# Password Safe V8

8.3.0 — Letzte Änderung: 2017/11/29

MATESO GmbH

# Inhaltsverzeichnis

**Herzlich Willkommen… 4**
Warum Password Safe? 6
Was gibt es Neues in Version 8? 8
Mit der richtigen Edition zum Ziel 10
Lizenzmodel 12

**Sicherheit 13**
Genutzte Verschlüsselungsalgorithmen 15
Externe Penetrationstests 17
IT-Security Made in Germany 20

**Erste Schritte 21**

**Architektur und Systemanforderungen 24**
Systemanforderungen MSSQL 27
Systemanforderungen Server 29
Systemanforderungen Client 33
Systemanforderungen WebClient 34

**Installation 36**
Installation AdminClient 38
Installation Client 42
Installation mit Parametern 48
Installation WebClient 49
Updates 59

**Berechtigungskonzept und Schutzmechanismen 62**
Manuelles Berechtigen 67
Nutzung von Rechtevorlagen 72
Mehrfachbearbeitung von Berechtigungen 73
Automatisiertes Berechtigen 79
Vererbung aus Organisationsstrukturen 81
Rechte vordefinieren 85
Arbeiten mit vordefinierten Rechten 88
Relevante Benutzerrechte 92
Geltungsbereich vordefinierter Rechte 93
Schutzmechanismen 95
Sichtbarkeit 98
Temporäre Berechtigungen 100
Sichtschutz 102
Siegel 105
Siegelübersicht 113

Freigabemechanismus ... 116

**Bedienung und Aufbau ... 119**
Ribbon ... 123
Filter ... 127
Anzeigemodus ... 132
Erweiterte Filtereinstellungen ... 134
Listenansicht ... 139
Lesebereich ... 145
Tags ... 149
Suche ... 152
Dashboard und Widgets ... 155
Tastaturkürzel ... 161

**Client Module ... 162**
Passwörter ... 165
Erstellen neuer Passwörter ... 169
Aufdecken von Passwörtern ... 173
Verschieben von Passwörtern ... 177
Formularfeldberechtigungen ... 179
Passworteinstellungen ... 182
Historie ... 183
Dokumente ... 187
Benachrichtigungen ... 190
Organisationsstruktur ... 194
Benutzerverwaltung ... 199
Benutzer Passwörter / Anmeldung am Client ... 202
Berechtigungen auf Organisationsstrukturen ... 206
Vererbung von Berechtigungen ... 208
Active Directory Anbindung ... 209
Ende zu Ende Verschlüsselung ... 212
Master Key Modus ... 219
Multifaktor-Authentifizierung ... 225
Yubico / Yubikey ... 229
Rollen ... 235
Formulare ... 238
Formulare wechseln ... 242
Logbuch ... 245
Anwendungen ... 247
Anlernen von Anwendungen ... 252
Sitzung aufzeichnen ... 258
Startparameter ... 262
SAP GUI Logon ... 265

Password Reset ... 268

**Hauptmenü ... 273**
Extras ... 274
Passwortrichtlinien ... 275
Passwortgenerator ... 279
Berichte ... 283
System Tasks ... 287
Siegelvorlagen ... 291
Tagverwaltung ... 293
Allgemeine Einstellungen ... 296
Import ... 297
Export ... 302
HTML WebViewer Export ... 305
Export Assistent ... 308
Benutzerrechte ... 311
Benutzereinstellungen ... 315
Administration ... 319
Konto ... 321

**SSO Agent ... 324**
Konfiguration ... 327
Addons ... 331
Anwendungen ... 336

**WebClient ... 342**
Funktionsumfang ... 343
Passwort Modul ... 344
Tag Modul ... 345
Bedienung ... 346
Header ... 348
Navigationsleiste ... 349
Filter- bzw. Strukturbereich ... 351
Menü ... 353
Listenansicht ... 355
Lesebereich ... 357
Einstellungen ... 358

**Admin Client ... 359**
Grundkonfiguration ... 360
Zertifikate ... 363
Einrichtungsassistent ... 369
Erstellen von Datenbanken ... 376
Migration ... 379

Vorbereitungen ... 381
Starten des Migrationslaufs ... 384
Zuordnung von Tags und OUs ... 388
Berechtigungen nach der Migration ... 391
Checkliste nach der Migration ... 393
Bedienung und Aufbau ... 397
Verwaltung von Datenbanken ... 402
Datenbank Firewall ... 405
Hauptmenü ... 408
Allgemeine Einstellungen ... 409
Backup-Einstellungen ... 410
Backupverwaltung ... 412
Desaster Recovery Szenarien ... 417
Lizenzeinstellungen ... 420
Erweiterte Einstellungen ... 422

**Offline Client ... 424**
Einrichten und Synchronisieren ... 426

**Hochverfügbarkeit ... 431**

**Versionshistorie ... 432**
Version 8.3.0.13358 ... 433
Version 8.2.0.12388 Hotfix 1 ... 436
Version 8.2.0.12343 ... 437
Version 8.1.1.11211 Hotfix 1 ... 441
Version 8.1.1.11106 ... 442
Version 8.1.0.10812 ... 444
Version 8.0.2.9978 Hotfix 2 ... 452
Version 8.0.2.9541 Hotfix 1 ... 453
Version 8.0.2.9278 ... 454
Version 8.0.1.9032 ... 456

# Herzlich Willkommen…

…in der offiziellen Hilfe des **Password Safe by MATESO**. Sowohl unsere Bestandskunden als auch alle Interessierten möchten wir in Form des folgenden Kompendiums beim Einstieg in die **Version 8** maximal unterstützen. Unsere Bestandskunden profitieren wie gewohnt von aktiver Softwarepflege, indem sie kostenlosen Zugang zum Upgrade auf die neue Version 8 erhalten. Kontaktieren Sie uns gerne über die Ihnen bekannten Kanäle, falls Sie weitere Informationen wünschen.

Falls Sie sich noch nicht sicher sind, welcher Plan am besten Ihren Anforderungen entspricht, nutzen Sie bitte unsere Erläuterung zu den Editionen.

> Ein wesentlicher Grundpfeiler des nie aufkommenden Stillstandes sind die stetigen Rückmeldungen unserer Kunden, welche uns durch die Äußerung von Wünschen und Anregungen tagtäglich zur kundenorientierten Weiterentwicklung unserer Produkte motivieren. Nur durch Ihre direkte Rückmeldung ist es möglich, die vorliegenden Hilfeseiten auch weiterhin an Ihre Bedürfnisse anzupassen.

Wir freuen uns sehr, dass Sie im Zuge einer für beide Seiten gehaltvollen Zusammenarbeit zukünftig auf den Password Safe Version 8 vertrauen. Viel Spaß beim Schmökern!

Ihr Password Safe Team

- Warum Password Safe?
- Was gibt es Neues in der Version 8?
- Mit der richtigen Edition zum Ziel

# Warum Password Safe?

## Die Abhängigkeit gegenüber Passwörtern…

…ist heutzutage größer denn je. Nirgendwo sind diese aus dem Tagesgeschäft von Unternehmen wegzudenken. Sie kommen überall und ständig zum Einsatz – und wollen dabei noch professionell verwaltet werden. Sicher sollen sie sein, mindestens zwölfstellig und dabei Groß- und Kleinschreibung sowie Sonderzeichen beinhalten. Im Optimalfall sollte für jeden Account ein separates Zugangskennwort genutzt werden, welches in kurzen zeitlichen Abständen regelmäßig geändert wird. Es ist schon schwer genug diese Herausforderung privat zu meistern. Innerhalb großer Unternehmen ist es jedoch unwahrscheinlich, dass man sich dieser Aufgabe ohne den Einsatz eines professionellen Passwortverwaltungstools adäquat und nach bestem Gewissen stellen kann.

## Die beliebige Skalierbarkeit…

…des Password Safe ermöglicht den Einsatz in sowohl KMUs, Großunternehmen als auch weltweit agierenden Konzernen. Die hierfür notwendige Flexibilität war ein treibendes Argument dafür, nicht die Vorgängerversion weiterzuentwickeln, sondern in Form einer kompletten Neuentwicklung den stetig voranschreitenden Anforderungen moderner und sicherheitsbewusster Unternehmen gerecht zu werden. Password Safe stellt in der Version 8 somit die perfekte Softwarelösung für all diejenigen Unternehmen dar, welche sicherheitsrelevante Daten wie Passwörter, Dokumente oder Zertifikate auf allerhöchstem Verschlüsselungsniveau effektiv verwalten wollen. Mittlerweile vertrauen über 10.000 Unternehmenskunden auf MATESO, den Marktführer für professionelles Passwortmanagement in Deutschland, Österreich und der Schweiz.


Jupiter
440044
Kirschelf2
optcna
sunrise
Internet_21
FRITZ!
bigfoot
apollo_13
HARRY-POTTER
schatzi
Steiman
Steffili
wolf3
megan_6
4444
Lilli_1
2dumm_13
ANZEINA
Enter Password

# Was gibt es Neues in Version 8?

## Versionshistorie

Die aktuellen Patchnotes sind stets unter folgendem Link abrufbar.

## Ein wesentlicher Grundpfeiler…

…des nie aufkommenden Stillstandes sind die stetigen Rückmeldungen unserer Kunden, welche uns durch Lob einerseits unseren richtigen Kurs bestätigt haben und uns anderseits durch die Äußerung von Wünschen und Anregungen tagtäglich zur kundenorientierten Weiterentwicklung unserer Produkte motivieren. Wir möchten uns hiermit für Ihr Feedback bedanken und Ihnen in Form von Password Safe Version 8 die folgenden Features ankündigen:

- Komplett überarbeitetes, intuitives Bedienkonzept
- Frei konfigurierbare Dashboards für den täglichen Überblick
- Neu entwickelte SSO-Engine für die Anmeldung an Anwendungen und Webseiten
- Neue moderne Addons für Browser
- Native RDP und SSH Integration
- Fortschrittliches Tag-System zur optimalen Klassifizierung Ihrer Daten
- Individuell anpassbare Suchfilter inkl. Volltextsuche
- Signifikante Leistungssteigerung durch die neu entwickelte Stateless Multi-Tier-Architektur
- Ende-zu-Ende Verschlüsselung (E2EE)
- Verwaltung privilegierter Accounts inkl. Password Reset und Password Discovery
- Maximale Verschlüsselung durch synchrone und asynchrone Verfahren
- Mehr-Faktor-Authentifizierung
- Rechte bis auf Datensatzebene inkl. temporärer Freigaben
- Umfangreiches Reporting für Audits
- U.v.m

## Berechtigungsadministration als Basis

Berechtigungsadministration auf Basis von Rollen und Organisationsstrukturen ist eines der zentralen Themen in Password Safe Version 8. Ziel ist es, die in einem Unternehmen existierenden Hierarchien innerhalb des Rollenkonzepts einwandfrei und lückenlos abzubilden. Durch einen Abgleich mit dem Active Directory können bereits bestehende Strukturen importiert und bei Bedarf angepasst werden. Sowohl Benutzerinformationen als auch Gruppenzugehörigkeiten werden somit direkt aus dem Microsoft Verzeichnisdienst übernommen. Optional unterbindet Ende-zu-Ende Verschlüsselung (E2EE), dass

private Benutzerschlüssel zum Server übermittelt werden, was zumindest theoretisch einen Angriffspunkt darstellen kann.

Mit Hilfe des ausgeklügelten Berechtigungskonzepts ist sichergestellt, dass jede Benutzergruppe, bzw. Abteilung, stets nur Zugang zu denjenigen Passwörtern erhält, auf die diese auch berechtigt sein sollen. Gestützt durch Assistenten, Rechtepresets sowie intuitiv gestaltete Vererbungsmethoden trägt man den Anforderungen hierarchisch verschachtelter Benutzerstrukturen in Großunternehmen und Konzernen Rechnung.

## Privilegiertes Passwortmanagement

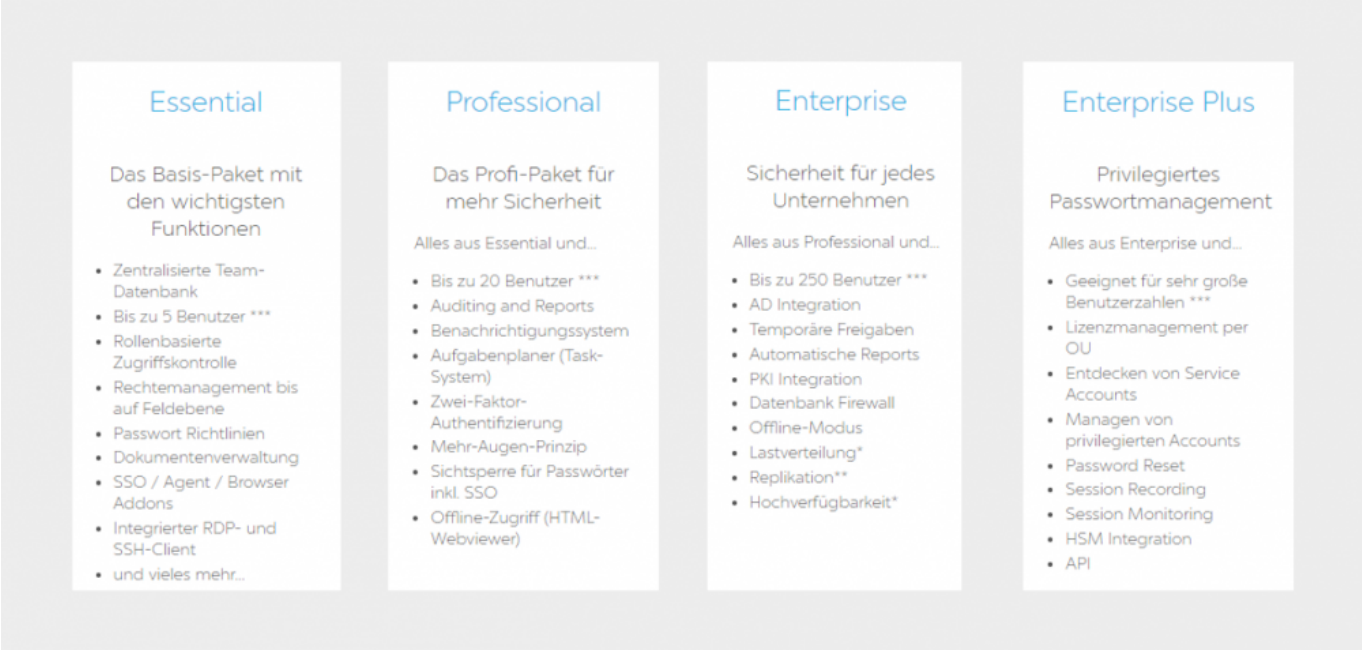
Service Accounts und administrative Zugänge mit weitreichenden Berechtigungen sind stets die zentralen Schwachstellen in Unternehmen und waren in der Vergangenheit vermehrt Einfallstor für Angreifer und Manipulationen. Aufgrund der Masse an existierenden, historisch gewachsenen Accounts, gestaltet sich deren Wartung und Verwaltung als durchwegs schwierig. Mit Password Discovery & Reset liefert MATESO nun zwei Werkzeuge zum Schutz dieser beliebten Angriffsziele. Password Discovery erstellt mittels Scan der vorhandenen Netzwerkstrukturen eine Liste an Accounts, welche direkt innerhalb des Password Safe erfasst werden. Diese Zugänge können daraufhin mit Hilfe von Password Reset bei Dienstkonten, Active Directory Zugängen oder auch Windows- und MSSQL-Benutzern nach frei definierbaren Zeiträumen automatisch neu gesetzt werden.

## SSO, Protokollierung und Reporting

Single Sign On (SSO) ist aus Firmenlandschaften nicht mehr wegzudenken. Mit Hilfe des neu konzipierten SSO-Agents ist die automatische Anmeldung an Websites intuitiv und einfach durchführbar. Auch Verbindungen über RDP oder SSH können problemlos automatisiert werden. Eine Besonderheit des Password Safe ist es, dass Passwörter für diese Zugänge stets durch eine Sichtsperre den Benutzern vorenthalten werden können. Besonders sicherheitskritische Anmeldungen können durch das Mehr-Augen-Prinzip des Siegelsystems zusätzlich abgesichert werden. Selbstverständlich ist Nachvollziehbarkeit von Änderungen durch Logs und Historie jederzeit gegeben. Auch Dokumente können in der Datenbank gepflegt und durch die integrierte Versionsverwaltung zwecks Protokollierung und eventueller Wiederherstellung archiviert werden. Password Safe v8 liefert mit dem vollkommen automatisierbaren Reporting-System zudem ein granular definierbares Werkzeug für Sicherheitsaudits.

# Mit der richtigen Edition zum Ziel

## Verfügbare Pläne




### Essential

Die Essential Edition ermöglicht den Einstieg in die Welt der professionellen Passwortverwaltung. Beachten Sie, dass beim Kauf stets genau 5 Benutzer enthalten sind. Die Essential Edition kann ausschließlich im Webshop erworben werden.

### Professional

Die Professional Edition ist für kleinere und mittlere Teams bis 20 Personen ausgelegt. Zusätzlich zu den in der Essential enthaltenen Grundfunktionalitäten sind Sichtsperre auf Passwörter, Single Sign On Agent sowie Reporting und Auditing möglich.

### Enterprise

Die Enterprise Edition richtet sich an größere Teams und firmenweite Roll-Outs mit maximal 250 Usern. Die Funktionen der Professional Edition werden ergänzt durch Active Directory Integration, temporäre Freigaben sowie die Möglichkeit, einen zweiten Faktor in die Anmeldung mit einzubeziehen.

### Enterprise Plus

Die Enterprise Plus Version ist praktisch für eine unbegrenzte Anzahl an Usern ausgelegt und beinhaltet sowohl eine API sowie die für große Konzerne unverzichtbaren Features Auto Discovery und Password Reset.

> Falls Sie weitere Informationen zu den Editionen oder deren Preisen haben, oder an einer Testlizenz interessiert sind, nutzen Sie bitte direkt den Weg über die offizielle Homepage.

# Lizenzmodel

## Wie erfolgt die Lizenzierung?

Die Lizenzierung im Password Safe erfolgt stets auf Basis der Benutzeranzahl. Das Named User Modell sieht demnach vor, dass jeder Benutzer seine eigene Lizenz erhält. Stichpunktartig gelten die folgenden Rahmenbedingungen:

- Es ist unerheblich, in welchem Umfang der Password Safe genutzt wird. Jeder Benutzer benötigt seine eigene Lizenz.
- Der Einsatz von Light Lizenzen ist (aktuell) nicht vorgesehen
- Auch die alleinige Nutzung des SSO Agent bedingt den Besitz einer vollwertigen Lizenz

## Module aus der Version 7

Im Gegensatz zur Version 7 existieren keinerlei Module mehr. Die Lizenzierung pro Rechner konnte in der Vorgängerversion noch mittels Modulen angepasst werden (Modul Ohne Clientlizenzierung). Dies ist nicht mehr nötig. Alle Lizenzierungsverfahren sind durch das oben genannte Lizenzmodel abgedeckt.

# Sicherheit

## IT-Sicherheit im Wandel

Es ist ein erklärtes Ziel, dass die digitalen Infrastrukturen Deutschlands zu den sichersten weltweit gehören sollen. Das im Juli 2015 in Kraft getretene **IT-Sicherheitsgesetz** soll hierfür die Blaupause bilden und wegbereitend die deutsche Vorreiterstellung im Kampf gegen digitale Bedrohungen sichern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI), welches ebenso für die **ISO 27001 Zertifizierung auf Basis der IT-Grundschutz-Kataloge** Verantwortlichkeit zeichnet, stellt hierfür schon seit langem die Weichen. Auch auf europäischer Ebene wird durch die **Richtlinie zur Netz- und Informationssicherheit (NIS)**, dem Pendant zum deutschen IT-Sicherheitsgesetz, der potentiellen Gefahrenlage Rechnung getragen. Durch die EU-weite Stärkung der Widerstandsfähigkeit gegenüber Risiken aus dem Internet sollen derlei kriminelle Energien weiter eingedämmt werden.


## Gefahren und Risiken

Dies ist als Reaktion auf eine Gefahrenlage einzuschätzen, welche konkreter nicht sein könnte: Das Bundeskriminalamt schätzt die Anzahl digitaler Angriffe auf deutsche Unternehmen auf 300.000 – am Tag. Auch die Netze des Bundes geraten laut dem Bundesamt für Verfassungsschutz über eine Million Mal jährlich ins Visier von Hackern mit finanziellem Interesse, politisch motivierten „Hacktivisten“ und natürlich auch Geheimdiensten. Das BKA warnt schon seit Jahren vor Erpressungswellen im Internet, sowohl im privaten Sektor wie auch im Firmenumfeld. Erworbene Diebesgüter in Form von sicherheitskritischen Unternehmensinterna sind regelmäßig Gegenstand von Erpressungen.

# Passwörter als Achillesferse

Aufgrund des raschen digitalen Wandels rückt besonders das Thema Passwortsicherheit immer mehr in den Fokus. Kennwörter, welche vor 5 Jahren noch als relativ sicher einzustufen waren, müssen aufgrund des technischen Fortschritts erneut auf den Prüfstand. Ausschließlich zufällig gewählte Passwörter mit einer entsprechenden Ziffernlänge können diese Problematik wirklich nachhaltig entschärfen. Darüber hinaus ist dafür Sorge zu tragen, dass diese Kennwörter in vordefinierten Intervallen geändert werden.

# Der Lösungsansatz des MATESO Password Safe

Die sichersten Passwörter sind immer noch diejenigen, welche den Usern komplett vorenthalten werden können. Über **automatische Eintragungen** ermöglicht man den Benutzern effizientes Arbeiten, ohne das Wissen um das Passwort freigeben zu müssen. Mittels fortschrittlichster Methoden des **Password Reset** sind diese Zugangskennwörter zudem automatisiert in beliebig kurzen Intervallen zurücksetzbar. Hinzu kommen Sicherheitsmechanismen, welche Zugang zu Systemen gemäß dem **Mehr-Augen-Prinzip** an die Erteilung einer Freigabe durch Berechtigte koppeln. All diese Routinen werden durch **hochkomplexe Verschlüsselungsverfahren** gesichert. Regelmäßige Penetrationstests sorgen dafür, dass die Software gezielt von unabhängigen Experten auf Schwachstellen in der Architektur sowie korrekten Einsatz modernster kryptographischer Technologien geprüft wird. Zusammenfassend: menschliches Fehlverhalten im Umgang mit Passwörtern muss durch technisch erzwungene Vorgaben und Workflows auf ein Minimum reduziert werden. Christian Strobel, COO der MATESO GmbH:

> Egal ob KMUs, globaler Konzern oder staatliche Behörde: Will man zukünftig das Risiko von Datenklau und IT-Terrorismus minimieren, ist einerseits die Auseinandersetzung mit der Thematik in ausreichendem Maße unabdingbar, andererseits der Einsatz einer professionellen Passwort Management Software alternativlos.

- Genutzte Verschlüsselungsalgorithmen
- Externe Penetrationstests
- IT-Security Made in Germany

# Genutzte Verschlüsselungsalgorithmen

## Verschlüsselungsalgorithmen

Sicherheit bildete schon während der Konzeptionierung stets einen der elementarsten Grundpfeiler, an dem sich alle weiteren Anforderungen orientieren und messen mussten. Auch parallel zur Entwicklungsphase wurden die theoretischen Konzepte von externen Sicherheitsunternehmen in Bezug auf Machbarkeit, sowie auf die Einhaltung von IT-Sicherheitsstandards geprüft. Erst auf Basis dieser Erkenntnisse wurden letztendlich Prototypen entwickelt, welche die Blaupause für das jetzige Password Safe in der Version 8 bilden. Folgende Verschlüsselungstechniken und Algorithmen kommen derzeit zum Einsatz:

- AES 256
- PBKDF2 mit 100.000 Iterationen für die Bildung von Benutzer Hashes
- PBKDF2 mit 1.000 Iterationen für die Hashes der Passwörter innerhalb der Datenbank
- RSA 4096 für Private- und Public-Key Verfahren

## Angewandte kryptografische Verfahren

Die Containerverschlüsselung der Passwörter basiert auf den genannten Algorithmen. Jeder Container hat einen eigenen, zufällig generierten Salt. Jedes Passwort, jeder Benutzer und jede Rolle besitzt ein eigenes Schlüsselpaar. Bei der Gewährung von Freigaben über Benutzer und Rollen finden hierarchische Verschlüsselungen der Passwörter innerhalb der Datenbank Anwendung. Zusätzlich nutzt Password Safe zum Ziele maximaler Sicherheit unter anderem die nachfolgenden kryptografischen Verfahren:

- Bei AD-Anbindung Wahl zwischen Ende-zu-Ende Verschlüsselung (E2EE – sicherster Modus) oder Masterkey Verfahren
- Schutz der Serverschlüssel per Hardware Sicherheitsmodul (HSM) über PKCS#11
- Brute-Force Schutz beim Login mit automatischer Sperre der anfragenden Clients
- Zertifikatsschutz bei der Nutzung von Anwendungen
- Zertifikatsabfrage bei Client/Server Verbindung. Optional auch mit eigener CA.
- Secure Sockets Layer (SSL) auf dem neusten Standard
- Passwörter werden erst dann verschlüsselt zum Client transportiert, wenn diese im Vorfeld explizit angefragt wurden. Mehr…

! Verschlüsselt werden ausschließlich Secrets. Metadaten werden aus Gründen der Suchgeschwindigkeit nicht verschlüsselt. In der Regel handelt es sich bei Secrets um

Passwörter. Die Entscheidung, welche Daten Secrets sind, liegt jedoch beim Kunden. Es ist zu beachten, dass nach Secrets nicht gesucht werden kann.

# Von uns getestete Security Hardwarekomponenten:

### HSM:

- SafeNet Luna SA – HSM mit Netzwerkanbindung
- SafeNet Luna PCI-E – Embedded-HSM

### Zwei-Faktor-Authentifizierung:

- SafeNet eToken Pass
- RSA SecurID 700
- Google Authenticator

# Externe Penetrationstests

## Penetrationstests durch die SySS GmbH

Seit mehr als 15 Jahren liegt der Fokus der SySS GmbH auf der Durchführung von Software Penetrationstests (PenTests), sowie der Wahrung maximaler Sicherheit von IT-Infrastrukturen in Unternehmen jeglicher Branche und Größe. Die Tübinger Sicherheitsspezialisten zählen mittlerweile branchenübergreifend mehr als 20 der DAX30 Konzerne zu ihren Kunden. Darüber hinaus vertrauen zudem auch staatliche Einrichtungen (Innenministerium, Bundeswehr, Deutsche Flugsicherung, …) dem Expertenurteil der SySS GmbH. Die professionelle Zusammenarbeit mit dem Branchenprimus in etlichen Iterationen stellte die Weichen für die Schließung und fortlaufende Vermeidung potentieller Sicherheitslücken.

## Pentest der Version 8.3.0

Aufgrund des immens gestiegenen Funktionsumfangs seit dem letzen Pentest, wurde die Version 8.3.0 einem erneuten Test unterzogen. Dieser konnte mit Bravour bestanden werden.

## Bestandteile des PenTests

Während des Tests wurden unter anderem die nachfolgenden Szenarien geprüft:

- Simulation clientseitiger Angriffe unterschiedlichster Ausprägungen
- Intensives Sourcecode Review
- Qualitative Beurteilung sämtlicher kryptografischer Verfahren

## Testbedingungen

Die SySS GmbH hatte zwecks lückenloser und granularer Durchführung der Tests jederzeit vollen Zugriff auf den Sourcecode sowie den Datenbankserver.

## Fazit des Tests


Den erfolgreich durchgeführten Test bescheinigte Sebastian Schreiber, Geschäftsführer der SySS GmbH.Hier einige Auszüge:

* Im Verlauf des Sicherheitstests war es der SySS GmbH nicht möglich, auf unautorisierte Weise auf geschützte Passwortinformationen und Dokumente fremder Benutzer der Softwareanwendung Password Safe 8 zuzugreifen, weder aus der Perspektive eines Benutzers mit Anmeldedaten noch aus der Perspektive eines externen Angreifers ohne Anmeldedaten. Die eingesetzten Verfahren bezüglich Authentifizierung, Autorisierung und Verschlüsselung sorgen nach Ansicht der SySS GmbH für einen effektiven Schutz der innerhalb der Anwendung gespeicherten sensiblen Daten.

* Nach Erkenntnissen der SySS GmbH ist ein Angreifer (…) nicht in der Lage, direkt auf Anmeldepasswörter im Klartext oder unverschlüsseltes RSA-Schlüsselmaterial von Benutzern zuzugreifen.

* Die Tatsache, dass ein Zugriff auf den privaten RSA-Schlüssel im Klartext nur mit vorheriger Eingabe des korrekten Passworts möglich ist und diese Authentifizierungsinformation somit von einer Person extern in das System der Anwendung Password Safe im Rahmen der Benutzeranmeldung eingebracht wird, bewertet die SySS GmbH als sehr positiv. Auch im Falle verschiedener Schwachstellen ist ein Angreifer dadurch nicht unmittelbar in der Lage, auf entsprechend verschlüsselte Daten wie Passwörter oder Dokumente zuzugreifen.

! Hinsichtlich der verwendeten Verschlüsselungsverfahren konnte die SySS GmbH im Rahmen des durchgeführten Sicherheitstests keine Schwachstellen finden.

Insgesamt bewertet die SySS GmbH das Sicherheitsniveau der getesteten Softwareversion der Anwendung Password Safe 8 als **sehr gut**.

# IT-Security Made in Germany

## Die TeleTrusT-Initiative

Die MATESO GmbH, wie auch der Password Safe and Repository selbst, sind Mitglied der TeleTrusT-Initiative “IT-Security Made in Germany”. Das Gütesiegel hat seine Wurzeln in der seit 2005 stark forcierten Zusammenarbeit des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft.

## Das Gütesiegel bescheinigt dem MATESO Password Safe in der Version 8 folgende Eigenschaften:

- Der Unternehmenshauptsitz ist in Deutschland
- Das Unternehmen bietet vertrauenswürdige IT-Sicherheitslösungen an
- Die angebotenen Produkte enthalten keine versteckten Zugänge
- Die IT-Sicherheitsforschung und -entwicklung des Unternehmens findet in Deutschland statt
- Das Unternehmen verpflichtet sich, den Anforderungen des deutschen Datenschutzrechtes zu genügen

# Erste Schritte

## Erste Schritte

Wir empfehlen Ihnen, sich bei der Installation von Password Safe Version 8 an die folgenden zehn Schritte zu halten. Es ist dringend zu empfehlen, dass alle durchgeführten Konfiguration, wie z.B. vergebene Passwörter und dergleichen, sauber notiert werden. Falls Sie während der Installation Lücken innerhalb der Hilfe finden, freuen wir uns sehr über eine kurze Rückmeldung. Sehr gerne ergänzen wir diese Punkte und stellen diese Ihnen sowie weiteren Password Safe Nutzern zur Verfügung.

### 1. Microsoft SQL Systemanforderungen

Microsoft SQL Server ist aufgrund des performanten Datenzugriffs, der weitläufigen Verbreitung sowie der umfangreichen Backupmöglichkeiten, das von uns eingesetzte Datenbankmanagementsystem.
Hier gehts zu den Systemanforderungen MSSQL

### 2. Systemanforderungen Anwendungsserver

Besonders die Unterkapitel benötigte Benutzer sowie Rechte auf die PowerShell Skripte sind zu beachten.
Hier gehts zu den Systemanforderungen des Anwendungsservers

### 3. Systemanforderungen Client

Die Anforderungen an die Clientumgebung sind durch uns separat definiert.
Hier gehts zu den Systemanforderungen des Clients

### 4. Installation des Admin Client


Gestützt durch einen Assistenten werden bei der Installation des Password Safe Admin Clients alle erforderlichen Parameter definiert.
Hier gehts zur Installation des Admin Clients

## 5. Password Safe Grundkonfiguration

Beim ersten Öffnen des Admin Clients startet direkt die Password Safe Grundkonfiguration. Diese geleitet per Assistent durch die Grundkonfiguration.
Hier gehts zu den Erläuterungen der Password Safe Grundkonfiguration

## 6. Authentifizierung am Admin Client

Nach dem Abschluss der Grundkonfiguration kann man sich direkt am Admin Client authentifizieren.

> Das Initialpasswort für den Admin Client lautet “admin”

## 7. Einrichtungsassistent

Der Einrichtungsassistent beinhaltet die Vergabe eines neuen Passwortes für den Password Safe Admin Client, die Einbindung der Lizenz sowie die Konfiguration der Datenbank- und SMTP- Einstellungen.
Hier gehts zum Einrichtungsassistenten

## 8. Erstellung von Datenbanken


Die MSSQL-Datenbanken können natürlich auch direkt über unseren Admin Client erstellt und organisiert werden.
Hier geht es zur Erstellung von Datenbanken

## 9. Installation des Clients


Die ebenso durch einen Assistenten begleitete Installation des Clients ist der erste Schritt, um Benutzern das Arbeiten mit Password Safe zu ermöglichen.

Hier gehts zur Installation des Clients

# 10. Erstellung von Datenbankprofilen

Die Anzahl der Datenbanken wird nicht lizenziert und ist demnach theoretisch beliebig. Um den Überblick zu wahren, hilft das Erstellen von Profilen, welche alle erforderlichen Parameter für eine erfolgreiche Anmeldung an einer Datenbank beinhalten.

Hier gehts zur Erstellung von Datenbankprofilen

# Architektur und Systemanforderungen

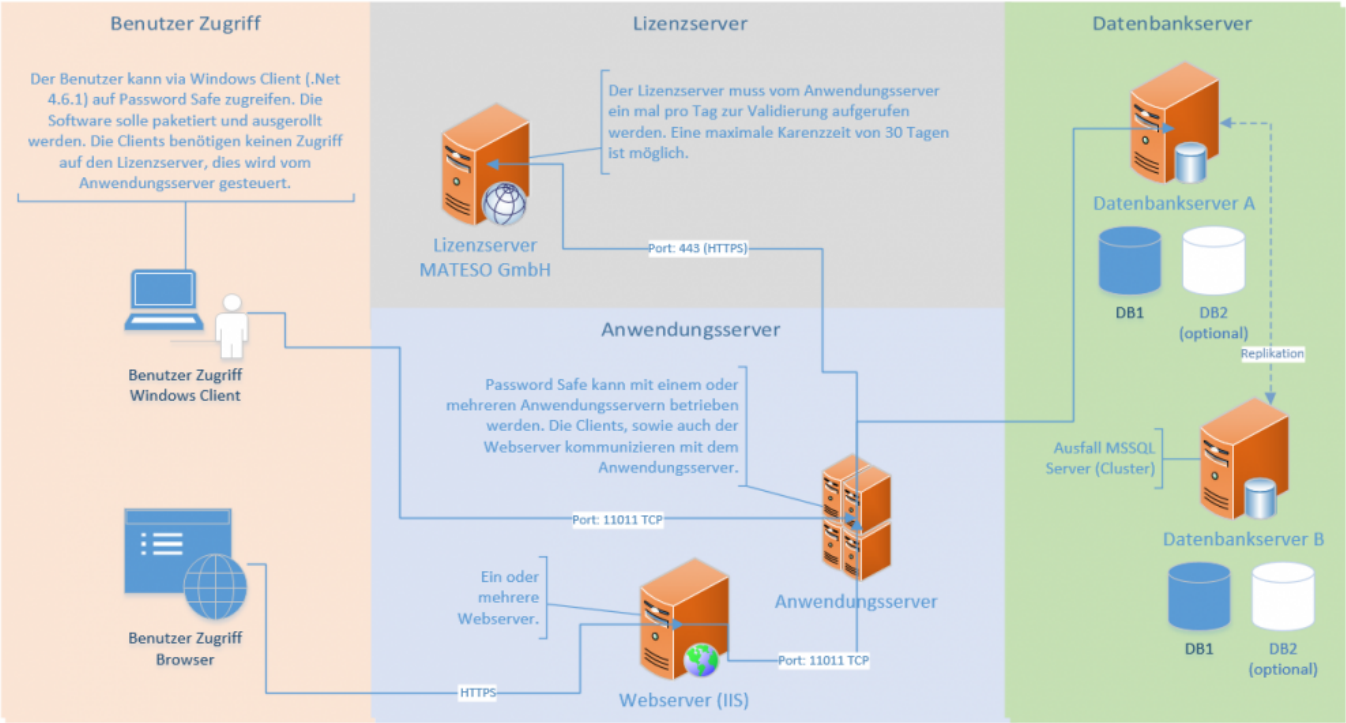
## Multi-Tier-Architektur

Die Struktur des Password Safe v8 basiert auf dem Prinzip der **Multi-Tier-Architektur**. Dieser mehrschichtige Aufbau der einzelnen Softwarekomponenten liefert die Basis für ein wohldurchdachtes und wegweisendes Sicherheitskonzept. Die Skalierbarkeit der drei separat agierenden Schichten ist jeweils beliebig. Dies hat zur Folge, dass der Password Safe v8 auch bei Konzernen mit sehr großen Benutzerzahlen sowie **weltweit verstreuten Standorten** effizient eingesetzt werden kann. Bei Nutzung der **„Ende-zu-Ende“ – Verschlüsselung** wird an den Clients ebenso das Verschlüsseln, bzw. Entschlüsseln der Daten durchgeführt. Dies stellt sicher, dass am Datenbankserver wie auch am Applikationsserver niemals unverschlüsselte Passwörter vorliegen. **Private- und Public-Key Verfahren** sorgen dafür, dass der private Schlüssel stets nur dem Benutzer vorliegt. Der Anwendungsserver kennt lediglich den Wert des öffentlichen Schlüssels und ist demzufolge nicht in der Lage, den Wert des Passwortes einzusehen.

Password Safe in der Version 8 kann in kleinen bis weltweiten Systemlandschaften eingeführt werden. Innerhalb der Multi-Tier-Architektur können beliebig viele Clients, Anwendungsserver und Datenbankserver angebunden werden. Es ist empfohlen, im Produktivsystem die Datenbank auf einem ausfallsicheren Cluster zu betreiben. Der Microsoft SQL Server kann die Daten, z.B.: via WAN an ein anderes Rechenzentrum replizieren. Ebenso empfehlen wir, jeweils einen separaten Windows Server bereitzustellen.

## Systemlandschaft

Die nachfolgende Übersicht bildet grafisch eine klassische Password Safe **Systemlandschaft** ab. In der Version 8 ist standortübergreifender Einsatz mit mehreren Datenbankservern möglich, welche dann mit Microsoft Bordmitteln untereinander synchronisiert werden. Für die Client-Verbindung können beliebig viele Anwendungsserver zur Verfügung gestellt werden, was aufgrund der Lastverteilung Arbeiten ohne nennenswerte Latenz ermöglicht. Besonders bei global aufgespannten Installationen bringt diese Technik enorme Performanzvorteile.




### Client (Präsentationsschicht)

Die Client-Schicht übernimmt die Darstellung aller Daten und Funktionen, welche vom Applikationsserver bereitgestellt werden.

### Applikationsserver (Business Logik)

Der Applikationsserver, auch Anwendungsserver genannt, ist für die gesamte Regulierung der Business Logik zuständig. Dieser Server liefert stets nur diejenigen Daten aus, für die dementsprechende Berechtigungen vorliegen. Die eingangs erläuterte Multi-Tier-Architektur ermöglicht den Einsatz mehrerer Applikationsserver und sorgt für effiziente Lastverteilung.

### Datenbankserver (Datenhaltung)

Aufgrund der weiten Verbreitung sowie der Möglichkeit, auch in großen und räumlich verteilten Umgebungen performanten Zugriff zu bieten, setzt Password Safe in der Version 8 im Hinblick auf die Datenhaltung komplett auf Microsoft SQL Server. Bei kleineren Installationen ist auch der Einsatz der kostenlosen Variante SQL Express möglich.

### Empfohlen sind somit mindestens drei Server:

- Datenbankserver (MSSQL)
- Anwendungsserver (Password Safe Dienste)
- Webserver (IIS)

! Wir empfehlen, im Produktivsystem die Datenbank auf einem ausfallsicheren Cluster zu betreiben. Der Microsoft SQL Server kann die Daten z.B. via WAN auf ein anderes Rechenzentrum replizieren. Ebenso empfehlen wir, je Funktion einen Windows Server bereitzustellen. Durch die Trennung der Systeme sind spätere Erweiterungen und Skalierungen einfacher umsetzbar. Dennoch ist die Trennung nicht zwingend erforderlich. Bei kleineren Installationen können demnach auch alle Komponenten auf einem Server installiert werden.

# Systemanforderungen MSSQL

## Benötigte Hardware

Zum Ziele der gesteigerten Ausfallsicherheit empfehlen wir, die Datenbank auf einem separaten MSSQL Datenbank Cluster zu installieren. Zusätzlich sollte die Datenbank in ein zweites, räumlich getrenntes Rechenzentrum gespiegelt werden. Nachfolgend unsere Empfehlung für den optimalen Betrieb:

- Min. Windows Server 2012 R2
- Empfohlen Windows Server 2016
- Min. 4 x CPU's
- Min. 16 GB RAM
- Min. 100 GB Festplattenspeicherplatz
- Installierter und bereits lizenzierter Microsoft MSSQL Server 2012 oder neuer (ab Express)

Der Applikationsserver benötigt die folgende Port Freigabe:

- Port 1433 TCP für die Kommunikation mit dem Anwendungsserver

> Unter folgendem Link ist ein Vergleich der unterschiedlichen MSSQL-Server-Editionen zu finden:
> **SQL Server Editionen**
> Hier sind auch die Kapazitätsgrenzen der einzelnen Editionen einsehbar.

## Benötigte Datenbanken

Während der Installation werden mindestens zwei Datenbanken angelegt:

1. die Konfigurationsdatenbank, welche sämtliche Einstellungen für die Anwendungsserver beinhaltet
2. die Hauptdatenbanken, welche alle Informationen über Benutzer und Datensätze halten

## Voraussetzungen

Das Erzeugen und Verwalten der beiden Datenbanken kann direkt über die Admin Konsole durchgeführt werden. Hierfür sind jedoch einige **Voraussetzungen** auf dem MSSQL-Server zu schaffen:

### Benutzer

Für die Password Safe V8 Datenbanken sollte ein spezifischer SQL-Benutzer verwendet werden. Der Server Admin (SA) kann zwar verwendet werden, ist aber nicht zwingend nötig. Der User benötigt demnach folgende Rechte:

- **dbCreator**: Sollen die Datenbanken über den AdminClient angelegt werden, muss der Benutzer das Recht **dbCreator** besitzen
- **dbOwner**: Werden die Datenbanken manuell am MSSQL Server erstellt und durch den AdminClient lediglich verwaltet, sind **dbOwner** Rechte ausreichend
- Es müssen auf jeden Fall **Leserechte auf die Masterdatenbank** bestehen

### Datenbanken

Je Password Safe Datenbank wird eine MSSQL-Datenbank benötigt. Es können mehrere Datenbanken auf einer SQL-Instanz betrieben werden. Da Password Safe V8 über das Berechtigungskonzept eine saubere Trennung aller Daten ermöglicht, ist in den meisten Anwendungsfällen eine einzige MSSQL-Datenbank ausreichend.

> **!** Die Datenbanken müssen zwingend die Collation **Latin1_General_CI_AS** haben. Sollte der SQL-Server eine andere Collation verwenden, kann Password Safe die Datenbank nicht korrekt erstellen. In diesem Fall muss die Datenbank serverseitig manuell mit der korrekten Collation erstellt und diese dann am Admin Client eingebunden werden.

Hier geht´s zurück zum Kapitel Erste Schritte

# Systemanforderungen Server

## Benötigte Hard- und Software

Die Business Logik wird durch den Applikationsserver verwaltet. Die Auslastung wird sowohl durch die Anzahl der Benutzer als auch durch die Menge an Server-Anfragen bestimmt. Um den optimalen Betrieb gewährleisten zu können, empfehlen wir die Bereitstellung der nachfolgenden Hardware-Ressourcen:

- Min. Windows Server 2012 R2 (aktueller Patchlevel-Stand ist zwingend notwendig!)
- Empfohlen Windows Server 2016
- Min. 4 x CPU's
- Min. 8 GB RAM
- Min. 40 GB Festplattenspeicherplatz
- Aktuelle .net Bibliothek (4.6.2 ist momentan die Mindestvoraussetzung)
- Firewall Freigabe
- Windows Management Framework 4.0 muss installiert sein! (Windows-Update KB2819745)

Der Applikationsserver benötigt die folgenden Port Freigaben:

- Port 443 HTTPS zur Verbindung zum MATESO Lizenzserver
- Port 11011 TCP zur Kommunikation mit den Clients oder dem Webserver IIS
- Port 11014 TCP für den Backupdienst
- Port 1433 TCP für die Kommunikation mit dem SQL Server

Der Windows Server 2012 R2 benötigt das aktuellste Patchlevel (SSL3, TLS)

Bei einer Anbindung außerhalb eines lokalen Netzwerkes (Beispielsweise über VPN) sollte darauf geachtet werden, dass die MTU auf 1500 Bytes (1472 Bytes + 28 Bytes für den Header) konfiguriert ist. Ansonsten werden die zu übertragenden Pakete fragmentiert, was zu einem deutlichen Performanceverlust führen kann.

## Webserver (IIS)

Es können mehrere Webserver für den Web-Zugriff konfiguriert werden, für die Nutzung des Web Access ist jedoch mindestens einer nötig. In der ersten Iteration von Version 8 ist der Zugriff via Webclient noch nicht mit allen Funktionen ausgestattet. Es folgen unsere Empfehlungen für optimalen Betrieb:

- Min. Windows Server 2012 R2 (aktueller Patchlevel-Stand ist zwingend notwendig!)
- Empfohlen Windows Server 2016
- Min. 4 x CPU's
- Min. 8 GB RAM
- Min. 40 GB Festplattenspeicherplatz
- Aktuelle .Net Bibliothek (4.6.1 ist momentan die Mindestvoraussetzung)
- SSL Zertifikat
- Firewall Freigabe falls nötig nach Zugriff konfigurieren (http, oder https)

# Benötigte Benutzer

Zur Konfiguration ist ein Benutzer nötig, über welchen sich der Password Safe Server am SQL-Server anmelden kann. Ebenso ist ein Benutzer nötig, welcher die Password Safe Dienste ausführt. Die verschiedenen Konstellationen sollen hier kurz erläutert werden.

### Dienstbenutzer

Der Dienstbenutzer führt den Password Safe Server-Dienst aus. Es kann hier folgendes konfiguriert werden:

- **AD Benutzer:** Wird im Format **Domain\Benutzername** und dem zugehörigen Passwort angegeben
- **Lokaler Benutzer:** Wird im Format **.\Benutzername** und dem zugehörigen Passwort angegeben
- **Lokales Systemkonto:** Kann über eine Checkbox aktiviert werden

> **!** Über den Dienstbenutzer werden die Datenbanken erstellt. Währenddessen werden Zertifikate erzeugt. Daher muss der **Dienstbenutzer lokaler Administrator** oder **Domänenadministrator** sein, da er sonst keine Rechte hat um in den Zertifikatsstore zu speichern.

### Backupdienstbenutzer

Prinzipiell wird der Backupdienst durch den Dienstbenutzer ausgeführt, im Expertenmodus kann jedoch auch ein anderer Benutzer verwendet werden. Für den Backupdienst-Benutzer gilt das gleiche, wie für den Dienstbenutzer.

### Benutzer für die SQL-Konfigurationsinstanz

Der Benutzer für die SQL-Konfigurationsinstanz meldet sich am SQL-Server an, um die Password Safe Datenbanken zu erstellen bzw. zu erzeugen. Hierfür kann sowohl ein AD-User als auch ein lokaler SQL-Benutzer verwendet werden. Es gibt folgende Möglichkeiten:

- **Dienstbenutzer:** Wird die Checkbox aktiviert, wird der hinterlegte Dienstbenutzer verwendet. Es gilt hier zu beachten, dass die Konfiguration nur über die Checkbox möglich ist. Der Dienstbenutzer darf hier nicht nochmals manuell eingerichtet werden.
- **SQL Benutzer:** Es kann auch ein SQL-Benutzer verwendet werden. Dieser wird entsprechend der Konfiguration am SQL-Server hinterlegt.

Sollen die Datenbanken vom Password Safe Server erstellt werden, benötigt der Benutzer dbCreator-Rechte. Alternativ dazu können die Datenbanken direkt durch den SQL-Server erstellt und vom Password Safe Server verwaltet werden. In diesem Fall genügen dbOwner Rechte.

### Konfigurationsbeispiele

**Variante 1:**
Es wird ein Service Benutzer im AD angelegt. Dieser wird als Dienstbenutzer angelegt, um sowohl den Password Safe Server Dienst als auch den Backup Dienst zu starten. Hierfür benötigt der Benutzer Rechte, um Dienste zu starten. Dieser Benutzer wird dann (durch aktivieren der Checkbox) für die SQL Konfigurationsinstanz verwendet.

**Variante 2:**
Als Dienstbenutzer wird ein lokaler User verwendet. Als Benutzer für die SQL-Konfigurationsinstanz wird ein lokaler SQL Benutzer inklusive Passwort angegeben. Dies könnte beispielsweise der standardmäßige sa-Benutzer sein.

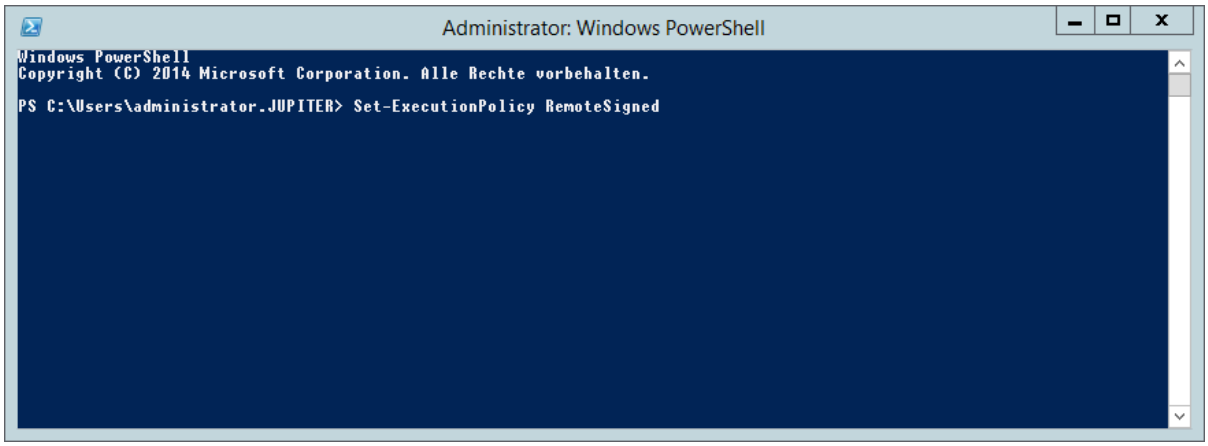
Die Kombination von lokalem System und Dienstbenutzer für die SQL Konfigurationsinstanz ist nicht möglich!

## Rechte auf Windows PowerShell

In Password Safe V8 wird an mehreren Stellen auf Windows PowerShell-Skripte zurückgegriffen. Diese sind beispielsweise nötig, um den zertifkatsgeschützten Serverschlüssel zu verwenden oder um das Server-Zertifikat anzulegen. Ebenso nutzt Password Reset diese Funktionalität. Es ist also zwingend nötig, dass die Windows Sicherheitsrichtlinie die Ausführung von PowerShell Skripten zulässt. Manuell kann dies wie folgt eingerichtet und geprüft werden:

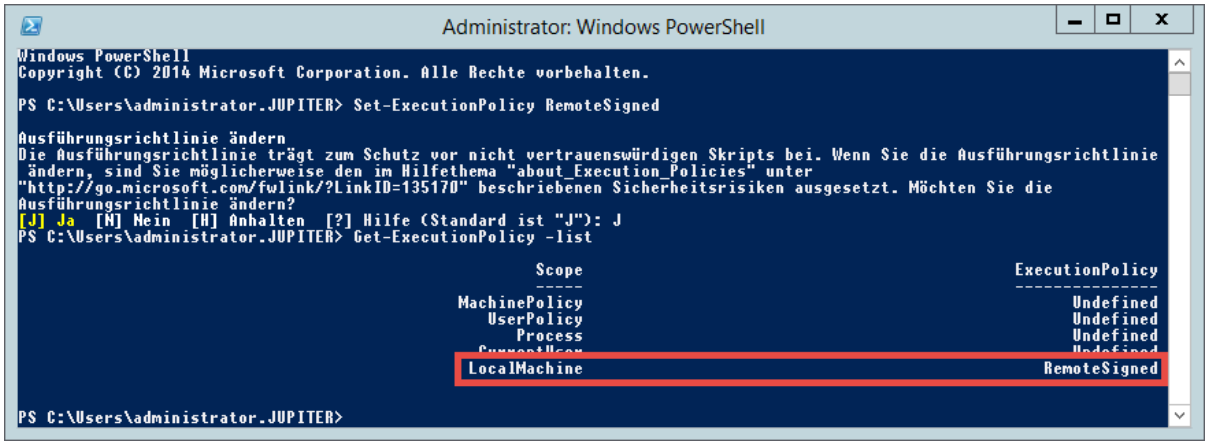
Windows Management Framework 4.0 muss installiert sein! (Windows-Update KB2819745)

Zunächst wird die PowerShell Konsole geöffnet und **Set-ExecutionPolicy RemoteSigned** eingegeben und bestätigt.




Im nächsten Schritt wird die Änderung der Richtlinie bestätigt.


Abschließend kann über **Get-ExecutionPolicy -list** die geänderte Richtlinie abgefragt werden.




Hier geht´s zurück zum Kapitel Erste Schritte

# Systemanforderungen Client

## Benötigte Hardware

Die Performanz ist minimal abhängig vom Client. Die Einstellungen des Benutzers werden direkt aus der MSSQL-Datenbank geladen. Folgend unsere Empfehlung für den optimalen Betrieb:

- Microsoft Windows ab Version 7 (aktuellster Patchlevel)
- Min. 2 x CPU's
- Min. 2 GB RAM
- Min. 40 GB Festplattenspeicherplatz
- Aktuelles .net Framework (4.6.2 ist momentan die Mindestvoraussetzung)
- Sollen RDP Verbindungen aufgebaut werden können, muss mindestens RDP 8.1 installiert sein

Die Clients benötigen folgende Port Freigaben:

- Port 11011 TCP zur Kommunikation mit dem Anwendungsserver
- Port 52120 TCP mit dem Addon

> Wir empfehlen den Client zu paketieren und auf den entsprechenden Maschinen zu installieren. Für die Paketierung stellen wir zudem ein MSI Paket zur Verfügung.

> Die Clients sind auf allen aktuellen Windows Versionen von Windows 7 bis Windows 10 lauffähig

### Einsatz im Terminalserverbetrieb

Der Client lässt sich auch auf einem Windows Terminalserver betreiben. Für die automatische Eintragung muss auf dem Terminalserver der SSO Agent als Dienst installiert werden.

Hier geht´s zurück zum Kapitel Erste Schritte

# Systemanforderungen WebClient

Der Password Safe WebClient kann prinzipiell auf allen aktuellen Webservern aufgesetzt werden. Hierfür wird ein entsprechendes SSL-Zertifikat für die https Anbindung benötigt. Der WebClient sollte im Idealfall immer die gleiche Version wie der Password Safe Server haben.

> Da jeder Webserver individuell installiert und konfiguriert ist, müssen detaillierte Kenntnisse des verwendeten Systems vorausgesetzt werden. Über unsere Partner kann die Installation gerne per Consulting übernommen werden.

## Unterstützte Webserver

Auf folgenden Systemen konnte der Password Safe WebClient erfolgreich getestet werden:

### IIS

- ab **Version 7**
- Modul **URL Rewrite**
- Modul **Application Request Routing**

### Apache

- ab **Version 2.4**
- Modul **mod_rewrite**
- Modul **mod_proxy**
- Modul **mod_ssl**
- Modul **mod_proxy_http**

### nginx

- ab **Version 1.13**

> Wie schon erwähnt, kann der Password Safe WebClient auf allen herkömmlichen Webservern betrieben werden. Aufgrund möglicher Seiteneffekte kann die reibungslose Funktion allerdings nicht auf allen verfügbaren Webservern garantiert werden. Im Zweifelsfall sollte die Funktion daher vorab getestet werden.

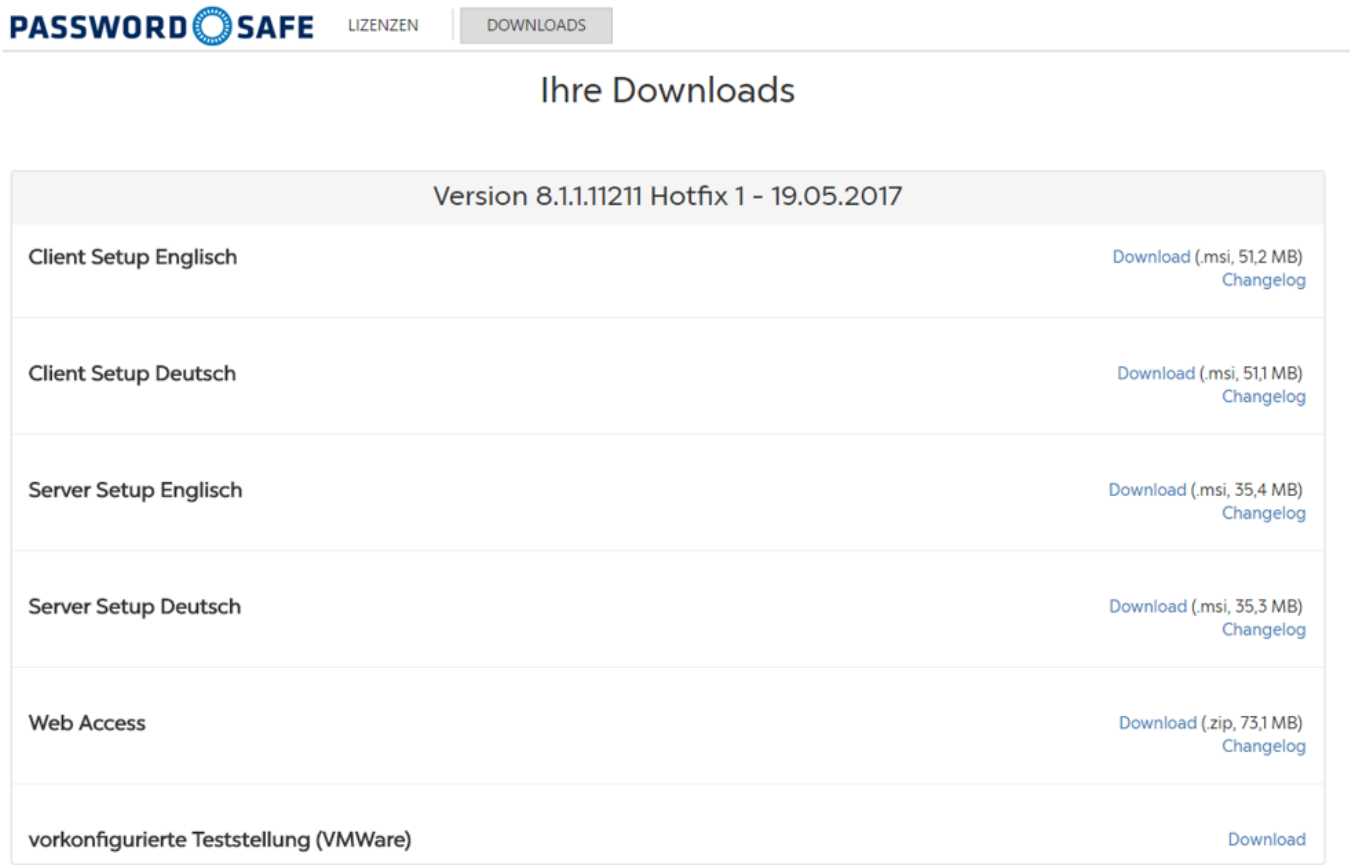
> Die Verbindung vom Browser zum Webserver muss über ein SSL-Zertifikat geschützt werden. Es wird ausdrücklich empfohlen hierfür ein Zertifikat eines Dienstleisters, wie z.B.: Thawte, zu erwerben. Wenn Sie kein offizielles Zertifikat erworben haben, so

stellen Sie bitte unbedingt sicher, dass dem Zertifikat entsprechend getraut wird. Anderenfalls wird das Zertifikat rot und somit unsicher im Browser angezeigt.

# Installation

## Installationsdateien

Die Installationsdateien sind direkt in unserem hierfür vorgesehenen Portal verfügbar




Die Zugangsdaten erhalten Sie bei Lizenzauslieferung. Bei Interesse an einer Testlizenz nutzen Sie bitte das hierfür vorgesehene Formular.

> Im Gegensatz zur Version 7 existiert keine Auslieferung von Zertifikaten. Ihr Zertifikat ist auf unserem Lizenzserver hinterlegt und kann mit den übermittelten Zugangsdaten abgerufen werden.

## Konzeptionierung vor der Installation

Password Safe soll die in einem Unternehmen existierenden Hierarchien in Form von differenzierbaren und präzise definierbaren Rechtestrukturen abbilden. Je genauer man diese hierarchischen Ordnungen

kennt, desto einfacher gestaltet sich die Umsetzung. Fehler in der Analysephase führen somit häufig zu Folgefehlern, welche nur mit großem Zeitaufwand korrigiert werden können. Es ist demnach unabdingbar der Konzeptionierung die nötige Aufmerksamkeit zu widmen. Wohl durchdachte und strikt geplante Projekte profitieren sowohl bei der Umsetzung, wie auch im laufenden Betrieb, stark von einem gründlich erfassten Projektplan.

## Dokumentation parallel zur Installation

> **!** Dokumentation ist ein wichtiger Bestandteil der Installation. Es ist dafür Sorge zu tragen, dass die genutzten Systeme und Zugänge lückenlos erfasst werden. Sowohl bei Veränderungen in der Zuständigkeit, als auch bei Anpassungen der Architektur, profitiert man signifikant von einem Nachschlagewerk in Form einer vollständig vorhandenen Password Safe Dokumentation.

## Definition von Verantwortlichkeiten

Wir empfehlen, für Password Safe einen festen Verantwortlichen inkl. Stellvertretung zu benennen – und diese Ansprechpartner adäquat zu schulen. In größeren Installationen ist es wahrscheinlich, dass die Verantwortlichkeit dementsprechend von mehreren Personen getragen werden muss. Es ist zwingend festzulegen, welche Personen(gruppen) Zugang zu den diversen Funktionalitäten innerhalb des Password Safe erhalten:

- Verwaltung der Organisationsstrukturen und Rollenmitgliedschaften
- Erstellung und Pflege von Formularen und Anwendungen
- Konfiguration der Einstellungen und Rechte sowie Sichtbarkeiten von Modulen
- Abgrenzung der Berechtigungen und Definition von Rechtevorlagen
- Ausarbeitung eines Zugriffskonzeptes:
    - In welchem Umfang und von wem werden die Datenbanken betreut?
    - Ist eine Trennung der administrativen Tätigkeiten notwendig?

Bei Bedarf leistet Ihnen unser erfahrenes Support-Team hierbei gerne Unterstützung.

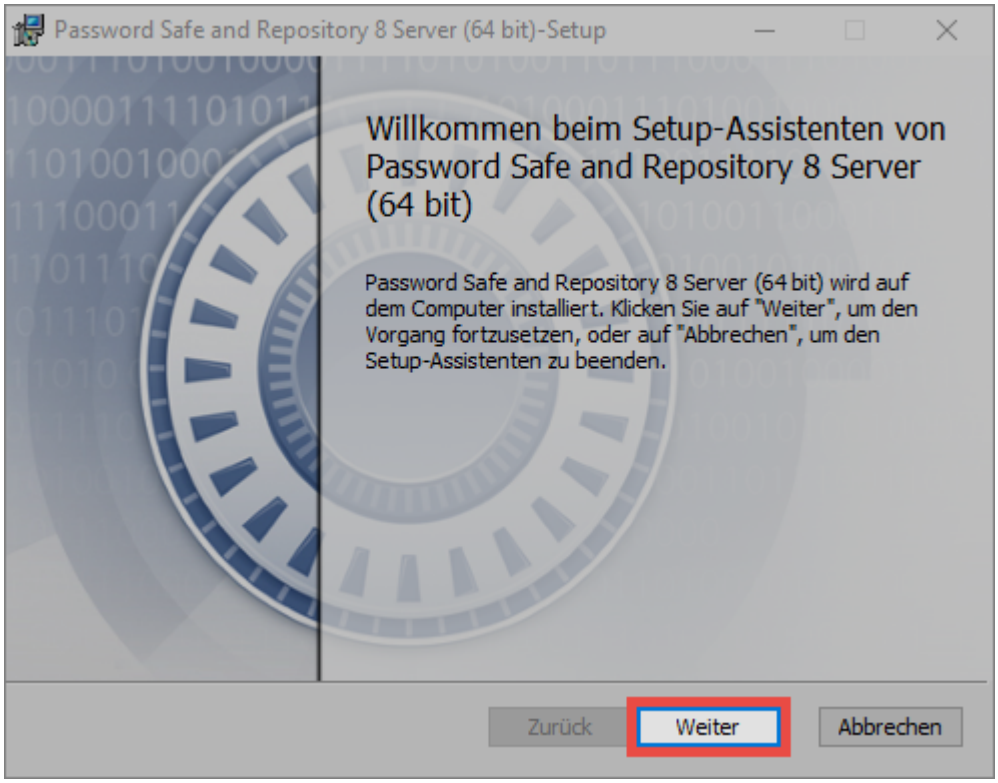
- Installation AdminClient
- Installation Client
- Installation WebAccess

# Installation AdminClient

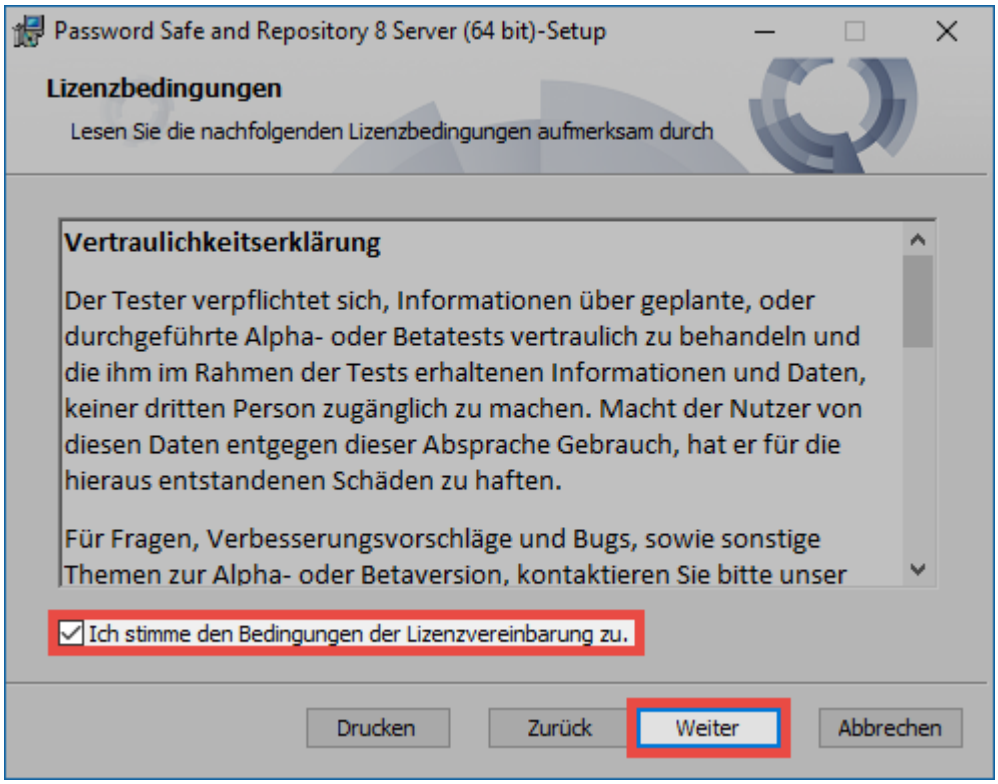
## Video Guide


## Anleitung

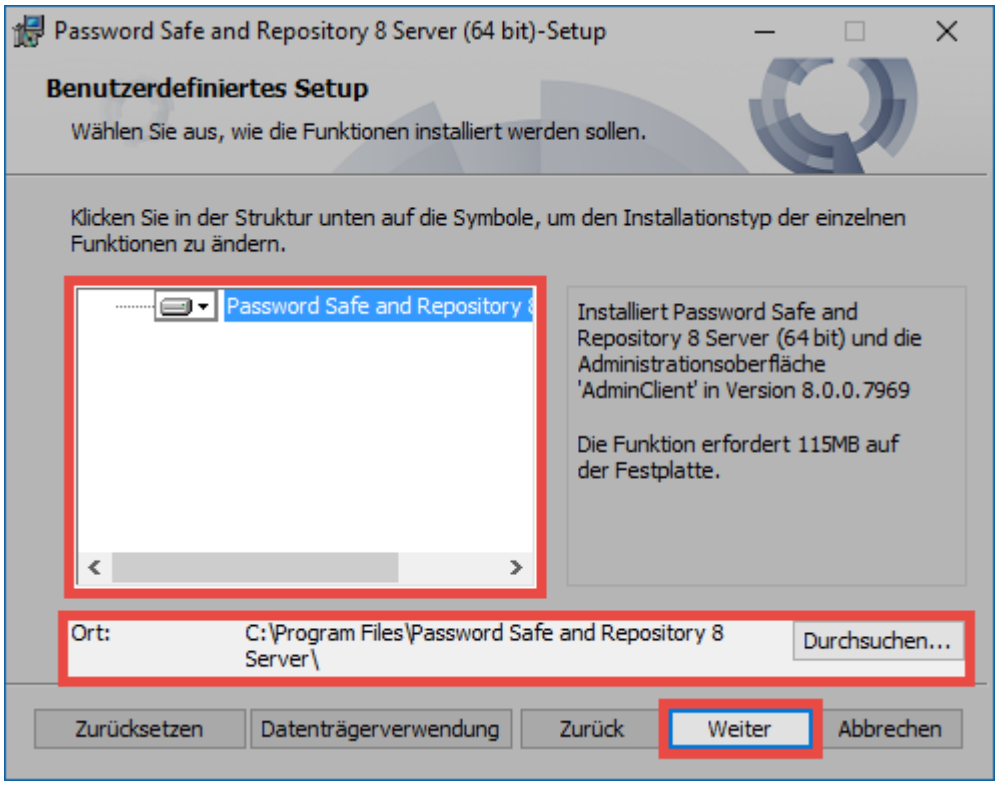
Die MSI-Installationsdateien sowie die zugehörigen Systemanforderungen Server. können direkt dem dementsprechenden Kapiteln entnommen werden. Die nachfolgende Schritt-für-Schritt Anleitung geleitet durch den Assistenten.



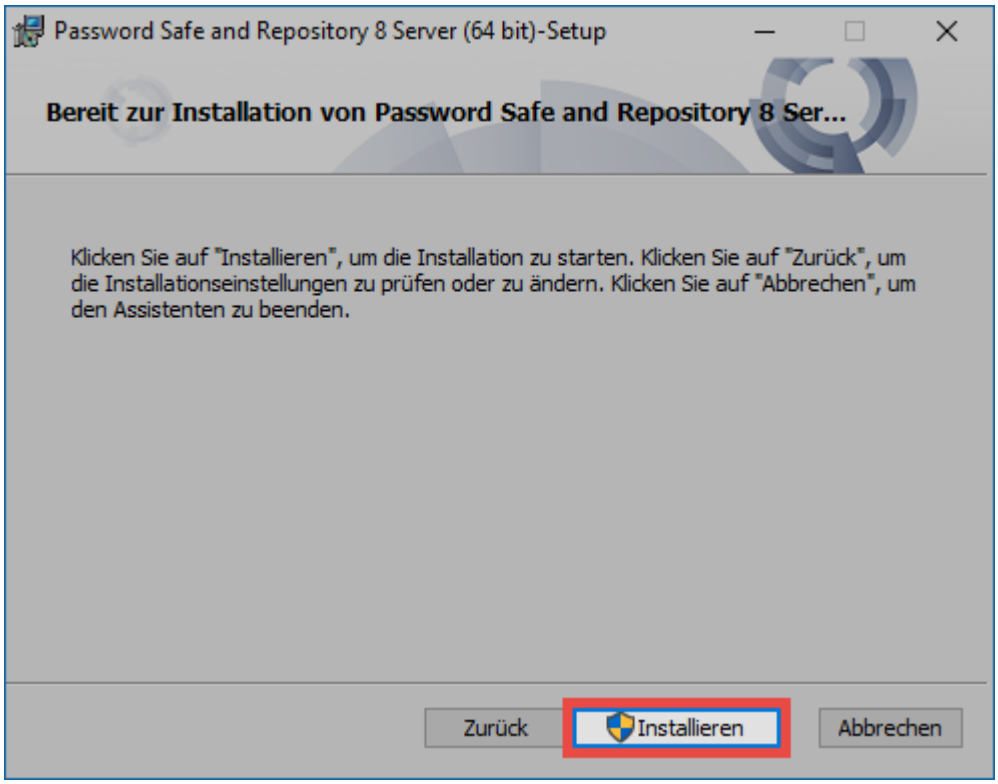

Zunächst müssen die Lizenzbedingungen gelesen und akzeptiert werden. Diese können auch gedruckt werden.



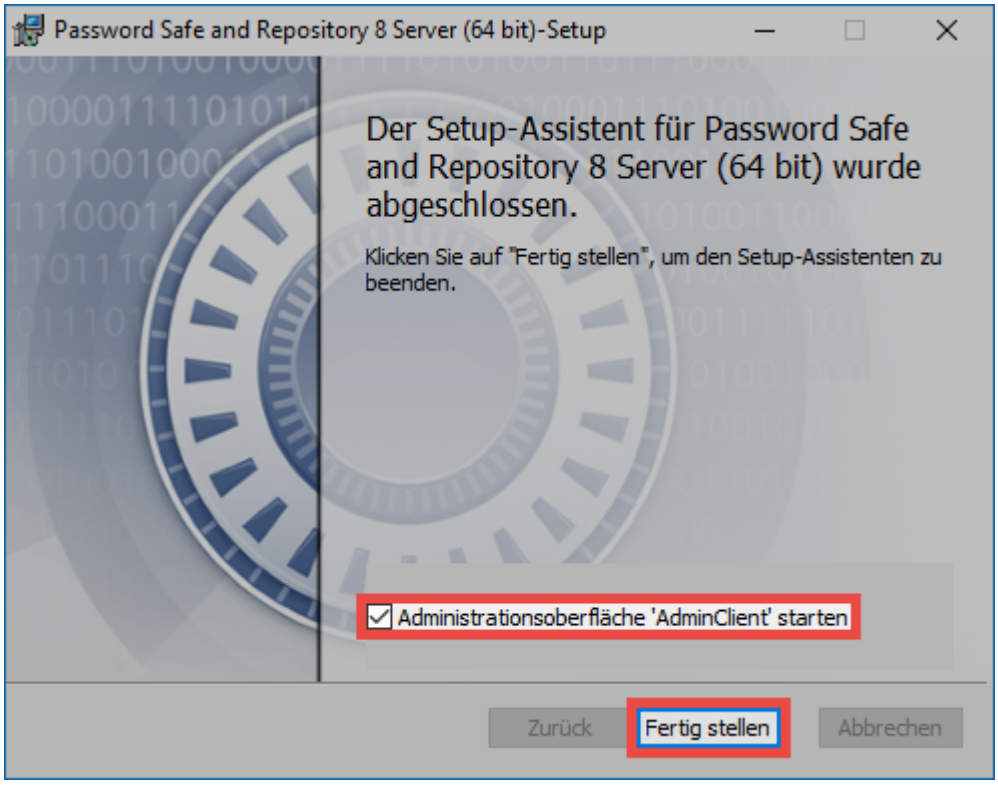

Im nächsten Schritt wird der Speicherort festgelegt. In der Regel kann der vorgeschlagene Speicherort beibehalten werden.




Im nächsten Schritt wird die Installation gestartet.

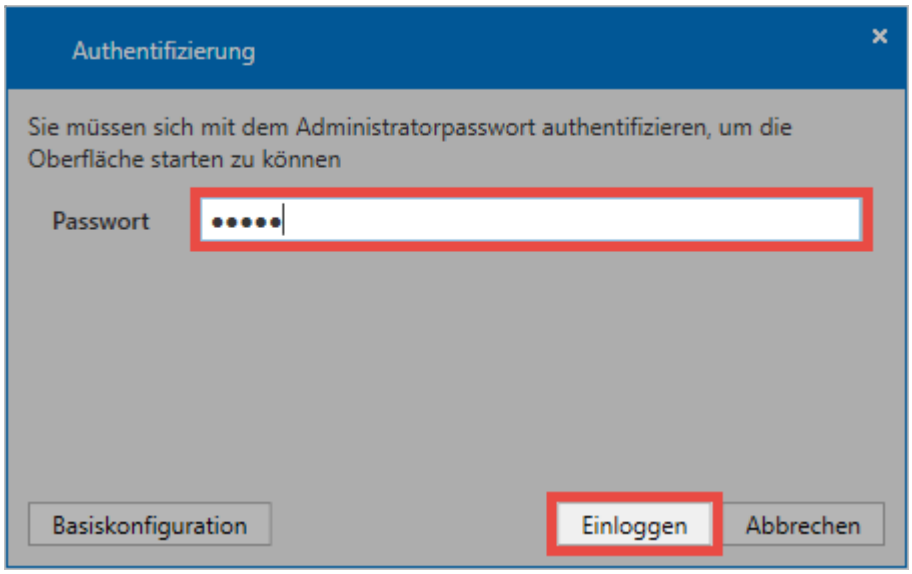



Der letzte Schritt schließt das Setup und öffnet (falls gewünscht) direkt den AdminClient.




## Authentifizierung

Nach der Installation kann man sich direkt am AdminClient anmelden.




Das Initialpasswort zur ersten Anmeldung lautet “admin”. Es sollte direkt nach der Anmeldung geändert werden.

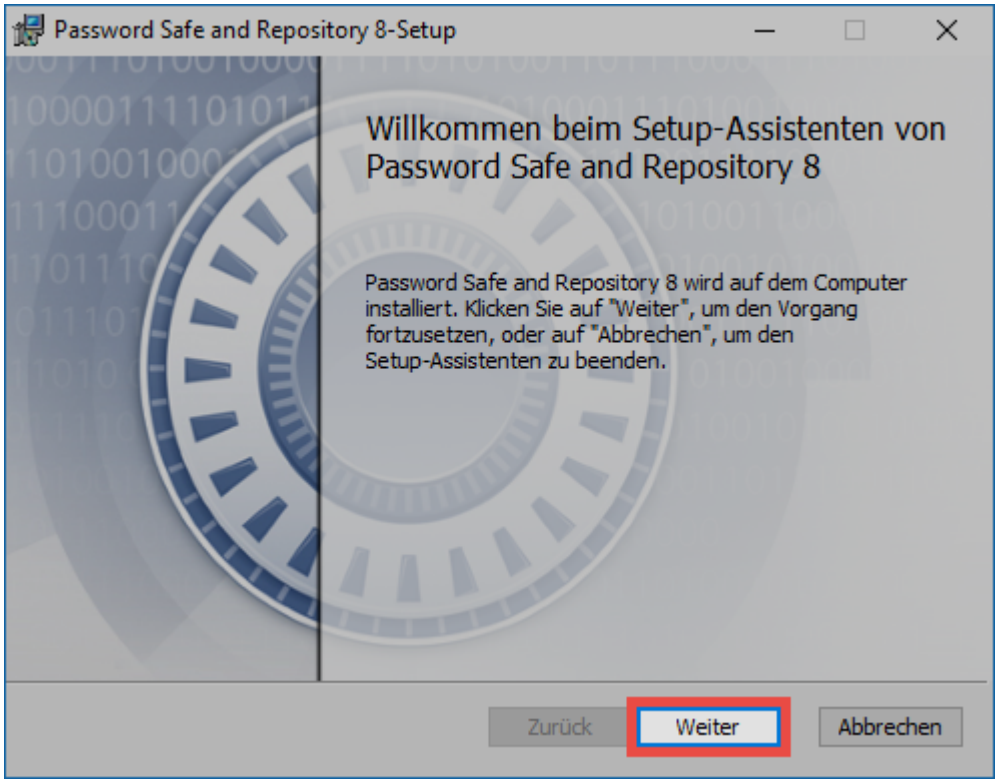
Hier geht´s zurück zum Kapitel Erste Schritte

# Installation Client

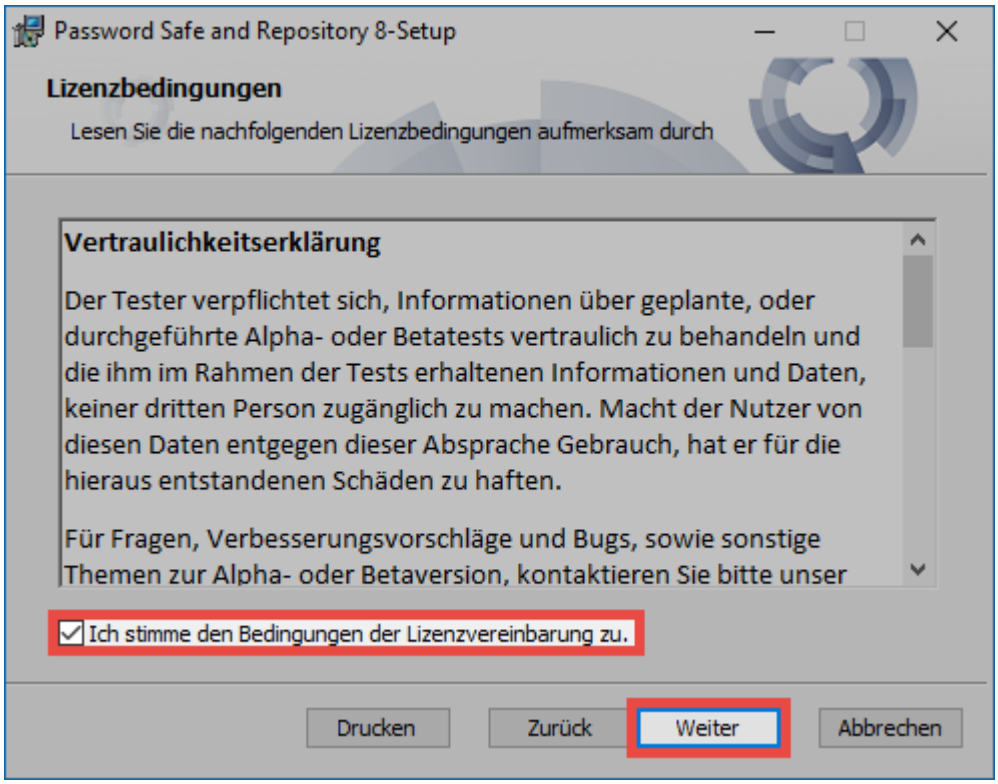
## Video Guide


## Anleitung

Die MSI-Installationsdateien sowie die zugehörigen Systemanforderungen Client können direkt dem dementsprechenden Kapiteln entnommen werden. Die nachfolgende Schritt-für-Schritt Anleitung geleitet durch den Assistenten.

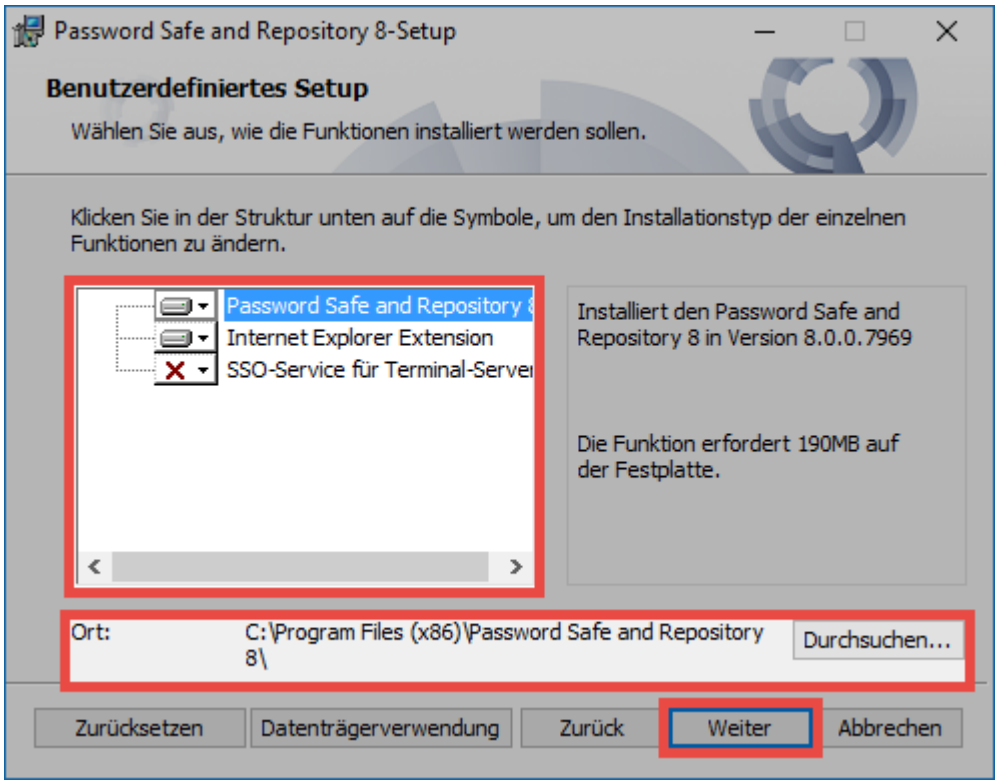



Zunächst müssen die Lizenzbedingungen gelesen und akzeptiert werden. Diese können auch gedruckt werden.



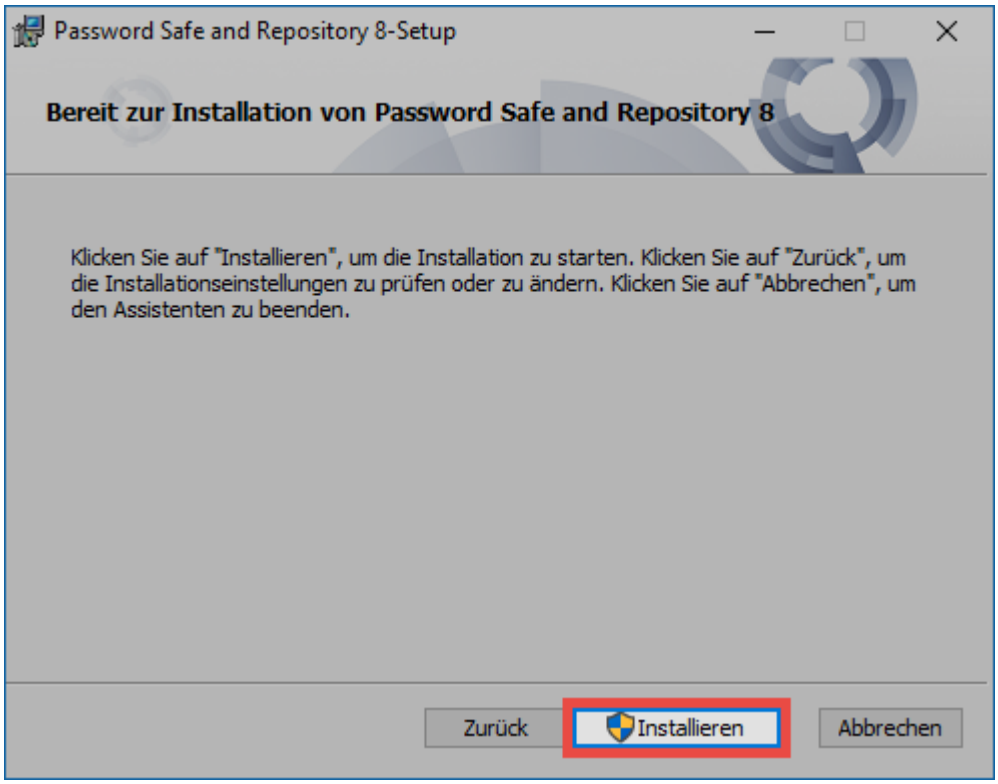

Im nächsten Schritt wird der Speicherort des Clients festgelegt. Ebenso wird hier definiert, ob weitere Komponenten installiert werden sollen.

- **Password Safe and Repository 8** installiert den Client
- **Internet Explorer Extension** wird benötigt, um Zugangsdaten automatisch an den Internet Explorer zu übergeben
- **SSO-Service für Terminal-Server** ermöglicht die automatische Eintragung im Terminalserver-Betrieb

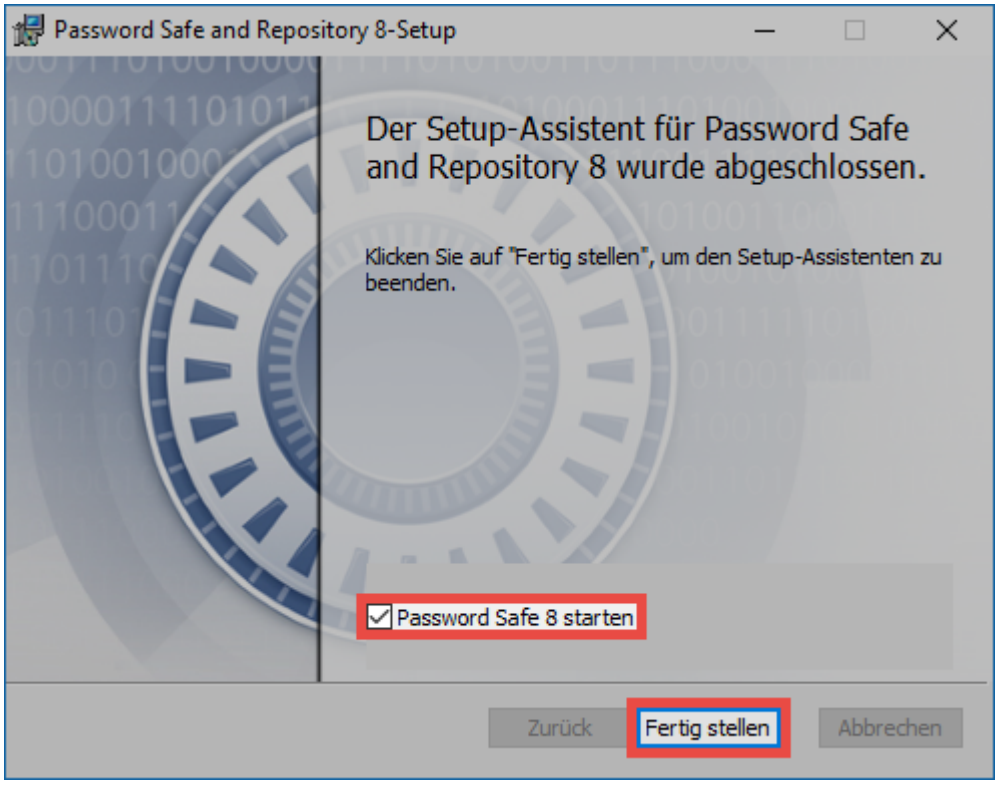



> **!** Bitte installieren Sie den SSO Service ausschließlich dann, wenn der Terminalserver Betrieb angedacht ist!

Der nächste Schritt startet die eigentliche Installation.

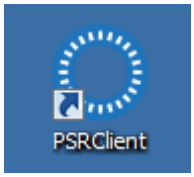



Der letzte Schritt schließt das Setup und öffnet den Client.

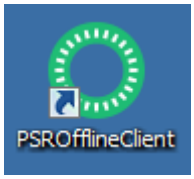


# Installierte Anwendungen

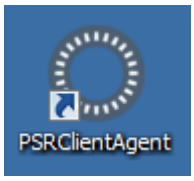
Es werden immer mehrere Anwendungen installiert.




Hierbei handelt es sich um den regulären Client.




Der Offline Client ermöglicht den Zugriff auf die Daten ohne Verbindung zum AdminClient.




Der SSO Agent stellt die Verbindung zwischen den Browser Addons und der Datenbank dar. Er ermöglicht die automatische Anmeldung ohne den Client geöffnet zu haben und läuft im Hintergrund.

# Einbinden einer Datenbank

Für die Verbindung zur Datenbank ist das Anlegen eines Datenbankprofils obligatorisch. Nachfolgende Informationen werden hierfür benötigt:

- **Profilname:** Name des Profils. Dieses wird zukünftig am Client angezeigt
- **IP Adresse:** Hier wird die IP-Adresse des Password Safe V8 Servers hinterlegt
- **Datenbankname:** Hier wird der Name der Datenbank angegeben

# Verteilen von Datenbankprofilen über die Registry

Selbstverständlich gibt es auch die Möglichkeit, Datenbankprofile zu verteilen. Über einen entsprechenden Registry Eintrag werden die Profile vorgegeben. Beim nächsten Programmstart werden diese dann in den Password Safe übernommen und innerhalb der Konfigurationsdatei gespeichert. Der Registry Eintrag wird unter **HKEY_CURRENT_USER\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles** erstellt. Hier wird dann ein neuer Schlüssel mit dem Namen der Datenbank angelegt. Der Schlüssel muss dann folgende Einträge bekommen:

**HostIP:** IP Adresse des Servers
**DatabaseName:** Name der Datenbank
**LastUserName:** Hier kann optional das Feld für den Benutzernamen vordefiniert werden


Wenn der entsprechende Registry Eintrag gesetzt ist und kein Datenbank Profil dazu existiert, wird das Profil beim nächsten Start angelegt. Profile, welche über diesen Weg erstellt werden, lassen sich am Client weder bearbeiten noch löschen.

Hier geht´s zurück zum Kapitel Erste Schritte

# Installation mit Parametern

## Worum geht es bei der Installation mit Parametern?

Die Installation des Password Safe Clients kann optional auch über die Kommandozeile aufgerufen werden. Bei dieser Methode ist ebenso die Übergabe von Parametern vorgesehen. Diese sind miteinander kombinierbar. In diesem Fall werden die einzelnen Parameter durch ein Leerzeichen voneinander getrennt. Die im Folgekapitel aufgeführten Parameter ermöglichen Anpassungen an der Art der Client-Installation.

## Aufruf über die Kommandozeile mit Parametern

Der Aufruf wird über die Kommandozeile gestartet: **MSI-FILE.msi [PARAMETER]**

### Parameter

- **INSTALL_IE_EXTENSION="0"**: Die Extension für den Internet Explorer wird nicht installiert. In der Liste der zu installierenden Komponenten im Setup ist demnach der Haken nicht gesetzt, kann jedoch vom Benutzer wieder gesetzt werden
- **SSO_START_VIA_REGISTRY="0"**: Deaktiviert das Aufführen des SSO Agents in den Windows Autostart
- **INSTALL_SSO_AGENT="0"**: Deaktiviert die Installation des SSO Agents. In der Liste der zu installierenden Komponenten im Setup ist demnach der Haken nicht gesetzt, kann jedoch vom Benutzer wieder gesetzt werden
- **INSTALL_OFFLINE_CLIENT="0"**: Deaktiviert die Installation des Offline Clients. In der Liste der zu installierenden Komponenten im Setup ist demnach der Haken nicht gesetzt, kann jedoch vom Benutzer wieder gesetzt werden

# Installation WebClient

> ! Dieses Kapitel behandelt ausschließlich die Erstinstallation. Die hier geschilderten Schritte dürfen bei einem Update **nicht** ausgeführt werden.

Zur Installation des WebClients wird im AdminClient das Modul WebClient bereitgestellt.

## Vorbereitungen zur Installation

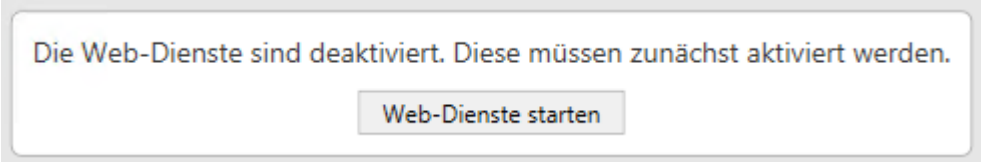
Um die Installation des WebClients ohne weitere Komplikationen durchführen zu können, sollten folgende Vorbereitungen getroffen werden:

### Systemanforderungen

Zunächst sollte sichergestellt sein, dass alle **Systemanforderungen** erfüllt sind.

### Webdienst

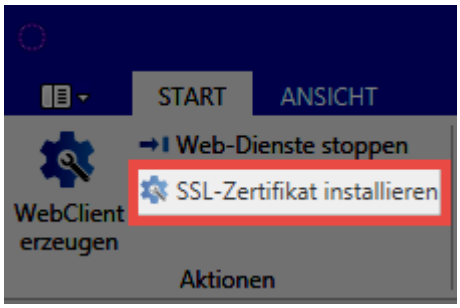
Beim ersten Aufruf des Moduls **WebClient** im **AdminClient** muss zunächst der Web Dienst gestartet werden.




Hierdurch wird der Password Safe Server neu gestartet. Abschließend wird im Modul **WebClient** die Konfigurationsoberfläche dargestellt.

### SSL Zertifikat

Weiterhin muss das **SSL Zertifikat** installiert werden.



Hierdurch wird das Zertifikat welches in der Grundkonfiguration selektiert wurde für die Verwendung mit dem WebClient konfiguriert. Es handelt sich hierbei um das **Verbindungszertifikat** zur Kommunikation zwischen Webserver und Password Safe Server.

> Im Hintergrund wird das Zertifikat hierbei über **netsh http add sslcert** passend zum konfigurierten Port (443 TCP) ins Betriebssystem eingebunden. Beim Deinstallieren wird mit **netsh http delete sslcert** gearbeitet

### Firewall

Der Port 443 TCP muss eingehend freigeschalten sein.

### Datenbanken

Alle **Datenbanken** welche im **WebClient** verwendet werden sollen, müssen hierfür freigegeben werden. Es genügt ein Doppelklick auf die entsprechende Datenbank. Nun kann die Option **Zugriff über WebClient aktivieren** ausgewählt werden.

# Installation

Der WebClient wird durch den AdminClient erzeugt und in einem ZIP Archiv bereitgestellt. Je nach verwendetem Webserver, wird das ZIP Archiv entsprechend erstellt. Ebenso unterscheidet sich die Installation. Unabhängig vom verwendeten Webserver müssen zunächst folgende Infos angegeben werden:

**Zieldatei**
Hier wird derjenige Ordner angegeben, in welchem das ZIP Archiv mit dem WebClient abgelegt werden soll.

> Wird auf dem IIS installiert wird im ZIP Archiv eine Datei mit dem Namen config.bat erstellt, welche schlussendlich das Einbinden am Webserver übernimmt.

**Server IP**
Rein informativ wird hier die IP Adresse des Password Safe Servers angezeigt.

> Es sollte geprüft werden ob die IP Adresse korrekt ist, da sonst der WebClient keine Verbindung bekommt. Sollte die IP Adresse nicht passen, muss diese in der Grundkonfiguration des AdminClients geändert werden.

**Webserver-Hostadresse**
Es muss die IP-Adresse bzw. der Hostname des Webservers angegeben werden.

**Port**
Hier wird der Port zum Ansprechen des WebClients hinterlegt.

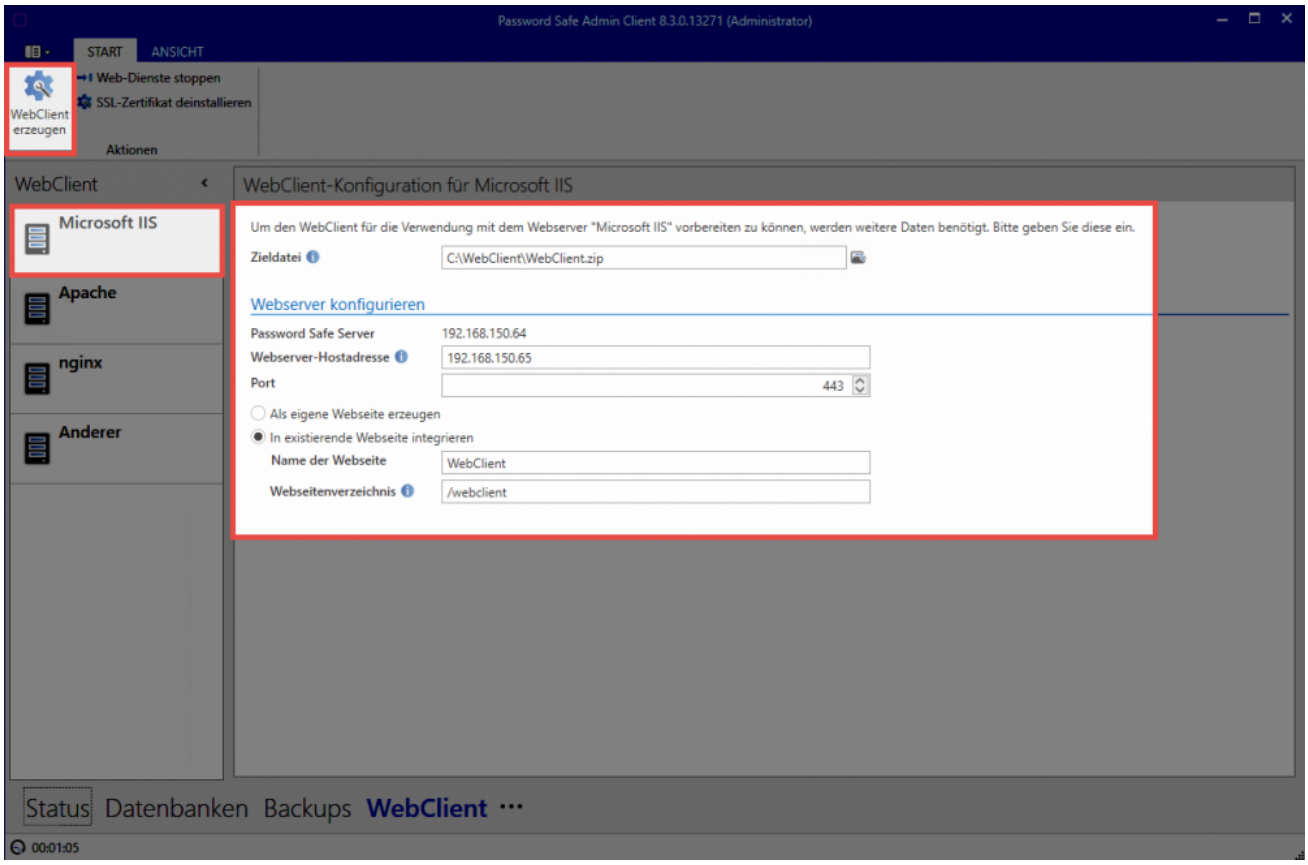
Nachfolgend werden alle weiteren Schritte bzw. die zu machenden Angaben pro Webserver erläutert.

## Microsoft IIS

Soll der **WebClient** auf einem Microsoft IIS betrieben werden, gibt es zwei Methoden zum Einbinden:

**Als eigene Webseite erzeugen**
Durch diese Option wird durch die config.bat am IIS direkt eine Webseite mit dem Namen “WebClient” eingebunden. Der WebClient wird hierbei im Standardverzeichnis C:\inetpub\wwwroot betrieben.

**In existierende Webseite integrieren**
setzt eine bestehende Webseite voraus. Es muss also zunächst auf dem IIS eine Webseite erzeugt werden. Im AdminClient muss dann der **Name der Webseite** angegeben werden. Ebenso muss unter **Webseitenverzeichnis** hinterlegt werden in welchem Ordner der Webclient betrieben werden soll. Das Format hierfür ist “/webclient”



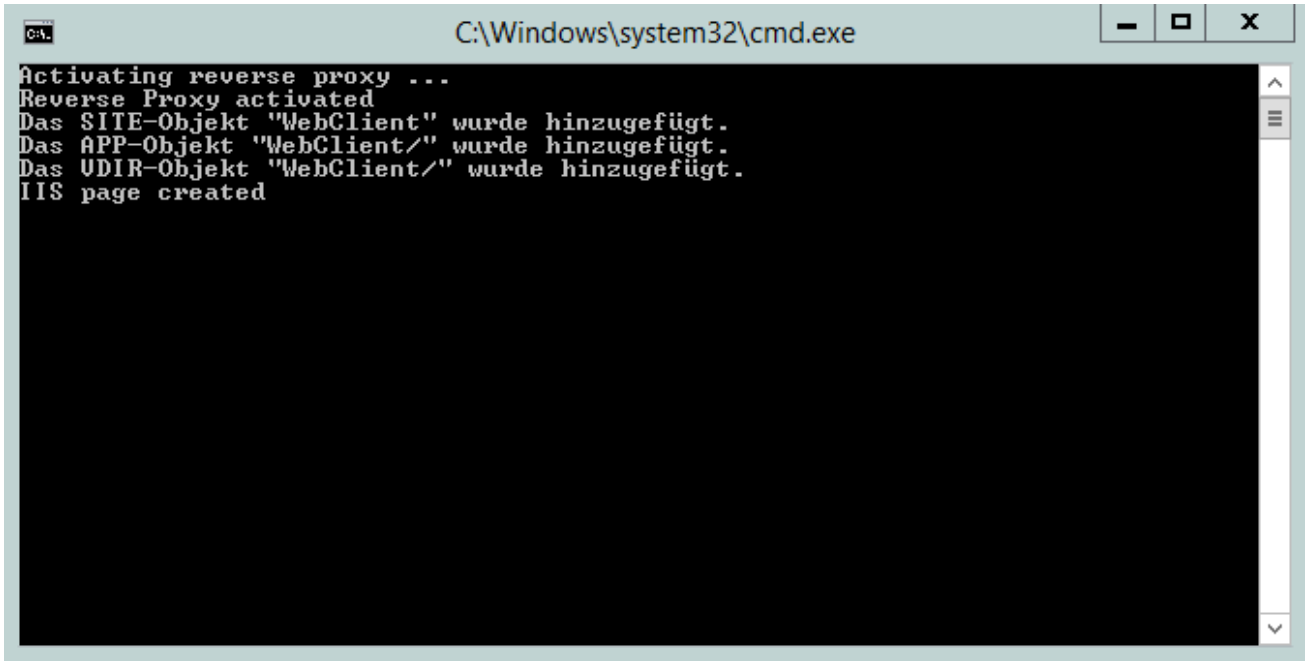
Sobald alle Einstellungen gesetzt sind, kann der WebClient über die entsprechende Schaltfläche in der Ribbon erzeugt werden. Ist das ZIP Archiv mit dem WebClient erzeugt, wird es auf den Webserver in das vorher festgelegte Verzeichnis (standardmäßig C:\inetpub\wwwroot) kopiert und dort in ein neues Verzeichnis entpackt.

### Config.bat

Im neu erstellten Verzeichnis **WebClient** ist die **config.bat** zu finden, welche nun als Administrator ausgeführt werden muss. Hierdurch wird der WebClient im IIS eingebunden.

> Falls die Systemvoraussetzungen nicht erfüllt sind, wird darauf hingewiesen, dass das Modul **URL Rewrite** und/oder **Application Request Routing** nachinstalliert werden müssen. In diesem Fall ist den Assistenten zu folgen welche direkt geöffnet werden. Anschließend muss die **config.bat** erneut ausgeführt werden.

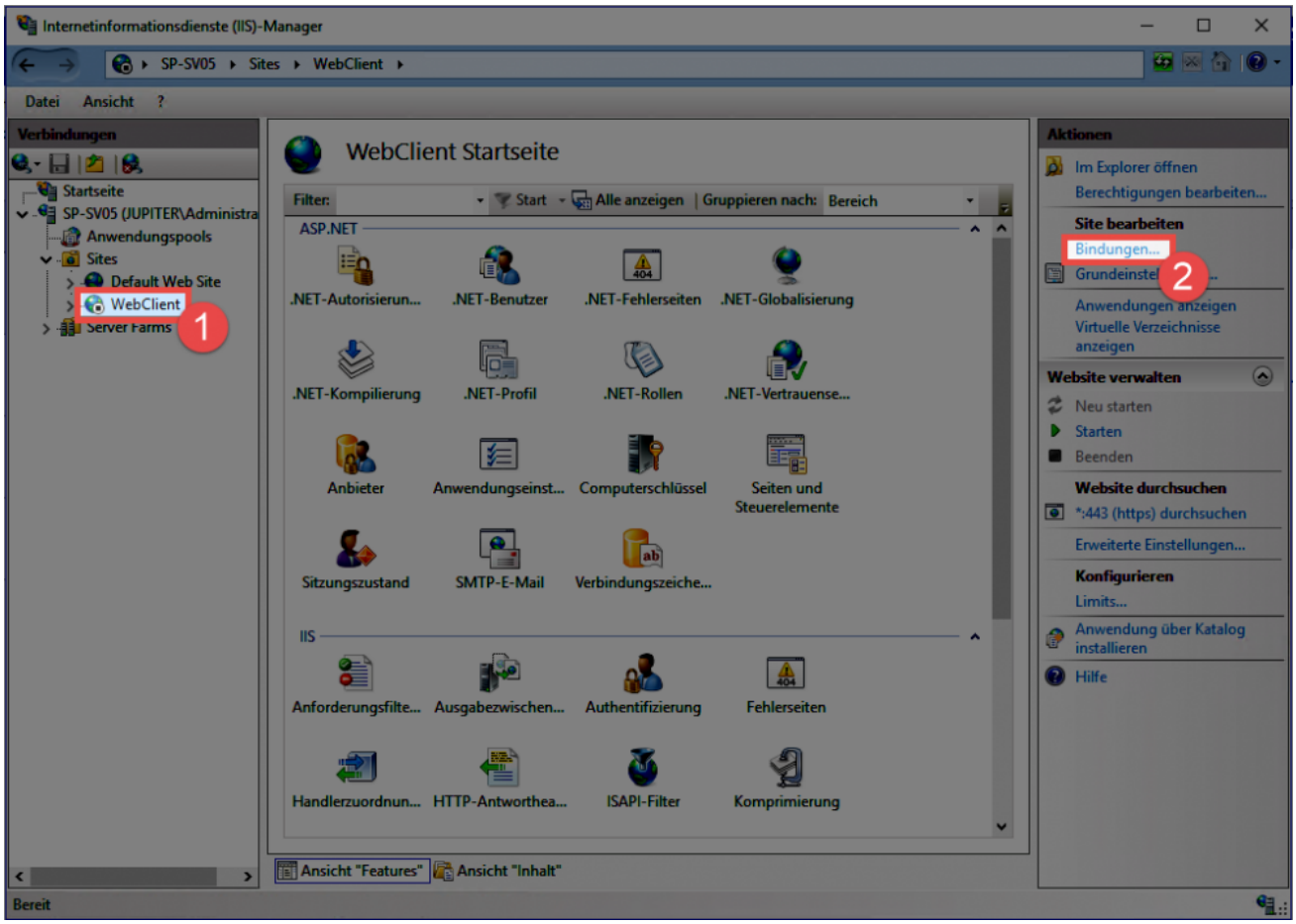
Wurde die Seite korrekt eingebunden, wird dies durch den Hinweis **IIS page created** entsprechend dargestellt.



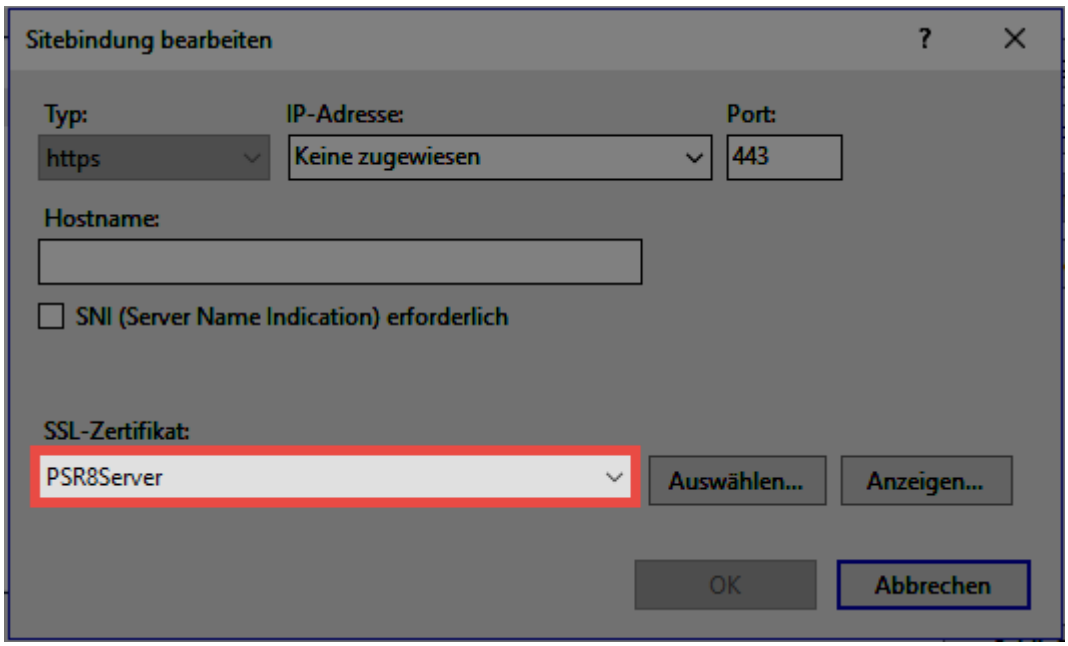

> Nach erfolgter Installation sollte die **config.bat** unbedingt gelöscht werden! Ebenso sollte die **config.bat** nicht für ein Update verwendet werden.

### Zertifikat

Abschließend muss das Zertifikat hinterlegt werden. Hierfür wird am IIS die erstellte Webseite selektiert. Ganz rechts werden nun die Bindungen geöffnet.




Nun wird der Eintrag **https** selektiert und zum Bearbeiten geöffnet. Hier wird dann das **SSL-Zertifikat** ausgewählt.



Der WebClient ist nun betriebsbereit und kann direkt aufgerufen werden. Weitere Infos sind am Ende des Kapitels unter Aufruf des WebClients zu finden.

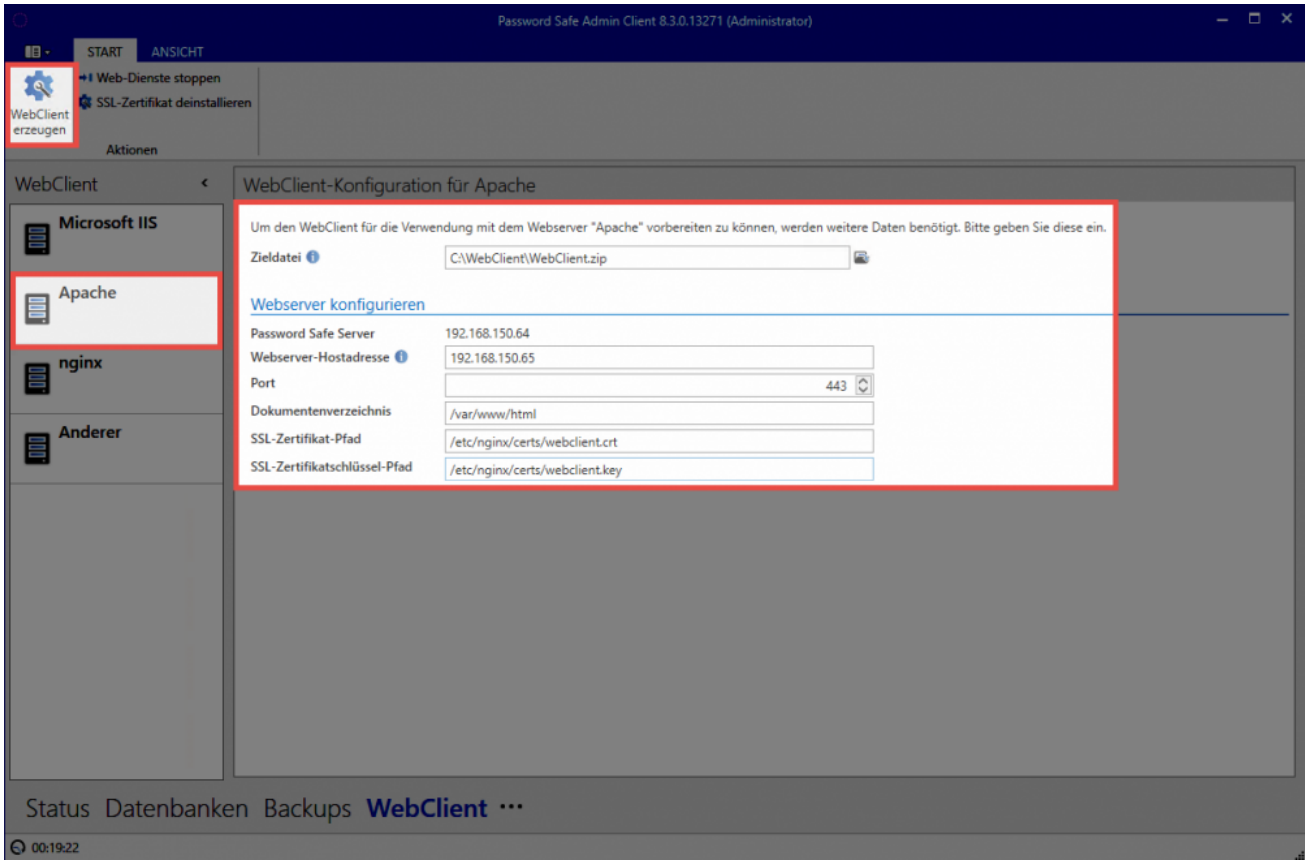
## Apache

Zum Einbinden des WebClients auf einem Apache Server müssen zunächst alle relevanten Einstellungen gesetzt werden:

**Dokumentenverzeichnis**
Hier wird angegeben, in welchem Ordner der WebClient betrieben werden soll.
Standardmäßig ist dies **/var/www/html**

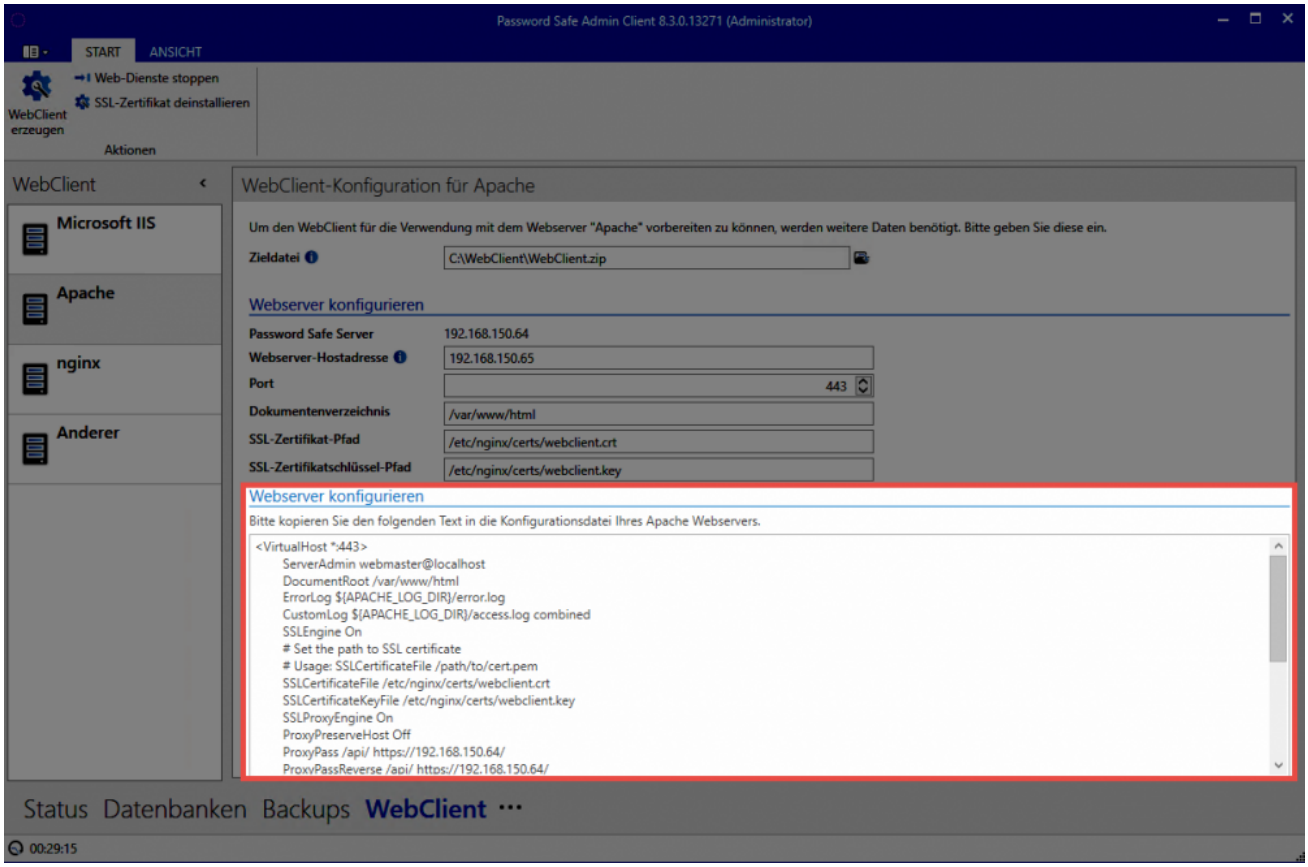
**SSL-Zertifikat-Pfad**
Es muss hier angegeben werden in welchem Verzeichnis das Zertifikat abgelegt wird.
Standardmäßig ist dies **/etc/nginx/certs/webclient.crt**

**SSL-Zertifikatsschlüssel-Pfad**
Schlussendlich muss noch hinterlegt werden, wo der Zertifikatschlüssel liegt.
Standardmäßig ist dies **/etc/nginx/certs/webclient.key**



Nachdem alle Einstellungen gemacht sind, wird der WebClient über den Button in der Ribbon erzeugt. Anschließend wird automatisch der Ordner, in welchem die ZIP Datei liegt geöffnet. Das Archiv wird nun entpackt und der Inhalt auf dem Webserver ins Dokumentenverzeichnis kopiert.

Die Konfiguration für den Apache wurde nun ebenfalls schon erzeugt und kann am AdminClient eingesehen werden.




Die Konfiguration kann hier direkt über STRG+A markiert und kopiert werden. Diese wird dann direkt am Apache eingebunden.

> Die Konfiguration des Apache Servers ist immer individuell. Daher kann hier nur grob das übliche Vorgehen in einer Standard Installation beschrieben werden.

**Standardkonfiguration**

Die Datei **/etc/apache2/sites-available/default-ssl.conf** wird (beispielsweise über “nano”) geöffnet. Nun wird alles zwischen `<IfModule mod_ssl.c>` und `</IfModule mod_ssl.c>` gelöscht und durch die Konfiguration vom Server ersetzt. Abschließend wird der Apache über **systemctl reload apache** neu gestartet.

Der WebClient ist nun betriebsbereit und kann direkt aufgerufen werden. Weitere Infos sind am Ende des Kapitels unter Aufruf des WebClients zu finden.

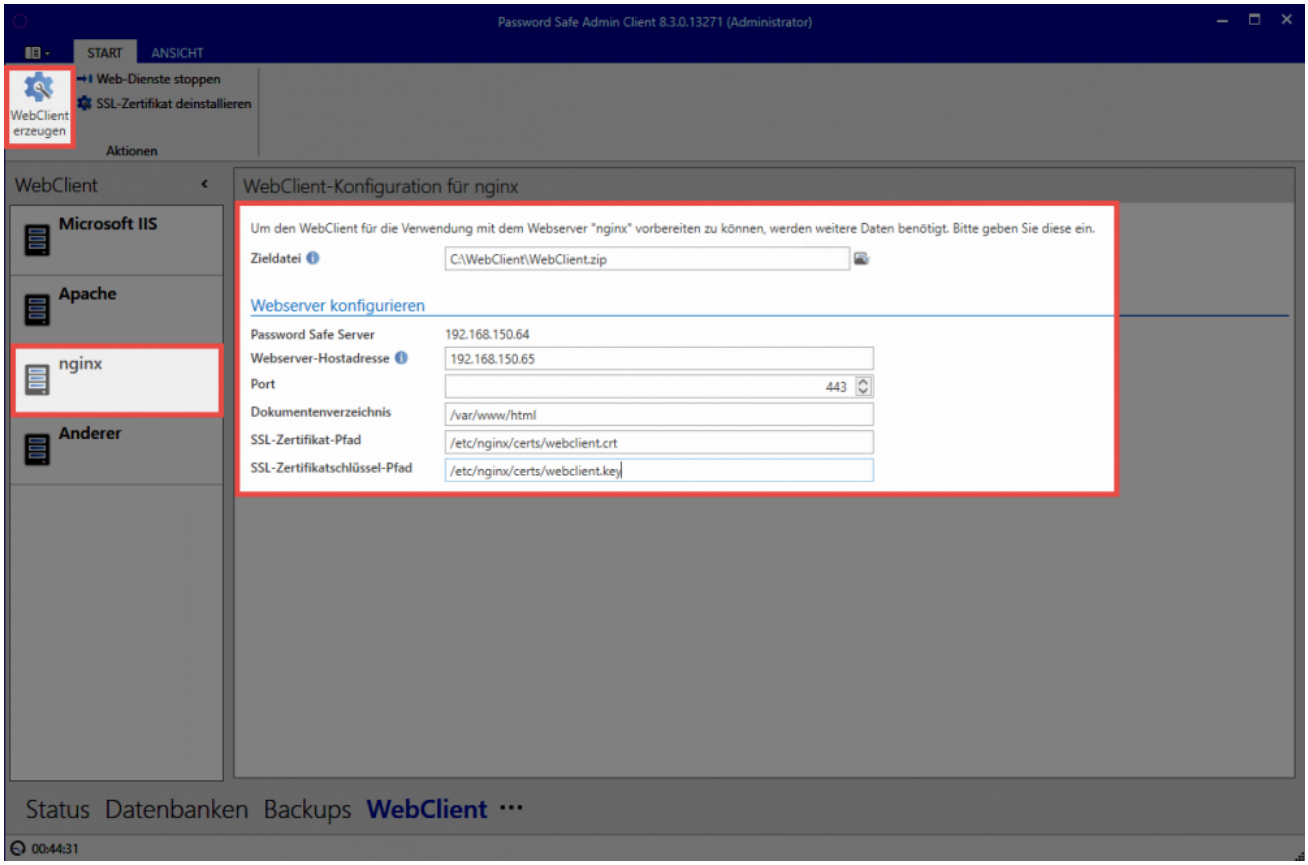
## nginx

Zum Einbinden des WebClients auf einem nginx Server müssen zunächst alle relevanten Einstellungen gesetzt werden:

**Dokumentenverzeichnis**
Hier wird angegeben, in welchem Ordner der WebClient betrieben werden soll.
Standardmäßig ist dies **/var/www/html**

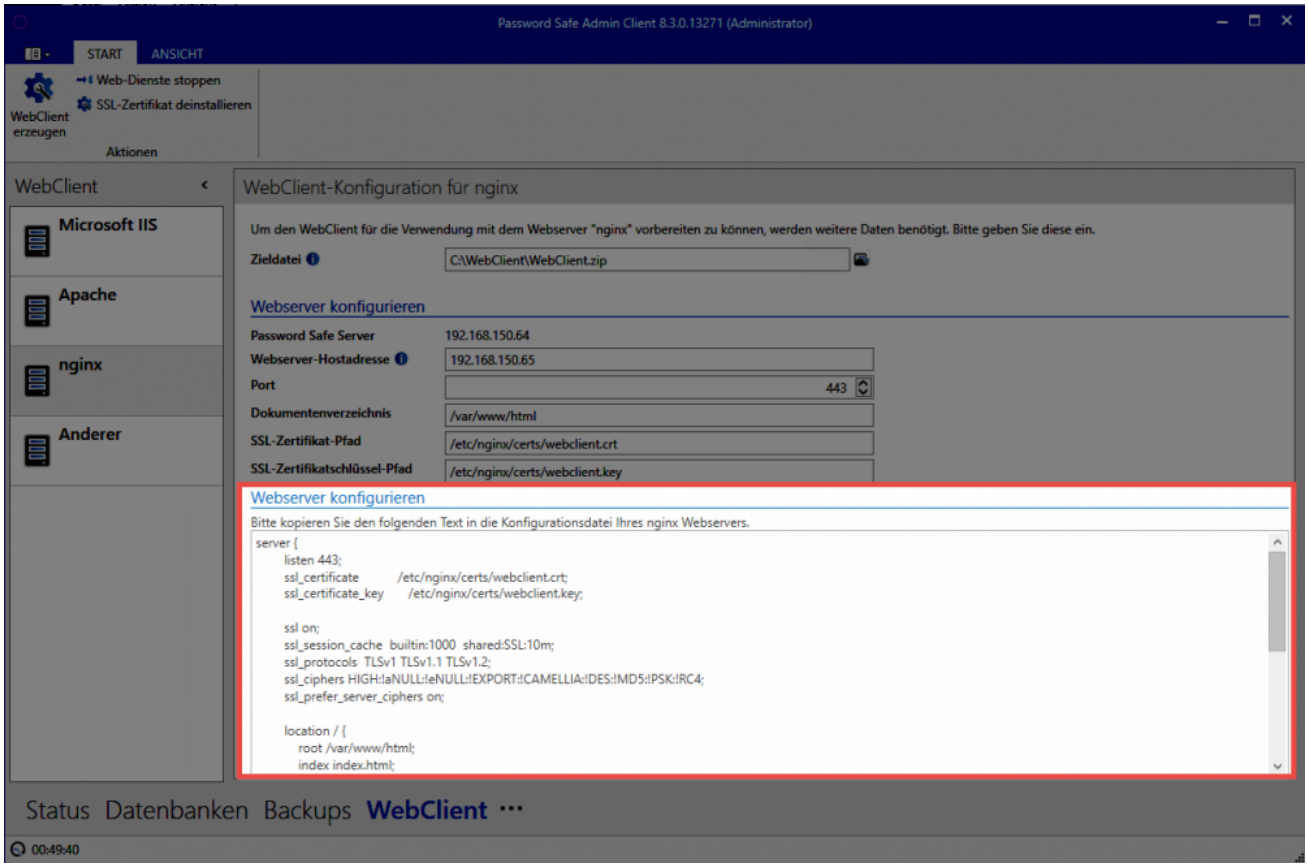
**SSL-Zertifikat-Pfad**
Es muss hier angegeben werden in welchem Verzeichnis das Zertifikat abgelegt wird.
Der Standardpfad lautet hierbei **/etc/nginx/certs/webclient.crt**

**SSL-Zertifikatsschlüssel-Pfad**
Schlussendlich muss noch hinterlegt werden, wo der Zertifikatschlüssel liegt.
Standardmäßig ist das **/etc/nginx/certs/webclient.key**



Wenn alle Einstellungen gesetzt sind, kann der WebClient über den Button in der Ribbon erzeugt werden. Es öffnet sich dann direkt der Ordner, in welchem die ZIP Datei liegt. Nun wird das Archiv entpackt und dessen Inhalt ins Dokumenteverzeichnis auf dem Webserver kopiert.

Zusammen mit der ZIP Datei wurde auch die Konfiguration für den nginx Server erzeugt. Diese kann direkt am AdminClient eingesehen werden.




Abschließend muss die Konfiguration noch am nginx eingebunden werden. Sie kann hierfür direkt am AdminClient kopiert werden.

> Jede Webserver Konfiguration ist individuell. An dieser Stelle kann daher nur das übliche Vorgehen in einer Standard Installation umrissen werden.

**Standardkonfiguration**

Zunächst wird die Datei **/etc/nginx/sites-available/default** geöffnet. Beispielsweise über “nano”. Nun wird der Eintrag `server { }` gesucht. Danach wird Konfiguration des AdminClient einfügt. Abschließend muss der Webserver über den Befehl **systemctl restart nginx** neu gestartet werden.

Der WebClient ist nun betriebsbereit und kann direkt aufgerufen werden.

# Aufruf des WebClients

Wie der WebClient aufgerufen werden kann, hängt von der Konfiguration des WebServers ab:

WebClient im **Basis-Verzeichnis** -> **https://hostname**
WebClient in einem **Unterverzeichnis** -> **https://hostname/pfad-zum-unterverzeichnis**
Port ist nicht gleich 443 -> **https://hostname:port/pfad-zum-unterverzeichnis**

# Updates

## Gründe für regelmäßige Updates

Unser Entwicklungsteam ist stets damit befasst die Software weiter zu entwickeln. Hierbei werden nicht nur Probleme behoben, sondern vor allem auch neue Features entwickelt um die Software bestmöglich an die Bedürfnisse unserer Kunden anzupassen. Es ist daher zu empfehlen regelmäßig Updates zu installieren. Nur so kann von den Weiterentwicklungen profitiert werden.

Die Dokumentationen beziehen sich immer auf den letzten verfügbaren Versionsstand. Sollte also Password Safe (beispielsweise im Aussehen oder auch im Funktionsumfang) von der Dokumentation abweichen, bietet es sich an zunächst auf die neueste Version zu aktualisieren.

> Über die Updateprüfung am Server oder am Client kann nach verfügbaren Updates gesucht werden. Die Updateprüfung am Client muss erst für Benutzer in den Einstellungen freigegeben werden. Wir empfehlen die Updateprüfung für normale Benutzer deaktiviert zu lassen, da sonst die Benutzer selbständig versuchen Updates zu installieren. Da sich ein neuerer Client nicht mit einem älteren Server verbinden kann, führt dies dazu, dass der Benutzer sich nicht mehr anmelden kann.

## Voraussetzungen

Vor einem Update sollten einige Voraussetzungen geprüft bzw. geschaffen werden.

### Prüfen der Softwarepflege

Das Recht Updates zu installieren wird mit der Softwarepflege erworben. Es gilt zu beachten, dass alle Updates installiert werden dürfen, solange die Softwarepflege aktiv ist. Bei abgelaufener Softwarepflege dürfen nur diejenigen Versionen verwendet werden, welche während der Laufzeit erschienen sind. Vor einem Update sollte also geprüft ob die Softwarepflege noch aktiv ist. Dies lässt sich einfach am AdminClient unter den Lizenzeinstellungen prüfen.

### Erstellen eines Backups

Ein Update ist immer ein tiefgreifender Eingriff in die bestehende Software. Daher sollte direkt vor einem Update ein entsprechendes Backup erstellt werden, um im Ernstfall keinen Datenverlust zu erleiden.

### Prüfen der Kompatibilität

Es wird stets versucht den AdminClient abwärtskompatibel zu gestalten. Leider ist dies nicht immer möglich. Daher sollte vor einem Update stets geprüft werden, mit welchen Client Versionen der AdminClient kompatibel ist. Die Versionshistorie der jeweiligen Version gibt hier Auskunft.

> ! Sollte das Passwort zur Anmeldung am AdminClient in der Datenbank gespeichert sein, so muss dieses unbedingt vor dem Update notiert bzw. zwischengespeichert werden!

### Aktuelle Installationsfiles

Die Installationsfiles können im Kunden.Informations-System herunter geladen werden:
https://license.passwordsafe.de/kis
Zum Anmelden nutzen Sie bitte einfach die Zugangsdaten welche Ihnen per E-Mail zugestellt wurden.

# Update

### Update des AdminClients

Der AdminClient wird einfach über die bestehende Installation drüber installiert.

> * Sofern die Dienste nicht vorab beendet wurden, gibt der Installationsassistent die Möglichkeit dazu. Werden die Dienste auch hier nicht beendet muss der Rechner abschließend neu gestartet werden. Es ist daher zu empfehlen, dass Sie die Password Safe Dienste vor dem Update beenden.

Weitere Infos zum Installationsassistenen sind dem Kapitel Installation AdminClient zu entnehmen

### Patchlevel Update der Datenbanken

Meistens sind die Datenbanken nach dem Update des AdminClients deaktiviert, da sie noch nicht den entsprechenden Patchlevel haben. Dies sollte direkt geprüft werden. Nach einer Anmeldung am AdminClient ist dies im Modul **Datenbanken** direkt ersichtlich. Sind die Datenbanken deaktiviert, können Sie direkt in der Ribbon über die entsprechende Schaltfläche wieder aktiviert werden. Während dessen wird der Patchlevel angehoben.

### Update der Clients

Auch die Updates der Clients erfolgt durch einfaches drüber installieren. Weitere Informationen sind im Kapitel Installation Client zu finden. Selbstverständlich kann das Update auch mit den Installationsparametern erfolgen.

### Update des WebClients

Zunächst muss der Anwendungsserver aktualisiert werden. Anschließend wird passend zum verwendeten Webserver ein neuer WebClient erzeugt. Nun sollte auf dem Webserver das Dokumentenverzeichnis komplett geleert werden. Der WebClient wird dann entpackt und auf den entsprechenden Webserver ins Dokumentenverzeichnis kopiert.

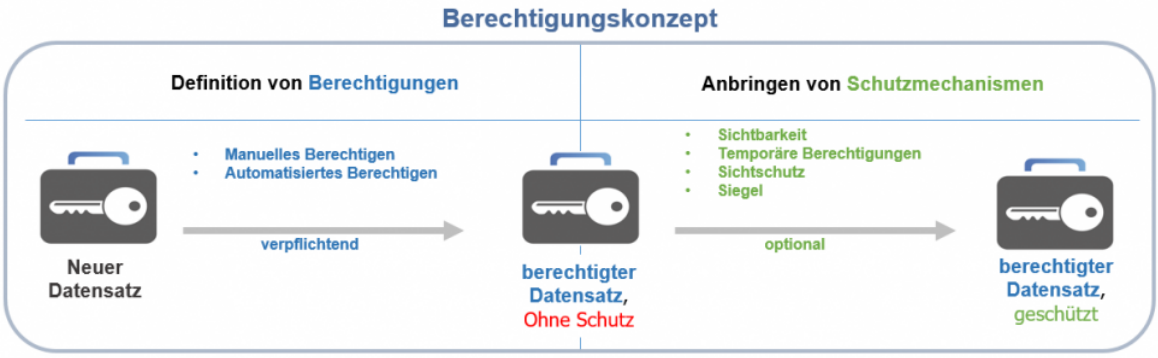
! Wird der WebClient auf einem IIS betrieben, wird mit dem Erstellen einer neuen Version eine neue **config.bat** erzeugt. Diese darf nicht ausgeführt werden, wenn der WebClient bereits installiert ist und sollte unbedingt nach erfolgtem Update gelöscht werden.

# Berechtigungskonzept und Schutzmechanismen

## Was ist das Berechtigungskonzept?

Die Stärke von Password Safe in der Version 8 ist es, auf alle erdenklichen Anforderungen in Bezug auf Berechtigungsmanagement die richtige Antwort parat zu haben. Um den manuellen Aufwand so gering wie möglich halten zu können, ist die Zusammenfassung mehrerer Benutzer in Rollen das Mittel der Wahl. Diese Rollen kann man dann entweder manuell oder automatisiert berechtigen. Für beide Varianten existieren mehrere Varianten, welche in den nachfolgenden Kapiteln exakt erläutert werden.

Neben der Definition von manuellen und automatischen Berechtigungen ist das (optionale) Anbringen von Schutzmechanismen Teil des Berechtigungskonzeptes. Die Schutzmechanismen sind den Berechtigungen somit nachgelagert. In der folgenden Grafik ist das Zusammenwirken all dieser Elemente veranschaulicht.




> Das Anbringen einer beliebigen Form der Berechtigung ist verpflichtend. Das Anbringen eines Schutzmechanismus ist optional.

> De facto ist die Konfiguration der Sichtbarkeit technisch Teil der Berechtigungen. Dennoch besitzt dieser Mechanismus “Schutzcharakter” und wird demnach in den Schutzmechanismen aufgeführt.

Bevor die nachfolgenden Kapitel manuelles und automatisches Berechtigen sowie die möglichen Schutzmechanismen behandeln, soll hier noch die grundlegende Mechanik des Berechtigungskonzeptes erläutert werden. Diese drei Grundpfeiler sind nachfolgend unumstößlich und wirken sich stets auf Berechtigungen jeder Art aus.

# Die drei Grundpfeiler des Berechtigungskonzeptes

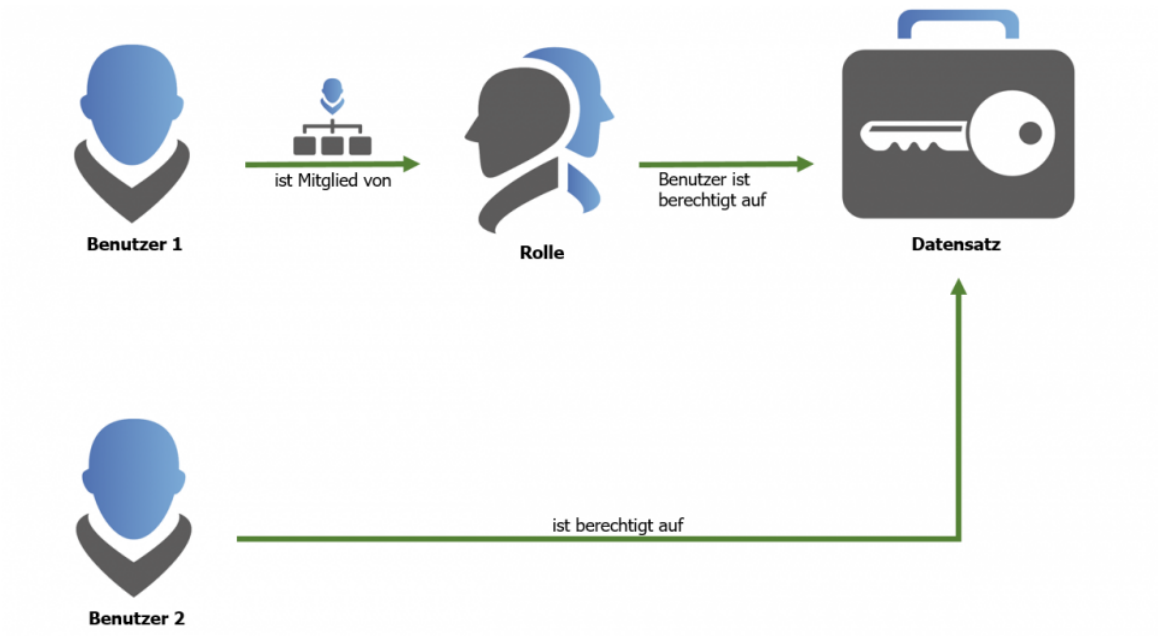
Das Abbilden unternehmensspezifischer Berechtigungsstrukturen kann im Aufwand stark variieren. Kleine Arbeitsgruppen wie auch international agierende Konzerne unterliegen im Password Safe bezüglich der Administration jedoch grundsätzlich den gleichen Gesetzmäßigkeiten. Das Grundkonzept basiert an sich nur auf wenigen Regeln, welche ohne Ausnahme immer gelten. Trotz der unzähligen, individuellen Stellschrauben kann man diese Grundregeln in drei wesentlichen Schritten zusammenfassen.

### 1. Berechtigungen nur für Benutzer oder Rollen

Soll die Berechtigung für einen Datensatz festgelegt werden, existieren grundsätzlich nur zwei Möglichkeiten:

1. Berechtigung für einen **Benutzer**
2. Berechtigung für eine **Rolle**

Eine Rolle ist technisch nichts anderes, als eine Zusammenfassung mehrerer Benutzer mit gleichgearteten Berechtigungen. Es bietet sich hierbei natürlich an, diese gemäß Ihrer im Unternehmen ausgeübten Tätigkeit in Rollen zu verwalten. Die Rolle “Administratoren” kann demnach mit weitläufigeren Berechtigungen versehen werden, als z.B. die Rolle “Vertriebsassistenz”. Diese rollenbasierte Vererbung ermöglicht in größeren Unternehmensstrukturen die Bewahrung der Übersicht sowie einfaches Vorgehen beim Hinzufügen neuer Mitarbeiter. Statt ihn einzeln berechtigen zu müssen, fügt man diesen einfach seiner ihm angedachten Rolle zu.

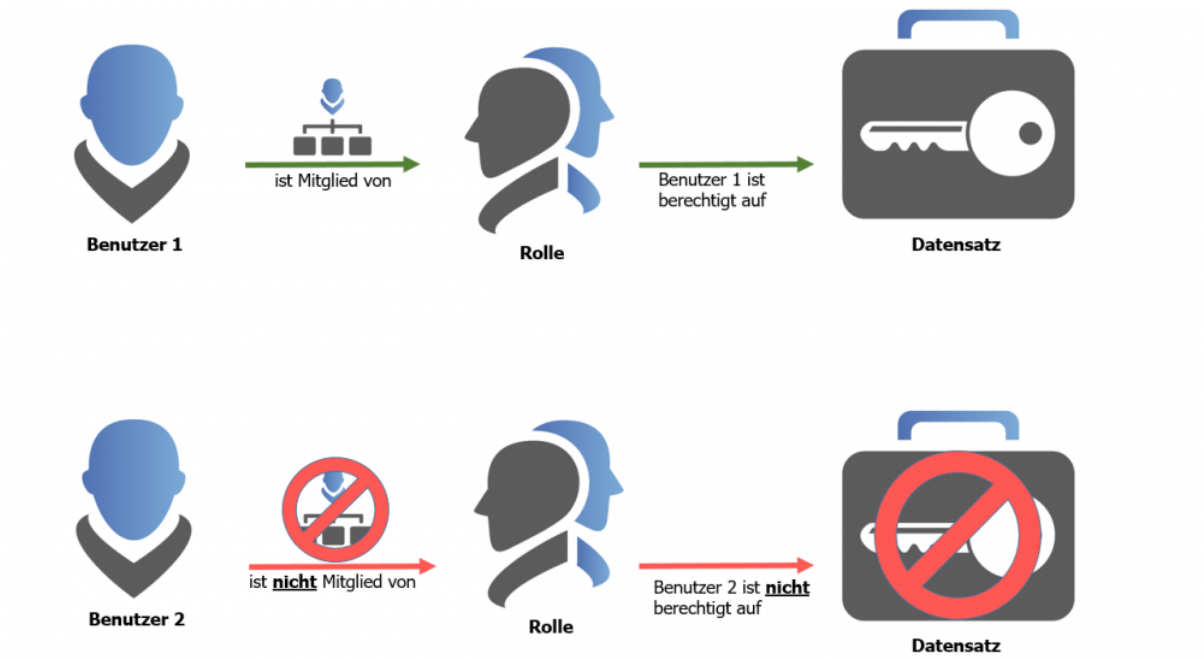


Es ist naheliegend, bei der Organisation von Zugängen rollenbasiert vorzugehen und nur in Ausnahmefällen einzelnen Mitarbeitern Rechte zu gewähren. Auch nicht planbare Personalausfälle müssen in solchen Konzepten bedacht werden. Das Arbeiten mit Rollen entschärft solche Risiken signifikant.

> Berechtigungen werden stets nur einem Benutzer oder einer Rolle gewährt!

### 2. Mitgliedschaft in Rollen

Der entscheidende Punkt ist die Mitgliedschaft in einer Rolle. Soll ein Mitarbeiter die Berechtigungen gemäß der ihm vorgesehenen Rolle nutzen können, **muss dieser zwingend Mitglied dieser Rolle sein**. Nur Mitglieder sehen diejenigen Datensätze, welche über die Rolle berechtigt wurden.

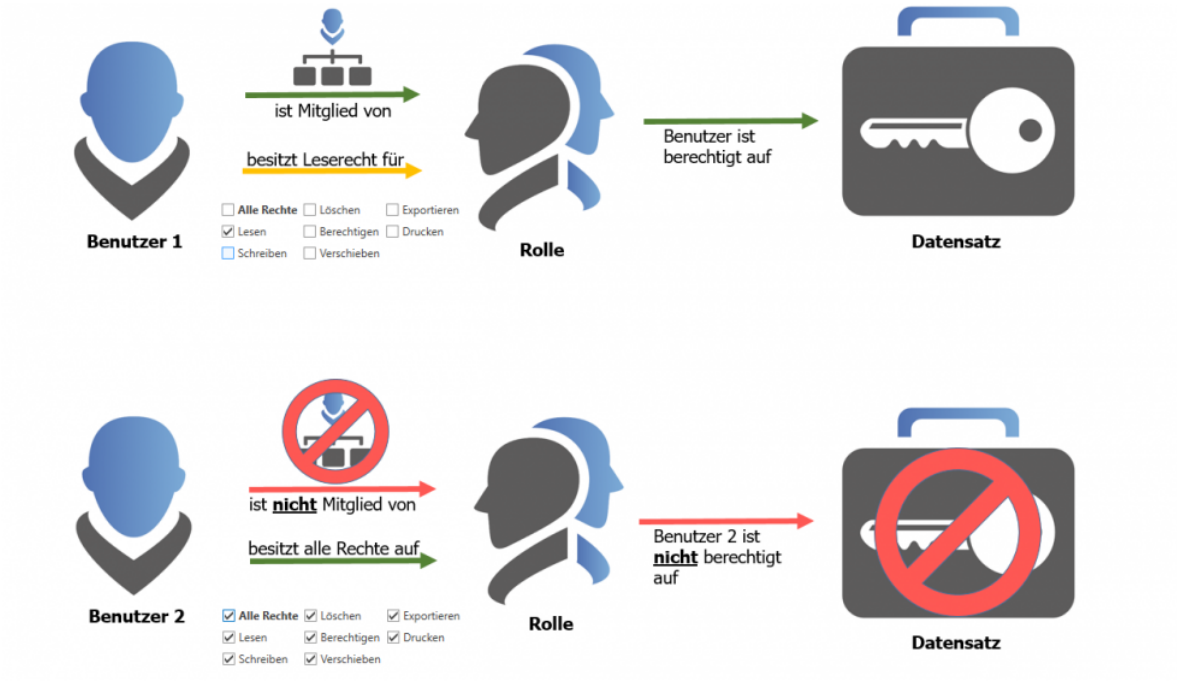



> Ein kleiner technischer Exkurs in die Art der Verschlüsselung kann bezüglich dem Grundverständnis sehr hilfreich sein. Jede Rolle besitzt ein Schlüsselpaar. Mit dem ersten Schlüssel werden Daten verschlüsselt. Zugang zu diesen Informationen erhält man dann nur mit dem zweiten Schlüssel. Die Mitgliedschaft in einer Rolle entspricht diesem zweiten Schlüssel.

### 3. Mitgliedschaft vs. Rechte auf Rollen

Das Wechselspiel zwischen Benutzern und Rollen ist ein Thema, dem man als administrierender Benutzer im Password Safe maximale Aufmerksamkeit widmen muss. Diese Mechanik bildet das grundlegende Fundament, um das Berechtigungskonzept verstehen zu können um dann maximal von

der individuellen Anpassbarkeit an beliebige Unternehmensstrukturen zu profitieren. Das folgende Schaubild soll dies anhand von zwei Benutzern verdeutlichen.




- **Benutzer 1** ist Mitglied der Rolle und dementsprechend berechtigt auf alle Datensätze, welche der Rolle angedacht sind. Auf die Rolle an sich besitzt er jedoch nur “Leserecht”. Das bedeutet, er kann die Rolle sehen, jedoch nicht “Bearbeiten, Verschieben oder gar Löschen”.
- **Benutzer 2** besitzt alle Rechte auf die Rolle. Er kann sogar durch “Berechtigen” weitere Benutzer der Rolle hinzufügen. Der entscheidende Punkt ist jedoch, dass er nicht Mitglied der Rolle ist. Er kann somit keine Datensätze einsehen, auf welche die Rolle berechtigt.

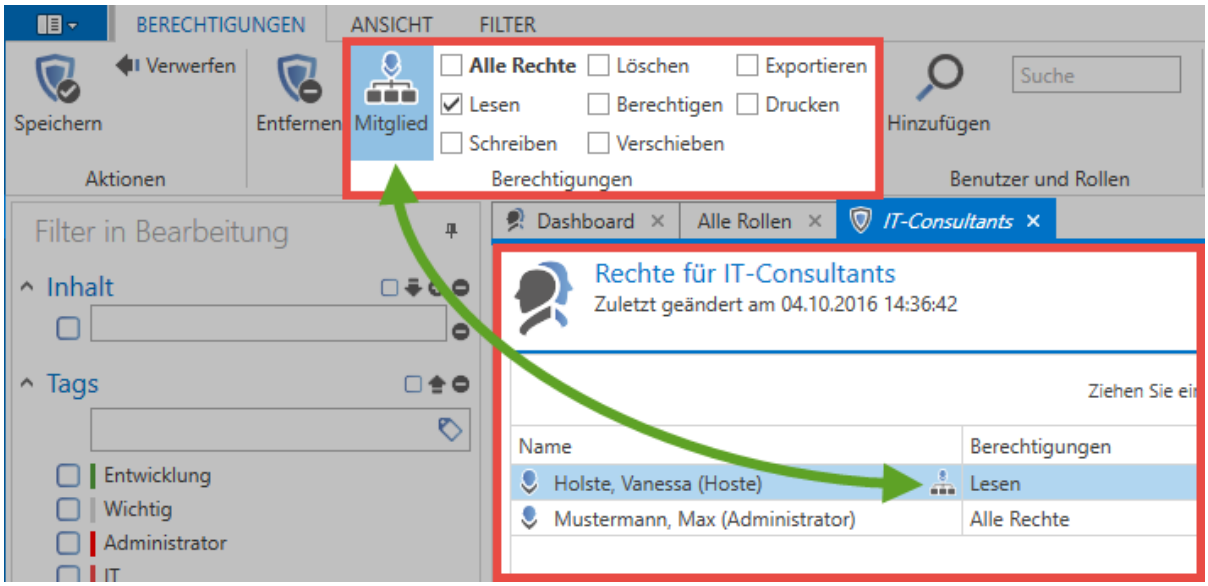
In der Praxis wäre der erste Benutzer ein klassischer User, der von Administratoren z.B. der Rolle Vertrieb zugeordnet wird und dementsprechend Datensätze einsehen kann. Der zweite Benutzer könnte der genannte Administrator sein. Dieser besitzt weitreichende Rechte auf die Rolle. Er kann diese beliebig bearbeiten und Benutzer hinzufügen. Er sieht jedoch keine Daten, welche dem Vertrieb zugeordnet sind. Hierzu fehlt ihm die Mitgliedschaft in der Rolle.

> Als Mitglied einer Rolle muss mindestens das Recht “Lesen” auf die Rolle gewährt werden!

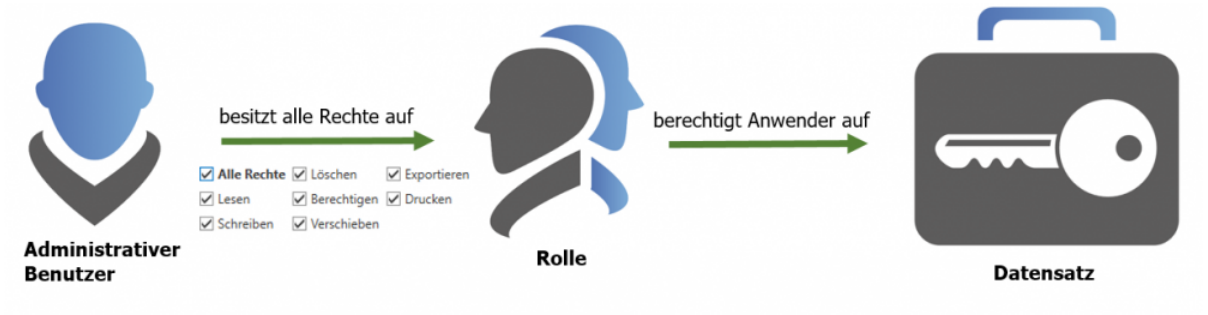
## Konkretes Beispiel und Konfiguration

Analog zum vorherigen Kapitel (Mitgliedschaft vs. Rechte auf Rollen) soll die Konfiguration einer Rolle anhand zweier Benutzer veranschaulicht werden. Die Konfiguration wird im Client Modul Rollen

vorgenommen. Durch Doppelklick auf die Rolle “IT-Consultants” in der Listenansicht öffnen wir deren Detailansicht.




- Der Benutzer “Holste” ist Mitglied der Rolle und kann dementsprechend auf diejenigen Datensätze zugreifen, für die die Rolle berechtigt ist. Er besitzt das obligatorische Leserecht auf die Rolle, welches Grundvoraussetzung ist, um Mitglied sein zu können. Welche exakten Rechte er auf den Datensatz besitzt wird nicht innerhalb der Rolle definiert! Dies ist im Folgekapitel festgelegt.
- Der Benutzer “Administrator” besitzt alle Rechte auf die Rolle, ist jedoch kein Mitglied! Er kann demnach keine Datensätze sehen, auf die die Rolle berechtigt. Er besitzt jedoch alle Rechte auf die Rolle und kann demnach Drucken, andere auf die Rolle berechtigen als auch diese löschen.




Anhand dieses Beispiels sieht man sehr gut, welche Vorteile das Konzept aufweist. Die komplette Trennung von administrativen Benutzern und Anwendern bringt erhebliche Vorteile mit sich. Natürlich muss das eine das andere nicht ausschließen. Ein Administrator kann natürlich vollen Zugriff auf die Rolle haben und ebenso Mitglied dieser sein! Die Grenzen sind fließend und im Password Safe beliebig definierbar.

# Manuelles Berechtigen

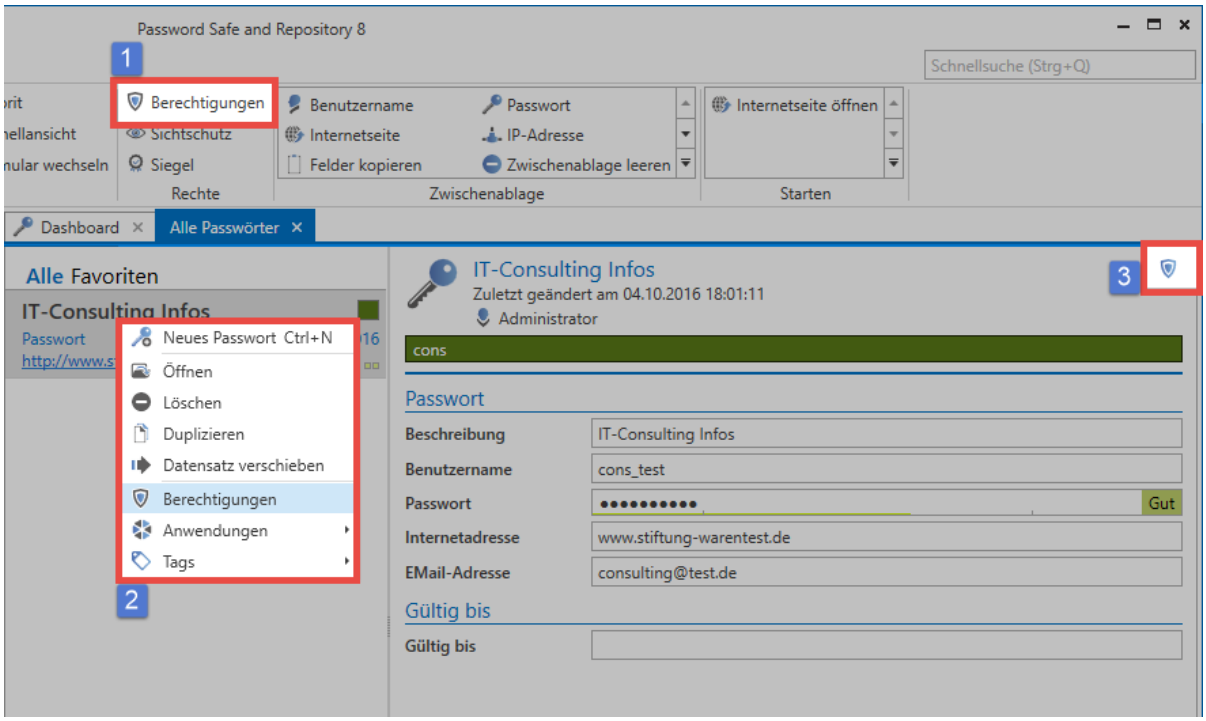
## Was sind manuelle Berechtigungen auf Datensätze?

Im Gegensatz zu automatisiertem Berechtigen greift beim manuellen Ansatz eben kein Automatismus. Diese Art der Berechtigung wird demnach für jeden Datensatz separat durchgeführt – bei der Neuanlage von Daten ist dieses Verfahren demnach weniger zu empfehlen. Will man dauerhaft effektiv arbeiten, sollte das automatisierte Berechtigen von Datensätzen bei der Erstellung von Passwörtern genutzt werden. Bei der Bearbeitung bereits bestehender Datensätze kommt in der Regel jedoch die manuelle Berechtigung zum Einsatz.

## Hinzufügen von weiteren Berechtigten

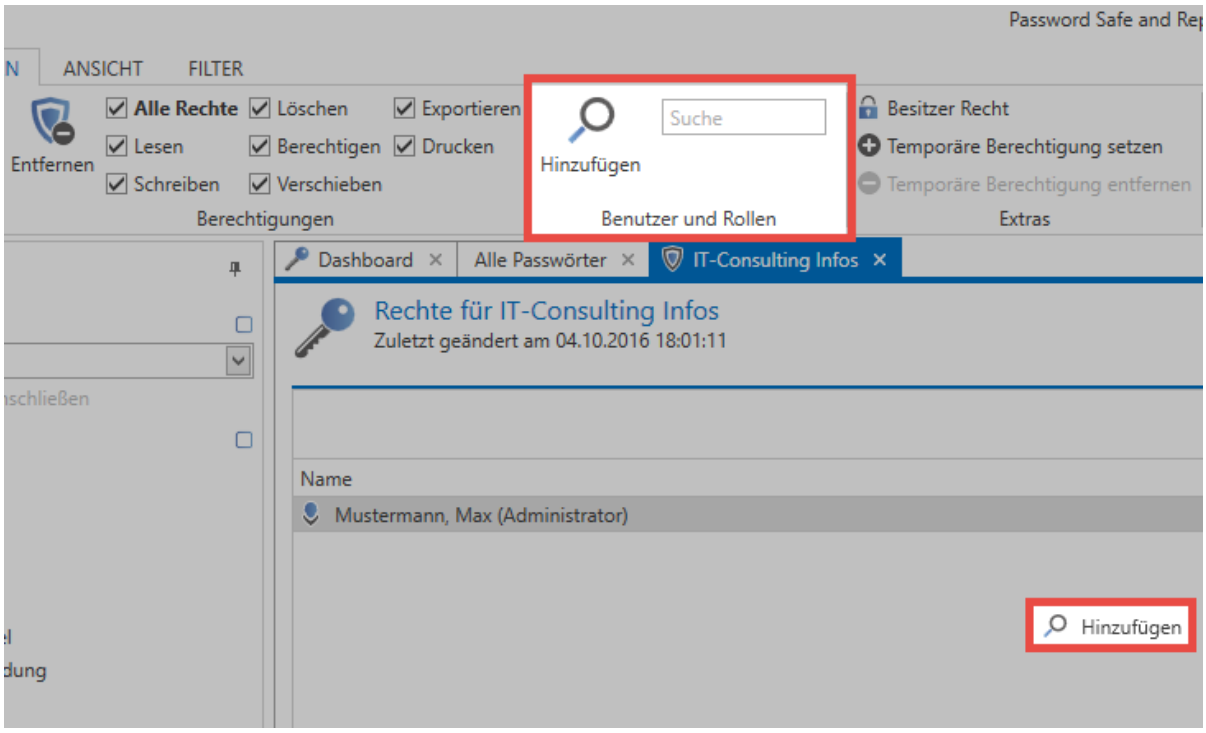
Im vorherigen Kapitel wurde geklärt, dass entweder ein Benutzer direkt, oder mehrere Benutzer zusammengefasst zu Rollen auf Datensätze berechtigt werden. Mit diesem Wissen kann nun ein Datensatz schlussendlich manuell berechtigt werden. Im Client Modul Passwörter erreicht man in der Listenansicht eines Datensatzes dessen Berechtigungen auf drei verschiedene Arten:

1. Icon in der Ribbon
2. Kontextmenü eines Datensatzes (Rechtsklick)
3. Icon am rechten Rand des Lesebereichs

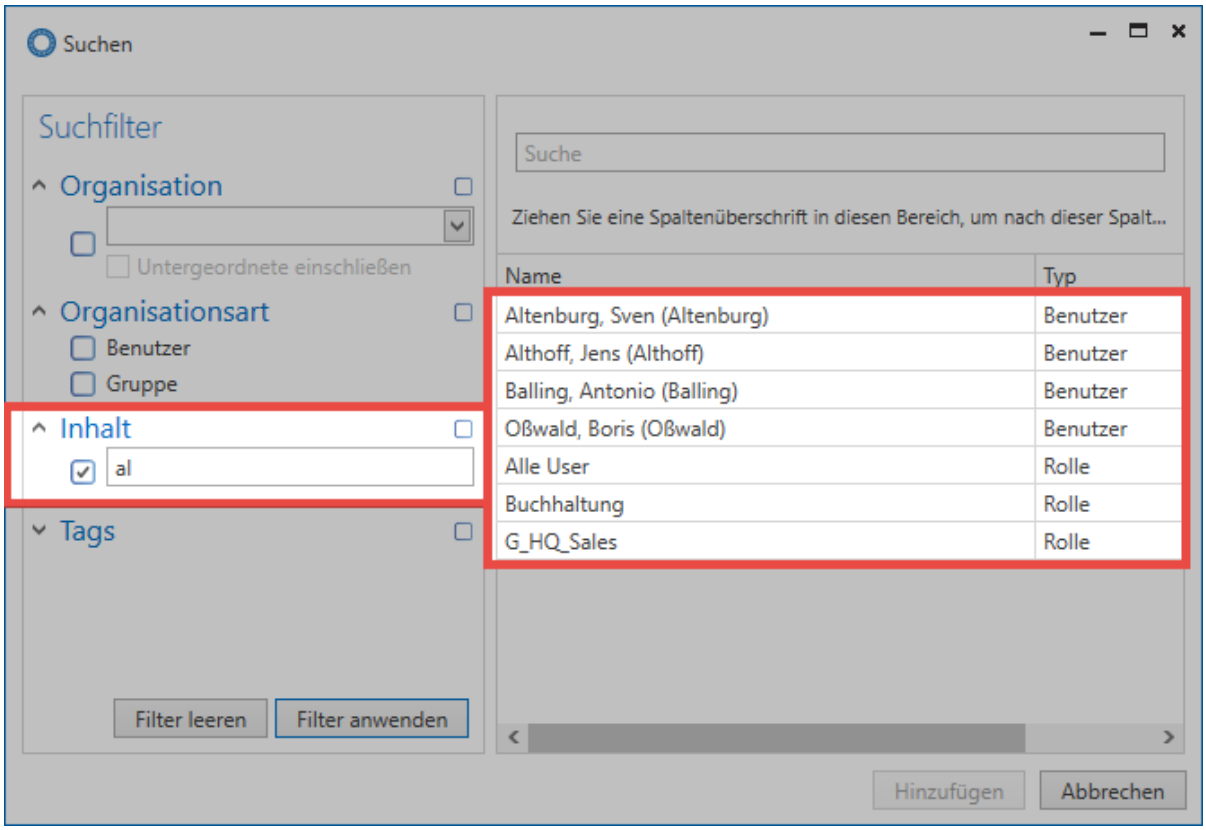


> Das Icon rechts im Lesebereich enthüllt “mouseover” die Information, ob der Datensatz persönlich oder öffentlich ist. Bei persönlichen Datensätzen ist der angemeldete Benutzer der einzige mit Berechtigungen!

Der Ersteller wird mit allen Rechten auf den Datensatz angelegt. Wie im Berechtigungskonzept beschrieben, können nun Rollen als auch Benutzer hinzugefügt werden. Sowohl über einen Rechtsklick im Tab, als auch über das entsprechende Icon in der Ribbon, gelangt man zum Suchfilter. Mit diesem kann man in wenigen Handgriffen diejenigen Benutzer ausfindig machen, welche auf den Datensatz berechtigt werden sollen.



