Documentation

Password Safe V8

FullClient – WebClient – Server

Topic:
Help

PASSWORD SAFE
by MATESO™
Enterprise Password Management

Inhaltsverzeichnis

Herzlich Willkommen … 6
- Warum Password Safe? 8
- Was gibt es Neues in Version 8? 9
- Mit der richtigen Edition zum Ziel 11
  - Lizenzmodell 12
  - Feature-Matrix 14

Sicherheit 18
- Genutzte Verschlüsselungsalgorithmen 20
- Externe Penetrationstests 22
- IT-Security Made in Germany 23
- Sicherheitslücken – Ist Password Safe betroffen? 24
  - Log4J 25
  - Spring4Shell 26
  - Robot 27

Erste Schritte 28

Architektur und Systemanforderungen 33
- Systemanforderungen MSSQL 36
- Systemanforderungen Server 38
- Systemanforderungen FullClient 42
- Systemanforderungen WebClient 43

Installation 45
- Installation AdminClient 47
- Installation Client 52
  - Installation mit Parametern 58
- Installation WebClient 59
- Installation Browser-Erweiterungen 70
  - Installation Chrome 71
  - Installation Mozilla Firefox 73
  - Installation Edge 75
  - Installation Safari 76
- Umzug des Servers 77
- Updates 82

Berechtigungskonzept und Schutzmechanismen 85
- Manuelles Berechtigen 90
  - Nutzung von Rechtevorlagen 95
  - Mehrfachbearbeitung von Berechtigungen 96
- Automatisiertes Berechtigen 102
  - Vererbung aus Organisationsstrukturen 104
  - Rechte vordefinieren 108
    - Arbeiten mit vordefinierten Rechten 111

Relevante Benutzerrechte ... 114
Geltungsbereich vordefinierter Rechte ... 115
Schutzmechanismen ... 117
Sichtbarkeit ... 119
Temporäre Berechtigungen ... 121
Sichtschutz ... 122
Siegel ... 125
Siegelübersicht ... 132
Freigabemechanismus ... 134

Bedienung und Aufbau ... 137
Ribbon ... 142
Filter ... 146
Anzeigemodus ... 151
Erweiterte Filtereinstellungen ... 153
Listenansicht ... 158
Lesebereich ... 164
Tags ... 167
Suche ... 170
Drucken ... 173
Dashboard und Widgets ... 178
Tastaturkürzel ... 183

Client Module ... 186
Passwörter ... 189
Erstellen neuer Passwörter ... 193
Aufdecken von Passwörtern ... 197
Verschieben von Passwörtern ... 200
Formularfeldberechtigungen ... 202
Passworteinstellungen ... 205
Historie ... 206
Papierkorb ... 210
Dokumente ... 211
Benachrichtigungen ... 215
Organisationsstruktur ... 218
Benutzerverwaltung ... 223
Benutzer Passwörter / Anmeldung am Client ... 228
Berechtigungen auf Organisationsstrukturen ... 233
Vererbung von Berechtigungen ... 235
Active Directory Anbindung ... 237
Ende zu Ende Verschlüsselung ... 239
Masterkey-Modus ... 247
RADIUS-Authentifizierung ... 256
Azure AD Anbindung ... 258
Erster Faktor ... 262
Multifaktor-Authentifizierung ... 267

Yubico / Yubikey ... 273
OTP (One-Time-Password) ... 278
Rollen ... 283
Formulare ... 285
Formulare wechseln ... 291
Logbuch ... 294
Anwendungen ... 296
SSO Anwendungen ... 300
Startparameter für SSO Anwendungen ... 305
RDP und SSH Anwendungen ... 308
RDP und SSH Sitzung aufzeichnen ... 311
SAML Anwendungen ... 315
Beispiele für Anwendungen ... 318
SSO-Anwendung für SAP GUI Logon ... 319
SAML-Anwendung für Dropbox ... 321
SAML-Anwendung für Postman ... 325
Password Reset ... 328
Voraussetzungen ... 330
Konfiguration ... 331
Password Safe Skripte ... 334
Benutzerdefinierte Skripte ... 340
Heartbeat ... 342
Rollback ... 345
Logbucheinträge unter Password Reset ... 347
Discovery Service ... 348
Voraussetzungen ... 349
Konfiguration ... 351
Gefundene Einträge ... 355
Konvertierung von Einträgen ... 360
Erstellte Passwörter ... 368
Löschen von Einträgen ... 370
Logbuch ... 372

Hauptmenü ... 374
Import ... 375
Export ... 380
HTML WebViewer-Export ... 381
Export Assistent ... 388
Extras ... 390
Berichte ... 391
Relevante Berichte ... 395
Passwortgenerator ... 402
System Tasks ... 405
Notfall WebViewer ... 409
Passwortrichtlinien ... 418
Siegelvorlagen ... 422

Tagverwaltung ... 424
Bildverwaltung ... 427
Papierkorbverwaltung ... 430
Allgemeine Einstellungen ... 433
Benutzerrechte ... 434
Übersicht aller Benutzerrechte ... 438
Benutzereinstellungen ... 443
Übersicht aller Einstellungen ... 447
Administration ... 454
Konto ... 456

SSO Agent ... 460
Konfiguration ... 463

Browser-Erweiterungen ... 467
Web Anwendungen ... 474
Passwörter speichern ... 479

LightClient ... 482
To do für die Administration ... 484
Errorcodes des LightClients ... 487
Checkliste LightClient ... 489

WebClient ... 490
Funktionsumfang ... 491
Tag System ... 492
Passwörter ... 493
Organisationsstruktur ... 495
Benutzerverwaltung ... 498
Rollen ... 499
Formulare ... 500
Benachrichtigungen ... 501
Anwendung ... 502
Logbuch ... 503
Dokumente ... 504
Bedienung ... 505
Filter- bzw. Strukturbereich ... 508
Header ... 509
Navigationsleiste ... 510
Menü ... 511
Listenansicht ... 513
Lesebereich ... 514
Footer ... 515
Benutzermenü ... 516
Einstellungen ... 518
Berechtigungs- und Schutzmechanismen ... 524
Probleme mit der Serververbindung ... 526

Mobile Geräte **527**

Admin Client **529**
Grundkonfiguration 530
DualStack IP aktivieren (IPv4 + IPv6) 533
Zertifikate 535
Discovery Service Zertifikate 540
SSL Verbindungszertifikate 541
Datenbank Zertifikate 546
Master Key Zertifikate 548
Passwort Reset Zertifikate 551
Einrichtungsassistent 552
Erstellen von Datenbanken 558
Bereinigung Rechteschlüssel 561
Datenbankeigenschaften 564
Datenbank Firewall 566
Syslog 569
Datenbankeinstellungen 570
Multifaktor-Authentifizierung 572
Sitzungs-Timeout 574
Verwaltung von Datenbanken 575
HSM Anbindung über PKCS#11 578
Migration 580
Vorbereitungen 582
Starten des Migrationslaufs 585
Zuordnung von Tags und OUs 588
Berechtigungen nach der Migration 591
Checkliste nach der Migration 592
Bedienung und Aufbau 596
Hauptmenü 601
Allgemeine Einstellungen 602
Backup-Einstellungen 603
Backupverwaltung 604
Automatisiertes Löschen von Backups 609
Desaster Recovery Szenarien 612
Lizenzeinstellungen 615
Erweiterte Einstellungen 617

Hochverfügbarkeit **618**

Offline Client **620**
Einrichten und Synchronisieren 622

How-to **626**
Wechseln eines SSL Verbindungszertifikats 627
WebViewer automatisiert per Mail erhalten 629
Felder kopieren 633

Rechte auf den Datensatz aber nicht auf das Passwortfeld 637
Anzeigen von Passwörtern mit möglicherweise falsch gesetzten Berechtigungen 641

API 644
Beispiele C# SDK 649
Beispiele Javascript SDK 659

Versionshistorie 661
Version 8.14.3.27962 663
Version 8.14.2.27917 665
Version 8.14.1.27830 668
Version 8.14.0.27745 671
Version 8.13.14.27679 674
Version 8.13.13.27522 677
Version 8.13.12.27427 679
Version 8.13.11.27156 682
Version 8.13.10.26901 686
Version 8.13.9.26689 689
Version 8.13.8.25983 692
Version 8.13.7.25979 693
Version 8.13.6.25933 695
Version 8.13.5.25731 698
Version 8.13.4.25228 702
Version 8.13.3.25194 704
Version 8.13.2.25151 706
Version 8.13.1.25117 708
Version 8.13.0.25027 711
Version 8.12.1.22757 716
Version 8.12.0.22707 718
Version 8.11.1.19828 Hotfix 1 729
Version 8.11.1.19823 731
Version 8.11.0.19788 733
Version 8.10.0.18473 Hotfix 2 741
Version 8.10.0.18516 Hotfix 1 746
Version 8.10.0.18472 751

Drittanbieter Lizenzen 756

Herzlich Willkommen …

… bei der offiziellen Hilfe von **Password Safe by MATESO**. Ob Bestandskunde oder Interessent für Password Safe – diese Hilfe unterstützt Sie bei Ihrem optimalen Einstieg in **Version 8**.

Danke, dass Sie beim Schutz Ihres Unternehmens auf Password Safe vertrauen. Wir wünschen Ihnen viel Spaß beim Entdecken Ihrer neuen Software!

[redacted]

[redacted]

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

Falls Sie noch nicht sicher sind, wie Sie weiter vorgehen möchten, nutzen Sie unsere Erläuterung zu den Editionen.

> Wir freuen uns immer über Wünsche und Anregungen, um unser Produkt bestmöglich Ihren Bedürfnissen anzupassen.

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 von Passwörtern …

… ist heutzutage größer denn je: Passwörter sind aus dem Unternehmensalltag nicht mehr 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 enthalten. Im Optimalfall wird für jeden Account ein separates Zugangskennwort genutzt, das natürlich in kurzen zeitlichen Abständen regelmäßig geändert wird. Es ist schon schwer genug, diese Herausforderung privat zu meistern. Für Unternehmen ist es allerdings fast schon unmöglich, hier ohne den Einsatz eines professionellen Passwortverwaltungstools auszukommen.

Durch seine beliebige Skalierbarkeit …

… kann Password Safe sowohl in KMUs als auch in weltweit agierenden Konzernen eingesetzt werden. Version 8 entspricht dabei den heutigen Sicherheitsanforderungen und bietet die perfekte Lösung für alle Unternehmen, die ihre sicherheitsrelevanten Daten (Passwörter, Dokumente, Zertifikate, …) auf allerhöchstem Verschlüsselungsniveau effektiv verwalten möchten. Mittlerweile vertrauen über 10.000 Unternehmenskunden auf MATESO, dem Marktführer für professionelles Passwortmanagement in Deutschland, Österreich und der Schweiz.

Was gibt es Neues in Version 8?

Versionshistorie

Die aktuellen Patchnotes sind stets hier abrufbar.

Ihr persönliches Preview

Unser Produkt entwickelt sich stetig weiter – mitunter dank unserer Kunden: Ihr Lob zeigt uns immer wieder, dass wir auf dem richtigen Kurs sind. Und durch Wünsche und Anregungen werden wir stets motiviert, noch besser zu werden. Als Dankeschön für Ihr Feedback möchten wir Ihnen einen exklusiven EInblick in die neuen Features von **Password Safe Version 8** gewähren:

- 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 den 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

Eines der zentralen Themen bei Version 8 ist die **Berechtigungsadministration** auf Basis von Rollen und Organisationsstrukturen. Mithilfe dieser Funktion können Unternehmens-Hierarchien innerhalb des Rollenkonzepts einwandfrei und lückenlos abgebildet werden. Dazu werden durch einen Abgleich mit dem Active Directory die bereits bestehenden Strukturen importiert und bei Bedarf angepasst. Benutzerinformationen und Gruppenzugehörigkeiten werden somit direkt aus dem Microsoft Verzeichnisdienst übernommen. Optional unterbindet **Ende-zu-Ende Verschlüsselung** (E2EE), dass private Benutzerschlüssel zum Server übermittelt werden. Somit werden Angriffspunkte unterbunden, noch bevor sie entstehen können.

Das ausgeklügelte Berechtigungskonzept stellt dabei sicher, dass jede Benutzergruppe/Abteilung stets nur Zugang zu Passwörtern erhält, auf die sie auch berechtigt ist. Diese Funktion bietet gerade für Großunternehmen und Konzerne starke Vorteile: Denn in Kombination mit Assistenten, Rechtepresets und intuitiv gestalteten Vererbungsmethoden können so auch hierarchisch verschachtelte Benutzerstruktur abgebildet werden.

Privilegiertes Passwortmanagement

Gerade Service Accounts und administrative Zugänge mit weitreichenden Berechtigungen bieten in Unternehmen immer wieder Anlaufstellen für Hacker 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, die automatisch in Password Safe erfasst werden. Mithilfe von **Password Reset** können diese Zugänge 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. Mithilfe des neu konzipierten SSO-Agents ist die automatische Anmeldung auf Websites intuitiv und einfach durchführbar. Auch Verbindungen über RDP oder SSH können so problemlos automatisiert werden. Eine Besonderheit von Password Safe ist bei diesen Zugängen ist, dass Passwörter den Benutzern durch eine Sichtsperrevorenthalten werden können. Besonders sicherheitskritische Anmeldungen können durch das **Mehr-Augen-Prinzip** des Siegelsystems zusätzlich abgesichert werden. **Logs und Historien** machen alle Änderungen jederzeit nachvollziehbar. Auch Dokumente werden in der Datenbank gepflegt und archiviert. Durch die integrierte Versionsverwaltung können diese protokolliert und bei Bedarf wiederhergestellt werden. Mit dem vollkommen automatisierbaren **Reporting-System** liefert Password Safe v8 zudem ein granular definierbares Werkzeug für Sicherheitsaudits.

Mit der richtigen Edition zum Ziel

Verfügbare Pläne

Professional

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

Enterprise

Die Enterprise Edition richtet sich an größere Teams und firmenweite Roll-Outs. 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 User-Anzahl** ausgelegt. Sie beinhaltet sowohl eine API sowie die für große Konzerne unverzichtbaren Features Auto Discovery und Password Reset.

> Für **weitere Informationen** zu den Editionen und Preisen oder bei Interesse an einer **Testlizenz** nutzen Sie bitte den direkten Weg über die offizielle Homepage.

Lizenzmodell

Wie erfolgt die Lizenzierung?

Die Lizenzierung erfolgt auf Basis eines **Strict Named User Modells**. Dieses sieht vor, dass jeder Benutzer eine eigene Lizenz erhält. Zudem werden die Verbindungen vom Client zum Server gezählt. Es gelten die folgenden Rahmenbedingungen:

- Jeder Benutzer benötigt mindestens seine eigene Lizenz. Egal, in welchem Umfang der Password Safe genutzt wird.
- Pro Lizenz kann ein Benutzer Account erstellt werden.
- Sofern die Benutzernamen identisch sind, kann ein Benutzeraccount auch in mehreren Datenbanken verwendet werden. Es wird dann nur eine Lizenz benötigt.
- Das Teilen von Benutzeraccounts ist nicht gestattet, es muss sich immer um die gleiche Person handeln.
- Der Einsatz von LightClient Lizenzen ist in der Enterprise Plus Edition möglich.
- Auch bei alleiniger Nutzung des SSO Agent wird eine Lizenz benötigt.
- Es können auf unterschiedlichen PCs oder Endgeräten maximal so viele Sessions gleichzeitige gestartet werden, wie es auch Benutzerlizenzen gibt. Die gleichzeitige Nutzung auf unterschiedlichen PCs oder Endgeräten benötigt jeweils eine Session. Ein Benutzer kann gleichzeitig bis zu 3 Sessions aufbauen (z.B. WindowsClient, WebClient, Smartphone oder Tablet).

Lizenzzählung

Die Lizenzzählung ist von den aktiven Sessions abhängig. Dabei gilt, dass ein Benutzer an einem Rechner maximal 2 Sessions benötigt. Hierbei benötigen der FullClient und/oder der SSO Agent jeweils eine Session. Das Addon im Servermodus läuft hierbei über den WebClient. Das Addon in Kombination mit dem SSO-Agent bedient sich hierbei der Session des FullClients. Bei gleichzeitiger Verwendung unterschiedlicher Clients können also evtl. zwei Sessions benötigt werden.

Beispiel:

Client Typ		Client Typ		verbrauchte Sessions
FullClient	+	SSO-Agent	=	**1 Session**
FullClient	+	Addon (SSO Agent)	=	**1 Session**
WebClient	+	Addon (Servermodus)	=	**1 Session**
FullClient	+	WebClient	=	**2 Sessions**
FullClient	+	Addon (Servermodus)	=	**2 Sessions**
FullClient	+	WebClient + Smartphone	=	**3 Sessions**
WebClient	+	Smartphone + Tablet	=	**3 Sessions**

Meldet sich ein Benutzer an einem weiteren Rechner an, so werden weitere Session aufgebaut und somit auch weitere Lizenzen verbraucht. Ein Benutzer kann gleichzeitig bis zu 3 Sessions aufbauen (z.B. WindowsClient, WebClient und Smartphone/Tablet).

Module aus der Version 7

In Version 7 konnte die Lizenzierung pro Rechner noch mittels Modulen angepasst werden (Modul Ohne Client-Lizenzierung). Module werden in Version 8 allerdings nicht mehr benötigt: Alle Lizenzierungsverfahren sind durch obiges Lizenzmodell abgedeckt.

Bei Fragen zur Lizenzierung steht unser **Vertriebsteam** gerne zur Verfügung.

