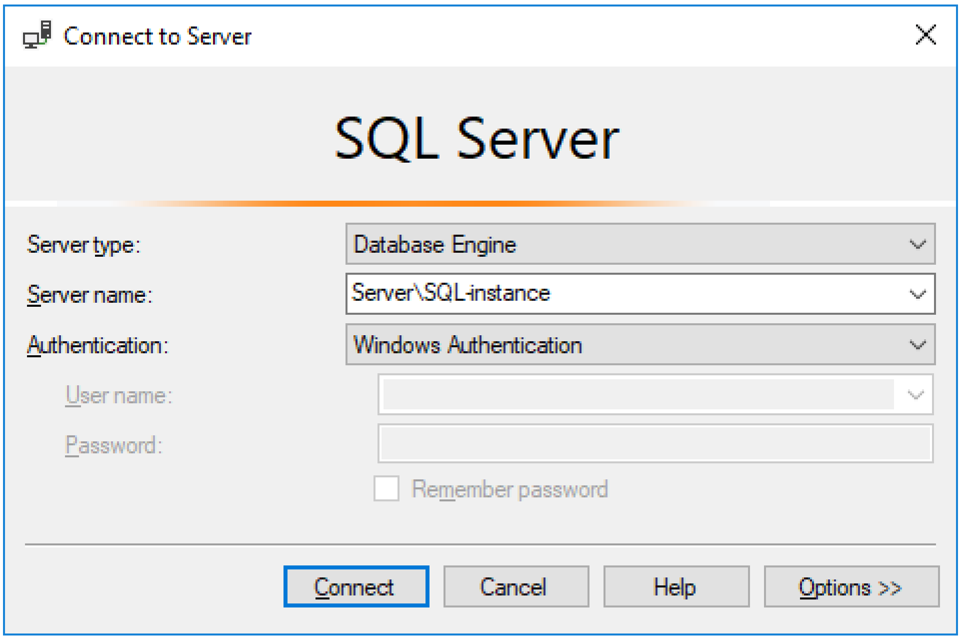
Service user

This setting is used to define the service user, which is needed to start the server service as well as the backup service. The “Use local system” setting starts the services with the local system account.

! The logged on user needs * local administrator rights * to properly configure the server and create databases.

SQL configuration instance

Under “SQL Server instance” the database server must be specified, including the SQL instance. For simplicity, you can copy the server name from the login window of the SQL server.



Server type: Database Engine
Server name: Server\SQL-instance
Authentication: Windows Authentication
User name:
Password:
□ Remember password

If the option “Service user” is selected, enter the user, which logs on to the SQL Server. Please note that “dbCreator” rights are necessary to create a configuration database. “dbOwner” rights are sufficient if the database is created manually on the SQL server and is only accessed here. Enter the name of the configuration database under “Database”.

Refer to the “System Requirements Server” section :#systemanforderungen-serverfor more information about your users.

Expert mode

Expert mode displays a menu item for configuring a backup user – the service user is used here by default. Furthermore, the SQL instance can be configured via “Connection string”.
The SSL certificate can also be configured to protect the client server connection. By default, a certificate is generated by the AdminClient However, you can also choose your own. Further information can be found directly in the section provided for this purpose.

! Exchanging or overwriting an existing certificate may cause warnings to the clients if the certificate is not trusted at each client.

Click here to return to the “Getting started” section

Certificates

Various different certificates are used to guarantee the security of Password Safe. The certificates are essential for the smooth operation of Password Safe. It is thus important that they are carefully backed up.

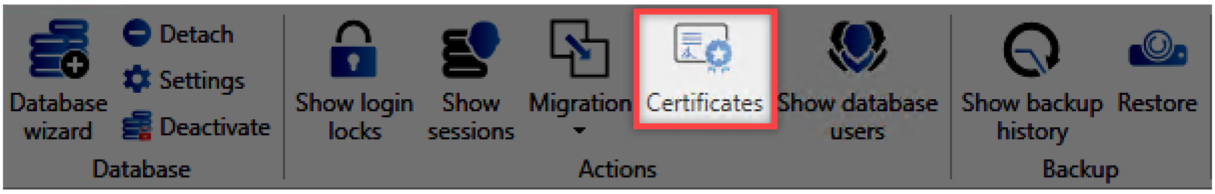
What certificates are used

The individual certificates are described in the following sections:

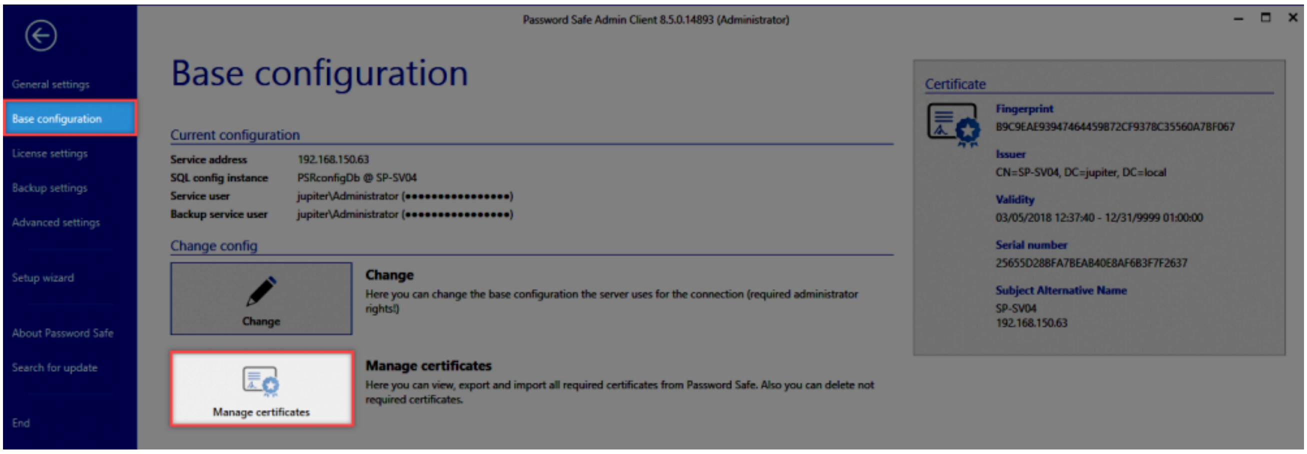
- SSL connection certificates
- Database certificates
- Master Key certificates
- Discovery service certificates
- Password Reset certificates

Calling up the certificate manager

There are two ways to open the certificate manager. The certificates for each specific database can be managed via the ribbon:



In the **Main menu**, it is also possible to start the certificate manager for all databases under the **basic configuration**:



Base configuration

Current configuration

Service address 192.168.150.63
SQL config instance PSRconfigDb @ SP-SV04
Service user jupiter\Administrator (●●●●●●●●●●●●●●●●)
Backup service user jupiter\Administrator (●●●●●●●●●●●●●●●●)

Change config

Change

Change
Here you can change the base configuration the server uses for the connection (required administrator rights!)

Manage certificates

Manage certificates
Here you can view, export and import all required certificates from Password Safe. Also you can delete not required certificates.

Certificate

Fingerprint
B9C9EAE93947464459B72CF9378C35560A7BF067

Issuer
CN=SP-SV04, DC=jupiter, DC=local

Validity
03/05/2018 12:37:40 - 12/31/9999 01:00:00

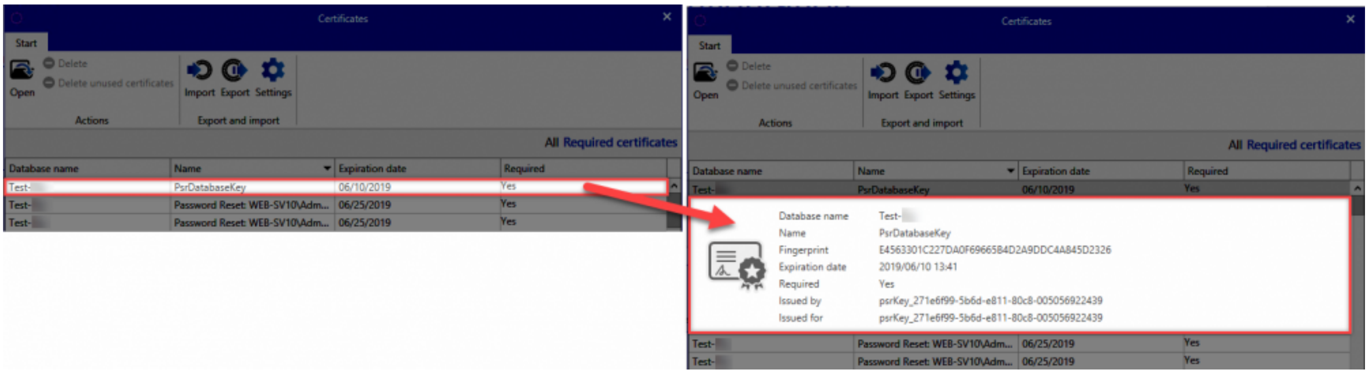
Serial number
25655D28BFA7BEAB40E8AF6B3F7F2637

Subject Alternative Name
SP-SV04
192.168.150.63

Operation of the certificate manager is always the same. The only difference is whether the certificates are displayed for each database or for all databases.

Checking existing certificates

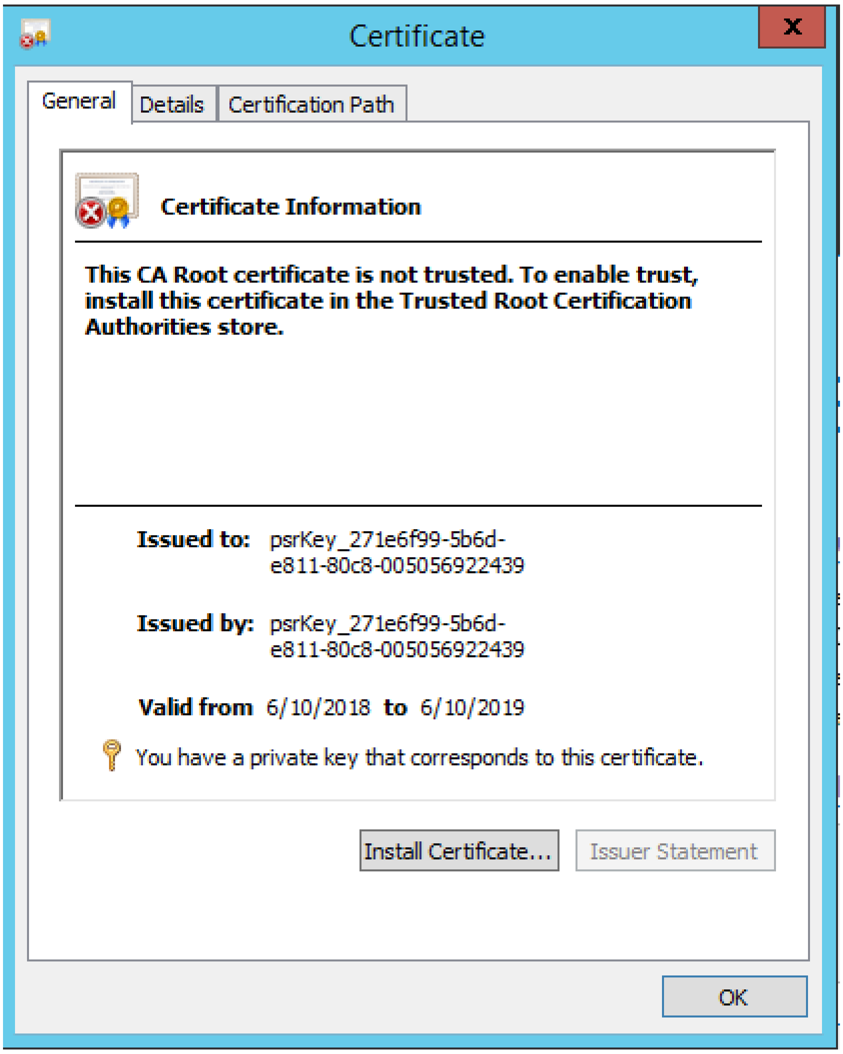
After opening the certificate manager, all certificates specific to Password Safe will be displayed. Clicking on the certificate will display further information.



Database name	Name	Expiration date	Required
Test-[redacted]	PsrDatabaseKey	06/10/2019	Yes
Test-[redacted]	Password Reset: WEB-SV10\Adm...	06/25/2019	Yes
Test-[redacted]	Password Reset: WEB-SV10\Adm...	06/25/2019	Yes

Database name	Test-[redacted]
Name	PsrDatabaseKey
Fingerprint	E4563301C227DA0F69665B4D2A9DDC4A845D2326
Expiration date	2019/06/10 13:41
Required	Yes
Issued by	psrKey_271e6f99-5b6d-e811-80c8-005056922439
Issued for	psrKey_271e6f99-5b6d-e811-80c8-005056922439

Double clicking on a certificate will open the Windows Certificate Manger for even more detailed information.



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: psrKey_271e6f99-5b6d-e811-80c8-005056922439

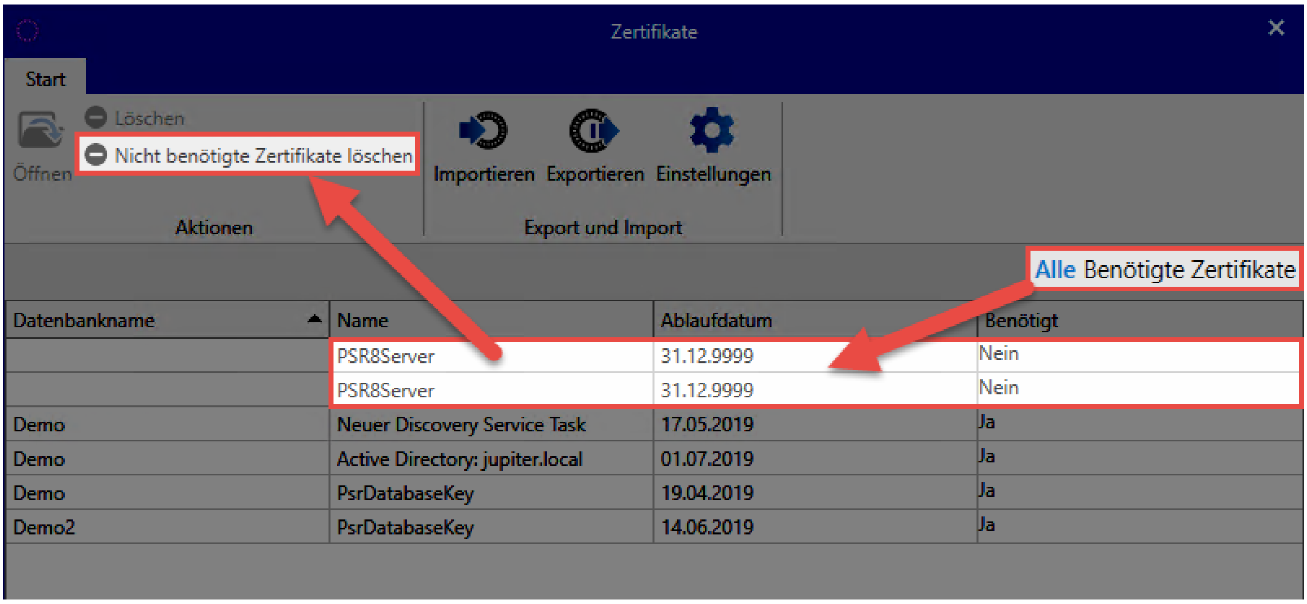
Issued by: psrKey_271e6f99-5b6d-e811-80c8-005056922439

Valid from 6/10/2018 to 6/10/2019

You have a private key that corresponds to this certificate.

Required certificates / deleting no longer required certificates

The overview will initially only display those certificates that are being used and are thus required. Clicking on **All** will also display the no longer required certificates. For example, it is possible that outdated certificates exist on the machine due to a test installation. These certificates can be easily deleted via the corresponding button in the ribbon.



Datenbankname	Name	Ablaufdatum	Benötigt
	PSR8Server	31.12.9999	Nein
	PSR8Server	31.12.9999	Nein
Demo	Neuer Discovery Service Task	17.05.2019	Ja
Demo	Active Directory: jupiter.local	01.07.2019	Ja
Demo	PsrDatabaseKey	19.04.2019	Ja
Demo2	PsrDatabaseKey	14.06.2019	Ja

Importing certificates

Previously backed up certificates can be integrated into the installation via the **Import** button. This merely requires you to enter the desired .pfx file and its password.

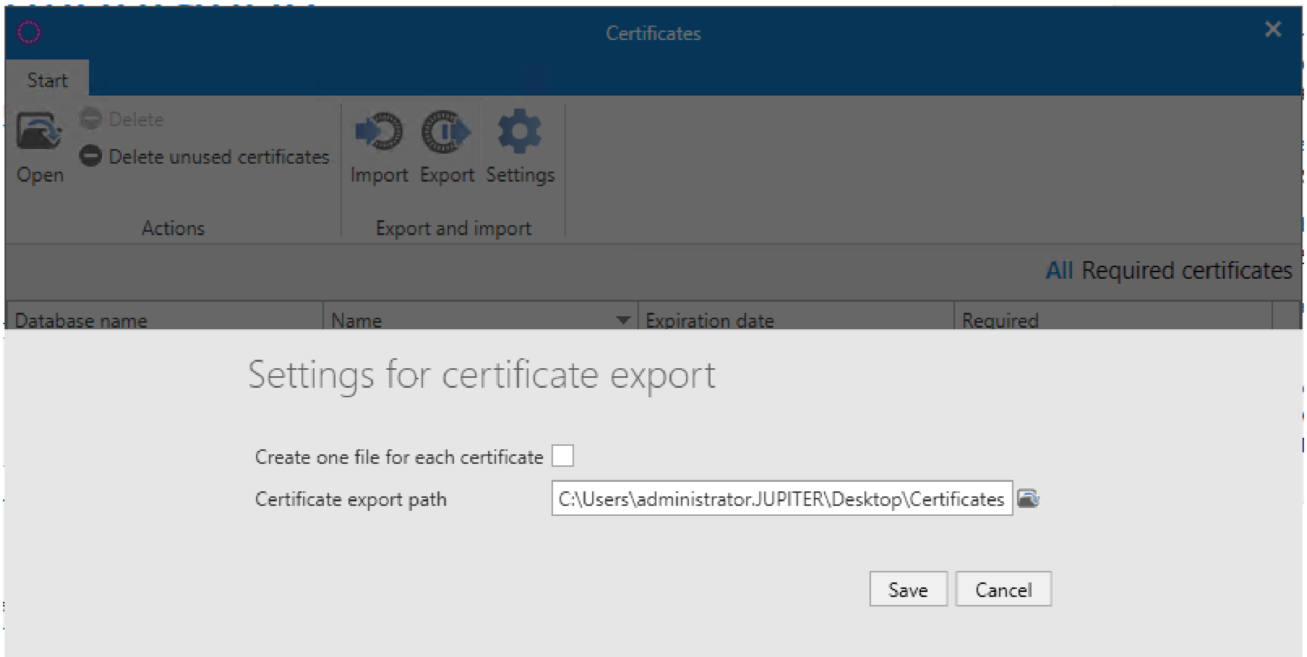
Exporting certificates

The relevant certificates will be backed up by clicking on **export**. A password firstly needs to be issued here. If a storage location has not yet been entered via the **settings**, you are firstly asked to enter it.

SSL connection certificates are not included in this process and are also not backed up. These certificates can be recreated if necessary.

Settings

You can define whether every certificate should be saved to its own file in the **settings**. If this option has not been activated, all relevant certificates will be backed up in one file. In addition, the storage location is defined in the settings.



Settings for certificate export

Create one file for each certificate □

Certificate export path C:\Users\administrator.JUPITER\Desktop\Certificates

Backing up certificates

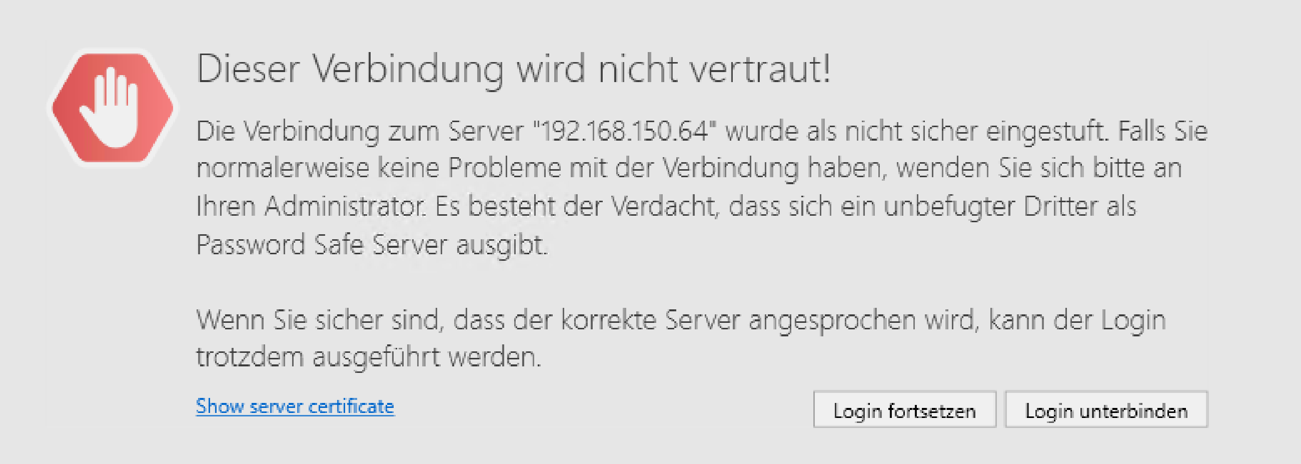
If you want to automatically back up the certificates on a cyclical basis, this can be done via the backup system. Further information can be found in the section Backup management.

SSL connection certificates

What is an SSL connection certificate?

The connection between clients and the server is secured via an SSL certificate. The **latest encryption standard TLS 1.2** is used here. It is also possible to create a certificate via the server, as well as to use an existing certificate with a CA. All computers on which a client is installed must trust the certificate. Otherwise, the following message will appear when the client is started:

This connection is not trusted!
The connection to the server is not considered secure.



Dieser Verbindung wird nicht vertraut!

Die Verbindung zum Server "192.168.150.64" wurde als nicht sicher eingestuft. Falls Sie normalerweise keine Probleme mit der Verbindung haben, wenden Sie sich bitte an Ihren Administrator. Es besteht der Verdacht, dass sich ein unbefugter Dritter als Password Safe Server ausgibt.

Wenn Sie sicher sind, dass der korrekte Server angesprochen wird, kann der Login trotzdem ausgeführt werden.

Windows Server 2012 R2 requires the latest patch level, since it has been delivered with SSL3, and has been extended to include TLS 1.2

! The service user creates the databases. A separate certificate is also generated for each database. Therefore, the **service user** must be a **local administrator** or a **domain administrator**, as otherwise they would have no rights to save data in the certificate store.

Structure of certificates

The following information applies to both the **Password Safe certificate** and also to your **own certificates**:

Alternative applicant

Communication between the client and server can only take place using the path that is stored in the certificate with the alternative applicant. Therefore, the Password Safe certificate stores all IP addresses for the server, as well as the hostname. When creating your own certificate, this information should also be saved under the alternative applicant.

Using the Password Safe certificate

The name of the PSR certificate is **PSR8Server**. This can be done via the basic configuration in the AdminConsole. The certificate is saved locally under:
Local computer -> own certificates -> certificates

> ✻ The certificate is valid from its creation up to the year 9999 – and is thus valid almost indefinitely. For this reason, it is not necessary to note any expiry date.

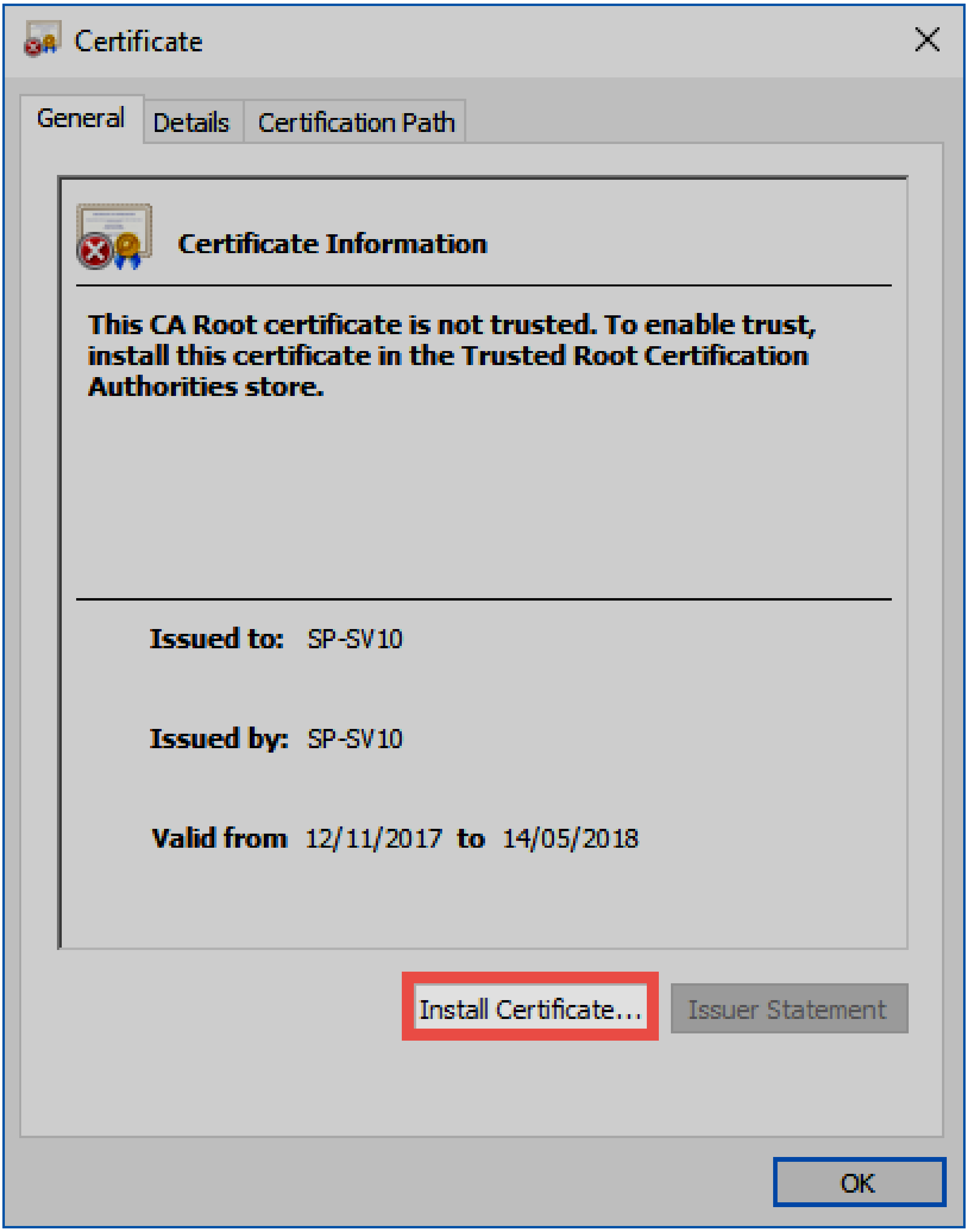
Distributing the Password Safe certificate

In order for the certificate to be trusted, it can be exported to the server and then imported to the clients. The following storage location needs to be selected here:
local computer -> trusted root certificate location -> certificates

The certificate can be both rolled out and distributed using group guidelines.

Manually importing the Password Safe certificate

If the Password Safe certificate is not rolled out, it is also possible to manually import the certificate. To do this, firstly open the certificate information. In the warning notification, the **Show server certificate** button is available for this purpose. In the following dialogue, select the option **Install certificate…**



Certificate Information

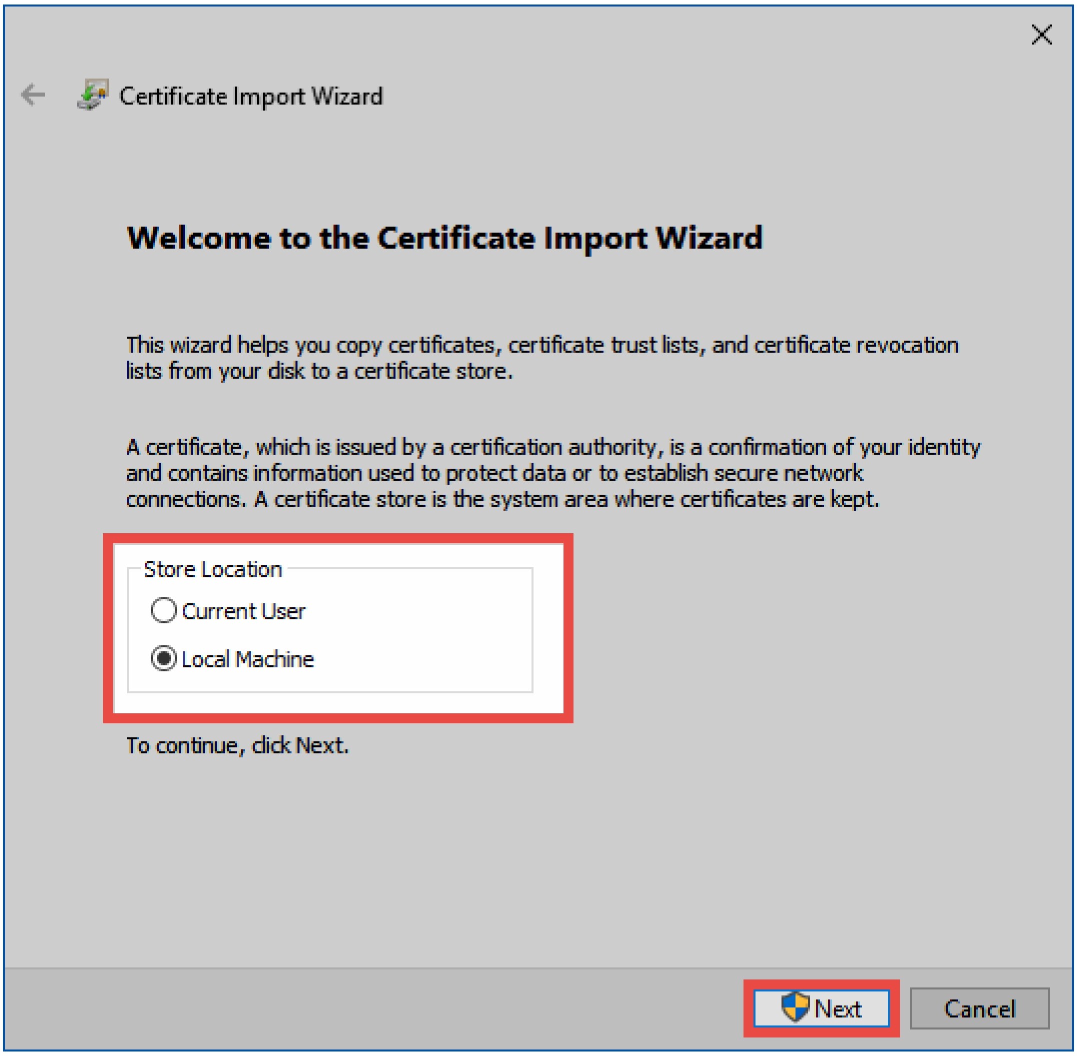
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SP-SV10

Issued by: SP-SV10

Valid from 12/11/2017 to 14/05/2018

A **Certificate import wizard** will open in which **Local computer** should be selected.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

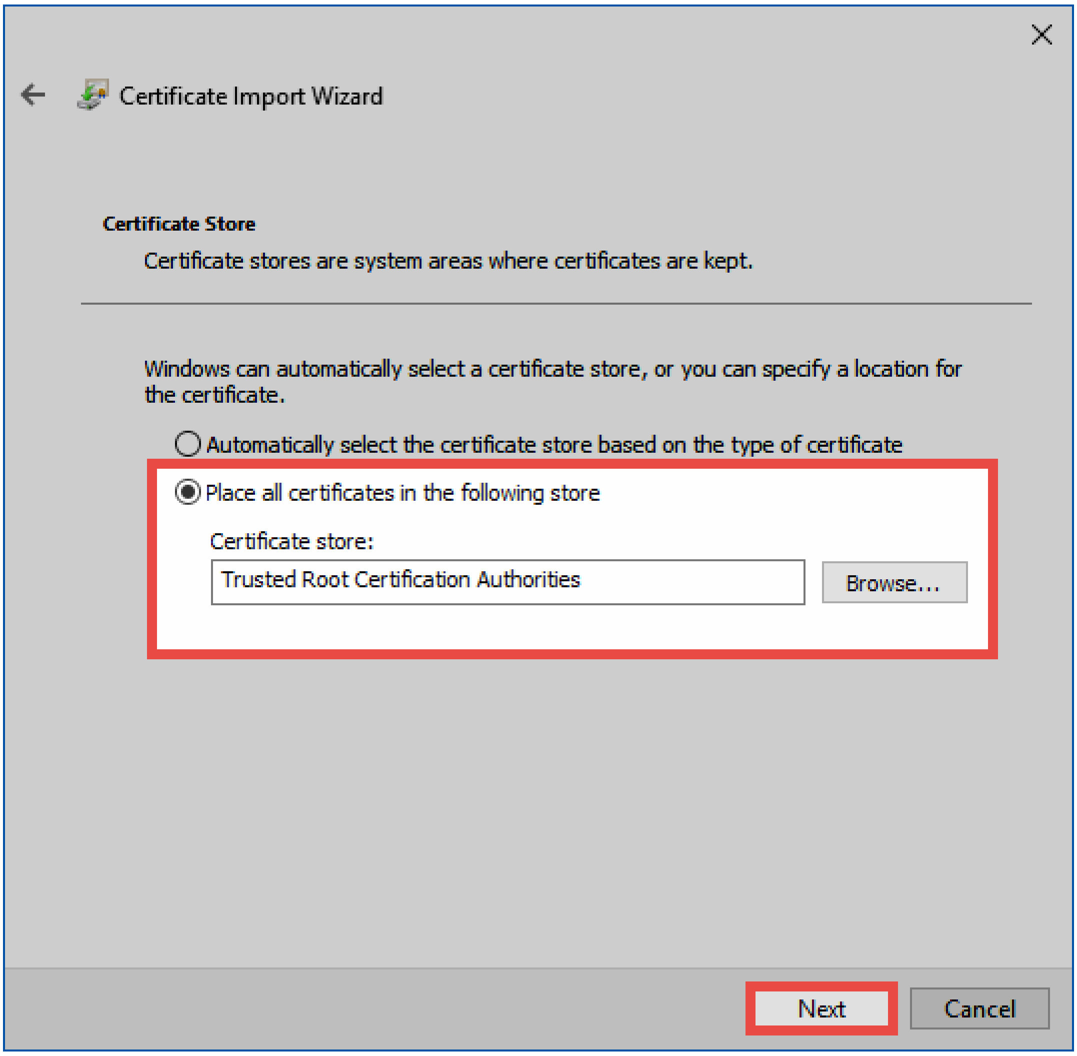
Store Location

○ Current User

● Local Machine

To continue, click Next.

In the next step, the storage location “trusted root certificate location” needs to be manually selected.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Finally, the installation needs to be confirmed once again.

The user logged in to the operating system requires rights to create certificates

Using your own certificate

If a CA already exists, you can also use your own certificate. You can specify this within the basic configuration. Please note that a server certificate for SSL encryption is used here. The CA must be configured so that all clients trust the certificate. It is necessary to adhere to the certification path.

! When creating the certificate, ensure that Password Safe only supports the Cryptographic Service Provider (CSP) and not the Key Storage Provider (KSP)

! When configuring, you must ensure that the clients can access the CA lock lists

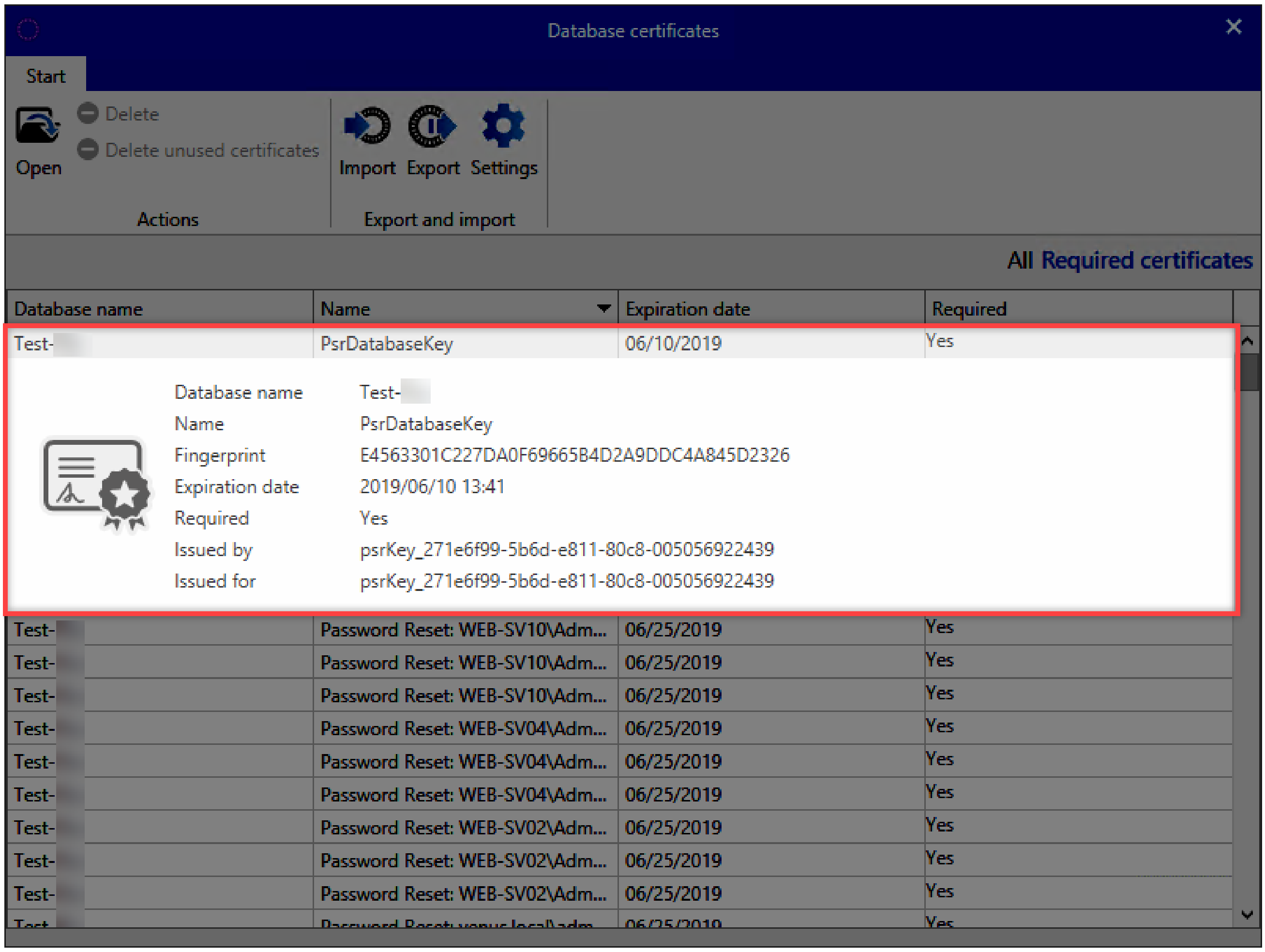
Wildcard certificates

Wildcard certificates are not supported. In theory, it should be possible to use them but we cannot help with the configuration. You can use wildcard certificates at your own responsibility.