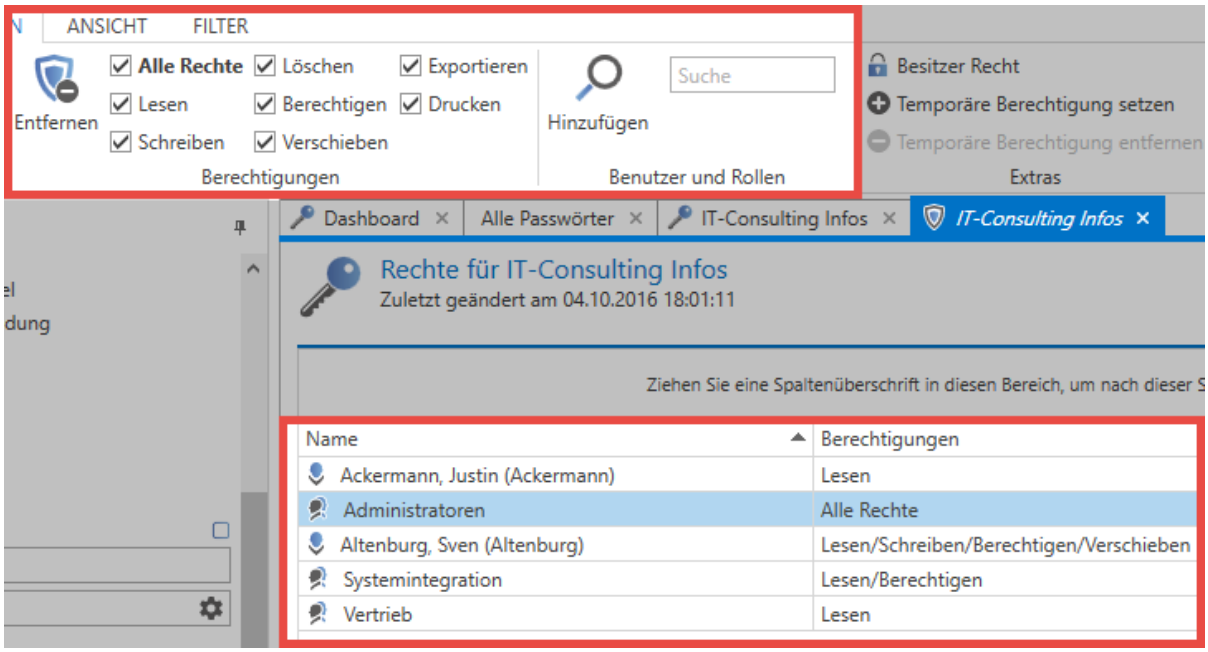

Der Suchfilter öffnet sich in einem separaten Tab. Der Filter lässt sich wie bekannt konfigurieren. Die Suche verhält sich analog zur Suche in der Listenansicht.




Auch die **Mehrfachauswahl** ist aktiviert und ermöglicht über die Windows-Standards Strg/Shift + linke Maustaste das Hinzufügen mehrerer Benutzer.

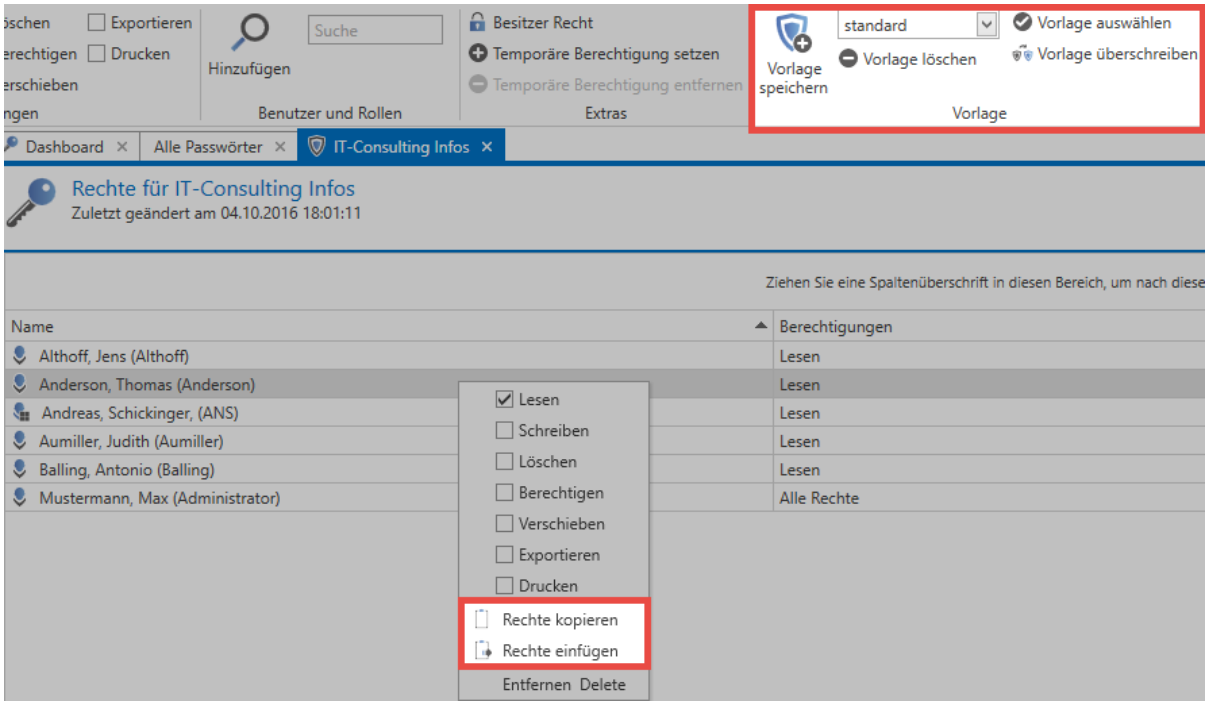
# Setzen und Entfernen von Berechtigungen

Standardmäßig erhalten alle hinzugefügten Benutzer oder Rollen lediglich das Recht “Lesen” auf den Datensatz. Dieses kann beliebig erweitert werden. Man kann mit den vorhandenen Hilfsmitteln sowohl Anwender, als auch administrative Rollen hinzufügen. Das eingangs genannte Recht “Lesen” ist ausreichend, um die Felder des Datensatzes einzusehen und das Passwort dann auch zu nutzen. Schreibrechte ermöglichen das Bearbeiten eines Datensatzes. **Das Recht “Berechtigen” ist nötig, um andere Benutzer auf den Datensatz zu berechtigen**. Ebenso wird dies bei der Konfiguration des Siegels als Grundlage herangezogen.




## Rechte übertragen

Über einen einfachen Rechtsklick auf einen Benutzer können im Kontextmenü Rechtekonfigurationen von Benutzern oder Rollen kopiert und auf andere übertragen werden. In diesem Zusammenhang ist auch die Nutzung von Rechtevorlagen sehr praktisch. Im Bereich “Vorlage” in der Ribbon können Sie konfigurierte Berechtigungen samt allen darin enthaltenen Benutzern speichern und bei anderen Datensätzen wiederverwenden.




Das Übertragen von Rechten sowie deren Wiederverwendung kann ein wichtiger Baustein sein, um Berechtigungsintegrität zu schaffen und zu wahren. Fehlkonfigurationen können durch diese Methode

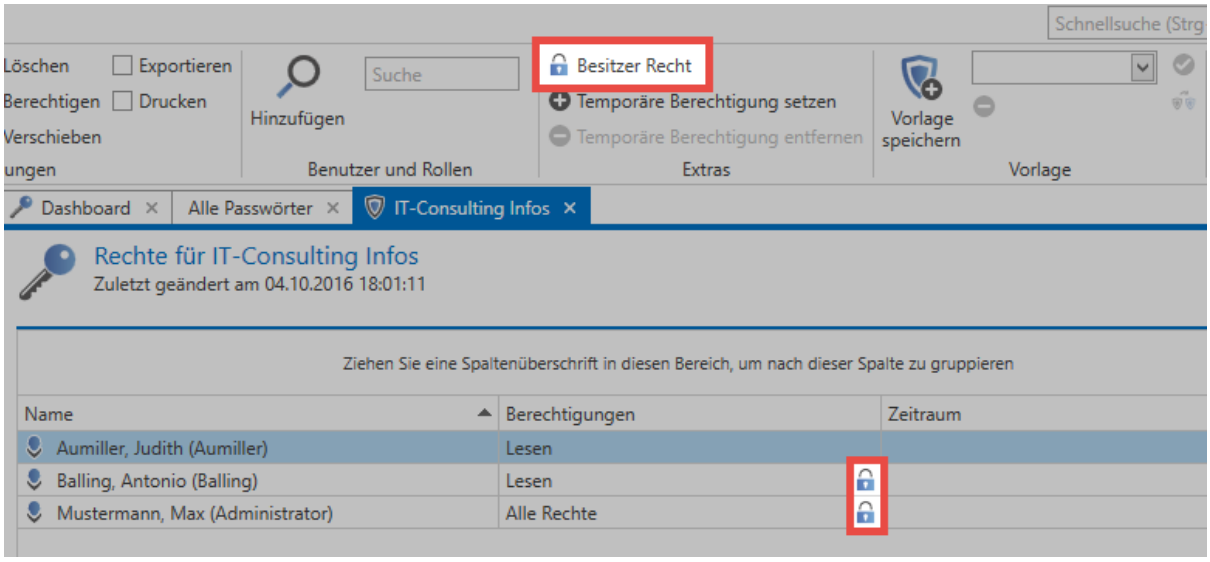
nicht ausgeschlossen werden, das Risiko wird jedoch deutlich minimiert. Selbstverständlich ist die korrekte Konfiguration dieser Vorlagen hierfür Voraussetzung.

## Das Hinzufügen-Recht

Innerhalb des Berechtigungskonzeptes genießt das “Hinzufügen-Recht” eine Sonderstellung. Hierbei geht es lediglich darum, ob ein Benutzer/eine Rolle innerhalb einer Organisationsstruktur z.B. einen neuen Datensatz erstellen darf. Dieses Recht kann schlussfolgernd nur im Modul Organisationsstrukturen gesetzt werden. Mehr…

## Besitzer Recht

Jedem Benutzer kann das Besitzer Recht zur Verfügung gestellt werden. Dieses Recht ist vielmehr eine **Garantie**. Einmal vergeben besteht keine Möglichkeit mehr, Benutzer oder Rollen mit Besitzer Recht aus den Berechtigungen eines Datensatzes zu entfernen. Dies ist nur noch durch den Benutzer oder die Rolle selbst möglich.



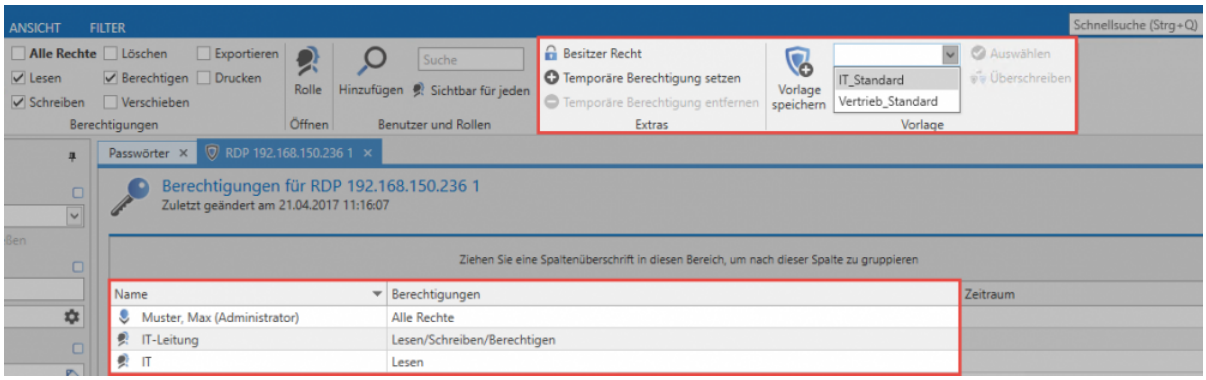

Das Besitzer Recht schützt somit vor dem Fall, dass andere Benutzer mit dem Recht “Berechtigen” wiederum andere aus dem Datensatz entfernen können.

> ! Das Besitzer Recht schützt nicht davor, dass ein Datensatz gelöscht werden kann. Nach wie vor kann jeder Benutzer mit Löschrecht den Datensatz entfernen!

# Nutzung von Rechtevorlagen

## Nutzung von Rechtevorlagen

Einmal konfiguriert können Berechtigungen stets wiederverwendet werden. Hierzu nutzt man die in der Ribbon zur Verfügung gestellte Funktionalität des **Speicherns von Berechtigungen als Vorlage**. Diese stehen dann global zur Verfügung und können auch auf andere Datensätze angewandt werden.




> Beim Speichern von Vorlagen sollte stets eine Bezeichnung gewählt werden, welche auch noch bei einer größeren Anzahl von Rechtevorlagen das sichere Unterscheiden ermöglicht.

Nichtsdestotrotz ist auch die Nutzung von Rechtevorlagen nur eine Arbeitserleichterung, welche nach wie vor manuell die Vergabe von Rechten vorsieht. Rechtevergabe in Form von Automatismen sind im Password Safe ebenso gegeben und werden einerseits im Kapitel Rechte vordefinieren, andererseits unter Vererbung aus Organisationsstrukturen behandelt.

# Mehrfachbearbeitung von Berechtigungen

## Worum geht es bei Mehrfachbearbeitung von Berechtigungen?

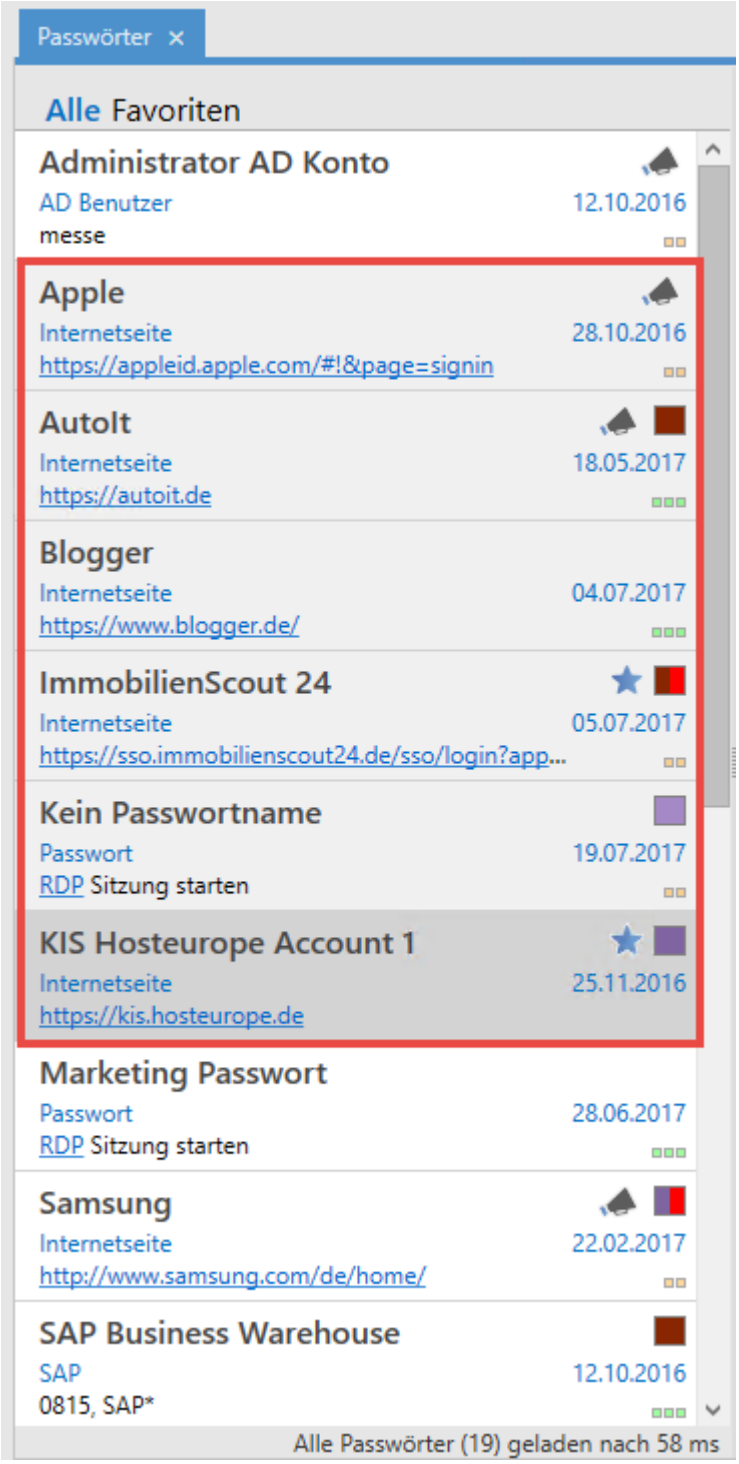
Im Rahmen der manuellen Anpassung von Berechtigungen ist auch die gleichzeitige Bearbeitung mehrerer Datensätze vorgesehen. Hierbei kann über unterschiedliche Mechanismen eine Auswahl der zu bearbeitenden Daten getroffen werden. Dies kann sowohl über eine selektive Auswahl in der Listenansicht geschehen, als auch über die Nutzung des Filter im Rahmen der Mehrfachbearbeitung. Beide Szenarien sind nachfolgend beschrieben.

## Mehrfachbearbeitung über die Listenansicht

Über die **Mehrfachbearbeitung innerhalb der Listenansicht** werden einzelne Rechte ergänzt oder entzogen. Hierbei werden die bestehenden Rechte **nicht überschrieben**.

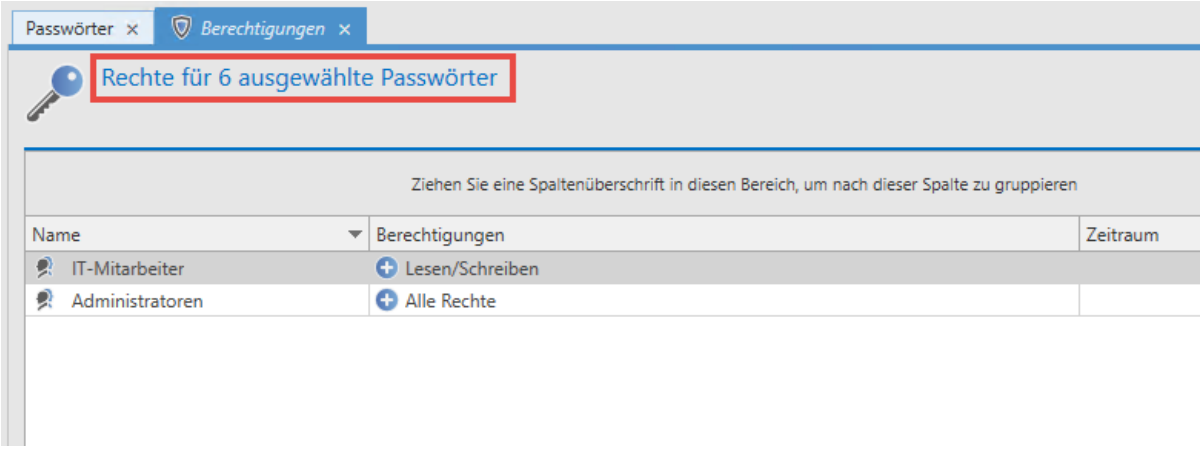
### Selektion der Datensätze

Innerhalb der Listenansicht kann mittels Shift, bzw. Strg. + Mausklick eine Mehrfachauswahl für Datensätze getroffen werden. Diese können durch die Selektierung gleichzeitig berechtigt werden. Wie üblich werden die markierten Datensätze in einer anderen Farbe angezeigt. Im nachfolgenden Schaubild sind 6 Datensätze markiert.




### Dialog zum Konfigurieren der Rechte

In der Ribbon wird über den Button **Berechtigungen** ein neuer Tab geöffnet, in welchem die zu vergebenden Rechte konfiguriert werden. Dort wird auch die Anzahl der Datensätze angezeigt, welche von den definierten Änderungen betroffen sind.




> Da sich die bereits vergebenen Rechte der selektierten Datensätze unterscheiden können, ist es nicht möglich die Rechte hier darzustellen.

### Rechte hinzufügen

Um ein Recht zu ergänzen, wird zunächst in der Ribbon über **Suchen und Hinzufügen** bzw. die **Suche** ein Benutzer oder eine Rolle selektiert. Anschließend werden wie gewohnt in der Ribbon die Berechtigungen ausgewählt. Durch das wird symbolisiert, dass die Rechte hinzugefügt werden. In folgendem Beispiel bekommt Hr. Steiner auf alle selektierten Datensätze Leserechte. Hr. Brewery erhält hingegen alle Rechte.

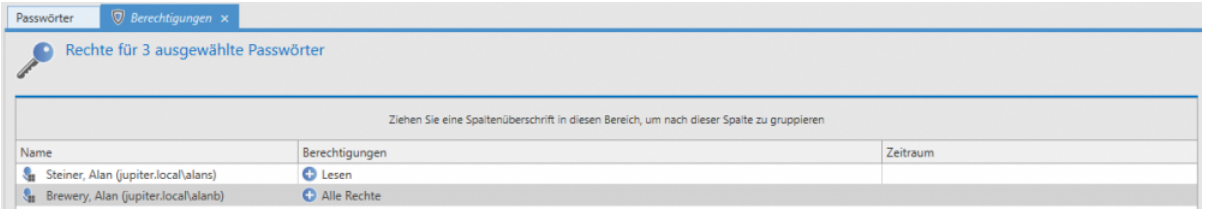
### Rechte reduzieren / Benutzer und Rollen aus der Berechtigung entfernen

Sollen Rechte entfernt werden, muss ebenfalls zunächst der zu bearbeitende Benutzer bzw. die gewünschte Rollen hinzugefügt werden. Über einen Klick auf **Rechte reduzieren** wird nun festgelegt, dass Rechte entzogen werden sollen. Dies wird durch das symbolisiert. Anschließend werden die zu entfernenden Rechte ausgewählt.

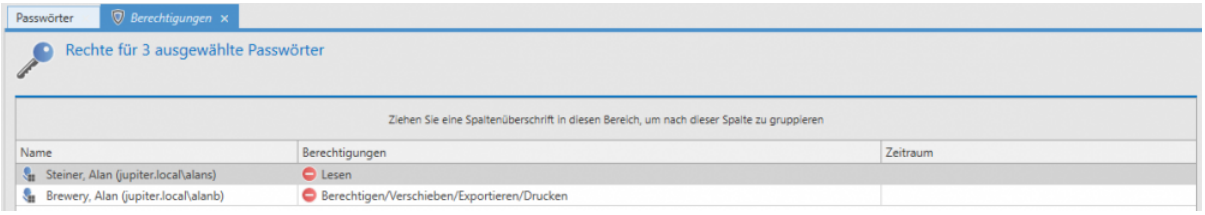
> Wird einem Benutzer oder einer Rolle das Recht **Lesen** entzogen, so wird der Benutzer komplett aus den Berechtigungen entfernt.

### Beispiele

In folgendem Beispiel bekommt Hr. Steiner auf alle selektierten Datensätze Leserechte. Hr. Brewery erhält hingegen alle Rechte:

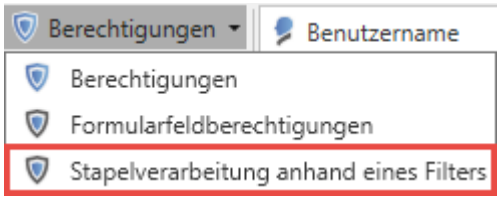



Hier wird Hr. Steiner das Leserecht entzogen. Da ohne das Leserecht keine anderen Rechte auf die Datensätze bestehen können, wird Hr. Steiner komplett aus den Berechtigungen entfernt. Hr. Brewery werden die Rechte Berechtigen, Verschieben, Exportieren und Drucken genommen. Davon ausgehend, dass er zuvor alle Rechte hatte, bleiben anschließend also noch die Rechte Lesen, Schreiben und Löschen übrig:




# Stapelverarbeitung anhand eines Filters

In manchen Fällen kann die Bearbeitung von Berechtigungen an sehr vielen Datensätzen von Nöten sein. Einerseits existiert die Restriktion auf maximal 1000 Datensätze, andererseits ist die Handhabung bei sehr vielen Datensätzen über die Listenansicht nicht immer die beste Wahl. Hierzu ist der Modus “Stapelverarbeitung anhand eines Filters” vorgesehen. Dieser wird direkt über die Ribbon initiiert.

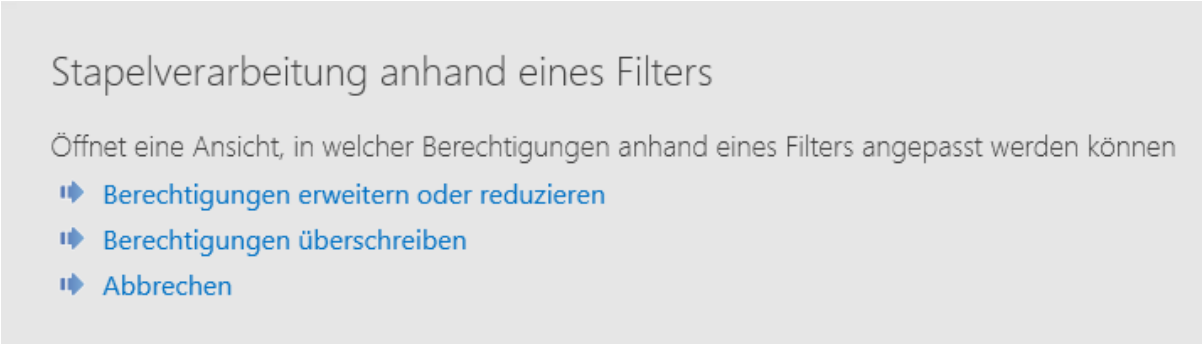



Im darauffolgenden Dialog wird festgelegt, ob vorhandene Berechtigungen erweitert, reduziert oder komplett überschrieben werden sollen. Entscheidet man sich hier für das **Erweitern bzw. Reduzieren** so wird die gleich Logik wie beim **Bearbeiten über die Listenansicht** verwendet. Es werden also keine bestehenden Rechte überschrieben.

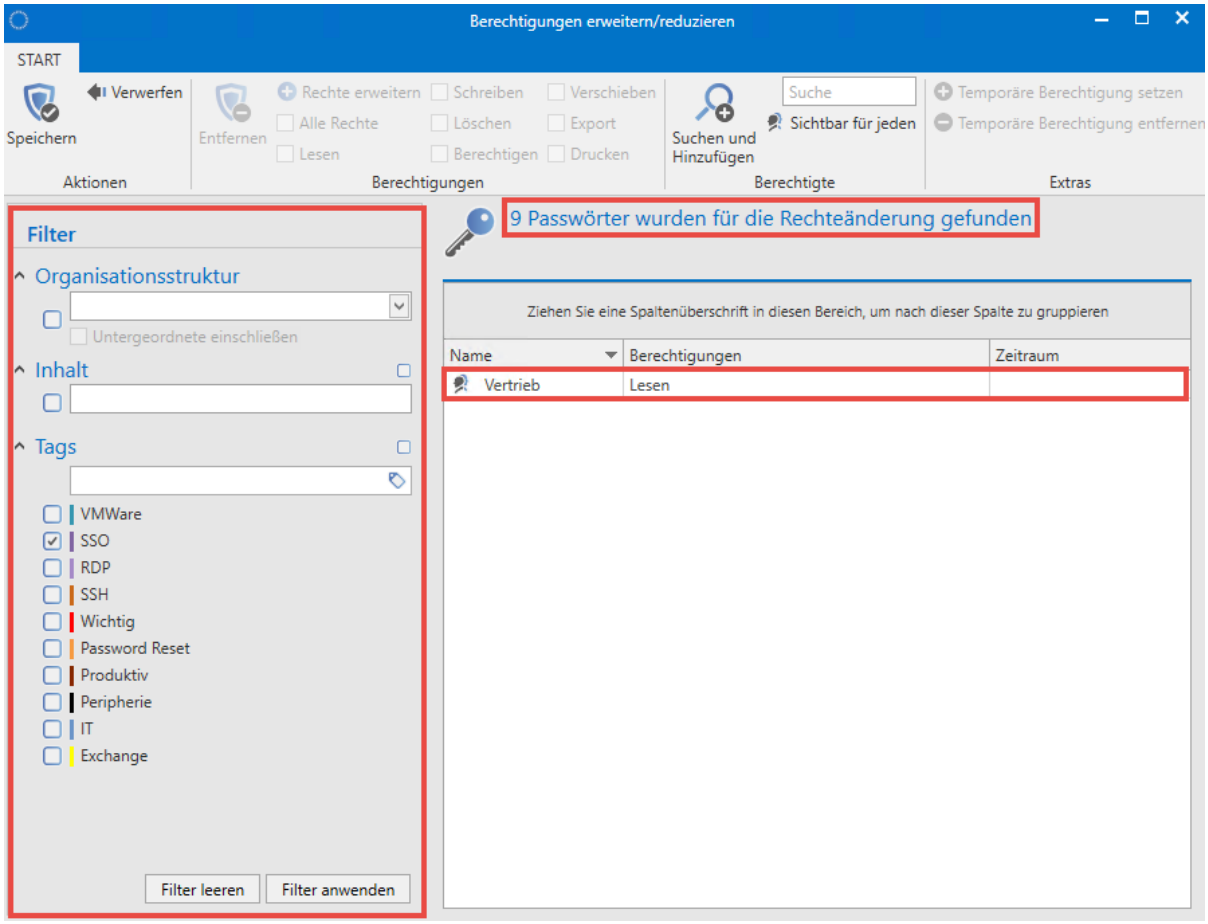
In der Variante **Berechtigungen überschreiben** werden zunächst alle bestehenden Rechte entfernt und durch die neu definierten Rechte ersetzt.

> ! Beim Überschreiben der Rechte ist äußerste Vorsicht geboten, da man sich durch diese Funktion schnell eine große Anzahl an Datensätzen unbrauchbar machen kann.

Der Modus ist standardmäßig inaktiv und muss zunächst über das Recht **Kann Stapelverarbeitung bei Berechtigungen anhand eines Filters durchführen** aktiviert werden.

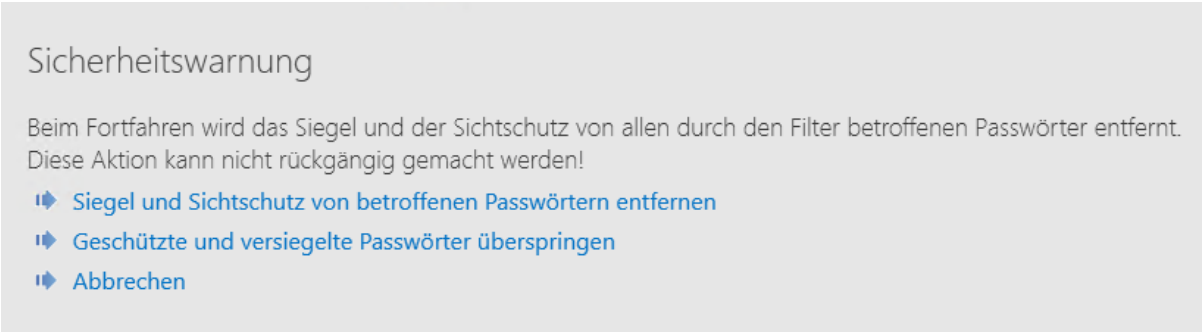



Die Auswahl der Datensätze welche bearbeitet werden sollen, wird durch den Filter selbst definiert. Als Default wird der derzeit konfigurierte Filter übernommen. Welche Datensätze von den Änderungen betroffen sein werden, wird in dieser Ansicht ebenso nicht aufgezeigt. Lediglich die Anzahl derer wird angezeigt. Im nachfolgenden Beispiel werden 9 Passwörter angepasst, indem die Rolle Vertrieb darauf lesend berechtigt wird.



### Siegel und Sichtschutz

Bei der Stapelverarbeitung können Datensätzen mit Siegel oder Sichtsperre nicht bearbeitet werden. Sind derartige Passwörter selektiert, so erscheint beim Ausführen der Stapelverarbeitung ein Dialog in welchem festgelegt wird, wie mit den Datensätzen umgegangen wird.




Hier kann nun entschieden werden, ob die betroffenen Datensätze übersprungen werden oder ob Siegel bzw. Sperre entfernt werden sollen. Entscheidet man sich für das **Entfernen** so muss der Vorgang nochmals durch die Eingabe einer PIN bestätigt werden.


! Das Entfernen von Siegel und Sichtsperren kann nicht mehr rückgängig gemacht werden!

* Je nach Anzahl der Datensätze kann das Anpassen der Rechte längere Zeit in Anspruch nehmen. Daher geschieht dieser Vorgang im Hintergrund. Über einen Hint wird der Abschluss der Berechtigung angezeigt.

# Automatisiertes Berechtigen

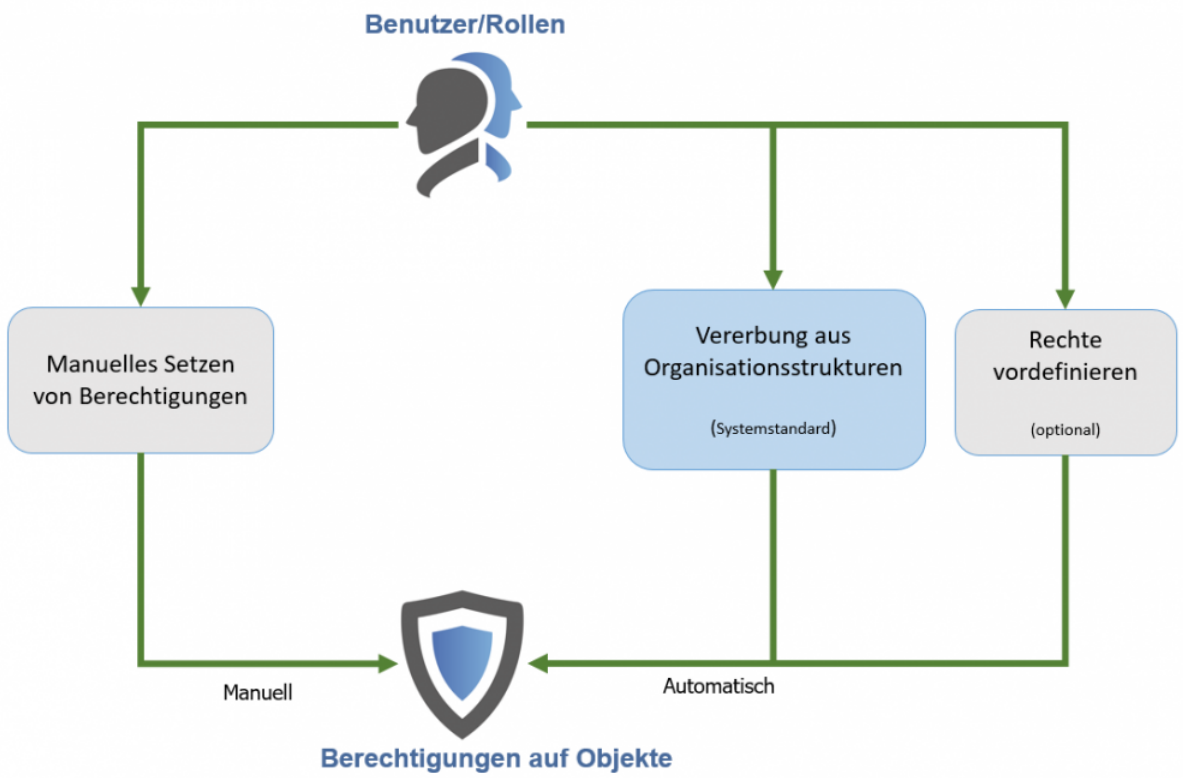
## Wiederverwendung von Berechtigungen

Grundsätzlich unterscheidet Password Safe mehrere Formen des Setzens von Berechtigungen:

1. Manuelles Berechtigen
2. Vererbung von Berechtigungen innerhalb Organisationsstrukturen
3. Nutzung von vordefinierten Rechten

- Bei der manuellen Konfiguration von Berechtigungen werden für jeden Datensatz die gewünschten Berechtigungen direkt konfiguriert. Automatismen und Vererbungen werden hierbei **nicht** genutzt.
- Sowohl die Nutzung vordefinierter Rechte als auch die Vererbung aus Organisationsstrukturen basieren beide auf der **automatisierten Wiederverwendung** bereits gesetzter Berechtigungen nach vorher definierten Regeln.

Das nachfolgende Schaubild beschäftigt sich demnach mit der Frage: **Wie erhalten Benutzer oder Rollen die Ihnen angedachten Berechtigungen?**

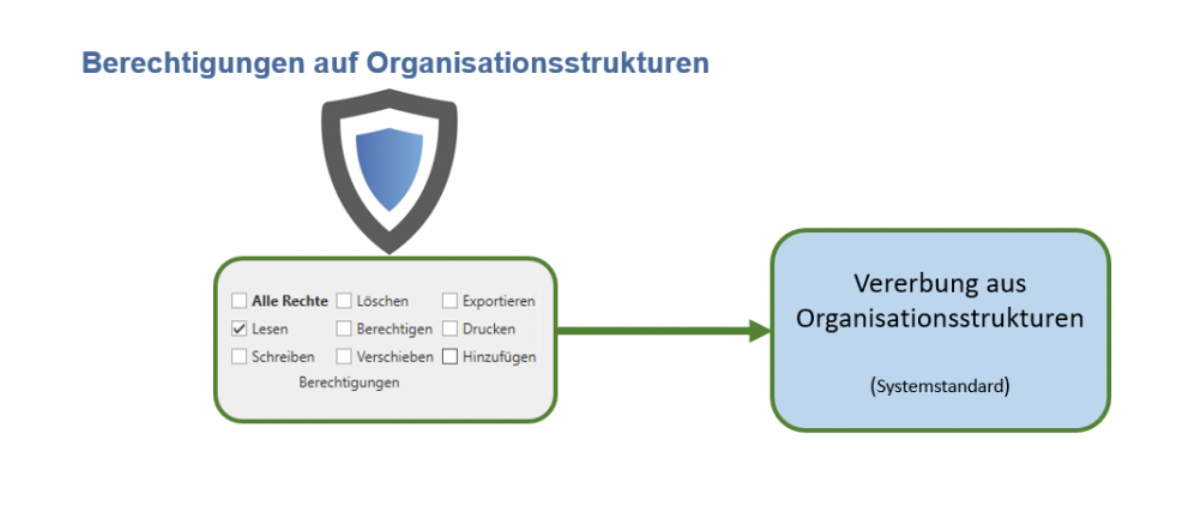


Die Vererbung aus Organisationsstrukturen ist systemseitig als **Standard** definiert. Dies kann in den Einstellungen konfiguriert werden. Die zugehörige Einstellung lautet “Berechtigungen vererben auf neuen Objekte (ohne Rechtevorlage). Weitere Infos…

# Vererbung aus Organisationsstrukturen

## Organisationsstrukturen als Basis

Ziel von Organisationsstrukturen ist es, die in einem Unternehmen gelebten Hierarchien und Abhängigkeiten der Mitarbeiter zueinander zu erfassen und abzubilden. Die Berechtigung dieser Strukturen erfolgt wie gewohnt über die Ribbon. Weitere Informationen zu diesem Thema können im Kapitel “Berechtigungen auf Organisationsstrukturen” eingesehen werden. Da man innerhalb der Organisationsstrukturen in der Regel bereits ein konkretes Berechtigungskonzept erstellt hat, wird dieses auch als Basis für weitere Berechtigungen herangezogen. Diese Form der Vererbung ist technisch einer Rechtevergabe gemäß **Ordnerzugehörigkeiten** gleichzustellen. Bei der Erstellung eines neuen Datensatzes erhält dieser Berechtigungen gemäß der in dieser Organisationseinheit definierten Berechtigungen.




## Relevante Benutzereinstellungen

Ob die genannte Form der Vererbung angewandt werden soll, wird über die Einstellungen in der Ribbon definiert. Die zugehörige Einstellung lautet “Berechtigungen vererben auf neue Objekte (ohne Rechtevorlage)”.

| Kategorie: Rechte | |
|---|---|
| Benutzerfeld nach dem Hinzufügen leeren | Deaktiviert |
| Berechtigungssuche: Schrittweise hinzufügen | Deaktiviert |
| Berechtigungen vererben auf neue Objekte (ohne Rechtevorlage) | Organisationseinheit |
| Benutzer aus den Berechtigungen bei neuen Objekten entfernen, wenn der Benutzer über eine Rolle berechtigt wird | Deaktiviert |

### mögliche Werte

- **Aus**: Berechtigungen auf OUs werden nicht vererbt

- **Organisationseinheit**: Berechtigungen beim Erstellen neuer Objekte werden gemäß den in der Ziel-Organisationseinheit definierten Rechten gesetzt.
- **Organisationseinheit und Benutzer**: Zusätzlich zur Vererbung aus Organisationseinheiten wird nun auch bei der Erstellung privater Datensätze die Vererbung gemäß den auf dem Benutzer konfigurierten Berechtigungen vorgenommen.

Ist die Vererbung auch auf Benutzer aktiviert, ist das Erstellen privater Datensätze an sich nicht mehr möglich. Bei der Erstellung neuer Datensätze, welche in der Organisationseinheit des angemeldeten Benutzers abgelegt werden sollen, werden nun die Berechtigungen auf den Datensatz gemäß der Berechtigungen auf den Benutzer vergeben.

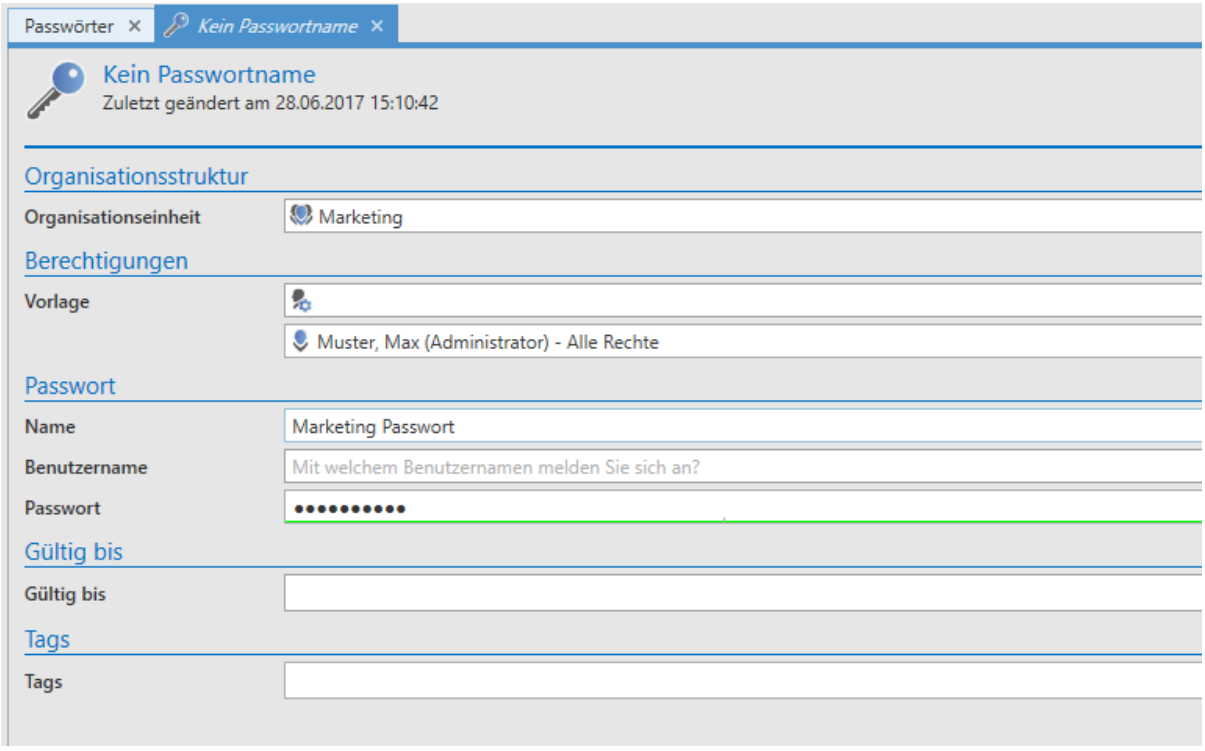
Ist ein vordefiniertes Recht vorhanden, überschreibt dieses stets Vererbungen aus Organisationsstrukturen

## Fallbeispiel

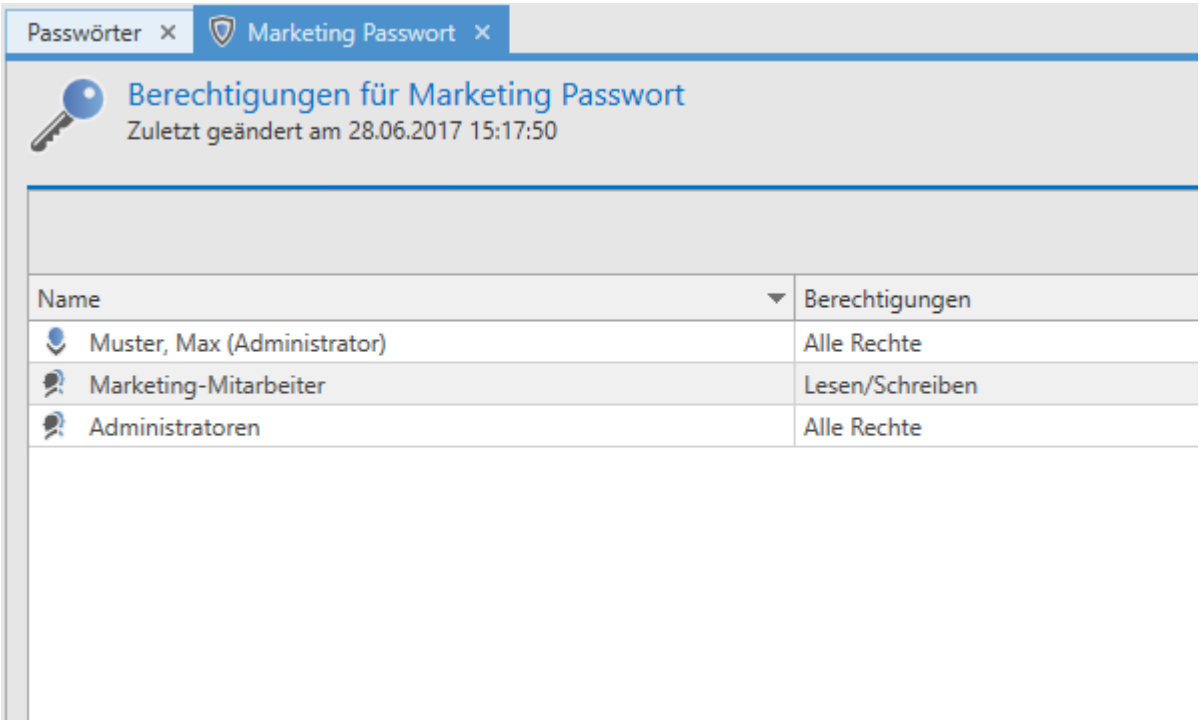
Betrachtet werden soll das Anlegen eines neuen Datensatzes in der Organisationsstruktur “Marketing”. Für die genannte Organisationsstruktur ist in den Einstellungen definiert, dass Berechtigungen auf neue Objekte gemäß der Organisationsstruktur vererbt werden sollen.

Nachfolgend die Berechtigungen auf die Organisationseinheit Marketing:


Nun wird ein neues Passwort in der Organisationseinheit “Marketing” erstellt.




Wichtig ist, dass für diese Organisationseinheit **kein** Preset definiert ist. Betrachtet werden sollen nun die Berechtigungen auf den soeben erstellten Datensatz.

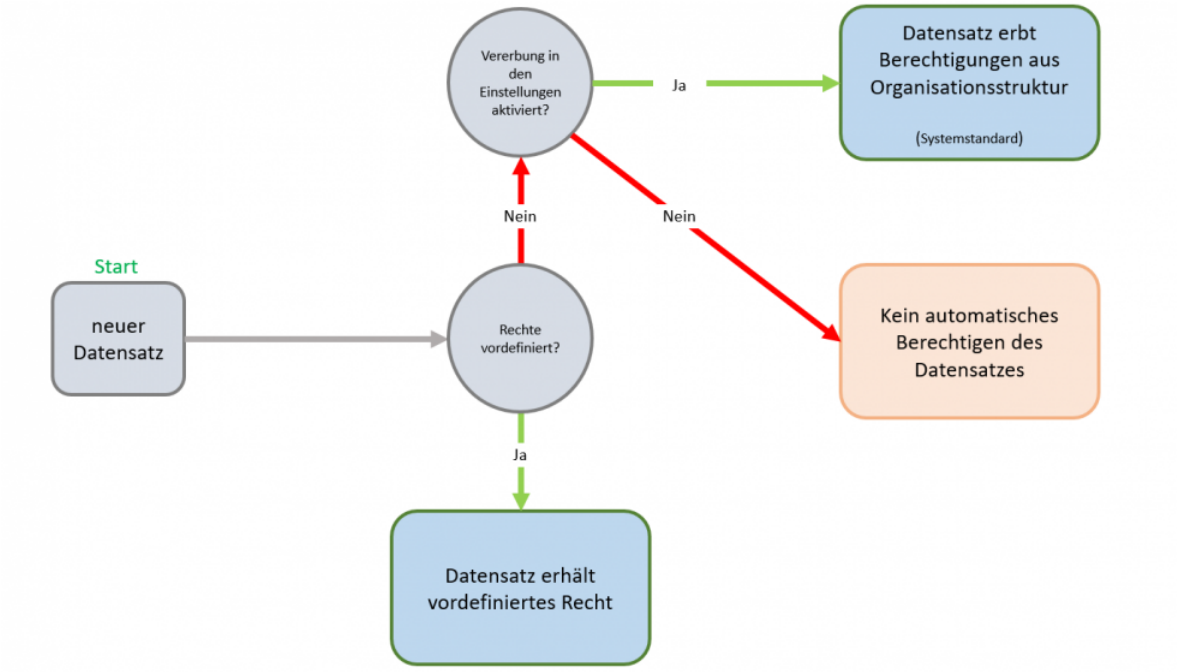



## Fazit

Beim Anlegen neuer Objekte wird einfach die Berechtigung des “Ablageortes” genutzt. Hierzu sind zwei Bedingungen nötig:

1. Es muss in den Einstellungen die Vererbung von Berechtigungen auf den Wert “Organisationseinheit” gesetzt sein
2. Es darf für die betreffende Organisationsstruktur kein vordefiniertes Recht existieren

Dieser Vorgang wird in nachfolgendem Schaubild verdeutlicht:



# Rechte vordefinieren

## Was sind vordefinierte Rechte?

Das Setzen von Berechtigungen auf Datensätzen kann natürlich stets für jeden Datensatz separat erfolgen. Obwohl man auf diese Art und Weise sehr granular jede angedachte Berechtigungsstruktur abdecken kann, ist dies nicht wirklich effizient. Einerseits ist der Konfigurationsaufwand zu hoch, andererseits besteht stets die Gefahr, dass Personen, welche ebenso auf Daten berechtigt sein sollten, vergessen werden. Hinzu kommt, dass viele Benutzer gar nicht das Recht haben sollen, Berechtigungen zu setzen. “Rechte vordefinieren” ist ein adäquates Mittel, durch die Nutzung von Automatismen die Vergabe von Berechtigungen zu erleichtern und die Fehlerquote zu senken. Nach deren Konfiguration auf der vorliegenden Seite widmen sich separate Kapitel dem Arbeiten mit vordefinierten Rechten sowie deren Geltungsbereich .

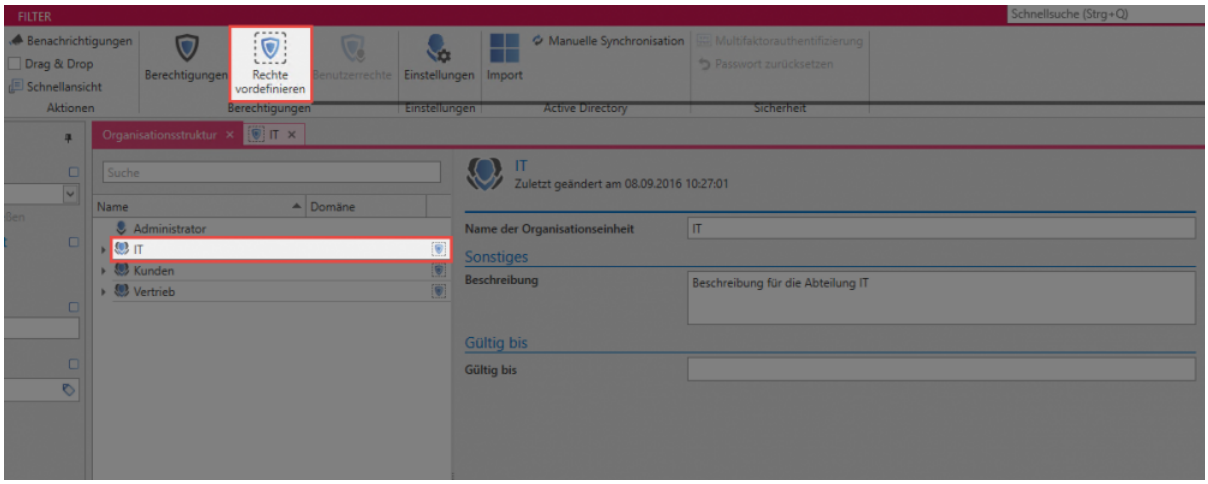
## Organisationsstrukturen als Basis

Organisationsstrukturen können im Password Safe in vielerlei Hinsicht sehr nützlich sein. Im vorliegenden Beispiel stellen Sie das Grundgerüst dar, auf dem die automatische Rechtevergabe fußt. Im weitesten Sinne sollten diese Organisationsstrukturen stets gemäß der vorhandenen Abteilungen in einem Unternehmen angelegt werden. Im nachfolgenden Beispiel soll im Speziellen eine IT-Abteilung betrachtet werden. Innerhalb dieser IT-Abteilung seien folgende 3 Hierarchien (Rollen) gegeben:

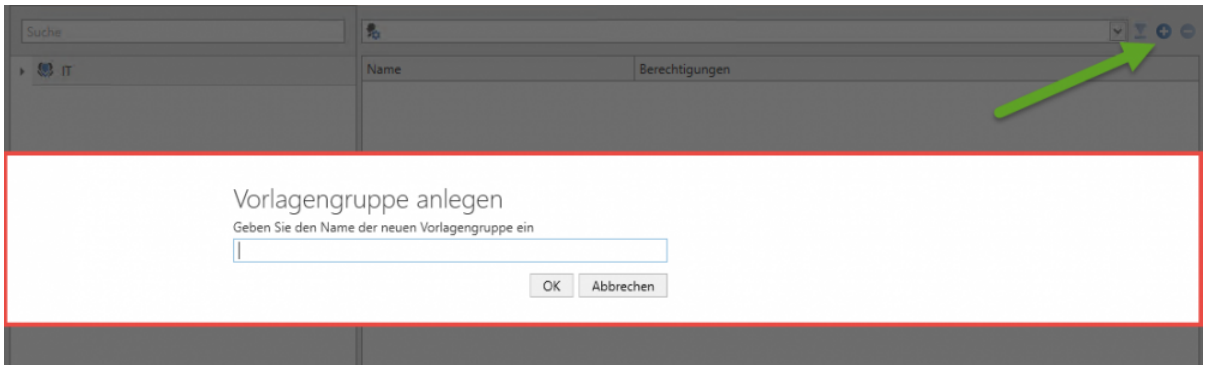
- **IT-Mitarbeiter**
- **IT-Leitung**
- **Administratoren**

## Rechte vordefinieren

In der Regel ist ein höher gestellter, leitender Angestellter mit umfangreicheren Rechten ausgestattet, als dies bei Auszubildenden der Fall ist. Diese Hierarchie und die damit verbundenen Berechtigungsstrukturen können vordefiniert werden. Im Modul Organisationsstruktur wählen wir nun diejenige OUs (Abteilung) aus, für die Rechte vordefiniert werden sollen und wählen **Rechte vordefinieren** in der Ribbon.



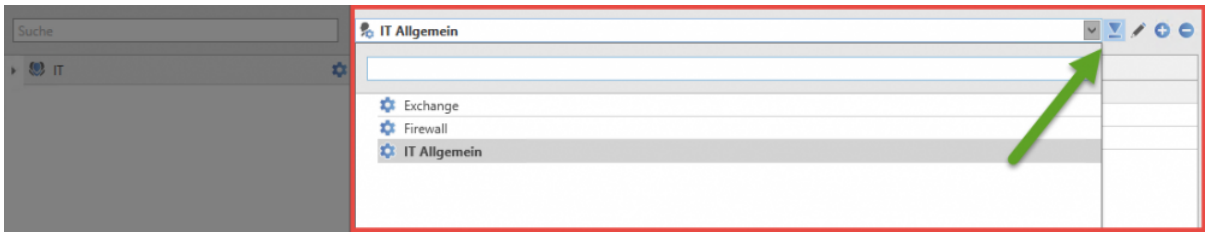

- **Erstellen der ersten Vorlagengruppe:** Über das Icon zum Hinzufügen neuer Vorlagengruppen (grüner Pfeil) erscheint ein modales Fenster, bei dem man einen möglichst aussagekräftigen Namen für die Vorlagengruppe wählt.




Sowohl über die Ribbon als auch über das Kontextmenü (rechte Maustaste) können nun Rollen und Benutzer in diese Vorlage übernommen werden. Dies wurde im nächsten Schritt bereits durchgeführt. Die Rolle **IT-Mitarbeiter** ist lediglich lesend berechtigt, die **IT-Leitung** besitzt zudem Schreibrechte sowie die Möglichkeit, Berechtigungen zu verwalten. **Administratoren** besitzen alle verfügbaren Rechte. Die Konfiguration der Rechtestrukturen ist innerhalb des hierfür vorgesehenen Kapitels erläutert.

# Hinzufügen weiterer Vorlagengruppen

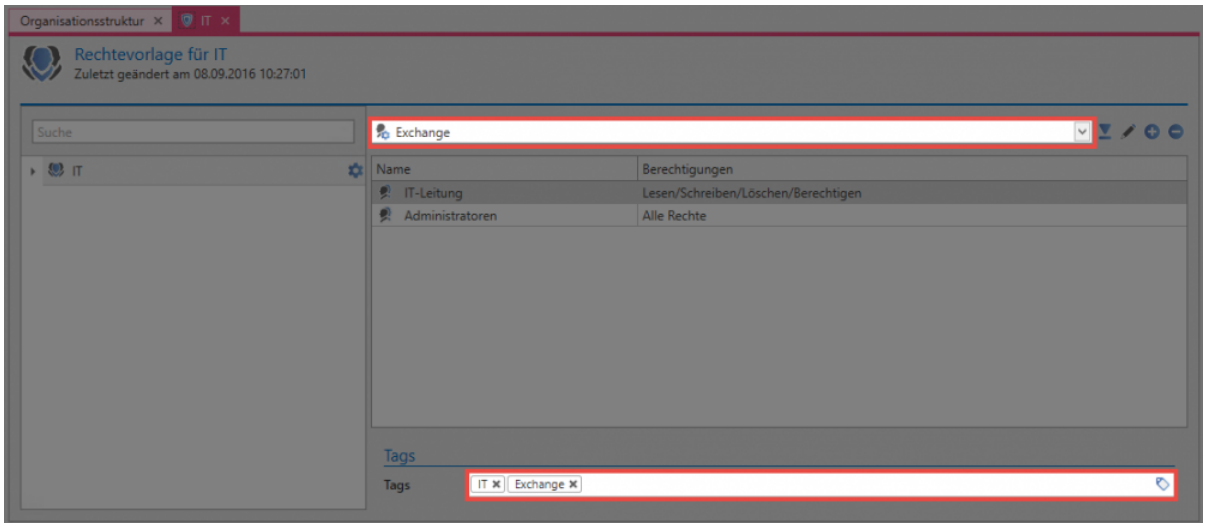
Auch innerhalb einer Abteilung können mehrere, unterschiedliche Rechtevorlagen konfiguriert werden. Dies mag zum Beispiel dann nötig sein, wenn innerhalb einer Abteilung mehrere Kompetenzbereiche existieren, welche jeweils sich unterscheidenden Berechtigungen unterliegen. Nachfolgend sind neben dem Bereich **IT-Allgemein** noch die Vorlagengruppen **Exchange** sowie **Firewall** definiert.




Direkt neben dem Dropdown Menü für die Auswahl der Vorlagengruppe kann eine **Standard-Vorlagengruppe** definiert werden (grüner Pfeil). Diese ist stets vorkonfiguriert, wenn man “IT” als OU zum Speichern von Datensätzen auswählt.

# Tagvergabe beim Vordefinieren von Rechten

Analog zur Definition von Berechtigungen innerhalb von Rechtevorlagen können auch **Tags** automatisch gesetzt werden. Die Konfiguration erfolgt analog zur Tagvergabe bei Datensätzen.




Dieses Vorgehen gewährleistet, dass bei Nutzung einer bestimmten Vorlagengruppe automatisch ein spezielles Tag vergeben wird. Fallbeispiele können Sie im hierfür vorgesehen Kapitel einsehen.

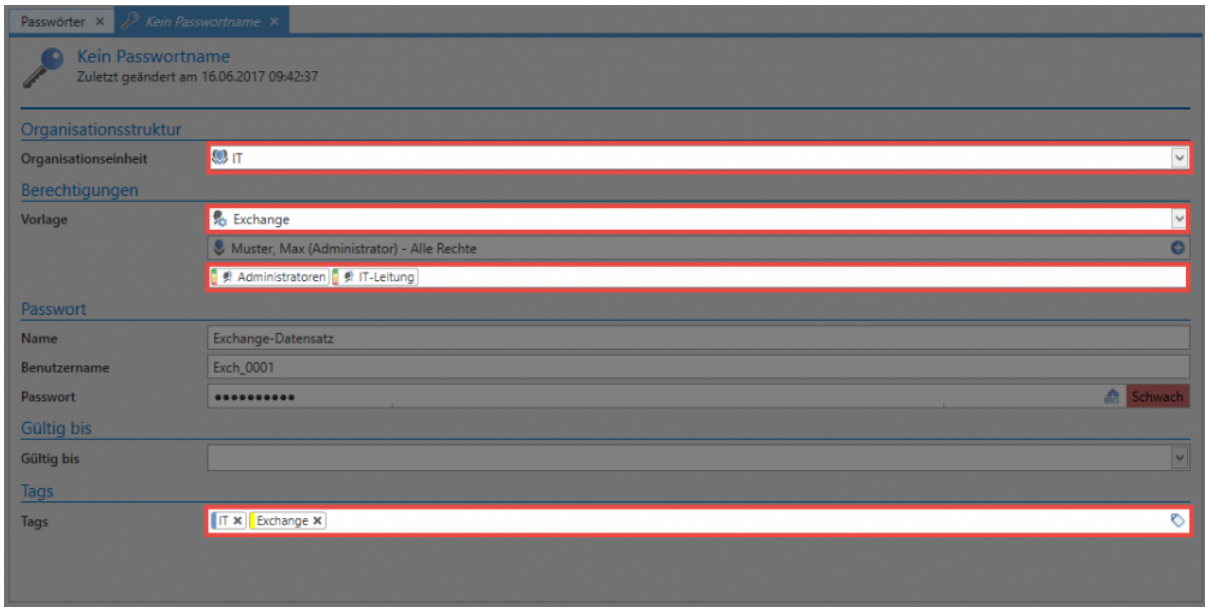
# Arbeiten mit vordefinierten Rechten

## Nutzung von vordefinierten Rechten beim Erstellen von Passwörtern

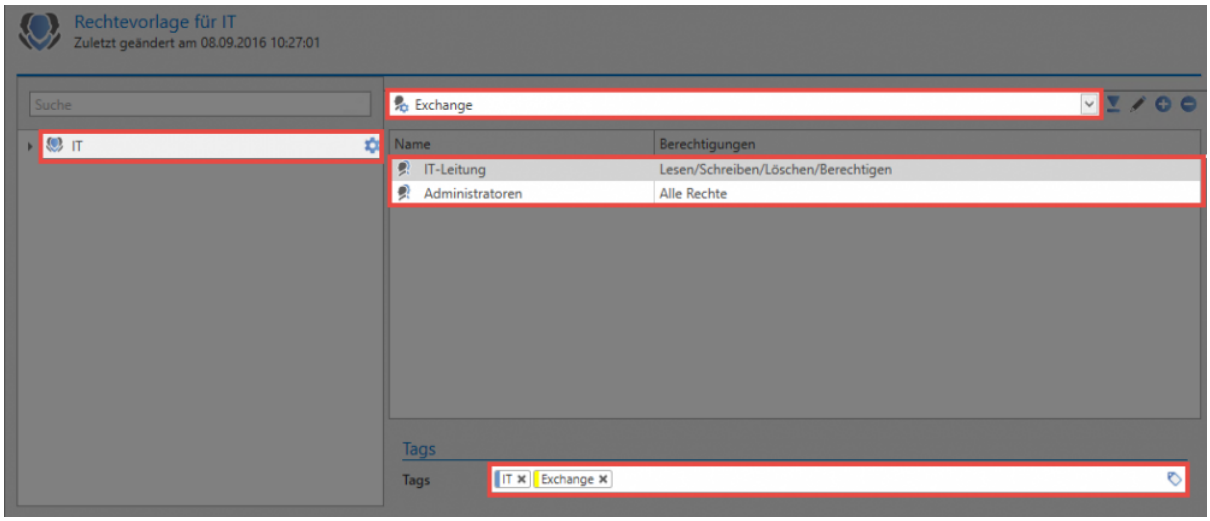
Nachdem man Rechte vorkonfiguriert hat, kann man dieses nun beim Erstellen von neuen Datensätzen auswählen. Hierzu geht man wie folgt vor:

- Auswahl Modul Passwörter
- “Neues Passwort” über die Ribbon
- Auswahl eines Formulars

Im daraufhin erscheinenden Fenster wurde nun die Organisationseinheit “IT” sowie die Vorlagengruppe “Exchange” ausgewählt.




Zum Vergleich hier die hinterlegte Rechtevorlage:



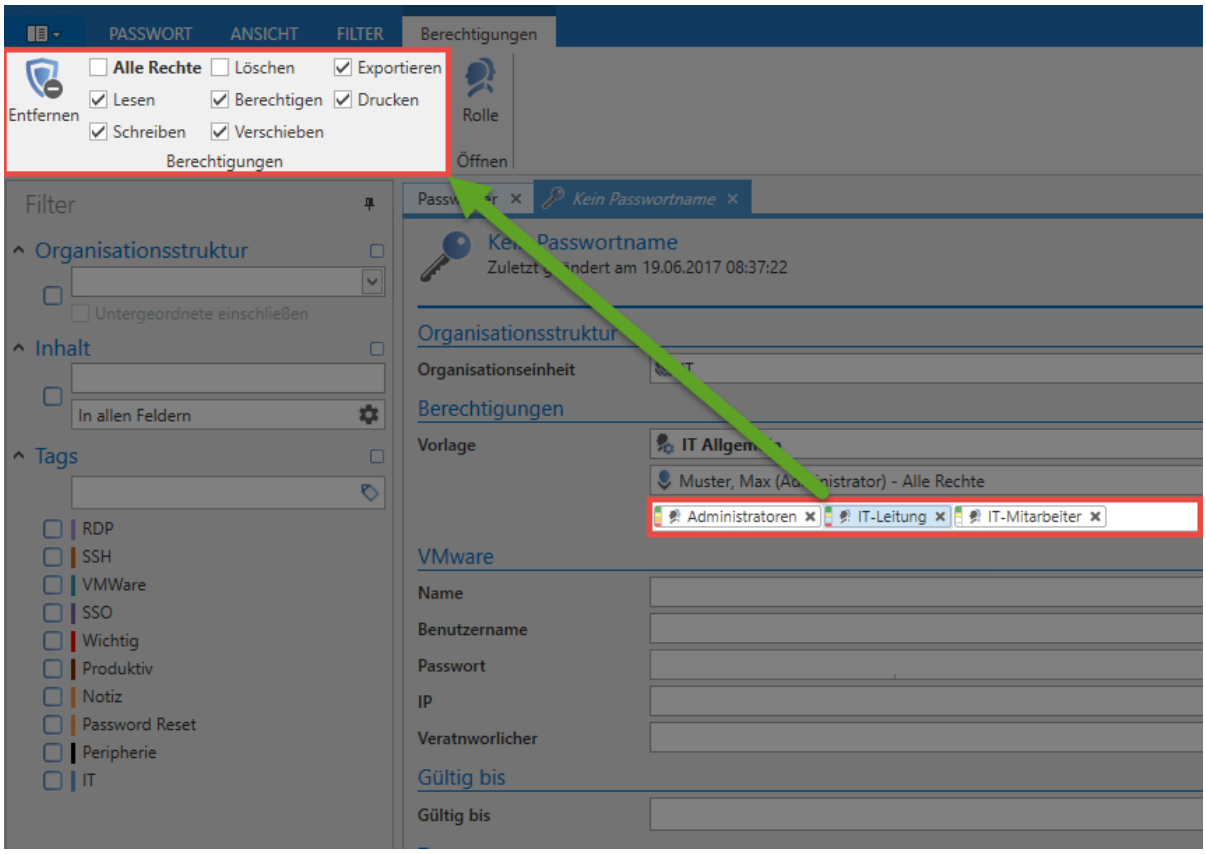

Der Zusammenhang ist offensichtlich. Es ist direkt einsehbar, dass durch das Auswählen der Organisationseinheit “IT” gemäß den in der Rechtevorlage konfigurierten Rechten die Rollen “IT-Leitung” wie auch die “Administratoren” berechtigt werden. **Ebenso werden die hinterlegten Tags “IT” und “Exchange” gesetzt**.

# Vorschau auf zu setzende Berechtigungen

Beim Einsatz von Rechtevorlagen sind über eine **Farbtabelle** die zu erteilenden Berechtigungen sehr schnell klassifizierbar. Die tatsächlichen Berechtigungen können wie gewohnt zusätzlich über die Ribbon eingesehen werden. Nachfolgend die Aufschlüsselung der Farben mit den zugehörigen Berechtigungen:

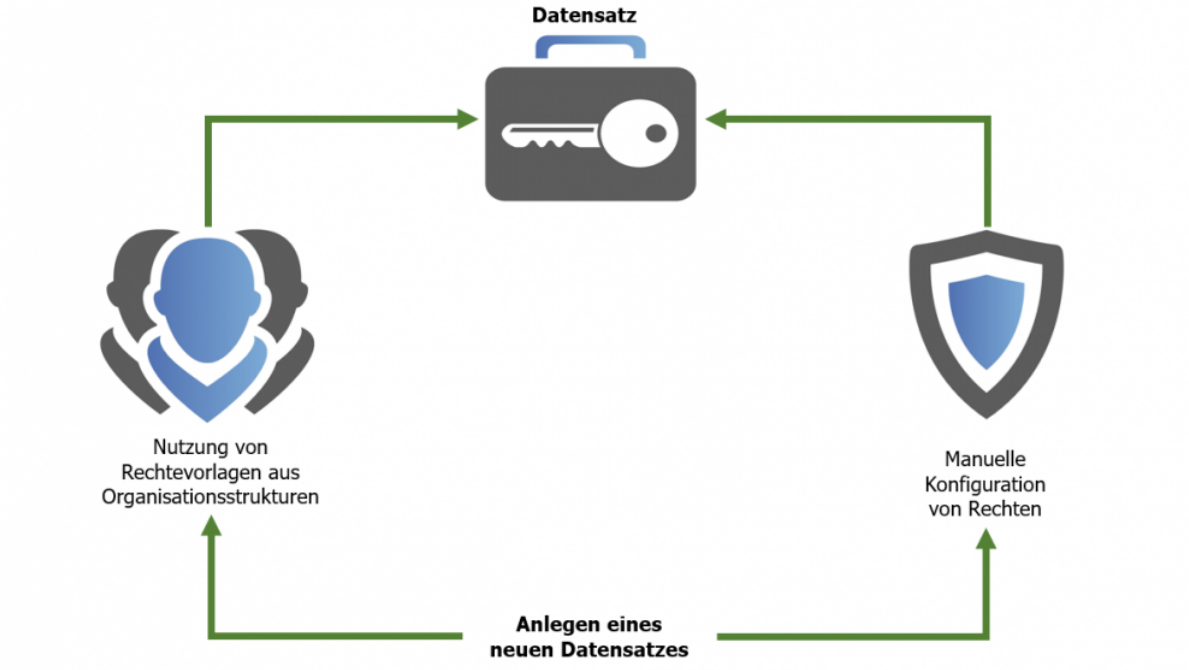
| Farbe | Berechtigung |
|---|---|
| Grün | Lesen |
| Gelb | Schreiben |
| Orange | Löschen |
| Rot | Berechtigen |

Darüber hinaus existieren noch weitere Rechte, welche jedoch nicht separat mit einer Farbe versehen werden. Ob die Rechte “Verschieben”, “Exportieren” und “Drucken” gesetzt sind oder nicht, kann direkt in der Übersicht in der Ribbon eingesehen werden. Es werden immer die Berechtigungen für die ausgewählte Rolle/Benutzer angezeigt – Im vorliegenden Fall für die Rolle “IT-Leitung”.




# Fazit

Das manuelle Setzen von Berechtigungen ermöglicht die Konfiguration von Rechten sowohl auf bestehende als auch auf neue Datensätze. Die Möglichkeit Rechte vorzudefinieren stellt hierzu eine sehr effiziente Alternative dar. Statt für jeden Datensatz Berechtigungen separat vergeben zu müssen, wird für jede Organisationsstruktur einmalig ein “Preset” definiert. Wurde dies durchgeführt reicht es zukünftig aus, dass lediglich die Organisationsstruktur beim Erstellen eines Datensatz ausgewählt wird. Die Berechtigung erfolgt dann automatisiert. Besonders vorteilhaft ist dieses Vorgehen dann, wenn Benutzer die Berechtigungen nicht selbst setzen sollen.




! Die Konfiguration von Berechtigungen kann wie beschrieben sowohl manuell als auch automatisch erfolgen. Will man einmal gesetzte Berechtigungen ändern, muss dies auf dem manuellen Weg erfolgen. Die Definition von Rechten im Nachhinein ist nicht möglich.

# Relevante Benutzerrechte

## Benutzerrechte für vordefinierte Rechte

Im Kapitel Benutzerrechte sind grundlegend alle Informationen zum Umgang mit Benutzerrechten erläutert. Dennoch soll nachfolgend auf die vier im Zusammenhang mit “Rechte vordefinieren” existierenden Benutzerrechte eingegangen werden.

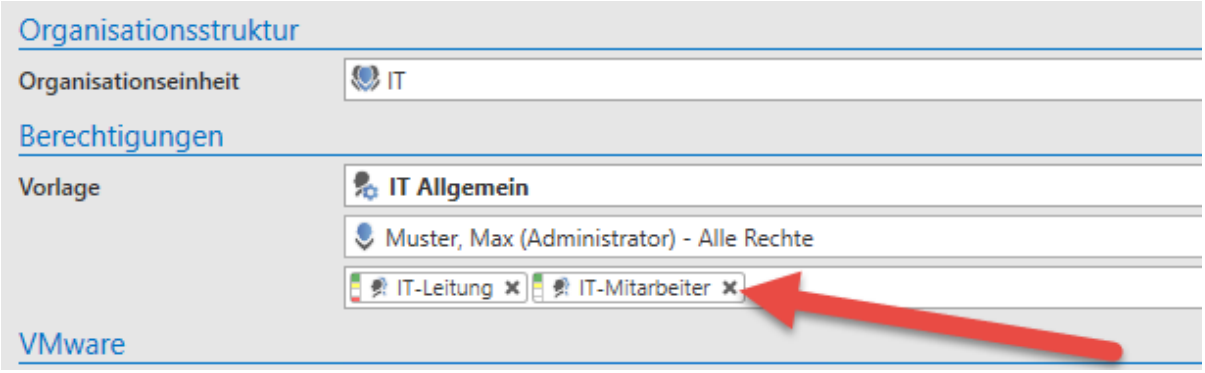
| Kategorie: Rechtevorlagen | | |
|---|---|---|
| Kann Standard-Rechtevorlage wechseln | Aktiviert | Global |
| Kann Rechtevorlagen verwalten | Aktiviert | Global |
| Kann Rechtevorlagen-Auswahl sehen | Aktiviert | Global |
| Kann Mitglieder aus Rechtevorlagen entfernen | Deaktiviert | Global |

- **Kann Standard-Rechtevorlagen wechseln:** Bei der Auswahl der Rechtevorlage können diverse Rechtevorlagegruppen ausgewählt werden. Um hier abweichend von der Standard-Vorlage andere Vorlagen auswählen zu können, benötigt man das Recht “Kann Standard-Rechtevorlagen wechseln”. Ohne dieses Recht ist man stets gezwungen, die Standard Vorlage zu nutzen.

- **Kann Rechtevorlagen verwalten:** Hat der Benutzer das Recht Rechtevorlagen zu verwalten, kann er die Verwaltung der Rechtevorlagen über den Button „Rechte vordefinieren“ öffnen. Für die vollständige Verwaltung der Rechtevorlagen einer Organisationseinheit werden die Rechte “Lesen” und “Berechtigen” auf die entsprechende Organisationseinheit benötigt.

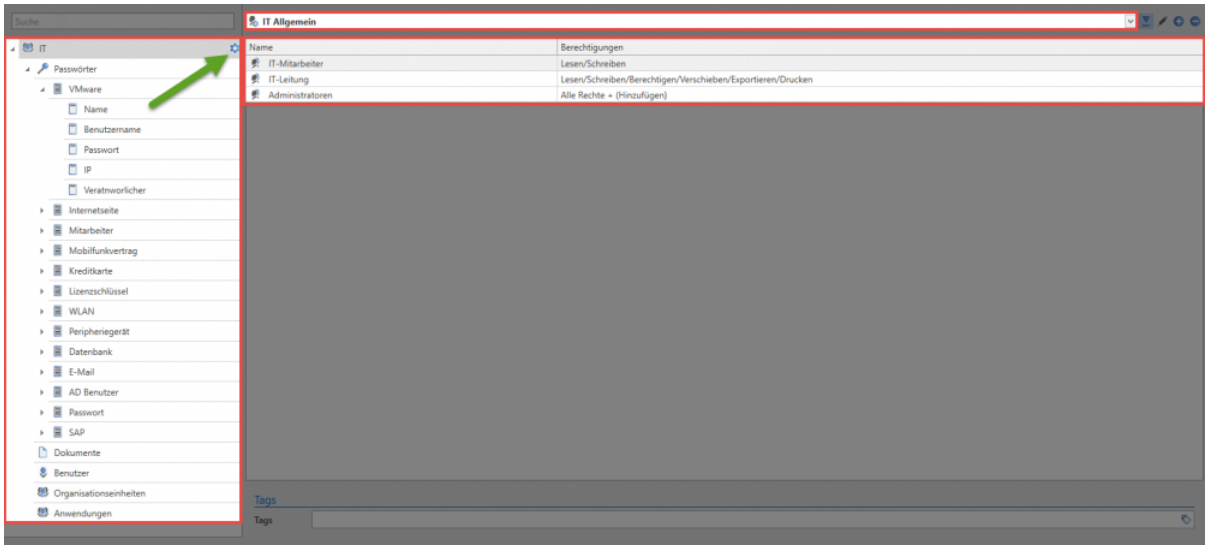
- **Kann Rechtevorlagen-Auswahl sehen:** Dieses Recht bestimmt, ob beim Erstellen neuer Datensätze die Rechtevorlagenauswahl angezeigt wird oder nicht. Ohne das Recht ist demnach nicht ersichtlich, für welche Rollen und Benutzer Benutzerrechte definiert werden.

- **Kann Mitglieder aus Rechtevorlagen entfernen:** Die innerhalb von Rechtevorlagen definierten Rollen können ohne dieses Recht nicht entfernt werden. Wenn man dieses Recht nicht gewährt, sind die in den Vorlagen definierten Rollen nun stets berechtigt auf Datensätze dieser Organisationsstruktur. Mit aktiviertem Benutzerrecht: Man kann Rollen nun über das x-Icon entfernen:



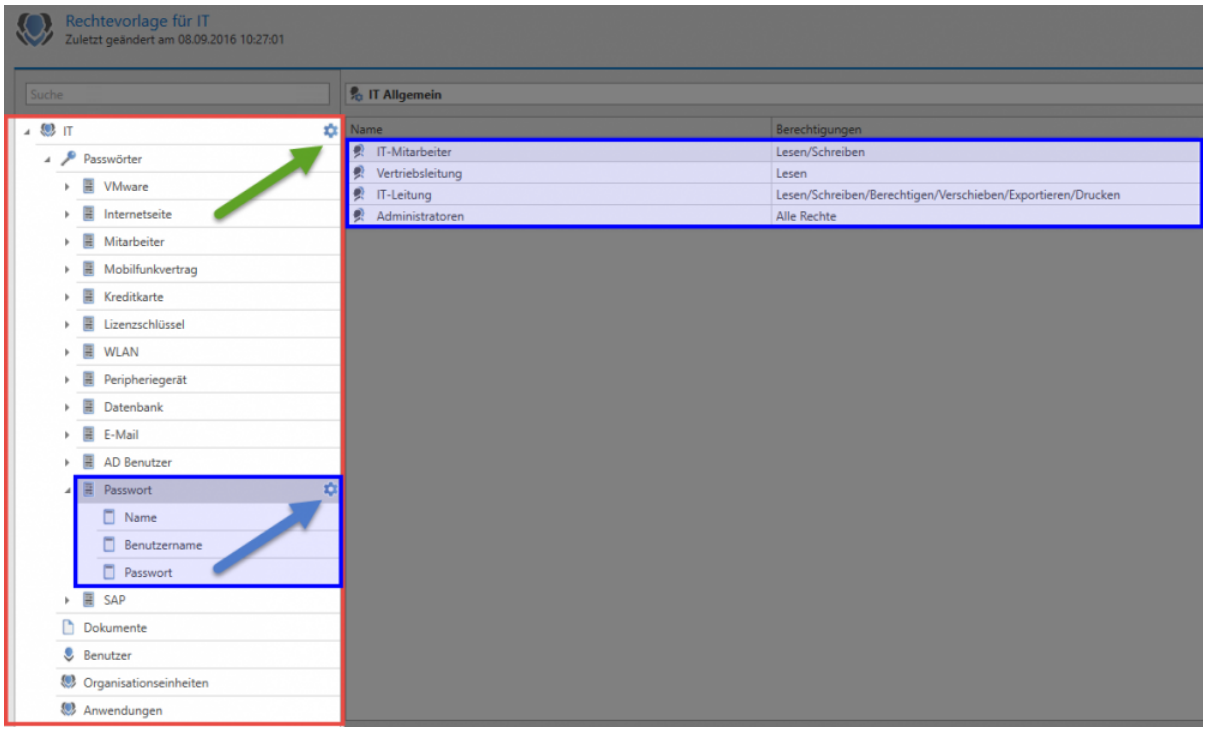
# Geltungsbereich vordefinierter Rechte

Generell werden alle für eine Organisationsstruktur vordefinierten Berechtigungen auf alle darunterliegenden Objekte angewandt. Diese können Passwörter, Formulare, Formularfelder Dokumente, Benutzer, Anwendungen oder auch andere, hierarchisch verschachtelte Organisationsstrukturen sein. Im folgenden Beispiel ist für die Organisationseinheit **IT** die Rechtevorlage **IT Allgemein** definiert.




Ist ein solches “Preset” definiert, erscheint in der jeweiligen Ebene das entsprechende Icon (= grüner Pfeil). Da unterhalb dieser Ebene keine weiteren Icons existieren bedeutet dies, dass das Preset für alle darunterliegenden Objekte ebenso gilt.

Im nachfolgenden Beispiel soll definiert werden, dass bei der Nutzung des Formulars “Passwort” zusätzlich zu den bisher berechtigten Rollen noch die Vertriebsleitung Leserecht besitzt.




Wie ersichtlich wird, behält für alle Objekte das Preset “IT Allgemein” seine Gültigkeit. Eine Ausnahme hierfür bildet das Formular “Passwort”, da für dieses ein eigenes Preset definiert (blauer Pfeil). Demnach werden alle mit dem Formular “Passwort” erstellten Datensätze wie definiert berechtigt (inkl. der Vertriebsleitung).

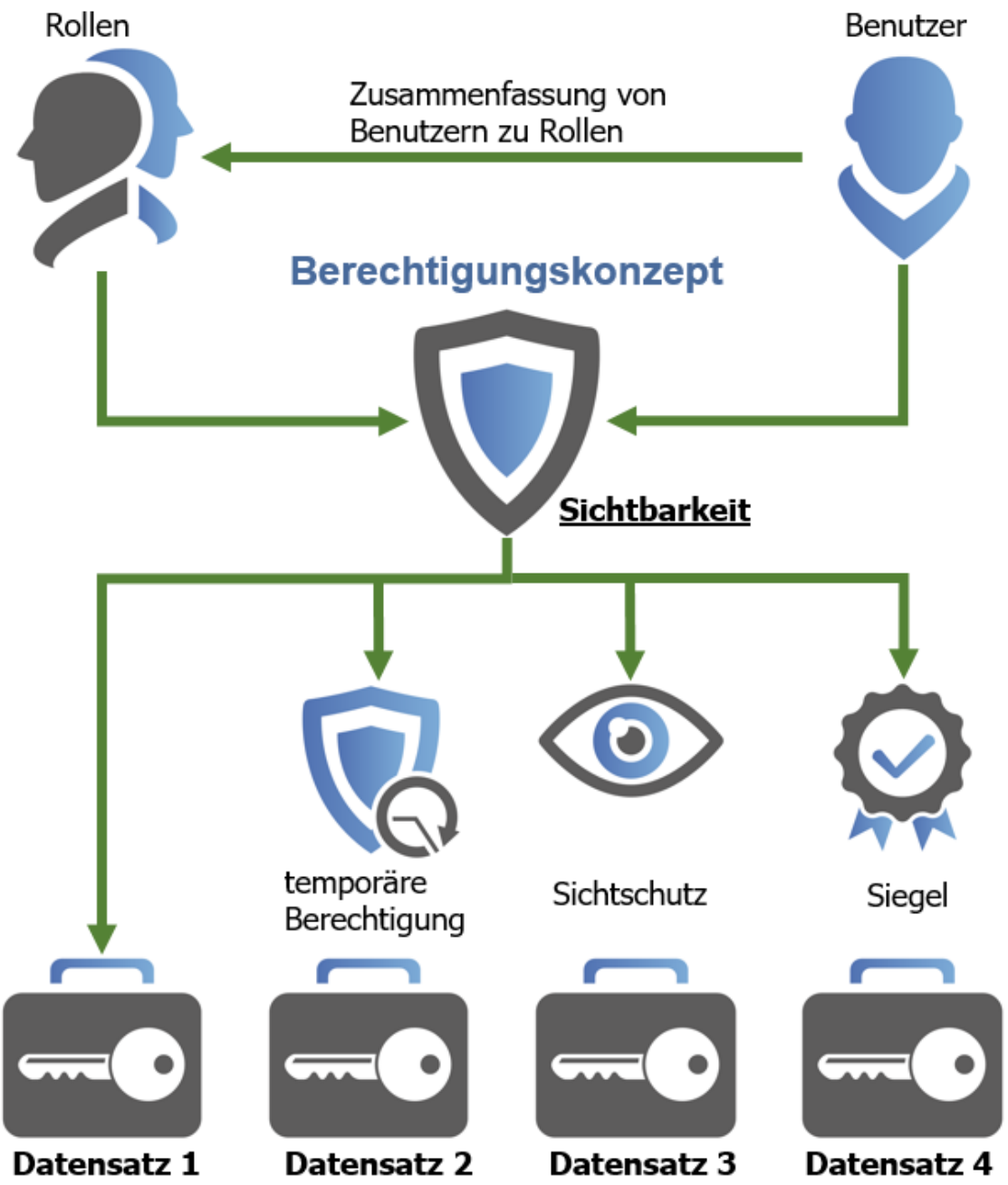
# Schutzmechanismen

## Was sind Schutzmechanismen?

Password Safe verfolgt als oberstes Ziel stets die Wahrung von Datensicherheit. Das **Berechtigungskonzept** stellt hierbei natürlich die wichtigste Komponente dar wenn es darum geht, Benutzer auf Daten im angedachten Ausmaß zu berechtigen. Konkret geht es hierbei um die Möglichkeit, bestimmte Informationen lediglich selektiv Mitarbeitern zur Verfügung zu stellen. Nichtsdestotrotz benötigt man über das Berechtigungskonzept hinaus noch weitere Schutzmechanismen, um komplexen Anforderungen gerecht zu werden.

- Die Sichtbarkeit wird nicht separat konfiguriert, sondern erfolgt direkt aus dem Berechtigungskonzept (Leserecht). Dennoch stellt diese einen wichtigen Baustein innerhalb der vorhandenen Schutzmechanismen dar, weshalb ihr ein separates Kapitel gewidmet wird.
- Durch die Konfiguration von temporären Berechtigungen gewährt man Benutzern oder Rollen zeitlich befristeten Zugriff auf Daten.
- Der Sichtschutz ermöglicht die Nutzung von Systemzugängen, ohne das Passwort Benutzern freigeben zu müssen. Der Wert des Passwortes bleibt stets verborgen.
- Um die Freigabe hochsensibler Zugangsdaten an ein Mehr-Augen-Prinzips zu binden, ist das Anbringen von Siegeln möglich. Die Konfiguration freigabeberechtigter Benutzer oder Rollen ist beliebig granular und stets an individuelle Anforderungen anpassbar.

In nachfolgender Grafik ist zusammenfassend die Eingliederung der vorhandenen Schutzmechanismen in das Berechtigungskonzept aufgeführt.




Im Zusammenspiel des Berechtigungskonzepts mit den Schutzmechanismen lassen sich quasi alle erdenklichen Szenarien abbilden. Es sei hierbei noch einmal erwähnt, dass das Berechtigungskonzept durch die Einschränkung der Sichtbarkeit auf Passwörter und Datensätze bereits ein sehr effektives Mittel ist. Dieses Konzept ist im Password Safe allgegenwärtig und soll nachfolgend in angemessenem Detail erläutert werden.

## Sichtbarkeit als Grundvoraussetzung

Es ist stets zu beachten, dass die **Sichtbarkeit** immer eine Grundvoraussetzung für das Anbringen weiterer Schutzmechanismen darstellt. Ein Datensatz, der einem Benutzer komplett vorenthalten wird (= kein Leserecht), kann selbstredend nicht mit weiteren Schutzmechanismen versehen werden.

Die Sichtbarkeit auf einen Datensatz ist stets die Grundvoraussetzung für das Anbringen weiterer Schutzmechanismen

## Kombination mehrerer Schutzmechanismen

Grundsätzlich existieren diverse Möglichkeiten bei der Verknüpfung der genannten Schutzmechanismen. Ein temporär gewährter Zugriff auf einen “sichtgeschützten” Datensatz ist genauso möglich, wie ein “sichtgeschützter” Datensatz, welcher zusätzlich durch ein Mehr-Augen-Prinzip gesichert wird. **Dennoch ist bei der Konfiguration zu beachten, dass temporäre Freigaben in Kombination mit Siegeln stets eine Gefahr darstellen**. Wenn für die Freigabe von Siegeln eine Zustimmung einer Person notwendig ist, welche nur temporäre Berechtigungen besitzt, besessen hat oder aber zukünftig besitzen wird, kann dies selbstverständlich mit konfigurierten Freigabekriterien kollidieren.

Die Kombination von Siegeln und temporären Freigaben ist nicht empfohlen, wenn freigabeberechtigte Benutzer lediglich temporär berechtigt sind.

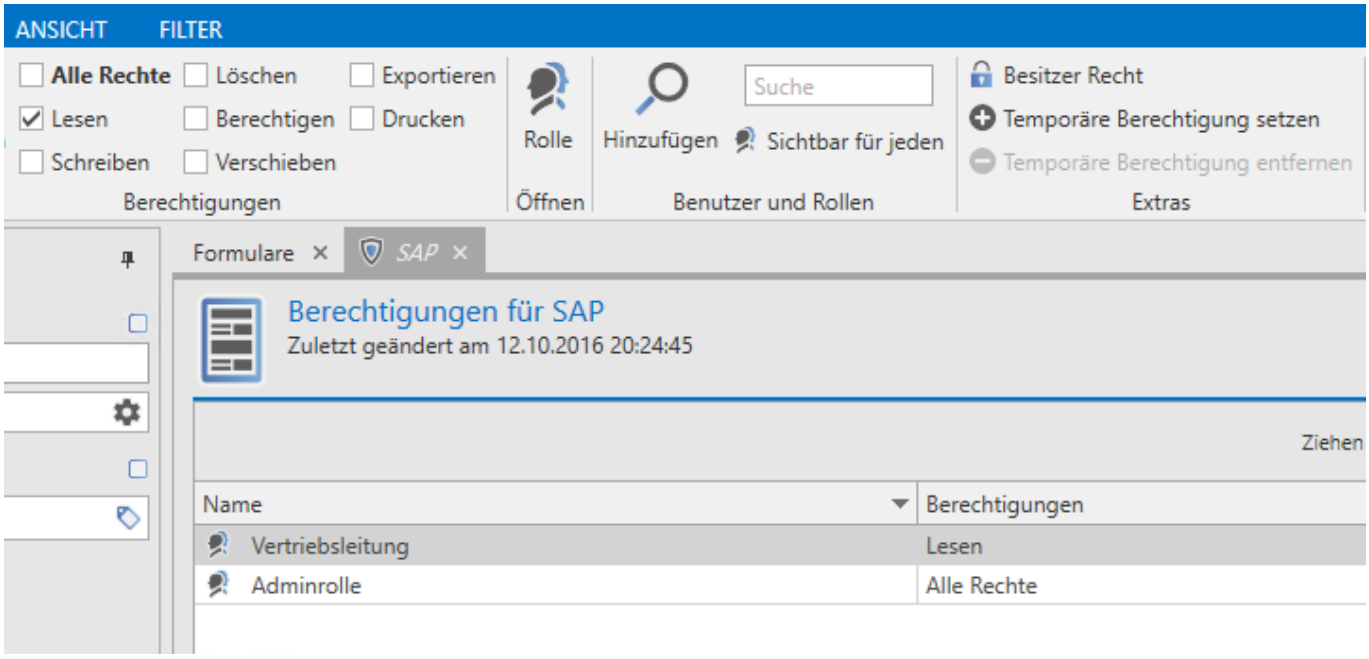
# Sichtbarkeit

## Sichtbarkeit von Daten

Die Nutzung des Filters stellt im Regelfall das Tor zur Anzeige der vorhandenen Datensätze dar. Dennoch ist der Aspekt deren Sichtbarkeit eng mit vorhandenen Berechtigungsstrukturen verwoben. Selbstverständlich sieht man nur stets jene Datensätze, auf die man auch mindestens lesend berechtigt ist. Dieses Dogma muss stets im Umgang bedacht werden. Tags unterliegen keinen Berechtigungen und können demnach stets als Filterkriterium herangezogen werden. Nichtsdestotrotz beinhaltet das gelieferte Ergebnis nur diejenigen Datensätze, auf die man selbst auch wirklich berechtigt ist. Ein schönes Beispiel hierfür ist das Tag “persönlicher Datensatz”. Jeder Benutzer kann seine eigenen Datensätze als persönlich markieren – dennoch wird jeder Benutzer natürlich nur seine eigenen persönlichen Datensätze finden können.

## Erschaffung autark arbeitender Arbeitsumgebungen

Die Möglichkeit, Sichtbarkeiten einzelner Objekte separat zu definieren, ist eine der der Besonderheiten innerhalb des Password Safe Berechtigungskonzeptes. Egal ob Datensätze, Dokumente, Organisationsstrukturen oder Rollen und Formulare: es kann stets definiert werden, ob ein Benutzer oder eine Rolle auf das Objekt Leserecht besitzt oder nicht. Jedes dieser Objekte kann über den Berechtigungsdialog in der Ribbon separat berechtigt werden. Dieser Ansatz ermöglicht die Erstellung von autark existierenden Abteilungen innerhalb einer Datenbank. Nachfolgend ist die Berechtigungsstruktur des Formulars SAP einsehbar. Demnach können aktuell lediglich die Vertriebsleitung und Administratoren neue Datensätze vom Typ SAP erstellen.



Grundsätzlich kann auf diese Art und Weise jede Abteilung eigenständig Formulare nutzen, Passwörter erstellen und Hierarchien verwalten. Besonders in sehr sensiblen Unternehmensbereichen ist eine derartige Abschottung oftmals erforderlich und auch erwünscht.

> Eine ebenso von Password Safe unterstütze **Alternative** wäre es, für jede Abteilung eine eigene MSSQL-Datenbank zu erstellen. Die physikalische Trennung ist jedoch gegenüber der eingangs erwähnten, auf Berechtigungen und Sichtbarkeit basierten Trennung der Daten deutlich verwaltungsintensiver.

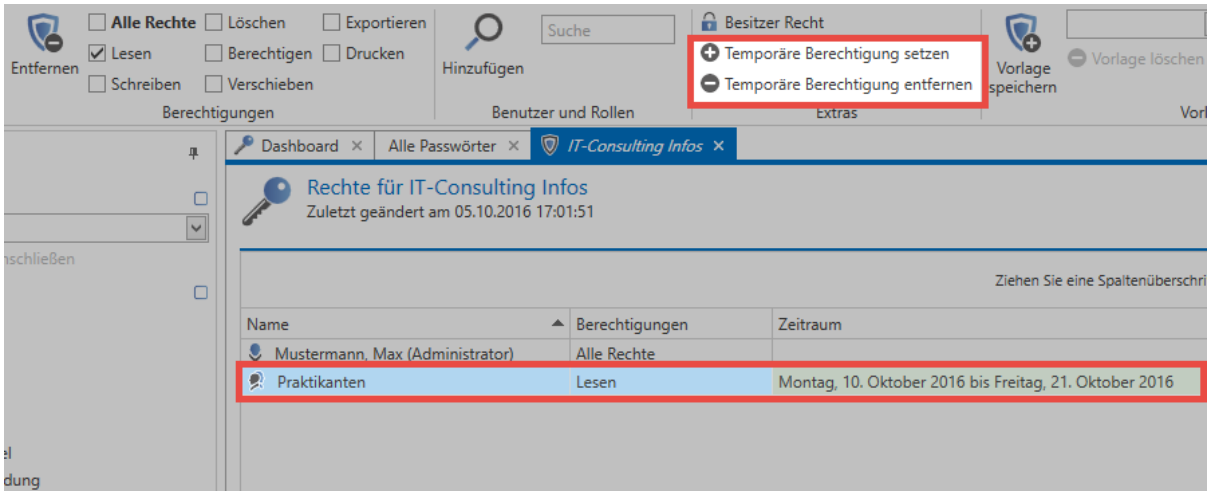
# Temporäre Berechtigungen

## Was sind temporäre Berechtigungen?

Bis dato wurden nur Berechtigungen behandelt, die zeitlich unbefristet waren. Eine gewährte Freigabe kann jedoch auch im Vorfeld mit einer zeitlichen Einschränkung versehen werden. Im Unternehmen nur für begrenzte Zeit tätige Benutzer, wie z.B. Praktikanten oder Werksstudenten, sind hier adäquate Anwendungsfälle.

### Konfiguration

Bei der Konfiguration der Berechtigungen auf Datensätze kann für jede Rolle eine temporäre Freigabe definiert werden. Hierbei wird das Startdatum wie auch das Enddatum gewählt. Gestartet wird die Konfiguration über den Bereich **Extras** in der Ribbon.




Im vorliegenden Beispiel wurde der Rolle “Praktikanten” für zwei Wochen Leseberechtigung auf einen Datensatz gewährt.

### Farbgebung

Die in der Spalte “Zeitraum” hinterlegte Farbe gibt Aufschluss über den derzeitigen Status der gewährten Berechtigung:

- **Braun:** Die temporäre Berechtigung ist konfiguriert, jedoch noch inaktiv. Der gewählte Zeitraum liegt demnach in der Zukunft.
- **Grün:** Die temporäre Berechtigung ist aktiv
- **Rot:** Der Zeitraum der temporären Berechtigung ist bereits abgelaufen, liegt demnach in der Vergangenheit

Die Vergabe von temporären Berechtigungen kann auch auf mehrere Rollen und Benutzer gleichzeitig angewandt werden. Die Mehrfachauswahl von Benutzer und Rollen erfolgt wie gehabt über Strg/Shift + linke Maustaste!

## Besonderheiten beim Berechtigungssystem

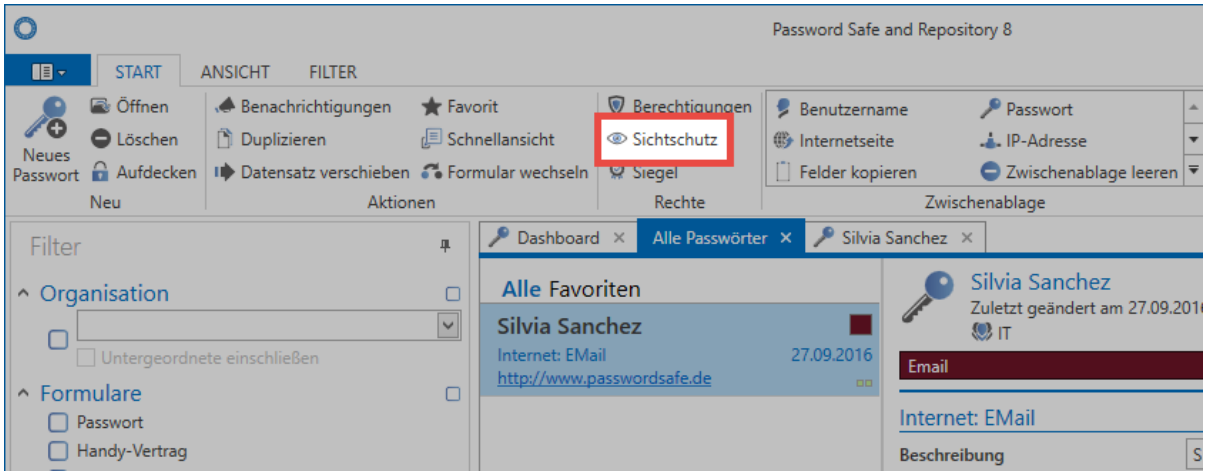
Designbedingt besitzen temporäre Berechtigungen viel Potential für Fehlkonfigurationen. Denkbar sind Konstellationen, bei denen der einzige Benutzer mit allen Rechten lediglich temporär berechtigt ist. Wenn diese Berechtigung dann abläuft, existiert kein voll berechtigter Benutzer mehr. Um diesem vorzubeugen, werden temporär berechtigte Benutzer anders gehandhabt.

Es muss immer mindestens ein Benutzer existieren, welcher das Recht “Berechtigen” auf einen Datensatz besitzt, der nicht lediglich temporär berechtigt ist.

# Sichtschutz

## Was ist der Sichtschutz?

Die sichersten Passwörter sind diejenigen, die man nicht kennt. Genau diesen Ansatz verfolgt der Sichtschutz. Er verhindert, dass das Passwort aufgedeckt werden kann, ermöglicht jedoch trotzdem die Nutzung über automatische Eintragungen. Angebracht werden kann dieser über den gleichnamigen Button in der Ribbon.




### Benötigte Berechtigungen

Analog zur Siegelkonfiguration ist das Recht **Berechtigen** auf den Datensatz Voraussetzung, um den Sichtschutz anbringen, bzw. wieder entfernen zu können. Benutzer, welche auf einen Datensatz das Recht **Berechtigen** besitzen, können nach Anbringen des Sichtschutzes den Datensatz weiterhin ohne Einschränkungen nutzen. Sichtschutz gilt demnach nur für Benutzer ohne genanntes Recht.

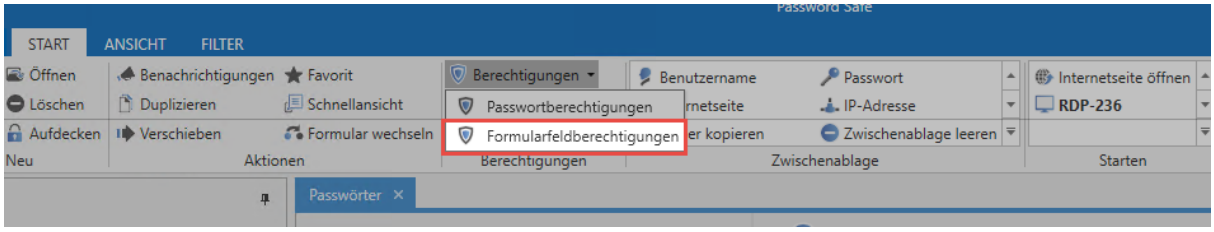
> Sichtschutz kann nur auf Datensätze mit vorhandenem Passwort angewendet werden!

## Anbringen des Sichtschutzes

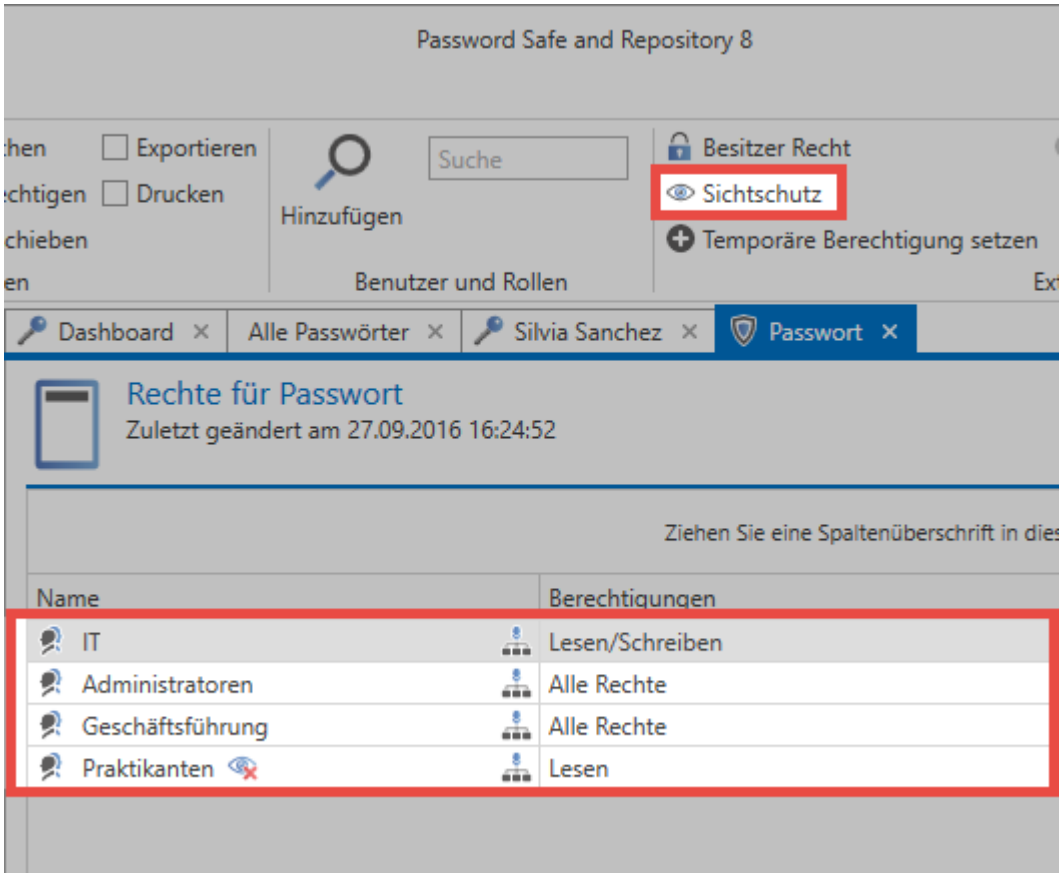
Über das Icon in der Ribbon können Berechtigte den Sichtschutz nach einer Sicherheitsabfrage anbringen. Standardmäßig gilt der Sichtschutz für all diejenigen, welche mindestens Leseberechtigung besitzen, jedoch nicht das Recht **Berechtigen**.

### Sichtschutz über Formularfeldberechtigungen

Alternativ ist das Anbringen des Sichtschutzes ebenso über die Formularfeldberechtigungen möglich. In der Detailansicht eines Datensatzes existiert hierfür ein separater Button in der Ribbon. Es ist zu beachten, dass das Passwortfeld markiert sein muss.




Die Besonderheit beim Setzen oder Bearbeiten des Sichtschutzes über die Formularfeldberechtigungen ist, dass man dort individuell entscheiden kann, für wen der Sichtschutz gelten soll. Im folgenden Beispiel wurde dementsprechend der Sichtschutz nur gegenüber der Rolle “Praktikanten* definiert, obwohl die Rolle “IT” das Recht **Berechtigen** ebenso nicht besitzt. Neben dem Namen der Rolle oder des Benutzers ist mit dem Icon symbolisiert, dass für Praktikanten der Sichtschutz gilt.




Über das Icon in der Ribbon wird Sichtschutz auf alle Benutzer angewandt, welche Leseberechtigung auf den Datensatz besitzen, jedoch nicht das Recht **Berechtigen**. Will

man genauer definieren, für wen der Sichtschutz gelten soll, ist dies zusätzlich über die **Formularfeldberechtigungen** möglich.

# Siegel

## Was sind Siegel?

Passwörter werden durch das Berechtigungskonzept selektiv den verschiedenen Benutzergruppen zur Verfügung gestellt. Dennoch existieren viele Szenarien, bei denen die Einsicht und Nutzung eines Datensatzes an eine im Vorfeld gewährte Freigabe gekoppelt sein soll. In diesem Zusammenhang stellt das Siegel einen effektiven Schutzmechanismus dar. Dieses Mehr-Augen-Prinzip schützt Passwörter, indem es diese durch granular definierbare Freigabemechanismen absichert. Will man ein Passwort einsehen, muss dies erst angefordert und freigegeben werden. Die erfolgte Freigabe kann auch temporärer Natur sein.

### Benötigte Berechtigungen

Um Siegel anlegen zu können wird zwingend das Recht **“Berechtigen”** auf den Datensatz benötigt. Darüber hinaus benötigt man Leserecht auf alle Benutzer und Rollen, welche im Siegel enthalten sind. Die exakte Konfiguration von Sichtbarkeit und Berechtigungen auf Datensätze sind im Kapitel Berechtigungskonzept exakt aufgeschlüsselt.

## Was wird genau versiegelt?

Auch bei versiegelten Datensätzen sind nicht alle Felder versiegelt. Dies trifft lediglich auf die schützenswerten Passwörter zu. Technisch gesehen wird nicht das Passwort selbst versiegelt. Es ist das Recht, ein Passwortfeld einzusehen, welches durch ein Siegel geschützt wird. Dies ermöglicht filigranste Konfigurationen, bei denen die eine Gruppe das Passwort ohne Einschränkungen benutzen kann, die andere Benutzergruppe jedoch das Passwort versiegelt vorfindet. Der Assistent unterstützt Benutzer beim Anbringen von Siegeln sowie der zukünftigen Pflege.

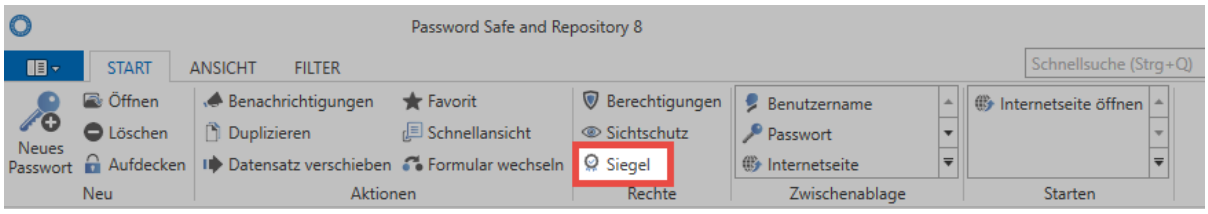
! Versiegelt wird niemals der komplette Datensatz! Lediglich das Recht, welches die Sicht auf ein Passwort gewährt, wird durch ein Siegel geschützt.

! Nur Datensätze mit einem Passwort können versiegelt werden!

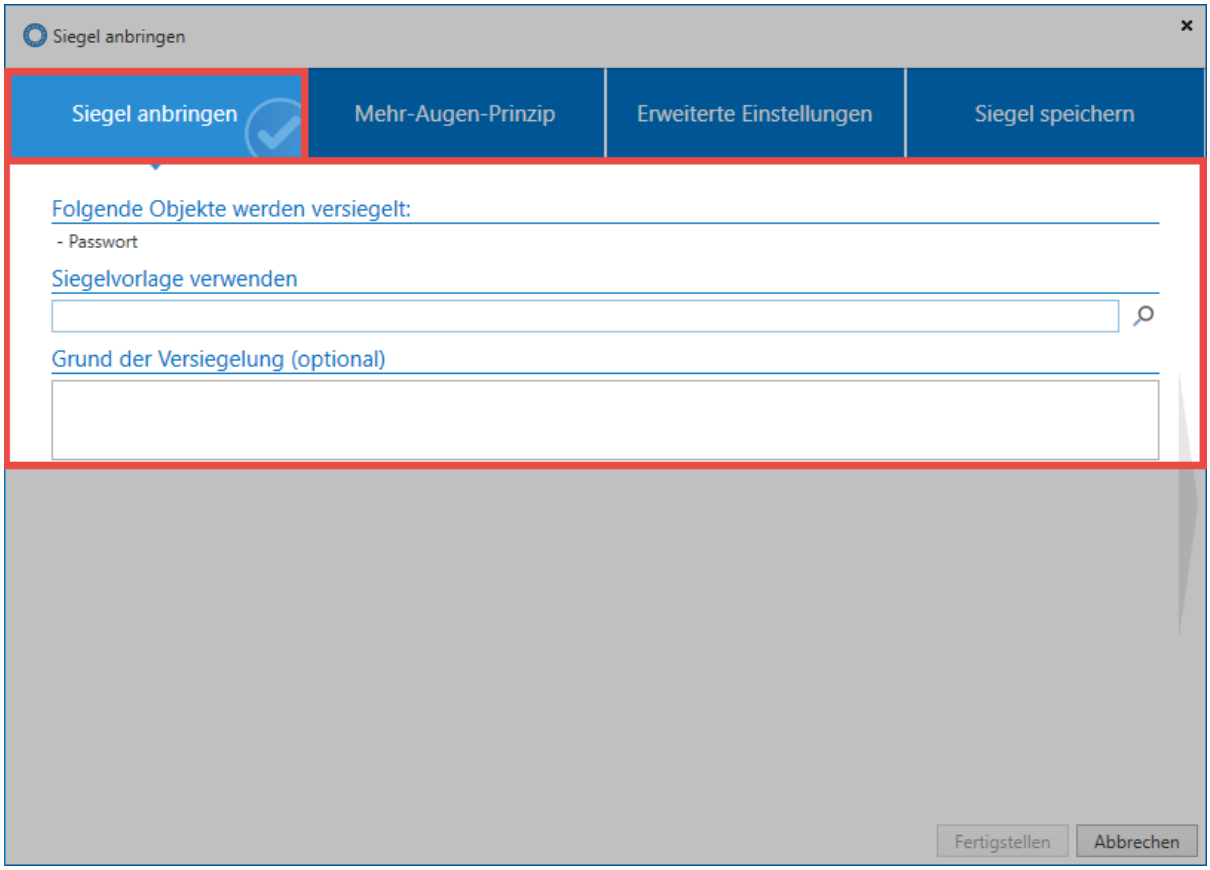
## Siegelassistent

Sämtliche Siegel-Konfigurationen werden im Assistenten vorgenommen. Sowohl das Anbringen von neuen Siegeln als auch das Bearbeiten und Löschen sind hier möglich. Auch der aktuelle Zustand eines Siegels ist in einer Übersicht einsehbar, welche ebenso über den Button in der Ribbon erreicht wird.

Beim Öffnen des Siegelassistenten über die Ribbon erscheint bei unversiegelten Datensätzen der Assistent, welcher in **vier Schritten** durch die Konfiguration des Siegels leitet.



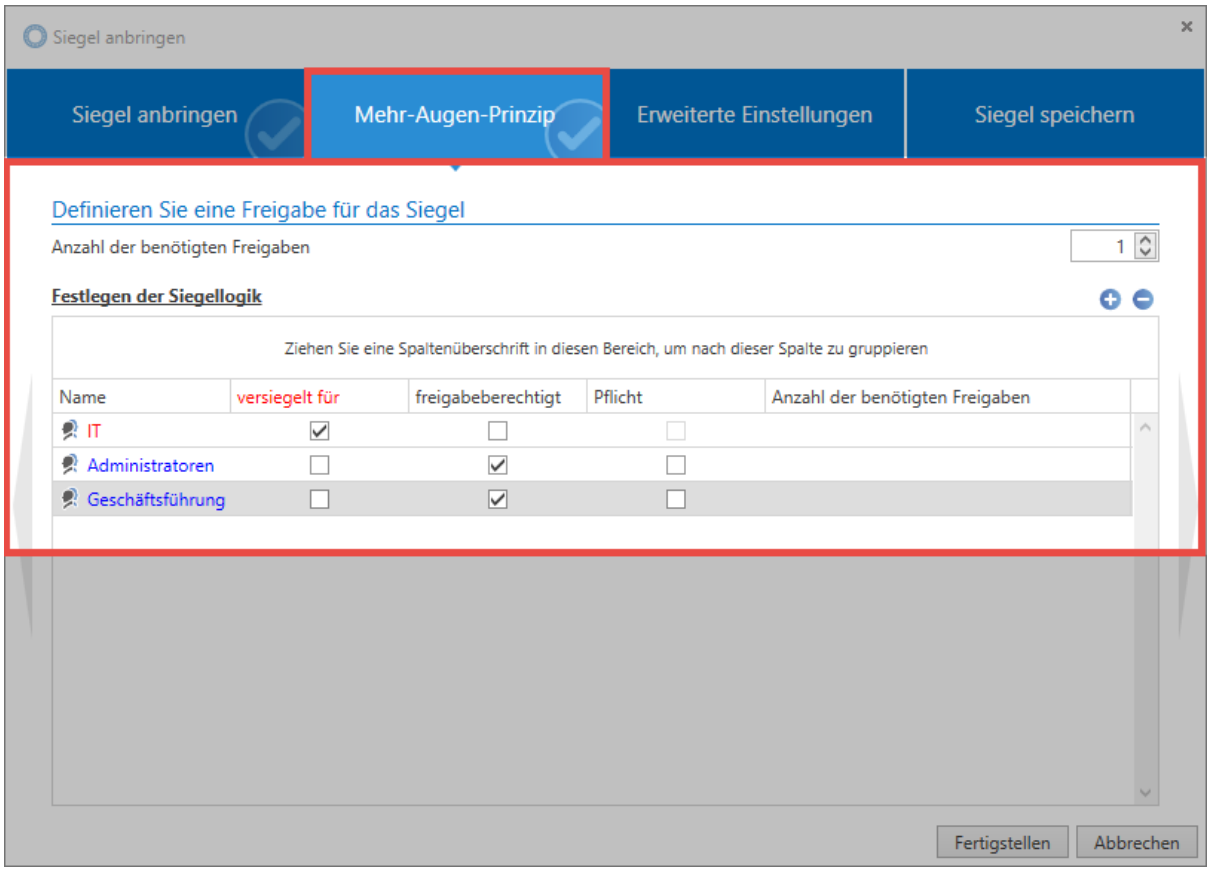

## 1. Siegel anbringen




Eingangs werden alle Objekte angezeigt, welche versiegelt werden. Dies können je nach Datensatz eines, oder auch mehrere sein. Ebenso ist die Nutzung bereits bestehender Siegelvorlagen möglich. Optional kann für jedes Siegel eine Begründung eingegeben werden.

## 2. Mehr-Augen-Prinzip

Die Siegellogik ist der elementarste Bestandteil dieses Schutzmechanismus. Hier wird definiert, welche Benutzer oder Rollen zukünftig den Datensatz versiegelt vorfinden, bzw. hierfür freigabeberechtigt sein sollen. Für all diejenige, für die der Datensatz versiegelt sein soll, werden rot dargestellt, alle Freigabeberechtigten blau.



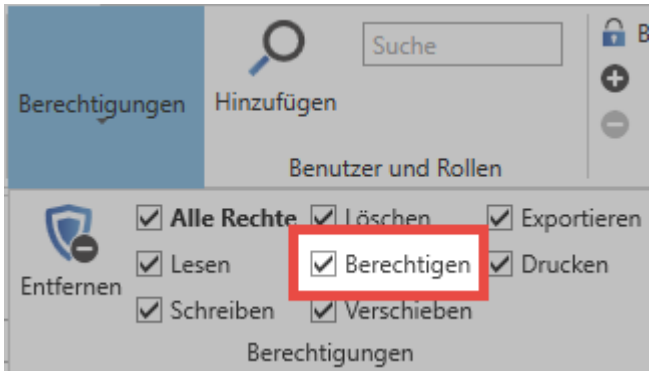

> Alle Benutzer und Rollen, für die der Datensatz nicht versiegelt ist, und die auch nicht freigabeberechtigt sind, werden grün dargestellt. Diese können den Datensatz unabhängig vom Siegel nutzen.

Um nicht jedwede Konfiguration manuell durchführen zu müssen, werden Rollen und Benutzer direkt aus den Berechtigungen des Datensatzes übernommen. Zum Vergleich die **“Berechtigungen”** für den Datensatz (einsehbar über die Ribbon).

Die Zusammenhänge sind offensichtlich. Es ist in der Regel gewünscht, dass Vorgesetzte die Freigaben für deren Mitarbeiter vergeben sollen. Demnach folgt auch die Siegellogik den vorhandenen Berechtigungen. Das folgende **Schema** wird angewandt:

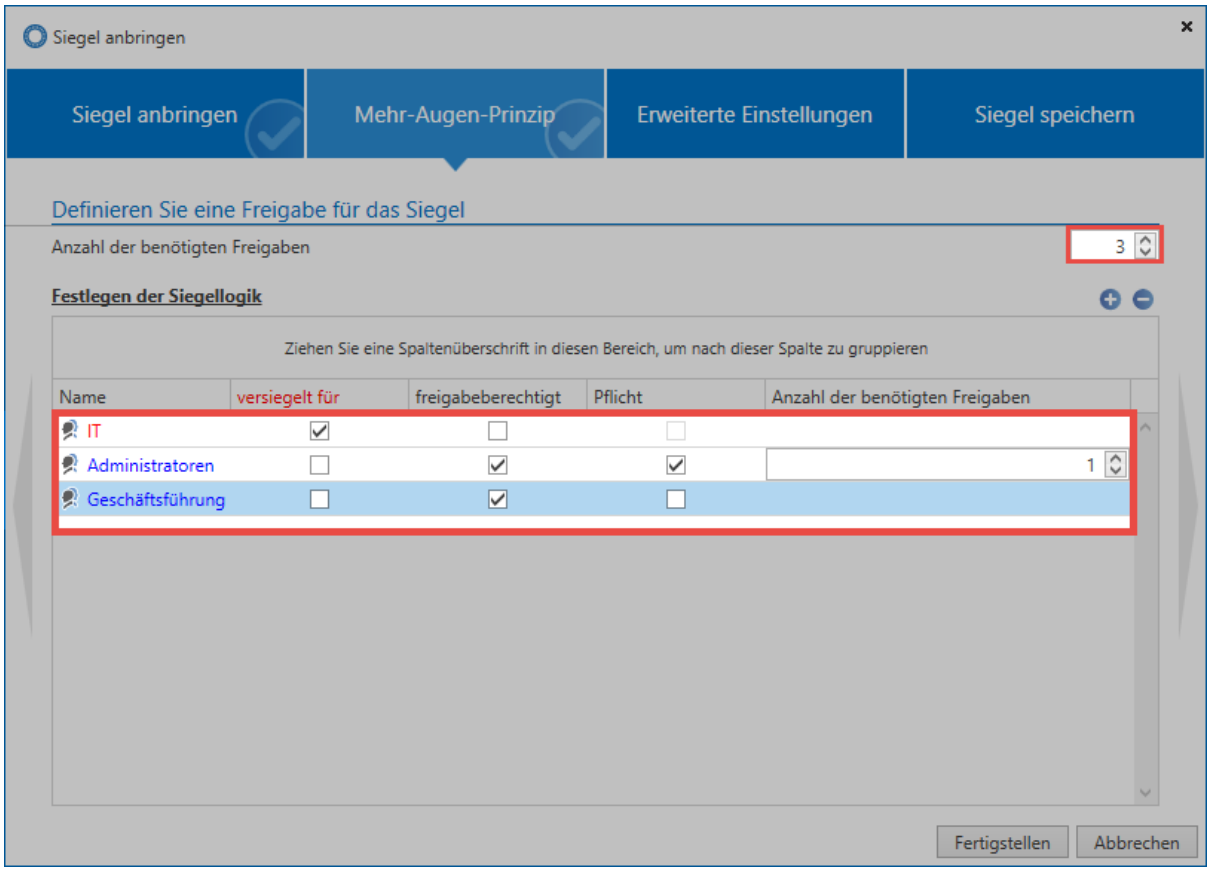
> Alle Benutzer und Rollen, welche das Recht “Berechtigen” auf den Datensatz besitzen, sind per default für das Siegel **“freigabeberechtigt”**. Alle Benutzer und Rollen, welche das Recht “Berechtigen” auf den Datensatz nicht besitzen, werden direkt in der Spalte **“versiegelt für”** übernommen.

Hier ein genauerer Blick auf die Berechtigungen der Rolle **Administratoren** auf den Datensatz:

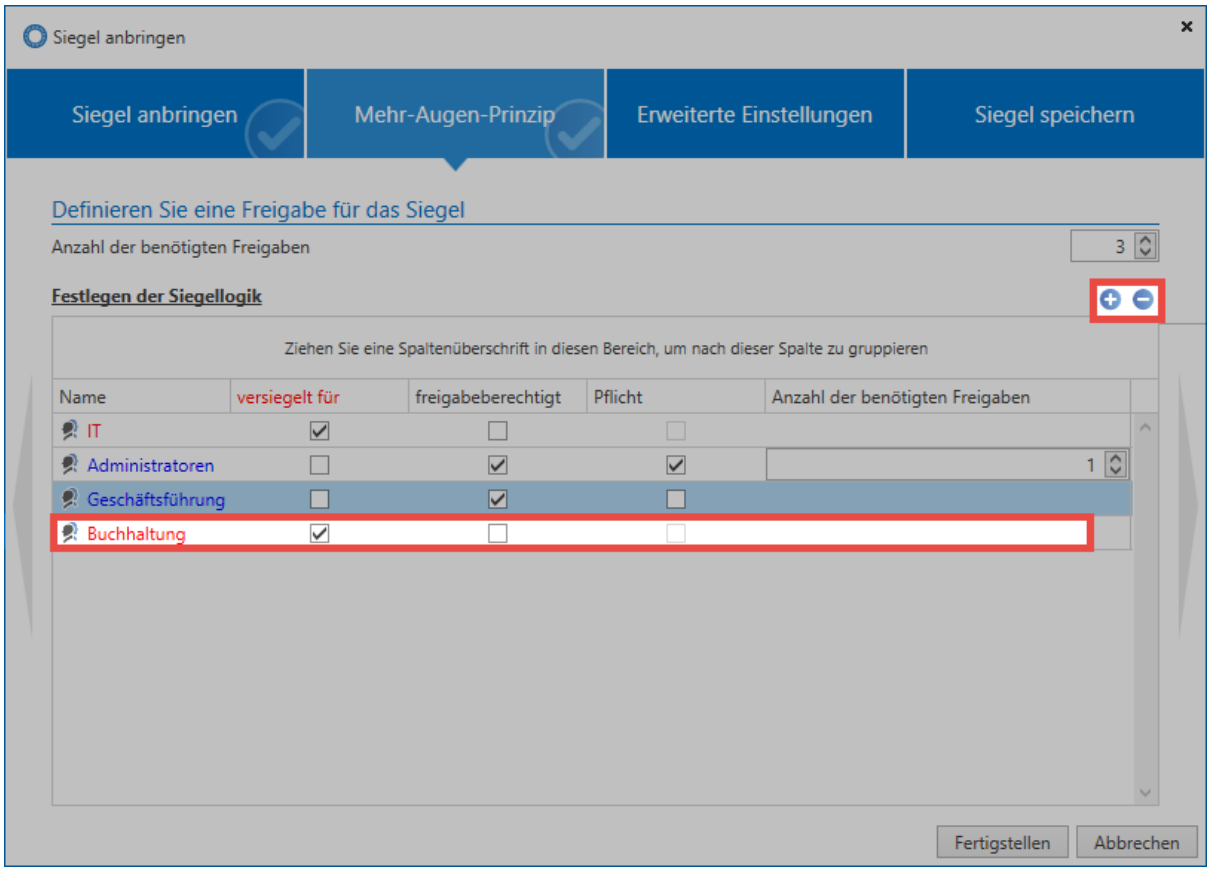



### Anpassungen an der Siegellogik

Obwohl standardmäßig die bereits existierenden Berechtigungen als Grundlage für das Versiegelungskonzept herangezogen werden, können diese natürlich angepasst werden. Die Anzahl der generell benötigten Freigaben ist genauso konfigurierbar wie auch die benötigte Anzahl an Freigaben aus einer Rolle. Im folgenden Beispiel wurde das Siegel insofern erweitert, dass insgesamt drei Freigaben notwendig sind, um eine Freigabe zu erhalten **(Mehr-Augen-Prinzip)**. Die Rolle der Administratoren wurde in der Pflichtspalte markiert. Das bedeutet, dass diese mindestens eine Freigabe erteilen muss. Zusammengefasst: Es müssen insgesamt drei Freigaben erfolgen, wobei die Gruppe der Administratoren mindestens eine Freigabe erteilen muss.




Um nicht nur abhängig von bestehenden Berechtigungen auf den Datensatz zu sein, können gerne auch weitere Benutzer dem Siegel hinzugefügt werden. Nachfolgend wurde die Rolle Buchhaltung unter “versiegelt für” hinzugefügt.

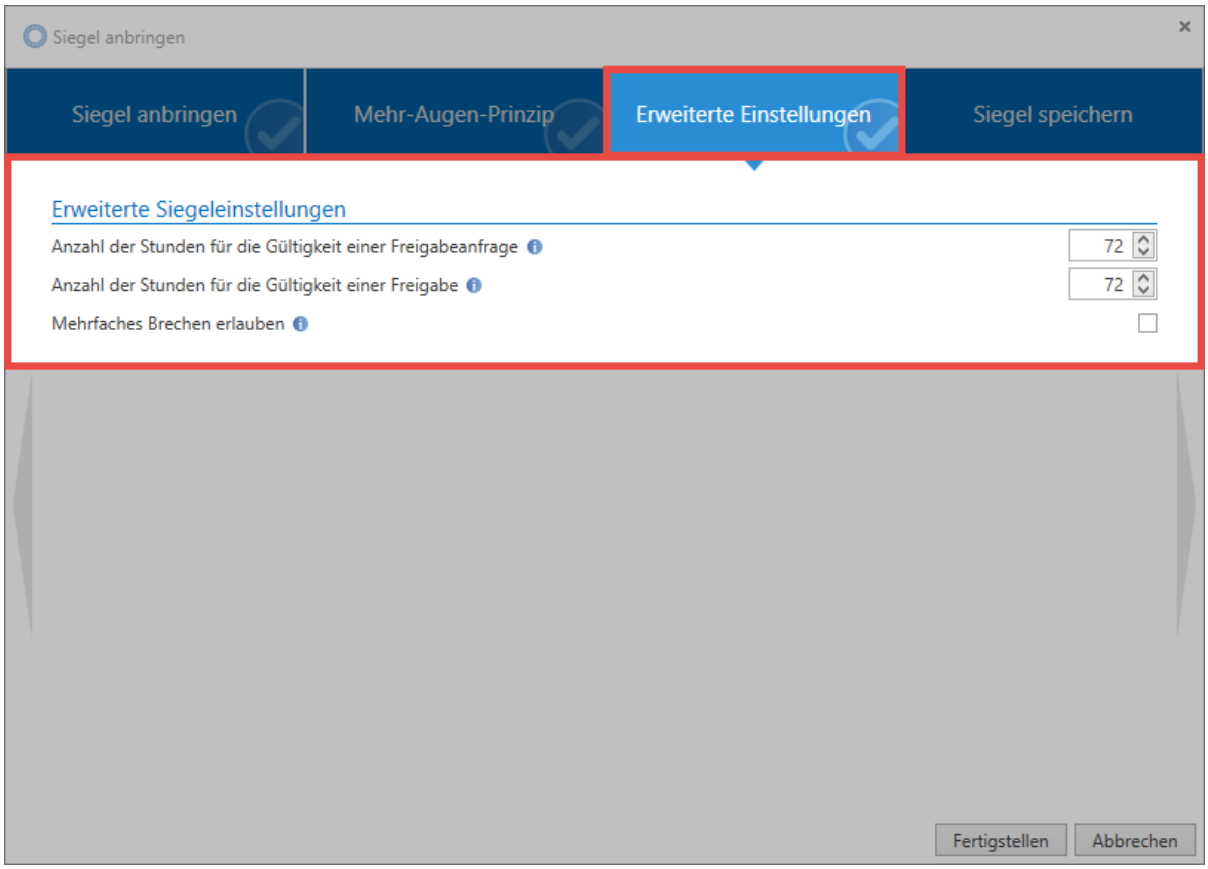



Wird eine Rolle oder ein Benutzer einem Siegel hinzugefügt, erhalten diese Nutzer gemäß der im Siegel gewährten Berechtigung auch Berechtigungen auf den Datensatz. Eine Rolle, die unter “versiegelt für” hinzugefügt wird, erhält das Recht “Lesen” auf den Datensatz. Beim Hinzufügen von Freigabeberechtigungen erhalten diese fortan die Rechte “Lesen, Schreiben, Löschen und Berechtigen”.

Alle Rollen, welche einmal dem Siegel hinzugefügt wurden, können nicht mehr über die Siegellogik entfernt werden. Dies ist nur noch direkt über die Berechtigungen des Datensatzes möglich!

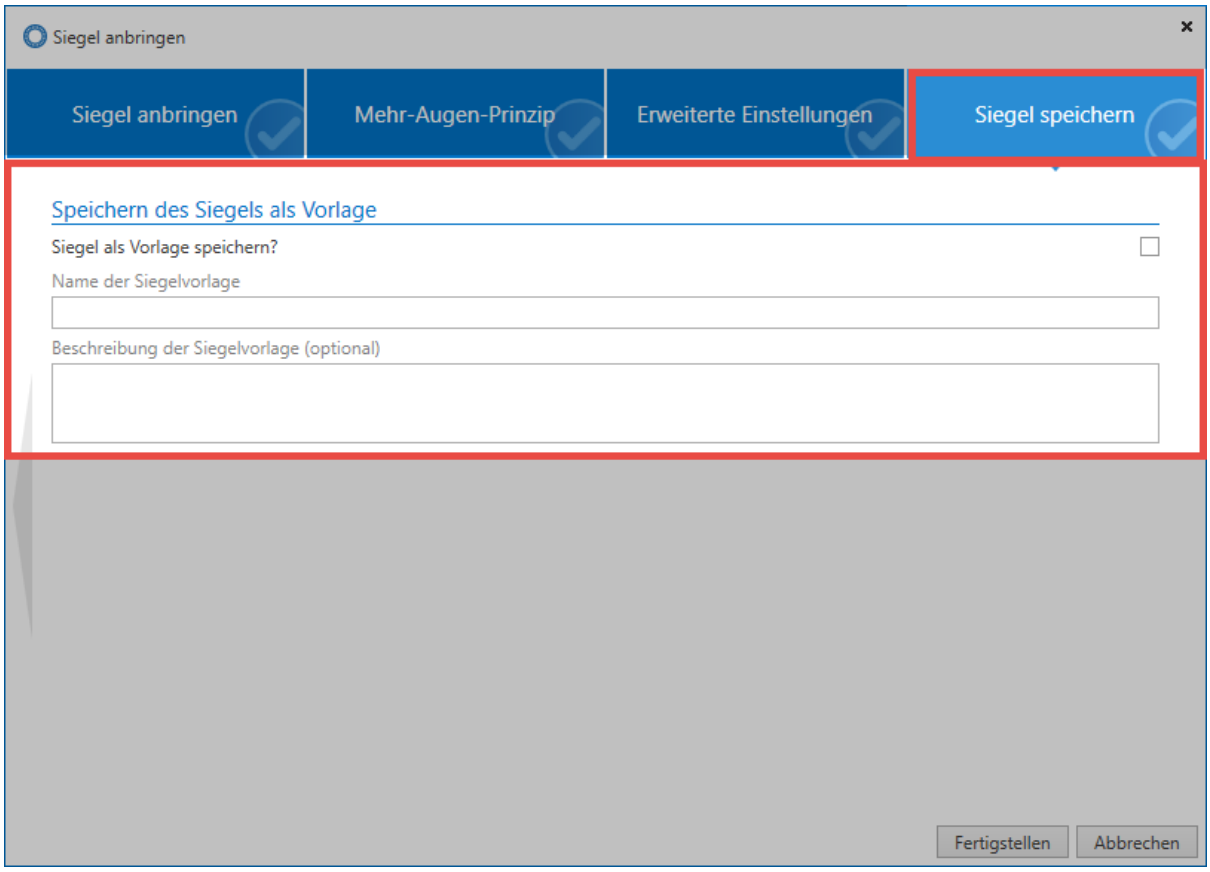
### 3. Erweiterte Einstellungen

Erweiterte Siegeleinstellungen ermöglichen die weitere Anpassung des Mehr-Augen-Prinzips. Sowohl die zeitliche Gültigkeit einer Freigabeanfrage, wie auch einer gewährten Freigabe kann konfiguriert werden. Mehrfachbruch definiert, ob nach dem Brechen eines Siegels durch einen User auch weitere User dieses noch brechen dürfen.




### 4. Siegel Speichern

Vor dem Abschließen des Assistenten besteht die Möglichkeit, die vorgenommene Konfiguration direkt in Form einer Vorlage abzuspeichern und zukünftig weiter zu verwenden. Siegelvorlagen können zwecks Übersicht optional mit einer Beschreibung versehen werden.




# Zusammenfassung

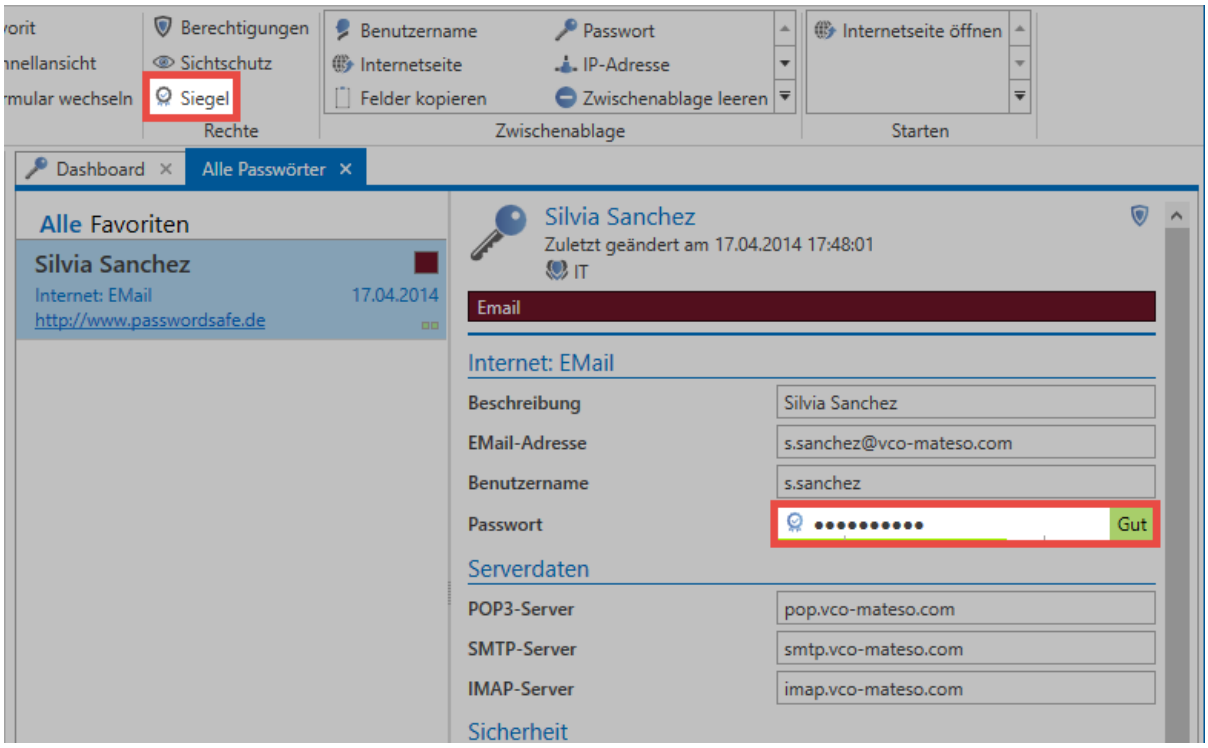
Die auf dem Datensatz bereits vorhandenen Rechte stellen die Basis für beliebig komplexe Siegelkonfigurationen. Es ist somit frei definierbar, welche Benutzer vor der Einsicht auf das Passwort einen Freigabemechanismus durchlaufen müssen. Auch die Rollen, welche Freigaben erteilen dürfen, sind frei definierbar. Eine stets zugängliche Siegelübersicht ermöglicht allen Freigabeberechtigten die Einsicht auf den aktuellen Zustand der Siegel. Das Kapitel Freigabemechanismus behandelt detailliert die einzelnen Schritte von der ersten Freigabeanfrage bis hin zur endgültigen Erteilung einer Freigabe.

- Siegelübersicht
- Freigabemechanismus

# Siegelübersicht

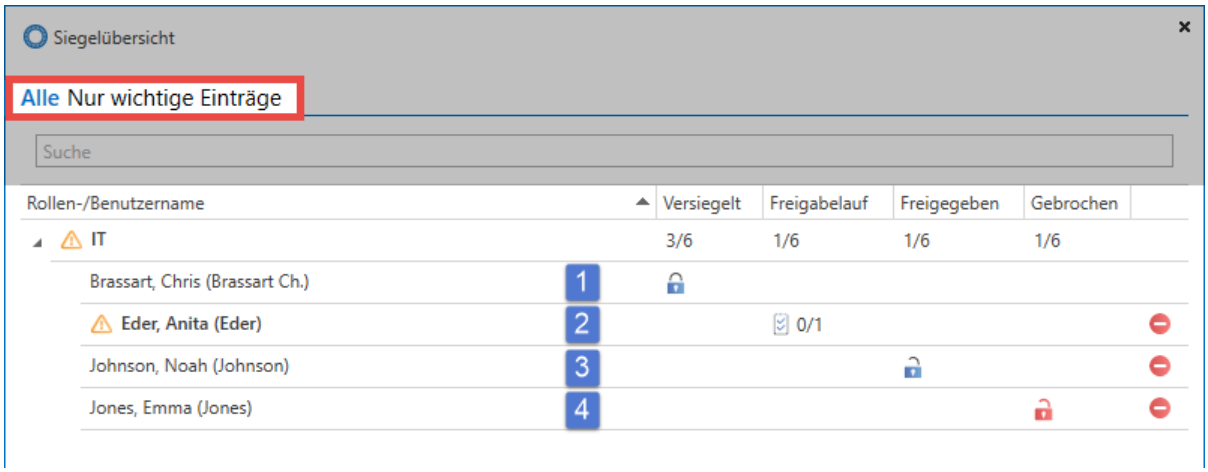
## Was ist die Siegelübersicht?

Freigabeberechtigte erhalten über die Siegelübersicht jederzeit Zugang zum aktuellen Zustand der vorhandenen Siegel. Die Übersicht ist sowohl über die Ribbon, als auch über das Icon im Passwortfeld des Lesebereichs zugänglich.




## Die vier Zustände eines Siegels

Grundsätzlich ermöglicht die Siegelübersicht einen Überblick über alle Benutzer, welche den Datensatz versiegelt vorliegen haben. Dies ist natürlich auch dann der Fall, wenn diese das Siegel über die Zugehörigkeit einer Rolle erhalten. Funktionen zum Bearbeiten und Löschen vorhandener Siegel stehen ebenso zur Verfügung. Zudem wird der aktuelle Zustand der Versiegelung in Form einer Freigabematrix dargestellt. Es existieren insgesamt **vier Zustände**, in denen sich ein Siegel befinden kann:




### 1. Versiegelt

Ist ein Datensatz für einen Benutzer **versiegelt**, wird für diesen die Möglichkeit das Passwort einzusehen durch das Siegel verhindert. Dies entspricht auch dem Zustand, wenn ein Siegel neu angebracht wurde. Durch das Zurücksetzen einer Anfrage über das Icon am rechten Bildschirmrand, werden aktuelle Anfragen einzelner Benutzer ebenfalls wieder in den Zustand “versiegelt” versetzt.

### 2. Freigabelauf

Hat ein Benutzer die Freigabe angefragt, befindet er sich im **Freigabelauf**. Dieser Zustand wird durch ein dementsprechendes Icon neben dem Benutzernamen hervorgehoben, da hier eine mögliche Freigabe aktiv durch Freigabeberechtigte gewährt werden kann. Nach diesen sog. **wichtigen Einträgen** kann ebenso in der Kopfzeile der Siegelübersicht im gleichnamigen Reiter gefiltert werden. Die maximale Gültigkeit einer Freigabeanfrage kann in den erweiterten Siegeleinstellungen konfiguriert werden. Ist die Frist abgelaufen, ohne dass genug Freigaben erzielt wurden, wird die Anfrage gelöscht und der Zustand “versiegelt” wiederhergestellt.

### 3. Freigegeben

Wurde eine Freigabe gewährt gilt ein Siegel als **freigegeben**. Die maximale Gültigkeit einer gewährten Freigabe ist in den erweiterten Siegeleinstellungen einschränkbar. Der Benutzer hat dann z.B. 24 Stunden Zeit, um die Freigabe anzunehmen und das Siegel zu brechen.

### 4. Gebrochen

Der tatsächliche **Siegelbruch** erfolgt, indem man Kenntnis über die erfolgte Freigabe erhält und nach einer Sicherheitsabfrage das Siegel aktiv bricht. Das Einsehen des Passwortes ist hierbei unerheblich. Einmal gebrochene Siegel können manuell durch das Icon rechts neben der Spalte für gebrochene Siegel zurückgesetzt werden. Hierbei wird der Zustand “Versiegelt” wiederhergestellt.

! Es macht logisch keinen Sinn, bereits eingesehene Passwörter neu zu versiegeln. Die Sicht auf das Passwort lag dem Benutzer vor. Demnach ist es nicht überwachbar, ob dieser das Passwort z.B. per Screenshot gesichert hat. In solchen Fällen ist die Vergabe eines neuen Passwortes die einzige Möglichkeit die Passwortsicherheit zu 100% zu gewährleisten!

# Freigabemechanismus

## Was ist der Freigabemechanismus?

Ein versiegeltes Passwort wird erst dann freigegeben, wenn die im Siegel geforderte Anzahl von Freigaben gewährt wurde. Freigaben können all diejenigen erteilen, die im Siegel als Freigabeberechtigte definiert wurden. Der Mechanismus beschreibt den kompletten Vorgang von der ersten Freigabeanfrage bis hin zur endgültigen Erteilung der Freigabe und dem Brechen des Siegels.

## Benutzer und Rollen im Freigabemechanismus

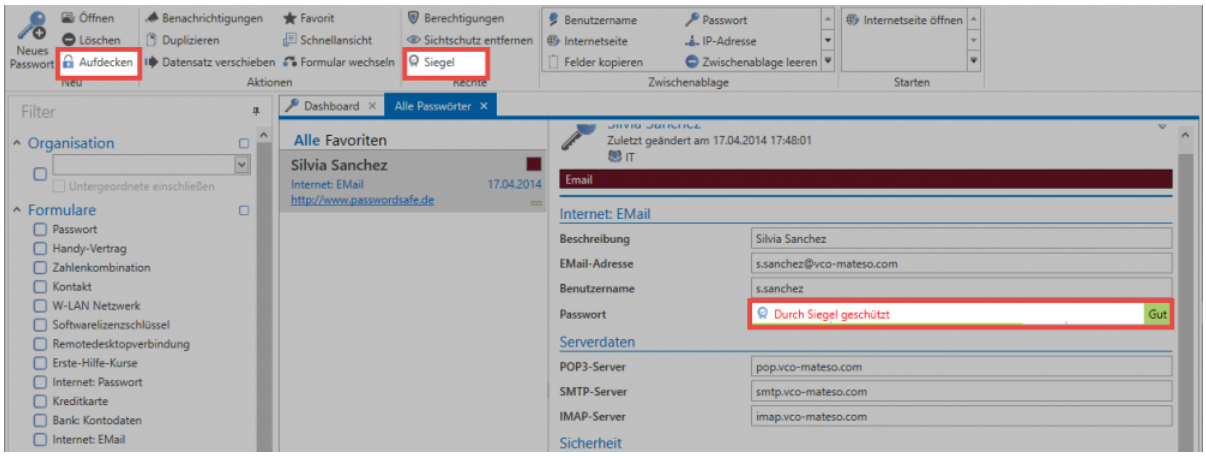
Wie bereits in den vorherigen Kapiteln erwähnt, schränken Siegel stets das Recht eines Benutzers ein, ein bestimmtes Passwort einzusehen. Auch wenn die Konfiguration in der Regel auf Rollenebene vorgenommen wird, ist selbstverständlich bei der Durchführung der Freigabe jeder Benutzer für seine eigene Anfrage verantwortlich. Auch wenn für eine Rolle ein Siegel definiert wird, werden technisch gesehen für jedes einzelne Mitglied der Rolle separate Siegel erstellt.

Getätigte Anfragen oder Freigaben gelten stets nur für den jeweiligen Benutzer!

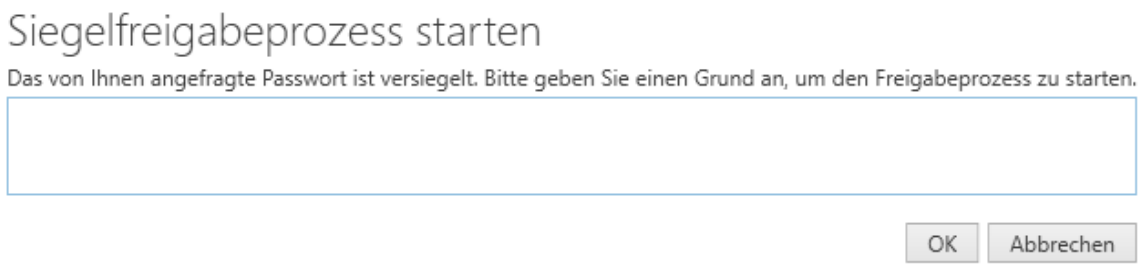
Ist ein Benutzer in mehreren Rollen eines Siegels Mitglied, wird stets das “stärkere” Recht angewendet. Freigaberecht überwiegt Leserecht.

### 1. Freigaben anfragen

Um eine Freigabe für versiegelte Passwörter zu erhalten, muss diese bei Freigabeberechtigten angefragt werden. Innerhalb des Password Safe Clients ist dies sowohl über die Buttons **Aufdecken** und **Siegel** in der Ribbon, als auch über das **Icon im Passwortfeld** des Datensatzes im Lesebereich möglich.



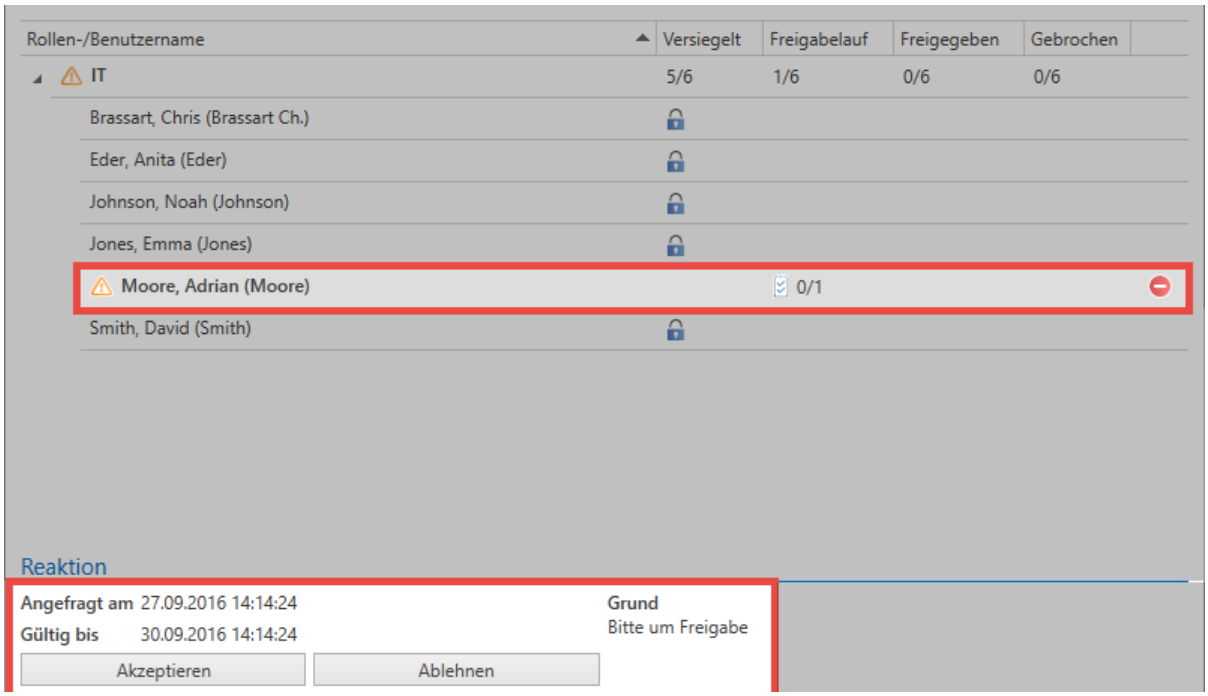

Es öffnet sich ein modales Fenster, mit Hilfe dessen man das Siegel anfragen kann. Die eingegebene Begründung wird Freigabeberechtigten angezeigt.



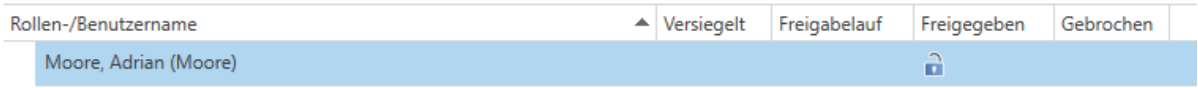

Alle Freigabeberechtigten erhalten die Benachrichtigung, dass der Benutzer das Siegel angefragt hat. Dies ist sowohl über das Modul Benachrichtigungen, als auch in der Siegelübersicht einsehbar.

### 2. Freigaben gewähren

Direkt über die genannte Benachrichtigung kann durch das Siegelsymbol in der Ribbon die Siegelübersicht geöffnet werden. Es wird durch das entsprechende Icon darauf aufmerksam gemacht, dass hier Handlungsbedarf besteht. Alle für eine Freigabe relevanten Daten werden innerhalb der Siegelübersicht veranschaulicht. Auch der in der Freigabe genannte Grund ist ersichtlich.

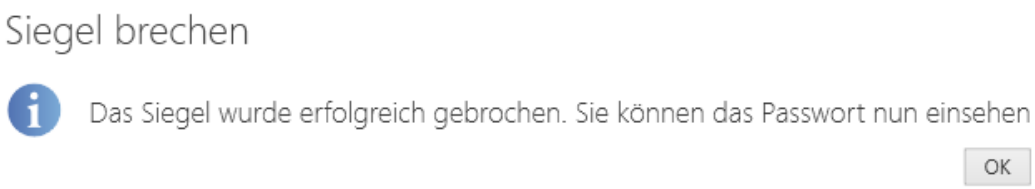



Ist die Freigabe gewährt, wird der Anfragende Im **Modul Benachrichtigungen** informiert. Man kann hier auch direkt das Siegel über die Ribbon öffnen und den nun freigegebenen Zustand einsehen.




### 3. Siegel brechen

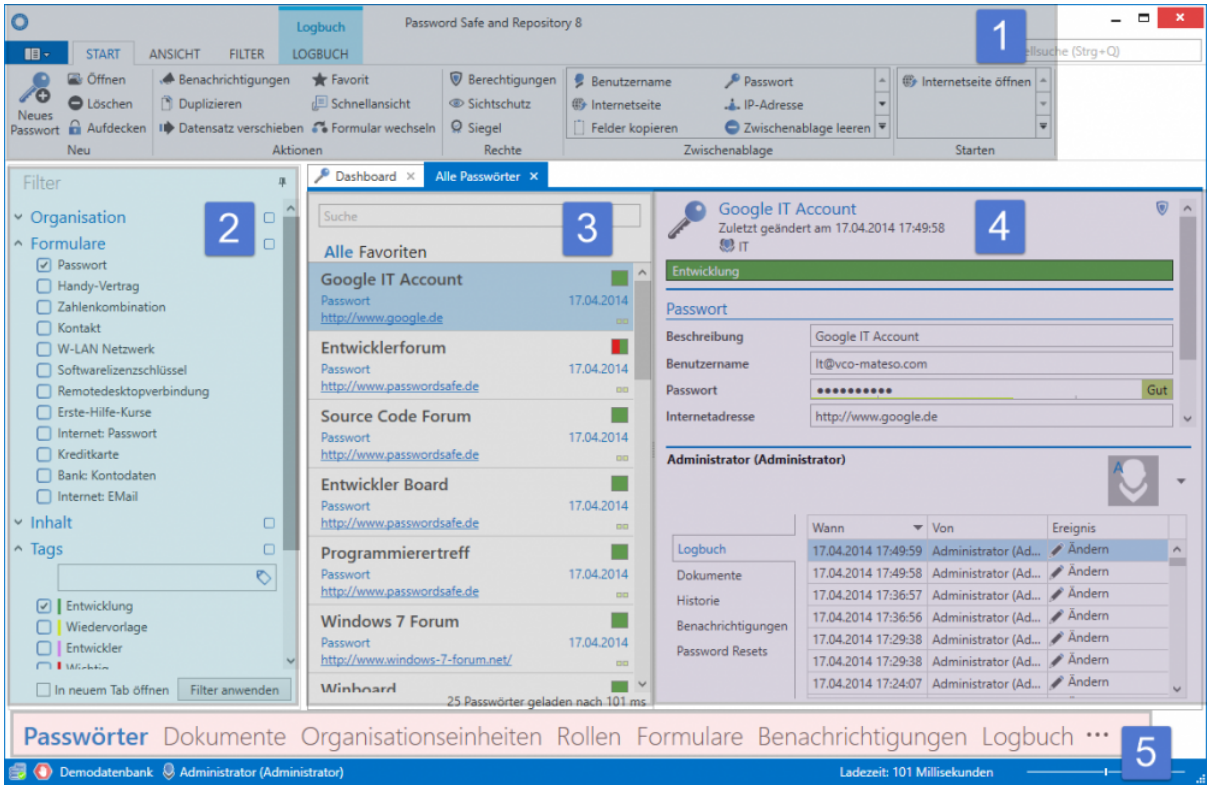
Sobald der anfragende Benutzer die Anzahl der benötigten Freigaben erhalten hat, wird dieser wie gewohnt über die Benachrichtigungen informiert. Das Siegel kann nun gebrochen werden. Ab diesem Zeitpunkt ist das Passwort durch den Benutzer einsehbar.



# Bedienung und Aufbau

## Clientaufbau

Der strukturierte und modulare Aufbau des Clients ermöglicht, dass man regelmäßig benötigte Funktionalitäten wiederkehrend an derselben Stelle findet. Obwohl man durch die Modulauswahl Zugang zu den diversen Bereichen des Password Safe erhält, bleiben die Bedienelemente konstant an den hierfür angedachten Positionen. Dieses intuitive Bedienkonzept sorgt für effizientes Arbeiten sowie eine minimale Einarbeitungszeit.



1. Ribbon

2. Filter

3. Listenansicht

4. Lesebereich

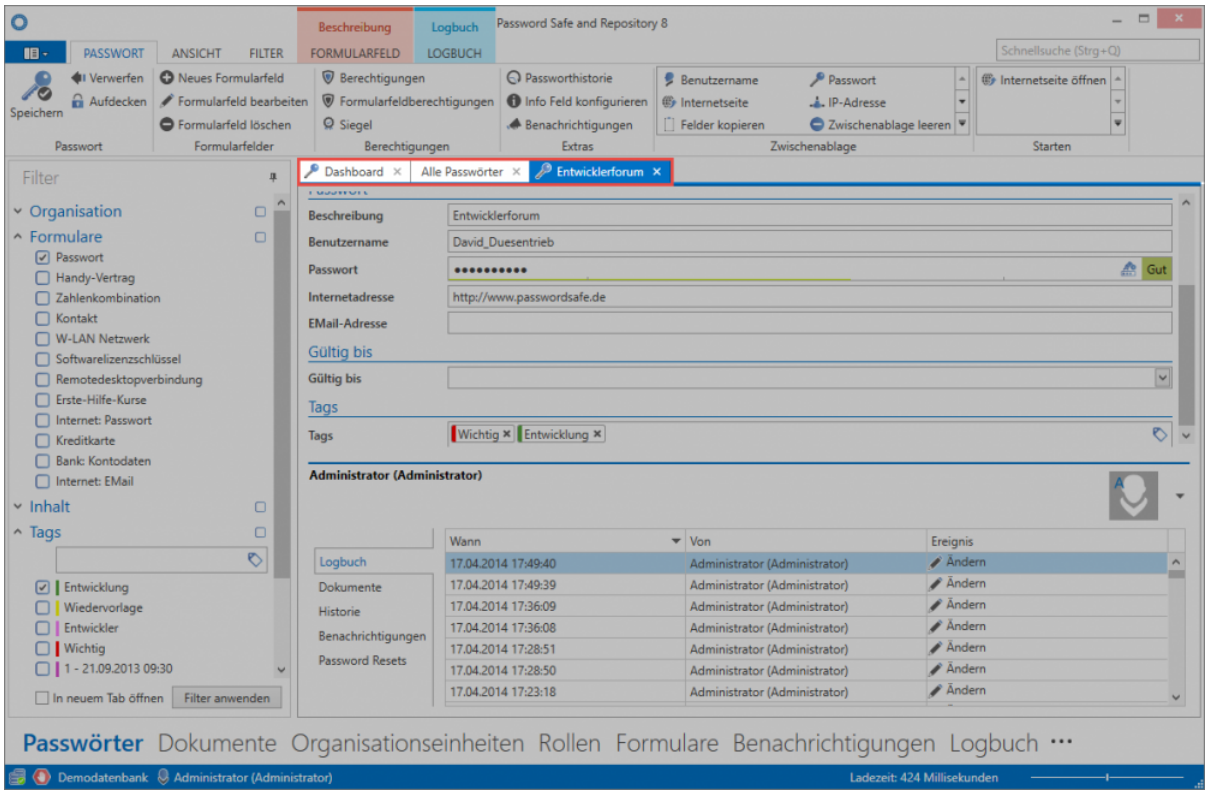
5. Tags

6. Suche

7. Dashboard und Widgets

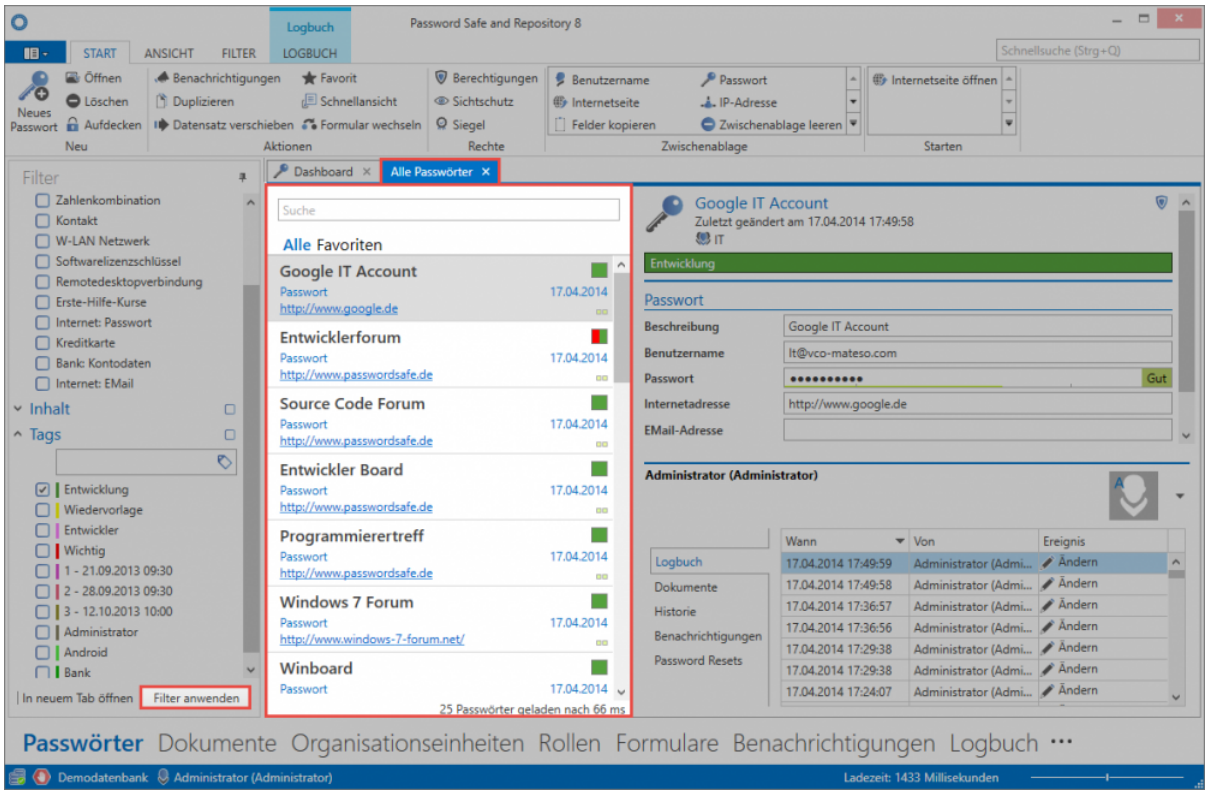
# Tabs

Tabs stellen innerhalb des Password Safe eine weitere Möglichkeit dar, zusammengehörige Informationen wohl sortiert in einem separaten Bereich abzubilden. Diese Registernavigation ermöglicht die Darstellung sowie den schnellen Zugriff und Wechsel zwischen relevanten Informationen. Das Ergebnis eines Filters mit speziellen Kriterien kann somit festgehalten werden, ohne dass erneutes Filtern das ursprüngliche Ergebnis überschreibt. Parallel können auch Detailinformationen zu Datensätzen in eigenen Tabs angesprochen werden. Selbstverständlich ist es möglich, die Reihenfolge von Tabs per Drag & Drop gemäß den individuellen Anforderungen anzupassen.



### Standard-Tab

Entsprechend dem aktiven Modul wird per Standard das angezeigte Tab **Alle Passwörter** umbenannt in das Pendant des jeweiligen Moduls. (Alle Dokumente, Alle Formulare, etc.)

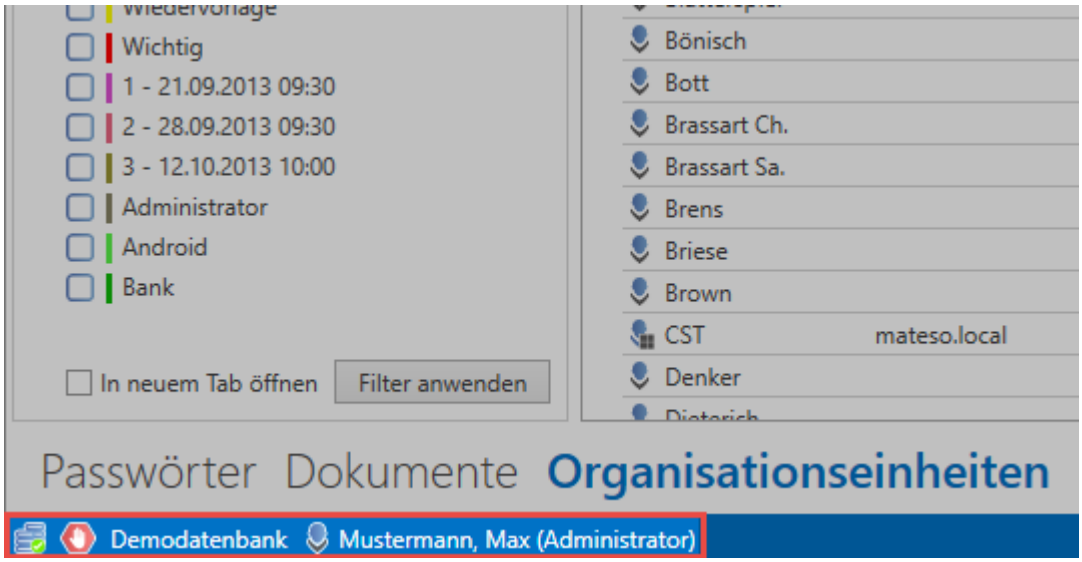



Obwohl der Name vermuten lässt, dass alle Datensätze der Datenbank dargestellt werden, entsprechen die in der Listenansicht angezeigten Datensätze den im Filter festgelegten Kriterien. Der Tab lässt sich schließen und kann durch eine erneute Anwendung des Filters wiederhergestellt werden.

