Documentation



Password Safe V8

FullClient – WebClient – Server

Topic:
Help

PASSWORD SAFE
by MATESO™
Enterprise Password Management

Table of Contents

Welcome… 6
- Why Password Safe? 8
- What is new in version 8? 9
- Achieving your goal with the right edition 11
  - Licence model 13
  - Feature matrix 15

Security 19
- Used encryption algorithms 21
- External penetration tests 23
- IT security made in Germany 24
- Sicherheitslücken – Ist Password Safe betroffen? 25
  - Log4J 26
  - Spring4Shell 27
  - Robot 28

Getting started 29

Architecture and system requirements 34
- MSSQL System Requirements 37
- Server system requirements 39
- Client system requirements 43
- System requirements for the WebClient 44

Installation 46
- Installation AdminClient 48
- Installation Client 52
  - Installation with parameters 57
- Installation of the WebClient 58
- Installation Browser Addons 69
  - Installation Chrome 72
  - Installation Mozilla Firefox 73
  - Installation Edge 74
  - Installation Safari 75
- Moving the server 76
- Updates 81

Authorization concept and protective mechanisms 84
- Manual setting of permissions 89
  - Using rights templates 94
  - Multiple editing of permissions 95
- Automated setting of permissions 101
  - Inheritance from organisational structures 102
  - Predefining rights 106
    - Working with predefined rights 111

Relevant user rights ... 115
Scope of validity for predefined rights ... 117
Protective mechanisms ... 119
Visibility ... 122
Temporary permissions ... 124
Password masking ... 126
Seals ... 129
Seal overview ... 136
Release mechanism ... 138

Operation and setup ... 141
Ribbon ... 146
Filter ... 149
Display mode ... 153
Advanced filter settings ... 155
List view ... 161
Reading pane ... 166
Tags ... 169
Search ... 171
Print ... 174
Dashboard and widgets ... 180
Keyboard shortcuts ... 185

Client Module ... 186
Passwords ... 189
Creating new passwords ... 193
Revealing passwords ... 197
Moving passwords ... 199
Form field permissions ... 201
Password settings ... 204
History ... 205
Papierkorb ... 209
Documents ... 210
Notifications ... 213
Organisational structure ... 217
Managing users ... 222
User passwords / logging in to client ... 226
Permissions for organisational structures ... 230
Inheriting permissions ... 232
Active Directory link ... 234
End-to-end encryption ... 236
Masterkey mode ... 243
RADIUS authentication ... 251
First factor ... 257
Multifactor authentication ... 262
Yubico / Yubikey ... 266

OTP (One-Time-Password) ... 271
Roles ... 273
Forms ... 276
Change form ... 281
Logbook ... 284
Applications ... 286
Learning the applications ... 292
Start parameters ... 298
RDP und SSH Anwendungen ... 301
Recording a session ... 304
Configuration of SAML ... 308
Beispiele für Anwendungen ... 312
SAP GUI logon ... 313
SAML application for Dropbox ... 315
SAML application for Postman ... 319
Password Reset ... 322
Requirements ... 323
Configuration ... 324
Password Safe scripts ... 327
User-defined scripts ... 332
Heartbeat ... 334
Rollback ... 337
Logbook entries under Password Reset ... 339
Discovery Service ... 340
Requirements ... 341
Configuration ... 343
Discovered entries ... 347
Converting entries ... 352
Created passwords ... 360
Deleting entries ... 362
Logbook ... 364

Main menu ... 366
Import ... 368
Export ... 373
HTML WebViewer export ... 376
Export wizard ... 383
Extras ... 385
Reports ... 387
Relevante Berichte ... 391
Password generator ... 393
System tasks ... 396
Emergency WebViewer ... 400
Password rules ... 408
Seal templates ... 412
Tag manager ... 414

Image management ... 417
Papierkorbverwaltung ... 420
General settings ... 421
User rights ... 422
Overview of all user rights ... 425
User settings ... 430
Overview of all settings ... 434
Administration ... 440
Account ... 442

SSO Agent ... 445
Configuration ... 447

Add-ons ... 451
Applications ... 458
How to save passwords ... 463

The LightClient ... 466
To do for Administration ... 468
Errorcodes of the LightClient ... 470
Checklist of the LightClient ... 472

WebClient ... 473
Functional scope ... 474
Tag system ... 475
Password module ... 476
Organisational structure module ... 478
User management ... 481
Roles module ... 482
Forms module ... 483
Notifications ... 484
Application ... 485
Logbook ... 486
Documents ... 487
Operation ... 488
Filter or structure area ... 491
Header ... 492
Navigation bar ... 493
Menu ... 494
List view ... 496
Reading pane ... 497
Footer ... 498
User menu ... 499
Settings ... 500
Authorization and protection mechanisms ... 504
Problems with the server connection ... 506

Mobile devices ... 507

AdminClient **509**
Basic configuration 510
Enable DualStack IP (IPv4 + IPv6) 514
Certificates 516
Discovery service certificates 520
SSL connection certificates 521
Database certificates 526
Master Key certificates 528
Password Reset certificates 530
Setup wizard 531
Creating databases 536
Settlement right key 539
Database properties 542
Database firewall 544
Syslog 547
Datenbankeinstellungen 548
Multifaktor-Authentifizierung 549
Sitzungs-Timeout 550
Managing databases 551
HSM connection via PKCS # 11 554
Migration 556
Preparations 558
Starting the migration process 560
Assigning tags and OUs 563
Permissions after migration 566
Checklist after migration 567
Operation and setup 571
Main menu 575
General settings 576
Backup settings 577
Backup management 578
Automated deletion of backups 583
Disaster recovery scenarios 584
License settings 587
Advanced settings 589

High availability **590**

Offline Client **591**
Setup and sync 593

How-to's **598**
Changing an SSL connection certificate 599
Automatically receiving the WebViewer via e-mail 601
Copy fields 606
Rights to the record but not to the password field 608
View passwords that may have incorrectly set permissions 609

API ... **610**
Beispiele C# SDK ... 614
Beispiele Javascript SDK ... 624

Version history ... **626**
Version 8.13.14.27679 ... 628
Version 8.13.13.27522 ... 631
Version 8.13.12.27427 ... 633
Version 8.13.11.27156 ... 636
Version 8.13.10.26901 ... 639
Version 8.13.9.26689 ... 642
Version 8.13.8.25983 ... 645
Version 8.13.7.25979 ... 646
Version 8.13.6.25933 ... 648
Version 8.13.5.25731 ... 651
Version 8.13.4.25228 ... 654
Version 8.13.3.25194 ... 656
Version 8.13.2.25151 ... 658
Version 8.13.1.25117 ... 660
Version 8.13.0.25027 ... 662
Version 8.12.1.22757 ... 667
Version 8.12.0.22707 ... 668
Version 8.11.1.19828 Hotfix 1 ... 677
Version 8.11.1.19823 ... 679
Version 8.11.0.19788 ... 681
Version 8.10.0.18473 Hotfix 2 ... 688
Version 8.10.0.18516 Hotfix 1 ... 693
Version 8.10.0.18464 ... 698

Third Party Licenses ... **702**

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]



[redacted]

https://www.youtube.com/embed/vgmfQsgCXBM?rel=0

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.



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

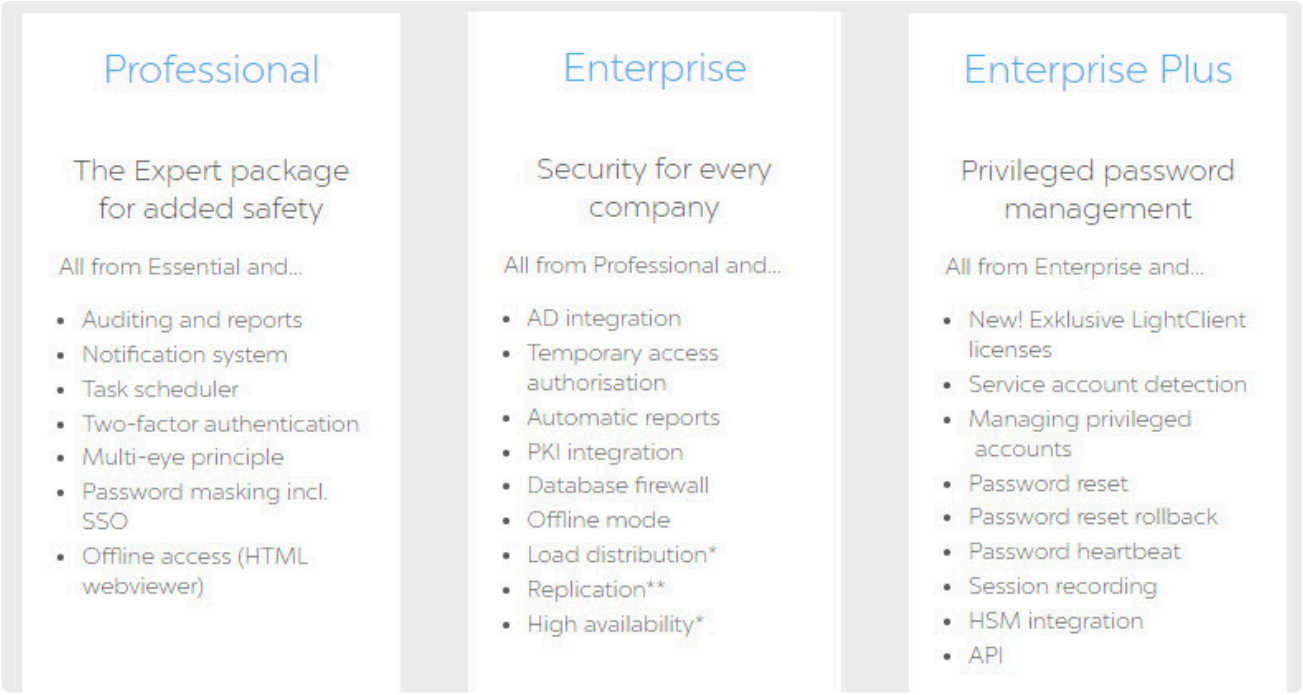
Service accounts and administrative access with far-reaching authorizations are always the key vulnerability points within companies, and have often been a gateway for attackers and manipulations. Maintenance and administration of existing, historical accounts are difficult due to their number. With 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

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**.

Professional

The Professional Edition is designed for small and medium-sized teams. 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. 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 is the licensing done?

Licensing in is based on a **Strict Named User Model**. Therefore, each user receives his or her own license. In addition, the connections from the client to the server are counted. The following general conditions apply:

- It does not matter to what extent Password Safe is used. Each user needs at least his own license.
- One user account can be created per license.
- If the user names are identical, a user account can also be used in several databases. Then only one license is needed.
- The sharing of user accounts is not permitted.
- The use of LightClient licenses are possible in the Enterprise Plus Edition.
- A license is also required for the exclusive use of SSO Agent.
- A maximum of as many simultaneous sessions as there are user licenses can be started on different PCs or terminals. Simultaneous use on different PCs or terminals requires one session each.

License counting

The license count depends on the active sessions. A user can use a maximum of 2 licenses on one computer. The FullClient and/or SSO Agent require one license each. The add-on in server mode runs via WebClient. The add-on in combination with the SSO agent uses the license of the FullClient. If different clients are used at the same time, two licenses may be required.

Example:

Client type		Client type		Used licenses
FullClient	+	SSO Agent	=	**1 License**
FullClient	+	Add-on (SSO Agent)	=	**1 License**
WebClient	+	Add-on (Server Mode)	=	**1 License**
FullClient	+	WebClient	=	**2 Licenses**
FullClient	+	Add-on (Server Mode)	=	**2 Licenses**

If a user logs on to another computer, further sessions are established and additional licenses are used.

Modules from Version 7

In version 7, the licensing per computer could still be adapted using modules (module without client licensing). However, modules are no longer required in version 8: All licensing procedures are covered by the above license model.

If you have any questions about licensing, please contact our **Sales team** .

Feature matrix

The editions at a glance

Security	Essential	Professional	Enterprise	Enterprise Plus
End-to-end encryption (E2EE)	•	•	•	•
Data Versioning (History)	•	•	•	•
Role-based Access Control (RBAC)	•	•	•	•
Password Retrieval by Reason Only	•	•	•	•
Password Generator	•	•	•	•
Protection via Transport Layer Security Connection (TSL)	•	•	•	•
Logbook with Filter Option	•	•	•	•
Registration service on the Internet	•	•	•	•
Functional Header Area	•	•	•	•
Optional Automatic Cleanups	•	•	•	•
Centralized Team Database	•	•	•	•
Audit-proof Logging	•	•	•	•
AES 256 Encryption / PBKDF2	•	•	•	•
RSA for long term Keys	•	•	•	•
Hierarchical Encryption for approvals via roles and users	•	•	•	•
Task System		•	•	•
Multi-Eye Principle (Seal)		•	•	•
Password Masking		•	•	•
Live Notifications		•	•	•
Two-Factor Authentication		•	•	•
Real-Time Updates		•	•	•
PKI Integration			•	•
Database Firewal			•	•
RADIUS Connection			•	•
Offline Access (Emergency Web Viewer 2FA-			•	•

protected)				
Session Recording				•
Productivity	**Essential**	**Professional**	**Enterprise**	**Enterprise Plus**
Platform-independent WebClient	•	•	•	•
Syslog server connection	•	•	•	•
Flexible Rights Templates	•	•	•	•
Password Policies	•	•	•	•
Document History	•	•	•	•
Add-on’s for all browsers	•	•	•	•
Inheritable User Settings and Rights	•	•	•	•
Integrated LightClient	•	•	•	•
Dynamic Dashboards	•	•	•	•
Terminal Server Support	•	•	•	•
Customizable Input Masks	•	•	•	•
App Synchronization	•	•	•	•
Print and Export	•	•	•	•
Clear Footer Area	•	•	•	•
Rights management down to Field Level	•	•	•	•
Production of External Links	•	•	•	•
Barrier-free Operation	•	•	•	•
Dynamic List/Customizable Grids	•	•	•	•
Switchable List View	•	•	•	•
PuTTY Client	•	•	•	•
Quick View	•	•	•	•
Registration and Training of Applications	•	•	•	•
Tabsystem	•	•	•	•
Learning capable search Filters with Full Text Search	•	•	•	•
Remote Access via integrated RDP Client	•	•	•	•
Customizable Info Area	•	•	•	•
Documents	•	•	•	•

Individual settings for Each Password	•	•	•	•
Quick Navigation	•	•	•	•
Organizational Structures	•	•	•	•
High Resolution of Text and Images	•	•	•	•
Tag Function	•	•	•	•
Restrictive Users	•	•	•	•
Intelligent Quick Search	•	•	•	•
Security Levels for Settings	•	•	•	•
Different Color Schemes	•	•	•	•
Auditing and Reports		•	•	•
WebViewer		•	•	•
Temporary Password Releases			•	•
Automatic Active Directory (AD) Synchronization			•	•
Heartbeat for Password Reset				•
Connection to Hardware Security Modules (HSM)				•
Exclusive LightClient Licenses				•
Automation	**Essential**	**Professional**	**Enterprise**	**Enterprise Plus**
Single Sign-on (SSO) Agent	•	•	•	•
Connection Locks	•	•	•	•
MSI Software Distribution	•	•	•	•
Shortcut Keys and Scripting Functionality	•	•	•	•
Integration of Active Directory (AD) with LDAP			•	•
Automatic Reports			•	•
Discovery Service for Service Accounts				•
Password Reset and Password Synchronization				•
Rollback for Password Reset				•
API Interface				•
Managing Privileged Accounts (Privileged Account Management)				•
High Availability	**Essential**	**Professional**	**Enterprise**	**Enterprise**

				Plus
SQL Clustering**	•	•	•	•
Scalability	•	•	•	•
Automatic Live Backups	•	•	•	•
Import of Important Data	•	•	•	•
Responsive WebClient (IIS, Apache, nginx)	•	•	•	•
Offline Access (HTML WebViewer via Browser)		•	•	•
Load Balancing across multiple Application Servers*			•	•
Offline Mode (via client)			•	•
SQL Server Replication (Distributed Locations)**			•	•

- The Essential and Professional plans allow for max. 1 application server; the Enterprise plan allows for max. 2 application servers. Any number of application servers may be used in the Enterprise Plus plan. (You will need to purchase each application server separately)
- External tools are required for the functionality (Microsoft Load Balancer or other load balancers).
- External tools are required for the functionality (Microsoft SQL Server).

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 for private and public key methods

All encryption algorithms used by Password Safe are FIPS compliant.

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

External penetration tests

The high security standards of Password Safe are regularly attested by external pentests of different providers. New functions in particular are always subjected to penetration tests in order to have them thoroughly checked before release. The resulting findings enable us to detect and eliminate potential vulnerabilities in advance.

Why we test regularly

In pentesting, external and certified security auditors look specifically for security gaps and weaknesses in the software that an attacker could exploit. Attack scenarios are simulated on the client side, the source code is checked and the quality of the cryptographic process is assessed. In this way, the security of Password Safe and the data stored in it is tested in advance in order to be able to offer our customers effective protection and minimize the risk of success of an attack.

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.



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

Sicherheitslücken – Ist Password Safe betroffen?

Verschaffe dir hier einen Überblick darüber, inwiefern Password Safe von aktuellen Sicherheitslücken betroffen ist und was du im Ernstfall tun kannst.

- Log4J
- Spring4Shell
- Robot

Log4J

Was ist passiert?

Die Sicherheitslücke in Log4j 2, einer weit verbreiteten Java-Protokollierungsbibliothek, ermöglicht die Ausführung von Remote-Codes, weshalb die Wahrscheinlichkeit hoch ist, dass dieser Angriff zur Übernahme ganzer Systeme genutzt werden kann. Die Lücke wurde auch in Minecraft-Servern entdeckt, über die Befehle in Chat-Protokolle eingegeben werden konnten, die dann an den Logger gesendet wurden. Genau das macht diese Schwachstelle so kritisch, denn die Logging-Bibliothek ist so weit verbreitet, dass sie leicht ausgenutzt werden kann. Aus diesem Grund arbeiten viele Open-Source-Betreuer derzeit an Korrekturen und Updates für unser Software-Ökosystem.

Ist Password Safe betroffen?

Da Password Safe nicht mit Java arbeitet, ist unsere Software nicht von dieser Sicherheitslücke betroffen. Es müssen also keine weiteren Maßnahmen von unseren Kunden ergriffen werden, wenn sie unsere noch unterstützten Versionen (8.10 oder höher) verwenden.

Wir möchten an dieser Stelle anmerken, dass Password Safe noch eine weitere Bibliothek verwendet – Log4js – die für Log4 Java Script steht und nichts mit der Bibliothek Log4j – Log4 Java – zu tun hat. Log4js ist also nicht betroffen und somit nicht sicherheitskritisch.

> Bitte die Software regelmäßig aktualisieren

Wenn eine Version unter 8.10 verwendet wird, empfehlen wir unseren Kunden dringend, so schnell wie möglich auf die neueste Version zu aktualisieren. Wir möchten auch darauf hinweisen, dass der Support für die Version 8.9 im November ausgelaufen ist. Nicht nur aus Gründen des Supports, sondern auch um immer auf dem aktuellen Stand der Sicherheit zu sein, ist ein Update auf die neueste Version dringend zu empfehlen.

Sicherheitsempfehlungen

Wenn Apache verwendet wird, sollten unsere Kunden beachten, dass dieser Server ebenfalls betroffen ist und das Problem bereits behoben wurde. Bitte also auch Apache aktualisieren, um sicher zu sein.

Zum Apache How-To

Auch wenn Password Safe nicht betroffen ist, sollten alle Systeme, die verwendet werden, überprüft werden. Generell empfehlen wir allen unseren Kunden, wenn möglich, eine verstärkte Protokollierung auf den Systemen einzurichten, die nicht anders oder vorübergehend deaktiviert werden können, um mögliche Angriffe zu registrieren.
https://logging.apache.org/log4j/2.x/security.html

Spring4Shell

Wie du wahrscheinlich schon mitbekommen hast, ist die Sicherheitslücke Spring4Shell derzeit in aller Munde. Diese betrifft das Java-Framework Spring, bei der es unter bestimmten Umständen zu RCE (Remote Code Execution) kommen kann.

> ! Password Safe nicht betroffen

Da Password Safe kein Java und somit auch nicht das Java Framework Spring nutzt, ist es davon auch nicht betroffen. Darüber hinaus müssten noch folgende Bedingungen erfüllt sein, damit diese Lücke entsteht:

- JDK9 oder höher
- Apache Tomcat (kein Spring Boot)
- Spring < 5.3.18, < 5.2.20 und alle älteren Versionen
- Dependency zu spring-webmvc oder spring-webflux

All diese Umstände treffen auf Password Safe nicht zu, weshalb wir hier Entwarnung geben können.

Robot

Was ist Robot?

(Return Of Bleichenbacher’s Oracle Threat) ROBOT ist eine Angriffsmöglichkeit auf Kryptografische Verfahren, bei der es unter günstigen Umständen dazu kommen kann, dass ein Angreifer den privaten Schlüssels des Servers berechnen kann und somit signieren und entschlüsseln kann. Somit ist auch die Möglichkeit für MITM-Angriffe gegeben.

Wie kann man sich schützen?

Der Beste Schutz gegen ROBOT ist sämtliche TLS_RSA Algorithmen zu deaktivieren.

Diese Lücke kann mit testssl.sh verifiziert werden.

Gefahr für Password Safe?

Da man nur beim Konfigurieren des Servers darauf achten muss, ist kein Password Safe Update nötig

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



https://www.youtube.com/embed/mWKzPWjlqIY?rel=0

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



https://www.youtube.com/embed/md7_VEdVuWM?rel=0

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



https://www.youtube.com/embed/9Fq_ev7vXhM?rel=0

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



https://www.youtube.com/embed/S79MNckgueM?rel=0

Architecture and system requirements

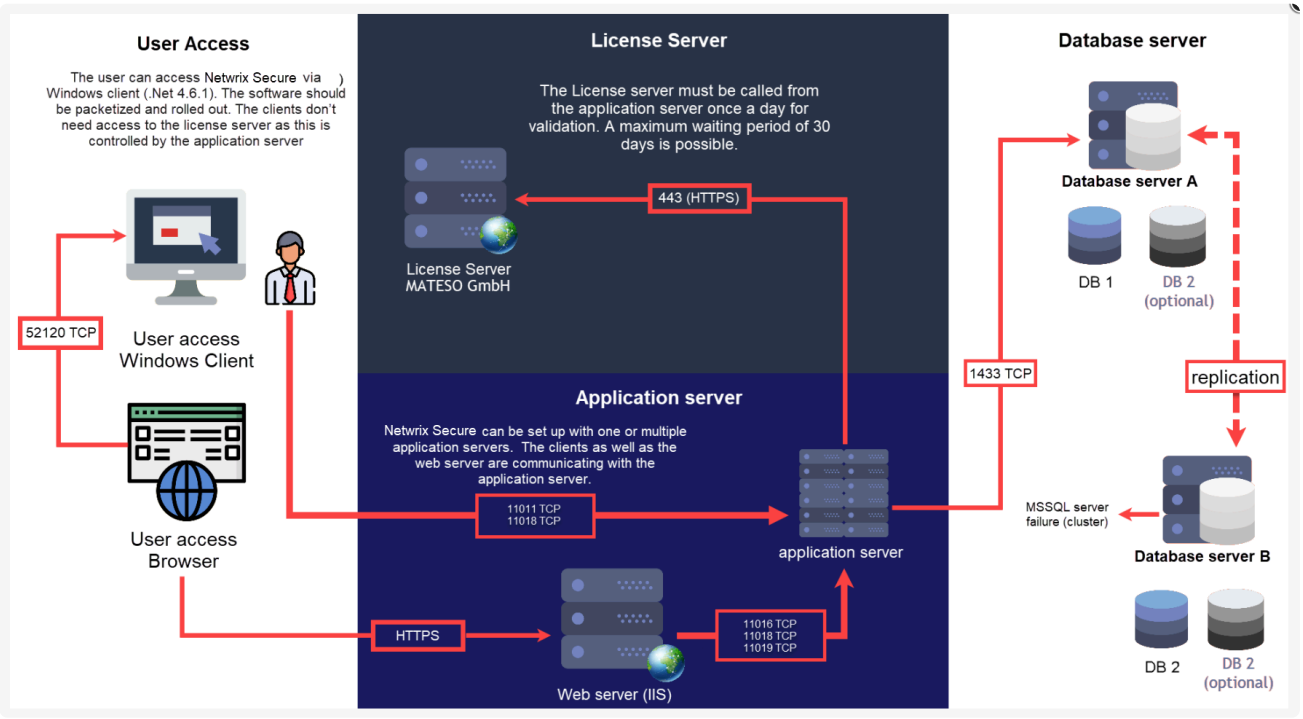
Multi-tier architecture

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.



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:

- Port 1433 TCP for communication with application server (incoming)

Server:

- Port 443 HTTPS for connection to MATESO license server (outgoing)
- Port 11011 TCP for communication with clients or web server IIS (incoming)
- Port 11014 TCP for the backup service (usually does not need to be unlocked)
- Port 11016 TCP for the Web services (incoming; only when using the WebClient)
- Port 11018 TCP for real-time update (incoming)
- Port 1433 TCP for communication with SQL Server (outgoing)

Client:

- Port 11011 TCP for communication with the application server (outgoing)
- Port 52120 TCP with the add-on (outgoing)

WebClient:

- Port 443 HTTPS zum Ansprechen des Webservers vom Client (eingehend)
- Port 11016 zur Kommunikation mit dem Anwendungsserver (ausgehend)
- Port 11018 für die Echtzeitaktualisierung (ausgehend)

MSSQL System Requirements

Required hardware

We recommend that you install the database on a separate MSSQL database cluster in order to prevent system failures. It 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
- 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 application server (incoming)

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.

Unfortunately, the Azure SQL server cannot currently be supported. Use of this server is thus at your own risk. Unfortunately, we cannot provide support in the event of any problems.

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 AdminClient, the user must have the **dbCreator** right.
- **dbOwner**: If the databases are created manually on the MSSQL server and are only managed by the AdminClient, **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 with the correct collation in order to subsequently link it 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!)
- At least 2 x CPU
- Min. 8 GB RAM
- Min. 40 GB hard disk space
- .net library 4.8.0or newer
- Firewall release
- Windows Management Framework 5.0 must be installed!

The application server requires that the following ports are enabled:

- Port 443 HTTPS for connection to MATESO license server (outgoing)
- Port 11011 TCP for communication with clients or web server IIS (incoming)
- Port 11014 TCP for the backup service (usually does not need to be unlocked)
- Port 11016 TCP for the Web services (incoming; only when using the WebClient)
- Port 11018 TCP for real-time update (incoming)
- Port 1433 TCP for communication with SQL Server (outgoing)

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.

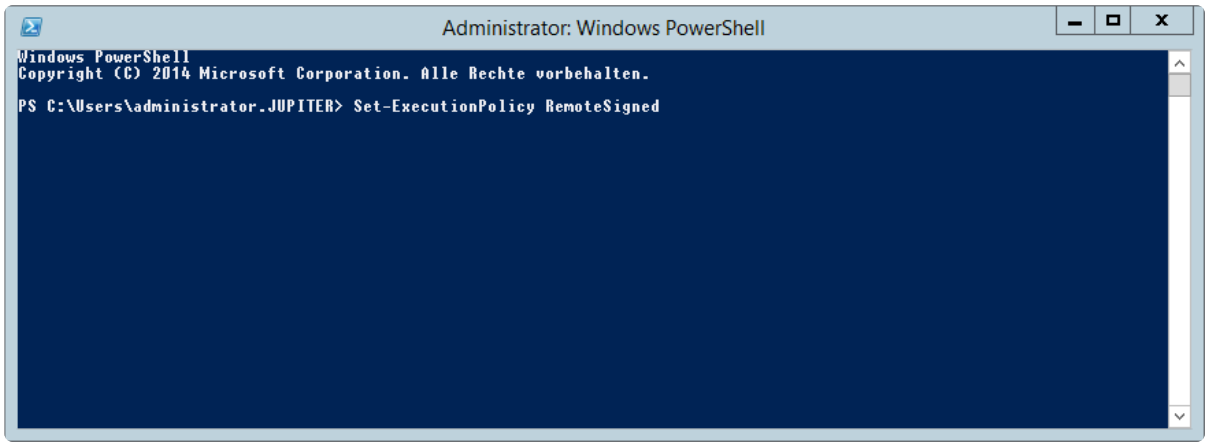
> ! It is not possible to combine local system and service users for the SQL configuration instance!

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)

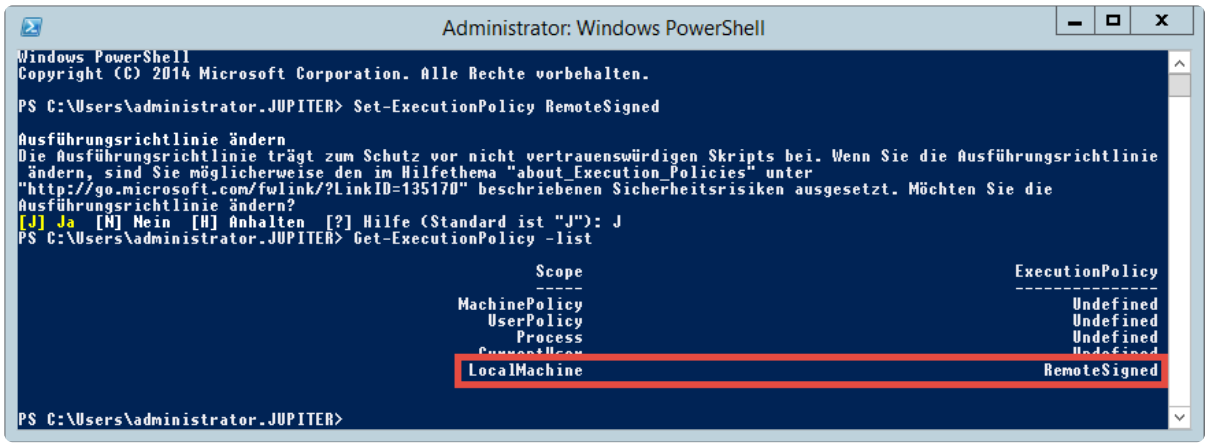
Open the PowerShell console. Enter **Set-ExecutionPolicy RemoteSigned** and confirm.



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



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



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
- .net library 4.8.0 or newer
- 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 (outgoing)
- Port 52120 TCP with the add-on (outgoing)

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.

The WebClient requires the following port shares:

- Port 443 HTTPS zum Ansprechen des Webservers vom Client (eingehend)
- Port 11016 zur Kommunikation mit dem Anwendungsserver (ausgehend)
- Port 11018 für die Echtzeitaktualisierung (ausgehend)

Supported web servers

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

IIS

- from **Version 7**
- **URL Rewrite** module version 2.1 or higher
- **Application Request Routing** module version 3.0 or higher
- **Websocket Protocol**

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.

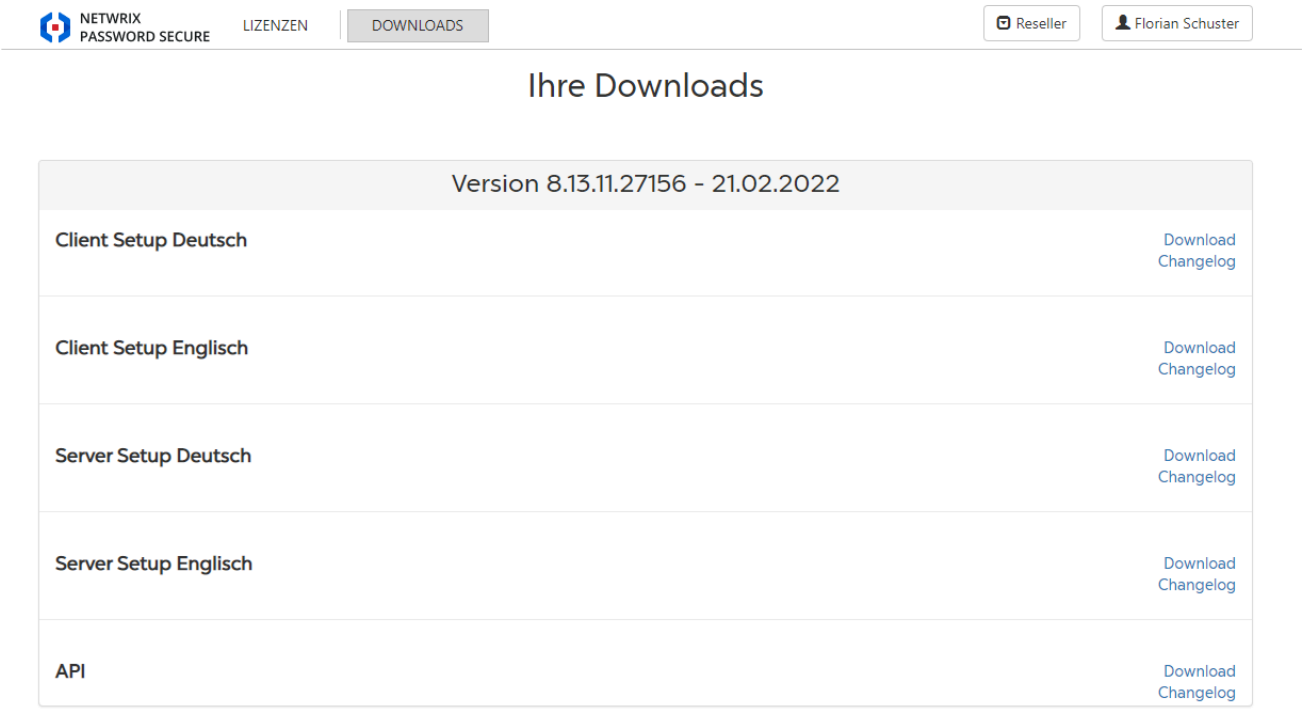
The connection between the browser and the web server must be protected by an SSL

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



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

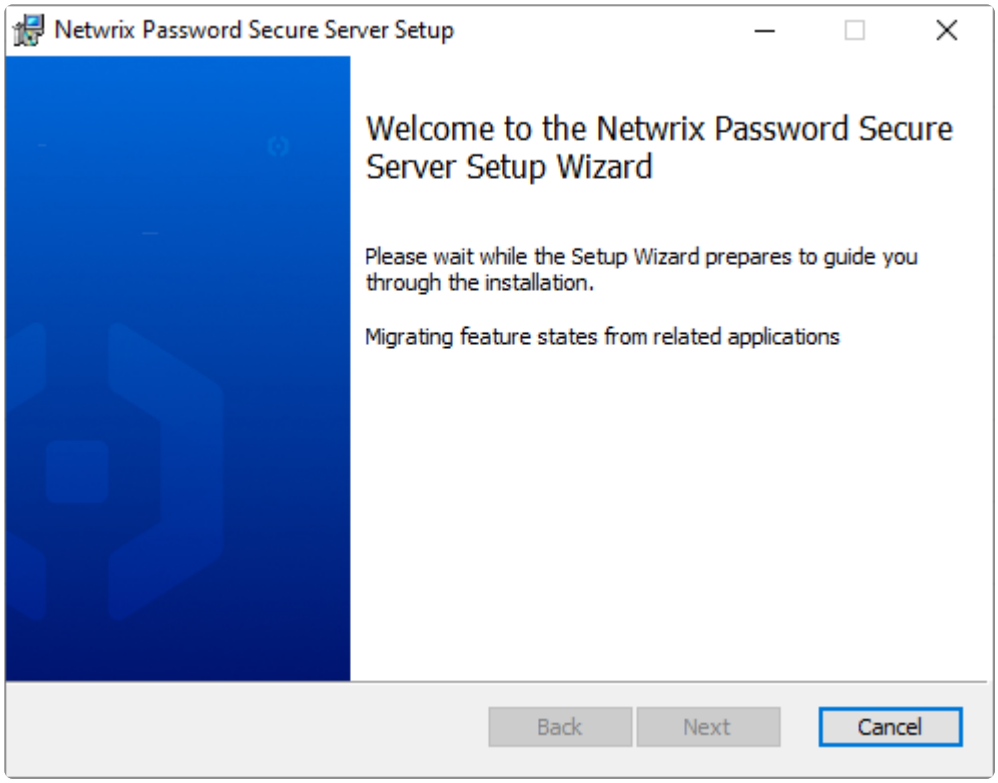


https://www.youtube.com/embed/mWKzPWjIqIY?rel=0

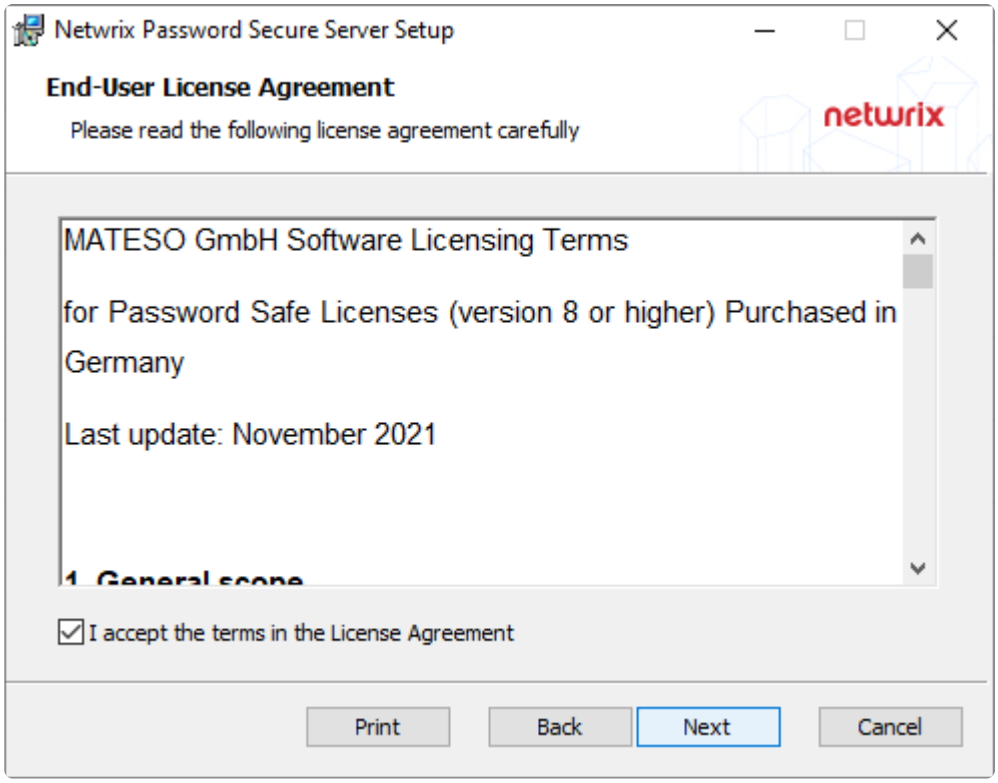
https://www.youtube.com/embed/mWKzPWjIqIY?rel=0

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.

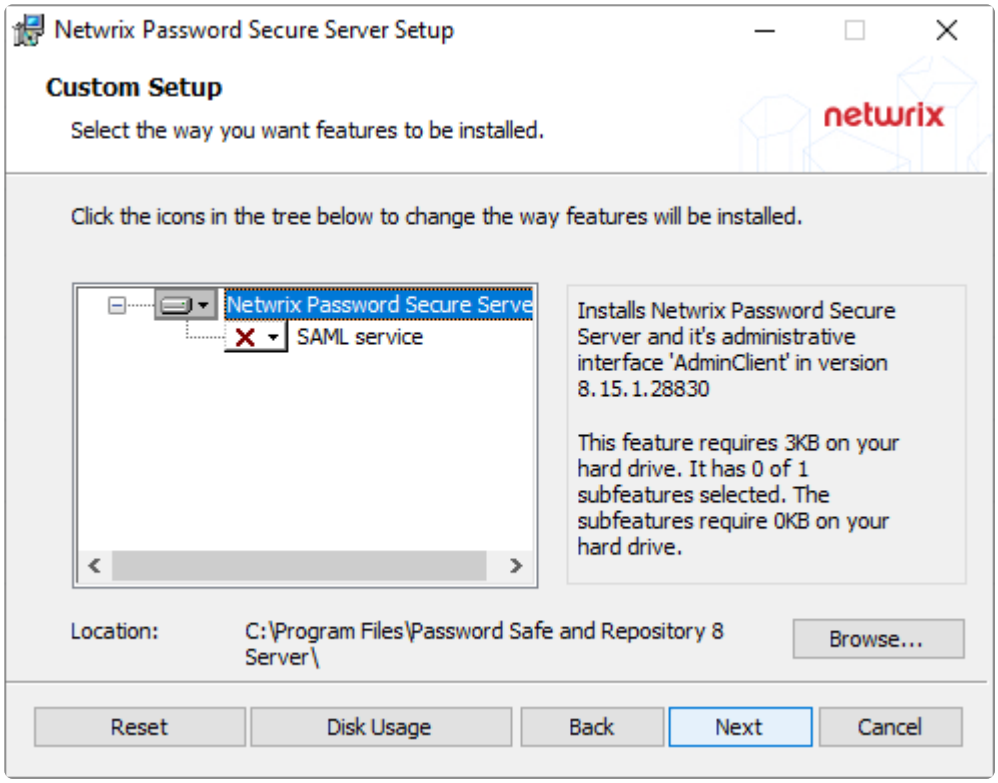


You are firstly required to read and accept the license terms. These can also be printed.

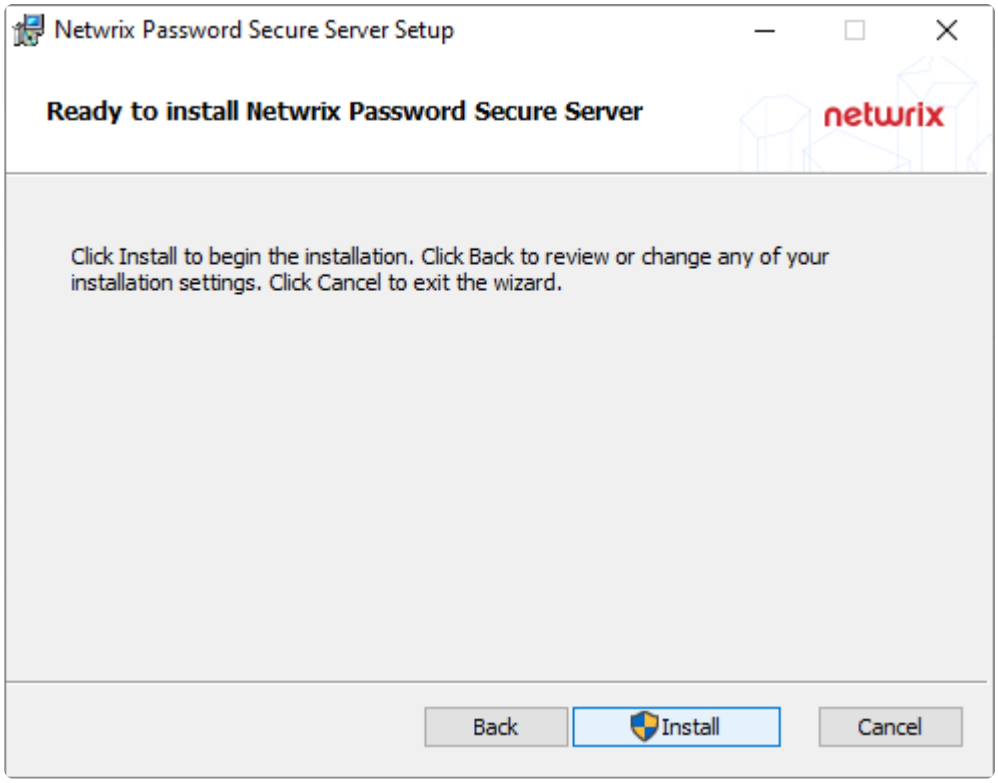


The next step is to define the location. As a rule, the suggested location can be retained.

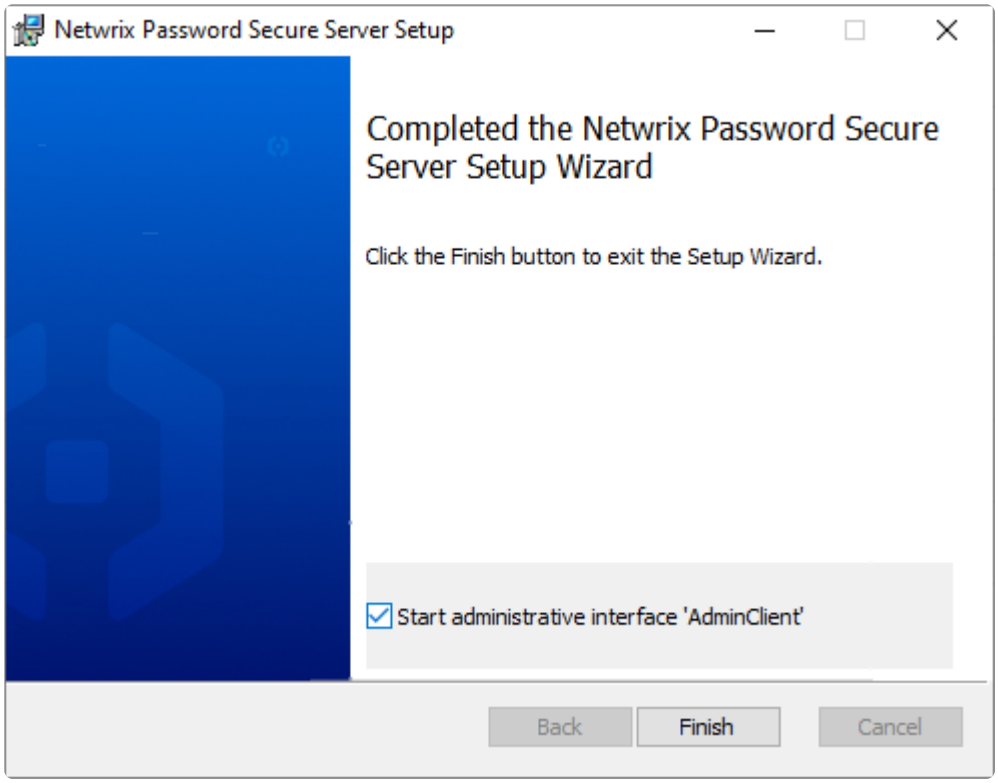
The SAML Service must only be selected if you want to use Password Safe as an identity provider. Otherwise, it will not be installed.



The next step is starting the installation.

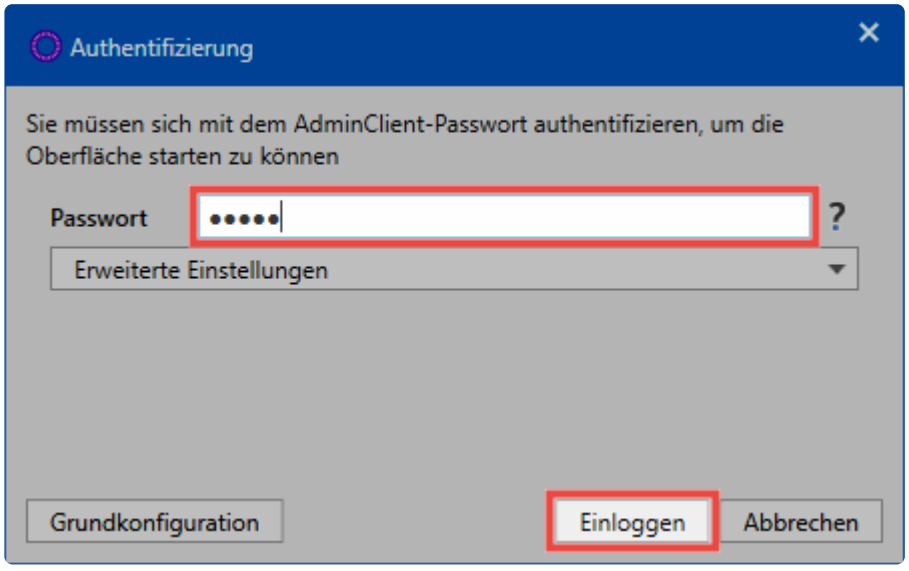


The last step closes the setup and opens (if desired) the AdminClient.



Authentication

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



> 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

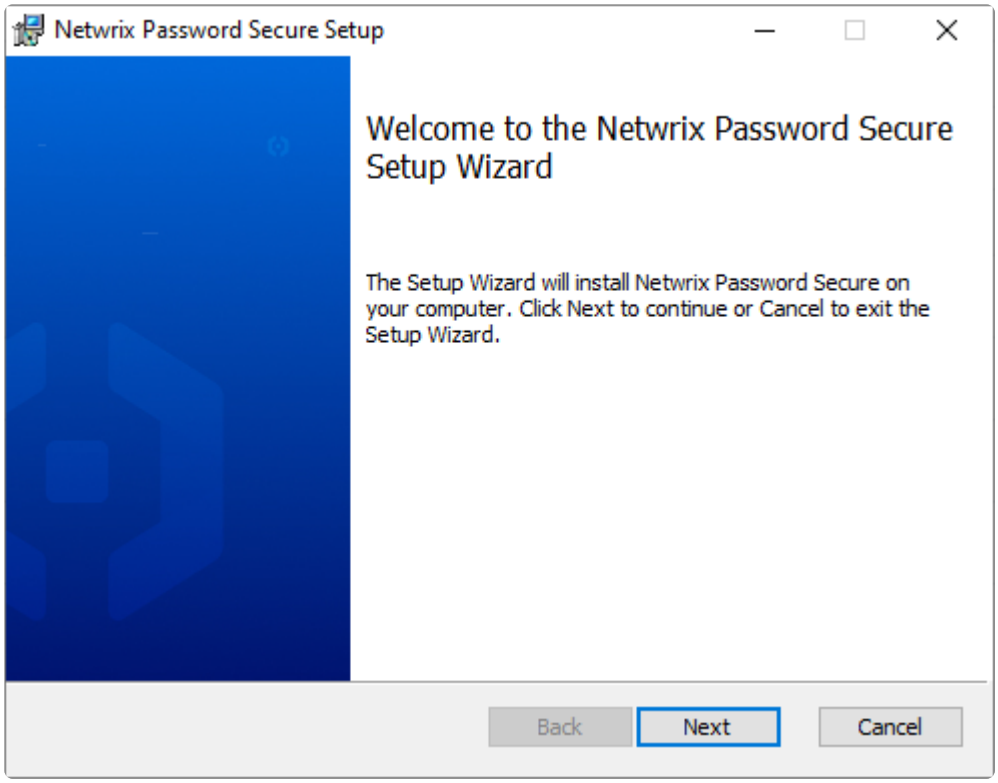


https://www.youtube.com/embed/9Fq_ev7vXhM?rel=0

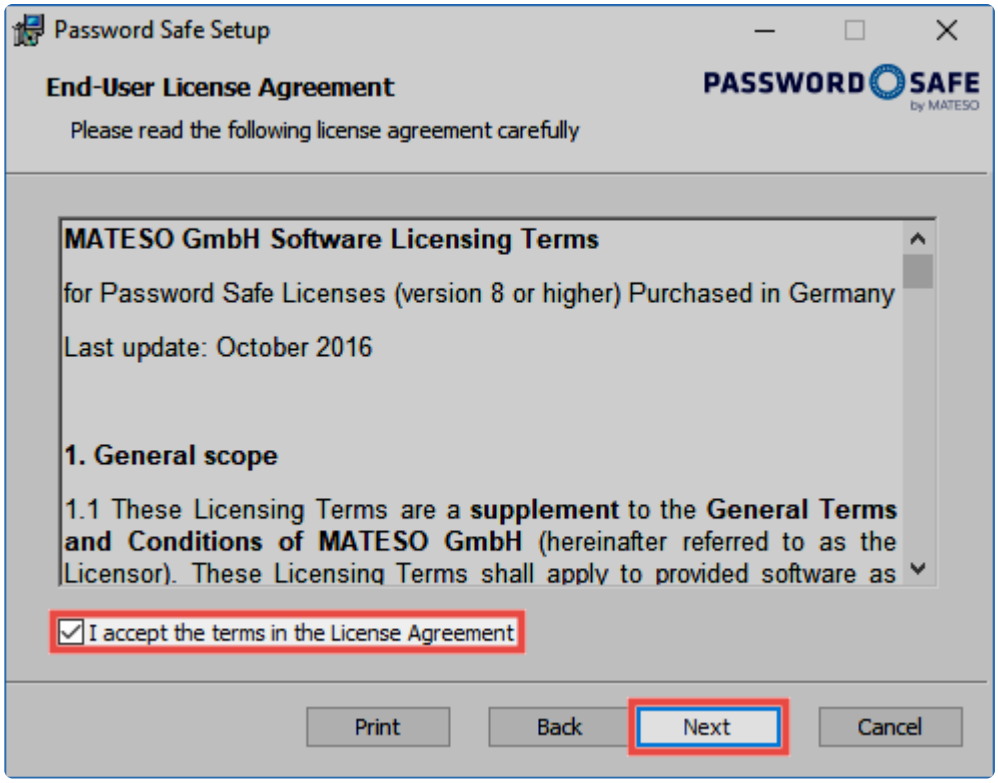
https://www.youtube.com/embed/9Fq_ev7vXhM?rel=0

Guide

The MSI installation files and the associated Client system requirements can be found in the corresponding sections. The following step-by-step guide will accompany you through the wizards.

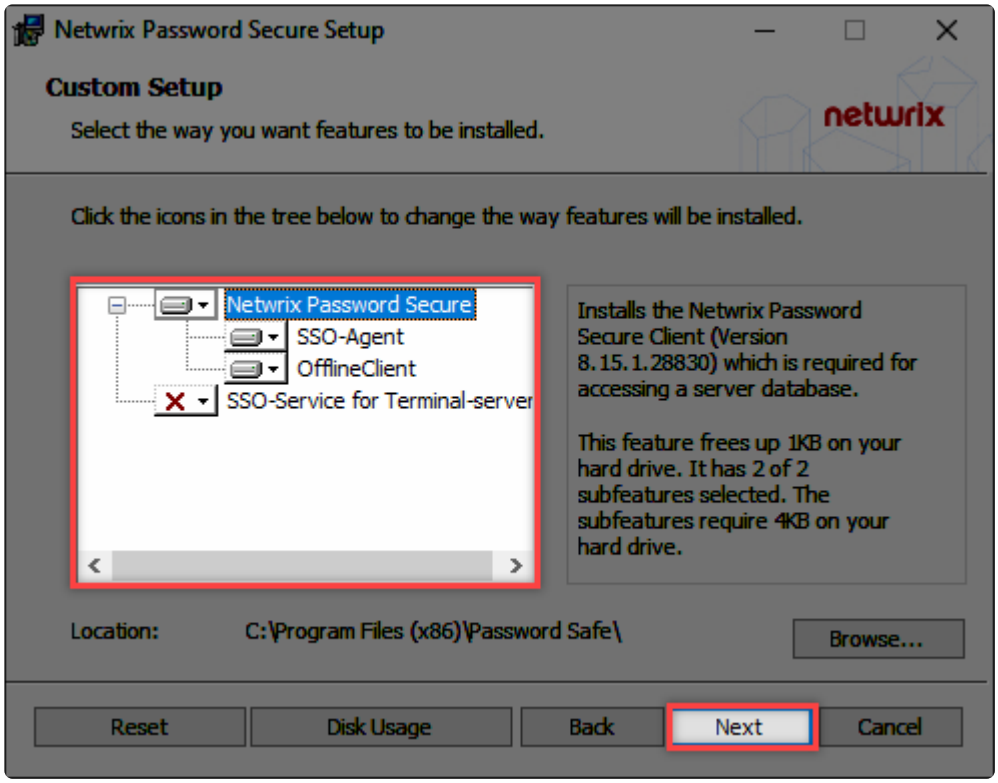


You are firstly required to read and accept the license terms. These can also be printed.



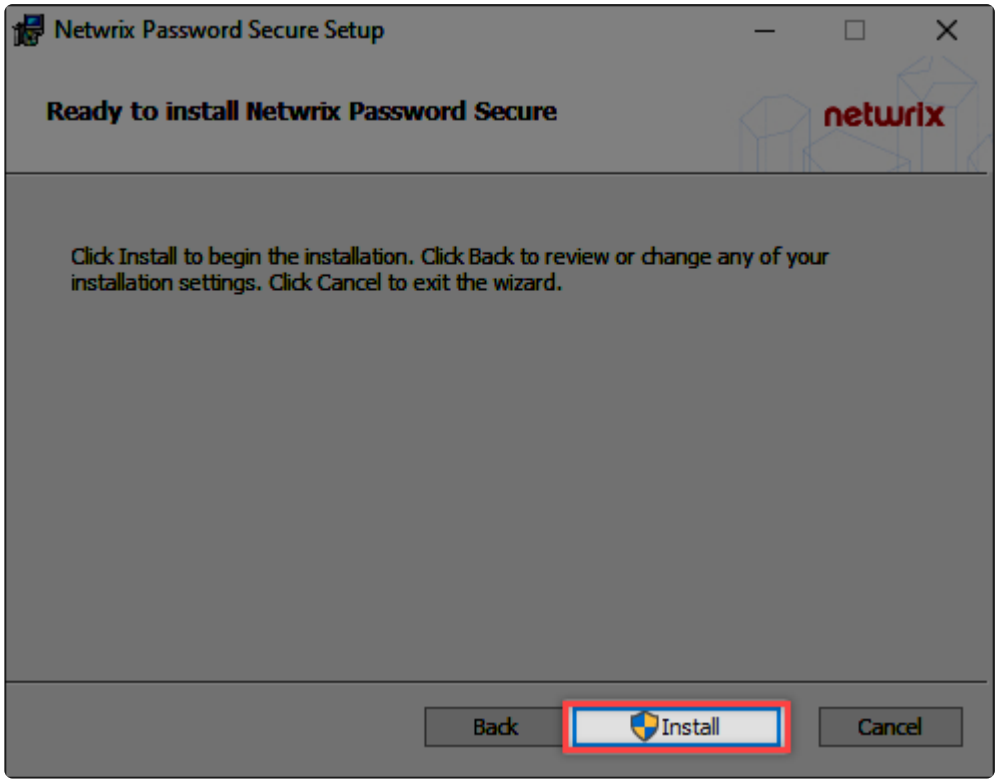
The next step is to define the location of the client. You can also define here whether additional components should be installed.

- **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

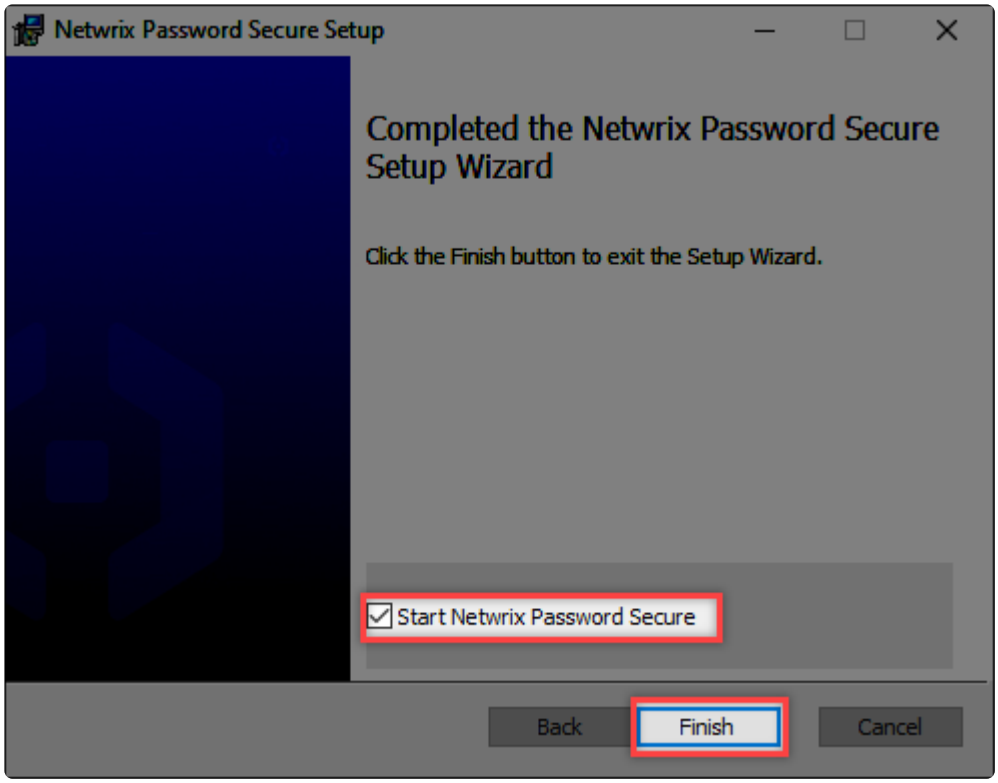


> ! Please install the SSO service only if the terminal server operation is devised!

The actual installation starts in the next step.



The last step finishes the setup and opens the client.



Installed applications

There are always several applications installed.



This is the regular Client.



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



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

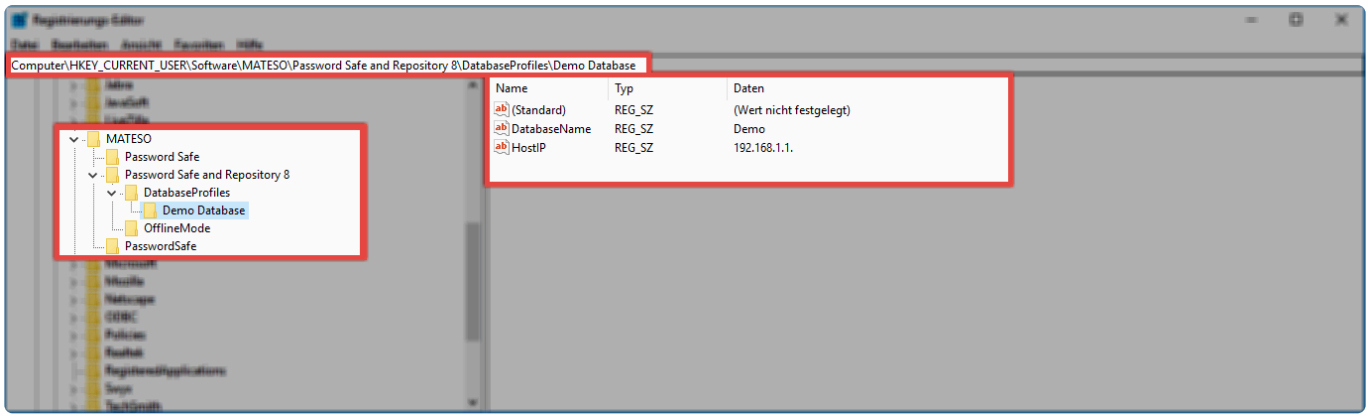
Distributing database profiles via the registry

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 data base connection can be made with the following keys:

HKEY_CURRENT_USER\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles
HKEY_LOCAL_MACHINE\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles

The structure of these keys is as follows:

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



Is the profile set with the following entries?
HKEY_LOCAL_MACHINE\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles

Then the last used date base as well as the last registered user are created with the following ID, when you log in for the first time:
HKEY_CURRENT_USER\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles

When the corresponding registry entry is set and no related database profile exists, the profile will be created at the next start-up. Please note that 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
- **IGNORE_TS_SERVICES="1"**: Deactivates the installation of the terminal server services, no matter on which system the installation is running

Installation of the WebClient

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

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

Preparations for installation

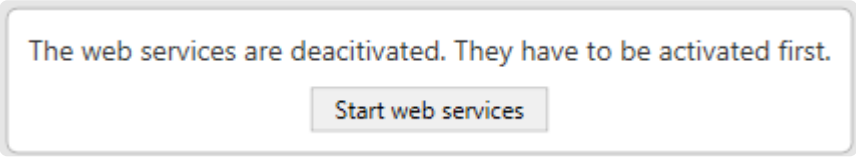
To carry out the installation of the WebClient without any further complications, the following preparations should be carried out:

System requirements

It should first be ensured that all of the **system requirements** 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 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.

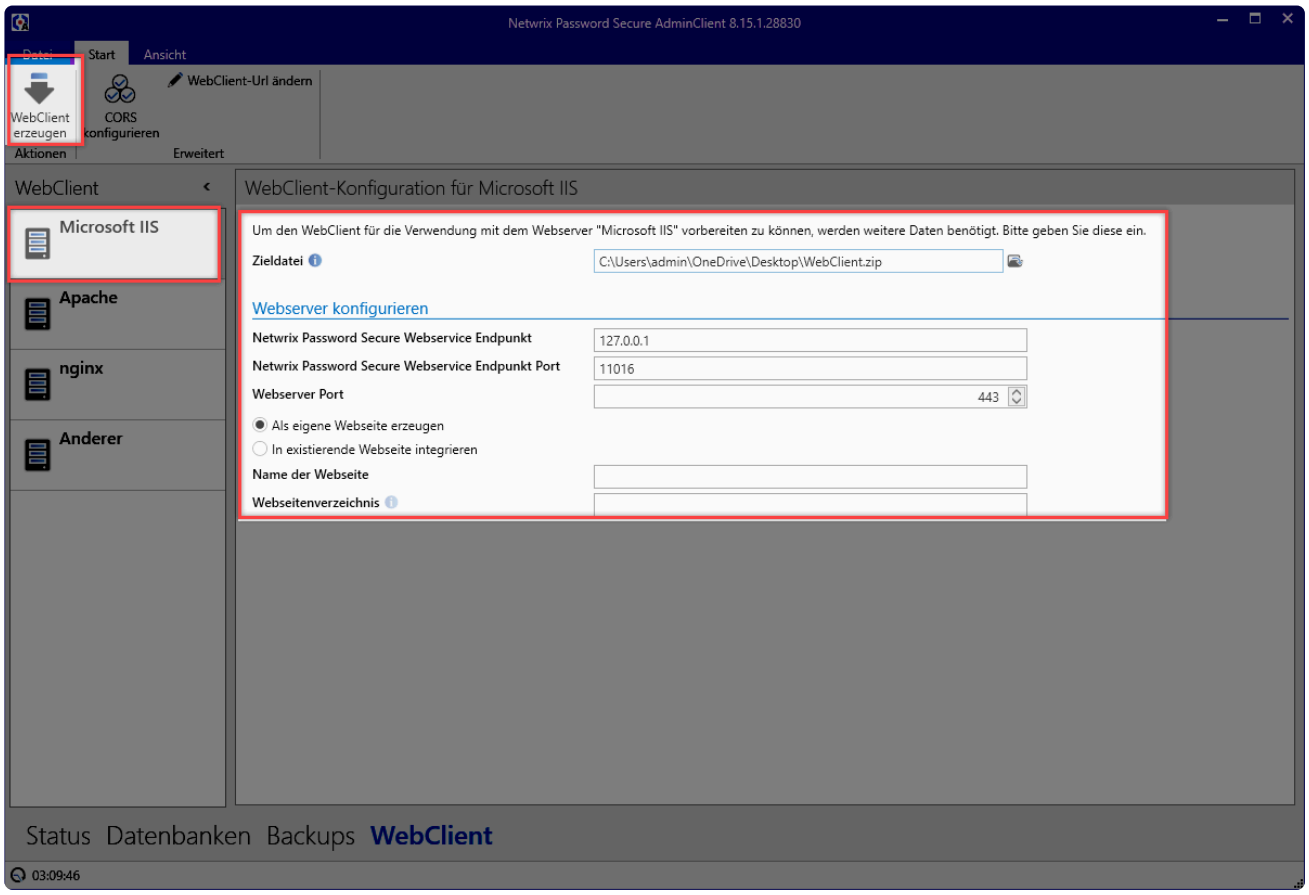
Microsoft IIS

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"



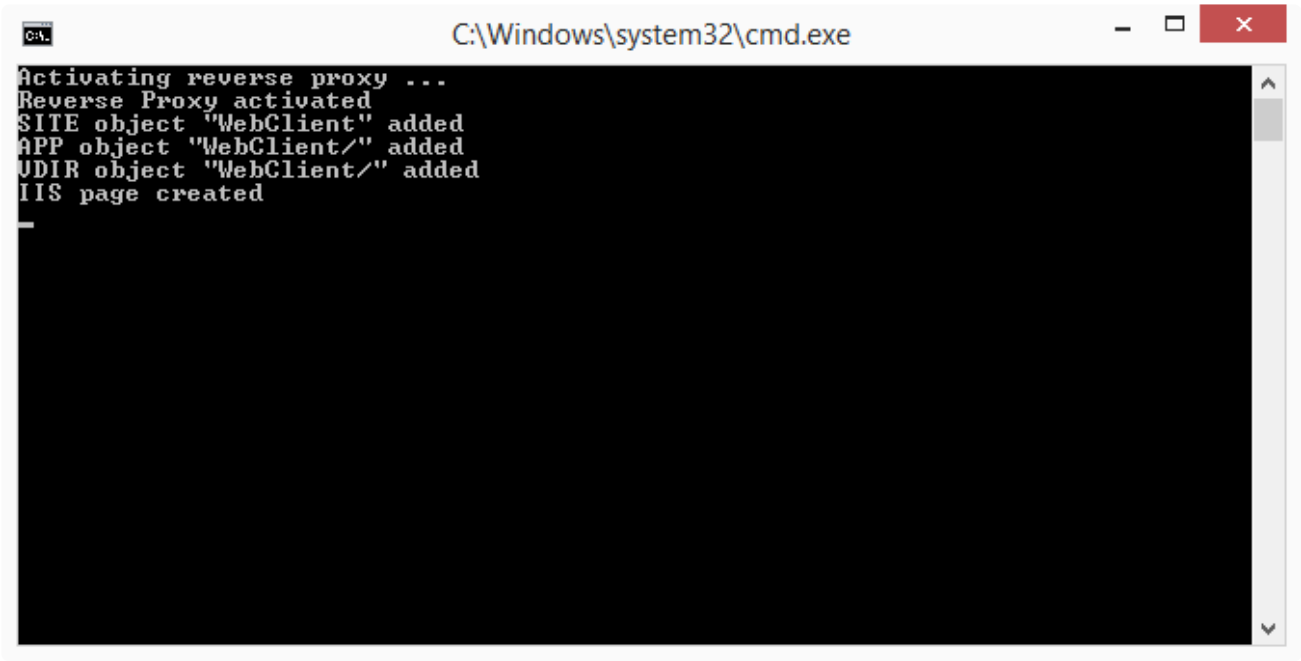
Once all of the settings have been entered, the WebClient can be created via the corresponding button in the ribbon. When the ZIP archive containing the WebClient has been created, it is copied to the previously defined directory (C:\inetpub\wwwroot as standard) and unzipped there to create a new directory.

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. In addition, it is necessary to install the **WebSocket Protokoll**. Afterwards, **config.bat** needs to be executed again.

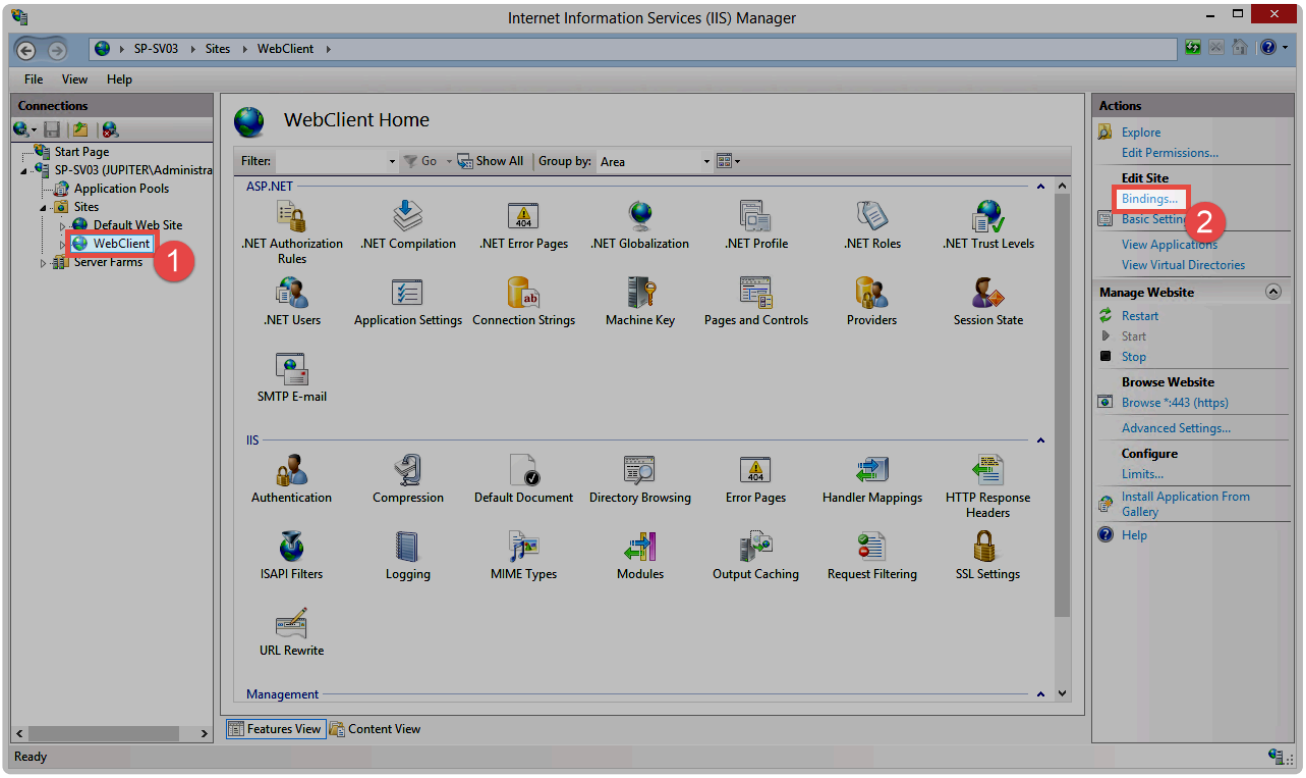
If the website has been correctly created, this will be correspondingly indicated by the notification **IIS page created**.



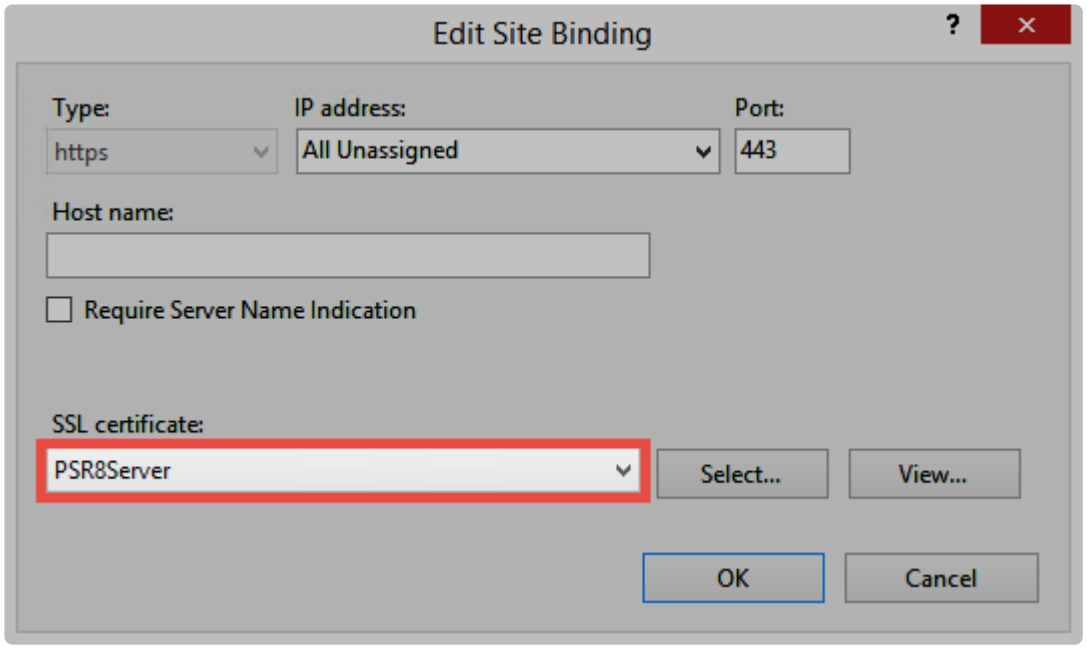
> ! Following a successful installation, it is imperative that **config.bat** is deleted! The **config.bat** file should also not be used for an “update”#updates!

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.



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”#zertifikate.

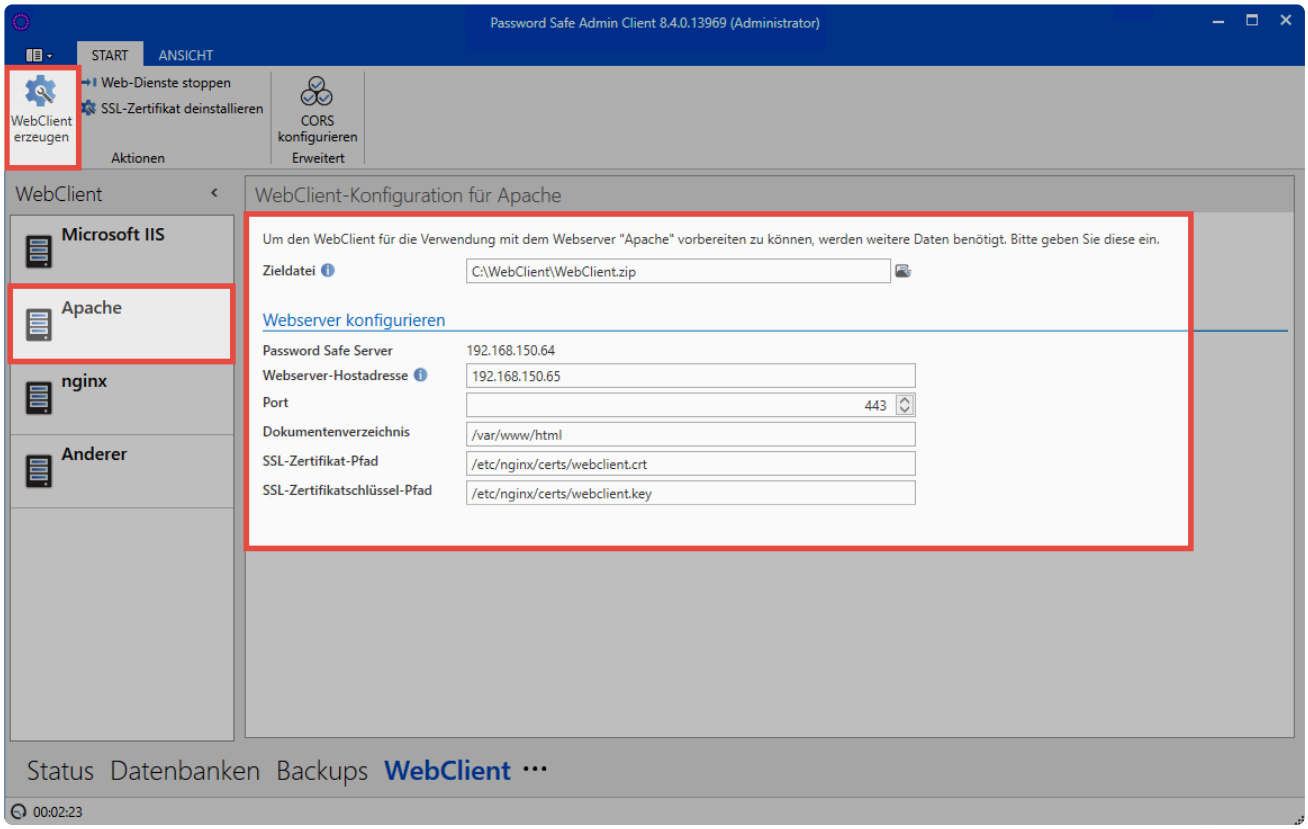
Apache

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**

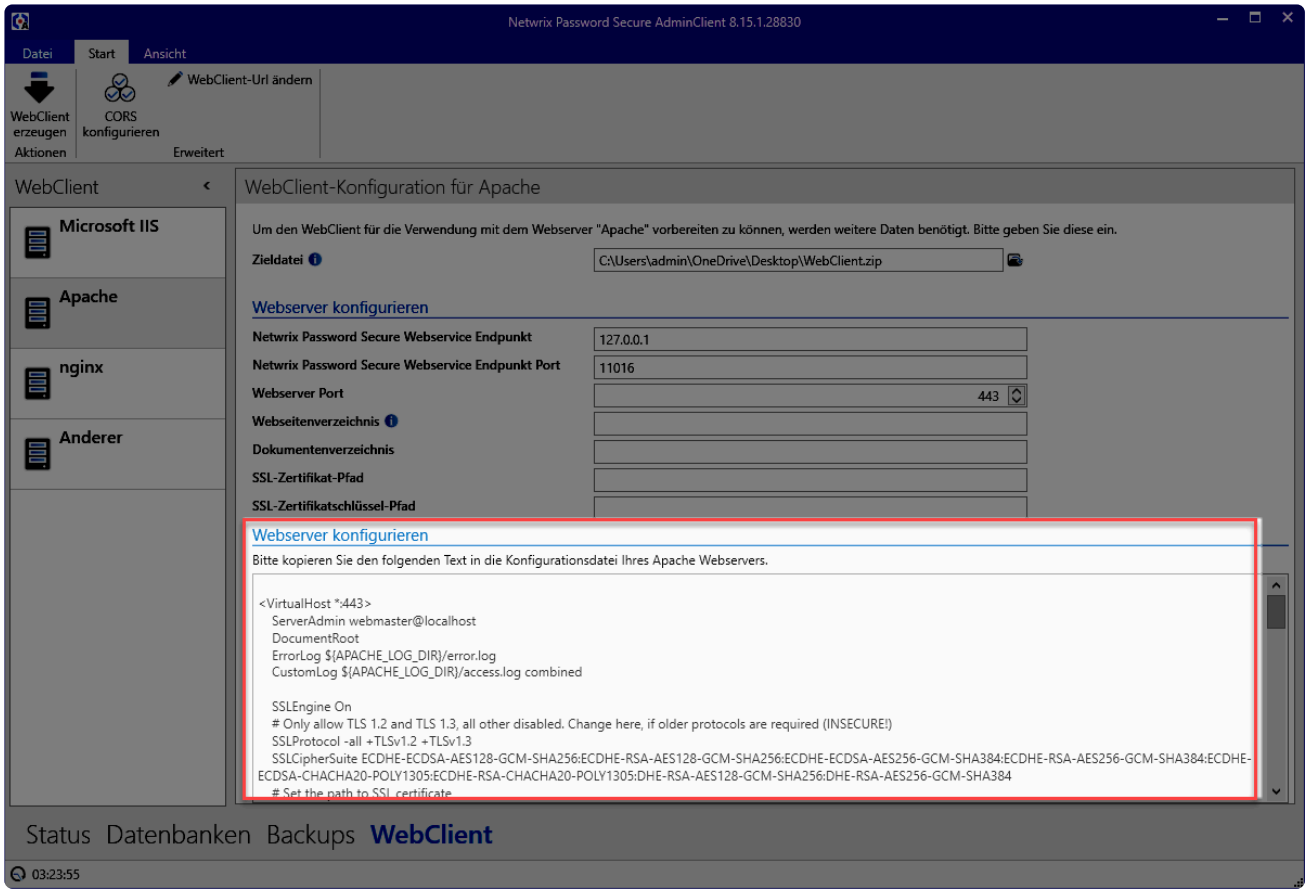
SSL certificate path
It is necessary to enter the directory in which the certificate will be saved here.

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



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.



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>` und `</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

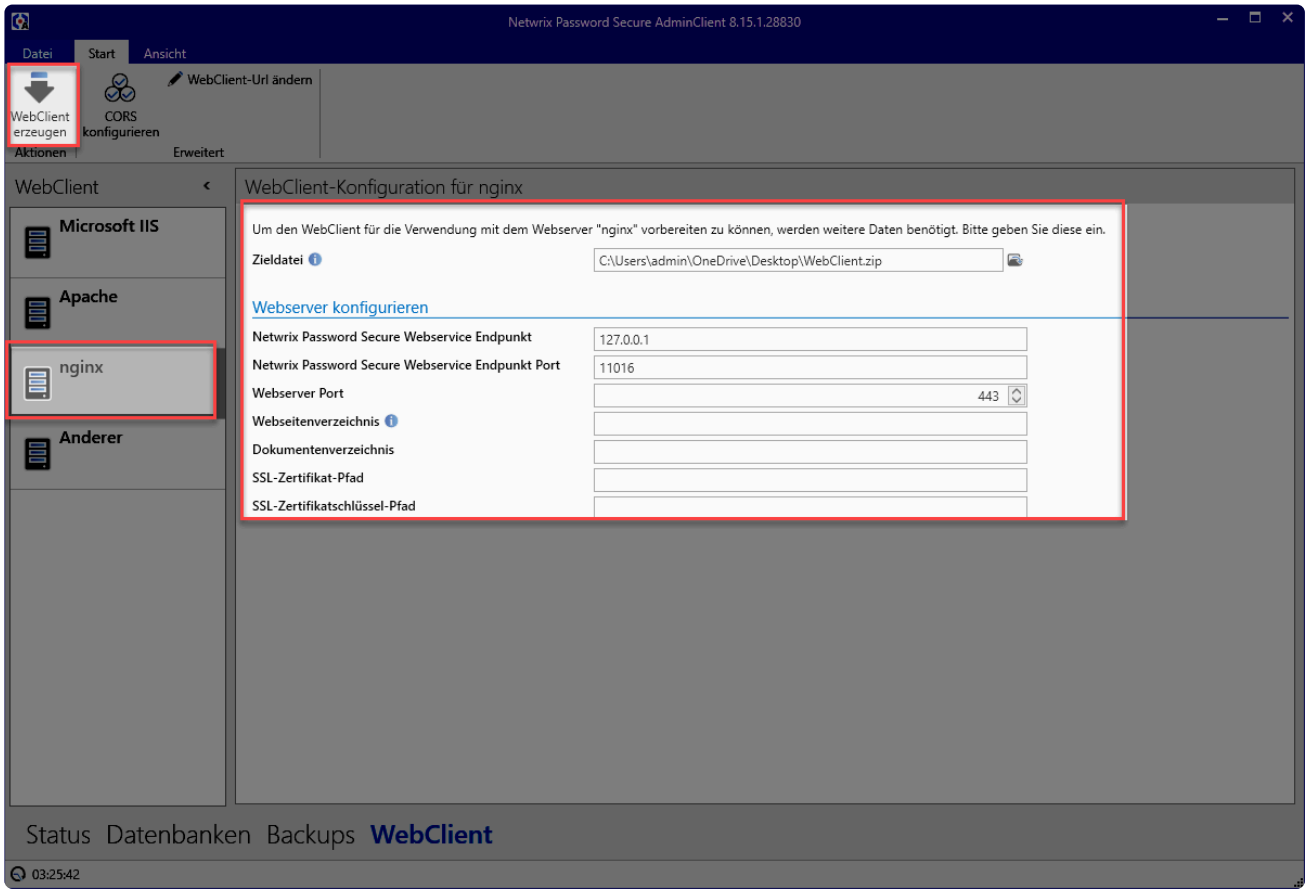
In order to integrate the WebClient onto an nginx server, it is first necessary to enter all of the relevant settings:

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

SSL certificate path

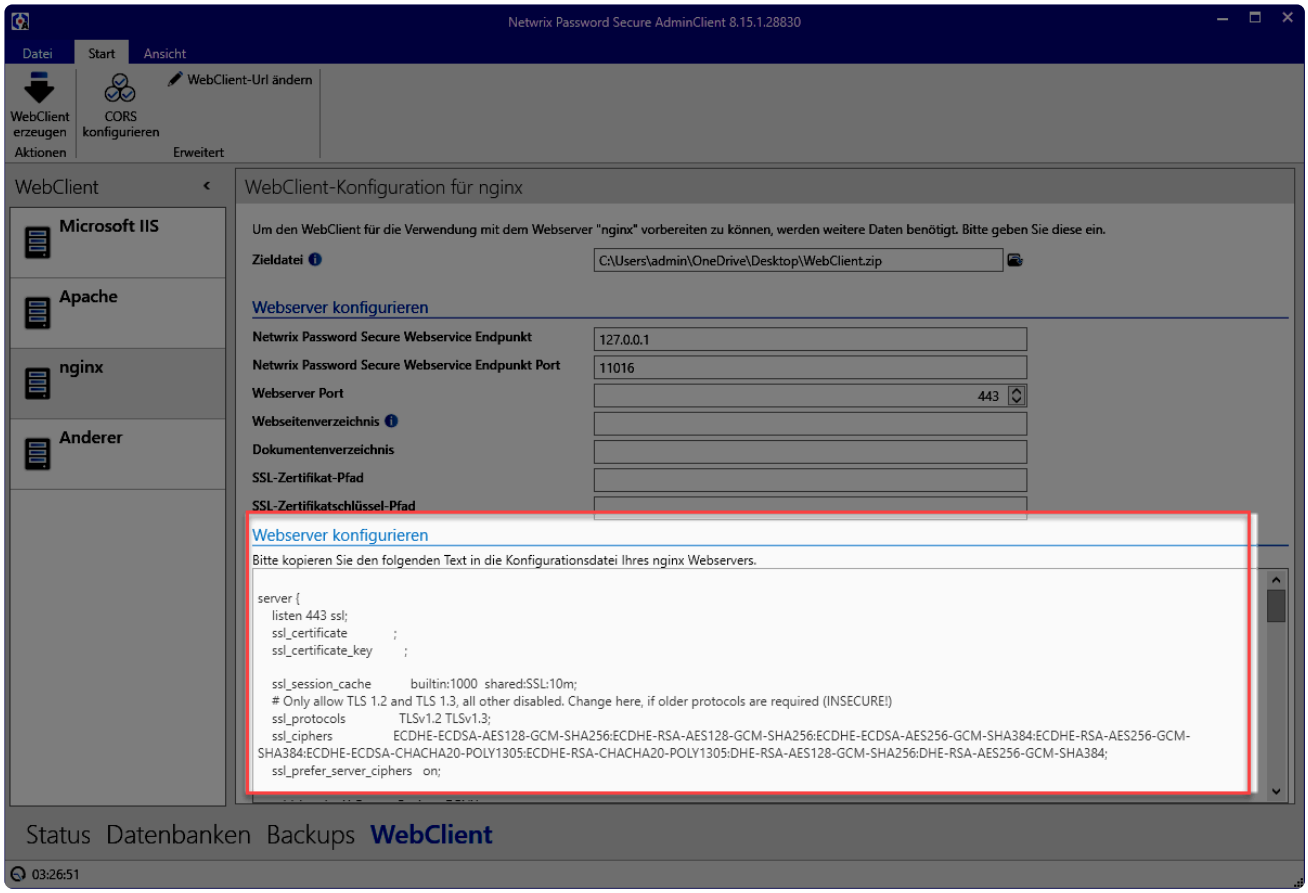
It is necessary to enter the directory in which the certificate will be saved here.
The standard path here is **/etc/nginx/certs/webclient.crt**

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**



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.



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.

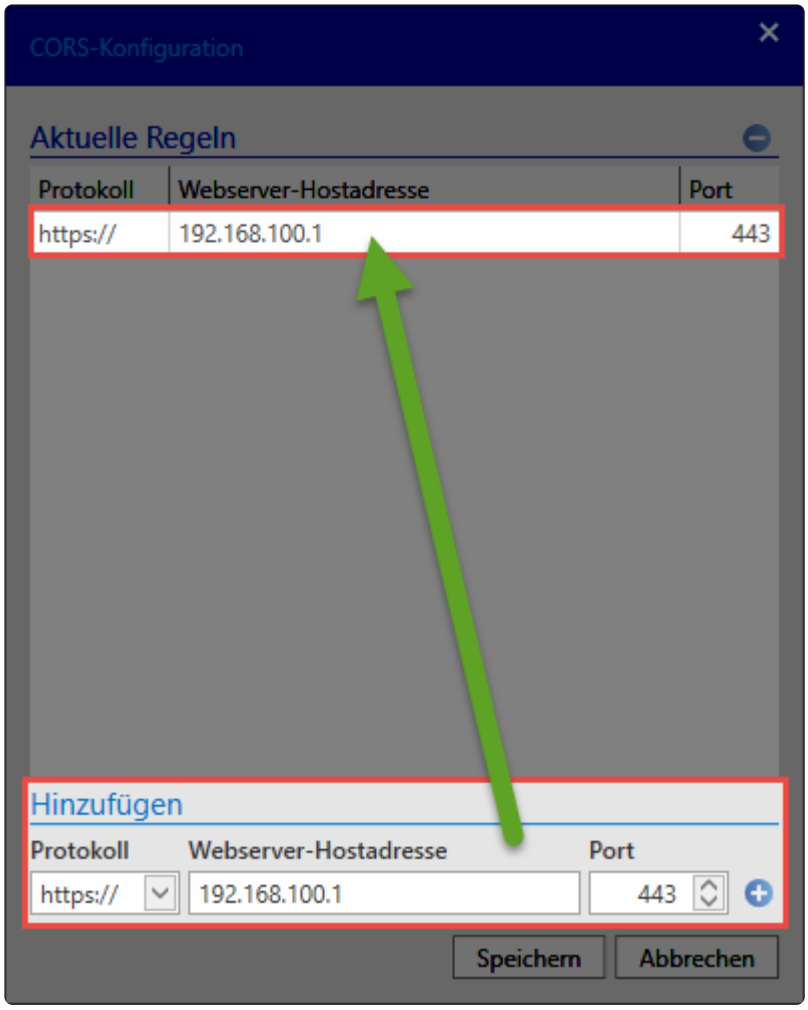
Standard configuration
The file **/etc/nginx/sites-available/default** is firstly opened. For example via “nano”. Now search for the entry `server { }`. The configuration for the AdminClient is then added. Finally, the web server is restarted using the command **systemctl restart nginx**.

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.



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**

Redirecting

Redirecting from http to https is also set up in the configuration for IIS, apache and nginx web servers.

In the case of an ISS web server, the redirect rule is written directly in the web server configuration. The binding for port 80 must also be configured in IIS for the redirect.

In the case of apache and nginx web servers, a corresponding configuration is created that needs to be manually added to the correct configuration file.

In order for the redirect to be used, it is important to ensure on apache and nginx web servers that no other host listens to port 80.

Installation Browser Addons

Currently, Addons for **Microsoft Internet Explorer**, **Microsoft Edge**, **Google Chrome** and also **Mozilla Firefox** are available. Since the installation differs depending on the browser, it will be discussed separately here.

> ! As the technology of Internet Explorer is outdated and Microsoft Edge is rebuilt, we are unfortunately forced to discontinue support for the respective add-ons.
> Both add-ons will no longer be developed from version 8.9 onwards. This also means that no more bugs will be fixed and no more support for them will take place. Therefore, the use of add-ons is at your own risk. As of version 8.11, both add-ons are no longer available.

Internet Explorer

The Internet Explorer addon can be installed directly together with the client. For this purpose, there is a corresponding option in the installer that is activated by default.

Google Chrome

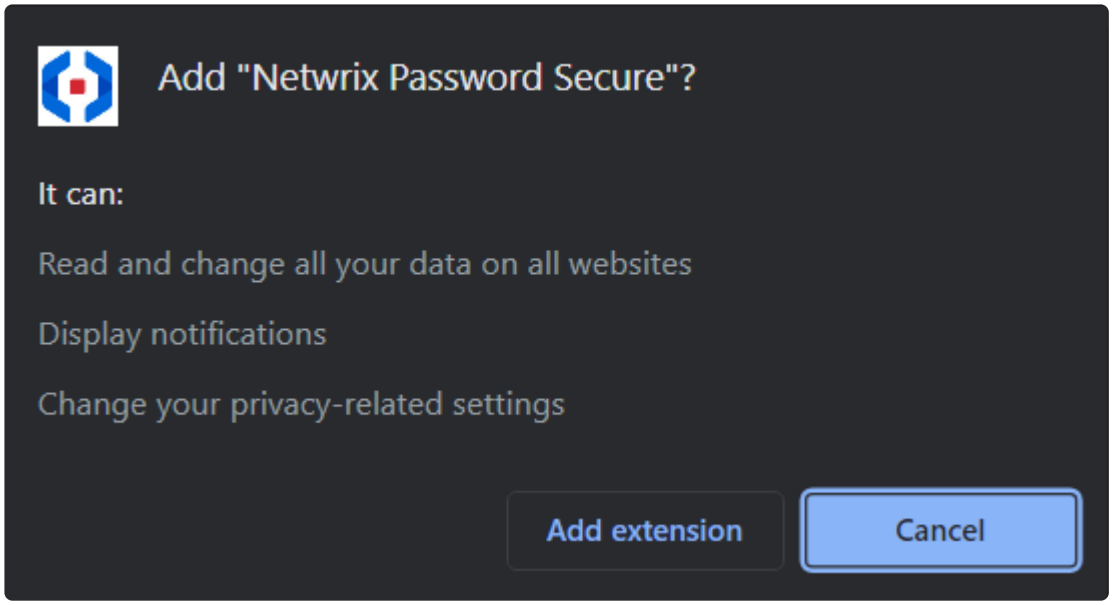
The Google Chrome addon is installed directly from the Google Store. This can be reached via the following link: **Password Safe Addon for Google Chrome**

Alternatively, the Google Store can be reached via the SSO agent. To do this, right-click on the icon to open the context menu. After another click on **install browser addons**, the Google Chrome addon can be selected. You will be redirected directly to the Google Store.

You can start the installation by clicking on **Add to Chrome**.



The addon will now be installed and the icon added to the browser.



Installation of the add-on via the WebClient

It is also possible to install the add-on via the WebClient.

To do this, click on the icon in the web client, which is located at the bottom of the page.

Firefox

You can download the Firefox addon via the following link:
Password Safe Addon for Firefox

Password Safe addon for Firefox

After the download, the add-on is simply dragged and dropped into the browser.

After confirmation, the addon will be installed and an icon created in the menu bar.

Edge (obsolete, therefore not recommended)

You can download the Edge addon via the following link:
Password Safe Addon for Edge

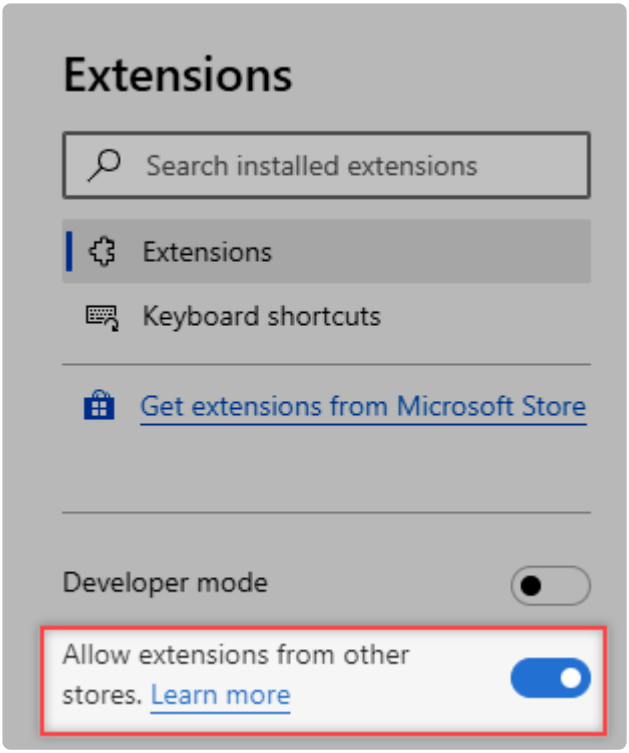
After the download, the archive is first unzipped. Then you have to open the appx file with a double-click.

After confirmation, it will be installed and an icon created in the menu bar.

Edge Chromium

Requirements:

In the extensions of the browser, it must be activated that **extensions from other stores** may be added.



To add the addon in Edge Chromium there are 2 possibilities:

- 1. install the add-on via the WebClient (how to do this is described in the section below)
- 2. installation via the Chrome Web Store. Here you will find the add-on.

Installation of the add-on via the WebClient

It is also possible to install the add-on via the WebClient.

To do this, click on the icon in the web client, which is located at the bottom of the page.

Safari

You can download the Safari addon via the following link: **Safari Addon**

For the installation, just double-click on the downloaded file. Finally, the Password Safe Logo must be dragged and dropped on the applications on the screen.

Installation Chrome

Google Chrome

The installation of the Google Chrome Add-on is done directly from the Google Store. You can access it via the following link: Password Safe Add-on for Google Chrome

Alternatively, you can also access the Google Store via the SSO Agent. To do this, right-click the icon to open the context menu. After a further click on **Install Browser Add-ons** the Google Chrome Add-on can be selected, whereupon you will be redirected directly to the Google Store.

The installation is started via **Add**.

The add-on is now installed and the icon is added to the browser.

Installing the add-on via the WebClient

It is also possible to install the add-on via the WebClient.

To do this, click on the icon in the web client, which is located at the bottom in the middle of the page.

Installation Mozilla Firefox

Firefox

The Firefox Add-on can be downloaded from the following link:
Password Safe Add-on for Firefox

After the download, the add-on is simply dragged and dropped into the browser.

After confirming a security question, it is installed and an icon is created in the menu bar.

Installation Edge

The Edge Add-on can be downloaded from the following link: **Edge Addon**
You will be redirected to the Microsoft Store when you open the link.

There you have the possibility to add the addon for the Edge.

Installation Safari

Safari

The Safari Add-on can be downloaded from the following link: **Safari Addon**
To install it, simply double-click on the downloaded file. A window will open where you then only need to drag and drop the Password Safe logo onto the applications.

Moving the server

Preparations

It is necessary to make some preparations so that the move can be completed without any problems.

1. Installing the SQL server

If the SQL server and the application server are on the same machine, the SQL server should be installed on the new machine first. It is necessary to observe the **system requirements** for this process.

2. Installing the server

The Password Safe server is installed next (see **System requirements**). The installation itself is described under **“Installation of the AdminClient**.

3. Basic configuration

After the server has been installed, the **basic configuration** is completed. A new configuration database will be created on the SQL server as a result. If you want to retain the old SQL server, it is necessary to give the configuration database a new name.

4. Deactivating the old server

The licence first needs to be deactivated before it can be activated on the new server (see options under **“License settings**). Now stop the server so that nothing more can be changed in the database.

Backing up the data

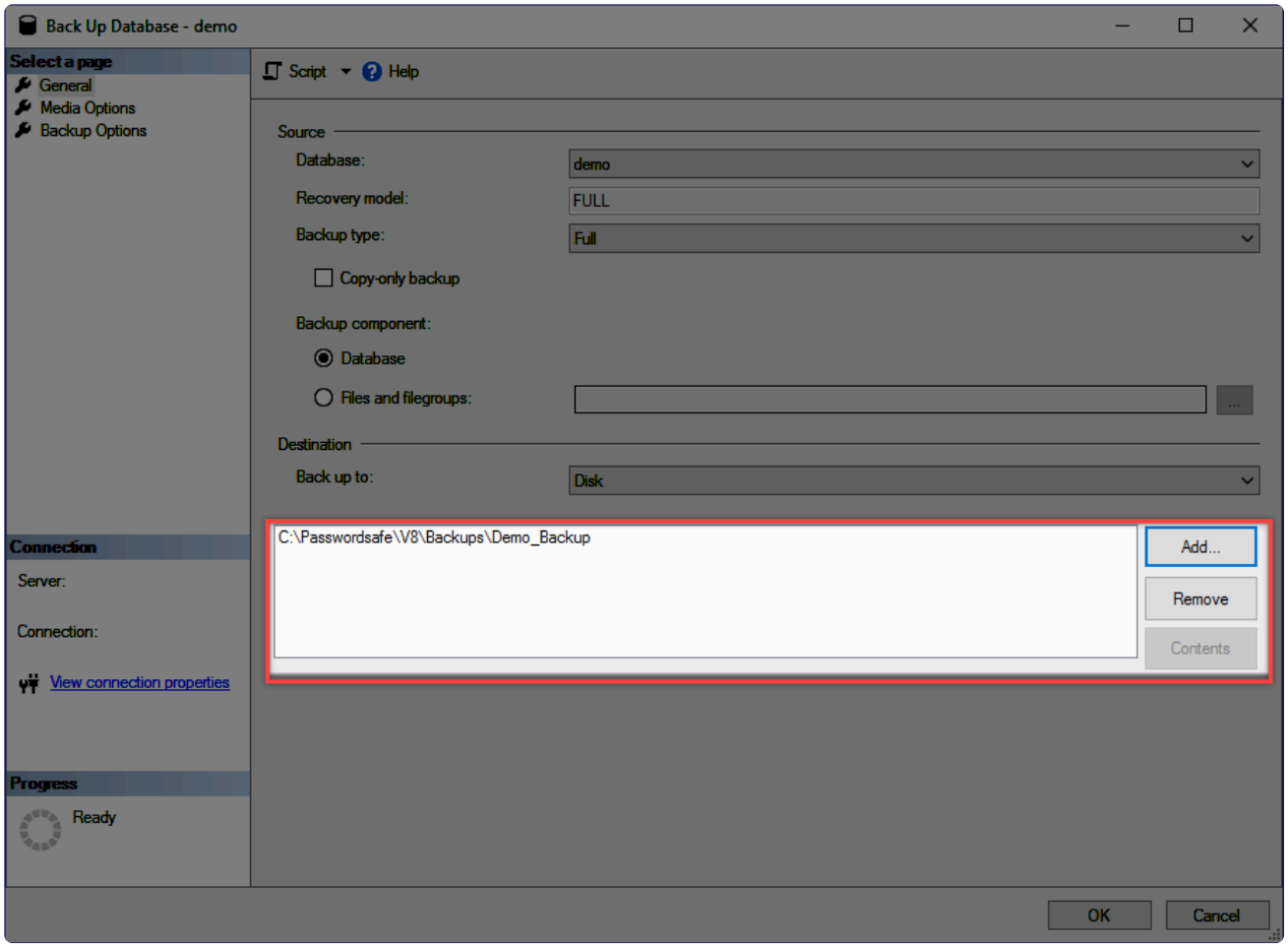
After making these preparations, the data from the old server can be backed up.

1. Backing up the system

If using a virtual machine, a backup of it should be created. The old version of the server can then be restored in the event of problems.

2. Backing up the database

In order to transfer the data to the new server, a backup of the database should be created. Although this is also possible via the AdminClient, we recommend carrying out the backup at the SQL level: right click on the database, then on **Tasks** and **Backup**. The desired target folder is selected in the following window.



3. Backing up the server certificate

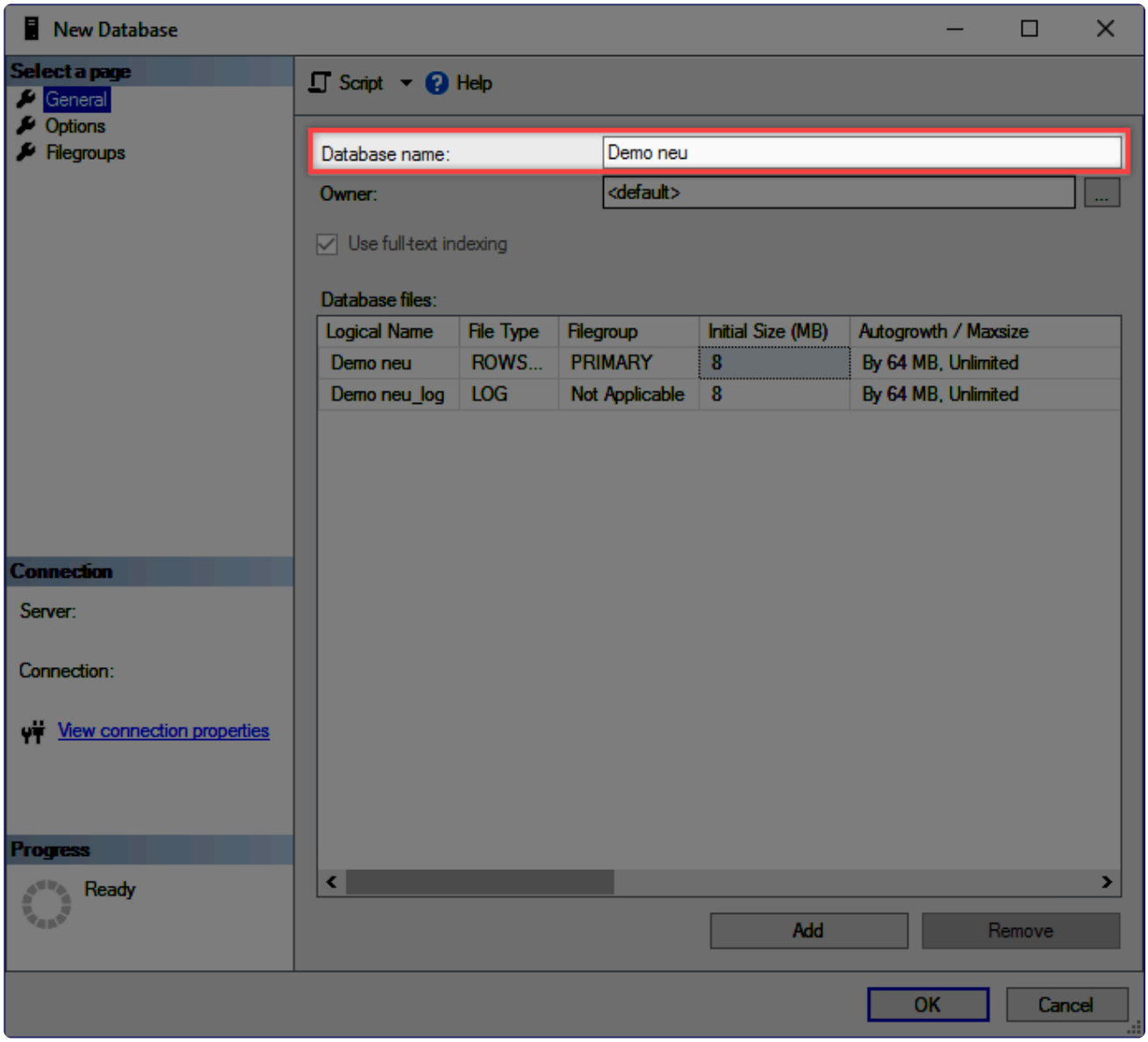
It is essential that the all available certificates are backed up. Depending on the installation, a different number of certificates are required here.

Configuring the new server

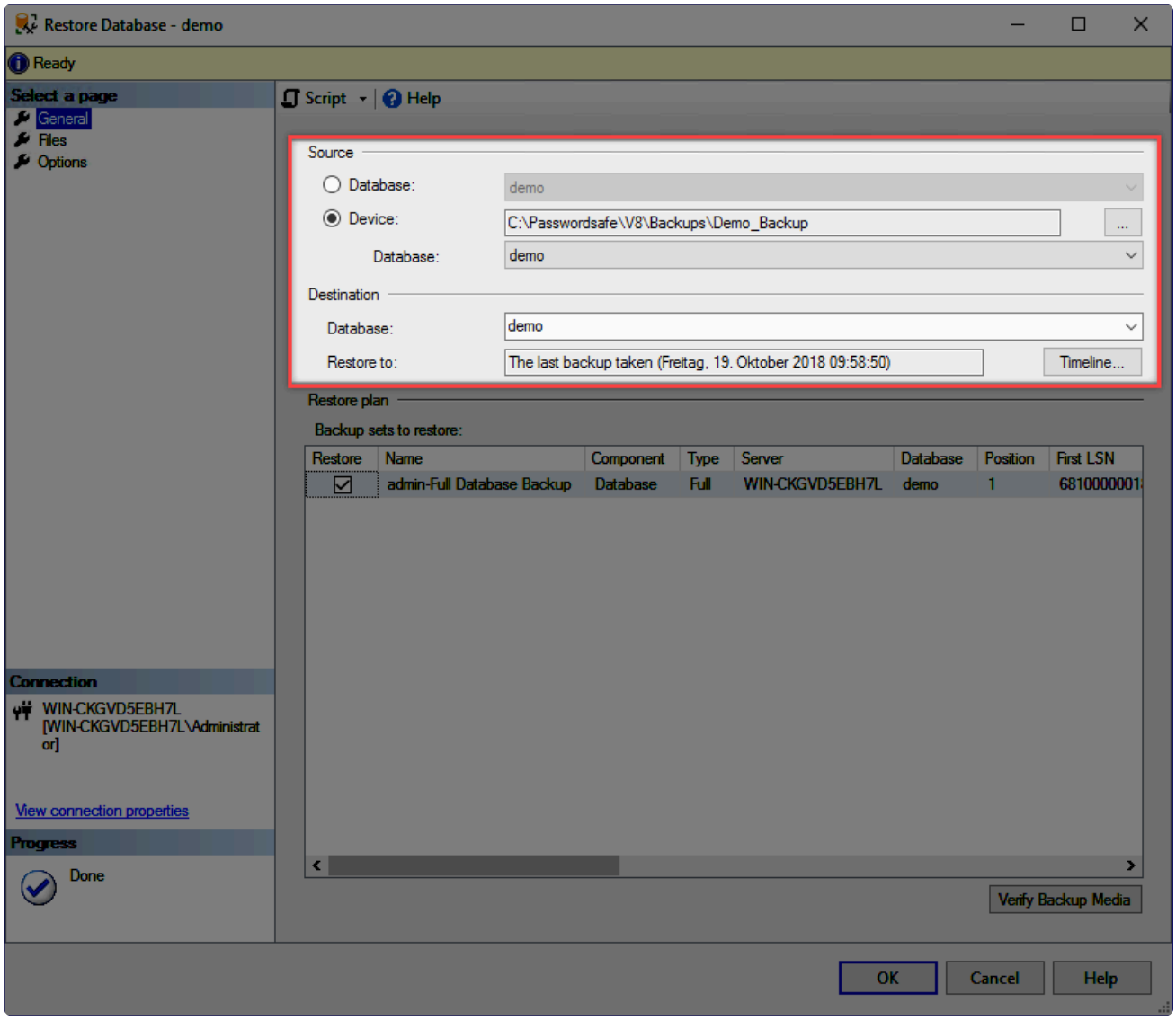
After the backed up data (database and certificate) has been transferred to the new server, it still needs to be integrated.

1. Integrating the database at the SQL level

Firstly, a new database is created on the SQL server. This option can be found in the SQL Management Studio after right clicking on **Databases**. It is usually sufficient to simply enter the database names.



As soon as the database has been created, the option **Restore** (under **Tasks**) can be selected by right clicking on the server. The **Database** is thus selected here. The backup now needs to be selected. It is also essential to check whether the correct database has been selected in the field “Target”.



This method can be also used to import backups that were directly created from the AdminClient.

2. Setting up the server

After the backup has been installed on the new database, you can be start the AdminClient and run the **setup wizard**. The setup wizard is used for (amongst other things) reactivating the licence. It is now possible to enter all of the desired configurations for the server.

3. Importing the certificates

The backed up certificates are imported via the certificate manager.

4. Integrating the database

Finally, the database is integrated onto the server via the **database wizard**.

Modifications on the client

If the IP and/or host name for the server has changed, it is necessary to create/roll out new **database profiles** from the client.

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. The password from the Admin Client should be made available at this point in any case. After the installation of the Admin Client, the database is only accessible when it is activated. If the password is only in the password safe, it should be temporarily stored at this point.

> ✻ 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.

> ✻ When updating to version 8.5.0.14896 or newer please note that **Port 11018** must be opened for the realtime API. Further information can be found in chapter Server System Requirements

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.

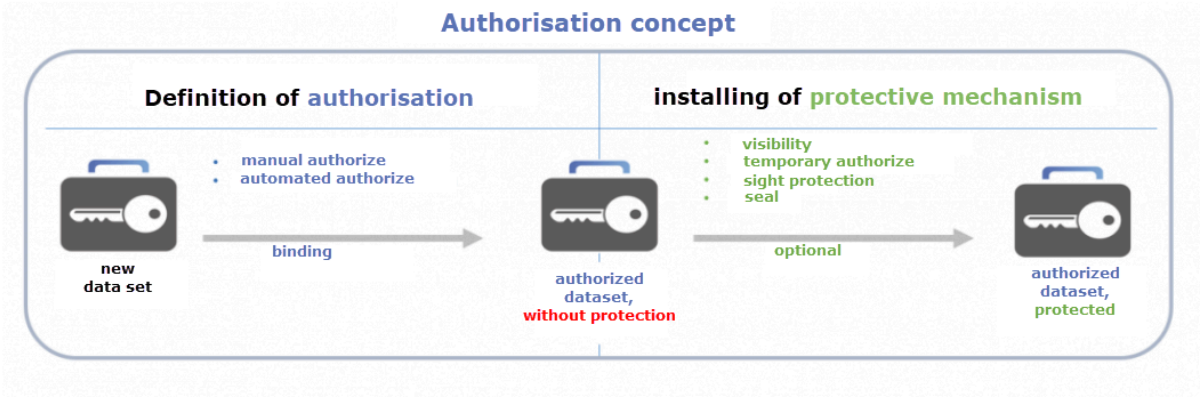
* If the WebClient is used, the module: **proxy_wstunnel** must be installed when using **Apache**. With **IIS** the **WebSocket Protocol** becomes necessary. Further information can be found in the chapter System requirements for WebClient. This applies to version 8.5.0.14896 or newer.

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

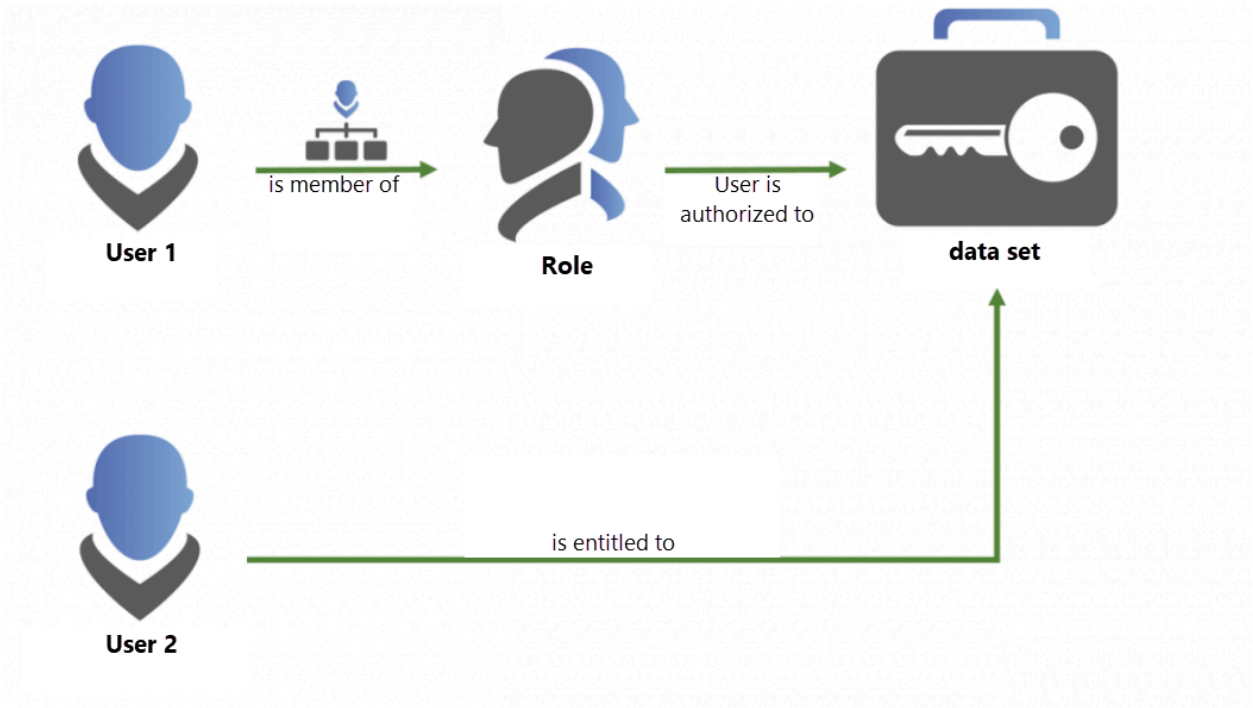
which always apply without exception. Despite the innumerable individual adjustment screws, these basic rules can be summarized in three essential steps.

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.

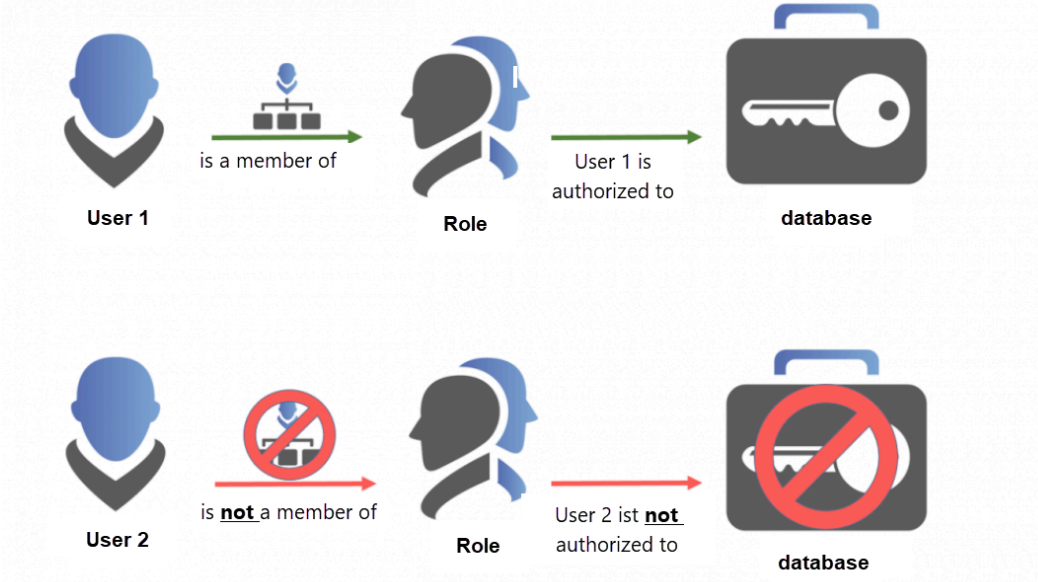


It is obvious to proceed with the organization of accesses using the concept of roles as a basis and only to grant rights individually to employees in exceptional cases. The unplanned absence of personnel must also be taken into account in such concepts. Working with roles defuses such risks significantly.

> Permissions are always granted to only one user or role!

2. Membership in roles

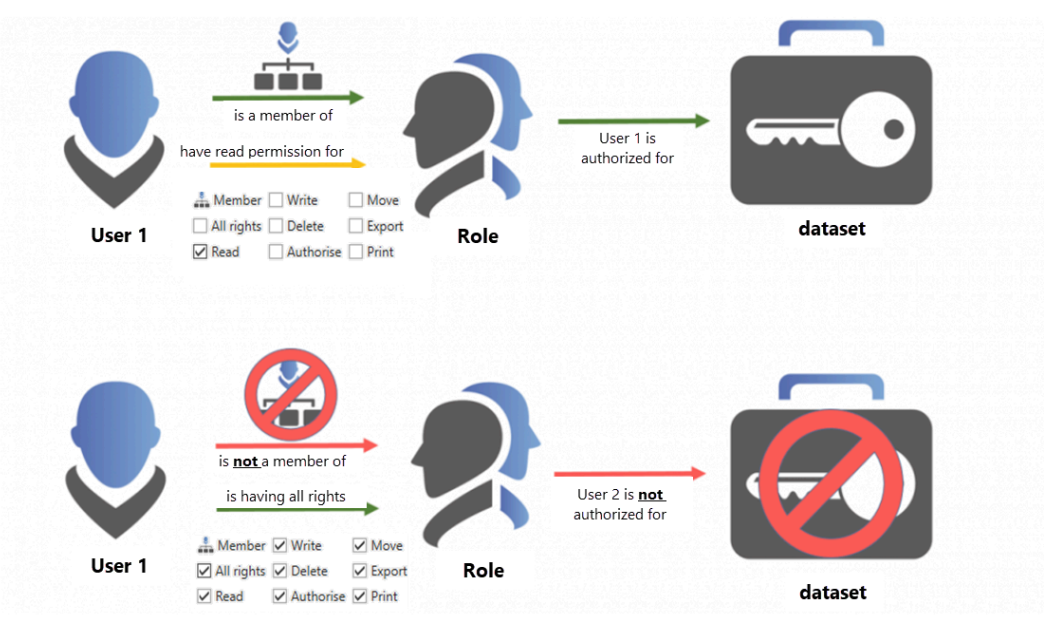
The key point is membership in a role. If an employee can use the authorizations according to the roles assigned to him, * he must be a member of the role *. Only members see the records that have been authorized for the role.



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.

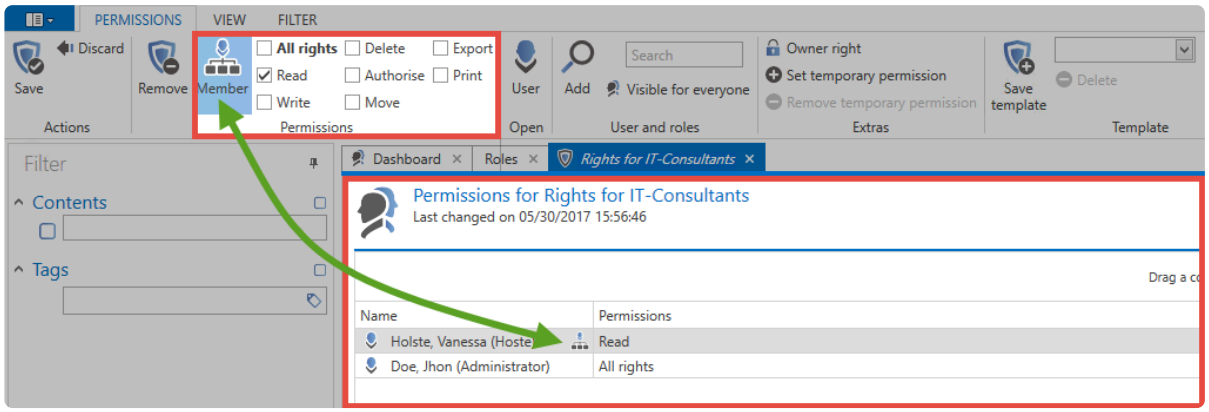
- **User 2** has all rights for the role. It can add additional users to the role by means of “authorise”. The crucial point, however, is that it is not a member of the role. It cannot, therefore, see any records for which the role is authorized.

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.

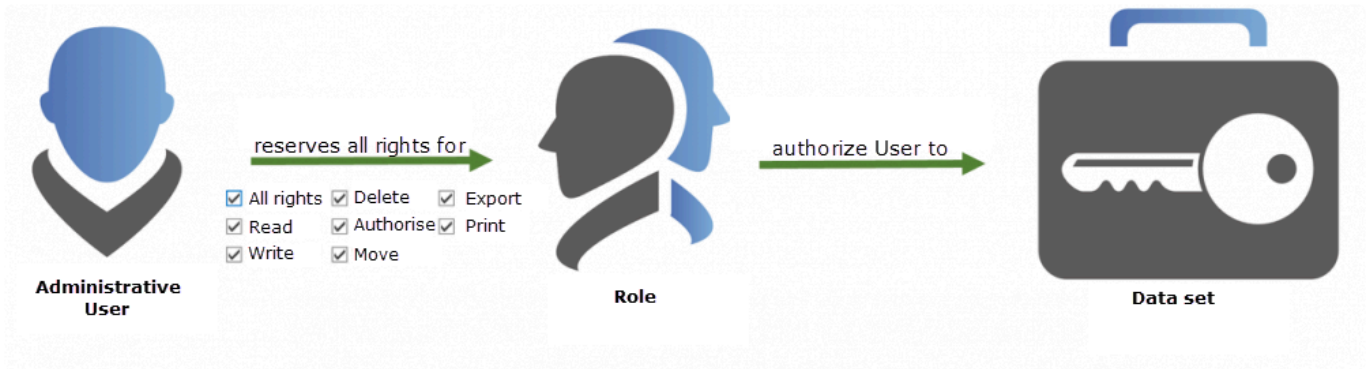
As a member of a role, it must have at least the “read” right for the role!

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.



- 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

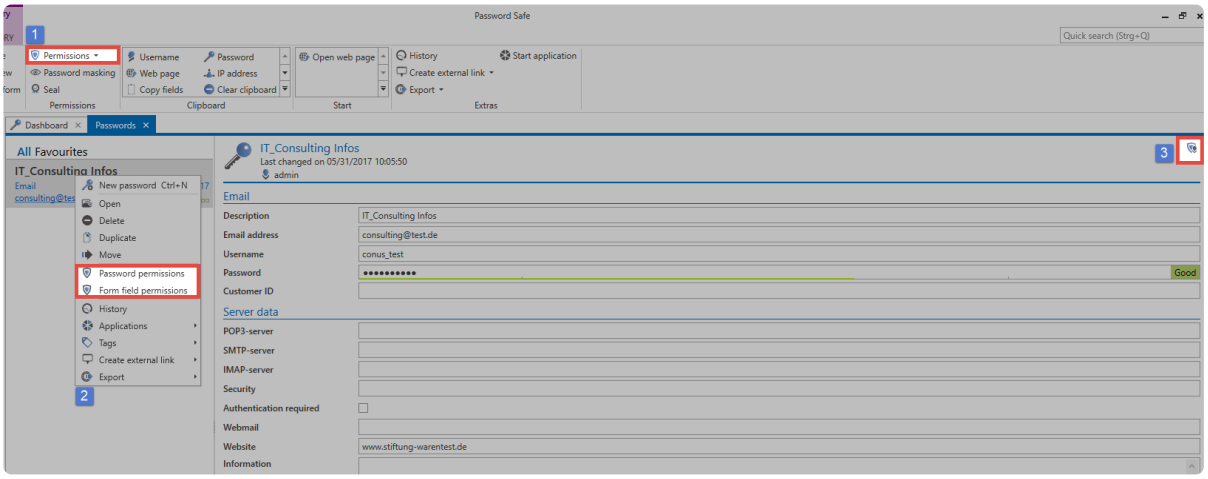
What is the manual setting of permissions for records?

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

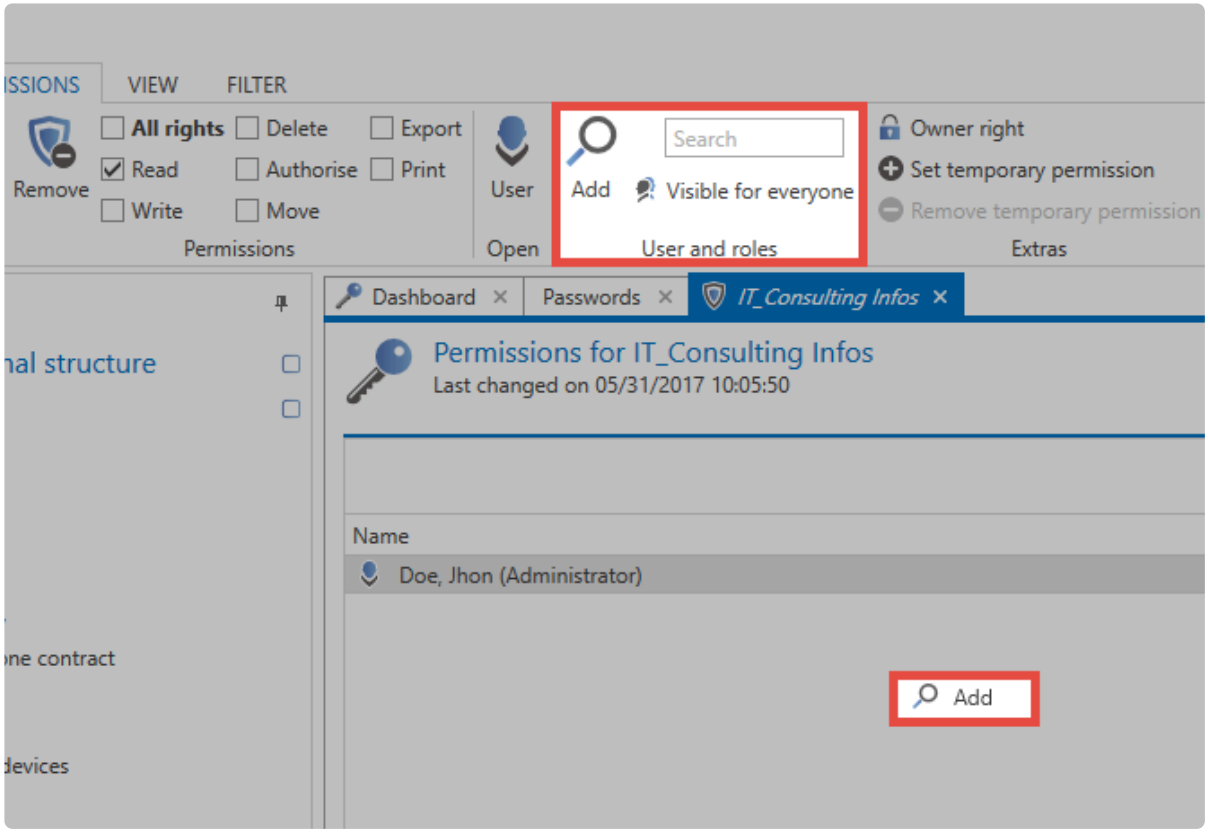
In the previous section, it was clarified that permissions for records are granted either directly to one user or to several users grouped in a role. With this knowledge, the permissions can as such be set manually for a record. In the Passwords client module, you can access the permissions in the list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

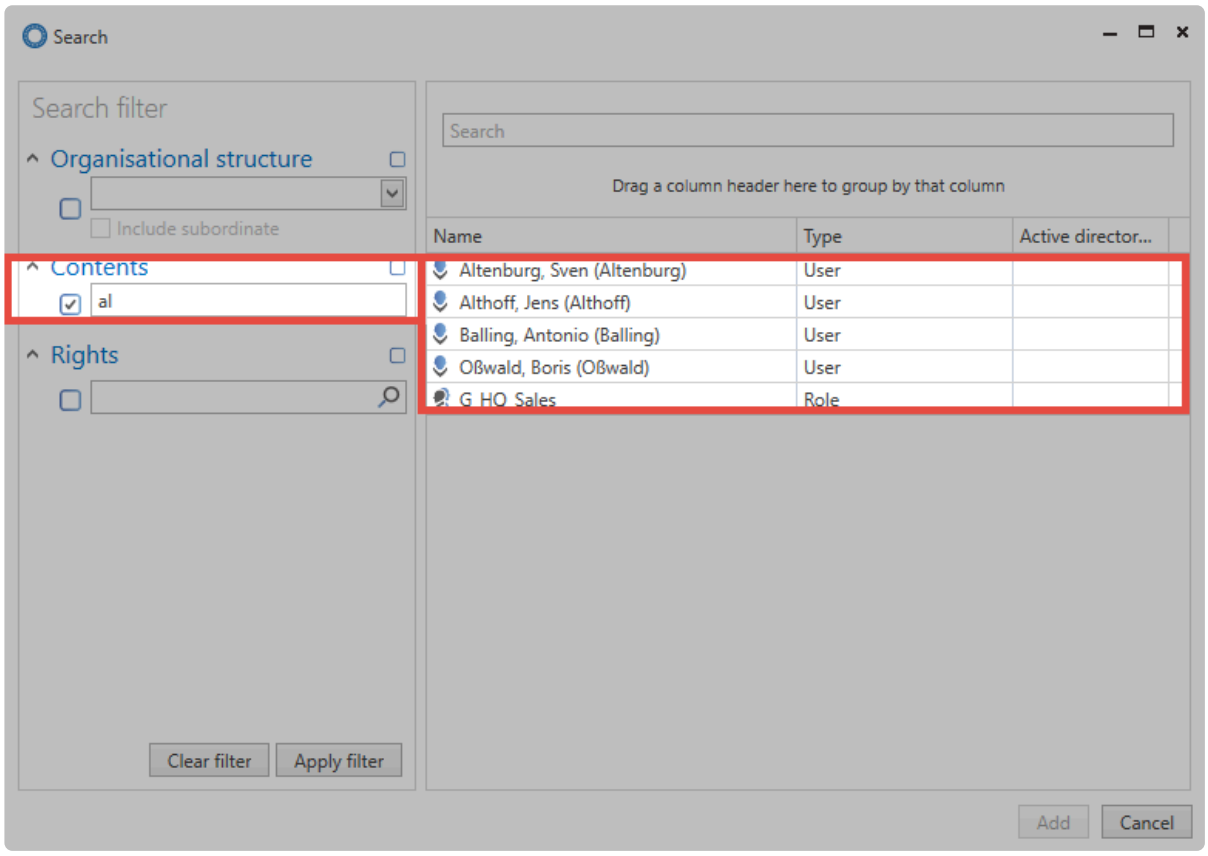


> The icon on the right of the reading pane reveals “mouseover” the information whether the record is personal or public. In case of personal data records, the user that is logged on is the only one who has permissions!

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.



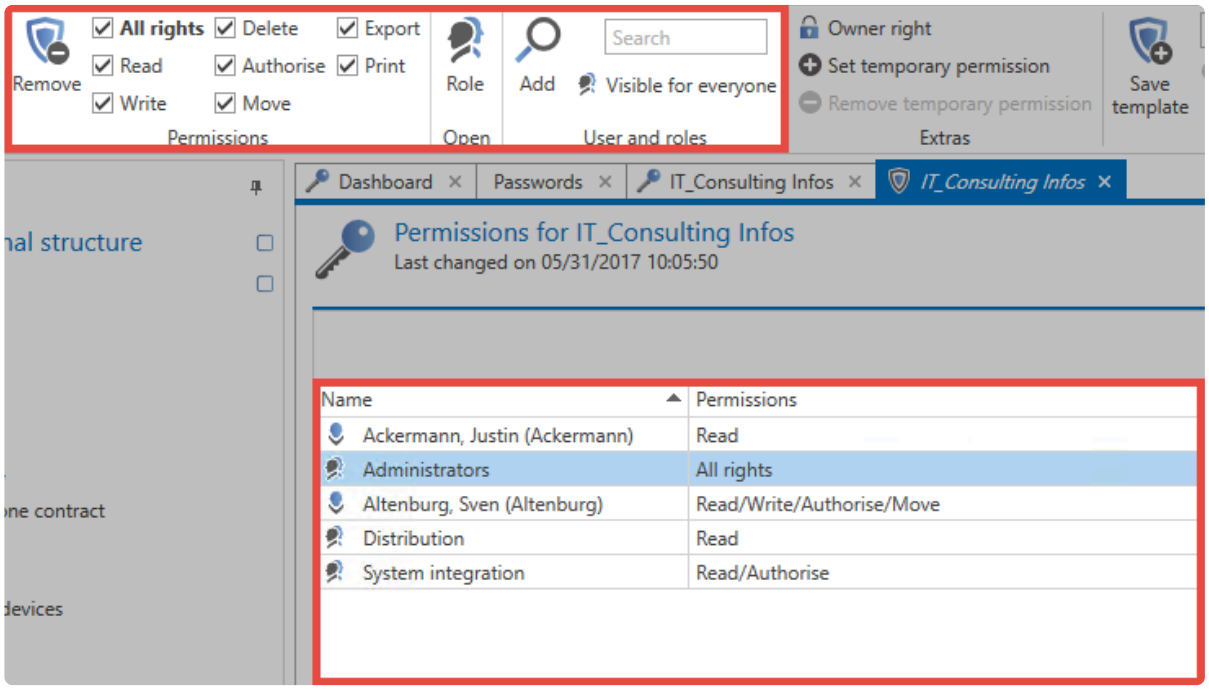
The search filter opens in a separate tab. The filter can be configured as usual. The search is similar to the search in the list view.



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

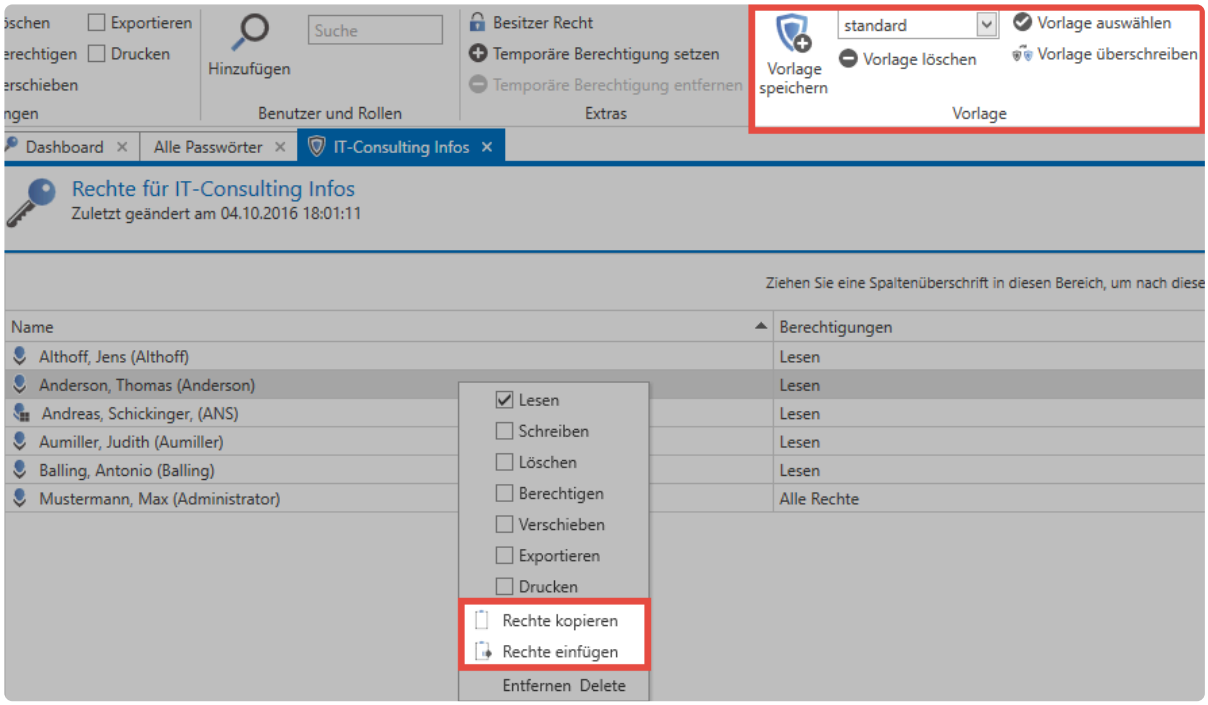
Setting and removing permissions

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.



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.



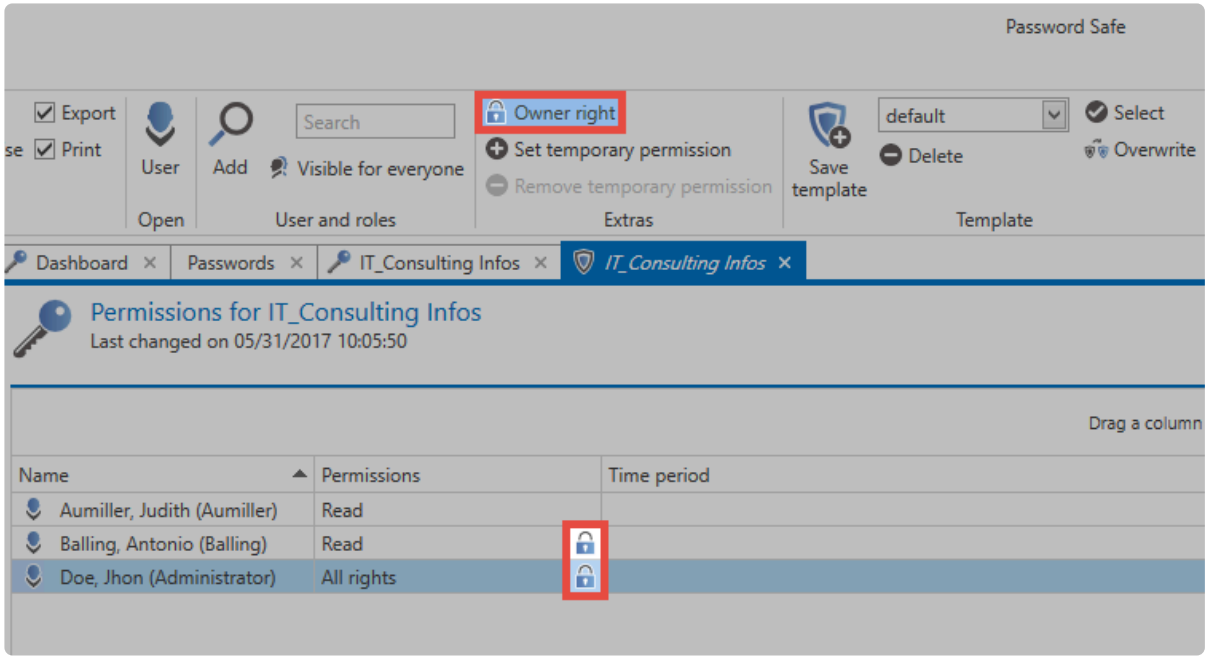
The transfer of rights and their reuse can be an important building block to create and maintain entitlement integrity. This method cannot rule out misconfigurations, but it will minimize the risk significantly. Of course, the correct configuration of these templates is a prerequisite.

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. This is only possible by the user or the role itself, as well as by users with the right “Is database administrator”.



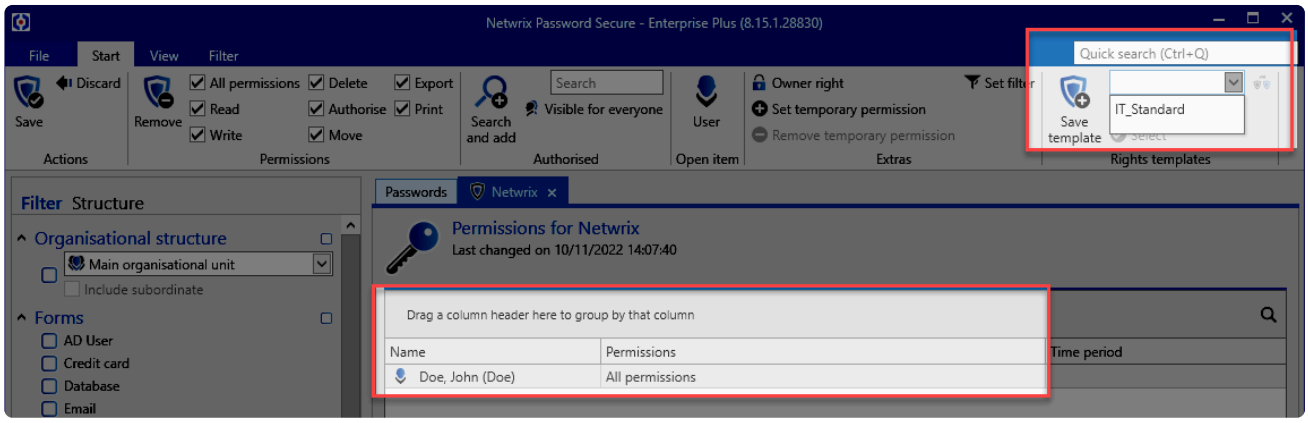
The owner right thus prevents other users who have the “Authorise” right from removing any users from the record.

> ! 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.



> 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.

Relevant rights

This mode is inactive by default and firstly needs to be activated.

User right

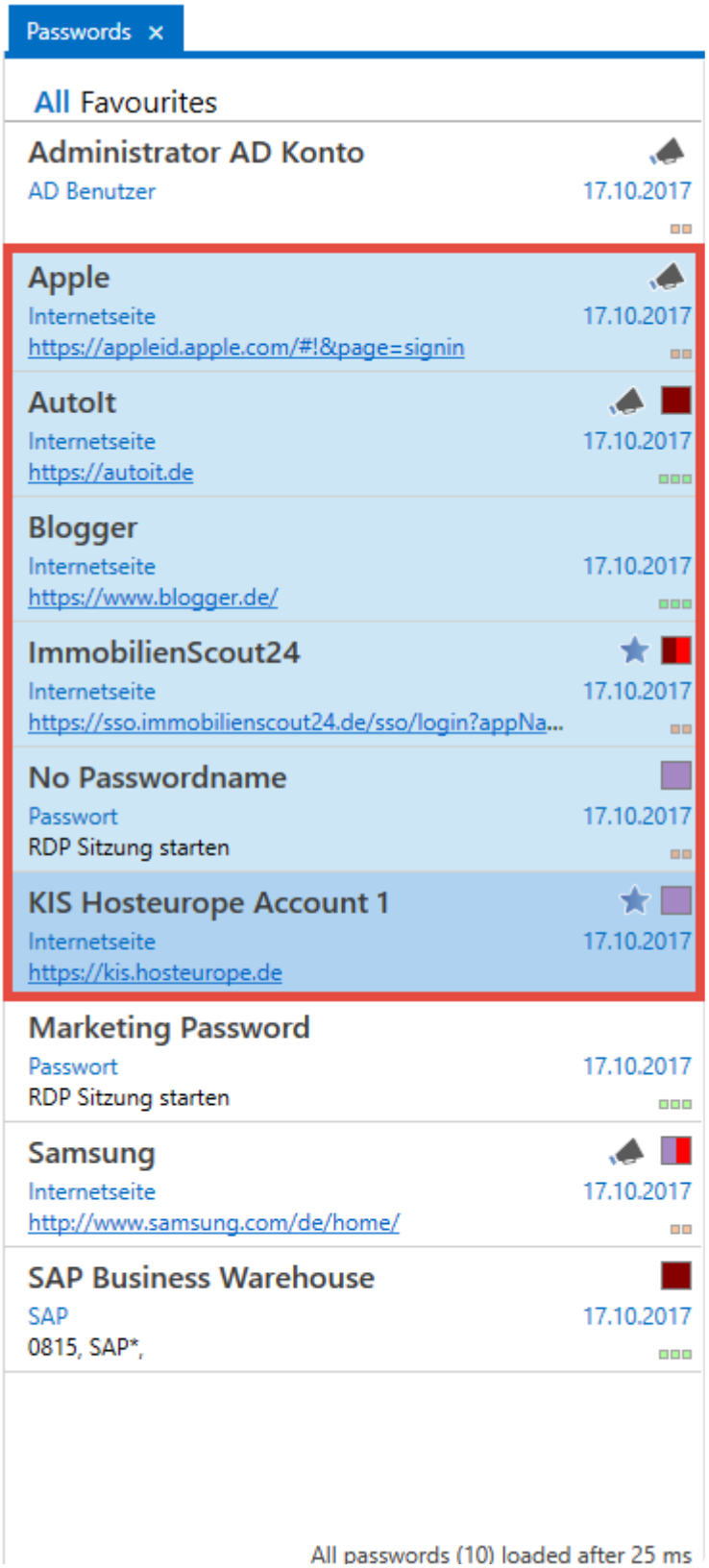
- Can carry out batch processing for permissions based on a filter

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.

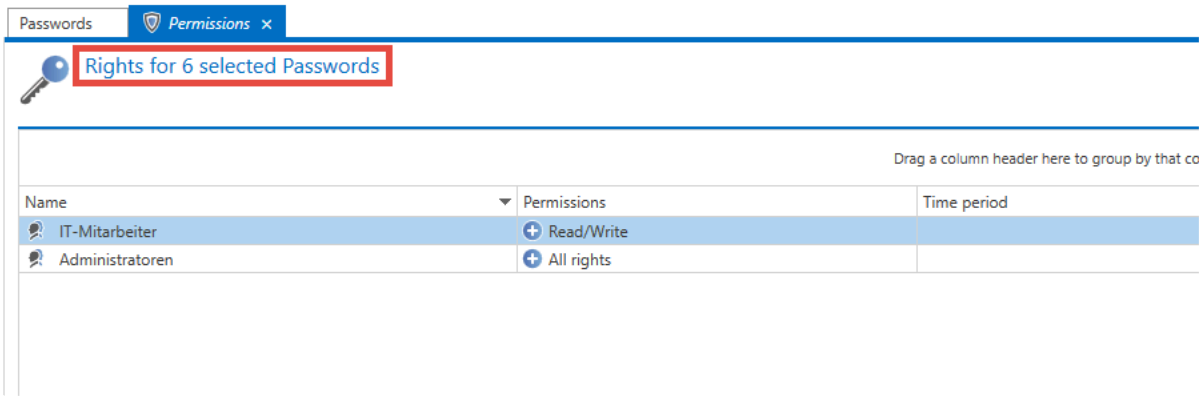
Selecting the records

In list view, 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.



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.



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.

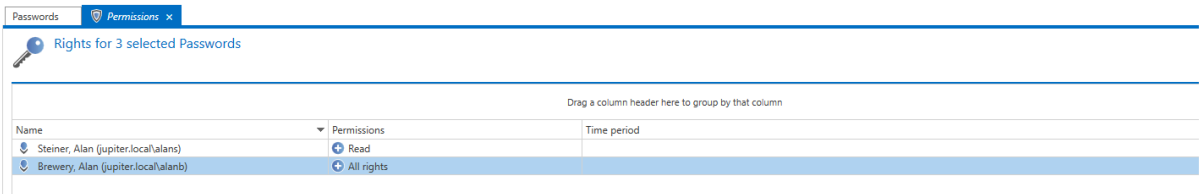
Reducing rights / removing users and roles from the permissions

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.

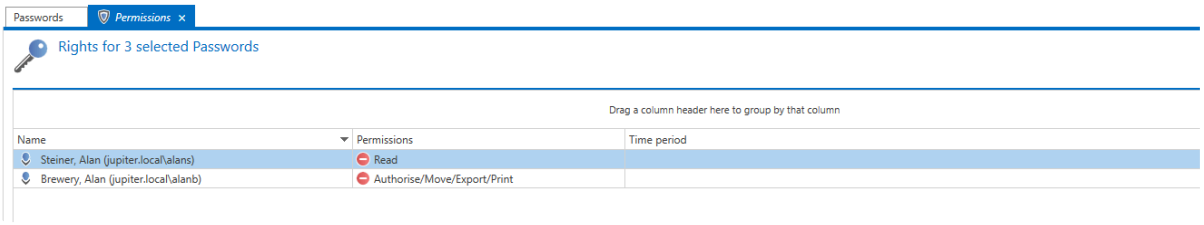
If the **read** right is to be removed for a user or role, the user will be completely removed from the permissions.

Examples

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

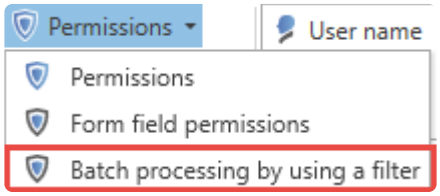


The read right will be removed here for Mr. Steiner. As removing the read right means that no other rights exist for the record, Mr. Steiner is completely removed from the permissions. The authorize, move, export and print rights are being removed from Mr. Brewery. Assuming that he previously had all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



Batch processing using a filter

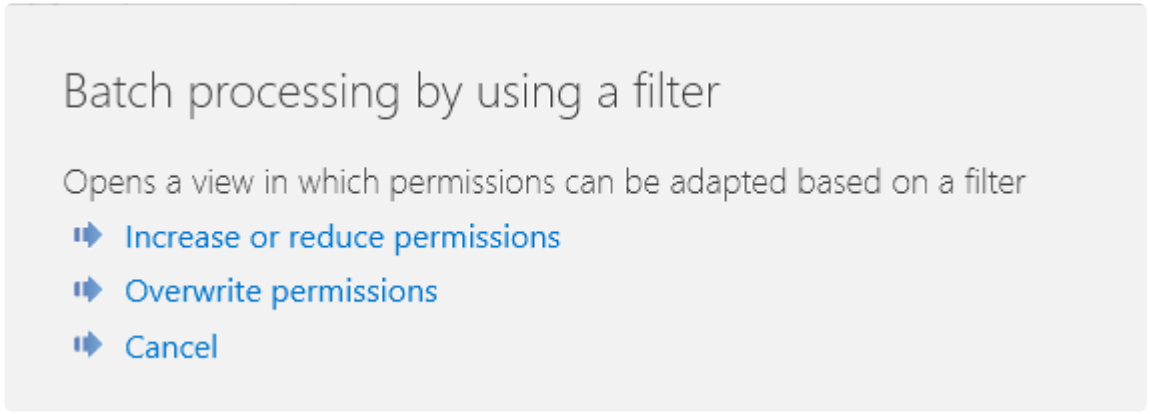
In some cases it is necessary to edit the permissions for a very large number of records. On the one hand, a maximum limit of 1000 records exists and on the other had, handling a very large number of records via list view is not always the best solution. The **Batch processing using a filter** mode has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



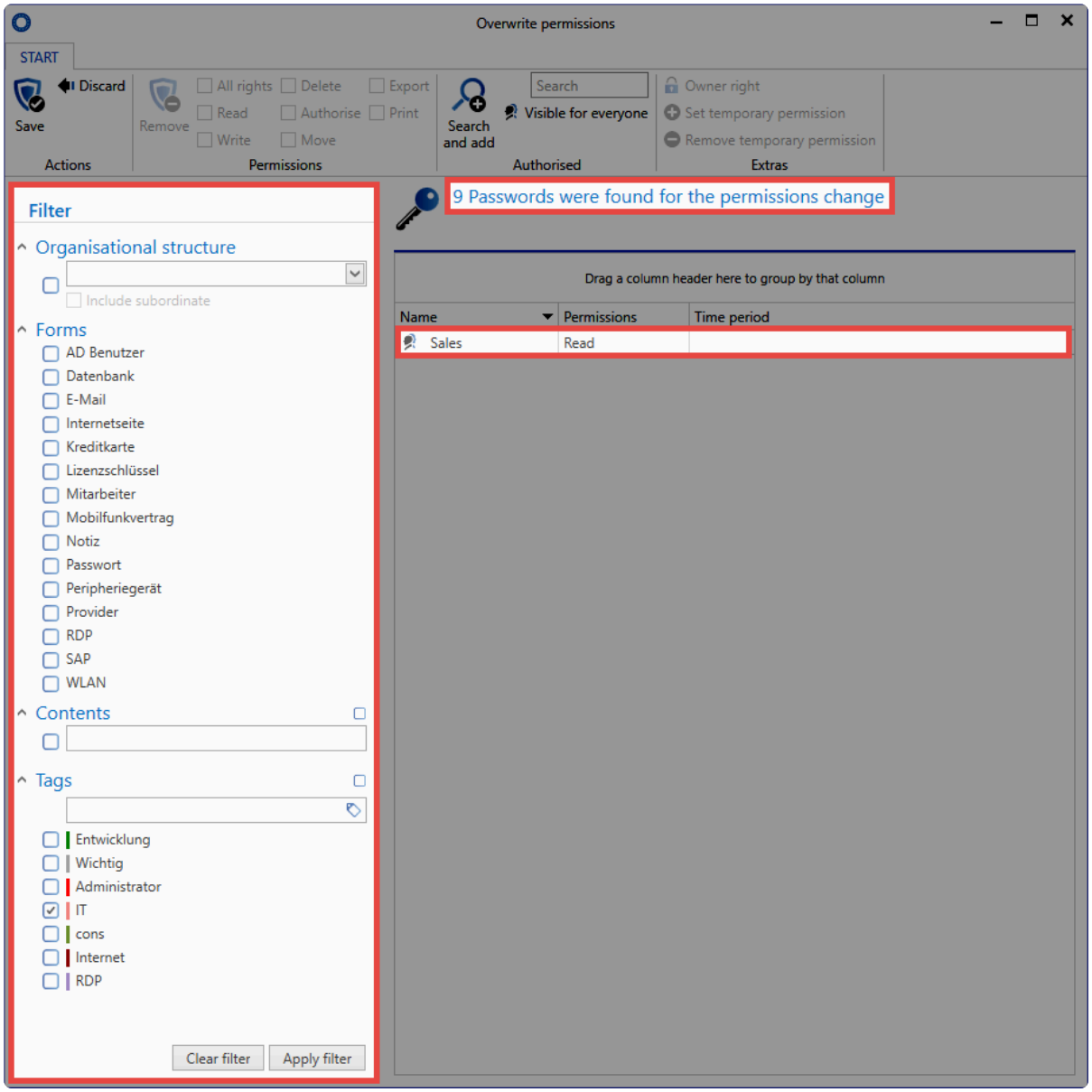
In the subsequent dialogue, you define whether you want to expand, reduce or completely overwrite existing permissions. If you select **expand or reduce** at this stage, the same logic as for **editing via list view** is used. No rights will thus be overwritten.

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.

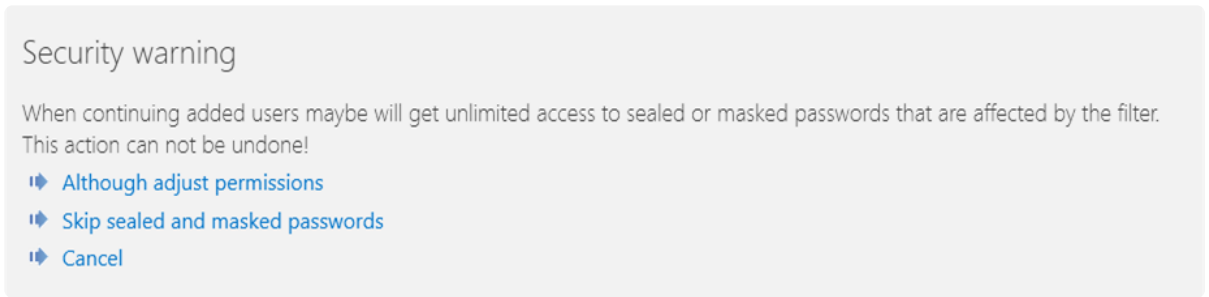


The filter itself defines the selection criteria for the records to be edited. The currently configured filter will be used as default. The records that will be affected by the changes are also not displayed in this view. Only the number of records is displayed. In the following example, 9 passwords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

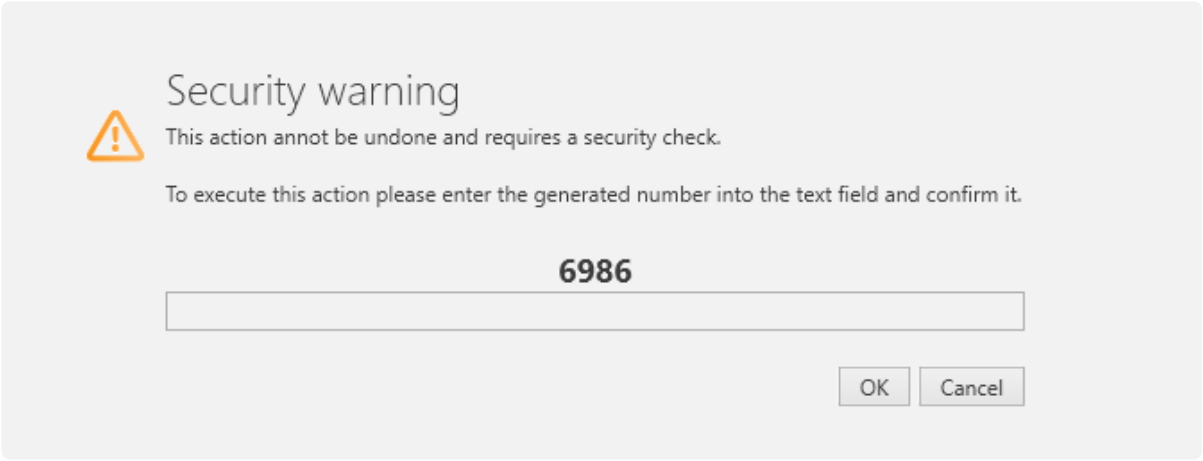


Seals and password masking

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.



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.



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

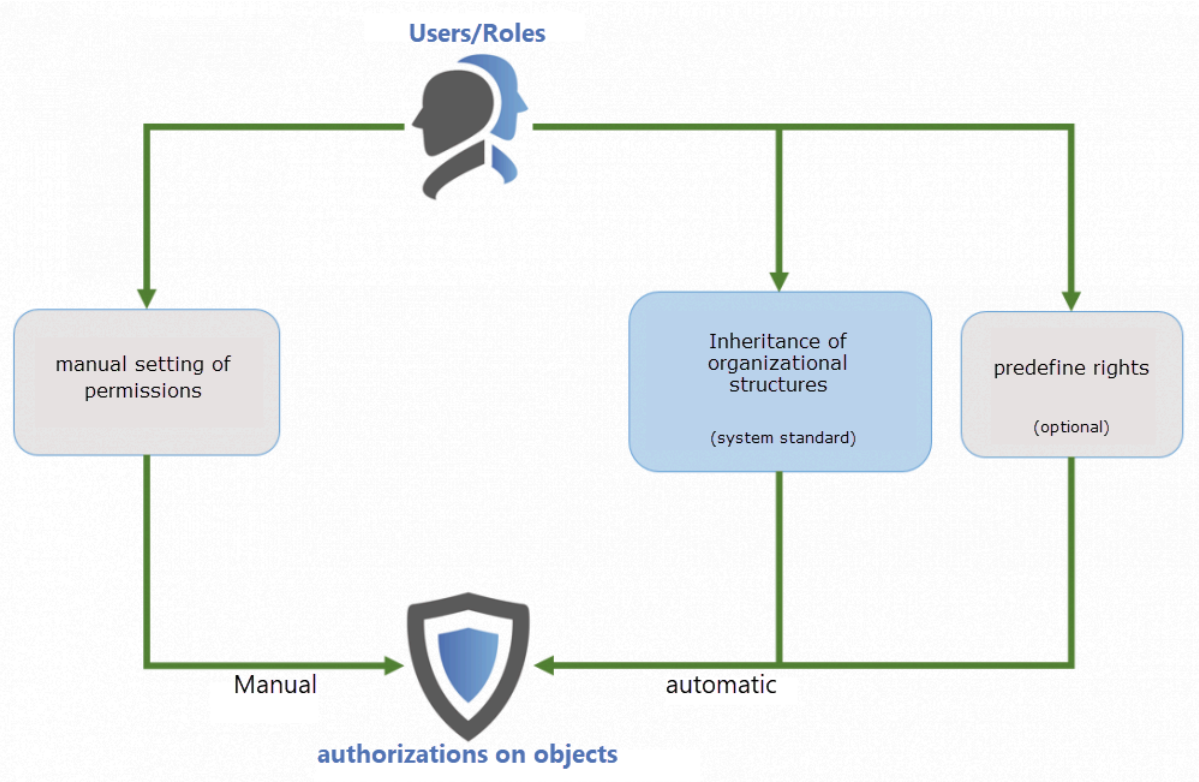
Reusing permissions

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?**

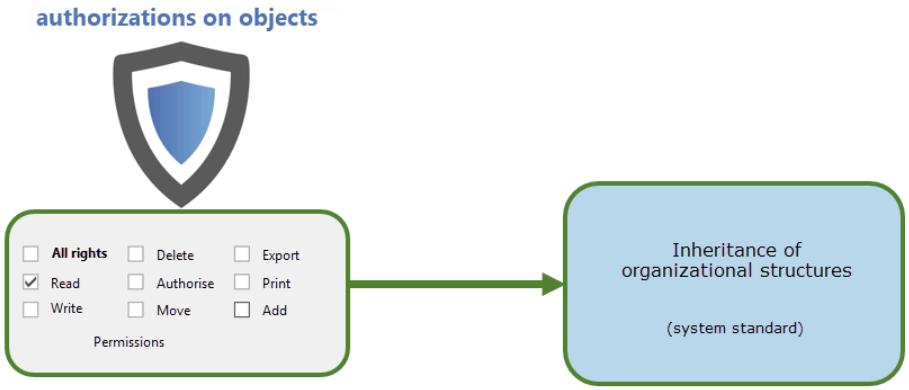


Inheritance from organisational structures is defined by **default** in the system. This can be configured in the settings. The relevant setting is “Inherit permissions for new objects (without rights template)”. “Further info…”:#vererbung-aus-organisationsstrukturen

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 already 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. It can be configured in more detail using two settings.

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

Inherit permissions for new objects (without rights template)

This setting is relevant for **newly created** records.

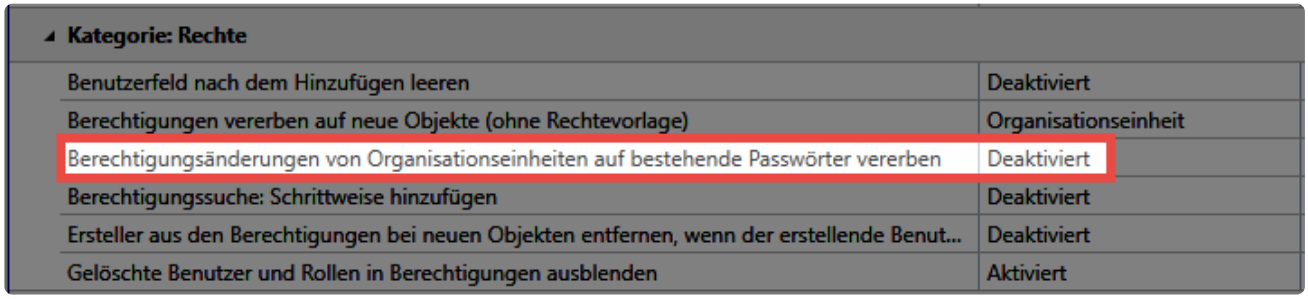


The following values can be configured:

- **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. This setting is **active by default**.
- **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.

Existing passwords inherit changes to the permissions for organisational units



This option means that changes to permissions for an organisational unit will be inherited by all passwords for this organisational unit. This setting is **active by default**. When inheriting permissions, a dialogue will be displayed that offers you the following options:

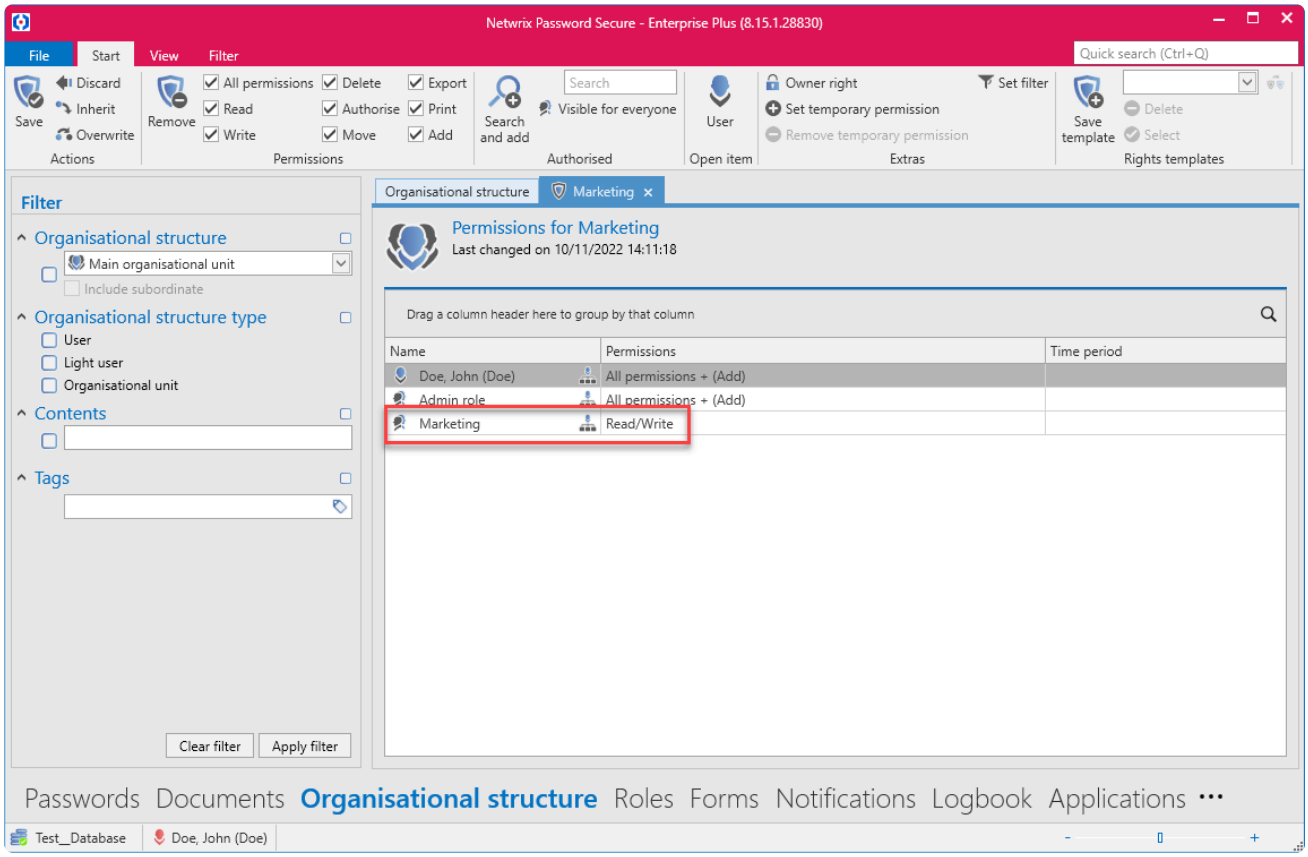
- **Increase or reduce permissions**: The permissions for the passwords are retained and are only increased or reduced by the change.
- **Overwrite permissions**: The permissions for the passwords are completely overwritten. This means that all permissions for a password are firstly removed and then the new permissions for the organisational unit are inherited.
- **Cancel inheritance**: The permissions are not inherited but are only changed in the organisational unit.

> The permissions are only inherited by existing passwords within the organisational unit. Therefore, the permissions are not inherited downwards throughout the entire structure.

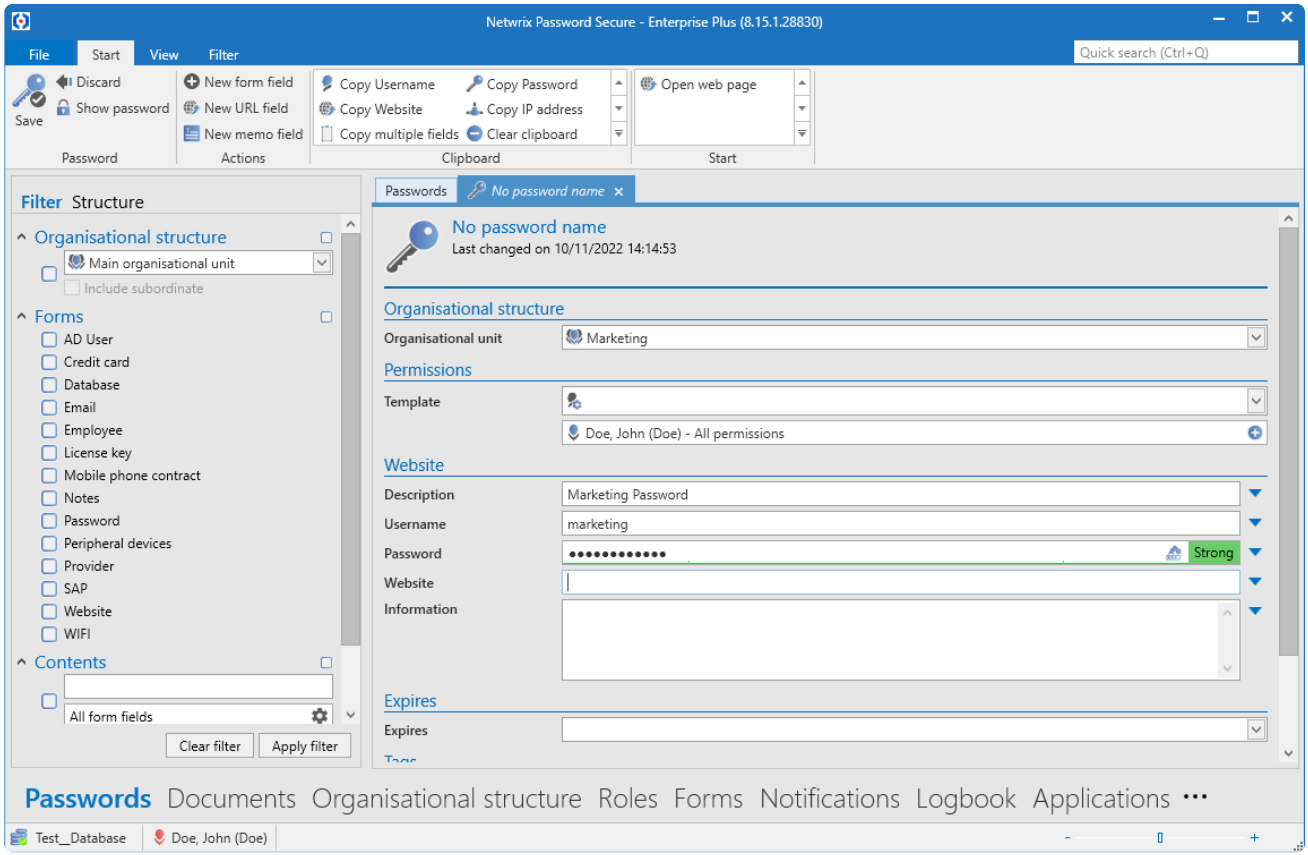
Example case

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.

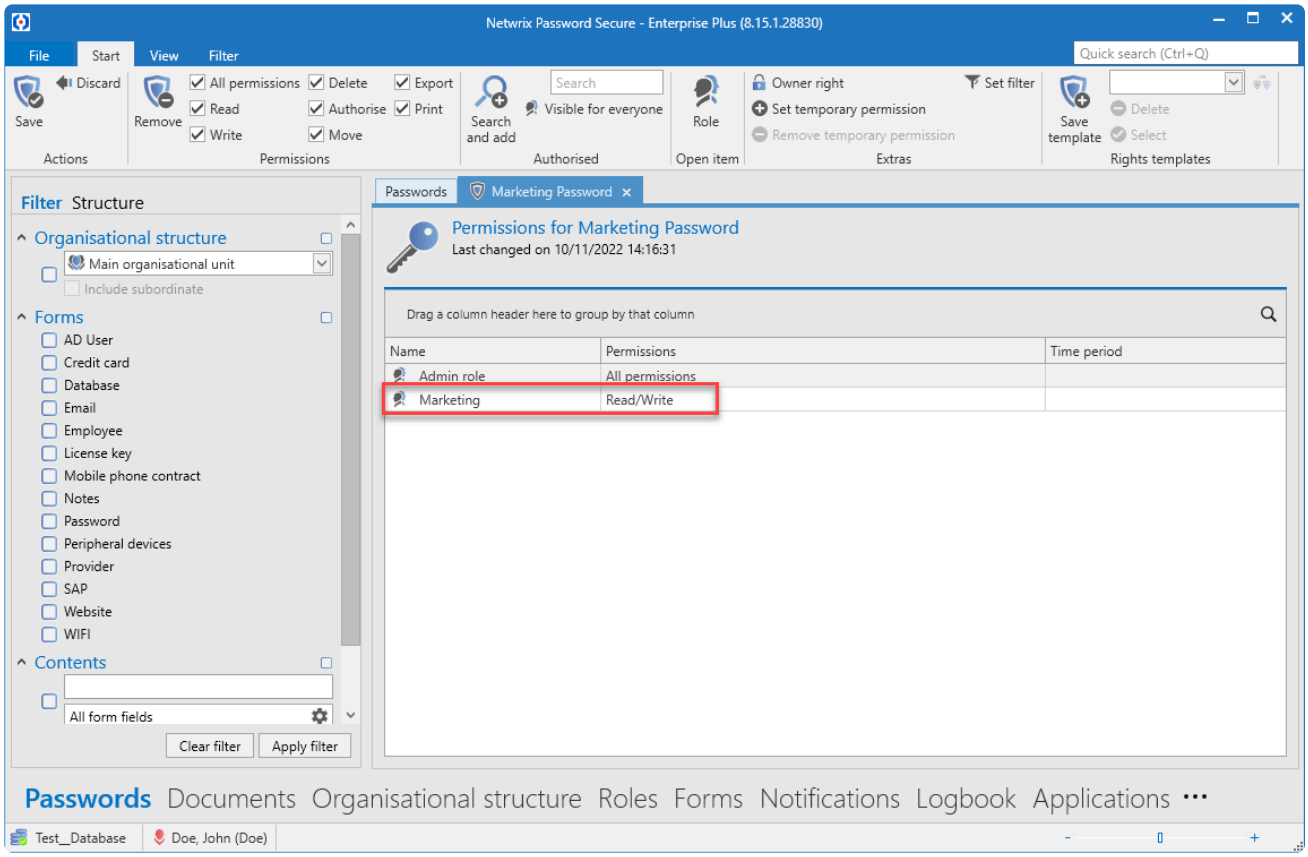
The permissions for the organisational unit “marketing” are shown below:



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



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

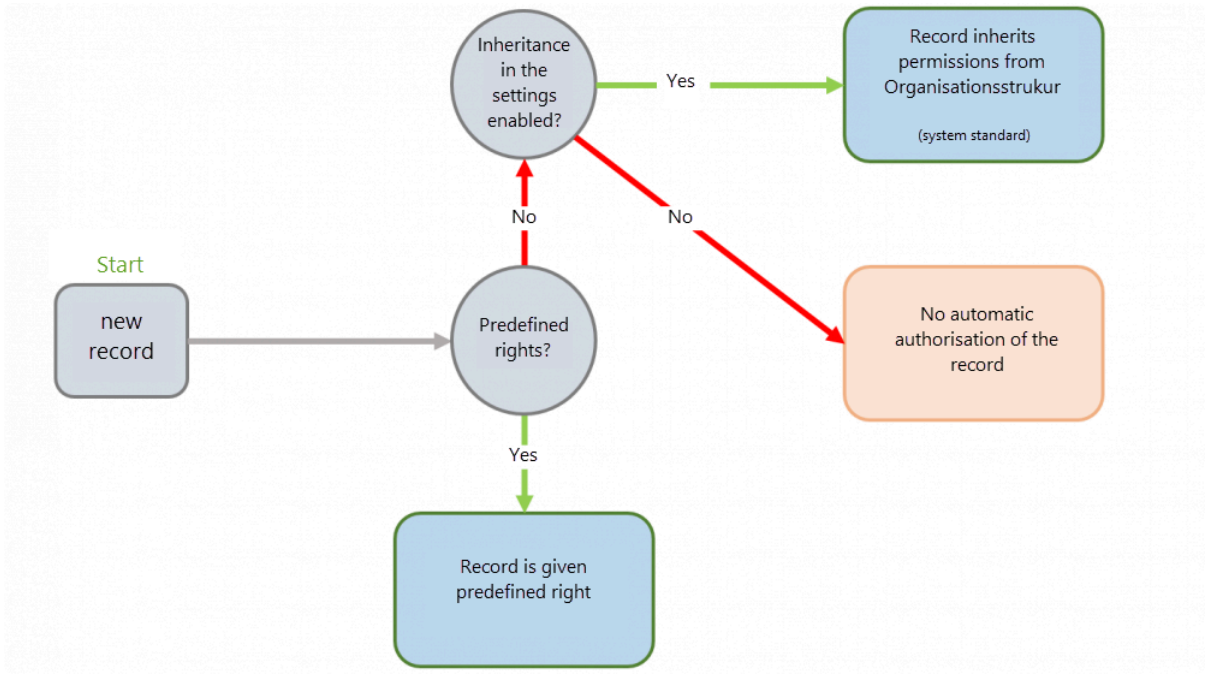


Conclusion

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:



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.

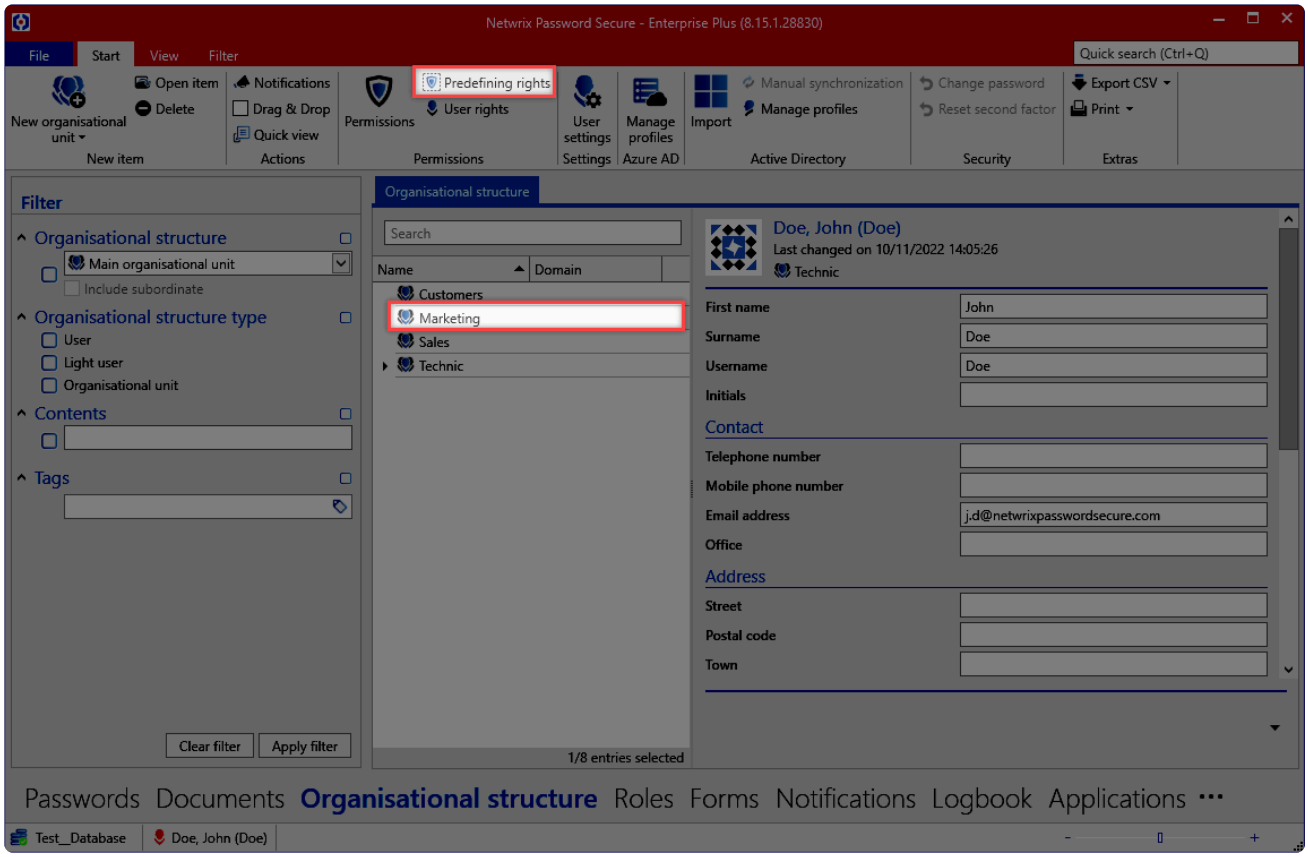
Organisational structures as a basis

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:

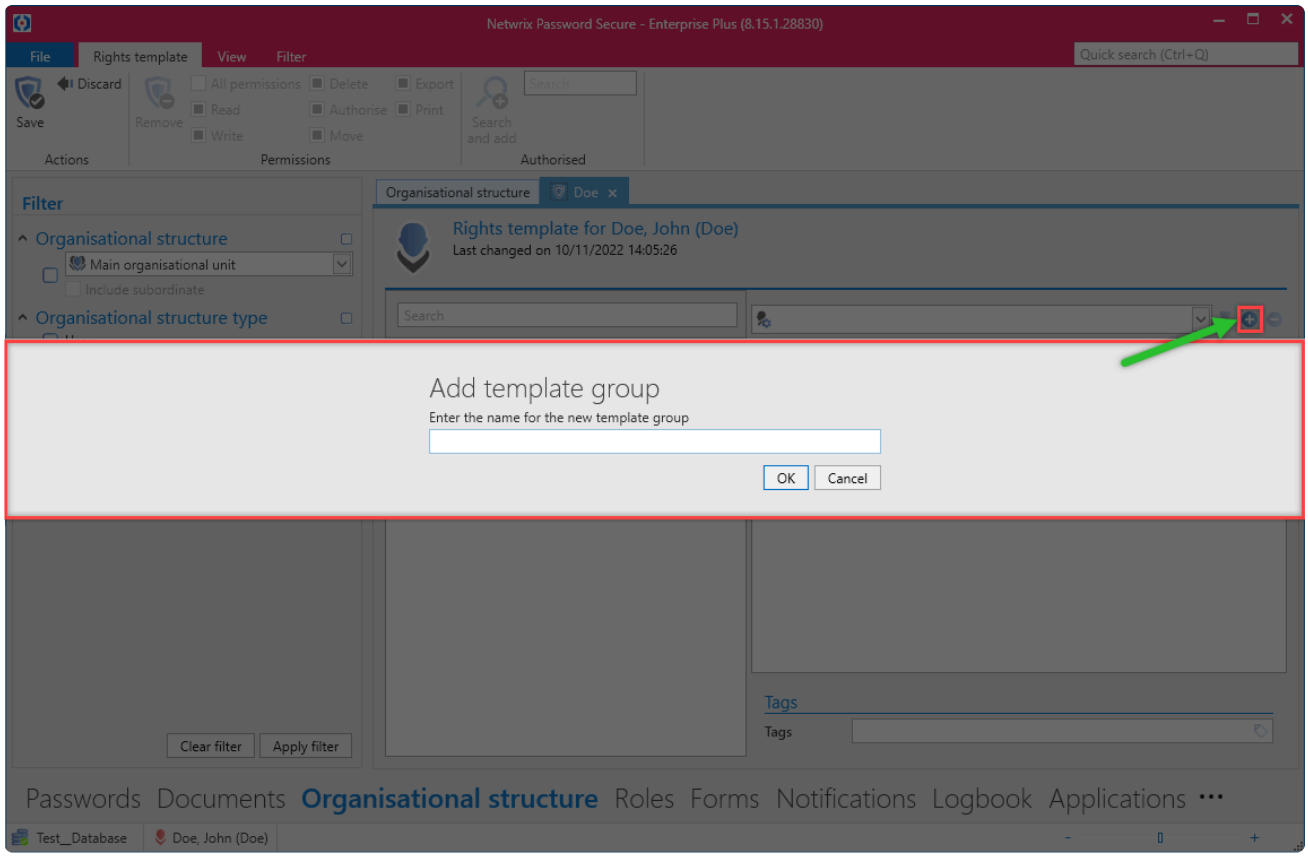
- **IT employee**
- **IT manager**
- **Administrator**

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.

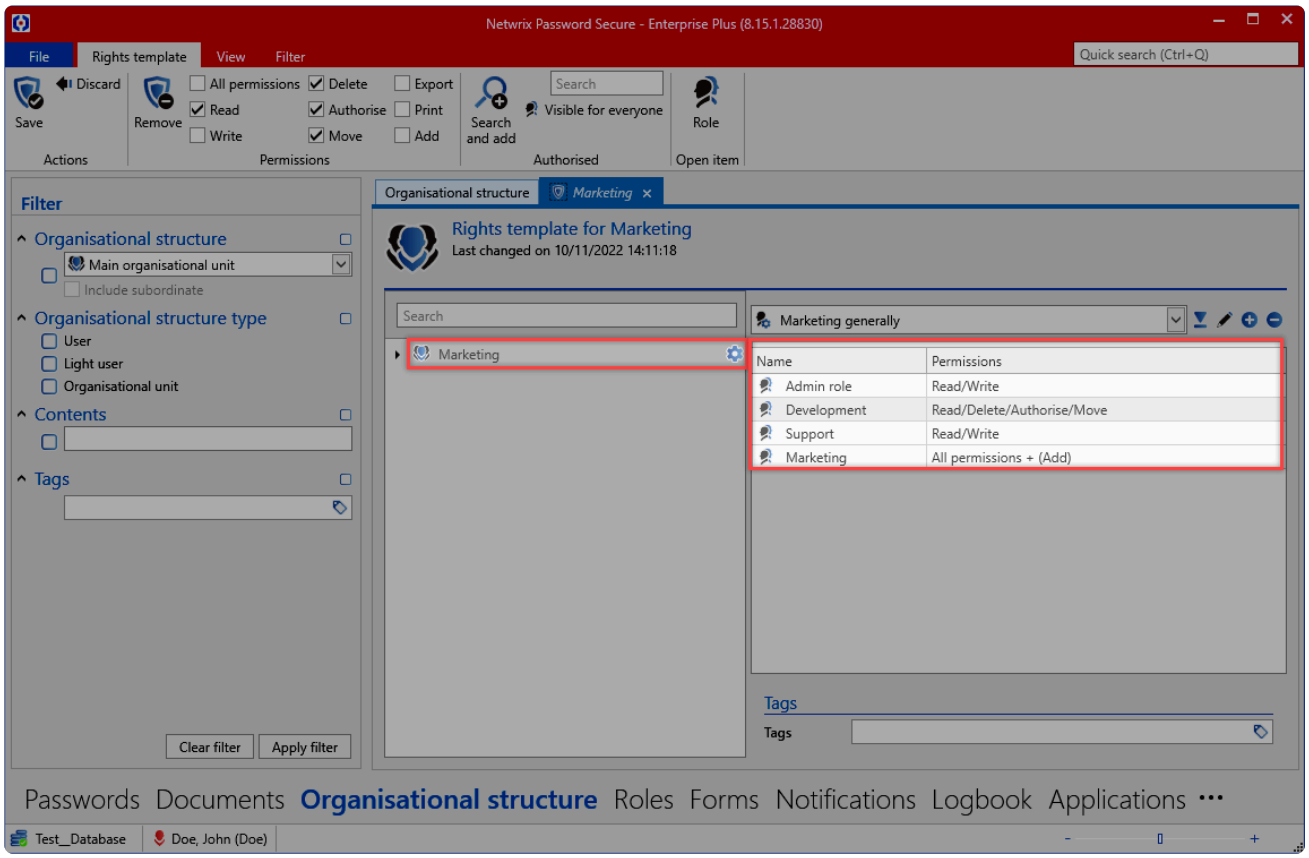


- **Creating the first template group:** A modal window will appear after clicking on the icon for adding a new template group (green arrow) in which a meaningful name for the template group should be entered.



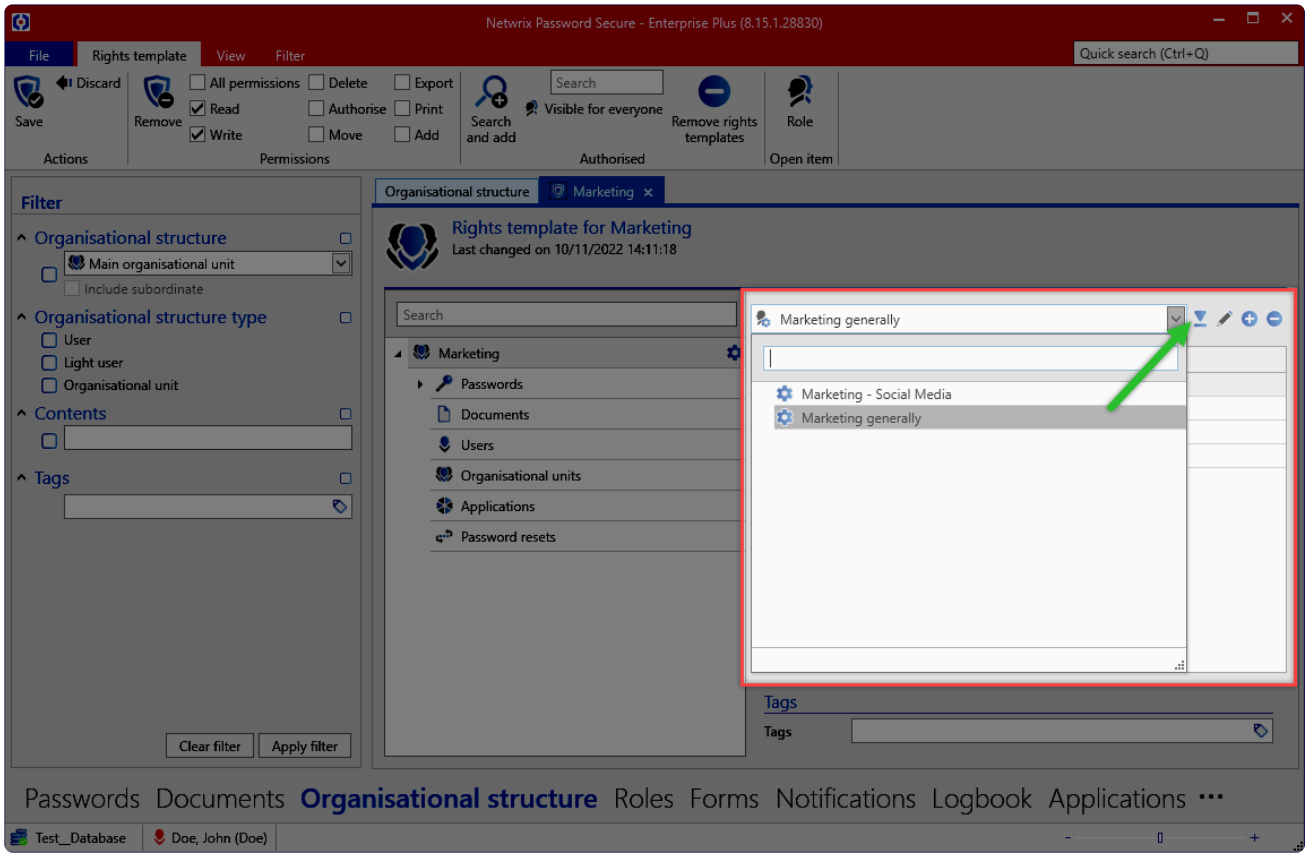
Roles and users can now be added to this template both via the ribbon and also via the context menu

(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.



Adding other template groups

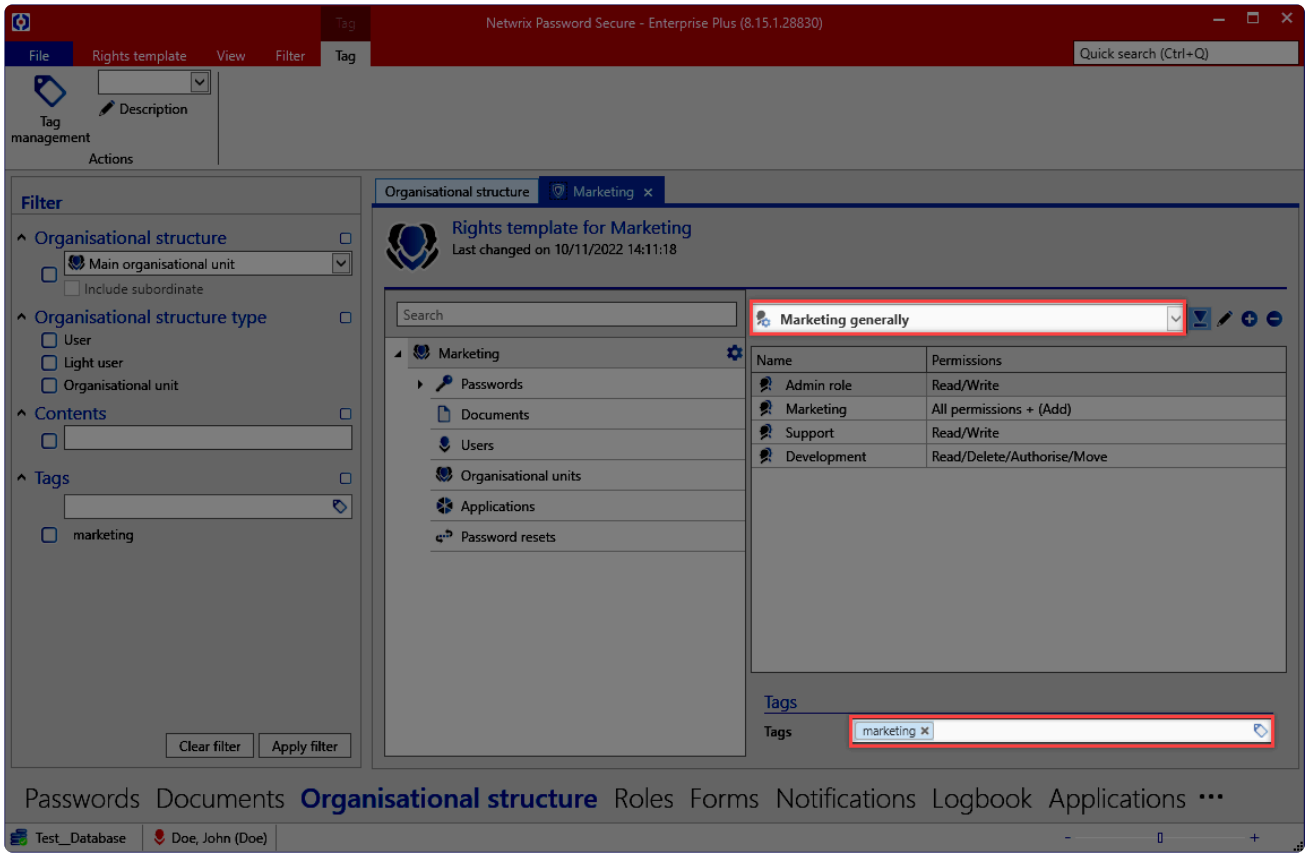
It is also possible to configure several different rights templates within one department. This may be necessary e.g. if there are several areas of competency within one department which should each receive different permissions. Alongside the **IT general** area, the template groups **Exchange** and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



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.