Database certificates

What is a database certificate?

A unique certificate is created for each database. This has the name **psrDatabaseKey**:



Database name	Name	Expiration date	Required
Test-	PsrDatabaseKey	06/10/2019	Yes
Test-	Password Reset: WEB-SV10\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV10\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV10\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV04\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV04\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV04\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV02\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV02\Adm...	06/25/2019	Yes
Test-	Password Reset: WEB-SV02\Adm...	06/25/2019	Yes
Test-	Password Reset: venus.local\adm...	06/25/2019	Yes

Database name	Test-
Name	PsrDatabaseKey
Fingerprint	E4563301C227DA0F69665B4D2A9DDC4A845D2326
Expiration date	2019/06/10 13:41
Required	Yes
Issued by	psrKey_271e6f99-5b6d-e811-80c8-005056922439
Issued for	psrKey_271e6f99-5b6d-e811-80c8-005056922439

The database certificate **does not encrypt the database**. Rather, it is used for the encrypted transfer of passwords from the client to the server in the following cases:

- Creation of a WebViewer via a task
- Creation of an AD profile protected by a master key
- Login of users imported from AD in Master Key mode

The database certificate **cannot** be replaced by your own certificate.

✻ The expiry date for the database certificate is not checked. The certificate thus does not need to be renewed.

! If the database is being moved to another server, it is **essential that the certificate is also transferred**!

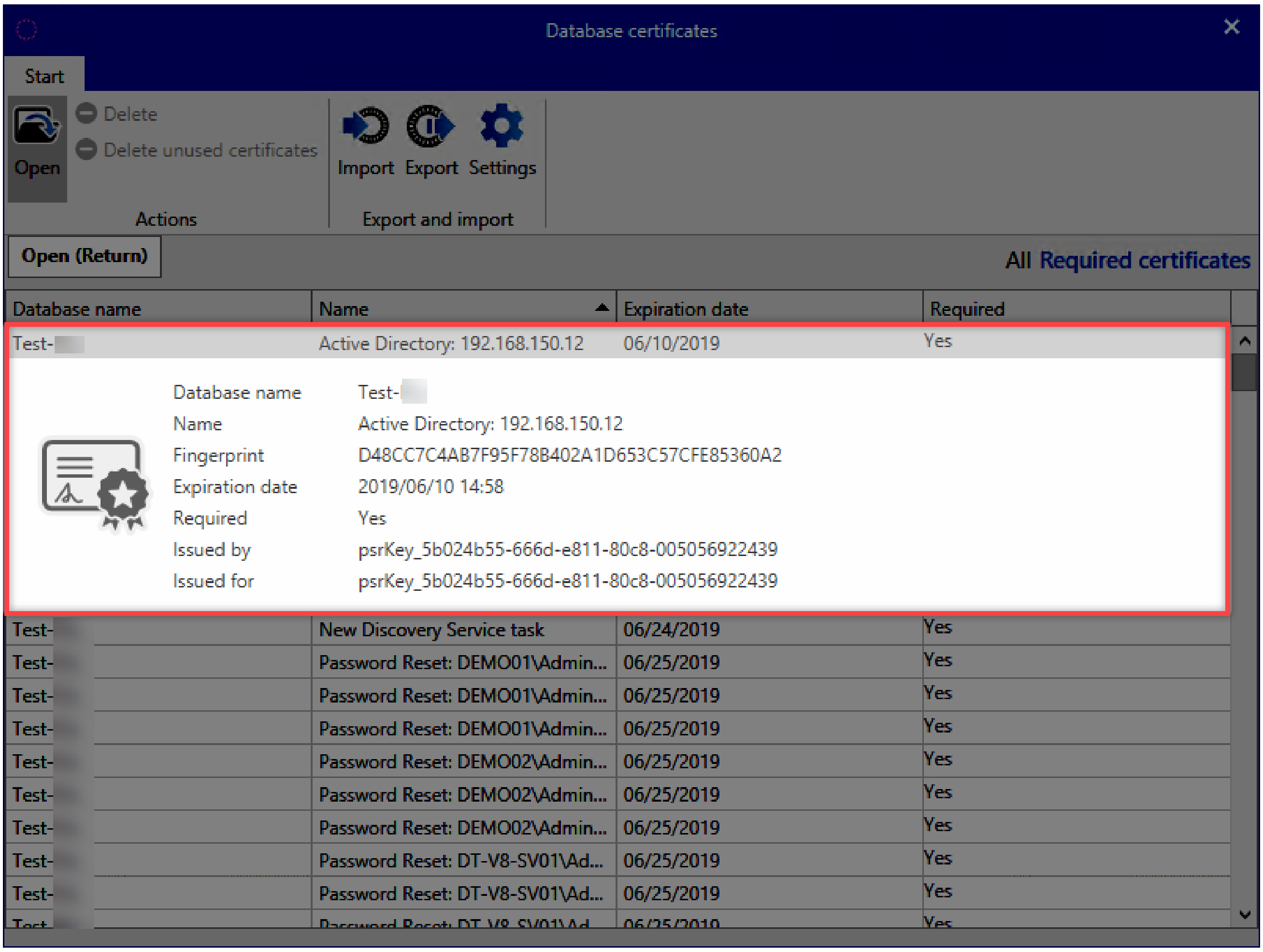
Exporting and importing the certificate

The section certificates explains how to back up the certificate and link it again.

Master Key certificates

What is a Master Key certificate?

If Active Directory is accessed via Master Key mode, a certificate will be created. This has the name **Active Directory: Domain**:



Database name	Name	Expiration date	Required
Test-[redacted]	Active Directory: 192.168.150.12	06/10/2019	Yes

Database name	Test-[redacted]
Name	Active Directory: 192.168.150.12
Fingerprint	D48CC7C4AB7F95F78B402A1D653C57CFE85360A2
Expiration date	2019/06/10 14:58
Required	Yes
Issued by	psrKey_5b024b55-666d-e811-80c8-005056922439
Issued for	psrKey_5b024b55-666d-e811-80c8-005056922439

Database name	Name	Expiration date	Required
Test-[redacted]	New Discovery Service task	06/24/2019	Yes
Test-[redacted]	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-[redacted]	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes
Test-[redacted]	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes
Test-[redacted]	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes

The Master Key certificate **cannot** be replaced by your own certificate.

The **certificates for Master Key mode** have an expiry date. However, this is not checked. The certificate thus does not need to be renewed.

! If the database is being moved to another server, it is **essential that the Master Key certificate is also transferred**!

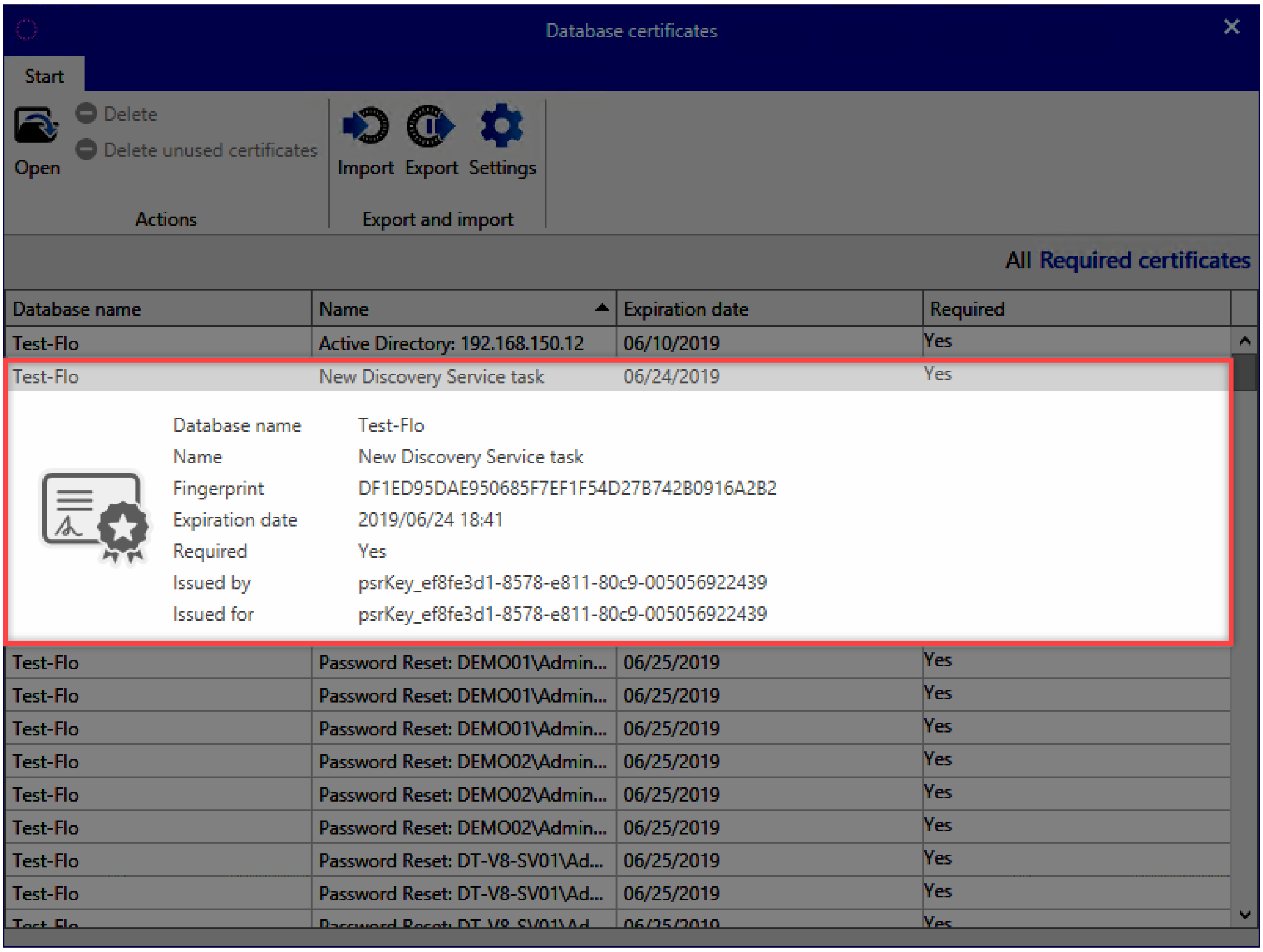
Exporting and importing the certificate

The section certificates explains how to back up the certificate and link it again.

Discovery service certificates

What is a discovery service certificate?

If a discovery service is created, a corresponding certificate is also created:



Database name	Name	Expiration date	Required
Test-Flo	Active Directory: 192.168.150.12	06/10/2019	Yes
Test-Flo	New Discovery Service task	06/24/2019	Yes

Database name Test-Flo
Name New Discovery Service task
Fingerprint DF1ED95DAE950685F7EF1F54D27B742B0916A2B2
Expiration date 2019/06/24 18:41
Required Yes
Issued by psrKey_ef8fe3d1-8578-e811-80c9-005056922439
Issued for psrKey_ef8fe3d1-8578-e811-80c9-005056922439

Database name	Name	Expiration date	Required
Test-Flo	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DEMO01\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DEMO02\Admin...	06/25/2019	Yes
Test-Flo	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes
Test-Flo	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes
Test-Flo	Password Reset: DT-V8-SV01\Ad...	06/25/2019	Yes

The discovery service certificate **cannot** be replaced by your own certificate.

The **certificates for the discovery service** have an expiry date. However, this is not checked. The certificate thus does not need to be renewed.

! If the database is being moved to another server, it is **essential that the discovery service certificate is also transferred**!

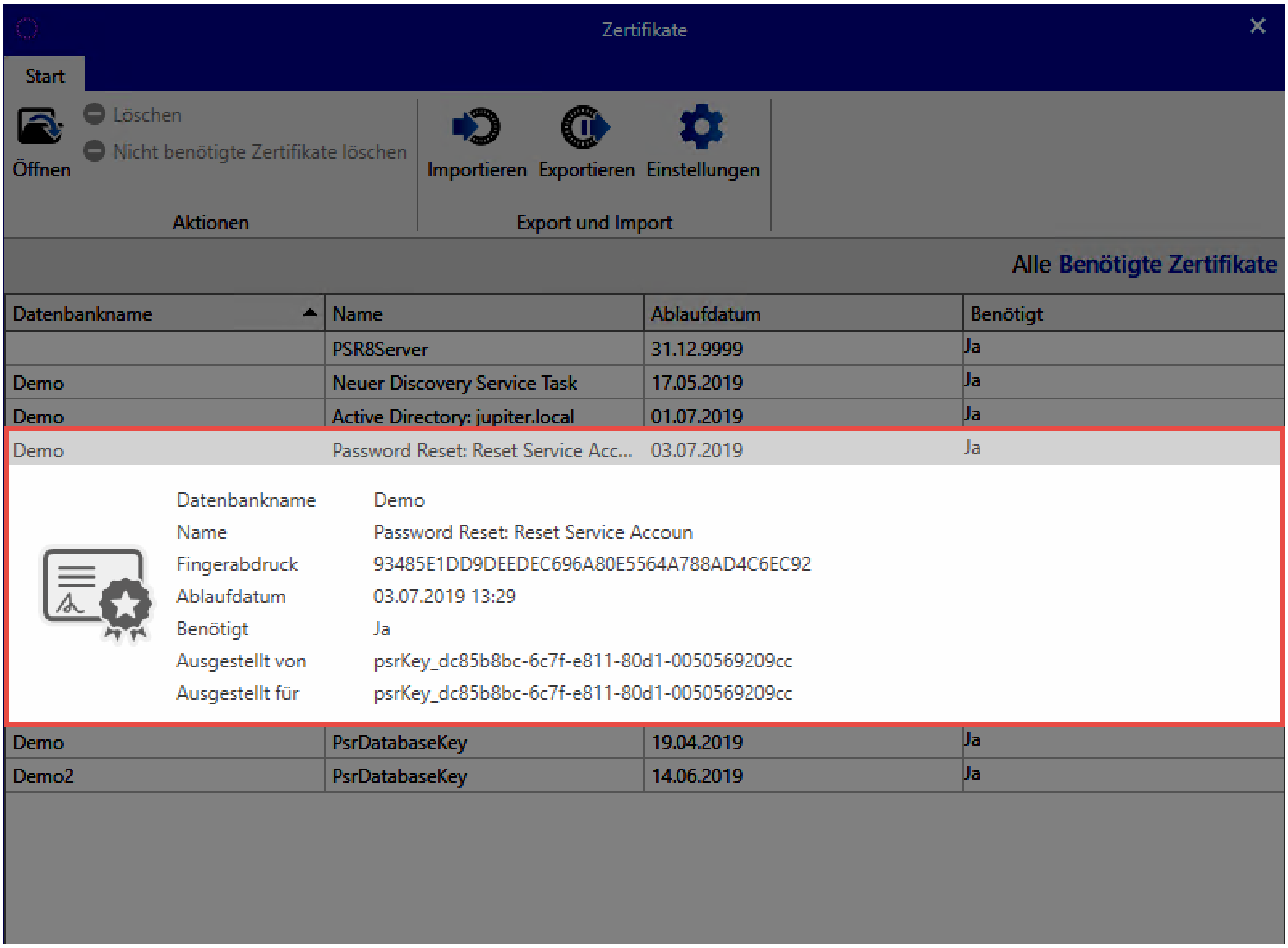
Exporting and importing the certificate

The section certificates explains how to back up the certificate and link it again.

Password Reset certificates

What is a Password Safe certificate?

If a Password Reset is created, a corresponding certificate is created. This ensures that the passwords are transferred in encrypted form.



Datenbankname	Name	Ablaufdatum	Benötigt
	PSR8Server	31.12.9999	Ja
Demo	Neuer Discovery Service Task	17.05.2019	Ja
Demo	Active Directory: jupiter.local	01.07.2019	Ja
Demo	Password Reset: Reset Service Acc...	03.07.2019	Ja
Demo	PsrDatabaseKey	19.04.2019	Ja
Demo2	PsrDatabaseKey	14.06.2019	Ja

Datenbankname	Demo
Name	Password Reset: Reset Service Accoun
Fingerabdruck	93485E1DD9DEEDEC696A80E5564A788AD4C6EC92
Ablaufdatum	03.07.2019 13:29
Benötigt	Ja
Ausgestellt von	psrKey_dc85b8bc-6c7f-e811-80d1-0050569209cc
Ausgestellt für	psrKey_dc85b8bc-6c7f-e811-80d1-0050569209cc

The Password Reset certificate **cannot** be replaced by your own certificate.

The **certificates for the Password Reset** have an expiry date. However, this is not checked. The certificate thus does not need to be renewed.

! If the database is being moved to another server, it is **essential that all Password Reset certificate is also transferred**!

Exporting and importing the certificate

The section certificates explains how to back up the certificate and link it again.

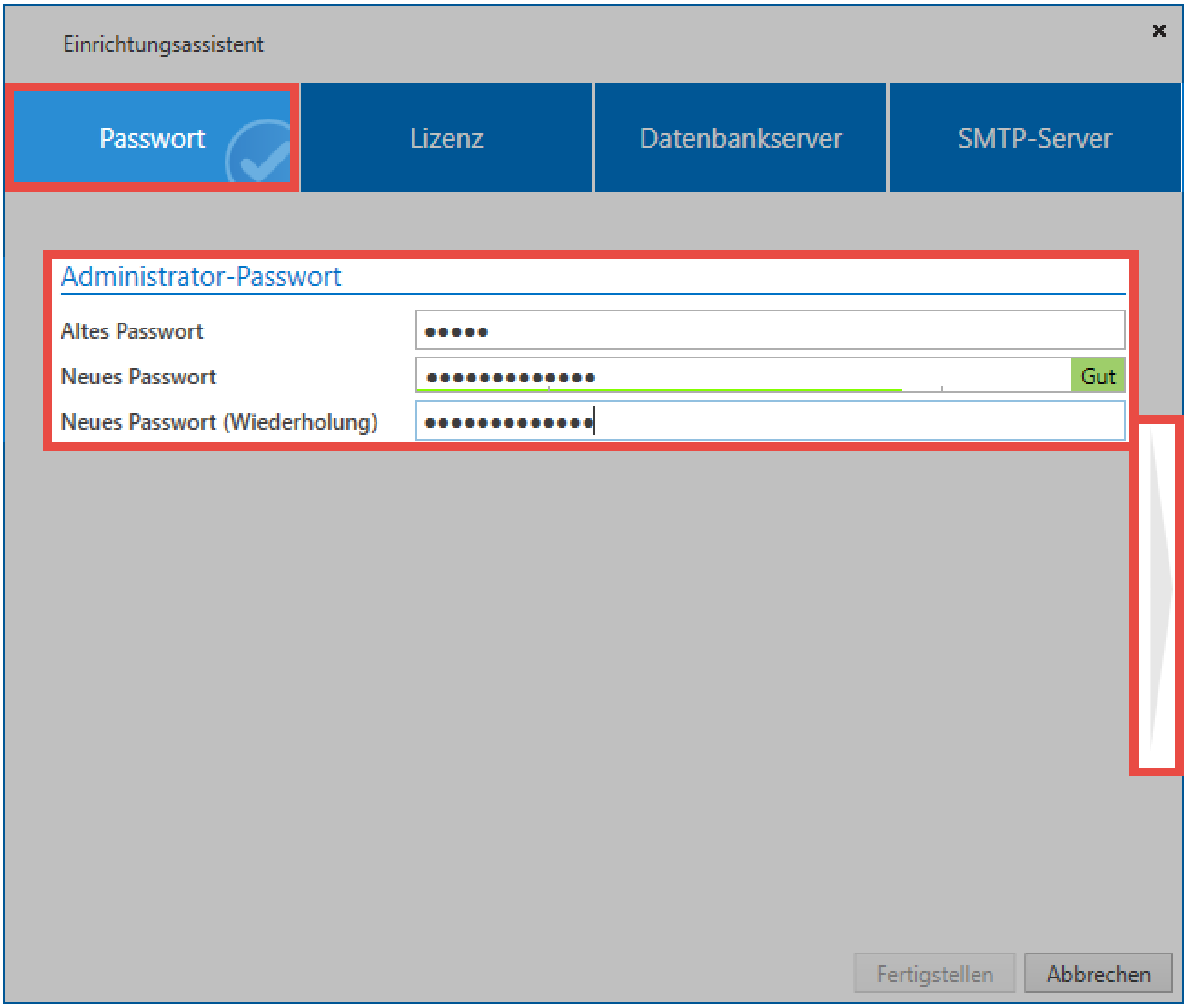
Setup wizard

What is the setup wizard?

The setup wizard contains all relevant settings for setting up Password Safe. The individual points can also be changed later on. Separate sections are available for each.

Defining the administrator password

The first step is to define the authentication password for the AdminClient. The initial password is “admin”. A new password needs to be entered during startup – this new password should be securely and properly documented. It can be subsequently changed in the general settings.



Administrator-Passwort

Altes Passwort ●●●●●

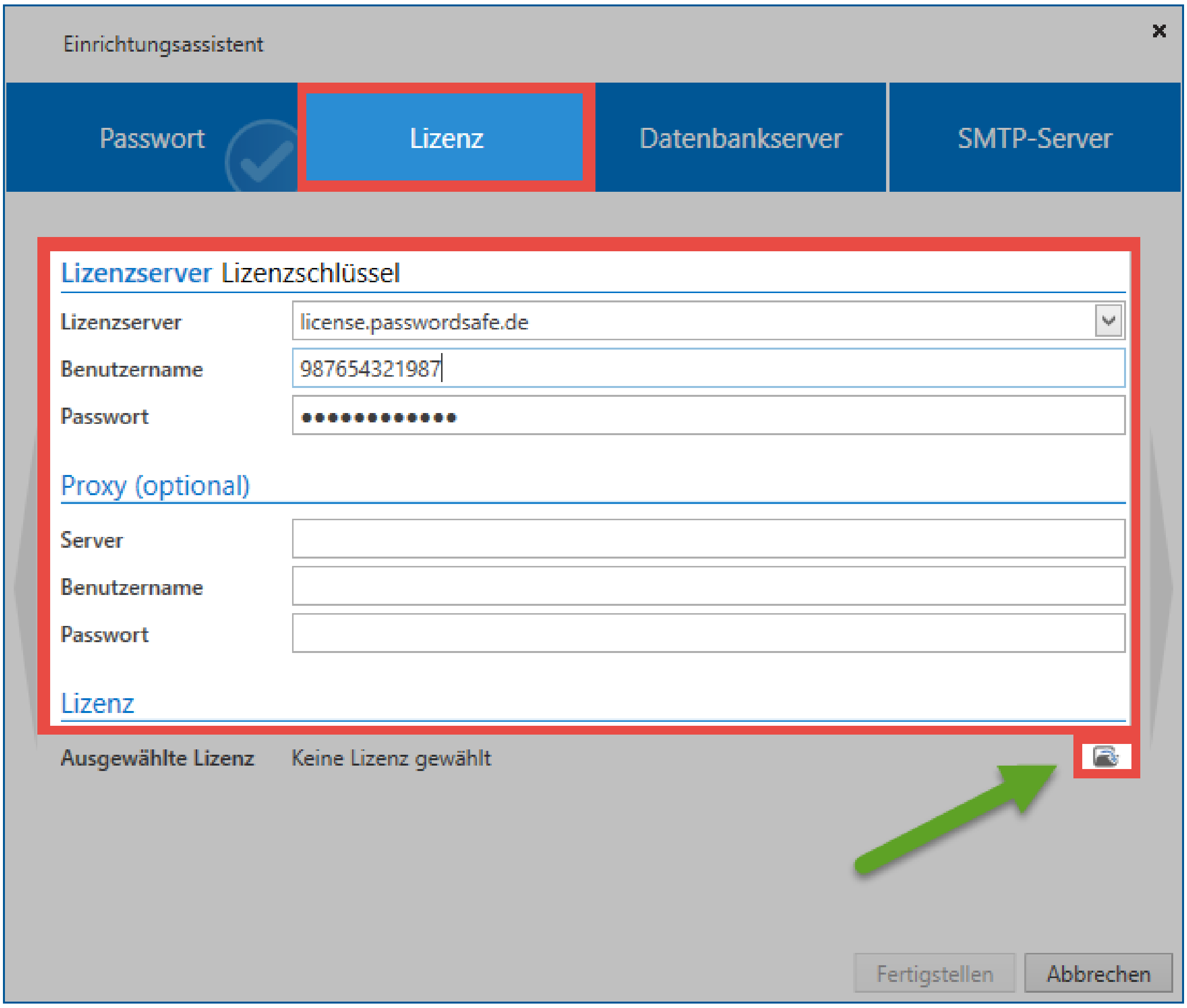
Neues Passwort ●●●●●●●●●●●●● Gut

Neues Passwort (Wiederholung) ●●●●●●●●●●●●●

The initial password is “admin”.

License settings

The second step is to complete the configuration for successively connecting to the licence server. This step can also be carried out later “in the licence settings”:#lizenzeinstellungen.



Lizenzserver: license.passwordsafe.de

Benutzername: 987654321987

Passwort: ●●●●●●●●●●●●

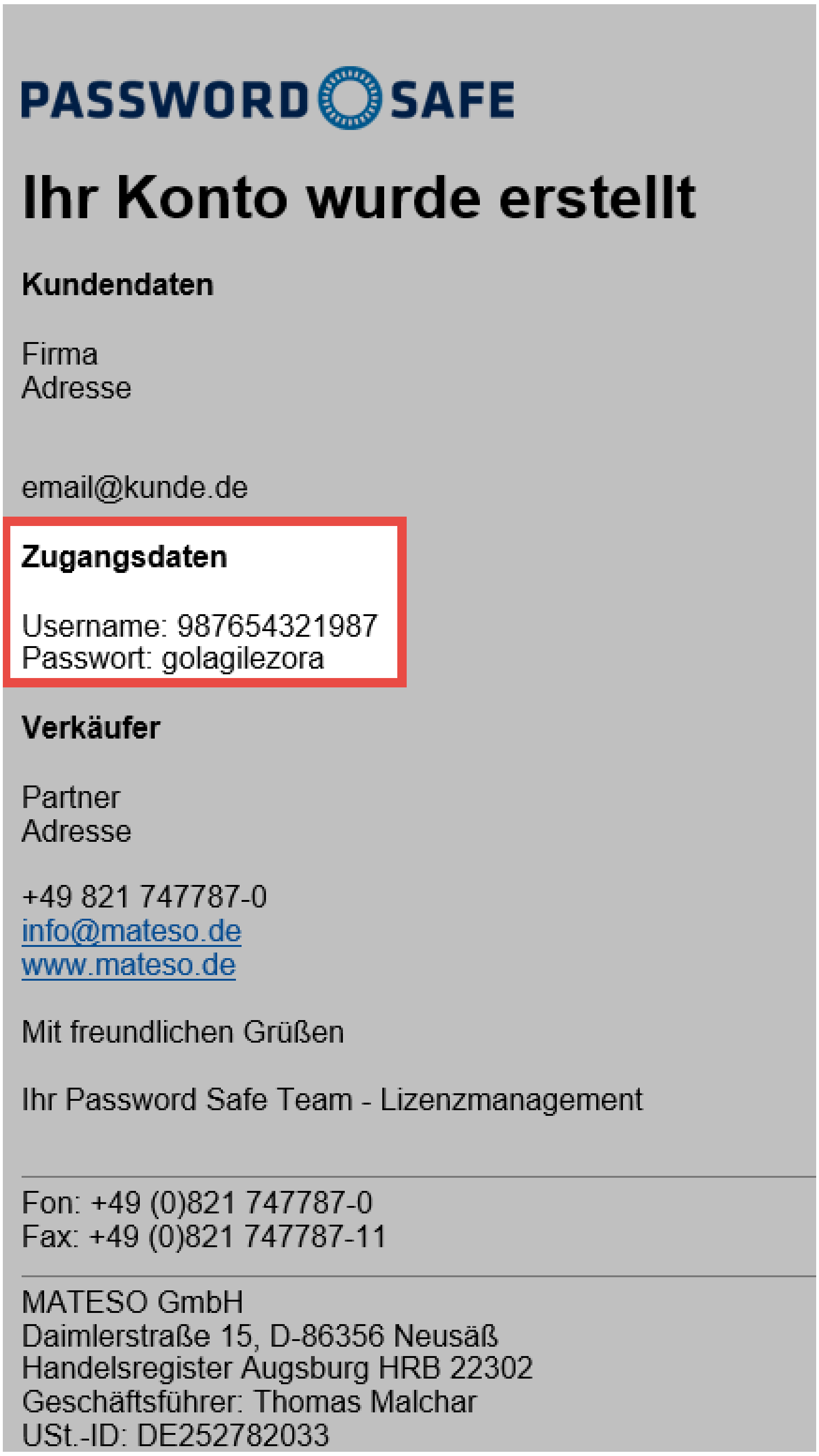
Server:

Benutzername:

Passwort:

Ausgewählte Lizenz: Keine Lizenz gewählt

“license.passwordsafe.de” should be entered in the field “Licence server”. The other access data (user name and password for the licence server will be sent to you by email).



Ihr Konto wurde erstellt

Kundendaten

Firma
Adresse

email@kunde.de

Zugangsdaten

Username: 987654321987
Passwort: golagilezora

Verkäufer

Partner
Adresse

+49 821 747787-0
info@mateso.de
www.mateso.de

Mit freundlichen Grüßen

Ihr Password Safe Team - Lizenzmanagement

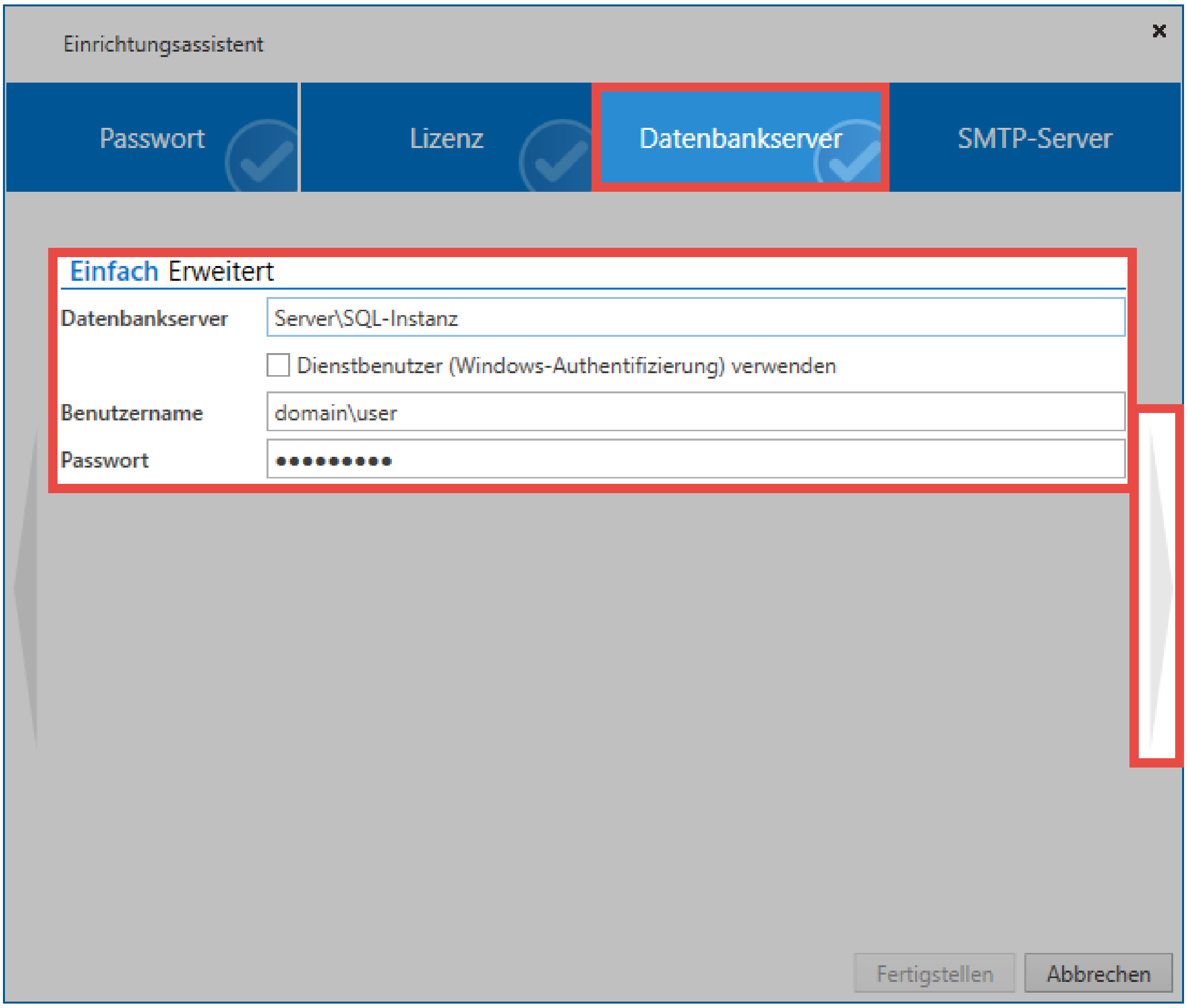
Fon: +49 (0)821 747787-0
Fax: +49 (0)821 747787-11

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Handelsregister Augsburg HRB 22302
Geschäftsführer: Thomas Malchar
USt.-ID: DE252782033

If necessary, access data for a possible proxy can also be issued – otherwise the proxy in the operating system will be used. You can then select and activate the required license by clicking on the corresponding button.

Database server

The configuration of the database server is also part of the “advanced settings”:#erweiterte-einstellungen and can also be edited there later on.



Datenbankserver: Server\SQL-Instanz

□ Dienstbenutzer (Windows-Authentifizierung) verwenden

Benutzername: domain\user

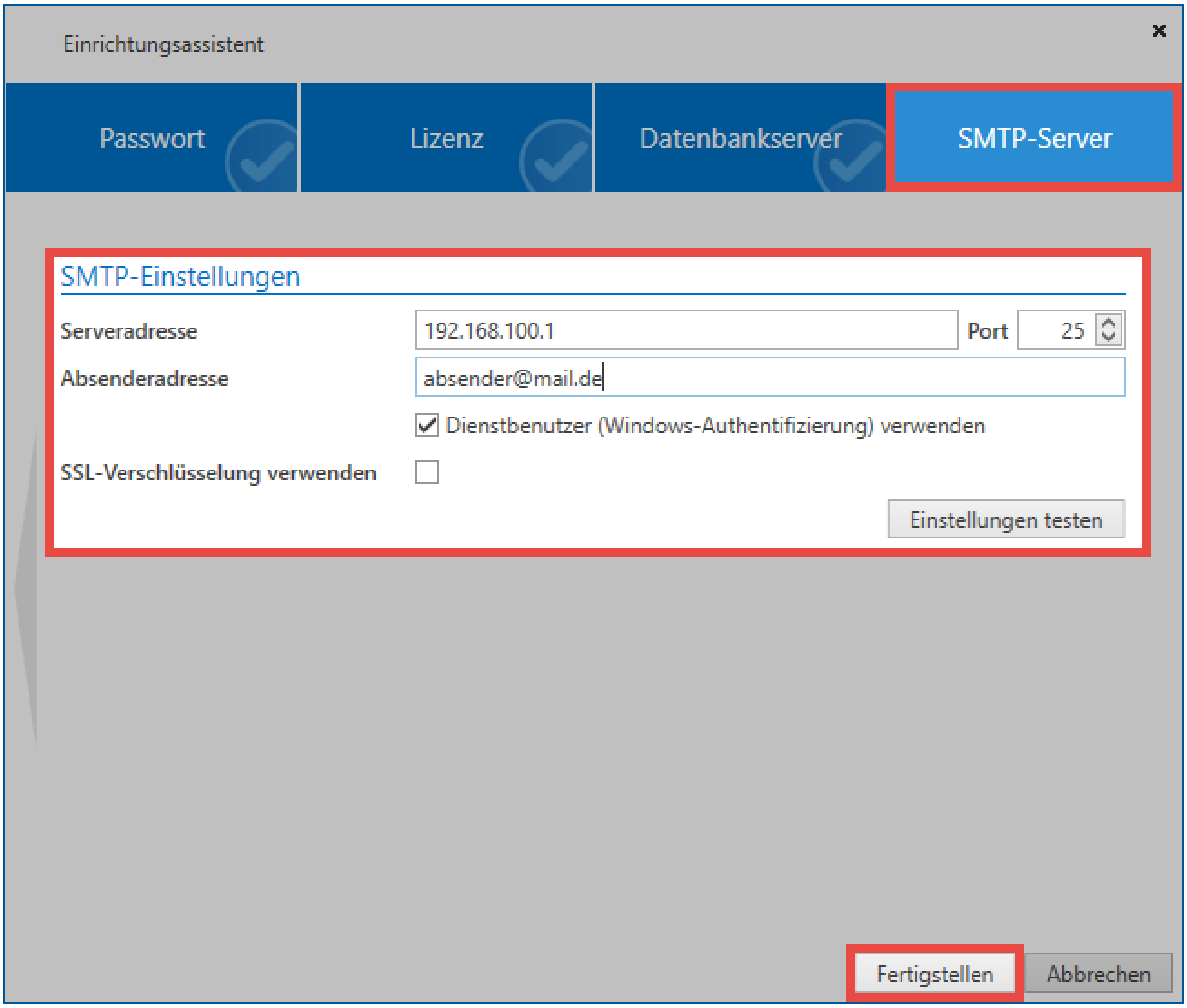
Passwort: ●●●●●●●●●

The database server must be specified along with the associated SQL instance. For simplicity, you can copy the server name from the login window of the SQL server.