## Client Footer Informationen

Unabhängig vom ausgewählten Modul sind im Footer-Bereich des Clients diverse Informationen dargestellt. Für weiterführende Informationen sind die Icons ebenso mit einem aussagekräftigen Mouseover-Text belegt.

- Verbindung zur Datenbank
- Rückmeldung, falls eine ungesicherte Verbindung besteht
- Nachname, Vorname (Benutzername) des angemeldeten Benutzers

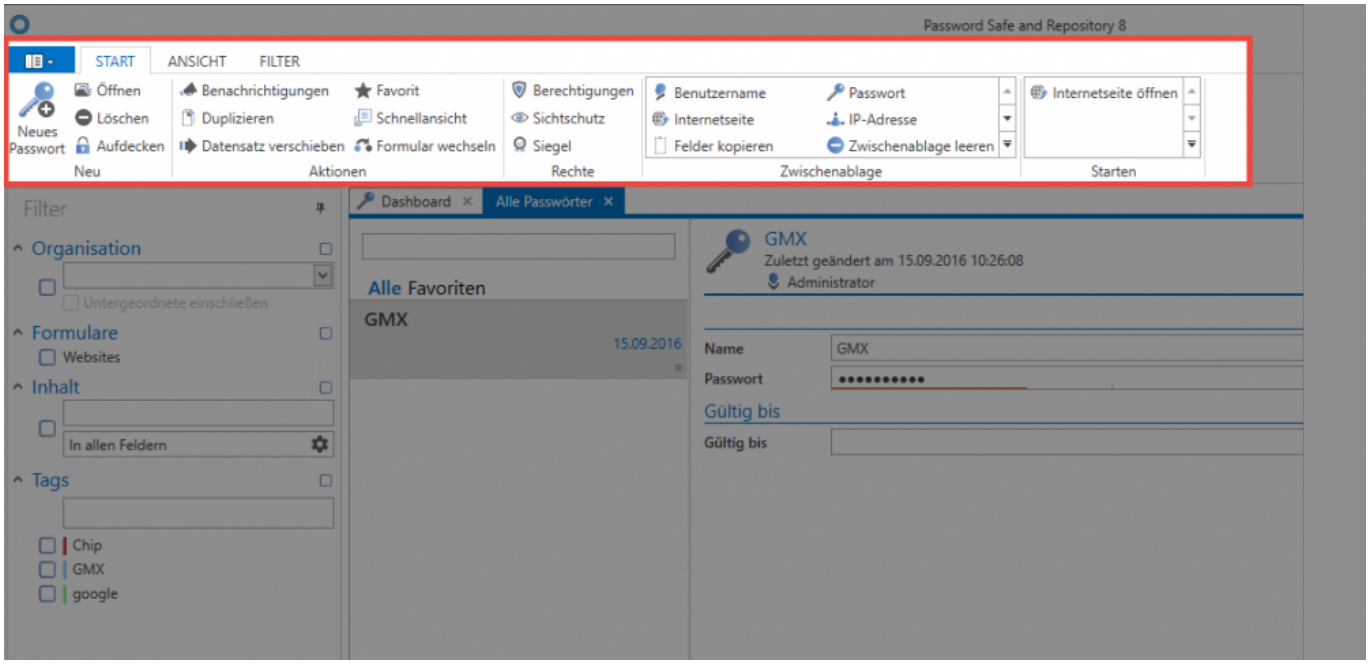



- Ribbon
- Filter
- Listenansicht
- Lesebereich
- Tags
- Suche
- Dashboard und Widgets
- Tastaturkürzel

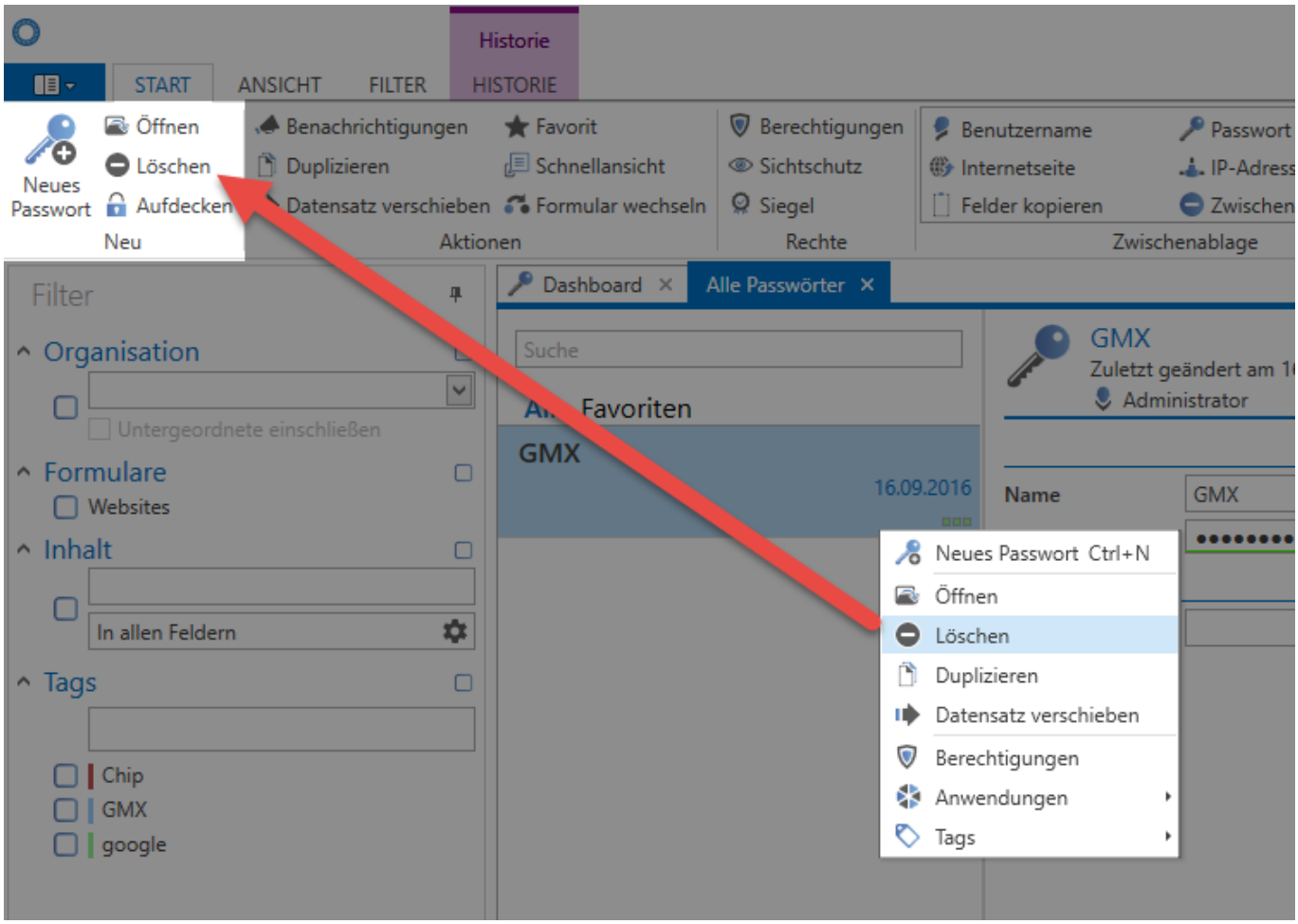
# Ribbon

## Was ist die Ribbon?

Die Ribbon ist das über alle Module hinweg verfügbare, zentrale Bedienelement in Password Safe Version 8. Die Bedienung erfolgt nahezu immer über die Ribbon im Kopfbereich des PSR Client.



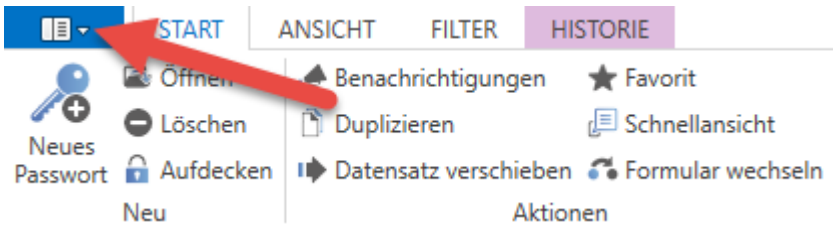

Die innerhalb der Ribbon verfügbaren Funktionalitäten richten sich dynamisch nach den derzeit verfügbaren Aktionen. Je nachdem, welches Objekt markiert ist, sind unterschiedliche Aktionen durchführbar. Die Auswahl des Moduls hat ebenso Auswirkungen auf die in der Ribbon möglichen Features. Natürlich lassen sich darüber hinaus die wichtigsten Aktionen per Kontextmenü (rechte Maustaste) steuern.




Dies betrifft hauptsächlich die sehr oft genutzten Features, wie z.B. Öffnen, löschen oder das Zuweisen von Tags. Eine vollständige Auflistung der möglichen Aktionen ist jedoch stets nur direkt in der Ribbon möglich. Dies gewährleistet, dass das Kontextmenü schlank gehalten werden kann.

# Zugang zum Client-Hauptmenü (Backstage)

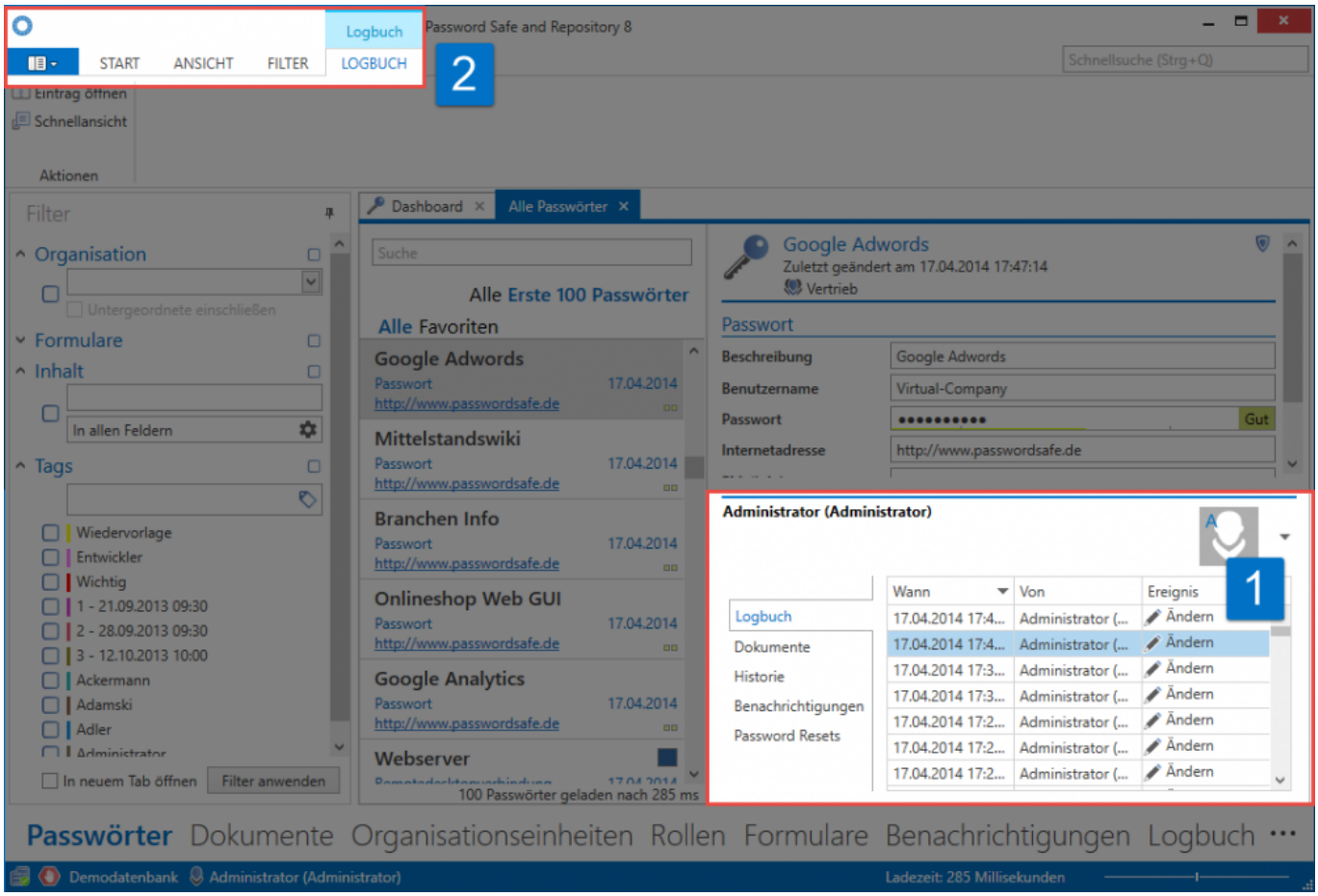
Über den Button links oben in der Ribbon ist der Zugang zu den Client-Einstellungen gewährleistet:




# Ribbon-Tabs

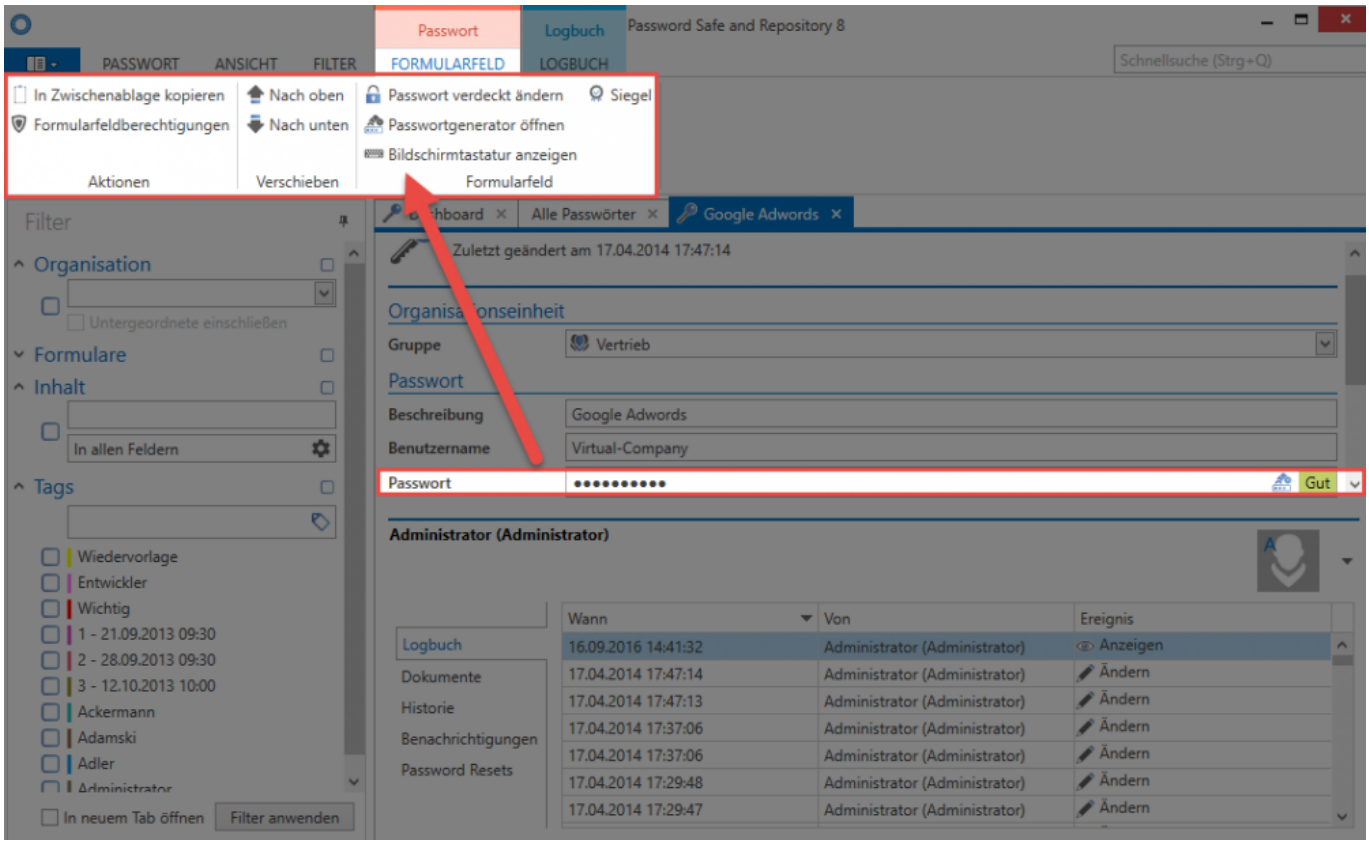
Im Header Bereich der Ribbon existieren Tabs, welche thematisch alle verfügbaren Operationen zusammenfassen. Per default ist modulübergreifend **Start, Ansicht und Filter** verfügbar. Wenn der

Footer des Lesebereichs geöffnet ist **(1)**, werden zudem weitere Tabs in der Ribbon sichtbar **(2)**. Diese enthalten, entsprechend der im Footer getroffenen Auswahl, weitere mögliche Aktionen.




## Content-Tabs

Durch Doppelklick eines Objektes in der Listenansicht öffnet sich ein neuer Tab mit dessen Detailansicht. Je nachdem, welches Formularfeld man markiert hat, öffnet sich in der Ribbon der dementsprechende Content Tab.

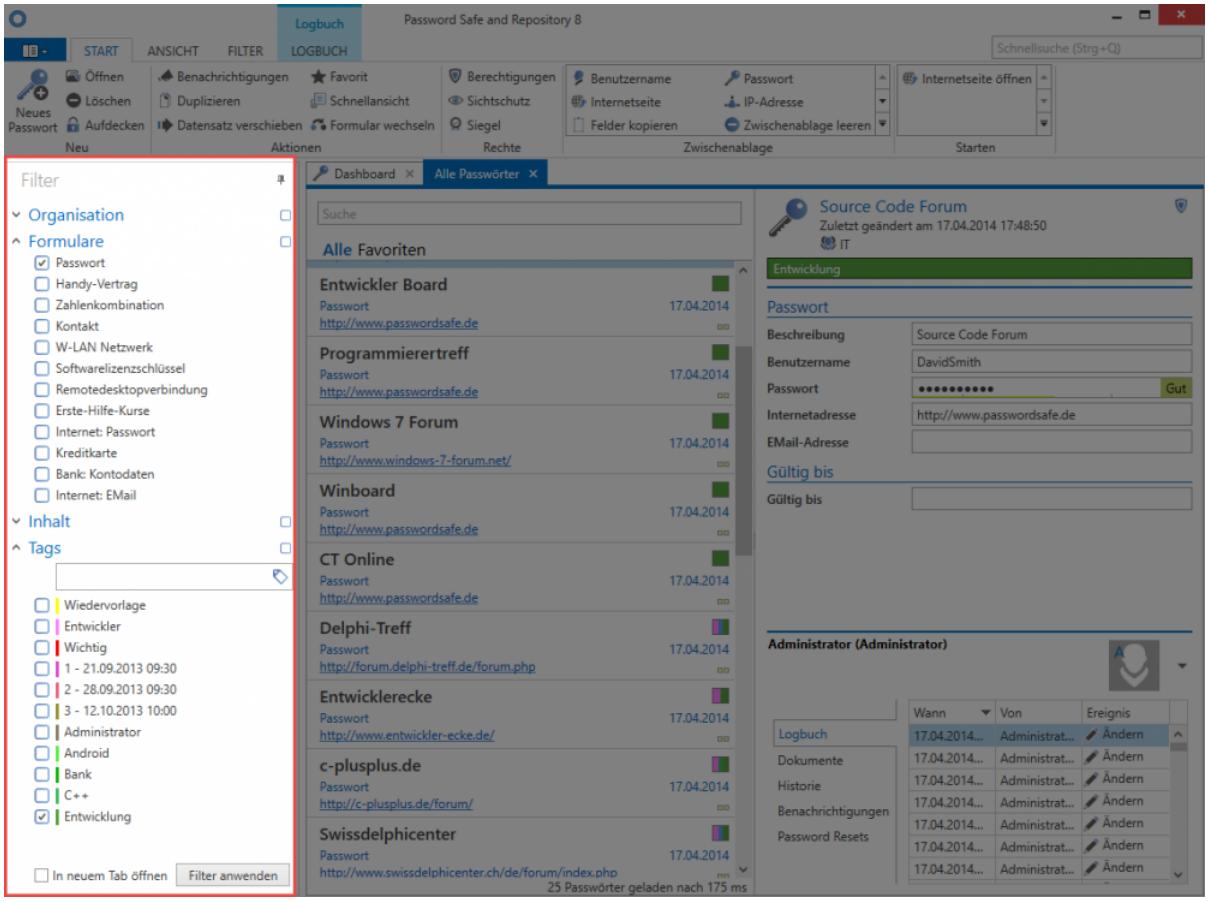



Gemäß dem markierten Formularfeld werden im Content Tab weitere Aktionen angeboten. Im Feld Passwort ist dies z.B. das Aufrufen des Passwortgenerators oder der Bildschirmtastatur, oder auch die Möglichkeit, dieses in die Zwischenablage zu kopieren.

# Filter

## Was ist der Filter?

Die frei konfigurierbaren Filter des PSR Client liefern sämtliche Methoden zum einfachen Auffinden gespeicherter Daten. Die Filterkriterien werden stets gemäß demjenigen Modul angepasst, in dem man sich aktuell befindet. Durch die Auswahl einer oder auch mehrerer Suchkriterien, und einem Klick auf „Filter anwenden“, wird die Ergebnismenge in der Listenansicht angezeigt. Bei Bedarf kann dieser Vorgang beliebig wiederholt und um weitere Restriktionen erweitert werden.




## Wer darf den Filter benutzen?

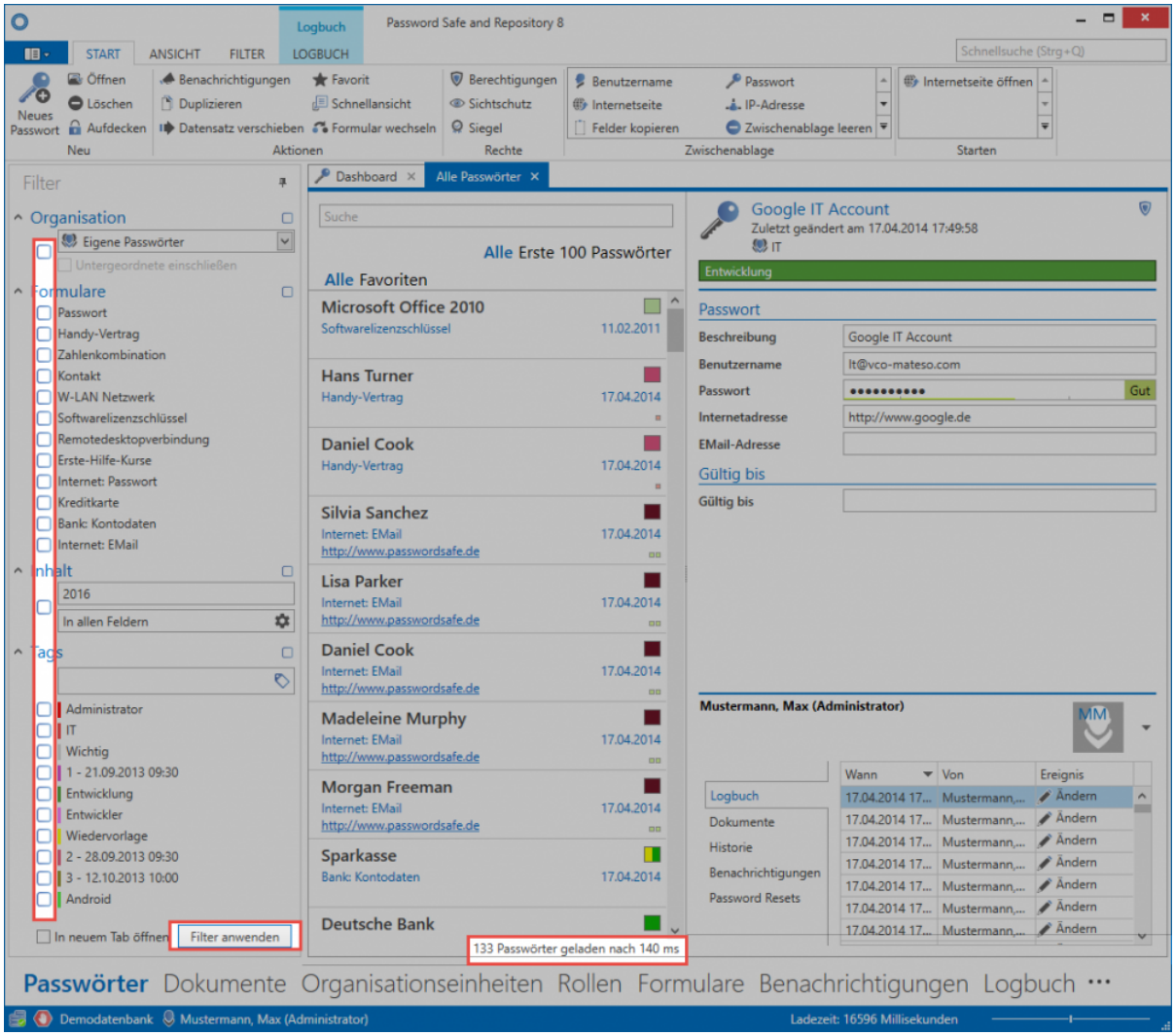
Der Filter stellt aufgrund der Möglichkeit, vorhandene Ergebnismengen gemäß individuellen Anforderungen einzuschränken, ein unverzichtbares Arbeitswerkzeug dar. Demzufolge ist es auch allen Benutzern möglich, den Filter zu nutzen. Selbstverständlich sind Restriktionen für Filterkriterien möglich. Dies bedeutet, dass durch Berechtigungen die möglichen Filterkriterien für einzelne Mitarbeiter eingeschränkt werden können. Ein Mitarbeiter kann z.B. nur dann nach dem Formular **Passwort** filtern, wenn er Leseberechtigung auf das Formular besitzt.

> **!** Tags können nicht berechtigt werden. Alle genutzten Tags sind demnach durch alle Mitarbeiter nutzbar. Die Anzeigereihenfolge im Filter wird durch die Häufigkeit der Nutzung festgelegt. Diese Handhabung ist nicht sicherheitskritisch, da Tags keinerlei Berechtigungen gewähren, sondern lediglich als unterstützende Maßnahme beim Filtern dienen.

# Anwendungsbeispiel

### Filtern ohne Kriterien

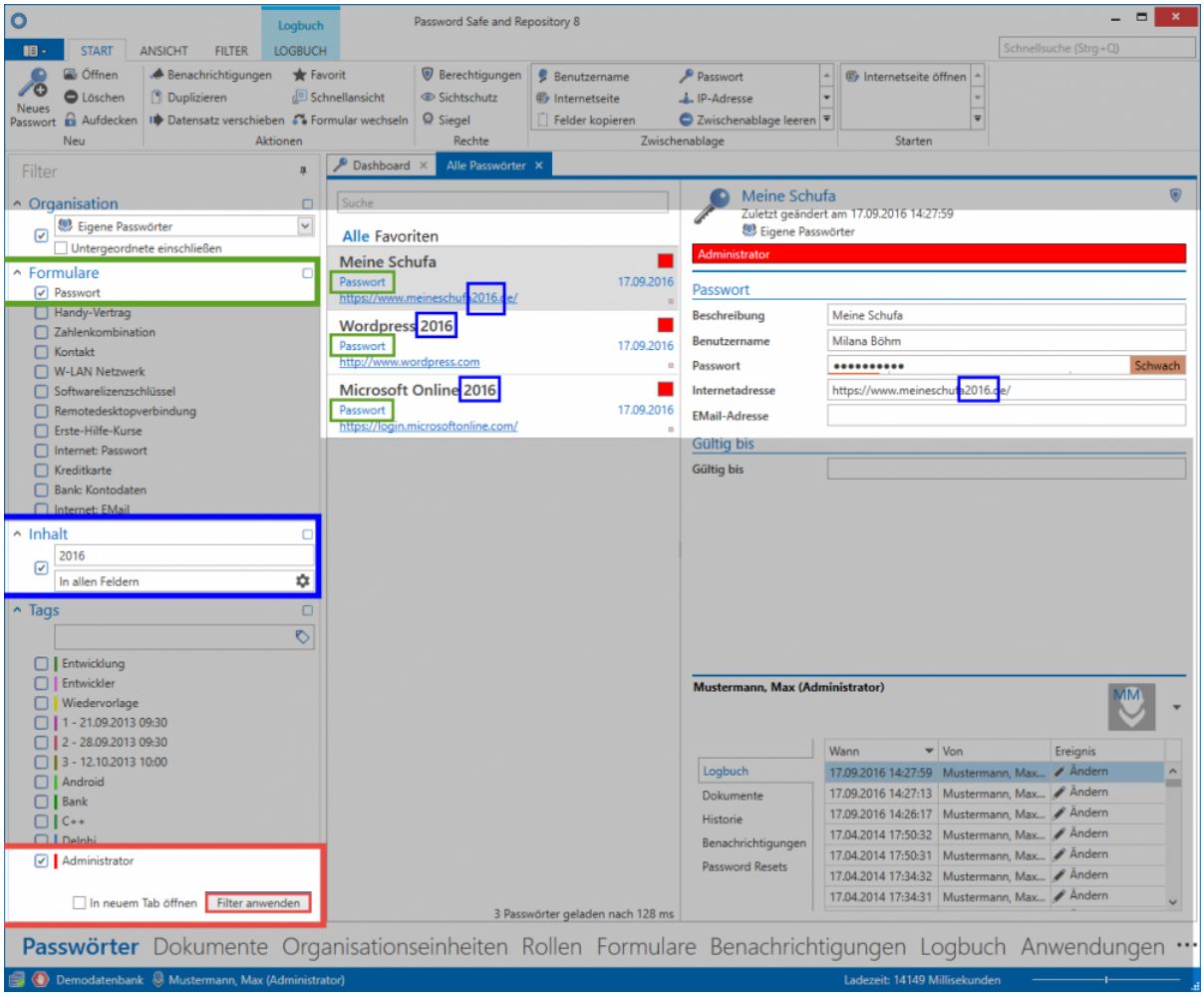
Durch Auswahl der gewünschten Kriterien, und dem Anwenden des Filters über den gleichnamigen Button, wird die Menge aller den Kriterien entsprechenden Datensätze in der Listenansicht wiedergegeben. Würde man **ohne Kriterium** den Filter anwenden, erhält man eine Auflistung aller Datensätze, auf die man generell berechtigt ist.



Wie man sehen kann, ist die Menge der Datensätze mit 133 nicht wirklich effizient verwaltbar. Es ist in den meisten Situationen nötig, dass durch das Hinzufügen von Filtern die Anzahl der Datensätze reduziert wird.

### Hinzufügen von Filterkriterien

Das Filterkriterium **Organisation** kann direkt bei den Berechtigungen ansetzen und die Anzahl der Datensätze gemäß vergebener Berechtigungen einschränken. Im vorliegenden Falle ist der angemeldete Benutzer auf diverse Bereiche berechtigt. Er möchte jedoch ausschließlich jene Datensätze einsehen, welche innerhalb der Organisationsstruktur dem Bereich **Eigene Passwörter** zugeteilt sind. Zusätzlich sollen weitere Einschränkungen durchgeführt werden, welche man in folgendem Satz ausformulieren könnte: “Liefere alle Datensätze aus meinen eigenen Passwörtern, welche mit dem Formular **Passwort** erstellt wurden, in denen der Ausdruck **2016** enthalten ist und die mit dem Tag **Administrator** versehen sind”.

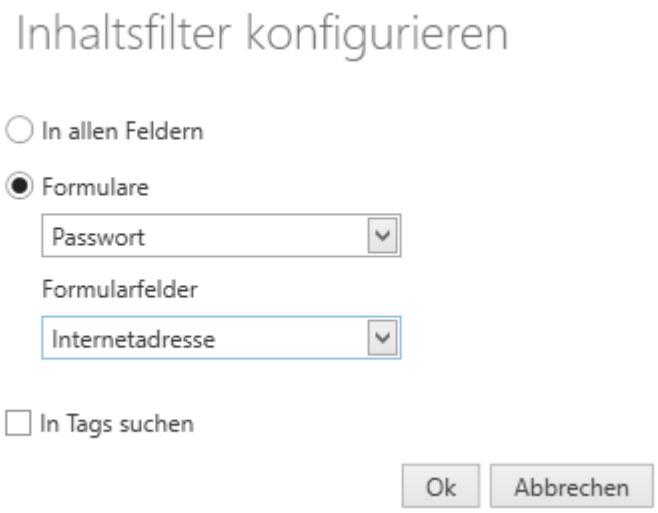


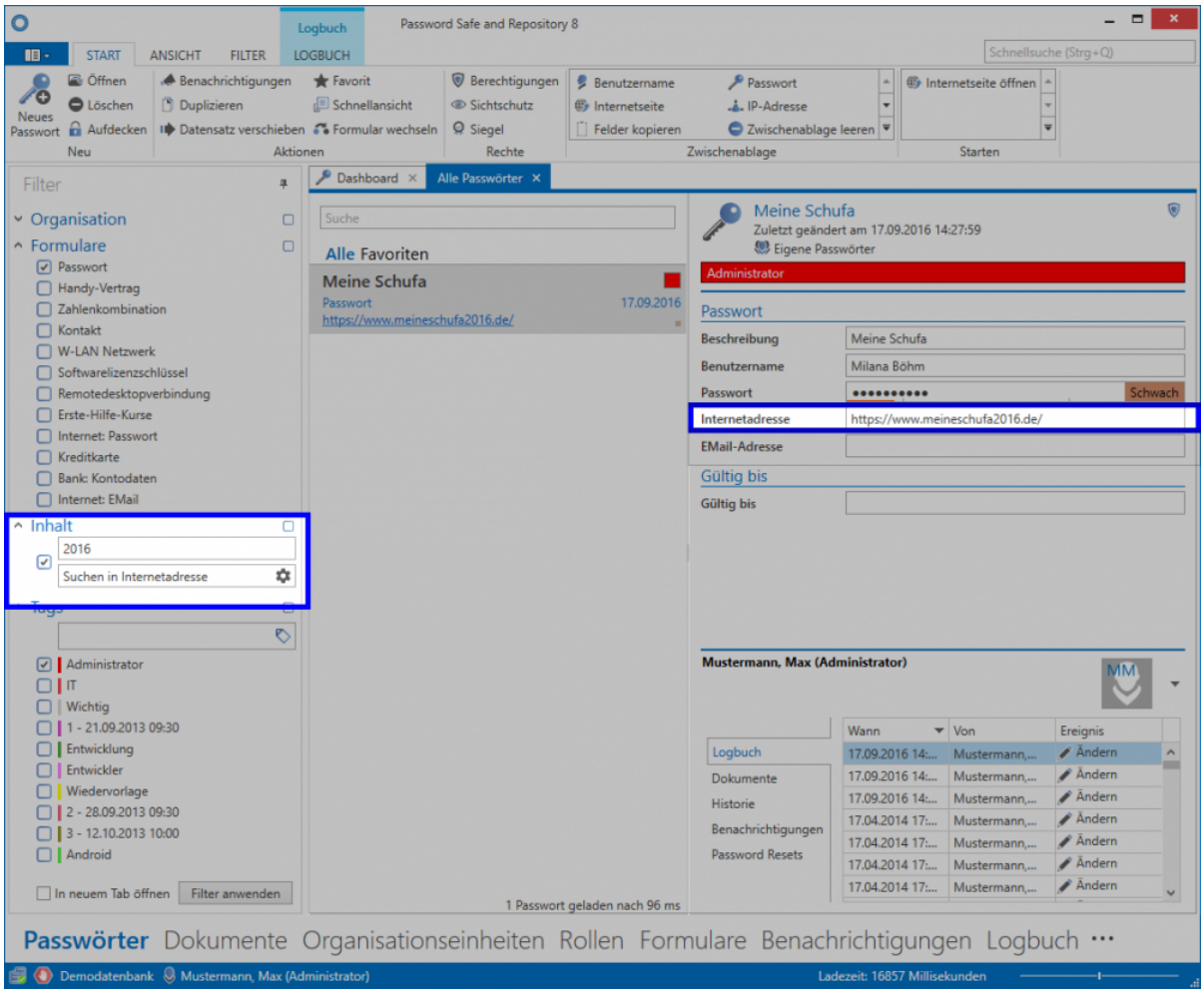

Wie ersichtlich liefert der Filter das gewünschte Ergebnis. Inwiefern die Filterkriterien mit den drei übrig gebliebenen Datensätzen übereinstimmen, ist farblich zugeordnet.

> **!** Beim Filtern mit mehreren Kriterien, wie z.B. Formulare, Inhalt und Tags, müssen zwingend alle Filterkriterien erfüllt werden. Es handelt sich demnach um eine logische “Und-Verknüpfung”. Weitere mögliche Verknüpfungsarten sind in den Erweiterten Filtereinstellungen detailliert beschrieben.

### Inhaltsfilter

Der Ausdruck **2016** ist im Datensatz **Meine Schufa** Teil der Internetadresse, bei **Wordpress 2016** sowie **Microsoft Online 2016** Teil der Beschreibung. Da im Inhaltsfilter die Suche **“in allen Feldern”** aktiviert ist, sind dementsprechend auch alle drei Datensätze Teil der Ergebnismenge und werden in der Listenansicht angezeigt. Man kann den Inhaltsfilter auch dermaßen konfigurieren, dass er ganz gezielt nach Ausdrücken in einem bestimmten Feld sucht. Das Icon direkt neben dem Ausdruck **“in allen Feldern”** öffnet die Konfiguration des Inhaltsfilters in einem modalen Fenster. Wie ersichtlich wurde konfiguriert, dass der Inhaltsfilter lediglich noch das Formular **Passwort**, und in diesem nur das Formularfeld **Internetadresse** berücksichtigen soll:






Es ist aufgrund des vorliegenden Beispiels sehr leicht zu abstrahieren, dass der Filter filigran den persönlichen Anforderungen anpassbar ist. Er ist somit das wichtigste Werkzeug, um einmal in der Datenbank abgelegte Daten auch wiederfinden zu können.

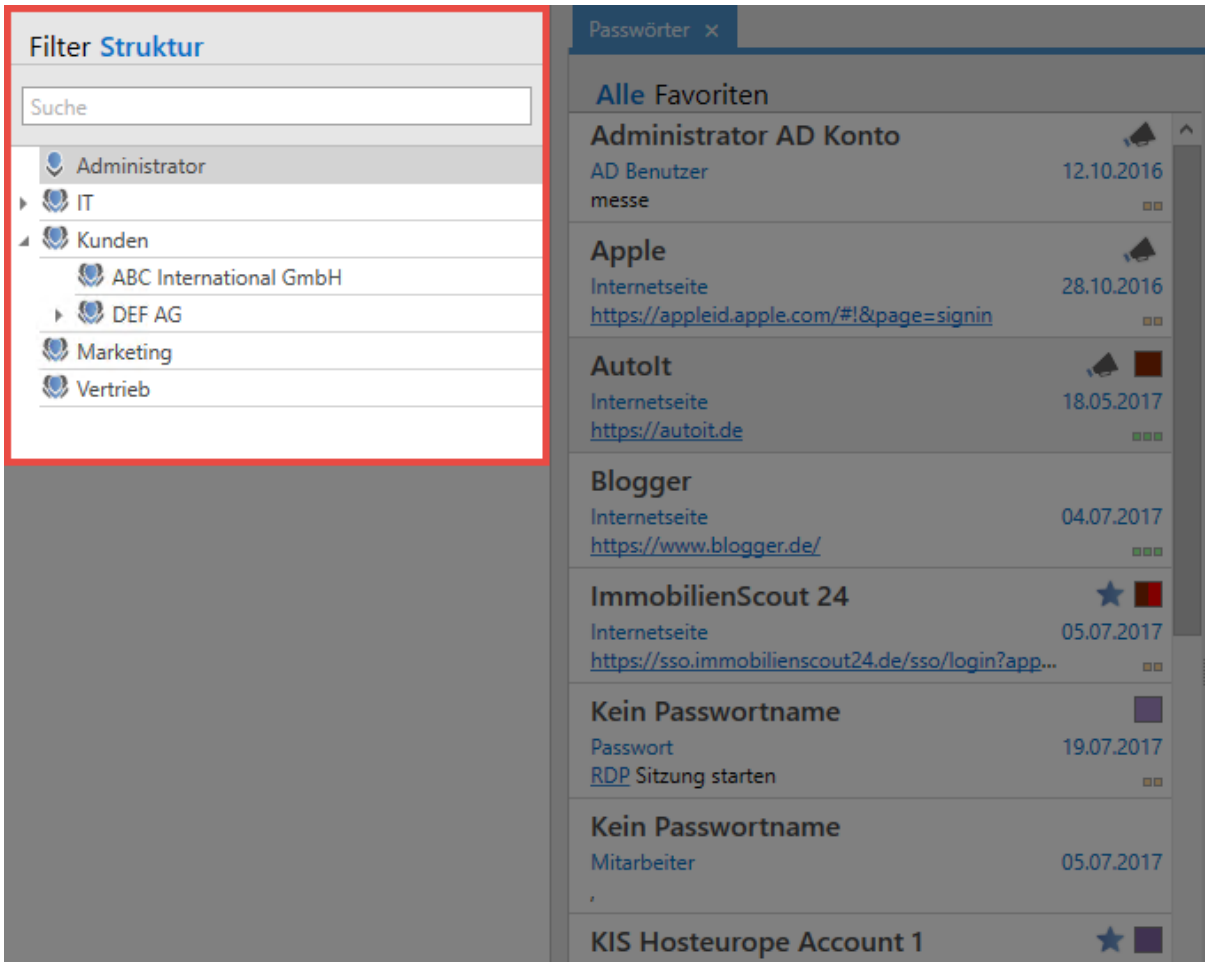
> **!** Die Effektivität des Filters ist eng mit der Datenintegrität verbunden. Nur, wenn Daten sauber gepflegt vorliegen, ist effizientes Arbeiten mit dem Filter gewährleistet. Es ist wichtig, dass Mitarbeiter im richtigen Umgang mit dem Filterwerkzeug, als auch beim Anlegen der Datensätze, geschult werden. Workshops weisen in diesem Zusammenhang die beste Erfolgsquote vor. Kontaktieren Sie uns gerne, falls Sie hierzu weitere Informationen wünschen.

# Anzeigemodus

## Welche Anzeigemodi existieren?

Zusätzlich zum bereits beschriebenen Filter kann optional auf die Strukturansicht gewechselt werden. Diese alternative Ansicht ermöglicht das Filtern einzig auf Basis der Organisationsstruktur. Diese Art der Filterung ist zwar auch in der standardmäßigen Filteransicht möglich, jedoch ist in der Strukturansicht die komplette Organisationsstruktur direkt einsehbar.

> Da es in der Password Safe Version 8 keine Ordner mehr gibt, kann die Strukturansicht nicht alle Funktionalitäten der Ordneransicht aus der Version 7 wiederspiegeln. Dennoch ist die Strukturansicht optisch an die Ordneransicht angelehnt um den Umstieg von Vorgängerversionen zu erleichtern.




Wie man sieht, ist in dieser Ansicht ausschließlich die Organisationsstruktur sichtbar. Bei Benutzern, welche stark strukturbasiert arbeiten möchten, wird diese Ansicht die richtige Wahl sein.

# Relevante Optionen

Im Zusammenhang mit dem Anzeigemodus existieren drei relevante Einstellungen:

| Kategorie: Filter | | |
|---|---|---|
| Anzeigemodus | Beides | Sicherheitsstufe 1 |
| Auf Filter springen bei Schnellsuche | Aktiviert | Sicherheitsstufe 1 |
| Zustand des Anzeigemodus beim Programmstart | Letzter Zustand | Sicherheitsstufe 1 |

- **Anzeigemodus**: Es kann definiert werden, ob der Standardfilter, der Strukturfilter oder beide angezeigt werden sollen. Wird letzte Option gewählt, kann zwischen beiden gewechselt werden.
- **Auf Filter springen bei Schnellsuche**: Nutzt man die Strukturansicht kann hier definiert werden, ob bei der Betätigung der Schnellsuche (rechts oben im Client) automatisch in den Standardfilter gewechselt werden soll
- **Zustand des Anzeigemodus beim Programmstart**: Es wird definiert, welcher Anzeigemodus bei Programmstart als default gesetzt werden soll.

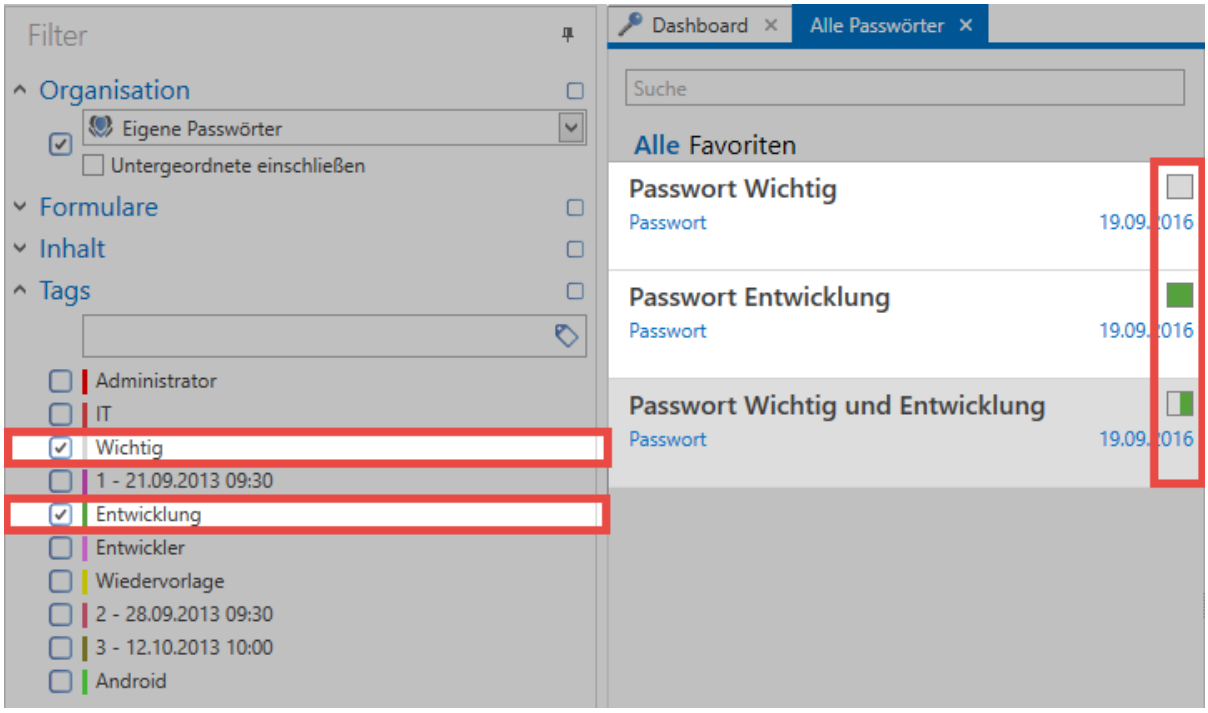
# Erweiterte Filtereinstellungen

## Verknüpfung von Filtern

Am Beispiel von Tags sind die beiden Möglichkeiten, mit denen man Filterkriterien verknüpfen kann, sehr einfach zu erklären. Folgende Optionen stehen zur Auswahl:

### 1. Logische “Oder-Verknüpfung”

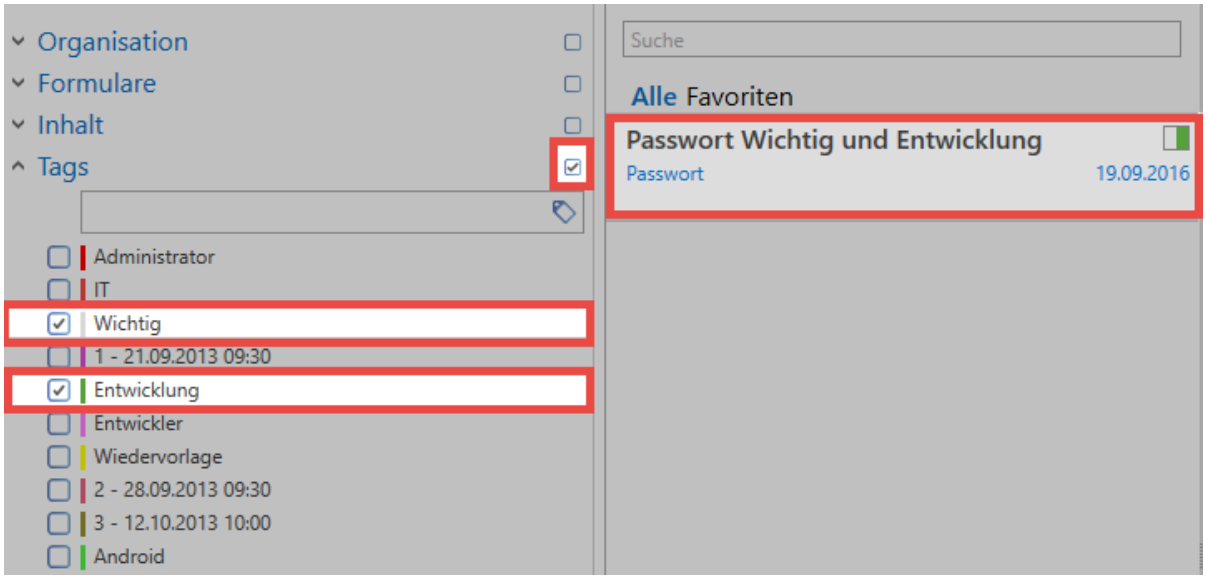
Standardmäßig ist der Filter in diesem Modus aktiv. In folgendem Beispiel sollen alle Datensätze gefunden werden, die mindestens einen der Tags **“Wichtig”** oder **“Entwicklung”** besitzen. Dies bedeutet auch, dass Datensätze entweder einen der Tags, oder auch beide besitzen können.




Aufgrund der farblichen Markierung der Tags in den Datensätzen ist ersichtlich, dass die ersten beiden Datensätze jeweils eines der Tags besitzen, das dritte beide Tags. Alle drei sind dennoch Teil der Ergebnismenge. **Es muss mindestens ein Filterkriterium erfüllt sein**.

### 2. Logische “Und-Verknüpfung”

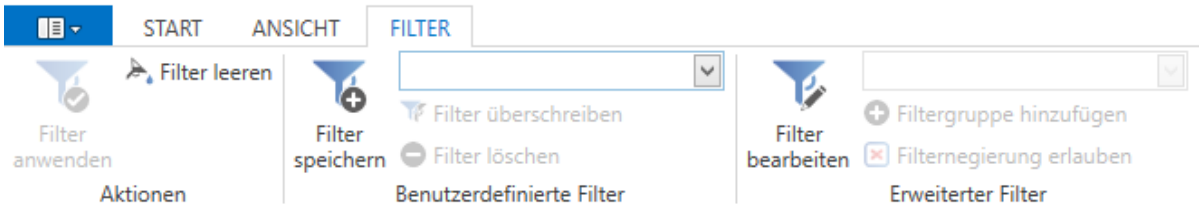
Aktiviert wird dieser Modus direkt durch die Checkbox im Filter. Jedes Filterkriterium besitzt seine eigene Checkbox.


**Im Gegensatz zur "Oder-Verknüpfung" müssen bei der "Und-Verknüpfung" zwingend beide Kriterien erfüllt sein**. Dementsprechend sind in dem vorliegenden Beispiel als Ergebnismenge nur diejenigen Datensätze aufgeführt, die sowohl das Tag **"Wichtig"**, also auch das Tag **"Entwicklung"** besitzen.

# Filter-Tab in der Ribbon

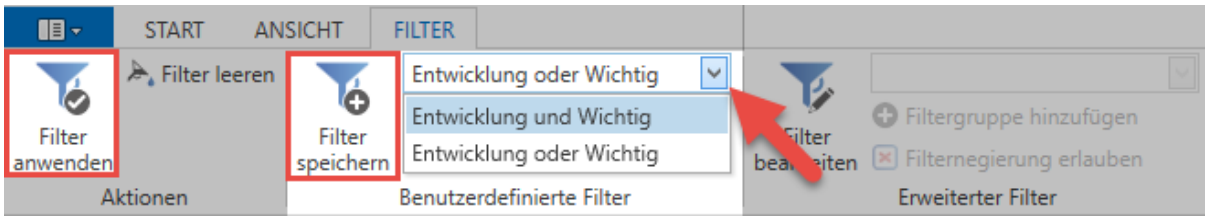
In der Ribbon ist ebenso die Filterverwaltung zu finden. Hier kann man z.B. die aktuell konfigurierten Filterkriterien erweitern, Filter speichern oder auch einfach sämtliche derzeit angewandten Filter leeren.




### Filter speichern, bearbeiten und löschen

Es bietet sich in vielen Fällen an, einmal definierte Filter zu speichern. Auf diese Art und Weise kann effizient auf bereits getätigte Filterergebnisse zurückgegriffen werden. Durch den Button "**Filter speichern**" wird man direkt aufgefordert, für diesen Filter einen aussagekräftigen Namen zu vergeben. Gespeichert wird der Filter gemäß der aktuell im Filter konfigurierten Kriterien. Dieser Filter ist nun im Auswahlmenü aufgelistet und kann fortan ausgewählt werden. Beachten Sie, dass eine getroffene Filterauswahl zwar sofort in den Filter übernommen, jedoch nicht automatisch durchgeführt wird. Es

muss hierzu der Filter angewendet werden. Sowohl der Button in der Ribbon, also auch das Pendant im Filter, führen hier zum gleichen Ergebnis.

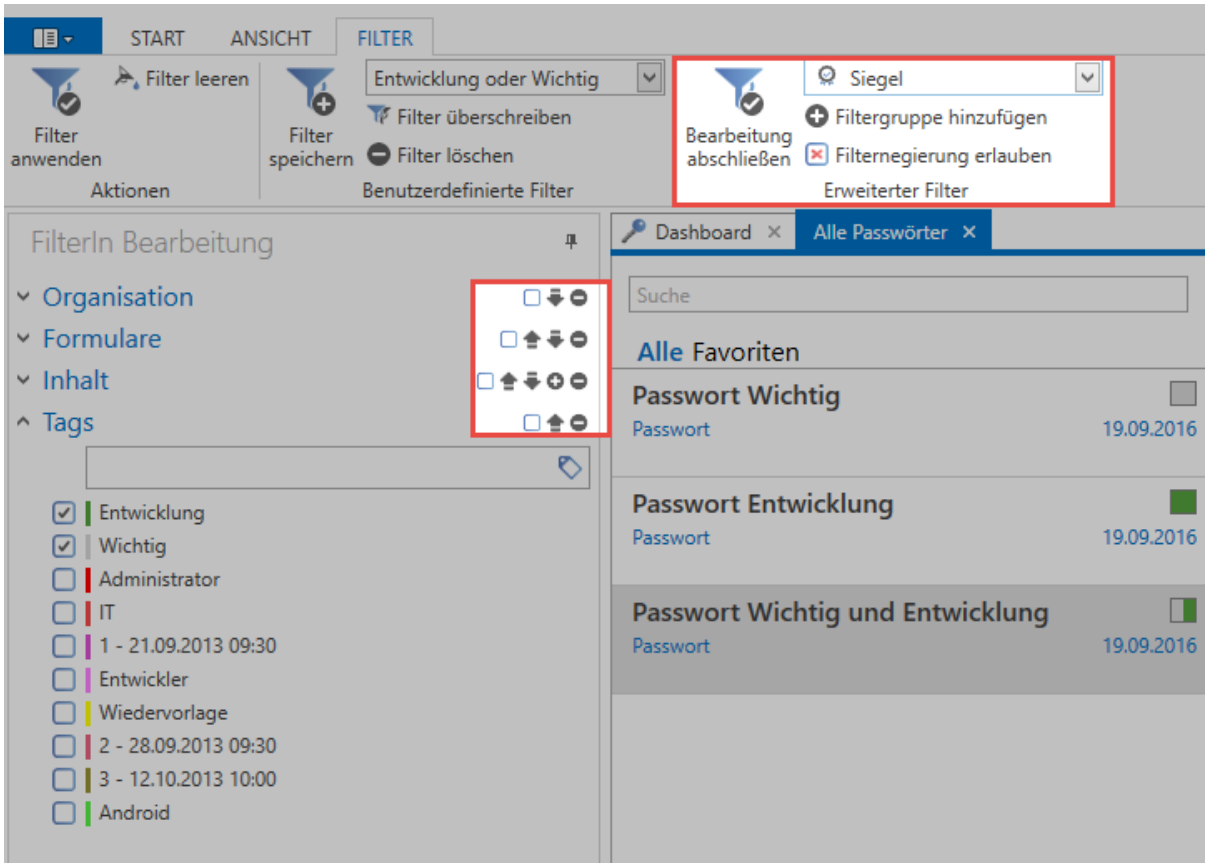



Das Löschen, sowie das Überschreiben vorhandener Filter, ist im Vorgehen identisch. Gelöscht wird stets der Filter, den man im Auswahlfeld markiert hat. Falls ein bereits existierender Filter überschrieben werden soll, bleibt der Name des Filters erhalten und wird mit den aktuell im Filter konfigurierten Filterkriterien überschrieben.

---

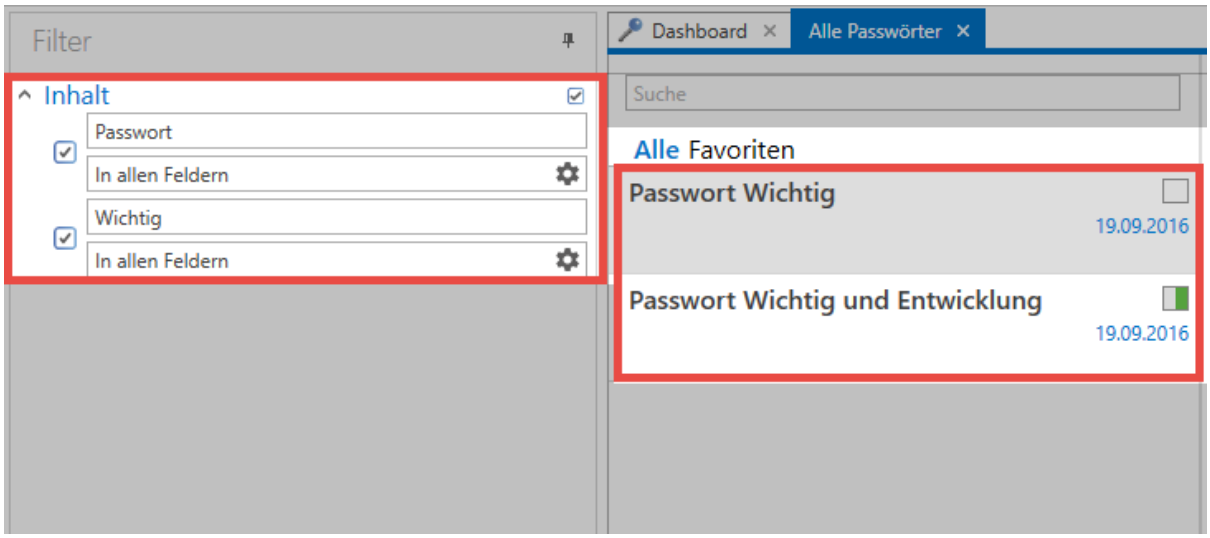
## Erweiterter Filter

In der Kategorie „Erweiterter Filter“ kann man den Filter beliebig anpassen, wie z.B. durch das Hinzufügen oder Entfernen von Filtergruppen. Durch einen Klick auf **“Filter bearbeiten”** wird der Bearbeitungsmodus aktiviert, durch **“Bearbeitung abschließen”** deaktiviert.



Über das Auswahlfeld können nun neue Filtergruppen hinzugefügt werden. Hierzu wird vorerst die gewünschte Filterart ausgewählt (im Beispiel ist das die Filtergruppe Siegel). Abgeschlossen wird der Vorgang durch **“Filtergruppe hinzufügen”**. Neu hinzugefügte Filtergruppen werden immer ganz unten im Filter eingereiht.

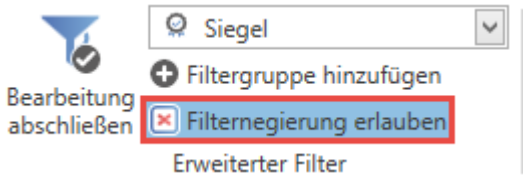
Im **Bearbeiten Modus** ändert sich, neben den möglichen Aktionen in der Ribbon, auch die Ansicht im Filter. Durch die Pfeiltasten wird bei Bedarf die Reihenfolge der Filtergruppen angepasst. Mit den Icons “Plus” und “Minus” können weitere Instanzen von bereits existierenden Filtergruppen erstellt, bzw. bestehende entfernt werden. Im nachfolgenden Beispiel wurde ein Inhaltsfilter hinzugefügt und alle weiteren Filtergruppen entfernt.



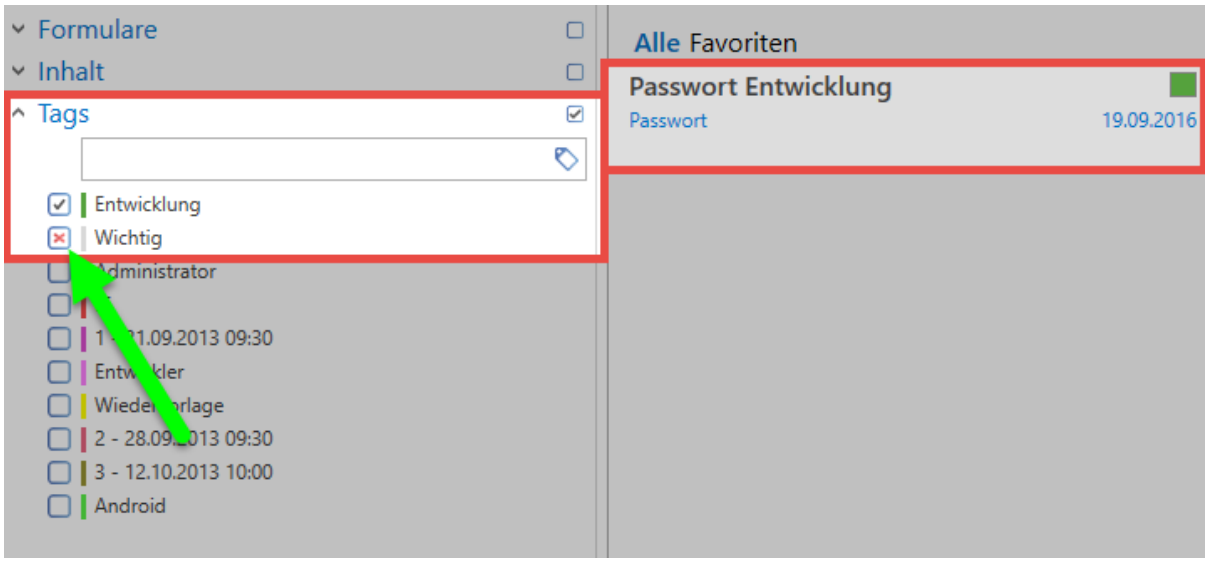

Im vorliegenden Beispiel wird ausschließlich der Inhaltsfilter genutzt – und das in zwei Instanzen! **Durch die aktivierte “Und-Verknüpfung” werden nun alle Datensätze angezeigt, bei denen sowohl das Wort “Passwort”, als auch der Ausdruck “Wichtig” enthalten sind.**

## Filternegierungen

Im Bearbeiten-Modus ist darüber hinaus die Möglichkeit gegeben, Kriterien zu negieren.




Man kann somit sehr exakt Filterergebnisse noch weiter verfeinern. Dies wird mit einer großen Zahl von in der Datenbank enthaltenen Datensätzen immer wichtiger, wenn trotz ausreichend gesetzter Filter die ausgegebene Menge an Daten nicht überschaubar ist.




Negierungen werden direkt in der Checkbox eines Elementes innerhalb einer Filtergruppe definiert. Ohne Negierungen hat man lediglich die Möglichkeit z.B. nach einem Tag zu suchen. Durch den Einsatz von Negierungen sind jetzt auch Abfragen wie folgend möglich:

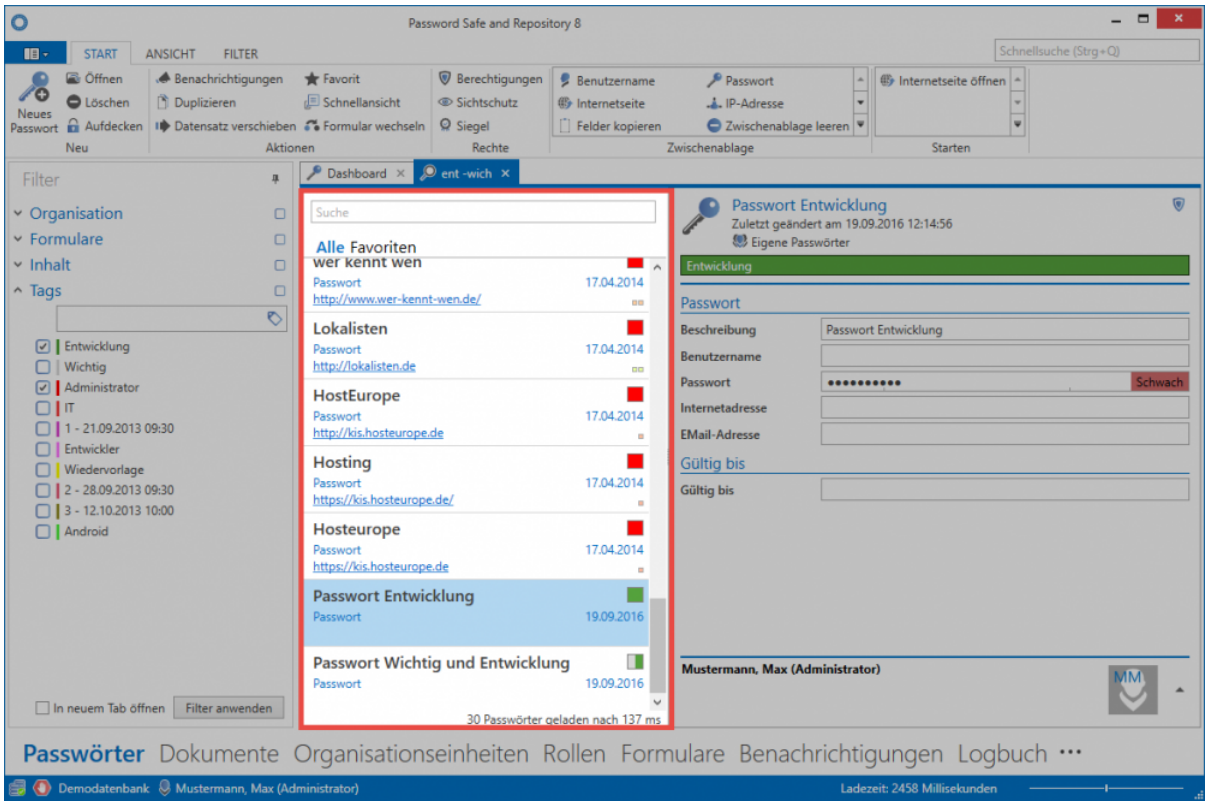
**“Liefere alle Datensätze, die das Tag “Entwicklung” haben, jedoch <u>nicht</u> mit “Wichtig” getaggt sind!”**

> **!** Um Negierungen effektiv nutzen zu können ist es wichtig, dass “Und-Verknüpfungen” stets aktiviert sind. Anders lassen sich Operationen mit Negierungen nicht mathematisch abbilden.

# Listenansicht

## Was ist die Listenansicht?

Zentral im Password Safe Client ist die Listenansicht zu finden und ist ein wesentlicher Bestandteil beim täglichen Arbeiten. Auch in Windows Betriebssystemen existieren Listenansichten. Klickt man im Windows Explorer auf einen Ordner, wird der Inhalt des Ordners in der Listenansicht wiedergegeben. Analog verhält es sich in Password Safe Version 8. Statt Ordnern wird jedoch der Inhalt der Listenansicht durch den aktuell angewendeten Filter definiert. **Dies bedeutet stets, dass die Listenansicht das Ergebnis eines durchgeführten Filters ist**. Zu dem in der Listenansicht aktuell markierten Datensatz werden im Lesebereich alle vorhandenen Formularfelder ausgegeben. Mit den beiden Reitern “Alle” und “Favoriten” kann zudem das Filterergebnis weiter eingeschränkt werden.



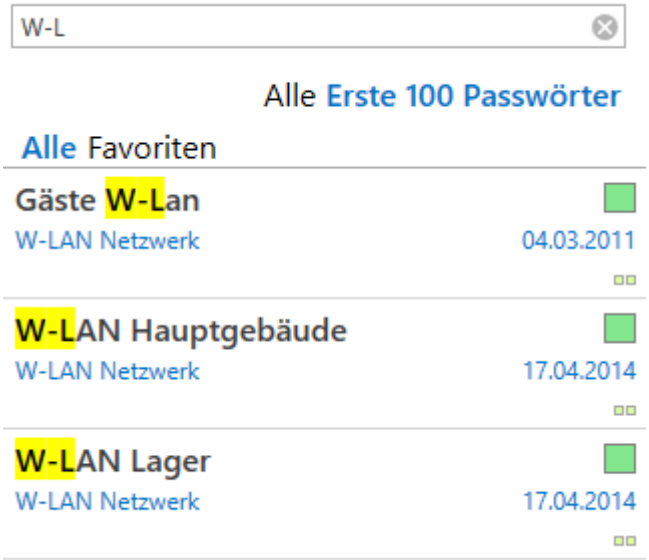

Unten in der Listenansicht wird die Anzahl der geladenen Datensätze sowie die hierfür benötigte Zeit angegeben.

> Bei mehr als 100 Listenelementen werden per default nur die ersten 100 Datensätze angezeigt. Dies soll verhindern, dass übermäßig große Datenbankabfragen stattfinden, bei denen die Ergebnismenge unüberschaubar ist. Es macht hierbei Sinn, die

Filterkriterien weiter zu verfeinern. Manuell kann durch betätigen des Buttons “Alle” im Header der Listenansicht dennoch auf die komplette Liste umgeschaltet werden.

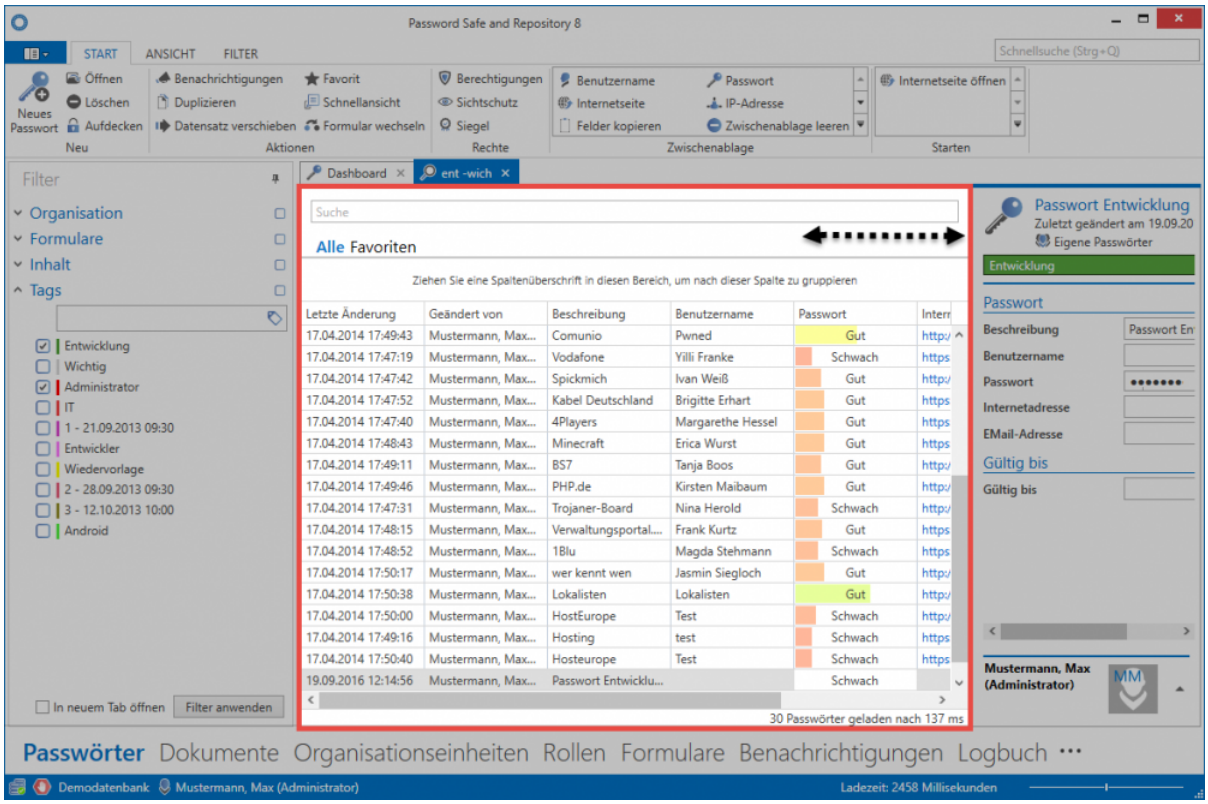
# Suche in der Listenansicht

Durch das Suchfeld können die durch den Filter gefundenen Ergebnisse bei Bedarf noch weiter verfeinert werden. Nachdem man den Suchbegriff eingegeben hat, wird automatisch (nach ca. einer halben Sekunde) die Ergebnismenge auf diejenigen Datensätze eingegrenzt, welche den Kriterien entsprechen. Der für die Suche genutzte Ausdruck wird gelb markiert.



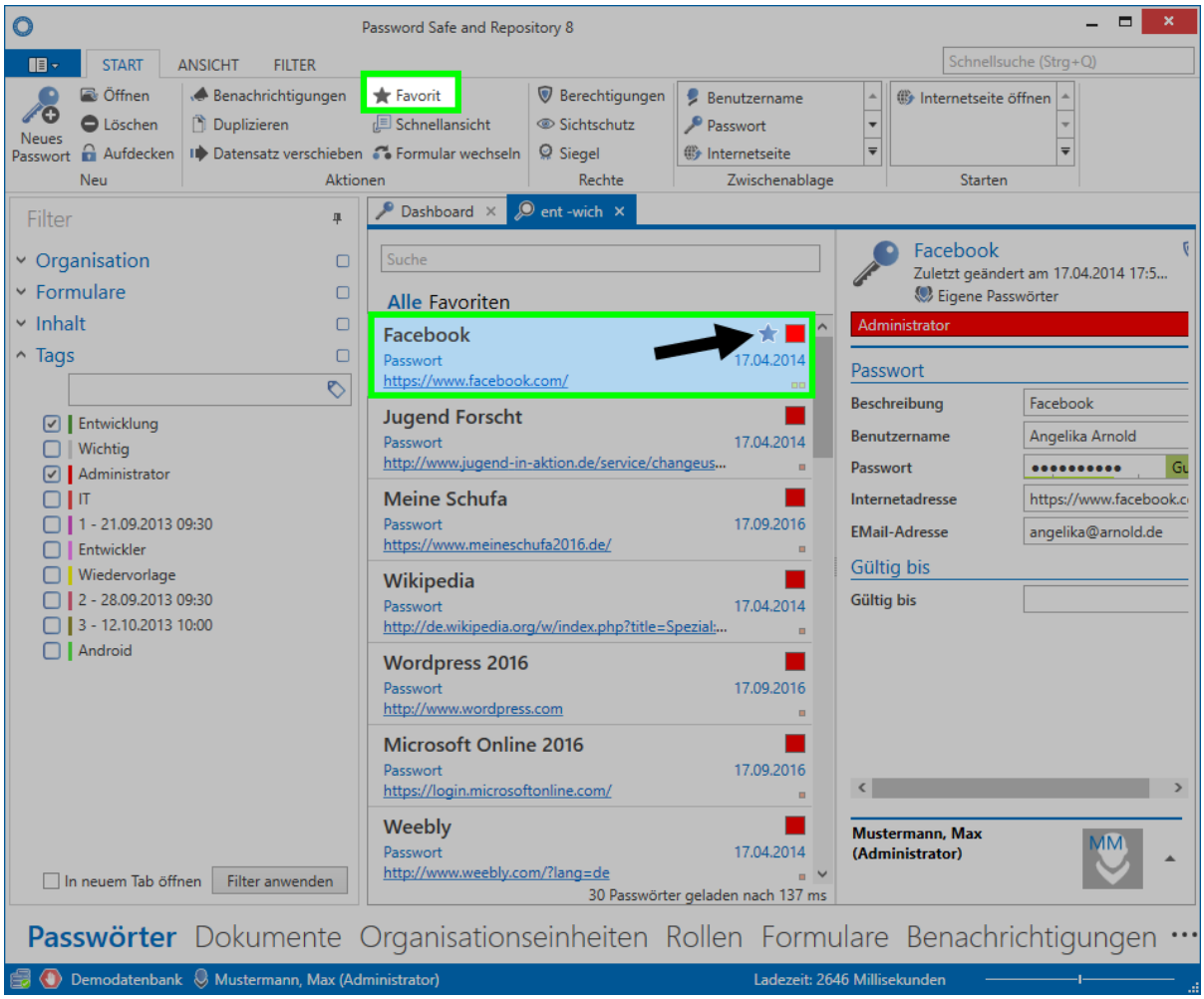

# Detaillierte Listenansicht

In der Standardansicht werden nur begrenzt Informationen über die Datensätze angezeigt. Die Breite der Listenansicht ist jedoch flexibel gestaltbar und kann per Maus justiert werden. Ab einem gewissen Punkt wechselt die Ansicht automatisch in die detaillierte Listenansicht, analog zur Vorgehensweise in Microsoft Outlook. Hierbei werden alle Formularfelder angezeigt

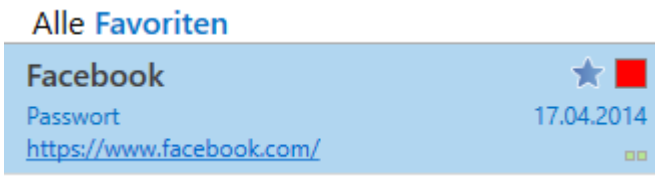



# Favoriten

Regelmäßig genutzte Datensätze können als Favorit markiert werden. Dieser Vorgang wird direkt in der Ribbon durchgeführt. Ein als Favorit markierter Datensatz wird in der Listenansicht mit einem Stern versehen.

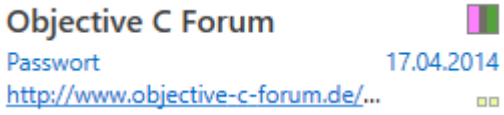



Das Filtern nach Favoriten erfolgt direkt in der Listenansicht. Hierzu wird einfach auf den Reiter **“Favoriten”** gewechselt.




# Weitere Symbole

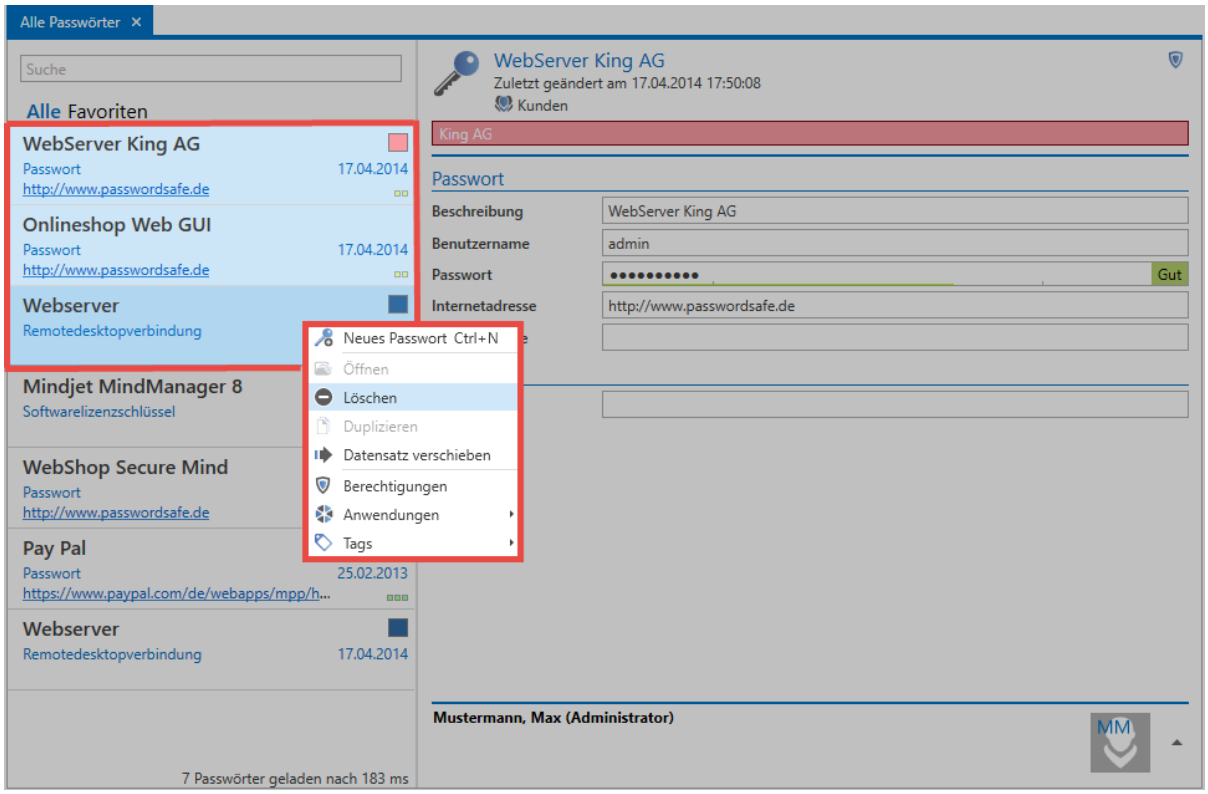
Jeder in der Listenansicht angezeigte Datensatz besitzt rechtsbündig mehrere Symbole. Diese geben farblich sowohl über die Passwortqualität, als auch die genutzten Tags Rückmeldung. Über Mouseover-Tooltips werden diese auch genau erläutert.



Die unterhalb des Passwort-Namens einsehbaren Informationen stammen aus dem Infofeld des zugehörigen Formulars und werden separat erläutert

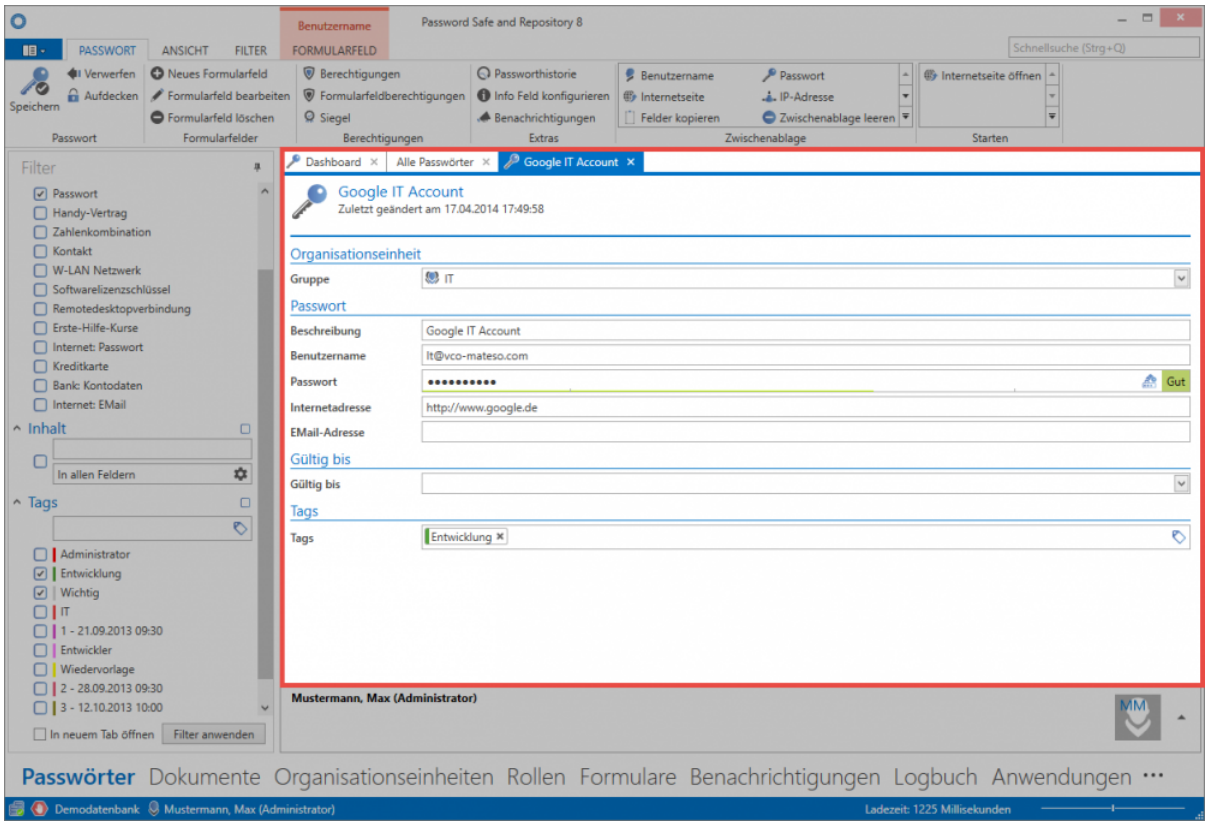
# Arbeiten mit Datensätzen

Alle den Filterkriterien entsprechenden Datensätze werden in der Listenansicht angezeigt. Diese können nun entweder über die Ribbon geöffnet, bearbeitet oder gelöscht werden. Viele Funktionen stehen auch direkt über das Kontextmenü zur Verfügung. Dies erreicht man über einen Rechtsklick auf den Datensatz. Hierbei ist ebenso Mehrfachauswahl möglich. Hierzu werden einfach, bei gedrückter Strg-Taste, die gewünschten Objekte markiert.




## Öffnen und Bearbeiten von Datensätzen

Durch einen Doppelklick, wie auch über das Kontextmenü (rechte Maustaste), können alle Datensätze aus der Listenansicht in einem eigenen Tab geöffnet werden. Nur in dieser Ansicht lassen sich Änderungen vornehmen. Diese Detailansicht öffnet sich in einem eigenen Tab, die Listenansicht wird hierdurch komplett verdeckt.

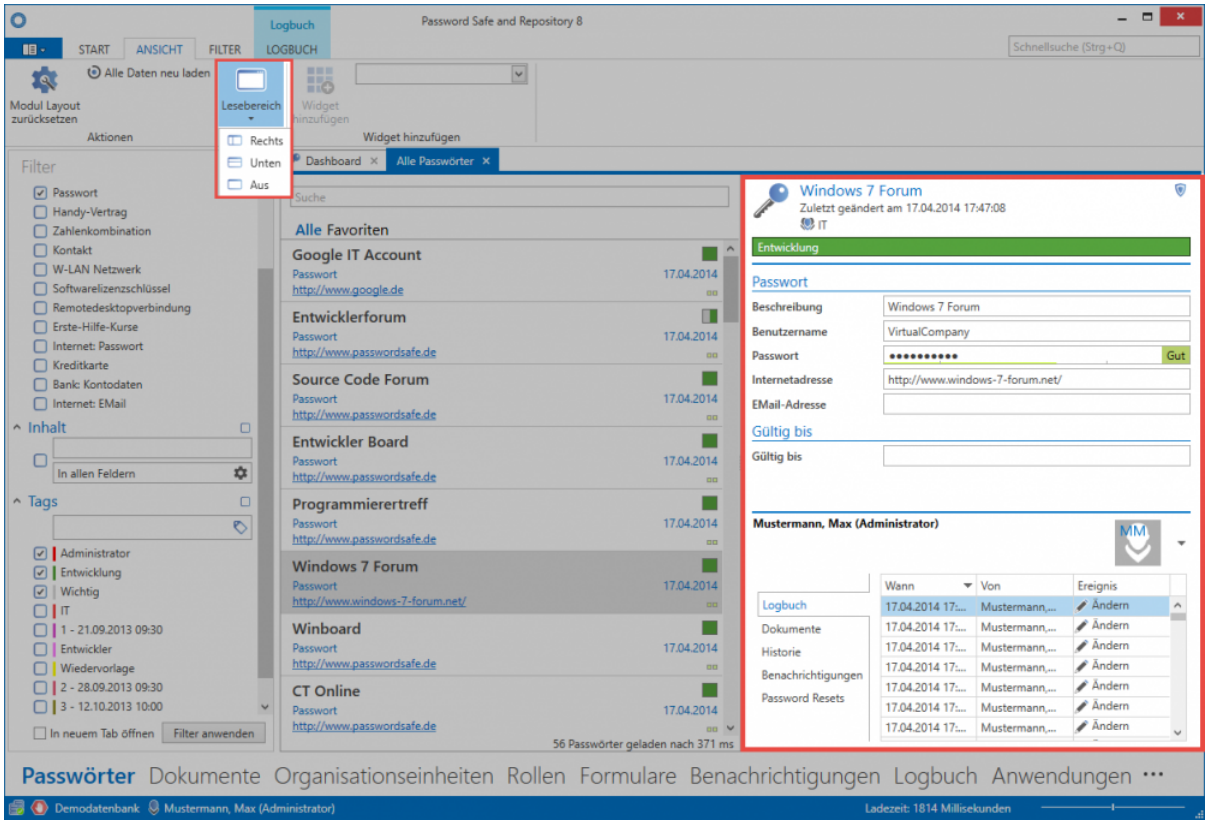



Das Arbeiten mit Datensätzen richtet sich natürlich stark nach der Art des Datensatzes. Egal ob Passwörter, Dokumente oder Organisationsstrukturen: Die Handhabe ist teils sehr unterschiedlich. Mehr Informationen hierzu entnehmen Sie deshalb bitte aus den jeweiligen Kapiteln über die einzelnen Module.

# Lesebereich

## Was ist der Lesebereich?

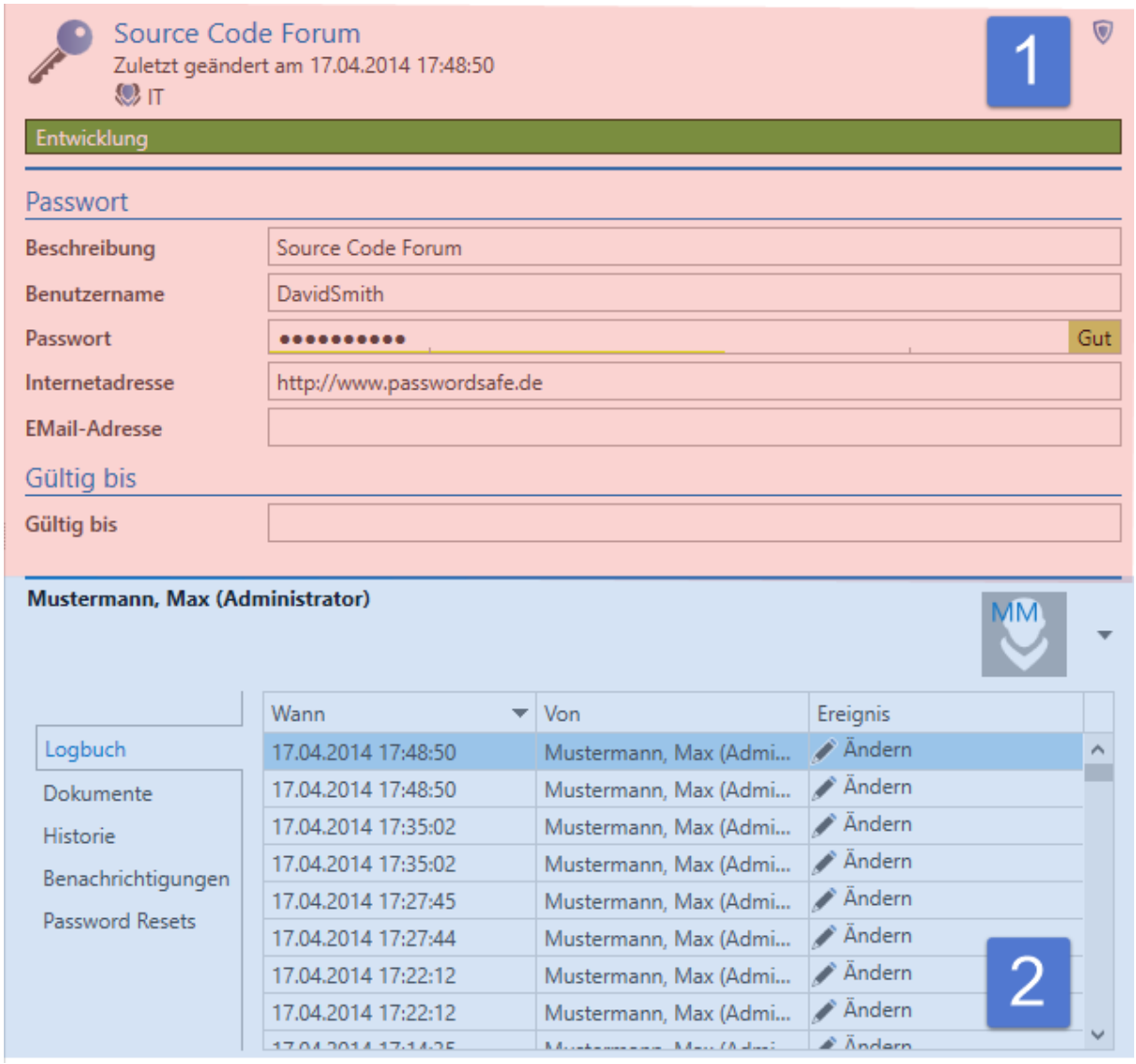
Der Lesebereich auf der rechten Seite des Clients entspricht stets der Detailansicht zu dem in der Listenansicht ausgewählten Datensatz. Der Lesebereich ist über die Ribbon komplett deaktivierbar. Zudem kann dort konfiguriert werden, ob die Anordnung des Lesebereich rechts, oder unterhalb der Listenansicht erfolgen soll.




## Unterteilung des Lesebereichs

Der Lesebereich ist in zwei Bereiche unterteilt:

1. **Detail-Bereich**
2. **Footer-Bereich**



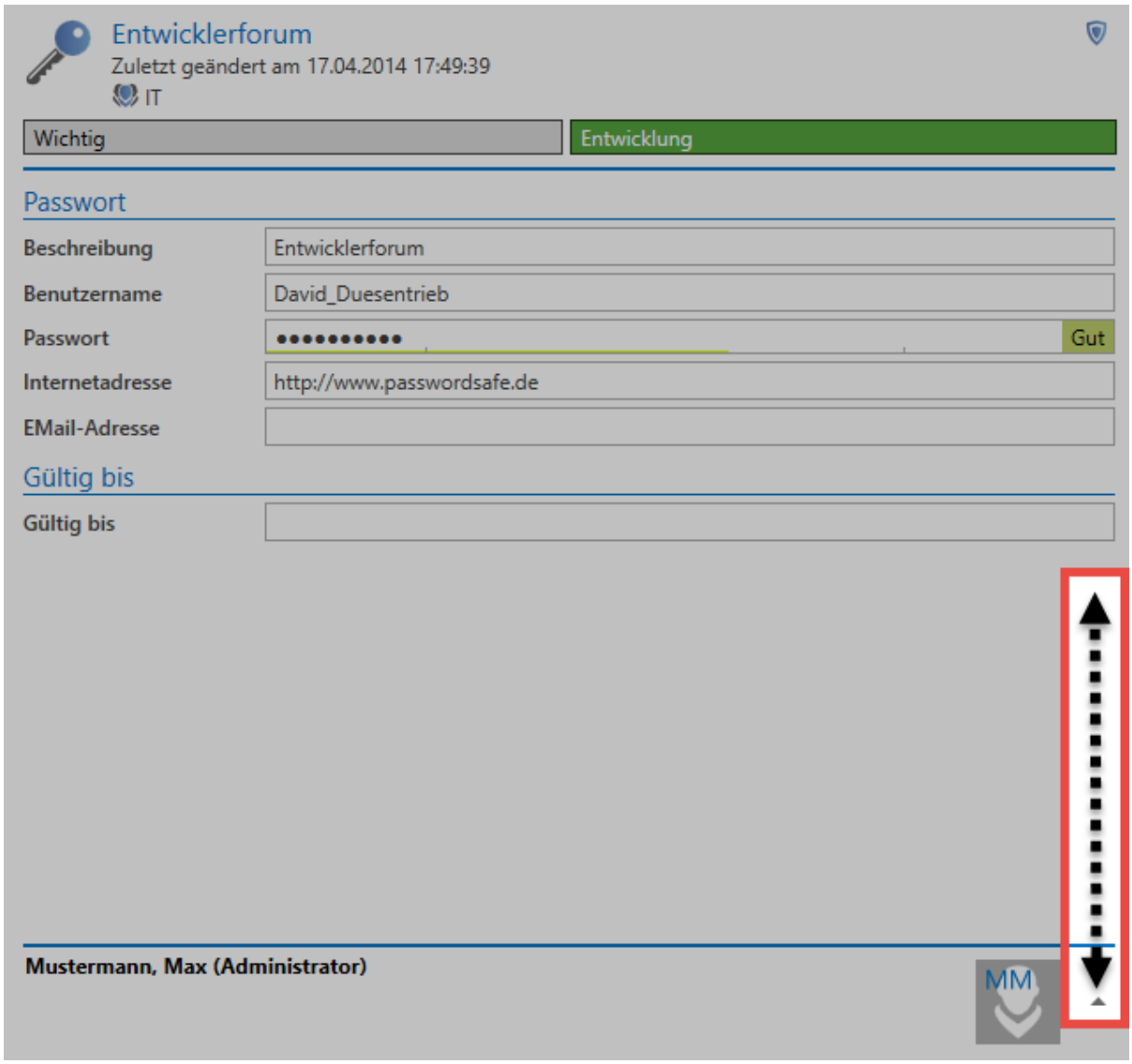

### 1. Detailbereich

Je nachdem welchen Datensatz Sie in der Listenansicht markiert haben, werden hier die dementsprechenden Felder angezeigt. In der Kopfzeile werden darüber hinaus auch die zugewiesenen Tags sowie Organisationsstrukturen angezeigt.

> **!** Es ist zu beachten, dass der Detail-Bereich nicht für das Bearbeiten von Datensätzen nutzbar ist! Dieser zeigt zwar alle Daten an – das Bearbeiten ist jedoch nur möglich, wenn der Datensatz geöffnet wurde.

### 2. Footer-Bereich

Im Footer-Bereich des Lesebereichs ist es möglich, sich für den aktuell ausgewählten Datensatz diverse Informationen anzeigen zu lassen. Über den hierfür vorgesehenen Button lässt sich dieser aktivieren, per default ist er ausgeblendet.




Der Zugang zum Logbuch, verknüpften Dokumenten, der Historie, Benachrichtigungen wie auch Password Resets sind hier separat über die Reiter erreichbar. Die einzelnen Elemente können sowohl über einen Doppelklick, als auch über die Schnellansicht (Leertaste) eingesehen werden. Beim Öffnen über Doppelklick öffnet sich stets ein separater Tab, die Schnellansicht öffnet lediglich ein modales Fenster.

! Die Sichtbarkeiten der einzelnen Reiter innerhalb des Footer-Bereichs sind über separate Benutzerrechte gesichert:

| Kategorie: Fußzeile Sichtbarkeit |
| --- |
| Kann in Fußzeile Historie sehen |
| Kann in Fußzeile Logbuch sehen |
| Kann in Fußzeile Dokumente sehen |
| Kann in Fußzeile die Metadaten von Dokumenten sehen |
| Kann in Fußzeile Benachrichtigungen sehen |
| Kann in Fußzeile Password Reset sehen |
| Kann in Fußzeile Mitgliedschaften sehen |

# Tags

## Was sind Tags?

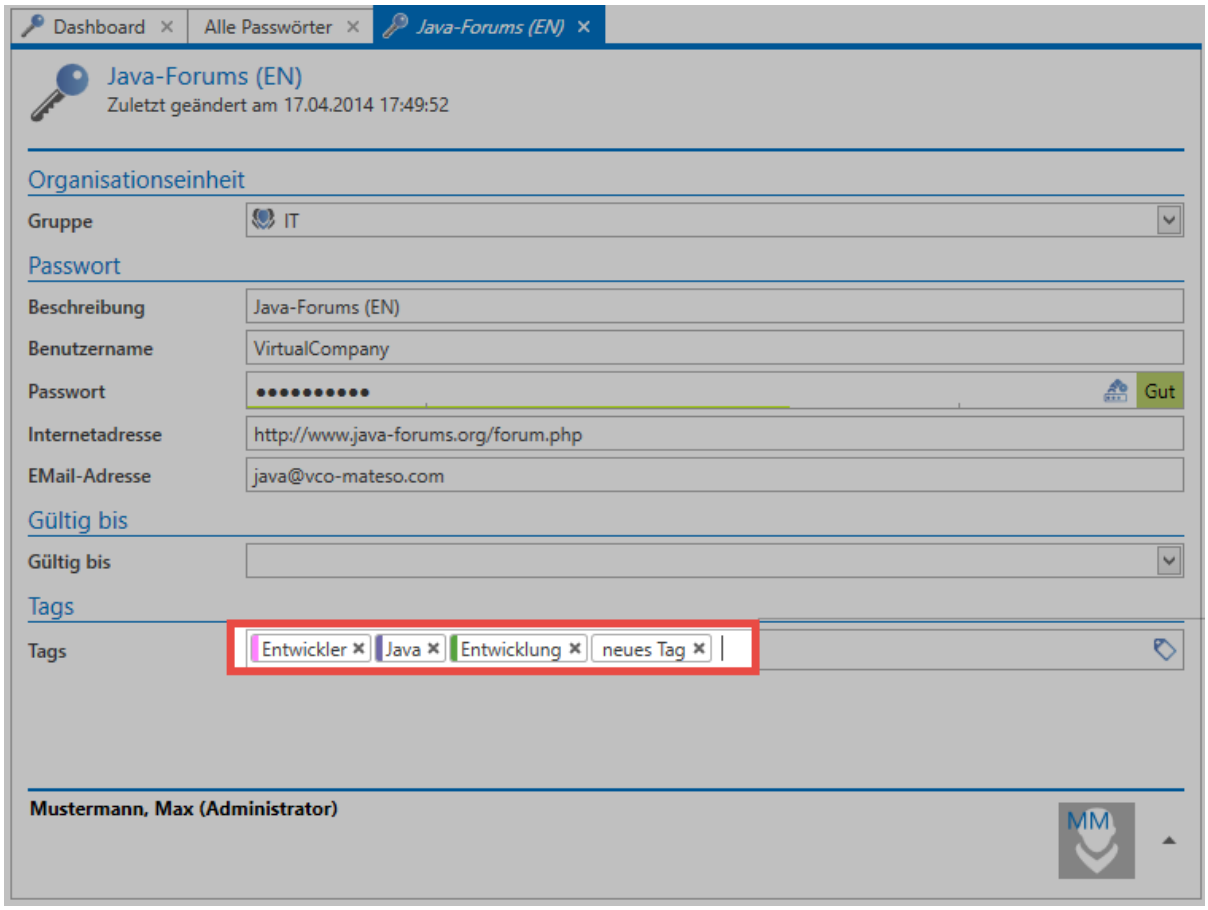
Das Tag-System ist im Password Safe allgegenwärtig. Fast jedes Objekt kann mit deren Hilfe klassifiziert und auch beschrieben werden. Ein Objekt kann mehrere solcher Tags besitzen. Diese werden immer im Kopfbereich des Datensatzes angezeigt. Optional können Tags mit Farben oder einem Beschreibungstext versehen werden. Sie prägen das Erscheinungsbild des Password Safe entscheidend und sind optisch eine große Hilfe, um auch in großen Datenmengen nicht den Überblick zu verlieren.

Tags besitzen keine Rechte – Jeder profitiert von allen Tags!

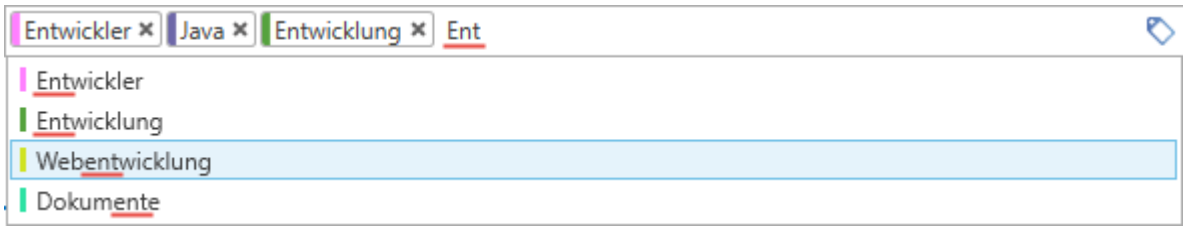
## Hinzufügen von Tags zu Datensätzen

Zum Erfassen neuer Tags ist das Recht **“Kann neue Tags anlegen”** erforderlich. Dieses Recht ist Teil der Benutzerrechte.

Tags können einerseits direkt bei der Erstellung neuer Datensätze, andererseits durch das Bearbeiten von Datensätzen hinzugefügt werden. Das Vorgehen ist hierbei identisch. Im Bearbeiten Modus finden sich die Tags stets an unterster Stelle.

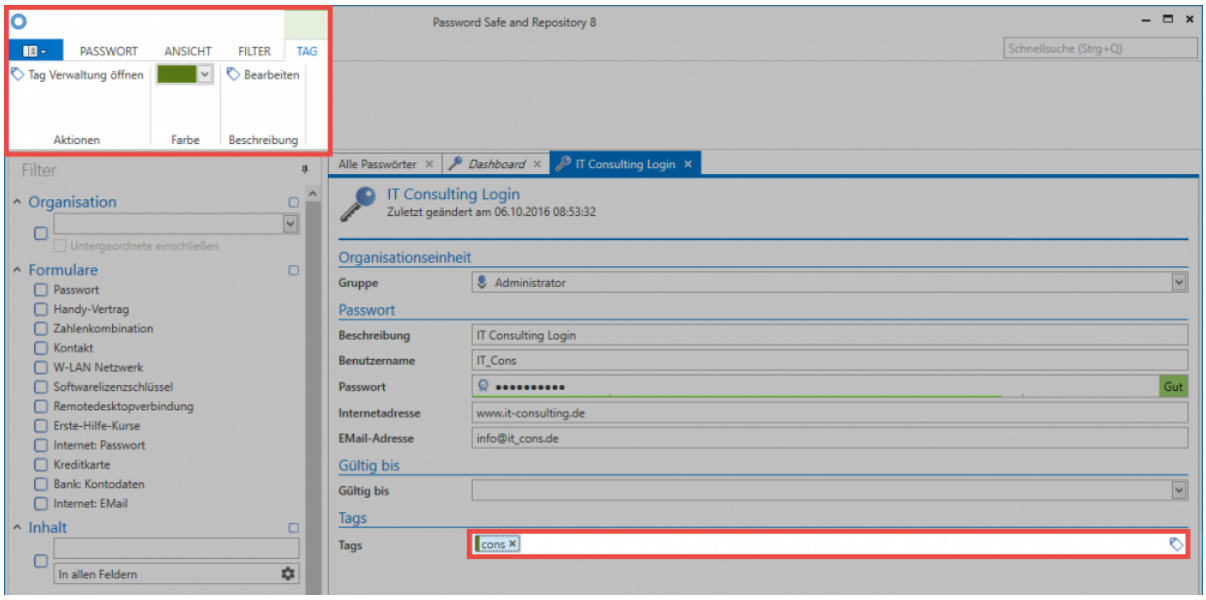



Die Bedienung ist hierbei intuitiv. Ab dem dritten eingegebenen Buchstaben werden bereits vorhandene Tags nach Volltext durchsucht. Falls der gewünschte Tag gefunden wurde, kann dieser hinzugefügt werden. Sowohl die Navigation mit Maus, also auch mit Tastatur, ist möglich. Falls ein neuer Tag angelegt werden soll, kann dies direkt mit “Return” durchgeführt werden.




# Tags in der Ribbon

Bearbeitet man einen Datensatz und markiert hierbei einen vorhandenen oder auch neuen Tag, erscheint in der Ribbon ein dementsprechendes Content Tab. Hier kann sowohl die Tagverwaltung geöffnet, als auch Farbe und Beschreibung des Tags direkt angepasst werden.




# Verwaltung von Tags

Für die Tagverwaltung steht in den Extras im Client ein separater Bereich zur Verfügung. Erläutert ist dieser in einem gesonderten Kapitel.

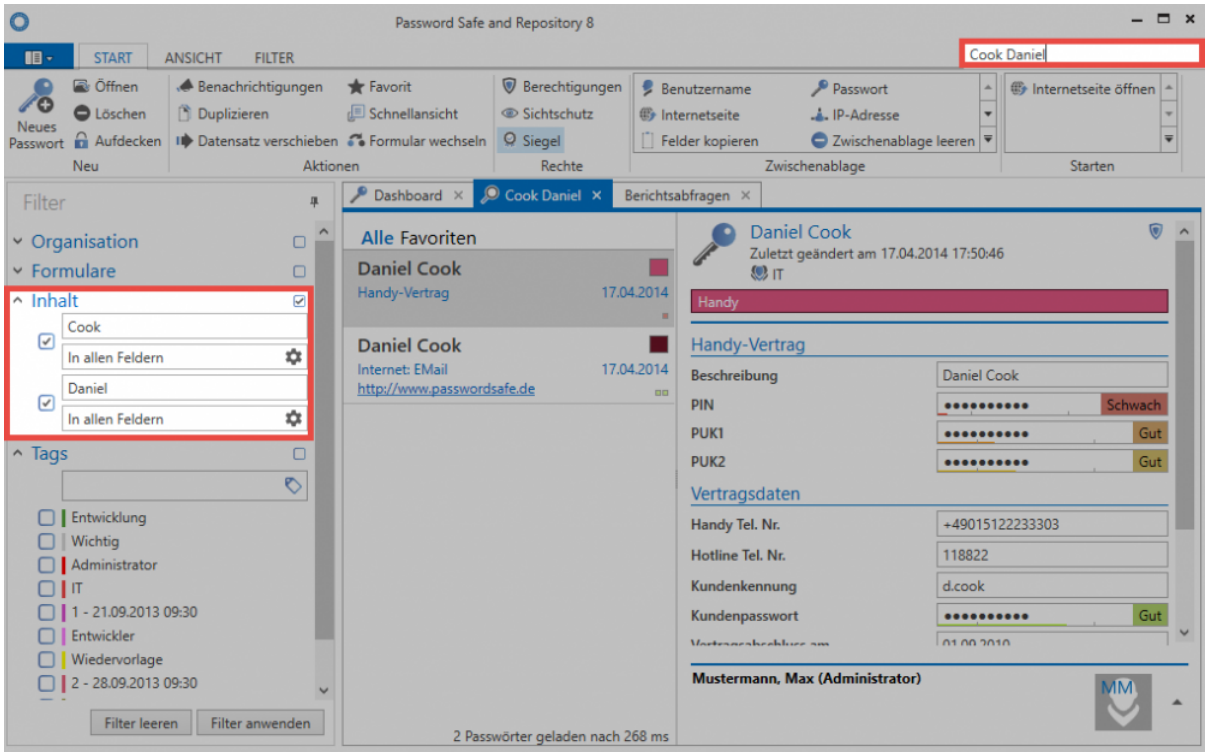
# Suche

## Was ist die Suche?

Mit Hilfe der Suche ist es möglich, in der Datenbank gespeicherte Daten effizient anhand gewählter Kriterien zu finden. Es existieren grundsätzlich 2 Suchmodi:

### 1. Schnellsuche

Rechts oben in der Ribbon steht jederzeit ein Suchfeld zur Verfügung, welches das aktuell geöffnete Modul durchsucht. Es handelt sich hierbei um eine Volltextsuche, die alle Felder und Tags außer dem Passwortfeld durchsucht.

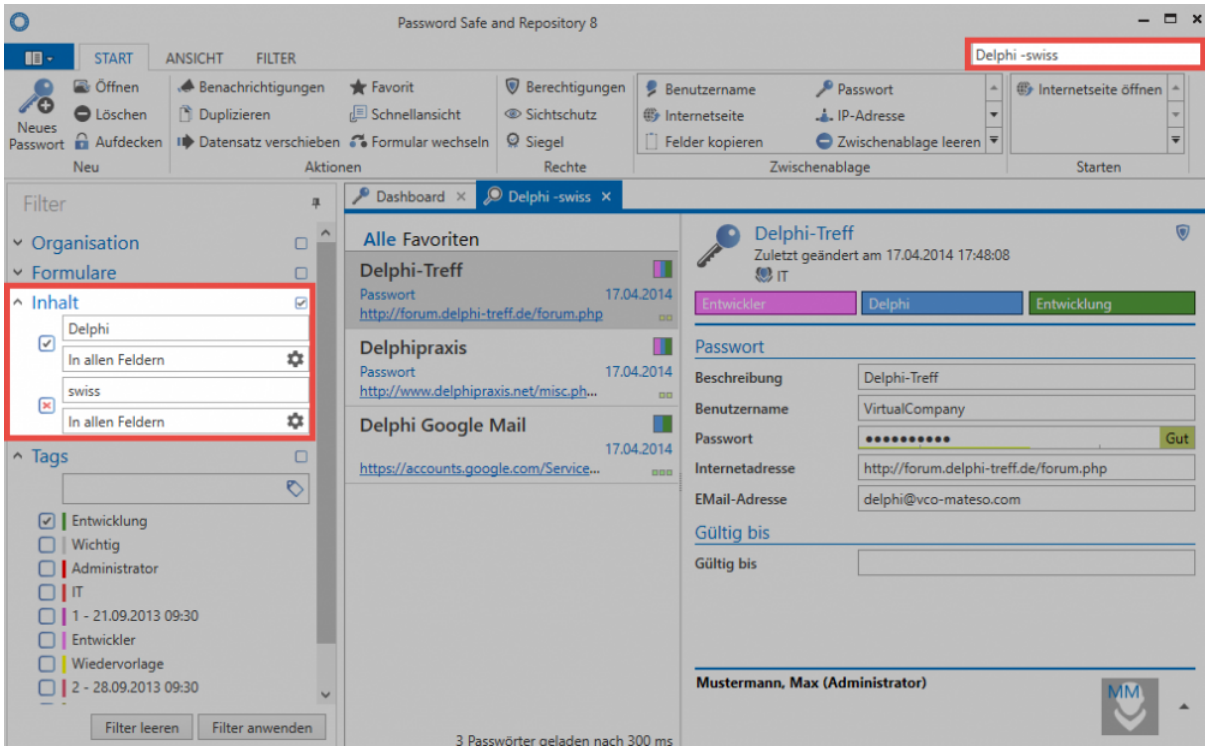



Die Schnellsuche ist eng mit dem Filter verbunden, da getätigte Suchanfragen direkt in einen oder mehrere Inhaltsfilter umgewandelt werden. Eine Suche kann auch mit durch Leerzeichen getrennten Begriffen durchgeführt werden, wie beispielsweise **Cook Daniel**. Es ist zu beachten, dass hierbei zwei getrennte Inhaltsfilter erstellt werden, welche logisch mit “und” verknüpft sind. Das bedeutet, dass beide Wörter im Datensatz vorkommen müssen. Die Reihenfolge spielt hierbei keine Rolle. Falls die Reihenfolge beachtet werden soll, muss man den Ausdruck in Anführungszeichen setzen: **“Cook Daniel”**. Die Suche ist nicht „case sensitiv“. Groß- und Kleinschreibung wird also nicht beachtet.

Über **Strg + Q** kann man direkt auf die Schnellsuche zugreifen!

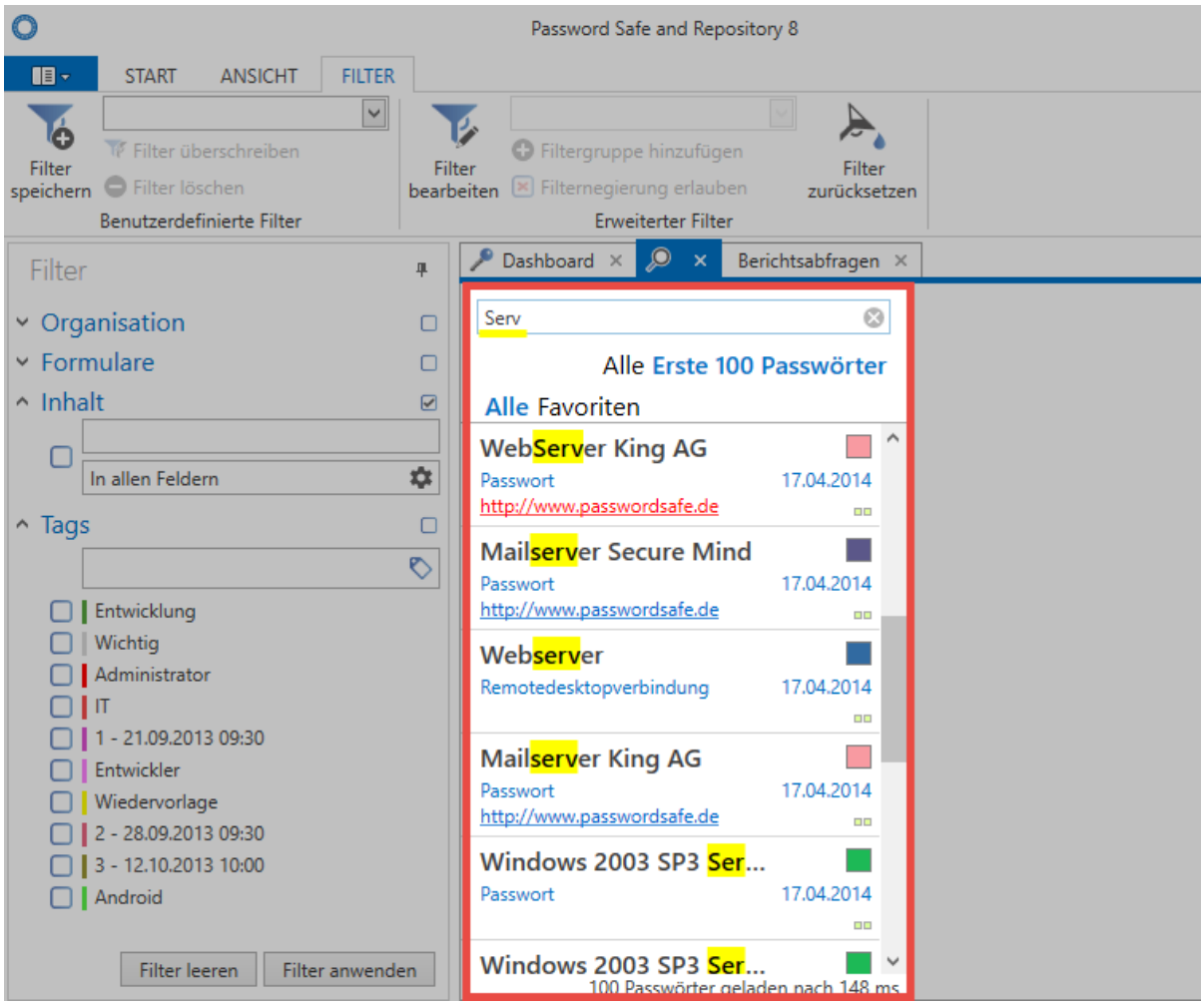
### Negierungen in der Schnellsuche

Negierungen schränken die Ergebnismenge dermaßen ein, dass bestimmte Kriterien nicht erfüllt sein dürfen. Im nachfolgenden Beispiel werden alle Datensätze gesucht, welche zwar den Ausdruck **Delphi** beinhalten, jedoch nicht den Ausdruck **swiss**. Die Notation, welche in der Schnellsuche eingegeben werden muss, lautet hierzu: **Delphi -swiss**




### 2. Listensuche

Mit der Listensuche im Header der Listenansicht kann die Ergebnismenge des Filters weiter durchsucht werden. Diese Art der Suche steht nahezu in jeder Liste zur Verfügung. Durchsucht wird nur die aktuell gefilterte Ergebnismenge. Passwortfelder werden nicht durchsucht. Die Suche ist live, daher wird mit jedem weiteren Zeichen, welches eingegeben wird, das Ergebnis weiter verfeinert. Es erfolgt automatisches “Highlighting” in gelber Farbe.




Beim Ausführen des Filters wird eine direkte Datenbankabfrage durchgeführt. Die Listensuche sucht lediglich innerhalb der bereits getätigten Abfrage.

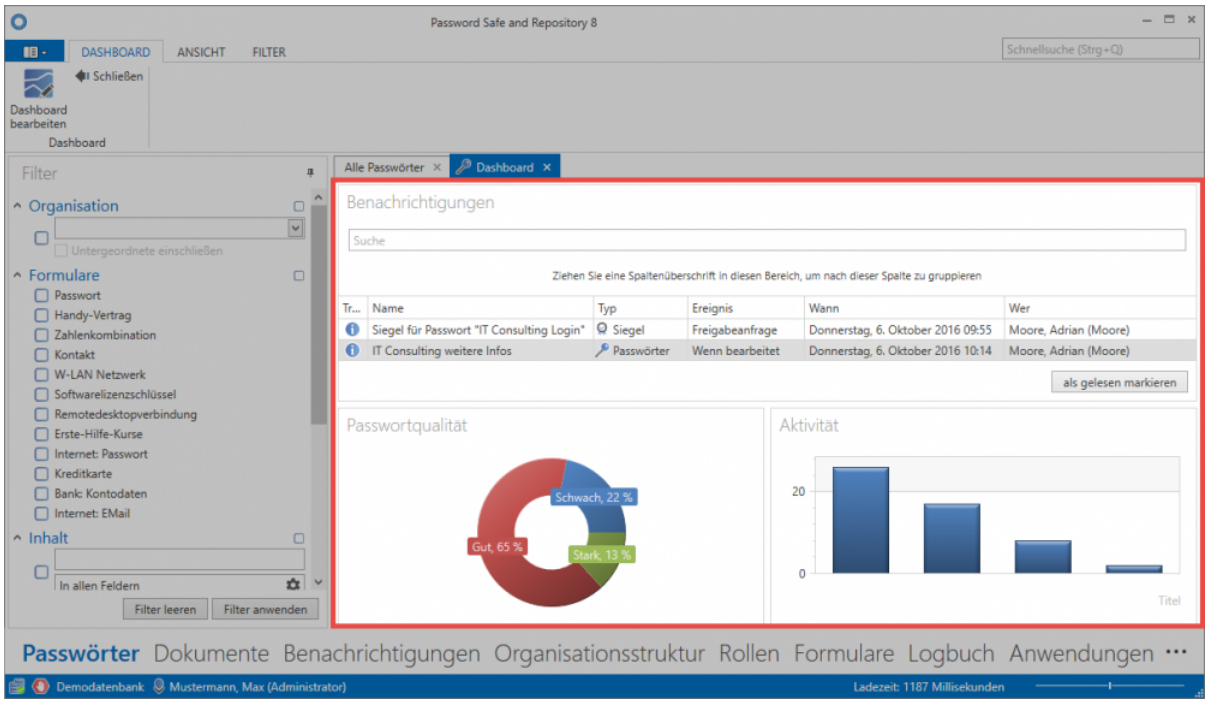
> Die Listensuche ist standardmäßig ausgeblendet und kann mit “**Strg + F**” aktiviert werden

# Dashboard und Widgets

> ! Aus Performancegründen ist das Dashboard per Standard deaktiviert. In den globalen Einstellungen kann die Option **“Dashboard beim Start anzeigen”** gesetzt werden.

## Was sind Dashboard und Widgets?

Die Menge der durch den Password Safe zur Verfügung gestellten Informationen kann besonders in großen Installationen erdrückend erscheinen. Dashboards erweitern die vorhandenen Filtermöglichkeiten um einen beliebig anpassbaren Info-Bereich, welcher visuell wichtige Ereignisse oder Fakten aufbereitet.



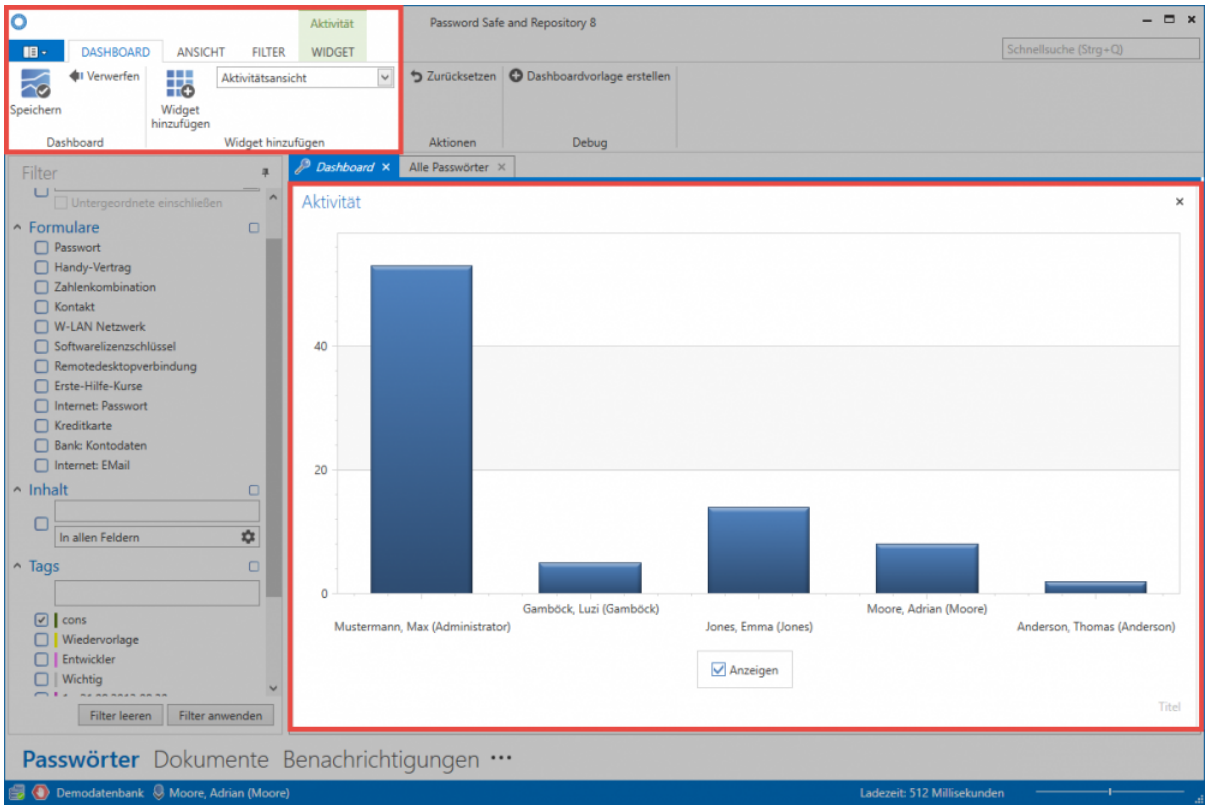

Dashboards sind in fast allen Client Modulen verfügbar. Für jedes einzelne Modul kann ein eigenes Dashboard festgelegt werden. **Widgets** entsprechen den einzelnen Modulen des Dashboards. Es existieren diverse Widgets, welche komplett individuell definierbar und auch separat konfigurierbar sind. Im obigen Beispiel sind drei Widgets aktiviert und geben Informationen über aktuelle Benachrichtigungen, Passwortqualität sowie Benutzeraktivität wieder. Die **maximale Anzahl der möglichen Widgets** wird in den Benutzereinstellungen verwaltet.

> * Das Dashboard kann über den Button im Tab geschlossen werden. Erneut angezeigt wird dieses über **Ansicht > Dashboard anzeigen** in der Ribbon!

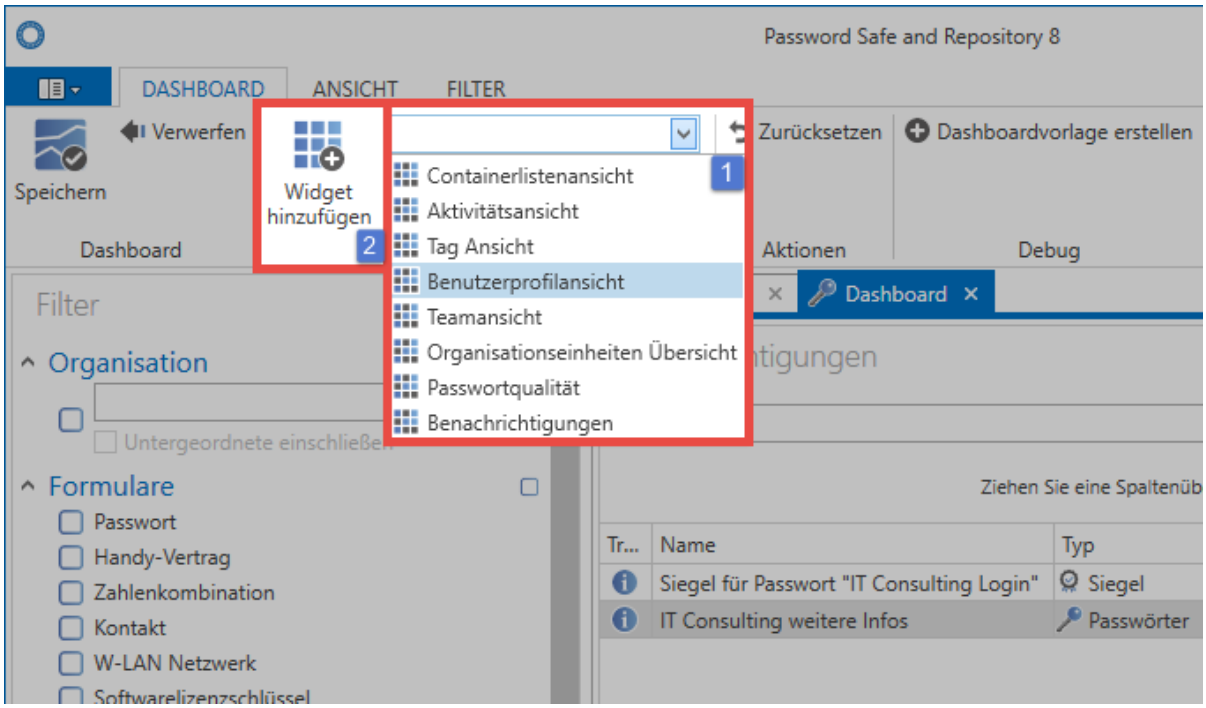
Die Anzeige des Dashboards ist grundsätzlich unkritisch, da der Benutzer nur diejenigen Daten einsehen kann, auf welche er auch berechtigt ist.

# Hinzufügen und Entfernen von Widgets

Bei aktiviertem Dashboard-Tab ist über die Ribbon der Bearbeitungsmodus für Dashboards aktivierbar. Das Hinzufügen sowie Bearbeiten von Widgets ist nur in diesem Modus möglich.

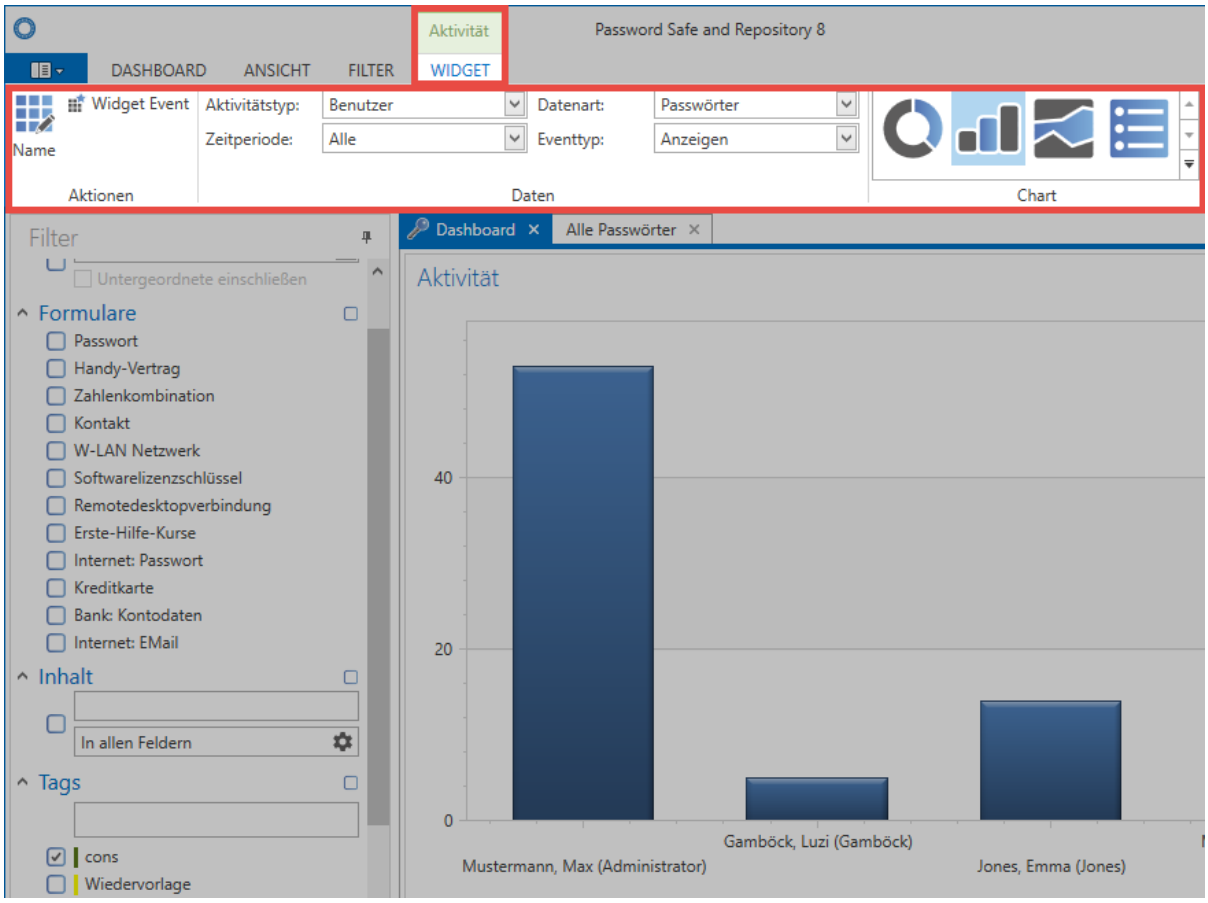



Über das Dropdown Menü wählt man nun das Widget aus, welches hinzugefügt werden soll **(1)**. Über den entsprechenden Button in der Ribbon **(2)** wird daraufhin das Widget dem Dashboard hinzugefügt. Die maximale Anzahl an Widgets, welche hinzugefügt werden können, sind in den Benutzereinstellungen konfigurierbar. Direkt im Dashboard kann im Bearbeitungsmodus jedes Widget auch wieder über die Schaltfläche am rechten oberen Rand entfernt werden. Beendet wird der Bearbeitungsmodus durch Speichern über die Ribbon.




# Anpassen von Widgets

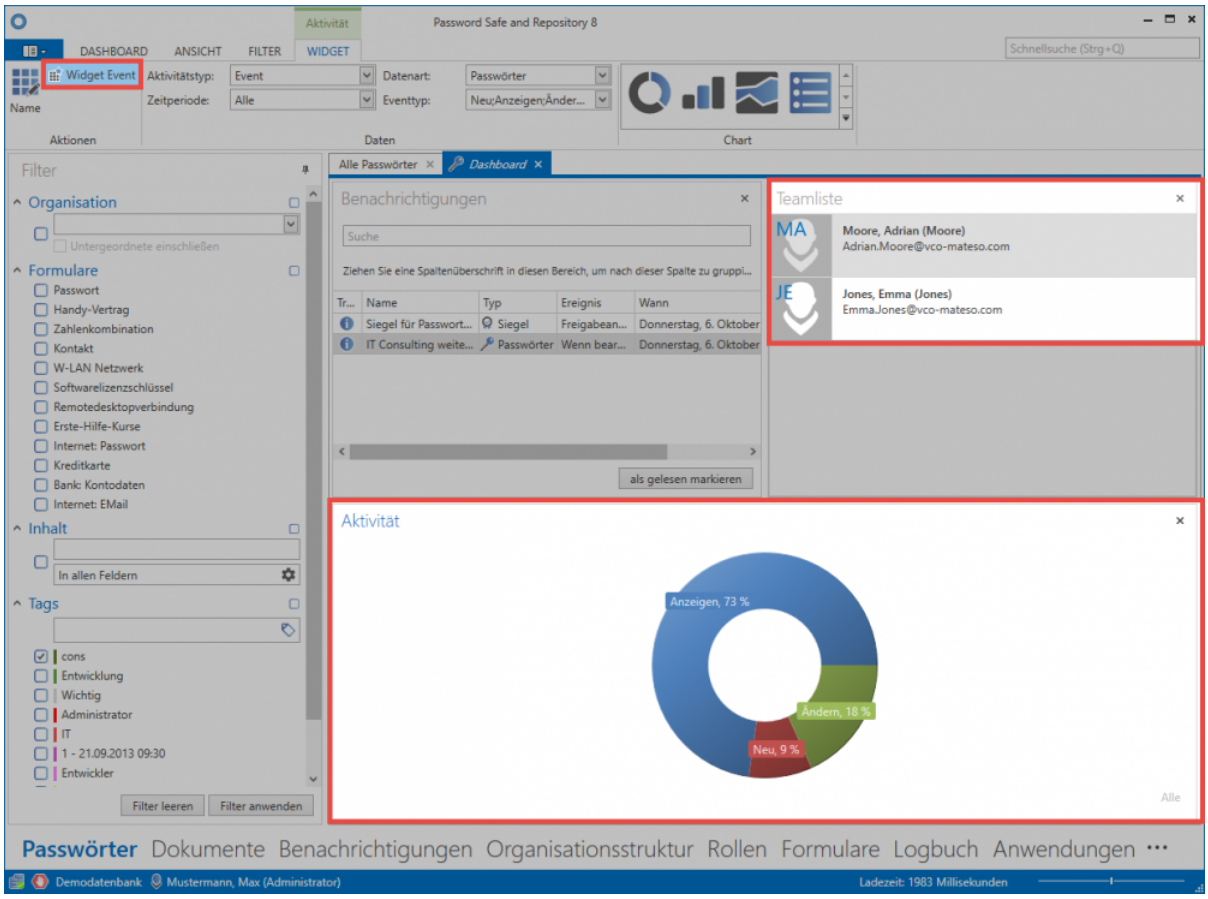
Im Bearbeitungsmodus kann man jedes Widget separat anpassen. Hierfür markiert man das Widget und wechselt in der Ribbon in das sich öffnende **Widget-Content-Tab**.




Für jedes Widget sind hier separate Variablen anpassbar. Im vorliegenden Beispiel wird angezeigt, wie oft sich Benutzer Passwörter angezeigt haben. Die Variablen sind natürlich je Widget individuell, da jeweils andere Informationen relevant sein können.

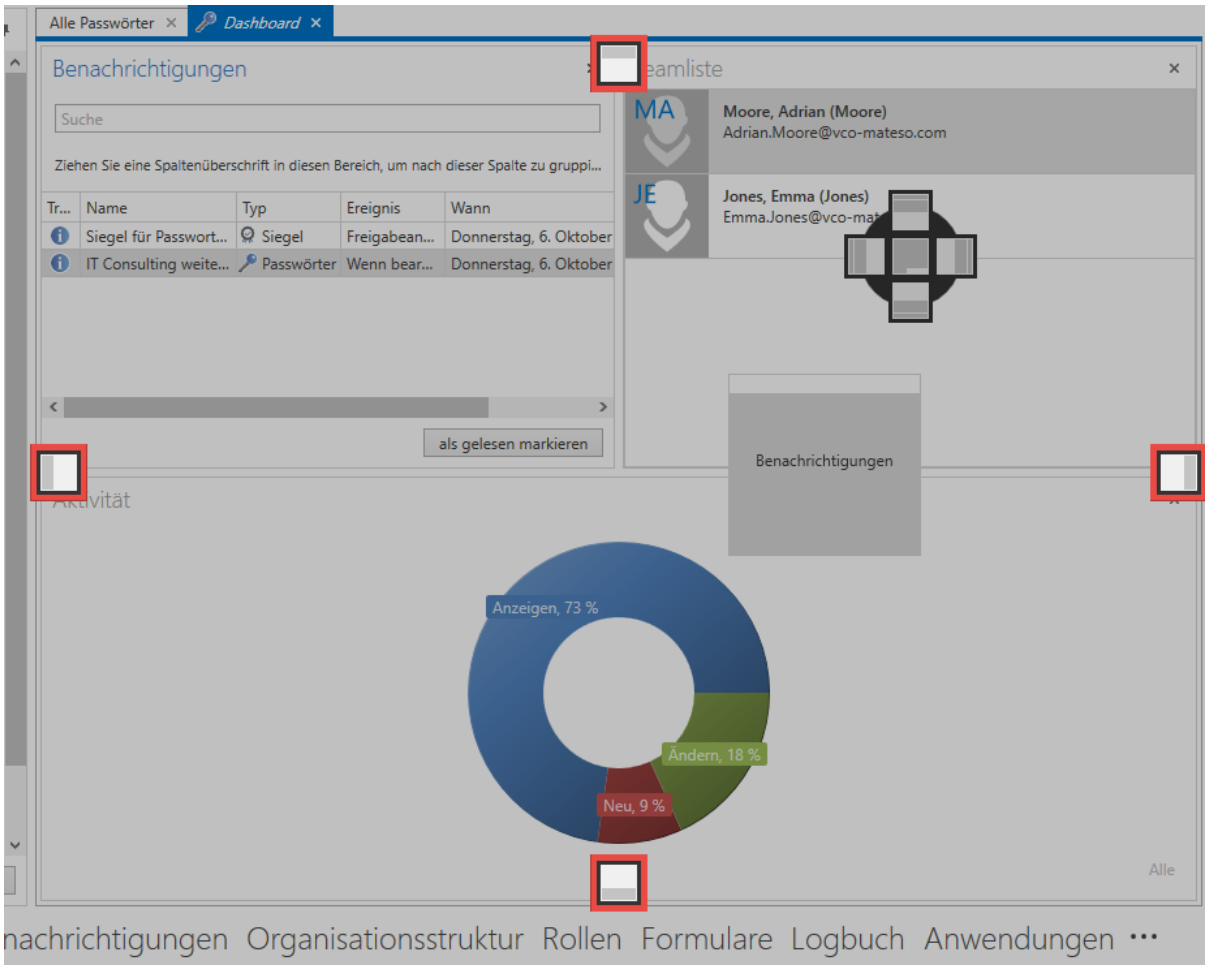
## Widget Event

In der Ribbon ist die Option **Widget Event** auswählbar. Hierdurch wird die Interaktion der Widgets untereinander aktiviert. In nachfolgendem Beispiel wurde dieses Feature für das Widget “Aktivität” aktiviert. Dies hat zur Folge, dass das Dashboard nicht nur alle Aktivitäten anzeigt, sondern diese auch nach dem im Widget **Teamliste** ausgewählten Benutzer filtert. Es handelt sich demnach um alle Aktivitäten des Benutzers “Moore”. Diese werden “live” gefiltert und in Echtzeit wiedergegeben.




# Anordnung der Widgets

Im Bearbeitungsmodus ist die Anordnung der Widgets frei definierbar. Durch Drag & Drop kann man ein Widget an den dementsprechenden Positionen (links, rechts, oben, unten) innerhalb des Dashboards positionieren.


Alle Passwörter
Dashboard
Benachrichtigungen
Suche
Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppi...
Tr...
Name
Typ
Ereignis
Wann
Siegel für Passwort...
Siegel
Freigabean...
Donnerstag, 6. Oktober
IT Consulting weite...
Passwörter
Wenn bear...
Donnerstag, 6. Oktober
als gelesen markieren
eamliste
MA
Moore, Adrian (Moore)
Adrian.Moore@vco-mateso.com
JE
Jones, Emma (Jones)
Emma.Jones@vco-mat
Benachrichtigungen
Aktivität
Anzeigen, 73 %
Ändern, 18 %
Neu, 9 %
Alle
nachrichtigungen
Organisationsstruktur
Rollen
Formulare
Logbuch
Anwendungen

# Tastaturkürzel

## Funktionsweise

Einige Aktionen können über Tastaturkürzel (Shortcuts) effizient ausgeführt werden. Konfiguriert werden diese im gleichnamigen Bereich innerhalb der globalen Benutzereinstellungen.

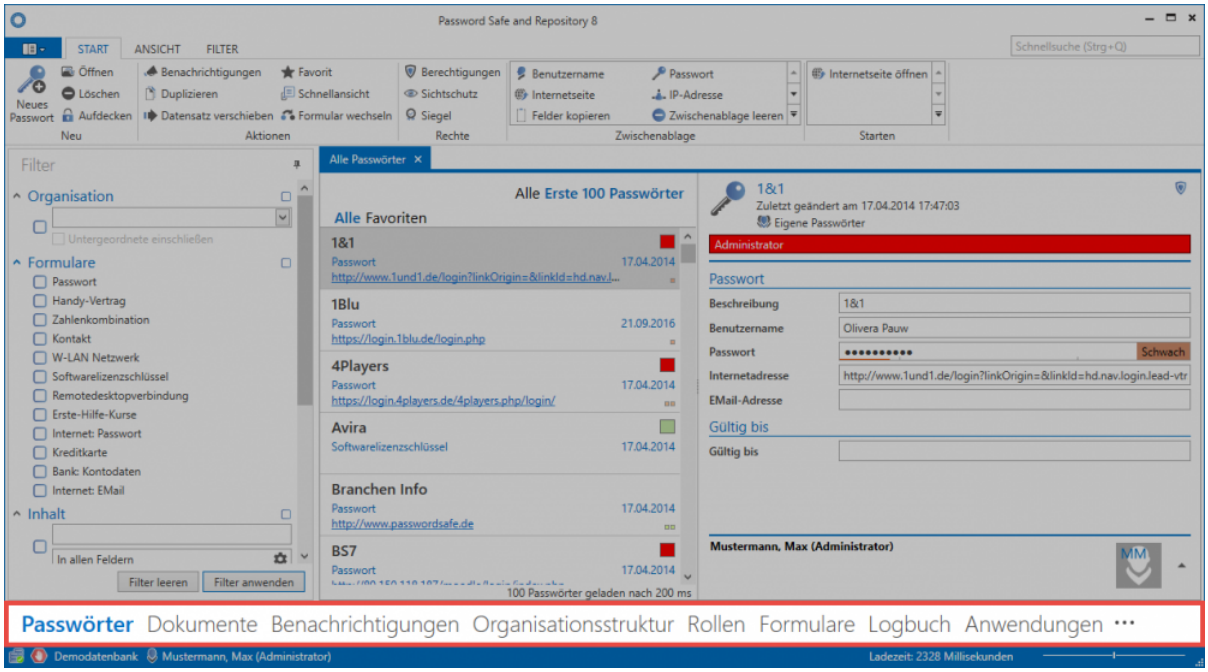
Folgende Tastaturkürzel sind verfügbar:

- **STRG+ ALT + U** übergibt den Benutzernamen aus dem selektierten Datensatz per Skript an das aktive Fenster
- **STRG+ ALT + S** startet ein Skript, welches aus dem selektierten Datensatz zunächst den Benutzernamen an das aktive Fenster übergibt. Anschließend wird ein TAB Sprung ausgeführt und das Passwort übergeben.
- **STRG+ ALT + P** trägt das selektierte Passwort über ein Skript in das aktive Fenster bzw. Feld ein
- **STRG+ ALT + R** übergibt per Eingabetaste aus dem selektierten Datensatz zunächst den Benutzernamen an das aktive Fenster. Anschließend wird ein TAB Sprung ausgeführt und das Passwort übergeben.

# Client Module

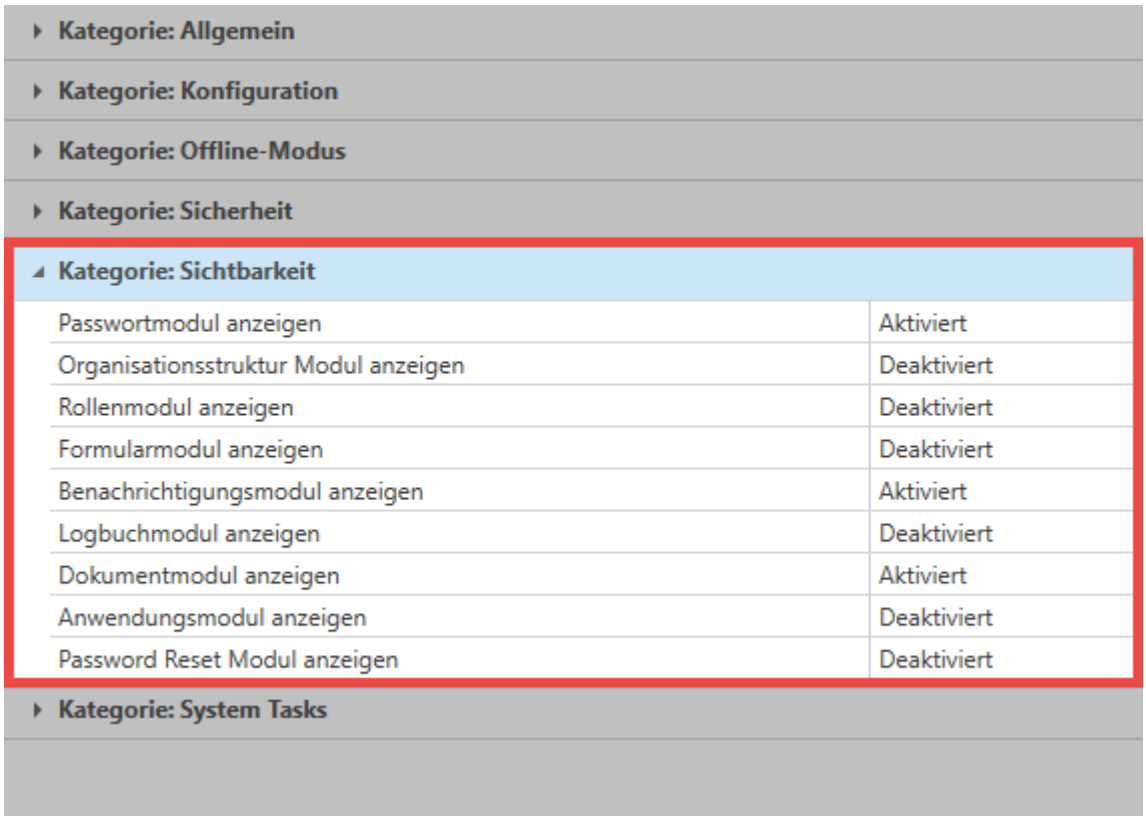
## Was sind Module?

Password Safe kann je nach Anforderung den speziellen Bedürfnissen der Benutzer angepasst werden. Diese Anforderung kann sowohl vom Benutzer ausgehen also auch durch administrative Benutzer aufgetragen sein. Das bedeutet, dass jeder nur genau jene Funktionalitäten erhält, die für seine speziellen Arbeiten auch erforderlich sind. Der Umfang an benötigten Features unterscheidet sich bei einem Administrator erheblich von denen eines normalen Anwenders. Der **modulare Aufbau** von Password Safe unterstützt diesen Ansatz indem nur genau jene Bereiche sichtbar sind, die auch wirklich vom jeweiligen User genutzt werden sollen.




## Sichtbarkeit von Modulen

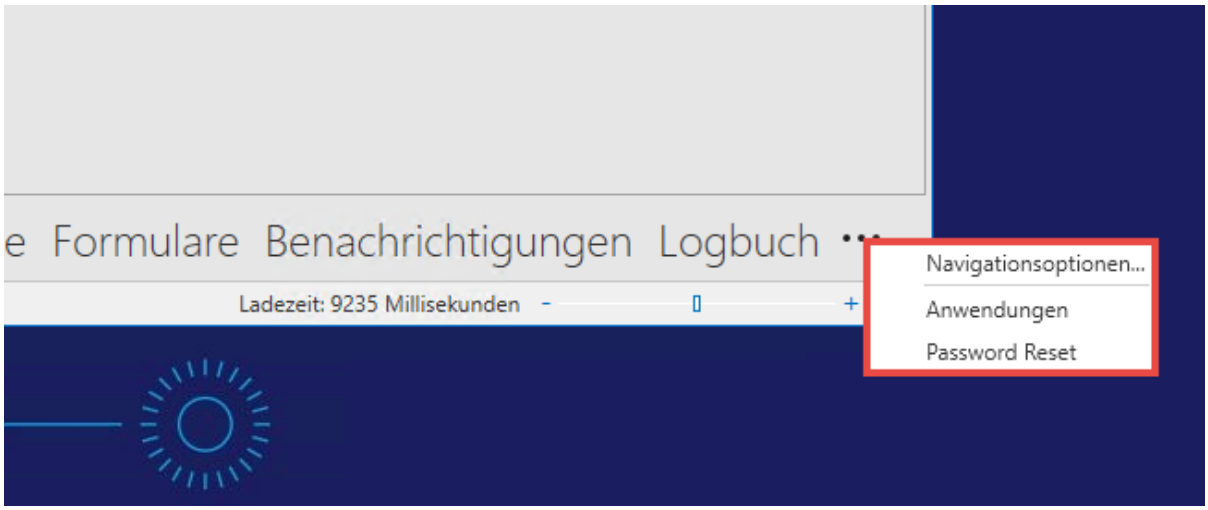
Die Module sind das Tor zu den diversen Features der Version 8. Analog zu den Features müssen demnach auch nicht alle Module allen Benutzerschichten zur Verfügung gestellt werden. Innerhalb der Benutzerrechte kann die **Sichtbarkeit der Module** individuell definiert werden.



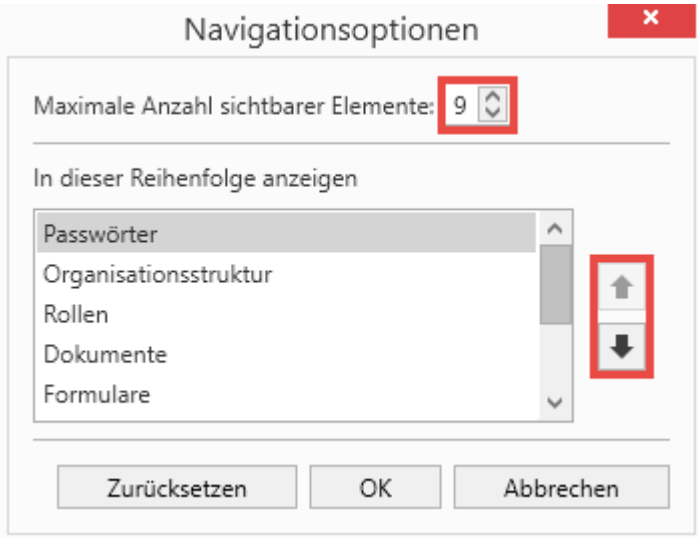

Die Sichtbarkeit der Module ist stets an die Bedürfnisse der individuellen Benutzergruppen anpassbar

## Sortierung der Module

Am rechten, unteren Ende der im Client dargestellten Module erreicht man über die drei Punkte das Menü “Navigationsoptionen”. Ebenso werden dort auch diejenigen Module angezeigt, auf die man gemäß der zuvor erläuterten Sichtbarkeit zwar berechtigt ist, welche jedoch z.B. aufgrund der Skalierung der Client-Größe ausgeblendet sind (im Beispiel Anwendungen und Password Reset).




Innerhalb der Navigationsoptionen können sowohl die maximale Anzahl der sichtbaren Elemente wie auch deren Sortierung definiert werden.




Die zuvor behandelte Sichtbarkeit von Module ist Grundvoraussetzung, um diese innerhalb der Navigationsoptionen sehen und sortieren zu können

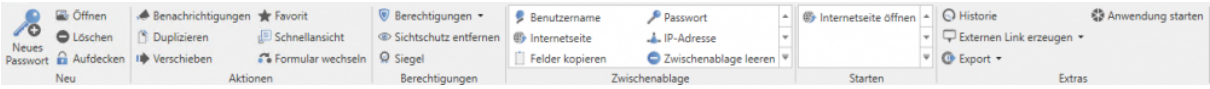
# Passwörter

## Was sind Passwörter?

In Password Safe v8 stellt der Datensatz mit den darin enthaltenen Passwörtern das zentrale Datenobjekt dar. Das Modul Passwörter liefert sowohl für Administratoren als auch Endbenutzer den zentralen Zugang für den täglichen Umgang mit diesen sensiblen und schützenswerten Daten. Frei definierbare Suchfilter im Zusammenspiel mit farblich hervorgehobenen Tag-Markierungen auf Datensätzen ermöglichen zielführendes Arbeiten. Mit Hilfe diverser Ansätze kann die gewünschte Form der Berechtigung an Objekten angebracht werden. Zudem unterstützt der ergonomisch strukturierte Aufbau des Moduls alle Benutzer im effizienten und zielgerichteten Arbeiten mit dem Password Safe. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert.


## Modulspezifische Ribbonfunktionen

Eine große Stärke der Ribbon ist es, stets situationsgerecht alle möglichen Aktionen anzubieten. Besonders innerhalb des Moduls **Passwörter** spielt die Ribbon mit einer Vielzahl von modulspezifischen Funktionen eine zentrale Rolle. Allgemeine Informationen zum Thema Ribbon stehen im hierfür vorgesehenen Kapitel bereit. Nachfolgend soll auf die modulspezifischen Ribbonfunktionen eingegangen werden.



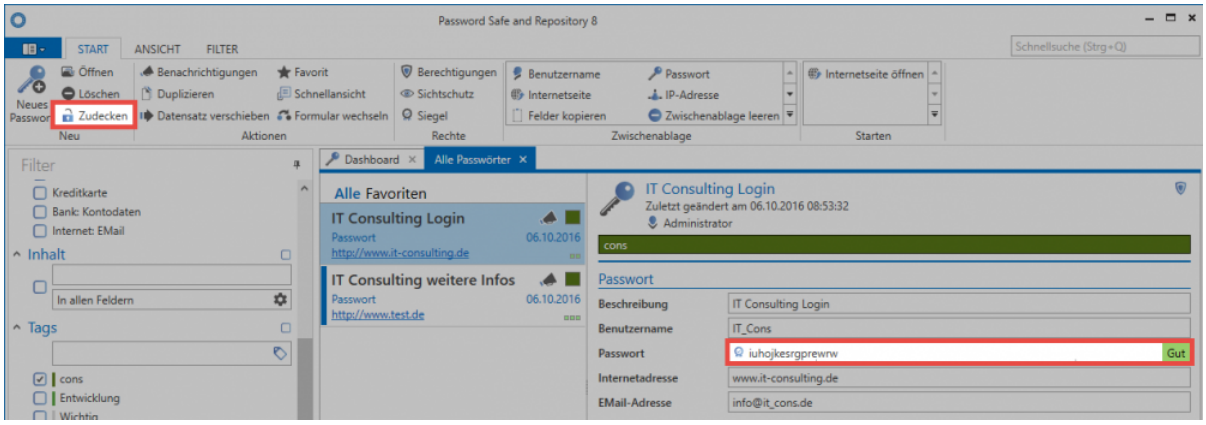

### Neu

- **Neues Passwort:** Sowohl über dieses Icon in der Ribbon als auch über das Kontextmenü der rechten Maustaste können neue Datensätze angelegt werden. Darüber hinaus ist der Shortcut “Strg + N” das vorgesehene Tastenkürzel. Der nächste Schritt ist die Auswahl eines geeigneten Formulars.

> ! Es wird das Benutzerrecht **Kann neue Passwörter anlegen** benötigt!

- **Öffnen**: Öffnet das in der Listenansicht markierte Objekt und gibt weitere Informationen des Datensatzes im Lesebereich wieder
- **Löschen** Entfernt das in der Listenansicht markierte Objekt. Es wird ein Logfile-Eintrag erstellt. (s. Logbuch)

- **Aufdecken**: Bei allen Datensätzen, die ein Passwortfeld besitzen, kann die Funktion Aufdecken genutzt werden. Hierbei werden die Passwörter im Lesebereich aufgedeckt und sind einsehbar. Im Beispiel ist dieses aufgedeckt, und kann über den Button **Zudecken** wieder verdeckt werden.




## Aktionen

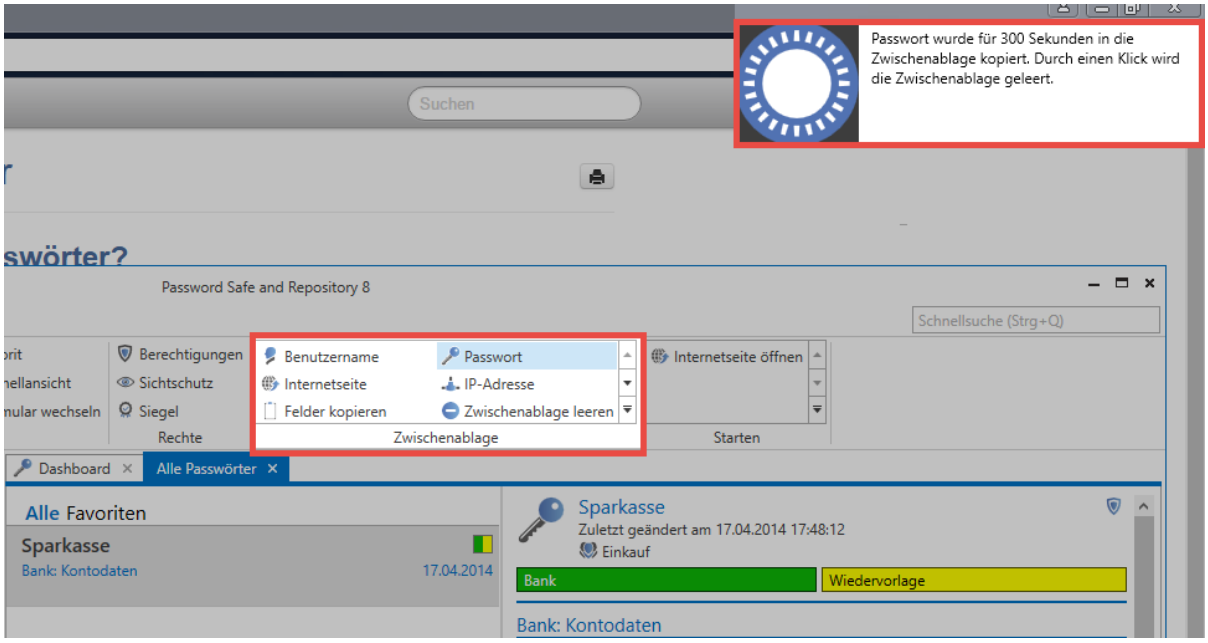
- **Benachrichtigungen**: Die Definition von Benachrichtigungen ermöglicht den stetigen Informationsfluss bei jedweder Form von Änderungen an Datensätzen. Die Ausgabe der Benachrichtigungen erfolgt in dem hierfür vorgesehenen Modul.
- **Duplizieren**: Das Duplizieren von Datensätzen erstellt eine exakte Kopie des in der Listenansicht markierten Datensatzes. Dies betrifft sowohl alle gespeicherten Informationen als auch definierten Berechtigungen.
- **Verschieben**: Verschiebt den in der Listenansicht markierten Datensatz in eine andere Organisationsstruktur. Mehr…
- **Favorit**: Der ausgewählte Datensatz wird als Favorit markiert. Oberhalb der Listenansicht kann jederzeit zwischen allen Datensätzen und Favoriten ausgewählt werden.
- **Schnellansicht**: Für den ausgewählten Datensatz öffnet sich 15 Sekunden lang ein modales Fenster mit allen verfügbaren Informationen **inklusive dem Wert des Passwortes**.
- **Formular wechseln**: Es ist möglich, für einzelne Datensätze das bisher genutzte Formular zu wechseln. Das “Mapping” der bisherigen Formularfelder kann direkt im sich öffnenden, modalen Fenster vorgenommen werden.

## Berechtigungen

- **Berechtigungen**: Sowohl Passwortberechtigungen als auch Formularfeldberechtigungen können über das sich öffnende Drop-Down Menü gesetzt werden. Über diesen Weg ist einzig die manuelle Berechtigung von Daten möglich. (s. Berechtigungskonzept)
- **Sichtschutz**: Das Verdecken von schützenswerten Passwörtern gegenüber unbefugten Benutzern stellt ein wesentliches Feature innerhalb des Sicherheitskonzepts im Password Safe dar. Die Funktionsweise dieses Mechanismus ist separat erläutert.
- **Siegel**: Auch dem Mehr-Augen-Prinzip im Password Safe ist ein eigenes Kapitel gewidmet.

## Zwischenablage

Ein dominantes Element in der Ribbon ist die Zwischenablage. Dieses existiert ausschließlich im Modul “Passwörter”. Durch einen **Mausklick auf das gewünschte Formularfeld eines Datensatzes in der Ribbon** wird dieses in die Zwischenablage kopiert.




Durch die Meldung im Stile der “Balloon Tipps” unter Windows ist erkenntlich, dass das Passwort nun für 300 Sekunden in die Zwischenablage abgelegt wurde. (Anmerkung: Die Dauer bis zur Bereinigung der Zwischenablage beträgt standardmäßig 60 Sekunden. Im vorliegenden Fall wurde dies über die Benutzereinstellungen angepasst.)

## Starten

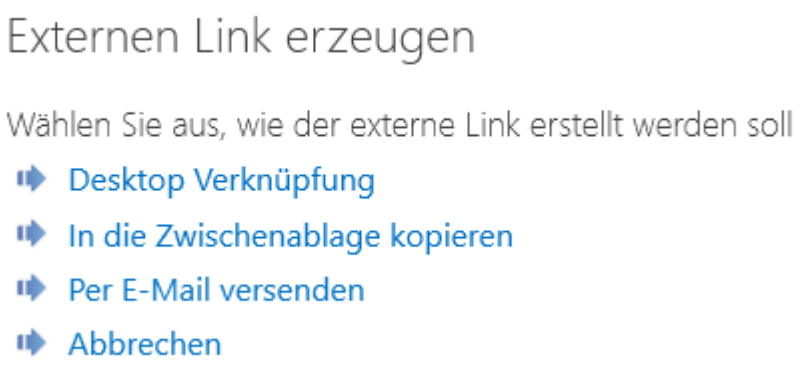
Erst die effiziente Nutzung von Automatismen bei Zugängen via RDP, SSH, generell Windows-Anwendungen oder Webseiten ermöglichen bequemes Arbeiten mit Passwörtern. (Unsichere) Eintragungen mit “Copy&Paste” können somit entfallen.

- **Internetseite öffnen**: Ist im Datensatz eine URL hinterlegt, kann diese hiermit direkt geöffnet werden
- **Anwendungen**: Wenn man Anwendungen mit Datensätzen verknüpft, können diese direkt über das “Starten-Menü” geöffnet werden

## Extras

- **Historie**: Das Icon öffnet die Historie des in der Listenansicht ausgewählten Datensatzes in einem neuen Tab. Durch die lückenlose Erfassung historischer Versionsstände von Passwörtern können nun mehrere Stände miteinander verglichen werden. Weitere Informationen zu dieser Thematik sind in einem eigenen Kapitel erfasst.