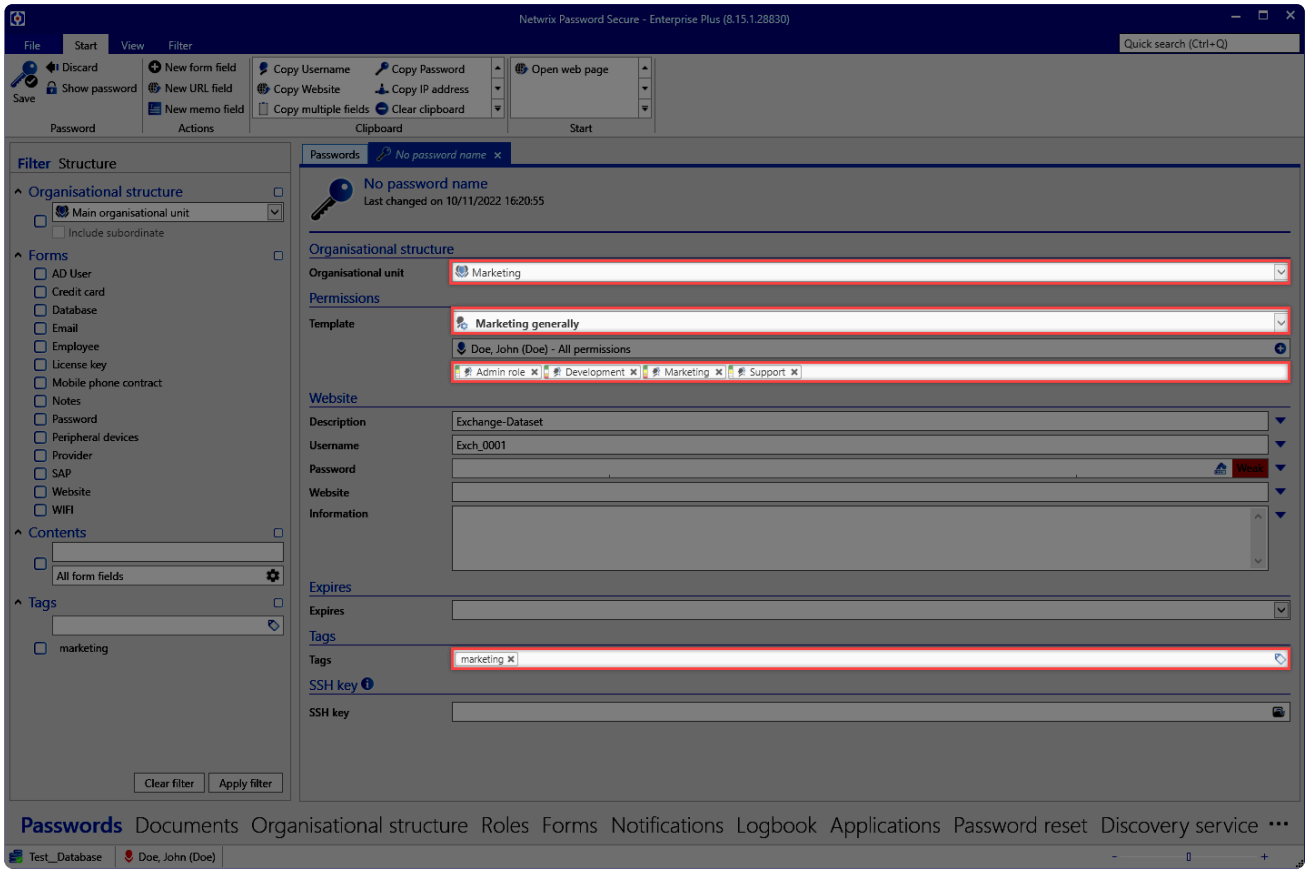
Working with predefined rights

Using predefined rights when creating passwords

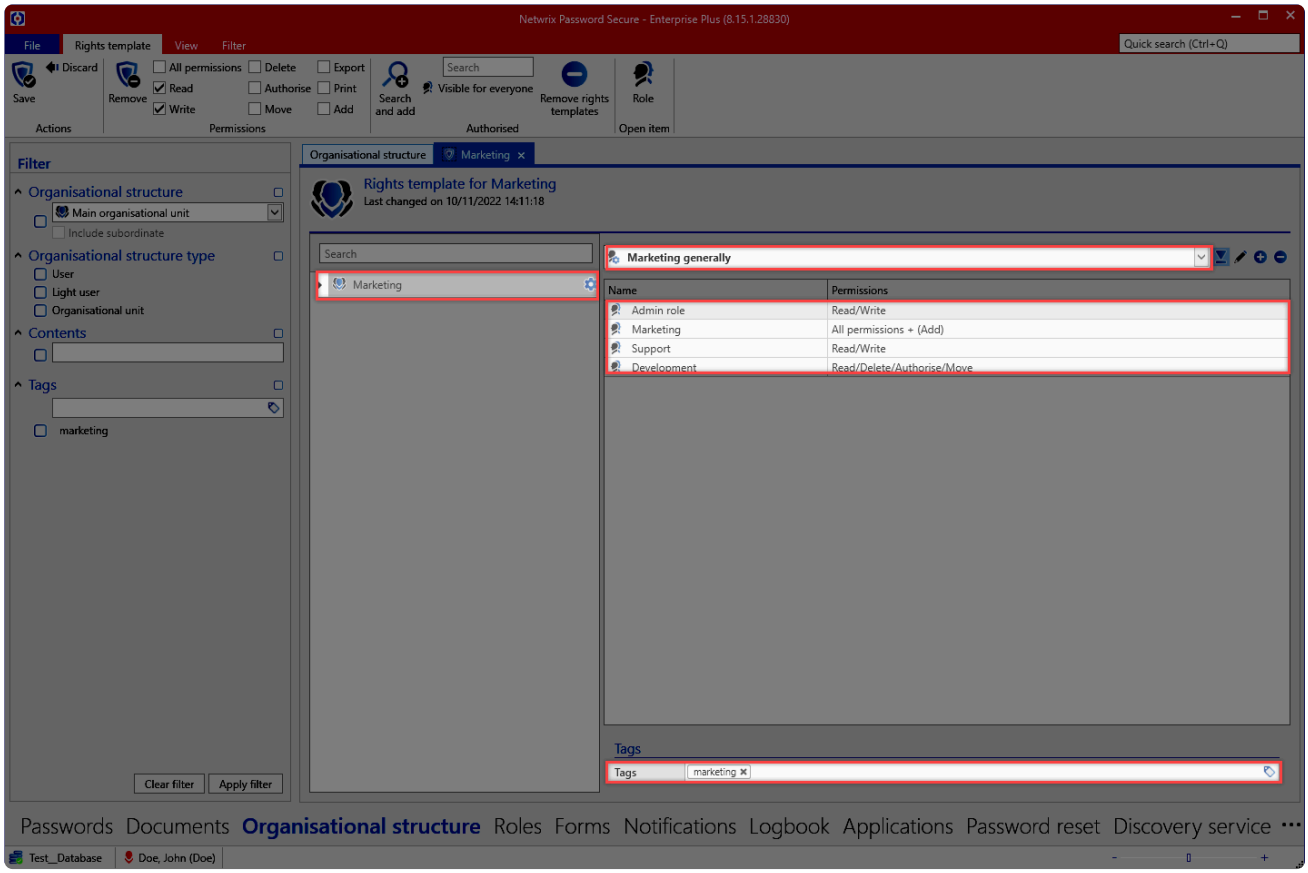
After you have preconfigured the rights, you can then use them to create new records. Proceed here as follows:

- 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.



Here is the underlying rights template as a comparison:



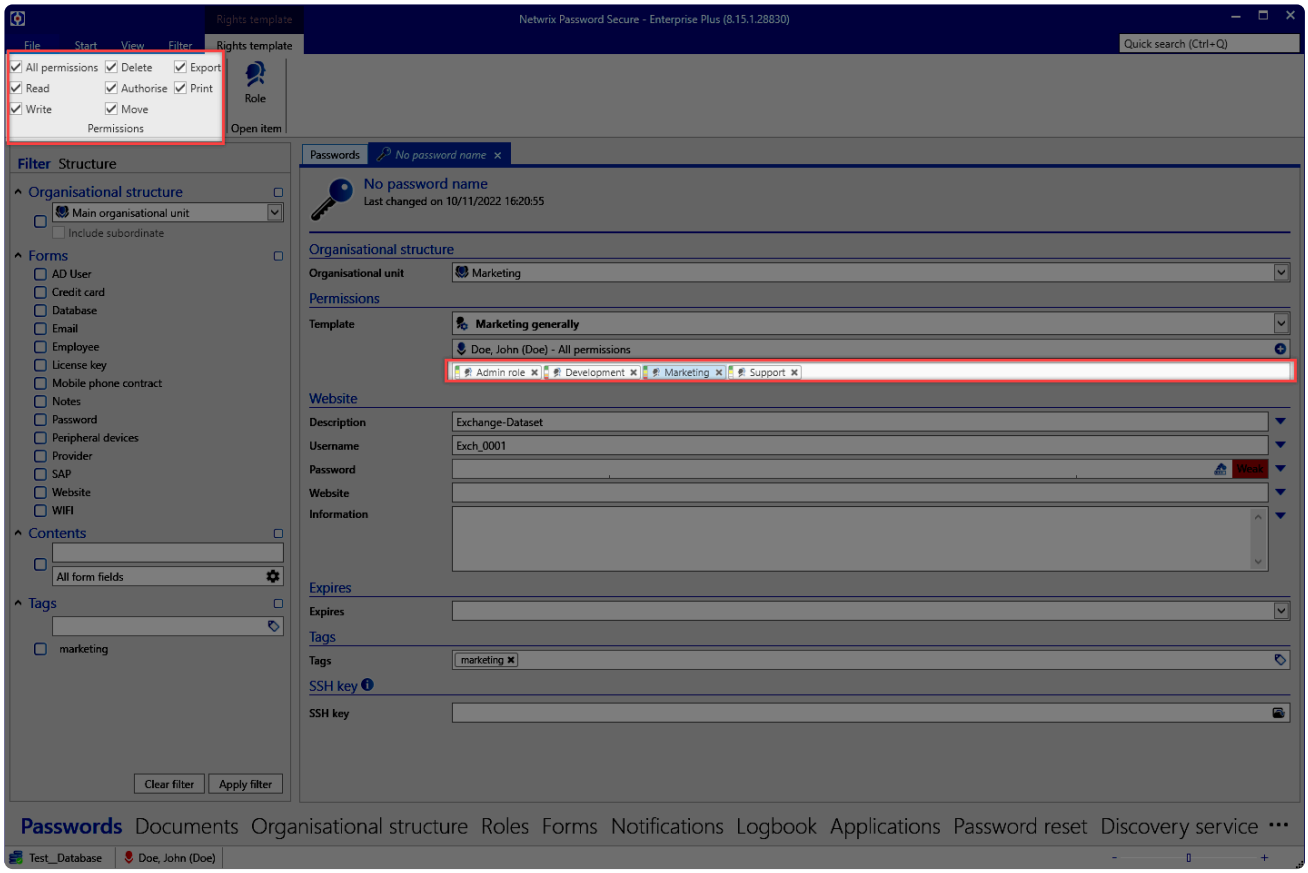
The relationship between them is obvious. It can be immediately seen that by selecting the organisational unit “IT” based on the rights configured in the rights template, permissions are granted for the roles “IT management” and also “Administrators”. **The underlying tags “IT” and “Exchange” are also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

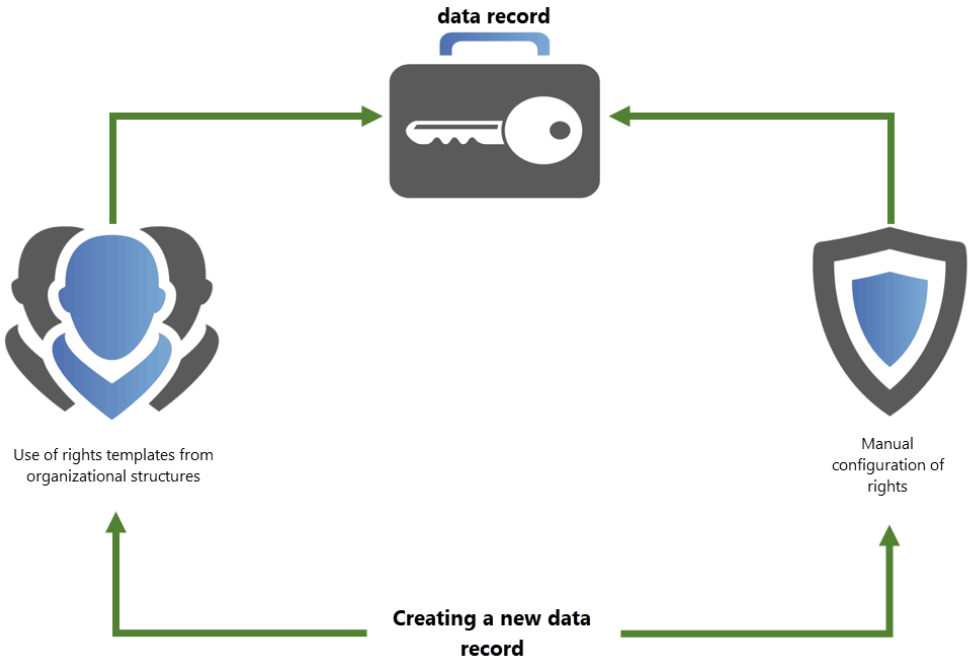
Colour	Permission
Green	Read
Yellow	Write
Orange	Delete
Red	Authorize

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”.



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.

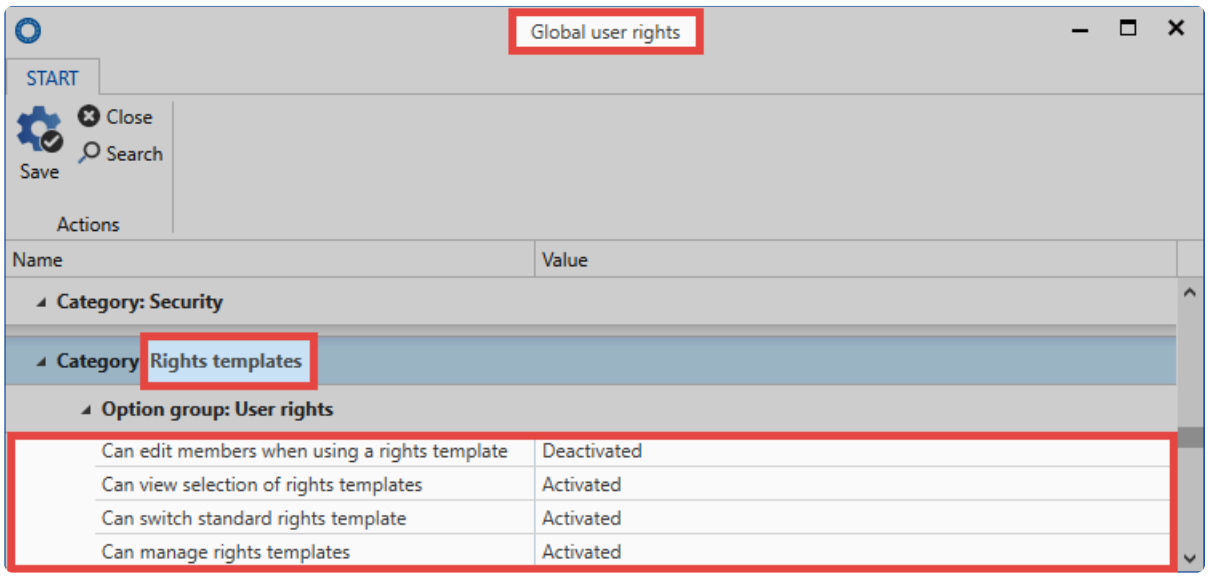


! The configuration of permissions can be carried out manually or automatically as described. If you want to change previously set permissions later, this has to be done manually. Retrospectively defining rights is not possible.

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.

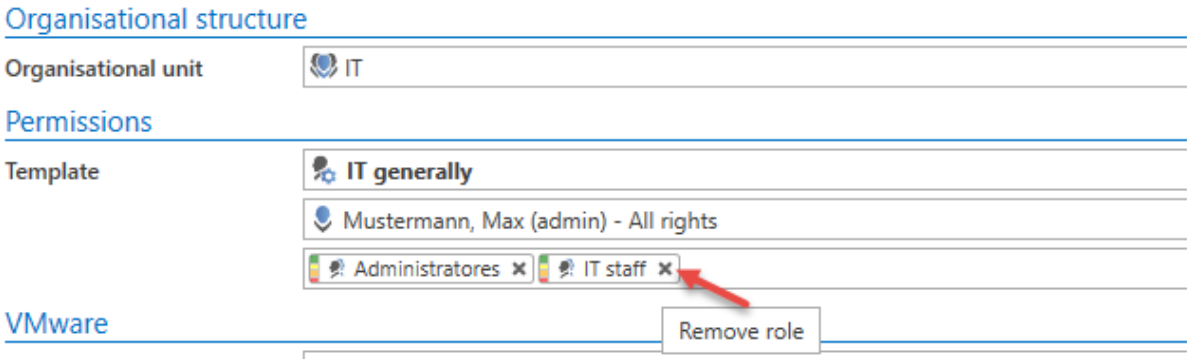


- **Can switch default rights templates:** When selecting the rights template, a diverse range of rights template groups can be selected. To be able to select a different template to the default template, the right “Can switch default rights templates” is required. If this right has not been granted,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

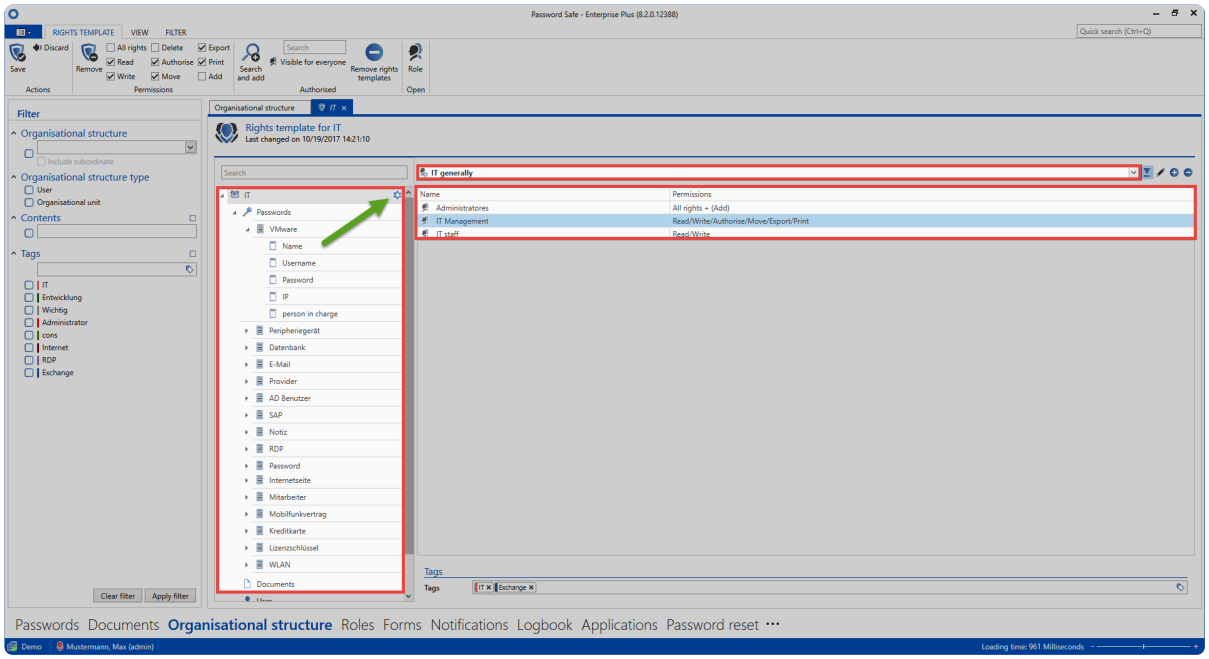
- **Can view selection of rights templates:** This right controls whether the rights template selection function is displayed or not when creating new records. If this right has not been granted, the user is thus not able to see for which roles and users the user rights are being defined.

- **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
Administratores
IT staff
Remove role
VMware

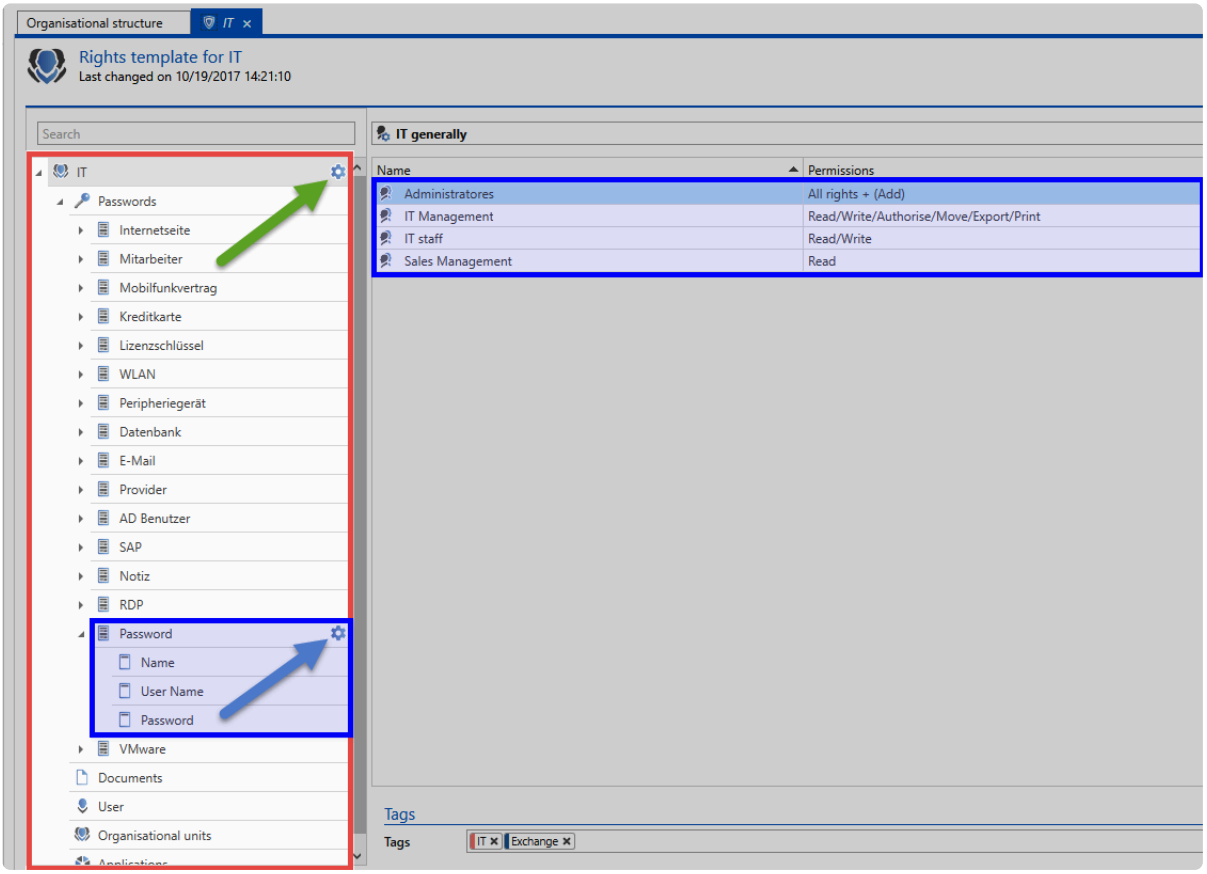
Scope of validity for predefined rights

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**.



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.



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).

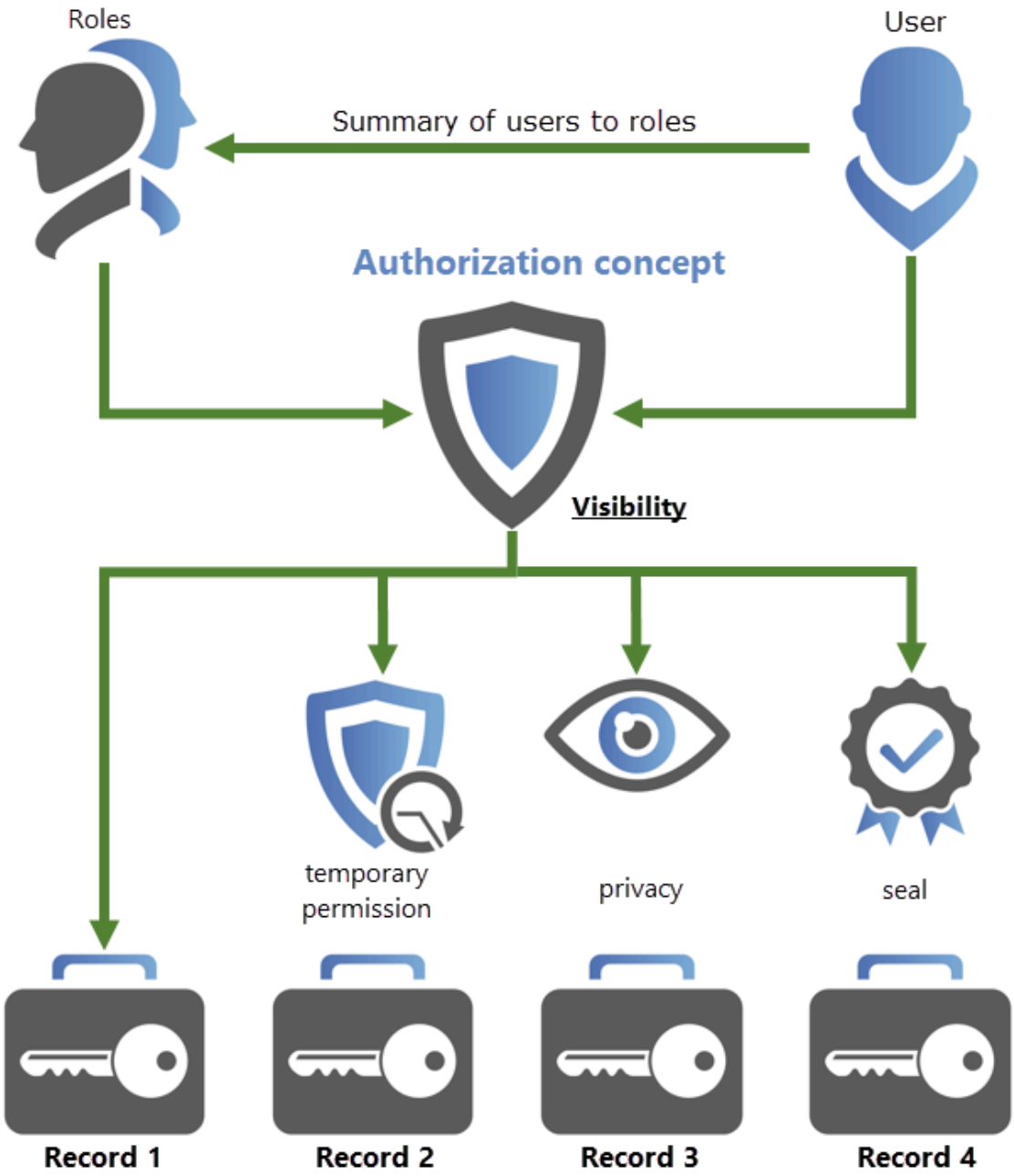
Protective mechanisms

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.

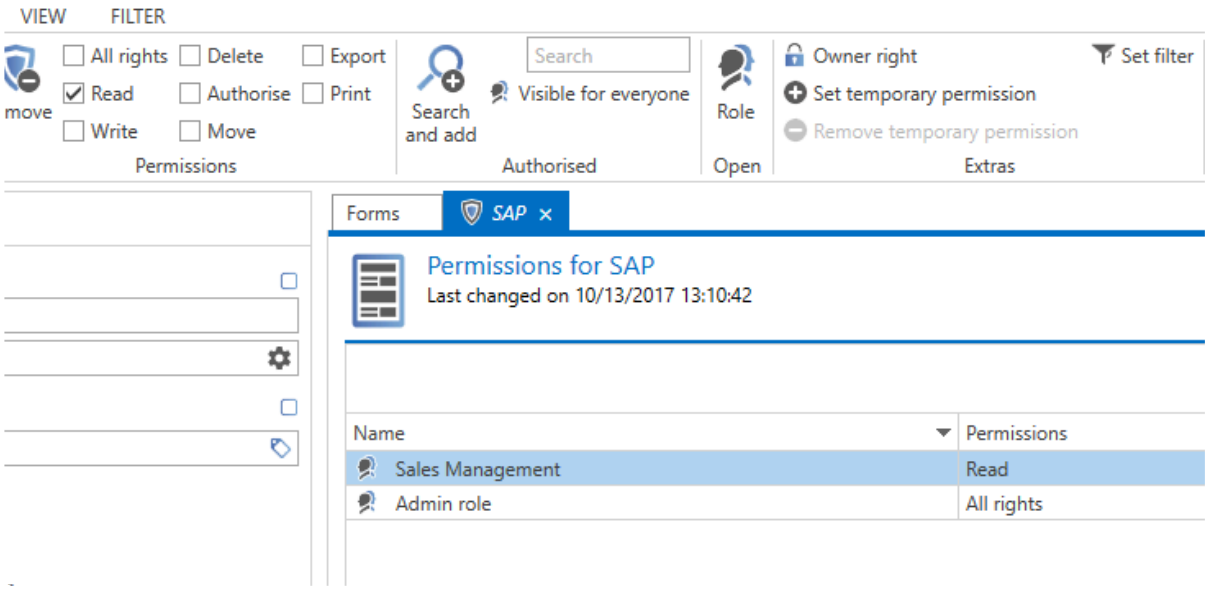
Visibility

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.



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.

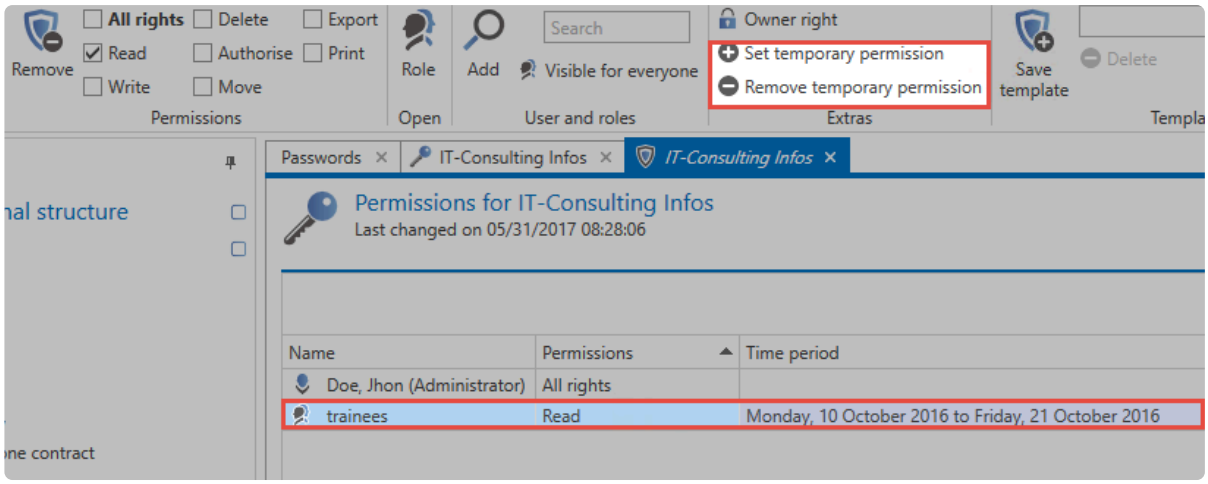
Temporary permissions

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.



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

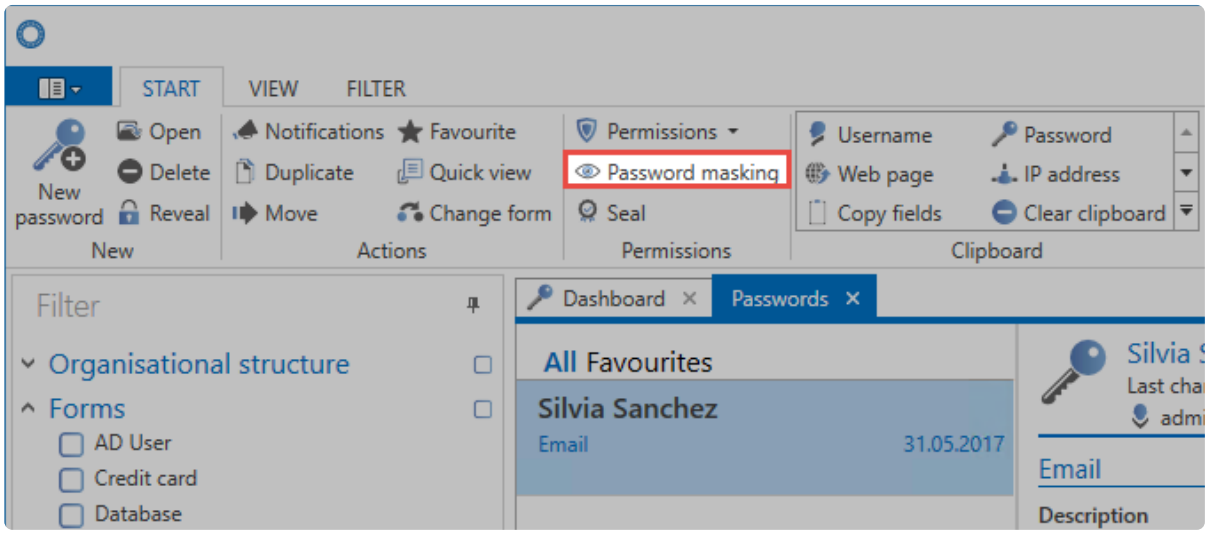
permissions. When these permissions expire, there is no longer any user with full permissions. To prevent this happening, users with temporary permissions are handled differently.

> ! 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.



Relevant rights

The following option is required to apply password masking.

User right

- Can apply password masking

Required permissions

In the same way as for the seal configuration, the **authorize** right for the record is required to apply 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.

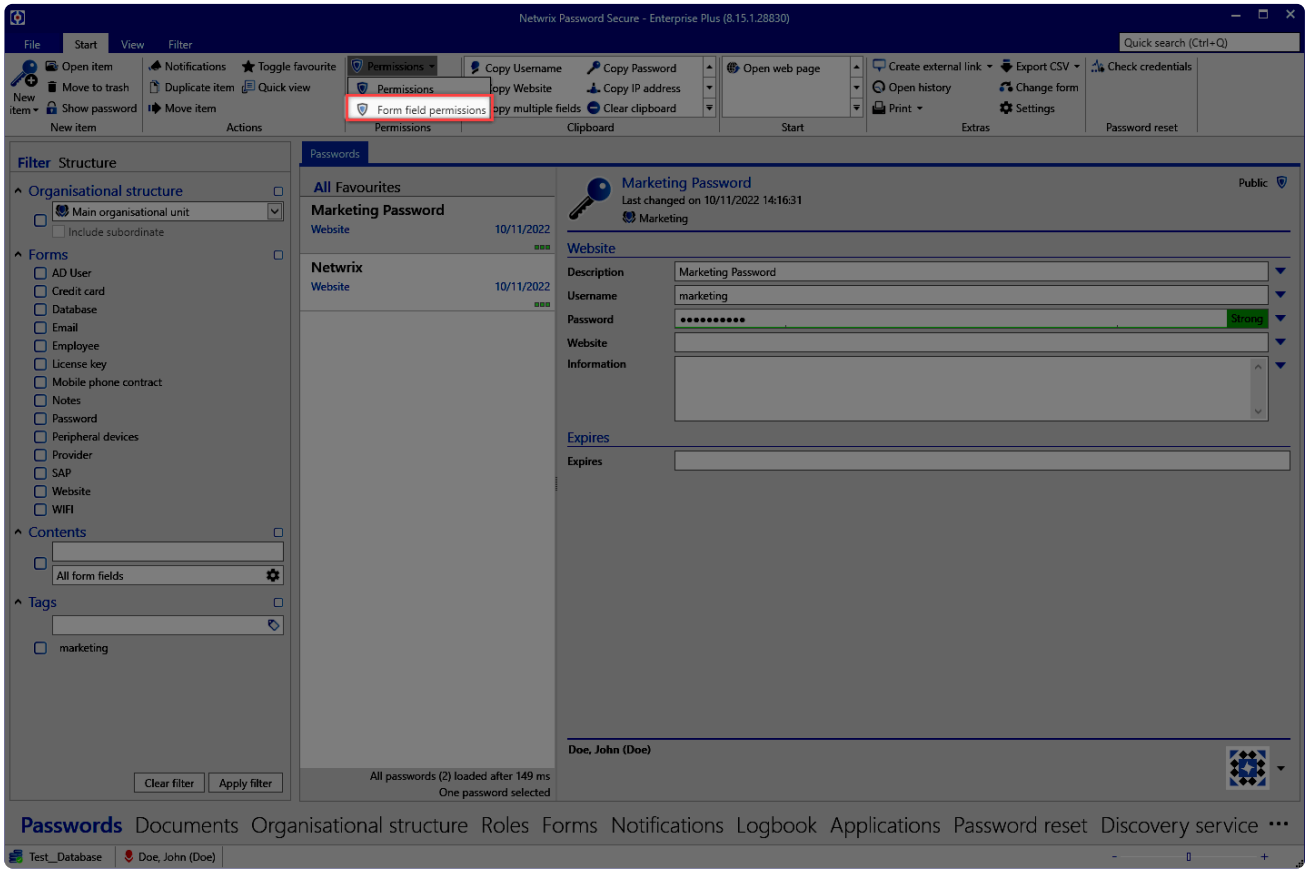
Password masking can only be applied to records with an existing password!

Applying password masking

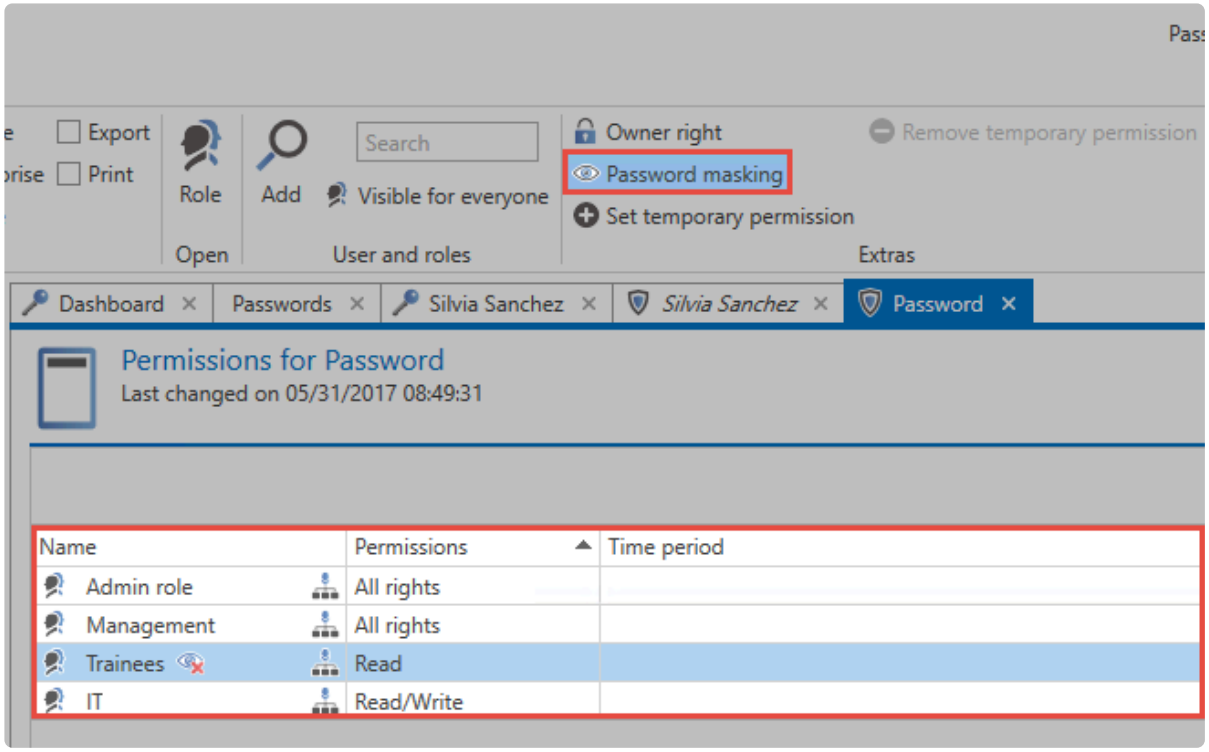
The icon in the ribbon allows users with the required permissions to apply password masking following a confirmation prompt. By default, the privacy is for all those who have at least reading permission, but not the right * entitled *.

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.



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.



✻ 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**.

✻ It is important to note that the login mask for records with password masking will be ”sent automatically*, even if the setting **Browser add-ons: Automatically send login masks** has been deactivated.

! The password masking only applies to those users who are authorized at the time of attachment to the record. If a record has the password masking and a user get´s authorized the record is **not protected** for this user. The password masking should then be removed and reset.

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.

Relevant rights

The following option is required to add a seal.

User right

- Can add seal

Required permissions

Firstly, the user must have the **"authorize"** right for the record in order to create seals. The read right to all users and roles that are contained in the seal is also required. 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.

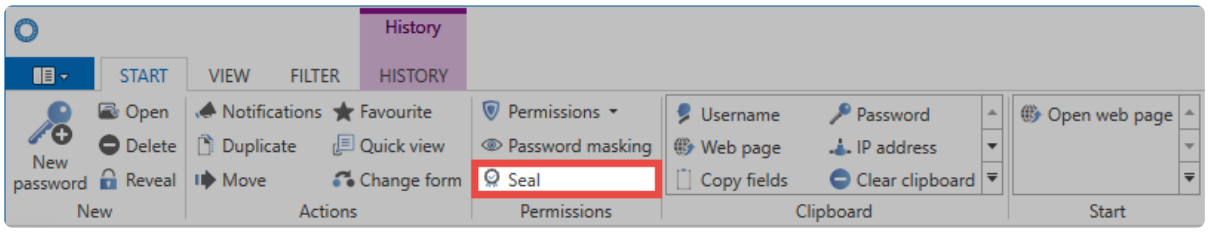
> ! The complete data set is never sealed! Only the right to view a password is protected by a seal.

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

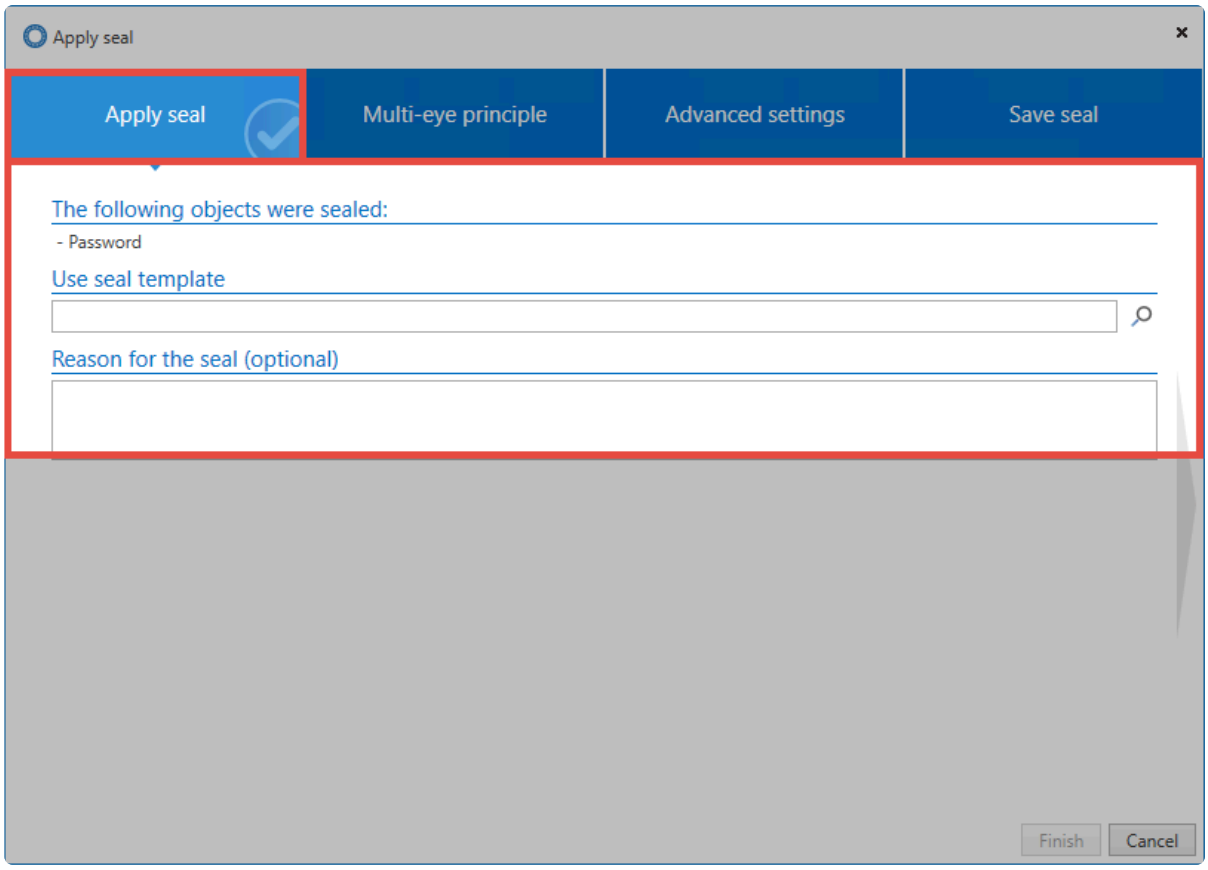
Seal wizard

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 wizard is opened via the ribbon, the wizard appears in the case of unsealed data sets, which runs in **four steps** through the configuration of

the seal.



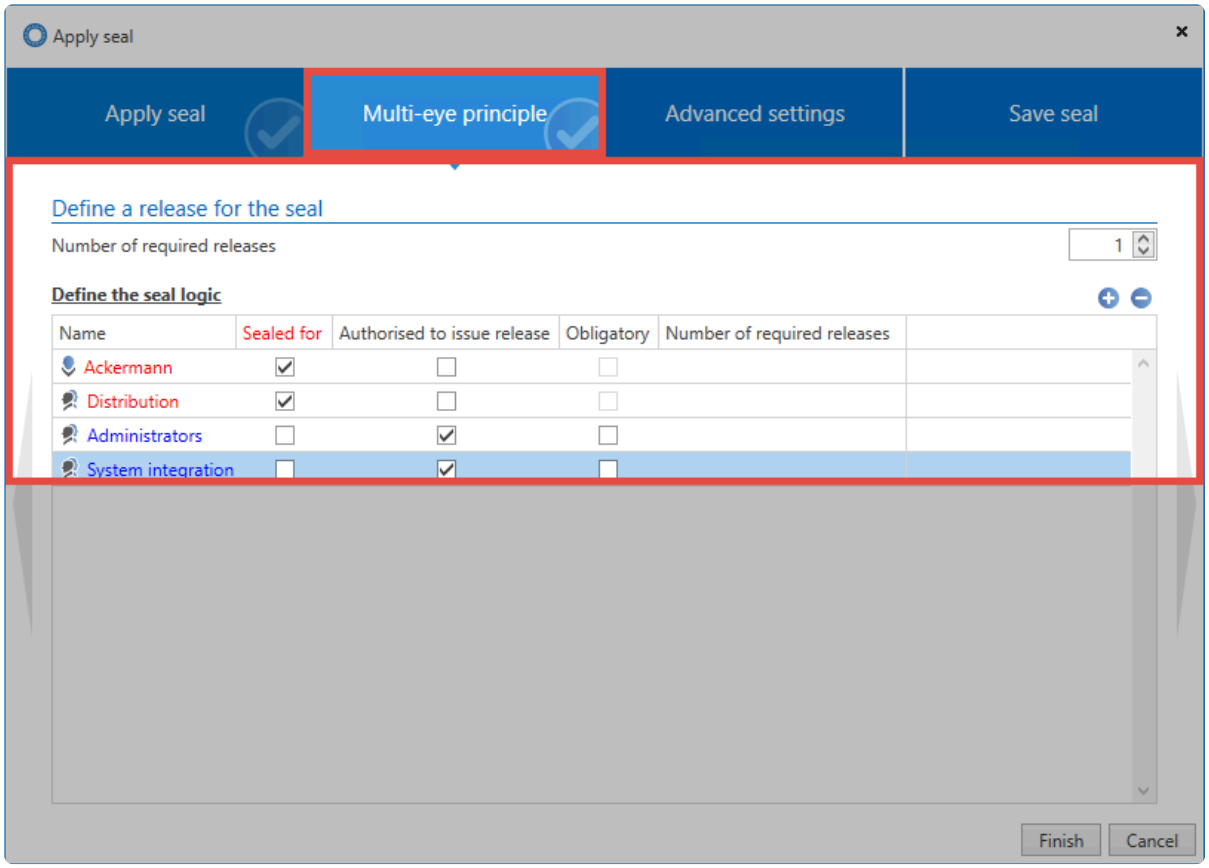
1. Apply seal



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.

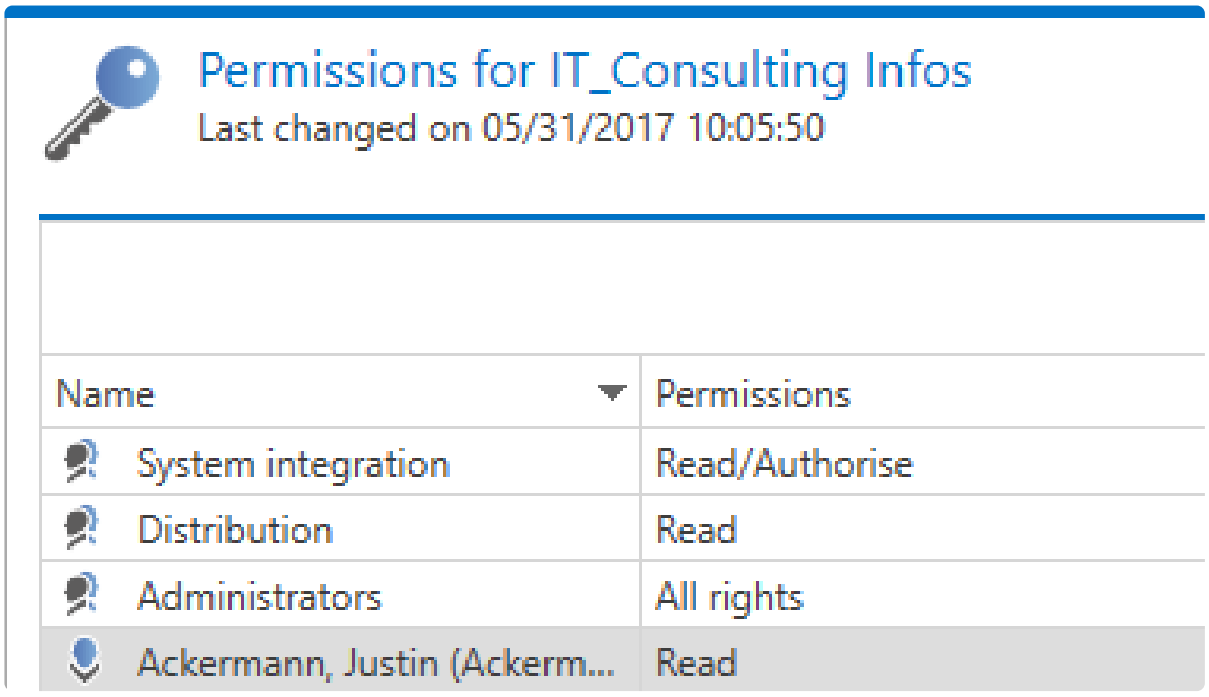
2. Double-check principle

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.



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).



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:

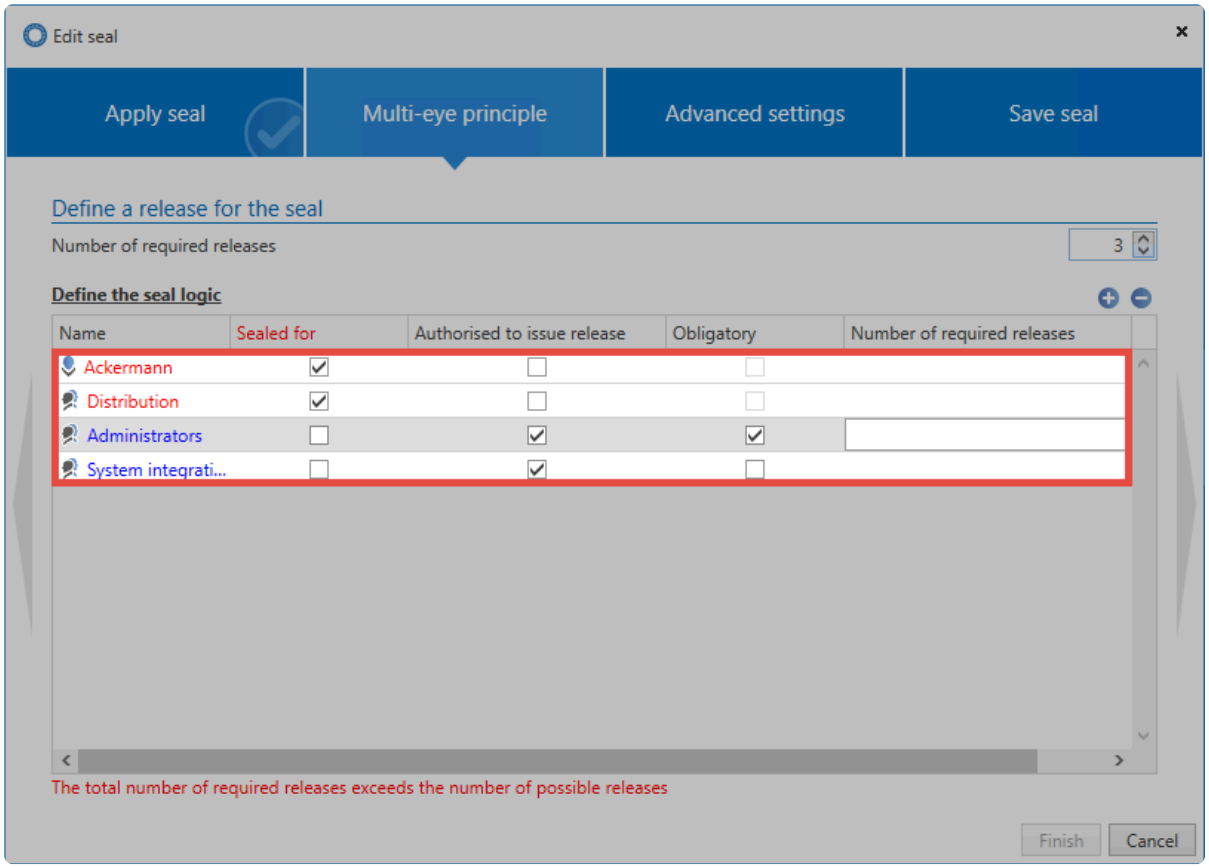
> ✻ All users and roles that have the “authorize” right to the record are **”authorized to issue a release”** for the seal by default. All users and roles that do not have the “authorize” right to the record are copied directly into the **”Sealed for”** column.

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

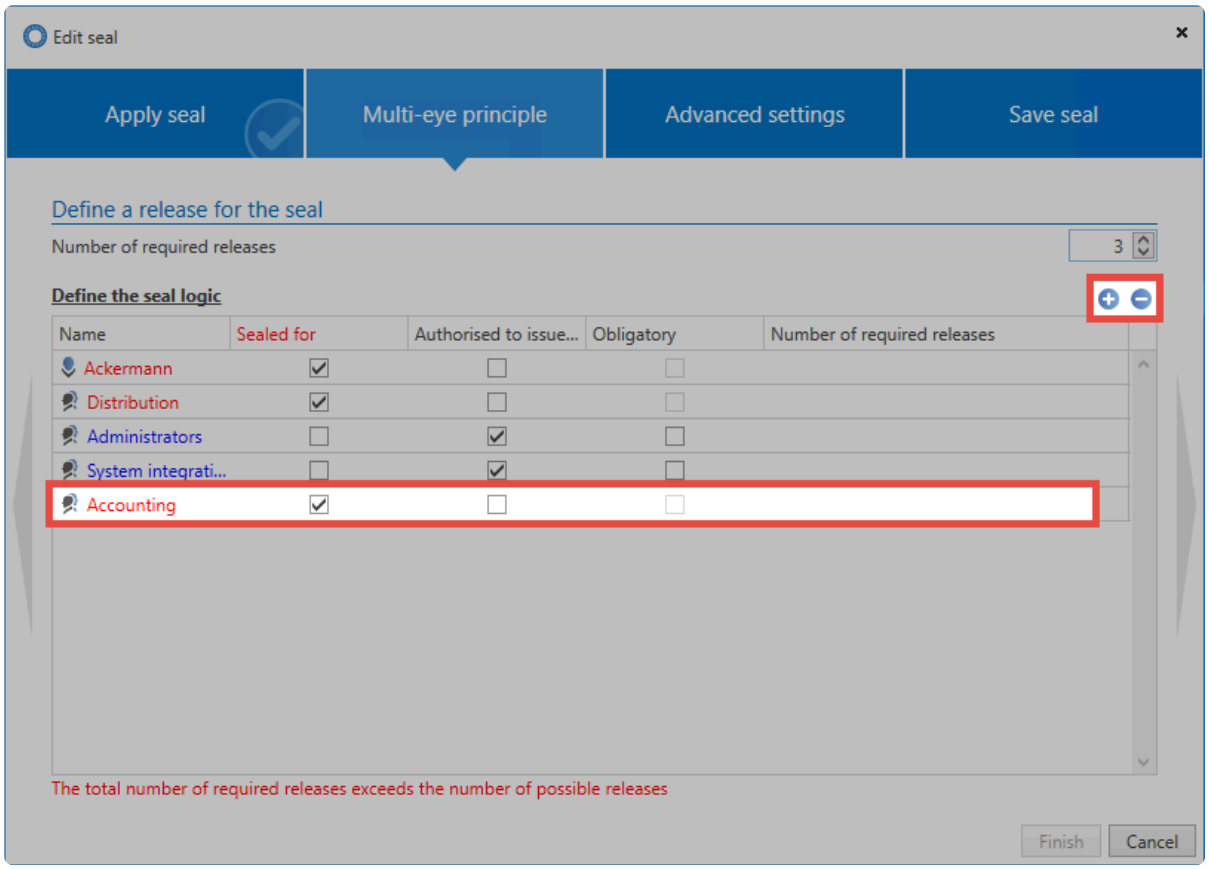


Adjusting the seal logic

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.



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.



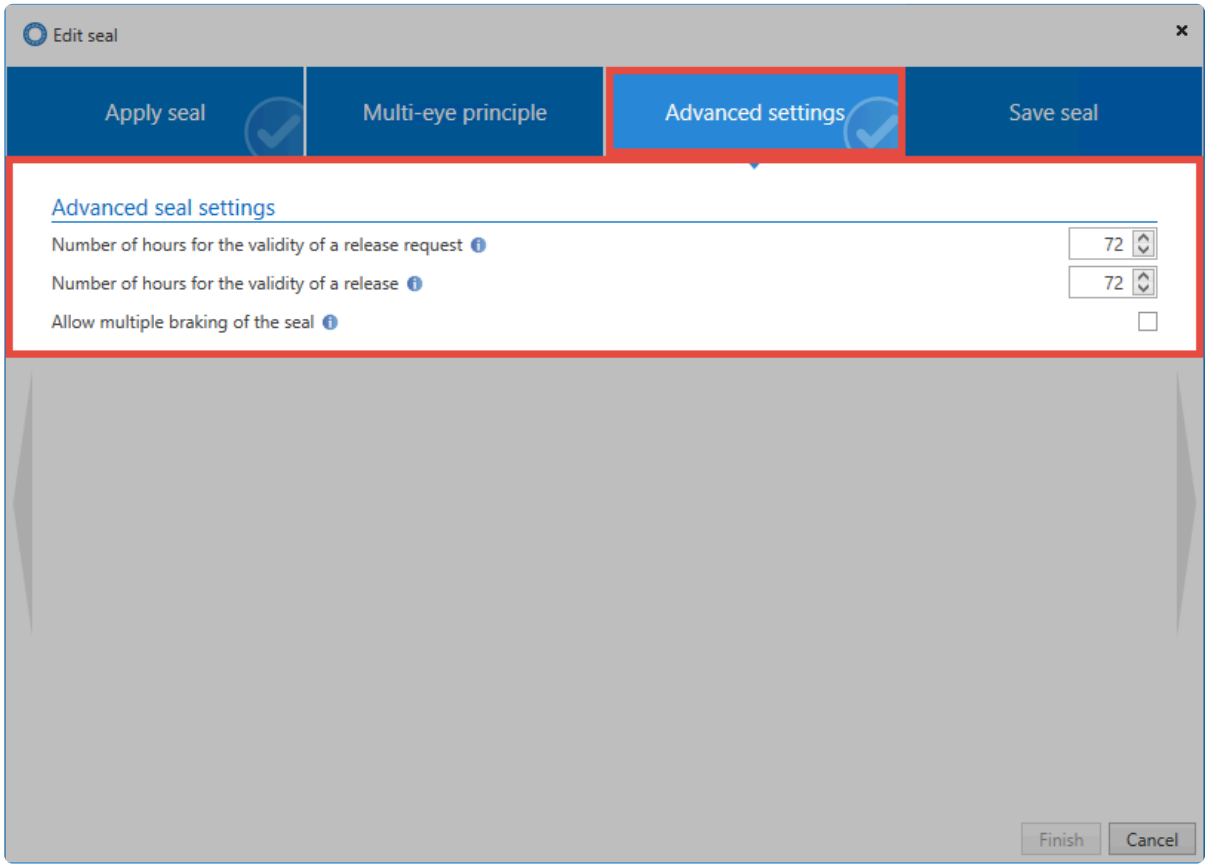
When a role or a user is added to a seal, these users also receive permissions on the record according to the authorization granted in the seal. A role that is added under “Sealed for” receives the “Read” right on the record. When you add authorization permissions, these will henceforth include the “Read,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

It is possible to seal records for a user who is also authorized to issue a release. In this constellation, it is important to ensure that at least one other user is authorized to issue a release. In principle, you should never be able to issue a release for yourself.

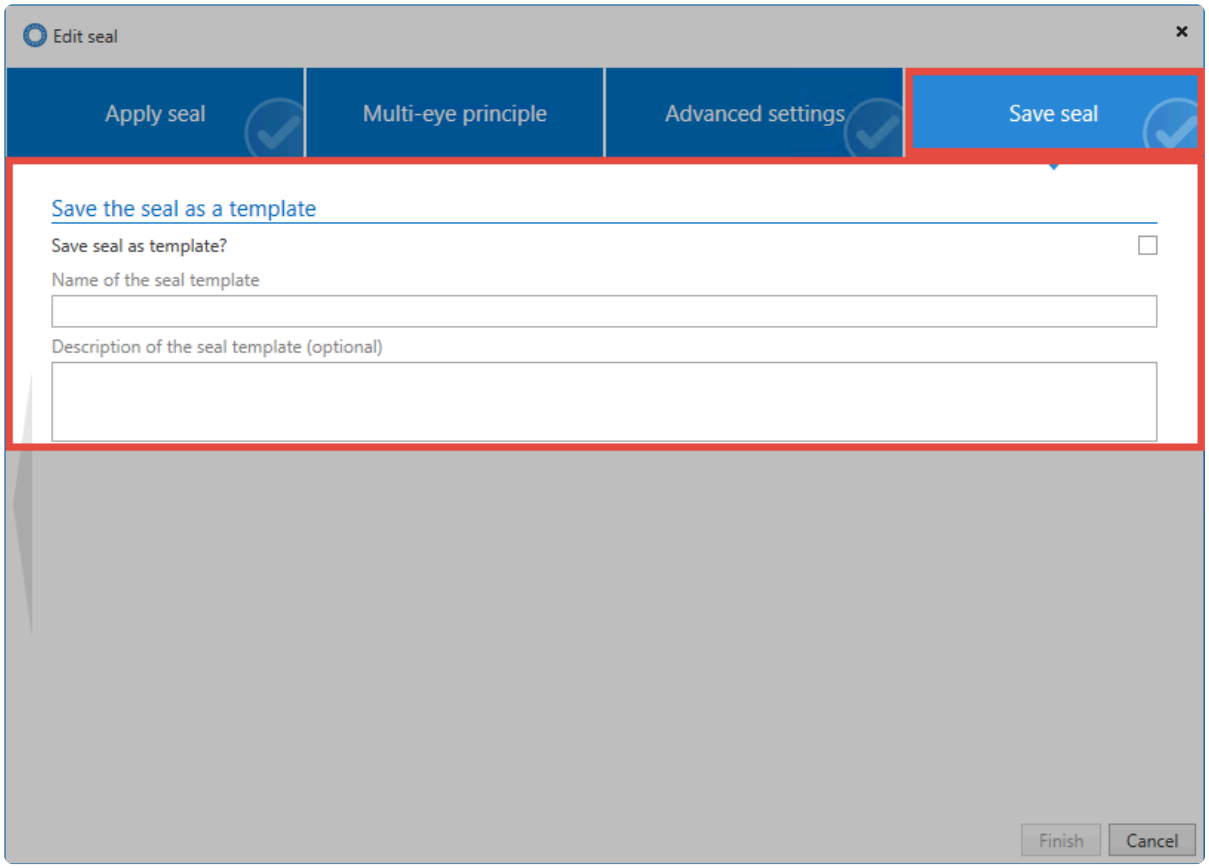
3. Advanced settings

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.



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.



Summary

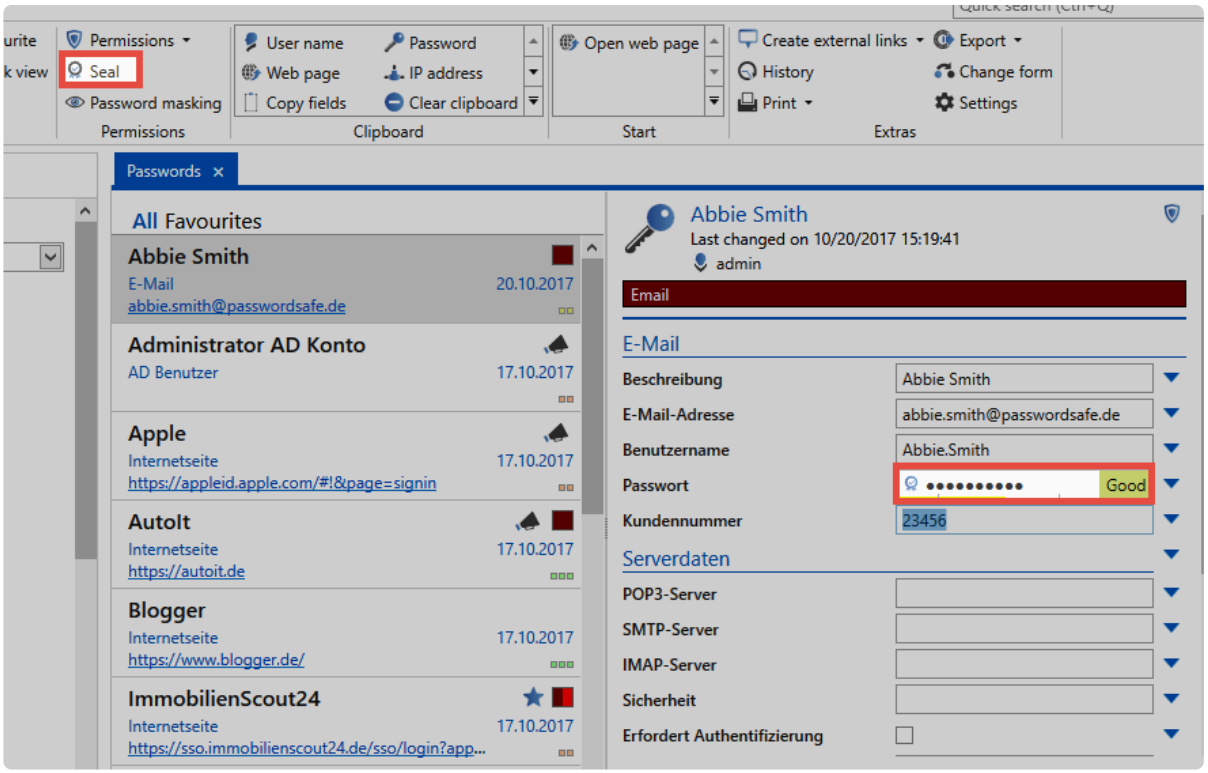
The rights already present on the data set form the basis for any complex seal configurations. It is thus freely definable which users have to go through a release mechanism before accessing the password. The roles, which may be granted, are freely definable. An always accessible seal overview allows 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

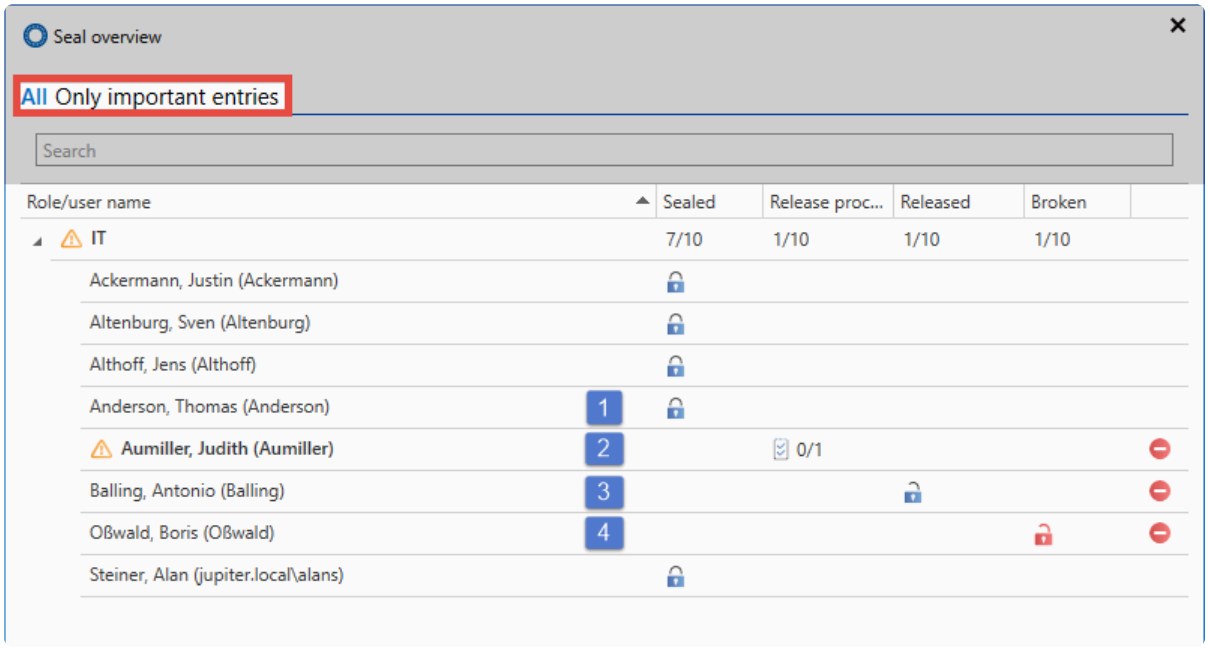
What is seal overview?

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.



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:



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

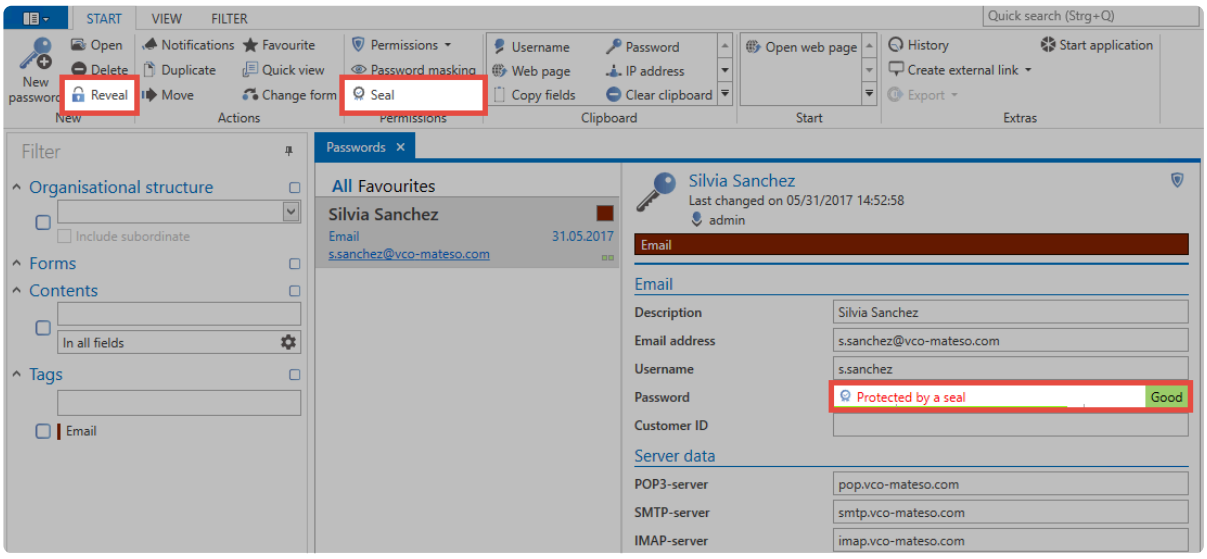
As noted in the previous sections, seals always restrict the right of a user to view a specific password. Even if the configuration is usually done at the level of the role, each user is naturally responsible for his own request when carrying out the release. Even if a seal is defined for a role, technically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

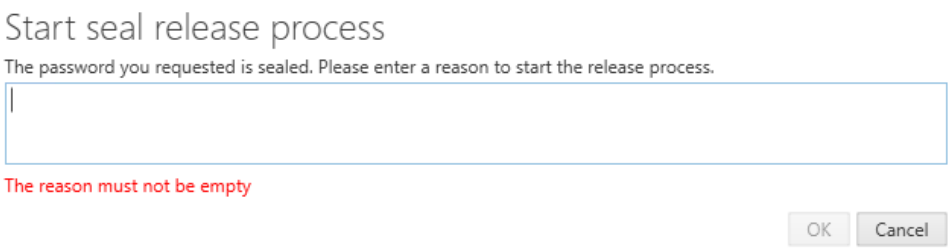
1. Requesting a release

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.



A modal window opens, which can be used to request the seal. The reason for the entry will be

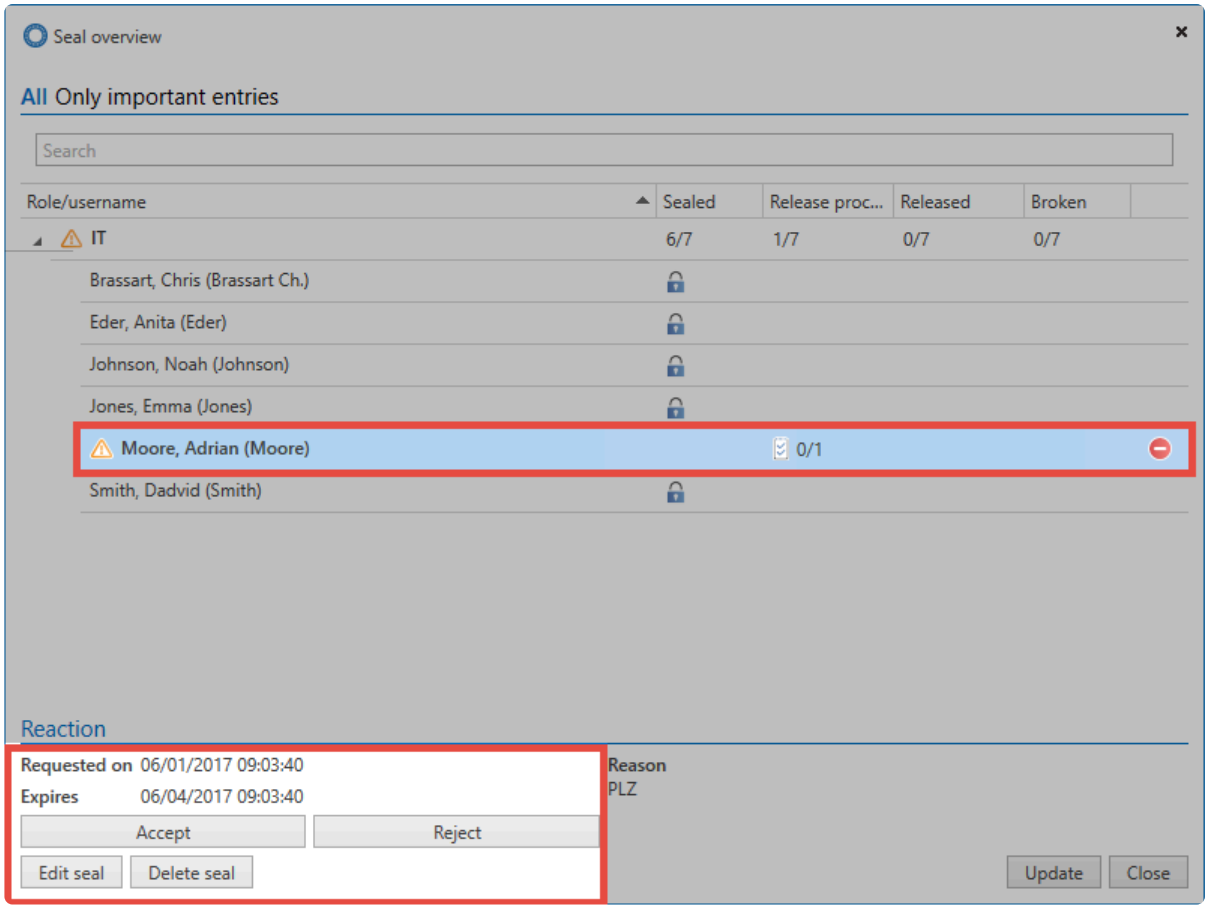
displayed to the users with the required permissions to issue the release.



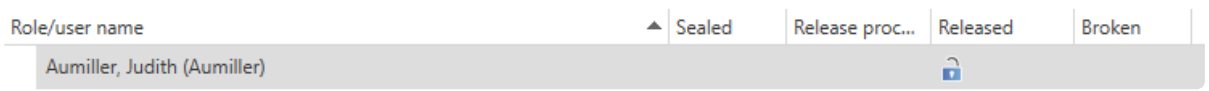
All user with the required permissions to issue the release will be notified that the user has requested the seal. This can be viewed via the module Notifications, as well as in the Seal overview.

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.

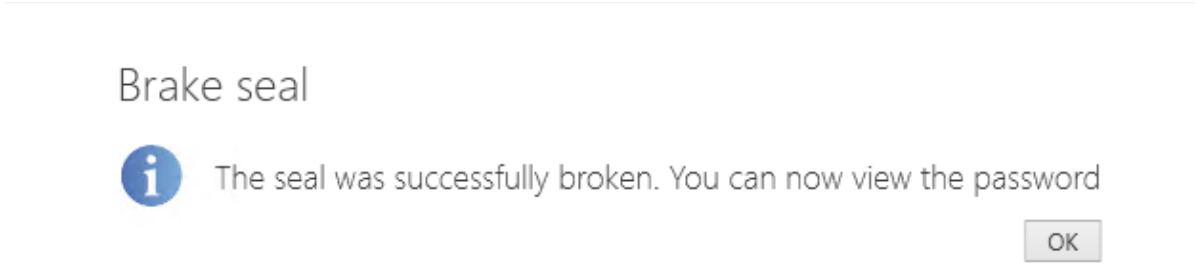


If the release is granted, the Inquirer Im * Module Notifications * will be informed. You can also open the seal directly from the ribbon and see the now released state.



3. Breaking the seal

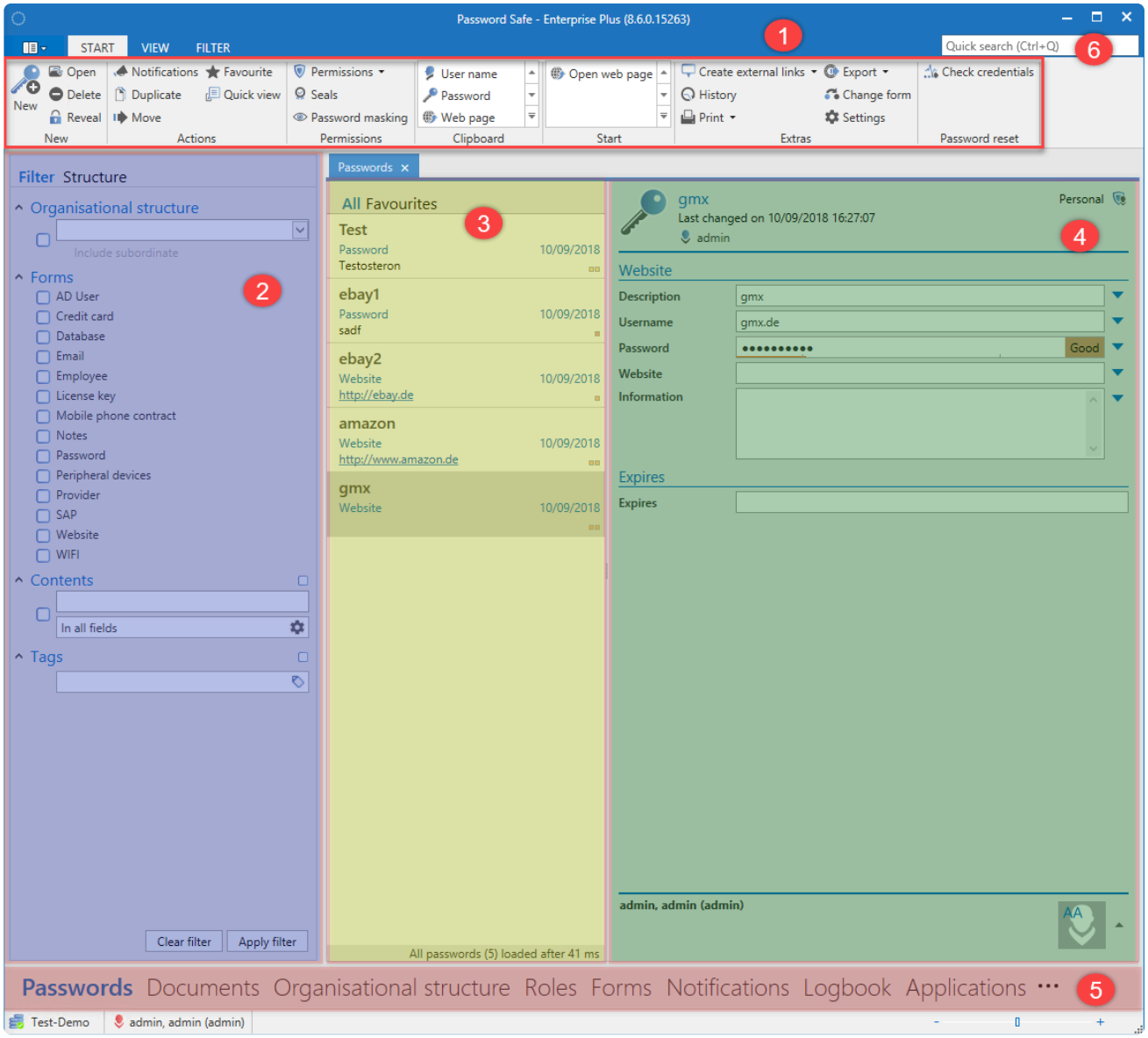
As soon as the requesting user has received the number of the required releases, he will be informed via the notifications as usual. The seal can now be broken. From this point on, the user will be able to see the password.

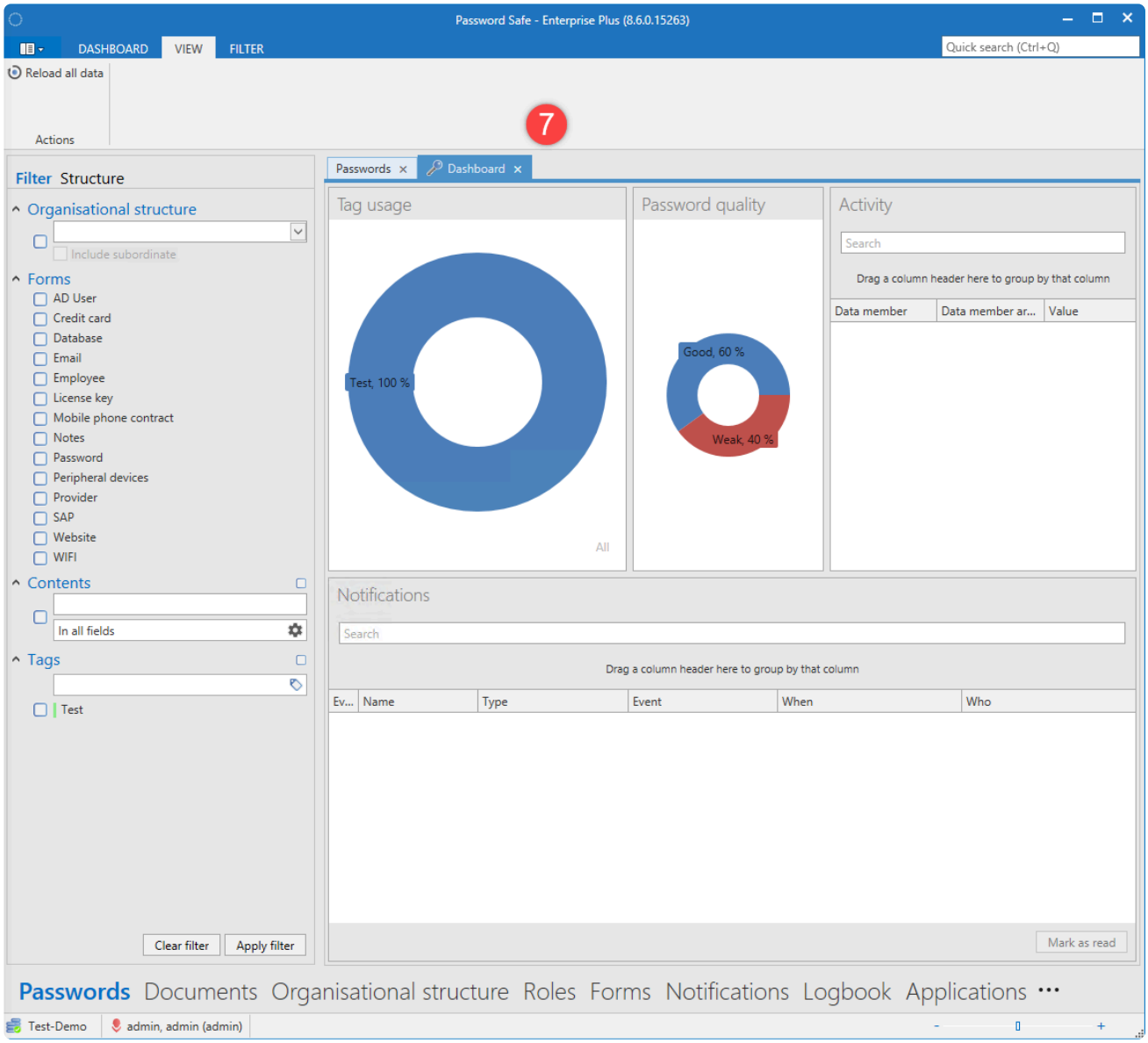


Operation and setup

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.





1. Ribbon

2. Filter

3. List view

4. Reading pane

5. Tags

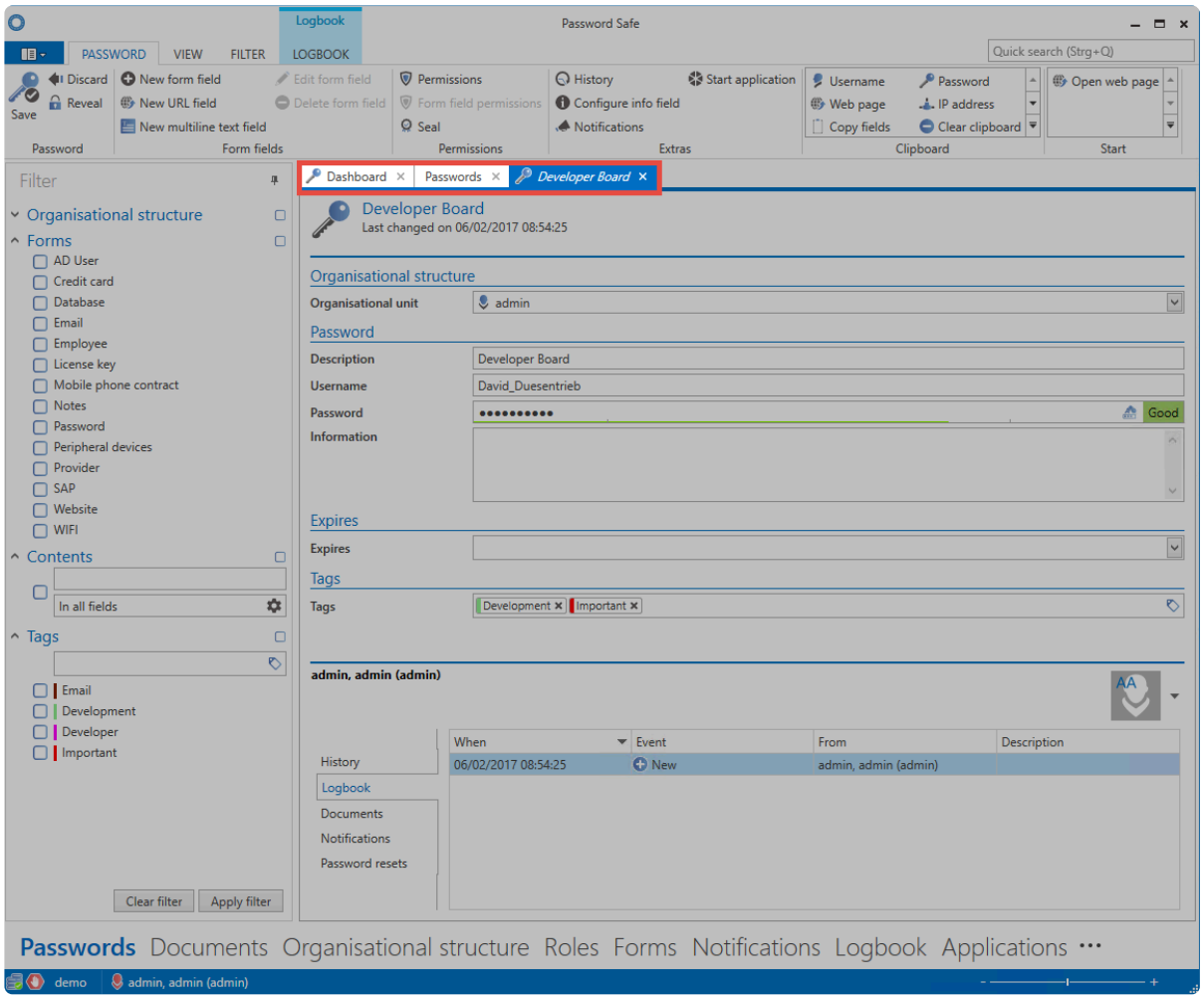
6. Search

7. Dashboard and widgets

TABs

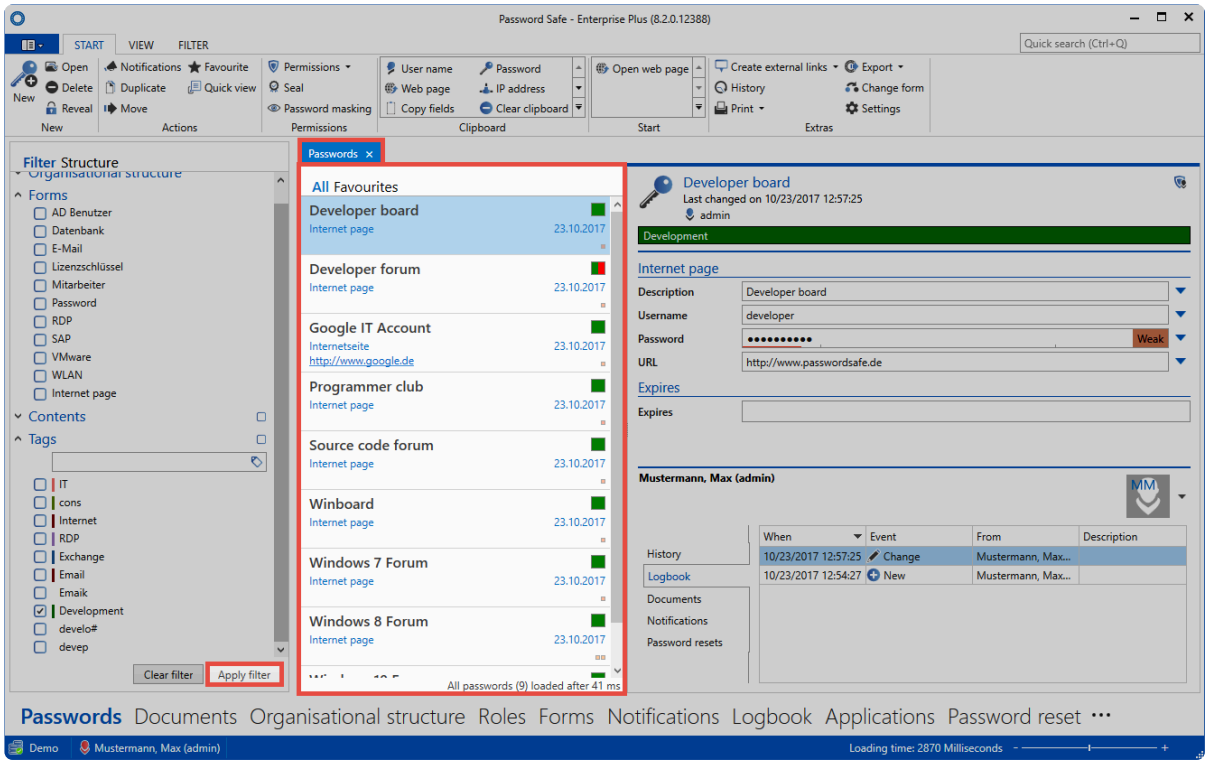
Tabs offer yet another option within the Password Safe to present related information in a separate area. This tab navigation enables you to display, quickly access and switch between relevant information. The results for a filter with specific criteria can thus be retained without the original result 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.



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.)

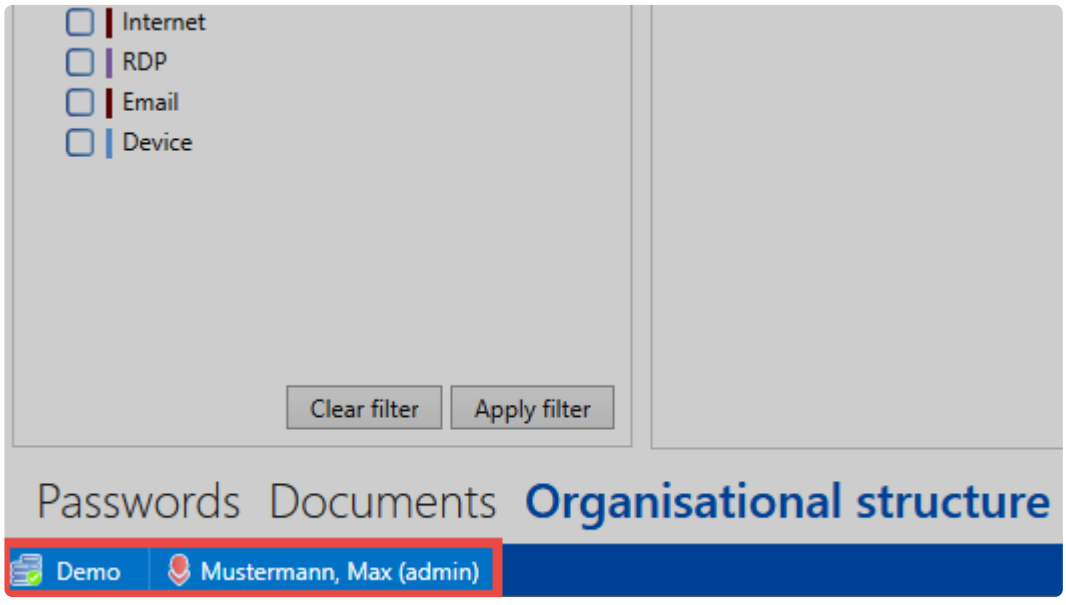


Although the name suggests that all records in the database are displayed, the records displayed in list view correspond to the criteria that have been defined in the filter. The tab closes and can be restored by reusing the filter.

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

Orientation

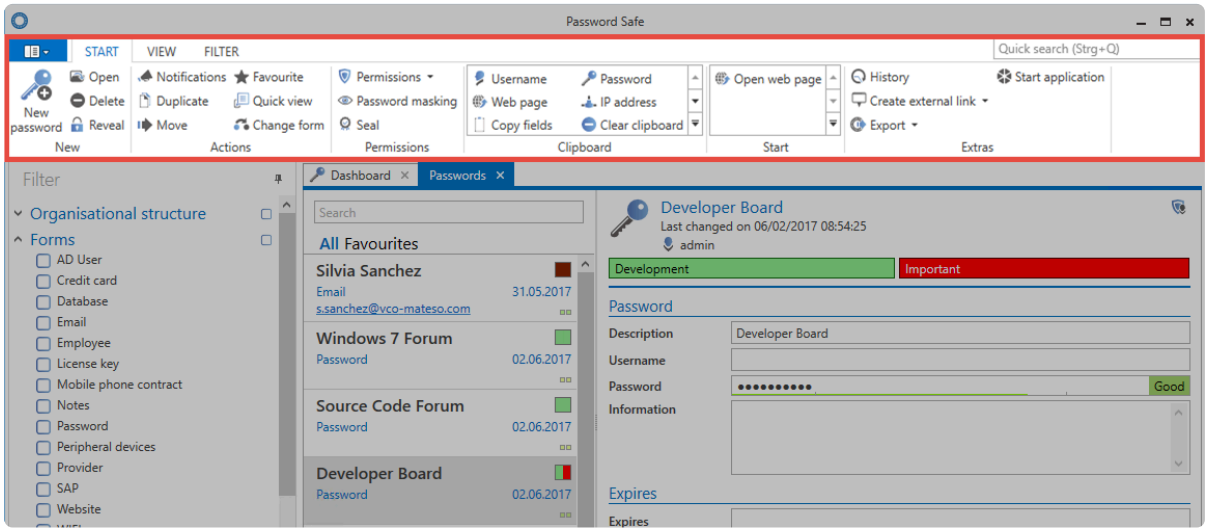
It is possible to change the alignment of the following objects:

- Active Directory
- Applications
- Notifications
- Reports
- Documents
- Forms
- Logbook
- Organisational structure
- Password reset
- Rules
- Roles
- Seal templates
- System tasks
- Forwarding Rules
- Profil picture in the reading pane

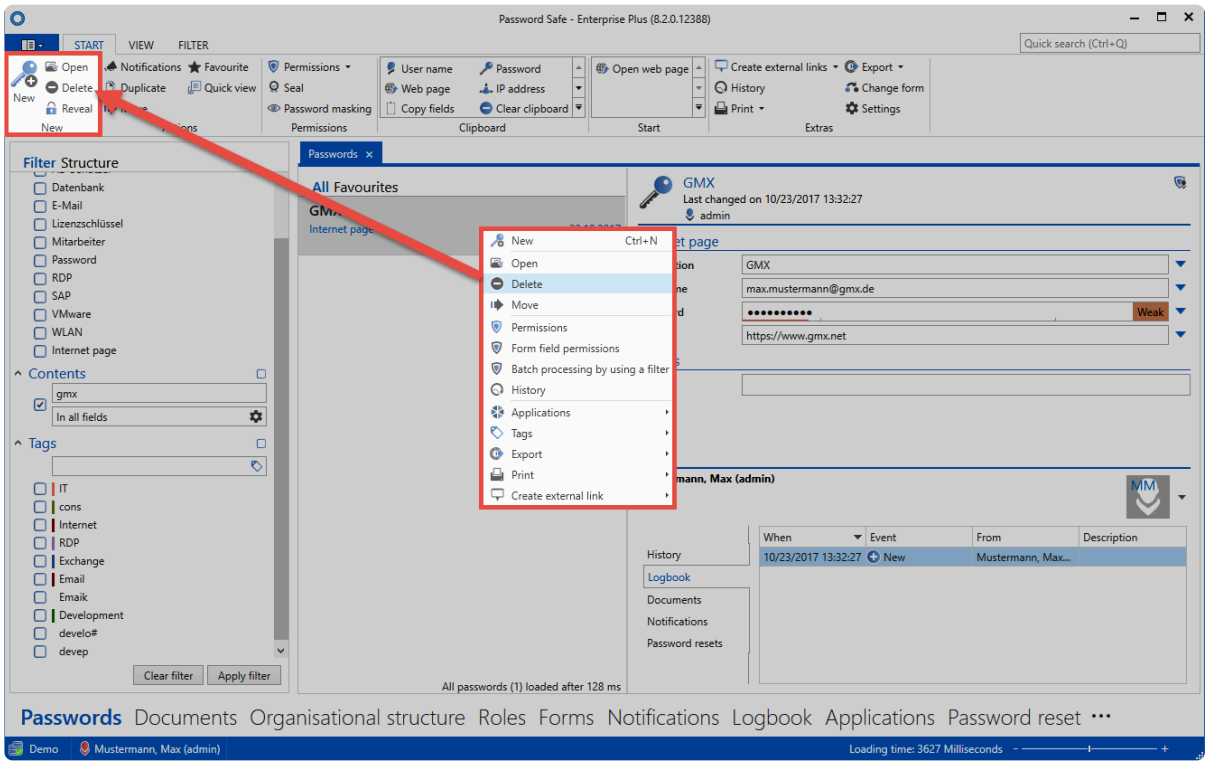
Ribbon

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.



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).

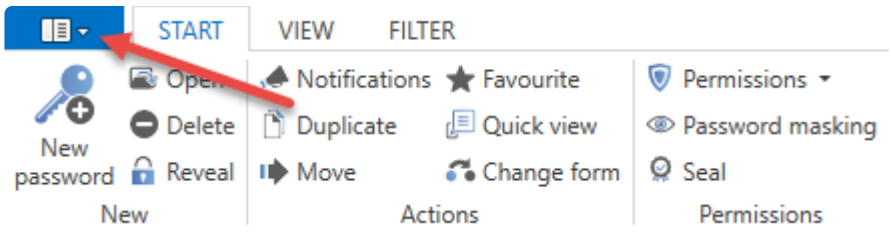


This mainly affects the very often used features such as opening, deleting or assigning tags. However, a

complete listing of the possible actions is always only possible directly in the ribbon. This ensures that the context menu can be kept lean.

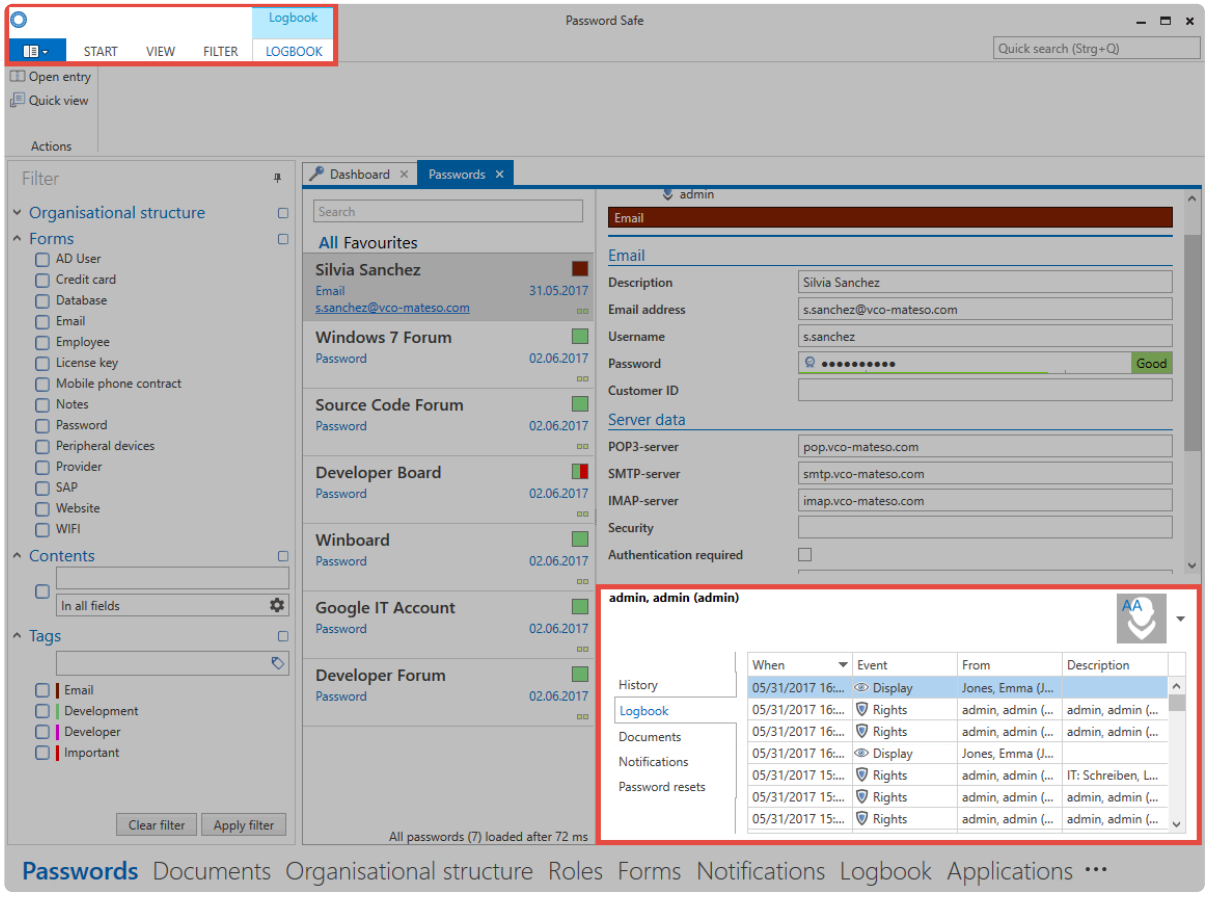
Access to the client main menu (backstage)

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



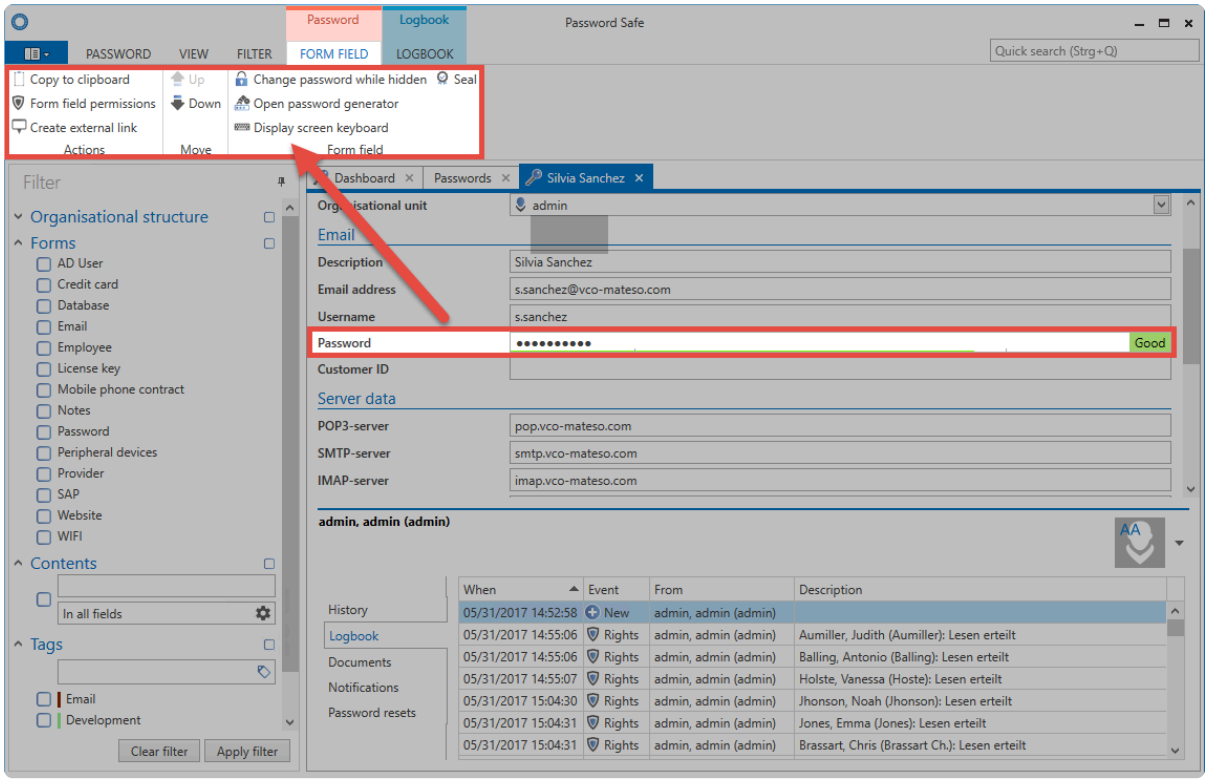
Ribbon tabs

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.



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.



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?

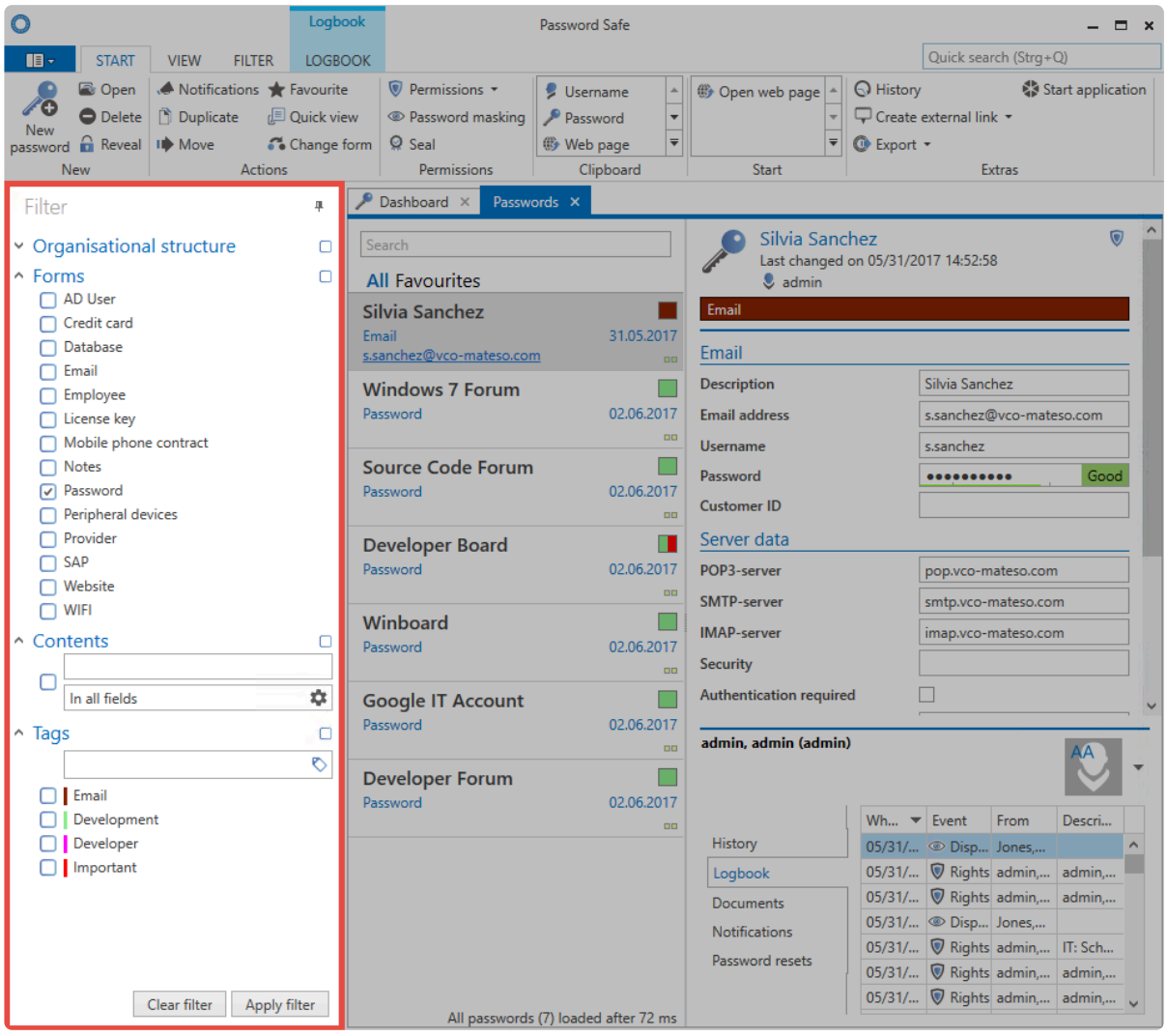
The freely configurable filters of the PSR client provide all methods for easy retrieval of stored data. The filter criteria are always adapted according to the module in which you are currently located. When you select one or several search criteria, and click on “Apply filter”, the results will be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

Relevant rights

The following option is required for editing filters:

User right

- Can edit filter



Who is allowed to use the filter?

The filter is an indispensable working tool because of the possibility to restrict existing results according

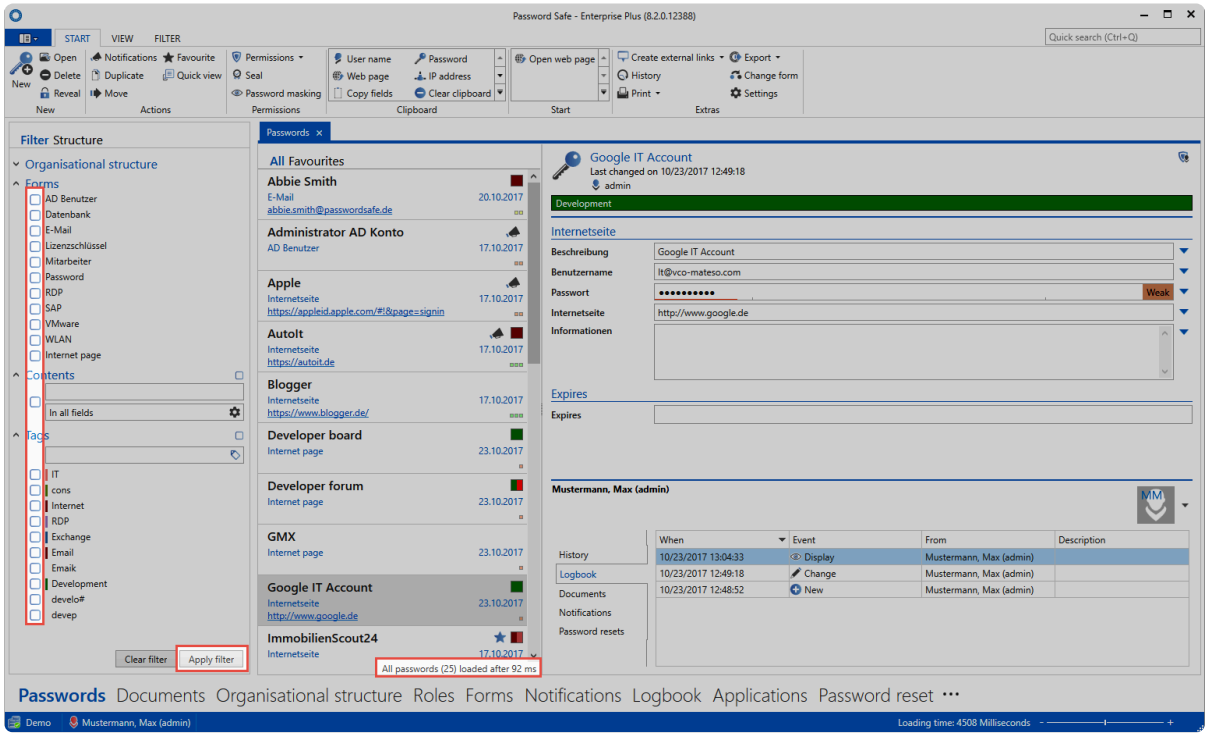
to individual requirements. Consequently, all users can use the filter. It is, of course, possible to place restrictions for filter criteria. This means that the filter criteria available to individual employees can be restricted by means of permissions. For example, an employee can only filter for the form **password** if he has the read permission for that form.

> ! There are no permissions for “tags”#tags. This means that any employee can use any tags. The display order in the filter is determined by the frequency of use. This process is not critical to security, since tags do not grant any permissions. They are merely a supportive measure for filtering.

Application example

Filter without criteria

By selecting the desired 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 records to which you generally have authorization.

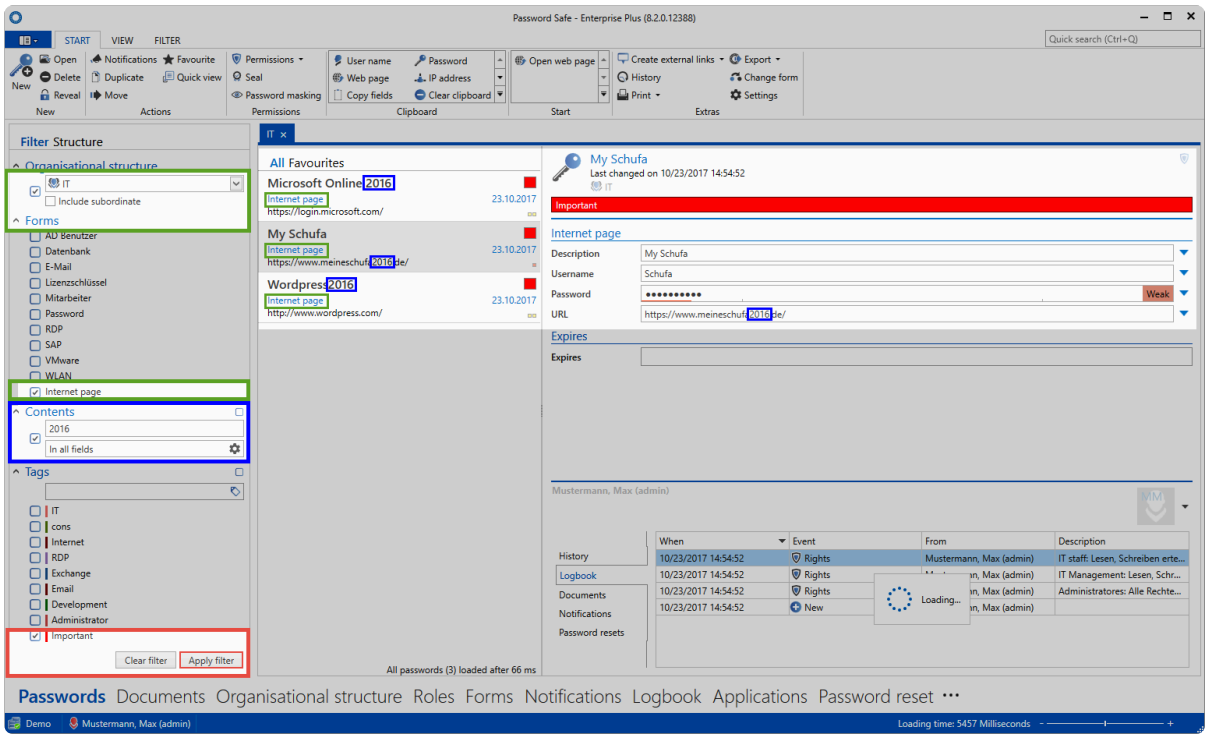


As you can see, 133 records are not really manageable. In most situations you will need to reduce the number of records by adding filters.

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**.

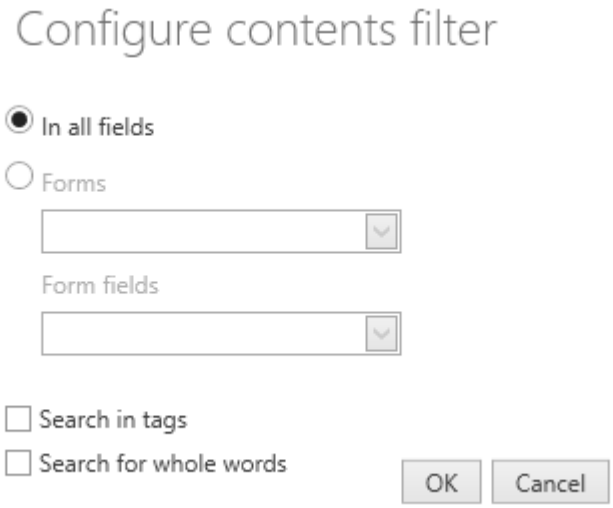


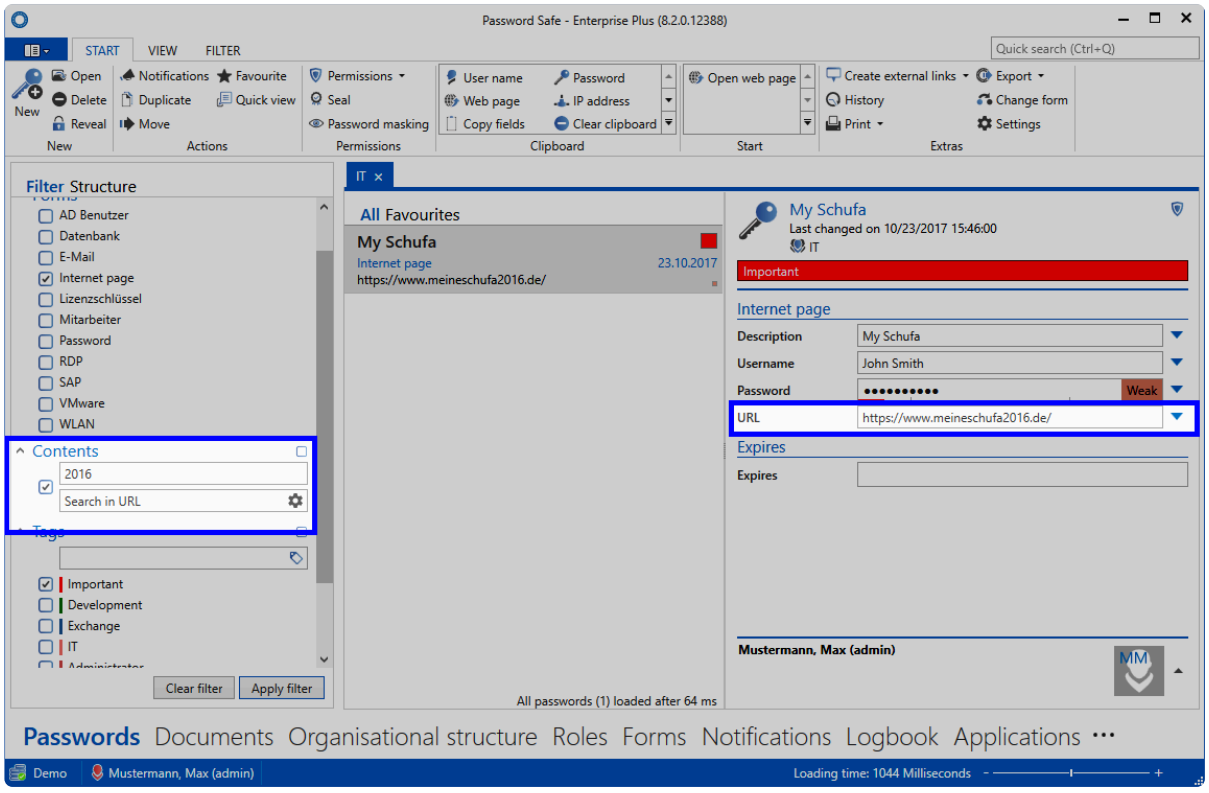
As can be seen, the filter delivers the desired results. The extent to which the filter criteria match the three remaining data sets is assigned in colour.

> ! 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 methods for linking criteria 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 also 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 can be seen, the content filter has been configured to only search in the form **password** and then only in the form field **Internet address**:





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.

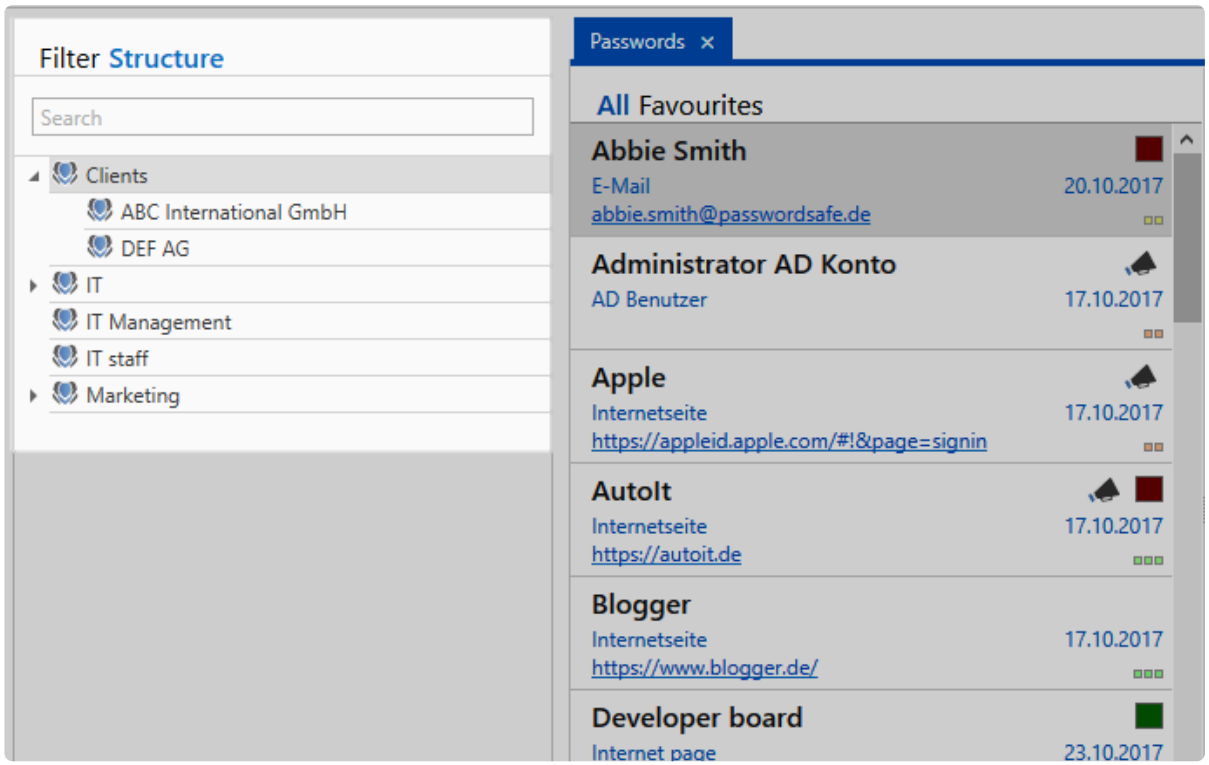
> ! The effectiveness of the filter is closely linked to data integrity. Only when data is kept clean, efficient operation with the filter is ensured. It is important that employees are trained in the correct handling of the filter tool as well as when creating the records. Workshops show the best success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

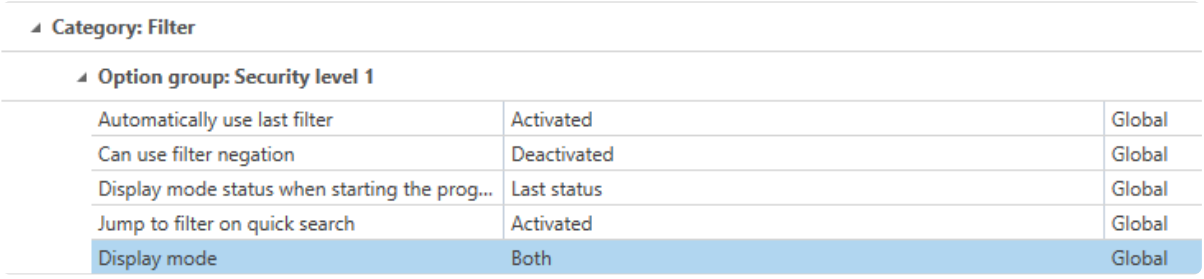
> As there are no longer any folders in Password Safe version 8, the structure view can not mirror all of the functionalities of the folder view in version 7. However, the structure view has been modelled on the folder view to make the changeover from the previous version easier.



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.

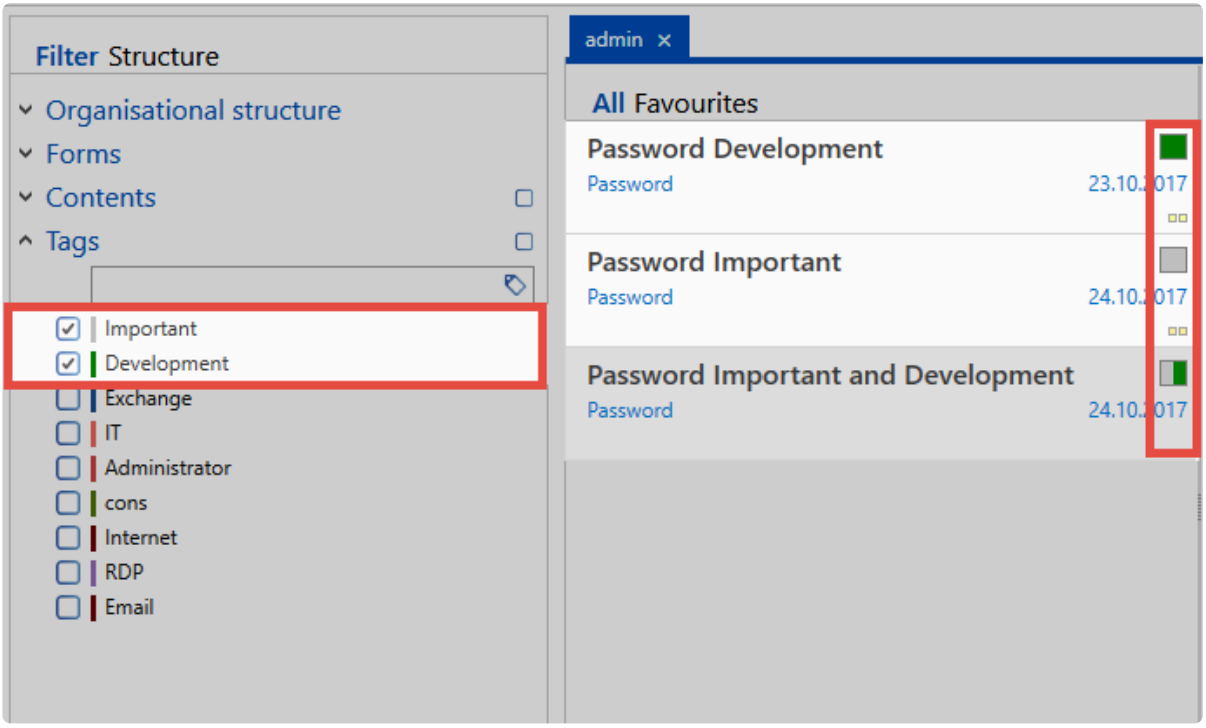
Advanced filter settings

Linking filters

The two options for linking the filter criteria are very 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, the user wants 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.

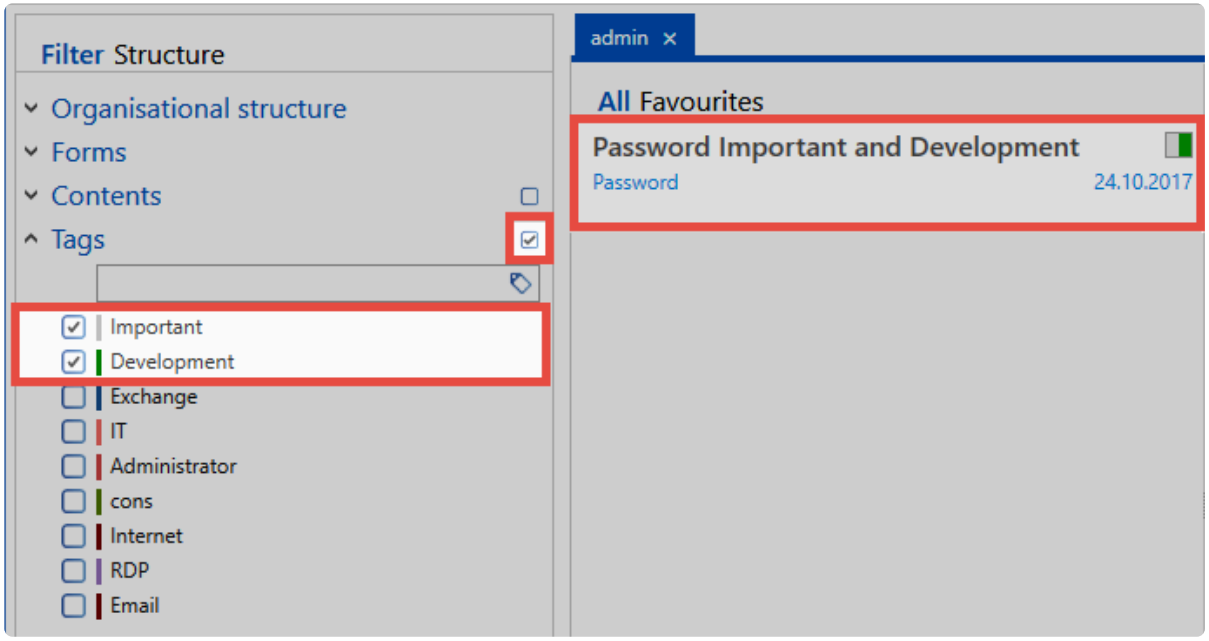


Due to the colour coding of the tags in the records, it can be seen that the first two records have one of the tags, while the third one has both tags. However, all three are included in the results. **At least one filter criterion must be met**.

2. Logical “And operator”

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

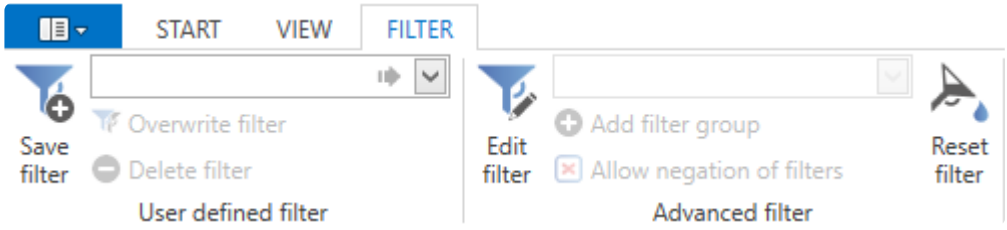




In contrast to the "OR link", the "AND link" must fulfil both criteria. Accordingly, only those records that have both the tag **"Important"** and the tag **"Development"** are listed in the results for this example.

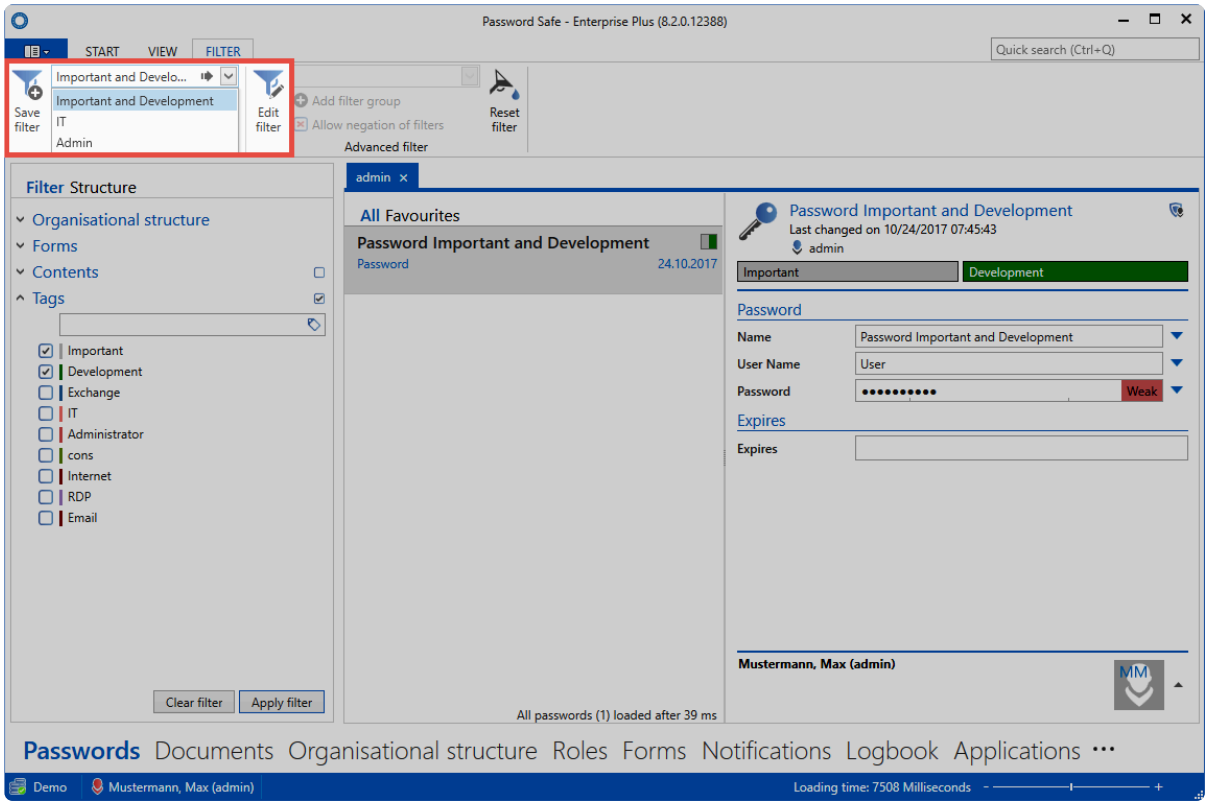
Filter tab in the ribbon

The filter management can also be found in the ribbon. Here, it is possible e.g. to expand the currently configured filter criteria, save the filter, or simply clear all currently applied filters.



Saving, editing, and deleting filters

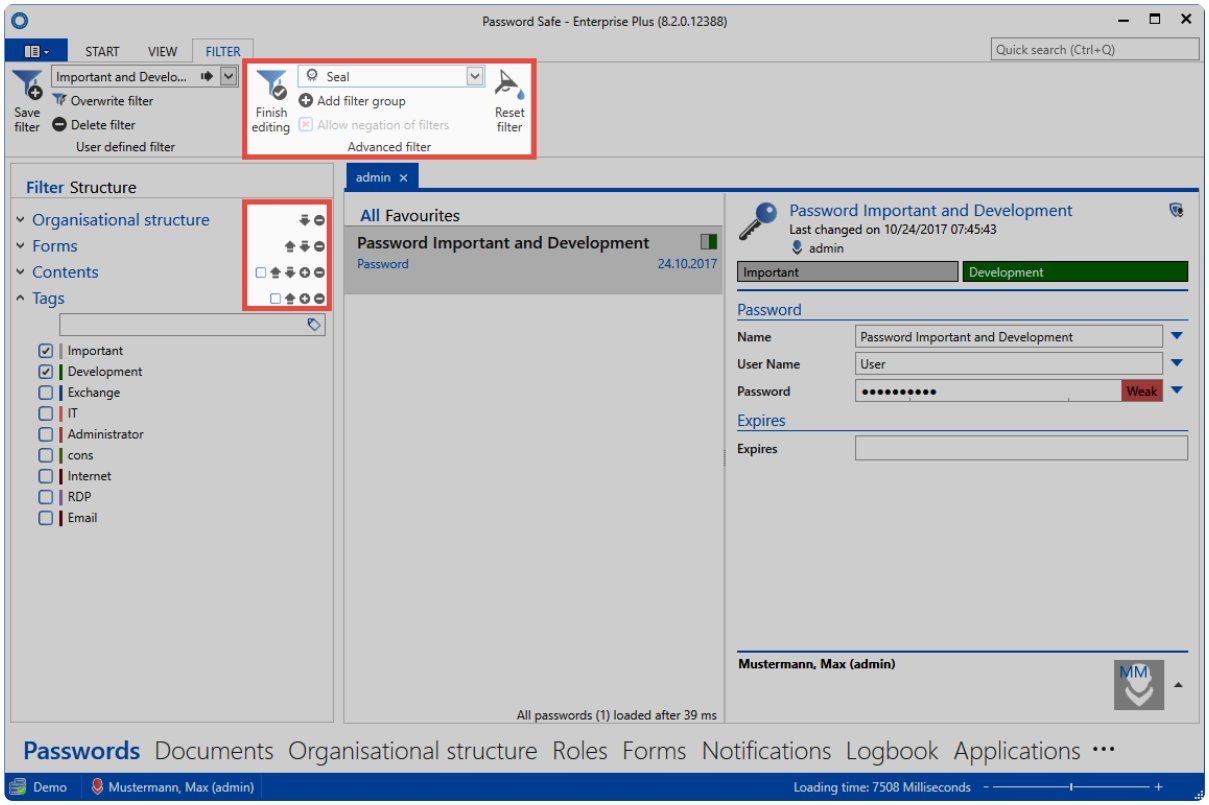
In many cases, it is recommended to store defined filters. In this way, it is possible to make efficient use of filter results from previous searches. The button "**Save filter**" directly prompts you to assign a meaningful name to this filter. The filter is saved according to the criteria currently 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.

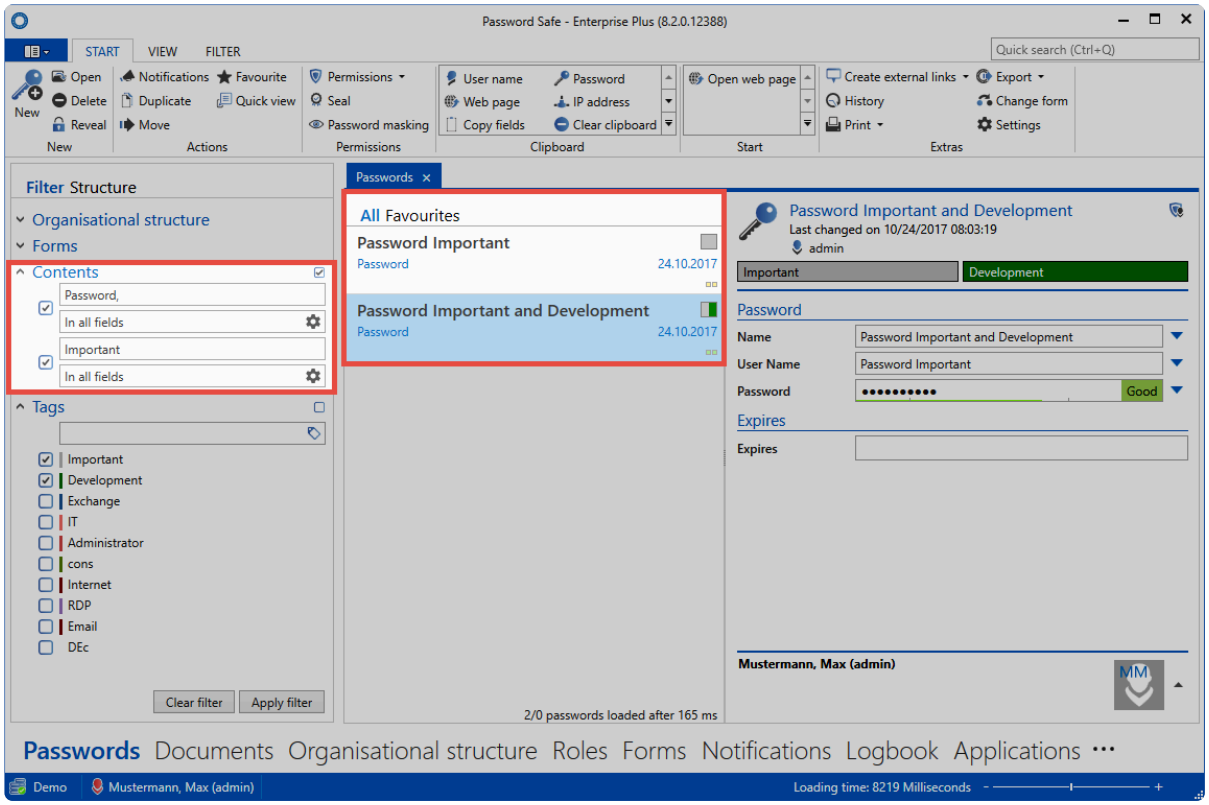
Advanced filter

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.



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

It is often important to be able to negate the filter.

Relevant settings

The following option must be taken into account:

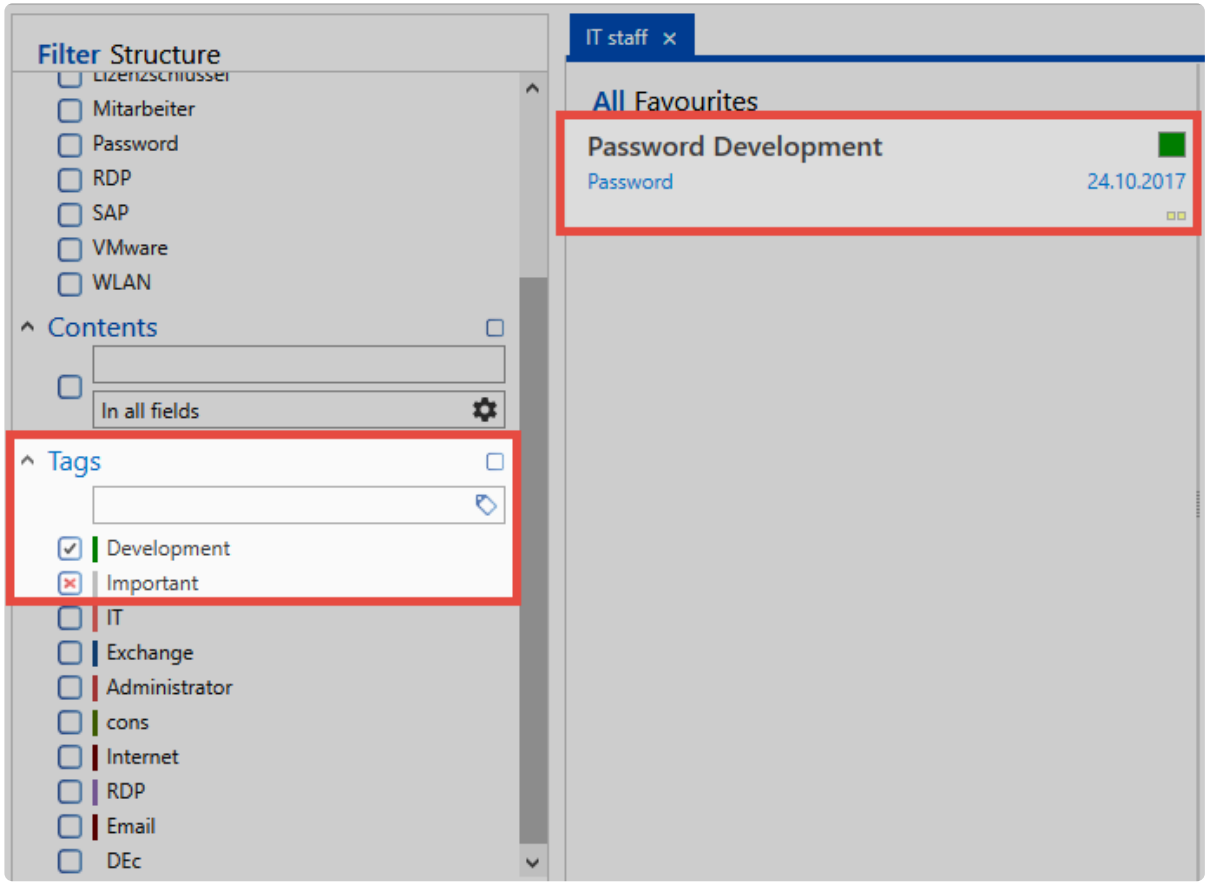
Setting

- Can use filter negation

It is also possible to negate criteria in edit mode.



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:

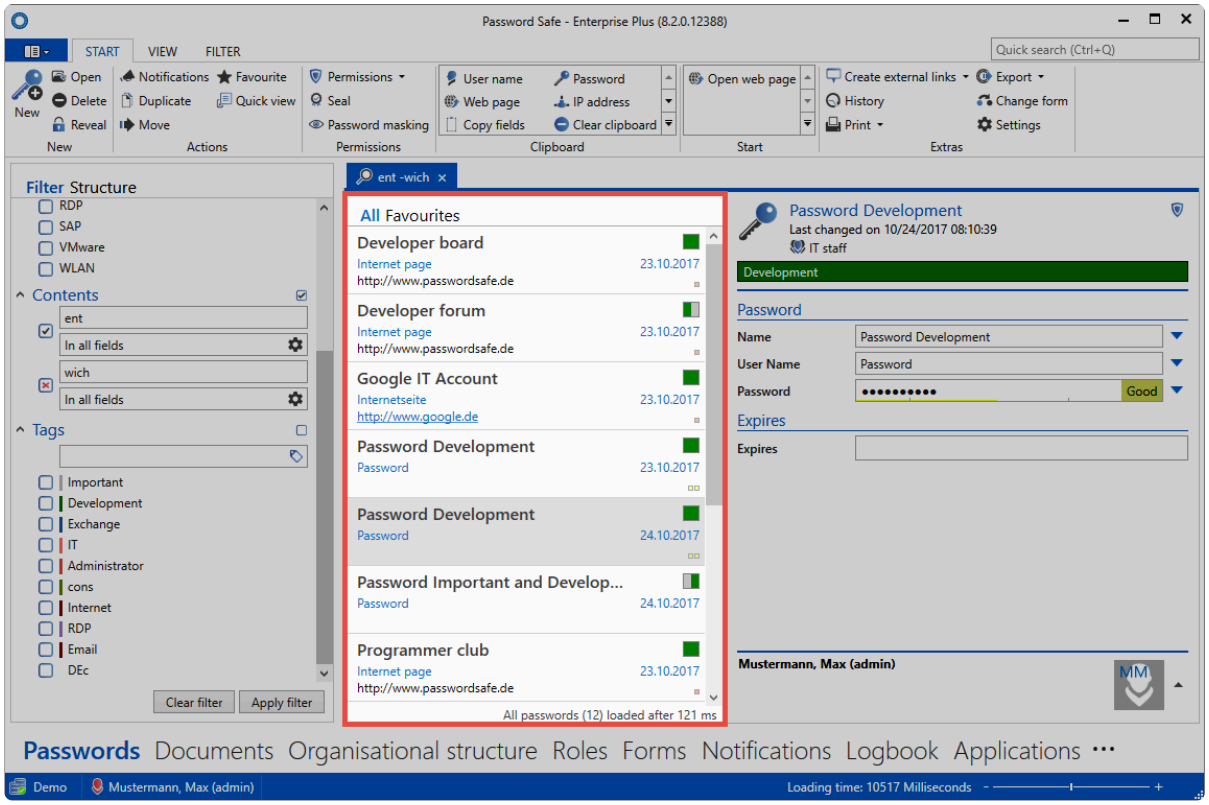
*"Deliver all records that have the tag "Development" but are not tagged with "Important"!

> ! 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.

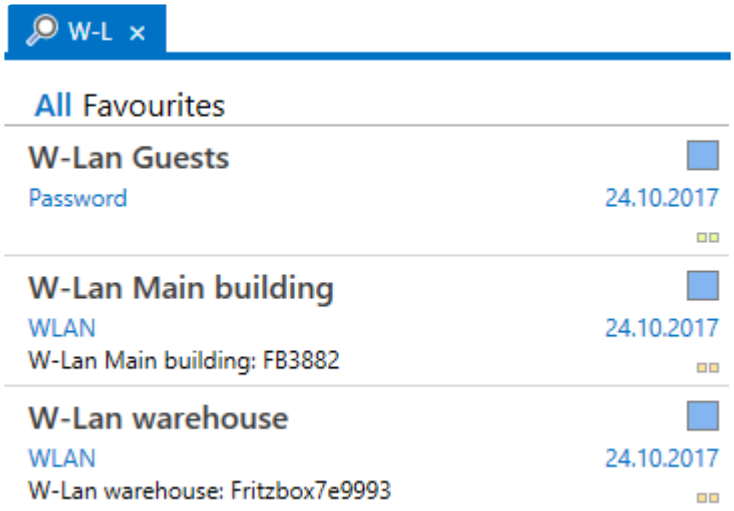


At the bottom of the list view, the number of loaded records and the time required for this are shown.

> 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.

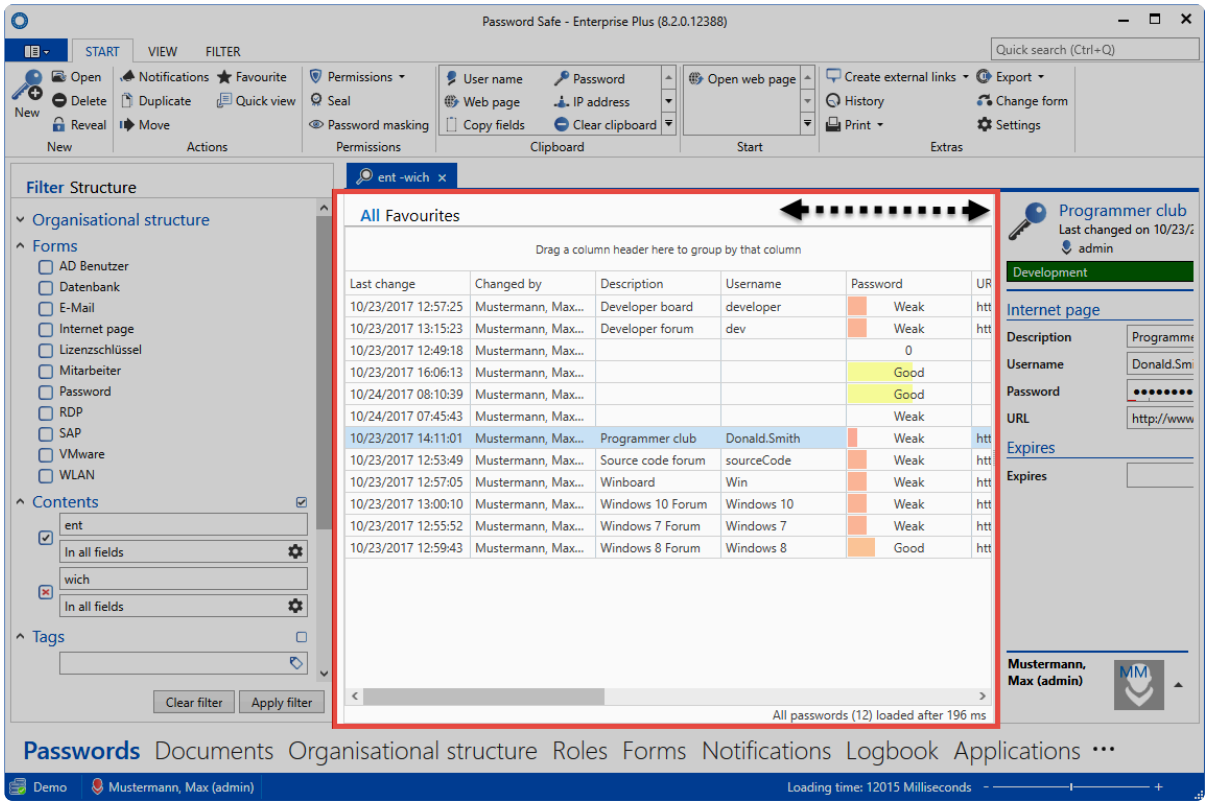
Searching in list view

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.



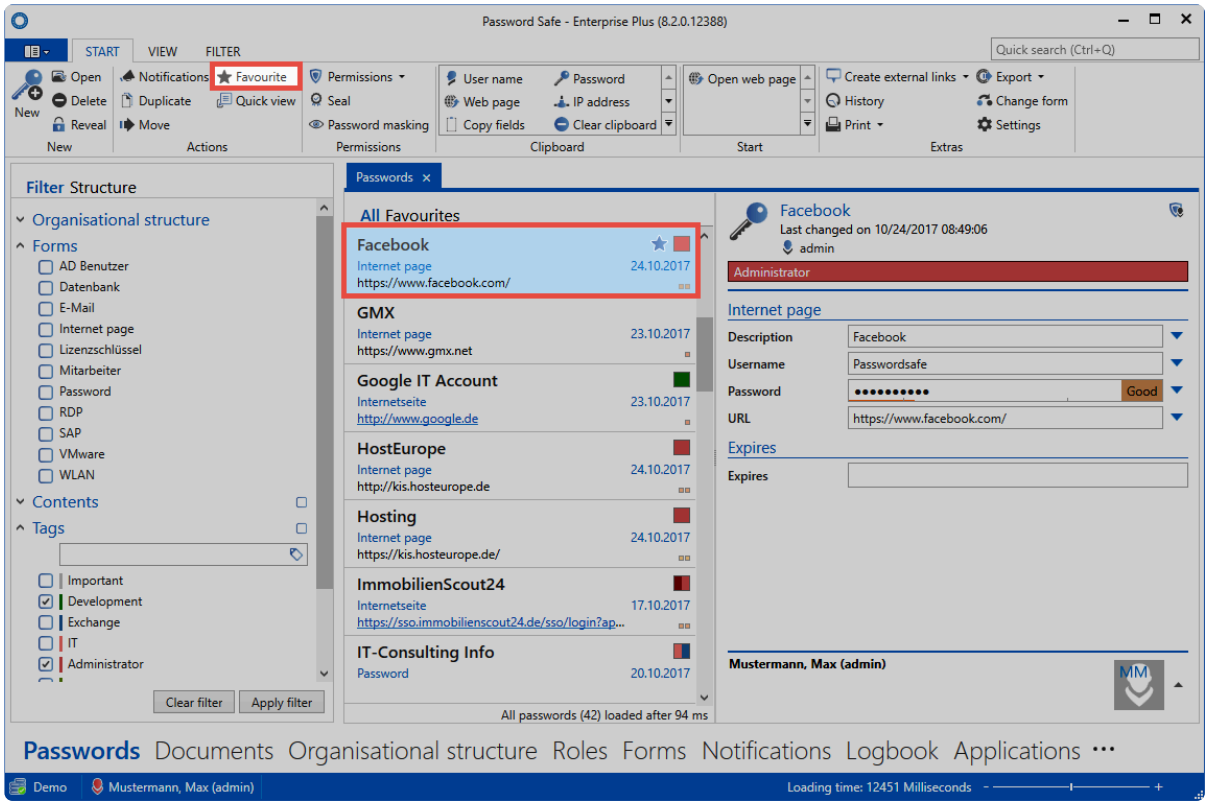
Detailed list view

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

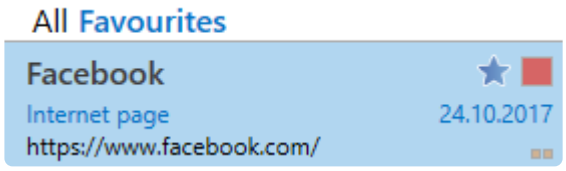


Favourites

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.

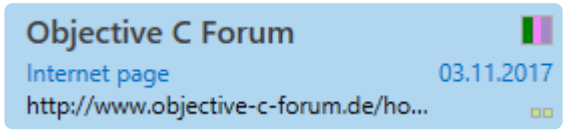


You can filter for favourites directly in the list view. For this purpose, simply switch to the **“Favourites”** tab.



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.

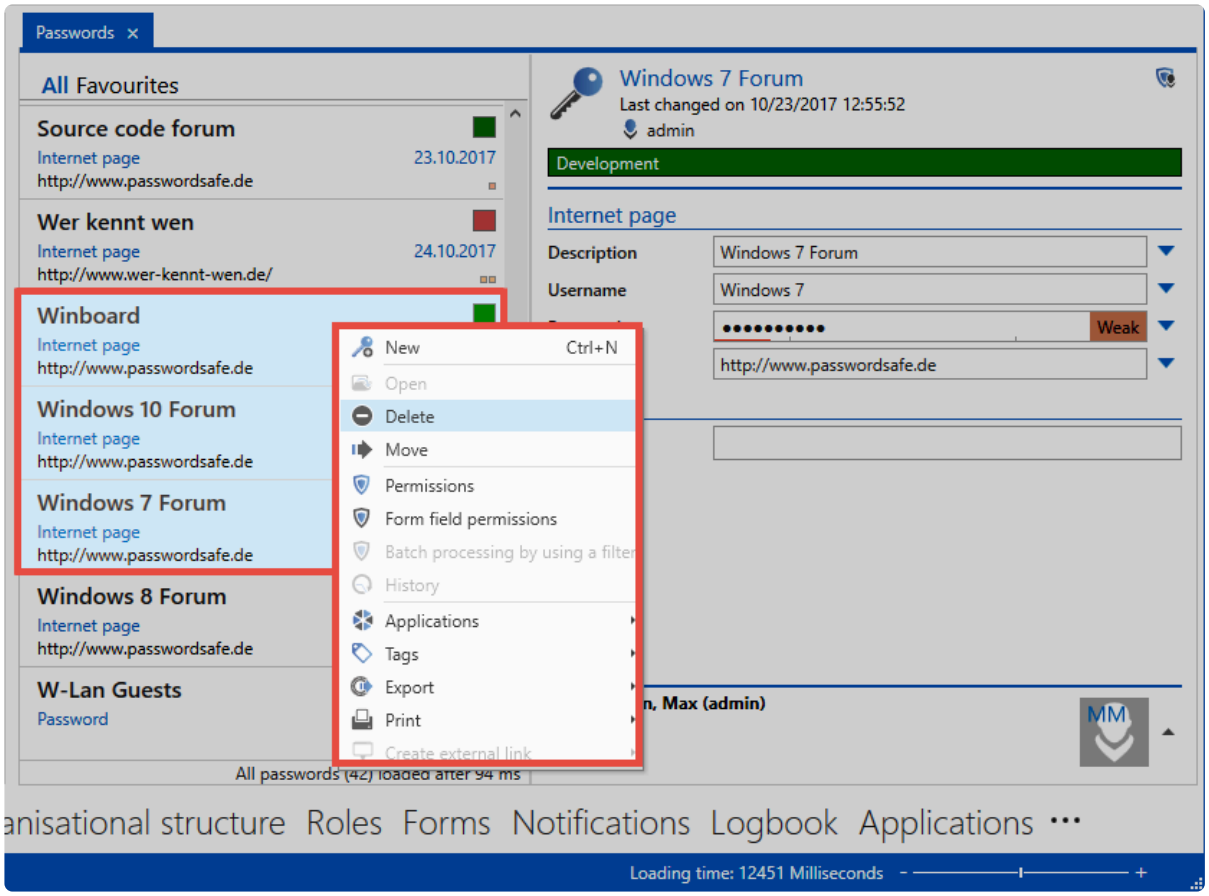


The information visible underneath the password name is taken from the info field for the associated form and will be explained separately

Working with records

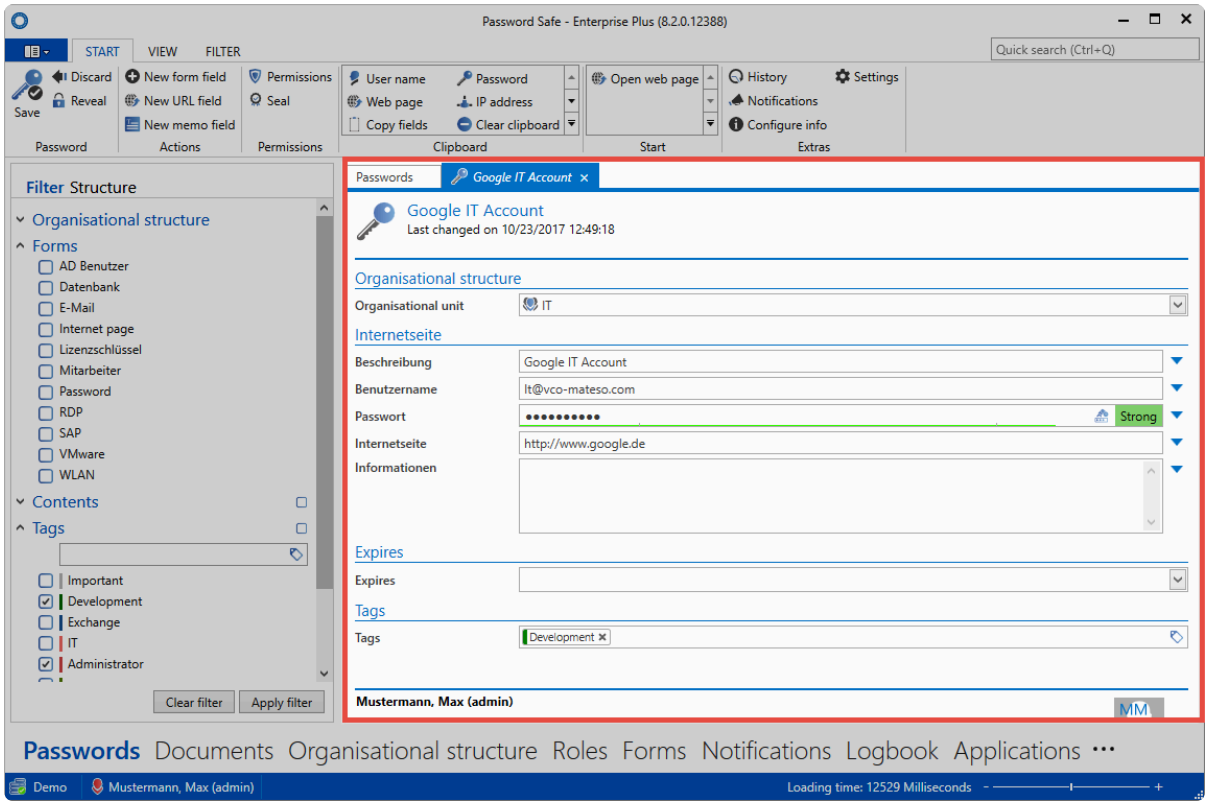
All records that correspond to the filter criteria are now displayed in list view. These can now be opened, edited, or deleted via the ribbon. Many functions are also available directly from the context menu. You

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.



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.

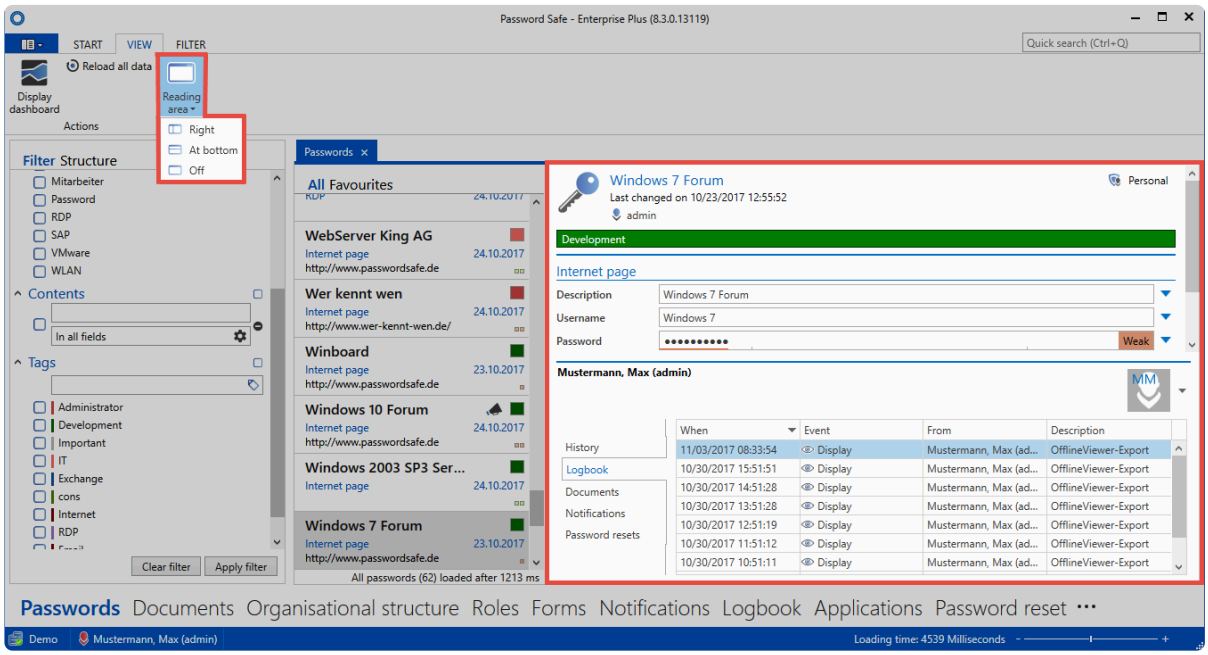


Working with data records depends of course on the type of the data record. Whether passwords, documents or organisational structures: The handling is partly very different. For more information, please refer to the respective sections on the individual “modules”.:#psr-client

Reading pane

What is the reading pane?

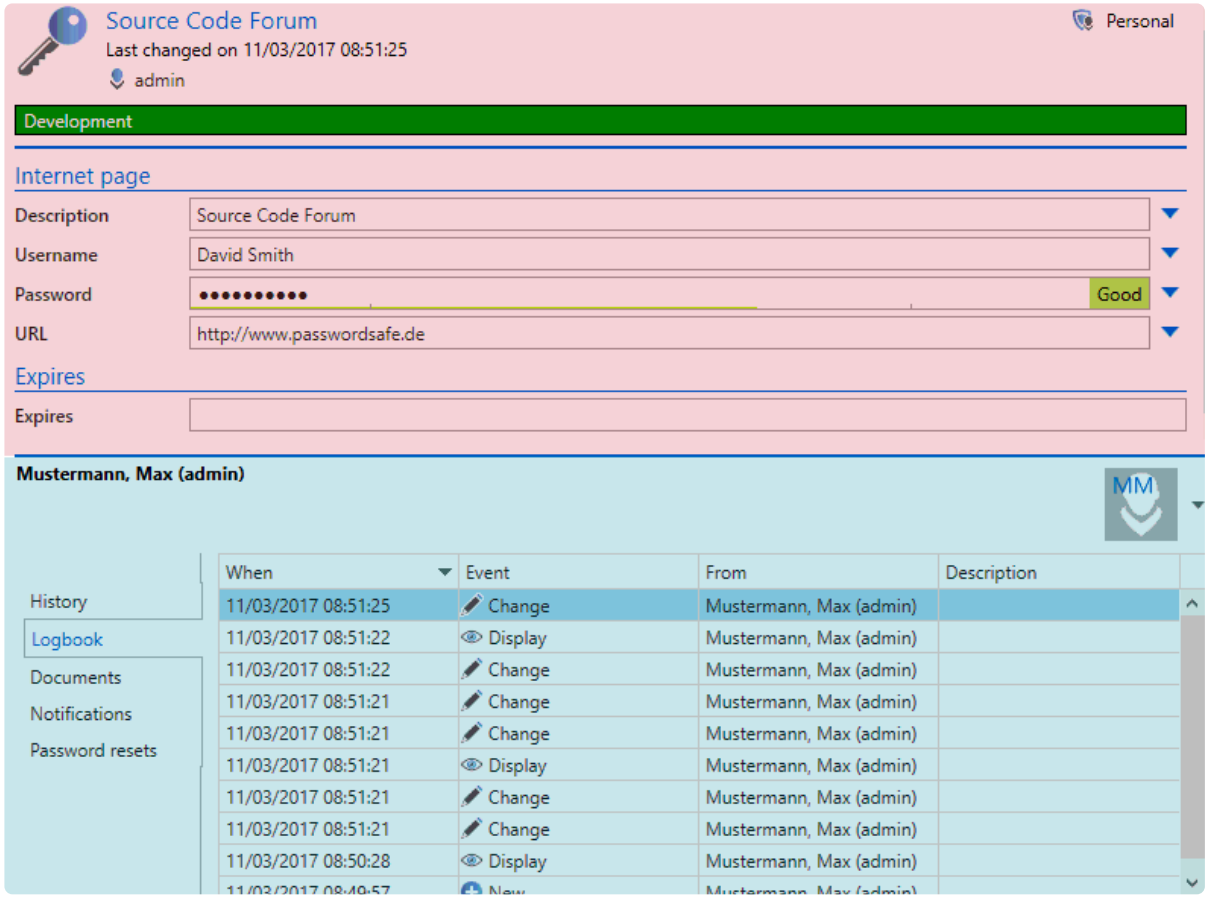
The reading pane on the right side of the client always corresponds to the detailed view of the selected record in the list view and can be completely deactivated via the ribbon. In addition, you can configure here the arrangement of the reading pane – either on the right, or underneath thelist view.



Structure of the reading pane

The reading pane is divided into two areas:

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



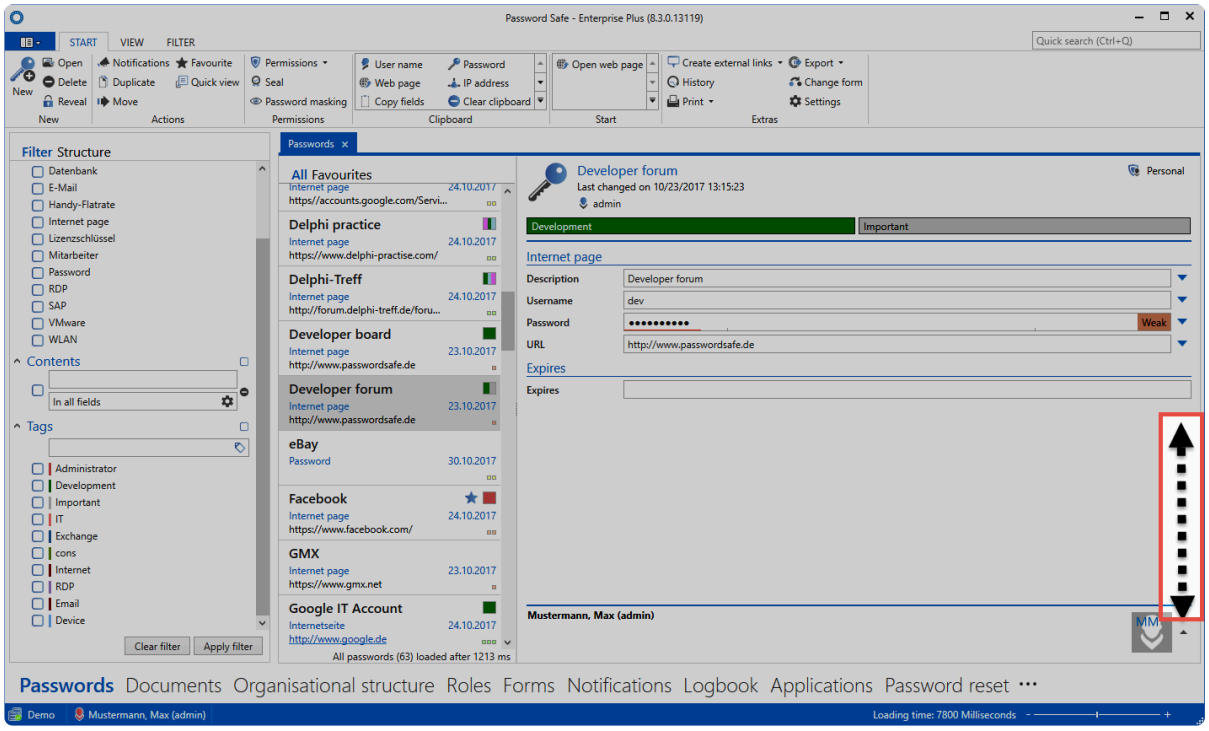
1. Details area

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.



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!

Relevant rights

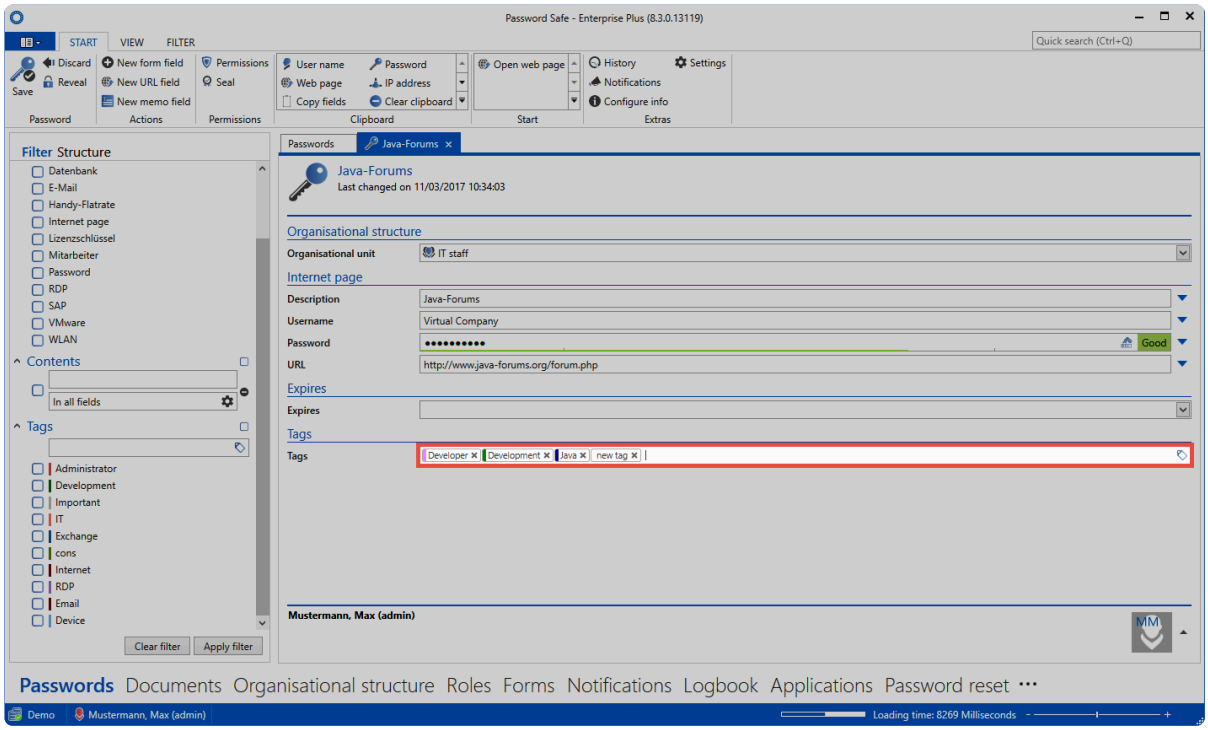
The following option is required for creating new tags.

User rights

- Can add new tags

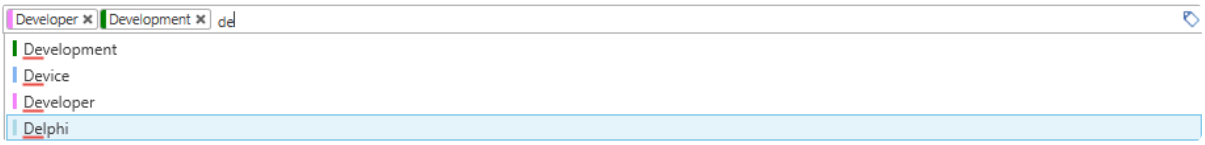
Adding tags to records

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.



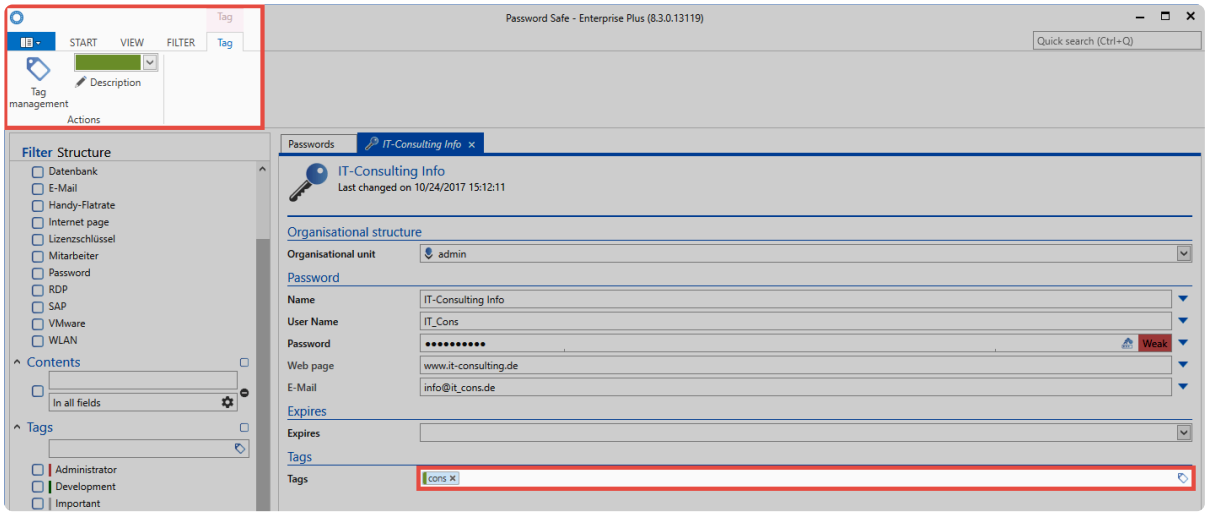
The operation is intuitive. From the third entered letter, existing tags are searched for full text. If the

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”.



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.



Management of tags

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

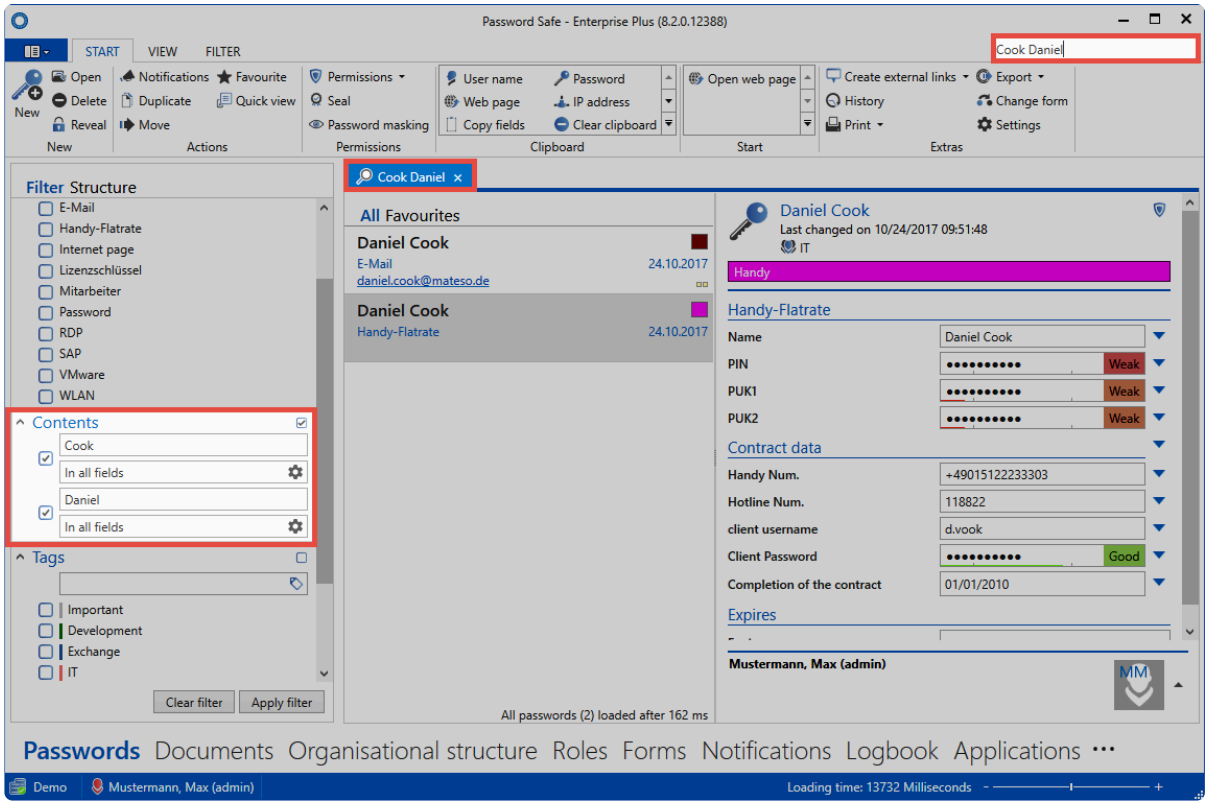
Search

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.



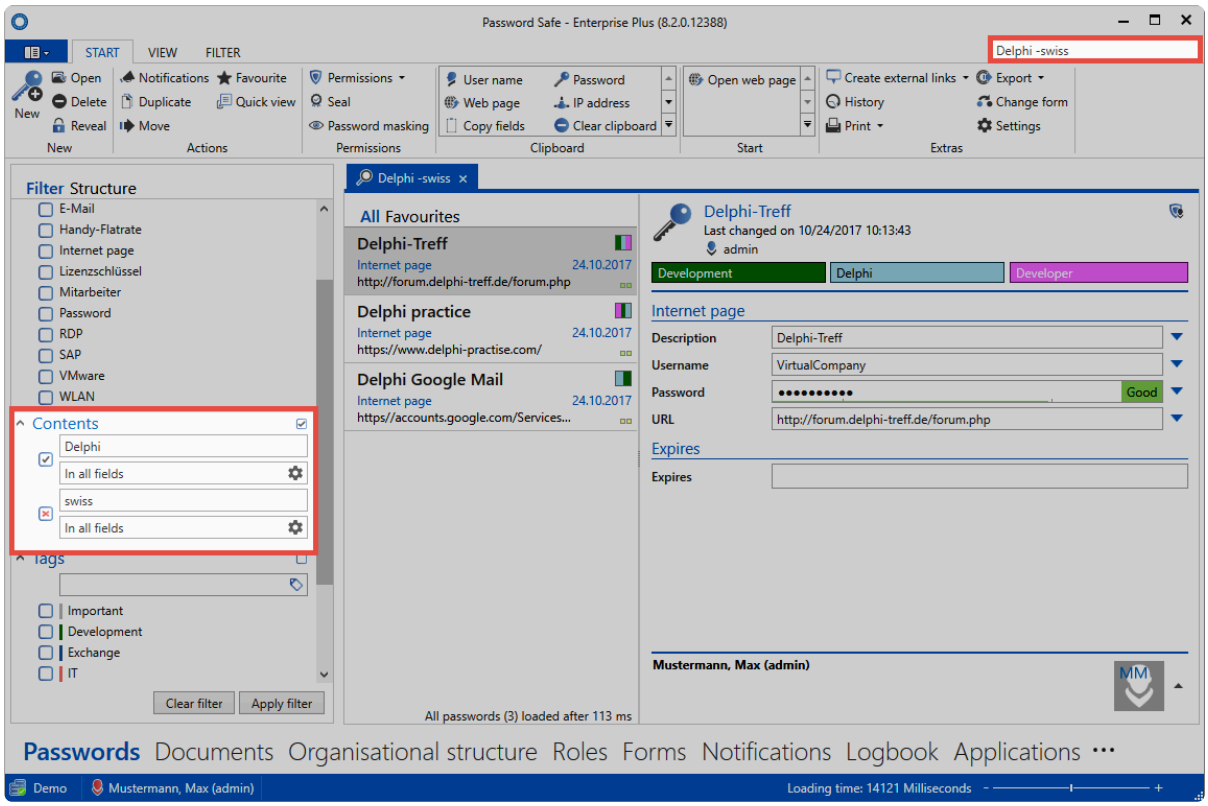
The fast search is closely linked to the filter, because search queries are converted directly into one or several content filters. You can also separate search terms using spaces, for example, **Cook Daniel**. Note that this search creates two separate content filters, +which are logically linked with “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

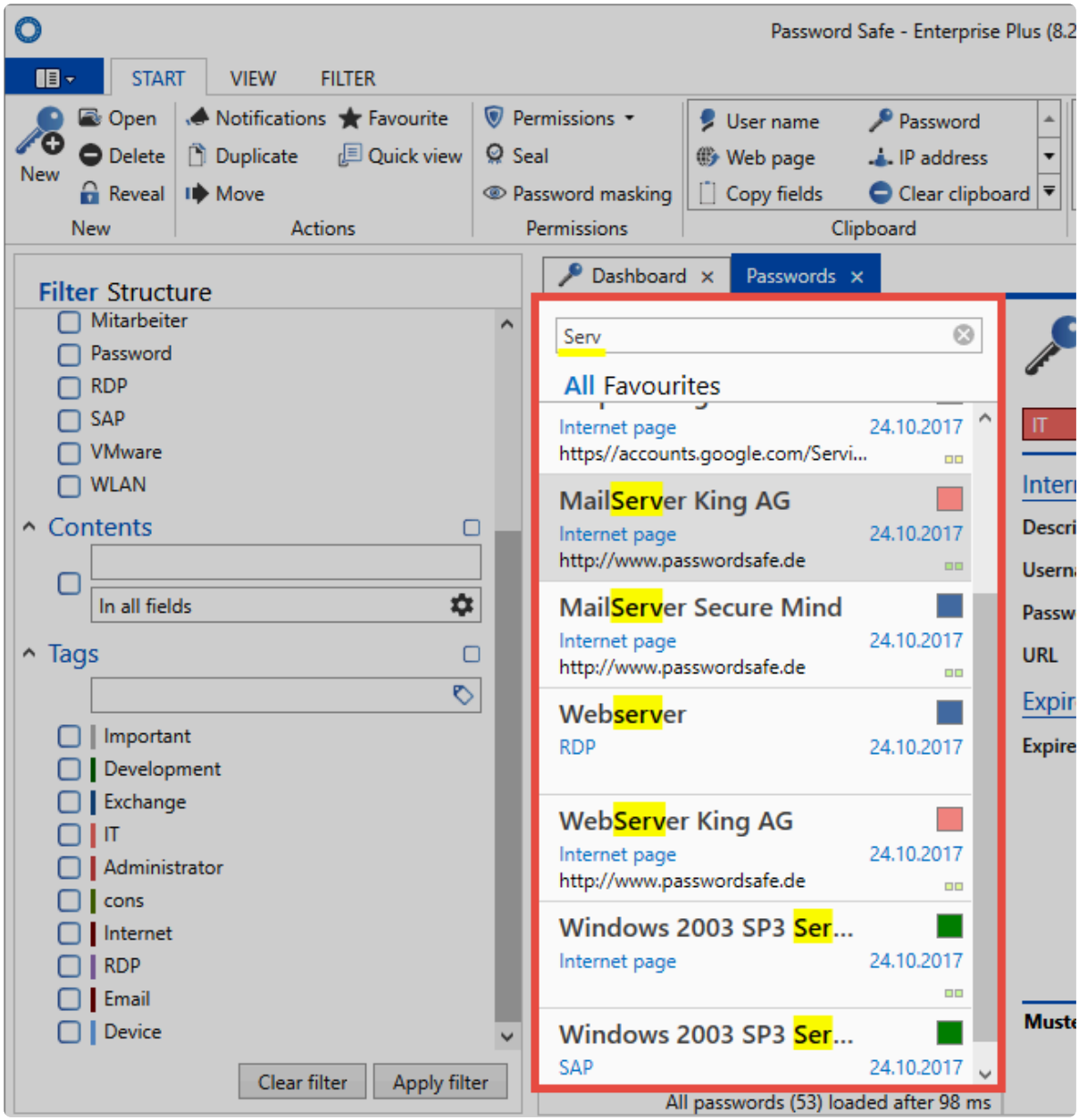
Negations restrict the results to such an extent that certain criteria may not be met. The following example searches for all records that contain the expression * Delphi **, but not the expression * swiss**

***. The notation, which must be entered in the quick search, is: *Delphi -swiss**



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**”

Print

What can the print function do?

It is often necessary to print out data stored in **Password Safe** for documentation purposes. The **Print** function is available in numerous areas of **Password Safe** for this purpose. It is possible to print out records such as e.g. passwords or also information about organisational units and much more.

Relevant rights

The following rights are relevant.

Record rights

- The **Print** right for the relevant record is required in each case.

User right

- Can print

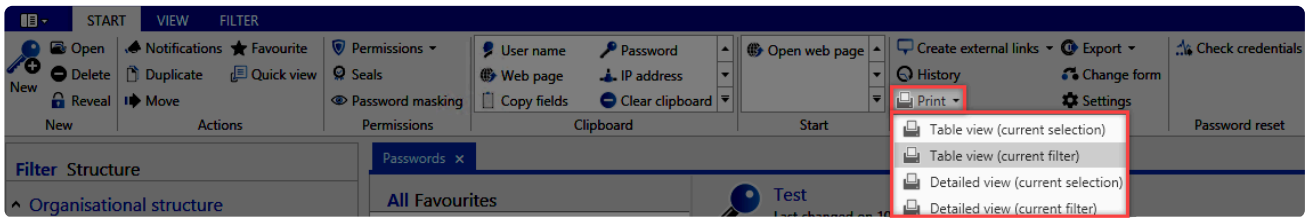
Availability

The print function is available in the following modules:

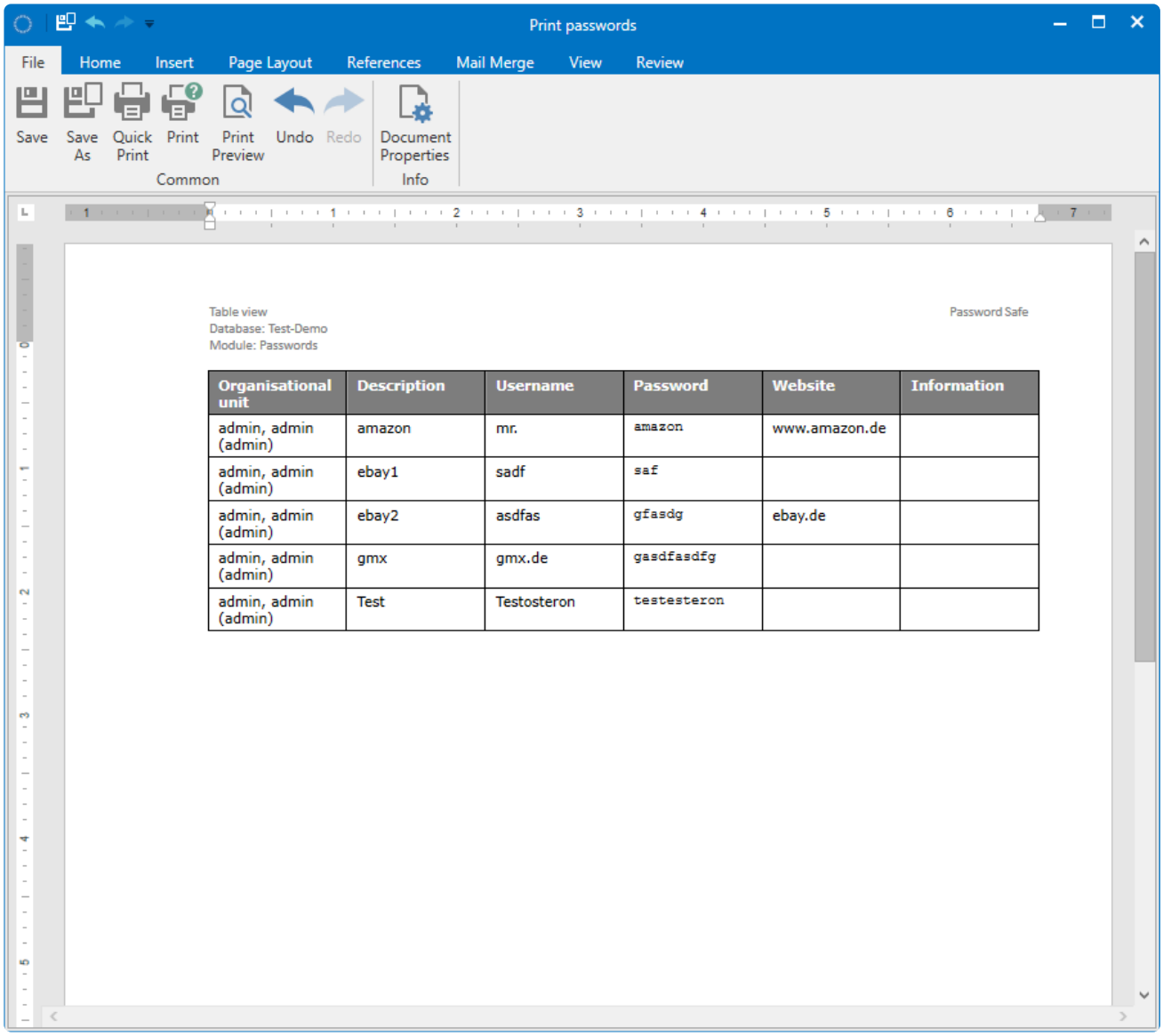
- Passwords
- Documents
- Organisational structure
- Roles
- Forms

Using the print function

The print function can be called up via the ribbon.



Firstly, it is necessary to select whether you want to print a table or a detailed view. The amount of data can also be defined. The individual menu items are described in detail further down in this section. After making your selection, the data is firstly prepared for printing. Depending on the amount of data, this may take a few minutes. The **print preview** is then opened.



The **print preview** accesses the functions of the printer driver. Depending on the printer or driver being used, the appearance and functions offered by the **print preview** may vary. The individual functions will thus not be described in detail here.

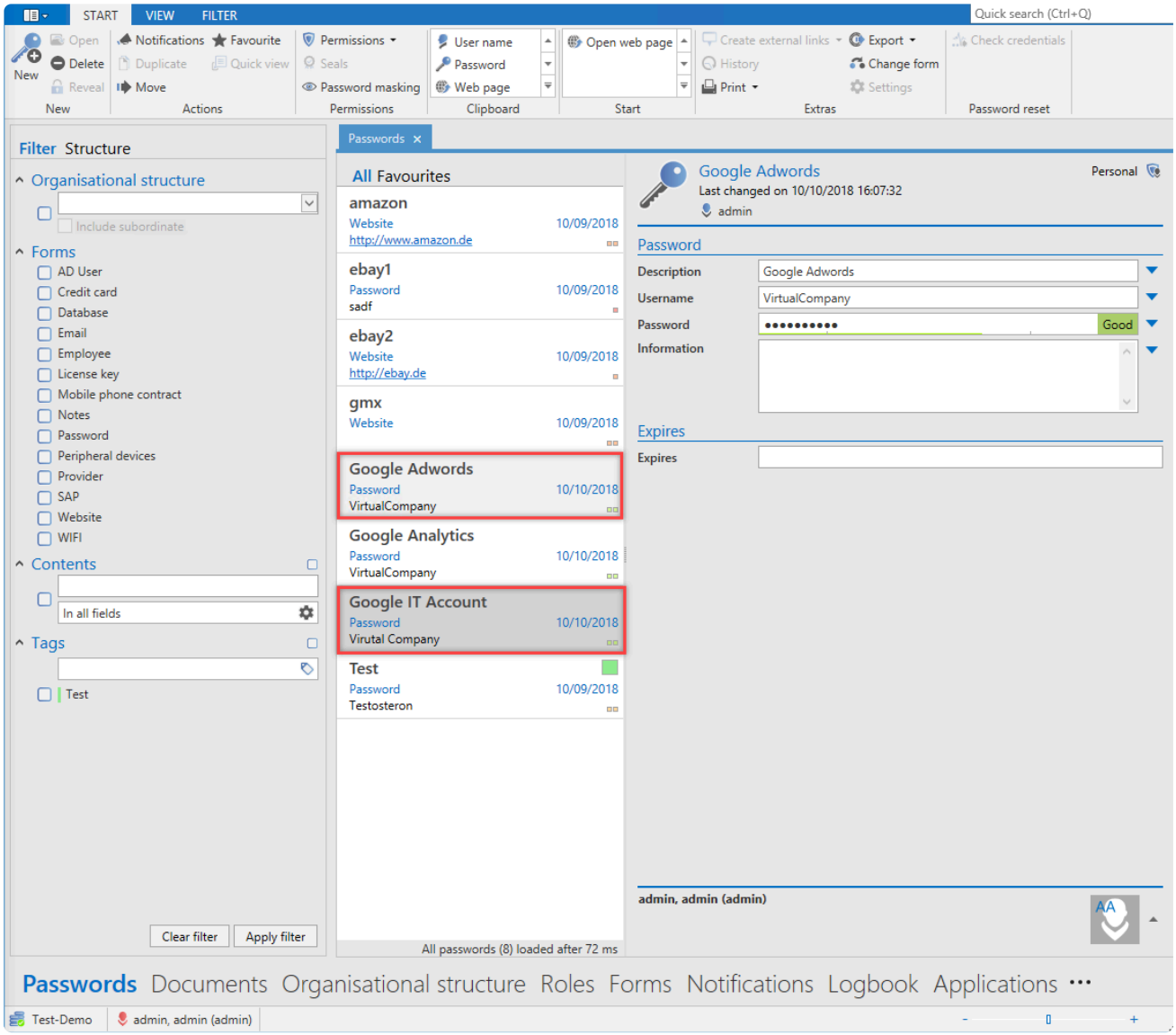
The printing process is ultimately started via the **print preview**. It is also possible to save the view or adjust the layout before printing.

Selecting the data to be printed

There are different options available for adapting the printing result to your personal requirements. The individual menu items will be explained here using the example of printing passwords.

Table view (current selection)

All **selected** records will be printed out. In the following example, **Google Adwords** and **Google IT Account** are thus printed out.



The data is printed here in table form.