The user that will be used to create the database on the SQL Server is also specified. The user therefore needs **dbCreator** rights. Alternatively, you can use the service user for this purpose. The “Advanced” button allows you to specify a **Connection String**.

SMTP server

The last step is to configure the SMTP server via which all emails are sent. This is also part of the “advanced settings”:#erweiterte-einstellungen should it be necessary to make changes later on.



SMTP-Einstellungen

Serveradresse: 192.168.100.1 Port: 25

Absenderadresse: absender@mail.de

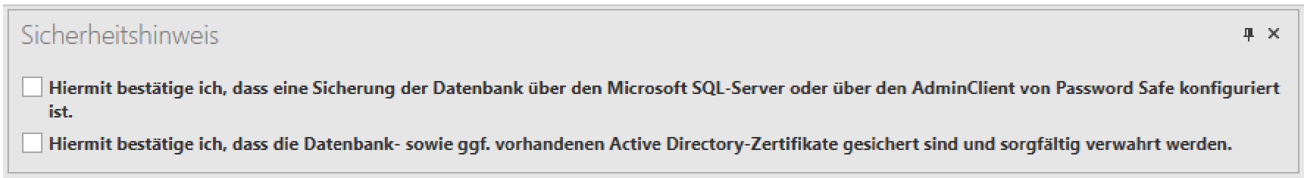
☑ Dienstbenutzer (Windows-Authentifizierung) verwenden

SSL-Verschlüsselung verwenden ☐

Once the data has been entered and successfully tested, the wizard can be completed by clicking on “Finish”.

Security notes

As soon as the setup wizard has been completed, two security notes will be displayed in the **Status** module that need to be confirmed:



Sicherheitshinweis

☐ **Hiermit bestätige ich, dass eine Sicherung der Datenbank über den Microsoft SQL-Server oder über den AdminClient von Password Safe konfiguriert ist.**

☐ **Hiermit bestätige ich, dass die Datenbank- sowie ggf. vorhandenen Active Directory-Zertifikate gesichert sind und sorgfältig verwahrt werden.**

! It is recommended that you only confirm the security notes when the corresponding point has actually been carried out. It is absolutely essential to ensure that regular “backups”:#backupverwaltung are created and the “certificates”:#zertifikate are backed up.

Click here to return to the “Getting started” section

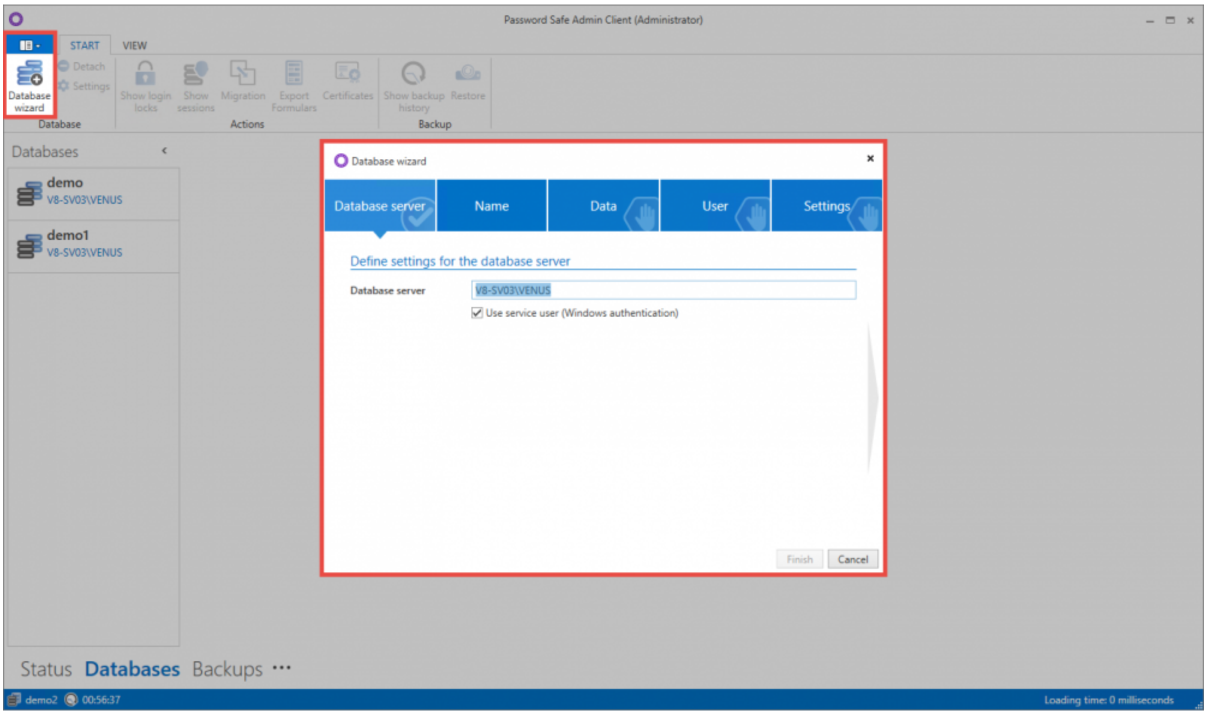
Creating databases

What are databases?

Databases contain all information on users, records, documents, etc. The changes to objects in Password Safe will also become part of the MSSQL database. Naturally, the regular creation of backups to secure this data should always have the highest priority. The **MSSQL** relational database management system is used in Password Safe version 8.

Creating databases

The creation of databases is supported by the database wizard, which is started directly from the ribbon. The individual tabs of the wizard are explained below:



Define settings for the database server

Database server: V8-SV03\VENUS

☑ Use service user (Windows authentication)

Database server

The first tab can be used to manually select the database server. By default, the value defined in the Advanced settings is preset. A user can also be entered or the service user can be selected instead.

Name

Enter the name of the new database here. Alternatively, you may select an existing database. A meaningful name makes it easier to differentiate between databases, especially when using multiple databases.

Data

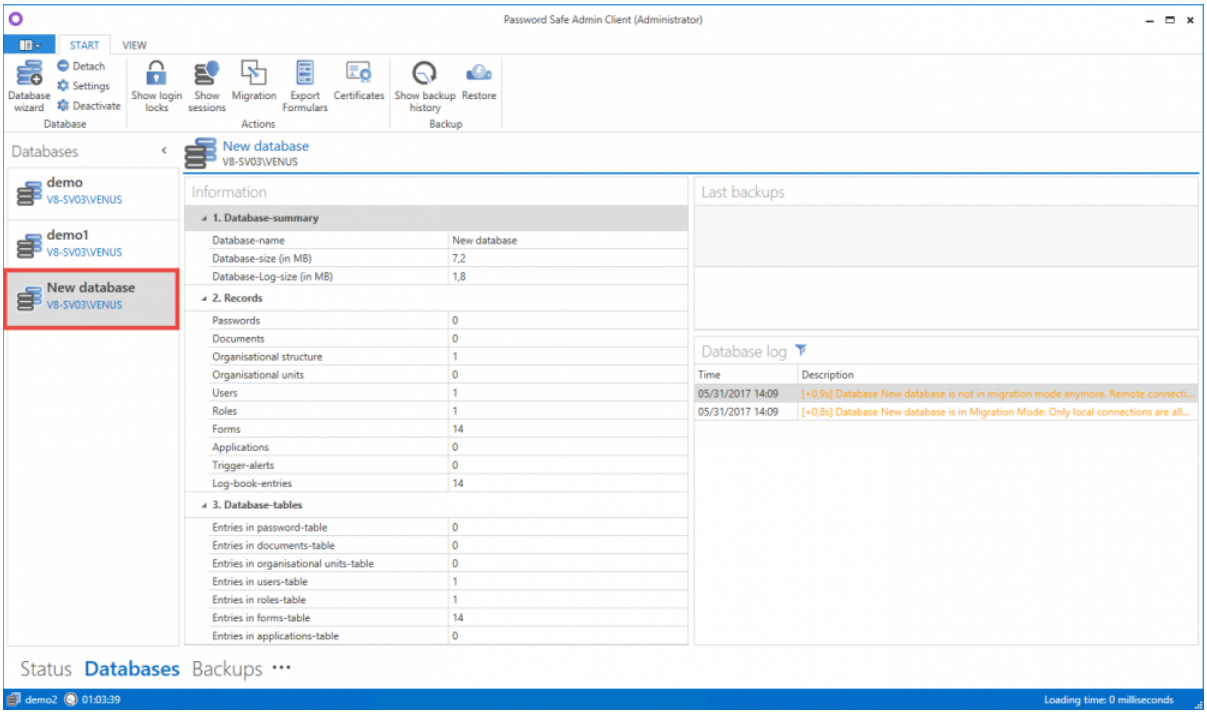
This setting can be used to define whether a template should be used. The template will provide the database with ready-made forms and dashboard settings that make it easier to get started. The user can select from English and German templates. However, it is also possible to proceed without a template – you will then start with a completely empty database. If you have a backup from Password Safe version 7, this can be migrated.

User

This setting is used to define the first user to be created – normally this is the administrator. If a migration is active, the user can be deleted after migration.

Finishing the database wizard

Once a database has been created successfully, “database migration” :#migrationstarts, provided it has been selected. If no data migration has been selected, the new database is created directly, and will be displayed in the database overview.



1. Database-summary	
Database-name	New database
Database-size (in MB)	7,2
Database-Log-size (in MB)	1,8
2. Records	
Passwords	0
Documents	0
Organisational structure	1
Organisational units	0
Users	1
Roles	1
Forms	14
Applications	0
Trigger-alerts	0
Log-book-entries	14
3. Database-tables	
Entries in password-table	0
Entries in documents-table	0
Entries in organisational units-table	0
Entries in users-table	1
Entries in roles-table	1
Entries in forms-table	14
Entries in applications-table	0

Time	Description
05/31/2017 14:09	[+0,9s] Database New database is not in migration mode anymore. Remote connecti...
05/31/2017 14:09	[+0,8s] Database New database is in Migration Mode: Only local connections are all...

Click here to return to the “Getting started” section

Migration

! It is always recommended that the migration to Password Safe version 8 is completed together with a certified partner/the manufacturer. “Please contact us”:https://www.passwordsafe.de/unternehmen/kontakt/ about this matter.

What is a migration?

✻ Migration describes the importing of data from the old Password Safe version 7. This section is thus only relevant for existing customers.

The database format used for version 7 differs fundamentally from the MSSQL database used by version 8. The migration involves the automatic porting of all data from version 7 to version 8. In this regard, the amendments to the authorization concept make it necessary to adapt the data to the new conditions.

! The user carrying out the migration can view all of the folders on the database during the process. The records themselves cannot be viewed by the user. The permissions granted for the records do not change during the migration process.

Fundamental changes to the operating concept

Password Safe version 8 is based on a completely new operating concept. The familiar folder structure from version 7 has been replaced here by organisational units which are supplemented by tags. The records are also no longer sorted by folder but instead categorised. The changes make the system significantly more flexible so that it can be adapted to individual requirements, as well as offering greater efficiency when locating saved information. The **organisational units** can handle the tasks previously performed by the folders. However, these tasks have been expanded. It is now possible, for example, to transfer settings to users via the organisational units.

Advantages

The new operating concept offers numerous advantages compared with version 7. It was previously only possible to assign a record to one single category via the folders – using folder memberships. In version 8, a record can be categorised via its membership of an organisational unit and also using any number of tags. This allows for much greater flexibility in the categorisation of the records. In version 7, it was often the case that numerous folders used precisely the same subfolders. This is where the **tags** now come into play. They can be universally used to categorise the records – which eliminates unnecessary redundancies.

Organisational units in structure view

In order to make the changeover from version 7 easier, the organisational units can also be displayed as a structure. In this case, the organisational units are thus used in a similar way to the previous concept using folders.

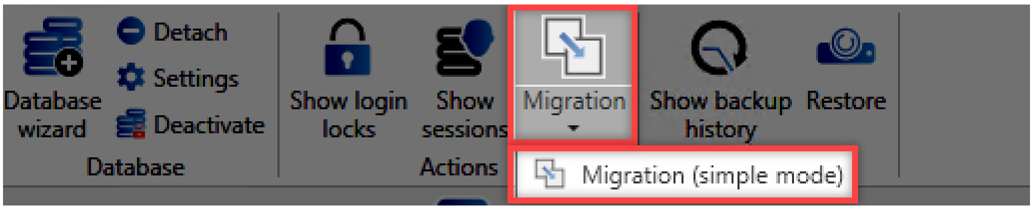
Categorisation during the migration

It is possible to define during the migration how the records previously saved in folders should be handled in the future. A "mapping" process is thus carried out to define the categorisation of these records. As part of the migration, it is possible for each folder to separately define whether it should be mapped as an organisational unit or as a tag. It is also possible to exclude individual folders from the migration. It is also possible to copy over the complete structure from version 7. To simplify the process, there is of course a wizard that is described in more detail in the corresponding section.

✻ The folders **Home, Search folders, All passwords and Favourites** are no longer required in version 8 and therefore do not have to be migrated.

H2(#easymigration). Easy migration – the use of the structure from version 7

If you want to continue to use the structure from version 7 in Password Safe version 8, **easy migration mode** is available for this purpose. It can currently only be started via the ribbon and not via the database wizards.



In easy migration mode, these is no assignment of tags and organisational units. Instead, all folders are migrated as organisational units. The database is also started directly from the client in structure view. You thus receive the familiar structure from version 7.

Parallel operation of versions 7 and 8

From a technical point of view, it is possible to operate versions 7 and 8 in parallel. However, parallel operation is not recommended since it may cause deviations between the records. It may also cause issues with automatic login.

Preparations

Preparations in version 8

Before migration, ensure that both the server and the client for version 8 are installed and can be used. Refer to the Getting started section for more information. In addition, you should specify **before** the migration whether Active Directory users should be imported in Master Key mode or using end-to-end encryption. The connection to Active Directory section will help you to make a decision.

! Master Key mode and the end-to-end encryption differ significantly. The decision about which mode to select will have a profound impact. Therefore, this decision should be taken with care. Further info…

Preparations in version 7

Email addresses

In the v7 database, all local users, as well as all users who are to be migrated in the **end-to-end mode**, must have an email address. Version 8 utilises a new process (PBKDF2) which enables the delivery of new, randomly generated passwords to the email addresses mentioned above.

No e-mails are sent in the test mode. Therefore, no email addresses must be stored. In this case, passwords must be manually assigned to the individual users. These must then be changed at the first login.

Backup, password, and private key

- A **valid backup** of version 7 must exist in .psx format
- The associated **private key** with the ending .prvkey is required for server databases.
- The **database password** is required (for single and multiuser databases)

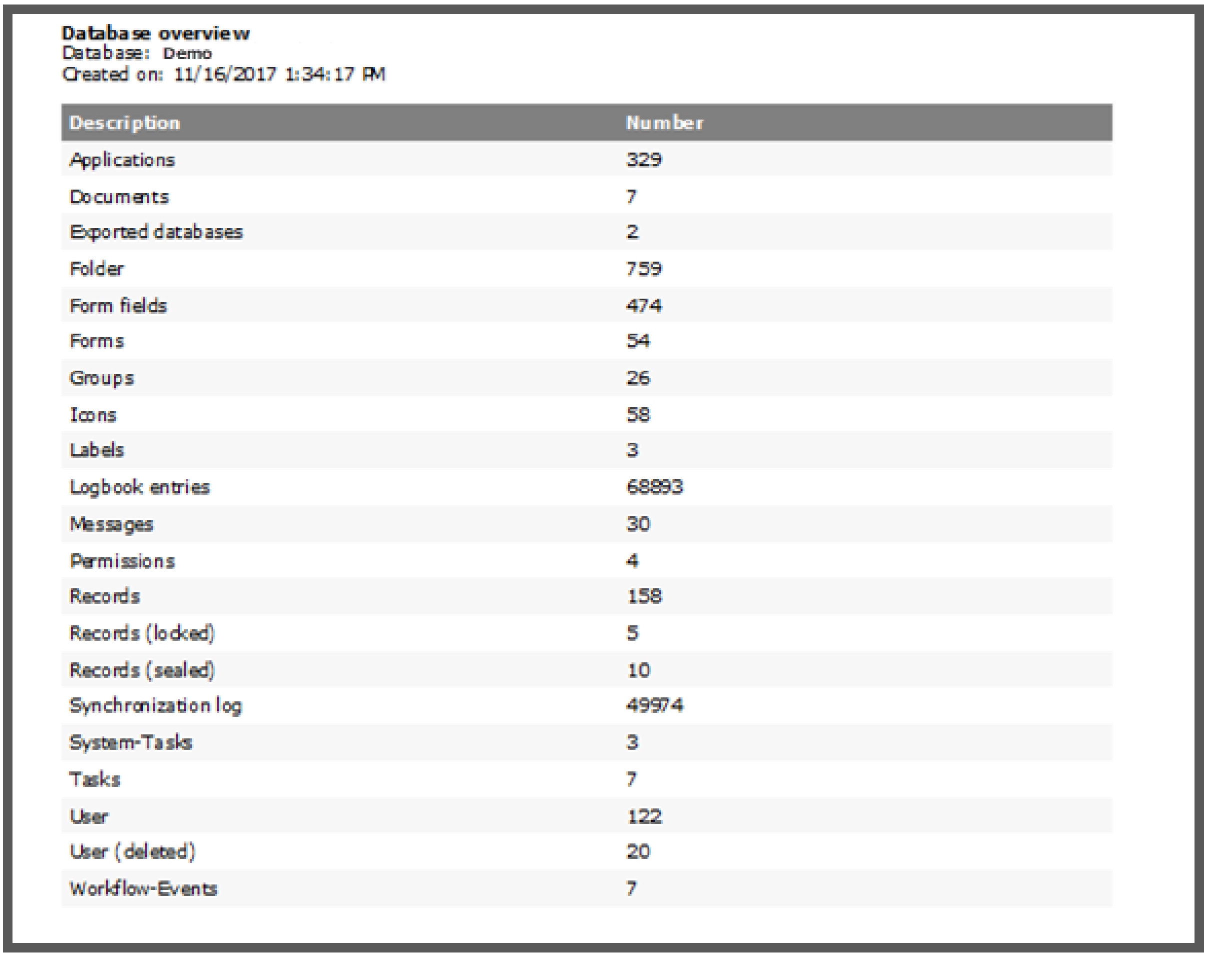
Offline mode and USB sticks

- All offline databases must be synchronized before the migration
- All USB sticks must be synchronized before the migration

The value for “Exported databases” shown in the database overview (see following subsection) is the sum of all offline databases and synchronized USB sticks.

Cleaning up the data set

The migration to version 8 is an opportune time to clean up the data on the existing version 7 database. On the one hand, this shortens the migration process, while on the other, it makes it easier to “get your bearings” in version 8. The database overview can be called up in version 7 via **Edit -> Reports -> Database overview** and is a very important source of information during the clean-up process.



Database overview
Database: Demo
Created on: 11/16/2017 1:34:17 PM

Description	Number
Applications	329
Documents	7
Exported databases	2
Folder	759
Form fields	474
Forms	54
Groups	26
Icons	58
Labels	3
Logbook entries	68893
Messages	30
Permissions	4
Records	158
Records (locked)	5
Records (sealed)	10
Synchronization log	49974
System-Tasks	3
Tasks	7
User	122
User (deleted)	20
Workflow-Events	7

- Records, documents, folders or applications that are no longer required should be deleted. Personal records and documents must be cleaned up by the user themselves.
- It is useful to adjust the folder structures in advance with a view to the migration
- Cleaning up the logbook (**Edit -> Database settings -> Logbook**) also often makes sense. There is an option to export data before deletion. The size of the logbook can be seen in the database overview.
- The size of the synclog is also shown in the database overview. If the value is more than 10,000, it should be deleted. Otherwise, this could massively increase the size of the backup file.

Labels from version 7 become tags in version 8. If necessary, labels can be used to “tag” data sets before migrating to define a specific area.

! Emptying the synclog should always be carried out with the help of technical support. In order to make an appointment, please contact technical support.

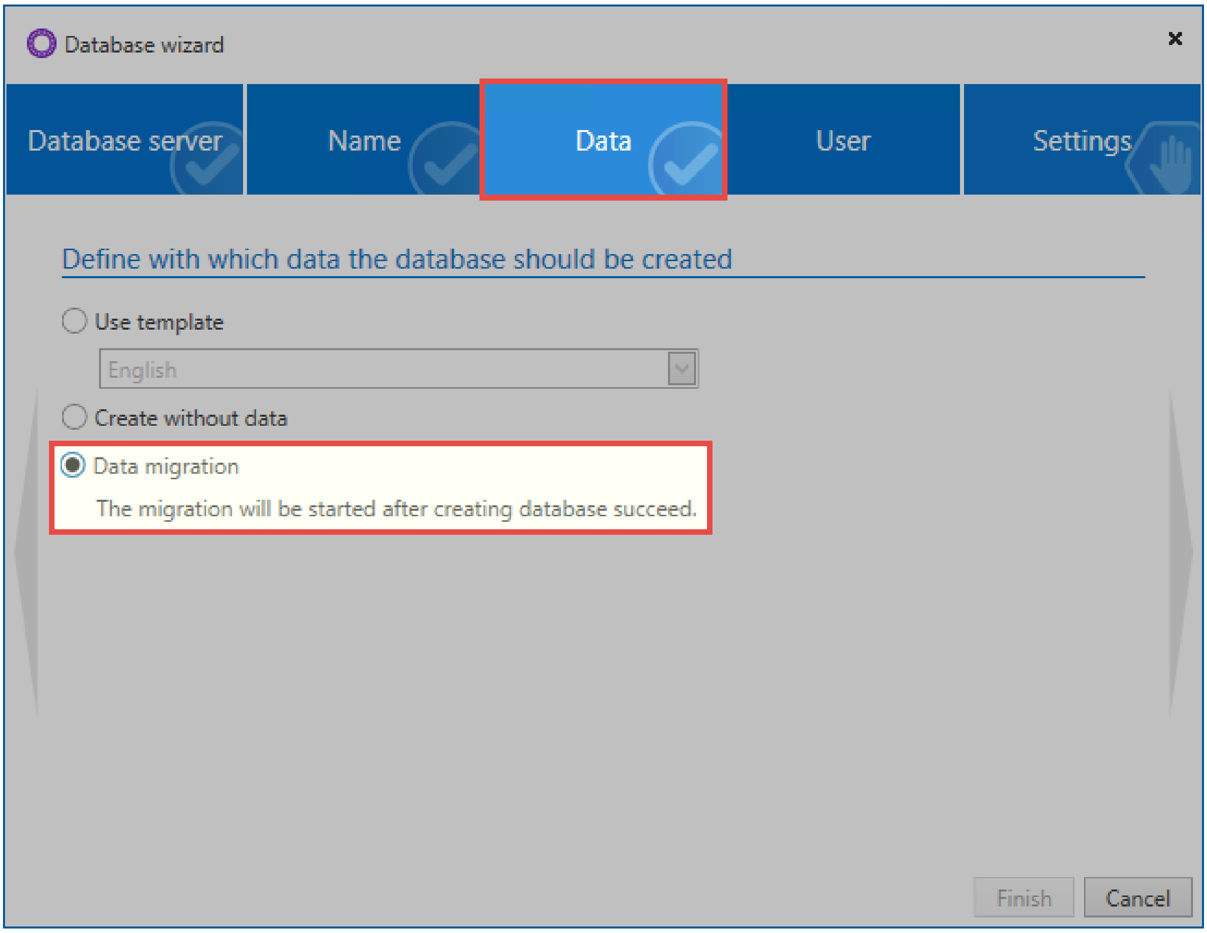
Starting the migration process

What is the migration process?

The migration process describes the actual porting process in which all data from a version 7 database is transferred to a new/existing version 8 database. The required amendments to the data set due to the redesign of the authorization concept are also carried out.

Starting the migration

Firstly, a new database is created as described in the section "Creating and managing databases": #erstellen-und-verwalten-von-datenbanken. The data migration is activated in the third step of the wizard.



Define with which data the database should be created

○ Use template

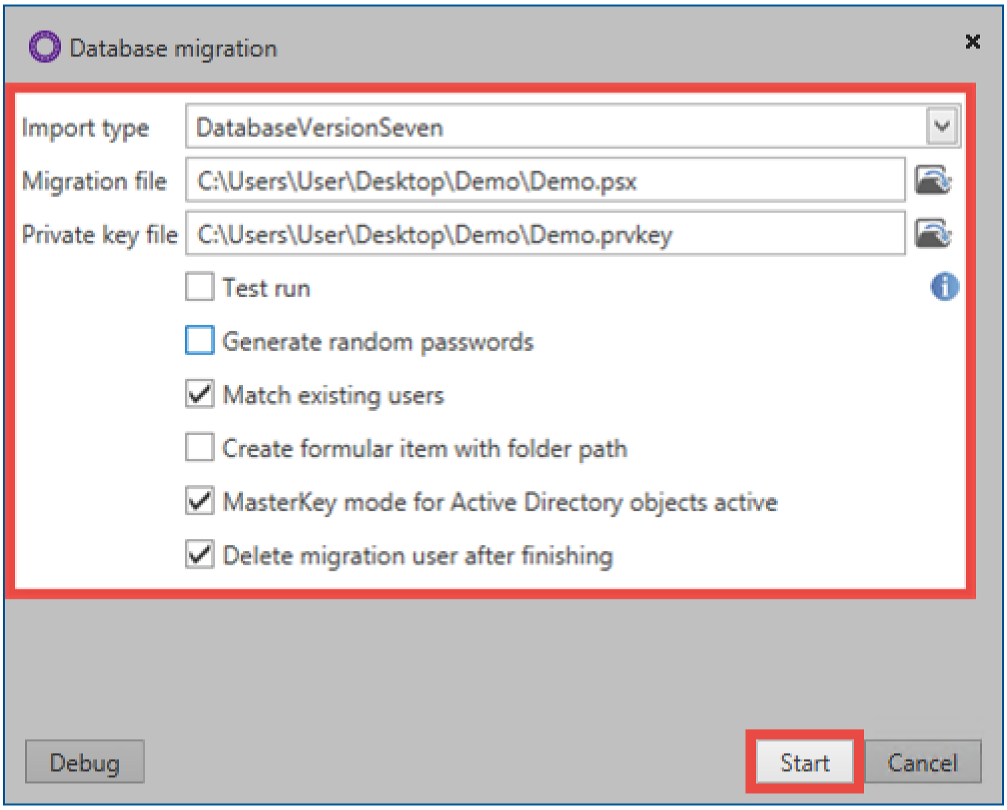
English

○ Create without data

● Data migration

The migration will be started after creating database succeed.

After completing the database wizard, you can go directly to the migration wizard.



Import type: DatabaseVersionSeven

Migration file: C:\Users\User\Desktop\Demo\Demo.psx

Private key file: C:\Users\User\Desktop\Demo\Demo.prvkey

☐ Test run

☐ Generate random passwords

☑ Match existing users

☐ Create formular item with folder path

☑ MasterKey mode for Active Directory objects active

☑ Delete migration user after finishing

- Select the desired **Import type**

Only an import from Password Safe v7 is currently supported. If you wish to migrate from older database versions, an intermediate step via version 7 must be carried out first.

- Under **Migration file**, select the previously created Password Safe V7 backup which is in .psx format
- In addition, when migrating a server database, the **private key file** in .prvkey format that belongs to the backup must be selected. Users are requested to **Enter the password** for single and multiuser databases.
- The complete migration is carried out as a test via the **test run**. Users do not receive passwords in this case and thus cannot log in. This step is only for test purposes.
- For local users or users in deactivated Masterkey mode, **randomly generated passwords** can be created. These are sent to users via email. If the passwords are not automatically generated, they need to be manually issued in the database.
- **Merging existing users**: If an existing database is migrated, any duplicate users are merged using the name. The rights will be added together. * If this option is inactive, a “*” is added to the name of the newly imported user. In the next run “**”, etc.
- **Create form field with folder path**: A form field is created that replaces the folder path from Password Safe version 7. This field contains every record and allows you to search based on the old folder path in future.

- **Master Key mode for Active Directory objects**: It is decided here whether the AD user is imported in Master Key mode or using end-to-end encryption. Note that a corresponding certificate is created in Master Key mode.
- If documents had their own folder structure in version 7, the **document folder can be added as an organisational unit**.
- The **migration user can be deleted** if required. In general, this user is no longer required after the migration because the administrator from the migrated backup is adopted as the user and used in the future.

! Before importing, you should carefully consider whether to import in Master Key mode or using end-to-end encryption. This setting cannot be changed afterwards. You can find further information on this in the section Active Directory link.

It should be noted that all local users as well as all those who will be migrated via end-to-end encryption will receive an email containing a randomly generated password. Users who are migrated in Master Key mode can continue to log in with the domain password.

After the process has been started, the data are analysed and processed. Depending on the database size, this step can take several hours.

If an error occurs, the wizard will generate a log file entry. This can be found under the path **C:\Users\User\AppData\Roaming\MATESO\Migration**.

Migration into an existing database

The data can also be migrated into an existing database via the ribbon. The migration process remains the same. This function allows multiple databases to be merged. Identical records, documents, forms, etc. are duplicated. **Exception**: Duplicated users will have a * added to the end of the name. They can, however, be merged together. Tags are not duplicated if they are written identically.

As soon as the migration starts, the database is in migration mode. As long as it is active, no logbook entries can be created. If users are connected to the database, they cannot use the database while the migration mode is active.

Assigning tags and OUs

✻ If **easy migration mode** is selected, there is no assignment process. Instead, all folders are classified as organisational units to create the structure from version 7.

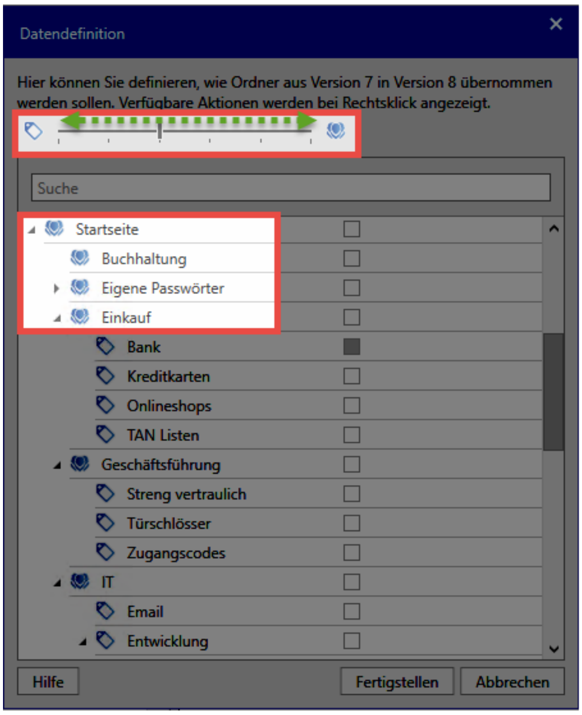
Why are tags and OUs assigned?

Following the previous step, the folder structure of version 7 is displayed. Due to the already mentioned amendments to the operating concept in version 8, it is now possible to define how the data will be categorised in future. This involves defining whether folders from version 7 are converted into an organisational unit or a tag in version 8. The icons shown in the overview have the following meanings:

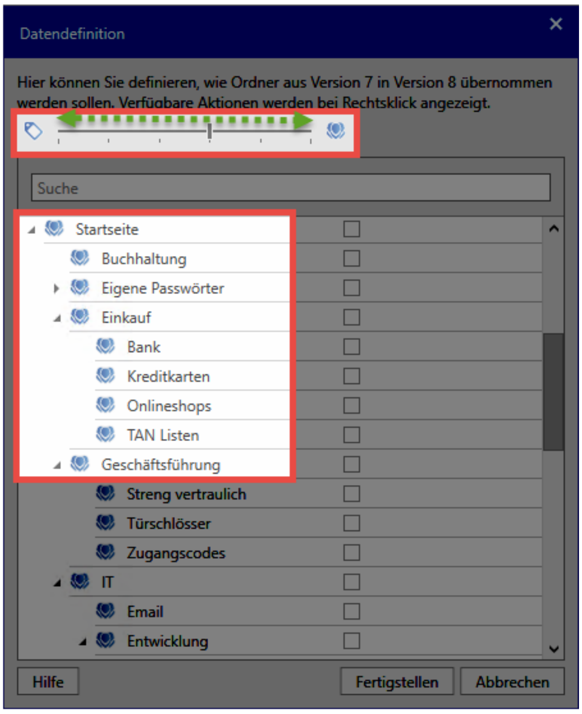
Migrate the folder as an organisational unit
Migrate the folder as a tag
✗ No category is created for the marked folder

The slider is used to define how far up the hierarchy folders will be converted into organisational units during the migration – all underlying folders will be converted into tags. Thus a certain pre-selection can be made, which can then be manually refined. Repeated clicking will switch between tag, organisational unit and unallocated folder.

✻ If the slider is moved fully to the right, all folders will be migrated as organisational units. The complete structure from version 7 will thus be copied over.



Hier können Sie definieren, wie Ordner aus Version 7 in Version 8 übernommen werden sollen. Verfügbare Aktionen werden bei Rechtsklick angezeigt.

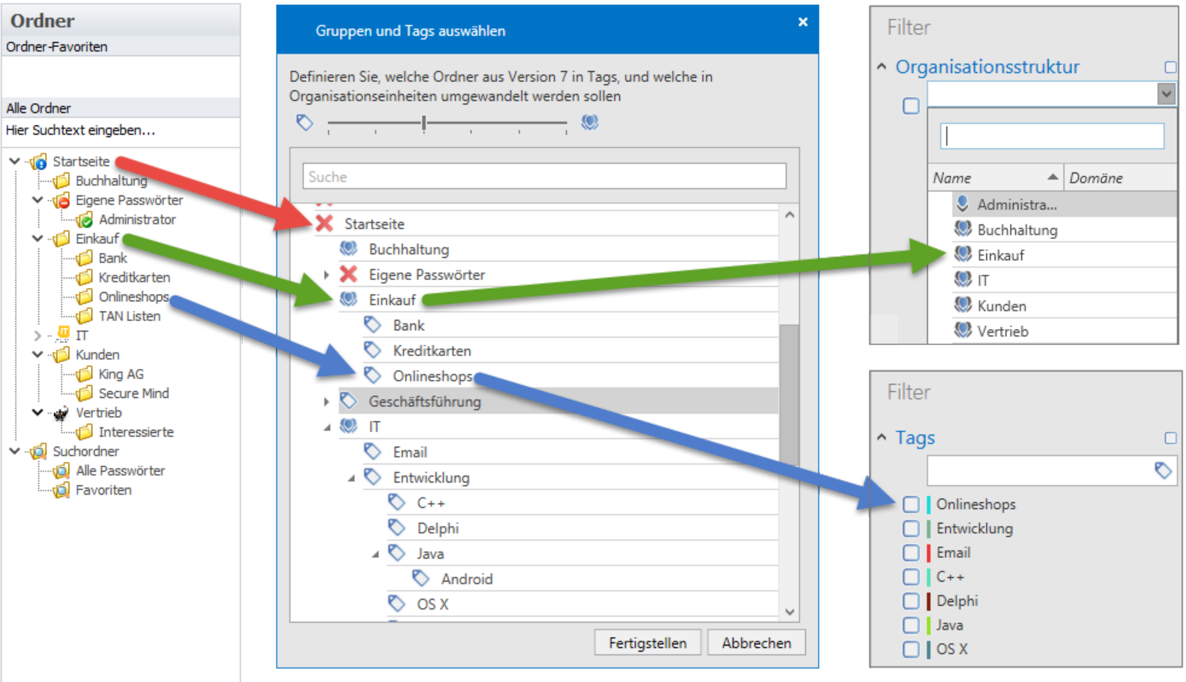


Hier können Sie definieren, wie Ordner aus Version 7 in Version 8 übernommen werden sollen. Verfügbare Aktionen werden bei Rechtsklick angezeigt.