- **Externen link erzeugen**: Es wird ermöglicht, für den in der Listenansicht markierten Datensatz einen externen link zu erzeugen. Hierfür stehen mehrere Möglichkeiten zur Auswahl:




- **Anwendung starten**: Im Gegensatz zum Starten von verknüpften Anwendungen, können über dieses Icon auch nicht verknüpfte Anwendungen direkt mit den Anmeldeinformationen des in der Listenansicht markierten Datensatzes gestartet werden.

- **Export**: Es ist möglich, sowohl alle selektierten Datensätze als auch durch den Filter definierte Daten in eine .csv Datei zu exportieren. Mehr…

# Erstellen neuer Passwörter

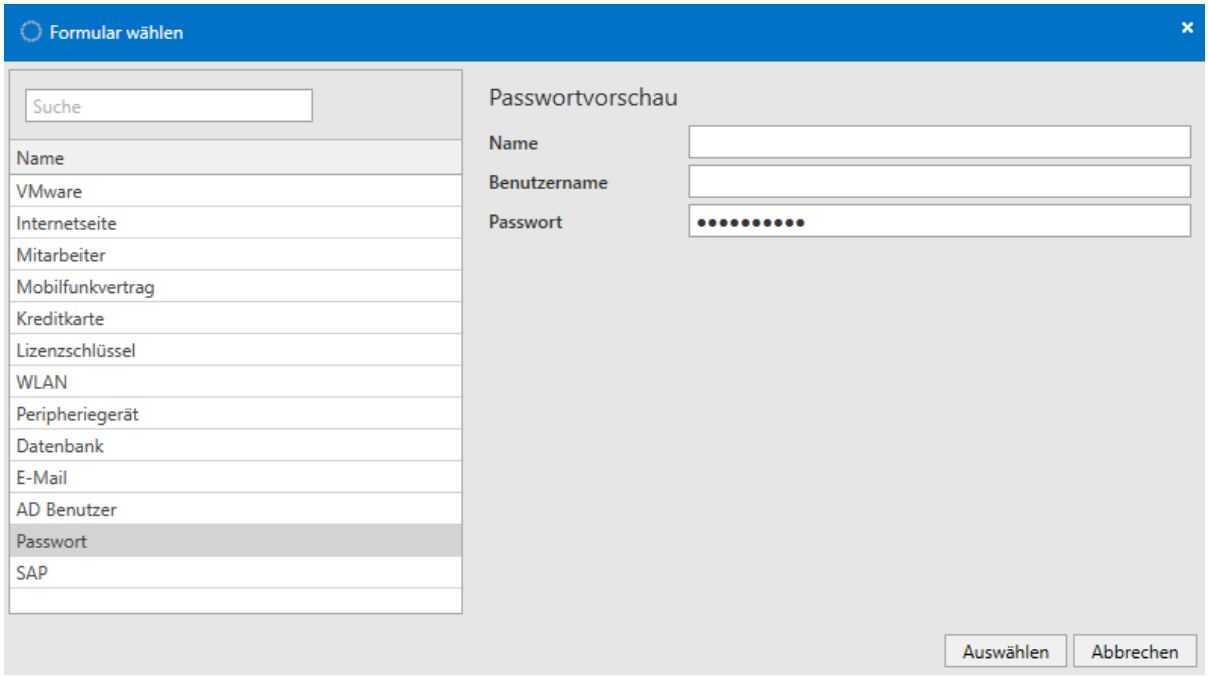
## Was ist das Erstellen neuer Passwörter/Datensätze?

Das Speichern eines Datensatzes/Passwortes hat zum Ziel, Informationen in der MSSQL-Datenbank abzuspeichern. Gestartet wird dieser Vorgang im Client Modul Passwörter. Entweder man nutzt das Icon in der Ribbon, das Tastenkürzel “STRG + N” oder das Kontextmenü der rechten Maustaste in der Listenansicht. Der nächste Schritt ist die Auswahl eines geeigneten Formulars, welche sich in einem modalen Fenster öffnet.

> ! Es wird das Recht **Kann neue Passwörter anlegen** sowie Sicht auf das **Modul Passwörter** benötigt

## Formularauswahl

Bei der Erstellung eines neuen Datensatzes kann man unter all denjenigen Formularen auswählen, auf welche der angemeldete Benutzer berechtigt ist. Um die Auswahl so einfach wie möglich zu gestalten, ist auf der rechten Seite eine Vorschau auf die anschließend enthaltenen Formularfelder gegeben.

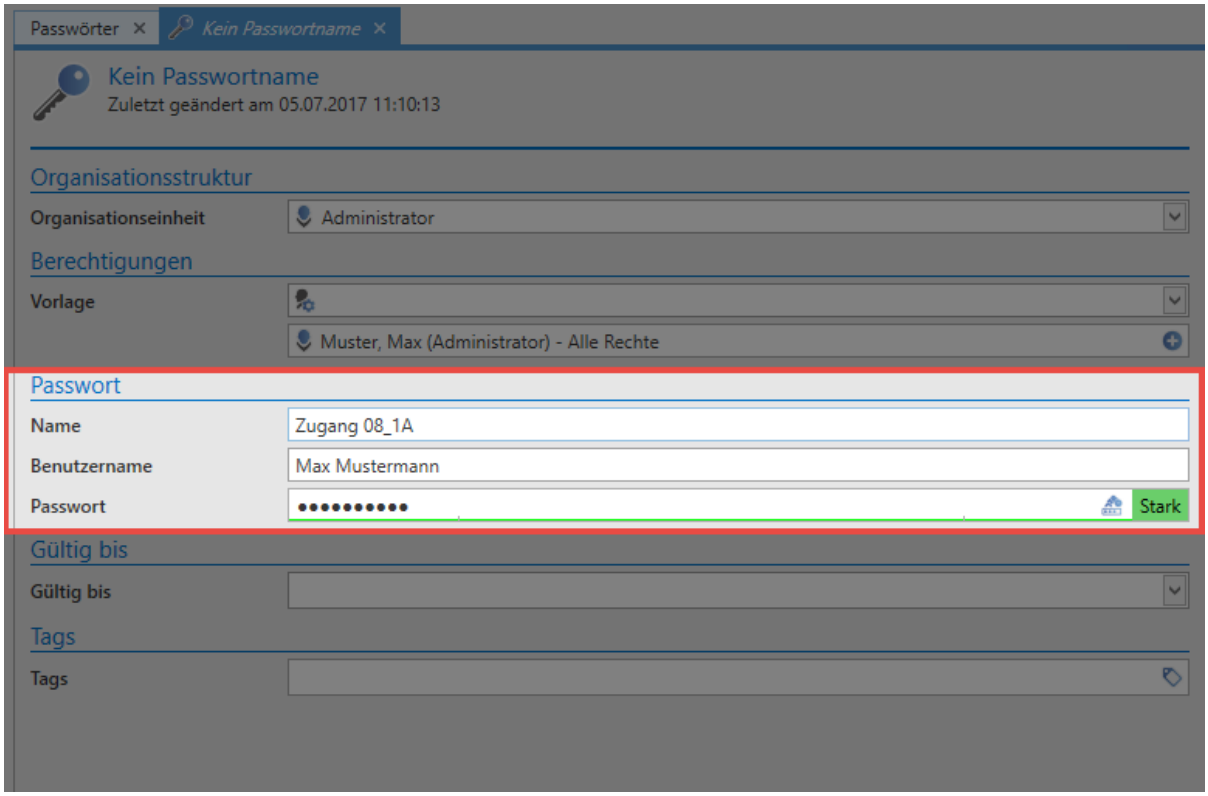



Im vorliegendem Beispiel sieht man, dass das links markierte Formular “Passwort” die drei Formularfelder “Name”, “Benutzername” sowie “Passwort” enthält. Formulare stellen somit die

**Schablonen** dar, gemäß derer Informationen abgespeichert werden sollen. (Die Verwaltung inkl. Berechtigung und Bearbeitung der vorhandenen Formulare ist in einem separaten Kapitel erläutert)

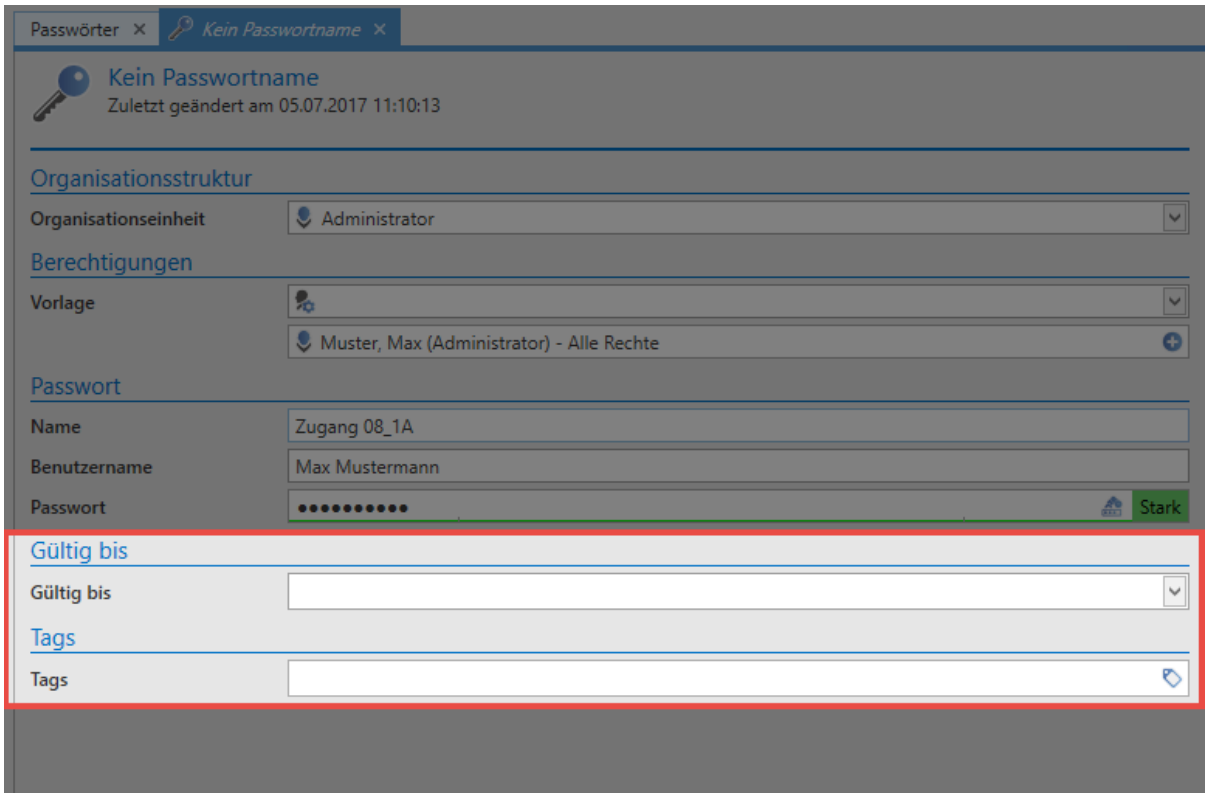
# Eintragen der Daten

Das Fenster für die Erstellung eines neuen Datensatzes öffnet sich stets in einem separaten Tab. Wie nachfolgend zu sehen ist, können nun gemäß des zuvor ausgewählten Formulars die dementsprechenden Formularfelder befüllt werden. Besonders zu erwähnen sind hier Passwortfelder, welche im Zuge von Passwortrichtlinien unterschiedlich gehandhabt werden können. Nach dem Befüllen aller Felder kann über die Ribbon gespeichert werden.




# Gültigkeit und Tags

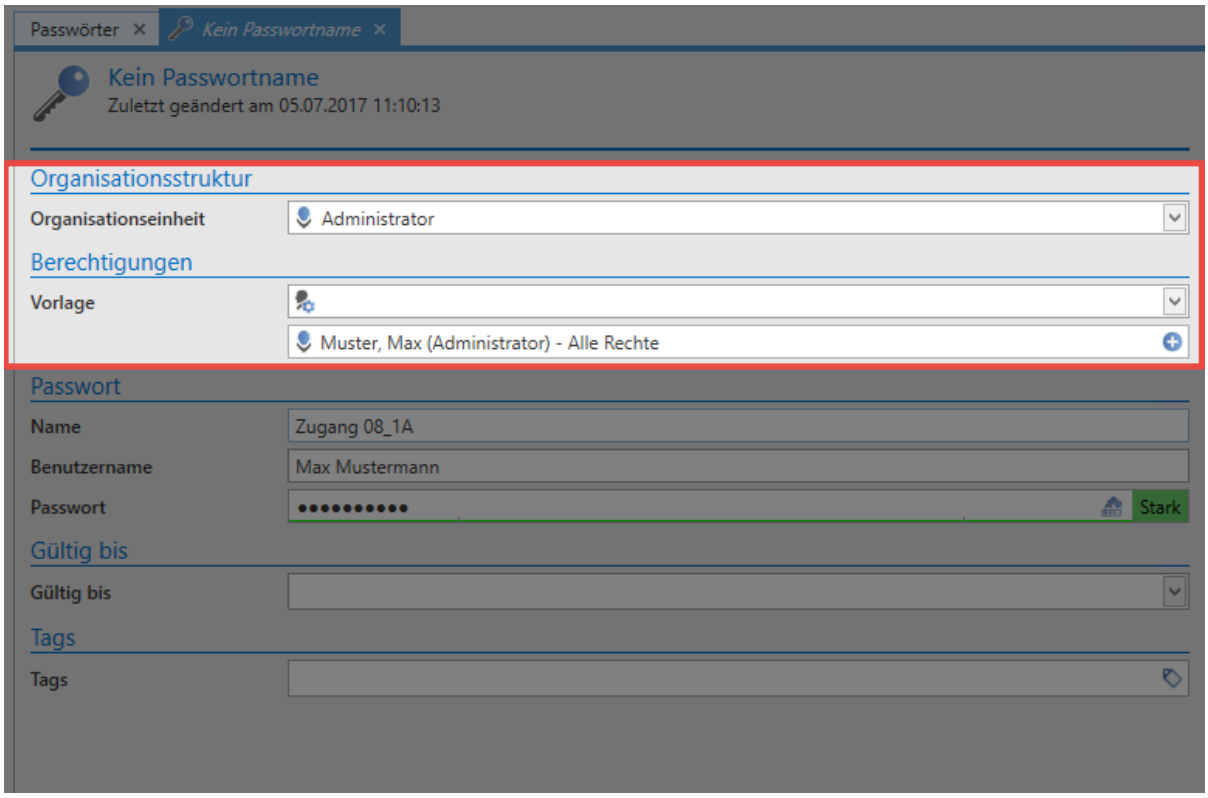
Unabhängig vom ausgewählten Formular ist für einen Datensatz stets eine Gültigkeit und Tags definierbar. Beide Werte sind optional.




- Die **Gültigkeit** legt ein Enddatum fest, bis zu dem der Datensatz gültig sein soll. Diese Informationen können zum Beispiel im Logbuch, bzw. in Berichten ausgewertet werden. Eine Auflistung aller abgelaufenen Passwörter an einen Benutzer, oder an weisungsbefugte Instanzen ist somit gegeben. Dennoch kann die Nutzbarkeit abgelaufener Passwörter aus Sicherheitsgründen nicht eingeschränkt werden.
- **Tags** sind frei definierbare Merkmale von Datensätzen, welche als Suchkriterium genutzt werden können. Auf diese Art und Weise können thematisch zusammenhängende Informationen auch gruppiert werden. Mehr…

# Setzen von Berechtigungen bei neuen Datensätzen

Es gibt grundsätzlich mehrere Ansätze, welche man beim Berechtigen neu erstellter Datensätze verfolgen kann. Alle sind bereits im Kapitel Berechtigungskonzept beschrieben. Wichtig ist hierbei, dass das **manuelle Berechtigen erst nach dem Speichern** eines Datensatzes möglich ist. Die automatisch zu setzenden Berechtigungen werden vor dem Speichern definiert. Wichtig ist in diesem Zusammenhang die Auswahl der Organisationsstruktur sowie die Berechtigungen eines Datensatzes.




- **Manuelles Berechtigen**: Will man den Datensatz manuell berechtigen, wählt man die Organisationsstruktur aus, in die der Datensatz abgelegt werden soll. Nach dem Speichern können danach über den Reiter Berechtigungen in der Ribbon manuell die Berechtigungen angepasst werden. Falls man lediglich einen persönlichen Datensatz erstellen möchte, auf die kein weiterer Benutzer berechtigt sein soll, wählt man lediglich die eigene Organisationsstruktur aus und schließt den Vorgang mit “Speichern” über die Ribbon ab.

> Ist für eine ausgewählte OU eine beliebige Form der automatischen Berechtigung aktiviert, wird diese stets priorisiert.

> Auch bei der Erstellung privater Datensätze kann optional eine Vererbung gemäß der Berechtigungen auf den angemeldeten Benutzer aktiv sein. Diese Option ist an separater Stelle erläutert.

- **Automatisches Berechtigen**: Das automatische Berechtigen von Datensätzen geschieht vor dem Speichern. Egal ob vordefinierte Rechte oder Rechtevererbung genutzt wird – die Konfiguration erfolgt stets im Bereich Organisationsstruktur, bzw. Berechtigungen. Das Speichern des Datensatzes schließt somit die Erstellung des Passwortes inkl. der Vergabe von Berechtigungen ab.

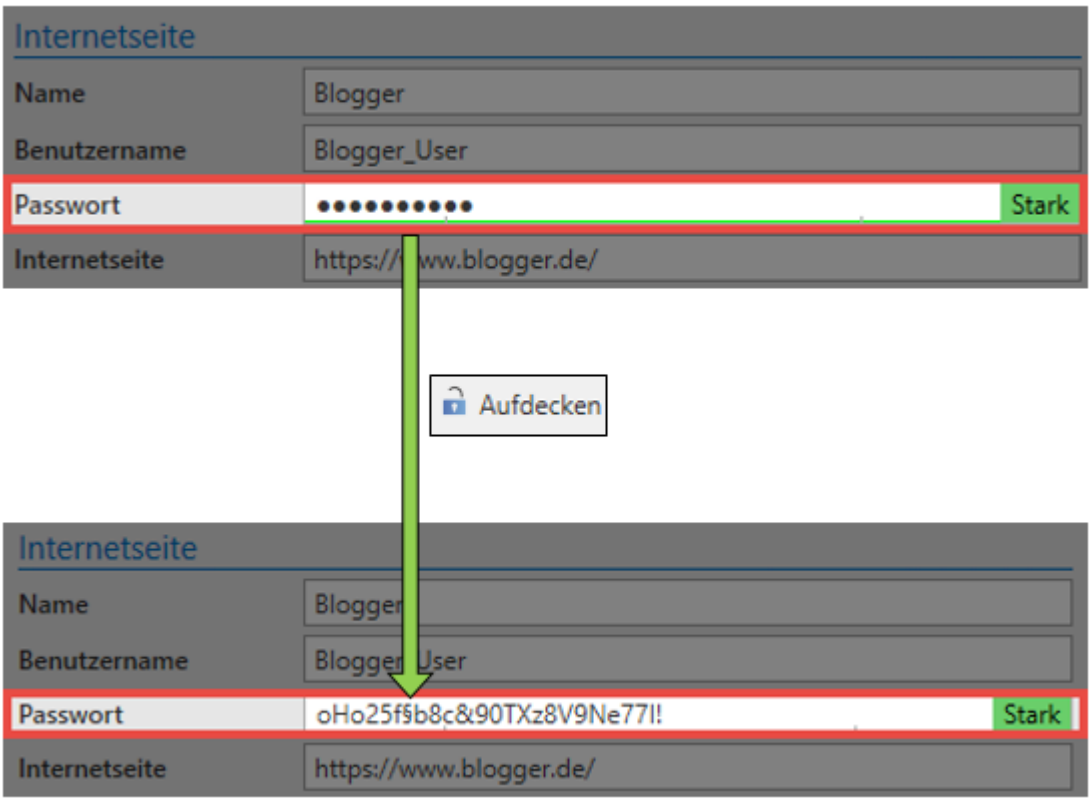
# Aufdecken von Passwörtern

## Worum geht es beim Aufdecken von Passwörtern?

Zwecks Performanz wird im Password Safe nicht jede Information aufseiten der MSSQL-Datenbank verschlüsselt. Lediglich das Passwort selbst (=secret) wird mit Hilfe der genutzten Verschlüsselungsalgorithmen verschlüsselt und schlussendlich in der MSSQL-Datenbank abgelegt. Da der Zugang zum MSSQL-Server selbst auch anderweitig über Zugriffsberechtigungen abgesichert ist, ermöglicht dieses Vorgehen **maximales Arbeitstempo** bei **gleichbleibend hoher Sicherheit** durch den Einsatz **ausgereifter, kryptographischer Methoden**. Das Aufdecken von Passwörtern beschreibt hierbei den Mechanismus, bei dem ein Passwort im Client dem Benutzer sichtbar gemacht wird. Dieser Umgang mit Passwörtern beschreibt sehr präzise den Stellungswert von Datensicherheit im Password Safe – nachfolgend soll dieser Vorgang deshalb detailliert beschrieben werden.

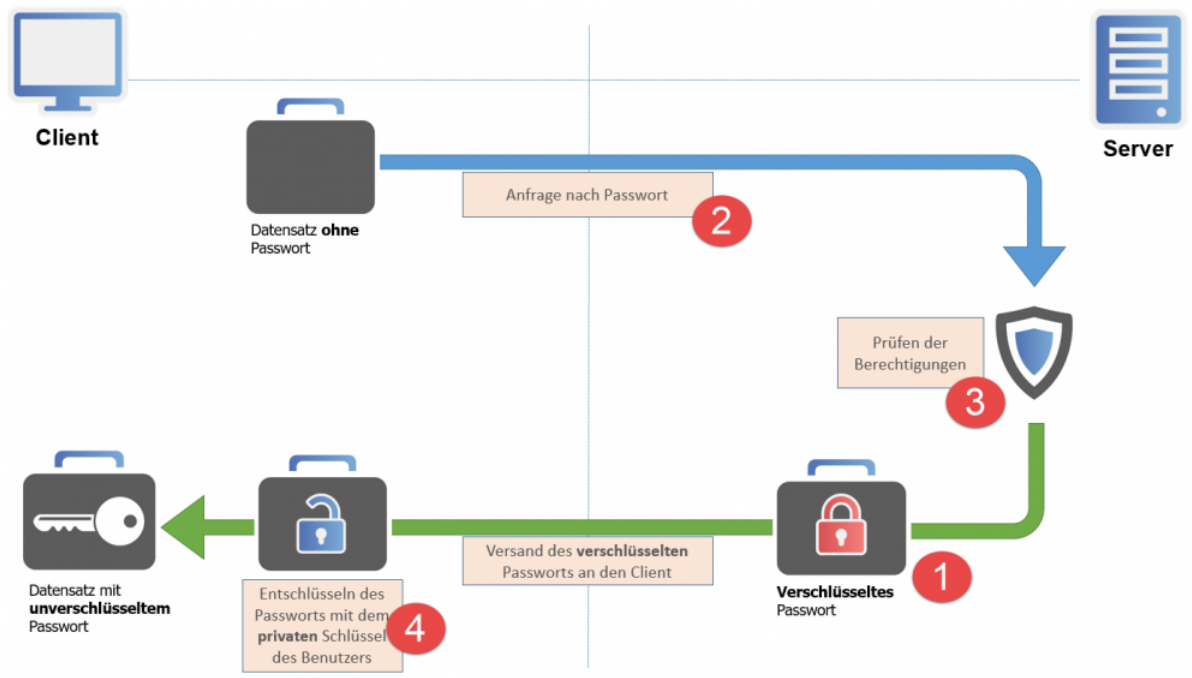
### Fallbeispiel

Der Datensatz “Blogger” ist in der Datenbank gespeichert und dem angemeldeten Benutzer einsehbar. Daraus erschließt sich, dass der Benutzer zumindest lesend auf den Datensatz berechtigt ist. Wie man dem Berechtigungskonzept entnehmen kann, hat der Benutzer demnach in der Regel auch Leserecht auf das Passwort selbst. Dies bedeutet, man kann über die Funktion “Aufdecken” den Wert des Passwortes einsehen.




# Aufdecken von Passwörtern – Schaubild

Wichtig ist in diesem Zusammenhang, dass das Wort “Aufdecken” dem Prozess nicht wirklich gerecht wird. Dies assoziiert **fälschlicherweise**, dass das Passwort dem Client bereits vorliegt und es nur noch aufgedeckt werden muss. Der im Hintergrund ablaufende Prozess bis zum Anzeigen des Passwortes ist jedoch bei weitem komplexer und soll nachfolgend beschrieben werden.




### 1. Aufbewahrung des Passwortes am Server

Auch wenn man es vermuten könnte…ein verdecktes Passwort (******) liegt in der Ausgangssituation weder dem Client noch dem Server im Klartext vor! Durch den Einsatz der beiden Verfahren **AES 256** sowie **RSA 4096** wird das Passwort **hybridverschlüsselt** als Teil der MSSQL-Datenbank aufbewahrt. Weder serverseitig noch am Client kann demnach aktuell Einsicht auf das Passwort genommen werden. Markiert man also einen Datensatz, ist das Passwort vor dem Aufdecken am Client noch gar nicht vorhanden, serverseitig ist es verschlüsselt gespeichert.

### 2. Verschlüsseltes Passwort wird angefragt

Der Auslöser für die Anfrage des Passwortes ist das Betätigen des “Aufdecken”-Buttons. Es wird ein Request an den Server gesendet, indem die Freigabe des verschlüsselten Passwortes beantragt wird. Der Server selbst besitzt den nötigen Schlüssel (private Key) zum Entschlüsseln nicht. Er kann demnach nur den **verschlüsselten Wert** liefern.

### 3. Prüfung der Berechtigungen

Ob eine wie unter 2. gestellte Anfrage eine Freigabe erhält, wird im Berechtigungskonzept definiert. Nach dem Eingang der Anfrage prüft der Server, ob der Benutzer die nötigen Rechte besitzt. Auch das Vorhandensein eventuell angebrachter Sicherheitsmechanismen, wie zum Beispiel eines Siegels oder dem Sichtschutz, werden geprüft. Erfüllt man die für eine Freigabe nötigen Anforderungen, versendet der Server nun das **verschlüsselte Passwort**. Im gleichen Arbeitsschritt erfolgt ein **Logfile-Eintrag**, welcher den Zugriff des Benutzers auf das Passwort dokumentiert.

### 4. Entschlüsseln des Passwortes am Client

Der Benutzer besitzt nun das verschlüsselte Passwort, welches diesem vom Server geliefert wurde. Der Benutzer selbst ist im Besitz des zur Entschlüsselung notwendigen **privaten Schlüssels** und kann nun den tatsächlichen Wert des Passwortes einsehen.

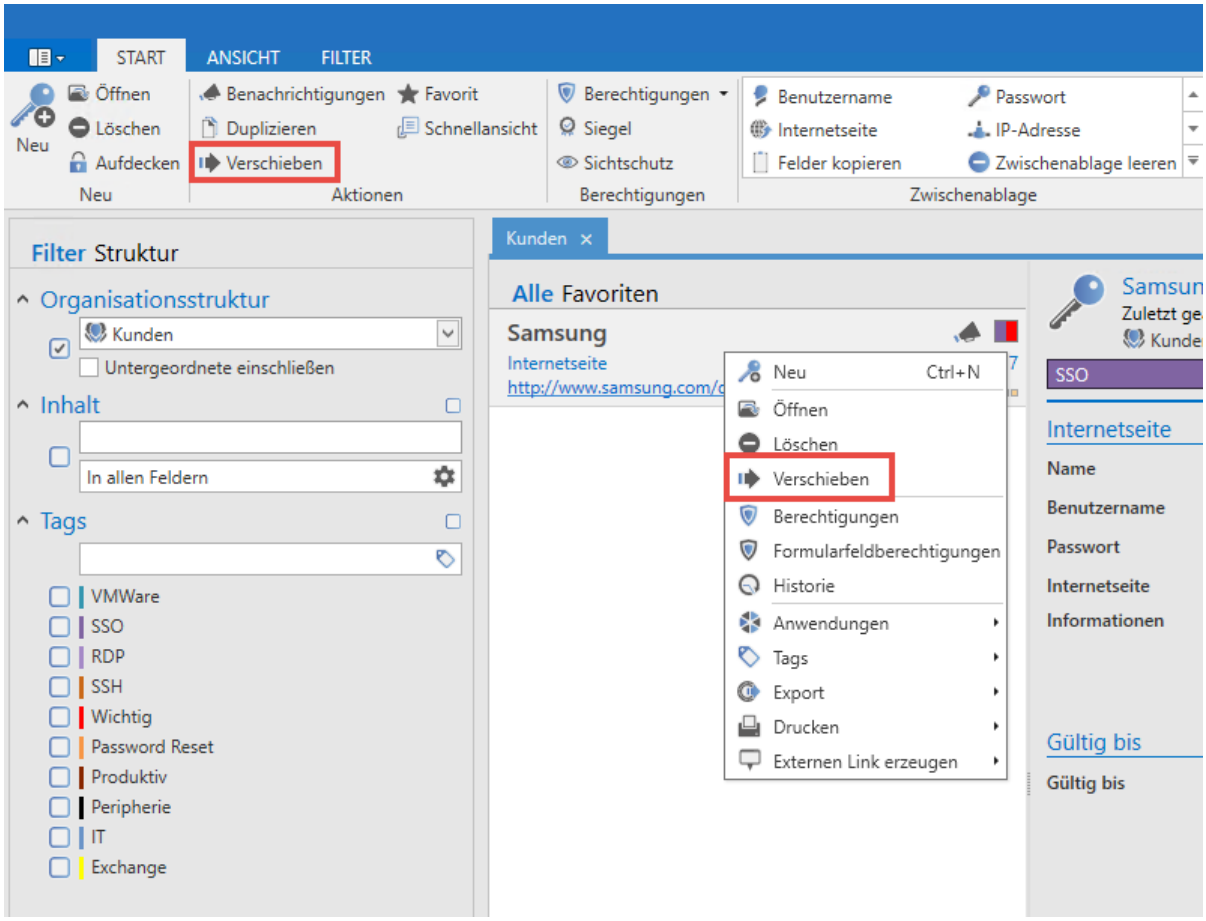
# Verschieben von Passwörtern

## Was passiert beim Verschieben des Datensatzes?

Daten können innerhalb des Password Safe in eine andere Organisationsstruktur verschoben werden. Dies muss nicht zwingend mit einer Änderung der Berechtigungen einhergehen (Die Auswirkungen sind unten separat beschrieben). Das Verschieben ohne Änderungen an Berechtigungen hat demnach hauptsächlich Auswirkungen auf die Filterung, bzw. die Suche nach Datensätzen.

## Wie verschiebt man Datensätze?

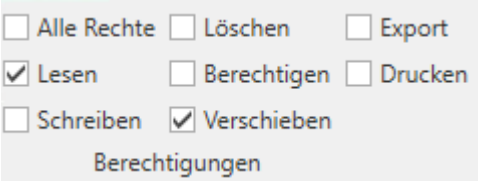
Das Verschieben von (markierten) Datensätzen erfolgt entweder in der Ribbon oder über das Kontextmenü der rechten Maustaste.



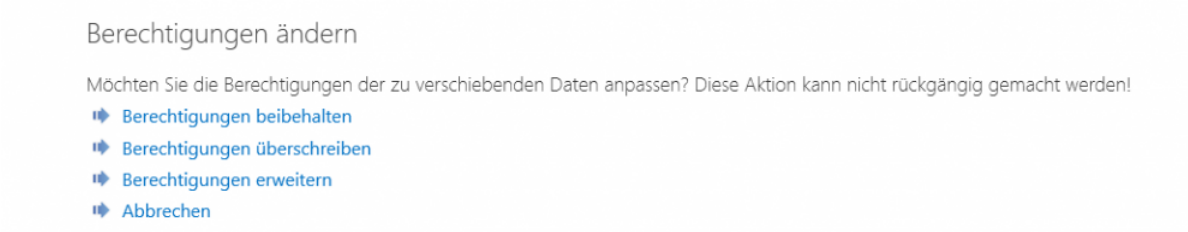

Es können ebenso mehrere Datensätze markiert und verschoben werden. Die getroffene Auswahl in Bezug auf die Berechtigungen gilt dann für alle Datensätze.

### Benötigte Berechtigungen

Für das Verschieben von Datensätzen ist kein gesondertes Benutzerrecht/Einstellung vorgesehen. Es ist einzig das Recht “Verschieben” auf dem Datensatz ausschlaggebend.




## Auswirkungen auf vorhandene Berechtigungen




- **Berechtigungen beibehalten**: Die Berechtigungen des Datensatzes werden durch das Verschieben nicht geändert und bleiben erhalten
- **Berechtigungen überschreiben**: Die Berechtigungen des Datensatzes werden durch die der Ziel-OU überschrieben
- **Berechtigungen erweitern**: Die vorhandenen Berechtigungen werden um die Berechtigungen der Ziel-OU erweitert

! Die gewählte Form der Berechtigung (Rechte vordefinieren, Vererbung aus Organisationsstrukturen) wird auch beim Verschieben von Datensätzen angewandt

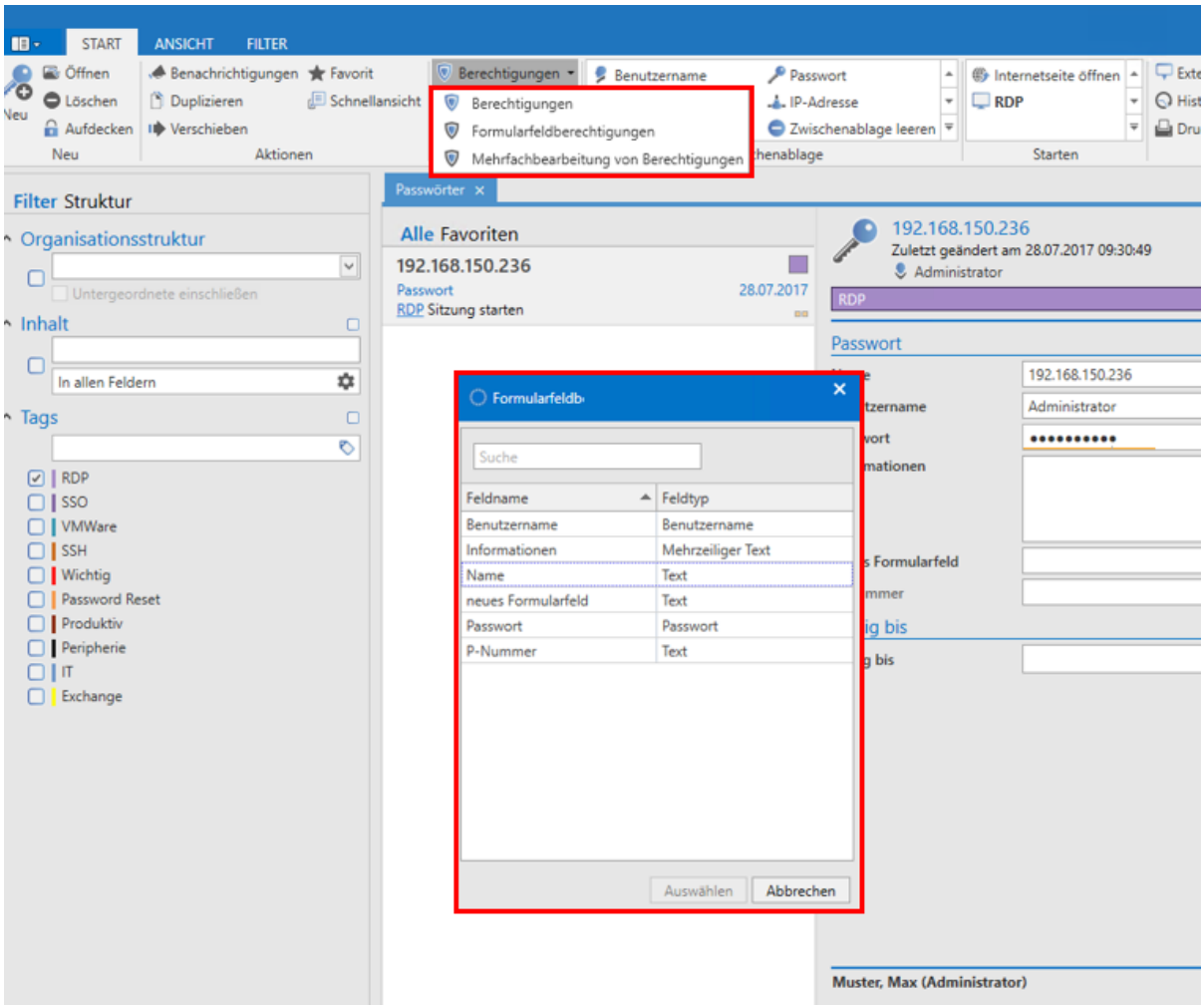
# Formularfeldberechtigungen

## Was sind Formularfeldberechtigungen?

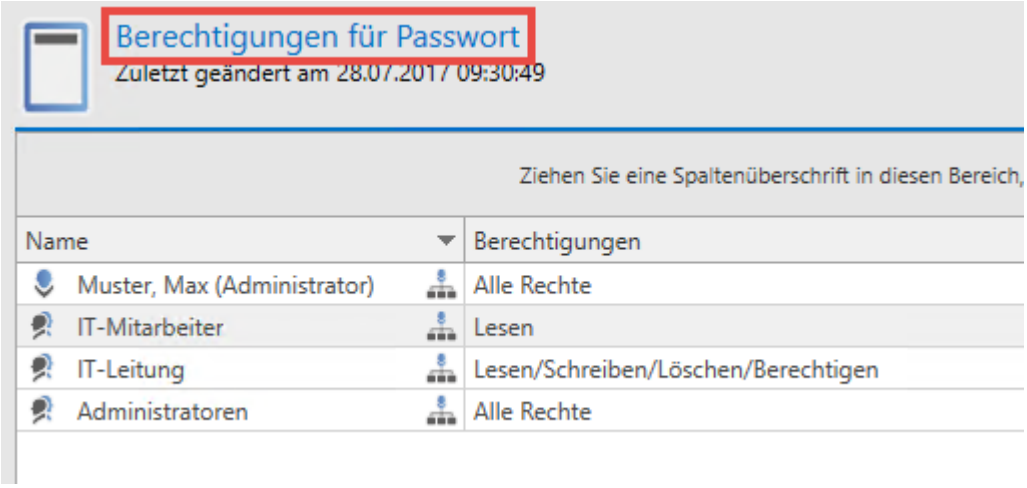
Im Berechtigungskonzept ist beschrieben, dass jedes Objekt für sich berechtigt werden kann. Diese Objekte können sowohl Datensätze, Formulare oder Benutzer sein. Password Safe geht hierbei noch einen Schritt weiter. Jedes einzelne Formularfeld eines Datensatzes kann separat berechtigt werden. Es ist somit möglich, das Passwortfeld eines Datensatzes auf eine andere Art und Weise zu berechtigen, als dies bei anderen Feldern der Fall ist.

## Konfiguration

Über die Ribbon können für den markierten Datensatz im Bereich “Berechtigungen” über ein Dropdown Menü die zugehörigen Formularfeldberechtigungen geöffnet werden.



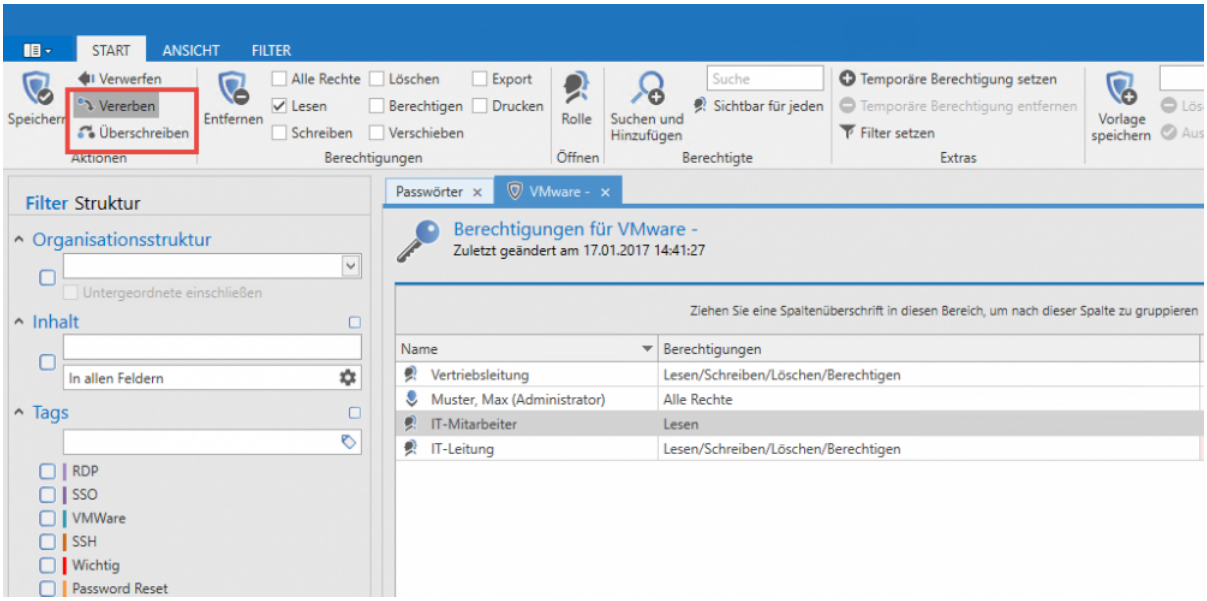
Das sich öffnende Fenster ermöglich die Auswahl desjenigen Formularfeldes, welches berechtigt werden soll. Im nachfolgenden Fall soll das Passwortfeld betrachtet werden.




Die nun konfigurierbaren Berechtigungen betreffen ausschließlich das Passwortfeld. Die anderen Formularfelder bleiben unberührt.

# Vererbung von Berechtigungen innerhalb von Datensätzen

Per Standard wird das Durchführen von Änderungen an Datensatzberechtigungen automatisch auf alle Formularfelder vererbt. Öffnet man die Berechtigungen eines Datensatzes über die Ribbon, gelten die konfigurierten Rechte demnach für alle Formularfelder. Dieser Mechanismus kann über die beiden Buttons “Vererben” und “Überschreiben” in der Ribbon an- und ausgeschalten werden.



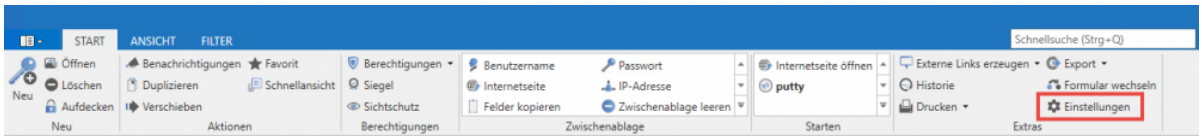
> ! Die Sichtbarkeit der genannten Icons wird über die Benutzerrechte **Kann Berechtigungen überschreiben** und **Kann Berechtigungen vererben** gesteuert.

Auf diese Weise besteht die Möglichkeit, dass Änderungen an den Berechtigungen eines Datensatzes nicht automatisch auf alle verfügbaren, darunterliegenden Formularfelder vererbt wird. Hierzu muss der Haken bei “Vererben” lediglich deaktiviert werden.

# Passworteinstellungen

## Was sind Passworteinstellungen?

In den Passworteinstellungen können diverse, die Passwörter betreffenden Option definiert werden. Zu finden sind diese in der Ribbon im Unterbereich “Extras”. Die Einstellungen öffnen sich in einem eigenen Tab.




### Kategorie: Browser

- **Standardbrowser**: Mit Hilfe dieser Option kann für jeden Datensatz separat ein Standardbrowser definiert werden. Es kann zwischen allen Browsern gewählt werden, welche unter Windows als Browser registriert wurden.

### Kategorie: SSO

- **Browser Addons**: Loginmasken automatisch befüllen: Es wird definiert, ob bei Anmeldungen über SSO die Loginmasken automatisch befüllt werden sollen. Dies ist dann der Fall, wenn der Benutzer auf eine Login Seite browst. Ist ein Datensatz für diese Seite hinterlegt, wird dieser bei aktivierter Option direkt befüllt. Anderweitig muss dieser Schritt über das Addon manuell erledigt werden. Sind mehrere Datensätze für diese Seite hinterlegt, muss der Benutzer in beiden Fällen manuell den Schritt über das Addon gehen.
- **Browser Addons**: Loginmasken automatisch absenden: Bei aktivierter Option wird nach dem Befüllen der Anmeldeinformationen der Anmeldebutton automatisch getätigt.

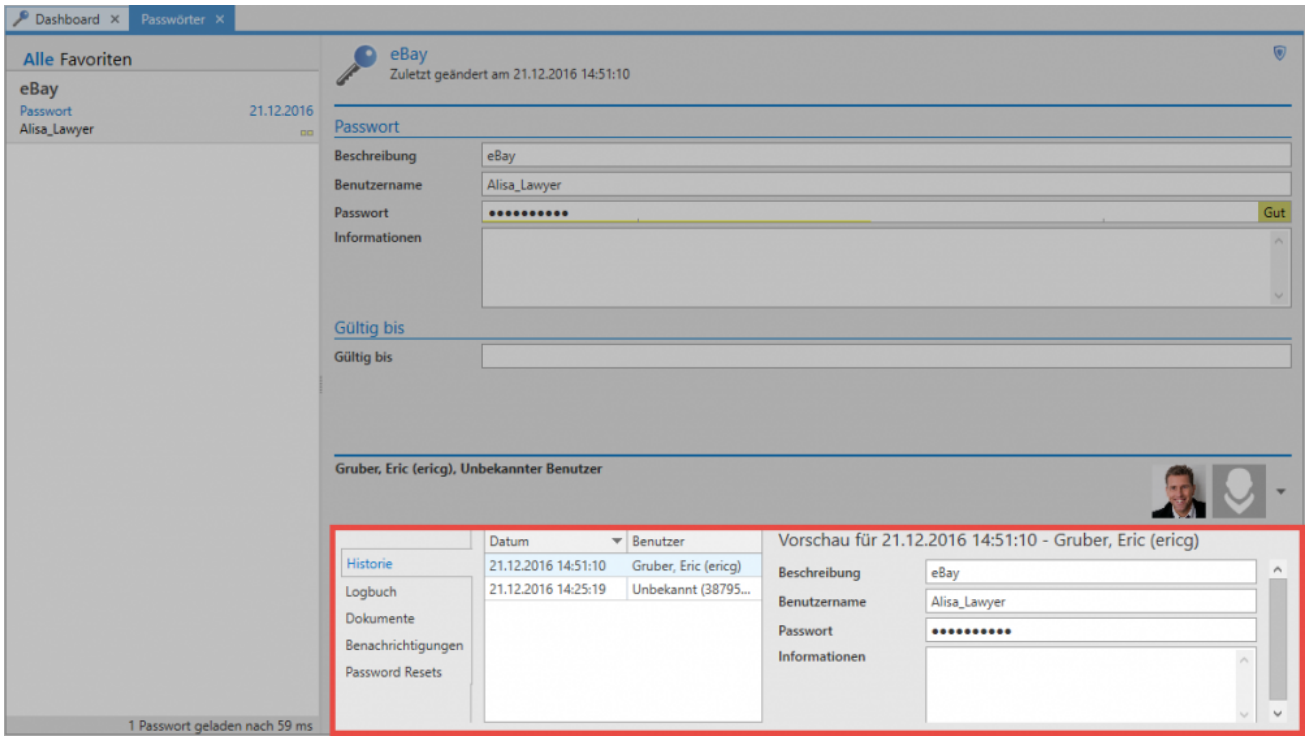
# Historie

## Was ist die Historie?

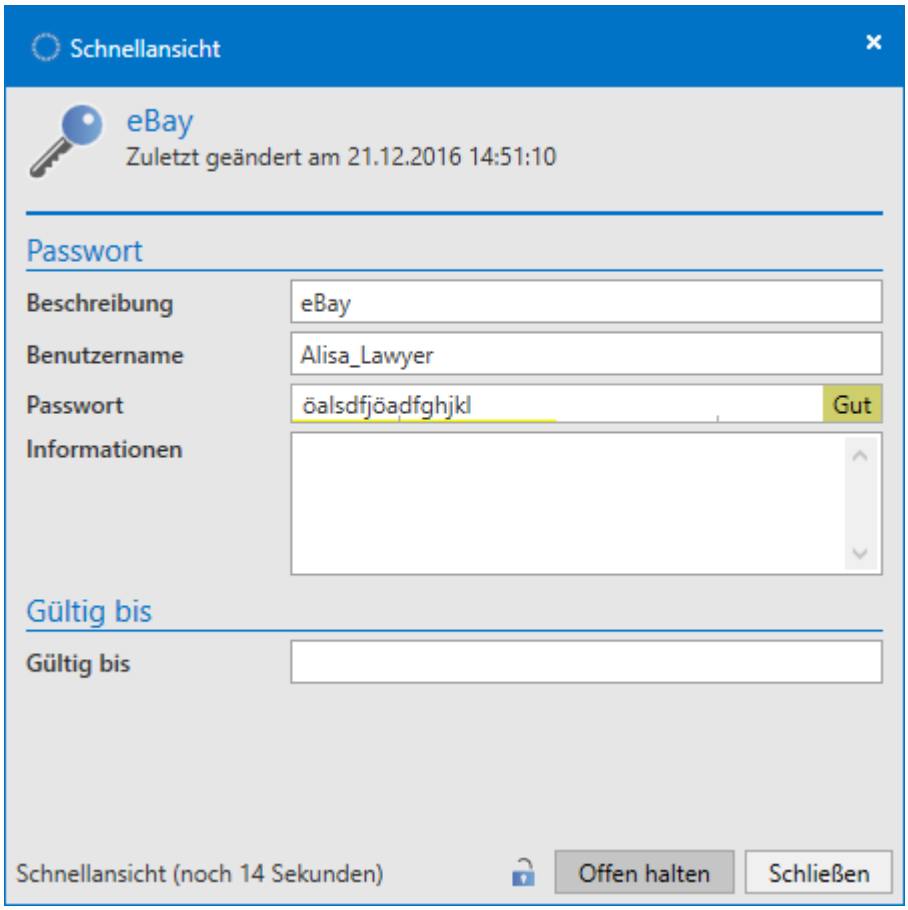
Neben dem Speichern und Verwahren von Passwörtern besitzt auch die Nachvollziehbarkeit von Änderungen an Datensätzen immense Relevanz. Die Historie ermöglicht die lückenlose Versionierung aller Formularfelder eines Datensatzes. Jede Veränderung von Datensätzen wird separat erfasst, gespeichert und kann demzufolge auch wiederhergestellt werden. Darüber hinaus ergibt sich die Möglichkeit, stets historische Werte mit dem aktuellen Stand zu vergleichen. Die Historie ist demnach ein unverzichtbarer Bestandteil in jedem Sicherheitskonzept.

## Die Historie im Lesebereich

Über den optional aufrufbaren Footerbereich kann man die Historie bereits im Lesebereich einsehen. Chronologisch sortiert sind alle historischen Einträge aufgelistet.

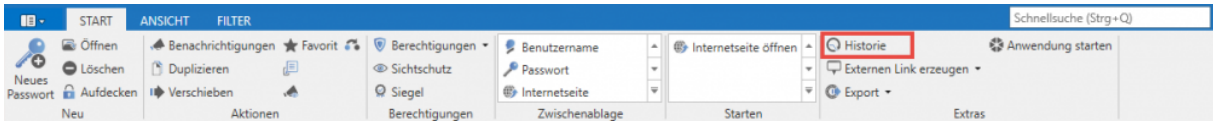



Links werden die verschiedenen Versionsstände untereinander angezeigt. Rechts daneben sind die Infos zur jeweiligen Version zu sehen. In der Ribbon unter **Historie** oder per Doppelklick lässt sich eine Schnellansicht einblenden.

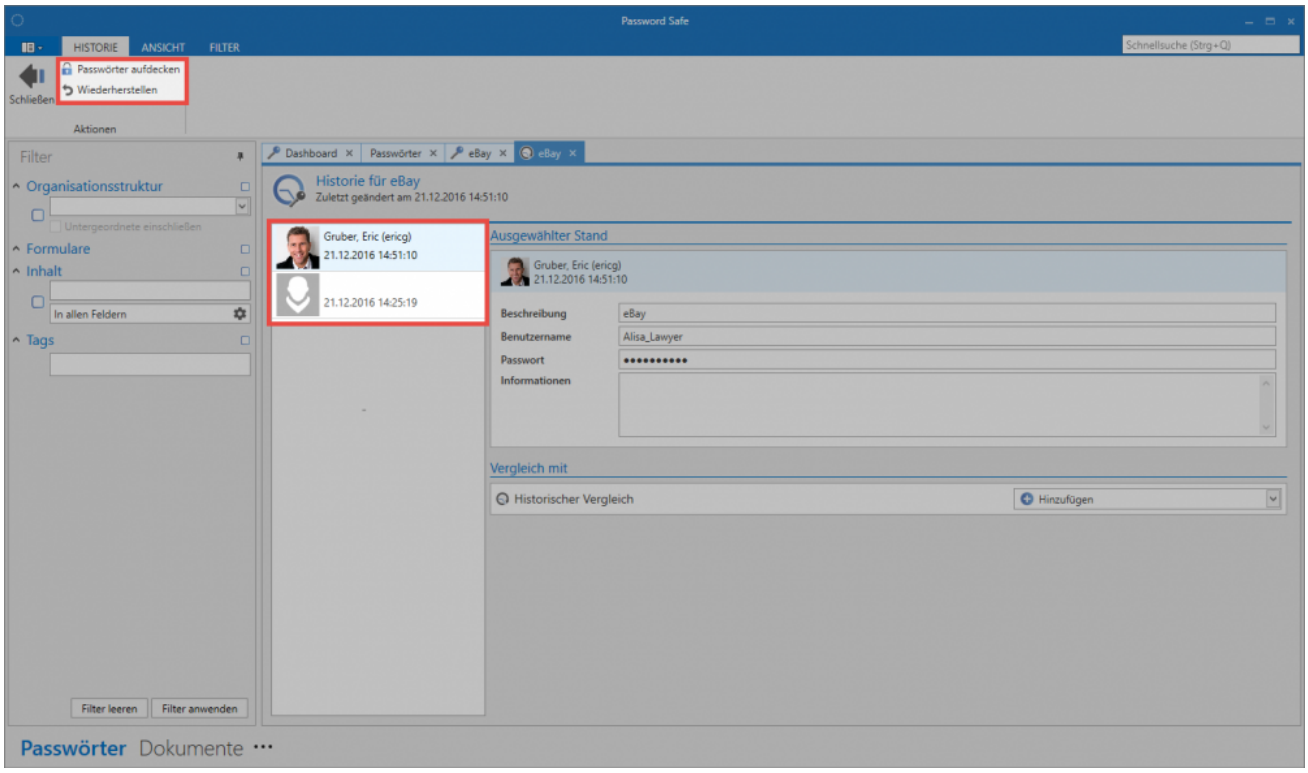



# Detaillierte Historie in den Extras

Im Reiter Start/Extras ist die detaillierte Historie des in der Listenansicht markierten Datensatzes aufrufbar.

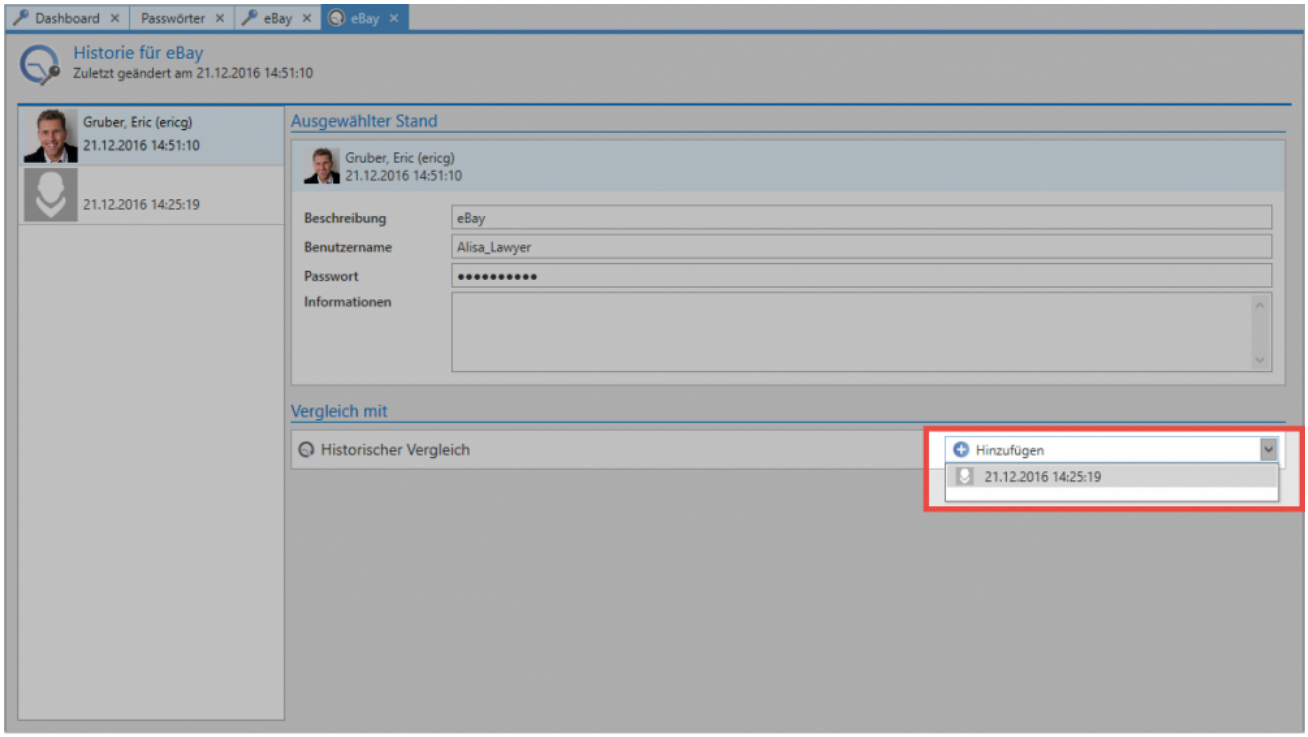



Die Historie des markierten Datensatzes öffnet sich in einem separaten Tab. In der Listenansicht sind nun alle verfügbaren Versionsstände mit Datum und Uhrzeit der letzten Änderung chronologisch sortiert aufgeführt.

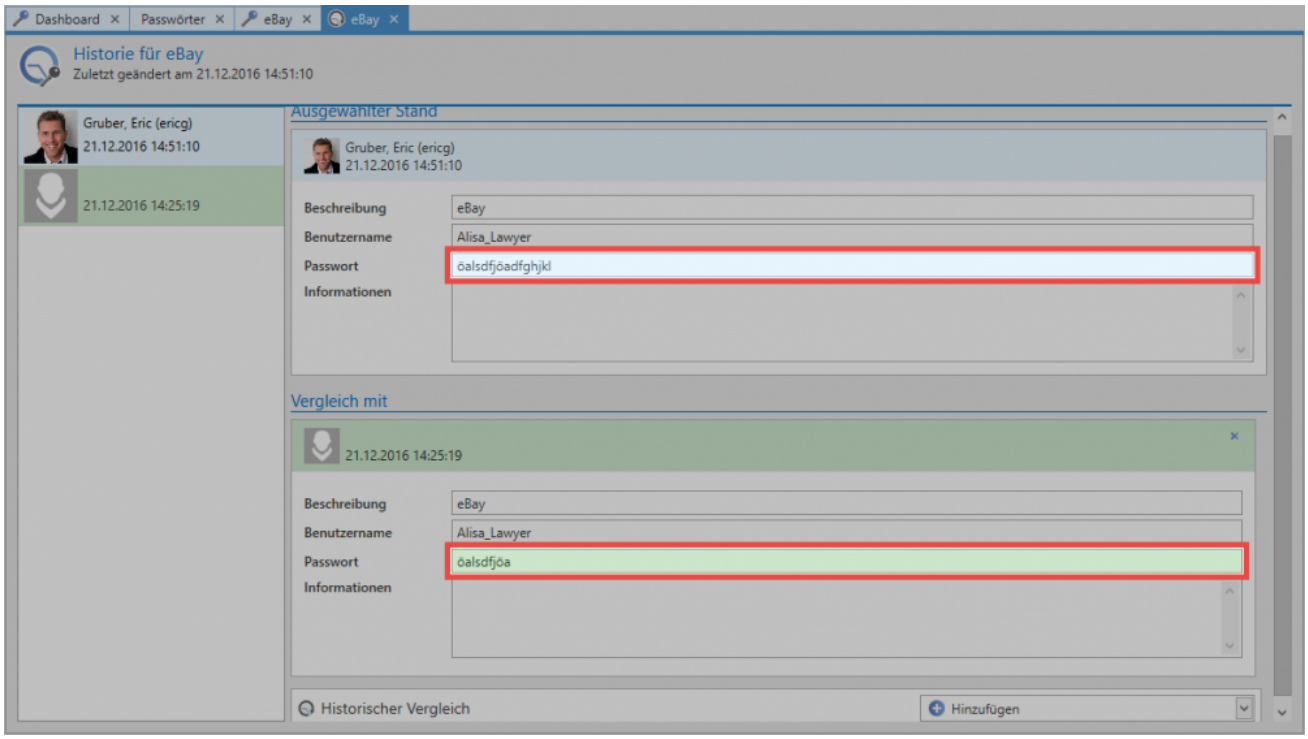



# Vergleich von Versionsständen

Zum Vergleichen müssen mindestens zwei Versionsstände ausgewählt werden. In der Listenansicht markiert man den ersten Versionsstand und fügt über den rechts angebrachten Button “Hinzufügen” rechts im Lesebereich einen weiteren hinzu, welcher mit dem ersten verglichen werden soll.



Falls Abweichungen zwischen den beiden Versionsständen existieren, werden diese nun farblich markiert.




# Versionen wiederherstellen

Über die Ribbon kann ein selektierter Stand wiederhergestellt werden. Der aktuelle Stand wird überschrieben und der Historie hinzugefügt

# Dokumente

## Was sind Dokumente?

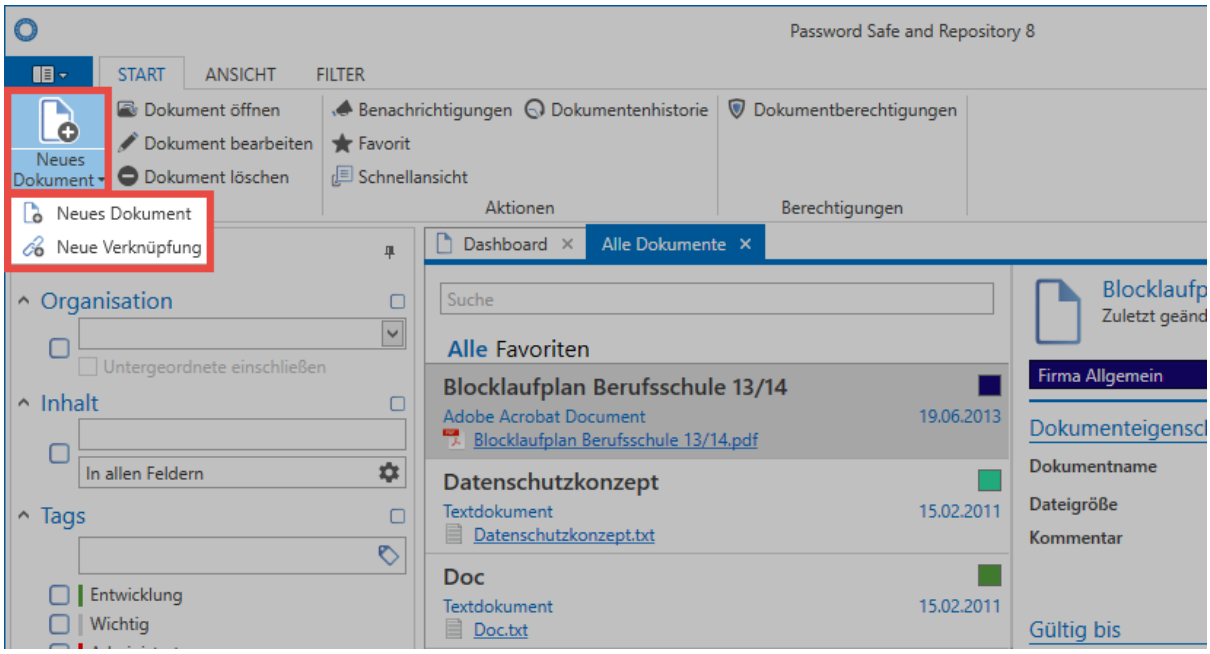
Sicherheitskritische Daten müssen nicht zwingend in Form von Passwörtern vorliegen. Um die einheitliche und sichere Datenhaltung auch abseits von Passwörtern nutzen zu können, bietet der Password Safe in der Version 8 effektive Werkzeuge für den professionellen Umgang mit schützenswerten Dokumenten oder Dateien. Durch die Möglichkeit, Dokumente gemäß der Berechtigungen mit anderen zu teilen, erhält man stets den aktuellen Stand eines Dokumentes und vermeidet Redundanzen. Komplettiert wird das Modul Dokumente durch die ausgereifte Versionsverwaltung, welche sämtliche in der Vergangenheit gespeicherten Versionen eines Dokumentes erfasst und demzufolge das Zurücksetzen auf historische Versionsstände ermöglicht. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert..


> ! Es wird das Recht **Kann neue Dokumente anlegen** benötigt

## Hinzufügen von Dokumenten

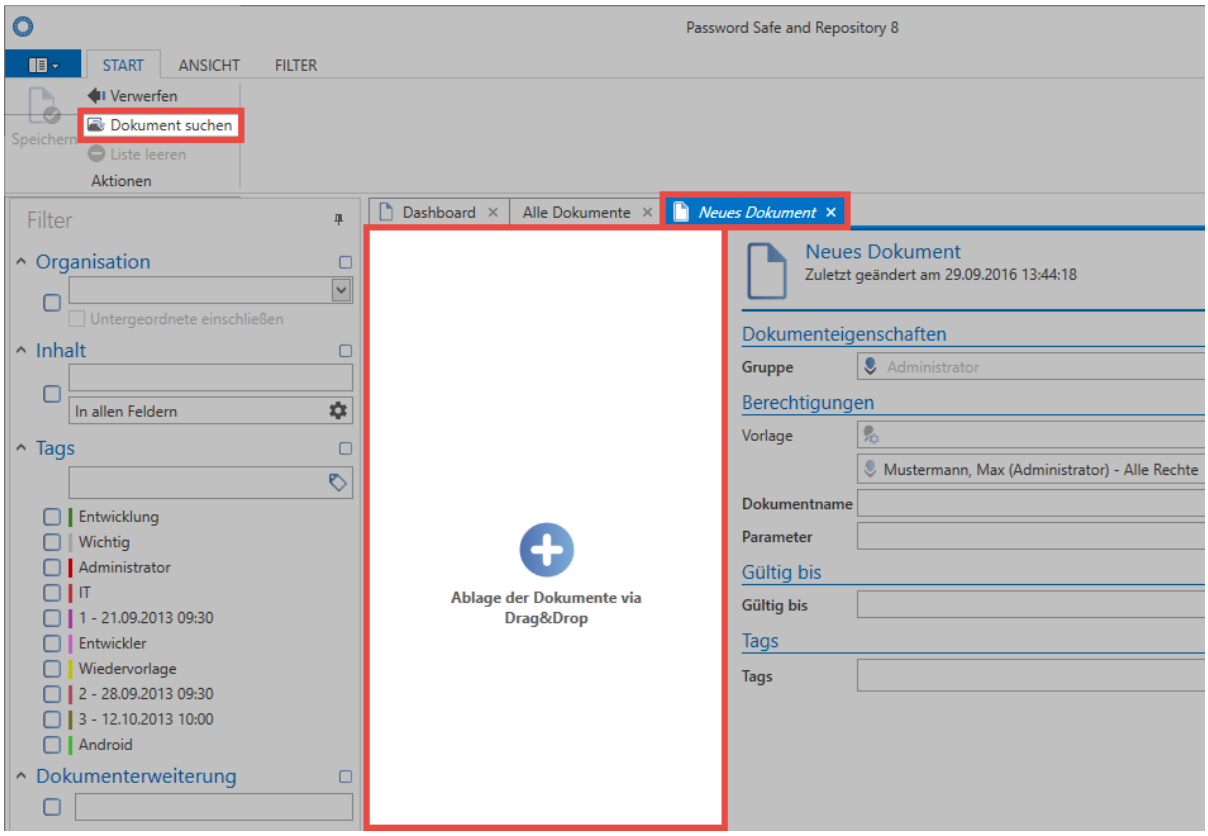
Es gibt zwei Arten Dokumente und Dateien in Password Safe v8 zu verwalten:

1. **Erstellen einer Verknüpfung:** Hierbei wird lediglich auf eine Datei verwiesen, welche lokal oder auf einem Netzlaufwerk liegt. Die Datei selbst wird nicht in der Datenbank gespeichert. Sowohl Versionsverwaltung als auch die Nachvollziehbarkeit von Änderungen in der Historie sind hierbei nicht möglich.
2. **Ablegen des Dokuments in der Datenbank:** Die Datei wird Teil der verschlüsselten Datenbank. Sie wird innerhalb der Datenbank gespeichert und kann zukünftig selektiv gemäß der Berechtigungen den Mitarbeitern für die weitere Bearbeitung zur Verfügung gestellt werden.




# Dokumentenauswahl

Bei der Selektion der hochzuladenden Datei können Sie entweder über die Explorer Ansicht Ihr Dateisystem durchsuchen, oder bequem per Drag & Drop Objekte hinzufügen. Letzteres gibt Ihnen die Möglichkeit direkt mehrere Dokumente in einem Schritt zu importieren.



# Versionsverwaltung

Das Herzstück einer jeden Dokumentenverwaltung ist die Möglichkeit, Änderungen an Dokumenten oder Dateien zu erfassen und zu archivieren. Sämtliche Versionen eines Dokumentes können miteinander verglichen, und bei Bedarf historische Zustände wiederhergestellt werden. Password Safe stellt diese Funktionalität über die Historie sowohl in der Ribbon, als auch im Footerbereich der Detailansicht eines Dokumentes zur Verfügung. Diese ist analog zur Historie von Passwörtern anwendbar. Das Zusammenspiel aus dem dokumentspezifischen Ereignislogbuch und der Historie bietet in der Summe eine lückenlose Auflistung jeglicher Informationen, welche Relevanz im Umgang mit sensiblen Daten aufweisen. Mit der Versionsverwaltung lassen sich beliebige historische Versionen eines Dokuments wiederherstellen.

# Benachrichtigungen

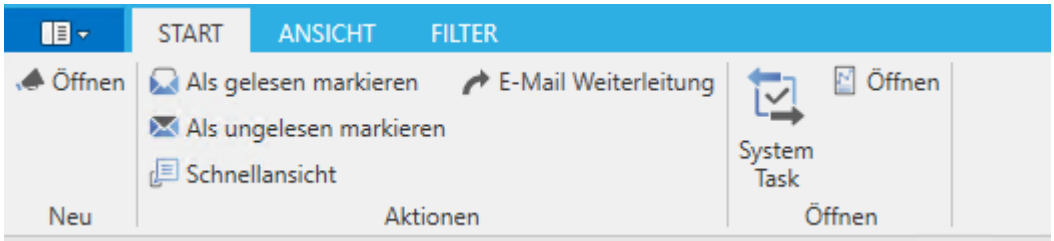
## Was sind Benachrichtigungen?

Mit dem Benachrichtigungssystem bleiben Sie stets über alle Ereignisse, welche Sie für wichtig erachten, auf dem Laufenden. In nahezu allen Modulen können Benutzer individuell konfigurieren, wann Sie Benachrichtigungen erhalten wollen. Alle konfigurierten Meldungen werden immer nur für den aktuell angemeldeten Password Safe Benutzer erstellt. Es ist nicht möglich, eine Benachrichtigung für einen anderen Benutzer zu erstellen. Jeder Benutzer kann und soll selbst definieren, welche Passwörter, welche Auslöser sowie Änderungen für Ihn wichtig und informativ sind. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert..


> Per Standard ist der Lesebereich in diesem Modul deaktiviert. Über den Reiter “Ansicht” in der Ribbon kann diese Darstellung aktiviert werden.

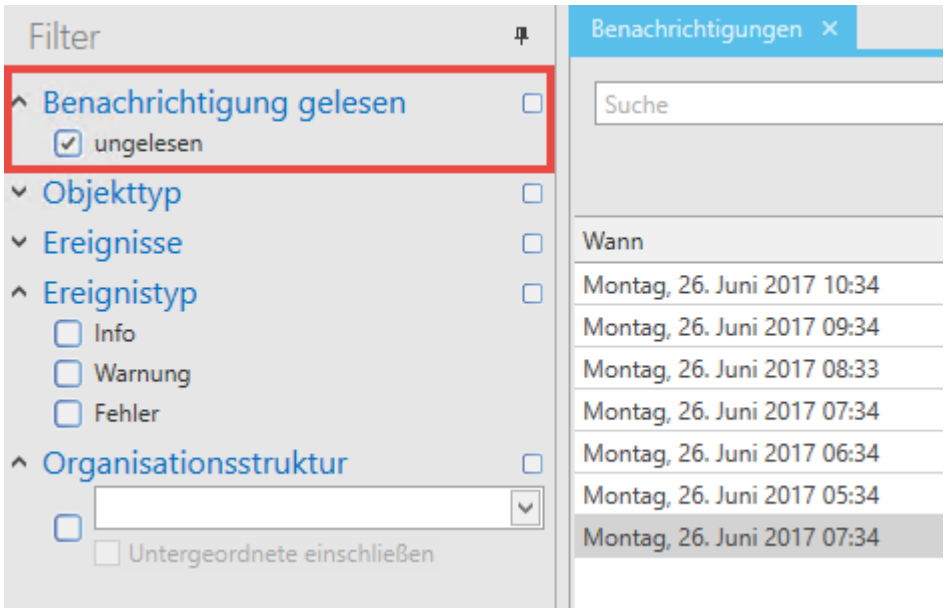
## Modulspezifische Ribbonfunktionen

Auch in den Benachrichtigungen existieren einige Ribbon-Funktionalitäten, welche ausschließlich in diesem Modul zur Verfügung stehen. Besonders das **Weiterleiten von wichtigen Mitteilungen an Email-Adressen** ermöglicht sowohl Administratoren als auch Benutzern ortsungebundene Kontrolle und Transparenz.




### Benachrichtigungen als gelesen markieren

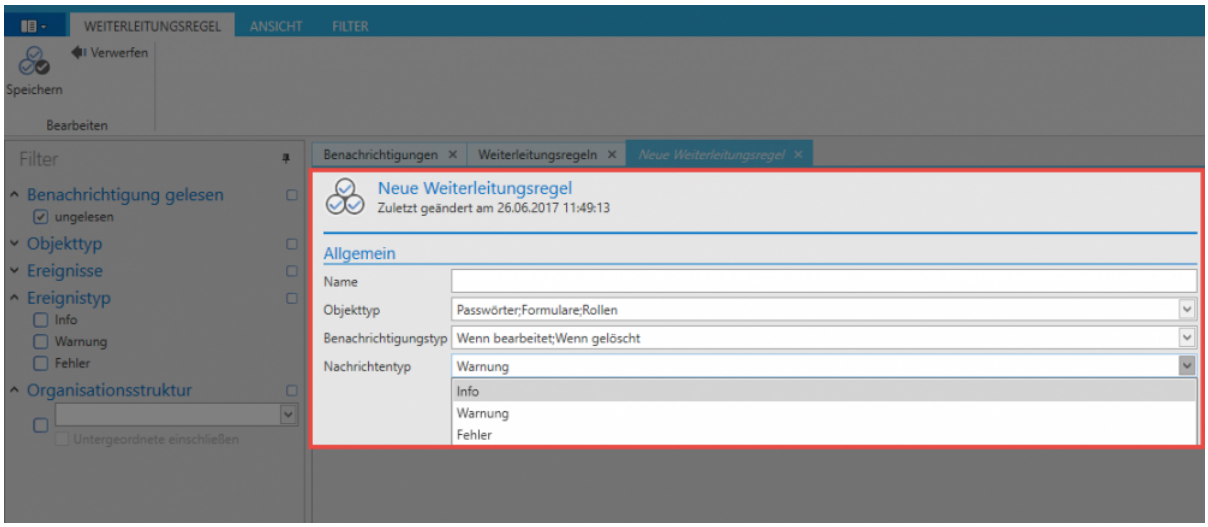
Über die beiden Buttons in der Ribbon ist es möglich, Benachrichtigungen als gelesen/ungelesen zu markieren. Besonders das in diesem Zusammenhang stehende Filterkriterium (s. nachfolgender Screenshot) ermöglicht das rasche Sortieren nach sowohl aktuellen als auch historischen Benachrichtigungen.




Das als gelesen/ungelesen Markieren ist sowohl über die Ribbon als auch über das Kontextmenü der rechten Maustaste möglich. Ist die dementsprechende Einstellung aktiviert, führt auch das Öffnen einer Benachrichtigung dazu, dass diese als gelesen markiert wird.

### E-Mail-Weiterleitung

Über die Ribbon können diverse Weiterleitungsregeln definiert werden. Eine Regel bestimmt, wann eine Benachrichtigung an ein E-Mail-Postfach weitergeleitet werden soll.



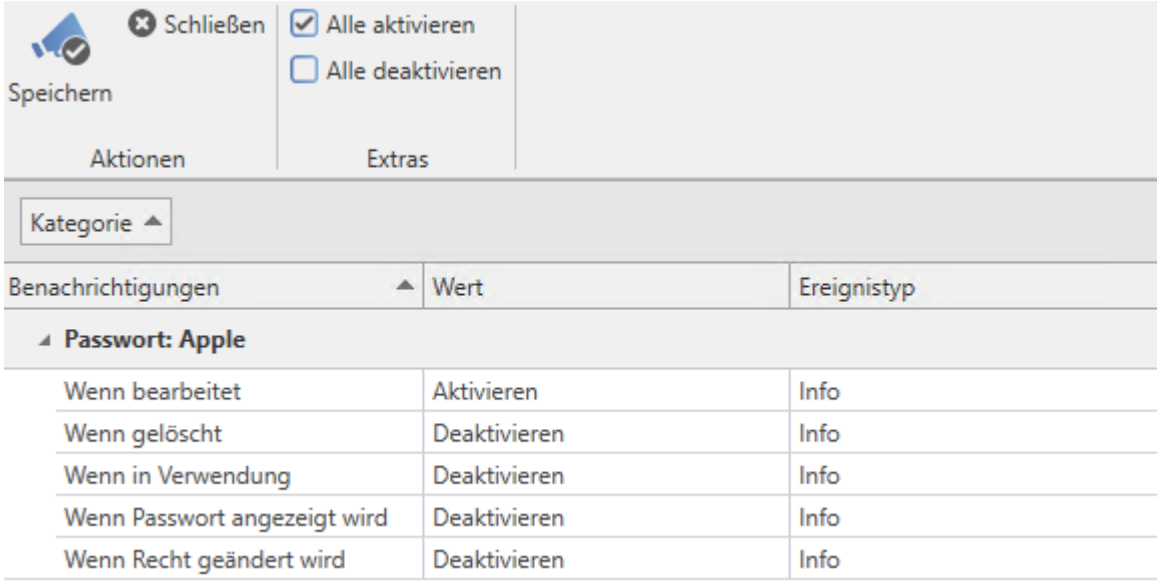

Im vorliegenden Fall werden alle Benachrichtigungen weitergeleitet, welche dem genannten Objekttyp (Passwörter, Formulare, Rollen) sowie dem Benachrichtigungstyp (Wenn bearbeitet, Wenn gelöscht) entsprechen. Zusätzlich kann noch nach dem Nachrichtentyp (=Ereignistyp) gefiltert werden.

> Voraussetzung für eine Weiterleitung ist, dass unter Konto im Hauptmenü für den angemeldeten Benutzer eine E-Mail Adresse hinterlegt ist

**Passwort Öffnet den die Benachrichtigung betreffenden Datensatz in einem separaten Tab**

# Manuelle Konfiguration von Benachrichtigungen

Unabhängig vom ausgewählten Modul können auf Objekte manuell Benachrichtigungen konfiguriert werden. Über die Ribbon im Reiter “Aktionen” öffnet sich folgender Dialog:



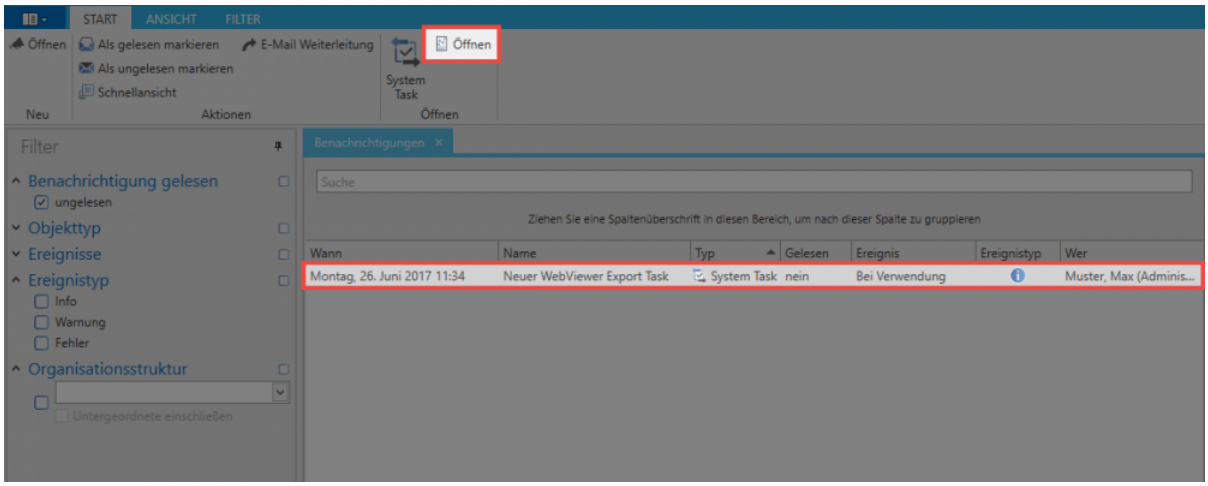

- **Benachrichtigung**: Definition des Auslösers
- **Wert**: Bestimmt, ob für den unter zuvor definierten Auslöser eine Benachrichtigung erzeugt wird. Im vorliegenden Datensatz “Apple” erfolgt diese nur, wenn der Datensatz bearbeitet wird.
- **Ereignistyp**: Bei erzeugten Benachrichtigungen kann zwischen “Info”, “Warnung” und “Fehler” unterschieden werden. Dies kann z.B. als zusätzliches Filterkriterium genutzt werden.

Im Gegensatz zu vorherigen Editionen erfolgt die Konfiguration von Benachrichtigungen am besten manuell. Auf diese Art und Weise kann man sicherstellen, dass wirklich nur bei relevanten Ereignissen eine Benachrichtigung ausgelöst wird.

# Weitere Auslöser von Benachrichtigungen

Zusätzlich zu den manuell konfigurierbaren Benachrichtigungen existieren im Password Safe weitere Auslöser, welche Benachrichtigungen nach sich ziehen können.

- **Siegel**: Freigabeanfragen für versiegelte Datensätze werden über das Benachrichtigungssystem abgewickelt
- **System Tasks**: Erstellt man automatisierte Berichte über System Tasks, werden diese auch in Form von Benachrichtigungen zur Verfügung gestellt. Wählt man eine solche Benachrichtigung aus, kann man über den dann in der Ribbon zur Verfügung stehenden Button direkt öffnen.



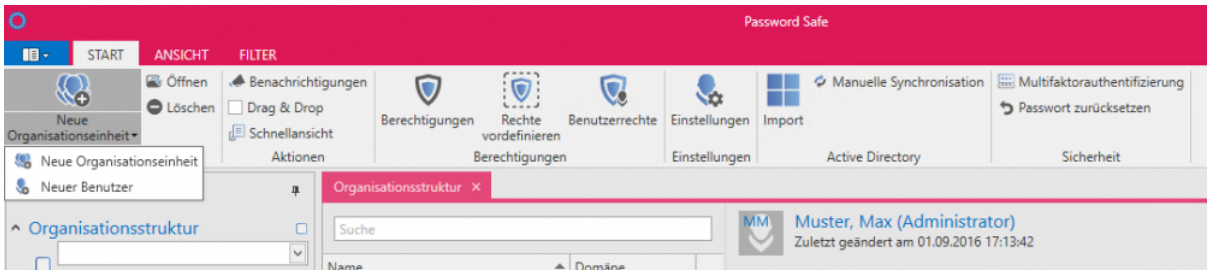
# Organisationsstruktur

## Was sind Organisationsstrukturen?

Die Ablage von Passwörtern oder Dokumenten erfolgt letztendlich immer gemäß definierter Organisationsstrukturen. Das Modul ermöglicht die Definition beliebig komplexer Strukturen, welche später die Basis für die systematische Ablage von Daten bilden. Eine Anlehnung an bereits vorhandene Organigramme des Unternehmens, bzw. der Abteilung, bietet sich hier oftmals an. Natürlich ist es auch möglich andere Kriterien, wie z.B. die ausgeübte Funktion/Tätigkeit, als Grundlage für die Erstellung von Hierarchien heranzuziehen. Es bleibt immer dem Kunden selbst überlassen, welche Struktur für den Einsatzzweck am sinnvollsten ist. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert.


## Modulspezifische Ribbonfunktionen

Die Bedienung der Ribbon unterscheidet sich in ein paar Punkten grundsätzlich von der Handhabung in anderen Modulen. Nachfolgend soll nur auf die sich unterscheidenden Elemente innerhalb der Ribbon eingegangen werden. Die restlichen Aktionen sind im Modul Passwörter bereits erläutert.

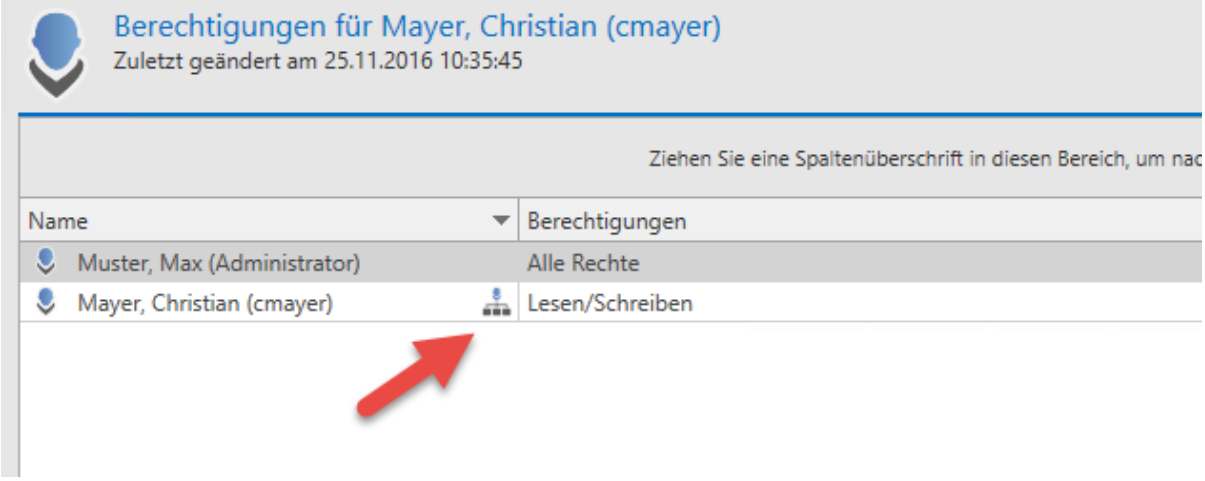



- **Neue Organisationseinheit/Benutzer**: Sowohl über die Ribbon, über den Shortcut “STRG + N” als auch über das Kontextmenü der rechten Maustaste können Neue Organisationseinheiten, bzw. neue Benutzer angelegt werden. Aufgrund der Komplexität existiert für diesen Unterpunkt separate Kapitel: neue Organisationsstrukturen / neue Benutzer
- **Drag & Drop**: Aktiviert man diese Option, ist das Verschieben von Benutzern oder Organisationseinheiten in der Listenansicht per Drag & Drop möglich
- **Berechtigungen**: Die Konfiguration von Berechtigungen innerhalb der Organisationsstruktur sind einerseits wichtig für die Administration der Struktur an sich, als auch als Grundlage für das Berechtigen gemäß der Vererbung aus Organisationsstrukturen. Dieses Nutzen von **“Rechte vordefinieren”** wird in einem separaten Abschnitt erläutert.

- **Einstellungen**: Können sowohl auf Benutzer als auch auf Organisationseinheiten konfiguriert werden. Näheres zu den Benutzereinstellungen…
- **Active Directory**: Die Anbindung an das Active Directory (ab der Enterprise Edition verfügbar) wird in einem eigenen Kapitel erläutert
- **Multifaktor-Authentifizierung**: Die Anmeldung nach positiver Authentifizierung durch einen weiteren Faktor schafft zusätzliche Sicherheiten. Mehr zum Thema…
- **Passwort zurücksetzen**: Administratoren können die Passwörter, mit denen sich Benutzer am Password Safe anmelden, auf einen definierbaren Wert zurücksetzen. Dies ist natürlich nur dann möglich, wenn die Active Directory Anbindung über die Ende zu Ende Verschlüsselung konfiguriert wurde. Im alternativen Master Key Modus wird die Authentifizierung an die korrekte Eingabe des AD-Passwortes gekoppelt.

> Für das Zurücksetzen eines Benutzerpasswortes ist die Mitgliedschaft in dem Benutzer Voraussetzung.

Nachfolgend eine Konfiguration eines Benutzers, bei der lediglich der Benutzer selbst Mitglied ist.




Diese Konfiguration ermöglicht, dass das Benutzerpasswort nicht durch Administratoren zurückgesetzt werden kann. Der Nachteil ist, dass bei Verlust des Passwortes technisch keinerlei Möglichkeit besteht, das Passwort systemseitig zu “resetten”.

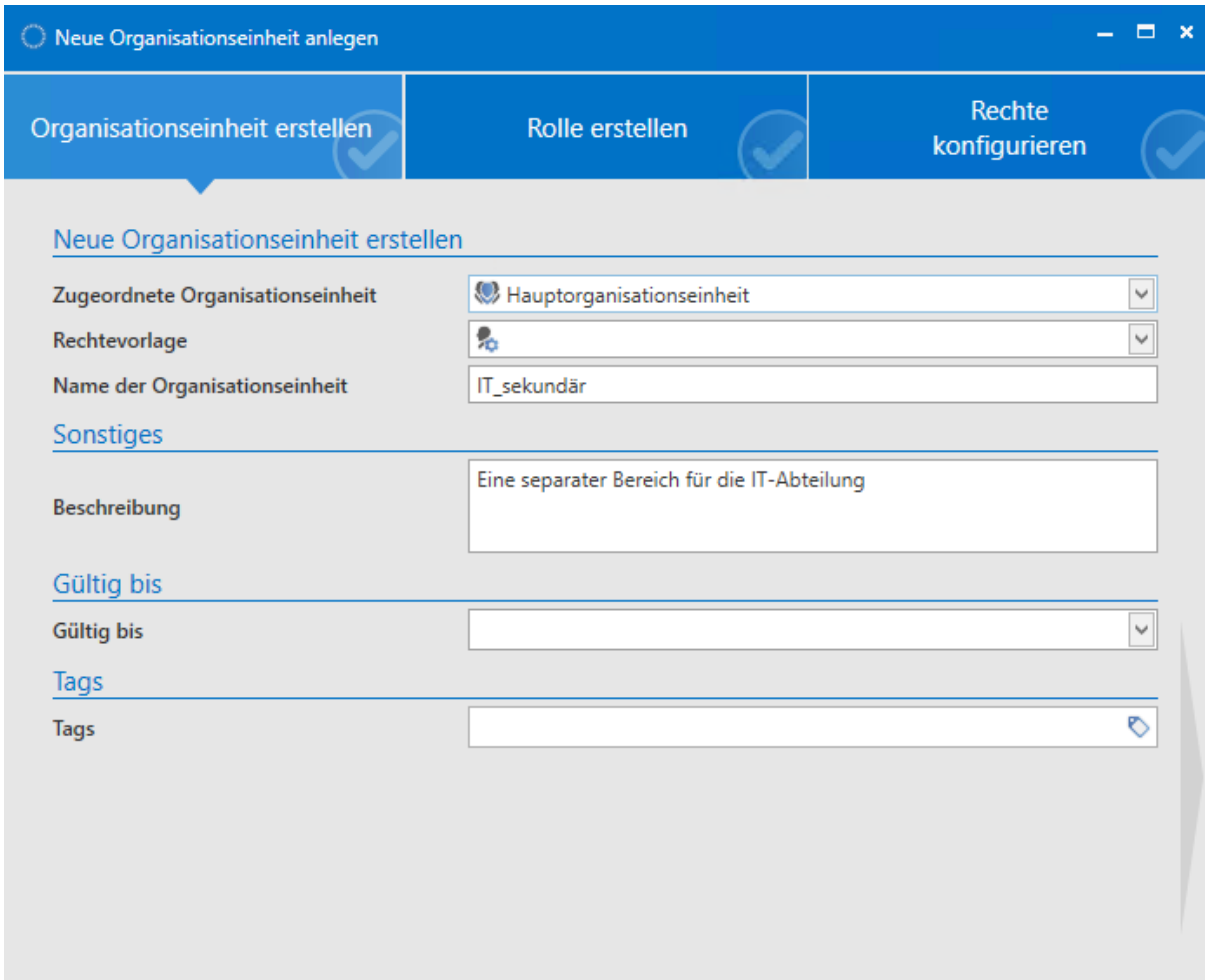
> Es wird **nicht** empfohlen, nur dem Benutzer selbst die Mitgliedschaft zu definieren. Bei Verlust des Passwortes kann anderweitig nicht eingegriffen werden.

# Anlegen lokaler Organisationseinheiten

> ! Es wird das Recht **Kann neue Organisationseinheiten anlegen** sowie Sicht auf das **Modul Organisationseinheiten** benötigt

Sowohl Benutzer als auch Organisationseinheiten selbst können wie gewohnt über die Ribbon (Alternativ über Ctrl. + N oder Kontextmenü) angelegt werden. Gestützt werden diese Vorgänge durch separate Assistenten. Nachfolgend wird eine neue Organisationseinheit erstellt:

### Organisationseinheit erstellen

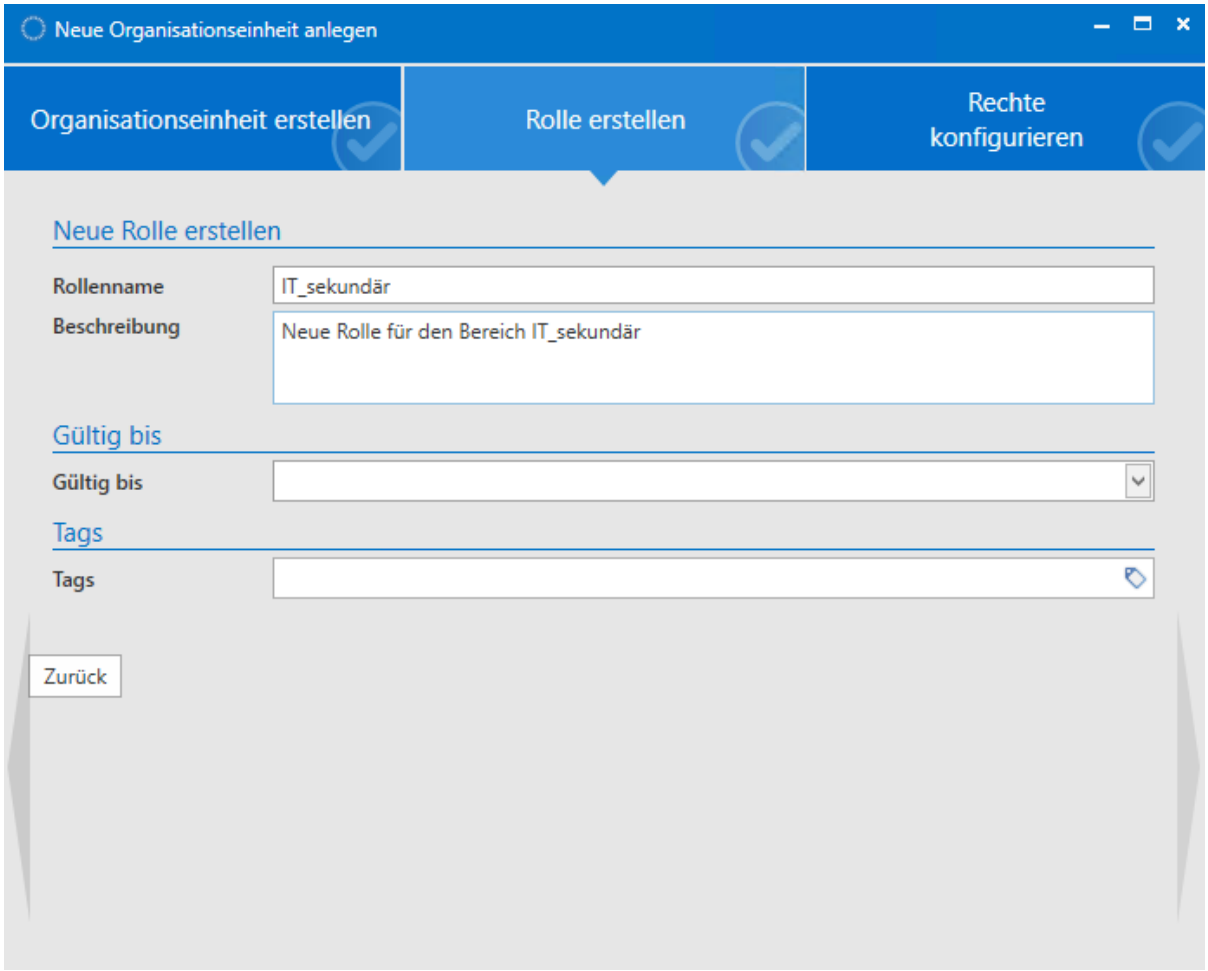



- **Zugeordnete Organisationseinheit**: Legt man hier die **Hauptorganisationseinheit** fest, erhält das neue Objekt keine Zuordnung an eine bestehende Organisationseinheit

- **Rechtevorlagengruppe**: Hat man unter “zugeordneter Organisationseinheit” eine bereits bestehende ausgewählt, kann man hier eine der dort vorhandenen Rechtevorlagengruppen auswählen

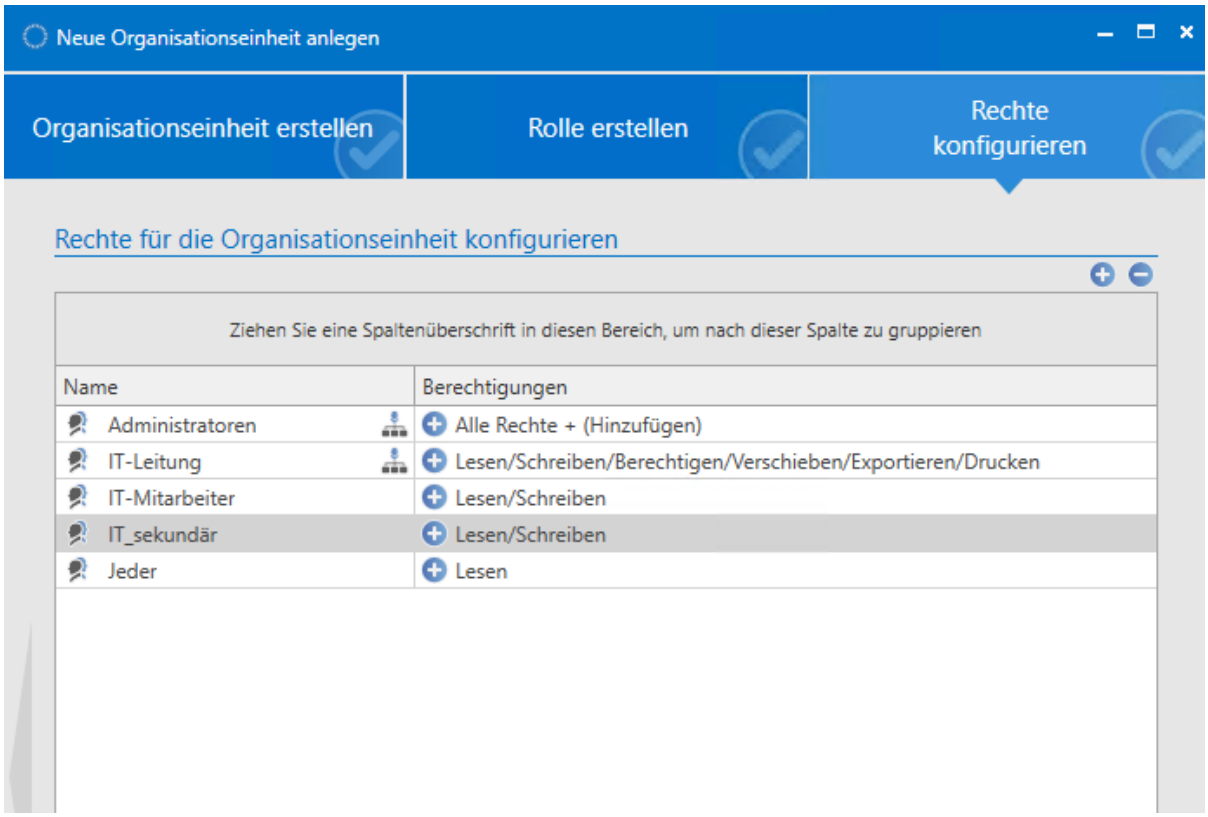
Als Default wird die in der Listenansicht markierte Organisationseinheit herangezogen. Dies betrifft die Felder “zugeordnete Organisationseinheit” wie auch “Rechtevorlage”.

### Rolle erstellen




Im Zuge der Erstellung einer neuen Organisationseinheit ist im Assistenten im zweiten Reiter das direkte Anlegen einer neuen Rolle möglich. Diese Rolle wird nicht nur erstellt, sondern auch mit “lesend” auf die neu erstellte Organisationseinheit berechtigt.

### Rechte konfigurieren




Im dritten Reiter des Assistenten sind die Berechtigungen auf die neu zu erstellende Organisationseinheit definierbar. Wurde im ersten Reiter eine zugeordnete Organisationseinheit, bzw. eine Rechtevorlagengruppe definiert, so erbt die neue Organisationseinheit deren Rechte. In diesem Zuge können diese Berechtigungen bei Bedarf angepasst werden.

# Benutzerverwaltung

## Wie werden im Password Safe Benutzer verwaltet?

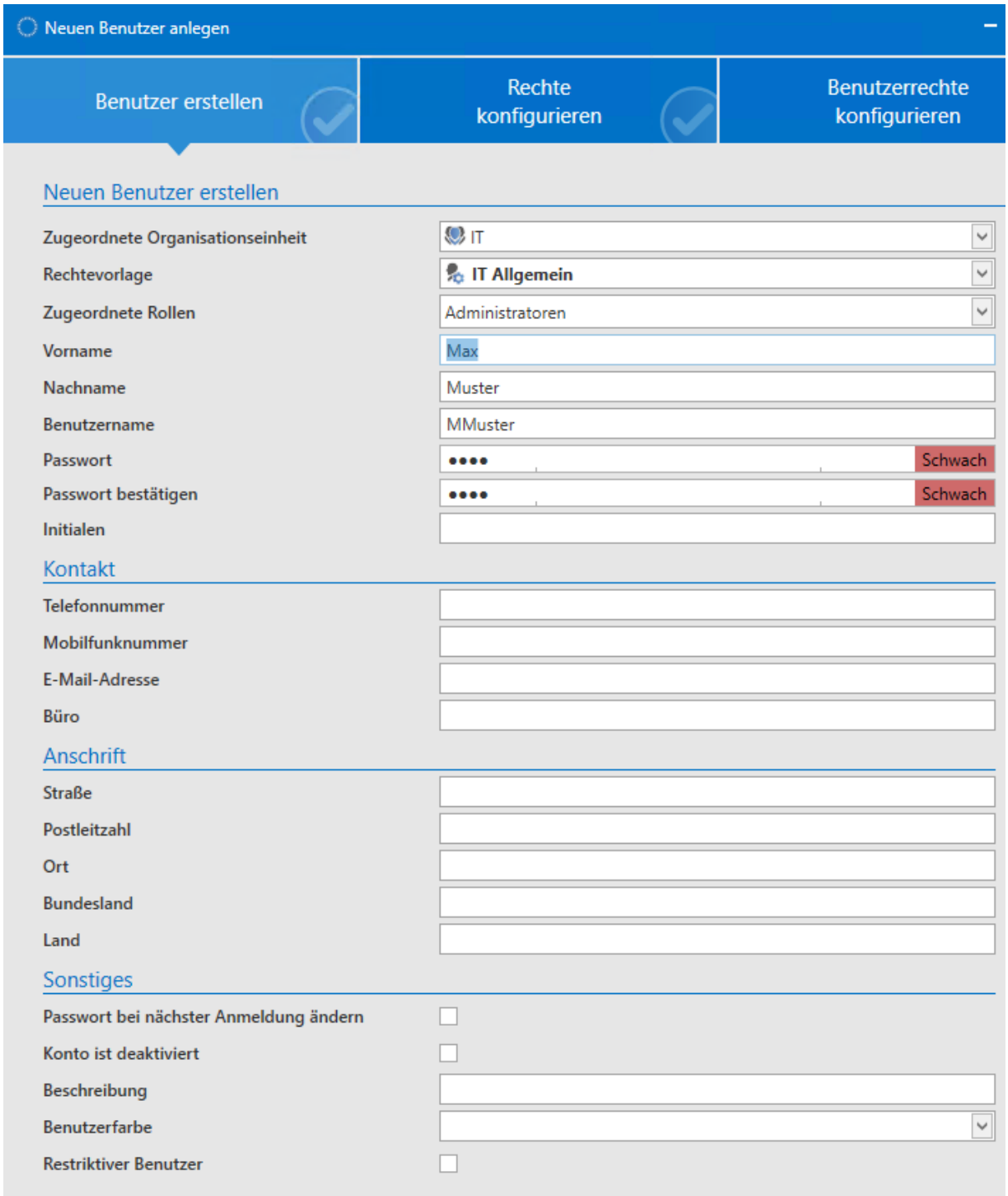
Die Art der Benutzerverwaltung hängt stark davon ab, ob das Active Directory angebunden wurde oder nicht. Im Master Key Modus bleibt das Active Directory das führende System. Demnach erfolgt die Benutzerverwaltung auch aufseiten des AD. Falls der Password Safe das führende System wird, wie z.B. beim Ende zu Ende Modus, erfolgt die Benutzerverwaltung im Modul Organisationsstrukturen. Auf die Details wird in den jeweiligen Kapiteln ausführlicher eingegangen. Mehr…

## Anlegen lokaler Benutzer

! Es wird das Recht **Kann neue Benutzer anlegen** sowie Sicht auf das **Modul Organisationseinheiten** benötigt

Grundsätzlich ist da Anlegen neuer Benutzer analog zum Erstellen einer lokalen Organisationseinheit durchzuführen. Nachfolgend soll deshalb nur auf die Unterschiede eingegangen werden.

## Benutzer erstellen




- **Zugeordnete Rollen**: Neuen Benutzern können direkt beim Erstellen eine oder mehrere Rollen zugewiesen werden
- **Passwort bei der nächsten Anmeldung ändern**: Der Benutzer wird bei der nächsten Anmeldung aufgefordert, sein Benutzerpasswort zu ändern (obligatorisch)
- **Konto ist deaktiviert**: Der Benutzer wird im Zustand “deaktiviert” erstellt. Das Konto ist demnach nicht nutzbar. Diese Option kann danach mit Schreibrechten auf einem Benutzer gesetzt/entfernt werden. Im Bearbeiten-Modus kann das Konto auch im laufenden Betrieb deaktiviert werden.

- **restriktiver Benutzer**: In vielen Unternehmen existieren Kontrollinstanzen, welche nur die Integrität und Hierarchien der Informationen zueinander überprüfen, jedoch nicht selbst produktiv mit denen arbeiten sollen. Ein Datenschutzbeauftragter könnte eine solche Person sein, ebenso in manchen Fällen auch ein Administrator. Dies wäre dann der Fall, wenn der Administrator zwar Personen berechtigen, jedoch selbst nicht Einsicht auf die Daten haben soll. Das Merkmal **restriktiver Benutzer** bezieht sich auf die Einschränkung im Hinblick der Einsicht auf das Passwortfeld. Es geht hier also um rein administrative Benutzer, bzw. Kontrollinstanzen.

Ein restriktiver Benutzer kann keine Passwörter einsehen

### Rechte konfigurieren

Im zweiten Reiter des Assistenten sind die Berechtigungen auf den neu zu erstellenden Benutzer definierbar. Wurde im ersten Reiter eine zugeordnete Organisationseinheit, bzw. eine Rechtevorlagengruppe definiert, so erbt der Benutzer diese Rechte. In diesem Zuge können diese Berechtigungen bei Bedarf angepasst werden.

### Benutzerrechte konfigurieren

Benutzer erhalten Benutzerrechte stets über eine Rolle, benutzerspezifisch oder global (vergl. Benutzerrechte). Ist im ersten Reiter “Benutzer erstellen” keine Rolle definiert, enthält der dritte Reiter demnach die global definierten Benutzerrechte.

# Import von Benutzern

Der Import aus dem Active Directory ist auf zwei Arten möglich, welche in einem separaten Kapitel beschrieben werden.

# Benutzer Passwörter / Anmeldung am Client

## Benutzer Passwörter

Je nach dem, um welchen Typ von Benutzer es sich handelt, bekommt er sein Passwort entweder in Password Safe zugewiesen oder die Anmeldung erfolgt mit den Zugangsdaten der Domäne. Auch die Anmeldung der Benutzer unterscheidet sich je nach Typ.

### Unterschiede bei den Benutzern und Passwörtern

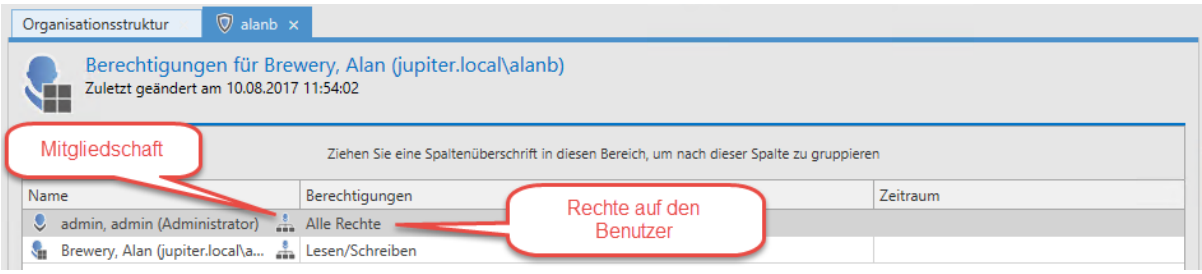
- **Lokale Benutzer**
  sind diejenigen Benutzer welche direkt in Password Safe erstellt werden. Diesen Benutzern muss direkt beim Anlegen ein Passwort zugewiesen werden. Werden lokale Benutzer aus einer älteren Version migriert, bekommen diese ein zufällig generiertes Passwort, welches per E-Mail zugestellt wird.

- **AD Benutzer im Ende zu Ende Modus**
  müssen ebenfalls in Password Safe mit einem Passwort versorgt werden. Auch diese Benutzer bekommen bei einer etwaigen Migration ein neues Passwort per E-Mail zugestellt.

- **AD Benutzer im Masterkey Modus**
  melden sich direkt mit Zugangsdaten der Domäne an. Es muss somit kein Passwort zugeteilt werden. Da sich diese Benutzer direkt gegenüber dem Active Directory authentifizieren, gilt immer das dort aktuell hinterlegte Passwort. Auch nach einer Migration können sich diese Benutzer direkt mit dem bekannten Passwort anmelden

### Benötigte Rechte

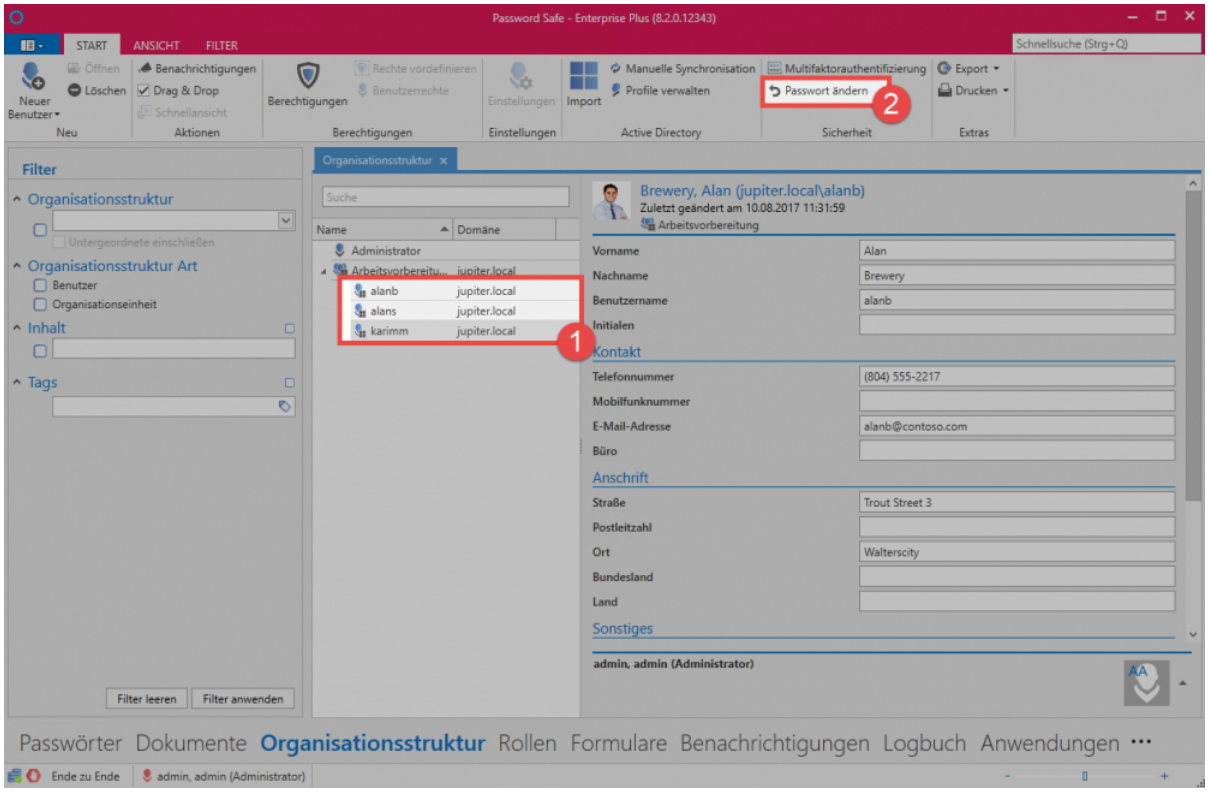
Um die Passwörter der Benutzer vergeben bzw. ändern zu können, sind verschiedene Rechte nötig. Voraussetzung ist zum einen das Benutzerrecht **Kann Organisationsstruktur Modul anzeigen**. Weiterhin sind die Rechte **Lesen** und **Schreiben** auf den Benutzer nötig. Schlussendlich wird auch die Mitgliedschaft des Benutzers benötigt. Standardmäßig haben der Benutzer selbst sowie derjenige Benutzer der ihn angelegt bzw. importiert hat, die Rechte sein Passwort zu ändern.



## Zuweisen und Ändern von Passwörtern

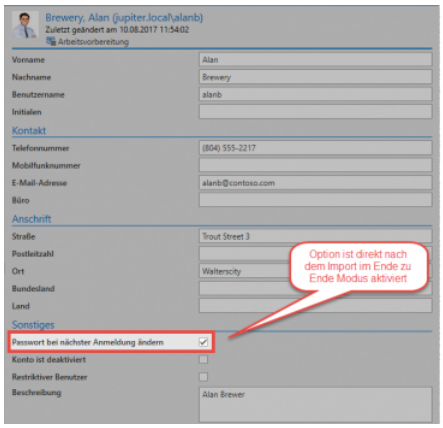
Wie bereits geschildert, bekommen lokale Benutzer das initiale Passwort direkt beim Erstellen zugewiesen. Anders verhält es sich bei Benutzern welche im Ende zu Ende Modus importiert werden. Diese haben direkt nach dem Import kein Passwort und können sich somit nicht anmelden. Es ist also nötig, nach dem Import die Passwörter zu vergeben.

Die Passwörter können direkt über die Ribbon zugewiesen bzw. geändert werden. Selbstverständlich ist hier auch eine Multiselektion möglich, falls beispielsweise mehreren, importierten Benutzern das gleiche Passwort gegeben werden soll.

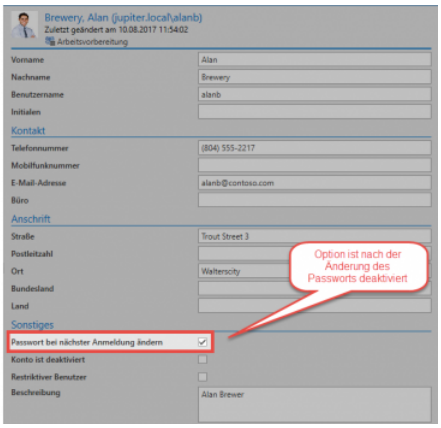



## Passwort bei nächster Anmeldung ändern

Gerade wenn mehrere Benutzer das gleiche Initialpasswort bekommen, ist es sinnvoll eine Änderung auf ein individuelles Passwort zu erzwingen. Hierfür gibt es eine entsprechende Option. Bei **lokalen Benutzern** kann diese während des Erstellens des Benutzers aktiviert werden. Bei **Benutzern im Ende zu Ende Modus** wird die Option aus Sicherheitsgründen direkt beim Import aktiviert. Nach erfolgter Anmeldung und Änderung des Passworts wird die Option automatisch deaktiviert.








### Sicherheit der Passwörter

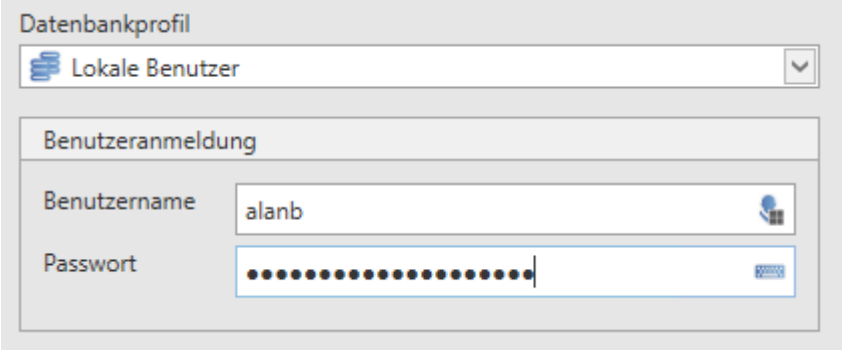
Um ein ausreichende Stärke der Passwörter zu gewährleisten, wird empfohlen eine entsprechende Passwort Richtlinie zu erstellen. Hier ist vor allem darauf zu achten, dass der Benutzername ausgeschlossen wird. Abschließend muss die Passwortrichtlinie noch als Benutzer Passwortrichtlinie festgelegt werden.

## Anmeldung an der Datenbank

Je nach Typ des Benutzers unterscheidet sich die Anmeldung an der Datenbank.

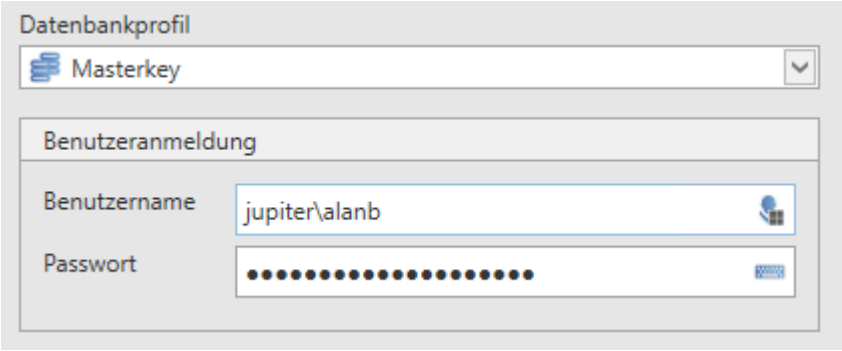
### Lokaler Benutzer

Die Anmeldung lokaler Benutzer erfolgt einfach mittels Benutzername und dem zugewiesenen Passwort.

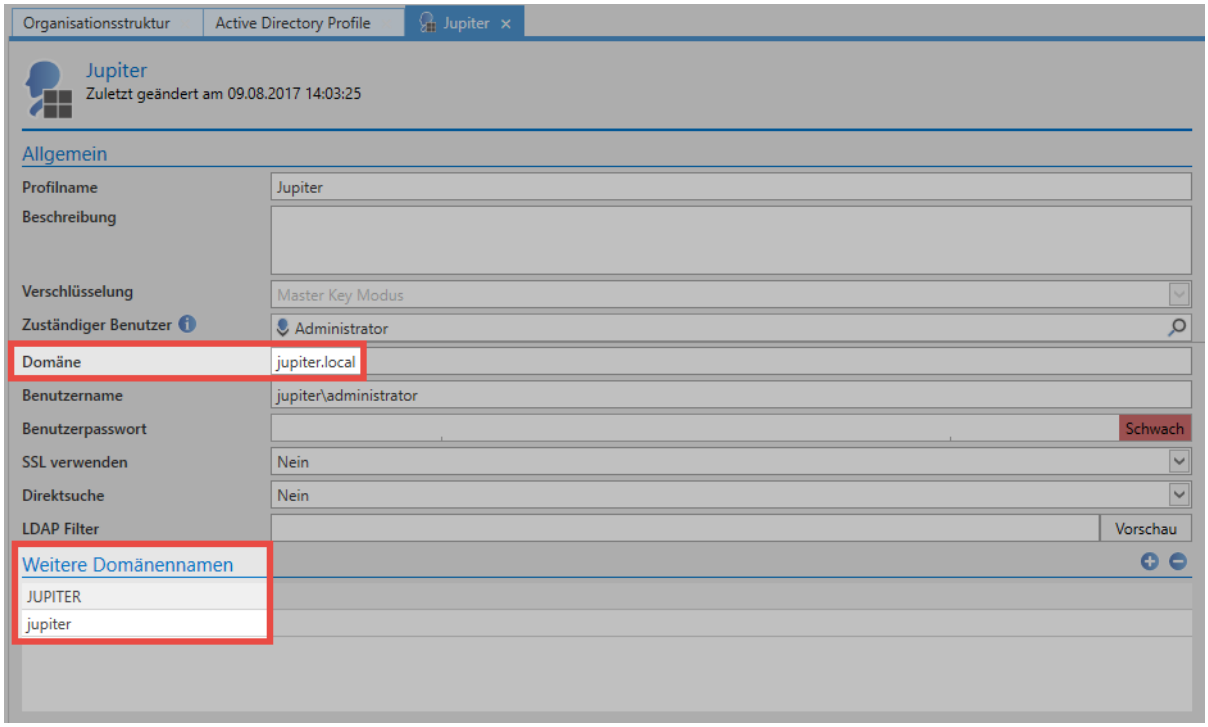



### AD Benutzer

Sofern nur eine Domäne konfiguriert ist, können sich Benutzer aus dem AD mit Benutzername und Passwort anmelden, wie die lokalen Benutzer auch. Sind mehrere Domänen konfiguriert oder gibt es einen lokalen Benutzer mit dem gleichen Namen, so muss die Domäne vorangestellt werden:




Die Domäne muss hierbei so angegeben werden, wie sie im AD Profil unter **Domäne** konfiguriert ist. Unter **Weitere Domänennamen** können andere Ausprägungen der Domäne hinterlegt werden.



# Berechtigungen auf Organisationsstrukturen

## Relevanz

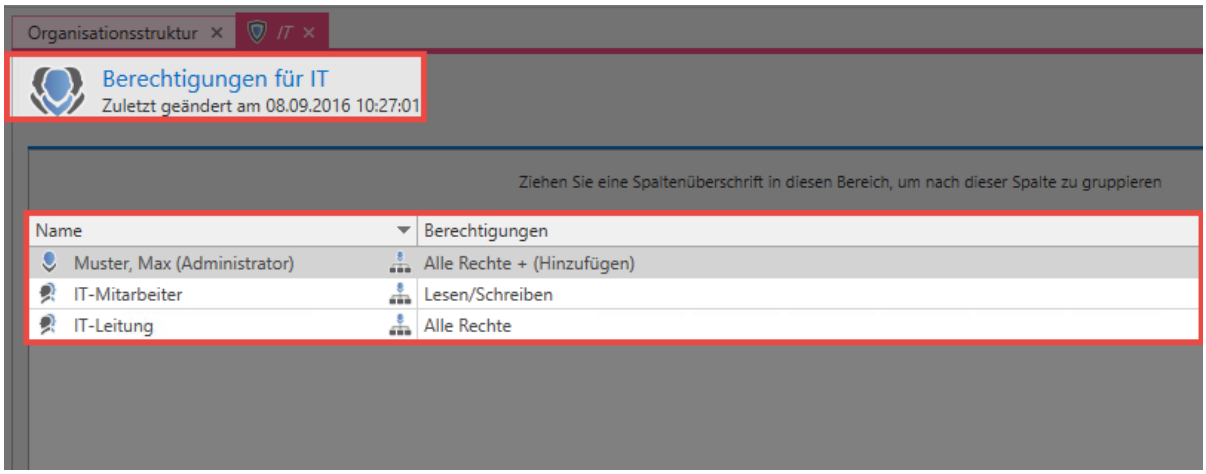
In erster Linie definiert man durch diese Berechtigungen, welche Benutzer/Rollen auf Organisationsstrukturen in welcher Form berechtigt sind. Darüber hinaus gibt es **zwei Mechanismen**, welche direkt auf den Berechtigungen von Organisationsstrukturen aufbauen.

1. **Einschränkung der Sichtbarkeit**: Bereits im Kapitel Sichtbarkeit wurde erläutert, dass das selektive Vorenthalten von Informationen ein sehr effektiver Schutzmechanismus ist. Die Konfiguration dieser Sichtbarkeit erfolgt direkt innerhalb der Berechtigungen auf Organisationsstrukturen.
2. **Vererbung von Berechtigungen auf Datensätze**: Als Systemstandard ist die Vererbung aus Organisationsstrukturen definiert. Das bedeutet, dass man zwischen den Berechtigungen auf eine Organisationsstruktur sowie den Berechtigungen auf Daten, welche in diesen Organisationsstrukturen liegen, **nicht** unterscheidet.

Die Gestaltung der Berechtigung von Organisationsstrukturen wirkt sich also auf vielerlei Arten auf das weitere Arbeiten mit dem Password Safe aus. Nachfolgende Grafik beschreibt die genannten Schnittstellen.


## Berechtigungen auf Organisationsstrukturen

Sowohl die Sichtbarkeit als auch Vererbungsmechanismen sollen nachfolgend nicht betrachtet werden. Es geht demnach ausschließlich um die Berechtigungen auf die eigentliche Organisationsstruktur. Es wird definiert, welche Benutzer und Rollen in welcher Form auf eine gegebene Organisationsstruktur berechtigt sind. Über die Ribbon oder über das Kontextmenü der rechten Maustaste können Berechtigungen für Organisationsstrukturen definiert werden. Es erscheint der Berechtigungs-Tab:




Die grundlegenden Mechaniken beim Setzen von Berechtigungen sind im Berechtigungskonzept ausführlich erklärt.

**Wichtig ist, dass man die hier angezeigten Berechtigungen auch richtig deutet! Es geht in obigem Beispiel um die Berechtigungen auf die "Organisationsstruktur IT"**. Der Benutzer Max Muster besitzt alle Rechte auf die Organisationsstruktur IT, kann demnach diese Struktur bearbeiten, löschen und auch Berechtigungen setzen.

## Das Hinzufügen-Recht

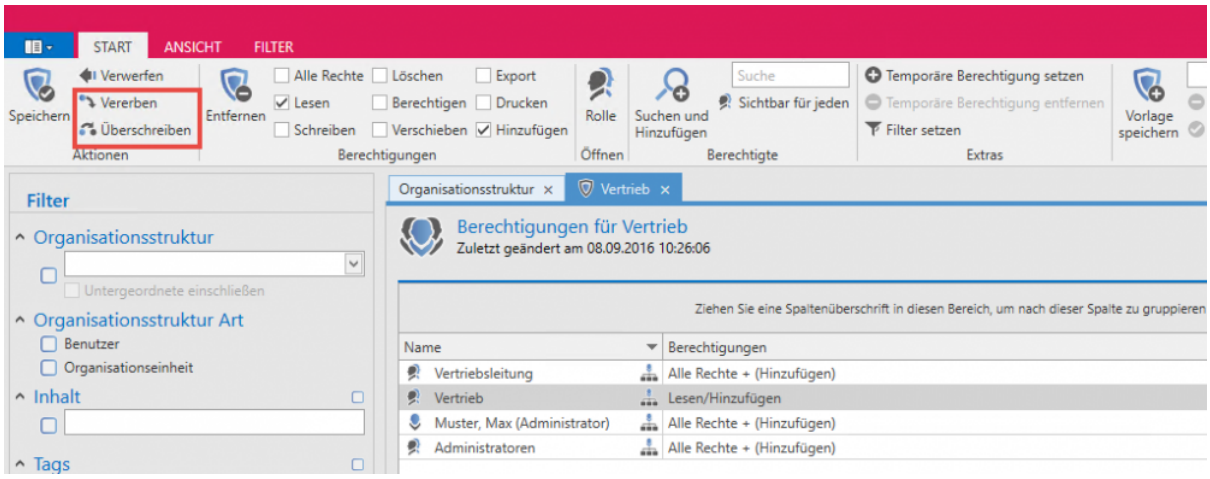
Das Recht "Hinzufügen" genießt unter den verfügbaren Rechten eine Sonderstellung, da es sich nicht auf die Organisationseinheit selbst bezieht, sondern auf Daten, welche darin erstellt werden. Pauschal kann man sagen, dass das Hinzufügen von Objekten in eine Organisationseinheit das Hinzufügen-Recht voraussetzt. Will man als Benutzer einen neuen Datensatz in einer Organisationseinheit ablegen, benötigt man das genannte Recht. Im obigen Beispiel wäre das Hinzufügen neuer Datensätze lediglich dem Administrator gestattet. Auch die IT-Leitung, welche alle anderen Rechte auf die Organisationsstruktur "IT" haben, besitzen nicht das Recht, neue Datensätze anzulegen.

Es geht beim Hinzufügen Recht lediglich um das Recht, Objekte in einer Organisationsstruktur anlegen zu dürfen.

# Vererbung von Berechtigungen

## Was wird vererbt in Organisationsstrukturen?

Öffnet man die Berechtigungen einer Organisationsstruktur, werden die aktuell konfigurierten Berechtigungen einsehbar. Im nachfolgenden Beispiel sind insgesamt vier Rollen in verschiedenem Maße auf die Organisationsstruktur berechtigt.




In der Ribbon stehen nun zwei markierte Optionen zur Verfügung.

- **Vererben**: Hierbei werden beim Speichern alle in der aktuellen Berechtigungsmaske definierten Konfigurationen auf darunterliegende Organisationsstrukturen vererbt. Die Berechtigungen verhalten sich additiv
- **Überschreiben**: Es werden beim Speichern alle definierten Konfigurationen auf darunterliegende Organisationsstrukturen angewendet. Die bisherigen Berechtigungen gehen verloren.

Beide Mechanismen sind durch eine Sicherheitsabfrage geschützt. Sind sowohl “Vererben” als auch “Überschreiben” gesetzt, verhält sich “Überschreiben” dominant.

> ! Beide Mechanismen sind nicht durch Benutzerrechte geschützt. Man benötigt das Recht **Berechtigen** auf der Organisationsstruktur, um die Vererbung, bzw. das Überschreiben zu aktivieren.

# Active Directory Anbindung

## Was sind Active Directory Profile?

Die Anbindung an das Active Directory (AD) wird über sogenannte AD-Profile hergestellt. Diese enthalten alle für eine Verbindung zum AD relevanten Informationen und ermöglichen den Import/die Synchronisation von Benutzern, Organisationseinheiten oder Rollen. Um unterschiedliche ADs anzusprechen, können selbstverständlich auch mehrere AD-Profile erstellt werden.

## Zwei Import Modi im Vergleich

Password Safe unterscheidet beim Import aus dem Active Directory zwischen zwei Modi, welche sich signifikant unterscheiden und in separaten Kapiteln erläutert werden.

- Ende zu Ende Verschlüsselung
- Master Key Modus

Prinzipiell unterscheiden sich beide Varianten durch das Vorhandensein der genannten Verschlüsselung. In der Lösung mit aktiver Ende zu Ende Verschlüsselung **(E2EE)** muss zwar auf Komfort verzichtet werden (s. Tabelle), der Gewinn an Sicherheit ist jedoch immens. Im Master Key Modus wird am Server ein Master Key erstellt, welcher auf alle Benutzer, Organisationseinheiten und Rollen voll berechtigt wird. Dies stellt einen zusätzlichen Angriffsvektor dar, welcher im Ende zu Ende Modus nicht gegeben ist. Im Gegenzug können jedoch im Master Key Modus die Benutzer über die Synchronisation mit dem Active Directory aktualisiert werden. Ebenso werden Zugehörigkeiten zu Organisationseinheiten und Rollen importiert. Im de facto sichereren Ende zu Ende Modus muss diese Synchronisation der Änderungen manuell durchgeführt werden.

> Es ist technisch möglich mehrere Profile mit unterschiedlichen Modi zu erstellen. Der Übersichtlichkeit halber ist dies jedoch nicht empfohlen.

| | Ende zu Ende Modus | Master Key Modus |
|---|---|---|
| **Ende zu Ende Verschlüsselung** | + | - |
| **Import von Benutzerinformationen** | + | + |
| **Import von Rollenzugehörigkeiten** | - | + |
| **Import von Zugehörigkeiten zu Organisationseinheiten** | - | + |
| **Synchronisation von Benutzerinformationen** | - | + |

| | | |
|---|---|---|
| **Synchronisation von Rollenzugehörigkeiten** | - | + |
| **Synchronisation von Zugehörigkeiten zu Organisationseinheiten** | - | + |
| **Benutzer kann in Password Safe bearbeitet werden** | + | - |
| **Organisationseinheit kann in Password Safe bearbeitet werden** | + | - |
| **Rollen können in Password Safe bearbeitet werden** | + | - |
| **Passwort kann in Password Safe geändert werden** | + | - |
| **Anmeldung mit dem Domänenkennwort** | - | + |
| **Password Safe ist das führende System** | + | - |
| **Active Directory ist das führende System** | - | + |

Wie man sieht, bietet **E2EE die höchstmögliche Sicherheit**. Das Ziel ist lediglich der Import von Benutzern, Organisationseinheiten und Rollen. Deren Verwaltung und Konfiguration muss komplett im Password Safe erfolgen. Im Gegensatz hierzu ermöglicht die Anbindung im **Master Key Modus den größtmöglichen Komfort**. Es werden nicht nur Benutzer, Organisationseinheiten und Rollen, sondern auch deren Verknüpfungen bzw. Zugehörigkeiten importiert. Eine Synchronisation mit dem Active Directory ist möglich – **Das AD wird als führendes System verwendet**.

# Benutzer, Gruppen und Rollen

Beim Import, bzw. der Synchronisation aus dem Active Directory, werden die Benutzer in Password Safe ebenso als Benutzer angelegt. Auch die Organisationseinheiten werden in Password Safe als solche verwendet.

Damit Password Safe schnell in die gegebene Infrastruktur integriert werden kann, können auch Rollen direkt aus dem Active Directory importiert werden. Namentlich werden hier Active Directory Gruppen zu Password Safe Rollen.

> * Gruppen in Gruppen Mitgliedschaften, welche im Active Directory vorkommen können, werden innerhalb des Password Safes nicht abgebildet. Es werden beide Gruppen als Rollen importiert, jedoch eigenständig und nicht in irgendeiner Form miteinander verknüpft.

> ! Wurde beim Active Directory Profil der Master Key Modus gewählt, gilt das AD als führendes System. Rollen, welche importiert wurden, können in diesem Modus nicht lokal in Password Safe geändert werden.

- Ende zu Ende Verschlüsselung
- Master Key Modus

# Ende zu Ende Verschlüsselung

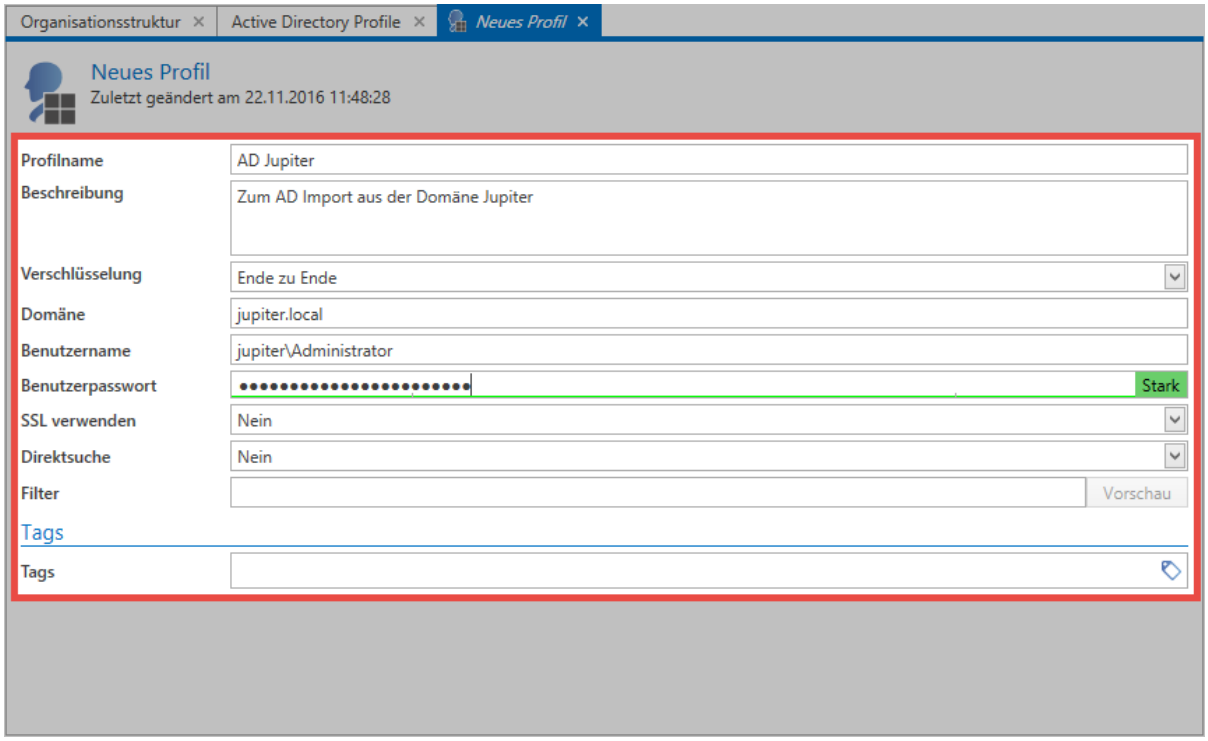
## Höchstmögliche Verschlüsselung

Das Active Directory Profil mit aktiver Ende zu Ende Verschlüsselung bietet derzeit die **höchstmögliche Sicherheit**. Importiert werden lediglich Benutzer, Organisationseinheiten sowie Rollen. Die Berechtigungen und das hierarchische Verhältnis der einzelnen Objekte zueinander muss im Password Safe separat konfiguriert werden. Der sich aus der Ende zu Ende Verschlüsselung ergebende Vorteil besteht darin, dass das Active Directory als mögliches Einfallstor “entschärft” wird. Im Master Key Modus besitzen Benutzer, welche das Active Directory kontrollieren, de facto kompletten Zugriff auf alle Passwörter, da das Zurücksetzen eines Windows-Benutzernamens die Anmeldung in fremdem Namen ermöglicht. Das Active Directory ist somit das führende System. **Mit aktiver E2EE benötigen Benutzer für den Password Safe ein eigenes Passwort**. Ein Zugang auf Benutzerdaten über das Active Directory ist demnach nicht gegeben.

## Erstellen des Profils

! Es wird das Recht **Kann neue Active Directory Profile anlegen** sowie Sicht auf das **Modul Organisationseinheiten** oder auf das “Modul Rollen” benötigt.

Das Erstellen eines neuen Profils wird über das Icon “Profile verwalten” in der Ribbon gestartet.

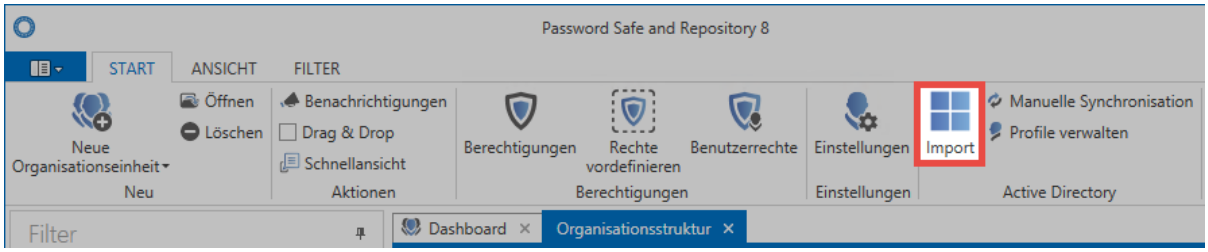


Im Feld “Verschlüsselung” muss “Ende zu Ende” gesetzt* werden

- Zum Zugriff auf das AD ist ein **Benutzer** nötig. Dieser wird im Format Domäne\Benutzer angegeben. Es ist zwingend nötig, dass dieser Zugriff auf das AD hat.
- Zum oben angegebenen Benutzer ist das zugehörige **Benutzerpasswort** (Domänenkennwort) nötig
- Falls das AD dies verlangt, kann die Verbindung über **SSL** aufgebaut werden
- Die **Direktsuche** ist bei sehr großen Strukturen zu empfehlen. Die Darstellung der Baumstruktur entfällt, Elemente können nur noch über die Suche gefunden und selektiert werden.
- Über den **Filter** kann über eine LDAP Query direkt ein AD-Pfad als Einstiegspunkt angeben werden

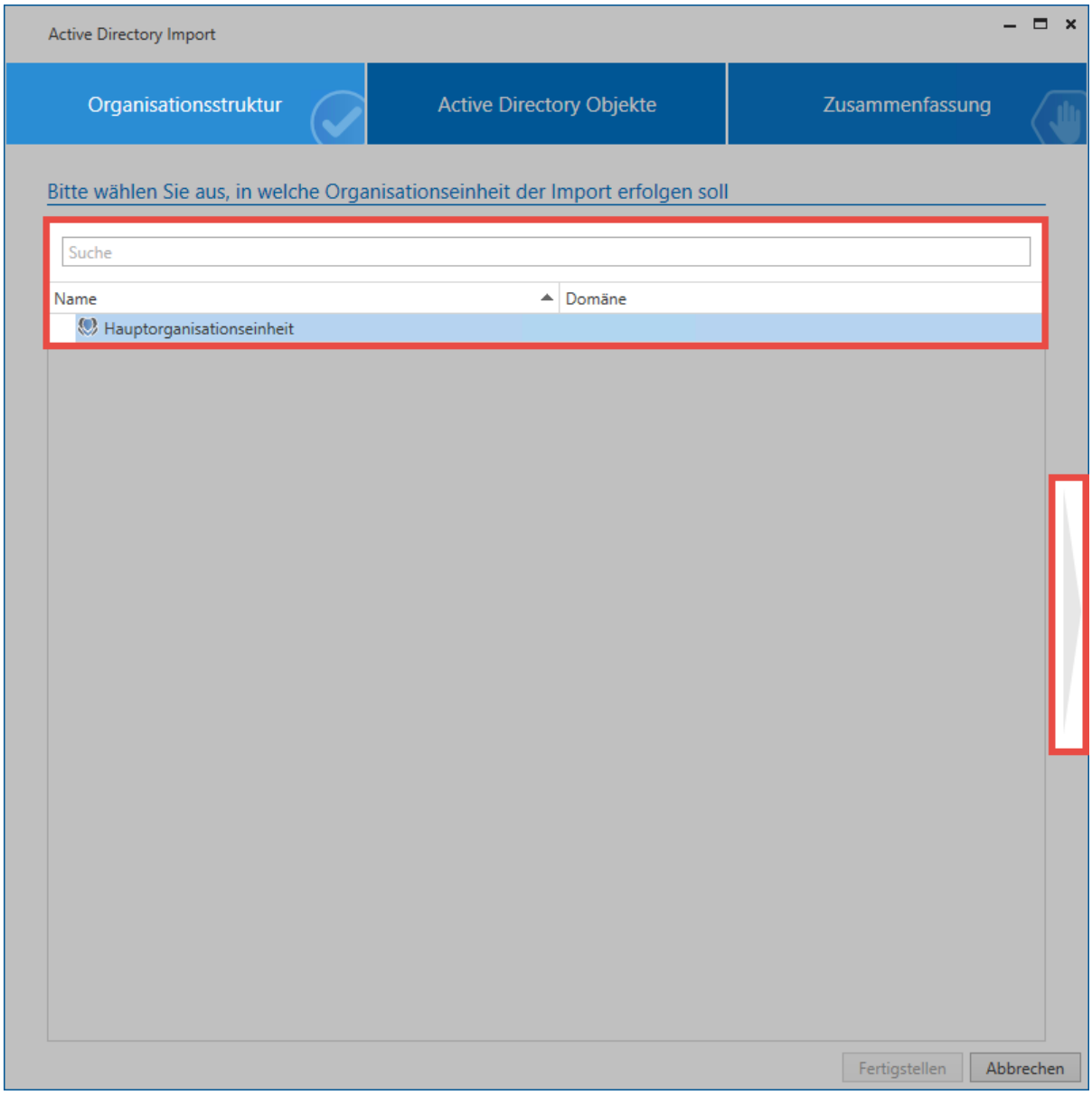
# Import

Der Import wird direkt in der Ribbon gestartet. Ein Assistent führt durch den kompletten Vorgang.



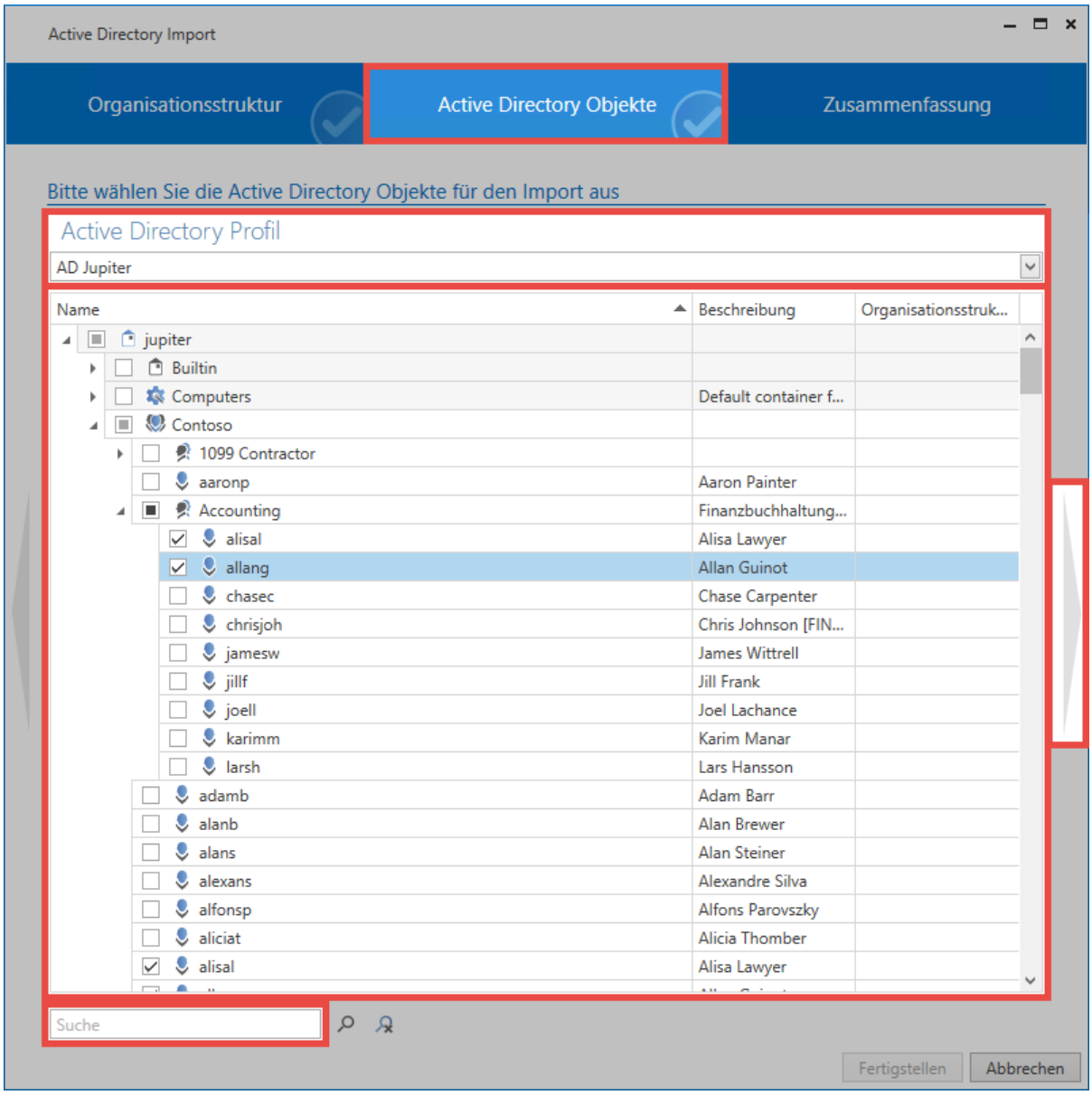

### Organisationsstruktur

Zunächst wird gewählt in welche Organisationseinheit der Import erfolgen soll. Existieren – wie in diesem Beispiel – noch keine Organisationseinheiten in der Datenbank, erfolgt der Import in die **Hauptorganisationseinheit**.




## Active Directory Objekte

Im nächsten Schritt erfolgt zunächst die Auswahl desjenigen Profils, mit dem importiert werden soll. Anschließend wählt man die Organisationseinheiten und/oder Benutzer zum Import aus. Hierfür steht eine Suche bereit.

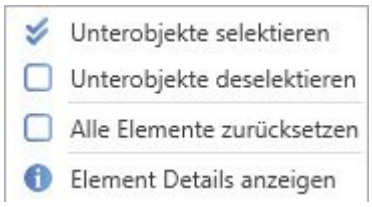



Es ist ersichtlich, dass die Organisationseinheiten **Jupiter** und **Contoso** Elemente beinhalten, welche importiert werden. Die Organisationseinheiten selbst werden nicht importiert. Die Markierung der Gruppe **Accounting** zeigt an, dass sowohl die Gruppe selbst als auch ein Teil der Unterelemente importiert werden.

Es gibt verschiedene Symbole, welche die zu importierenden Elemente kennzeichnen.

☑ Das Element selbst und alle eventuell vorhandenen Unterelemente werden importiert
■ Das Element selbst und ein Teil seiner Unterelemente werden importiert
▣ Das Element wird nicht importiert, beinhaltet jedoch Elemente welche importiert werden

Innerhalb der Liste ist über die rechte Maustaste ein Kontextmenü einsehbar, welches hilfreiche Funktionen zur Selektion der einzelnen Elemente bereitstellt.

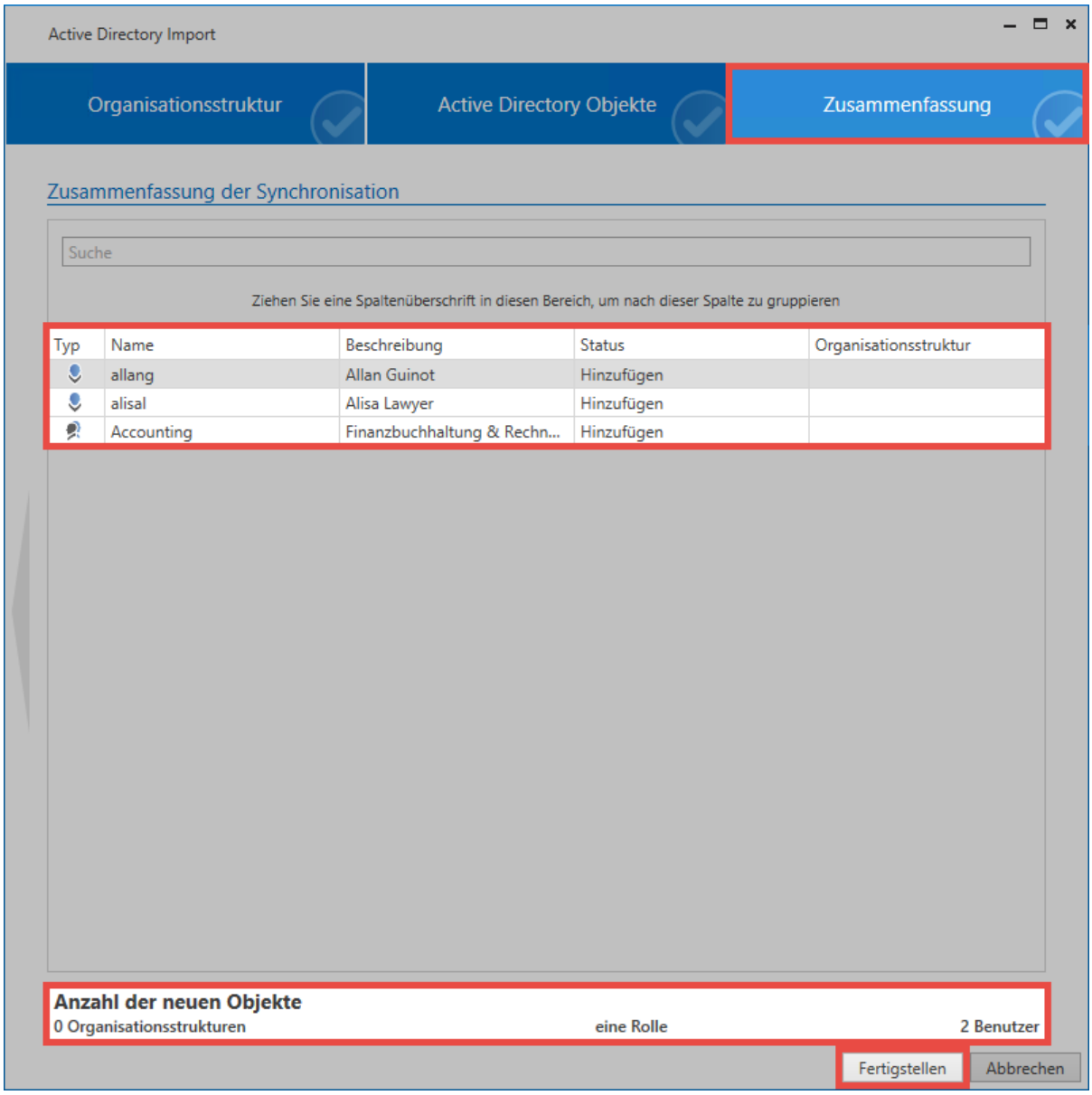



- **Unterobjekte selektieren** markiert alle Unterobjekte, welche **direkt** unter dem aktuellen Objekt liegen
- **Unterobjekte deselektieren** entfernt die Markierungen bei allen Unterobjekten, welche **direkt** unter dem aktuellen Objekt liegen
- **Alle Elemente zurücksetzen** entfernt alle bisher gesetzten Markierungen
- **Element Details anzeigen** listet alle Informationen auf, welche zum aktuellen Objekt verfügbar sind

> Lassen sich einzelne Benutzer, Organisationseinheiten oder Rollen nicht zum Import markieren, wurden diese bereits über ein anderes Profil importiert

### Zusammenfassung

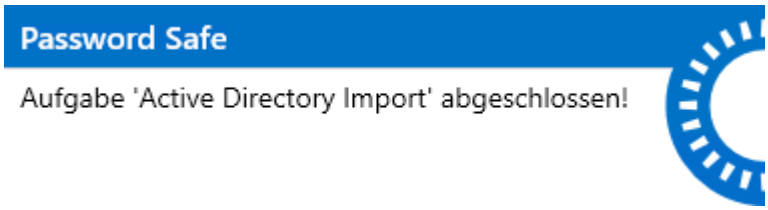
Die letzte Seite fasst zusammen, welche Objekte in welcher Form bearbeitet werden. Es sind sowohl die Namen als auch die Beschreibungen der Elemente zu sehen. In der Spalte **Status** wird dargestellt, ob das Objekt neu hinzugefügt, aktualisiert oder deaktiviert wird. In der letzten Spalte ist ersichtlich, in welche Organisationseinheit das Element importiert wird. Ganz unten wird die Anzahl der Objekte summiert.




Das Erstellen der Zusammenfassung kann – je nach Umfang – mehrere Minuten in Anspruch nehmen.

### Importvorgang

Der Import selbst wird im Hintergrund durch den Server durchgeführt. Die einzelnen Elemente tauchen also nach und nach in der Liste auf. Je nach Menge der importierenden Daten kann dies auch längere Zeit in Anspruch nehmen. Wurde der Import beendet, erhält man eine Rückmeldung.




Da in diesem Modus die Ende zu Ende Verschlüsselung beibehalten wird, bekommt der Server keinen Schlüssel um bereits importierte Benutzer mit dem AD abzugleichen. Eine Synchronisation mit dem AD findet also nicht statt. Ebenso können keine Mitgliedschaften importiert werden. Nach dem Import müssen die Benutzer zukünftig manuell den entsprechenden Organisationseinheiten und Rollen zugewiesen werden.

# Importierte Benutzer und Organisationseinheiten

Im Ende zu Ende Modus verhalten sich die importierten Benutzer wie lokale Benutzer. Die Benutzer können/müssen im Password Safe manuell bearbeitet werden. Die Zugehörigkeiten zu Organisationseinheiten und/oder Rollen müssen manuell angepasst werden.

### Anmeldung an Password Safe

Benutzer, welche in diesem Modus importiert werden, können sich **nicht** mit dem Domänenkennwort anmelden. Vielmehr wird Ihnen beim Import der Benutzername als Passwort hinterlegt. Dieses kann durch den Administrator oder den Benutzer selbst bei der ersten Anmeldung geändert werden.

# Master Key Modus

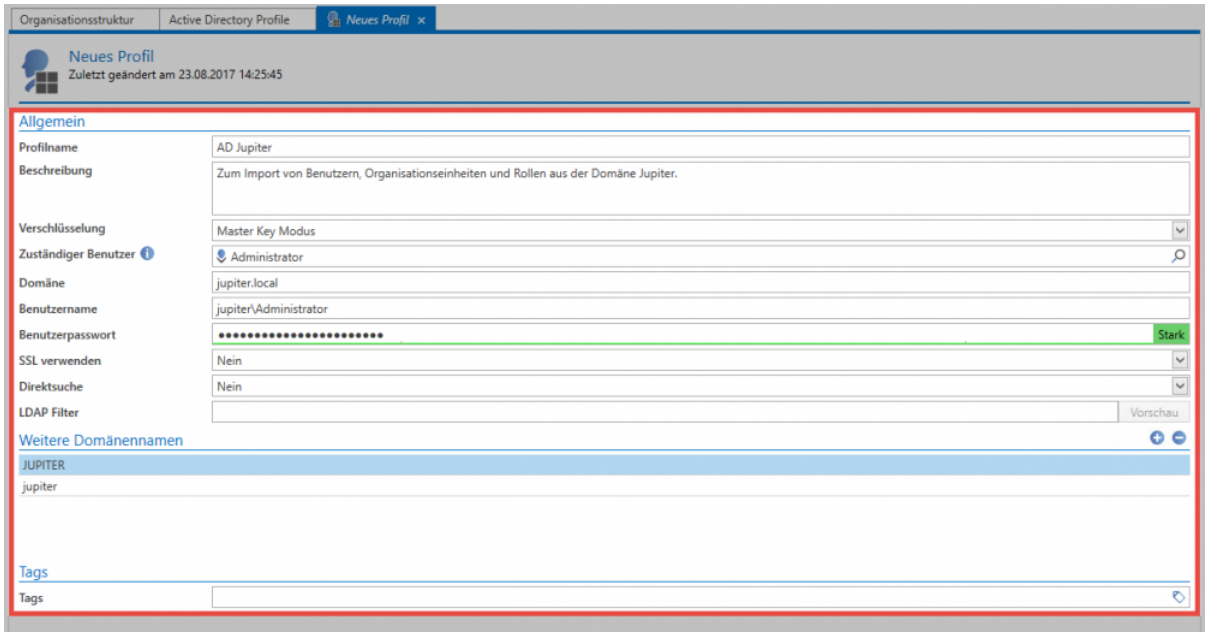
## Maximaler Komfort

Im Gegensatz zum Ende zu Ende Modus, welcher die Sicherheit an erste Stelle stellt, bietet der Master Key Modus maximalen Komfort. Es werden nicht nur Benutzer, Organisationseinheiten und Rollen, sondern auch deren Verknüpfungen, bzw. Zugehörigkeiten importiert. Eine Synchronisation zum Aktualisieren der Informationen und Zugehörigkeiten ist möglich. **Das Active Directory wird in diesem Szenario als führendes System verwendet**.

## Erstellen des Profils

> ! Es wird das Recht **Kann neue Active Directory Profile anlegen** sowie Sicht auf das **Modul Organisationseinheiten** oder auf das **Modul Rollen** benötigt

Die Profilverwaltung wird über das gleichnamige Icon in der Ribbon gestartet.




Im Profil müssen folgende Informationen angegeben werden:

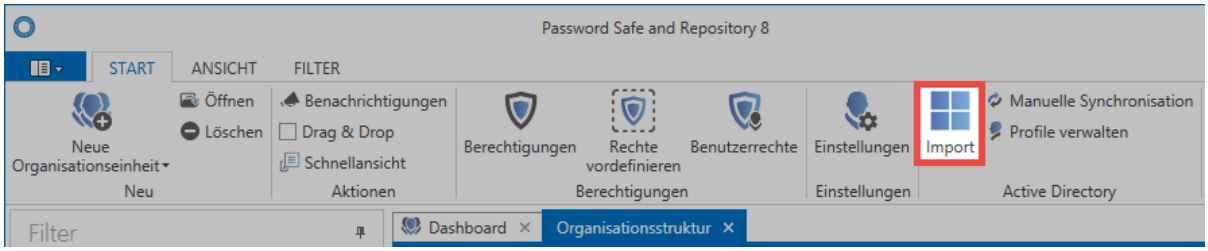
- **Profilname**
- Eine optionale **Beschreibung**
- Bei der **Verschlüsselung** wird der Master Key Modus ausgewählt

Bei bereits erstellten Profilen kann die Verschlüsselung nicht mehr geändert werden

- Unter **Domäne** wird angegeben, welche Domäne ausgelesen wird. Der hier hinterlegte Wert wird dann auch zur Authentifizierung verwendet,sofern unter **Weitere Domänennamen** keine alternativen Schreibweisen hinterlegt sind.
- Es muss ein lokaler **Benutzer** (beispielsweise der Administrator) oder ein bereits importierter User angegeben werden. In dessen Namen findet der Import statt.
- Zum Zugriff auf das AD ist ein **Benutzer** nötig. Dieser wird im Format Domäne\Benutzer angegeben. Es ist zwingend nötig, dass er Zugriff auf das AD hat.
- zugehöriges **Benutzerpasswort** (Domänenkennwort) des Benutzers
- Falls das AD dies verlangt, kann die Verbindung über **SSL** aufgebaut werden
- Die **Direktsuche** ist bei sehr großen Strukturen zu empfehlen. Die Baumstruktur entfällt, Elemente können dann nur noch über die Suche gefunden und selektiert werden.
- Mit dem **Filter** kann über eine LDAP-Query direkt ein AD-Pfad als Einstiegspunkt angeben werden.
- Unter **Weitere Domänennamen** können alternative Schreibweisen der Anmeldedomäne hinterlegt werden. Diese müssen dann der Schreibweise im Loginfenster entsprechen. Wird die Domäne beispielsweise mit **jupiter.local** oder einer IP Adresse angesprochen, so kann die Anmeldung nur dann mit **jupiter\benutzer** erfolgen, wenn **jupiter** hier hinterlegt ist.

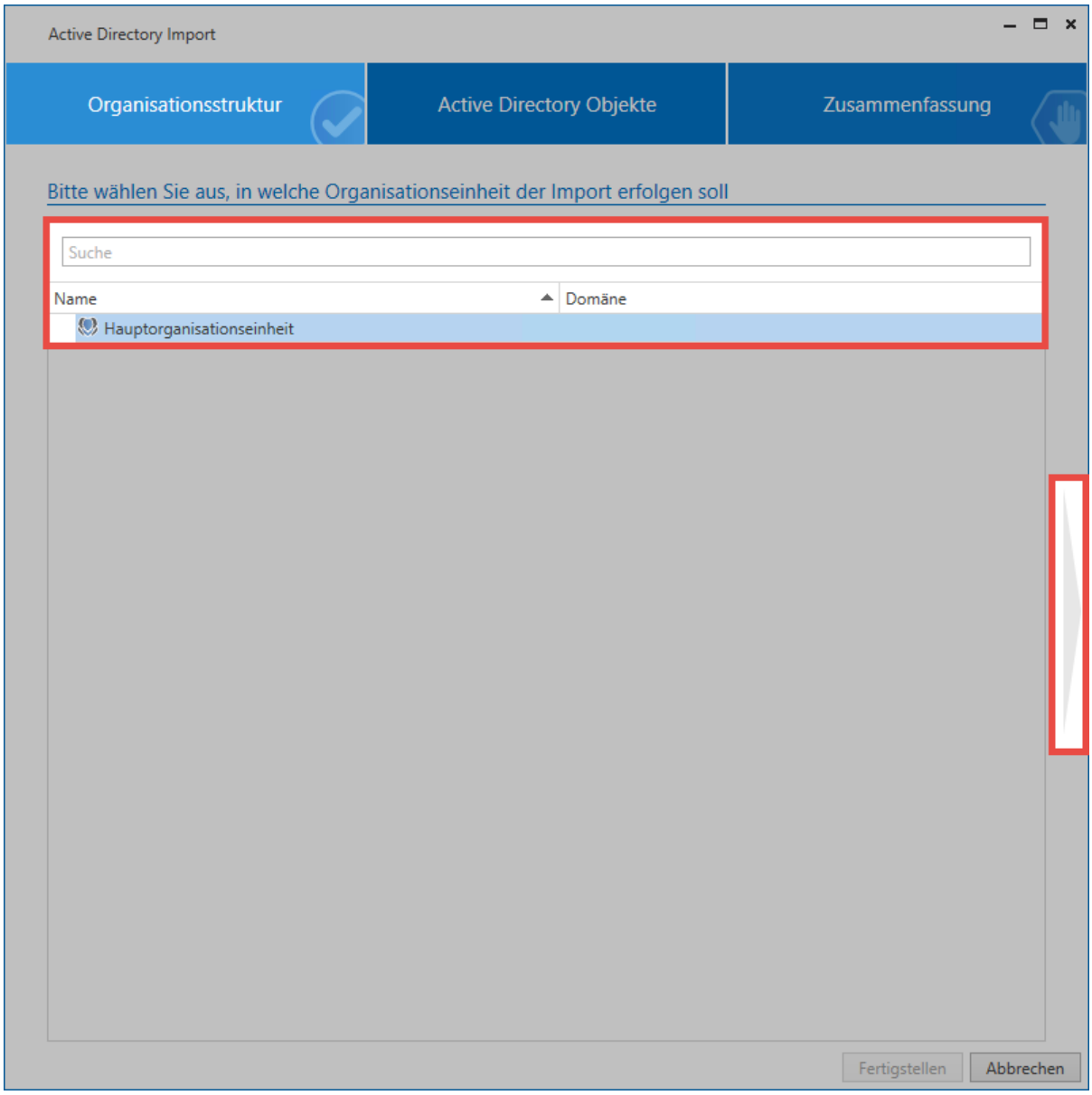
# Import

Der Import kann direkt in der Ribbon gestartet werden. Ein Assistent führt durch den kompletten Vorgang.