Feature-Matrix

Die Editionen auf einen Blick

Sicherheit	Essential	Professional	Enterprise	Enterprise Plus
Ende-zu-Ende-Verschlüsselung (E2EE)	•	•	•	•
Datenversionierung (Historie)	•	•	•	•
Rollenbasierte Zugriffskontrolle (RBAC)	•	•	•	•
Passwort-Abruf nur durch Begründung	•	•	•	•
Passwortgenerator	•	•	•	•
Sitzungsverwaltungen	•	•	•	•
Schutz durch Transport Layer Security Verbindung (TSL)	•	•	•	•
Logbuch mit Filtermöglichkeit	•	•	•	•
Anmelde-Service im Internet	•	•	•	•
Funktioneller Headerbereich	•	•	•	•
Optionale automatische Bereinigungen	•	•	•	•
Zentralisierte Team-Datenbank	•	•	•	•
Revisionssichere Protokollierung	•	•	•	•
AES 256 Encryption / PBKDF2	•	•	•	•
RSA für Langzeitschlüssel	•	•	•	•
Hierarchische Verschlüsselung für Freigaben über Rollen und Benutzer	•	•	•	•
Generieren von One-Time-Password	•	•	•	•
Tasksystem		•	•	•
Mehr-Augen-Prinzip (Siegel)		•	•	•
Sichtschutz für Passwörter		•	•	•
Live-Benachrichtigungen		•	•	•
Zwei-Faktor-Authentifizierung		•	•	•
Echtzeitaktualisierungen		•	•	•
PKI-Integration			•	•
Datenbank-Firewall			•	•

RADIUS-Anbindung			•	•
Offline-Zugriff (Notfall Web Viewer 2FA-geschützt)			•	•
Session-Recording				•
Produktivität	**Essential**	**Professional**	**Enterprise**	**Enterprise Plus**
Plattformunabhängiger WebClient	•	•	•	•
Syslogserver-Anbindung	•	•	•	•
Flexible Rechtevorlagen	•	•	•	•
Passwortrichtlinien	•	•	•	•
Dokumenten-Historie	•	•	•	•
Add-ons für alle Browser	•	•	•	•
Vererbbare Benutzereinstellungen und -rechte	•	•	•	•
Integrierter LightClient	•	•	•	•
Dynamische Dashboards	•	•	•	•
Terminalserver-Unterstützung	•	•	•	•
Anpassbare Eingabemasken	•	•	•	•
App-Synchronisation	•	•	•	•
Drucken und Export	•	•	•	•
Übersichtlicher Footer-Bereich	•	•	•	•
Rechtemanagement bis auf Feldebene	•	•	•	•
Produktion von externen Links	•	•	•	•
Barrierefreie Bedienung	•	•	•	•
Dynamische Listen/Anpassbare Grids	•	•	•	•
Umschaltbare Listenansicht	•	•	•	•
PuTTY-Client	•	•	•	•
Schnellansicht	•	•	•	•
Eintragung und Anlernen von Anwendungen	•	•	•	•
Tabsystem	•	•	•	•
Lernfähige Suchfilter mit Volltextsuche	•	•	•	•
Fernzugriff über integrierten RDP-Client	•	•	•	•
Anpassbarer Infobereich	•	•	•	•

Dokumente	•	•	•	•
Individuelle Einstellungen pro Passwort	•	•	•	•
Schnellnavigation	•	•	•	•
Organisationsstrukturen	•	•	•	•
Hohe Auflösung von Texten und Bildern	•	•	•	•
Tag-Funktion	•	•	•	•
Restriktive Benutzer	•	•	•	•
Intelligente Schnellsuche	•	•	•	•
Sicherheitsstufen für Einstellungen	•	•	•	•
Verschiedene Farbschemen	•	•	•	•
Auditing und Reports		•	•	•
WebViewer		•	•	•
Temporäre Freigaben für Passwörter			•	•
Automatische Active Directory (AD) Synchronisation			•	•
Heartbeat für Password Reset				•
Anbindung an Hardware-Sicherheitsmodule (HSM)				•
Exklusive LightClient-Lizenzen				•
Automation	**Essential**	**Professional**	**Enterprise**	**Enterprise Plus**
Single Sign-on (SSO) Agent	•	•	•	•
Verbindungssperren	•	•	•	•
MSI-Softwareverteilung	•	•	•	•
Tastenkürzel und Scriptingfunktionalität	•	•	•	•
Integration des Active Directory (AD) mit LDAP			•	•
Automatische Reports			•	•
Discovery Service für Dienstkonten				•
Password Reset and Password Synchronization				•
Rollback für Password Reset				•
API-Schnittstelle				•
Managen von privilegierten Accounts (Privileged				•

Account Management)				
Identity Provider				•
Hochverfügbarkeit	**Essential**	**Professional**	**Enterprise**	**Enterprise Plus**
SQL-Clustering**	•	•	•	•
Skalierbarkeit	•	•	•	•
Automatische Live-Backups	•	•	•	•
Import wichtiger Daten	•	•	•	•
Responsive WebClient (IIS, Apache, nginx)	•	•	•	•
Offline-Zugriff (HTML-WebViewer über Browser)		•	•	•
Lastverteilung über mehrere Anwendungsserver*			•	•
Offline-Modus (über Client)			•	•
SQL-Server-Replikation (verteilte Standorte)**			•	•

*Im Essential und Professional Plan sind max. 1 Anwendungsserver, im Enterprise Plan sind max. 2 Anwendungsserver erlaubt. Im Enterprise Plus Plan können beliebig viele Anwendungsserver eingesetzt werden (Jeder Anwendungsserver muss separat erworben werden).

*Für die Funktionalität sind externe Tools notwendig (Microsoft Load Balancer oder andere Load Balancer).

**Für die Funktionalität sind externe Tools notwendig (Microsoft SQL Server).

Sicherheit

IT-Sicherheit im Wandel

Die digitalen Infrastrukturen Deutschlands gehören weltweit zu den sichersten. Dafür wurde im Juli 2015 das **IT-Sicherheitsgesetz** wegbereitend eingeführt, um eine Vorrreiterstellung im Kampf gegen digitale Bedrohungen einzunehmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI), das auch für die **ISO 27001 Zertifizierung auf Basis der IT-Grundschutz-Kataloge** verantwortlich ist, hat dafür schon vor langer Zeit die Weichen gestellt. Die in der **Richtlinie zur Netz- und Informationssicherheit (NIS)** definiert Maßnahmen gewährleisten zudem ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der europäischen Union.

Gefahren und Risiken

All das sind Reaktionen auf eine Gefahrenlage, die 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 Bundesamt für Verfassungsschutz jährlich über eine Million Mal ins Visier von Hackern. Die Motive sind unterschiedlicher Natur: Finanzielles, aber auch politisches Interesse, wie bei den sogenannten “Hacktivisten” und Geheimdiensten. Das BKA warnt schon seit Jahren vor Erpressungswellen im Internet gegen Privatpersonen und Unternehmen. Gerade sicherheitskritische Unternehmensinterna sind regelmäßig Ziel von Angriffen.

Passwörter als Achillesferse

Aufgrund des raschen digitalen Wandels rückt besonders das Thema Passwortsicherheit immer mehr in den Fokus: Kennwörter, die vor wenigen Jahren noch als sehr sicher galten, müssen aufgrund des technischen Fortschritts erneut auf den Prüfstand. Es wird empfohlen, nur zufällig gewählte Passwörter mit einer entsprechenden Länge zu verwenden und diese auch regelmäßig zu ändern.

Der Lösungsansatz des MATESO Password Safe

Die sichersten Passwörter sind immer noch diejenigen, die der User gar nicht kennt: Die Funktion **automatisches Eintragen** ermöglicht den Nutzern effizientes Arbeiten ohne ein Passwort überhaupt zu wissen.
Mithilfe von **Password Reset** können Passwörter außerdem automatisiert in beliebig kurzen Intervallen zurückgesetzt werden. Dazu kommen diverse Sicherheitsvorkehrungen wie das **Mehr-Augen-Prinzip**: Hier erhält der Benutzer nur Zugang zu Systemen, wenn ihm die Freigabe von dafür berechtigten Personen erteilt wurde. All diese Routinen werden durch **hochkomplexe Verschlüsselungsverfahren** gesichert. Durch regelmäßige Penetrationstests wird die Software von unabhängigen Experten gezielt auf Schwachstellen in der Architektur sowie den korrekten Einsatz modernster kryptographischer Technologien geprüft. Zusammenfassend: Menschliches Fehlverhalten im Umgang mit Passwörtern muss durch technisch erzwungene Vorgaben und Workflows auf ein Minimum reduziert werden.

Egal ob KMU, globaler Konzern oder staatliche Behörde: Will man zukünftig das Risiko von Datendiebstahl 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 hat oberste Priorität bei Password Safe. Schon während der Entwicklungsphase wurde das Konzept der Software von unabhängigen Sicherheitsunternehmen auf Einhaltung der IT-Sicherheitsstandards geprüft. Erst auf Basis dieser Erkenntnisse wurde letztendlich Password Safe entwickelt.

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 für Private- und Public-Key Verfahren

Alle von Password Safe verwendeten Verschlüsselungsalgorithmen sind **FIPS** konform.

Angewandte kryptografische Verfahren

Diese Algorithmen bilden die Basis für die Containerverschlüsselung von Passwörtern. Jeder Container hat dabei einen eigenen, zufällig generierten Salt. Jedes Passwort, jeder Benutzer und jede Rolle besitzt ein eigenes Schlüsselpaar. Um maximale Sicherheit zu erzielen, nutzt Password Safe zusätzlich folgende 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. Welche Daten Secrets sind, entscheidet der Kunde. Nach Secrets kann auch nicht gesucht werden.

Von uns getestete Security Hardwarekomponenten:

HSM:

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

Siehe auch Kapitel **HSM**.

Zwei-Faktor-Authentifizierung:

- SafeNet eToken Pass
- RSA SecurID 700
- Google Authenticator

Externe Penetrationstests

Externe Penetrationstests

Die hohen Sicherheitsstandards von Password Safe werden durch externe Pentests unterschiedlicher Anbieter regelmäßig bezeugt. Gerade neue Funktionen werden stets Penetrattionstests unterzogen, um diese vor Veröffentlichung eingehend prüfen zu lassen. Durch die daraus resultierenden Erkenntnisse können potentielle Schwachstellen schon im Vorfeld aufgespürt und beseitigt werden.

Warum wir regelmäßig testen

Beim Pentest suchen externe und zertifizierte Sicherheitsprüfer gezielt nach Sicherheitslücken und Schwächen in der Software, die ein Angreifer ausnutzen könnte. Hierbei werden etwa clientseitig Angriffsszenarien simuliert, der Sourcecode überprüft und das kryptografische Verfahren qualitativ beurteilt. Somit wird die Sicherheit von Password Safe und den darin gespeicherten Daten schon im Voraus getestet, um unseren Kunden effektiven Schutz bieten zu können und das Erfolgsrisiko eines Angriffs zu minimieren.

IT-Security Made in Germany

Die TeleTrusT-Initiative & Password Safe

Die MATESO GmbH, wie auch Password Safe selbst, sind Mitglied der TeleTrusT-Initiative “**IT-Security Made in Germany**”.
Das Gütesiegel wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert.

Password Safe entspricht den hohen Standards des Gu¨tesiegels. MATESO garantiert durch seinen deutschen Unternehmenshauptsitz IT-Security Made in Germany. Mit deutschsprachigen Ansprechpartnern, lokal verfu¨gbaren Vertriebs-, Dienstleistungs- und Schulungspartnern sowie deutschen Hotline-Nummern bestätigen wir den hohen Servicestandard unserer Software.

Die Kriterien

Als TeleTrust-Mitglied verpflichtet sich MATESO die fu¨nf fu¨r das Qualitätszeichen maßgeblichen Kriterien zu erfu¨llen:

- Der Unternehmenshauptsitz ist in Deutschland.
- MATESO bietet vertrauenswu¨rdige IT-Sicherheitslösungen an.
- Die angebotenen Produkte enthalten keine versteckten Zugänge (“**Backdoors**”).
- Die IT-Sicherheitsforschung und -entwicklung von Password Safe findet in Deutschland statt.
- MATESO verpflichtet sich, den Anforderungen des deutschen Datenschutzrechtes zu genu¨gen.

Sicherheitslücken – Ist Password Safe betroffen?

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

- Log4J
- Spring4Shell
- Robot

Log4J

Was ist passiert?

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

Ist Password Safe betroffen?

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

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

> Bitte die Software regelmäßig aktualisieren

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

Sicherheitsempfehlungen

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

Zum Apache How-To

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

Spring4Shell

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

> ! Password Safe nicht betroffen

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

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

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

Robot

Was ist Robot?

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

Wie kann man sich schützen?

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

Diese Lücke kann mit testssl.sh verifiziert werden.

Gefahr für Password Safe?

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

Erste Schritte

Erste Schritte

Wir empfehlen Ihnen, sich bei der Installation von Password Safe an folgende Schritte zu halten. Zudem sollten Sie alle durchgeführten Konfigurationen, wie z.B. vergebene Passwörter, sauber notieren.

Falls Sie während der Installation Lücken innerhalb der Hilfe finden, freuen wir uns über eine kurze Rückmeldung.

1. Microsoft SQL Systemanforderungen

Aufgrund des performanten Datenzugriffs, der weitläufigen Verbreitung sowie der umfangreichen Backupmöglichkeiten verwendet der Password Safe Microsoft SQL Server als Datenbankmanagementsystem.

Hier geht es zu den Systemanforderungen MSSQL

2. Systemanforderungen Anwendungsserver

Beachten Sie besonders die Unterkapitel **benötigte Benutzer** sowie **Rechte auf die PowerShell Skripte**.

Hier geht es zu den Systemanforderungen des Anwendungsservers

3. Systemanforderungen Client

Die Anforderungen an die Clientumgebung werden separat beschrieben.

Hier geht es zu den Systemanforderungen des Clients

4. Installation des Admin Client

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

Mit Hilfe des Assistenten werden bei der Installation des Password Safe Admin Clients alle erforderlichen Parameter konfiguriert.

Hier geht es zur Installation des Admin Clients

5. Password Safe Grundkonfiguration

Beim ersten Öffnen des Admin Clients startet direkt die Password Safe Grundkonfiguration.

Hier geht es zu den Erläuterungen der Password Safe Grundkonfiguration

6. Authentifizierung am Admin Client

Nach dem Abschluss der Grundkonfiguration können Sie 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. Zudem erfolgt die Einbindung der Lizenz sowie die Konfiguration der Datenbank- und SMTP-Einstellungen.

Hier geht es zum Einrichtungsassistenten

8. Erstellung von Datenbanken

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

Die MSSQL-Datenbanken können Sie auch direkt über den Admin Client erstellen und verwalten.

Hier geht es zur Erstellung von Datenbanken

9. Installation des Clients

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

Die Installation des Clients ist der erste Schritt, um Benutzern das Arbeiten mit Password Safe zu ermöglichen.

Hier geht es zur Installation des Clients

10. Erstellung von Datenbankprofilen

Die Anzahl der Datenbanken wird **nicht** lizenziert und ist demnach theoretisch beliebig.

Hier geht es zur Erstellung von Datenbankprofilen

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

Architektur und Systemanforderungen

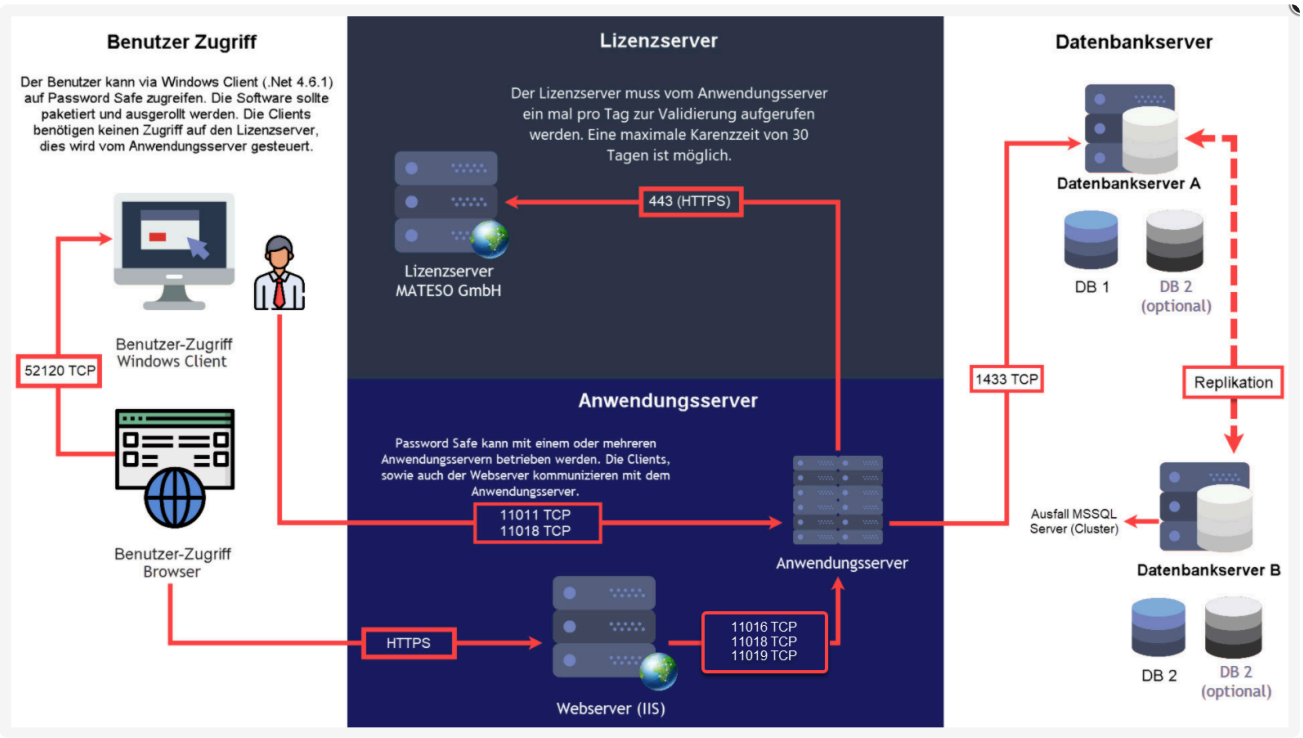
Multi-Tier-Architektur

Die Struktur von Password Safe v8 basiert auf dem Prinzip der **Multi-Tier-Architektur**, bei dem die einzelnen Softwarekomponenten mehrschichtig aufgebaut sind. Diese drei separat agierenden Schichten sind beliebig skalierbar. Daher kann Password Safe v8 auf von Konzernen mit sehr vielen Benutzern sowie **weltweit verteilten Standorten** eingesetzt werden. Dank der **“Ende-zu-Ende” Verschlüsselung** werden die Daten direkt an den Clients verschlüsselt bzw. entschüsselt. Damit wird sichergestellt, dass am Datenbankserver wie auch am Applikationsserver niemals unverschlüsselte Passwörter vorliegen. Das **Private- und Public-Key Verfahren** sorgt dafür, dass der private Schlüssel nur dem Benutzer vorliegt. Der Anwendungsserver kennt nur den öffentlichen Schlüssel und kann daher ein Passwort nicht einsehen.

Password Safe in der Version 8 kann in kleinen als auch weltweiten Systemlandschaften betrieben werden: Innerhalb der Multi-Tier-Architektur können beliebig viele Clients, Anwendungsserver und Datenbankserver angebunden werden. Es ist empfehlenswert, die Datenbank im Produktivsystem 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

Folgend sieht man die grafische Darstellung einer klassischen Password Safe **Systemlandschaft**. In der Version 8 können standortübergreifend mehrere Datenbankserver eingesetzt werden, die dann mit Microsoft Bordmitteln untereinander synchronisiert werden. Für die Client-Verbindung können beliebig viele Anwendungsserver verwendet werden. Dies ermöglicht aufgrund der Lastverteilung Arbeiten ohne Verzögerungen. Besonders bei global aufgespannten Installationen bringt diese Technik enorme Performanzvorteile.



Client (Präsentationsschicht)

Die Client-Schicht übernimmt die Darstellung aller Daten und Funktionen, die 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 auch entsprechende Berechtigungen vorliegen. Die Multi-Tier-Architektur ermöglicht den Einsatz mehrerer Applikationsserver und sorgt für ein 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. Für jede Funktion sollte ebenso ein Windows Server bereitgestellt werden. Durch die Trennung der Systeme sind spätere Erweiterungen und Skalierungen einfacher umsetzbar. Dennoch ist die Trennung nicht zwingend

erforderlich: Bei kleineren Installationen können auch alle Komponenten auf einem Server installiert werden.

Zusammenfassung aller Portfreigaben:

MSSQL:

- Port 1433 TCP für die Kommunikation mit dem Anwendungsserver (eingehend)

Server:

- Port 443 HTTPS zur Verbindung zum MATESO Lizenzserver (ausgehend)
- Port 11011 TCP zur Kommunikation mit den Clients oder dem Webserver IIS (eingehend)
- Port 11014 TCP für den Backupdienst (muss in der Regel nicht freigegeben werden)
- Port 11016 TCP für die Webdienste (eingehend; nur bei Einsatz des WebClients)
- Port 11018 TCP für die Echtzeitaktualisierung (eingehend)
- Port 1433 TCP für die Kommunikation mit dem SQL Server (ausgehend)

Client:

- Port 11011 TCP zur Kommunikation mit dem Anwendungsserver (ausgehend)
- Port 52120 TCP mit der Browser-Erweiterung (ausgehend)
- Port 11018 TCP für die Echtzeitaktualisierung (ausgehend)

WebClient:

- Port 443 HTTPS zum Ansprechen des Webservers vom Client (eingehend)
- Port 11016 zur Kommunikation mit dem Anwendungsserver (ausgehend)
- Port 11018 für die Echtzeitaktualisierung (ausgehend)
- Port 11019 für SAML

Systemanforderungen MSSQL

Benötigte Hardware

Um Ausfällen vorzubeugen empfehlen wir, die Datenbank auf einem separaten MSSQL Datenbank Cluster zu installieren. Zusätzlich sollte sie in ein zweites, räumlich getrenntes Rechenzentrum gespiegelt werden. Nachfolgend unsere Empfehlung für den optimalen Betrieb:

- min. Windows Server 2012 R2
- 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 Portfreigabe:

- Port 1433 TCP für die Kommunikation mit dem Anwendungsserver (eingehend)

> Unter folgendem Link finden Sie einen Vergleich der unterschiedlichen MSSQL-Server-Editionen:
> **SQL Server Editionen**
> Sie können hier auch die Kapazitätsgrenzen der einzelnen Editionen einsehen.