Further options can be opened via the context menu (right mouse button):

- Categorise all sub-objects as organisational units
- Categorise all sub-objects as tags
- Ignore all sub-objects
- Delete all previous markings

In the following **diagram**, a possible process for assigning the folders to organisational units and tags is illustrated:



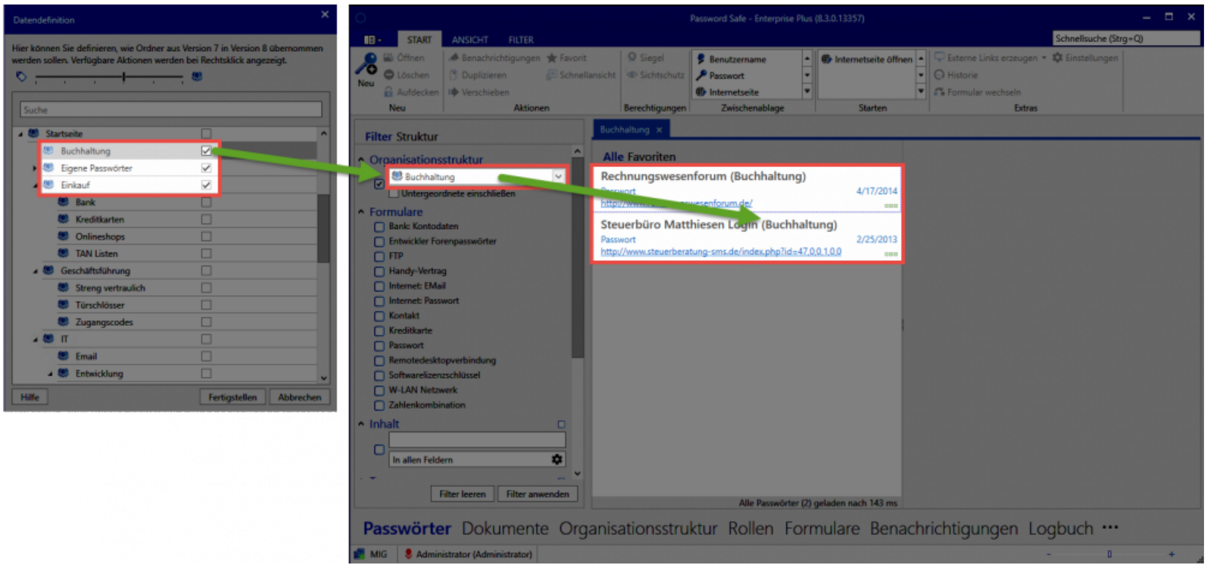
Gruppen und Tags auswählen

Definieren Sie, welche Ordner aus Version 7 in Tags, und welche in Organisationseinheiten umgewandelt werden sollen

Home and the search folders do not need to be imported. Importing personal folders is also not recommended. In this case, the records are assigned to the organisational unit of the respective users. The migration process also provides you with the opportunity to clean up all folders with no content.

! The user carrying out the migration can view all of the folders on the database during the process. The records themselves cannot be viewed by the user.

It is also possible to include the folder names in the record description. For this purpose, a corresponding button is provided for every folder.



Datendefinition

Hier können Sie definieren, wie Ordner aus Version 7 in Version 8 übernommen werden sollen. Verfügbare Aktionen werden bei Rechtsklick angezeigt.

This option can be activated for all folders via the context menu.

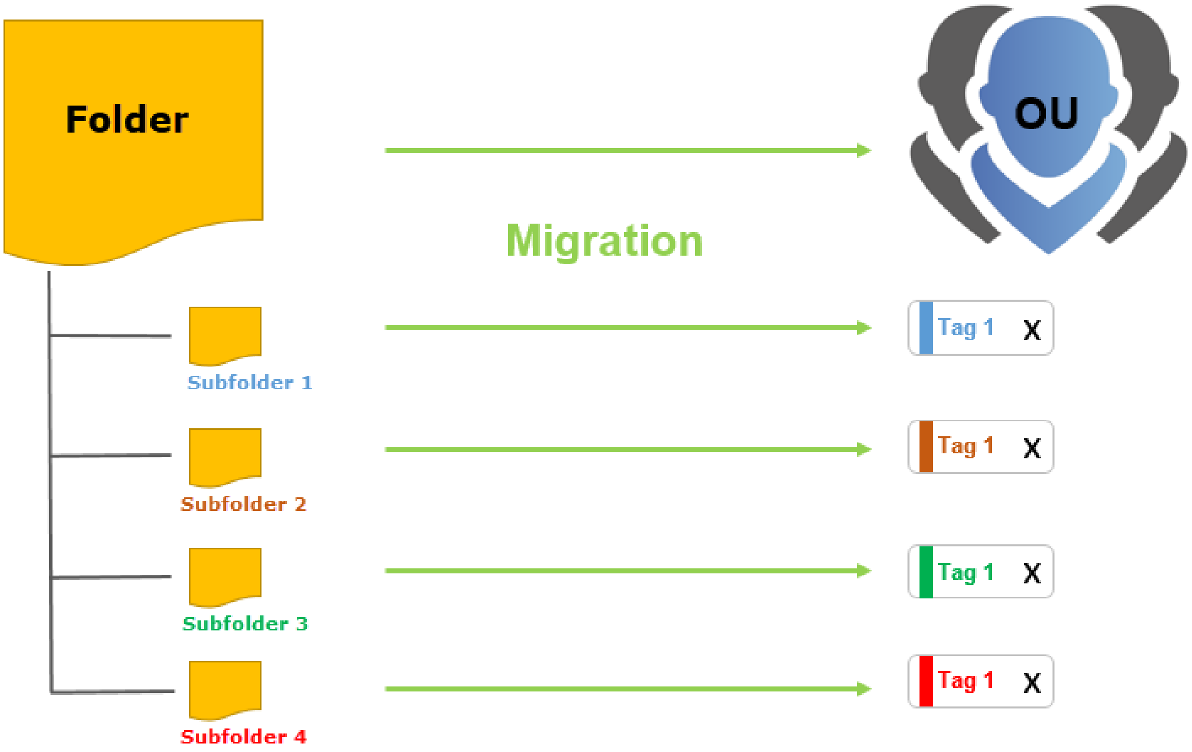
Finishing the migration

Press the **Finish** button to transfer the data to the database. **The migration can take several hours depending on its scope**. If Master Key mode has not been selected, the imported users will receive randomly generated passwords via email and can directly log in. At the first login, these passwords must be changed. If configured, the user who carried out the migration is immediately deleted.

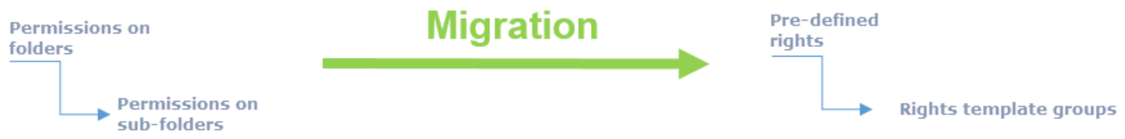
Permissions after migration

What happens to the permissions from the original folders?

Folder structures are responsible for, amongst other things, structured data management in version 7. As described in the previous section, the mapping process to OUs and tags is directly carried out during the migration process. Depending on the configuration, folders are converted into OUs and subfolders into tags:



Naturally, the folders in version 7 also act as the basis for the permissions. If a record was created in a folder, the record is granted with permissions in the same way as the permissions for the associated folder. As long as only a few folders from version 7 are “mapped” into organisational units as part of the migration in version 8, this process does not change. A rights preset is automatically defined for the organisational unit (**predefined rights**) that is used to automatically grant the intended rights to records created in future. The subfolders had their own permissions. Due to the assignment of tags from subfolders, a new mechanism needs to be used because tags do not posses any rights. To enable a uniform system to be created, the rights template groups associated with the predefined rights can be helpful here.



Permissions on folders
Permissions on sub-folders
Migration
Pre-defined rights
Rights template groups

Checklist after migration

Database overview v7 and v8

In order to compare the state of the database before and after the migration, the database overview in version 7 already mentioned as part of the preparations for the migration and its equivalent in version 8 can be very helpful. As there are a number of differences in version 8, not all of the values will match. All of the cleanups to the database are also relevant (see the preparation section). The following section describes the individual values in both database overviews.

Records

- The total number of all records must be the same in versions 7 and 8
- This includes personal records. The overview always shows the number of all passwords in both versions.

In version 7, all of the passwords for which a user has permissions can be viewed under “All passwords”. In version 8, this can not always be checked because version 8 can issue a maximum of 1000 passwords. If a user has permissions for more than 1000 records, you will need to adjust the filter correspondingly.

Seals

Seals are migrated differently, depending on their form in version 7. For security reasons, the number of sealed records should also be compared.

- **Seals with release mechanisms** are migrated in such a way that users / groups with the permissions to issue a release in version 7 are also granted the permissions to issue releases in version 8
- **Seals without release mechanisms** are not migrated as seals. In version 7, applying a seal without a release mechanism was used to send a notification when a user viewed the password. A corresponding notification is configured in version 8 when this type of seal mechanism is imported. Although the mechanism is retained, it is no longer displayed as a seal.
- In version 8, users from **Light seals** are stored in the seal but are not authorised to issue a release. The record will also not be sealed for this user group. They are thus not affected by the existing seal and can open the record without having to break the seal.
- The **reasons for breaking a seal** from version 7 are adopted.
- However, those users who had the required permissions to edit the seal in version 7 are handled differently. These users are ignored by the migration because all users with the required permissions to release the seal are permitted to edit it in version 8 – they are thus **linked to the authorization system** from now on (see section on seals).

- The seal history has become obsolete without replacement

Releases

- In the releases area, there may be deviations after a completed migration because the releases configured via the workflow system are removed. (The workflow system no longer exists in version 8)

Locking

- Locked records are protected in version 8 with password masking
- The users who were allowed to edit the lock in version 7 are not locked in version 8.

RDP connections

- Records based on the **Remote desktop connection** form are split during the migration. Records are created with the login data. The connection data are stored in the corresponding RDP applications. These are then linked directly to the records. You can find further information on this in the Applications section.

Applications

- Applications from version 7 are converted as far as possible. However, it is possible that individual applications have to be re-learned again. However, all web pages should be able to be filled automatically without major problems. After the migration, all users have the right role to read all applications. If this is not desired, the rights must be correspondingly adapted.

> In Password Safe version 8, you can usually enter login data for websites automatically without the application – web applications are therefore only necessary in exceptional cases. Therefore, it is a good idea to delete any imported web applications. The filter allows you to quickly select them.

User

Users from version 7 are copied one-to-one. The login for migrated users will differ depending on the type of user and the mode in which it was migrated.

- **Local users** will receive a new, randomly generated password by e-mail. This password is used for the initial login.
- **AD users in end-to-end mode** get a new password for initial login by e-mail. This is carried out with just the user name **without** the domain entered in front of it.
- **AD users in Master Key mode** can log in directly with their domain password. Here, too, the login is completed without the domain added in front.

Groups

- All groups from version 7 become roles in version 8.
- In version 8, there are **no longer any** groups in group nesting – there are only roles in a flat hierarchy. This can result in more roles than there were in version 7.

Roles

During migration, some roles are created by default to map the version 7 permissions in version 8. This affects the visibility of

- Applications
- User
- Forms
- Roles

> ✻ The administrator becomes a member of these roles during the migration. Following the migration, these should be checked and adapted where necessary.

Custom icons

- Your own icons will not be imported because they are no longer available in version 8

Labels

- Labels from version 7 become tags in version 8.
- The colour is maintained
- If necessary, labels can be used to “tag” data sets before migration to define a specific area

Tasks and messages

- Tasks and messages from version 7 are not migrated

Folders

- Since there are no folders in version 8, they are imported as organisational units or tags in the migration wizard. Since users in version 7 have personal folders (for example for messages and tasks), the number can vary greatly.

Workflow Events

- Password Safe version 8 does not currently have any workflow system. Configured events are thus not imported.
- Notifications configured in the workflow system can now be created using the module of the same name.

System tasks

- System tasks in version 8 differ significantly from those in version 7. A migration is not possible.

Logbook entries

- All logbook entries for the topics password, group, document, application, label, user, folder, seal templates, seal and form are imported and displayed.

Forms

- Only forms that have a password assigned to them are imported. The number may therefore differ.

Documents

- All documents from version 7 are migrated
- The folder in which the document was located is converted into a tag
- Any parent folders are ignored
- The rights to documents are copied
- You can link to records in the footer of the reading pane of the record

External links

- External links are not migrated.

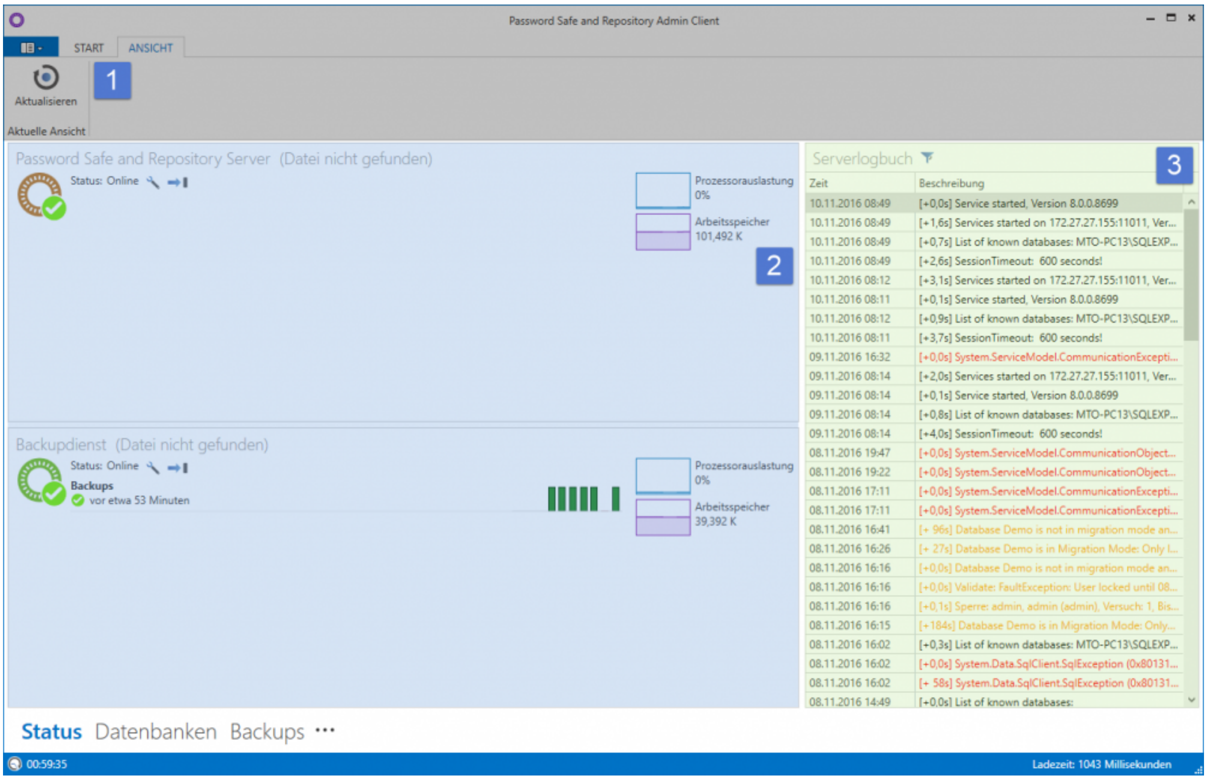
Operation and setup

Structure of the AdminClient

The structure of the AdminClient is based to a high degree on the structure of the actual client. The control elements such as the ribbon and the info and detail areas can be derived from the section dealing with the client.

An initial password is required for the first login on server. The password is “admin”. This password should be changed directly after login and carefully documented.

Status module



Password Safe and Repository Server (Datei nicht gefunden)

Status: Online

Prozessorauslastung 0%

Arbeitsspeicher 101,492 K

Backupdienst (Datei nicht gefunden)

Status: Online

Backups

vor etwa 53 Minuten

Prozessorauslastung 0%

Arbeitsspeicher 39,392 K

Serverlogbuch

Zeit	Beschreibung
10.11.2016 08:49	[+0,0s] Service started, Version 8.0.0.8699
10.11.2016 08:49	[+1,6s] Services started on 172.27.27.155:11011, Ver...
10.11.2016 08:49	[+0,7s] List of known databases: MTO-PC13\SQLEXP...
10.11.2016 08:49	[+2,6s] SessionTimeout: 600 seconds!
10.11.2016 08:12	[+3,1s] Services started on 172.27.27.155:11011, Ver...
10.11.2016 08:11	[+0,1s] Service started, Version 8.0.0.8699
10.11.2016 08:12	[+0,9s] List of known databases: MTO-PC13\SQLEXP...
10.11.2016 08:11	[+3,7s] SessionTimeout: 600 seconds!
09.11.2016 16:32	[+0,0s] System.ServiceModel.CommunicationExcepti...
09.11.2016 08:14	[+2,0s] Services started on 172.27.27.155:11011, Ver...
09.11.2016 08:14	[+0,1s] Service started, Version 8.0.0.8699
09.11.2016 08:14	[+0,8s] List of known databases: MTO-PC13\SQLEXP...
09.11.2016 08:14	[+4,0s] SessionTimeout: 600 seconds!
08.11.2016 19:47	[+0,0s] System.ServiceModel.CommunicationObject...
08.11.2016 19:22	[+0,0s] System.ServiceModel.CommunicationObject...
08.11.2016 17:11	[+0,0s] System.ServiceModel.CommunicationExcepti...
08.11.2016 17:11	[+0,0s] System.ServiceModel.CommunicationExcepti...
08.11.2016 16:41	[+ 96s] Database Demo is not in migration mode an...
08.11.2016 16:26	[+ 27s] Database Demo is in Migration Mode: Only l...
08.11.2016 16:16	[+0,0s] Database Demo is not in migration mode an...
08.11.2016 16:16	[+0,0s] Validate: FaultException: User locked until 08...
08.11.2016 16:16	[+0,1s] Sperre: admin, admin (admin), Versuch: 1, Bis...
08.11.2016 16:15	[+184s] Database Demo is in Migration Mode: Only...
08.11.2016 16:02	[+0,3s] List of known databases: MTO-PC13\SQLEXP...
08.11.2016 16:02	[+0,0s] System.Data.SqlClient.SqlException (0x80131...
08.11.2016 16:02	[+ 58s] System.Data.SqlClient.SqlException (0x80131...
08.11.2016 14:49	[+0,0s] List of known databases:

00:59:35

Ladezeit: 1043 Millisekunden

1. Ribbon

As usual the ribbon can be found above. Because the module is purely informative, there is no functionality in the ribbon, except for updating the view

2. Notification area

- The info area shows the status of the specific services. Click the 🔧 icon to configure services. By default, the base configuration is used. If necessary, individual parameters can be replaced or adapted to personal requirements.
- You can start and stop a specific service via ➡ ▮
- On the right side of the info area, the utilization of the processor and main memory is displayed over two curves.
- In the “Backup service” area, the last backups are displayed using a diagram. There is a green bar for a successful backup, a red symbolizes a failed backup. Additional information is displayed via a mouseover.

3. Server log

The server logbook shown on the right of the screen monitors and controls the server. It shows all relevant actions on the server in a comprehensible way, always displaying the last 100 entries. The entries are marked as follows:

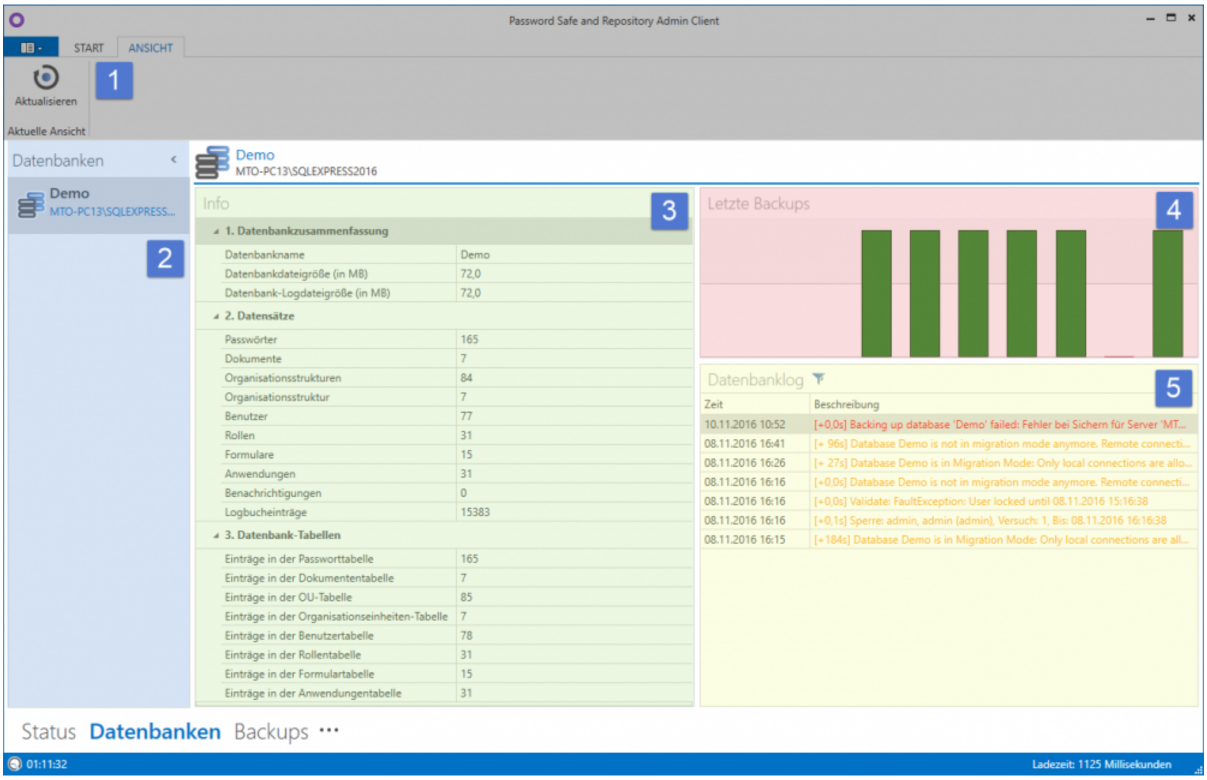
Expected actions	black
Events that require attention	orange
Problems and crashes	red

- Expected actions – such as starting and stopping services – are displayed in black
- All events (e.g. failed login attempts) that require attention are displayed in orange
- All problems (e.g. crashes) are marked in red

The server logbook can be sorted in ascending and descending order by date and description via the column headings. The period shown can be limited using ▼.

Databases module

Databases are managed in a dedicated module. All relevant information on the existing databases can also be called up – completely without accessing the SQL server.



1. Datenbankzusammenfassung	
Datenbankname	Demo
Datenbankdateigröße (in MB)	72,0
Datenbank-Logdateigröße (in MB)	72,0
2. Datensätze	
Passwörter	165
Dokumente	7
Organisationsstrukturen	84
Organisationsstruktur	7
Benutzer	77
Rollen	31
Formulare	15
Anwendungen	31
Benachrichtigungen	0
Logbucheinträge	15383
3. Datenbank-Tabellen	
Einträge in der Passworttabelle	165
Einträge in der Dokumententabelle	7
Einträge in der OU-Tabelle	85
Einträge in der Organisationseinheiten-Tabelle	7
Einträge in der Benutzertabelle	78
Einträge in der Rollentabelle	31
Einträge in der Formulartabelle	15
Einträge in der Anwendungentabelle	31

Zeit	Beschreibung
10.11.2016 10:52	[+0,0s] Backing up database 'Demo' failed: Fehler bei Sichern für Server 'MT...
08.11.2016 16:41	[+ 96s] Database Demo is not in migration mode anymore. Remote connecti...
08.11.2016 16:26	[+ 27s] Database Demo is in Migration Mode: Only local connections are allo...
08.11.2016 16:16	[+0,0s] Database Demo is not in migration mode anymore. Remote connecti...
08.11.2016 16:16	[+0,0s] Validate: FaultException: User locked until 08.11.2016 15:16:38
08.11.2016 16:16	[+0,1s] Sperre: admin, admin (admin), Versuch: 1, Bis: 08.11.2016 16:16:38
08.11.2016 16:15	[+184s] Database Demo is in Migration Mode: Only local connections are all...

1. Ribbon

2. Database overview

In the database overview, all databases listed alphabetically. This section can be minimised using the arrow symbol on the top, left edge. Right-click on one of the databases to display a context menu with all available functions.

3. Notification area

The Info area displays all the information about the database currently selected in the database overview. This information is divided into the three subsections “Database summary, Data sets and Database tables”.

4. Recent backups

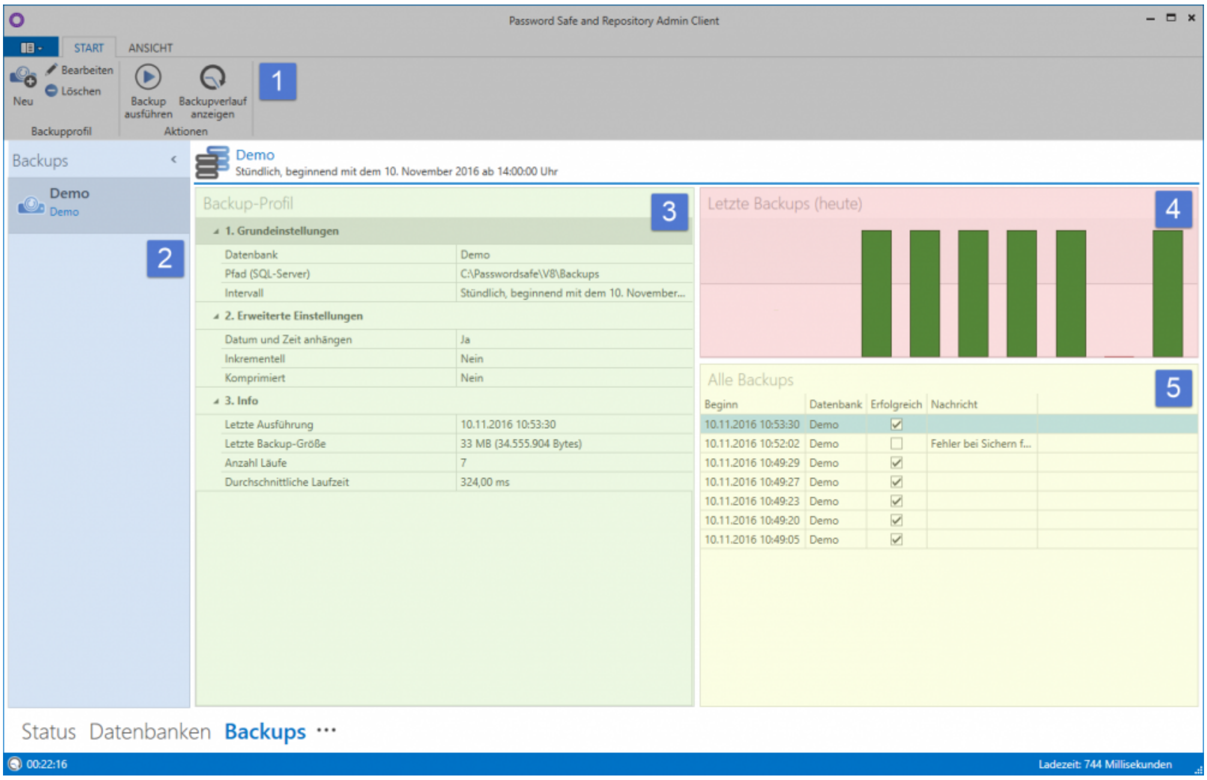
List of recent backups. Can be sorted by date

5. Database log

The database log is used to monitor and control the specific databases. All relevant actions for the selected database are displayed in a comprehensible manner in one list. The categorisation is carried out in the same way as the server log according to the colours applied.

Backups module

There is also a separate module for configuring the backups. This means that all backups can be configured and managed directly from the AdminClient.



Demo
Stündlich, beginnend mit dem 10. November 2016 ab 14:00:00 Uhr

Backup-Profil

1. Grundeinstellungen	
Datenbank	Demo
Pfad (SQL-Server)	C:\Passwordsafe\V8\Backups
Intervall	Stündlich, beginnend mit dem 10. November...
2. Erweiterte Einstellungen	
Datum und Zeit anhängen	Ja
Inkrementell	Nein
Komprimiert	Nein
3. Info	
Letzte Ausführung	10.11.2016 10:53:30
Letzte Backup-Größe	33 MB (34.555.904 Bytes)
Anzahl Läufe	7
Durchschnittliche Laufzeit	324,00 ms

Alle Backups

Beginn	Datenbank	Erfolgreich	Nachricht
10.11.2016 10:53:30	Demo	☑	
10.11.2016 10:52:02	Demo	☐	Fehler bei Sichern f...
10.11.2016 10:49:29	Demo	☑	
10.11.2016 10:49:27	Demo	☑	
10.11.2016 10:49:23	Demo	☑	
10.11.2016 10:49:20	Demo	☑	
10.11.2016 10:49:05	Demo	☑	

1. Ribbon

2. Backup overview

All configured backups are listed here. The overview can be minimized to the left. Other functions are available via right-click

3. Notification area

The notification area is divided into three sections. The “Basic settings, Advanced settings and Info” sections for the selected database can be used

4. Recent backups

The last backups are displayed in a list on the right.

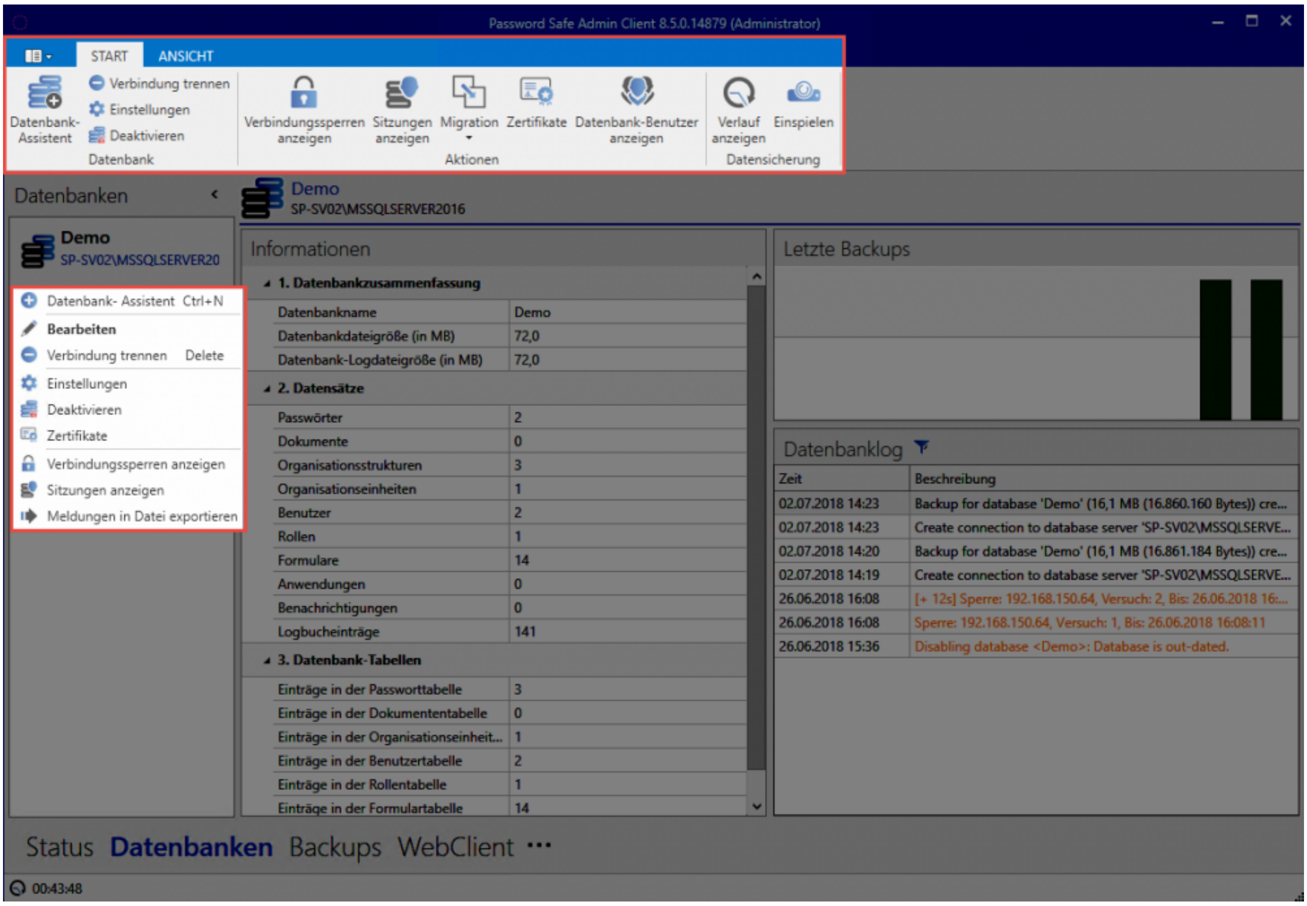
5. All backups

A tabular overview shows all previous backups. The view can be sorted as usual. Here you can see at a glance, when which database was saved and whether the backup was successful.

Managing databases

Managing a database

The available actions can be selected via the context menu that is accessed using the right mouse button or also via the ribbon.



1. Datenbankzusammenfassung	
Datenbankname	Demo
Datenbankdateigröße (in MB)	72,0
Datenbank-Logdateigröße (in MB)	72,0
2. Datensätze	
Passwörter	2
Dokumente	0
Organisationsstrukturen	3
Organisationseinheiten	1
Benutzer	2
Rollen	1
Formulare	14
Anwendungen	0
Benachrichtigungen	0
Logbucheinträge	141
3. Datenbank-Tabellen	
Einträge in der Passworttabelle	3
Einträge in der Dokumententabelle	0
Einträge in der Organisationseinheit...	1
Einträge in der Benutzertabelle	2
Einträge in der Rollentabelle	1
Einträge in der Formulartabelle	14

Datenbanklog

Zeit	Beschreibung
02.07.2018 14:23	Backup for database 'Demo' (16,1 MB (16.860.160 Bytes)) cre...
02.07.2018 14:23	Create connection to database server 'SP-SV02\MSSQLSERVE...
02.07.2018 14:20	Backup for database 'Demo' (16,1 MB (16.861.184 Bytes)) cre...
02.07.2018 14:19	Create connection to database server 'SP-SV02\MSSQLSERVE...
26.06.2018 16:08	[+ 12s] Sperre: 192.168.150.64, Versuch: 2, Bis: 26.06.2018 16:...
26.06.2018 16:08	Sperre: 192.168.150.64, Versuch: 1, Bis: 26.06.2018 16:08:11
26.06.2018 15:36	Disabling database <Demo>: Database is out-dated.

Database settings

All database settings are saved in the database. It is necessary to log in to the database before editing the settings. Any user that exists in the database can be used for this purpose. You can always restore Global settings via the ribbon.

Multifactor authentication

This area can be used to configure which services will be used for multi-factor authentication. The available services are: **RSA Secure ID**, **SafeNet**, **YubiKey NEO**, and **YubiKey Nano**. After selecting the required service, specify the respective access data. You must also configure various services. In this case, you can specify on the client which methods will be used by the individual users.

Further information on this subject can be found in the section **Multifactor authentication**.

PKCS#11

Via the PKCS # 11 interface, the server keys can be protected via a hardware security module (HSM). The interface can be configured here.

Automatic clean up

If desired, the **logbook**, **notifications**, **session recordings** and also the **historical documents** can be automatically cleaned up here. You merely have to enter how old the data needs to be before it is deleted. Logbook entries can be exported before the deletion process.

> ! It is important to note that the logbook is also used for the filter functions. If the logbook is regularly cleaned up, it is possible that the full functions of the filter will no longer be available.

Database actions

Show connection locks

In the ribbon, all connection locks can be displayed. To do this, you must first log in to the database. All locked users will be displayed in a list. The following is displayed:

- User name (if known)
- Reason for lock
- Number of login attempts
- Expiry of the lock. The user can be unlocked by right-clicking on an entry.

A user can be locked manually using the corresponding button. It is necessary to select the user, configure the expiration of the lock and specify a reason.

Show / disconnect sessions

You can use the corresponding button to display all currently connected clients. After selecting a session, the connection can be disconnected.

Migration

Once a database has been selected, the “Migration”:#migration can be started via the ribbon. This also allows multiple version 7 databases to be merged into one.

! When the migration is started, the database is set to migration mode. For the duration of the migration, it is not possible to log in to the database – users who are already logged in will be sent a corresponding message. The sessions will, however, remain open so that users can continue working as soon as the migration is complete.

Certificates

Management of the certificates is very important. This is described in the section certificates.

Display database users

This button can be used to call up statistics about the users in the respective databases. It shows you which users are active in which database. Naturally, this list can also be exported.

Data backup

Here you can view the history of all backups or also a single backup.

Show history

All backups of the database are displayed hierarchically in a sortable list.

Importing

A backup can be restored here. This can be done via a file or from the history. The procedure is described under Backup management

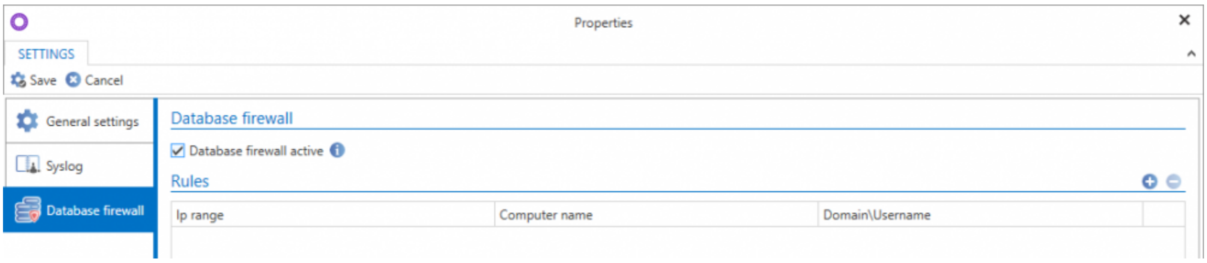
Database firewall

What is the database firewall?