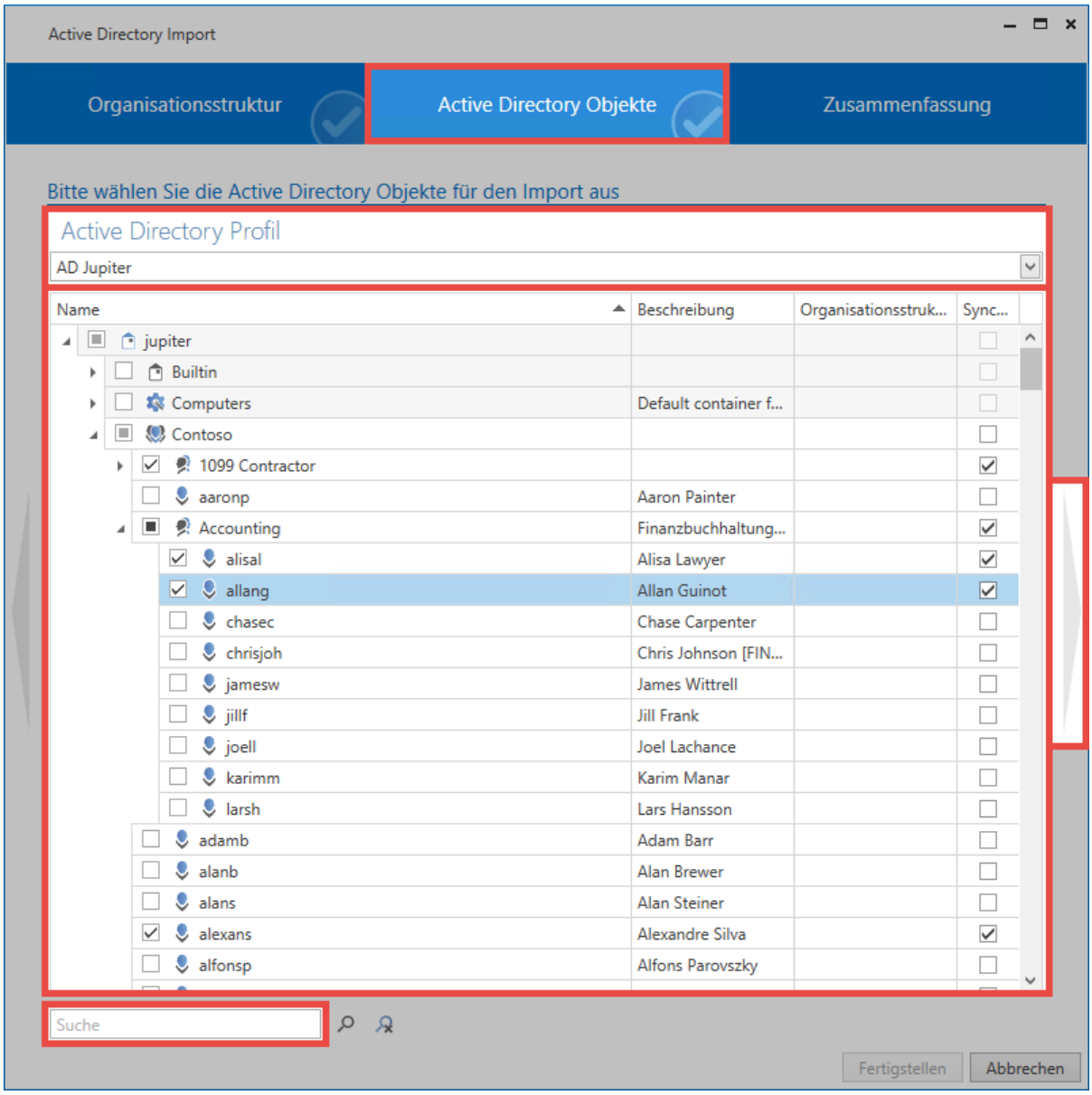

### Organisationsstruktur

Zunächst wird gewählt, in welche Organisationseinheit der Import erfolgen soll. Existieren – wie in diesem Beispiel – noch keine Organisationseinheiten in der Datenbank, erfolgt der Import in die **Hauptorganisationseinheit**.




## Active Directory Objekte

Im nächsten Schritt erfolgt zunächst die Auswahl des Profils, mit welchem importiert werden soll. Anschließend wählt man Organisationseinheiten und/oder Benutzer zum Import aus. Hierfür steht eine Suche bereit.




Hier ist zu sehen, dass die Organisationseinheiten **Jupiter** und **Contoso** Elemente beinhalten, welche importiert werden. Die Organisationseinheiten selbst werden nicht importiert. Die Gruppe **1099 Contractor** wird inklusive aller Unterelemente importiert. Die Markierung der Gruppe **Accounting** zeigt an, dass sowohl die Gruppe selbst als auch ein Teil der Unterelemente importiert werden. Die Haken in der letzten Spalte sorgen dafür, dass die Elemente bei zukünftigen Synchronisationsläufen beachtet werden.

Es gibt verschiedene Symbole, welche die zu importierenden Elemente kennzeichnen.

☑ Das Element selbst und alle eventuell vorhandenen Unterelemente werden importiert
■ Das Element selbst und ein Teil seiner Unterelemente werden importiert
▣ Das Element wird nicht importiert, beinhaltet jedoch Elemente welche importiert werden

Über einen Rechtsklick in die Liste erhält man ein Kontextmenü, welches hilfreiche Funktionen zur Selektion der einzelnen Elemente bereitstellt.


Es gibt verschiedene Symbole welche darstellen welche Elemente importiert werden.

☑ Das Element selbst und alle eventuell vorhandenen Unterelemente werden importiert
■ Das Element selbst und ein Teil seiner Unterelemente werden importiert
▣ Das Element wird nicht importiert, beinhaltet jedoch Elemente welche importiert werden

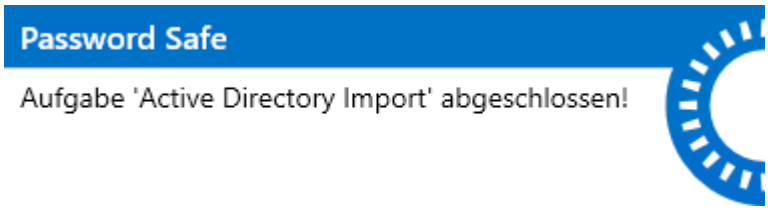
> Lassen sich einzelne Benutzer nicht zum Import markieren, so wurden Sie bereits über ein Ende zu Ende verschlüsseltes Profil importiert.

### Zusammenfassung

Die letzte Seite fasst zusammen, welche Objekte in welcher Form bearbeitet werden. Es sind sowohl die Namen als auch die Beschreibungen der Elemente zu sehen. In der Spalte **Status** wird dargestellt, ob das Objekt neu hinzugefügt, aktualisiert oder deaktiviert wird. In der letzten Spalte ist ersichtlich, in welche Organisationseinheit das Element importiert wird. Ganz unten ist die Anzahl der Objekte zu sehen.

### Importvorgang

Der Import wird im Hintergrund durch den Server durchgeführt. Die einzelnen Elemente tauchen also nach und nach in der Liste auf. Je nach Menge der importierenden Daten kann dies auch längere Zeit in Anspruch nehmen. Wurde der Import beendet, wird dies über einen Hint symbolisiert.




## Importierte Benutzer und Organisationseinheiten

Die im Master Key Modus importierten Benutzer und Organisationseinheiten können im Password Safe nicht bearbeitet werden. Etwaige Änderungen müssen also im AD vorgenommen und synchronisiert

werden. **Somit wird das AD zum führenden System**. Zugehörigkeiten in Organisationseinheiten oder Rollen werden ebenfalls synchronisiert und müssen im AD gesetzt werden. In Organisationseinheiten oder Rollen, welche in Password Safe erzeugt wurden, können die User direkt in Password Safe aufgenommen werden.

### Anmeldung an Password Safe

Benutzer, welche in diesem Modus importiert werden, können sich mit dem Domänenkennwort anmelden. Es gilt zu beachten, dass bei der Anmeldung keine Domäne angegeben werden muss. Selbstverständlich kann die Anmeldung zusätzlich durch die Multifaktor-Authentifizierung ergänzt werden.

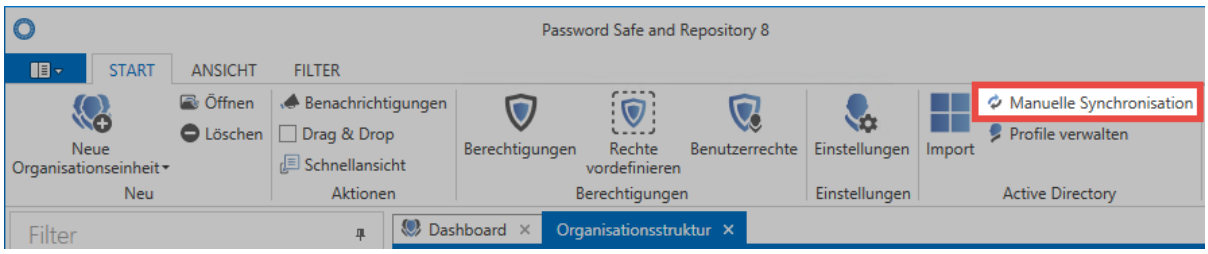
# Synchronisation

Bei einer Synchronisation werden alle relevanten Informationen der Benutzer, Organisationseinheiten und Rollen (Namen, E-Mail, usw.) aktualisiert. Geänderte Zugehörigkeiten zu Organisationseinheiten und Rollen werden angepasst. Ebenso werden Benutzer – entsprechend den Einstellungen im AD – aktiviert bzw. deaktiviert. Neue Benutzer und entsprechend definierten Rollen werden importiert.

> Wurde beim Import eines Benutzers der Haken in der Spalte **Synchronisation** nicht gesetzt, finden keine Änderungen statt.

### Manuelle Synchronisation

Über die entsprechende Schaltfläche in der Ribbon kann die Synchronisation jederzeit manuell gestartet werden.




Anschließend wird das gewünschte Profil gewählt und die Synchronisation schlussendlich gestartet. Wie auch der initiale Import, läuft die Synchronisation im Hintergrund. Der Abschluss wird ebenfalls durch einen “Hint” angezeigt.

### Synchronisation über System Tasks

Ebenso kann die Synchronisation automatisiert durchgeführt werden. Dies wird im Zuge der System Tasks ermöglicht.

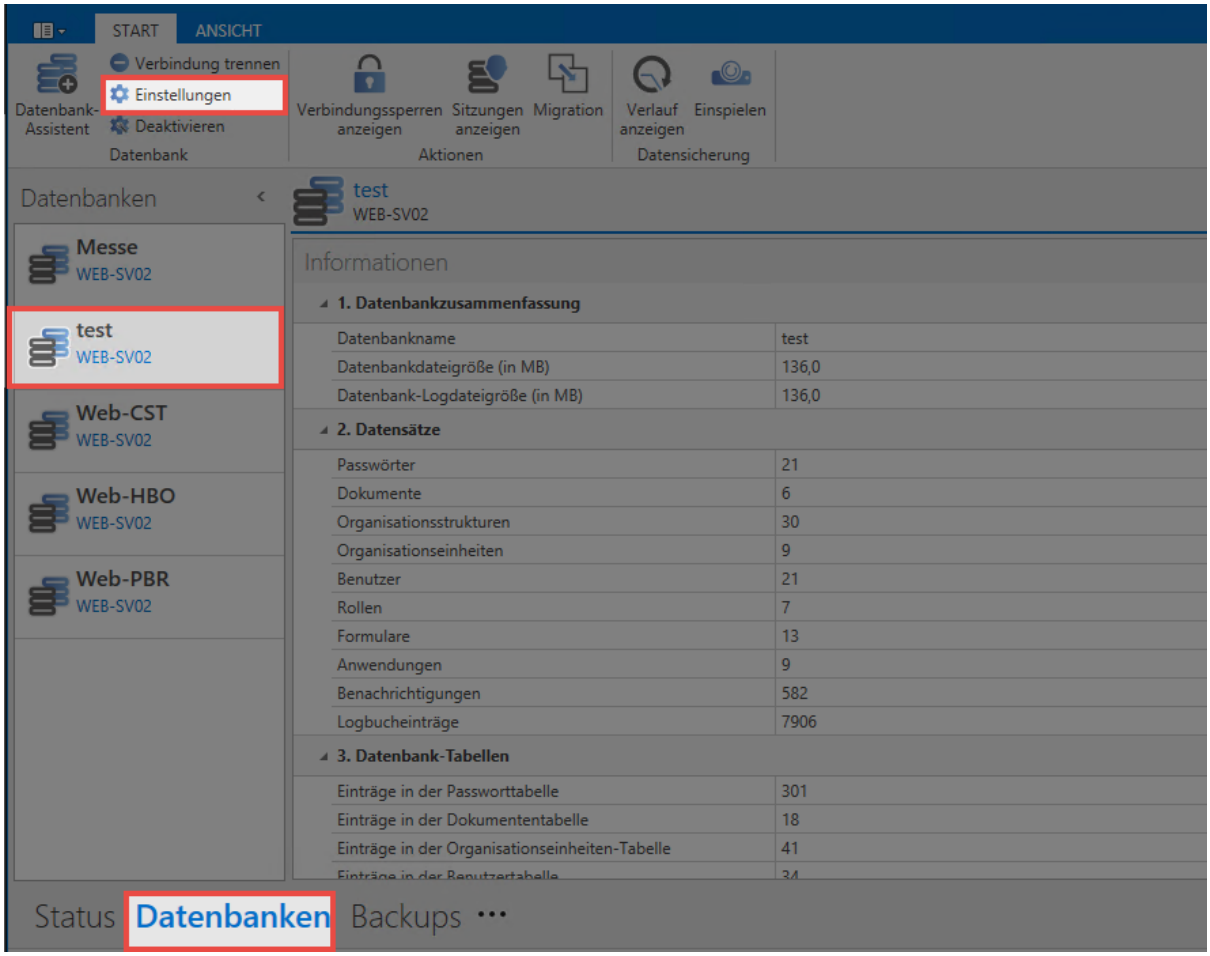
# Multifaktor-Authentifizierung

## Was ist Multifaktor-Authentifizierung?

Über die Multifaktor-Authentifizierung kann die Anmeldung – zusätzlich zum Passwort – mit einem weiteren Faktor abgesichert werden. Das Einrichten einer Multifaktor-Authentifizierung kann entweder durch den Administrator oder den Benutzer erfolgen.

## Voraussetzungen

Damit Multi Faktor Authentifizierung auf einer Datenbank genutzt werden kann, muss dies am Admin Client zuvor aktiviert werden. Im Modul Datenbanken öffnet man hierfür über die Ribbon die Einstellungen der markierten Datenbank.



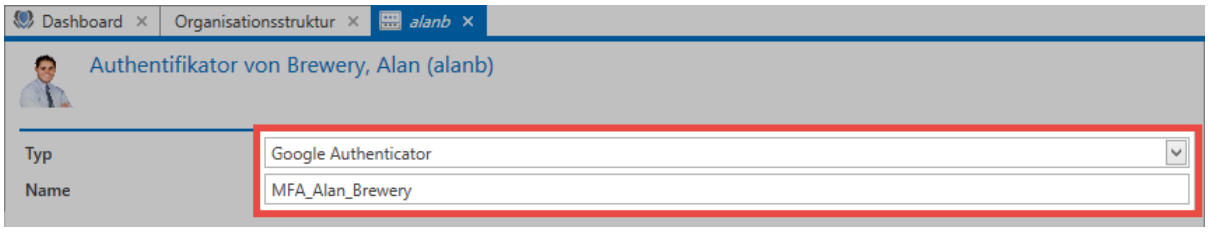

Innerhalb der Einstellungen kann dann für jede Schnittstelle separat definiert werden, ob diese auf der Datenbank benutzt werden darf.


### weitere Einstellungen

In den Benutzereinstellungen kann darüber hinaus noch die “Gültigkeitsdauer eines Multi Faktor Authentifizierungstokens in Minuten definier werden.

# Konfiguration von Multi Faktor Authentifizierung

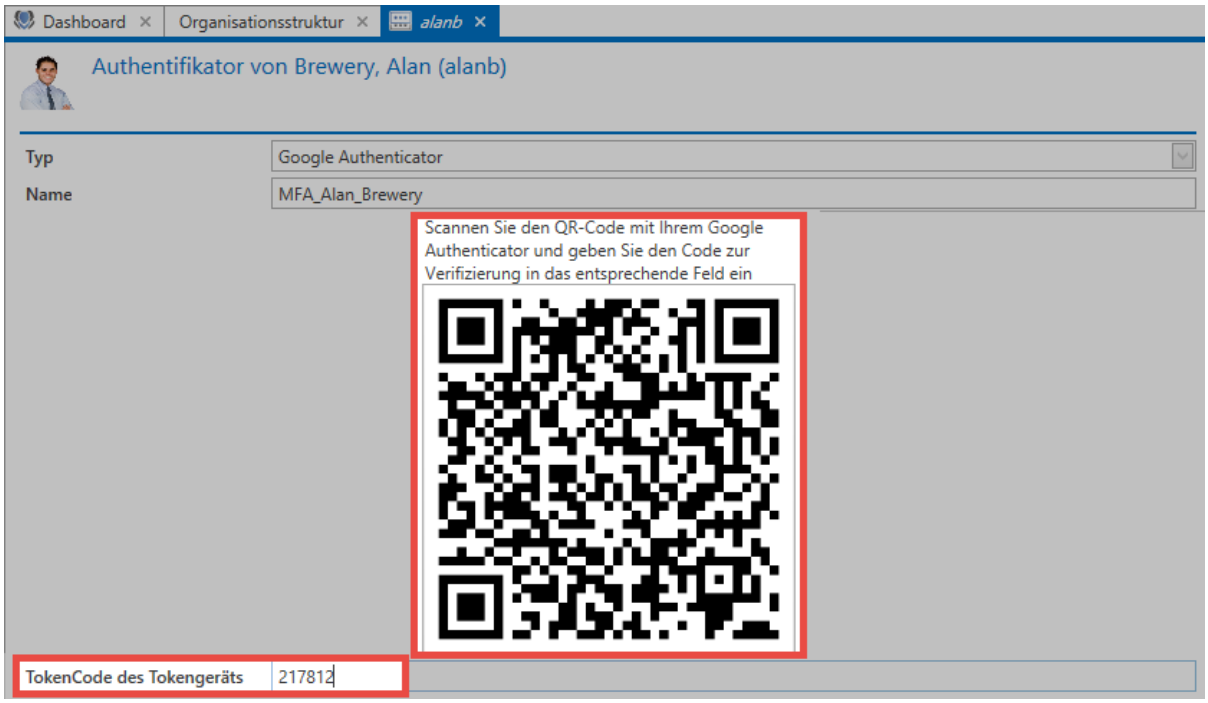
Hierfür selektiert man im Modul Organisationsstruktur den Benutzer und wählt die Schaltfläche “Multifaktor-Authentifizierung” in der Ribbon.




Es wird die gewünschte Art der Authentifizierung ausgewählt und betitelt. Dieser Name wird auch beim Login dem Benutzer angezeigt. Je nach gewünschtem Authentifizierungstyp unterscheidet sich das weitere Vorgehen.

# Google Authenticator

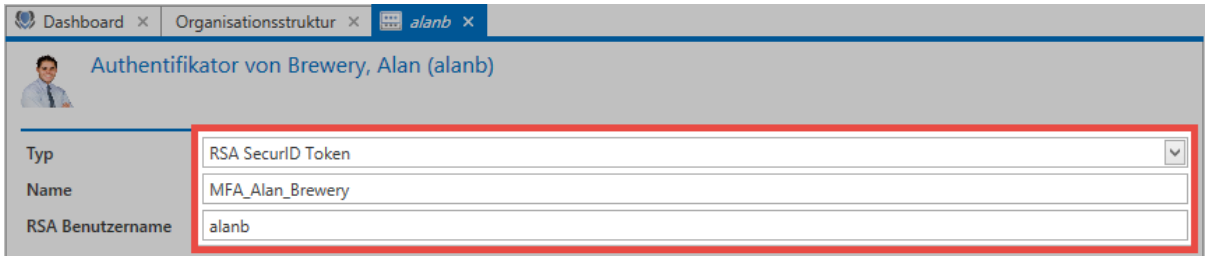
Voraussetzung hierfür ist, dass die entsprechende App auf einem Smartphone gestartet ist. Nachdem der Name für die Authentifizierung vergeben wurde, generiert man über den entsprechenden Button ein neues “Secret”. Es wird ein QR-Code angezeigt, welcher mit der Google Authenticator App des Smartphones gescannt werden muss.




Sobald die Google Authenticator App den QR-Code erkannt hat, gibt Sie eine 6-stellige PIN zurück. Diese wird dann im entsprechenden Feld eingetragen. Abschließend klickt man in der Ribbon auf **Anlegen**.

# RSA SecurID Token

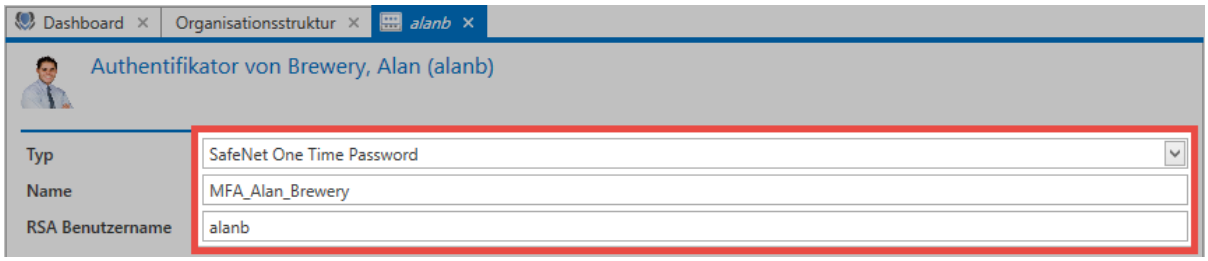
Zum Einrichten der Multifaktor-Authentifizierung mittels RSA SecurID gibt man einfach den RSA Benutzernamen an und klickt direkt in der Ribbon auf **Anlegen**.




Voraussetzung für die Verwendung von RSA SecurID Token ist, dass am Admin Client in Datenbank Einstellungen die Zugangsdaten hinterlegt wurden.

# SafeNet One-Time-Password

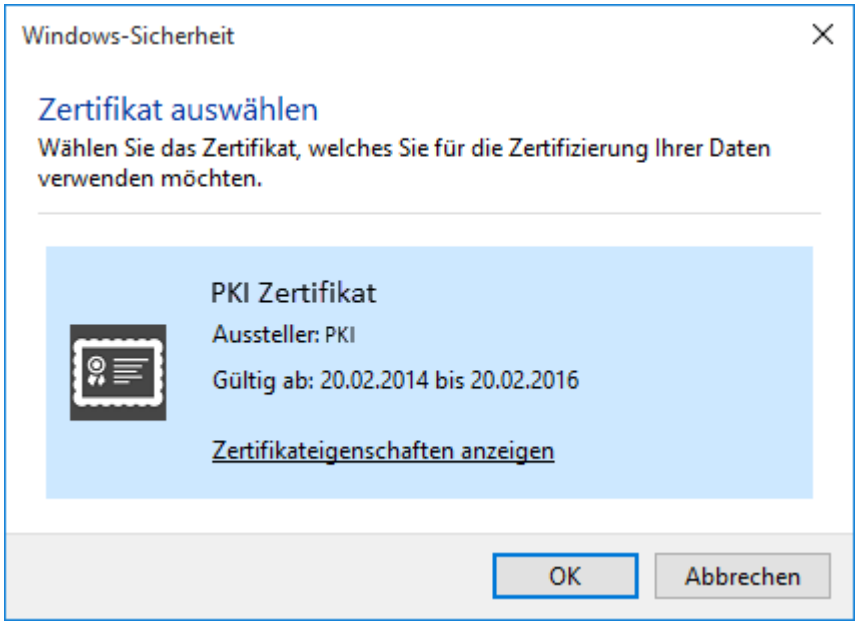
Die Multifaktor-Authentifizierung mittels SafeNet One-Time-Password wird mit dem SafeNet Benutzernamen eingerichtet.




Voraussetzung für die Verwendung von SafeNet One-Time-Password Token ist, dass am Admin Client in Datenbank Einstellungen die Zugangsdaten hinterlegt wurden.

# Public-Key-Infrastruktur

Für die Einrichtung mittels PKI öffnet man über den Button **Auswählen** zunächst das Menü zur Wahl des gewünschten Zertifikats. Es werden alle in Frage kommenden Zertifikate angezeigt.




Nun selektiert man einfach das gewünschte Zertifikat aus bestätigt den Vorgang.

# Yubico One Time Password

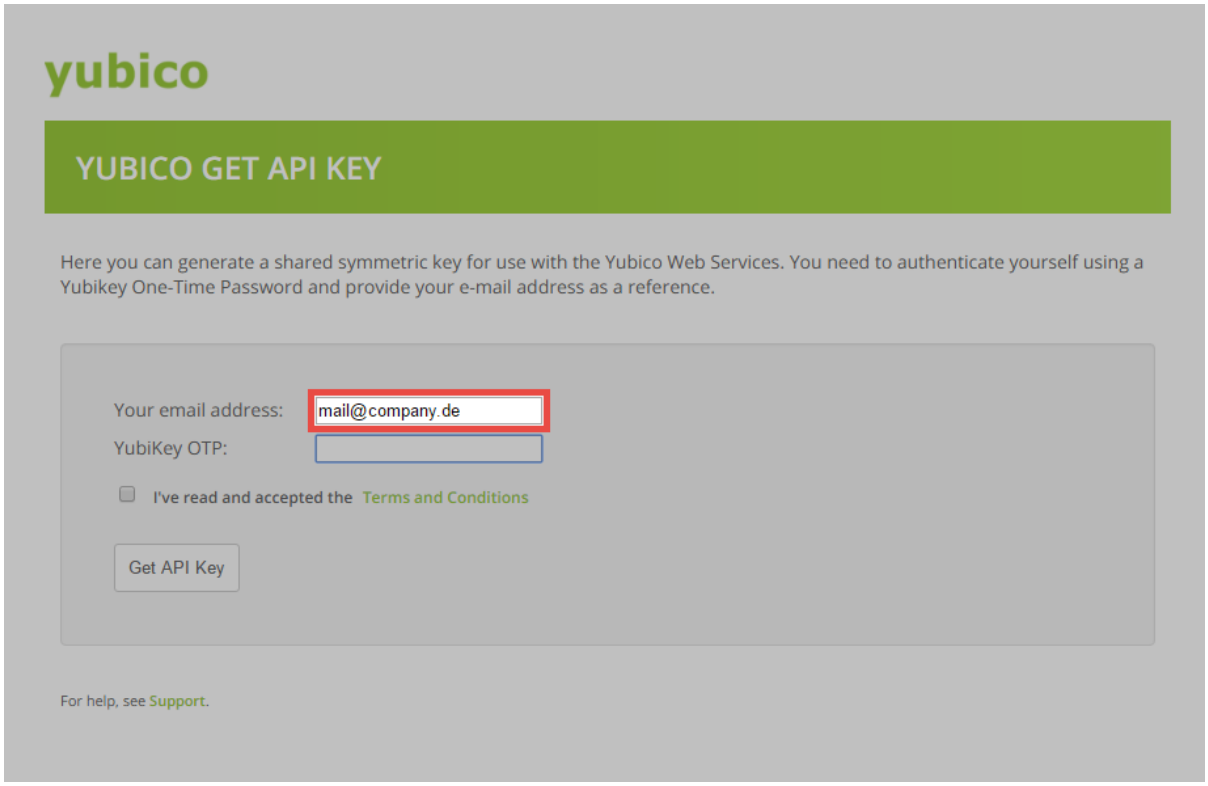
Die Konfiguration der Multifaktor-Authentifizierung mittels Yubico One Time Password wird in einem gesonderten Kapitel beschrieben.

# Yubico / Yubikey

## Einrichtung der Multifaktor-Authentifizierung

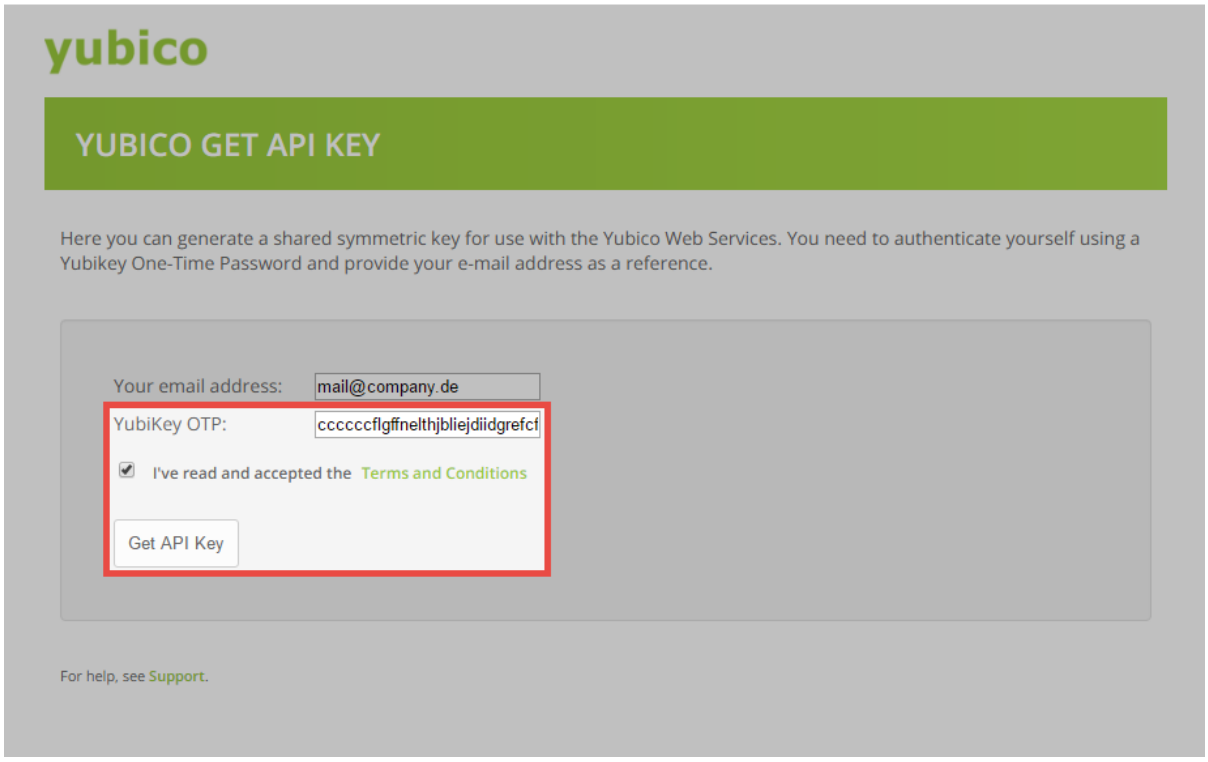
### Anfordern des Yubico API Keys

Zur Konfiguration muss ein API Key angefordert werden. Hierzu wird der folgende Link aufgerufen und eine E-Mailadresse angegeben: https://upgrade.yubico.com/getapikey/

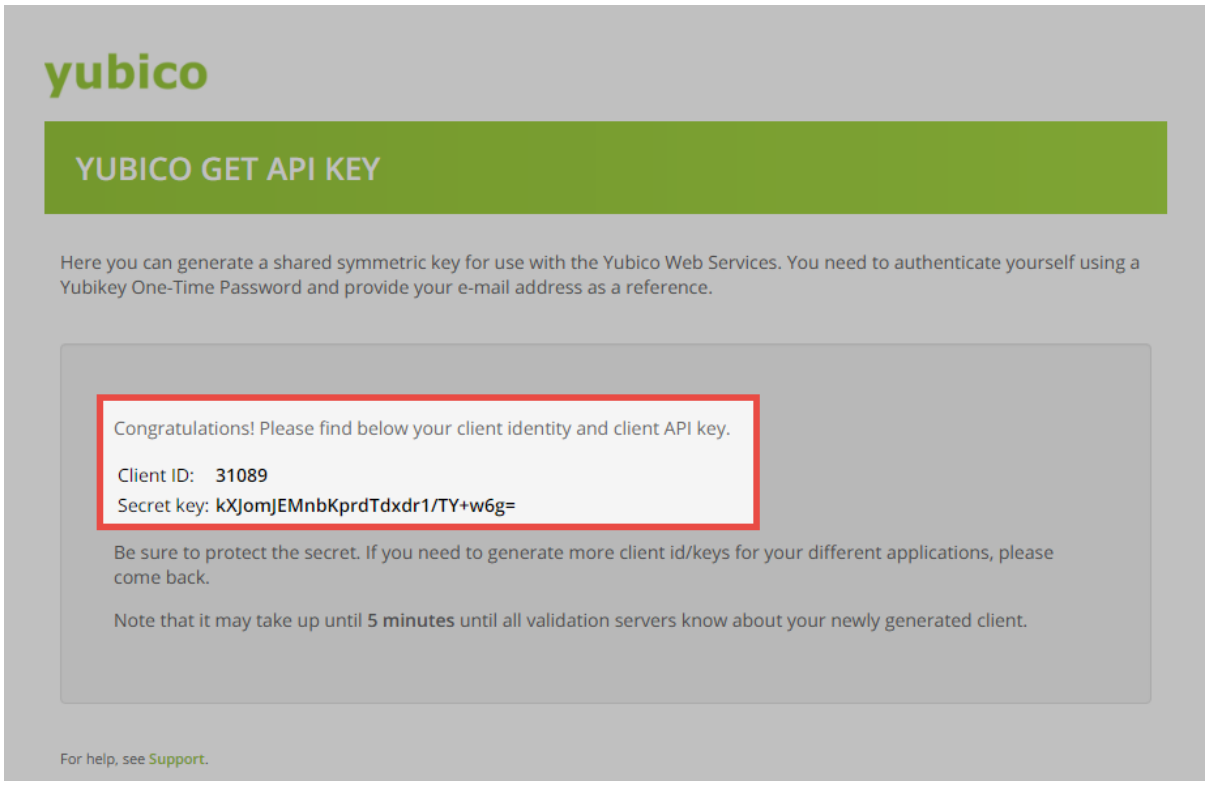



Anschließend wird über den Yubikey ein **One Time Password** erzeugt. Der verwendete Yubikey muss hierfür lediglich an der richtigen Stelle berührt werden.

Das **One Time Password** wird direkt in das entsprechende Feld geschrieben.

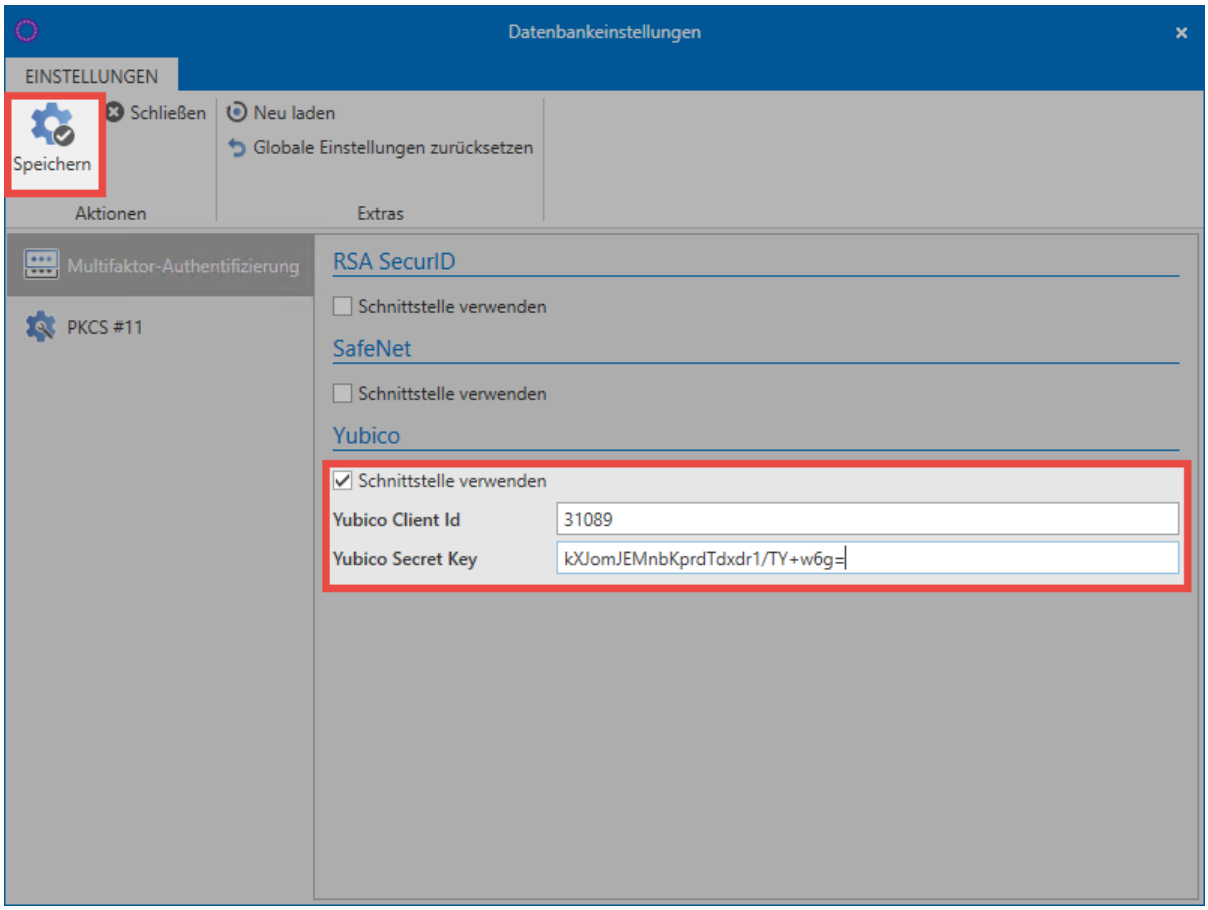



Nachdem den allgemeinen Geschäftsbedingungen zugestimmt wurde, kann der API Key angefordert werden.




### Konfiguration der Yubikey API

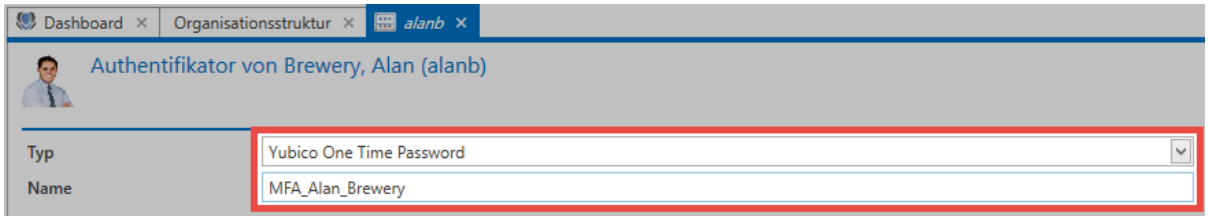
Die eigentliche Einrichtung der Multifaktor-Authentifizierung erfolgt am Admin Client im Modul **Datenbanken**. Zunächst wird die gewünschte Datenbank selektiert und dann in der Ribbon die **Eigenschaften** aufgerufen.
Anschließend müssen die **Yubico Client ID** sowie der **Yubico Secret Key** eingetragen und gespeichert werden.




Die Schnittstelle ist nun fertig eingerichtet und kann verwendet werden.

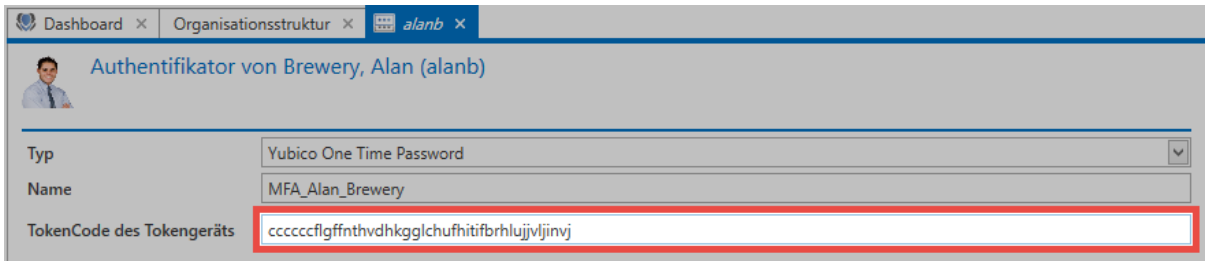
# Konfiguration der Multifaktor-Authentifizierung für Benutzer

Die Konfiguration der Multifaktor-Authentifizierung findet am Password Safe Client statt. Sie kann durch den Benutzer selbst im Backstage unter Konto erfolgen. Ebenso ist es möglich, dass die Konfiguration für andere Benutzer im Modul Organisationsstrukturen geschieht. Der Ablauf ist in beiden Fällen identisch. Um den Yubikey zu konfigurieren, wird einfach **Yubico One Time Password** gewählt sowie der Multifaktor-Authentifizierung ein Name gegeben.



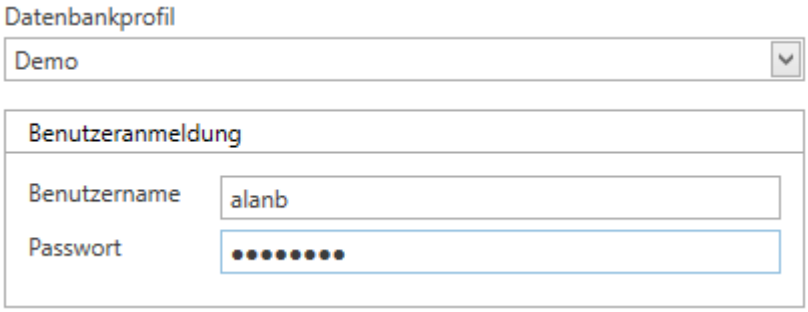

Klicken Sie nun auf speichern. Nun wird in das Feld für den Token geklickt und über den Yubikey ein Token erzeugt. Beim **Yubikey NEO** genügt hierfür das Berühren des Touchfelds. Beim **Yubikey Nano** muss ebenfalls lediglich “berührt” werden.

Der Token wird direkt in das entsprechende Feld eingetragen. Nach dem Speichern ist die Multifaktor-Authentifizierung fertig konfiguriert.



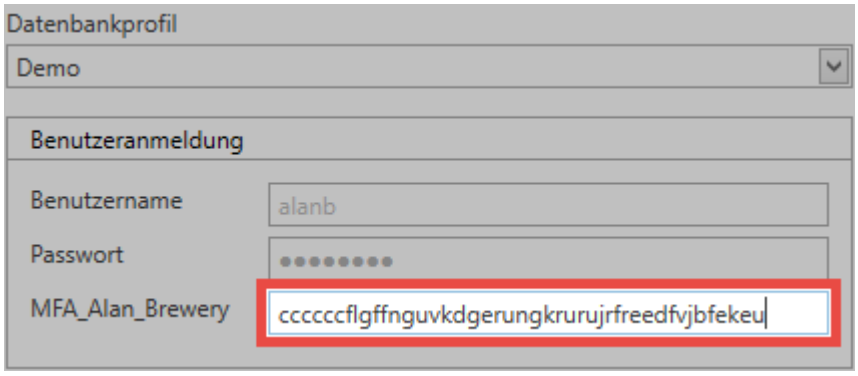

# Anmeldung mit dem Yubikey

Zur Anmeldung mit Multifaktor Authentifizierung wird zunächst die Datenbank ausgewählt und anschließend **Benutzername** und das **Passwort** eingegeben und bestätigt.




Nach der ersten Authentifizierung mittels Passwort wird ein weiteres Feld für das **One Time Password** eingeblendet.


Nachdem das Feld durch einen einfachen Klick den Fokus erhalten hat, wird durch das Berühren des Yubikeys das **One Time Password** eingetragen.

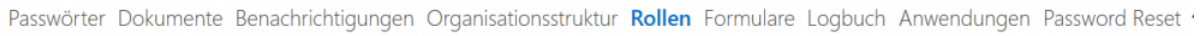



Der Benutzer wird nun angemeldet.

# Rollen

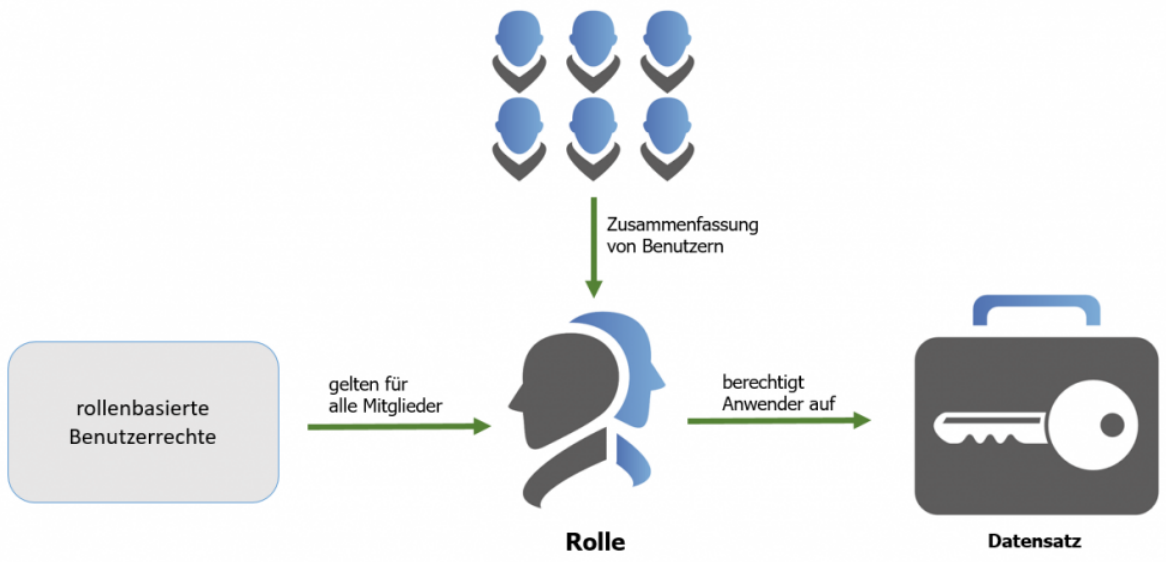
## Was sind Rollen?

Jeder Mitarbeiter in einem Unternehmen ist letztendlich Mitglied einer Abteilung und/oder Teil einer bestimmten Funktionsebene. Diese Abteilungen oder Gruppierungen werden innerhalb von Password Safe durch das Rollenkonzept abgebildet. Die Berechtigungen können somit rollenbasiert konfiguriert und vererbt werden. Das Modul „Rollen“ sollte nur administrativ tätigen Benutzern zur Verfügung gestellt werden. Es bietet sich demnach an die Sichtbarkeit der Rollenverwaltung stark einzuschränken. Über das Rollenkonzept ist es ebenso möglich, die Verwaltung von Abteilungen oder separaten Bereichen komplett an Dritte zu delegieren. Das Berechtigungskonzept gewährleistet, dass Benutzern lediglich Zugriff auf diejenigen Rollen gewährt wird, auf welche diese auch berechtigt sind. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert.




## Rollen im Fokus

Die Konfiguration von Rollen ist die Basis für das Berechtigungskonzept. Natürlich wäre die Berechtigung auf Daten auch auf Benutzerebene möglich. Durch die Nutzung von Rollenzugehörigkeiten lässt sich jedoch der administrative Aufwand drastisch reduzieren und die Übersicht wahren. Zusätzlich zu den Berechtigungen auf Daten werden ebenso Benutzerrechte im günstigsten Fall über Rollen abgebildet.

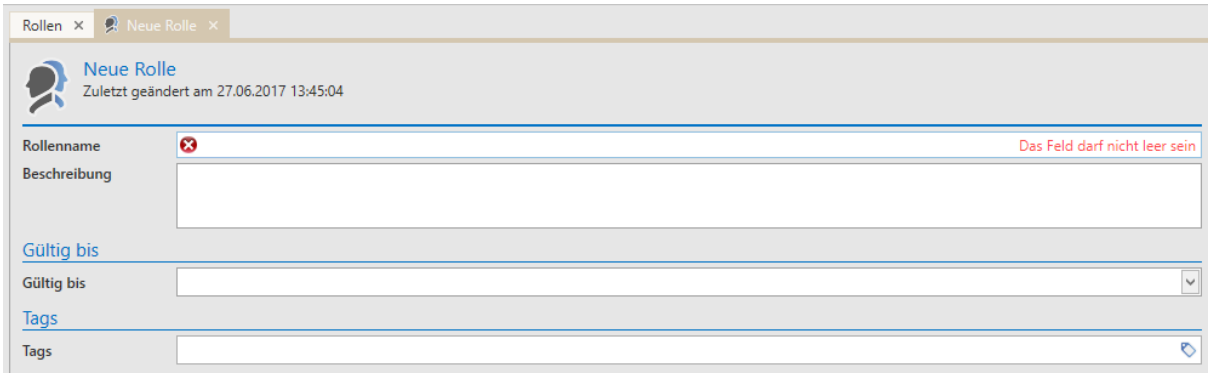


Wie man sieht sind Rollen die zentralen Objekte innerhalb des Password Safe. Sie bilden die unverzichtbare Brücke zwischen Benutzern und Berechtigungen jedweder Art.

# Erstellung und Berechtigen neuer Rollen

> ! Es wird das Recht **Kann neue Rollen anlegen** sowie Sicht auf das **Modul Rollen** benötigt

Befindet man sich im Modul “Rollen”, entspricht das Erstellen neuer Rollen funktionell dem Erstellen neuer Datensätze. Sowohl über die Ribbon als auch über das Kontextmenü der rechten Maustaste können Rollen angelegt werden.




Alle mit Rollen und dem Berechtigungskonzept in Verbindung stehenden Informationen werden in einem eigenen Kapitel erläutert.

# Konzeptphase

Analog zur Handhabung der Organisationsstrukturen, sollte man sich auch im Vorfeld mit den angedachten Rollenkonzepten genauestens beschäftigen. Das Abbilden der in einem Unternehmen vorhandenen Strukturen stellt die Weichen für den Erfolg des Password Safe. Erst nachdem ein detaillierter Entwurf erstellt wurde, und sämtliche von allen Projektbeteiligten gewünschten Anforderungen erfüllt sind, sollte man sich mit der Gestaltung der Rollen in Password Safe beschäftigen.

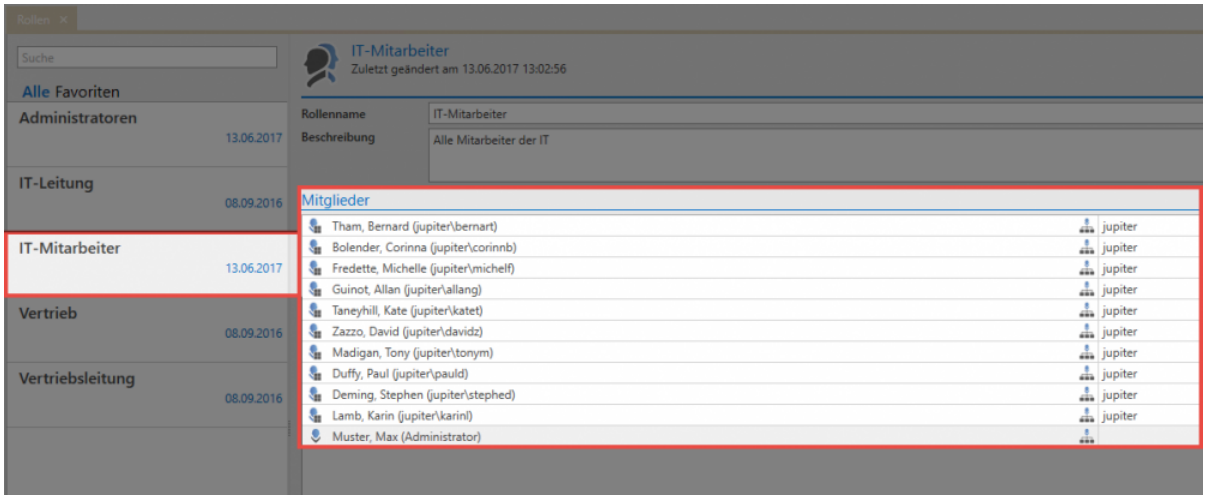
# Warum gibt es keine Gruppen?

Password Safe erzwingt durch das Rollenkonzept die Vermeidung unnötiger Strukturen. Eine Gruppe-in-Gruppen Verschachtelung wird nicht unterstützt – und ist gar nicht nötig. Die sich dadurch ergebende Performanzsteigerung sowie gesteigerte Übersicht fördert Effizienz und Effektivität. Durch das elegante Zusammenspiel von Organisationsstrukturen, Rollen und granularen Filtermöglichkeiten können sämtliche kundenspezifischen Szenarien abgedeckt werden.

Die Verschachtelung von Rollen ist architekturbedingt nicht nötig!

# Übersicht auf Rollenmitglieder

Zusätzlich zur Ansicht im Berechtigungsdialog ist auch schon im Lesebereich eine Auflistung aller **Mitglieder** einer Rolle vorhanden. Alle des Weiteren Berechtigten ohne die Rollenmitgliedschaft werden nicht berücksichtigt.



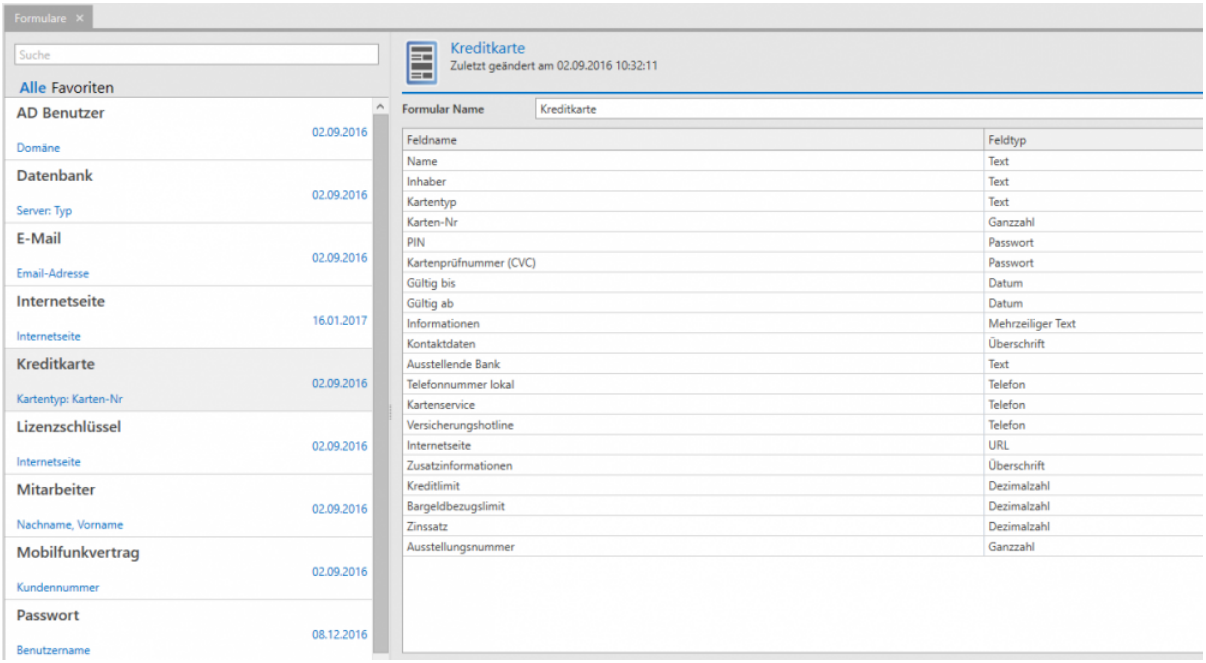
# Formulare

## Was sind Formulare?

Es ist bei der Erstellung eines neuen Datensatzes unabdingbar, stets alle für den angedachten Anwendungsfall relevanten Daten abzufragen. **Formulare** stellen in diesem Zusammenhang die **Schablonen der zu speichernden Informationen** dar. Die Administrierbarkeit der existierenden Formulare stellt in erster Linie die Vollständigkeit der zu speichernden Daten sicher. Dennoch ist auch deren Nutzen als effektives Filterkriterium nicht zu verachten! Formulare prägen das Arbeiten mit dem Password Safe v8 nachhaltig und müssen demzufolge durch die Administration mit der nötigen Sorgfalt verwaltet und gepflegt werden. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Module an zentraler Stelle erläutert.


## Standardformulare

Password Safe wird mit einer Reihe von Standardformularen ausgeliefert – diese sollten in der Regel alle gängigen Anforderungen abdecken. Das Anpassen der Standardformulare an individuelle Anforderungen ist natürlich dennoch möglich.

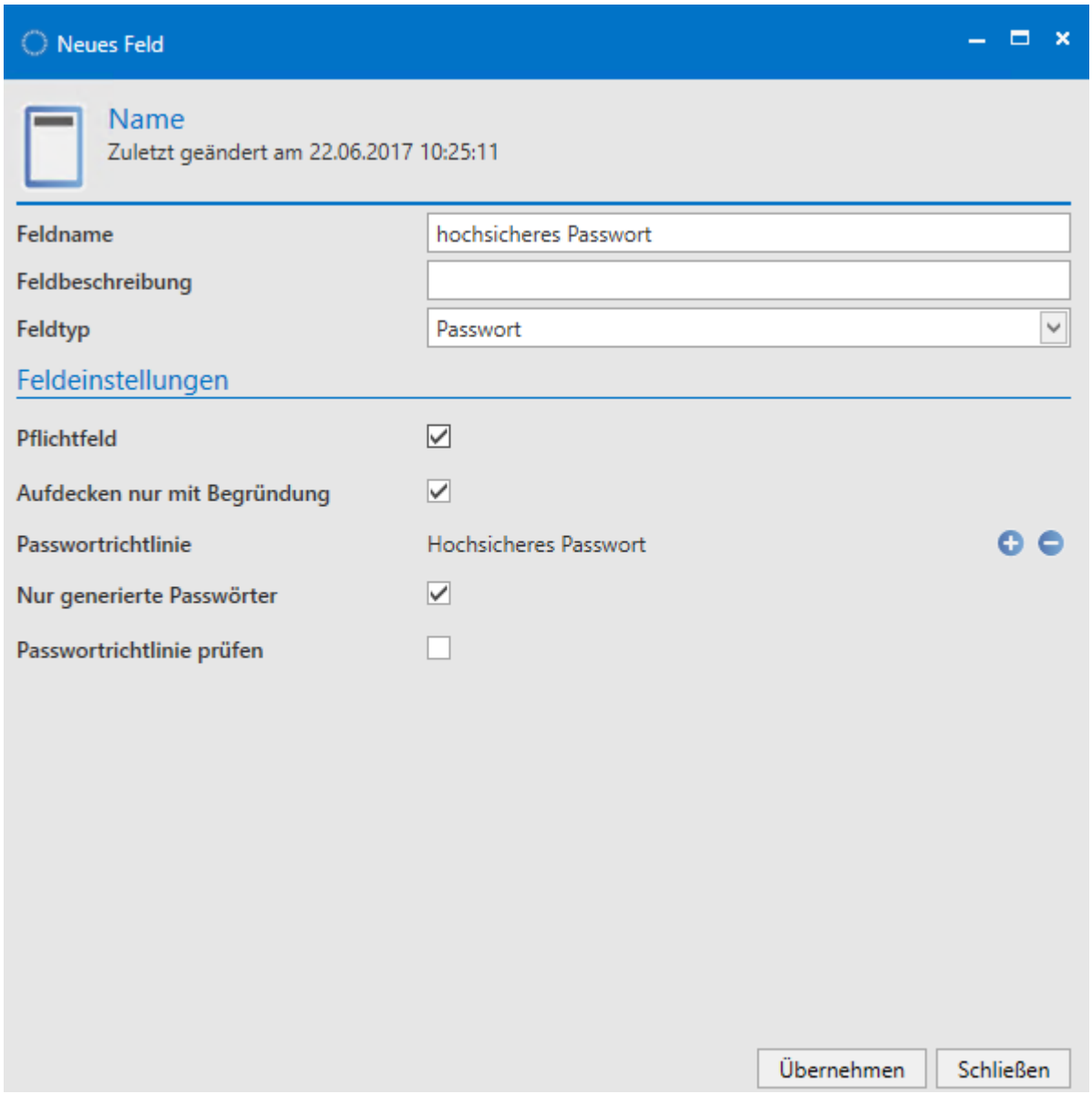



Zu dem in der Listenansicht ausgewählten Formular erscheint im Lesebereich die zugehörige Vorschau. Sowohl Feldname als auch Feldtyp sind einsehbar.

# Erstellen neuer Formulare

> ! Es wird das Recht **Kann neue Formulare anlegen** sowie Sicht auf das **Modul Formulare** benötigt

Sowohl über die Ribbon, den Shortcut “Strg + N* als auch über das Kontextmenü der rechten Maustaste kann man den Assistenten zum Erstellen neuer Formulare starten. Innerhalb des Assistenten können über die gleichen Mechanismen nun neue Formularfelder angelegt werden. Je nach ausgewähltem Feldtyp ergeben sich für den Bereich **Feldeinstellungen** andere Optionen. Nachfolgend wird dies am Beispiel für den Feldtyp “Passwort” deutlich. Die Reihenfolge, in der beim Anlegen neuer Datensätze Formularfelder abgefragt werden, entspricht der Reihenfolge innerhalb des Formulars. Über die zugehörigen Buttons in der Ribbon kann diese angepasst werden.



Für den Feldtyp “Passwort” ergeben sich demnach die “Feldeinstellungen Pflichtfeld, Aufdecken nur mit Begründung, nur generierte Passwörter und Passwortrichtlinie prüfen”. Diese können nun nach Belieben definiert werden. (**Anmerkung:** Die Auswahl von Passwortrichtlinien ist innerhalb der Feldeinstellungen möglich, deren Definition ist Teil der Optionen im Hauptmenü)

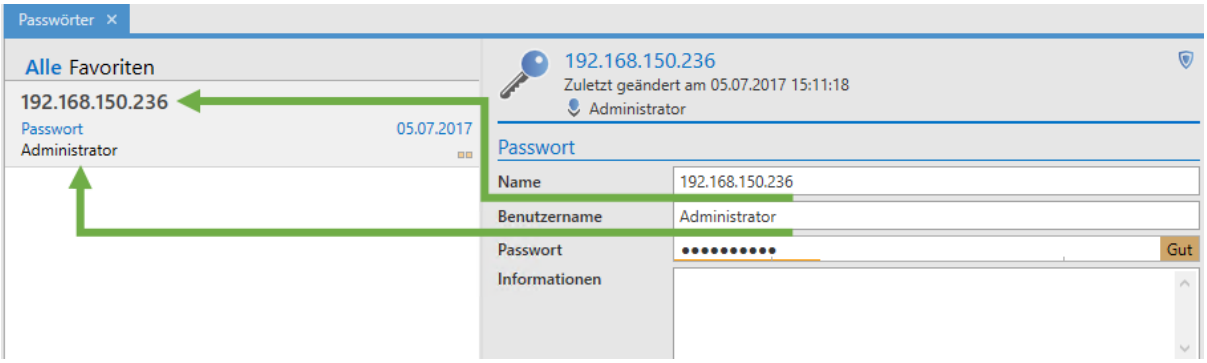
> ! Ist ein Formular angelegt, kann man dieses beim Erstellen neuer Datensätze auswählen. Voraussetzung hierfür ist, dass der angemeldete Benutzer auf das Formular mindestens Leseberechtigung besitzt.

# Berechtigungen auf Formulare

Analog zu anderen Objekten (Datensätze, Rollen, Dokumente,…) können auch Formulare berechtigt werden. Dies stellt sicher, dass einerseits nicht jeder existierende Formulare bearbeiten kann, andererseits können Formulare auf diese Art und Weise selektiv Benutzergruppen zur Verfügung gestellt werden. Auf diese Art und Weise ist sichergestellt, dass Übersichtlichkeit gewahrt wird und Benutzer nicht mit für diese irrelevanten Informationen konfrontiert sind. Das Formular “Kreditkarte” mag vielleicht Relevanz innerhalb der Buchhaltung haben, Administratoren sollten dieses in der Regel eher nicht brauchen.

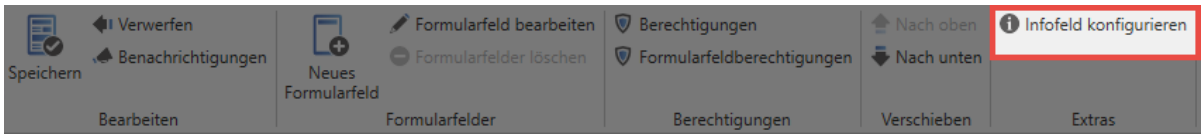
# Infofeld konfigurieren

Jeder Datensatz besitzt unterhalb des obligatorischen Datensatznamens in der Listenansicht weitere Informationen. Im nachfolgenden Beispiel wird zusätzlich zum Namen des Passworts noch der Benutzername angezeigt. Dazwischen findet sich in blauer Schrift der Name des Formulars.

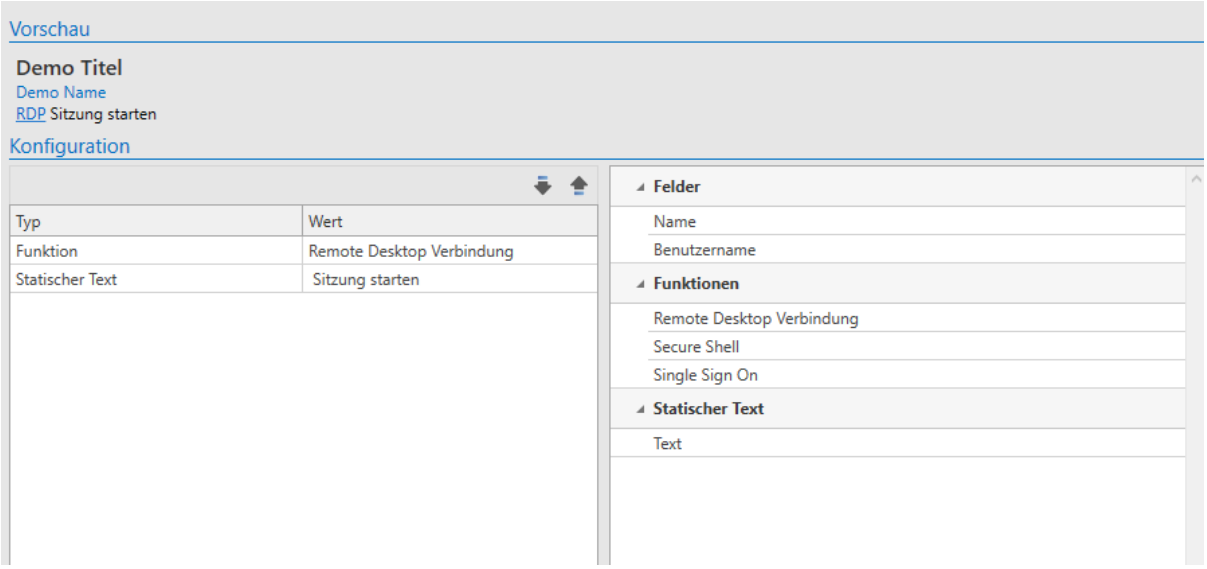



Der Name des Datensatzes (192.168.150.236) sowie des Formulars (Passwort) können nicht angepasst werden – diese werden immer angezeigt. Aktuell wird noch der im Datensatz hinterlegte Benutzer (Administrator) angezeigt. Dies ist im Infofeld des Formulars konfigurierbar. Man kann somit für jedes Formular separat definieren, welche Informationen innerhalb der Listenansicht eines Datensatzes direkt eingesehen werden sollen. Die Konfiguration des Infofeldes erfolgt, indem man im Modul Formulare das

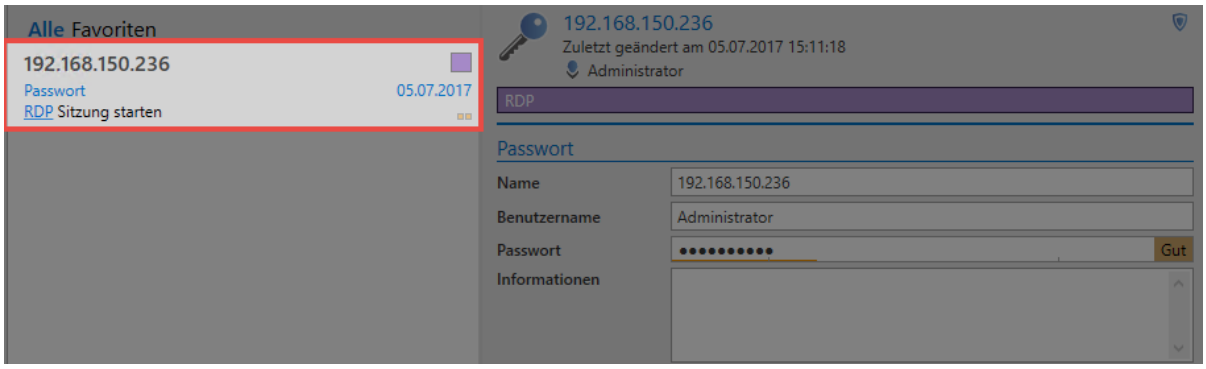
anzupassende Formular mit einem Doppelklick im Bearbeiten-Modus öffnet und anschließend die Schaltfläche **Infofeld konfigurieren** in der Ribbon betätigt.




Es öffnet sich wieder ein separates Tab, welches uns nun per Drag & Drop die Gestaltung des Infobereichs ermöglicht. Die rechts verfügbaren Felder können in das linke Konfigurationsfenster “gezogen” werden. Im nachfolgenden Beispiel soll im Infobereich “RDP Sitzung starten” sichtbar sein, wobei nur das Wort “RDP” mit einer Funktion belegt wird, nämlich dem Starten des RDP Managers. Im oberen Bereich existiert eine Vorschau.



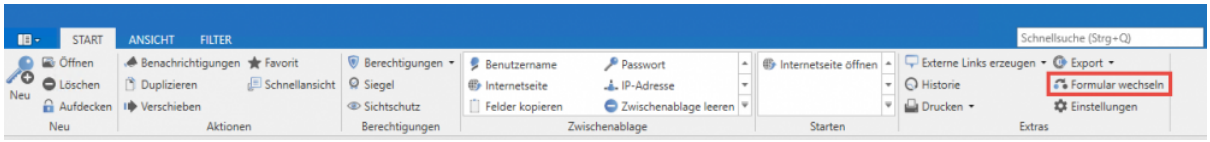

Das Infofeld des Formulars wurde nun aktualisiert. Das Aufrufen der RDP-Session ist nun direkt aus der RDP Session heraus möglich.



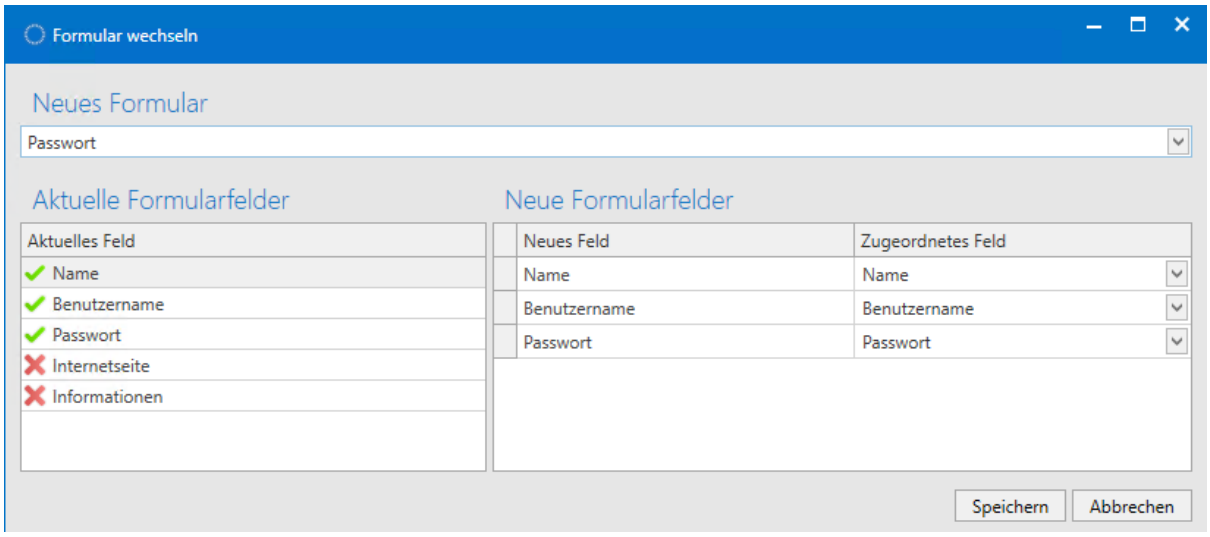
# Formulare wechseln

## Das Wechseln von Formularen

In manchen Fällen kann es notwendig sein, dass man das Formular eines Datensatzes wechselt. In diesen Fällen geht es meistens um Konsolidierungen von bestehenden Daten oder Anpassungen an etwaige Änderungen in Bezug auf die Datenstruktur. Die Funktionalität sind in der Ribbon unter “Extras/ Einstellungen” verfügbar.




Im nachfolgenden Schaubild ist der Dialog einsehbar, welcher das “Mapping” der Formularfelder des bisher genutzten Formulars mit denen des neuen Formulars gegenüberstellt. Hier wird versucht einen Datensatz, welcher bisher dem Formular “Internetseite” zugehörig war, auf das Formular “Passwort” (rechts) zu “mappen”.




Das Dropdown Menü ermöglich die Auswahl des Ziel-Formulars. Im Unteren Bereich erfolgt die Gegenüberstellung von aktuellen und neuen Formularfeldern.

- **Grüne Markierungen** kennzeichnen Felder, welche bereits im neuen Formular zugewiesen wurden
- **Rote Markierungen** kennzeichnen Felder ohne Zuweisung

! Bitte beachten Sie, dass Informationen auf diese Art und Weise verloren gehen können! Im Beispiel wären dies die Felder “Internetseite” sowie “Informationen”.

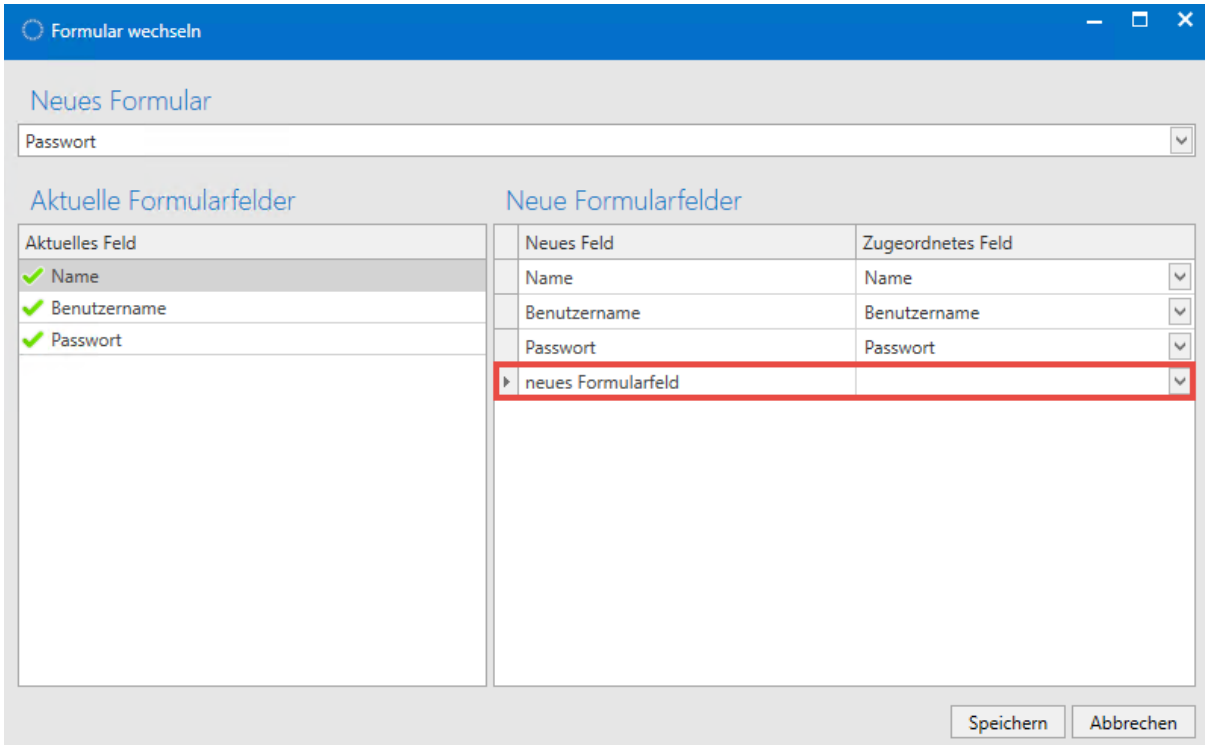
! Es wird das Benutzerrecht **Kann Formular eines Passworts wechseln** benötigt

# Auswirkungen von Anpassungen an Formularen auf bestehende Datensätze

Grundsätzlich gilt die Ausgangssituation, dass Änderungen an Formularen bestehende Datensätze nicht betreffen. Das bedeutet, dass ein Datensatz, welcher mit einem bestimmten Formular erstellt wurde, auch nach der Anpassung/Änderung dieses Formulars keine Änderung erfährt. Er verbleibt in seinem Originalzustand. Dennoch gibt es Methoden, wie Anpassungen an Formularen auch in bereits bestehende Datensätze übernommen werden können. Hierzu gibt es zwei Möglichkeiten:

## Formular wechseln

Betätigt man (wie im vorherigen Kapitel erwähnt) den Button “Formular wechseln”, wird als Standard das bereits vorhandene Formular gesetzt. Wurde dieses nun zwischenzeitlich geändert, wird direkt das neue Formularfeld angezeigt und nach dem Speichern übernommen.



### Formularänderungen auf Passwörter anwenden

Die Einstellung “Formularänderungen auf Passwörter anwenden” ermöglicht, dass Änderungen an Formularen erzwungen werden. Dies wird wirksam beim Bearbeiten des Datensatzes! Es ist hierbei unerheblich, ob am Datensatz Veränderungen vorgenommen wurden. Allein das erneute Bearbeiten und Speichern des Datensatzes führt die Anpassung des Formulars herbei.

**Folgende Berechtigungen/Konfigurationen müssen gegeben sein:**

- Der Benutzer, welche die Änderung vornehmen will, benötigt Leserecht auf das Formular
- Man benötigt Schreibrechte auf den Datensatz (sowie die anzupassenden Formularfelder)
- Versiegelte und sichtgeschützte Datensätze bleiben unangetastet

## Fazit

Beiden Varianten gemeinsam ist, dass Anpassungen an Formularen nicht automatisiert herbeigeführt werden können. Bereits bestehende Datensätze werden also nicht automatisch angepasst. Es muss demnach manuell die Änderung übernommen werden. Im ersten Fall ist der manuelle Schritt die Nutzung der Funktion “Formular wechseln”. Im zweiten Fall genügt schon das Bearbeiten und Speichern des Datensatzes.

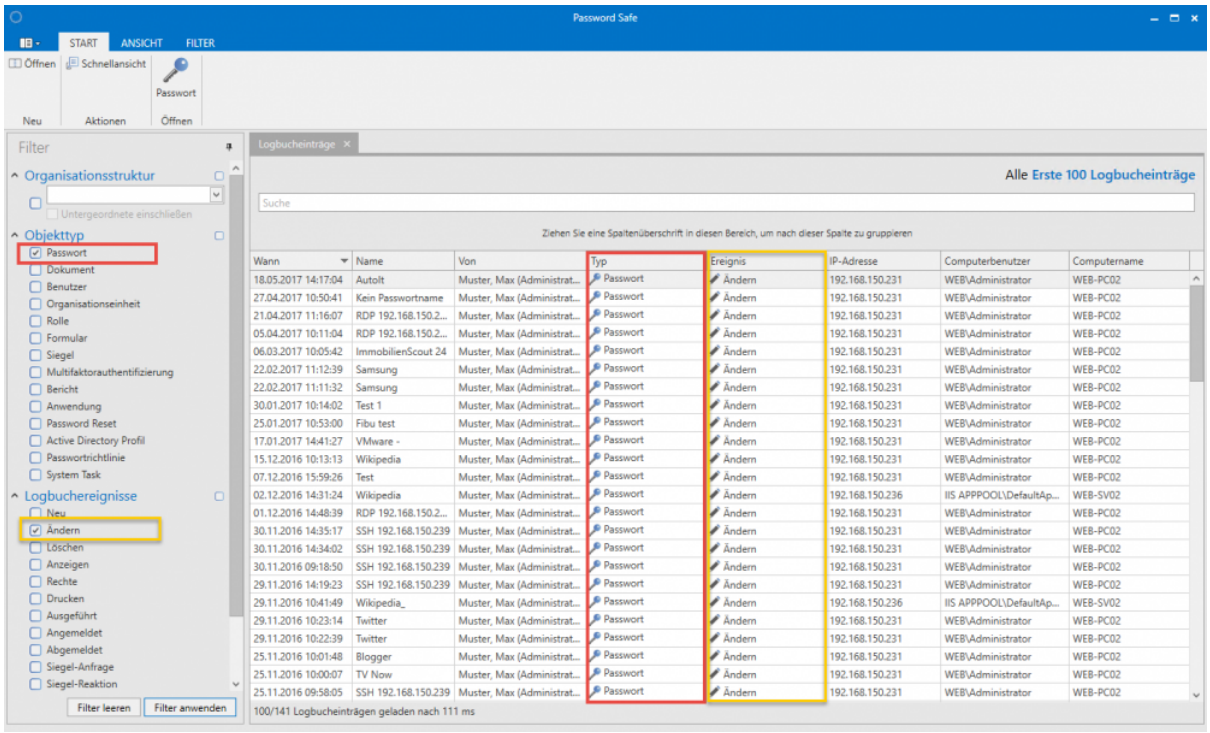
# Logbuch

## Was ist das Logbuch?

Password Safe protokolliert jegliche Interaktionen der Benutzer. Über das gleichnamige Modul können diese Einträge eingesehen und gefiltert werden. Hierdurch kann an zentraler Stelle jederzeit nachvollzogen werden, welcher Benutzer wann genau welche Änderungen vorgenommen hat. Dieses Modul ist (theoretisch) als unkritisch einzustufen, da der Mitarbeiter nur auf diejenigen Logbucheinträge Zugriff hat, auf die er auch tatsächlich berechtigt ist. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert.

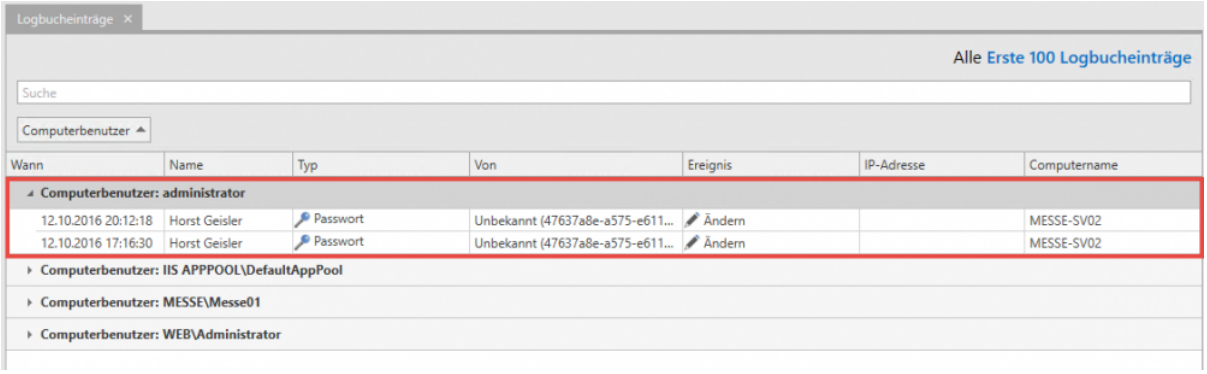

## Einsatz des Filters im Logbuch

Wie in allen anderen Modulen auch kann man im Logbuch den Filter nutzen, um die Anzahl der ausgegebenen Elemente gemäß definierbarer Kriterien einzugrenzen. Im nachfolgenden Beispiel sucht man nach Logbucheinträgen, welche am Objekttyp “Passwort” vorgenommen wurden und dem Ereignis “Ändern” entsprechen. Kurz gesagt: Es wird nach Änderungen an Passwörtern gefiltert.



# Gruppierungen im Logbuch

Die sich daraus ergebende Auflistung kann darüber hinaus noch durch Drag & Drop der Spaltenüberschriften gruppiert werden. Nachfolgend wurde dies anhand der Gruppierung der Spalte “Computerbenutzer” vorgenommen. Die gefilterten Informationen geben nun also all Ergebnisse aus, welche Änderungen an Passwörtern durch den Computerbenutzer “administrator” entsprechen.



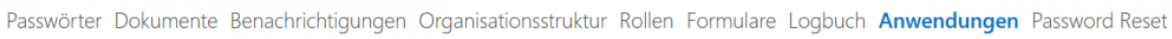

# Revisionssicherheit

Password Safe verfolgt bei der Handhabung des Logbuchs aktuell einen kompromisslosen Weg. Es wird jede Zustandsänderung in erfasst und in der MSSQL-Datenbank abgelegt. Es ist nicht vorgesehen, dass selektiv die Auslöser eines Logbuch-Eintrags definiert werden können. Nur diese Herangehensweise ermöglicht die revisionssichere und somit unverfälschbare Nachvollziehbarkeit von Änderungen.

# Anwendungen

## Was sind Anwendungen?

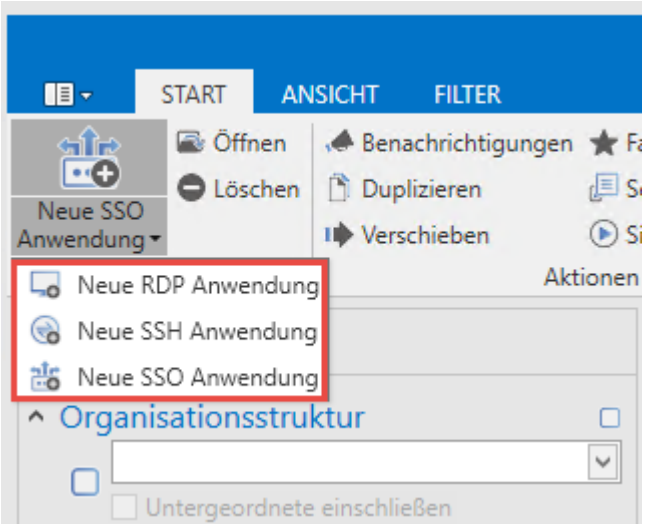
Mit Hilfe von Anwendungen kann die automatisierte Anmeldungen an verschiedenen Systemen konfiguriert werden. Besonders im Zusammenspiel mit diversen Schutzmechanismen profitiert das Unternehmen somit in Bezug auf Sicherheit, da komplexe Passwörter automatisiert und für den Benutzer verdeckt in Anmeldemasken eingefügt werden. Zur Verfügung stehen hier verschiedenen Typen wie Remote Desktop (RDP), Secure Shell (SSH), allgemeine Anwendungen (SSO) und Web. Die Single Sign On Engine bietet unzählige Konfigurationsmöglichkeiten, um eine automatische Anmeldung an nahezu jeder Art von Software zu realisieren. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert.




> Das automatisierte Anmelden an Webseiten wird über den SSO Agent abgedeckt.

## Die drei Arten von Anwendungen

Password Safe unterscheidet drei verschiedene Arten von Anwendungen.

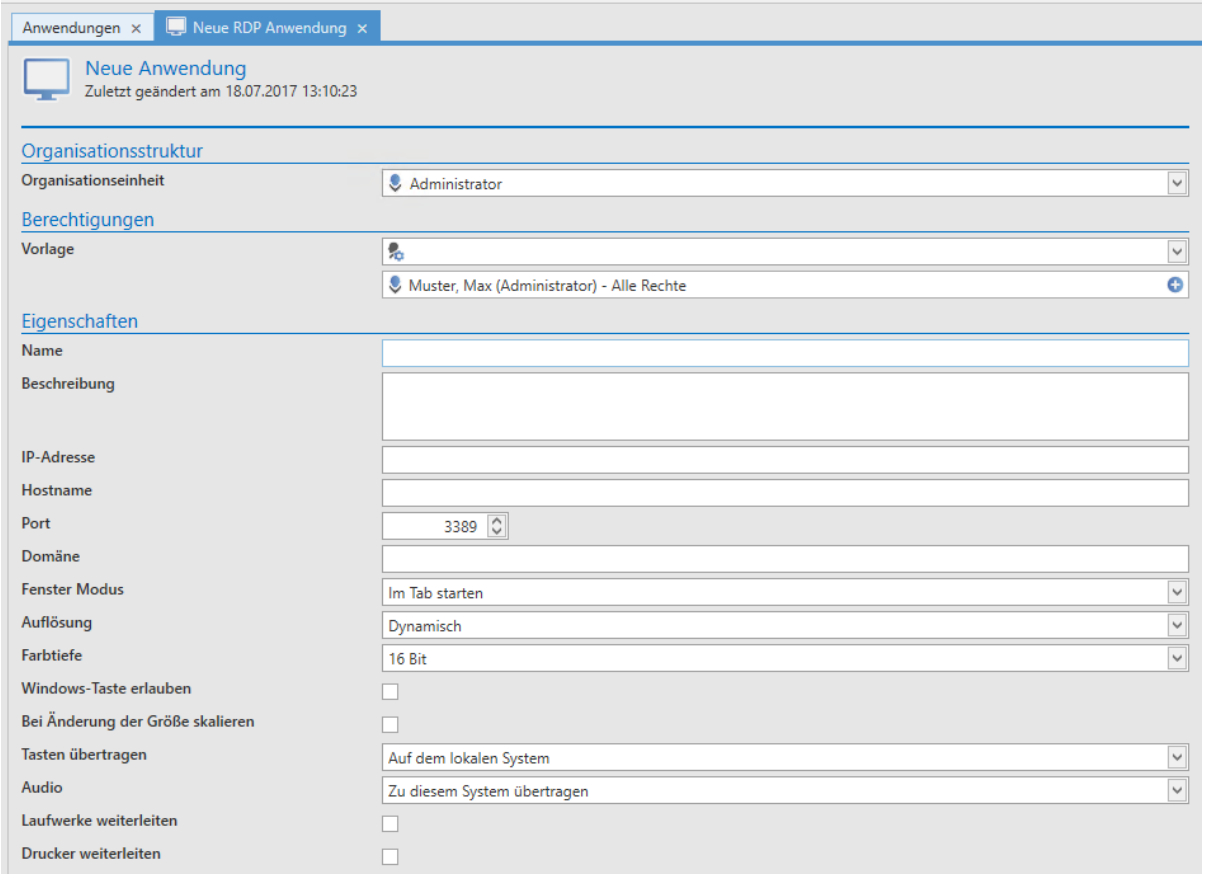



In Bezug auf die Handhabung lassen sich **RDP und SSH** Anwendungen gut zusammenfassen. Beide Anwendungstypen können (optional) im Password Safe “embedded” dargestellt werden. Die jeweilige Sitzung öffnet sich demnach in einem eigenen Tab im Lesebereich. In der Kategorie **SSO Anwendungen** werden alle weiteren Formen der automatisierten Anmeldung zusammengefasst. Wie

genau diese erstellt und genutzt werden, wird im Folgekapitel behandelt. Hierzu zählen alle Formen von Windows Anmeldemasken wie auch Anwendungen für Webseiten. Diese werden – im Gegensatz zu RDP und SSH – nicht embedded gestartet, sondern öffnen sich wie gewohnt im eigenen Fenster. Diese SSO Anwendungen müssen im Vorfeld einmalig definiert werden. Innerhalb des Password Safe spricht man hierbei auch vom Anlernen von Anwendungen. Im Gegensatz hierzu können RDP und SSH komplett innerhalb des Password Safe sowohl definiert als auch gestartet werden.

# RDP und SSH

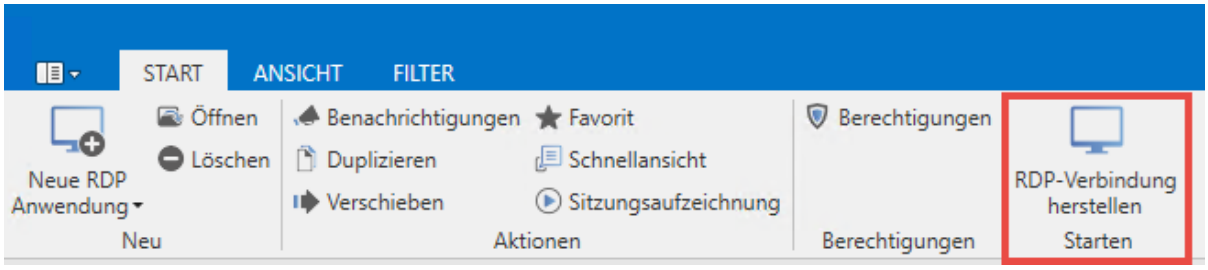
Über die Ribbon als auch über das Kontextmenü der rechten Maustaste kann eine neue RDP/SSH Anwendung erstellt werden. Es öffnet sich jeweils das entsprechende Formular, bei der man die Variablen für eine Verbindung definieren kann.



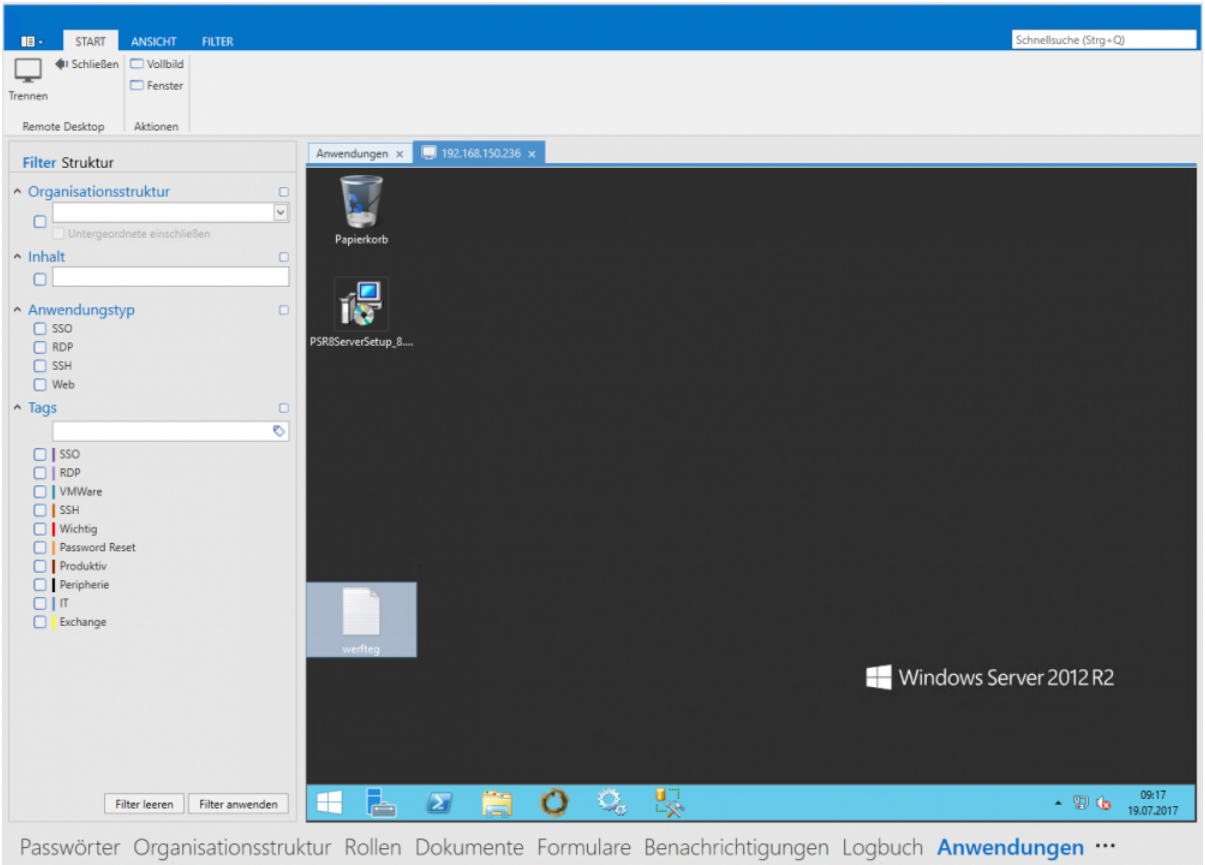

Diese Variablen entsprechen genau auch denjenigen, welche man (hier am Beispiel RDP) bei der Erstellung einer RDP-Verbindung über “mstsc” konfigurieren kann. Ob die Verbindung in einem Tab, im Vollbildmodus oder in einem Fenster gestartet werden soll, kann im Feld **“Fenstermodus”** definiert werden.

## Arbeiten mit RDP- und SSH-Anwendungen

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

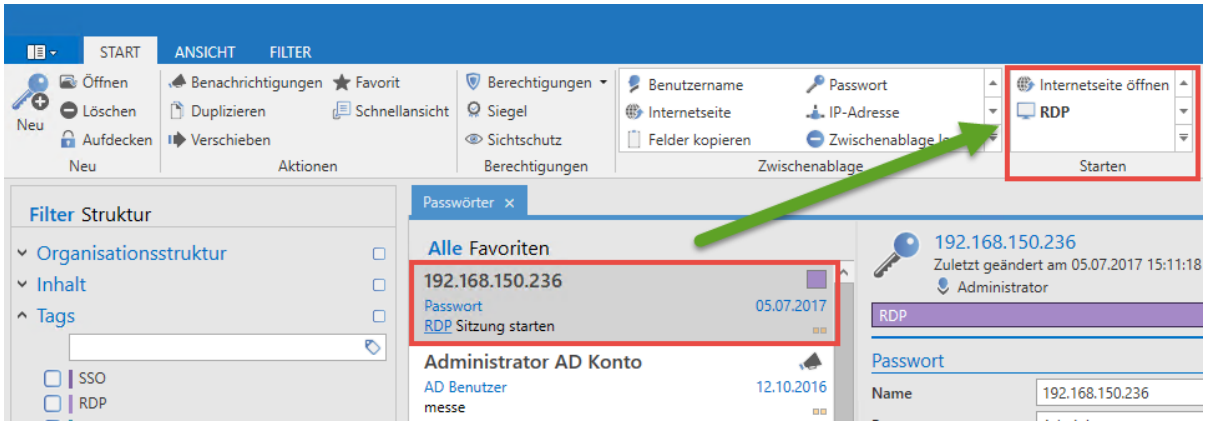



Password Safe versucht sich nun, mit den zur Verfügung stehenden Informationen am Zielsystem anzumelden. Daten, welche im Formular nicht hinterlegt wurden, werden direkt beim Öffnen der Session abgefragt. Es ist demnach auch möglich, erst nach dem Starten der Password Safe Anwendung die IP Adresse und/oder das Passwort anzugeben. Sind alle Daten abgefragt, öffnet sich die RDP Sitzung in einem Tab – falls definiert (Feld Fenster Modus in der Anwendung):

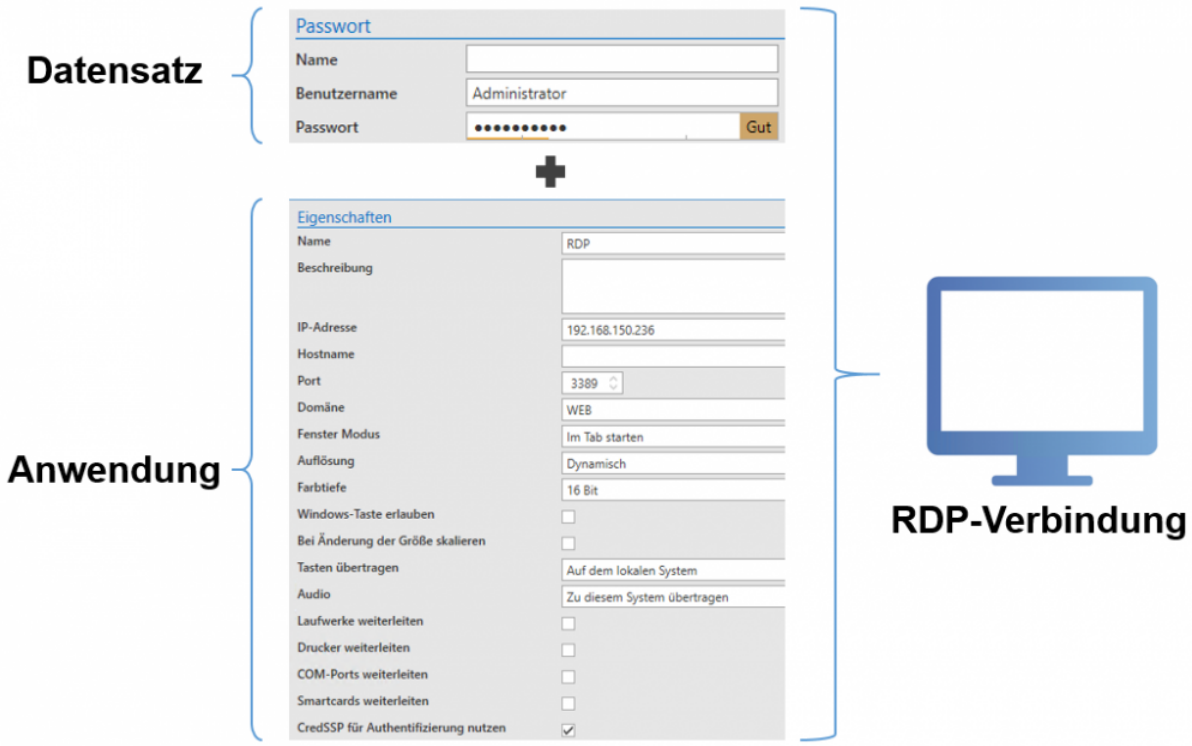


# Verbindung von Datensätzen und Anwendungen

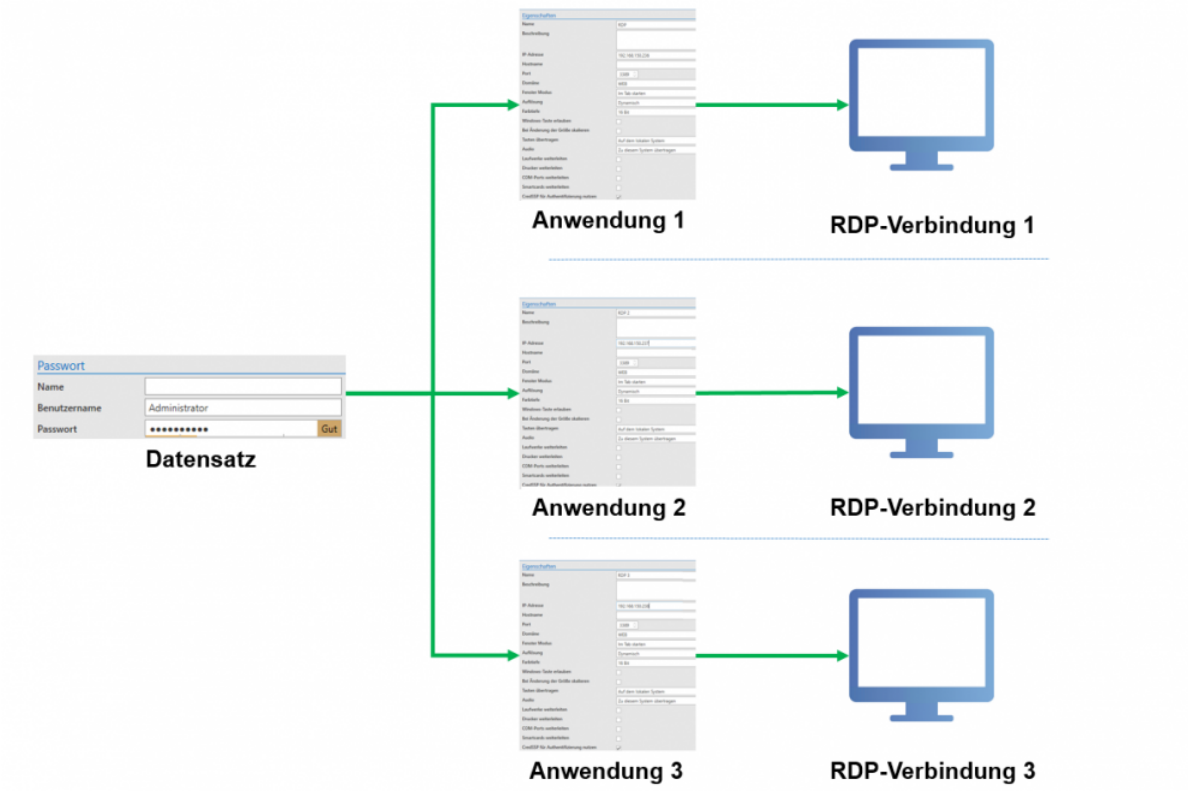
Die Anwendung definiert demnach die Rahmenbedingungen für die angestrebte Verbindung sowie optional auch das Zielsystem. Durch das Verbinden von Datensätzen mit Anwendungen kann nun die komplette Anmeldung automatisiert abgebildet werden. Wenn der Datensatz nun auch Benutzername und Passwort liefert, liegen alle für eine Anmeldung erforderlichen Informationen vor. Verknüpft werden Anwendungen und Datensätze über den Reiter “Starten” in der Ribbon. Ist diese Verknüpfung für einen Datensatz hergestellt, ist die 1-Click-Anmeldung am Zielsystem möglich.




Das nachfolgende Beispiel soll dies anhand einer RDP-Verbindung veranschaulichen:



Es könnte auf diese Art und Weise auch ein Datensatz mit mehreren Zielsystemen verknüpft werden. Benutzername und Datensatz werden aus dem Datensatz gespeist, Alle verbleibenden, für die Anmeldung erforderlichen Informationen, kommen aus den unterschiedlichen Anwendungen. Im nachfolgenden Beispiel wäre ein Datensatz (Benutzername und Passwort) mit mehreren Zugängen verknüpft.




Dies ist in der Regel durchaus sehr verbreitetes Szenario. Dennoch soll darauf hingewiesen werden, dass das Ansprechen mehrere Server mit einem einzigen Passwort sicherheitstechnisch bedenklich ist. Es wird in der Regel empfohlen, für jeden Server/Zugang ein eigenes Passwort zu vergeben.

> Es besteht die Möglichkeit in der Anwendung das Feld **IP Adresse** leer zu lassen. Existiert ein Feld **IP Adresse** im verknüpften Datensatz existiert, dann wird diese Adresse verwendet. Wenn es auch im Datensatz keine IP Adresse gibt, erscheint ein Popup in welchem die gewünschte IP manuell eingetragen werden kann.

# Anlernen von Anwendungen

## Welche Anwendungen müssen angelernt werden?

Wie bereits im vorherigen Kapitel erwähnt, sind RDP und SSH komplett in den Password Safe embedded. Diese müssen also nicht gesondert angelernt werden. Alle weiteren Anwendungen unter Windows werden einmalig angelernt.

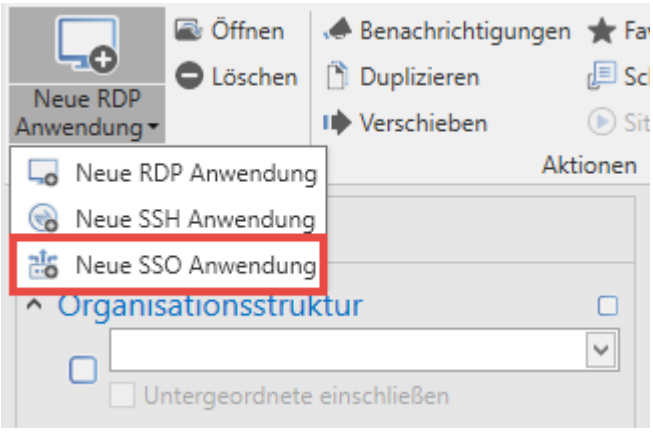
### Was passiert beim Anlernen?

Der Datensatz hält Benutzername und Passwort. Beim Anlernen erfolgt die Definition der Arbeitsschritte. Das Ergebnis entspricht quasi einem Skript welches definiert, wo genau die Anmeldedaten eingetragen werden sollen. In Password Safe wird die fertiggestellte Arbeitsanweisung selbst auch “Anwendung” genannt.

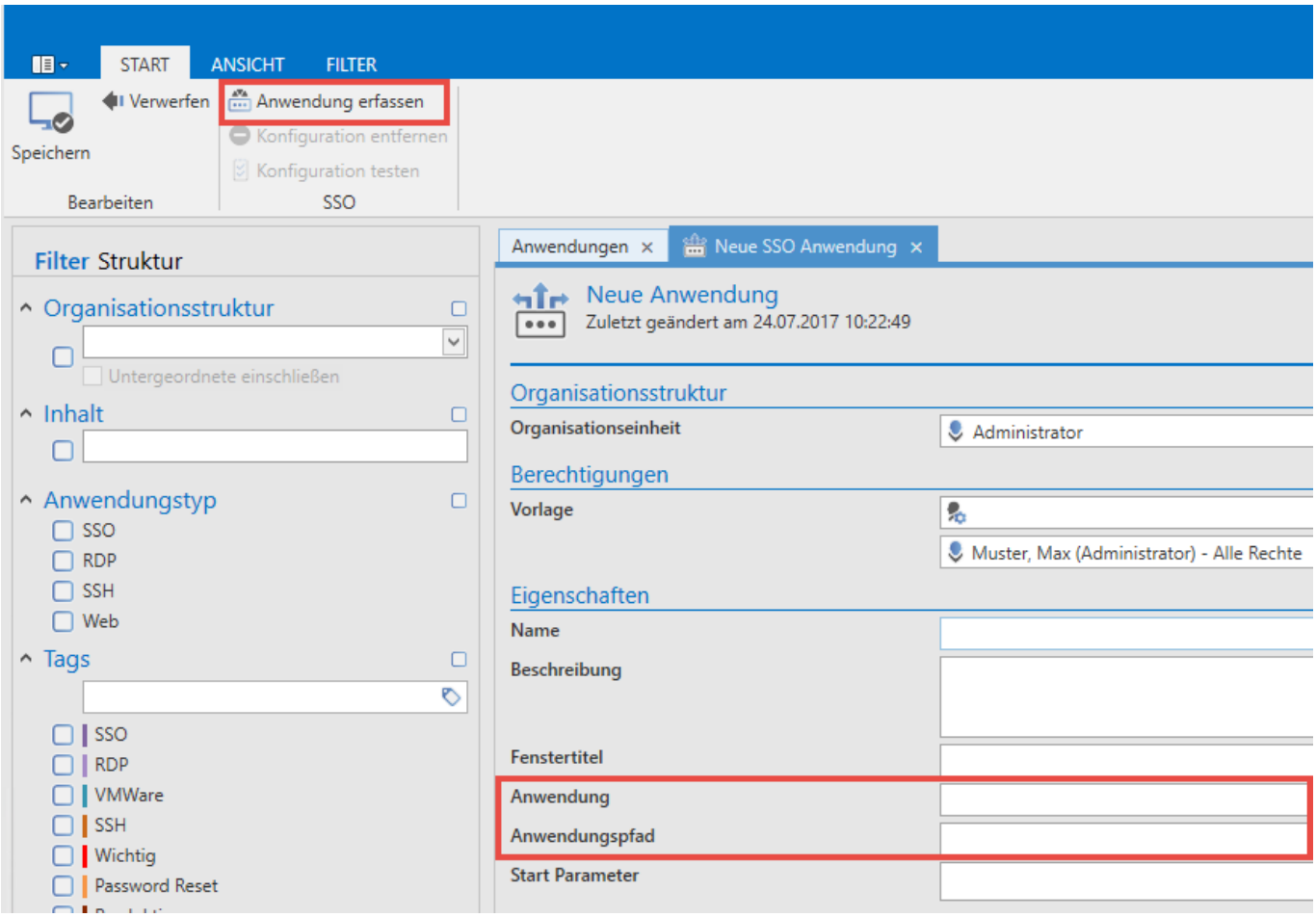
## Konfiguration

> ! Für die Erstellung von Anwendungen ist das Benutzerrecht “Kann neue Anwendungen anlegen” erforderlich

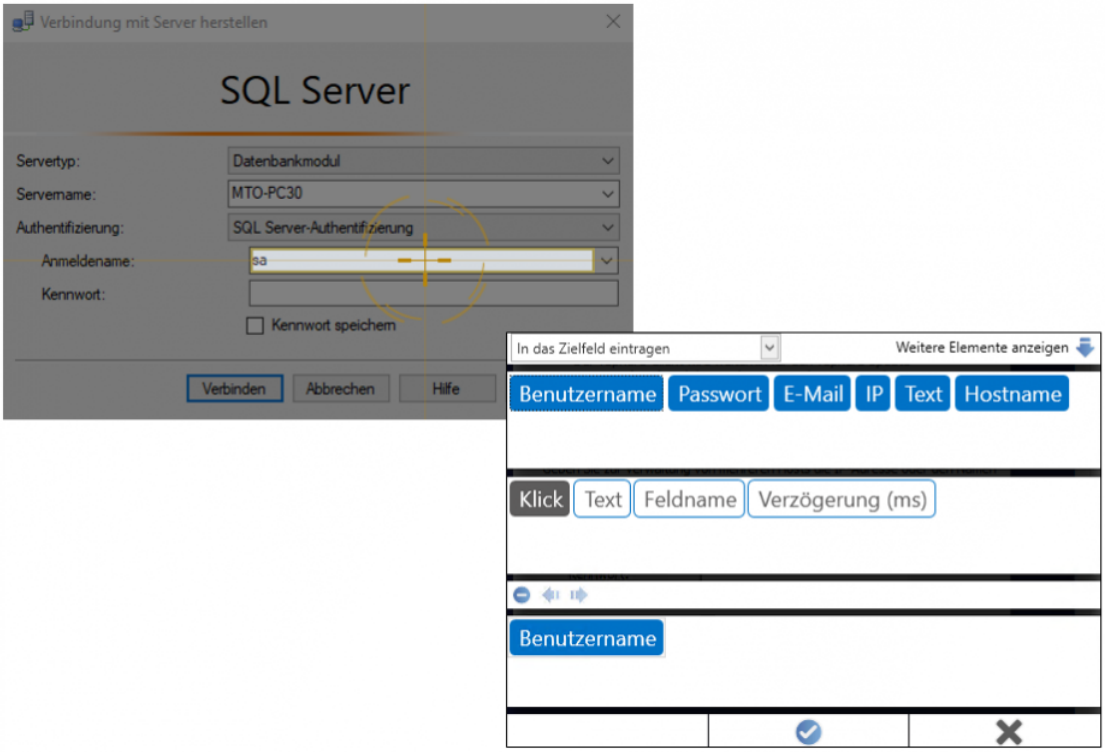
Im ersten Schritt erstellt man über die Ribbon eine neue SSO Anwendung.



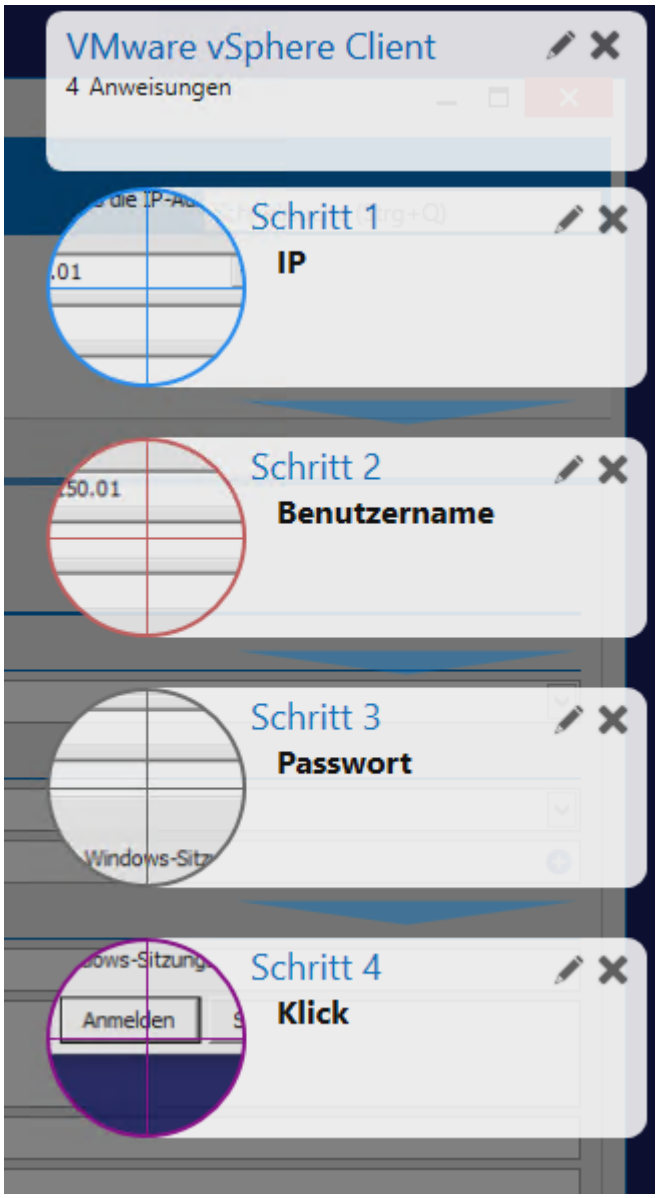

Im sich öffnenden Tab können nun diverse Eigenschaften für die Anwendung definiert werden. Die Felder **Fenstertitel**, **Anwendung** sowie **Anwendungspfad** werden nicht manuell befüllt. Dies erfolgt über den Button **Anwendung erfassen** in der Ribbon:



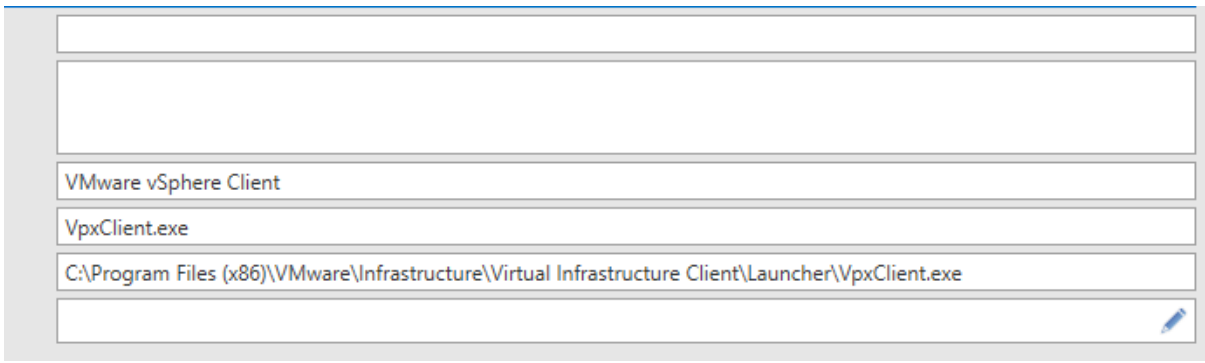

Es erscheint nun ein Fadenkreuz. Dieses ermöglicht das eigentliche “Mapping”, bzw. die Zuweisung der Zielfelder. Nachfolgend ist zu sehen, wie die Feldzuweisung für den Benutzernamen am Beispiel der Anmeldung an SQL Server abläuft. Analog erfolgt dies auch bei der Zuweisung aller weiteren Felder, die automatisch eingetragen werden sollen. Die Vorgehensweise ist immer dieselbe. Man wählt das Feld aus, welches automatisiert eingetragen werden soll und entscheidet dann, mit welcher Information dieses gefüllt werden soll.




Parallel zum vorherigen Arbeitsschritt wird am rechten Bildschirmrand jede bereits getätigte Zuweisung dargestellt. In diesem Beispiel wurde der VMware vSphere Client mit insgesamt 4 Anweisungen gespeist: IP, Benutzername, Passwort sowie das Klicken des Buttons für die abschließende Anmeldung.



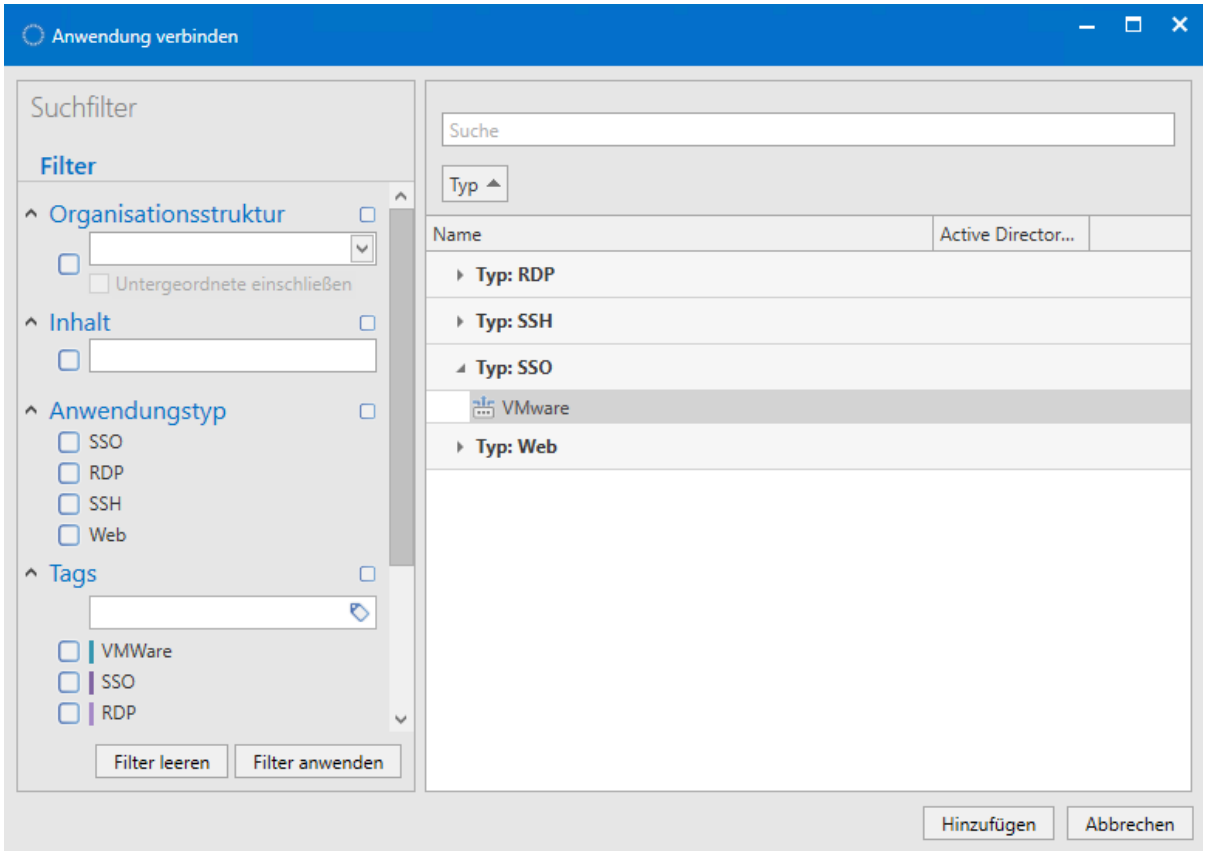

Hat man alle Felder zugewiesen, verlässt man mit der Eingabetaste die Anwendungserfassung. Es wurden nun die eingangs erwähnten Felder “Fenstertitel”, “Anwendung” und “Anwendungspfad” automatisch befüllt.



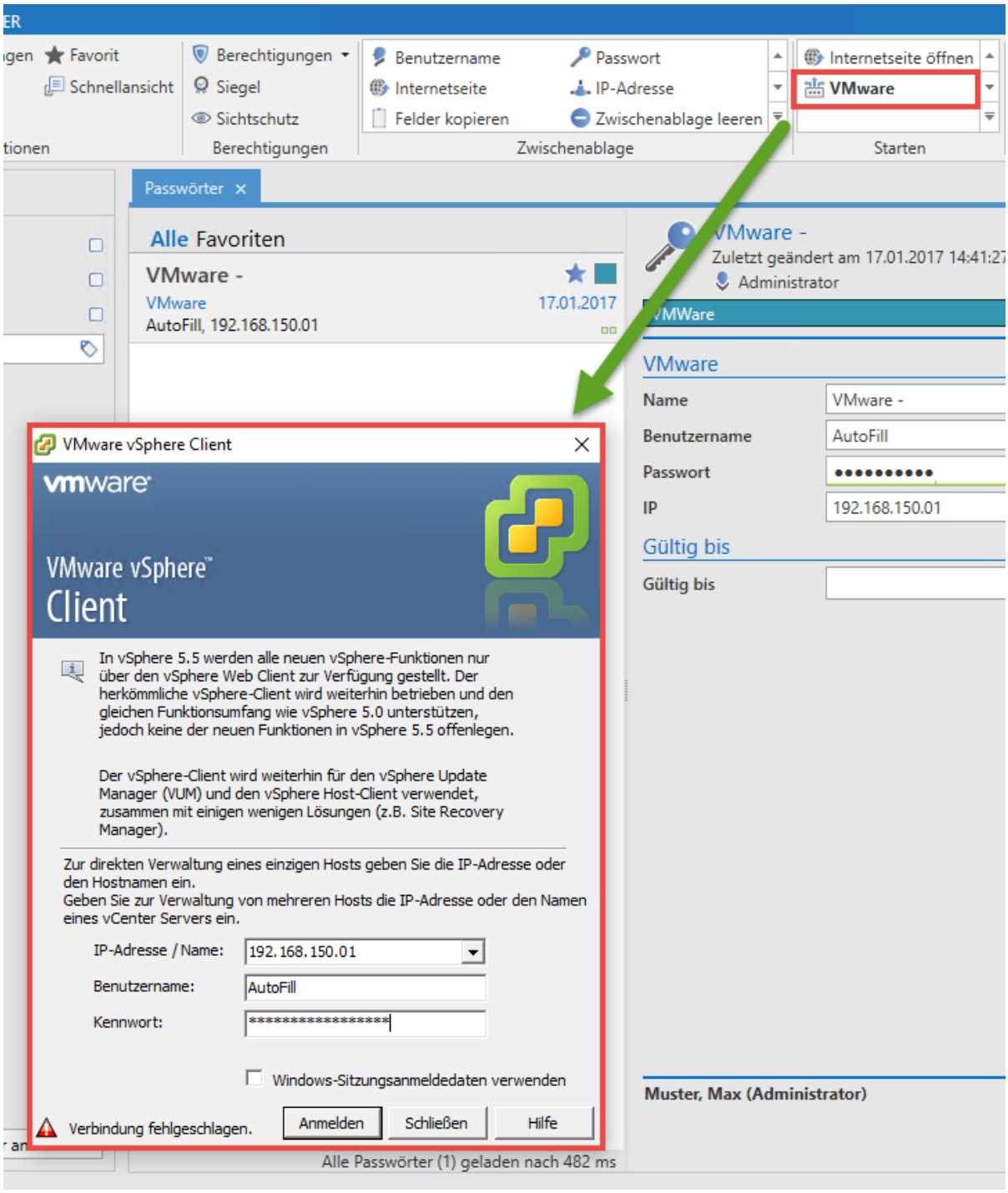
Wie zu sehen ist, wird direkt die .exe Datei referenziert. Wenn bei allen Anwendern dementsprechend die Anwendung am selben Ablageort gespeichert ist, kann diese Anwendung dann auch von allen weiteren Benutzern angesprochen werde.

# Verknüpfen von Datensätzen mit Anwendungen

Im Modul Passwörter kann nun direkt die erstellte Anwendung verknüpft werden. Hierzu markiert man den zu verknüpfenden Datensatz und öffnet über die Ribbon im Reiter “Starten” das Menü “Anwendung verbinden”. Es öffnet sich die Auswahl aller zur Verfügung stehenden Anwendungen. Dort kann nun die zuvor erstellte Anwendung “VMware” verknüpft werden.




Wurde die Verknüpfung hergestellt, kann zukünftig diese Anwendung direkt über die Ribbon gestartet werden. Das Betätigen des Buttons öffnet direkt die verknüpfte Anwendung.




! Anwendungen unterliegen in Bezug auf Berechtigungen den gleichen Gesetzmäßigkeiten wie Passwörter, Rollen oder Dokumente. Man kann also für jede Anwendung separat definieren, welche Benutzerschicht diese verwenden darf.

# Sitzung aufzeichnen

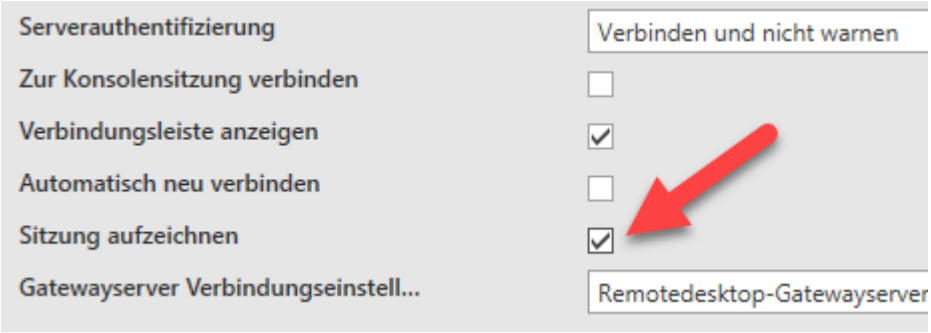
## Was ist die Sitzungsaufzeichnung (Session Recording)?

Über die Sitzungsaufzeichnung – auch als Session Recording bekannt – ist es möglich RDP- und SSH-Sitzungen visuell aufzuzeichnen. Diese Aufzeichnungen können dann anschließend angesehen und ausgewertet werden. Hierbei ist es auch möglich dies so einzuschränken, dass nur der Benutzer selbst oder eine zugewiesene Person, wie z.B. ein Sicherheitsbeauftragter, diese Aufzeichnungen ansehen und auswerten kann.

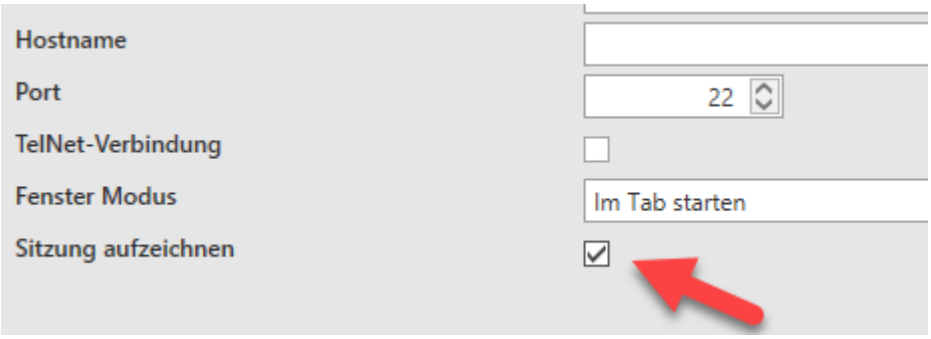

> Beachten Sie, dass die Sitzungsaufzeichnung Speicherplatz innerhalb der Datenbank benötigt. Die Aufnahmen werden zwar Ressourcensparend abgelegt, jedoch variiert die Speichergröße sehr stark mit dem Inhalt. Je mehr sich in der aufgezeichneten Sitzung tut, je höher ist auch der Speicherverbrauch.

Die Sitzungaufzeichnugen müssen bei der jeweiligen RDP- oder SSH-Anwendung erst aktiviert werden, damit die Aufzeichnung statt findet.

RDP




SSH

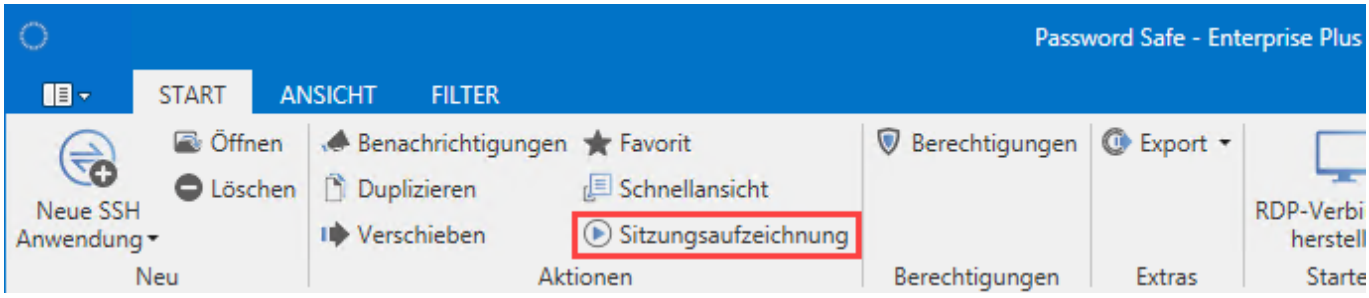


Ist die Einstellung aktiviert, so wird beim nächsten Verbindungsaufbau die Aufzeichnung automatisch gestartet.

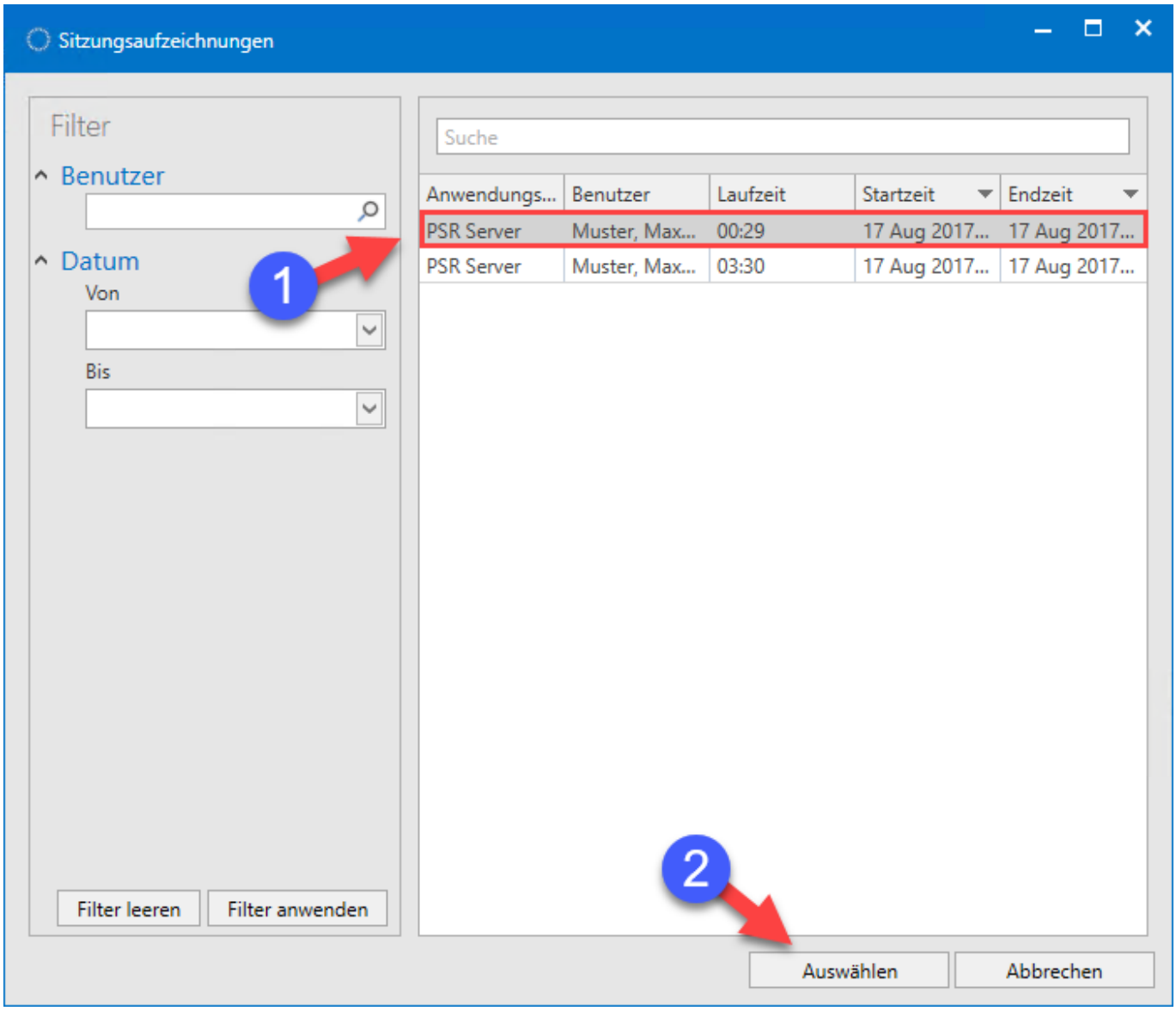
> Die Aufzeichnungen werden bereits während der Aufnahme zum Server und in die Datenbank gestreamt. Somit gehen auch bei einem Verbindungsabbruch keine Aufzeichnungen verloren und sind bis zu einem Verbindungsabbruch oder Ende der Sitzung sofort gespeichert.

## Sitzungsaufzeichnungen ansehen

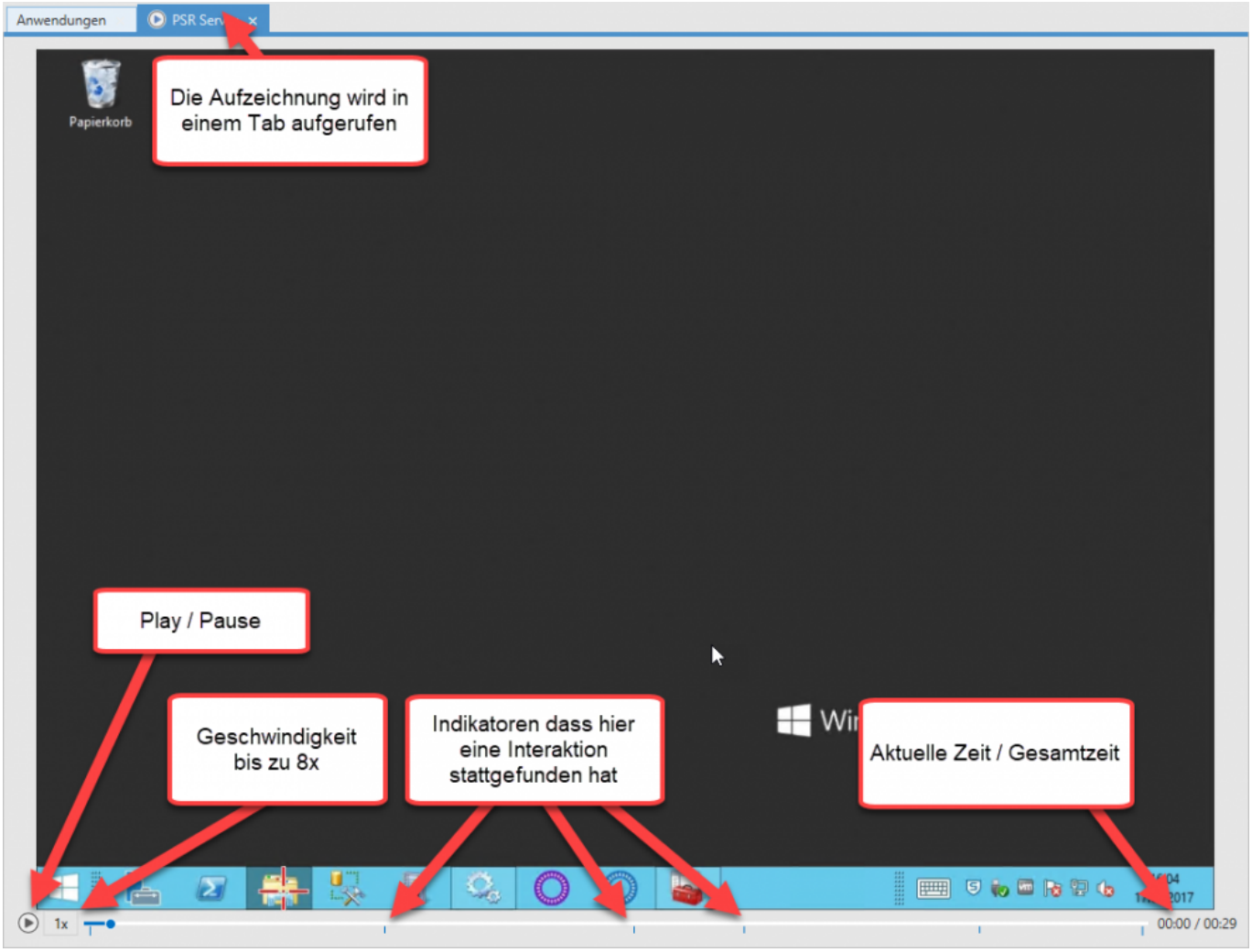
Sind Aufzeichnungen für eine Anwendung vorhanden, so können diese im Modul Anwendungen aufgerufen und angesehen werden.




Innerhalb der Sitzungsaufzeichnungen kann wie gewohnt über den Filter nach Aufzeichnungen gesucht werden. Hierbei hat man die Möglichkeit das Suchergebnis nach Datum und Benutzern einzuschränken. Ebenso kann im rechten Bereich über die Listensuche nach allen Spalteninhalten weiter gefiltert werden.




Nachdem eine Sitzungsaufzeichnung ausgewählt wurde, öffnet sich ein neues Tab indem man sich die Aufzeichnung ansehen kann. Über die Ribbon kann die Funktion “Untätigkeit überspringen” aktiviert werden, so kann eine Aufzeichnung effektiv schnell durchgesehen werden um lediglich die relevanten Aktionen zu sehen.




Wann werden Indikatoren gesetzt?

- Mausklick
- Tastaturbefehle

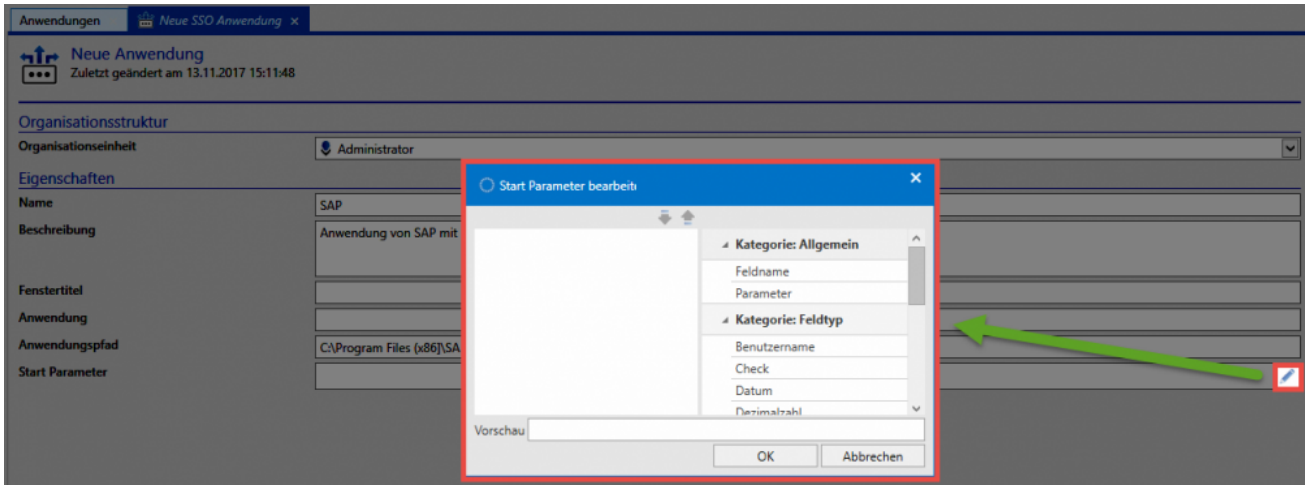
# Startparameter

## Startparameter für SSO Anwendungen

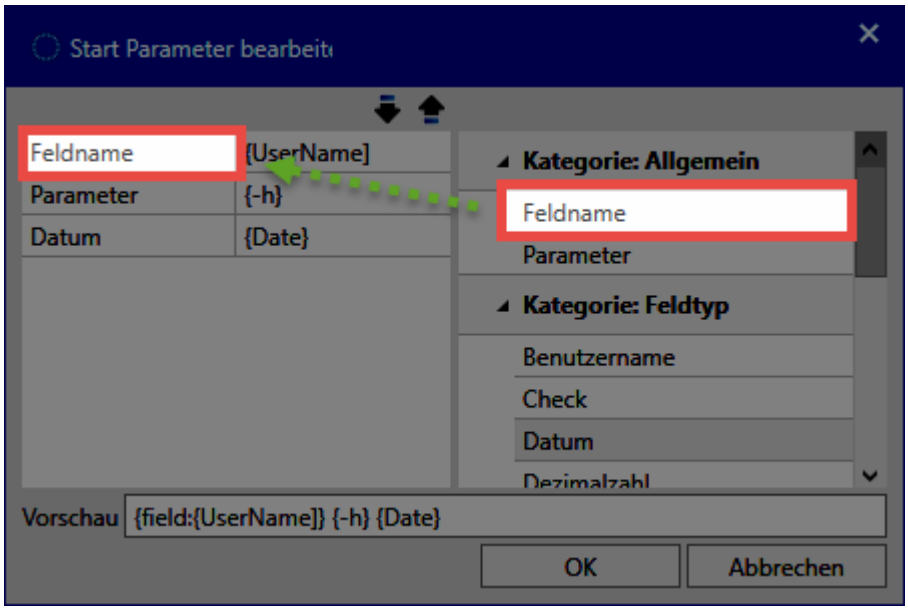
Beim Erstellen bzw. Bearbeiten einer SSO Anwendung können Startparameter definiert werden. Beim Start der Anwendung werden diese Parameter dann direkt mit übergeben. Beispielsweise um das Programm direkt mit diversen Grundeinstellungen zu starten. Die entsprechenden Parameter sind direkt beim Hersteller der Software zu erfragen bzw. in der Dokumentation nachzusehen.

## Konfiguration der Parameter

Die Parameter können direkt in der Anwendung im entsprechenden Feld eingetragen werden. Alternativ steht auch ein Konfigurationsfenster zu Verfügung.




Hier können die benötigten Elemente per Drag&Drop von der rechten auf die linke Seite gezogen werden.




Hierbei stehen Kategorien zur Verfügung:

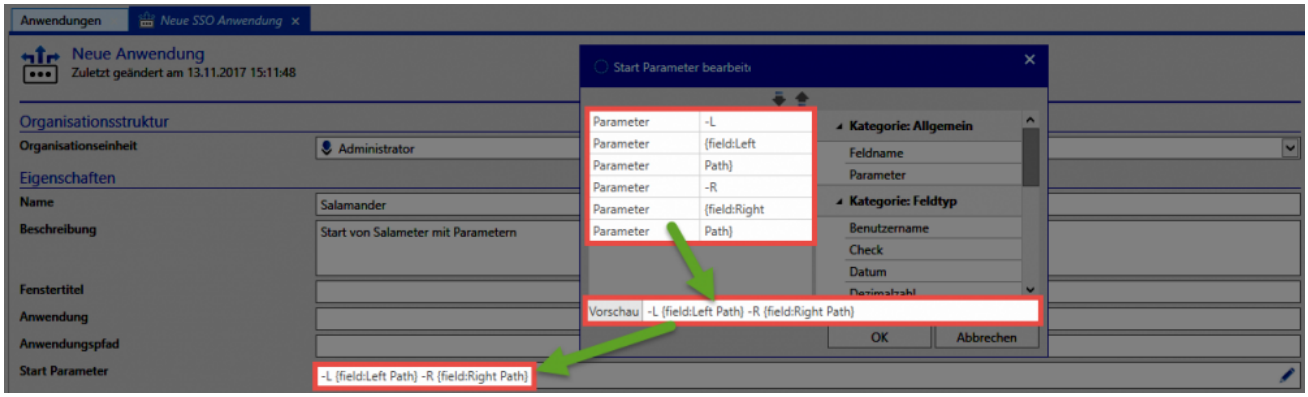
- Über **Parameter** werden lediglich die Parameterbezeichnungen **Feldname** oder **Parameter** vorgegeben. Diese müssen dann manuell ergänzt werden.
- über die Parameter der Kategorie **Feldname** können Felder direkt angesprochen werden also direkt die Feldnamen übergeben.

## Beispiel

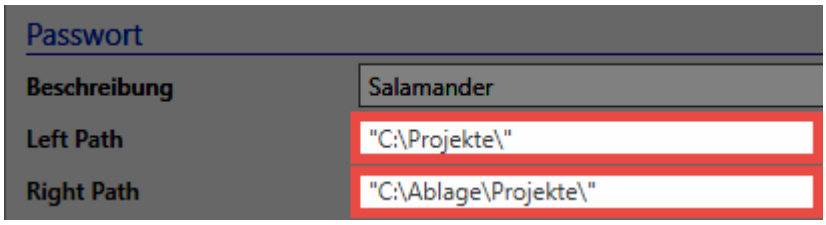
In diesem Beispiel wurden für die Anwendung Salamander folgende Startparameter definiert:

- -L (für Ordner Pfad in der linken Spalte)
- -R (für Ordner Pfad in der rechten Spalte)

Für beide werden jeweils die Passwort Felder mit dem Namen “Left Path” und “Right Path” übergeben.




Verknüpft wird die Anwendung schlußendlich mit folgendem Passwort:




Beim Start von Salamander werden die Platzhalter durch die Feldnamen ersetzt. Es wird also statt

**-L {field:Left Path} -R {field:Right Path}**

folgender Startparameter übergeben:

**-L “C:\Projekte\” -R “C:\Ablage\Projekte”**

# Platzhalter für Felder

Über bestimmte Platzhalter können Felder anhand ihres Typen oder anhand ihres Namens eingefügt werden. Am einfachsten gelingt das über das oben beschriebene Konfigurationsfenster.

| Feldtyp | Platzhalter |
|---|---|
| Text | {Text} |
| Passwort | {Password} |
| Datum | {Date} |
| Check | {Check} |
| URL | {Url} |
| E-Mail | {Email} |
| Telefon | {Phone} |
| Liste | {List} |
| Überschrift | {Header} |
| Mehrzeiliger Text | {Memo} |
| Mehrzeiliger Passwort Text | {PasswordMemo} |
| Ganzzahl | {Int} |
| Gleitkommazahl | {Decimal} |
| Benutzername | {UserName} |
| IP-Adresse | {Ip} |
| Feldname eingeben | {field:name} |

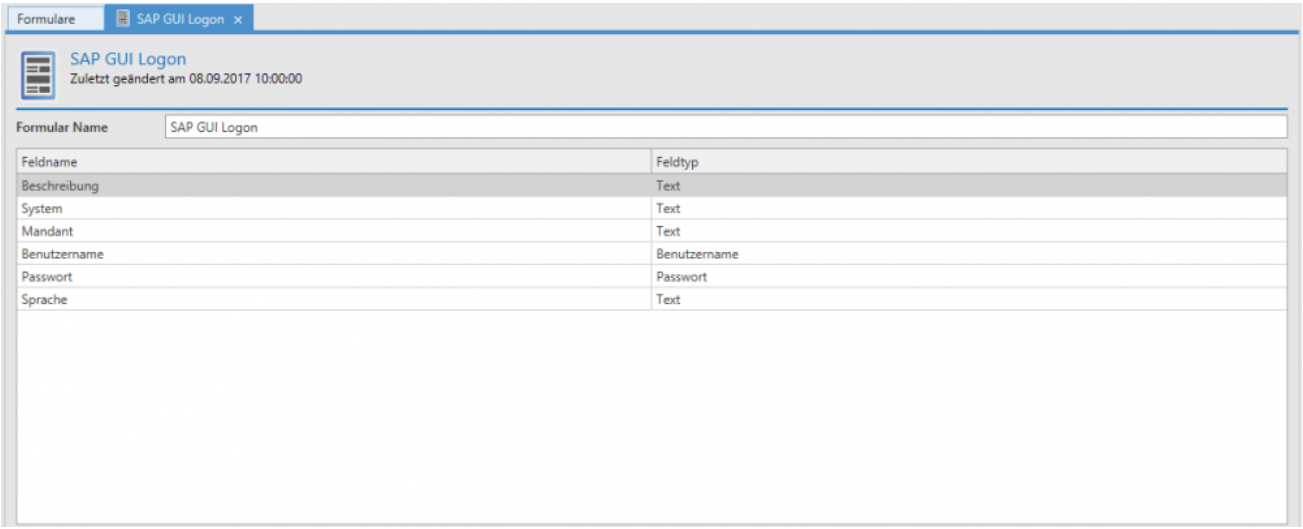
# SAP GUI Logon

## Grundlegende Informationen

“Die Anmeldung an SAP kann über “”:”#startparameter realisiert werden. Voraussetzung hierfür ist, dass die Anmeldung über “SAPshortcut” ausgeführt wird.
Unter “”:https://wiki.scn.sap.com/wiki/display/NWTech/SAPshortcut werden alle verfügbaren Parameter gelistet.

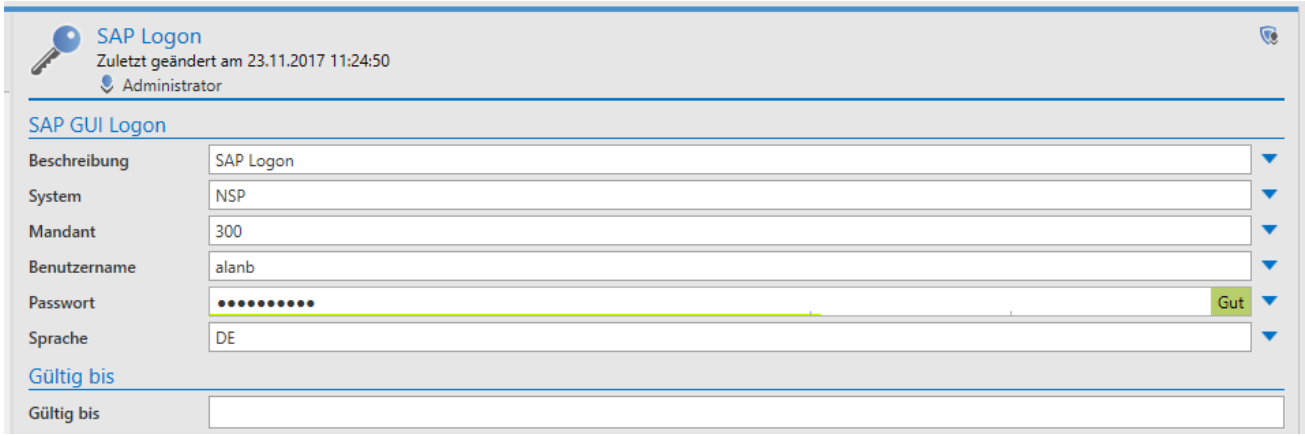
## Formular

Zunächst sollte ein Formular den benötigten Feldern erzeugt werden. Dies könnte wie folgt aussehen:



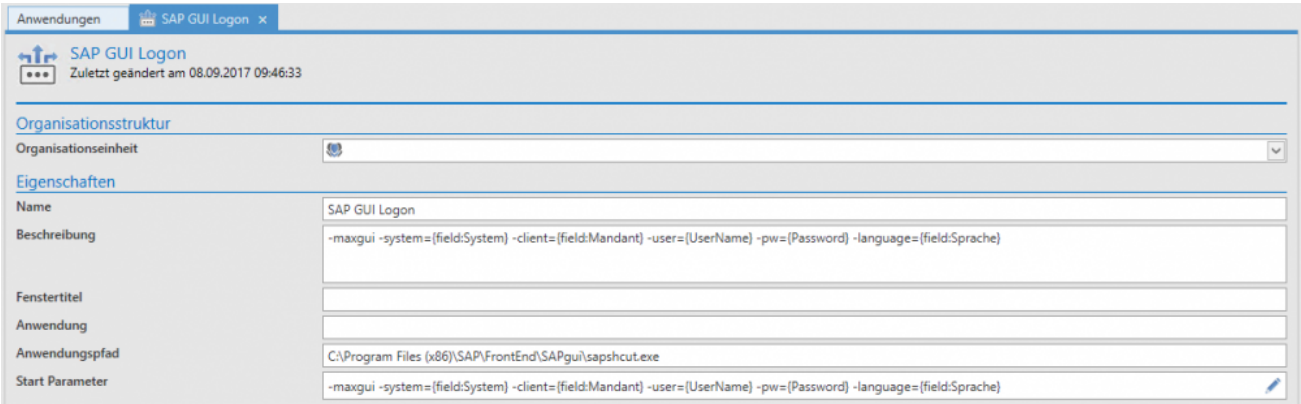

## Datensatz

Über das Formular wird dann ein entsprechender Datensatz erstellt:



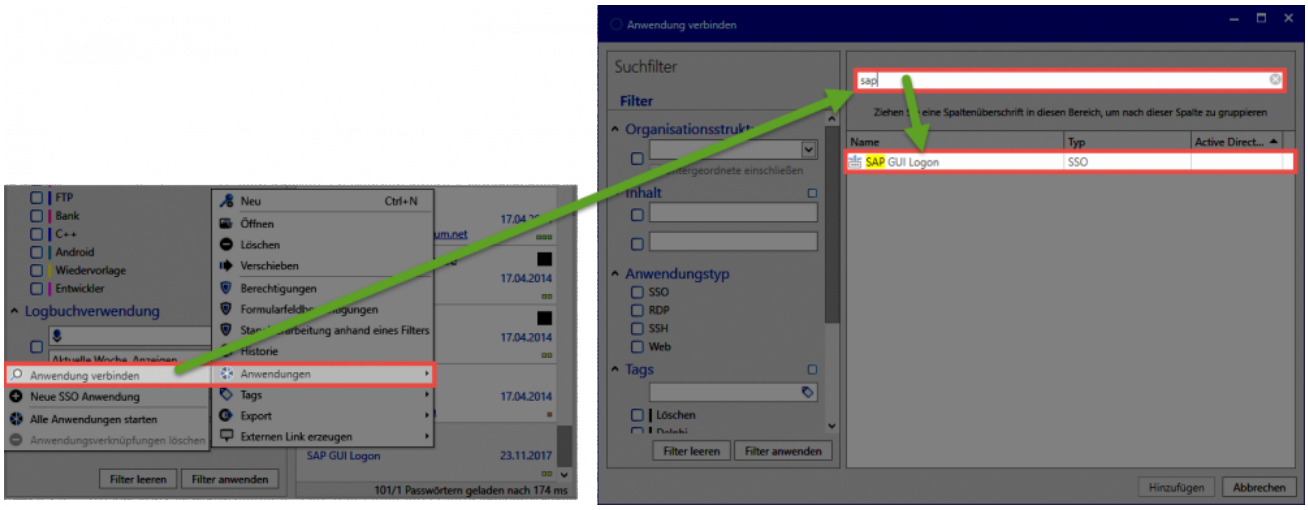

# Anwendung

Nun muss eine entsprechende SSO Anwendung erstellt werden.




# Verknüpfung

Der Datensatz muss nun mit der Anwendung verknüpft werden. Hierfür wird über einen Rechtsklick auf den Datensatz das Kontextmenü geöffnet. Darin kann dann über **Anwendungen** und **Anwendung verbinden** die zuvor erstellte Anwendung selektiert werden.

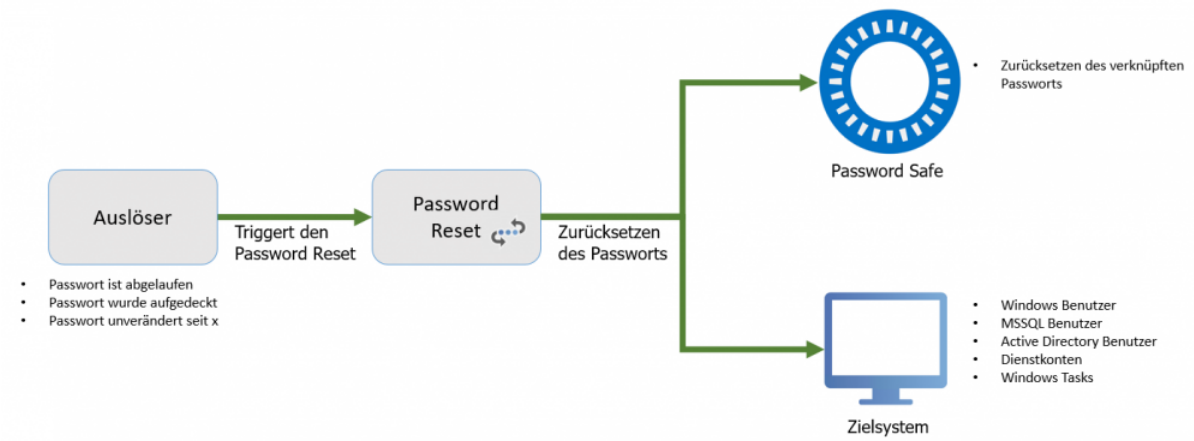



Die Verknüpfung wird schlussendlich in der Ribbon angezeigt. Durch einen Klick darauf wird nun SAP geöffnet wobei die Parameter zur Anmeldung direkt mit übergeben werden.

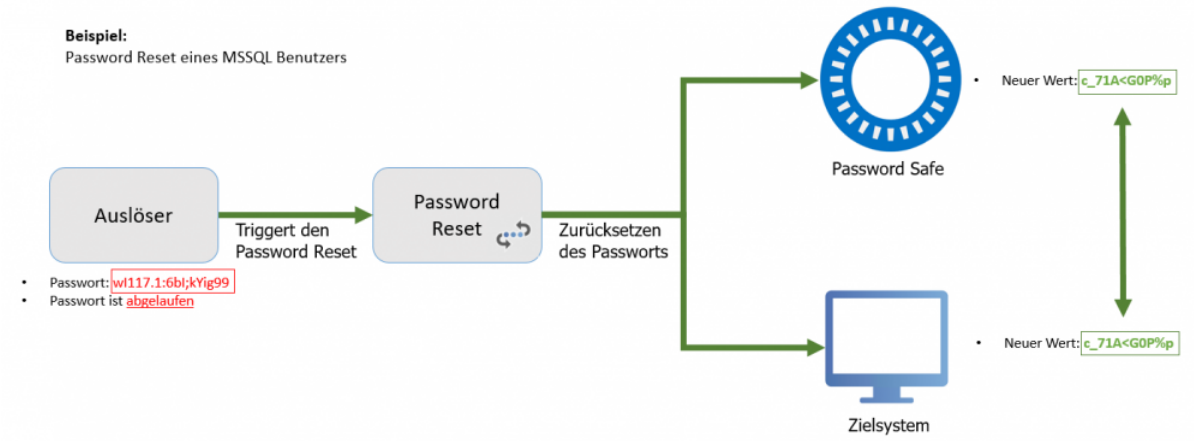
# Password Reset

## Was ist Password Reset?

Die sichersten Passwörter sind die, die man nicht kennt. Password Reset ermöglicht das Zurücksetzen von Passwörtern auf einen neuen und unbekannten Wert gemäß frei definierbarer Auslöser. Ein solcher Auslöser kann sowohl ein definierbares Intervall sein oder eine bestimmte Aktion des Benutzers. **Der Wert des Passwortes wird sowohl im Password Safe als auch im Zielsystem geändert**.




Dieser Vorgang soll anhand eines konkreten Beispiels nachfolgend erläutert werden. Das Passwort für den MSSQL Benutzer ist abgelaufen. Der Password Reset setzt somit sowohl im Password Safe als auch im Zielsystem das Passwort auf einen neuen Wert.




! Password Reset ist ausschließlich Teil der **Enterprise Plus Edition**

! Es wird dringend empfohlen, dass Password Reset **in Zusammenarbeit mit zertifizierten Partnern** konfiguriert wird. Die angestrebte Arbeitserleichterung durch die Nutzung genannter Automatismen geht einher mit einer Vielzahl von Risiken.

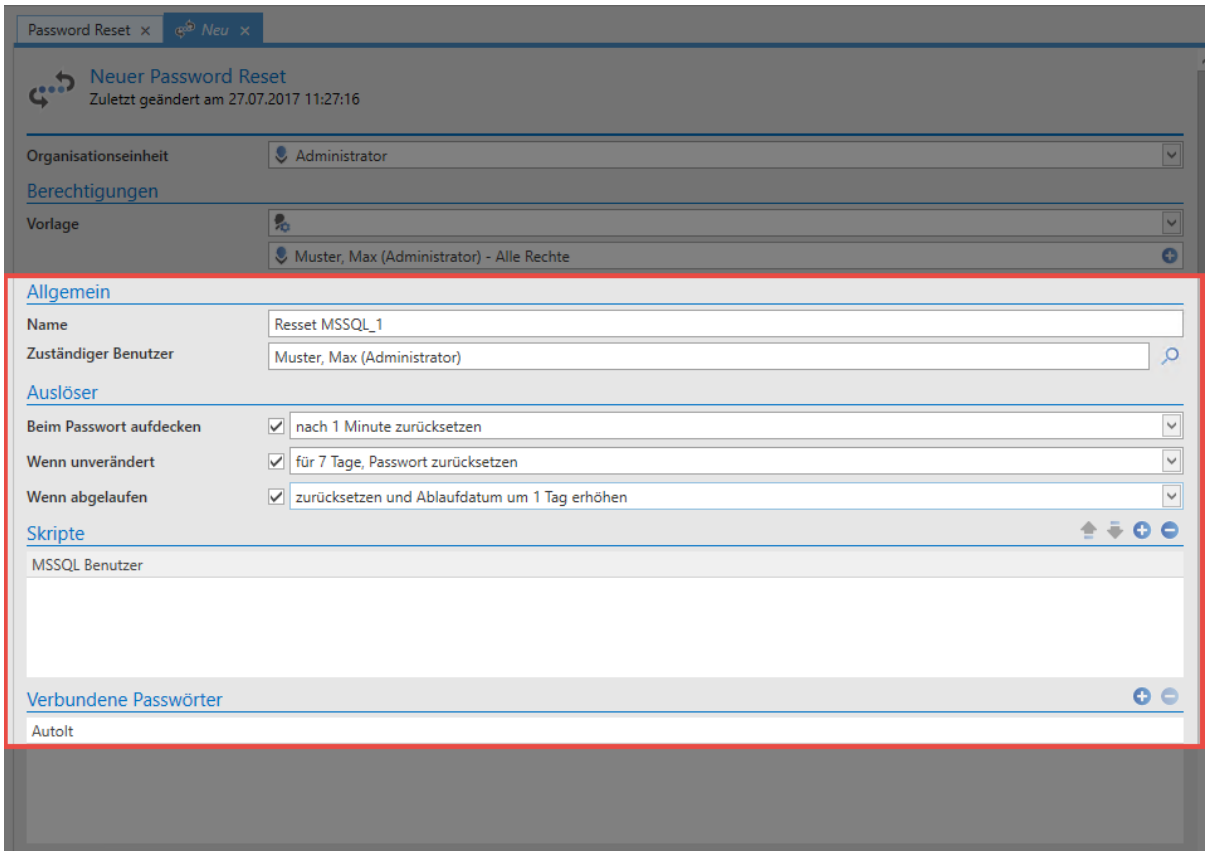
# Erstellung eines Password Reset

Es werden die Benutzerrechte “Password Reset Modul anzeigen” sowie “Kann neue Password Resets anlegen” benötigt.

Über die Ribbon sowie über das Tastenkürzel “Strg + N” können im Modul Password Reset direkt neue Password Resets angelegt werden. In Bezug auf Berechtigungen verhält sich ein Password Reset exakt wie jedes andere Objekt auch. Es kann gezielt gesteuert werden, welcher Benutzer welches Password Reset sehen und nutzen kann.

# Konfiguration

Die Konfiguration eines neuen Password Resets besteht aus vier Schritten. In den Bereichen “Allgemein”, “Auslöser”, “Skripte” sowie “Verbundene Passwörter” werden alle für die Konfiguration notwendigen Bedingungen und Variablen definiert.