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 beinhalten

Voraussetzungen

Die Datenbanken erzeugen und verwalten Sie direkt über die Admin Konsole. Schaffen Sie hierfür folgende **Voraussetzungen** auf dem MSSQL-Server:

Benutzer

Verwenden Sie für die Verwaltung der Password Safe V8 Datenbanken einen spezifischen Benutzer. Der Server Admin (SA) kann zwar verwendet werden, ist aber nicht zwingend nötig. Der User benötigt 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

Jede Password Safe Datenbank entspricht einer MSSQL-Datenbank. Sie können mehrere Datenbanken auf einer SQL-Instanz betreiben. Da Password Safe V8 über das Berechtigungskonzept eine saubere Trennung aller Daten ermöglicht, ist in den meisten Anwendungsfällen eine einzige 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 erstellen Sie die Datenbank serverseitig manuell mit der korrekten Collation. Anschließen binden Sie diese dann am Admin Client ein.

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 gleichzeitig aktiven Benutzer als auch durch die Menge an gleichzeitigen Server-Anfragen bestimmt. Um den optimalen Betrieb zu gewährleisten, empfehlen wir folgende Hardware-Konfiguration:

- min. Windows Server 2012 R2 (aktueller Patchlevel-Stand ist zwingend notwendig!)
- min. 2 x CPU's
- min. 8 GB RAM
- min. 40 GB Festplattenspeicherplatz
- .net Bibliothek 4.8.0 oder neuer
- Firewall-Freigabe
- Windows Management Framework 5.0 muss installiert sein

Der Applikationsserver benutzt die folgenden Ports:

- Port 443 HTTPS zur Verbindung zum MATESO Lizenzserver (ausgehend)
- Port 11011 TCP zur Kommunikation mit den Clients oder dem Webserver IIS (eingehend)
- Port 11014 TCP für den Backupdienst (muss in der Regel nicht freigegeben werden)
- Port 11016 TCP für die Webdienste (eingehend; nur bei Einsatz des WebClients)
- Port 11018 TCP für die Echtzeitaktualisierung (eingehend)
- Port 1433 TCP für die Kommunikation mit dem SQL Server (ausgehend)

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

> Achten Sie bei einer Anbindung außerhalb eines lokalen Netzwerkes (beispielsweise über VPN), 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)

Für den Web-Zugriff wird ein Webserver benötigt. Für eine bessere Performance gerade bei größeren Installationen können auch mehrere Webserver konfiguriert werden. Wir empfehlen folgende Hardware-Konfiguration für jeden Webserver:

- min. Windows Server 2012 R2 (aktueller Patchlevel-Stand ist zwingend notwendig!)
- min 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 den sich der Password Safe Server am SQL-Server anmelden kann. Ebenso wird ein Benutzer, der die Password Safe Dienste ausführt, benötigt. Im Folgenden werden die verschiedene Konstellationen erläutert:

Dienstbenutzer

Der Dienstbenutzer führt den Password Safe Server-Dienst aus. Hier kann 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. Sonst fehlen ihm die Rechte, um in den Zertifikats-Store zu speichern.

Backupdienst-Benutzer

Prinzipiell wird der Backupdienst durch den Dienst-Benutzer ausgeführt. Im Experten-Modus kann jedoch auch ein anderer Benutzer verwendet werden. Für den Backupdienst-Benutzer gilt dasselbe wie für den Dienst-Benutzer.

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:** Bei aktivierter Checkbox wird der hinterlegte Dienst-Benutzer verwendet. Bitte beachten Sie, 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.

> * Für die Erstellung der Datenbanken durch den 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 Dienst-Benutzer angelegt, um sowohl den Password Safe Server Dienst als auch den Backup Dienst zu starten. Dafür benötigt der Benutzer Rechte, um Dienste starten zu können. Dieser Benutzer wird dann (durch Aktivieren der Checkbox) für die SQL-Konfigurationsinstanz verwendet.

Variante 2:
Als Dienst-Benutzer 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.

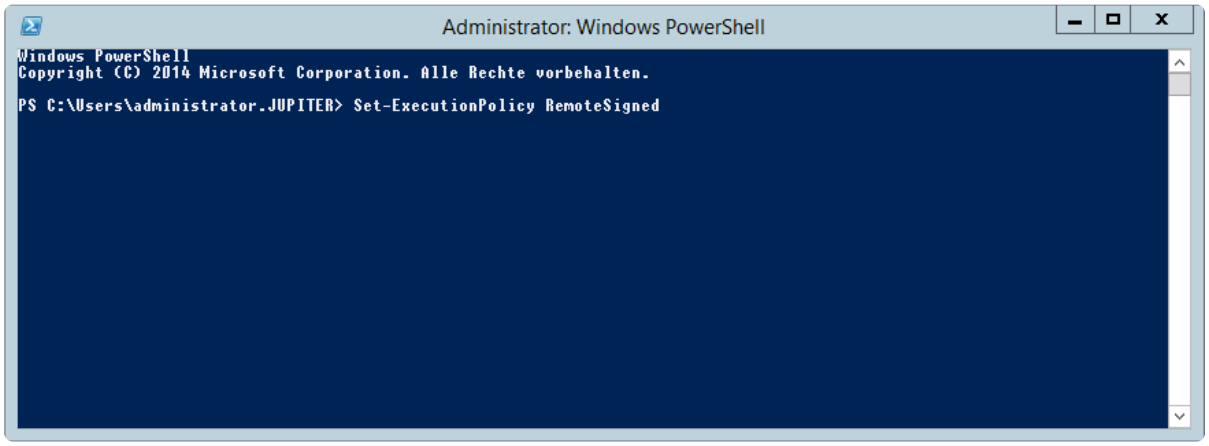
> ! Für die SQL-Konfigurationsinstanz ist die Kombination von lokalem System und Dienst-Benutzer nicht möglich!

Rechte auf Windows PowerShell

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

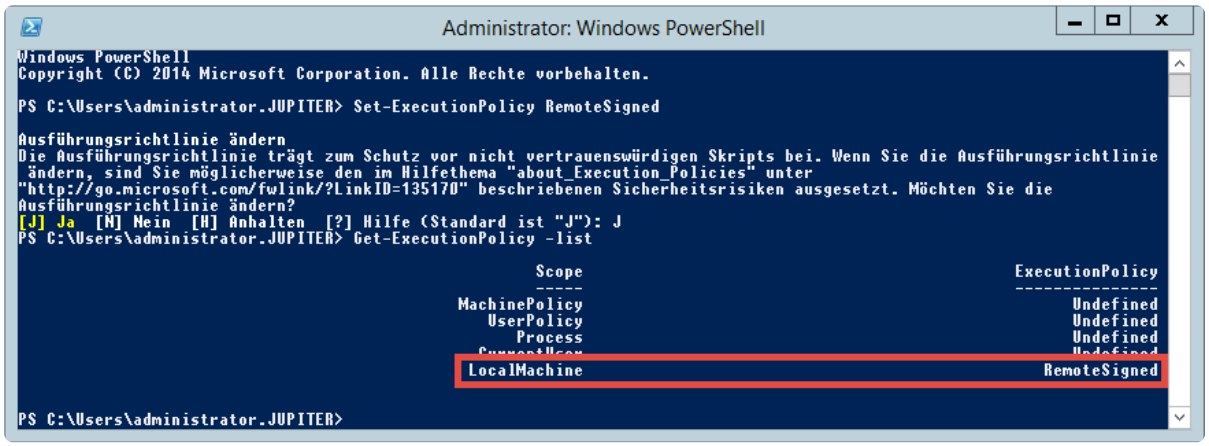
> ! Windows Management Framework 4.0 muss installiert sein (Windows-Update KB2819745)!

Öffnen Sie die PowerShell Konsole und geben **Set-ExecutionPolicy RemoteSigned** ein.



Bestätigen Sie die Änderung der Richtlinie.

Abschließend besteht die Möglichkeit über **Get-ExecutionPolicy -list** die geänderte Richtlinie abzufragen.



Hier geht´s zurück zum Kapitel Erste Schritte

Systemanforderungen FullClient

Benötigte Hardware

Der FullClient läuft unter allen Windows Betriebssystemen ab Version 7. Für den optimalen Betrieb empfehlen wir folgende Hardware Konfiguration:

- Microsoft Windows ab Version 7 (aktuellster Patchlevel)
- min. 2 x CPU’s
- min. 2 GB RAM
- min. 40 GB Festplattenspeicherplatz
- .net Bibliothek 4.8.0 oder neuer
- Sollen RDP Verbindungen aufgebaut werden können, muss mindestens RDP 8.1 installiert sein.

Der FullClient benötigt folgende Port Freigaben:

- Port 11011 TCP zur Kommunikation mit dem Anwendungsserver (ausgehend)
- Port 52120 TCP mit der Browser-Erweiterung (ausgehend)
- Port 11018 TCP für die Echtzeitaktualisierung (ausgehend)

> Wir empfehlen, den FullClient zu paketieren und auf den entsprechenden Endgeräten zu installieren. Das entsprechende MSI-Paket finden Sie in unserem Download-Portal.

Einsatz im Terminalserver-Betrieb

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

Wir empfehlen, dass der WebClient den gleichen Versionsstand wie der Application Server hat. Der Password Safe WebClient kann auf allen aktuellen Webservern aufgesetzt werden. Das für die gesicherte https-Anbindung benötigte SSL-Zertifikat kann beispielsweise über eine entsprechende Zertifizierungsstelle ausgestellt werden. Alternativ können Sie ein bereits für die Top-Level-Domain vorhandenes Zertifikat verwenden.

> Da jeder Webserver individuell installiert und konfiguriert ist, werden detaillierte Kenntnisse des verwendeten Systems vorausgesetzt. Bei Bedarf sind Ihnen unsere Partner gerne bei der Installation behilflich.

Der WebClient benötigt folgende Port Freigaben:

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

Unterstützte Webserver

Der Password Safe WebClient wurde auf folgenden Systemen erfolgreich getestet:

IIS

- ab **Version 7**
- Modul **URL Rewrite** ab Version 2.1
- Modul **Application Request Routing** ab Version 3.0
- Modul **WebSocket Protocol**

Apache

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

nginx

- ab **Version 1.13**

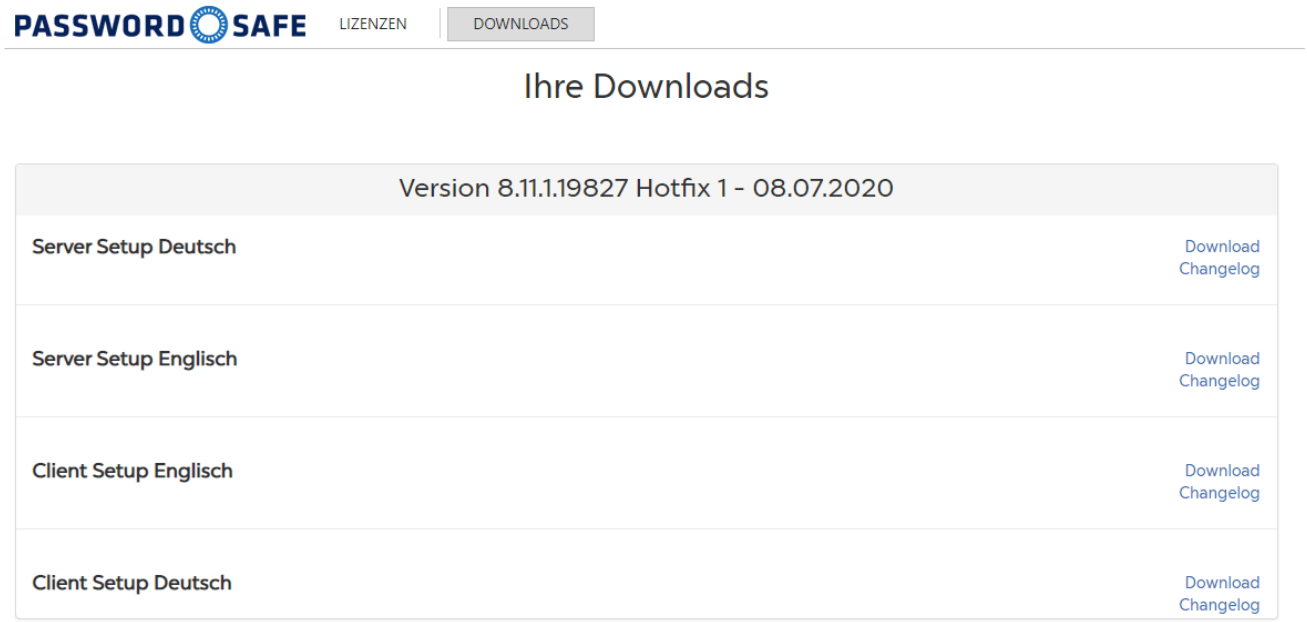
> Sollten Sie einen anderen als die oben aufgeführten Systeme verwenden wollen, testen Sie im Vorfeld einer produktiven Nutzung alle Funktionen. Aufgrund möglicher Seiteneffekte kann die reibungslose Funktion in diesem Fall nicht garantiert werden.

! Die Verbindung vom Browser zum Webserver muss über ein SSL-Zertifikat geschützt werden. Es wird ausdrücklich empfohlen, hierfür ein Zertifikat eines Dienstleisters zu erwerben. Wenn Sie kein offizielles Zertifikat erworben haben: Stellen Sie bitte unbedingt sicher, dass dem Zertifikat entsprechend getraut wird. Anderenfalls erscheint eine entsprechender Hinweis im Browser, dass das Zertifikat unsicher ist.

Installation

Installationsdateien

Die Installationsdateien finden Sie in unserem Download-Portal.



Die Zugangsdaten erhalten Sie zusammen mit der Lizenz. Für eine Testlizenz nutzen Sie bitte das hierfür vorgesehene Formular.

> ✻ Ab Password Safe Version 8 werden keine Zertifikate mehr ausgeliefert. Ihr Zertifikat ist auf unserem Lizenzserver hinterlegt und kann mit den übermittelten Zugangsdaten abgerufen werden.

Konzeption vor der Installation

Durch Password Safe werden Unternehmenshierarchien in Form von differenzierbaren und präzise definierbaren Rechtestrukturen abgebildet. Je genauer man diese hierarchischen Ordnungen kennt, desto einfacher gestaltet sich die Umsetzung. Fehler in der Analysephase können somit häufig zu Folgefehlern führen, deren Korrektur sehr zeitaufwendig ist. Der Konzeptionierung sollte deshalb unbedingt die nötige Aufmerksamkeit gewidmet werden.

Dokumentation parallel zur Installation

> ! Dokumentation ist ein wichtiger Bestandteil der Installation. Tragen Sie dafür Sorge, dass die genutzten Systeme und Zugänge lückenlos erfasst werden. Sowohl bei Veränderungen in der Zuständigkeit als auch bei Anpassungen der Architektur ist ein

Nachschlagewerk in Form einer vollständig vorhandenen Password Safe Dokumentation von Vorteil.

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 von 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 WebClient

Installation AdminClient

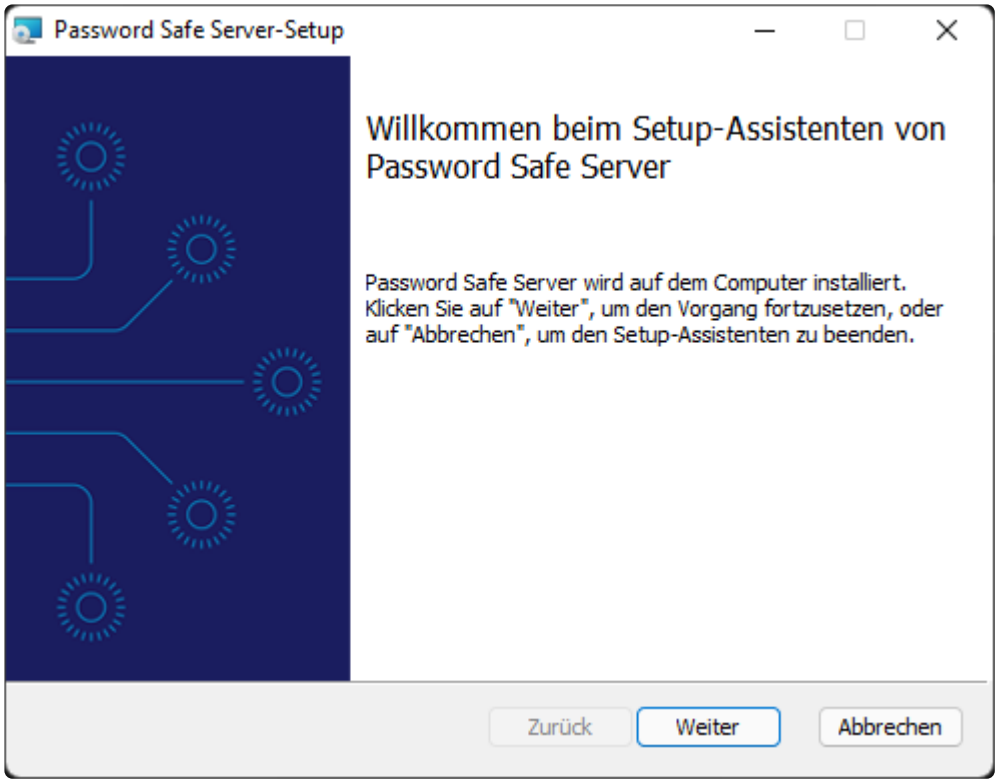
Video Guide

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

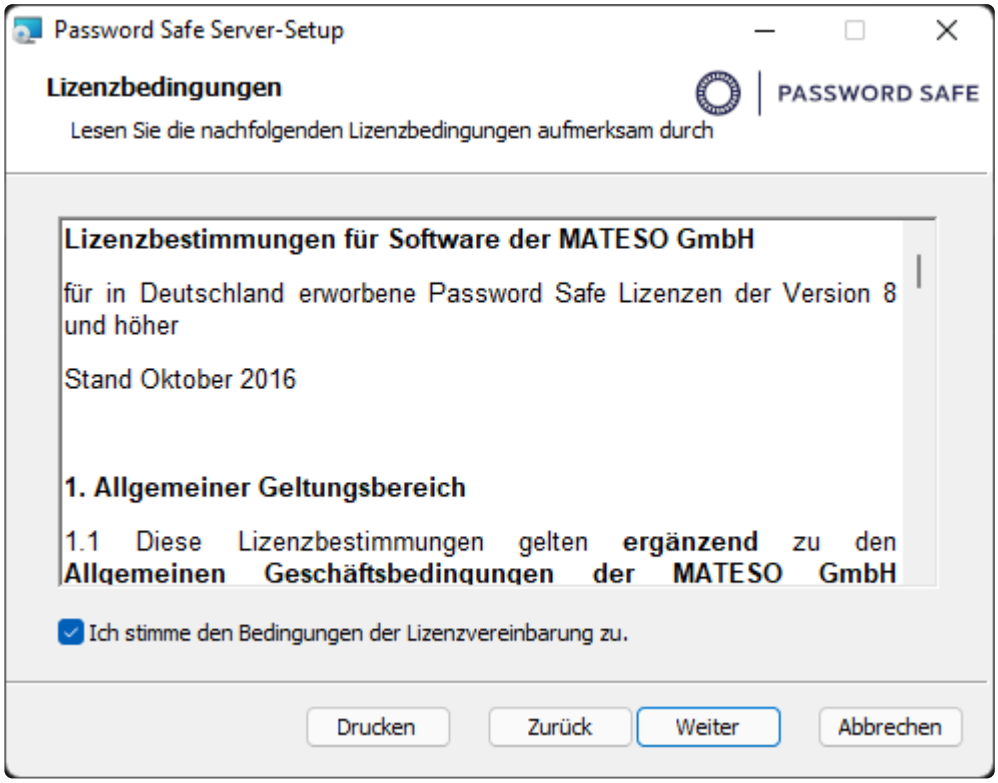
https://www.youtube.com/embed/mWKzPWjlqIY?rel=0

Anleitung

Die MSI-Installationsdateien sowie die zugehörigen Systemanforderungen Server finden Sie in den entsprechenden Kapiteln. Die nachfolgende Schritt-für-Schritt-Anleitung führt Sie durch den Assistenten.