The database firewall enables you to regulate access to the database. A whitelist policy is used for this process. Firewall rules are used to allow access to the database in individual cases.

Activating the firewall

The firewall can be directly activated in the database settings.



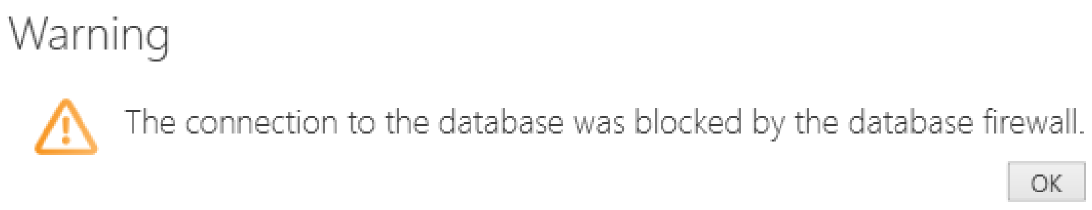
Database firewall

☑ Database firewall active

Rules

Ip range	Computer name	Domain\Username

Access to the firewall is blocked after it has been activated. Login attempts are directly blocked.

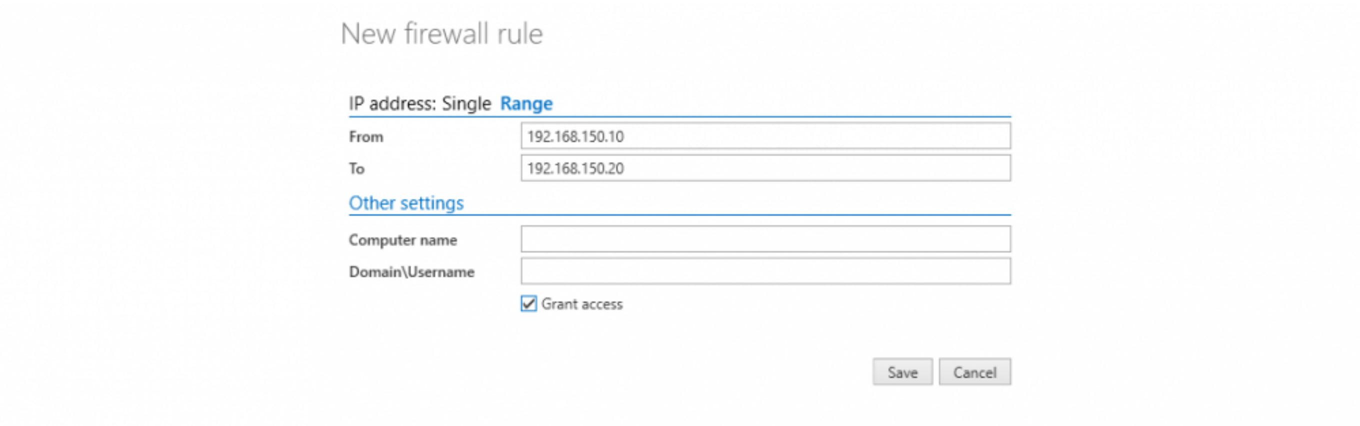


Warning

The connection to the database was blocked by the database firewall.

Firewall rules

The rules already set are displayed in the section on the right. The icons ⊕ and ⊖ can be used to add or also delete rules. Rules can be edited by double clicking on them.



New firewall rule

IP address: Single **Range**

From: 192.168.150.10

To: 192.168.150.20

Other settings

Computer name:

Domain\Username:

☑ Grant access

The following possibilities exist:

- Access from an individual computer is allowed via the **IP address**.
- A **Range** of multiple **IP addresses** can also be optionally selected.
- It is also possible to regulate access using the **Computer name**.
- Finally, access can also be allowed for a certain Windows user. For example, the administrator can be allowed access irrespective of the computer being used.
- The setting **Grant access** defines whether access is allowed or blocked. This is symbolised by a corresponding icon.

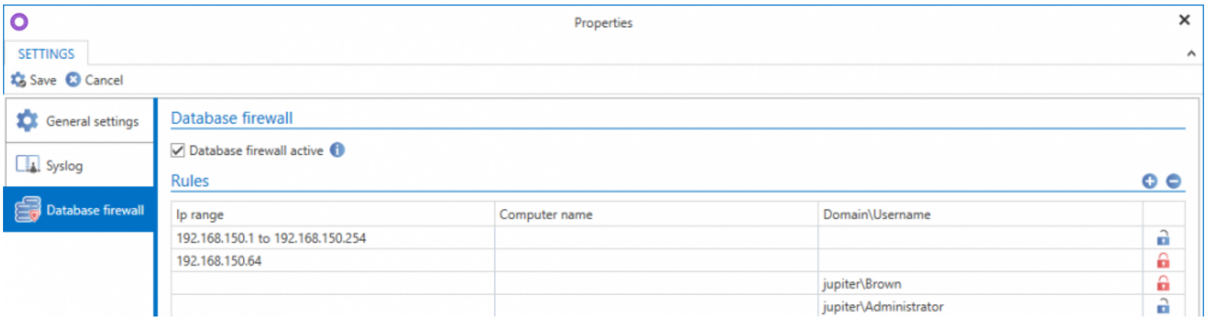
Naturally, the rules can also be combined. It is thus possible e.g that only one defined user can access one database from a certain IP address.

The conditions are always combined using **AND operators**

If two or more rules overlap, the rule with the least rights will always be applied. For example, if a rule allows access from a range of IP addresses but another rule blocks a specific computer within this range then the rule blocking the computer is applied.

Examples

The functionality of the firewall will be explained in more detail using the following rules:



Database firewall

☑ Database firewall active

Rules

Ip range	Computer name	Domain\Username	
192.168.150.1 to 192.168.150.254			🔓
192.168.150.64			🔒
		jupiter\Brown	🔒
		jupiter\Administrator	🔓

Approving an IP range (Rule 1)

The first rule in the example allows access from a range of IP addresses from 192.168.150.1 to 192.168.150.254

Locking a particular computer (Rule 2)

The computer with the IP 192.168.150.64 is within the range defined in Rule 1. Access from this PC is blocked using this rule.

Blocking an individual user (Rule 3)

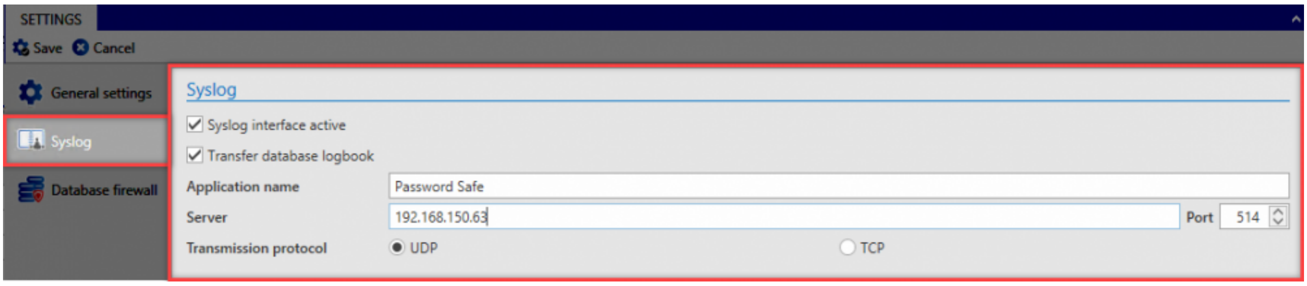
If you want to block a particular user (perhaps because they have left the company) then this is also possible.

Computer-independent access for a user (Rule 4)

This rule grants access to the administrator. It is irrelevant which computer the administrator uses to log in to the database.

Syslog

If desired, the server logs and also the logbook can be transferred to a Syslog server. Double clicking on a database allows you to access its settings. The corresponding menu items can be found there.



Syslog

☑ Syslog interface active

☑ Transfer database logbook

Application name: Password Safe

Server: 192.168.150.63 Port: 514

Transmission protocol: ● UDP ○ TCP

After activating the Syslog interface via the corresponding option, it is possible to configure the Syslog server. If desired, the entire logbook can also be transferred via another option.

HSM connection via PKCS # 11

What is the HSM connection?

The HSM connection ensures that the server keys can be outsourced to the HSM. This ultimately leads to an increased protection because the keys are not directly in the server’s access. The connection is effected via PKCS # 11.

Requirements

In order to be able to connect an HSM, the following conditions have to be met:

- An executable HSM has to be available.
- The PKCS # 11 drivers have to be installed on the application server.
- The Enterprise Plus Edition has to be licensed.
- The device is set up via the Administrator database on the AdminClient

! Please note, if an HSM is to be used, the database also has to be set up thoroughly. It is currently not possible to transfer an existing database to an HSM.

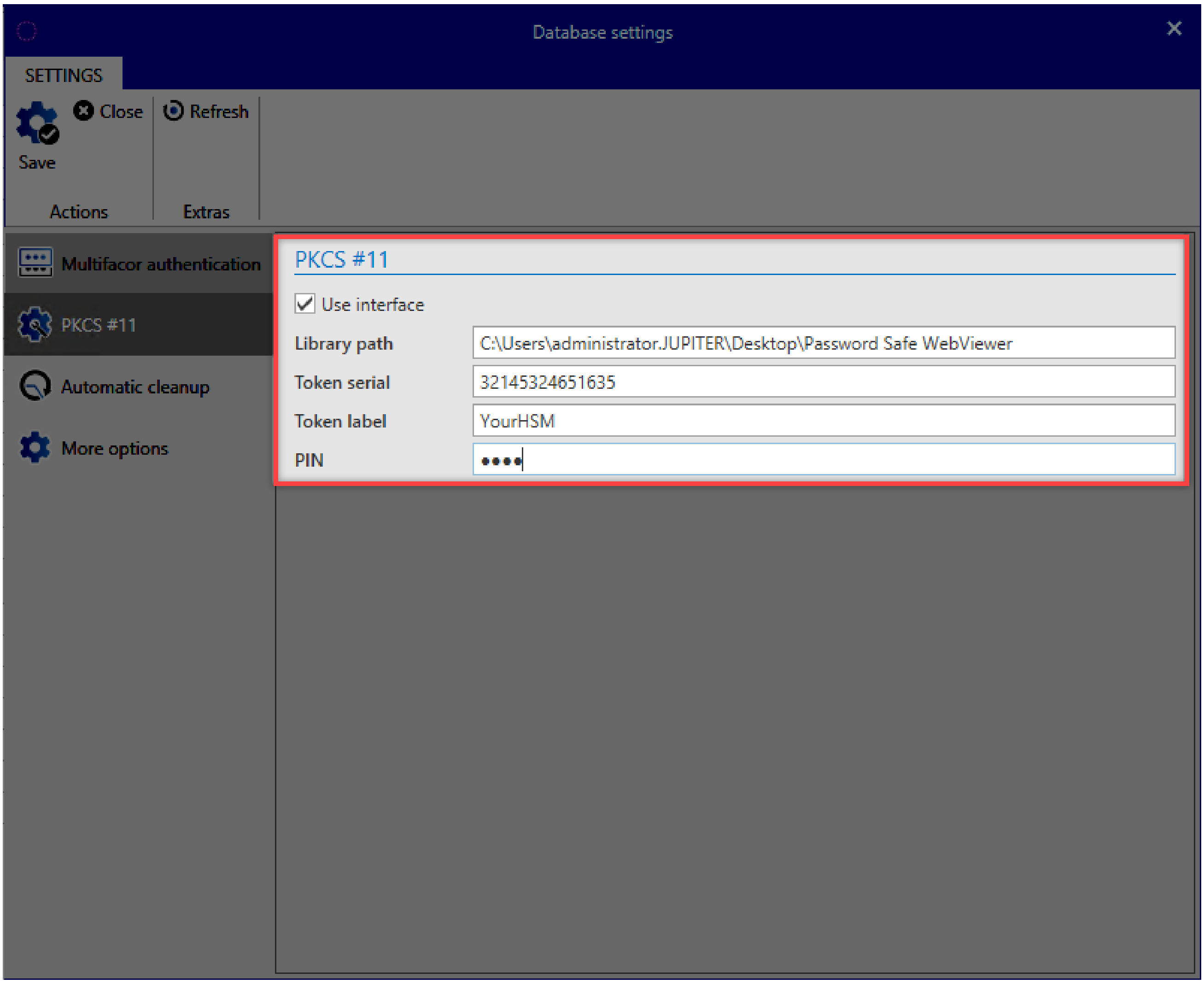
Hardware tested by MATESO GmbH

Basically every HSM should work with PKCS # 11 interface. However, if you use an HSM that does not belong to the following products that we have tested, it is recommended that you try it in advance in a test or POC.

- SafeNet Luna SA – HSM with network connection
- SafeNet Luna PCI-E – Embedded HSM

Installation

The installation is set up on the AdminClient via the database settings



PKCS #11

☑ Use interface

Library path: C:\Users\administrator.JUPITER\Desktop\Password Safe WebViewer

Token serial: 32145324651635

Token label: YourHSM

PIN: ••••

- **Library path**: Here you can find the installed PKCS # 11 driver of the HSM.
- **Token-Serial**: The serial number of the token is given here.
- **Token Label**: The name of the token.
- **PIN**: Finally, the PIN is specified for authentication at the token.

Use by Password Safe

As soon as the HSM is connected, all server keys are transferred to the HSM. This is definitely the database certificate. If the AD has been connected in Masterkey mode, the masterkey will also be transferred to the HSM. Then the certificates are no longer stored in the certificate store of the application server, but centrally managed by the HSM. All other keys are not stored on the HSM, but derived from the masterkeys. Therefore, Password Safe rarely accesses the HSM, for example, at server startup or at the AD Sync. As a result, the load on the HSM can be kept low.

Main menu

What is the main menu?

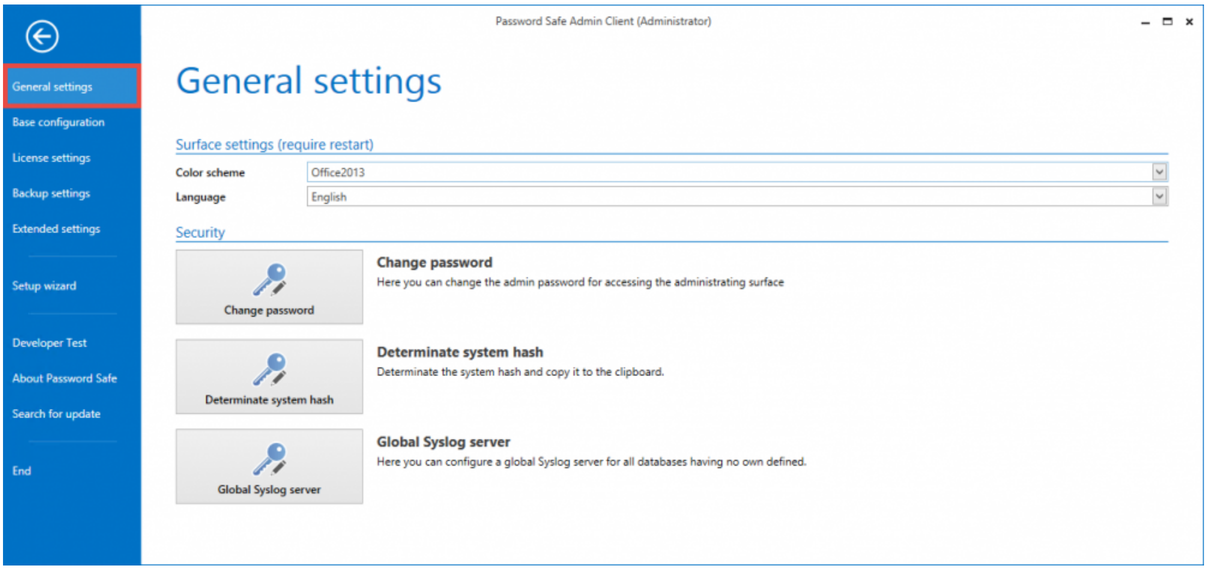
The operation and structure of the Main menu/Backstage menu is the same for the Main menu on the client. This area can be used independently of the currently selected module.

- General settings
- “Backup settings”:#backup-einstellungen
- “License settings”:#lizenzeinstellungen
- “Advanced settings”:#erweiterte-einstellungen

General settings

What are general settings?

Within the general settings, surface settings regarding the colour scheme as well as the language used are configured. The password for logging in to the AdminClient can also be changed here.



General settings

Surface settings (require restart)

Color scheme: Office2013

Language: English

Security

Change password

Here you can change the admin password for accessing the administrating surface

Determinate system hash

Determinate the system hash and copy it to the clipboard.

Global Syslog server

Here you can configure a global Syslog server for all databases having no own defined.

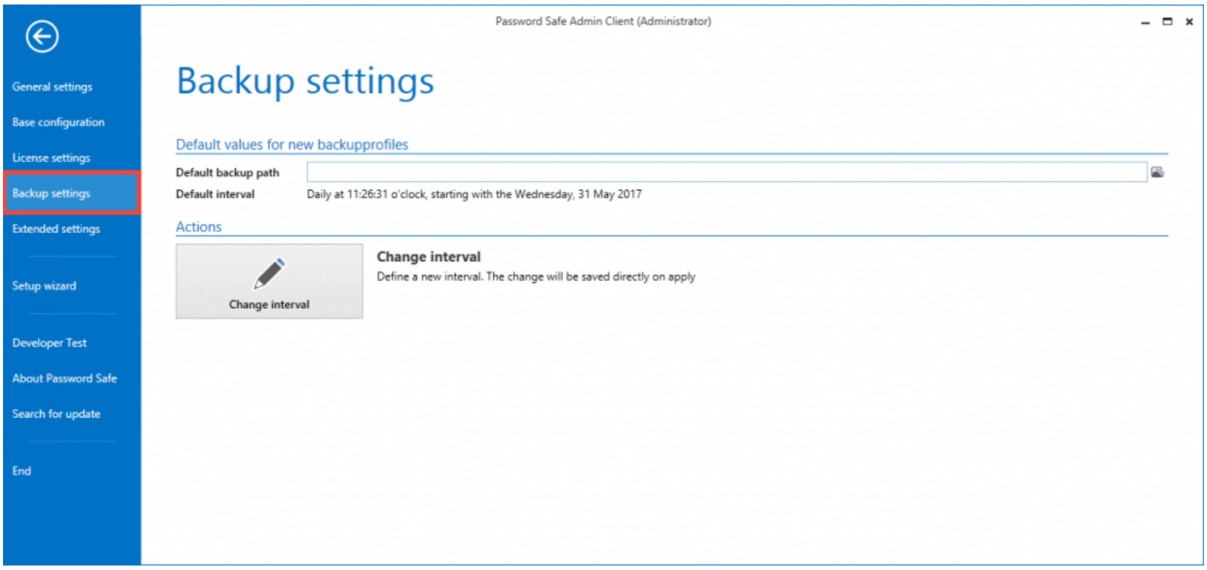
Determining the system hash

This function determines the system hash, and copies it to the clipboard. This hash is used for the offline license.

Backup settings

What are backup settings?

Within the backup settings the default values for the execution of backups can be defined.



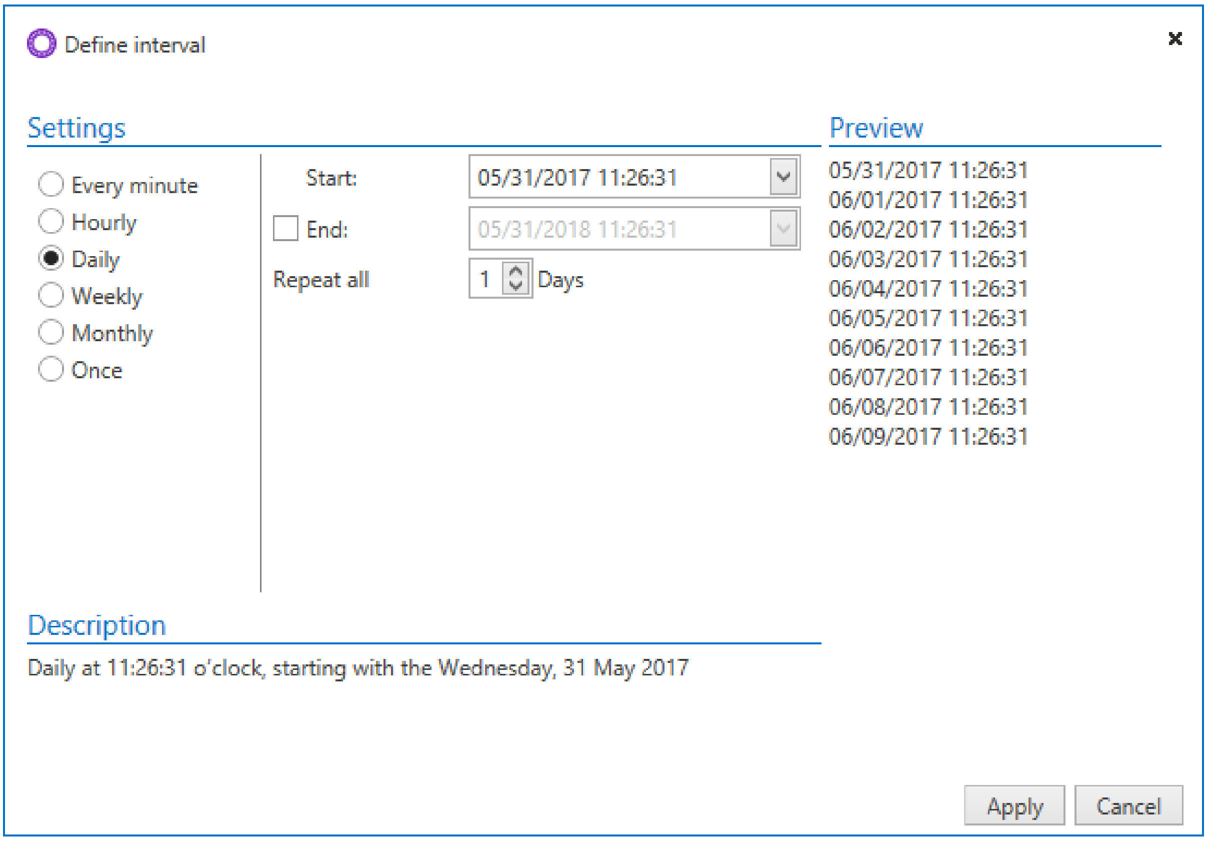
Default backup path

Default interval Daily at 11:26:31 o'clock, starting with the Wednesday, 31 May 2017

Change interval
Define a new interval. The change will be saved directly on apply

Interval settings

The interval for backups can be customized as needed. A separate assistant is available for this purpose.



Settings

○ Every minute
○ Hourly
● Daily
○ Weekly
○ Monthly
○ Once

Start: 05/31/2017 11:26:31

□ End: 05/31/2018 11:26:31

Repeat all 1 Days

Preview

05/31/2017 11:26:31
06/01/2017 11:26:31
06/02/2017 11:26:31
06/03/2017 11:26:31
06/04/2017 11:26:31
06/05/2017 11:26:31
06/06/2017 11:26:31
06/07/2017 11:26:31
06/08/2017 11:26:31
06/09/2017 11:26:31

Description

Daily at 11:26:31 o'clock, starting with the Wednesday, 31 May 2017

Backup management

Introduction

Regular backups of the data should always be part of every security concept. If you wish to create backups directly on the SQL server, you should also include the Password Safe databases. If no central backups are carried out at the SQL level, you can create backup profiles using the AdminClient. The backups themselves will then be generated on the SQL Server.

Difference between an incremental and full backup

A complete backup always saves all data in a database. An incremental backup also creates a complete image of the database as the first step. In future, only the changes since the backup created at the beginning will be saved. This saves both time and memory capacity.

Backup concept

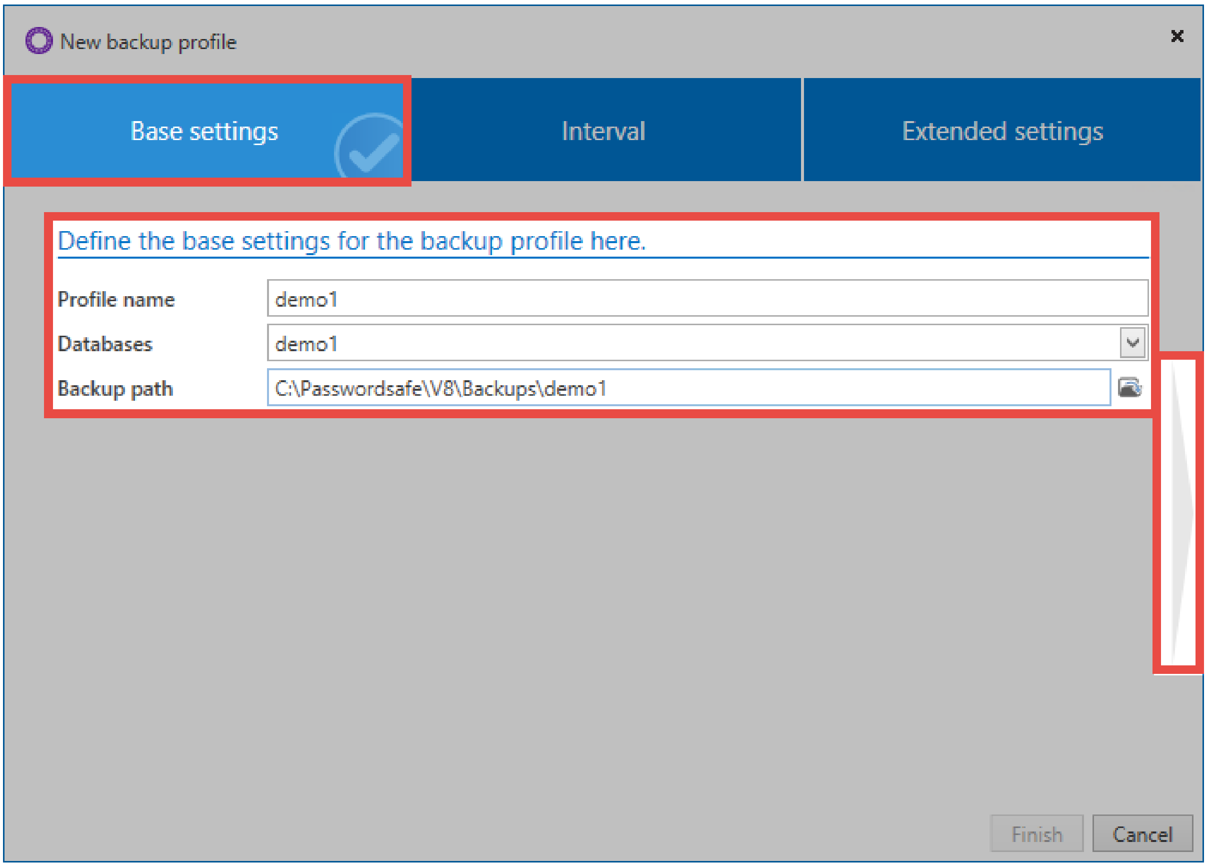
It is recommended that an incremental backup is run every hour. In addition, a full backup should be created once a week.

Managing the backup schedule

Creating a backup schedule

You can create a new schedule via the ribbon. This is facilitated by a wizard. All the information entered under “Backup settings”:#backup-einstellungen will be used by default.

A profile name is entered first. The desired databases are also selected. You also need to specify the directory for the backups.



Define the base settings for the backup profile here.

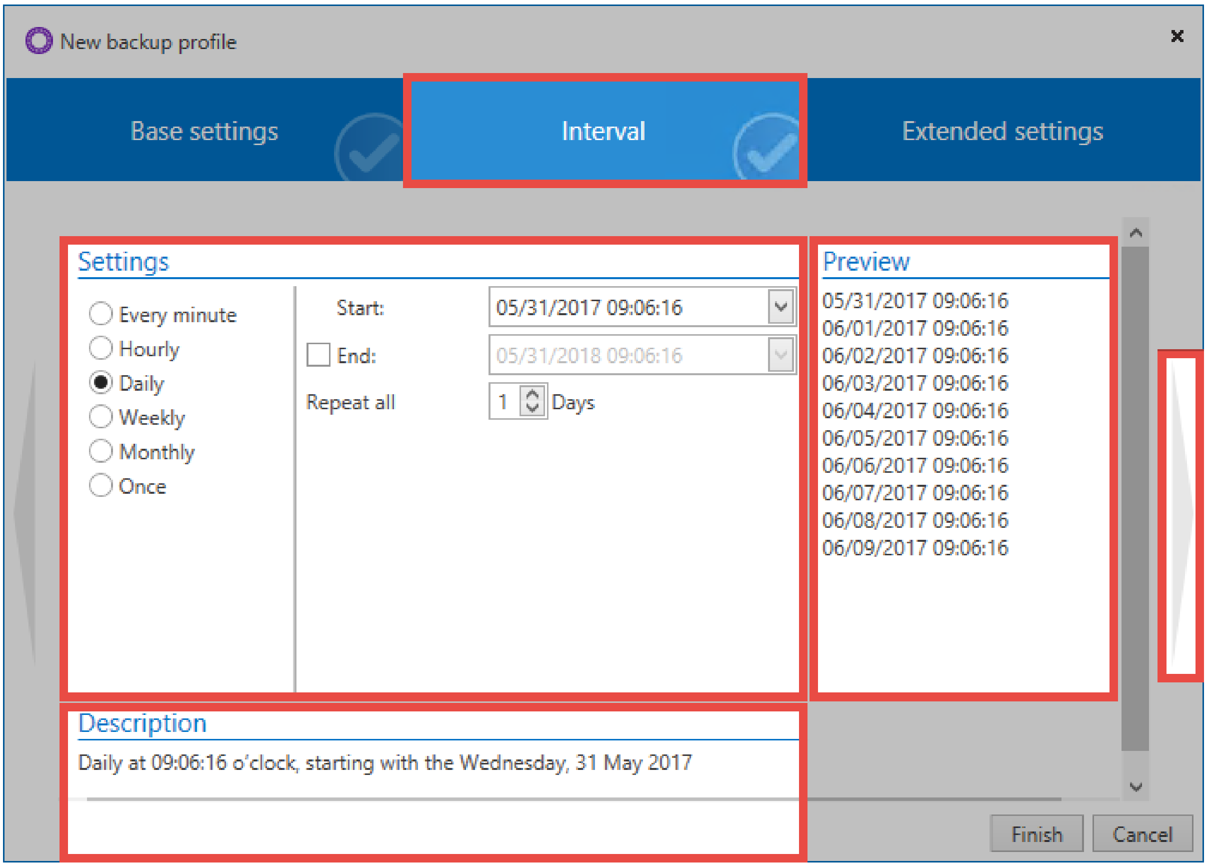
Profile name: demo1

Databases: demo1

Backup path: C:\Passwordsafe\V8\Backups\demo1

It must be a directory on the SQL server.

Now set the time interval for creating the backups. A preview on the right will show when the backups will be created in future. An end date can be optionally entered.



Settings

○ Every minute
○ Hourly
● Daily
○ Weekly
○ Monthly
○ Once

Start: 05/31/2017 09:06:16

□ End: 05/31/2018 09:06:16

Repeat all 1 Days

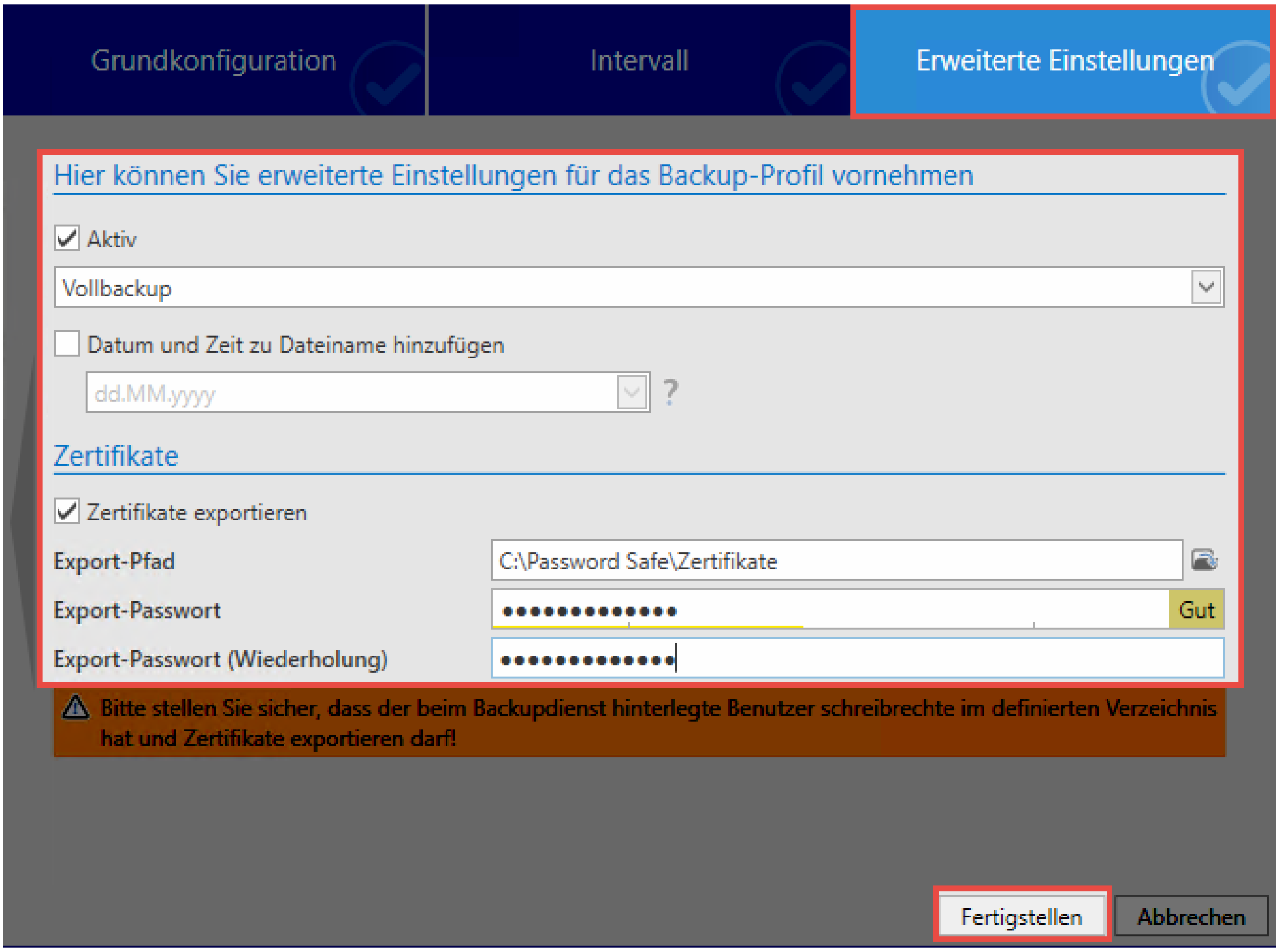
Preview

05/31/2017 09:06:16
06/01/2017 09:06:16
06/02/2017 09:06:16
06/03/2017 09:06:16
06/04/2017 09:06:16
06/05/2017 09:06:16
06/06/2017 09:06:16
06/07/2017 09:06:16
06/08/2017 09:06:16
06/09/2017 09:06:16

Description

Daily at 09:06:16 o'clock, starting with the Wednesday, 31 May 2017

In the advanced settings, you can configure whether the backup should be activated directly. It is also possible to specify whether to create incremental backups. If the date and time are added to the file name, a new backup is created with each run. If this is not done, the last backup is always overwritten. The service user can be used to create the backup or a service user can be specified with a corresponding name and password.
In addition, you can enter here whether the required certificates should be saved using a backup task. Further information can be found in the section Certificates.



Hier können Sie erweiterte Einstellungen für das Backup-Profil vornehmen

☑ Aktiv

Vollbackup

□ Datum und Zeit zu Dateiname hinzufügen

dd.MM.yyyy ?

Zertifikate

☑ Zertifikate exportieren

Export-Pfad	C:\Password Safe\Zertifikate
Export-Passwort	••••••••••••• Gut
Export-Passwort (Wiederholung)	•••••••••••••

⚠ Bitte stellen Sie sicher, dass der beim Backupdienst hinterlegte Benutzer schreibrechte im definierten Verzeichnis hat und Zertifikate exportieren darf!