### Allgemein

- **Name**: Bezeichnung für den Password Reset
- **Zuständiger Benutzer**: Alle durchgeführten Password Resets werden innerhalb des Password Safe auch festgehalten (Logbuch,…). Damit diese Schritte einem Benutzer zugewiesen werden können, wird unter “zuständiger Benutzer” ein im Password Safe erfasster Benutzer ausgewählt.

### Auslöser

Auslöser beschreiben die Umstände die erfüllt sein müssen, damit ein Password Reset ausgeführt wird. Es stehen insgesamt drei mögliche Auslöser zur Verfügung:

- Zurücksetzen des Passworts x Minuten, nachdem das Passwort eingesehen wurde
- Zurücksetzen des Passworts, wenn dies seit x Tagen nicht verändert wurde
- Zurücksetzen des Passworts, wenn es seit x Tagen abgelaufen ist

Es muss mindestens ein Auslöser aktiviert sein, damit der Password Reset aktiv ist. Das Deaktivieren aller Auslöser entspricht der Inaktivität des Password Reset. Es können alle drei Auslöser unabhängig voneinander ein- und ausgeschalten werden. Aus einer der drei Kategorien kann jeweils nur eine Auswahl getroffen werden.

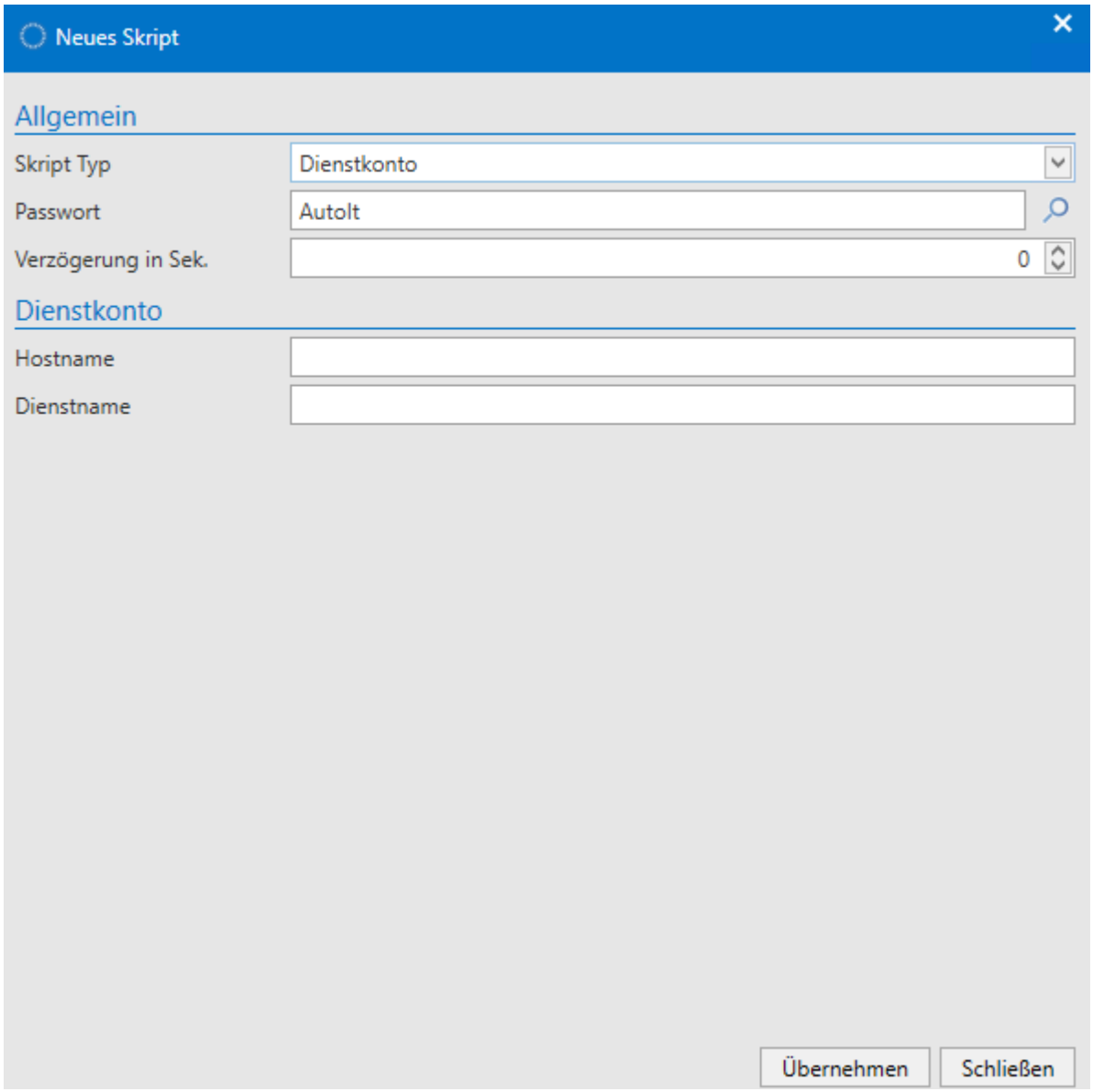
> Innerhalb des Password Safe prüf minütlich ein separater System Task, ob ein Auslöser zutrifft.

### Skripte

Aktuell können die nachfolgenden Systeme automatisch zurückgesetzt werden (Skripttypen).

- Windows Benutzer
- MSSQL Benutzer
- Active Directory Benutzer
- Dienstkonten
- Windows Tasks

Nach der Auswahl erscheint ein neuer Dialog, bei dem die Auswahl über den Typ des “zu resettenden” Systems getroffen wird.



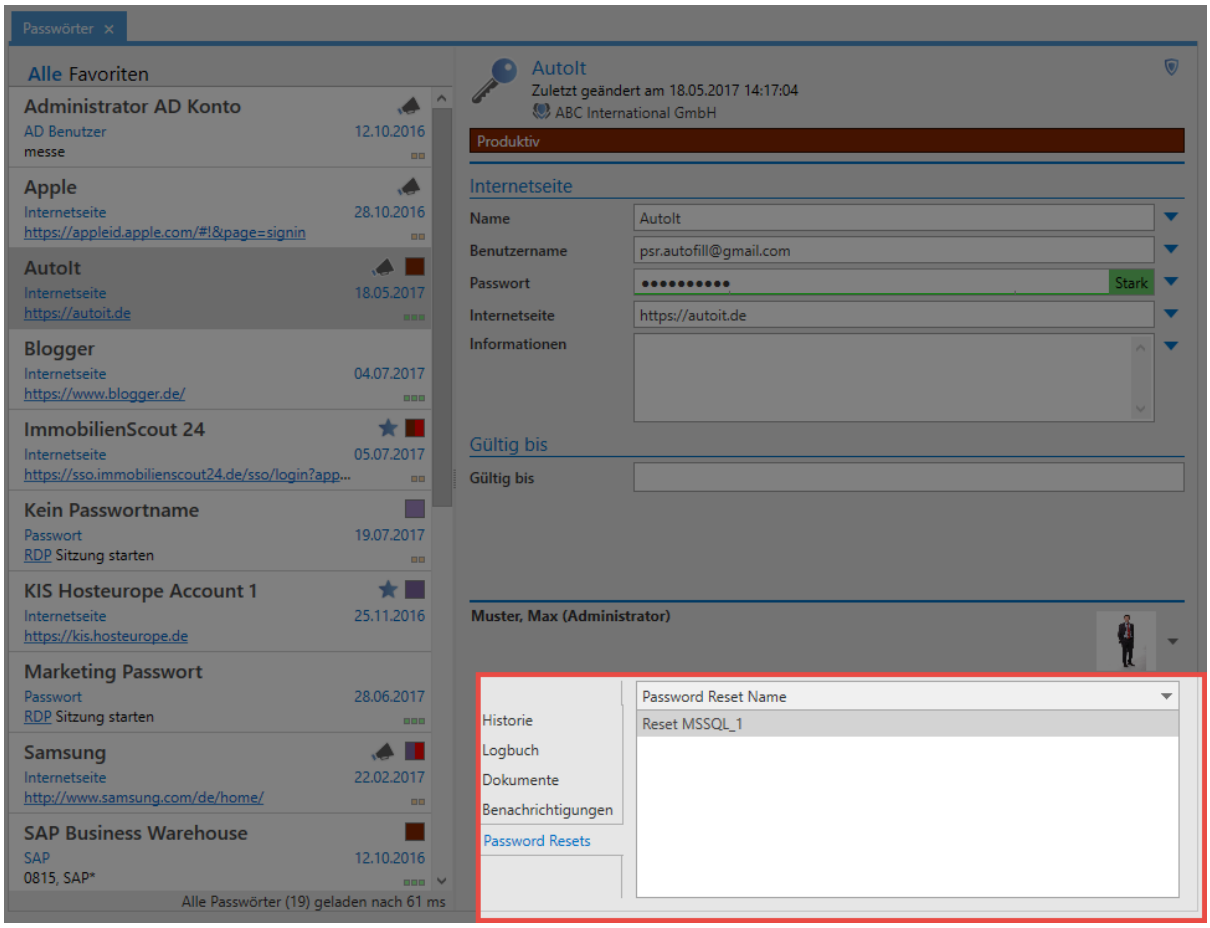

- **Skript Typ**: Es wird unter den möglichen Skripttypen ausgewählt.
- **Passwort**: Es werden die Credentials desjenigen Datensatzes angegeben, der den Password Reset auch schlussendlich durchführen wird.

Es werden spezifisch die benötigten Informationen abgefragt. Ist der Reset eines MSSQL Benutzers angedacht, benötigt man z.B. die Angabe der MSSQL Instanz sowie den genutzten Port.

> Es ist auch möglich einen Password Reset ohne ein zugehöriges Skript zu erstellen. In diesem Fall wird das Passwort der verbundenen Datensätze (s. Folgepunkt) lediglich im Password Safe geändert, jedoch nicht in einem Zielsystem.

## Verbundene Passwörter

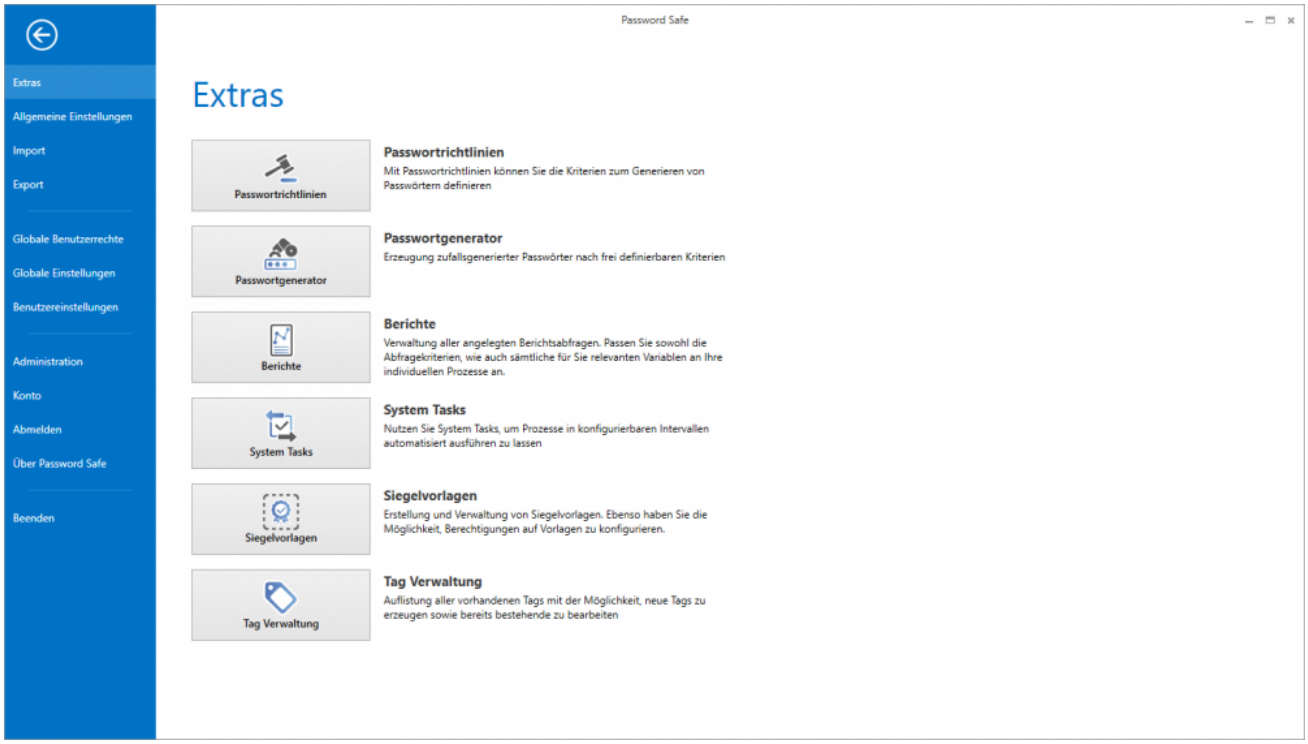
Unter “verbundene Passwörter” werden alle Datensätze aufgelistet, welche mit dem Password Reset gemäß der gewählten Auslöser resettet werden sollen. Eine Angebe mehrerer Objekte ist möglich. Auch im Footer des Lesebereichs ist das verknüpfte Password Reset nach einer erfolgreichen Konfiguration einsehbar.



# Hauptmenü

## Was ist das Hauptmenü/Backstage?

Alle Einstellungen, welche nicht an ein bestimmtes Modul gebunden sind, werden im Backstage definiert. Dadurch sind die Einstellungen jederzeit und in jedem Modul komfortabel erreichbar.



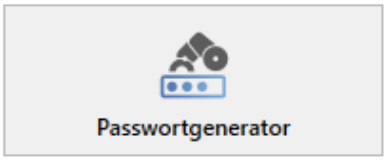

- Extras
- Allgemeine Einstellungen
- Import
- Export
- Benutzerrechte
- Benutzereinstellungen
- Administration
- Konto

# Extras

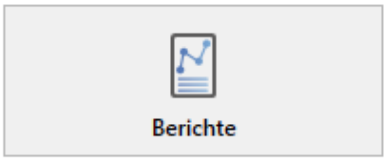
## Was sind Extras?

Password Safe liefert diverse unterstützende Features, welche nicht direkt Mehrwerte bieten, sondern meistens auf bestehenden Ansätzen aufbauen und diese funktional erweitern. Es geht um Arbeitserleichterungen, welche in der Summe das Arbeiten mit dem Password Safe erleichtern.

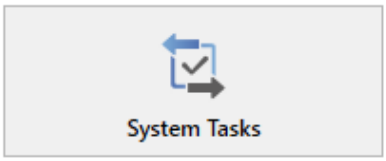

**Passwortrichtlinien**
Mit Passwortrichtlinien können Sie die Kriterien zum Generieren von Passwörtern definieren



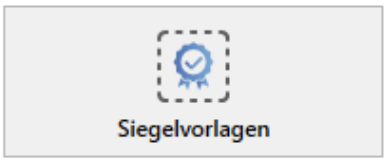

**Passwortgenerator**
Erzeugung zufallsgenerierter Passwörter nach frei definierbaren Kriterien



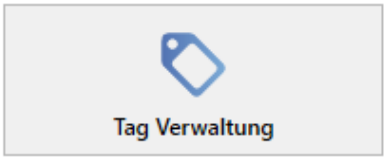

**Berichte**
Verwaltung aller angelegten Berichtsabfragen. Passen Sie sowohl die Abfragekriterien, wie auch sämtliche für Sie relevanten Variablen an Ihre individuellen Prozesse an.




**System Tasks**
Nutzen Sie System Tasks, um Prozesse in konfigurierbaren Intervallen automatisiert ausführen zu lassen




**Siegelvorlagen**
Erstellung und Verwaltung von Siegelvorlagen. Ebenso haben Sie die Möglichkeit, Berechtigungen auf Vorlagen zu konfigurieren.



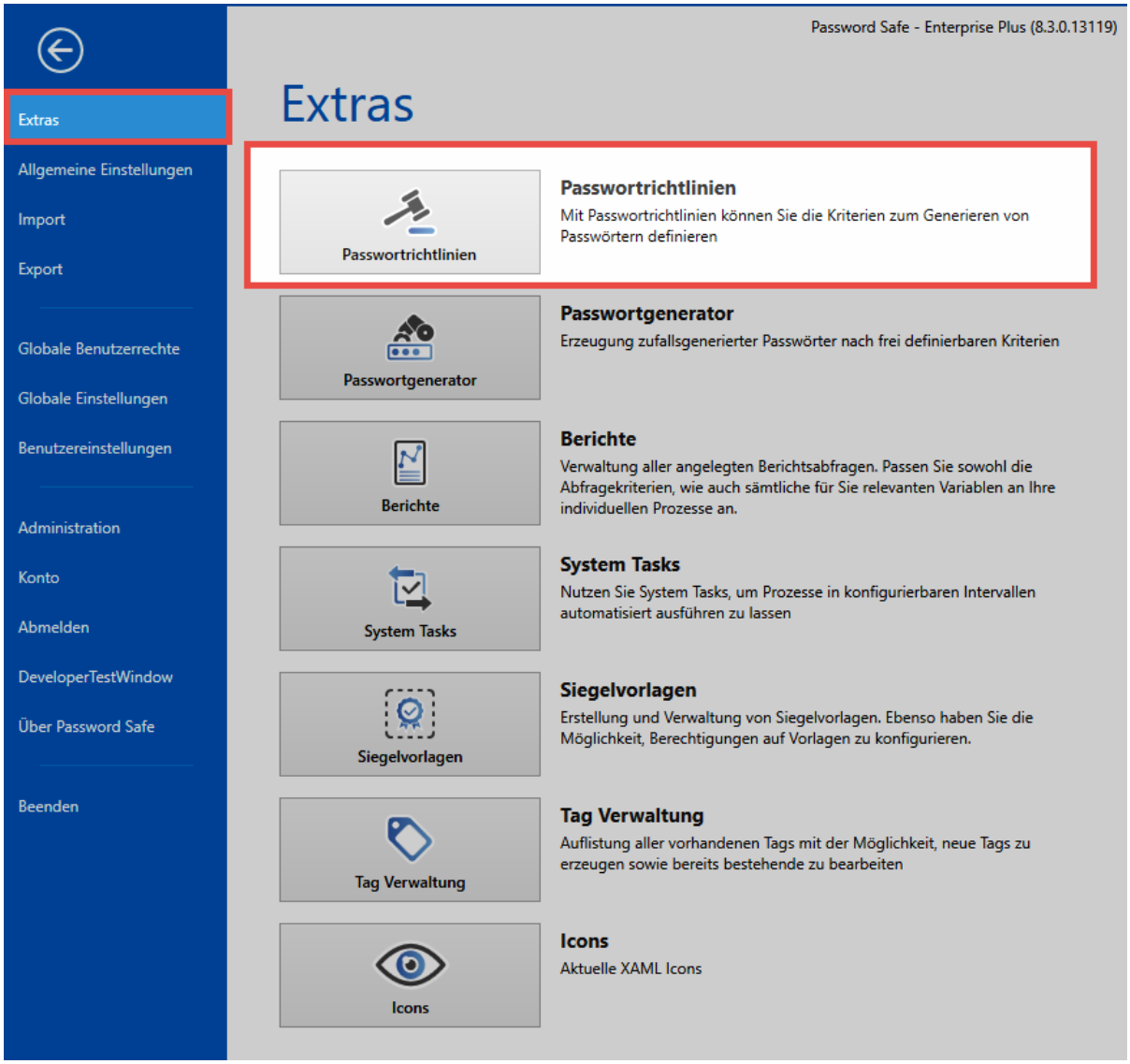

**Tag Verwaltung**
Auflistung aller vorhandenen Tags mit der Möglichkeit, neue Tags zu erzeugen sowie bereits bestehende zu bearbeiten

- Passwortrichtlinien
- Passwortgenerator
- Berichte
- System Tasks
- Siegelvorlagen
- Tagverwaltung

# Passwortrichtlinien

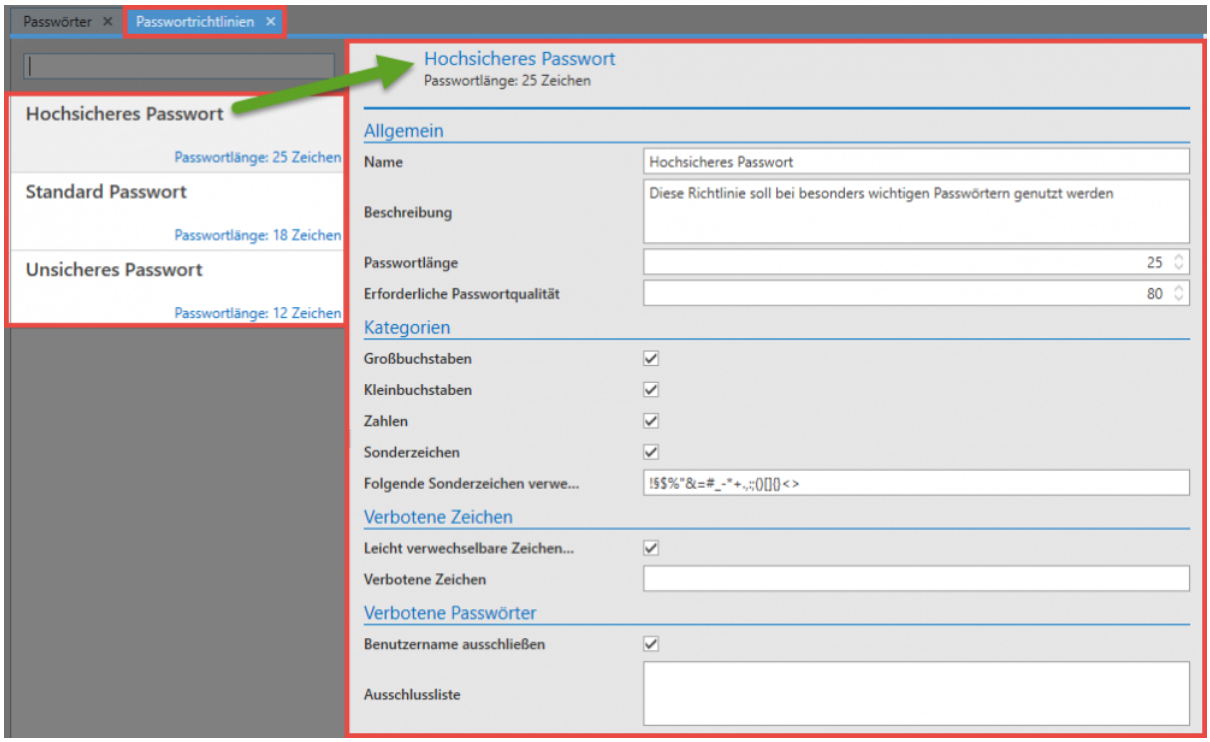
## Was sind Passwortrichtlinien?

Es wird generell empfohlen, dass Passwörter aus mindestens 12 unterschiedlichen Zeichen bestehen, komplex sind und automatisiert erstellt werden. Richtlinien stellen Vorgaben dar, an welche man Benutzer binden kann – man erzwingt sozusagen den Einsatz von Passwörtern einer bestimmten Komplexität. Vorhandene Richtlinien können auch in anderen Bereichen wiederverwendet werden.




## Verwaltung von Passwortrichtlinien

Wählt man unter Hauptmenü/Extras “Passwortrichtlinien” aus, erscheinen die verfügbaren Passwortrichtlinien in einem separaten Tab im derzeit aktiven Modul.




Im vorliegenden Schaubild sind insgesamt 3 Passwortrichtlinien dargestellt. Da in der Listenansicht die Richtlinie “Hochsicheres Passwort” ausgewählt wird, ist im Lesebereich zur rechten dementsprechend die Konfiguration dieser Richtlinie einsehbar:

- **Allgemein**: Die **Passwortlänge** von 25 gibt die minimale Anzahl von Zeichen an, welche ein Passwort gemäß der vorliegenden Richtlinie erfüllen muss. Die erforderliche **Passwortqualität** ist ein internes Maß an Sicherheit, welche für diese Richtlinie errechnet wurde. Dieser Wert liegt immer zwischen 1 (sehr unsicher) und 100 (maximale Sicherheit).
- **Kategorien**: Es gibt insgesamt vier Kategorien, aus denen ein Passwort bestehen kann. Es kann sowohl definiert werden, welche dieser Kategorien genutzt werden sollen als auch wie viele davon.
- **Verbotene Zeichen**: Auch das Ausschließen von manchen Sonderzeichen ist möglich. Diese müssen dann ohne Trennzeichen in der Liste eingetragen werden.
- **Verbotene Passwörter**: Bestimmte Passwörter sowie der Benutzername können ebenso auf die Liste der verbotenen Passwörter geführt werden
- **Richtlinienvorschau**: Bei der Erstellung von neuen Richtlinien wird gemäß der getätigten Konfiguration ein Passwortbeispiel generiert. Dies ist nur der Fall bei Passwörtern mit einer Mindestlänge von 3 Zeichen!

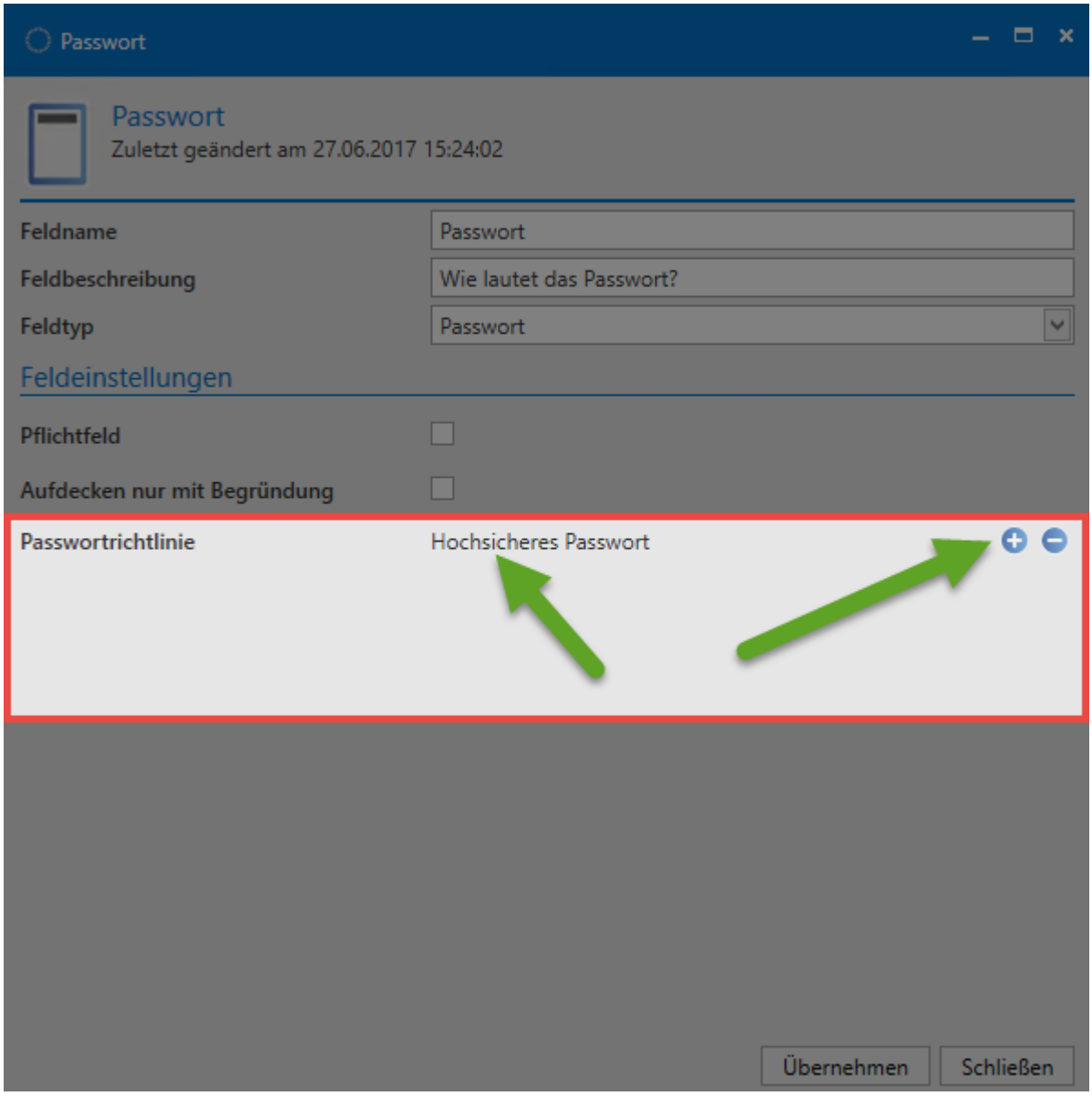
# Einsatz von Passwortrichtlinien

Einmal definierte Richtlinien können auf zwei verschiedene Art und Weisen produktiv genutzt werden:

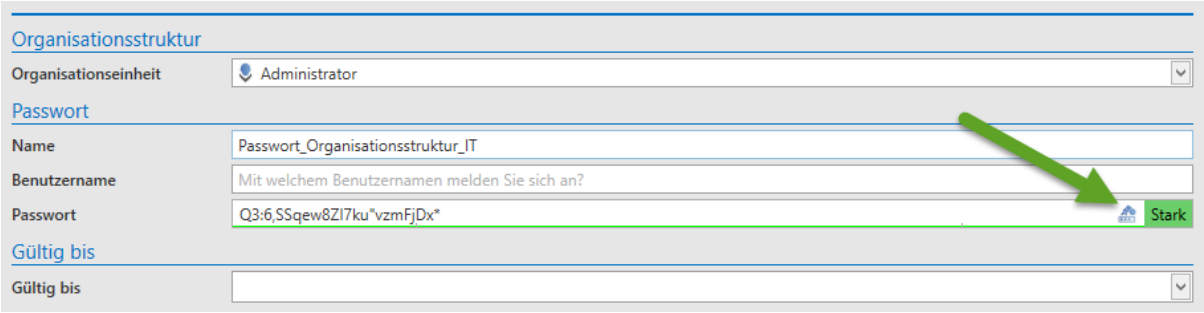
- Nutzung innerhalb des Passwortgenerators

- Vorgabe im Passwortfeld eines Formulars:

Definiert man in Formularen ein Passwortfeld, kann eine der definierten Passwortrichtlinien als Vorgabe gesetzt werden. Dies hat zur Folge, dass bei der Erstellung eines neuen Passwortes stets diese Vorlage genutzt wird. Auf diese Art und Weise stellt man sicher, dass für bestimmte Passwörter stets die geforderte Komplexität erreicht wird.




Ist auf einem Formular nun eine solche Richtlinie definiert, kann man bei der Erstellung eines neuen Passwortes lediglich einen neuen Zufallswert für das Passwort definieren. Hierzu nutzt man das Icon am rechten Ende des Passwortfeldes.




# Standardrichtlinie für Benutzerpasswörter definieren

Falls nicht der Master Key Modus genutzt wird, können Benutzer im Password Safe ihre Passwörter ändern. Welche Passwortstärke genutzt werden soll, kann durch den Einsatz von Standard-Passwortrichtlinien durch die Administration festgelegt werden. Mehr…

# Sichtbarkeit

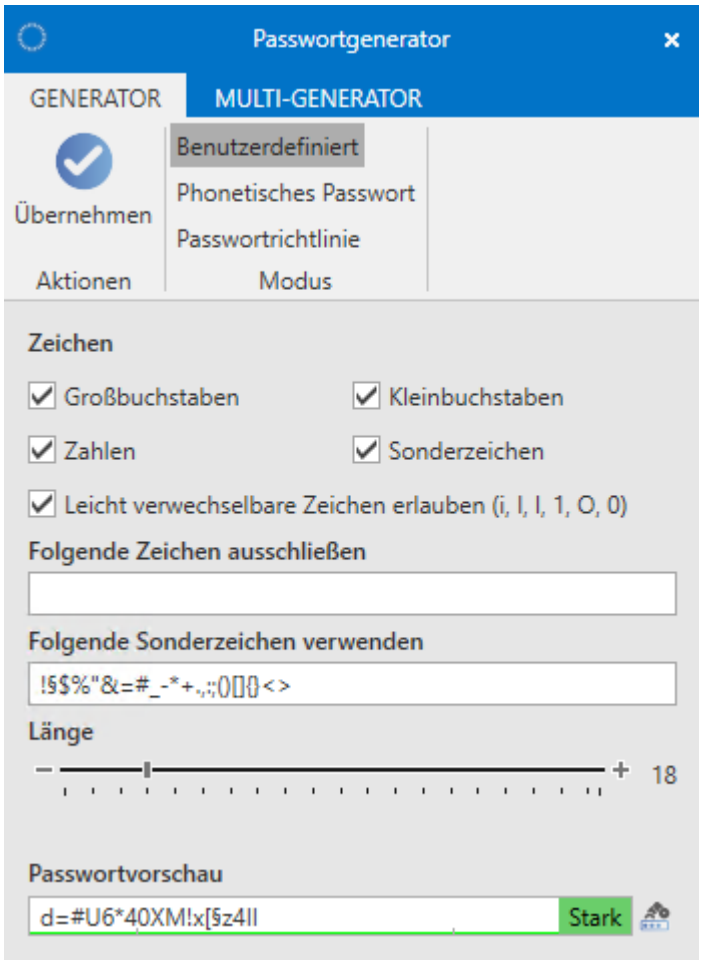
Passwortrichtlinien selbst unterliegen keinerlei Berechtigungen. Alle erstellten Richtlinien stehen somit allen Benutzern zur Verfügung. Die Richtlinien werden über das Hauptmenü verwaltet.

> Die Verwaltung der Richtlinien ist nur möglich, wenn der Benutzer das entsprechende Benutzerrecht besitzt

# Passwortgenerator

## Was ist der Passwortgenerator?

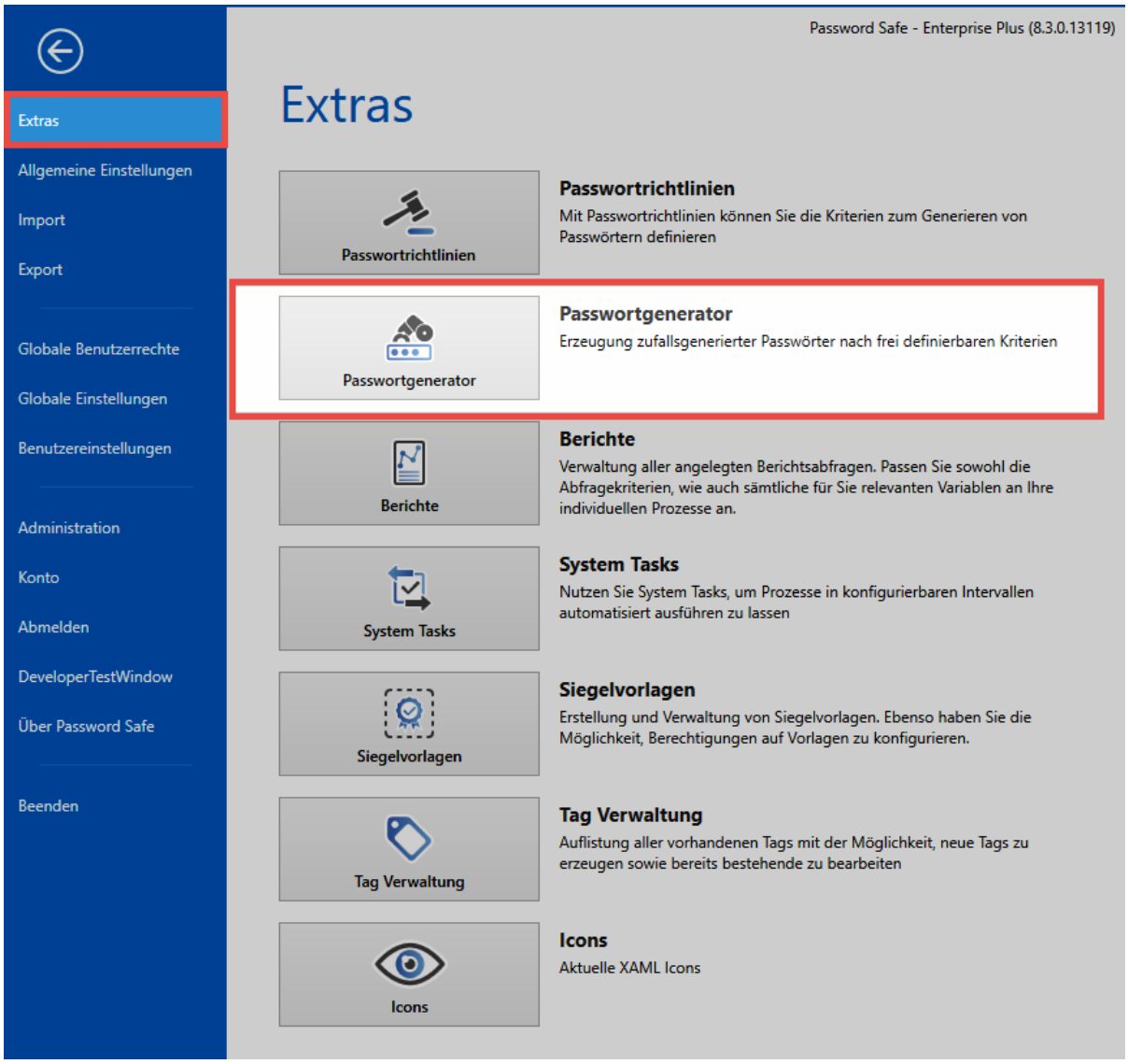
Die Komplexität von Passwörtern wird grundsätzlich durch deren Zufälligkeit bestimmt. Um zu 100% auf rein zufällig erstellte Passwörter zugreifen zu können, ist ein Algorithmus zum Erstellen von Passwörtern unerlässlich. Der Passwortgenerator liefert dies und ist komplett in die Software eingebunden.




## Öffnen des Passwortgenerators

Der Passwortgenerator kann auf verschiedenen Wegen geöffnet werden:

- **Hauptmenü/Extras/Passwortgenerator**: Hierbei wird der Passwortgenerator direkt aufgerufen. Dort kreierte Passwörter können in die Zwischenablage kopiert werden.



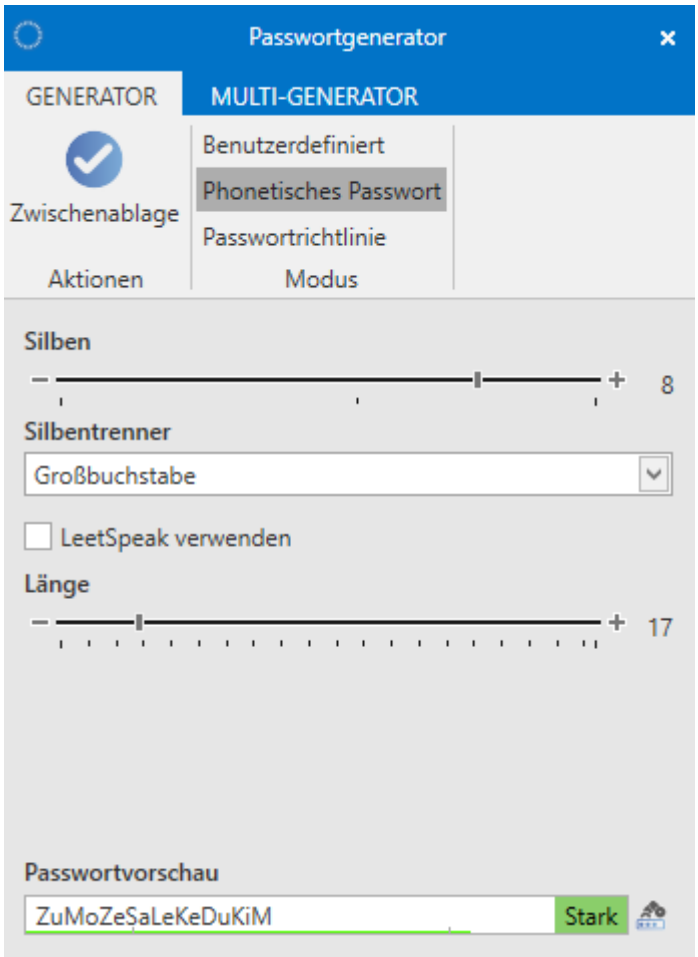

- **Beim Erstellen neuer Datensätze**: Hierbei markiert man das Passwortfeld im Lesebereich und kann dann in der Ribbon im Reiter “Formularfeld” den Passwortgenerator direkt öffnen. Dort erstelle Passwörter werden über den Button “Übernehmen” direkt in das Passwortfeld des neuen Datensatzes eingetragen. Alternativ: Rechts im Passwortfeld im Lesebereich kann der Generator ebenso aufgerufen werden.

# Funktionsweise

Unter **Zeichen** definiert man die Zeichengruppen, welche Teil des Passwortes sein sollen. Analog können auf diese Art und Weise auch (Sonder)Zeichen ausgeschlossen werden. Nachdem die Passwortlänge bestimmt wurde, existiert am unteren Rand des Passwortgenerators eine Vorschau auf ein den konfigurierten Kriterien entsprechendes Passwort. Rechts neben der Passwortvorschau lässt sich über das Icon die “Shuffle-Funktion” aktivieren, welche gemäß den definierten Kriterien ein neues Passwort kreiert.

### Phonetische Passwörter

Diese Form von Passwörtern zeichnet sich dadurch aus, dass man Sie sich verhältnismäßig gut merken kann (sie sind “lesbar”) und dennoch keinen Bezug zu Begriffen aus Wörterbüchern besitzen. Definiert werden hier nur die Anzahl der Silben sowie die Gesamtlänge. Optional kann noch für die Form der Silbentrennung sowie LeetSpeak verwendet werden.




### Passwortrichtlinie

Bereits definierte Passwortrichtlinien können für das automatische Erzeugen neuer Passwörter herangezogen werden

## Multi-Generator

Der Multigenerator ermöglicht das automatische Erstellen von bis zu 200 Passwörtern. Die Konvention, nach der diese Passwörter erzeugt werden, entspricht stets den vorher definierten Vorgaben. Diese können sein

- Benutzerdefiniert
- Phonetische Passwörter

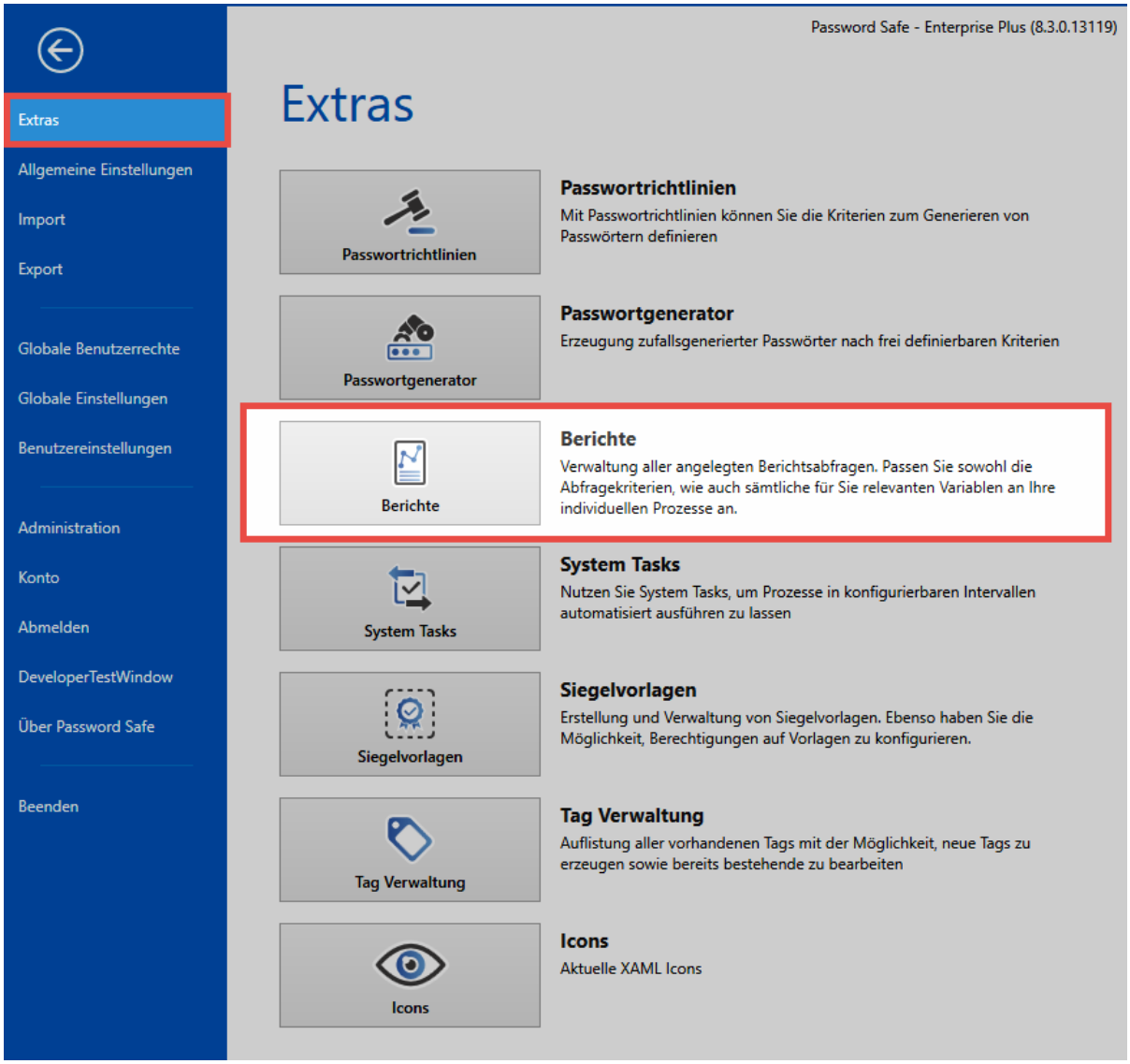
- Passwortrichtlinien

Die erzeugten Passwörter werden im lokalen Benutzerverzeichnis in einer Textdatei gespeichert und können auf Wunsch sofort geöffnet werden.

# Berichte

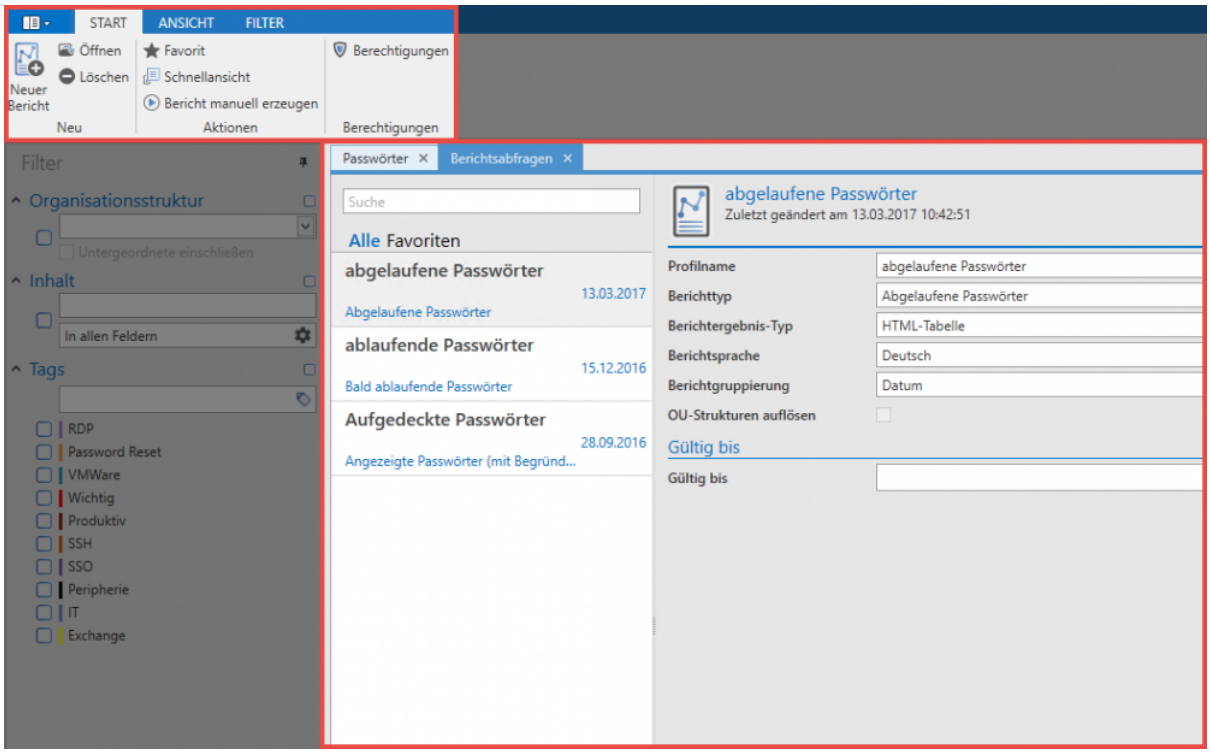
## Was sind Berichte?

Ausführliches Berichtswesen ist ein wichtiger Bestandteil der fortwährenden Überwachung von Abläufen im Password Safe. Ähnlich den punktuell konfigurierbaren Benachrichtigungen enthalten auch Berichte Informationen, welche man selektiv definieren kann. Der Unterschied besteht hauptsächlich im Auslöser. Benachrichtigungen sind an ein Event gekoppelt, welches den Auslöser einer Benachrichtigung darstellt. Im Gegensatz hierzu ermöglichen Berichte die tabellarische Auflistung frei definierbarer Aktionen zu einem selbst wählbaren Zeitpunkt – der Auslöser ist demnach das Erstellen eines Berichtes. Dieser Vorgang kann weiterhin über System Tasks automatisiert werden.



Berichte enthalten stets nur diejenigen Informationen, auf die man auch berechtigt ist.

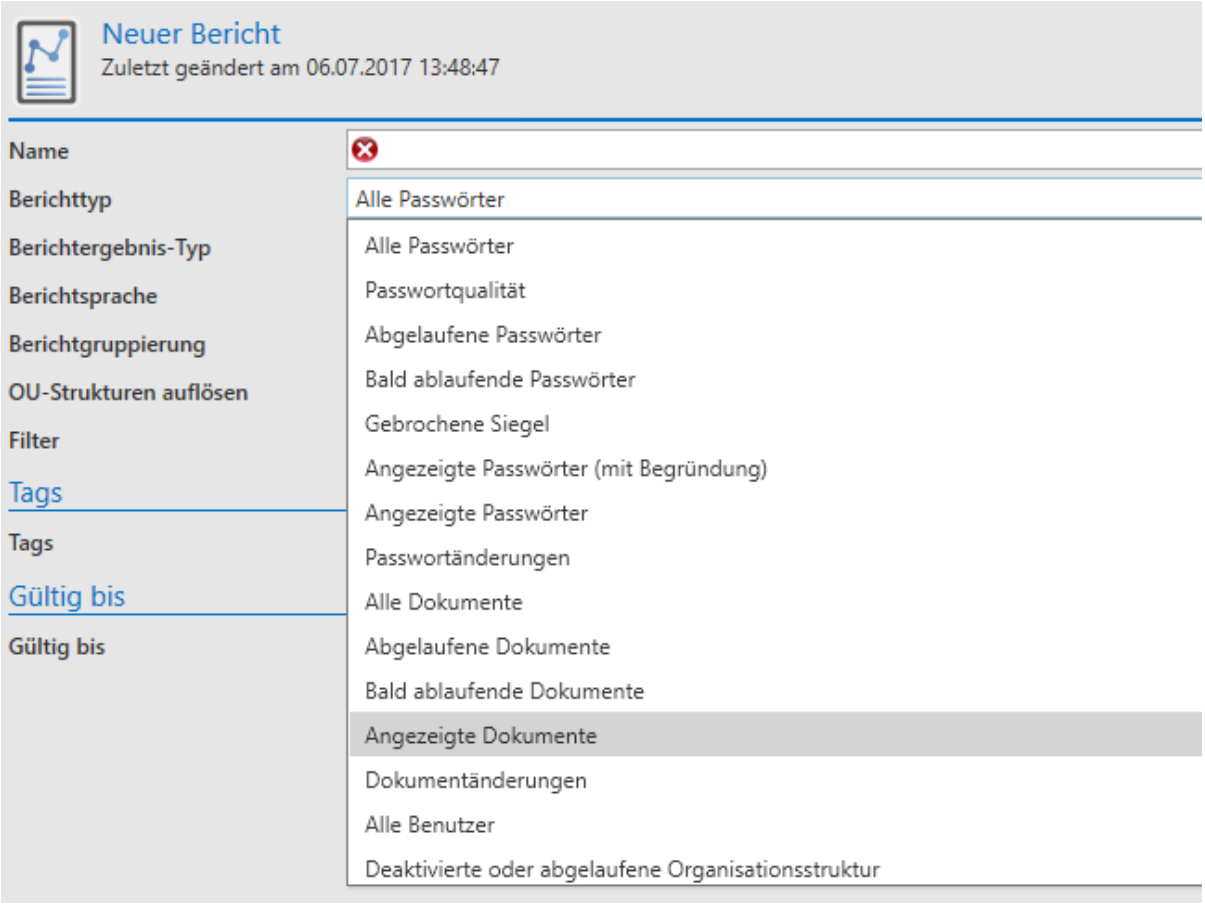
Über Hauptmenü/Extras/Berichte öffnet sich im aktuellen Modul ein separates Tab zum Verwalten bestehender und Erstellen neuer Berichte. Es ist irrelevant, in welchem Modul sich die Berichte öffnen, der Inhalt ist stets der gleiche.




Der Filter zur linken besitzt im Zuge der Berichte keinerlei Relevanz. Obwohl Berichte auch theoretisch “getagt” werden können, wirkt sich das Filtern nicht auf die Berichte aus. In der Listenansicht sind aktuell drei konfigurierte Berichtsabfragen gespeichert.

# Erstellen von Berichtsabfragen

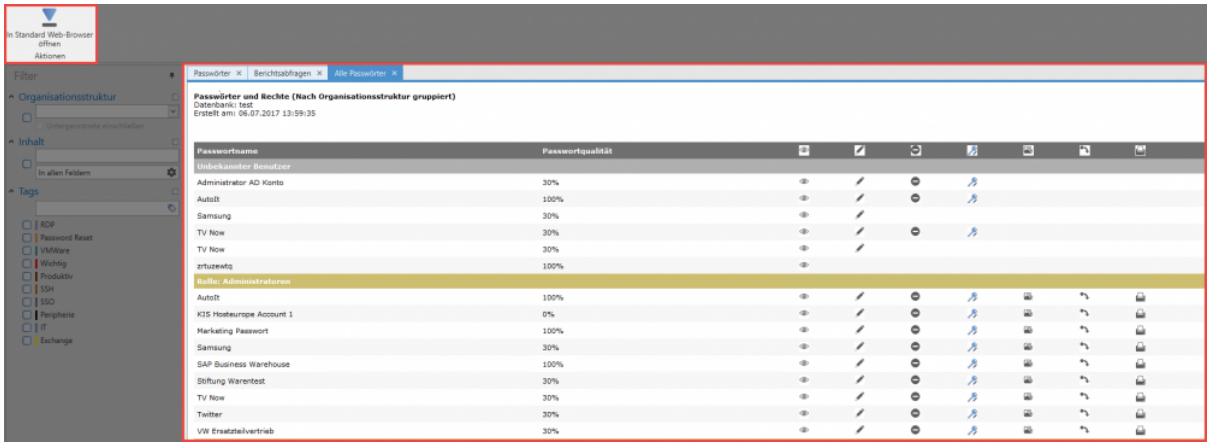
Über die Ribbon wie auch über das Kontextmenü der rechten Maustaste können in der Listenansicht neue Berichtsabfragen erstellt werden. Es öffnet sich wieder in einem separaten Tab das Formular für das Erstellen einer neuen Berichtsabfrage. Neben diversen Variablen wird hier der Berichttyp per Dropdown-Liste festgelegt. Es existieren derzeit mehrere Dutzend Berichttypen.




Per Nutzung des Filters kann der Wirkungsbereich des Berichts beispielsweise auf eine bestimmte OU oder lediglich eine Auswahl an Tags festgelegt werden. Nach dem Speichern wird der Bericht nun in der Liste der Berichtsabfragen angezeigt.

# Berichte manuell erzeugen

Über die Ribbon kann nun ein manueller Bericht erzeugt werden. Dieser öffnet sich in einem separaten Tab und kann auf Wunsch im als Standard definierten Web-Browser dargestellt werden.



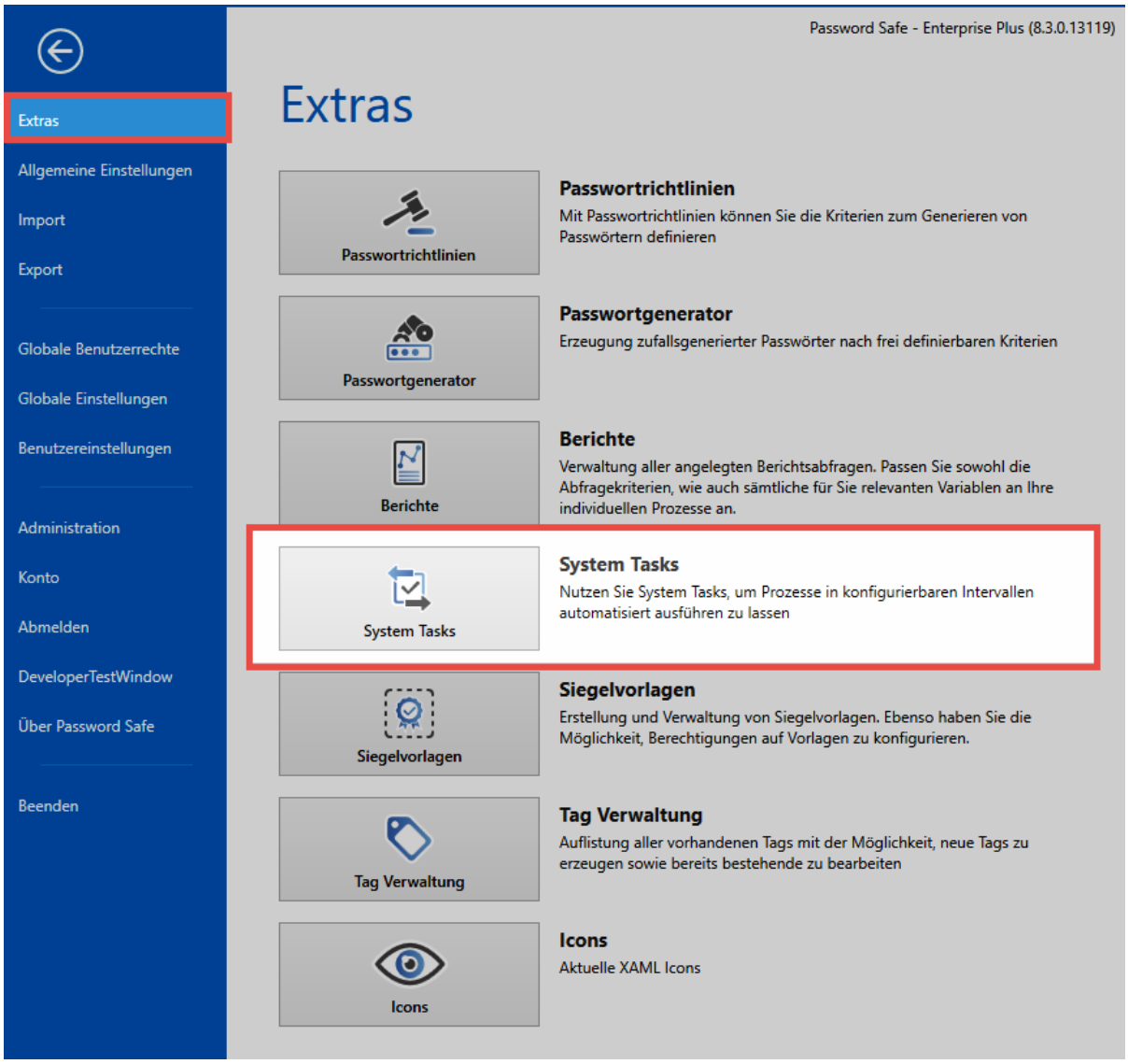
# Automatischer Versand über System Tasks

In der Regel werden Berichte nicht manuell erzeugt, sondern werden automatisch an definierbare Adressaten versandt. Dies wird im Zuge der System Tasks möglich, welche Vorgänge dieser Natur zeitgesteuert ablaufen lassen können. Mehr…

# System Tasks

## Was sind System Tasks?

Password Safe unterstützt Administratoren und Benutzer durch die Automatisierung wiederkehrender Aufgaben. Dies wird über System Tasks abgebildet. Vordefinierte Aufgaben können somit in frei definierbaren Intervallen automatisch durchgeführt werden.




## Was kann automatisiert werden?

Aktuell existieren vier verschiedene Arbeitsschritte, welche durch System Tasks automatisiert abgebildet werden können:

- **HTML-WebViewer Export**: Exportiert eine frei definierbare Auswahl an Datensätzen in eine mittels AES 256 verschlüsselte HTML-Datei. Die Datei wird in Form von Benachrichtigungen abgelegt.
- **Berichte**: Erstellt automatisiert einen Bericht, welcher in den Benachrichtigungen ausgegeben wird. Es muss zuvor eine Berichtsabfrage erstellt worden sein.
- **Netzwerk Dienst-Scan**: Sucht in definierbaren Zyklen nach Dienstkonten im Netzwerk
- **Active Directory Synchronisation**: Der Abgleich mit dem Active Directory kann ebenso über System Tasks automatisiert werden. Das Active Directory Profil muss zuvor erstellt werden. Es gilt zu Beachten, dass nur **Masterkey Profile** automatisch abgegelichen werden können.

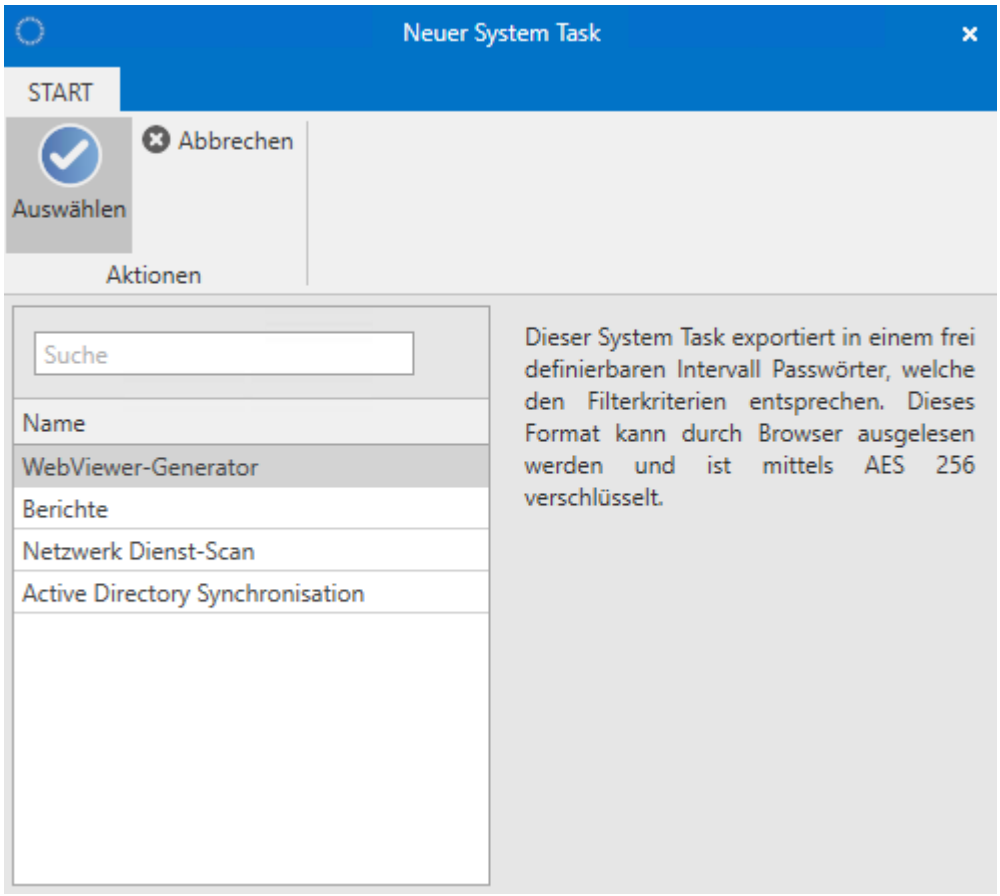
# Voraussetzungen

Es existiert für jeden der vier aufgeführten Anwendungsfälle ein separates Benutzerrecht:

| Kategorie: System Tasks |
| --- |
| Kann WebViewer Export System Tasks verwalten |
| Kann Reporting System Tasks verwalten |
| Kann DiscoverService System Tasks verwalten |
| Kann Active Directory System Tasks verwalten |

# Erstellen von System Tasks

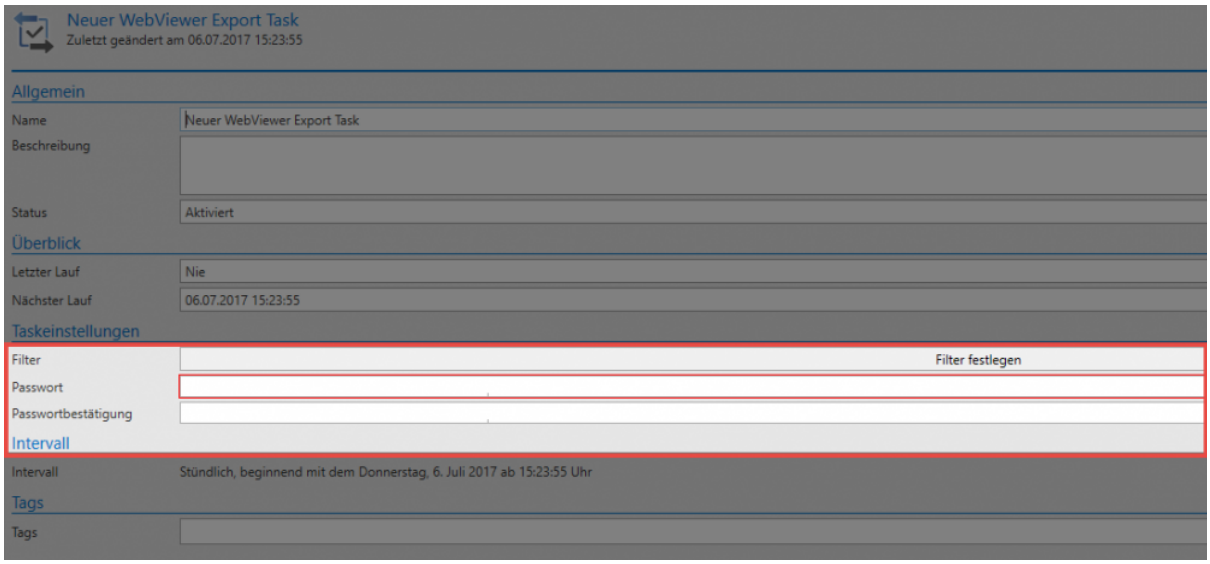
Wie gewohnt wird das Erstellen von System Tasks entweder über die Ribbon oder über das Kontextmenü der rechten Maustaste initiiert. Nachfolgend wird unter den vier genannten Arbeitsschritten derjenige ausgewählt, welchen man durch System Tasks automatisieren möchte.




Selbstverständlich besitzen die vier Arbeitsschritte auch Gemeinsamkeiten bei der Konfiguration.

- **Status**: Standardmäßig ist der System Task aktiviert und startet sofort nach dem Speichern gemäß dem definierten Intervall. Falls man den System Task hier deaktiviert, wird er zwar gespeichert, aber noch nicht aktiviert.
- **Nächster Lauf**: Hier wird beschrieben, wann der System Task das erste Mal anlaufen wird, bzw. bereits gelaufen ist (falls man diesen schon erstellt hat und nun bearbeitet)
- **Intervall**: Es wird definiert, in welchem Intervall der System Task ablaufen soll. Es sind alle Abstufungen zwischen minütlich und einmalig möglich. Ein Enddatum ist ebenso optional gegeben.

Nachfolgend sind die Unterschiede der vier zu automatisierenden Arbeitsschritte erläutert. Diese Unterschiede sind immer Teil der Taskeinstellungen innerhalb des System Task Formulars – hier gezeigt am Beispiel eines zu konfigurierenden HTML-WebViewer Exportes.




### HTML-WebViewer

- **Filter**: Es wird per Filter definiert, welche Passwörter exportiert werden sollen.
- **Passwort**: Der HTML-WebViewer erstellt eine verschlüsselte HTML Datei. Das Passwort wird hier definiert und muss bestätigt werden.

### Berichte

- **Berichtsabfrage**: Die unter Berichte definierten Berichtsabfragen stehen zur Auswahl und können ausgewählt werden.

### Dienst Scan

- **Dienst Scan Task**: Im Zuge von Password Reset wird das Passwort für den Dienst zugewiesen.

### Active Directory Synchronisierung

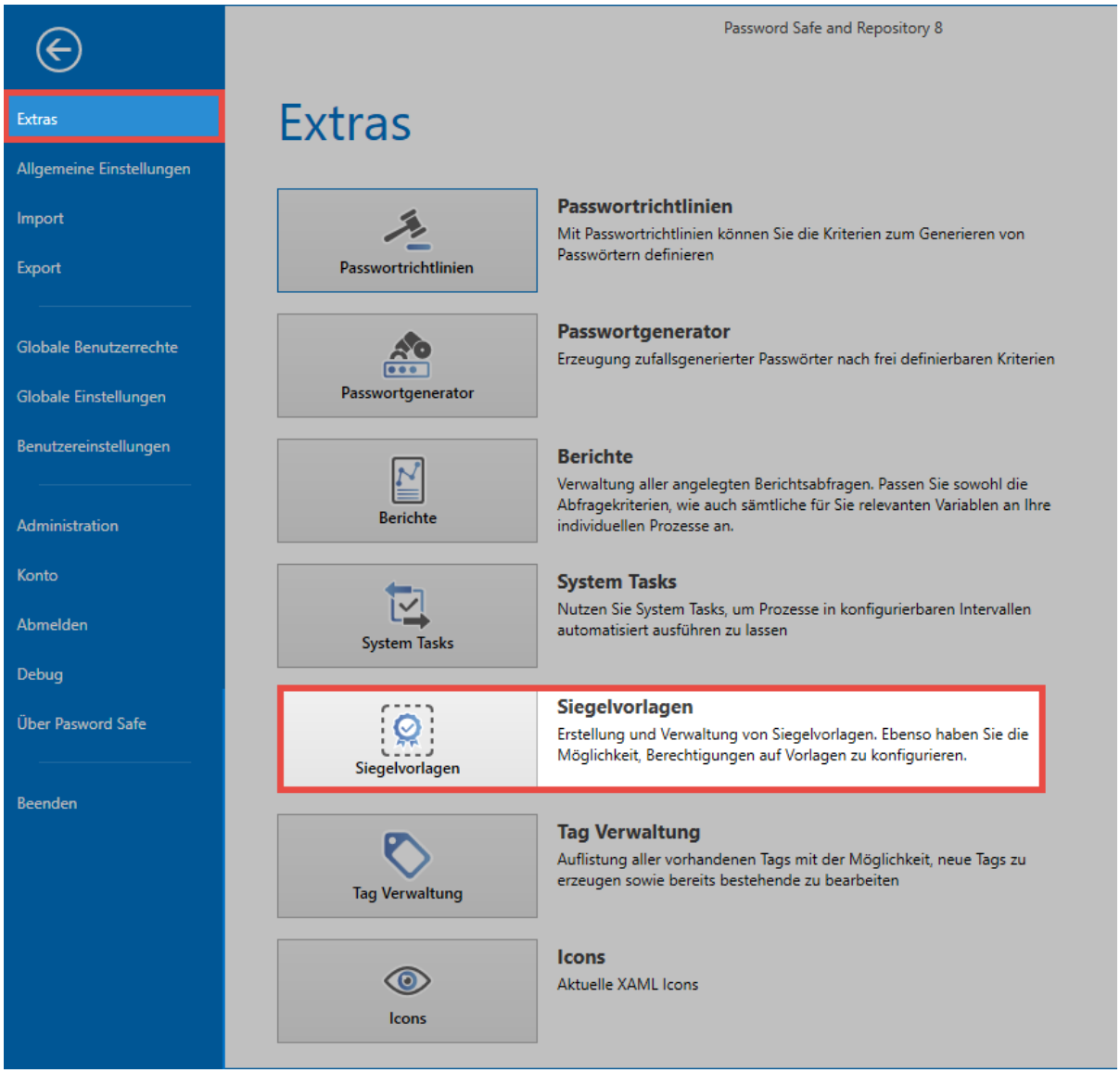
- *Das zur Synchronisierung nötige Active Directory Profil wird aus den vorhandenen ausgewählt.

> Tags könnten zwar für einzelne System Tasks definiert werden – Sie besitzen jedoch keinerlei Relevanz und können auch nicht als Filterkriterium in System Tasks genutzt werden.

# Siegelvorlagen

## Was sind Siegelvorlagen?

Die Konfiguration von Siegeln muss wohl durchdacht und fehlerfrei sein. Es bietet sich unbedingt an, den einmal investierten Aufwand in Form von Siegelvorlagen abzuspeichern. Die Automatisierung immer wiederkehrender Aufgaben wird in diesem Zusammenhang zeitliche Abläufe extrem beschleunigen. Einmal definiert können Vorlagen mit wenigen Handgriffen an Datensätzen angebracht werden. Auch die Anpassung bereits erstellter Schablonen gestaltet sich in den Siegelvorlagen als übersichtlich und sehr schnell zielführend.

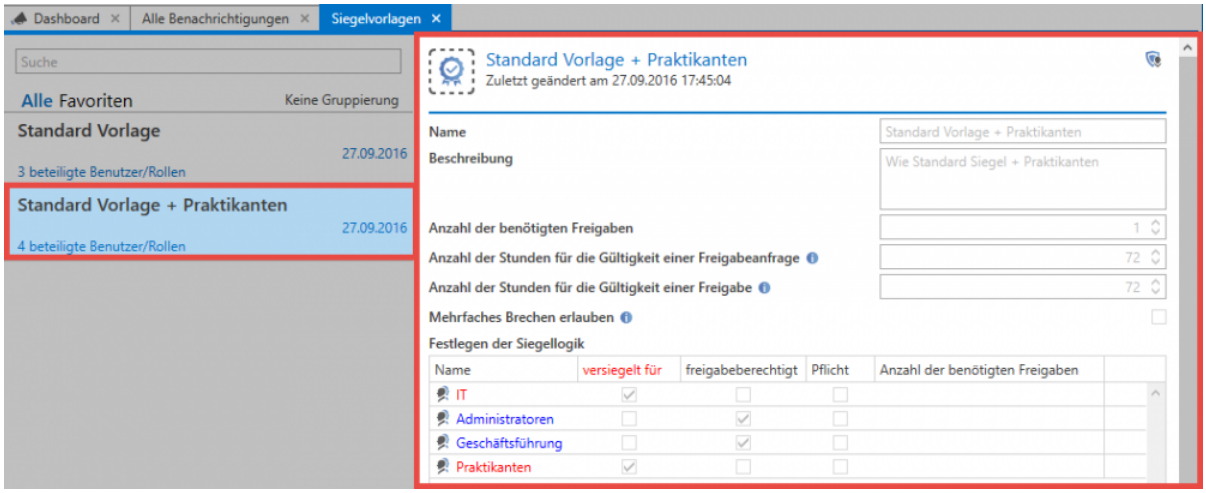


Die Bearbeitung der Standardvorlagen öffnet sich in einem eigenen Tab im aktiven Modul

# Erstellung von Vorlagen

Es wird das Recht **Kann Siegelvorlagen verwalten** benötigt

Bei der Erstellung von Siegeln kann über den Assistenten das Siegel als Vorlage gespeichert werden. Alle auf diese Art und Weise gespeicherten Vorlagen werden in der Übersicht der Siegelvorlagen aufgelistet. Weiterhin ist es hier möglich bestehende Vorlagen direkt zu bearbeiten oder Neue über den Button in der Ribbon zu erstellen. Dies geschieht analog zur Vorgehensweise im Siegelassistenten.

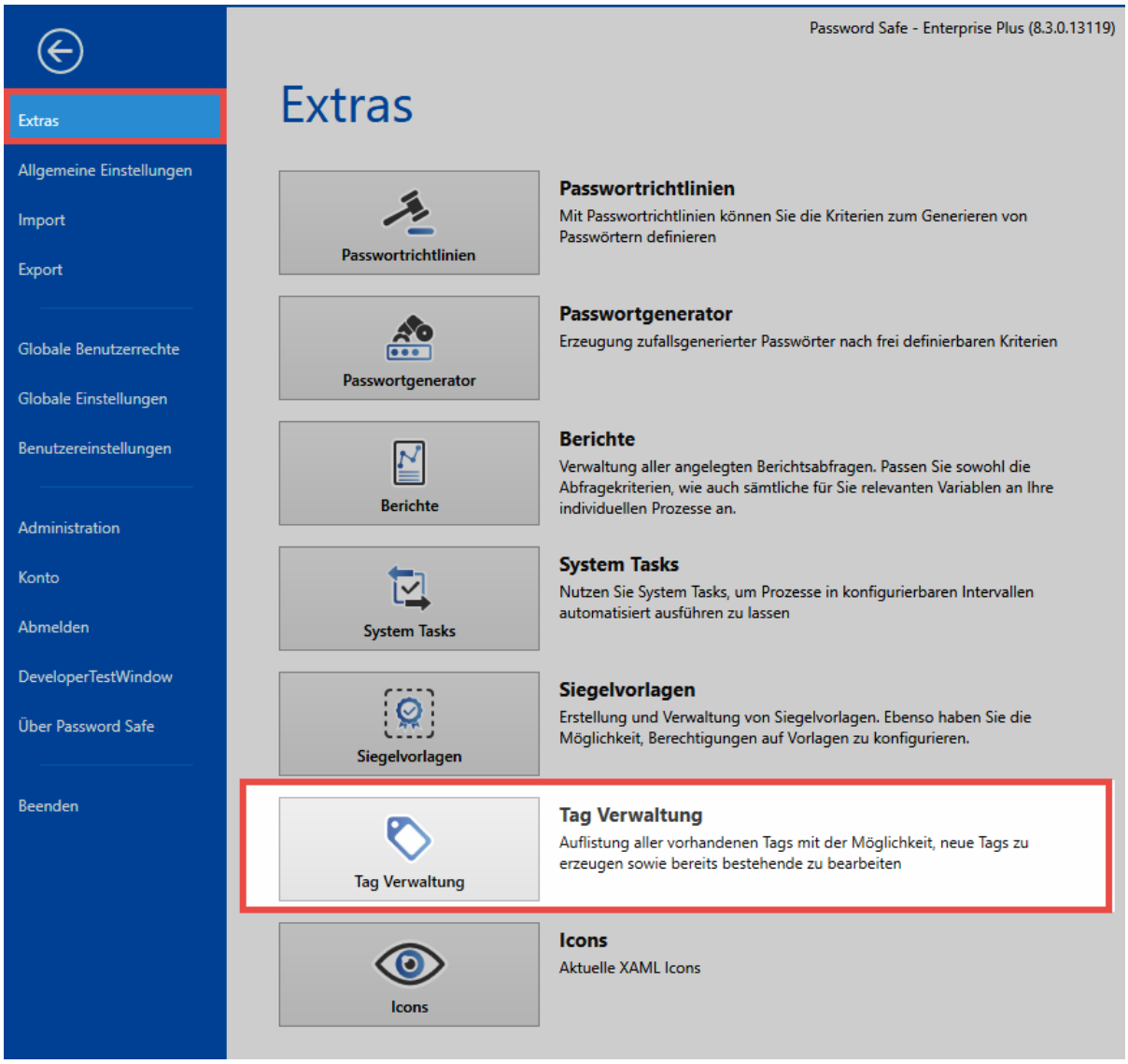


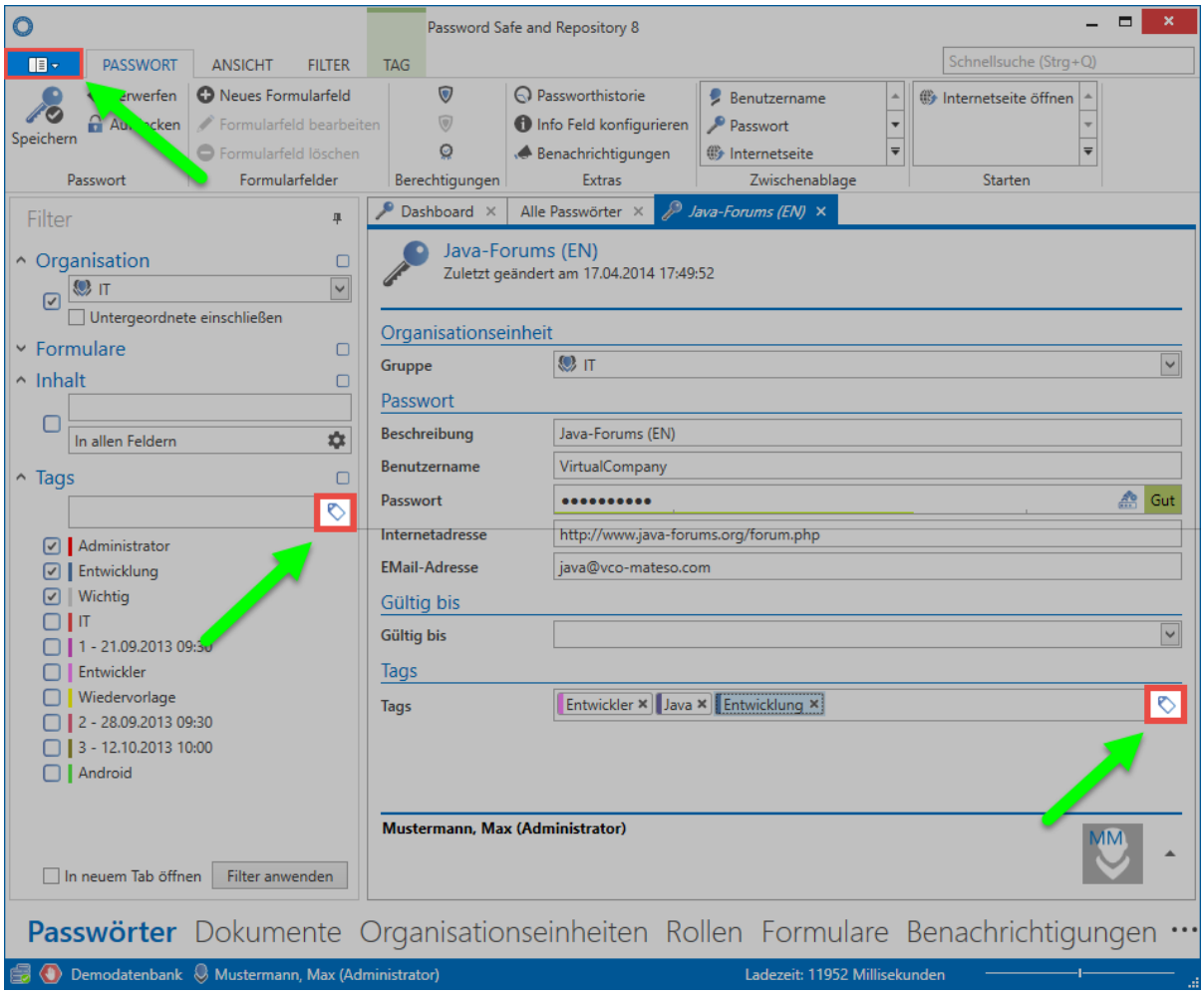

Sind Vorlagen einmal angelegt, können diese bei der Erstellung neuer Siegel direkt ausgewählt werden.

# Tagverwaltung

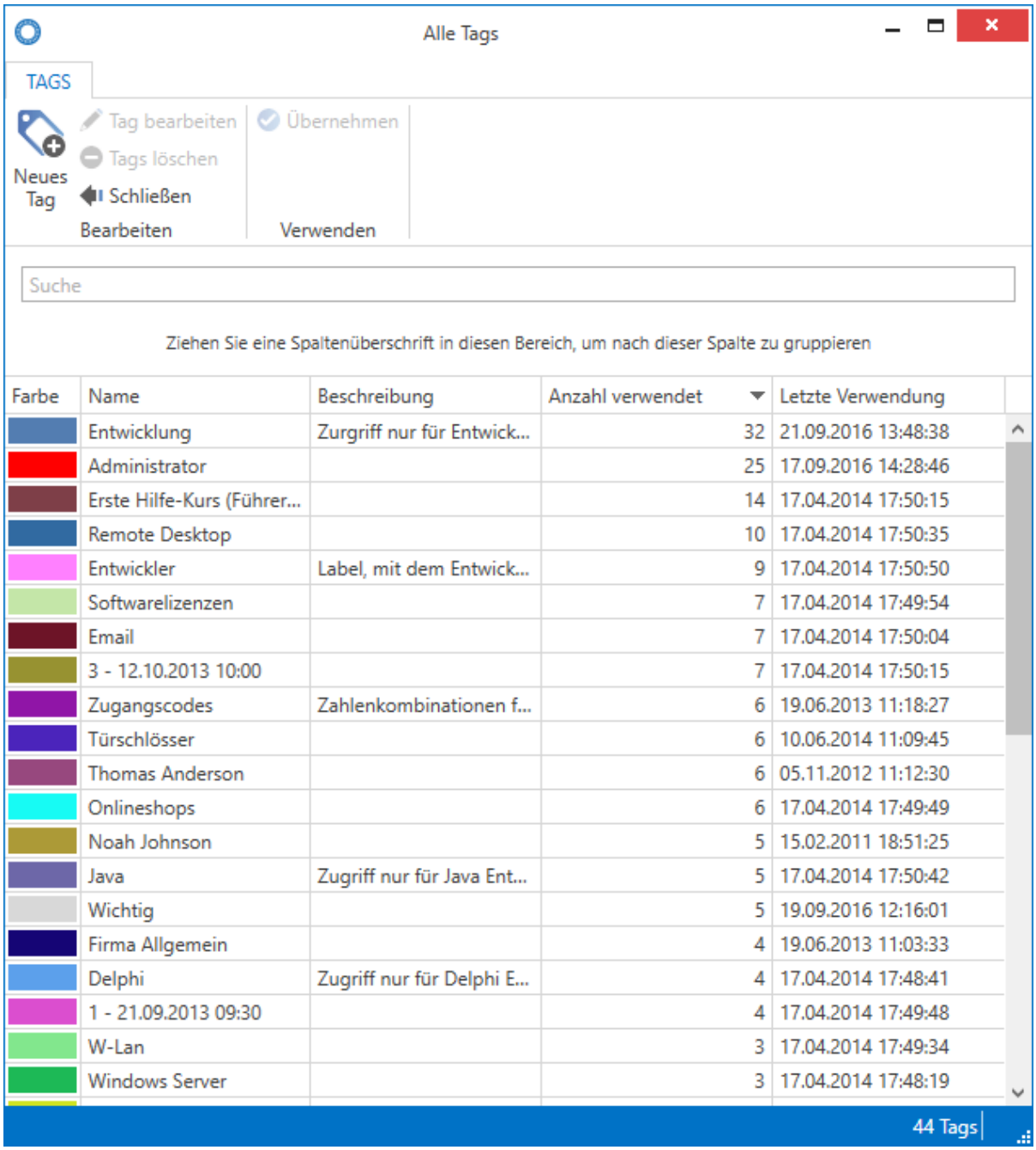
## Was ist die Tagverwaltung?

Alle existierenden Tags können direkt in der Tagverwaltung eingesehen, bearbeitet und gelöscht werden. Erreicht werden kann diese über den Filter, innerhalb des “Bearbeiten-Modus” eines Datensatzes sowie über das Hauptmenü unter der Gruppierung “Extras”.






Die Tagverwaltung selbst ist ein übersichtlich aufgebautes Werkzeug, mit dem man alle relevanten Informationen einsehen und bearbeiten kann. Auch die Zuweisung der Farben kann hier vorgenommen werden. Die Spalte “Anzahl verwendet” zeigt hierbei an, wie oft ein Objekt mit dem jeweiligen Tag versehen wurde. Auf diese Art und Weise behält man den Überblick und kann nicht mehr benötigte Tags entfernen.




! Zum Verwalten von Tags ist das Benutzerrecht **Tags verwalten** erforderlich. Dieses Recht ist Teil der Benutzerrechte.

! Das Löschen von Tags ist nur dann möglich, wenn mit diesen keinerlei Daten mehr verknüpft sind

# Allgemeine Einstellungen

## Was sind allgemeine Einstellungen?

Die **Allgemeinen Einstellungen** sind Benutzer bezogen. Somit kann jeder Benutzer die Software auf die eigenen Bedürfnisse anpassen. Folgende Optionen können konfiguriert werden:

### Farbschema

Es stehen mehrere Windows Farbschemata zur Auswahl. Das Farbschema **Colorful** stellt z.B. verschiedene Farben bereit, welche das unterscheiden der Module in der Software erleichtern. Wird das Farbschema geändert, muss der Client neu gestartet werden.

### Sprache

Es kann zwischen Deutsch und Englisch gewählt werden. Nach dem Ändern der Sprache muss der Client neu gestartet werden.

### Starte Anwendung minimiert im Benachrichtigungsbereich

Soll Password Safe im Hintergrund betrieben werden, kann der Client direkt minimiert gestartet werden. Der Zugriff erfolgt dann im Benachrichtigungsbereich.

### Anwendung beim Schließen minimieren

Ist diese Option aktiv, wird der Password Safe Client durch das Schließen des Fensters nicht geschlossen, sondern lediglich minimiert. Er läuft dann im Hintergrund weiter. Das ordnungsgemäße Beenden des Password Safe ist dann nur noch über das Hauptmenü möglich.

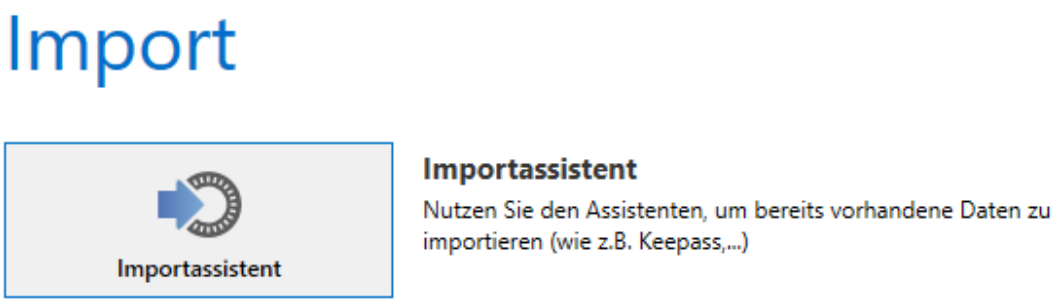
h4.Mit Windows starten

Selbstverständlich kann der Password Safe Client auch direkt mit Windows gestartet werden.

# Import

## Was ist der Import?

Falls vor dem Password Safe bereits ein anderes Passwort Verwaltungs-Tool genutzt wurde, können diese Daten in den Password Safe übernommen werden. Unterstützt werden die Formate .csv sowie im Speziellen Keepass (.xml). Beide Varianten können im Importassistenten abgebildet werden, welcher über Hauptmenü/Import gestartet wird.



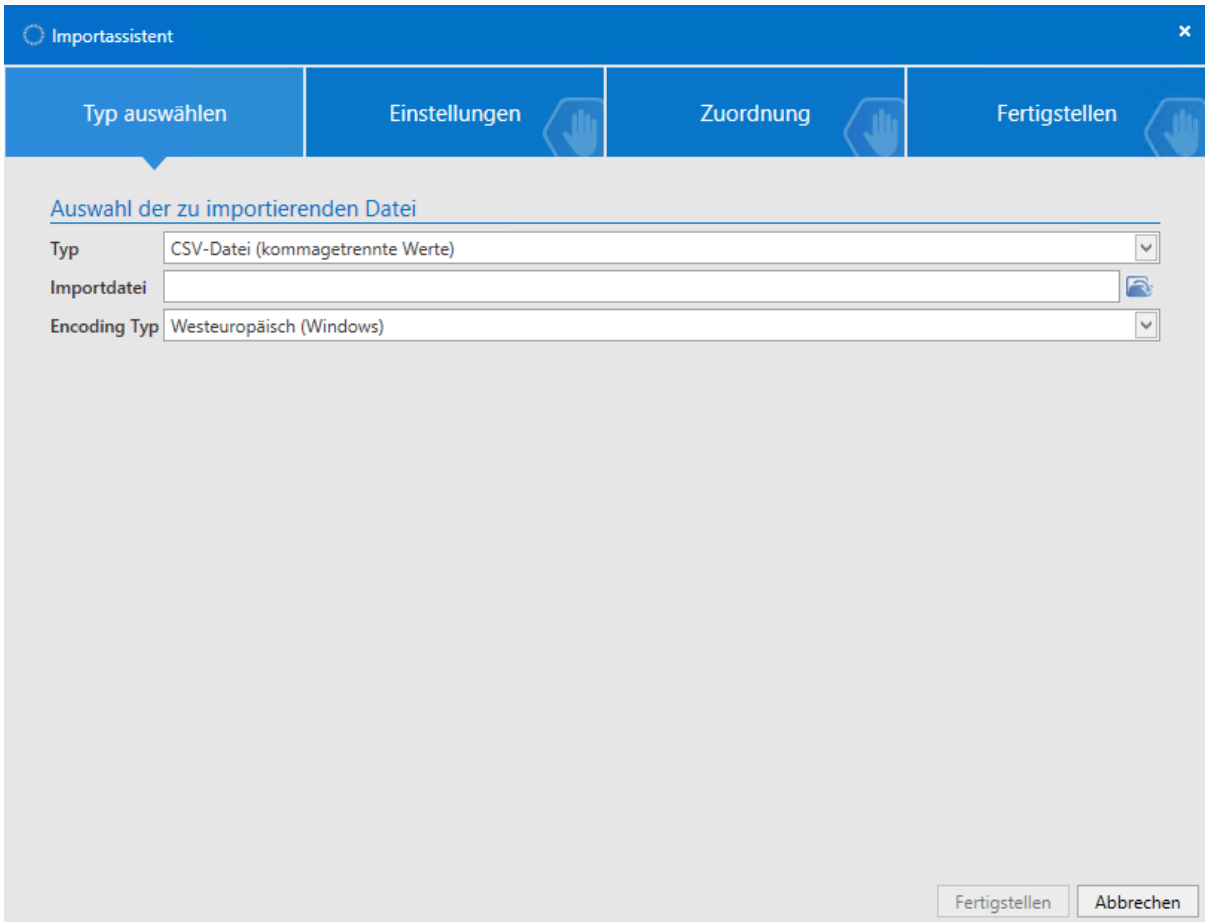

## Voraussetzungen

Ob Daten importiert werden dürfen, ist durch ein dementsprechendes Benutzerrecht gesichert.


## Der Importassistent

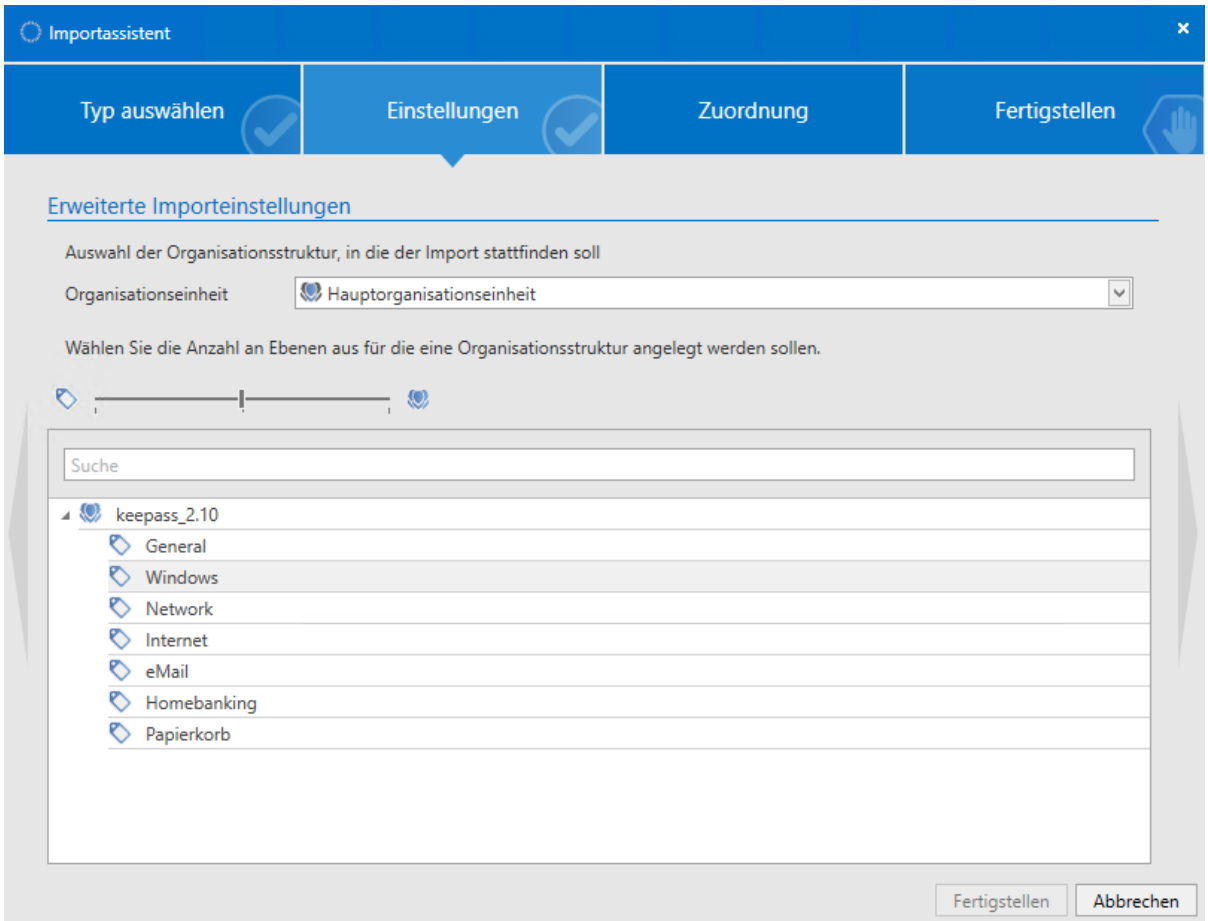
In vier Schritten unterstützt der Assistent den Import von Daten in den Password Safe.

## Typ auswählen




Im ersten Schritt definiert man die Datei, aus welcher der Import erfolgen soll. Erst, wenn der festgelegte Typ mit der angegebenen, zu importierenden Datei übereinstimmt, kann der zweite Schritt in die Einstellungen gegangen werden.

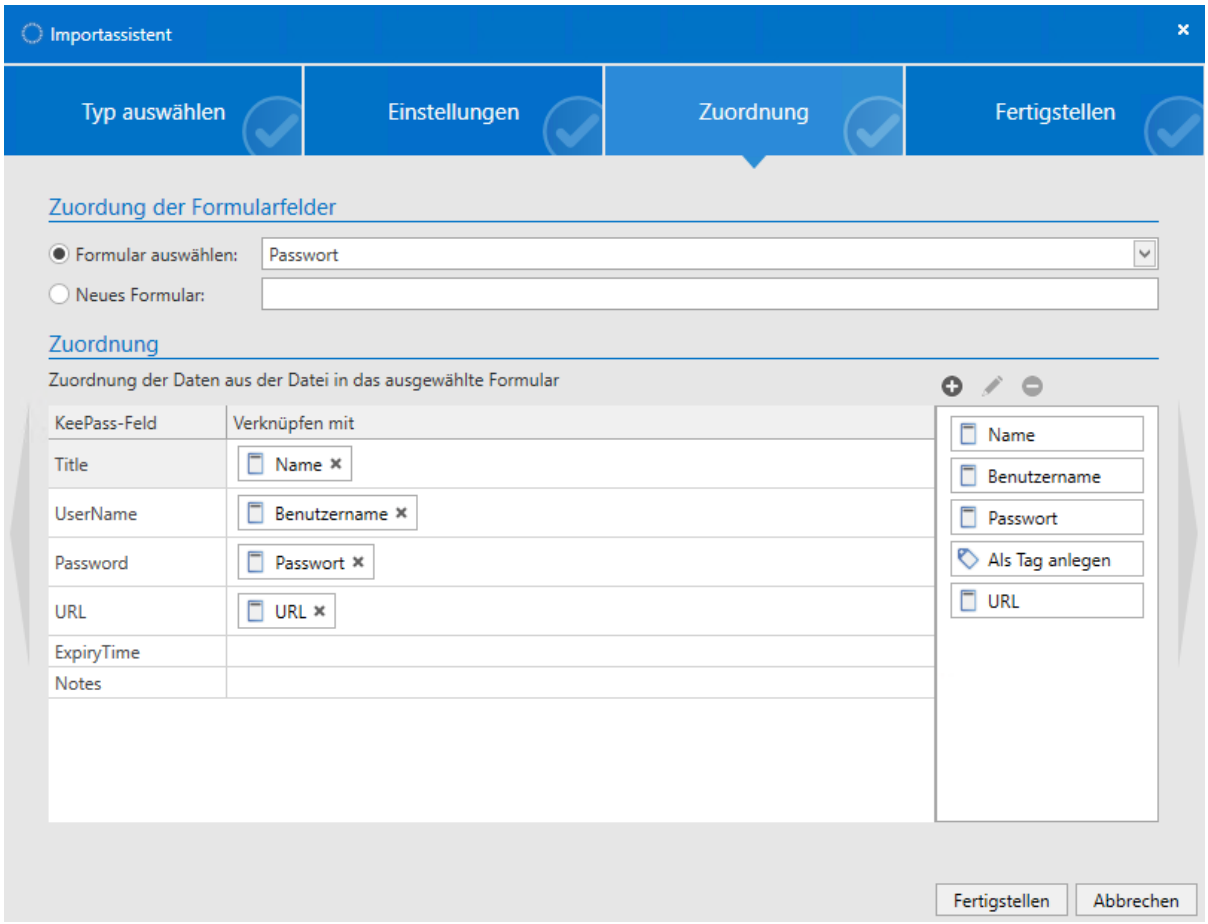
## Einstellungen




1. In den Einstellungen wird zuerst definiert, in welcher Hierarchieebene die zu importierende Struktur gespeichert werden soll. Wie ersichtlich wird aktuell in die Hauptorganisationseinheit importiert. Über ein Dropdown-Menü kann auch eine der bestehenden Organisationseinheiten als übergeordnete Instanz definiert werden.
2. Der Schieberegler bestimmt, ob die zu importierenden Strukturen als Organisationseinheit oder als Tag importiert werden sollen. Ganz links bewirkt der Schieberegler, dass lediglich tags erstellt werden, rechts werden alle Objekte als Organisationsstruktur angelegt. Darüber hinaus kann über das Kontextmenü der rechten Maustaste jedes Objekt separat konfiguriert werden. Auch das Ignorieren von Ordnern ist möglich.

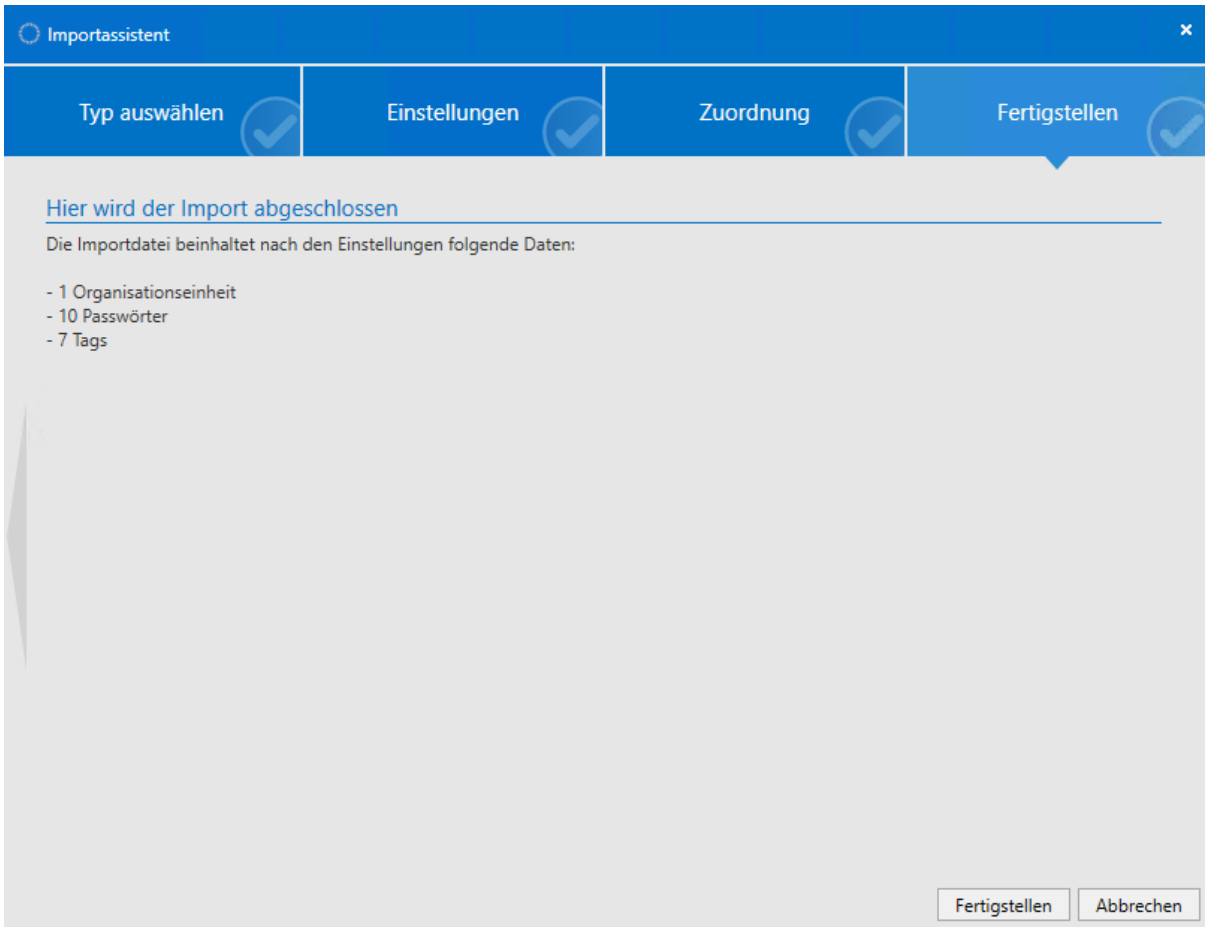
> Es existieren keine Ordner im Password Safe. Aufgrund dessen muss beim Import festgelegt werden, ob ein Ordner eine Organisationsstruktur werden soll, oder als Tag angelegt wird. Das gleiche Verfahren kommt auch bei der Migration zum Einsatz.

## Zuordnung der Formularfelder




Im dritten Schritt erfolgt die Zuordnung der Formulare aus der zu importierenden Datei in bereits bestehende Formulare. Da Formularfelder auch anders benannt sein können, muss die Zuordnung manuell per Drag & Drop erfolgen. Je nachdem, welches Formular in der obersten Zeile ausgewählt wurde, können Formularfelder aus der Liste rechts nun per Drag & Drop den zu importierenden Formularfeldern zugeordnet werden. Auch die Erstellung von neuen Formularen ist möglich.

## Fertigstellen




Im abschließenden Arbeitsschritt werden die getroffenen Einstellungen in einer Auflistung der zu importierenden Objekte zusammengefasst. “Fertigstellen” schließt den Assistenten und startet den Import.

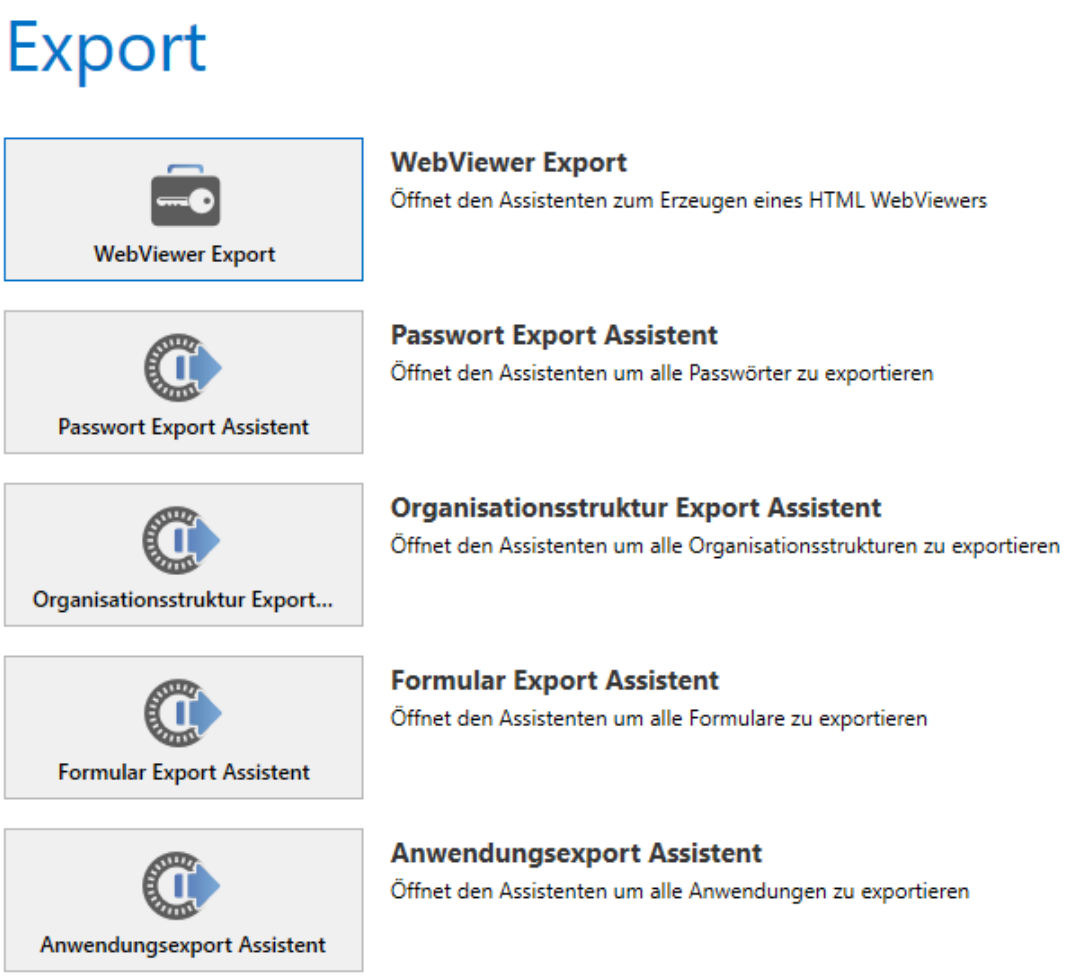
# Export

## Was ist der Export?

Der Export dient dem Extrahieren von in der MSSQL-Datenbank gespeicherten Daten. Sowohl punktuell (manuell) wie auch per automatisiertem System Task können Informationen auf diese Art und Weise dem Password Safe entnommen werden.

> ! Bitte beachten Sie, dass das Extrahieren von Passwörtern stets eine Abschwächung des Sicherheitskonzeptes mit sich bringt. Die Aussagekraft des Logbuchs leidet definitiv unter Export von Daten, da jene Daten nicht mehr der Revision unterliegen können. Besonders beim Passwort Export Assistenten ist dieser Aspekt zu beachten, da das Export-Ergebnis nicht separat durch ein Passwort geschützt werden kann.

Aufgerufen wird der Export über Hauptmenü/Export. Es gibt grundsätzlich zwei Arten von Export, den WebViewer Export sowie den Export Assistenten. Letzterer unterteilt sich thematisch jedoch in vier Unterkategorien.

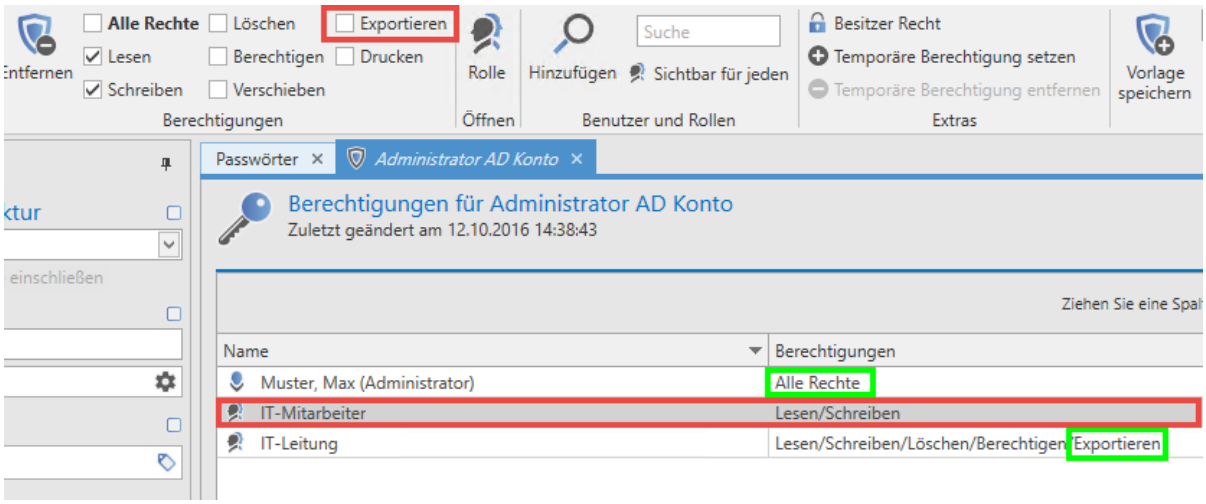



Der WebViewer Export erzeugt eine durch ein Passwort geschützt HTML-Datei. Im Gegensatz hierzu wird durch den Export Assistenten eine offene und ungeschützte .csv Datei erstellt.

## Voraussetzungen

Ob ein Datensatz exportiert werden darf oder nicht, ist durch Berechtigungen gesichert. Diverse Sicherheitsmechanismen greifen. Restriktionen können sowohl auf Seiten des Datensatzes wie auch über Benutzerrechte vorliegen

- **Die Berechtigungen des Datensatzes**: Ob ein Datensatz exportiert werden darf, wird in den Berechtigungen auf den Datensatz definiert




Im vorliegenden Beispiel ist die markierte Rolle IT-Mitarbeiter nicht berechtigt, den Datensatz zu exportieren. Die IT-Leitung hingegen besitzt das Recht. Darüber hinaus besitzt der Administrator alle Rechte, was auch das Exportieren beinhaltet.

- **Das Benutzerrecht "Exportieren"**: Es existiert in der Kategorie "Allgemein" ein Benutzerrecht, welches einem Benutzer das Recht für den Export gewährt. Ist dieses Recht nicht gegeben, kann generell **keine** Form des Exports durchgeführt werden.


Soll ein Datensatz exportiert werden, muss sowohl das Benutzerrecht vorliegen als auch die dementsprechende Berechtigung auf dem Datensatz vorhanden sein. Das Benutzerrecht definiert, ob man **generell** exportieren darf, die Berechtigungen auf Datensätzen bestimmen, **welche** Datensätze exportiert werden dürfen.

# HTML WebViewer Export

## Was ist der HTML WebViewer Export?

Diese Art des Exports extrahiert selektiv Datensätze aus der Datenbank und schützt diese durch ein Passwort. Das ausgegebene Format ist eine mittels AES 256 verschlüsselte HTML-Datei. Das angesprochene Passwort wird im Rahmen des Assistenten vergeben.

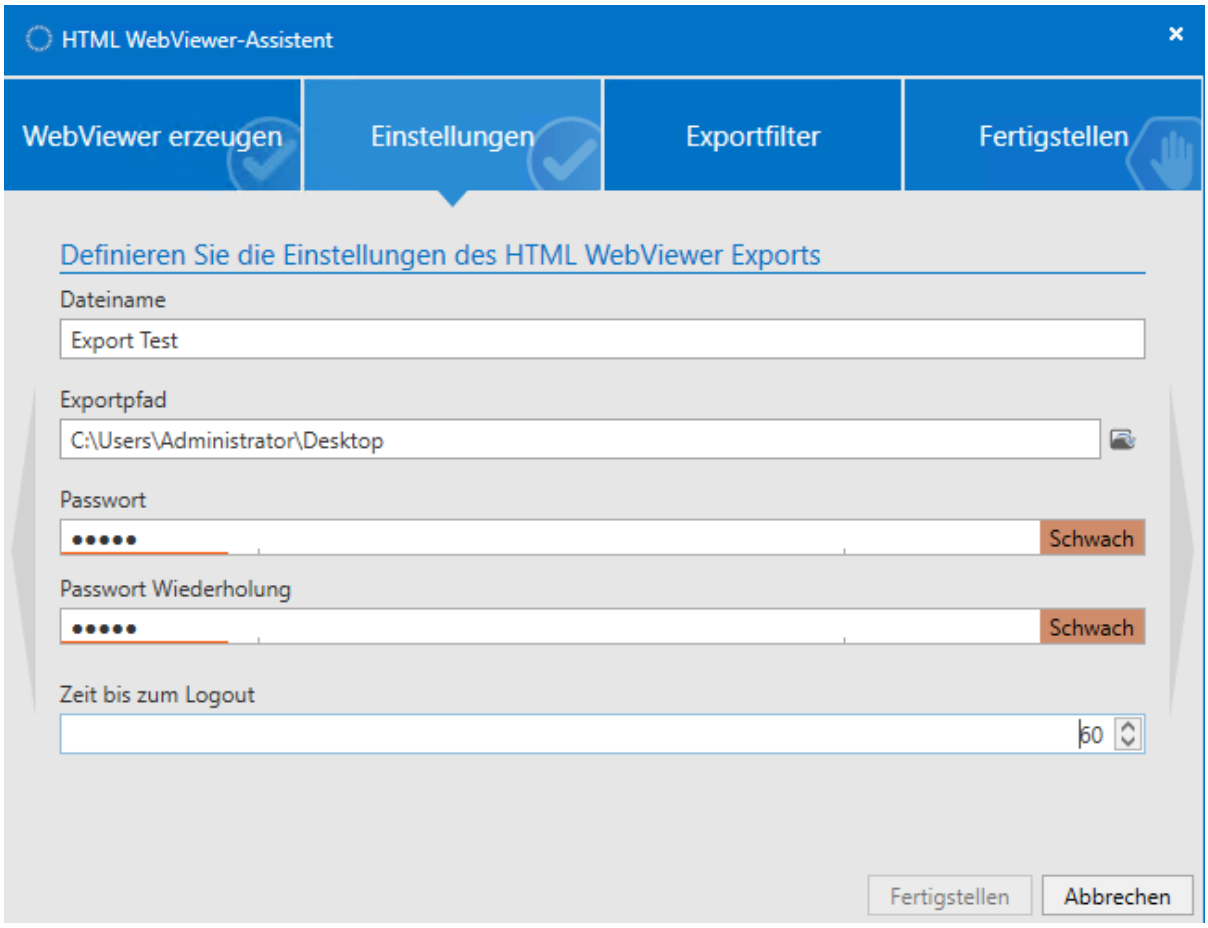
### (zusätzliche) Voraussetzungen für die Nutzung des HTML-WebViewer Exports

Zusätzlich zu den bereits genannten Voraussetzungen existiert für den WebViewer Export in der “Kategorie Sicherheit” ein separates Benutzerrecht, welches gesetzt sein muss.

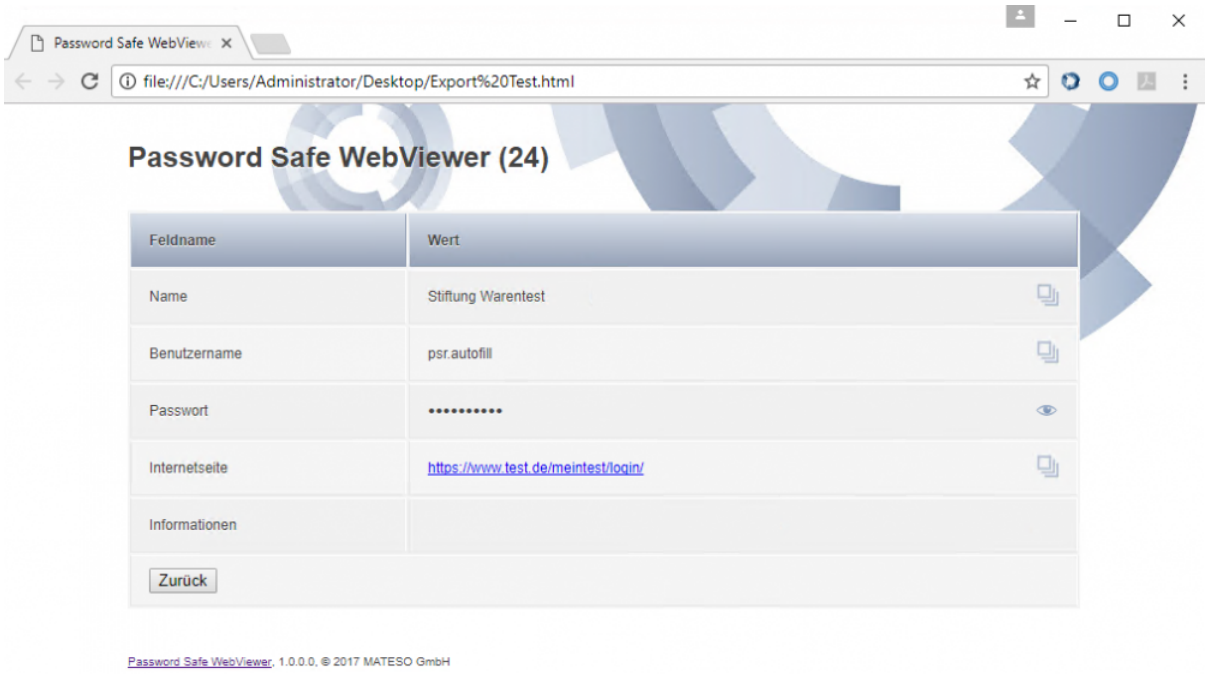
| Kategorie: Sicherheit |
| --- |
| Kann persönliche Datensätze erstellen |
| Kann Optionen der Sicherheitsstufe ändern |
| Kann HTML WebViewer exportieren |
| Kann globale Einstellungen bearbeiten |
| Kann Passwortrichtlinien verwalten |
| Ist Datenbank-Administrator |
| Kann gesperrte Benutzer verwalten |
| Kann Autologin verwalten |
| Kann Datenbanksitzungen verwalten |
| Kann Kategorien der Passwortrichtlinien verwalten |
| Kann Aufzeichnungen einer Anwendung verwalten |
| Kann Active Directory Profile verwalten |
| Kann Besitzerrecht setzen |

### Der WebViewer Export Assistent

Der Assistent geleitet durch sämtliche Konfigurationen bis hin zur Erstellung der HTML-Datei.




Innerhalb der **Einstellungen** definieren Sie diverse Variablen des Exports. Das Passwort entspricht dem Wert, welcher dem Adressaten der Datei zum Öffnen bekannt sein muss. Die Zeit bis zum Logout definiert die Zeitspanne, welche nach dem Öffnen der Datei bei Inaktivität zum Schließen der Datei führt. Danach muss das Passwort erneut eingegebene werden. Der **Exportfilter** definiert anhand der konfigurierbaren Filterkriterien, welche Passwörter exportiert werden sollen. Die Konfiguration ist analog zum Filter des Client durchführbar. Unter **Fertigstellen** wird die voraussichtliche Anzahl der zu exportierenden Datensätze ausgegeben sowie der Vorgang abgeschlossen.




Die erzeugte HTML-Datei kann verschickt und in beliebigen Browsern geöffnet werden. Der Timer am oberen Bildschirmrand beschreibt die verbleibende Zeit bis zum Schließen der Datei aufgrund von Inaktivität.

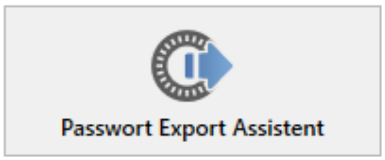
! Es wird für das Entschlüsseln der erzeugten WebViewer Datei zwingend JavaScript vorausgesetzt

! In E-Mailprogrammen, welche eventuell kein JavaScript ausführen können, muss die HTML-Datei über den normalen Browser geöffnet werden

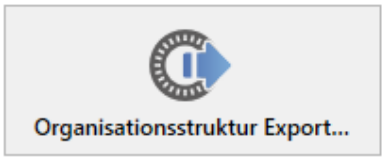
# Export Assistent

## Welche Export Assistenten existieren?

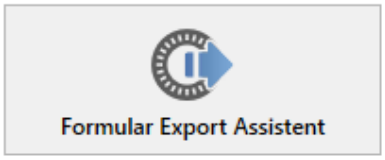
Es existieren insgesamt vier verschiedene Exportassistenten.




**Passwort Export Assistent**
Öffnet den Assistenten um alle Passwörter zu exportieren




**Organisationsstruktur Export Assistent**
Öffnet den Assistenten um alle Organisationsstrukturen zu exportieren




**Formular Export Assistent**
Öffnet den Assistenten um alle Formulare zu exportieren


**Anwendungsexport Assistent**
Öffnet den Assistenten um alle Anwendungen zu exportieren

Funktionell unterscheiden sich diese nur in Bezug auf die zu exportierenden Daten. Unterschieden wird zwischen Passwörtern, Organisationsstrukturen, Formularen und Anwendungen. **Da die Handhabung aller vier Assistenten identisch ist, soll nachfolgend lediglich der Passwort Export Assistent betrachtet werden**. Funktionell unterscheiden sich die übrigen drei nicht von diesem.

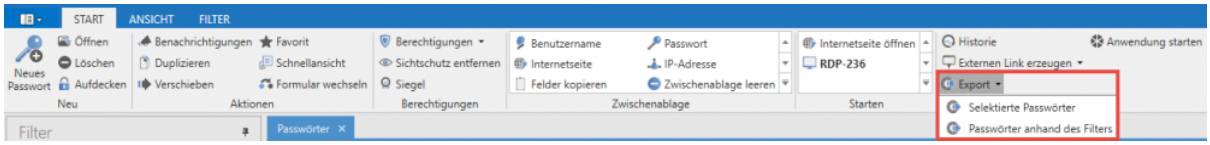
## Was ist der Passwort Export Assistent?

Der Assistent ermöglicht das Exportieren von Datensätzen in das gängige .csv Format. Im Gegensatz zum WebViewer Export ist die zu erzeugende Datei nicht durch ein Passwort geschützt. Es ist selbstredend, dass mit diesem Feature behutsam umgegangen werden muss.

## Starten des Passwort Export Assistenten

Der Export Assistent kann auf unterschiedlichen Wegen erreicht werden:

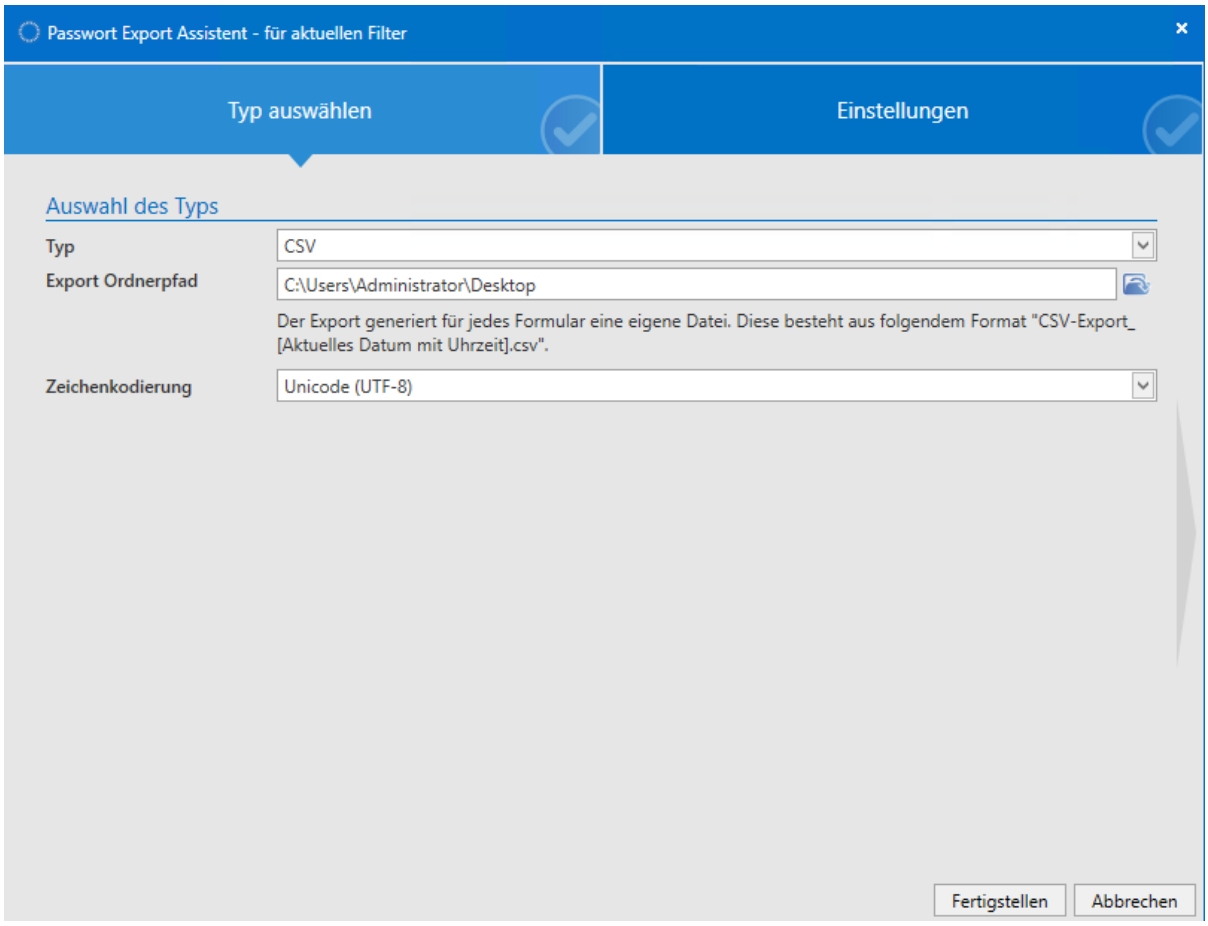
- **Starten über Hauptmenü/Extras**: Ruf man den Assistenten auf, werden stets alle Passwörter exportiert, auf die der angemeldete Benutzer berechtigt ist. Bei einem Administrator mit Berechtigungen für alle Datensätze entspricht das Ergebnis der Ausgabe aller Passwörter der Datenbank.
- **Starten über die Ribbon**: In der Ribbon im Modul Passwörter kann der Export ebenso angestoßen werden.




Der Passwort Export Assistent kann über die Ribbon auf zwei Arten aufgerufen werden. **Selektierte Passwörter** exportiert nur die in der Listenansicht markierten Passwörter, wohingegen **Passwörter anhand des Filters** als Kriterium die aktuell definierte Filtereinstellung ansetzt.

## Der Assistent

Innerhalb des Assistenten werden diverse Variablen für den Export sowie der Speicherort definiert. Eine zugehörige Vorschau ist ebenso enthalten.



Nach Fertigstellung des Assistenten wird der gewünschte Export erzeugt und auf dem definierten Ablageort gespeichert.

! Erneut soll auf die Sensibilität dieser sehr sicherheitskritischen Exportfunktion hingewiesen werden. Da man die für den Export nötigen Berechtigungen in der Regel nur hierarchisch höher gestellten Benutzer/Rollen zuteilt, bekommt dieses Thema eine noch viel sicherheitskritischere Relevanz: Es können alle Passwörter exportiert werden, auf die man berechtigt ist. Administratoren können dadurch (gewollt oder ungewollt) per se mehr Schaden anrichten.

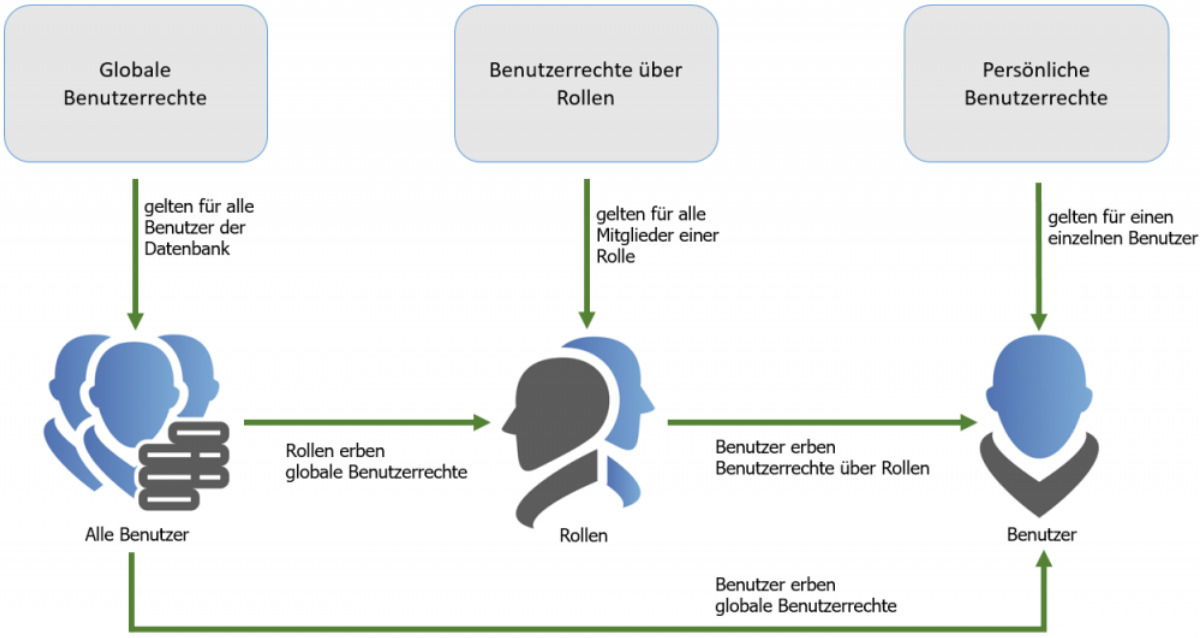
# Benutzerrechte

## Was sind Benutzerrechte?

In den Benutzerrechten wird der Zugang zu Funktionalitäten konfiguriert. Sowohl die Sichtbarkeit einzelner Module als auch die Nutzung von Import, Export oder die Verwaltung von Rechtevorlagen fallen unter anderem in diese Kategorie. Eine vollständige Auflistung ist direkt in den Benutzerrechten einsehbar.

## Verwaltung von Benutzerrechten

Alle Benutzerrechte ausschließlich auf Benutzerebene zu verwalten wäre zeitintensiv und somit unverhältnismäßig in Bezug auf Pflege und Wartung. Analog zum Berechtigungskonzept bietet sich eine Herangehensweise an, bei der mehrere Benutzer zusammengefasst werden. Nichtsdestotrotz muss die Möglichkeit gegeben sein, zusätzlich auf individuelle Anforderungen einzelner Benutzer einzugehen. Wiederum sollten manche Funktionalitäten allgemein zur Verfügung gestellt werden können. Um dem allem gerecht zu werden, bietet Password Safe ein dreistufiges Konzept.



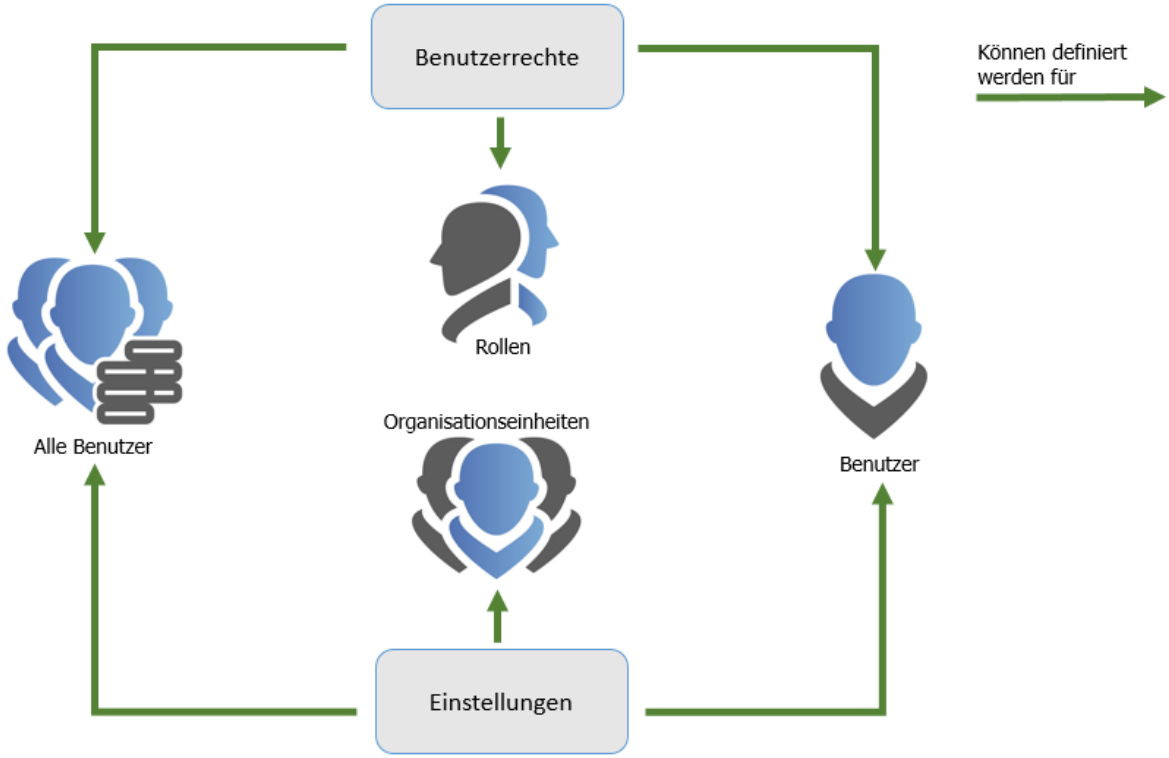

Am Ende der Benutzerrechte steht immer der Benutzer im Mittelpunkt. Dieser erhält Benutzerrechte stets auf einem der drei folgenden Wege:

1. Das **persönliche Benutzerrecht** gilt immer nur für einen bestimmten Benutzer. Konfiguriert wird dies stets über das Modul Organisationsstrukturen.

2. **Benutzerrechte über Rollen** gelten für alle Mitglieder einer Rolle und werden im Modul Rollen definiert
3. Das **globale Benutzerrecht** gilt ausnahmslos für alle Benutzer einer Datenbank. Die Konfiguration hierfür kann in den Client Einstellungen vorgenommen werden.

Es ist irrelevant auf welchem Weg ein Benutzer ein Benutzerrecht erhält. Am Ende zählt nur, dass er ein Recht auf einem der drei genannten Wege auch wirklich bekommt. Zwecks der angesprochenen Verwaltbarkeit ist es zu empfehlen, Benutzerrechte an Rollen zu binden und bei Bedarf durch globale Benutzerrechte zu ergänzen.

! Zusätzlich zu persönlichen und globalen Benutzerrechten werden (im Gegensatz zu Einstellungen) Benutzerrechte nicht über Organisationseinheiten, sondern über Rollen vergeben!



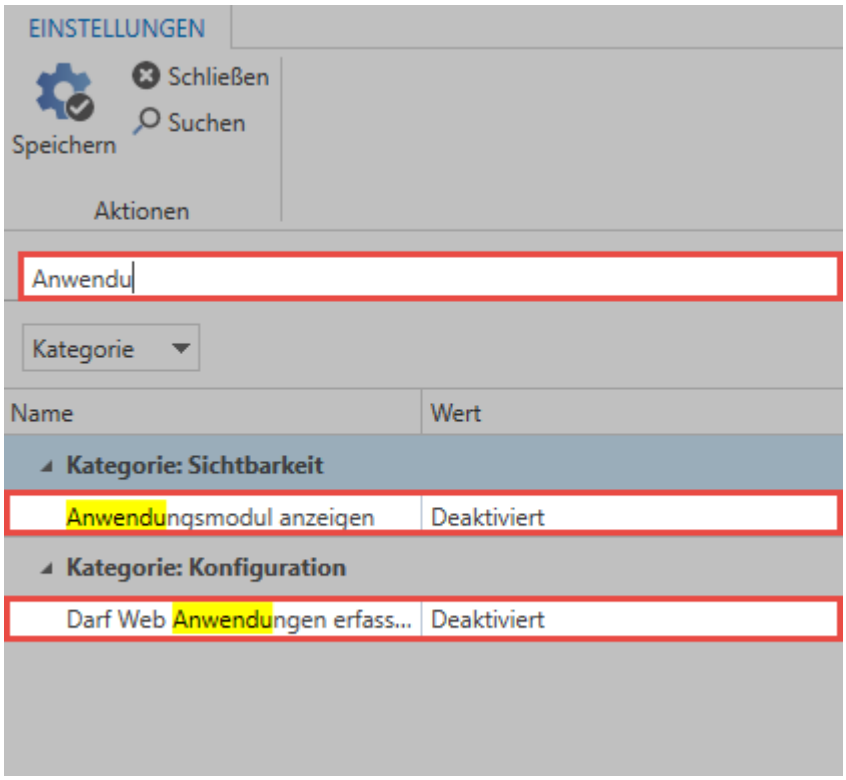

# Konfiguration der Sicherheitsstufe

Ein essentiell wichtiges Element, welches ebenso in den Benutzerrechten festgelegt wird, ist die **Sicherheitsstufe**. Diese ist die Basis für die Konfiguration der Benutzereinstellungen.

| Name | Wert |
|---|---|
| **Kategorie: System Tasks** | |
| Kann Active Directory System Tasks verwalten | Deaktiviert |
| Kann DiscoverService System Tasks verwalten | Deaktiviert |
| Kann Password Reset System Tasks verwalten | Deaktiviert |
| Kann Reporting System Tasks verwalten | Deaktiviert |
| Kann OfflineViewer Export System Tasks verwalten | Deaktiviert |
| **Kategorie: Sichtbarkeit** | |
| Password Reset Modul anzeigen | Deaktiviert |
| Anwendungsmodul anzeigen | Deaktiviert |
| Dokumentmodul anzeigen | Aktiviert |
| Logbuchmodul anzeigen | Deaktiviert |
| Benachrichtigungsmodul anzeigen | Aktiviert |
| Formularmodul anzeigen | Deaktiviert |
| Rollenmodul anzeigen | Deaktiviert |
| Organisationsmodul anzeigen | Deaktiviert |
| Passwortmodul anzeigen | Aktiviert |
| **Kategorie: Sicherheit** | |
| Kann Datenbanksitzungen verwalten | Deaktiviert |
| Kann Autologin verwalten | Deaktiviert |
| Kann gesperrte Benutzer verwalten | Deaktiviert |
| Kann Passwortrichtlinien verwalten | Deaktiviert |
| Kann globale Einstellungen bearbeiten | Deaktiviert |
| Kann HTML OfflineViewer exportieren | Deaktiviert |
| Kann Optionen der Sicherheitsstufe ändern | Sicherheitsstufe 1 |
| **Kategorie: Offline-Modus** | |
| Zeitspanne, wie lange der Offline-Modus ohne Serververbindung benutzt werden kann | Zugriff nach sieben Tagen sperren |
| **Kategorie: Konfiguration** | |
| Siegelvorlagen verwalten | Aktiviert |
| Tags verwalten | Deaktiviert |
| User darf Rechtevorlagen konfigurieren | Deaktiviert |
| Darf Web Anwendungen erfassen | Deaktiviert |
| **Kategorie: Allgemein** | |
| User darf Rechtevorlagen ändern | Deaktiviert |
| Exportieren | Deaktiviert |
| Importieren | Deaktiviert |

# Suche innerhalb der Benutzerrechte

Aufgrund der Vielzahl an möglichen Konfigurationen unterstützt die Suche das schnelle Auffinden der gewünschten Konfiguration immens. Funktionell orientiert sich diese wie gewohnt an der Listensuche.


EINSTELLUNGEN
Speichern
Schließen
Suchen
Aktionen
Anwendu
Kategorie
Name
Wert
Kategorie: Sichtbarkeit
Anwendungsmodul anzeigen
Deaktiviert
Kategorie: Konfiguration
Darf Web Anwendungen erfass...
Deaktiviert

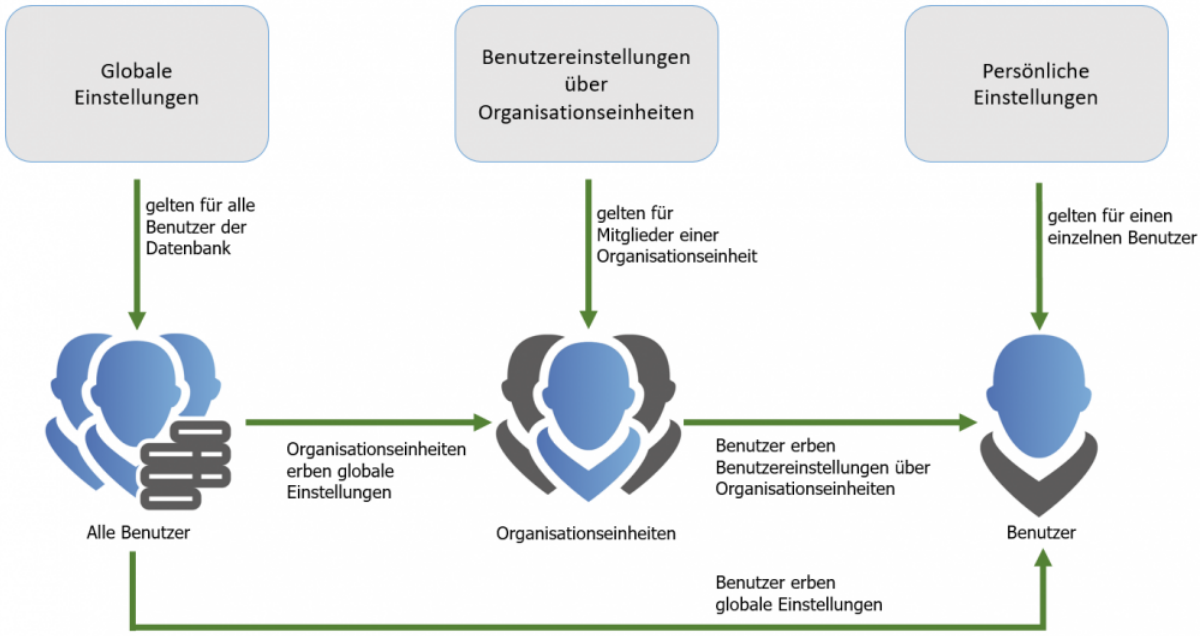
# Benutzereinstellungen

## Was sind Benutzereinstellungen

Innerhalb des Password Safe existieren viele Funktionen, welche an die Bedürfnisse von Benutzern angepasst werden können. Ebenso ist es möglich, für optische Darstellungen diverse Parameter festzulegen. Sowohl auf **Benutzerebene**, **global** als auch über **Organisationseinheiten**, können diese Einstellungen vererbt werden. Darüber hinaus existiert ein Sicherheitsstufenkonzept, welches die Kategorisierung der User in fünf Schichten vornimmt. Die Verwaltung von Einstellungen kann somit an das Vorhandensein der benötigten Sicherheitsstufe gekoppelt werden.

## Verwaltung von Benutzereinstellungen

Die Konfiguration der Benutzereinstellungen ähnelt stark dem Vorgehen bei Benutzerrechten. Auch hier existieren insgesamt drei Möglichkeiten, mit denen ein Benutzer seine Einstellungen definieren kann, bzw. von anderer Stelle konfiguriert bekommt. Zwecks einfacher Verwaltbarkeit bietet es sich erneut an, die User nicht einzeln zu konfigurieren, sondern mehrere gleichberechtigte Benutzer zusammenfassend mit Einstellungen zu versehen.

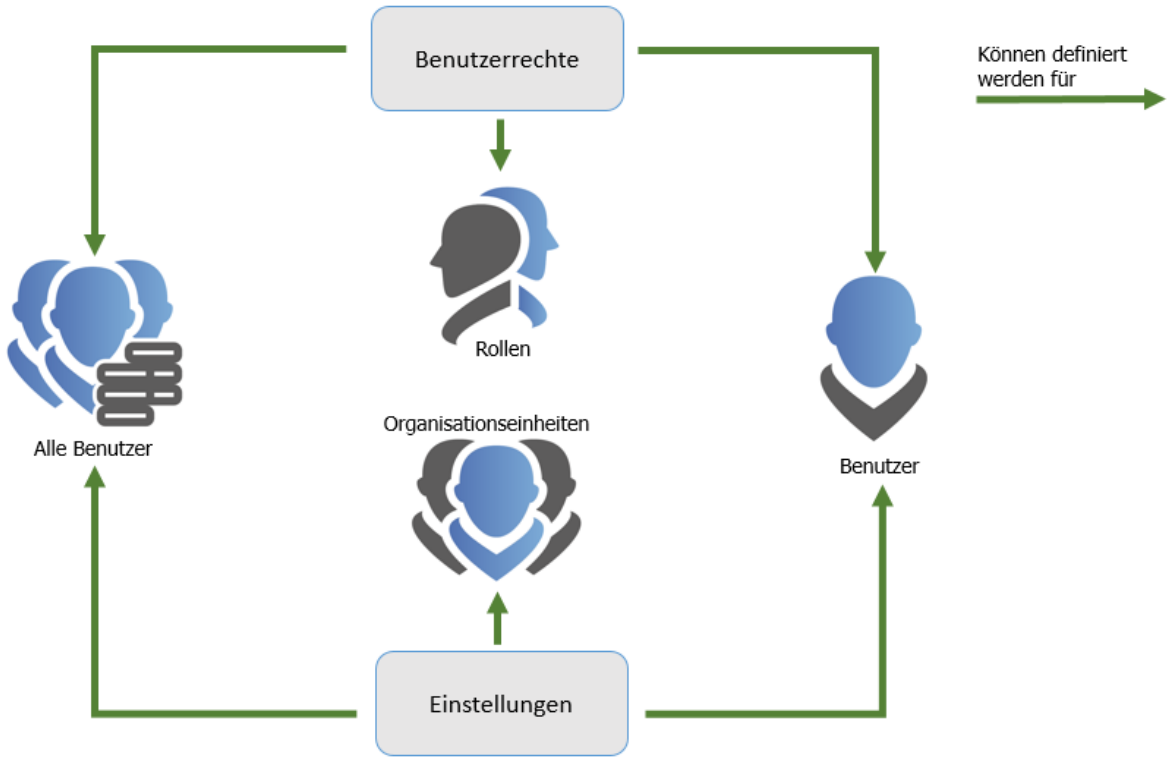



Auch bei den Einstellungen steht immer der Benutzer im Mittelpunkt des Interesses. Dieser erhält seine Einstellungen stets auf einem der drei folgenden Wege:

1. **Persönliche Einstellungen** gelten immer nur für einen bestimmten Benutzer. Konfiguriert werden diese stets über das Modul Organisationsstruktur.

2. **Einstellungen über Organisationseinheiten** gelten für alle Mitglieder einer Rolle und werden im Modul Organisationsstruktur definiert
3. **Globale Einstellungen** gelten ausnahmslos für alle Benutzer einer Datenbank. Die Konfiguration hierfür wird in den Client Einstellungen vorgenommen.

! Zusätzlich zu persönlichen und globalen Einstellungen werden (im Gegensatz zu Berechtigungen) Einstellungen nicht über Rollen, sondern über Organisationseinheiten vergeben!

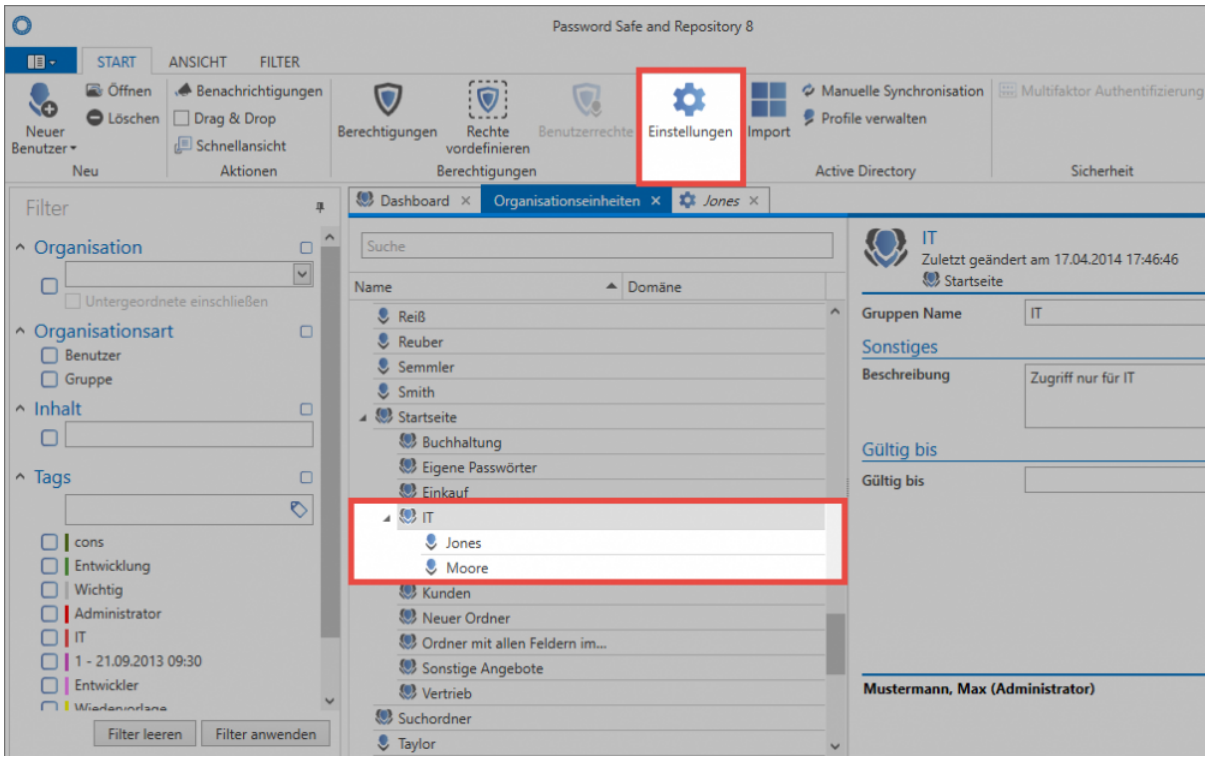



# Vererbung von Benutzereinstellungen

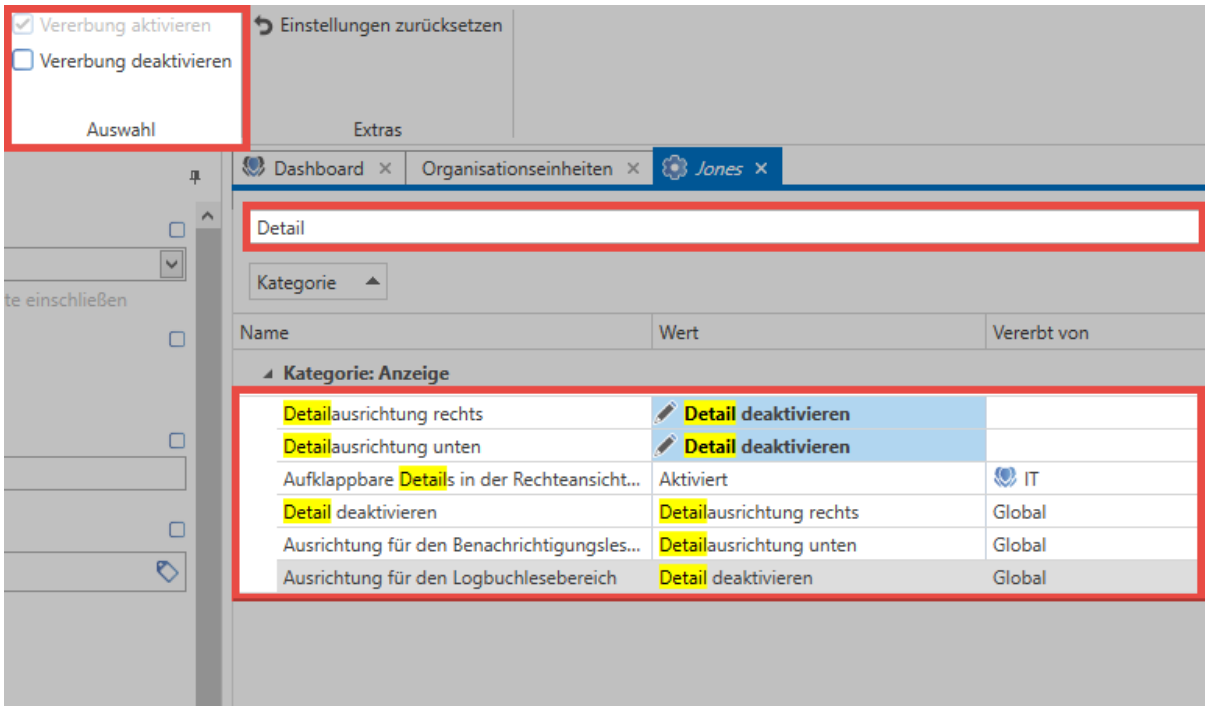
Lässt man die personenbezogenen Einstellungen außen vor, bleiben zwei Möglichkeiten zur Vererbung von Einstellungen:

1. globale Vererbung
2. Vererbung auf Basis von Mitgliedschaft in Organisationseinheiten (OU)

Globale Einstellungen werden wie gehabt in den Client Einstellungen konfiguriert. Die Vererbung über Organisationseinheiten erfolgt im Modul Organisationsstruktur. Alle Benutzer, welche einer Organisationseinheit zugeordnet sind, erben alle Benutzereinstellungen dieser OU. Im vorliegenden Fall erben die Benutzer “Jones” und “Moore” alle Einstellungen aus der Organisationseinheit “IT”:




Über den Button “Einstellungen” in der Ribbon kann man sich sowohl für Organisationseinheiten als auch für Benutzer die Einstellungen einsehen. Die Vielzahl der Einstellungsmöglichkeiten können durch die bekannten Suchmechanismen eingeschränkt werden.



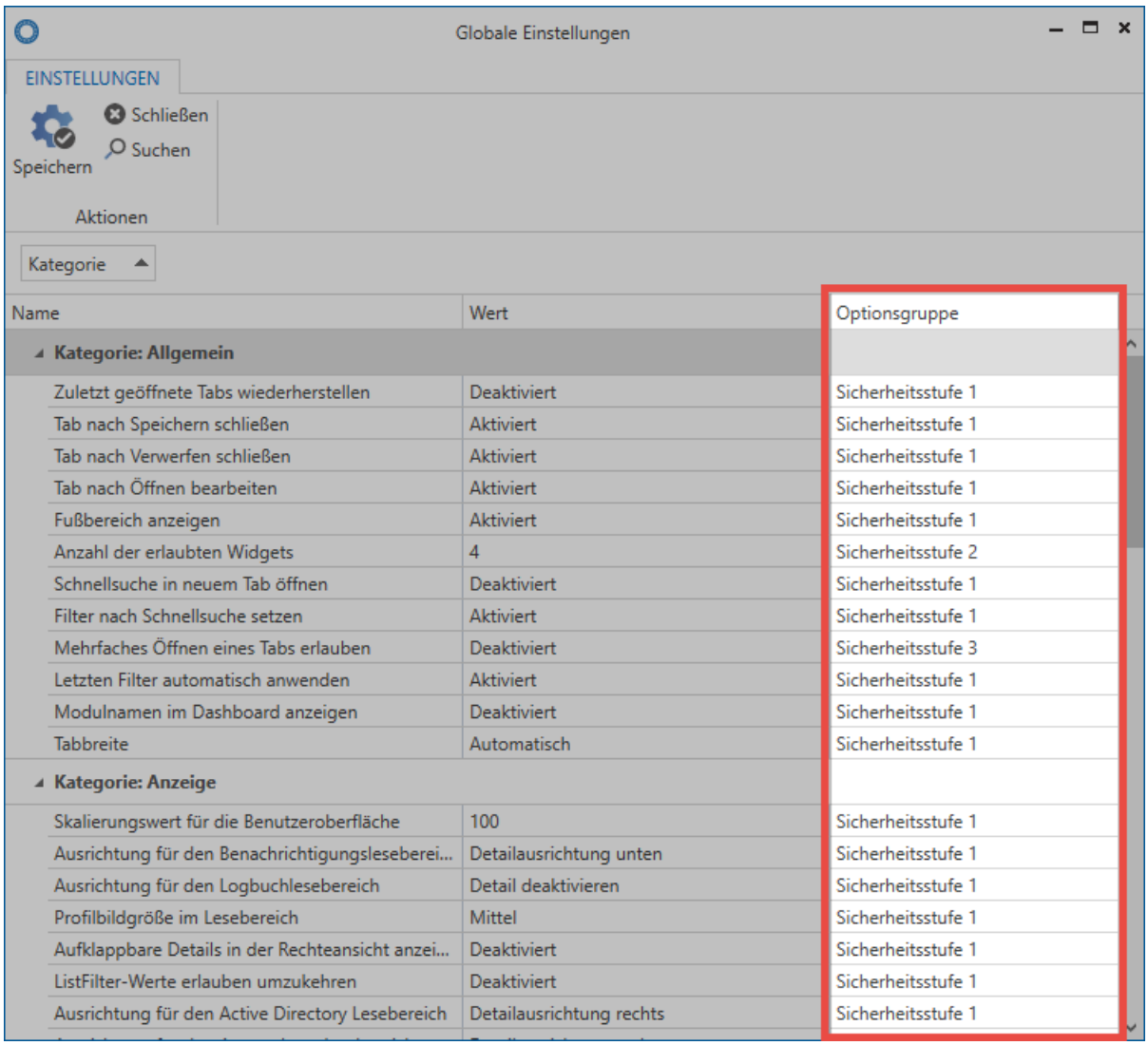

Im vorliegenden Schaubild ist die Benutzereinstellung des Users “Jones” geöffnet. Zwecks Übersicht wurde nach dem Suchbegriff “Detail” gefiltert. In der Spalte **“Vererbt von”** ist ersichtlich, dass einige Einstellungen global, bzw. von der Organisationseinheit “IT” geerbt wurden. Die beiden obersten

Optionen weisen keinen Wert in der Spalte auf. Grund ist, dass dieser Parameter auf Benutzerebene definiert wurde.

> In der Ribbon kann die Vererbung für einzelne Einstellungen gezielt deaktiviert werden!

# Sicherheitsstufen

Um gewährleisten zu können, dass Benutzer stets nur diejenigen Einstellungen beeinflussen können, auf die sie berechtigt sind, wird in den globalen Einstellungen eine Einteilung in Optionsgruppen vorgenommen. Durch eine Kategorisierung von Sicherheitsstufe 1 bis 5 können somit gleichgeartete Optionen zusammengefasst und dementsprechend den Benutzern zur Verfügung gestellt werden.

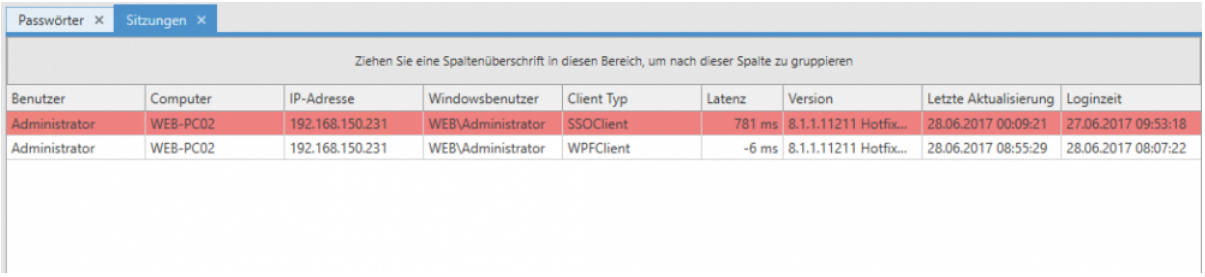



Wer genau welche Sicherheitsstufen ändern darf ist Teil der Benutzerrechte. Wie bei allen Rechten üblich erhält man dies entweder über globale Vererbung, über die Rolle oder als direkt auf den Benutzer gewährtes Recht.

# Administration

## Sitzungen

Über den Menüpunkt **Sitzungen** können alle Benutzer, welche mit der Datenbank verbunden sind, angezeigt werden. Diese Seite hat rein informativen Charakter, es können demnach keine Konfigurationen vorgenommen werden.



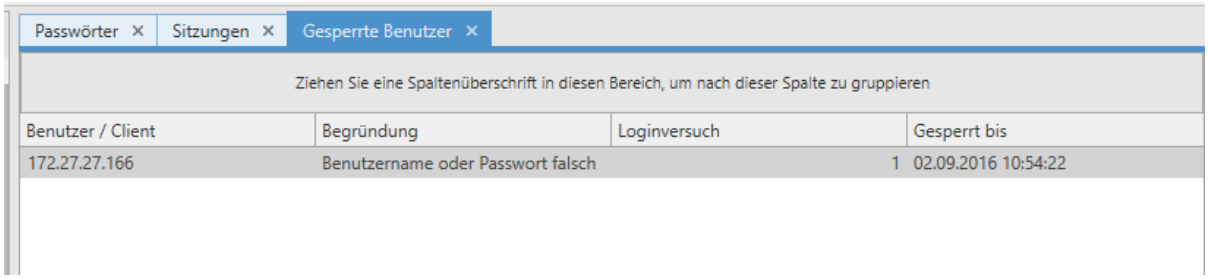

Die Sitzungsansicht starten im derzeit aktiven Modul in einem separaten Tab.

## Gesperrte Benutzer

Alle derzeit gesperrten Benutzer können ebenfalls abgerufen werden. Es gibt hierfür zwei Szenarien:

1. **Benutzername korrekt, Passwort falsch**: Der Benutzername wird angezeigt
2. **Benutzername falsch**: Der Client wird angezeigt

Darüber hinaus sind die Anzahl der versuchten Logins sowie die Dauer der jeweiligen Sperrung einsehbar.




## Standard Passwortrichtlinien

Sowohl für Benutzerpasswörter als auch für WebViewer Exporte können Passwortrichtlinien definiert werden, welche dann eingehalten werden müssen. Im folgenden Fall muss ein Benutzerpasswort mindestens der Richtlinie “Standard Passwort” entsprechen, um valide zu sein.