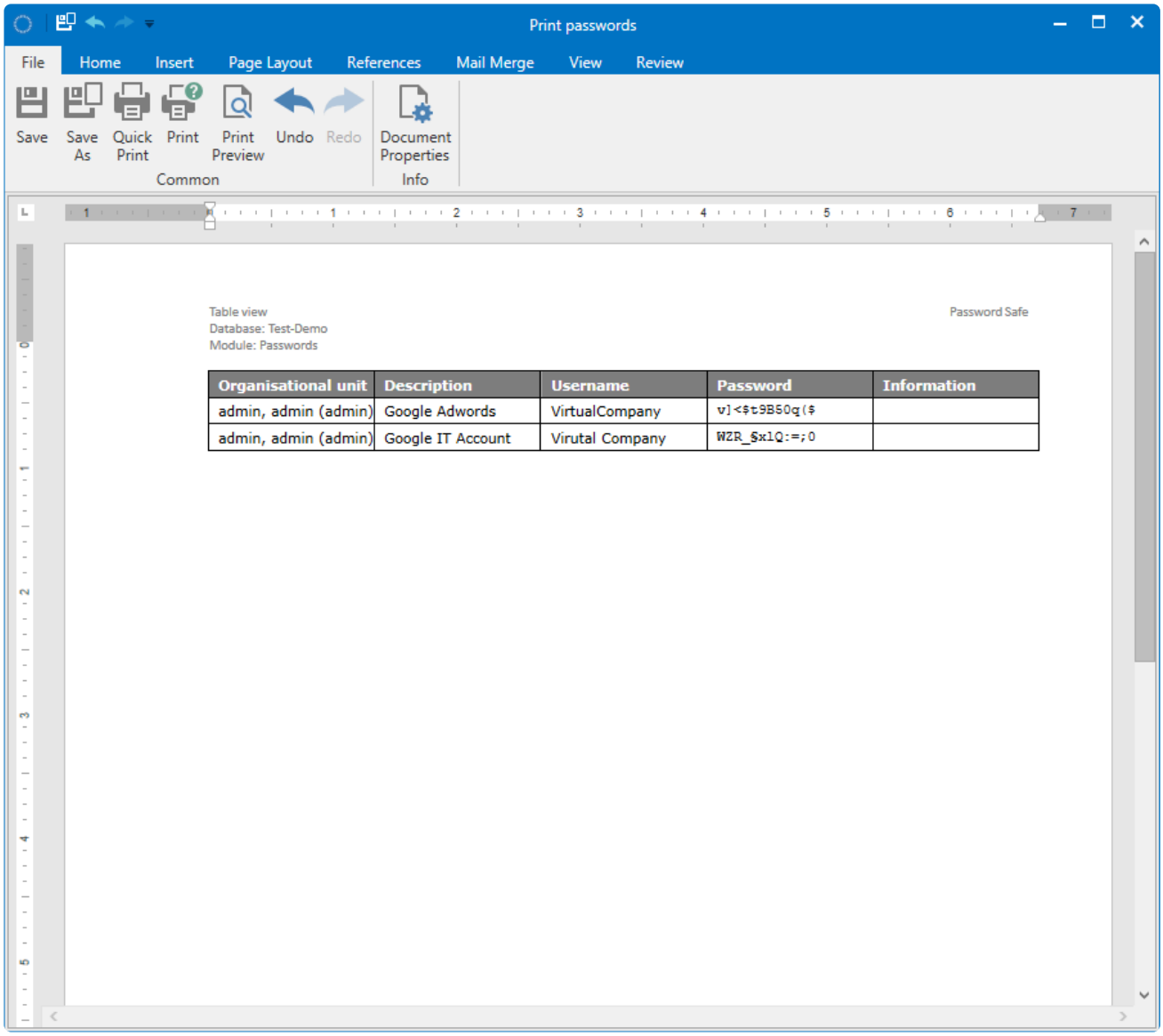
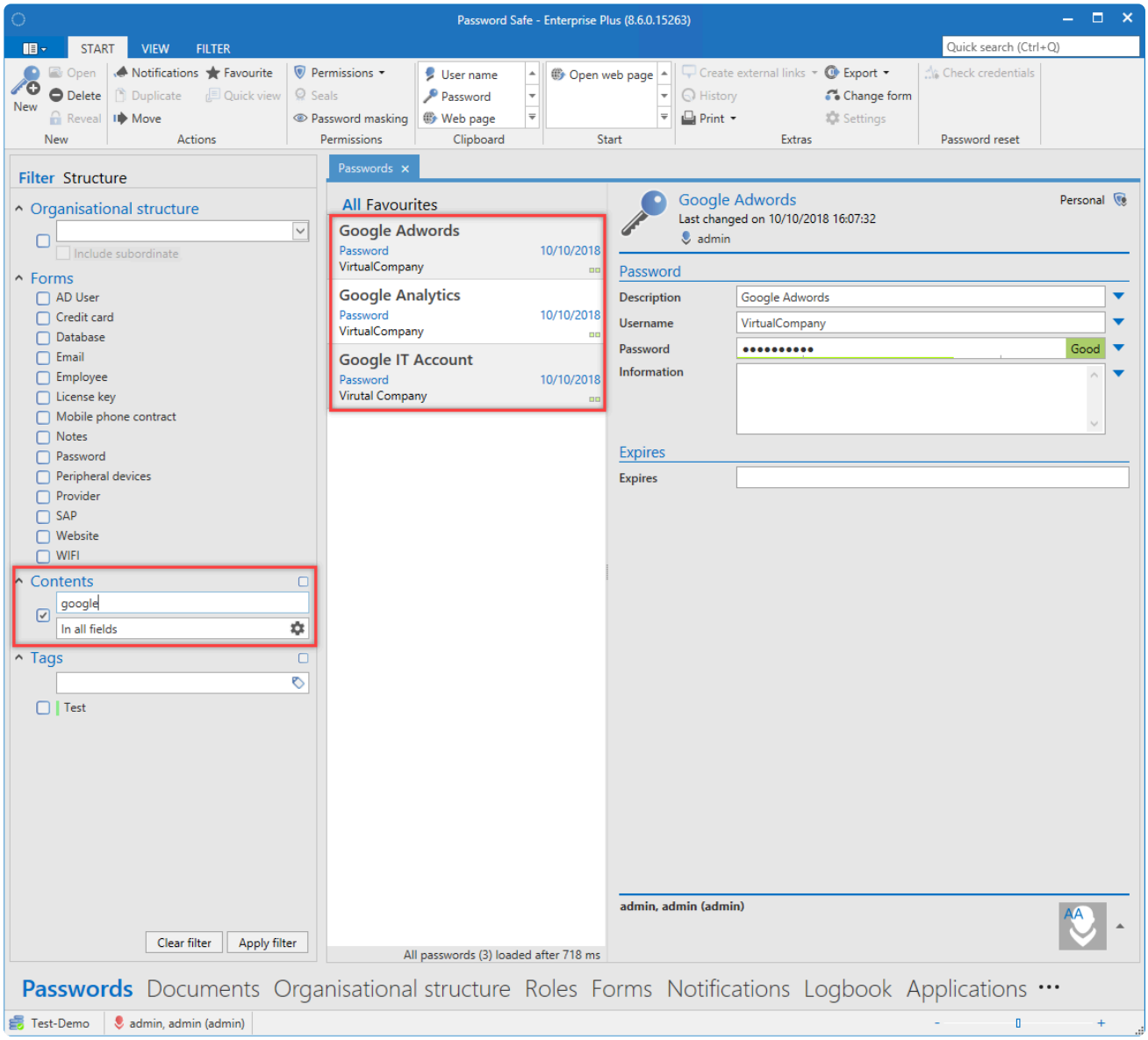


Table view (current filter)

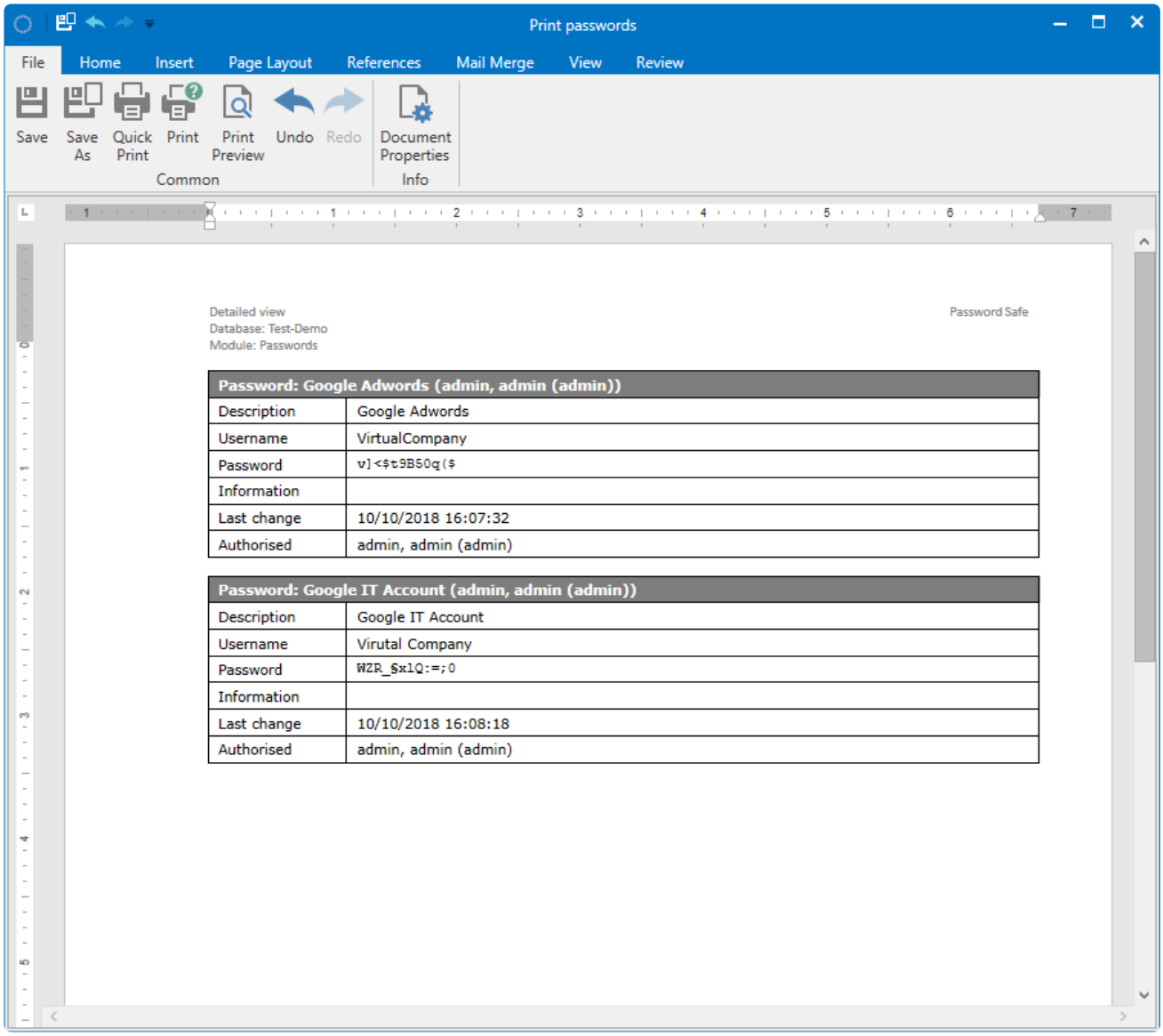
All currently **filtered** records will be printed out here. In this example, all seven records are thus printed out.



They are printed out – as described above – in table form.

Detailed view (current selection)

This option also prints out the currently selected records. However, a detailed view is printed out in this case.



Detailed view (current filter)

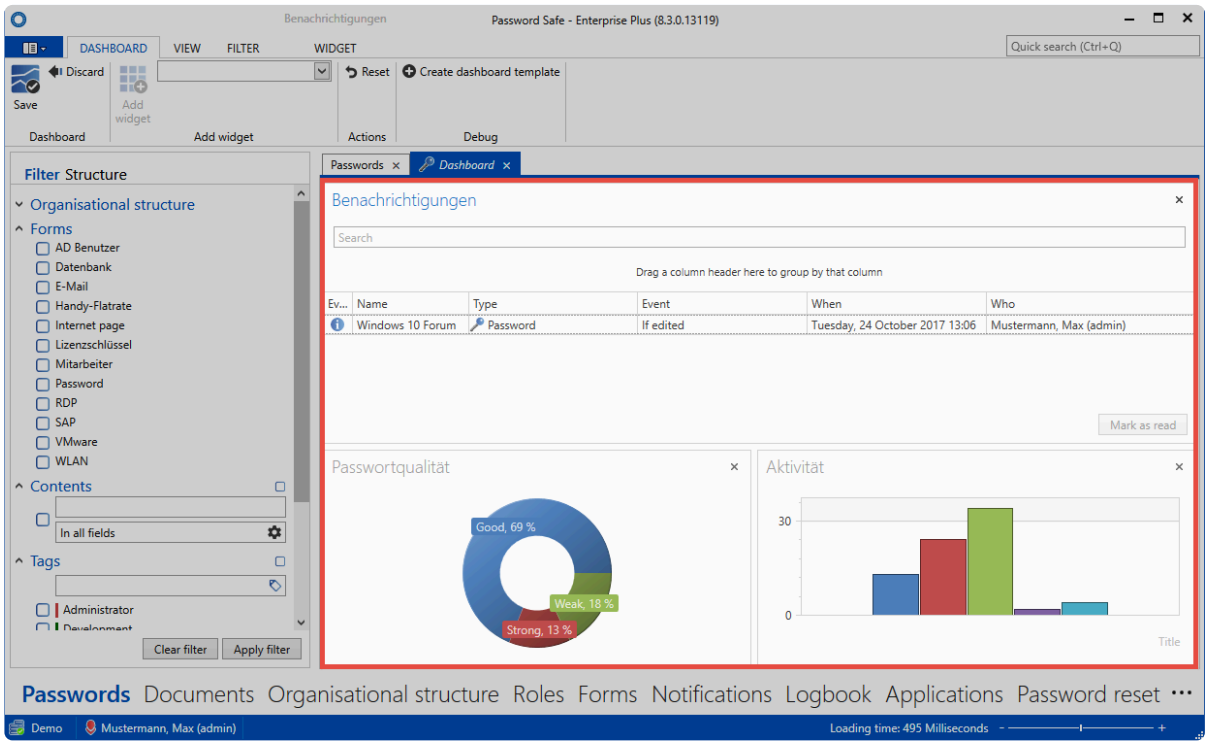
This function can be used to print out all filtered records in detailed view as described above.

> It should be noted that the amount of data generated via this function can quickly become very large.

Dashboard and widgets

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.



Dashboards are available in almost all client modules. A separate dashboard can be set for each individual 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.

Relevant settings

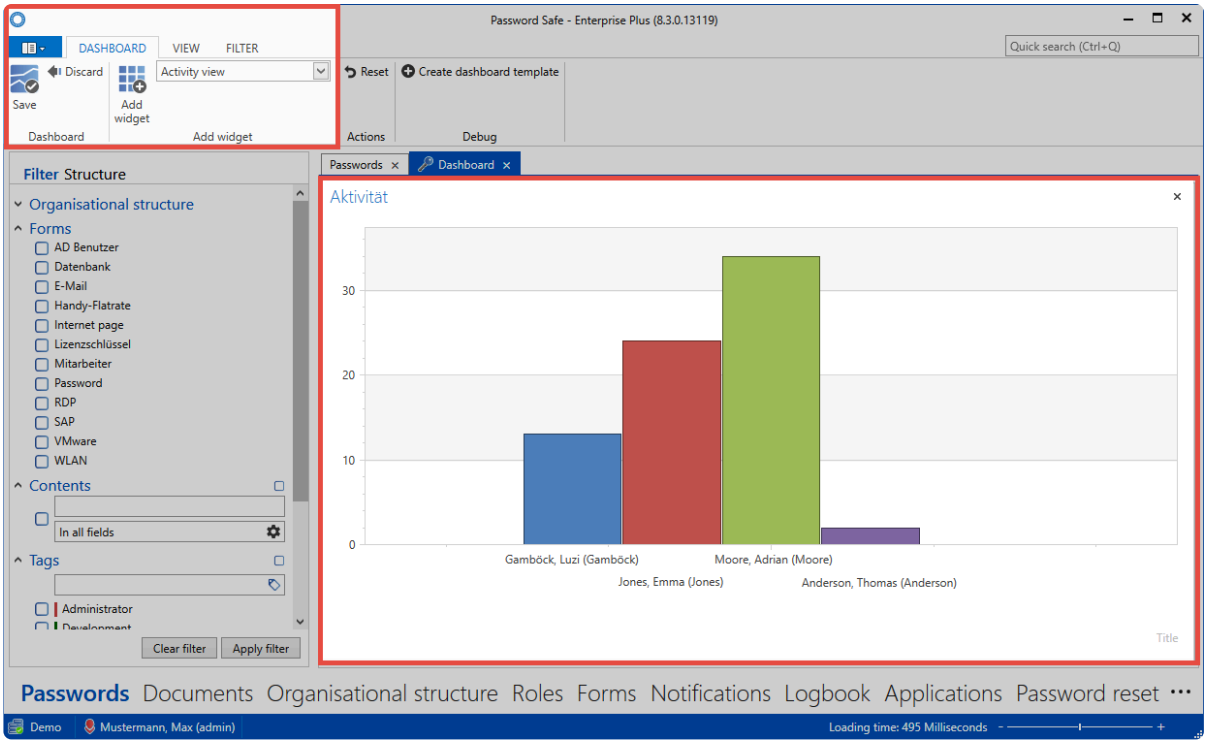
The following options are available in combination with the dashboard and widgets.

Settings

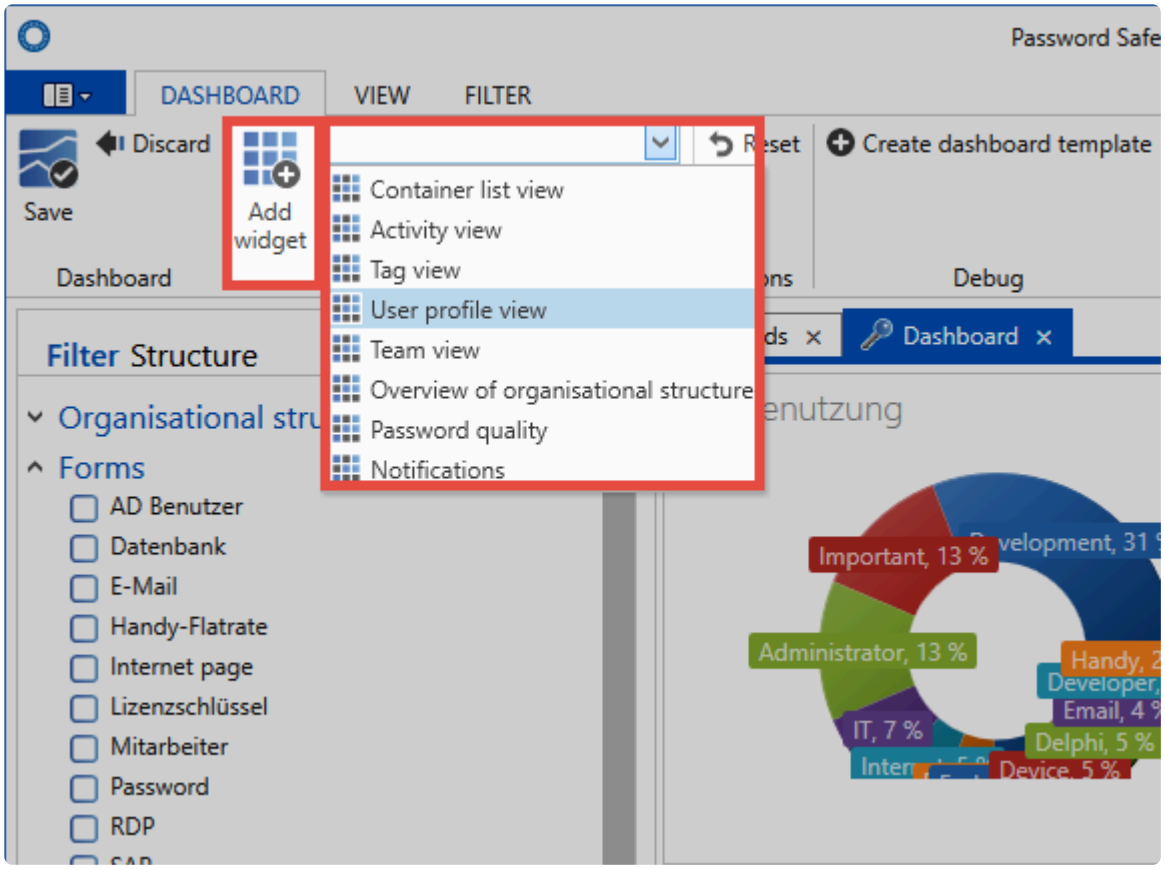
- Display dashboard on startup
- Display module names on dashboard
- Number of allowed widgets
- Display remaining amount of data in the widget

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.

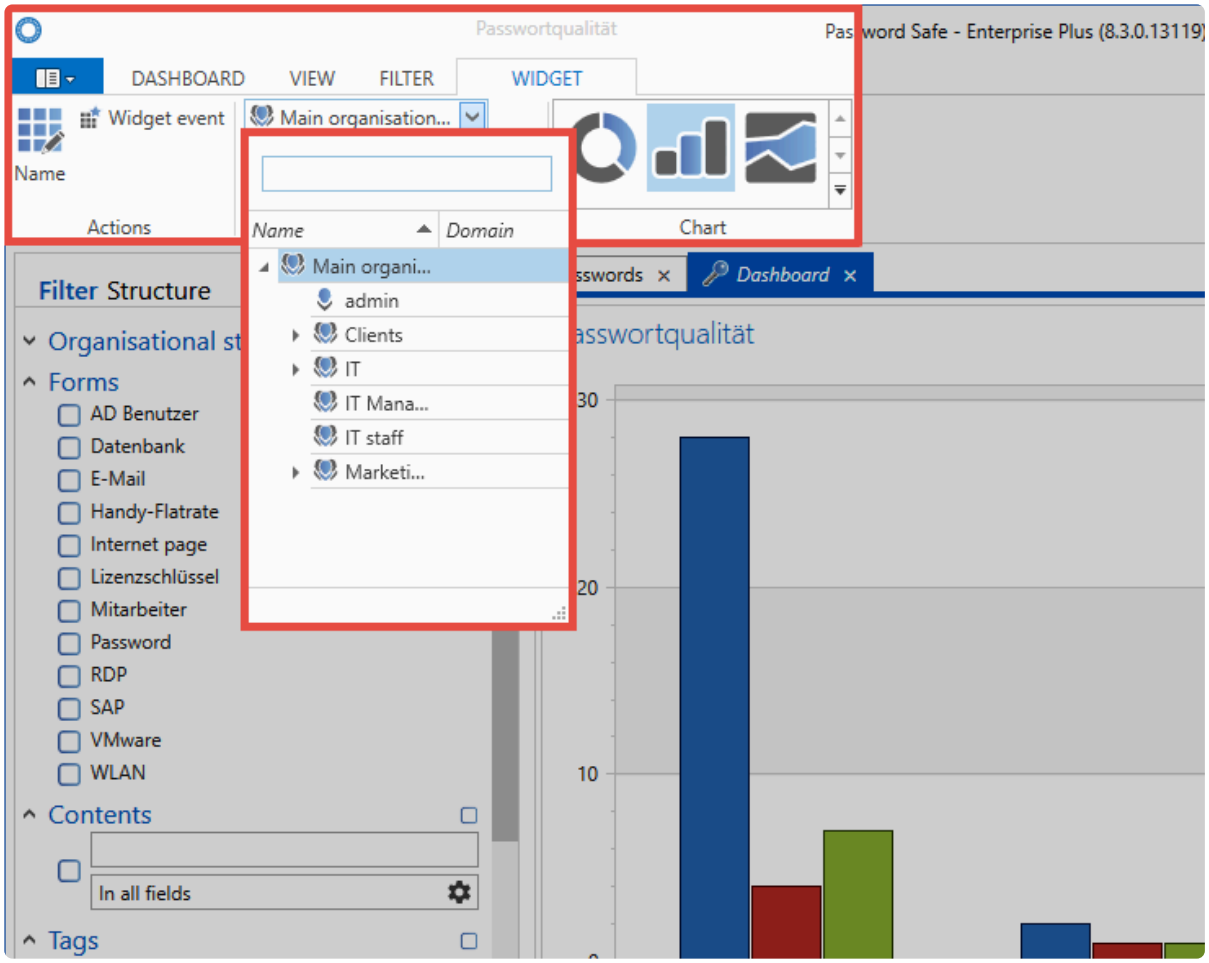


Use the drop-down menu to select the widget to be added * (1) **. Then add the widget to the dashboard using the corresponding button in the ribbon *(2)**. The maximum number of widgets that can be added can be configured in the user settings. In editing mode, any widget can be directly removed from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



Customizing widgets

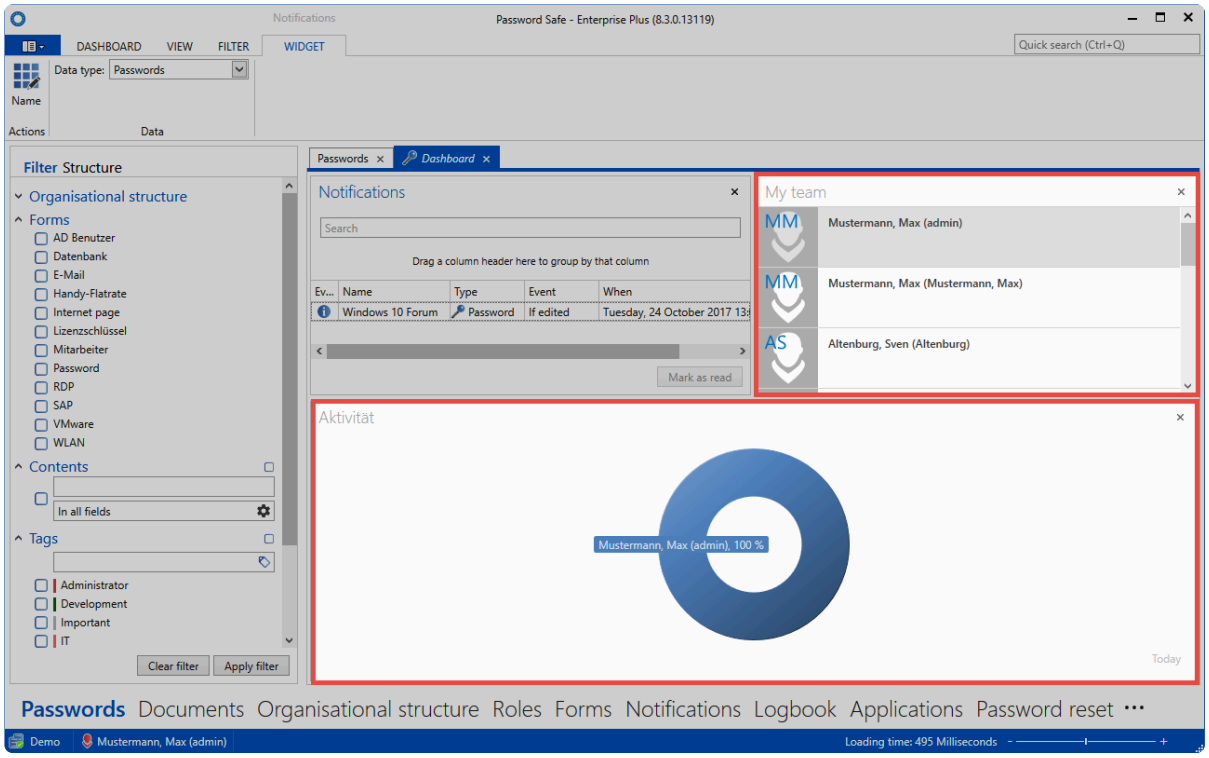
In the editing mode, you can customize each widget separately. To do this, select the widget and switch to the * widget content tab * in the ribbon.



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.

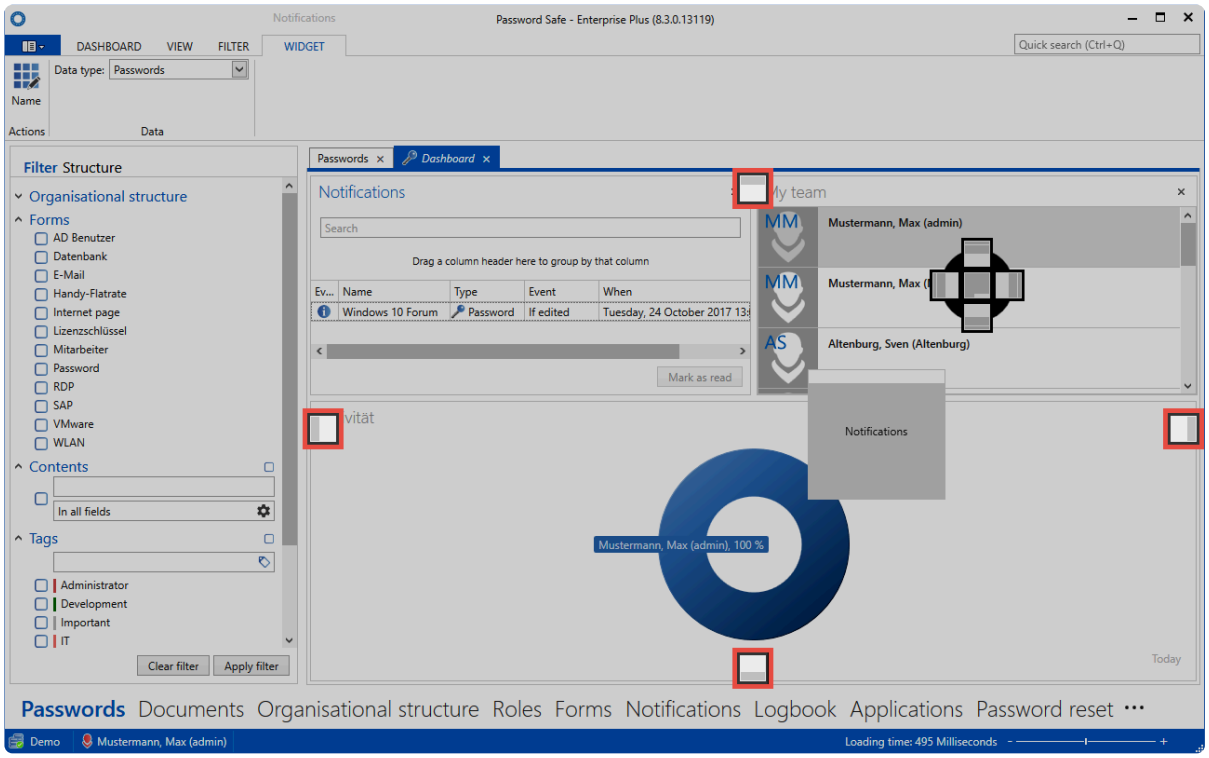
Widget event

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.



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).



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.

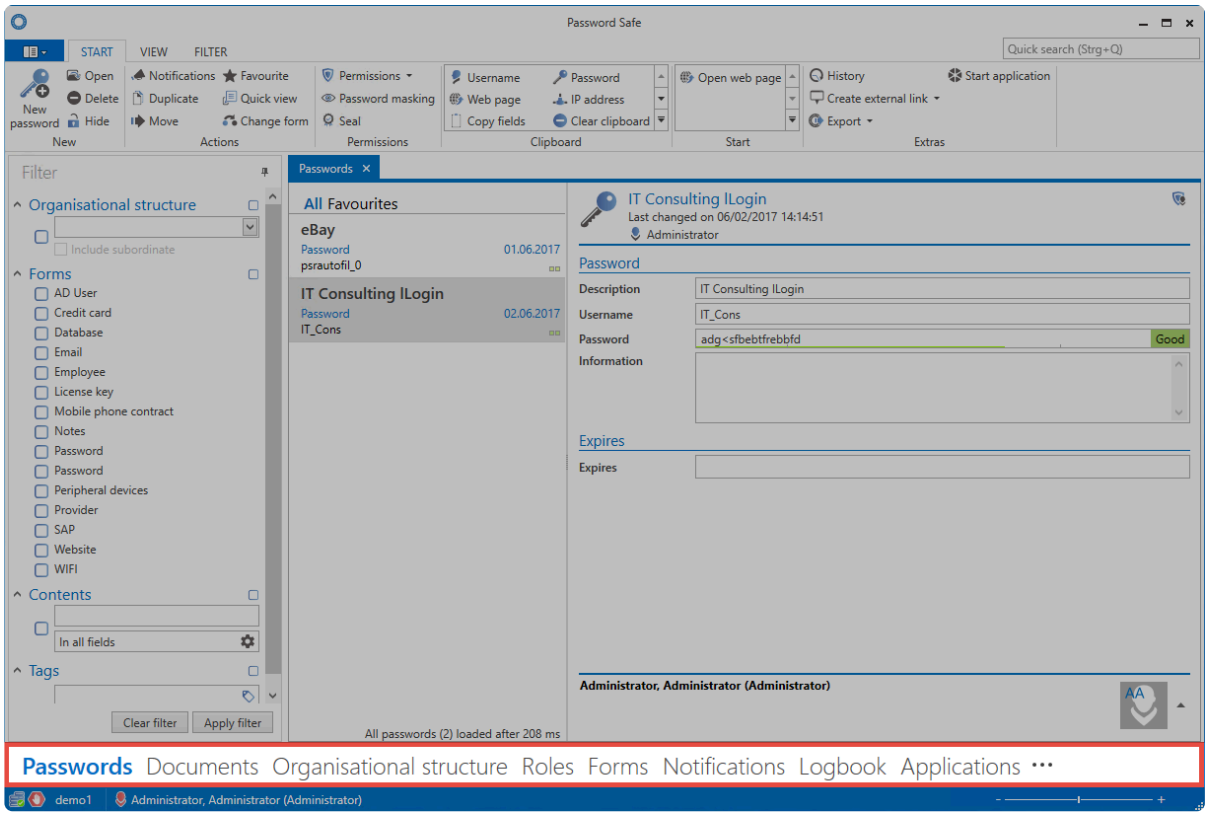
The following keyboard shortcuts are available:

- **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

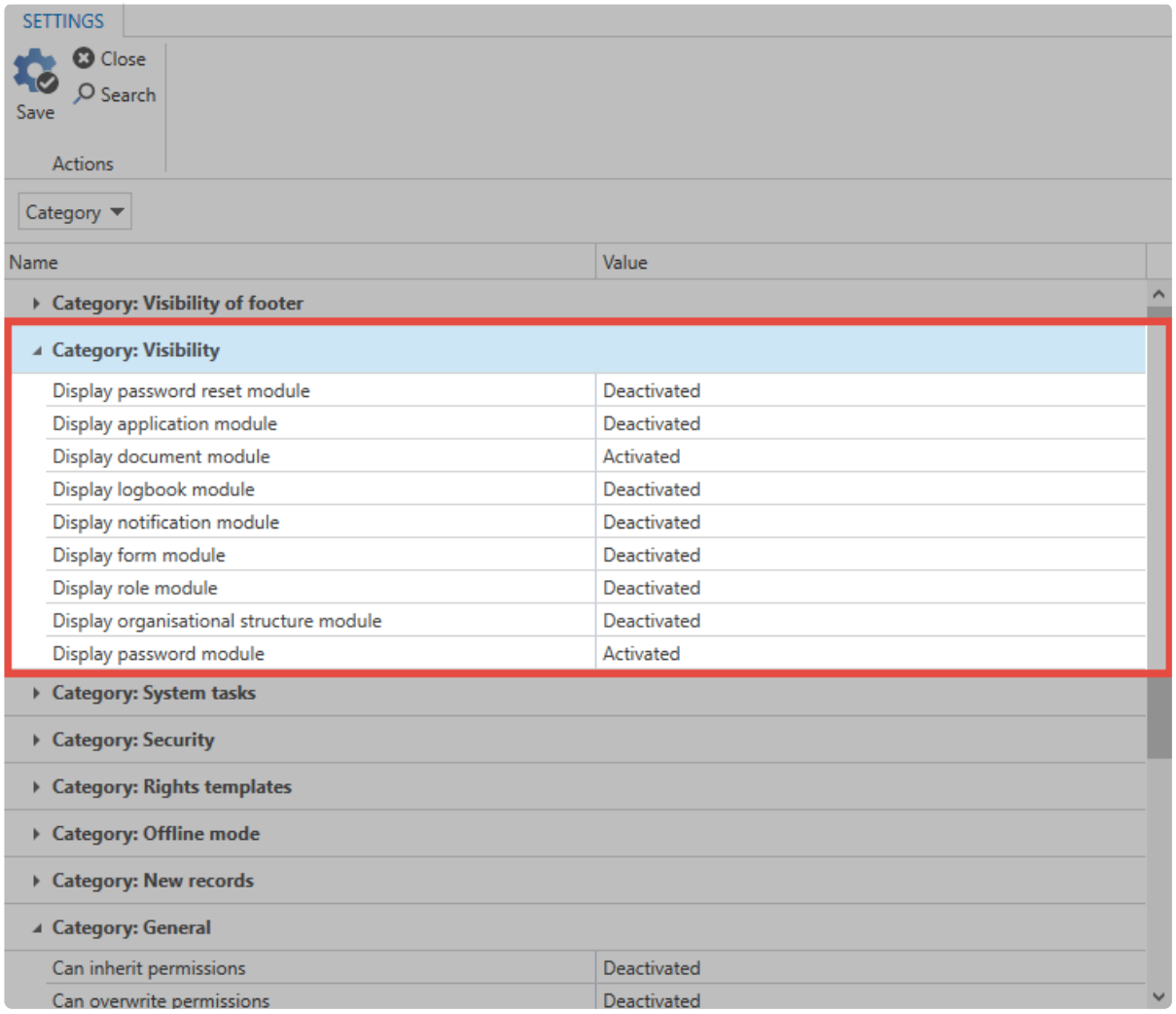
What are modules?

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.



Visibility of modules

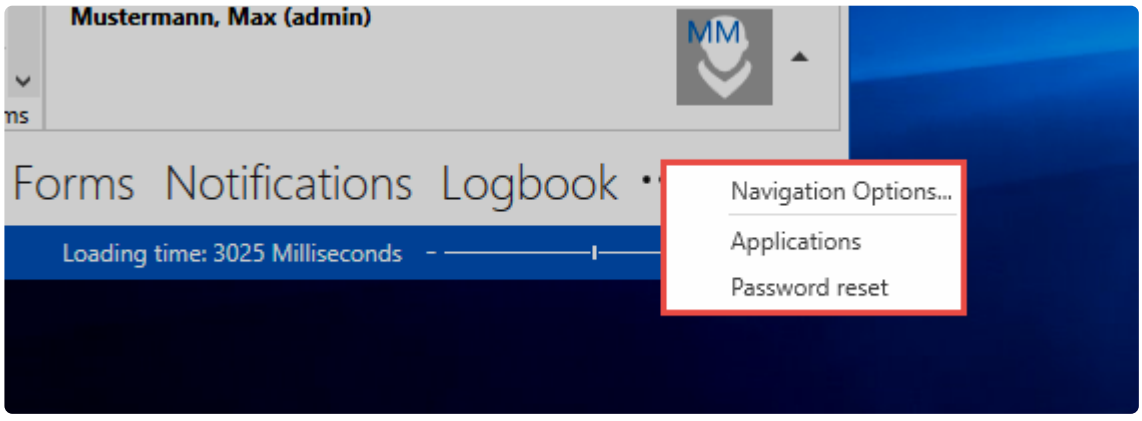
The modules are the gateway to the various features of version 8. Similarly to the features, not all modules have to be made available to all user layers. The **Visibility of modules** can be defined individually within the user rights.



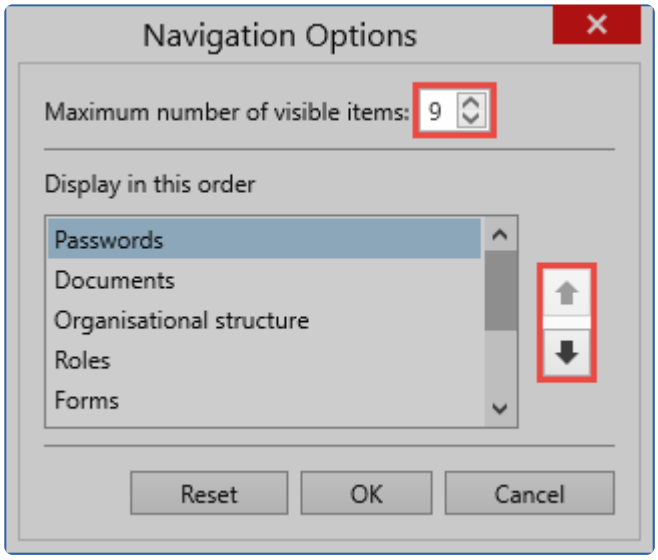
The visibility of modules can always be adapted to the needs of individual user groups

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.

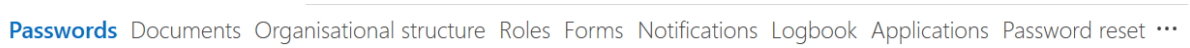


The previously described visibility of the modules is a basic requirement for viewing and sorting them in the navigation options

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 administrators and end users with central access to the passwords on a daily basis for the purpose of handling this sensitive data that requires protection. 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 **Masking** is explained in a similar way to the other modules in one place.



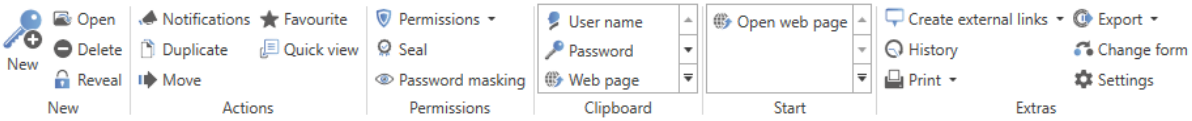
Prerequisite

The following user right is required for adding new passwords:

- **Can add new passwords**

Module-specific ribbon functions

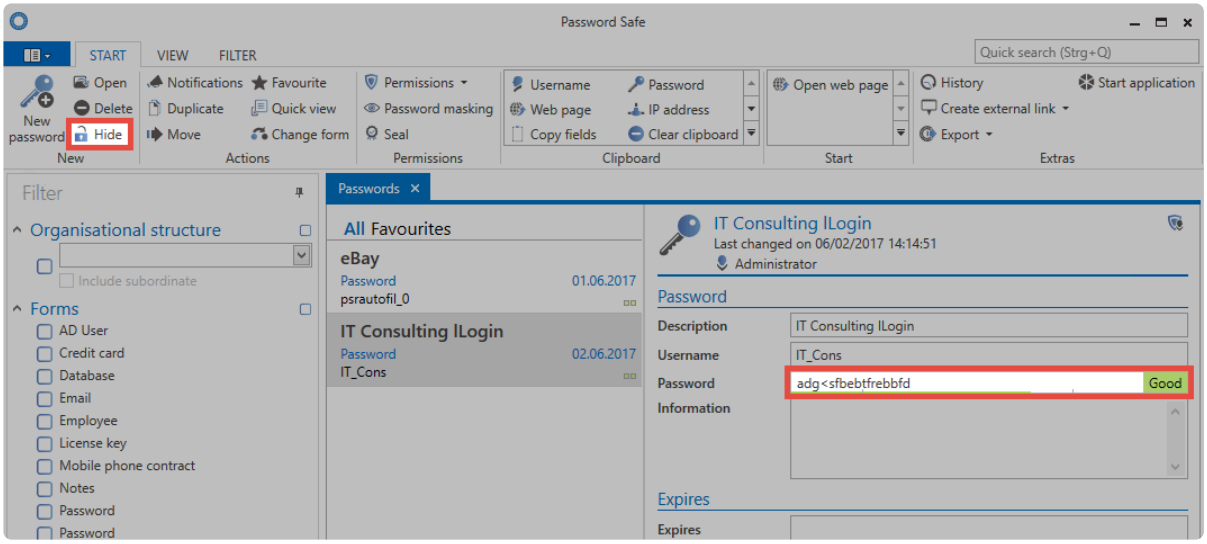
A great strength of the ribbon is that it offers access to all possible actions relevant to the situation at all times. Especially within the “Passwords” module, the ribbon plays a key role due to the numerous module-specific functions. General information on the subject of the ribbon is available in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



New

- **New password:** New passwords can be added via this icon in the ribbon, via the context menu that is accessed using the right mouse button and via the shortcut (Ctrl + N). The next step is to select a suitable form.

- **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, the passwords have been revealed and can be hidden again with the **Hide** button.



Actions

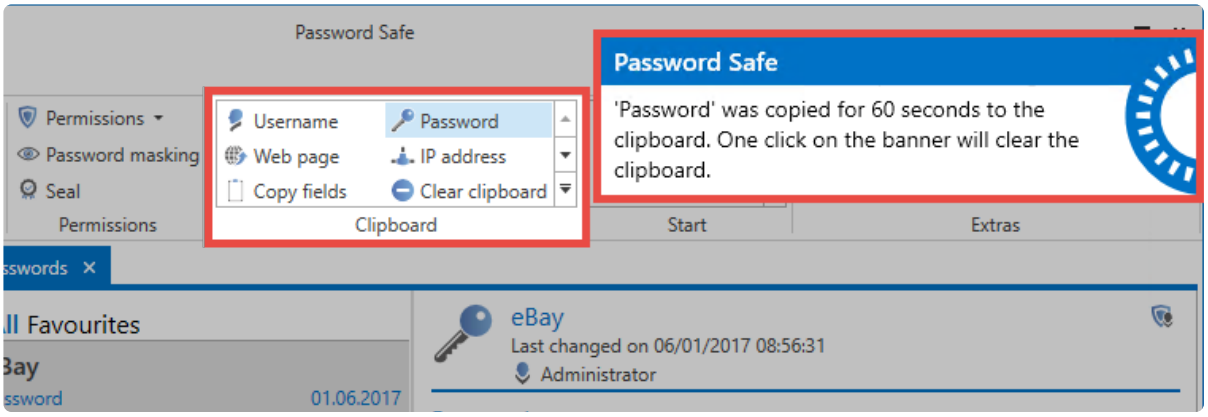
- **Notifications**: Defining notifications enables a constant flow of information about any type of change to records. The issuing of notifications is carried out in the module designed for this purpose.
- **Duplicate**: Duplicating creates an exact copy of the record in a new tab. Here it is possible to edit the data set further.
- **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 for a record in the ribbon** will copy it to the clipboard.



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.)

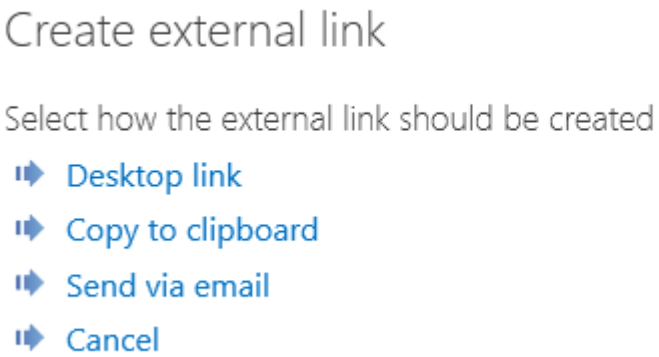
Start

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

- **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:



> ! If several sessions are opened on a client, an external link is always called in the first session.

- **History**: This icon opens the history for 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.

- **Print**: This option can be used to open the print function.
- **Export**: It is possible to export both all the selected records and also the data defined by the filter to a .csv file. More…
- **Change form**: This option can be used to assign a new form to the selected passwords.
- **Settings**: The password settings are described in a separate section.

The **password** module is based on the module of the same name in the WebClient. Both modules have a different scope and design. However, they are almost identical to use.

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. 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.

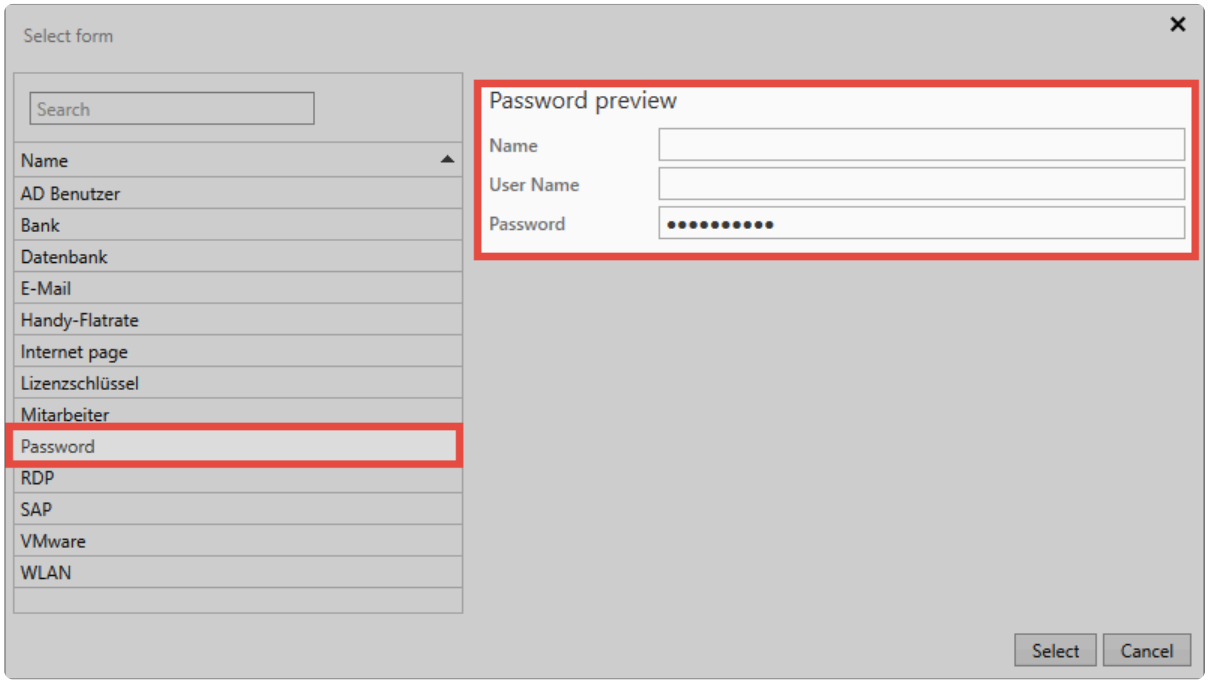
Requirements

The following 2 user rights are required:

- **Can add new passwords**
- **Display password module**

Selecting a form

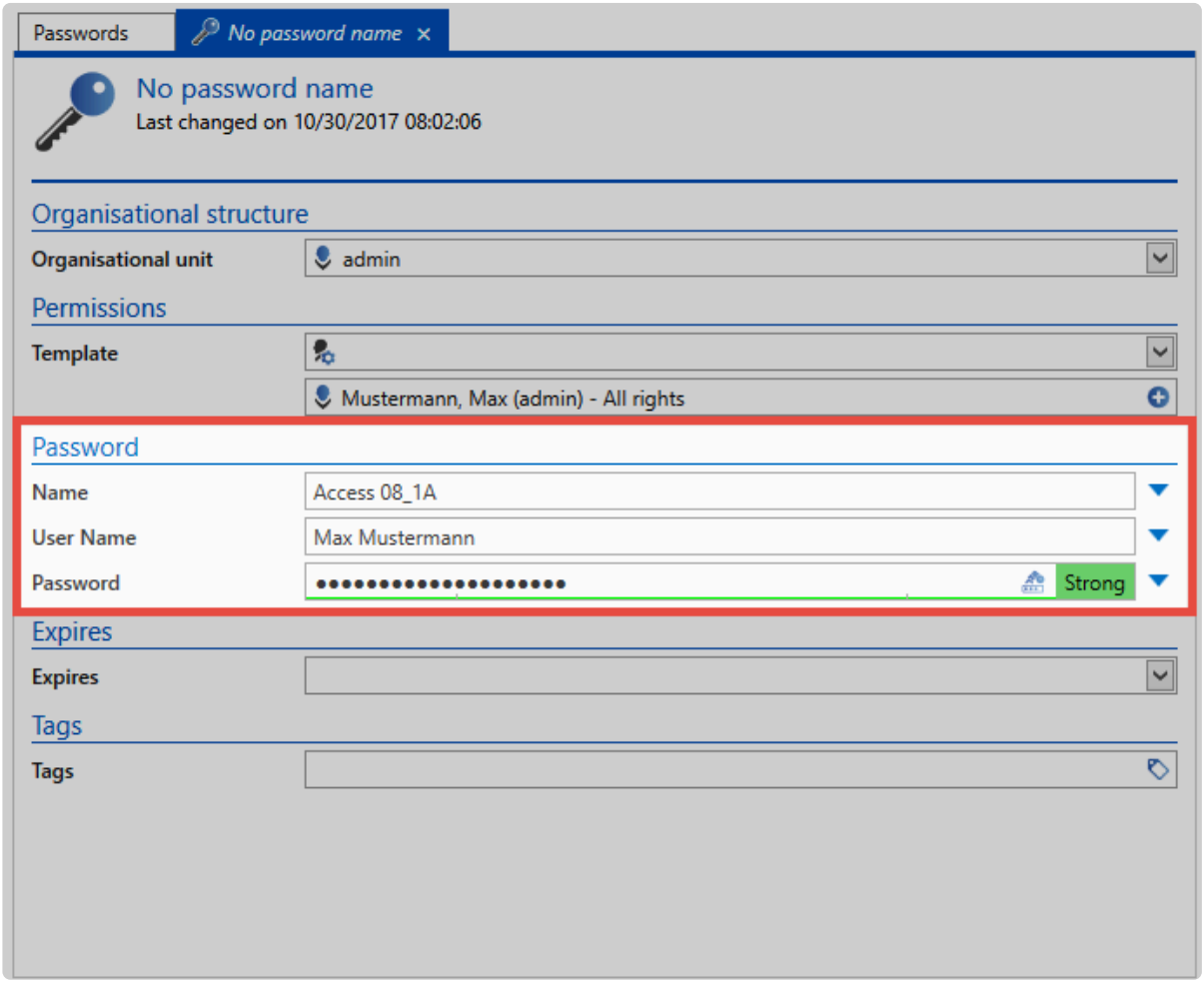
When creating a new record, it is possible to select from all the forms for which the logged-in user has the required permissions. To make the selection process as easy as possible, a preview of the form fields included in the form is shown on the right hand side.



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)

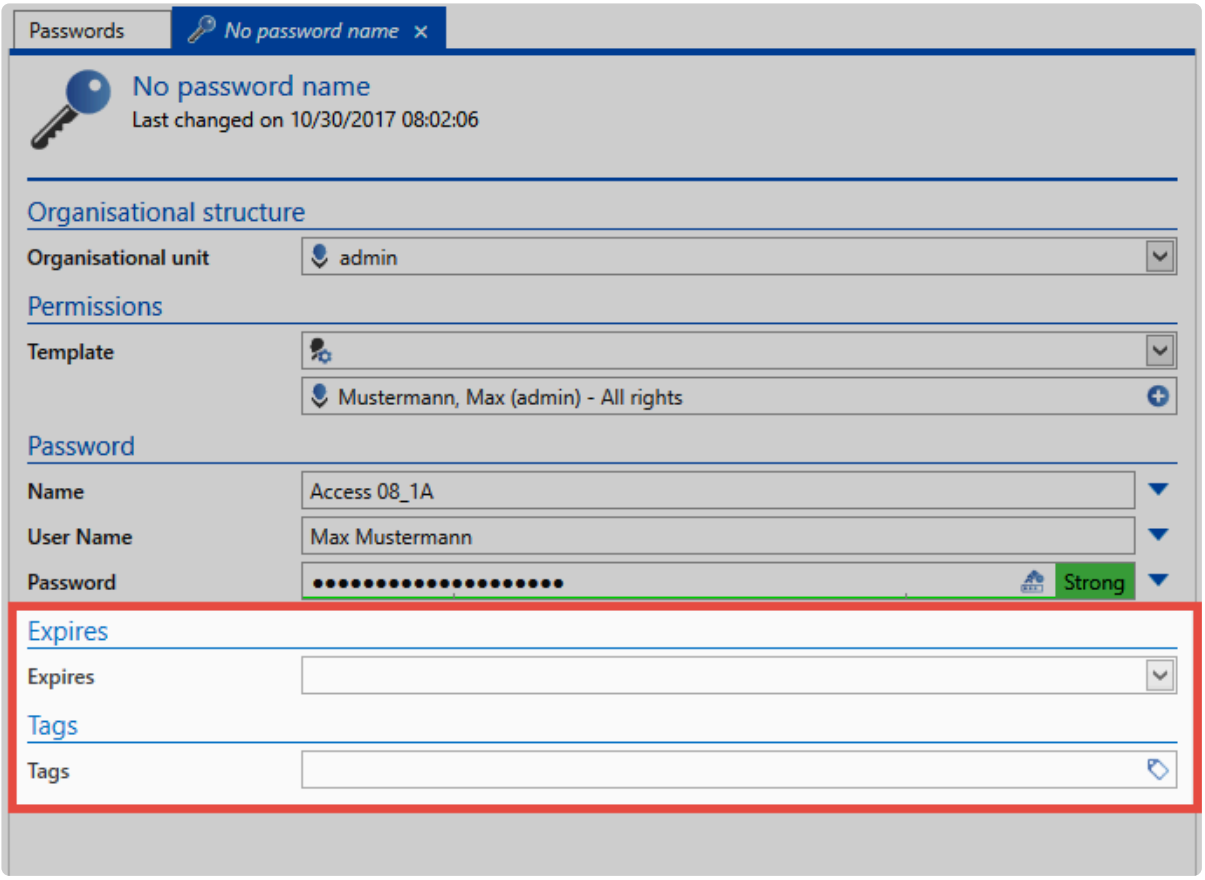
Entering data

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.



Validity and tags

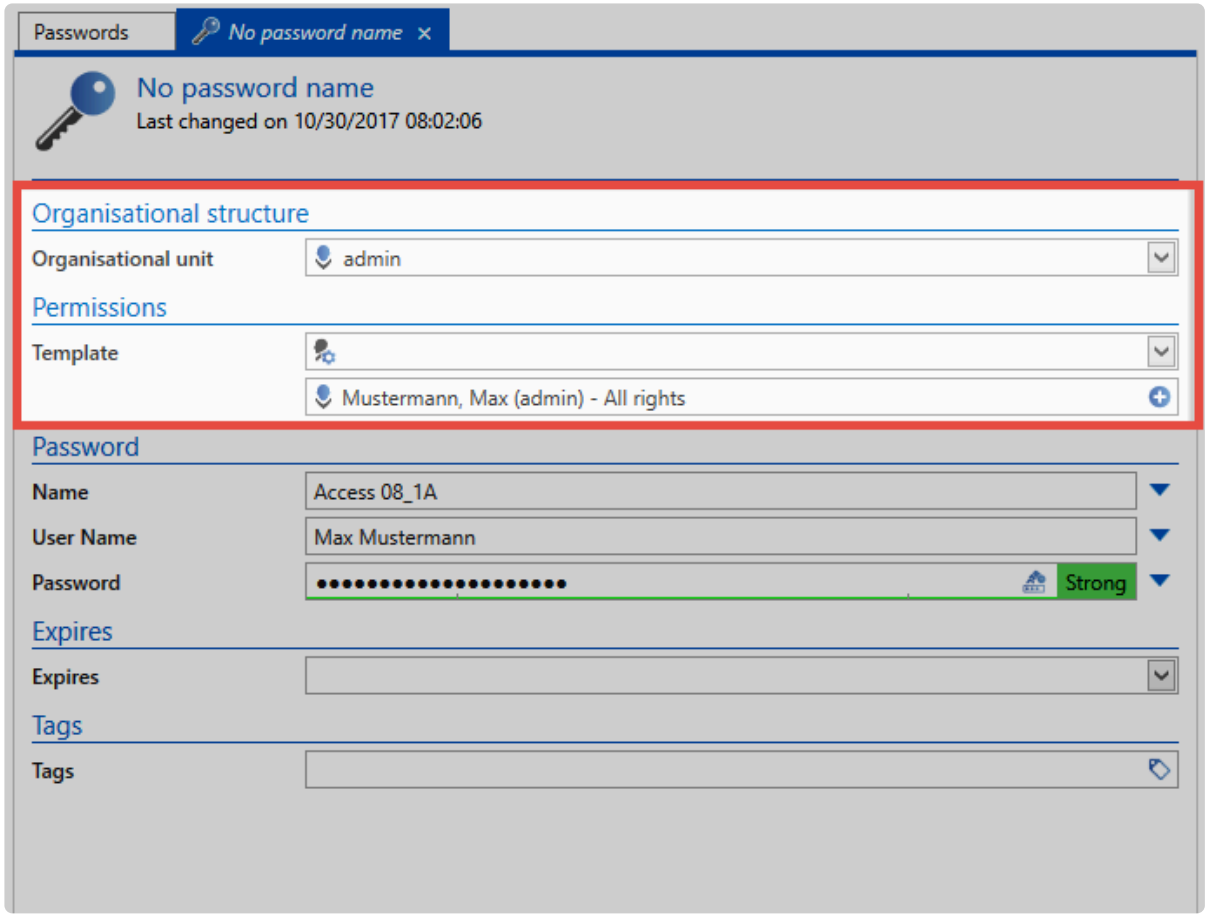
Irrespective of the selected form, it is always possible to define the validity and tags for a record. Both values are optional.



- 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.



- **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.

✻ 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.

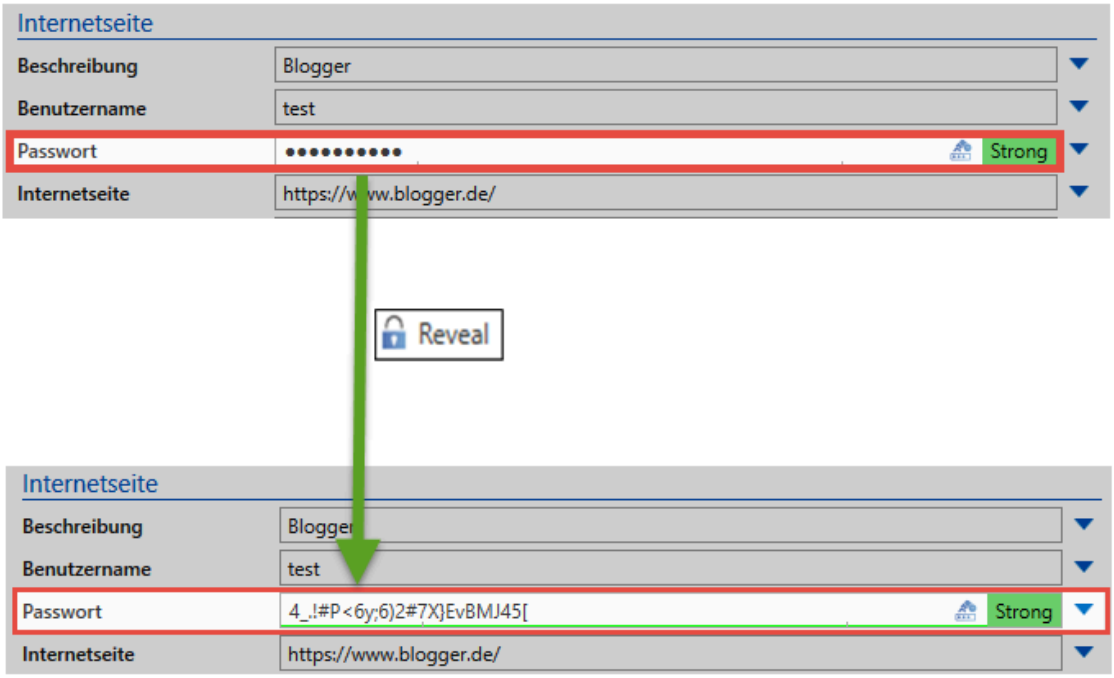
Revealing passwords

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.

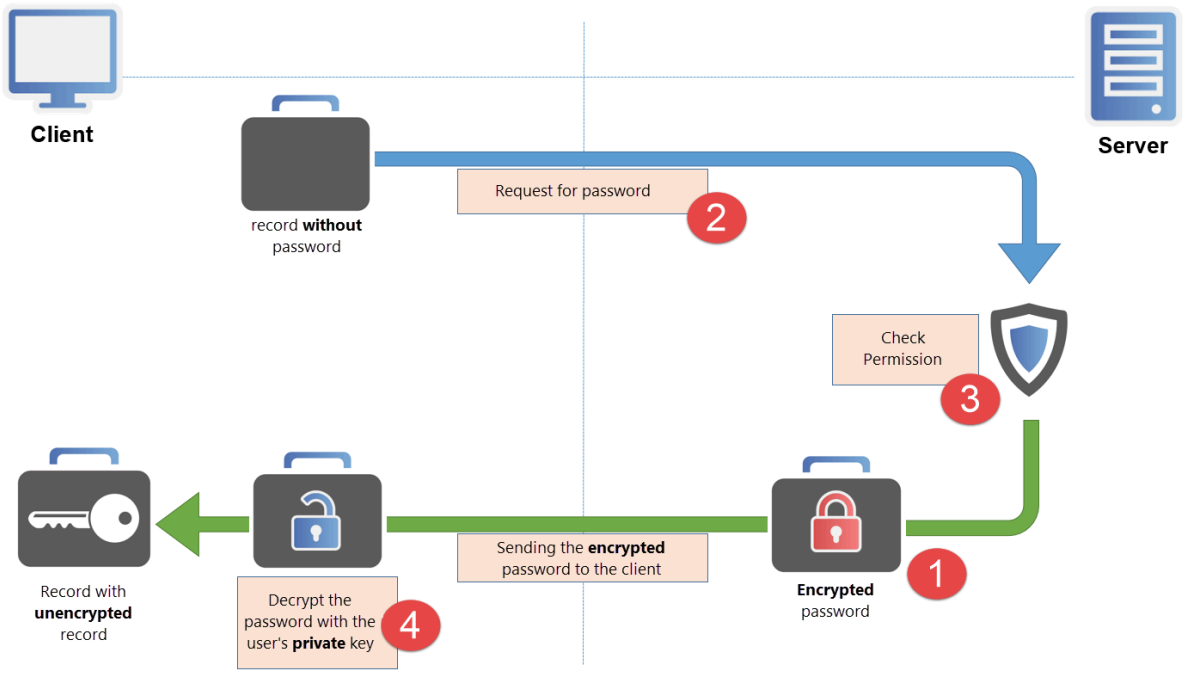
Example case

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.



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.



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**. 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.

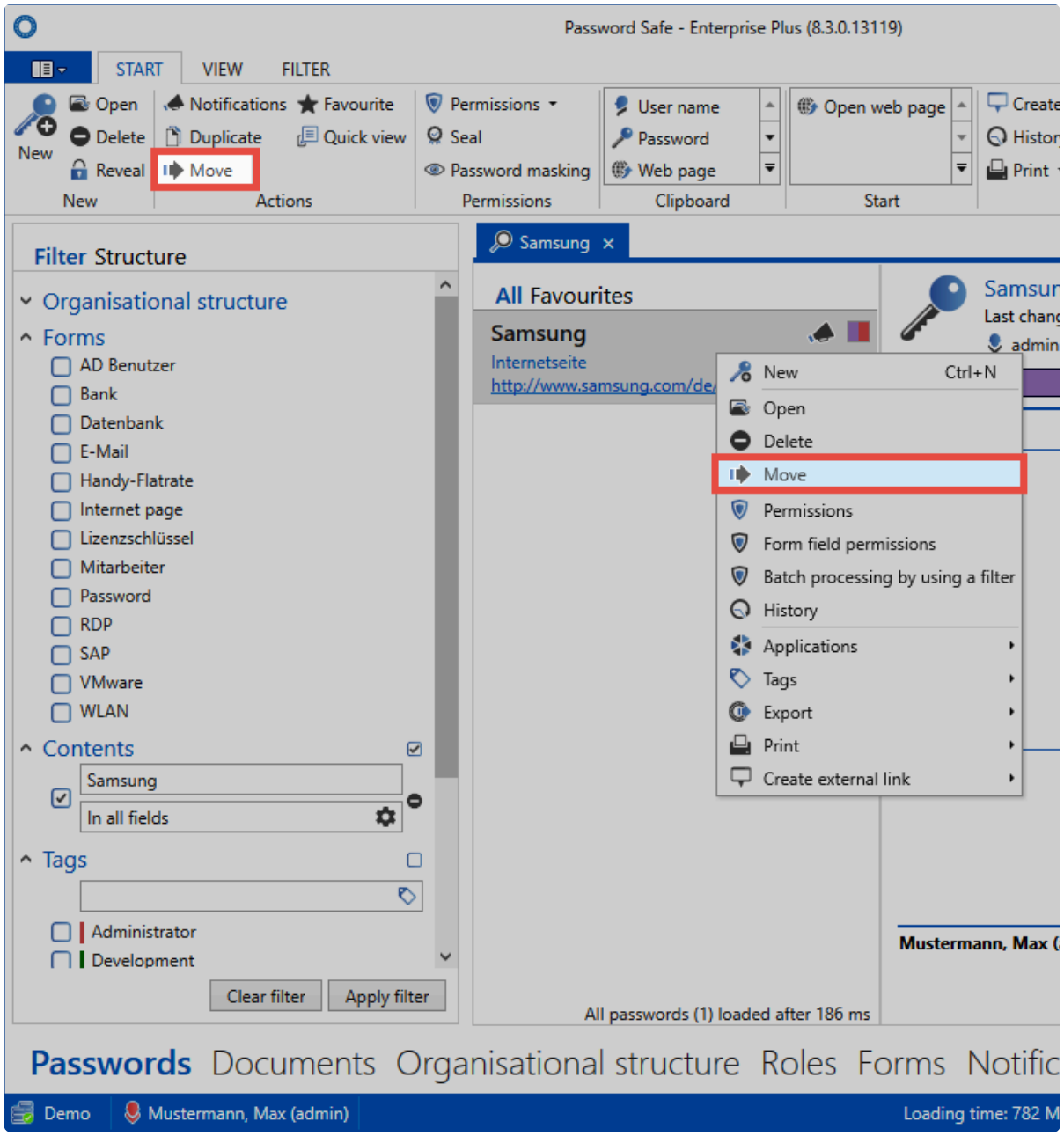
Moving passwords

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?

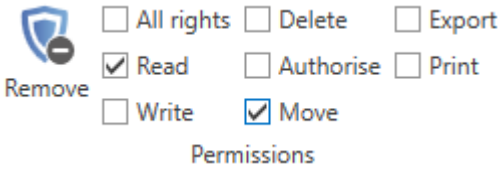
The (marked) records are moved either via the ribbon or via the context menu that is accessed using the right mouse button.



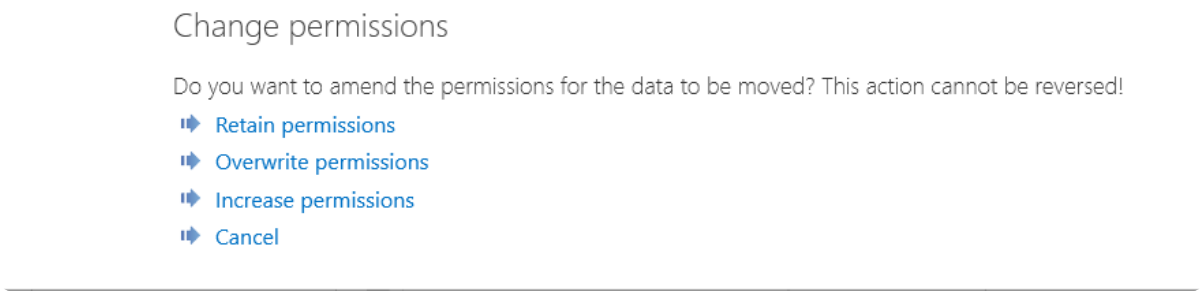
Multiple records can also be marked and moved. The selected permissions are then valid for all records in this case.

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



- **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 allows separate permissions to 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.

Relevant rights

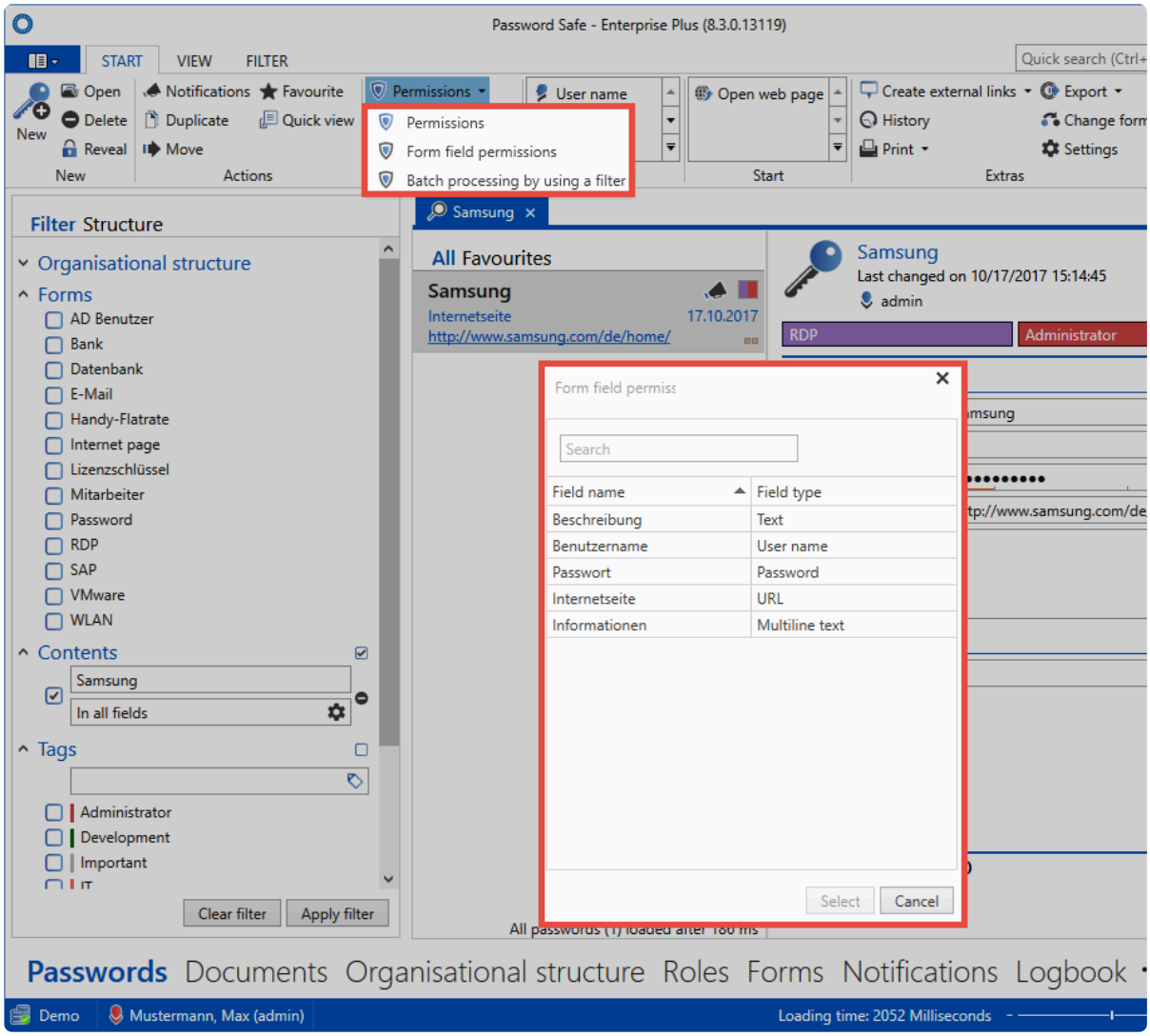
The following options are required to view **“inherit”** and **“overwrite”** icons.

User right

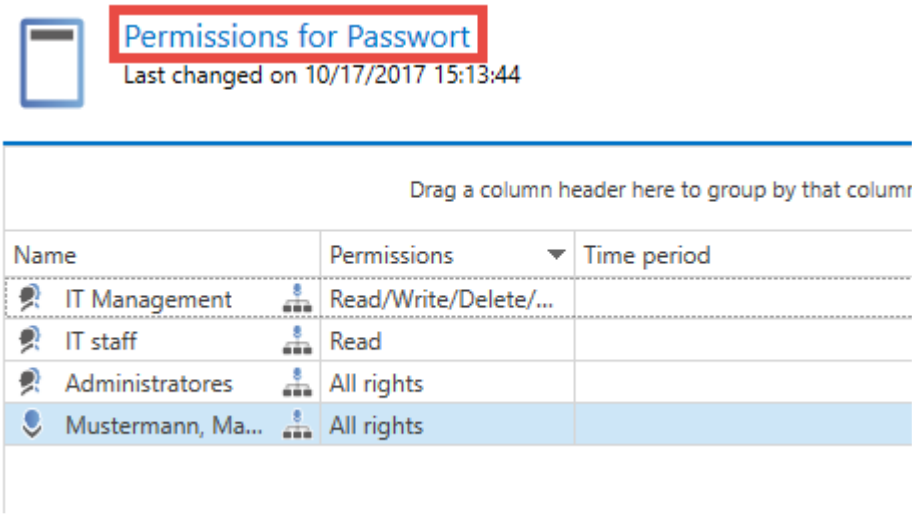
- Can overwrite permissions
- Can inherit permissions

Configuration

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



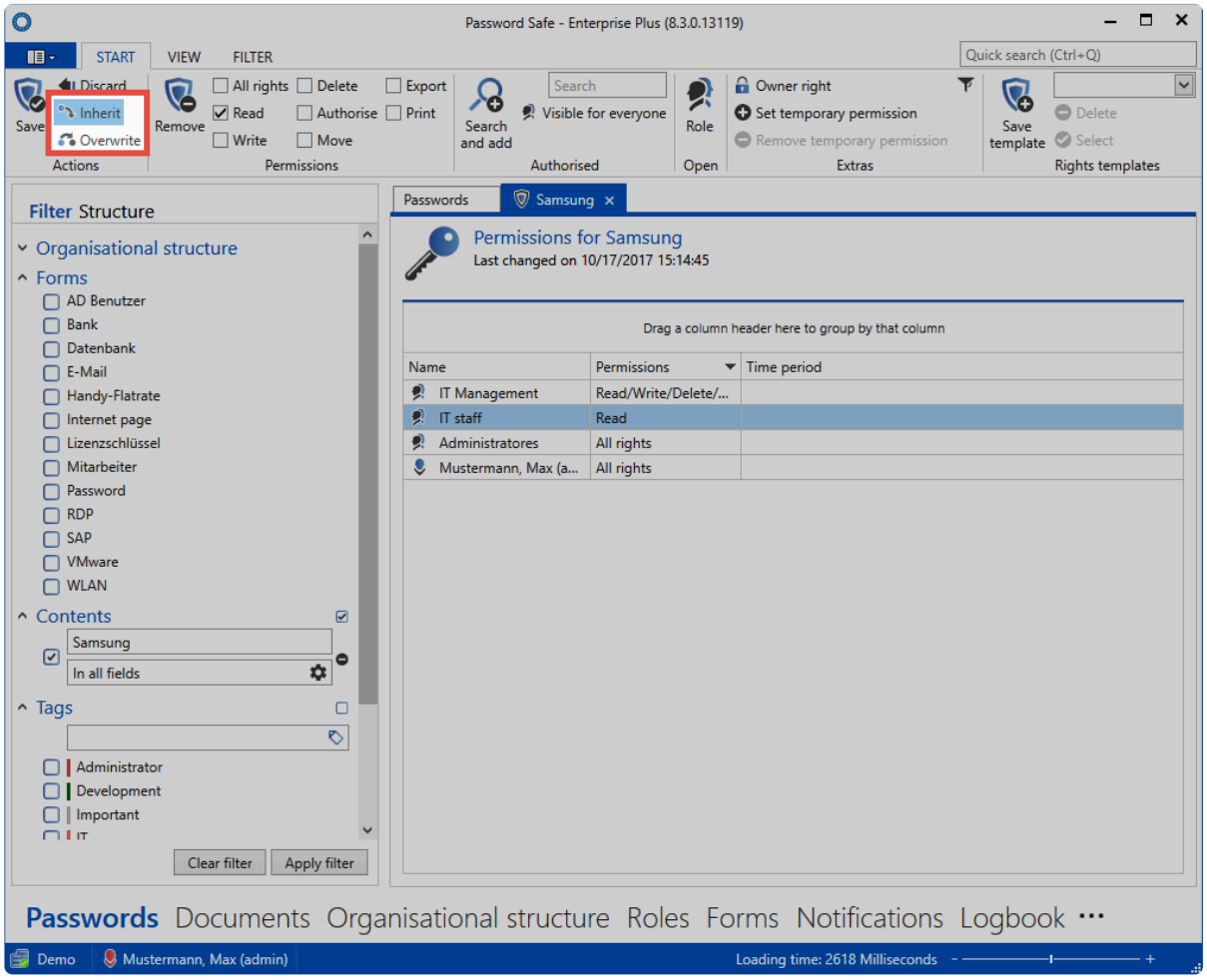
The window that opens allows you to select the relevant form field for which you want to grant permissions. The following example focuses on the password field.



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.

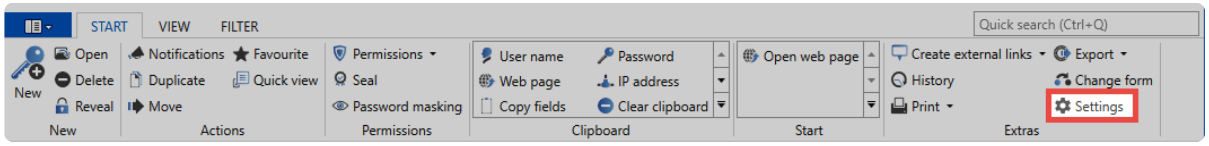


In this way, you have the option of deciding whether changes to the permissions for a record are automatically inherited or not by all available underlying form fields. It is only necessary to remove the tick from the “Inherit” field.

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.

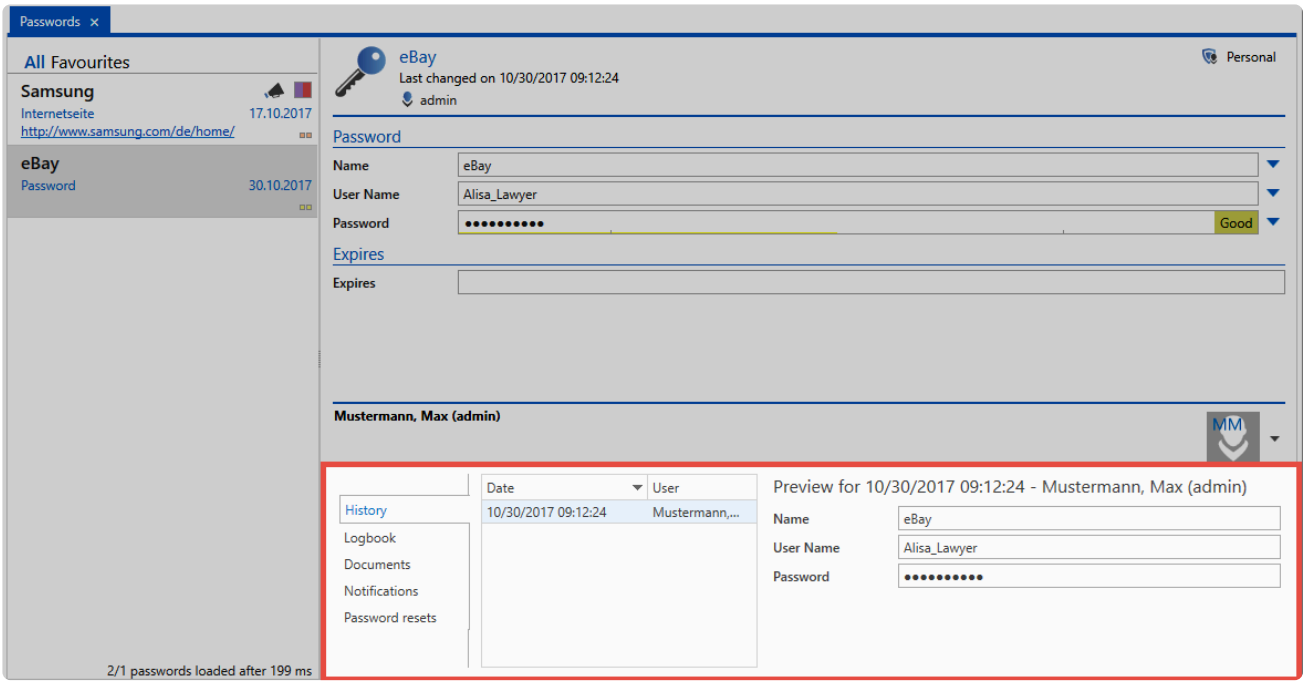
History

What is the history?

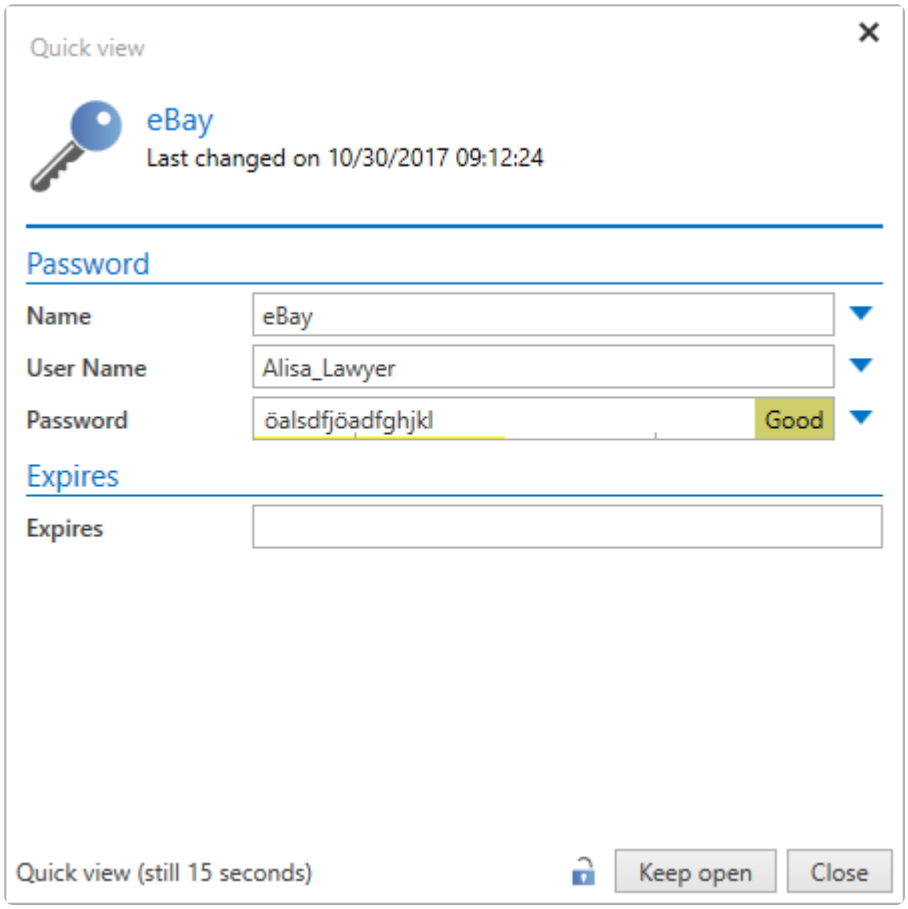
Alongside saving passwords and keeping them safe, the ability to trace changes to records also has great relevance. The history maintains a seamless account of the versions for all form fields in a record. Every change to records is separately recorded, saved and can thus also be restored. In addition, 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.

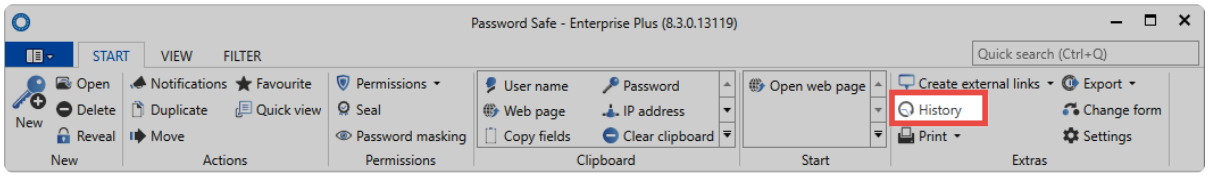


The different versions are displayed one below the other on the left. The info for each respective version can then be seen alongside on the right. A quick view can be displayed via the **History** in the ribbon or via a double click.

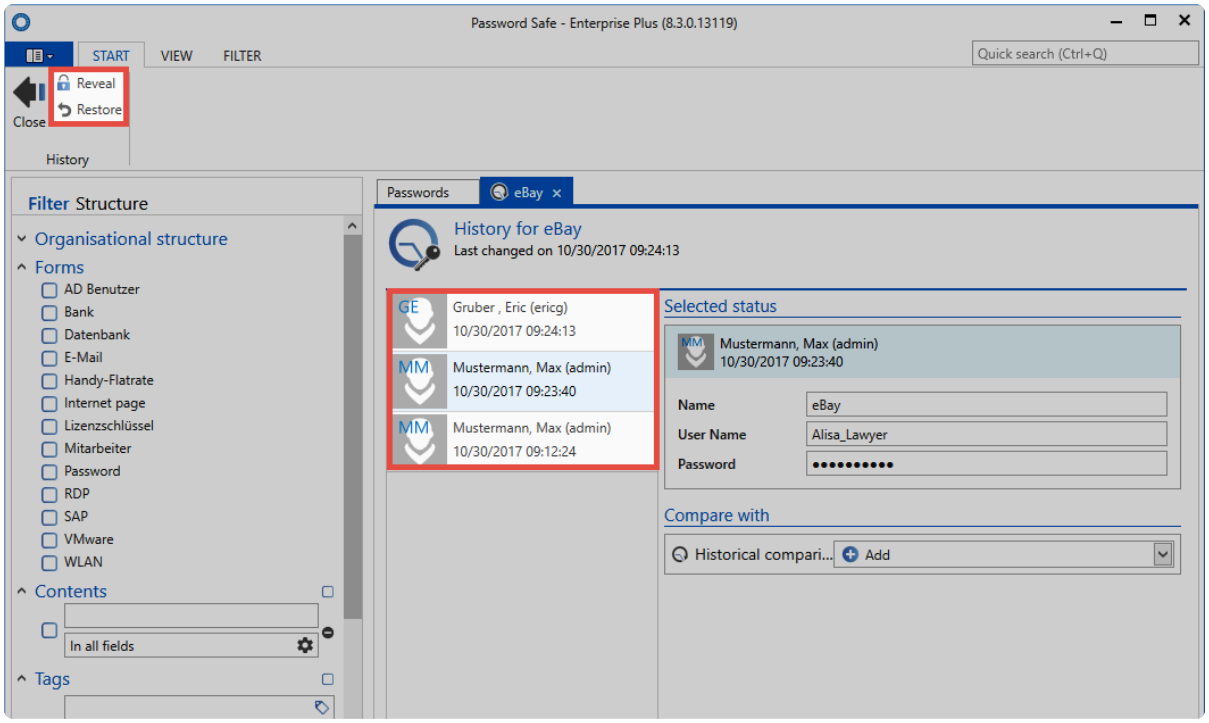


Detailed history in the Extras

The detailed history for the record marked in list view can be called up in the Start/Extras tab.

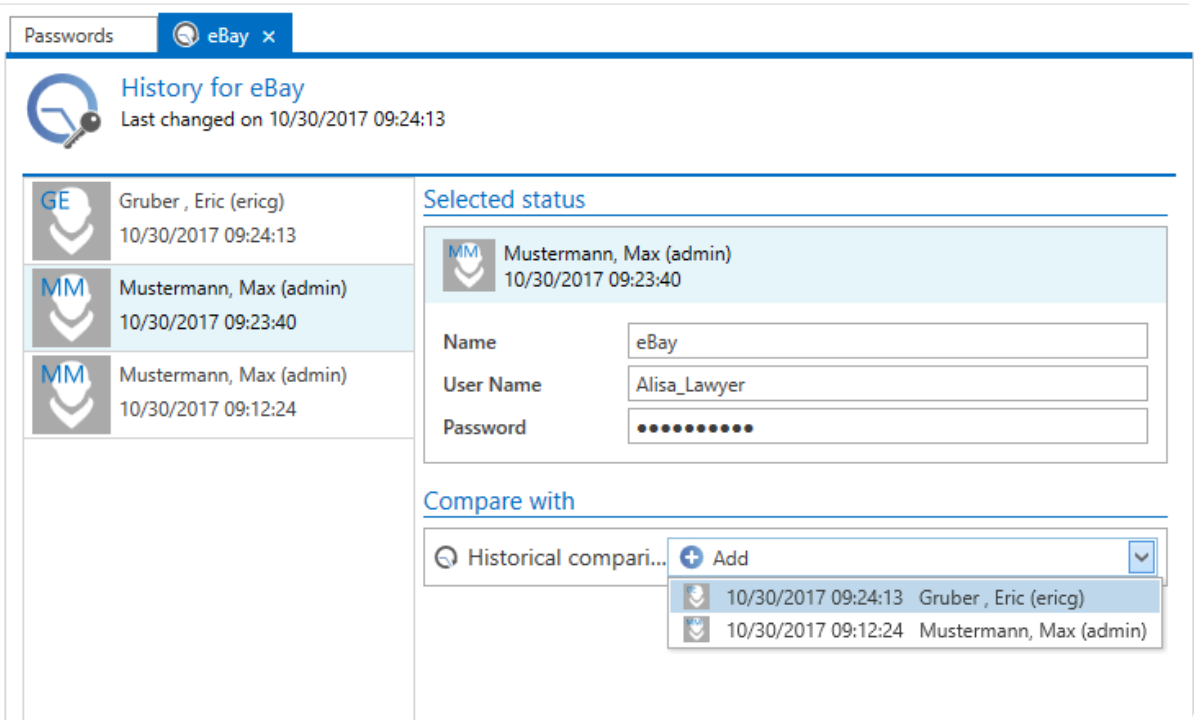


The history for the marked record opens in a separate tab. In list view, all of the available versions with the date and time of their last change are sorted in chronological order.

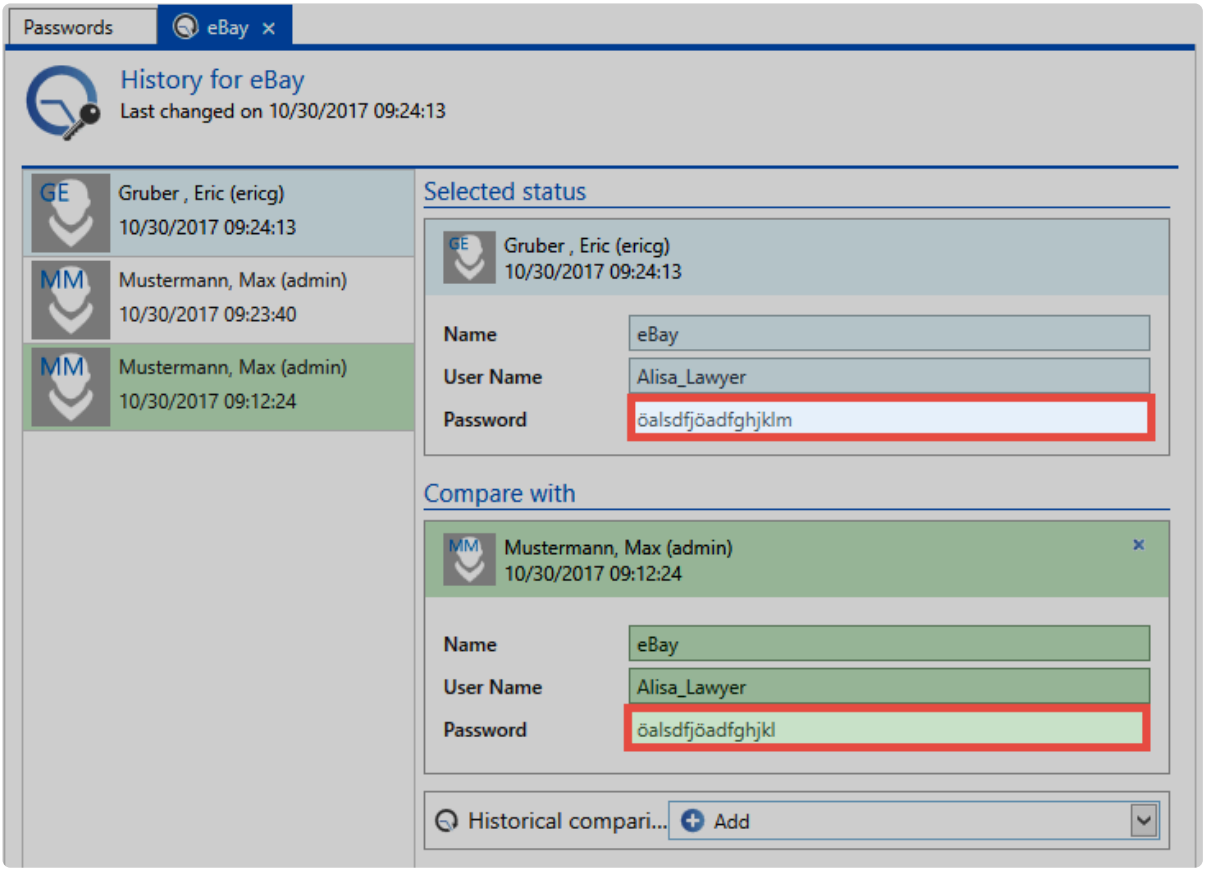


Comparison of versions

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.



If deviations exist between the two versions, these will be highlighted in colour.



Restoring versions

A selected status can be restored via the ribbon. The current state is overwritten and added to the history

Papierkorb

Mit dieser Option können Sie gelöschte Passwörter, auf die Sie berechtigt sind einsehen und endgültig löschen.

Vorgehensweise beim Löschen von Passwörter

Um Passwörter in den Papierkorb zu legen gibt es 2 mögliche Vorgehensweisen. Wählen Sie dafür die entsprechenden Passwörter aus und klicken in der Ribbon auf **In Papierkorb legen** (1) oder Rechtsklicken Sie auf die Passwörter und wählen dann **In Papierkorb legen**.

Sie erhalten dann die Anfrage, ob Sie diese Aktion tatsächlich durchführen wollen.

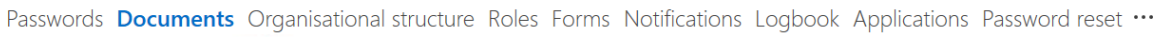
Verwalten des Papierkorbs

Die Verwaltung des Papierkorbs finden Sie **hier**

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..



Relevant rights

The following option is required to add new documents.

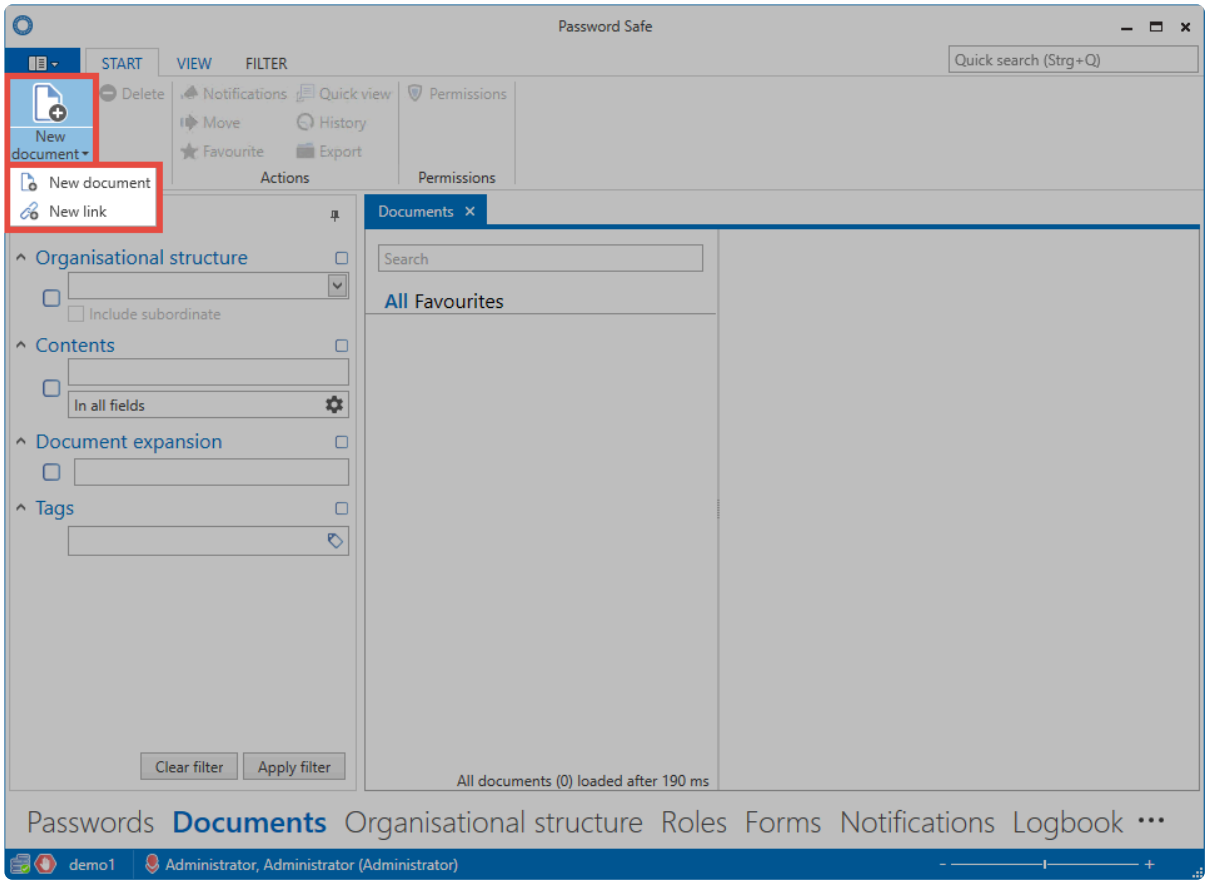
User right

- Can add new documents

Adding documents

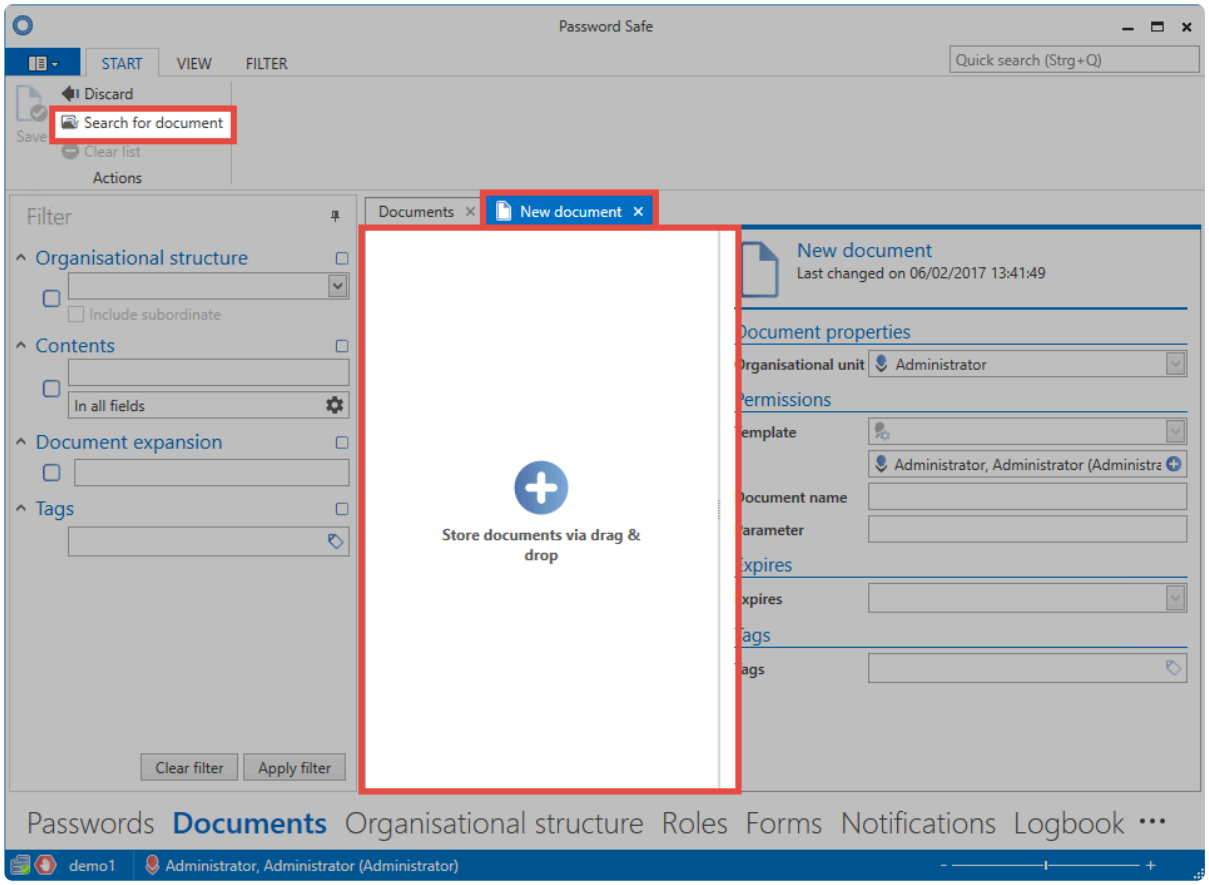
There are two ways to manage documents and files in Password Safe v8:

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.



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.

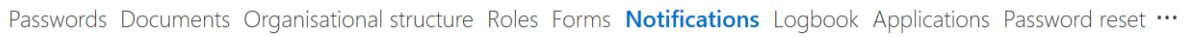
The file size for a **linked document** can only be updated if the document was opened using Password Safe.

If desired, the document history can be automatically cleaned up. This option can be configured on the **AdminClient**. Further information can be found in the section **Managing databases**.

Notifications

What are notifications?

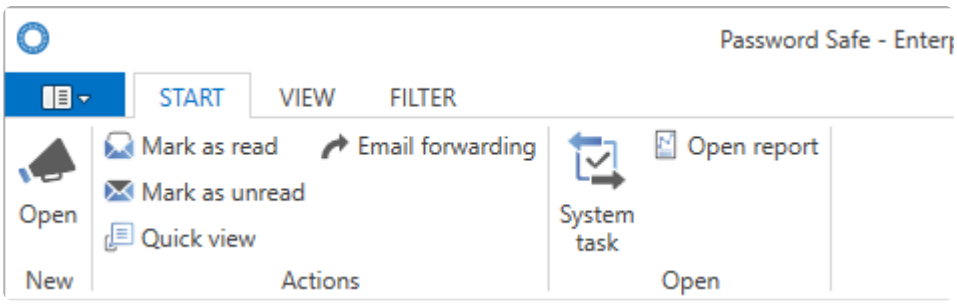
With the notification system, you are always up-to-date on all events that you consider important. Almost all modules allow users to configure when to receive notifications. All configured messages are only created for the currently registered Password Safe user. It is not possible to create a notification 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.

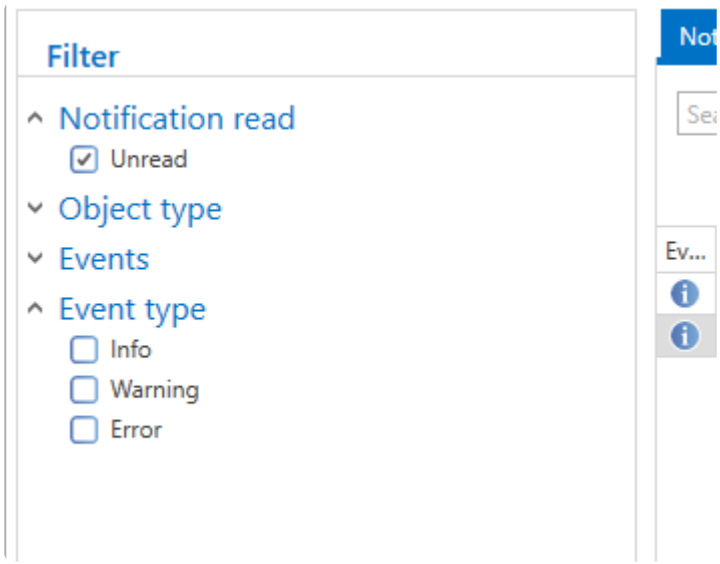
Module-specific ribbon functions

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

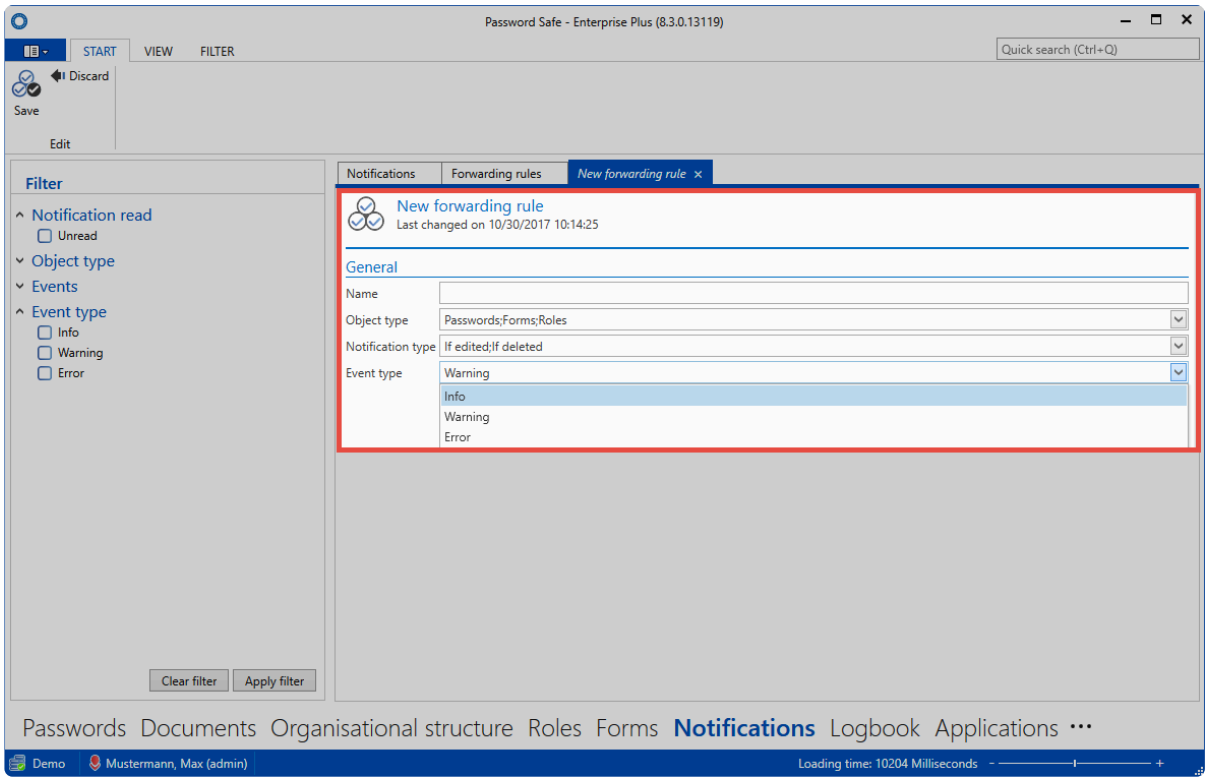
The two buttons on the ribbon enable you to mark notifications as read/unread. In particular, the filter criterion available in this context (see following screenshot) enables fast sorting according to current and also historical notifications.



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.

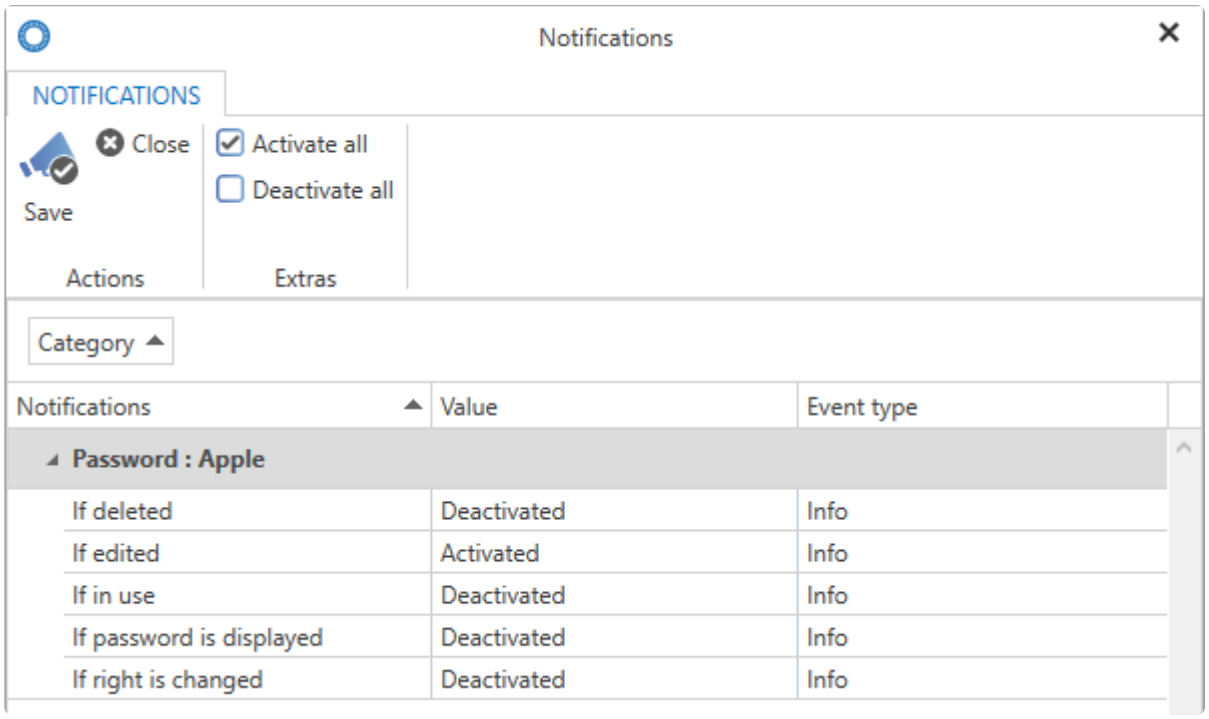


In this example, all notifications that match the stated object type (passwords, forms, roles) and notification type (when edited, when deleted) are forwarded. In addition, it is also possible to filter according to the notification type (=event type).

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

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:



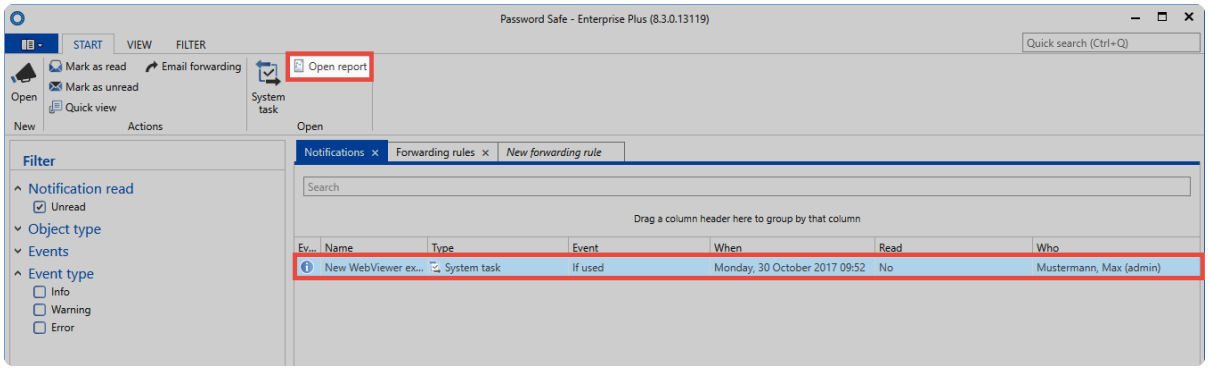
- **Notification**: Definition for the trigger
- **Value**: Defines whether a notification should be created for the previously defined trigger. In the example for the “Apple” record, this only occurs when the record is edited.
- **Event type**: The event type for the generated notifications can be either “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.



Automatic deletion of old notifications

If desired, notifications can be automatically cleaned up. This option can be configured on the **AdminClient**. Further information can be found in the section **Managing databases**.

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 **Masking** is explained in a similar way to the other modules in one place.

Passwords Documents **Organisational structure** Roles Forms Notifications Logbook Applications Password reset ···

Relevant rights

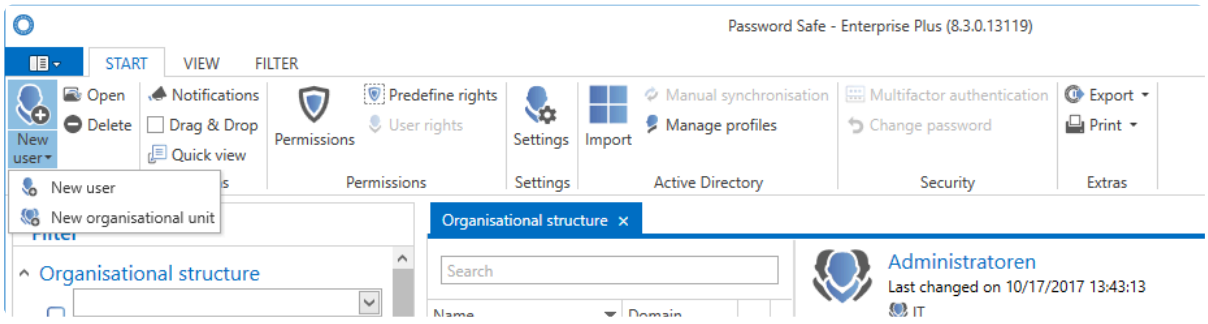
The following options are required for adding new organisational structures.

User rights

- Can add new organisational units
- Display organisational structure module

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.



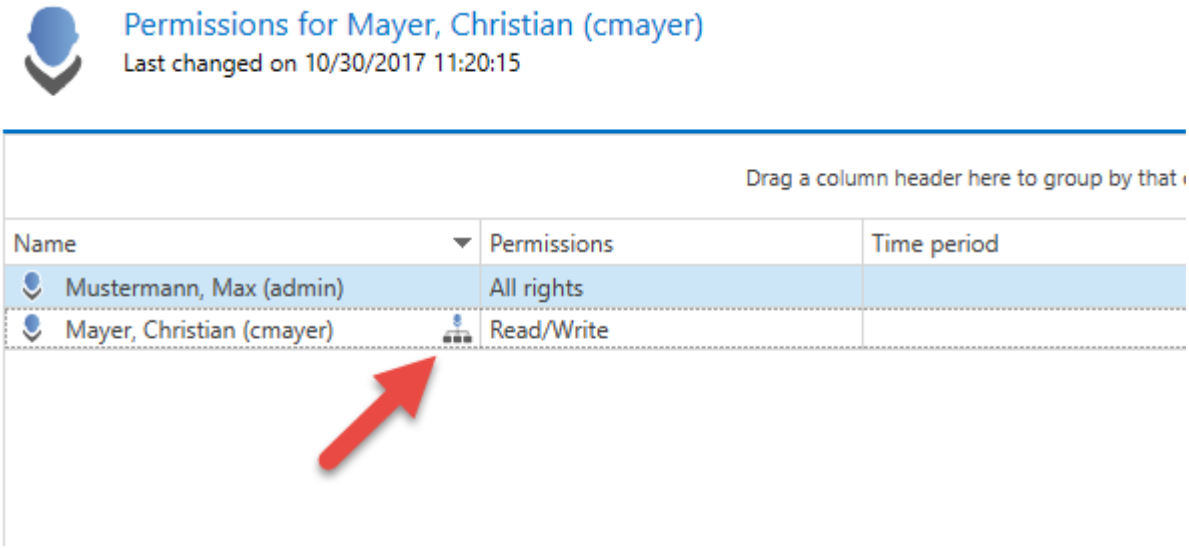
- **New organisational unit/user**: New organisational units or new users can be added via the ribbon, the keyboard shortcut “CTRL + N” or also the context menu that is accessed using the right mouse button. Due to its complexity, there is a separate section for this function: New organisational structures / new users
- **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.



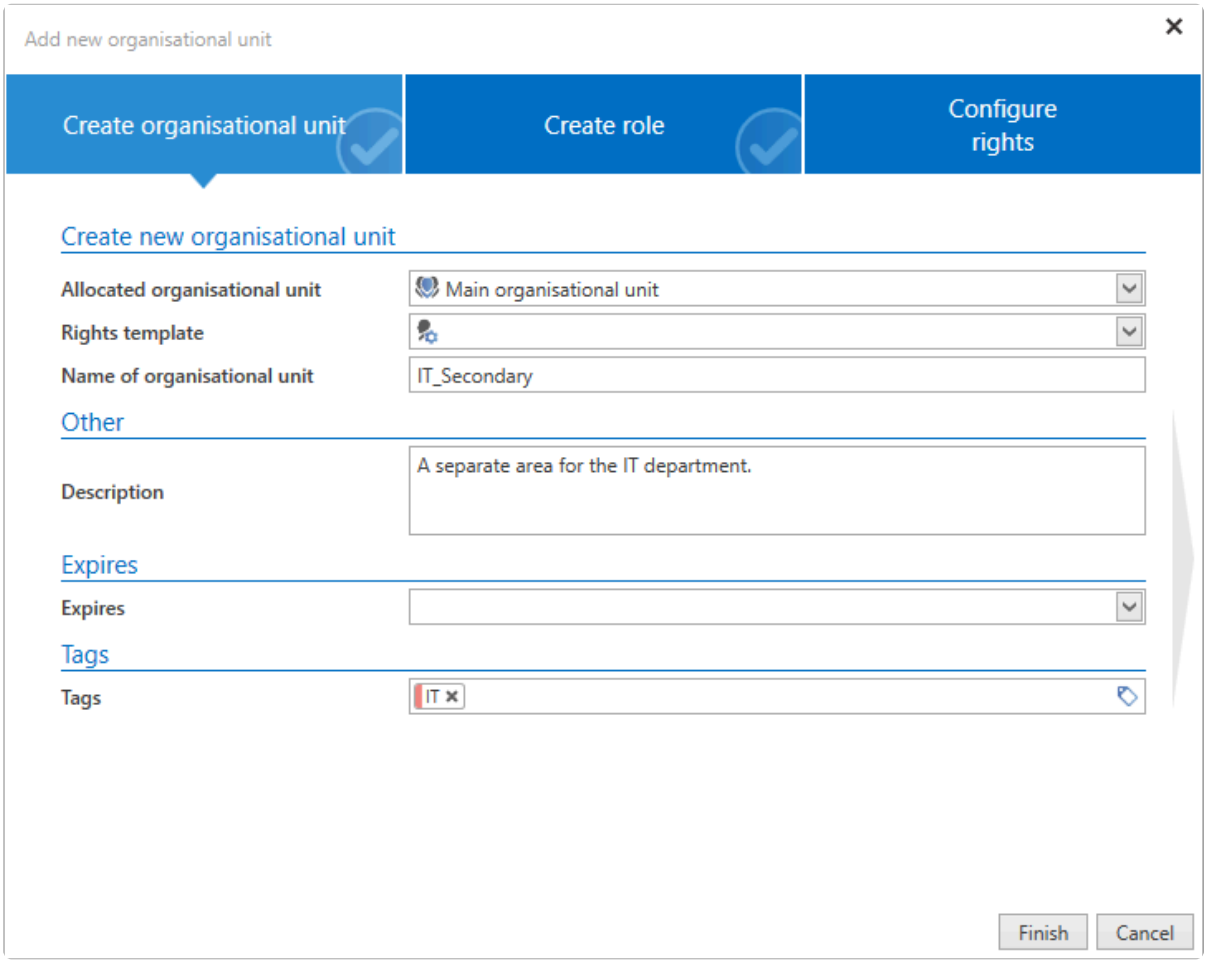
This configuration means that the user password cannot be reset by administrators. The disadvantage is that if the password is lost there is no technical solution for "resetting" the password in the system.

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

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

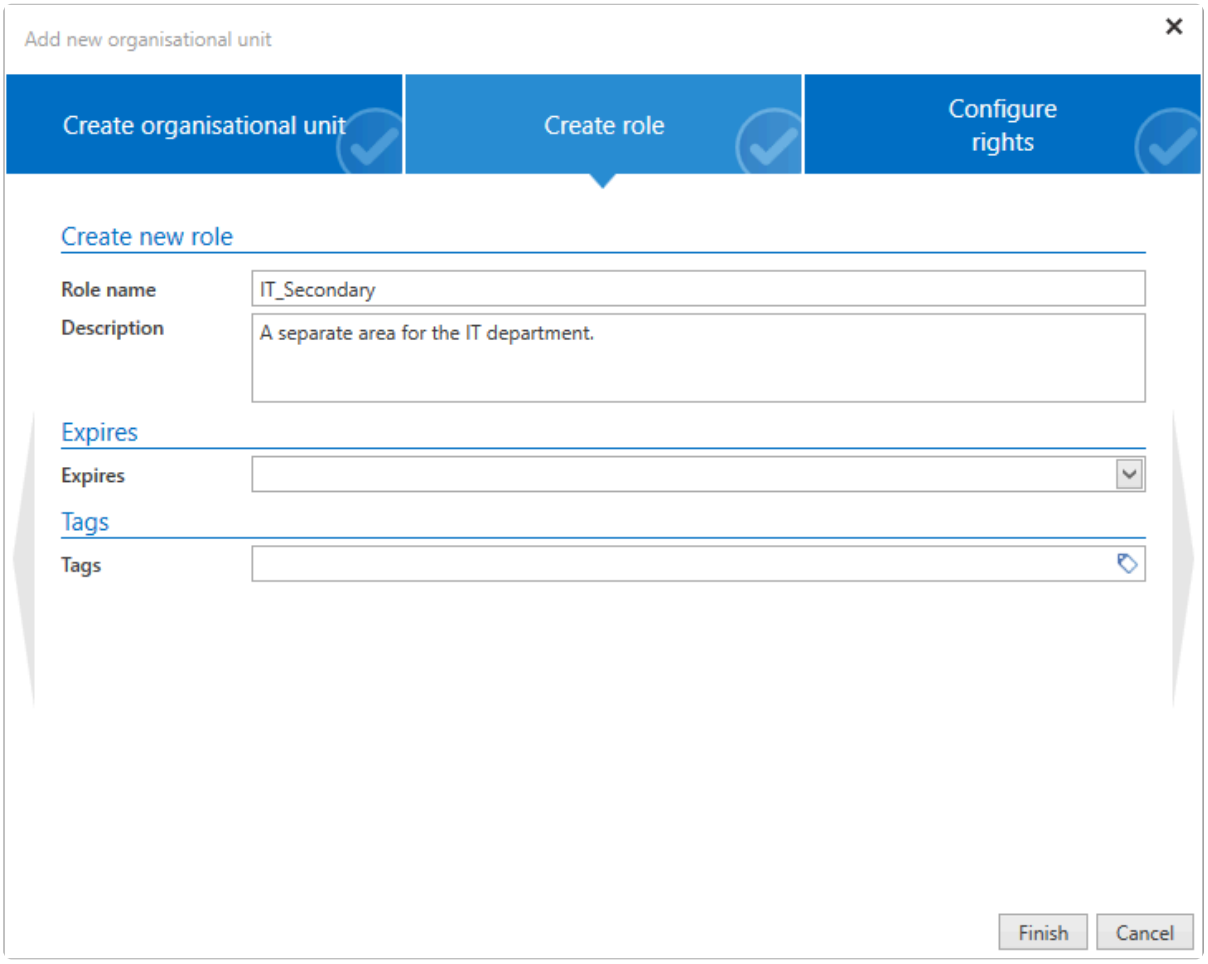


- **Allocated organisational unit**: If the new object is defined here as a **main organisational unit**, it is not allocated to an existing organisational unit

- **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

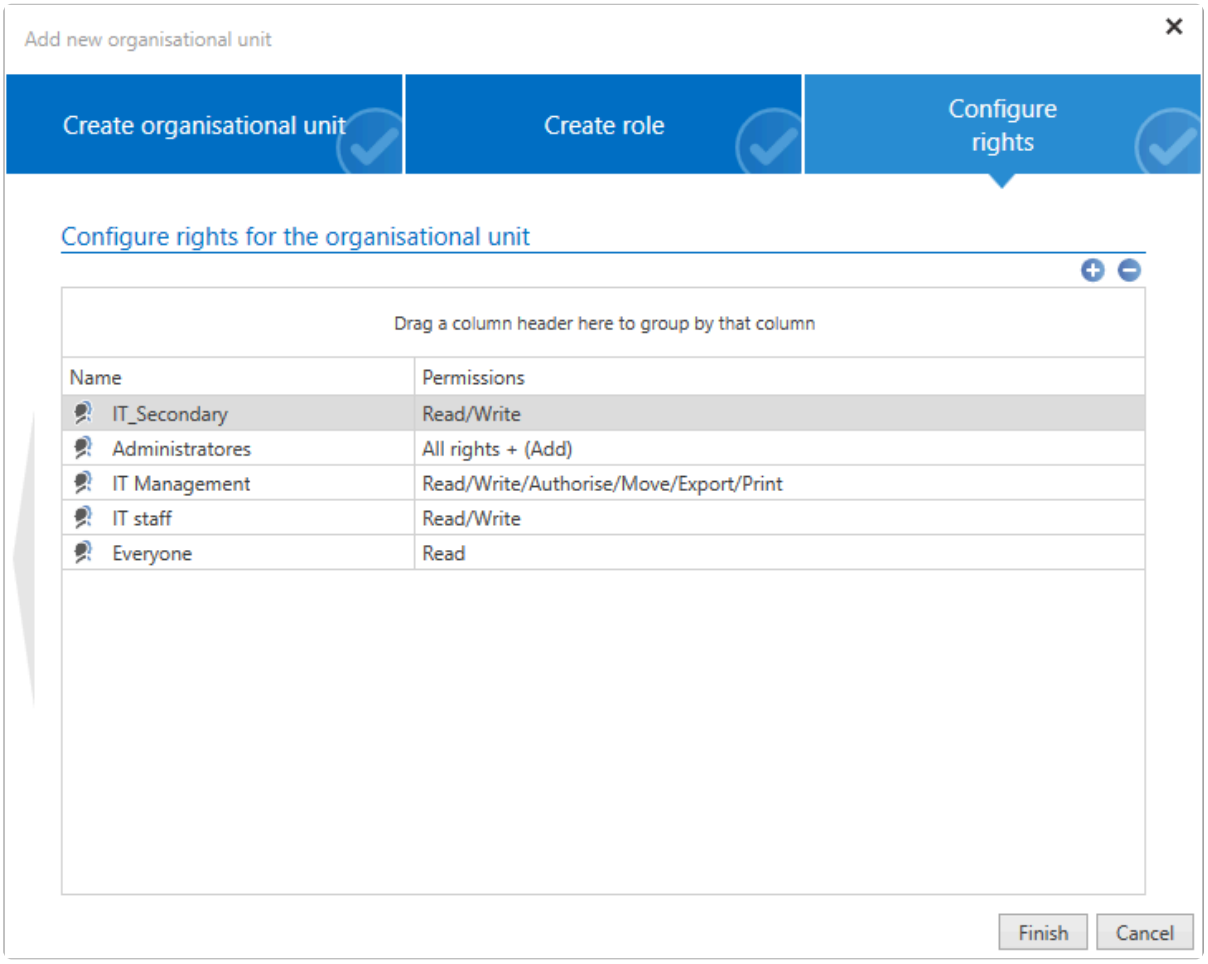
The organisational unit marked in list view will be used as a default. This applies to the fields “allocated organisational unit” and also “rights template”.

Create role



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



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.

The **organisational structure** module is based on the WebClient module of the same name. Both modules have a different scope and design but are almost identical to use.

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 also 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…

Relevant rights

The following options are required to add local users.

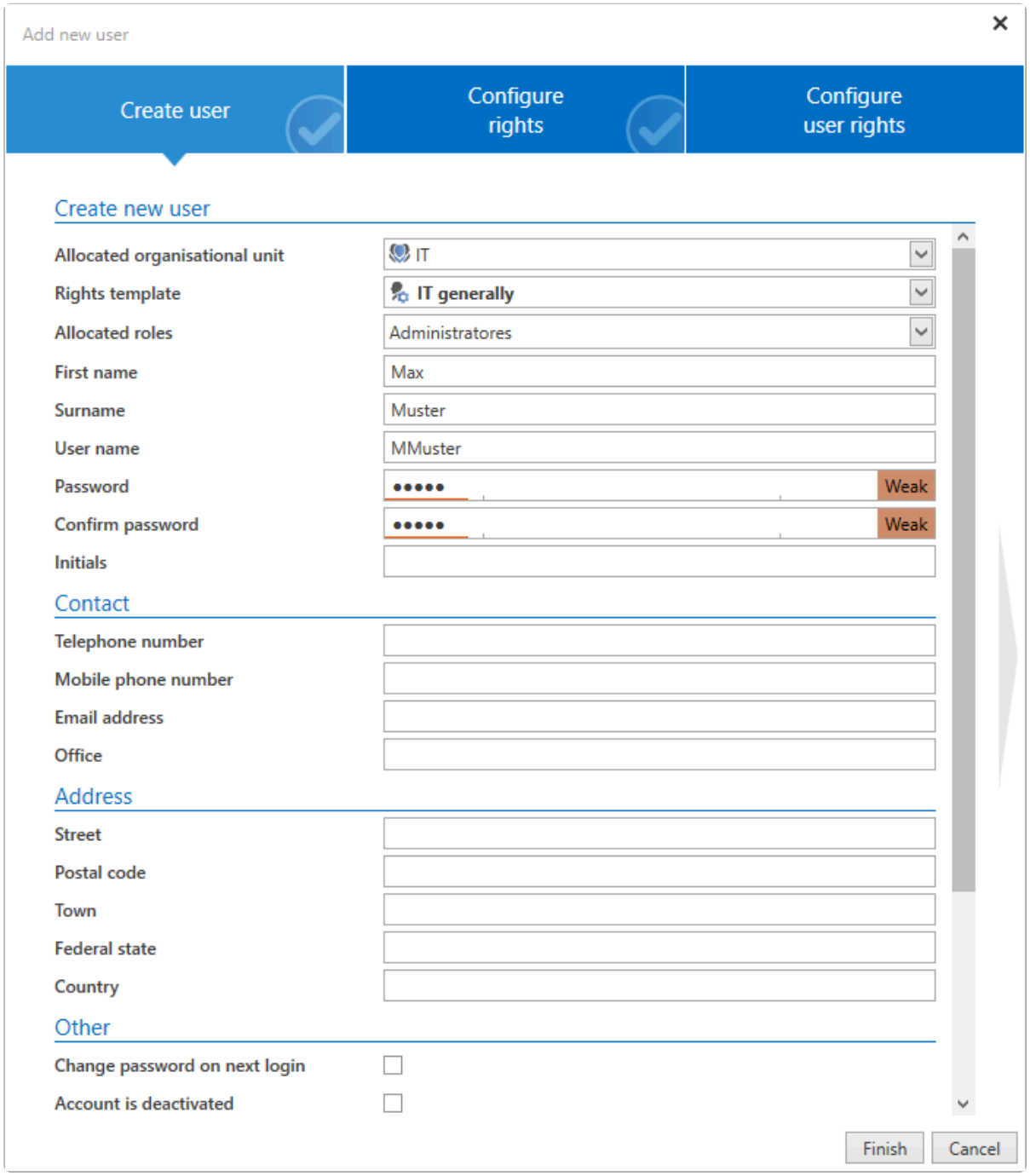
User rights

- Can add new users
- Display organisational structure module

Adding local users

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



- **Allocated roles**: New users can directly be allocated one or more rolls when they are created
- **Change password on next login**: The user will be requested 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 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 licenses

There are two different types of licenses in **Enterprise Plus**, **FullClient and LightClient licenses.** In all other editions you can only purchase FullClient licenses.
Please note that licensed LightClient users are not able to use the FullClient. However, FullClient Users can also switch to the LightClient.

> For licensing reasons, it is not intended to switch from a FullClient user to a LightClient user!

Our sales team will be happy to answer any questions you may have about licensing.

Display data to which the user is authorized

In order to display the data to which a user is authorized, you must right-click on the corresponding user in the organizational structure. In the context menu that opens, you will find the following options under **displaying data records**:

- Password
- Documents
- Forms
- Rolls
- Uses
- Password Reset
- System Tasks

- Seal templates

All authorizations for a data record are taken into account, regardless of whether you are authorized by a role or the user.

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

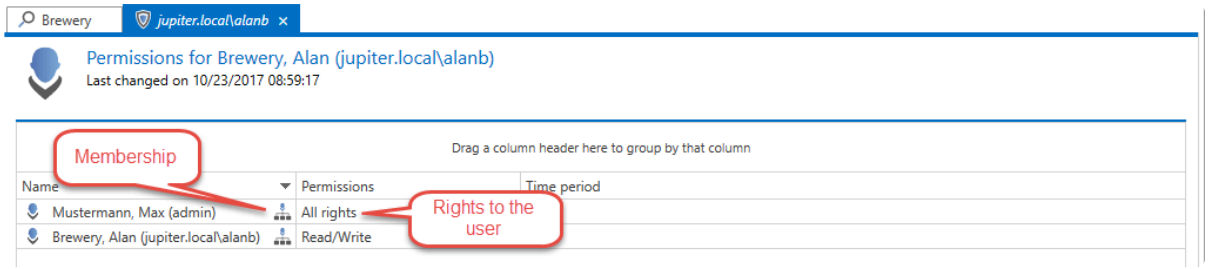
- **Local users**
  Local users are those users that were directly created in Password Safe. These users must be directly assigned a password when they are created. If local users are migrated from older versions, they receive a randomly generated password that is sent to them via email.

- **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.

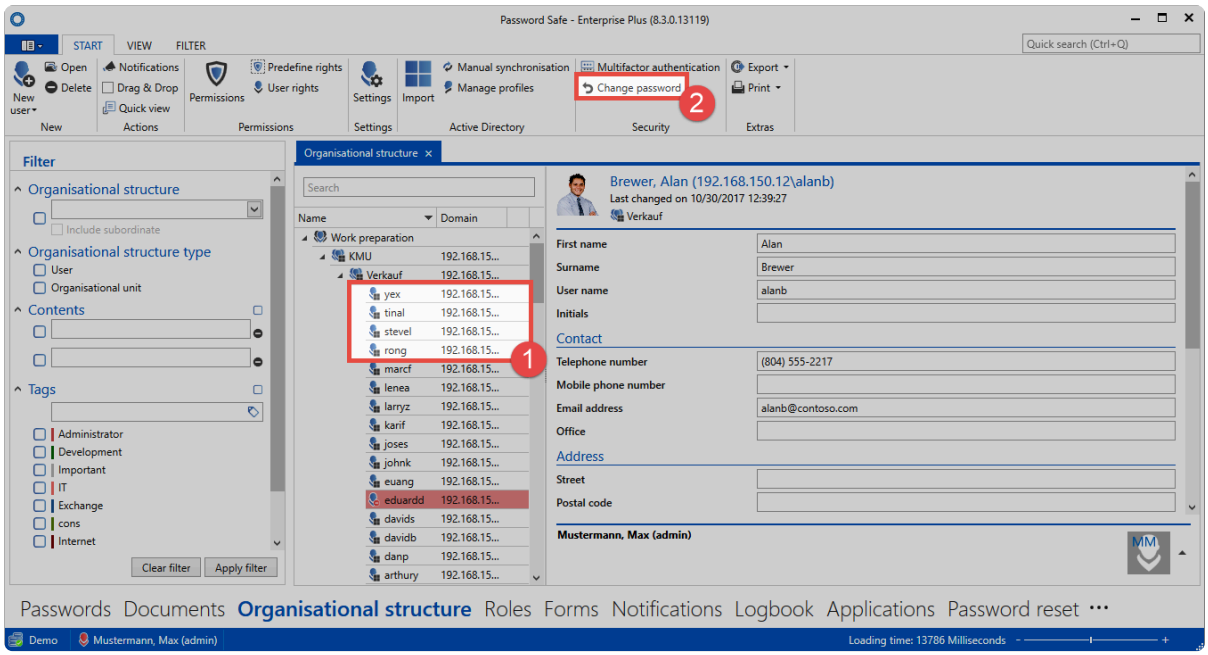


Assigning and changing passwords

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.

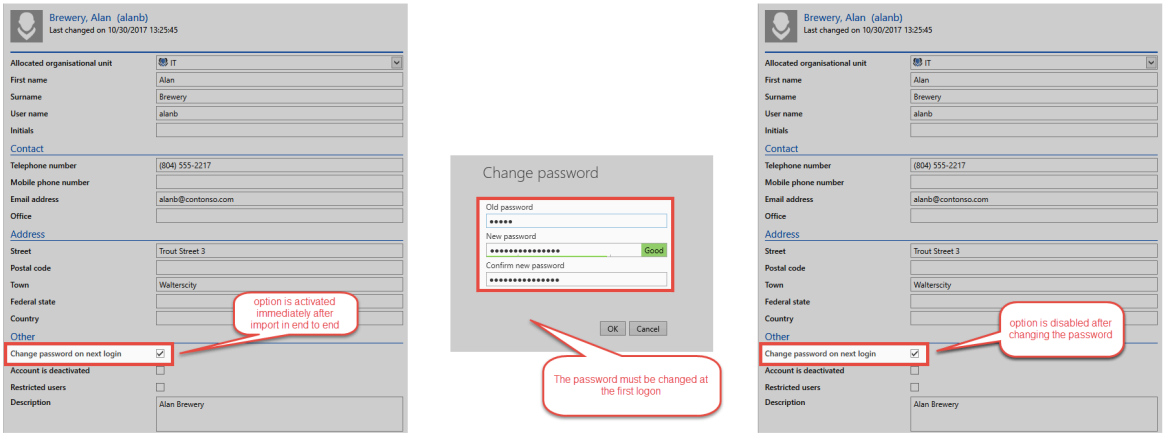
The passwords can be directly assigned or changed via the ribbon. Naturally, it is also possible to select

multiple users if e.g. several imported users should be assigned the same password.



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.



Security of passwords

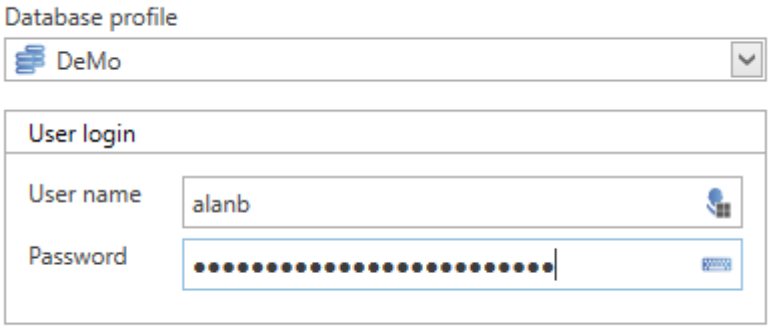
To guarantee that passwords are sufficiently strong, it is recommended that corresponding “password rules”:#passwortrichtlinien are created. It is especially important to ensure here that user names are excluded. The password rule then still needs to be defined as a “user password rule”:#administration.

Logging in to the database

The process for logging into the database differs depending on the type of user.

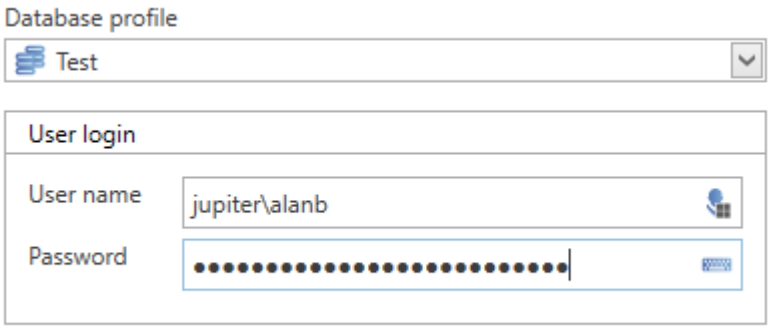
Local user

Local users simply log in using their user name and the assigned password.

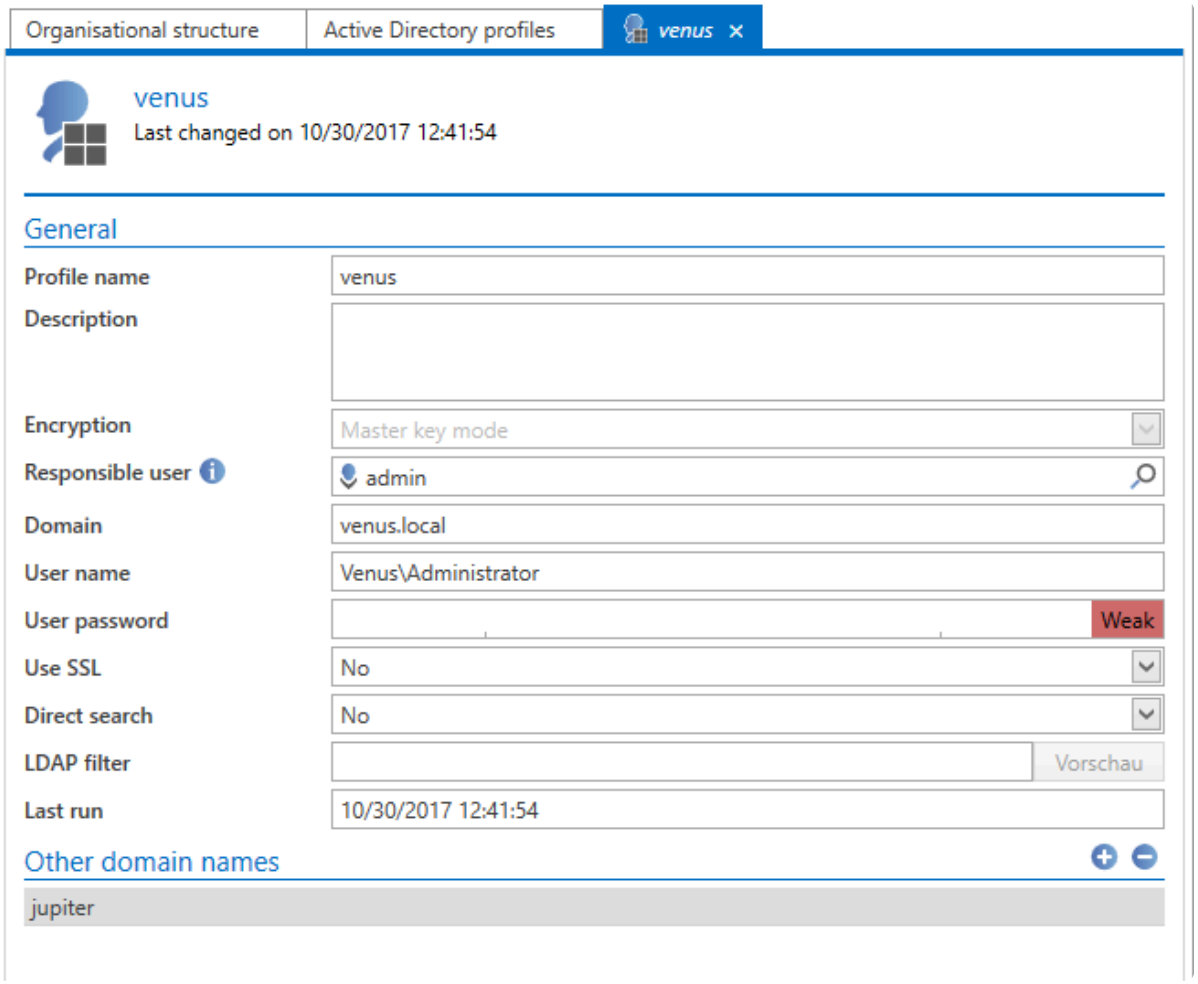


AD user

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:



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.



The logon to the client is automatically forwarded to the SSO Agent and other clients on the same computer. The same applies to logging on to the SSO Agent.

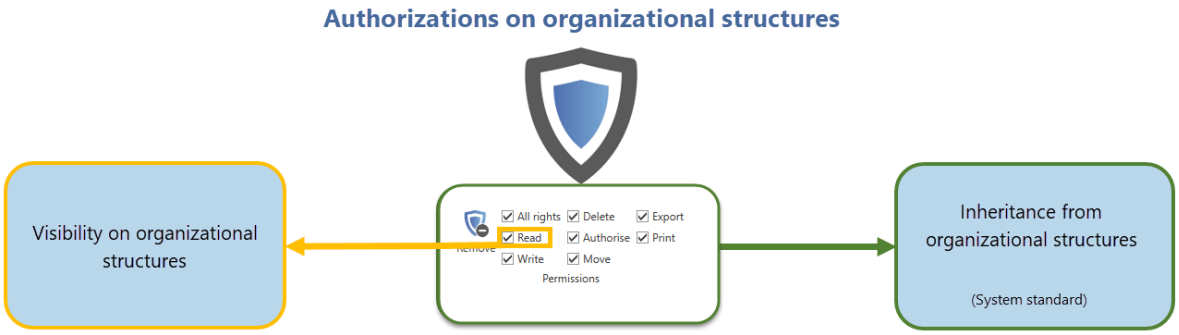
Permissions for organisational structures

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.



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:



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

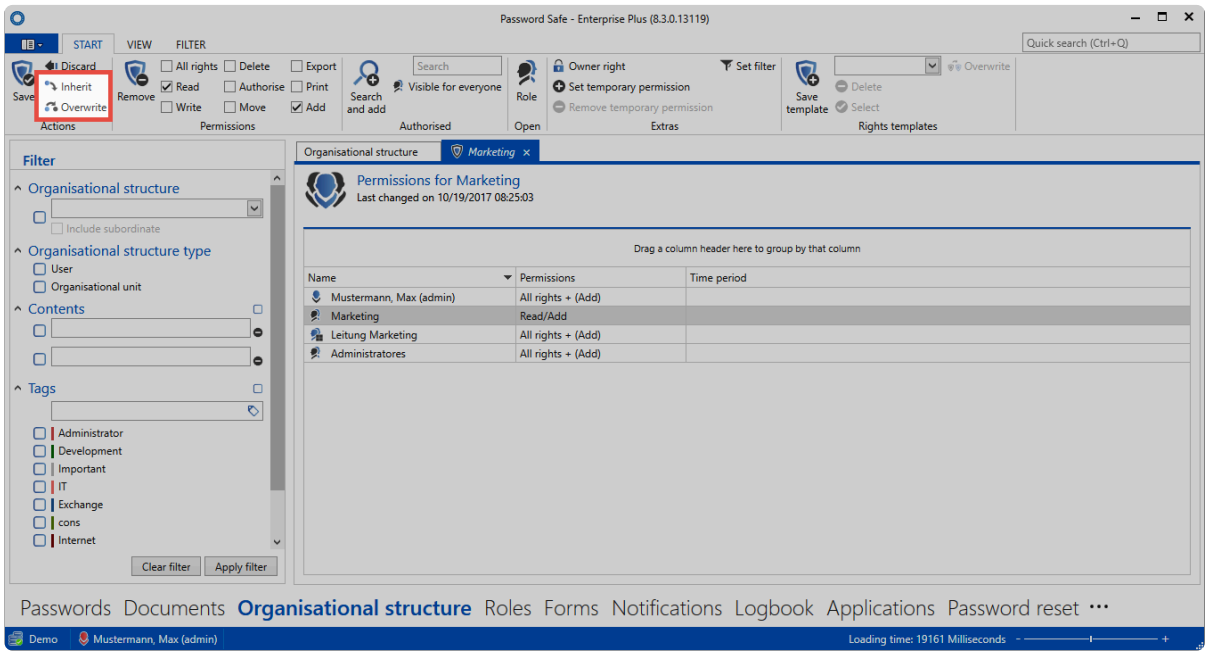
The "add" right holds a special position amongst the available rights because it does not refer to the organisational unit itself but rather to data that will be created within it. In general, it is fair to say that to add objects in an organisational unit requires the add right. If a user wants to add 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.



Relevant rights

The following options are required to view **“inherit”** and **“overwrite”** icons.

User right

- Can overwrite permissions
- Can inherit permissions

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.

Comparison of the modes	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	-	+
Autologin	+	+

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
- 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.

Relevant rights

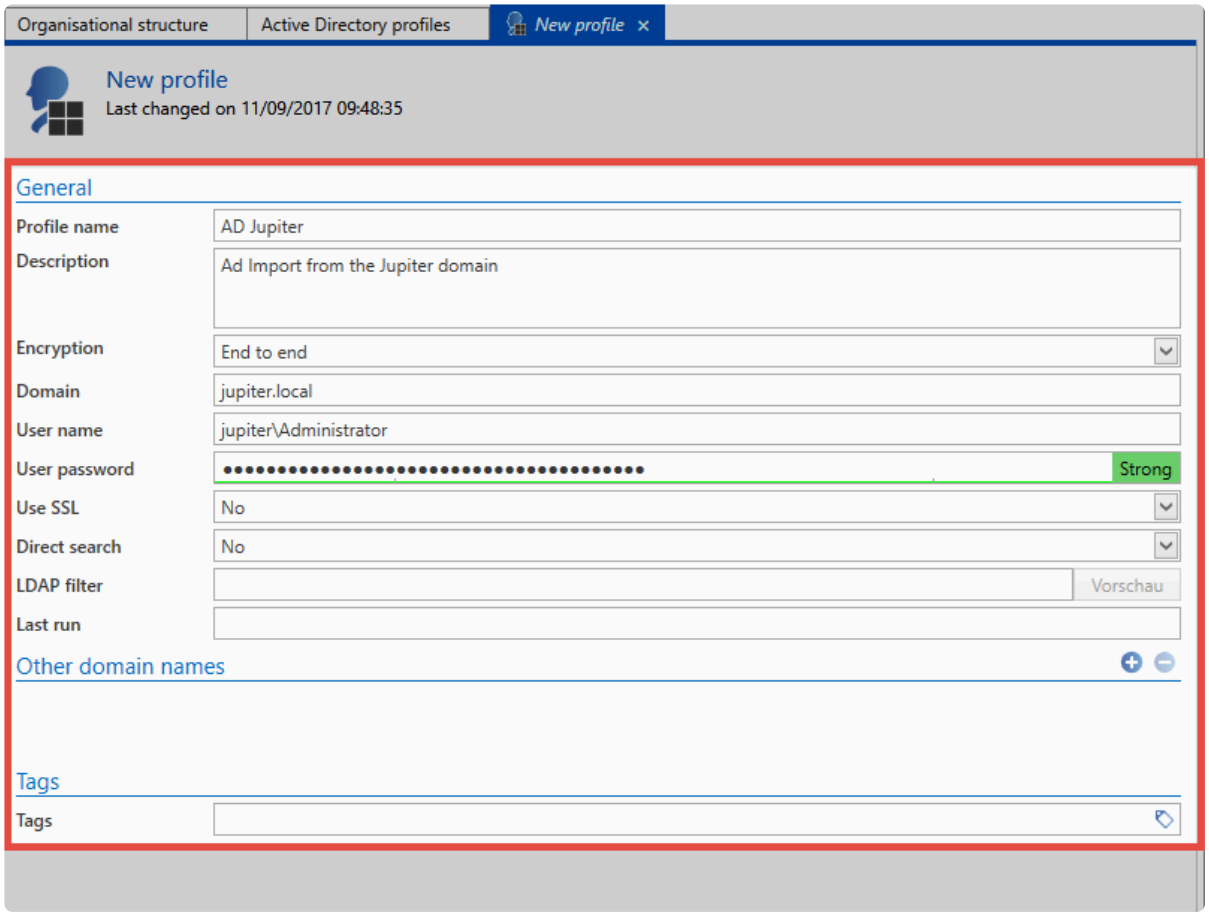
The following options are required to add new profiles.

User right

- Can add new Active Directory profiles
- Display organisational structure module
- Display role module

Creating profiles

The process for creating a new profile is started via the icon “manage profiles” on the ribbon.



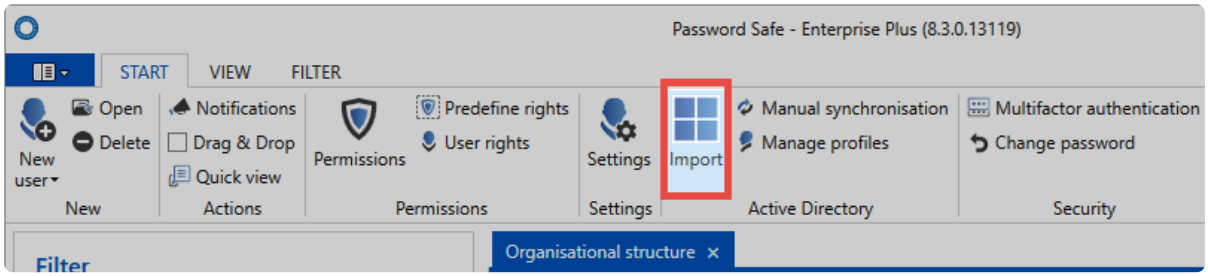
"End-to-end" needs to be set* in the "Encryption" field

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
- **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.
- Various security options – so-called AuthenticationTypes Enumeration – can be selected for the connection of the AD to Password Safe.
  - Secure
  - SecureSocketsLayer
  - ReadOnlyServer
  - Signing
  - Sealing

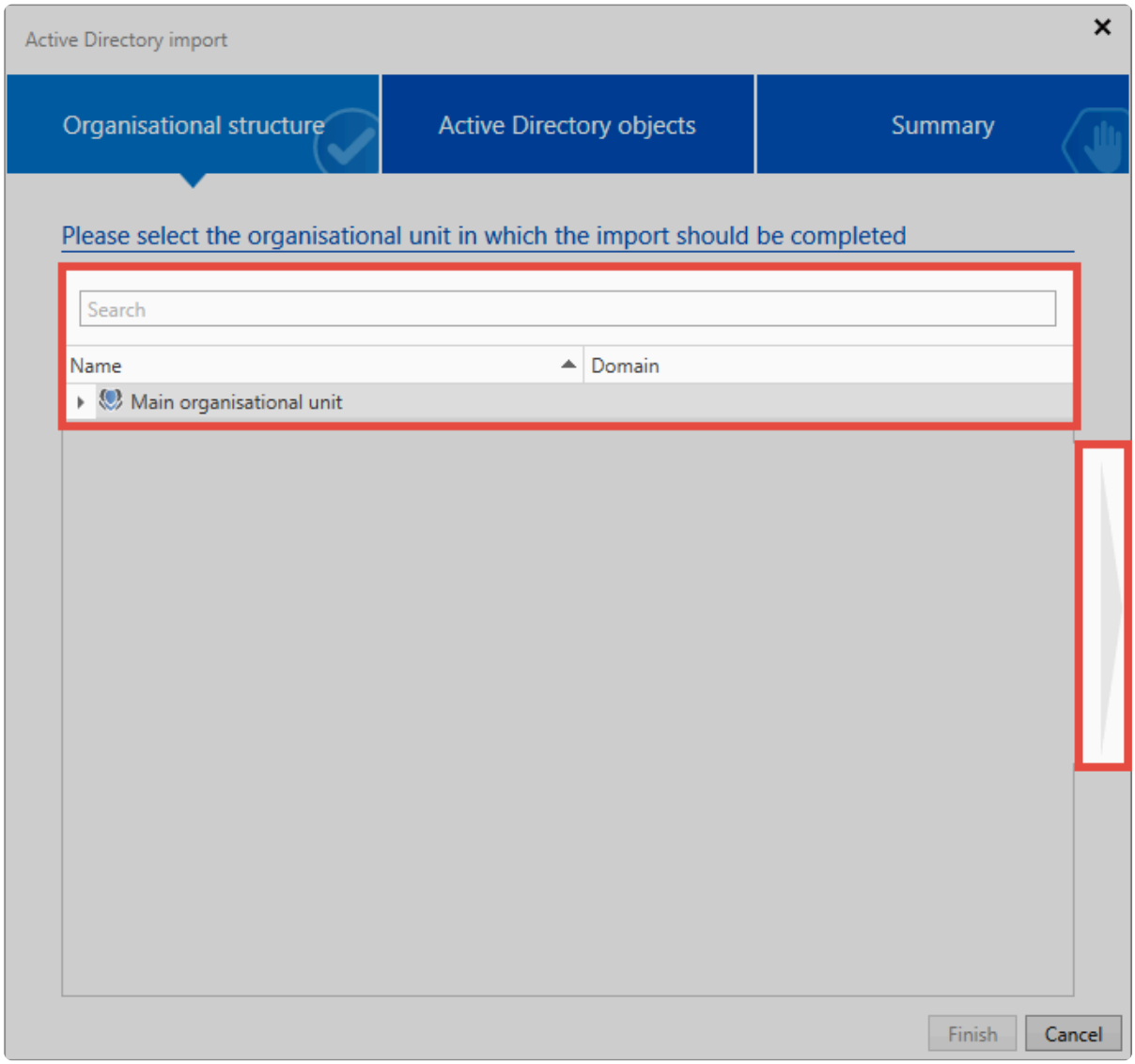
Import

The import is started directly in the ribbon. A wizard guides the user through the entire operation.



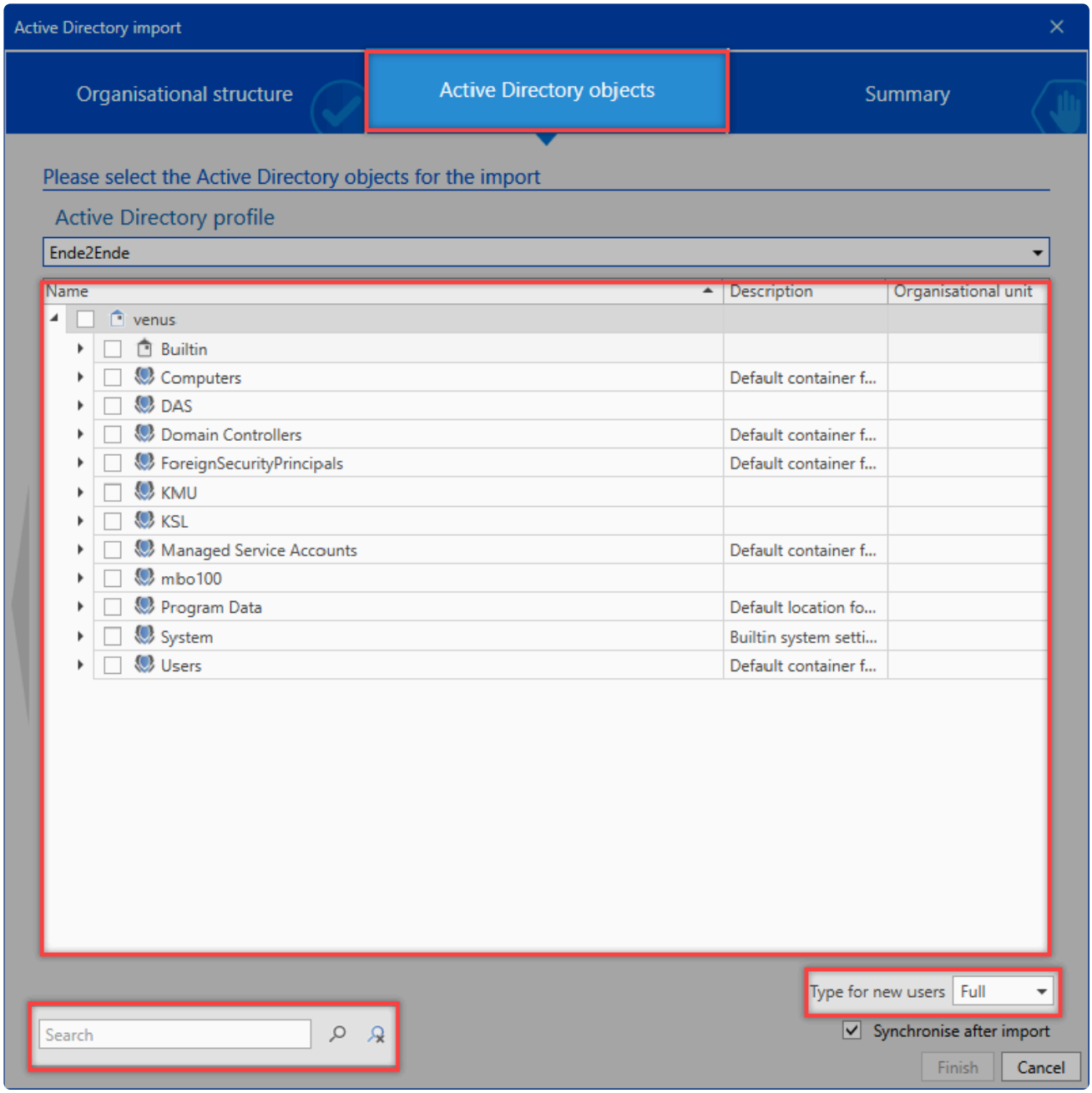
Organisational structure

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.

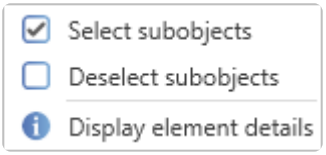


It can be seen that the organisational units **Jupiter** and **Contoso** contain items to be imported. The organisational units themselves will not be imported. The check next to the group **Accounting** indicates that the group itself will be imported along with some of its sub-elements.

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.



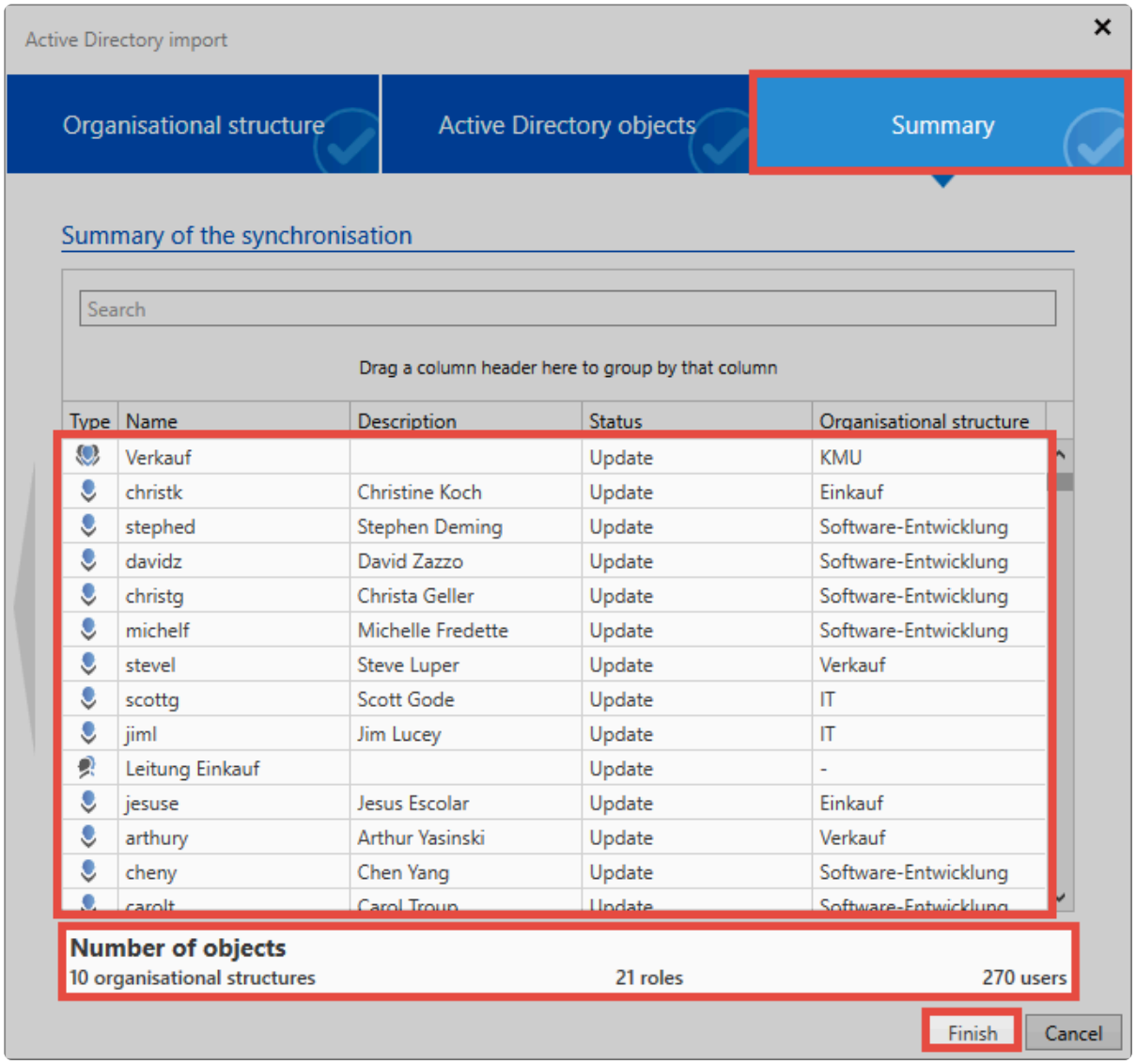
- **Select sub-objects** selects all sub-objects that are located **directly** below the current object
- **Deselect sub-objects** removes tags from all sub-objects that are located **directly** below the current object
- **Reset all items** removes all previously set tags
- **Display element details** lists all information that is available for the current element

In the lower area you can specify whether the users just selected for import should be created as **Light" or *Full** users.

If individual users, organisational units, or roles cannot be selected for import, they have already been imported via another profile

Summary

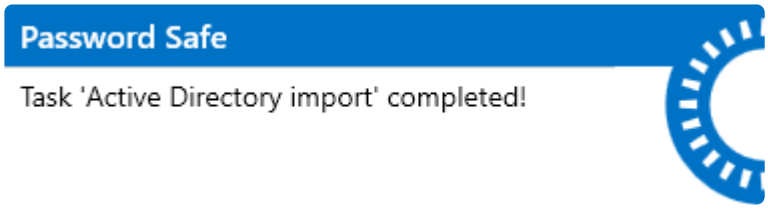
The last page summarises which objects will be edited and in what form. It specifies the names of the elements along with their descriptions. The **Status** column specifies whether the object is added, updated, or disabled. The last column specifies the organisational unit into which the element is imported. The number of objects is added together at the bottom.



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.



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?	None	None	None

In end-to-end mode, **no role affiliations** are issued during the import or synchronisation.

Logging into Password Safe

Users imported in this mode can **not** login with the domain password. Rather, a password is generated during import. This password is sent to the users by e-mail. If a user has not entered an e-mail address, the user name is entered as the password. The initial password can be changed by the administrator or the user himself at the first login.

Masterkey mode

Maximum convenience

In contrast to end-to-end mode, which places the main focus on security, Masterkey 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**.

Relevant rights

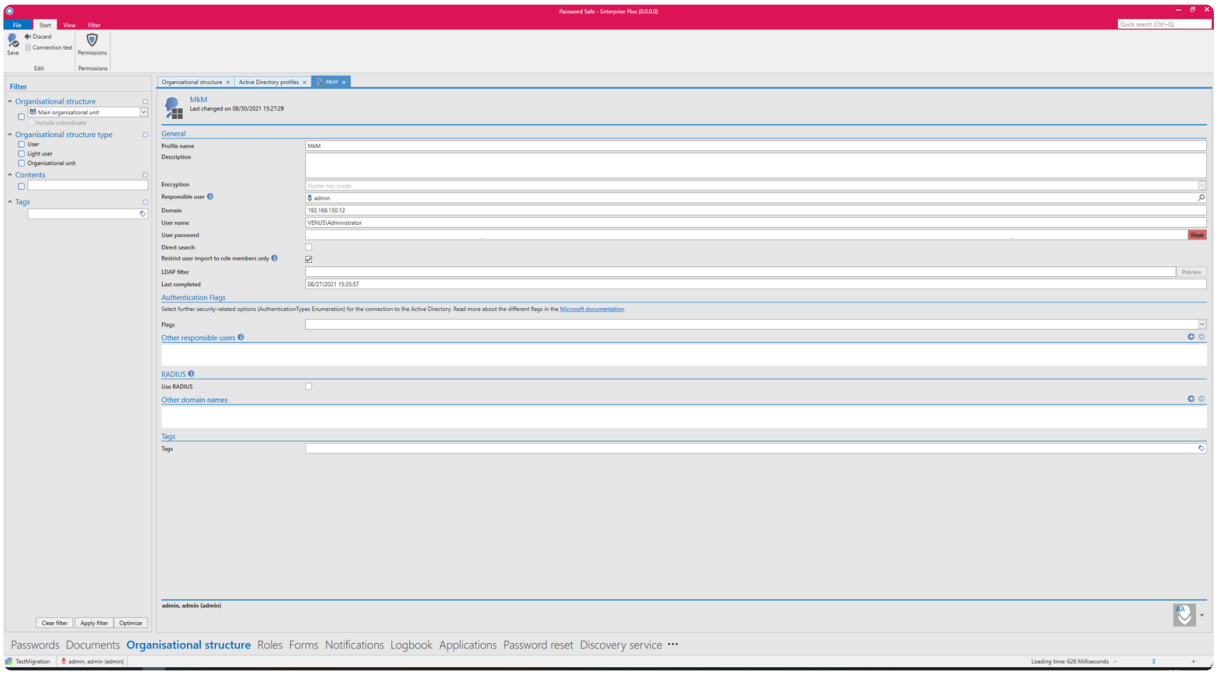
The following options are required to add new profiles.

User right

- Can add new Active Directory profiles
- Display organisational structure module
- Display role module

Creating profiles

Profile management is started via the icon of the same name on the ribbon.



The following information must be provided in the profile:

- **Profile name**
- An optional **description**
- Masterkey 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.
- **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.
- By activating the checkbox **Restrict user import to role members only**, a simplified mode is activated. In this mode, only AD users who are members of at least one role are imported. As soon as they are no longer a member of at least one role, they are deleted from Password Safe.
- By activating the checkbox **Force update on next synchronisation**, **ALL** records will be updated on the next synchronisation, regardless of whether the record has changed in the Active Directory or not. (This checkbox is automatically activated when you have edited the other responsible users and is deactivated again after the next synchronisation).
- The **LDAP filter** can be used to directly specify an AD path as an entry point via an LDAP query.
- Various security options – so-called AuthenticationTypes Enumeration (**Flags**) – can be selected for the connection of the AD to Password Safe.
    - Secure
    - SecureSocketsLayer
    - ReadOnlyServer
    - Signing
    - Sealing

The first two options are already activated by default when configuring a new profile. If a connection is not possible, deactivate SecureSocketsLayer and try again.

- **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.

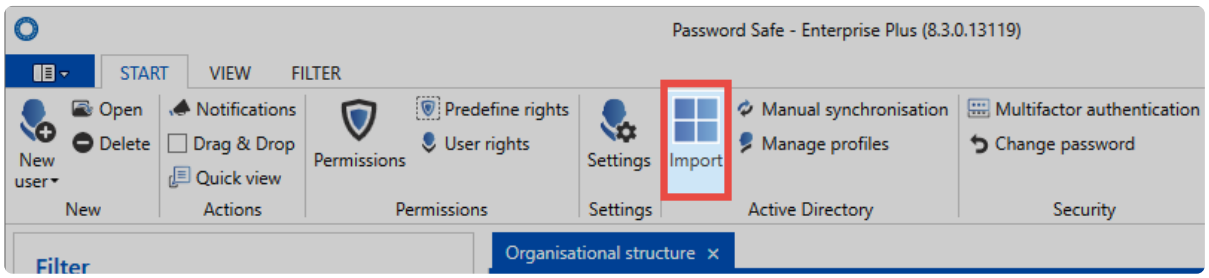
The master key is added in form of a certificate. It is **essential to back up** the generated certificate! If the database is being moved to another server, the certificate also needs to be transferred! Further information can be found in the section Certificates.

You can now use the option to integrate a RADIUS server. Read more in the following

chapter

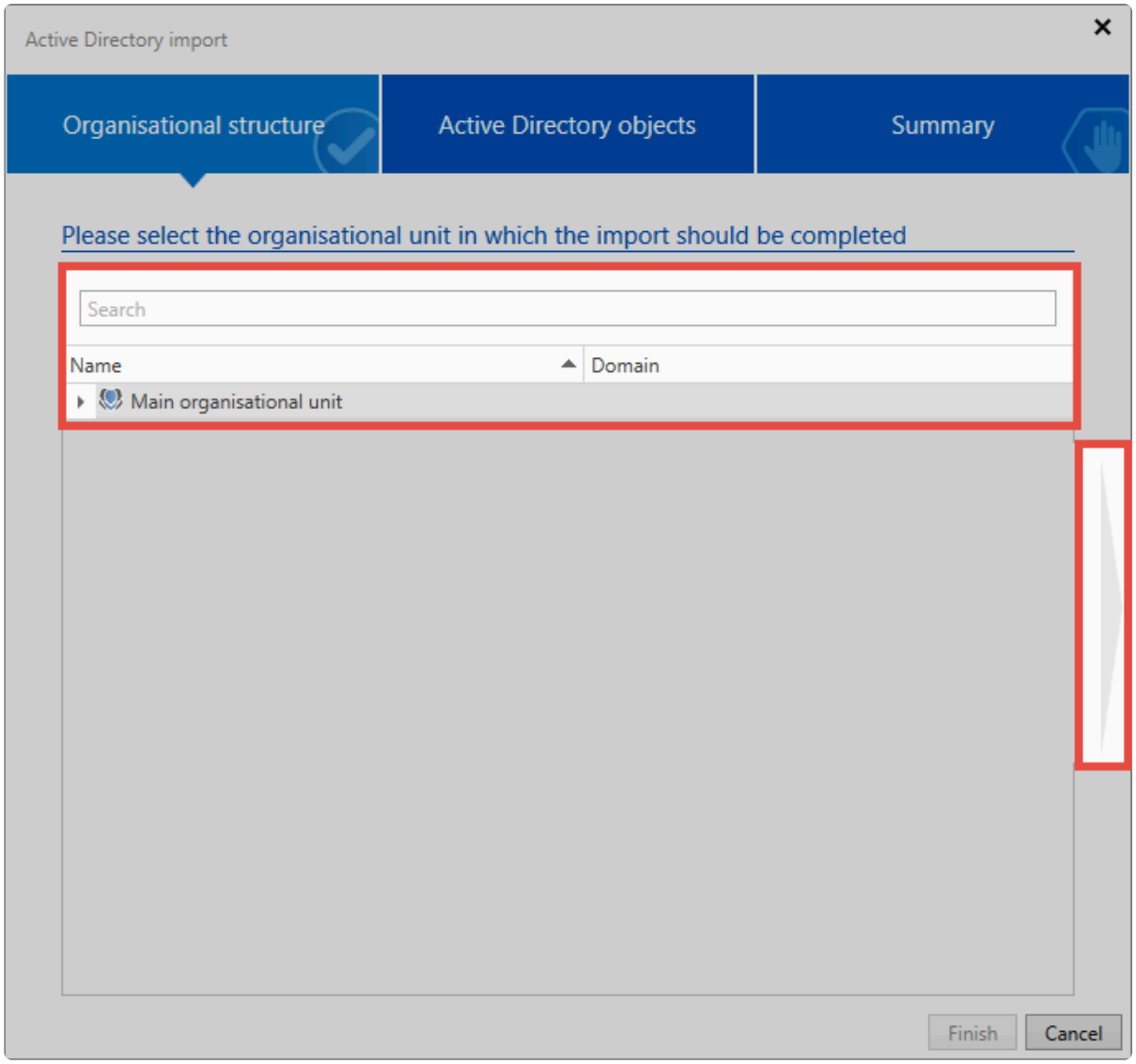
Import

You can start the import directly in the ribbon. A wizard guides the user through the entire operation.



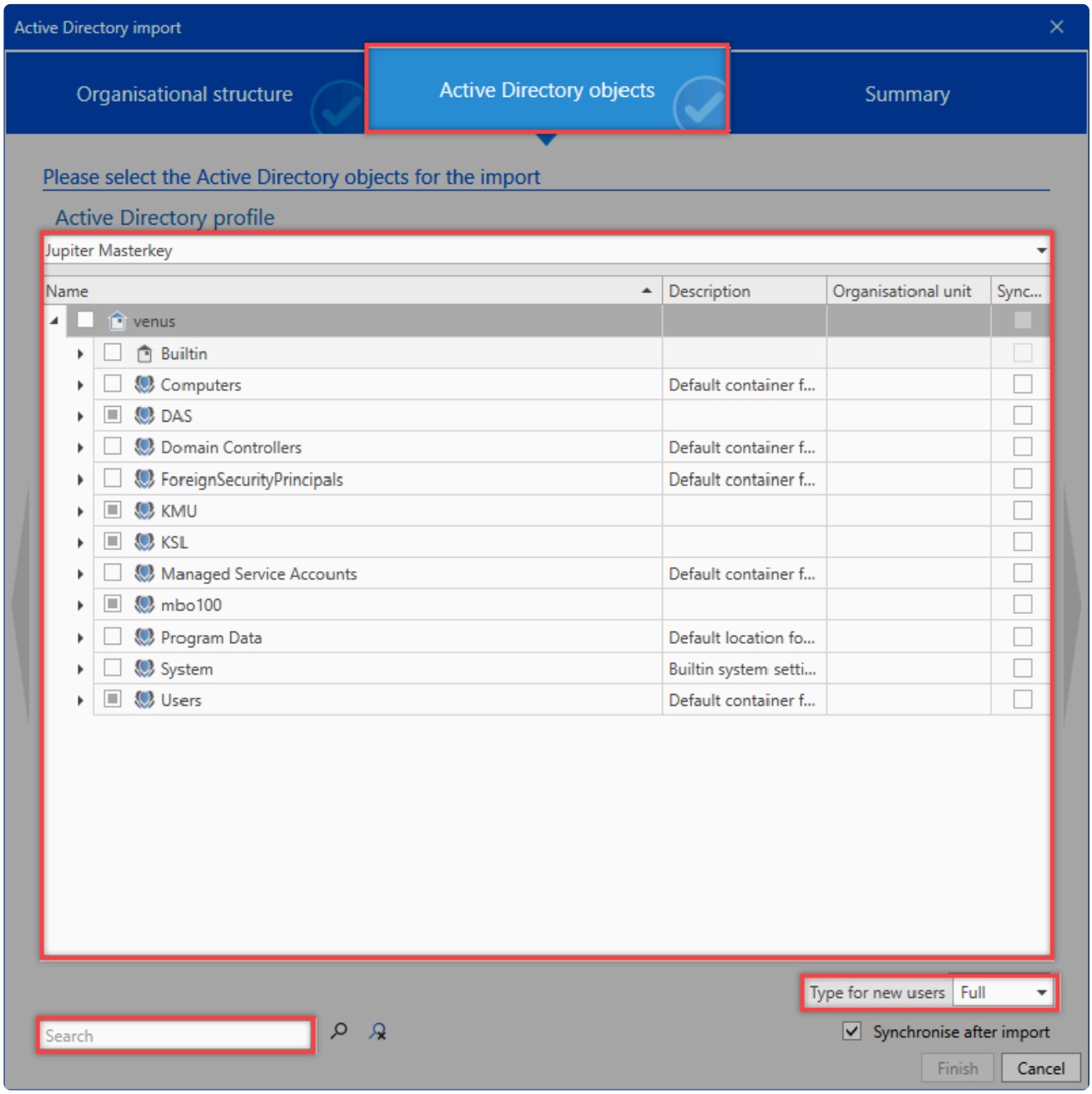
Organisational structure

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**.



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.

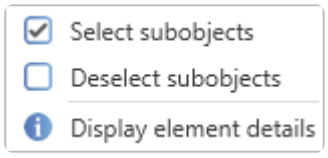


As you can see, the organisational units **Jupiter** and **Contoso** contain items to be imported. The organisational units themselves will not be imported. The group **1099 Contractor** is imported including all sub-elements. The check next to the group **Accounting** indicates that the group itself will be imported along with some of its sub-elements. The ticks in the last column ensure that the elements are observed in future synchronisation 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.



If individual users cannot be selected for import, they have already been imported via an end-to-end encrypted profile.

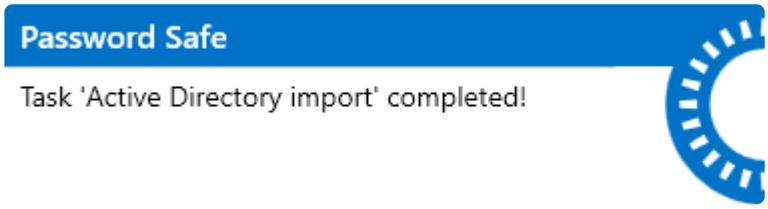
In the lower area you can specify whether the users just selected for import should be created as **Light" or *Full** users.

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.



Imported users and organisational units

The users and organisational units imported in Masterkey 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 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.

Logging into Password Safe

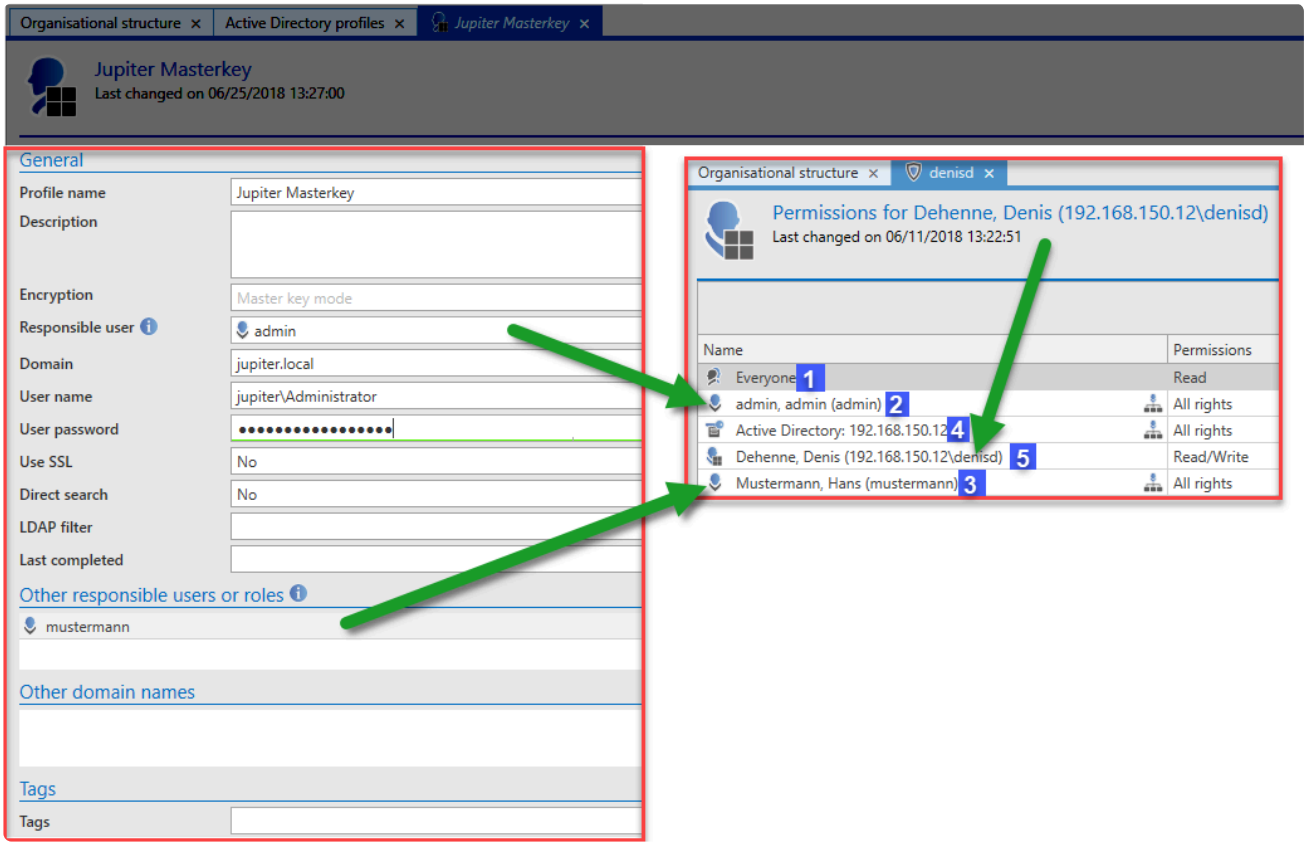
Users who are imported using this mode can log in with the domain password. Please note that no domain needs to be specified when logging in. Of course, the login process can also be supplemented with multifactor authentication.

Logging on using Kerberos works “automatically”. As long as the corresponding Kerberos server is accessible, the users in the domain authenticate themselves via Kerberos using their domain password. If the logon via Kerberos does not work – e.g. due to incorrect configuration of the domain controller – the logon via the NTLM protocol is attempted. However, these are all settings that have to be made on the domain controller and have nothing to do with Password Safe.

Logging on to Password Safe using SSO via Kerberos is currently not possible.

Permissions to imported objects

The rights to be issued to imported users are explained in the following example:



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 keys as 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.

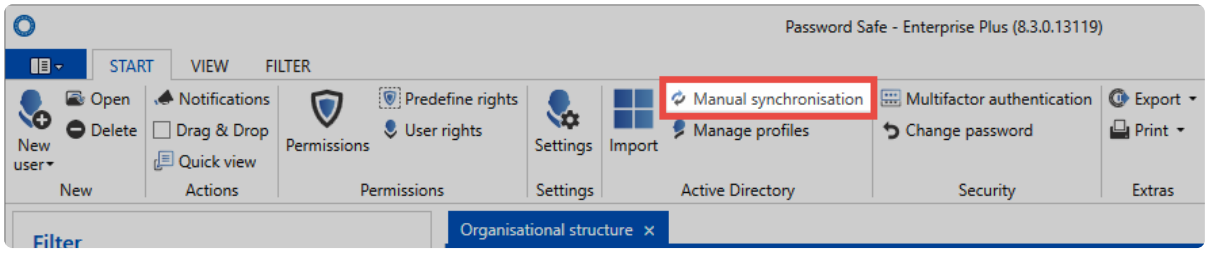
Synchronization

During synchronization, all relevant information for users, organisational units and roles (names, email, etc.) is updated. Changed affiliations for roles are adjusted. Likewise, users are activated or deactivated according to the settings in the AD. If the membership of organizational units is to be changed, this can be done by **Drag & Drop**. New users and correspondingly defined roles are imported.

If the tick was not set in the **Synchronisation** 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 via the system tasks.

Deleting or removing users

If a user is deleted in Active Directory, it is also deleted in Password Safe during the next synchronisation. For this purpose, it is necessary for the user to be imported as a **synchronisable** user.

If the user is only deleted from Password Safe but retained in Active Directory, a synchronisation needs to be carried out to delete it from the database. For this purpose, the wizard is called up via **import**. The first step is to select an organisational unit. This has no effect when simply deleting a user. The second step is to search for the user. Both ticks are removed.

After checking the summary, the process is concluded. The synchronisation is completed and the user is deleted from the database.

RADIUS authentication

What is the RADIUS authentication?

RADIUS (Remote Authentication Dial-In User Service) is a client-server protocol used primarily for authentication and authorization of users during dial-up connections in corporate networks. Password Safe can also benefit from the advantages of a RADIUS server. In particular, multi-factor authentication should be mentioned here. But all other RADIUS-typical functions can also be used. Further information can be found for example at **Wikipedia**.

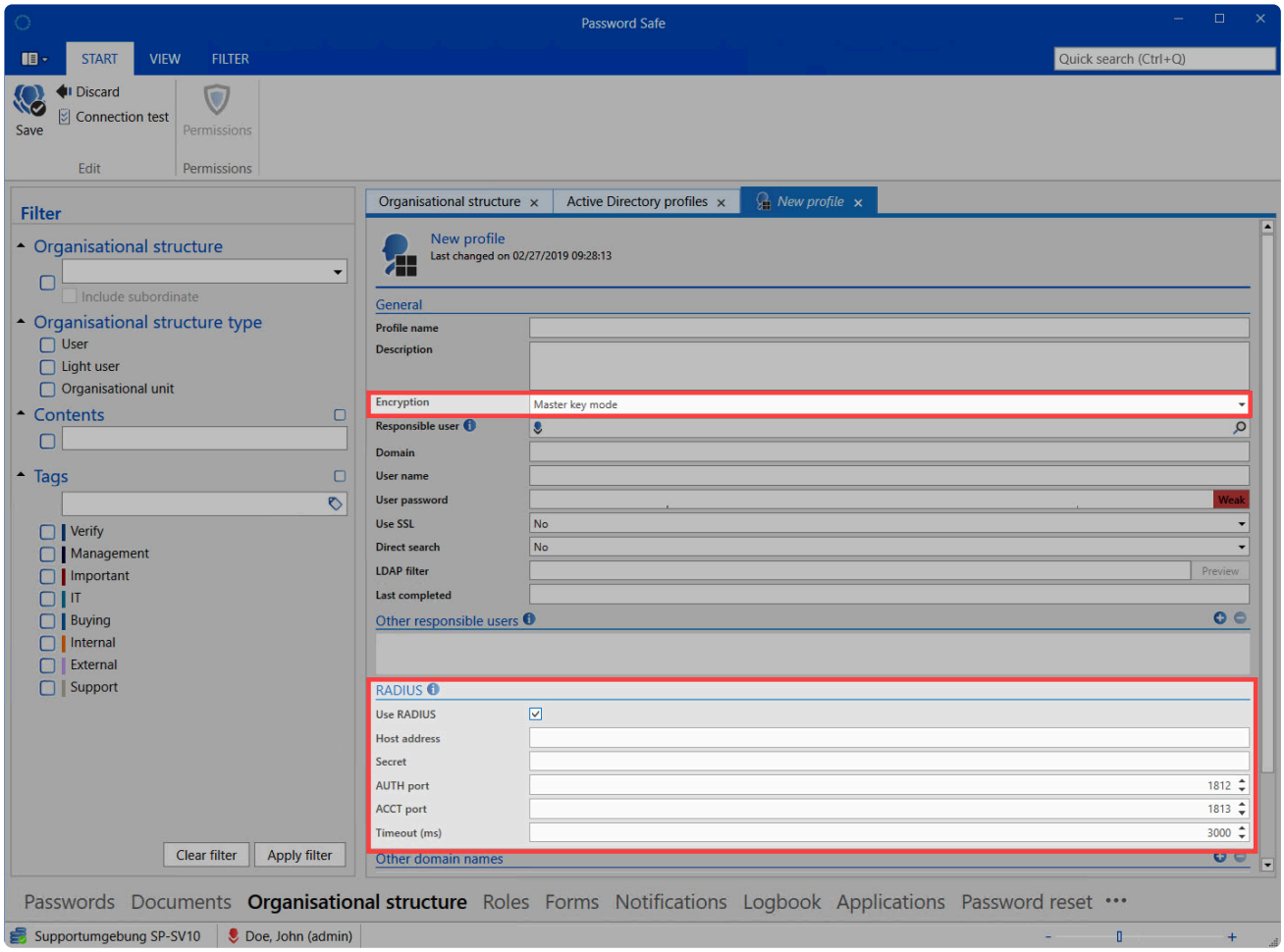
Requirements

In order for Password Safe to address a RADIUS server, the following requirements must be met:

- A RADIUS server must be available and accessible via the network.
- Access to the Password Safe AdminClient must be set up on the RADIUS server.
- A corresponding Secret must be configured for access.
- In Password Safe, users must have been imported from the AD in masterkey mode.

Configuration

The actual connection of the RADIUS server is simple:



Use RADIUS First; the usage is activated.
Host Address The address of the RADIUS server is stored here.
Secret Refers to the secret stored for the Password Safe AdminClient.
AUTH Port The so-called AUTH port of the RADIUS server is specified here.
ACT Port The ACCT port of the RADIUS server can also be stored; if required.
Timeout The time the RADIUS server has to react; can also be configured.

Azure AD connection

Why Azure AD?

More and more companies use cloud services. Therefore, also the management of users is outsourced. Instead of a classic Active Directory via LDAP, an Azure AD is used more often. Password Safe integrates the possibility to bring in users and roles from Azure. To use users and roles from multiple Azure ADs, you can create multiple profiles.

Differences to the LDAP connection

The connection to the Azure AD differs in one special point from the connection to a conventional Active Directory. While Password Safe queries the users, groups, and roles actively from the conventional AD, the Azure AD is pushing them automatically to our server. For this a so-called SCIM service is used.

To login to Password Safe, after entering the username a popup opens for the authentication with the entered Microsoft account. Here, a possible configured second factor is also requested. The authentication is handled via the Open ID Connect protocol.

Linking Azure AD

Below you will find instructions on how to connect Azure AD to Password Safe. In the Azure portal, go to the management page of your Azure Active Directory. Use an account with administrative permissions for this. During this, login to Password Safe with an account that has the user right “Display organisational structure module“, “Can manage Azure AD profiles”, and “Can create new Azure AD profiles” enabled.

Preparations in the Azure portal

1. Note the “Tenant ID” of the Azure AD – you will need this later for the configuration in Password Safe
2. Navigate in your Azure AD to “Enterprise applications”
3. Add an own application, that is not listed in the Azure Gallery – in our example, we name it “MATESO Password Safe”
   Note: A key feature of Password Safe is that it is self-hosted by our customers. However, to be listed in Azure Gallery, a SaaS model is required. Therefore, Password Safe is not available in the Azure Gallery.
4. When the application was created successfully, you are redirected to it automatically
5. Note the “Application ID” – again, this is needed later
6. In the navigation, click “Users and groups”
7. Add the Users and groups that should be available in Password Safe
8. Navigate to the “Provisioning“ entry
9. Configure the Provisioning Mode to “Automatic”
10. Keep the browser tab open and switch to Password Safe

> ! The import of Azure groups as Password Safe roles is only possible if you have booked the Azure package **Azure AD Premium P2**!

Create an Azure AD profile in Password Safe

1. Navigate to the module “Organisational structure” or “Roles”
2. In the toolbar, click on “Manage profiles” in the category “Azure AD”
3. Create the profile with your information
4. Insert the Tenant ID and the Application ID you noted before
5. As soon as the profile has been saved, a popup opens for generating a token
6. Choose a desired expiration date (max. 10 years) and click “Generate token”
7. Note down the values of the fields “Tenant URL” and “Secret Token”
8. Switch back to the Azure portal

Provisioning configuration

1. Fill the fields “Tenant URL” and “Secret Token” with the information provided by Password Safe
2. Click “Test Connection”
3. When the test has been successful, click on “Save” at the top of the page
4. Back on the “Provisioning” page, click “Start provisioning“
5. In the settings of the provisioning, check if “Provisioning Status“ is set to “On”
6. All allocated users and groups are created in Password Safe now

> ✻ The default provisioning interval is 40 Minutes. So it may take this amount of time until the users and roles are shown in Password Safe.

> ! Please note that Azure establishes the connection to Password Safe. For this, the client URL must be accessible from an external network and any used SSL certificate must be valid!
> If the users are not created in Password Safe, see the Azure Enterprise Application **Provisioning log** for more information.

Configuration of the login

1. To make sure Azure users are able to log in to Password Safe, a few further configuration steps are required.
2. In Azure, navigate to the Overview page of your Azure AD
3. Navigate to “App registrations“
4. If no application is displayed, click “All applications”
5. Click on “MATESO Password Safe” and navigate to “Authentication“
6. Click on “Add a platform“, select “Mobile and desktop applications“ and configure the required URIs

For which client?	What URI is required?

WebClient	**Custom URI:** https://WEBCLIENT_URL/authentication/login-via-oidc
FullClient & SSO Agent	https://login.microsoftonline.com/common/oauth2/nativeclient
iOS & Android	**Custom URI:** psrmobile://auth
Google Chrome Extension	**Custom URI:** https://bpjfchmapbmjeklgmlkabfepflgfckip.chromiumapp.org
Microsoft Edge Extension	**Custom URI:** https://ahdfobpkkckhdhbmnpjehdkepaddfhek.chromiumapp.org
Firefox Extension	**Custom URI:** https://28c91153e2d5b36394cfb1543c897e447d0f1017.extensions.allizom.org/

! In order for your users to be able to log in to the FullClient on the desktop with the imported users, WebView2 from Microsoft must also be installed on each end device. This is required to be able to display general websites (Azure login page) in the FullClient.

Set API permissions

Finally, the API permissions for the Azure API have to be set, so the login to Password Safe can be performed successfully.

1. Navigate to “API permissions” and click “Add a permission“
2. Select “Microsoft Graph” and then “Delegated permissions”
3. Set the checkboxes for “openid” and “profile” just under “OpenId permissions”
4. Click on “Add permissions”
5. Click on “Grant admin consent for YOUR_AD_NAME”

Frequently Asked Questions

Is it possible to migrate from LDAP to Azure AD?

Currently, an automated migration from LDAP users (E2E as well as MasterKey) to Azure AD users is **not possible**!

Which port is used for the SCIM endpoint for provisioning users/groups from Azure AD to Password Safe Application Server?

11015 is the port that will be used for the communication from Azure AD to Password Safe.

Does Azure AD work on servers that are only available internally?

An integration on servers, that are not accessible from external sources, the integration of Azure AD is

also possible. For this, you can use the Provisioning Agent.

1. Download the Provisioning Agent from here
2. Install the Provisioning Agent on the server with the Password Safe Server
3. Start “AAD Connect Provisioning Agent Wizard”
4. Select “On-premises application provisioning Azure AD to application”, click next
5. Click “Authenticate” and authenticate with a user.This user should be a Hybrid administrator or a global administrator.
6. Click “Confirm”
7. Wait for the application to finish the registration in Azure
8. Switch to the Azure Portal
9. Click “Azure Active Directory”
10. Click “Enterprise applications”
11. Click “New application”
12. Search for “On-premises SCIM app”
13. Click “On-premises SCIM app”
14. Adjust the name
15. Click “Create”
16. Wait for the operation to end
17. Click the created application in the overview of “Enterprise applications”
18. Click “Provisioning”
19. Click “Get started”
20. Set provisioning mode “Automatic”
21. Unhide “On-Premises Connectivity”
22. Assign the just installed agent to this application by selecting it and click “Assign Agent(s)”
23. It takes about 20 minutes until the agent is correctly connected to your application and you can proceed.
24. continue with “Provisioning configuration” on this help page above

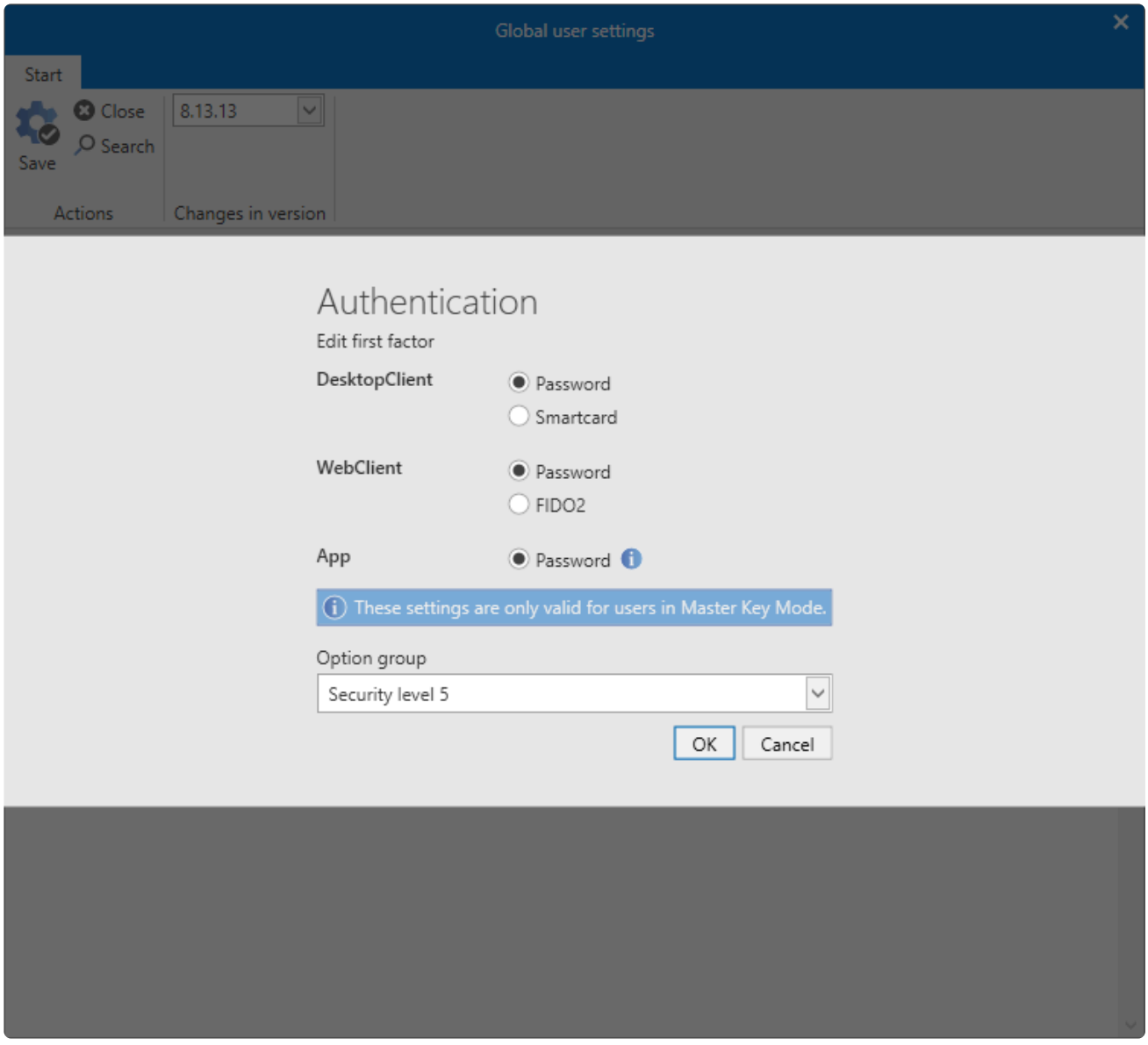
First factor

What is meant by first factor?