Backup run

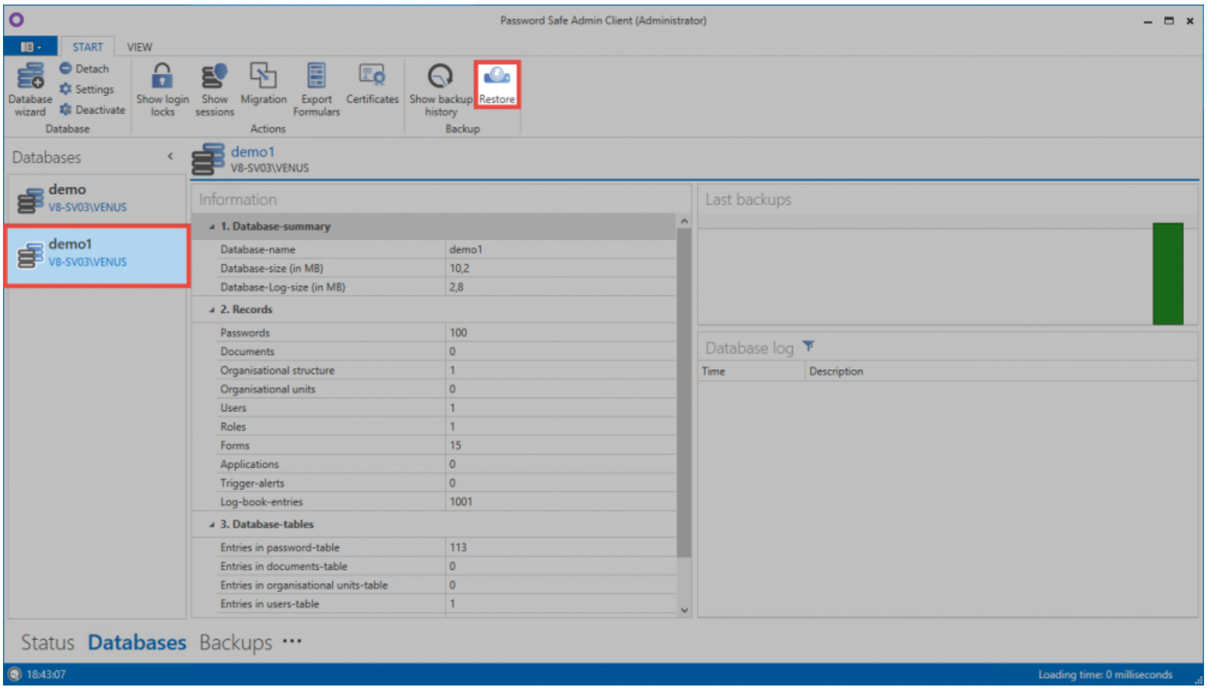
The backups are executed by the SQL server in the background. If an error occurs, this is indicated in “orange” in the backup list. Information about any errors issued by the SQL server is displayed under all backups. A backup will be automatically deactivated if it does not run 5x in a row. This will be marked in the list in red. The schedule cannot be reactivated directly. You will need to open it and amend it.

Other backup actions

A selected schedule can be deleted via the ribbon. The wizard for a schedule can be called up by double-clicking on it to make any changes. In addition, a backup can be started directly via the ribbon at any time. The backup service must be running for this purpose. You can also display this in the history.

Restoring data from a backup

Restoring data from backups is performed using the database module. Data can only be restored to existing databases. Firstly, select the required database. You can now select **Insert** in the ribbon.



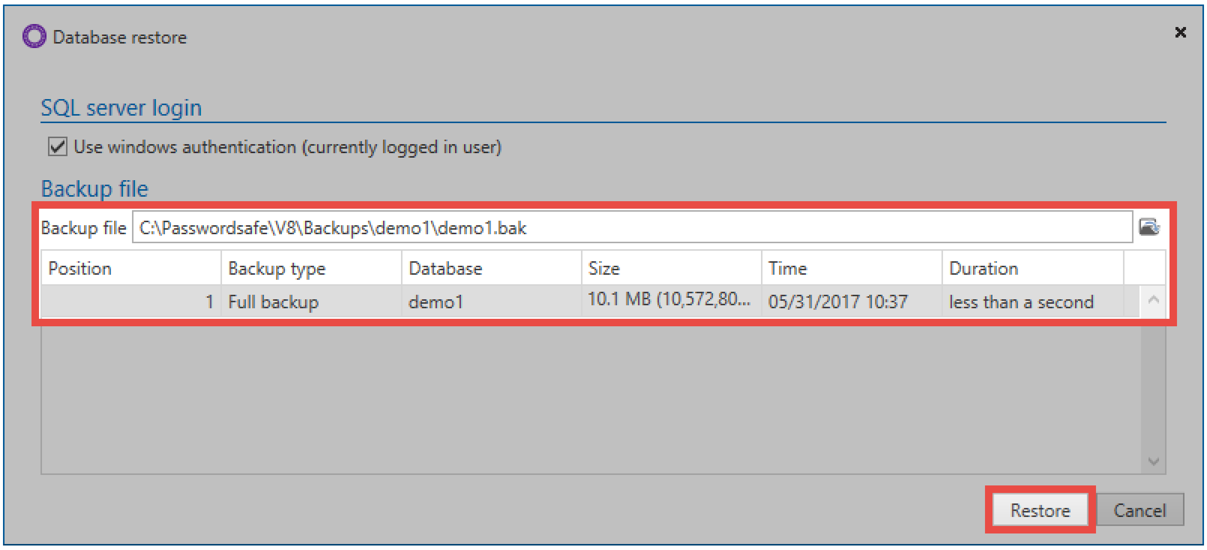
demo
V8-SV03\VENUS

demo1
V8-SV03\VENUS

Information

1. Database-summary	
Database-name	demo1
Database-size (in MB)	10,2
Database-Log-size (in MB)	2,8
2. Records	
Passwords	100
Documents	0
Organisational structure	1
Organisational units	0
Users	1
Roles	1
Forms	15
Applications	0
Trigger-alerts	0
Log-book-entries	1001
3. Database-tables	
Entries in password-table	113
Entries in documents-table	0
Entries in organisational units-table	0
Entries in users-table	1

If necessary, firstly enter login data for the user that logs in to the SQL server – although the service user is generally used here. Now select the backup file. All the backups contained in the file will then be displayed. Now simply click on **Restore** to restore the backup to the existing database.



SQL server login

☑ Use windows authentication (currently logged in user)

Backup file

Backup file C:\Passwordsafe\V8\Backups\demo1\demo1.bak

Position	Backup type	Database	Size	Time	Duration
1	Full backup	demo1	10.1 MB (10,572,80...	05/31/2017 10:37	less than a second

Disaster recovery scenarios

Finding a quick solution in the event of a disaster

In our experience, Password Safe is usually installed in IT in a central location. If the system fails, it must be possible to gain access to the passwords again as quickly as possible. This section is designed to help you quickly find a solution in the event of a problem.

Prevention

It is extremely important to create a sensible recovery plan and to make corresponding preparations. Unfortunately, it is not possible to supply a finished recovery plan because it always needs to be created individually. The following points should be taken into account in this process:

Creating backups

It is of course essential in the event of a disaster that you can access a backup that is as up-to-date as possible. Therefore, it is necessary to regularly create “backups”:#backupverwaltung.

Who is responsible in the event of a disaster?

The first thing to decide is who should take action in the event of a disaster. Corresponding deputies should also be defined. The responsible employee should have the corresponding rights within Password Safe.

Providing the required passwords

What passwords do those people responsible need in order to restore Password Safe?

- Domain password to log into the specific computer
- Password for the AdminClient
- Access data for the service user
- Access data for the SQL user
- Password for logging into Password Safe

Furthermore, it must be ensured that the responsible user has access to these passwords at all times. The following options are possible:

- Store the passwords in the company safe
- Create corresponding “offline databases”:#offline-client

- Periodically create a HTML WebViewer file with automatic delivery via a system task including “email forwarding”:#benachrichtigungen

Disaster scenarios

The following section will describe various disaster scenarios including the possible recovery steps.

Scenario 1

Problem:
Database is corrupt

Solution:
Restore the database from a backup.

Scenario 2

Problem:
Database server is faulty

Solution:
Install the database server on new hardware. If the server name changes as a result, the licence needs to be reactivated. If the licence has already been activated multiple times, it may be that it can only be released again by MATESO. If the SQL instance name changes, the connection to the database server needs to be reconfigured on the application server. This is carried out via the basic configuration.
Any existing offline databases will continue to function properly.

Scenario 3

Problem:
Application server faulty

Solution:
New installation on new hardware. The licence must be reactivated. If the server name has changed, it may be that the licence can only be released again by MATESO. The basic configuration must be completed to restore the connection to the database server. If the server name changes, the database profile on the client needs to be amended.
Any existing offline databases need to be recreated!

Scenario 4

Problem:
Both servers are faulty but passwords from Password Safe are required urgently.

Solution:

Install the database server and application server on new hardware. The licence must be reactivated. Restore the database from the backup. The basic configuration must be completed to restore the connection to the database server. If the licence has already been activated multiple times, it may be that it can only be released again by MATESO.

Any existing offline databases need to be recreated!

Scenario 5

Problem:

As for Scenario 4 but the Active Directory is also not available.

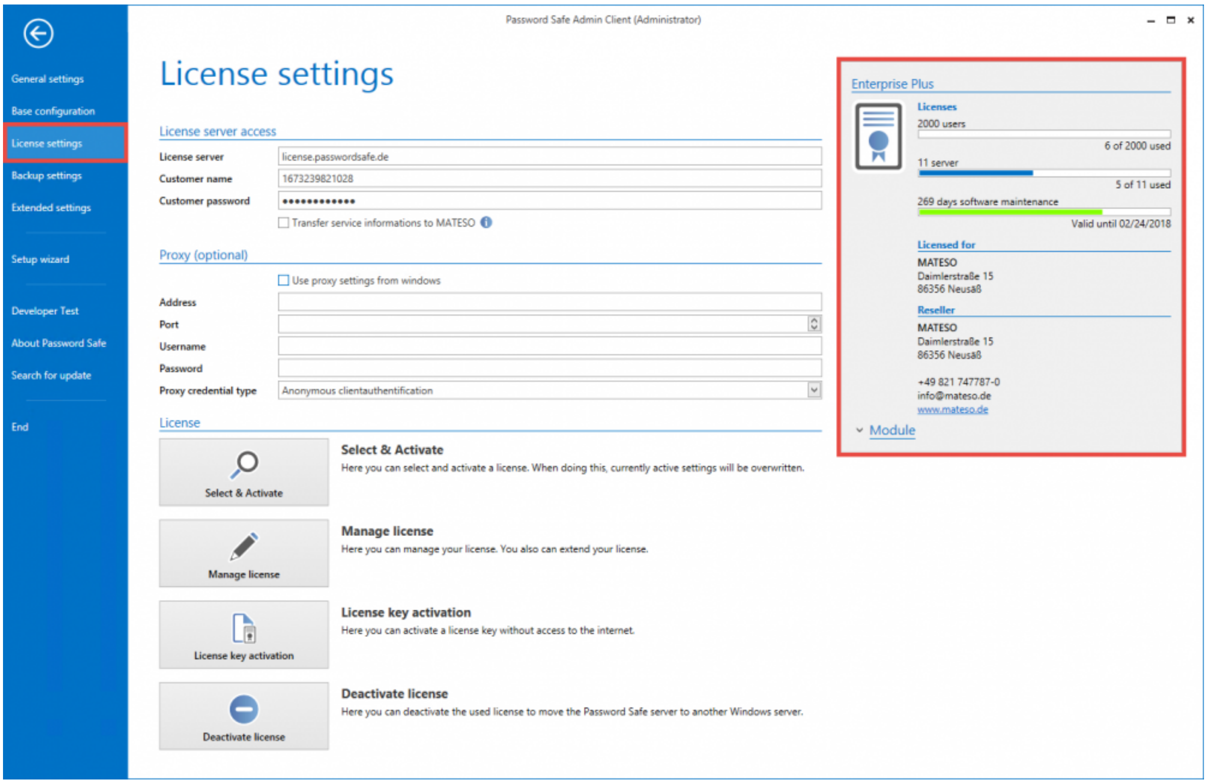
Solution:

As described for scenario 4. If the user was imported in end-to-end mode, you can also log in without an AD connection. Users imported in Masterkey mode cannot log in. Therefore, it is recommended that you create special, local emergency users for such cases.

License settings

What are license settings?

Licenses for the Password Safe are managed within the license settings. In addition, all current license details are displayed in the window provided for this purpose.



License settings

License server access

License server: license.passwordsafe.de

Customer name: 1673239821028

Customer password: ●●●●●●●●●●●●●

□ Transfer service informations to MATESO

Proxy (optional)

□ Use proxy settings from windows

Address:

Port:

Username:

Password:

Proxy credential type: Anonymous clientauthentification

License

Select & Activate
Here you can select and activate a license. When doing this, currently active settings will be overwritten.

Manage license
Here you can manage your license. You also can extend your license.

License key activation
Here you can activate a license key without access to the internet.

Deactivate license
Here you can deactivate the used license to move the Password Safe server to another Windows server.

Enterprise Plus

Licenses
2000 users
6 of 2000 used
11 server
5 of 11 used
269 days software maintenance
Valid until 02/24/2018

Licensed for
MATESO
Daimlerstraße 15
86356 Neusäß

Reseller
MATESO
Daimlerstraße 15
86356 Neusäß

+49 821 747787-0
info@mateso.de
www.mateso.de

Licenses

! Version 7 licenses cannot be used for Password Safe Version 8. “Please contact us”: http: //www.passwordsafe.de to obtain a version 8 license.

Licenses are linked via the MATESO license server. Here are the details:

- license.passwordsafe.de
- IP: 185.48.116.55
- Port 443 TCP (standard HTTPS port)

Ensure that this server is accessible. You may also use Proxy servers. The license is retrieved from the server and stored in the server configuration. The license will be checked every hour, and updated as required. The retention time is 30 days. If there is no internet connection, you can continue to work for 30 days. If this period should cause problems, please contact us.

Integrating and managing licenses

After purchase, you will receive the required license information in the form of “customer name” and “password”. Enter this information directly into the **License Server Access** area. Use the **Select and Activate** button to establish a connection to the license server. You can select the acquired licenses from a list. The license can be now used.

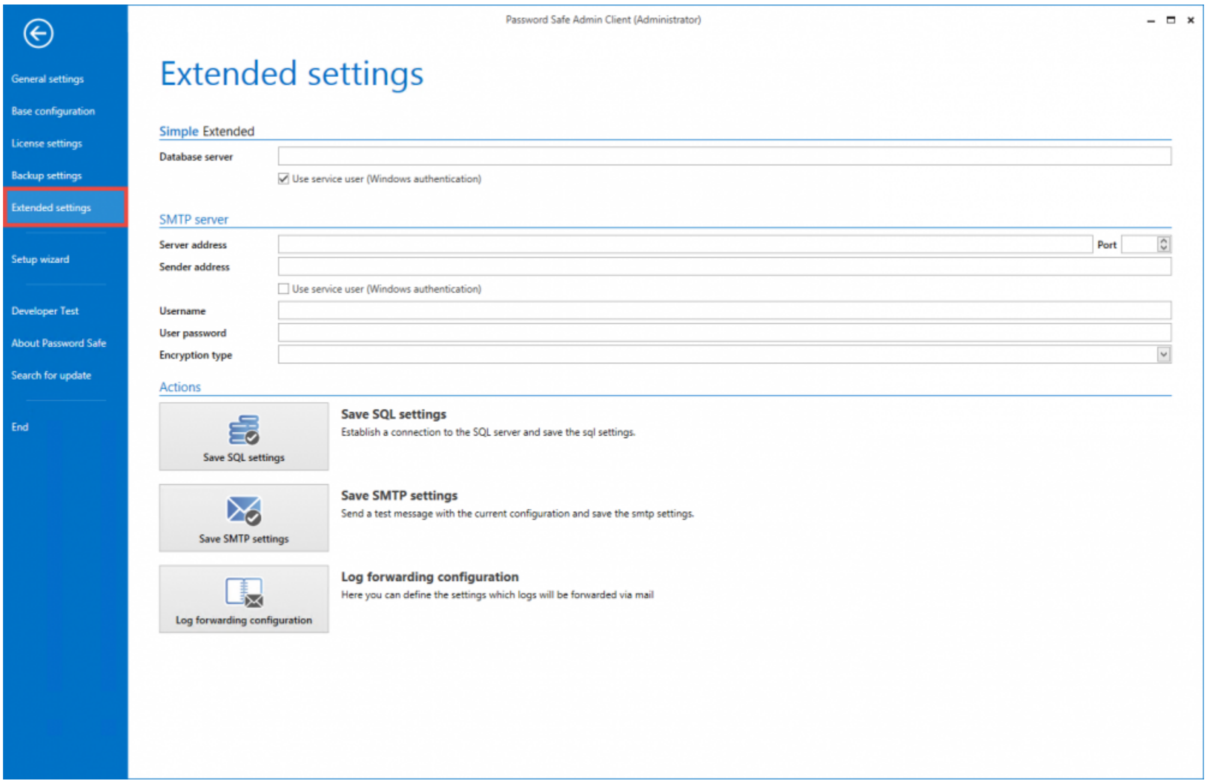
> ✻ Optionally, you may specify a proxy. By default, the proxy stored in the operating system is used.

> ! The licence is called up in the context of the service user. If you experience connection problems, the firewall and, if relevant, the proxy should be checked.

Advanced settings

What are advanced settings?

Global standard default values are specified in the advanced settings.



Extended settings

Simple Extended

Database server

☑ Use service user (Windows authentication)

SMTP server

Server address Port

Sender address

□ Use service user (Windows authentication)

Username

User password

Encryption type

Actions

Save SQL settings
Establish a connection to the SQL server and save the sql settings.

Save SMTP settings
Send a test message with the current configuration and save the smtp settings.

Log forwarding configuration
Here you can define the settings which logs will be forwarded via mail

Database server

The database server stored here is used as a default value when rebuilding databases. There are 2 modes:

Simple mode

In simple mode, the path to the database server including the user and the associated password can be specified. You may use the service user for this purpose.

Advanced mode

In extended mode, the connection string can be specified, which contains both the server, the user and the password

SMTP server

By configuring the SMTP server you define all settings for emails, which the server should send, eg via the notification system. At the final save, the connection is directly tested for functionality. The “Save SMTP settings” button becomes active only after a change has been made.

Offline Client

What is the offline client?

The offline client enables you to work without an active connection to the Password Safe server. If the corresponding setting has been configured, the local copy of the server database will be automatically synchronized according to freely definable cycles. This ensures that you can always use a (relatively) up-to-date version of the database offline.

Facts

- “Microsoft SqlServer Compact 4.0.8876.1” is used for creating offline databases
- The database is encrypted using AES-128 or SHA-256. A so-called “platform default” is used for this purpose
- In addition, RSA encryption processes are used
- More on this subject…::https://technet.microsoft.com/en-us/library/gg592949(v=sql.110).aspx

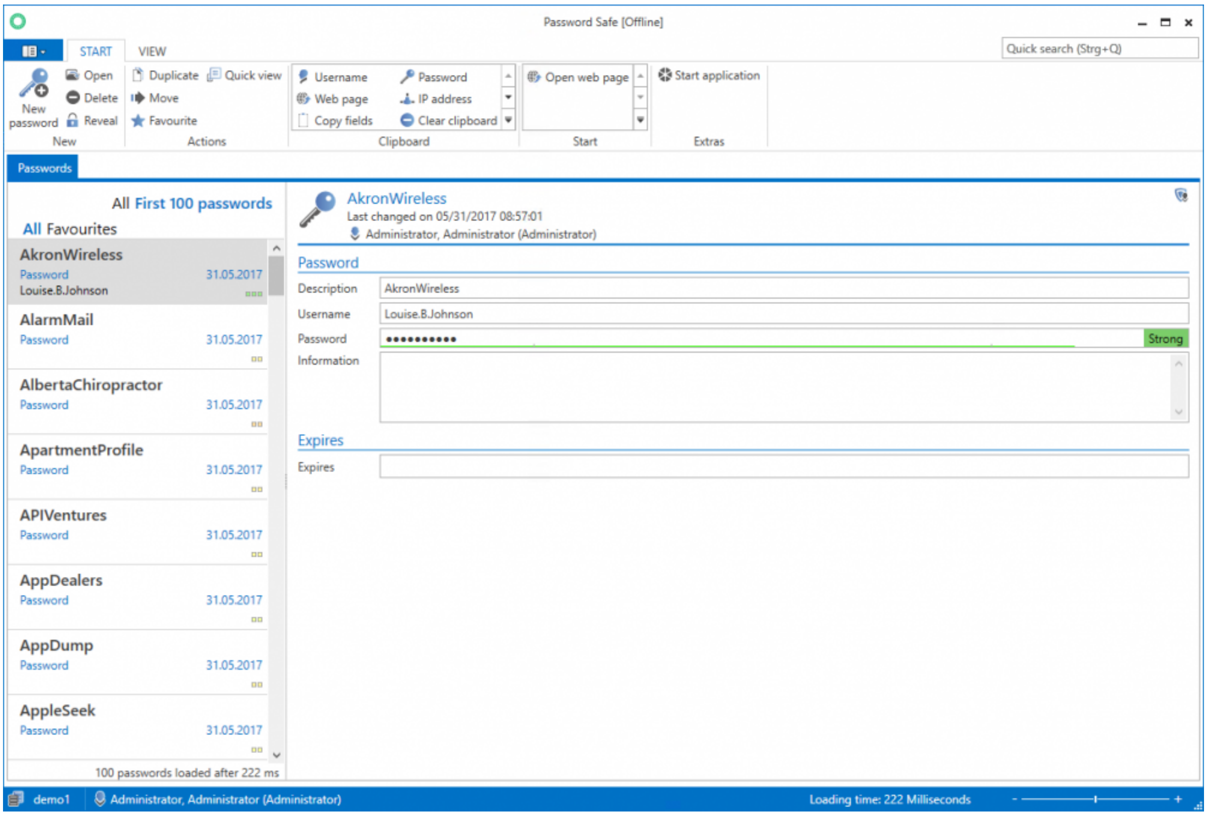
Installation

The offline client is automatically installed together with the main client. No database profiles need to be created – this task is performed by the client during the initial synchronization, together with the creation of the offline database.

Operation

Operation of the offline client is generally based on the operation of the main client. Since the offline client only has a limited range of functions, the following must be taken into account with regards to its operation:

- There is no dashboard
- Only the password module is available
- The filter is not available. Records are found using the quick search
- The automatic login data entry can be performed via the SSO agent, independently of the offline client



AkronWireless
Password 31.05.2017
Louise.B.Johnson

AlarmMail
Password 31.05.2017

AlbertaChiropractor
Password 31.05.2017

ApartmentProfile
Password 31.05.2017

APIVentures
Password 31.05.2017

AppDealers
Password 31.05.2017

AppDump
Password 31.05.2017

AppleSeek
Password 31.05.2017

100 passwords loaded after 222 ms

AkronWireless
Last changed on 05/31/2017 08:57:01
Administrator, Administrator (Administrator)

Password

Description	AkronWireless
Username	Louise.B.Johnson
Password	●●●●●●●●●●● Strong
Information	

Expires

Expires	

demo1 Administrator, Administrator (Administrator) Loading time: 222 Milliseconds

What data is synchronised?

Seals enhance the security concept in Password Safe to include a double-check principle that can be defined in fine detail. This means that releases for protected information are linked to the positive authentication of one or more users. Naturally, it is not possible to issue these releases when the server is not connected. For this reason, sealed records are not synchronized and thus do not form part of offline databases.

Otherwise, all records for which the user has the **export right** are synchronised.

Records with **password masking** are adopted into the offline database and can be used as normal.

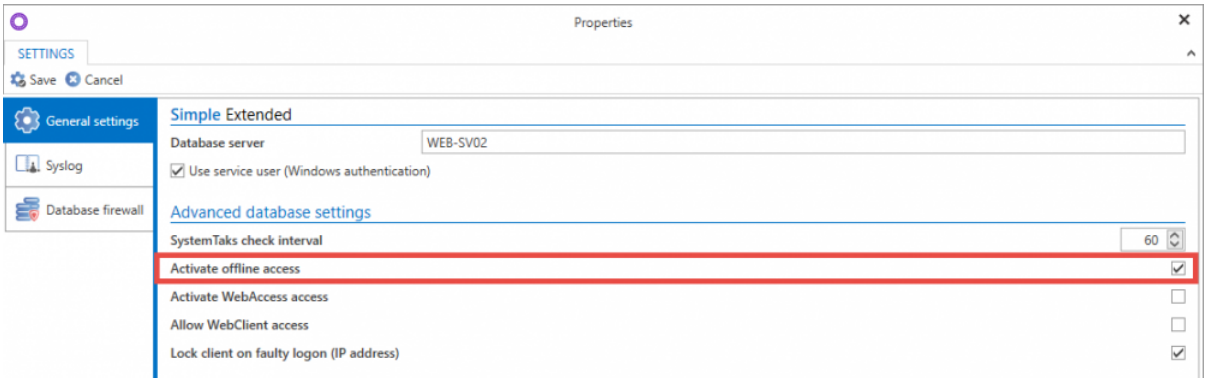
Setup and sync

Setting up the offline database

It is important to ensure that the right requirements have been met before setting up the offline client. The following configurations need to be defined in both the AdminClient and also the user rights/user settings.

Requirements

To set up offline databases, this option must firstly be activated in the AdminClient. This process is carried out separately for each database in the database view in the AdminClient in the “General settings” (right click on the database). This is also possible to do when the database is initially created.



Database server WEB-SV02

☑ Use service user (Windows authentication)

SystemTaks check interval 60

Activate offline access ☑

Activate WebAccess access □

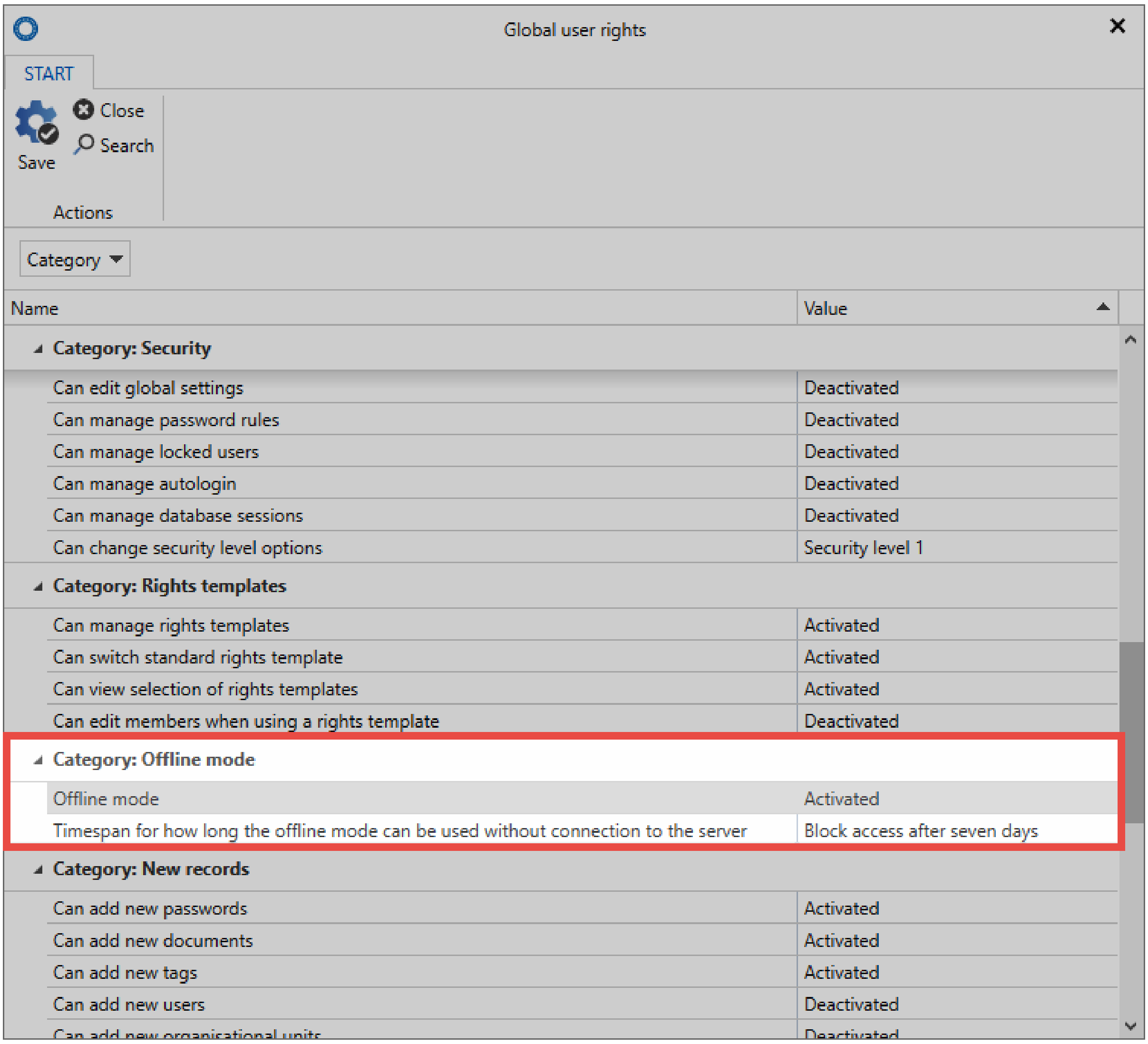
Allow WebClient access □

Lock client on faulty logon (IP address) ☑

You will find further information on this subject in the sections: Creating databases and Managing databases

User rights

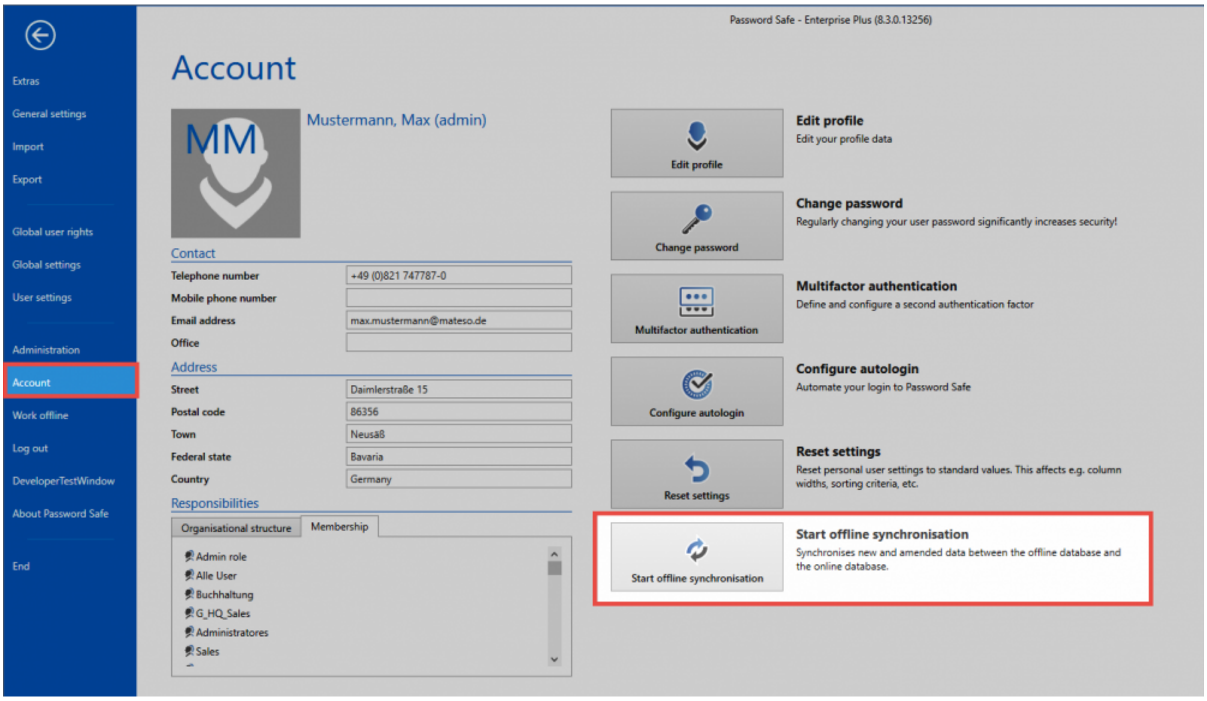
The user requires the “offline mode” right. In addition, how long offline mode can be used without a server connection can be defined in the user rights.



Name	Value
Category: Security	
Can edit global settings	Deactivated
Can manage password rules	Deactivated
Can manage locked users	Deactivated
Can manage autologin	Deactivated
Can manage database sessions	Deactivated
Can change security level options	Security level 1
Category: Rights templates	
Can manage rights templates	Activated
Can switch standard rights template	Activated
Can view selection of rights templates	Activated
Can edit members when using a rights template	Deactivated
Category: Offline mode	
Offline mode	Activated
Timespan for how long the offline mode can be used without connection to the server	Block access after seven days
Category: New records	
Can add new passwords	Activated
Can add new documents	Activated
Can add new tags	Activated
Can add new users	Deactivated
Can add new organisational units	Deactivated

Creating an offline database

The synchronization with the offline database can generally be carried out automatically. However, **the first synchronization must be carried out manually**. The synchronization is started via the Main menu/Account.



Password Safe - Enterprise Plus (8.3.0.13256)

Account

Mustermann, Max (admin)

Contact

Telephone number	+49 (0)821 747787-0
Mobile phone number	
Email address	max.mustermann@mateso.de
Office	

Address

Street	Daimlerstraße 15
Postal code	86356
Town	Neusäß
Federal state	Bavaria
Country	Germany

Responsibilities

- Admin role
- Alle User
- Buchhaltung
- G_HQ_Sales
- Administratores
- Sales

Edit profile Edit your profile data

Change password Regularly changing your user password significantly increases security!

Multifactor authentication Define and configure a second authentication factor

Configure autologin Automate your login to Password Safe

Reset settings Reset personal user settings to standard values. This affects e.g. column widths, sorting criteria, etc.

Start offline synchronisation Synchronises new and amended data between the offline database and the online database.

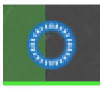
> ✻ The offline databases are stored locally under the following path: %appdata%\MATESO\Password Safe and Repository Client\OfflineDB

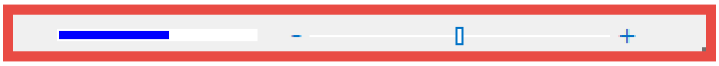
An offline database can be created per user and client for each online database. This makes it possible to use several offline databases with an offline client.

Synchronization

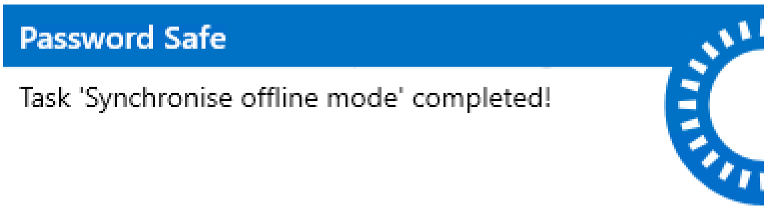
In order to keep the data always consistent, the offline database must be synchronized regularly. Synchronization is automatically performed by the client in the background. The interval can be freely configured in the settings. The synchronization is completed every 30 minutes by default. When creating and editing records, it is also possible to synchronize outside of the synchronization cycle so that the changes are directly available offline. In addition, the synchronization can also be started manually in Backstage via “Account”.

A running synchronization is displayed in the icon in the task bar as well as by a status bar in the client:





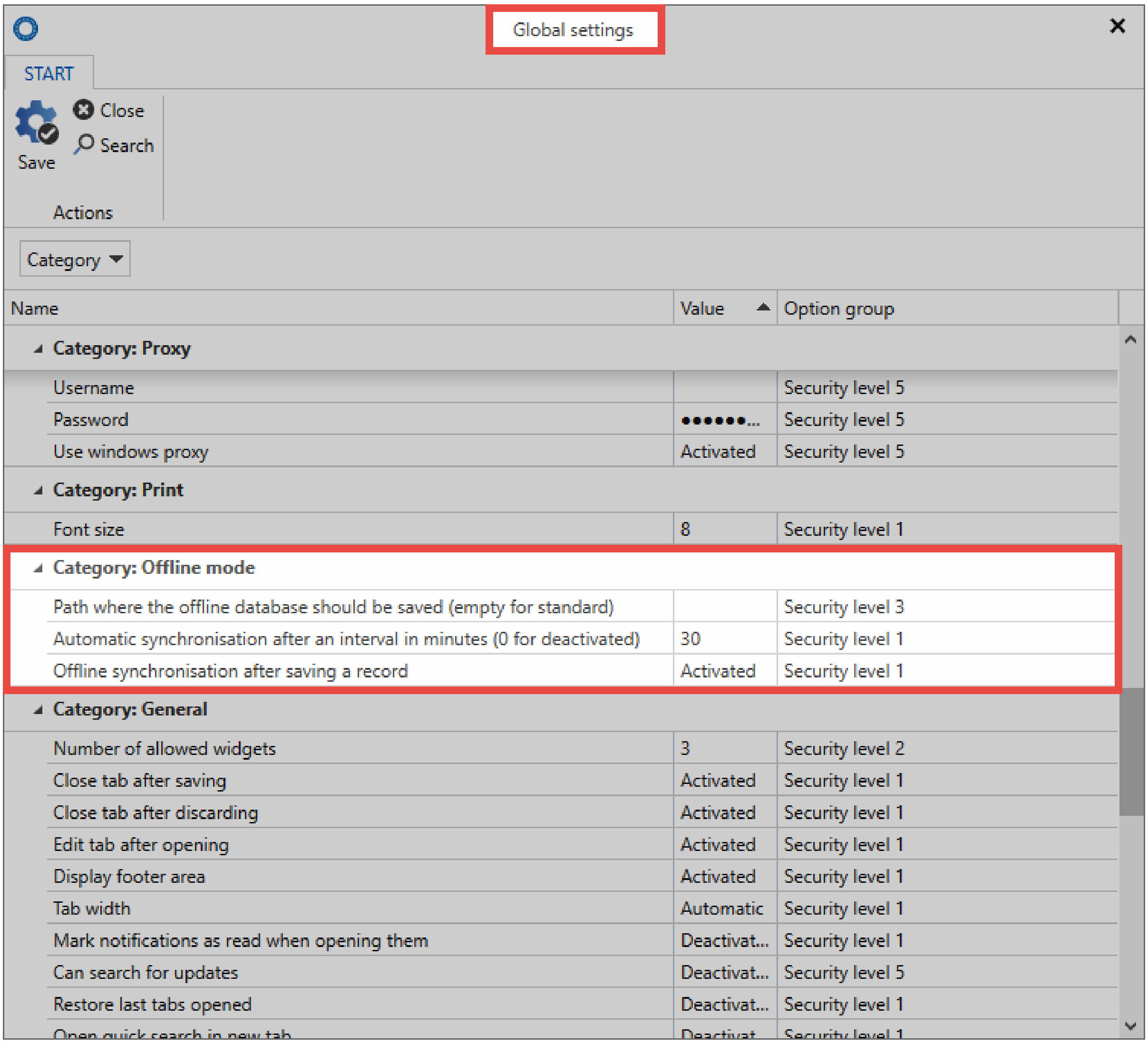
As soon as the synchronization is completed, this is indicated by a hint.