Standard Passwortrichtlinien

| Kategorie | Richtlinie | | |
|---|---|---|---|
| Benutzer Passwortrichtlinie | Standard Passwort | | |
| WebViewer Passwortrichtlinie | | | |

- Benötigte Benutzerrechte: Um Die Passwortrichtlinien für genannte Passwörter definieren zu können, existiert ein separates Benutzerrecht “Kann Kategorien der Passwortrichtlinien verwalten”

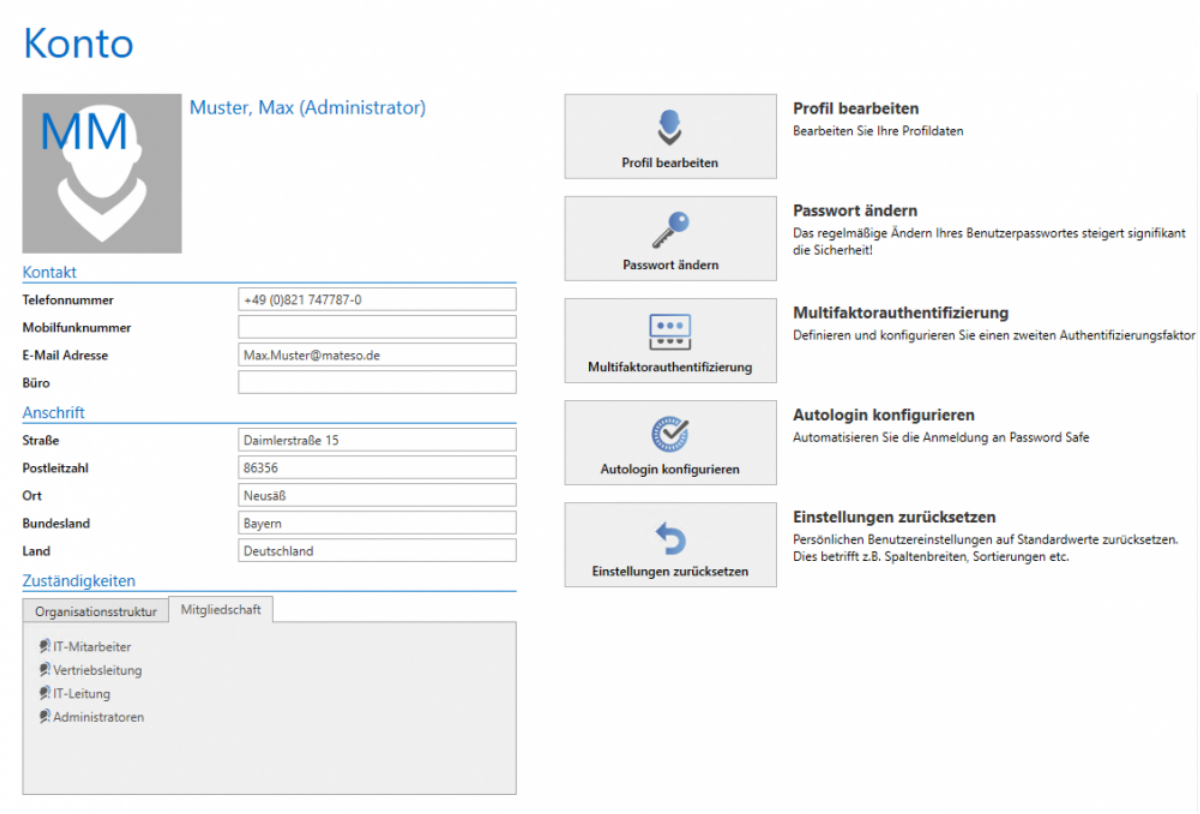
**Kategorie: Sicherheit**

- Kann persönliche Datensätze erstellen
- Kann Optionen der Sicherheitsstufe ändern
- Kann HTML WebViewer exportieren
- Kann globale Einstellungen bearbeiten
- Kann Passwortrichtlinien verwalten
- Ist Datenbank-Administrator
- Kann gesperrte Benutzer verwalten
- Kann Autologin verwalten
- Kann Datenbanksitzungen verwalten
- Kann Kategorien der Passwortrichtlinien verwalten
- Kann Aufzeichnungen einer Anwendung verwalten
- Kann Active Directory Profile verwalten
- Kann Besitzerrecht setzen

# Konto

## Was ist das Konto?

Im Konto können Benutzer die Konfiguration sämtlicher benutzerspezifischer Information vornehmen. Es ist zu beachten, dass im Falle des angewandten Master Key Verfahrens Benutzerdaten stets aus dem Active Directory erfolgen – eine Bearbeitung jener Informationen im Password Safe ist somit noch vorgesehen.




## Profil bearbeiten

Alle in den Rubriken Kontakt und Anschrift geführten Informationen können unter “Profil bearbeiten” definiert werden. Manche Bereiche des Profils überschneiden sich thematisch mit der **Benutzerverwaltung**. Diese Informationen sind in einem separaten Kapitel erläutert.

> Bei Benutzern, welche Master Key Modus aus dem AD importiert wurden, können keine Änderungen vorgenommen werden. Alle Informationen werden hier aus dem AD übernommen.

# Benutzerbild bearbeiten

Durch Klicken des Profilbildes kann ein neues Bild hinzugefügt, bzw. das vorhandene ersetzt oder gelöscht werden.

> Bei Benutzern, welche mit Hilfe des Master Key Modus aus dem AD importiert wurden, können keine Änderungen vorgenommen werden. Ist im AD ein Bild hinterlegt, so wird dieses übernommen.

# Passwort ändern

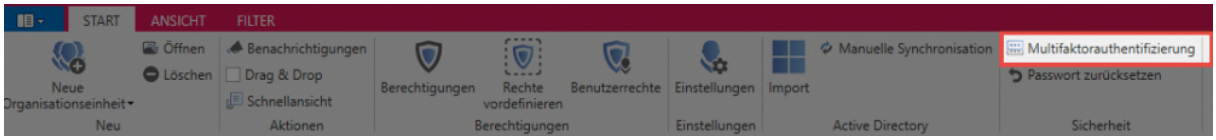
Es wird empfohlen, regelmäßig das Benutzerpasswort zu ändern. Will man ein neues Passwort nutzen, ist im Vorfeld die Eingabe des bisherigen Passworts erforderlich. Die Stärke des Passworts wird direkt dargestellt.

> Benutzer welche mit Hilfe des Master Key Modus aus dem AD importiert wurden, melden sich mit dem Domänenkennwort an. Daher kann hier kein Passwort konfiguriert werden.

> Die Stärke des Benutzerpasswortes kann durch die Administration durch die Vorgabe von Passwortrichtlinien vorgegeben werden. Mehr...

# Multifaktor Authentifizierung

Die Multifaktor Authentifizierung bietet zusätzlichen Schutz durch eine zweite Authentifizierung bei der Anmeldung über einen Hardware Token. Die Konfiguration erfolgt über die Ribbon im Bereich “Sicherheit”. Mehr...




# Autologin konfigurieren

Über diese Option kann die Anmeldung an Password Safe automatisiert werden. Zum Einrichten genügt es das Passwort zweimal anzugeben und zu speichern.

> ! Die automatische Anmeldung ist als sicherheitskritisch einzustufen. Es sollte bedacht werden, dass hierdurch auf alle Daten zugegriffen werden kann, wenn beispielsweise vergessen wird den Rechner zu sperren.

## Einstellungen zurücksetzen

Ein Klick auf diese Schaltfläche setzt alle Benutzerspezifischen Einstellungen wie z.B. die Spaltenbreite, Farbschema und dergleichen, auf die Standardwerte zurück.

## Offline-Synchronisation starten

Hat man Änderungen am Datenbestand vorgenommen und möchte nicht die nächste automatische Synchronisation abwarten, kann die Offline Synchronisation auch manuell gestartet werden. Die Synchronisation läuft hierbei im Hintergrund und wird über einen Statusbalken im Footer sowie im Icon dargestellt. Mehr…

# SSO Agent

## Was ist der SSO Agent?

Der SSO Agent ist für die automatische Eintragung von Anmeldedaten in Anwendungen zuständig. Auf diese Art und Weise können Anmeldungen ohne die Kenntnis um das Passwort durchgeführt werden, was besonders im Zusammenspiel mit dem Sichtschutz ein wertvolles Werkzeug sein kann. Es wird über das Berechtigungskonzept festgelegt, welche Benutzer einen Zugang nutzen sollen. Das Passwort bleibt dennoch verborgen, da die Eintragung durch den Password Safe durchgeführt wird.

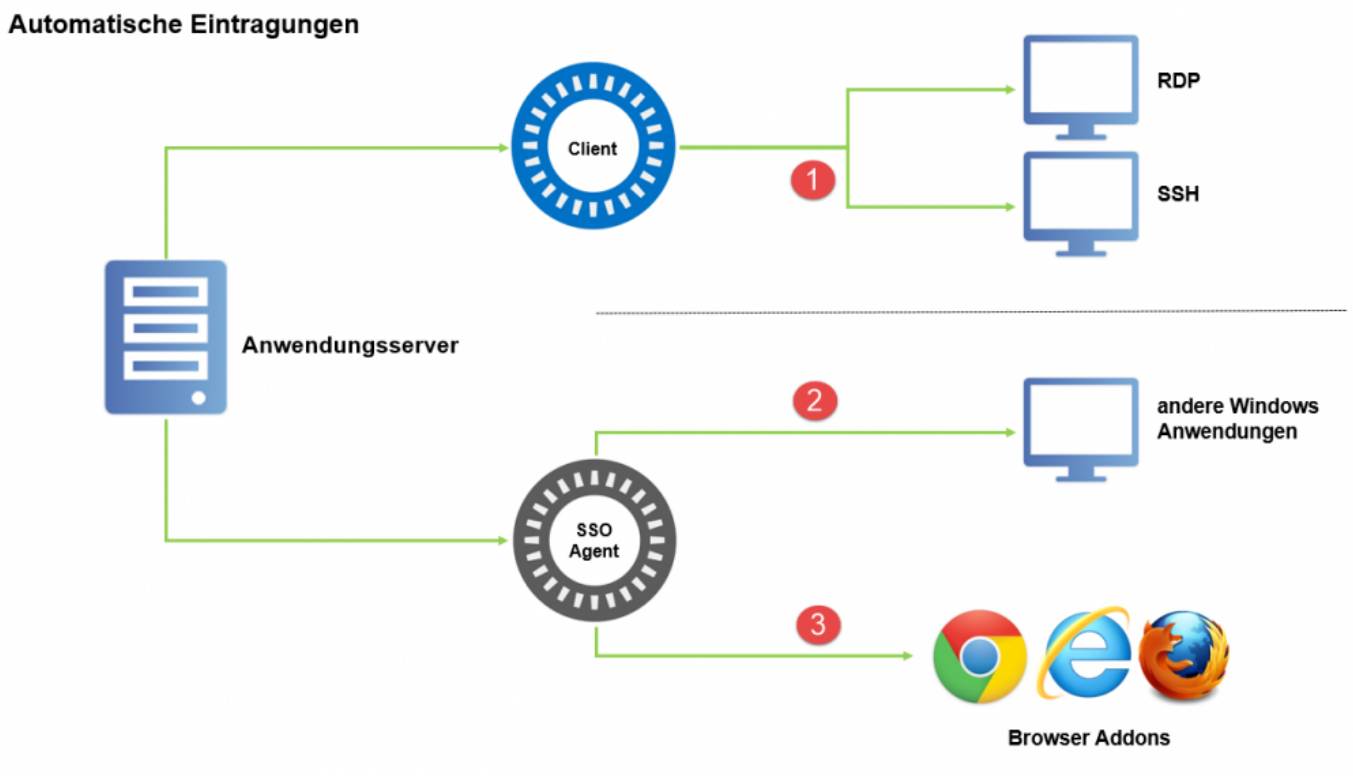
## Voraussetzungen

Der SSO Agent wird zusammen mit dem Password Safe Client installiert und kann von Usern dann (ausreichend Berechtigungen vorausgesetzt) benutzt werden. Eine separate Installation ist demnach nicht nötig. Es wird sowohl für den Client wie auch für den SSO Agent eine eigene Desktop Verknüpfung erstellt.

! Für das Erfassen von neuen Webanwendungen wird das Recht “Kann Webanwendungen erfassen” benötigt

## Funktionsweise

Die Funktionsweise des SSO Agents wird in nachfolgendem Schaubild erläutert.




Das automatisierte Starten von RDP- und SSH-Sessions (1) wird nicht über den SSO Agent gestartet. Hierfür werden Anwendungen im Password Safe Client erstellt und genutzt. Die Erstellung und Nutzung dieser Verbindungen sind im dementsprechenden Kapitel ausführlich erläutert.

Das automatische Starten von allen verbleibenden Verbindungsarten ist Aufgabe des **SSO Agents**. Es existieren die nachfolgend genannten Arten:

- **Eintragungen in Windows Anwendungen**: Neben den genannten RDP- und SSH-Sitzungen können auch andere Windows Anwendungen automatisiert werden (2). Ein wesentlicher Unterschied ist, dass die beiden genannten Verbindungen innerhalb eines separaten Tabs “embedded” errichtet werden können. Andere Anwendungen, wie z.B. VMware, werden wie gewohnt direkt gestartet (mehr…). Der SSO Agent übernimmt in diesem Fall die Kommunikation zwischen dem Anwendungsserver und den Windows Anwendungen.

- **Eintragungen an Websites**: Password Safe kann die Anmeldung an Websites automatisieren. Das bedeutet, dass man über die Addons die gewünschte Anmeldung einmal konfiguriert und zukünftig (analog zum Vorgehen bei der Nutzung von Favoriten) effizient nutzen kann. Der SSO Agent bildet hierbei die **Schnittstelle** (3) zwischen dem Anwendungsserver und den verfügbaren Browser Addons (Google Chrome, Internet Explorer und Mozilla Firefox).

Der Agent kann mehrere Datenbanken gleichzeitig ansteuern

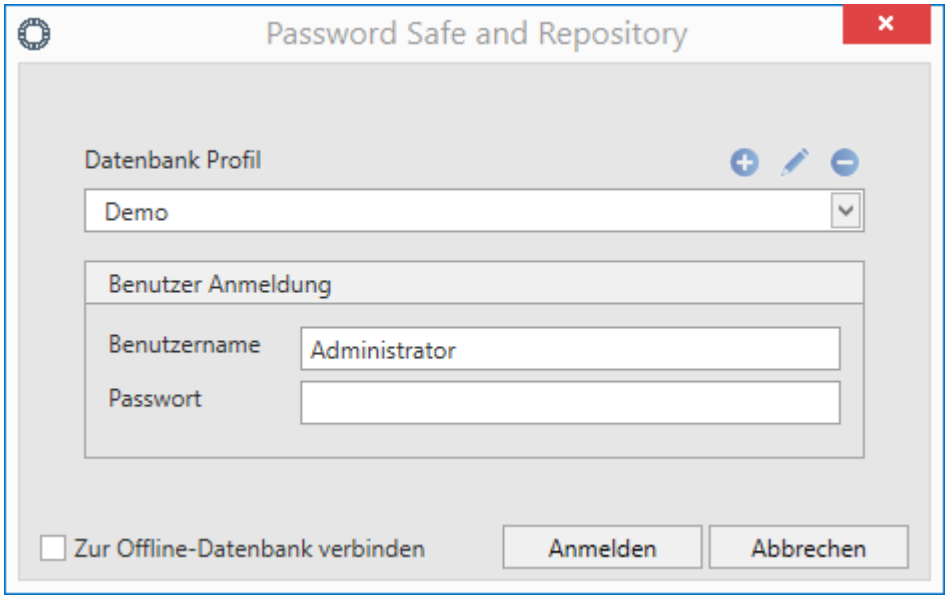
# Fazit

Da der SSO Agent direkt mit dem Anwendungsserver verbunden ist, können Eintragungen auch ohne den Hauptclient durchgeführt werden. Ausnahmen hierzu bilden RDP- und SSH-Verbindungen. Diese bleiben zwingend Teil des Clients. Der SSO Agent bildet somit eine schlanke Alternative für die Nutzung des Clients mit den beiden angesprochenen Einschränkungen. Selbstverständlich werden dennoch alle durchgeführten Arbeitsschritte Teil des Logbuches und sind stets nachvollziehbar.

# Konfiguration

## Starten des SSO Agents

Über die Desktop Verknüpfung, welche beim Installieren automatisch erstellt wird, kann der SSO Agent direkt gestartet werden. Die Anmeldedaten entsprechen den regulären Benutzerdaten des Client.

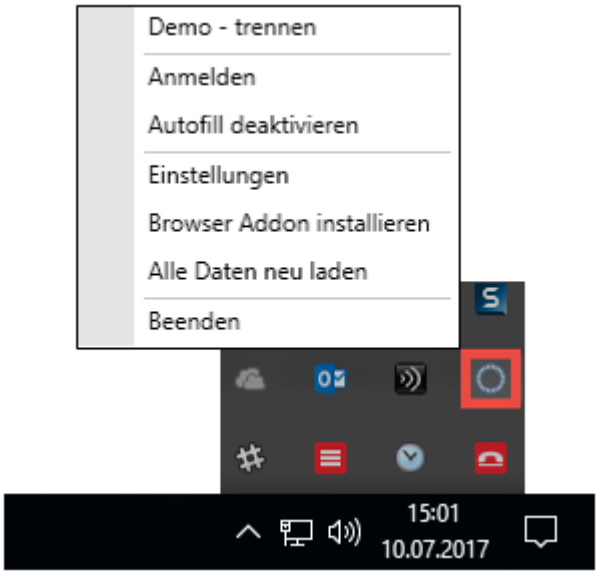



Zur Anmeldung wird zunächst die gewünschte Datenbank sowie die zugehörigen Anmeldedaten ausgewählt. Der SSO Agent stellt alle am Client konfigurierten Datenbanken zur Verfügung. Auch die Erstellung von Profilen ist wie gewohnt möglich, um die Verbindungsdaten zu bestimmten Datenbanken zukünftig effizient nutzen zu können.

> Der Agent greift auf die gleiche Konfigurationsdatei zu wie der Client. Alle Änderungen an Profilen wirken sich also auch auf den Client aus. Neue Profile können somit auch über den SSO Agent erstellt werden.

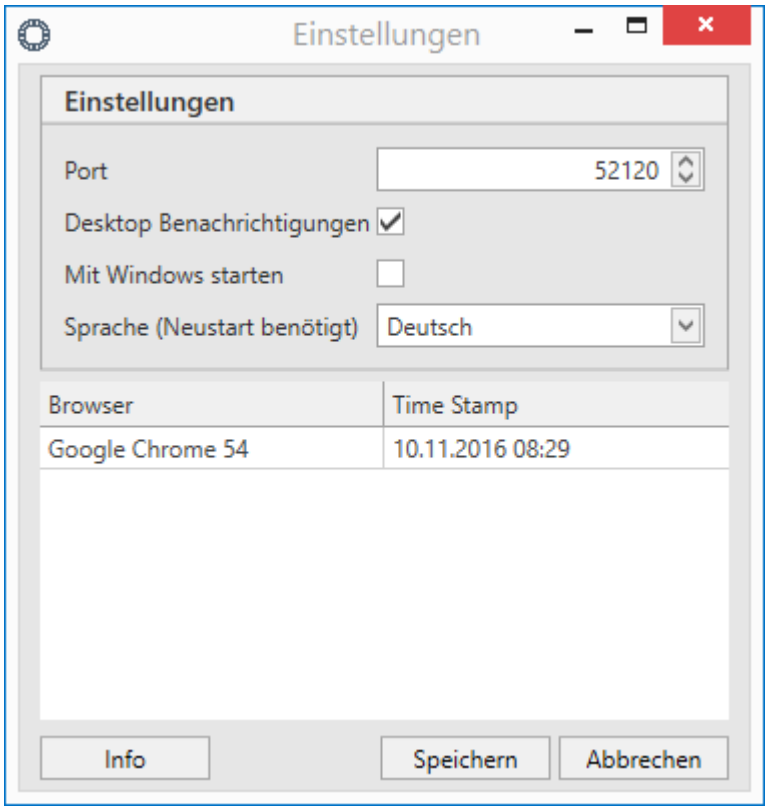
## Funktionen über das Kontextmenü

Nach der erfolgreichen Anmeldung läuft der SSO Agent vorerst im Hintergrund. Ein Kontextmenü kann über einen Rechtsklick auf das Icon im System-Tray geöffnet werden.




- **Trennen**: Verbindung zur Datenbank herstellen/trennen. (bei mehreren Datenbanken werden alle Verbindungen angezeigt)
- **Anmelden** ermöglicht die Anmeldung an einer weiteren Datenbank
- **Autofill deaktivieren / aktivieren** bietet die Möglichkeit, die automatische Eintragung temporär abzuschalten
- Über die **Einstellungen** können diverse Variablen definiert werden
- **Browser Addon installieren** startet die Installation des Google Chrome oder Mozilla Firefox Addons.
- **Mit Addon verbinden** ermöglicht die Kopplung von Addon und Agent (steht nur im Terminalserver Betrieb zur Verfügung)

### Einstellungen




- Der **Port** zur Verbindung mit der Datenbank muss in der Regel nicht geändert werden. Sollte er anderweitig belegt sein, kann er hier neu definiert werden. Wird der Port hier angepasst, muss er im Addon ebenso geändert werden.
- Im Terminalserver Betrieb kann über **Terminal Server Ports** eine Range definiert werden, aus welcher sich der Terminalserver zur Verbindung bedient. Der Standard ist hier 1000. Hier ist in der Regel keine Anpassung nötig. Ebenso kann im Terminalserver Betrieb die sogenannte **Terminal Server Kennung** ausgelesen werden. Es handelt sich hier um eine einzigartige ID, welche den Agent am Addon einwandfrei ausweist. Die Kennung muss bei der ersten Verbindung im Addon angegeben werden.
- Die **Desktop Benachrichtigungen** blenden diverse Informationen, wie z.B. das Eintragen von Daten, ein
- **Mit Windows starten** nimmt den SSO Agent in das Autostart Menü auf
- Im unteren Bereich wird aufgeführt, mit welchen Addons der SSO Agent derzeit verknüpft ist

# Der SSO Agent im Terminalserver Betrieb

Für den Terminalserver Betrieb muss zunächst ein Pairing stattfinden, bei welchem der SSO Agent mit den gewünschten Addons verbunden wird.

### Voraussetzungen

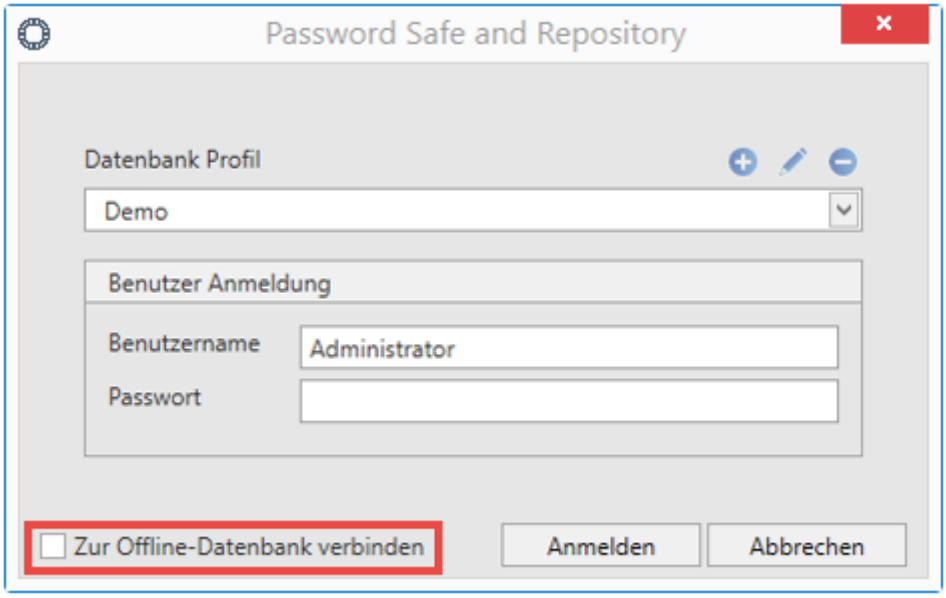
Vor dem Pairing muss sichergestellt sein, dass das gewünschte Addon installiert ist. Weiterhin muss der Terminalserver Dienst installiert sein. Dieser wird zusammen mit dem Client installiert.

### Pairing

Zunächst wird am Agent im Kontextmenü der Punkt **Mit Addon verbinden** gewählt. Im nächsten Fenster wählt man dann den gewünschten Browser aus, welcher sich daraufhin öffnet.
Nun erscheinen die Einstellungen des Addons. Hier ist in der Regel bereits die Terminalserver Kennung eingetragen. Es muss also nur noch bestätigt werden.

## Zusammenspiel mit Offline Datenbanken

Der SSO Agent kann auch Verbindungen zu Offline Datenbanken herstellen. Beim Login kann direkt auf die Offline Datenbank verbunden werden, sofern eine existiert. Besteht keine Serververbindung, wird direkt das Verbinden zur Offline Datenbank vorgeschlagen.



# Addons

## Was sind Addons?

Will man direkt aus dem Browser auf die Datenbank zugreifen benötigt man ein Browser Addon für die Verbindung zum SSO Agent. Der Agent ist über das Icon im System Tray aufrufbar, wohingegen das Addon im Menübereich des jeweiligen Browsers zu finden ist. Verfügbar sind die Addons aktuell für Mozilla Firefox, Google Chrome und Microsoft Internet Explorer. Die Addons sind zuständig für die automatische Eintragung an Webseiten.


> Die Eintragungen werden (unter anderem) durch Anwendungen durchgeführt. Die Erstellung dieser werden im Folgekapitel erläutert.

## Installation

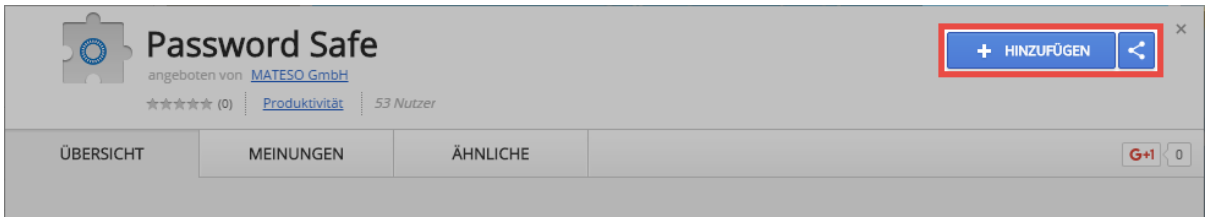
Die Addons für Google Chrome und Mozilla Firefox können direkt über den SSO Agent herunter geladen werden. Über einen Rechtsklick auf das Icon wird das Kontextmenü geöffnet. Nach einem weiteren Klick auf **Browser Addons installieren** kann das gewünschte Addon ausgewählt werden. Da die eigentliche Installation der Addons unterschiedlich abläuft, wird nachfolgend separat darauf eingegangen:

### Internet Explorer

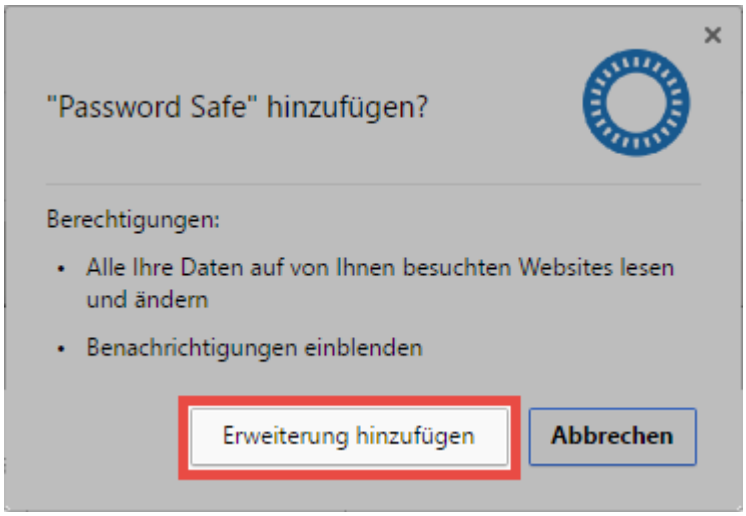
Das Internet Explorer Addon kann direkt zusammen mit dem Client installiert werden. Hierfür gibt es im Installer eine entsprechende Option, welche standardmäßig aktiviert ist.

### Google Chrome

Die Installation des Google Chrome Addons wird über den SSO Agent gestartet. Man gelangt direkt in den Google Store, wo über **Hinzufügen** die Installation gestartet wird.




Das Addon wird nun installiert und im Browser das Icon hinzugefügt.




### Firefox

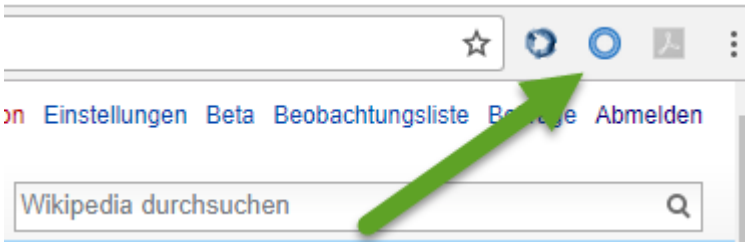
Das Firefox Addon kann unter folgendem Link herunter geladen werden:

Password Safe Addon für Firefox

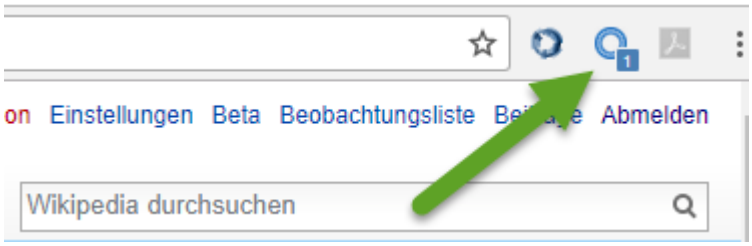
Nach dem Download wird das Addon einfach per Drag and Drop in den Browser gezogen. Nach Bestätigung einer Sicherheitsfrage wird dieses installiert und in der Menüleiste ein Icon erstellt.

# Verbindung mit dem SSO Agent

Sind die Punkte Installation des Addons und Verbindung mit dem SSO Agent abgeschlossen, öffnet man den gewünschten Browser. Es erscheint ein Fenster, in dem man die Sicherheit der Verbindung bestätigt. Über einen einfachen Klick erfolgt das Pairing. Das Addon ist ab diesem Zeitpunkt berechtigt, Daten vom SSO Agent abzufragen. Ab diesem Zeitpunkt ist dann im gewünschten Browser ein **neues Icon** sichtbar:




Wird das Icon in dieser Form dargestellt bedeutet dies, dass das Addon zwar installiert ist, jedoch aktuell noch keine Verbindung zum SSO Agent besitzt. Erst **nach der Anmeldung am Agent** (über das Icon im System Tray) erhält man eine Windows Benachrichtigung über die erfolgreiche Anmeldung. Besteht die Verbindung zum Agent wird direkt am Icon die **Anzahl der für die aktuelle Internetseite verfügbaren Datensätze** angezeigt.




Eine tiefgestellte “0” bedeutet, dass man am Agent erfolgreich angemeldet wurde.

# Einstellungen

Alle Einstellungen welche die Addons betreffen werden zentral am Client gesetzt. Über das System der Benutzereinstellungen können diese global, pro Organisationseinheit oder pro Benutzer gesetzt werden. In der Kategorie **SSO** sind folgende Optionen zu finden, welche sich direkt auf die Addons auswirken:

- **Browser Addons :Loginmasken automatisch absenden** sorgt dafür, dass nach dem Eintragen der Zugangsdaten direkt eine Anmeldung erfolgt. Es ist also kein manueller Klick nötig
- Über **Browser Addons: Loginmasken automatische befüllen** wird erreicht, dass die Zugangsdaten ohne Rückfrage eingetragen werden, wenn eine Webseite erkannt wird.

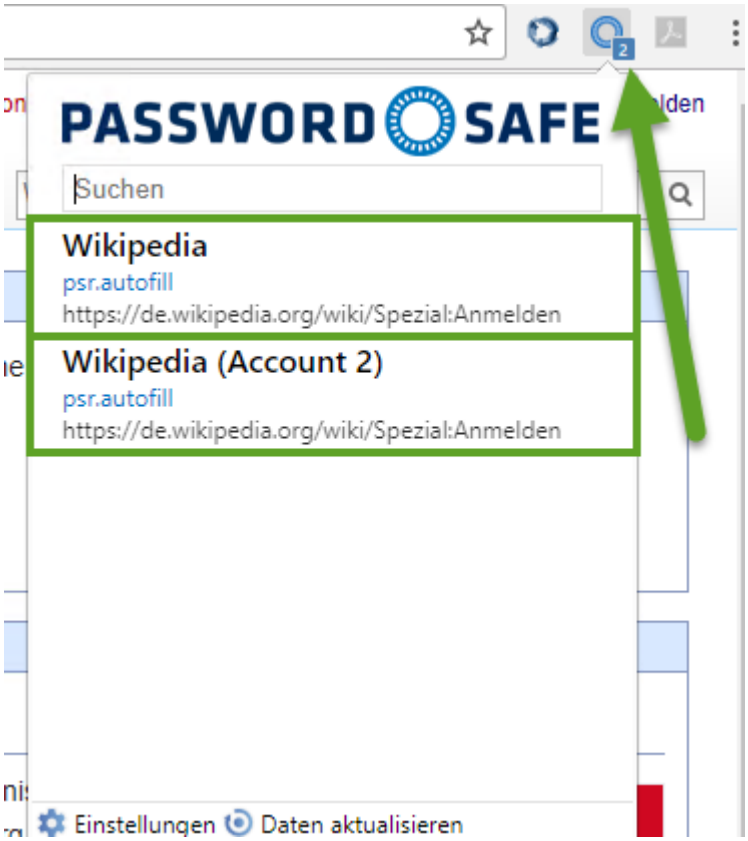
Ebenso wirkt sich die Option **Standardbrowser** auf die Addons aus. Hier wird festgelegt in welchem Browser die Webseiten aus dem Client heraus geöffnet werden.

Die oben genannten Einstellungen können auch pro Datensatz gesetzt werden. Weiterführende Infos sind hier zu finden: “

# Arbeiten mit den Addons

> Ein Datensatz kann nur dann für Eintragungen genutzt werden, wenn dieser ein Formularfeld vom Typ “Url” besitzt

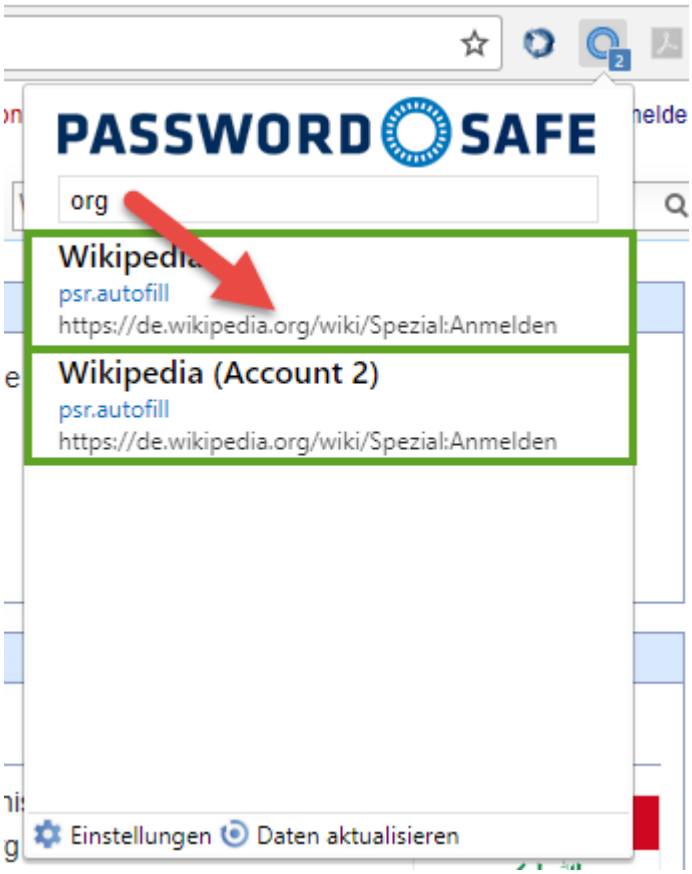
Die im vorherigen Kapitel erwähnte, tiefgestellte Zahl ist einerseits nur bei einer aktiven Anmeldung verfügbar, andererseits sagt diese bereits viel über die **Anzahl der möglichen Eintragungen** aus. Wenn hier z.B. eine “2” angezeigt wird, kann man über das Icon direkt denjenigen Account auswählen, mit dem man sich anmelden möchte.




Voraussetzung war bisher immer, dass man manuell über den Browser genau zu der Webseite navigiert, welche man auch nutzen möchte. Diese Navigation kann auch durch den Password Safe übernommen werden – wie im nachfolgenden Kapitel beschrieben wird.

### Suche und Navigation

Aktuell wurde immer davon ausgegangen, dass der Benutzer manuell zu derjenigen Seite navigiert, für die er eine automatische Eintragung nutzen möchte. Diese Art zu Arbeiten ist möglich, jedoch nicht ausreichend komfortabel. Das Addon ist analog zur Vorgehensweise bei Lesezeichen nutzbar. Über das Suchfeld kann direkt auf Basis der Datensätze in der Datenbank gesucht werden. Voraussetzung ist nach wie vor, dass der Datensatz eine URL besitzt.

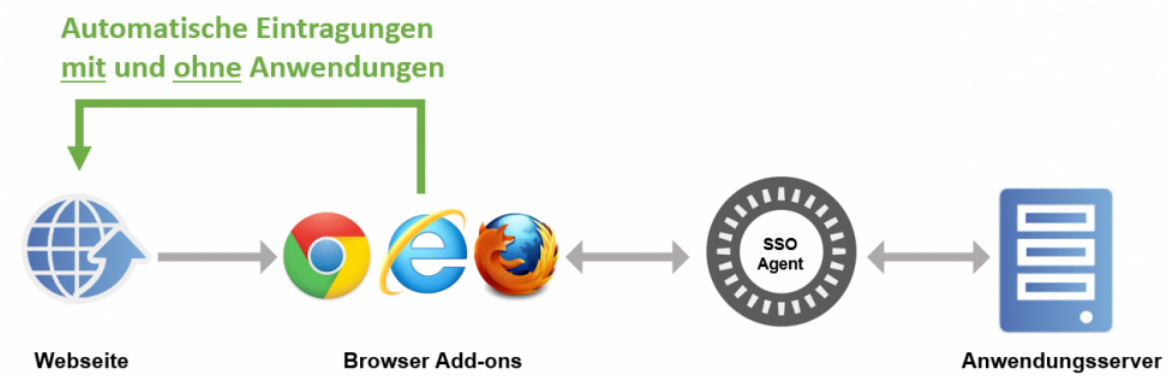



Im Bild ist ebenso ersichtlich, dass neben dem Namen des Datensatzes (Wikipedia) auch ebenso die URL durchsucht wird. Die den Suchkriterien entsprechenden Treffer werden angezeigt und können direkt über die Pfeiltasten oder die Maus selektiert werden. Die gewählte Internetseite wird in einem separaten Tab geöffnet.

# Anwendungen

## Was sind Anwendungen?

Viele Webseiten können ohne weitere Konfiguration befüllt werden. Mittels Scannen der Website werden gezielt eintragungsfähige Felder gesucht, in die dann Benutzername und Passwort eingetragen werden. Ein weiterer Prozess ist demnach nicht notwendig. Bei denjenigen Webseiten, welche nicht direkt befüllt werden können, muss manuell eine Anwendung erstellt werden. Dies entspricht einer Arbeitsvorschrift welche genau definiert, welche Informationen in welche Zielfelder eingetragen werden sollen. Das vollständige Skript, welches die Zuweisung beschreibt, nennt man **Anwendung**.




Das Schaubild beginnt mit der Navigation des Benutzers zu einer Webseite. Es wird nun (auf Umwegen über das Addon und den SSO Agent) am Anwendungsserver geprüft, ob für diese Seite Datensätze hinterlegt sind, auf die der aktuell angemeldete Benutzer berechtigt ist. Wenn dies der Fall ist, werden die für die Anmeldung erforderlichen Informationen verschlüsselt bis zum Browser Addon versandt. Erst am Addon wird das Passwort kurz vor der Eintragung entschlüsselt. Bei der Eintragung selbst existieren zwei Arten, die **Eintragung ohne Anwendung** und die **Eintragung mit Anwendung**.

### Eintragungen ohne Anwendung

Bei den meisten Webseiten reicht die Eintragung ohne die Nutzung von Anwendungen aus, da die Felder direkt richtig zugewiesen werden können (Mapping). Bei aufgerufenen Webseiten wird im Hintergrund geprüft, ob eine Loginmaske gefunden wurde. Anhand der URL wird nun geprüft, ob es in den verbundenen Webseiten Datensätze gib, welche zur Seite passen. Hierbei muss lediglich der Hostname inkl. Endung wie .de und .com übereinstimmen. Wenn der angemeldete Benutzer auch auf diesen Datensatz berechtigt ist, werden die Daten nun vom SSO Agent abgefragt. **Wichtig: Bis zu diesem Zeitpunkt hat das Addon keinerlei Kenntnis von Passwörtern!**. Anschließend werden die Daten eingetragen. Hierbei gilt, dass der Benutzername in das erste auf der Seite auffindbare Benutzernamensfeld übermittelt wird. Auch das Passwort wird in das erste auf der Seite auffindbare

Passwortfeld eingetragen. Sofern automatisches Anmelden in den Einstellungen aktiv ist, wird auch das Klicken des Anmeldebuttons direkt ausgeführt.

# Eintragung mit Anwendung

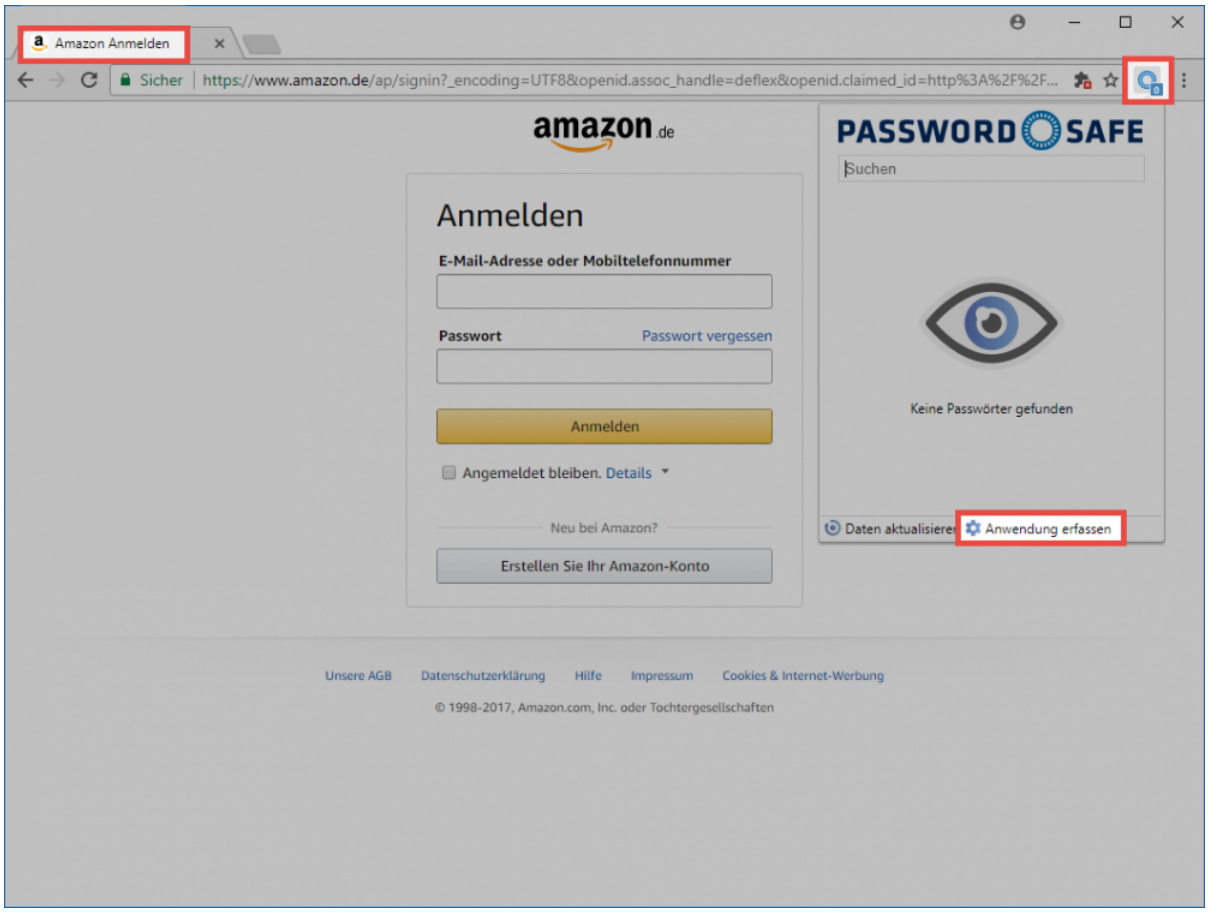
Bei manchen Webseiten ist die Erkennung der einzutragenden Felder nicht automatisiert möglich. Für solche Fälle ist die Erstellung einer Anwendung nötig. Auch wenn mehr als zwei Felder übergeben werden sollen, ist es nötig eine Anwendung zu erzeugen. Mit “Anwendung” ist hierbei eine Arbeitsanweisung gemeint, anhand derer die Felder befüllt werden sollen. Es geht also um die Zuweisung von Feldern aus dem Datensatz zu dem zugehörigen Feld auf der Webseite. Dieses Mapping muss nur einmal konfiguriert werden. Die Anwendung ist fortan für die Eintragung der Daten in die Felder der Webseite zuständig. Im nachfolgenden Beispiel wird die Eintragung aus dem Client heraus vorgenommen. Dies ist natürlich auch über die Browser Addons analog möglich. Die Vorgehensweise bleibt die gleiche.


Technisch wird anhand der URL geprüft, ob der Datensatz zur Seite passt. Lediglich der Hostname inkl. Endung (“.de” und “.com”) müssen hierbei übereinstimmen.

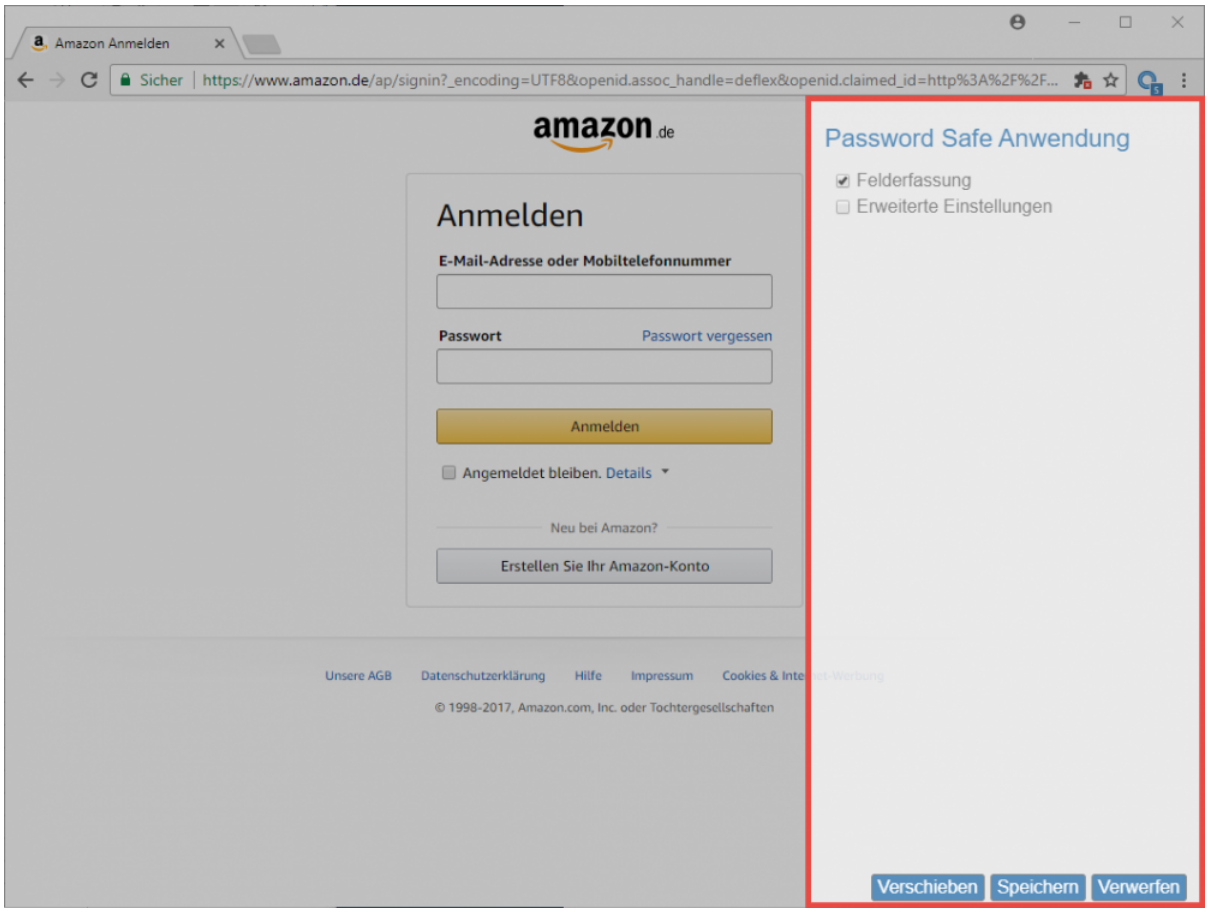
# Anwendungen erfassen

> ! Zum Erfassen von Anwendungen ist das Benutzerrecht **Kann neue Anwendungen vom Typ Web anlegen** vorausgesetzt

Falls die Anmeldemaske einer Webseite nicht automatisch befüllt werden kann, muss eine Anwendung manuell erfasst werden. Zum Erfassen wird zunächst die gewünschte Webseite aufgerufen. Anschließend wird über das Icon das Addons aufgerufen. Hier ist dann der Menüpunkt **Anwendung erfassen** zu finden.



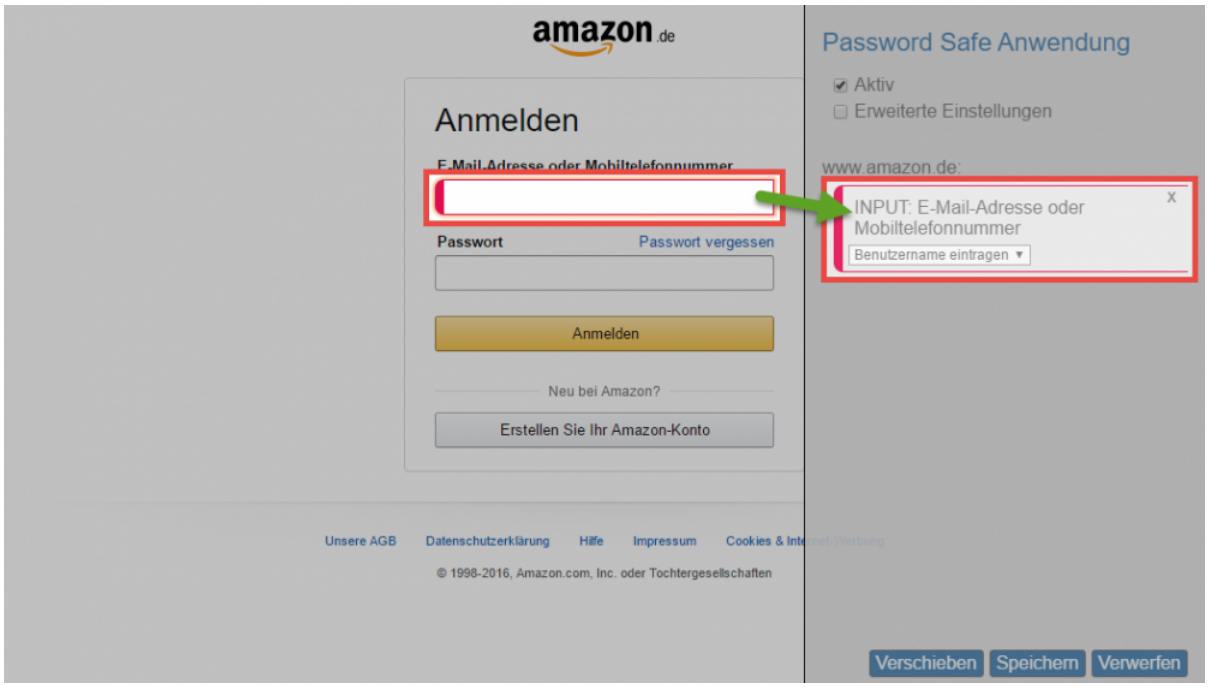

Nun öffnet sich ein modales Fenster. Hier wird nun die eigentliche Anwendung angelegt.



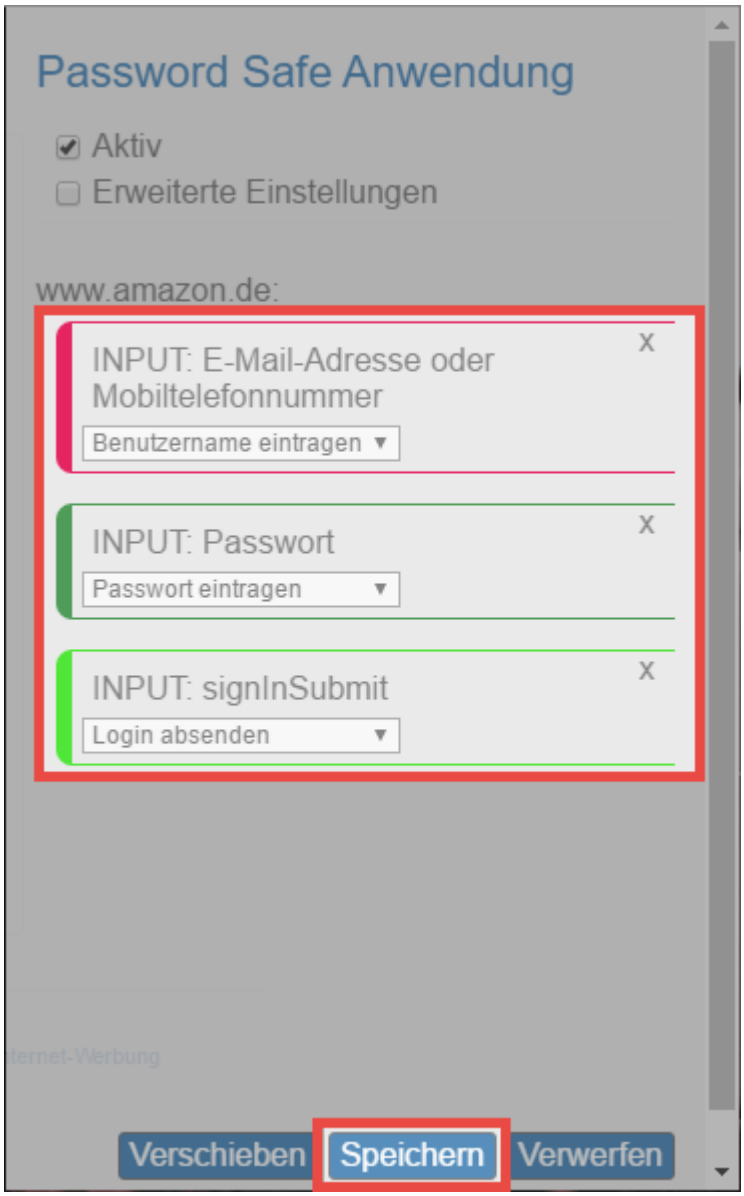

Folgende Optionen stehen zur Auswahl:

- Die Schaltfläche **Felderfassung** ermöglicht das Aussetzen der Felderfassung
- Über **Erweiterte Einstellungen** lässt sich für jedes Feld separat eine Verzögerung bei der Eintragung der Daten festlegen. Dies ergibt Sinn, wenn auf träge agierenden Webseiten anderweitig die Eintragung nicht sauber ablaufen würde.
- Über **Verschieben** kann die Position des modalen Fensters geändert werden, wenn durch dieses das Anmeldefenster verdeckt ist

Zum Erfassen wird in der Webseite in das erste auszufüllende Feld geklickt. Dieses wird direkt in die Liste im modalen Fenster übernommen. Zur besseren Identifikation werden zusammengehörige Felder farblich markiert.




Im Feld selbst wird der Feldtyp (z.B. INPUT) und die Feldbeschriftung angezeigt. Zudem wird direkt eine Aktion vorgeschlagen, welche zum Feldtyp passt, wie z.B. das Eintragen des Benutzernamens. Auf Wunsch kann die Aktion selbstverständlich angepasst werden. Sind alle Felder erfasst, wird nochmals geprüft ob die Aktionen korrekt sind. Abschließend kann dann die Anwendung gespeichert werden.

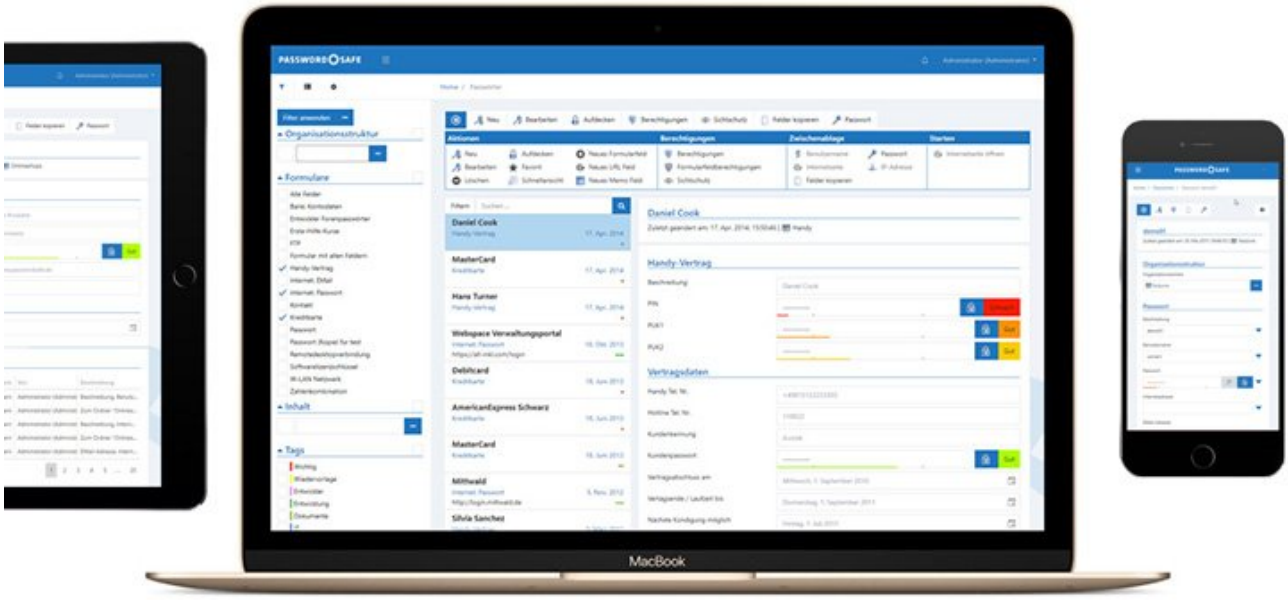



Die gespeicherte Anwendung steht nun zur Benutzung bereit und kann über das Addon genutzt werden.

# WebClient

## Was ist der WebClient

Mit der Password Safe Version 8.3.0 wird der bisherige WebAccess durch den **WebClient** ersetzt. Durch den komplett neu entwickelten **WebClient** wurde die Basis für eine stetige Erweiterung des Funktionsumfangs gesetzt. Das angestrebte Ziel ist es, den Funktionsumfang des Clients komplett auch im WebClient bereitzustellen. Der **WebClient** wird also ständig erweitert werden.
Alle aktuell verfügbaren Funktionen sind im Kapitel **Funktionsumfang** ersichtlich.




Der **Password Safe WebClient** ermöglicht plattformunabhängigen Zugriff auf die Datenbank per Browser. Es ist irrelevant, ob mit Microsoft Windows, macOS oder Linux gearbeitet wird, lediglich JavaScript muss unterstützt werden. Da der **Password Safe WebClient** responsive entwickelt wurde, kann er zudem auch auf allen mobilen Geräten wie Tablets und Smartphones benutzt werden.

Der **WebClient** orientiert sich sowohl optisch als auch in Bezug auf die Bedienung am Password Safe Client. Wie gewohnt können Benutzer nur auf diejenigen Daten zugreifen, für die sie auch berechtigt sind. Die Installation wird im Kapitel **Installation WebClient** beschrieben.

> Obwohl der WebAccess durch den WebClient obsolet geworden ist, kann er dennoch mit dem Server der Version 8.3.0 weiter betrieben werden.

# Funktionsumfang

Durch den **WebClient** wurde die Basis für eine stetige Erweiterung gesetzt. Der jeweils aktuelle Funktionsumfangs wird an dieser Stelle erläutert. Der Übersichtlichkeit halber, werden die jeweiligen Module in eigenen Unterkapitel behandelt.

- Passwort Modul
- Tag Modul

# Passwort Modul

Im **Passwort Modul** stehen aktuell folgende Funktionen zur Verfügung:

- Anlegen
- Löschen
- Editieren
- Passwort aufdecken
- Schnellsuche
- Formularfelder hinzufügen/bearbeiten
- Mit Tags versehen
- Duplizieren
- Verschieben
- Schnellansicht (Passwörter automatisch aufdecken)
- Favoriten
- Filter
- Struktur-Filter
- Berechtigen / Rechte bearbeiten
- Formularfeldberechtigungen
- Passwort verdeckt ändern
- Passwort-Generator mit Richtlinien
- In Zwischenablage kopieren
- Internetseite öffnen
- Logbuch ansehen
- Siegel/Sichtschutz anzeigen
- Deutsch/Englisch
- Benutzerpasswort ändern, falls „Passwort bei nächster Anmeldung ändern“ aktiv
- Benachrichtigungen anzeigen
- Tastaturnavigation
    - ALT+Q: Schnellsuche
    - ALT+N: Neuer Datensatz
    - ALT+S: Speichern in Edit/Neu-Ansicht
    - ALT+DEL: Selektierten Datensatz löschen
    - Pfeil nach oben/unten in Liste: Auswahl ändern
    - Pfeil nach rechts/links in Liste: Seite nach vorn/zurück
    - Enter: Selektierten Datensatz öffnen

# Tag Modul

Das **Tag Modul** stellt aktuell folgende Funktionen bereit:

- Anlegen
- Löschen
- Editieren

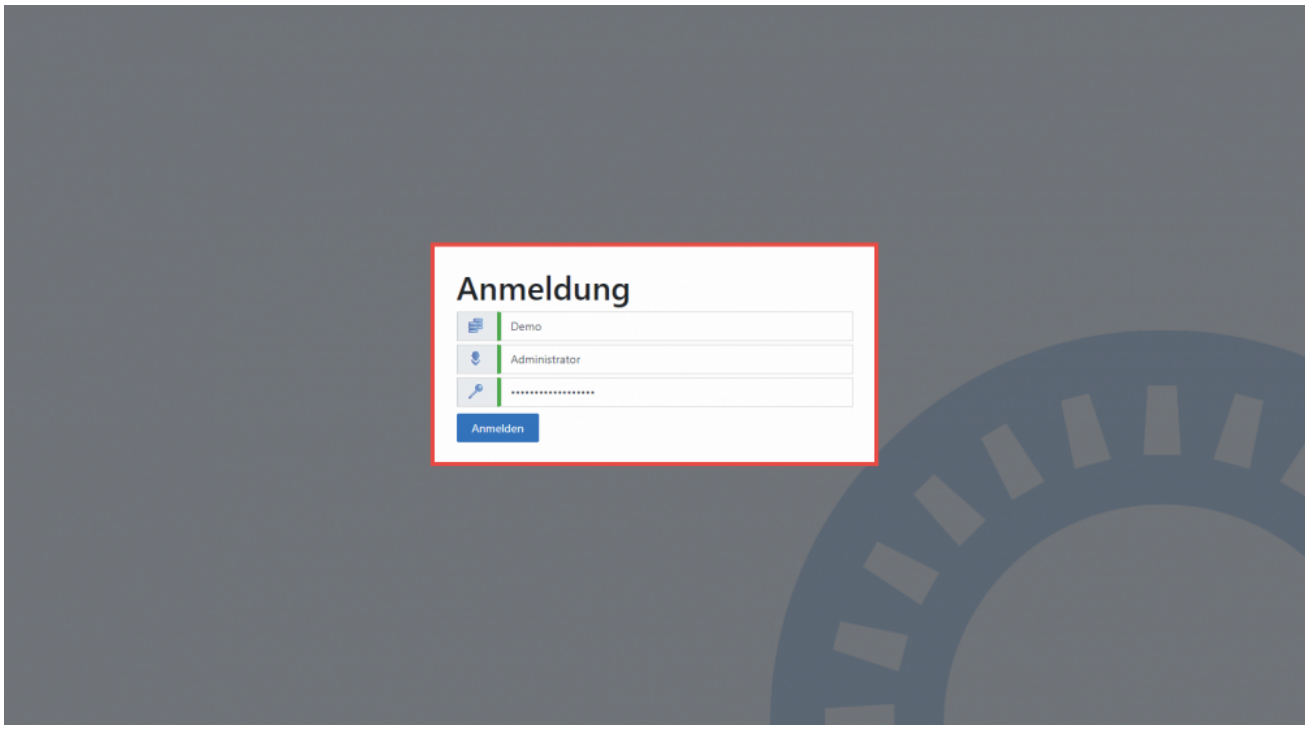
# Bedienung

Die Bedienung des WebClients wurde soweit als möglich an die Bedienung des Password Safe Clients angelehnt. Dennoch gibt es einige Unterschiede zu beachten, welche hier geschildert werden.

## Login

Am WebClient gibt es keine Datenbank Profile. Es stehen alle Datenbanken welche für den WebClient freigegeben wurden zur Verfügung. Zum Login müssen also folgende Infos eingegeben werden:

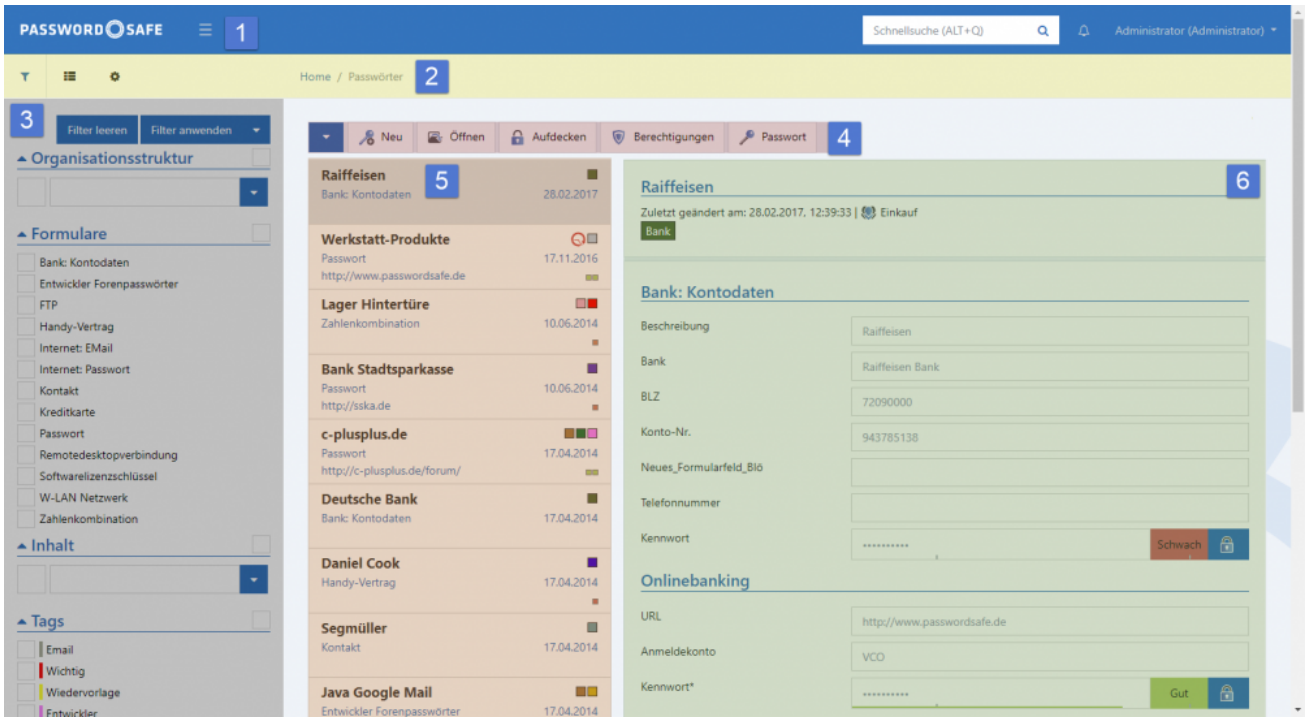
**Datenbankname**
**Benutzername**
**Passwort**




Nach erfolgreichem Login wird der zuletzt verwendete Datenbankname sowie der zuletzt angemeldete Benutzer gespeichert. Somit genügt bei der nächsten Anmeldung das Passwort.

## Aufbau

Der WebClient ist in mehrere Bereiche aufgeteilt, welche hier Beschrieben werden sollen.




## 1. Header

Der Header stellt einige essentielle Funktionen bereit.

## 2. Navigationsleiste

In der Navigationsleiste kann zwischen verschiedenen Ansicht hin und her geschaltet werden. Ebenso lassen sich hier die Einstellungen aufrufen.

## 3. Filter bzw. Strukturbereich

Wie auch am Client, kann zwischen Filter und Struktur gewählt werden.

## 4. Menüleiste

Die vom Client bekannte Ribbon wurde im WebClient durch eine Menüleiste ersetzt.

## 5. Listenansicht

In der Listenansicht sind die aktuell über den Filter selektierten Datensätze zu sehen.

## 6. Lesebereich

Der Lesebereich zeigt die Details zum jeweils selektierten Element dar.

# Header

Der Header stellt folgende Funktionen bereit.


### 1. Logo

Das Logo entspricht einem Homebutton. Man gelangt also immer wieder auf die standardmäßige Ansicht.

### 2. Filter ein- und ausblenden

Wie auch am Client kann der Filter bzw. Strukturbereich ein- und ausgeblendet werden.

### 3. Schnellsuche

Die Schnellsuche ist an die Schnellsuche biete die gleichen Funktionen wie die Schnellsuche des Clients. Sie durchsucht die komplette Datenbank in allen Feldern, außer dem Passwortfeld.

### 4. Benachrichtigungen

Hier wird man über eingehende Nachrichten informiert. Ebenso kann man über einen Klick die Nachrichten abrufen.

### 5. Account

Unter dem Account ist der aktuell angemeldete Benutzer zu sehen. Über einen Klick darauf kann man sich abmelden.

# Navigationsleiste

Die Navigationsleiste stellt folgende Funktionen bereit.


### 1. Filter

Hierüber kann die Ansicht auf den Filter umgeschaltet werden.

### 2. Struktur

Schaltet vom Filter auf die Struktur.

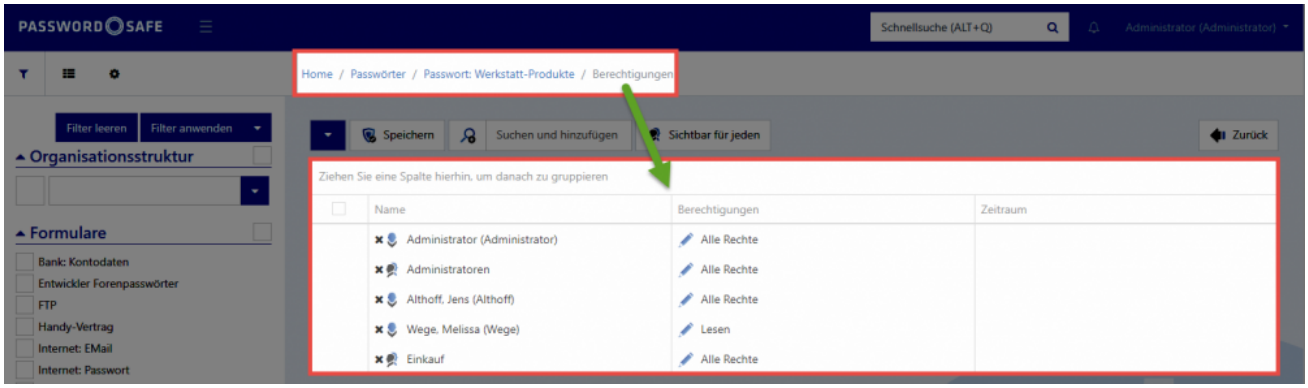
### 3. Einstellungen

Blendet die Eintellungen ein.

### 4. Bread Crumbs

Die sogenannten Bread Crumbs stellen eine sekundäre Navigation innerhalb des WebClients dar. Sie bieten die Möglichkeit, den Weg zurück zum ursprünglich ausgewählten Element zu finden oder andere Ebenen schnell zu erreichen. Die Bread Crumbs stellen also den logischen Pfad bis hin zur aktuellen Position dar.

#### Beispiel




Hier wurde von der Startseite, im Modul Passwörter, in das Passwort “Werkstatt-Produkte” und schlussendlich auf dessen Berechtigungen navigiert. Die ersten drei Ebenen sind blau markiert und fungieren somit als Links. Über einen Klick auf **Passwörter** gelangt man also wieder zurück in das

Passwort Modul. Ein Klick auf **Passwort: Werkstatt-Produkte** bringt den Anwender zurück auf das Passwort selbst.

# Filter- bzw. Strukturbereich

Wie auch am Client, kann zwischen Filter und Struktur gewechselt werden. Hierfür stehen in der Navigationsleiste folgende Buttons bereit:


### 1. Filter

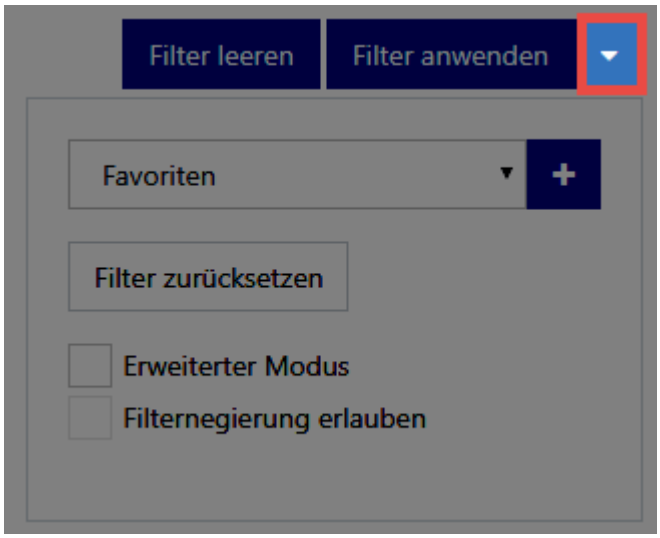
Der Filter im WebClient ist an den Filter der Clients angelehnt. Daher soll hier lediglich auf die WebClient spezifischen Eigenschaften eingegangen werden.

#### Bedienung des Filters

Die Bedienung des **WebClient Filters** unterscheidet sich kaum von der des **Client Filters**. Es ist lediglich zu beachten, dass die Schaltflächen **Filter leeren** und **Filter anwenden** über dem Filter stehen. Ebenso findet man direkt über dem **WebClient Filter** die Möglichkeit diesen zu konfigurieren.

#### Konfiguration des Filters

Die Konfiguration des Filters kann über folgende Schaltfläche eingeblendet werden:




Hier kann man sowohl neue **Filtergruppen hinzufügen** als auch den aktuellen **Filter zurücksetzen**. Über den **erweiterten Modus** erhält man die Möglichkeit einzelne Filtergruppen zu löschen oder zu verschieben. Ebenso kann die **Filternegierung erlaubt** werden.

### 2. Struktur

Die Struktur lässt absolut genau wie die des Clients bedienen.

# Menü

## Was ist das Menü?

Die vom Client bekannte Ribbon wurde im WebClient durch ein Menü ersetzt. Somit stellt das Menü das zentrale Bedienelement des WebClients dar. Die innerhalb des Menüs verfügbaren Funktionen richten sich dynamisch nach den derzeit verfügbaren Aktionen. Je nachdem in welcher Ansicht man sich gerade befindet, sind also unterschiedliche Aktionen möglich.

## Menüleiste

Das Menü kann zwei Ausprägungen annehmen. In der Regel wird die **Menüleiste** angezeigt welche die **wichtigsten Funktionen** darstellt. Exemplarisch soll das am Beispiel des Passwort Moduls verdeutlicht werden.


### 1. Menü erweitern

Über diese Schaltfläche kann das Menü maximiert werden

### 2. Neu

Hierüber kann der Assistent zum Anlegen eines neuen Datensatzes aufgerufen werden.

### 3. Öffnen

Stellt das selektierte Passwort im Lesebereich mit allen Details dar.

### 4. Aufdecken

Blendet das Passwort ein.

### 5. Berechtigungen

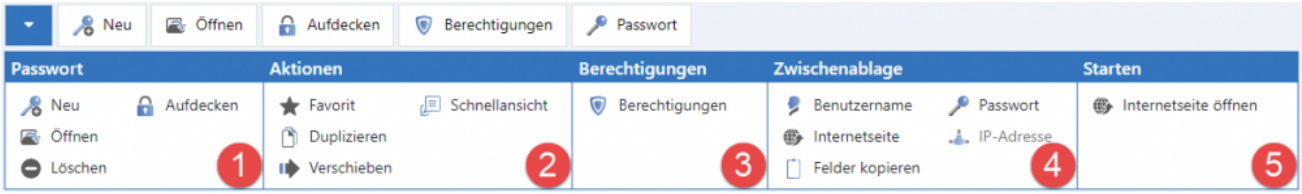
Über diesen Button werden die Rechte des Datensatzes konfiguriert.

### 6. Passwort

Übernimmt das Passwort in die Zwischenablage

# Erweitertes Menü

Wird das Menü – wie oben bereits erläutert – **maximiert**, stehen **alle Funktionen** zur Verfügung. Die Funktionen der Menüleiste wiederholen sich hier. Das Menü ist in mehrere Bereiche unterteilt. Diese entsprechen 1 zu 1 den Bereichen aus der Ribbon des Clients.




In unserem Beispiel stellt sich das Menü wie folgt dar:

### 1. Passwort

Dieser Bereich bietet weitere Aktionen zum bearbeiten von Passwörtern. Beispielsweise das **Öffnen** oder auch **Löschen**.

### 2. Aktionen

Über die Aktionen kann das Passwort beispielsweise als **Favorit** markiert oder auch **Dupliziert** werden.

### 3. Berechtigungen

Dieser Bereich bietet keine weiteren Funktionen als das Öffnen der Berechtigungen.

### 4. Zwischenablage

In diesem Bereich kann man alle verfügbaren Felder in die Zwischenablage übernehmen

### 5. Starten

Soll eine Webseite aufgerufen werden, so ist das hier möglich.

> Wie schon geschildert ist das Menü dynamisch und tritt somit in verschiedensten Ausprägungen auf. Die Grundfunktion ist jedoch immer gleich: In der Menüleiste sind die Grundfunktionen zu finden, im erweiterten Menü dann alle Funktionen.

# Listenansicht

## Was ist die Listenansicht

Das Zentrale Element zur Navigation im WebClient ist die Listenansicht, welche die gefilterten Elemente übersichtlich darstellt. Da die Listenansicht des WebClients die gleichen gleichen Funktionen wie die Listenansicht des Clients zur Verfügung stellt, soll an dieser Stelle auf das Kapitel **Listenansicht** verwiesen werden.


## Besonderheiten

In folgenden Punkten unterscheidet sich die Listenansicht von der des Clients:

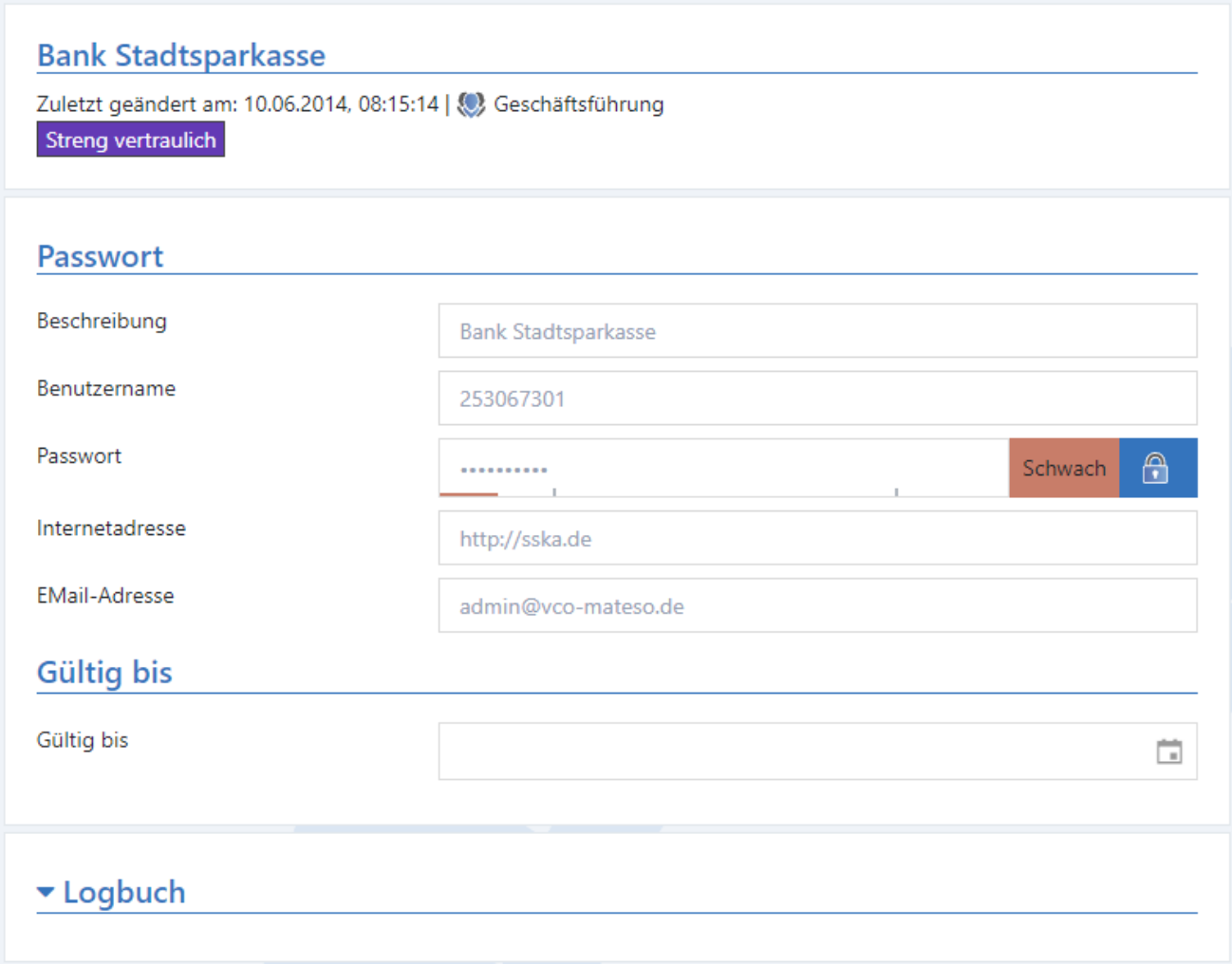
- Es ist keine Multiselektion möglich

- Die Listenansicht kann nicht individuell angepasst werden
- Es gibt – wie im Browser üblich – keine Kontextmenüs

# Lesebereich

## Was ist der Lesebereich

Wie auch die Listenansicht ist der Lesebereich des WebClients nahezu mit dem des Clients identisch. Deshalb soll auch hier auf das entsprechende Kapitel Lesebereich verwiesen werden.




Es gibt – wie im Browser üblich – keine Kontextmenüs

# Einstellungen

Die Einstellungen werden über die Navigationsleiste aufgerufen. Es stehen folgende Optionen zur Verfügung:

## Sprache

Hier kann durch einfachen Klick **Deutsch** bzw. **Englisch** gewählt werden. Die Änderung geschieht live und benötigt keinen Neustart des Browsers.

## Tags

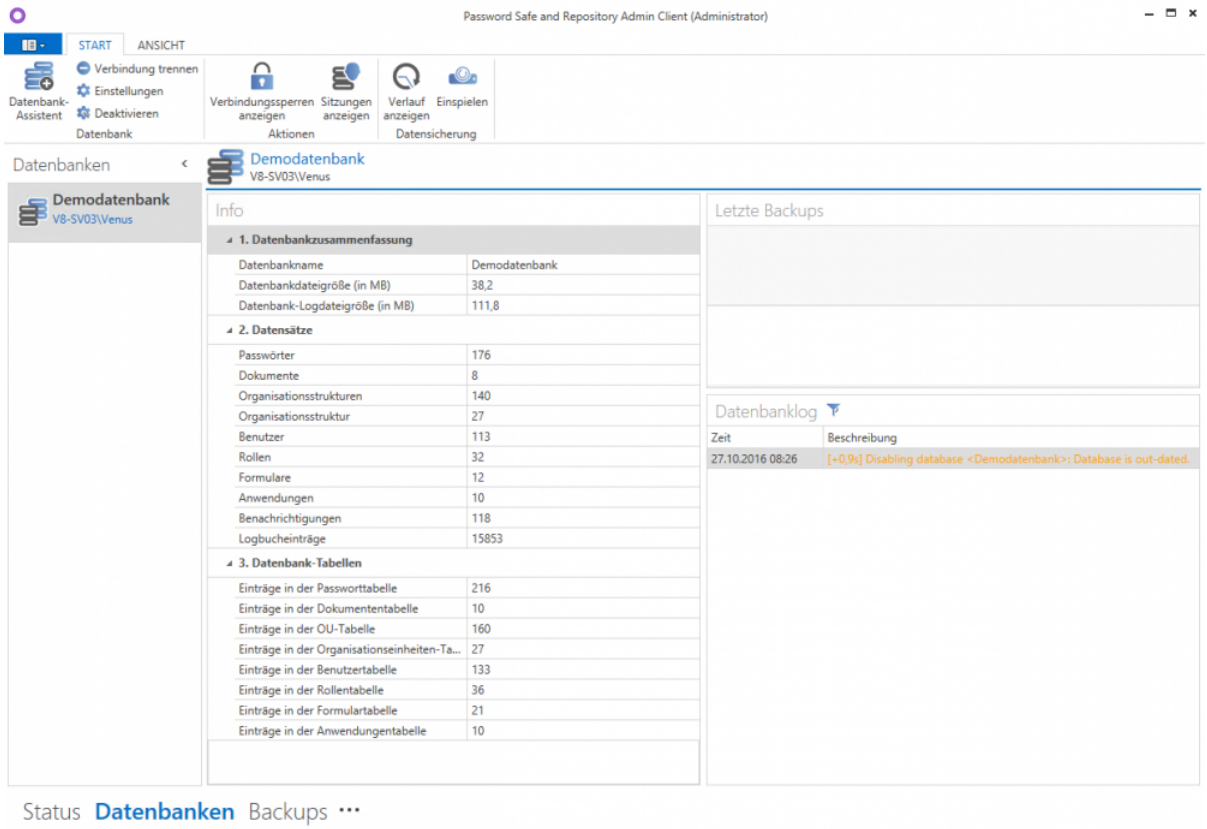
Hier wird die Tagverwaltung aufgerufen.

# Admin Client

## Was ist der Admin Client?

Der Admin Client übernimmt die zentrale Verwaltung der Datenbanken sowie die Konfiguration der Backup Profile. Darüber hinaus stellt dieser die überaus wichtige **Schnittstelle zum Password Safe Lizenzserver** zur Verfügung. Hinzu kommen die Verwaltung global zu definierender Einstellungen sowie die Konfiguration von Profilen zum Versenden von Emails. Installation des Admin Client…

> Das Initialpasswort für den Admin Client lautet “admin”

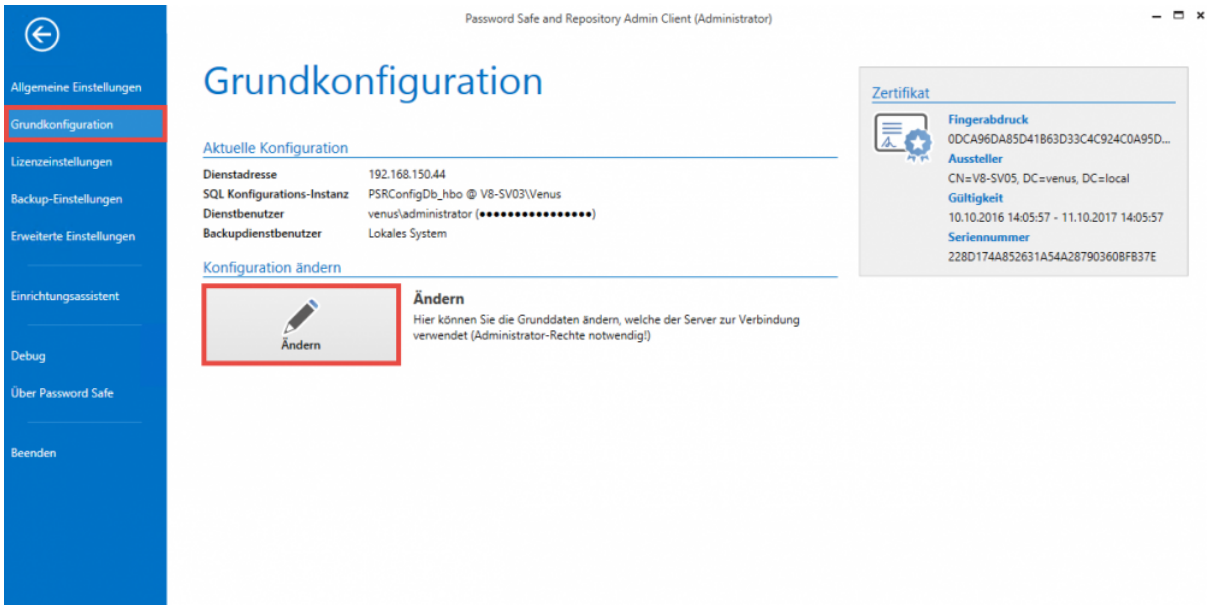



Der Serverdienst stellt so gesehen die Schnittstelle zwischen dem Client und dem SQL-Server dar. Der Admin Client ist hierbei für die Konfiguration des Serverdienstes zuständig. Er ermöglicht somit die zentrale Verwaltung der Datenbanken, ohne auf den SQL-Server Zugriff zu haben. Dies stellt im Bezug auf Organisation und Berechtigungen einen immensen Vorteil dar.

# Grundkonfiguration

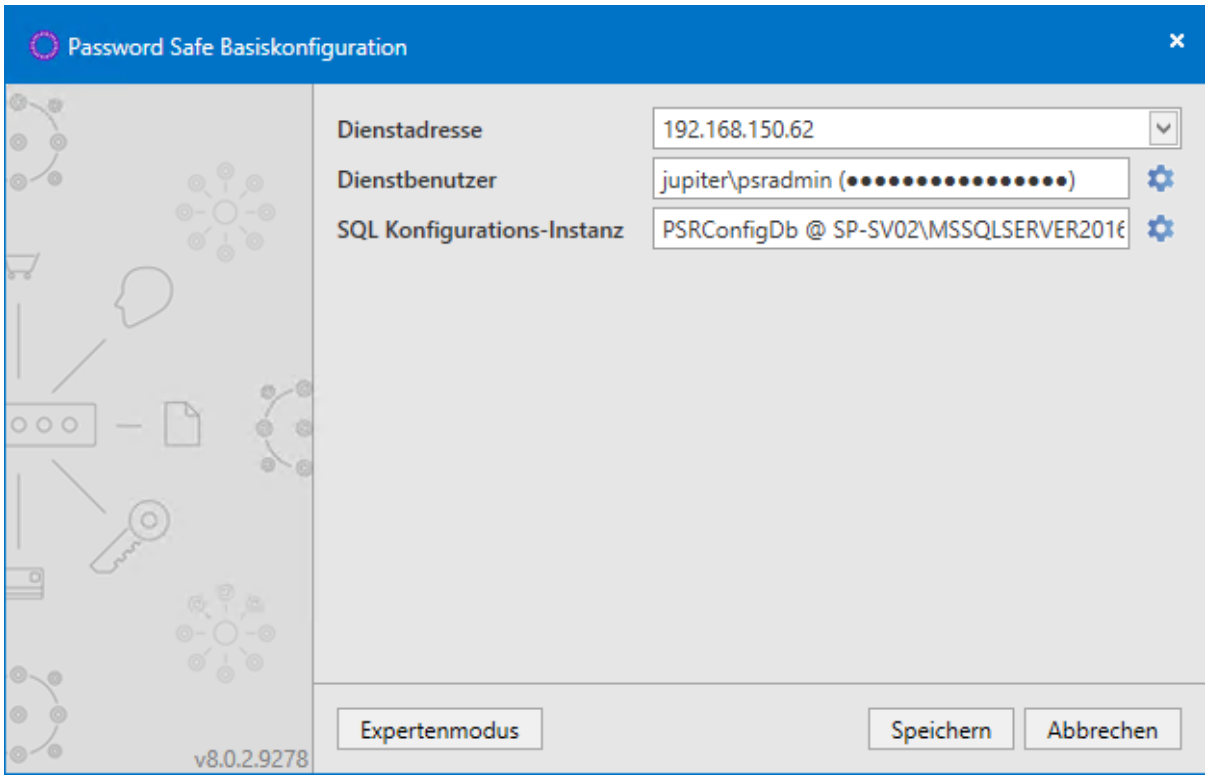
## Was ist die Grundkonfiguration?

Innerhalb der Grundkonfiguration wird die Verbindung zum SQL-Server, bzw. zu den Datenbanken, definiert. Die Grundkonfiguration erscheint beim ersten Start des Admin Client und kann in der Grundkonfiguration jederzeit aufgerufen werden.




## Die Grundkonfiguration

Zur Konfiguration steht ein eigener Assistent bereit:




### Dienstadresse

Die Dienstadresse des SQL-Servers kann über das Drop Down Menü ausgewählt werden. Es muss zwingend derjenige Adapter gewählt werden, über welchen der Admin Client den SQL-Server auch ansprechen kann.

> Die Loopback Adresse 127.0.0.1 sollte hier nicht verwendet werden.

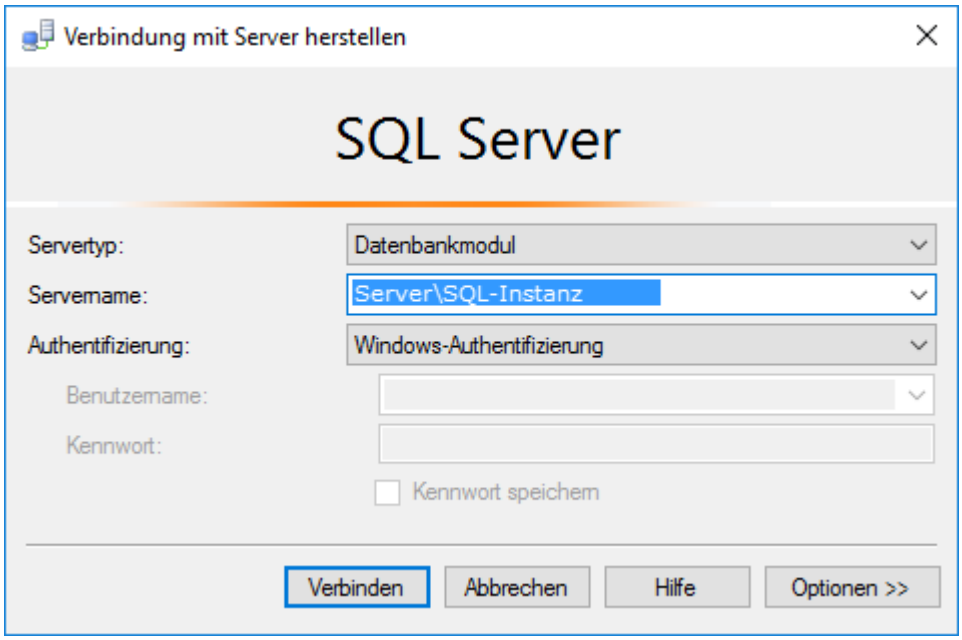
### Dienstbenutzer

Festlegung des Dienstbenutzers, welcher für den Start des Serverdienstes sowie des Backupdienstes vorgesehen ist. Über die Option “Lokales System verwenden” werden die Dienste mit dem Lokalen Systemkonto gestartet.

> Der hinterlegte Dienstbenutzer benötigt **lokale Administratorenrechte**, um den Server korrekt zu konfigurieren und Datenbanken erstellen zu können.

### SQL-Konfigurations-Instanz

Unter “SQL-Server Instanz” muss der Datenbankserver inklusive der SQL-Instanz angegeben werden. Der Einfachheit halber kann man den Servernamen aus dem Loginfenster des SQL-Servers kopieren.




Ist die Option “Dienstbenutzer” selektiert, wird derjenige User angegeben, welcher sich am SQL Server anmeldet. Es ist zu beachten, dass zum Erstellen einer Konfigurationsdatenbank **dbCreator** Rechte nötig sind. Wird die Datenbank am SQL-Server manuell erstellt und hier nur angesprochen, reichen **dbOwner** Rechte aus. Unter “Datenbank” wird der Name der Konfigurationsdatenbank angegeben.

> Weitere Informationen über die verwendeten Benutzer sind im Kapitel Systemanforderungen Server zu finden.

### Expertenmodus

Der Expertenmodus blendet einen Menüpunkt zur Konfiguration eines Backup-Benutzers ein – als Standard wird der Dienstbenutzer verwendet. Weiterhin kann die SQL-Instanz über “Connection String” konfiguriert werden.
Ebenso kann hier das SSL-Zertifikat zum Schutz der Client Server Verbindung konfiguriert werden. Standardmäßig wird durch den Admin Client ein Zertifikat erzeugt. Es kann jedoch auch ein eigenes ausgewählt werden. Nähere Informationen sind direkt im hierfür vorgesehenen Kapitel einsehbar .

> ! Durch das Austauschen, bzw. Überschreiben eines bestehenden Zertifikats, kann es zu Warnhinweisen an den Clients kommen, wenn dem Zertifikat nicht an jedem Client getraut wird.

Hier geht´s zurück zum Kapitel Erste Schritte

# Zertifikate

## SSL Verbindungszertifikate

Die Verbindung zwischen Clients und Server wird mittels SSL-Zertifikaten gesichert. Hier wird auf den **aktuellsten Verschlüsselungsstandard TLS 1.2** zurückgegriffen. Es ist sowohl möglich, über den Server ein Zertifikat zu erstellen, als auch über eine CA ein bereits bestehendes Zertifikat zu nutzen. Alle Rechner, auf dem ein Client installiert wird, müssen dem Zertifikat trauen. Anderweitig erscheint beim Starten des Clients die Meldung:

**Dieser Verbindung wird nicht getraut!**
Die Verbindung zum Server wird als nicht sicher eingestuft.


Windows Server 2012 R2 benötigt den aktuellsten Patchlevel, da dieser mit SSL3 ausgeliefert und im Nachhinein mit TLS 1.2 erweitert wurde

Über den Dienstbenutzer werden die Datenbanken erstellt. Währenddessen wird pro Datenbank ebenfalls ein eigenes Zertifikat erzeugt. Daher muss der **Dienstbenutzer lokaler Administrator** oder **Domänenadministrator** sein, da er sonst keine Rechte hat, um in den Zertifikatsstore zu speichern.

## Aufbau der Zertifikate

Folgende Informationen gelten sowohl für das Password Safe Zertifikat als auch für eigene Zertifikate:

### Alternativer Antragsteller

Die Kommunikation zwischen Client und Server kann nur auf demjenigen Weg erfolgen, welcher im Zertifikat beim alternativen Antragsteller hinterlegt ist. Das Password Safe Zertifikat nimmt daher alle IP-Adressen des Servers sowie den Hostname auf. Beim Erstellen eines eigenen Zertifikats sollten also ebenso diese Informationen unter dem alternativen Antragsteller hinterlegt werden.

## Nutzung des Password Safe Zertifikates

Die Bezeichnung des PSR Zertifikates ist **PSR8Server**. Erstellt werden kann dies über die Grundkonfiguration in der AdminConsole. Das Zertifikat liegt lokal unter:
**lokaler Computer -> eigene Zertifikate -> Zertifikate**

> Das Zertifikat ist nach Erstellung ein Jahr lang gültig. Danach muss ein neues erstellt und wie beschrieben verteilt werden.

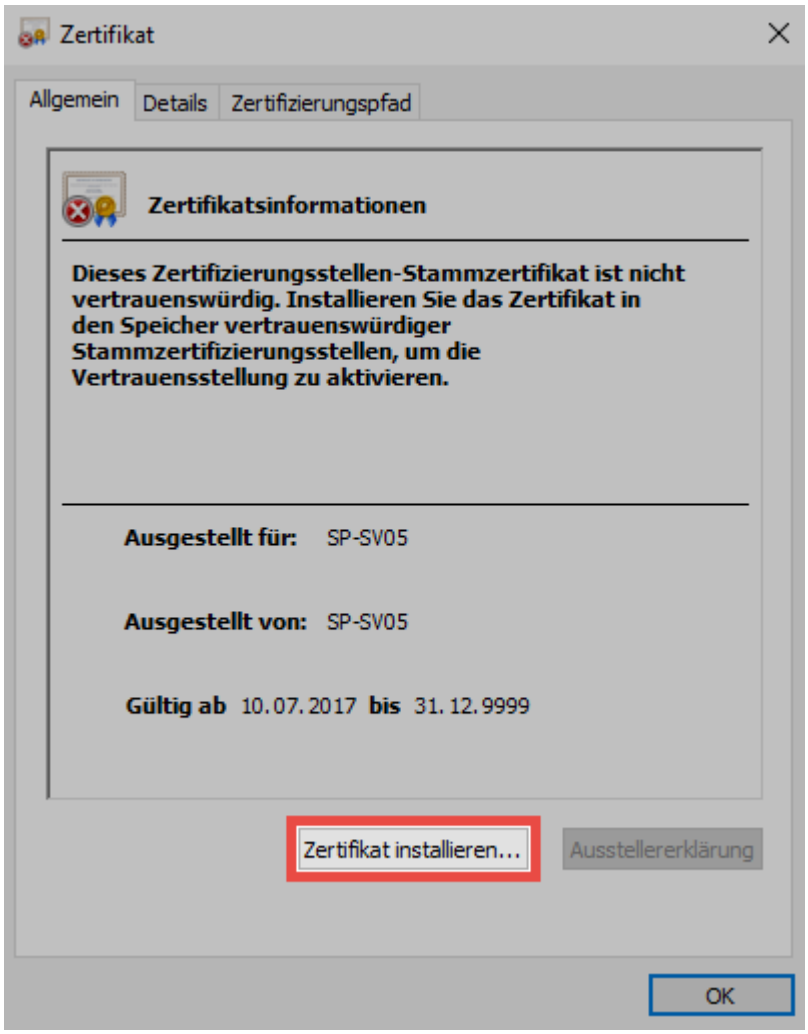
### Verteilen des Password Safe Zertifikats

Um dem Zertifikat zu trauen, kann dieses am Server exportiert und danach an den Clients importiert werden. Hierbei muss folgender Speicher gewählt werden:
**lokaler Computer > vertrauenswürdige Stammzertifizierungsstellen -> Zertifikate**

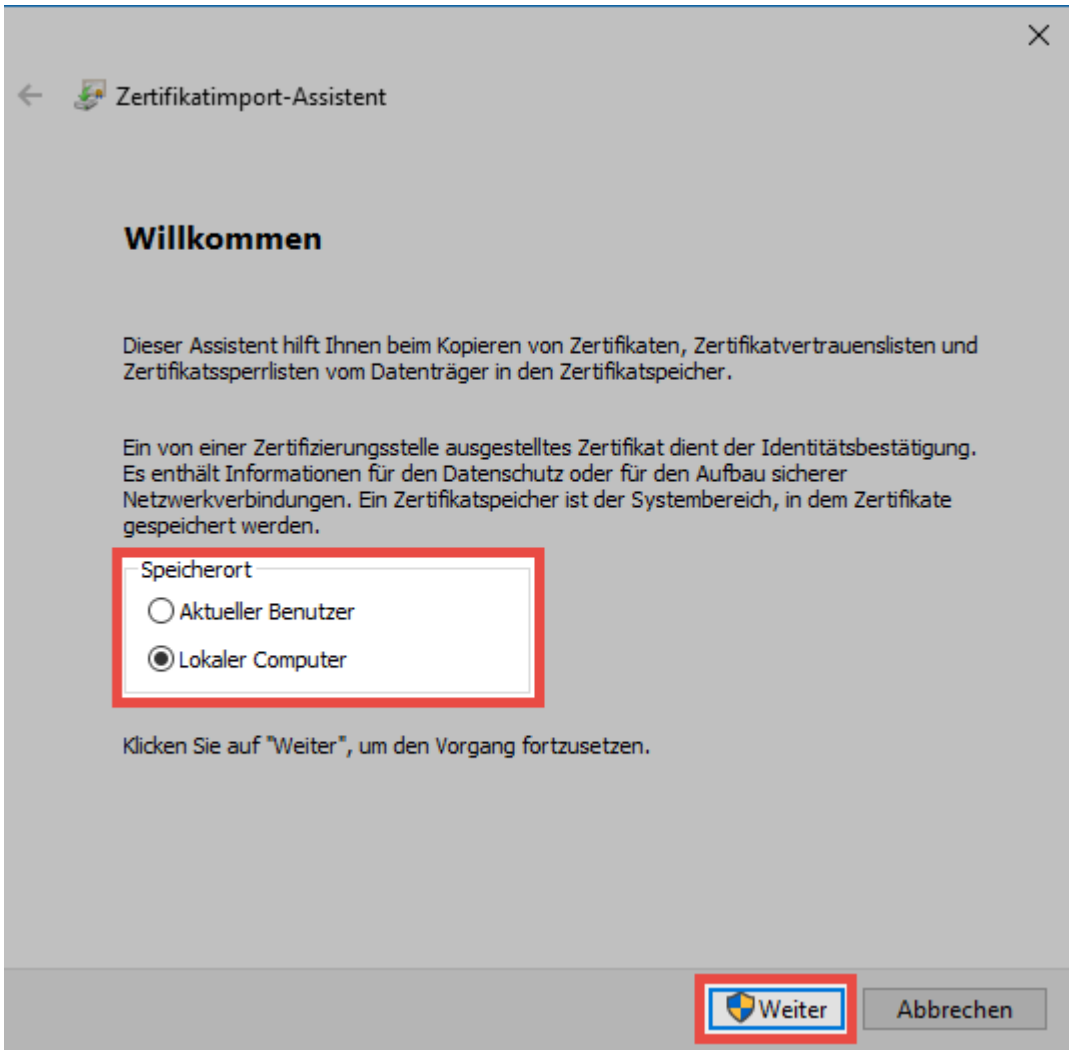
Das Zertifikat kann über Gruppenrichtlinien verteilt als auch ausgerollt werden.

### Manuelles Importieren des Password Safe Zertifikats

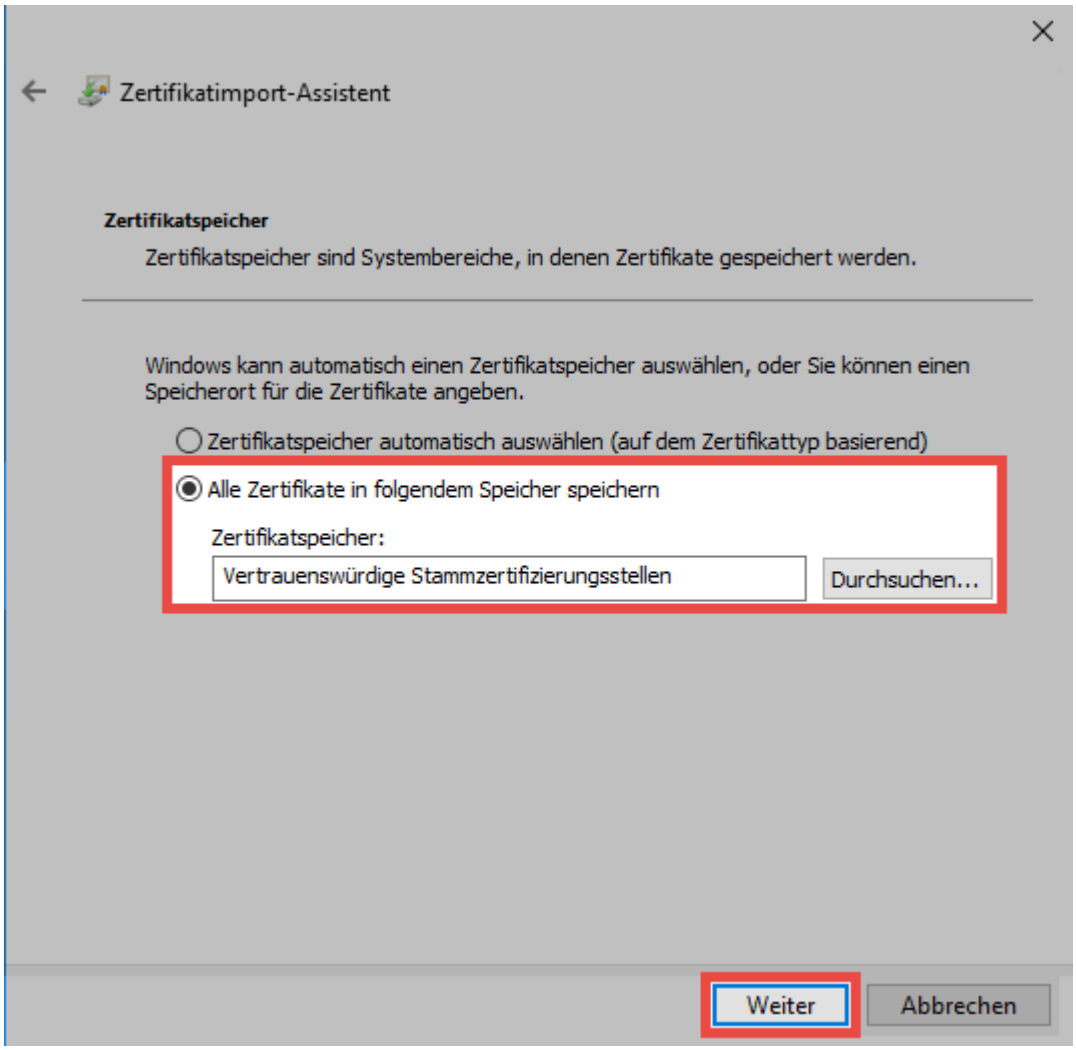
Wird das Password Safe Zertifikat nicht ausgerollt, so besteht auch die Möglichkeit das Zertifikat manuell zu importieren. Hierfür werden zunächst die Zertifikatsinformationen geöffnet. In der Warnmeldung steht hierfür die Schaltfläche **Show server certificate** bereit. Im folgenden Dialog wählt man zunächst die Option **Zertifikat installieren…**




Es öffnet sich der **Zertifikatimport-Assistent** in welchem zunächst **Lokaler Computer** gewählt wird.




Im nächsten Schritt muss der Speicher “Vertrauenswürdige Stammzertifizierungsstellen” manuell gewählt werden.




Abschließend muss die Installation nochmals bestätigt werden.

> Der am Betriebssystem angemeldete Benutzer benötigt Rechte, um Zertifikate erstellen zu können

## Nutzung eines eigenen Zertifikates

Ist bereits eine CA vorhanden, kann auch ein eigenes Zertifikat genutzt werden. Innerhalb der Grundkonfiguration kann dieses ausgewählt werden. Es gilt zu beachten, dass hier ein Server-Zertifikat zur SSL-Verschlüsselung verwendet wird. Die CA muss so konfiguriert werden, dass alle Clients dem Zertifikat trauen. Hierfür ist nötig, dass der Zertifizierungspfad eingehalten wird.

> Bei der Erstellung des Zertifikats ist darauf zu achten, dass Password Safe lediglich den Cryptographic Service Provider (CSP) und nicht den Key storage provider (KSP) unterstützt

! Bei der Konfiguration muss beachtet werden, dass die Clients die Sperrlisten der CA erreichen können

### Wildcard Zertifikate

Wildcard Zertifikate können leider nicht unterstützen werden. Theoretisch sollte die Verwendung zwar möglich sein, wir können jedoch bei der Konfiguration keine Hilfestellung bieten. Daher erfolgt der Einsatz von Wildcard Zertifikaten auf eigene Verantwortung.

## Datenbank Zertifikate

Pro Datenbank wird ein eigenes Zertifikat erstellt. Dieses trägt den Namen “psrKey”, gefolgt von einer einmaligen GUID. Beispielsweise: **psrKey_25717957-fcc1-e611-9953-c86000c4a2aa**

## Zertifikat für den Masterkey Modus

Wird ein Active Directory über den **Masterkey Modus** angesprochen, wird hierfür ebenfalls ein Zertifikat erstellt. Die Nomenklatur entspricht derjenigen der Datenbank Zertifikate.

* Sowohl die **Datenbank Zertifikate** als auch die **Zertifikate für den Masterkey Modus** haben ein Ablaufdatum. Dies wird jedoch nicht geprüft. Diese Zertifikate müssen also nicht erneuert werden.

! Die erstellten Zertifikate sollten unbedingt gesichert werden! Bei Verlust kann die Datenbank nicht mehr verwendet werden! Das Sicher geschieht über die Zertifikatsverwaltung des Betriebssystems. Dort kann das Zertifikat über einen Rechtsklick exportiert werden.

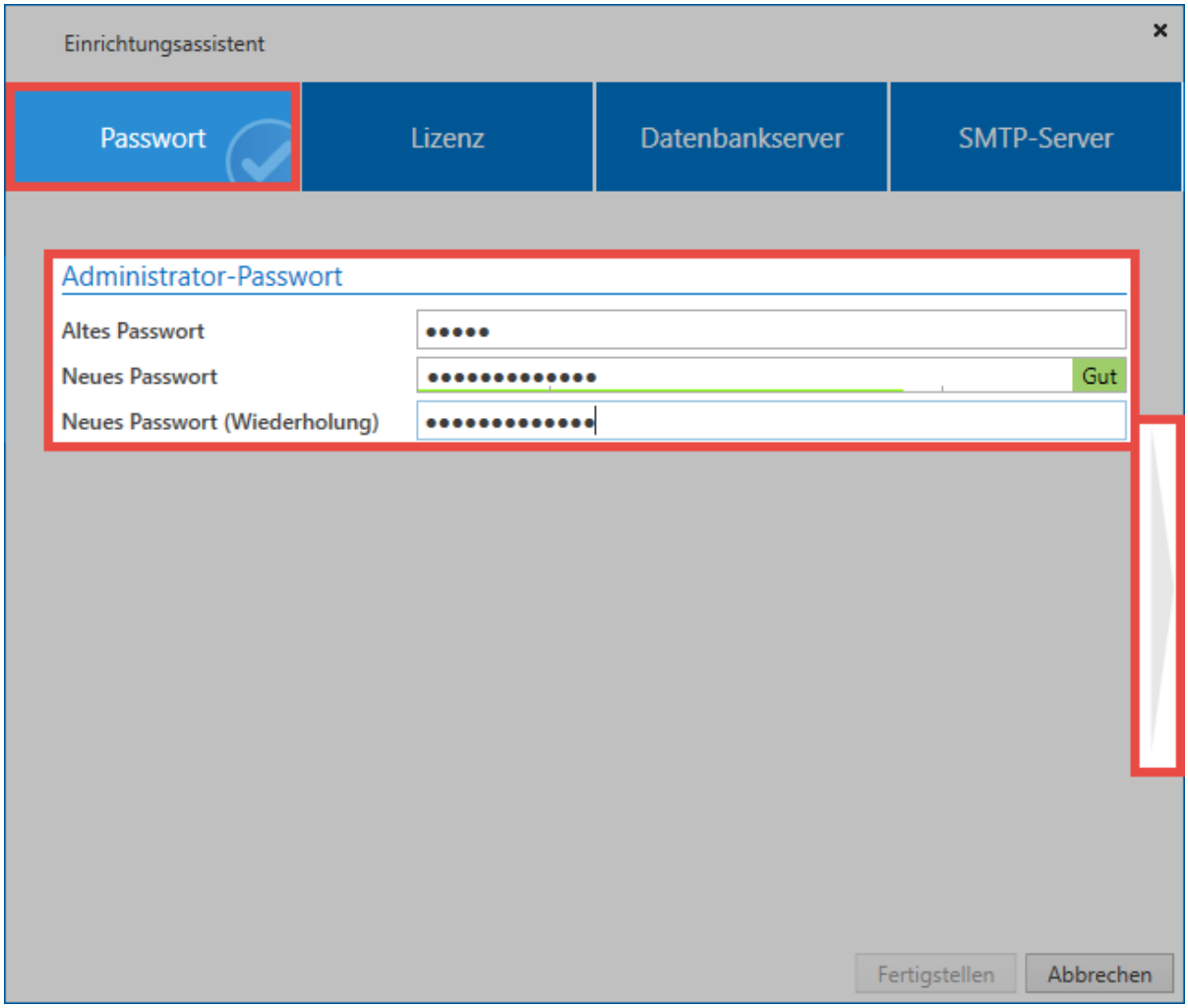
# Einrichtungsassistent

## Was ist der Einrichtungsassistent?

Der Einrichtungsassistent beinhaltet alle relevanten Einstellungen im Zuge der Einrichtung von Password Safe. Die einzelnen Punkte können ebenso im Nachhinein geändert werden. Hierzu existieren jeweils separate Kapitel.

### Administrator-Passwort definieren

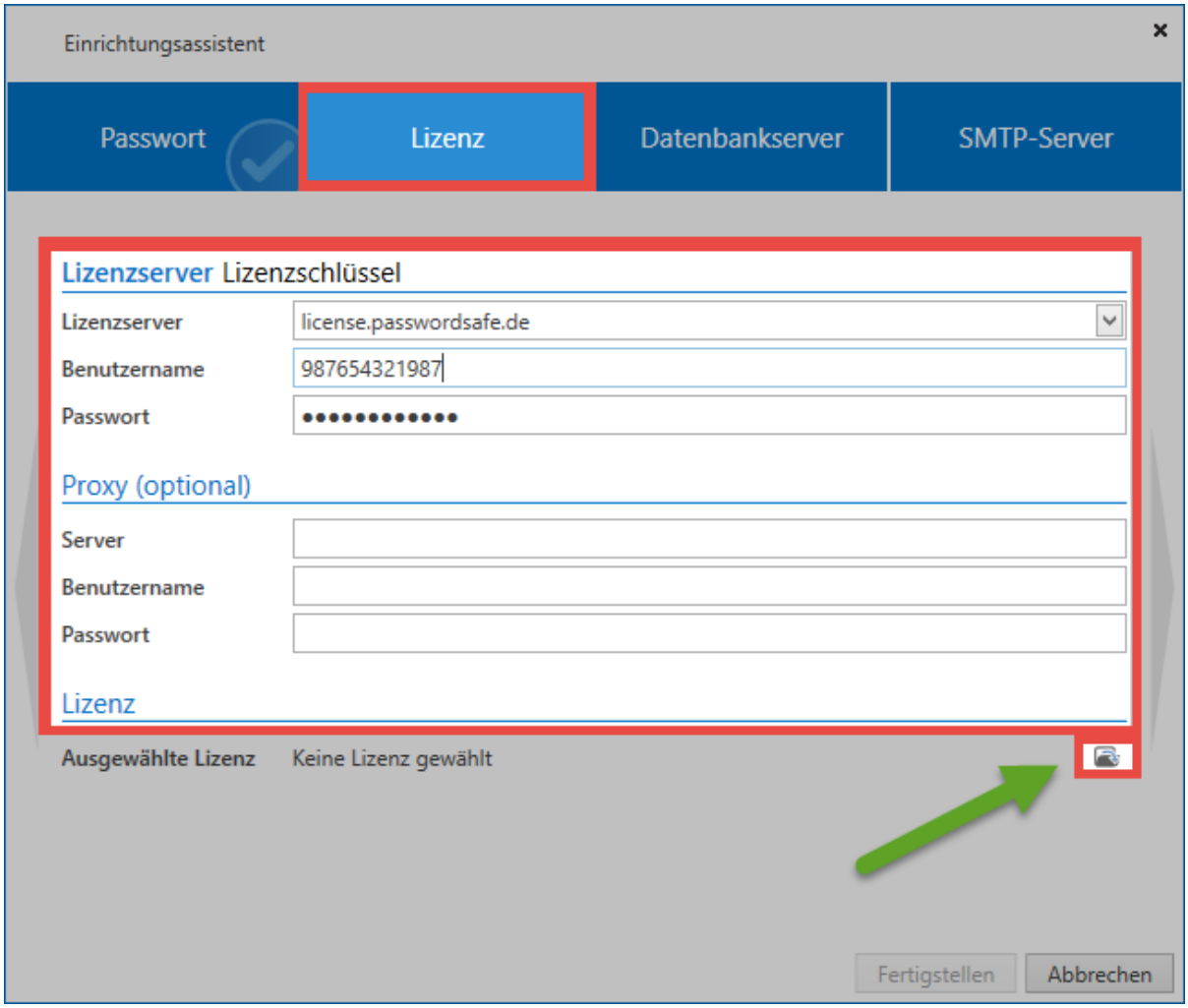
Im ersten Schritt wird das Authentifizierungspasswort für den Admin Client festgelegt. Das Initialpasswort lautet “admin”. Dieses muss bei Start neu vergeben werden – das neue Passwort ist sicher und wohl dokumentiert aufzubewahren. Im Nachhinein kann dies in den allgemeinen Einstellungen geändert werden.



Das Initialpasswort lautet “admin”.

### Lizenzeinstellungen

Im zweiten Schritt wird die Konfiguration für eine erfolgreiche Anbindung an den Lizenzserver vorgenommen. In den Lizenzeinstellungen kann dies auch im Nachhinein durchgeführt werden.




Um Feld Lizenzserver ist “license.passwordsafe.de” zu hinterlegen. Die weiteren Zugangsdaten (Benutzername und Passwort zum Lizenzserver werden per E-Mail zugestellt.

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

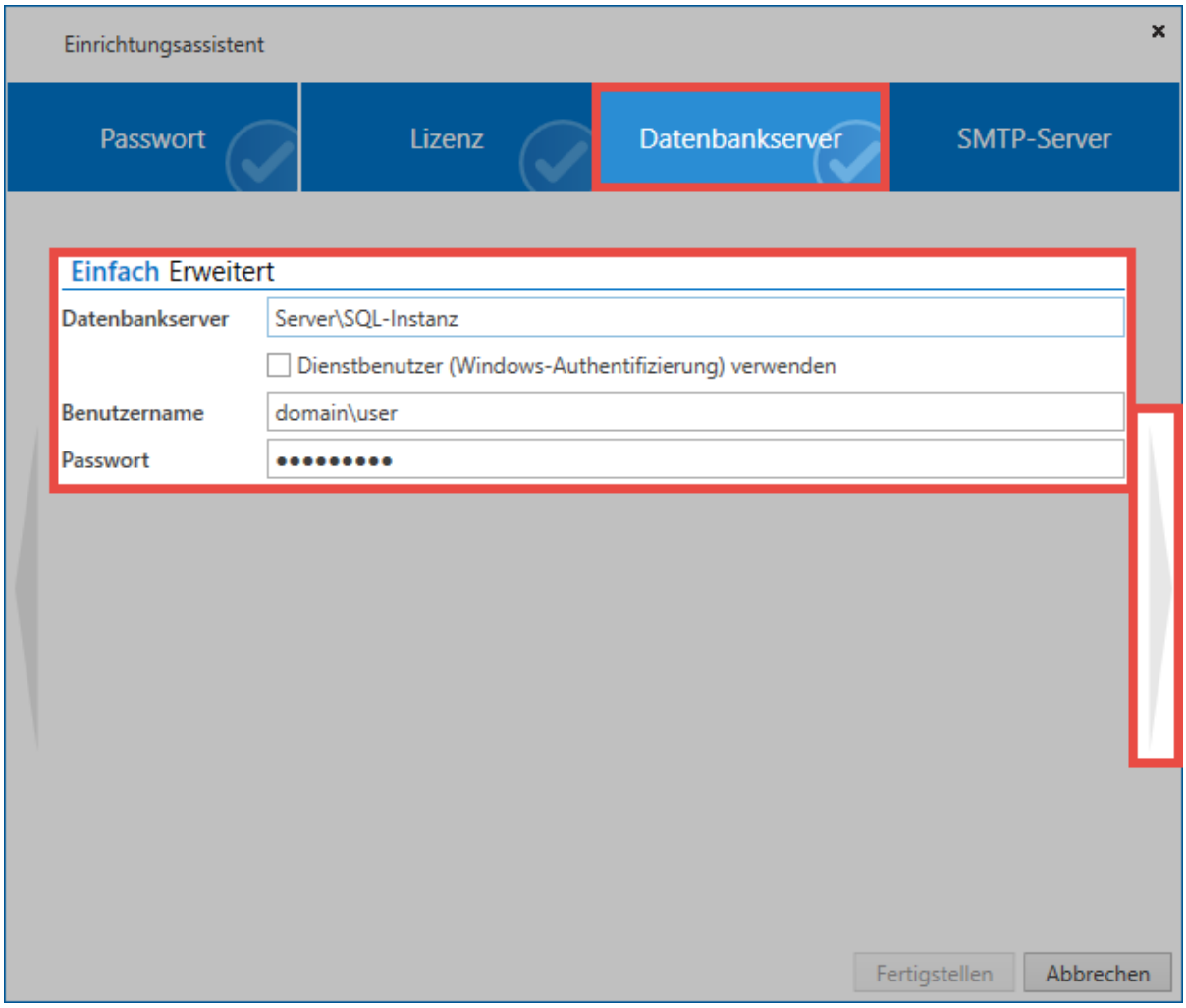
---

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Handelsregister Augsburg HRB 22302
Geschäftsführer: Thomas Malchar
USt.-ID: DE252782033

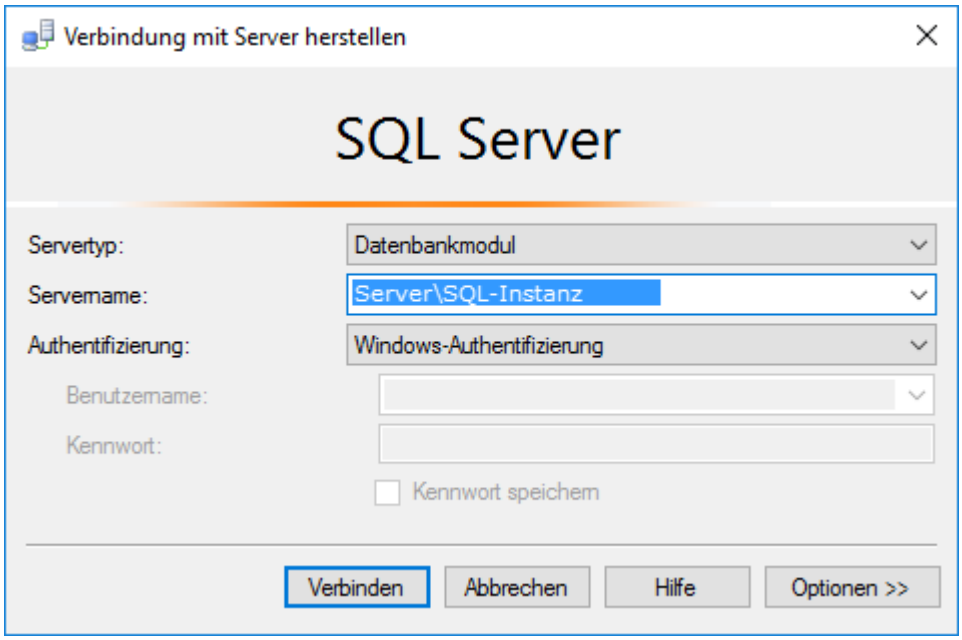
Falls nötig, können ebenso Zugangsdaten für einen etwaigen Proxy angegeben werden – ansonsten wird der im Betriebssystem hinterlegte Proxy verwendet. Über die entsprechende Schaltfläche kann dann die gewünschte Lizenz ausgewählt und aktiviert werden.

### Datenbankserver

Die Konfiguration des Datenbankservers ist ebenso Teil der erweiterten Einstellungen und kann dort im Nachhinein geändert werden.



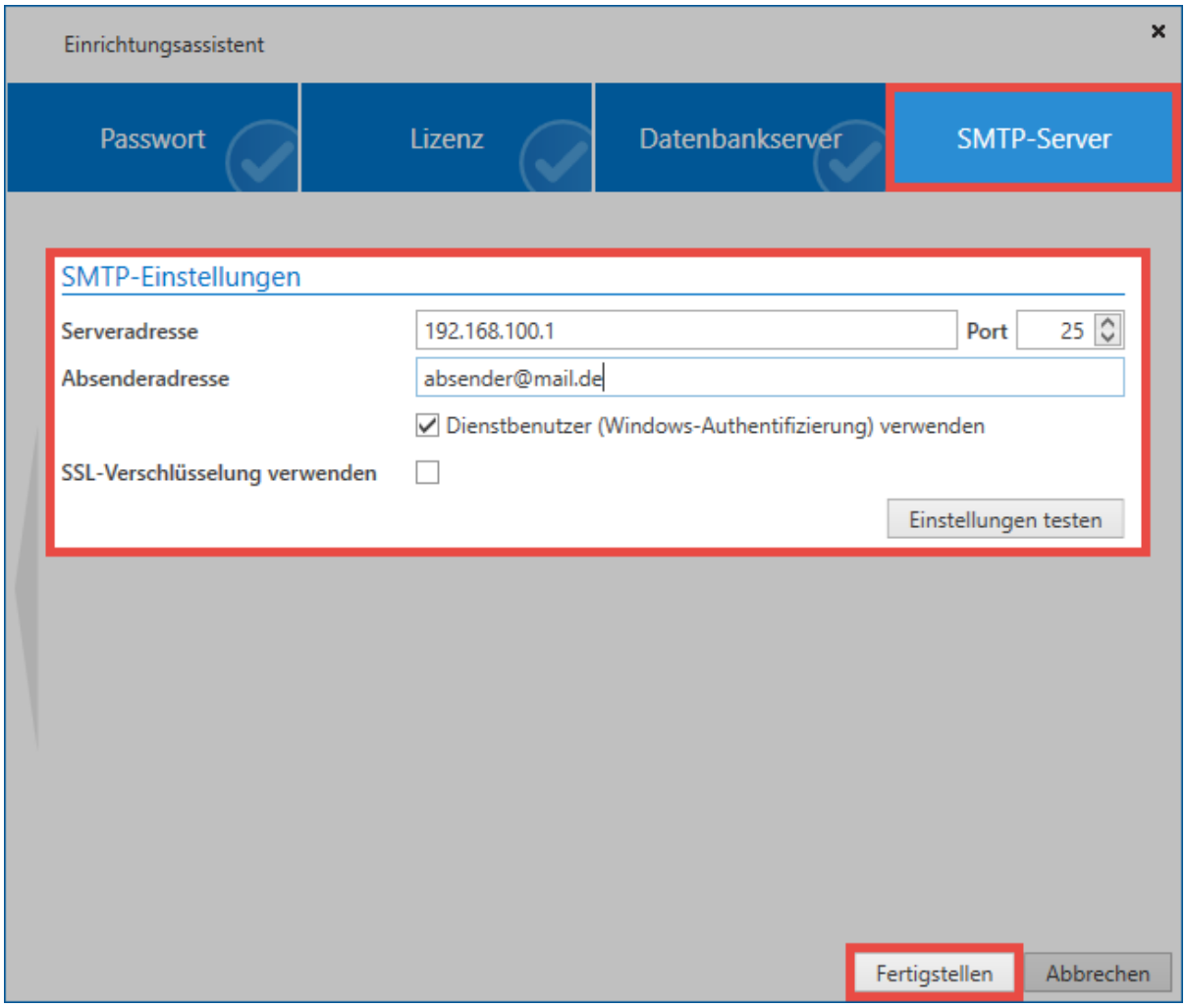

Der Datenbankserver muss inklusive der zugehörigen SQL Instanz angegeben werden. Der Einfachheit halber kann man den Servernamen aus dem Loginfenster des SQL-Servers kopieren.




Weiterhin wird derjenige Benutzer angegeben, in dessen Kontext am SQL-Server die Datenbank erstellt wird. Der Benutzer benötigt also **dbCreator** Rechte. Alternativ kann hier auch der Dienstbenutzer verwendet werden. Über die Schaltfläche “Erweitert” erhält man die Möglichkeit, einen **Connection String** anzugeben.

### SMTP-Server

Im letzten Schritt wird der SMTP-Server konfiguriert, über welchen alle E-Mails verschickt werden. Auch dies ist Teil der erweiterten Einstellungen, falls im Nachhinein Änderungen vorgenommen werden müssen.




Sobald die Daten eingegeben sind und erfolgreich getestet wurden, kann der Assistent über einen Klick auf “Fertigstellen” abgeschlossen werden.

### Sicherheitshinweise

Sobald der Einrichtungsassistent eingerichtet ist, werden im Modul **Status** zwei Sicherheitshinweise eingeblendet, welche bestätigt werden müssen:


! Es wird empfohlen die Sicherheitshinweise erst dann zu bestätigen, wenn die entsprechenden Punkte tatsächlich erledigt sind. Es ist unbedingt darauf zu achten, dass regelmäßige Backups erstellt und die Zertifikate werden.

Hier geht´s zurück zum Kapitel Erste Schritte

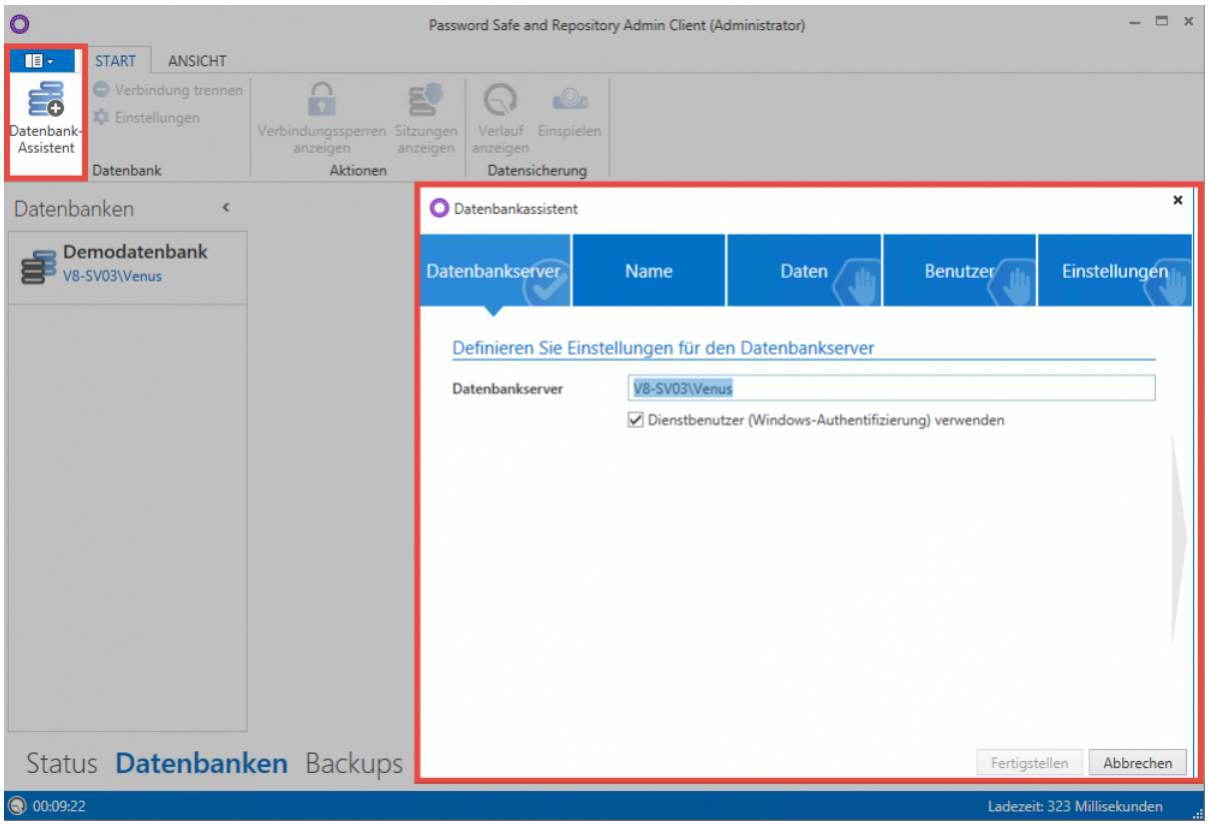
# Erstellen von Datenbanken


## Was sind Datenbanken?

Datenbanken beinhalten alle Informationen zu Benutzern, Datensätzen, Dokumenten oder dergleichen. Ebenso werden die Änderungen an Objekten im Password Safe ebenso Teil der MSSQL Datenbank. Selbstverständlich sollte der regelmäßigen Erstellung von Backups, und somit der Sicherung dieser Daten, stets die allerhöchste Priorität zu Teil werden. Für Password Safe Version 8 kommt das relationale Datenbankmanagementsystem **MSSQL** zum Einsatz.

## Erstellen von Datenbanken

Die Erstellung von Datenbanken wird durch den Datenbankassistenten unterstützt, welcher direkt über die Ribbon gestartet wird. Nachfolgend eine Erläuterung zu den einzelnen Reitern:



### Datenbankserver

Die Auswahl des Datenbankservers kann im ersten Reiter manuell definiert werden. Standardmäßig ist der in den erweiterten Einstellungen definierte Wert voreingestellt. Es kann darüber hinaus ein Benutzer hinterlegt oder auf den Dienstbenutzer zurückgegriffen werden.

### Name

Hier wird der Name der neuen Datenbank angegeben. Alternativ kann auch eine bestehende Datenbank selektiert werden. Ein aussagekräftiger Name erleichtert besonders im Zusammenspiel mehrerer Datenbanken deren Unterscheidung.

### Daten

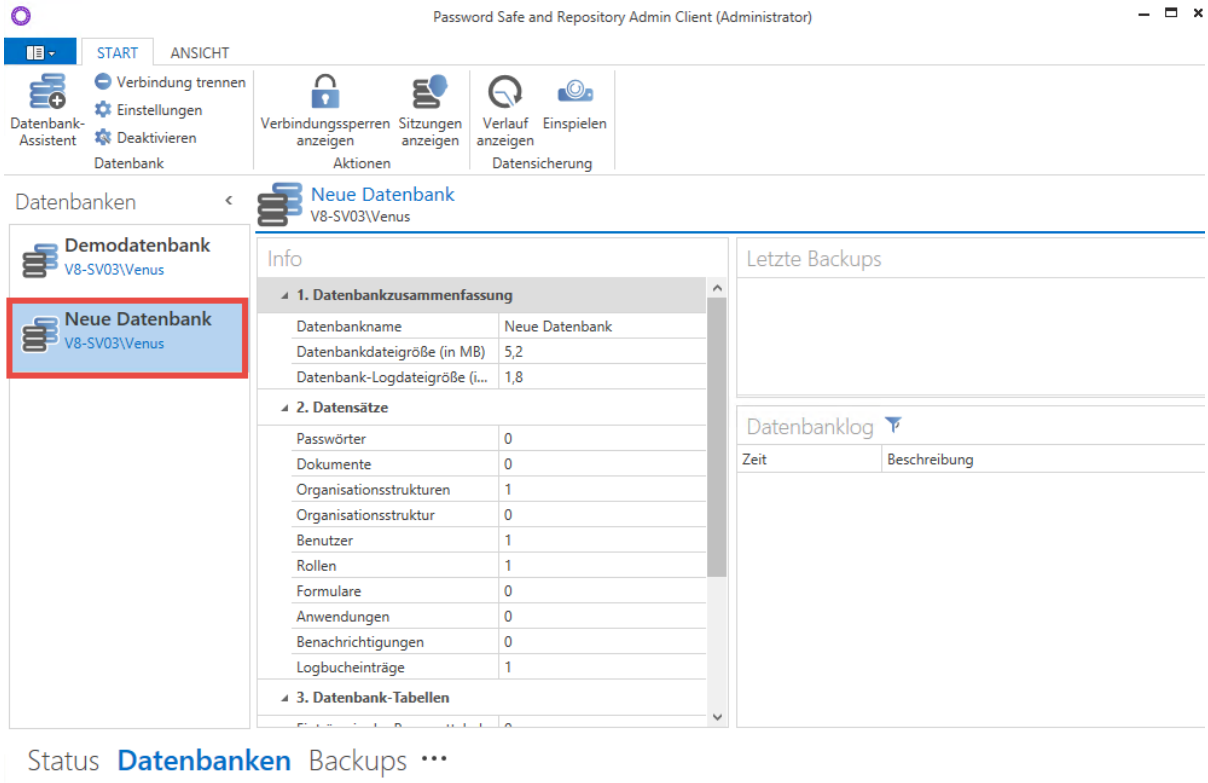
Es kann selektiert werden, ob eine Vorlage verwendet werden soll. Über die Vorlage erhält die Datenbank vorgefertigte Formulare und Dashboard-Einstellungen, welche den Einstieg erleichtern. Es kann zwischen der deutschen und der englischen Vorlage ausgewählt werden. Es ist jedoch auch möglich ohne Vorlage fortzufahren, um eine komplett leere Datenbank zu erhalten. Haben Sie ein Backup aus einer Password Safe Version 7, kann dieses migriert werden.

### Benutzer

Es folgt die Definition des initial anzulegenden Benutzers – üblicherweise ist dies der Administrator. Ist die Migration aktiv, kann der User nach der Migration wieder gelöscht werden.

## Abschließen des Datenbankassistenten

Nach der erfolgreichen Erstellung einer Datenbank startet die Datenbankmigration, sofern diese ausgewählt wurde. Wurde keine Datenmigration gewählt, wird die neue Datenbank direkt angelegt und in der Datenbankübersicht angezeigt.




Hier geht´s zurück zum Kapitel Erste Schritte

# Migration

! Es wird zu jedem Zeitpunkt empfohlen, die Migration in den Password Safe Version 8 begleitet durch einen zertifizierten Partner/den Hersteller durchzuführen. Bitte kontaktieren Sie uns gerne in dieser Angelegenheit.

## Was ist die Migration?

* Die Migration behandelt den Import von Daten aus der alten Password Safe Version 7. Relevant ist dieses Kapitel demnach nur für Bestandskunden.

Das Datenbankformat der Version 7 unterscheidet sich grundlegend von der in der Version 8 eingesetzten MSSQL-Datenbank. Die Migration beinhaltet demnach die automatische Portierung aller Daten aus der Version 7 in die Version 8. In diesem Zuge ist es, bedingt durch die Anpassungen am Berechtigungskonzept, nötig, die Daten auf die neuen Gegebenheiten anzupassen.

! Während der Migration erhält der ausführende Benutzer Einsicht auf alle Ordner der Datenbank. Die Datensätze selbst sind während der Migration dem ausführenden Benutzer nicht einsehbar. Die Berechtigungen auf Datensätze ändern sich während des Migrationsprozesses nicht.

## Grundlegende Änderungen am Bedienkonzept

Password Safe **Version 8** setzt auf ein komplett neues Bedienkonzept, welches **ohne Ordnerstruktur** auskommt – Datensätze werden nun kategorisiert. Sowohl die Einteilung in Organisationseinheiten als auch die Nutzung von Tags spielen hierbei eine entscheidende Rolle. Die Änderungen ermöglichen deutlich flexiblere Anpassungsmöglichkeiten an individuelle Anforderungen sowie gesteigerte Effizienz bei Auffinden gespeicherter Informationen.

Da es in der Version 8 keine Ordner mehr gibt, muss während der Migration festgelegt werden, wie ehemals in Ordnern abgelegte Datensätze zukünftig gehandhabt werden sollen. Es erfolgt also ein “Mapping”, welches festlegt, wie diese Datensätze kategorisiert werden sollen. Man kann im Zuge der Migration für jeden Ordner separat festlegen, ob dieser als Organisationseinheit oder als Tag abgebildet werden soll. Ebenso können einzelne Ordner von der Migration ausgenommen werden. Um die Arbeit zu erleichtern steht natürlich ein entsprechender Assistent bereit, welcher im entsprechenden Kapitel näher erläutert wird.

Die Ordner **Startseite, Suchordner, Alle Passwörter und Favoriten** werden in der Version 8 nicht mehr benötigt und müssen daher nicht mit migriert werden.

### Parallelbetrieb von Version 7 und 8

Technisch gesehen ist es möglich Version 7 und 8 parallel zu betreiben. Dies kann jedoch nicht empfohlen werden, da es dadurch zu Abweichungen der Datenbestände kommen kann. Die automatische Anmeldung kann im Parallelbetrieb ebenfalls zu Problemen führen.

# Vorbereitungen

## Vorbereitungen Version 8

Vor der Migration sollte sichergestellt sein, dass sowohl der Server als auch der Client der Version 8 installiert sind und verwendet werden können. Informationen hierzu sind dem Kapitel Erste Schritte zu entnehmen. Weiterhin sollte **vor** der Migration festgelegt werden, ob Active Directory Benutzer im Master Key Modus oder Ende zu Ende verschlüsselt importiert werden sollen. Das Kapitel Active Directory Anbindung hilft bei der Entscheidungsfindung.

> ! Der Master Key Modus und die Ende zu Ende Verschlüsselung unterscheiden sich erheblich voneinander. Die Entscheidung, welchen Modus man wählt, hat demnach auch tiefgreifende Auswirkungen. Daher sollte diese Entscheidung sorgfältig geprüft und getroffen werden. Weitere Infos…

## Vorbereitungen Version 7

### E-Mail Adressen

In der v7 Datenbank muss bei allen lokalen Benutzern sowie allen Usern, welche im **Ende zu Ende Modus** migriert werden sollen, eine E-Mail Adresse hinterlegt sein. In der Version 8 kommt ein neues Verfahren zum Einsatz (PBKDF2), in dessen Zuge der Versand von neuen, zufallsgenerierten Passwörtern an diese genannten E-Mailadressen vorgesehen ist.

> * Im Testmodus werden keine E-Mails versandt. Daher müssen hierfür keine E-Mail Adressen hinterlegt sein. In diesem Fall müssen den einzelnen Benutzern manuell Passwörter zugewiesen werden. Diese müssen dann beim ersten Login geändert werden.

### Backup, Passwort und Private Key

- Es muss eine **gültige Datensicherung** der Version 7 im .psx Format vorliegen
- Bei Serverdatenbanken wird der zugehörige **private key** mit der Endung .prvkey benötigt.
- Es wird das **Datenbankpasswort** benötigt (bei Single- und Multiuser-Datenbanken)

### Offline Modus und USB-Sticks

- Alle Offline-Datenbanken müssen vor der Migration synchronisiert werden
- Alle USB-Sticks müssen vor der Migration synchronisiert werden

Der in der Datenbankübersicht (s. nachfolgendes Unterkapitel) genannte Wert “exportierte Datenbanken” entspricht der Summe aller Offline-Datenbanken und synchronisierten USB-Sticks.

# Bereinigung des Datenbestands

Es ist im Zuge der Migration auf die Version 8 ein günstiger Zeitpunkt, den Datenbestand der vorhandenen Version 7 Datenbank zu bereinigen. Dies verkürzt einerseits die Länge der Migration, andererseits erleichtert es das “Zurechtfinden” in der Version 8. Die Datenbankübersicht kann in der Version 7 über **Bearbeiten -> Reports -> Datenbankübersicht** aufgerufen werden und stellt während der Bereinigung eine sehr wichtige Informationsquelle dar.

**Datenbank Übersicht**
Datenbank: Entwicklerdatenbank
Erstellt am: 15.12.2016 10:54:13

| Beschreibung | Anzahl |
|---|---|
| Anwendungen | 328 |
| Aufgaben | 6 |
| Benutzer | 117 |
| Benutzer (gelöscht) | 10 |
| Datensätze | 170 |
| Datensätze (gesperrt) | 5 |
| Datensätze (versiegelt) | 10 |
| Dokumente | 7 |
| Exportierte Datenbanken | 1 |
| Formulare | 53 |
| Formularfelder | 454 |
| Freigaben | 4 |
| Gruppen | 26 |
| Icons | 58 |
| Labels | 3 |
| Logbuch-Einträge | 21089 |
| Nachrichten | 29 |
| Ordner | 690 |
| Synchronisationslog | 1072 |
| System-Tasks | 3 |
| Workflow-Events | 7 |

- Nicht mehr benötigte Datensätze, Dokumente, Ordner oder Anwendungen sollten gelöscht werden. Die Bereinigung persönlicher Datensätze und Dokumente müssen durch die Benutzer selbst durchgeführt werden.
- Es bietet sich an, Ordnerstrukturen mit Ausblick auf die Migration schon im Vorfeld anzupassen
- Auch eine Bereinigung des Logbuchs (**Bearbeiten -> Datenbank Einstellungen -> Logbuch**) macht oftmals Sinn. Es steht eine Option bereit, um Daten vor dem Löschen zu exportieren. Die Größe des Logbuchs ist in der Datenbankübersicht aufgeführt.

- In der Datenbankübersicht ist ebenso die Größe des Synclogs enthalten. Sollte dieser Wert über 10.000 liegen, sollte er gelöscht werden. Anderweitig kann dies zu einer massiven Vergrößerung der Backup-Datei führen.

Labels aus der Version 7 werden in der Version 8 zu Tags. Falls notwendig, kann man mit Labels vor der Migration Datensätze „Taggen“ und so einen bestimmten Bereich bereits vor der Migration definieren.

Das Leeren des Synclog sollte stets begleitet durch den technischen Support durchgeführt werden. Zwecks Terminvereinbarung kontaktieren Sie bitte den technischen Support.

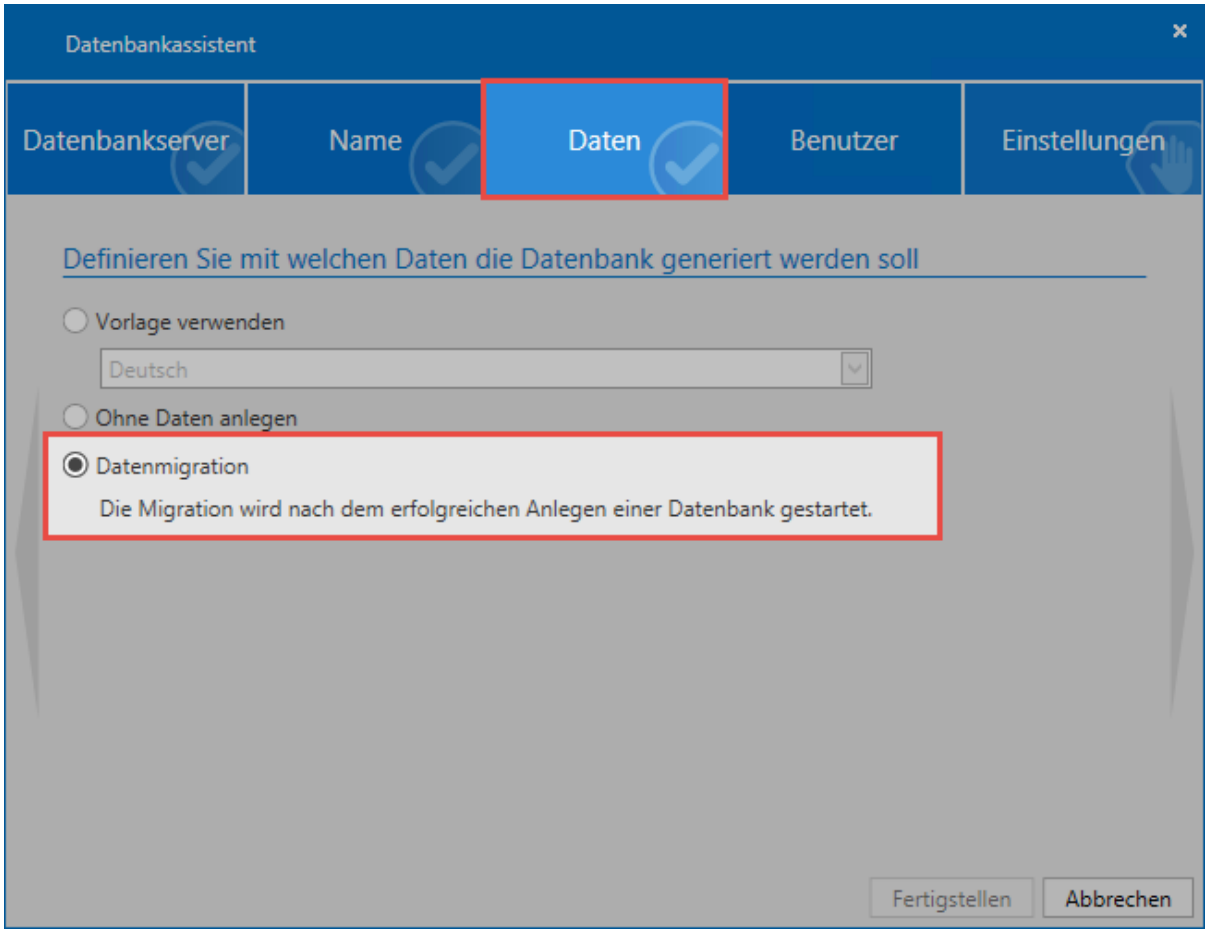
# Starten des Migrationslaufs

## Was ist der Migrationslauf?

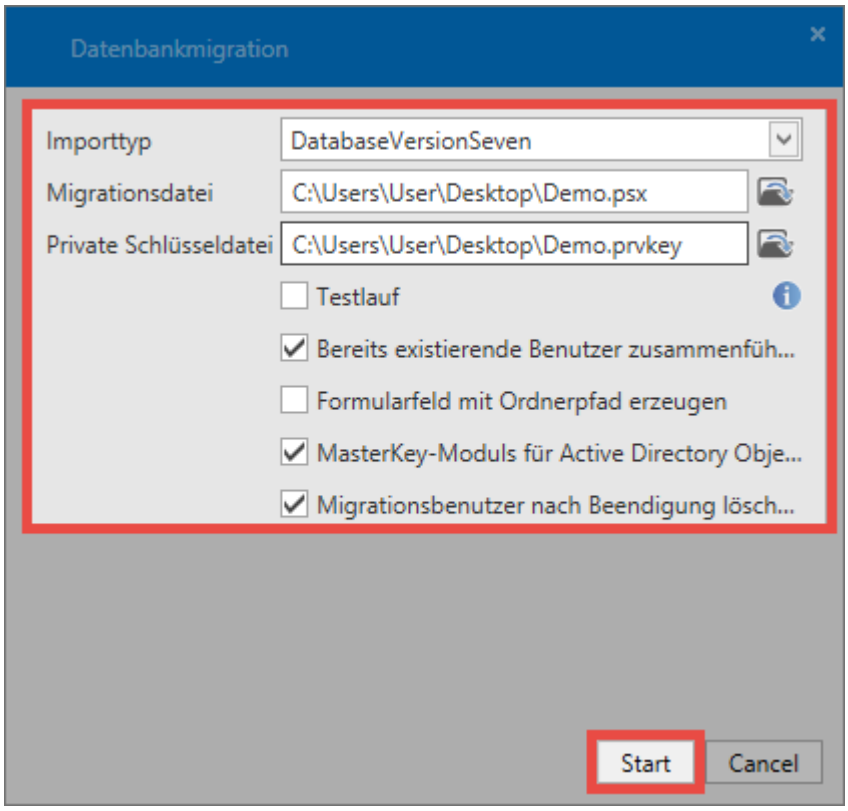
Der Migrationslauf beschreibt die tatsächliche Durchführung der Portierung, bei der alle Daten aus einer Datenbank der Version 7 in eine neue/vorhandene Datenbank der Version 8 umgewandelt werden. Ebenso werden die aufgrund der Umgestaltung des Berechtigungskonzeptes notwendigen Anpassungen am Datenbestand durchgeführt.

## Starten der Migration

Zunächst wird wie im Kapitel Erstellen und Verwaltung von Datenbanken beschrieben eine neue Datenbank erstellt. Im dritten Schritt des Assistenten wird die Datenmigration aktiviert.




Nach Abschluss des Datenbankassistenten gelangt man direkt in den Migrationsassistenten.




- Es wird der gewünschte **Importtyp** gewählt

> Momentan wird nur ein Import aus Password Safe v7 unterstützt. Falls Migrationen älterer Datenbankversionen angestrebt werden, muss der Zwischenschritt über die Version 7 genommen werden.

- Unter **Migrationsdatei** wird das zuvor erstellte Password Safe v7-Backup im Format **.psx** ausgewählt
- Es muss bei der Migration einer Serverdatenbank die zugehörige **private Schlüsseldatei** im Format .prvkey ausgewählt werden. Bei Single- und Multiuser Datenbanken wird zur **Eingabe des Passworts** aufgefordert.
- Über den **Testlauf** wird die komplette Migration als Probelauf durchgeführt. Benutzer erhalten in diesem Zuge keine Passwörter und können sich somit nicht anmelden. Dieser Schritt dient nur zu Testzwecken.
- Für lokale Benutzer bzw. im bei deaktiviertem Masterkey Modus, können **zufällige Passwörter erzeugt** werden. Diese werden den Benutzern per E-Mail zugestellt. Werden die Passwörter nicht automatisch erzeugt, müssen Sie in der Datenbank manuell vergeben werden.
- **Bereits existierende Benutzer zusammenführen**: Wird eine bestehende Datenbank migriert, werden evtl. doppelt vorhandene Benutzer anhand des Namens zusammengeführt. Die Rechte werden addiert. Ist die Option inaktiv, wird dem neu importierten Benutzer am Namen ein “*” angehängt. Beim nächsten Lauf “**” usw.

- **Formularfeld mit Ordnerpfad erzeugen**: Es wird ein Formularfeld erzeugt, das den Ordnerpfad aus der Password Safe Version 7 auflöst. Dieses Feld erhält jeder Datensatz und ermöglicht zukünftig die Suche anhand des alten Ordnerpfades.
- **Master Key Modus für Active Directory Objekte**: Es wird entschieden, ob die AD-Benutzer im Master Key Modus oder Ende zu Ende verschlüsselt importiert werden. Es gilt zu beachten, dass im Master Key Modus ein entsprechendes Zertifikat erstellt wird.
- Hat man in der Version 7 eine eigene Ordnerstruktur für die Dokumente, so können die **Dokumentordner als Organisationseinheit angelegt** werden.
- Auf Wunsch kann der **Migrationsbenutzer gelöscht** werden. In der Regel wird dieser nach der Migration nicht mehr benötigt, da der Administrator aus dem migrierten Backup als Benutzer übernommen und zukünftig genutzt wird.

! Man sollte vor dem Import genau abwägen, ob man im Master Key Modus oder Ende zu Ende verschlüsselt importiert. Dies kann rückwirkend nicht mehr geändert werden. Weitere Informationen dazu finden Sie im Kapitel Active Directory Anbindung.

Es gilt zu beachten, dass alle lokalen Benutzer sowie jene, welche mit der Ende zu Ende Verschlüsselung migriert werden, eine E-Mail mit einem zufallsgenerierten Passwort erhalten. Benutzer, welche im Master Key Modus migriert werden, können sich weiterhin mit dem Domänenkennwort anmelden.

Nach dem Start werden die Daten analysiert und aufbereitet. Je nach Datenbank Größe kann dieser Schritt mehrere Stunden beanspruchen.

Sollte ein Fehler auftreten, erzeugt der Assistent einen Logfile-Eintrag. Dieser ist im Pfad **C:\Users\User\AppData\Roaming\MATESO\Migration** zu finden.

## Migration in eine bestehende Datenbank

Über Ribbon kann die Migration auch in eine bestehende Datenbank erfolgen. Der Ablauf der Migration bleibt gleich. Durch diese Funktion können mehrere Datenbanken zusammengeführt werden. Hierbei werden gleichlautende Datensätze, Dokumente, Formulare usw. doppelt angelegt. **Ausnahme**: Benutzer können doppelt angelegt werden und bekommen einen * am Ende des Namen. Sie können aber auch zusammengeführt werden. Tags werden nicht doppelt angelegt, sofern Sie identisch geschrieben sind.

Sobald die Migration startet, befindet sich die Datenbank im Migrationsmodus. Solange dieser aktiv ist, können keine Logbucheinträge erstellt werden. Sind Benutzer mit der

Datenbank verbunden, können Sie die Datenbank nicht verwenden, solange der Migrationsmodus aktiv ist.

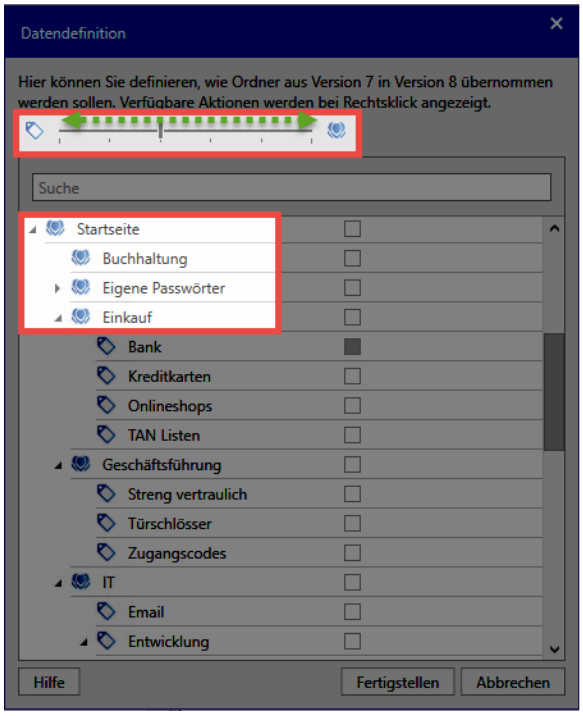
# Zuordnung von Tags und OUs

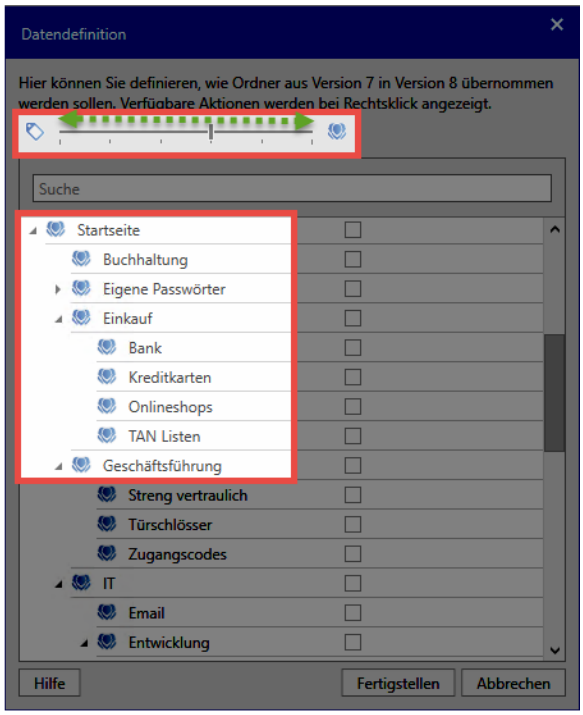
## Warum eine Zuordnung von Tags und OUs?

An den vorherigen Arbeitsschritt anschließend wird nun die Ordnerstruktur der Version 7 dargestellt. Aufgrund der eingangs bereits genannten Änderungen am Bedienkonzept der Version 8 muss festgelegt werden, wie die Daten zukünftig kategorisiert werden sollen. Da Ordner nicht mehr existieren wird festgelegt, welcher Ordner aus der Version 7 in der Version 8 in eine Organisationseinheit, bzw. ein Tag, umgewandelt werden soll. Die Bedeutung der Icons in der Ansicht sind nachfolgend aufgeschlüsselt:

- migriert den Ordner als Organisationseinheit
- migriert den Ordner als Tag
- legt fest, dass zu markiertem Ordner keine Kategorie erstellt wird

Über den Schieberegler wird festgelegt, bis in welche hierarchische Ebene im Zuge der Migration Ordner in Organisationseinheit umgewandelt werden sollen – alle darunterliegenden Ordner werden zu Tags. So kann eine gewisse Vorauswahl getroffen werden, welche dann noch manuell verfeinert werden kann. Durch wiederholtes “Klicken” wird zwischen Tag, Organisationseinheit und Ordnern ohne Zuordnung durchgeschalten.



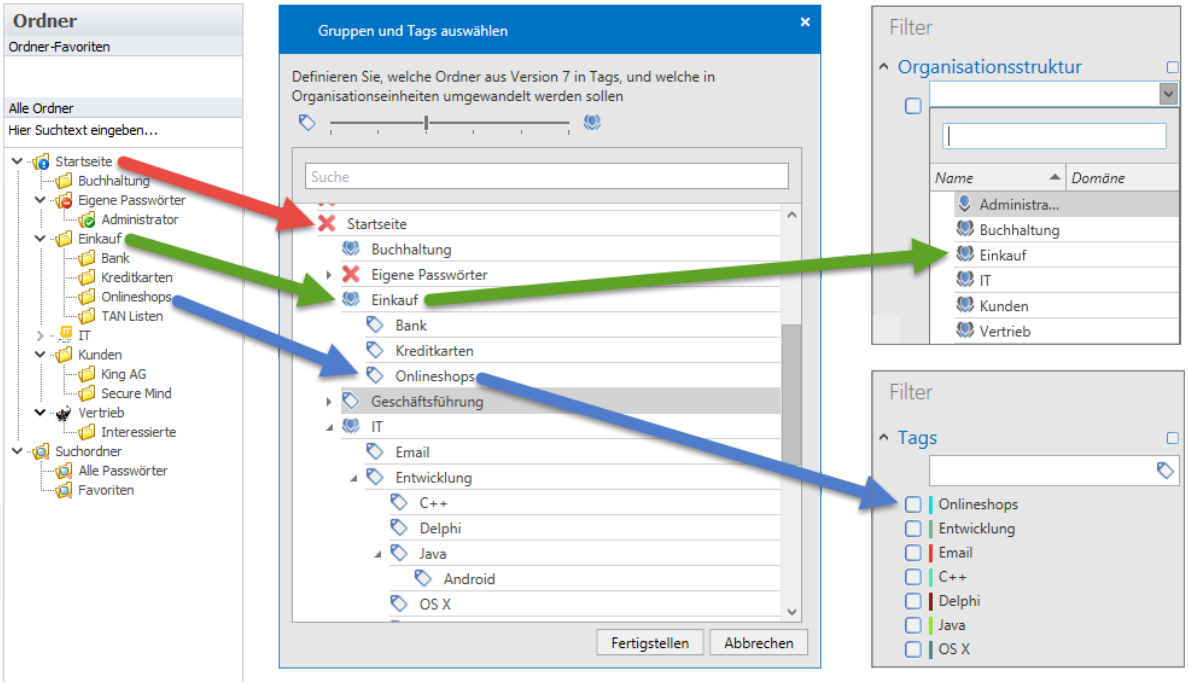




Über das Kontextmenü (rechte Maustaste) eröffnen sich weitere Optionen:

- Kategorisierung aller Unterobjekte als Organisationseinheit

- Kategorisierung aller Unterobjekte als Tag
- Alle Unterobjekte ignorieren
- Löschen aller zuvor gesetzten Markierungen

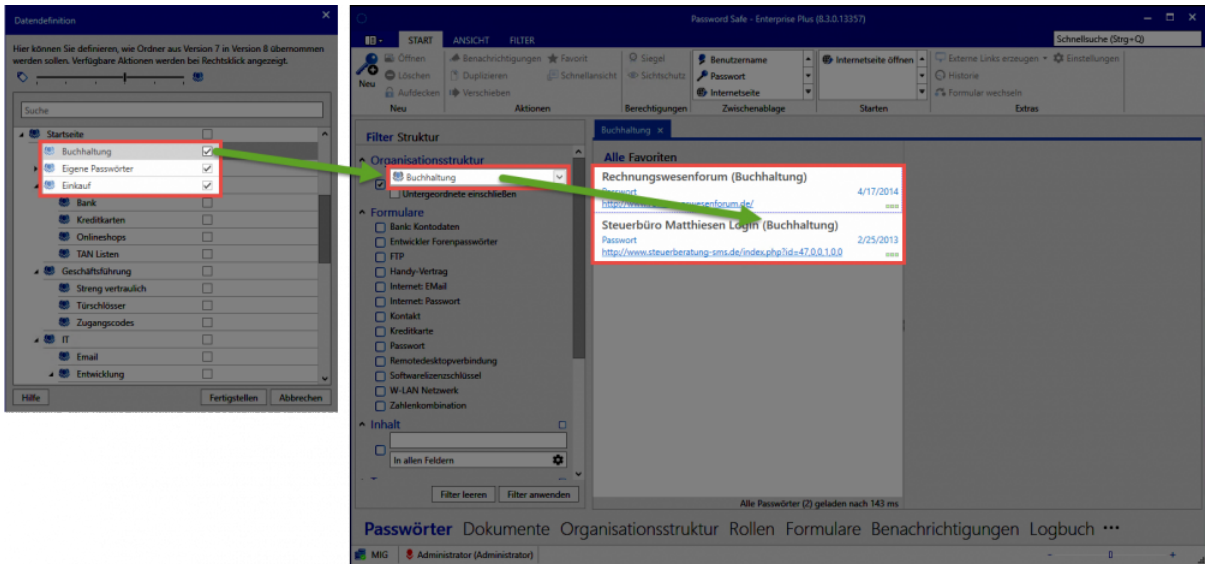
Im nachfolgenden **Schaubild** ist ein mögliches Vorgehen bei der Zuweisung von Ordnern zu Organisationseinheiten und Tags abgebildet:




Die Startseite sowie die Suchorder müssen nicht importiert werden. Der Import persönlicher Ordner wird ebenso nicht empfohlen. Die Datensätze werden in diesem Fall der Organisationseinheit des jeweiligen Benutzers zugeordnet. Im Zuge der Migration bietet sich darüber hinaus die Bereinigung aller Ordner ohne Inhalt an.