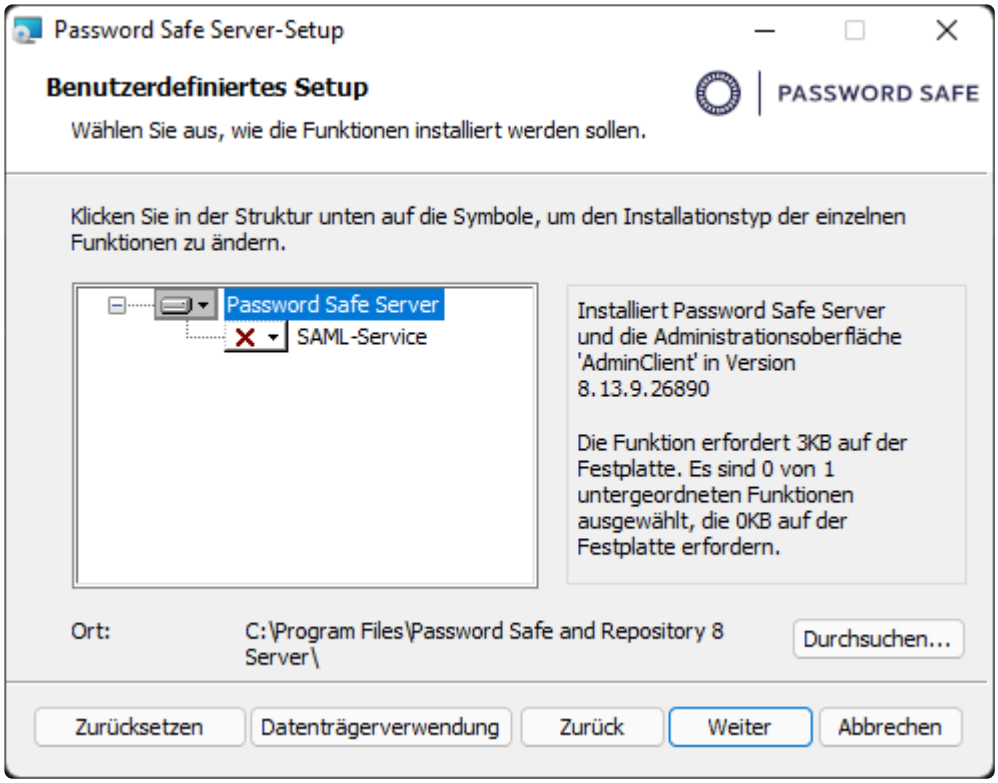


Schritt 1: Lizenzbedingungen lesen und akzeptieren (Druck-Funktion verfügbar)

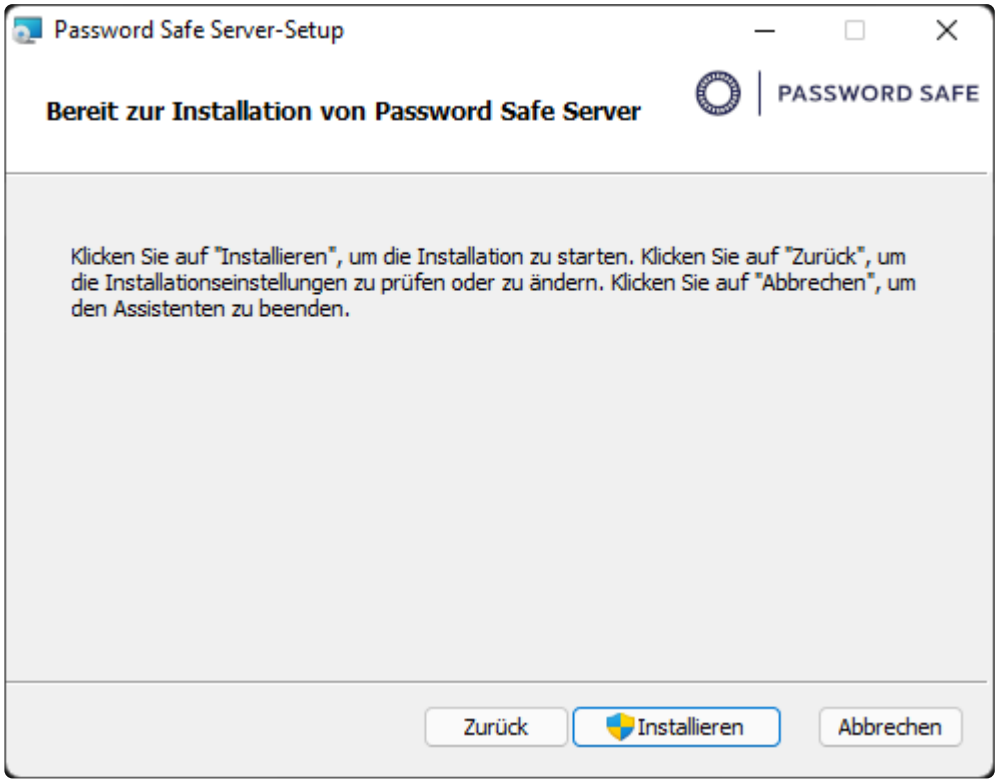


Schritt 2: Speicherort festlegen: In der Regel kann der vorgeschlagene Speicherort beibehalten werden.

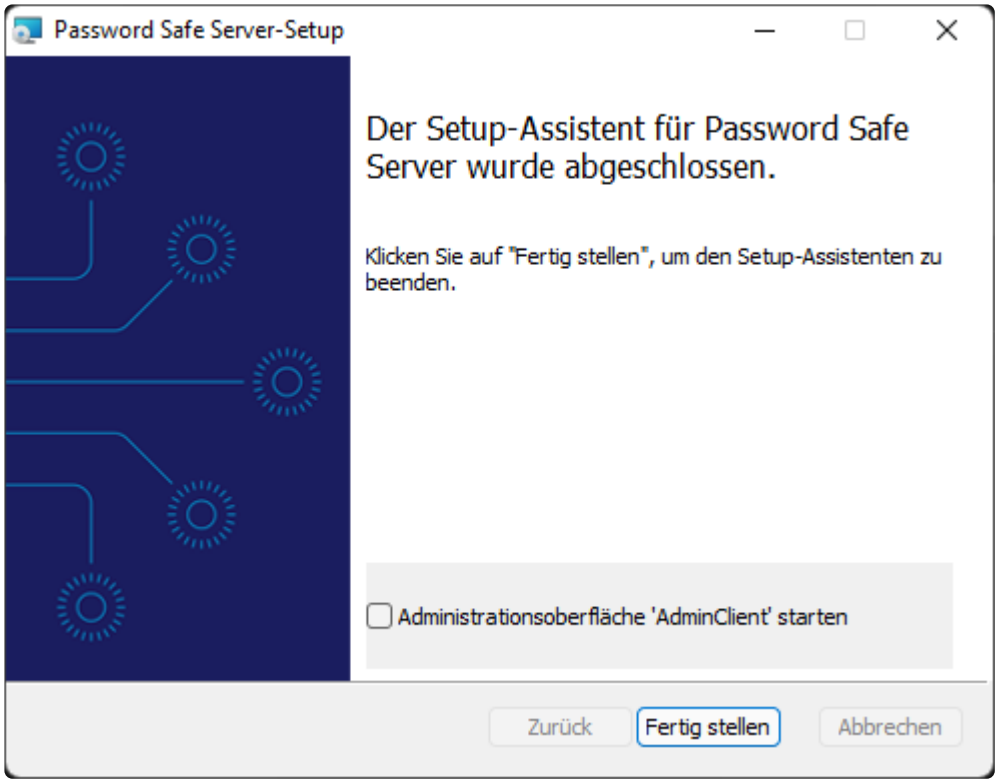
Der SAML-Service muss nur selektiert werden, wenn Sie Password Safe als Identity Provider zu verwenden wollen. Andernfalls wird er nicht installiert.



Schritt 3: Start der Installation

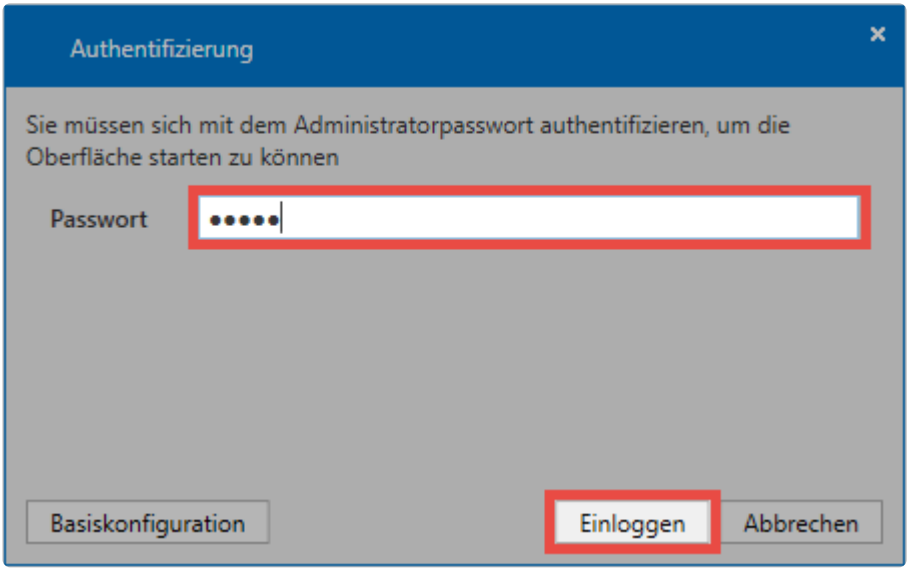


Schritt 4: Setup schließen und (falls gewünscht) direkt den AdminClient öffnen



Authentifizierung

Nach der Installation können Sie sich direkt am AdminClient anmelden.



Das Initial-Passwort zur ersten Anmeldung lautet “admin”. Es wird empfohlen das Passwort direkt nach der Anmeldung zu ändern.

Hier geht´s zurück zum Kapitel Erste Schritte

Installation mit Parametern

Die Installation des Password Safe Servers kann optional auch über die Kommandozeile gestartet

werden. Bei dieser Methode können auch Parameter übergeben werden. Folgend finden Sie die möglichen Parameter.

Aufruf über die Kommandozeile mit Parametern

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

IGNORE_FRAMEWORK_CHECK="1"

Dabei wird bei der Installation nicht überprüft, ob .NET Framework 4.8 installiert ist, sondern führt die Installation direkt aus.

Installation Client

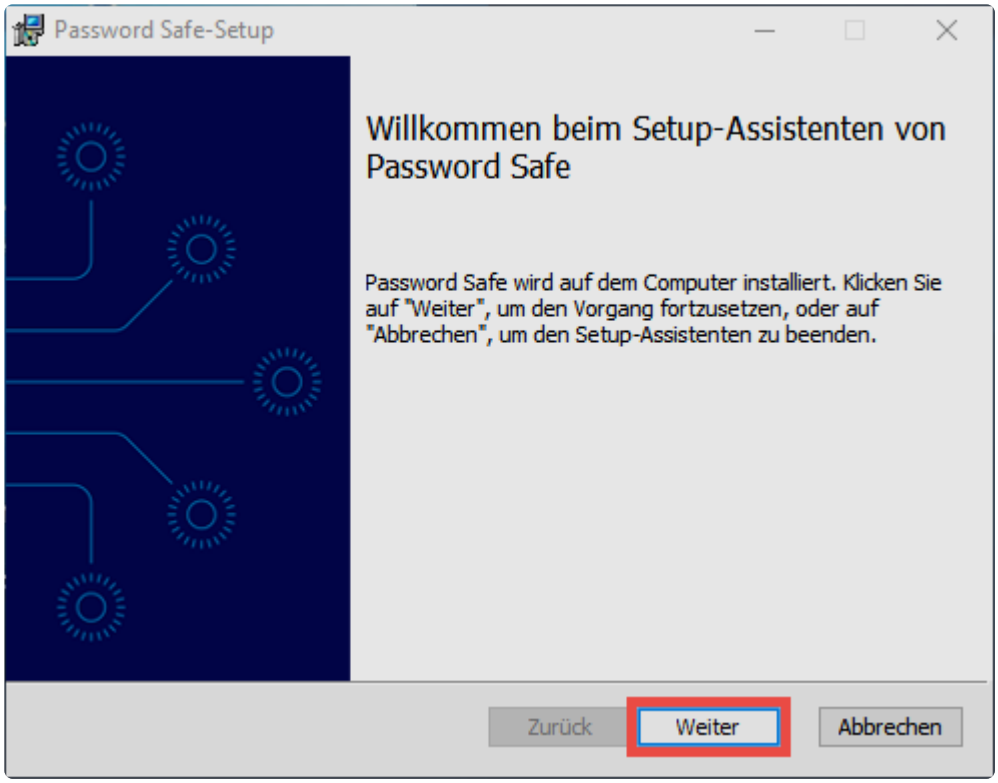
Video-Guide

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

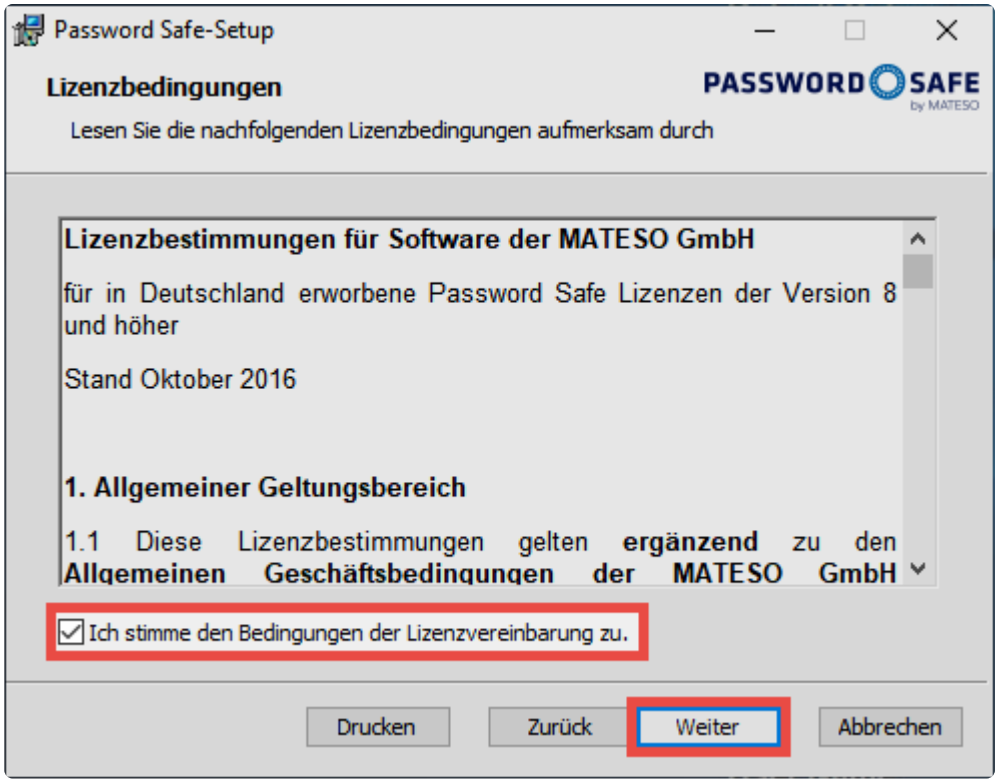
https://www.youtube.com/embed/9Fq_ev7vXhM?rel=0

Anleitung

Die MSI-Installationsdateien finden Sie in unserem Download-Portal. Die Systemanforderungen für den Client findet Sie in dem entsprechenden Kapitel. Die nachfolgende Schritt-für-Schritt-Anleitung leitet Sie durch den Assistenten.



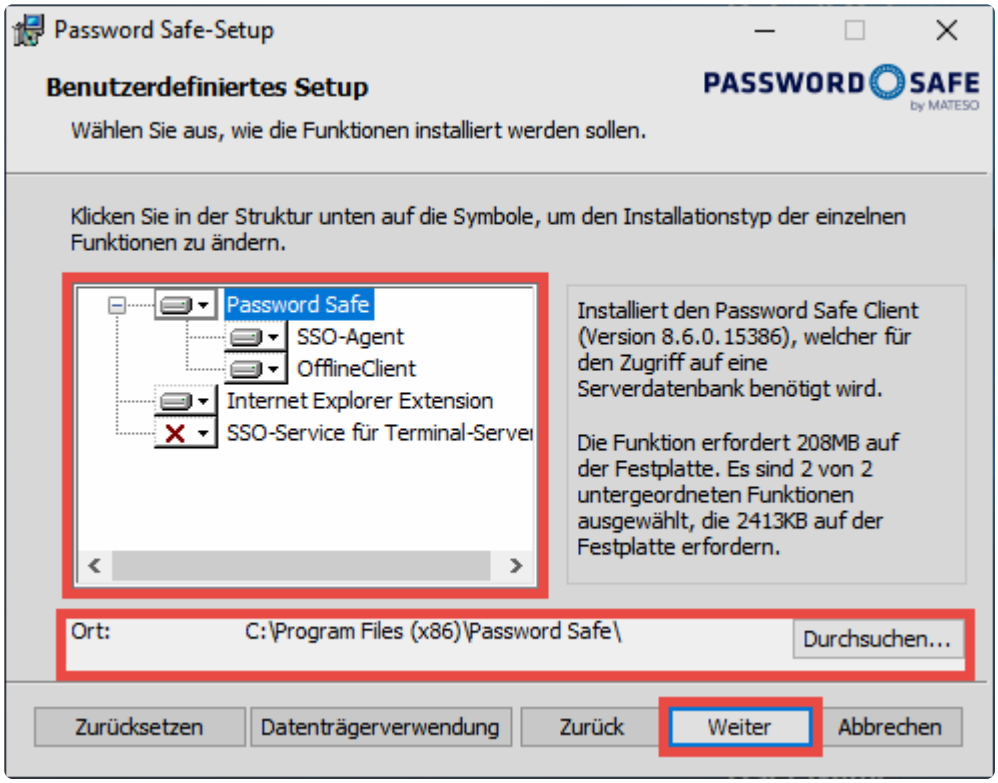
Schritt 1: Lizenzbedingungen lesen und akzeptieren (Druck-Funktion verfügbar)



Schritt 2: Speicherort festlegen. Zudem können weitere Komponenten für die Installation ausgewählt werden.

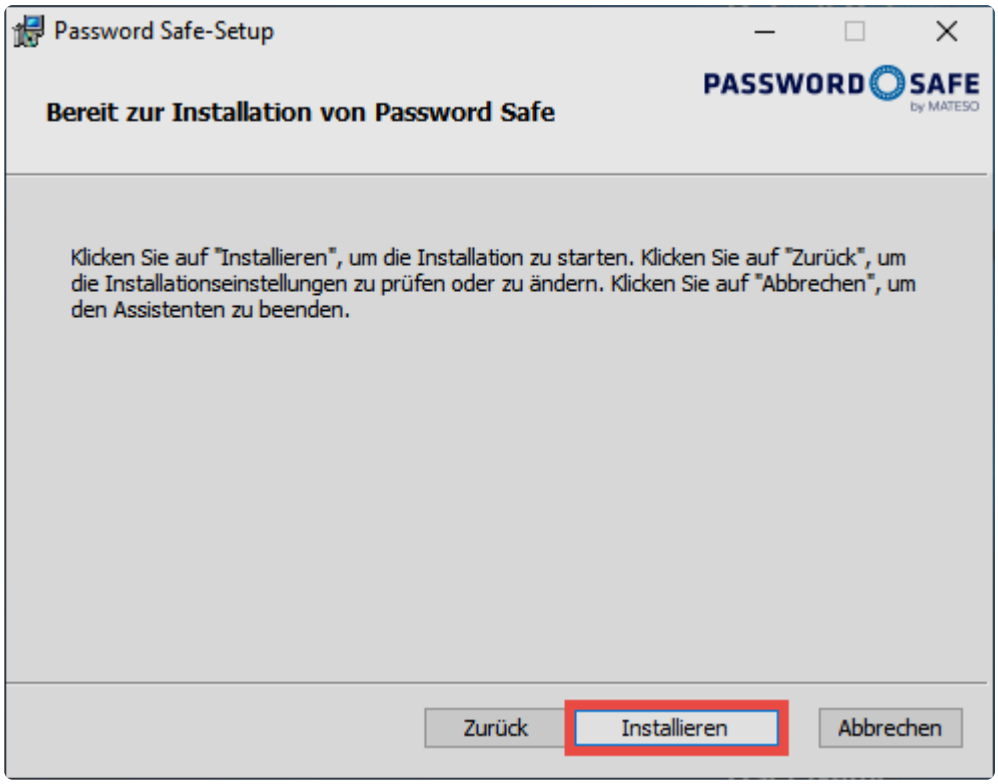
- **Password Safe and Repository 8** installiert den Client.
- **Internet Explorer Extension** wird benötigt, um Zugangsdaten automatisch an den Internet Explorer zu übergeben.