It is a process that regulates access to our system.

Requirements

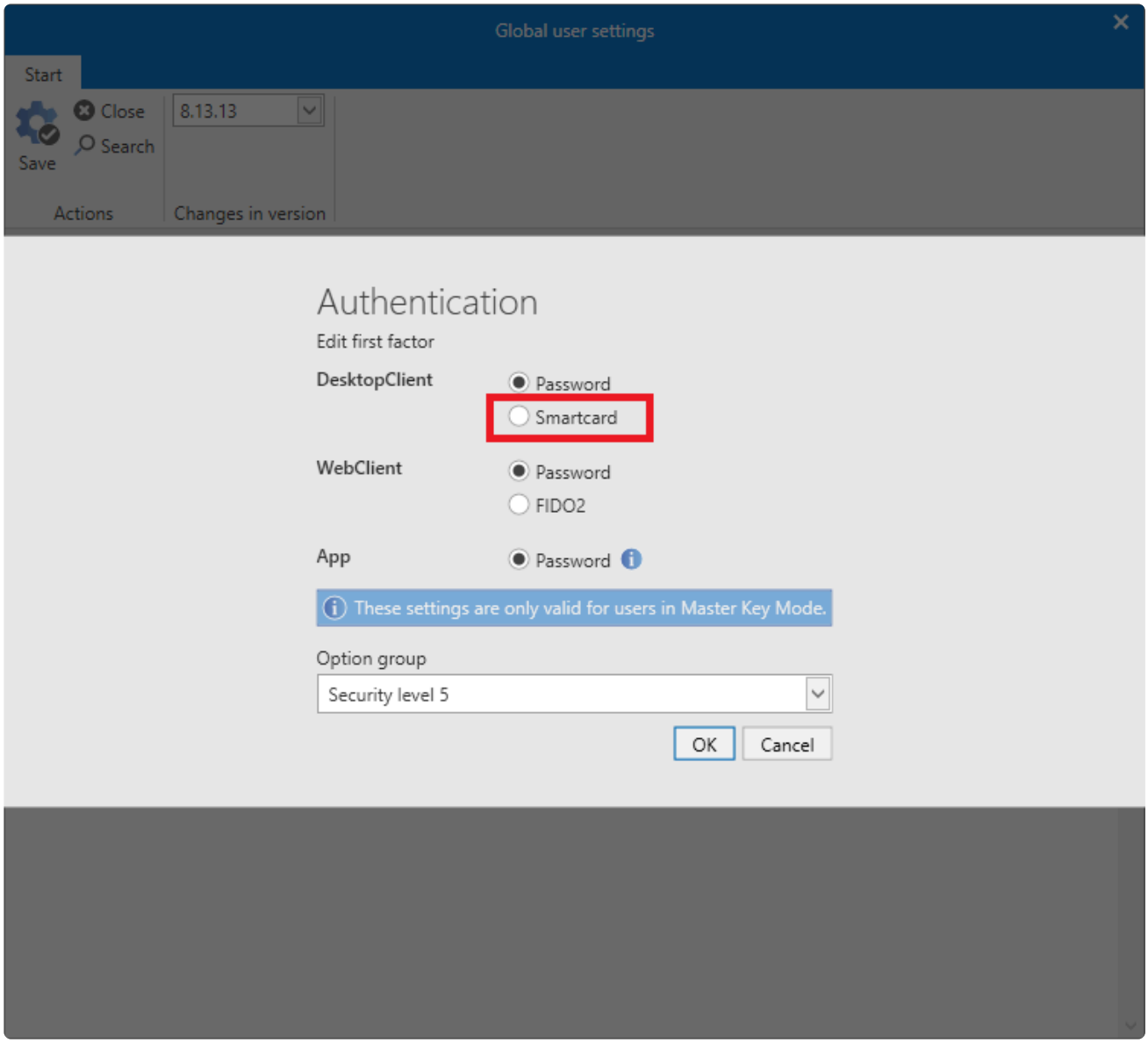
With the user setting **Edit first factor** you have the possibility to define another factor for authentication than the standard password.



Factors

Smartcard (only on FullClient)

The configuration is done via the user setting **First factor**.



This option is only valid for users in master key mode

The smartcard logon tries to determine whether the certificate belongs to the user to be logged on based on the applicant in the smartcard certificate. This is done using regex, the default regex “^{username}[.@\\/-_:]({domain})$” or “^({domain})[.@\\/-_:]({username})$” is applied to the applicant. In this case, “{username}” is replaced with the user to be registered and “{domain}” is replaced with the domain in the AD profile in the regex and if the regex query is positive, the user is registered. If the format of your applicant in your certificates is not compatible with these two regex queries, you must set a custom regex query in the Admin Client. Please note that “{username}” for username and “{domain}” for the AD domain SHOULD be present in the regex query. If the domain must be explicitly specified, it must be written in capital letters.

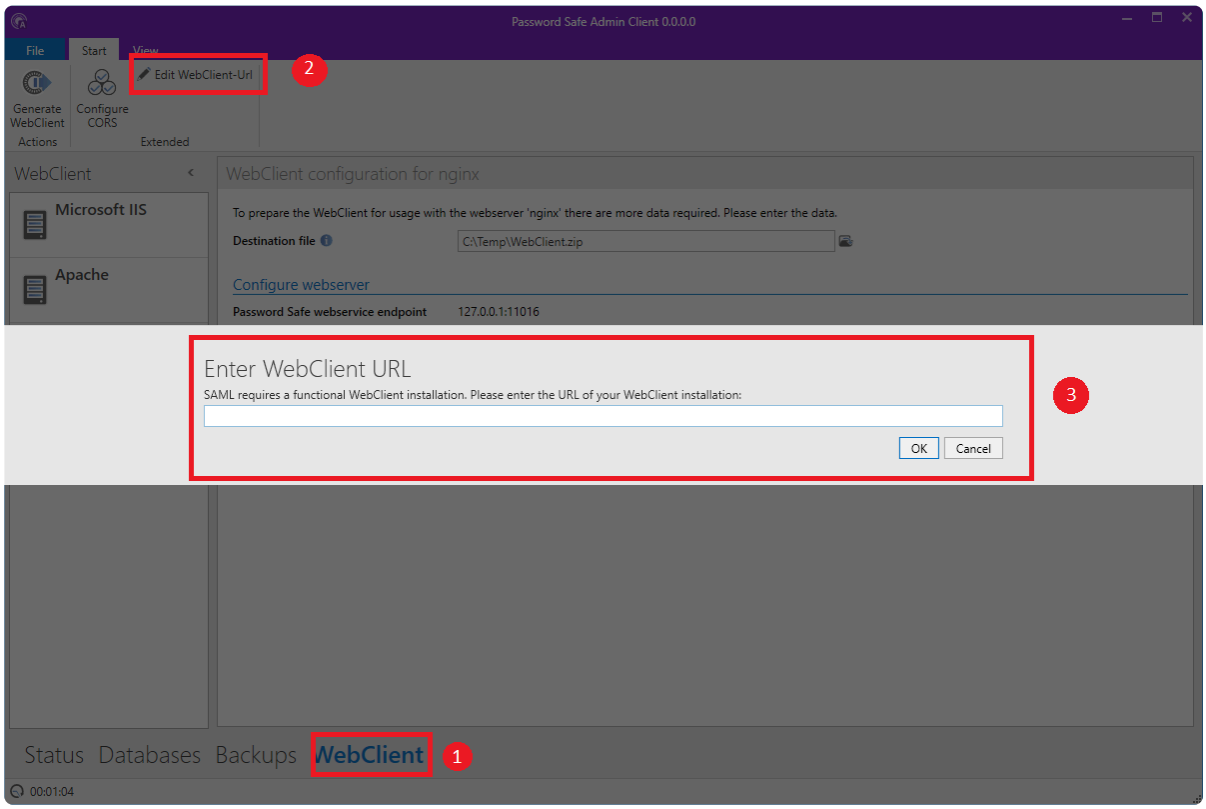
In addition, the smartcard certificate must of course also be valid on the server!

Fido2 (only at the WebClient)

Requirement

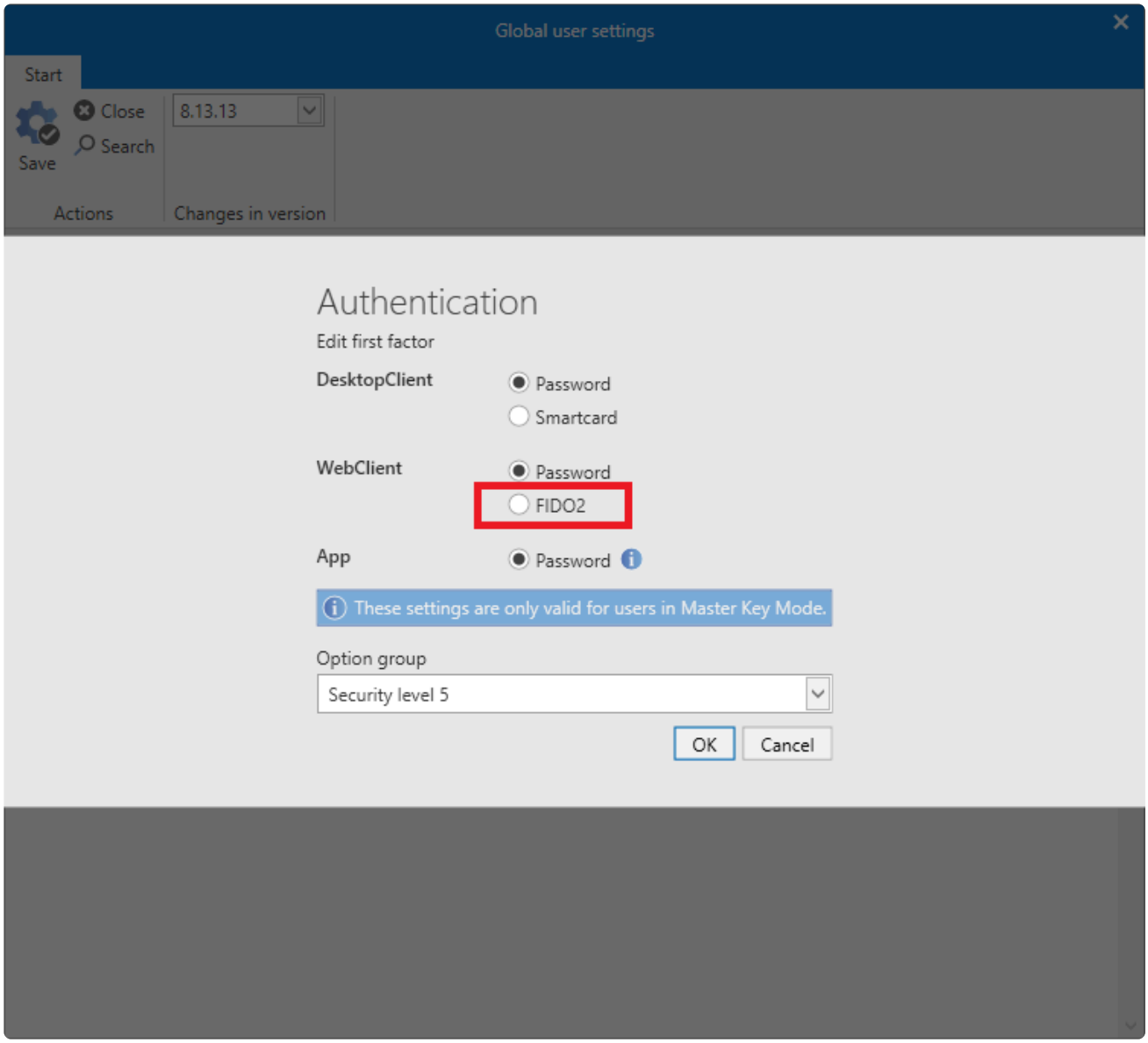
For Fido2 it is mandatory that SMTP is configured. In addition, an e-mail address must be stored for the AD users.

Furthermore, the URL of the WebClient must be stored in the Admin Client:

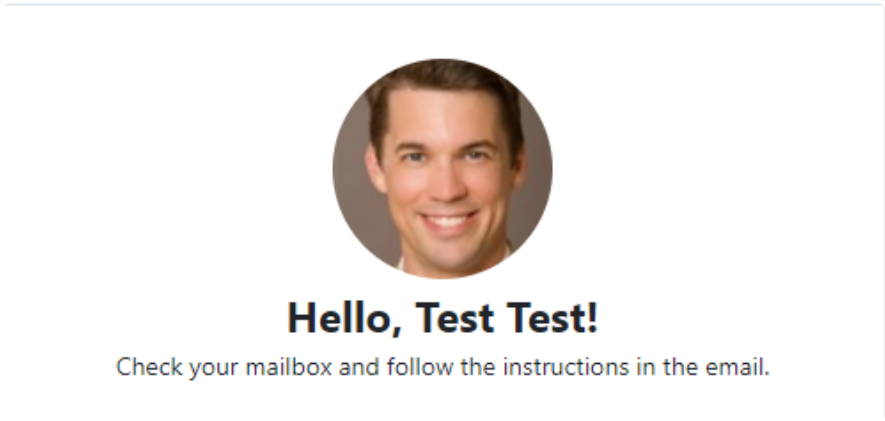


Configuration

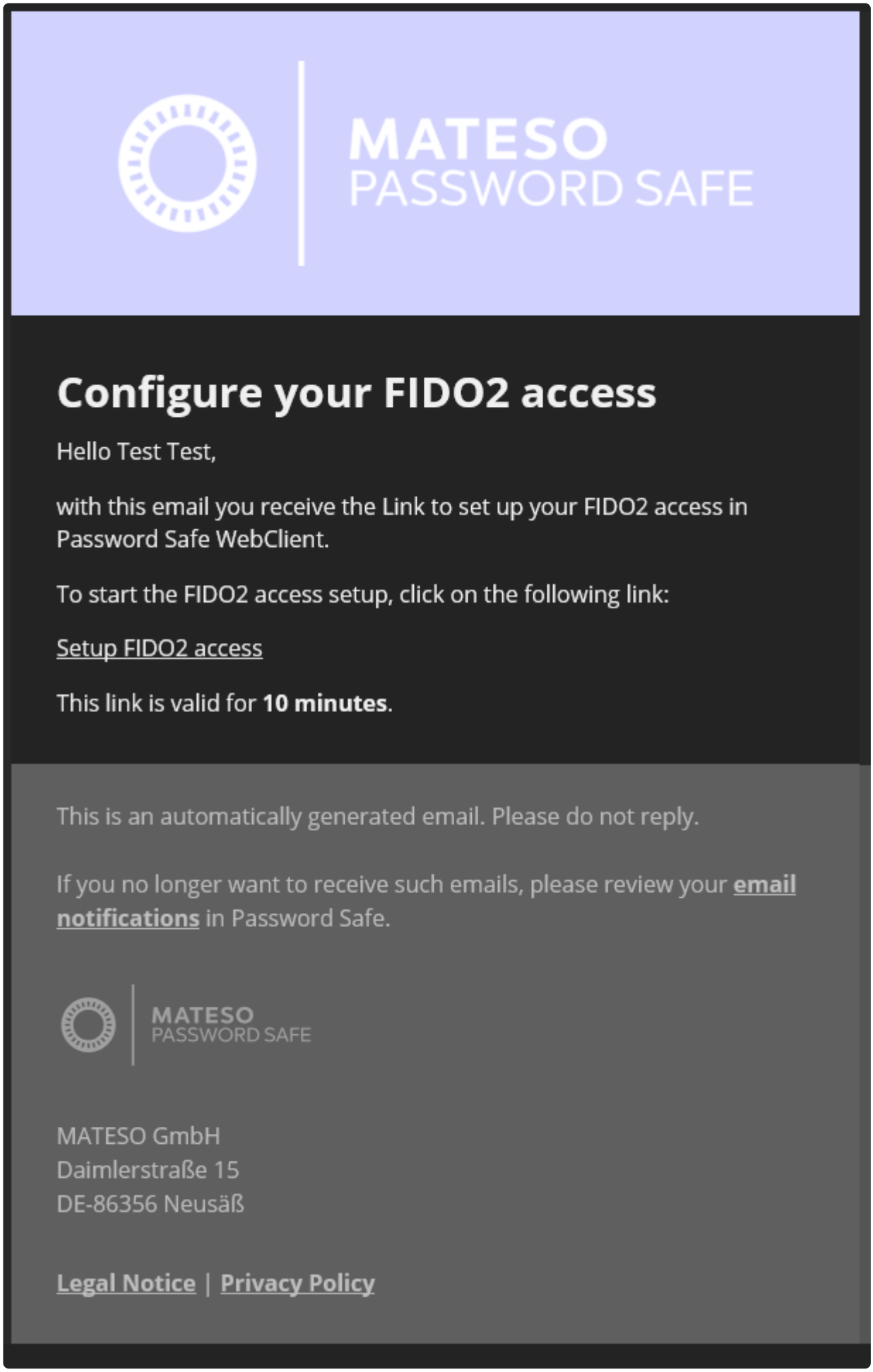
The configuration is done via the user setting **First Factor**.



As soon as an AD user logs on to the WebClient, he gets the following prompt:



In the email box of the corresponding user the further configuration takes place:


MATESO
PASSWORD SAFE
Configure your FIDO2 access
Hello Test Test,
with this email you receive the Link to set up your FIDO2 access in Password Safe WebClient.
To start the FIDO2 access setup, click on the following link:
Setup FIDO2 access
This link is valid for 10 minutes.
This is an automatically generated email. Please do not reply.
If you no longer want to receive such emails, please review your email notifications in Password Safe.
MATESO
PASSWORD SAFE
MATESO GmbH
Daimlerstraße 15
DE-86356 Neusäß
Legal Notice | Privacy Policy

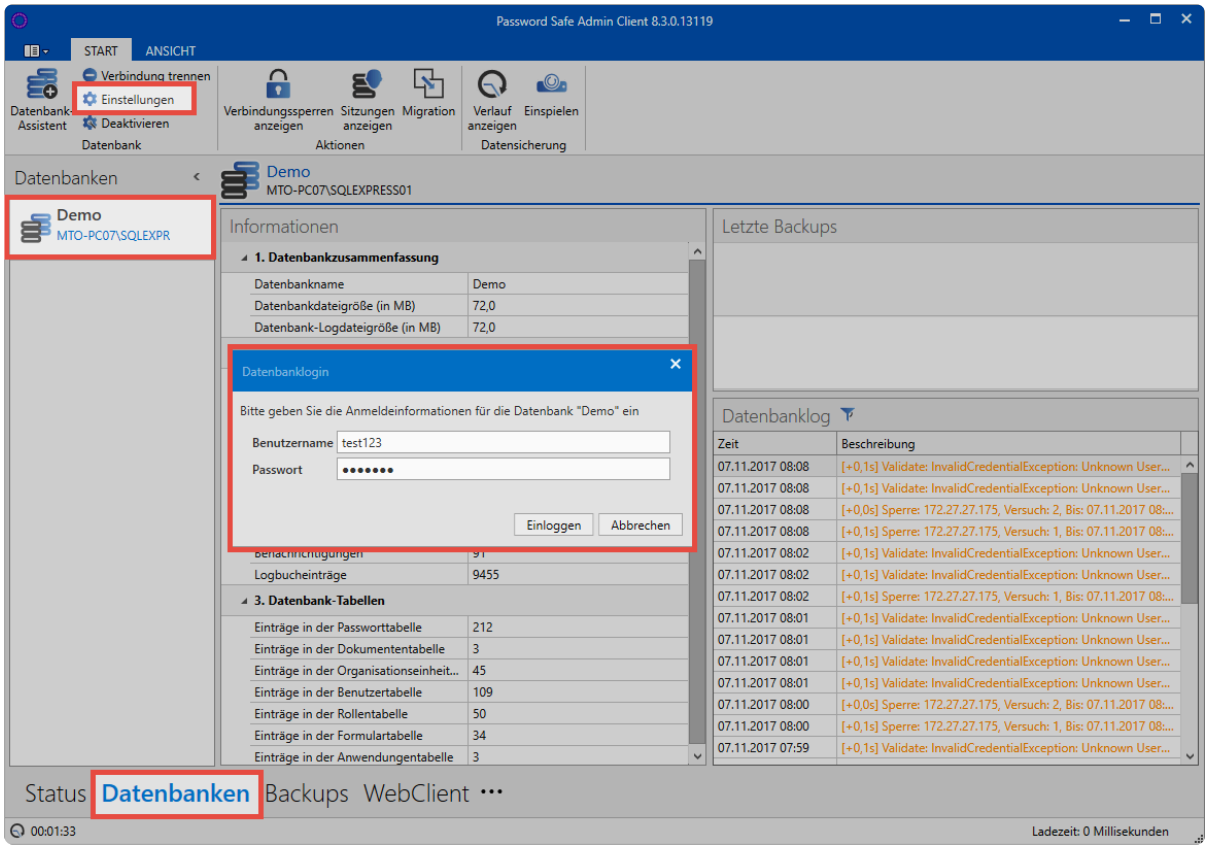
Multifactor authentication

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.



It is possible to separately define in the settings whether it is permitted to use each interface on the database.



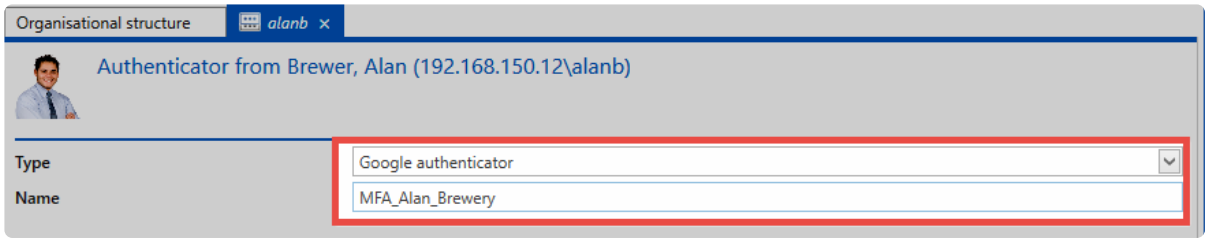
Other settings

In the user settings, it is also possible to define the “Length of validity of a multifactor authentication token” in minutes.

> In order for a user (administrator) to be able to **configure** multifactor authentication for **other users**, the user must have the rights **read**, **write**, **delete** and **authorize**. It is important that these rights exist before Multifactor Authentication is set up.

Configuration of multifactor authentication

In the organisational structure module, you select the user and the interface “Multifactor authentication” in the ribbon.



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

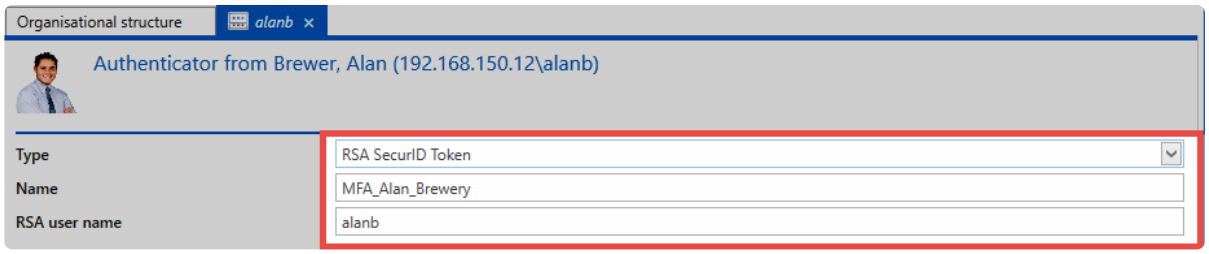
The prerequisite for this is that the relevant app has been started on a smartphone. After the name has been assigned for the authentication, you generate a new secret via the corresponding button. A QR code is displayed, which must be scanned using the Google Authenticator app on a smartphone.



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

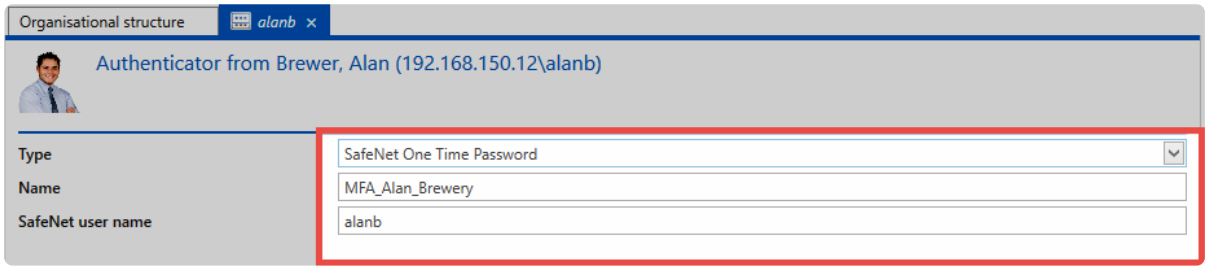
To set up multifactor authentication using RSA SecurID, simply enter the RSA user name and click **Create** directly in the ribbon.



> 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

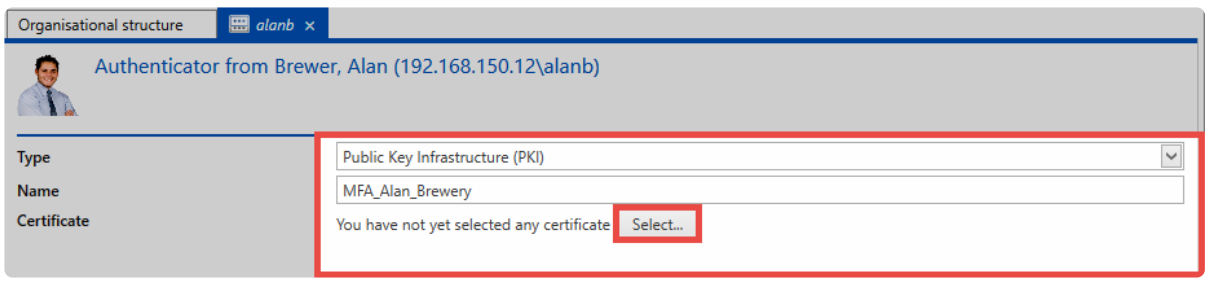
Multifactor authentication using SafeNet One-Time Password is set up using the SafeNet user name.



> 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.



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.

Delete Multifactor Authentication (MFA)

The multifactor authentication can be deleted by the user himself or by another user with sufficient authorization. The rights **Read**, **Write**, **Authorize** and **Delete** are required for another user to perform the deletion.

In order to delete a file, you should go to the main menu. Under **Account** you will find the item **Multifactor Authentication**. An alternative way is to enter the management of multifactor authentication via the organizational structure. To do so, select the corresponding user and click on the **Multifactor Authentication** ribbon.

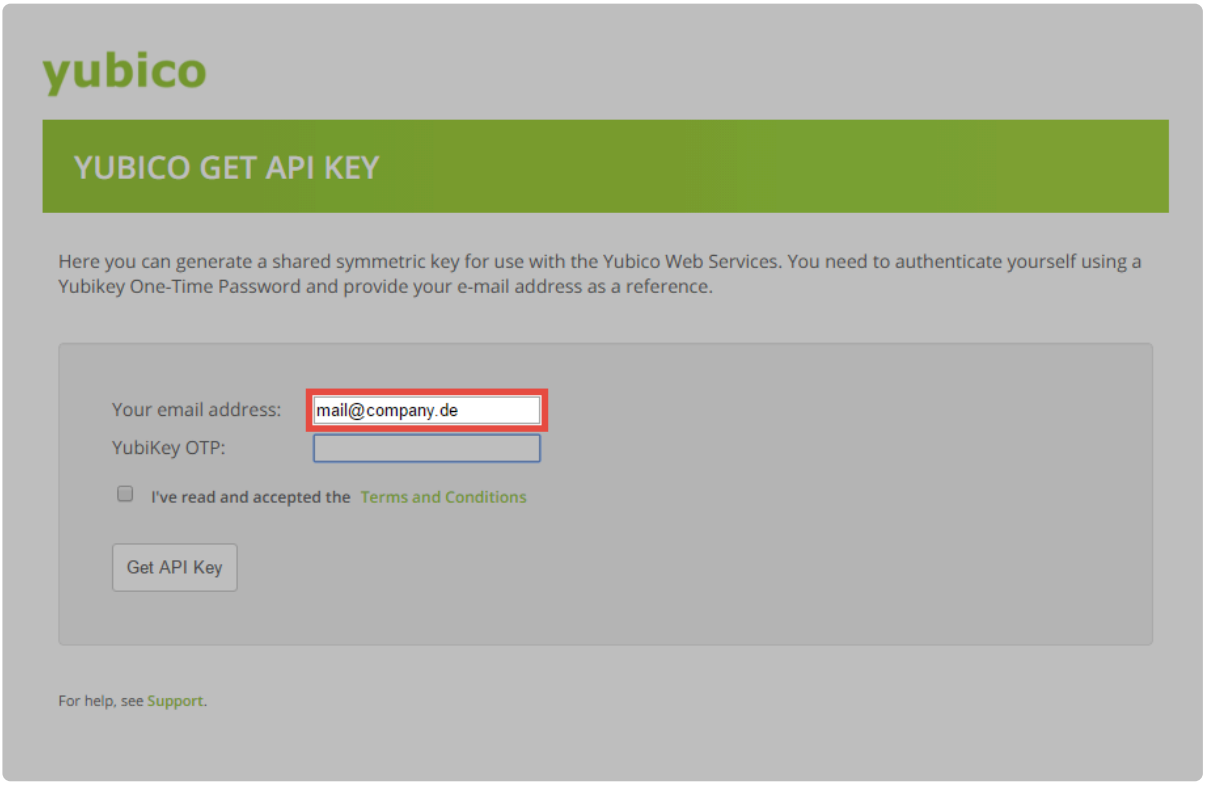
In the administration of the multi-factor authentication you will then find in the ribbon the possibility to delete the stored MFA.

Yubico / Yubikey

Setting up multifactor authentication

Requesting the Yubico API key

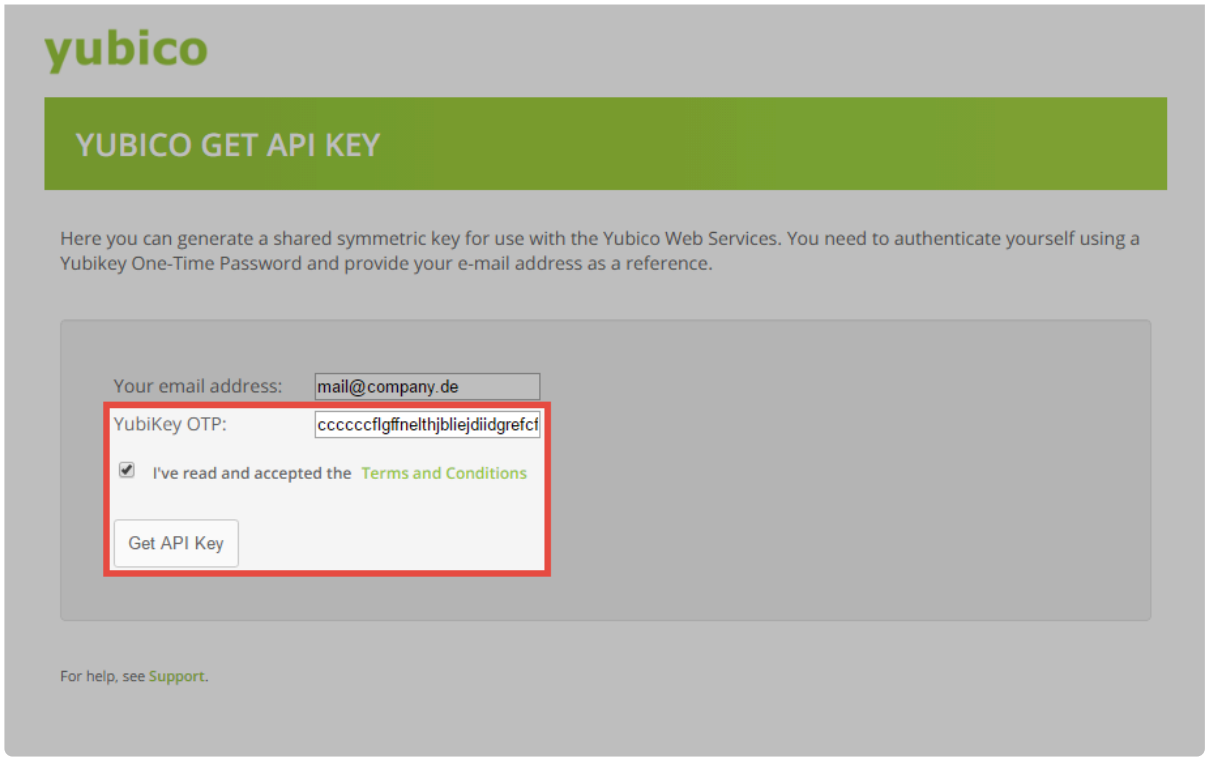
An API key must be requested for configuration. For this purpose, use the following link and enter an e-mail address: https://upgrade.yubico.com/getapikey/



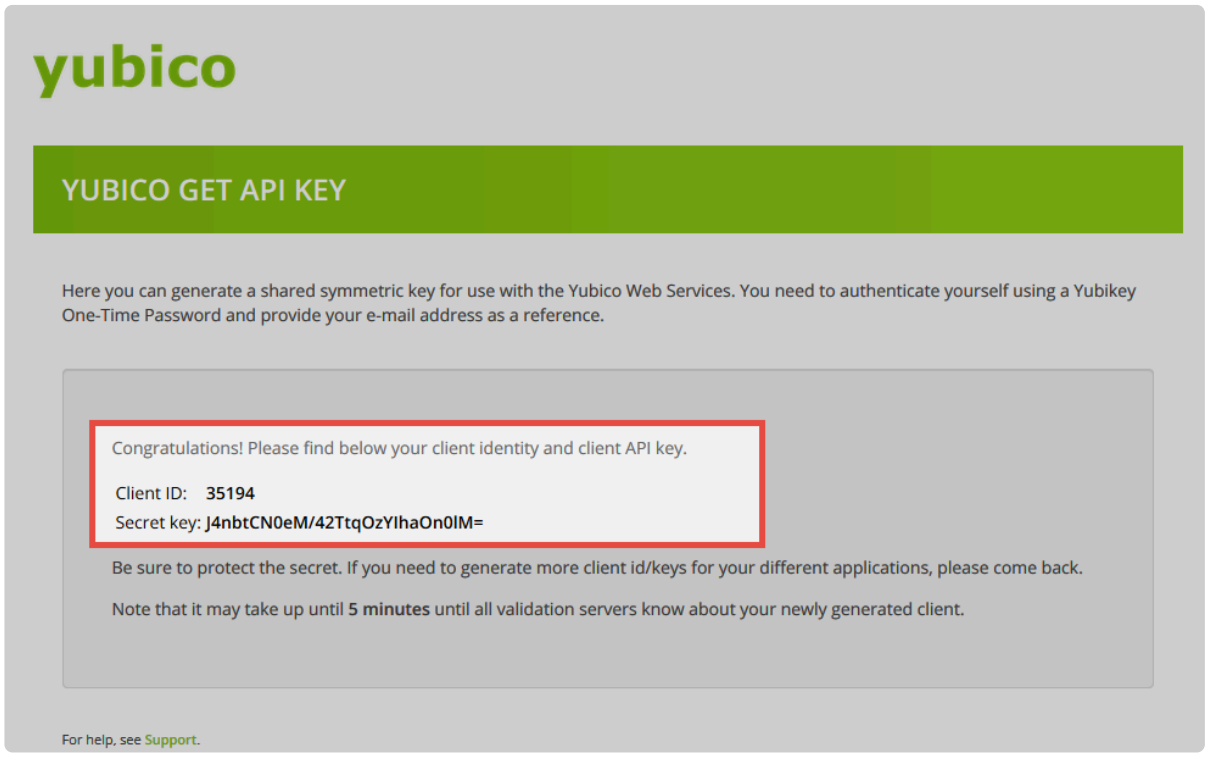
Yubikey will then generate a **One Time Password**. The Yubikey used must only be touched in the right place.



The **One Time Password** is entered directly into the corresponding field.

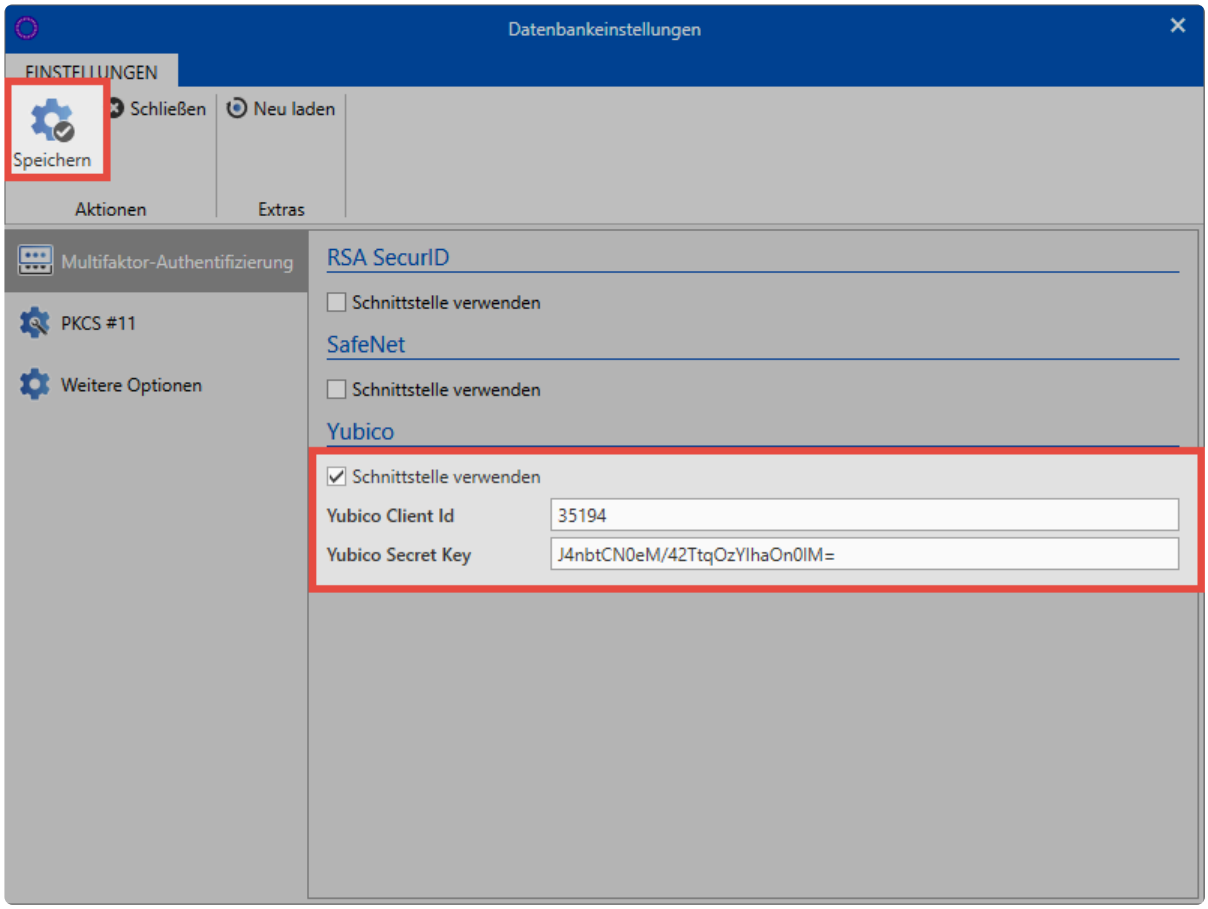


Once the general terms and conditions have been approved, the API Key can be requested.



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.

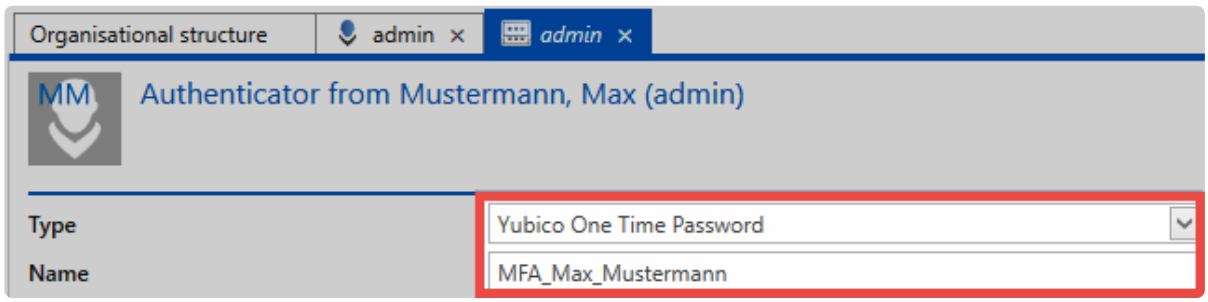


The interface is now ready and can be used.

> The HTTPS endpoint “https://api.yubico.com/wsapi/2.0/verify” is used for communication with Yubico. Please make sure that the Password Safe Server can connect to this endpoint.

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.

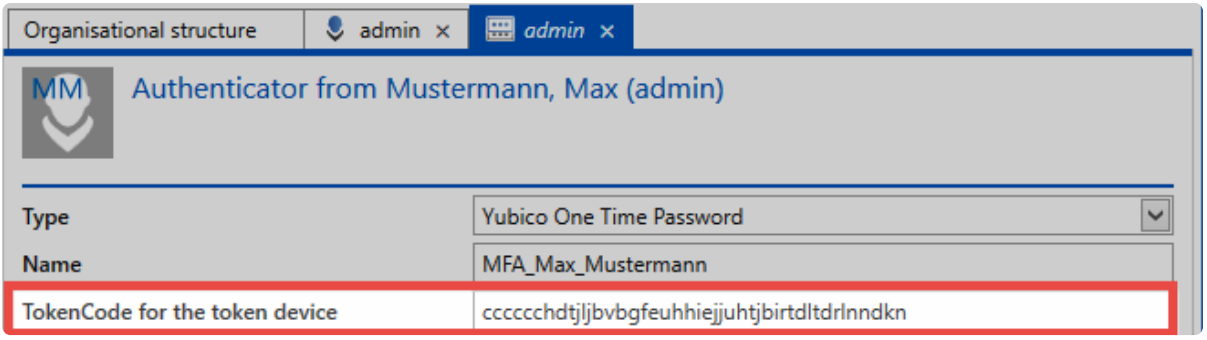


And then click on save. Now click in the field for the token and create a token using the Yubikey. For

Yubikey NEO, you only need to touch the touch panel. The same applies to **Yubikey Nano**.

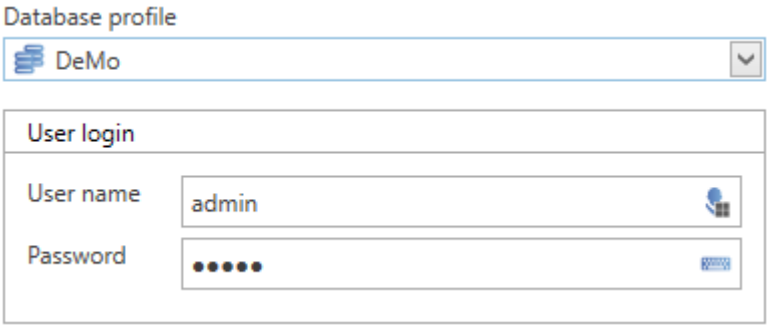


The token is entered directly into the corresponding field. The multifactor authentication is configured once you've clicked on save.

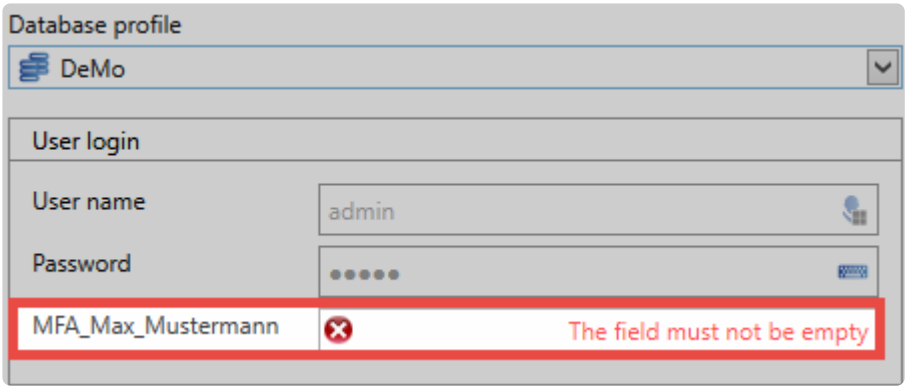


Logging in with the Yubikey

To login with Multifactor Authentication, the database is first selected and then **User Name** and **Password** are entered and confirmed.

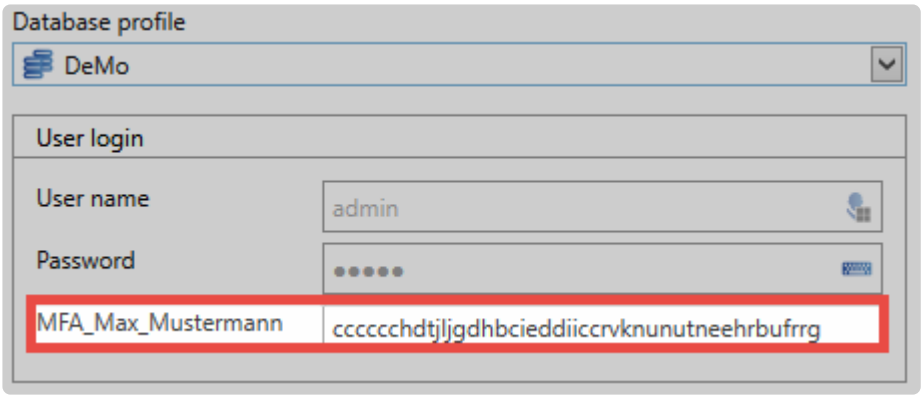


After the first password authentication, another field for the **One Time Password** is displayed.



Click on the field to highlight it, and enter the **One Time Password** by touching the Yubikeys.





The user is now logged on.

OTP (One-Time-Password)

Using OTP in Password Safe

A one-time password is a password that is valid once and can be used for authentication or transactions. Accordingly, each additional authentication or authorization requires a new one-time password.

Establishment

To set up OTP in Password Safe, proceed as follows.

1. Create form with OTP field

Create a new form or add an OTP field to an existing form:

2. Create password

You assign the new or customized form to existing passwords and edit them or create a new password with the new or customized form.

Next, the OTP field must be configured. For this purpose the key (secret) of the desired website/ application is stored in Password Safe:

As soon as the secret has been deposited and the password saved, the setup is complete.

OTP in HTML WebViewer and Emergency WebViewer

OTP in HTML WebViewer

- 1. Set up OTP
- 2. Create HTML WebViewer
- 3. Open the created HTML WebViewer

How to use the HTML WebViewer can be read in the chapter with the same name.

OTP in Emergency WebViewer

The special feature of the Emergency WebViewer is that the stored OTP secret is also displayed.

In order to use the One-Time-Password in the emergency WebViewer you have to proceed as follows:

- 1. Set up OTP
- 2. Emergency HTML WebViewer Export Task Create

- 3. Open the created emergency WebViewer

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 **Masking** is explained in a similar way to the other modules in one place.

Passwords Documents Organisational structure **Roles** Forms Notifications Logbook Applications Password reset ···

Relevant rights

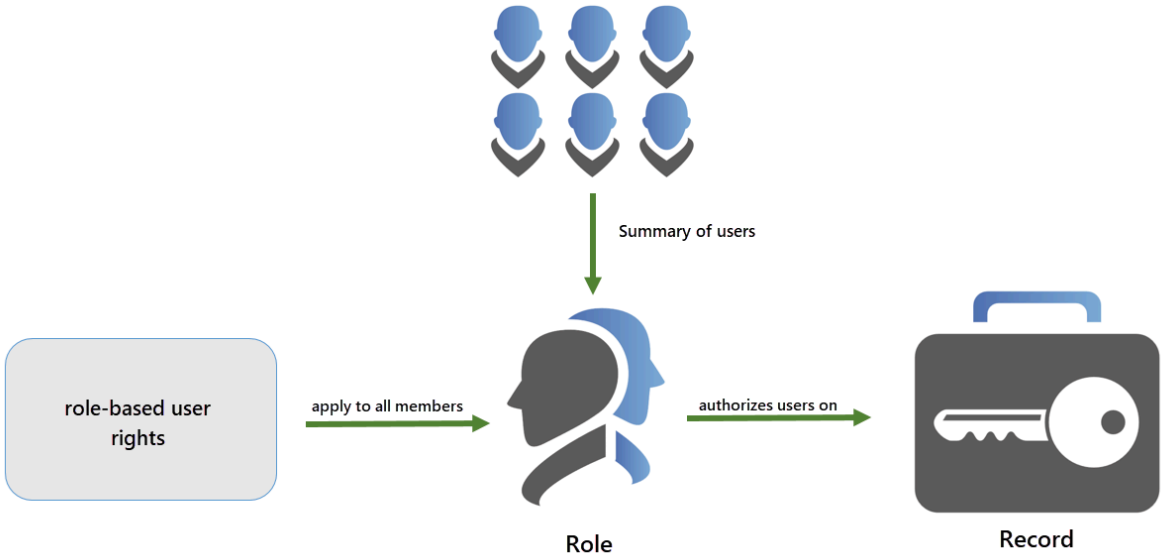
The following options are required.

User right

- Can add new roles
- Display role module

Roles in focus

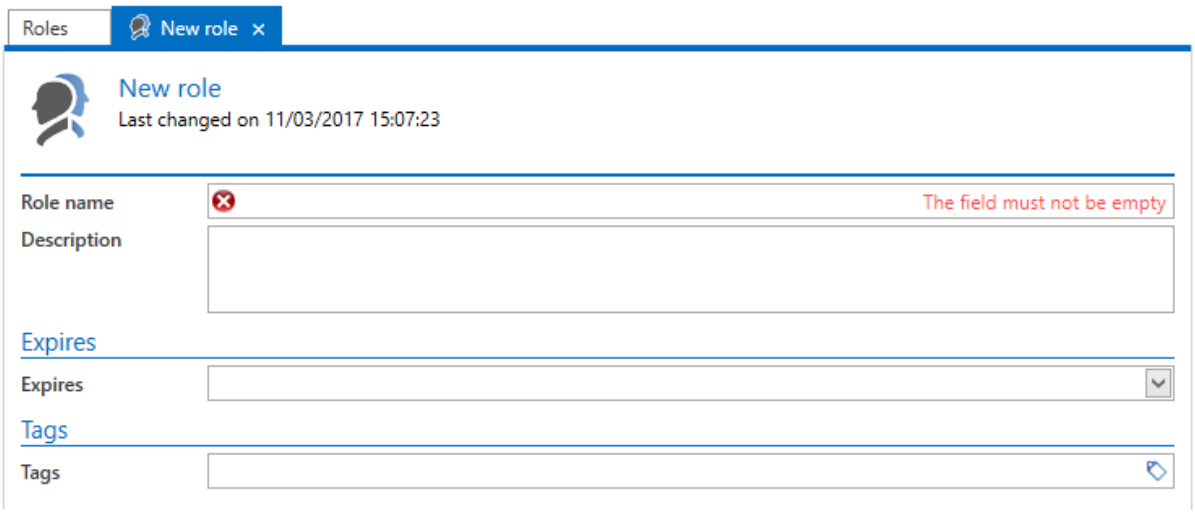
The configuration of roles is the basis for the authorization concept. Of course, the permissions for data could also be set at a user level. However, the use of roles can dramatically reduce the administrative burden, and it helps to keep an overview. In addition to the authorizations for data, user 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

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.



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?

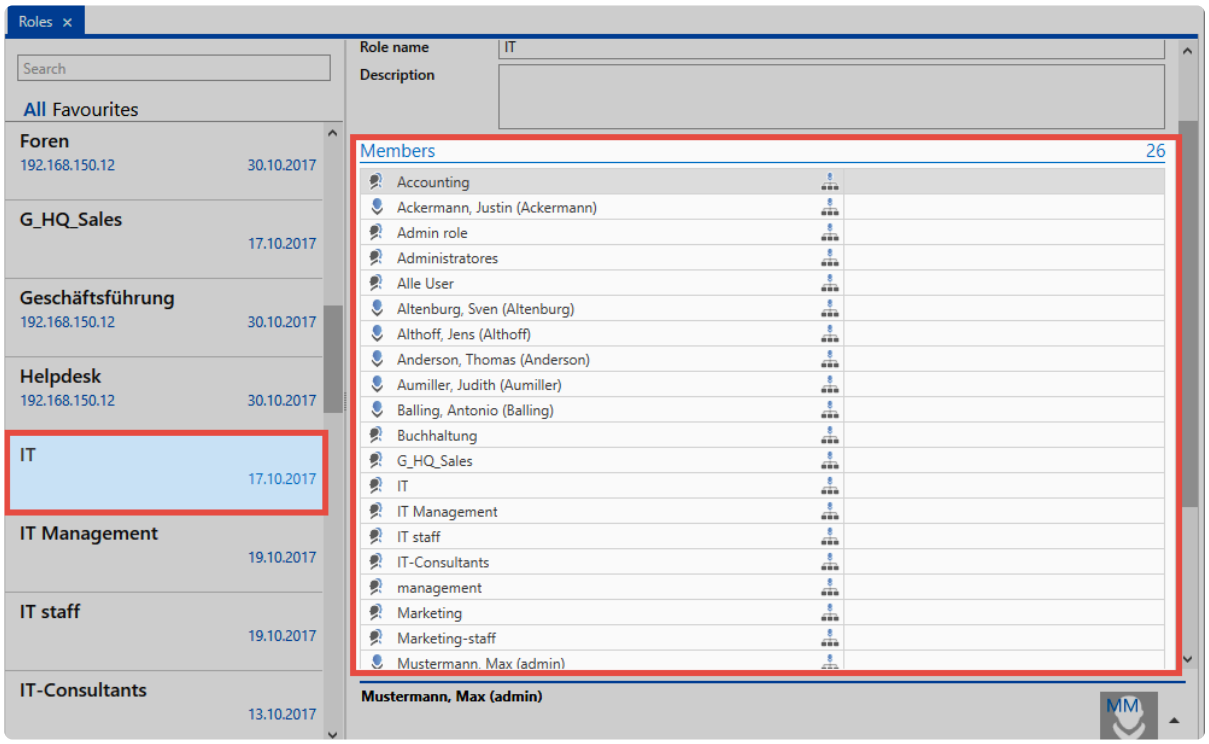
Password Safe enforces the avoidance of unnecessary structures through the role concept. A group-in-group nesting is not supported – and is not necessary at all. The resultant increase in performance as well as increased overview promotes efficiency and effectiveness. The elegant interplay of organisational 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.



The **roles** module is based on the WebClient module of the same name. Both modules have a different scope and design but are almost identical to use.

Forms

What are forms?

When creating a new data record, it is always indispensable to query all relevant data for the intended application. In this context, **Forms** represent templates for the information which have to be stored. The manageability of existing forms primarily ensures the completeness of the data which have 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 **Masking** is explained in a similar way to the other modules in one place.



Relevant rights

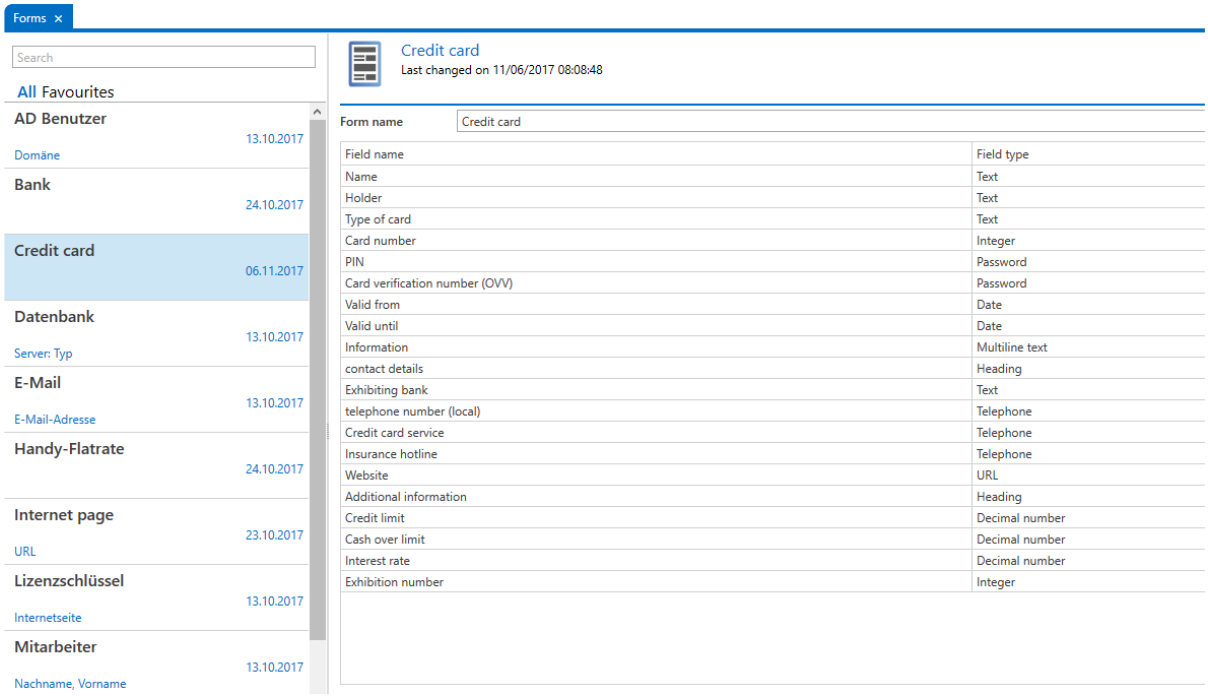
The following options are required to add new forms.

User right

- Can add new forms
- Display form module

Standard forms

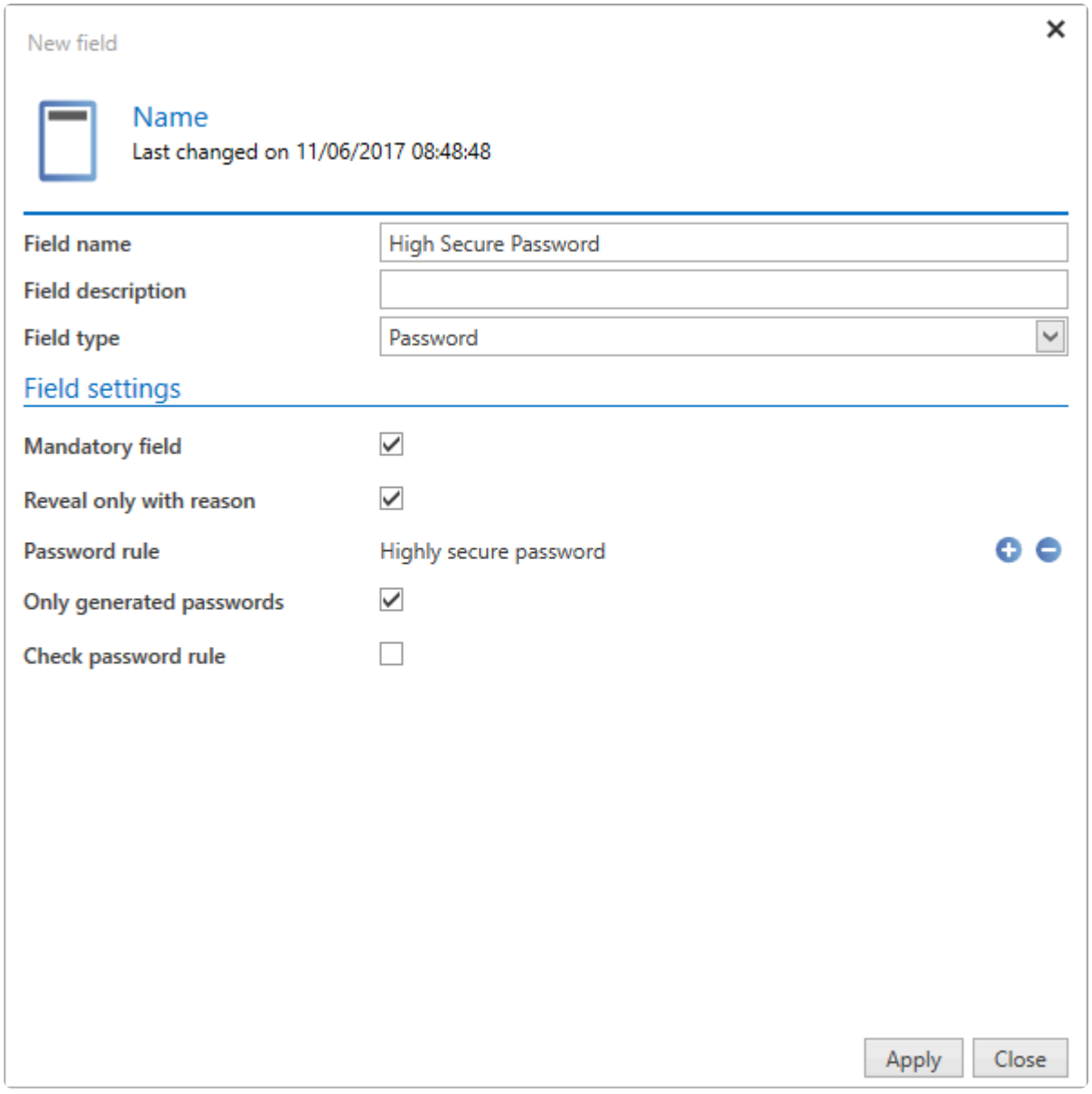
Password Safe is supplied with a series of standard forms – these should generally cover all standard requirements. Naturally, it is still possible to adapt the standard forms to your individual requirements.



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 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.



The following field settings thus appear for the field type “Password”: “Mandatory field, reveal only with reason, check only generated passwords and password policy”. 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)

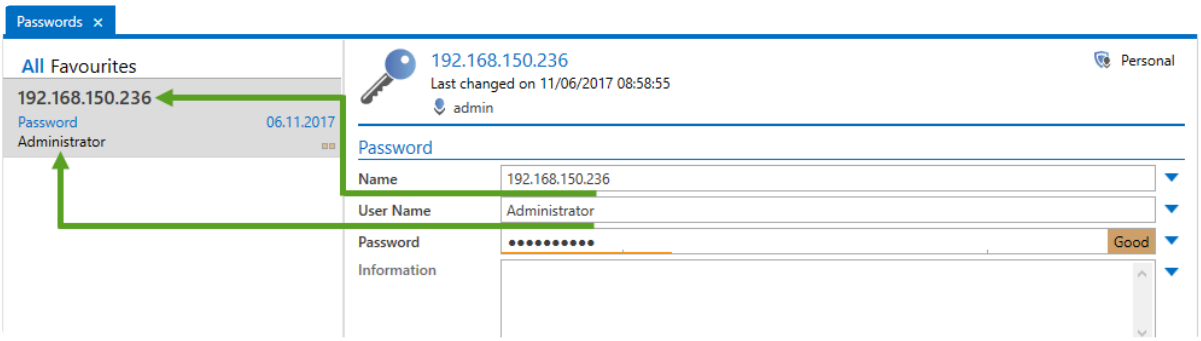
> ! If a form has been created, it can then be selected for use when creating new records. The prerequisite is that the logged-in user has at least read rights to the form.

Permissions for forms

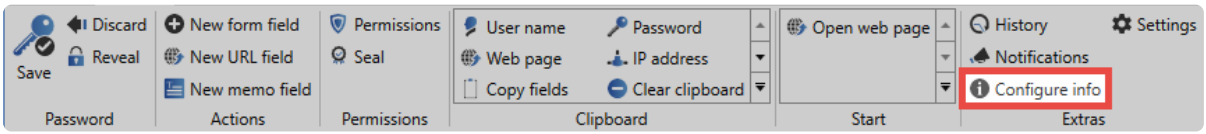
In the same way as for other objects (records, roles, documents,…), permissions can also be granted for forms. On the one hand, this ensures that not everyone can edit existing forms, while on the other hand, it allows you to make forms available to selective groups. This ensures that clarity is maintained 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

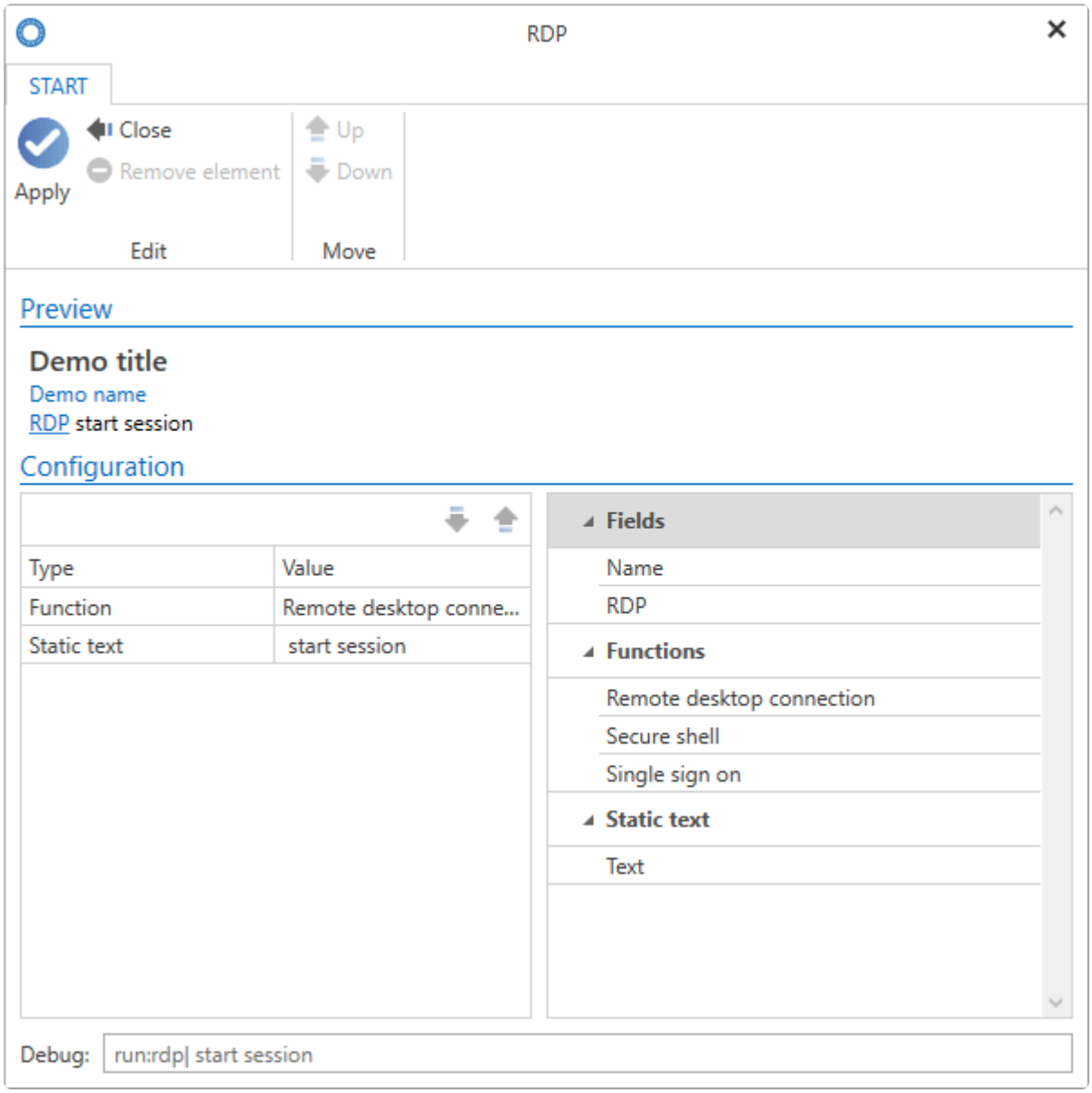
Every record displays other information underneath the obligatory name of the record in list view. In the following example, the user name is also displayed in addition to the name of the password. The name of the form is displayed in between in a blue font.



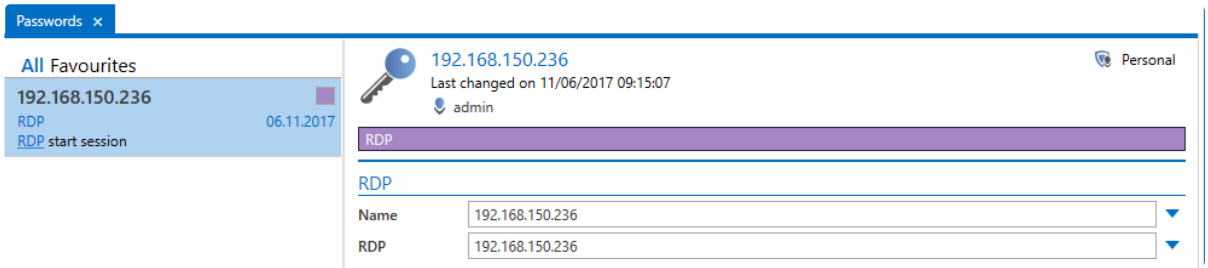
The name of the record (192.168.150.236) and the form (password) cannot be adjusted – these are always displayed. The user (Administrator) that is still saved for the record is currently displayed. This can be configured in the info field for the form. It is thus possible to separately define for each 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 which has 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.



The info field for the form is now updated. It is now possible to start the RDP session directly in the RDP session.



> The **forms** module is based on the WebClient module of the same name. Both modules have a different scope and design but are almost identical to use.

Standard form

There are two possible ways to define a standard form.

Via the “standard form” user setting

- Screenshot

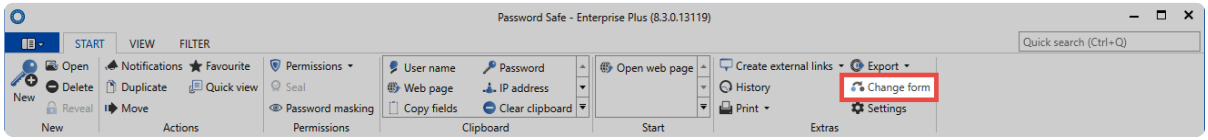
Via the form selection:

- Screenshot

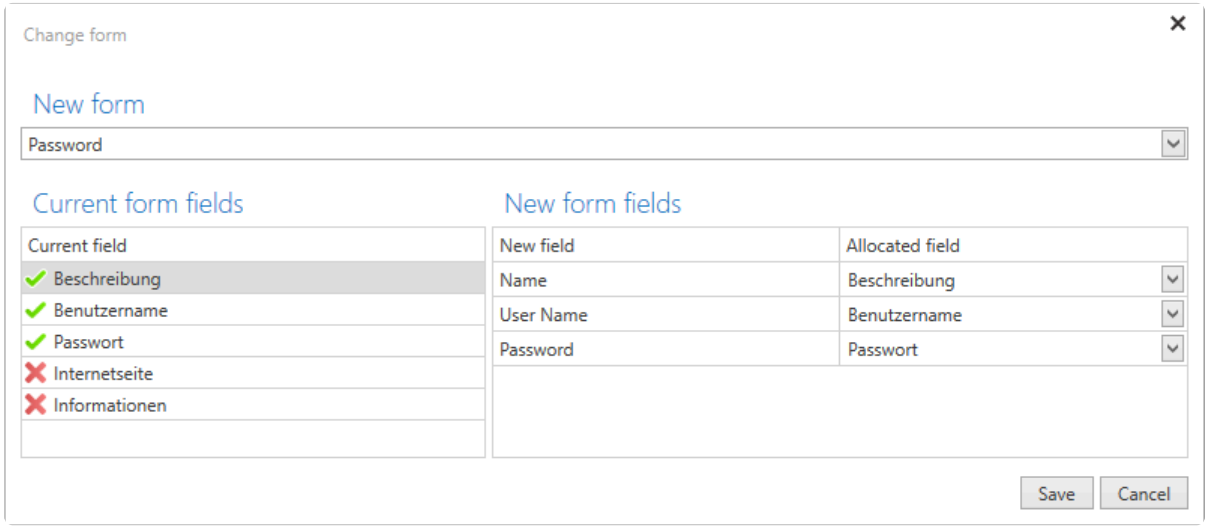
Change form

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).



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

Relevant rights

The following options are required to change forms.

User right

- Can change form for a password

! Please note that information could be lost during this process! In the example, this

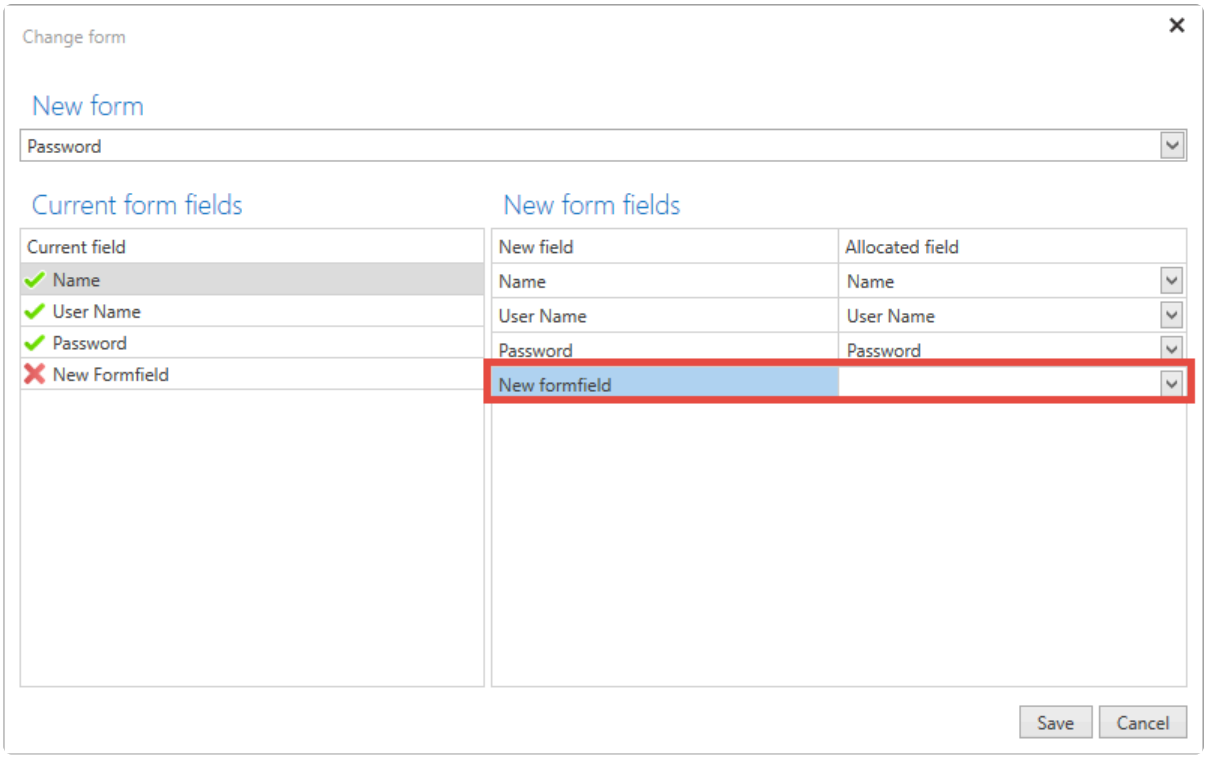
applies to the fields “Website” and “Information”.

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.



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”, “write” and “authorize” rights for the record (and the form to be edited) are required.
- 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 a logbook?

Password Safe logs all user interactions. These entries can be viewed and filtered via the logbook. The logbook thus records which user has made exactly what changes. This module is (theoretically) classified as uncritical. This is because the employee only has access to those logbook entries to which he is actually entitled. The configuration of **Masking** is explained in a similar way to the other modules in one place.

Passwords Documents Organisational structure Roles Forms Notifications **Logbook** Applications Password reset ···

Relevant rights

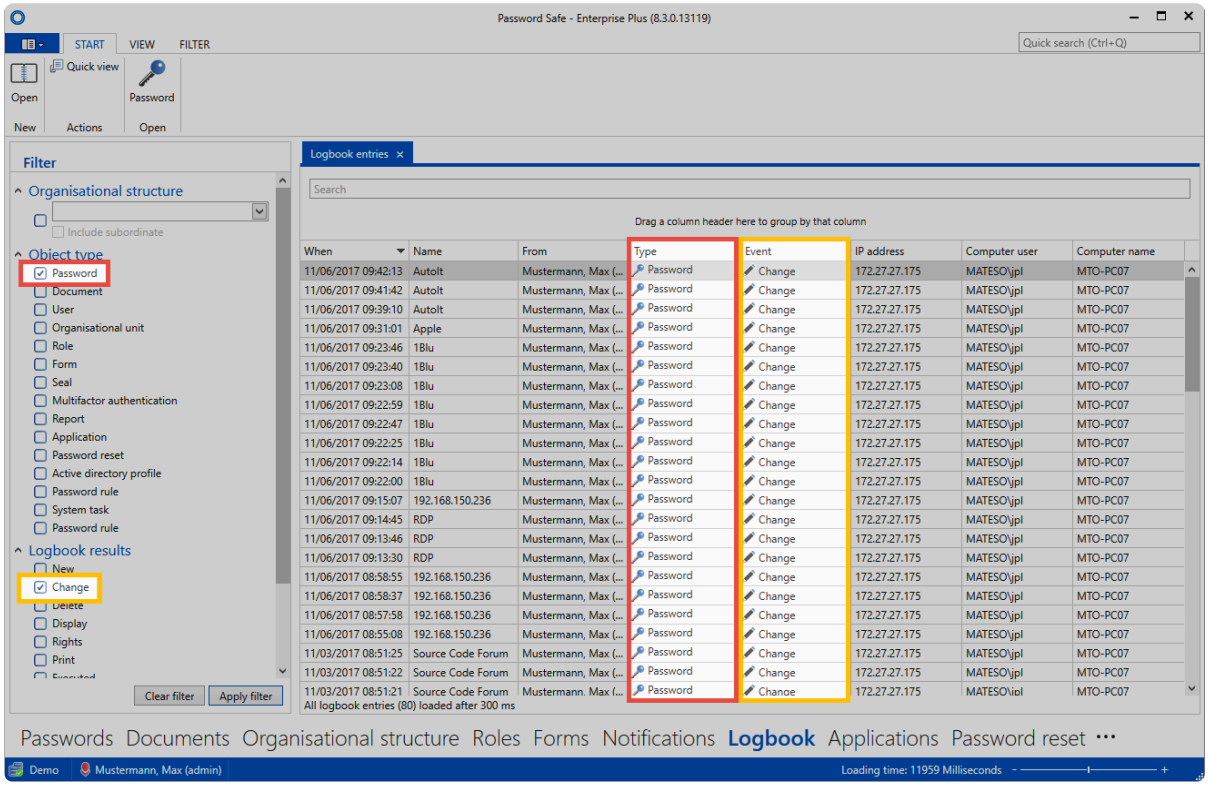
The following options are required:

User right

- Display logbook module

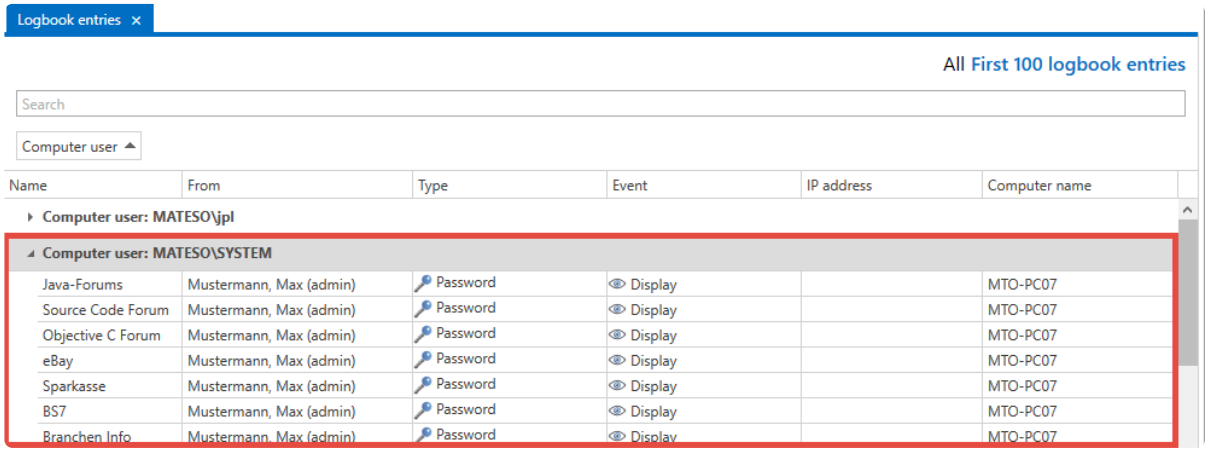
Use of the filter in the logbook

As is the case in all other modules, you can also use the filter in the logbook. This enables you 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.



Grouping in the logbook

This list can also be grouped together by dragging and dropping column headers – see the following grouping of the columns for **computer user**. The filtered results now show all changes to passwords carried out by the computer user “administrator”.



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. It is only by using this process that changes are completed in a traceable and audit-proof manner to prevent falsification.

> If desired, the logbook can be automatically cleaned up. This option can be configured on the **AdminClient**. Further information can be found in the section **Managing databases**.

Transferring to a Syslog server

The logbook can also be completely transferred to a Syslog server. Further information on this subject can be found in the section **Syslog**

Applications

What are applications?

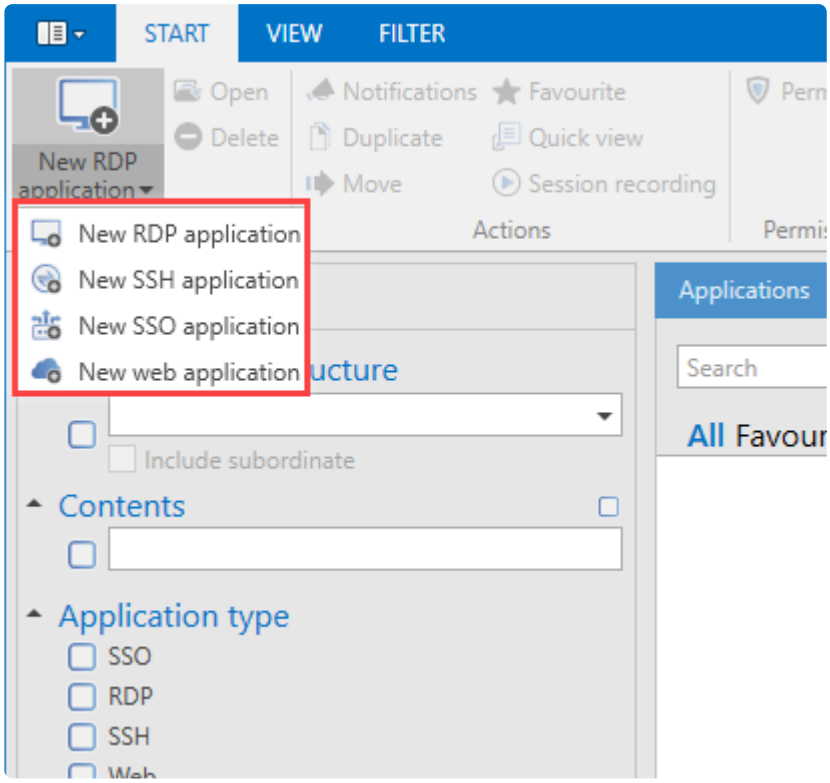
Applications can be used to configure automated logins to various systems. Especially when combined with various protective mechanisms, the company thus benefits in terms of security because complex passwords are automated and entered in the login masks in concealed form for the user. Various types are available, such as Remote Desktop (RDP), Secure Shell (SSH), general applications (SSO) and web applications. The Single Sign On Engine offers countless configuration options to enable automatic logon to almost any kind of software. The configuration of **Masking** is explained in a similar way to the other modules in one place.

Passwords Documents Organisational structure Roles Forms Notifications Logbook **Applications** Password reset ···

Automatic logins to websites are covered by the SSO agent.

The four types of applications

Password Safe varies between four different types of applications: RDP, SSH, SSO and web applications.

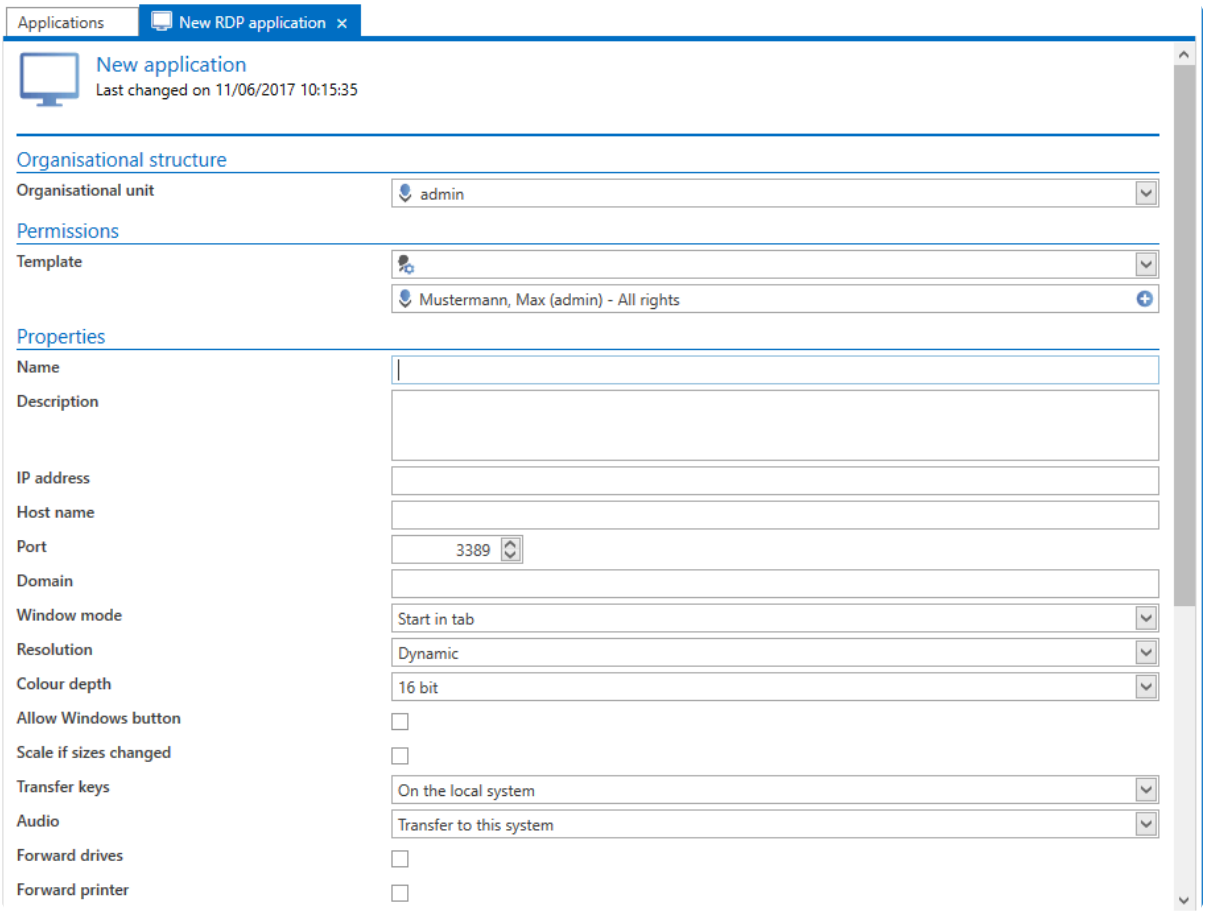


In terms of how they are handled, **RDP and SSH** applications can be covered together. Both types of application can be (optionally) “embedded” in Password Safe. The relevant session then opens in its own tab in the reading pane. All other forms of automatic logins are summarised in the **SSO applications** and **web applications** categories. How exactly these logins are created and used is

covered in the next section and in the ‘web applications”:#anwendungen-erfassen chapter. 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

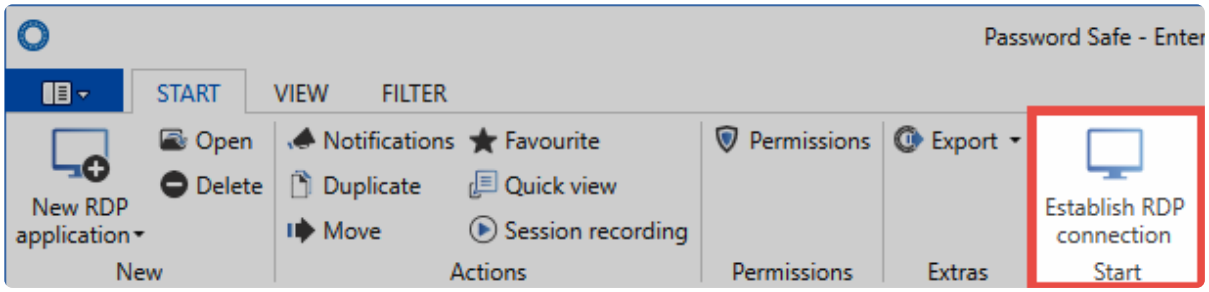
A new RDP/SSH application can be created via the ribbon or also the context menu that is accessed using the right mouse button. A corresponding form opens in each case where the variables for a connection can be defined.



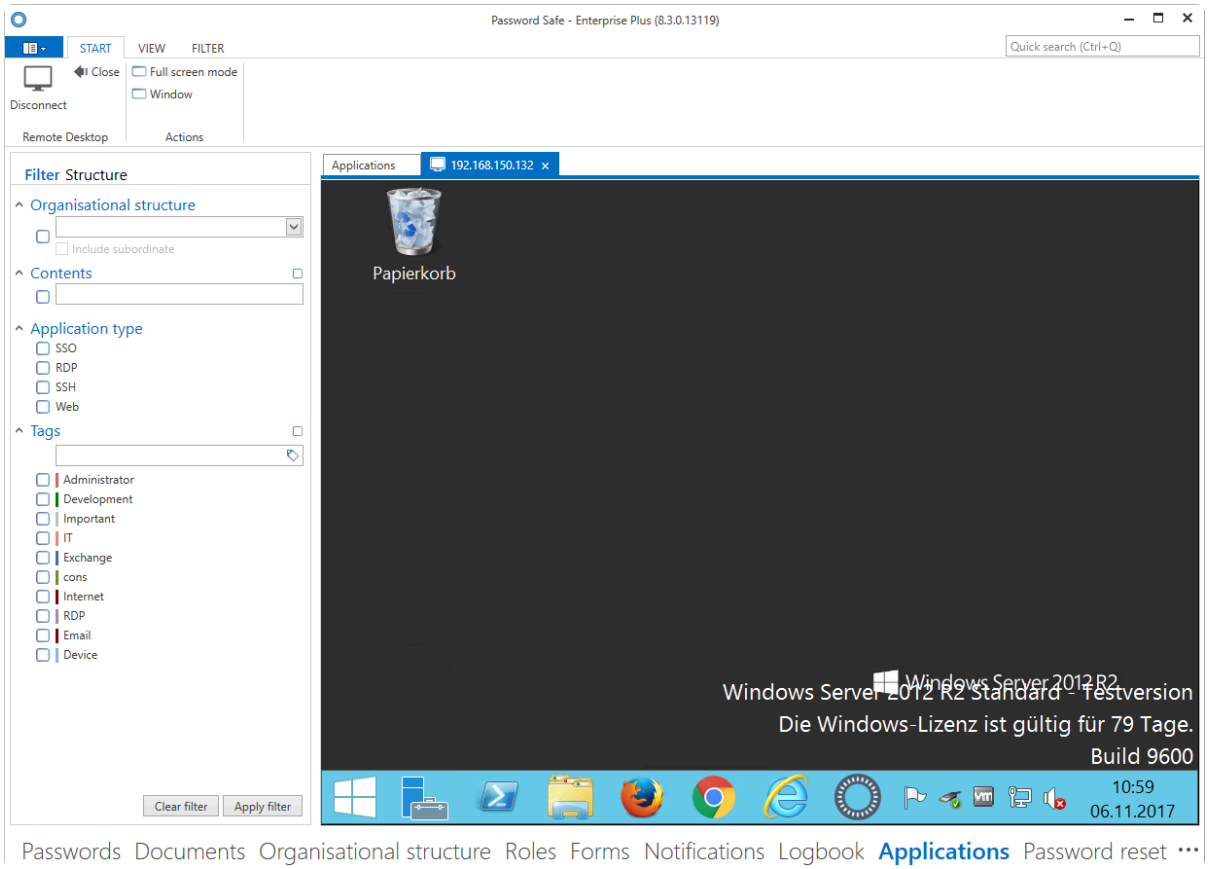
These variables also correspond precisely to those (using the example of RDP here) that can be configured when creating an RDP connection via “mstsc”. Whether the connections should be started in a tab, full screen mode or in a window can be defined in the field **“window mode”**.

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):



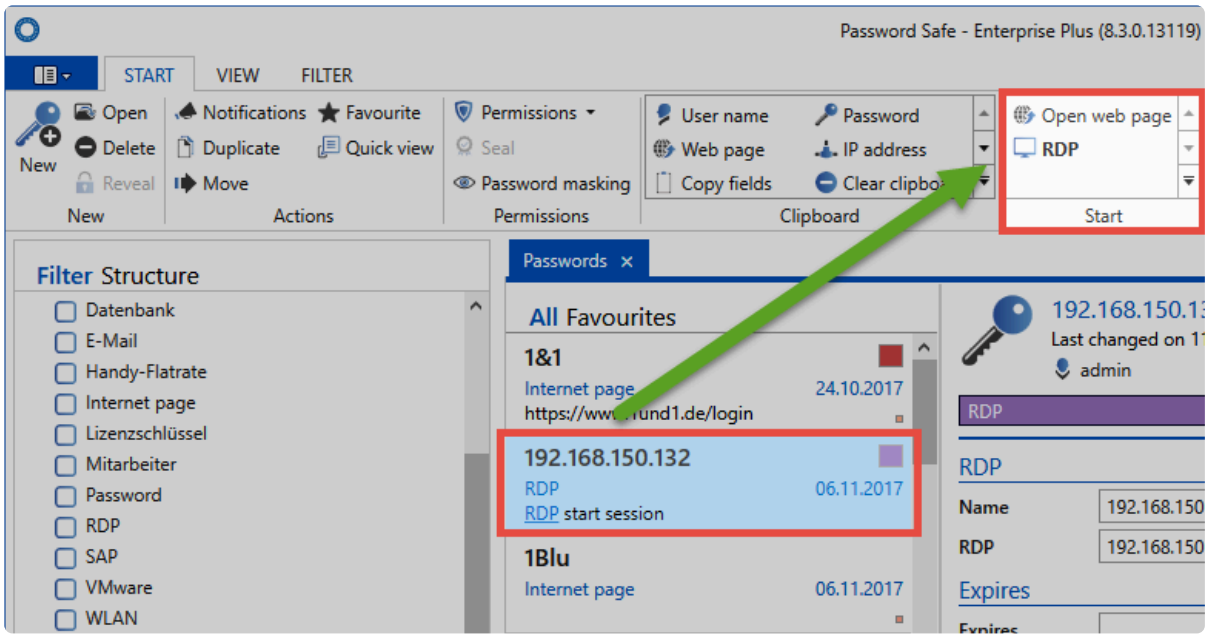
Logging in via SSH certificates

It is also possible to complete the authentication process using SSH certificates. For this purpose, the certificate is saved as a document in .ppk format. (It may be necessary to firstly approve this file ending in the settings). The document is then linked to the record via the footer. The record does not need to have a password. However, it is necessary for the record to be linked to a SSH 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,

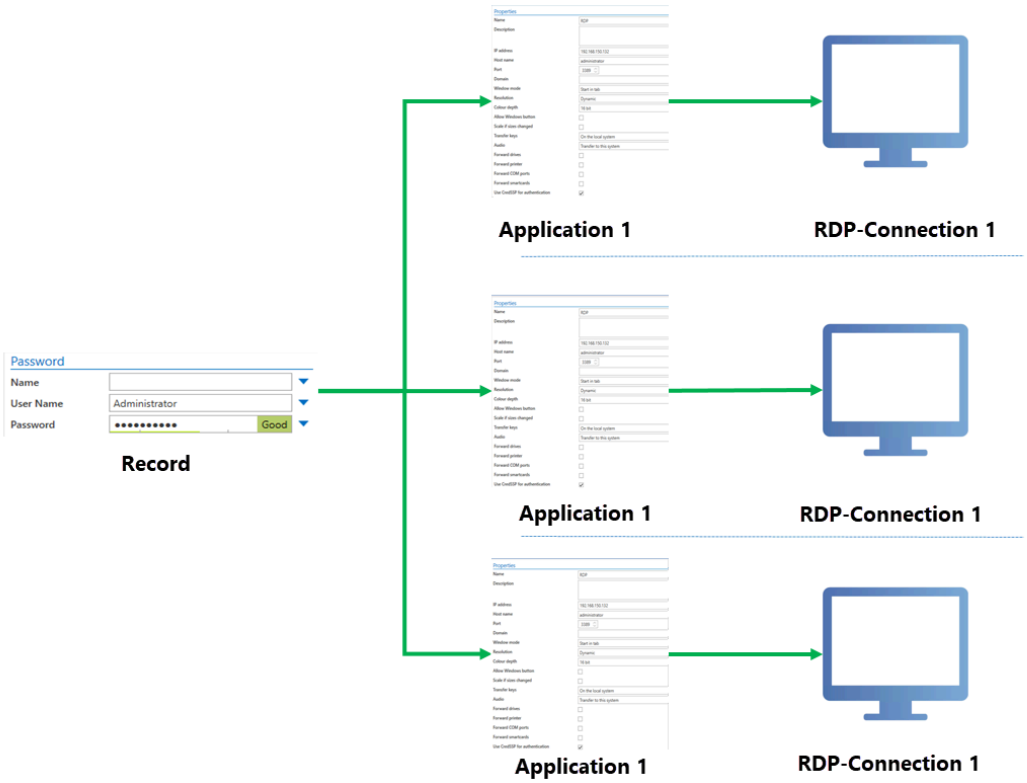
a 1-click login to the target system is possible.



The following example illustrates this process using an RDP connection:



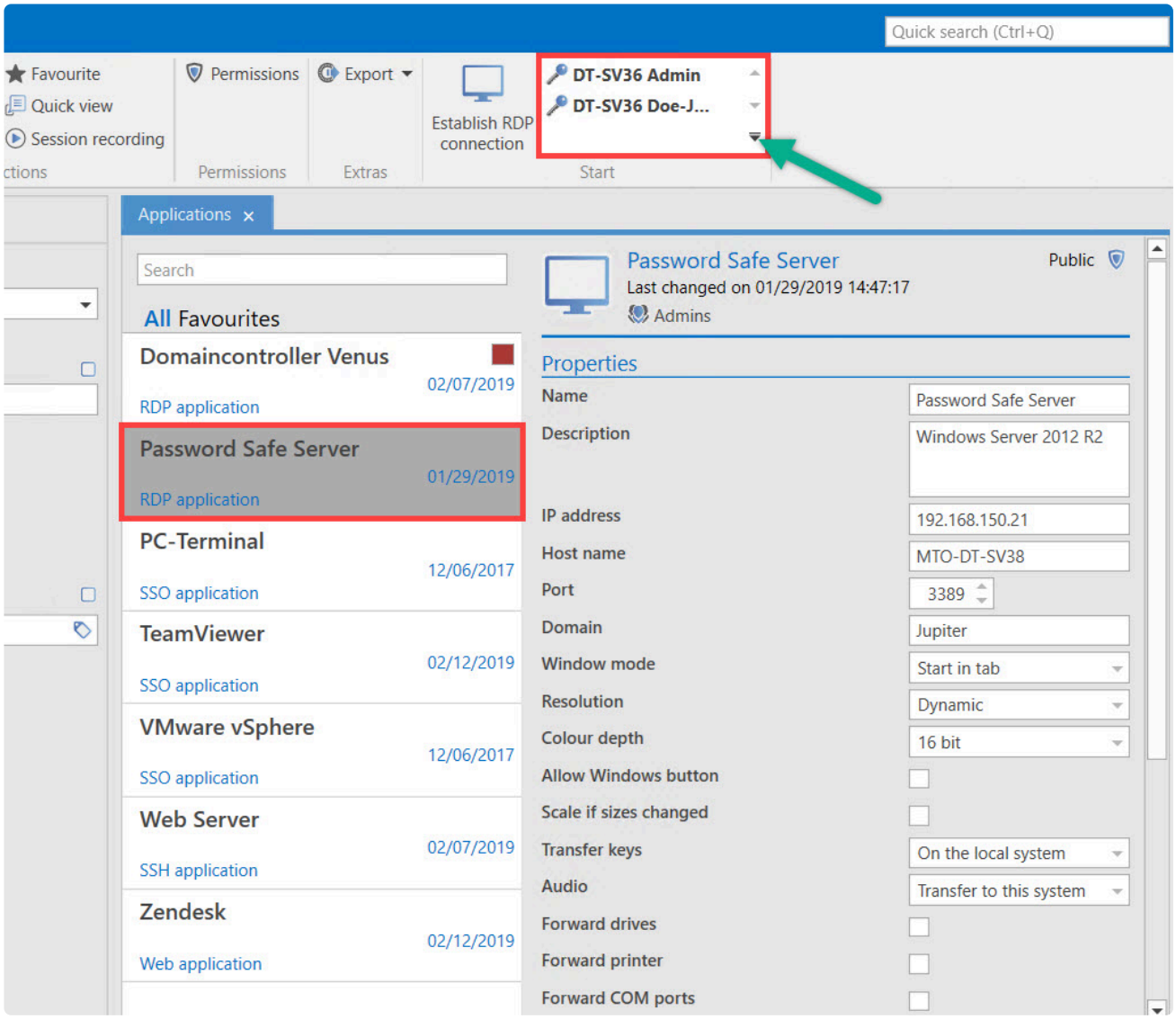
A record can also be linked to multiple target systems in this manner. The user name and record are supplied by the record, while all other information necessary for the login is supplied by the different applications. In the following example, a record (user name and password) is linked to multiple 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.

Alternatively, it is possible to connect several records with one RDP connection.
In this way, you can combine different users with an RDP connection and register them straightforward.


Quick search (Ctrl+Q)
Favourite
Quick view
Session recording
Permissions
Export
Establish RDP connection
DT-SV36 Admin
DT-SV36 Doe-J...
Permissions
Extras
Start
Applications
Search
All Favourites
Domaincontroller Venus
02/07/2019
RDP application
Password Safe Server
01/29/2019
RDP application
PC-Terminal
12/06/2017
SSO application
TeamViewer
02/12/2019
SSO application
VMware vSphere
12/06/2017
SSO application
Web Server
02/07/2019
SSH application
Zendesk
02/12/2019
Web application
Password Safe Server
Last changed on 01/29/2019 14:47:17
Admins
Public
Properties
Name
Password Safe Server
Description
Windows Server 2012 R2
IP address
192.168.150.21
Host name
MTO-DT-SV38
Port
3389
Domain
Jupiter
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

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”.

Relevant rights

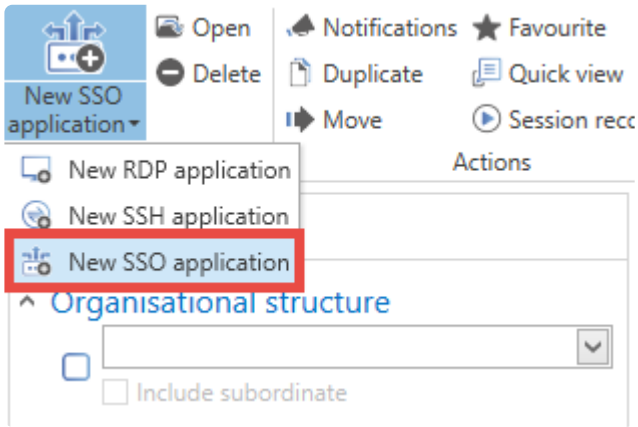
The following options are required.

User right

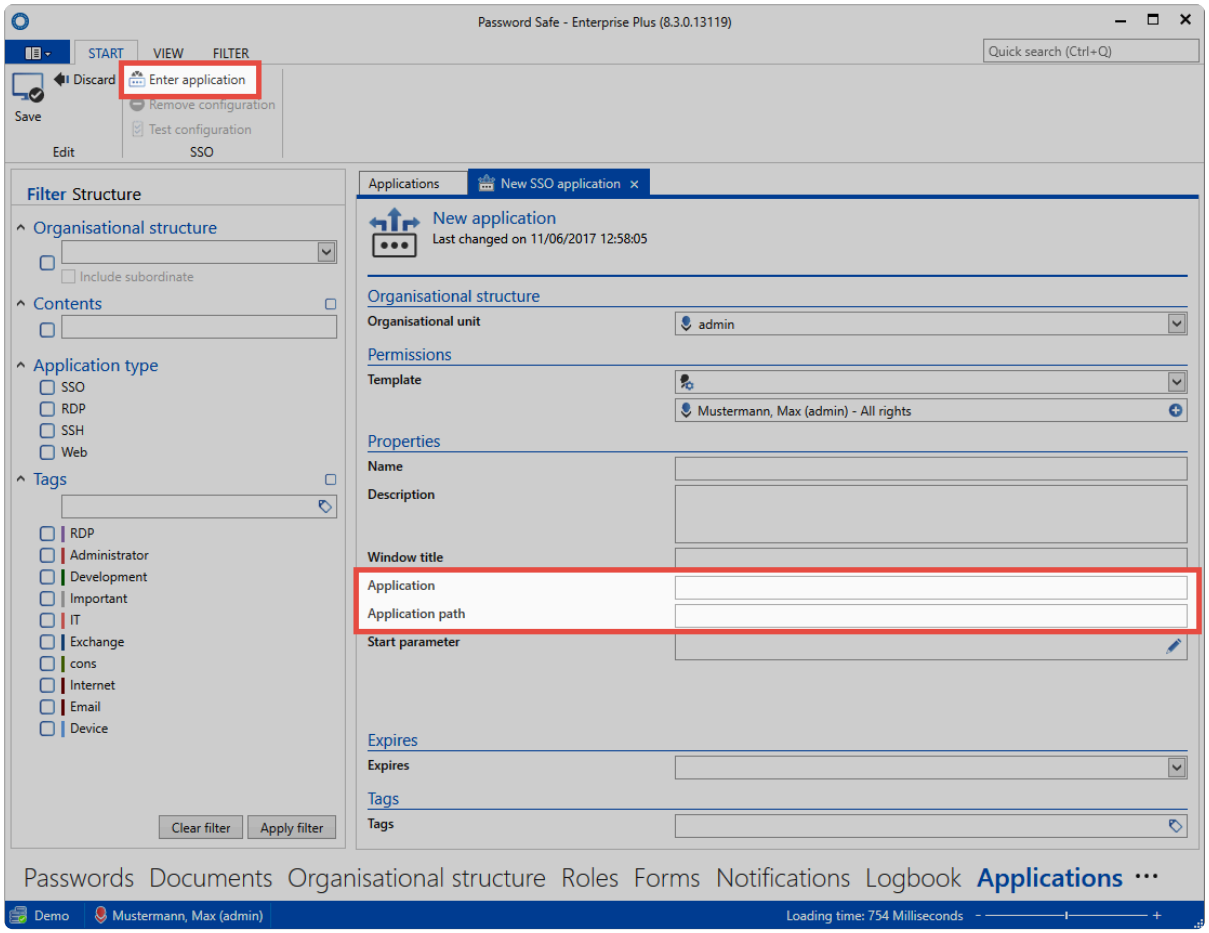
- Can add new RDP applications
- Can add new SSH applications
- Can add new SSO applications
- Can add new web applications

Configuration

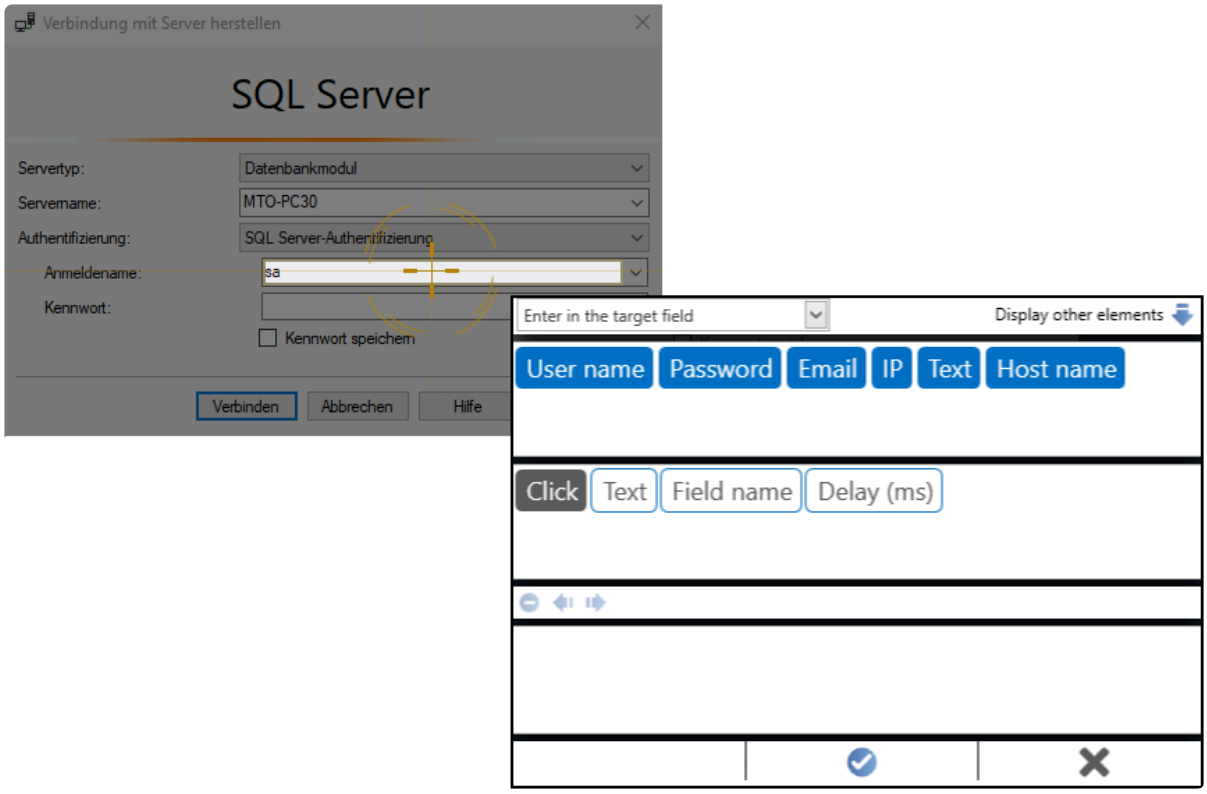
First, a new SSO application is created via the ribbon.



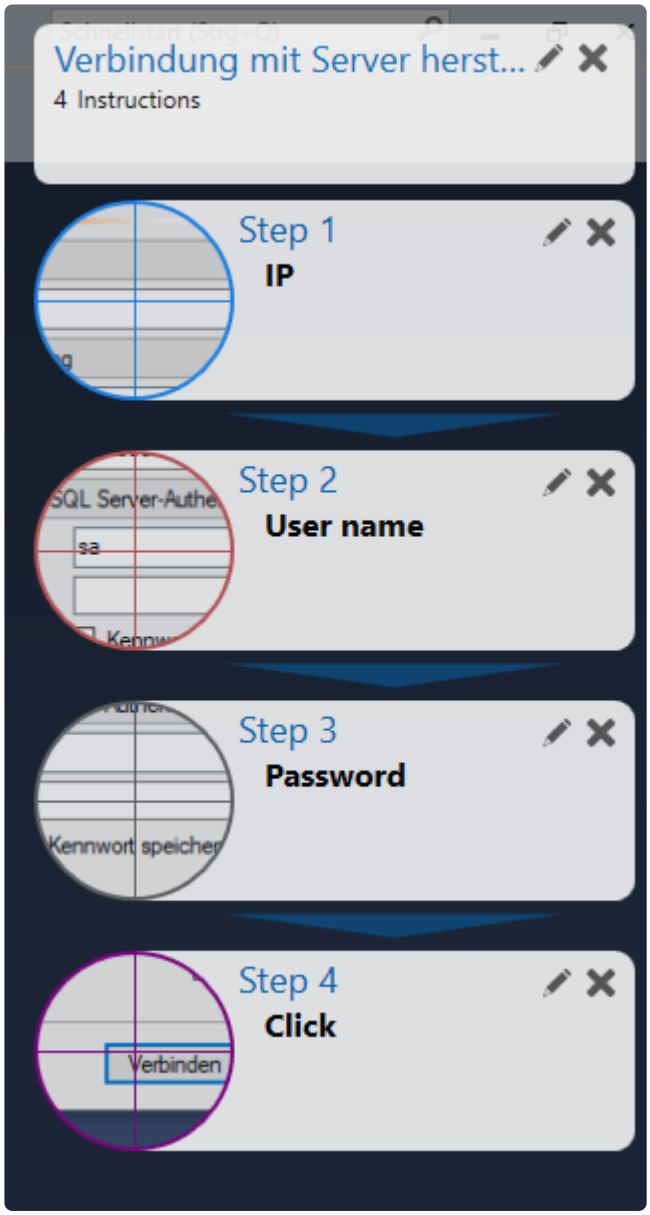
Various properties for the application can now be defined in the tab that opens. The fields **Window title**, **Application** and **Application path** are not manually filled. This is done via the **Create application** button in the ribbon:



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.

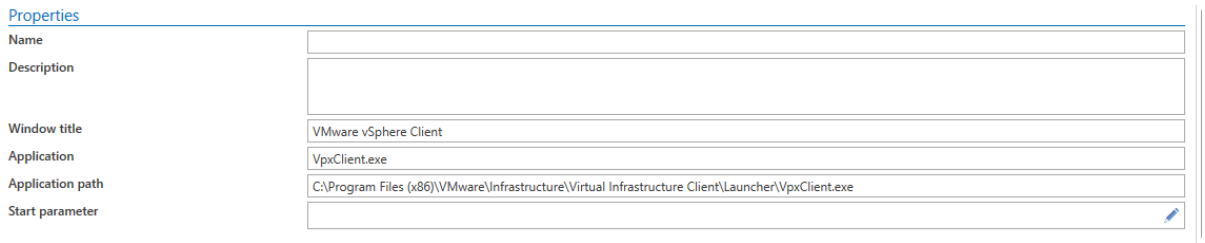


In parallel to the previous step, all of the already assigned fields will be displayed on the right edge of the screen. In this example, the VMware vSphere Client has a total of 4 assigned fields: IP, user name, password and clicking the button to subsequently confirm the login.



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.

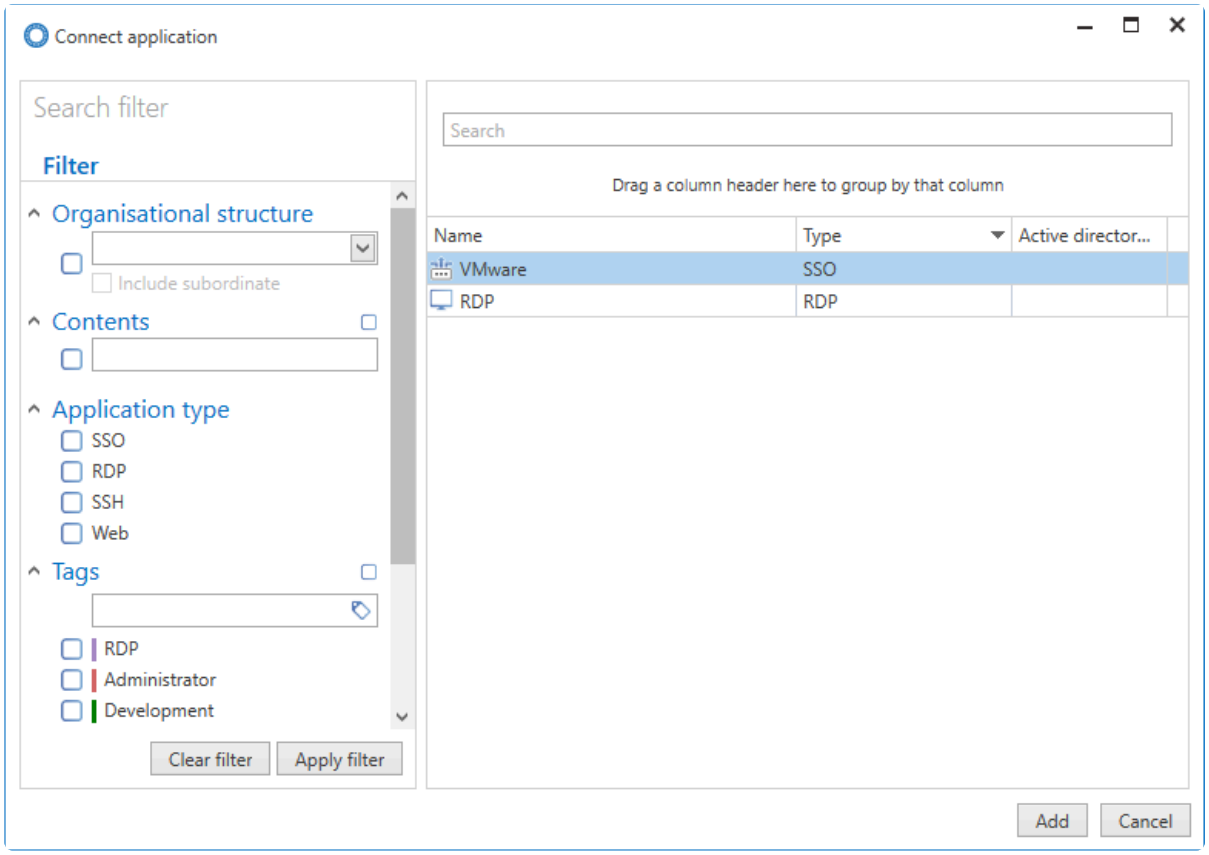
Once you have assigned all of the fields, you can exit the application process using the enter button. The fields “Window title”, “Application” and “Application path” mentioned at the beginning are now automatically filled.



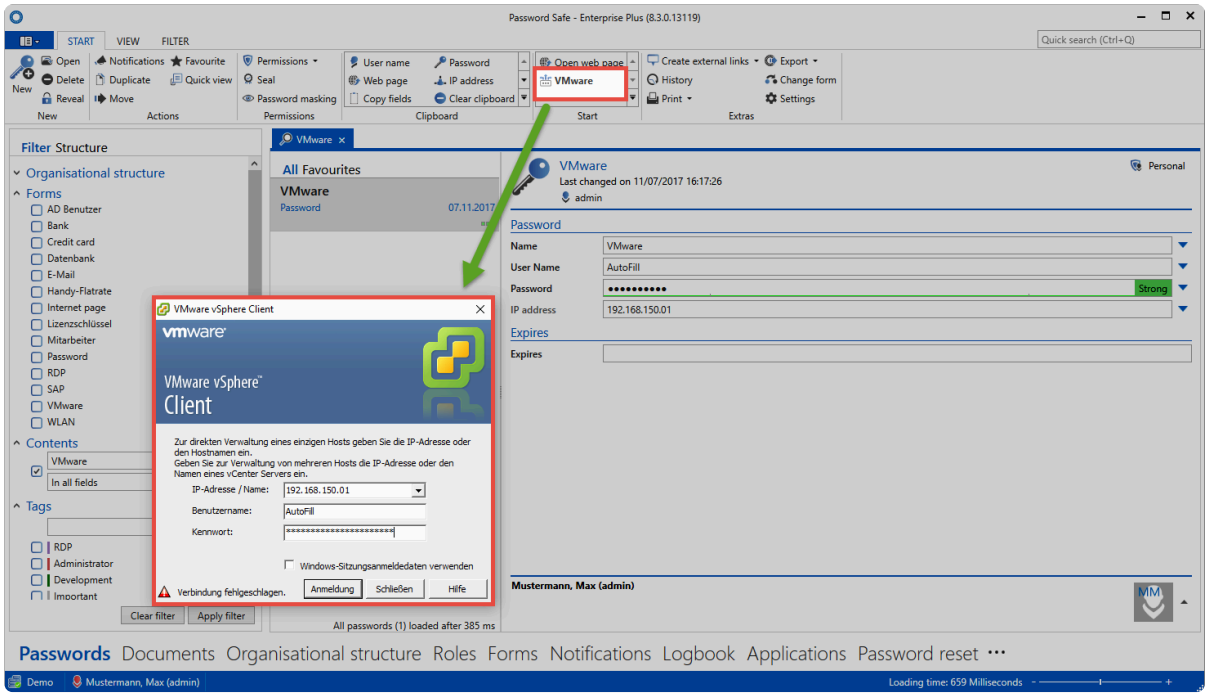
As you can see, the .exe file is directly referenced. If the application is saved to the same storage location for all users, it can then also be accessed by all other users.

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”.



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.



! 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.

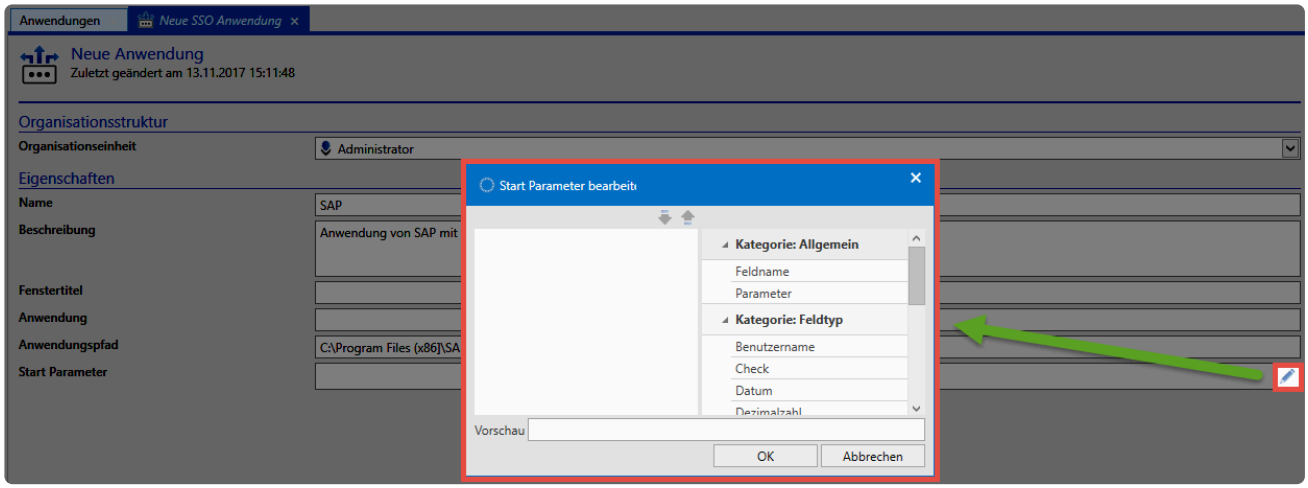
Start parameters

Start parameters for SSO applications

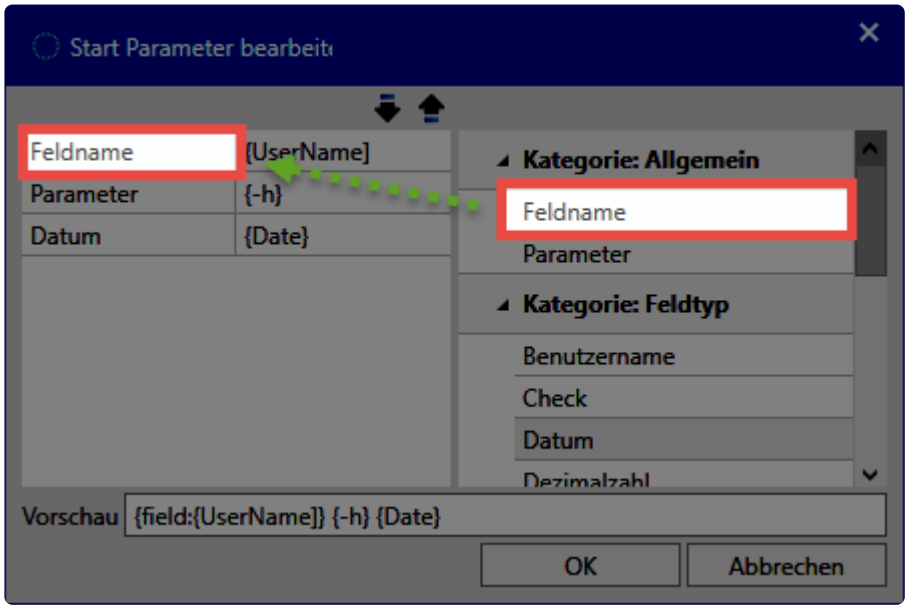
Start parameters can be defined when creating or editing an SSO application. These parameters are immediately transferred when starting the application. This is done, for example, to directly start the program with various basic settings. The corresponding parameters should be requested from the manufacturer 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.



Different categories are available here:

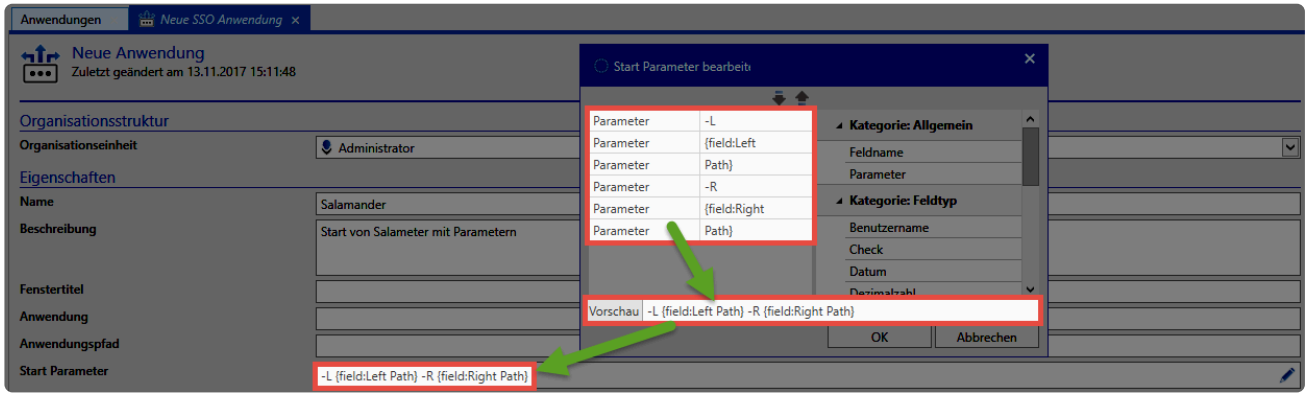
- In the **Parameter** category, only the parameter descriptions **Field name** or **Parameter** are available. These then need to be manually supplemented.
- The parameters in the **Field name** category can directly address the fields, meaning directly transfer the field names.

Example

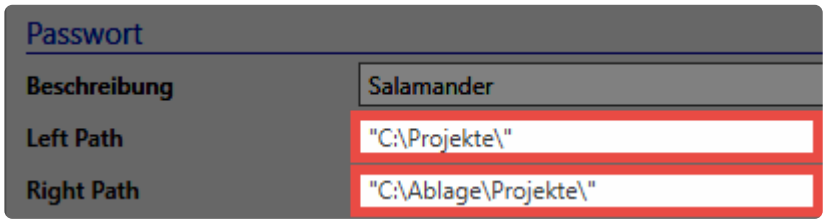
In this example, the following start parameters have been defined for the Salamander application:

- -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.



The application is then linked with the following password:



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.

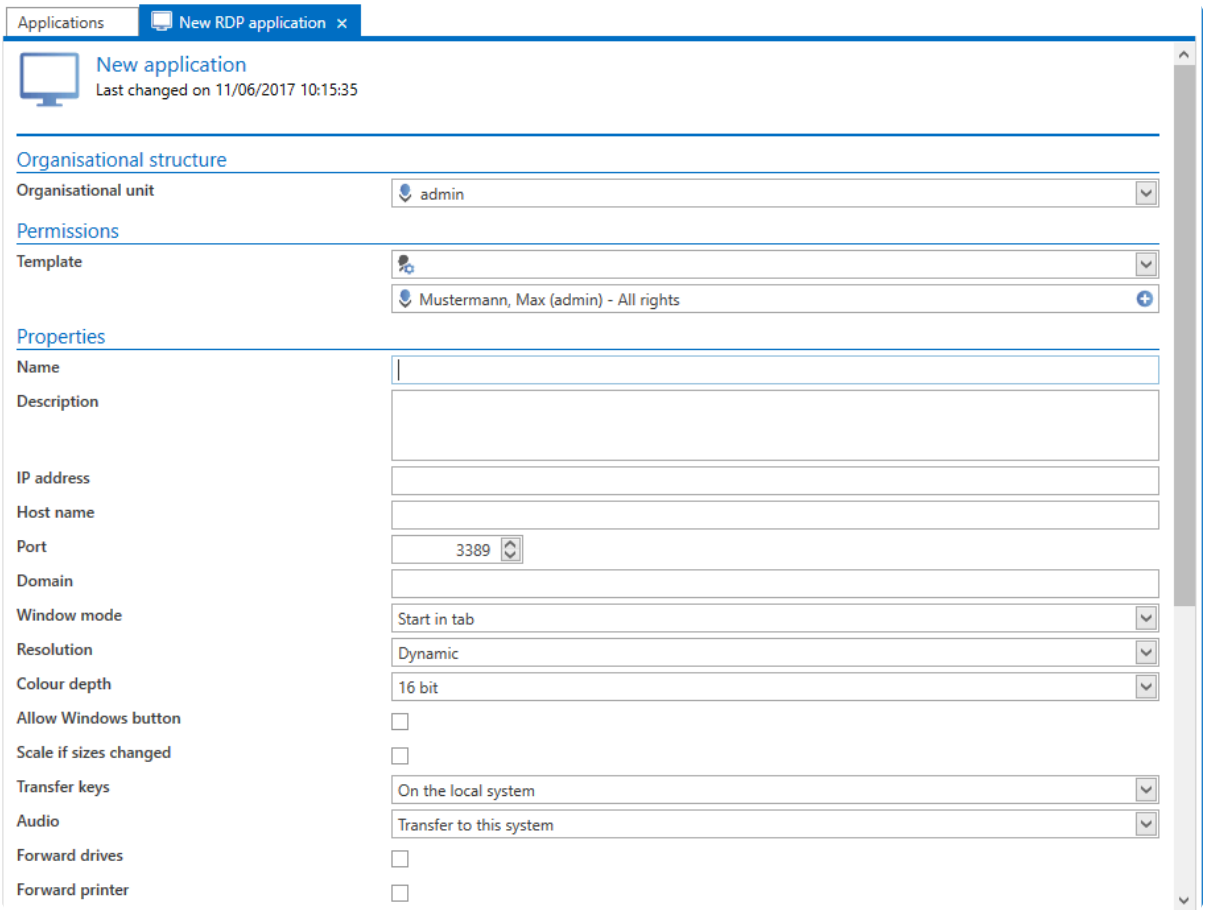
Field type	Placeholder
Text	{Text}
Password	{Password}
Date	{Date}
Check	{Check}
URL	{Url}
Email	{Email}
Phone	{Phone}
List	{List}
Header	{Header}
Multiline text	{Memo}
Multiline password text	{PasswordMemo}
Integer	{Int}
Floating-point number	{Decimal}
User name	{UserName}
IP address	{Ip}
Enter field name	{field:name}

RDP und SSH Anwendungen

Sowohl **RDP- also auch SSH-** Anwendungen können in Password Safe “embedded” dargestellt werden. D.h., die jeweilige Sitzung öffnet sich in einem eigenen Tab im **Lesebereich**.

Erstellen von RDP und SSH Anwendungen

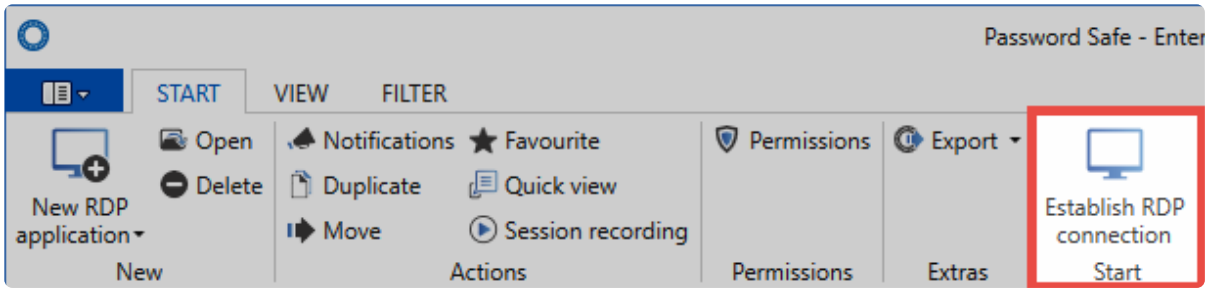
Eine neue RDP- oder SSH- Anwendung kann über die Ribbon oder das Kontextmenü der rechten Maustaste erstellt. Es erscheint das entsprechende Formular, in dem Sie die Variablen für eine Verbindung definieren.



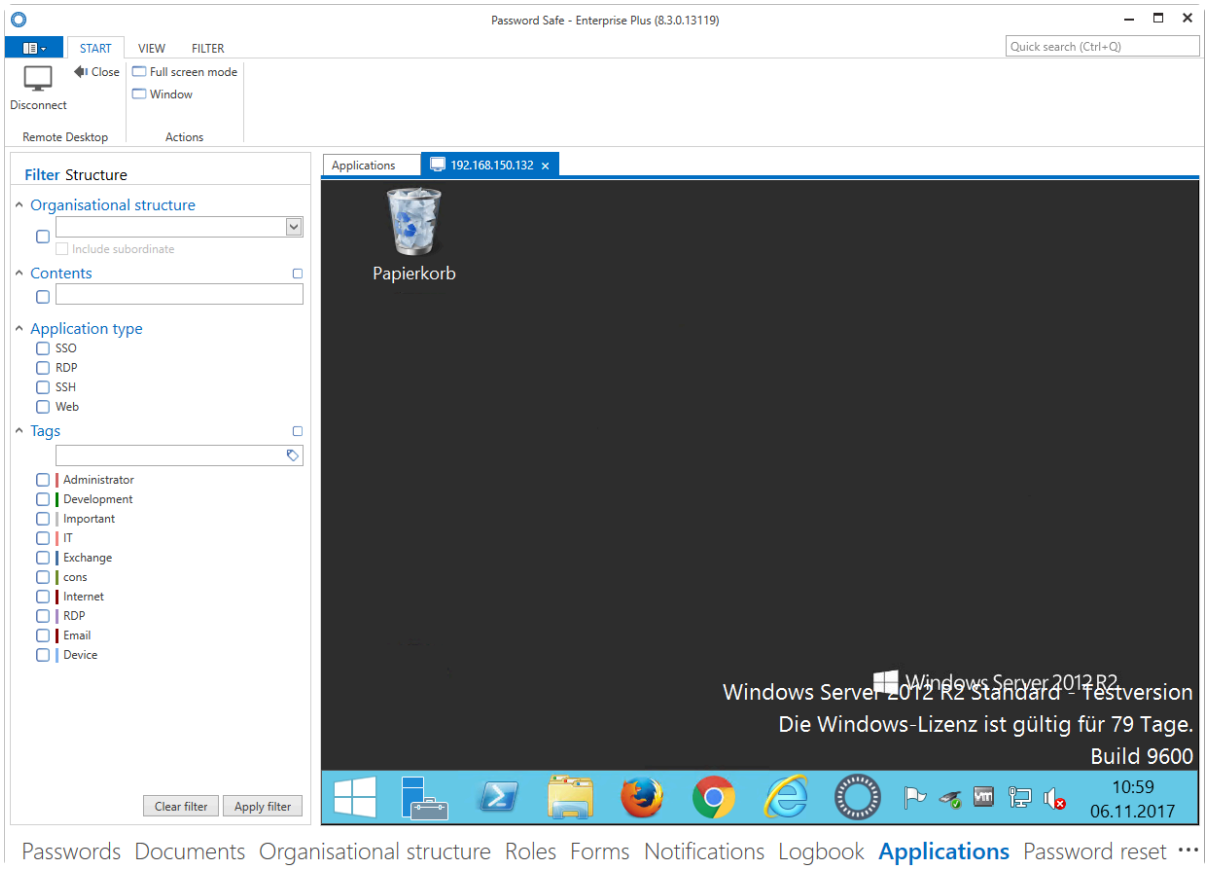
Diese Variablen entsprechen genau denjenigen, die man (hier am Beispiel RDP) bei der Erstellung einer RDP-Verbindung über “mstsc” konfigurieren kann. Im **Fenstermodus** wird definiert, ob die Verbindung in einem Tab, im Vollbildmodus oder in einem separaten Fenster gestartet werden soll.

Arbeiten mit RDP- und SSH-Anwendungen

Hat man z.B. eine RDP-Anwendung erstellt, kann diese direkt über die Ribbon gestartet werden. Mit dem Icon **RDP-Verbindung herstellen** wird die Verbindung zur gewünschten Session aufgebaut.



Password Safe versucht nun, sich mit den verfügbaren Informationen am Zielsystem anzumelden. Nicht im Formular hinterlegte Daten werden direkt beim Öffnen der Session abgefragt. Es ist somit auch möglich, erst nach dem Starten der Password Safe Anwendung die IP-Adresse und/oder das Passwort anzugeben. Sind alle Daten abgefragt, öffnet sich die RDP-Sitzung in einem Tab – falls definiert (Feld Fenstermodus in der Anwendung):



Anmeldung über SSH-Zertifikate

Es ist ebenfalls möglich, die Authentifizierung über SSH-Zertifikate zu realisieren. Hierfür wird das Zertifikat im Format .ppk als Dokument abgelegt (Eventuell muss die Dateiendung zunächst über die Einstellungen freigegeben werden). Über den Footer wird dann das Dokument mit dem Datensatz verknüpft. Der Datensatz muss kein Passwort enthalten, aber dafür mit einer SSH-Anwendung verknüpft sein.

Tastaturkürzel

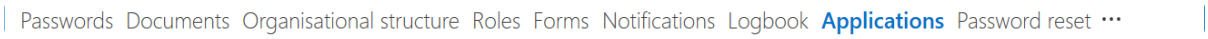
Password Safe unterstützt verschiedene Tastaturkürzel zum Übertragen von – beispielsweise –

Benutzernamen und Passwort in die entsprechende Anwendung. Hierbei ist jedoch zu beachten, dass dies nur funktioniert, wenn die Anwendung direkt aus Password Safe heraus geöffnet wird.

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.



Relevant rights

The following options are required to manage sessions for an application.

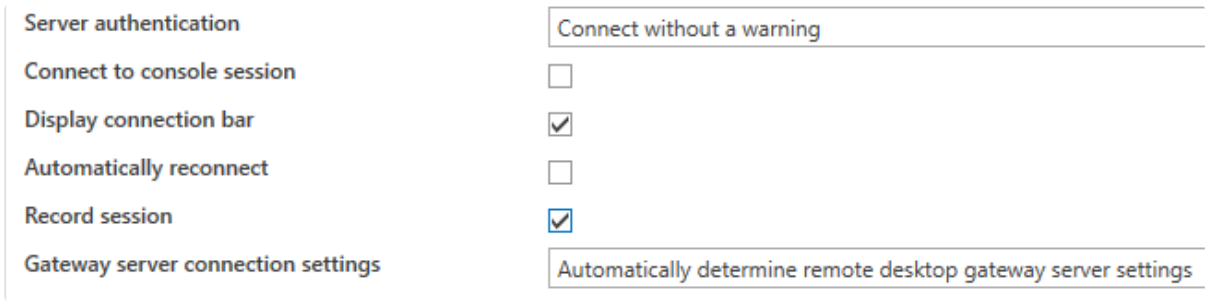
User right

- Can manage recordings for an application

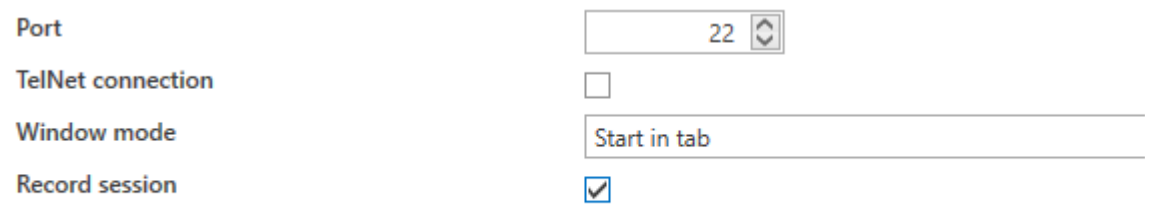
> Please note that session recording uses memory in the database. Although the way the recordings are saved is efficient in terms of resources, the required amount of memory varies greatly depending on the content. The more that is done during the recorded session, the higher the memory usage.

Session recording firstly needs to be activated for the relevant RDP or SSH application before it can take place.

RDP



SSH



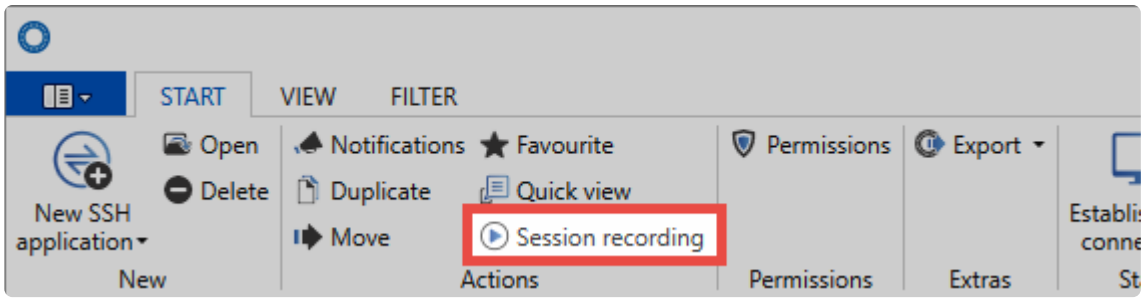
If the setting has been activated, the recording will start automatically the next time a connection is

established.

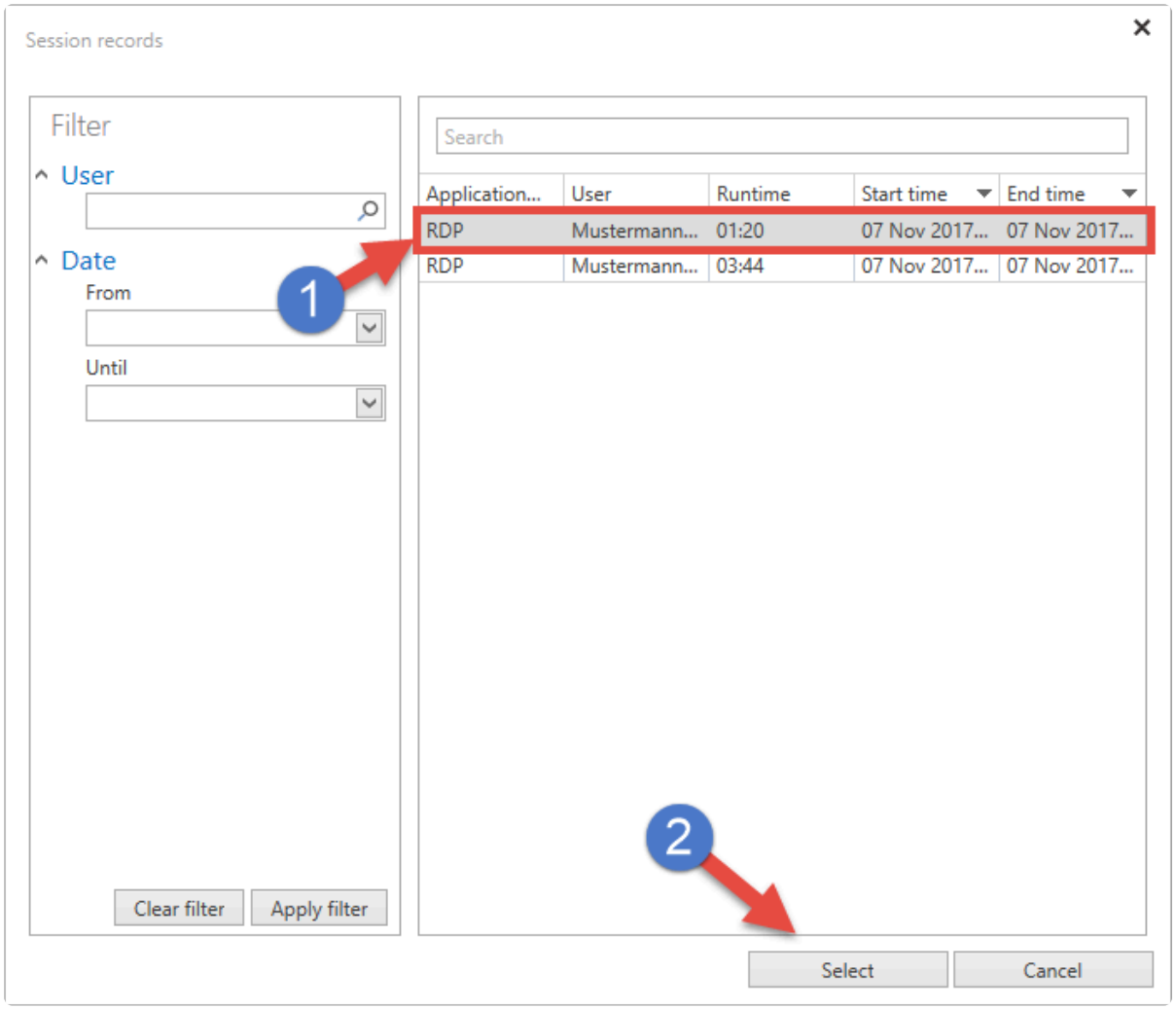
> The recordings are already streamed to the server and into the database during the recording process. Therefore, no recordings are lost even if the connection is terminated. They are immediately saved until the connection is terminated or until the end of the session.

Viewing the session recordings

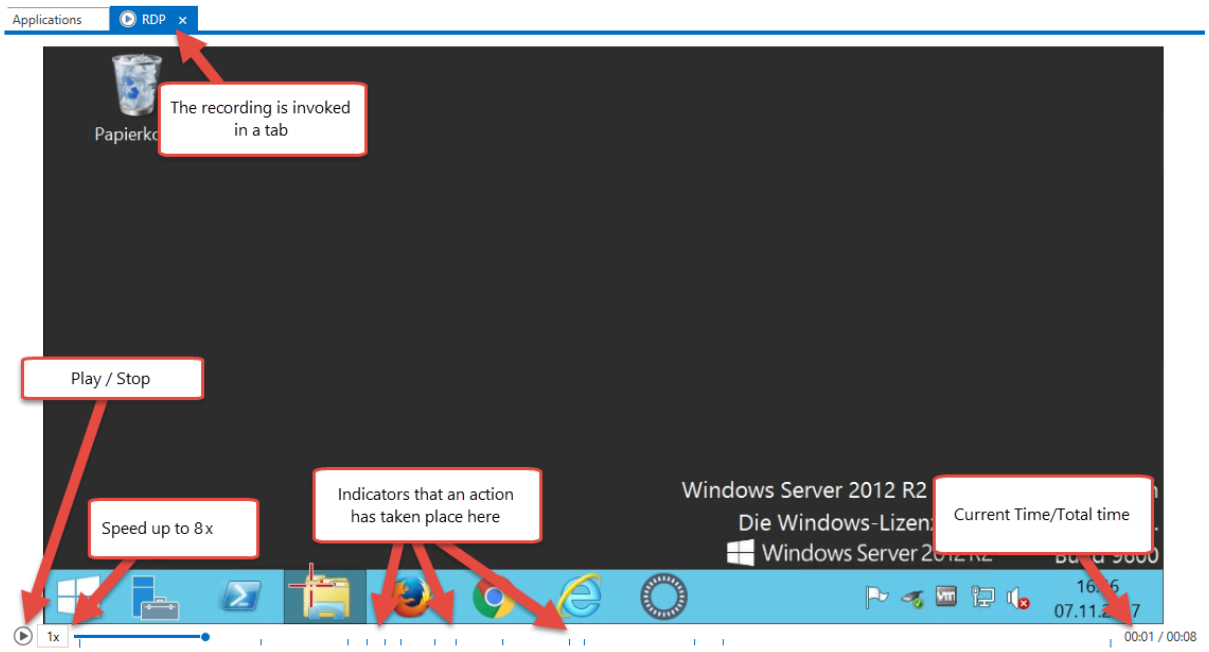
If recordings exist for an application, these can be called up and viewed in the Applications module.



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.



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

Automatic deletion of old recordings

If desired, recordings can be automatically cleaned up. This option can be configured on the **AdminClient**. Further information can be found in the section **Managing databases**.

Configuration of SAML

What is SAML?

The Security Assertion Markup Language (SAML) is an XML framework for exchanging authentication and authorization information. It provides functions to describe and transmit security-related information. This means that you can use one set of credentials to log in to many different websites. It is much easier to manage one login per user than separate logins for email, Customer Relationship Management (CRM) software, Active Directory, and more.

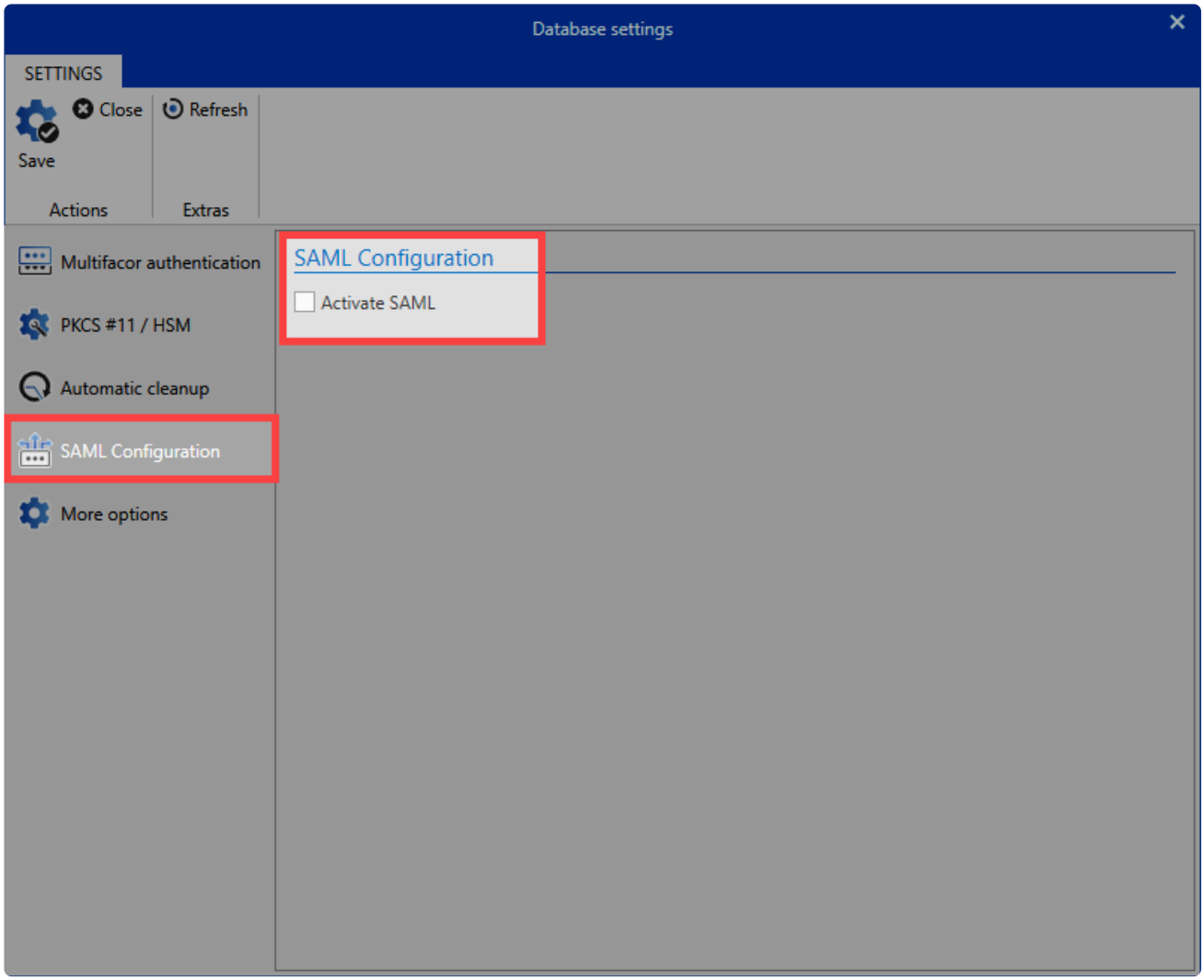
Preconditions

In order for the users to be able to use SAML, “SMTP” must be set up and an e-mail address must be stored with the corresponding users.
In addition, the WebClient is mandatory. Therefore, the WebClient must already be “set up or installed”.

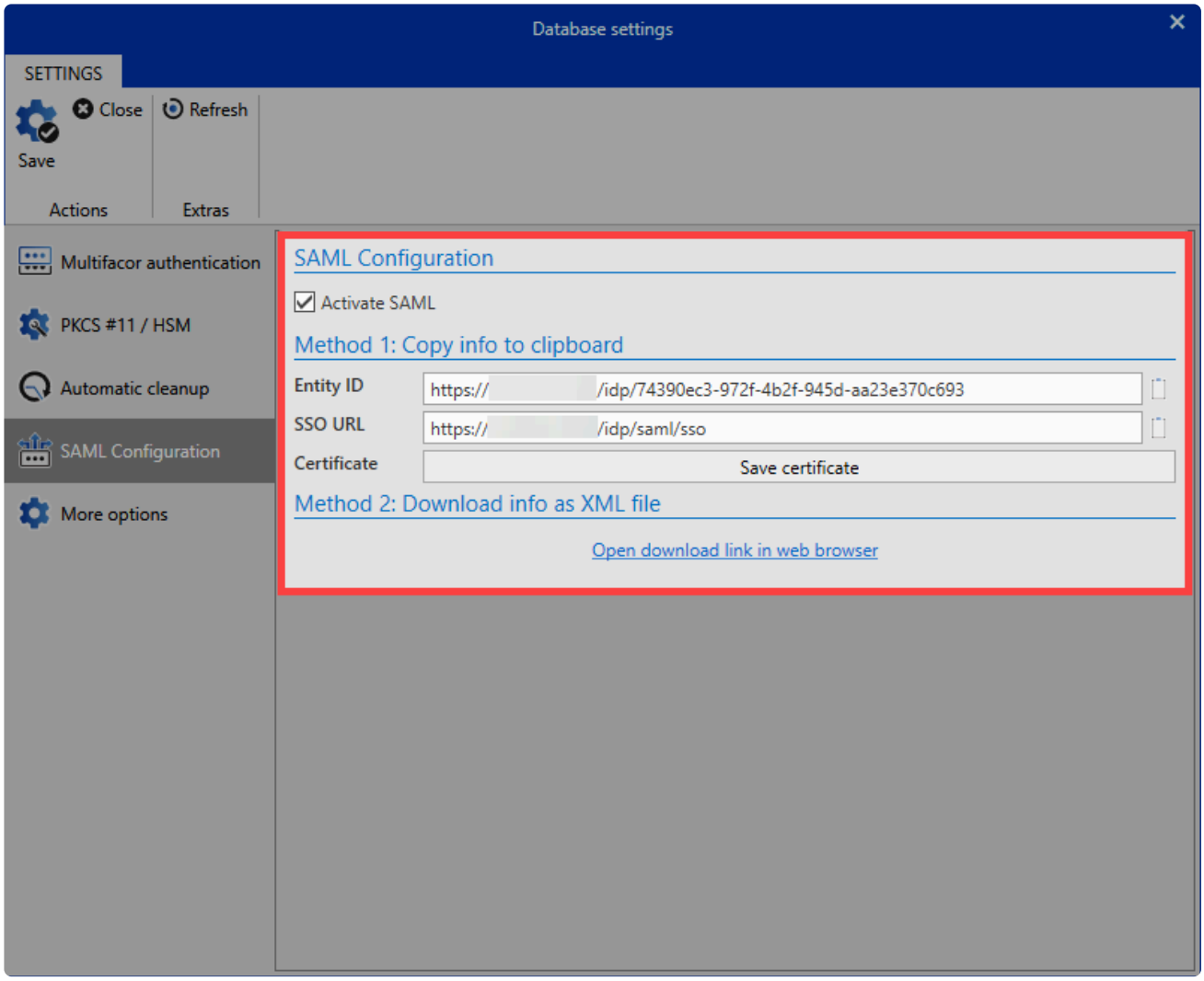
Configuration

In order to create **SAML applications**, SAML must first be activated.

This is implemented in the settings of the database in the Admin Client:

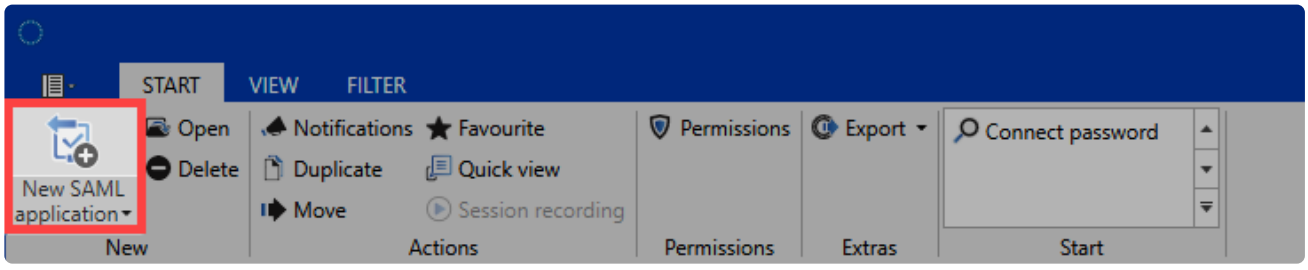


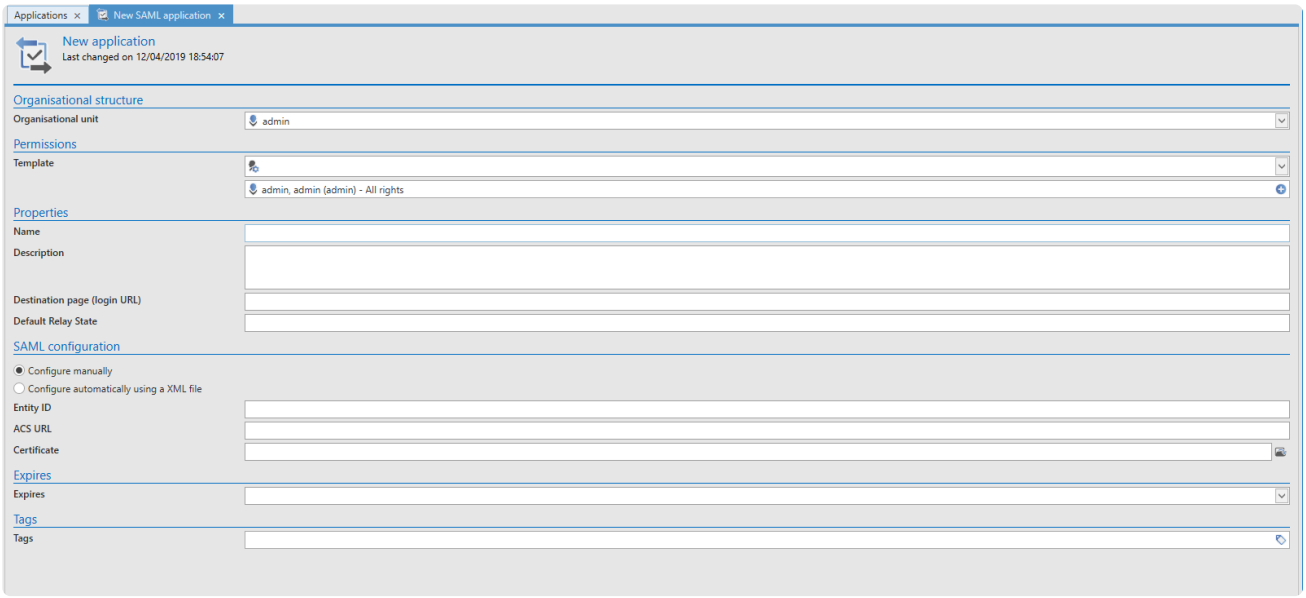
As soon as the checkbox is ticked, the next step is to enter the URL of the WebClient. The SAML configuration screen should then look like this:



The screen is left open and the configuration is continued at FullClient.
To do this, log on to the client as usual and switch to the **Applications** module. Select a **new SAML application** and fill it with the relevant data from the service provider.

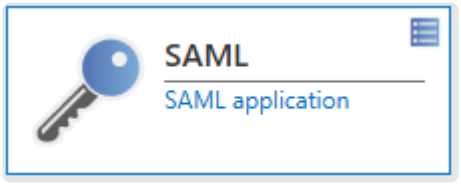
> The data of the service provider, which are entered in the FullClient, can be found at the respective provider. This differs from provider to provider.





In addition, the data must be stored in the **Admin Client** at the service provider.

After the successful entry of all data, the last necessary step is the verification of the user. This is done by clicking on the tile. This gives the user an e-mail with which he can verify himself.



After verification, the **SAML application** can be started from the LightClient view.

! As this is a passwordless authentication, it is not necessary to link the **SAML application** with a password.

✻ Setup and configuration instructions for **Dropbox** and **Postman** can be found in the corresponding chapters.

Beispiele für Anwendungen

Folgend finden Sie Beispiele aus Praxis zum Erstellen von Anwendungen:

- **SSO-Anwendung für SAP GUI Logon**
- **SAML-Anwendung für Dropbox**
- **SAML-Anwendung für Postman**

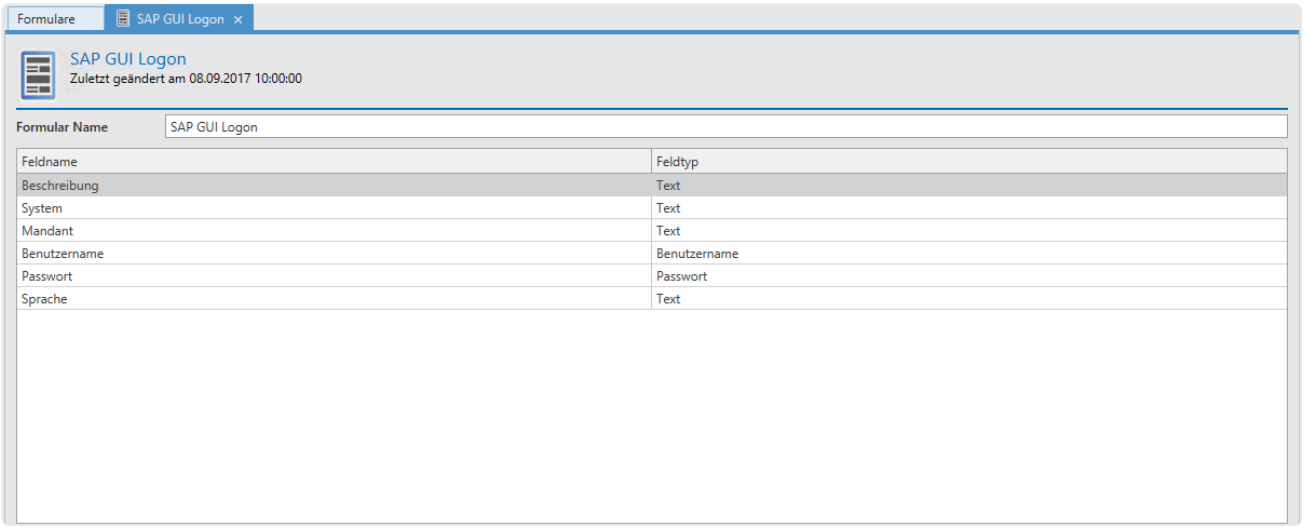
SAP GUI logon

Fundamental information

Logging into SAP can be achieved via “”:#startparameter. The prerequisite here is for the login process to be carried out via “SAPshortcuttextileRef:4469804076347be2e17db7:linkStartMarker:”.
All available parameters are listed under “”:https://wiki.scn.sap.com/wiki/display/NWTech/SAPshortcut.

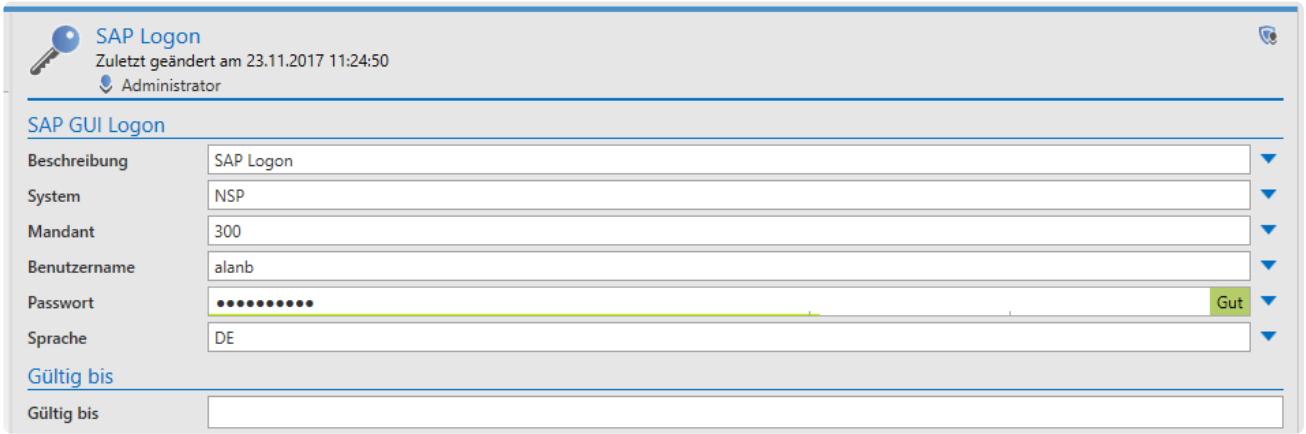
Form

Firstly, a “form”:#formulare should be created with the required fields. This could look like this:



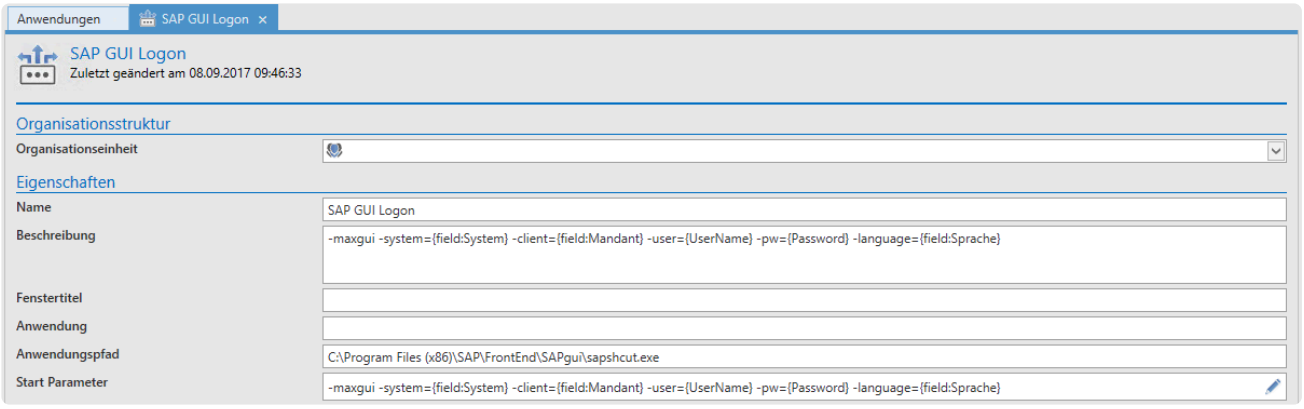
Record

A corresponding record is then created via the form:



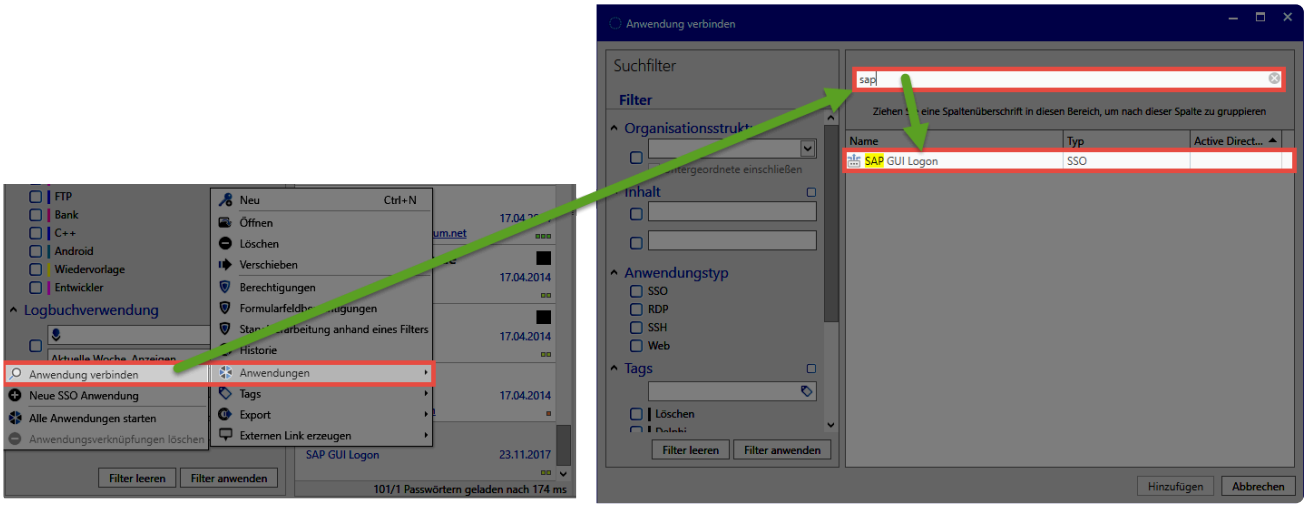
Application

A corresponding SSO application now needs to be created.



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**.



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.

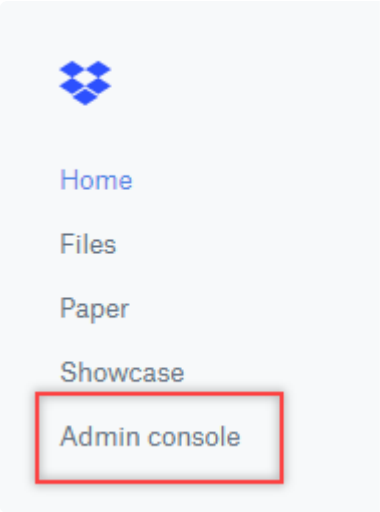
SAML application for Dropbox

SAML Configuration Example for Dropbox

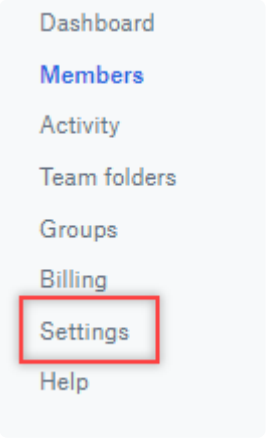
This chapter explains in more detail how to configure the SAML application for **Dropbox**. It is assumed that SAML has already been activated on the Admin Client.

1. Log in as administrator at the **Dropbox**

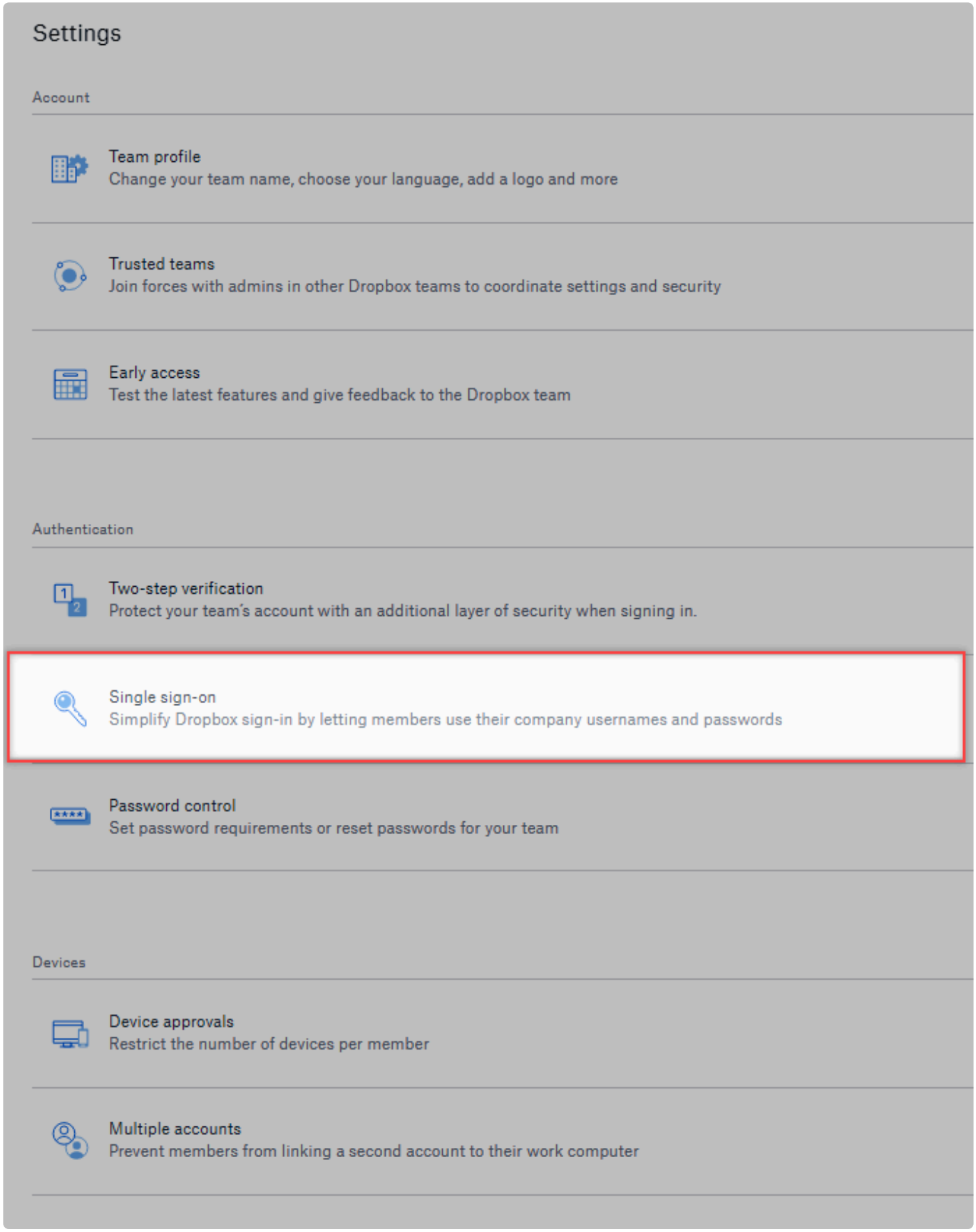
2. Open the Admin Console



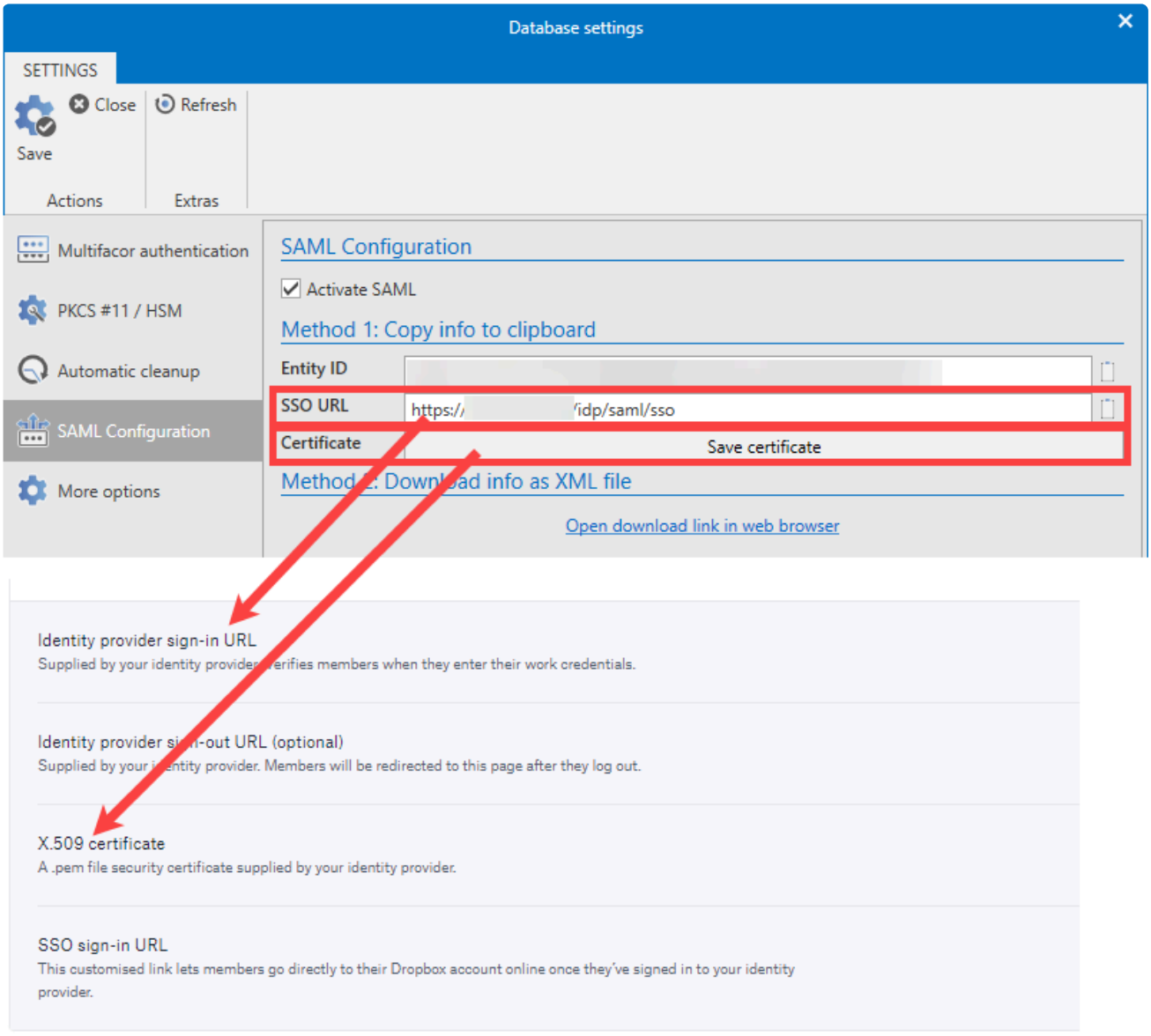
3. Open Settings



4. Single Sign On

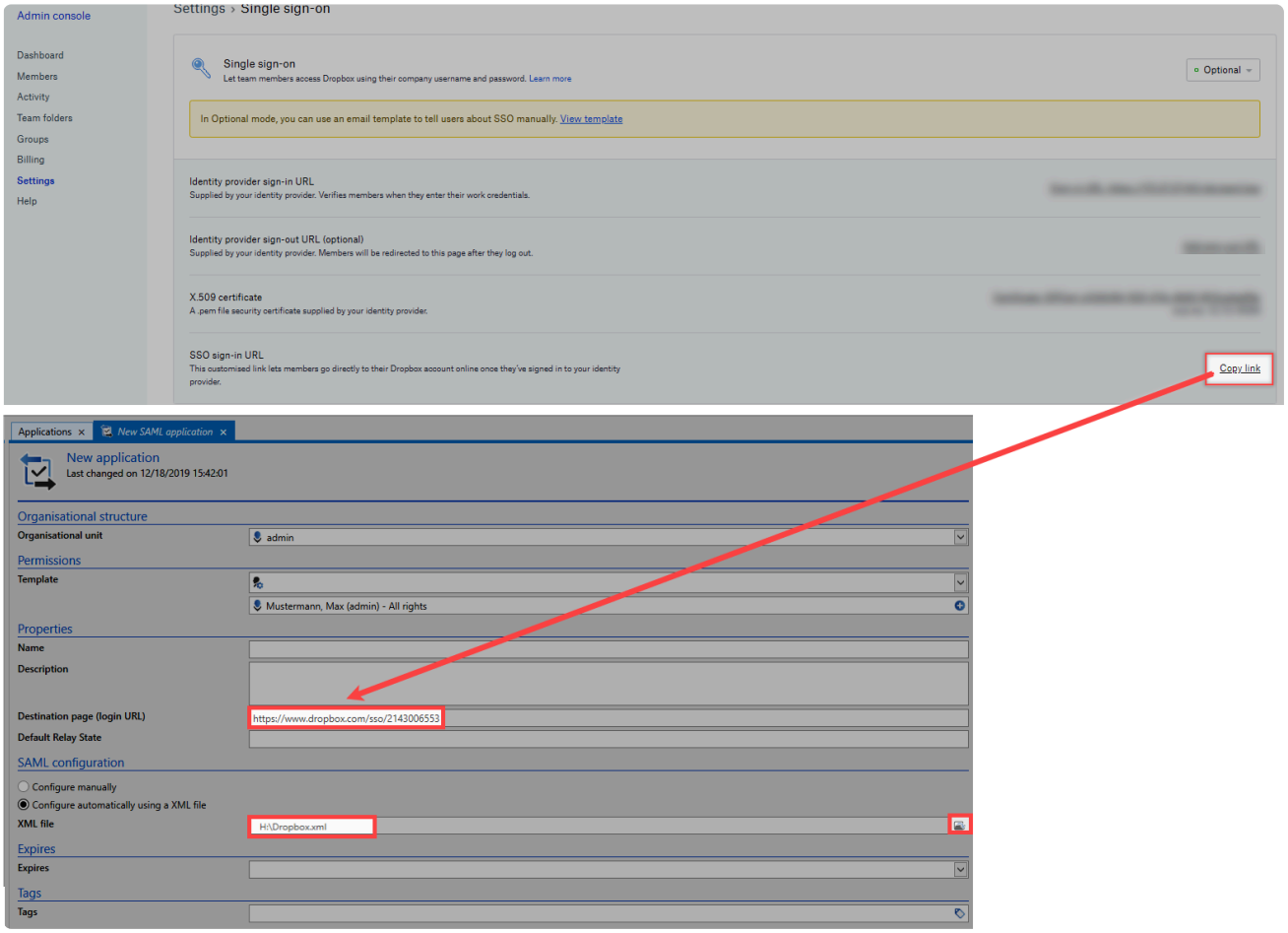


5. This is where the data SSO URL and the certificate from the Admin Client must be deposited.



6 In the FullClient, a new SAML application must be created in the Applications module.

7. Then the target page (login URL) and the XML file must be stored in the application.



The XML file must look like this.

8. The application can now be executed via the LightClient.

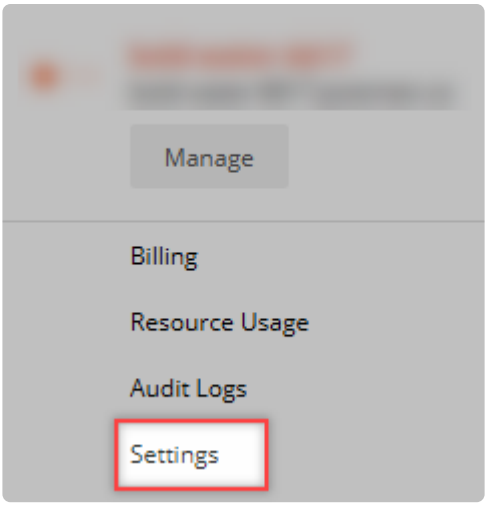
SAML application for Postman

SAML configuration example for Postman

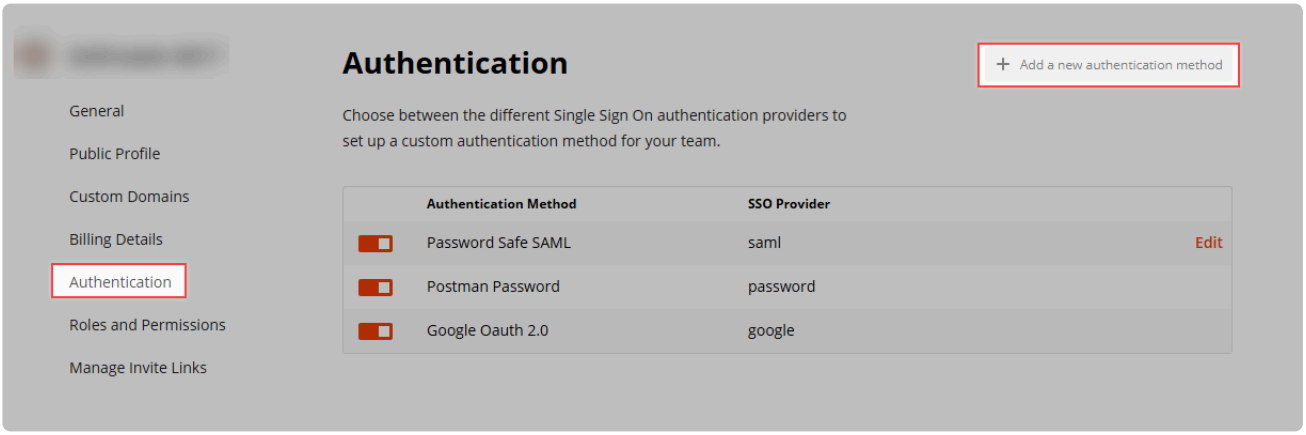
This chapter explains how to configure the SAML application for **Postman**. It is assumed that SAML has already been activated on the admin client.

1. First, you register with Postman.

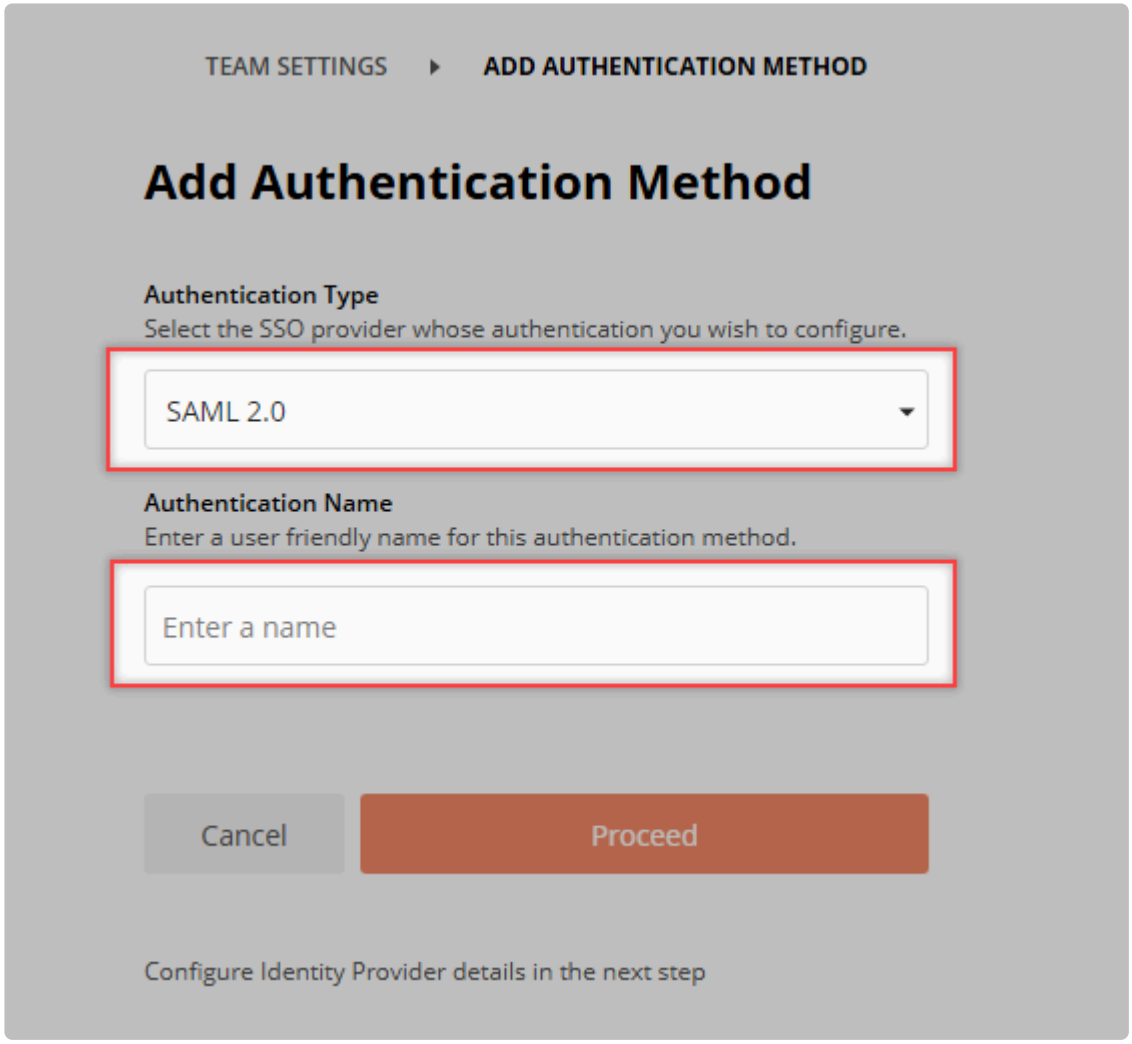
2. After logging in, click on the avatar and select **“Settings “**.



3. Then click on **Authentication**. Select a new method in the upper right corner.



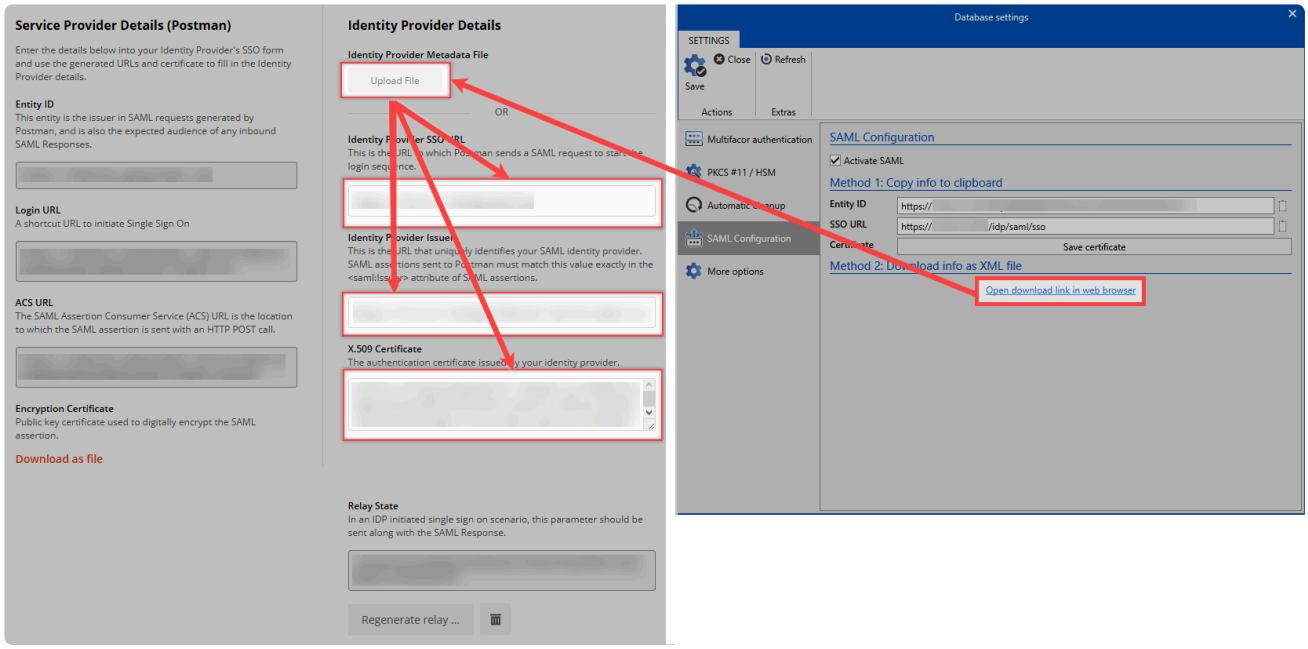
4. Here the Authentication Type must be defined with **SAML 2.0** and any useful Authentication Name.



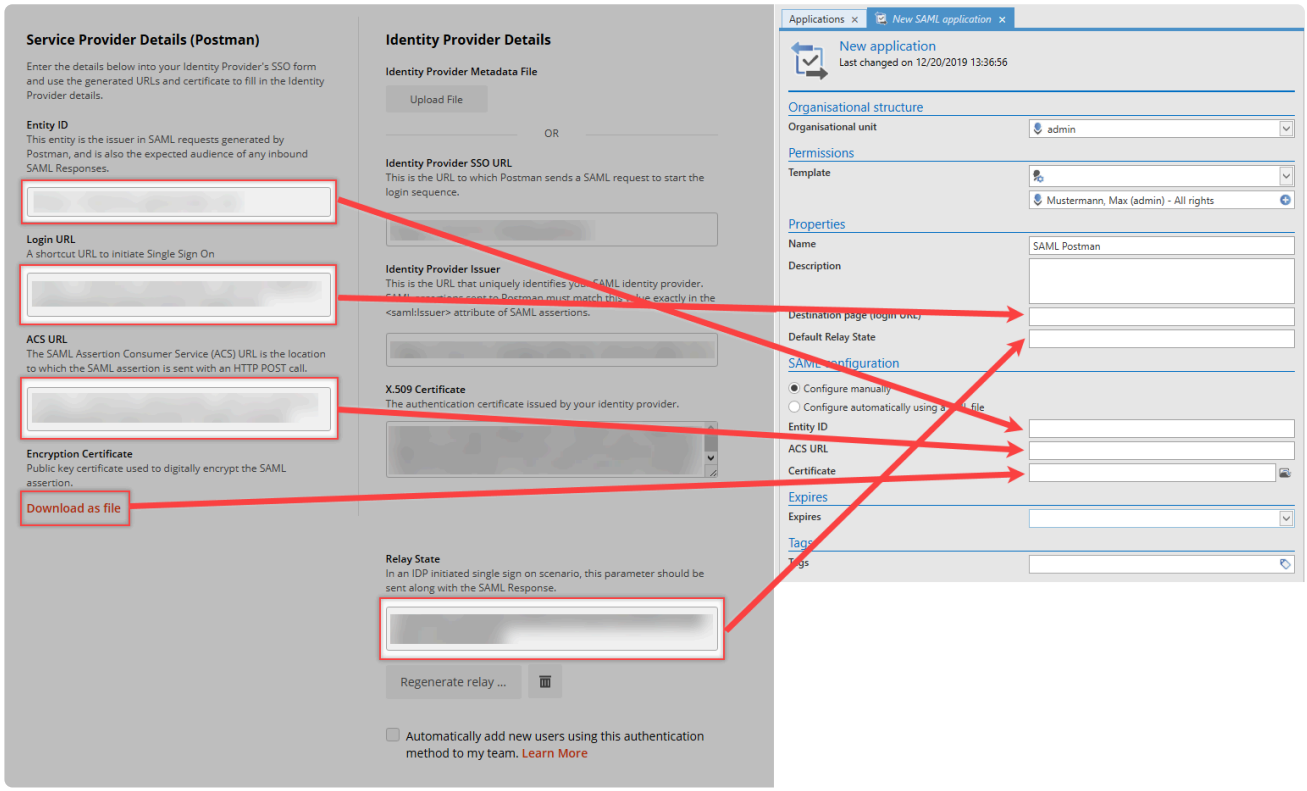
Then you come to the actual configuration.

5. Store Provider Details

- **5.1 Identity Provider Details**
  The data from the Admin Client is uploaded as XML or stored manually.



- **5.2 Service Provider Details**
  The service provider details are now copied to the application in the Password Safe Client.

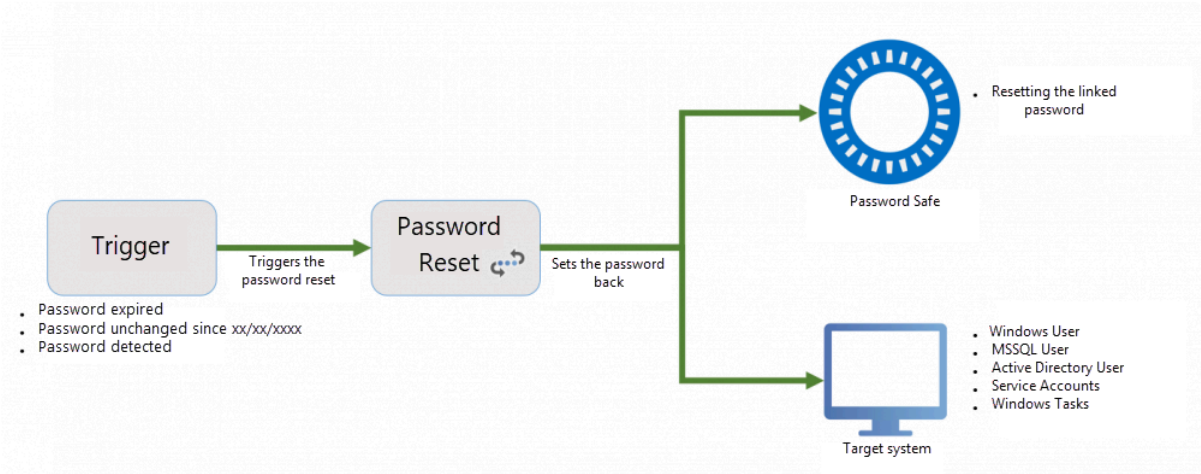


> Please note that a **Relay State** is required. This value can be created in the **Configure Identity Provider Details View**.

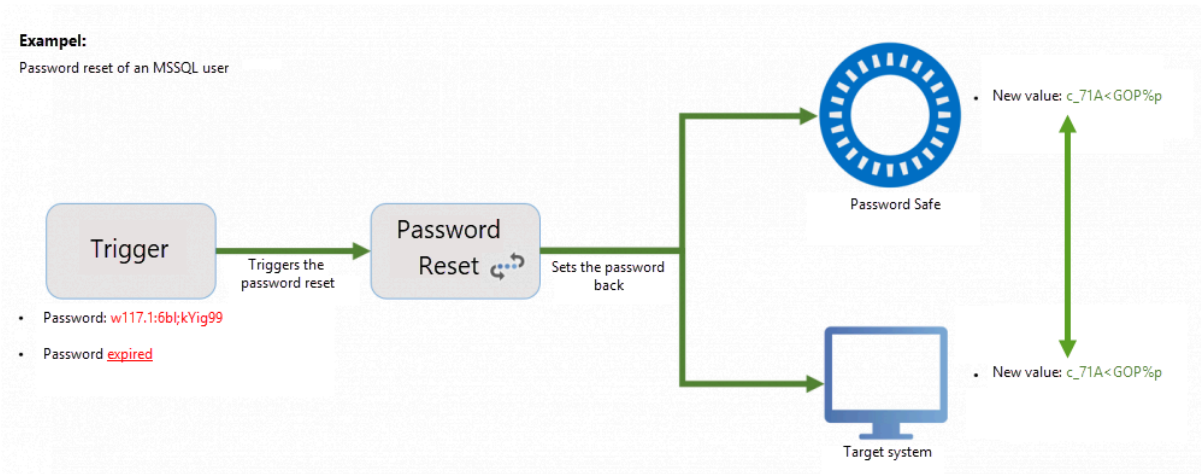
Password Reset

What is a 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.



If an error occurs during the execution of a password reset, the affected reset is blocked with all associated passwords. This is noted in the logbook with an entry “blocked”.

Due to the complexity of the process, 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.

Requirements

Availability

Password Reset is exclusively available in the **Enterprise Plus Edition**.

Relevant rights

The following options are required for creating a Password Reset.

User rights

- Can add new Password Resets
- Display Password Reset module

Requirements

- A password that has administrative rights to the relevant target computers must have been saved in Password Safe.
- The Microsoft Remote Admin Tools must be saved on the target system.
- The target system must be accessible via the network.