Während der Migration erhält der ausführende Benutzer Einsicht auf alle Ordner der Datenbank. Die Datensätze selbst sind während der Migration dem ausführenden Benutzer nicht einsehbar.

Es besteht auch die Möglichkeit die Ordnernamen in die Datensatzbeschreibung aufzunehmen. Hierfür steht bei jedem Ordner eine entsprechende Schaltfläche bereit.




Über das Kontextmenü, kann die Option für alle Ordner gesetzt werden.

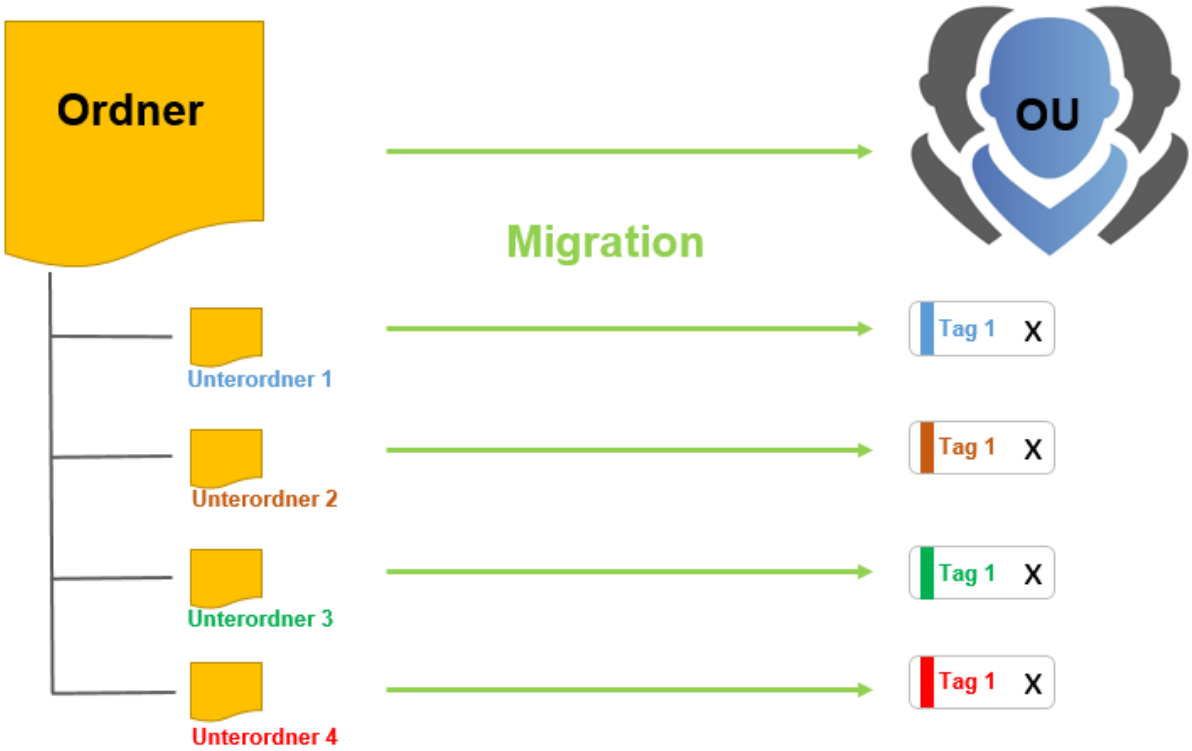
# Abschließen der Migration

Über **Fertigstellen** werden die Daten in die Datenbank übertragen. **Die Migration kann – je nach Umfang – durchaus mehrere Stunden dauern**. Falls kein Master Key Modus gewählt ist bekommen die importierten Benutzer per E-Mail zufallsgenerierte Passwörter und können sich direkt anmelden. Beim ersten Anmelden müssen diese Passwörter geändert werden. Falls konfiguriert, wird der Benutzer, mit dem die Migration durchgeführt wurde, direkt gelöscht.

# Berechtigungen nach der Migration

## Was geschieht mit den Berechtigungen aus den ursprünglichen Ordnern?

Ordnerstrukturen sind in der Version 7 unter anderem für die strukturierte Datenhaltung verantwortlich. Wie im vorherigen Kapitel beschrieben erfolgt das Mapping auf OUs und Tags direkt im Migrationsprozess. Je nach Konfiguration werden aus Ordnern OUs, aus Unterordnern Tags:




Natürlich sind Ordner in der Version 7 auch die Basis für Berechtigungen. Erstellte man einen Datensatz in einem Ordner, so wurde der Datensatz analog zu den Berechtigungen des zugehörigen Ordners berechtigt. Solange nur vereinzelte Ordner aus der Version 7 im Rahmen der Migration auf Organisationseinheiten in der Version 8 “gemappt” werden, ändert sich dieses Vorgehen nicht. Es wird für die Organisationseinheit automatisch ein Rechtepreset definiert (**vordefinierte Rechte**), welches zukünftig zu erstellenden Datensätzen automatisch die vorgesehenen Rechte gibt. Die Unterordner hatten Ihre eigenen Berechtigungen. Da bei der Zuordnung von Tags aus Unterordnern nun Tags werden können, muss ein neuer Mechanismus angewendet werden, da Tags keine Rechte besitzen. Um ein einheitliches System verfolgen zu können, helfen hier die den vordefinierten Rechten zugehörigen Rechtevorlagengruppen weiter.


Berechtigungen auf Ordner
Berechtigungen auf Unterordner
Migration
Vordefinierte Rechte
Rechtevorlagengruppen

# Checkliste nach der Migration

## Datenbankübersicht v7 und v8

Um den Zustand der Datenbank vor und nach der Migration gegenüberstellen zu können, ist die bereits im Rahmen der Migrationsvorbereitungen genannte Datenbankübersicht der Version 7 sowie das Pendant der Version 8 sehr hilfreich. Da die Version 8 in vielerlei Hinsicht Unterschiede vorweist, werden nicht alle Werte übereinstimmen. Hinzu kommen etwaige Bereinigungen der Datenbank (s. Kapitel Vorbereitungen). Auf die einzelnen Werte der beiden Datenbankübersichten soll nachfolgend eingegangen werden.

### Datensätze

- Die Anzahl aller Datensätze muss in Version 7 und 8 übereinstimmen
- Auch persönliche Datensätze werden hier gezählt. Auf beiden Seiten wird in der Übersicht immer die Anzahl aller Passwörter dargestellt.

> In der Version 7 können unter „Alle Passwörter“ all diejenigen Passwörter eingesehen werden, auf welche ein Benutzer berechtigt ist. Dies kann in der Version 8 ggf. nicht immer überprüft werden, da die Version 8 maximal 1000 Passwörter ausgeben kann. Ist ein Benutzer auf mehr als 1000 Datensätze berechtigt, muss der Filter dementsprechend angepasst werden.

### Siegel

Siegel werden – je nach Ausprägung in der Version 7 – unterschiedlich migriert. Sicherheitshalber sollte die Anzahl der versiegelten Datensätze ebenso abgeglichen werden.

- **Siegel mit Freigabemechanismen** werden so migriert, dass freigabeberechtigte Nutzer/Gruppen aus der Version 7 auch in Version 8 freigabeberechtigt sind
- **Siegel ohne Freigabemechanismen** werden nicht als Siegel migriert. In der Version 7 bewirkt das Anbringen eines Siegels ohne einen Freigabemechanismus, dass eine Benachrichtigung versandt wird, wenn ein Benutzer das Passwort einsieht. Beim Import derlei Siegelmechanismen wird in der Version 8 eine dementsprechende Benachrichtigung konfiguriert. Der Mechanismus bleibt demnach erhalten, er wird jedoch nicht mehr als Siegel dargestellt.
- Benutzer aus **Leichten Siegeln** werden in der Version 8 im Siegel hinterlegt, sind jedoch nicht freigabeberechtigt. Der Datensatz wird für diese Benutzergruppe auch nicht versiegelt. Sie sind also vom vorhandenen Siegel nicht betroffen und können den Datensatz öffnen, ohne das Siegel brechen zu müssen.
- **Begründungen für den Siegelbruch** aus der Version 7 werden übernommen.

- Eine Abweichung existiert es bei denjenigen Benutzern, welche in der Version 7 das Siegel bearbeiten durften. Diese werden bei der Migration ignoriert, da in der Version 8 stets alle freigabeberechtigten Benutzer das Siegel bearbeiten dürfen – es besteht also fortan eine **Kopplung an das Berechtigungssystem** (vgl. Kapitel zu Siegeln).
- Die Siegelhistorie entfällt ersatzlos

### Freigaben

- Im Bereich Freigaben kann es zu Abweichungen nach einer durchgeführten Migration kommen, da über das Workflow System konfigurierte Freigaben entfallen (Workflow System existiert in der Version 8 nicht mehr)

### Sperren

- Gesperrte Datensätze werden in der Version 8 mit einer Sichtsperre versehen
- Benutzer, welche in der Version 7 die Sperre bearbeiten durften, werden in der Version 8 nicht gesperrt.

### RDP Verbindungen

- Datensätze, welche auf dem Formular **Remotedesktopverbindung** basieren, werden während der Migration gesplittet. Es werden Datensätze mit den Anmeldedaten erstellt. Die Verbindungsdaten werden in entsprechenden RDP Anwendungen hinterlegt. Diese werden dann direkt mit den Datensätzen verknüpft. Weitere Informationen dazu finden Sie im Kapitel Anwendungen.

### Anwendungen

- Anwendungen aus der Version 7 werden – soweit möglich – konvertiert. Es ist jedoch möglich, dass einzelne Anwendungen nochmals neu angelernt werden müssen. Alle Webseiten sollten jedoch ohne große Probleme wieder automatisch befüllt werden können. Nach der Migration sind alle User über eine entsprechende Rolle lesend auf alle Anwendungen berechtigt. Sollte dies nicht gewünscht sein, müssen die Rechte dementsprechend angepasst werden.

> In der Password Safe Version 8 funktioniert die automatische Eintragung in Webseiten meist ohne Anwendung – Web Anwendungen sind also nur in Ausnahmefällen nötigt. Daher bietet es sich an, evtl. importierte Web Anwendungen zu löschen. Der Filter gibt die Möglichkeit, diese schnell zu selektieren.

### Benutzer

Benutzer aus der Version 7 werden eins zu eins übernommen. Je nachdem, um welchen Benutzertyp es sich handelt und in welchem Modus migriert wird, unterscheidet sich die Anmeldung der migrierten Benutzer.

- **Lokale Benutzer** erhalten ein neues, zufällig generiertes Passwort per E-Mail zugeschickt. Mit diesem erfolgt die initiale Anmeldung.
- **AD Benutzer im Ende zu Ende Modus** bekommen per E-Mail ein neues Passwort zur initialen Anmeldung. Diese erfolgt nur mit dem Benutzernamen, **ohne** vorangestellte Domäne.
- **AD Benutzer im Master Key Modus** können sich direkt mit Ihrem Domänenkennwort anmelden. Auch hier gilt, dass die Anmeldung ohne vorangestellte Domäne erfolgt.

### Gruppen

- Alle Gruppen aus Version 7 werden in der Version 8 zu Rollen.
- In Version 8 gibt es **keine** Gruppen in Gruppen Verschachtelungen mehr – es existieren nur noch Rollen in einer flachen Hierarchie. Hieraus können also mehr Rollen resultieren als in der Version 7 vorhanden waren.

### Rollen

Während der Migration werden standardmäßig einige Rollen erstellt, um die Berechtigungen der Version 7 in der Version 8 abzubilden. Dies betrifft die Sichtbarkeiten auf

- Anwendungen
- Benutzer
- Formulare
- Rollen

> Der Administrator erhält während der Migration Mitgliedschaft auf diese Rollen. Nach der Migration sollten diese geprüft und nach Bedarf angepasst werden.

### Eigene Icons

- Eigene Icons werden nicht importiert, da es diese in der Version 8 nicht mehr gibt

### Labels

- Labels aus der Version 7 werden in der Version 8 zu Tags.
- Die Farbe wird beibehalten
- Falls notwendig kann man mit Labels vor der Migration Datensätze „Taggen“ und so einen bestimmten Bereich bereits vor der Migration definieren

### Aufgaben und Nachrichten

- Aufgaben und Nachrichten aus Version 7 werden nicht migriert

### Ordner

- Da es in der Version 8 keine Ordner mehr gibt, werden diese im Migrationsassistenten als Organisationseinheiten oder Tags importiert. Da die Benutzer in der Version 7 persönliche Order (beispielsweise für Nachrichten und Aufgaben) haben, kann die Anzahl hier stark schwanken.

### Workflow Events

- Password Safe Version 8 verfügt aktuell über kein Workflow System. Konfigurierte Events werden demnach nicht importiert.
- Im Workflow System konfigurierte Benachrichtigungen können nun über das gleichnamige Modul abgebildet werden.

### System Tasks,

- System Tasks der Version 8 unterscheiden sich deutlich von denen der Version 7. Eine Migration ist nicht möglich.

### Logbuch Einträge

- Alle Logbucheinträge zu den Themen Passwort, Gruppe, Dokument, Anwendung, Label, Benutzer, Ordner, Siegelvorlagen, Siegel und Formular werden importiert und dargestellt.

### Formulare

- Es werden nur diejenigen Formulare importiert, denen ein Passwort zugeordnet ist. Die Anzahl kann also abweichen.

### Dokumente

- Alle in der Version 7 vorhandenen Dokumente werden migriert
- Derjenige Ordner, in welchem sich das Dokument befand, wird zu einem Tag
- Alle evtl. übergeordneten Ordner werden ignoriert
- Die Rechte auf die Dokumente werden übernommen
- Eine Verknüpfung mit Datensätzen ist im Footer des Lesebereichs des Datensatzes möglich

### Externe Links

- Externe Links werden nicht migriert.

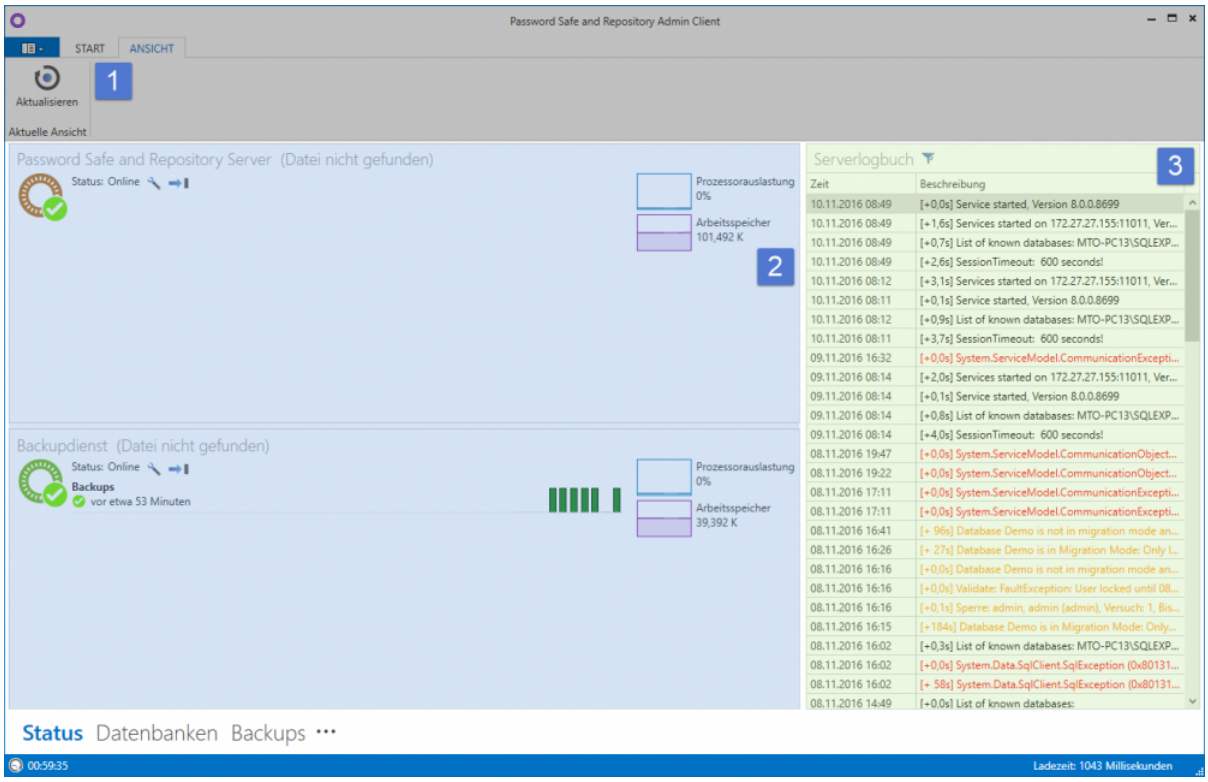
# Bedienung und Aufbau

## Aufbau des Admin Clients

Der Aufbau des Admin Clients ist stark an die Struktur des eigentlichen Clients angelehnt. Die Bedienelemente wie Ribbon, Info- und Detailbereich lassen sich dementsprechend aus dem Kapitel bezüglich des Clients ableiten.

> Zur ersten Anmeldung am AdminClient wird ein Initialpasswort benötigt. Dieses lautet “admin”. Direkt nach der Anmeldung sollte es geändert und sauber dokumentiert werden.

## Das Modul Status




### 1. Ribbon

Wie gewohnt ist oben die Ribbon zu finden. Da das Modul ein rein informatives ist, gibt es in der Ribbon keine Funktionen, außer dem Aktualisieren der Ansicht

### 2. Infobereich

- Der Infobereich links zeigt die Status der einzelnen Dienste an. Über das Icon können die Dienste konfiguriert werden. Standardmäßig wird die Konfiguration aus der Basiskonfiguration verwendet. Falls nötig können einzelne Parameter ersetzt bzw. auf die persönlichen Bedürfnisse angepasst werden.
- Über kann der jeweilige Dienst gestoppt bzw. gestartet werden
- Rechts im Infobereich werden über zwei Kurven jeweils die Auslastung von Prozessor und Arbeitsspeicher dargestellt.
- Im Bereich “Backupdienst” werden über ein Diagramm die letzten Backups dargestellt. Hierbei steht ein grüner Balken für ein erfolgreiches Backup, ein roter symbolisiert dementsprechend ein fehlgeschlagenes. Mouseover werden weitere Informationen eingeblendet.

### 3. Serverlogbuch

Rechts im Bild wird das Serverlogbuch dargestellt und dient der Überwachung und Kontrolle des Servers. Es stellt alle relevanten Aktionen am Server nachvollziehbar dar, wobei immer die letzten 100 Einträge angezeigt werden. Hierbei gilt:

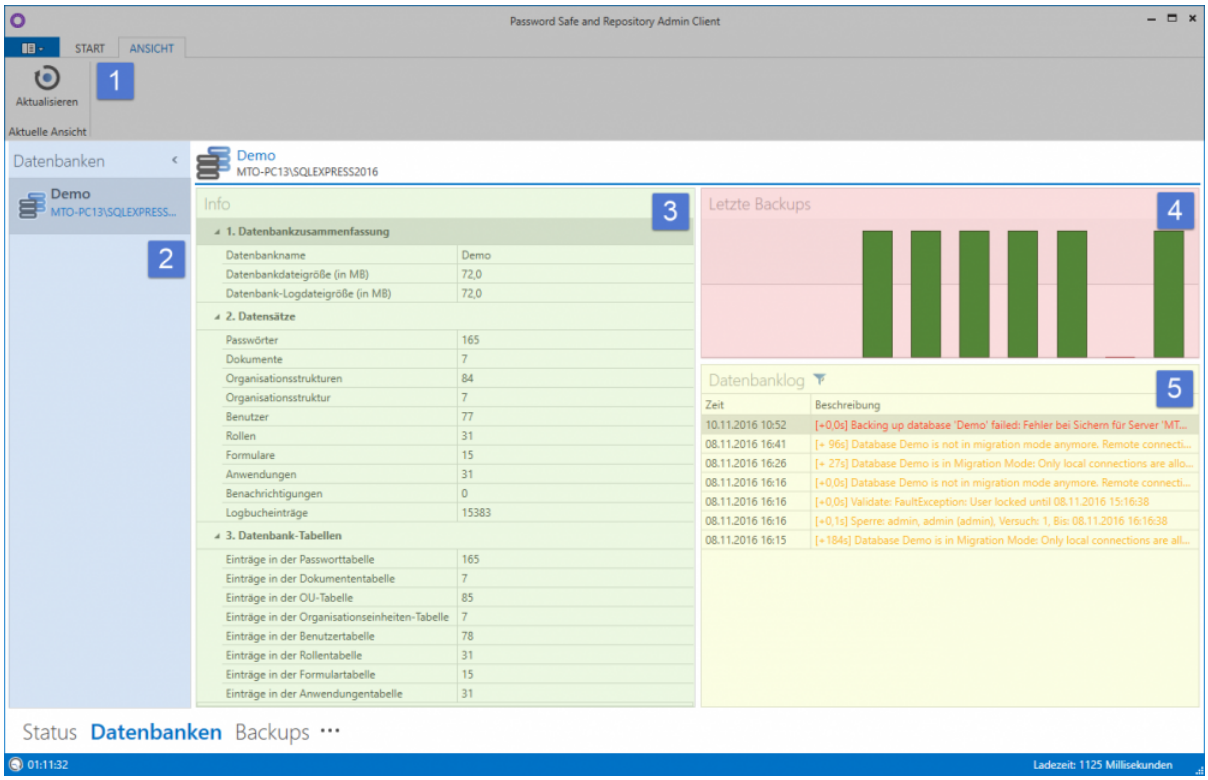
| | |
|---|---|
| Erwartete Aktionen | schwarz |
| Ereignisse, welche Aufmerksamkeit fordern | orange |
| Probleme und Abbrüche | rot |

- Erwartete Aktionen – wie z.B. das Starten und Beenden von Diensten – werden schwarz dargestellt
- Alle Ereignisse (z.B. fehlgeschlagene Loginversuche), welche Aufmerksamkeit erfordern, sind orange dargestellt
- Alle Probleme (z.B. Abbrüche) werden rot eingefärbt

Das Serverlogbuch kann über die Spaltenüberschriften nach Datum und Beschreibung auf- und absteigend sortiert werden. Über lässt sich der dargestellte Zeitraum einschränken.

# Das Modul Datenbanken

Datenbanken werden in einem eigenen Modul verwaltet. Ebenso können alle relevanten Informationen zu den vorhandenen Datenbanken abgerufen werden – ganz ohne Zugriff auf den SQL-Server.




## 1. Ribbon

## 2. Datenbankenübersicht

In der Datenbankenübersicht alle Datenbanken alphabetisch sortiert aufgeführt. Dieser Bereich kann über das Pfeilsymbol am oberen, linken Rand minimiert werden. Über einen Rechtsklick auf eine der Datenbanken, wird ein Kontextmenü mit allen verfügbaren Funktionen eingeblendet.

## 3. Infobereich

Im Infobereich werden alle Infos zur aktuell in der Datenbankenübersicht selektierten Datenbank dargestellt. Diese sind in die drei Unterbereiche “Datenbankzusammenfassung, Datensätze und Datenbanktabellen “ unterteilt.

## 4. Letzte Backups

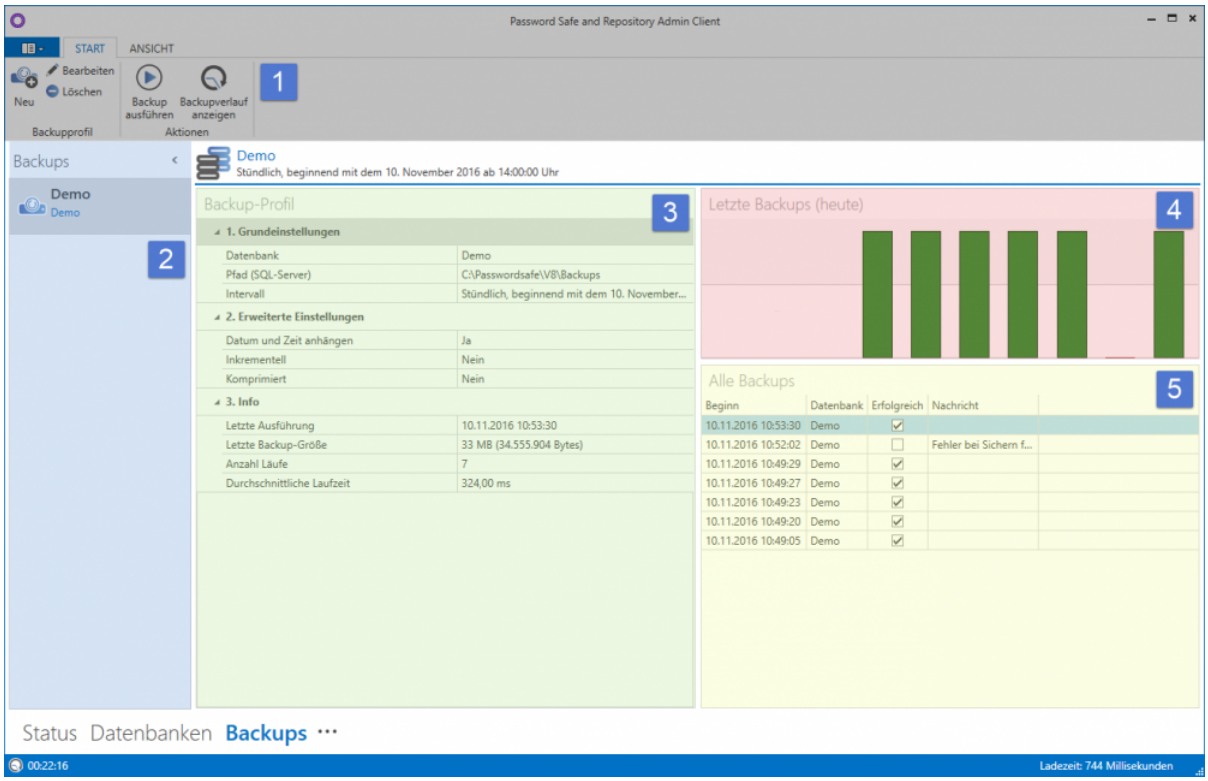
Liste der zuletzt gelaufenen Backups. Kann nach Datum sortiert werden

## 5. Datenbanklog

Der Datenbanklog dient der Überwachung und Kontrolle der einzelnen Datenbanken. Es werden alle relevanten Aktionen zur selektierten Datenbank nachvollziehbar in einer Liste dargestellt. Analog zum Serverlog erfolgt eine Kategorisierung gemäß der genutzten Farbe.

# Das Modul Backups

Auch zur Konfiguration der Backups gibt es ein eigenes Modul. Somit können sämtliche Backups direkt im Admin Client konfiguriert und verwaltet werden.




### 1. Ribbon

### 2. Backupübersicht

Hier werden alle konfigurierten Backups aufgeführt. Kann nach links minimiert werden. Weitere Funktionen über Rechtsklick

### 3. Infobereich

Der Infobereich ist in drei Bereiche aufgeteilt. Es sind die “Grundeinstellungen, erweiterte Einstellungen sowie Infos” zur ausgewählten Datenbank nutzbar

### 4. Letzte Backups

Rechts werden in einer Liste die zuletzt gelaufenen Backups dargestellt.

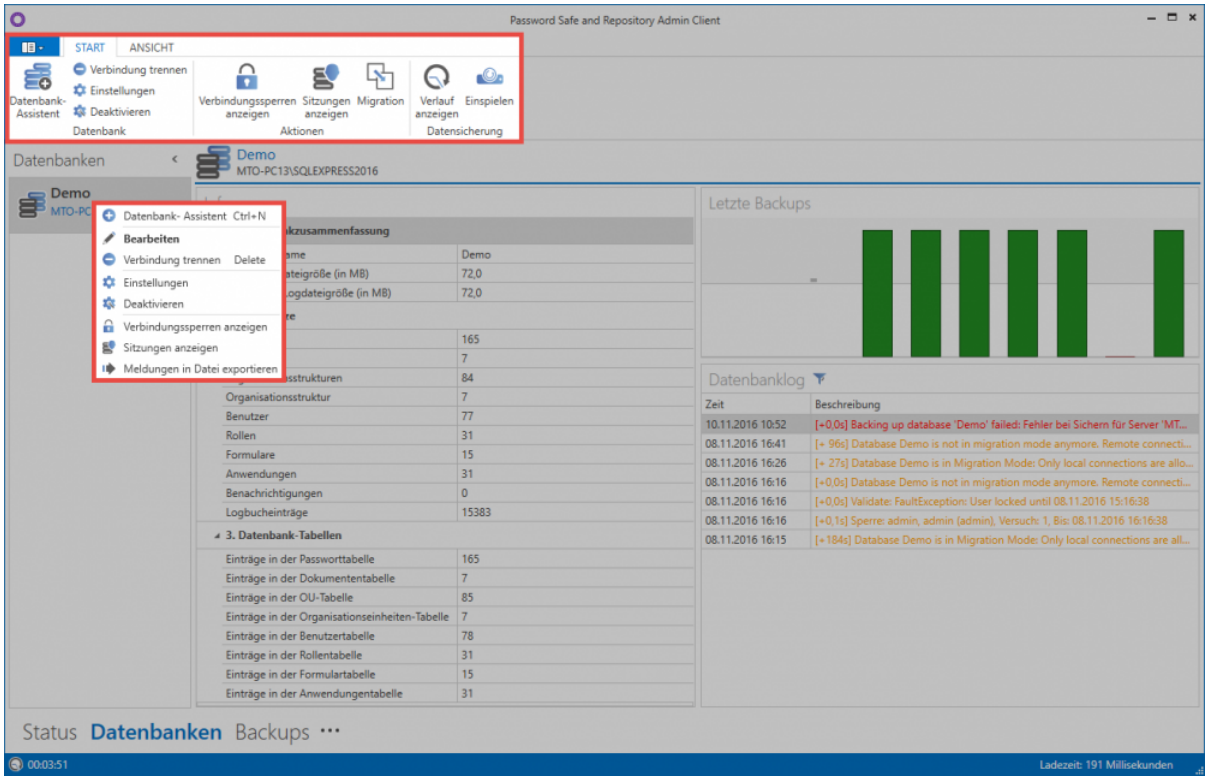
### 5. Alle Backups

Eine tabellarische Übersicht stellt alle bisherigen Backups dar. Die Ansicht kann – wie gewohnt – sortiert werden. Hier ist auf einen Blick zu sehen, wann welche Datenbank gesichert wurde und ob das Backup erfolgreich war.

# Verwaltung von Datenbanken

## Datenbank verwalten

Sowohl über das Kontextmenü der rechten Maustaste als auch über die Ribbon können die zur Verfügung stehenden Aktionen selektiert werden.




## Datenbankeinstellungen

Sämtliche Datenbankeinstellungen sind in der Datenbank hinterlegt. Um die Einstellungen zu bearbeiten ist zuvor eine Anmeldung nötig. Hierfür kann jeder beliebige, in der Datenbank existente Benutzer, verwendet werden. Über die Ribbon können stets die globalen Einstellungen wiederhergestellt werden.

### Multifaktor-Authentifizierung

In diesem Bereich kann konfiguriert werden, welche Dienste für eine Multifaktor Authentifizierung verwendet werden sollen. Verfügbar sind **RSA Secure ID**, **SafeNet** sowie **YubiKey NEO** und **YubiKey Nano**. Nach Selektion des gewünschten Dienstes, werden die jeweiligen Zugangsdaten angegeben. Es ist auch mehrere Dienste zu konfigurieren. In diesem Fall kann dann am Client ausgewählt werden, welches Verfahren die Einzelnen Benutzer verwenden.

Weiterführende Informationen zu diesem Thema sind im Kapitel **Multifaktor-Authentifizierung** zu finden.

### PKCS#11

Über die PKCS#11 Schnittstelle können die Serverschlüssel über ein Hardwaresicherheitsmodul (HSM) geschützt werden. Hier kann Schnittstelle konfiguriert werden.

# Datenbankaktionen

### Verbindungssperren anzeigen

In der Ribbon können alle Verbindungssperren angezeigt werden. Hierfür muss man sich zunächst an der Datenbank anmelden. In einer Liste werden dann alle gesperrten User angezeigt. Angezeigt werden:

- Benutzername (sofern bekannt)
- Grund der Sperre
- Anzahl der Loginversuche
- Ablauf der Sperre. Über einen Rechtsklick auf einen Eintrag kann der Benutzer entsperrt werden.

Über die entsprechende Schaltfläche kann ein User manuell gesperrt werden. Es muss der User gewählt werden, der Ablauf der Sperre konfiguriert und ein Grund angegeben werden.

### Sitzungen anzeigen / trennen

Über die entsprechende Schaltfläche können alle aktuell verbundenen Clients angezeigt werden. Nach Selektion einer Sitzung kann die Verbindung getrennt werden.

### Migration

Nach dem Auswählen einer Datenbank kann über die Ribbon die Migration gestartet werden. Über diesen Weg können auch mehrere Version 7 Datenbanken zu einer zusammengeführt werden.

> **!** Durch den Start der Migration wird die Datenbank in den Migrationsmodus gesetzt. Für die Dauer der Migration ist eine Anmeldung an der Datenbank nicht mehr möglich – bereits angemeldete Benutzer bekommen einen entsprechenden Hinweis. Die Sessions bleiben jedoch bestehen, so dass die Benutzer direkt weiter arbeiten können, sobald die Migration beendet ist.

# Datensicherung

Hier kann sowohl der Verlauf aller getätigten Backups angezeigt als auch ein Backup eingespielt werden.

### Verlauf anzeigen

Alle Backups der Datenbank werden hierarchisch in einer sortierbaren Liste dargestellt.

### Einspielen

Hierüber kann ein Backup rückgesichert werden. Dies kann über eine Datei oder aus der Historie heraus geschehen. Beschrieben wird der Vorgang unter Backupverwaltung

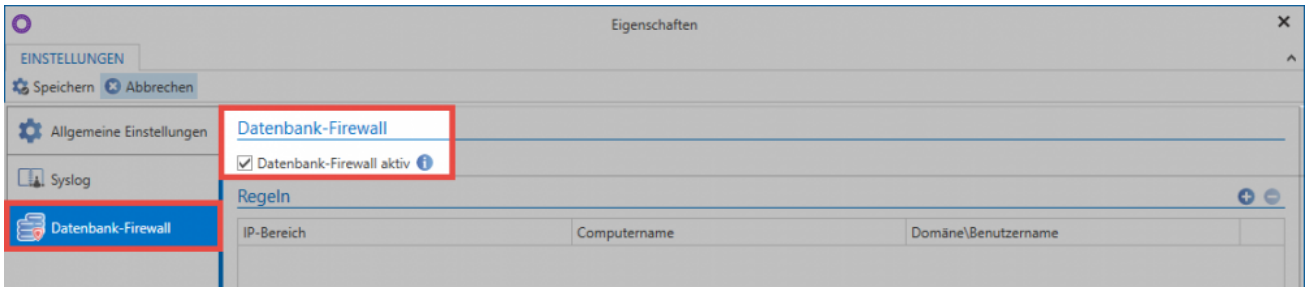
# Datenbank Firewall

## Was ist die Datenbank Firewall?

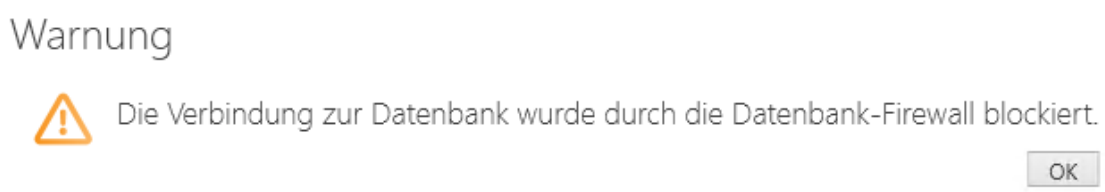
Die Datenbank Firewall ermöglicht es den Zugriff auf die Datenbank zu reglementieren. Hierbei wird auf eine Whitelist gesetzt. Über Firewall Regeln können dann einzelne Zugriffe freigegeben werden.

## Aktivieren der Firewall

Die Firewall kann direkt in den Datenbank Einstellungen aktiviert werden.




Nach dem Aktivieren ist der Zugriff auf die Firewall gesperrt. Anmeldeversuche werden direkt blockiert.




## Firewall Regeln

Im rechten Bereich werden bereits gesetzte Regeln angezeigt. Über und können Regeln hinzugefügt oder auch gelöscht werden. Über einen Doppelklick werden Regeln bearbeitet.


Es stehen folgende Möglichkeiten bereit:

- Über die **IP-Adresse** wird der Zugriff von einem einzelnen Rechner aus erlaubt.
- Optional kann auch ein **Bereich** für mehrere **IP-Adressen** gewählt werden.
- Ebenso ist es möglich die Freigabe über den **Computernamen** zu regeln.
- Schlussendlich kann auch der Zugriff für einen bestimmten Windowsbenutzer freigegeben werden. Beispielsweise um den Administrator unabhängig vom Rechner zu berechtigen.
- Über **Zugriff gewähren** wird festgelegt, ob der Zugriff erlaubt oder blockiert wird. Dies wird über entsprechende Icons symbolisiert.

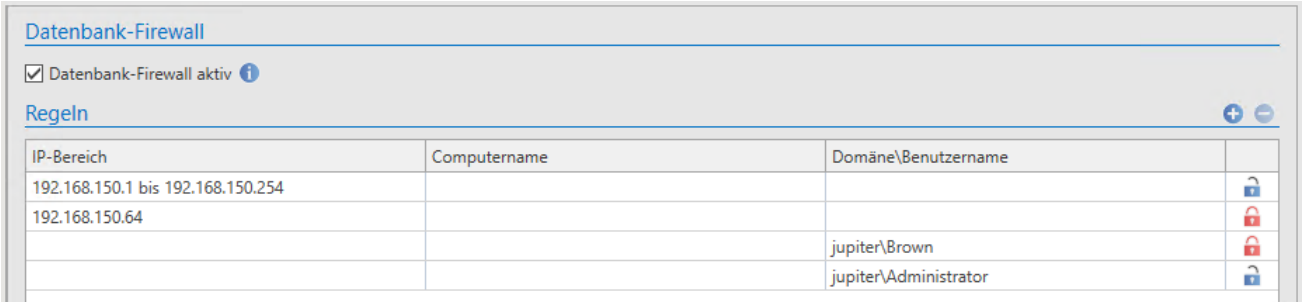
Selbstverständlich können die Regeln auch kombiniert werden. Somit kann z.B. festgelegt werden, dass sich von einer bestimmten IP Adresse aus nur ein definierter Benutzer anmelden kann.

> Die Kombination von Bedingungen erfolgt immer über **UND-Verknüpfungen**

Überschneiden sich zwei bzw. mehrere Regeln, so gilt immer, dass die Regel mit den geringeren Rechten überwiegt. Gibt beispielsweise eine Regel den Zugriff für eine IP-Range frei, während eine andere Regel einen speziellen Rechner innerhalb dieser Range blockiert, so greift selbstverständlich die Sperre.

# Beispiele

Anhand folgender Regeln soll die Funktionsweise näher verdeutlicht werden:




### Freigabe einer IP Range (Regel 1)

Die erste Regel aus dem Beispiel gibt die IP-Range von 192.168.150.1 bis 192.168.150.254 frei

### Sperre eines bestimmten Rechners (Regel 2)

Der Rechner mit der IP 192.168.150.64 befindet sich innerhalb der Range welche über Regel 1 freigegeben wurde. Der Zugriff von diesem PC aus wird über diese Regel verhindert.

### Sperre eines einzelnen Bentuzers (Regel 3)

Soll ein bestimmter Benutzer gesperrt werden (beispielsweise weil er die Firma verlassen hat) so ist dies ebenfalls möglich.

### Rechnerunabhängige Freigabe eines Benutzers (Regel 4)

Über diese Regel bekommt der Administrator Zugriff gewährt. Hierbei ist es egal, von welchem Rechner aus er sich anmelden möchte.

# Hauptmenü

## Was ist das Hauptmenü

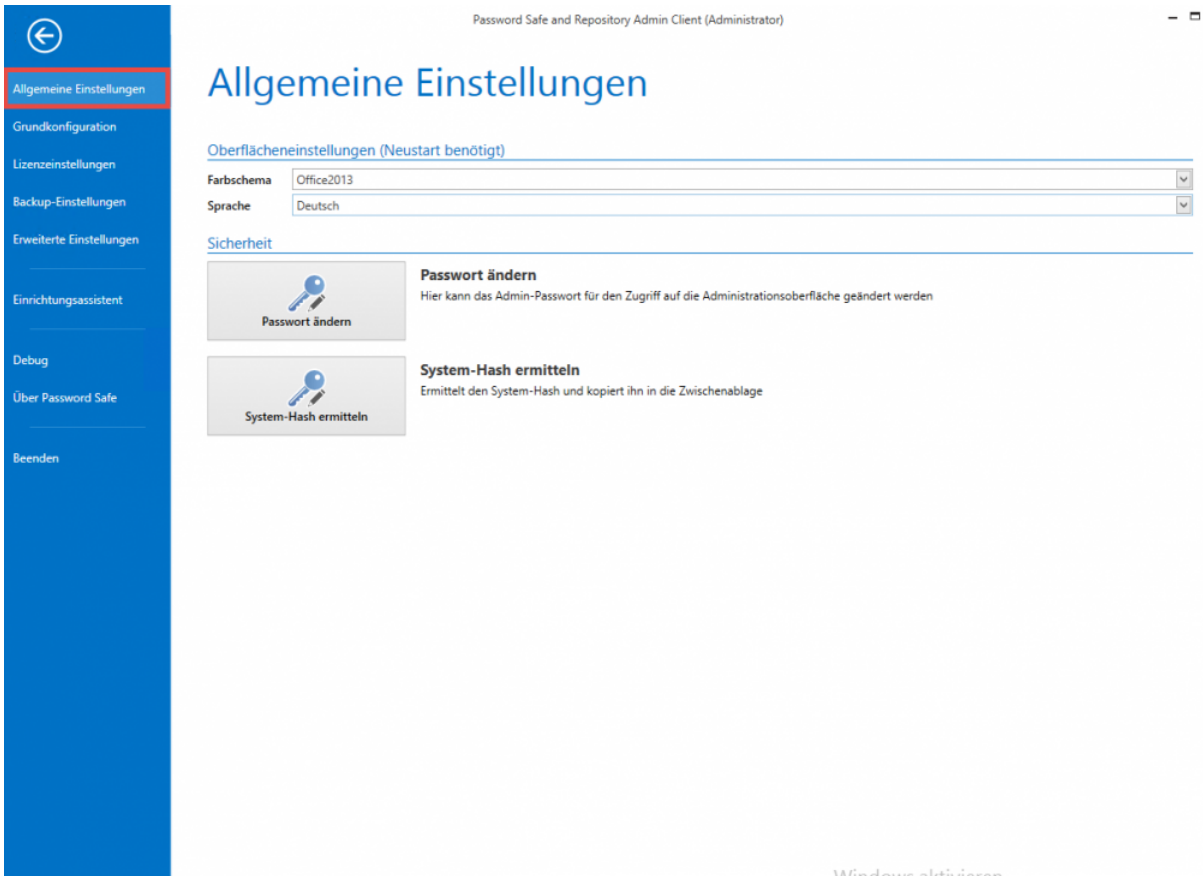
Analog zum Hauptmenü des Clients erfolgt die Bedienung und der Aufbau des Hauptmenüs/Backstage-Menüs. Dieser Bereich ist unabhängig vom aktuell ausgewählten Modul nutzbar.

- Allgemeine Einstellungen
- Backup-Einstellungen
- Lizenzeinstellungen
- Erweiterte Einstellungen

# Allgemeine Einstellungen

## Was sind die allgemeinen Einstellungen?

Innerhalb der allgemeinen Einstellungen werden Oberflächeneinstellungen bezüglich des Farbschemas sowie die genutzte Sprache konfiguriert. Ebenso kann hier das Passwort für die Anmeldung am Admin Client geändert werden.



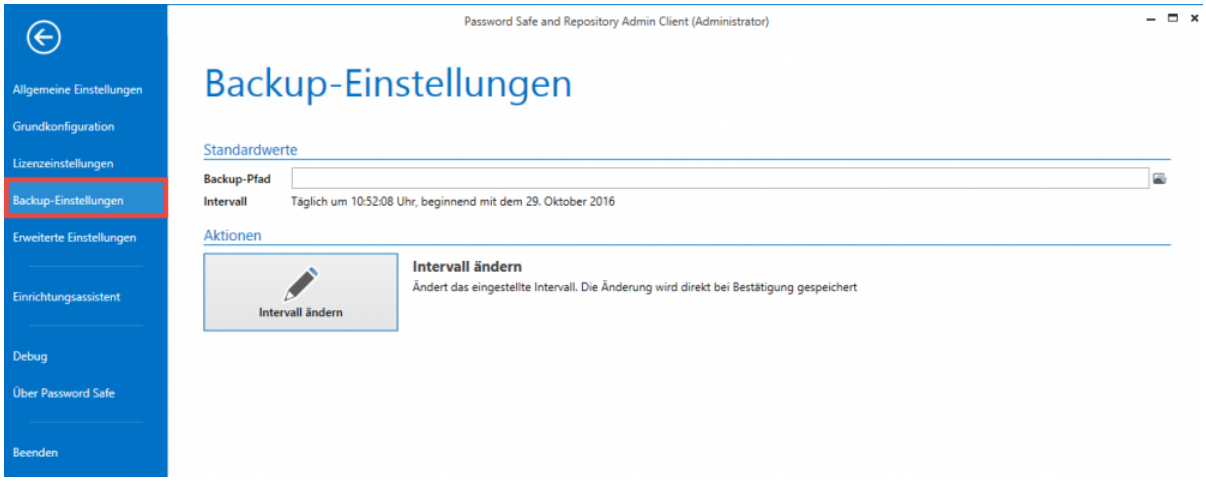

## System-Hash ermitteln

Diese Funktion ermittelt den System Hash und kopiert ihn in die Zwischenablage. Dieser Hash wird für die Offline Lizenz gebraucht.

# Backup-Einstellungen

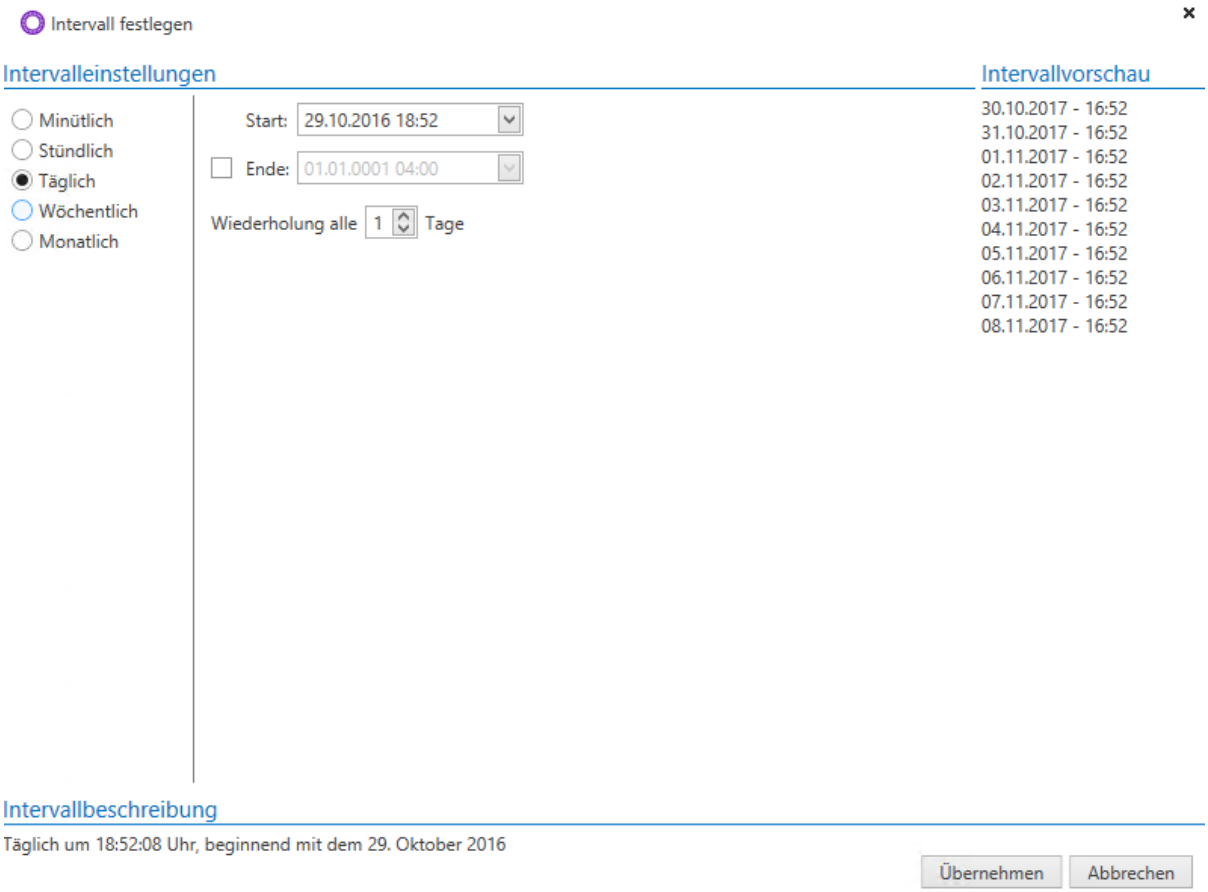
## Was sind Backup-Einstellungen?

Innerhalb der Backup-Einstellungen können die Standardwerte für die Durchführung von Datensicherungen festgelegt werden.




## Intervalleinstellungen

Das Intervall für Backups lässt sich beliebig definieren. Hierfür steht eigens ein Assistent bereit.


Intervall festlegen
Intervalleinstellungen
Intervallvorschau
Minütlich
Stündlich
Täglich
Wöchentlich
Monatlich
Start: 29.10.2016 18:52
Ende: 01.01.0001 04:00
Wiederholung alle 1 Tage
30.10.2017 - 16:52
31.10.2017 - 16:52
01.11.2017 - 16:52
02.11.2017 - 16:52
03.11.2017 - 16:52
04.11.2017 - 16:52
05.11.2017 - 16:52
06.11.2017 - 16:52
07.11.2017 - 16:52
08.11.2017 - 16:52
Intervallbeschreibung
Täglich um 18:52:08 Uhr, beginnend mit dem 29. Oktober 2016
Übernehmen
Abbrechen

# Backupverwaltung

## Einleitung

Das regelmäßige Sichern von Daten in Form von Backups sollte stets Teil jedes Sicherheitskonzeptes sein. Sollten am SQL Server zentral Backups erstellt werden, sollten die Password Safe Datenbanken hier ebenso aufgenommen werden. Werden keine zentralen Backups auf SQL-Ebene verwendet, können über den Admin Client Backup-Profile erstellt werden. Die Backups selbst werden dann am SQL-Server erzeugt.

## Unterschied zwischen differentiellem und Vollbackup

Im Vollbackup wird immer der komplette Datenstand einer Datenbank gesichert. Ein differentielles Backup erzeugt im ersten Schritt ebenfalls ein komplettes Abbild der Datenbank. Zukünftig werden dann jedoch lediglich Änderungen zum eingangs erstellten Backup gesichert. Hierdurch kann sowohl Zeit als auch Speicherplatz gespart werden.

## Backupkonzept

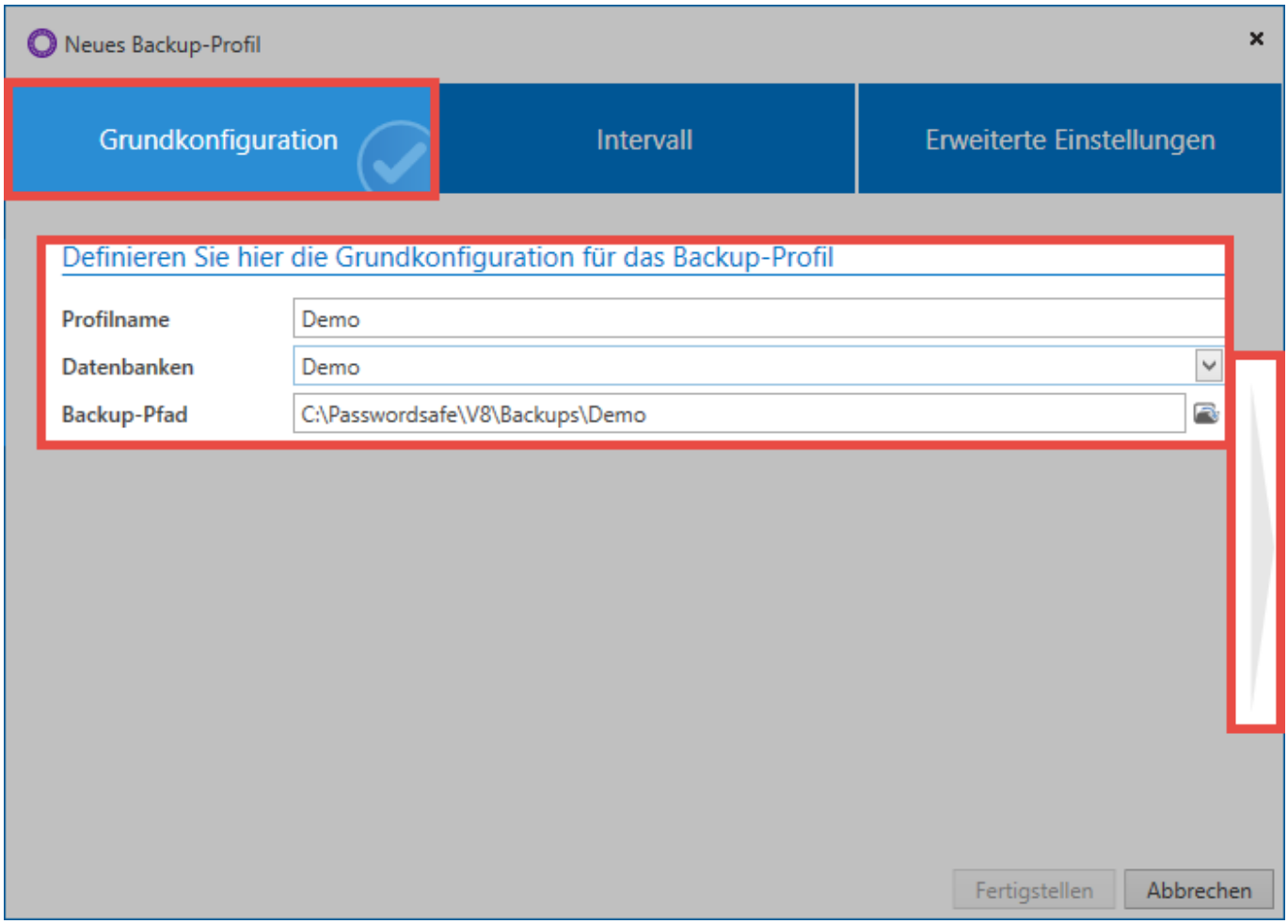
Empfohlen wird stündlich ein differentielles Backup zu erstellen. Zusätzlich sollte einmal in der Woche ein komplettes Backup erzeugt werden.

## Backup Zeitpläne verwalten

### Backup Zeitplan erstellen

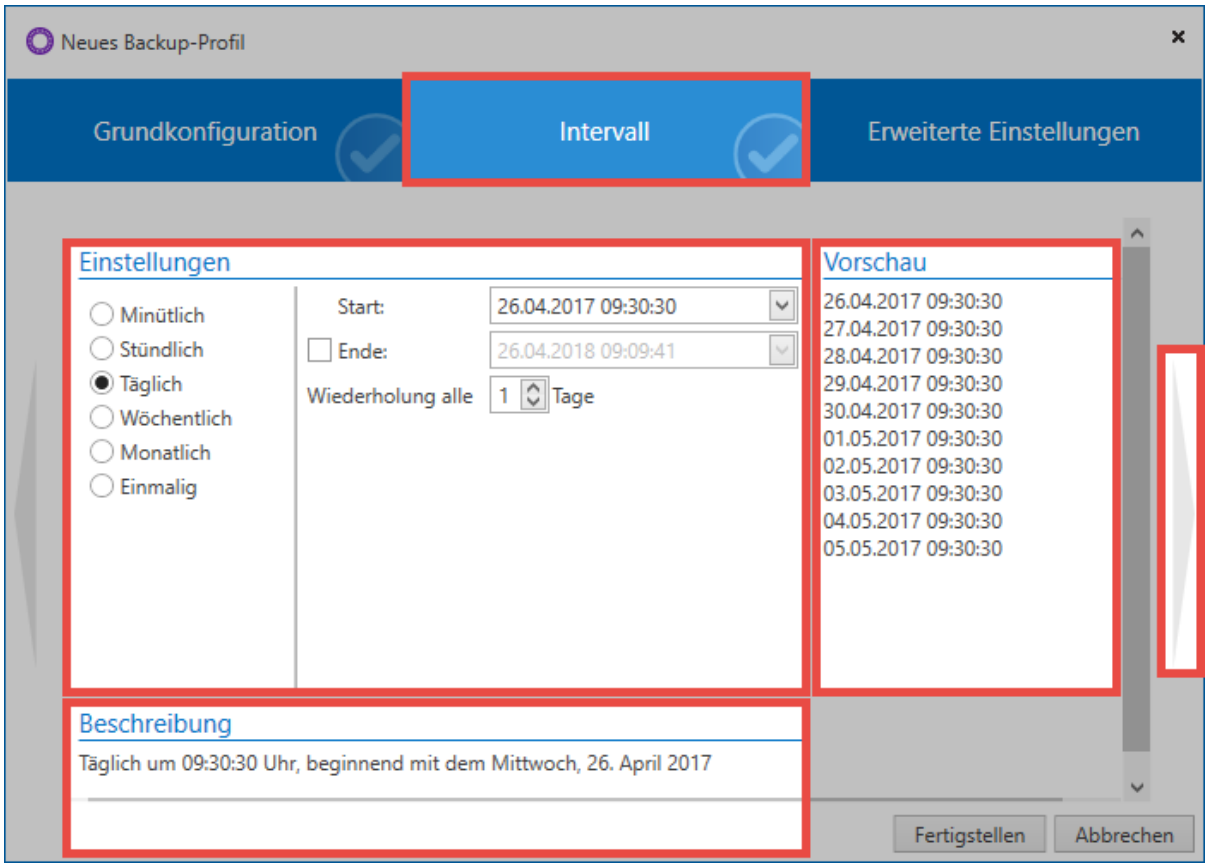
Über die Ribbon kann ein neuer Zeitplan erzeugt werden. Dies wird durch einen Assistenten erleichtert. Alle unter Backup-Einstellungen definierten Angaben, werden als Standard herangezogen.

Zunächst wird ein Profilname vergeben, zudem werden die gewünschten Datenbanken ausgewählt. Weiterhin muss festgelegt werden, in welchem Verzeichnis die Backups erzeugt werden sollen.

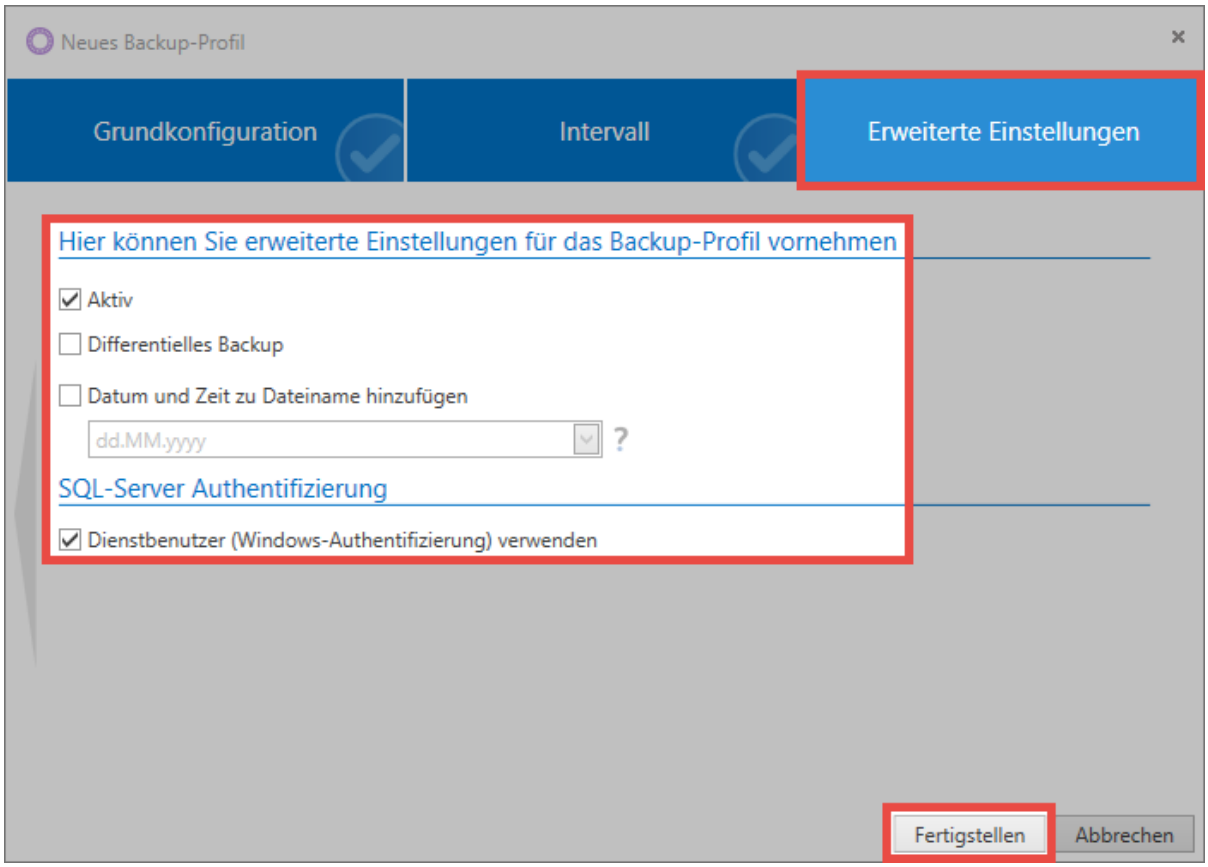



Es handelt sich hier um ein Verzeichnis direkt auf dem SQL-Server.

Nun wird das Intervall festgelegt in welchem die Backups erzeugt werden. Rechts wird in einer Vorschau dargestellt, wann die Backups zukünftig erstellt werde. Ein Enddatum kann optional angegeben werden.




In den erweiterten Einstellungen wird zunächst konfiguriert, ob das Backup direkt aktiv geschaltet werden soll. Zudem kann hier festgelegt werden, ob differentielle Backups erzeugt werden sollen. Werden dem Dateinamen Datum und Uhrzeit hinzugefügt, so wird mit jedem Lauf ein neues Backup erzeugt. Geschieht dies nicht, wird immer das letzte Backup überschrieben. Zum Erstellen des Backups kann der Dienstbenutzer verwendet oder ein Servicebenutzer mit Namen und Passwort angegeben werden.




### Lauf der Backups

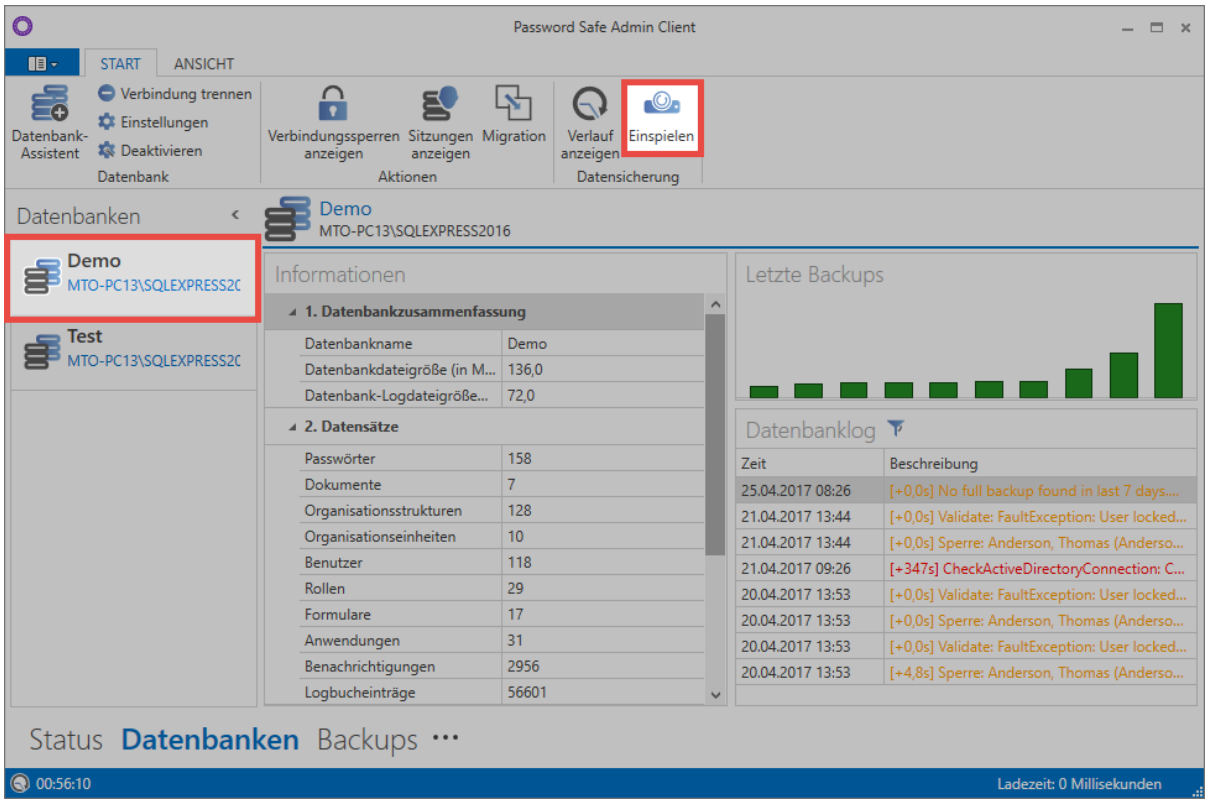
Die Backups werden durch den SQL-Server im Hintergrund ausgeführt. Wenn ein Fehler auftritt, wird dies in der Backupliste “orange” dargestellt. Unter alle Backups werden Informationen zum Fehler angezeigt, sofern der SQL-Server welche ausgibt. Läuft ein Backup 5x in Folge nicht, wird es automatisch deaktiviert. Dies wird in der Liste “rot” dargestellt. Der Zeitplan kann nicht direkt reaktiviert werden. Man muss ihn öffnen und anpassen.

### Weitere Backup Aktionen

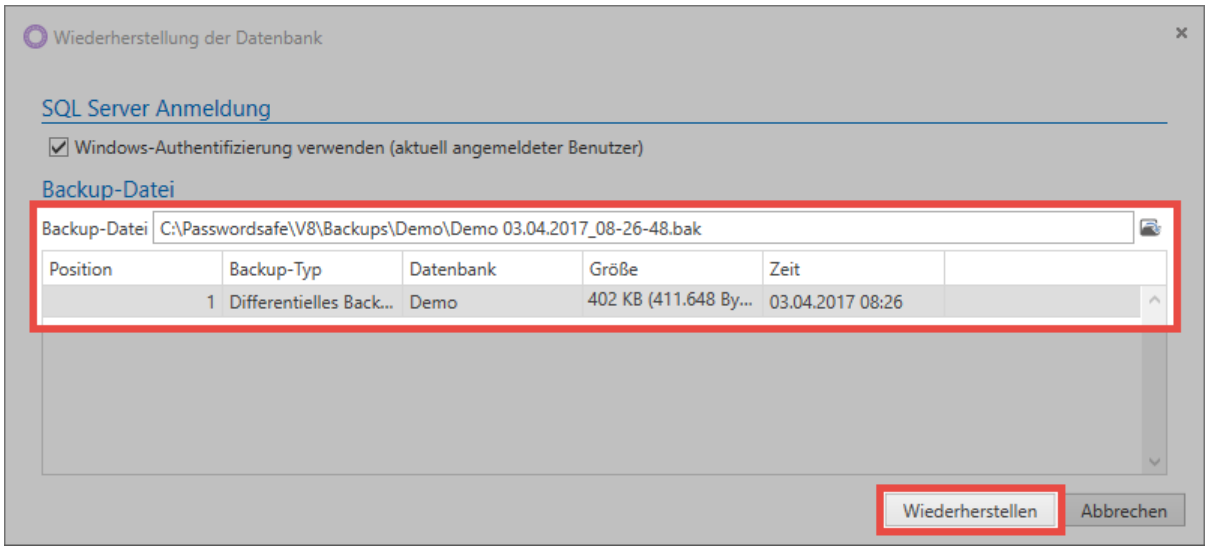
Über die Ribbon kann ein selektierter Zeitplan gelöscht werden. Über einen Doppelklick kann der Assistent eines Zeitplans aufgerufen werden um diesen zu ändern. Zudem kann über die Ribbon jederzeit ein Backup direkt gestartet werden. Hierfür muss der Backupdienst laufen. Ebenso kann man sich dies im Verlauf anzeigen lassen.

## Backup rücksichern

Das Rücksichern von Backups geschieht im Modul Datenbanken. Es kann nur in bestehende Datenbanken gesichert werden. Zunächst wird die gewünschte Datenbank ausgewählt. Nun kann in der Ribbon **Einspielen** gewählt werden.




Falls nötig, wird zunächst derjenige Benutzer angegeben, welcher sich am SQL-Server anmeldet – in der Regel wird jedoch der Dienstbenutzer verwendet. Nun kann die Backup-Datei ausgewählt werden. Anschließend werden alle in der Datei enthaltenen Backups dargestellt. Es genügt nun ein Klick auf **Wiederherstellen** um das Backup in die bestehende Datenbank zurückzuspielen.



# Desaster Recovery Szenarien

## Im Desaster Fall zu einer schnellen Lösung

Erfahrungsgemäß steht Password Safe in der IT an einer zentralen Stelle. Sollte es zu einem Ausfall kommen, muss so schnell als irgendwie möglich wieder Zugriff auf die Passwörter möglich sein. Dieses Kapitel soll helfen im Fall der Fälle schnell zu einer Lösung zu gelangen.

## Prävention

Es ist extrem wichtig einen sinnvollen Recoveryplan zu erstellen und entsprechende Vorbereitungen zu treffen. Leider kann kein fertiger Recoveryplan ausgeliefert werden, da dieser immer individuell erstellt werden muss. Folgende Punkte sollten dabei berücksichtigt werden:

### Erzeugen von Backups

Essentiell ist natürlich, im Desasterfall auf ein möglichst aktuelles Backup zugreifen zu können. Daher ist es nötig regelmäßig Backups zu erzeugen.

### Wer ist im Desasterfall zuständig?

Es sollte zunächst betrachtet werden, wer im Desasterfall eingreifen kann. Auch entsprechende Stellvertreter sollten festgelegt werden. Die zuständigen Mitarbeiter sollten innerhalb von Password Safe entsprechende Rechte haben.

### Bereitstellung der nötigen Passwörter

Welche Passwörter benötigen die Zuständigen um Password Safe wieder zum Laufen zu bringen?

- Domänenkennwort um sich an den einzelnen Rechner anmelden zu können
- Passwort für den Admin Client
- Zugangsdaten des Dienstbenutzers
- Zugangsdaten des SQL Nutzers
- Passwort zur Anmeldung an Password Safe

Weiterhin muss sichergestellt sein, dass die zuständigen Benutzer jederzeit Zugriff auf diese Passwörter haben. Folgende Möglichkeiten kommen in Frage:

- Hinterlegen der Passwörter im Firmentresor
- Erstellen entsprechender Offline Datenbanken

- Zyklisches Erstellen einer HTML WebViewer Datei mit automatisiertem Versand per System Task inklusive einer E-Mail-Weiterleitung

# Desaster Szenarien

Folgend sollen verschieden Desaster Szenarien inklusive möglicher Recovery Möglichkeiten beleuchtet werden.

## Szenario 1

**Problem:**
Datenbank korrupt

**Lösung:**
Datenbank wird aus einem Backup wiederhergestellt.

## Szenario 2

**Problem:**
Datenbank-Server defekt

**Lösung:**
Datenbank Server wird auf neue Hardware installiert. Ändert sich dadurch der Servername muss die Lizenz neu aktiviert werden. Wurde die Lizenz bereits mehrfach aktiviert, kann es sein, dass diese durch die MATESO wieder freigegeben werden muss. Ändert sich der SQL Instanz Name muss am Anwendungsserver die Verbindung zum Datenbankserver neu konfiguriert werden, dies gelingt über die Grundkonfiguration.
Eventuell vorhandene Offline Datenbanken funktionieren weiterhin.

## Szenario 3

**Problem:**
Applikationsserver defekt

**Lösung:**
Neu Installation auf neue Hardware. Die Lizenz muss neu aktiviert werden. Ändert sich der Servername kann es sein, dass die Lizenz durch die MATESO wieder freigegeben werden muss. Die Grundkonfiguration muss durchgeführt werden um die Anbindung an den Datenbankserver wiederherzustellen. Ändert sich der Servername, müssen die Datenbankprofile an den Clients angepasst werden.
Eventuell vorhandene Offline Datenbanken müssen neu erstellt werden!

## Szenario 4

**Problem:**
Beide Server defekt, Passwörter aus dem Password Safe werden aber dringend benötigt.

**Lösung:**
Datenbank Server und Anwendungsserver wird auf neue Hardware installiert. Es muss die Lizenz neu aktiviert werden. Restore der Datenbank aus Backup. Die Grundkonfiguration muss durchgeführt werden um die Anbindung an den Datenbankserver wiederherzustellen. Wurde die Lizenz bereits mehrfach aktiviert, kann es sein, dass diese durch die MATESO wieder freigegeben werden muss.
Eventuell vorhandene Offline Datenbanken müssen neu erstellt werden!

## Szenario 5

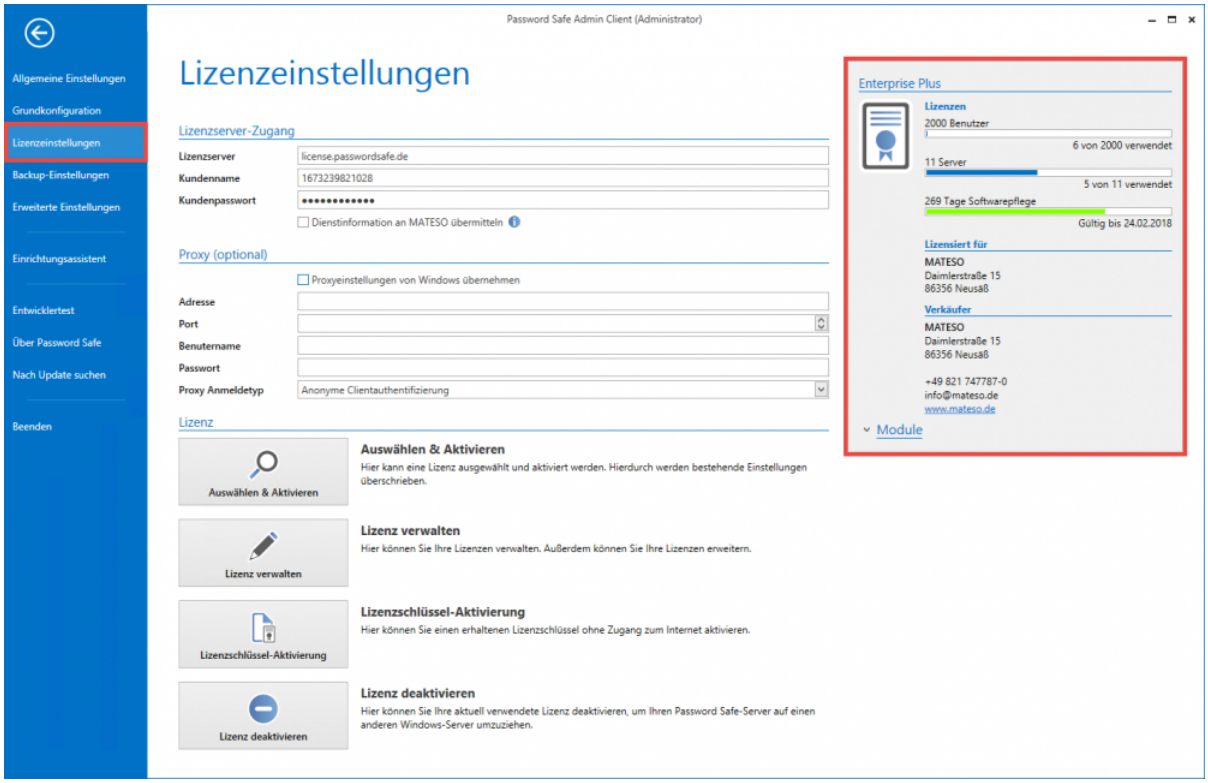
**Problem:**
Wie Szenario 4, aber zusätzlich ist auch Active Directory nicht verfügbar.

**Lösung:**
Wie unter Szenario 4. Sind die User im Ende zu Ende Modus importiert worden, können Sie sich auch ohne AD Anbindung anmelden. User welche im Masterkey Modus importiert wurden, können sich nicht anmelden. Daher ist es empfehlenswert spezielle, lokale Notfall User für solche Fälle zu erstellen.

# Lizenzeinstellungen

## Was sind Lizenzeinstellungen?

Innerhalb der Lizenzeinstellungen werden die Lizenzen für den Password Safe verwaltet. Darüber hinaus sind im hierfür vorgesehenen Fenster alle aktuellen Lizenzdetails dargestellt.




## Lizenzen

> ! Version 7 Lizenzen können für die Nutzung des Password Safe Version 8 nicht genutzt werden. Bitte kontaktieren Sie uns zwecks der Ausstellung einer Version 8 Lizenz.

Angebunden werden die Lizenzinformationen über den MATESO Lizenzserver. Nachfolgend die Details:

- license.passwordsafe.de
- IP: 185.48.116.55
- Port 443 TCP (Standard HTTPS-Port)

Es ist dafür Sorge zu tragen, dass dieser Server erreichbar ist. Proxy Server können optional verwendet werden. Die Lizenz wird vom Server abgerufen und in der Server Konfiguration hinterlegt. Die Lizenz

wird fortan stündlich geprüft und ggf. aktualisiert. Die Vorhaltezeit beträgt 30 Tage. Sollte also keine Internetverbindung vorhanden sein, kann man demnach noch 30 Tage weiter arbeiten. Falls diese Vorhaltezeit Probleme verursachen sollte, bitten wir Sie um individuelle Kontaktaufnahme.

## Einbinden und Verwalten von Lizenzen

Nach dem Kauf werden die nötigen Lizenzinformationen in Form von “Kundenname” und “Passwort” zur Verfügung gestellt. Diese Informationen werden direkt im Bereich **Lizenzserver-Zugang** konfiguriert. Durch den Button **Auswählen und Aktivieren** wird eine Verbindung zum Lizenzserver aufgebaut. Die erworbenen Lizenzen werden nun dargestellt und können selektiert werden. Die Lizenz ist nun nutzbar.

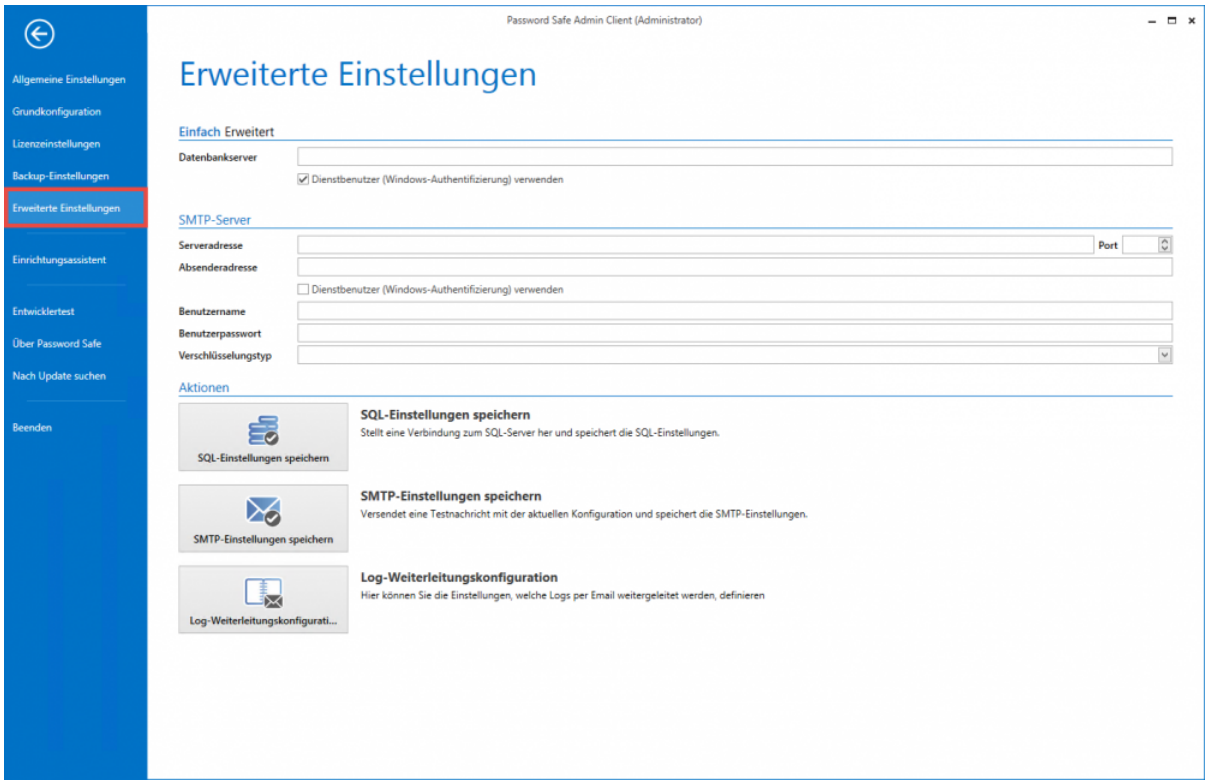
Optional kann ein Proxy angegeben werden. Standardmäßig wird der im Betriebssystem hinterlegte Proxy verwendet.

Die Lizenz wird im Kontext des Dienstbenutzers abgerufen. Bei Verbindungsproblemen sind also die Firewall und ggf. der Proxy dahingehend zu prüfen.

# Erweiterte Einstellungen

## Was sind erweiterte Einstellungen?

Innerhalb der erweiterten Einstellungen werden globale Standardwerte definiert.




## Datenbankserver

Der hier hinterlegte Datenbankserver wird beim Neuerstellen von Datenbanken als Standardwert verwendet. Hierbei existieren 2 Modi:

### Einfacher Modus

Im einfachen Modus kann der Pfad zum Datenbankserver inklusive dem Benutzer und dem zugehörigen Passwort angegeben werden. Alternativ kann ebenso der Dienstbenutzer verwendet werden.

### Erweiterter Modus

Im erweiterten Modus kann der Connection String angegeben werden, welcher sowohl den Server, den User als auch das Passwort enthält

# SMTP-Server

Durch Konfiguration des SMTP-Servers definiert man sämtliche Einstellungen für Emails, welche der Server, z.B. über das Benachrichtigungssystem, verschicken soll. Beim abschließenden Speichern wird die Verbindung direkt auf Funktionalität getestet. Die Schaltfläche “SMTP Einstellungen speichern” wird erst nach einer getätigten Änderung aktiv.

# Offline Client

## Was ist der Offline Client?

Der Offline Client ermöglich das Arbeiten ohne aktive Verbindung zum Password Safe Server. Hat man es an entsprechender Stelle konfiguriert, synchronisiert sich die lokale Replik der Serverdatenbank in frei definierbaren Zyklen selbstständig und sorgt somit dafür, dass man stets einen (relativ) aktuellen Stand der Datenbank mobil nutzen kann.

### Fakten

- Bei der Erstellung von Offline-Datenbanken kommt “Microsoft SqlServer Compact 4.0.8876.1” zum Einsatz
- Verschlüsselung der Datenbank mittels AES 128 bzw. SHA 256. Hierbei wird auf den sogenannte “Platform Default” gesetzt
- Zusätzliche werden RSA Verschlüsselungsverfahren genutzt
- Mehr zu diesem Thema…

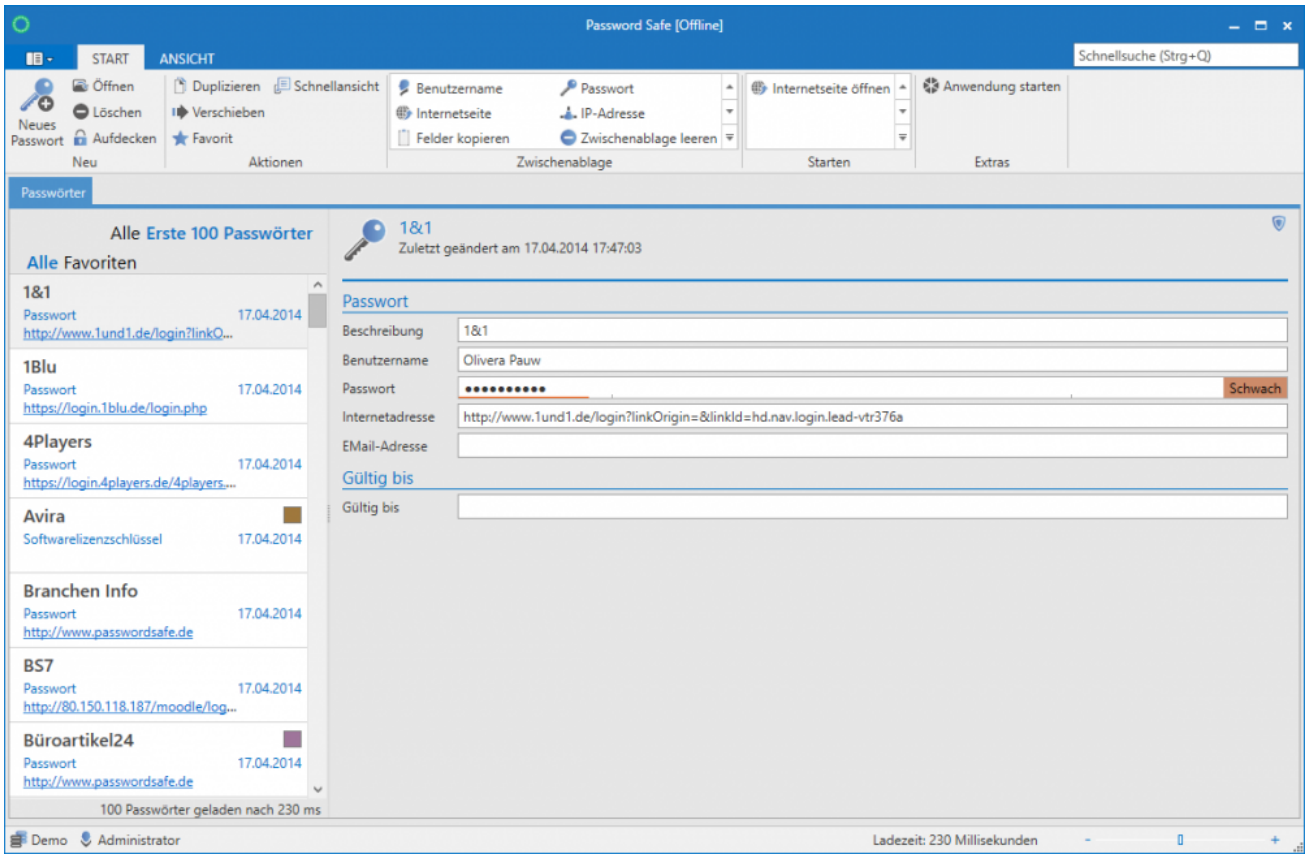
## Installation

Der Offline Client wird zusammen mit dem Haupt Client automatisch installiert. Es müssen keine Datenbankprofile erstellt werden – diese Aufgabe übernimmt der Client beim ersten Synchronisieren zusammen mit dem Erstellen der Offline Datenbank.

## Bedienung

Die Bedienung des Offline Clients ist grundsätzlich an die Handhabung des Hauptclients angelehnt. Da der Offline Client dennoch nur eingeschränkten Funktionsumfang besitzt, gilt bezüglich der Bedienung folgendes zu beachten:

- Es existiert kein Dashboard
- Es ist ausschließlich das Passwort Modul verfügbar
- Der Filter ist nicht verfügbar. Das Auffinden der Datensätze erfolgt über die Schnellsuche
- Die automatische Eintragung ist über den SSO Agent unabhängig vom Offline Client möglich




# Nicht synchronisierbare Daten

Siegel erweitern das Sicherheitskonzept des Password Safe um ein granular definierbares Mehr-Augen-Prinzip. Dies bedeutet, dass Freigaben auf geschützte Informationen an eine positive Rückmeldung aus der Authentifizierung durch einen oder mehrere Benutzer gekoppelt sind. Diese Freigaben sind natürlich nicht einholbar, wenn keine Server-Verbindung besteht. Aus diesem Grund werden versiegelte Datensätze nicht synchronisiert und sind demnach auch nicht Bestandteil von Offline Datenbanken.

> Dennoch gilt: Datensätze mit Sichtschutz werden in die Offline Datenbank übernommen und können wie gewohnt verwendet werden

# Einrichten und Synchronisieren

## Einrichten der Offline Datenbank

Für die Einrichtung des Offline Client gilt es im Vorfeld die richtigen Voraussetzungen zu schaffen. Sowohl am Admin Client selbst als auch in den Benutzerrechten/Benutzereinstellungen sind die nachfolgend aufgeführten Konfigurationen durchzuführen.

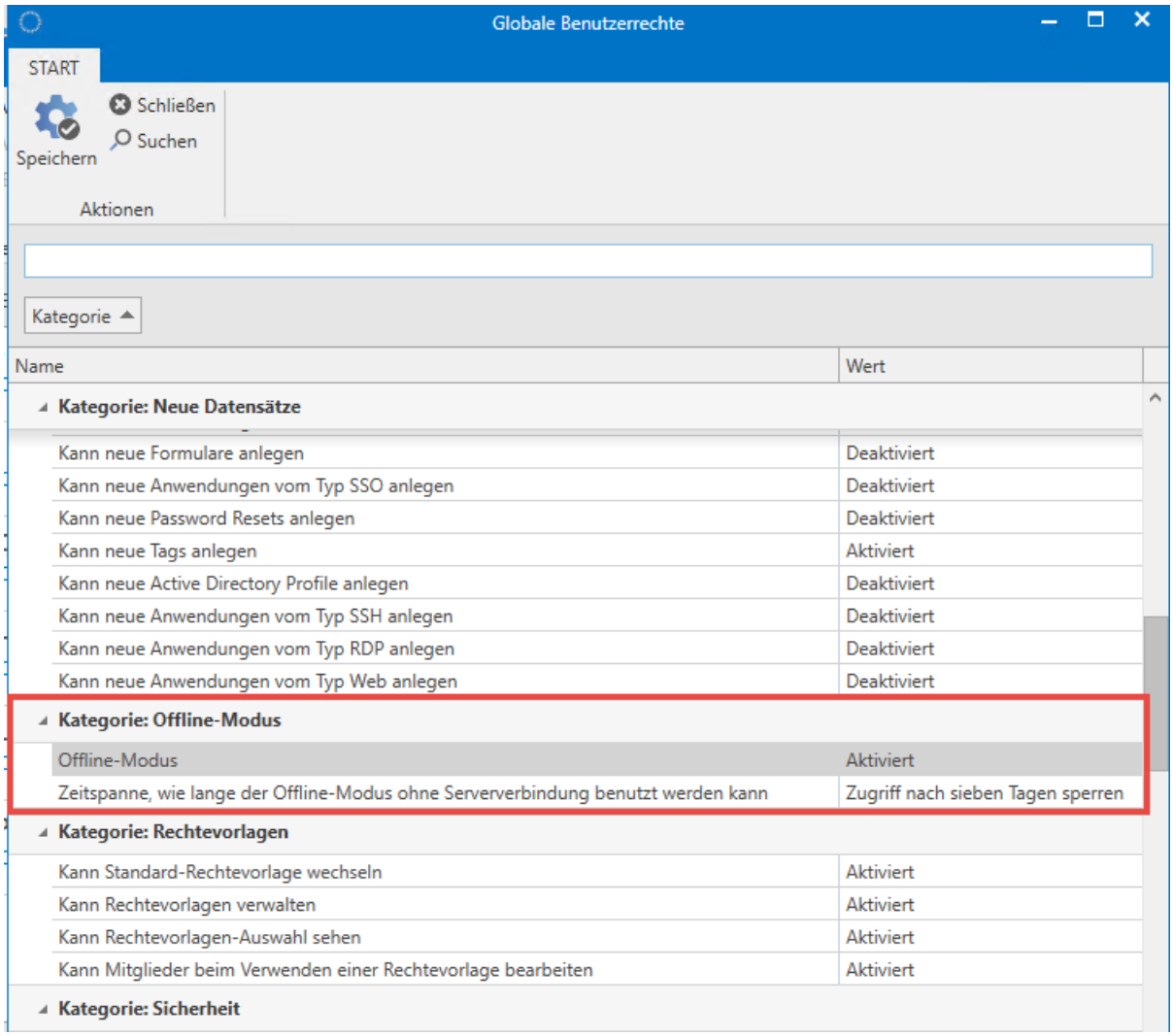
### Voraussetzungen

Um Offline Datenbanken einrichten zu können, muss dies erst grundsätzlich am Admin Client aktiviert werden. Dies wird in der Datenbankübersicht am Admin Client für jede Datenbank separat in den “Allgemeinen Einstellungen” (Rechtsklick auf die Datenbank) durchgeführt. Ebenso ist dies bereits beim initialen Erstellen der Datenbank möglich.


Weitere Infos zu diesem Thema finden Sie in den Kapiteln: Erstellen von Datenbanken und Verwaltung von Datenbanken

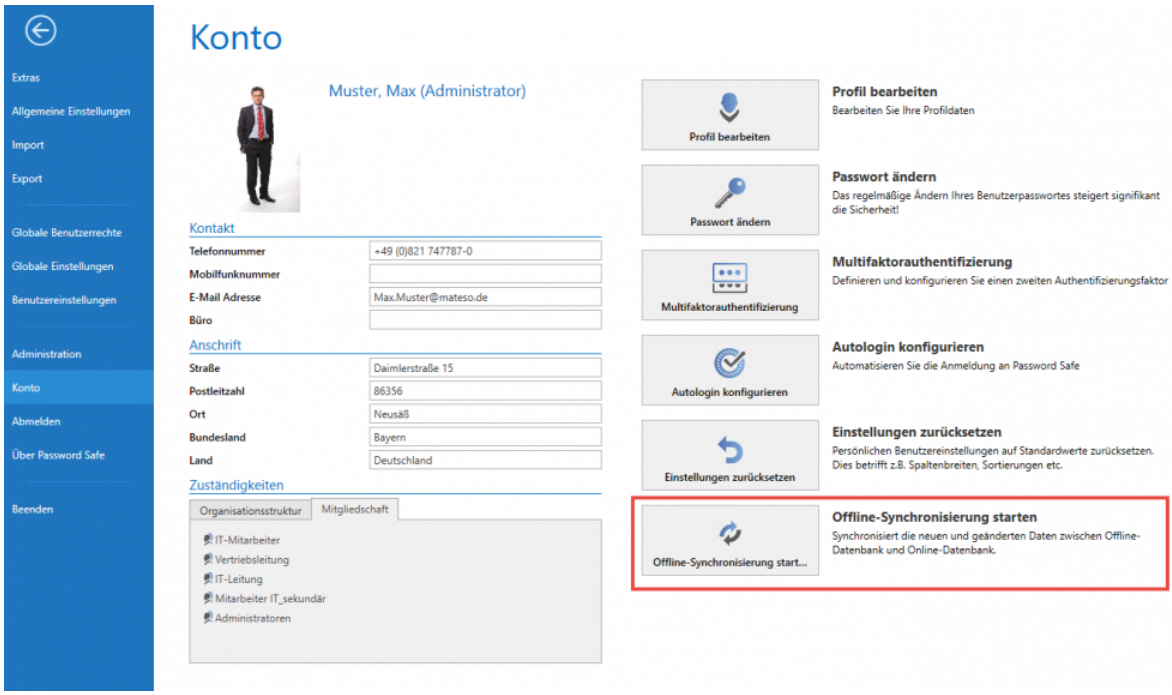
### Benutzerrechte

Der Benutzer benötigt das Recht “Offline-Modus”. Darüber kann in den Benutzerrechten die Zeitspanne definiert werden, wie lange der Offline-Modus ohne Serververbindung genutzt werden kann.




## Einrichten einer Offline Datenbank

Grundlegend kann die Synchronisation mit der Offline Datenbank automatisch erfolgen. Dennoch muss **das erste Mal manuell** angestoßen werden. Hierzu wird unter Hauptmenü/Konto die Synchronisation initiiert.




> Gespeichert werden die Offline Datenbanken lokal unter folgendem Pfad: %appdata%\MATESO\Password Safe and Repository Client\OfflineDB

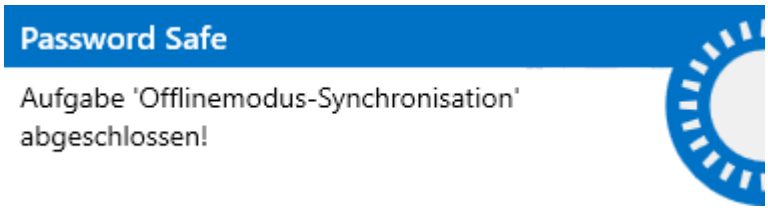
Es pro Benutzer und Client für jede Online Datenbank eine Offline Datenbank erstellt werden. Somit ist es möglich, mit einem Offline Client mehrere Offline Datenbanken zu verwenden.

# Synchronisation

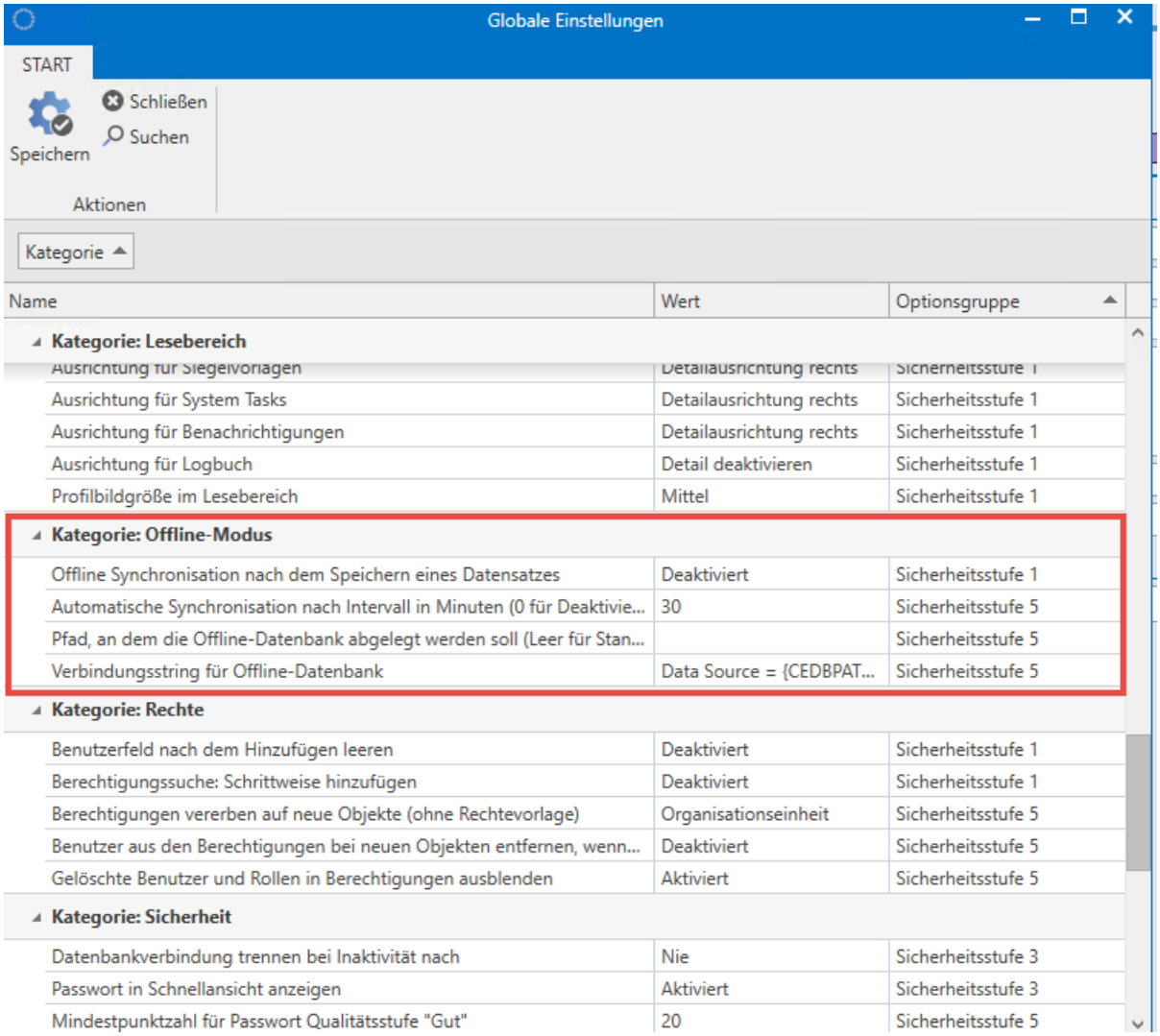
Um die Daten immer konsistent zu halten, muss die Offline Datenbank regelmäßig synchronisiert werden. Die Synchronisation wird durch den Client automatisch im Hintergrund ausgeführt. Das Intervall hierfür kann in den Einstellungen frei konfiguriert werden. Standardmäßig wird alle 30 min synchronisiert. Beim Anlegen und Bearbeiten von Datensätzen kann auch azyklisch synchronisiert werden, damit die Änderungen direkt offline verfügbar sind. Darüber hinaus kann im Backstage über “Konto” kann die Synchronisation auch manuell gestartet werden.

Eine laufende Synchronisation wird sowohl im Icon in der Taskleiste als auch im Client durch einen Statusbalken angezeigt:

Sobald die Synchronisation abgeschlossen ist, wird dies durch einen Hint dargestellt.




# Relevante Einstellungen




Anhand der genannten vier Einstellungen kann der Offline Modus konfiguriert und personalisiert werden:

- **Offline Synchronisation nach dem Speichern eines Datensatzes**: Die Synchronisation der Offline Datenbank erfolgt direkt nach dem Speichern eines Datensatzes. Es gilt zu beachten, dass dies nur diejenigen Datensätze betrifft, welche vom angemeldeten Benutzer gespeichert werden. Änderungen anderer Benutzer lösen keine Synchronisation aus!
- **Automatische Synchronisation nach Intervall**: Es wird das Intervall definiert, welches zyklisch zu einer Synchronisation der Offline Datenbank führt. Der Standard beträgt 30 Minuten.

- **Pfad, an dem die Offline Datenbank abgelegt werden soll**: Lässt man dieses Feld leer, wird der Systemstandard genutzt. Anderweitig kann auch direkt der Ablageort der Offline Datenbank angegeben werden.
- *Verbindungsstring für Offline Datenbank:

# Hochverfügbarkeit

## Was ist Hochverfügbarkeit?

Durch Hochverfügbarkeit soll der weitere Betrieb des Password Safe im Schadensfall gewährleistet werden. Damit dieses Feature genutzt werden kann, muss **im Vorfeld** eine Reihe von Voraussetzungen erfüllt werden.

> ! Da die Konfiguration der Hochverfügbarkeit komplexer Natur ist, wird deren Umsetzung (in der Regel) im Rahmen von Consultingstunden umgesetzt. Bei Interesse kontaktieren Sie uns bitte direkt, bzw. den für Sie zuständigen Partner.

## Voraussetzungen

Folgende Punkte sollten bei der Konfiguration beachtet werden.

- Für die Replikation der Datenbank muss zwingend MSSQL Enterprise Version genutzt werden (auch bei der Replikation zwischen mehreren Standorten)
- Für eine bessere Absicherung empfehlen wir, die Password Safe Datenbank auf einem eigenen Cluster zu betreiben
- Pro Standort muss ein Password Safe Applikationsserver lizenziert werden. Jeder Applikationsserver besitzt seine eigene Konfigurationsdatenbank.

### Load Balancer

- Um die Auslastung des Servers zu reduzieren, kann vor die Applikationsserver ein Load Balancer geschaltet werden
- Wird kein Load Balancer verwendet, erfolgt die Verteilung des Datenbankprofils bei den Benutzern generell über die Registry

Wurde die Datenbank in “Standort A” inkl. AD-Profil erstellt, so müssen diese Zertifikate dort exportiert und auf dem Server Standort B importiert werden. Die Datenbank wird mittels MSSQL Technologie repliziert und kann als bestehende Datenbank im Password Safe am Standort B eingebunden werden. Fällt der Applikationsserver in Standort A aus, muss der Server in der Registry ausgetauscht (Standort B) und an die Benutzer mittels Gruppenrichtlinien (GPO) neu ausgerollt werden.

# Versionshistorie

Die bisher veröffentlichten Versionen und die zugehörigen Changelogs sind unter den folgenden Kapiteln zu finden.


- Version 8.2.0.12343
- Version 8.1.1.11211 Hotfix 1
- Version 8.1.1.11106
- Version 8.1.0.10812
- Version 8.0.2.9978 Hotfix 2
- Version 8.0.2.9541 Hotfix 1
- Version 8.0.2.9278
- Version 8.0.1.9032

# Version 8.3.0.13358

### Veröffentlichung

29.11.2017

### Kompatibilität

Zum AdminClient der Version 8.3.0.13358 sind folgende Client Versionen kompatibel:

Version 8.2.0.12343
Version 8.2.0.12388 Hotfix 1

Der WebAccess wird mit Version 8.3.0.13358 durch den neuen WebClient ersetzt.

### Neu

- Der WebClient ist nun verfügbar und kann über den AdminClient eingerichtet werden.
- Es kann nun bei System Tasks ausgewählt werden, auf welchen Server diese ausgeführt werden sollen.
- Wenn "Sitzung aufzeichnen" aktiviert ist, erscheint nun beim Verbinden zu einer RDP- oder SSH-Anwendung eine Meldung zum Zustimmen. Beim Bestätigen der Meldung wird ein Logbucheintrag erstellt.
- Bei Änderungen an den Berechtigungen einer Organisationseinheit, kann nun konfiguriert werden, dass die geänderten Berechtigungen auch auf Passwörter angewandt werden. Hierzu wurde eine neue Einstellung hinzugefügt.
- Neue Einstellung am Client hinzugefügt, um die Gültigkeit von Sitzungen einzustellen.
- Password Reset kann nun für Linux eingerichtet werden.
- Benachrichtigungen können nun für bestimmte Benutzer oder Rollen konfiguriert werden.
- Rollen können endgültig gelöscht werden und wiederhergestellt werden.

### Verbesserung

- Es wird nun bei Active Directory Profilen die letzte Synchronisation angezeigt.
- Das Verhalten beim Anlegen und Verwenden von Tags wurde verbessert.
- Automatisch hinzugefügte Filterelemente (z.B. bei Schnellsuche) können nun immer entfernt werden.
- Die Suche in den Google Chrome- und Mozilla Firefox-Addons verbessert, wenn nach einem exakten Datensatznamen gesucht wird.
- Die Updateprüfung beachtet nun die Proxy-Einstellungen des Servers.
- In der Backup Historie am AdminClient kann nun nach Datum gefiltert werden.
- Mehrere Anpassungen an dem System der Fortschrittsleiste durchgeführt.
- Es wurde eine eigene Bildschirmtastatur im Client implementiert.

- Es kann nun am AdminClient bei Backup-Logs nach einem Datum gefiltert werden.
- Die Bildschirmtastatur kann nun am SSO Agent über "Strg+Shift+K" geöffnet werden.
- Die Validierung von dem Feldtyp "Hostname" wurde angepasst.
- Der Sichtschutz wird nun in der Vorschau von Passwörtern angezeigt.
- Das Verhalten bei der Offline-Synchronisation von neuen Datensätzen, wenn ein Fehler auftritt, wurde überarbeitet.
- Die Synchronisierung von Active Directory-Objekten im Master Key-Modus wurde verbessert.
- Die Performance beim Anzeigen von Mitgliedschaften in der Vorschau wurde verbessert.
- Es wird nun im Kopfbereich angezeigt, ob eine Benachrichtigung für andere Benutzer konfiguriert ist.
- Über das Tastaturkürzel "F12" können nun Passwörter auf- und zugedeckt werden.
- Verhalten beim Nutzen einer leeren Schnellsuche angepasst.
- Checkbox in den Einstellungen bei Dokumenterweiterungen hinzugefügt, um Dokumente ohne Erweiterung zu erlauben.
- Erlaubte Dokumenterweiterungen sind nicht mehr Case Sensitive.

### Änderung

- Crash Reports werden nun in AppData abgelegt.
- Für die Einrichtung einer Multifaktor Authentifizierung wird nun beim eigenen Benutzer auf das Recht "Schreiben" und bei anderen Benutzern auf Recht "Berechtigen" geprüft.
- Server Zertifikate werden nun mit SHA-512 verschlüsselt.
- Es ist nun möglich das "Besitzer Recht" vom eigenen Benutzer zu entfernen, wenn kein Berechtigen-Recht vorhanden ist.

### Behoben

- Fehler behoben, bei welchem man sich am SSO Agent nicht an mehreren Datenbanken anmelden konnte.
- Fehler beim Wechsel zur aktiven Instanz behoben.
- Das Benutzerrecht "Kann Mitglieder beim Verwenden einer Rechtevorlage bearbeiten" wird nun im Organisationseinheiten Assistenten beachtet.
- Falsche Ansicht beim Reduzieren der Berechtigungen bei "Jeder" behoben.
- Gelöschte Felder können nun über die Historie wiederhergestellt werden.
- Ein Fehler bei dem HTML WebViewer-Export bei den Spalten Benutzername, Passwort und URL wurde behoben.
- Fehler behoben, bei welchem gelöschte Mitglieder von Rollen bei der Active Directory Synchronisation hinzugefügt wurden.
- Historischer Vergleich funktioniert nun auch, wenn es nur einen historischen Eintrag gibt.
- Die Eingabe von Datumswerten wurde korrigiert.
- Fehlende Dateien am AdminClient hinzugefügt, sodass Backups bei getrennten Password Safe- und SQL-Server wieder erstellt und wiederhergestellt werden können.

- Benutzer können sich nun am OfflineClient mit einer Kombination aus Domäne und Benutzername anmelden.
- Fehler bei versiegelten Passwörtern behoben, wenn Benutzer über Rollen berechtigt waren.
- Timing Problem bei der automatischen Eintragung behoben, wodurch falsche Daten eingetragen werden konnten.
- Fehler behoben, bei welchem Benutzer über Rollen kein versiegeltes Passwort aufdecken konnten.
- Während des Speichervorgangs von Berechtigungen können nun die Rechte nicht mehr bearbeitet werden.
- Fehler beim Anbringen eines Sichtschutzes behoben, bei welchem der Rechte-Schlüssel entfernt werden konnte.
- Die Client-Sitzung wird nun ordentlich getrennt, wenn das Betriebssystem heruntergefahren wird.
- Fehler beim Setzen von "Mitglied" in den Berechtigungen bei Benutzern behoben.
- Beim Öffnen einer URL über die Passwortliste wird nun der konfigurierte Browser in den Einstellungen des Passworts berücksichtigt.
- Absturz behoben, wenn der Server abgeschalten ist und beim SSO Agent ein automatischer Login konfiguriert ist.
- Fehler bei der Passwortprüfung behoben, wenn bei Richtlinien die Einstellung "Anzahl Kategorien, aus denen Zeichen enthalten sein müssen" auf "Alle" eingestellt wurde.
- Beim Keepass-Import werden nun auch Rechte-Vorlagen auf importierte Organisationseinheiten angewandt.
- Datumsformat der Passwortliste korrigiert, wenn der Client in englisch verwendet wurde.
- Speicherleak im Server behoben.
- Fehlermeldung beim Anlegen neuer Benutzer wird nun korrekt angezeigt, wenn das Passwort nicht mit der Standardrichtlinie übereinstimmt.
- Optionen für Passwörter vom aktuellen Benutzer geladen, wenn sie im Passwort nicht direkt konfiguriert wurden.
- Einstellungen für die Tastaturkürzel werden korrekt beachtet.
- AdminClient zeigt alle lizensierten Einstellungen an, wenn der AdminClient zum ersten Mal geöffnet wird.
- Fehler behoben beim Verwenden einer Standard-Rechtevorlage, bei welchem die Vorlage nicht korrekt ausgewählt wurde.

# Version 8.2.0.12388 Hotfix 1

### Veröffentlichung

17.08.2018

### Kompatibilität

Zum AdminClient der Version 8.2.0.12388 sind folgende Client und WebAccess Versionen kompatibel:

- Version 8.2.0.12343

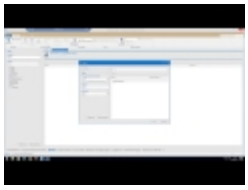
### Behoben

- Ein Fehler beim Verwenden von “Mitglied” in den Berechtigungen von Rollen wurde behoben.
- Das fehlende Benutzerrecht “Kann Drucken” wurde hinzugefügt.

# Version 8.2.0.12343

### Veröffentlichung

09.08.2017



### Kompatible Client und WebAccess Versionen

In dieser Version ist leider keine Abwärtskompatibilität gegeben. Ein gleichzeitiges Update von AdminClient, aller Clients und des WebAccess ist also zwingend nötig.

### Neu

- Wechsel zwischen Filter und Struktur möglich.
- Anwendungen können nun exportiert werden.
- Neue Einstellung hinzugefügt um gelöschte Benutzer oder Rollen in den Berechtigungen auszublenden.
- Bei der Migration werden nun Ordner, welche als Tags ausgewählt werden, als Tagvorlagen migriert.
- Es kann nun nach Mitgliedern einer Rolle im Hinzufügen-Dialog bei Berechtigungen gefiltert werden.
- Änderungen am Formular können nun auf Bestandsdaten über eine Einstellung angewandt werden.
- Neue Benutzerrechte zum Siegel anlegen, Sichtschutz anlegen und Verwalten von Formularfeldern bei Passwörtern hinzugefügt.
- Bei der Migration kann nun definiert werden, dass Ordnernamen in die Beschreibung der Datensätze aufgenommen werden.
- Es können nun Installationsparameter für das Client-Setup übergeben werden. Hiermit kann die Internet Explorer Extension und der automatische Start des SSO Agent deaktiviert werden.
- Es wurden Funktionsmenüs hinzugefügt, über welche bestimmte Aktionen zu Formularfeldern durchgeführt werden können.
- Neuen Feldtyp “Hostname” hinzugefügt. Ist in einer Anwendung keine IP-Adresse oder Hostnamen hinterlegt, wird nun der Feldtyp “Hostname” aus dem Passwort verwendet zum Verbindungsaufbau verwendet.
- Es ist nun möglich SSO Agent sowie OfflineClient im Setup zu deaktivieren.

- Die automatische Offline-Synchronisation kann nun über eine Einstellung deaktiviert werden. Es wurde außerdem eine weitere Einstellung hinzugefügt, mit welcher ein Sychronisationsintervall definiert werden kann.
- Es kann nun durch eine neue Einstellung konfiguriert werden, welche Dokumentenerweiterungen (Dateiendungen) zugelassen werden.
- Wird der Verbindung zum Server nicht getraut, kann nun beim Anmelden das SSL-Zertifikat des Servers geöffnet und importiert werden.
- Es ist nun durch eine neue Filtergruppe möglich nach Objekten zu filtern, welche Tags enthalten oder keine besitzen.
- Es wird nun eine Statusleiste am Client angzeigt, wenn dieser auf einer älteren Version betrieben wird als der Server.
- Es ist nun möglich die Dienste über den AdminClient neu zu starten.
- Passwörter, Dokumente und Rollen können nun ausgedruckt werden. Hierbei wird auf das Recht “Drucken” geprüft.
- Der Fenstertitel der Anwendung kann nun mit verschiedenen Parametern (z.B. Version, Edition) konfiguriert werden.
- Es wurde eine neue Filtergruppe für Rechtevorlagen hinzugefügt.
- Neue Benutzerrechte hinzugefügt, um Benutzer oder Organisationseinheiten endgültig zu löschen.
- Aus der Berechtigungsansicht kann nun ein Rechtefilter erzeugt werden.
- Neue Filtergruppe für Datensätze mit Sichtschutz hinzugefügt.
- Bei einem Passwort können nun Einstellungen wie Autofill, Autosubmit oder der Standardbrowser konfiguriert werden.
- Beim Verschieben von Datensätzen gibt es nun die Möglichkeit, die vordefinierten Rechte oder die Rechtevererbung anzuwenden.
- Bei der Migration können nun Dokumentordner aus Version 7 als Organisationseinheit angelegt werden.

### Verbesserung

- Erhebliche Performancesteigerung bei Tabs (Öffnen, Laden, Schließen)
- Die Galerie für die Zwischenablage kann nun in den Einstellungen konfiguriert werden.
- Mehrere Verbesserungen an der Oberfläche der Clients durchgeführt.
- Verbesserungen bei der Synchronisation zum Offline-Modus durchgeführt.
- Das “Exportieren”-Recht wird nun korrekt bei allen Arten von Exports beachtet.
- Tagvorlagen werden nun auch beim KeePass und CSV-Import beachtet.
- Die Sortierung im Modul Organisationsstruktur wurde überarbeitet.
- Benutzerkennwörter können nun in der Listenansicht auch per Mehrfachauswahl über die Ribbon oder Rechtsklick zurückgesetzt werden.
- Große Berichte werden nun schneller geschlossen.
- Beim Importieren von Benutzern durch einen Active Directory Import wird nun das Recht zum Benutzer anlegen geprüft.
- In Active Directory-Profilen können nun alternative Domänennamen festgelegt werden.
- Hinzufügen und Entfernen einer Multi-Faktor-Authentifizierung werden nun Protokolliert (Logbuch).

- Das Besitzer Recht kann nun nicht mehr auf “Jeder” angebracht werden.
- Die Setup-Shortcuts bleiben nun bei einem Update bestehen und werden nur bei Deinstallation entfernt.
- Beim Export von Passwörtern werden nun lediglich die Passwortfelder nicht exportiert, wenn das Passwort versiegelt ist oder einen Sichtschutz hat.
- Aus dem Active Directory im Master Key-Modus importierte Objekte können nun verschoben und Benutzer restriktiv gesetzt werden.
- Mitglied kann nun über die Mehrfachauswahl gesetzt werden.
- Active Directory-Profile, welche noch mit gelöschten Active Directory-Objekten verknüpft sind, können nun nicht mehr gelöscht werden.
- Verbesserung der Client Performance durchgeführt.
- Es werden nun auch Suchordner bei der Migration angezeigt. Diese sind standardmäßig deaktiviert.
- Bei der Migration werden nun Felder mit den Namen “Host”, “Hostname”, “Computer” und “Computername” als Feldtyp “Hostname” migriert.
- Die Fehlerausgabe der Migration in bestimmten Fällen wurde verbessert.
- Versiegelte Datensätze werden nun auch beim Web Viewer exportiert, wenn der Benutzer das Passwort einsehen kann.
- Bei einem Migrationsfehler kann nun der Pfad, in welchem das entsprechende Log abgelegt wird, direkt geöffnet werden.
- Die Fortschrittsleiste beim Speichern von Berechtigungen wurde verbessert.
- Dokumentordner werden bei der Migration nun hierarchisch als Tag angelegt.
- Alle Clients zeigen nun beim Starten einen Splashscreen an.
- Es werden nun Benachrichtigungen für erteilte Siegelfreigaben erstellt.
- Bei RDP-Anwendungen kann nun ein Gatewayserver konfiguriert werden.
- Benachrichtigungen können nun auch über Mehrfachauswahl konfiguriert werden.
- Beim CSV- und KeePass-Import können nun bestehende Tags angehängt werden.
- Die Eintragung über Tastenkombinationen in der Passwortliste wurde verbessert.
- Beim Speichern von Berechtigungen erscheint nun ein Hinweis, wenn Berechtigungen vererbt oder überschrieben werden.
- Einige Schutzmechanismen eingefügt, so dass der Serverschlüssel nicht mehr entfernt werden kann.
- MARS (Multiple Active Result Sets) lässt sich nun am AdminClient pro Datenbank konfigurieren.

### Änderung

- Es wird nun die Berechtigung “Schreiben” benötigt, um Benachrichtigungen auf andere Benutzer zu konfigurieren.
- Ist die Einstellung “Letzten Filter automatisch anwenden” deaktiviert, so wird nun die Listenansicht ohne Ergebnisse des Moduls geladen.
- Wird beim CSV- oder KeePass-Import in der Zuordnung ein Feld als Organisationseinheit angelegt, dann wird nun eine neue Organisationseinheit angelegt und die Passwörter werden dieser zugewiesen.

- Es wird nun beim Importieren von Active Directory-Benutzern im Ende-zu-Ende Modus das initiale Benutzerpasswort per E-Mail versendet, insofern beim Benutzer eine E-Mail-Adresse hinterlegt und ein SMTP-Server konfiguriert ist.
- Durch die Grundkonfiguration erstelle Zertifikate sind nun bis zum 31.12.9999 gültig.
- Die Optionen der Browser Addons “Autofill” und “Autosubmit” werden nun in den Einstellungen des Clients konfiguriert.
- Der letzte Zustand von “Vererben” und “Überschreiben” wird nun nicht mehr gespeichert. Bei Passwörtern und Formularen ist “Vererben” nun per Standard aktiviert und kann nur durch das entsprechende Benutzerrecht deaktiviert werden. Bei Organisationseinheiten werden nun immer beide Funktionen angezeigt.
- Berechtigungen von lokalen oder Active Directory Organisationseinheiten werden nun nur auf Organisationseinheiten des selben Typs vererbt. Es wird nun geprüft, ob es sich um lokale Organisationseinheiten sowie um das selbe Active Directory Profil handelt.

### Behoben

- Ein Fehler beim erneuten Importieren von Active Directory Objekten wurde behoben.
- Fehler behoben, wenn bei einem versiegelten Passwort die Eintragung per Skript verwendet wurde.
- Es wird nun ein korrekter Text in der Sitzungsliste bei einer Anmeldung über die API angezeigt.
- Verschachtelte Gruppen-Mitgliedschaften werden bei der Migration nun korrekt aufgelöst.
- Falsches Verhalten beim Verwenden der Einstellung “Tab nach Verwerfen schließen” behoben.
- Ein Absturz beim Scrollen durch die Passwortliste wurde behoben.
- Fehler bei der Skalierung und dem Vollbild-Modus bei RDP-Anwendungen wurden behoben.
- Ein Fehler in der Historie von migrierten Datensätzen wurde behoben.
- Ein Fehler bei der Migration von Passwörtern mit einem “&”-Zeichen in einer Feldbeschriftung wurde behoben.
- Ein Fehler beim Verschieben von Passwörtern auf den angemeldeten Benutzer wurde behoben.
- Ein Fehler, bei welchem Datenbanken mit einem Minus im Namen nicht eingebunden werden konnten, wurde behoben.
- Ein Fehler beim Web Viewer Export wurde behoben, bei welchem nach bestimmten Zeichen (z.B. “<”) der restliche Inhalt des Feldes nicht exportiert wurde.
- Ein Fehler beim Starten des Firefox Addons wurde behoben, wenn der Agent nach dem Browser gestartet wurde.
- Ein Fehler bei URLs mit mehr als 12.000 Zeichen behoben.
- Bei veränderten Windows DPI Einstellungen werden die Oberflächen des Internet Explorer Addons nicht mehr falsch dargestellt.
- Beim Passwort-Export werden nun alle Feldtypen wie z.B. Datum und Liste korrekt exportiert.

# Version 8.1.1.11211 Hotfix 1

### Veröffentlichung

19.05.2017

### Behoben

- Die Vererbung von Rechtevorlagen (Rechte vordefinieren) wird nun nicht mehr auf Benutzer angewandt.

# Version 8.1.1.11106

### Veröffentlichung

08.05.2017

### Neu

- Neues Benutzerrecht zum Verwalten von Sitzungsaufzeichnungen hinzugefügt.
- Es ist nun möglich das Umschalten der Ansichten beim Anpassen der Breite zu deaktivieren.
- Es wird nun visuell dargestellt, wenn die Gültigkeit von Objekten bald erreicht wird oder überschritten ist.
- Offline-Datenbanken können nun gelöscht werden.
- Konfigurierte Rechtevorlagen werden nun im Modul Organisationsstruktur visuell dargestellt.
- Neues Benutzerrecht zum Verwalten von Active Directory Profilen hinzugefügt.
- Rechtevorlagen (Rechte vordefinieren) werden nun auf untergeordnete Organisationseinheiten vererbt.

### Verbesserung

- Rollen können nun nach der Active Directory Domäne und Gültigkeitsdatum sortiert und gruppiert werden.
- Benutzerkennwörter können nun in der Listenansicht zurückgesetzt werden.
- Internetseiten ohne “https://” können nun über die Galerie geöffnet werden.
- Es können nun mehrere Rechtevorlagen gleichzeitig gelöscht werden.
- RDP- und SSH-Fenster sind nun nicht zwingend im Vordergrund und werden in der Taskleiste angezeigt.
- Das “Hinzufügen”-Recht ist nun auch im Organisationseinheiten-Assistent konfigurierbar.
- Beim Anlegen von SSO Anwendungen können nun Verzögerungen angelernt werden.
- Beim Anbringen und Löschen von Siegeln in der Passwort bearbeiten Ansicht wird nun die Anzeige direkt aktualisiert.
- Funktionen in der Ribbon bei Benutzern werden nur noch angezeigt, wenn die nötigen Berechtigungen auf den Benutzer vorhanden sind.
- Der AdminClient wird nun neu gestartet, wenn die Dienstadresse in der Grundkonfiguration geändert wird.
- Die Zeichenbegrenzung bei URL-Feldern wurde erweitert.
- Anpassung der Fehlermeldung, wenn die Client-Version veraltet ist.
- Anpassung des Verhaltens beim Scrollen in der Passwortliste durchgeführt.
- Alle Siegelaktionen werden nun protokolliert und im Logbuch angezeigt.
- Die Logbuch-Filterung ist nun auch ohne angegebenen Benutzer möglich. Ist kein User definiert werden die Logbucheinträge von allen Benutzern geladen.

### Behoben

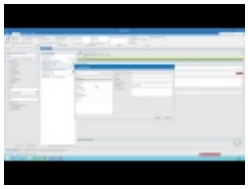
- Absturz beim Entfernen von “Jeder” in den Berechtigungen behoben.
- Ein sporadischer Absturz beim Verwenden der Schnellsuche wurde behoben.
- Fehler behoben, bei welchem beim Anlegen von neuen Benutzern, der anlegende Benutzer nicht korrekt berechtigt wurde.
- Beim Active Directory Import und der Synchronisation wird nun das Hinzufügen auf den zuständigen Benutzer im Profil übertragen.
- Die SMTP-Konfiguration kann nun auch gespeichert werden, wenn Benutzername und Passwort leer sind.
- Ein Fehler bei Dokumenten wurde behoben, wenn Rechtevorlagen oder Vererbung verwendet wurde.
- Fehler beim Nutzen von SLDAP behoben, bei welchem die Anmeldung von Master Key Benutzern nicht möglich war.
- Es wurden Abstürze behoben, wenn die Serververbindung getrennt wurde.
- Proxy wird nun korrekt aus der Datenbank geladen und in der Oberfläche am AdminClient angezeigt.

# Version 8.1.0.10812

### Veröffentlichung

04.04.2017

> **!** WICHTIG: Damit Passwörter in Organisationseinheiten abgelegt werden können, ist es nach dem Update zwingend erforderlich, allen Rollen sowie berechtigten Benutzern das neue “Hinzufügen” Recht zu bei den jeweiligen Organisationseinheiten zu erteilen. Nur dann ist es möglich, neue Passwörter zu erfassen.



### Neu

- Es können nun Standardwerte in Formularen festgelegt werden.
- Eine neue Einstellung zum Konfigurieren der Anzahl der anzuzeigenden Objekten in den Modullisten wurde eingefügt.
- Es wird nun ein Datenbank-Icon bei der Profilauswahl angezeigt, Registry-Datenbanken sind nun anhand des Icons erkennbar.
- Session Recording ist nun verfügbar.
- Neues Recht bei Organisationseinheiten hinzugefügt, über welches bestimmt wird, welche Benutzer Passwörter unter dieser Organisationseinheit anlegen können.
- Es kann nun eine Datenbank-Firewall am AdminClient konfiguriert werden.
- Ein neues Benutzerrecht zum Unterbinden von privaten Passwörtern wurde hinzugefügt.
- Mitgliedschaften werden nun bei Benutzern und Rollen angezeigt.
- Es ist nun durch eine neue Filtergruppe möglich, nach deaktivierten bzw. abgelaufenen Objekten zu Filtern.
- Es ist nun möglich am AdminClient Lizenzen zu deaktivieren.
- Änderungen an Berechtigungen werden nun im Logbuch protokolliert.
- Dokumente können nun exportiert werden.
- Es kann nun beim Verbindungsaufbau von RDP- oder SSH-Anwendungen eine Server- oder IP-Adresse hinterlegt werden, wenn in der Anwendung keine Daten vorhanden sind.
- Neues Benutzerrecht zum Anlegen von Tags hinzugefügt.
- Bei MouseOver über den Datenbanknamen werden nun Verbindungsinformationen zu der Datenbank angezeigt.
- Über das Backstage kann nun in den Offline- oder Onlinemodus gewechselt werden.

- Neue Einstellung zum Vererben von Berechtigungen wurde hinzugefügt.
- Neue Einstellung zum Verwenden des Offline-Modus hinzugefügt.
- Passwörter können nun als CSV-Datei exportiert werden.

### Verbesserung

- Es wird nun eine eindeutige Fehlermeldung angezeigt, wenn ein Vollbackup nicht gefunden werden konnte.
- Es kann nun ausgewählt werden, dass für bestimmte SSO-Anwendungen bei der Eintragung nicht nachgefragt werden soll, welche Daten verwendet werden sollen.
- Der SSO Agent muss nun nicht mehr neu gestartet werden, wenn der Port geändert wird.
- Performanceverbesserung bei der Navigation in der Formularauswahl.
- Um das Verwenden von falschen Daten zu verhindern, werden beim Start der Migration nun die zwischengespeicherten Daten geleert.
- Anwendungsverknüpfungen in der Passwortliste sind nun alphabetisch sortiert.
- Neu hinzugefügte Mitglieder einer Rolle werden nun bei der Active Directory-Synchronisation beachtet.
- Beim Duplizieren von Daten wird nun eine Fortschrittsanzeige angezeigt.
- Der SSO Agent wird nun automatisch aktualisiert, wenn ein Passwort mit einer Anwendung verknüpft wird.
- Die Beschreibung einer Active Directory-Gruppe wird nun auch synchronisiert.
- Die Migration von Dokumenten ist nun möglich.
- Active Directory-Objekte, die explizit von dem Import in Password Safe ausgeschlossen sind, werden nun bei der Migration beachtet.
- Korrekturen an der Sitzungszählung wurden durchgeführt.
- Diverse Anpassungen bei der Zählung und Prüfung von Sitzungen wurden durchgeführt.
- Der V7-Administrator wird nun bei der Migration auf alle Anwendungen und Rollen vollberechtigt.
- Die Ladezeit und Anzahl der initial geladenen Objekte werden nun in allen Ansichten angezeigt.
- Nicht vollständig angezeigte Texte können nun an weiteren Stellen per Mouseover angezeigt werden.
- Bei der Active Directory-Zusammenfassungsseite werden nun die auszuschließenden Elemente berücksichtigt.
- Der SSO Agent zeigt nun eine Benachrichtigung an, wenn der Port bereits belegt ist.
- Am SSO Agent wurde die Erkennung der Login Buttons erweitert.
- Werden Texte in der Dokumentenliste nicht vollständig angezeigt, können diese per Mouseover nun angezeigt werden.
- Die Reihenfolge der Spalten in der Ribbon wurde in allen Modulen angepasst.
- Im Active Directory-Assistenten kann nun konfiguriert werden, ob nach dem Import synchronisiert werden soll.
- Anpassungen am Intervall-Layout am AdminClient wurden durchgeführt.
- Die Initialen aus dem Active Directory werden nun übernommen.
- Im Bearbeiten-Modus wird nun der Fokus auf das erste Textfeld gesetzt.
- Es wird nun auch der Typ Computer im Active Directory Assistenten angezeigt.

- Bei ungültigen Active Directory-Objekttypen wird nun eine aussagekräftige Fehlermeldung angezeigt.
- Eine falsche Warnung beim initialisieren des Active Directory-Assistenten, wurde entfernt.
- Beim Erstellen eines neuen Profils am WebAccess wird nun das erste Feld fokussiert.
- Bei Formularfeldern kann nun ein Standardwert vorgegeben werden.
- Beim Hinzufügen von mehreren Tags, wird nun eine Fortschrittsanzeige eingeblendet.
- Bei der Konfiguration eines SMTP-Servers wurden Anpassungen vorgenommen.
- Anpassung am Layout von Siegel und Siegelvorlagen durchgeführt.
- Die Rechte des Datenbank-Administrators wurden aktualisiert.
- Gibt es keine Rechtevorlage, werden nun die Berechtigungen der zugeordneten Organisationsstruktur vererbt, wenn die Einstellung dementsprechend aktiviert ist.
- Ein Button zum Öffnen der Hilfe wurde beim Login am AdminClient hinzugefügt.
- Neu hinzugefügte Formular- und Passwortfelder erhalten nun die Berechtigungen des dazugehörigen Formulars bzw. Passwortes.
- Im Benutzer- und Organisationseinheitenassistent wird nun die Einstellung bezüglich der Rechtevererbung beachtet.
- Standard-Richtlinien können nun entfernt werden.
- Anpassungen am Vorgang durchgeführt, wenn einem Benutzer das Passwort zurückgesetzt wird.
- Das Fenster des SSO Agents ist nun in der Größe anpassbar.
- Optimierungen zum schnelleren Anwendungsstart implementiert.
- Allgemeine Verbesserungen an der Performance durchgeführt.
- Die Prüfung auf eine Richtlinie bei Passwörtern kann nun optional eingestellt werden.
- Benachrichtigungen werden nun als gelesen markiert, wenn diese über eine Siegel- oder Rechteanfrage-Benachrichtigung geöffnet werden.
- Es können nun Rechtevorlagen entfernt werden.
- Das Benutzerbild wird nun auch im Ende zu Ende Modus bei vorhandenen Benutzern synchronisiert.
- Neue Funktion und Einstellung hinzugefügt, über welche ein Benutzer aus den Berechtigungen entfernt wird, wenn er ein Objekt anlegt.
- In allen Schnellansichten wird nun ein Fenstertitel angezeigt.
- Der Seitenaufbau wurde am WebAccess verbessert.
- Man erhält nun eine Rückmeldung am WebAccess, wenn kein Recht auf das Passwortmodul vorhanden ist.
- Beim Passwort verdeckt ändern, wird nun das erste Feld standardmäßig fokussiert.
- Active Directory LDAP-Filter für Import und Synchronisation angepasst, sodass ohne ‘Domain-Objekt’ als Wurzelelement gefiltert werden kann.
- Anpassungen bei der Vorschau vom LDAP-Filter im Active Directory-Profil vorgenommen.
- Anpassung der Fehlermeldung am Client, wenn die Yubico Schnittstelle nicht korrekt konfiguriert ist.
- Bestehen keine Rechte auf den Offline-Modus, Import oder Export, werden die entsprechenden Funktionen nun ausgegraut dargestellt.
- Wird ein Siegel gebrochen, erhalten nun alle Freigabeberechtigten eine Benachrichtigung.

- Es kann nun bei der Anmeldung an der Datenbank eine Bildschirmtastatur verwendet werden.
- In der Benutzervorschau und Schnellansicht werden nun die Mitgliedschaften angezeigt.
- Am WebAccess wird nun eine korrekte Meldung angezeigt, wenn versucht wird, ein am Client gelöschtes Passwort zu bearbeiten.
- Anpassungen für den Proxyserver, bei den Lizenzeinstellungen am AdminClient vorgenommen.
- Performance-Optimierung des Browser Addons für Google Chrome und Mozilla Firefox durchgeführt.
- Anpassungen durchgeführt, wenn ein Passwort keine Beschreibung enthält.
- Anpassungen für die automatische Anmeldung bei Google durchgeführt.
- In den Berechtigungen eines Benutzers kann nun “Mitglied” vergeben werden.
- Textliche Anpassungen am SSO Agent sowie an den Browser Addons durchgeführt.
- Siegelbenachrichtigungen und Rechteanfragen sind nun unter Benachrichtigungen ersichtlich.
- In der Listenansicht bei Passwörtern wurde die Uhrzeit entfernt.
- Anpassungen bei der Anzeige der Fortschrittsanzeige wurden durchgeführt.
- Anpassung am WebAccess bei der Darstellung von langen Benutzernamen durchgeführt.
- Das Verhalten am AdminClient bei der Auswahl einer Datenbank, welche serverseitig nicht mehr existiert wurde angepasst.
- Anpassung beim Datum festlegen bei temporären Berechtigungen durchgeführt.
- Die Formularauswahl wird nun nicht mehr angezeigt, wenn man nur Zugriff auf ein Formular hat.
- Anpassung bei der Darstellung der Dauer einer Migration durchgeführt.
- Die Datei mit den Informationen zu der abgeschlossenen Migration wird nun in der korrekten Sprache angelegt und der Pfad, unter welchem diese Datei abgelegt wurde, kann direkt geöffnet werden.
- Es wird nun ein Hinweis auf den SQL Browser-Dienst bei einer externen Instanz in der Grundkonfiguration angezeigt.
- Es kann nun die Domäne im Spalteneditor bei Rollen aus dem Active Directory angezeigt werden.
- “Strg + C” bei Passwörtern öffnet nun einen Dialog zum Kopieren der Felder.
- Das Verhalten für die Funktion “Sichtbar für Jeden” wurde beim Rechte vordefinieren überarbeitet.
- Leichte Performanceverbesserung beim An- und Abmelden durchgeführt.
- Es kann nun am OfflineClient eine Richtlinie bei Passwortfeldern ausgewählt werden.
- Verbesserungen beim Erkennen der aktuellen Sitzung am AdminClient durchgeführt.
- Rechtevorlagen beim Rechte vordefinieren können nun umbenannt werden.
- Anpassung des Textes, wenn die Lizenz oder Softwarepflege abläuft.
- Treten beim Löschen von Objekten Fehler auf, wird nun eine aussagekräftige Fehlermeldung angezeigt.
- Bei einem Klick auf die hinterlegte E-Mai-Adresse bei Benutzern, öffnet sich nun das Standard E-Mail-Programm.
- Es kann nun der zuständige Benutzer bei einem Active Directory-Profil im Master Key-Modus gewechselt werden.
- Benutzereinstellungen die eine höhere Sicherheitsstufe benötigen werden nun ausgeblendet.
- Mehrere Anpassungen am Active Directory Import und bei der Synchronisation durchgeführt.

### Behoben

- Ein Fehler beim Verwenden von Umlauten im Benutzernamen oder Passwort beim Anmelden am Web Access wurde behoben.
- Ein Fehler beim Import von mehrfach verschachtelten Active Directory-Strukturen wurde behoben.
- Es wurde ein Fehler am SSO Agent behoben, bei welchem bei mehreren verbundenen Datenbanken lediglich die Daten der ersten Datenbank entschlüsselt werden konnten.
- Fehler behoben, bei welchem zu viele Active Directory-Elemente synchronisiert wurden.
- Ein Fehler bei der Migration von Active Directory-Rollen wurde behoben, wenn die Migration nicht im MasterKey-Modus durchgeführt wurde.
- Ein Absturz der Migration wurde behoben, wenn Active Directory-Profile aufgrund einer zu geringen Edition nicht migriert werden konnten.
- Der Client funktioniert nun wieder in einer Citrix Umgebung.
- Das Passwortfeld wird nun nicht mehr geleert, wenn es verdeckt bearbeitet wird.
- Die Vererbung von verschachtelten Active Directory-Gruppenkonstrukten wird nun beim Active Directory-Import korrekt angewandt.
- Benutzer unterhalb von Active Directory-Gruppen werden nun bei der Synchronisation korrekt beachtet.
- Ein Absturz beim Öffnen des Backstages durch ein Tastenkürzel wurde behoben.
- Änderungen im Offline Modus werden nun wieder korrekt synchronisiert.
- Im Active Directory gelöschte Objekte werden nun auch bei der Synchronisation entfernt.
- Der Feldname von Feldern mit dem Typ “Überschrift” kann nun wieder bearbeitet werden.
- Es wurde ein Fehler beim Verteilen von Datenbankprofilen über die Registry behoben.
- Passwortrichtlinien, die mit gelöschten Passwortfeldern verbunden waren, können nun wieder gelöscht werden.
- Ein Fehler bei der Migration, wenn diese über eine Stunde andauerte, wurde behoben.
- Daten eines Intervalls werden nun bei Änderungen an der Konfiguration nicht verworfen.
- Das Wiederherstellen eines historischen Passworts funktioniert nun wieder.
- Dokumente können nun migriert werden.
- Anwendung minimiert starten verhält sich wieder korrekt.
- Favorit wird nicht mehr in der Ribbon angezeigt, wenn es keine Suchergebnisse gibt.
- Der Wechsel zur aktiven Instanz funktioniert nun auch, wenn der Client minimiert ist.
- Fehler behoben, bei welchem die erste Sitzung eines SSO Agents beim Beenden nicht korrekt entfernt wurde.
- Mehrere Fehlerbehebungen bei externen Links wurden durchgeführt.
- Ein Fehler wurde behoben, bei welchem nach zu schnellem An- und Abmelden der Server abgestürzt ist.
- Ein Fehler beim Verwenden von Password Safe unter Citrix wurde behoben.
- Das Recht zum Verschieben wird in der Bearbeiten-Ansicht nun nur geprüft, wenn die Organisationseinheit verändert wurde.
- Die Instanz-Nachfrage erscheint nun nicht mehr beim Öffnen des ersten Clients auf Terminalservern.
- Label werden bei der Migration wieder korrekt mit Passwörtern verknüpft.

- Für die Multifaktorauthentifizierung werden nun keine Werte generiert, die nicht der Plausibilitätsprüfung entsprechen.
- Das Wiederherstellen eines differentiellen Backups ist nun auch möglich, wenn das dazugehörige Vollbackup nicht in derselben Datei enthalten ist.
- Am AdminClient wird nun bei neuen Backupprofilen die aktuelle Uhrzeit verwendet.
- Datenbankprofile aus der Registry werden nicht mehr in der Konfigurationsdatei gespeichert und ein Fehler beim Verteilen der Profile per Registry wurde behoben.
- Ein Absturz beim Öffnen eines Benutzers, wenn während des Ladens permanent Maustasten gedrückt wurden, wurde behoben.
- Fehler bei der Darstellung von System Tasks nach dem Aktualisieren wurde behoben.
- Ein Fehler wurde behoben, bei welchem Passwörter nicht aufgedeckt werden konnten, wenn die Benutzer migrierte MasterKey-Benutzer sind.
- Ein Formularwechsel mit Feldern, welche eine Begründung benötigen, ist nun möglich.
- Ein Fehler, bei der Verwendung der Passwortrichtlinie am AdminClient, wurden behoben.
- Ein Absturz am AdminClient bei der Migration wurde behoben, wenn auf eine Datei zugegriffen wird, welche von einem anderen Prozess verwendet wird.
- Ein Problem, wenn zwei Active Directory-Synchronisationen gleichzeitig auf einer Datenbank durchgeführt werden, wurde behoben.
- Ein Absturz beim Öffnen des Datenbank Assistenten, wenn keine Verbindung zum Server besteht, wurde behoben.
- Ein Fehlverhalten, wenn die Benutzerdaten eines Clients ungültig werden, wurde behoben.
- Die Information, ob ein Objekt synchronisiert werden soll, wird nun auch nach einer Active Directory-Synchronisation beibehalten.
- Enthält eine Sitzung falsche Benutzerdaten, wird der Benutzer nun abgemeldet.
- Durch zu schnelles wiederholtes Passwort öffnen am WebAccess wird nun kein Fehler ausgelöst.
- Beim Verteilen eines WebAccess-Profils, ist die Sitzung nun nicht mehr automatisch abgelaufen.
- Ein Fehler, bei welchem die Active Directory-Zusammenfassung keinen zugeordneten Namen angezeigt hat, wurde behoben.
- Beim Löschen von mehreren Password Resets tritt nun kein falsches Ladeverhalten auf.
- Ein Fehler am WebAccess, beim Verwenden einer Rechtevorlage mit Benutzern auf die kein Lese-Recht besteht, wurde behoben.
- Anpassung am WebAccess durchgeführt, wenn versucht wird ein Passwort zu speichern, ohne die nötigen Rechte zu besitzen.
- Fehler beim Wechseln des Profils im Active Directory-Assistenten behoben.
- Die Passwortstärke ist nun in Listenansicht ersichtlich.
- Unter Status am AdminClient wird nun die Version sowie der Status der Server-Dienste korrekt angezeigt.
- Ein Fehler wurde behoben, bei welchem ein Fenster bei Tastatureingabe geschlossen wurde.
- Fehler behoben, bei welchem Standardrichtlinien nicht korrekt beachtet wurden.
- Ein Absturz am Client wurde behoben, wenn durch den AdminClient die Sitzung getrennt wird.
- Im Active Directory gelöschte Objekte werden nun bei Synchronisation entfernt.
- Deaktivierte Richtlinienprüfung wird nun auch bei der Migration beachtet.

- Ein Fehlverhalten wurde behoben, bei welchem durch Öffnen der Hilfe eine Warnung am AdminClient geschlossen wurde.
- Ein Fehler bei der Synchronisierung im Ende zu Ende-Modus wurde behoben.
- Ein Fehler, bei welchem keine Verbindung zum SSO Agent auf Terminalservern hergestellt werden konnte, wurde behoben.
- Ein Fehler beim Setzen von Berechtigungen auf Formularfelder bei der Migration wurde behoben.
- Überschreiten Objektinformationen aus dem Active Directory die maximale Zeichenlänge, werden diese beim Import bzw. bei der Synchronisation entsprechend abgeschnitten.
- Gruppen werden in der Migration korrekt erkannt, wenn der zuletzt angelegte Benutzer in Version 7 als gelöscht markiert wurde.
- Ein Fehler, bei der Migration von gesperrten Passwörter, wurde behoben.
- Das Wiederherstellen in der Historie von Passwörtern mit Begründung ist nun möglich.
- Ein Fehler beim Beenden von RDP-Anwendungen wurde behoben.
- Ein Fehlverhalten bei mehrmaligem Speichern, welches das Aufdecken von Passwörtern verhinderte, wurde korrigiert.
- Fehler am SSO Agent behoben, wenn dieser mit einer Offline-Datenbank verbunden war, konnten Passwörter mit Sichtschutz kopiert werden.
- Fehler am SSO Agent behoben, bei welchem die automatische Eintragung bei einer Verbindung zur Offline-Datenbank nicht funktionierte.
- Fehler behoben, bei welchem im Dashboard eine endlose Ladeanzeige dargestellt wurde.
- Fehler beim Setzen des Fokus nach nutzen der Schnellsuche behoben.
- Fehler behoben, bei welchem nach dem Speichern eines Passworts, dieses nicht angezeigt werden konnte.
- Ein Fehler, bei welchem Dokumente nicht über externe Links geöffnet werden konnten, wurde behoben.
- Fehler behoben, bei welchem Rechtevorlagen beim Erstellen von neuen Benutzern oder Organisationseinheiten nicht korrekt angezeigt wurden.
- Anwendungen ohne Namen aus Version 7 werden nun korrekt migriert.
- Die Einstellung für das Trennen der Datenbankverbindung nach einer gewissen Zeit funktioniert nun korrekt.
- Es treten nun keine Fehler auf, wenn das Passwort zum Authentifizieren am AdminClient geändert wird.
- Ist für ein Formularfeld das Verwenden von generierten Passwörtern festgelegt, wird die Funktion zum Passwort ändern nun ausgeblendet.
- Beim Verwenden einer Rechtevorlage können nun die selbst hinzugefügten Berechtigungen entfernt werden.
- Die Zeitdifferenz zum Server wird nun beim initialisieren des Google Authenticators am WebAccess korrekt angezeigt.
- Im OfflineClient wird nun “Sichtbar für jeden” korrekt beachtet.
- Fehler behoben, bei welchem in einer bestimmten Konstellation in der Siegelübersicht keine Benutzer oder Rollen angezeigt wurden.
- Wird ein Passwort verdeckt geändert, wird es nun im Tab als Änderung erkannt.

- Ein Fehler bei der Migration mit zusammengeführten Benutzern wurde behoben.

# Version 8.0.2.9978 Hotfix 2

### Veröffentlichung

17.02.2017

### Verbesserung

- Die Standard Richtlinien können nun entfernt werden.
- Am Admin Client wurde ein Button zum Öffnen der Hilfe hinzugefügt.

### Behoben

- Ein Bug welcher zu Abstürzen beim Öffnen des Datenbank Assistenten führte, wenn keine Verbindung zum Server besteht, wurde behoben.
- Ein Fehler, beim Setzen von Berechtigungen auf Formularfeldern bei der Migration, wurde behoben.
- Ein Fehler, bei der Verwendung der Passwortrichtlinie am Admin Client, wurde behoben.
- Es wurde ein Fehler behoben, bei welchem die Standard Richtlinien nicht korrekt beachtet wurden.
- Am WebAccess wurde ein Fehler beim Verwenden einer Rechtevorlage mit Benutzern auf die kein Lese-Recht besteht, behoben.
- Ein Fehler, bei welchem keine Verbindung zum SSO Agent auf Terminalservern hergestellt werden konnte, wurde behoben.

# Version 8.0.2.9541 Hotfix 1

### Veröffentlichung

20.01.2017

### Verbesserung

- Um das Verwenden von falschen Daten zu verhindern, werden beim Start der Migration werden nun sämtliche Caches geleert.
- Die Beschreibung einer AD-Organisationseinheit wird nun auch synchronisiert.
- Diverse Anpassungen bei der Zählung und Prüfung von Sitzungen wurden durchgeführt.
- Der V7-Administrator wird nun bei der Migration auf alle Anwendungen und Rollen vollberechtigt.
- Bei der AD-Zusammenfassungsseite werden nun die auszuschließenden Elemente berücksichtigt.

### Behoben

- Ein Fehler beim Import von mehrfach verschachtelten AD-Strukturen wurde behoben.
- Fehler behoben, bei welchem zu viele AD-Elemente synchronisiert wurden.
- Ein Absturz der Migration wurde behoben, wenn AD-Profile aufgrund einer zu geringen Edition nicht migriert werden konnten.
- Die Vererbung von verschachtelten AD-Gruppen-Konstrukten wird nun beim AD-Import korrekt angewandt.
- Benutzer unterhalb von AD-Gruppen werden nun bei der Synchronisation korrekt beachtet.
- Ein Fehler bei der Migration von AD-Rollen im Ende-zu-Ende-Modus wurde korrigiert.
- Im Active Directory gelöschte Objekte werden nun auch bei der Synchronisation entfernt.
- Neu hinzugefügte Mitglieder einer Rolle werden nun bei der AD-Synchronisation beachtet.
- AD-Objekte, die explizit von dem Import in Password Safe ausgeschlossen sind, werden nun bei der Migration beachtet.
- Ein Fehler bei der Migration, wenn diese über eine Stunde andauerte, wurde behoben.
- Fehler behoben, bei welchem die erste Sitzung eines ClientAgents beim Beenden nicht korrekt entfernt wurde.
- Ein Fehler wurde behoben, bei welchem nach zu schnellem An- und Abmelden der Server abgestürzt ist.
- Ein Fehler beim Verwenden von Password Safe unter Citrix wurde behoben.
- Die Instanz-Nachfrage erscheint nun nicht mehr beim Öffnen des ersten Clients auf Terminalservern.
- Fehler bei der Migration mit langen Werten behoben.
- Datenbankprofile aus der Registry werden nicht mehr in der Konfigurationsdatei gespeichert und ein Fehler beim Verteilen der Profile per Registry wurde behoben.
- Dokumente können nun migriert werden.

# Version 8.0.2.9278

### Veröffentlichung

22.12.2016

### Neu

- In der Mehrfachbearbeitung von Rechten können nun Rechtevorlagen ausgewählt werden.
- Anwendungen können nun über eine Funktion in der Ribbon gestartet werden, ohne diese mit einem Datensatz zu verknüpfen.
- Das Layout der Multifaktorauthentifizierung im Login wurde überarbeitet.
- Bei einem Passwortfeld ohne Berechtigungen können nun Rechte angefragt werden. Dies löst eine Benachrichtigung für berechtigte Benutzer aus.
- Es existieren nun neue Benutzerrechte für die Sichtbarkeit einzelner Reiter innerhalb der Fußzeile.
- Yubico OneTimePassword kann nun als Authentifikator verwendet werden.
- Wird beim Öffnen der Grundkonfiguration kein Zertifikat gefunden, wird dieses nun automatisch erzeugt.

### Verbesserung

- Die Intervall-Beschreibung wird nun auch außerhalb der Intervall-Konfiguration angezeigt.
- Fehlerhaftes Verhalten von Verbindungssperren in der Übersicht wurde korrigiert.
- Der Zeilenumbruch der URL wird am Web Access nun lediglich unter bestimmten Bedingungen durchgeführt.
- Es ist nun möglich, dynamische Startparameter in SSO Anwendungen zu konfigurieren.
- Im Anwendungspfad einer SSO Anwendung können nun Umgebungsvariablen verwendet werden.
- Anpassungen am Layout von Intervallen wurden durchgeführt.
- Die Konfiguration eines globalen Syslog-Servers ist nun möglich.
- Formularfelder können nun auch beim KeePass-Import als Tag angelegt werden.
- Die Visualisierung des Loginbereiches im Web Access wurde angepasst.
- Es kann nun ein Standard für Passwortrichtlinien am AdminClient konfiguriert werden.
- Am AdminClient wurde eine Passwortrichtlinie implementiert, welche bei der Vergabe von Passwörtern innerhalb des AdminClients genutzt wird.
- Speichern per STRG + S sowie das Schließen per ESC funktioniert nun an allen Clients.
- Passwortfelder, welche nur mit Begründung geöffnet werden dürfen, können nun auch im WebAccess aufgedeckt werden.
- Im Rechtefilter ist es nun möglich, nach Berechtigten mit Mitgliedschaft zu filtern.
- Die Option “Sichtbar für jeden” wird nun beim Active Directory Import im Master Key Modus angewendet.
- Die Berechtigungen von Organisationseinheiten, welche durch ein Active Directory Profil im Master Key Modus importiert wurden, können nun bearbeitet werden.

- In den Browser Addons wird nun zur Erkennung von passenden Passwörtern die URL des Tabs verwendet.
- Favoriten können nun mit Mehrfachselektion gesetzt werden.
- Bei Active Directory Benutzern, die durch ein Ende-zu-Ende Profil importiert werden, wird nun das Standard Rechte-Preset der zugeordneten Organisationseinheit angewendet.
- Aufdecken von Passwortfeldern mit Begründung ist im Offline Modus nicht möglich.

### Behoben

- Die Sortierung nach Datum wurde korrigiert.
- Fehler beim Hinzufügen einer Richtlinie in einer bestimmten Konstellation wurden behoben.
- Ein Fehler wurde behoben, wodurch Formulare nicht dupliziert werden konnten.
- Es wurde ein Fehler behoben, durch den es am Offline Client nicht möglich war, Benutzernamen und Passwort im Login einzugeben.
- Änderungen an Rechten werden nun im Logbuch angezeigt.
- Es wurde ein Fehler beim Active Directory Import behoben, durch welchen Objekte falsch reaktiviert wurden.
- Es wurde im Web Access ein Fehler behoben, welcher nach einer falschen Eingabe die Anzeige des Headers unterbunden hat.
- Es wurde ein Fehler behoben, durch den ein neues Passwort nicht gespeichert werden konnte, wenn über die Ribbon ein neues Memo- oder URL Feld hinzugefügt wurde.
- Diverse Fehler im Zusammenhang mit dem Active Directory Import wurden behoben.
- Fehler bei der Eingabe einer Begründung zum Aufdecken eines Passworts wurden behoben.
- Das Fenster des Internet Explorer Addons öffnet nun nicht mehr außerhalb des sichtbaren Bereichs.
- Es wurden Fehler bei der Eintragung behoben, wenn der SSO Agent mit mehreren Datenbanken verbunden war.
- Datensätze, die nach einer Offline Synchronisation versiegelt wurden, werden bei der nächsten Synchronisation aus der Offline Datenbank entfernt.
- Bei den Berechtigungen eines Benutzers kann die Mitgliedschaft nicht mehr verändert werden.
- Wenn man im Offline Client ein Passwort selektiert, auf das man über eine Rolle berechtigt ist, wird keine Fehlermeldung mehr angezeigt.
- Ein Fehler bei der Nutzung manueller Eintragungen im Internet Explorer wurde behoben.

# Version 8.0.1.9032

### Veröffentlichung

28.11.2016

### Neu

- Es kann nun nach Updates gesucht werden.
- Der Passwortgenerator sowie die Galerie Anpassung verhält sich im OfflineClient wieder korrekt.
- Eine neue Einstellung zum Zuweisen von Richtlinien für bestimmte Kategorien wurde “Administration” hinzugefügt.
- Beim Löschen von Objekten wird nun eine Fortschrittsanzeige eingeblendet.
- Die Anmeldung an der Datenbank kann nun automatisiert werden.
- Ist eine automatische Anmeldung eingerichtet, wird diese nun ebenfalls am ClientAgent genutzt.
- In den Widgets “Aktivitätsansicht” und “Tag Ansicht” kann nun nach der anzuzeigenden Datenanzahl gefiltert werden.
- Neue Option hinzugefügt, um die Anzahl der Elemente in einem Widget zu begrenzen.
- Im ClientAgent können nun durch eine neue Funktion die Browser Addons installiert werden.
- Bei der Feldzuordnung beim Import können nun neue Felder hinzugefügt, bearbeitet und entfernt werden.
- Die Lizenzübersicht zeigt nun die verbleibende Zeit zur nächsten Prüfung sowie den endgültigen Ablauf an.
- Es können nun über ein URL-Parameter Profile beim Web Access angelegt werden.
- Ein neues Benutzerrecht zum Überschreiben von Rechten wurde hinzugefügt.
- Syslog-Konfiguration am Admin Client ist nun möglich.
- Das Erstellen von externen Links ist nun möglich.
- Es ist nun möglich, die Berechtigungen von Formularfeldern von mehreren Passwörtern gleichzeitig zu konfigurieren.
- Datenbankprofile können nun über die Registry verteilt werden.
- Lizenzwarnungen werden nun in der Statusleiste des Clients angezeigt.

### Verbesserung

- Gleitkommazahl-Felder zeigen nun am OfflineClient die definierte Beschreibung an.
- Im Datenbank-Assistenten kann nun zwischen Deutsch und Englisch als Sprache der Datenbankvorlage gewählt werden.
- Anpassungen am Layout von Intervallen bei System Tasks wurden durchgeführt.
- Der Button zur Durchführung eines HTML WebViewer Exports ist nun ausgegraut, wenn der Benutzer kein Recht auf den Export hat.
- Passwörter können am OfflineClient nun schneller bearbeitet werden.

- Formulare ohne Berechtigung werden in der Formularauswahl am OfflineClient nicht mehr angezeigt.
- Verbundene Passwörter eines Password Resets können nun direkt nach dem Öffnen eines Password Resets entfernt werden.
- Im Browser Addon wird nun der Feldtyp “E-Mail-Adresse” zur Eintragung der Daten verwendet, wenn es im Passwort den Feldtyp “Benutzername” nicht
- Das Standardintervall bei neuen System Tasks wurde auf eine Stunde gesetzt.
- Man erhält nun eine Benachrichtigung, wenn die automatische Anmeldung fehlschlägt.
- Performanceverbesserung beim Laden von Organisationsstrukturen.
- Konfigurierbare Scripting Shortcuts erweitert um Einfügen, Bild auf, Bild ab, Pos1, Ende und Entfernen.
- Bei gesperrten Benutzern wird nun der Name oder die Client IP angezeigt.
- Die Mehrfachauswahl ist nun auch bei Passwortrichtlinien möglich.
- Breite des Migrationsfensters wurde angepasst, sodass die Texte ausgeschrieben sind.
- Performanceverbesserung beim Active Directory-Import durchgeführt.
- Die Suchleiste am OfflineClient lässt sich nun per STRG + F einblenden.
- Es wird nun die Systemsprache als Standardsprache am AdminClient verwendet.
- Es wurden zusätzliche Plausibilitäten bei Weiterleitungsregeln eingefügt.
- Bei Rechtevorlagen-Gruppen kann nun der gesetzte Standard einer Vorlage wieder entfernt werden.
- OfflineViewer wurde zu WebViewer umbenannt.
- Es wurden verschiedene Änderungen an der Synchronisation zum OfflineClient vorgenommen.
- Man erhält nun eine Benachrichtigung, wenn bereits eine Password Safe Instanz geöffnet ist und versucht wird eine weitere Instanz zu öffnen.
- Performanceverbesserung der Active Directory-Zusammenfassungsseite durchgeführt.
- Benutzereinstellungen und Benutzerrechte für Rechtevorlagen werden nun auch am Web Access beachtet.
- Bei bestimmten Konstellationen wurde in den Rechtevorlagen kein Symbol angezeigt, auch wenn eine Konfiguration existierte.
- Umstrukturierungen der Kategorien in den Einstellungen wurden durchgeführt.
- Die Ansichten im Ribbon Backstage Bereich können nun per STRG + F5 aktualisiert werden.
- Ein Fehler bei einem bestimmten Textqualifizierer beim Import wurde behoben.
- Beim Verschieben von Passwörtern wird nun der Ladebalken in der Statusleiste angezeigt.
- Bei Anpassungen an den Rechten wird nun auch eine Fortschrittsanzeige angezeigt.
- Die Datenbankinformationen am AdminClient wurden angepasst.
- Es wird nun auch korrekt gespeichert, wenn lediglich “Sichtbar für jeden” im Assistenten beim Benutzer anlegen konfiguriert wird.
- Die Mehrfachauswahl ist nun auch bei Siegelvorlagen möglich.
- Es erscheint nun eine Nachfrage, bevor Daten beim Erstellen eines neuen Passworts aus der Zwischenablage übernommen werden.
- Textliche Änderungen vorgenommen.

### Behoben

- Es wurde behoben, dass der AdminClient durch einen Fehler beendet wird, wenn kein Standarddatenbankserver hinterlegt ist.
- Verlinkte SSO-Anwendungen können nun auch am OfflineClient genutzt werden.
- Es wurde ein Fehler behoben, bei welchem es nicht möglich war, Passwörter am Web Access zu speichern.
- Fehler behoben, dass bei dem HTML WebViewer keine Login Maske angezeigt wurde.
- Es wurde im OfflineClient behoben, dass bei einem Klick in ein Tag-Feld ein Fehler aufgetreten ist.
- Fehler behoben, dass bei der Auswahl von “Überschreiben” und “Zusammenführen” beim Import die Passwörter nicht korrekt angelegt werden konnten.
- Falsches Verhalten beim Löschen von Benutzern, Organisationseinheiten und Rollen aus dem Active Directory wurde behoben.
- Versucht man sich mit falschen Daten am Lizenzserver anzumelden, erhält man nun eine entsprechende Rückmeldung.
- Passwörter können im OfflineClient wieder aufgedeckt werden.
- Siegel funktioniert nun auch auf Formularfeldebene korrekt.
- Es ist nun möglich die Galerie in der Ribbon auf den Standard zurückzusetzen.
- Es wurden weitere Fehlerbehebungen bei der automatischen Anmeldung vorgenommen.
- Es wurden Fehler bei der SSO Scripteintragung behoben.
- Es wurde behoben, dass bei bestimmten Widgets keine Daten angezeigt wurden.
- Fehler bei der automatischen Anmeldung am ClientAgent behoben.
- Es wurde ein Fehler behoben, dass bei der Eintragung mit einer bestimmten Rechtekonstellation ein Fehler bei Windows Anwendungen auftrat.
- Eine Korrektur am Intervall wurde durchgeführt.
- Mehrere Fehler bezüglich dem Active Directory-Import behoben.
- Es wurde behoben, dass bei der Profilauswahl das falsche Profil selektiert wurde.
- Grafische Anpassung bei der Feldzuordnung beim Import.
- Selektionsproblem bei den Profilen wurde auch am Web Access behoben.
- Es wurde ein Fehler bei der Selektierung beim Active Directory-Import behoben.
- Es wurde ein Fehler beim Beenden des ClientAgents auf Terminalservern behoben.
- Es wurde ein Fehler behoben, bei welchem der Client beendet wurde.
- Weitere Anpassungen an der Log-Weiterleitung wurden durchgeführt.
- Verschiedene Fehler beim Import wurden behoben.
- Es wurde ein Fehler behoben, bei welchem ein Ladebalken am AdminClient bestehen blieb.
- Textliche Anpassung beim Datenbankbericht.
- Es wurde ein Fehler bei der automatischen Anmeldung behoben, wenn versuchte sich auf einen Server mit ungesicherter Verbindung anzumelden.
- Ein Fehler beim Verwenden von Mehrzeiligen Textfeldern wurde behoben.
- Ein Fehler beim Wechsel der Selektion während des Löschens von Organisationsstrukturen wurde behoben.
- Die Scrollbars in den Lizenzeinstellungen verhalten sich nun korrekt.

- Fehler behoben, bei welchem es nicht möglich war, Objekte zu verschieben.
- Bei der Mehrfachselektierung kann nun jedes Recht einzeln verwalten werden.
- Kleinere allgemeine Anpassungen vorgenommen.
- Basiskonfiguration wurde zu Grundkonfiguration umbenannt.
- Kleinere Fehler beim Active Directory-Import behoben.
- Es wurde ein Fehler behoben, bei welchem der ClientAgent nicht angezeigt wurde.
- Es wurde ein Fehler behoben, durch welchen es möglich war, die Lizenz am AdminClient mehrfach zu aktivieren.
- Es wurde behoben, dass Startparameter bei SSO-Anwendungen nicht gespeichert werden konnten.
- Es wurde ein Fehler behoben, dass der letzte Benutzer oder die letzte Rolle mit einem Rechteschlüssel als berechtigter entfernt werden konnte.
- Das Entfernen von Tags ist nun mit Leserecht auf einen Datensatz möglich.
- Es wurde ein Fehler behoben, wodurch das Zurücksetzen der Einstellungen im Internet Explorer Addon nicht möglich war.
- Beim Überschreiben von gleichnamigen Passwörtern durch den Import wird nun auch die zugeordnete Organisationseinheit aktualisiert.
- Datenbanken können nun mit differentiellen Backup gesichert werden.
- Es ist nun möglich, mehrere Vollbackups in einer Datei abzulegen.
- Es wurde ein Fehler behoben, wodurch das Start- und Enddatum einer temporären Berechtigung nicht korrekt geladen wurde.
- Die Active Directory Kategorie in der Ribbon der Rollenliste wird nun nicht mehr angezeigt, wenn die AD Integration nicht lizenziert ist.
- Es wurde ein Fehler behoben, wodurch die globale Option zum Verwenden der Filter Negierung nicht überschrieben werden konnte.
- Das Infofeld bei Passwörtern kann nun wieder konfiguriert werden.
- Ein Fehler wurde behoben, bei welchem die Fortschrittsanzeige beim Löschen von Passwörtern stehen geblieben ist.
- Es kann nun am AdminClient konfiguriert werden, ob Informationen des Password Safe-Dienstes übermittelt werden sollen.

  * Sichtgeschützte Passwörter können am OfflineClient nicht mehr in die Zwischenablage kopiert werden.