- **SSO-Service für Terminal-Server** ermöglicht die automatische Eintragung im Terminalserver-Betrieb.

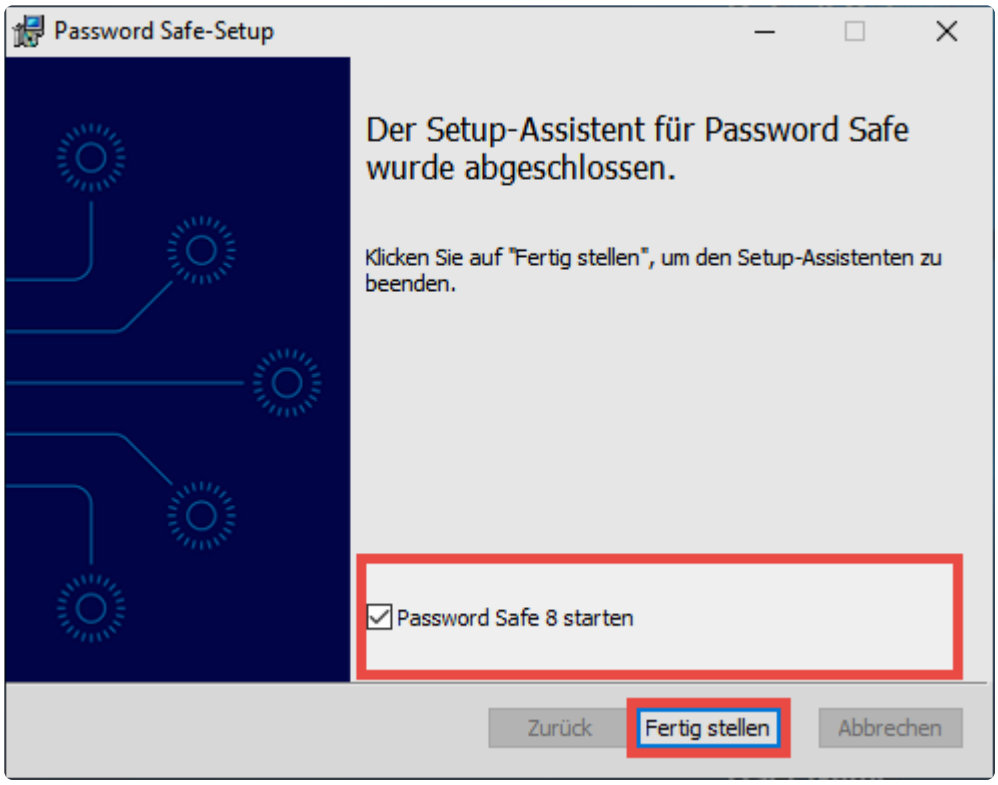


> ! Bitte installieren Sie den SSO-Service nur dann, wenn Sie den Betrieb von Terminal-Servern planen!

Schritt 3: Start der Installation.



Schritt 4: Setup schließen und (falls gewünscht) direkt den Client öffnen.



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-Erweiterungen und der Datenbank dar. Er läuft im Hintergrund und ermöglicht die automatische Anmeldung ohne geöffneten Client.

Einbinden einer Datenbank

Für die Verbindung zu einer Datenbank muss ein Datenbankprofil angelegt werden. Folgende Informationen sind dafür notwendig:

- **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

Es gibt auch die Möglichkeit Datenbankprofile über die Registry zu verteilen. Ein entsprechender Registry-Eintrag gibt die Profile dann vor. Beim nächsten Programmstart werden diese dann in Password Safe übernommen und in der Konfigurationsdatei gespeichert. Die Anbindung der Datenbank kann über folgende Schlüssel erfolgen:

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

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

Der Aufbau der Schlüssel ist wie folgt:

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

Sollte das Profil über die ID **HKEY_LOCAL_MACHINE\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles** verteilt werden, dann werden bei der ersten Anmeldung die zuletzt verwendete Datenbank sowie der zuletzt angemeldete Benutzer unter folgender ID hinterlegt: **HKEY_CURRENT_USER\SOFTWARE\MATESO\Password Safe and Repository 8\DatabaseProfiles**

Datenbankprofil über Install.cmd verteilen

Alternativ können Sie das Datenbankprofil auch durch ein Ausführen des folgenden Skripts in einer Install.cmd bereitstellen.

Skript:

```
@Echo off
echo A Script to set a Registry value using Windows Intune
REM registry key
set key="HKCU\Software\MATESO\Password Safe and Repository 8\DatabaseProfiles\DATENBANK
reg add %key% /f
reg add %key% /v DatabaseName /t REG_SZ /d DATENBANKNAME /f
reg add %key% /v HostIP /t REG_SZ /d HostIP /f
if errorlevel 1 (
echo Error installing reg key
exit /b 1
) else (
echo Installed regkey
)
exit /b 0
```

Dieses Script lässt sich per C:\Windows\System32\iexpress.exe in eine EXE-Datei packen und in einem beliebigen MDM-System ausbringen

Wenn der entsprechende Registry-Eintrag gesetzt ist und kein Datenbank-Profil dazu existiert, wird das Profil beim nächsten Start angelegt. Bitte beachten Sie, dass sich auf diese Weise erstellte Profile am Client weder bearbeiten noch löschen lassen.

Hier geht´s zurück zum Kapitel Erste Schritte

Installation mit Parametern

Die Installation des Password Safe Clients kann optional auch über die Kommandozeile gestartet werden. Bei dieser Methode können auch Parameter übergeben werden. Diese sind miteinander kombinierbar. In diesem Fall werden die einzelnen Parameter durch ein Leerzeichen voneinander getrennt. Folgend finden Sie die möglichen Parameter.

Aufruf über die Kommandozeile mit Parametern

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

Parameter

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. Er 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. Er kann jedoch vom Benutzer wieder gesetzt werden.

IGNORE_TS_SERVICES=“1”

Deaktiviert die Installation des Terminalserver-Dienstes, egal, auf welchem System die Installation erfolgt.

IGNORE_FRAMEWORK_CHECK=“1”

Dabei wird bei der Installation nicht überprüft, ob .NET Framework 4.8 installiert ist, sondern führt die Installation direkt aus.

Installation WebClient

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

Vorbereitungen zur Installation

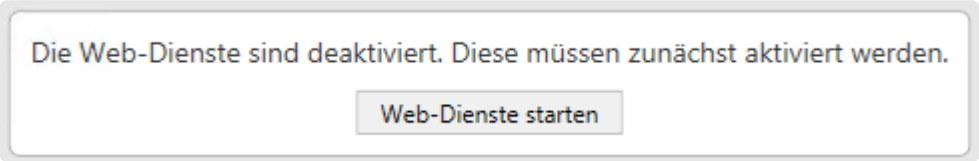
Um die Installation des WebClients ohne weitere Komplikationen durchführen zu können, treffen Sie bitte folgende Vorbereitungen:

Systemanforderungen

Stellen Sie sicher, dass alle **Systemanforderungen** erfüllt sind.

Webdienst

Sarten Sie beim ersten Aufrufen des Moduls **WebClient** im **AdminClient** den Webdienst.



Dadurch wird der Password Safe Server neu gestartet. Anschließend wird im Modul **WebClient** die Konfigurationsoberfläche dargestellt.

SSL-Zertifikat

Beim Start der Webdienste wird das in der Grundkonfiguration selektierte Zertifikat für die Verwendung in den Webdiensten konfiguriert und an den Port 11016 angebunden. Dabei handelt es sich um das Verbindungszertifikat zur Kommunikation zwischen Webserver und Password Safe Server.

> ✻ Im Hintergrund wird das Zertifikat über **netsh http add sslcert** passend zum konfigurierten Port (11016 TCP) ins Betriebssystem eingebunden. Beim Deinstallieren wird mit **netsh http delete sslcert** gearbeitet.

Firewall

Der Port 11016 TCP muss durchgehend freigeschaltet sein.

Datenbanken

Alle **Datenbanken**, welche im **WebClient** verwendet werden sollen, müssen hierfür auch freigegeben werden (mit Doppelklick auf die entsprechende Datenbank). Nun können Sie die Option **Zugriff über WebClient aktivieren** auswählen.

Installation

Den WebClient erzeugen Sie im AdminClient. Er wird in einem ZIP-Archiv bereitgestellt. Je nach verwendetem Webserver wird das ZIP-Archiv dementsprechend erstellt. Auch die Installation unterscheidet sich. Unabhängig vom verwendeten Webserver, geben Sie zunächst folgende Infos an:

Zieldatei
Benennen Sie hier den Ordner, in welchem das ZIP-Archiv mit dem WebClient abgelegt werden soll.

✻ Installieren Sie den WebClient auf dem IIS, wird im ZIP-Archiv eine Datei mit dem Namen config.bat erzeugt. Diese übernimmt das Einbinden am Webserver.

! Hier darf **nicht das Installationsverzeichnis** des AdminClients verwendet werden.

Server IP
Zur Information wird hier die IP-Adresse des Password Safe Servers angezeigt.

✻ Bitte prüfen Sie, ob die IP-Adresse korrekt ist. Sonst kann keine Verbindung zum WebClient hergestellt werden. Sollte die IP-Adresse nicht passen, müssen SIe diese in der Grundkonfiguration des AdminClients ändern.
Webserver-Hostadresse
Geben Sie hier die IP-Adresse, bzw. den Hostname des Webservers an.

Port
Hinterlegen Sie hier den Port zum Ansprechen des WebClients.

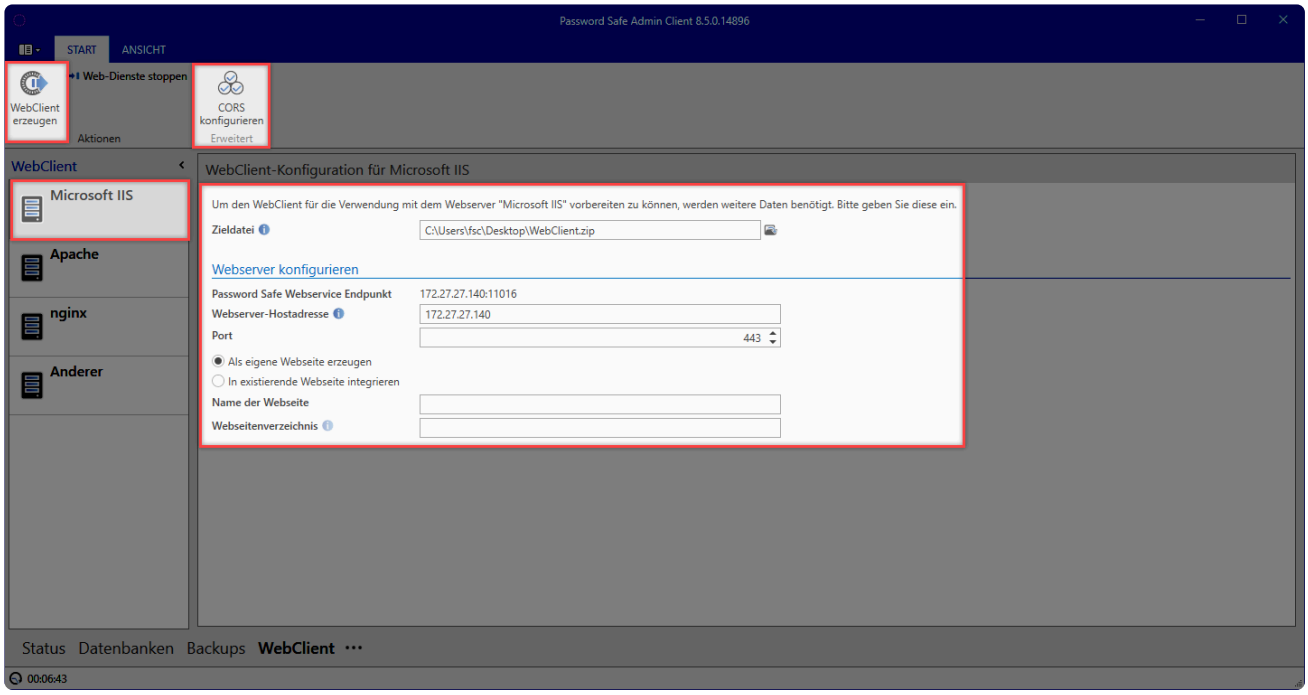
Nachfolgend werden alle weiteren Schritte, bzw. die nötigen Angaben pro Webserver, erläutert.

Microsoft IIS

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

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

In existierende Website integrieren
Setzt eine bestehende Website voraus. Sie müssen also also vorab auf dem IIS eine entsprechende Website erzeugen. Im AdminClient geben Sie dann den **Name der Website** an. Unter **Websitenverzeichnis** hinterlegen Sie, in welchem Ordner der WebClient betrieben werden soll. Das Format hierfür ist “/webclient”



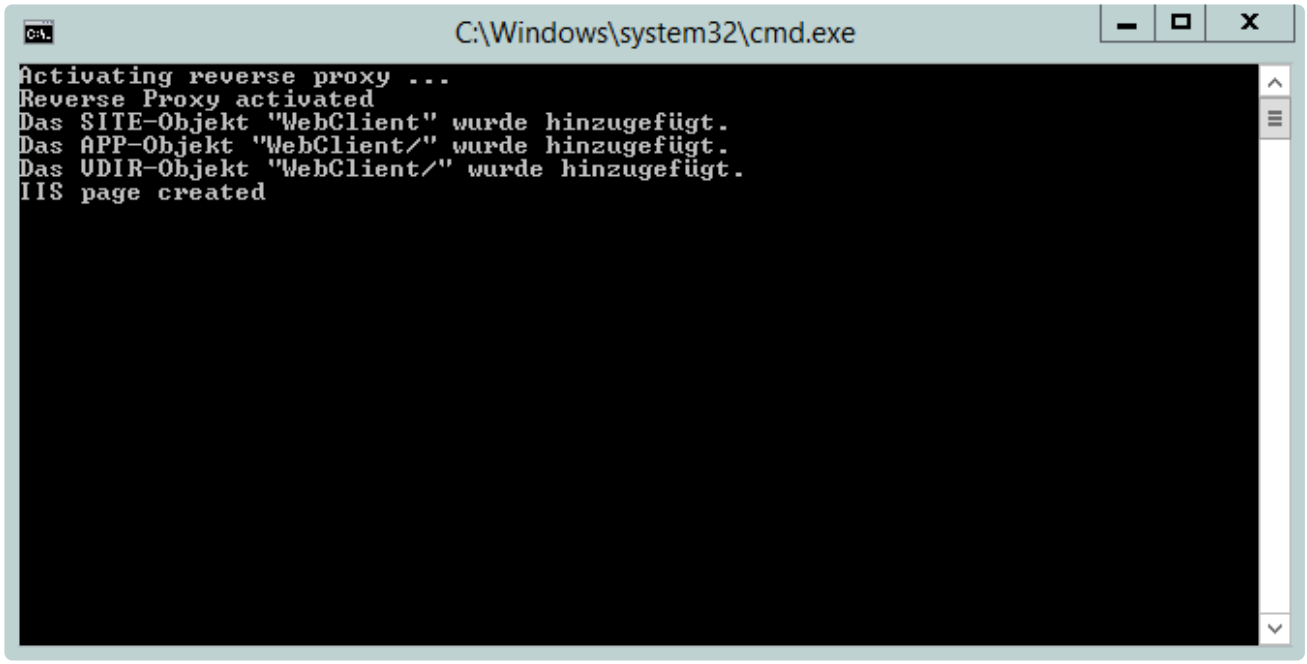
Sobald alle Einstellungen gesetzt sind, können Sie den WebClient über die entsprechende Schaltfläche in der Ribbon erzeugen. Wurde das ZIP-Archiv mit dem WebClient erzeugt, kopieren Sie es auf den Webserver in das vorher festgelegte Verzeichnis (standardmäßig C:\inetpub\wwwroot) und entpacken es dann dort in ein neues Verzeichnis.

Config.bat

Im neu erstellten Verzeichnis **WebClient** finden Sie die Datei **config.bat**. Führen Sie diese als Administrator aus. Dadurch 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 muss. In diesem Fall folgen Sie einfach dem Assistenten. Dieser wird automatisch geöffnet. Außerdem muss das **WebSocket-Protokoll** installiert und die **config.bat** erneut ausgeführt werden.

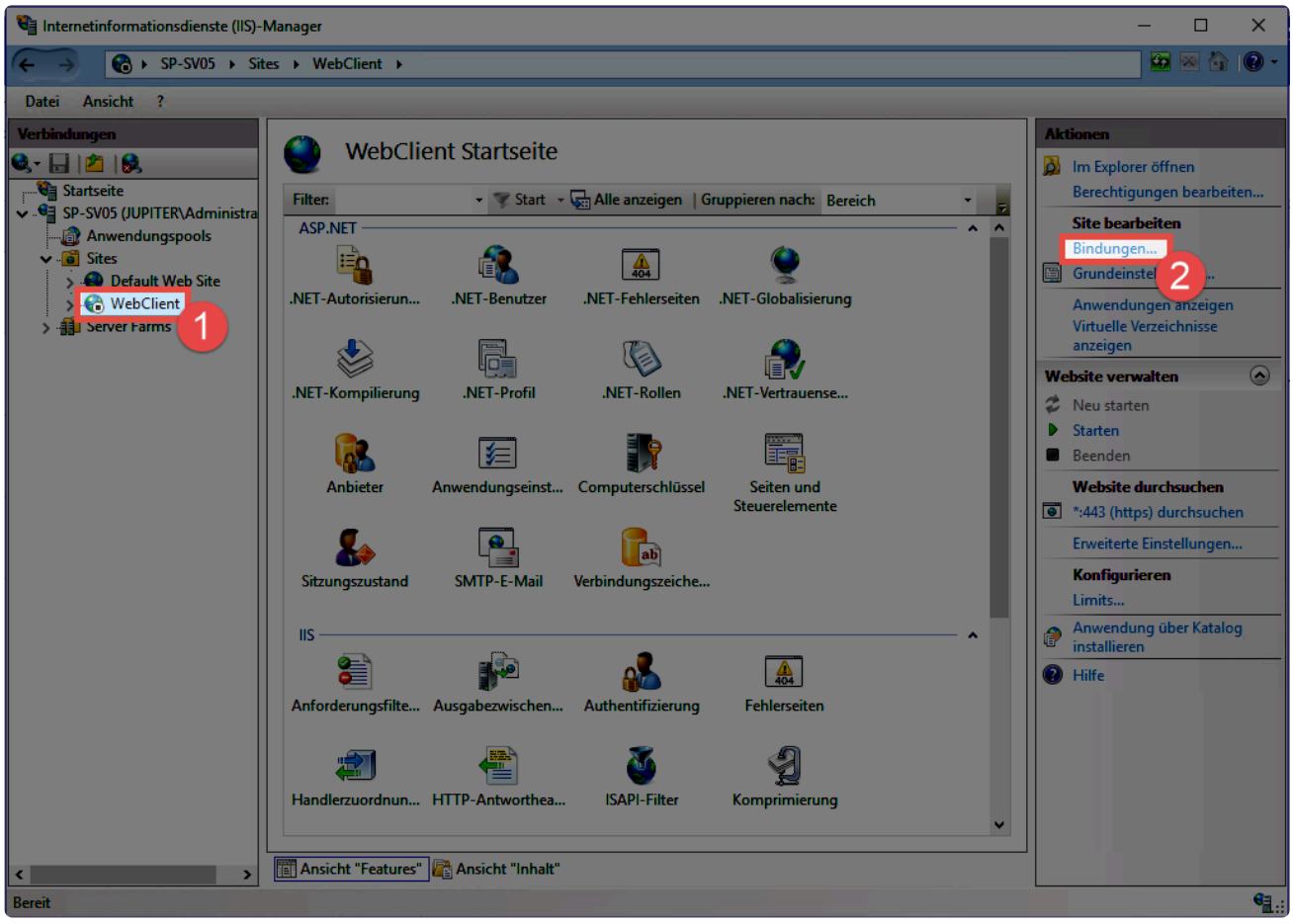
Haben Sie die Seite korrekt eingebunden, wird dies durch den Hinweis **IIS page created** entsprechend dargestellt.