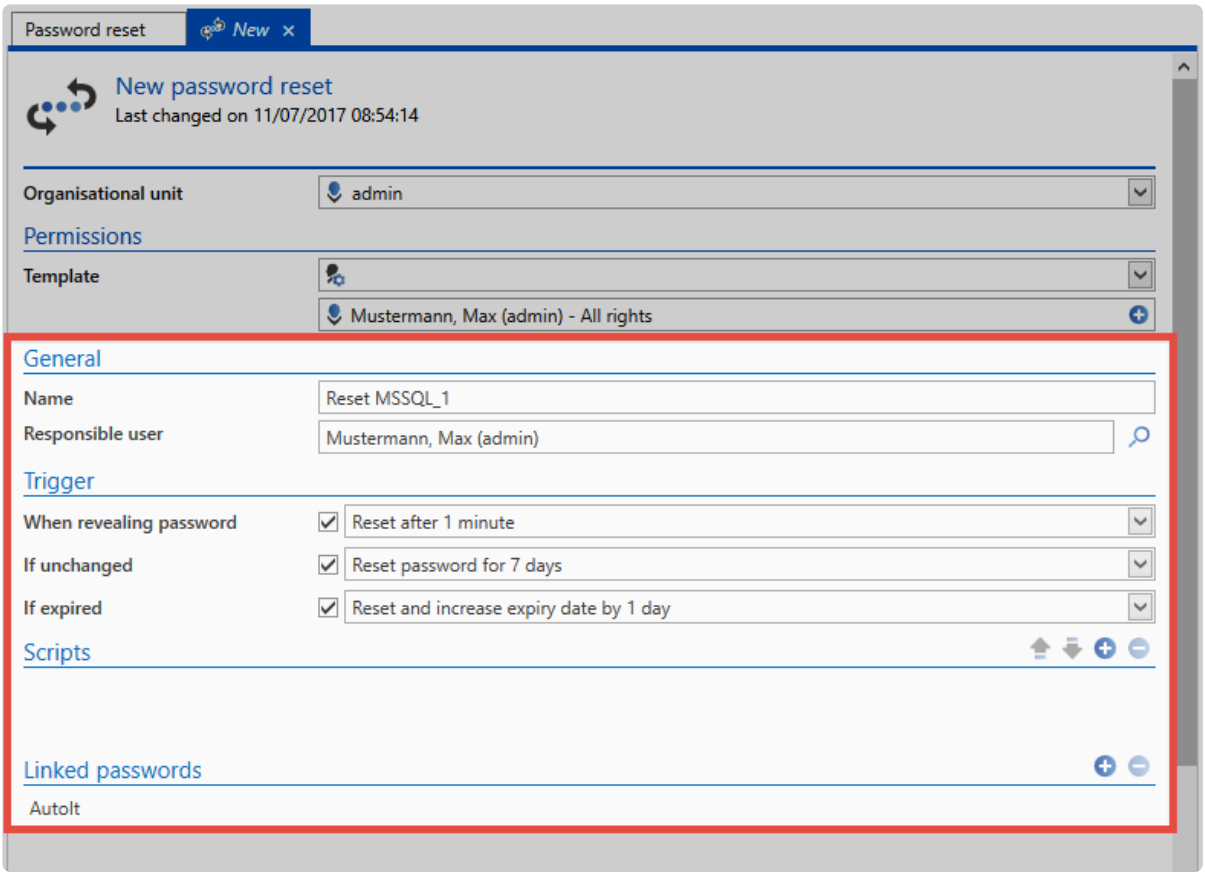
Configuration

Creating a Password Reset

New Password Resets can be directly added via the ribbon or the keyboard shortcut “Ctrl + N” in the Password Reset module. With regards to setting permissions, a Password Reset behaves in precisely the same way as every other object. It is thus possible to precisely control 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”.



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:

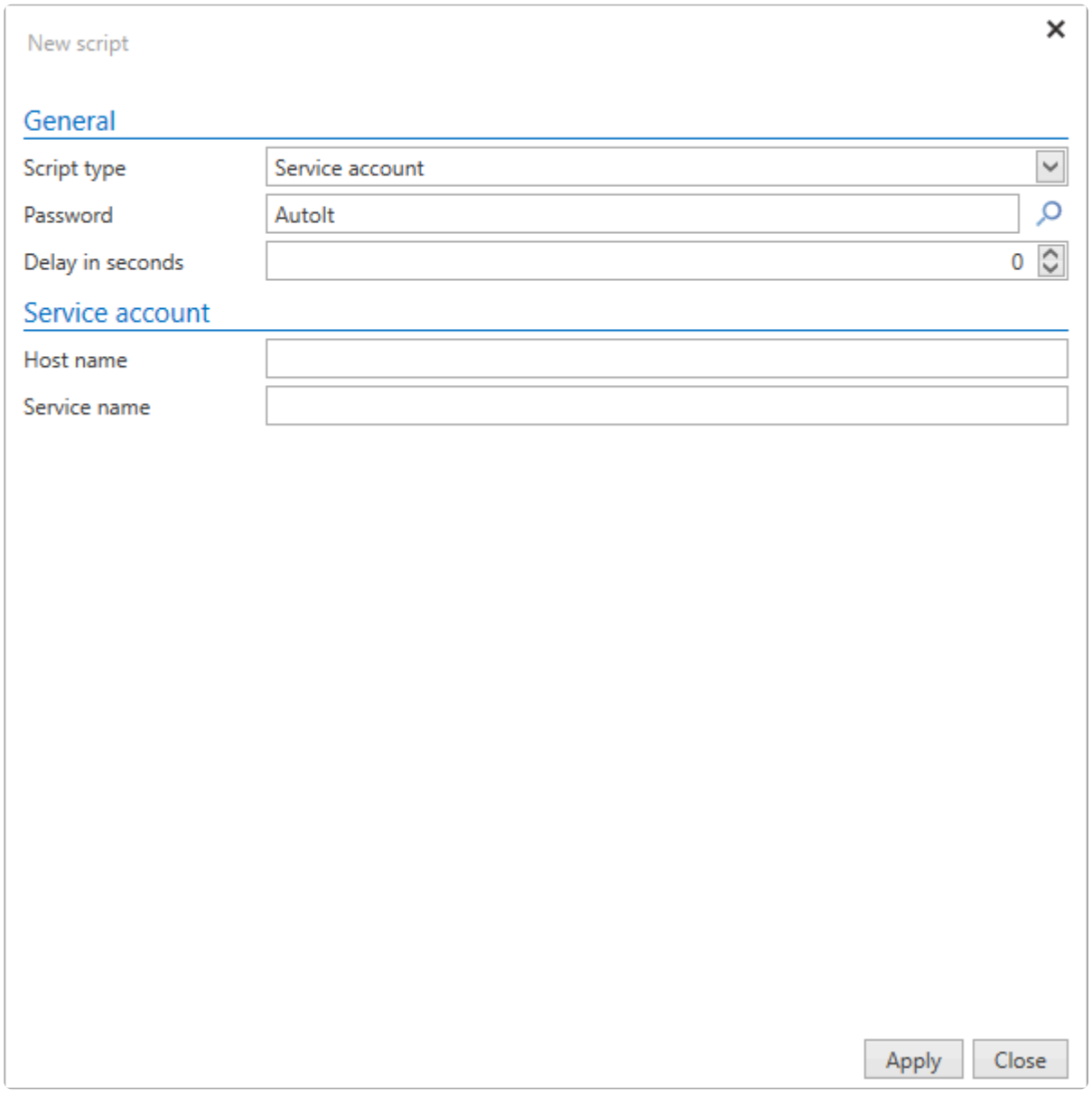
- Reset the password x minutes after the password has been viewed
- Reset the password when it has not been changed for x days
- Reset the password when it has been expired for x days

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

A new dialogue appears after the selection in which the type of system “to be reset” can be defined.



- **Script type**: You select here from the possible script types.
- **Password**: The credentials for the record that will ultimately carry out the Password Reset.

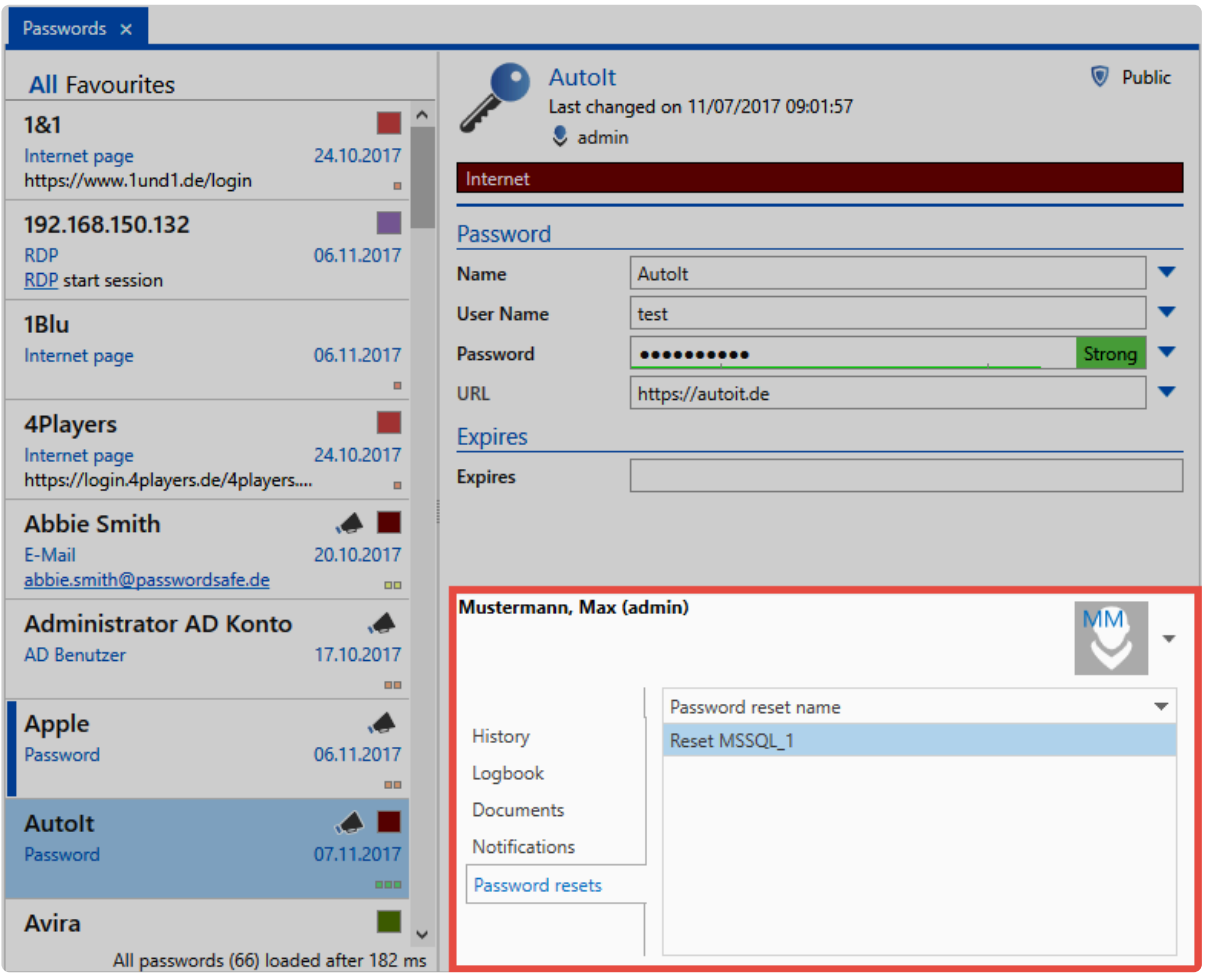
The required information is specifically requested in each case. For example, if the reset is for an MSSQL user, the MSSQL instance and the port used needs to be entered.

The functions and configuration process are described in detail in the section Scripts.

> 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”. Multiple objects can be entered. The linked Password Reset is also visible in the footer of the reading pane once it has been successfully configured.

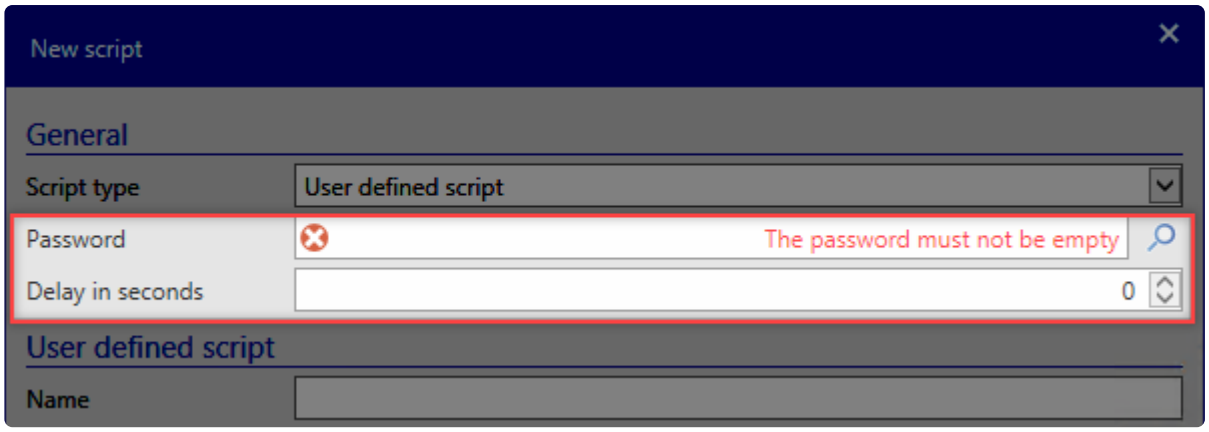


Password Safe scripts

Available scripts

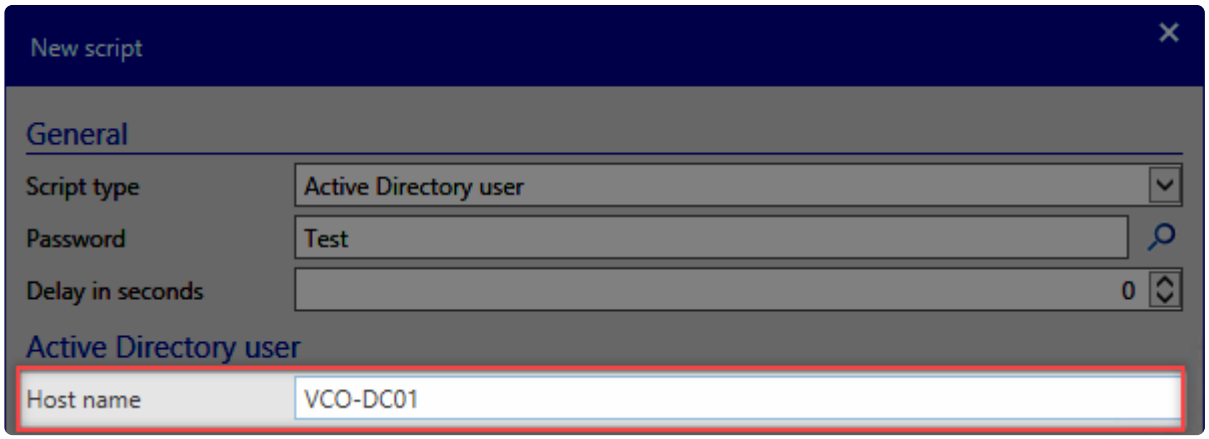
The following scripts are supplied and can be directly used. In all scripts, a password is firstly selected in the upper section. This is **not** the password that will be reset on the target system. Instead, a user should be entered here that can complete the rest of the process on the target system. This password thus requires administrative rights to the target system.

A delay can also be configured in every script. This may be necessary, for example, if a password is changed in AD and it is firstly distributed to other controllers.



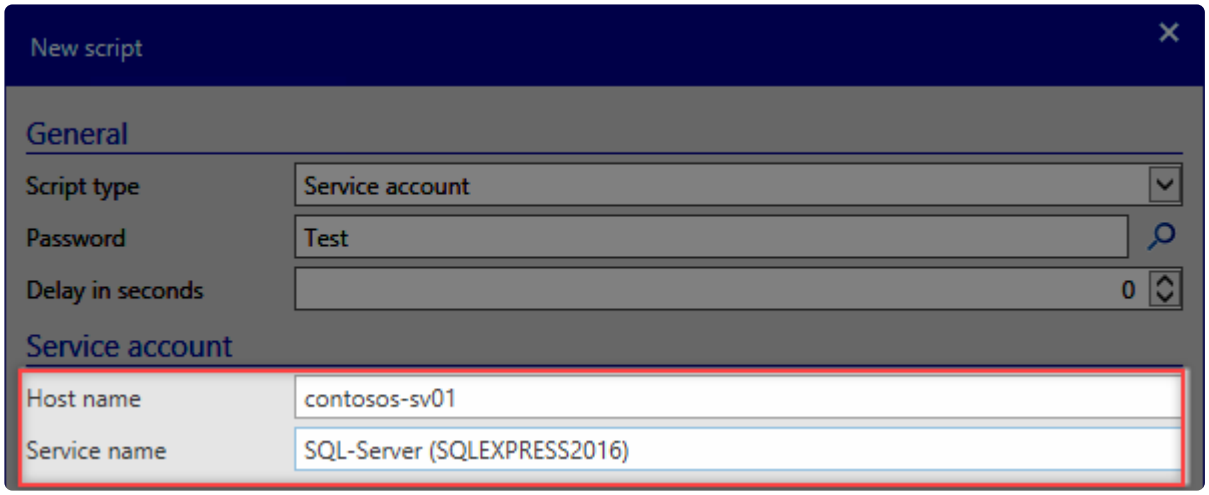
Active Directory user

This script is responsible for changing passwords for Active Directory users (domain users). Access to Active Directory is configured here under **Hostname**.

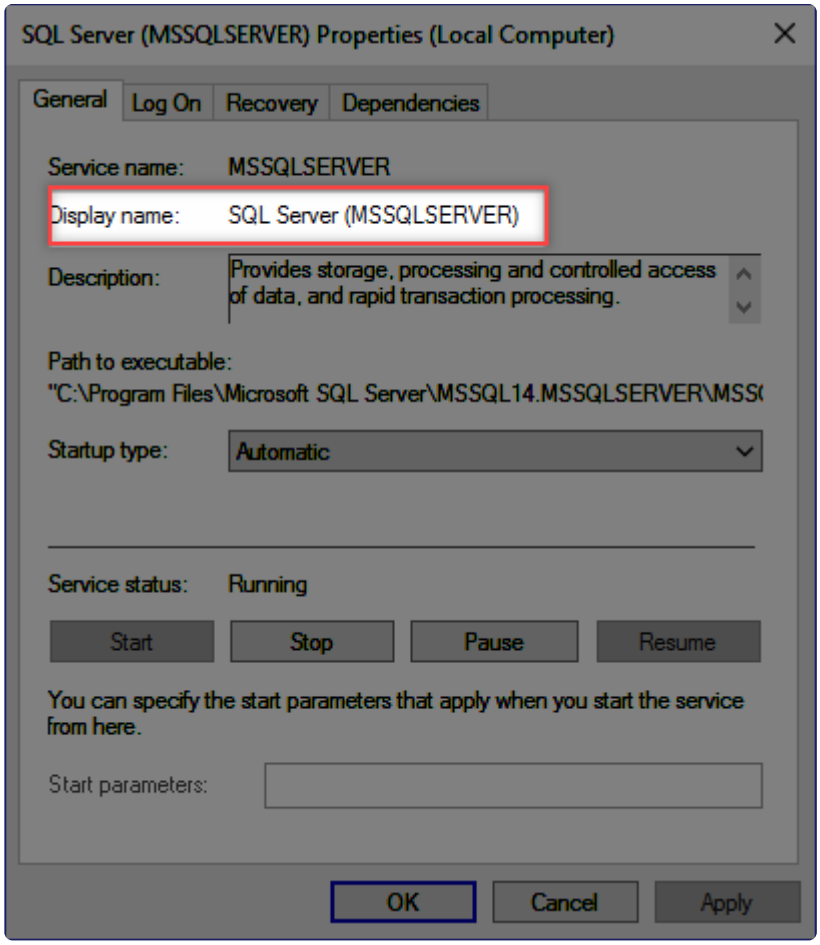


Service accounts

This script changes the access data within a service. Both the user and also the password can be changed. The **host name** – i.e. the target computer – and the **service name** are saved here.



Please note that the **display name** for the **service** needs to be used.



The access data in the associated password can be saved as follows:

Local user

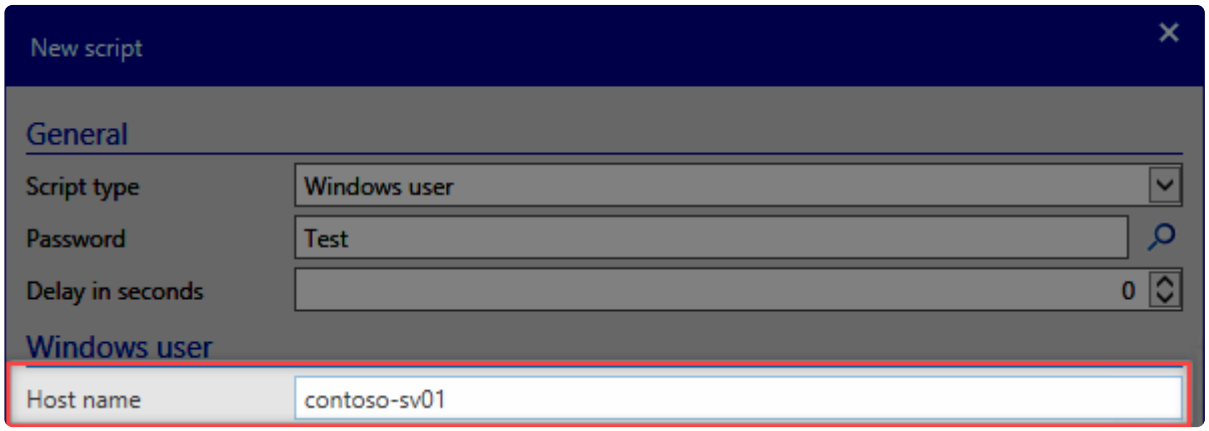
[Username]
\[Username]
.\[Username]
[Computer]\[Username]

Active Directory user

[Domain]\[Username]

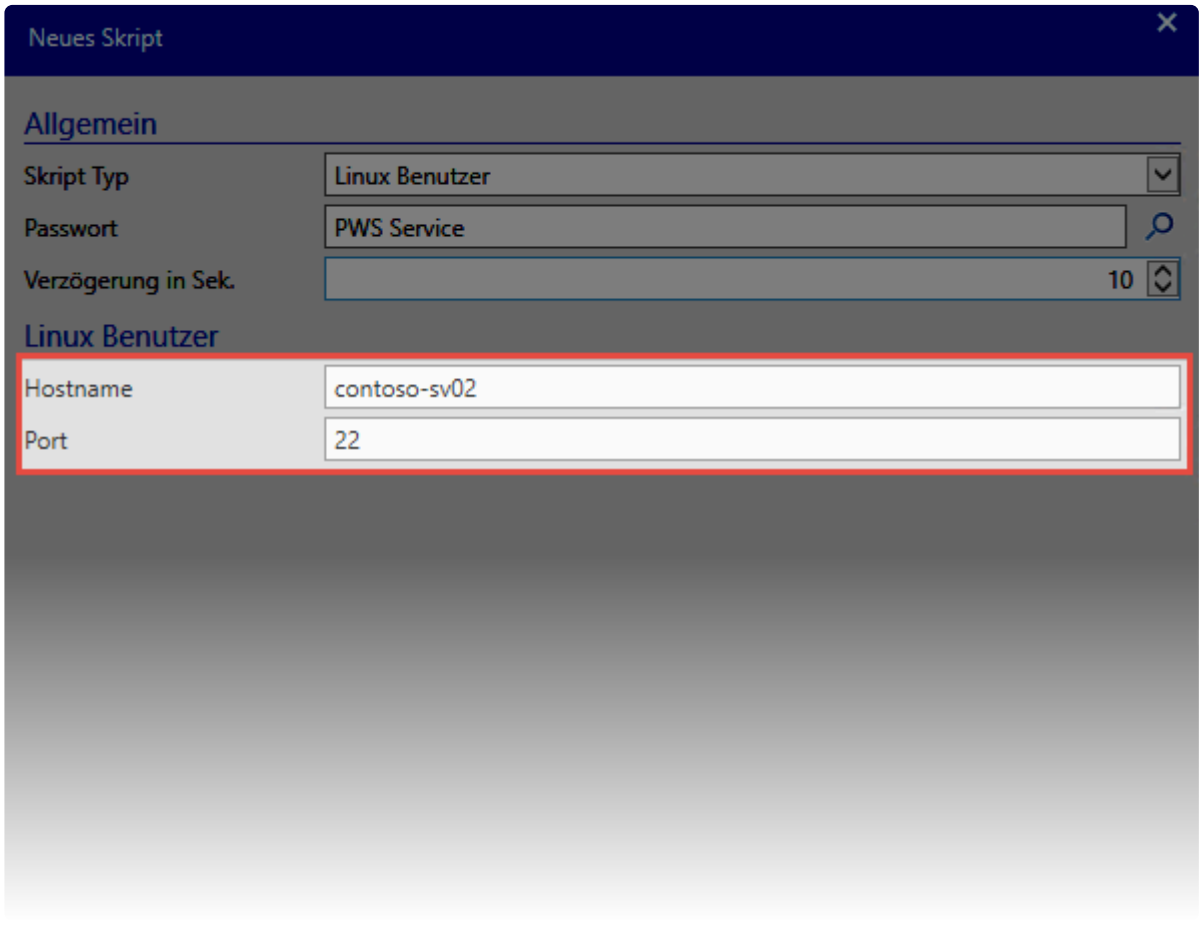
Windows user

This script can be used to reset the passwords for local Windows users. Only the **host name** needs to be saved here.



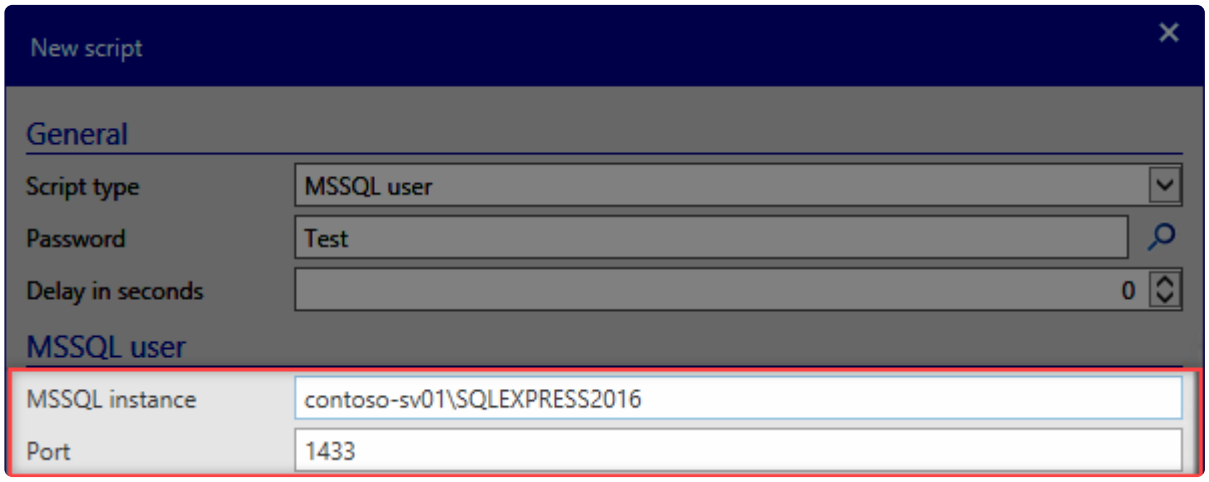
Linux user

Linux users can also be reset in the same way as Windows users. It is also only necessary to enter the **host name** and the **port** here.

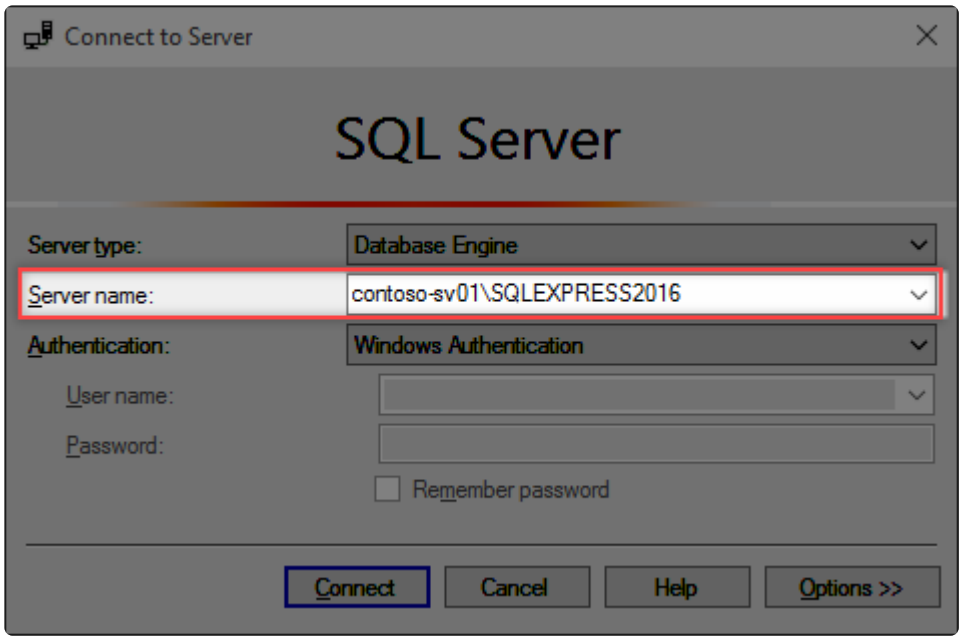


MSSQL user

This script resets passwords for local MSSQL users. It is only necessary to enter the **MSSQL instance** and the **port**.



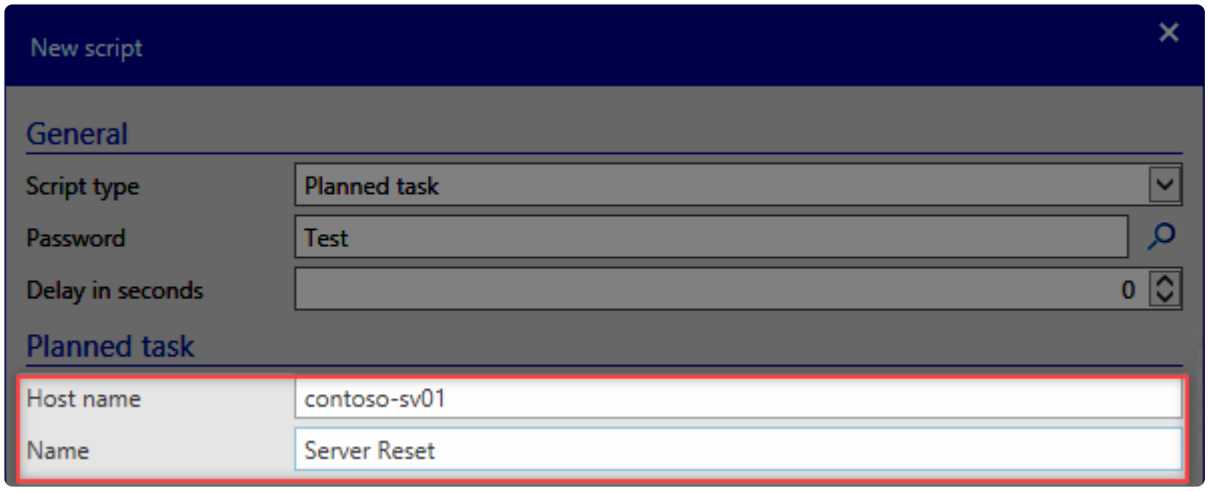
The name of the MSSQL instance can be taken from the login window for the SQL Management Studio.



If a domain user is being used to log in to the SQL server, the user needs to be managed via the script **Active Directory user**.

Planned task

The passwords for users of Windows Task Scheduler can be changed using this script. The **host name** of the computer on which the task will run and the **name** of the task itself are entered.


New script
General
Script type
Planned task
Password
Test
Delay in seconds
0
Planned task
Host name
contoso-sv01
Name
Server Reset

User-defined scripts

Individual solutions using your own scripts

If your requirements cannot be met using the **supplied scripts**, it is also possible to create your own Powershell scripts. These scripts need to meet certain requirements to be used in Password Safe.

Storage location, name and call

The scripts must be saved in the following directory:
C:\ProgramData\MATESO\Password Safe and Repository Service\System\PowerShell

The scripts are saved in the **format .ps1**.

Structure of the scripts

The PowerShell scripts must have the following structure:

RunScript function

Password Safe always calls the RunScript function.

```
function RunScript
param (
        [String]$HostName,
        [String]$UserName,
        [String]$NewPassword,
        [String]$CredentialsUserName,
        [Security.SecureString]$CredentialsPassword
    )
```

The following standard parameters can be used here:

- **UserName:** The user name for which the password should be changed
- **Password:** The password that should be reset
- **CredentialsUserName:** The user name of the user authorized to carry our the reset (e.g. administrator)
- **CredentialsPassword:** The password of the authorized user

Scriptblock

The **scriptblock** can be used when the script should run in the context of another user. The actual change is then carried out in the **scriptblock**.

It is important in this case that you provide Password Safe with feedback about what has been changed via a **Write-Output**. The following example simply uses the outputs **true** or **false**. However, it is also

conceivable that an error message or similar is output.

```
$scriptBlock = {param ($UserName, $Password)
    // Make changes to SAP
    if($OK) {
        Write-Output "true"
    } else {
        Write-Output "false"
    }
```

Naturally, CredentialsUserName and CredentialsPassword can also be directly used in the script (i.e. without the scriptblock). You can view the supplied MSSQL script as an example.

Invoke

A credential then still needs to be created. This is then transferred to the **scriptblock** using the **invoke** command. It is also important in this case to provide Password Safe with feedback about all errors via **Write-Output** or **throw [System.Exception]**.

Heartbeat

What is the heartbeat?

The heartbeat checks whether passwords in Password Safe match the login data on the relevant systems. This process ensures that the passwords do not differ from one another.

Requirements

The heartbeat is only available for passwords that are linked to a properly functioning Password Reset.

Supported script types

The passwords for the following script types can be tested:

- Windows user
- MSSQL user
- Active Directory users
- Linux user

Further information can be found in the section Scripts.

Testing using heartbeat

The testing process using the heartbeat can be executed via various methods.

Testing via Password Reset

The heartbeat is always carried out before the first resetting process using a Password Reset. After the script has run, the testing process is carried out again. Further information on this process can also be found in the section Rollback.

Manual testing

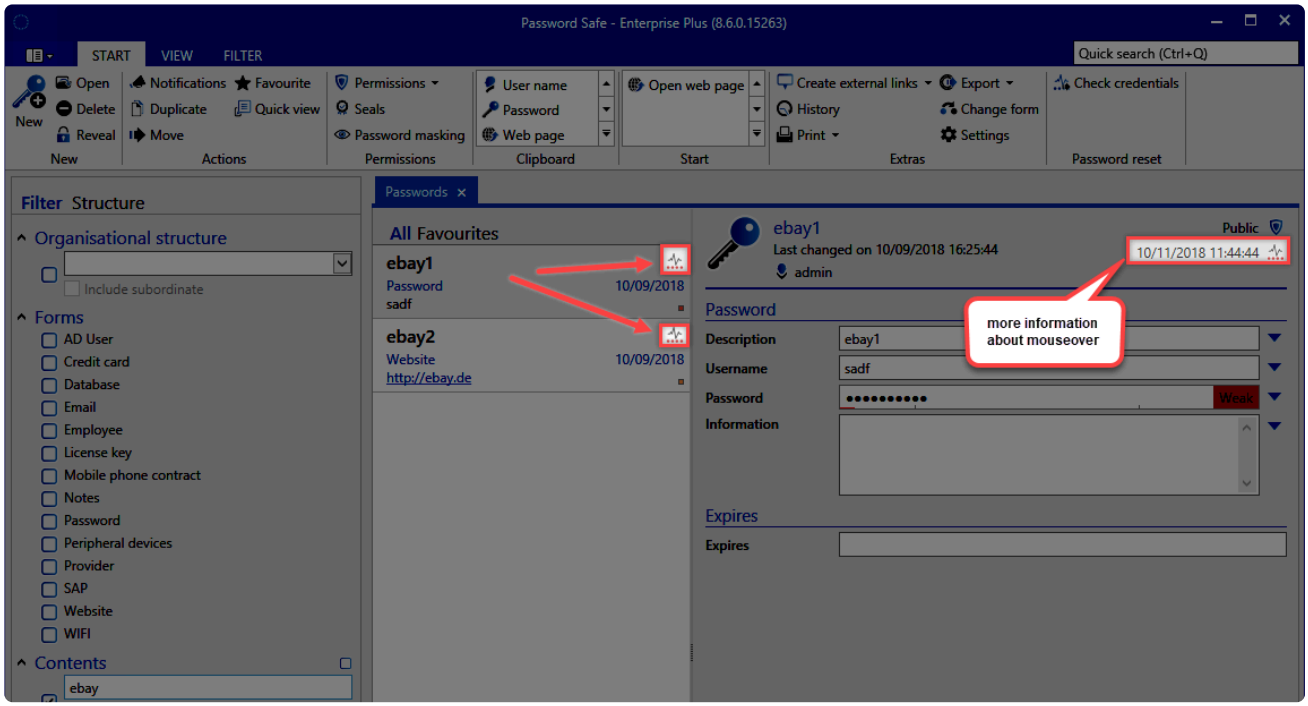
The heartbeat can be executed in the ribbon for the password module by clicking on **Check login data**. The currently marked password is always tested.

Automatic testing via the password settings

It is also possible to configure the heartbeat to run cyclically. It can be configured either via the global settings or directly in the password settings.

Results of the tests

The results of the test can be viewed in the **passwords module**.



The date when it was last executed can be seen at the top of the reading pane. The success of the testing process is indicated alongside using a coloured icon. Further information can be displayed by moving the mouse over the icon.

The icon has three different versions. These have the following meanings:

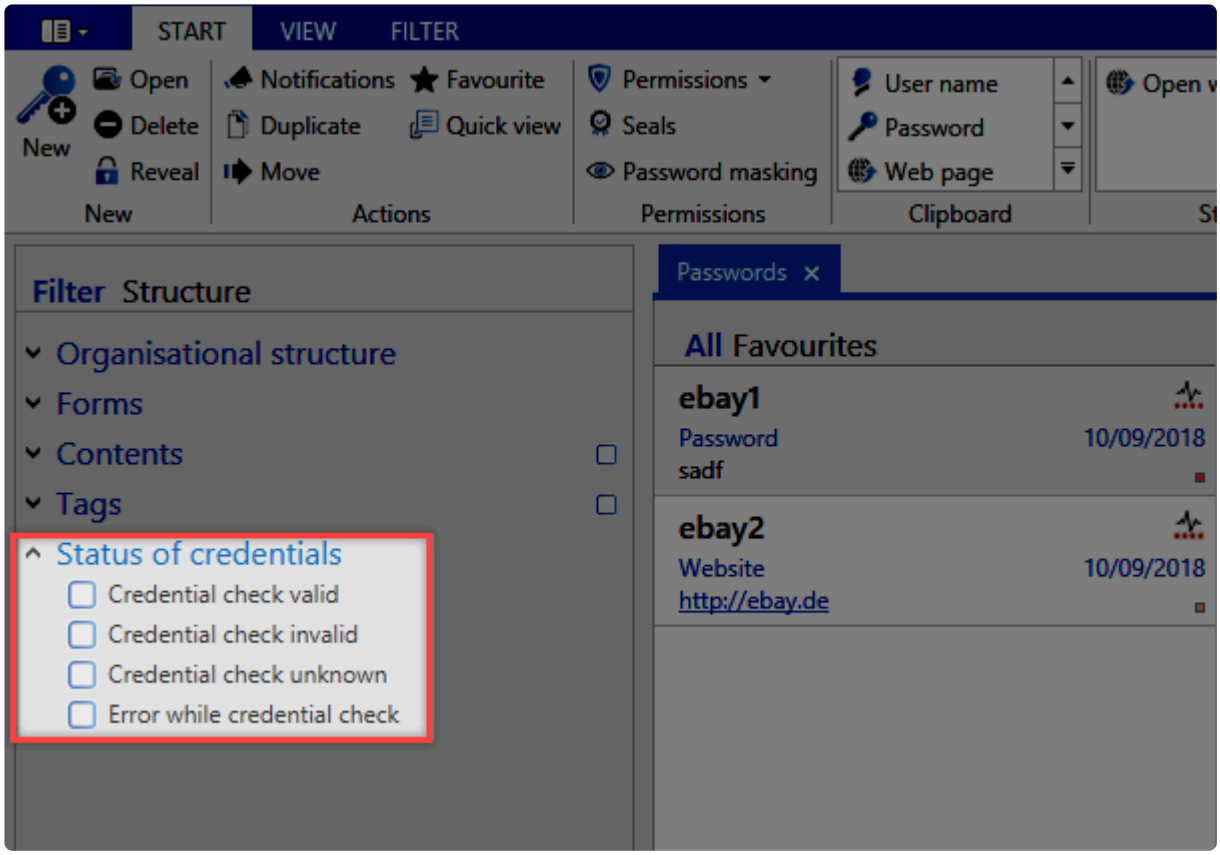
The last test was successful. The password is correct

The test could not be performed. For example, the password could not be reached.

The last test was completed. However, the password is different to the one on the target system.

Filtering the results

The filter can be configured using the filter group **Status of the login data** so that the tested records can be selected.


START
VIEW
FILTER
New
Open
Delete
Reveal
Notifications
Duplicate
Move
Favourite
Quick view
Permissions
Seals
Password masking
User name
Password
Web page
Open v
New
Actions
Permissions
Clipboard
Filter Structure
Organisational structure
Forms
Contents
Tags
Status of credentials
Credential check valid
Credential check invalid
Credential check unknown
Error while credential check
Passwords
All Favourites
ebay1
Password
sadf
10/09/2018
ebay2
Website
http://ebay.de
10/09/2018

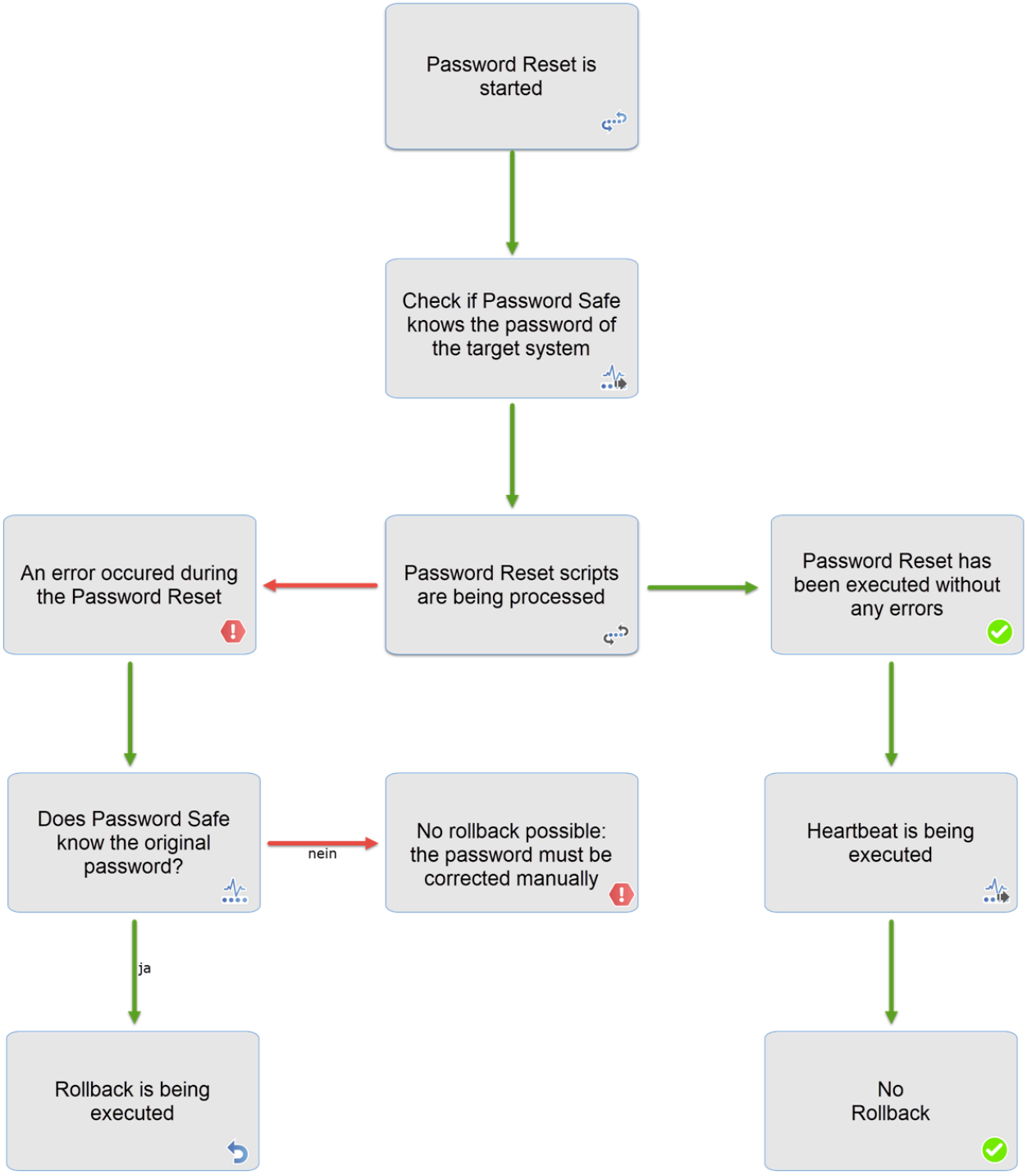
Rollback

What is a rollback?

If an error occurs while running a script, a rollback is initiated. This ensures that the original password is restored.

When does a rollback run?

The following diagram shows when and according to which criteria a rollback is initiated:



Procedure

If a rollback needs to be run, all scripts for the Password Reset are executed once again. The last password in the history is used for this process.
No new historical entry is created after the rollback.

Logbook

The logbook can be used to see if a rollback has been run and if it was successful. After a rollback, the password should be checked once again as a precaution.

Logbook entries under Password Reset

Subsequently all possible logbook entries in connection with Password Reset are listed

The password reset first checks with the first script (via the heartbeat) whether the password is correct:

Logbook Type	Logbook Record
Login data valid	Container
Login data invalid	Container
Check errors during login data	Container

Afterwards all scripts of the password reset are executed one after the other and the following logbook entries are written:

Logbook type	Logbook record
Execute	Password Reset
Execute Rollback	Password Reset
Execution Error	Password Reset
Error during rollback	Password Reset

If an attempt was made to perform a rollback, but the rollback cannot be performed because the old password was incorrect before the reset, or the first script is of the type “user-defined”, the following logbook entry is written:

Logbook type	Logbook record
Error during rollback	Password Reset

If a password reset has failed and an attempt is made to perform a rollback, the reset is blocked for one day and the following logbook entry is written: (It does not matter if the rollback worked or not)

Logbook type	Logbook record
Password Reset blocked	Password Reset

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 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

Password Safe offers the solution to this problem: The security of the network can be significantly increased using a combination of **Discovery Service** and **Password Reset**. 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 three 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.

Requirements

Availability

The **Discovery Service** is exclusively available in the **Enterprise Plus Edition**.

Relevant rights

The following options are required to use the discovery service:

User rights

- Show discovery service module
- Can manage discovery service system tasks

Requirements

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 be a member of admin for the corresponding group of domains. Otherwise, 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 section 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 section 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

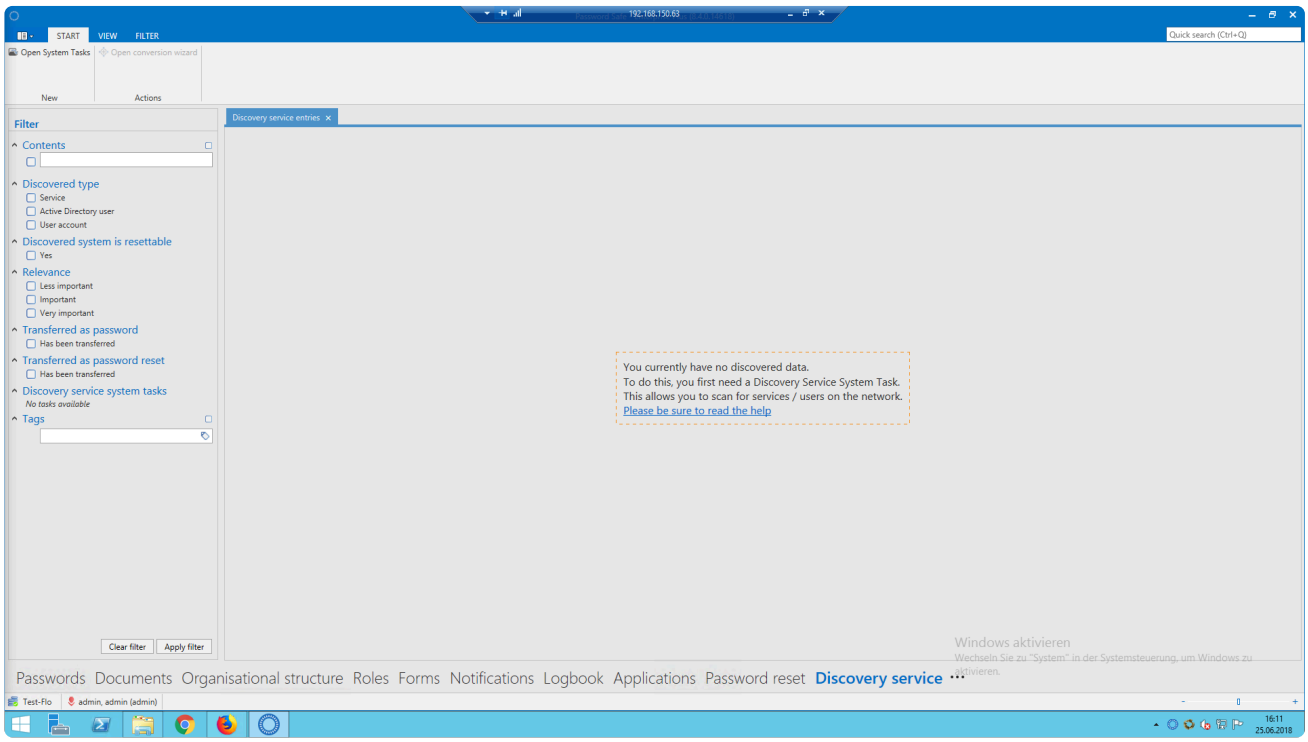
Computer name (Hostname):

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**. 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.

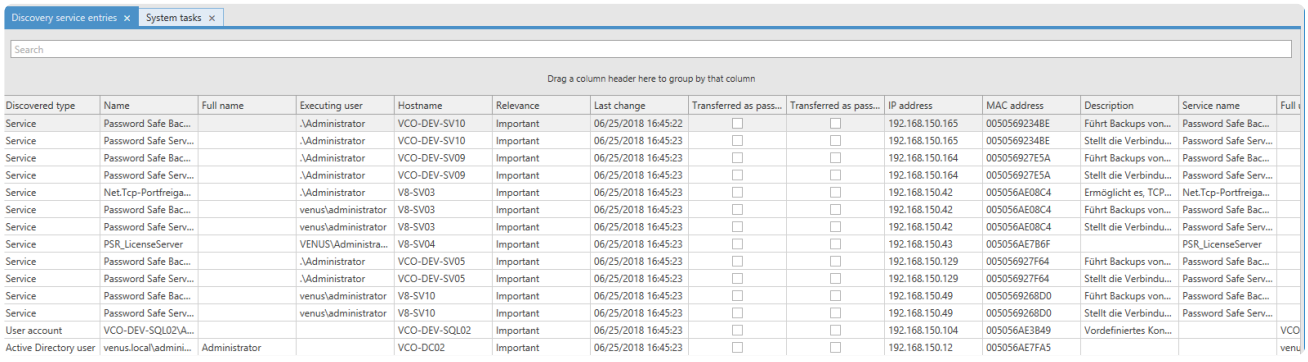
Configuration

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**.



Once a **System Task** has been completed, the data discovered during the search is listed in a table:



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	0050569234BE	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.

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:

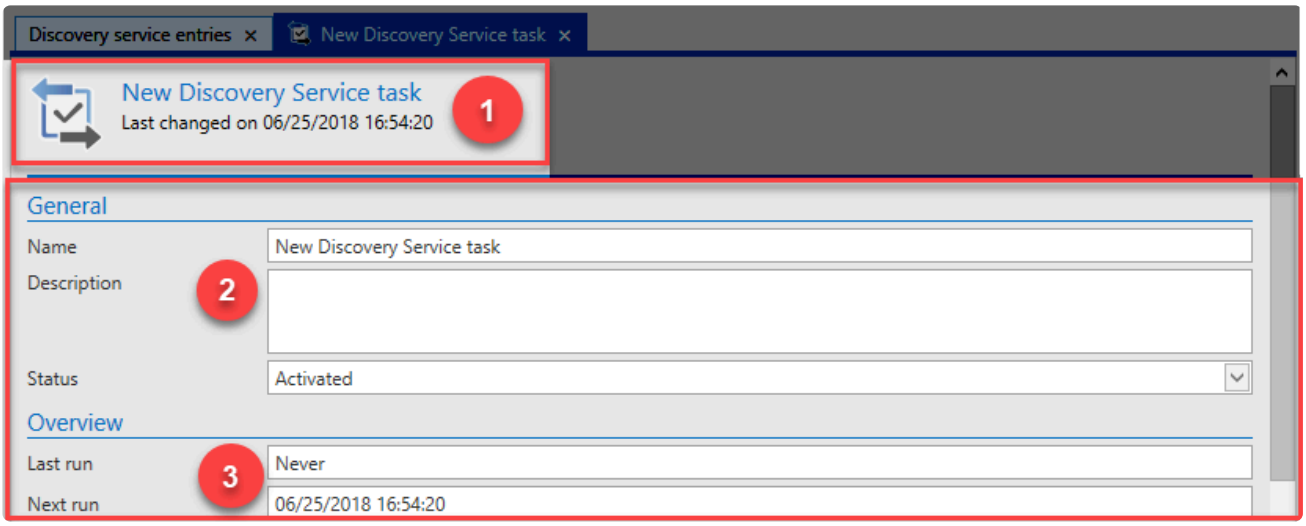
- Service accounts
- Active Directory users
- User accounts

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**.

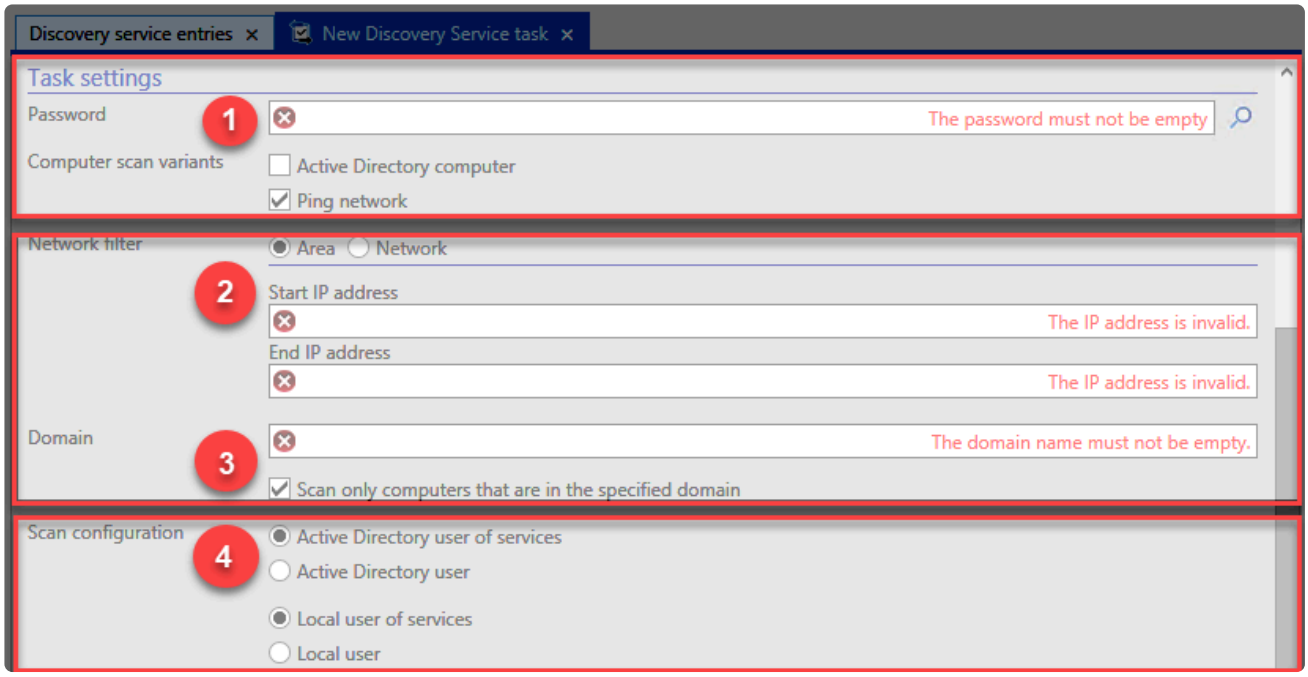


1. Shows information about the **Discovery Service Task**.
2. In the **General** section, the name of the **Discovery Service Task** is entered (optionally with a description).
   The **Status** is always set to **Activated** by default but it can also be set to **Deactivated** in the configuration.
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.

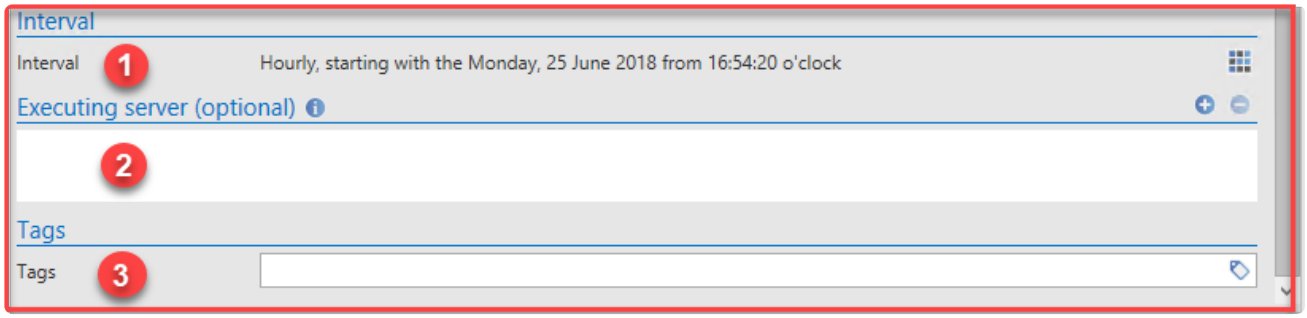


1. **Password** and **Computer scan variants:** The required password must already have been issued and it requires corresponding rights for the domain.
   Active Directory computer: Only those computers that are in Active Directory are scanned (there is also the option of using it individually or pinging 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.



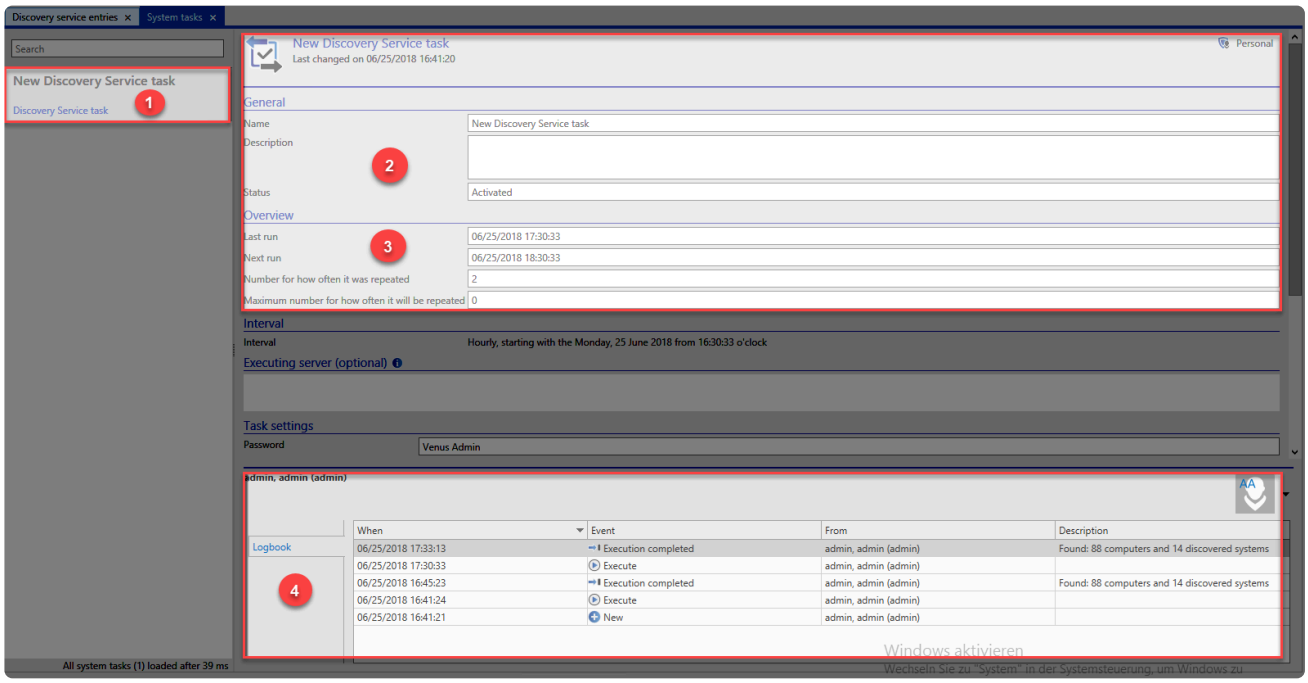
1. **Interval:** The interval at which the **Discovery Service Task** should be executed is defined here. The default setting is hourly, one year after adding the **Discovery Service Task**. The interval can be adjusted in minutes or set to be executed only once (optionally with an end date).
2. **Executing 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. The system then 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**.



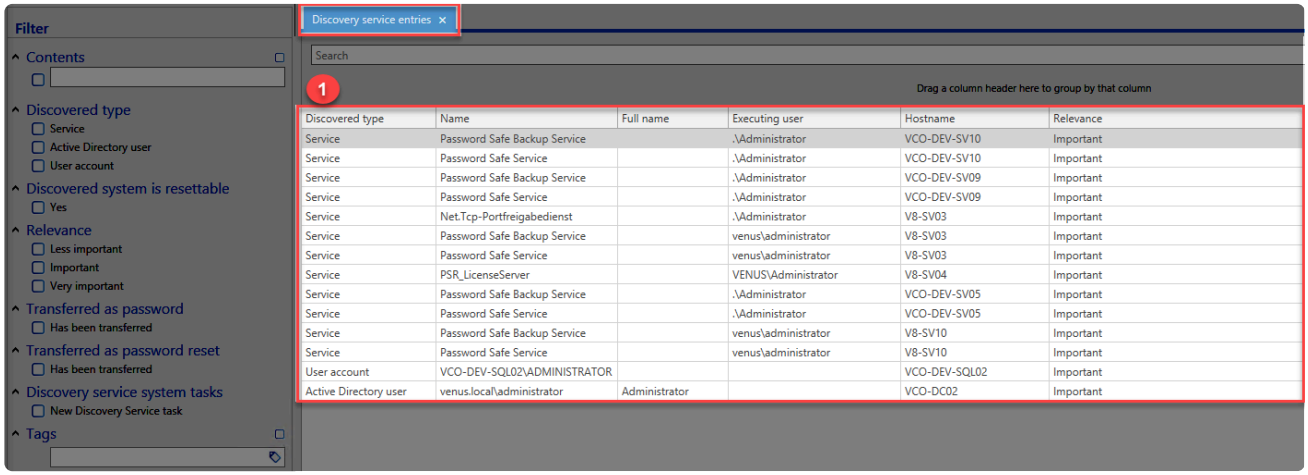
The **Discovery Service Task** needs to be carefully configured. The configurable sections are described below.

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

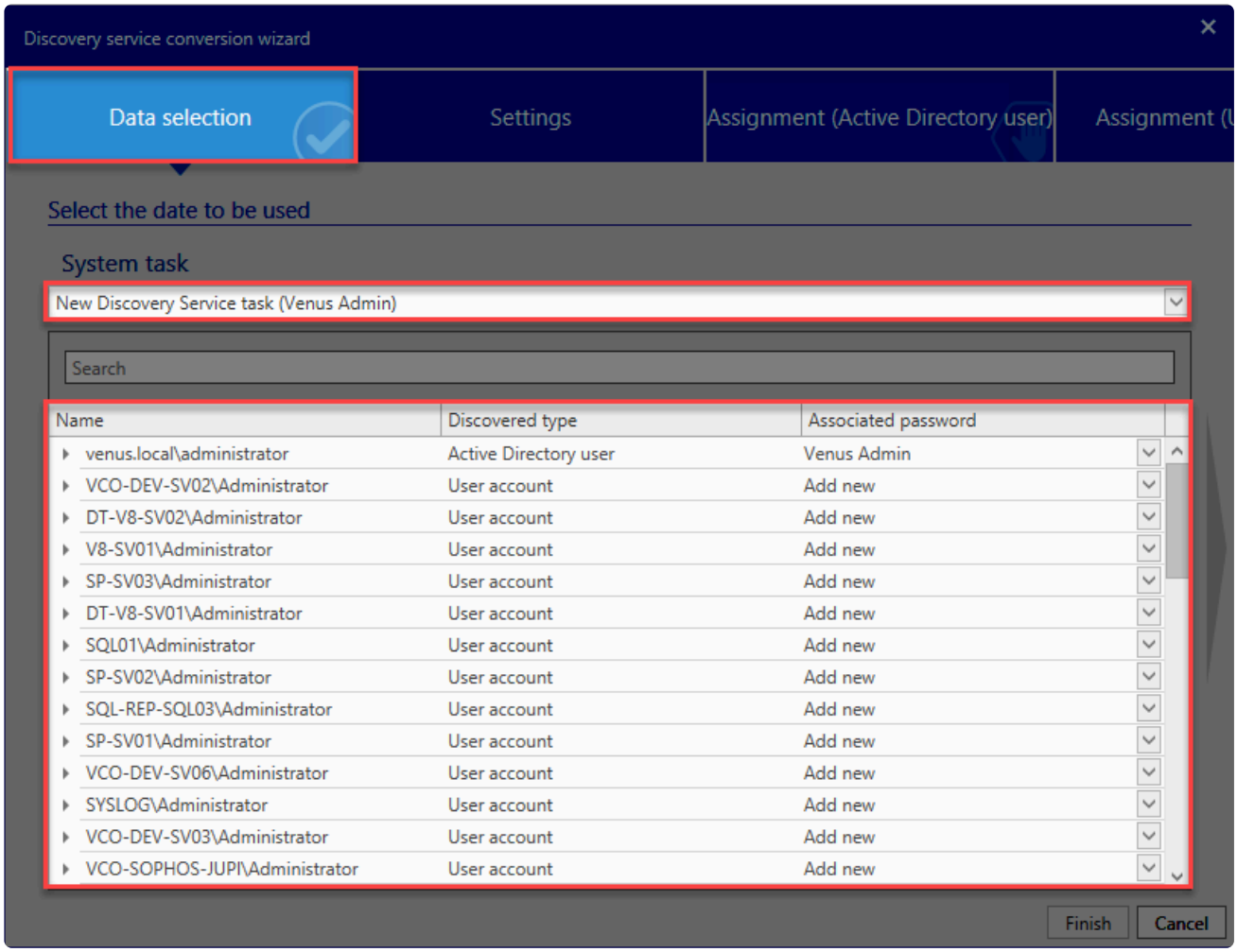
The successful execution of a **Discovery Service Task** is a requirement for the **Discovery Service entries**. The discovered data is listed in table form in the **Discovery Service module** and can be correspondingly organised using the **Discovery Service System Task** filter.



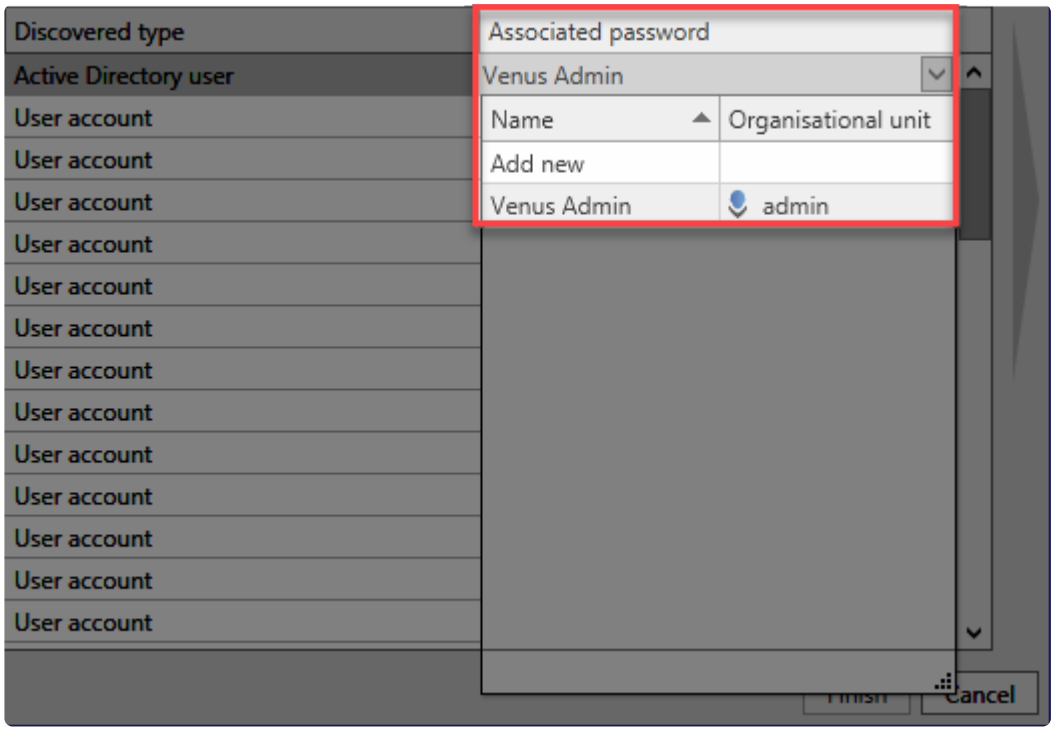
1. In this section, the **Discovery Service entries** that were discovered by the **Discovery Service Task** and selected for the **Conversion Wizard** are displayed.

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**.



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.

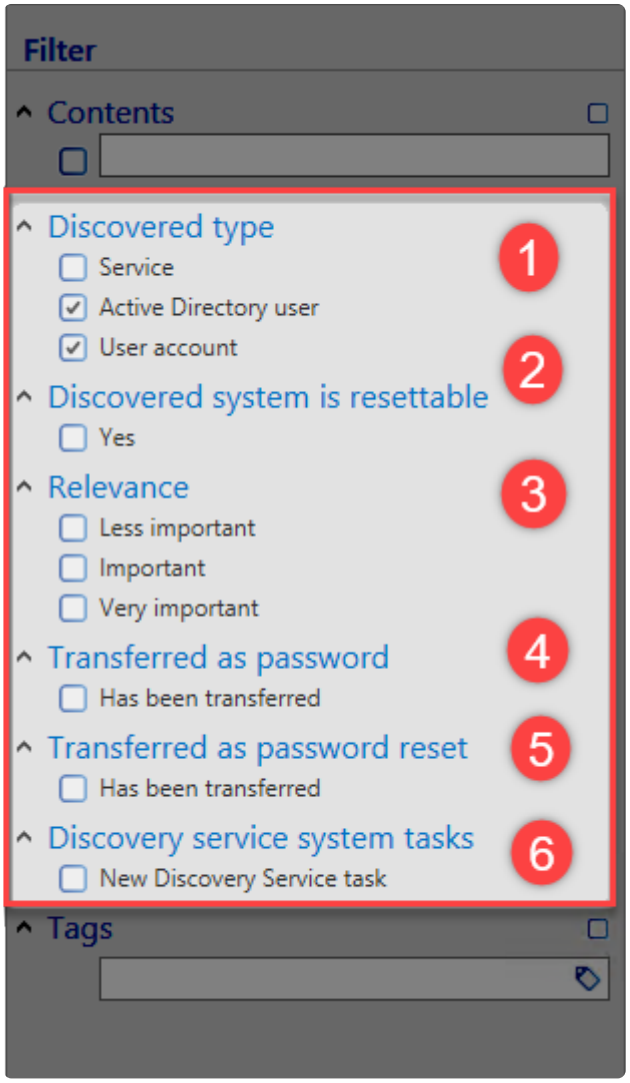


For **Active Directory users**, it is possible to assign an existing **password**.

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:



Description of the **filter with the special options for the Discovery Service entries:**

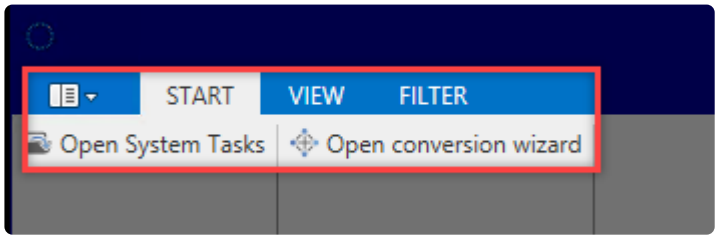
1. **Discovered type** The discovered entries can be filtered here according to their type.
2. **Discovered system is resettable:** Indicates whether a Password Reset can be created from the discovered data.
3. **Relevance:** Grading the importance of the discovered system.
   A high relevance means 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**.



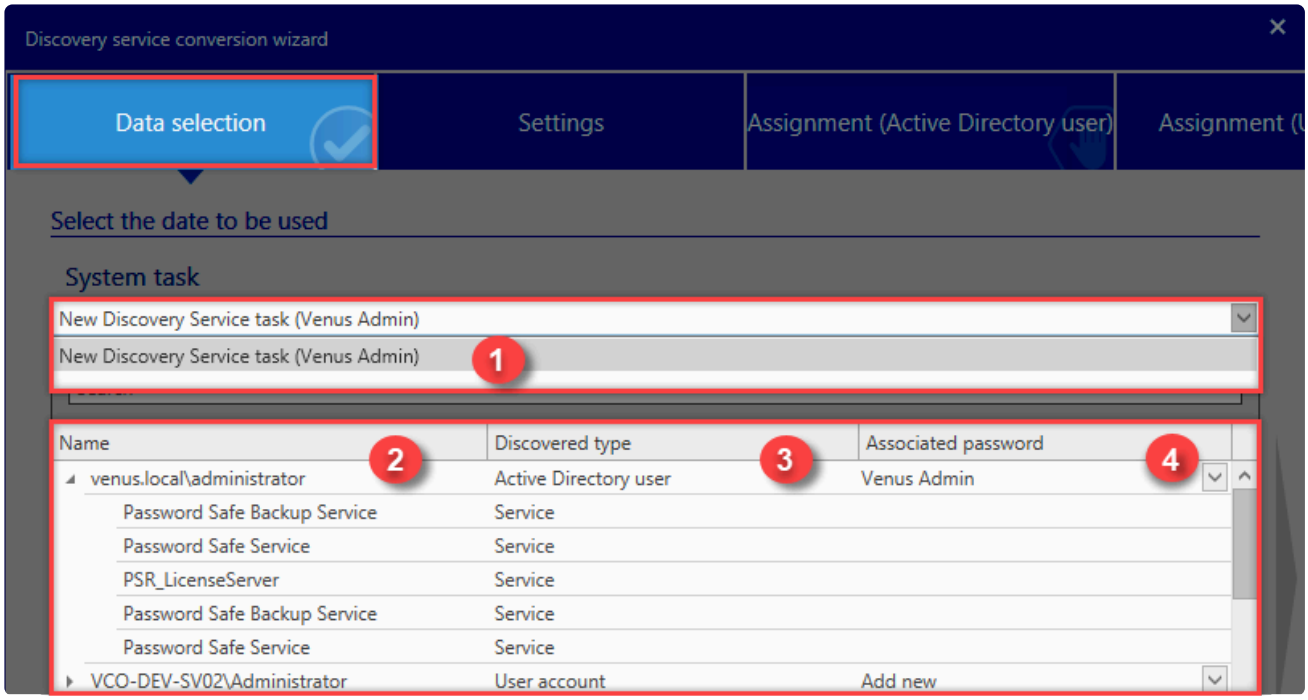
After the **Discovery Service Task** has been successfully executed, the entries are available in the **Discovery Service**. Further processing of the entries is then carried out using the **Conversion Wizard**.
For processing in the **Conversion Wizard**, the network is scanned for the following types:

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

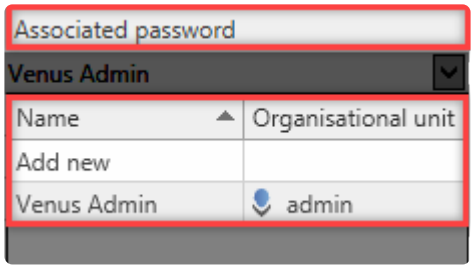
In the **Discovery Service** table, the user selects the entries for which he wants to add a **Password Reset** or **password**. The user then clicks on the **Conversion Wizard** and the **Discovery Service Cinversion Wizard** opens for further editing.



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.

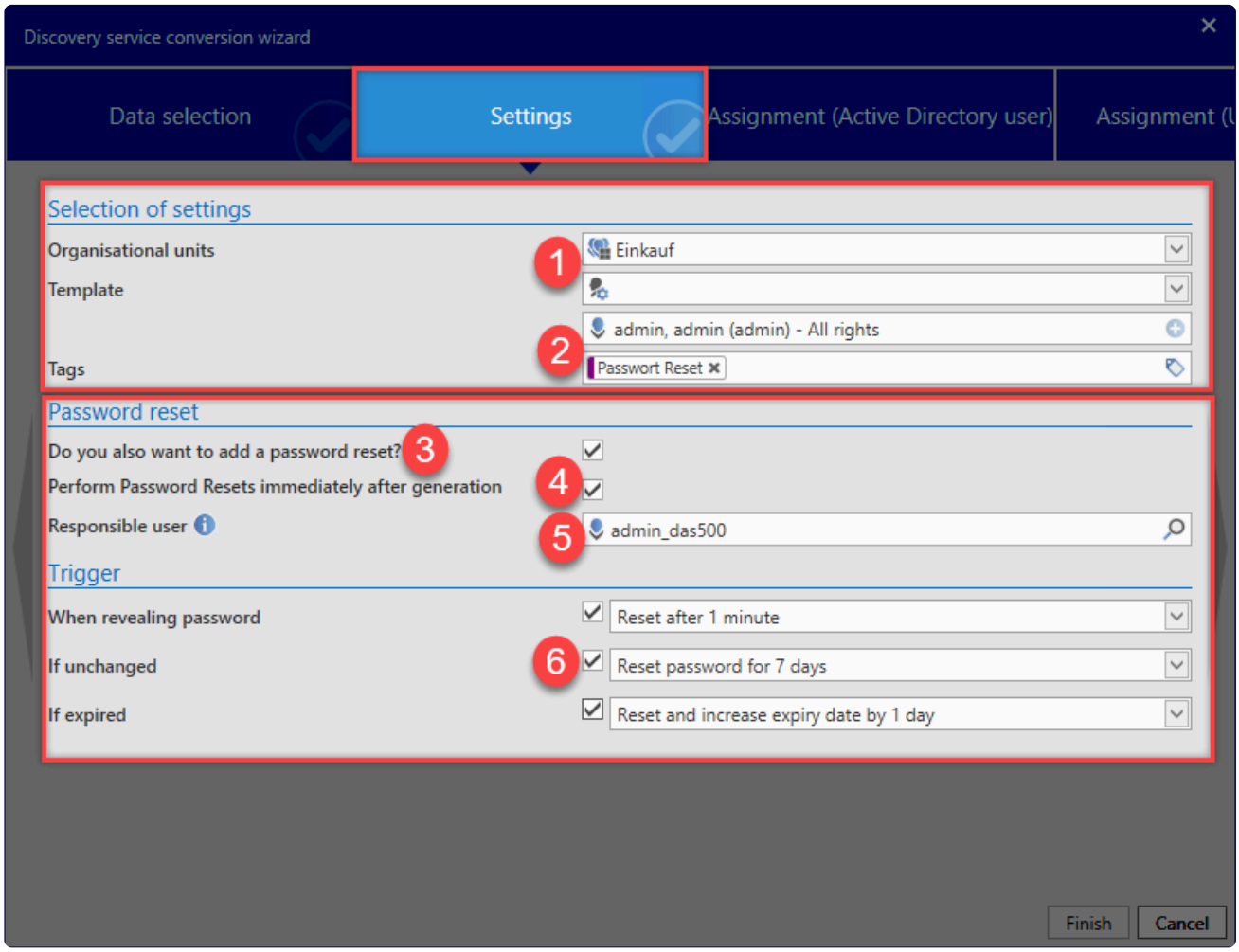
The following image shows the options **add new password** or retain **existing password**.



In addition, the **organisational unit** in which the existing password is located is displayed.

Settings

The **Password Reset** is configured in the **Settings** Ribbon.

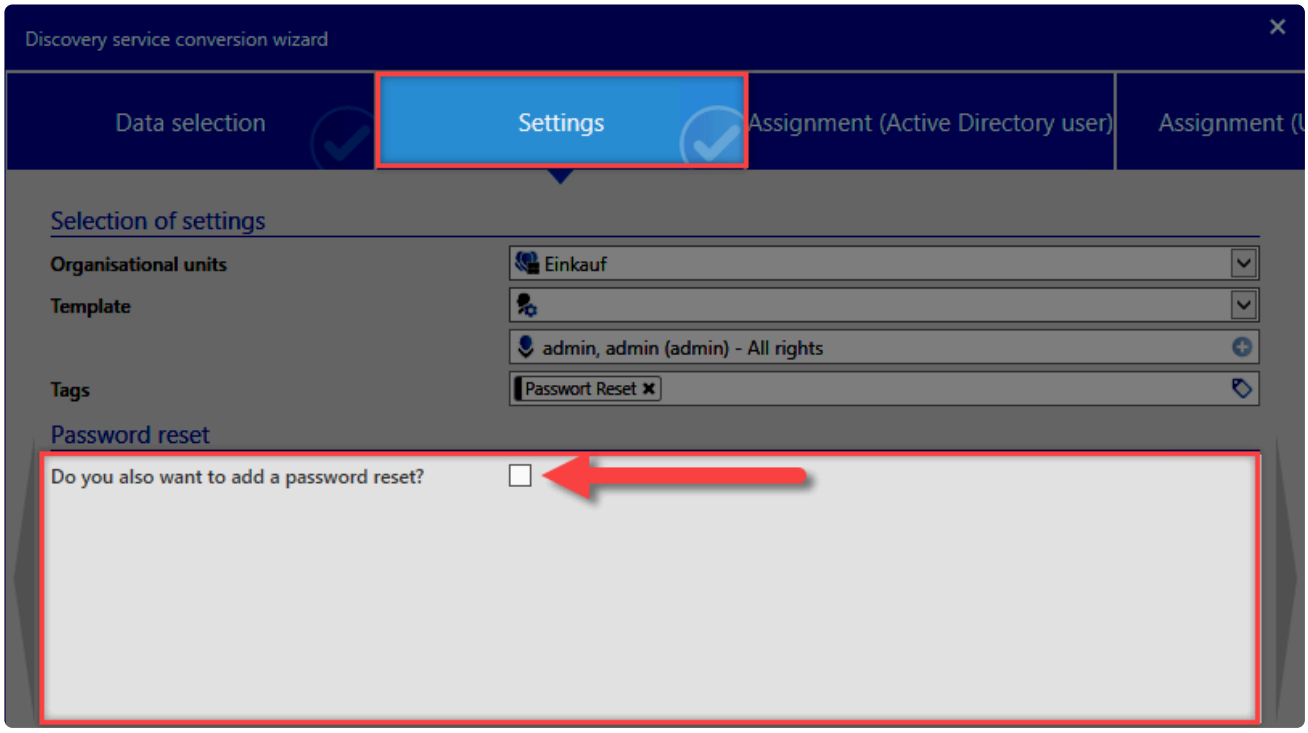


The **settings** will be described in more detail below:

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.

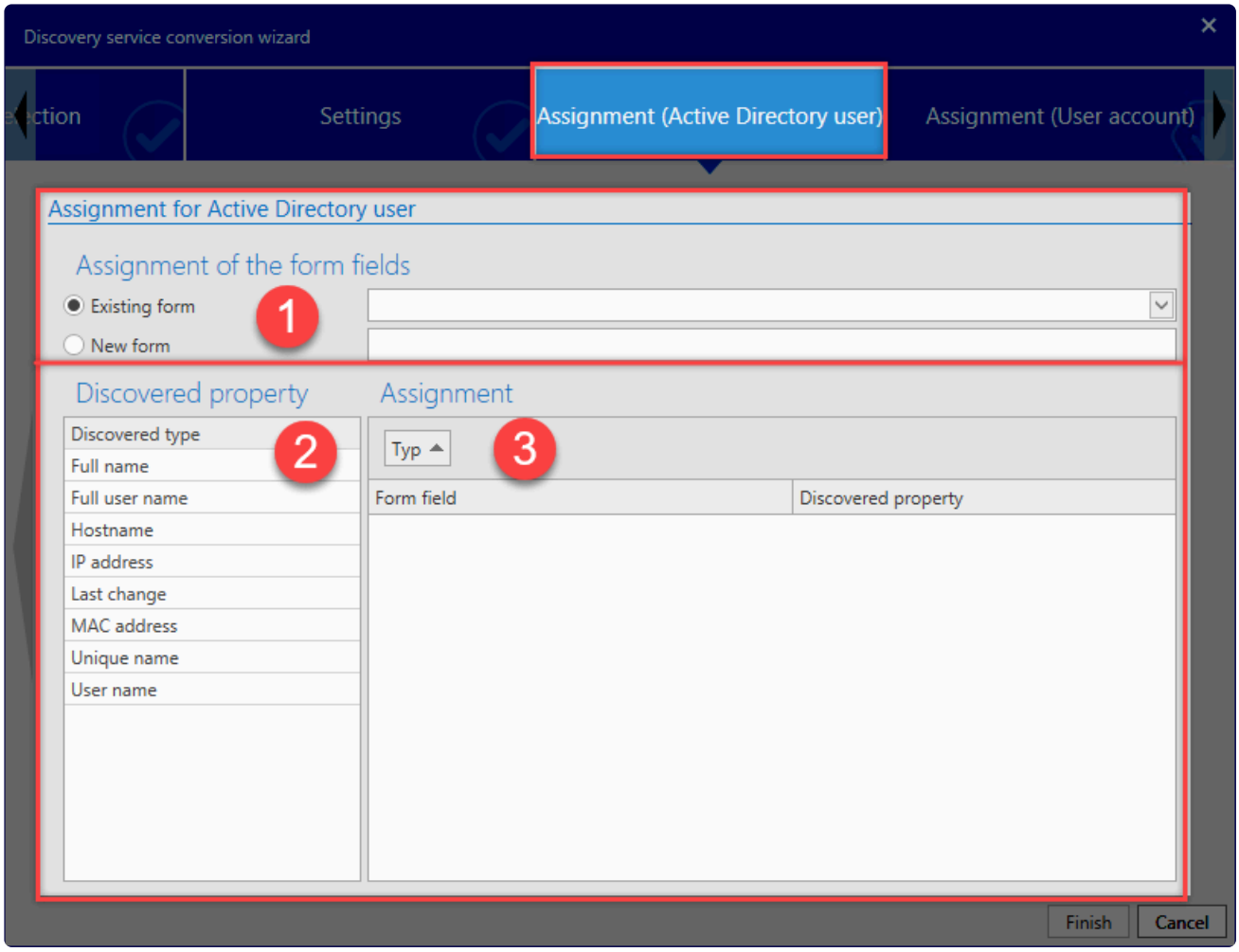


> ! After clicking on **Finish**, one or more **passwords will be created** but **no corresponding Password Resets will be created!**

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.

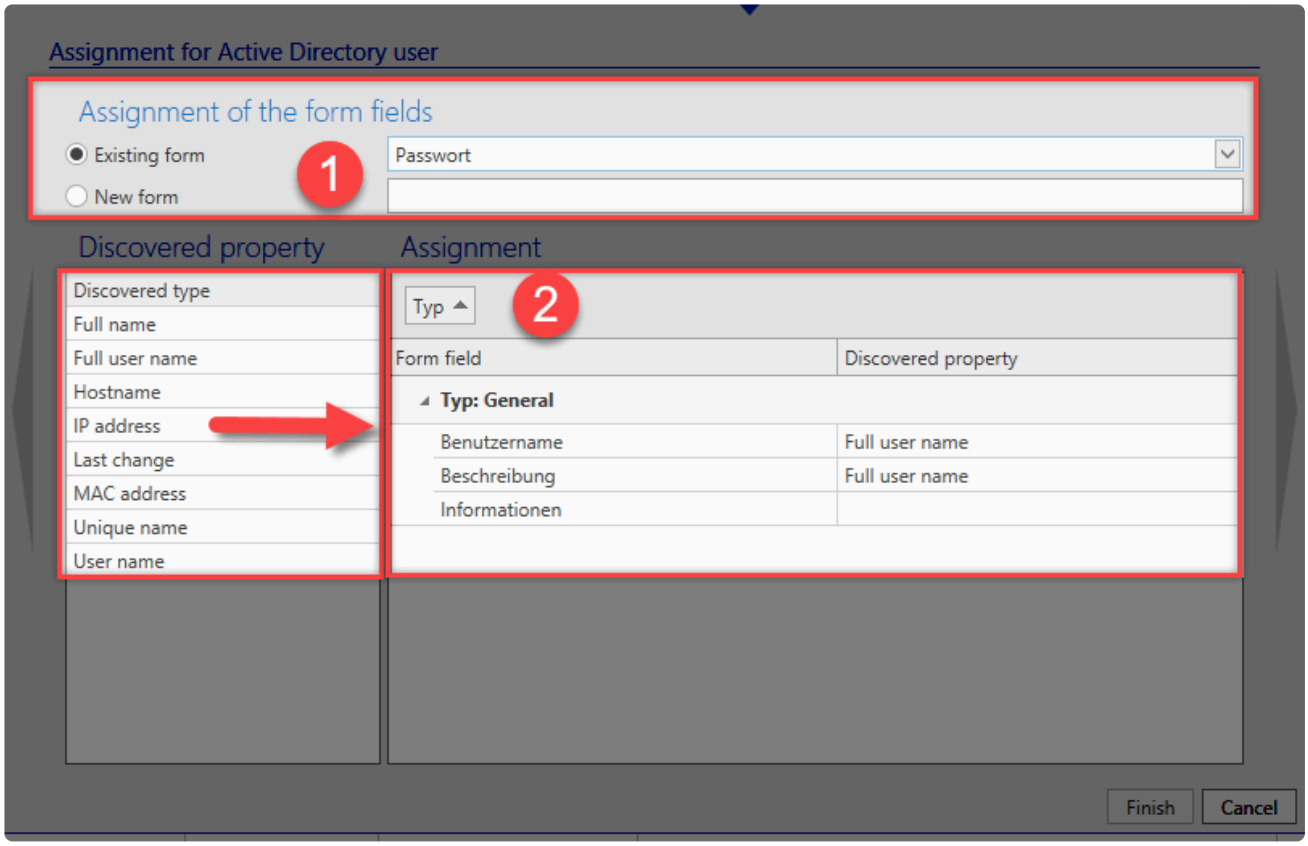
The following images shows the **Assignment (Active Directory user)** Ribbon



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

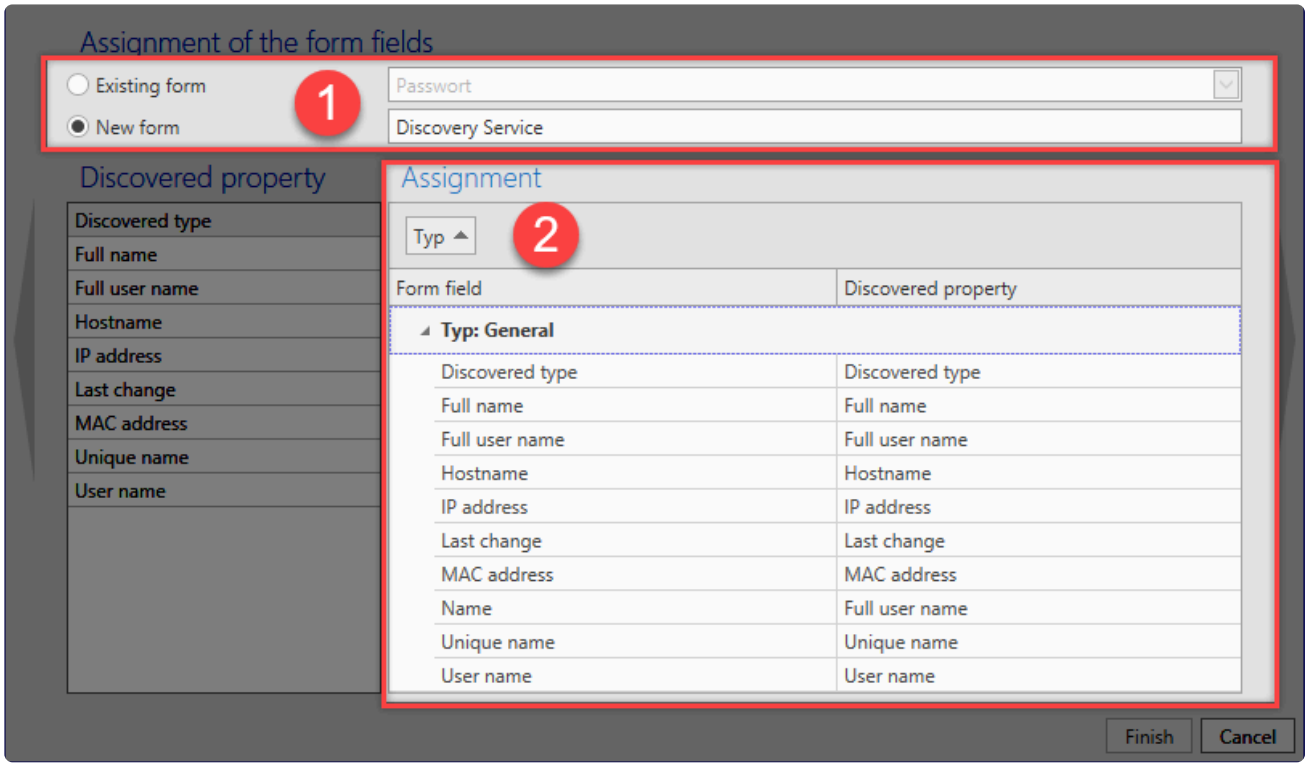
“Existing form” selected



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

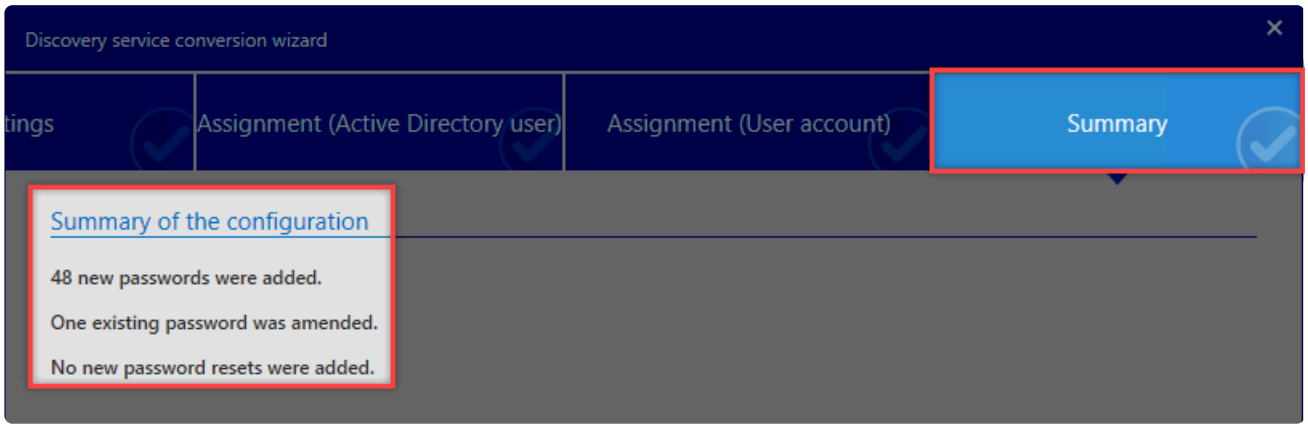


Procedure:

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**.



Confirmation prompt

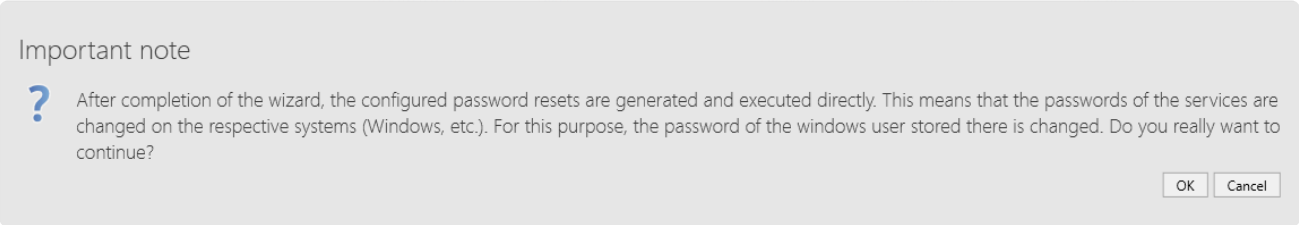
An important aspect of **Password Safe V8** is the **security** of passwords on systems. In the **Discovery Service**, a **security measures** is thus triggered at the **last step** for creating **Password Resets**.
If the option **Execute Password Resets immediately after they are created** is used 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.



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!**

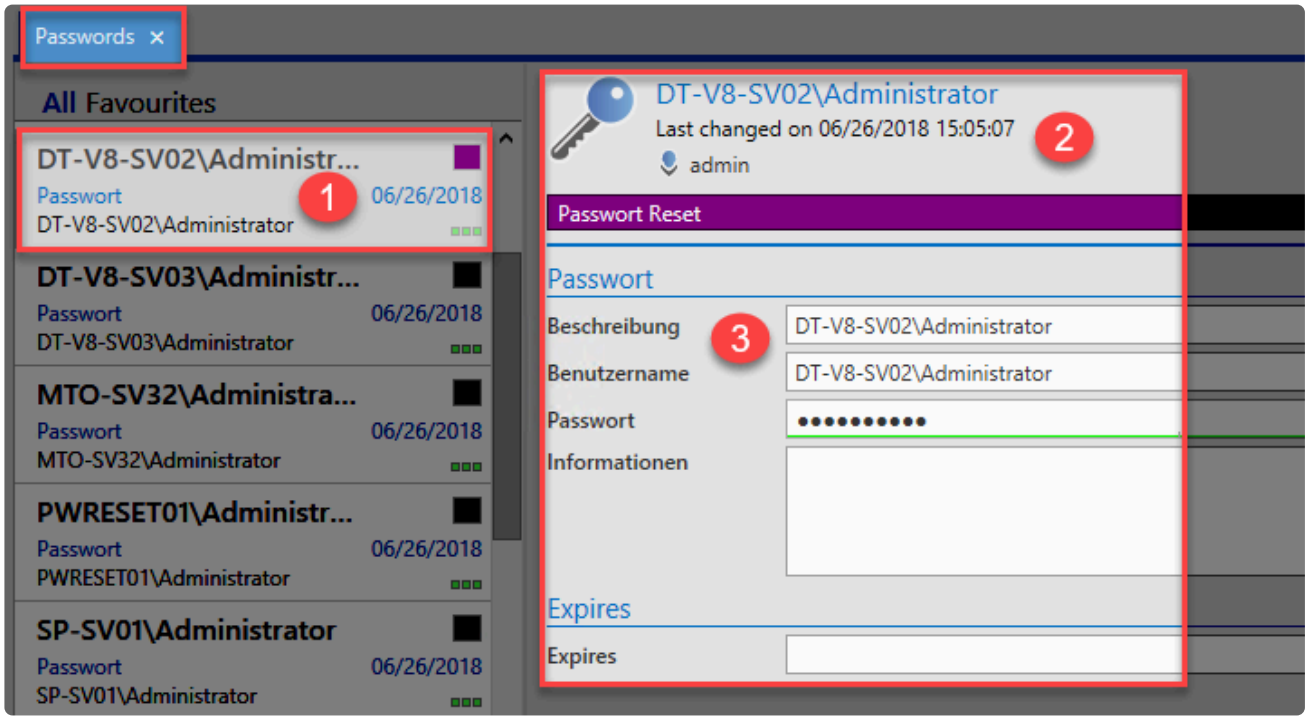


After **entering the displayed number** and **confirming with OK**, the process is **executed immediately** and the **Password Resets** are carried out and the **associated passwords changed**.

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.

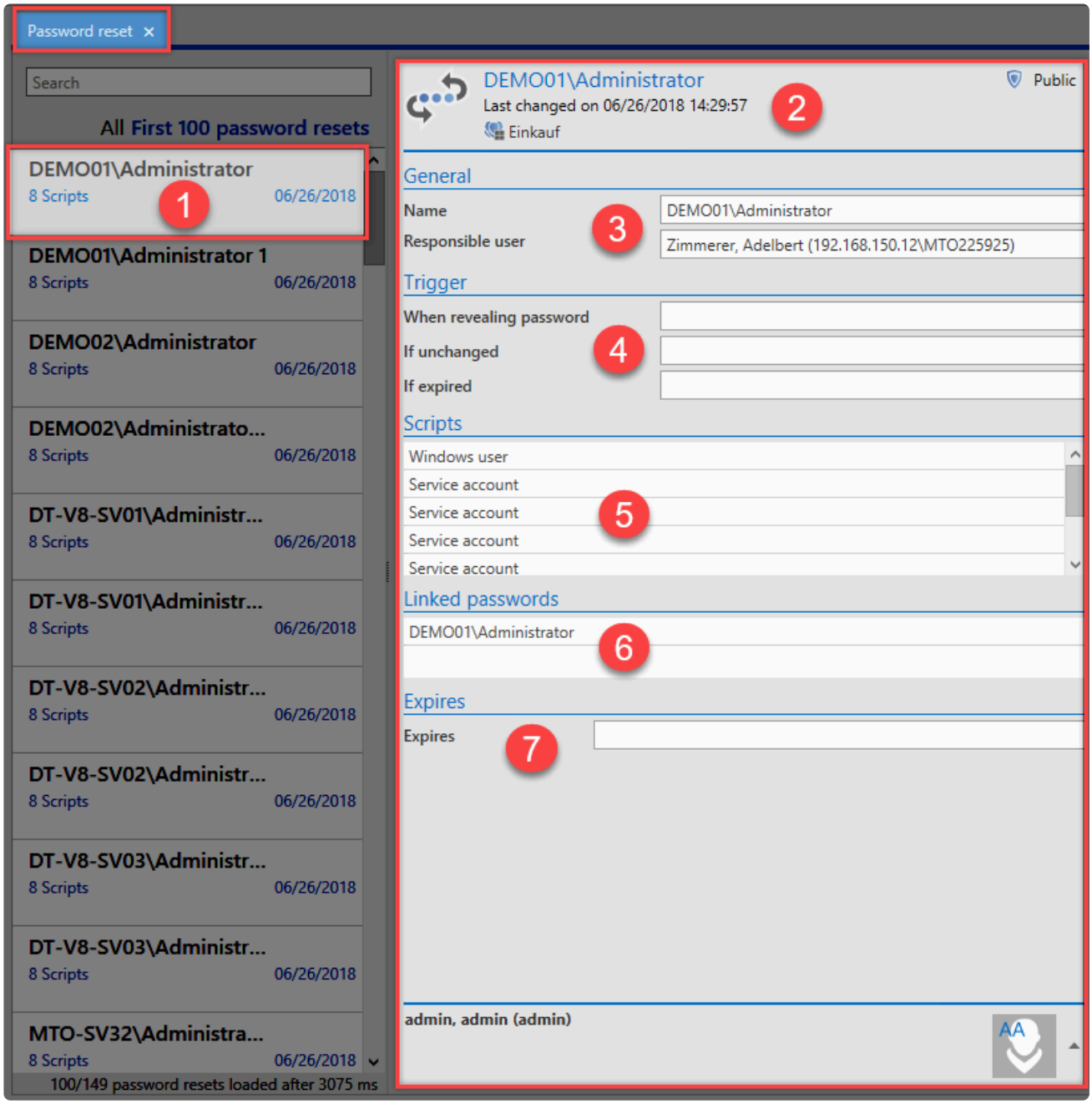
Password



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.



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)

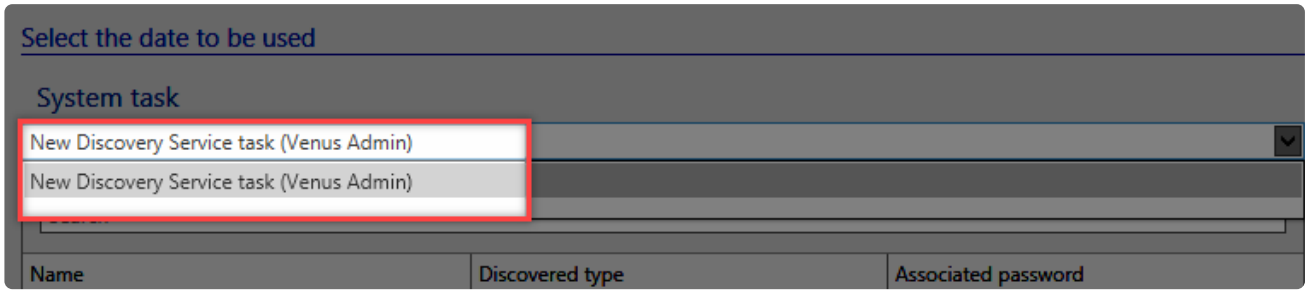
This data can then be used to create a **Password Reset** for the user for the discovered **Discovery Service entry**.
The **Password Reset** is activated via the corresponding trigger that has been set.

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**.



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

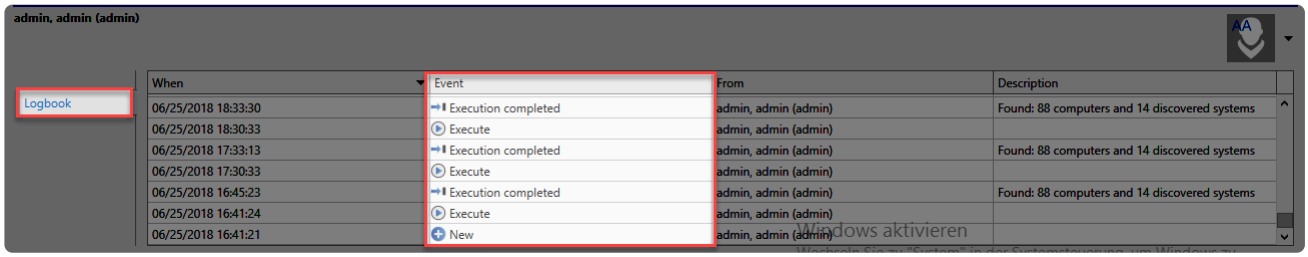
Task B

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



The following **events** are displayed in the **logbook for the footer** and in the **logbook module**:

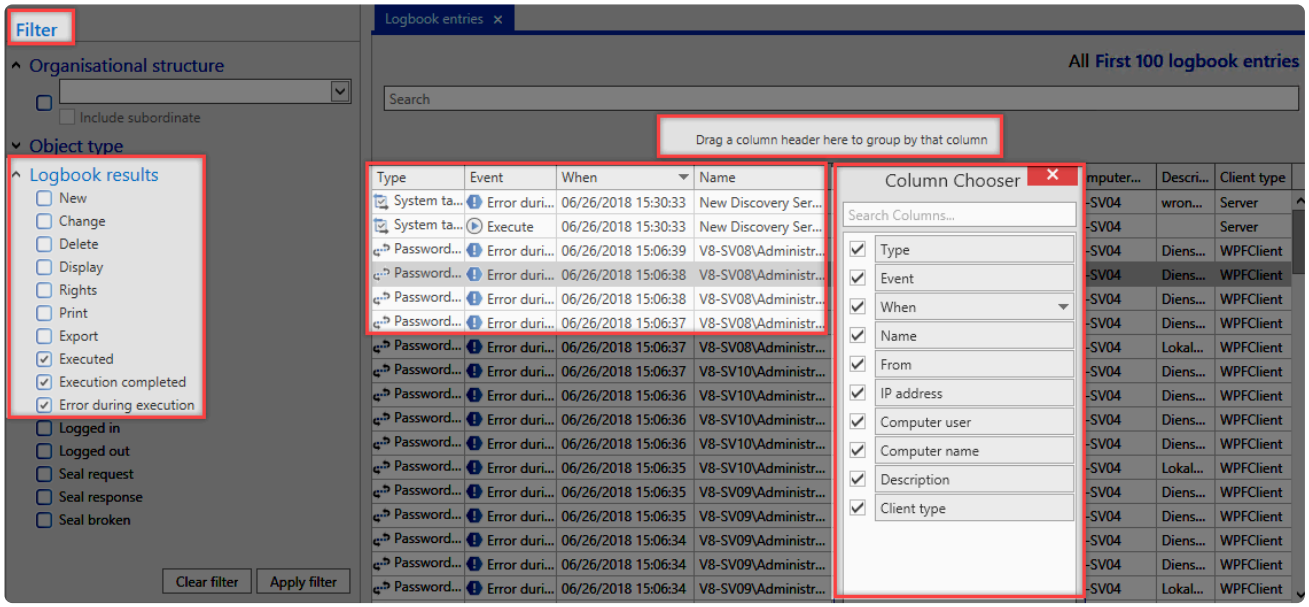
1. New
2. Change
3. Execute
4. Execution completed
5. Error during execution

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.



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.

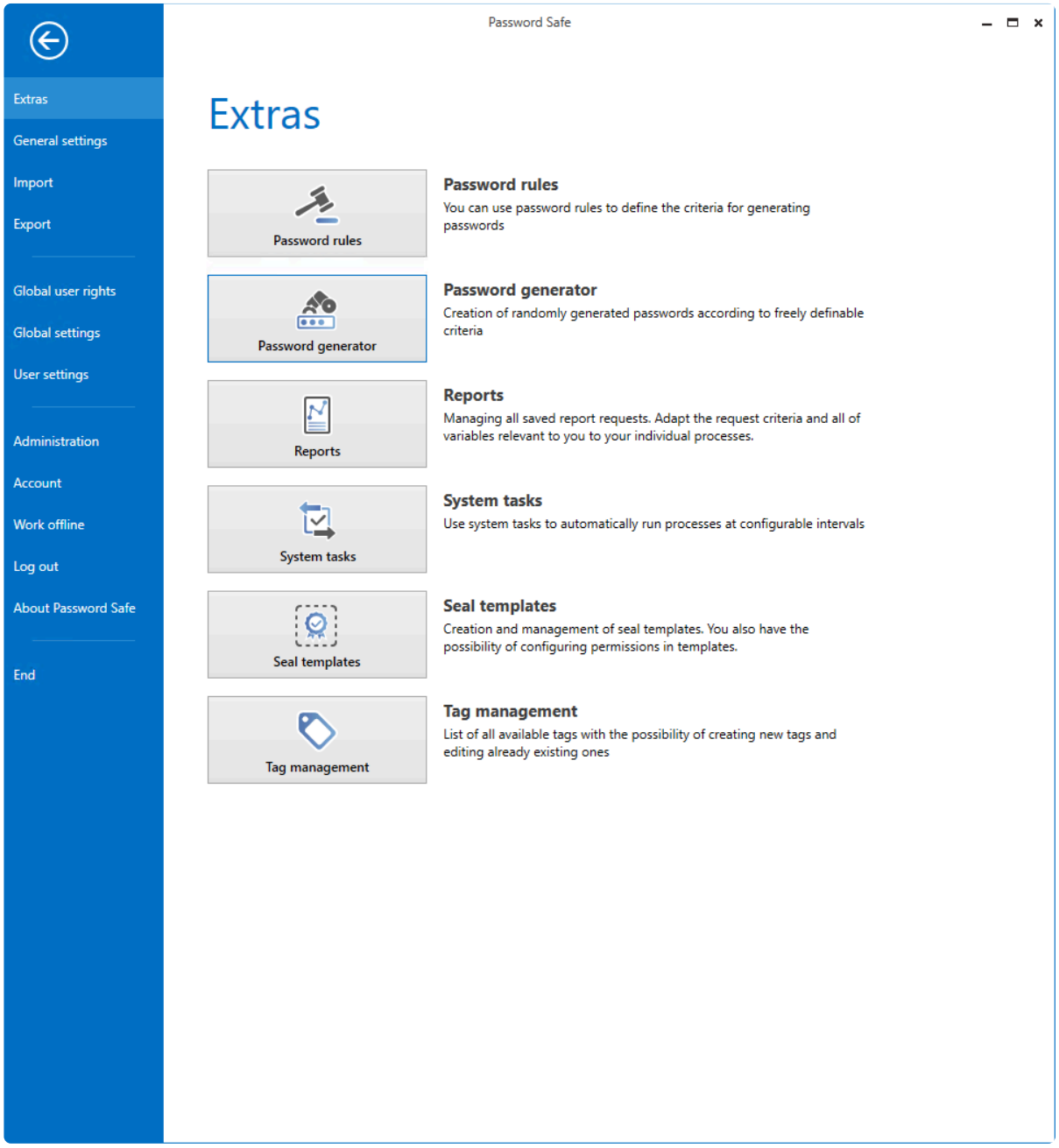


The column editor can be used to arrange and display the data in the table according to their importance.

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.



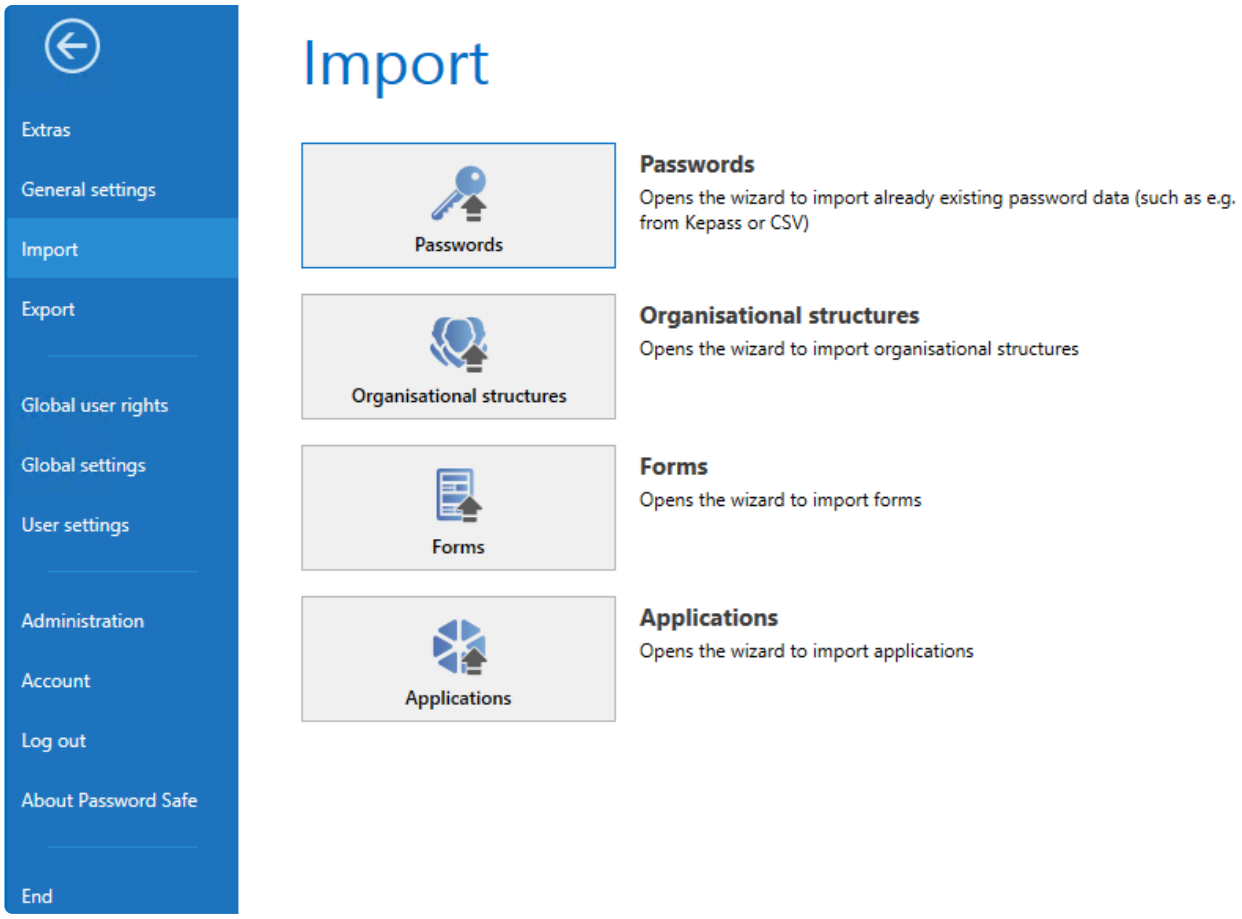
- Extras
- General settings
- Import
- Export
- User rights
- User settings
- Administration

- Account

Import

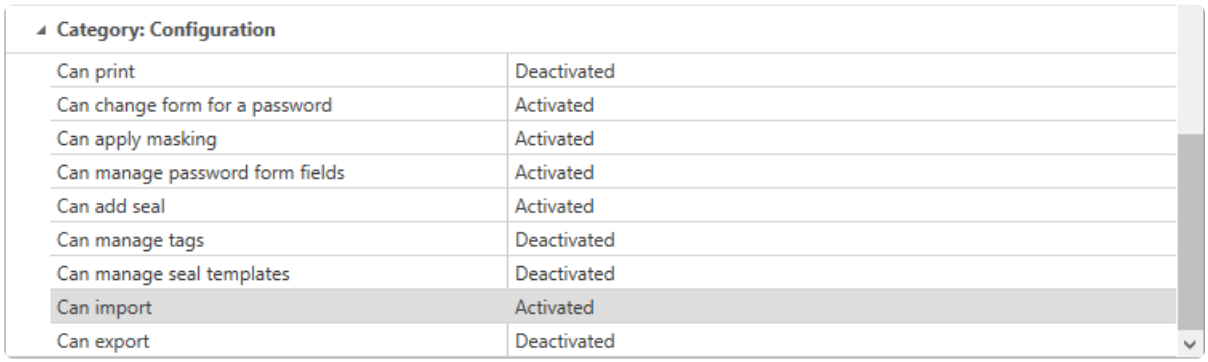
What is an import?

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.



Requirements

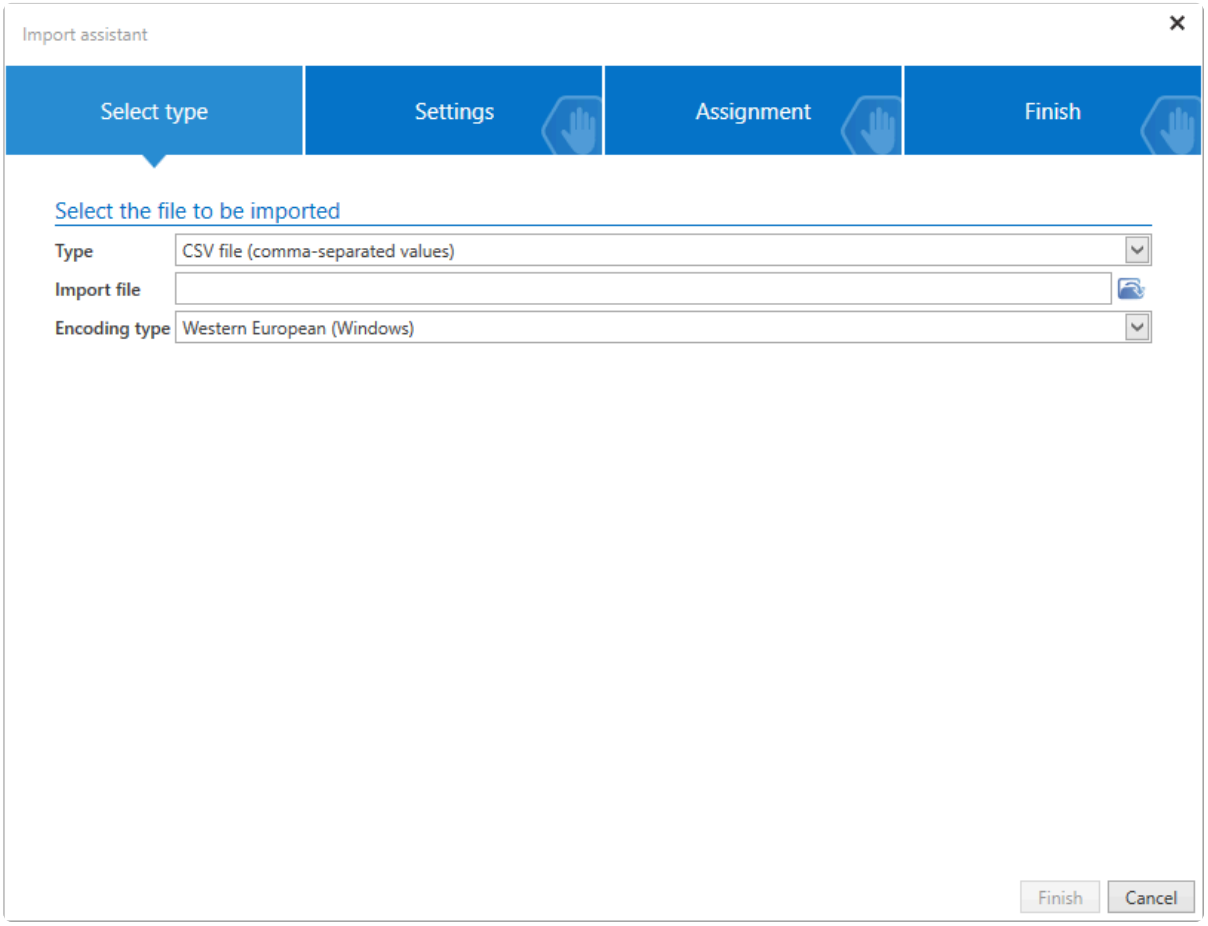
Whether the user is permitted to import data is controlled by the corresponding user right.



The import wizard

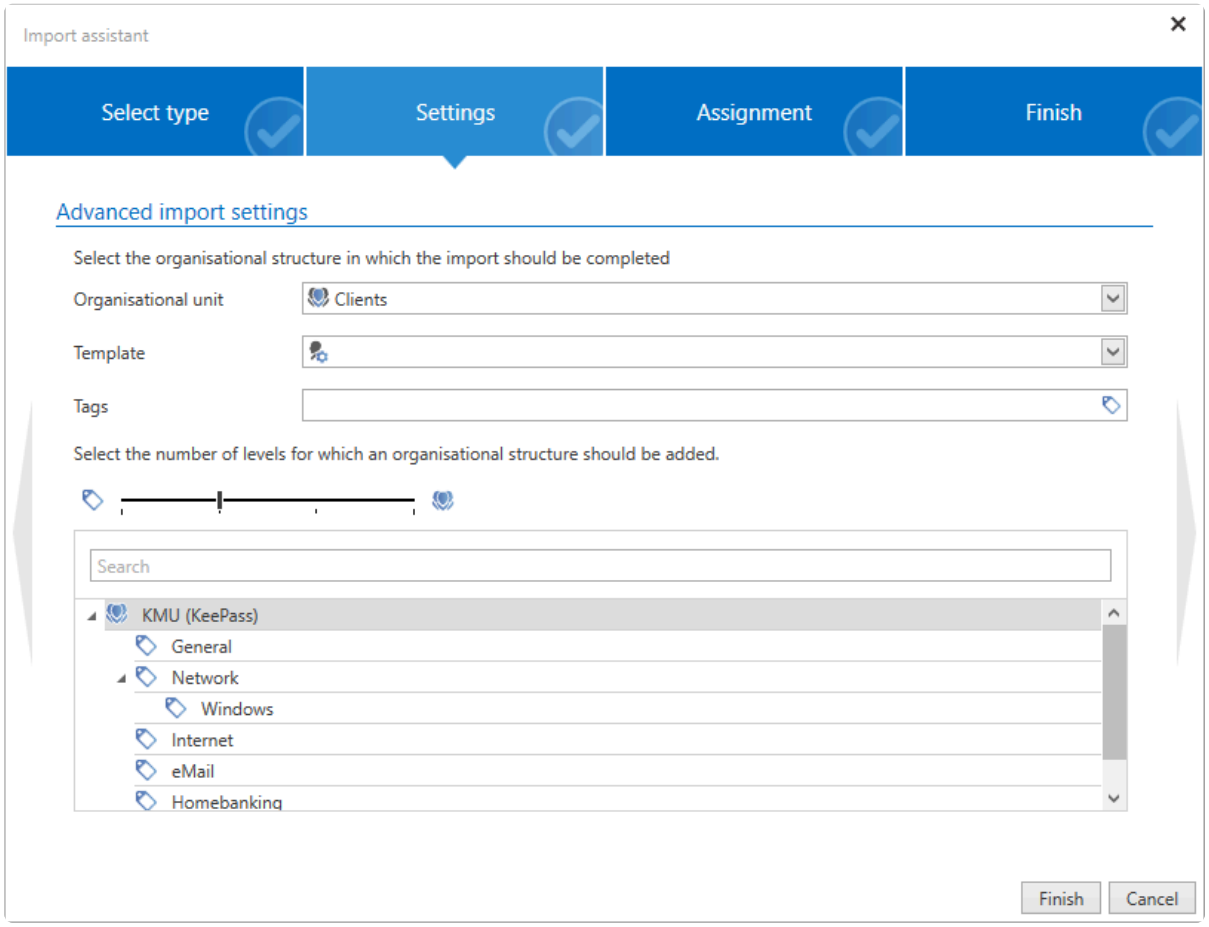
The wizard supports the import of data into Password Safe in four steps.

Select type



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.

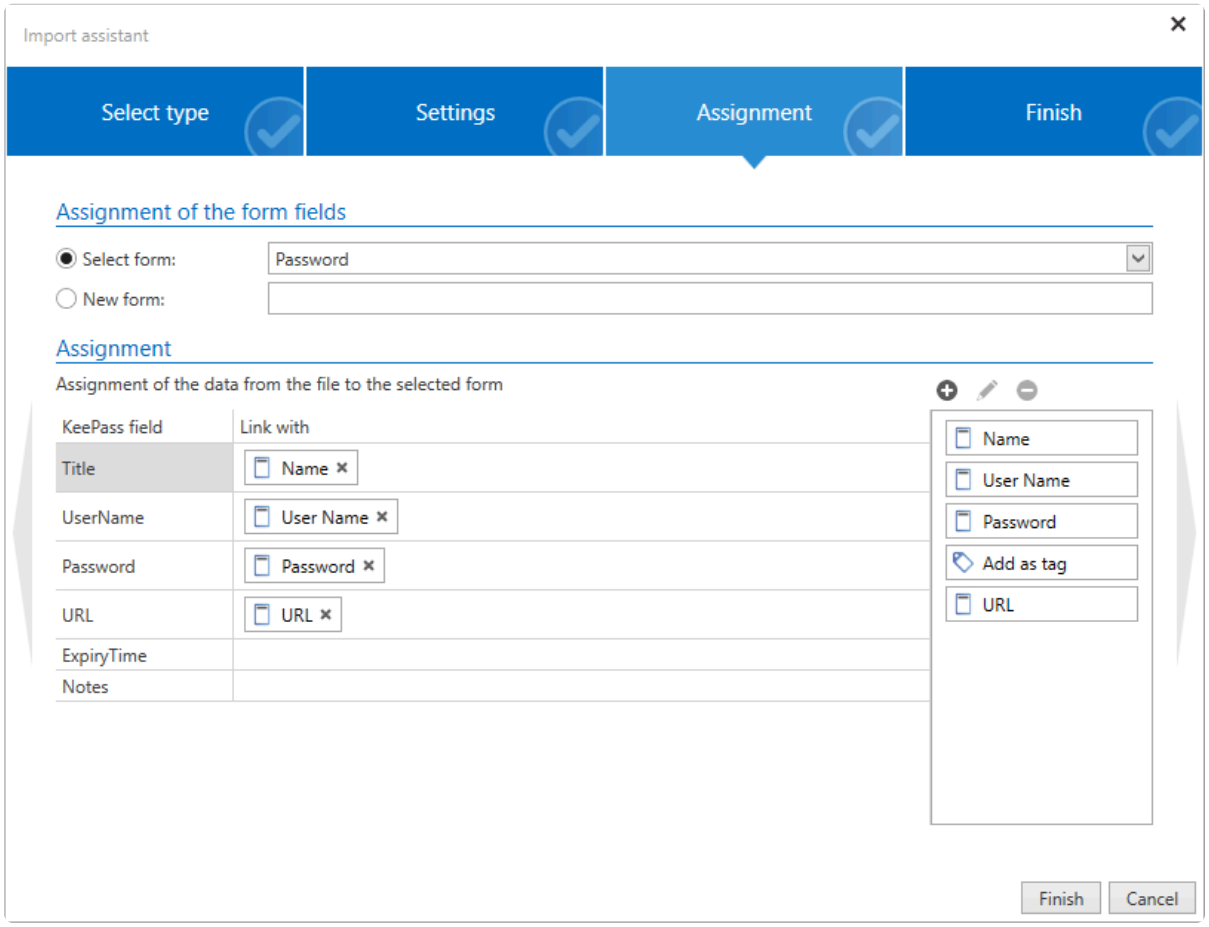
Settings



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.

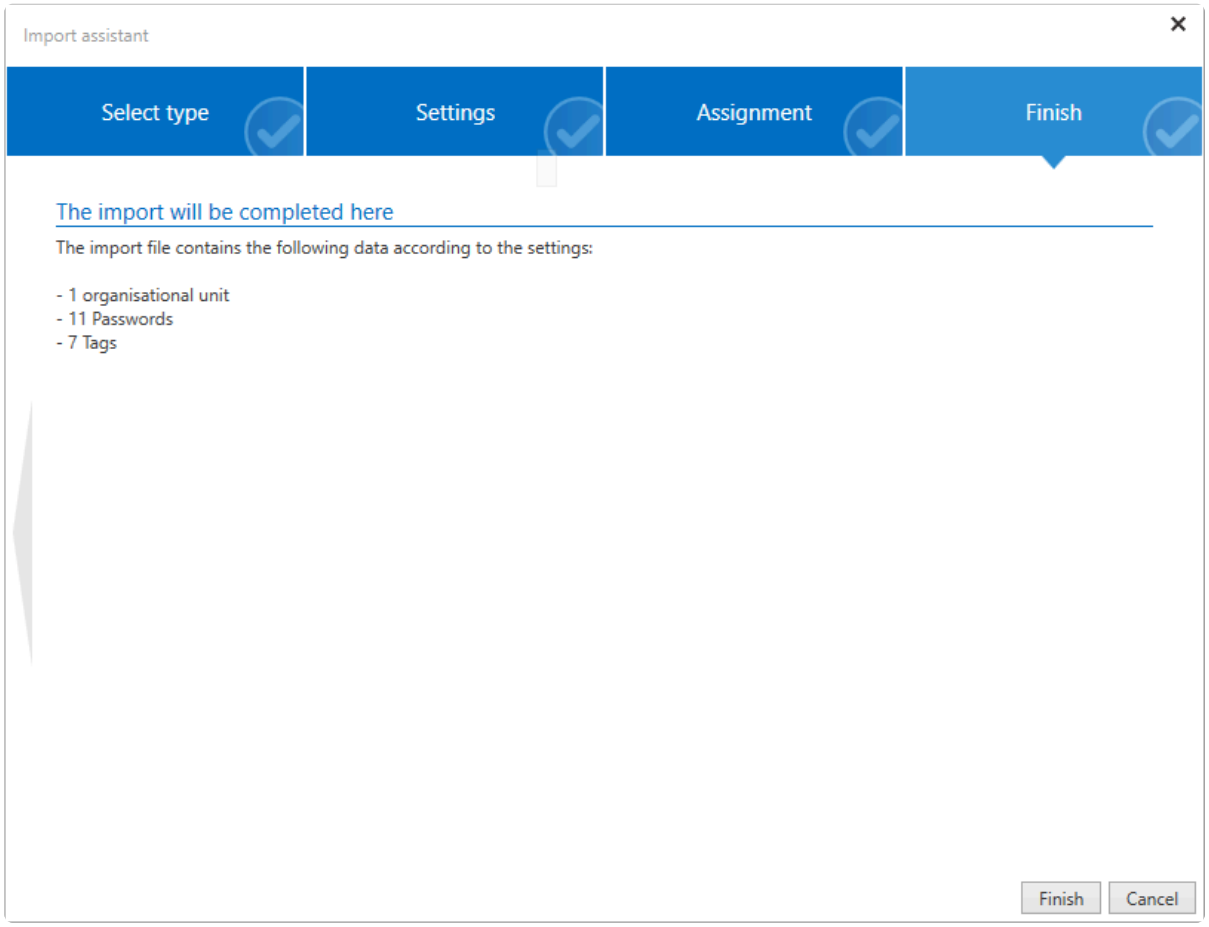
No folders exist in Password Safe. For this reason, it is necessary to define whether a folder is saved as an organisational structure or as a tag during the import. The same process is also used for the migration.

Assignment of the form fields



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



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.

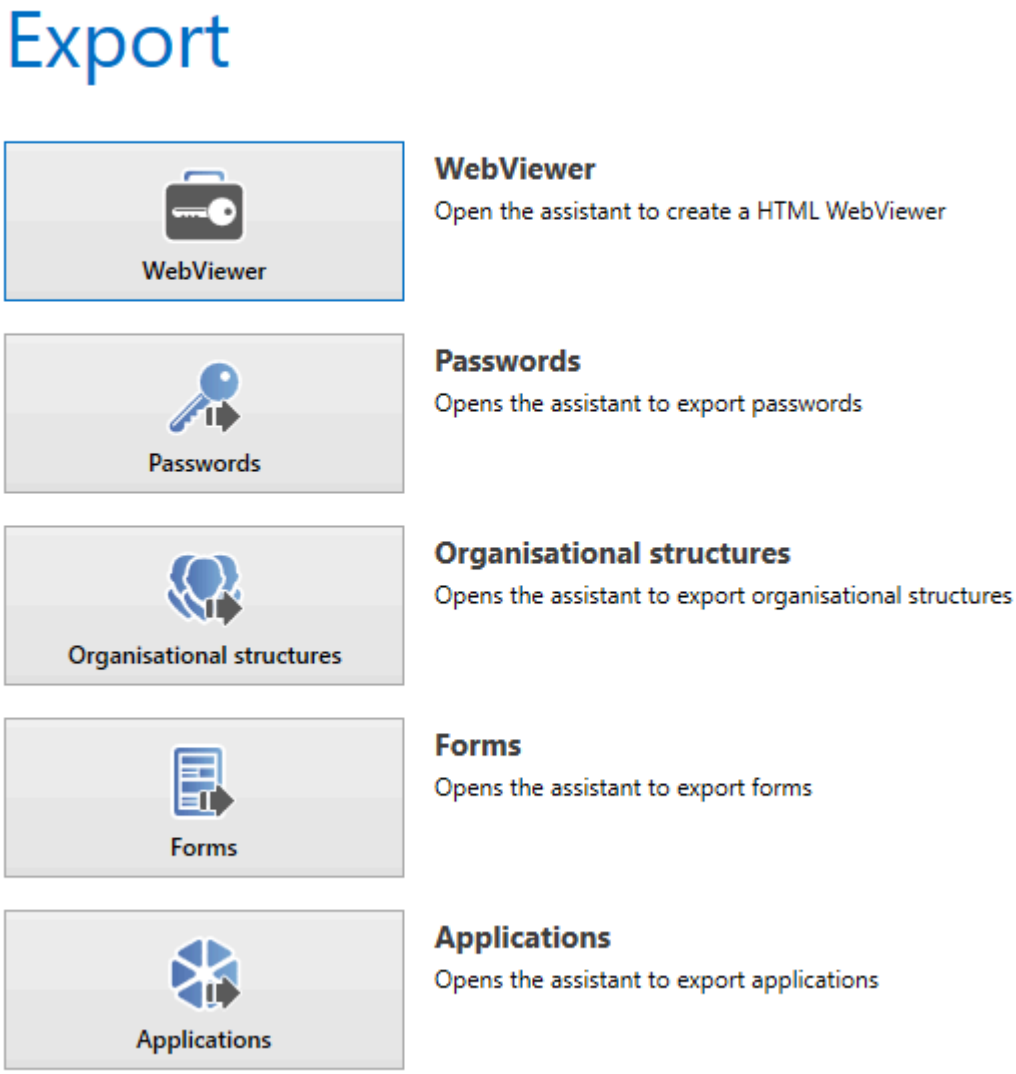
Export

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 from 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 “#logbuch 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.

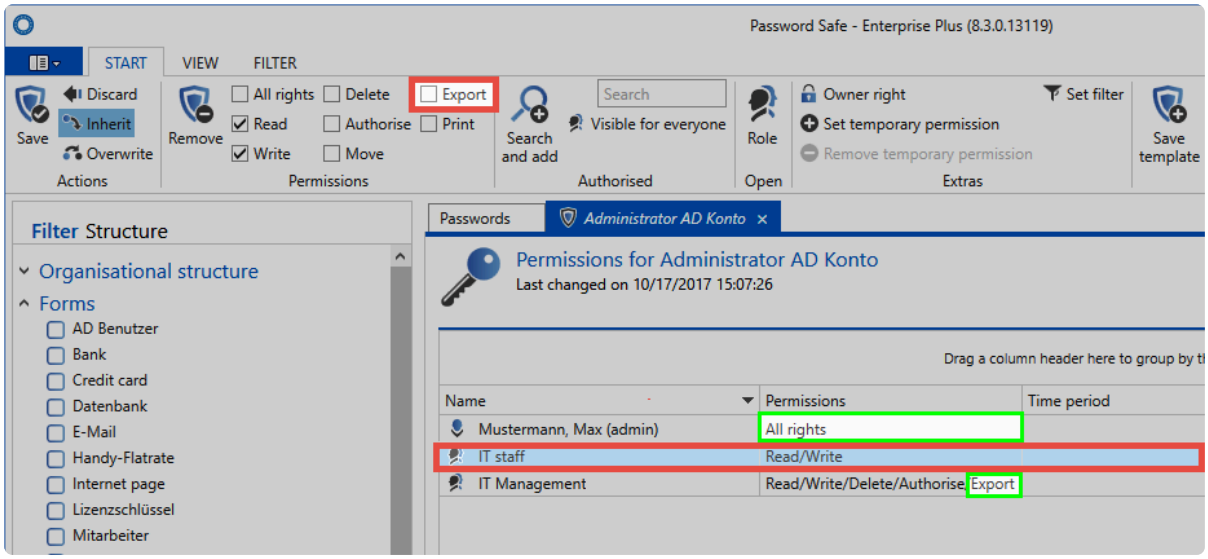


The WebViewer export creates a HTML file protected by a password. In contrast, the export wizard creates an open and unprotected .csv file.

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



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.

Relevant right

The following option is required.

User right

- Can export

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”:#genutzte-verschl-sselungsalgorithmen
- The export of the file is protected using a corresponding user right
- The user requires the **export right** for the passwords

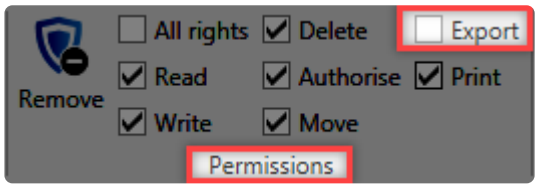
Required rights

The **export right for the WebViewer** is configured via the **user rights**:

User right

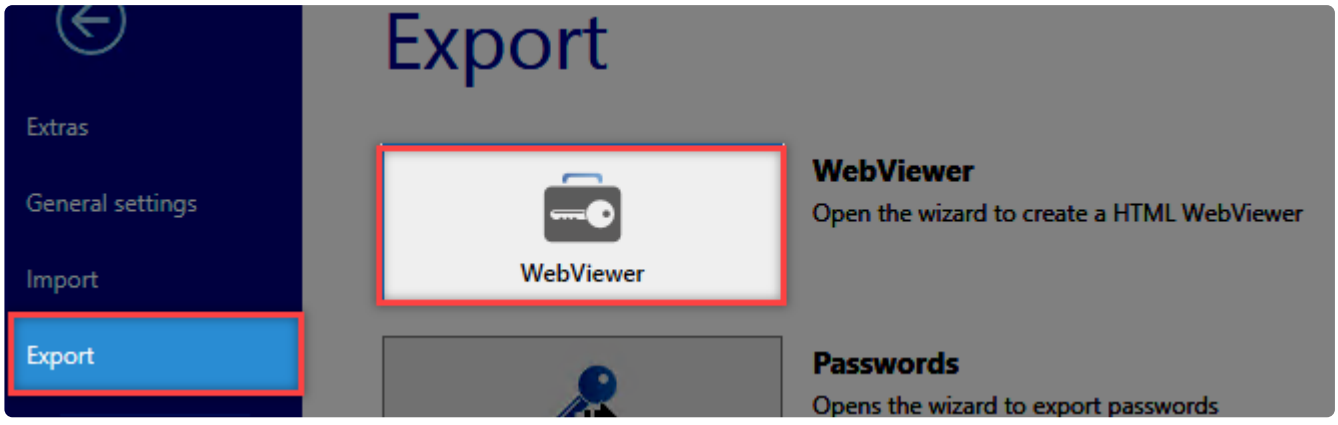
- Can export HTML WebViewer

The **export right** for the password is configured as normal via the ribbon:



Exporting a HTML file

The **HTML file** is created on the user*s client and started in the **Main menu** under **Export WebViewer**.



The **HTML WebViewer Wizard** carries out the * WebViewer export*.

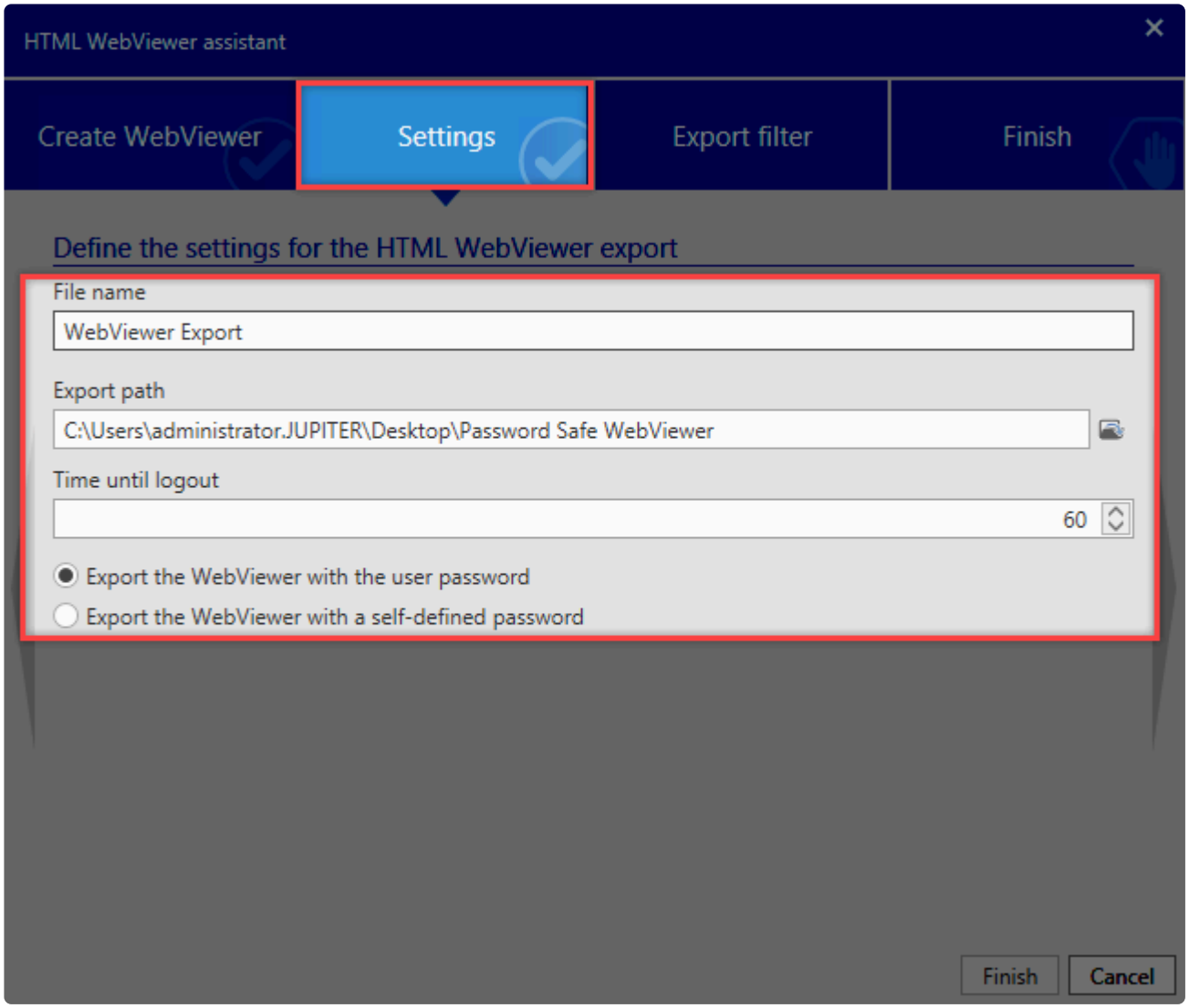
Create WebViewer

General information and notes about the export are displayed under **Create WebViewer**.

Settings

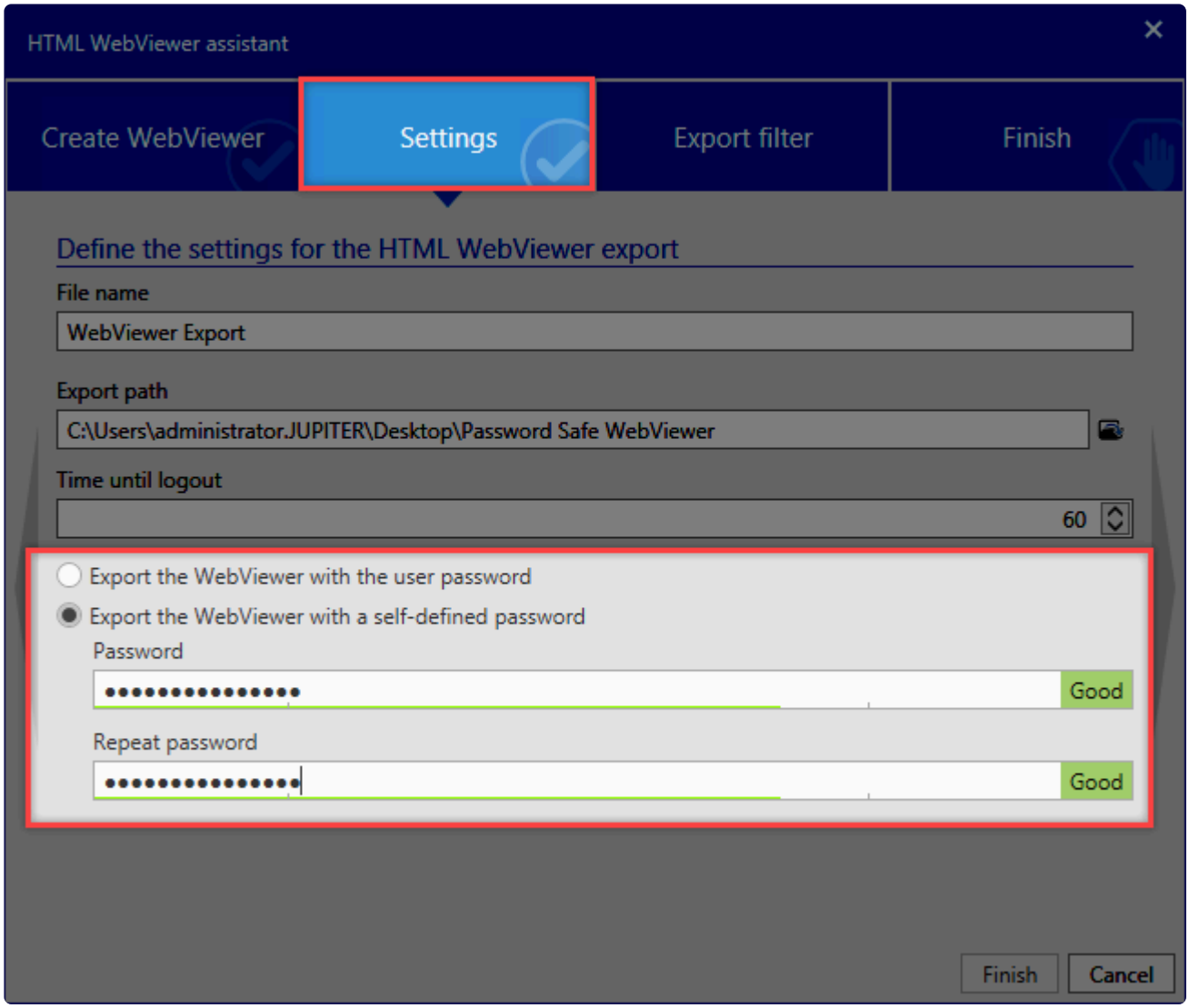
General information such as the **Name** and **Export path** for the **HTML file** can be entered here.

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.



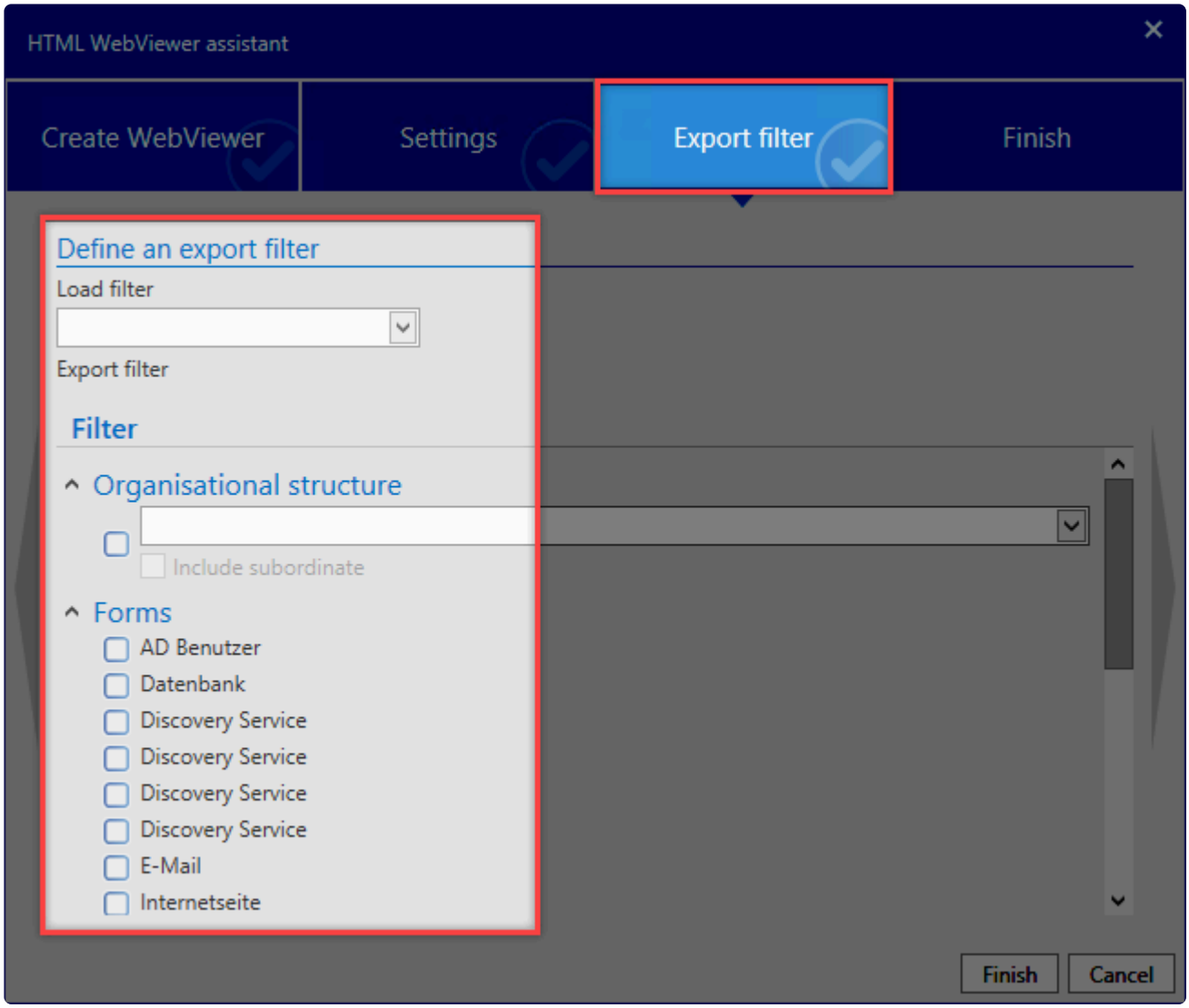
- WebViewer export with an Active Directory user*

If an **Active Directory user** is carrying out the * WebViewer export*, a **password** needs to be explicitly entered.



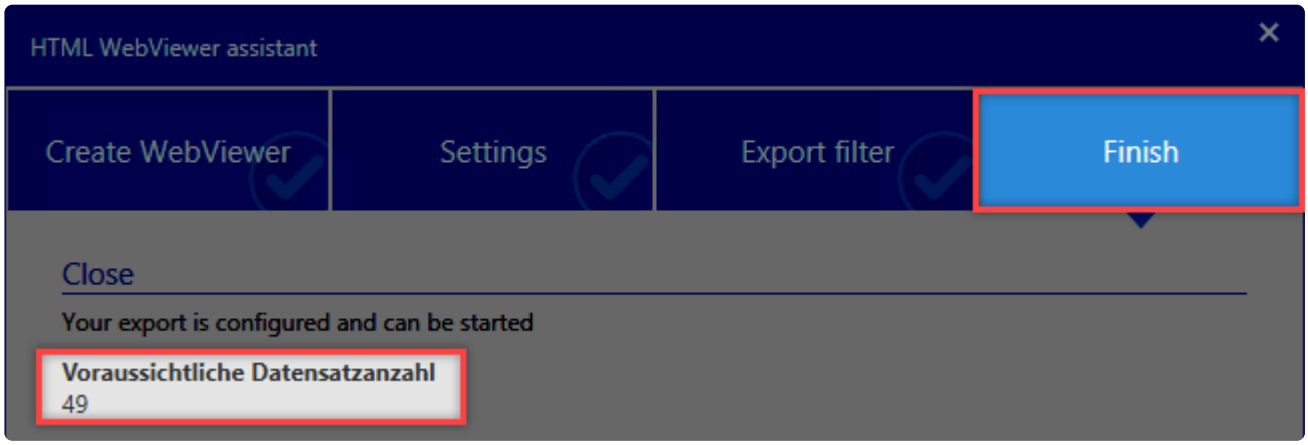
Export filter

The **export filter** works in the same way as the filters for the modules.

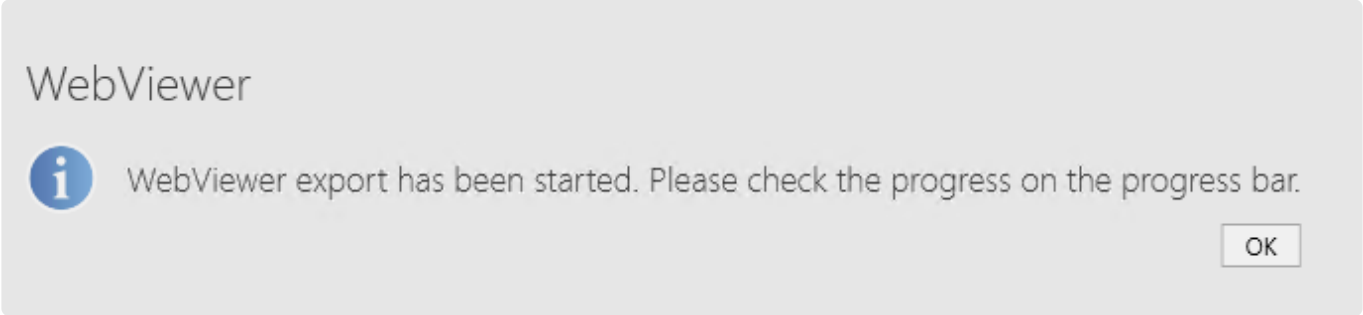


Finish

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.



A subsequent note provides you with information about the export process.



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**

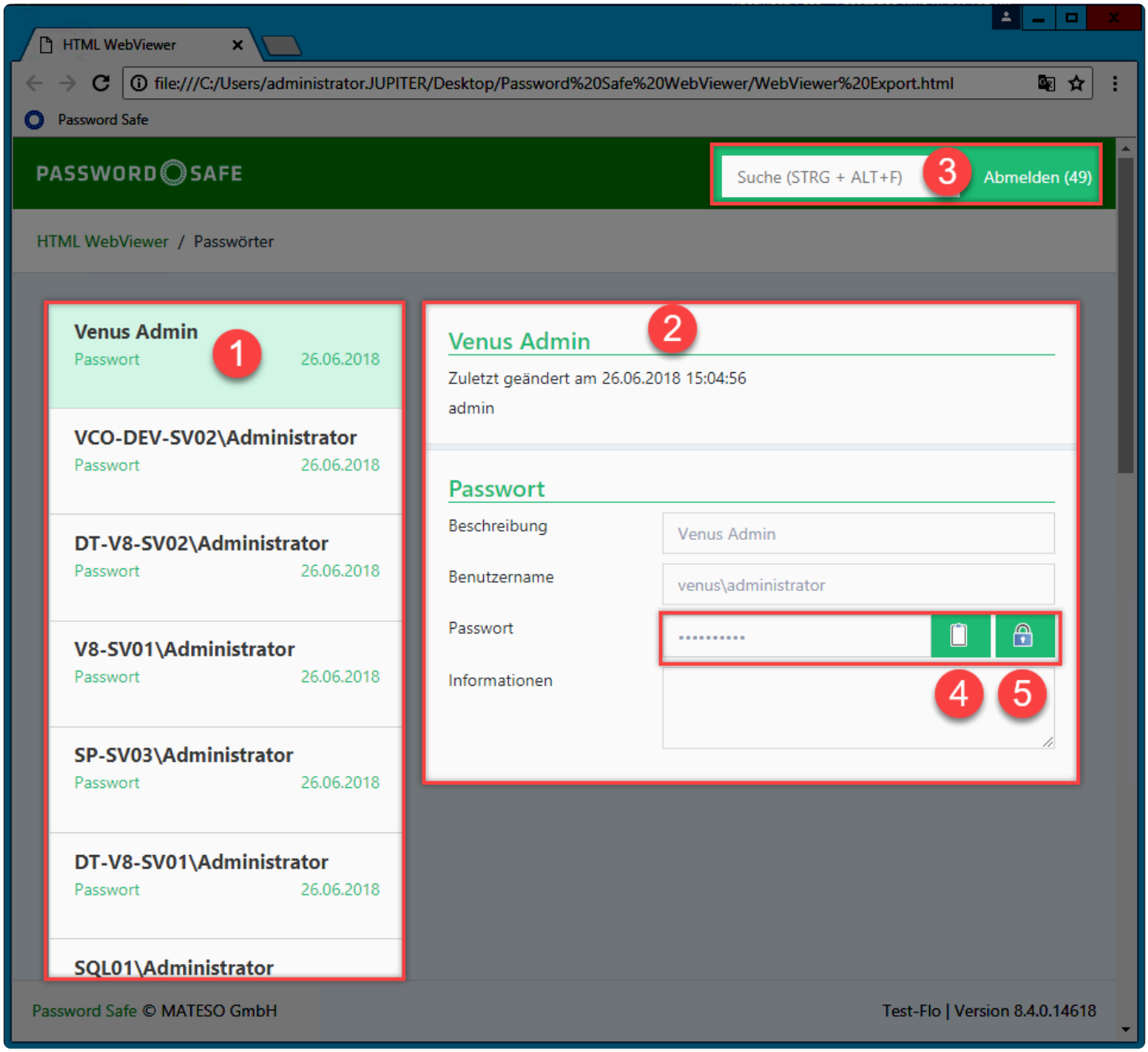


Overview

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.



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.

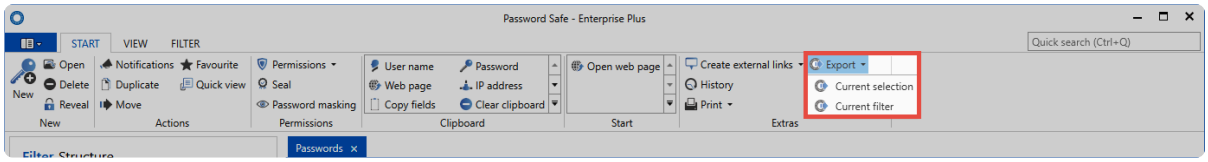
What is the password export wizard?

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:

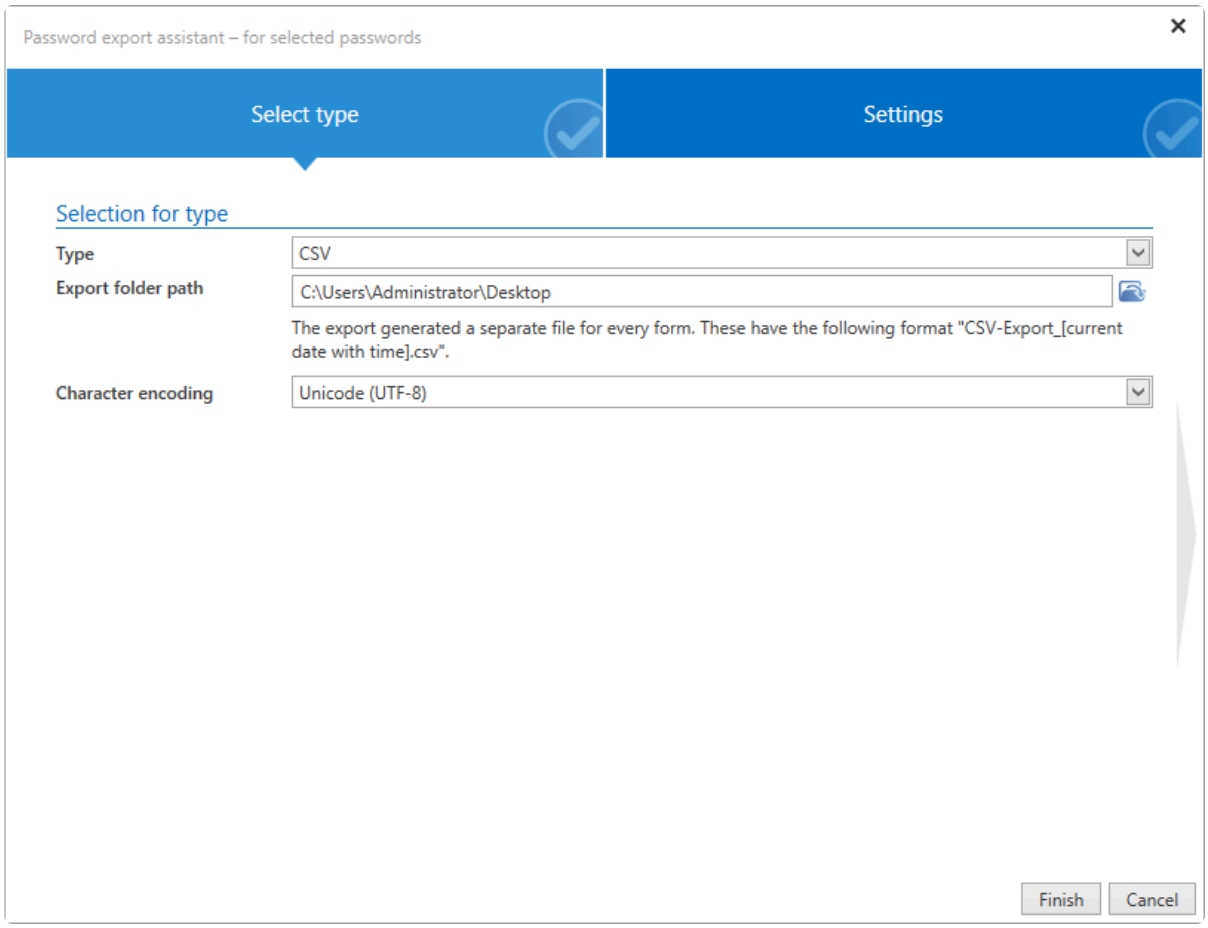
- **Starting via Main menu/Extras**: If the wizard is opened, the export will include all passwords for which the registered user has the required permissions. If the user is an administrator with permissions for all records, the export will include all passwords in the database.
- **Starting via the 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.



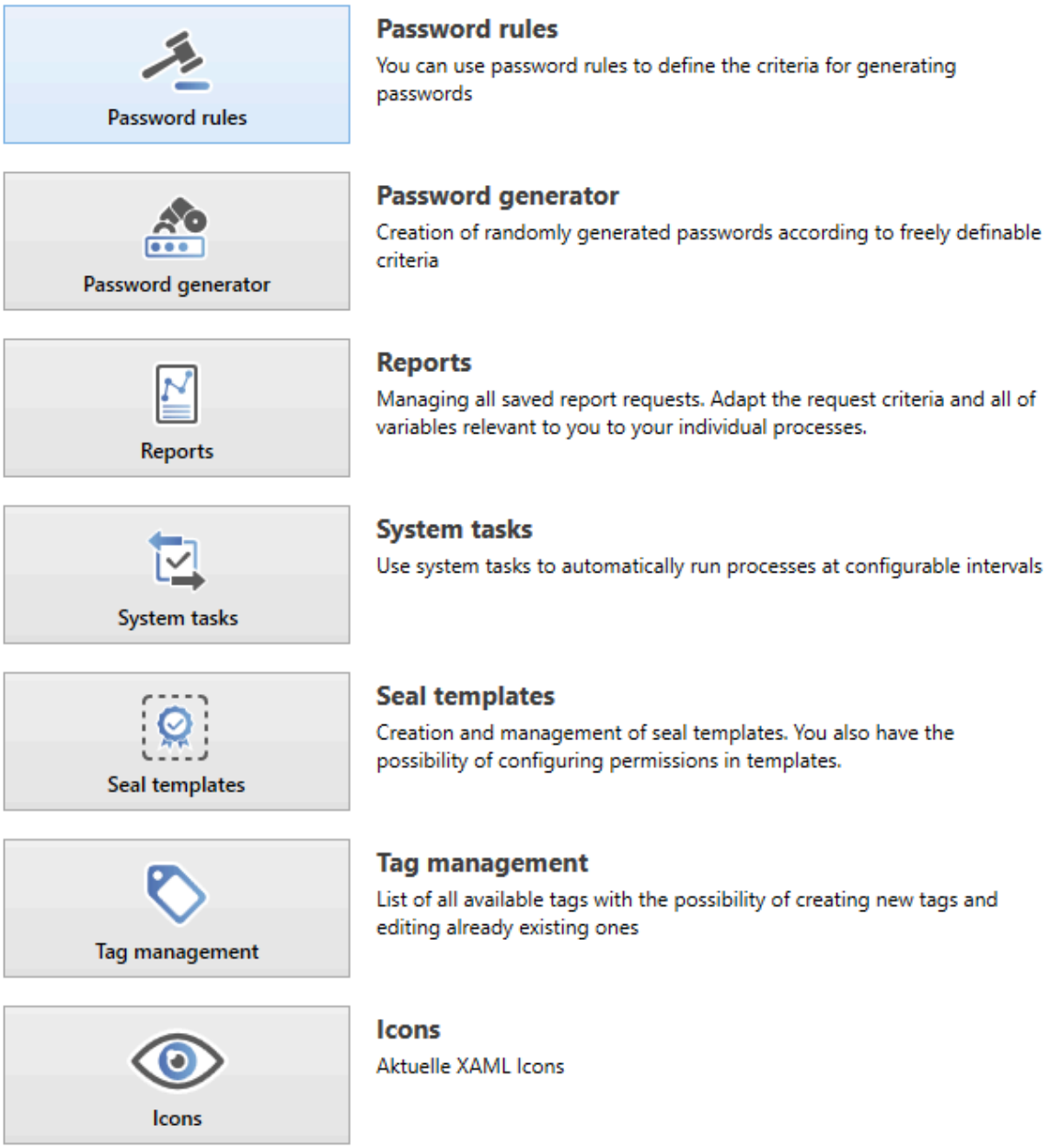
Once the wizard has been completed, the desired export is created and saved to the defined storage location.

> ! 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.

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.



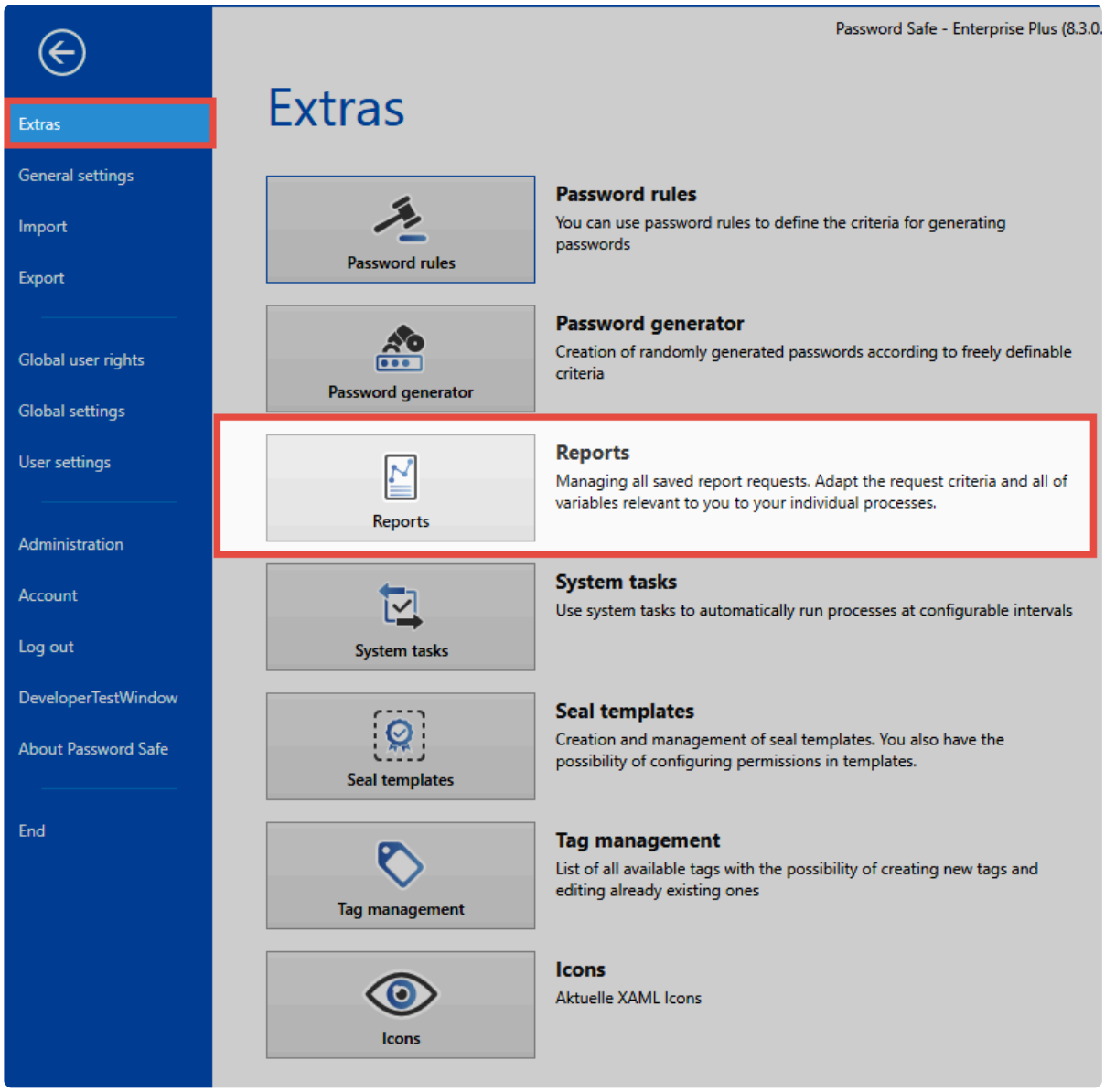
- Password rules
- Password generator
- Reports
- System tasks
- Seal templates
- Tag management

- Image management

Reports

What are reports?

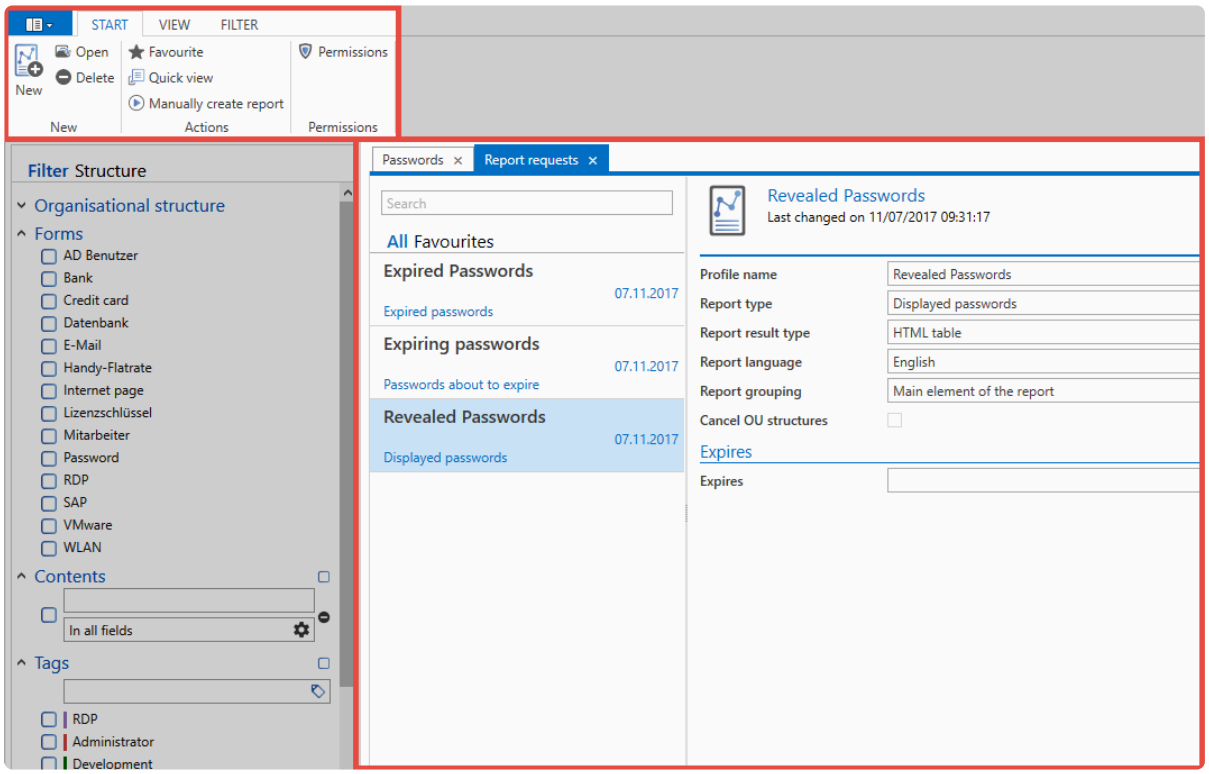
Comprehensive reporting is an important component of the ongoing monitoring of processes in Password Safe. Similar to selectively configurable notifications, reports also contain information that can be selectively defined. The difference is mainly the trigger. Notifications are linked to an event, which 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.



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

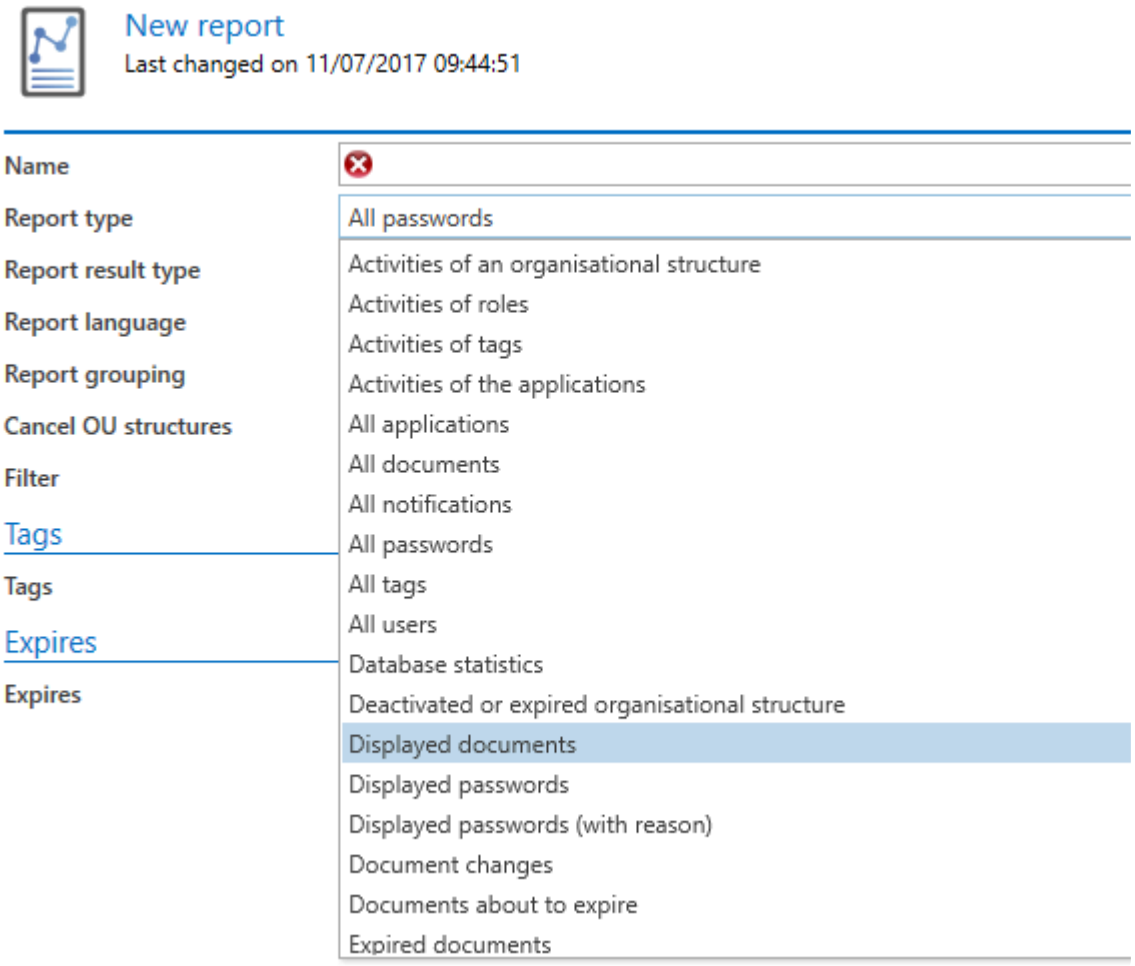
contents are always the same.



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

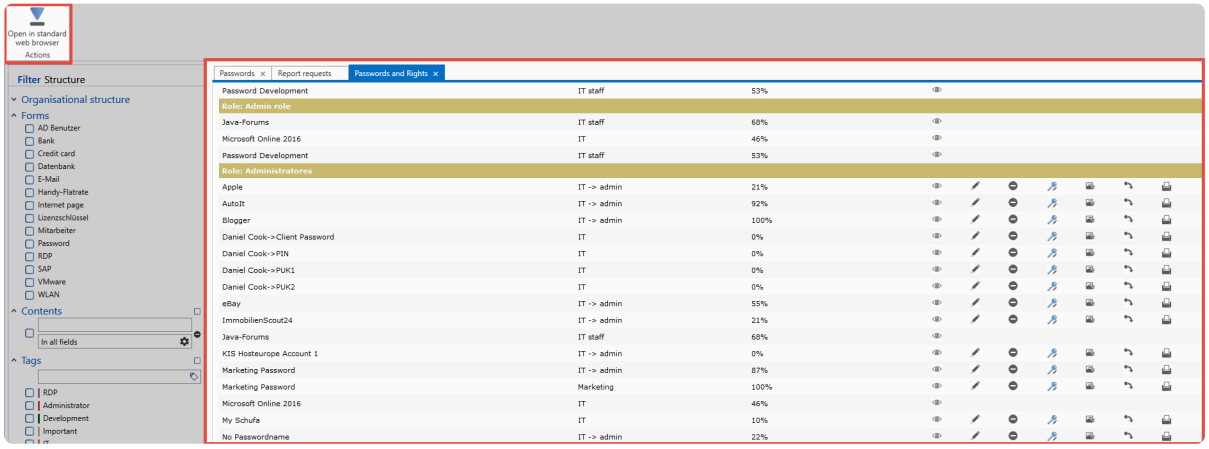
New report requests can be created in list view via the ribbon or also the context menu that is accessed using the right mouse button. The form for creating a new report request again opens in a separate tab. Alongside a diverse range of variables, the report type can be defined using a drop-down list. There are currently dozens of report types available.



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.



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…

Relevante Berichte

In diesem Kapitel finden Sie häufig verwendete Berichte und wie Sie diese konfigurieren.

Berechtigungen auf Passwörter

Oftmals ist es interessant zu wissen, welcher User / Rolle auf welche Passwörter berechtigt ist. Den Bericht können Sie wie folgt erstellen.

Bericht:

- **Berichtstyp**: Alle Passwörter
- **Berichtsergebnis-Typ**: HTML-Tabelle
- **Berichtsgruppierungen**: Berechtigte Organisationsstruktur

Filter

Beim Filter müssen Sie ein weiteres Filterattribut hinzufügen.

- Filter **Rechte** hinzufügen
- entsprechende Rolle oder Benutzer im neuen Filter auswählen

Nach dem definieren des Filter kann der Bericht erzeugt werden.

Zugriffe auf die Passwörter

Auch interessant ist es zu wissen, wer wann welches Passwort bearbeitet, geöffnet oder gelöscht hat. Der Bericht sieht dann wie folgt aus.

Bericht

- **Berichtstyp**: Logbucheinträge
- **Berichtsergebnis-Typ**: HTML-Tabelle
- **Berichtsgruppierungen**: Datum

Filter

Hier können Sie nach den gewünschten Attributen filtern. Dabei gibt es unzählige Kombinationen

Nachdem der gewünschte Filter eingestellt ist, muss der Bericht nur noch erzeugt werden.

Bald ablaufende Passwörter

Definitiv interessante Abfrage bei Datenbanken, in welcher es viele Passwörter mit Ablaufdatum gibt. So wird der Bericht konfiguriert.

Bericht

- **Berichtstyp**: Bald ablaufende Passwörter
- **Berichtsergebnis-Typ**: HTML-Tabelle
- **Berichtsgruppierungen**: Datum

Filter

Ein Filter muss bei dieser Abfrage nicht definiert werden

Abgelaufene Passwörter

Der Pendant zu den **bald ablaufenden Passwörter** sind die abgelaufenen Passwörter.

Bericht

- **Berichtstyp**: Bald ablaufende Passwörter
- **Berichtsergebnis-Typ**: HTML-Tabelle
- **Berichtsgruppierungen**: Datum

Filter

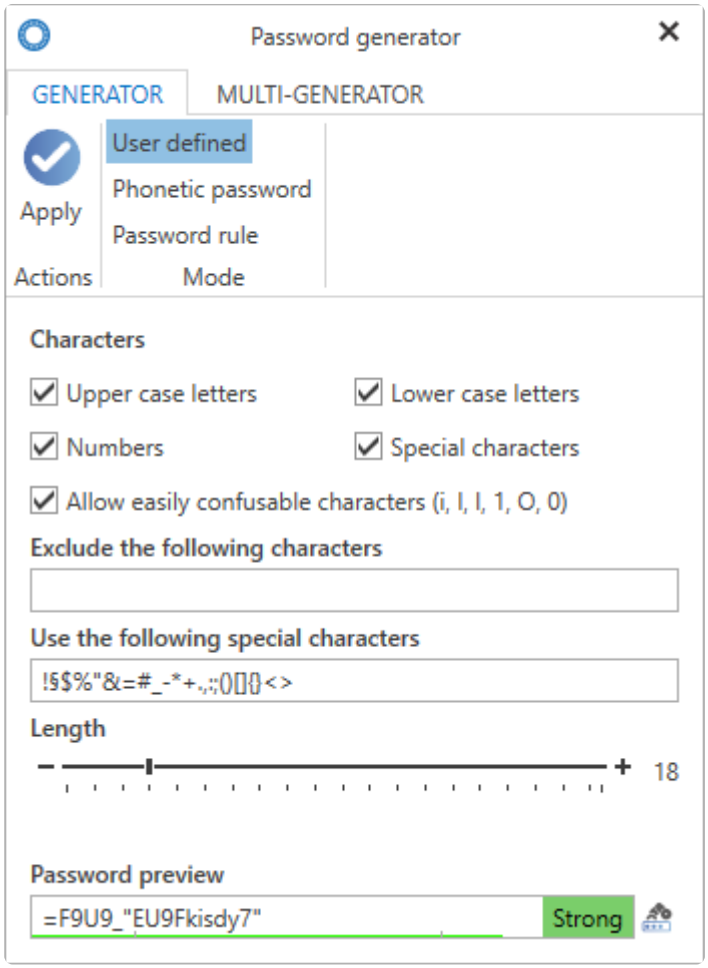
Ein Filter muss bei dieser Abfrage nicht definiert werden

Die hier genannten Berichte entsprechen einer kleinen Auswahl und spiegeln den vollen Umfang nicht dar.

Password generator

What is the password generator?

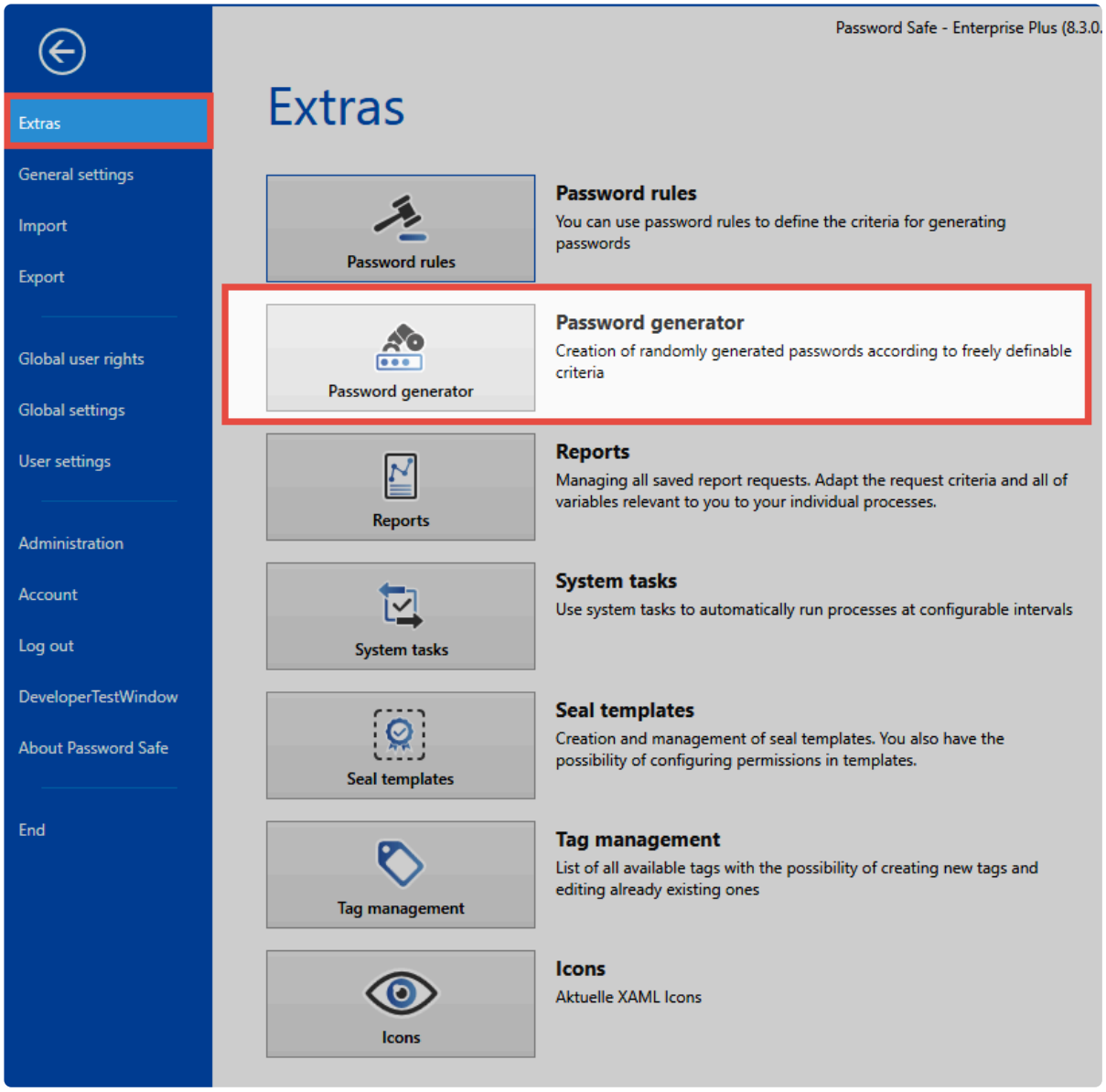
The complexity of passwords is generally determined by their randomness. In order to be able to rely 100% on the fact that the passwords are randomly generated, an algorithm for generating passwords is indispensable. The password generator performs this function and is completely integrated into the software.



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.



- **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.

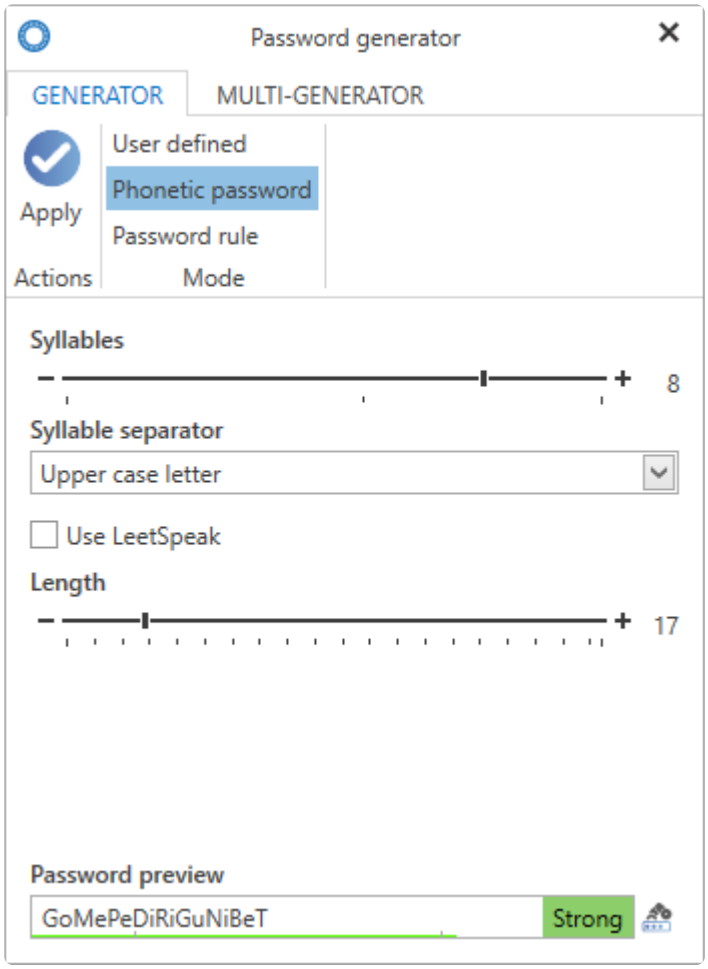
Functionality

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.



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:

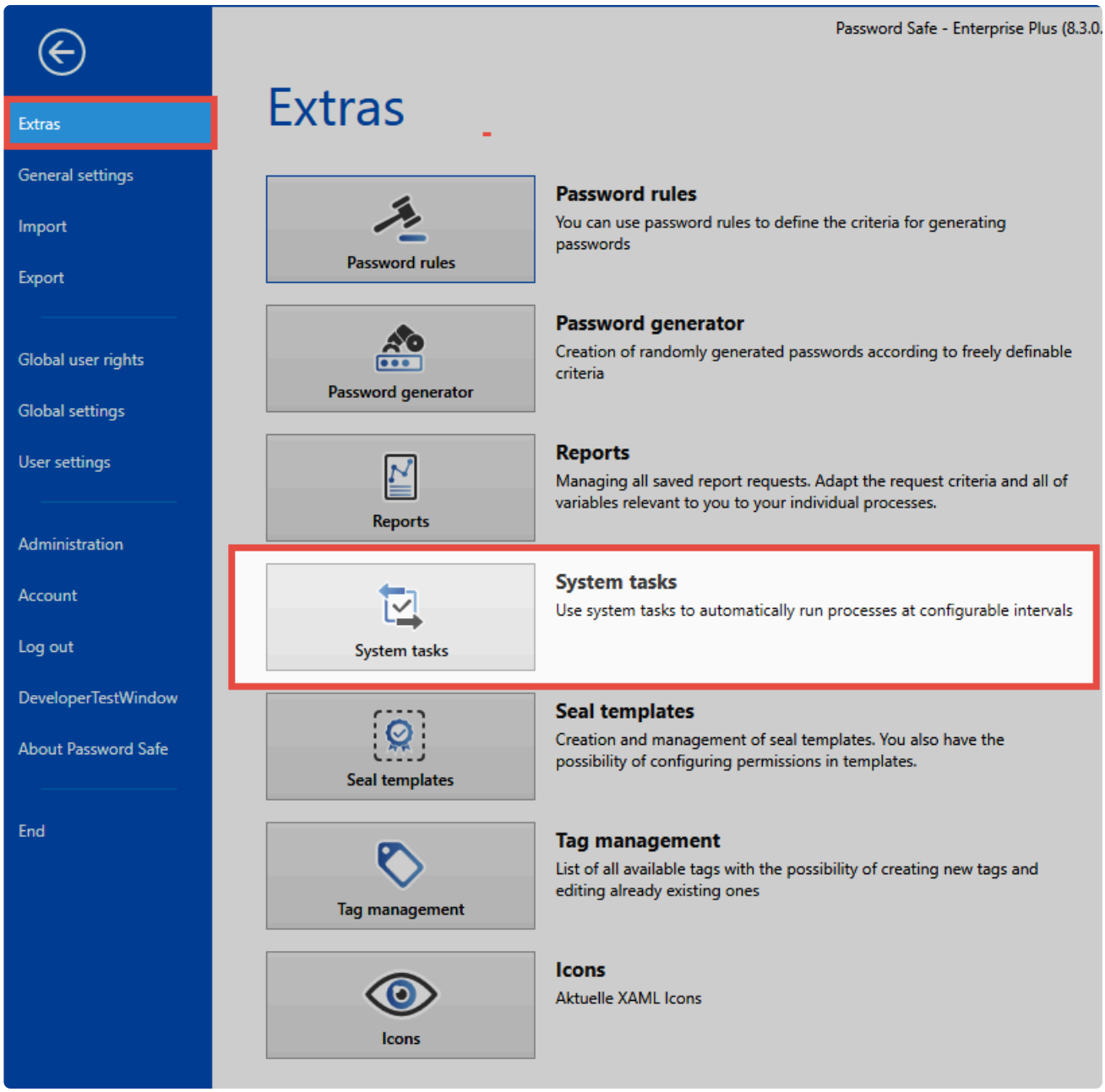
- User defined
- Phonetic passwords
- Password rules

The generated passwords are saved in a text file in the local user directory and can be opened immediately if desired.

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.



Relevant rights

The following options are required for managing system tasks.

User right

- Can manage Active Directory system tasks
- Can manage system task reports

- Can manage discovery service system tasks
- Can manage Emergency WebViewer export system tasks
- Can manage WebViewer export system tasks

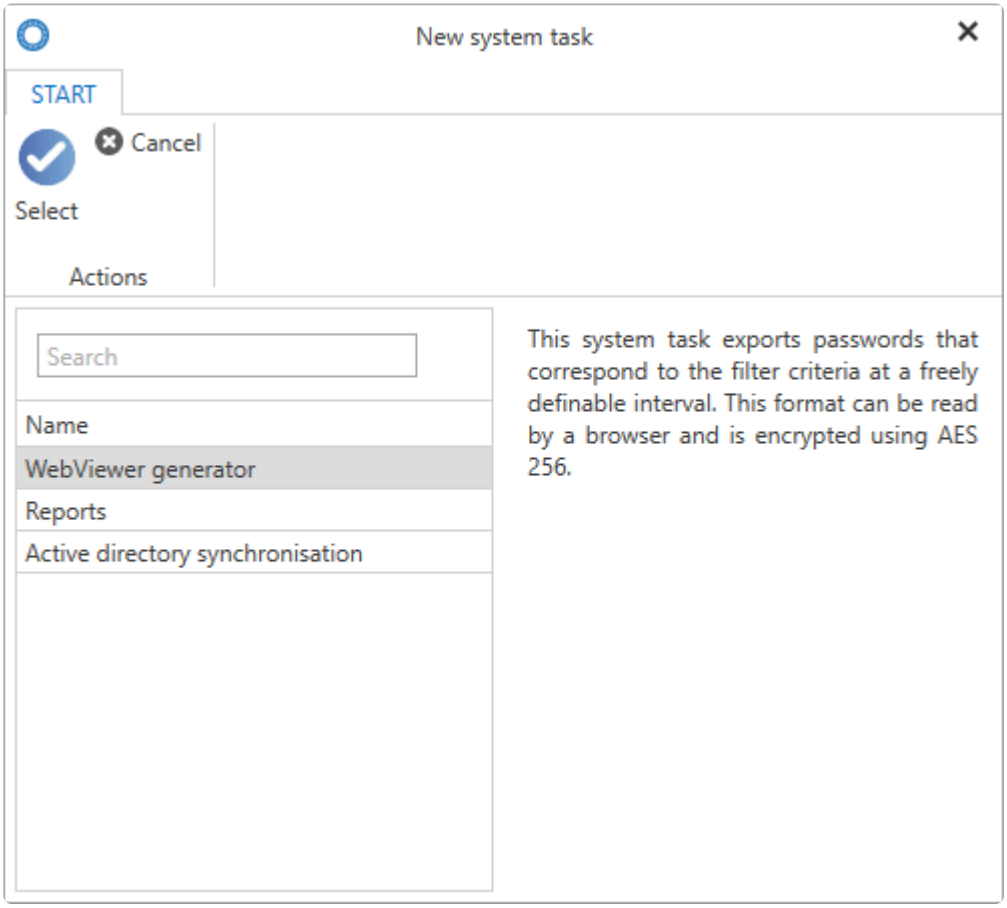
What can be automated?

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.

Creating system tasks

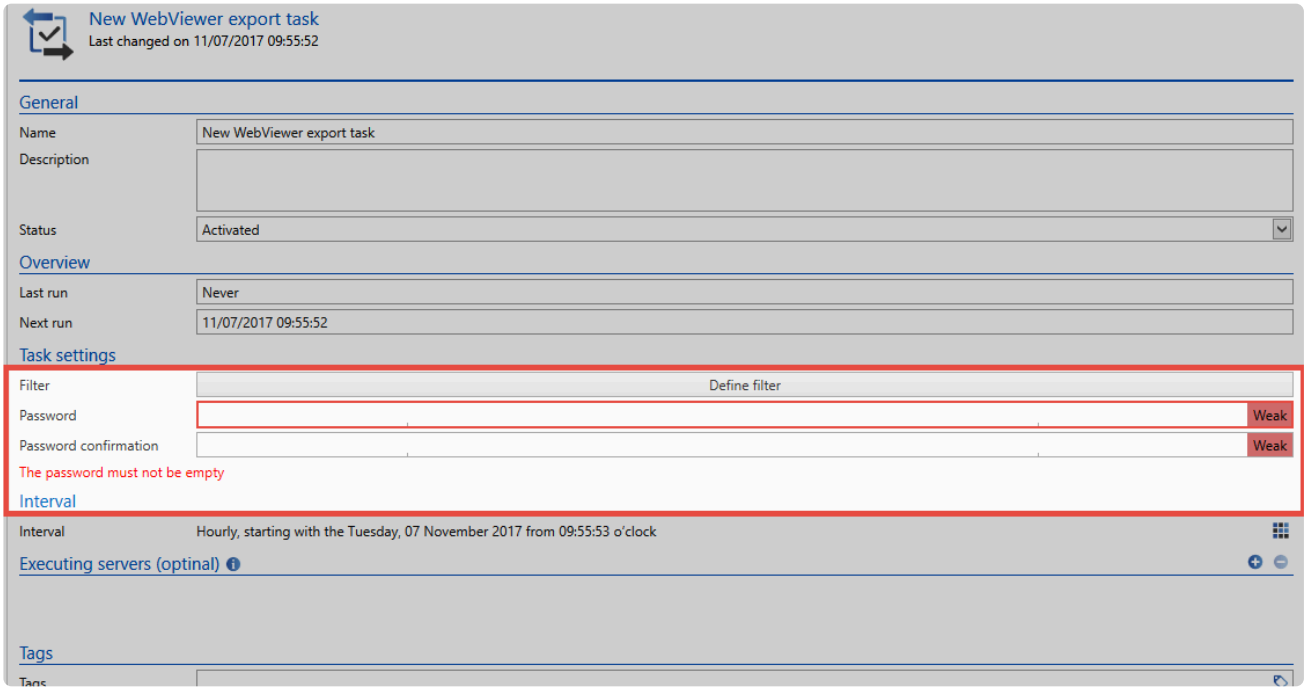
System tasks can be initiated as usual via the ribbon or also the context menu that is accessed using the right mouse button. The desired process to be automated using system tasks is then selected from the four above-mentioned work processes.