Password Safe

Task 'Synchronise offline mode' completed!

Relevant settings



Name	Value	Option group
Category: Proxy		
Username		Security level 5
Password	●●●●●●...	Security level 5
Use windows proxy	Activated	Security level 5
Category: Print		
Font size	8	Security level 1
Category: Offline mode		
Path where the offline database should be saved (empty for standard)		Security level 3
Automatic synchronisation after an interval in minutes (0 for deactivated)	30	Security level 1
Offline synchronisation after saving a record	Activated	Security level 1
Category: General		
Number of allowed widgets	3	Security level 2
Close tab after saving	Activated	Security level 1
Close tab after discarding	Activated	Security level 1
Edit tab after opening	Activated	Security level 1
Display footer area	Activated	Security level 1
Tab width	Automatic	Security level 1
Mark notifications as read when opening them	Deactivat...	Security level 1
Can search for updates	Deactivat...	Security level 5
Restore last tabs opened	Deactivat...	Security level 1
Open quick search in new tab	Deactivat	Security level 1

Offline mode can be configured and personalised using the four settings mentioned:

- "Offline synchronization after saving a record": The synchronization of the offline database is completed directly after saving a record. It is important to note that this only applies to those records that are saved by the user who is logged in. Changes made by another user do not trigger any synchronization!

- **Automatic synchronization after an interval**: This setting is used to define the interval at which a synchronization of the offline database will be periodically carried out. The default value is 30 minutes.
- **Path where the offline database should be saved**: If this field is left empty, the system default is used. The storage location for the offline database can otherwise be entered directly.

Mobile devices

Synchronisation with mobile devices

There are plans to develop apps tailored specifically to Password Safe version 8. As this project is very time intensive and other issues currently have a higher priority, the synchronisation process will be temporarily carried out using the apps for Password Safe version 7.

WebClient as an alternative

An alternative to the synchronisation process is to use the Password Safe WebClient. This is responsive and can thus be operated on all standard smartphones and tablets.

Advantages

The WebClient offers the following advantages:

- **Live data**
  The WebClient connects directly to the database and thus always has access to the latest data. This highlights the biggest disadvantage of the apps. The apps only ever provide access to the status at the time of the synchronisation. If data have been changed since the synchronisation, this will not be available on the mobile device.

- **Functional scope**
  The WebClient currently has a much larger range of functions than the apps. It is possible, for example, to use sealed or masked passwords.

- **Convenience**
  No synchronisation is necessary because the WebClient directly accesses the database.

Disadvantages

The WebClient requires an active Internet connection to access the data.

Conclusion

Ideally, the WebClient and the apps are used together in combination. The WebClient provides permanent access to the latest data, while the data saved on the app can be accessed if there is no Internet connection in an exceptional situation.

Apps

Apps are currently available for iOS, Android and also Windows Phone devices. They can be directly installed on the mobile device via the Apple App Store, Windows App Store or Google Playstore. The apps are naturally available free of charge.

Settings

Settings related to the synchronisation are available on both the client and the server.

Server-based settings

The synchronisation has to be activated for each database on the AdminClient. The corresponding option can be found in the database settings.

Client-based settings

The following settings on the client are worth mentioning:

- **Validity of the mobile database without synchronisation in days**
  This setting defines how long the mobile database can be used without synchronisation. Once this period has expired, it is no longer possible to log into the database.

- **Maximum number of login attempts before deleting the database**
  In order to protect the data against unauthorized access, it is possible to define the maximum number of failed login attempts before the mobile database is deleted.

Required rights

The user rights are used to define how and via which route the user is permitted to carry out a synchronisation

- **Can synchronise mobile devices**
  The general right to synchronise is issued to the user here. This right always allows a synchronisation to be carried out via WiFi.

The following rights can additionally define the route via which the synchronisation can be carried out:

- **Mobile cloud synchronisation via Dropbox** available for iOS and Android
- **Mobile cloud synchronisation via Google Drive** available for Android
- **Mobile cloud synchronisation via iCloud** available for iOS
- **Mobile cloud synchronisation via iTunes** available for iOS
- **Mobile cloud synchronisation via OneDrive** available for Windows Phone

Synchronization

Requirements

A mobile database needs to be created before the first synchronisation. In addition, it is important to ensure that the required rights have been issued.

Synchronisation via the app

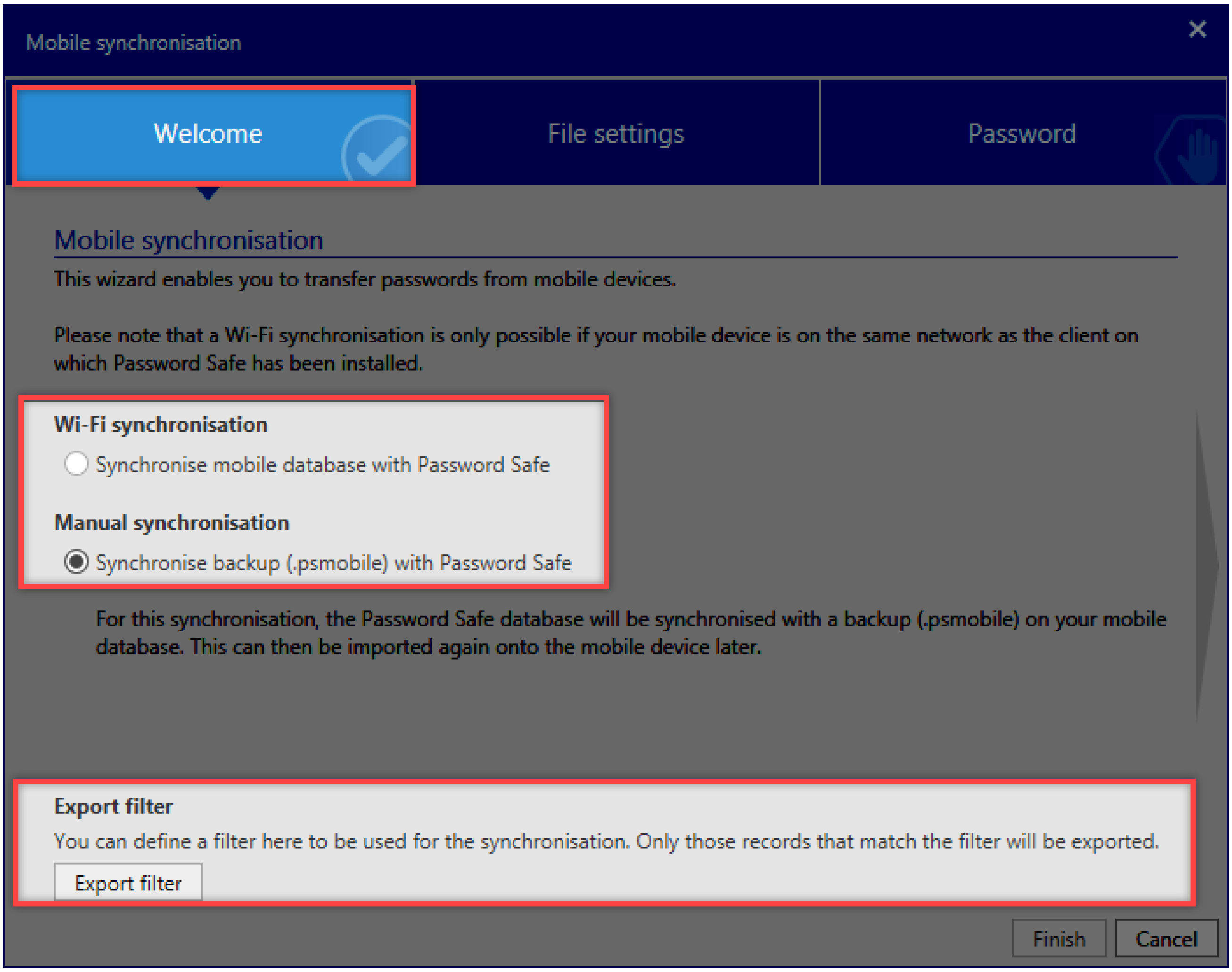
The different routes and processes for the synchronisation are described in detail in the documentation for the relevant app. These can be found under the following links:

Password Safe app for iOS
Password Safe app for Android
Password Safe app for Windows Phone

> ✻ All of the screenshots for the client refer to documentation for the version 7 apps. Therefore, they look different to the client in version 8. However, the functionality of the app is either identical or very similar.

Synchronisation via the client

The synchronisation is started in “Backstage” under **Account** on the Password Safe client. A corresponding wizard guides you through the synchronisation. In the first step of the wizard, you select whether the synchronisation should be completed via **WiFi** or **manually**. In addition, the export filter can be used to select which records are synchronised.



Mobile synchronisation

This wizard enables you to transfer passwords from mobile devices.

Please note that a Wi-Fi synchronisation is only possible if your mobile device is on the same network as the client on which Password Safe has been installed.

Wi-Fi synchronisation

○ Synchronise mobile database with Password Safe

Manual synchronisation

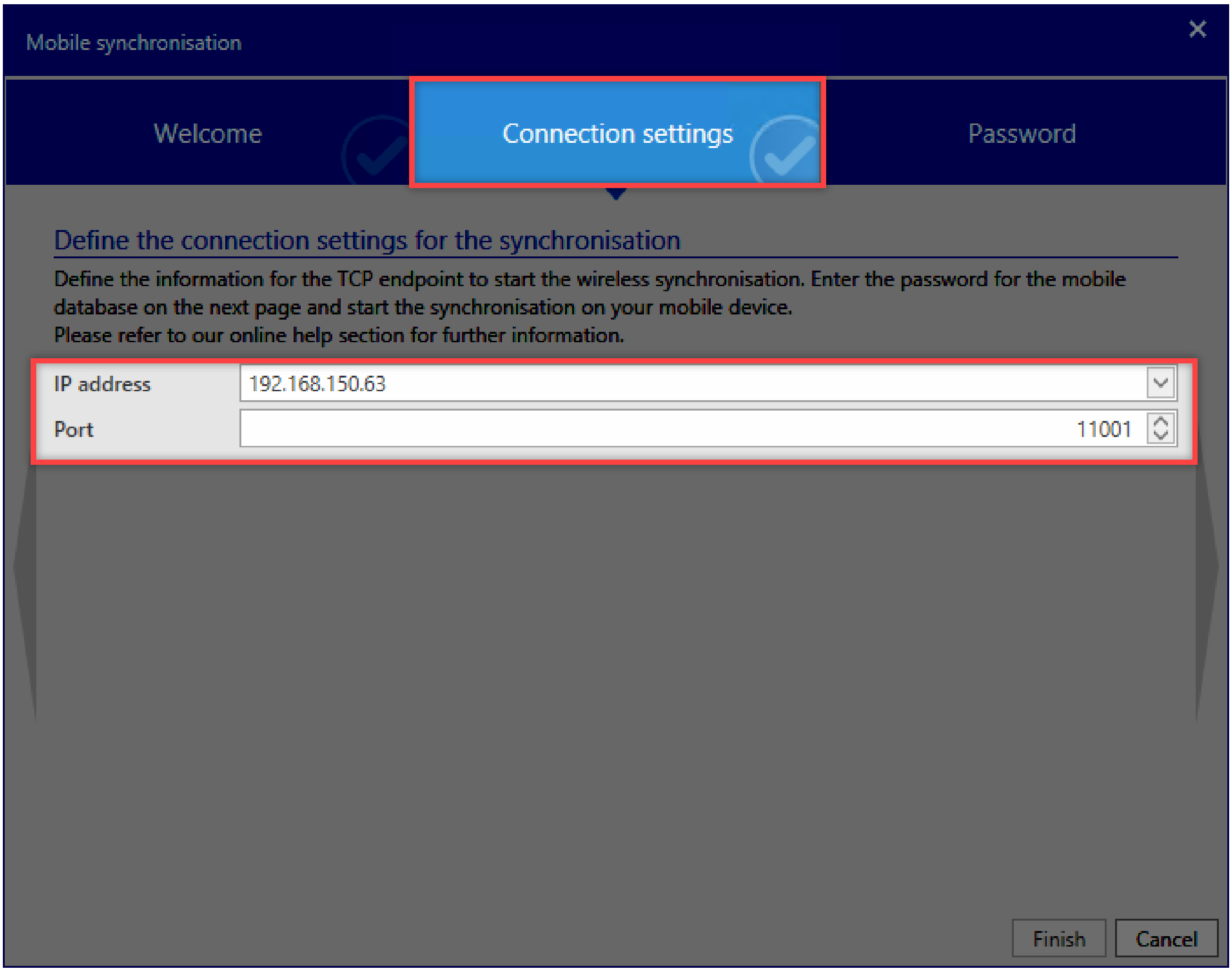
● Synchronise backup (.psmobile) with Password Safe

For this synchronisation, the Password Safe database will be synchronised with a backup (.psmobile) on your mobile database. This can then be imported again onto the mobile device later.

Export filter

You can define a filter here to be used for the synchronisation. Only those records that match the filter will be exported.

The second step is used to select the adapter via which the synchronisation is carried out. If manual synchronisation has been chosen, the storage location for the synchronisation file is selected.



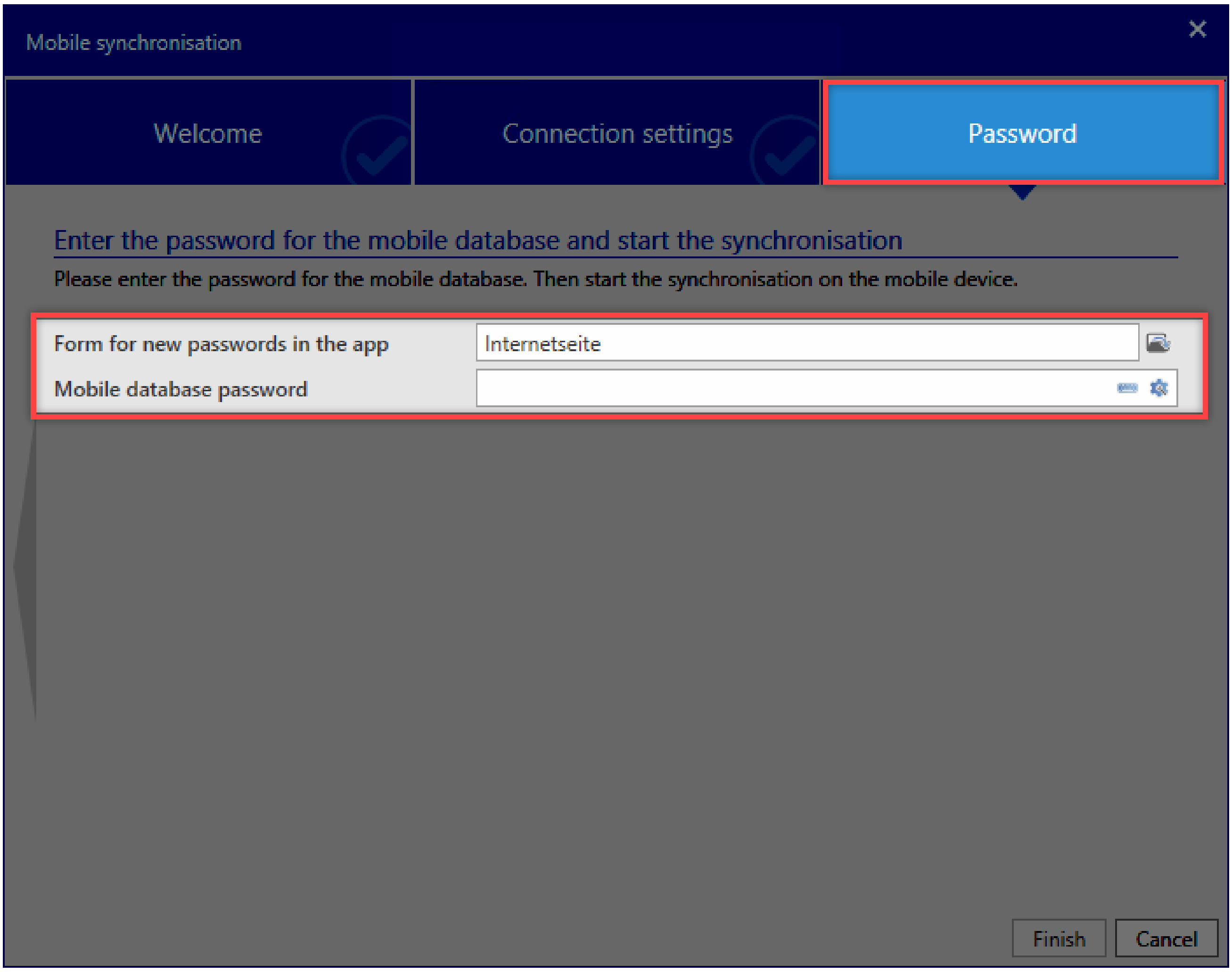
Define the connection settings for the synchronisation

Define the information for the TCP endpoint to start the wireless synchronisation. Enter the password for the mobile database on the next page and start the synchronisation on your mobile device.
Please refer to our online help section for further information.

IP address 192.168.150.63

Port 11001

In the final step, it is possible to define which form can be used to create new records in the app. The **password for the mobile database** is also entered here.



Enter the password for the mobile database and start the synchronisation

Please enter the password for the mobile database. Then start the synchronisation on the mobile device.

Form for new passwords in the app	Internetseite
Mobile database password	

High availability

What is high availability?

High availability is designed to guarantee the further operation of Password Safe in the event of damage. A series of requirements need to be met **in advance** in order to use this feature.

! As the configuration of high availability is complex, it is (generally) implemented during a consultation. If you are interested in this feature, please contact us directly or contact your responsible partner.

Requirements

The following points should be observed during the configuration.

- It is essential that MSSQL Enterprise Version is used for replicating the database (even in the case of a replication across multiple locations)
- To achieve a better level of protection, we recommend operating the Password Safe database on its own cluster
- A Password Safe application server needs to be licensed for each location. Every application server has its own configuration database.

Load balancer

- To reduce the load on the server, a load balancer can be installed upstream of the application server
- If no load balancer is used, the distribution of the database profiles for the users is generally carried out via the registry

If a database is set up at ”location A” including an AD profile, the certificate needs to exported there and then imported onto the server at “location B”. The database is replicated using MSSQL technology and can be integrated as an existing database into Password Safe at “location B”. If the application server at “location A” fails, the server in the registry needs to be replaced (location B) and rolled out again to users using group rules (GPO).

API

In der Enterprise Plus Edition steht eine **REST API** zur Verfügung. Über diese Schnittstelle ist es möglich Password Safe “von außen anzusprechen” um beispielsweise Daten für andere Programme auszulesen.
Die API ist für **C#** und **JavaScript** verfügbar.

In der JavaScript Version der API sind alle Enums unter dem globalen Objekt “PsrApiEnums” zu finden.

Voraussetzungen und Download

Die API ist ausschließlich in der Enterprise Plus Edition verfügbar. Im Kunden Informations System kann der API-Client für die gewünschte Programmiersprache herunter geladen werden. Um die API nutzen zu können müssen im **AdminClient**, im Modul **WebClient** die Webservices aktiviert werden.

Verwendung der API

Das zentrale Objekt ist „PsrApi“. Dieses enthält diverse „Manager“, welche die gesamte Business Logik enthalten. Zunächst muss ein „PsrApi“-Objekt angelegt werden, der einzige Übergabeparameter dieser Klasse ist der Hostname oder die IP-Adresse des Endpoints (= Password Safe Server).

C#

```
var psrApi = new PsrApi(„passwordsafe.company.com“);
```

JavaScript

```
const psrApi = new PsrApi(„passwordsafe.company.com“)
```

Login

Ohne einen vorherigen Login ist die Verwendung der API nicht möglich. Der erste Parameter der Login-Methode ist die gewünschte Datenbank, gefolgt von Benutzername und dem Passwort. Zu Beachten gilt, dass alle Methoden der API, die einen Server-Call nach sich ziehen, asynchron implementiert sind. In C# werden also Objekte des Typs „Task“ und in JavaScript Objekte des Typs „Promise“ zurück gegeben.

C#

```
await psrApi.AuthenticationManager.Login(„Company“, „username“, „password“);
```

JavaScript

```
await psrApi.authenticationManager.login(„Company“, „username“, „password“)
```

Methoden

Anschließend können alle Methoden der API verwendet werden. So kann mann beispielsweise nach Datensätzen suchen und ein Passwort entschlüsseln:

C#

```
// Passwörter, Formulare und Dokumente sind alle Container
var conMan = psrApi.ContainerManager;

// Den Standard-Filter für Passwörter abrufen
var passwordListFilter = await conMan.GetContainerListFilter(PsrContainerType.Password,

var contentFilter = passwordListFilter.FilterGroups.OfType<PsrListFilterGroupContent>()
if (contentFilter != null)
{
    // Nach Passwörtern suchen, die „mateso“ enthalten
    contentFilter.Search = "mateso";
    contentFilter.FilterActive = true;
}

// Alle Passwörter abrufen, die dem Filter entsprechen
var passwords = await conMan.GetContainerList(PsrContainerType.Password, passwordListFi

// Das Formularfeld vom Typ Passwort suchen
var passwordItem = passwords.FirstOrDefault(p => p.Items.Any(i => i.ContainerItemType =
if (passwordItem != null)
{
    // Wert des Formularfelds entschlüsseln
    var plainText = await conMan.DecryptContainerItem(passwordItem);
    Console.WriteLine("Plaintext value of the container item: " + plainText);
}

// Logout nach vollendeter Arbeit nicht vergessen, um tote Sitzungen zu verhindern
await psrApi.AuthenticationManager.Logout();
```

JavaScript

```
// Passwörter, Formulare und Dokumente sind alle Container
const conMan = psrApi.containerManager

// Den Standard-Filter für Passwörter abrufen
const passwordListFilter = await conMan.getContainerListFilter(PsrApiEnums.PsrContainer

const contentFilter = passwordListFilter.FilterGroups.find(fg => 'SearchList' in fg).Se
if (contentFilter) {
  // Nach Passwörtern suchen, die "mateso" enthalten
  contentFilter.Search = 'mateso'
  contentFilter.FilterActive = true
}

// Alle Passwörter abrufen, die dem Filter entsprechen
const passwords = await conMan.getContainerList(PsrApiEnums.PsrContainerType.Password,

// Das Formularfeld vom Typ Passwort suchen
const passwordItem = passwords
  .find(p => p.Items.some(i => i.ContainerItemType === PsrApiEnums.PsrContainerItemType
  .find(i => i.ContainerItemType === PsrApiEnums.PsrContainerItemType.ContainerItemPass
if (passwordItem) {
  // Wert des Formularfelds entschlüsseln
  const plainText = await conMan.decryptContainerItem(passwordItem)
  console.log('Plaintext value of the container item: ' + plainText)
}

// Logout nach vollendeter Arbeit nicht vergessen, um tote Sitzungen zu verhindern
await psrApi.authenticationManager.logout()
```

Technische Dokumentation

Die komplette technische Dokumentation der API ist unter folgendem Link zu finden: Password Safe API

Version history

The previously released versions and the corresponding change logs can be found in the following sections.

- Version 8.4.0.14618
- Version 8.3.0.14422 Hotfix 1
- Version 8.3.0.13378
- Version 8.2.0.12388 Hotfix 1
- Version 8.2.0.12343
- Version 8.1.1.11211 Hotfix 1
- Version 8.1.1.11106
- Version 8.1.0.10812
- Version 8.0.2.9978 Hotfix 2
- Version 8.0.2.9541 Hotfix 1
- Version 8.0.2.9278
- Version 8.0.1.9032

Version 8.5.0.14896

! In the older versions, there were bugs, which may lead to problems when uncovering passwords. These have been fixed in the current version 8.3.0.14422 hotfix 1. If an older version is used, it is highly recommended to install version 8.5.0.14896 Thus, it is ensured that the problems no longer occur in the future.
It is also important to update the WebClient. You can find further information about the update procedure in the chapter “Update”: {TOPIC-LINK + updates}.

Release

07-11-2018

Compatibility

The following client versions are compatible with AdminClient Version 8.5.0.14896

- Windows Client Version 8.4.0.14618
- Windows Client Version 8.5.0.14896
- WebClient Version 8.3.0.14422
- WebClient Version 8.4.0.14569
- WebClient Version 8.5.0.14896

When updating to version 8.5.0.14896 please note that **Port 11018** must be opened for the realtime API. Further information can be found in chapter Server System Requirements

If the WebClient is used, the module: **proxy_wstunnel** must be installed when using **Apache**. With **IIS** the **WebSocket Protocol** becomes necessary. Further information can be found in the chapter System requirements for WebClient

New

- Realtime updates can be configured in the settings of the database.
- PKCS # 11 settings can now be defined when creating a new database.
- It is now possible to configure that a reason is required when connecting to a RDP or SSH application. Therefor a new setting (by default active) has been added.
- API now supports multi-factor authentication at login.
- It is now possible to compare users of all databases via the “Show database users” feature in the AdminClient.

- Certificates of a database can now be managed in the “Database” module of the AdminClient.
- Database certificates can now be backed up via the backup profile.
- The new user overview of the AdminClient also shows the capacity of the user licenses.

Improvements

- Form fields in passwords of type ‘Heading’ can no longer be focused.
- SSO applications are now started with the configured parameters.
- The setting “Automatically send login masks” is now also taken into account during submission via template (web application).
- The “ps8” protocol for external links has been improved.
- When configuring notifications for multiple objects, the progress bar is now used.
- Layout of the filter in the WebClient has been changed.
- At the WebClient the number of activated filter groups will be displayed in the filter icon.
- Improved the WebClient layout for mobile devices.
- The columns “Tags” and “Form” are now available in the list view of passwords in the OfflineClient.
- When changing the form of multiple passwords, the progress bar is now used.
- It is now prevented that records can be opened after being deleted by other clients.
- General adjustments when discarding changes were made.
- The Google Chrome and Firefox browser extensions display more than five passwords.
- The security level for the customizable window caption setting can now be configured.
- The URL of applications of type “Web” can now be edited.
- The WebViewer configuration can be adjusted without having to reenter the password.
- It is now displayed in the WebViewer export if more passwords exist than can be exported.
- The file size of WebViewer exports was reduced.
- The database wizard now checks if the entered database name already exists and prevents the creation of the database if necessary.
- Improved window size of remote desktop applications.
- Seal release requests are now sent to users and users of roles, even if the requesting user does not have the read permission on the entities.
- Improved customization of grid views.
- Improved buttons in the overview of locked users.
- Subject Alternative Names are now displayed in the AdminClient in the “Base configuration”.
- Performance improvement when working with a high number of databases.
- Environment variables are now supported in the path of offline databases.

Changes

- All documents that are saved simultaneously now receive the same authorizations.
- The user right “Can manage password form fields” now also determines the creation of new fields.
- Already existing Active Directory users are no longer imported during migration.
- Migration now takes the port from the hostname field of version 7, if neither a port field was found, nor a port was specified in the IP address field.

- The setting for maximum number of records is no longer taken into account for the WebViewer export. Depending on the configured filter, all passwords are now exported.
- The password policy managament of the AdminClient was moved to the “General settings”.

Fixed

- The configuration of the TelNet connection is now displayed in the reading pane of SSH applications.
- The selected users in the filter groups will be also cleared when clearing the filter in the WebClient.
- Fixed an issue with the Internet Explorer addon, which sometimes did not open a new webpage via the addon.
- Fixed an issue that after changing a password the reading pane did not refresh.
- Fixed an issue that historic entries of passwords were marked as changed even if there were no changes.
- Offline synchronization has been revised and several bugs have been fixed.
- The export and import of forms now takes over default values and policy information.
- The export and import of applications now takes over the gateway server settings.
- Fixed an offline synchronization issue that could result in duplicate form fields.
- Autofill works if there are more than five passwords available for a website.
- Fixed an issue that it was not possible to open form fields by clicking on the button in the notifications and loogbook module.
- Fixed an issue with web applications that own fields of type ‘Password’ were not filled correctly.
- Setting “Disconnect database connection due to inactivity after” works correctly in the WebClient if it is changed at runtime.
- Fixed a bug that Offline synchronization was not possible for Master Key users if an Autologin is configured.
- When sorting by date fields, empty values are now considered.
- Added missing texts for Discovery Service.
- The SSO-Agent now only permits local connections.
- Fixed an issue during automatic cleanup and export of log entries.
- RDP applications now always start centered, if the windowed mode is used.
- Fixed a memory leak during login and logout at the client.
- Fixed error when restarting the services with the AdminClient.
- Fixed error regarding the browser autofill when there is no protocol defined in the URL field.
- An existing SMTP configuration can be reset with the wizard of the AdminClient by removing the mail server address.
- The SSO-Agent now only responds to requests of the user it is running on.
- Permissions on forms with multiline password text can be configured again.

Version 8.4.0.14618

! In the older versions, there were bugs, which may lead to problems when uncovering passwords. These have been fixed in the current version 8.3.0.14422 hotfix 1. If an older version is used, it is highly recommended to install version 8.4.0.14618. Thus, it is ensured that the problems no longer occur in the future.
It is also important to update the WebClient. You can find further information about the update procedure in the chapter “Update”: {TOPIC-LINK + updates}.

Release

05-08-2018

Compatibility

The following client versions are compatible with AdminClient Version 8.4.0.14618

- Windows Client Version 8.4.0.14618
- WebClient Version 8.3.0.13347 (not recommended!)
- WebClient Version 8.3.0.14422
- WebClient Version 8.4.0.14569

✻ The WebAccess, which has already been replaced by the WebClient in version 8.3.0, will no longer be delivered in version 8.4.0.14476. If the WebAccess is still in use, it must now be replaced by the WebClient.

New

- A new user right “Can share personal passwords” has been added. If the user right is deactivated, it is not possible to authorize other users or roles on personal passwords.
- A new system task “Disaster WebViewer export” has been implemented. A new user right for the task is also added.
- A new user right to put out the deleted organisational units permanently has been added.
- The database logbook can now be transferred to the Syslog server.
- Additional responsible users for Active Directory profiles can now be set in Master Key mode. The additional responsible users can synchronize the Active Directory profile.
- It is now possible to create new tags when creating and editing passwords at the WebClient.
- Further user rights and settings are now taken into account at the WebClient.
- The autologin can now also be used for Active Directory users in Master Key mode.
- Sealed passwords are now symbolized in Reports of the type ‘All passwords’.
- The multiple editing of permissions can now be used at the WebClient.

- A new (password) setting “Exact domain check” to configure if passwords with the same domain in the URL will be displayed in the addons has been added.
- The sealing functions are now available at the WebClient.
- New settings to display or hide each tab in the footer have been added.
- User rights and user settings can now be configured at the WebClient.
- Password settings can now be opened and configured at the WebClient.
- Password masking can now be set and removed at the WebClient.
- A new user right “Can edit filter” has been added.
- Load time is now displayed at the WebClient.
- New module Discovery Service is now available.
- Users can now change their password at the WebClient.
- Database and user name can now be passed via URL parameters at the WebClient.
- The images of the last users who changed the password are now displayed in the footer at the WebClient.
- Notifications can now be configured at the WebClient.
- Connected applications can now be managed at the WebClient.
- External links can now be generated at the WebClient.
- JavaScript and C # API are now available.
- Logbook entries, notifications, session recordings and historical documents can now be cleaned up automatically via the AdminClient (by using the database administrator).
- The simple mode for migration is now available. This can be selected after creating a new Database. In this mode all folders are automatically created as organisational units.
- The password history is now available at the WebClient.

Improvements

- Interval configuration in the backup wizard will now be displayed correctly.
- The capture of SSO applications and the automatic entry have been revised.
- In Active Directory profiles it is now possible to configure additional responsible users or roles. That allows other users and roles to synchronize with the Active Directory profile.
- The search when using negated filters has been improved.
- The quick search in OfflineClient when using the Shortcut “CTRL+Q” has been improved.
- The automatic entry can now also be used in RDP sessions in Password Safe. This requires a delay for about 500 ms (depends on the system) before actions in the script.
- Adaptations were made to the system task “WebViewer export”, so password configuration is no longer needed.
- Issuing errors when creating users and organisational units are now more detailed. If errors occure due to invalid settings or rights during creation, the user or the organisational unit is created without the invalid configuration.
- At the AdminClient the backup type can now be selected via a combo box (previously checkbox) for backup profiles.
- Log entries are now created when printing objects and using (SSO) applications.
- The progress bar and error output at the WebClient has been improved.

- The transfer of data from the clipboard for new passwords has been improved. Fields can now be copied, modified and be used when creating a new password. Copied fields from version 7 can now be used when creating new passwords in version 8.
- The SSO Terminal service now generates logs in the Event log if the system is not a terminal server.
- The configuration of columns (groups) is now saved.
- The behaviour of the BaseConfig if an error appears has been improved. In addition, a more meaningful error message is now displayed for SQL Server login problems.
- Naming of categories in log forwarding at the AdminClient has been improved.
- Further adjustments were made to the seal.
- Depending on the module, different filter groups are now available.
- The horizontal scroll bar and the display in the organisational structure module have been improved.
- It is now possible to use proxy when using authentication via Yubico (YubiKey).
- When overwriting the permissions are now completely renewed (previously the executing user had to be retained in the permissions).
- The membership can now also be set if the own user has rights via “Everyone” on other users.
- The footer in the Client is now refreshed after “Reload all data” (CTRL + F5).
- The text for opening a WebViewer file in the notification module has been adapted.
- The appearance of forwarded Emails of WebViewer files has been adapted.
- The manually creating of reports is now using the progress bar.
- The performance when loading and displaying organisational units at the WebClient has been improved.
- Several adjustments were made when activating a license.
- When using ‘Change form’, the values can now be transferred between the fields ‘Host name’ and ‘Text’.
- The layout of the WebClient has been improved for mobile devices.

Changes

- Only user rights which are activated for the own user can be set/activated. Database administrators can still set all user rights.
- When applying seals, the creator has to be authorized to issue release.
- The manual WebViewer export via the backstage now uses the new WebViewer.
- It is now possible to set users and roles as “sealed for” and “authorized to release issue”. Users and roles who both have a status can accept requests from others but have to request the seal release themselves.
- The Internet Explorer Compatibility View is now automatically disabled for the WebClient.
- The WebAccess has been removed completely.
- During KeePass import, folders with the same name are now created multiple times as an organisational unit.
- The user setting “Use permissions from organisational units for passwords” has been increased to security level 5 for new databases.

- The SSL certificate for the WebClient is now automatically installed. The button to install the SSL certificate manually has been removed.
- The right ‘delete’ is now required to delete users, organisational units or roles permanently.
- For technical reasons, Master Key users can now only execute the WebViewer export with a self-defined password.

Fixed

- A crash when connecting an application with a password has been fixed.
- Differential backups will be written into the same file as the matching full backup.
- A bug when using automatic entry via shortcuts and multiple tabs with passwords has been fixed.
- When changing the form of passwords, the permissions of the password fields are applied.
- A bug during login to the WebClient if certain special characters are used in the password has been fixed.
- The password generator is now hidden if the password is sealed for the current user.
- A bug in the field assignment has been fixed if there are empty fields when importing CSV and KeePass files.
- An incorrect plausibility check on AdminClient when changing the port of the Web Server configuration has been fixed.
- The configuration of the number of password policy categories at the AdminClient is now saved correctly.
- At the AdminClient the first backup profile is now visible after the creation.
- The buttons to edit and delete a form field are greyed out at the WebClient if the setting “Apply form changes to passwords” is activated.
- A bug that it was not possible to save rights templates in the permissions has been fixed.
- A bug that no category could be selected at the AdminClient when configuring log forwarding has been fixed.
- An error when setting memberships if the user only has permissions on the target user via a role has been fixed.
- The password quality indicator now scales correctly at the WebClient.
- A bug that the filter negation could not be set correctly when configuring reports has been fixed.
- A bug when saving the expiration date for new documents has been fixed.
- Several bugs when comparing passwords in the history have been fixed.
- A bug that it was not possible to save a date with special values has been fixed.
- Vowel mutations are now recognized as lowercase and uppercase letters during the policy check.
- It is not possible anymore to restore the document history if the document history is deactivated in the setting.
- A bug at the AdminClient that, after saving the base configuration again, incorrect SQL user credentials were transferred has been fixed.
- The horizontal scrollbar in the organisational structure module now works even with nested structures.
- Linked documents can now be opened by clicking on the URL field with UNC (network) path information.

- The document history button is now hidden if the setting is disabled.
- A bug that an incorrect static text was displayed on logbook entries of reports has been fixed.
- Several bugs in the addons have been fixed.
- A bug that it was not possible to delete passwords has been fixed.
- It is now possible that the offline license can be activated via the wizard at the AdminClient.
- Further adjustments were made to the layout of the Metropolis Themes.
- An issue that it was not possible to reveal passwords after inheritance has been fixed.
- A bug that ‘Everyone’ received all rights after performing Active Directory synchronization through system tasks has been fixed.
- An issue that saving passwords (with a URL field) took longer if the SSO Agent is active has been fixed.
- The password policy now checks for the correct plausibility at the AdminClient.
- Several bugs when using Yubico authentication have been fixed.
- Several bugs during import (CSV, KeePass) of passwords have been fixed.
- A bug that tags were not set when using predefined rights has been fixed.
- A bug that system tasks were executed twice in a particular constellation has been fixed.
- A bug when importing organisational structures has been fixed.
- Widgets with lists now display the correct headings.
- Several bugs when exporting and importing CSV files have been fixed.
- Several bugs in module ‘Documents’ have been fixed.