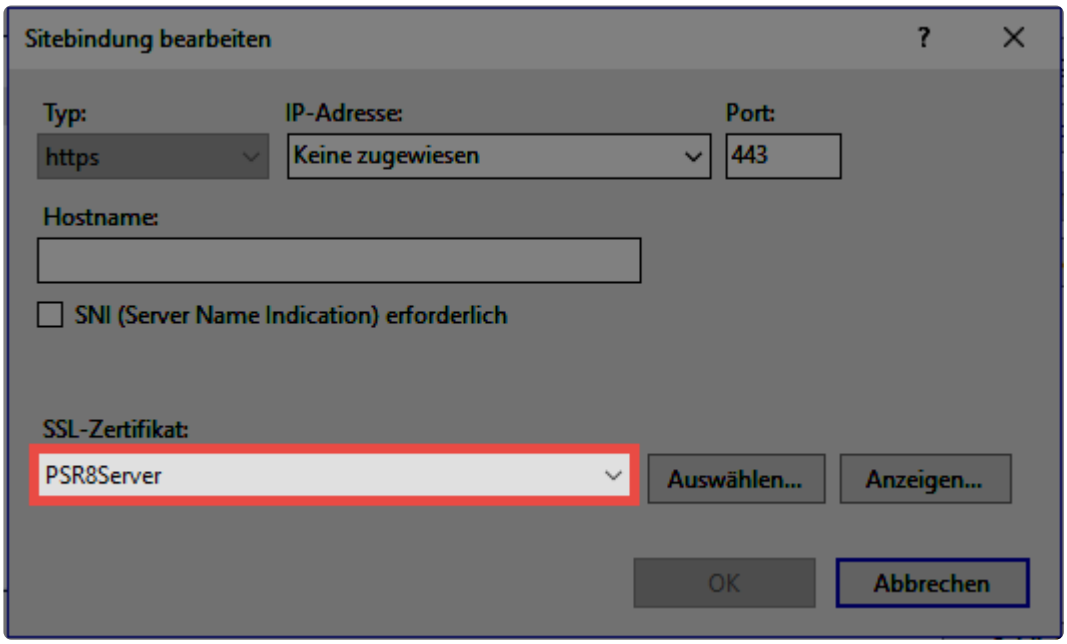
> ! Nach erfolgter Installation sollten Sie die **config.bat** unbedingt löschen! Ebenso sollte die **config.bat** nicht für ein Update verwendet werden!

Zertifikat

Abschließend hinterlegen Sie das Zertifikat. Hierfür selektieren Sie am IIS die erstellte Website. Ganz rechts öffnen Sie dann die **Bindungen**.



Nun öffnen Sie den Eintrag **https** zum Bearbeiten. Hier wählen Sie dann das **SSL-Zertifikat** aus.



Weiterhin muss das Password Safe Zertifikat am Password Safe Server exportiert und am IIS unter **lokaler Computer > vertrauenswürdige Stammzertifizierungsstellen -> Zertifikate** importiert werden. Weitere Infos finden Sie im Kapitel “Zertifikate Zertifikate.

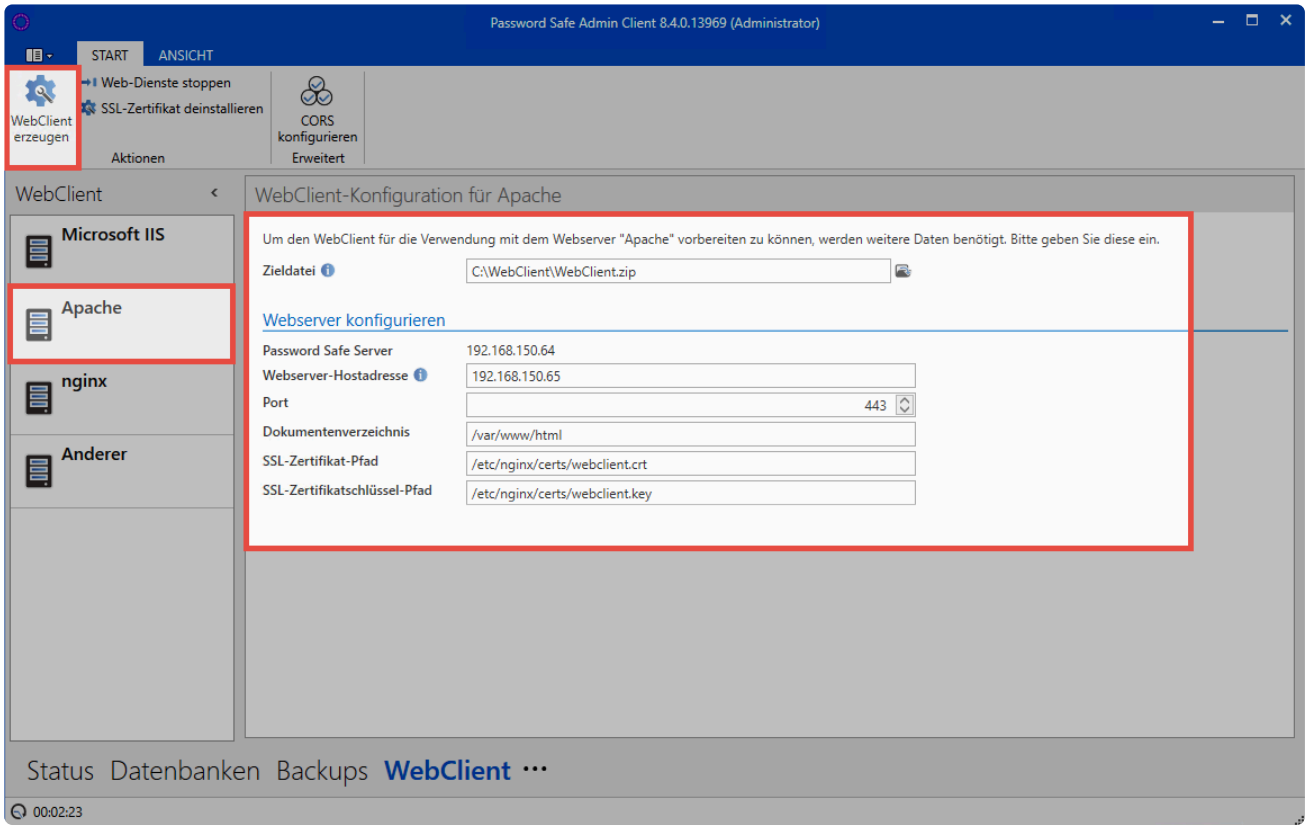
Apache

Zum Einbinden des WebClients auf einem Apache Server setzen Sie zunächst alle relevanten Einstellungen:

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

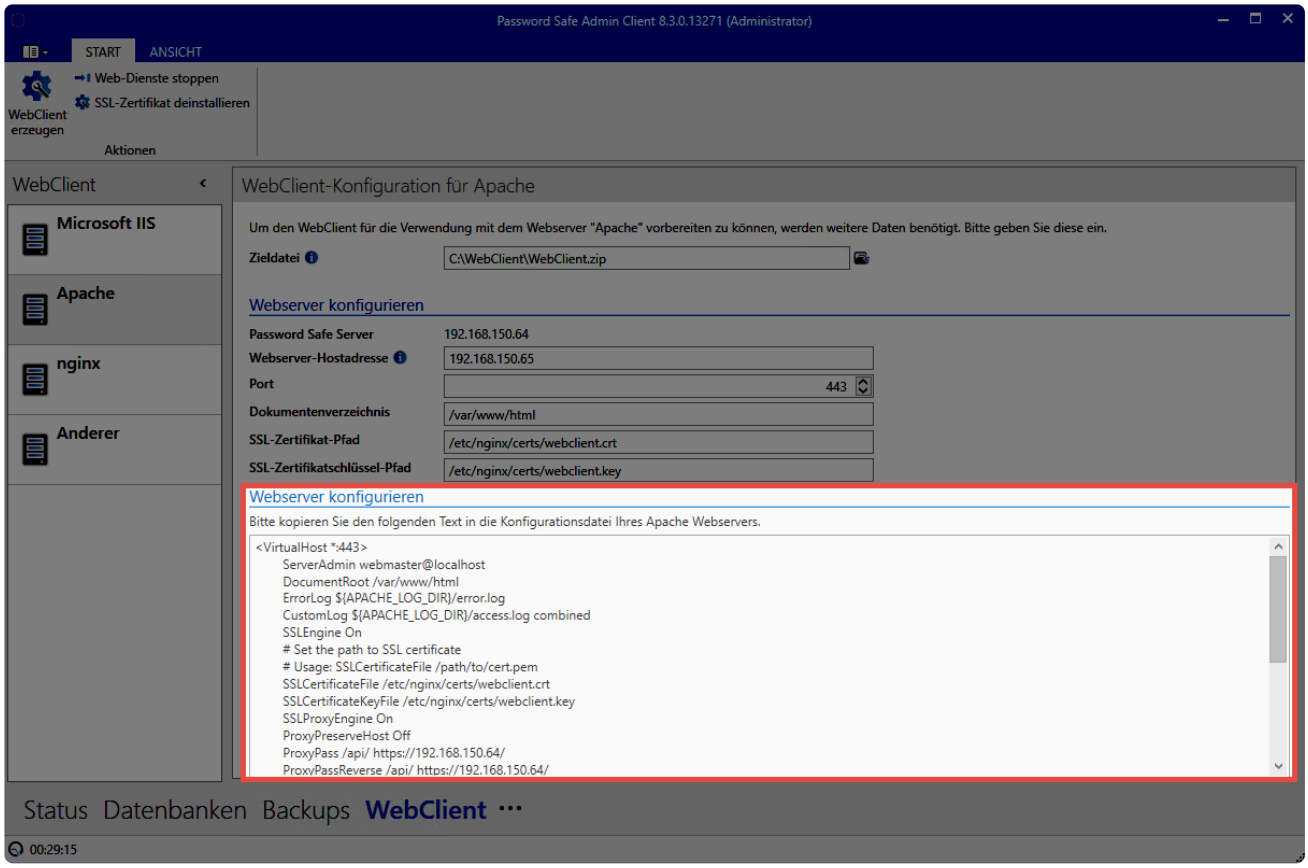
SSL-Zertifikat-Pfad
Hier benennen Sie das Verzeichnis in welchem das Zertifikat abgelegt wird.

SSL-Zertifikatsschlüssel-Pfad
Geben Sie hier an, wo der Zertifikatsschlüssel liegt.



Nachdem alle Einstellungen übernommen sind, erzeugen Sie den WebClient über den Button in der Ribbon. Anschließend wird der Ordner, in dem die ZIP-Datei liegt, automatisch geöffnet. Entpacken Sie nun das Archiv und kopieren den Inhalt ins Dokumentenverzeichnis des Webservers.

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



Markieren Sie die Konfiguration über STRG+A und kopieren diese. Sie 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. Starten Sie abschließend den Apache über **systemctl reload apache** neu.

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

nginx

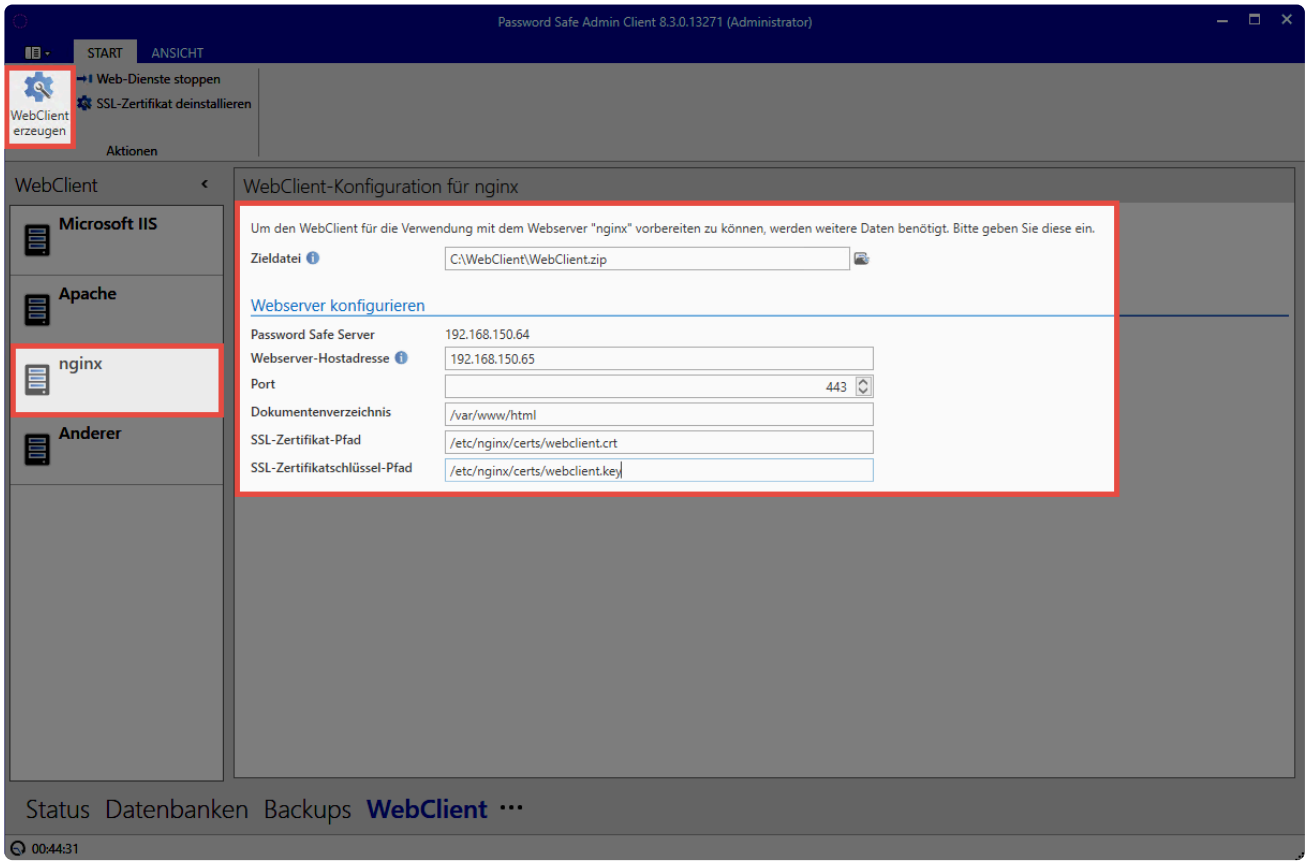
Zum Einbinden des WebClients auf einem nginx Server setzen Sie zunächst alle relevanten Einstellungen:

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

SSL-Zertifikat-Pfad
Benennen Sie hier das Verzeichnis in welchem das Zertifikat abgelegt wird.

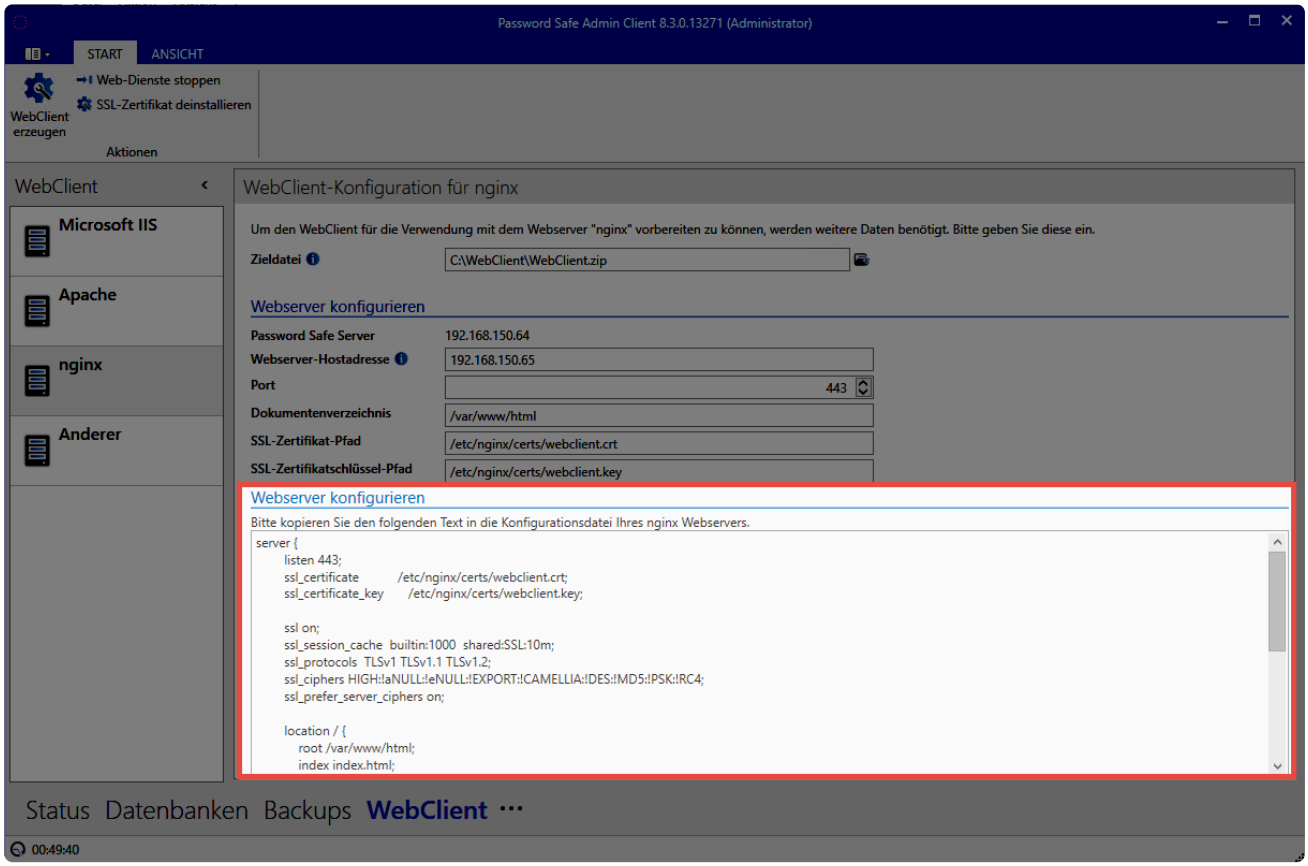
Der Standardpfad lautet hierbei **/etc/nginx/certs/webclient.crt**

SSL-Zertifikatsschlüssel-Pfad
Schlussendlich hinterlegen Sie hier, wo der Zertifikatsschlüssel liegt.
Standardmäßig ist das **/etc/nginx/certs/webclient.key**



Wenn alle Einstellungen gesetzt sind, können Sie den WebClient über den Button in der Ribbon erzeugen. Es öffnet sich dann direkt der Ordner, in dem die ZIP-Datei liegt. Nun entpacken Sie das Archiv und kopieren dessen Inhalt ins Dokumentenverzeichnis auf dem Webserver.

Zusammen mit der ZIP-Datei wurde auch die Konfiguration für den nginx Server erzeugt. Diese können Sie direkt am AdminClient einsehen.



Abschließend binden Sie die Konfiguration noch am nginx ein. Sie kann hierfür direkt am AdminClient kopiert werden.