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.



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.

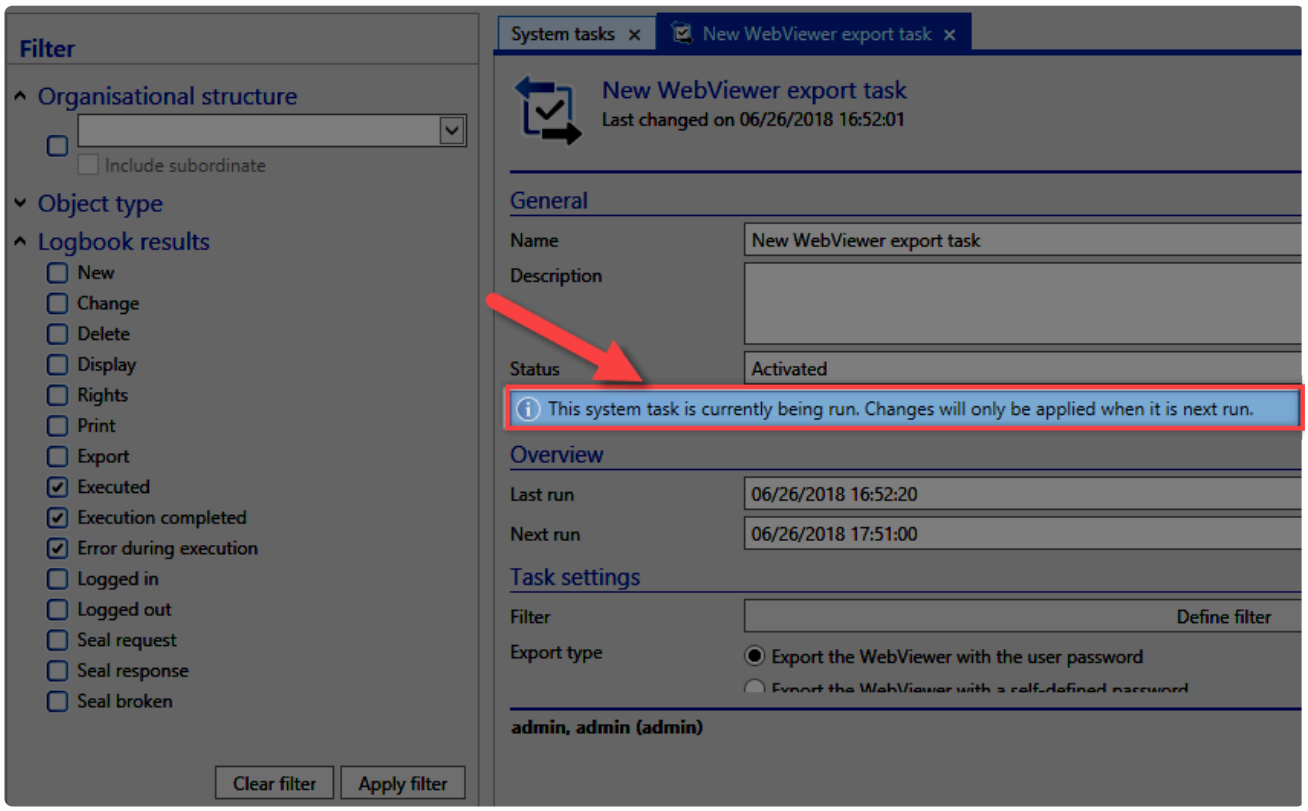
Emergency WebViewer export

- 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.



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!

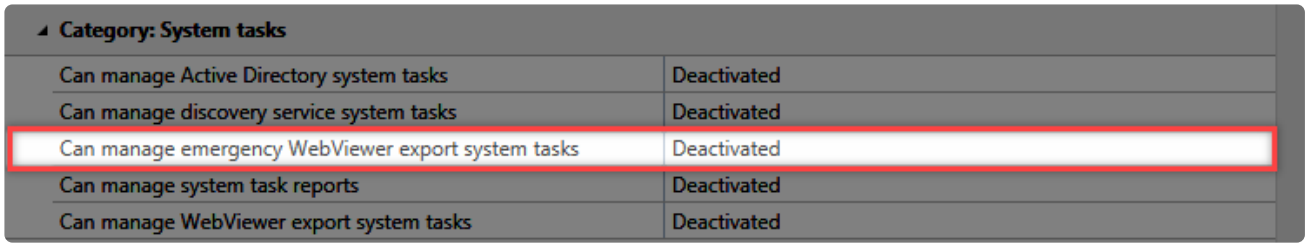
Data security

- Naturally, the HTML WebViewer file is “encrypted”:#genutzte-verschl-sselungsalgorithmen
- 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**:



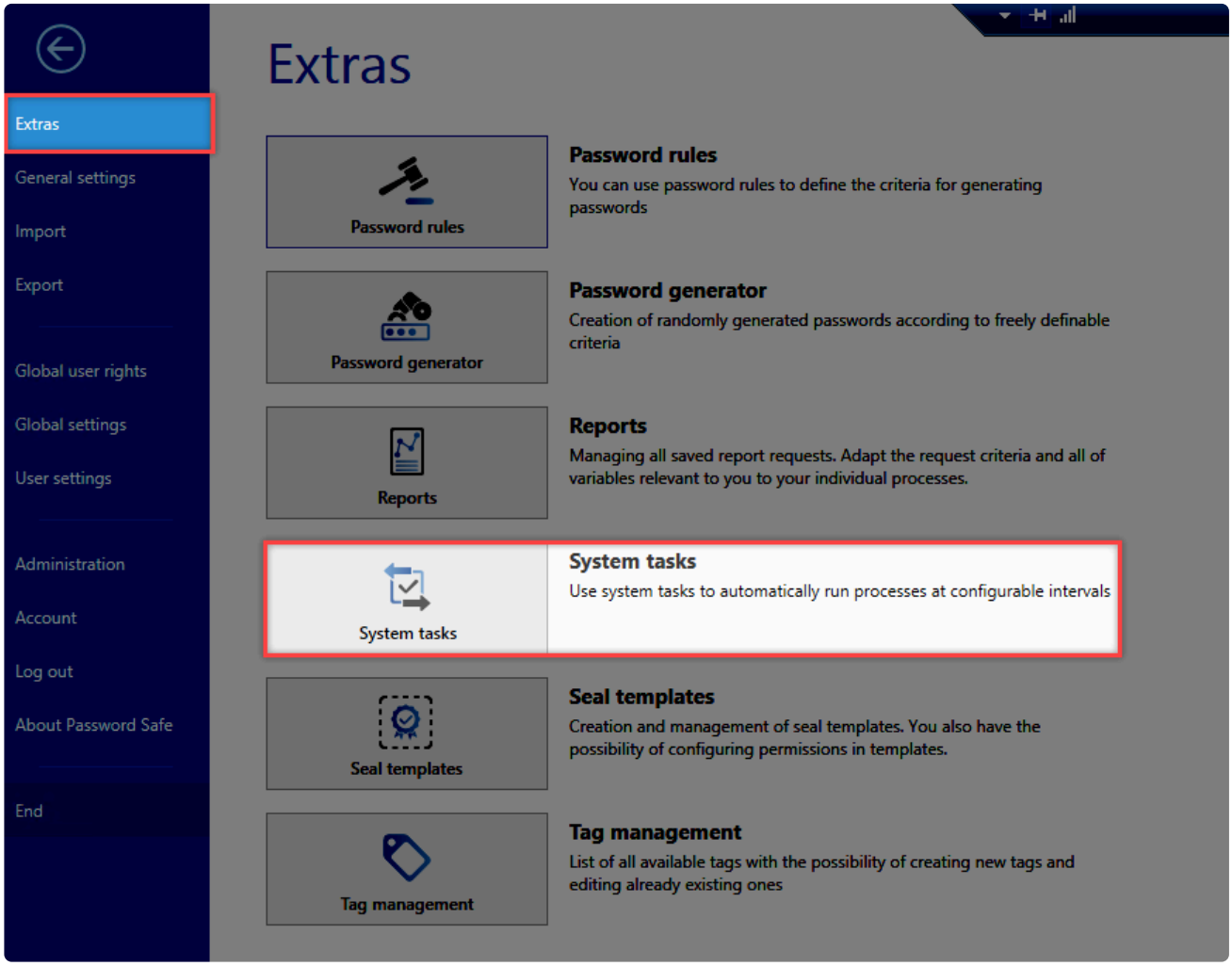
Emergency WebViewer.html and PrivateKey.prvkey

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.

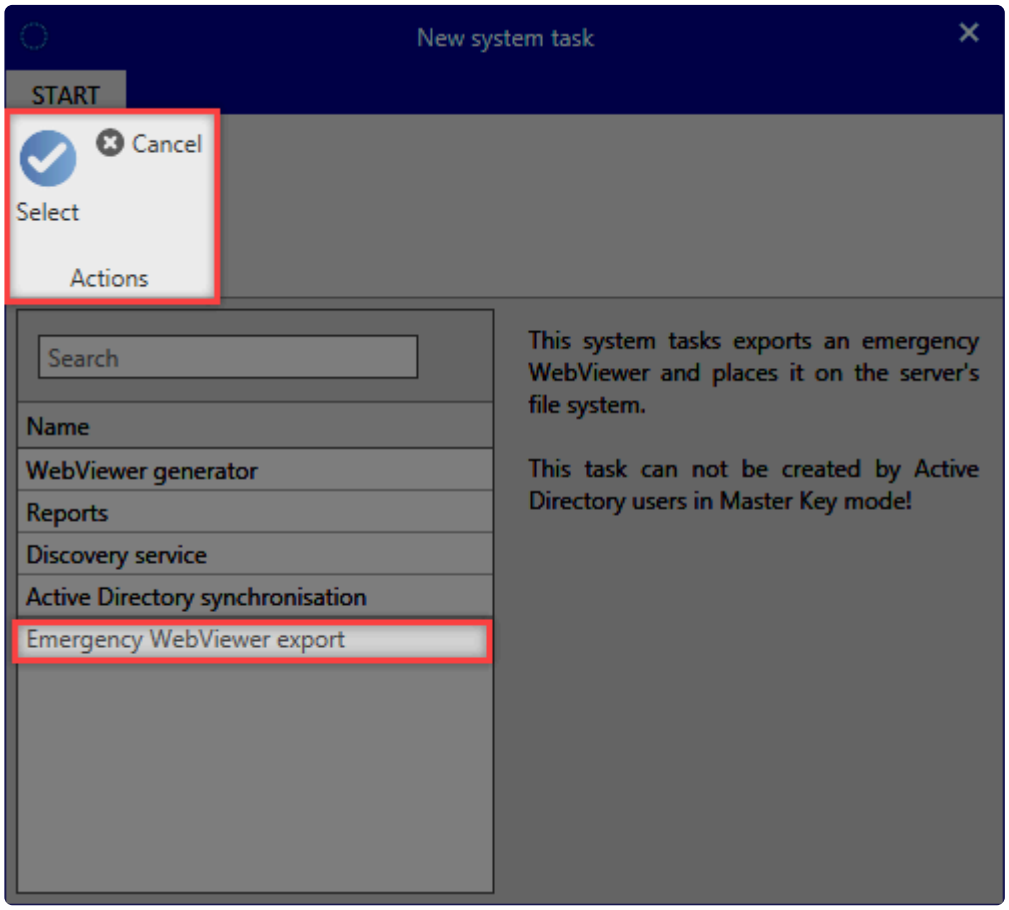
Calling up the Emergency WebViewer Export

The Emergency WebViewer Export is set up as a **system task**. It can be called up in the main menu under **Extras** -> **System Tasks**.

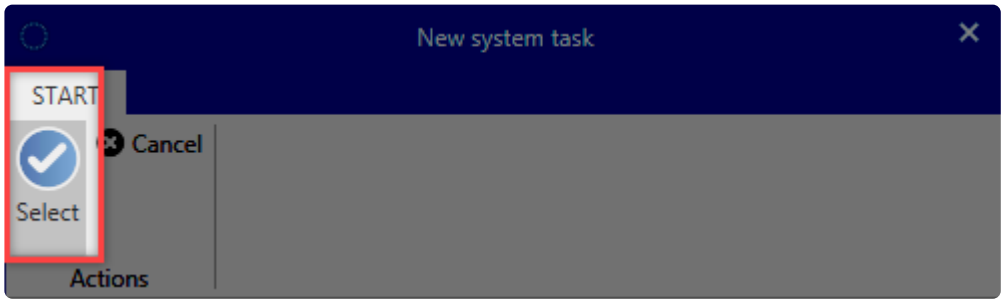


Creating a Emergency WebViewer Export file

Clicking on **New** opens a new window and the **Emergency WebViewer Export** can be selected. The **configuration page** is then displayed.

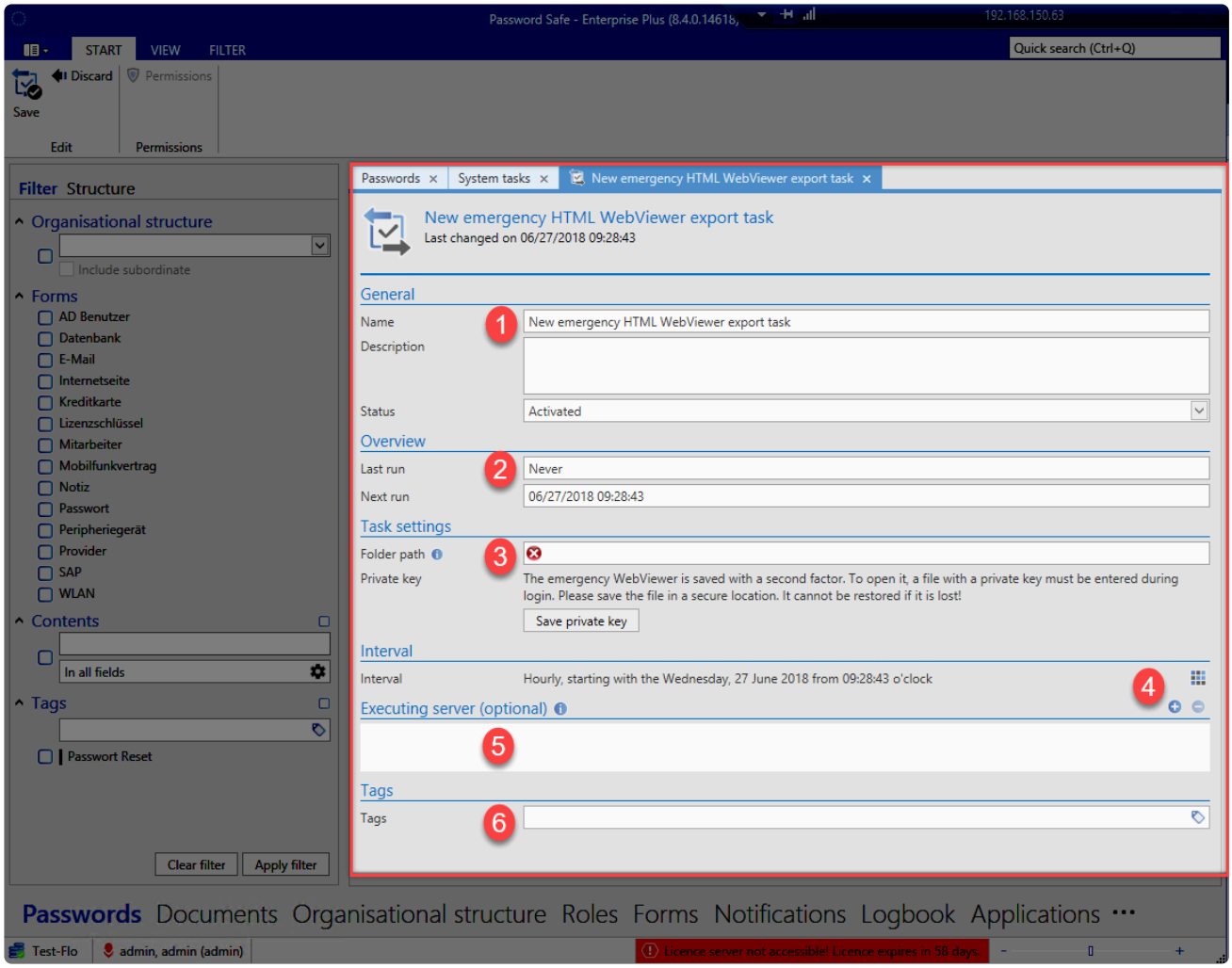


It is not possible to use the **Emergency WebViewer Export** with an **Active Directory user**.



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.

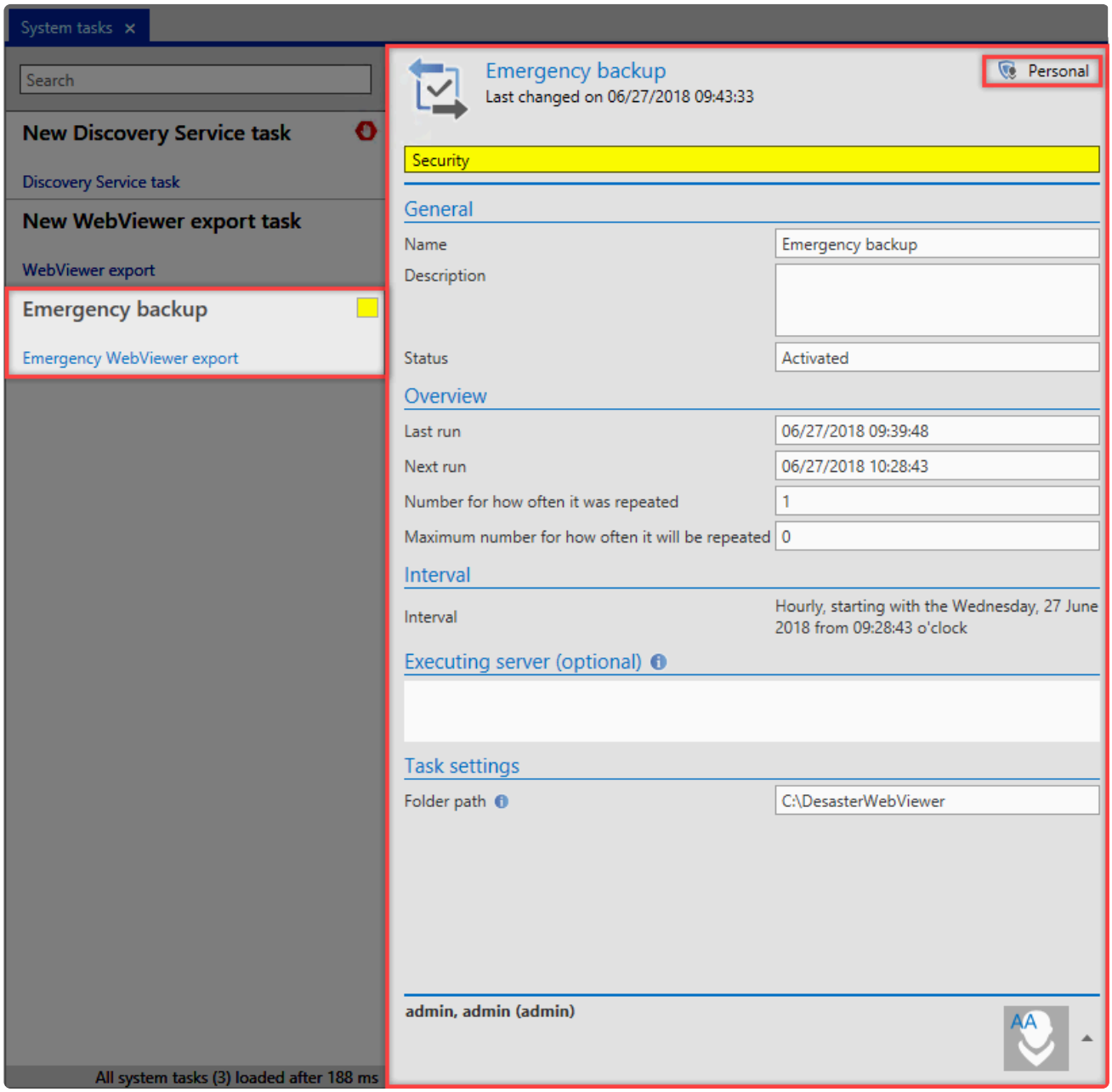


1. **General**
   Name: Enter a unique name
   Description: Enter additional information
   Status: Execution: *Activated*/Deactivated
2. **Overview**
   Last run: Information display
   Next run: Information display
3. **Task settings**
   Folder path: Enter from the perspective of the server
   Private 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 tasks

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.



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

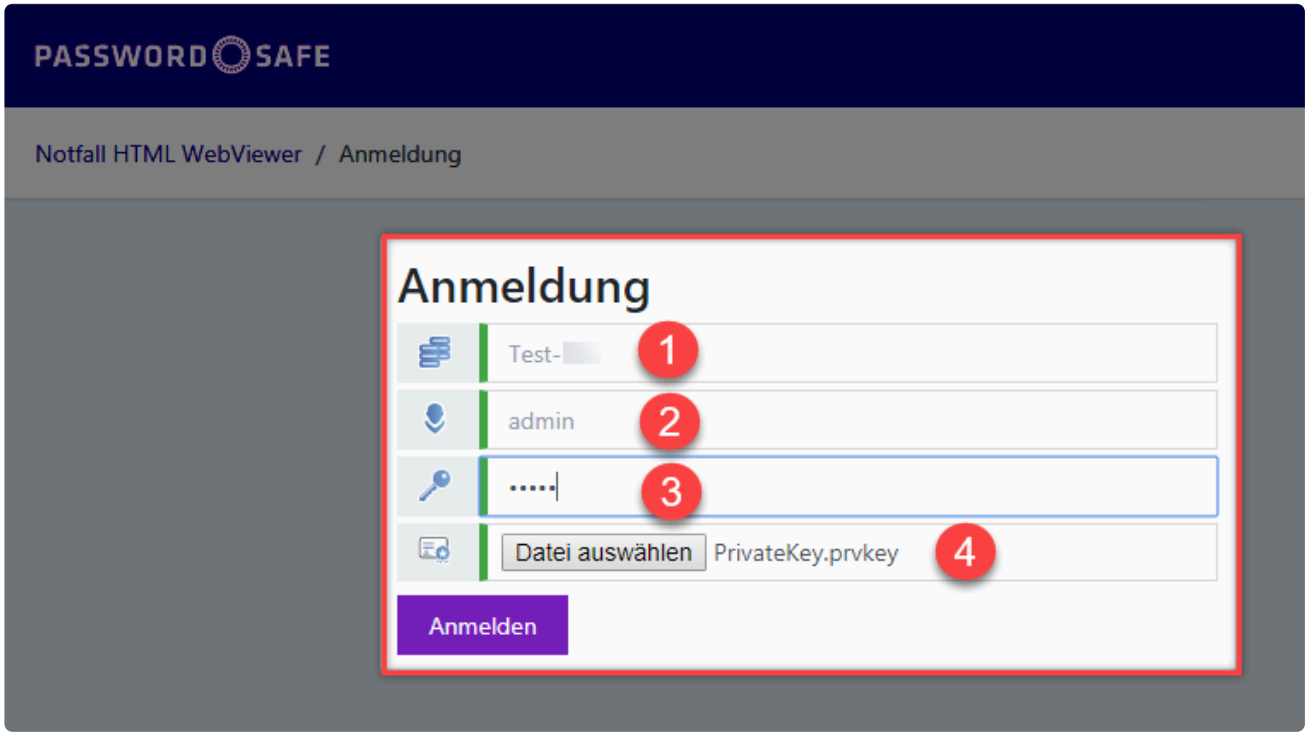
key **PrivateKey.prvkey** needs to be securely saved by the **user**!*

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

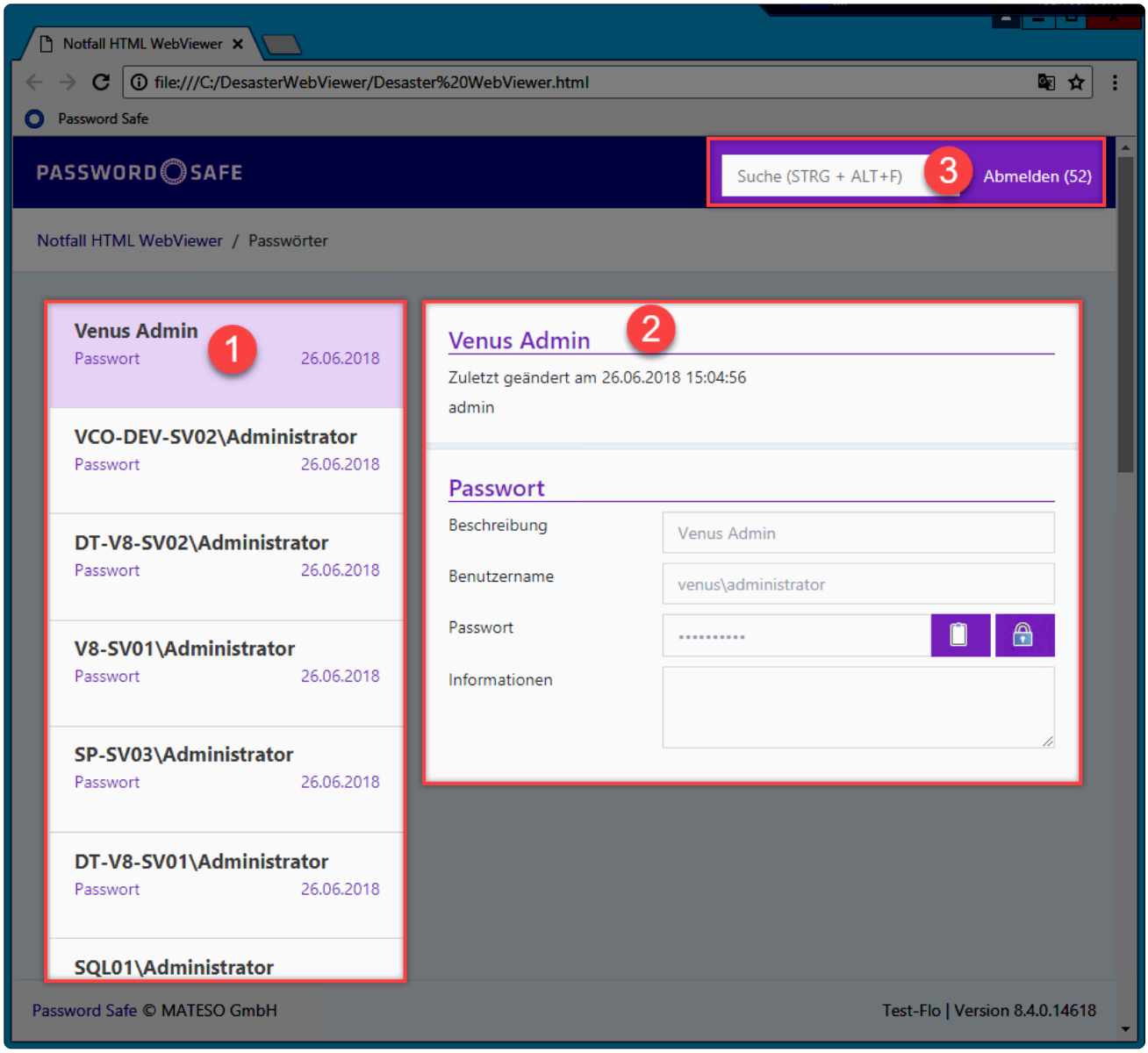
1. Database: Predefined
2. User: Predefined
3. Password: **User password (must be entered by the user)**
4. Key: **PrivateKey.prvkey**



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



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.

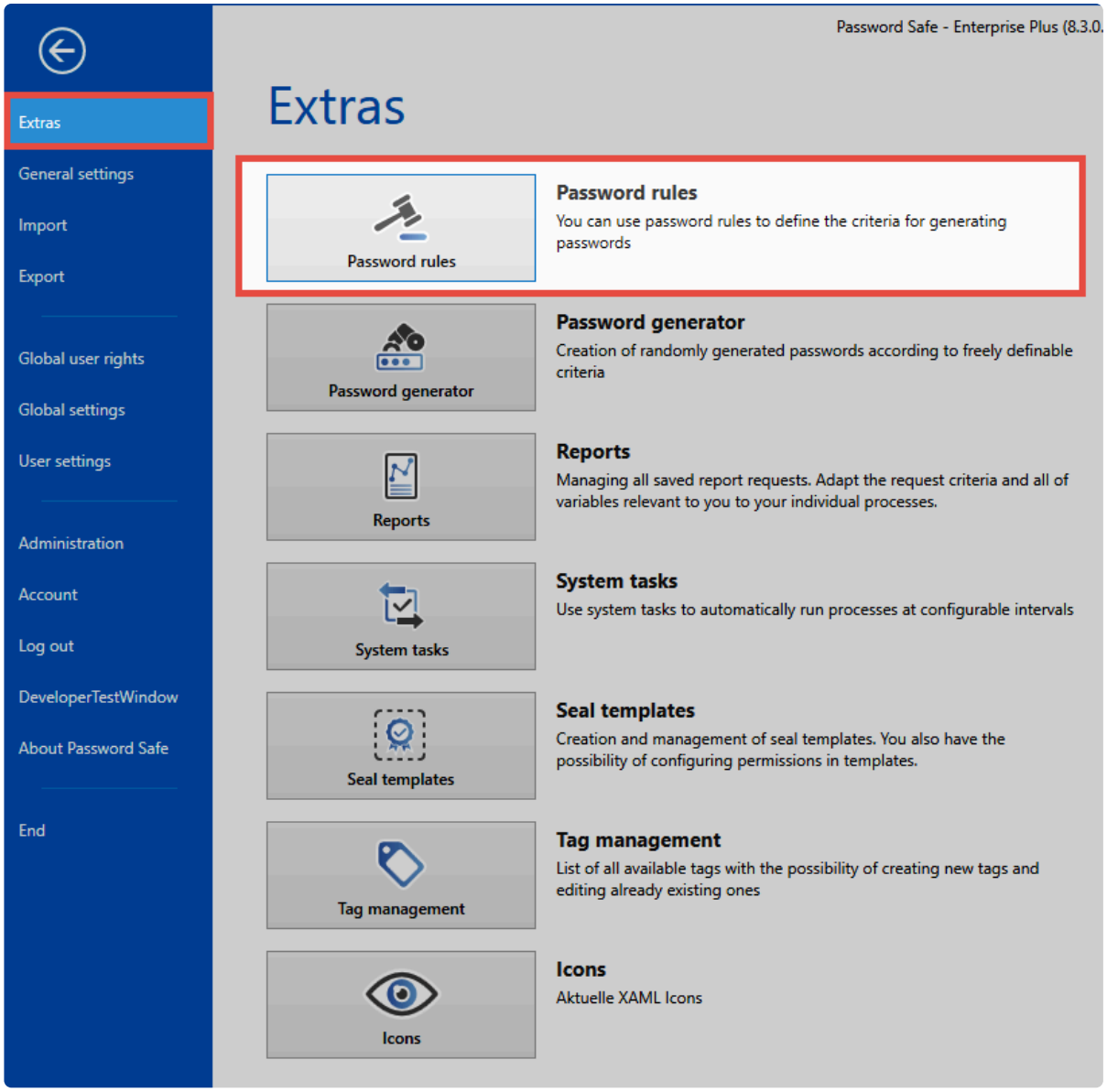


The user can log in again using the **password** and **key** as described above. After successfully logging in, the **Emergency WebViewer Export overview** is displayed again.

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.



Relevant right

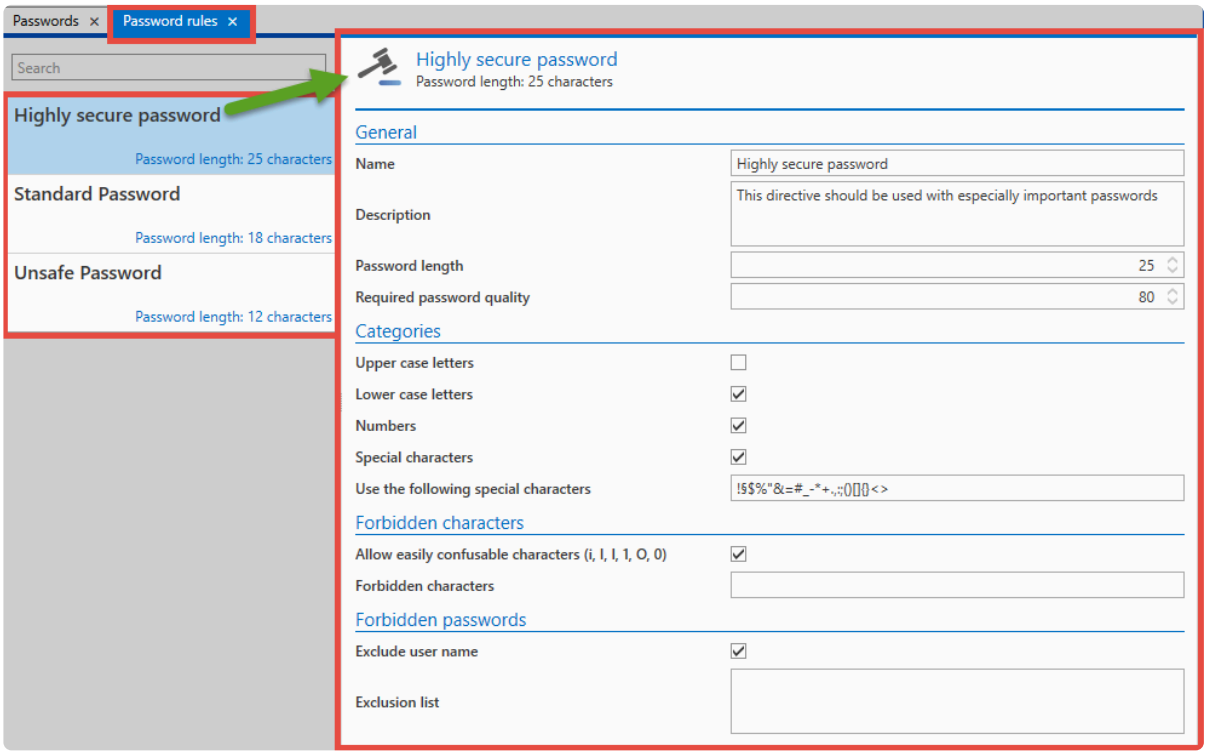
The following option is required to manage password rules.

User right

- Can manage password rules

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.



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:

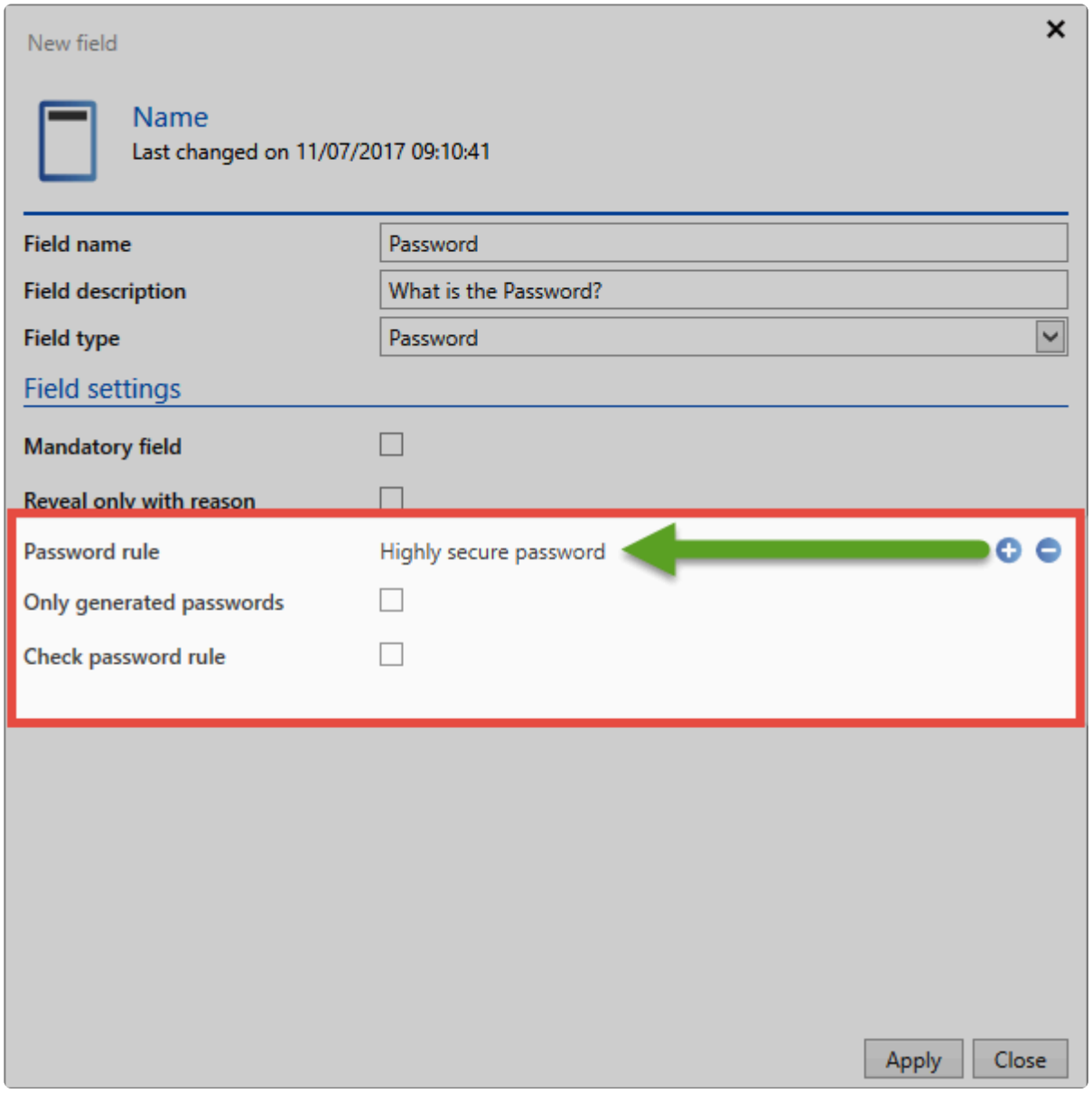
- **General**: The **Password length** of 25 is the minimum number of characters that a password needs to contain according to this rule. The required **Password quality** is an internal measure of security, which is calculated for this rule. This value always lies between 1 (very unsecure) and 100 (maximum 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

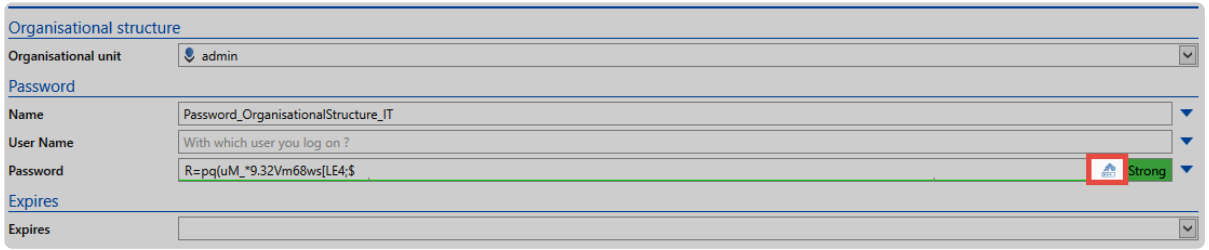
Once password rules have been defined, they can be productively used in two different ways:

- 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.



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.



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

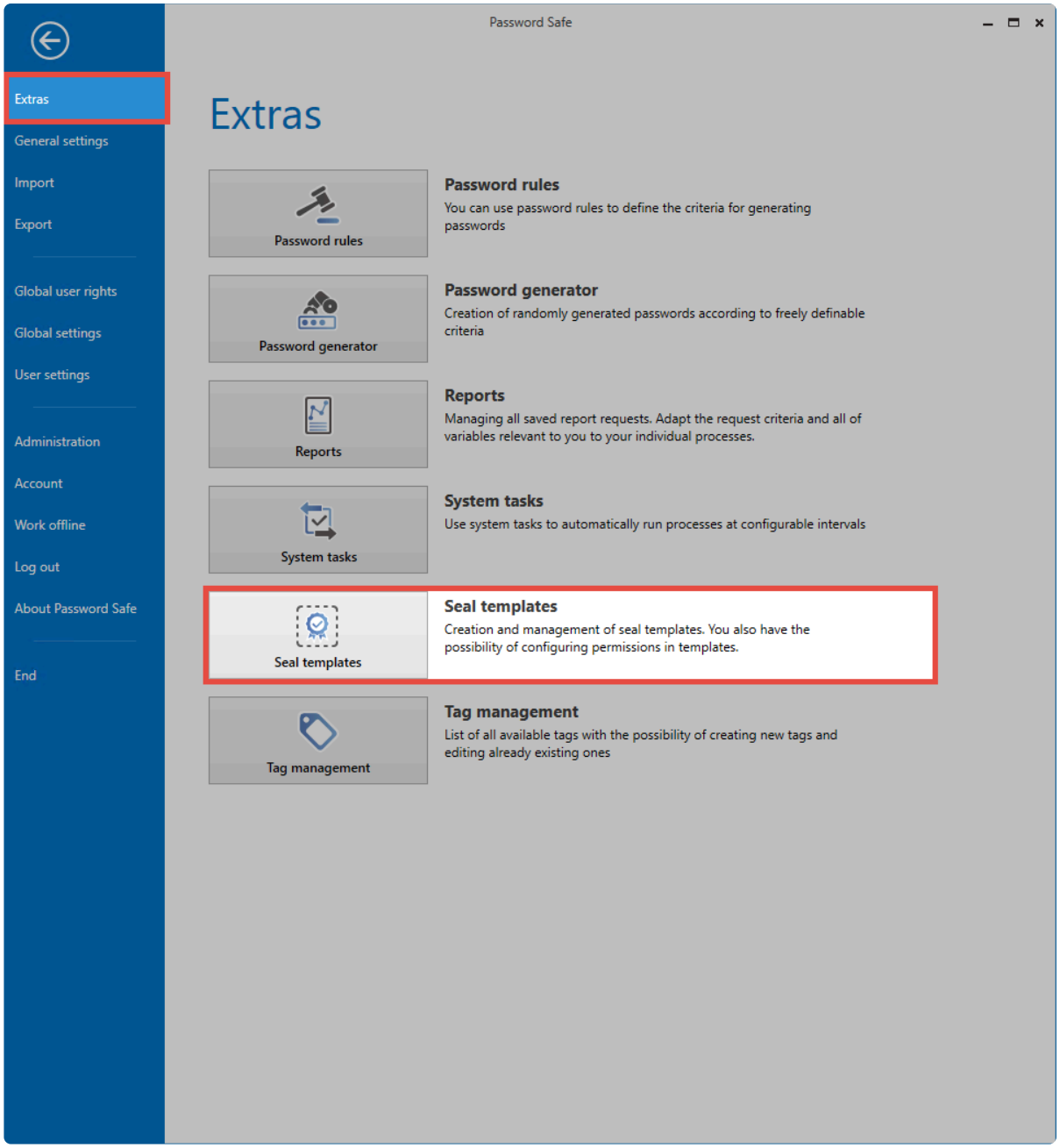
The password rules themselves are not subject to any permissions. All defined rules are therefore available to all users. The rules are managed from the Main menu.

Users can only manage the rules if they have the appropriate user right

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.

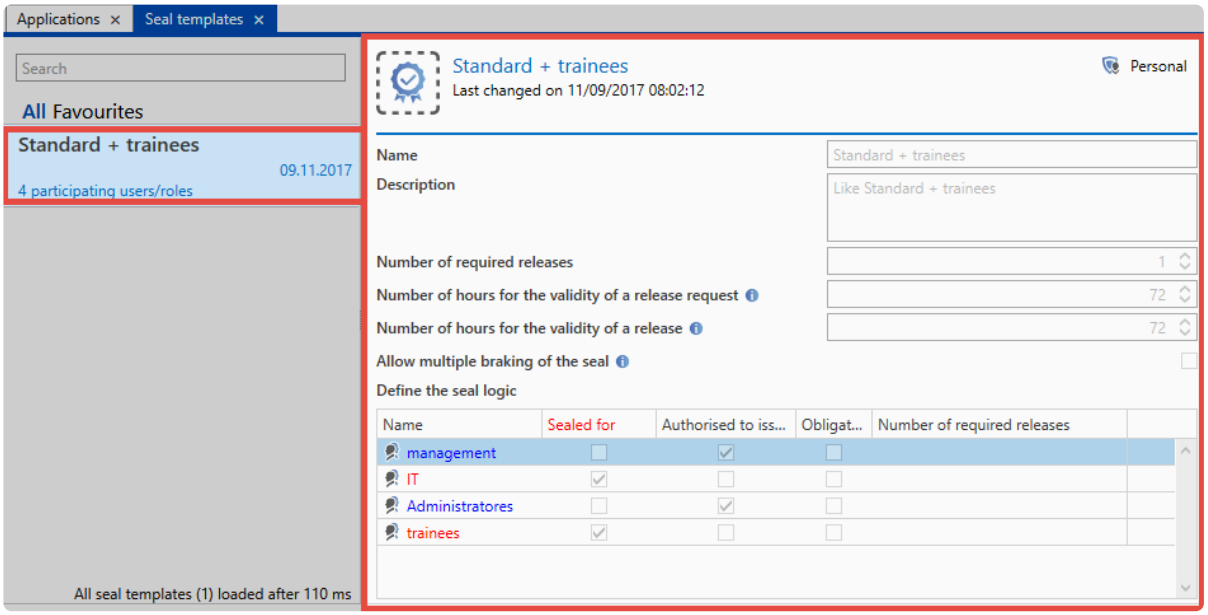


A separate tab opens in the active module in order to edit the default templates

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.

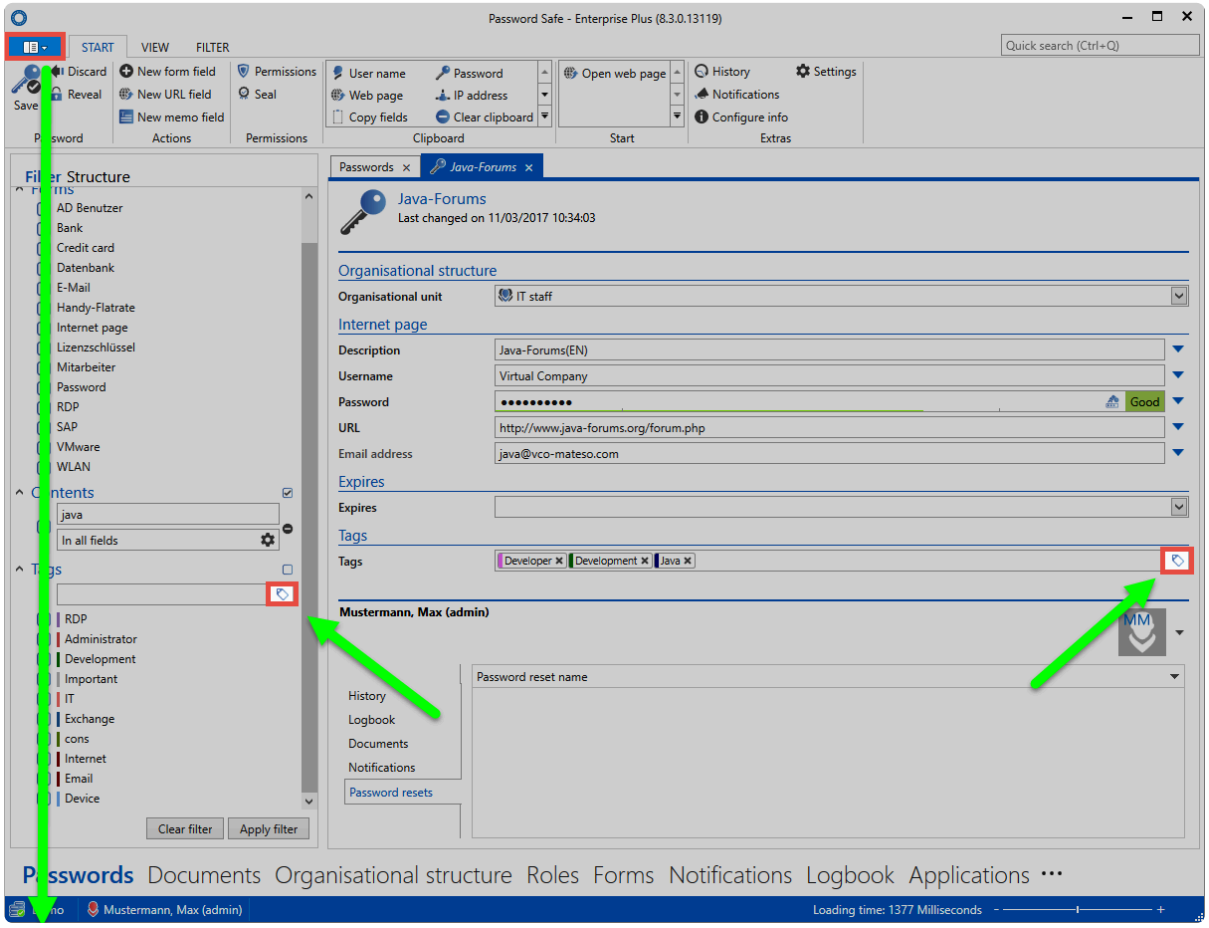


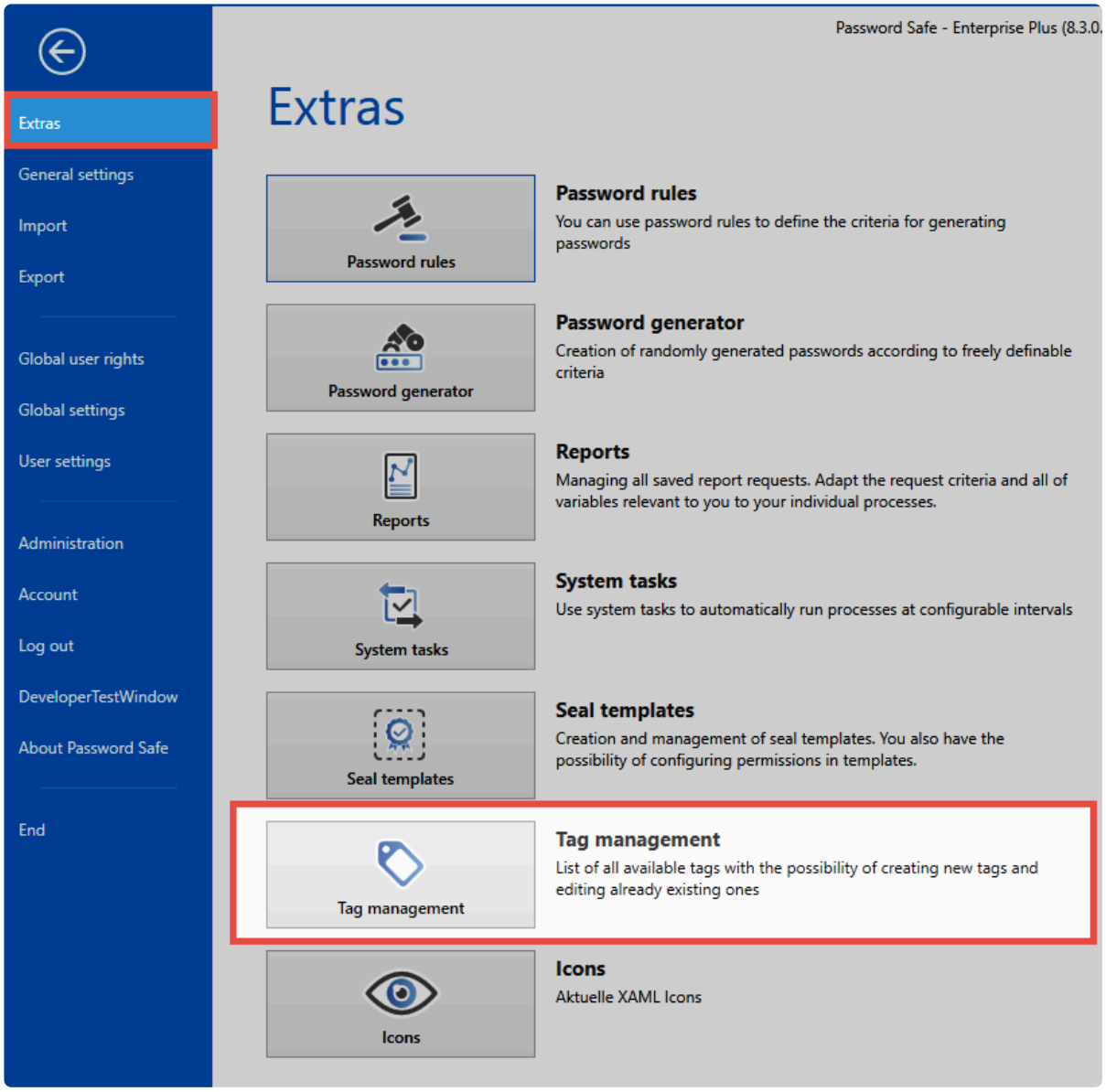
Once templates have been added, they can be immediately used for the creation of new seals.

Tag manager

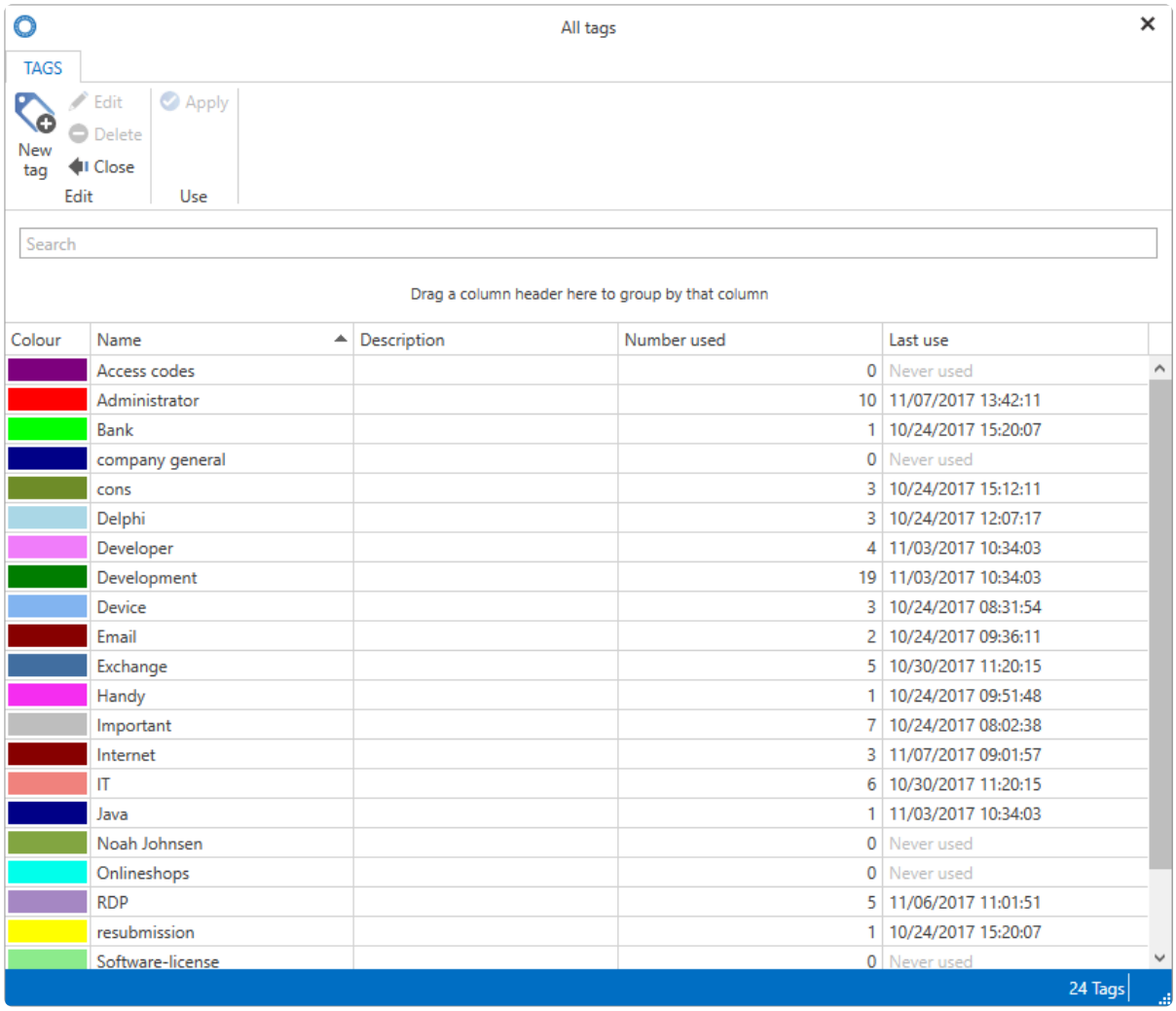
What is the tag manager?

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”.





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.



Relevant rights

The following option is required for managing tags

User right

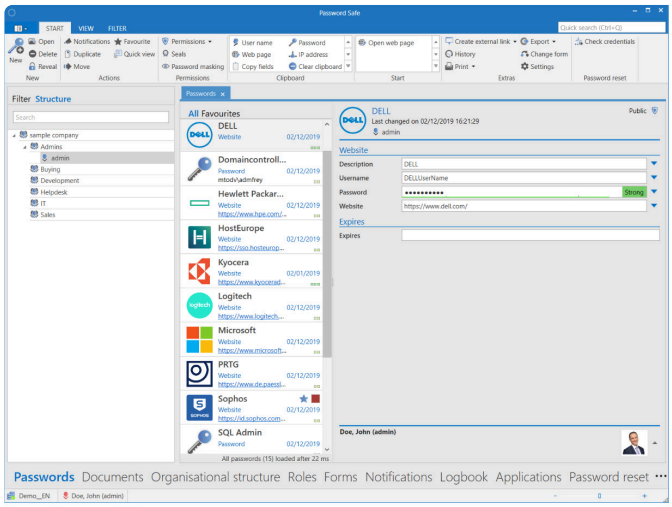
- Manage tags

> ! It is only possible to delete tags if there are no more data associated with them

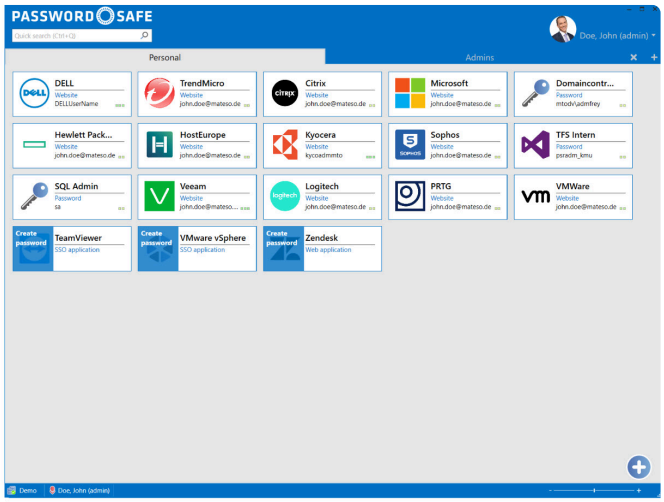
Image management

What is image management?

All logos and icons are managed in the image management. They can then be linked to the corresponding data records. The images are then displayed in the LightClient as well as in the list view of the client.



Windows Client



Light Client

Relevant rights

The following options are required:

- Can upload new password images
- Can manage password images

> It is important that the setting **“Ask for Favicon-Download “** is only considered, if the right **“Can upload new password images “** has been activated!

Managing Icons/Logos

There are two ways to upload icons.

1. By creating or saving the dataset.

In order to import favicons directly when saving the data set, the following preconditions must be met:

- Setting **“Ask Favicon-Download “** is activated.
- A URL is stored in the data record.

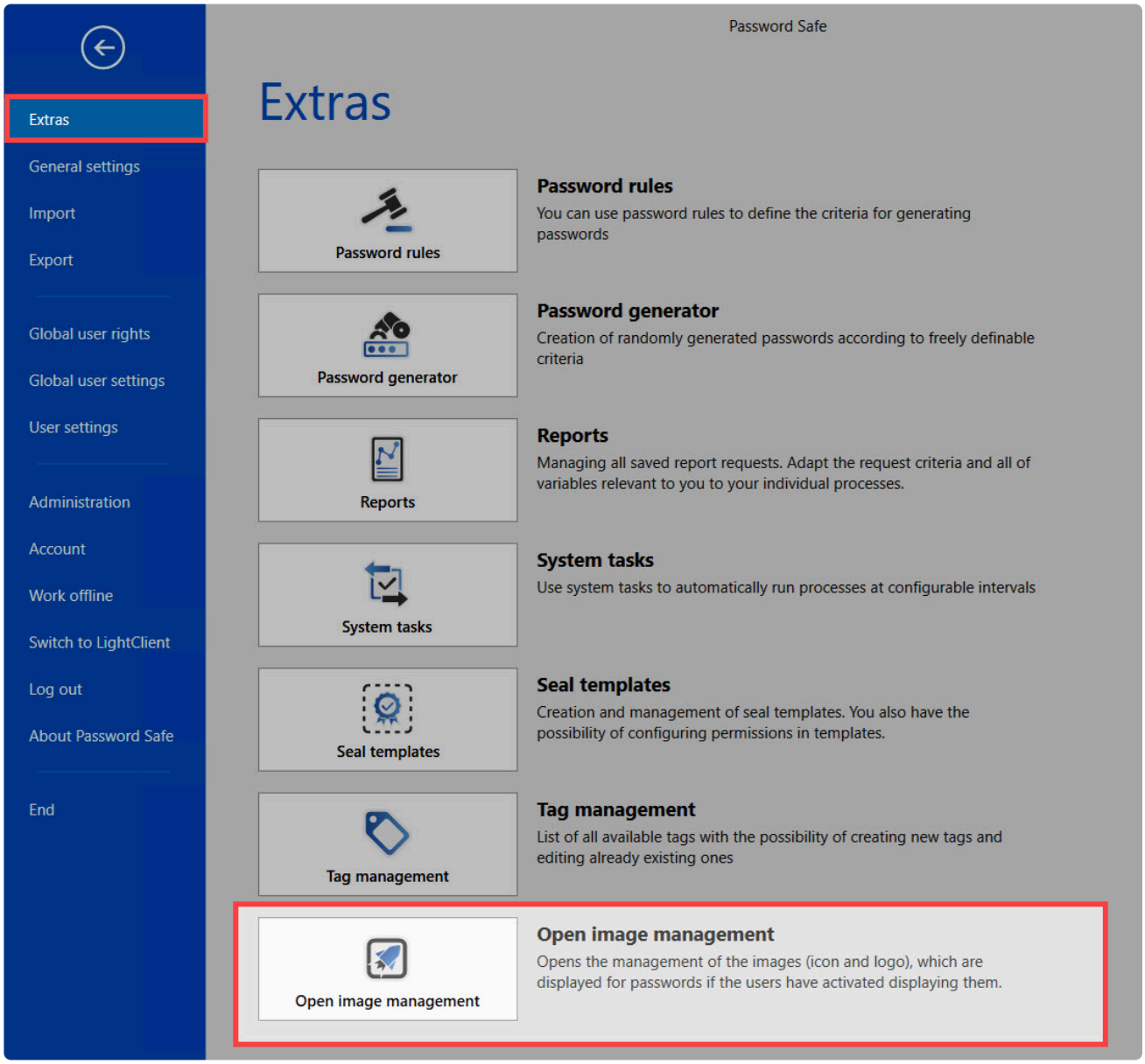
If these preconditions are met, the stored URL is checked for the favicon when saving the data record. If

a favicon is found, it will be imported into the database and displayed in the data record in future.

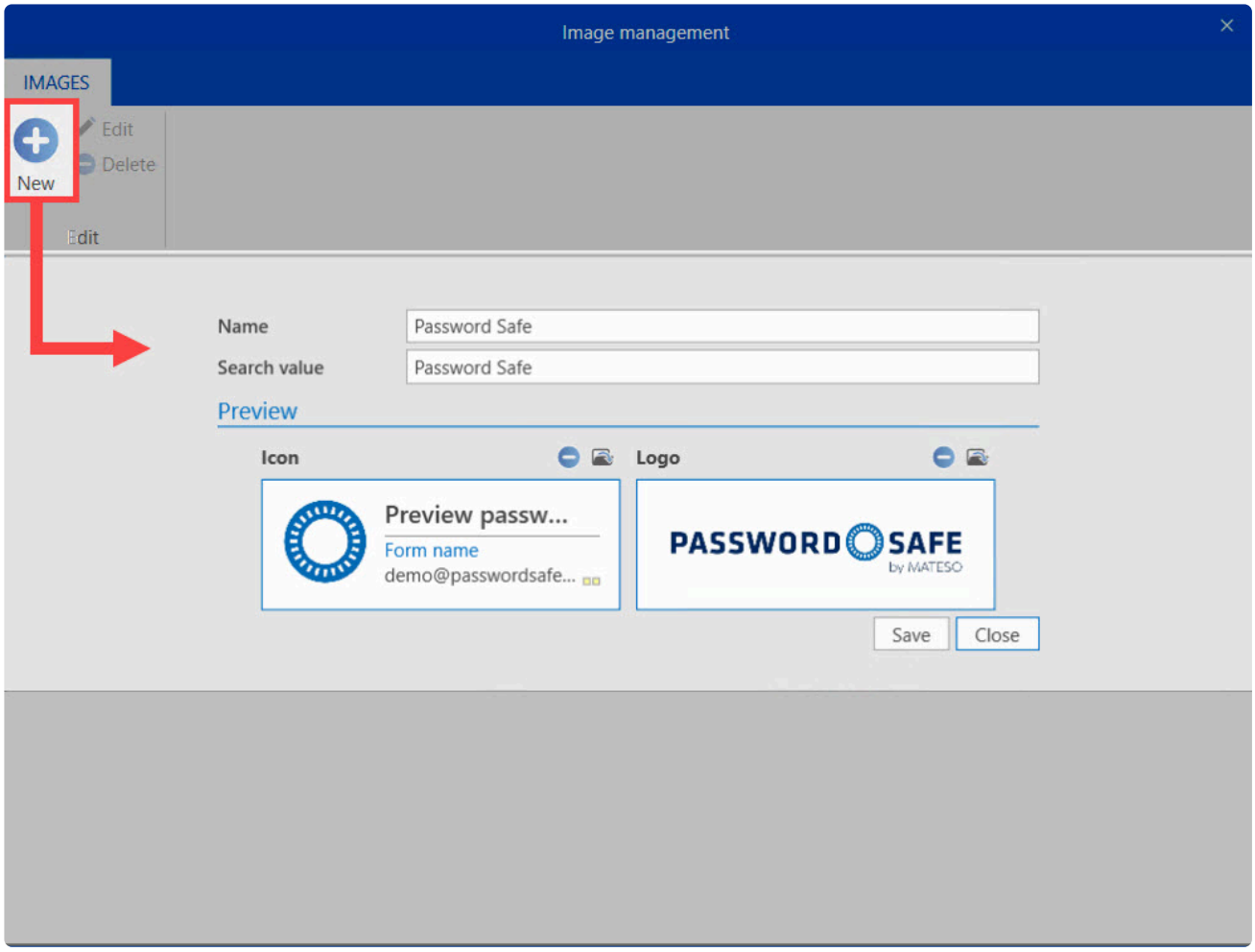
If there are several deposited, always use the first one.

2. Manual filing

In the main menu in extras you can find the image management. Here, you have the possibility to store icons and logos manually.



Click on the **+** symbol to open the mask for creating images.



- **Name** Name the picture here.
- **Search value** The following priority must be observed:
  - **Passwords**: first URL in the password (if several URLs are stored) -> attached tags -> password name -> names of connected applications
  - **Applications**: URL stored in the application -> attached tags -> application name
- This symbol can be used to upload locally saved icons and logos.

Please note that the icons and logos are not stored locally, but in the database.

Conditions

The following conditions must be met for icons/logos to be uploaded and saved accordingly:

- The maximum size of an image file is 100 MB.
- Supported formats are png, jpg, bmp, ico, .svg
- Several search values can be separated by a comma (“Netflix.de, Netflix.com”).

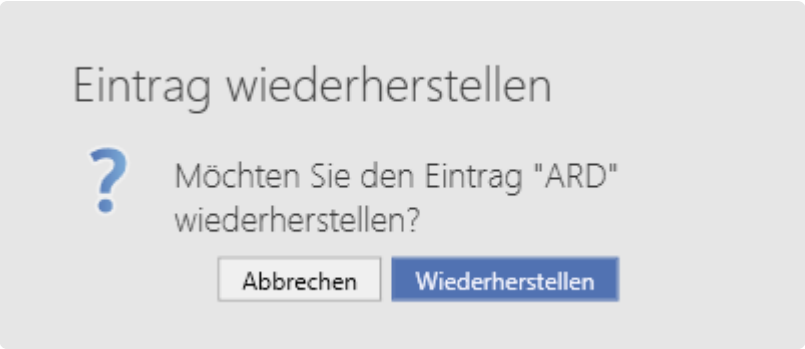
Papierkorbverwaltung

Hier kann der angemeldete Benutzer seinen Papierkorb verwalten. Es werden alle gelöschten Passwörter angezeigt, auf die der Benutzer berechtigt ist.

Funktionen

Folgende Funktionen stehen Ihnen zur Verfügung:

- **Wiederherstellen**: Es werden die ausgewählten Passwörter wieder hergestellt.



- **Endgültig löschen**: Die ausgewählten Passwörter werden endgültig gelöscht. Damit können diese nicht mehr wiederhergestellt werden.
- **Papierkorb leeren**: Der komplette Papierkorb wird endgültig gelöscht, somit kann keines dieser Passwörter wiederhergestellt werden.

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.

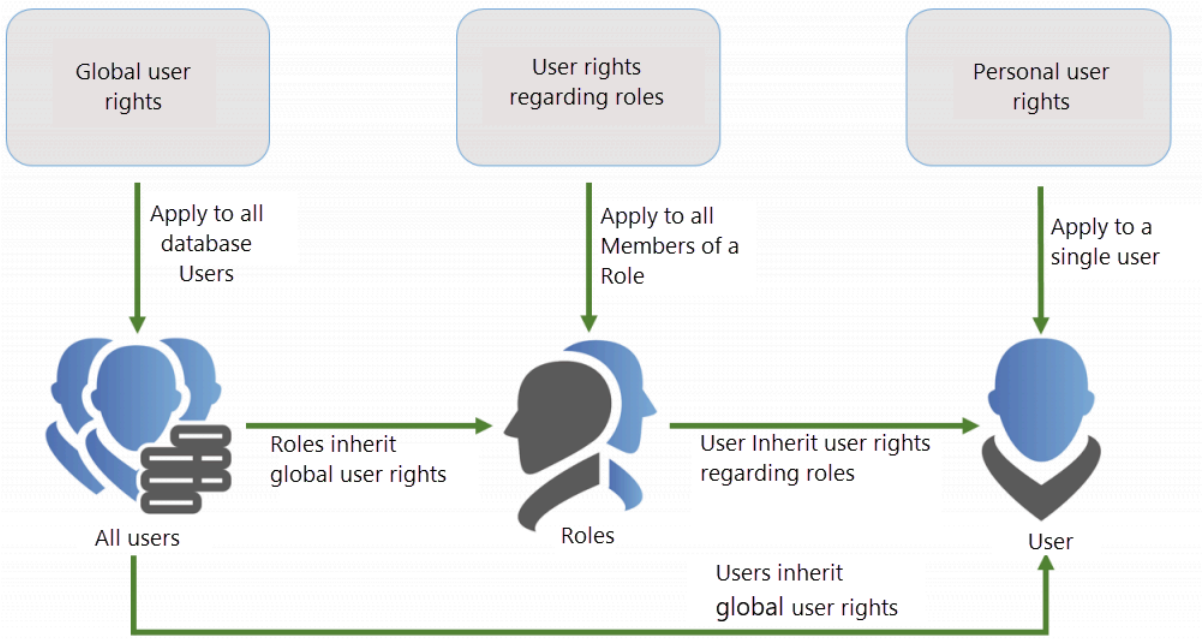
User rights

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.



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.

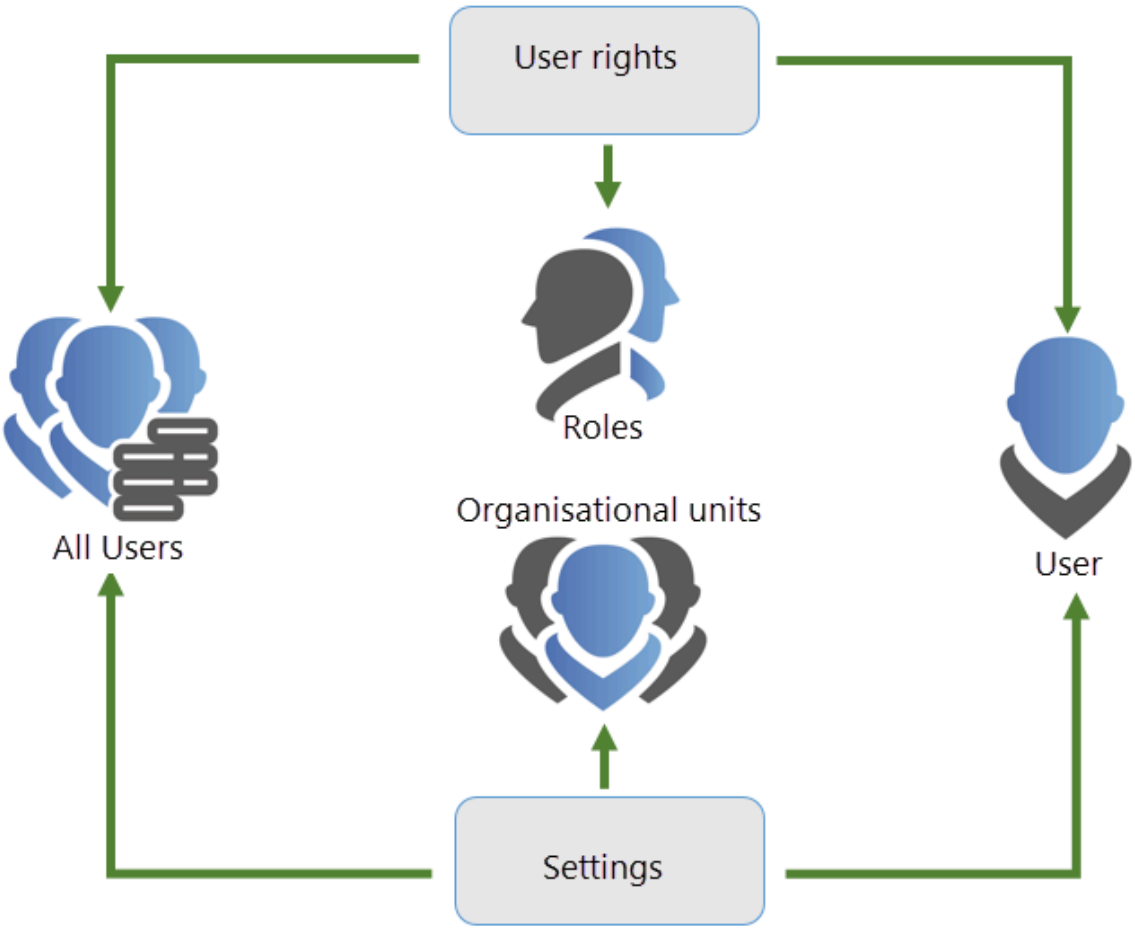
User rights to roles apply to all members of a role and are specified in the roles module

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.



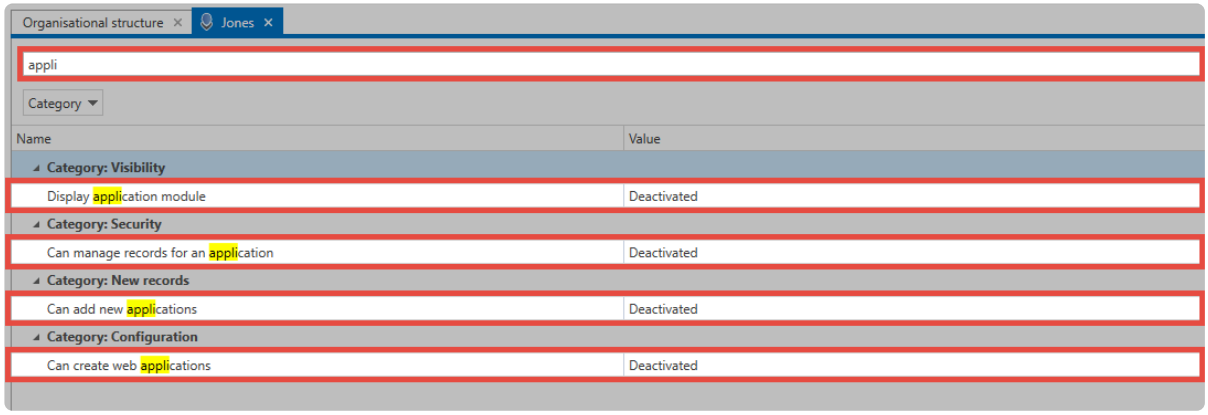
Configuring the security level

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

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.



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.
- The user can also remove other users from the rights if they have the owner right.

Overview of all user rights

This section lists all of the existing user rights. If a right is explained in more detail in another section, you can navigate directly to this section by clicking on the link in the **Section** column. The rights are grouped according to categories to provide a better overview.

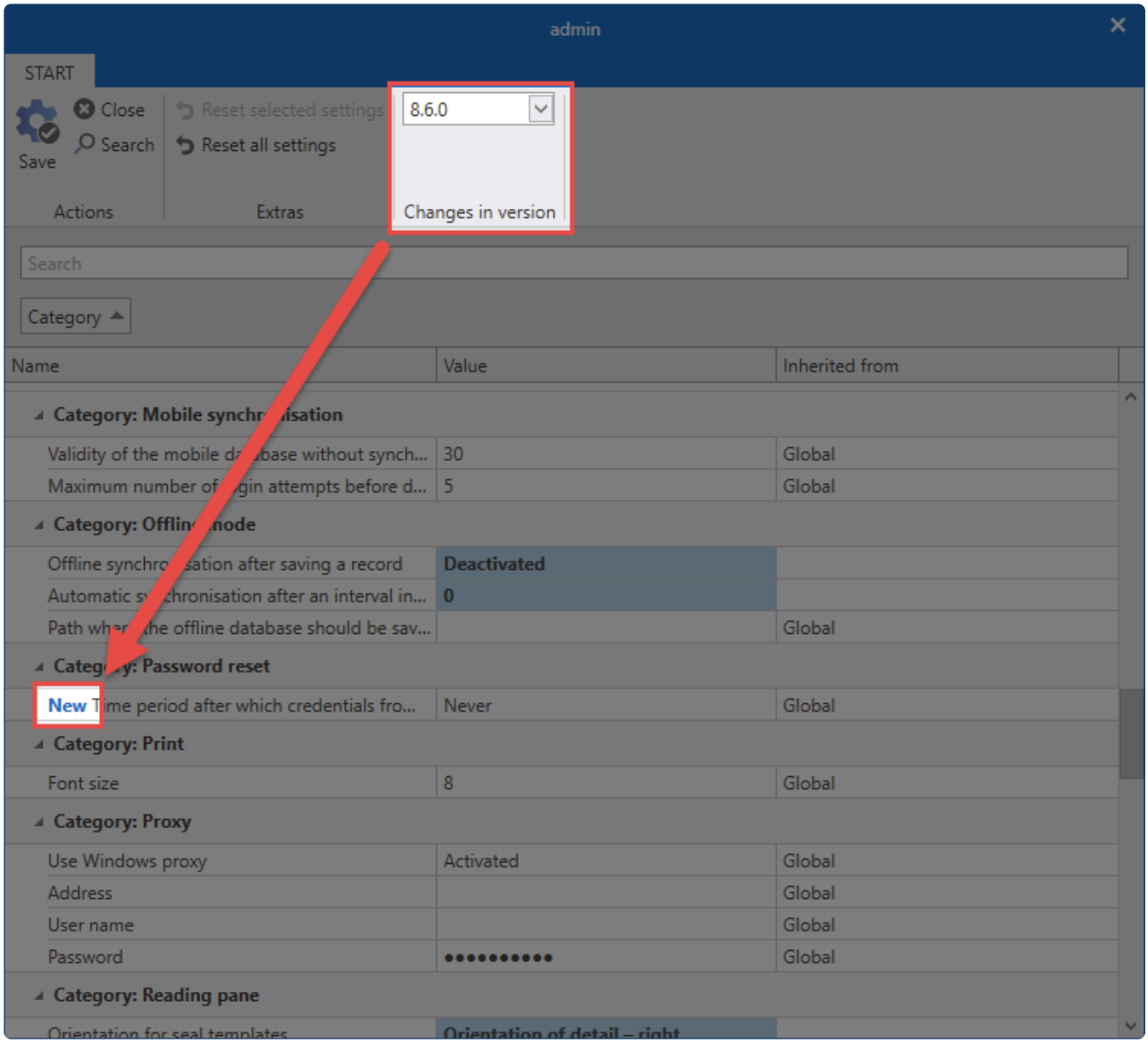
Category: General	**User right**	**new**
Can overwrite permissions	Form field permissions	
Test	Testlink	
Can inherit permissions	Form field permissions	
Category: Footer area	**User right**	**new**
Can see notifications in the footer area	Reading pane	
Can see the metadata for documents in the footer area	Reading pane	
Can see documents in the footer area	Reading pane	
Can see the history in the footer area	Reading pane	
Can see the logbook in the footer area	Reading pane	
Can see the Password Reset in the footer area	Reading pane	
Category: Configuration	**User right**	**new**
Can print	Print	
Can export	Export	
Can edit filter	Filter	
Can change form for a password	Change form	
Can import	Import	
Can manage password form fields		
Can apply password masking	Password masking	
Can apply seal	Seal	
Can manage seal templates	Seal templates	
Can manage tags	Tags	
Can close tab of own organizational unit in LightClient		
Category: Mobile synchronisation	**User right**	**new**
Can synchronise with mobile devices	Mobile devices	
Category: New records	**User right**	**new**
Can add new Active Directory profiles	End to end / Master Key	

Can add new RDP applications	Learning the applications	
Can add new SSH applications	Learning the applications	
Can add new SSO applications	Learning the applications	
Can add new web applications	Learning the applications / Applications	
Can add new users	Managing users	
Can add new documents	Documents	
Can add new forms	Forms	
Can add new organisational units	Organisational structures / Managing users	
Can add new Password Resets	Password Reset	
Can add new passwords	Passwords / Creating new passwords	
Can add new roles	Roles	
Can add new tags	Tags	
Can add individual passwords via LightClient		
Can add new passwords images		
Cand add new SAML applications		
Category: Offline mode	**User right**	**new**
Offline mode	Setting up and synchronizing	
Timespan for how long the offline mode can be used without connection to the server	Setting up and synchronizing	
Kategorie: Rights	**User right**	**new**
If non-administrators select “Override permissions” when moving items, keep existing permissions for administrators		✔
Category: Rights templates	**User right**	**new**
Can edit members when using a rights template		
Can manage rights templates	Relevant user rights	
Can view selection of rights templates	Relevant user rights	
Can switch standard rights template	Relevant user rights	
Category: Security	**User right**	**new**
Is database administrator		

Can manage Active Directory profiles		
Can authorize other users to use personal passwords		
Can manage records for an application	Recording a session	
Can manage autologin	Account	
Can set owner rights		
Can manage database sessions		
Can permanently delete the deleted users		
Can permanently delete the deleted organisational structures		
Can view deleted organisational structures		
Can permanently delete the deleted roles		
Can view deleted roles		
Can manage locked users		
Can edit global settings		
Can export HTML WebViewer	HTML WebViewer	
Can change security level options		
Can manage password rules	Password rules	
Can create personal records		
Can configure standard password rules	Administration	
Can carry out batch processing for permissions based on a filter	Multiple editing of permissions	
Can manage password images		
Category: Visibility	**User right**	**new**
Display application module	Client Module	
Display notification module	Client Module	
Show discovery service module	Client Module / Discovery service	
Display document module	Client Module	
Display form module	Client Module / Forms	
Display logbook module	Client Module / Logbook	
Display organisational structure module	Client Module / Organisational structure	
Display Password Reset module	Client Module / Password	

	Reset	
Display password module	Client Module / Creating new passwords	
Display roles module	Client Module / End-to-end / Master Key / Roles	
Category: System tasks	**User right**	**new**
Can manage Active Directory system tasks	System task	
Can manage system task reports	System task	
Can manage discovery service system tasks	System task / Discovery service	
Can manage Emergency WebViewer export system tasks	System task TOPIC-LINK+system-tasks}	
Can manage WebViewer export system tasks	System task	

There is a version selection box in the user rights. The options that were newly added in the selected version are correspondingly marked in the list.



This makes it easier for administrators to correctly configure new options before they release the update for all employees.

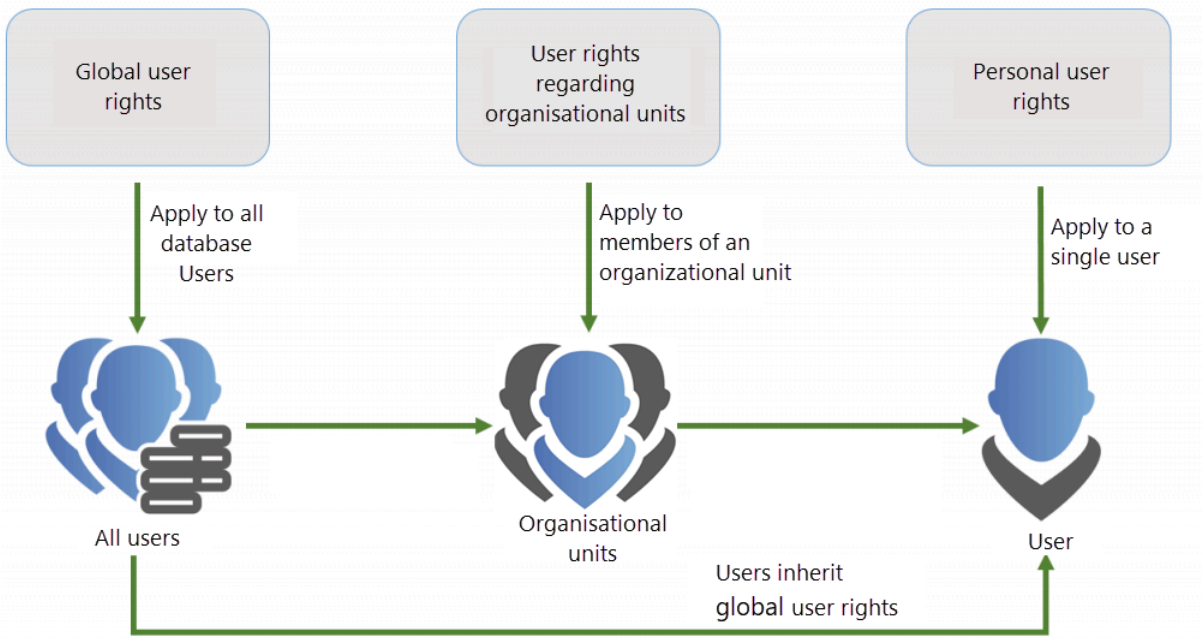
User settings

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.

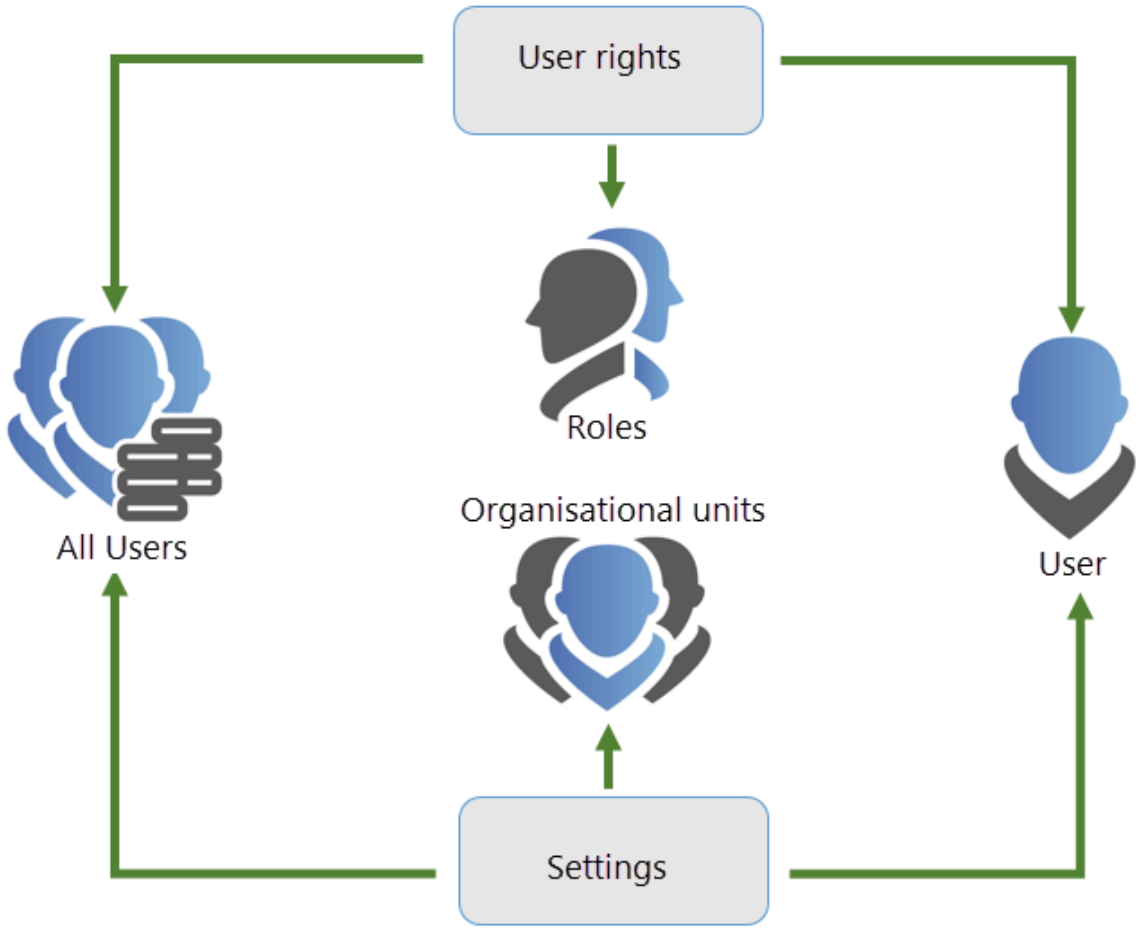


The focus is always on the user, also when it comes to user rights. It can obtain its settings in one of the following three ways:

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!

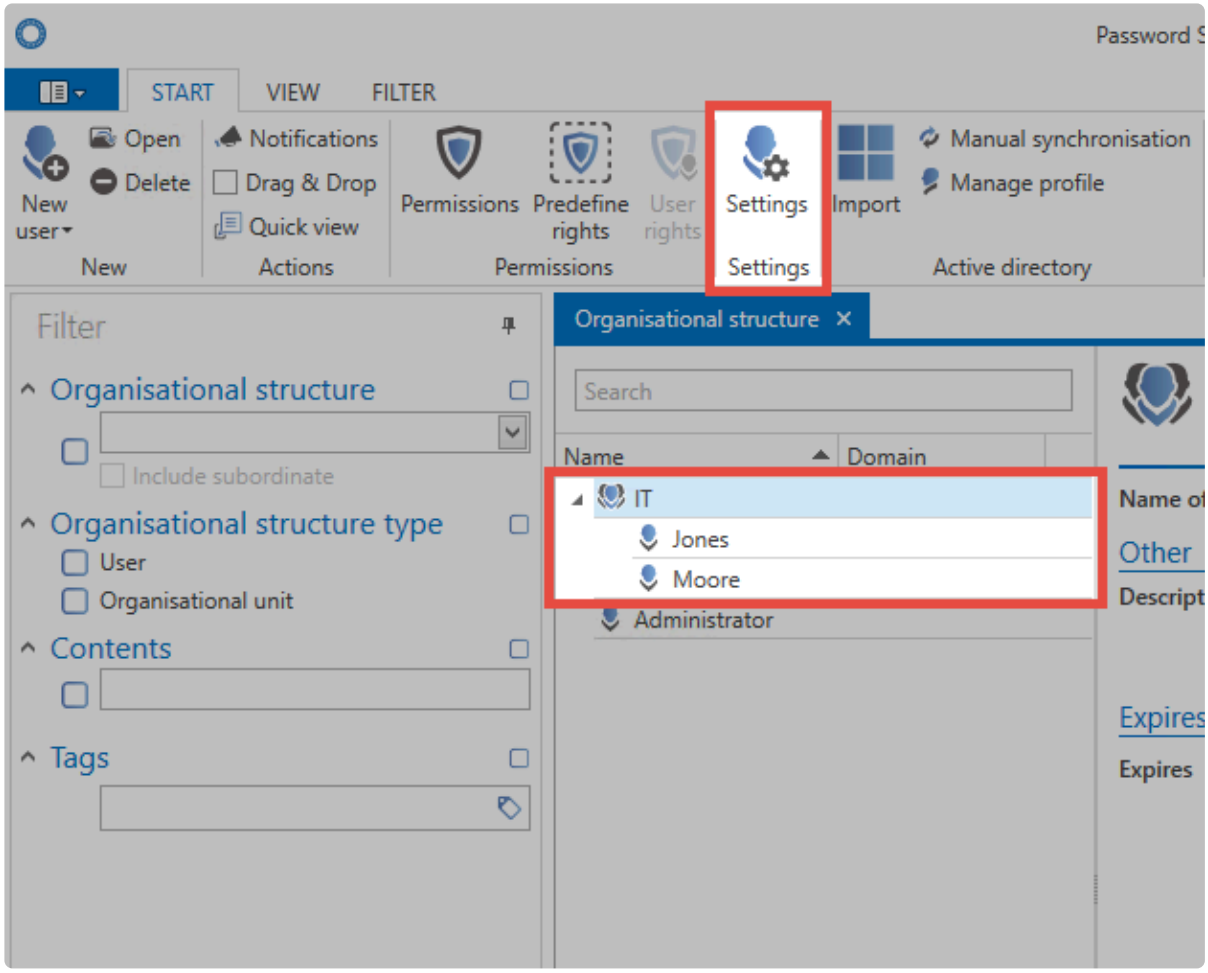


Inheritance of user settings

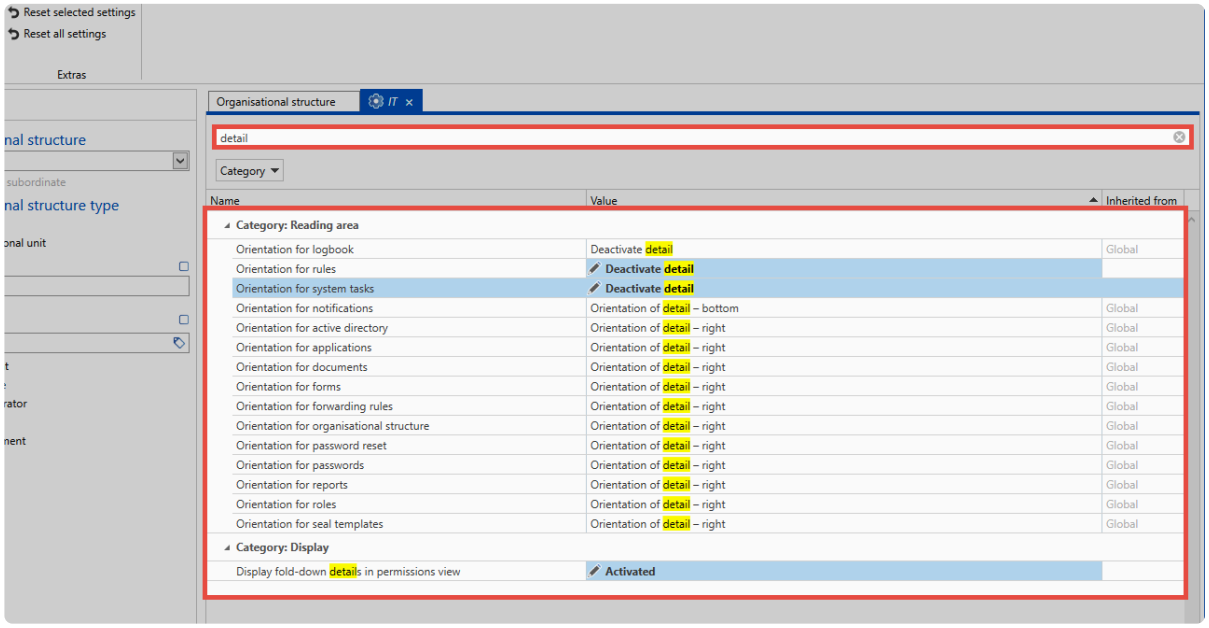
If you leave the personal settings on the outside, there are two ways to inherit settings:

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.

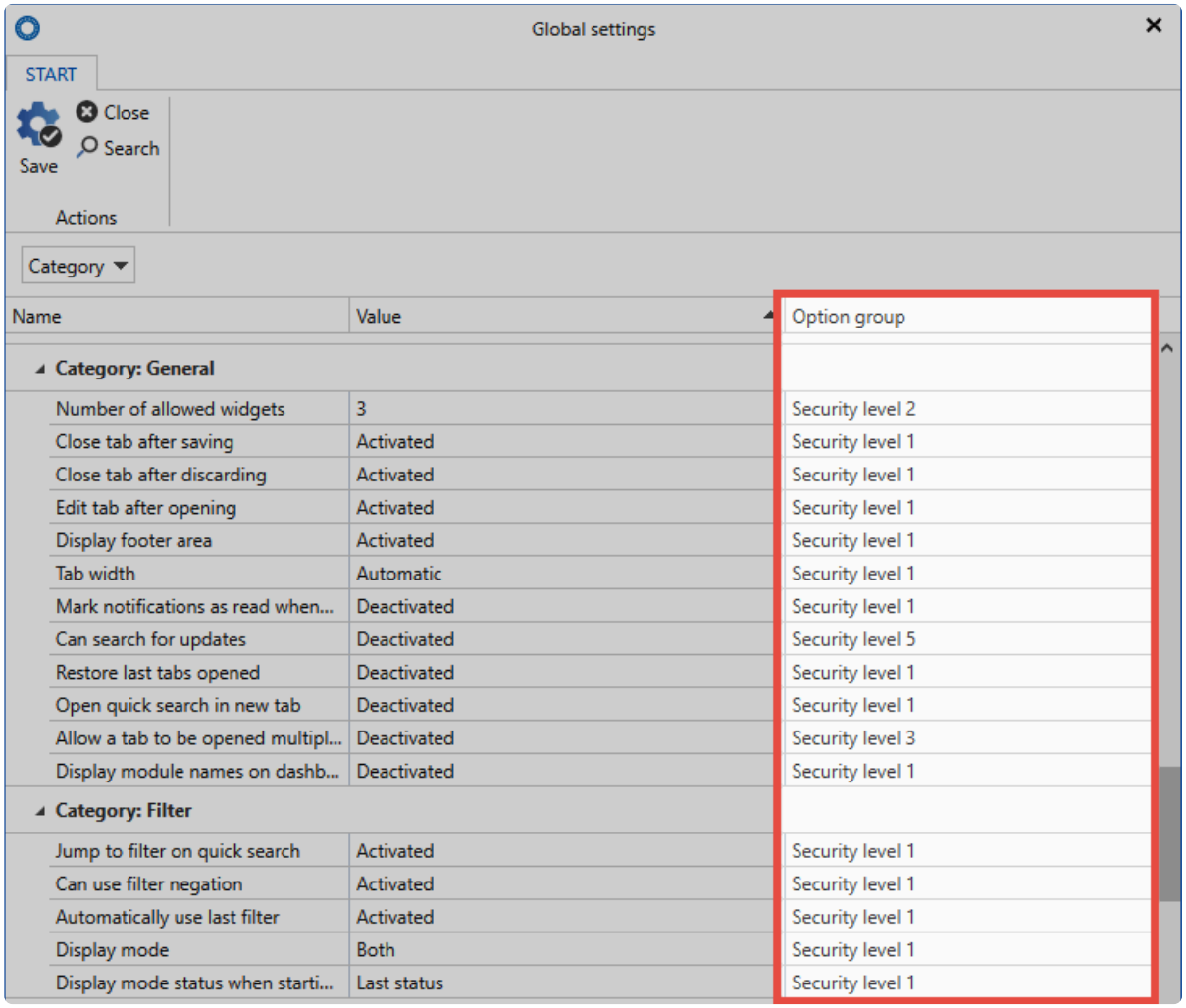


The diagram shows the settings for the user “Jones”. The search has been filtered by the term “Detail”. The column **“Inherited from”** shows that some settings have been inherited globally, or by the organisational unit “IT”. The top two options have no value in the column. This is because this parameter 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.



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.

Overview of all settings

This section lists all of the existing settings. If a setting is explained in more detail in another section, you can navigate directly to this section by clicking on the link in the **Section** column. The settings are grouped according to categories to provide a better overview.

Category: General	Setting	Section	new
Number of allowed widgets	Dashboard & widgets		
Mark notifications as read when opening them			
Can search for updates			
Allow a tab to be opened multiple times			
Display module name on dashboard	Dashboard & widgets		
Open quick search in new tab			
Edit tab after opening			
Close tab after saving			
Close tab after discarding			
Tab width			
Restore last tabs opened			
Ask for favicon download			
Category: Display	**Setting**	**Section**	**new**
Customizable window caption			
Display fold-down details in permissions view			
Change lists when widening in table view			
Display path for the organisational structure in the header			
Scaling value for the user interface			
Display kind of password in full client			
Display kind of passwords in LightClient			
Switch logo view on mouse over in LightClient			
Category: Browser	**Setting**	**Section**	**new**
Standard browser			
Category: Dashboard	**Setting**	**Section**	**new**
Display dashboard on startup	Dashboard & widgets		
Display remaining amount of data in the widget			

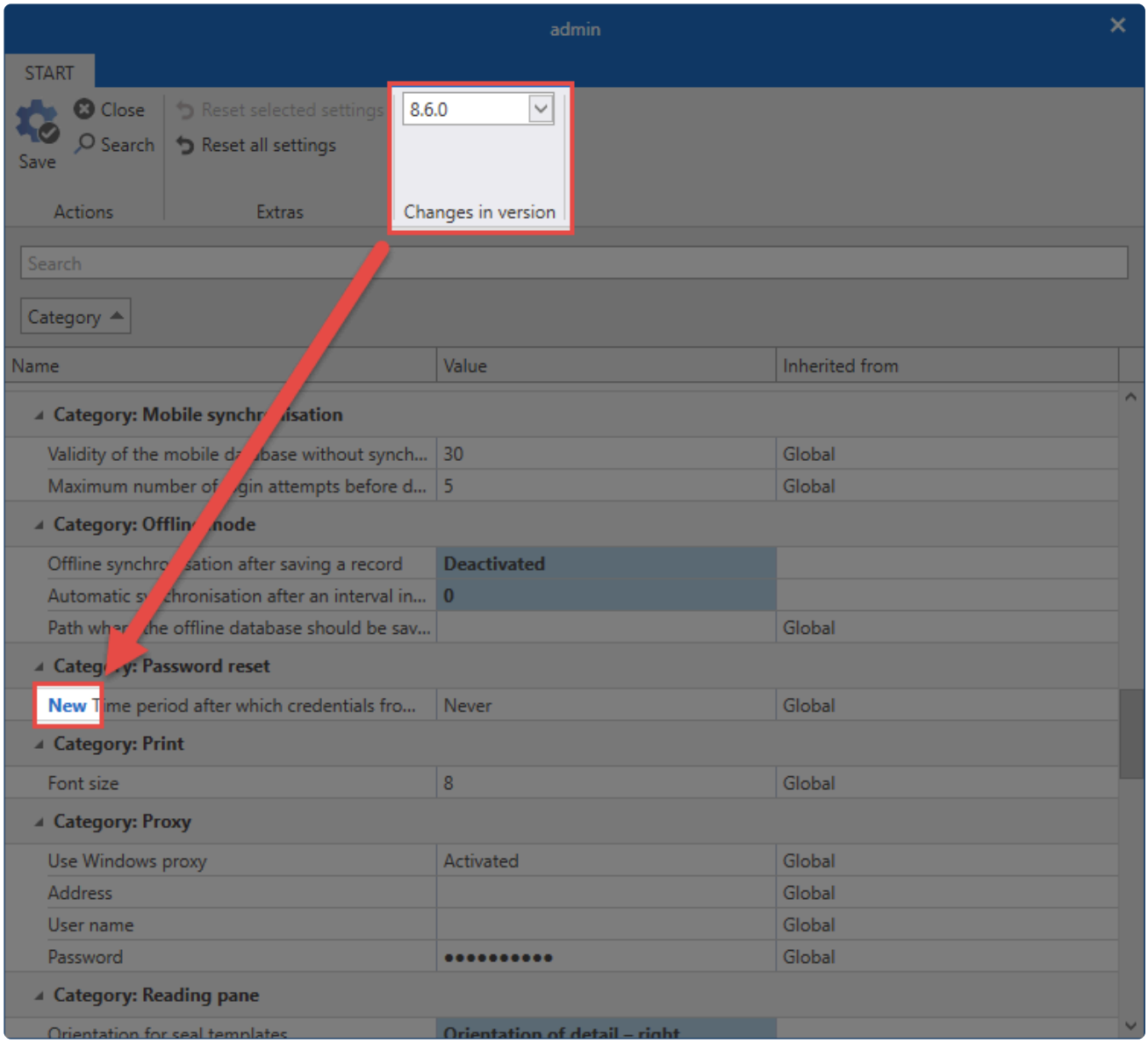
Category: Record	Setting	Section	new
Number of initially loaded records			
Display records as “about to expire” if the remaining days are less than			
Apply form changes to passwords			
Display total number of filter results			
Maximal number of search results for **all**			
Category: Documents	**Setting**	**Section**	**new**
Document history			
Permitted document extensions			
Maximum size in MB			
Category: Print	**Setting**	**Section**	**new**
Font size			
Category: Real-time update	**Setting**	**Section**	**new**
Refresh notifications in real time			
Category: Filter	**Setting**	**Section**	**new**
Display mode	Display mode		
Jump to filter on quick search	Display mode		
Can use filter negation	Advanced filter settings		
Automatically use last filter	Display mode		
Display mode status when starting the program	Display mode		
Category: Footer area	**Setting**	**Section**	**new**
Show notifications in the footer area	Reading pane		
Show documents in the footer area	Reading pane		
Display footer area	Reading pane		
Show history in the footer area	Reading pane		
Show logbook in the footer area	Reading pane		
Show metadata in the footer area	Reading pane		
Show Password Resets in the footer area	Reading pane		
Category: Configuration	**Setting**	**Section**	**new**
Display animation in SSO configuration window			

You must enter a reason for establishing the RDP connection	Operation & set up		
You must enter a reason for establishing the SSH connection			
Password Safe user directory			
Default form (for LightClient)			
Start LightClient on next login			
Include subordinated organizational units in LightClient			
Category: Reading pane	**Setting**	**Section**	**new**
Orientation for Active Directory	Operation & set up		
Orientation for applications	Operation & set up		
Orientation for notifications	Operation & set up		
Orientation for reports	Operation & set up		
Orientation for documents	Operation & set up		
Orientation for forms	Operation & set up		
Orientation for logbook	Operation & set up		
Orientation for organisational structure	Operation & set up		
Orientation for Password Reset	Operation & set up		
Orientation for passwords	Operation & set up		
Orientation for rules	Operation & set up		
Orientation for roles	Operation & set up		
Orientation for seal templates	Operation & set up		
Orientation for system tasks	Operation & set up		
Orientation for forwarding rules	Operation & set up		
Size of profile image in reading area	Operation & set up		
Category: Mobile synchronisation	**Setting**	**Section**	**new**
Validity of the mobile database without synchronisation in days (0 = no limit on validity)	Mobile devices		
Maximum number of login attempts before deleting the database (0 = unlimited)	Mobile devices		
Category: Offline mode	**Setting**	**Section**	**new**
Automatic synchronisation after an interval in minutes (0 for deactivated)	Setting up and synchronizing		
Offline synchronisation after saving a record	Setting up and		

	synchronizing		
Path where the offline database should be saved (empty for standard)	Setting up and synchronizing		
Category: Proxy	**Setting**	**Section**	**new**
Address			
User name			
Password			
Use Windows proxy			
Category: Rights	**Setting**	**Section**	**new**
Clear user field after adding			
Inherit permissions for new objects (without rights template)	Inheritance from organisational structures		
Existing passwords inherit changes to the permissions for organisational units	Inheritance from organisational structures		
Permission search: Add gradually			
Delete user from the permissions for new objects when the user creating the new object is authorized via a role			
Hide deleted users and roles in permissions			
Category: Security	**Setting**	**Section**	**new**
Change rule for the user password			
Disconnect database connection due to inactivity after			
Deactivate inactive users			
Confirmation of authenticity on login			
Length of validity of the multifactor authentication token (minutes)			
Minimum score for password quality level “good”			
Minimum score for password quality level “strong”			
Display password in quick view			
PKI: Enforce validity period for certificates			
PKI: Certificate hash methods			
PKI: Checking mode for certificate chains			

Time period after which inactive sessions will be deleted from the server			
Category: SSO	**Setting**	**Section**	**new**
Browser add-ons: Exact domain check	Add-ons		
Browser add-ons: Automatically send login masks	Add-ons		
Browser add-ons: Automatically fill login masks	Add-ons		
Browser addons: Show password			✔
Category: Keyboard shortcuts	**Setting**	**Section**	**new**
Execute script to enter the password in the selected window			
Execute script to enter the user name in the selected window			
Execute script to enter the user name and password in the selected window			
Execute script to enter the user name and password in the selected window using the Enter button			
Category: Clipboard	**Setting**	**Section**	**new**
Clearing the clipboard			
Clear clipboard on closing			
Clear clipboard on minimising			
Clipboard gallery			

There is a version selection box in the settings. The options that were newly added in the selected version are correspondingly marked in the list.

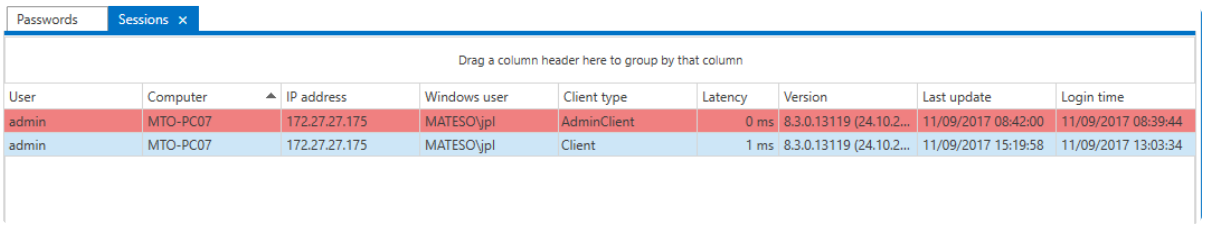


This makes it easier for administrators to correctly configure new options before they release the update for all employees.

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.



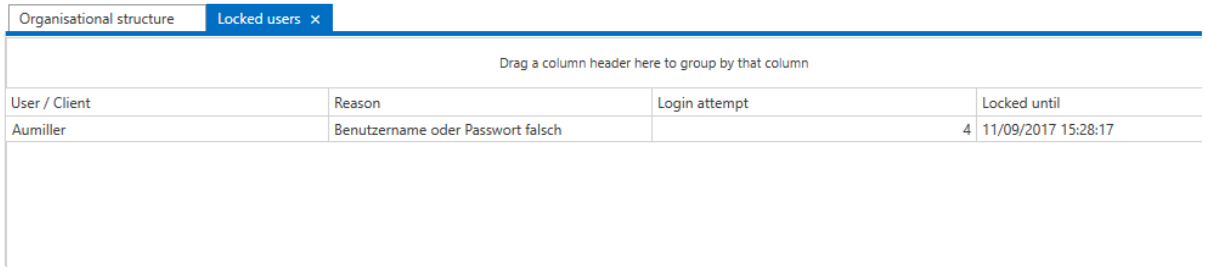
The session view starts in the currently active module in a separate tab.

Locked users

All currently locked users can also be retrieved. There are two scenarios here:

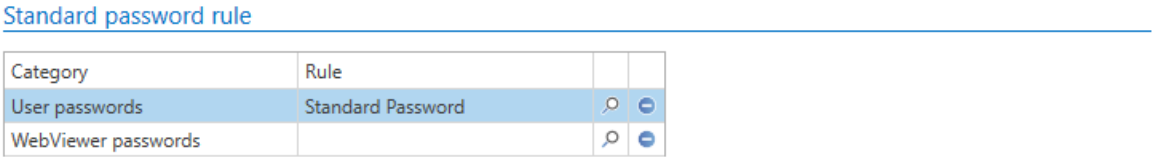
1. **User name correct, password incorrect**: The user name is displayed
2. **User name incorrect**: The client is displayed

In addition, the number of attempted logins and the length of time that the user was locked in each case can be seen.



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.



Relevant right

There is a separate option for defining the password rules for named passwords.

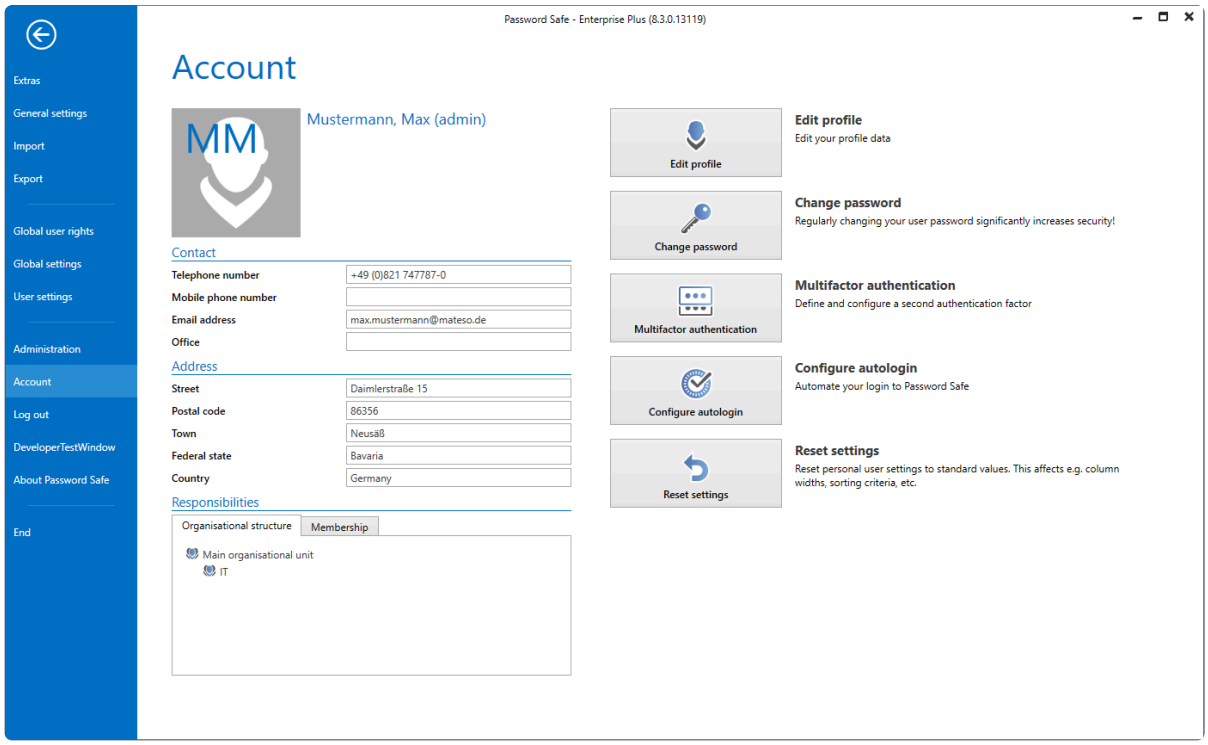
User right

- Can configure standard password rules

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.



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.

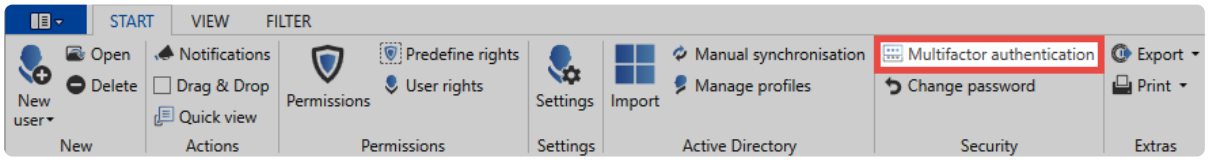
> Users who were imported from AD with the aid of Master Key mode log in with the domain password. Therefore, no password can be configured in this case.

> The strength of the user password can be stipulated by administration through the issuing of password rules. More…

> If a user changes his or her password, all sessions that are still open are automatically terminated.

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 autologin is linked to the hardware and thus will not work on a different computer. If you change the hardware or the hardware ID, an existing autologin needs to be recreated.

Relevant right

Option to manage the autologin

User right

- Can manage autologin

> ! The automatic login should be handled as a process critical to security. 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.

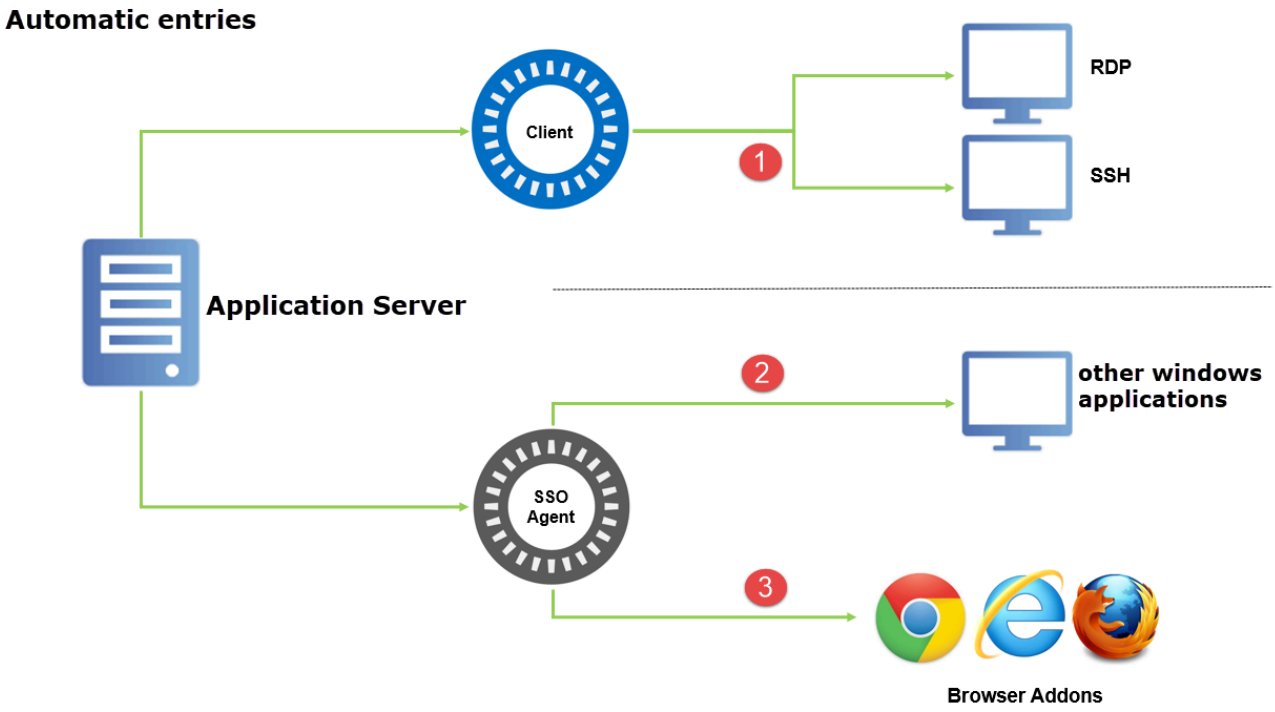
User rights

The right **Can create web applications** is required for creating new web applications

> The agent can control multiple databases at the same time

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).

> For entering data on websites, the record must contain at least the following fields: **User name**, **password**, **URL**.

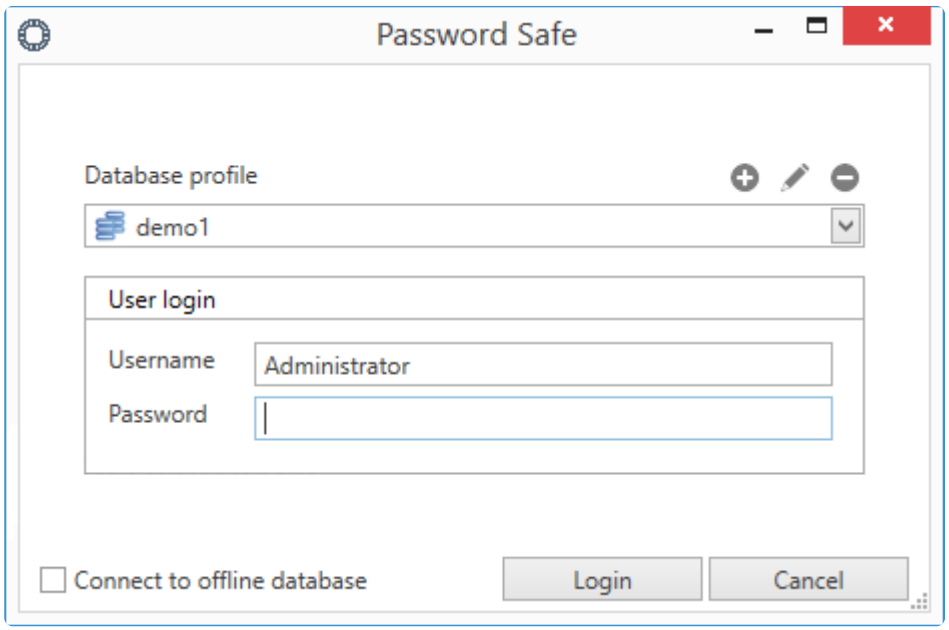
Conclusion

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.



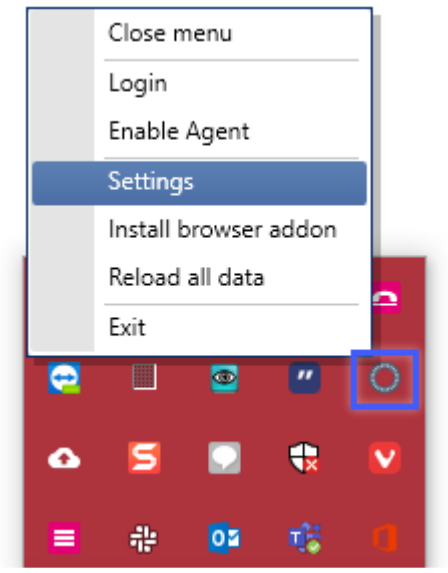
To log in, the desired database and the associated login data are firstly selected. The SSO agent makes all of the databases configured on the client available. It is also possible to create profiles as usual so that the connection data for certain databases can be used efficiently in the future.

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.

The following is required to ensure that data is entered on websites: **User name**, **password**, **URL**

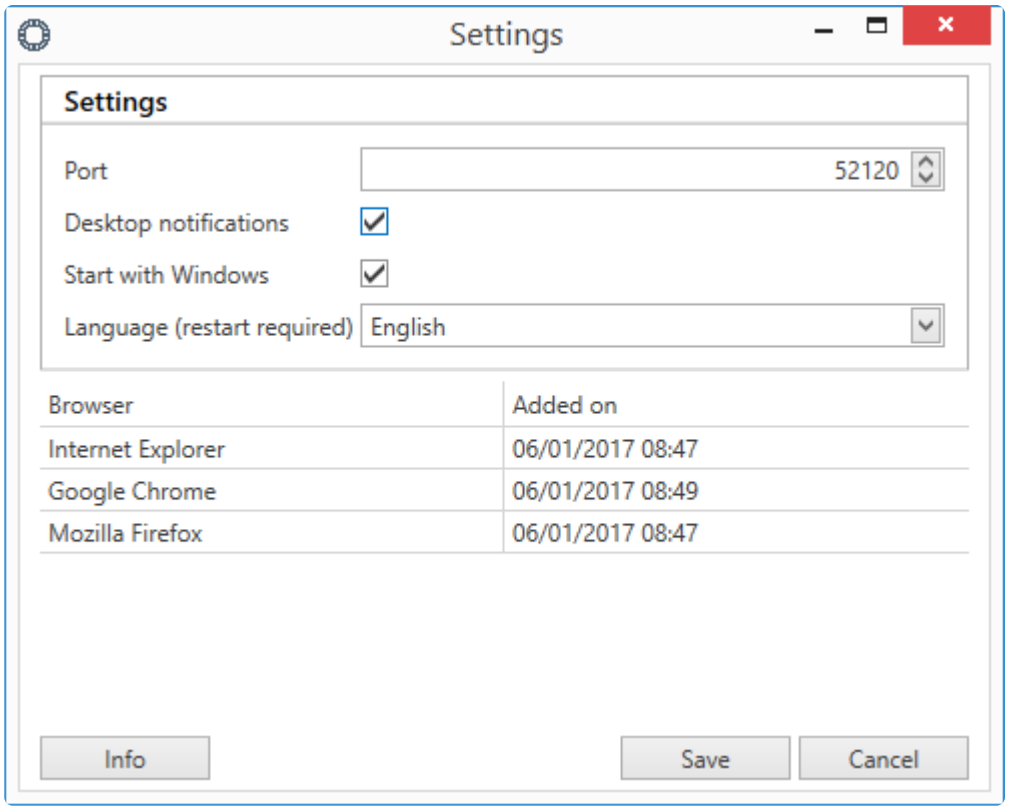
Context menu functionality

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)

Settings



- 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”:#addons 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 theSSO 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

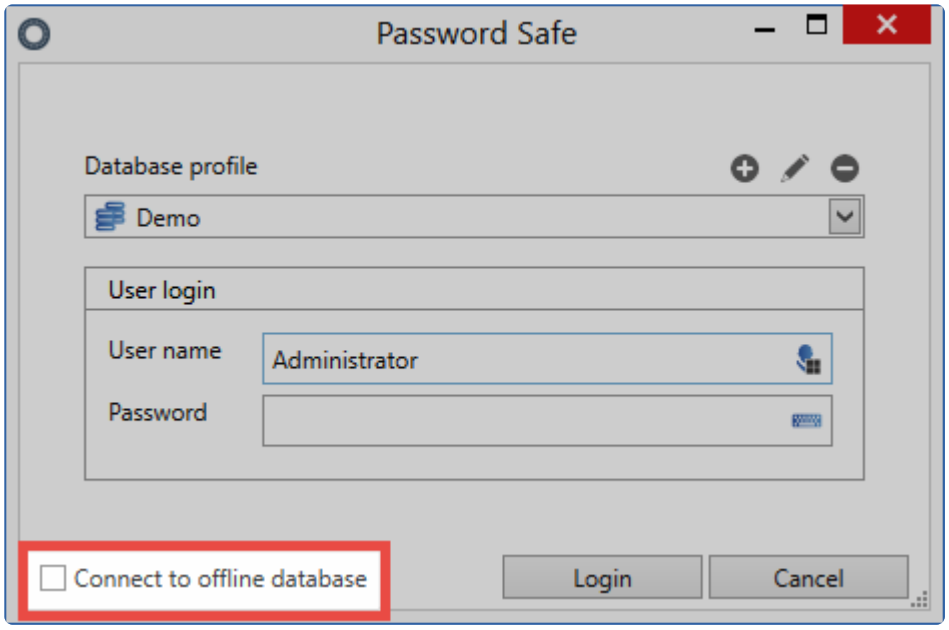
First, select the item **Connect to add-on** from the context menu in the agent. In the next window, select the desired browser. The browser will then open
and the settings for the add-on will be displayed. Usually, the terminal server ID has already been entered here. You just need to confirm it.

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.


Password Safe
Database profile
Demo
User login
User name
Administrator
Password
Connect to offline database
Login
Cancel

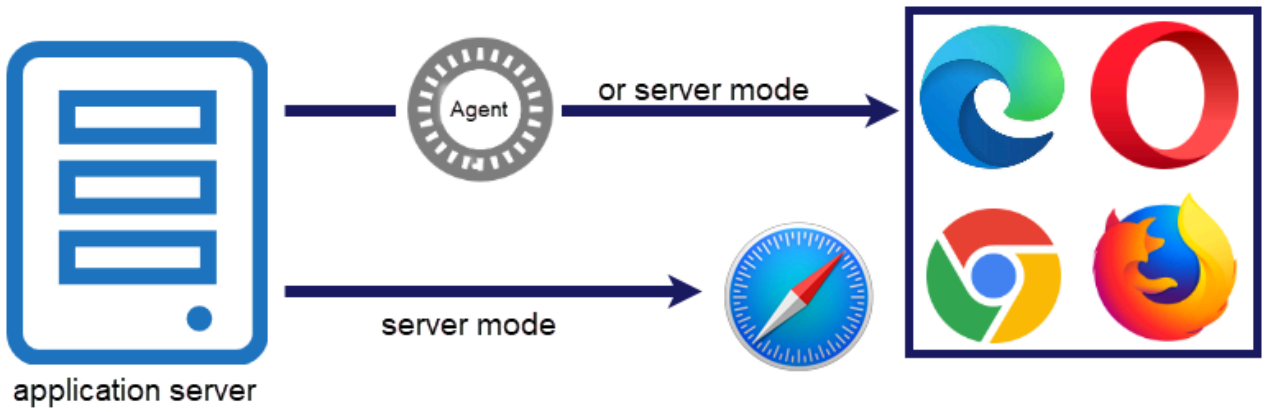
Add-ons

What are add-ons?

The passwords can also be used in the browser via browser add-on. It is possible to search for passwords via add-on. The user can search for passwords in the add-on, transfer them to the clipboard or enter them in the input mask of the website automatically. The automatic login may require applications.

In order to provide the data, the add-on needs a connection to the database. This can be set up in two ways, either via **SSO Agent** or directly in **server mode**.

Currently, add-ons are available for the following browsers: **Microsoft Internet Explorer**, **Microsoft Edge**, **Google Chrome**, **Mozilla Firefox** and **Safari**.



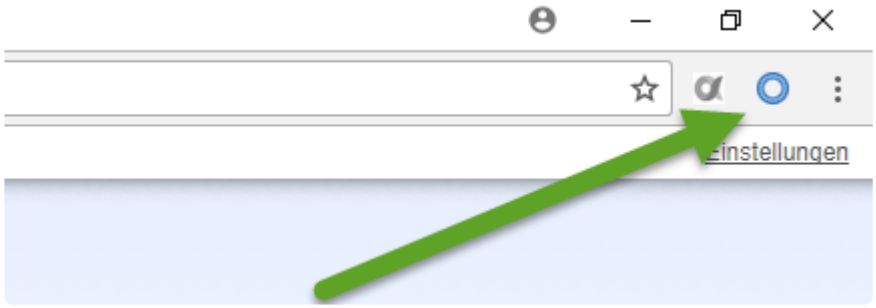
! As the technology of Internet Explorer is outdated and Microsoft Edge is rebuilt, we are unfortunately forced to discontinue support for the respective add-ons.
Both add-ons will no longer be developed from version 8.9 onwards. This also means that no more bugs will be fixed and no more support for them will take place. Therefore, the use of add-ons is at your own risk. As of version 8.11, both add-ons are no longer available.

Installation

Please find more information about the installation on: Installation Browser Add-ons

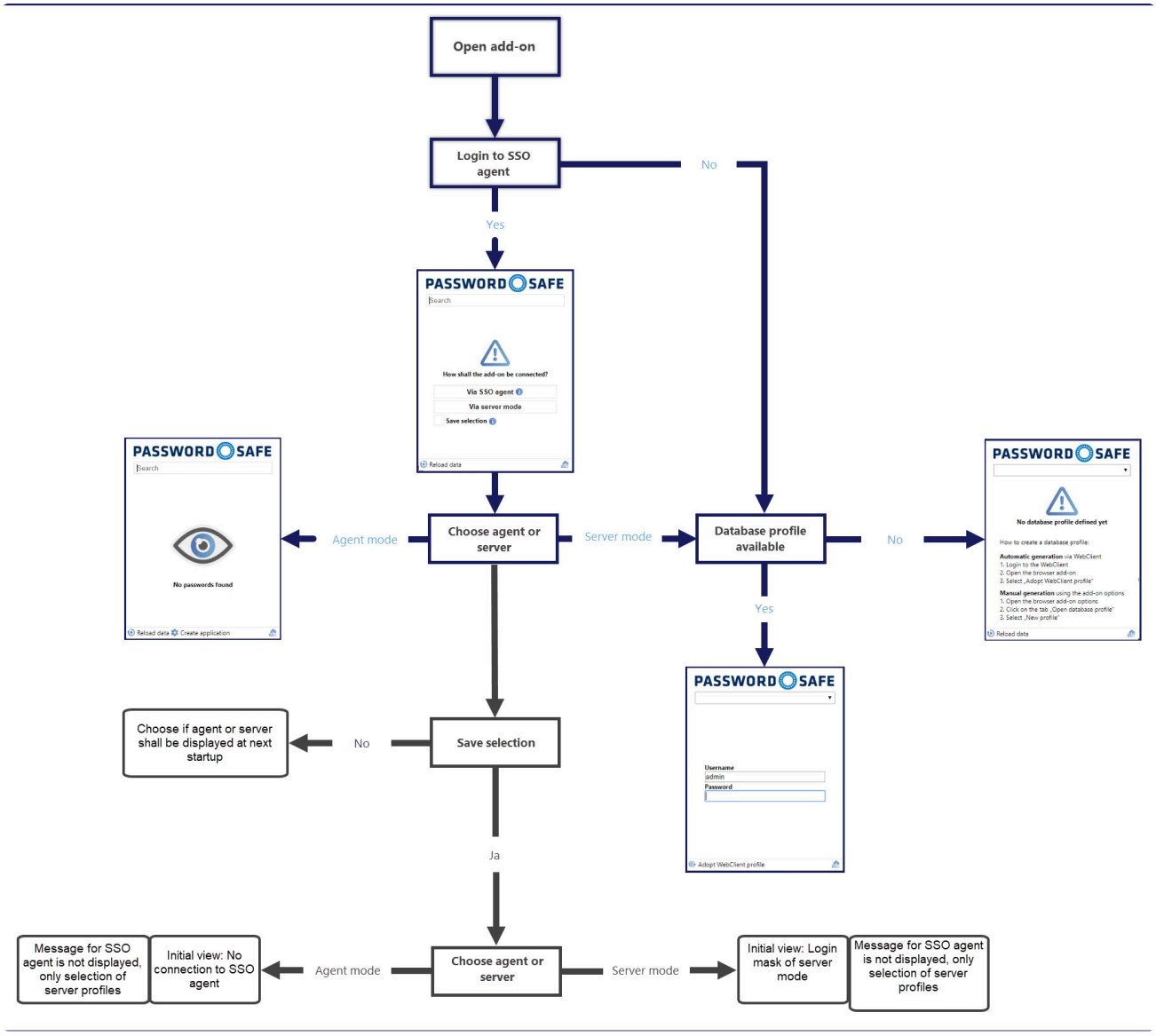
Connection via SSO agent or server mode

If the Installation of the add-on has 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:

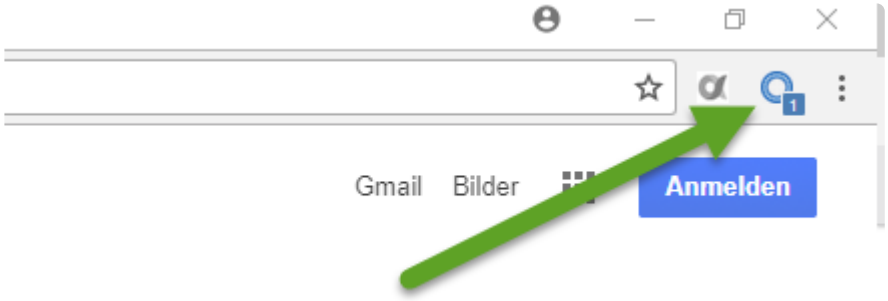


If the icon is displayed as shown, it means that although the add-on has been installed, a connection has not yet been established with the SSO agent. Only **after logging into the agent** (via the icon in the system tray) will you receive a Windows notification about the successful login. If a connection to the agent has been established, the **number of available records for the current website** will be directly displayed on the icon.

The following picture explains the exact procedure for connecting in detail:



After successful connection, the **number of data records available for the current Internet page** is displayed on the icon.

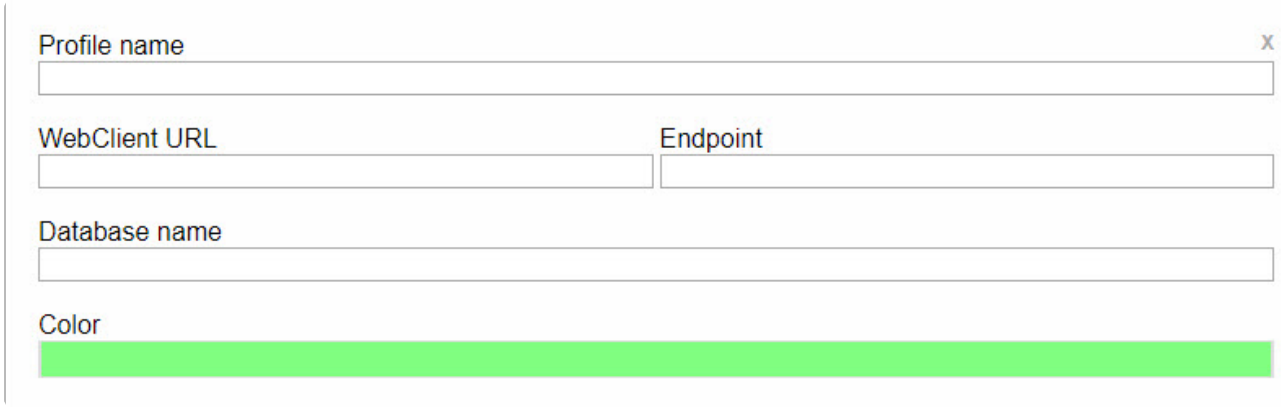


The subscript “0” means that the add-on has a connection to the database.

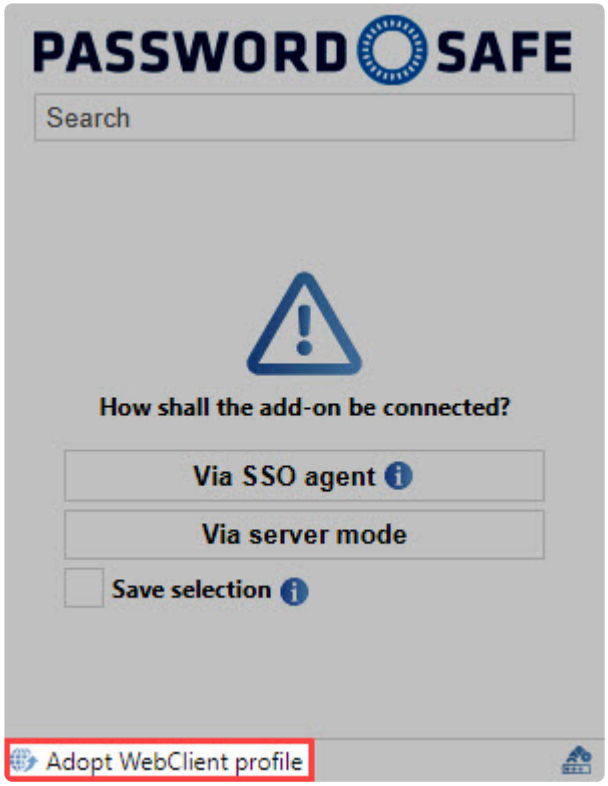
Database profiles

The server mode must know which database profile it is connected to. There are two ways of setting up a database profile:

- First, the database profile can be created manually. Therefore, he following information is required: IP address, WebClient URL and database name. Please note that **/api** is appended to the end of the IP address.



- It is also possible that the database profile is filled out automatically. For this, you need to log on to a database via WebClient. By clicking on the add-on in the WebClient, its profile can be taken over. Now all necessary information such as profile name, IP address, WebClient and database name are transferred.



The chapter WebClient describes how to transfer the database name and the user name into the URL of the WebClient.

The server mode benefits

The server mode offers the following advantages:

- No terminal service is required in terminal server operation.
- SSO is no longer required.

Please note that SSO applications only work via SSO agent. If you are in server mode and the SSO agent has not been started, SSO applications do not work!

Settings

All settings that relate to the add-on are made centrally on the client. The user settings system can be used to enter them 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: “

> It is important to note that the login mask for records with password masking will be ”sent automatically*, even if the setting **Browser add-ons: Automatically send login masks** has been deactivated.

Working with add-ons

> A record can only be used for entering data if it has a form field of type “URL”.

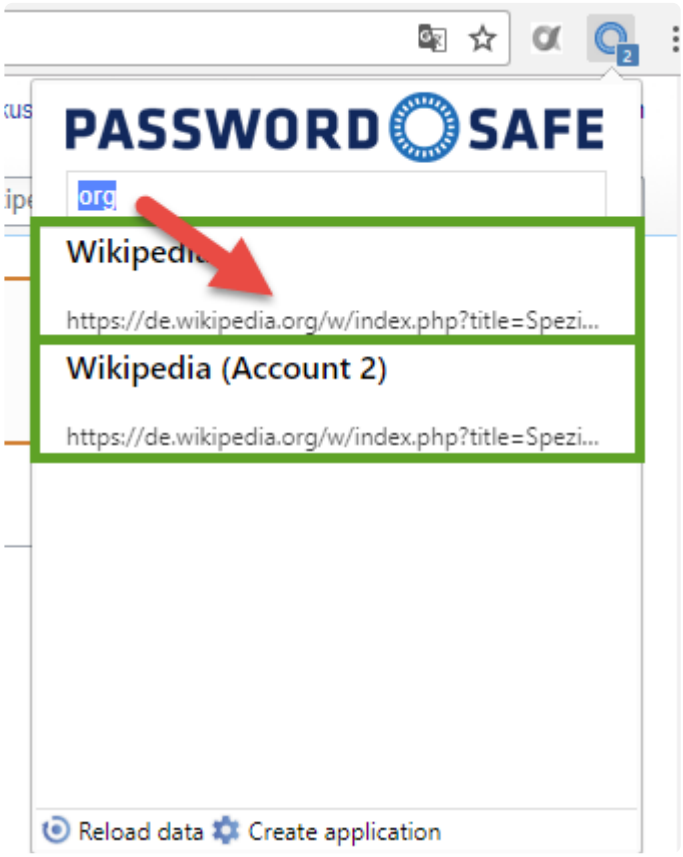
The subscript number mentioned in the previous section is only available with active logins and therefore already says a lot about the “Number of possible entries”. For example, if the number “2” is shown, you can directly select the account you want to log in with.



Previously, the prerequisite was that you had to navigate manually 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.

Search and navigation

It is currently assumed that the user has to navigate manually 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.



The screenshot shows that the URL and 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**”:#passworteinstellungen.

The process will be explained by 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 addon, i.e.

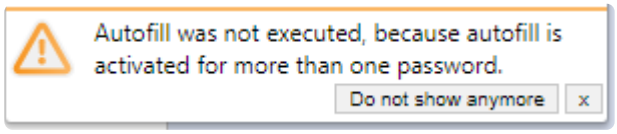
www.passwordsafe.de, **help.passwordsafe.de** and **license.passwordsafe.de**

The **Exact domain check** is activated for all three passwords:
On **www.passwordsafe.de**, no passwords for the subdomains are displayed in the addon. 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 addon.

Several passwords for one website

If a user opens a page and multiple passwords with the autofill function are possible for this website, no entries will be made unlike in older versions. Instead, the following message appears in a pop-up:

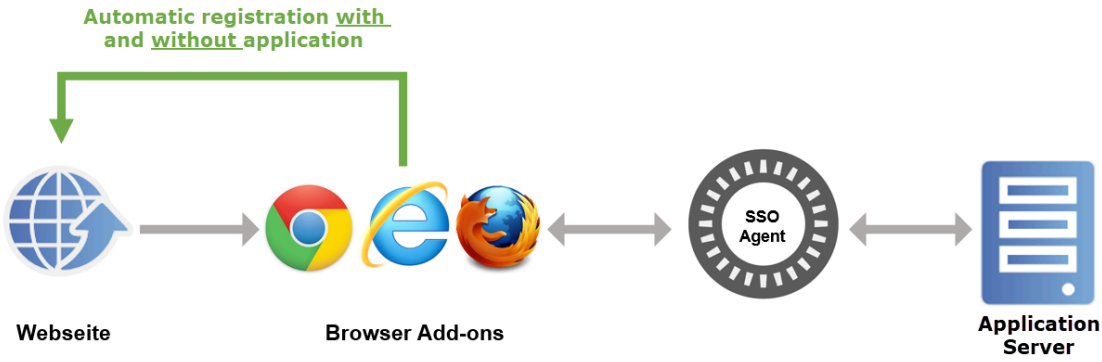


However, if the autofill function is only activated for one password but multiple passwords are possible, the password with the autofill function is entered.
If the user clicks on a record in the pop-up, this record is entered as normal (as was the case previously).

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**.

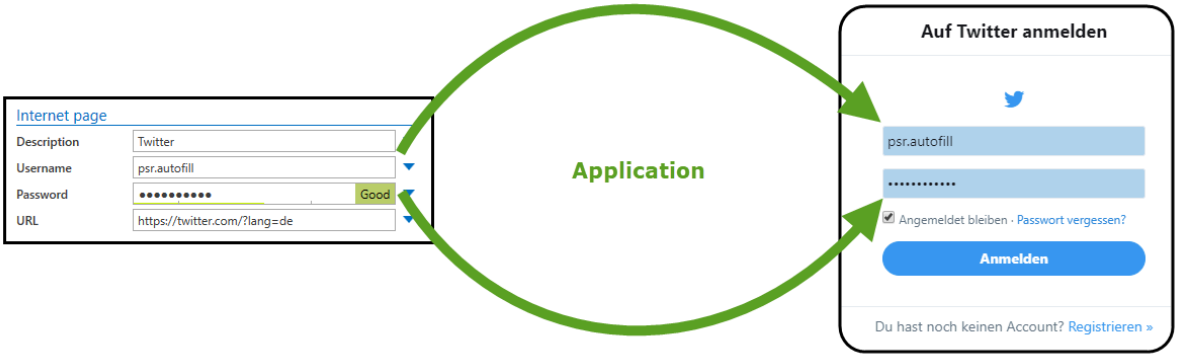
Data entry without application

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.

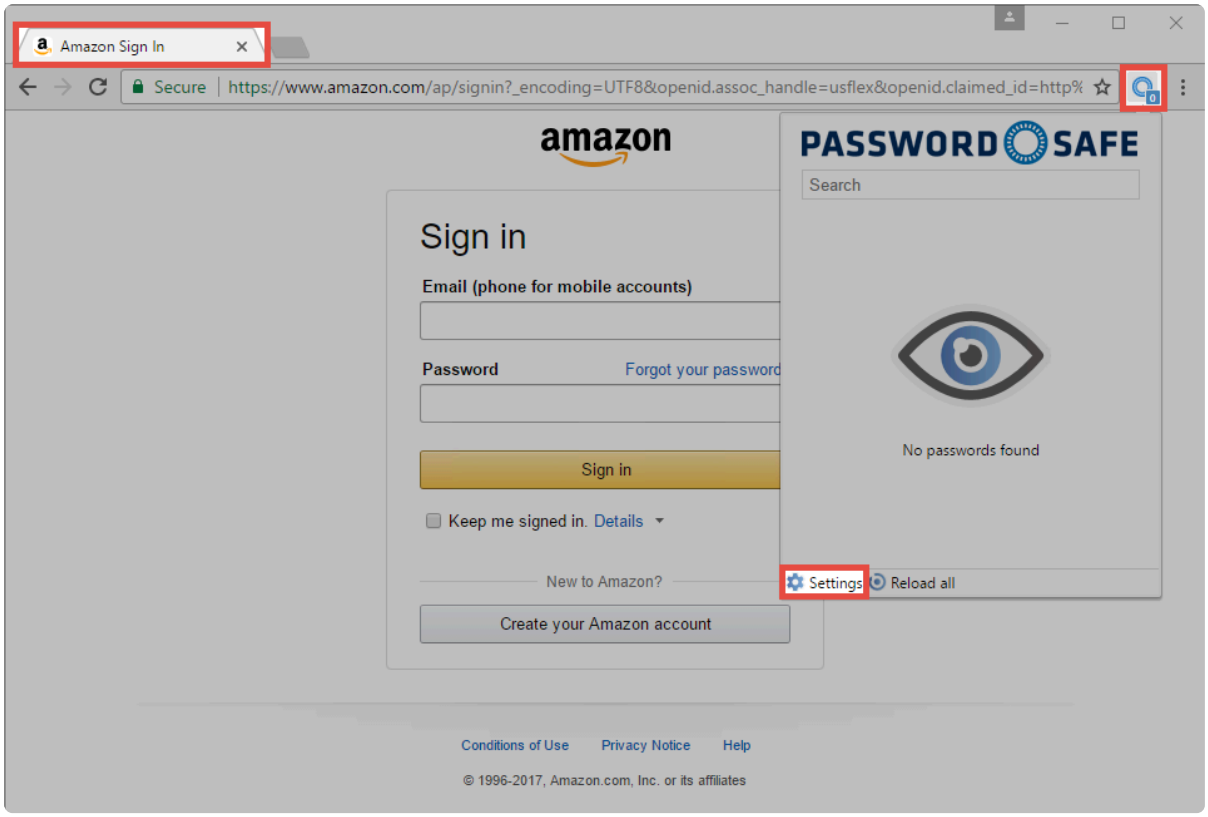


The URL is checked to see whether the record matches the web page. It is only necessary for the hostname including the domain suffix (“.de” or “.com”) to match.

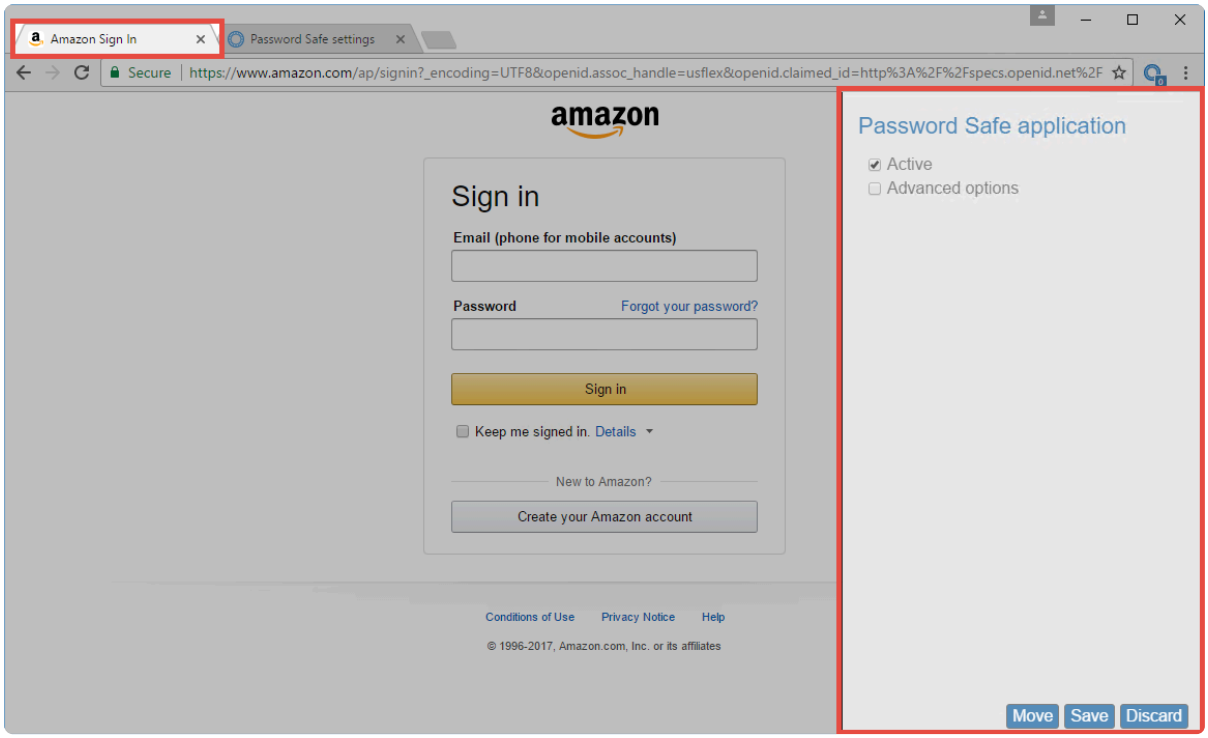
Creating applications

> ! 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.



A modal window now opens. The actual application is now created here.

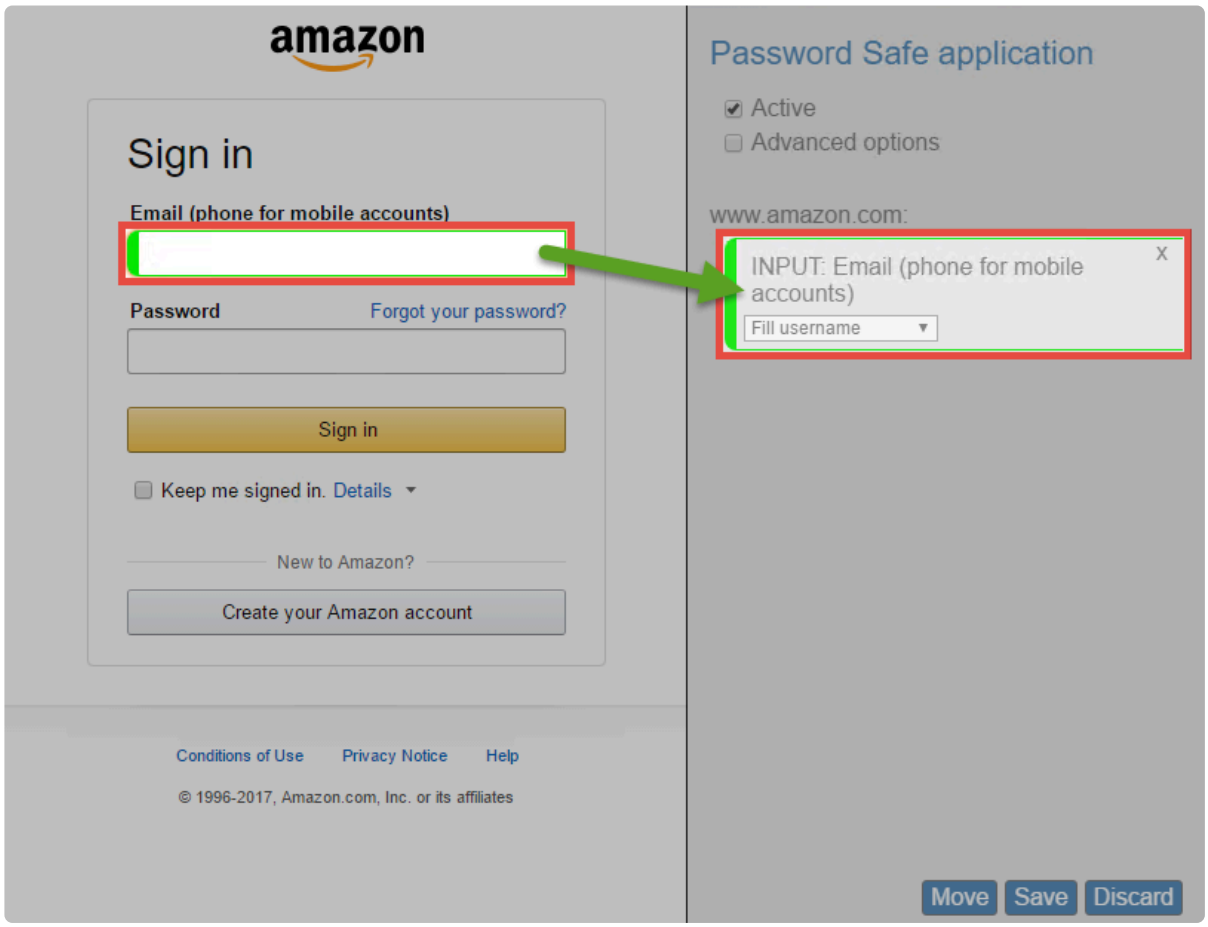


The following options are available:

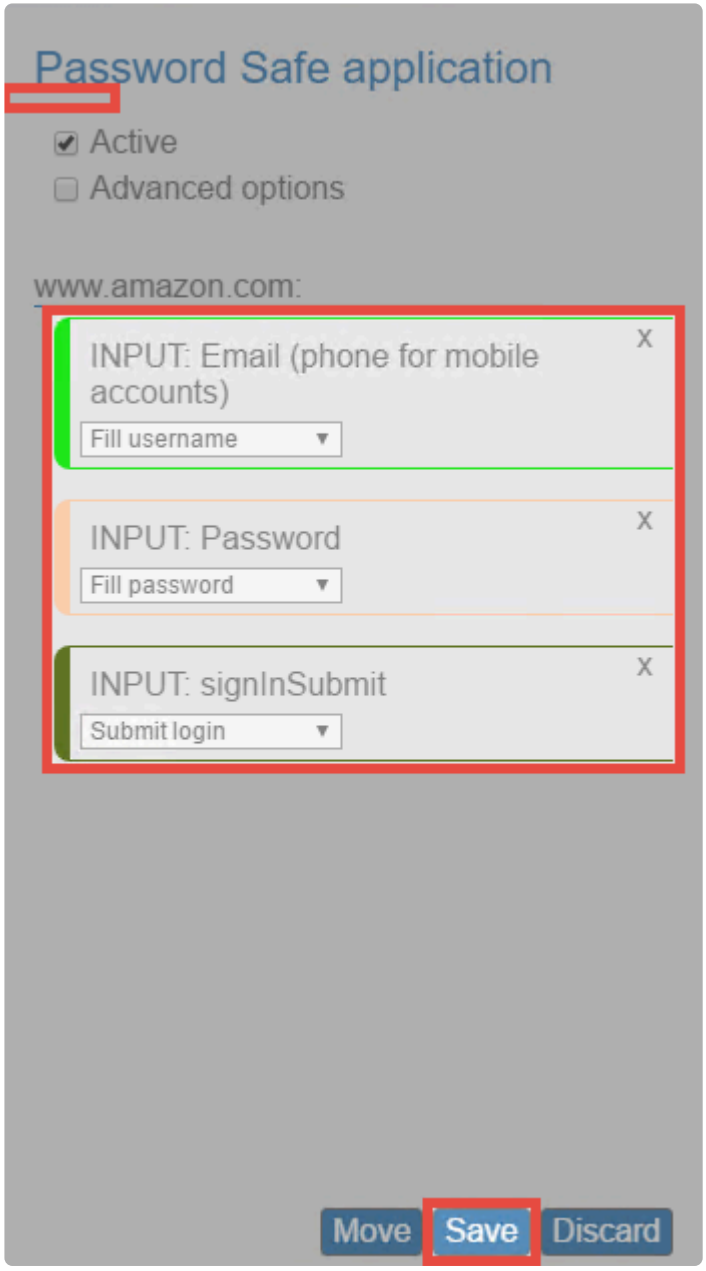
- The button *Capture fields” enables you to leave out the process for capturing fields
- **Advanced settings** allows you to define a delay separately for each field when entering the data. This is sensible when the process of entering the data would otherwise not run smoothly on sluggish websites.
- 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.



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.



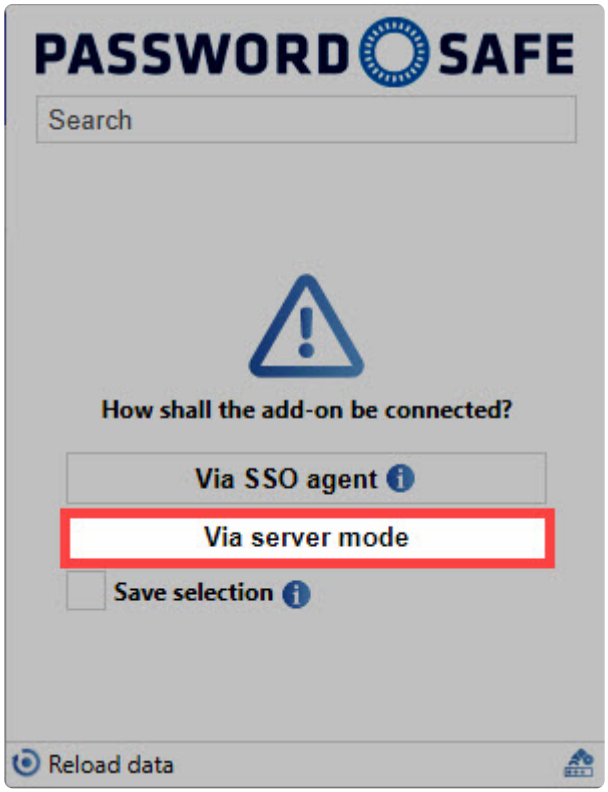
The saved application is now available for the user and can be used via the add-on.

How to save passwords

Hot wo save passwords via add-on

This chapter describes how to store passwords via add-on.

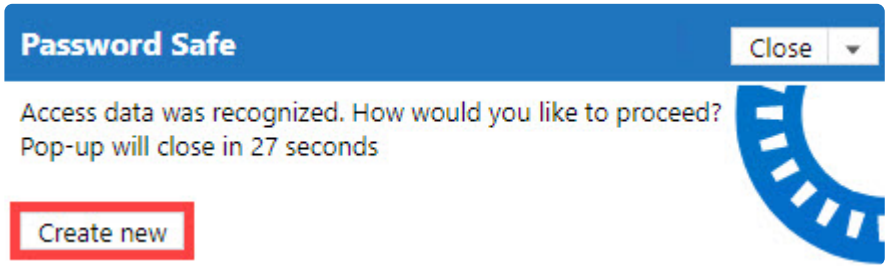
> ! You can only save passwords in server mode. Read here how to select the server mode.



How to save passwords

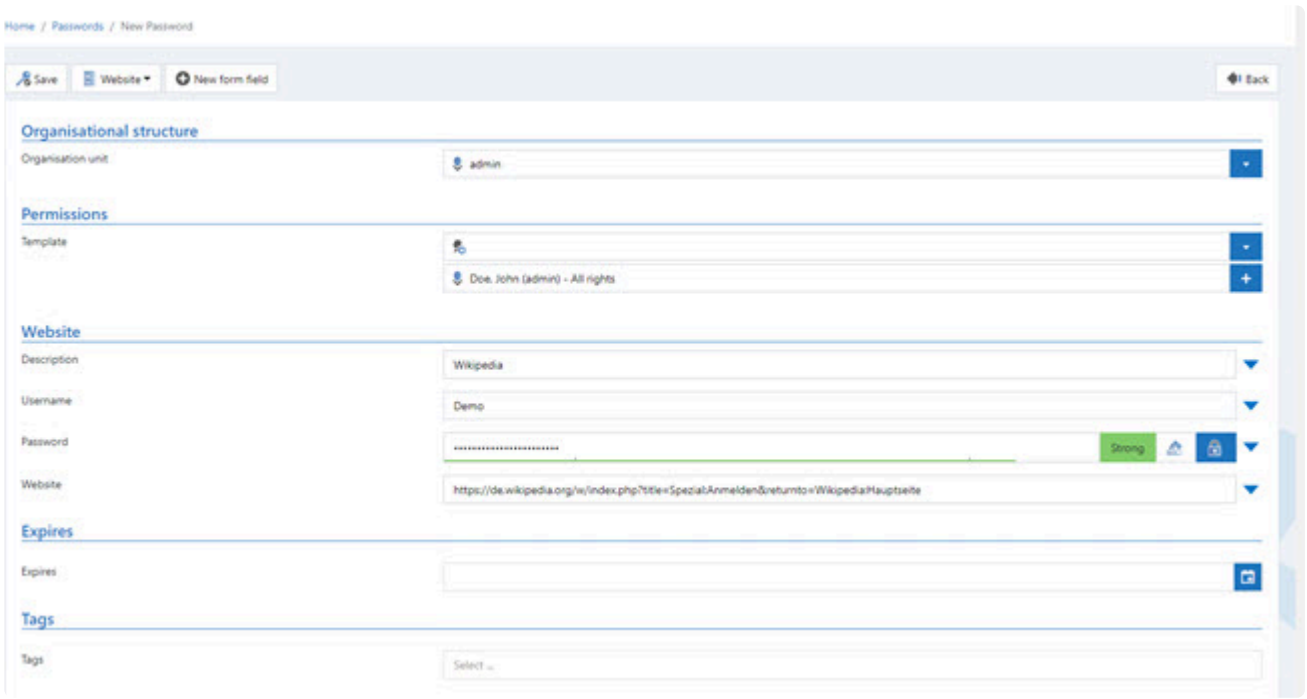
New access data

With the setup and login via server mode, the access data can now be added automatically. When visiting a website whose credentials have not yet been stored in Password Safe, you get automatically asked whether they should be created.



By confirming, you will be directly forwarded to the WebClient and registered there.
If there are less fields in the deposited or selected form than in the login mask, the missing fields are

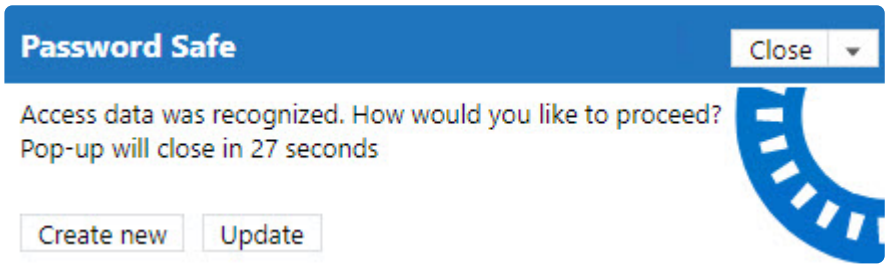
automatically created as web form fields by default.



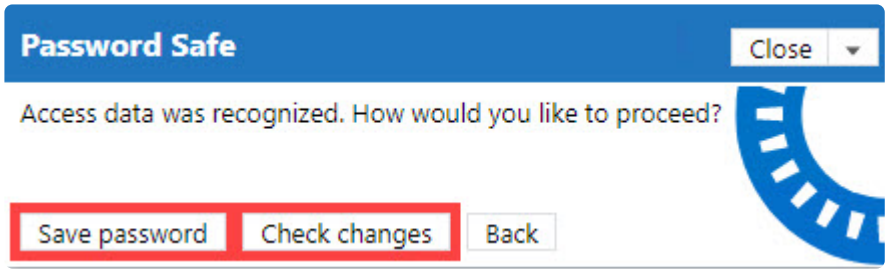
The right **"Can manage password form fields "** must be activated, so that web form fields can be created at all.

Known access data

If you log in to a login screen with changed access data, you can update this automatically. To do this, log on to the login screen of the changed page as usual. Thereupon a message appears that new access data has been recognized. Now you can optionally decide to create a new dataset or update an already known dataset.



- **Save password**: The password will be exchanged without opening the WebClient.
- **check changes**: The WebClient is opened and you are logged in. The previous password has been replaced by the new one. However, the storage must be carried out manually.



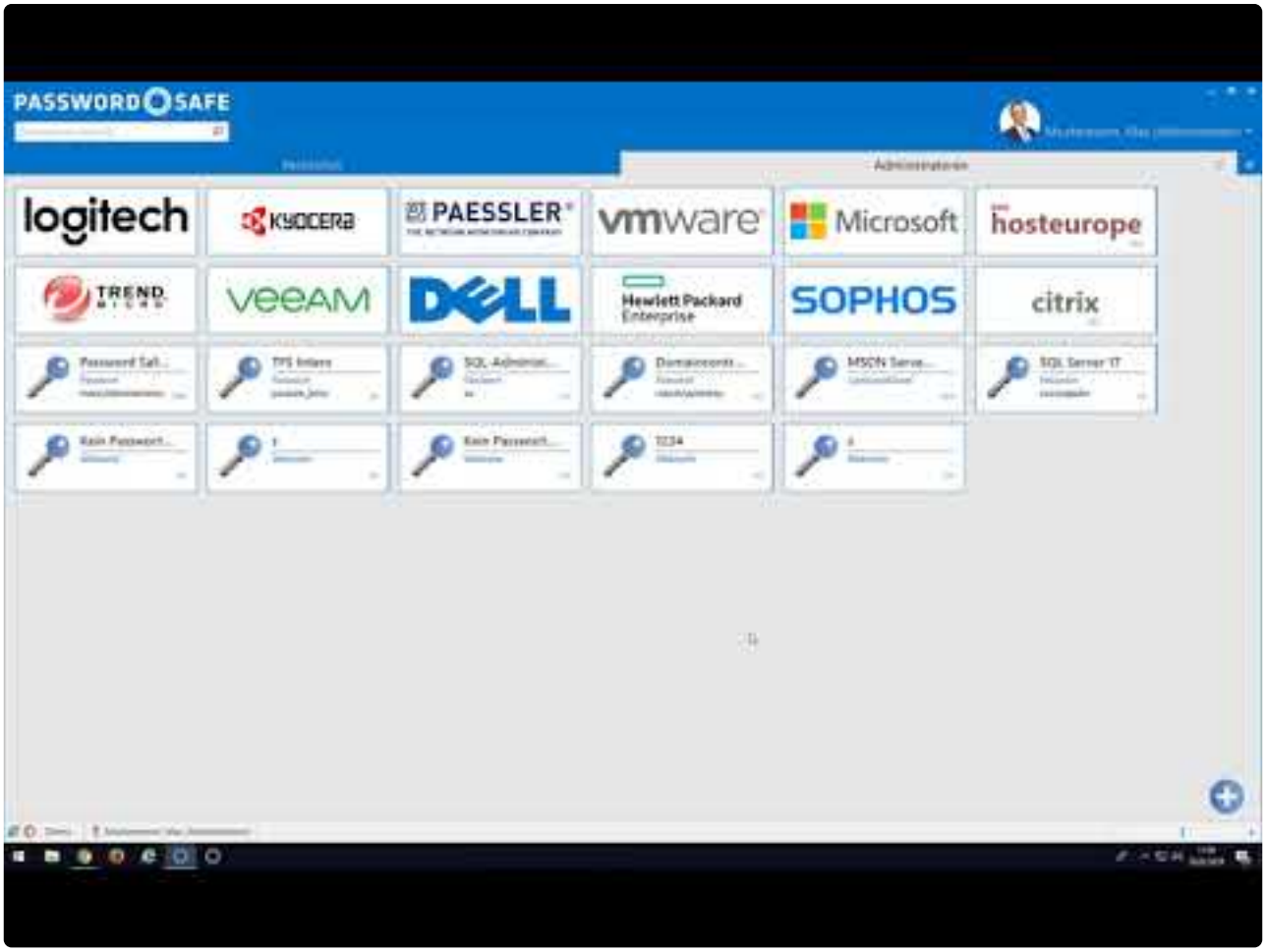
The following prerequisites apply so that a data record is considered to already exist:

- The URL must be identical.
- The user name must be identical.
- The entry must be made by the add-on and the change must only affect the password.

The LightClient

What is the LightClient about?

The LightClient is a lean tool for every end user. It guarantees quick and easy access to the daily needed passwords. Although the LightClient has a limited range of functions, it can be operated intuitively and without previous knowledge or training by any user. The LightClient is designed for up to 50 passwords. The LightClient introduces to professional password management. It is also the ideal tool for the daily handling of passwords.



https://www.youtube.com/embed/vHw5bouSZ9M?rel=0

Requirements & required rights

You don’t need any special permission to use the LightClient. However, the handling of the LightClients can be set via rights and settings. Read more in chapter **To do for Administration**.

Installation

The LightClient is installed directly with the FullClient, so you don’t need any special installation. For further information, visit the chapter **Installation Client**.

Functions

The function and operation of the LightClient are described here: Help LightClient

To do for Administration

Conditions for using the LightClient

The LightClient allows end users to easily manage their passwords in Password Safe without any training or prior knowledge. In order to ensure proper operation, the administration has to make a few preparations first. This will be further discussed in the following.

> ✻ To make the LightClient transition as easy and smooth as possible for the user, the administration can orient towards this **checklist**.

Relevant rights and settings

This section lists the **rights and settings** the user needs to work with the LightClient. The administration can adjust these rights and settings at its own discretion.

Rights

User right	Chapter	New
Can create individual passwords in the LightClient		✔
Can upload new password images.		✔
Can manage password images.		✔
Can close tab of own organizational unit in the LightClient		✔

Settings

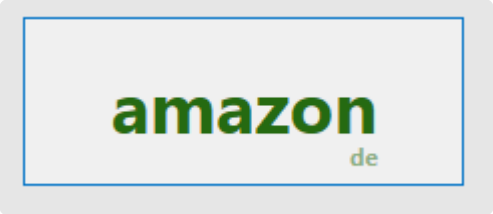
Settings	Chapter	New
Ask for Favicon download.		✔
Display of passwords in the LightClient		✔
Display of passwords in the FullClient		✔
Logo view with MouseOver in the LightClient		✔
Standard form (for the LightClient)		✔
Start LightClient at next login		✔
Include subordinate organizational units in the LightClient		✔

Password Management in the LightClient

There are several ways to provide/create passwords in the LightClient.

Predefined passwords

Predefined passwords have already been created on the FullClient. LightClient users must at least obtain **the right to read** a record in order to use the password.



Creating passwords via applications

In order to use applications on the LightClient, the administration must first create them on the FullClient. By clicking on the application, the end user can easily generate secure passwords. To be able to use the application, the user needs at least the authorization to **read**.

Further information on this topic can be found in the chapter Applications.



Creating passwords via applications without applications

Please consider the following **rights and settings** so that LightClient users can create new passwords.

User rights:

- **Can create individual passwords in the LightClient**

Setting:

Default form (for LightClient) Otherwise, no form can be assigned to the new password.

- **Add right** to the organizational unit of the user

LightClient Password Management

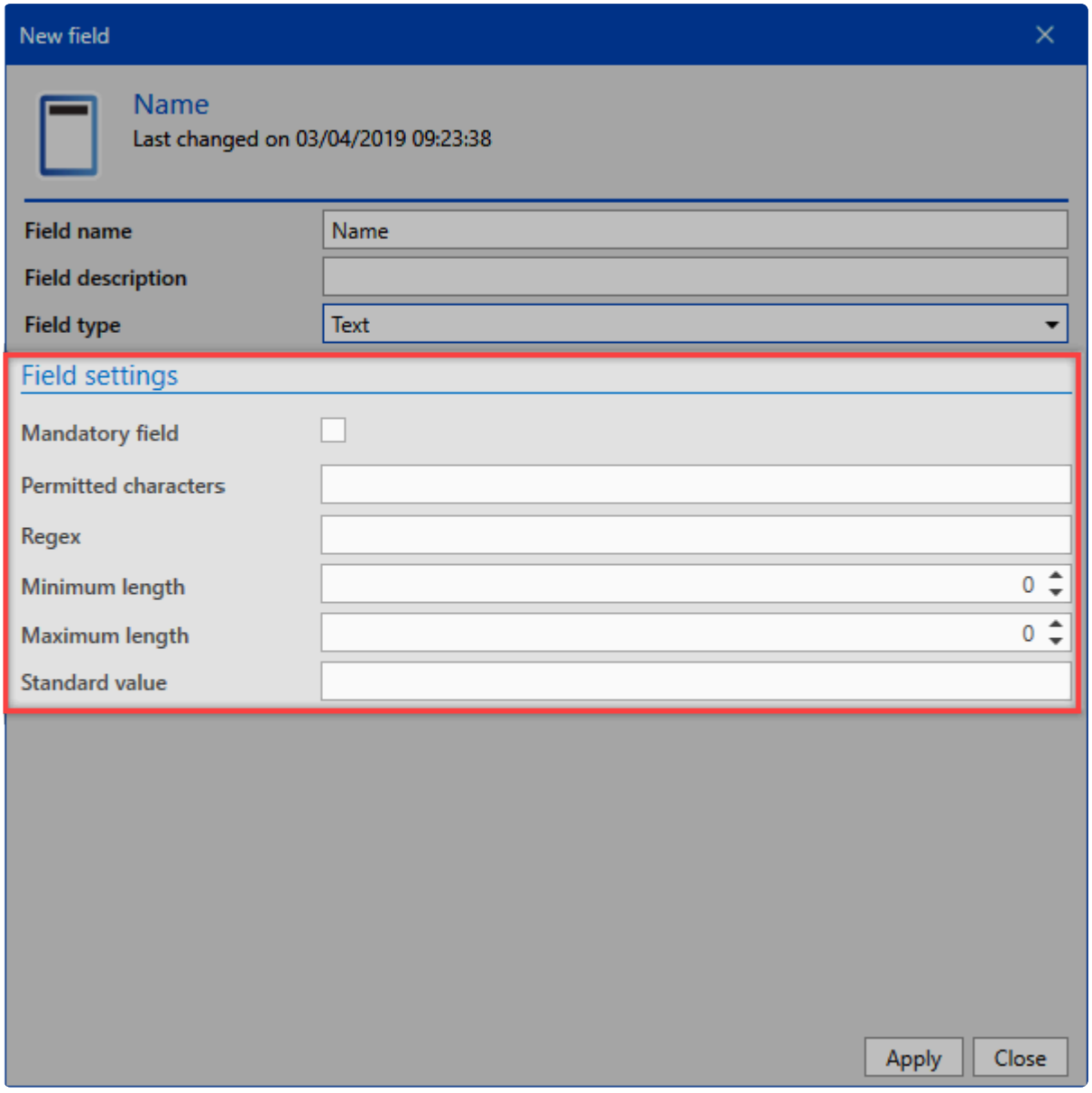
Errorcodes of the LightClient

Error codes for administration

If problems with the LightClient should appear, they are classified by error codes. These codes help the administration to stop problems even more quickly and solve them. There are 7 different types of error codes:

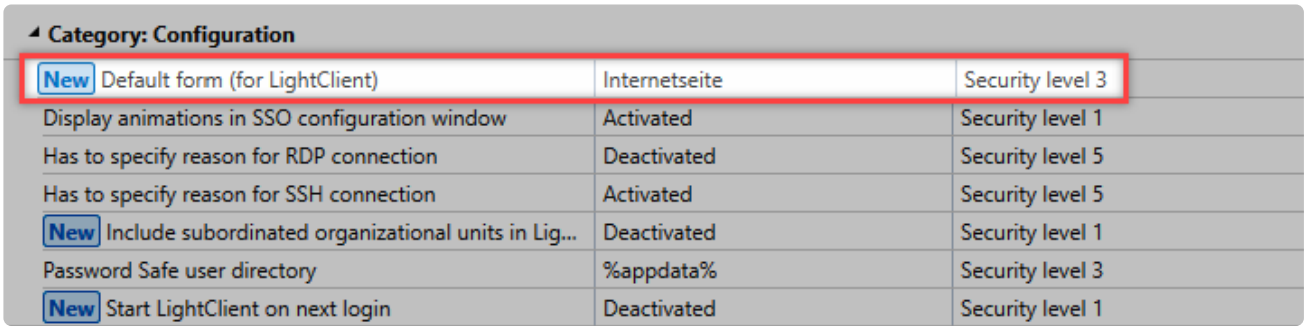
SavePasswordUnknown
An unexpected error has occurred. Further information can be found in the event display of the application server.

SavePasswordPlausibilityField
The plausibility has not been fulfilled when saving a password. The mandatory fields of the deposited form should be checked.



NoDefaultForm

No standard form was selected. The form can be stored in the settings under **Standard form (for the LightClient})**.



Category: Configuration		
New Default form (for LightClient)	Internetseite	Security level 3
Display animations in SSO configuration window	Activated	Security level 1
Has to specify reason for RDP connection	Deactivated	Security level 5
Has to specify reason for SSH connection	Activated	Security level 5
New Include subordinated organizational units in Lig...	Deactivated	Security level 1
Password Safe user directory	%appdata%	Security level 3
New Start LightClient on next login	Deactivated	Security level 1

DefaultFormNotFound
The rights of the form must be checked. The user must have at least the permission to **read** the form.

DefaultFormMissingFields
The form has been set correctly. However, the field types in the form must be checked. At least required: Text, user name, password, URL.

DefaultFormImpossiblePlausibility
When creating a password for an application, there is a field which is not displayed. Therefore, the plausibility in fields should be checked.

NoValidOrganisation
Is only relevant for the web view of the LightClient. It is activated if you want to create a password using the add-on and the user does not have an OU in which to create it.

Checklist of the LightClient

Checklist for setting the LightClient

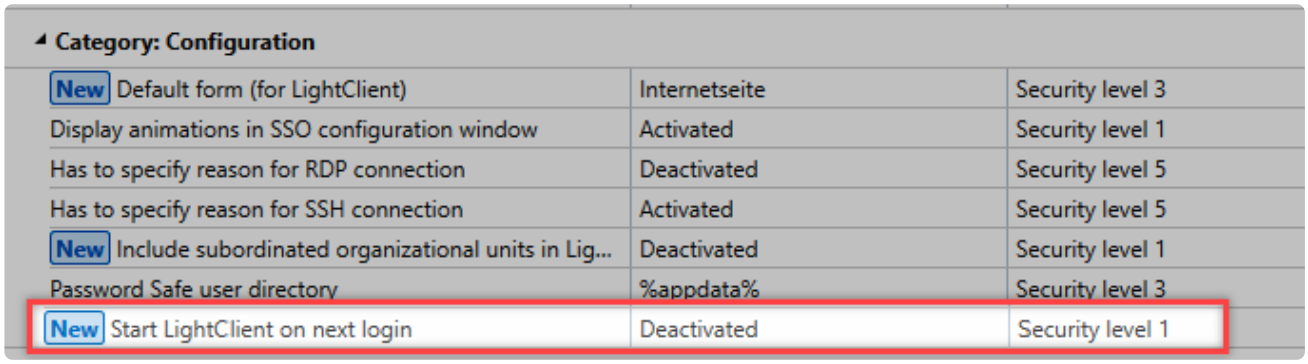
This checklist helps the administrator in setting the LightClient. To work smoothly with the LightClient, the following points must be observed:

1. Select form
The stored form must cover all required field types. At least required: **Text, username, password, URL**

2. Set display of the LightClient or FullClient
The setting **Display passwords in LightClient & display passwords in FullClient** allows you to configure the display of both clients. The passwords can be displayed with an icon, logo or in text form.

3. Are users in the right organizational unit?
Check if the user is in the correct organizational unit. The **add** right to the organizational unit is also required so that users can create passwords in the LightClient.

4. Define user as LightClient user
You can either define the user directly as LightClient user. This works by changing the user type accordingly.
Alternatively, you can activate the setting **Start LightClient at next login**. This will prompt the user to log in to the LightClient.

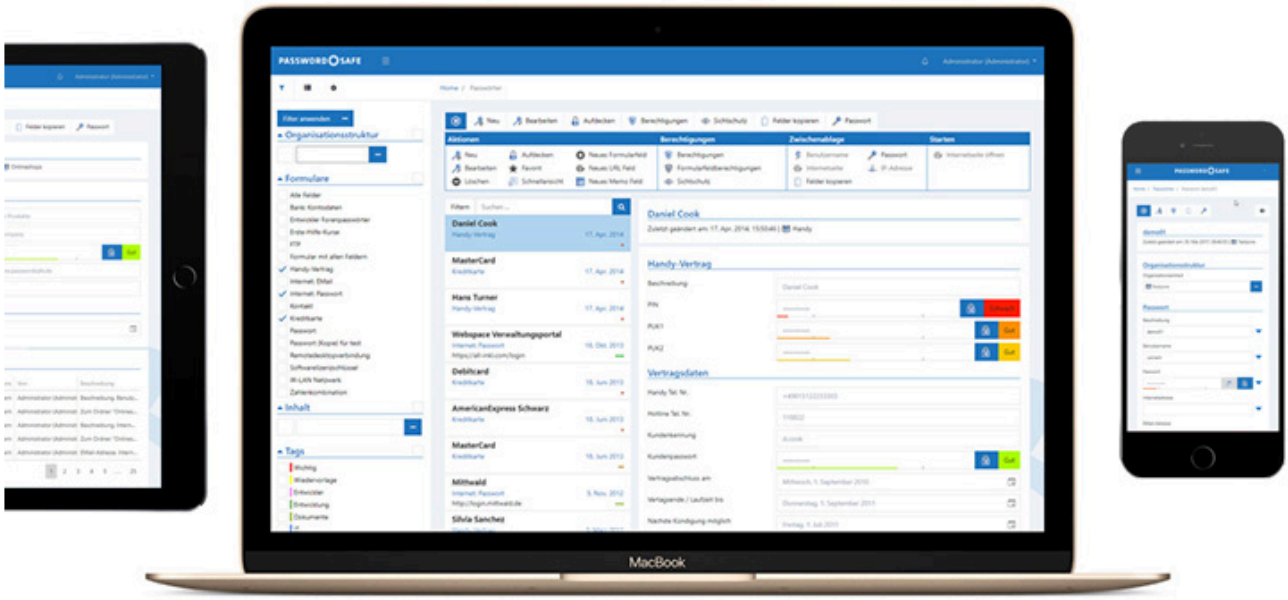


5. Add default applications (optional)
It is advised to create the applications, which shall be stored as passwords, beforehand.

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 system
- Organisational structure module
- Roles module
- Forms module
- Notifications
- Logbook
- Applications
- Documents

Tag system

The **tag system** currently offers the following functions:

- Add
- Delete
- Edit

Password module

The **Password Module** currently provides the following functions:

- Create
- Delete
- Edit
- Uncover password
- Quick search
- Add/edit form fields
- Tagged
- Duplicate
- Move
- Quick view (passwords automatically reveal)
- Favorites
- Filter
- Structural filter
- Authorization/edit rights
- Form field authorizations
- Change password undercover
- Password generator with guidelines
- Copy to clipboard
- Open Internet page
- View logbook
- Display seal/visibility protection
- German/English
- Change user password, if “Change password at next login” is active
- Show notifications
- Keyboard navigation
    - ALT+Q: Quick search
    - ALT+N: New record
    - ALT+S: Save in Edit/New View
    - ALT+DEL: Delete selected record
    - Arrow up/down in list: Change selection
    - Right/left arrow in list: Page forward/backward
    - Enter: Open selected record
- Privacy screen
- Seal
- Print
- Create external link
- History
- Change form
- Export
- WebViewer Export

The WebClient module **Password** module is based on the module of the same name that is located in the client. Both modules differ in scope and design, but are nevertheless almost identical in terms of operation.

Organisational structure module

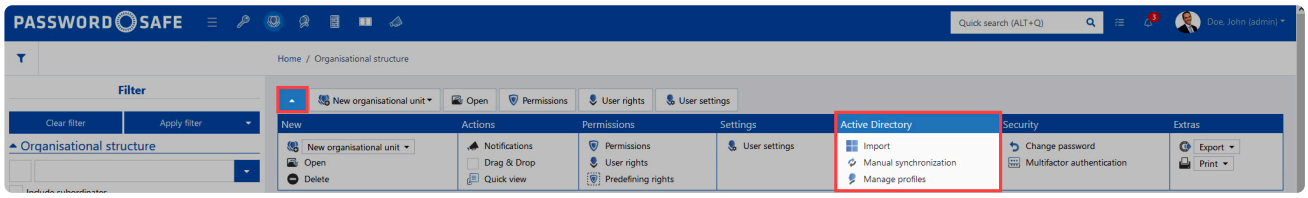
The following functions are currently available in the **organisational structure module**:

- Adding/editing/deleting/authorizing users / organisational structures
- Notifications
- Drag & Drop
- Filter
- Quick view
- User settings
- User rights
- Changing passwords
- Print

> The WebClient module **organisational structure** is based on the client module of the same name. Both modules have a different scope and design but are almost identical to use.

AD connection in the WebClient

The Active Directory connection in the WebClient works similiar to the Client. Here you can find further information to this topic.

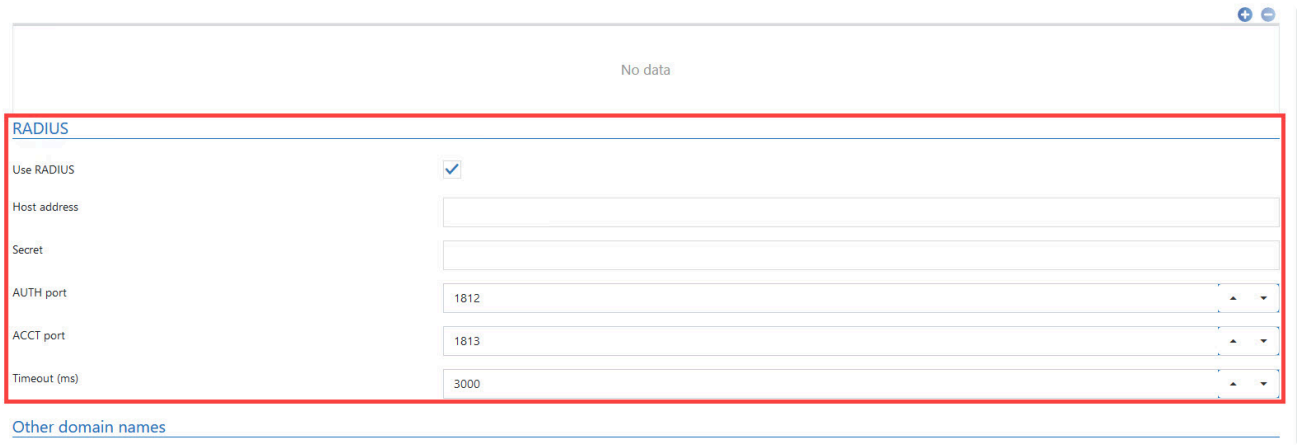


The WebClient offers the following functions:

- Import
- Manual synchronisation
- Manage profiles

Radius

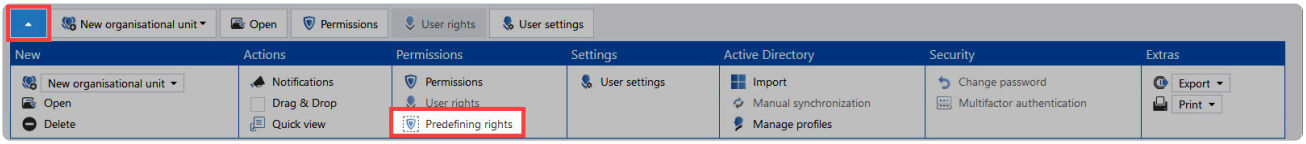
You can reach the Radius server, if the import is in the Masterkey mode. The Radius server will be provided in the Active Directory profile and will therefore deliver the possible authentication methods in future. You will find further informations in the **Radius Server** chapter.



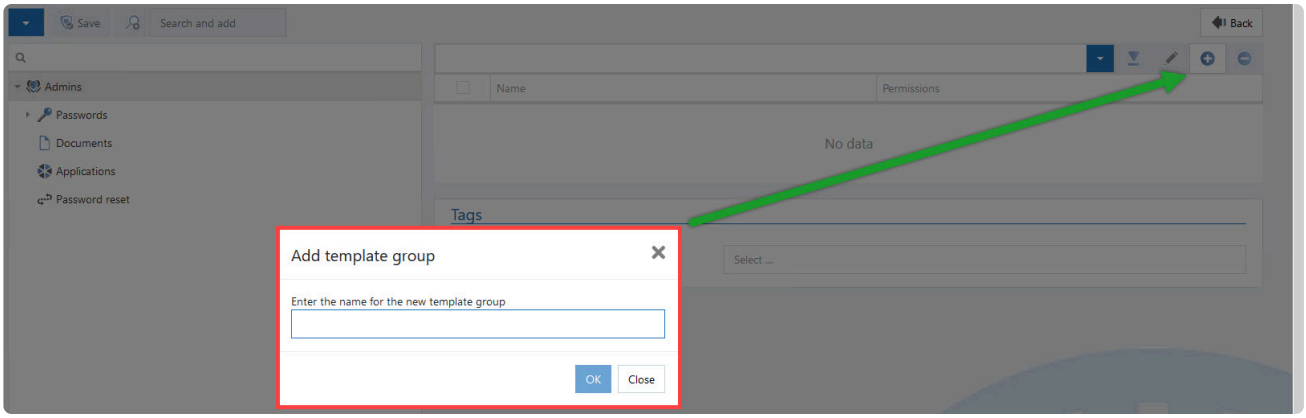
Predefining rights

To **predefine rights** in the WebClient, the procedure is the same as in the Client. Read more …

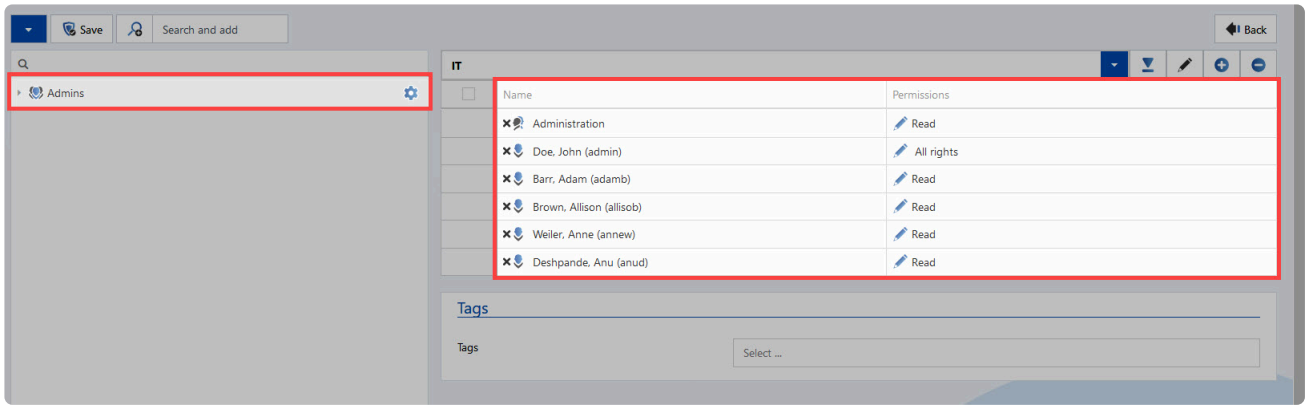
Go to the module organisational structure to choose the organisation unit for which the rights shall be predefined. Then choose **Predefine rights** in the menu bar.



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.

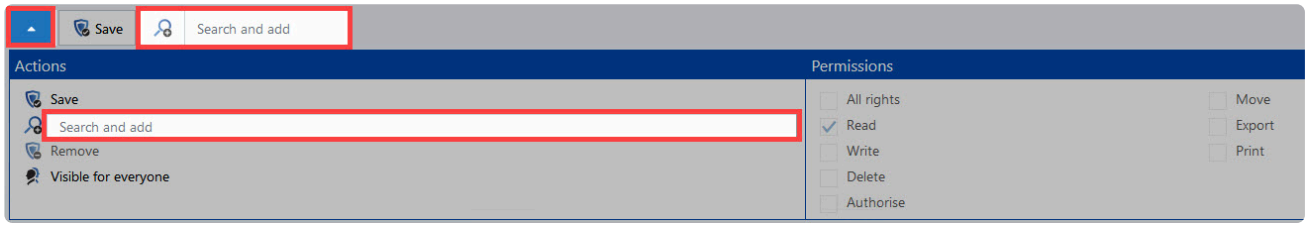


Now you can add the appropriate roles and users.



You can add users and roles in different ways:

- Add the appropriate roles and users at the toolbar under **Search and add**.
- Click on the loupe to see all the users and roles.



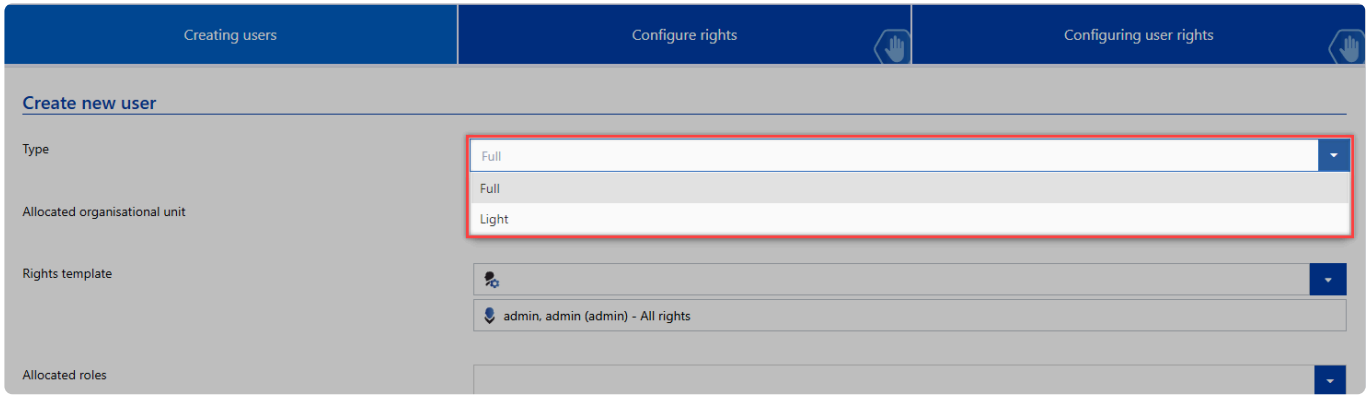
User management

How are the users managed in the WebClient?

The user management strongly depends on whether the Active Directory has been connected or not. In Master Key mode, the Active Directory remains the leading system. In all other modes, the user administration is carried out via the organizational structure module.

Creating local users

When creating new users, you must pay attention to whether it is a **Light user** or a **Full user**.



Roles module

The following functions are currently available in the **roles module**:

- Add
- Delete
- Notifications
- Favourites
- Quick view
- Permissions
- User rights
- Print

The WebClient module **roles** is based on the client module of the same name. Both modules have a different scope and design but are almost identical to use.

Forms module

The following functions are currently available in the **forms module**:

- Add
- Open
- Delete
- Notifications
- Duplicate
- Favourite
- Quick view
- Permissions
- Print
- Export

The WebClient module **forms** is based on the client module of the same name. Both modules have a different scope and design but are almost identical to use.

Notifications

The **permission module** exists of the following features:

- Filter function
- Seal function
- Mark message as read/unread
- Quick view (use button and space bar)
- Mail forwarding

The WebClient module **permissions** is based on the same called client module notifications. Both modules differ in range and design. However, the handling is almost the same.

Application

The following functions are currently available in the **Application module**:

Web & SAML applications:

- Create
- Manage
- Delete

> A detailed explanation of how to configure SAML can be found in the chapter “Configuration of SAML”

General functions:

- Notifications
- Duplicate
- Move
- Favourite
- Quick view
- Connect password

> The WebClient module **Applications** is based on the client module of the same name “Applications”. Both modules differ in scope and design, but the operation is almost identical.

Logbook

The **logbook module** exists of the following features:

- Filter function
- Quick view

> The WebClient module **logbook** is based on the same called client module logbook. Both modules differ in range and design. However, the handling is almost the same.

Differences to the logbook on the Client:

The following options are not available yet in the **WebClient**. If needed, you can use them on the Client.

- Documents
- Multifactor authentication
- Report configuration
- Applications
- Password Reset
- Password rules
- Sytem Task

Documents

The following functions are currently available in the **Document module**:

- New
  New document can be added in the following ways:
  - Right click -> search
  - Search via the navigation bar
  - By Drag & Drop (by dragging the document into the window)
- Open properties
- Update document
- Notifications
- Move
- Favourite
- Quick view
- Export
- Authorizations
- Create external link
- Print
- History

The WebClient module **Documents** is based on the client module of the same name “Documents”. Both modules differ in scope and design, but the operation is almost identical.

Operation

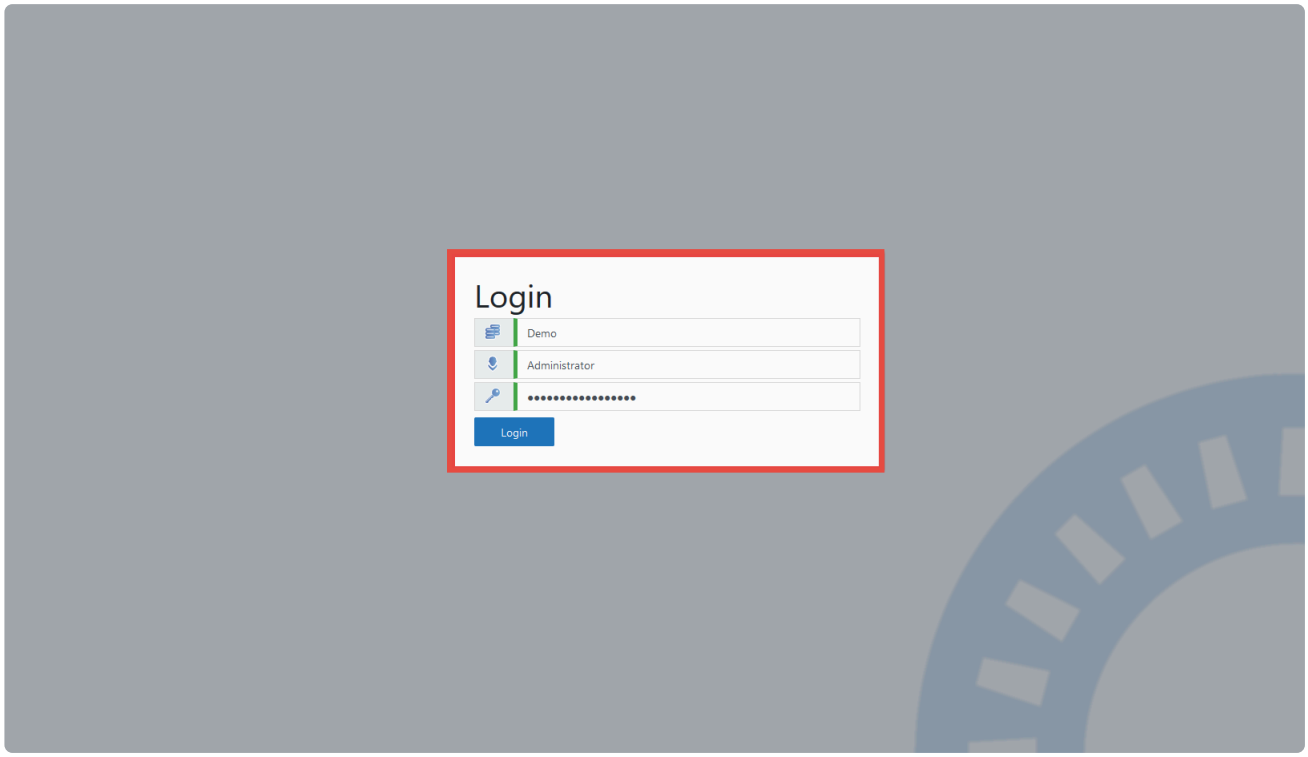
Operation of the WebClient has been based as far as possible on the operation of the Password Safe client. Nevertheless, there are some differences that need to be noted and they are described here.