Version 8.3.0.14422 Hotfix 1

! In the older versions, there were bugs, which may lead to problems when uncovering passwords. These have been fixed in the current version 8.3.0.14422 Hotfix 1. If an older version is used, it is urgently recommended to install this hotfix. Thus, it can be ensured that the problems no longer occur in the future.

Release

04-16-2018

Compatibility

The following client versions are compatible with AdminClient version 8.3.0.14422 Hotfix 1:

- Version 8.2.0.12343
- Version 8.2.12388 Hotfix 1
- Version 8.3.0.13378

Improvement

- Made adjustments when overriding permissions. The performing user can now be removed when overwriting.

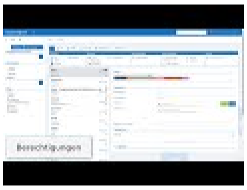
Fixed

- Improved security when using the WebClient. All Webservice-Endpoints gives back “false” in the “Access-Control-Allow-Credentials”-Header.The CORS settings have been corrected. The ability to configure multiple servers will come with version 8.4.0
- XSS vulnerability in created reports has been fixed.
- Fixed a bug on the WebClient where passwords could not be uncovered after using inheritance from organizational units.
- Fixed a bug where the membership could not be set for other users.
- Fixed a bug where passwords could not be revealed in certain constellations.
- Fixed a bug where passwords could not be revealed after moving.

Version 8.3.0.13378

Release

11-29-2017



Compatibility

The following client versions are compatible with AdminClient version 8.3.0.13378:

- Version 8.2.0.12343
- Version 8.2.0.12388 Hotfix 1

> ✻ If you intend to use offline mode, it is imperative that version 8.3.0.13378 of the client is used.

WebAccess is replaced in version 8.3.0.13378 by the new WebClient.

New

- The WebClient is now available and can be set up via the AdminClient.
- For system tasks, the server on which the system task should run can now be selected.
- If “session recording” is activated, a notification asking for confirmation is displayed when connecting to an RDP or SSH application. A logbook entry is created if the notification is confirmed.
- In the case of changes to permissions for an organisational unit, it is now possible to specify that the changed permissions are also applied to passwords. A new setting has been added for this purpose.
- A new setting has been added on the client to set the validity of sessions.
- Password Reset can now be set up for Linux.
- Notifications can now be configured for specific users or roles.
- Roles can be completely deleted and restored again.

Improvement

- The last synchronisation is now displayed for Active Directory profiles.

- The behaviour of the system when creating and managing tags has been improved.
- Automatically added filter elements (e.g. for quick search) can now always be removed.
- The search function in the Google Chrome and Mozilla addons has been improved for when searching for the precise name of a record.
- The update check now takes account of the proxy settings for the server.
- In the backup history on the AdminClient, it is now possible to filter based on the date.
- Multiple amendments have been made to the progress bar system.
- The client has been given its own screen keyboard.
- It is now possible to filter based on the date in backup logs on the AdminClient.
- The screen keyboard can now be opened on the SSO agent via “Ctrl+Shift+K”.
- The validation of the field type “Hostname” has been adapted.
- Masking is now displayed in the password preview.
- The behaviour of the offline synchronisation for new records when an error occurs has been amended.
- The synchronisation of Active Directory objects in Masterkey mode has been improved.
- The performance of the system when displaying memberships in the preview has been improved.
- The header area now shows whether a notification has been configured for other users.
- The keyboard shortcut “F12” can be used to reveal and hide passwords.
- The behaviour of the system when using an empty quick search has been amended.
- A checkbox has been added to the settings for document extensions to enable documents without extensions.
- Permitted document extensions are no longer case sensitive.

Changes

- Crash reports are now saved in AppData.
- When setting up multifactor authorisation, the “write” right is now checked for the current user and the “permissions” right is checked for other users.
- Server certificates are now encrypted using SHA-512.
- It is now possible for a user to remove their own “owner right” when no authorise right is held.

Fixed

- An error where it was not possible to log into multiple databases on the SSO agent has been fixed.
- Error when switching to the active instance has been fixed.
- The user right “Can edit members when using a rights template” is now taken into account in the organisational units wizard.
- Incorrect view when reducing the permissions for “all” has been fixed.
- Deleted fields can now be restored via the history.
- An error during a HTML WebViewer export for the columns user name, password and URL has been fixed.
- An error where deleted members of roles were added during the Active Directory synchronisation has been fixed.

- The historical comparison now also works when there is only one historical entry.
- The entry of date values has been corrected.
- Missing files have been added to the AdminClient so that backups on separate Password Safe and SQL servers can be created and restored again.
- Users can now log into the offline client with a combination of domain and user name.
- An error with sealed passwords where users were granted permissions via roles has been fixed.
- A timing problem during automatic entry where incorrect data could be entered has been fixed.
- An error where users could not reveal sealed passwords via roles has been fixed.
- It is now no longer possible to edit rights while the permissions are being saved.
- An error when applying masking where the rights key could be removed has been fixed.
- The client session is now properly disconnected when the operating system is shut down.
- An error when using “Membership” in the permissions for users has been fixed.
- When opening a URL via the password list, the browser configured in the password settings will now be taken into account.
- A crash when the server is switched off and an automatic login has been configured on the SSO agent has been fixed.
- An error when checking the password where the setting “Number of categories from which characters must be used” has been set to “All” in the rules has been fixed.
- Rights templates will now be applied to imported organisational units during the Keepass import.
- The date format for the password list has been corrected for when the client is being used in English.
- A memory leak on the server has been fixed.
- An error message when adding new users and the password does not comply with the standard rules is now displayed correctly.
- Password options for the current user are loaded when they have not been directly configured for the password.
- Settings for the keyboard shortcut are being correctly taken into account.
- AdminClient displays all licensed settings when AdminClient is opened for the first time.
- An error when using a standard rights template where the template was not correctly selected has been fixed.

Version 8.2.0.12388 Hotfix 1

Release

08-17-2018

Compatibility

The following client and WebAccess versions are compatible with AdminClient version 8.2.0.12388:

- Version 8.2.0.12343

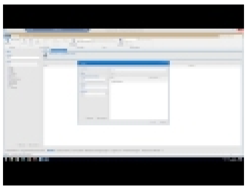
Fixed

- An error when using “Membership” in the permissions for roles has been fixed.
- The missing user right “Can print” was added.

Version 8.2.0.12343

Release

08-09-2017



Compatible client and WebAccess versions

This version is unfortunately not backwards compatible. Therefore, a simultaneous update of the AdminClient, all clients and WebAccess is absolutely necessary.

New

- Switching between the filter and structure is now possible.
- Applications can now be exported.
- New setting added to hide deleted users or roles in the permissions.
- Folders selected as tags will now be migrated as tag templates during the migration.
- It is now possible to filter based on members of a role in the add dialogue for permissions.
- Changes to a form can now be applied to existing data via a setting.
- New user rights for adding seals, adding password masking and managing form fields for passwords have been added.
- It can now be defined in the migration that folder names are adopted in the description of the record.
- Installation parameters for the client setup can now be transferred. This enables the Internet Explorer extension and the automatic startup for the SSO agent to be deactivated.
- Function menus have been added via which certain action can be carried out on form fields.
- New field type “Hostname” added. If no IP address or hostname is saved for an application, the field type “Hostname” from the password is now used for establishing the connection.
- It is now possible to deactivate the SSO agent and the offline client in the setup.
- The automatic offline synchronization can now be deactivated via a setting. In addition, a further setting has been added with which a synchronization can be defined.
- A new setting can now be used to define which document extensions (file endings) are permitted.
- If the connection to the server is not trusted, the SSL certificate for the server can now be opened and imported during the login process.
- A new filter group now makes it possible to filter objects according to whether they contain a tag or not.
- A status bar is now displayed on the client if an older version is being operated than the server.

- It is now possible to restart services via the AdminClient.
- Passwords, documents and roles can now be printed out. The “print” right is checked during this process.
- The window caption for the application can now be configured using various parameters (e.g. Version, Edition).
- A new filter group for rights templates has been added.
- New user rights added to completely delete users or organisational units.
- A rights filter can now be generated in permissions view.
- A new filter group for records with password masking has been added.
- Settings such as autofill, autosubmit or the default browser can now be configured for a password.
- It is now possible when moving records to apply predefined rights or rights inheritance.
- The document folder from version 7 can now be added as an organisational unit during the migration.

Improvement

- Significant improvement in performance for tabs (opening, loading, closing)
- The gallery for the clipboard can now be configured in the settings.
- Multiple improvements made to the user interface for the client.
- Improvements made to the synchronization in offline mode.
- The “Export”- right is now being correctly observed for all types of exports.
- Tag templates are now also being observed for KeepAss and CSV imports.
- Sorting in the organisational structure has been revised.
- User passwords can now be reset in list view also using multiple selections via the ribbon or a right mouse click.
- Larger reports are now concluded quicker.
- When importing users via an Active Directory import, the user’s add right is now checked.
- In Active Directory profiles, alternative domain names can now be defined.
- Adding and deleting a multifactor authentication is now logged (logbook).
- The owner right can now no longer be granted to “all”.
- The setup shortcuts now remain in place after an update and are only removed after a deinstallation.
- When exporting passwords, the only time password fields are not exported is when the password is sealed or masked.
- Objects imported from Active directory in Master Key mode can now be moved and users can be applied with restrictions.
- Members can now be set using multiple selections.
- Active Directory profiles that are still linked to deleted Active Directory objects can now no longer be deleted.
- Improvement to the client performance implemented.
- Search folders are now also displayed during the migration. These are deactivated by default.
- During the migration, only fields with the names “Host”, “Hostname”, “Computer” and Computername” with field type “Hostname” are migrated.

- The error messages for the migration have been improved in certain cases.
- Sealed records are now also exported for the WebViewer if the user has the permissions to view the password.
- In the event of a migration error, only the path where the corresponding log was saved can be directly opened.
- The progress bar for the saving of permissions has been improved.
- The document folder is now saved hierarchically as a tag during the migration.
- All clients now display a splash screen on startup.
- Notifications are now created for issued seal releases.
- A Gateway server can now be configured for RDP applications.
- Notifications can now also be configured using multiple selections.
- Existing tags can now be attached for CSV and KeePass imports.
- Entry using key combinations in the password list has been improved.
- A note now appears when saving permissions if they are inherited or overwritten.
- Some protective mechanisms have been added so that the server key can no longer be deleted.
- MARS (Multiple Active Result Sets) can now be configured on the AdminClient for each database.

Changes

- The “write” right is now required to configure notifications for other users.
- If the setting “Automatically use last filter” has been deactivated, list view will now be loaded without results for the module.
- If a field is saved as an organisational unit in the assignment for CSV or KeePass imports, a new organisational unit is now created and the password is assigned to it.
- When importing Active Directory users in end-to-end mode, the initial user password is now sent by email as long as the user has saved an email address and a SMT server has been configured.
- Certificates generated by the basic configuration are now valid until 31.12.9999.
- The “autofill” and “autosubmit” options for the browser add-on are now configured in the settings for the client.
- The last status for “inheritance” and “overwriting” is now no longer saved. “Inheritance” is now activated by default for passwords and forms and can only be deactivated with the corresponding user right. Both functions are now always displayed for organisational units.
- Permissions for local or Active Directory organisational units are now only inherited by organisational units of the same type. Whether the system is dealing with local organisational units or the same Active Directory profile is now checked.

Fixed

- An error during the reimport of Active Directory objects has been fixed.
- An error where a script is used to enter sealed passwords has been fixed.
- The correct text for a login via the API is now displayed in the session list.
- Nested group memberships are now correctly disbanded during the migration.
- Incorrect behaviour when using the setting “Close tab after discarding” has been fixed.

- A crash when scrolling through the password list has been fixed.
- An error in scaling and full screen mode for RDP applications has been fixed.
- An error in the history of migrated records has been fixed.
- An error in the migration of passwords with a &”-character in a field caption has been fixed.
- An error when moving passwords to the registered user has been fixed.
- An error where databases with a minus in the name could not be integrated has been fixed.
- An error in the WebViewer export, in which the remaining content of the field after certain characters (e.g. “<”) was not exported, has been fixed.
- An error when starting the Firefox add-on when the agent started after the browser has been fixed.
- An error with URLs with more than 12,000 characters has been fixed.
- When the windows DPI settings are amended, the user interface for the Internet Explorer add-on is no longer incorrectly displayed.
- All field types such as e.g. date and list are now correctly exported in the password export.

Version 8.1.1.11211 Hotfix 1

Release

05-19-2017

Fixed

- The inheritance of rights templates (predefining rights) is now no longer associated with the user.

Version 8.1.1.11106

Release

05-08-2017

New

- A new user right for managing session records has been added.
- It is now possible to deactivate the switching of views when adjusting the width.
- A visual indication now shows when the term of validity for objects will soon be reached or has been exceeded.
- Offline databases can now be deleted.
- Configured rights templates are now visually displayed in the organisational structure module.
- A new user right for managing Active Directory profiles has been added.
- Rights templates (predefining rights) are now inherited by underlying organisational units.

Improvement

- Roles can now be sorted and grouped according to the Active Directory domain and date of validity.
- User passwords can now be reset in list view.
- Websites without “https://” can now be opened via the gallery.
- Multiple rights templates can now be deleted simultaneously.
- RDP and SSH windows are now not forced into the foreground and are displayed on the task bar.
- The “add”- right can now also be configured in the organisational unit wizard.
- Delays can now be learnt when creating SSO applications.
- When creating and deleting seals in password editing view, the view is now immediately updated.
- Functions in the ribbon for users are now only displayed if the user possesses the required permissions.
- The AdminClient is now restarted if the service address in the basic configuration is changed.
- The character limit for URL fields has been expanded.
- Amendment to the error message when the client version is outdated.
- An amendment to the behaviour when scrolling in the password list has been implemented.
- All seal actions are now logged and displayed in the logbook.
- Logbook filtering is now also possible without a defined user. If no user has been defined, the logbook entries can be loaded by all users.

Fixed

- A crash when removing “all” from the permissions has been fixed.
- A sporadic crash when using the quick search has been fixed.
- An error where a user creating new users was not given the correct permissions has been fixed.

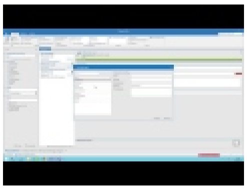
- For an Active Directory import and synchronization, the add right is now transferred to the responsible user for the profile.
- The SMTP configuration can now also be saved when the user name and password are empty.
- An error with documents when rights templates or inheritance were being used has been fixed.
- An error when using SLDAP, where it was not possible for Master Key user to login, has been fixed.
- Crashes that caused the server connection to be lost have been fixed.
- The proxy is now being correctly loaded from the database and shown on the user interface for the AdminClient

Version 8.1.0.10812

Release

04-04-2017

> ! IMPORTANT: In order for passwords to be stored in organisational units, it is imperative to give all roles and authorized users the new “add” right to the respective organisational units after the update. Only then is it possible to record new passwords.



New

- Standard values can now be defined in forms.
- A new setting has been added to configure the number of objects to be displayed in the module lists.
- A database icon will now be shown during selection of the profile, registry databases are now recognisable based on the icon.
- Session recording is now available.
- New right has been added to organisational units. It determines which users can add passwords for this organisational unit.
- A database firewall can now be configured on the AdminClient.
- A new user right has been added to prevent private passwords.
- Memberships will now be displayed by users and roles.
- It is now possible to filter according to deactivated or expired objects using a new filter group.
- It is now possible to deactivate licences on the AdminClient.
- Changes to permissions will now be logged in the logbook.
- Documents can now be exported.
- A server or IP address can now be added when establishing a connection to RDP or SSH applications if there are no data available in the application.
- A new user right has been added to create tags.
- Connection information about the database will now be displayed by moving the mouse over the database names.
- It is now possible to switch to offline or online mode via the backstage.
- A new setting has been added for inheriting permissions.
- A new setting has been added for using offline mode.

- Passwords can now be exported into a CSV file.

Improvement

- A clear error message is now displayed when a full backup could not be found.
- When logging on to certain SSO Applications, you now have an option not to be asked which data should be used.
- The SSO agent now no longer needs to be restarted if the port is changed.
- Performance improvement when navigating in the form selection function.
- To prevent the use of incorrect data, cached data is now deleted when the migration is started.
- Application links in the password list are now sorted alphabetically.
- Newly added members for a role are now taken into account in the Active Directory synchronization.
- A progress bar is now shown when duplicating data.
- The SSO agent will now be automatically updated when a password is linked to an application.
- The description of an active directory group will now also be synchronised.
- The migration of documents is now possible.
- Active directory objects that are explicitly excluded from the import in Password Safe will now be taken into account by the migration.
- The session count has been corrected.
- Various modifications to the counting and checking of sessions have been completed.
- The V7 administrator is now given full permissions for all applications and roles during the migration
- The loading time and the number of initially loaded objects will now be displayed in all views.
- Text that is not completely shown can now be displayed in more sections by moving the mouse over the text.
- The elements to be excluded are now taken into account in the active directory summary page.
- The SSO agent now displays a notification when the port is already occupied.
- The identification of the login button has been extended in the SSO agent.
- If texts are not shown completely in the document list, they can now be displayed by moving the mouse over the text.
- The sequence of the columns in the ribbon has been modified in all modules.
- In the Active Directory assistant, it can now be configured whether the synchronization should be run after import.
- Modifications to the interval layout in the AdminClient were carried out.
- The initials from the active directory will now be adopted.
- In editing mode, the focus is now placed on the first text field.
- The type “computer” will now also be displayed in the active directory assistant.
- If Active Directory object types are invalid, a meaningful error message will now be displayed.
- An incorrect warning when initialising the Active Directory wizard has been removed.
- When setting a new profile in WebAccess, the focus will be placed on the first field.
- A standard value can now be predefined for form fields.
- A progress bar is now displayed when adding multiple tags.

- Modifications to the configuration of an SMTP server have been carried out.
- Modification to the layout for seals and seal templates carried out.
- The permissions for the database administrator have been updated.
- If there is no permissions template, the permissions for the assigned organisational structure will now be inherited if the corresponding setting has been activated.
- A button to open the help function has been added during login to the AdminClient.
- Newly added forms and password fields now contain the permissions for the associated forms and passwords.
- In the user and organisational unit assistant, the setting for the inheritance of permissions will now be taken into account.
- Standard rules can now be removed.
- Modifications to the process for resetting the password for a user have been carried out.
- The size of the window for the SSO agent can now be adjusted.
- Optimisations have been implemented for faster application start-up.
- General improvements to performance carried out.
- Checking a rule for passwords can now be optionally set.
- Notifications are now marked as read if they have been opened via a seal or permission request notification.
- Permission templates can now be removed.
- The user image will now also be synchronised in the end-to-end mode for existing users.
- A new function and setting has been added via which a user is removed from the permissions if he/she adds an object.
- A window caption is now displayed for all quick views.
- The page structure for WebAccess has been improved.
- A response is now received in WebAccess if no right for the password module is held.
- When changing a password in hidden mode, the focus is now placed on the first field as standard.
- Active directory LDAP filter for import and synchronization has been modified so that a filter can be run without a “domain object” as the root element.
- Modifications carried out to the preview for the LDAP filter in the active directory profile.
- Modifications to the error message in the client if the Yubico interface has not been correctly configured.
- If the user has no permissions for offline mode, import or export, the corresponding functions will be greyed out.
- If a seal is broken, all users who have release rights to the password receive a notification.
- A screen keyboard can now be used for login to the database.
- Memberships are now displayed in the user preview and the quick view.
- In WebAccess, a correct message is now displayed if an attempt is made to edit a password that has been deleted on the client.
- The licence settings on the proxy server have been modified on the AdminClient.
- Performance has been optimised for the browser add-ons for Google Chrome and Mozilla Firefox.
- Modifications have been carried out for when a password does not contain a description.
- Automatic login to Google has been modified.

- The setting “Member” can now be entered in the permissions for a user.
- The text for the SSO agent and the browser add-ons has been modified.
- Seal notifications and permission requests can now be viewed under notifications.
- The time has been removed from the list view for passwords.
- The display of the progress bar has been modified.
- WebAccess when displaying long user names has been modified.
- The behaviour of the AdminClient when selecting a database that no longer exists on the server side has been modified.
- The definition of the date for temporary notifications has been modified.
- The form selection function is no longer displayed if the user only has access to a form.
- How the duration of a migration is displayed has been modified.
- The file containing information on the completed migration is now saved in the correct language, and the path where this file has been saved can be directly opened.
- A note is now displayed on the SQL browser service for an external instance in the basic configuration.
- The domain in the column editor can now be displayed for roles from the Active Directory.
- “Strg + C” in the passwords section now opens a dialogue for copying the fields.
- The behaviour of the “Visible for everyone” function has been reworked when predefining rights.
- Performance when logging in and out has been slightly improved.
- A rule for password fields can now be selected on the offline client.
- Improvements to the recognition of the current session on the AdminClient have been carried out.
- The permission template can now be renamed when predefining rights.
- Adaptation of the text when the license or software maintenance expires.
- If errors occur when deleting objects, a meaningful error message will now be displayed.
- When you click on the stored email address for users, the default email program opens.
- The responsible user can now be switched to an Active Directory profile in master key mode.
- User settings that require a higher level of security are now dimmed.
- Several customizations were made to the Active Directory import and synchronization.

Fixed

- An error when using umlauts in usernames or passwords to login to WebAccess has been fixed.
- An error when importing multiple nested active directory structures has been fixed.
- An error on the SSO agent where only the data for the first database could be unencrypted if there were multiple nested databases has been fixed.
- An error where too many active directory elements were synchronised has been fixed.
- An error during the migration of active directory roles where the migration was not completed in masterkey mode has been fixed.
- A system crash during migration when active directory profiles could not be migrated due to the version of the edition being too old has been fixed.
- The client now works again in a Citrix environment.
- The password field is now no longer emptied when edited in hidden mode.

- Inheritance of nested active directory group constructions is now correctly applied for the active directory import.
- Users below active directory groups are now correctly taken into account during the synchronization.
- A system crash when opening the backstage using a keyboard shortcut has been fixed.
- Changes in offline mode will now be correctly synchronised again.
- Objects deleted in the Active Directory will now also be removed during the synchronization.
- Field names for the field type “Heading” can now be edited again.
- An error when distributing database profiles via the registry has been fixed.
- It is now once again possible to delete password rules that were connected to deleted password fields.
- An error during the migration where it took over an hour to complete has been fixed.
- Data for an interval are now not discarded for changes to the configuration.
- Restoring a historical password now works again.
- Documents can now be migrated.
- The function for starting an application minimised works correctly again.
- Favourites are no longer shown in the ribbon if there are no search results.
- Switching to the active instance now also works if the client has been minimised.
- An error where the first session of an SSO agent was not correctly removed when it was ended has been fixed.
- Multiple errors dealing with external links have been fixed.
- An error where the server crashed when logging in and out too quickly has been fixed.
- An error when using Password Safe under Citrix has been fixed.
- The “move” right is now only checked in edit view when the organisational unit has been changed.
- The instance query now only appears when opening the first client on terminal servers.
- Labels are correctly linked with passwords again for the migration.
- Values that do not pass the plausibility check now won’t be generated for the multifactor authentication.
- Restoring a differential backup is now also possible if the associated full backup is not contained in the same file.
- The current time will now be used on the AdminClient for new backup profiles.
- Database profiles from the registry are no longer saved in the configuration file and an error when distributing the profile via the registry has been fixed.
- A system crash when opening a user that was caused by permanently pressing the mouse buttons during the loading process has been fixed.
- An error when displaying a system task after updating has been fixed.
- An error where passwords could not be revealed if users were migrated masterkey users has been fixed.
- A form change with fields that require a reason is now possible.
- An error during the use of the password rule on the AdminClient has been fixed.
- A system crash in the AdminClient during migration when a file was accessed that was being used by another process has been fixed.

- A problem when two active directory synchronizations were carried out on a database at the same time has been fixed.
- A system crash when opening the database assistant if no connection to the server existed has been fixed.
- An error when the user data for a client was invalid has been fixed.
- The information about whether an object should be synchronised is now retained even after an active directory synchronization.
- If a session contains incorrect user data, the user is now logged out.
- No error is now triggered by repeatedly opening a password too quickly in WebAccess.
- When distributing a WebAccess profile, the session no longer automatically expires.
- An error where the active directory summary did not display any allocated names has been fixed.
- If deleting multiple password resets, there is no longer any incorrect loading behaviour.
- An error in WebAccess when using a permission template with users that have no “read” rights has been fixed.
- WebAccess has been modified for when attempting to save a password without the required permissions.
- An error when switching profiles in the active directory assistant has been fixed.
- The password strength is now visible in list view.
- The version and the status of the server service is now correctly displayed under status on the AdminClient.
- An error where a window was closed following a keyboard entry has been fixed.
- An error where standard rules were not correctly taken into account has been fixed.
- A system crash on the client when the session is severed by the AdminClient has been fixed.
- Objects deleted in the Active Directory will now be removed during the synchronization.
- Deactivated rule checks are now also taken into account during the migration.
- An error where a warning on the AdminClient was closed when opening the help function has been fixed.
- An error during synchronization in end-to-end mode has been fixed.
- An error where no connection to the SSO agent could be established on terminal servers has been fixed.
- An error when setting permissions for form fields during the migration has been fixed.
- If object information from the Active Directory exceeds the maximum character length, it will be correspondingly shortened during import or synchronization.
- Groups are correctly recognised during migration if the last user added in version 7 has been marked as deleted.
- An error during the migration of locked passwords has been fixed.
- Restoring in the password history is now possible with a reason.
- An error when ending RDP applications has been fixed.
- An error where repeated saving prevented the passwords from being revealed has been corrected
- An error on the SSO agent where passwords with masking could be copied when connected with an offline database has been fixed.

- An error on the SSO agent where automatic sign-on did not work when connected to an offline database has been fixed.
- An error where an endless loading display was shown on the dashboard has been fixed.
- An error when setting the focus after using the quick search has been fixed.
- An error where a password could not be displayed correctly after it was saved has been fixed.
- An error where documents could not be opened via external links has been fixed.
- An error where permission templates were not correctly displayed when creating new users or organisational units has been fixed.
- Applications without a name from version 7 will now be correctly migrated.
- The setting for disconnecting the database connection after a certain period of time now works correctly.
- No errors now occur if the password for authentication on the AdminClient has been changed.
- If the use of generated password is defined for a form field, the function for changing the password is now hidden.
- When using a permission template, you can now remove the permissions you have added yourself.
- The time difference to the server is now correctly displayed when initialising the Google authenticator in WebAccess.
- The “Visible for everyone” function is now correctly taken into account on the offline client.
- An error where no users or roles were displayed in a particular configuration in the Seal overview has been fixed.
- If you change a hidden password, a change will be shown in the tab.
- An error during the migration of combined users has been fixed.

Version 8.0.2.9978 Hotfix 2

Release

02-17-2017

Improvement

- Standard rules can now be removed.
- A button to open the help function has been added to the AdminClient.

Fixed

- An error causing system crash when opening the database assistant if no connection to the server existed has been fixed.
- An error when setting permissions for form fields during the migration has been fixed.
- An error during the use of the password rule on the AdminClient has been fixed.
- An error where standard rules were not correctly taken into account has been fixed.
- An error in WebAccess when using a permission template with users that have no “read” rights has been fixed.
- An error where no connection to the SSO agent could be established on terminal servers has been fixed.

Version 8.0.2.9541 Hotfix 1

Release

01-20-2017

Improvement

- To prevent the use of incorrect data, all cached data is now deleted when the migration is started.
- The description of an AD organisational unit will now also be synchronised.
- Various modifications to the counting and checking of sessions have been completed.
- The V7 administrator is now given full permissions for all applications and roles during the migration
- The elements to be excluded are now taken into account in the AD summary page.

Fixed

- An error when importing multiple nested AD structures has been fixed.
- An error where too many AD items were synchronised has been fixed.
- A system crash during migration when Active Directory profiles could not be migrated due to the version of the edition being too old has been fixed.
- Inheritance of nested AD group constructions is now correctly applied for the AD import.
- Users below AD groups are now correctly taken into account during the synchronization.
- An error during the migration of AD roles in end-to-end mode has been fixed.
- Objects deleted in the Active Directory will now also be removed during the synchronization.
- Newly added members for a role are now taken into account in the Active Directory synchronization.
- Active Directory objects that are explicitly excluded from the import in Password Safe will now be taken into account by the migration.
- An error during the migration where it took over an hour to complete has been fixed.
- An error where the first session of a client agent was not correctly removed when it was ended has been fixed.
- An error where the server crashed when logging in and out too quickly has been fixed.
- An error when using Password Safe under Citrix has been fixed.
- The instance query now only appears when opening the first client on terminal servers.
- An error during the migration of data with long values has been fixed.
- Database profiles from the registry are no longer saved in the configuration file and an error when distributing the profile via the registry has been fixed.
- Documents can now be migrated.

Version 8.0.2.9278

Release

12-22-2016

New

- In the multiple editing of rights, rights templates can now be selected.
- Applications can now be started using a function in the ribbon without linking them to a record.
- The layout of the multifactor authentication in the login has been reworked.
- In the case of a password field with no authorizations, rights can now be requested. This triggers a notification for authorized users.
- There are now new user rights for the visibility of individual tabs within the footer.
- Yubico OneTimePassword can now be used as an authenticator.
- If no certificate is found when opening the basic configuration, this is now automatically generated.

Improvement

- The interval description is now also displayed outside the interval configuration.
- Incorrect behaviour of connection locks in the overview has been corrected.
- The URL redirection is now only performed on WebAccess under certain conditions.
- It is now possible to configure dynamic start parameters in SSO applications.
- Environment variables can now be used in the application path of an SSO application.
- The layout of intervals has been modified.
- It is now possible to configure a global syslog server.
- Form fields can now be created as tags during the KeePass import.
- The visualization of the login area in the WebAccess has been adjusted.
- Default password rules can now be configured on the AdminClient.
- A password guideline has been implemented at the AdminClient, which is used to pass passwords within the AdminClient.
- Saving via CTRL + S as well as closing via ESC now works on all clients.
- Password fields, which can only be opened with justification, can now also be found in the WebAccess.
- In the right filter, it is now possible to filter according to eligible members with membership.
- The “Visible for Everyone” option is now applied to Active Directory Import in Master Key mode.
- You can now edit the authorizations of organisational units that have been imported via an Active Directory profile in Master Key mode.
- In the browser add-ons, the URL of the tab is now used to identify passwords.
- Favourites can now be set with multiple selection.
- For Active Directory users imported through an end-to-end profile, the default rights preset of the assigned organisational unit is now applied.

- Revealing password fields with reason is not possible in offline mode.

Fixed

- Sorting by date has been corrected.
- An error when adding a policy in a particular configuration has been fixed.
- An error when forms could not be duplicated has been fixed.
- An error where it was not possible to enter the user name and password at the offline client when logging in has been fixed.
- Changes to permissions will now be displayed in the logbook.
- Fixed an error with Active Directory Import that caused objects to be reactivated incorrectly.
- An error in WebAccess, which prevented the header from displaying after an incorrect entry had been made, has been fixed.
- An error where a new password could not be saved when adding a new memo or URL field via the ribbon has been fixed.
- Various errors related to the Active Directory import have been fixed.
- Errors when entering a reason to reveal a password have been fixed.
- The window of the Internet Explorer add-on no longer opens outside the visible area.
- Errors when signing on, where the SSO agent was connected to multiple databases, have been fixed.
- Records that were sealed after offline synchronization will be removed from the offline database the next time they are synchronized.
- For user authorizations, the membership of a user cannot be changed.
- No error message will be displayed if you select a password, for which you are authorized via a role, in the offline client.
- An error when making manual entries in Internet Explorer has been fixed.

Version 8.0.1.9032

Release

11-28-2016

New

- You can now check for updates.
- The password generator and the gallery customization behave correctly in the OfflineClient.
- A new setting for assigning policies to specific categories has been added to Administration.
- A progress bar is now displayed when deleting objects.
- The login to the database can now be automated.
- If an automatic login has been set up, it is now also used on the client agent.
- In the “Activity View” and “Tag View” widgets, you can now filter by the data number to be displayed.
- New option added to limit the number of items in a widget.
- In the ClientAgent, the browser add-ons can now be installed with a new function.
- New fields can now be added, edited and removed during field mapping during import.
- The license overview now shows the remaining time for the next test as well as the final sequence.
- It is now possible to create profiles with WebAccess via a URL parameter.
- A new user right to override rights has been added.
- It is now possible to configure Syslog on the AdminClient
- Creating external links is now possible.
- It is now possible to configure the permissions of form fields from multiple passwords at the same time.
- Database profiles can now be distributed over the registry.
- License alerts are now displayed in the client’s status bar.

Improvement

- Floating-point fields now display the defined description at the OfflineClient.
- In the database assistant, you can now choose between German and English as the language of the database template.
- The layout of intervals for system tasks has been modified.
- The button for executing an HTML WebViewer export is now grayed out, if the user has no right to the export.
- Passwords can now be processed faster at the OfflineClient.
- Forms without authorization are no longer displayed in the form selection at the OfflineClient.
- Associated passwords of a password reset can now be removed directly after opening a password reset.

- In the browser add-on, the field type “e-mail address” is now used to enter the data if the field type “user name” is not in the password
- The default interval for new system tasks has been set to one hour.
- You will be notified when automatic login fails.
- Performance when loading organisational structures has been improved.
- Insert, Page Up, Page Down, Home, End, and Delete have been added to the configurable scripting shortcuts.
- The name or the client IP is now displayed for locked users.
- Multiple selection has been added as an option for password guidelines.
- The width of the migration window has been adjusted, so that the texts are now written in full.
- Performance improvement performed with Active Directory import.
- The search bar at the OfflineClient can now be displayed by pressing CTRL + F.
- The system language is then used as the standard language at the AdminClient.
- Additional plausibility was introduced for forwarding rules.
- In the case of rights template groups, the set standard of a template can now be removed again.
- OfflineViewer has been renamed to WebViewer.
- Various changes have been made to the synchronization with the OfflineClient.
- You will receive a notification if a Password Safe instance is already open, and you attempt to open another instance.
- Performance enhancement of the Active Directory summary page.
- User settings and user rights for rights templates are now also taken into account at WebAccess.
- For certain configurations, no icon was displayed in the rights templates, even if a configuration existed.
- Restructuring of the categories in the settings was carried out.
- You can now update the views in the ribbon backstage area using CTRL + F5.
- Fixed an error with a particular text qualifier during import.
- When moving passwords, the loading bar is now displayed in the status bar.
- A progress indicator is now displayed for adjustments to the rights.
- The database information on the AdminClient has been adapted.
- It is now saved correctly, if only “Visible for everyone” is configured in the wizard create user.
- Multiple selection has been added as an option for seal templates.
- A request now appears before data is copied from the clipboard when a new password is created.
- Text has been changed.

Fixed

- It has been fixed that the AdminClient is terminated by an error if no default database server is stored.
- Linked SSO applications can now also be used on the OfflineClient.
- An error where it was not possible to save passwords to the WebAccess has been fixed.
- An error where no login screen was displayed in the HTML WebViewer has been fixed.
- An error in the Offline Client when clicking in a tag field has been fixed.

- An error where the passwords could not be created correctly when selecting “overwrite” and “merge” during import.
- Incorrect behaviour when deleting users, organisational units, and roles from Active Directory has been fixed.
- If you attempt to log on to the license server with incorrect data, you will now receive a corresponding feedback.
- Passwords can be shown again in the Offline Client.
- Seal now works correctly also at the form field level.
- You can now restore the gallery in the ribbon to the default settings.
- Other errors during automatic login have been fixed.
- Errors when entering SSO scripts have been fixed.
- Error when no data was displayed with some widgets has been fixed.
- Error when automatically logging on to the client agent has been fixed.
- An error in Windows applications when logging in with specific rights has been fixed.
- The interval has been corrected.
- Several errors related to Active Directory import have been fixed.
- Error when wrong profile was selected in the profile selection has been fixed.
- Field assignment during import has been graphically modified.
- Selection problem for the profiles has also been fixed on the WebAccess.
- An error when selecting Active Directory import has been fixed.
- An error when terminating the client agent on terminal servers has been fixed.
- An error where the client was terminated has been fixed.
- Log forwarding has been adjusted.
- Various errors during the import have been fixed.
- An error where the progress bar gets stuck on the AdminClient has been fixed.
- Database report text have been modified.
- An error when logging in automatically to an unsecured server has been fixed.
- An error when using multi-line text fields has been fixed.
- An error when changing the selection while deleting organisational structures has been fixed.
- The scrollbars in the license settings now behave correctly.
- An error where it was not possible to move objects has been fixed.
- In the case of multiple selection, each right can now be managed individually.
- Minor general adjustments have been made.
- Basic configuration has been renamed to basic configuration.
- Fixed minor issues with Active Directory import.
- An error where the client wasn’t shown has been fixed.
- An error has been fixed which enabled the license to be activated multiple times on the AdminClient.
- It has been fixed that startup parameters could not be saved for SSO applications.
- Fixed a bug that could remove the last user or the last role with a right-only privilege.
- Removing tags is now possible with readability to a data record.
- Fixed an issue that did not allow you to reset the settings in Internet Explorer add-on.

- When overwriting passwords of the same name through the import, the assigned organisational unit is now also updated.
- Databases can now be backed up with differential backup.
- It is now possible to place several full backups into one file.
- Fixed an issue where the start and end date of a temporary permission was not loaded correctly.
- The Active Directory category in the ribbon of the roles list is no longer displayed if the AD Integration is not licensed.
- Fixed an error that could not override the global option to use filter negation.
- The infofield for passwords can now be reconfigured.
- Fixed a bug where the progress indicator stopped when deleting passwords.
- You can now configure at the AdminClient whether to transfer information from the Password Safe service.
- Sealed passwords on the offline client cannot be copied to the clipboard.