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

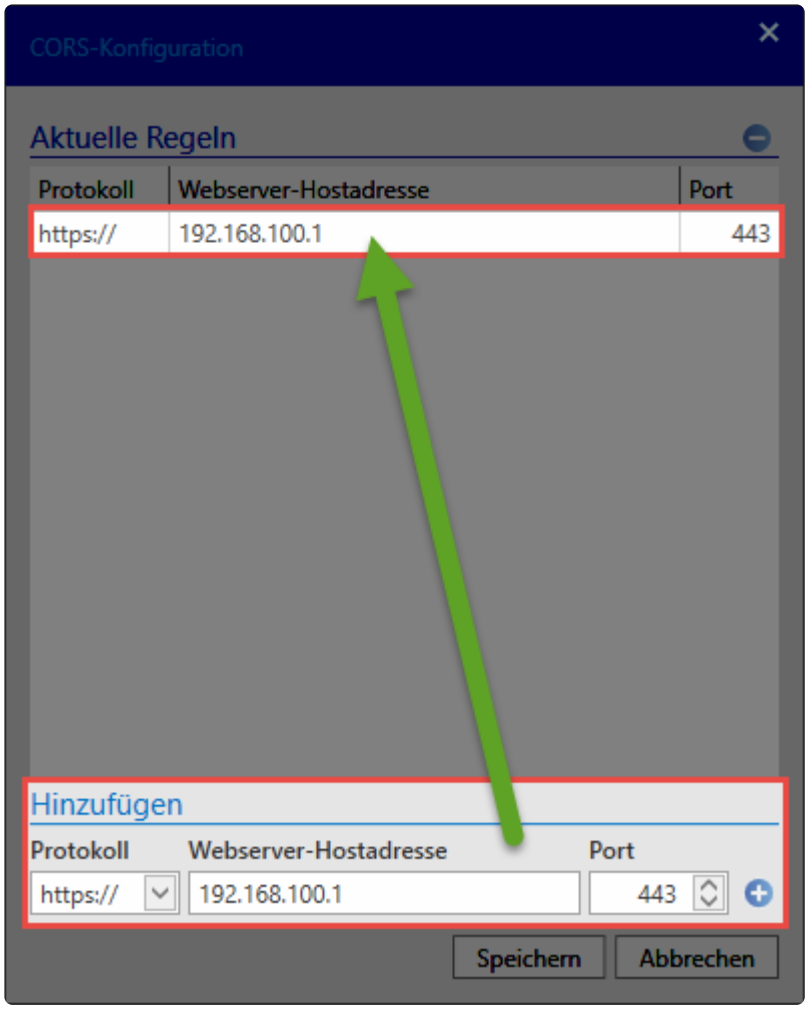
Standardkonfiguration
Zunächst wird die Datei **/etc/nginx/sites-available/default** geöffnet. Beispielsweise über “nano”. Suchen Sie nun den Eintrag `server { }`. Fügen Sie danach die Konfiguration des AdminClient ein. Abschließend starten Sie den Webserver über den Befehl **systemctl restart nginx** neu.

Der WebClient ist nun betriebsbereit und kann direkt aufgerufen werden.

CORS Konfiguration

In der Ribbon finden Sie eine Schaltfläche für die sogenannte **CORS-Konfiguration**. Diese müssen Sie zwingend ausführen, bevor der WebClient verwendet werden kann. Hierdurch wird eine Liste von erlaubten CORS Domains hinterlegt. Gegen diese können dann Requests über den WebClient abgeglichen werden. Nur falls der Origin-Header eines Requests in den erlaubten Domains vorhanden ist, wird der Request erfolgreich durchgeführt.

Zum Hinzufügen einer Domain tragen Sie diese einfach unten im Dialog ein. Über einen Klick auf übernehmen Sie dann den Eintrag nach oben in die Liste.



In der Regel reicht es aus, die IP zu hinterlegen, die auch als **Webserver Hostadresse** hinterlegt wurde.

Aufruf des WebClients

Wie Sie den WebClient aufrufen, 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**

Weiterleitung

Mit den Konfigurationen der Webserver IIS, Apache und nginx wird auch die Weiterleitung von http auf https erzeugt.

Beim IIS wird die Weiterleitungsregel direkt in die Webserverkonfiguration geschrieben. Für die Weiterleitung muss beim IIS zusätzlich noch im Binding der Port 80 konfiguriert werden.

Für die Webserver apache und nginix wird eine entsprechende Konfiguration erzeugt, die manuell in die korrekte Konfigurationsdatei hinzugefügt werden muss.

Damit Sie die Weiterleitung nutzen können, müssen Sie bei den Webservern apache und nginx darauf achten, dass kein weiterer Host mehr auf Port 80 hört.

Installation Browser-Erweiterungen

Die Browser-Erweiterungen bieten Ihnen die Möglichkeit, Ihre Anmeldedaten in die Eingabemasken der entsprechenden Webseiten eintragen zu lassen. Aktuell sind Browser-Erweiterungen für den **Edge**, **Google Chrome**, **Safari** sowie **Mozilla Firefox** verfügbar.

Da sich die Installation je nach Browser unterscheidet, finden Sie die Installation der browserspezifischen Erweiterung in den entsprechenden Kapiteln:

- Chrome
- Mozilla Firefox
- Edge
- Safari

Im Rahmen der Installation wird man gebeten, folgende Berechtigungen zuzulassen:

- Alle Ihre Daten auf von Ihnen besuchten Webseiten lesen und Ändern
  => zum Erkennen der Felder für die Zugangsdaten
- Benachrichtigungen einblenden
  => Zum Anzeigen von Benachrichtigungen, ob beispielsweise neue Zugangsdaten gespeichert werden sollen
- Datenschutzeinstellungen ändern
  => zum Deaktivieren des browser-internen Password-Managers

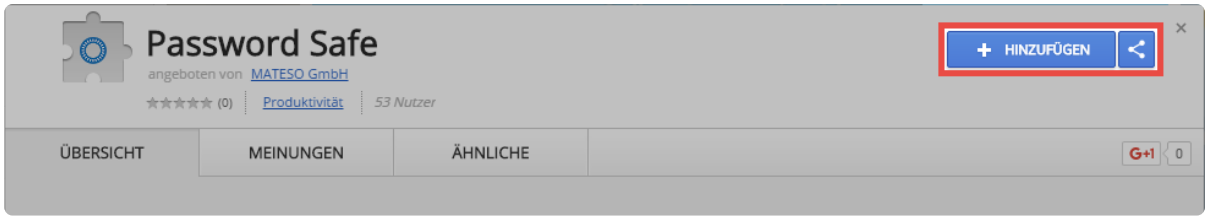
Installation Chrome

Google Chrome

Die Installation des Google Chrome Erweiterung erfolgt direkt über den Google Store. In diesen gelangen Sie über folgenden Link: **Password Safe Erweiterung für Google Chrome**

Alternativ können Sie auch über den SSO Agent den Google Store aufrufen. Hierfür öffnen Sie – über einen Rechtsklick auf das Icon – das Kontextmenü. Nach einem Klick auf **Erweiterung hinzufügen** können Sie das Google Chrome Erweiterung auswählen. Sie werden dann direkt in den Google Store weiter geleitet.

Starten Sie die Installation über **Hinzufügen**.

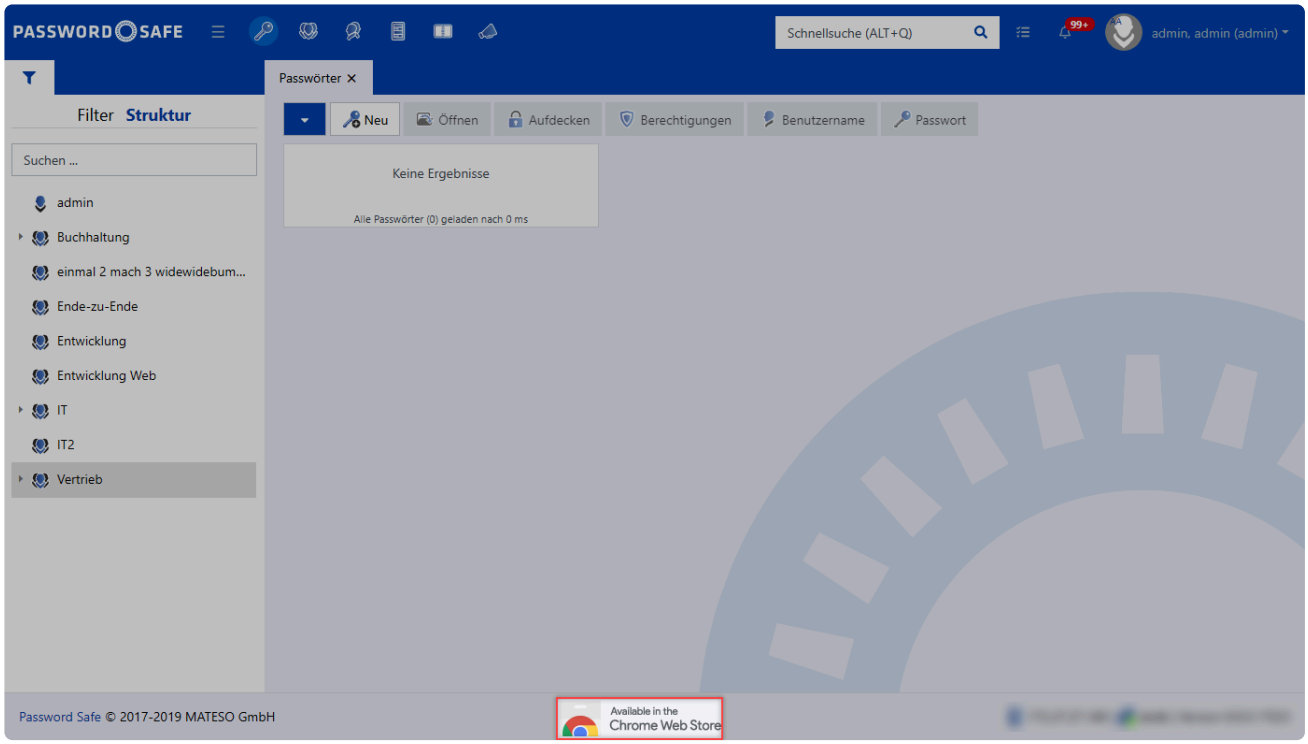


Die Browser-Erweiterungen wird nun installiert. Im Browser wird das Icon hinzugefügt.

Installation des Browser-Erweiterungen über den WebClient

Sie können die Erweiterung auch über den WebClient installieren.

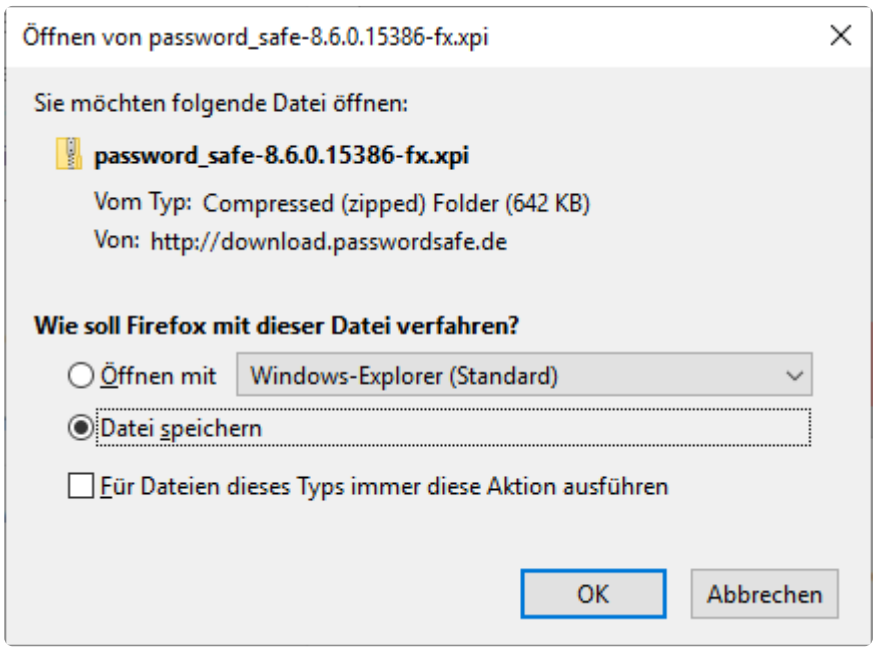
Dafür klicken Sie im Webclient auf das Icon, welches sich unten in der Mitte der Seite befindet.


PASSWORD SAFE
Schnellsuche (ALT+Q)
admin, admin (admin)
Passwörter
Filter Struktur
Suchen ...
admin
Buchhaltung
einmal 2 mach 3 widewidebum...
Ende-zu-Ende
Entwicklung
Entwicklung Web
IT
IT2
Vertrieb
Neu
Öffnen
Aufdecken
Berechtigungen
Benutzername
Passwort
Keine Ergebnisse
Alle Passwörter (0) geladen nach 0 ms
Password Safe © 2017-2019 MATESO GmbH
Available in the Chrome Web Store

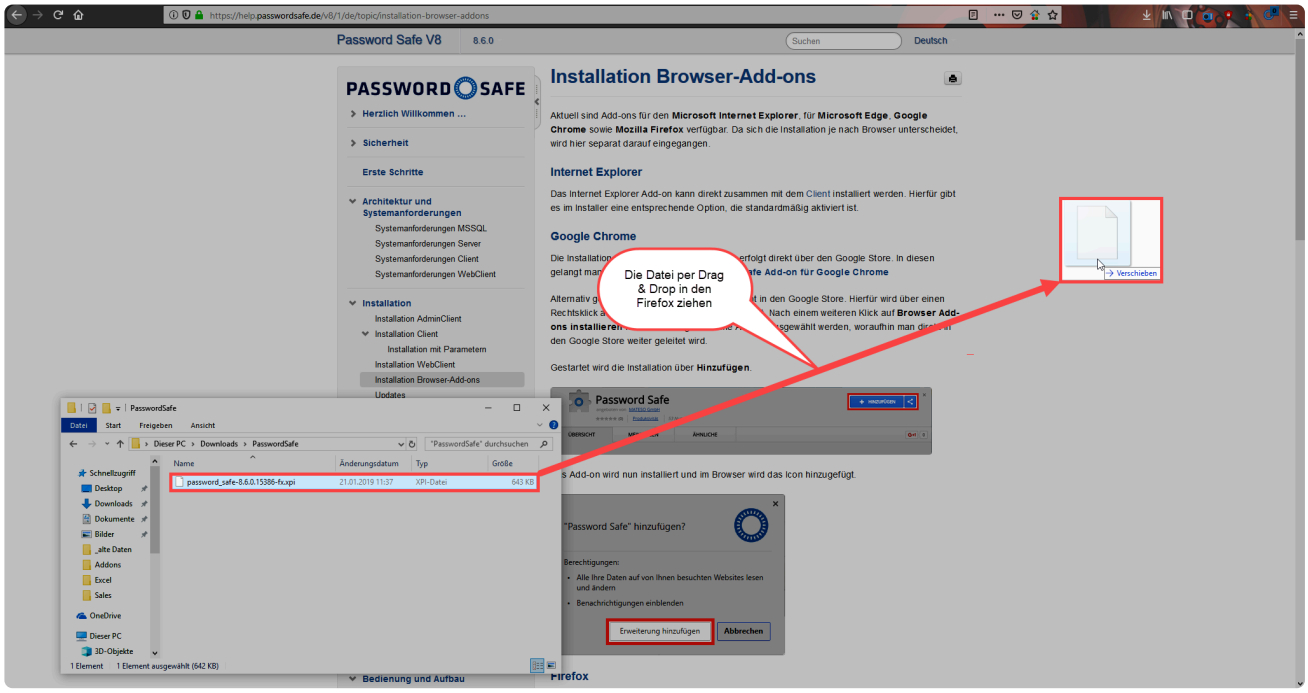
Installation Mozilla Firefox

Firefox

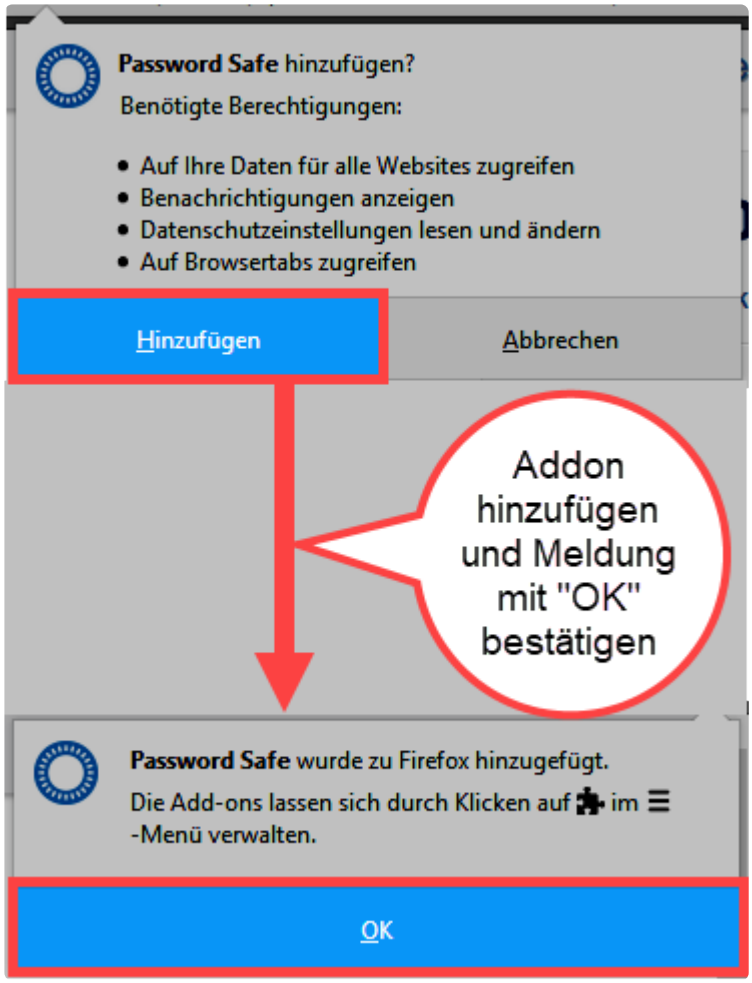
Die Firefox Erweiterung können Sie unter folgendem Link herunterladen:
[Password Safe Browser-Erweiterung für Firefox]



Nach dem Download ziehen Sie die Erweiterung einfach per Drag-and-Drop in den Browser.

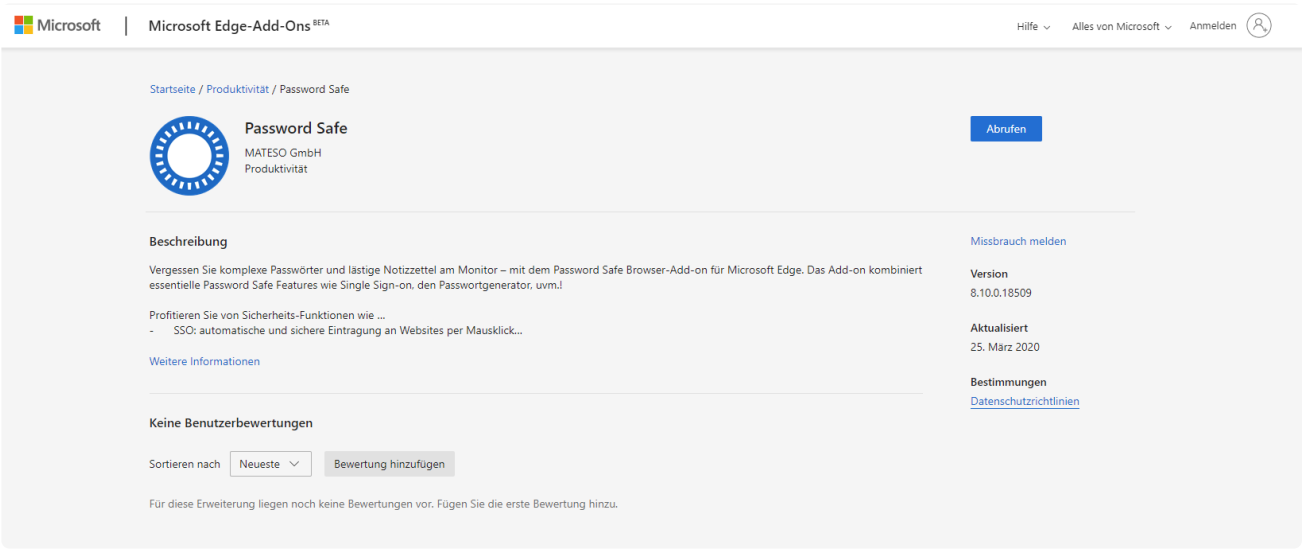


Nach Bestätigung einer Sicherheitsfrage wird dieses installiert und in der Menüleiste ein Icon erstellt.