There is also a LightClient in the WebClient. Everything worth knowing can be found at the following link: web view LightClient

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



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 **&**.

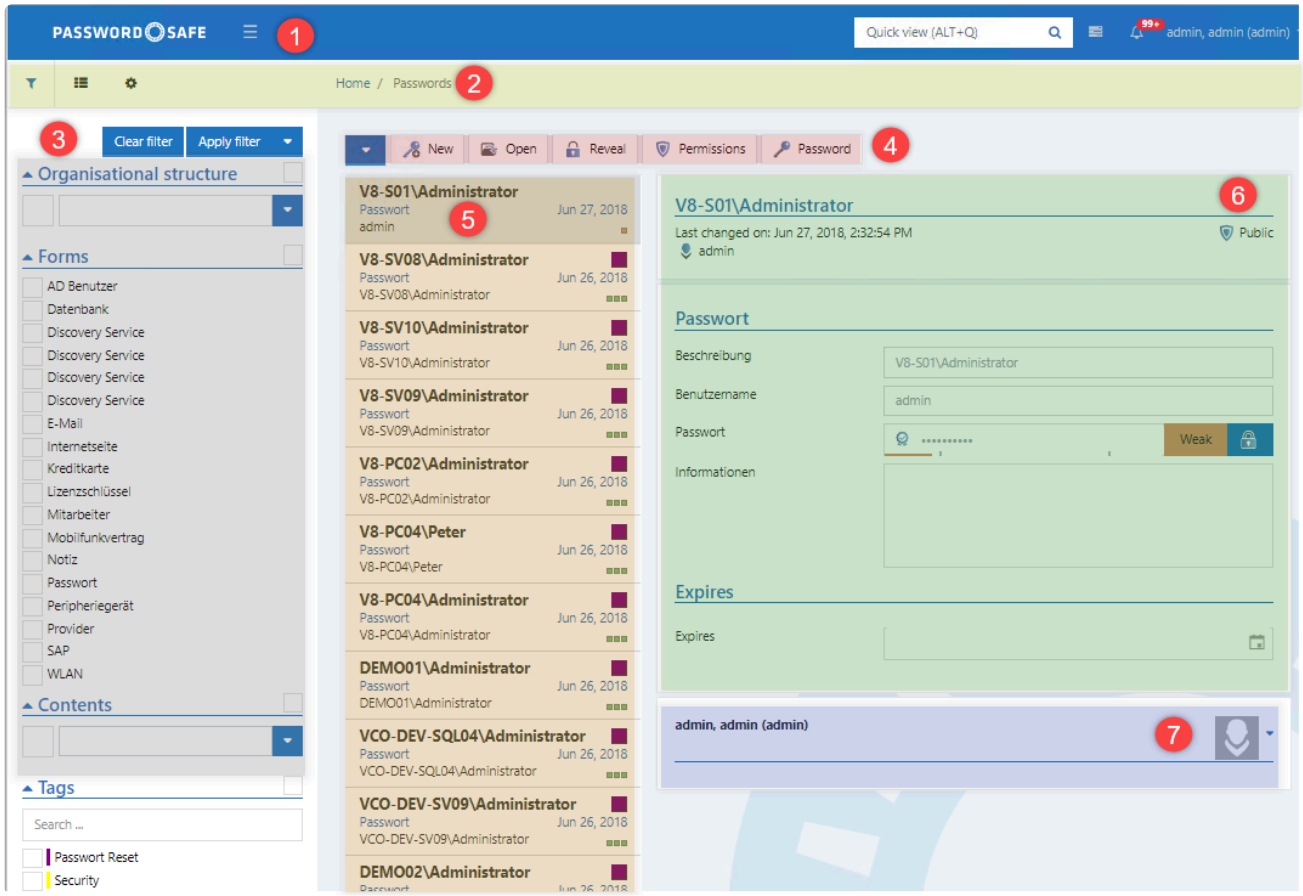
Example

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.

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

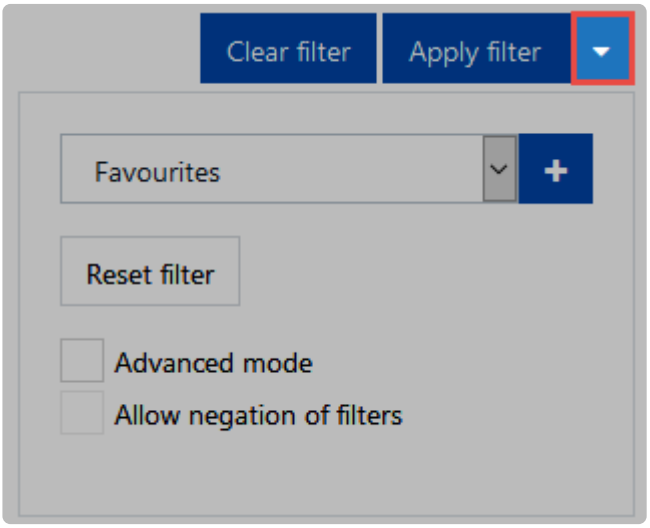
The filter on the WebClient is based on the “filter on the client:#filter. Therefore, only those characteristics specific to the WebClient will be described here.

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.

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. Modules

As is also the case on the client, modules like passwords, organisational structures, roles and forms can be managed here.

4. 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.

5. Quick search

Upcoming tasks like export, import, print and so on are displayed here.

6. Notifications

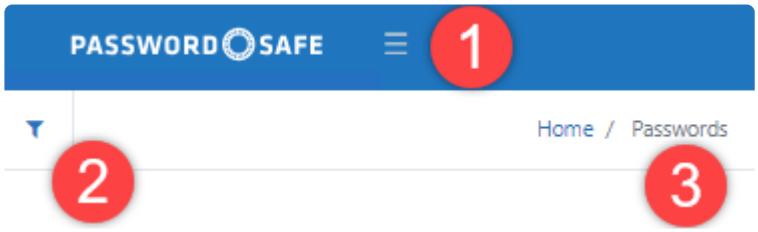
here you will be informed about incoming notifications. The notification can also be called up by clicking on it.

7. 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.

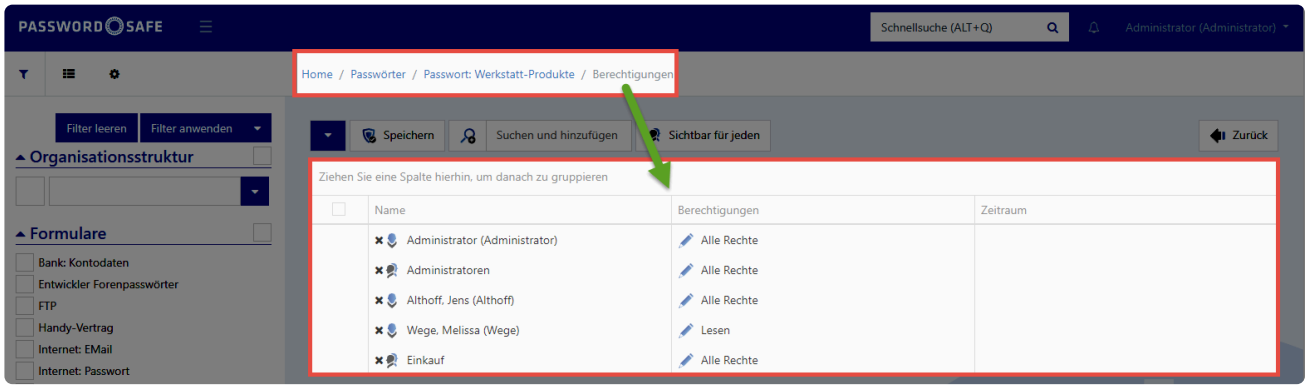
2. Structure

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



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.

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

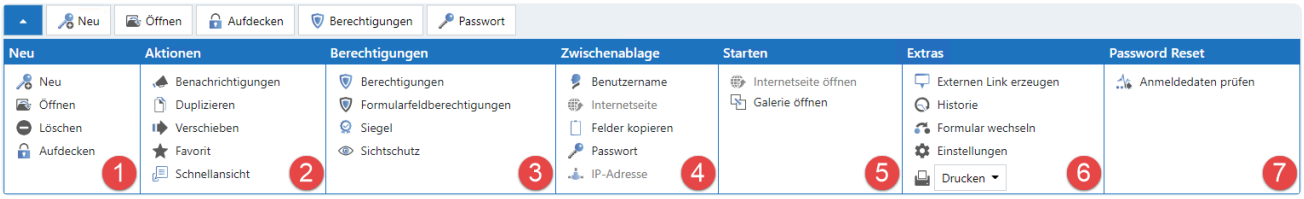
This button is used to configure the rights for the record.

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

A website can be called up 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.

6. Extras

All of the additional functions can be found here. These functions correspond to the main client and will be described in the next section:
Password extras

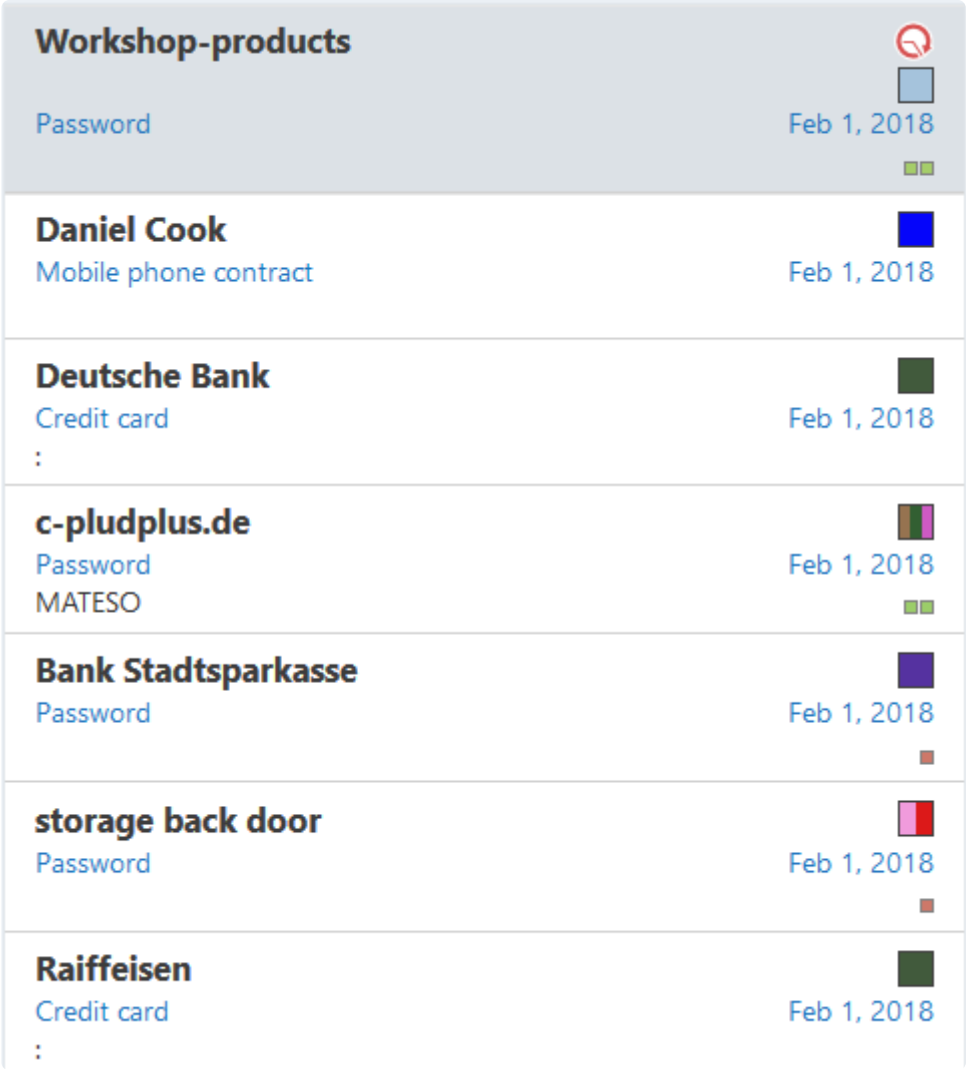
7. Password Reset

The functions of the Password Reset can be found here.

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.



Special features

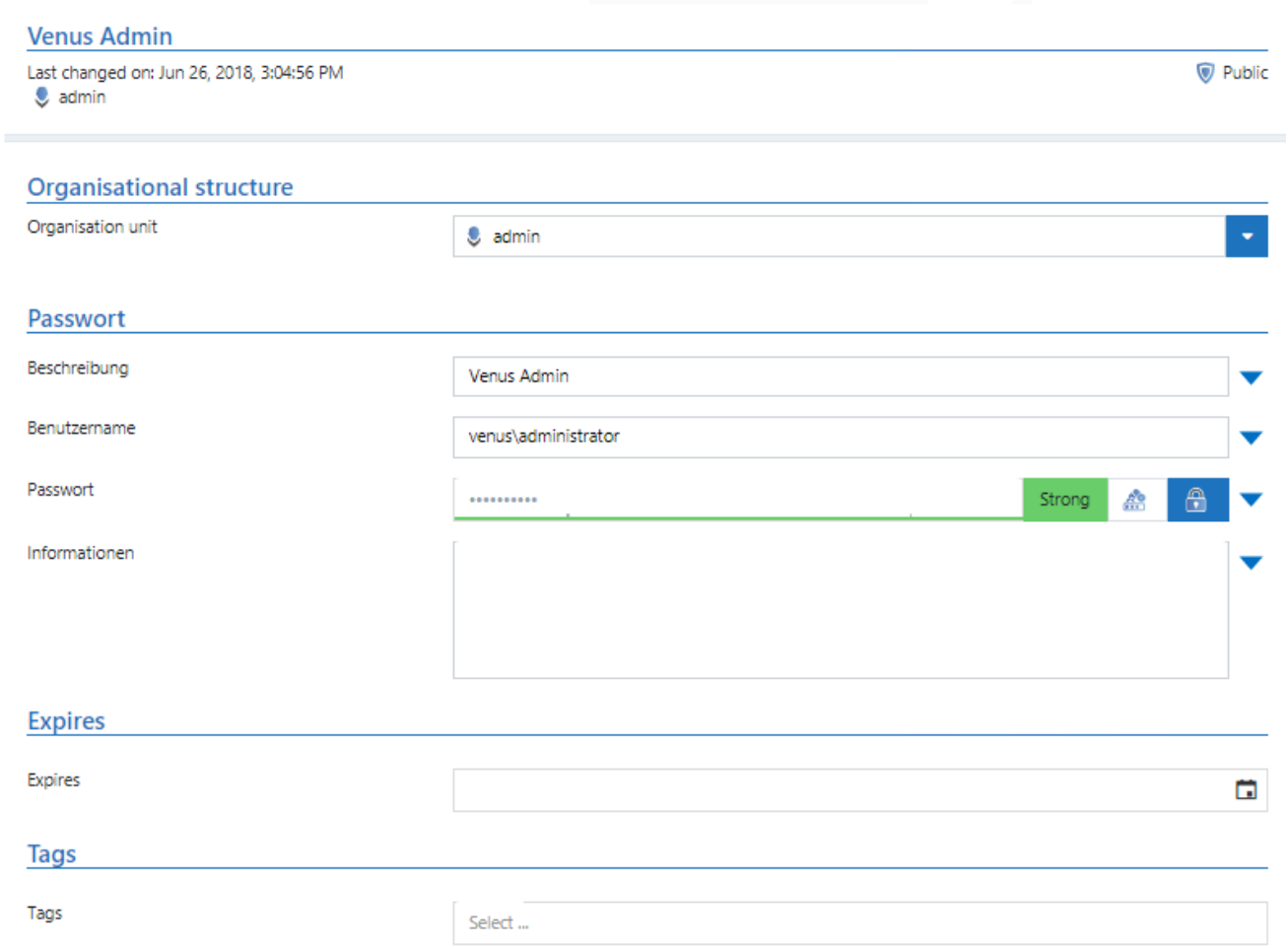
The list view differs from that on the client in the following areas:

- 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.

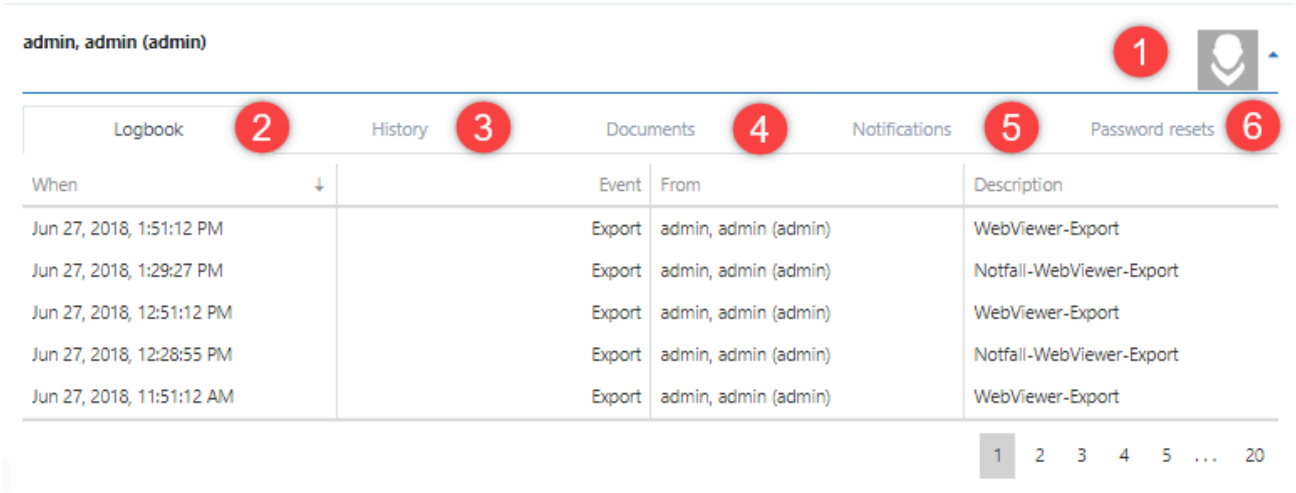


Various information is displayed on the header – as is the case with the client. For example, the tags for the records or information on whether the record is public or private. Password masking is also symbolised here.

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.



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.

User menu

The user menu can be found in the upper right corner of the WebClient. A right click on the logged in user opens it.

- Screenshot

Options in the user menu

- Screenshot

Settings

All possible settings can be viewed in the following chapter settings.

Switch to LightClient

What the LightClient is able to do in the web view can be inspected here.

Help

A click on help takes you directly to the Password Safe documentation page.

Lock

This locks the user who is currently logged in and only needs to enter his password to use the web client again.

Log out

The logged in user is logged out. All relevant information is now required to log on again.

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.

Extras

Seal management

Here you have the possibility to manage templates for seals.

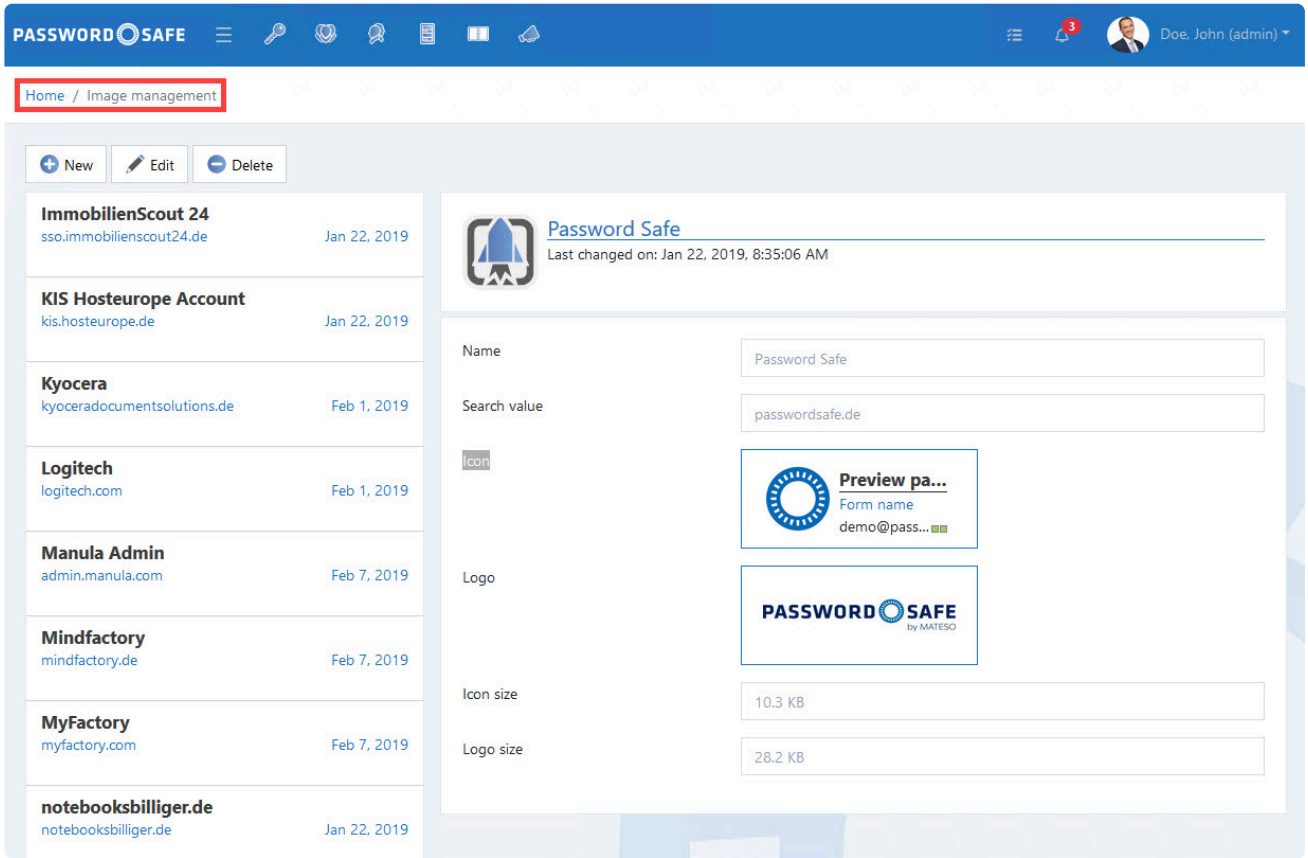
- Screenshot

Tag management

The tag management allows you to manage the tags.

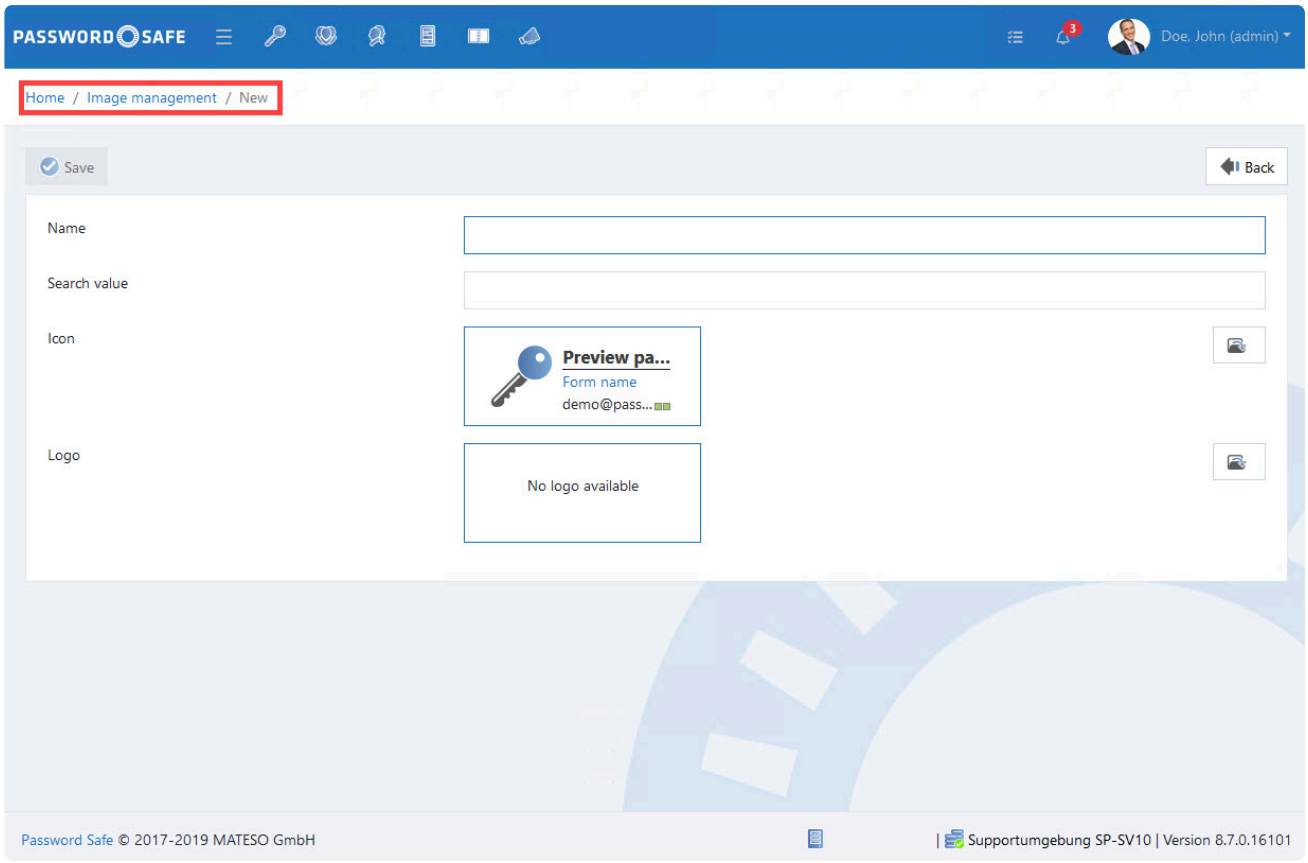
Image management

With the image management, you can manage your icons and logos easily and quickly.

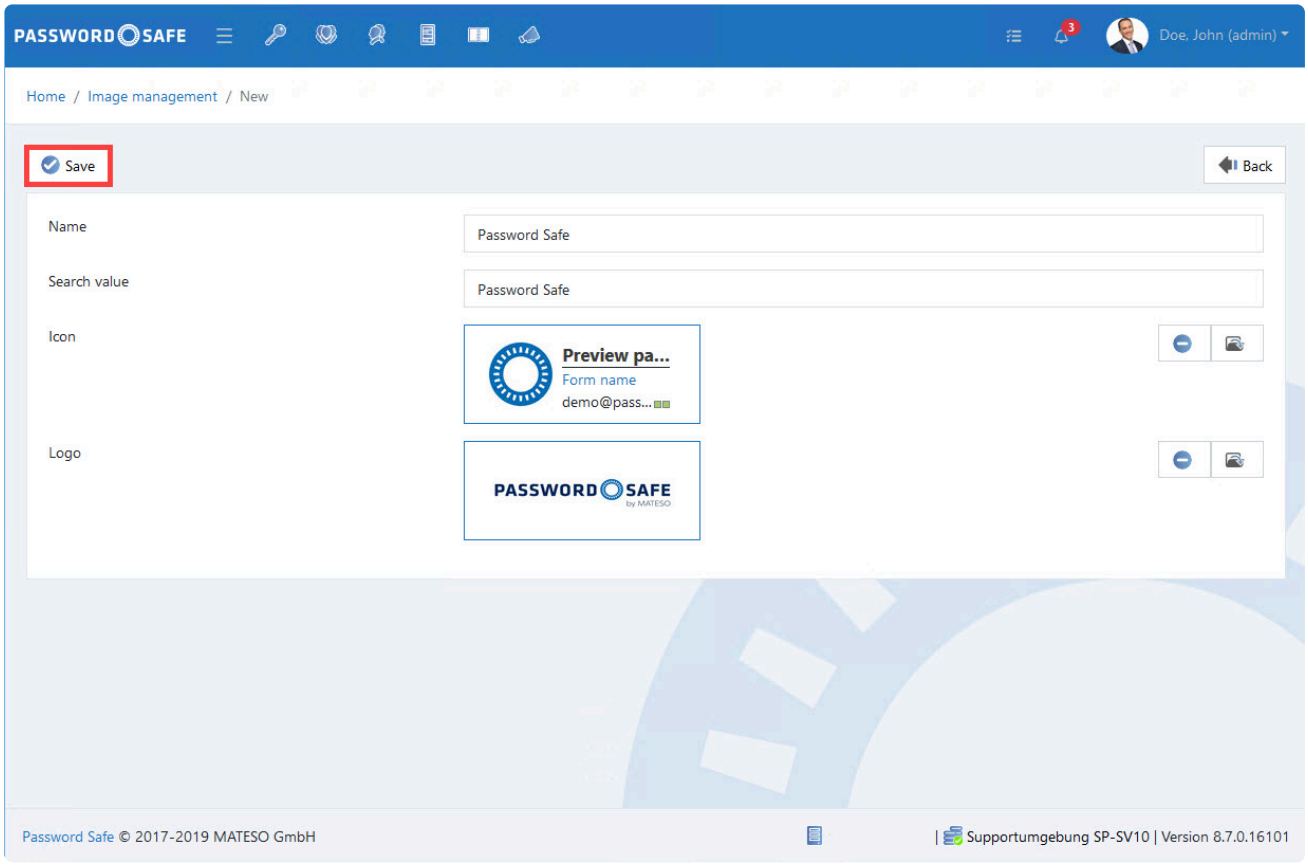


Adding icons and logos

By clicking on the **New** button, the input mask will open.

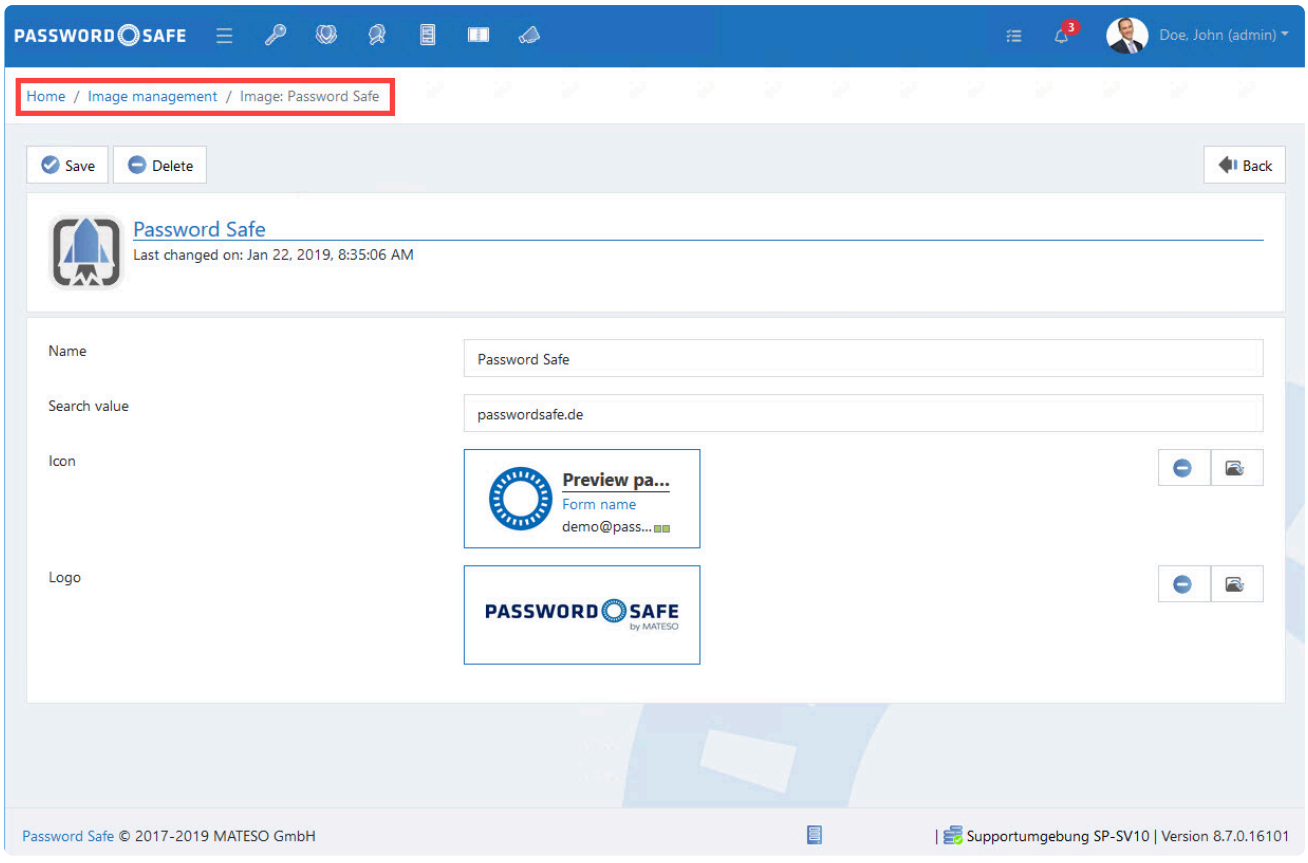


After filling in and uploading the icon/logo, the process only needs to be saved.



Edit / Delete icons and logos

If an icon and/or logo is outdated, you can edit or even delete the stored icons/logos.



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

Account

Here it is possible to change the password of the logged in user.

Authorization and protection mechanisms

Security and protection on the WebClient

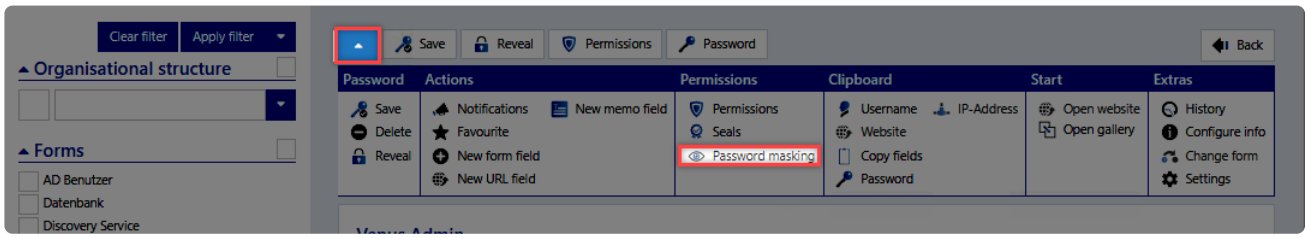
As with the client, the records can be protected on the WebClient with different mechanisms. The authorizations on records can also be managed in the WebClient. During the development of the WebClient, there was always taken care that the operation is identical to the operation of the client. Since the 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.

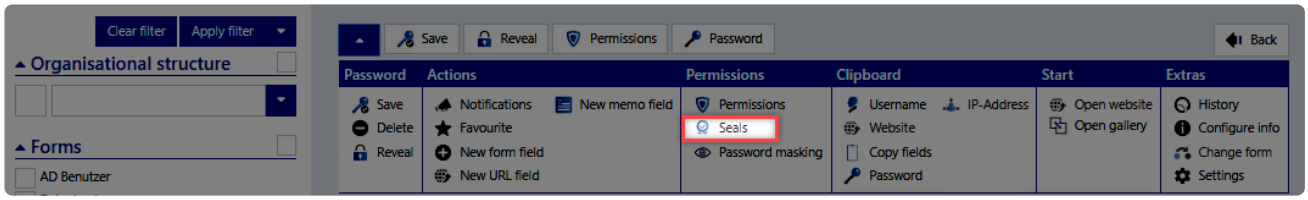


The corresponding button is only displayed if the logged in user has the sufficient rights.
If a record is provided with a privacy protection, this is shown in the header of the password.

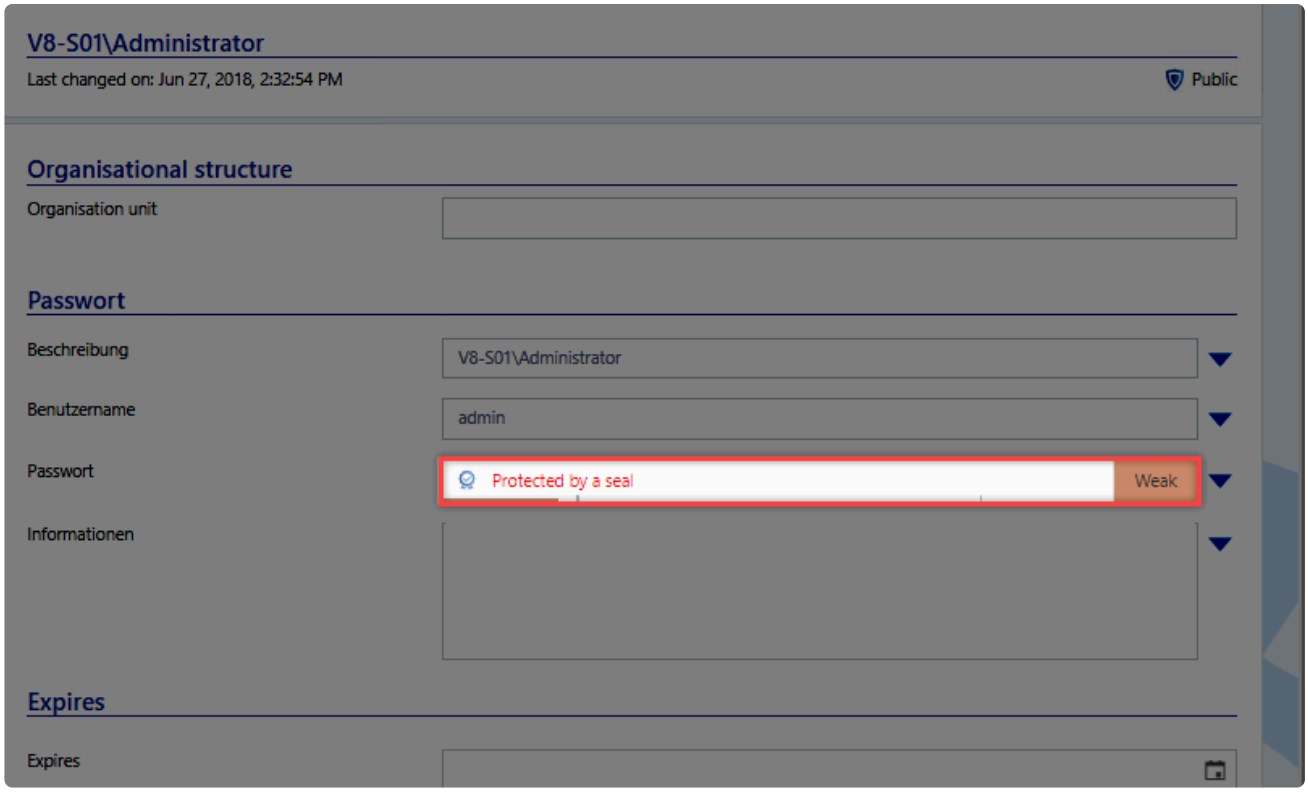


Seal

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.



Problems with the server connection

If no connection can be established from the WebClient, there are several possible causes:

Server not started

First, you should check whether the application server is running.

Service not started

The Windows service administration should be used to check whether the **Password Safe Service** has been started.

Port not released

Port 11016 TCP must be released on the application server.

CORS not configured

Make sure that the CORS configuration has been implemented. Further information can be found in chapter Installation WebClient

Mobile devices

The new Password Safe Mobile App – mobile and simple!

With version 8.10 we have created the perfect complement to the client: **The Password Safe Mobile App**!
With its **convenient** interface, the Password Safe Mobile App offers the perfect prerequisite for every user to find their way around **quickly** and **easily**.

For detailed documentation of the **Password Safe Mobile App**

Screenshot

> Please note that as of version 8.10.0, the previous version 7 App is no longer compatible.

Security is our ambition

No matter whether you work with a smartphone or a tablet, you benefit from the highest possible security on all iOS and Android devices. All passwords are not only available on the mobile device, but can also be automatically transferred to websites. So you can use highly complex and therefore secure passwords and don’t have to remember them anymore. The Password Safe Mobile App thus combines security and convenience. In addition, the use of a local database ensures that passwords can be accessed even when no

Functions

The functionalities of **password management**, **SSO**, **synchronization** and **tab system** are even more extensive and detailed in the specially created **documentation**.

Password management

The new **Password Safe mobile app** keeps all **passwords** safe. They can not only be stored securely but also structured conveniently.

SSO

The most important convenience feature of the Password Safe Mobile app is the possibility of entering passwords directly into log-in masks of other apps or browser pages. The configuration and correct use can be found out in the corresponding chapters for **iOS** and **Android**.

Synchronization

Since the data exchange between mobile database and server database is done automatically in the background, there is no need to worry about the actuality of the data. More detailed information about synchronization can be found **here**.

Tab system

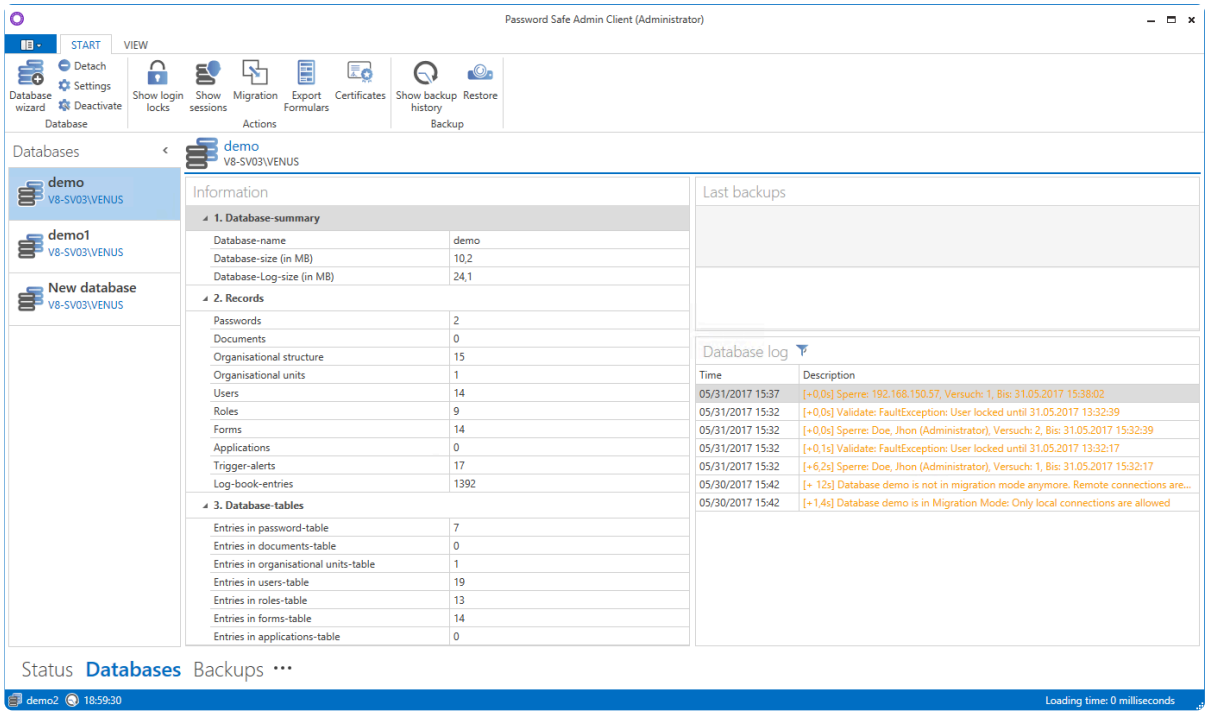
With the new and simplified tab system, the handling for the individual user has been made uncomplicated and clear. The affiliation of the passwords is visible at a glance. The exact handling of the tab system can be read in the chapter **Tabs**.

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”

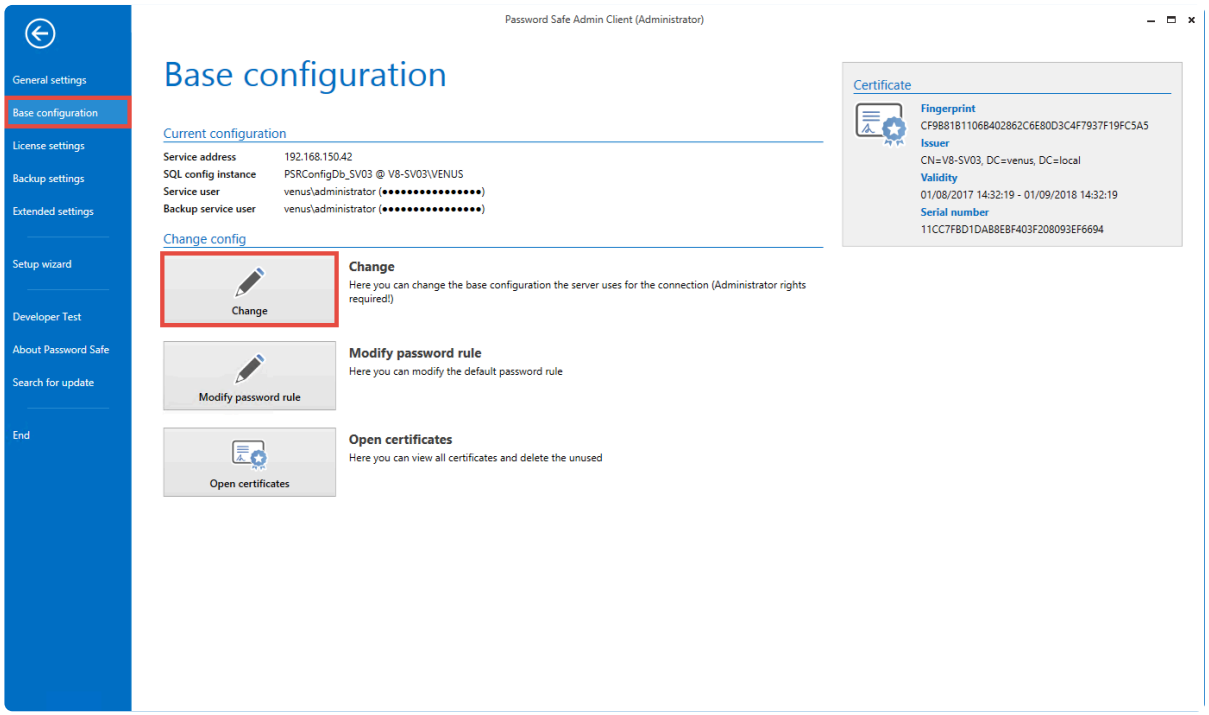


In this sense, the server service represents the interface between the client and the SQL server. The AdminClient is responsible for configuring the server service. It allows the central administration of the databases without having access to the SQL server. This is a huge advantage with regards to organization and authorizations.

Basic configuration

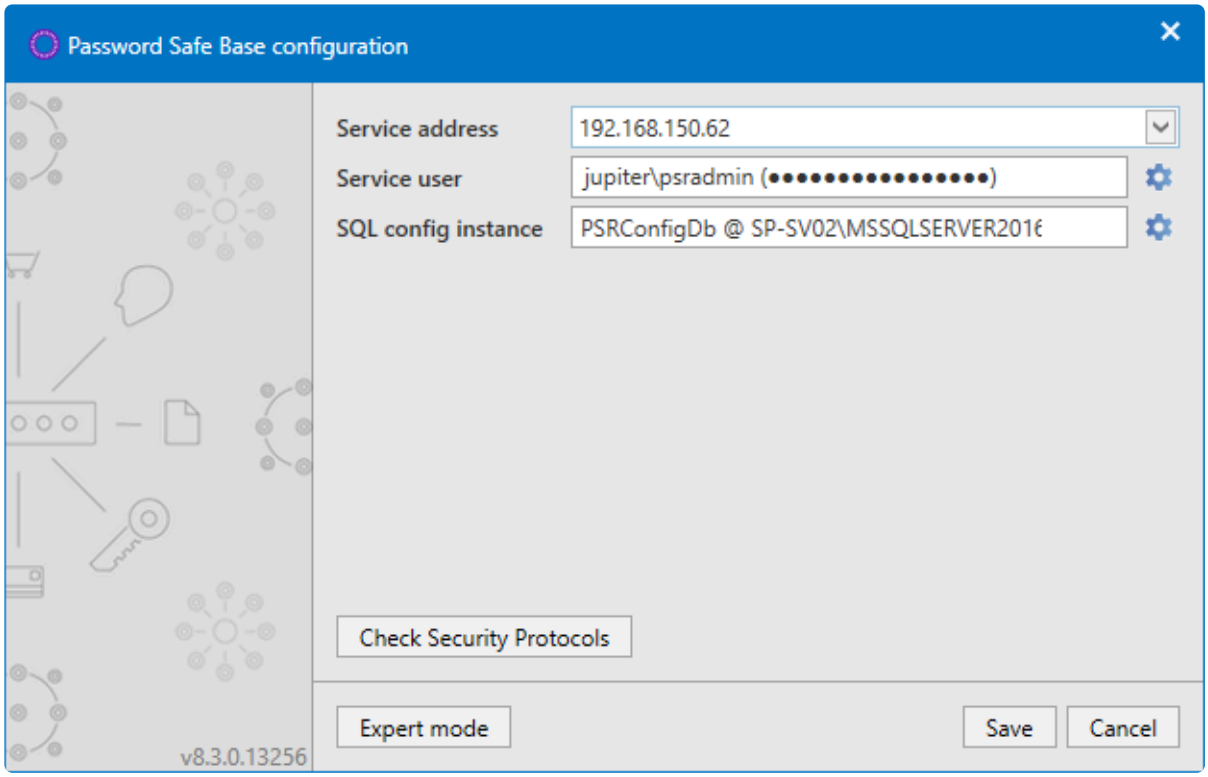
What is basic configuration?

Within the basic configuration, the connection to the SQL server or to the databases is defined. The basic configuration appears the first time the AdminClient is started and can be called up at any time in the basic configuration.



The basic configuration

A special wizard is available to carry out the configuration:



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.

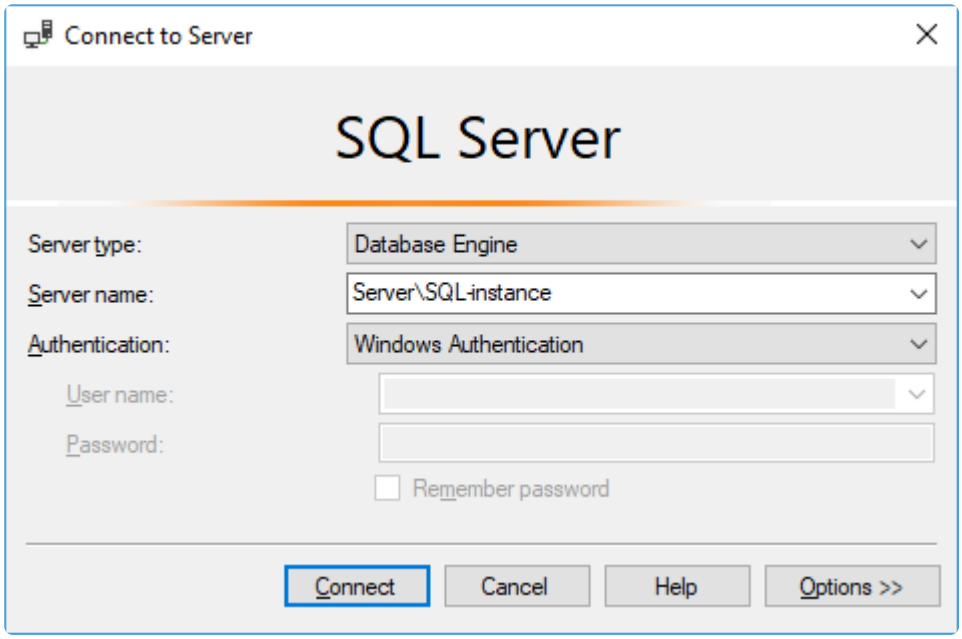
Service user

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 defined service 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.



If the option “Service user” is selected, enter the user that 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 for server section for more information about the users.

Expert mode

Expert mode displays additional menu options for advanced configurations:

Backup service user

You can use a dedicated user to run the backup here. The service user is selected by default.

SQL configuration instance

This menu item can be configured in **expert mode** via a so-called **connection string**.

Certificate

The SSL connection certificate can also be configured under this item 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 by each client.

Allow host mode

Host mode is no longer supported since version 8.13.

Activating caching

Caching is activated by default to improve performance. The so-called SqlBroker is registered for the database on the SQL server here. The following is cached:

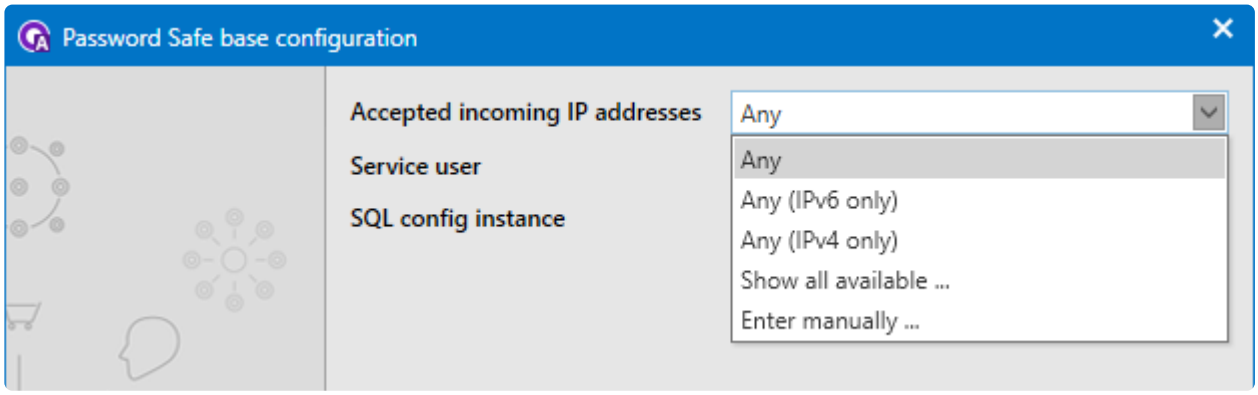
- The roles of the individual users
- The structure of the organisational units
- All settings

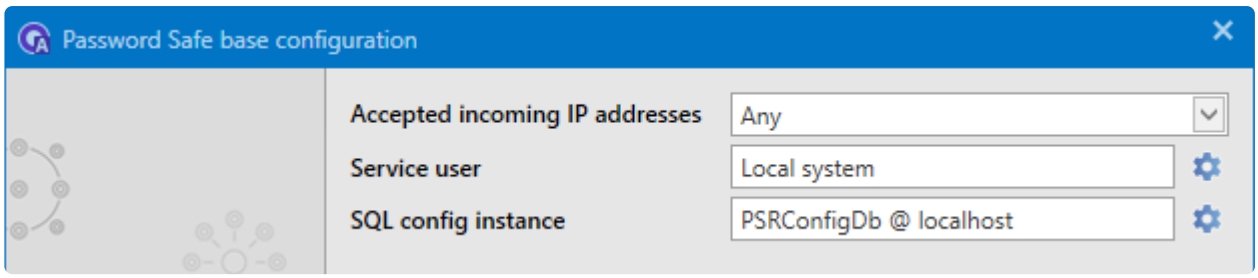
> If this option is changed, the server needs to be restarted so that the change can take effect.

Click here to return to the “Getting started” section

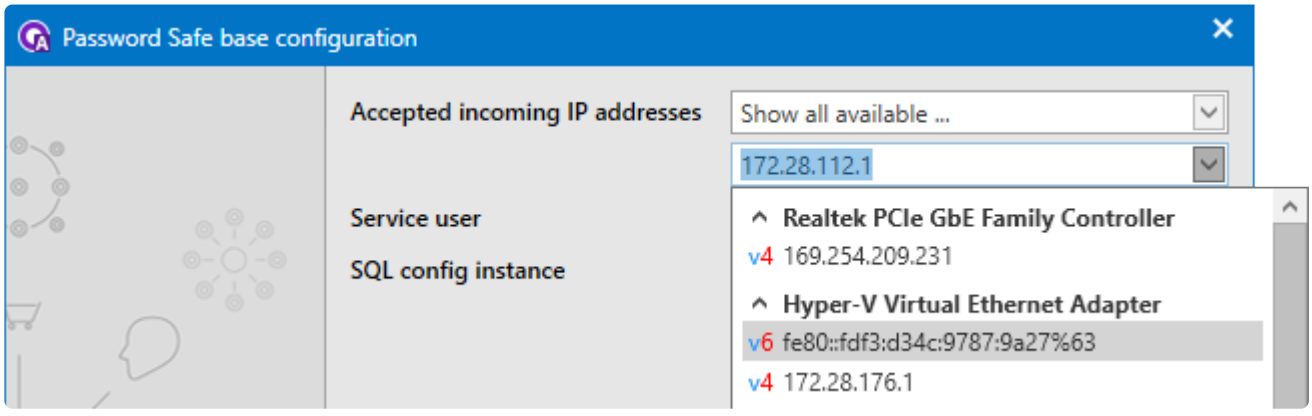
Enable DualStack IP (IPv4 + IPv6)

We now have a DropBox control for the IP address configuration. The default value for this configuration is “Any”, this settings also enables the DualStack IP mode. The settings “Any (IPv6 only)” and “Any (IPv4 only)” set the ForceIpAddress attribute to the respective ANY-addresses “[::]” (for IPv6) and “0.0.0.0” (for IPv4).

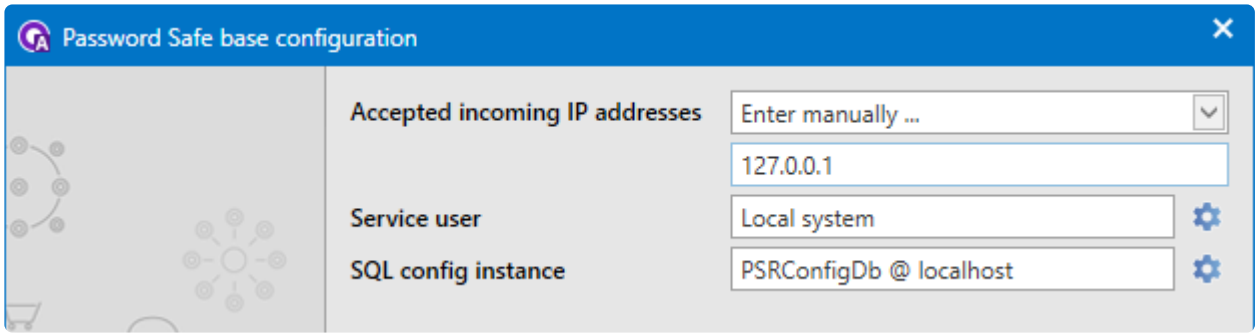


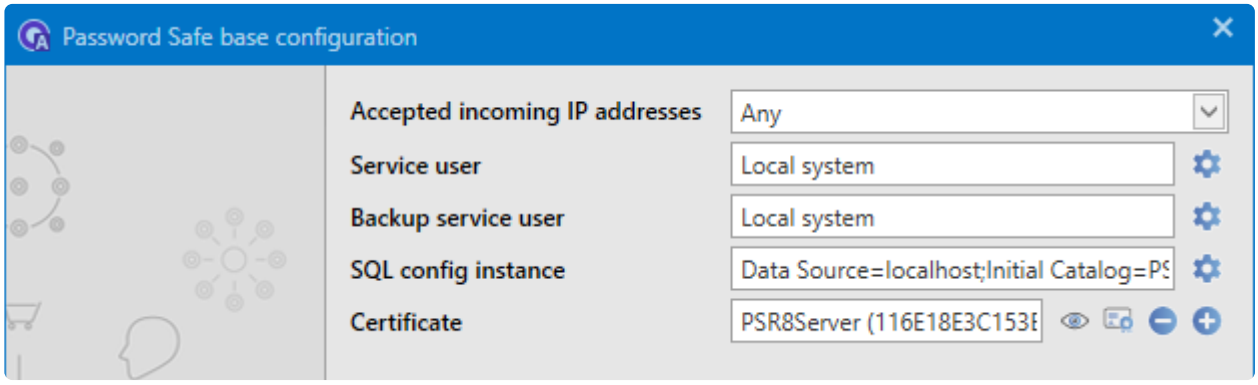


The “Show all available …” option adds the familiar DropDown control to select one of the systems IP addresses.



The “Enter manually …” option adds the TextBox control for the previously known “Static service address” configuration. Consequentially the “Static service address” field was removed from the “Expert Options” and the corresponding warning is also gone.


Password Safe base configuration
Accepted incoming IP addresses
Enter manually ...
127.0.0.1
Service user
Local system
SQL config instance
PSRConfigDb @ localhost


Password Safe base configuration
Accepted incoming IP addresses
Any
Service user
Local system
Backup service user
Local system
SQL config instance
Data Source=localhost;Initial Catalog=PS
Certificate
PSR8Server (116E18E3C153E

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:

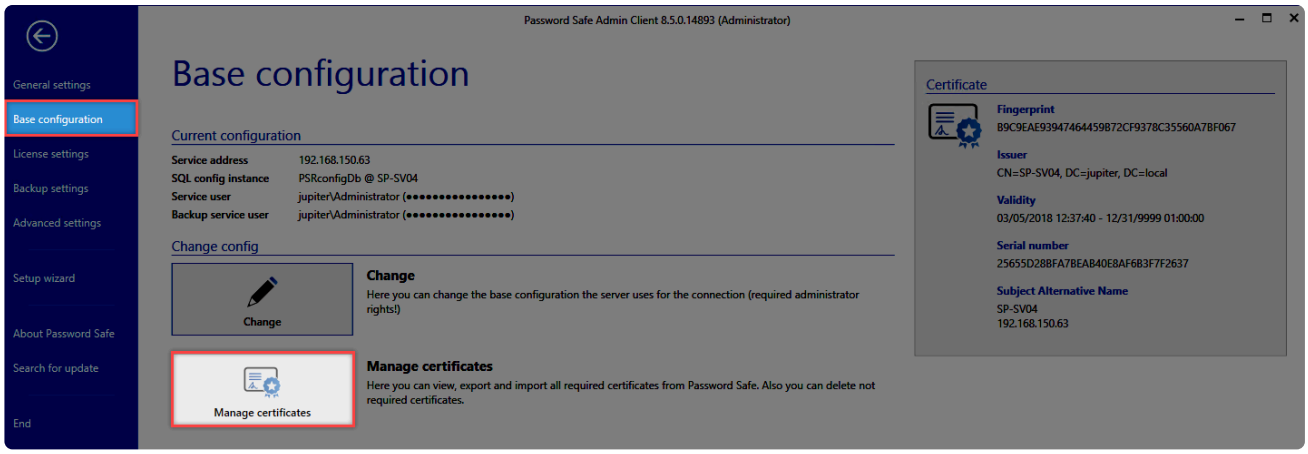
- SSL connection certificates
- Database certificates
- Master Key certificates
- Discovery service certificates
- Password Reset certificates

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:



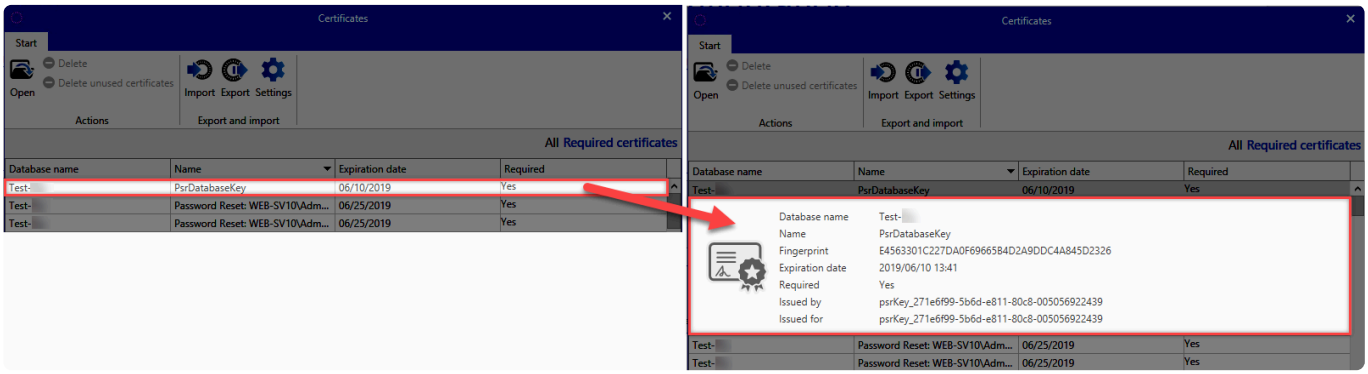
In the **Main menu**, it is also possible to start the certificate manager for all databases via the **basic configuration**:



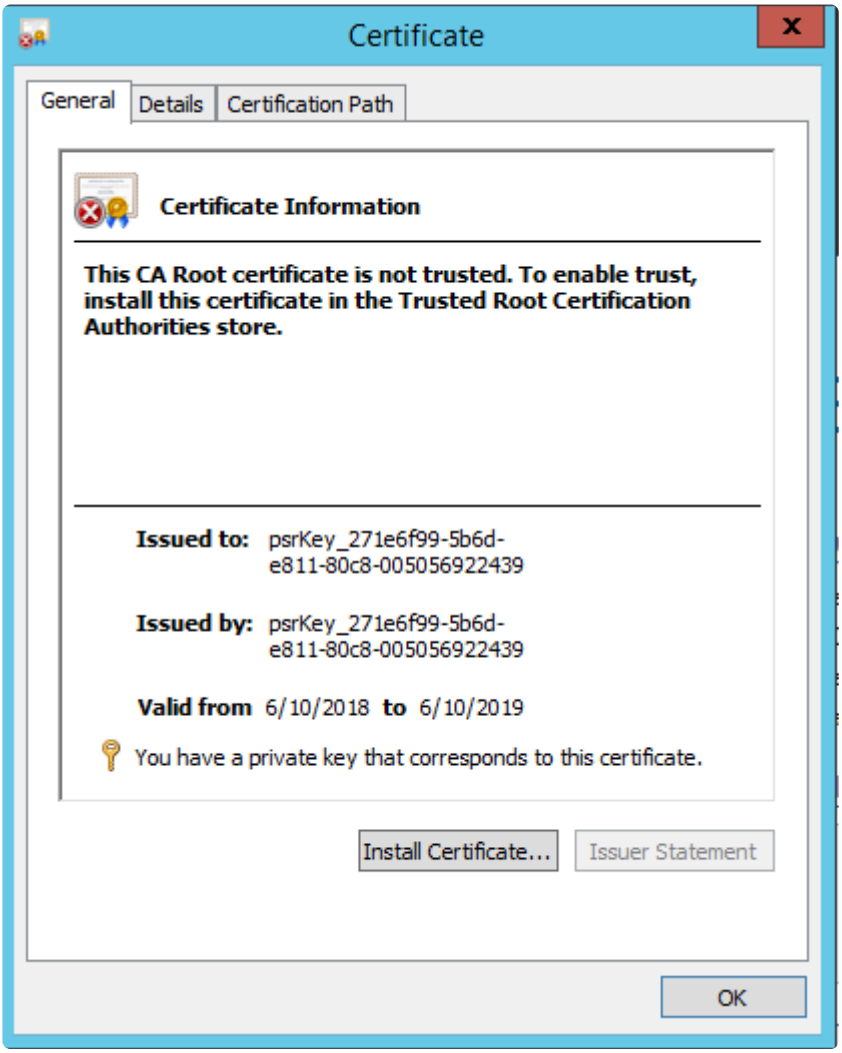
Operation of the certificate manager is always the same. The only difference is whether the certificates are displayed for each database or for all databases.

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.

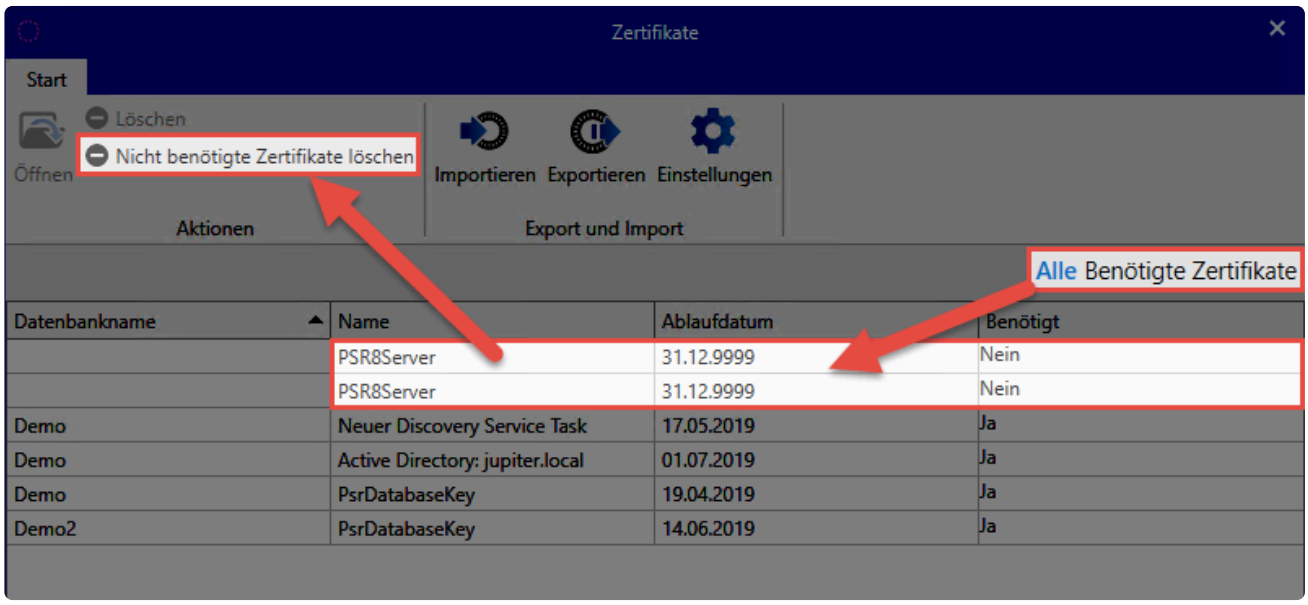


Double clicking on a certificate will open the Windows Certificate Manger to provide more detailed information.



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.



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.

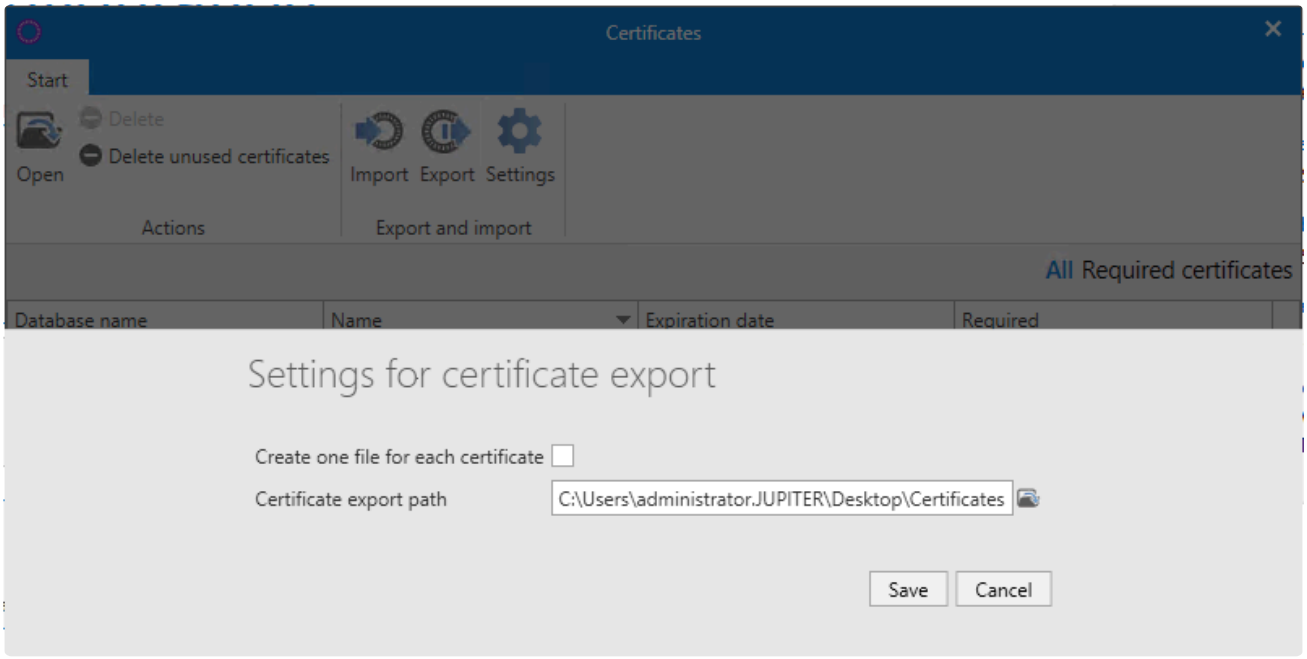
Exporting certificates

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.



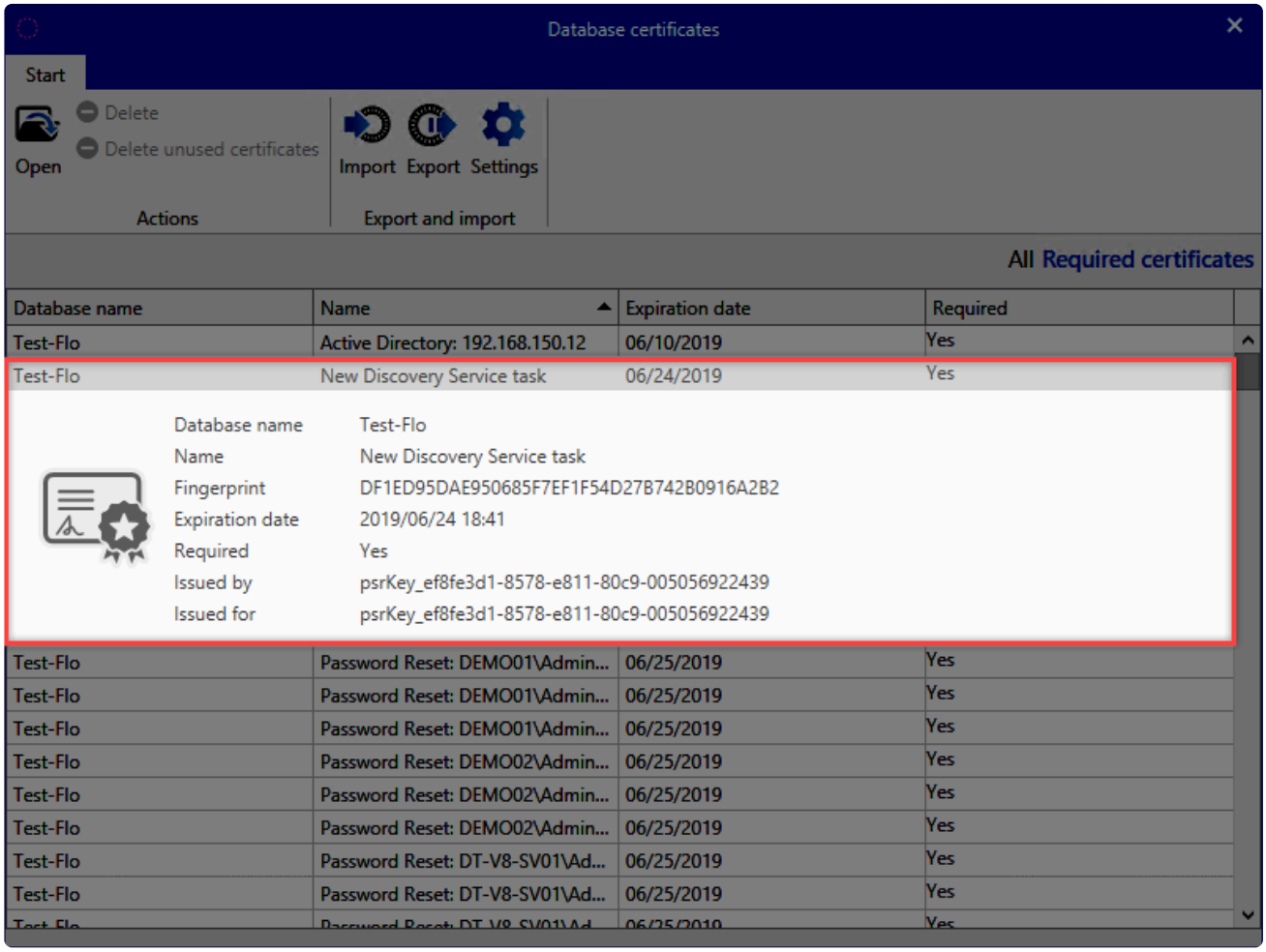
Backing up certificates

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.

Discovery service certificates

What is a discovery service certificate?

If a discovery service is created, a corresponding certificate is also created:



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.

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.



✻ 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.

All information (including the IP address) are stored as DNS name.

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.

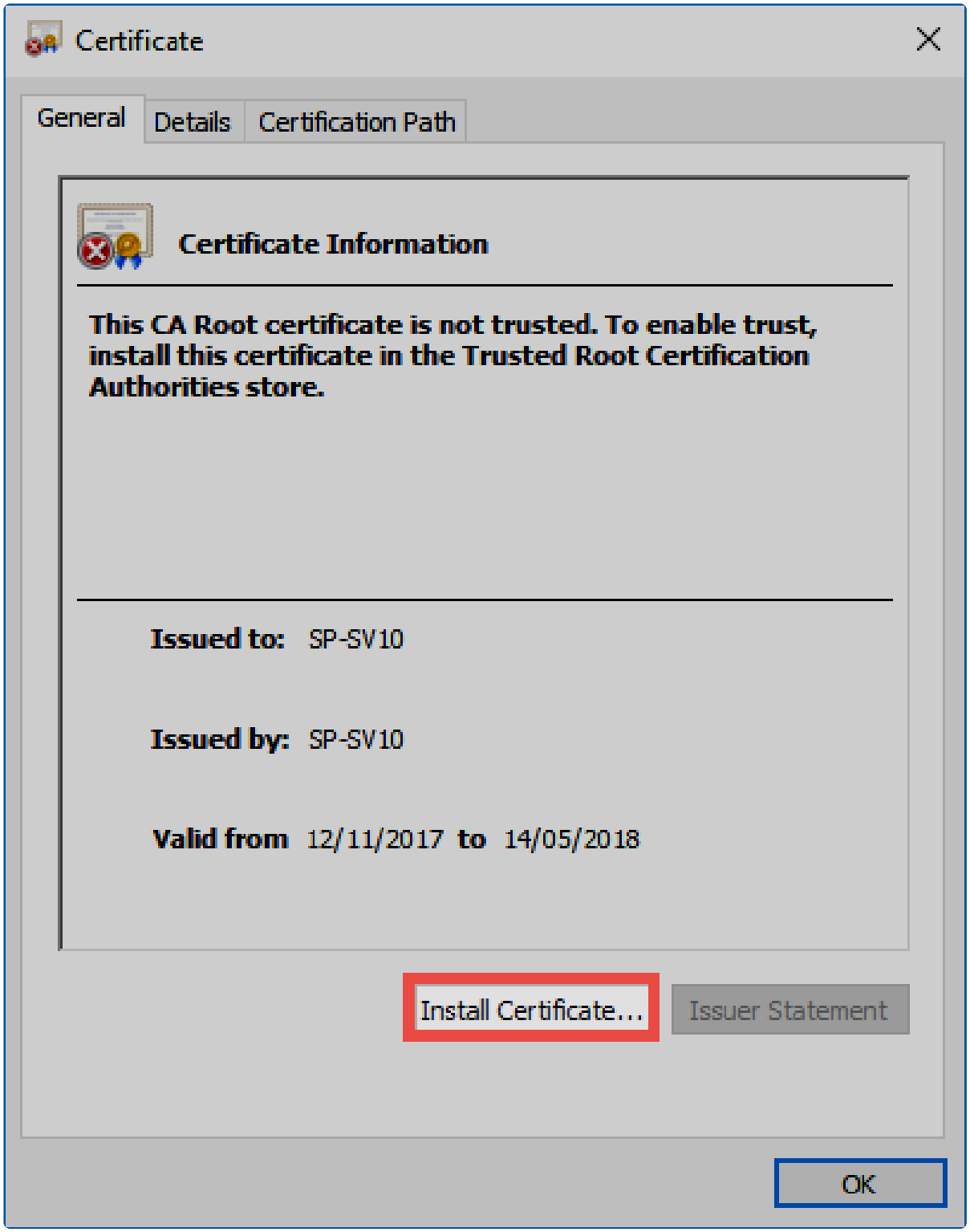
Distributing the Password Safe certificate

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

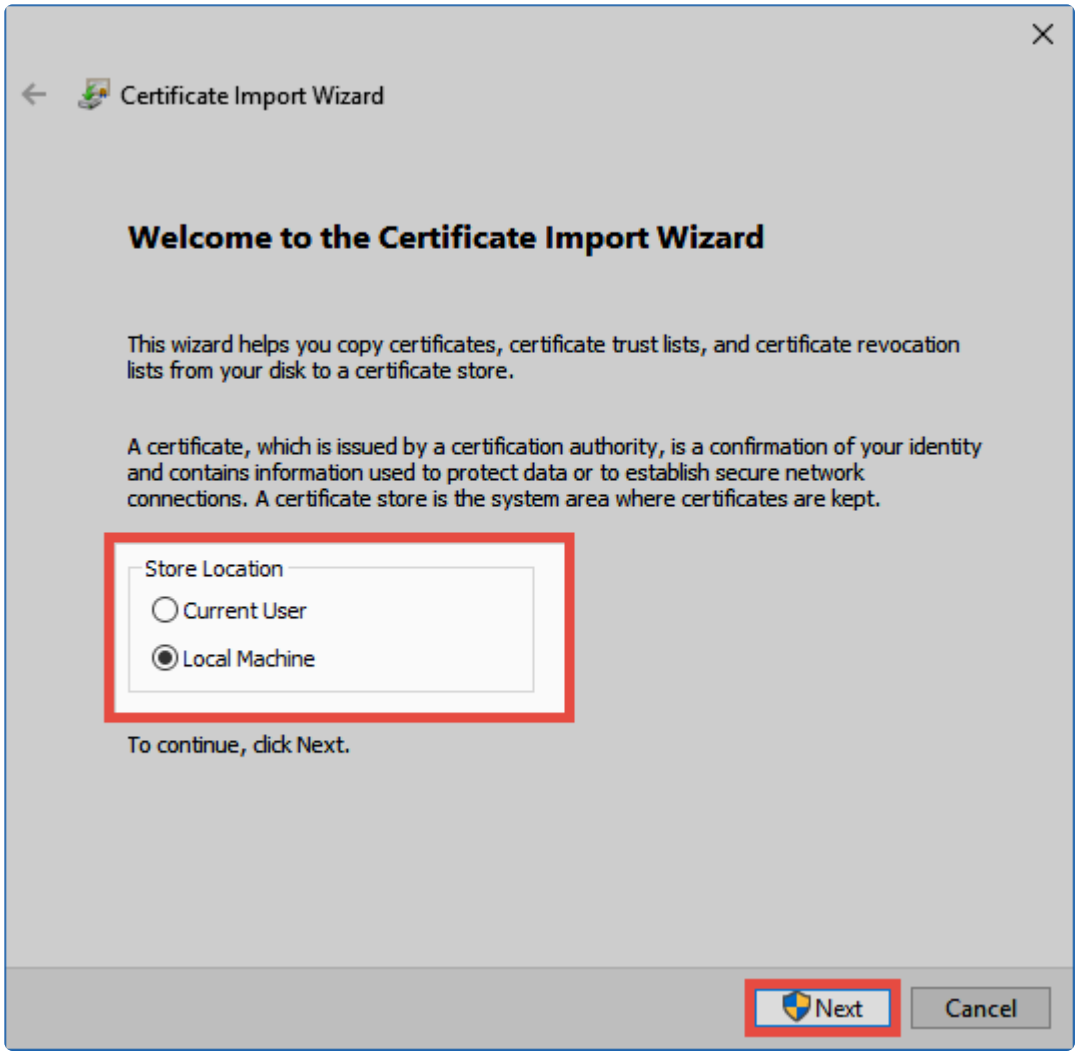
The certificate can be both rolled out and distributed using group guidelines.

Manually importing the Password Safe certificate

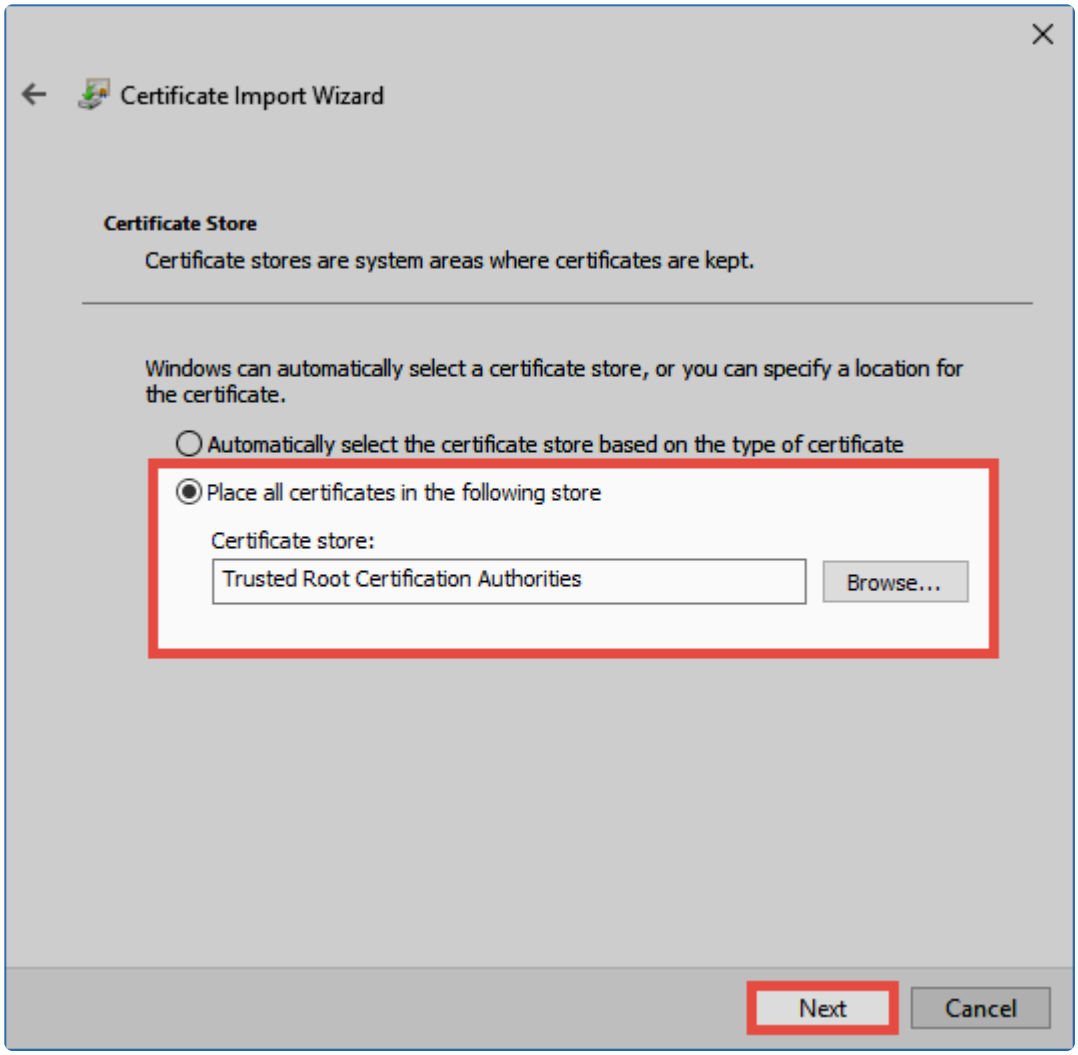
If the Password Safe certificate is not rolled out, it is also possible to manually import the certificate. To do this, firstly open the certificate information. In the warning notification, the **Show server certificate** button is available for this purpose. In the following dialogue, select the option **Install certificate…**



A **Certificate import wizard** will open in which **Local computer** should be selected.



In the next step, the storage location “trusted root certificate location” needs to be manually selected.



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 configuring, you must ensure that the clients can access the CA lock lists

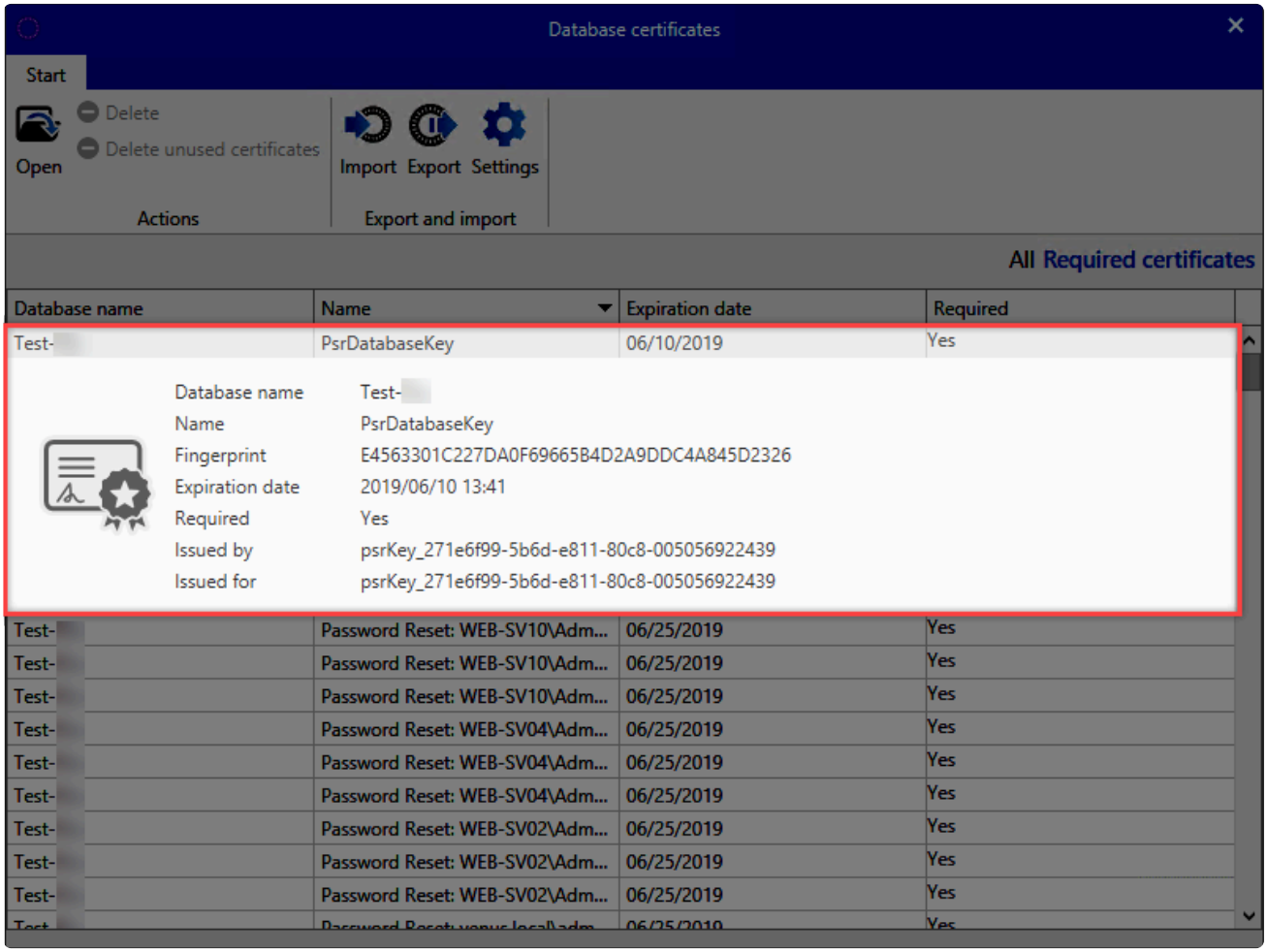
Wildcard certificates

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**:



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**!

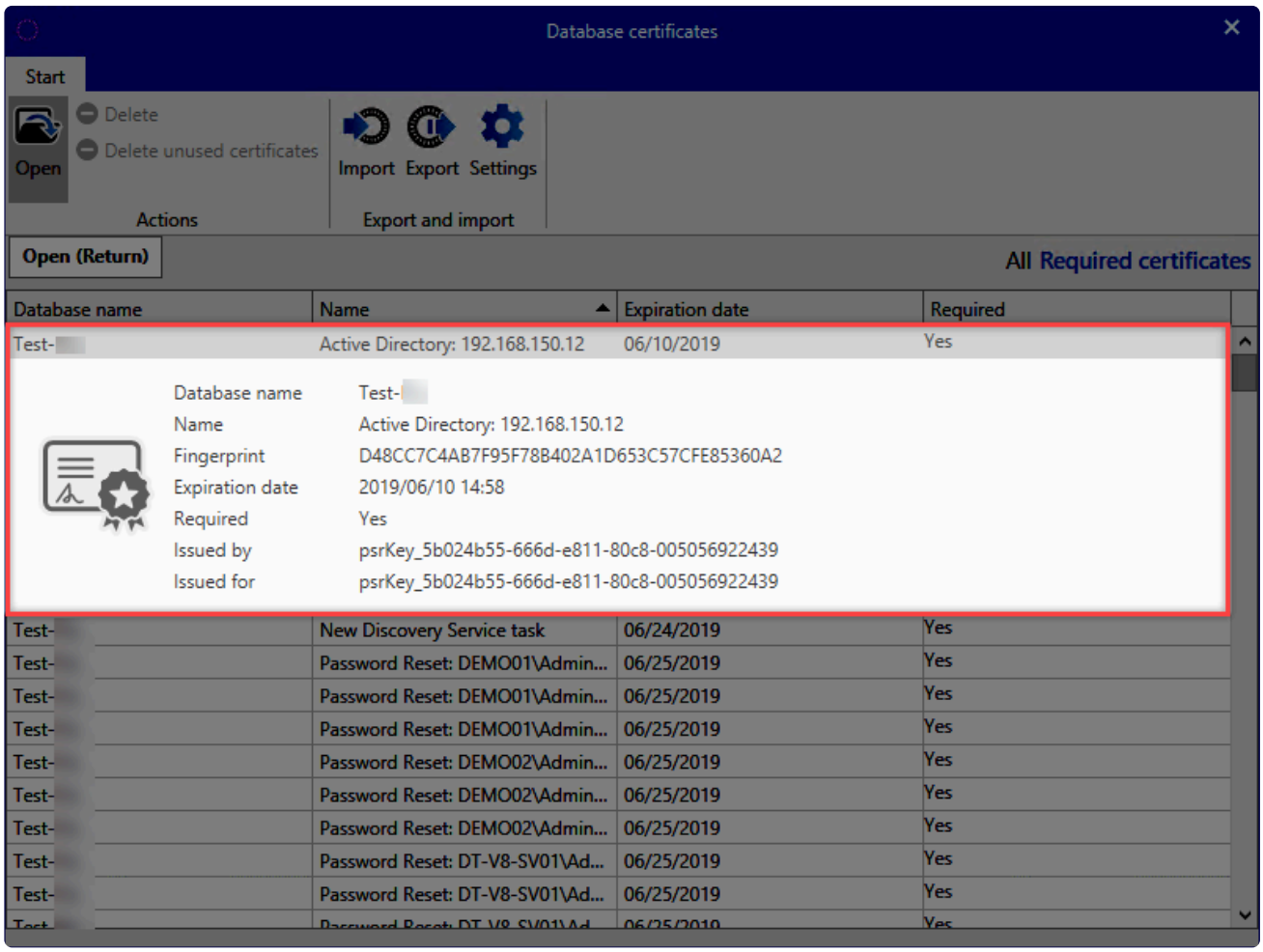
Exporting and importing the certificate

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**:



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**!

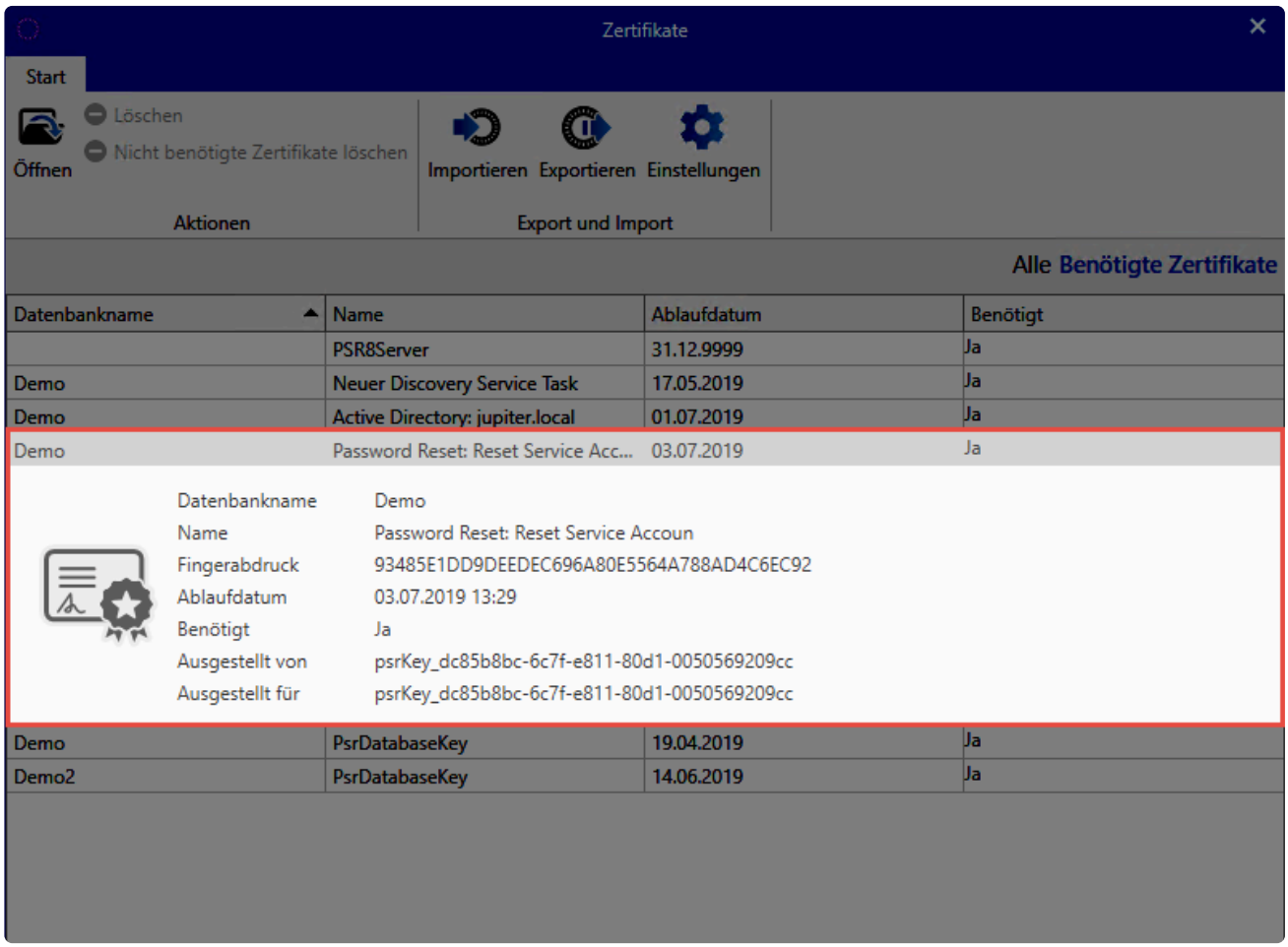
Exporting and importing the certificate

The section certificates explains how to back up the certificate and link it again.

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.



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.

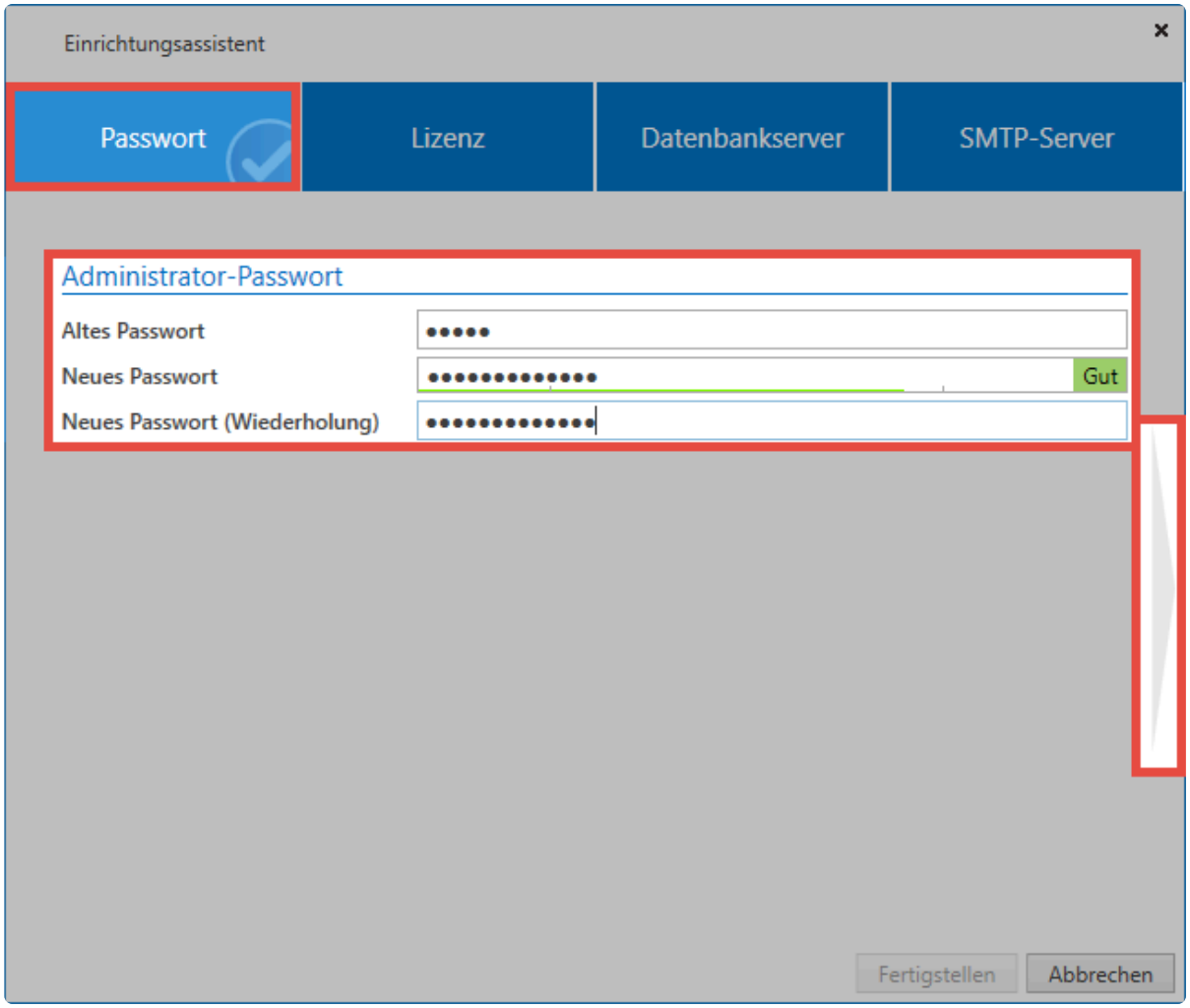
Setup wizard

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

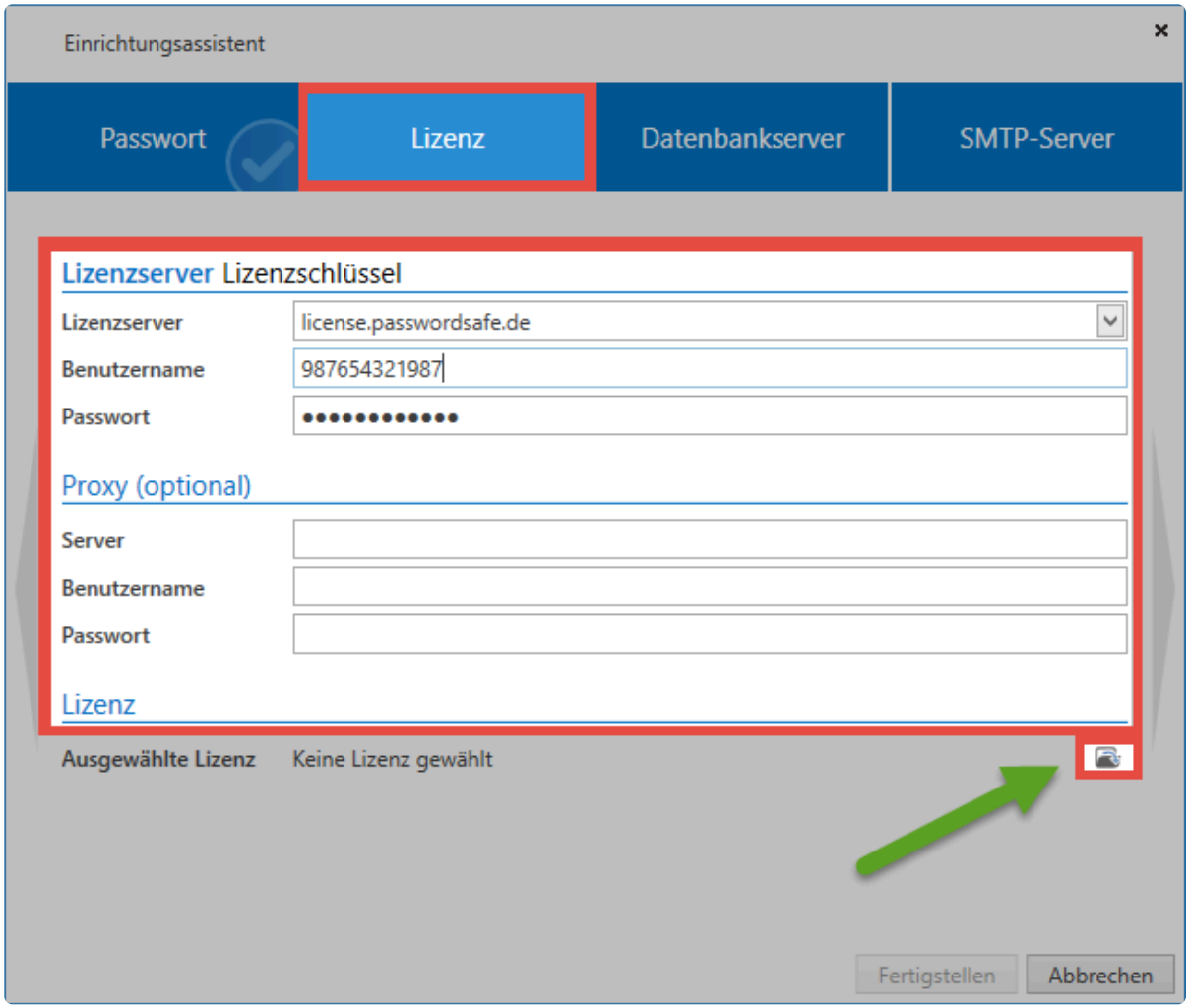
The first step is to define the authentication password for the AdminClient. The initial password is “admin”. A new password needs to be entered during startup – this new password should be securely and properly documented. It can be subsequently changed in the general settings.



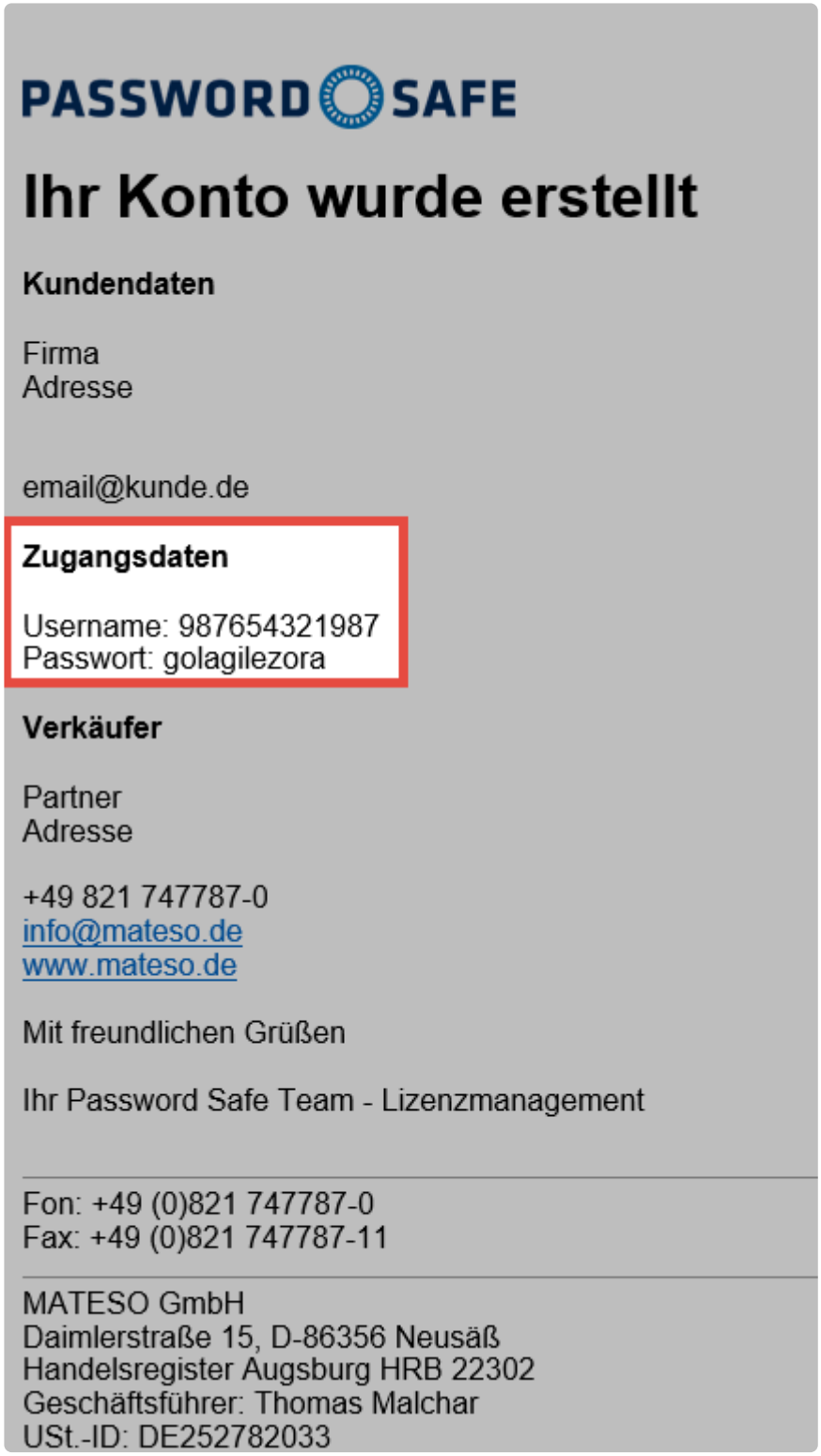
The initial password is “admin”.

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.



“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).



PASSWORD SAFE

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

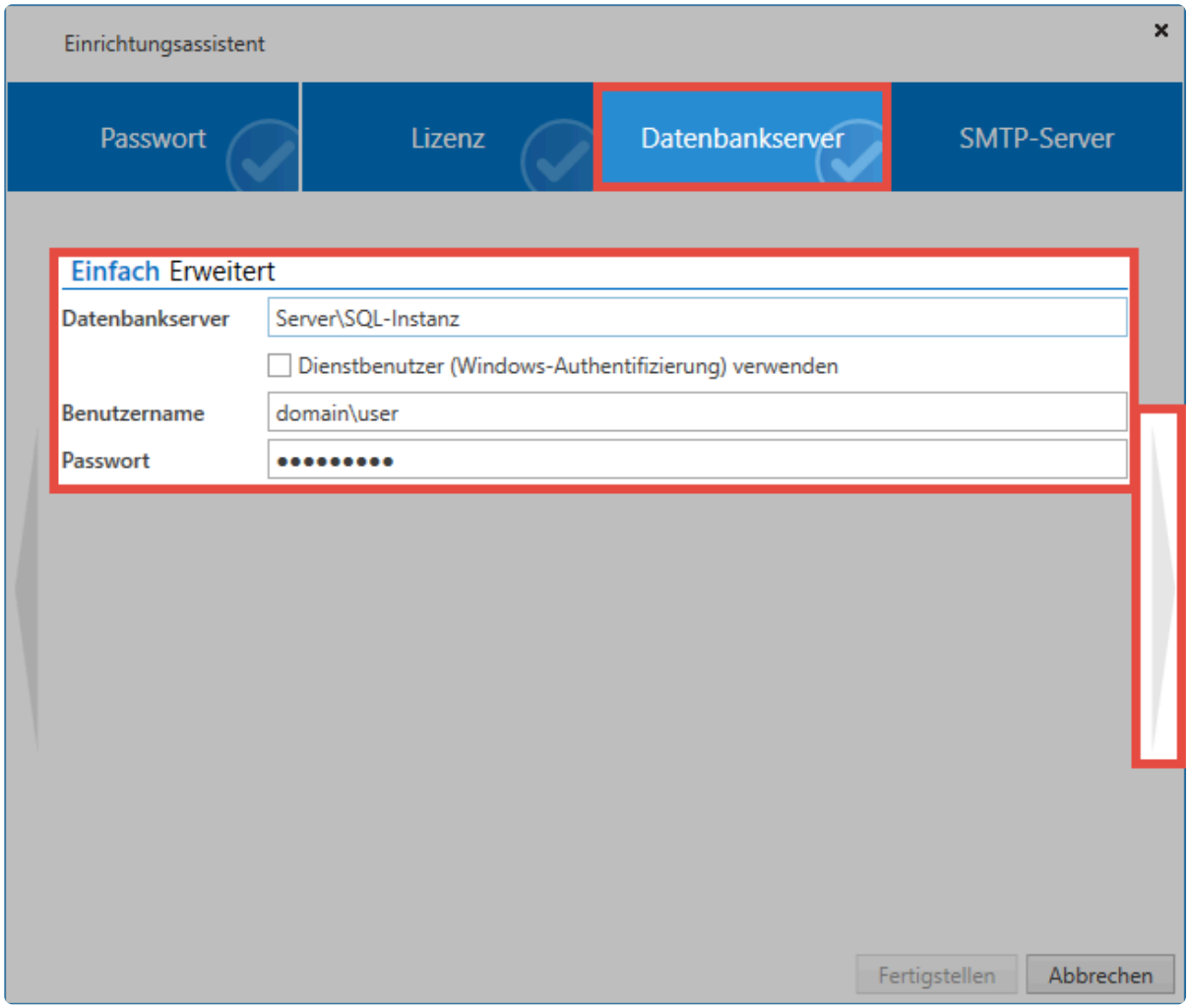
Fon: +49 (0)821 747787-0
Fax: +49 (0)821 747787-11

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.

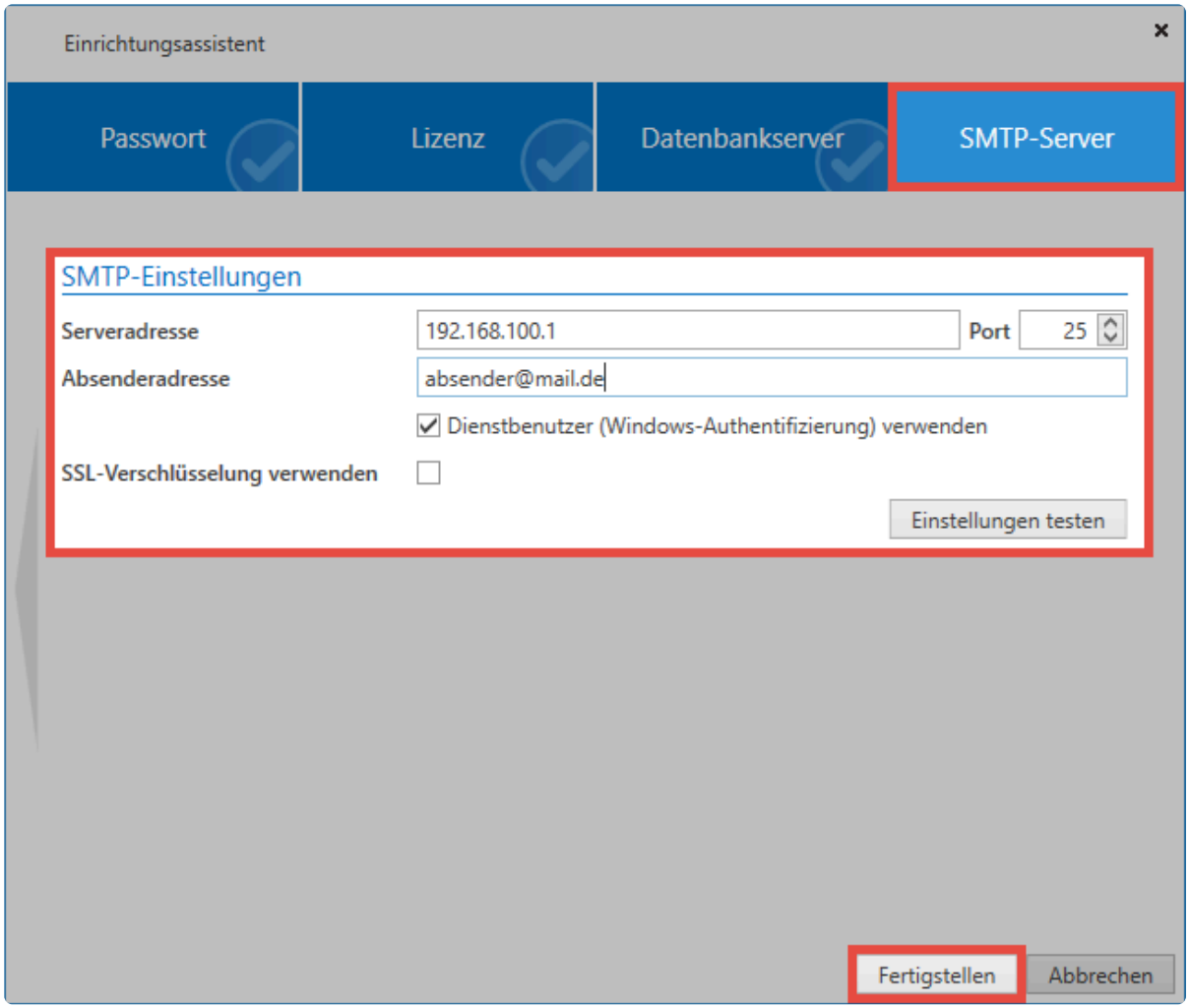


The database server must be specified along with the associated SQL instance. For simplicity, you can copy the server name from the login window of the SQL server.

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.



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:



> ! 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



https://www.youtube.com/embed/md7_VEdVuWM?rel=0

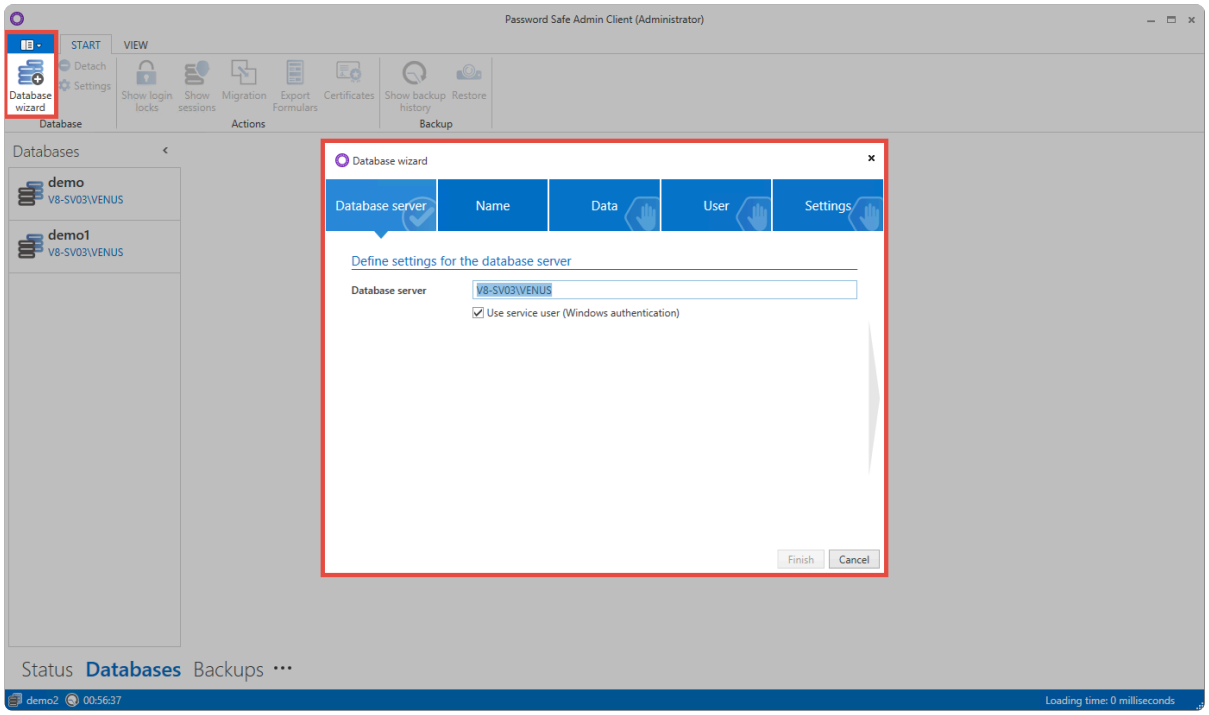
https://www.youtube.com/embed/md7_VEdVuWM?rel=0

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:



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

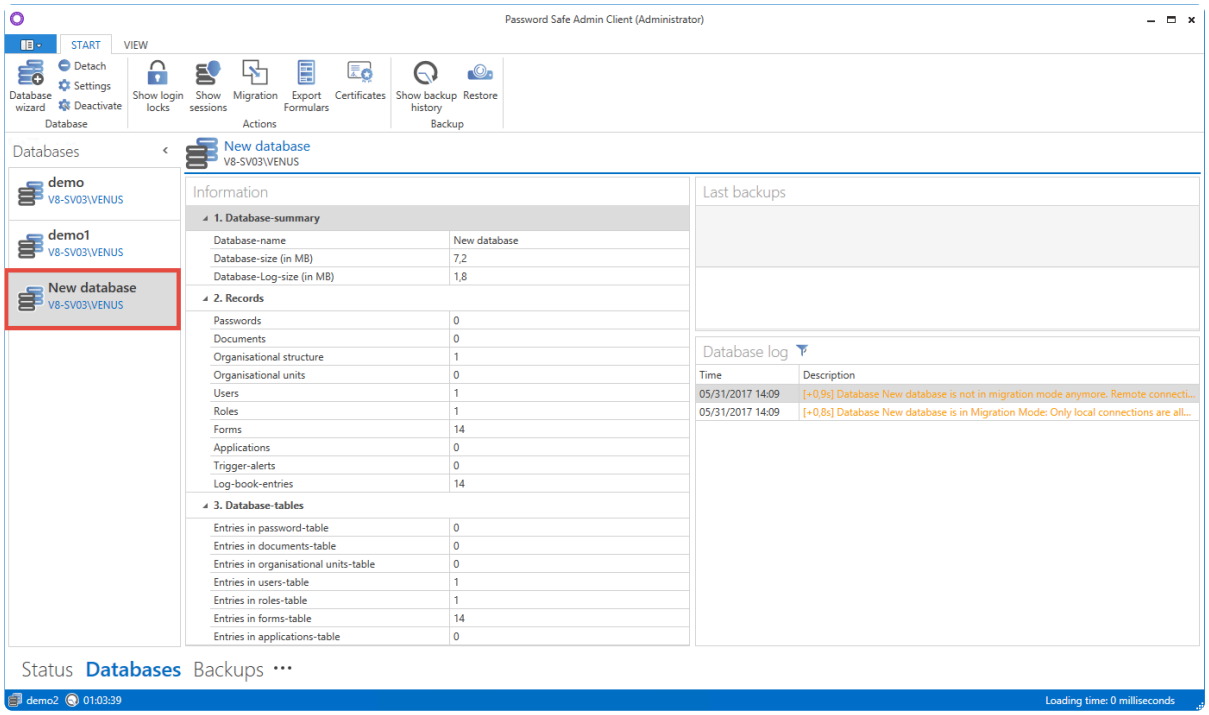
This setting can be used to define whether a template should be used. The template will provide the database with ready-made forms and dashboard settings that make it easier to get started. The user can select from English and German templates. However, it is also possible to proceed without a template – 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.

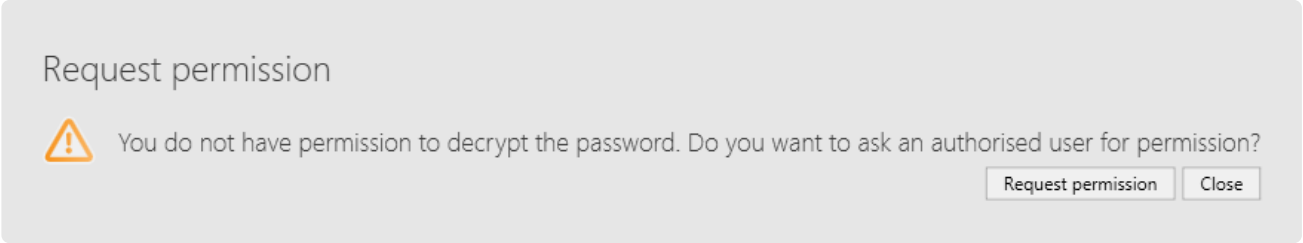


Click here to return to the “Getting started” section

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:



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

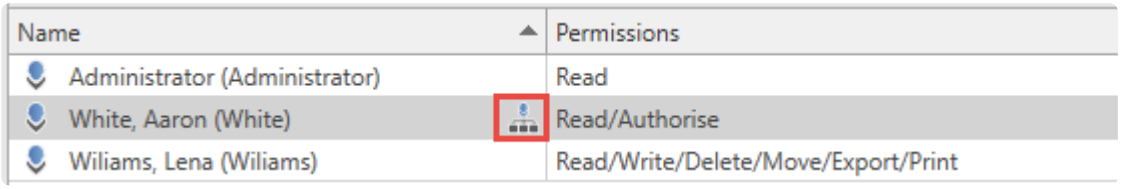
Passwords in which users / roles without a legal key or with a legal key but without an authorization right exist:

```
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.



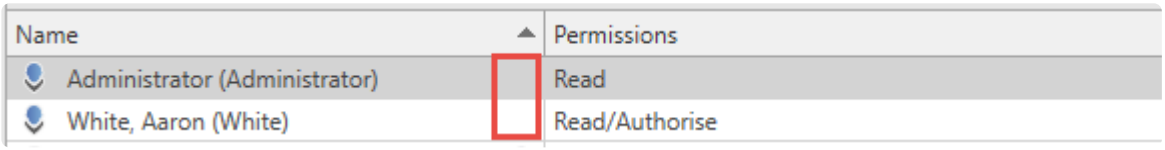
When logging on to the database via the client, a cleanup task is started automatically. This task always runs with the logged in user. In this case – as far as it is possible with the user – all affected passwords are corrected. Thus, when all users have logged in once, all affected passwords should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

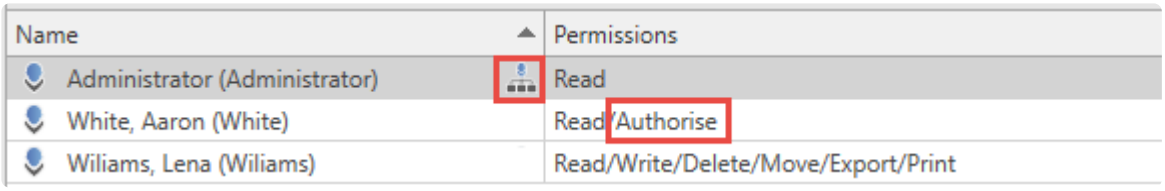
In the first case, no user / role has the right key on the password. Thus, no user can decrypt or correct the password.



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

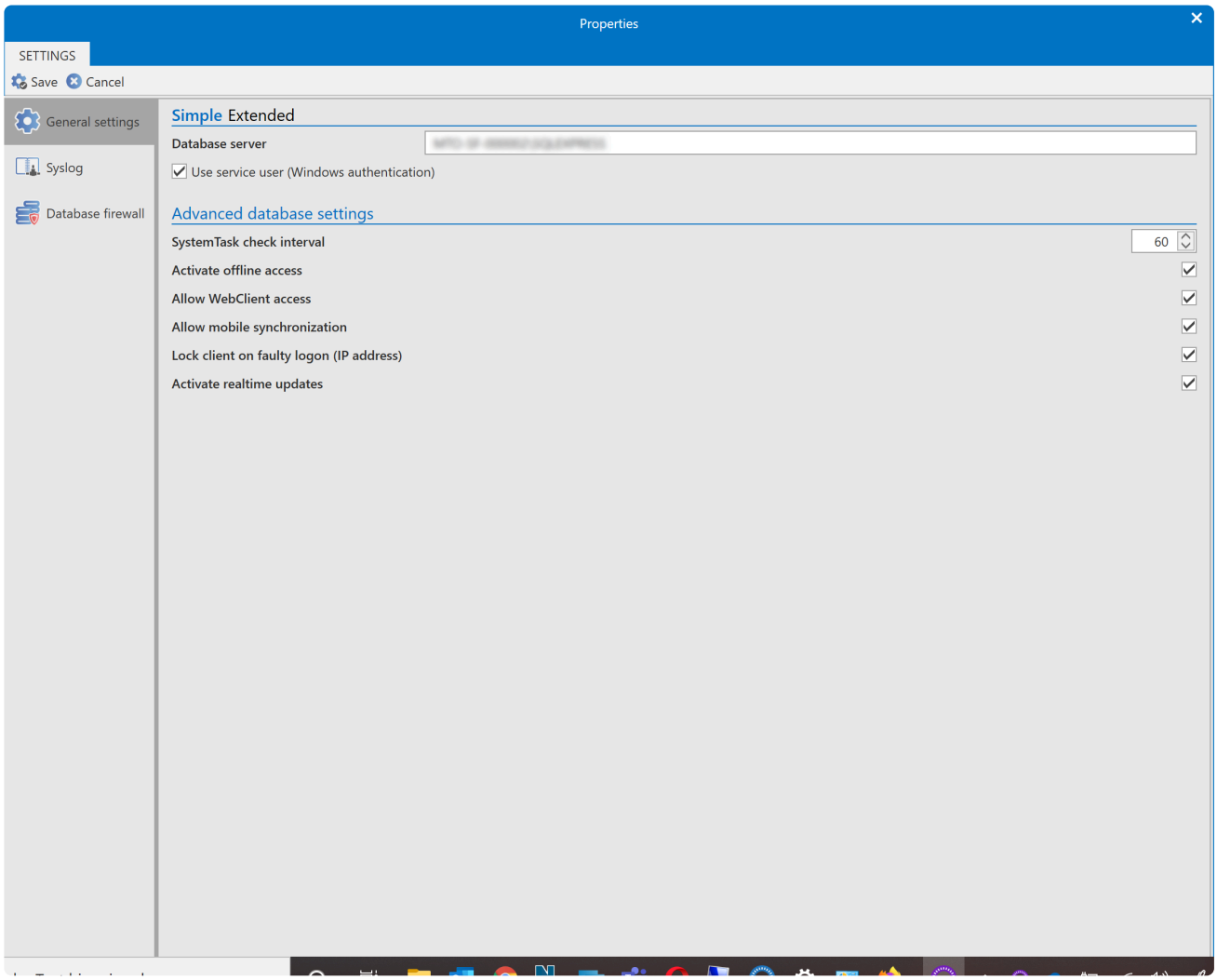
In the second case, there are users / roles who have the right key but not the right to claim. As far as the number of irreparable passwords is limited, these can be used to check the form field permissions manually.



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.

Database properties

The properties of a database can be opened by double-clicking on the database. No login to the database is required.



Properties

The following options can be edited:

- **General settings**
- **Syslog**
- **Database firewall**

General Settings

The following can be defined in the **General Settings**:

- **Database server** – here the SQL instance can be specified again.
- **SystemTask check interval** – specifies the time interval in which the check interval for SystemTasks should run (**default set to 60 minutes**)
- **Enable offline access** – Activate/deactivate the offline client

- **Activate access via web client** – Activate/deactivate the web client (**active by default**)
- **Allow mobile synchronization** – Activate/deactivate synchronization with mobile devices
- **Lock clients if login is incorrect (IP address)** – Lock IP if login is incorrect
- **Enable real-time update** – Enables/disables real-time update between clients (**default is active**)

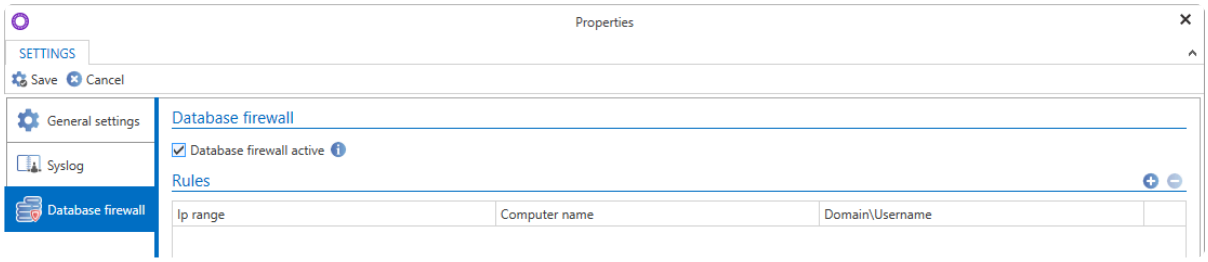
Database firewall

What is the database firewall?

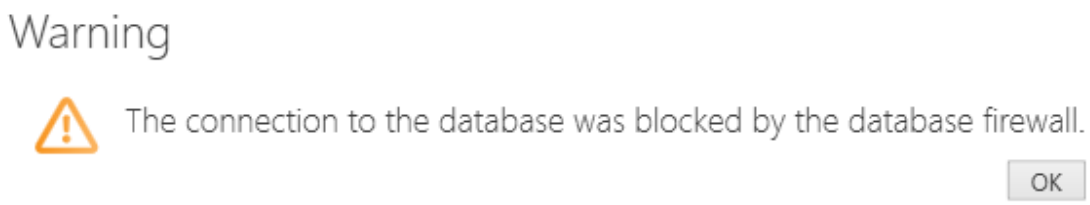
The database firewall enables you to regulate access to the database. A whitelist policy is used for this process. Firewall rules are used to allow access to the database in individual cases.

Activating the firewall

The firewall can be directly activated in the database settings.

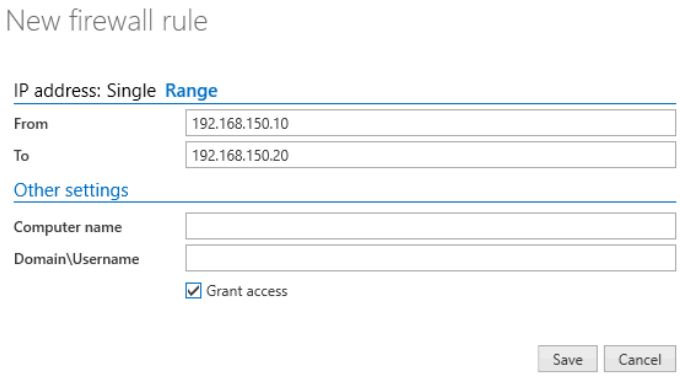


Access to the firewall is blocked after it has been activated. Login attempts are directly blocked.



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.



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.

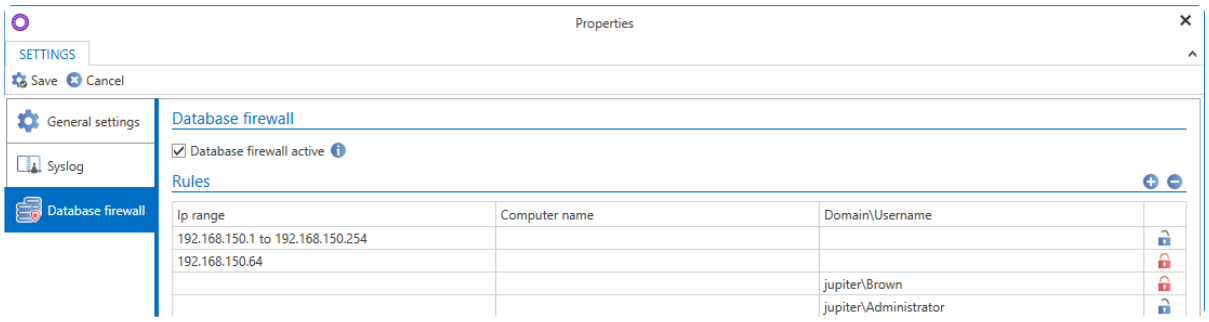
Naturally, the rules can also be combined. It is thus possible e.g that only one defined user can access one database from a certain IP address.

> 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:



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.

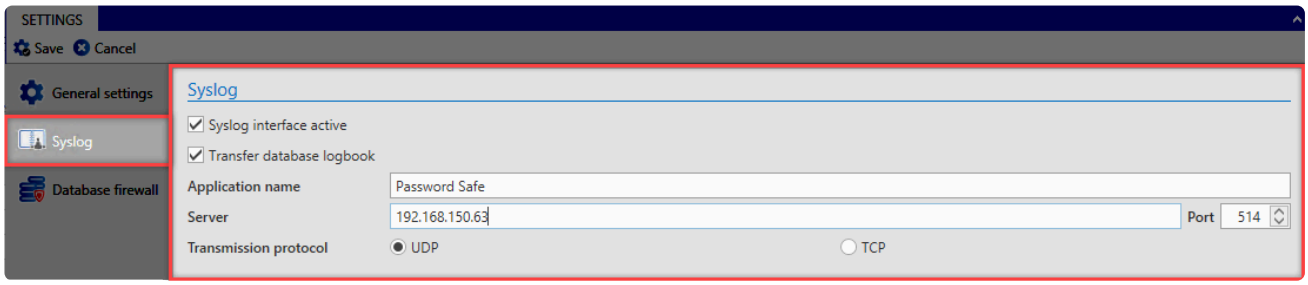
Computer-independent access for a user (Rule 4)

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.



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.

Datenbankeinstellungen

Zum Öffnen der Einstellungen einer Datenbank selektieren Sie diese und klicken in der Ribbon auf “Einstellungen”. Alternativ können Sie mit der rechten Maustaste das Kontextmenü öfnnen und dort auf “Eigenschaften” klicken. Im nächsten Schritt werden Sie aufgefordert, Ihr Admin-Passwort einzugeben. Danach öffnet sich ein Fenster mit den Einstellungen.

Einstellungen

Folgende Einstellungen können Sie jetzt vornehmen:

- Authentifizierung
- **Multifaktor-Authentifizierung**
- **Sitzungs-Timeout**
- PKSC #11/ HSM
- Automatische Bereinigung
- SAML-Konfiguration
- Löschen von Benutzern
- Weitere Optionen

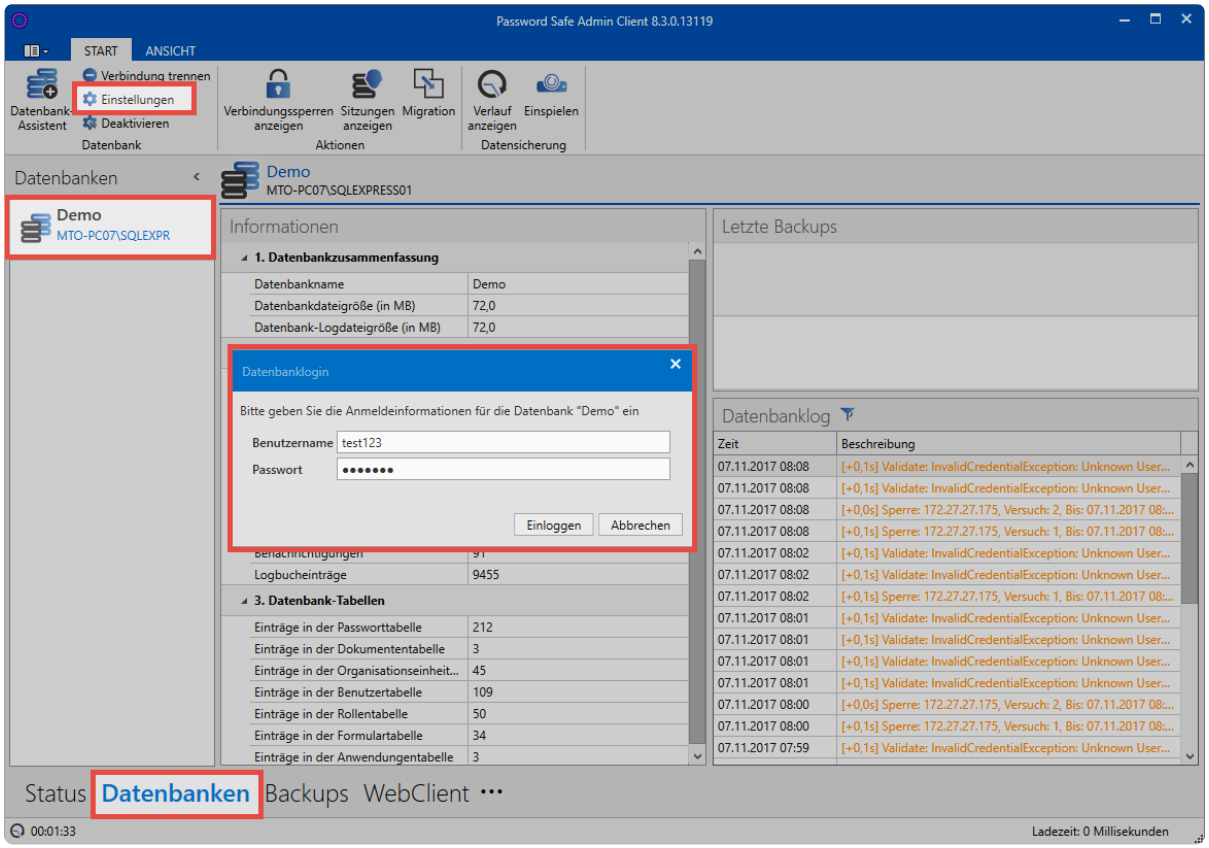
Multifaktor-Authentifizierung

Was ist Multifaktor-Authentifizierung?

Über die Multifaktor-Authentifizierung wird die Anmeldung am Password Safe durch einen weiteren Faktor abgesichert. Die eigentliche Einrichtung findet im Client statt. Die konfigurierten en können anschließend von jedem Benutzer verwendet werden

Aktivierung verschiedener Faktoren

Wählen Sie im Modul **Datenbanken** eine Datenbank aus und öffnen deren Einstellungen über die Ribbon..



In den Einstellungen legen Sie fest, welche zweiten Faktoren verwenden werden können.

> Sofern Sie für PKI Zertifikate ohne KeyUsageFlag “Verschlüsselung (Encipherment)” verwenden wollen, deaktivieren Sie die entsprechende Checkbox.

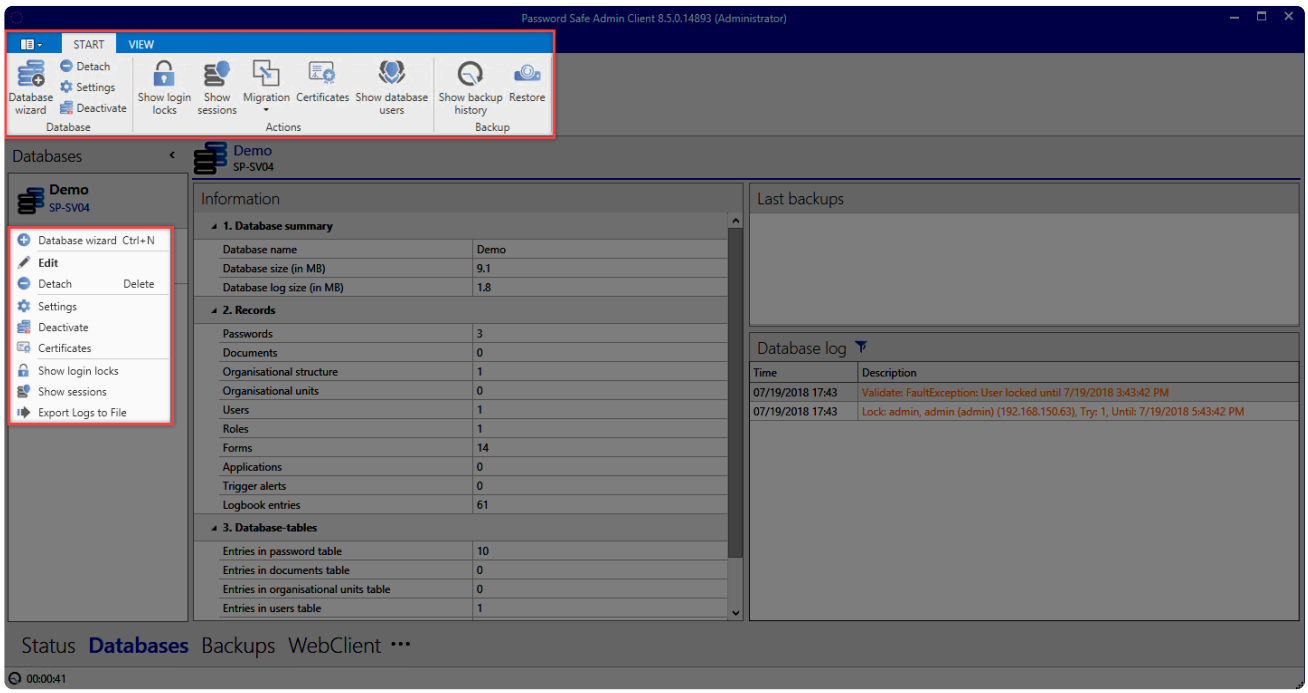
Sitzungs-Timeout

Hier können Sie individuell für die einzelnen Clients einstellen, wann eine inaktive Verbindung zum Anwendungsserver automatisch beendet wird. Wählen Sie dazu im Dropdown die gewünschte Zeitspanne aus und Speichern die Einstellung mittels klick auf “Speichern

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.



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

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:

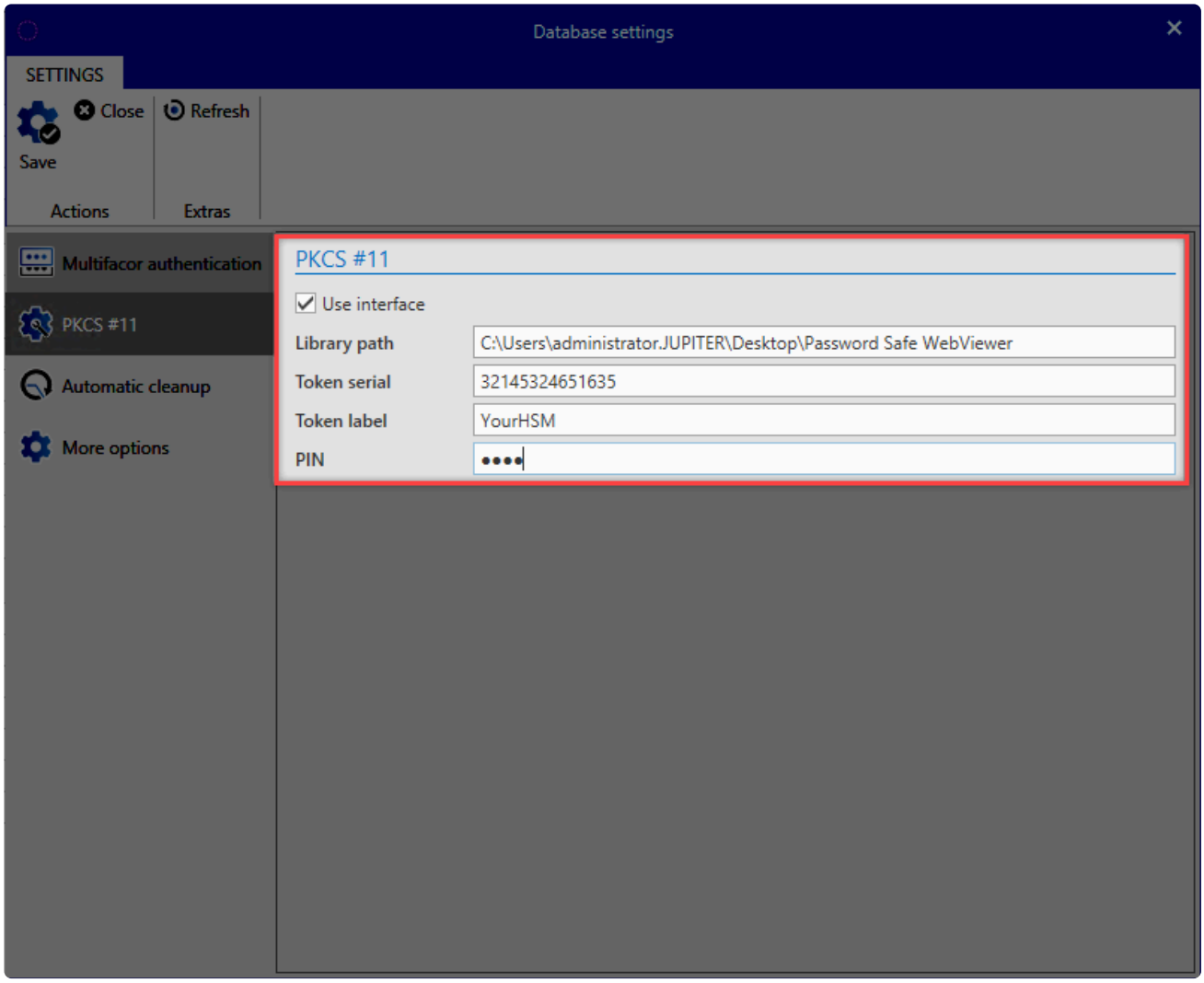
- An executable HSM has to be available.
- The PKCS # 11 drivers have to be installed on the application server.
- The Enterprise Plus Edition has to be licensed.
- The device is set up via the Administrator database on the AdminClient

! 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.

h2. Hardware compatibility

In principle, any HSM should work with the PKCS#11 interface. However, it is recommended to try this out in a test position or a POC beforehand
h2. Installation

The installation is set up on the AdminClient via the database settings



- **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.

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.

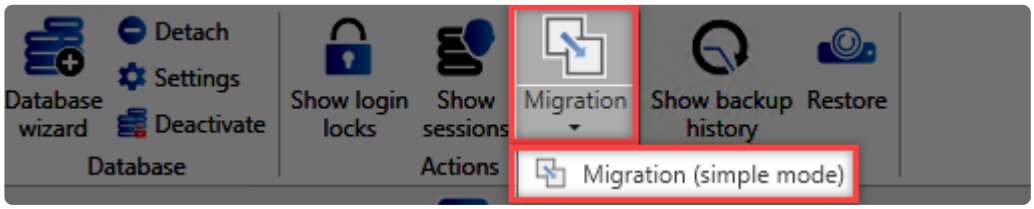
Categorisation during the migration

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)

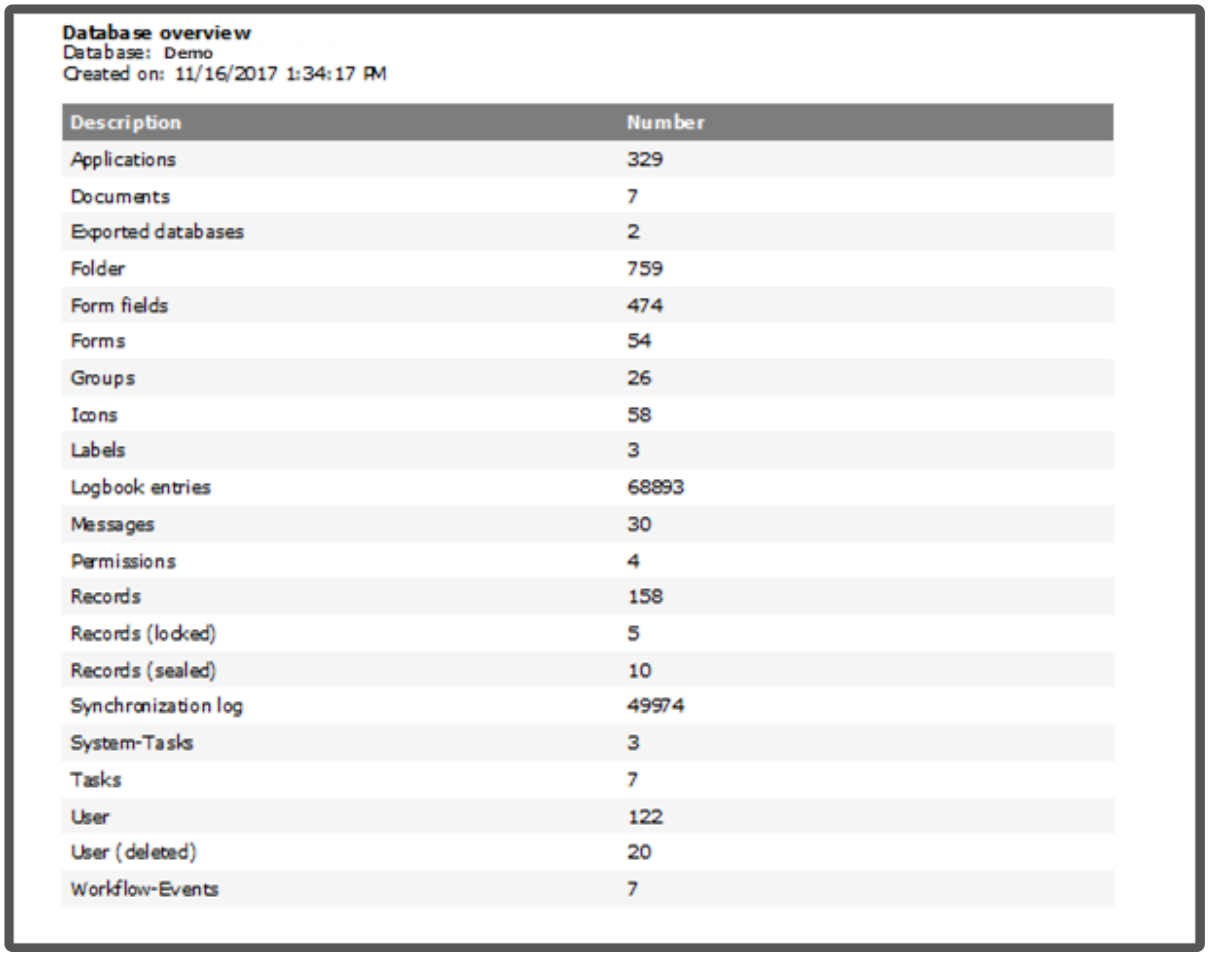
Offline mode and USB sticks

- 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.

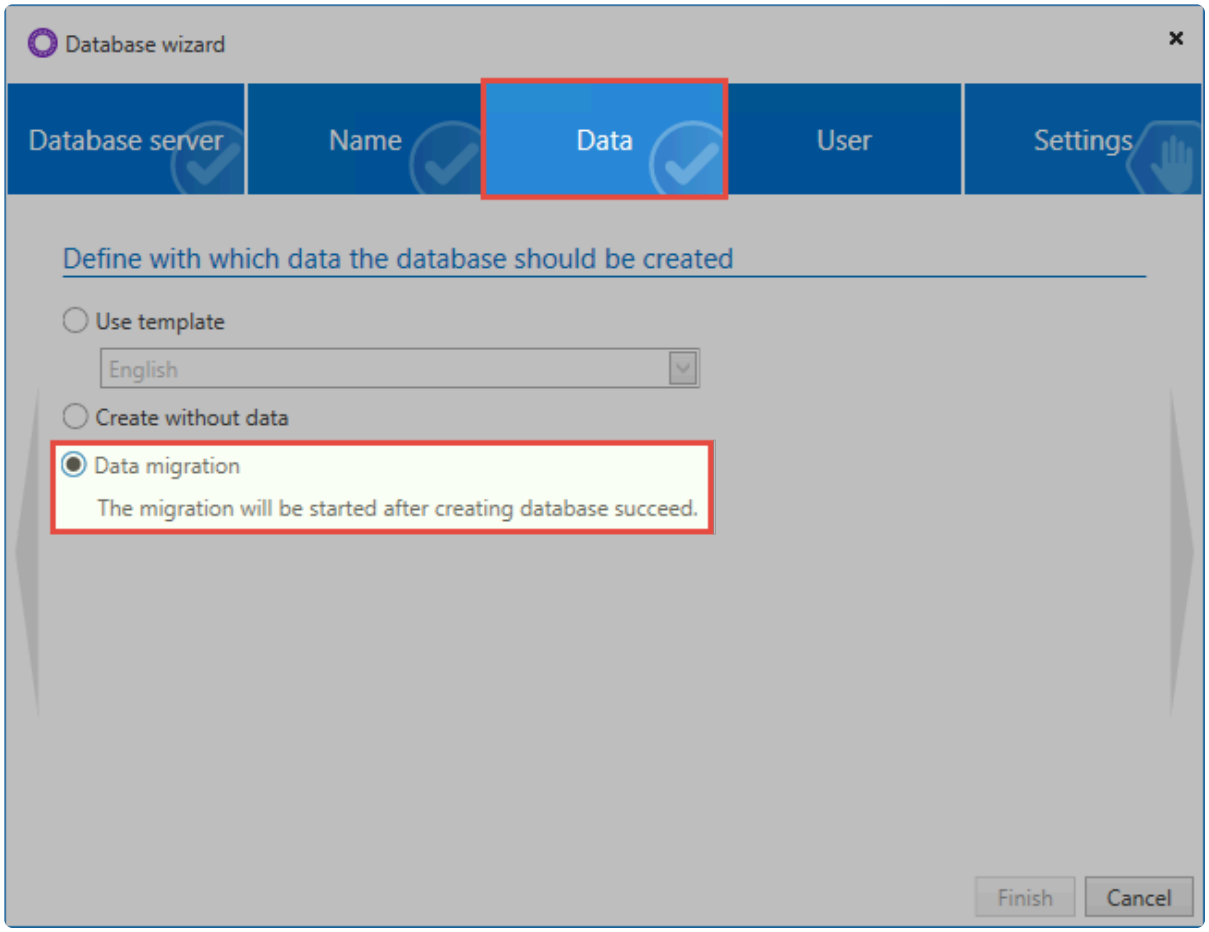
Starting the migration process

What is the migration process?

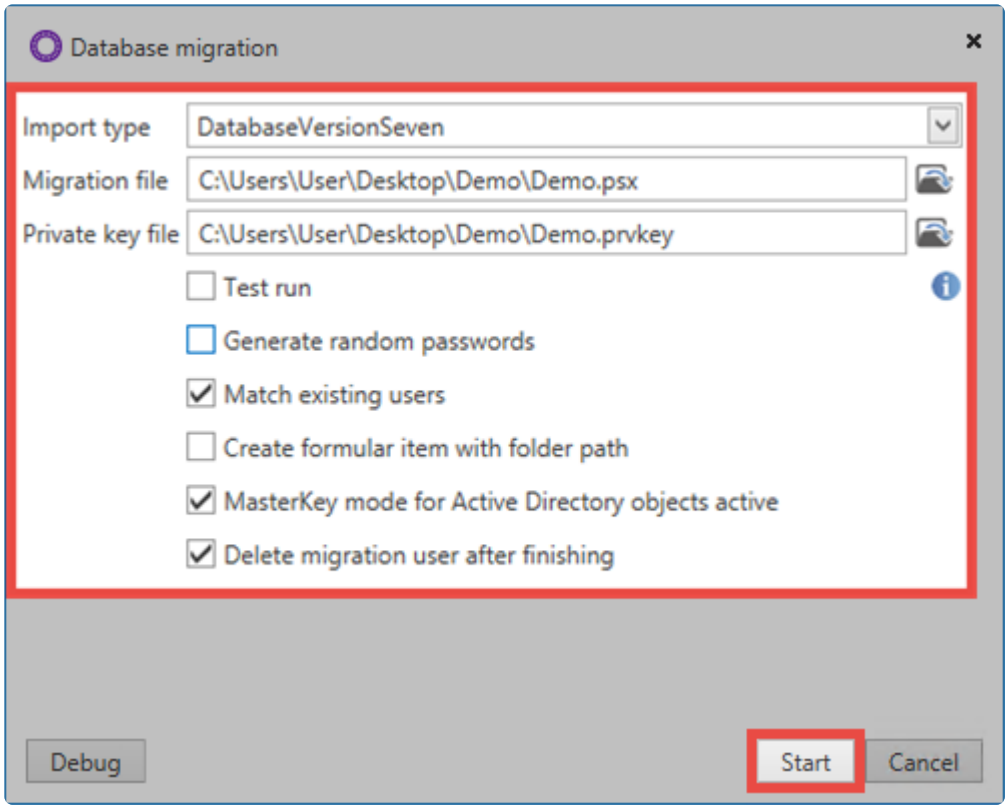
The migration process describes the actual porting process in which all data from a version 7 database is transferred to a new/existing version 8 database. The required amendments to the data set due to the redesign of the authorization concept are also carried out.

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.



After completing the database wizard, you can go directly to the migration wizard.



- 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**.

- It is recommended that the **migration user is deleted**, as this is authorized by the migration to all records in the database! As a rule, this user is no longer required after the migration, since the administrator is taken as the user from the migrated backup and will be 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.

> ! If several databases are to be migrated into one, this must be done with the same migration user. This user may therefore only be deleted during the migration of the last database.

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.

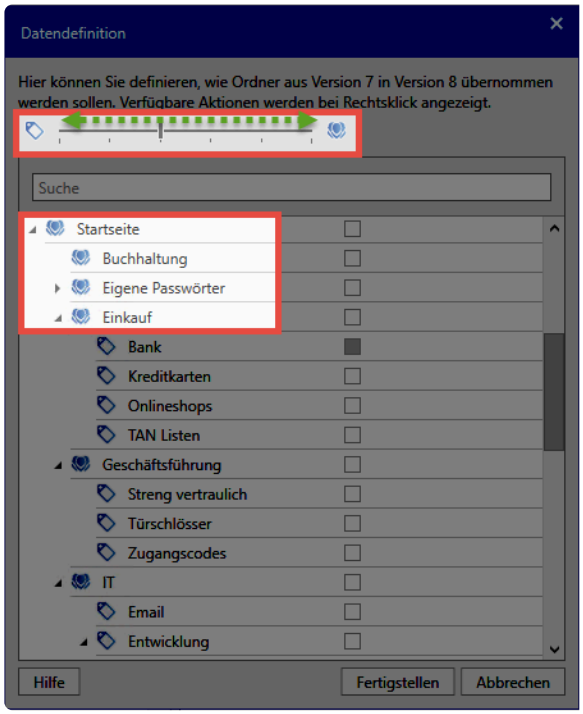
Why are tags and OUs assigned?

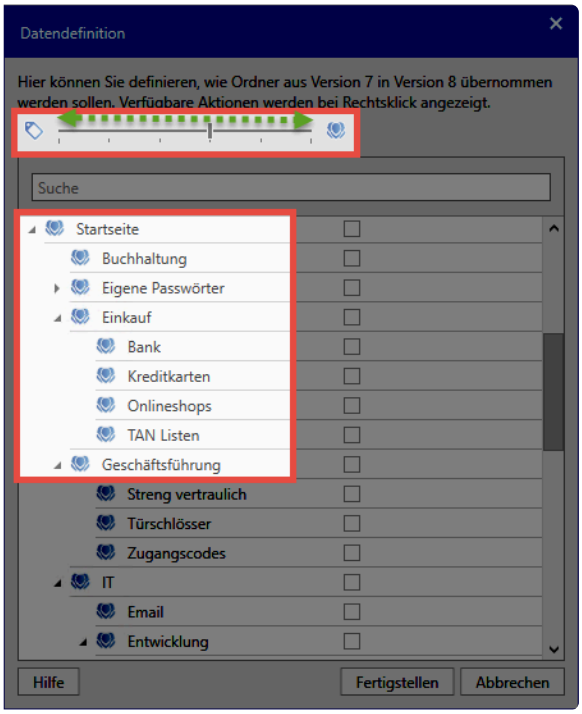
Following the previous step, the folder structure of version 7 is displayed. Due to the already mentioned amendments to the operating concept in version 8, it is now possible to define how the data will be categorised in future. This involves defining whether folders from version 7 are converted into 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.

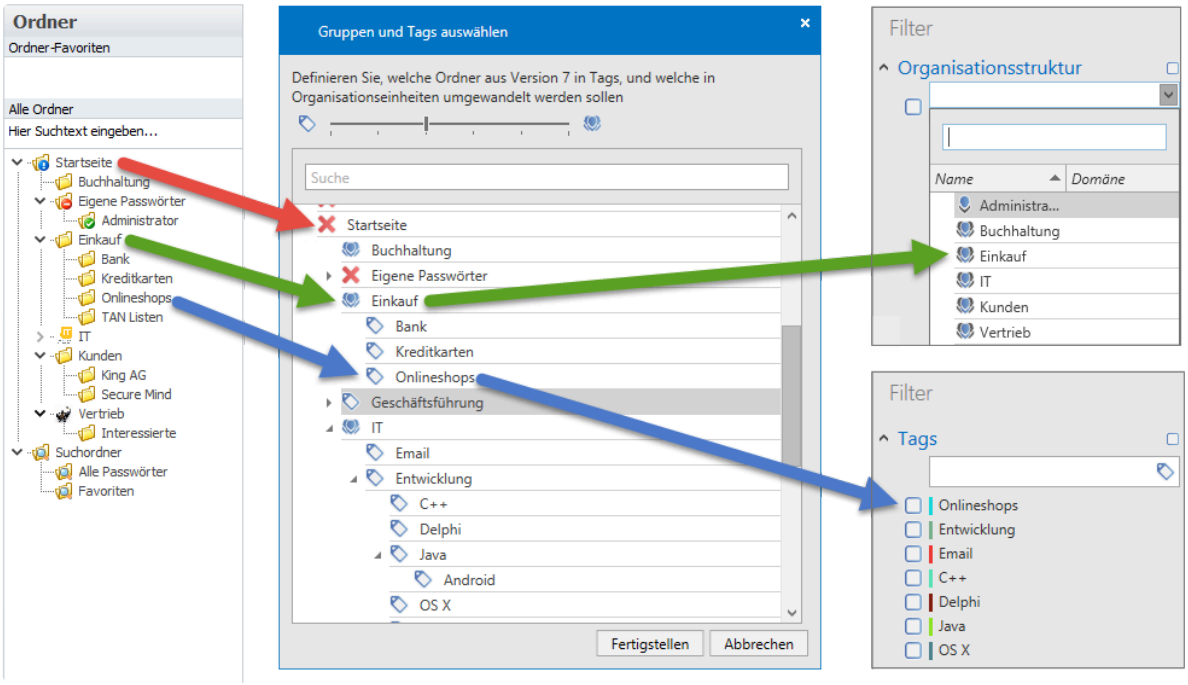




Further options can be opened via the context menu (right mouse button):

- Categorise all sub-objects as organisational units
- Categorise all sub-objects as tags
- Ignore all sub-objects
- Delete all previous markings

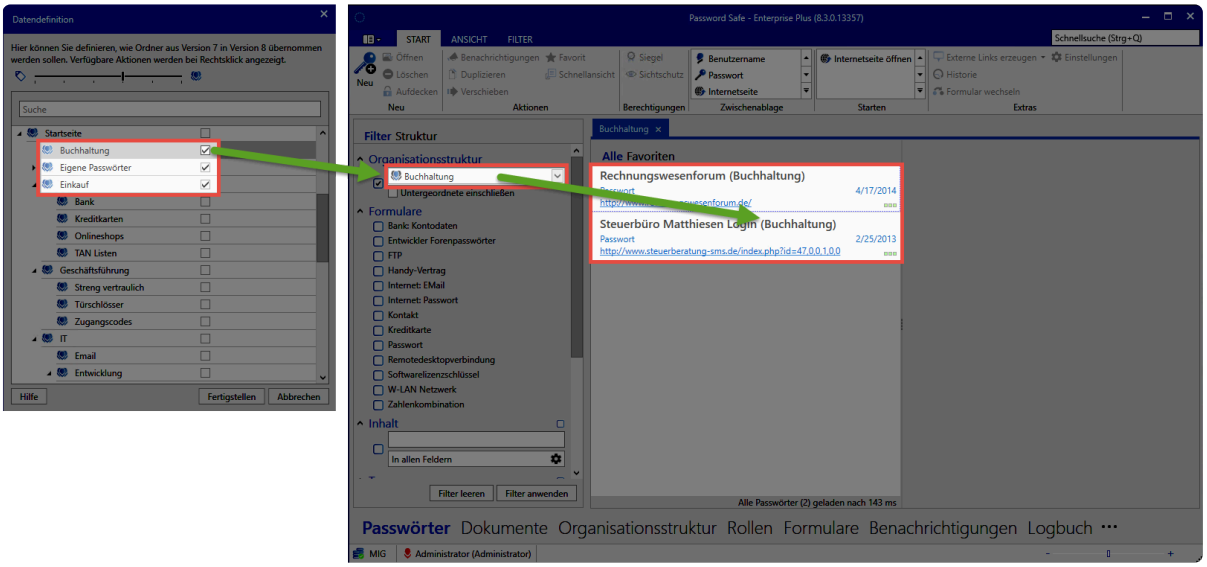
In the following **diagram**, a possible process for assigning the folders to organisational units and tags is illustrated:



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.



This option can be activated for all folders via the context menu.

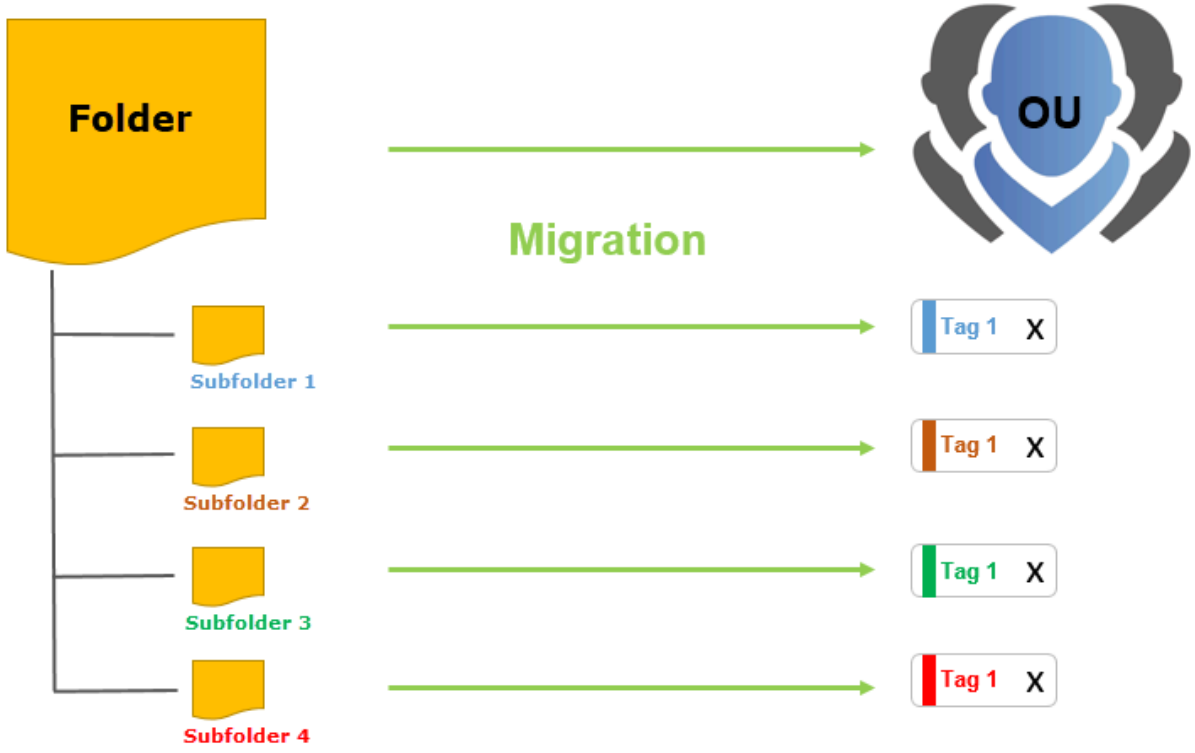
Finishing the migration

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.



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.

> ! In version 7 it was possible to configure a rights template so that no user has the right to access records. This was often used for personal data sets so that they could not be shared. In version 8 you can control the sharing of personal data sets with a user right. However, it is mandatory that at least one user has the right to access each record. For this reason, the rights are adjusted during migration. First of all, it is checked whether someone is authorized to delete the affected data records. If this is the case, these users or roles are also given the Authorization right. If no one is authorized to delete, all set rights are extended by the Authorized Right.

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.

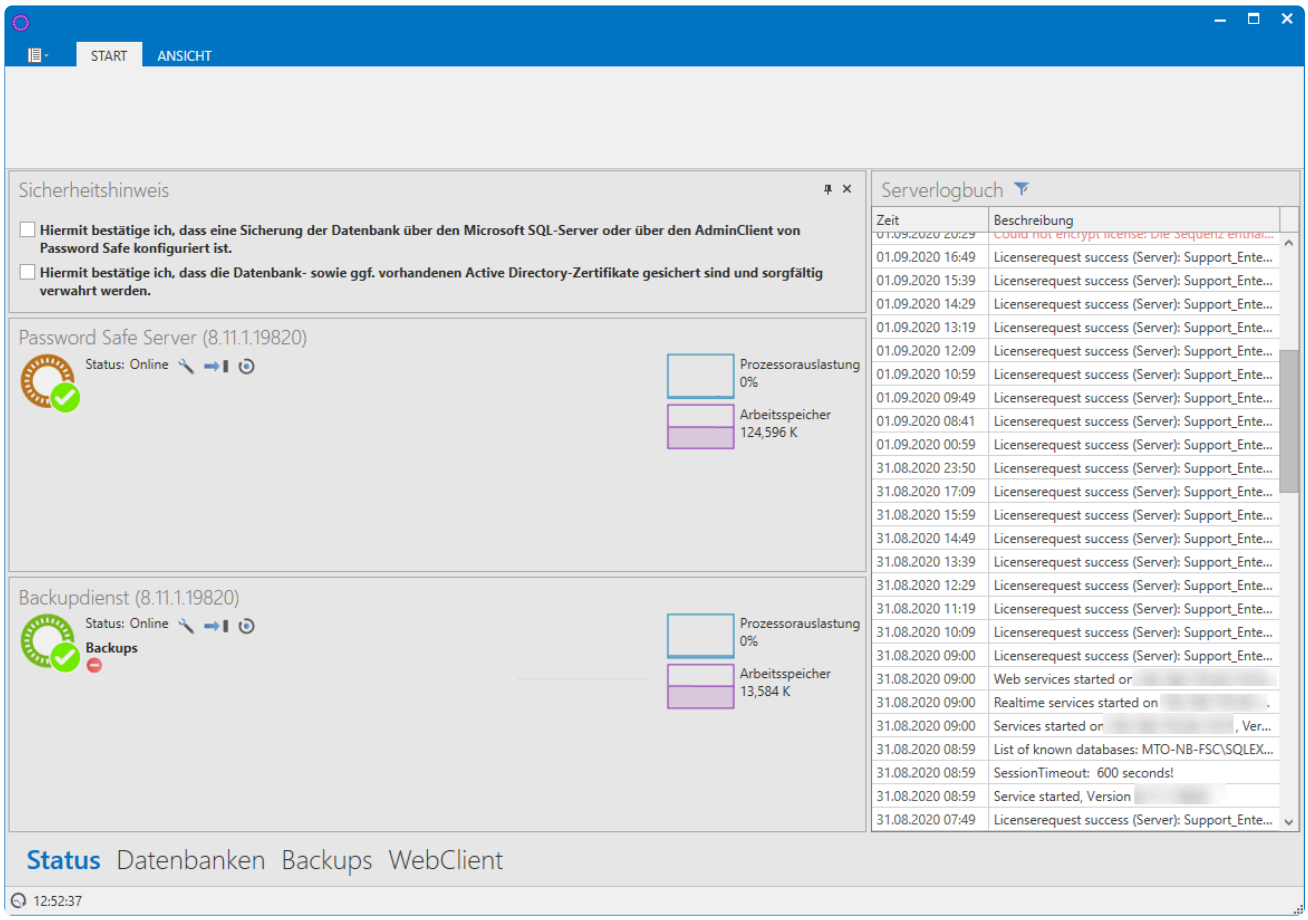
Operation and setup

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 AdminClient. The password is “admin”. This password should be changed directly after login and carefully documented.

Status module



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:

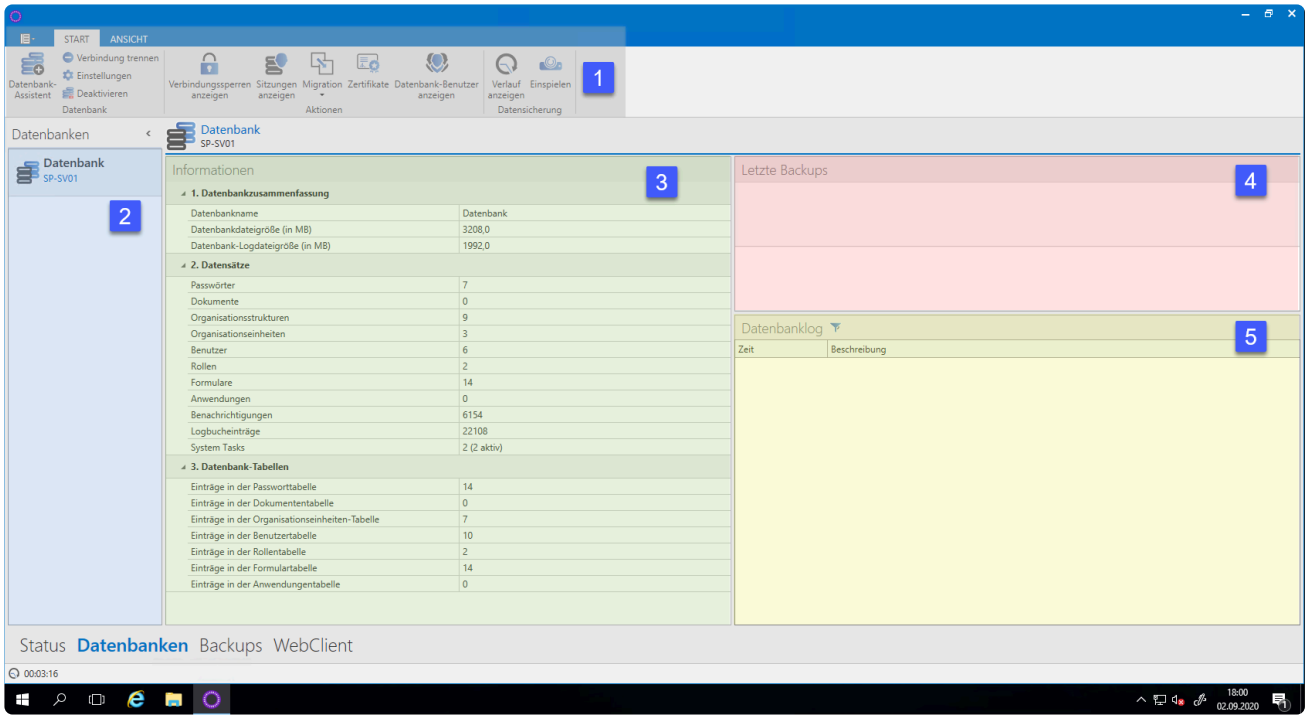
Expected actions	black
Events that require attention	orange
Problems and crashes	red

- 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. 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

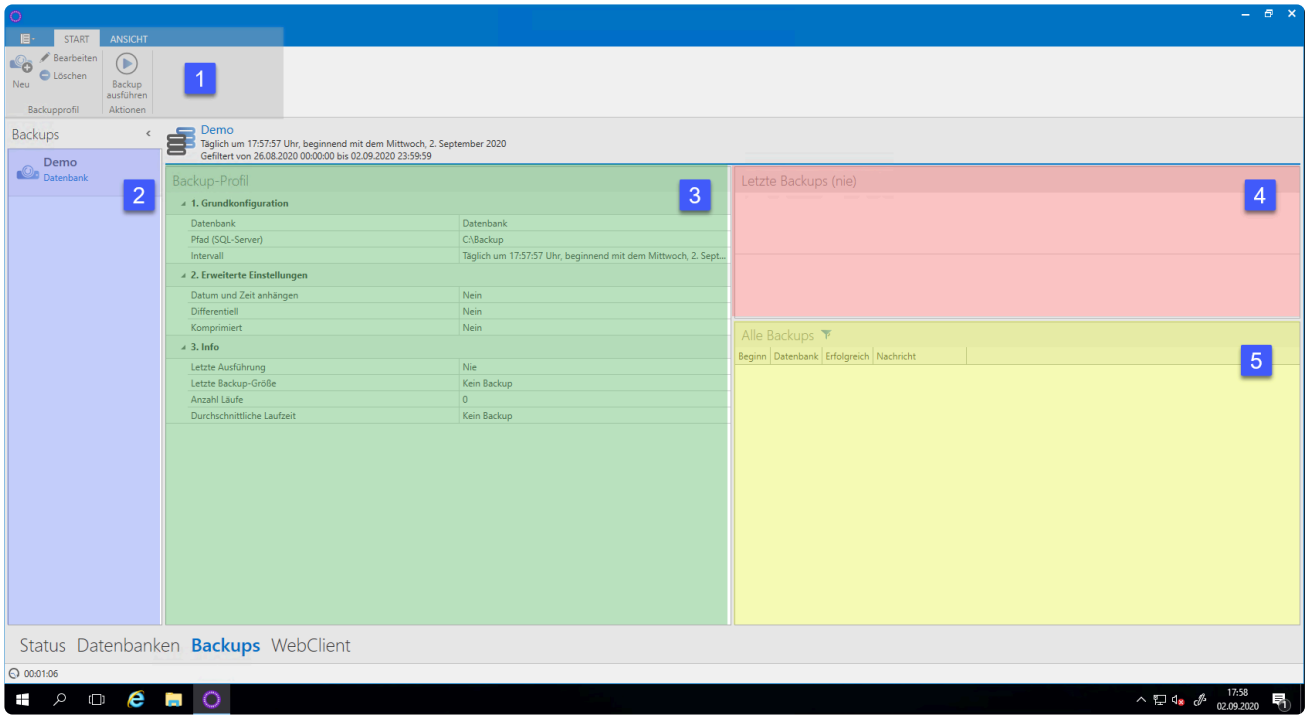
List of recent backups. Can be sorted by date

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.



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.

Main menu

What is the main menu?

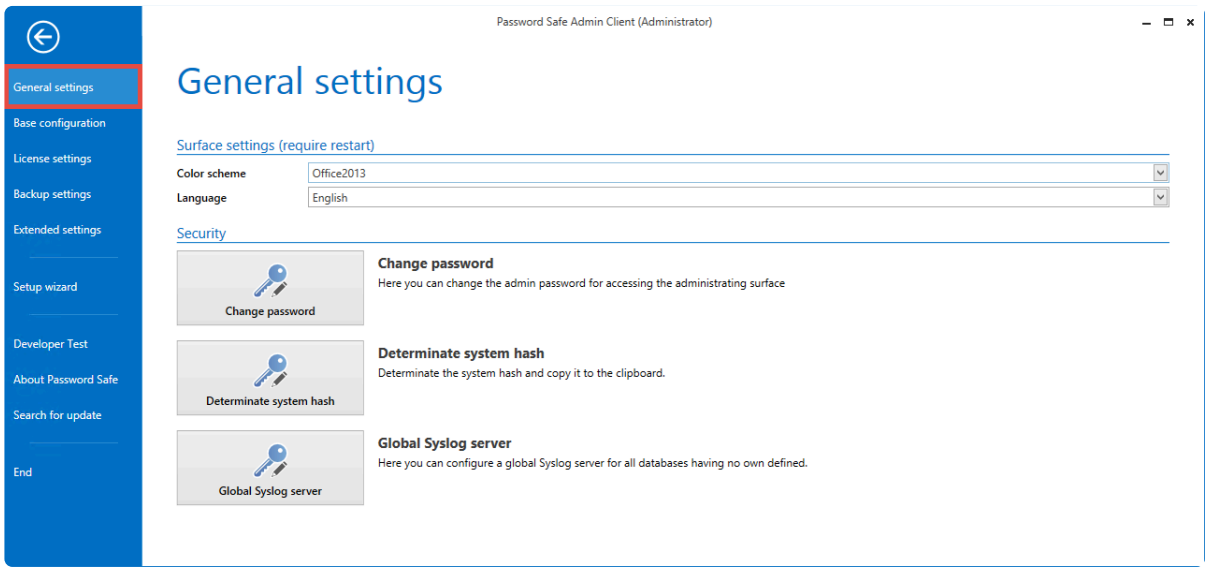
The operation and structure of the Main menu/Backstage menu is the same for the Main menu on the client. This area can be used independently of the currently selected module.

- General settings
- Backup settings
- License Settings
- Advanced settings

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.



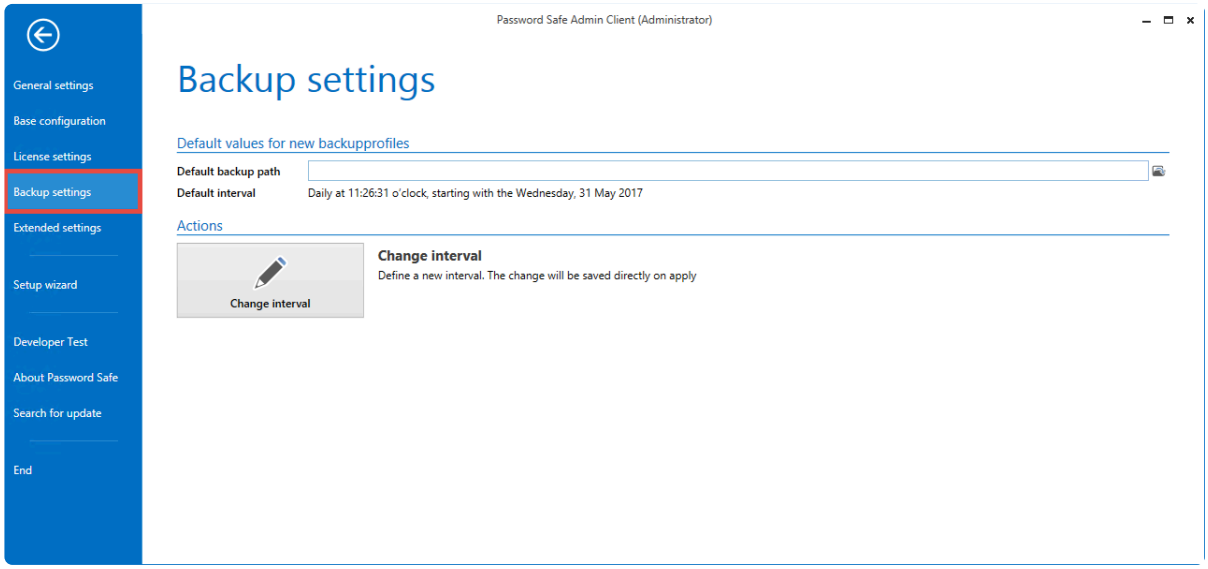
Determining the system hash

This function determines the system hash, and copies it to the clipboard. This hash is used for the offline license.

Backup settings

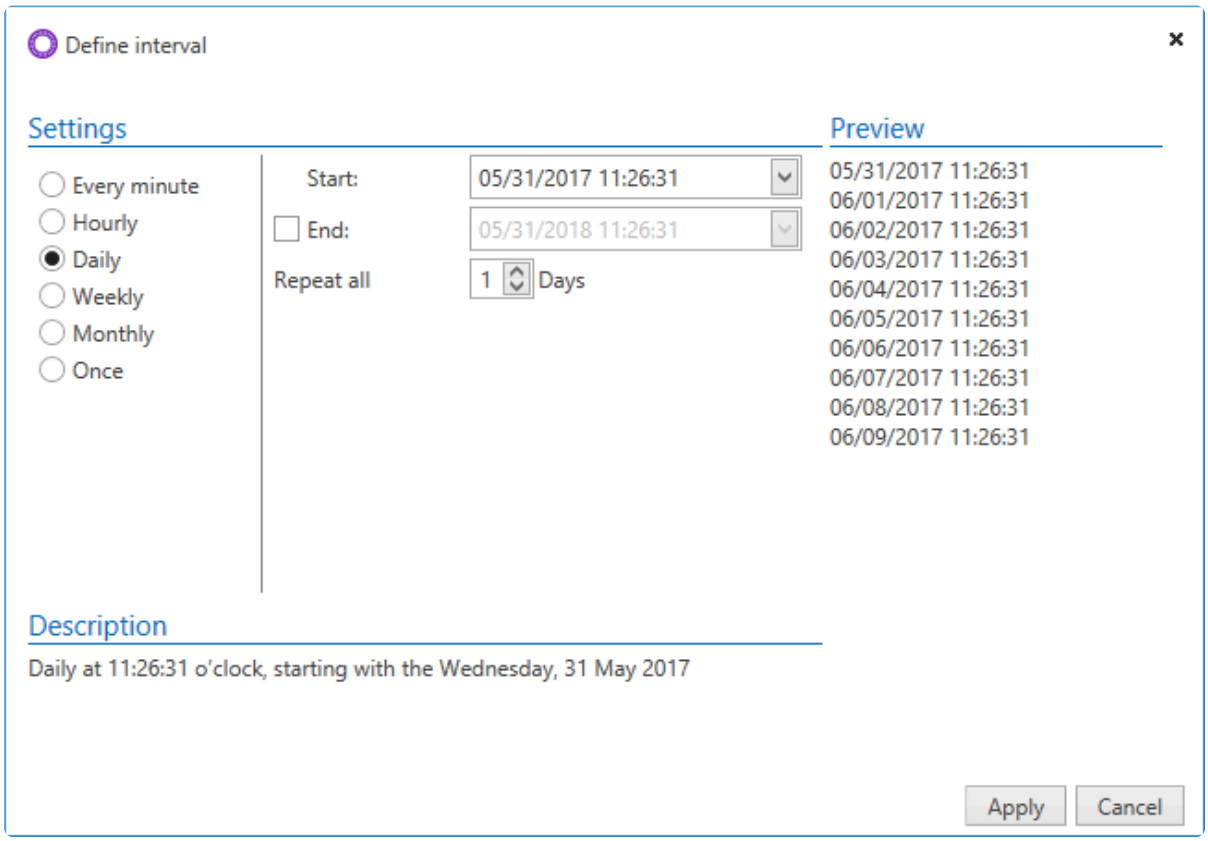
What are backup settings?

Within the backup settings the default values for the execution of backups can be defined.



Interval settings

The interval for backups can be customized as needed. A separate assistant is available for this purpose.



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

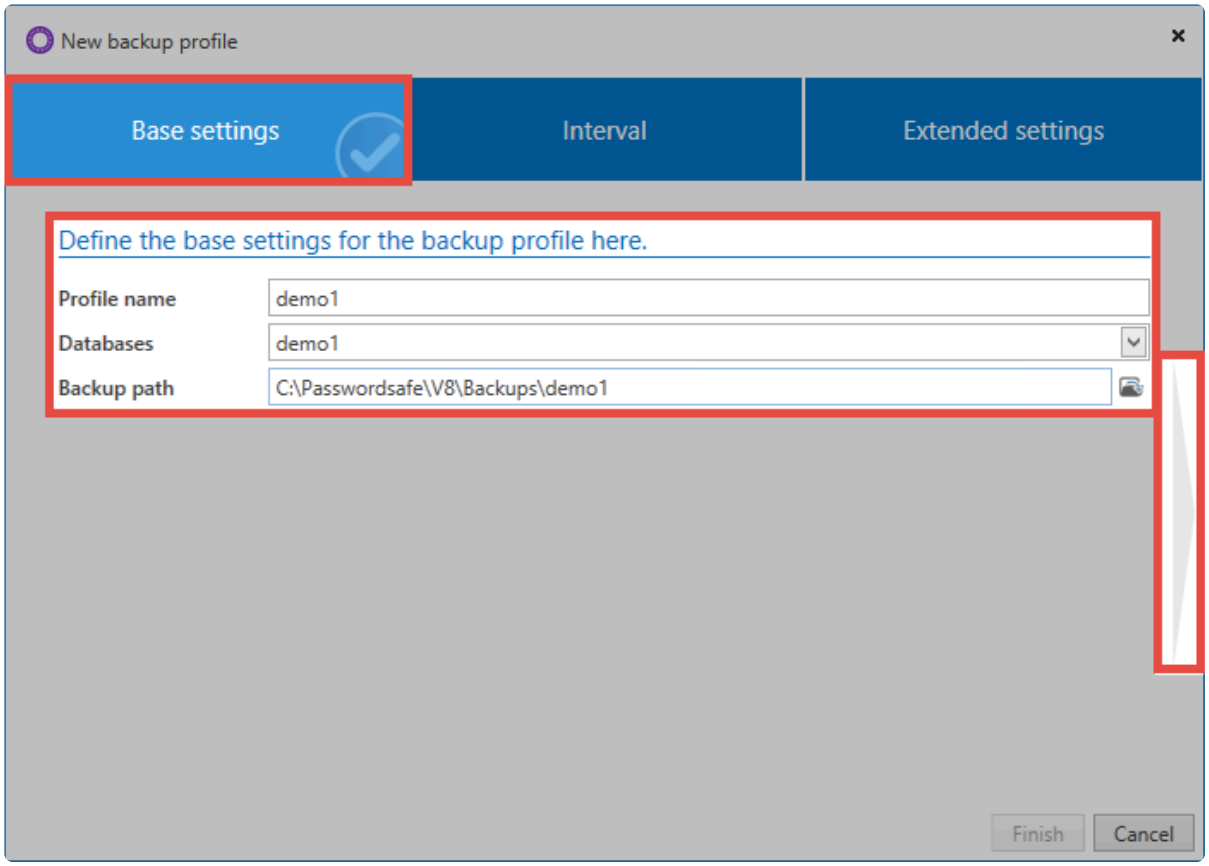
It is recommended that an incremental backup is run every hour. In addition, a full backup should be created once a week.

Managing the backup schedule

Creating a backup schedule

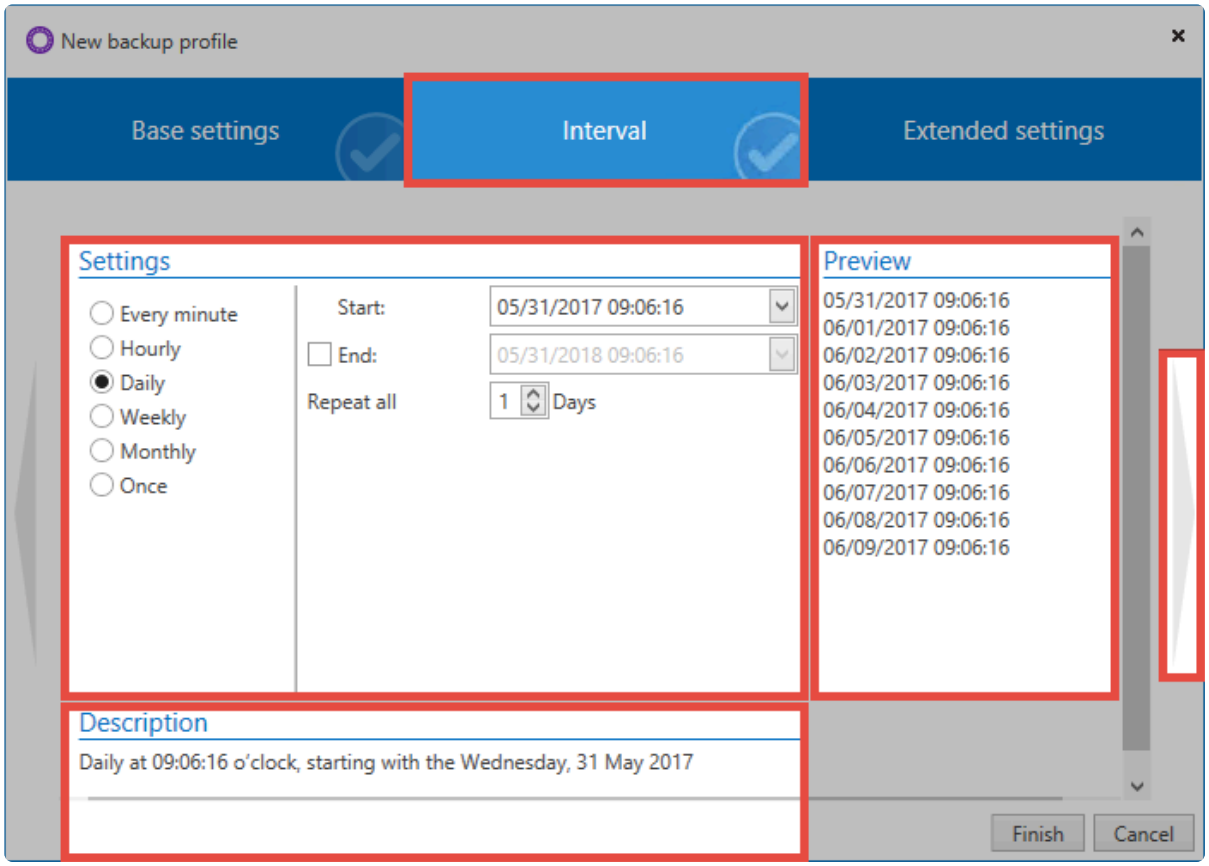
You can create a new schedule via the ribbon. This is facilitated by a wizard. All the information entered under “Backup settings”:#backup-einstellungen will be used by default.

A profile name is entered first. The desired databases are also selected. You also need to specify the directory for the backups.

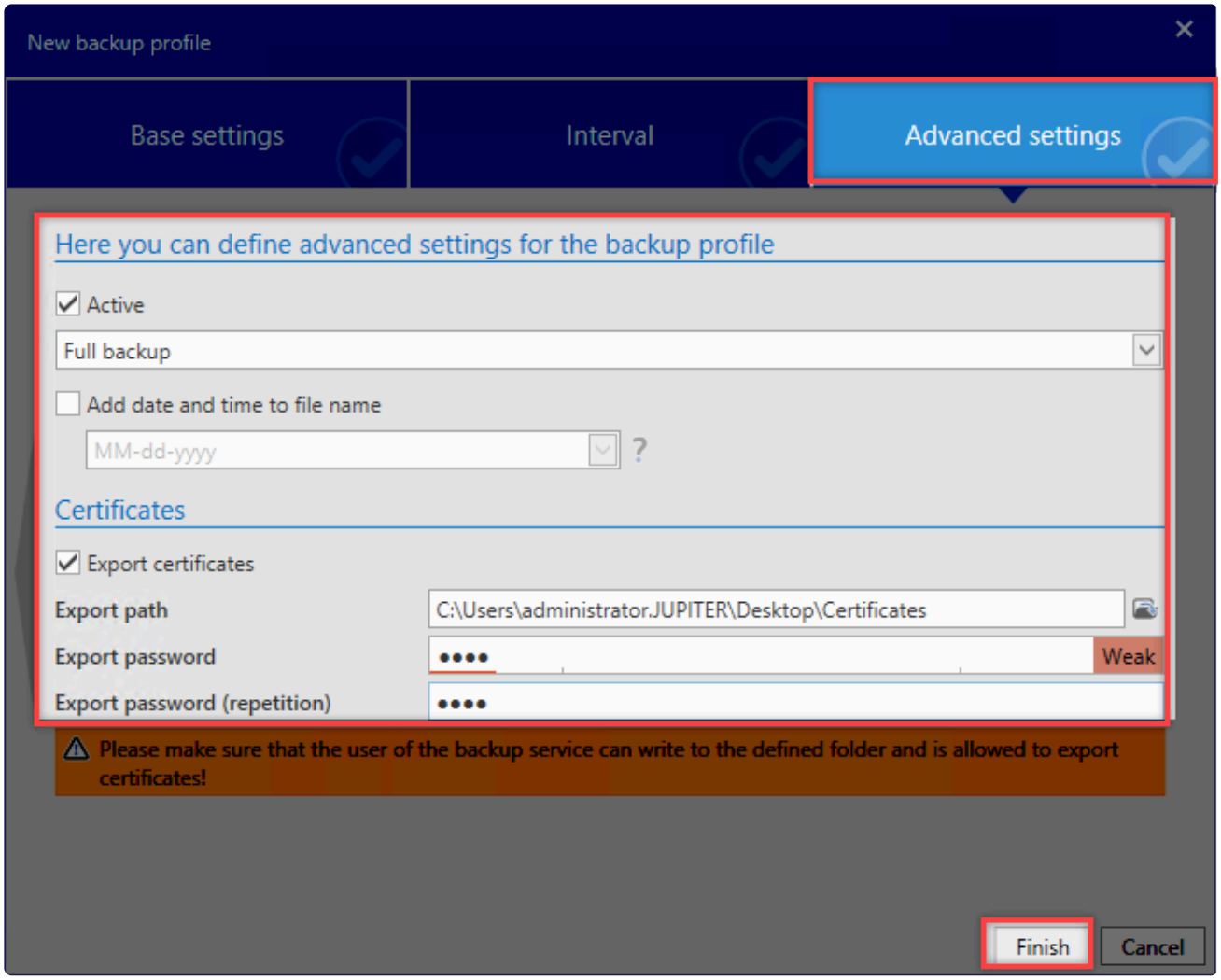


It must be a directory on the SQL server.

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.



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.



Backup run

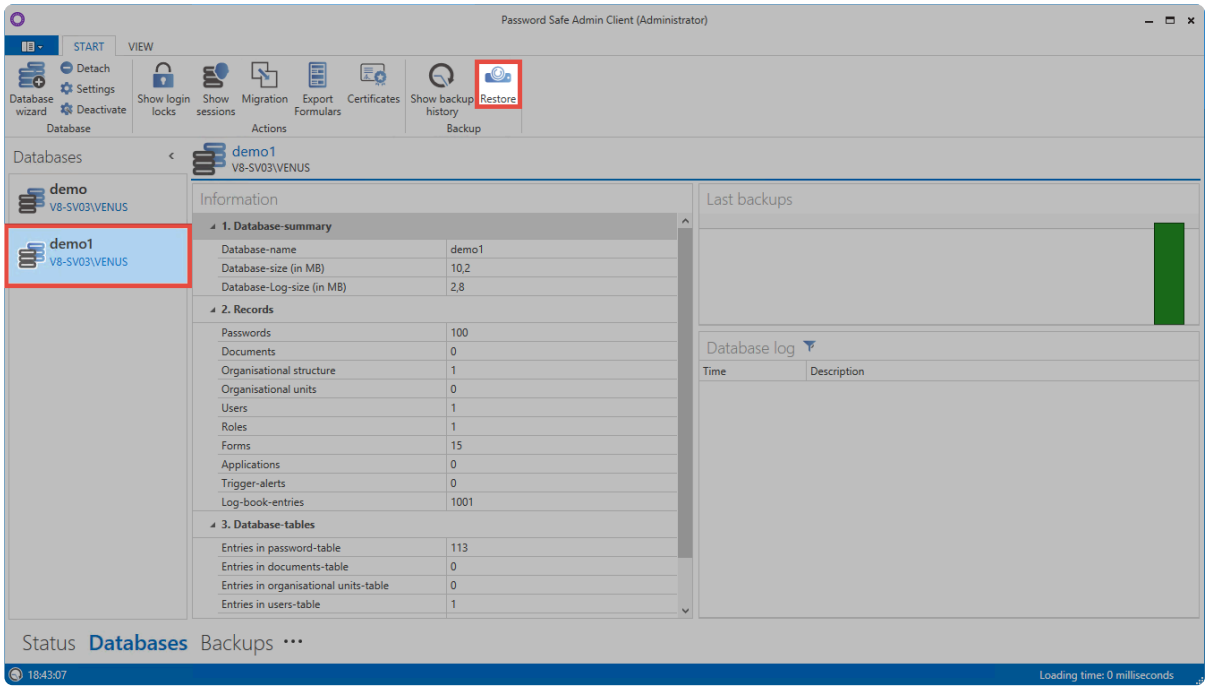
The backups are executed by the SQL server in the background. If an error occurs, this is indicated in “orange” in the backup list. Information about any errors issued by the SQL server is displayed under all backups. A backup will be automatically deactivated if it does not run 5x in a row. This will 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

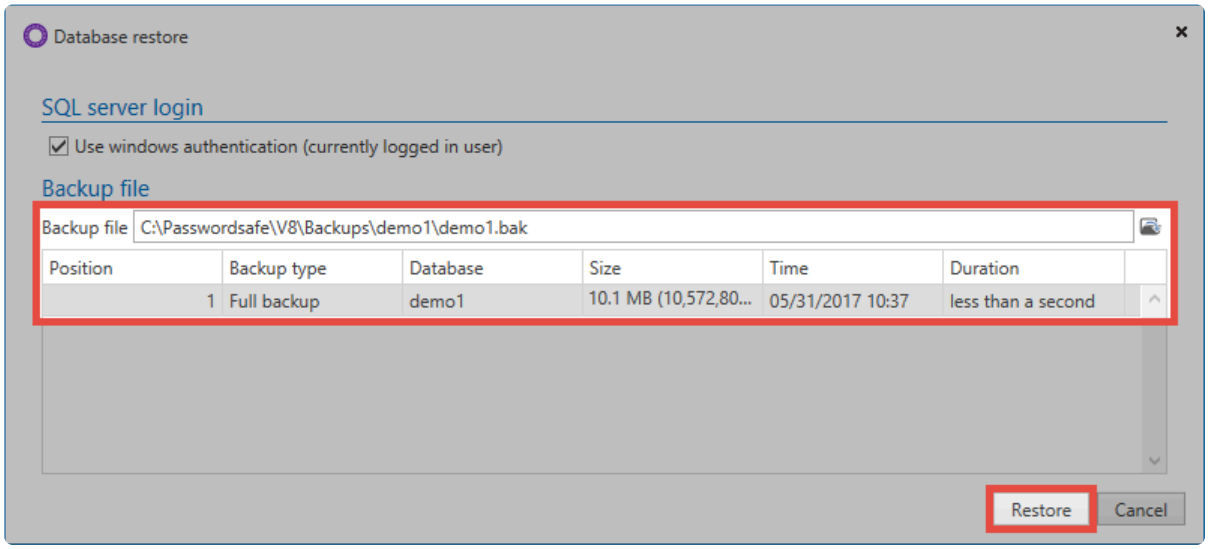
A selected schedule can be deleted via the ribbon. The wizard for a schedule can be called up by double-clicking on it to make any changes. In addition, a backup can be started directly via the ribbon at any time. The backup service must be running for this purpose. You can also display this in the history.

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.



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.



Automated deletion of backups

It is possible to delete backups automatically after a certain period of time. This can be useful if you append date and time to the backups and thus generate new files daily.

- Screenshot

Requirement

It must be ensured that the user who sets up the automated deletion has **sysadmin privileges** on the SQL server.

Furnishing

To be able to use the automatic cleanup, it must be activated first.

- Screenshot

For a proper function of the automatic deletion, the following must be defined:

- the age of the backups which have to be deleted
- the SQL instance
- all paths where the automatic cleanup of the backup files is to be performed.

- Screenshot

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

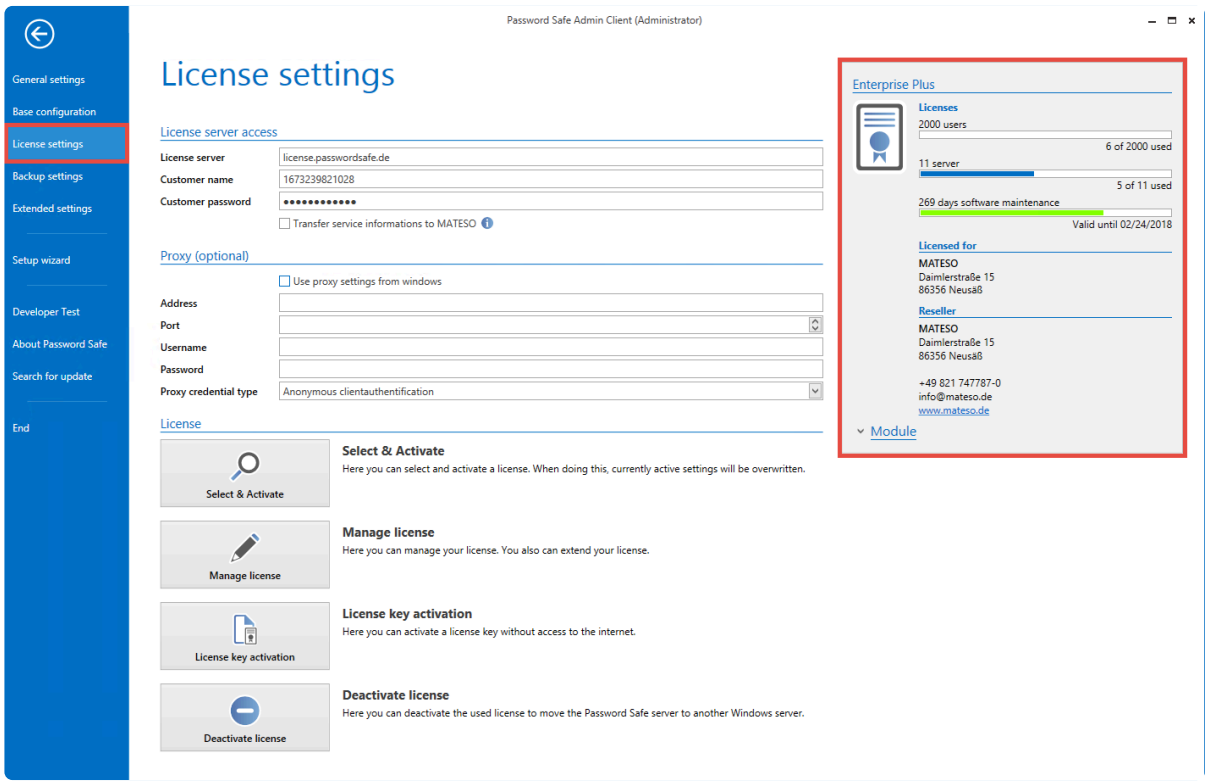
Problem:
As for Scenario 4 but the Active Directory is also not available.

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.



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: 13.74.32.103
- 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.

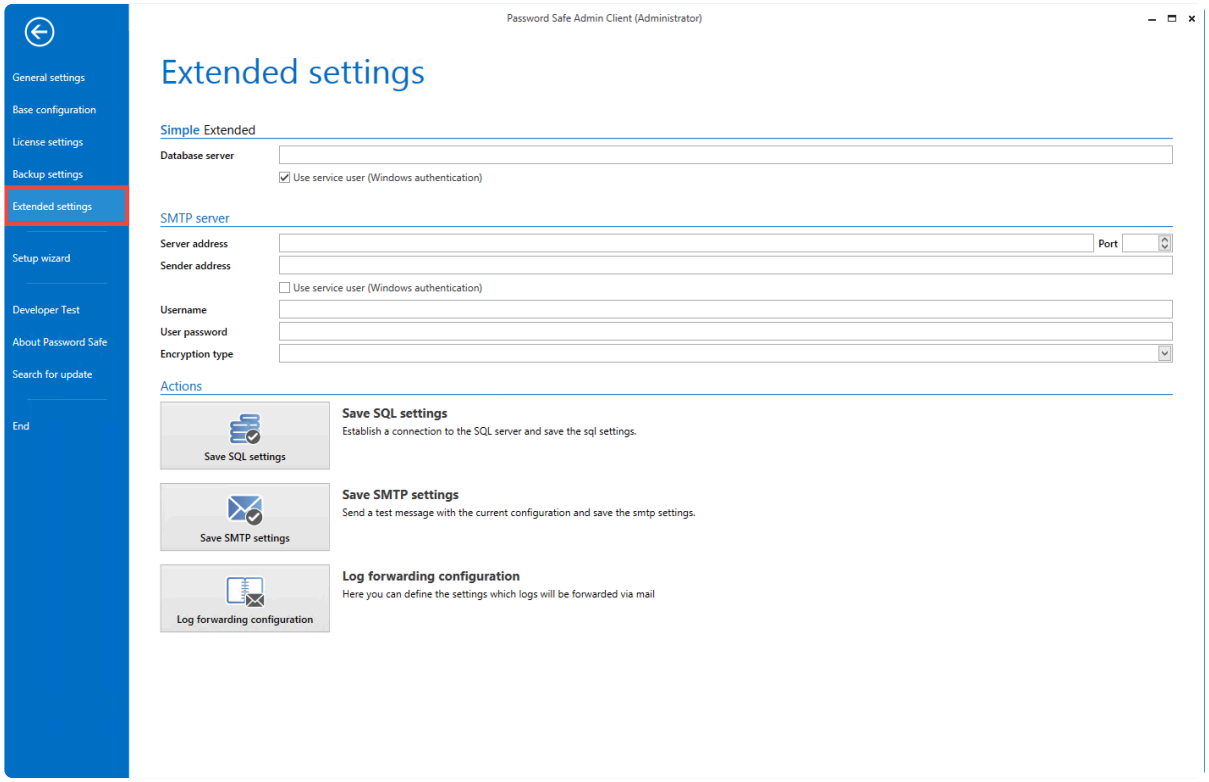
Optionally, you may specify a proxy. By default, the proxy stored in the operating system is used.

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.



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.

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).

> ✻ Only **peer-to-peer transaction replication** is tested. If a different type of replication is used, it should be tested in advance.

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

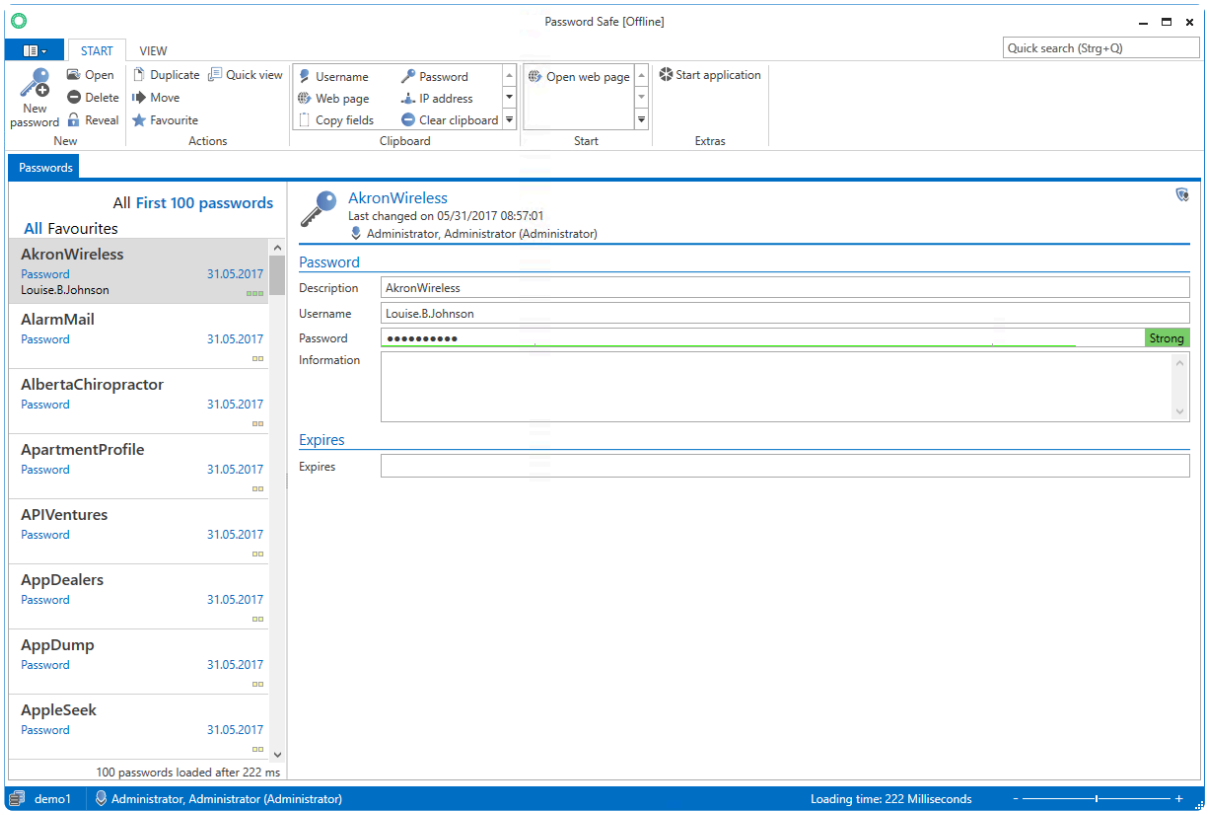
Installation

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



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.

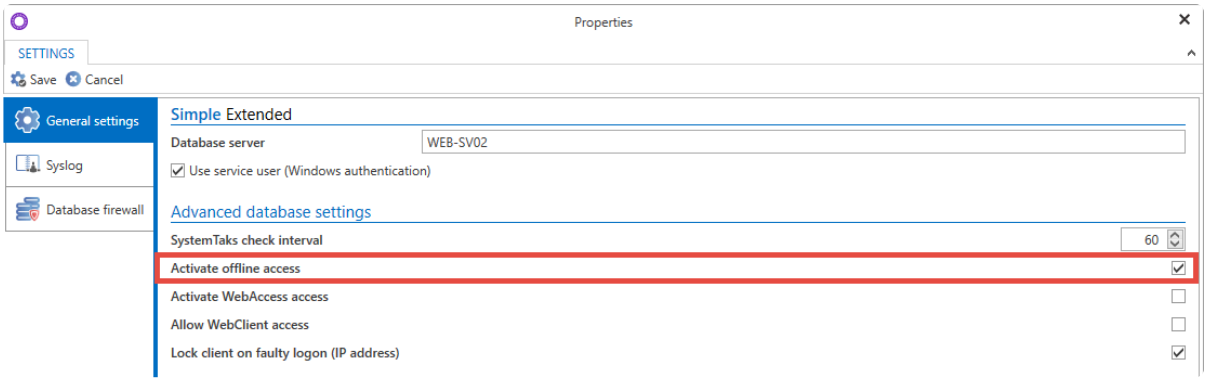
Setup and sync

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

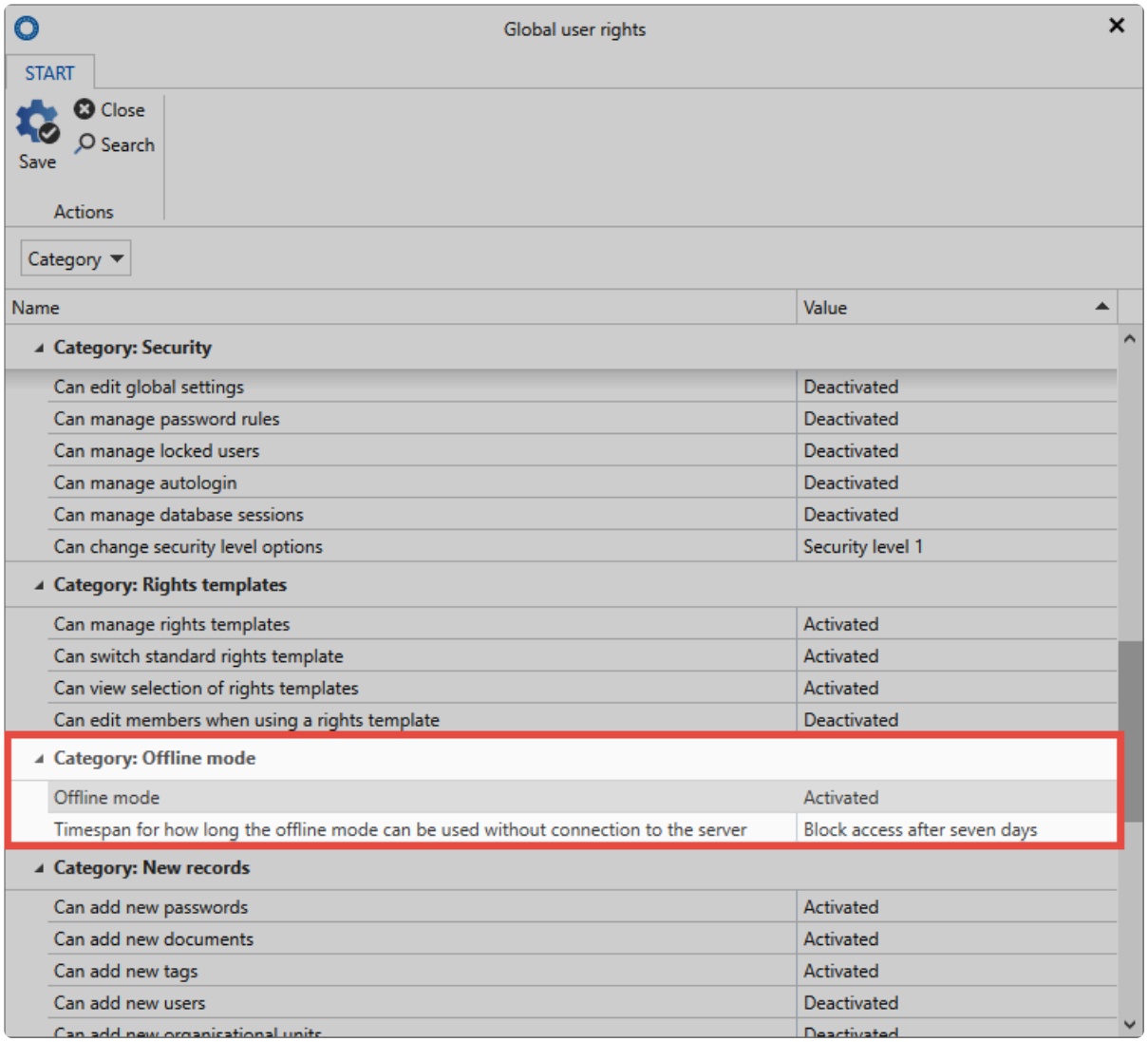
To set up offline databases, this option must be activated in the AdminClient first. This process is carried out separately for each database in the database view in the AdminClient in the “General settings” (right click on the database). This is also possible to do when the database is initially created.



You will find further information on this subject in the sections: Creating databases and Managing databases

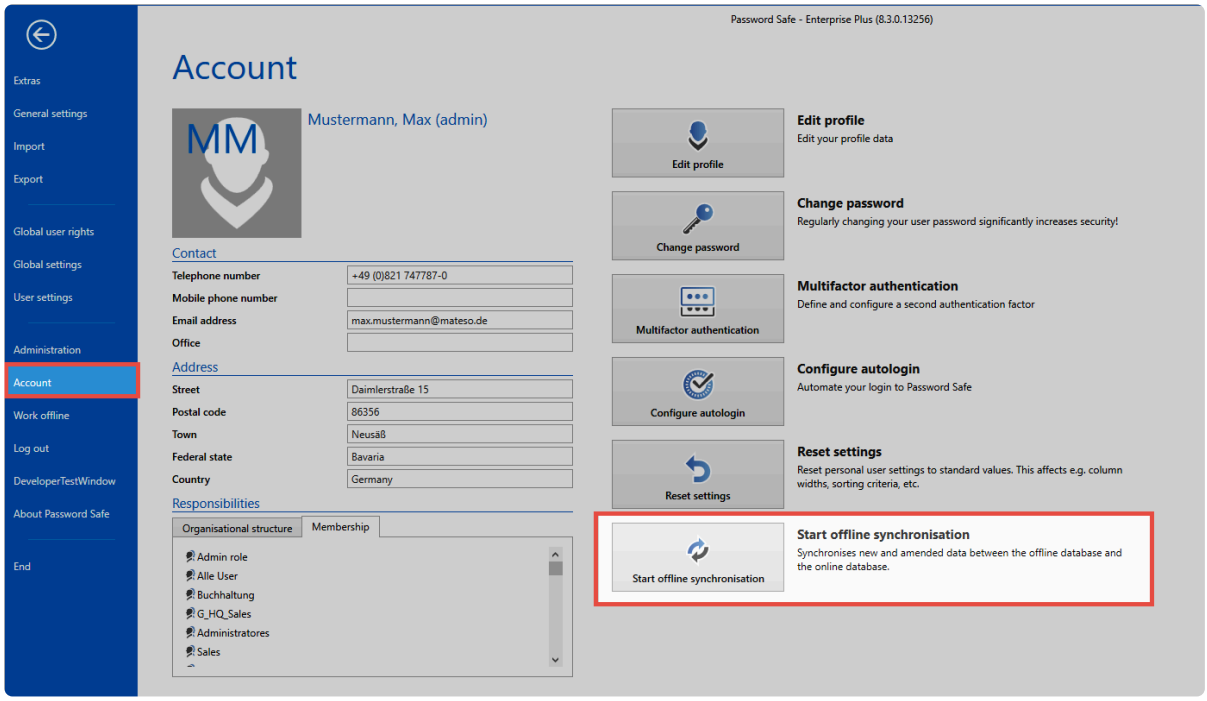
User rights

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.



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.



> The offline databases are stored locally under the following path: %appdata%\MATESO\Password Safe and Repository Client\OfflineDB

An offline database must be created per user and client for each online database. This makes it possible to use several offline databases with an offline client.

Synchronization

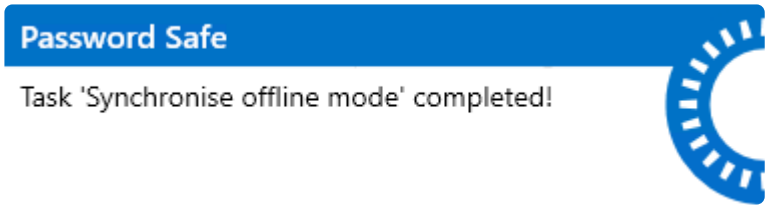
In order to keep the data always consistent, the offline database must be synchronized regularly. Synchronization is automatically performed by the client in the background. The interval can be freely configured in the settings. The synchronization is completed every 30 minutes by default. When creating 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:

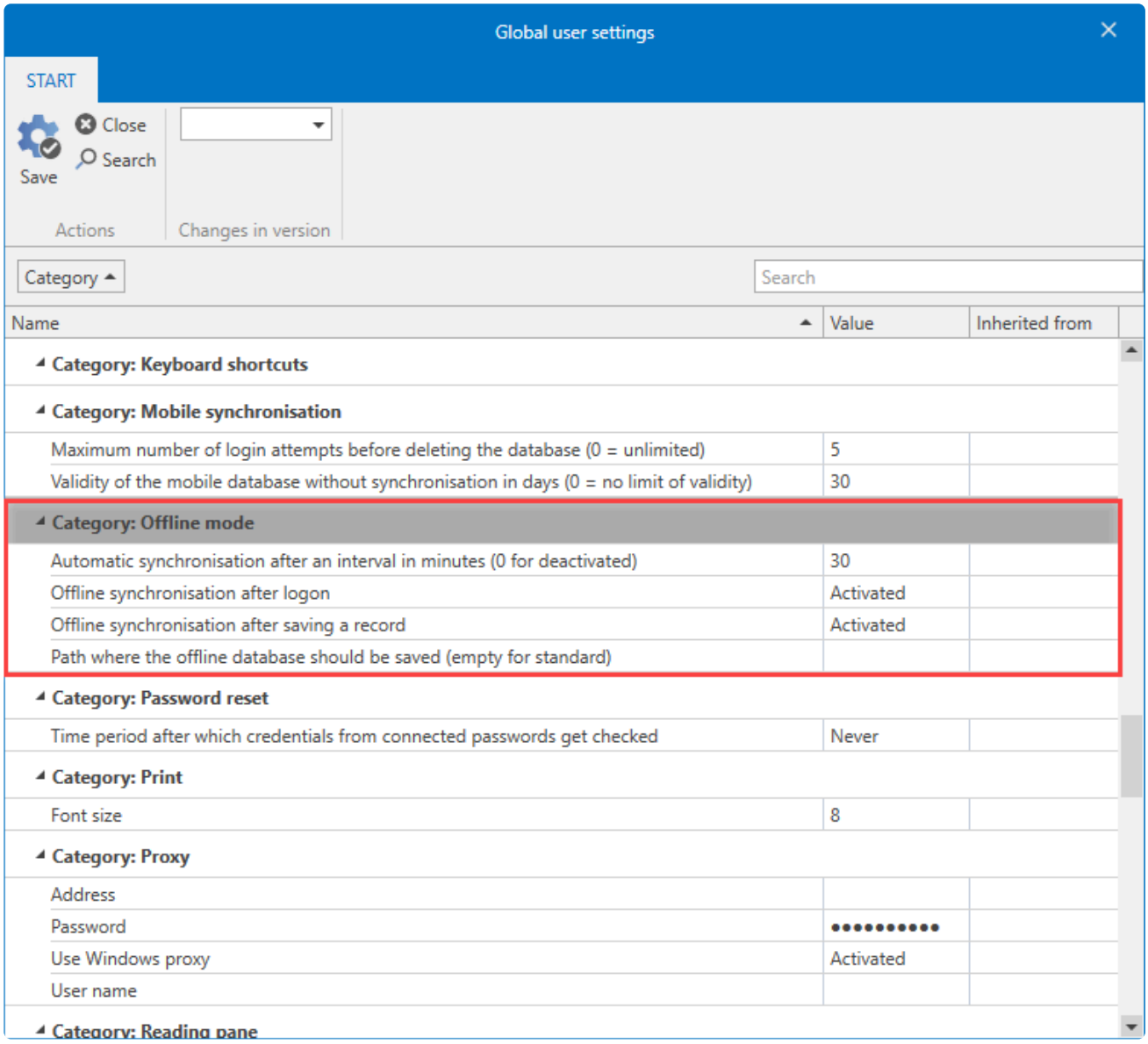




As soon as the synchronization is completed, this is indicated by a hint.



Relevant settings



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!
- **Offline synchronization after login**: If this option is active, the offline database is synchronized after each restart of the client.
- **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. Otherwise, the storage location for the offline database can be entered directly.

How-to’s

In order to make using Password Safe easier, various “How-to’s” on frequently raised topics will appear here. They describe solutions to certain tasks and requirements. The How-to’s are mainly targeted at the end user. However, administrators are also sure to find valuable information here.

The series of instructions will be constantly expanded in future. The following How-to’s are currently available:

- Automatically receiving the WebViewer via e-mail
- Changing a SSL connection certificate

Changing an SSL connection certificate

Specifications

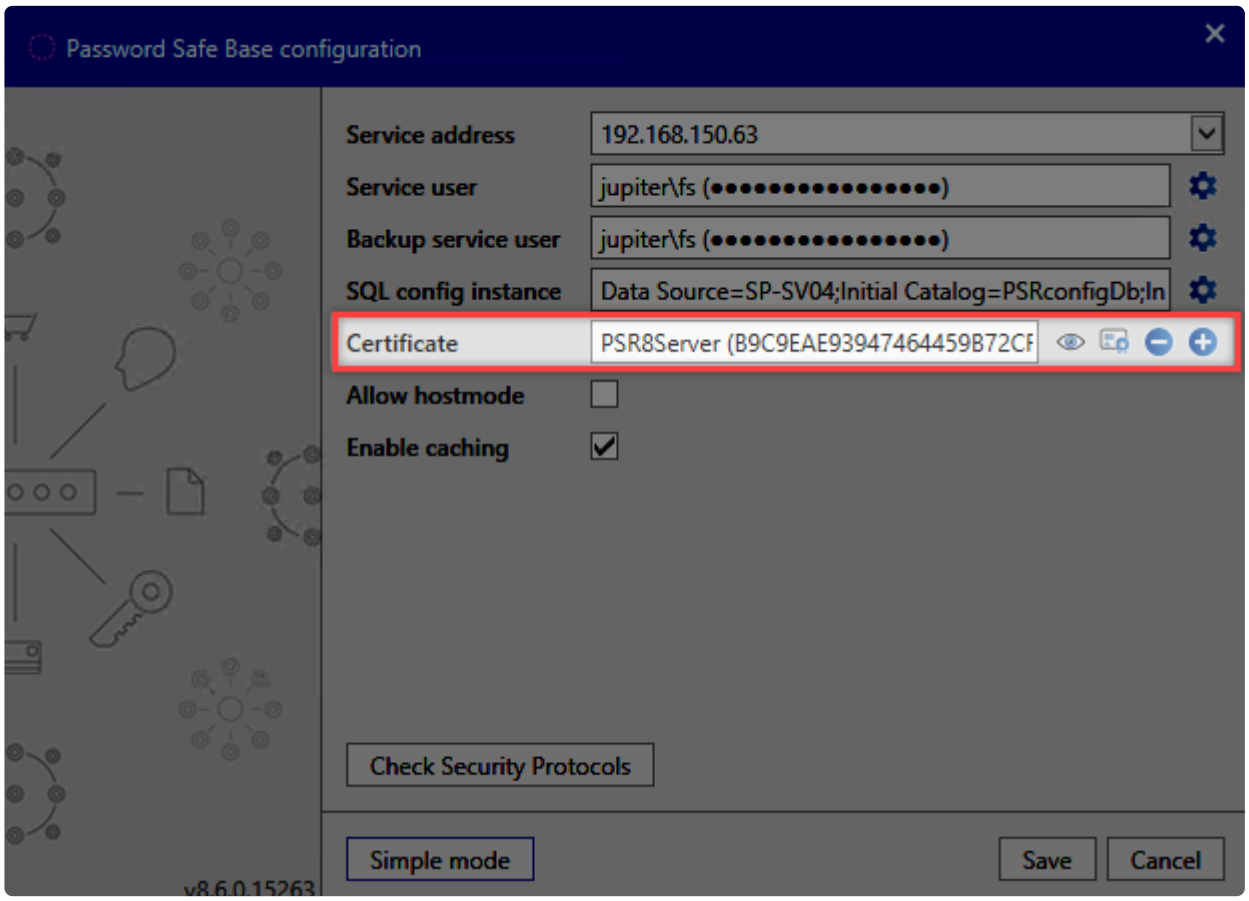
An SSL connection certificate needs to be changed because e.g. it has expired.

Requirements

Access to **AdminClient** is required.

Changing the certificate

Firstly, log into the AdminClient. Now open theBasic configuration. Open the configuration menu using the **Change** button. And then open **Expert mode**. The currently saved certificate is now visible here.



The buttons next to the certificate have the following functions (from left to right):

- Retrieve information about the certificate
- Select an existing certificate
- Discard a certificate
- Create a new self-signed certificate

Information on the certificates

Selecting an existing certificate

All of the certificates that can be used by Password Safe are displayed here. Therefore, they have to meet the requirements specified under **SSL connection certificates**.

Creating a new self-signed certificate

If no CA is available, you can also use your own self-signed certificate. It is important to note that it will need to be distributed after it has been changed on the client. Further information is available in the section **certificates**.

> In versions 8.0.0 to 8.2.0, the certificates were created with a validity of one year and thus they can expire. If you want to replace an expired certificate, you should firstly update to the latest available version. The certificate will then be valid until the year 9999 and is thus valid almost indefinitely.

Automatically receiving the WebViewer via e-mail

Specifications

A HTML WebViewer should be created once at 10:00 every day. The user wants to be able to call up the WebViewer via his e-mail inbox so that he can also access it when not in the office.

Requirements

The HTML WebViewer can be generated from the Professional Edition onwards. The SMTP server needs to be set up in advance using the setup wizard or alternatively in the backstage under Advanced settings.

Required user rights

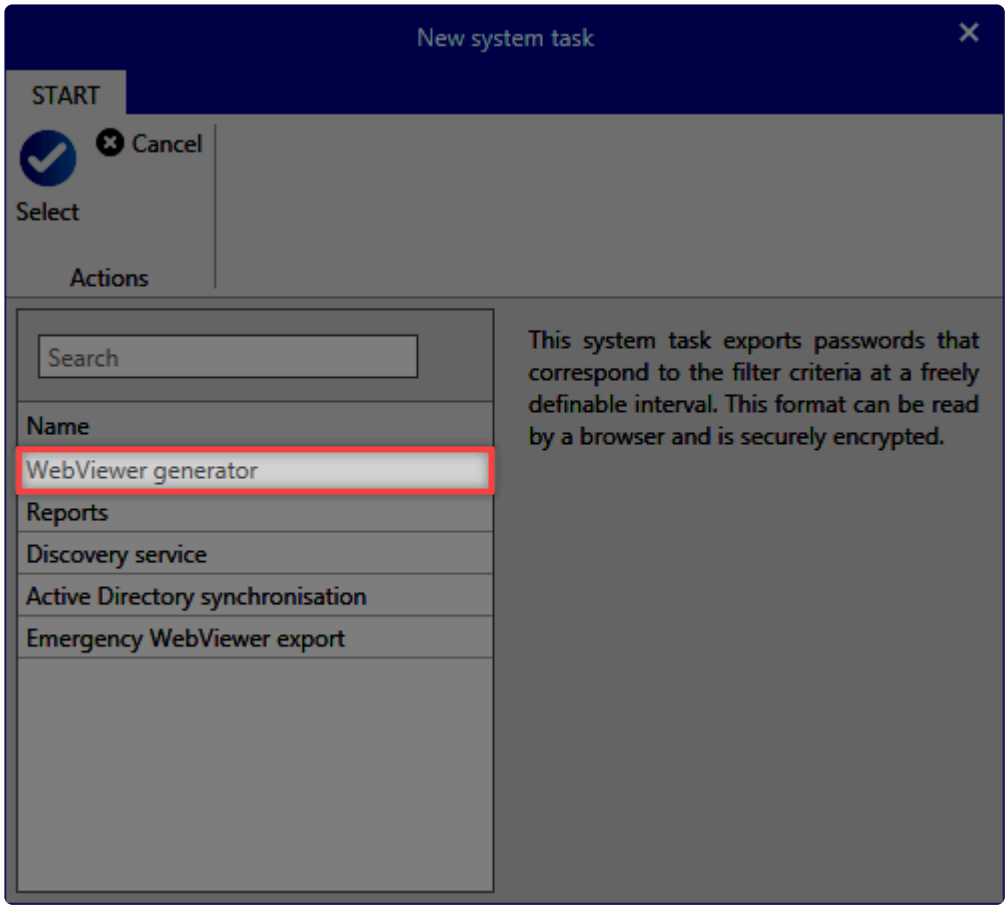
- Can export HTML WebViewer
- Can manage WebViewer export system tasks
- Display notification module

In addition, **export rights** to the desired passwords are required.

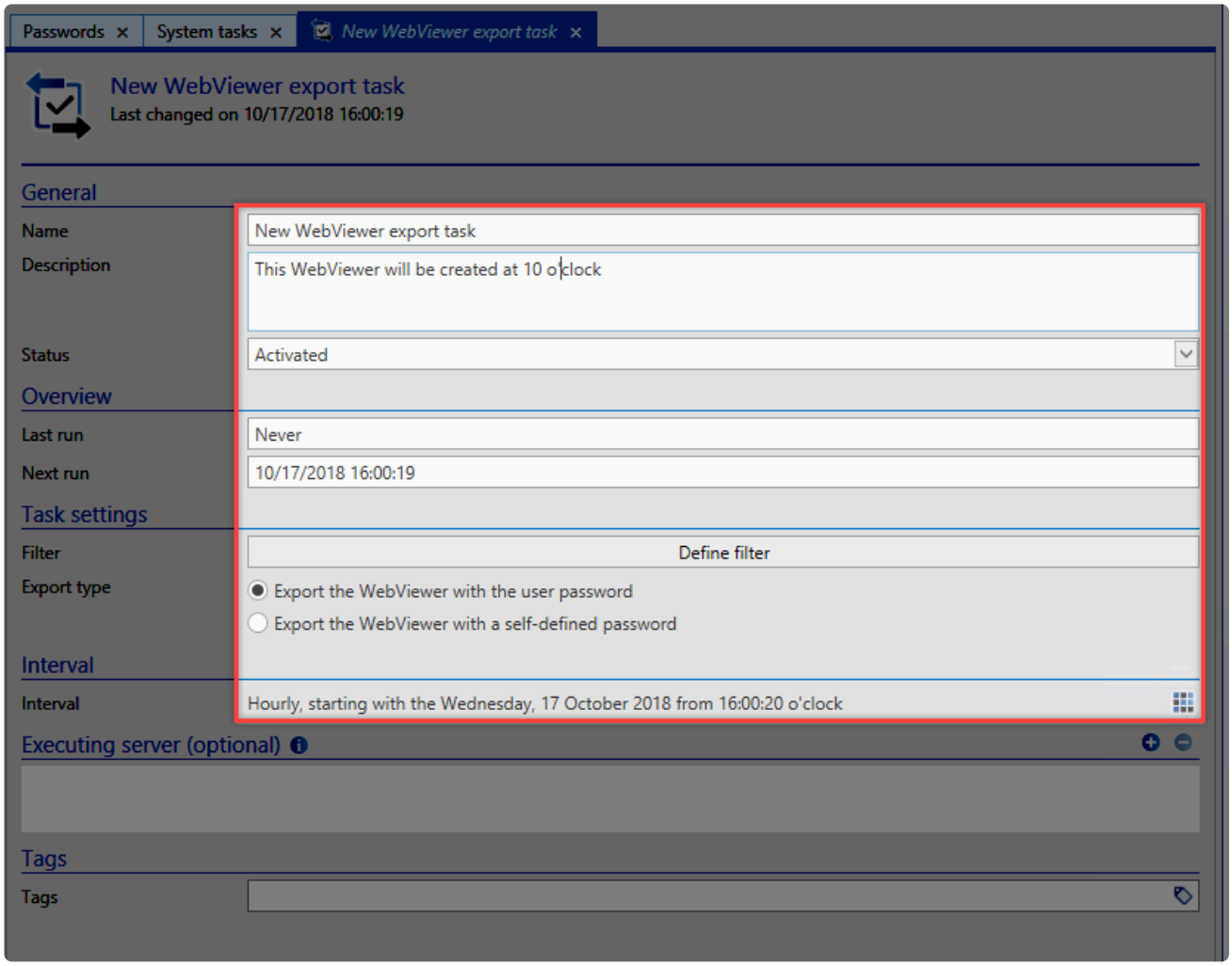
Configuration

Setting up a task

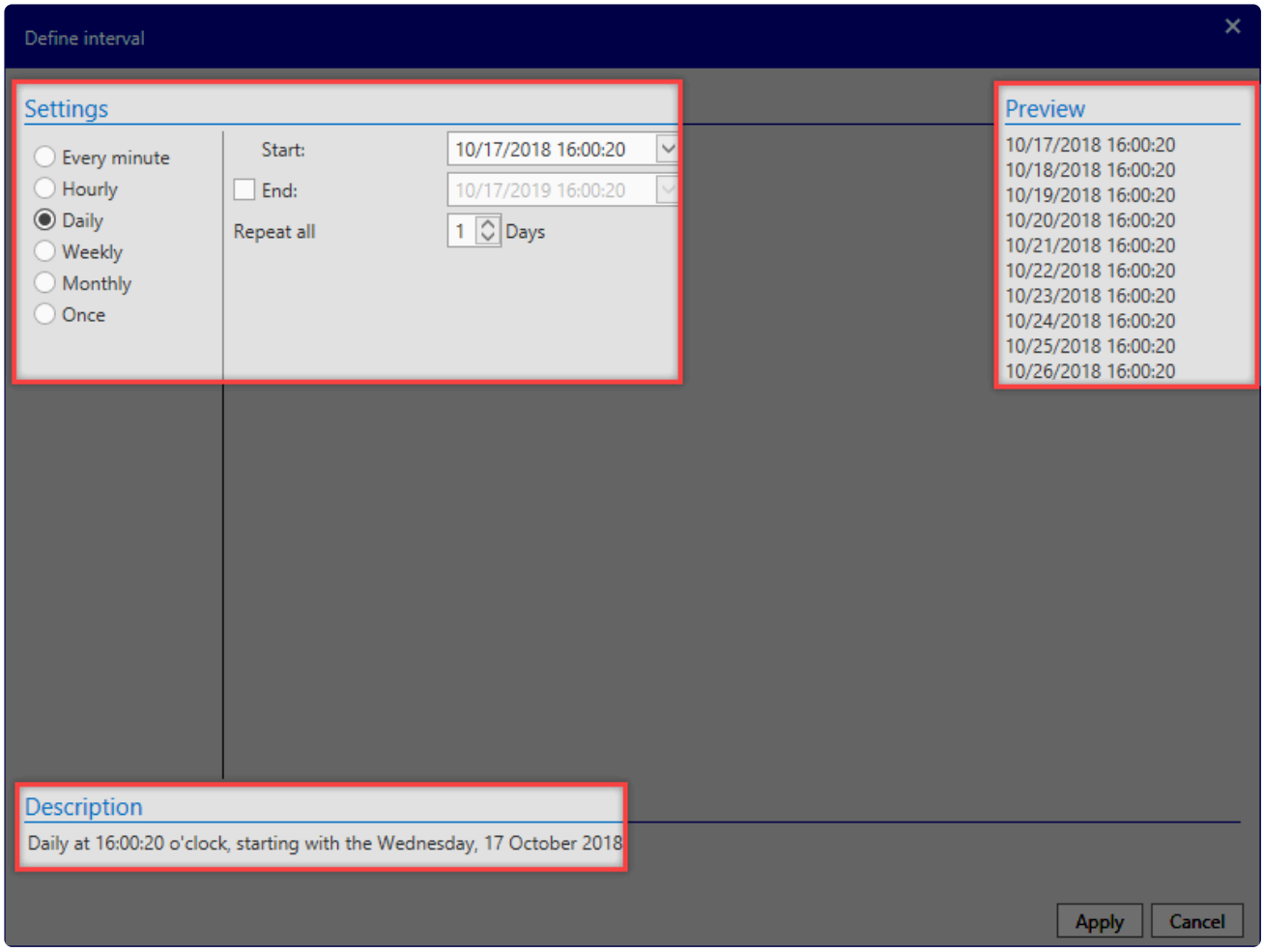
Firstly, the option for managing **System Tasks** is opened in the main menu (backstage). The “New” button is now used to create a new task. A **WebViewer generator** is selected here:



The WebViewer is then configured as required.

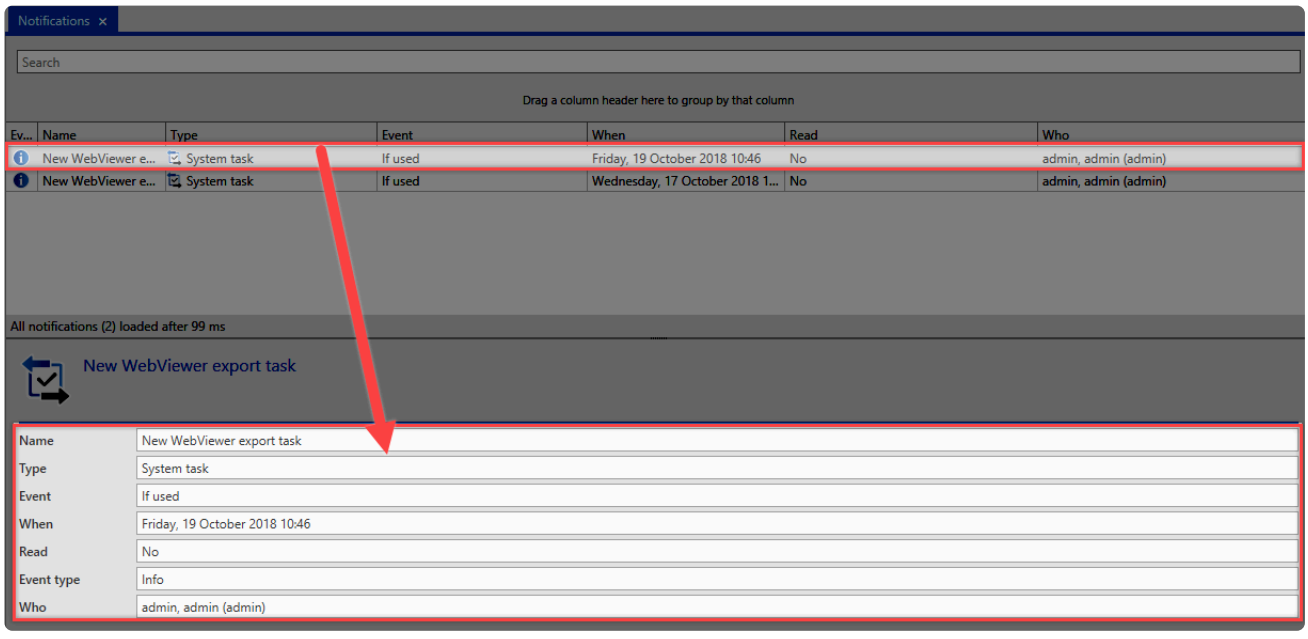


An interval of 10:00 every day is set.

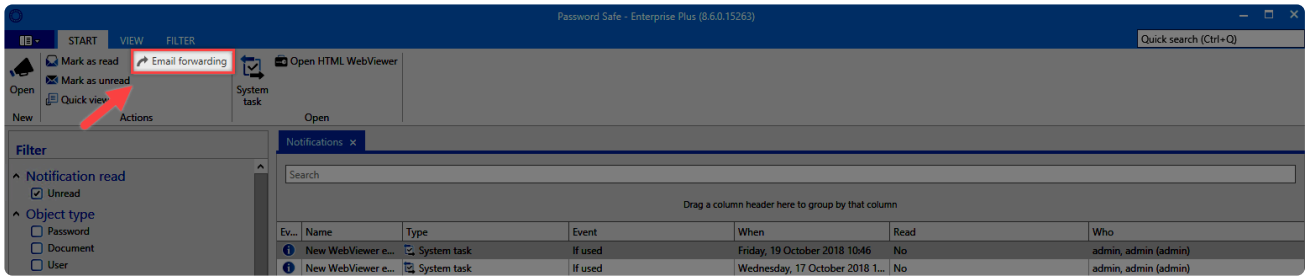


Configuring email forwarding

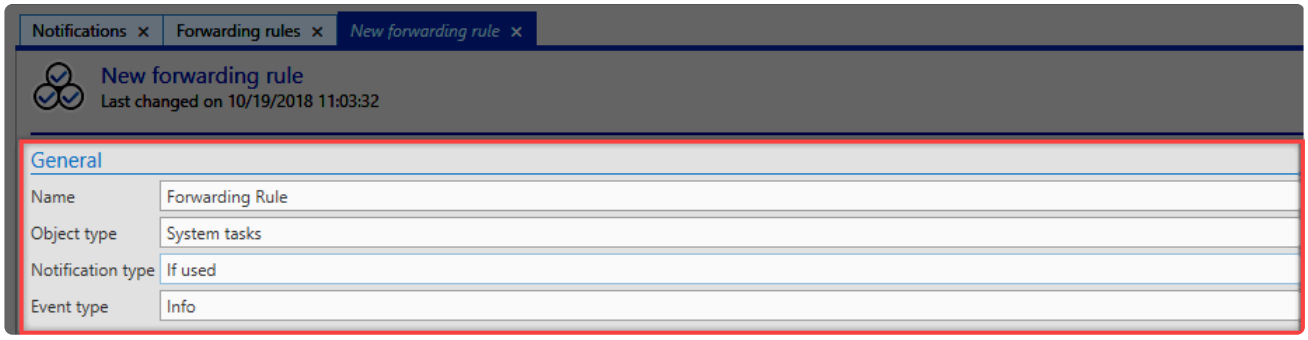
After the task has been run, the WebViewer that was created is delivered to the [notification module](#).



E-mail forwarding is also set up via the ribbon in the **notifications** module.



In the next step, a new forwarding rule is created via **New**. The required settings are shown on the screenshot.



Copy fields

Request

- A copy of a record is to be created, but it should have different rights or use a different form.
- After a successful migration, individual data records are to be transferred from version 7 to version 8.
- Individual data records are to be transferred from one database to another.

Requirements

An already complete data set is required.

Required user rights

- Can create new passwords
- Read rights on the data record

Configuration

Procedure in Version 8

Select the desired record to be copied.

You can now select **Copy Fields** in the ribbon

As soon as this is selected, another window will open. Here you can define exactly which fields are to be copied. Basically all fields are already selected. You can also decide whether the field names should also be copied.

Attention: If a record is to be duplicated, this check mark must be set!

If a new record is now created, a message will appear stating that data has already been found in the clipboard. Here you can decide whether you want to transfer the data.

If the message is confirmed with **Yes**, the data is automatically filled with **exact** the same field name. If the field names are not the same, no data is entered here.

Now the remaining fields (if available) can be filled and the record can be saved. Afterwards the rights can be set.

Procedure with data from version 7

To transfer a few data records from version 7 to version 8 quickly and easily, the fields can also be copied here.

The following steps must be observed:

1. Select the data set to be transferred to version 8
2. Right-click on the data set and select **Copy Field**

3. Select the fields which are to be copied by multiselect and also set the hook at **incl. description**.
4. Confirm with **Copy**.

5. Switch to version 8 and add a new data set.
6. Now the same message appears again, that data was found in the clipboard and whether it should be entered.

7. After confirmation of the message, the registration will be made
8. Confirm with Save
9. Now the rights can also be defined

Rights to the record but not to the password field

Request

One or more users should have access to a record, but not to the password field.

Requirements

A data record must exist.

Required user rights

- Can manage password form fields
- Read and authorization right on the data record

Configuration

First a data set must be selected. Then, right-click on the record to open the form field permissions.

Now you can decide for which form fields the permissions should apply. If these should apply to the password field, this must also be selected.

Tip: Several fields can also be selected simultaneously using Multiselect.

Next, the permissions can be set as desired. If a user is already authorized to the record with read permission, he or she is already here. If it is now desired that the user is not allowed to see the password field, he must be removed from the permissions. After the desired changes have been made, the whole thing must be confirmed with Save.

If it has now been configured correctly, the user who is not allowed to have access to the password field will have the following view:

Now the user has the possibility to request the right by clicking on the icon in the form field. Afterwards the permission request can be confirmed.

This request for rights can now be confirmed by a sufficiently authorized user. This is done via the module Permissions. Therefore the authorization for the module Notifications is also required.

The release is then carried out by confirming the rights request. For this, the requesting user must be granted the right manually.

Thus the user now also has access to the form field **Password**.

View passwords that may have incorrectly set permissions

Explanation of the hotfix in version 8.10

Currently there is a critical bug in version **8.10** which could possibly lead to passwords being authorized incorrectly. By checking a wrong permission, users could select a different permission template. When saving the password, however, only the default rights template is used. This only applies to users for whom the (global) right **“Can manage rights templates “** is deactivated.

Therefore we have published a hotfix after extensive testing. In order not to take any unnecessary risk, we ask users of version 8.10 to install the latest hotfix. You can download it via the update search in the software or the Customer Information System.

Who it concerns

This manual only concerns version **8.10**. If your default rights template in this version contains more rights than the optionally selected one, you can use this guide to check whether rights have been set incorrectly. This filter outputs the passwords for which an incorrect rights template may have been selected.

Required user rights

- Can edit filters
- Read rights on the data record

Procedure

Instructions for the administrator

1. Open Password Safe
2. Select the **Passwords** module
3. Open the filter view and click on “Edit filter”

4. Add the filter group “Logbook”

5. Close filter processing
6. Open the settings for the filter group Logbook usage by clicking on the gear wheel.

7. Please enter the date on which you updated or migrated to version 8.10 as the start date. If you do not know the date, please use 14.02.2020, the date of the official release.

Enter the present day as the end date. As a result, you will get a list of all passwords that are **possibly** affected by this error, so you can check them.

API

The Enterprise Plus Edition features a **API**: This interface can be used to “address Password Safe externally” in order to, for example, read data for other programs. The API can only be accessed via our wrappers using **C#** and **JavaScript**.

In the JavaScript version of the API, all enums can be found under the global object “PsrApiEnums”.

Requirements and download

The API is exclusively available in the Enterprise Plus Edition. The API client for the desired programming language can be downloaded from the Customer Information System. In order to use the API, web services must have been activated on the AdminClient in the **WebClient** module.

Using the API

The central object is “PsrApi”. It contains various “managers” that contain the entire business logic. First a “PsrApi” object must be created. The only transfer parameter of this class is the endpoint of the Password Safe WebServices. If the WebClient is in use, “call-des-webclient/api” can be used as the endpoint. Otherwise the Password Safe Server, i.e. “ip-des-servers:11016”, must be used directly.

C#

```
var psrApi = new PsrApi(„passwordsafe.company.com/api“);
```

JavaScript

```
const psrApi = new PsrApi(„passwordsafe.company.com/api“)
```

Login

If you do not log in to the system in advance, it is not possible to use the API. The first parameter for the login method is the desired database, followed by the user name and password. It is important to note that all methods for running the API that initiate a server call are implemented asynchronously. “Task” objects are returned in C# and “Promise” objects are returned in JavaScript.

C#

```
await psrApi.AuthenticationManager.Login(„Company“, „username“, „password“);
```

JavaScript

```
await psrApi.authenticationManager.login(„Company“, „username“, „password“)
```

Methods

All methods for the API can then be used. For example, you can search for records and decrypt a password:

C#

```
using System;
using System.Linq;
using System.Threading.Tasks;
using PsrApi.Data;
using PsrApi.Data.Enums;


namespace CSharpSDK
{
    class Program
    {
        static async Task Main(string[] args)
        {
            // After login you can use all functions of the API.
            // Insert your access data in the places marked with #.
            var psrApi = new PsrApi.PsrApi("#");
            await psrApi.AuthenticationManager.Login("#", "#", "#");

            // Passwords are in the context of the API container.
            // The ContainerManager is necessary for handling.
            var conMan = psrApi.ContainerManager;

            // To be able to filter for specific passwords, you need a filter of type P
            // To do this, you need to retrieve the default filter for passwords.
            var passwordListFilter = await conMan.GetContainerListFilter(
                PsrContainerType.Password, true);

            // In a second step you can search the default filter for a filter object c
            var contentFilter = passwordListFilter.FilterGroups
                .OfType<PsrListFilterGroupContent>().FirstOrDefault()
                ?.SearchList.FirstOrDefault();

            if (contentFilter != null)
            {
                // Replace the # digit with your search term.
                // In addition, the filter must be marked as Active.
                contentFilter.Search = "#";
                contentFilter.FilterActive = true;
            }
```

```
            // Now your searched passwords can be retrieved
            // using the previously configured filter.
            var passwords = await conMan.GetContainerList(
                PsrContainerType.Password, passwordListFilter);

            var passwordContainer = passwords.FirstOrDefault();
            if (passwordContainer != null)
            {
                // To make your searched password visible in plain text,
                // you need to search for the first password field
                // in the list of ContainerItems in your password
                var passwordItem = passwordContainer.Items
                    .FirstOrDefault(i => i.ContainerItemType == PsrContainerItemType.Co

                // The found ContainerItem can then be decrypted.
                var decryptedPasswordString = await conMan.DecryptContainerItem(passwor

                // After that you can use the password in plain text
               Console.WriteLine("Your password is: " + decryptedPasswordString);
            }

            // If the API is no longer needed,
            // you must log out of the current session again.
            await psrApi.AuthenticationManager.Logout();
        }
    }
}
```

JavaScript

```
(async function() {

  const { PsrApi, PsrApiEnums } = require('./src/psrApi')
  const { PsrContainerType, PsrContainerItemType } = PsrApiEnums

  // After login you can use all functions of the API.
  // Insert your access data in the places marked with #.
  const psrApi = new PsrApi('#')
  await psrApi.authenticationManager.login('#', '#', '#')

  // Passwords are in the context of the API container.
  // The ContainerManager is necessary for handling.
  const conMan = psrApi.containerManager

  // To be able to filter for specific passwords, you need a filter
  // of type PsrListFilterGroupContent.
```

```
  // To do this, you need to retrieve the default filter for passwords.
  const passwordListFilter = await conMan.getContainerListFilter(
    PsrContainerType.Password, true)

  // In a second step you can search the default filter for a filter
  // object of type PsrListFilterGroupContent.
  const contentFilter = passwordListFilter.FilterGroups
    .find(fg => 'SearchList' in fg).SearchList[0]

  if (contentFilter) {
    // Replace the # digit with your search term.
    // In addition, the filter must be marked as Active.
    contentFilter.Search = '#'
    contentFilter.FilterActive = true
  }

  // Now your searched passwords can be retrieved
  // using the previously configured filter.
  const passwords = await conMan.getContainerList(
    PsrContainerType.Password, passwordListFilter)

  const passwordContainer = passwords[0]
  if (passwordContainer) {
    // To make your searched password visible in plain text,
    // you need to search for the first password field
    // in the list of ContainerItems in your password.
    const passwordItem = passwordContainer.Items
      .find(i => i.ContainerItemType === PsrContainerItemType.ContainerItemPassword)

    // The found ContainerItem can then be decrypted.
    const decryptedPasswordString = await conMan.decryptContainerItem(passwordItem)

    // After that you can use the password in plain text.
    console.log('Your password is: ', decryptedPasswordString)
  }

  // Don't forget logout after completed work to prevent dead sessions
  await psrApi.authenticationManager.logout()

})()
```

Technical documentation

You can find the complete technical documentation for the API under the following link: Password Safe API

Beispiele C# SDK

> ! Alle folgenden Funktionen (außer Login und Logout) müssen in einem authentifizierten Kontext aufgerufen werden. Verwenden Sie also zuerst die Login-Funktion, bevor Sie eine der folgenden Funktionen ausführen.

Mit Benutzername und Passwort einloggen

```
private static async Task Login()
{
    // Accept invalid certificates - until .NET Framework 4.6
    // When using .NET Framework 4.7 or higher, you need to
    // create an own HttpClientHandler and set the callback there
    ServicePointManager.ServerCertificateValidationCallback += (sender, cert, chain, ss

    Console.Write("Enter your endpoint IP's to proceed (xxx.xxx.xxx.xxx): ");
    var endpointIp = Console.ReadLine();

    var psrApi = new PsrApi($":11016");

    Console.WriteLine($"Available databases: {string.Join(", ", await psrApi.GetActiveD

    Console.Write("Database: ");
    var database = Console.ReadLine();

    Console.Write("Username: ");
    var username = Console.ReadLine();

    Console.Write("Password: ");
    var password = ReadPassword();
    var mfaRequest = await psrApi.AuthenticationManager.Login(database, username, passw

    if (mfaRequest != null)
    {
        await PerformMultiFactorAuth(mfaRequest, psrApi, database, username, password);
    }

    psrApi.ServerStatusChanged += (sender, status) => Console.WriteLine(status);
    psrApi.SessionExpired += async (sender, e) =>
    {
        Console.WriteLine("Session has expired");
        //For example, you could relogin here...
    };
```

```
    Console.WriteLine($"Logged in; Session expiring at: { psrApi.SessionExpirationUtc?.

    psrApi.RealtimeEventManager.ServerMessageReceived += (sender, args) =>
        Console.WriteLine(args.ServerMessage.Message + $" was received ({args.ServerMes
    psrApi.RealtimeEventManager.ContainerChanged += (sender, args) =>
        Console.WriteLine(args.Container.DataName() + $" was changed ({args.EventType.T
    psrApi.RealtimeEventManager.RoleChanged += (sender, args) =>
        Console.WriteLine(args.Role.DataName() + $" was changed ({args.EventType.ToStri
    psrApi.RealtimeEventManager.UserChanged += (sender, args) =>
        Console.WriteLine(args.User.DataName() + $" was changed ({args.EventType.ToStri
    psrApi.RealtimeEventManager.GroupChanged += (sender, args) =>
        Console.WriteLine(args.Group.DataName() + $" was changed ({args.EventType.ToStr
    psrApi.RealtimeEventManager.DataBindingChanged += (sender, args) =>
        Console.WriteLine(args.DataBinding.DataId + $" was changed ({args.EventType.ToS

    _psrApi = psrApi;
}

private static async Task PerformMultiFactorAuth(PsrMultiFactorAuthenticationRequest mf
{
    if (mfaRequest.AuthenticatorType == PsrMultiFactorAuthType.Pki)
    {
        var pkiFields = GetCertificatePkiFields(mfaRequest);

        mfaRequest.RequiredFields.ToList().Find(f => f.Type == PsrMultiFactorField.Sign
        mfaRequest.RequiredFields.ToList().Find(f => f.Type == PsrMultiFactorField.Cert
    }
    else
    {
        foreach (var field in mfaRequest.RequiredFields)
        {
            Console.Write($"Enter 2nd factor '{mfaRequest.DisplayName}' ({field.Type.To
            var mfa = field.Type == PsrMultiFactorField.Pin || field.Type == PsrMultiFa
                ? ReadPassword()
                : Console.ReadLine();
            field.Value = mfa;
        }
    }

    await psrApi.AuthenticationManager.Login(database, username, password, mfaRequest.R
}

private static PkiFields GetCertificatePkiFields(PsrMultiFactorAuthenticationRequest mf
{
    Console.WriteLine("Select a certificate from the store");
    var store = new X509Store("MY", StoreLocation.CurrentUser);
    store.Open(OpenFlags.ReadOnly | OpenFlags.IncludeArchived);
```

```
    var collection = store.Certificates.Find(X509FindType.FindByKeyUsage, X509KeyUsageF
    var selectedCert = X509Certificate2UI.SelectFromCollection(collection, "Select a ce
        X509SelectionFlag.SingleSelection)[0];
    if (!(selectedCert.PrivateKey is RSACryptoServiceProvider csp))
    {
        throw new Exception();
    }

    string signedHash;
    using (var hashAlgo = HashAlgorithm.Create(HashAlgorithms.Sha1.ToString()))
    {
        if (hashAlgo == null)
        {
            throw new Exception();
        }

        var hash = hashAlgo.ComputeHash(mfaRequest.DataToSign);
        var oid = CryptoConfig.MapNameToOID(HashAlgorithms.Sha1.ToString());
        var bytes = csp.SignHash(hash, oid);
        signedHash = Convert.ToBase64String(bytes);
    }

    return new PkiFields()
    {
        SignedDataId = signedHash,
        CertificateThumbPrint = selectedCert.Thumbprint
    };
}

public class PkiFields
{
    public string SignedDataId;
    public string CertificateThumbPrint;
}
```

Ausloggen

```
await _psrApi.AuthenticationManager.Logout();
Console.WriteLine("PsrApi logged out")
```

Ein Passwort für den eigenen Benutzer erstellen

```
var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, PasswordGener
var passwordContainer = new PsrContainer
```

```
{
    ContainerType = PsrContainerType.Password,
    Items = new List<PsrContainerItem>
    {
        new PsrContainerItem
        {
            Name = "Name",
            ContainerItemType = PsrContainerItemType.ContainerItemText,
            Value = "MyPsrApiPassword_SIMPLE",
        },
        new PsrContainerItem
        {
            Name = "Password",
            ContainerItemType = PsrContainerItemType.ContainerItemPassword,
            PlainTextValue = "utlra secret password goes here",
        },
    }
};

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, _psr
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Ein Passwort für eine Organisationseinheit erstellen

```
var passwordContainer = new PsrContainer
{
    ContainerType = PsrContainerType.Password,
    Items = new List<PsrContainerItem>
    {
        new PsrContainerItem
        {
            Name = "Name",
            ContainerItemType = PsrContainerItemType.ContainerItemText,
            Value = "MyPsrApiPassword_SIMPLE",
        },
        new PsrContainerItem
        {
            Name = "Password",
            ContainerItemType = PsrContainerItemType.ContainerItemPassword,
            PlainTextValue = "utlra secret password goes here",
        },
    }
};

// find the organisational unit to put our new password (we take the most top ou)
```

```
var filter = new PsrListFilter
{
    DataStates = PsrDataStates.StateActive,
    FilterGroups = new List<PsrListFilterGroup>
    {
        new PsrListFilterGroupOrganisationUnitType
        {
            TypeFilters = new List<PsrListFilterObjectOrganisationUnitType>
            {
                new PsrListFilterObjectOrganisationUnitType
                {
                    FilterActive = true,
                    OrganisationUnitType = PsrFilterOrganisationUnitType.FilterOrganisa
                }
            }
        }
    }
};
var ouGroups = await _psrApi.OrganisationUnitManager.GetOrganisationUnitStructure(filte
var topLevelOu = ouGroups?.FirstOrDefault();
var targetOu = topLevelOu?.OrganisationUnit ?? _psrApi.CurrentUser;

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, targ
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Ein Passwort mittels einem bestimmten Formulars für den eigenen Benutzer erstellen

```
var formsFilter = await _psrApi.ContainerManager.GetContainerListFilter(PsrContainerTyp
var availableForms = await _psrApi.ContainerManager.GetContainerList(PsrContainerType.F

if (!availableForms.Any())
{
    Console.WriteLine("no forms found");
    return;
}

var passwordContainer = _psrApi.ContainerManager.CreateContainerFromBaseContainer(avail

var textField = passwordContainer.Items.FirstOrDefault(ci => ci.ContainerItemType == Ps
if (textField != null) textField.Value = "MyPsrApiPassword_FORM";

var urlField = passwordContainer.Items.FirstOrDefault(ci => ci.ContainerItemType == Psr
if (urlField != null) urlField.Value = "https://www.passwordsafe.de";
```

```
var passwordField = passwordContainer.Items.FirstOrDefault(ci => ci.IsPasswordItem());
if (passwordField != null)
{
    var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, PasswordG
    passwordField.PlainTextValue = newPassword;
}

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, _psr
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Passwörter mit Hilfe der Inhaltssuche finden

```
var filter = new PsrContainerListFilter
{
    DataStates = PsrDataStates.StateActive,
    FilterGroups = new List<PsrListFilterGroup>
    {
        new PsrListFilterGroupContent
        {
            SearchList = new List<PsrListFilterObjectContent>
            {
                new PsrListFilterObjectContent
                {
                    FilterActive = true,
                    Search = "MyPsrApiPassword_",
                }
            }
        }
    }
};

var passwords = await _psrApi.ContainerManager.GetContainerList(PsrContainerType.Passwo
Console.WriteLine($"{passwords.Count()} Passwords found with Content 'MyPsrApiPassword_
```

Ein Passwort mittels der ID finden

```
var password = await _psrApi.ContainerManager.GetContainer(id);
if (password != null) Console.WriteLine($"Password {password.DataName()} retrieved by G
```

Ein Passwort aktualisieren

```
private static async Task UpdatePassword(PsrContainer updatePassword)
{
```

```
    var textField = updatePassword.Items.FirstOrDefault(ci => ci.ContainerItemType == P
    if (textField != null) textField.Value = "MyPsrApiPassword_UPDATE";

    var passwordField = updatePassword.Items.FirstOrDefault(ci => ci.IsPasswordItem());
    if (passwordField != null)
    {
        var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, Passw
        passwordField.PlainTextValue = "UPDATED_SECRET_PASSWORD_" + newPassword;
    }

    await _psrApi.ContainerManager.UpdateContainer(updatePassword);
    Console.WriteLine($"Password {updatePassword.Id} updated");
}
```

Ein Passwort löschen

```
await _psrApi.ContainerManager.DeleteContainer(deletePassword);
Console.WriteLine($"Password {deletePassword.Id} deleted");
```

Benutzer zum Mitglied einer Rolle machen

```
private static async Task MakeUserRoleMember(Guid userId, Guid roleId)
{

    var role = await _psrApi.RoleManager.GetRole(roleId);
    var user = await _psrApi.OrganisationUnitManager.GetOrganisationUnitUser(userId);
    var rights = (await _psrApi.RightManager.GetLegitimateDataRightsWithTemporalRights(
    rights.Add(new PsrDataRight
    {
        DataId = roleId,
        LegitimateId = userId,
        Legitimate = user,
        IncludeDataRightKey = true,
        Rights = PsrRights.RightRead
    });
    await _psrApi.GenericRightManager.SaveRights(new List<PsrData> { role }, rights, fa
}
```

Eine Organisationseinheit anhand des Namens finden

```
private static async Task<IEnumerable<PsrOrganisationUnitStructure>> FindOrganisationUn
{
    var filterGroups = new List<PsrListFilterGroup>
```

```
    {
        new PsrListFilterGroupContent
        {
            SearchList = new List<PsrListFilterObjectContent>
            {
                new PsrListFilterObjectContent
                {
                    FilterActive = true,
                    Search = name,
                }
            }
        }
    };

    // if we should search in a specified parent, we have to add this as filter conditi
    if (parent != null)
    {
        filterGroups.Add(new PsrListFilterGroupOrganisationUnit
        {
            OrganisationUnitFilter = new PsrListFilterObjectOrganisationUnit
            {
                FilterActive = true,
                SelectedOrganisationUnitId = parent.Id
            }
        });
    }

    var ouContentFilter = new PsrListFilter
    {
        DataStates = PsrDataStates.StateActive,
        FilterGroups = filterGroups
    };

    return (await _psrApi.OrganisationUnitManager.GetOrganisationUnitStructure(ouConten
}
```

Erstellen einer Organisationseinheit unterhalb einer bereits existierenden

```
private static Task<PsrOrganisationUnitGroup> CreateOrgainsationUnitGroup(string name,
{
    var rsa = new PsrRsa();
    var group = new PsrOrganisationUnitGroup
    {
        GroupName = name,
```

```
        PublicKey = rsa.PublicKey,
    };

    var encryptedGroupKey = PsrEncryption.EncryptWithPublicKey(_psrApi.CurrentUser.Publ
    return _psrApi.OrganisationUnitManager.AddOrganisationUnitGroup(group, _psrApi.Curr
}
```

Überprüfen, ob eine Organisationseinheit unterhalb einer bestimmten Organisationseinheit existiert und wenn nicht Erstellen dieser.

```
private static async Task<PsrOrganisationUnit> CheckIfOuExists(string parentOuName, str
{
    var myParentOu = (await FindOrganisationUnitsByName(parentOuName)).FirstOrDefault()
    if (myParentOu == null)
    {
        Console.WriteLine("Parent-OU doesn't exist");
        return null;
    }

    var myChildOu = (await FindOrganisationUnitsByName(findOrCreateOuName, myParentOu.O
    if (myChildOu != null)
    {
        Console.WriteLine("ou found -> not creating anything");
        return myChildOu.OrganisationUnit;
    }

    Console.WriteLine("ou not found -> we create now the ou group");
    return await CreateOrgainsationUnitGroup(findOrCreateOuName, myParentOu.Organisatio
}
```

Alle Benutzer finden, die Datenbank-Administrator sind

```
private static async Task LoadAllDatabaseAdmins()
{
    var onlyUserOus = new PsrListFilter
    {
        FilterGroups = new List<PsrListFilterGroup>
        {
            new PsrListFilterGroupOrganisationUnitType
            {
                TypeFilters = new List<PsrListFilterObjectOrganisationUnitType>
                {
```

```
                    new PsrListFilterObjectOrganisationUnitType
                    {
                        FilterActive = true,
                        OrganisationUnitType = PsrFilterOrganisationUnitType.FilterOrga
                    }
                }
            }
        }
    };

    Console.WriteLine($"Following Users have the Database Admin Right:");
    var organisationUnitUsers = await _psrApi.OrganisationUnitManager.GetOrganisationUn
    foreach (var user in organisationUnitUsers.Select(ous => ous.OrganisationUnit as Ps
    {
        var rightsOfUsers = await _psrApi.OptionManager.GetOptions(new List<PsrOptionGr
        var dbAdminRight = rightsOfUsers.FirstOrDefault(r => r.Name == PsrUserRightDefa
        if (dbAdminRight is PsrOptionBoolean bDbAdminRight && bDbAdminRight.ValueBoolea
        {
            Console.WriteLine($"- {user.UserName}");
        }
    }
}
```

Beispiele Javascript SDK

> ! Alle folgenden Funktionen (außer Login und Logout) müssen in einem authentifizierten Kontext aufgerufen werden.

Benutzer hinzufügen

```
const { EncryptWithPassword, EncryptWithPublicKey } = require('../node/lib/MtoEncryptic
const { MtoPbkdf2GenerateSalt } = require('../node/lib/MtoPbkdf2');
const MtoRsa = require('../node/lib/MtoRsa');

const createUser = async (api, username, password, parentId) => {
  const encodedPassword = unescape(encodeURIComponent(password))
  const pwHash = MtoPbkdf2GenerateSalt(encodedPassword, 16, 100000, 32)
  const rsa = new MtoRsa()
  rsa.generateKeyPair()
  const encryptedPrivateKeyWithPassword = EncryptWithPassword(encodedPassword, rsa.priv

  // Membership of current API user
  const currentUserRsa = new MtoRsa()
  currentUserRsa.publicKeyFromXml(api.currentUser.PublicKey)
  const encryptedPrivateKeyWithPublicKey = EncryptWithPublicKey(currentUserRsa, rsa.pri

  const user = {
    UserName: username
  }

  await api.organisationUnitManager.addOrganisationUnitUser(
    user,
    pwHash.key,
    pwHash.salt,
    rsa.publicKeyToXml(),
    encryptedPrivateKeyWithPassword,
    encryptedPrivateKeyWithPublicKey,
    parentId
  )
}
```

Tag hinzufügen

```
// Data may be any PsrData like PsrContainer, PsrRole, PsrOrganisationUnitUser …
const addTag = async (api, data, tagId) => {
  const dataTags = data.DataTags
```

```
  dataTags.push({
    DataId: data.Id,
    TagId: tagId
  })

  await api.tagManager.setDataTags(dataTags, data.Id)
}
```

Version history

The previously released versions and the corresponding changelogs can be found in the following sections.

- Version 8.13.14.27679
- Version 8.13.13.27522
- Version 8.13.12.27427
- Version 8.13.11.27156
- Version 8.13.10.26901
- Version 8.13.9.26689
- Version 8.13.8.25983
- Version 8.13.7.25979
- Version 8.13.6.25933
- Version 8.13.5.25731
- Version 8.13.4.25228
- Version 8.13.3.25194
- Version 8.13.2.25151
- Version 8.13.1.25117
- Version 8.13.0.25027
- Version 8.12.1.22757
- Version 8.12.0.22707
- Version 8.11.1.19828 Hotfix 1
- Version 8.11.1.19823
- Version 8.11.0.19788
- Version 8.10.0.18473 Hotfix 2
- Version 8.10.0.18516 Hotfix 1
- Version 8.10.0.18464
- Version 8.9.0.17993 Hotfix 2
- Version 8.9.0.17702 Hotfix 1
- Version 8.9.0.17656
- Version 8.8.0.18002 Hotfix 3
- Version 8.8.0.17596 Hotfix 2
- Version 8.8.0.17168 Hotfix 1
- Version 8.8.0.17146
- Version 8.7.0.18000 Hotfix 3
- Version 8.7.0.16698 Hotfix 2
- Version 8.7.0.16387 Hotfix 1
- Version 8.7.0.16245
- Version 8.6.0.15386 Hotfix 1
- Version 8.6.0.15368
- Version 8.5.0.14896
- Version 8.4.0.14618
- Version 8.3.0.13378
- Version 8.2.0.12343
- Version 8.3.0.14422 Hotfix 1
- Version 8.2.0.12388 Hotfix 1

- Version 8.1.0.10812
- Version 8.1.1.11106
- Version 8.1.1.11211 Hotfix 1
- Version 8.0.2.9541 Hotfix 1
- Version 8.0.2.9978 Hotfix 2
- Version 8.0.1.9032
- Version 8.0.2.9278

Version 8.13.14.27679

Release

29h of March 2022

Compatibility

The following client versions are compatible with AdminClient version 8.13.14.27679

- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Verison 8.13.14.27679
- WebClient Verison 8.13.13.27522
- WebClient Verison 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.10.0.18473 Hotfix 3 as well as the Android 9 OS for the mobile app has stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

The handling of AD profiles is supported only with the latest clients

New

FullClient

- The readability of the action buttons has been optimized for better understanding in the navigation / ribbon.

WebClient

- The readability of the action buttons has been optimized for better understanding in the navigation / ribbon.

LightClient

- The readability of the action buttons has been optimized for better understanding in the navigation / ribbon.

LightClient in the web view

- The readability of the action buttons has been optimized for better understanding in the navigation / ribbon.

Changes

FullClient

- We changed to the new Yubico endpoint api.yubico.com. The old APIs api(n).youbico.com are no longer supported by Yubico.

LightClient

- We canged to the new Yubico endpoint api.yubico.com. The old APIs api(n).youbico.com are no longer supported by Yubico.

Please make sure Password Safe has access to the new API.

Improvements

FullClient

- Messages during a Keepass import have been optimized.

LightClient in the web view

- The appearance of empty tiles including text added key logo has been improved.

Fixed

FullClient

- Users can now log in with a smartcard certificate if it contains only the last part of a username.

> Please update to version 8.13.14 if smartcards are in use.

- During an RDP session, the window is no longer scaled when returning to window mode.

Server

- System tasks are stopped when an error occurs.
- There is no longer an incorrect SQL connection string displayed that generated an error message when a backup was performed AND MARS was active.
- When using a license on a standby machine in Hybernate mode, the license is valid again after 30 days in Hybernate mode.

LightClient

- Users can now log in with a smartcard certificate if it contains only the last part of a username.

LightClient in the web view

- Users can delete the user right to create passwords under certain conditions if the user rights “Can add individual passwords via LightClient” AND “Can create personal records” have been granted.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.14.27679-de.msi)
`5335503d5d1d1ef0703d39a48224766de87d4099541cbe1030cd6af02bb24afa442c77402fb0ad33ddd8e`

English Server Setup (pss8.13.14.27679-en.msi)
`a02bd2c7086208620b207c5d4eaf188c212d9839c73aa5817347af9ad664af704de81e5e4ee0bd02defc6`

German Client Setup (psc8.13.14.27679-de.msi)
`52a5539424440935e8f75eeba4a461183e232920ca30430e856c5c47a6e56becc3e5170f8571cb02fe977`

English Client Setup (psc8.13.14.27679-en.msi)
`d44a00e384dcb1c9347a20c0aab5ef03b831af7b6db2ad08c633e8e7a588a13b8f484f46edb3b2d459b57`

Version 8.13.13.27522

Release

14th of March 2022

Compatibility

The following client versions are compatible with AdminClient version 8.13.13.27522

- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Verison 8.13.13.27522
- WebClient Verison 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.10.0.18473 Hotfix 3 as well as the Android 9 OS for the mobile app has stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

The handling of AD profiles is supported only with the latest clients

New

LightClient in the Web View

- If there are no passwords stored in Password Safe yet, new users will receive hints about further actions to find their way around faster.

Improvements

FullClient

- Update of the integrated PuTTY version to version 0.76

LightClient

- Update of the integrated PuTTY version to version 0.76

Fixed

Server

- Users of Professional and MSP licenses can also be deleted again without Active Directory integration.

MSP

- Users of Professional and MSP licenses can also be deleted again without Active Directory integration.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.13.27522-de.msi)
`02d44733b306c85708dd25fa8b745d3bf3b5e6d29db7e56ab2f1125cef1dc486d27c99249710dabc5514e`

English Server Setup (pss8.13.13.27522-en.msi)
`4622dd0a3bd569ec439457789a6198b310c0703ead111d50857c0f42592328575b8638e8e4f7cf916a006`

German Client Setup (psc8.13.13.27522-de.msi)
`7f82e162b2fed7f06e682c9cecaf5c2f96c6606dbe1782b42d0bcaad74d4f493690f3381ff356aee5d87a`

English Client Setup (psc8.13.13.27522-en.msi)
`abc3184c3fc65f16d49a41f8628b81cd2fc753897abf39813ea904dad341d8bdc15e11eebadeb67429f0c`

Version 8.13.12.27427

Release

28th of February 2022

Compatibility

The following client versions are compatible with AdminClient version 8.13.12.27427

- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Verison 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.10.0.18473 Hotfix 3 as well as the Android 9 OS for the mobile app has stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

The handling of AD profiles is supported only with the latest clients

New

WebClient

- On the web, LightClient users can now change the user interface language without having to switch to the FullClient.

Improvements

FullClient

- The RDP tab on the desktop now also shows information such as the hostname, password name, and IP address, if available.

Fixed

FullClient

- When importing CSVs, the “Remember selection for subsequent passwords” checkbox now also works for the “Create new” selection.
- Passwords can be saved to the desktop again when a user is logged in via SSO agent.

WebClient

- The tag selection for a password – especially when there are several hundred tags – works faster now.
- The security level of the settings in the “Global user settings” can no longer be changed.

Server

- A user can no longer start an AD import/sync even if he is neither the master key user nor the additional responsible user of an AD profile and there is no error message anymore.
- When changing from or to summertime, system tasks are executed at the correct time again.

Android App

- The mobile app can synchronize again if a password was moved to a unit when using two organizational units, overwriting permissions.

iOS App

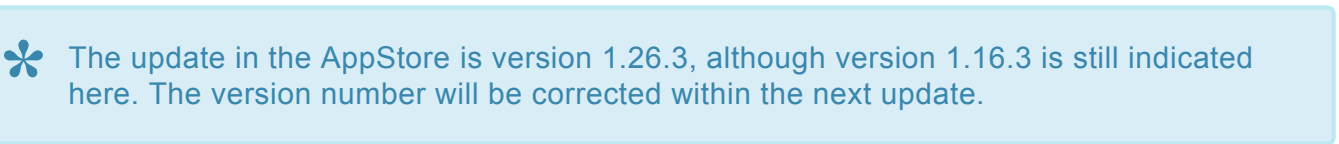
- The mobile app can synchronize again if a password was moved to a unit when using two organizational units, overwriting permissions.*

SSO Agent

- Passwords can now be saved in the FullClient on the desktop again when a user is logged in via SSO Agent.

LightClient in the Web View

- A tooltip for the “Create new password” button has been added.
- A tooltip for the list view has been added.



Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.12.27427-de.msi)

5d6ac7c7b9a42eb09c6b11df33febf3d90140a16c82139abc140c88a31f7bb6b967fb81f28a657f8d96a6

English Server Setup (pss8.13.12.27427-en.msi)

62894d51ccebb21ce45370628c8e858f322981ee2aeea734b73eb302dea64f6cc30f8ab7554d426766c86

German Client Setup (psc8.13.12.27427-de.msi)

65951207888d648d6be2f57a81e887f1a05e17a561a31c913118d228a14062d7334e0f9dee8ae5984ff50

English Client Setup (psc8.13.12.27427-en.msi)

5d9a05048d2cc250dece4c9117449a32a3dbc76506be08fa986827566508ff7ac0d2aded2dbe1d7e9662c

Version 8.13.11.27156

Release

15th of February 2022

Compatibility

The following client versions are compatible with AdminClient version 8.13.11.27156

- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.10.0.18473 Hotfix 3 as well as the Android 9 OS for the mobile app has stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

* The handling of AD profiles is supported only with the latest clients

Improvements

FullClient

- For the display of passwords in plain text, the font "Monotype" was deposited for better readability.

WebClient

- Improved display of the user avatar
- Display feedback to users when adding/removing their second factor
- For the display of passwords in plain text, the font "Monotype" was deposited for better readability.

- Improved performance while decrypting passwords in the WebClient

Server

- Improved IP address filter speed

AdminClient

- Changes of webserver config are more noticeable for administrators now.

Android App

- For the display of passwords in plain text, the font “Monotype” was deposited for better readability.

iOS App

- For the display of passwords in plain text, the font “Monotype” was deposited for better readability.

OfflineClient

- For the display of passwords in plain text, the font “Monotype” was deposited for better readability.

LightClient

- For the display of passwords in plain text, the font “Monotype” was deposited for better readability.

LightClient in the Web View

- The design of the tile view has been made more user-friendly.
- For the display of passwords in plain text, the font “Monotype” was deposited for better readability.
- Applications that cannot be used in the WebLightClient are now hidden.
- Improved display of the user avatar
- The linking of applications within the edit/create view has been made easier.
- Display feedback to users when adding/removing their second factor
- Improved performance while decrypting passwords in the WebClient

Fixed

FullClient

- It is possible again to print a very large number of passwords.
- It got fixed that the DesktopClient crashed during offline synchronization under special circumstances.
- When using Windows 11, the automatic logout could lead to a non-responding client.
- The YubiKey could not be configured in the DesktopClient as the autologout had been triggered.
- In AD, additional responsible users are no longer deleted when saving if the current user does not have read permission for them.
- Under special conditions, a password could not be saved.

WebClient

- It is possible to print a very large number of passwords again.
- The deactivated user right “Can export” did not worked properly in special circumstances in the

WebClient.
- Responsible users in an Active Directory profile could be deleted.

Server

- Additional responsible users won't be added to the permissions of users/roles from that profile.
- When using the "Restrict userimport to role members" mode in the AD-Import-Wizard the excludelist is used.
- Responsible users in an Active Directory profile could be deleted.

Browser Extension

- The connection with the SSO Agent for using the browser extension works automatically again.

SSO Client

- The connection with the SSO Agent for using the browser extension works automatically again.

LightClient

- The YubiKey could not be configured in the DesktopClient as the autologout had been triggered.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.11.27156-de.msi)
f8b93cebd2637e7409c18f627ea047898ff0bc36d60d62702d96cb9c9865deb019610f43dc8a71ec4ae6f

English Server Setup (pss8.13.11.27156-en.msi)
46d5ac713707e847669e45e9e1a21606a88321be087b3949b73e6f6f3205b6886a8e4f1b81d1e62d6ea59

German Client Setup (psc8.13.11.27156-de.msi)
046324ebd35615f42f3ddd52d71d2ec9fb46cd07a4a8b69ac307c422853d6d3ba338f9721c756942d34ae

English Client Setup (psc8.13.11.27156-en.msi)
8134cefc9ddc465a31851c0dd429e5c0b3ea44953692479a32f8a1cec85d05ad47217e347344e5d81fc45

Version 8.13.10.26901

Release

17th of January 2022

Compatibility

The following client versions are compatible with AdminClient version 8.13.10.26901

- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.9.0.17993 Hotfix 2 has stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

Server

- The installation of the SAML service is now optional.

! Customers who use SAML must activate the installation of the SAML service when updating to version 8.13.10. Otherwise, this service will no longer work. If the installation is forgotten, a corresponding message appears in the AdminClient.

AdminClient

- All databases deactivated by an update can be reactivated at the same time.

LightClient in the Web View

- Passwords can be displayed in a list.

Improvements

WebClient

- The selection of tags has been optimised.

LightClient in the Web View

- The button for creating a new password has been positioned more prominently.
- The selection of tags has been optimised.

Fixed

FullClient

- The automatic session timeout now finally disconnects the connection.
- A customized table view is saved permanently.
- The filter for logbook entries shows the correct results for a report.
- Restrictive users can’t change passwords.
- Notes are displayed during the CSV import if a user wants to create organisational units despite lacking permissions.
- CSV Files containing datasets with quotes are also imported.
- The approval process for a seal also works when two users need to approve the seal.

WebClient

- Restrictive users can’t change passwords.
- The approval process for a seal also works when two users need to approve the seal.

AdminClient

- After the update to version 8.13.9, offline licenses could no longer be activated.

Browser Extensions

- Newly recognized credentials are correctly transferred to the WebClient again.
- If the system language is not German or English, English is used.

LightClient

- The automatic session timeout now finally disconnects the connection.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.10.26901-de.msi)

`feb423403492910afc57f774e788621177526bacec64f01ae100ffe77756fe7423846355893cd493ff361`

English Server Setup (pss8.13.10.26901-en.msi)

`5120058ad9a6b6a44842fa2d59ae92e7d736e82fe078da77adb54dcd86a91ddb3093374c7effdd3323434`

German Client Setup (psc8.13.10.26901-de.msi)

db66f4ef3d4874bc73e34d9f1ff664dcb446ef4f4f853beb6c3f9c7d65879f5e47d82f7039155794ba6c5

English Client Setup (psc8.13.10.26901-en.msi)

fff957f3eff180cbdb7413ed8bdfaf6624999955d25ae1043acb0fd68f0c828755abd79f355d0331cf77d

Version 8.13.9.26689

Release

20th of December 2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.9.26689

- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.9, support for version 8.0.1.19032 through version 8.9.0.17993 Hotfix 2 is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient

- If Auto-Login is activated, a new password is automatically saved after it has been entered for the first time.

Server

- The installation is also possible without configuring an SMTP connection.

LightClient in the Web View

- Users can start the seal release process and break a seal after confirmation.

Improvements

FullClient

- Changing a form of multiple, different passwords has been improved.

- The libraries for using smartcards as the first factor have been updated.

Server

- The libraries used for encrypting the data on the HSM have been updated.

> ! Users of a hardware security module are requested to install the current version on a test system first.

Add-ons

- The entry of credentials in the corresponding fields has been improved.
- The default value for the (global) user setting “Automatically send login masks” has been set to activated and the security level was increased to 3. This only affects databases that will be created in the future.

mobile Apps

- Notifications have been integrated to inform the user why an activated second factor may not be requested.

Fixed

FullClient

- The “_archived” folder in the AD can be retrieved via the Import Wizard.
- The content search is also applied to email fields.
- The number of password a tag is used for also includes the passwords in the trash.
- In the history of a record, the user name of an Active Directory user is also displayed instead of just its ID.
- Locally stored .ppk key files linked with a password can be used for SSH connections.

WebClient

- The “_archived” folder in the AD can be retrieved via the Import Wizard.
- The content search is also applied to email fields.
- The number of password a tag is used for also includes the passwords in the trash.
- In the history of a record, the user name of an Active Directory user is also displayed instead of just its ID.

Server

- The messages to the syslog server are also transmitted if it is connected to Password Safe via TCP.
- The IP filter for two-factor authentication now works for all clients, even if the setting “Requires second factor” is activated for a user.
- Changes made to an object in the WebClient are also saved in the logbook.

Add-ons

- Passwords can't – if this option is activated – be copied to the clipboard without specifying a reason.

SSO Client

- If cross-client login is activated, the profile used is also displayed in the SSO Agent after the login in the DesktopClient.

LightClient in the Web View

- When creating a password, additional users can be authorised.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.9.26689-de.msi)
c16c67d226a18f05fffcefa5681d64dba67fcbe86484667b6417ddf0f2d392ab4a200a35c0d12ed2af9b4

English Server Setup (pss8.13.9.26689-en.msi)
11624ca1aeecffcdf02670d4361d2c7a4a4f175fe06acec299b2509667bd434a44ad86e1c3e12171e35ea

German Client Setup (psc8.13.9.26689-de.msi)
aa3ea99e70520eb77872e354f18b4fe5ef6c2424bb14fac25831d9c888b1f34f7c519158878d0d309ae7f

English Client Setup (psc8.13.9.26689-en.msi)
5bd9fb8c456584b35c368ab0dca62df9f93f1246c0d53abe381e238b99d6898162f8bef03919b71a7a08d

Version 8.13.8.25983

Release

2nd of December 2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.8.25983

- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

Fixed

Users who were temporarily authorised to access an object could still see this object after the end of the authorisation, but could no longer access the contents.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.8.25983-de.msi)
`4de754247c1f22bea5e12ea4725bb0145d1d2864f1d5097d979e222b546da0adb7608406c3e3a6222f759`

English Server Setup (pss8.13.8.25983-en.msi)
`59f2af1735b0e9ec51ed5ace144fb119ed08fc8c972603ba17ce37792576923d221d148d8ebd3ff420da2`

German Client Setup (psc8.13.8.25983-de.msi)
`7676b976e084d899ffce2eb5abc50321c49aa322e56f724f8af1f1cdc8551c53f4a1e14aef6c532bcc6d0`

English Client Setup (psc8.13.8.25983-en.msi)
`425a99283fa667554ec1909a4b2a7783a49341ba5ffc24caeee980ea8df48f5fd16683f0f4133572f5461`

Version 8.13.7.25979

Release

25th of October 2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.7.25979

- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

> ! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

LightClient and LightClient in the Web View

- Users can edit or delete additionally added fields.

Enhancement

FullClient

- When importing a CSV file, it is automatically checked for the encoding used.
- Passwords can be moved from the edit view to the Trash.

WebClient

- Passwords can be moved from the edit view to the Trash.

LightClient and LightClient in the Web View

- Passwords can be moved from the edit view to the Trash.

AdminClient

- PKI certificates without the 'KeyEncipherment' flag can now also be used as a second factor.

Fixed

FullClient

- One-time passwords can also be created without a secret.
- The permissions can now also be reduced again using a template.

Server

- The message in case of a missing connection to the SQL server has been optimised.

AdminClient

- The message in case of a missing connection to the SQL server has been optimised.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.7.25979-de.msi)
6f30f9f0989ad541ecf0da2971ce3adbb0d474e06bc7ccc8c80220666a09a43ace40abd064598da438823

English Server Setup (pss8.13.7.25979-en.msi)
ea6c16721fc2db12f88478783922e767dfaa463f88e7a55beaff4b3dc07391e995344627c31acb34e3124

German Client Setup (psc8.13.7.25979-de.msi)
fe1f4e7d331691a5683463550fc024c5e6e70a45b8a912befec4af822618485009117f5c45efda37badda

English Client Setup (psc8.13.7.25979-en.msi)
fb7d6660a05d6550b980ee0214f4b7ad3ab3afea14fdf8de2904caade5009e4de3412cc9f9a75a7584b61

Version 8.13.6.25933

Release

11th of October 2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.6.25933

- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

> ! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient

- Deactivated users are now only displayed in the Organizational Units module

WebClient

- Deactivated users are now only displayed in the Organizational Units module

LightClient

- When creating a password, users can choose from different forms and add additional fields.

LightClient in the Web View

- When creating a password, users can choose from different forms and add additional fields.

MSP

- The database name is permanently visible at each customer.
- The name of the client as well as the database can be changed.

Improvements

LightClient in the Web View

- The search field as well as the search results can be reset via a button.
- Adding new tabs has been made more intuitive.
- The tab “all passwords” is always displayed by default.

Fixed

FullClient

- The Password Reset also works with the https:// protocol.
- Active Directory users in end-to-end mode are imported only if the SMTP connection is working.
- The sealing of a password has been accelerated.
- The quick search, as well as the filter search, shows all objects that contain the search term.
- An RDP connection in the separate window can be closed using the “Close” button.

WebClient

- When a user is prompted to change the password, an existing password policy takes effect.
- With the user setting “Edit tab after opening” disabled, some options were missing in the menu of a password field.
- Active Directory users in end-to-end mode are imported only if the SMTP connection is working.
- The sealing of a password has been accelerated.
- The quick search, as well as the filter search, shows all objects that contain the search term.

Android App

- Synchronization now works without a realtime connection.

iOS App

- Synchronization now works without a realtime connection.

API

- Passwords are transmitted encrypted by the JavaScript SDK.

MSP

- Despite the activated option, no automatic reports could be created.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.6.25933-de.msi)

```
15972f7ca3bd6f535599cc587c21b8132a3bab5171d4f05f7ad09e4a2c216d61aa87bf066a8316487efc3
```

English Server Setup (pss8.13.6.25933-en.msi)

```
71beba69780646aead27a8e20315768dfb73c205493f4ed7a84214e13796fc877385acc4d9251625841a2
```

German Client Setup (psc8.13.6.25933.msi)

1017e3e794bdc70f44492cc28d63a99a8175cc766c5e352ea6693eb9110f52ef575a6a4e3871abf57c925

English Client Setup (psc8.13.6.25933-en.msi)

6a3db708f9e87ddc88a014dce6c6b15ed84b889b9672f3b1ebe9698188f6cebb8006940919190965bc59a

Version 8.13.5.25731

Release

13.09.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.5.25731

- Windows Client Version 8.13.5.25731
- WebClient Version 8.13.5.25731

> ! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient

- It is possible to have reports generated on the changes made by Active Directory imports.
- The function "Exclude last X passwords" has been removed from the password policies.
- The login process has been adapted to make it more difficult for possible attackers to guess valid usernames.
- Users can duplicate passwords only if they are also authorized to the corresponding form.
- When creating a new AD profile, the two flags "Secure" and SecureSocketsLayer" are activated by default.
- Active Directory objects can now be created or deleted in Password Safe simply by belonging to an Active Directory group.
- The email notifications include the organisational unit where the Secret is located.
- The tab with the list view in each module can't be closed.

WebClient

- The login process has been adapted to make it more difficult for possible attackers to guess valid usernames.
- The opening and closing of the filter have been optimised and the mobile view adapted.
- Users can duplicate passwords only if they are also authorized to the corresponding form.
- A direct search for Active Directory objects has been integrated.
- Active Directory objects can now be created or deleted in Password Safe simply by belonging to an Active Directory group.
- The email notifications include the organisational unit where the Secret is located.
- The tab with the list view in each module can't be closed.

Server

- TLS 1.2 and 1.3 are the two standard versions for encrypted communication.
- If a user changes his password, all sessions that are still open are terminated.
- The Discovery Service Scan has been optimised.
- Password Safe is now DualStack capable.

AdminClient

- The timeout of an active session can now be set individually for each client.

LightClient

- The login process has been adapted to make it more difficult for possible attackers to guess valid usernames.

LightClient in the Web View

- The login process has been adapted to make it more difficult for possible attackers to guess valid usernames.

Improvements

FullClient

- SSH connections using a key file are easier to configure.

Browser Extensions

- If the IP filter is activated, a possible second factor is no longer queried.

Fixed

FullClient

- The default form can be reset in the global user settings.
- The DesktopClient only prevents Windows from shutting down if changes are not saved.
- The widget “My Team” in the dashboard shows all members of the selected organisational unit.
- A translation error in the report “Logbook entries” has been corrected
- RDP sessions in the external window can also be displayed in full screen.
- When importing passwords, only the user himself has permission for the passwords.
- The keyboard shortcuts work again in RDP sessions.
- The cross-client login works again.
- Authentication using Kerberos is possible again.
- Notifications can only be seen by the user who configured them.

WebClient

- The default form can be reset in the global user settings.
- The form of an existing password can only be changed with the right “Authorise” or “Delete”.
- The quality of a password is checked again when the form is changed.

- The export of passwords or organisational units has been optimised.
- When selecting possible forms for creating a password, you can navigate through the forms using the scrollbar.
- During the AD import, all sub-objects are also selected when an object is selected and then synchronised.
- Authentication using Kerberos is possible again.
- The link to the Firefox Add-on Store now uses the https:// protocol
- Notifications can only be seen by the user who configured them.

AdminClient

- Databases deleted in the MSSQL Server Management Studio are deactivated in the AdminClient.

Browser-extensions

- Logging in via the SSO agent works if the browser extension is configured accordingly.
- The auto-fill via the SSO Agent has been accelerated.

SSO Client

- The cross-client login works again.
- The auto-fill has been accelerated.

LightClient

- Authentication using Kerberos is possible again.

LightClient in the Web View

- In the password generator – if any have been configured – the corresponding password policies are available for selection.
- Users with an exclusive LightClient license can move passwords to other organisational units.
- Authentication using Kerberos is possible again.
- Users with LightClient-only licenses can tag passwords.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.5.25731-de.msi)
`56cb7260d587d50afceca87ef53772c3106ec192de88695b247495022c768e03ac9a6a4e5e273f74c98d4`

English Server Setup (pss8.13.5.25731-en.msi)
`05fb18e29549b94f8b238cbe1904d44240af7bcd48a802d64ea9bb50d6e9149daffc46ceae942771de772`

German Client Setup (psc8.13.5.25731.msi)
`cd4a82995f45d19d1d4aa306025e296b1142fbd74c0da1ffbd2b8a3078ffeb9a58bbcb86f732d9f411c5f`

English Client Setup (psc8.13.5.25731-en.msi)
`473ef56a4d9f1cf12800437bdf869cbf7a5b4993079f9cd401206344c07285838c02e75d108f68fa62de1`

Version 8.13.4.25228

Release

16.08.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.4.25228

- Windows Client Version 8.13.4.25228
- Windows Client Version 8.13.3.25194
- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.4.25228
- WebClient Version 8.13.3.25194
- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

LightClient in the Web View

- The TAGs are also displayed in the quick view.

Improvements

FullClient

- SSH connections using a key file are easier to configure.

Fixed

FullClient

- Seal templates can be edited even if a role involved in the sealing process has been deleted.
- The search again looks for the exact term. The fuzzy search for similar terms can be activated in the filter.

WebClient

- Roll members could not release a seal.
- Seal templates can be edited even if a role involved in the sealing process has been deleted.
- The search again looks for the exact term. The fuzzy search for similar terms can be activated in the filter.

MSP

- The name of a database can also contain a hyphen.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.4.25228-de.msi)
763c7cc99f131083d74427c67b817aa867e7934c8620bc255efbc5682e6f6baf43b0050f2f3db26f59903

English Server Setup (pss8.13.4.25228-en.msi)
fed9f56f15527aa0e7ba78be13c2a13b9fc32047bab78eeb64bb61656ee611e23ed23f6d8b2d8a8b3f8ad

German Client Setup (psc8.13.4.25228.msi)
1f339736e763fb50235aa4328110a3b022f4b22e9ad51c9894aca60fe10154f08f9242845ce684847427

English Client Setup (psc8.13.4.25228-en.msi)
af6c13f9910d5b6f5bc9bc499c1673878d5825cfed3dee953d8b05c2c3491a68f3b012948334416ead64d

Version 8.13.3.25194

Release

02.08.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.3.25194

- Windows Client Version 8.13.3.25194
- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.3.25194
- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

! With the release of 8.13.0, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

Fixed

FullClient

- The QR code for setting up the second factor is displayed correctly.
- In the Active Directory Import overview, all nested groups are also displayed.
- Password Safe checks the validity of the server certificate correctly again
- The check of permissions when editing passwords and forms have been optimised.

WebClient

- When deselecting groups in the Active Directory Import overview, all objects underneath are also deselected.
- In the Active Directory Import overview, all nested groups are also displayed.
- Double-clicking on a document starts the download of this document.
- The check of permissions when editing passwords and forms have been optimised.

Server

- The application server does not crash if the IDP server could not be started.

Browser-extensions

- If the browser extension is activated, the internal password manager of the browser is deactivated.

> ! After updating to the latest version of the browser extension, the message “To re-enable, accept the new permissions “ appears. By confirming, the internal password manager is deactivated and the browser extension can be used again.

mobile App

- The field for entering an OTP no longer disappears when switching to an Authenticator app.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.3.25194-de.msi)

```
763c7cc99f131083d74427c67b817aa867e7934c8620bc255efbc5682e6f6baf43b0050f2f3db26f59903
```

English Server Setup (pss8.13.3.25194-en.msi)

```
fed9f56f15527aa0e7ba78be13c2a13b9fc32047bab78eeb64bb61656ee611e23ed23f6d8b2d8a8b3f8ad
```

German Client Setup (psc8.13.3.25194.msi)

```
1f339736e763fb50235aa4328110a3b022f4b22e9ad51c9894aca60fe10154f08f9242845ce6848474279
```

English Client Setup (psc8.13.3.25194-en.msi)

```
af6c13f9910d5b6f5bc9bc499c1673878d5825cfed3dee953d8b05c2c3491a68f3b012948334416ead64d
```

Version 8.13.2.25151

Release

05.07.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.2.25151

- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

> ! With the release of 8.13, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient and WebClient

- The permissions of DB admins on a password remain if the password is moved by a normal user.

Fixed

FullClient

- Active Directory users can also be imported without a stored e-mail address.

WebClient

- Active Directory users can also be imported without a stored e-mail address.
- After logging in to the WebClient via the browser extension, a user could not change his password.

Server

- Cross-client login works when both IP addresses and DNS entries are stored as subject alternative names in the connection certificate.

AdminClient

- A database can also be activated if the SQL Server collation is case sensitive.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.2.25151-de.msi)

8c2d446692aaf2c42643aacfa930202adb12040c38d7c24a48ee6013346539e1058f40d48bee0ac89e0c2

English Server Setup (pss8.13.2.25151-en.msi)

e06926d06dc961a100f524aa9be1f0923e47b03ec4e3ffa43baa7d43bdf9b4052a20bd317926f25a4574b

German Client Setup (psc8.13.2.25151.msi)

8b50af0a5250d18f3434f72a32c5daa0d51d4eeae0fba0031daf4c58d4b38c91f2b8503aa10aa10524283

English Client Setup (psc8.13.2.25151-en.msi)

e06926d06dc961a100f524aa9be1f0923e47b03ec4e3ffa43baa7d43bdf9b4052a20bd317926f25a4574b

Version 8.13.1.25117

Release

18.06.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.0.25027

- Windows Client Version 8.13.1.25117

- WebClient 8.13.0.25027
- WebClient 8.13.1.25117

> ! With the release of 8.13, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient and WebClient

- Additional connection settings (AuthenticationTypes Enumeration) can be used for the connection of the Active Directory.
- The predefined values of some standard settings have been adjusted. The following changes only become active for new databases.
  - "Download website icon automatically" has been changed from inactive to active.
  - "Document history" has been changedfrom inactive to active.
  - Include subordinate organisational units in LightClient" has been changed from inactive to active.
  - Remove creator from permissions for new objects if the creating user is authorised via a role" has been set from inactive to active.
  - Browser Addons: Exact Domain Check" was set from inactive to active.
  - Can create individual passwords in LightClient" has been changed from inactive to active.
  - Show Notification Module" has been changed from inactive to active.
  - Security level for "Show records as expiring soon if their remaining days are less than" has been lowered to level 1.
  - Security level for "Standard form" has been lowered to level 1.
  - Security level for "Customisable window title" increased to level 5.
  - Security level of all permissions in the category "Footer" has been increased to level 5.
  - "Validity in days of mobile database without synchronisation" has been reduced to 7 days.
  - "Maximum size in MB" has been reduced from 100 to 10.
- The predefined values of some default settings have been adjusted. The following changes become active for both new and existing databases.

- “Can use filter negation” was changed from inactive to active and removed from the settings.
- The module “Footer” was removed from the global user settings.
- “Empty user field after adding” was set from active to inactive and removed from the settings.
- “Permission search: Add step by step” was set from active to inactive and removed from the settings.
- “Clear Clipboard on Minimise” has been set from active to inactive and removed from the settings.
- The user setting “Browser Addons: Show Password” is now in the password settings.

Fixed

FullClient

- Users who are not displayed in the activated LDAP filter are automatically deleted during synchronisation.
- The verification of passwords associated with a password reset no longer worked due to a code adjustment in version 8.13.
- Some users could not log in with the reference to “An item with the same key has already been added”.

WebClient

- Users who are not displayed in the activated LDAP filter are automatically deleted during synchronisation.
- The verification of passwords associated with a password reset no longer worked due to a code adjustment in version 8.13.

Server

- Custom scripts for password reset now use SecureString as CredentialPassword.

AdminClient

- Login to the AdminClient also works if ’0.0.0.0’ (IPv4) or ‘::0’ (IPv6) is used as IP address.

Setup Check hashes (SHA-512 Hash)

German Server Setup (pss8.13.1.25117-de.msi)
`eaad17bd5ff3639dd330e544d2c7e044c2efabdc3334ca3c3551f51e8fbb8574a8f2239e9fa5a4a64ef6f`

English Server Setup (pss8.13.1.25117-en.msi)
`0eb35d304cf446f910edec4c40bc709642d77149f191797eff8c5f7d2bf2f5065b140062b1c72fa968c21`

German Client Setup (psc8.13.1.25117.msi)
`32993a01592a56eb2be8c41690438c778aa28d14d4acdce00f447b2b5c9d1f42be3f67c235a957a321b13`

English Client Setup (psc8.13.1.25117-en.msi)
`434d269289d730125026c1989799abdcc5d0b7eb6ea3c882f7956872c9059ccb215a1c0a711a582f3b11d`

Version 8.13.0.25027

Release

14.06.2021

Compatibility

The following client versions are compatible with AdminClient version 8.13.0.25027

- Windows Client Version 8.13.0.25027
- WebClient 8.13.0.25027

> ! With the release of 8.13, support for version 8.0.1.19032 through version 8.6.0.15386 hotfix is stopped. The reasons for this are that these versions are outdated versions that no longer meet today's security standards.

New

FullClient

- A new graphical user interface "Office 2019 Colorful" has been added.
- Passwords linked to a document are displayed in the footer area of the document.
- Graphical adjustments to the interface have been made.
- Passwords that have been moved to the trash can be deleted permanently.
- Passwords that have been moved to the trash can be restored.
- Deleted passwords are now moved to a trash can
- The opened tabs are now more clearly marked.
- Documents can be linked with passwords via the "Documents" module.
- The user can see at a glance in their account which devices they are logged in with.
- The notifications have been improved.

WebClient

- New Config Headers for the web server have been implemented.
- The notifications in the seal process link to the seal view of the relevant password.
- When a notification is selected, a new tab opens with detailed information.
- The number of selected records is displayed in the list view in the "Organisational Units" module.
- Passwords linked to a document are displayed in the footer area of the document.
- The passwords can be sorted alphabetically and by date of change in the WebViewer.
- The mailing for a seal request contains a link to the seal overview.
- Passwords that have been moved to the trash can be deleted permanently.
- Passwords that have been moved to the trash can be restored.
- Deleted passwords are now moved to a trash can

- The opened tabs are now more clearly marked.
- Documents can be linked with passwords via the “Documents” module.
- The user can see at a glance in their account which devices they are logged in with.
- The notifications have been improved.

Server

- New Config Headers for the web server have been implemented.
- Users that are deleted in the Active Directory will also be deleted in Password Safe during the next synchronisation.
- Active Directory objects that cannot be imported are greyed out when configuring the Active Directory import.
- Active Directory users can also log in to the Password Safe with their “User Principal Name”.
- A new logbook entry “restored” for passwords has been integrated.
- A password policy must be followed when creating new users.
- If a user is deactivated or deleted, all open connections are closed.
- The user name of deleted users is still displayed in the logbook.
- QR Codes für MFA werden innerhalb von Password Safe generiert.

AdminClient

- In the list of database users, a tool tip indicates the type of user via mouse over.
- Beim Anlegen einer Datenbank muss für den Datenbank Administrator eine E-Mail-Adresse hinterlegt werden.

Add-ons

- The browser extension icon indicates when the user is logged out.

Android App

- The log files can be shared via other apps in case of problems.

iOS App

- The log files can be shared via other apps in case of problems.

SSO Client

- If a user is logged in to a database and selects it in the dropdown, no login screen appears but a note that the user is already logged in.

OfflineClient

- Users can search and sort by organisational units.

LightClient

- Passwords that have been moved to the trash can be deleted permanently.
- Passwords that have been moved to the trash can be restored.
- Deleted passwords are now moved to a trash can
- The notifications have been improved.

LightClient in the Web View

- The details of a password can be displayed.
- Passwords that have been moved to the trash can be deleted permanently.
- Passwords that have been moved to the trash can be restored.
- Deleted passwords are now moved to a trash can
- The notifications have been improved.

MSP

- Customer management has been integrated into the AdminClient
- Test customers can be created, managed, deactivated and deleted in the customer administration.
- The number of available licences can be set individually for each customer
- In the customer administration, customers can be created, managed, deactivated and deleted.
- Additional options can be booked individually for each client.
- A dashboard has been integrated for information on active licences and booked options including the resulting costs for each customer.

Improvements

FullClient

- The configuration of the email notifications is now located in the account settings.
- If a user does not have the right to create an object in an organisational unit, a corresponding error message appears.
- The option “Automatically use last filter” has been optimised.
- The search has been optimised: Similar sounding values will now also be displayed.
- The error handling when importing passwords has been optimised
- The search for values in the user settings has been optimised.
- The use of smart cards for passwordless login has been optimised.
- The use of the wizards has been optimised.
- The validation of the values in the user settings has been improved.

WebClient

- The configuration of the email notifications is now located in the account settings.
- If a user does not have the right to create an object in an organisational unit, a corresponding error message appears.
- The configuration of the expiry date of a password has been optimised.
- The search has been optimised: Similar sounding values will now also be displayed.
- The search for values in the user settings has been optimised.
- The use of the wizards has been optimised.
- The validation of the values in the user settings has been improved.

Server

- The Active Directory import has been improved. When adding new users to a role, the status quo of the already associated users remains untouched.
- If a user does not have the right to create an object in an organisational unit, a corresponding error message appears.

- The option “Automatically use last filter” has been optimised.

AdminClient

- The use of the wizards has been optimised.

LightClient

- The search has been optimised: Similar sounding values will now also be displayed.

LightClient in the Web View

- The search has been optimised: Similar sounding values will now also be displayed.

Fixed

FullClient

- A notification can be sent for passwords that have expired or will soon expire.
- The progress bar shows the remaining time in the form of a coloured bar.
- The import of passwords has been improved.
- The quick search in the structure view has been optimised.
- Standard forms can now also be set and reset individually for each user.
- Very long passwords – for example, RSA private key – no longer crash the client.

WebClient

- When a seal request is reset, the user name of the requesting user is displayed in the confirmation.
- The quick view can be closed using the“ESC” key.
- The distinction between active and inactive elements during the AD import has been improved.
- The quick search in the structure view has been optimised.
- Log in with IPv& addresses is possible even if the database firewall is activated.
- Standard forms can now also be set and reset individually for each user.
- The fields in an Active Directory profile can only be edited with the appropriate right.

Server

- A notification can be sent for passwords that have expired or will soon expire.
- Log in with Google Authenticator as the second factor also works if the first number of the token is a zero.

AdminClient

- The database benchmark test also works for databases with special characters in the name.

Add-ons

- Users with special characters can log in to the addon
- Passwords with password masking and seal are entered into the corresponding websites when the seal is broken.

Android App

- Passwords can be moved to other organisational units.
- Opening the blacklist no longer causes the application to crash.

iOS App

- The QR Code scanner has been adapted.
- Passwords can be moved to other organisational units.

Version 8.12.1.22757

Release

01.02.2021

Compatibility

The following client versions are compatible with AdminClient version 8.12.1:

- Windows Client Version 8.12.1
- Windows Client Version 8.12.0

- WebClient version 8.12.1
- WebClient version 8.12.0

- Password Safe Mobile Apps 1.19

Updating to **Version 8.12.0** requires **.net version 4.8.0** or newer on both the application server and clients. Therefore **check** if this is given on all relevant devices **before installation**.

New

Add-ons

- Users with activated FIDO2 can log in to the addon with their Active Directory password.

Fixed

FullClient

- Users with special characters in their username can configure any activated second factor.
- Users whose profiles are distributed via registry entries can log in again.
- A user with a smartcard as the first factor for login cannot configure an automatic login.

WebClient

- Users with special characters in their username can configure any activated second factor.
- The structure view in the “Passwords” module is displayed again.
- Users with special characters in their names and passwords can be created.

AdminClient

- Users who use a self-created certificate with only the server name but no associated IP address can open the database settings.

Version 8.12.0.22707

Release

21.01.2021

Compatibility

The following client versions are compatible with AdminClient version 8.12:

- Windows Client Version 8.12.0
- WebClient version 8.12.0
- Password Safe Mobile Apps 1.19

> Updating to **Version 8.12.0** requires **.net version 4.8.0** or newer on both the application server and clients. Therefore **check** if this is given on all relevant devices **before installation**.

New

FullClient

- When an organisational unit is finally deleted, the view is automatically reloaded.
- A typing assistance for passwords has been integrated.
- When configuring the Google Authenticator, the secret is also displayed.
- User settings have been extended by the options for password-less login.
- Users can log in using a smartcard.
- After entering the username, the corresponding profile picture is displayed – if stored.
- When a new database certificate is created, all login factors encrypted with it are reset.
- The session list of connected devices shows Android and iOS apps including the respective version.
- The right “Apend” can be selected only in the rights filter of the “Organisational units” module.
- Open tabs can be closed using “CTRL + W” or the middle mouse button.
- Records can also be duplicated without the permission “can create personal records” as long as the target is not the own user.
- Tooltips for password import have been added.
- User settings can also be inherited to Active Directory profiles.

WebClient

- A typing assistance for passwords has been integrated.
- Users can log in using a FIDO2 token.
- User settings have been extended by the options for password-less login.

- After entering the username, the corresponding profile picture is displayed, if stored.
- The secret shown during the configuration of the Google Authenticator can be copied to the clipboard.
- When a new database certificate is created, all login factors encrypted with it are reset.
- Configuration options for password notifications have been adapted.
- When a SAML application is started, a notification is triggered.
- The right “Apend” can be selected only in the rights filter of the “Organisational units” module.
- User settings can also be inherited to Active Directory profiles.

AdminClient

- If a database certificate no longer exists, a new one can be created.
- When creating a connection certificate during the basic configuration, several alternative applicants can be entered.
- The session list of connected devices shows Android and iOS apps including the respective version.
- Networks can be specified in which a configured second factor is not required for login.
- An alternative Crypto Service Provider can be specified for logging in using a smartcard.

Add-ons

- The login process of the add-on has been optimised.
- The error message for autofill in case of multiple passwords for one website has been adapted.

Android App

- A typing assistance for passwords has been integrated.
- A password generator for creating secure passwords has been integrated.
- Users can create new objects in the tab “All passwords” and assign them to themselves.

iOS App

- A password generator for creating secure passwords has been integrated.
- Users can create new objects in the tab “All passwords” and assign them to themselves.

h4 LightClient

- A typing assistance for passwords has been integrated.

Improvements

FullClient

- The display of tags in the list view has been optimised.
- The process for resetting the second factor – if activated – has been optimised.
- If two AD profiles with the same domain exist and one of them is deleted, the second one will still work.
- The configuration of the second factor – if required – has been optimised.
- If a user wants to authenticate, a configured session timeout is ignored.

WebClient

- The process for resetting the second factor – if activated – has been optimised.
- Configuration of the second factor – if required – has been optimised

AdminClient

- The export of database certificates has been optimised.

Add-ons

- The automatic filling out of login masks has been optimised.

LightClient

- If a user is searching for an organisational unit that is already open, he switches directly to the corresponding tab.

LightClient in the Web View

- The view of the LightClient in the web view has been optimised for mobile devices.

Fixed

FullClient

- The conext menu in the list view has been optimised.
- The configuration of a one-time password has been optimised.
- The configuration of a password reset has been optimised.
- The configuration of the Discovery Service Tak has been optimised.
- The version from which the option is available is shown in the user rights.
- The configuration of the filter has been optimised.
- The colour themes “Office 2019 Black”, “Dark Gray“and “Metropolis Dark” have been adjusted.
- Notifications for objects of other users can only be enabled with the “Writing” permission.
- After successful import of passwords, the view is automatically reloaded.
- The time until automatic logout of the WebViewer has been limited to a maximum of one day.
- Each member of a role can add other users to the role independet of the permission he has to the user.
- When switching to another module, any filter settings are no longer applied.
- The seal overview has been optimised.
- The clipboard action in the ribbon are only available with a selected password.
- The configuration of system tasks has been optimised.
- The buttons for overwriting and inheriting permissions are only displayed if the permissions have been edited.
- When moving passwords to other organisational units, the respective owner rights are retained.
- The tag management in rights templates has been optimised.
- If more than one instance is opened, all further instances remain connected to the application server until logoff.
- In case of a SSO application with several associated passwords, you can choose between them.
- The last active second factor can only be deactivated if the option “Second factor is required” is also deactivated for all organisational units.In the “Roles” module, the list view is automatically

updated after editing a role.
- If a document saved in Password Safe is edited and exceeds the maximum permitted file size, a corresponding error message appears when saving.
- If the “Edit Tab after opening”“ option is disabled, the two options “Remove configuration” and “Enter application” in the ribbon are enabled when “Edit” is clicked in the “Applications” module.
- If the main window is scaled, the footer area is also scaled accordingly.
- When trying to print a sealed password despite having print permission, a corresponding error message appears.
- It is not possible to assign users or organisational units to a single user with drag & drop.
- When a new document is created, the organisational unit of the creator is prefilled.
- Password policies cannot be set for multi-line text fields in passwords.
- The view of the import summary has been optimised.
- The report view in the FullClient has been optimised
- The form field for the user password has been adapted.
- If a user tries to remove another user’s permission key in “Permissions”, an error message is displayed stating that this action is not possible.
- If no application is selected, the “Connect password” button is disabled.
- Temporary permissions for ‘Everyone’ are now saved correctly in permission templates.
- A user can see a sealed password in the quick view when he is not affected by the seal.
- Names of the filter groups in the “Discovery Service” module have been harmonised.
- If a selection of forms is to be printed in the list view, the number of printable form fields is displayed in relation to the number of all fields with read access.
- If the user right “Can carry out batch processing for permissions based on a filter” is activated, the rights of a user are reduced for all filtered passwords.
- When importing organisational units, they can only be subordinated to other organisational units.
- Moving an object generates a new logbook entry “Moved”.
- During Copy & Paste of hostname and servicename in a script for a password reset all spaces are removed.
- The tab name of a newly created object is retained if “Reload all data” is clicked during the creation.
- When you create a new report, the tab name is named accordingly.
- The counting of user licenses when using Active Directory has been adjusted.
- The process of capturing applications has been adapted.
- If the seal for a password with protection is broken, a corresponding note on the protection appears.
- The context menu in the module “Passwords” has been adapted.
- Users without appropriate rights can’t predefine rights for an organisational unit.
- New columns have been added to the system task list view.
- The filter group “Tags” has been adapted.
- When editing an open seal, you will be prompted to assign a new password.
- In the module“Notifications”, seal templates can be opened directly using the “seal template” button.
- The preview of a document can only be opened with the appropriate right.The context menu in the user rights /user settings has been adapted.
- The configuration of the “on use” notification has been extended.
- The summary of an Active Directory import shows the correct assignment of users to the corresponding organisational units.
- An error handling for final deletion of users has been adapted.

- Documents can also be filtered by file name extension.
- Changed form field types are recognized during a form change.
- The filter group “Rights” in the module “Passwords” have been adapted.
- If users in the Active Directory are moved to another organisational unit, they will also be moved accordingly during the next synchronisation.
- The behavior of the buttons in the ribbon in all modules has been harmonised.
- Only users with the permission “Add” can create new organisational units during an Active Directory import.
- When empty groups are imported from the Active Directory, the corresponding permissions and memberships are set.
- A user cannot edit the memberships of other users in roles without appropriate rights.
- The scaling options of window size of RDP applications have been adapted.
- When downgrading to an edition with lower functionality, modules that are not included in that edition will no longer be displayed.
- The input mask for new password guidelines has been adapted.
- If a password is opened whose form has been changed in the meantime, a message appears when closing the form to indicate whether the changes should be discarded.
- In formulars, new fields can be added with the name of deleted form fields.
- The objects displayed in a filter group are updated when a saved filter is opened.
- The local user “.\user” of the target system now also works for RDP connections.
- Invalid characters in the name of a multi-factor authentication are filtered out.
- If an Active Directory synchronisation was not successful, a corresponding error message is displayed.
- The functionality has been optimised when minimising RDP applications in Password Safe.
- When an Active Directory user is imported, the associated description is also imported.
- Any number of passwords can be assigned to an application without the client freezing when the passwords are displayed.If the license module is missing, an error message is displayed in the logbook for the corresponding system task.
- If a user edits the permissions of several roles simultaneously, his membership status remains unchanged until he explicitly edits it.
- An active filter is reset when creating a new report.
- Keepass folders can only be imported in organisational units, not in users.
- For web applications the URL field is a mandatory field.
- When Windows is shut down, any active SSO Agent or Full Client Sessions is automatically terminated.
- The filter group “Validity state” has been optimised.
- No error message appears when viewing the metadata of linked documents.
- Despite repeated double-clicks on a notification / logbook entry, the object is only opened once.
- When importing applications, the correct date for “valid until” is imported.
- A click on the blue arrow opens the context menu for editing the field contents of a password regardless of whether the tab can be edited immediately or only by clicking on “Edit” in the ribbon.
- Negating an organisational unit filter also displays users outside organisational units.
- The number of data records has no influence on the login to the WebViewer.
- Adjusting the window size of an RDP or SSH connection no longer causes logbook entries.
- Filter adjustments made for a report are retained after the report is saved.
- Offline synchronisation is performed according to the possible settings.
- The checkbox “Restricted user” is greyed out if the “Edit” right is missing.
- Logbook entries can be filtered by “Execution started” or “Execution finished”.

- When a field type is changed in a form, the corresponding default value changes too.
- Import of CSV files reworked
- The preview of the import wizard in all modules has been harmonised.
- Notification messages in form fields have been adapted.
- Deactivated users with active MFA can log into Password Safe after activation via synchronisation.
- Open RDP connections do not disconnect when switching to another module and back.
- Shortcuts “CTRL+ALT+S” and “CTRL+ALT+V” enter username and password in the corresponding fields.
- Buttons to change passwords and configure OTPs are grayed out for restrictive users.
- The context menu has been adjusted systemwide.
- The sisplay error in read-only mode of a Discovery Service task has been fixed.
- When entering the secret for a one-time password, the focus is set on the field.
- With the appropriate permission “Can create new RDP applications”, RDP applications can be duplicated.
- The column editor now also works with a scaling greater than 100%.
- The notification of an already broken seal is also displayed when editing an affected password.
- The seal release process has been optimised when using short validity periods.
- The cross-client login remains active when opening the OfflineClient.
- When a user adjusts permissions on passwords using group permissions, an error message appears for the passwords to which the user has no permission.
- When creating a new role using “CTRL+N”, the focus in the tab is set to the first input field.
- The calculation of the password quality has been optimised.
- Passwords can only be duplicated with the appropriate right “can create passwords”.
- Users can search for tags and assign them to objects even without the right “Can manage tags”.

WebClient

- The sealing process has been optimised.
- When moving passwords to other organisational units, the respective owner rights are retained.
- Notifications are also displayed in the mobile view of the browser.
- The tag management in rights templates has been optimised.
- In case of a SSO application with several associated passwords, you can choose between them.
- Graphical adjustments in the Active Directory profile have been made.
- The last active second factor can only be deactivated if the option “second factor is required” is also deactivated for all organisational units.
- The WebClient can be reloaded using “F5”, even if an organisational unit is selected in the “Organisational Structure” module.
- If there are objects in a list for which the print permission is not available, a corresponding error message appears when you try to print the list.
- Error messages are only visible if a user is logged in.
- When a seal is broken, the corresponding password is displayed in the notification module when the “Password” button is clicked and the seal overview is displayed when the “Seal” button is clicked.
- If a user tries to remove another user’s permission key in “Permissions”, an error message is displayed stating that this action is not possible.
- Search results in the “organisational structure” module are displayed as soon as you start typing the search term.
- Multiple tags cannot be edited at the same time.

- Authorized users can print sealed passwords.
- If no application is selected, the “Connect password” button is disabled.
- If the user setting “Mark notifications as read when opening them” is activated, notifications opened in the quick view are marked as read.
- The description field is displayed in the quick view of all items.
- The quick view of notifications shows the date and time.
- Moving an object generates a new logbook entry “Moved”.
- The context menu in the “Notifications” module has been modified.
- The quick view in all modules has been harmonised.
- The button “Delete passwords” in the ribbon in the module “Applications” is only active if there are corresponding linked passwords.
- In the case of nested organisational units, the topmost one cannot be moved to a lower-level one.
- Duplicated applications are assigned to the organisational unit or user that duplicates them.
- Applications can be marked as public or personal.
- Color differentiation of temporary permissions have been adapted.
- The sorting of the toolbar groups has been adapted.
- If users in the Active Directory are moved to another organisational unit, they will also be moved accordingly during the next synchronisation.
- The grouping of passwords by date has been optimised.
- When downgrading to an edition with lower functionality, modules that are not included in that edition will no longer be displayed.
- When creating a new document in an organisational unit, an existing standard rights template should be selected and entered accordingly.
- The protocol “lns://” is supported.
- The list view in the modules “Notifications” and “Logbook” has been harmonised.
- When creating a new organisational unit, it will be displayed in the structural filter when switching to the “Passwords” module.
- Any number of passwords can be assigned to an application without the client freezing when the passwords are displayed.
- The behavior when clicking on notification icon in the mobile view has been adjusted.
- The view in the module “Notifications” has been customized.
- Users can only see the settings of other users with the right “Authorise”.
- When saving with “ALT + S”, all form fields are saved.
- The text about the number of selected objects in the list view has been adjusted.
- Multi select using “SHIFT” and arrow keys works in all modules.
- Editing of rights will only take effect after saving.
- For web applications the URL field is a mandatory field.
- The filter group “Validity state” has been optimised.
- Use “ALT + S” to save new objects in the “Organisational Units” module.
- Newly created users or organisational units are marked in the list view after saving.
- When a document is created, a log entry “New” is written.
- Overlong texts are wrapped in delete confirmation.
- Negating an organisational unit filter also displays users outside organisational units.
- Tooltips when creating a new document corrected.
- Buttons to change passwords and configure OTPs are grayed out for restrictive users.
- Width of the quick search have been adjusted.
- The calculation of the password quality has been optimised.
- Users can search for tags and assign them to objects even without the right “can manage tags”.

Server

- The migration from V7 to V8 has been optimised.
- LightClient licenses are only counted in the Enterprise Plus Edition.
- Improved license validation for virtual machines without hardware IDs.
- When importing passwords that contain inverted commas, they are recognised as such.
- During the Active Directory import, only users with a stored e-mail can be imported.
- The “admin role” is translated correctly when creating a database using an English template.
- When editing the rights of several roles, an error message appears when adding new users if the editor himself is not a member of one or more of these roles.
- Database profiles can be distributed to users via the registry.
- Users deactivated in Active Directory are no longer synchronised with Password Safe.
- Changes to the Emergency WebViewer are active immediately after saving.
- Discovery Service also scans the services on the server on which it was started.

AdminClient

- The “admin role” is translated correctly when creating a database using an English template.
- If the user has no permission, an error message appears when trying to create a backup profile.
- Invalid characters in the database name are replaced by an underscore when a backup is created.
- IP blocks can be edited in the Login locks overview.
- The configuration settings for “nginx” server has been updated.
- Users are highlighted in the database user view according to their status.
- When importing a database backup, the entered credentials are used for login.
- The backup functionality has been optimised.
- The dialog for the migration from V7 to V8 has been adapted.
- The context menu has been adjusted systemwide.
- The error message at expired password of an AdminClient user has been adapted.
- If the license check for a particular database fails in host mode, the error message displays the database name.
- The local time is displayed correctly.

Add-ons

- The safari add-on has been optimised.
- Only the passwords of the exact domain are suggested. Passwords of domains that are part of them are no longer suggested.
- The process of creating a new password via add-on has been optimised.

Android App

- The automatic logout has been optimised.
- The synchronisation with the Password Server has been optimised.
- The typing assistance has been optimised.
- Apps on a self-defined blacklist are excluded from autofill.When creating a password, each input field is validated directly, and any errors are displayed next to the fields or in the fields.
- The scrolling behavior in the mobile App has been optimised.
- Changes to the configuration by switches are saved.

iOS App

- The automatic logout has been optimised.
- The synchronisation with the Password Server has been optimised.
- The typing assistance has been optimised.
- When creating a password, each input field is validated directly and any errors are displayed next to the fields or in the fields.
- The scrolling behavior in the mobile App has been optimised.
- The performance of the iOS App has been optimised.

API

- Error messages when calling functions via the API have been adapted.
- Changing the user password is only possible by entering the old password first.

SSO Agent

- When the agent is started minimized, a login window opens when clicking “Login”.
- Data from the offline database can be filled into the corresponding applications using the SSO agent.
- When Windows is shut down, any active SSO agent or FullClient sessions are automatically terminated.
- The login to the SSO agent has been optimised.
- When restarting an active SSO agent, the login screen is displayed.
- The context menu has been adjusted systemwide.

OfflineClient

- The error messages during synchronization has been adapted.
- Passwords are also checked in the OfflineClient according to configured password policies.
- The context menu has been adjusted systemwide.

LightClient

- The ontext menu has been adjusted.
- Possible error messages when logging off have been adapted.

LightClient in the Web View

- When searching for SAML applications, the number of found applications is displayed.
- Shortcut can beused to save a data set.

Version 8.11.1.19828 Hotfix 1

Release

21.01.2021

Compatibility

The following client versions are compatible with AdminClient Version 8.11.1.19828 Hotfix 1

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.7.0.18000 Hotfix 3
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.8.0.18002 Hotfix 3
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.9.0.17993 Hotfix 2
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.10.0.18473 Hotfix 2
- Windows Client Version 8.11.0.19788
- Windows Client Version 8.11.1.19823
- Windows Client Version 8.11.1.19828 Hotfix 1

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.7.0.18000 Hotfix 3
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.8.0.18002 Hotfix 3
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.9.0.17993 Hotfix 2
- WebClient Version 8.10.0.18464
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.10.0.18473 Hotfix 2
- WebClient Version 8.11.0.19788
- WebClient Version 8.11.1.19823
- WebClient Version 8.11.1.19828 Hotfix 1

- Password Safe Mobile Apps 1.19

Fixed: API interface: possible workaround for enabled second factor.

New

FullClient

- When copying the One-Time-Password (OTP), any spaces are removed.

OfflineClient

*When copying the One-Time-Password (OTP), any spaces are removed.

Fixed

FullClient

*System tasks with weekly or monthly interval have been adjusted.
*Users can only choose between different rights templates when creating passwords if they have the right “Can view selection of rights templates”.

- Passwords are also saved if additional form fields are added during creation.
- Changes to the rights of organisational units have a direct effect on associated passwords.

WebClient

*The WebClient also works in Internet Explorer.

AdminClient

*The migration process from Password Safe V7 to V8 has been optimised.

Add-ons

- In a terminal server session the addon for Google Chrome connects to the SSO client if the appropriate settings are made.

API

*The Library “web-socket-sharp.dll” has been added.

OfflineClient

- The password can be copied to the clipboard via the ribbon or field menu.

Version 8.11.1.19823

Release

07-06-2020

Compatibility

The following client versions are compatible with AdminClient Version 8.11.1.19823

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788
- Windows Client Version 8.11.1.19823

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788
- Windows Client Version 8.11.1.19823

- Password Safe Mobile Apps 1.19

New

FullClient

- When copying the One-Time-Password (OTP), any spaces are removed.

OfflineClient

*When copying the One-Time-Password (OTP), any spaces are removed.

Fixed

FullClient

*System tasks with weekly or monthly interval have been adjusted.
*Users can only choose between different rights templates when creating passwords if they have the right “Can view selection of rights templates”.

- Passwords are also saved if additional form fields are added during creation.
- Changes to the rights of organisational units have a direct effect on associated passwords.

WebClient

*The WebClient also works in Internet Explorer.

AdminClient

*The migration process from Password Safe V7 to V8 has been optimised.

Add-ons

- In a terminal server session the addon for Google Chrome connects to the SSO client if the appropriate settings are made.

API

*The Library “web-socket-sharp.dll” has been added.

OfflineClient

- The password can be copied to the clipboard via the ribbon or field menu.

Version 8.11.0.19788

Release

05-15-2020

Compatibility

The following client versions are compatible with AdminClient Version 8.11.0.19788

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788

- Password Safe Mobile Apps 1.19

Attention
Since the technology of the **Internet Explorer** is outdated, we are unfortunately forced to discontinue support for the add-on. It is no longer developed since version 8.9.0 and will not been delivered since version 8.11.0. Please note that no more bugs will be fixed here and no more support will be provided for this add-on. The use of the add-on is therefore at your own risk.

New

FullClient

- In the report type “Password Age”, the creation date of the passwords is also displayed.
- Instead of the numbers, the corresponding number of dashes is displayed for covered one-time passwords.
- An external link to a one-time password field copies the corresponding token to the clipboard.

WebClient

- When creating or editing passwords, documents, organizational units, roles or forms, new tags can be created or existing ones selected.
- When creating new passwords, both the organizational unit and rights templates can be selected. When editing passwords, only the organizational unit can be selected. If you change the organizational unit, the rights of any rights template overwrite the existing rights of the password.

LightClient in the Web View

- When creating or editing passwords, documents, organizational units, roles or forms, new tags can be created or existing ones selected.
- If you are in the tab of the main organizational unit (all passwords), new passwords can also be created from there.
- When creating and editing passwords, new tags can be created or existing ones can be selected. In addition, several tags can be assigned to a password at the same time in the Tag Management.
- If you create a new password in a tab, the organizational unit of the tab and – if available – the corresponding rights template is displayed. If the password is then created under an organizational unit other than the one of the tab, the password is not displayed in the tab.
- The tab “Main organizational unit” was renamed to “All passwords”. In this tab, passwords can now also be created using the “+” button familiar from other tabs.
- Passwords can be moved to other organizational units. The rights of the passwords are overwritten by the rights the organizational unit has based on a rights template.
- Passwords can be moved to other organizational units via an entry in the context menu. The password is then no longer displayed in the open tab.
- If passwords are edited, you can now select organizational units to which the passwords should be moved.

AdminClient

- When you set up your iOS or Android app, you must select the “List in database list for mobile devices” checkbox in the database settings for a database in host mode to appear in the list of available databases.

Password Safe App

- The apps for Android and iOS support one-time password functionality.
- When creating and editing passwords via the iOS or Android app, you can also select organizational units and rights templates.

API

- The One-Time-Password has also been included in the API.

Server

- All licences are counted centrally on the Password Safe Server.
- In the emergency WebViewer, both the one-time password and the corresponding secret are displayed.

Improvement

FullClient

- Passwords without a user with “Authorization Rights” in a V7 database will be assigned a user with “Authorization Rights” when migrating to V8.

WebClient

- A WebViewer export can be triggered in the WebClient.

Password Safe App

- The one-time password for a web page is automatically copied to the clipboard in the iOS as well as in the Android app during autofill.

Add-on

- A two-tier password via the add-on is also entered if the option “Automatically fill login masks” is disabled.

Fixed

FullClient

- Unnecessary spaces in the notification configuration settings have been removed.
- When creating a new form the ribbon elements “Permissions”, “Form field permissions” and “Configure info” are hidden.
- In the “Configuration” category of the user settings, the main organizational structure can no longer be selected as default organizational unit.
- When configuring RDP applications, “Desktop width” and “Desktop height” may only be editable if the “Scale when resizing” option is activated.
- If you use the TAB key to jump to the drop-down menu for selecting the field type and change it using the arrow keys, the field name is automatically changed accordingly.
- When editing users in the organizational structure the language icon in the ribbon shows the actually selected language.
- If a user without authorization wants to uncover a password field and ignores the note asking for authorization for authorized users, the password field remains covered.
- Any report tasks still running will be aborted when the user logs off and the user will be logged out.
- If you log on to the FullClient via SSO-Agent, a WebViewer export can also be performed.
- In the case of a database migrated from V7 to V8, when an organizational unit is finally deleted,

only this organizational unit is deleted. This is also recorded in the logbook. All subordinate organizational units are not deleted.
- The context menu for column headings in the column view has been standardized in all modules.
- When you create a new tag in the FullClient, the size of the form field does not adapt to the character length of the tag.
- The error message for object descriptions greater than 255 characters has been standardized in all modules.
- If several users are selected in the “Organizational Units” module, the “Multifactor Authentication” button in the ribbon is grayed out.
- Users who are authorized to use a password but not authorized to access users or roles will receive an error message when they try to open these users or roles.
- A selected column in the user / role search will always display the first or last value of the column, depending on the sorting.
- When creating an application, only one element can be selected and edited at a time.
- All users involved * active as creator or passive as user or role in a rights template * are saved correctly in the logbook when a password is created.
- Documents with a file extension greater than 10 characters can be saved.
- If all rights are selected, the checkbox “All rights” is deselected when any right is deselected.
- The tool tip for the form fields “Internet address” and “IP address” has been adapted.
- When creating passwords with a rights template, the permissions assigned to both the complete password and individual form fields are saved correctly for the respective user.
- Passwords in which invalid regular expressions have been entered are not saved and the user is shown an error message.
- The progress bar of the offline synchronization is no longer displayed if a user logs off during the synchronization and a new user logs on. After a user logs off automatically and a new user logs on, the user is not asked for his or her access data again for the offline synchronization that starts automatically.
- If a user manually creates a data record with the setting “Remove creator from the permissions for new objects if the creating user is authorized via a role” activated, this user is authorized to the data record.
- If an Active Directory import is performed in “MasterKey Mode”, nested groups are also imported.
- Special characters in the file name of documents are removed during export.
- Results from searches using filters are displayed correctly when switching to the tree view.
- If a client loses the connection to the server when cross-client login is activated and reconnects, the active user is automatically logged in again.
- In the ribbon, the buttons “Inherit” and “Override” of permissions are only available in edit mode.
- If the “Edit Tab after opening” setting is disabled, reports cannot be edited.
- Changes of permissions of organizational units are inherited correctly to the corresponding passwords.
- Passwords with seal protection can only be deleted by authorized users.
- Intervals in which reports are to be created can be defined.
- The password reset is only carried out if the corresponding license is available.
- Autofill of passwords with seal or privacy protection also works via the iOS App.
- Users with the “Delete” right can also delete passwords with stored tags.
- You can remove temporary permissions on a record that are in the future.
- If the user setting “Edit tab after opening” is deactivated, the button “Edit” is displayed in the ribbon after opening a record.
- A password can only be created if an organizational unit is selected.

- If the “Close tab after saving” setting is disabled, only one forwarding rule will be created in the “Notifications” module when saving this rule.
- An entry of the Active Directory profile is displayed in the logbook when you press the “Open” button.
- When deleting a seal template, a notification is sent.
- When deleting an Active Directory profile, the corresponding certificates are also deleted.
- The overview of all notifications has been adjusted.
- The most recent and therefore active status of a password cannot be restored.
- Entry using SSO has been implemented for numerous applications.
- When restoring documents, the corresponding metadata is also restored.
- When creating new passwords, only a notification about the creation is generated.
- One-time passwords are treated the same in the Full and WebClient.
- The list view was unified in all modules.
- The options of the respective Password Safe editions have been adapted.
- The list view for displaying the date of the last modification of a record has been unified in all modules.
- Changes to a form info are displayed directly in the list view after saving.
- Rights can also be added and removed for several simultaneously selected data records.
- When editing a password with a one-time password field, neither the countdown of the OTP runs nor the progress bar is displayed.
- After editing and saving a password with a One-Time-Password field, the secret of the OTP is not reset, but is retained.
- In the table view in the module “Passwords” the One-Time-Password is not displayed.
- When duplicating passwords, the field for selecting a rights template is not displayed.
- When trying to display a deleted password, a corresponding error message is displayed.
- Restricted users cannot reveal passwords during a WebViewer export.
- Users without the “Add” right cannot assign documents to another organizational unit.
- Passwords with a One-Time-Password as mandatory field cannot be saved without configured Secret.
- The “Remove” button is displayed once in the context menu for configuring new rights for an organizational unit.
- The owner right for an object can only be removed by the owner himself or the database administrator.
- When printing passwords with an unconfigured one-time password, the fields for the one-time password and / or the corresponding secret are empty.
- When scaling the main window, the footer area is also scaled accordingly.
- If an attempt is made to print a sealed password despite having print permission, a corresponding error message is displayed.
- It is not possible to assign users or organizational units to a single user using Drag&Drop.
- When creating a new document, the organizational unit of the creator is prefilled.
- When printing passwords with an unconfigured One-Time Password, the fields for the One-Time Password and/or the corresponding Secret are empty.
- Password policies cannot be set for multi-line text fields in passwords.
- The import summary view has been customized.
- The report view in the FullClient has been customized
- The form field for the user password was adapted.
- The “Can manage rights template” right can also be used to select and assign rights templates of an organizational unit other than the default rights template.

WebClient

- The name “Account” of form templates with this name is displayed correctly in the template selection.
- For inherited user settings, the system displays the organizational unit from which the setting was inherited.
- Roles from an Actice Directory in master key mode cannot be deleted.
- The view can be reloaded using “F5”, even if an organizational unit is selected in the “Organizational Structure” module.
- All tags are displayed in the tag administration.
- If there are objects in a list for which the print permission is not available, a corresponding error message will appear when trying to print the list.
- Error messages are only visible if a user is logged on.
- Search results in the “Organizational structure” module are already displayed when you start typing the search term.

LightClient in the Web View

- It is not possible to create passwords without the right “Can create individual passwords in the LightClient”.
- All tags are displayed in the tag administration of the WebClient.
- The name “Account” of form templates with this name is displayed correctly in the template selection.
- In the case of inherited user settings, the organizational unit from which the setting was inherited is displayed.
- You cannot create multiple tabs with the same organizational unit.
- Error messages are only visible if a user is logged on.
- Search results in the “Organizational Structure” module are already displayed when you start typing the search term.

OfflineClient

- Changes to the expiry date of a database are saved and synchronized correctly.
- The tabs with the results of the quick search in the OfflineClient can be closed.
- If the number of records is less than the value defined in the option “Number of initially loaded records”, the OfflineClient shows the actual number of records. Otherwise the defined value is displayed.
- When opening a password in the OfflineClient with the appropriate rights, no error message is displayed.

Add-on

- The SSO agent automatically inserts the logon data from the offline database into the corresponding applications.
- Only one logon window can be open at a time for the SSO agent.

AdminClient

- During the first installation of the AdminClient, the system checks whether the necessary database could be created when saving the basic configuration. If this was not possible, the basic configuration is not saved and an error is displayed and you can check the settings again.

- The “Admin role” is translated correctly when creating a database using an English template.
- The proxy settings for Yubico can be changed in the AdminClient.
- Users with two-factor authentication enabled cannot log in to the AdminClient. A corresponding error message appears.
- The error message if the DB-Admin removes himself from an organizational unit and wants to save these changes has been modified.
- Only log entries are sent that were created after the forwarding rule was created.

Server

- In “end-to-end” mode during Active Directory import, the rights are inherited correctly according to the organizational unit in which an imported user is located.
- A deactivated but still valid license can also be reactivated via the setup wizard.
- In case of an unsuccessful password reset the corresponding error messages are displayed.

Password Safe App

- During the initial login to the Password Safe App, the password field is greyed out for a certain time if the wrong access data is entered. Only after this time can the password be entered again.
- Changing the password in the Password Safe app after being prompted caused an error that caused the app to crash. The password can now be changed without any problems after a prompt.
- Newly created passwords in a user’s organisational unit in the Password Safe App are not synchronised with the server if the right “Can create personal data records” has been deactivated in the meantime.
- In the Password Safe App, when a one-time password is displayed, the first and last three digits are separated by a space.
- The Password Safe App for iOS supports databases with 20,000 records and more.
- In Password Safe App for iOS, a web page with a one-time password will not display an error message if it is not configured.
- The AutoFill function for the Password Safe App for Android has been optimized.
- When creating a new database profile in the Password Safe App for Android, all existing passwords are synchronized correctly. When a web page is called, the corresponding password is suggested.
- Passwords generated in the Password Safe App for Android and synchronised with the Password Safe Server are automatically entered by the autofill of the app on the corresponding web pages.

Add-on

- The two-tier registration for the website “https://signin.techsmith.com” now also works with the browser add-on for Google Chrome and Safari.
- Even if the WebClient session has expired, passwords can still be created in the WebClient via the browser add-on.
- A two-tier password is entered via the add-on when connected to the add-on via the SSO agent.
- The Internet Explorer add-on is no longer supported and is no longer available with version 8.11.

Version 8.10.0.18473 Hotfix 2

Release

21.01.2021

Compatibility

The following client versions are compatible with AdminClient Version 8.10.0.18473 Hotfix 2

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.7.0.18000 Hotfix 3
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.8.0.18002 Hotfix 3
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.9.0.17993 Hotfix 2
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.10.0.18473 Hotfix 2

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.7.0.18000 Hotfix 3
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.8.0.18002 Hotfix 3
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.9.0.17993 Hotfix 2
- WebClient Version 8.10.0.18464
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.10.0.18473 Hotfix 2

- Password Safe Mobile Apps 1.18

Fixed: API interface: possible workaround for enabled second factor.

Please note that are display errors in the logbook, when older clients are used. However,

the functionality of the logbook is fully available. With an client update to the latest version, this display error no longer occurs.

Attention
As the technology of Internet Explorer is outdated, we are unfortunately forced to discontinue support for the add-on.
The add-on will no longer be developed since version 8.9. This also means that no more bugs will be fixed and no more support for them will take place. Therefore, the use of the add-on is at your own risk. As of version 8.11, the add-on will not be longer available.

Hotfix 1

By checking an wrong permission, users could select a different right template for an OU, but only the default right template was used while save.

New since 8.10.0.18464

WebClient

- Passwords can now also be connected to applications. For this purpose, the new function Connect Password on start has been added to the menu. This allows you to connect applications, open Internet pages and delete existing application shortcuts.
- To set up the Password Safe Mobile app, a mobile access via QR code is displayed in the WebClient settings under Account Settings of the user. With the mobile app, the QR code can be scanned to create a shortcut and perform a login.
- With the new Reset Settings function in the account settings, the personal user settings can now be reset to the default value.
- The user picture can now also be edited in the WebClient.

Add-on

- For websites with 2-step login, the correct data is now entered into the user field as well as the password field via autofill.

Improvements since 8.10.0.18464

General

- Active Directory users can now authenticate themselves to Password Safe using UPN (User Principal Name).
- Login to the database is prevented if the offline database has expired (synchronisation is no longer possible).
- If the admin is prompted to change his password, a window is now displayed, asking him to switch to the client for this purpose.

- The selection of the add-on connection is now set in the options via radio buttons.
- For the SSO Agent, enabling the Starting the application minimized in the notification area option causes only the icon to be displayed in the tray.

FullClient

- The quick search now also works in the tree view for the modules Passwords, Documents, Applications and Password Reset.
- If the user does not log in within the expiration period (180 days), it is automatically extended again by 180 days.

WebClient

- In the Applications module, the passwords associated with the application are displayed in the Start menu.
- In the Role module, a member can be selected in the preview and the data can be displayed via Quick View.
- When creating a new password in the tree view, it can be assigned to an organizational unit.
- Several New Record tabs can now be opened in the mmodules Passwords, Documents, Organizational Structure, Roles and Applications.

LightClient

- Autologin can now be activated.
- The password can now be changed.
- Existing organizational units in the web mode can now be closed by middle mouse button or by ALT+W.
- The main organizational unit in the web mode can now be added.

Changes since 8.10.0.18464

FullClient

- When creating a new organizational unit, the name of this unit is now limited to 255 characters.
- When opening an external link, the record is opened as a tab in the foreground.

AdminClient

- In the server exception, the IP address and the computer name are now also output.

Fixed with 8.10.0.18464

General

- The database timeout for SQL Server now also applies to migrations.
- The Client no longer interprets deleted users and roles as Everyone when using permission templates.
- On the OfflineClient, the quick search tabs can now be closed using the X on the password.
- The AdminClient now correctly deactivates the excisting license when a new license is activated.
- In the web mode of the LightClient, passwords can be created again correctly using the add-on.

- If the plausibility check is aborted on the SSO agent when changing the password, the username is now checked correctly again.

FullClient

- In the Forms module, you can create a new form again using the CTRL+N shortcut.
- Passwords can now be changed independently of the Can manage password form fields right.
- In the Logbook module, the type Active Directory Profile can be opened and displayed directly via the respective button.
- With the Essential license the notification window can be displayed again.
- In the structure view of the modules Passwords, Documents, Applications and Password Reset the organizational structure is entered correctly when creating an object, if the right Can create personal records is deactivated.
- The names of the passwords in an error message during CSV import are now displayed correctly again.
- The password list in the password module now also retains the set format when switching between all passwords and favorites.
- If the user setting Restore last tabs opened is enabled, no additional list tabs are added when the forms and roles module is started.
- The documents in the Documents module (office documents Word, Excel and PowerPoint) can only be edited if the associated programs are not opened.
- In the notification module, a seal notification is displayed correctly again when clicking on the Seal button.
- The error message for seal break requests for passwords with more than one password field is displayed correctly again. The error message for seal break requests for more than one confirmation has also been corrected.
- Custom shortcuts work correctly even with open records.
- In the Organization Wizard the creator of the organizational unit is displayed correctly in Configure rights.
- If you open a password via an external link, password fields cannot be edited as they are in read-only mode.
- With a KeePass file, the imported organizational units are created under the selected organizational unit.
- If a user is imported via the Active Directory, a user type can be specified for the user. The user type Full / Light will be converted correctly again during import.
- Multiple logon with registry profiles is no longer possible.
- During a migration (V7 database) passwords are created in the next higher organizational unit if the folder with the passwords is ignored during import.
- In the seal overview, users who are members of a role and at the same time sharing permissions are no longer displayed as sealed.
- The SSO agent will be prevented from connecting to the database again if the logon data has once been invalid. The SSO agent also deletes expired sessions or logon data which has become invalid. A corresponding message is displayed.
- For a KeePass file, the rights templates are correctly applied to imported organizational units during import.

WebClient

- After editing permissions of a password, the Personal / Public status updates automatically.

- A new form can be provided with a new tag. After saving the template, the tag is displayed in the tag management after a refresh.
- In the modules, navigation can be done with the arrow keys and the quick search can be displayed via space bar.
- The information for software maintenance is displayed correctly in the menu bar during notification.
- The Security category is no longer duplicated in the user rights and global rights.
- In Quick View, the checkboxes of a password are protected against changes by read-only.
- The error message in the seal overview after a seal break request is displayed correctly again.
- In the password module the quick search in the structural filter works correctly again.
- In the structure view of the password module the quick search in the filter works correctly again.
- An automatic login via the add-on on the WebClient is now available again.

Add-on

- The user name is displayed again.
- If the login is incorrect, the login data is not entered again.
- For passwords without a login mask, the passwords can no longer be revealed.

Version 8.10.0.18516 Hotfix 1

Release

04-30-2019

Compatibility

The following client versions are compatible with AdminClient Version 8.10.0.18516 Hotfix 1

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464
- Windows Client Version 8.10.0.18516 Hotfix 1

Please note that are display errors in the logbook, when older clients are used. However, the functionality of the logbook is fully available. With an client update to the latest version, this display error no longer occurs.

Attention
As the technology of Internet Explorer is outdated, we are unfortunately forced to discontinue support for the add-on.
The add-on will no longer be developed since version 8.9. This also means that no more bugs will be fixed and no more support for them will take place. Therefore, the use of the add-on is at your own risk. As of version 8.11, the add-on will not be longer available.

Hotfix 1

By checking an wrong permission, users could select a different right template for an OU, but only the

default right template was used while save.

New since 8.10.0.18464

WebClient

- Passwords can now also be connected to applications. For this purpose, the new function Connect Password on start has been added to the menu. This allows you to connect applications, open Internet pages and delete existing application shortcuts.
- To set up the Password Safe Mobile app, a mobile access via QR code is displayed in the WebClient settings under Account Settings of the user. With the mobile app, the QR code can be scanned to create a shortcut and perform a login.
- With the new Reset Settings function in the account settings, the personal user settings can now be reset to the default value.
- The user picture can now also be edited in the WebClient.

Add-on

- For websites with 2-step login, the correct data is now entered into the user field as well as the password field via autofill.

Improvements since 8.10.0.18464

General

- Active Directory users can now authenticate themselves to Password Safe using UPN (User Principal Name).
- Login to the database is prevented if the offline database has expired (synchronisation is no longer possible).
- If the admin is prompted to change his password, a window is now displayed, asking him to switch to the client for this purpose.
- The selection of the add-on connection is now set in the options via radio buttons.
- For the SSO Agent, enabling the Starting the application minimized in the notification area option causes only the icon to be displayed in the tray.

FullClient

- The quick search now also works in the tree view for the modules Passwords, Documents, Applications and Password Reset.
- If the user does not log in within the expiration period (180 days), it is automatically extended again by 180 days.

WebClient

- In the Applications module, the passwords associated with the application are displayed in the Start menu.
- In the Role module, a member can be selected in the preview and the data can be displayed via Quick View.

- When creating a new password in the tree view, it can be assigned to an organizational unit.
- Several New Record tabs can now be opened in the mmodules Passwords, Documents, Organizational Structure, Roles and Applications.

LightClient

- Autologin can now be activated.
- The password can now be changed.
- Existing organizational units in the web mode can now be closed by middle mouse button or by ALT+W.
- The main organizational unit in the web mode can now be added.

Changes since 8.10.0.18464

FullClient

- When creating a new organizational unit, the name of this unit is now limited to 255 characters.
- When opening an external link, the record is opened as a tab in the foreground.

AdminClient

- In the server exception, the IP address and the computer name are now also output.

Fixed with 8.10.0.18464

General

- The database timeout for SQL Server now also applies to migrations.
- The Client no longer interprets deleted users and roles as Everyone when using permission templates.
- On the OfflineClient, the quick search tabs can now be closed using the X on the password.
- The AdminClient now correctly deactivates the excisting license when a new license is activated.
- In the web mode of the LightClient, passwords can be created again correctly using the add-on.
- If the plausibility check is aborted on the SSO agent when changing the password, the username is now checked correctly again.

FullClient

- In the Forms module, you can create a new form again using the CTRL+N shortcut.
- Passwords can now be changed independently of the Can manage password form fields right.
- In the Logbook module, the type Active Directory Profile can be opened and displayed directly via the respective button.
- With the Essential license the notification window can be displayed again.
- In the structure view of the modules Passwords, Documents, Applications and Password Reset the organizational structure is entered correctly when creating an object, if the right Can create personal records is deactivated.
- The names of the passwords in an error message during CSV import are now displayed correctly again.
- The password list in the password module now also retains the set format when switching between

all passwords and favorites.
- If the user setting Restore last tabs opened is enabled, no additional list tabs are added when the forms and roles module is started.
- The documents in the Documents module (office documents Word, Excel and PowerPoint) can only be edited if the associated programs are not opened.
- In the notification module, a seal notification is displayed correctly again when clicking on the Seal button.
- The error message for seal break requests for passwords with more than one password field is displayed correctly again. The error message for seal break requests for more than one confirmation has also been corrected.
- Custom shortcuts work correctly even with open records.
- In the Organization Wizard the creator of the organizational unit is displayed correctly in Configure rights.
- If you open a password via an external link, password fields cannot be edited as they are in read-only mode.
- With a KeePass file, the imported organizational units are created under the selected organizational unit.
- If a user is imported via the Active Directory, a user type can be specified for the user. The user type Full / Light will be converted correctly again during import.
- Multiple logon with registry profiles is no longer possible.
- During a migration (V7 database) passwords are created in the next higher organizational unit if the folder with the passwords is ignored during import.
- In the seal overview, users who are members of a role and at the same time sharing permissions are no longer displayed as sealed.
- The SSO agent will be prevented from connecting to the database again if the logon data has once been invalid. The SSO agent also deletes expired sessions or logon data which has become invalid. A corresponding message is displayed.
- For a KeePass file, the rights templates are correctly applied to imported organizational units during import.

WebClient

- After editing permissions of a password, the Personal / Public status updates automatically.
- A new form can be provided with a new tag. After saving the template, the tag is displayed in the tag management after a refresh.
- In the modules, navigation can be done with the arrow keys and the quick search can be displayed via space bar.
- The information for software maintenance is displayed correctly in the menu bar during notification.
- The Security category is no longer duplicated in the user rights and global rights.
- In Quick View, the checkboxes of a password are protected against changes by read-only.
- The error message in the seal overview after a seal break request is displayed correctly again.
- In the password module the quick search in the structural filter works correctly again.
- In the structure view of the password module the quick search in the filter works correctly again.
- An automatic login via the add-on on the WebClient is now available again.

Add-on

- The user name is displayed again.

- If the login is incorrect, the login data is not entered again.
- For passwords without a login mask, the passwords can no longer be revealed.

Version 8.10.0.18464

Release

02-14-2019

Compatibility

The following client versions are compatible with AdminClient Version 8.10.0.18464

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18464

Please note that are display errors in the logbook, when older clients are used. However, the functionality of the logbook is fully available. With an client update to the latest version, this display error no longer occurs.

Attention
As the technology of Internet Explorer is outdated, we are unfortunately forced to discontinue support for the add-on.
The add-on will no longer be developed since version 8.9. This also means that no more bugs will be fixed and no more support for them will take place. Therefore, the use of the add-on is at your own risk. As of version 8.11, the add-on will not be longer available.

New

WebClient

- Passwords can now also be connected to applications. For this purpose, the new function Connect

Password on start has been added to the menu. This allows you to connect applications, open Internet pages and delete existing application shortcuts.
- To set up the Password Safe Mobile app, a mobile access via QR code is displayed in the WebClient settings under Account Settings of the user. With the mobile app, the QR code can be scanned to create a shortcut and perform a login.
- With the new Reset Settings function in the account settings, the personal user settings can now be reset to the default value.
- The user picture can now also be edited in the WebClient.

Add-on

- For websites with 2-step login, the correct data is now entered into the user field as well as the password field via autofill.

Improvements

General

- Active Directory users can now authenticate themselves to Password Safe using UPN (User Principal Name).
- Login to the database is prevented if the offline database has expired (synchronisation is no longer possible).
- If the admin is prompted to change his password, a window is now displayed, asking him to switch to the client for this purpose.
- The selection of the add-on connection is now set in the options via radio buttons.
- For the SSO Agent, enabling the Starting the application minimized in the notification area option causes only the icon to be displayed in the tray.

FullClient

- The quick search now also works in the tree view for the modules Passwords, Documents, Applications and Password Reset.
- If the user does not log in within the expiration period (180 days), it is automatically extended again by 180 days.

WebClient

- In the Applications module, the passwords associated with the application are displayed in the Start menu.
- In the Role module, a member can be selected in the preview and the data can be displayed via Quick View.
- When creating a new password in the tree view, it can be assigned to an organizational unit.
- Several New Record tabs can now be opened in the mmodules Passwords, Documents, Organizational Structure, Roles and Applications.

LightClient

- Autologin can now be activated.

- The password can now be changed.
- Existing organizational units in the web mode can now be closed by middle mouse button or by ALT+W.
- The main organizational unit in the web mode can now be added.

Changes

FullClient

- When creating a new organizational unit, the name of this unit is now limited to 255 characters.
- When opening an external link, the record is opened as a tab in the foreground.

AdminClient

- In the server exception, the IP address and the computer name are now also output.

Fixed

General

- The database timeout for SQL Server now also applies to migrations.
- The Client no longer interprets deleted users and roles as Everyone when using permission templates.
- On the OfflineClient, the quick search tabs can now be closed using the X on the password.
- The AdminClient now correctly deactivates the excisting license when a new license is activated.
- In the web mode of the LightClient, passwords can be created again correctly using the add-on.
- If the plausibility check is aborted on the SSO agent when changing the password, the username is now checked correctly again.

FullClient

- In the Forms module, you can create a new form again using the CTRL+N shortcut.
- Passwords can now be changed independently of the Can manage password form fields right.
- In the Logbook module, the type Active Directory Profile can be opened and displayed directly via the respective button.
- With the Essential license the notification window can be displayed again.
- In the structure view of the modules Passwords, Documents, Applications and Password Reset the organizational structure is entered correctly when creating an object, if the right Can create personal records is deactivated.
- The names of the passwords in an error message during CSV import are now displayed correctly again.
- The password list in the password module now also retains the set format when switching between all passwords and favorites.
- If the user setting Restore last tabs opened is enabled, no additional list tabs are added when the forms and roles module is started.
- The documents in the Documents module (office documents Word, Excel and PowerPoint) can only be edited if the associated programs are not opened.
- In the notification module, a seal notification is displayed correctly again when clicking on the Seal button.

- The error message for seal break requests for passwords with more than one password field is displayed correctly again. The error message for seal break requests for more than one confirmation has also been corrected.
- Custom shortcuts work correctly even with open records.
- In the Organization Wizard the creator of the organizational unit is displayed correctly in Configure rights.
- If you open a password via an external link, password fields cannot be edited as they are in read-only mode.
- With a KeePass file, the imported organizational units are created under the selected organizational unit.
- If a user is imported via the Active Directory, a user type can be specified for the user. The user type Full / Light will be converted correctly again during import.
- Multiple logon with registry profiles is no longer possible.
- During a migration (V7 database) passwords are created in the next higher organizational unit if the folder with the passwords is ignored during import.
- In the seal overview, users who are members of a role and at the same time sharing permissions are no longer displayed as sealed.
- The SSO agent will be prevented from connecting to the database again if the logon data has once been invalid. The SSO agent also deletes expired sessions or logon data which has become invalid. A corresponding message is displayed.
- For a KeePass file, the rights templates are correctly applied to imported organizational units during import.

WebClient

- After editing permissions of a password, the Personal / Public status updates automatically.
- A new form can be provided with a new tag. After saving the template, the tag is displayed in the tag management after a refresh.
- In the modules, navigation can be done with the arrow keys and the quick search can be displayed via space bar.
- The information for software maintenance is displayed correctly in the menu bar during notification.
- The Security category is no longer duplicated in the user rights and global rights.
- In Quick View, the checkboxes of a password are protected against changes by read-only.
- The error message in the seal overview after a seal break request is displayed correctly again.
- In the password module the quick search in the structural filter works correctly again.
- In the structure view of the password module the quick search in the filter works correctly again.
- An automatic login via the add-on on the WebClient is now available again.

Add-on

- The user name is displayed again.
- If the login is incorrect, the login data is not entered again.
- For passwords without a login mask, the passwords can no longer be revealed.

Third Party Licenses

Here you can find all used 3rd party libraries for MATESO Password Safe.

Table of Content

- Autofac.WebApi2 (Version: 6.1.0)
- Autofac (Version: 6.3.0)
- Castle.Core (Version: 4.4.1)
- CliWrap (Version: 3.4.1)
- DeepEqual (Version: 2.0.0)
- EntityFramework.SqlServerCompact (Version: 6.4.4)
- EntityFramework (Version: 6.4.4)
- Esprima (Version: 2.1.2)
- FaviconFetcher (Version: 1.2.0)
- Fido2 (Version: 2.0.2)
- Fleck (Version: 1.2.0)
- Hardcodet.NotifyIcon.Wpf (Version: 1.1.0)
- IPAddressRange (Version: 4.2.0)
- IdentityModel.OidcClient (Version: 5.0.0)
- IdentityModel (Version: 6.0.0)
- InputSimulator (Version: 1.0.4.0)
- LinqKit.Core (Version: 1.2.0)
- MailKit (Version: 3.1.1)
- MaxMind.GeoIP2 (Version: 5.1.0)
- MessagePack (Version: 2.3.85)
- Newtonsoft.Json (Version: 13.0.1)
- NoGit (Version: 0.1.0)
- Node.js (Version: 5.3.0)
- PCSC (Version: 5.1.0)
- PeterO.Cbor (Version: 4.5.2)
- Pkcs11Interop (Version: 5.1.2)
- Portable.BouncyCastle (Version: 1.9.0)
- PriorityQueue (Version: 0.1.0)
- PuTTY (Version: 0.76)
- QRCoder (Version: 1.4.3)
- Radius (Version: 2.0.0.2)
- SSH.NET (Version: 2020.0.1)
- SharpVectors.Reloaded (Version: 1.7.7)
- SuperSocket.ClientEngine.Core (Version: 0.10.0)
- Tanneryd.BulkOperations.EF6 (Version: 1.4.1)
- UAParser (Version: 3.1.47)
- WebSocket4Net (Version: 0.15.2)
- WebSocketSharp (Version: 1.0.3-rc11)
- Z.EntityFramework.Plus.EF6 (Version: 6.13.10)
- xxHash4net (Version: 1.2.0)

Licenses

Autofac.WebApi2 (Version: 6.1.0)
Authors: Autofac Contributors
URL: https://autofac.org/

The MIT License (MIT)

Copyright © 2014 Autofac Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

———————————————————————————————————————

Autofac (Version: 6.3.0)
Authors: Autofac Contributors
URL: https://autofac.org/

The MIT License (MIT)

Copyright © 2015 Autofac Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Castle.Core (Version: 4.4.1)
Authors: Castle Project Contributors
URL: http://www.castleproject.org/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of

Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty,

indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2004-2020 Castle Project – http://www.castleproject.org/ Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

CliWrap (Version: 3.4.1)
Authors: Tyrrrz
URL: https://github.com/Tyrrrz/CliWrap

The MIT License (MIT)

Copyright © Oleksii Holub

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DeepEqual (Version: 2.0.0)

Authors: James Foster
URL: http://github.com/jamesfoster/DeepEqual

The MIT License (MIT)

James Foster 2018

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

EntityFramework.SqlServerCompact (Version: 6.4.4)
Authors: Microsoft
URL: http://go.microsoft.com/fwlink/?LinkID=263480

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on

(or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with

Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. © Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

EntityFramework (Version: 6.4.4)
Authors: Microsoft
URL: http://go.microsoft.com/fwlink/?LinkID=263480

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii)

beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that

such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. © Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Esprima (Version: 2.1.2)
Authors: Sebastien Ros
URL: https://github.com/sebastienros/esprima-dotnet

BSD-3-Clause

Sebastien Ros

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation and/or
other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors
may be used to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FaviconFetcher (Version: 1.2.0)
Authors: Nathan Belue
URL: https://github.com/ComputerGhost/FaviconFetcher

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Fido2 (Version: 2.0.2)
Authors: Fido2
URL: https://github.com/abergs/fido2-net-lib

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Fleck (Version: 1.2.0)
Authors: statenjason
URL: https://github.com/statianzo/Fleck

The MIT License (MIT)

Copyright Jason Staten 2010-2018. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Hardcodet.NotifyIcon.Wpf (Version: 1.1.0)
Authors: Philipp Sumi, Robin Krom, Jan Karger
URL: https://github.com/hardcodet/wpf-notifyicon

The Code Project Open License (CPOL) 1.02

Copyright © 2009-2021 Philipp Sumi

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are: * Source Code and Executable Files can be used in commercial applications; * Source Code and Executable Files can be redistributed; and * Source Code can be modified to create derivative works. * No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is
provided “as-is”. * The Article accompanying the Work may not be distributed or republished without the Author’s
consent
This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License (“Author”).

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE
(“LICENSE”). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK
OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS
OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN

CONSIDERATION OF YOUR
ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF
THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK. 1. Definitions. 1. “Articles” means, collectively, all articles written by Author which describes how the Source
Code and Executable Files for the Work may be used by a user. 2. “Author” means the individual or entity that offers the Work under the terms of this License.

3. “Derivative Work” means a work based upon the Work or upon the Work and other pre-existing works. 4. “Executable Files” refer to the executables, binary files, configuration and any required data files included in the Work. 5. “Publisher” means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You. 6. “Source Code” refers to the collection of source code and configuration files used to create the Executable Files. 7. “Standard Version” refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author. 8. “Work” refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles. 9. “You” is you, an individual or entity wishing to use the Work and exercise your rights under this License. 2. Fair Use/ Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws. 3. License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below: 1. You may use the standard version of the Source Code or Executable Files in Your own applications. 2. You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License. 3. You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file. 4. You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution. 5. The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author’s consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author. Any subroutines or modules supplied by You and linked into the Source Code or Executable Files of this Work shall not be considered part of this Work and will not be subject to the terms of this License. 4. Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work. 5. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions: 1. You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files. 2. You agree not to advertise or in any way imply that this Work is a product of Your own. 3. The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author. 4. You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented. 5. You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code

agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License. 6. You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work. 6. Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS. 7. Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You. 8. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 9. Termination. 1. This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License. 2. If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically. 3. Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above. 10. Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice 11. Miscellaneous 1. This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author. 2. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable. 3. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in

writing and signed by the party to be charged with such waiver or consent. 4. This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

IPAddressRange (Version: 4.2.0)
Authors: J.Sakamoto
URL: https://github.com/jsakamoto/ipaddressrange/

Copyright © 2012-2021 J.Sakamoto, Mozilla Public License 2.0

Mozilla Public License Version 2.0

1. Definitions 1.1. “Contributor” means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software. 1.2. “Contributor Version” means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor’s Contribution. 1.3. “Contribution” means Covered Software of a particular Contributor. 1.4. “Covered Software” means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof. 1.5. “Incompatible With Secondary Licenses” means (a) that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or (b) that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License. 1.6. “Executable Form” means any form of the work other than Source Code Form. 1.7. “Larger Work” means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software. 1.8. “License” means this document. 1.9. “Licensable” means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License. 1.10. “Modifications” means any of the following: (a) any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or (b) any new file in Source Code Form that contains any Covered Software. 1.11. “Patent Claims” of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version. 1.12. “Secondary License” means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses. 1.13. “Source Code Form” means the form of the work preferred for making modifications. 1.14. “You” (or “Your”) means an individual or a legal entity exercising rights under this License. For legal entities, “You” includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity. 2. License Grants and Conditions 2.1. Grants Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license: (a) under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and (b) under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution. 2.3. Limitations on Grant Scope The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor: (a) for any code that a Contributor has removed from Covered Software; or (b) for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or © under Patent Claims infringed by Covered Software in the absence of its Contributions. This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4). 2.4. Subsequent Licenses No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3). 2.5. Representation Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License. 2.6. Fair Use This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents. 2.7. Conditions Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1. 3. Responsibilities 3.1. Distribution of Source Form All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form. 3.2. Distribution of Executable Form If You distribute Covered Software in Executable Form then: (a) such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and (b) You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License. 3.3. Distribution of a Larger Work You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s). 3.4. Notices You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies. 3.5. Application of Additional Terms You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction. 4. Inability to Comply Due to Statute or Regulation If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except

to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it. 5. Termination 5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice. 5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate. 5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination. 6. Disclaimer of Warranty Covered Software is provided under this License on an “as is” basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer. 7. Limitation of Liability Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party’s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You. 8. Litigation Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims. 9. Miscellaneous This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor. 10. Versions of the License 10.1. New Versions Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number. 10.2. Effect of New Versions You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward. 10.3. Modified Versions If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License). 10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the

License, the notice described in Exhibit B of this License must be attached. Exhibit A – Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B – “Incompatible With Secondary Licenses” Notice

This Source Code Form is “Incompatible With Secondary Licenses”, as defined by the Mozilla Public License, v. 2.0.

IdentityModel.OidcClient (Version: 5.0.0)
Authors: Dominick Baier, Brock Allen

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or

its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work

and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

IdentityModel (Version: 6.0.0)
Authors: Dominick Baier, Brock Allen
URL: https://github.com/IdentityModel/IdentityModel

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on

(or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with

Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

InputSimulator (Version: 1.0.4.0)
Authors: Michael Noonan
URL: http://inputsimulator.codeplex.com

The MIT License (MIT)

Copyright 2009-2013

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LinqKit.Core (Version: 1.2.0)
Authors: Joseph Albahari, Tomas Petricek, Scott Smith, Tuomas Hietanen, Stef Heyenrath
URL: https://github.com/scottksmith95/LINQKit

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MailKit (Version: 3.1.1)
Authors: Jeffrey Stedfast
URL: http://www.mimekit.net/

The MIT License (MIT)

.NET Foundation and Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MaxMind.GeoIP2 (Version: 5.1.0)
Authors: MaxMind.GeoIP2
URL: https://github.com/maxmind/GeoIP2-dotnet

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this

definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR

PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

MessagePack (Version: 2.3.85)
Authors: neuecc, aarnott
URL: https://github.com/neuecc/MessagePack-CSharp

The MIT License (MIT)

© Yoshifumi Kawai and contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Newtonsoft.Json (Version: 13.0.1)
Authors: James Newton-King
URL: https://www.newtonsoft.com/json

The MIT License (MIT)

Copyright © James Newton-King 2008

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NoGit (Version: 0.1.0)
Authors: Pavel Nezhencev
URL: https://github.com/whyleee/nogit

The MIT License (MIT)

© 2015 Pavel Nezhencev

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

_____

Node.js (Version: 5.3.0)
Authors: Node.js Foundation
URL: https://nodejs.org/

Node.js is licensed for use as follows:

“”“
Copyright Node.js contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.
“”“

This license applies to parts of Node.js originating from the
https://github.com/joyent/node repository:

“”“

Copyright Joyent, Inc. and other Node contributors. All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
“”“

The Node.js license applies to all parts of Node.js that are not externally maintained libraries.

The externally maintained libraries used by Node.js are:

- V8, located at deps/v8. V8’s license follows: “”“ This license applies to all parts of V8 that are not externally maintained libraries. The externally maintained libraries used by V8 are:

– PCRE test suite, located in test/mjsunit/third_party/regexp-pcre.js. This is based on the test suite from PCRE-7.3, which is copyrighted by the University of Cambridge and Google, Inc. The copyright notice and license are embedded in regexp-pcre.js. – Layout tests, located in test/mjsunit/third_party. These are based on layout tests from webkit.org which are copyrighted by Apple Computer, Inc. and released under a 3-clause BSD license. – Strongtalk assembler, the basis of the files assembler-arm-inl.h, assembler-arm.cc, assembler-arm.h, assembler-ia32-inl.h, assembler-ia32.cc, assembler-ia32.h, assembler-x64-inl.h, assembler-x64.cc, assembler-x64.h, assembler-mips-inl.h, assembler-mips.cc, assembler-mips.h, assembler.cc and assembler.h. This code is copyrighted by Sun Microsystems Inc. and released under a 3-clause BSD license. – Valgrind client API header, located at third_party/valgrind/valgrind.h This is release under the BSD license. These libraries have their own licenses; we recommend you read them, as their terms may differ from the terms below. Copyright 2006-2012, the V8 project authors. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- C-Ares, an asynchronous DNS client, located at deps/cares. C-Ares license follows: “”“ /* Copyright 1998 by the Massachusetts Institute of Technology. * * Permission to use, copy, modify, and distribute this * software and its documentation for any purpose and without * fee is hereby granted, provided that the above copyright * notice appear in all copies and that both that copyright * notice and this permission notice appear in supporting * documentation, and that the name of M.I.T. not be used in * advertising or publicity pertaining to distribution of the * software without specific, written prior permission. * M.I.T. makes no representations about the suitability of * this software for any purpose. It is provided “as is” * without express or implied warranty. “”“

- OpenSSL located at deps/openssl. OpenSSL is cryptographic software written by Eric Young (eay@cryptsoft.com) to provide SSL/TLS encryption. OpenSSL’s license follows: “”“ /* == * Copyright © 1998-2011 The OpenSSL Project. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in * the documentation and/or other materials provided with the * distribution. * * 3. All advertising materials mentioning features or use of this * software must display the following acknowledgment: * “This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit. (http://www.openssl.org/)” * * 4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to * endorse or promote products derived from this software without * prior written permission. For written permission, please contact * openssl-core@openssl.org. * * 5. Products derived from this software may not be called “OpenSSL” * nor may “OpenSSL” appear in their names without prior written * permission of the OpenSSL Project. * * 6. Redistributions of any form whatsoever must retain the following * acknowledgment: * “This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit (http://www.openssl.org/)” * * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS’‘ AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED * OF THE POSSIBILITY OF SUCH DAMAGE. * == * * This product includes cryptographic software written by Eric Young * (eay@cryptsoft.com). This product includes software written by Tim * Hudson (tjh@cryptsoft.com). * */ “”“

- HTTP Parser, located at deps/http_parser. HTTP Parser's license follows: “”“ http_parser.c is based on src/http/ngx_http_parse.c from NGINX copyright Igor Sysoev.

Additional changes are licensed under the same terms as NGINX and copyright Joyent, Inc. and other Node contributors. All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- ESLint is located at tools/eslint. ESLint's license follows: “”“ ESLint Copyright © 2013 Nicholas C. Zakas. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- tools/cpplint.py is a C++ linter. Its license follows: “”“ # Copyright © 2009 Google Inc. All rights reserved. # # Redistribution and use in source and binary forms, with or without # modification, are permitted provided that the following conditions are # met: # # * Redistributions of source code must retain the above copyright # notice, this list of conditions and the following disclaimer. # * Redistributions in binary form must reproduce the above # copyright notice, this list of conditions and the following disclaimer # in the documentation and/or other materials provided with the # distribution. # * Neither the name of Google Inc. nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR # A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT # OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, # SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT # LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, # DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY # THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE # OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- lib/punycode.js is copyright 2011 Mathias Bynens and released under the MIT license. “”“ * Punycode.js * Copyright 2011 Mathias Bynens * Available under MIT license “”“

- tools/gyp. GYP is a meta-build system. GYP’s license follows: “”“ Copyright © 2009 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- Zlib at deps/zlib. zlib’s license follows: “”“ /* zlib.h — interface of the ‘zlib’ general purpose compression library version 1.2.8, April 28th, 2013

Copyright © 1995-2013 Jean-loup Gailly and Mark Adler This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu */ “”“

- npm is a package manager program located at deps/npm. npm’s license follows: “”“ Copyright © Isaac Z. Schlueter All rights reserved.

npm is released under the Artistic 2.0 License. The text of the License follows: ———— The Artistic License 2.0 Copyright © 2000-2006, The Perl Foundation. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. Preamble This license establishes the terms under which a given free software Package may be copied, modified, distributed, and/or redistributed. The intent is that the Copyright Holder maintains some artistic control over the development of that Package while still keeping the Package available as open source and free software. You are always permitted to make

arrangements wholly outside of this license directly with the Copyright Holder of a given Package. If the terms of this license do not permit the full use that you propose to make of the Package, you should contact the Copyright Holder and seek a different licensing arrangement. Definitions “Copyright Holder” means the individual(s) or organization(s) named in the copyright notice for the entire Package. “Contributor” means any party that has contributed code or other material to the Package, in accordance with the Copyright Holder’s procedures. “You” and “your” means any person who would like to copy, distribute, or modify the Package. “Package” means the collection of files distributed by the Copyright Holder, and derivatives of that collection and/or of those files. A given Package may consist of either the Standard Version, or a Modified Version. “Distribute” means providing a copy of the Package or making it accessible to anyone else, or in the case of a company or organization, to others outside of your company or organization. “Distributor Fee” means any fee that you charge for Distributing this Package or providing support for this Package to another party. It does not mean licensing fees. “Standard Version” refers to the Package if it has not been modified, or has been modified only in ways explicitly requested by the Copyright Holder. “Modified Version” means the Package, if it has been changed, and such changes were not explicitly requested by the Copyright Holder. “Original License” means this Artistic License as Distributed with the Standard Version of the Package, in its current version or as it may be modified by The Perl Foundation in the future. “Source” form means the source code, documentation source, and configuration files for the Package. “Compiled” form means the compiled bytecode, object code, binary, or any other form resulting from mechanical transformation or translation of the Source form. Permission for Use and Modification Without Distribution (1) You are permitted to use the Standard Version and create and use Modified Versions for any purpose without restriction, provided that you do not Distribute the Modified Version. Permissions for Redistribution of the Standard Version (2) You may Distribute verbatim copies of the Source form of the Standard Version of this Package in any medium without restriction, either gratis or for a Distributor Fee, provided that you duplicate all of the original copyright notices and associated disclaimers. At your discretion, such verbatim copies may or may not include a Compiled form of the Package. (3) You may apply any bug fixes, portability changes, and other modifications made available from the Copyright Holder. The resulting Package will still be considered the Standard Version, and as such will be subject to the Original License. Distribution of Modified Versions of the Package as Source (4) You may Distribute your Modified Version as Source (either gratis or for a Distributor Fee, and with or without a Compiled form of the Modified Version) provided that you clearly document how it differs from the Standard Version, including, but not limited to, documenting any non-standard features, executables, or modules, and provided that you do at least ONE of the following: (a) make the Modified Version available to the Copyright Holder of the Standard Version, under the Original License, so that the Copyright Holder may include your modifications in the Standard Version. (b) ensure that installation of your Modified Version does not prevent the user installing or running the Standard Version. In addition, the Modified Version must bear a name that is different from the name of the Standard Version. © allow anyone who receives a copy of the Modified Version to make the Source form of the Modified Version available to others under (i) the Original License or (ii) a license that permits the licensee to freely copy, modify and redistribute the Modified Version using the same licensing terms that apply to the copy that the licensee received, and requires that the Source form of the Modified Version, and of any works derived from it, be made freely available in that license fees are prohibited but Distributor Fees are allowed. Distribution of Compiled Forms of the Standard Version or Modified Versions without the Source (5) You may Distribute Compiled forms of the Standard Version without the Source, provided that you include complete instructions on how to get the Source of the Standard Version. Such instructions must be valid at the time of your distribution. If these instructions, at any time while you are carrying out such distribution, become invalid, you must provide new instructions on demand or cease further distribution. If you provide valid instructions or cease distribution within thirty days after you become aware that the instructions are invalid, then you do not forfeit any of your rights under this license. (6) You may Distribute a Modified Version in Compiled form without the Source, provided that you comply with Section 4 with respect to the Source of the Modified Version. Aggregating or Linking the Package (7) You may

aggregate the Package (either the Standard Version or Modified Version) with other packages and Distribute the resulting aggregation provided that you do not charge a licensing fee for the Package. Distributor Fees are permitted, and licensing fees for other components in the aggregation are permitted. The terms of this license apply to the use and Distribution of the Standard or Modified Versions as included in the aggregation. (8) You are permitted to link Modified and Standard Versions with other works, to embed the Package in a larger work of your own, or to build stand-alone binary or bytecode versions of applications that include the Package, and Distribute the result without restriction, provided the result does not expose a direct interface to the Package. Items That are Not Considered Part of a Modified Version (9) Works (including, but not limited to, modules and scripts) that merely extend or make use of the Package, do not, by themselves, cause the Package to be a Modified Version. In addition, such works are not considered parts of the Package itself, and are not subject to the terms of this license. General Provisions (10) Any use, modification, and distribution of the Standard or Modified Versions is governed by this Artistic License. By using, modifying or distributing the Package, you accept this license. Do not use, modify, or distribute the Package, if you do not accept this license. (11) If your Modified Version has been derived from a Modified Version made by someone other than you, you are nevertheless required to ensure that your Modified Version complies with the requirements of this license. (12) This license does not grant you the right to use any trademark, service mark, tradename, or logo of the Copyright Holder. (13) This license includes the non-exclusive, worldwide, free-of-charge patent license to make, have made, use, offer to sell, sell, import and otherwise transfer the Package with respect to any patent claims licensable by the Copyright Holder that are necessarily infringed by the Package. If you institute patent litigation (including a cross-claim or counterclaim) against any party alleging that the Package constitutes direct or contributory patent infringement, then this Artistic License to you shall terminate on the date that such litigation is filed. (14) Disclaimer of Warranty: THE PACKAGE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS “AS IS’ AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT ARE DISCLAIMED TO THE EXTENT PERMITTED BY YOUR LOCAL LAW. UNLESS REQUIRED BY LAW, NO COPYRIGHT HOLDER OR CONTRIBUTOR WILL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING IN ANY WAY OUT OF THE USE OF THE PACKAGE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ———— “Node.js” and “node” trademark Joyent, Inc. npm is not officially part of the Node.js project, and is neither owned by nor officially affiliated with Joyent, Inc. Packages published in the npm registry (other than the Software and its included dependencies) are not part of npm itself, are the sole property of their respective maintainers, and are not covered by this license. “npm Logo” created by Mathias Pettersson and Brian Hammond, used with permission. “Gubblebum Blocky” font Copyright © by Tjarda Koster, http://jelloween.deviantart.com included for use in the npm website and documentation, used with permission. This program uses several Node.js modules contained in the node_modules/ subdirectory, according to the terms of their respective licenses. “”“

- tools/doc/node_modules/marked. Marked is a Markdown parser. Marked’s license follows: “”“ Copyright © 2011-2012, Christopher Jeffrey (https://github.com/chjj/)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR

COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- test/gc/node_modules/weak. Node-weak is a node.js addon that provides garbage collector notifications. Node-weak’s license follows: “”“ Copyright © 2011, Ben Noordhuis

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED “AS IS” AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. “”“

- ICU’s license follows: From http://source.icu-project.org/repos/icu/icu/trunk/license.html “”“ ICU License – ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE Copyright © 1995-2014 International Business Machines Corporation and others All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder. All trademarks and registered trademarks mentioned herein are the property of their respective owners. Third-Party Software Licenses This section contains third-party software notices and/or additional terms for licensed third-party software components included within ICU libraries. 1. Unicode Data Files and Software COPYRIGHT AND PERMISSION NOTICE Copyright © 1991-2014 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html. Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the “Data Files”) or Unicode software and any associated documentation (the “Software”) to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) this copyright and permission notice appear with all copies of the Data Files or Software, (b) this copyright and permission notice appear in associated documentation, and © there is clear notice in each modified Data File or in the Software

as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified. THE DATA FILES AND SOFTWARE ARE PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder. 2. Chinese/Japanese Word Break Dictionary Data (cjdict.txt) # The Google Chrome software developed by Google is licensed # under the BSD license. Other software included in this distribution # is provided under other licenses, as set forth below. # # The BSD License # http://opensource.org/licenses/bsd-license.php # Copyright © 2006-2008, Google Inc. # # All rights reserved. # # Redistribution and use in source and binary forms, with or # without modification, are permitted provided that the following # conditions are met: # # Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. # Redistributions in binary form must reproduce the above # copyright notice, this list of conditions and the following # disclaimer in the documentation and/or other materials provided with # the distribution. # Neither the name of Google Inc. nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. # # # The word list in cjdict.txt are generated by combining three word lists listed # below with further processing for compound word breaking. The frequency is generated # with an iterative training against Google web corpora. # # * Libtabe (Chinese) # – https://sourceforge.net/project/?group_id=1519 # – Its license terms and conditions are shown below. # # * IPADIC (Japanese) # – http://chasen.aist-nara.ac.jp/chasen/distribution.html # – Its license terms and conditions are shown below. # # ————-COPYING.libtabe —— BEGIN———————— # # /* # * Copyrighy © 1999 TaBE Project. # * Copyright © 1999 Pai-Hsiang Hsiao. # * All rights reserved. # * # * Redistribution and use in source and binary forms, with or without # * modification, are permitted provided that the following conditions # * are met: # * # * . Redistributions of source code must retain the above copyright # * notice, this list of conditions and the following disclaimer. # * . Redistributions in binary form must reproduce the above copyright # * notice, this list of conditions and the following disclaimer in # * the documentation and/or other materials provided with the # * distribution. # * . Neither the name of the TaBE Project nor the names of its # * contributors may be used to endorse or promote products derived # * from this software without specific prior written permission. # * # * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # * “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS # * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE # * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, # * INCIDENTAL, SPECIAL, EXEMPLARY,

OR CONSEQUENTIAL DAMAGES # * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR # * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) # * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, # * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) # * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED # * OF THE POSSIBILITY OF SUCH DAMAGE. # */ # # /* # * Copyright © 1999 Computer Systems and Communication Lab, # * Institute of Information Science, Academia Sinica. # * All rights reserved. # * # * Redistribution and use in source and binary forms, with or without # * modification, are permitted provided that the following conditions # * are met: # * # * . Redistributions of source code must retain the above copyright # * notice, this list of conditions and the following disclaimer. # * . Redistributions in binary form must reproduce the above copyright # * notice, this list of conditions and the following disclaimer in # * the documentation and/or other materials provided with the # * distribution. # * . Neither the name of the Computer Systems and Communication Lab # * nor the names of its contributors may be used to endorse or # * promote products derived from this software without specific # * prior written permission. # * # * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # * “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS # * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE # * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, # * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR # * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) # * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, # * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) # * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED # * OF THE POSSIBILITY OF SUCH DAMAGE. # */ # # Copyright 1996 Chih-Hao Tsai

Beckman Institute, University of Illinois

c-tsai4uiuc.edu http://casper.beckman.uiuc.edu/~c-tsai4 # # ————————-COPYING.libtabe——-END———————————————— # # # ————————-COPYING.ipadic——-BEGIN———————————————— # # Copyright 2000, 2001, 2002, 2003 Nara Institute of Science # and Technology. All Rights Reserved. # # Use, reproduction, and distribution of this software is permitted. # Any copy of this software, whether in its original form or modified, # must include both the above copyright notice and the following # paragraphs. # # Nara Institute of Science and Technology (NAIST), # the copyright holders, disclaims all warranties with regard to this # software, including all implied warranties of merchantability and # fitness, in no event shall NAIST be liable for # any special, indirect or consequential damages or any damages # whatsoever resulting from loss of use, data or profits, whether in an # action of contract, negligence or other tortuous action, arising out # of or in connection with the use or performance of this software. # # A large portion of the dictionary entries # originate from ICOT Free Software. The following conditions for ICOT # Free Software applies to the current dictionary as well. # # Each User may also freely distribute the Program, whether in its # original form or modified, to any third party or parties, PROVIDED # that the provisions of Section 3 (“NO WARRANTY”) will ALWAYS appear # on, or be attached to, the Program, which is distributed substantially # in the same form as set out herein and that such intended # distribution, if actually made, will neither violate or otherwise # contravene any of the laws and regulations of the countries having # jurisdiction over the User or the intended distribution itself. # # NO WARRANTY # # The program was produced on an experimental basis in the course of the # research and development conducted during the project and is provided # to users as so produced on an experimental basis. Accordingly, the # program is provided without any warranty whatsoever, whether express, # implied, statutory or otherwise. The term “warranty” used herein # includes, but is not limited to, any warranty of the quality, # performance, merchantability and fitness for a particular purpose of # the

program and the nonexistence of any infringement or violation of # any right of any third party. # # Each user of the program will agree and understand, and be deemed to # have agreed and understood, that there is no warranty whatsoever for # the program and, accordingly, the entire risk arising from or # otherwise connected with the program is assumed by the user. # # Therefore, neither ICOT, the copyright holder, or any other # organization that participated in or was otherwise related to the # development of the program and their respective officials, directors, # officers and other employees shall be held liable for any and all # damages, including, without limitation, general, special, incidental # and consequential damages, arising out of or otherwise in connection # with the use or inability to use the program or any product, material # or result produced or otherwise obtained by using the program, # regardless of whether they have been advised of, or otherwise had # knowledge of, the possibility of such damages at any time during the # project or thereafter. Each user will be deemed to have agreed to the # foregoing by his or her commencement of use of the program. The term # “use” as used herein includes, but is not limited to, the use, # modification, copying and distribution of the program and the # production of secondary products from the program. # # In the case where the program, whether in its original form or # modified, was distributed or delivered to or received by a user from # any person, organization or entity other than ICOT, unless it makes or # grants independently of ICOT any specific warranty to the user in # writing, such person, organization or entity, will also be exempted # from and not be held liable to the user for any such damages as noted # above as far as the program is concerned. # # ————————-COPYING.ipadic——-END———————————————— 3. Lao Word Break Dictionary Data (laodict.txt) # Copyright © 2013 International Business Machines Corporation # and others. All Rights Reserved. # # Project: http://code.google.com/p/lao-dictionary/ # Dictionary: http://lao-dictionary.googlecode.com/git/Lao-Dictionary.txt # License: http://lao-dictionary.googlecode.com/git/Lao-Dictionary-LICENSE.txt # (copied below) # # This file is derived from the above dictionary, with slight modifications. # —— # Copyright © 2013 Brian Eugene Wilson, Robert Martin Campbell. # All rights reserved. # # Redistribution and use in source and binary forms, with or without modification, # are permitted provided that the following conditions are met: # # Redistributions of source code must retain the above copyright notice, this # list of conditions and the following disclaimer. Redistributions in binary # form must reproduce the above copyright notice, this list of conditions and # the following disclaimer in the documentation and/or other materials # provided with the distribution. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND # ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED # WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE # DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR # ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; # LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON # ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS # SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. # —— 4. Burmese Word Break Dictionary Data (burmesedict.txt) # Copyright © 2014 International Business Machines Corporation # and others. All Rights Reserved. # # This list is part of a project hosted at: # github.com/kanyawtech/myanmar-karen-word-lists # # —— # Copyright © 2013, LeRoy Benjamin Sharon # All rights reserved. # # Redistribution and use in source and binary forms, with or without modification, # are permitted provided that the following conditions are met: # # Redistributions of source code must retain the above copyright notice, this # list of conditions and the following disclaimer. # # Redistributions in binary form must reproduce the above copyright notice, this # list of conditions and the following disclaimer in the documentation and/or # other materials provided with the distribution. # # Neither

the name Myanmar Karen Word Lists, nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND # ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED # WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE # DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR # ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; # LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON # ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS # SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. #

——— 5. Time Zone Database ICU uses the public domain data and code derived from Time Zone Database for its time zone support. The ownership of the TZ database is explained in BCP 175: Procedure for Maintaining the Time Zone Database section 7. 7. Database Ownership The TZ database itself is not an IETF Contribution or an IETF document. Rather it is a pre-existing and regularly updated work that is in the public domain, and is intended to remain in the public domain. Therefore, BCPs 78 [RFC5378] and 79 [RFC3979] do not apply to the TZ Database or contributions that individuals make to it. Should any claims be made and substantiated against the TZ Database, the organization that is providing the IANA Considerations defined in this RFC, under the memorandum of understanding with the IETF, currently ICANN, may act in accordance with all competent court orders. No ownership claims will be made by ICANN or the IETF Trust on the database or the code. Any person making a contribution to the database or code waives all rights to future claims in that contribution or in the TZ Database. “”“

———

PCSC (Version: 5.1.0)
Authors: Daniel Mueller
URL: https://github.com/danm-de/pcsc-sharp

Copyright © 2007-2019 Daniel Mueller
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Changes to this license can be made only by the copyright author with
explicit written consent.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PeterO.Cbor (Version: 4.5.2)
Authors: Peter Occil
URL: https://github.com/peteroupc/CBOR

Creative Commons Legal Code

CC0 1.0 Universal CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN “AS-IS” BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY
FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS
PROVIDED HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an “owner”) of an original work of authorship and/or a database (each, a “Work”).

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works (“Commons”) that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the “Affirmer”), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and

publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

1. Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following: i. the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work; ii. moral rights retained by the original author(s) and/or performer(s); iii. publicity and privacy rights pertaining to a person's image or likeness depicted in a Work; iv. rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below; v. rights protecting the extraction, dissemination, use and reuse of data in a Work; vi. database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and vii. other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof. 2. Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose. 3. Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose. 4. Limitations and Disclaimers. a. No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document. b. Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law. c. Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work. d. Affirmer understands and acknowledges that Creative Commons is not a party to this

document and has no duty or obligation with respect to this CC0 or use of the Work.

Pkcs11Interop (Version: 5.1.2)
Authors: Jaroslav Imrich
URL: https://www.pkcs11interop.net/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or

counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields

enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2012-2021 The Pkcs11Interop Project Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Portable.BouncyCastle (Version: 1.9.0)
Authors: Claire Novotny
URL: https://www.bouncycastle.org/csharp/

The MIT License (MIT)

© 2000-2021 Legion of the Bouncy Castle Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PriorityQueue (Version: 0.1.0)
Authors: Denis Shulepov
URL: https://github.com/dshulepov/ConcurrentPriorityQueue

The MIT License (MIT)

Copyright 2015

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PuTTY (Version: 0.76)
Authors: Simon Tatham
URL: https://www.putty.org

PuTTY is copyright 1997-2021 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, Josh Dersch, Lars Brinkhoff, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

QRCoder (Version: 1.4.3)
Authors: Raffael Herrmann
URL: https://github.com/codebude/QRCoder/

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Radius (Version: 2.0.0.2)
Authors: Front Porch Inc.
URL: https://github.com/frontporch/Radius.NET

The MIT License (MIT)

Copyright 2016

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SSH.NET (Version: 2020.0.1)
Authors: Renci
URL: https://github.com/sshnet/SSH.NET/

The MIT License (MIT)

2012-2021, RENCI

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SharpVectors.Reloaded (Version: 1.7.7)
Authors: Elinam LLC (Japan)
URL: https://github.com/ElinamLLC/SharpVectors

BSD-3-Clause

Copyright © 2010 – 2021 Elinam LLC

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SuperSocket.ClientEngine.Core (Version: 0.10.0)
Authors: Kerry Jiang
URL: http://www.supersocket.net/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the

Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing

herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Tanneryd.BulkOperations.EF6 (Version: 1.4.1)
Authors: Måns Tånneryd

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii)

beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that

such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2017-2021 Tånneryd IT AB Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

UAParser (Version: 3.1.47)
Authors: enemaerke
URL: https://github.com/ua-parser/uap-csharp

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute

must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright 2020 Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

WebSocket4Net (Version: 0.15.2)
Authors: Kerry Jiang
URL: http://websocket4net.codeplex.com/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that

Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or

class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

WebSocketSharp (Version: 1.0.3-rc11)
Authors: sta
URL: http://sta.github.io/websocket-sharp

The MIT License (MIT)

© 2010-2016 sta.blockhead

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Z.EntityFramework.Plus.EF6 (Version: 6.13.10)
Authors: ZZZ Projects
URL: https://entityframework-plus.net/

The MIT License (MIT)

Copyright © ZZZ Projects

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal

in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

---

xxHash4net (Version: 1.2.0)
Authors: ailen0ada
URL: https://github.com/ailen0ada/xxHash4net

BSD 2-Clause License (http://www.opensource.org/licenses/bsd-license.php)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