Password Safe hinzufügen?
Benötigte Berechtigungen:
Auf Ihre Daten für alle Websites zugreifen
Benachrichtigungen anzeigen
Datenschutzeinstellungen lesen und ändern
Auf Browsertabs zugreifen
Hinzufügen
Abbrechen
Addon hinzufügen und Meldung mit "OK" bestätigen
Password Safe wurde zu Firefox hinzugefügt.
Die Add-ons lassen sich durch Klicken auf im ☰ -Menü verwalten.
OK

Installation Edge

Die Edge Browser-Erweiterung können Sie unter folgendem Link herunter laden: **Edge Erweiterung**
Sie werden dann direkt auf den Microsoft Store weitergeleitet.



Dort bekommen Sie dann die Möglichkeit die Erweiterung für den Edge hinzuzufügen.

Installation Safari

Safari

Die Safari Browser-Erweiterung können Sie unter folgendem Link herunterladen: **Safari Browser-Erweiterung**
Zur Installation klicken Sie doppelt auf die heruntergeladene Datei. Es öffnet sich ein Fenster, in welchen dann nur noch das Password Safe Logo per Drag and Drop auf die Anwendungen gezogen werden muss.

Umzug des Servers

Vorbereitungen

Damit der Umzug problemlos verläuft, Sollten Sie einige Vorbereitungen treffen.

1. Installation des SQL-Servers

Befinden sich SQL-Server und Anwendungsserver auf der gleichen Maschine, installieren Sie zunächst den SQL-Server auf der neuen Maschine. Beachten Sie hierbei bitte die **Systemvoraussetzungen**.

2. Installation des Servers

Als nächstes installieren Sie den Password Safe Server (siehe **Systemvoraussetzungen**). Die Installation selbst wird unter **Installation AdminClient** beschrieben.

3. Grundkonfiguration

Nach der Installation des Servers erfolgt die **Grundkonfiguration**. Dadurch wird auf dem SQL-Server eine neue Konfigurationsdatenbank erzeugt. Sollte der alte SQL-Server bestehen bleiben, müssen Sie für die Konfigurationsdatenbank einen neuen Name vergeben.

4. Deaktivieren des alten Servers

Deaktivieren Sie zuerst die Lizenz, bevor sie Sie auf dem neuen Server aktivieren können (siehe die Option unter den **Lizenzeinstellungen**). Nun stoppen Sie den Serverdienst, damit in der Datenbank nichts mehr geändert werden kann.

Sichern der Daten

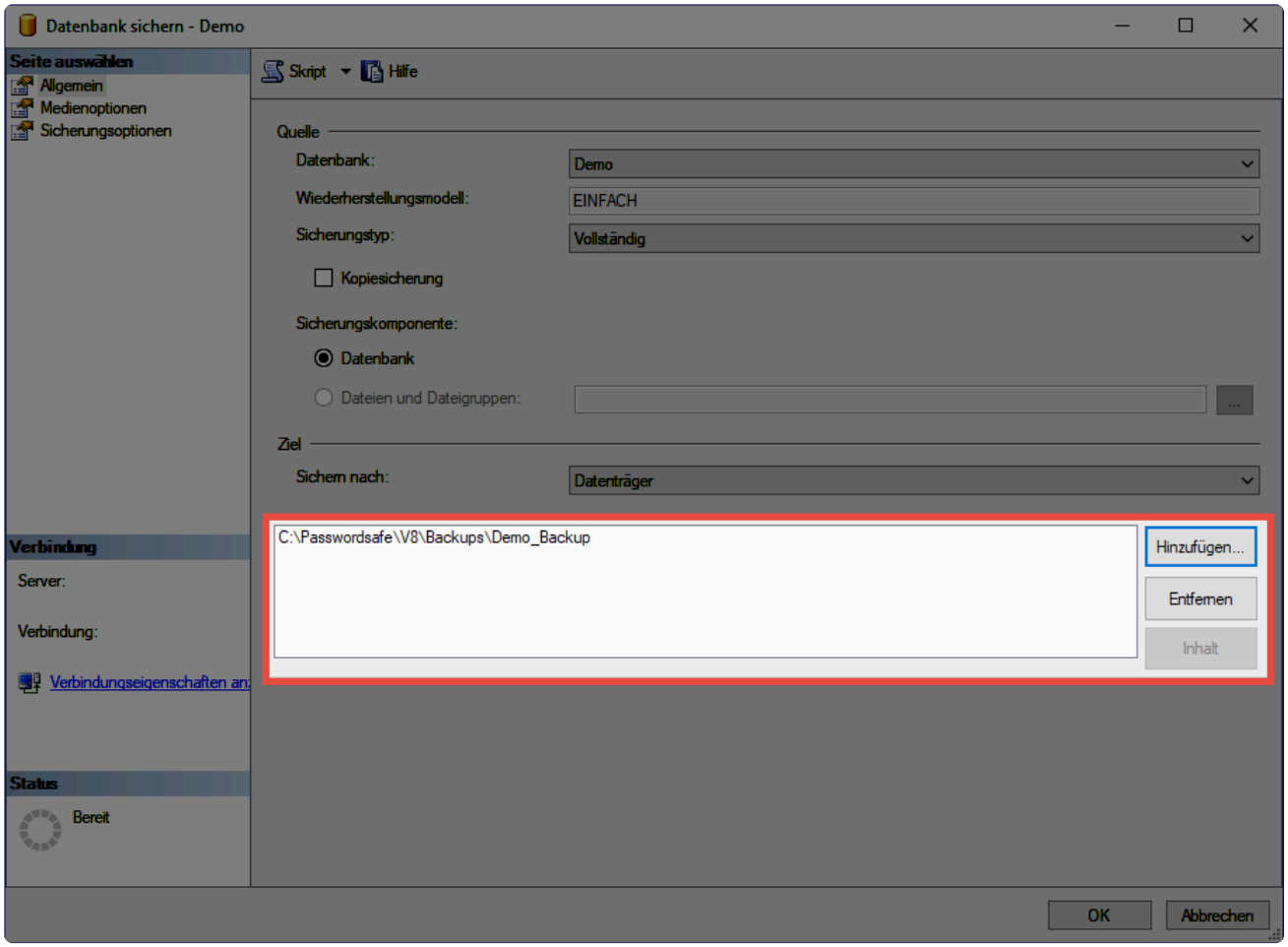
Nach diesen Vorbereitungen können Sie die Daten vom alten Server sichern.

1. Backup des Systems

Erstellen Sie ein Backup, falls Sie eine virtuelle Maschine einsetzen. Bei Problemen kann so der alte Stand des Servers wiedererlangt werden.

2. Backup der Datenbank

Um die Daten auf den neuen Server zu übertragen, erstellen Sie ein Backup der Datenbank. Obwohl das auch über den AdminClient möglich ist, empfehlen wir das Backup auf SQL-Ebene: mit Rechtsklick auf die Datenbank, dann **Tasks** und **Sichern**. Im folgenden Fenster wird der gewünschte Zielordner ausgewählt.



3. Backup der Server-Zertifikate

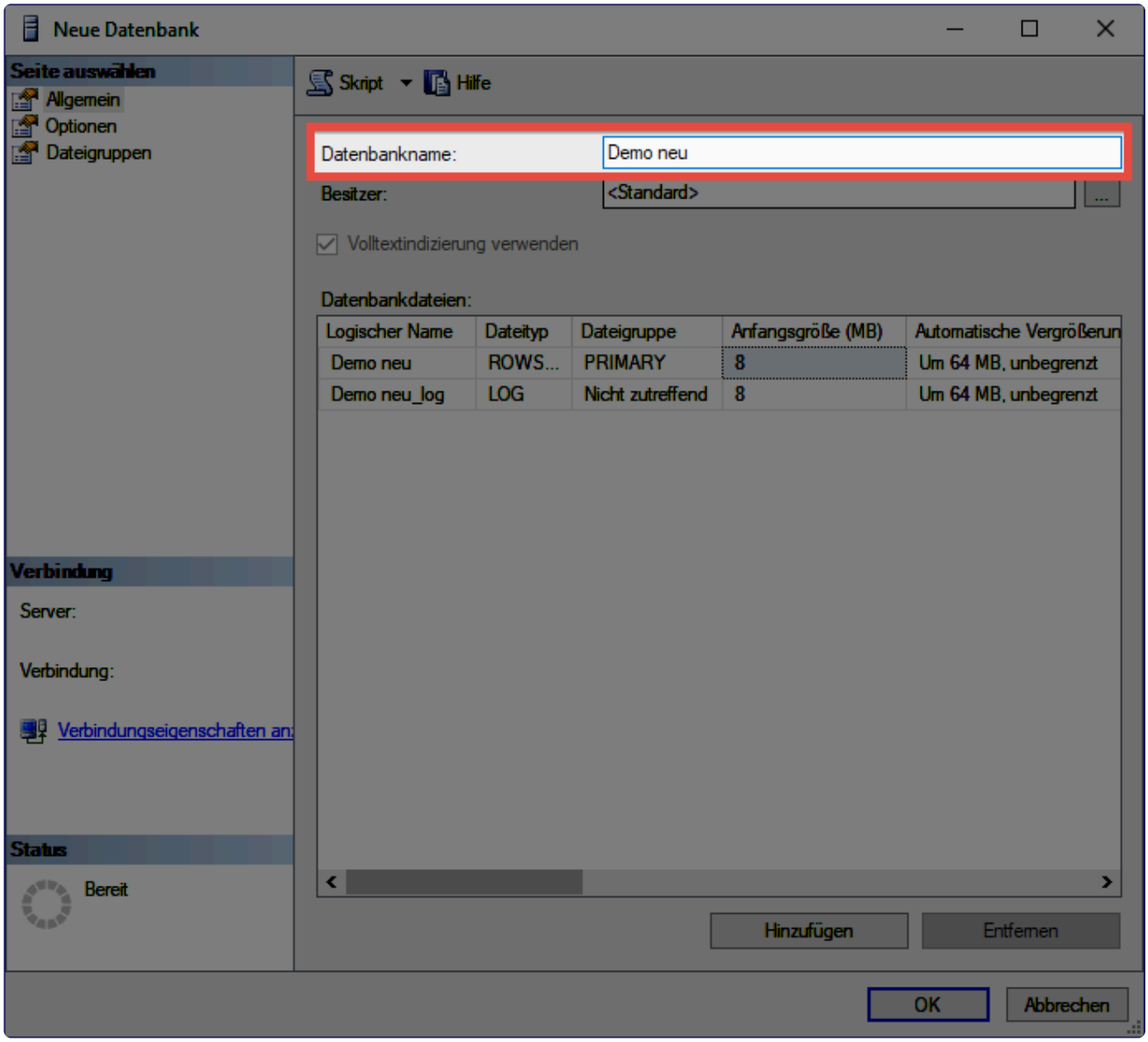
Alle verfügbaren **Zertifikate** sollten Sie unbedingt sichern. Je nach Installation werden hier mehr oder weniger Zertifikate benötigt.

Konfiguration des neuen Server

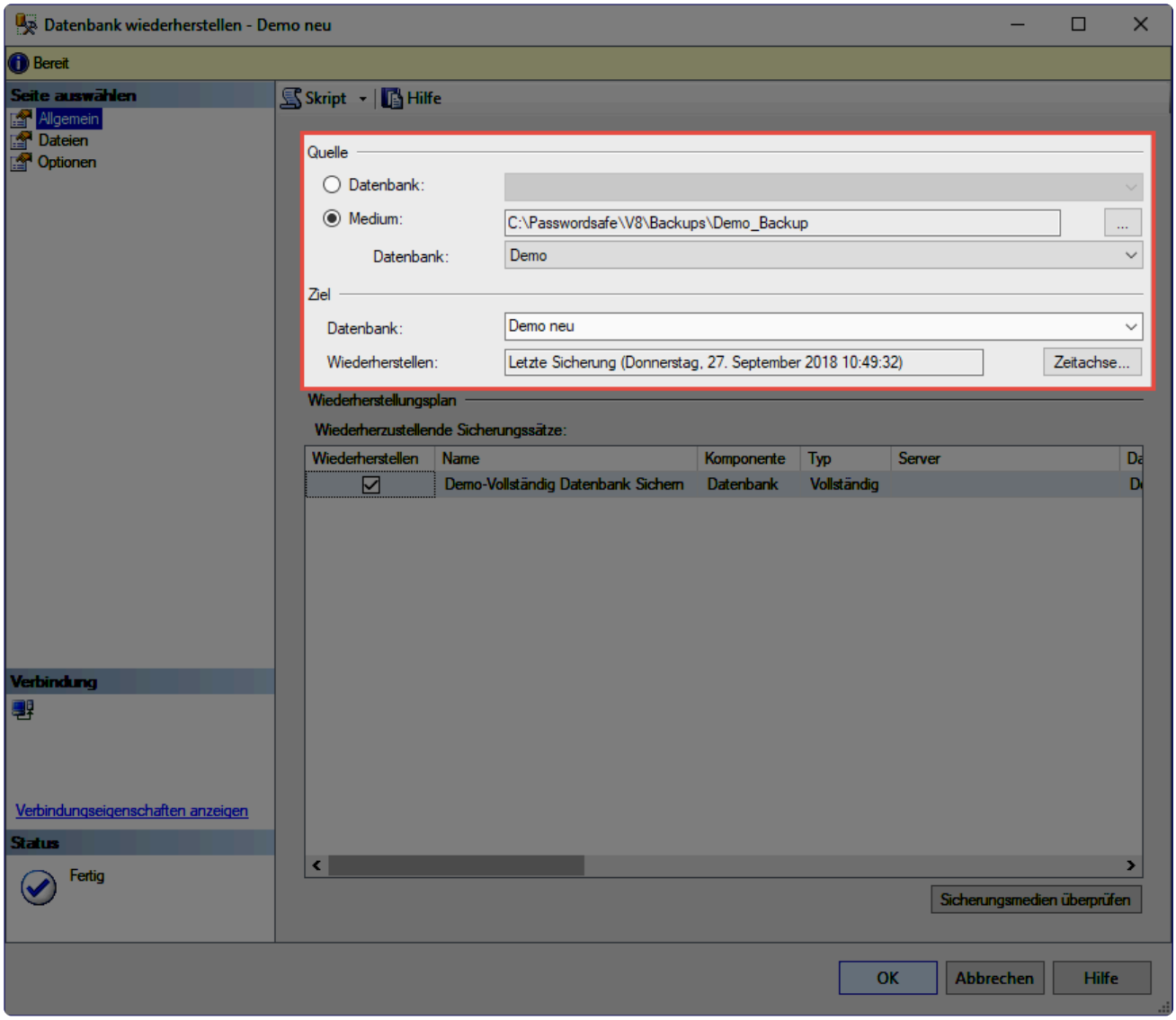
Nachdem die gesicherten Daten (Datenbank und Zertifikate) auf den neuen Server übertragen wurden, müssen Sie diese noch einbinden.

1. Einbinden der Datenbank auf SQL-Ebene

Zuerst erstellen Sie am SQL-Server eine neue Datenbank. Die Option finden Sie im SQL Management Studio nach einem Rechtsklick auf **Datenbanken**. In der Regel reicht es, wenn Sie hier nur den Datenbanknamen angeben.



Sobald die Datenbank erzeugt wurde, können Sie – über einen Rechtsklick darauf – (unter **Tasks**) den Punkt **Wiederherstellen** auswählen. Hier wird dann schließlich die **Datenbank** selektiert. Nun wählen Sie Backup aus. Prüfen Sie unter **Ziel**, ob die korrekte Datenbank selektiert ist.



> Über diesen Weg können auch Backups importiert werden, die direkt aus dem AdminClient heraus erzeugt wurden.

2. Einrichten des Servers

Nachdem das Backup in die neue Datenbank eingespielt wurde, starten Sie den AdminClient. Der **Einrichtungassistent** wird ausgeführt. Über den Einrichtungsassistent aktivieren Sie – unter anderem – die Lizenz. Nun bietet es sich an, alle gewünschten Konfigurationen des Servers vorzunehmen.

3. Import der Zertifikate

Über die Zertifikatsverwaltung importieren Sie die gesicherten Zertifikate.

4. Anbinden der Datenbank

Zuletzt erstellen Sie am Server die Datenbank über den **Datenbank-Assistenten**.

Anpassungen am Client

Sofern sich die IP und/oder der Hostname des Servers geändert hat, müssen vom Client neue **Datenbankprofile** ausgerollt/erstellt werden.

Updates

Gründe für regelmäßige Updates

Unser Entwicklungsteam arbeitet stets an der Weiterentwicklung der Software. Hierbei werden nicht nur Probleme behoben, sondern vor allem auch neue Features entwickelt. So kann unsere Software bestmöglich an die Bedürfnisse unserer Kunden angepasst werden. Wir empfehlen Ihnen deshalb, regelmäßig Updates zu installieren. Nur so können Sie stets von neuen Features und Verbesserungen profitieren.

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 können Sie nach verfügbaren Updates suchen. Die Updateprüfung am Client muss erst für die Benutzer in den Einstellungen freigegeben werden. Wir empfehlen Ihnen, die Updateprüfung für normale Benutzer deaktiviert zu lassen, da diese sonst selbstständig versuchen könnten, 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 Sie einige Voraussetzungen prüfen und ggf. schaffen.

Prüfen der Softwarepflege

Das Recht, Updates zu installieren, wird mit der Softwarepflege erworben. Beachten Sie, dass alle Updates installiert werden dürfen, solange diese aktiv ist. Bei abgelaufener Softwarepflege dürfen nur Versionen verwendet werden, die während der Laufzeit erschienen sind. Vor einem Update sollten Sie also prüfen, ob die Softwarepflege noch aktiv ist. Dies lässt sich einfach am AdminClient unter den Lizenzeinstellungen abfragen.

Erstellen eines Backups

Ein Update ist immer ein tiefgreifender Eingriff in die bestehende Software. Bitte erstellen Sie direkt vor einem Update ein entsprechendes Backup, um im Ernstfall keinen Datenverlust zu erleiden.

Prüfen der Kompatibilität

Wir versuchen stets, den AdminClient abwärtskompatibel zu gestalten. Leider ist dies nicht immer möglich. Daher sollten Sie vor einem Update stets prüfen, 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,

muss dieses unbedingt vor dem Update notiert bzw. zwischengespeichert werden!

Aktuelle Installations-Files

Die Installations-Files können Sie im Kunden-Informationssystem herunterladen:
https://license.passwordsafe.de/kis
Zur Anmeldung nutzen Sie einfach die Zugangsdaten, die Sie per E-Mail erhalten haben.

Update

Update des AdminClients

Der AdminClient wird einfach über die bestehende Installation installiert. Das Passwort vom Admin Client sollte an dieser Stelle auf jeden Fall verfügbar gemacht werden. Nach dem Durchführen der Installation des Admin Clients ist die Datenbank erst erreichbar, wenn diese aktiviert wird. Sollte das Passwort also lediglich im Password Safe liegen, sollte es an dieser Stelle temporär zwischengespeichert werden.

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. Wir empfehlen daher, die Password Safe Dienste vor dem Update zu beenden.

Weitere Infos zum Installationsassistenten sind dem Kapitel Installation AdminClient zu entnehmen.

Update der Clients

Auch die Updates der Clients werden einfach über die bestehenden Installationen installiert. 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 erzeugen Sie einen neuen WebClient. Nun leeren Sie auf dem Webserver das Dokumentenverzeichnis. Dann entpacken Sie den WebClient und kopieren Ihn auf den entsprechenden Webserver ins Dokumentenverzeichnis.

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.

Kommt der WebClient zum Einsatz, müssen Sie bei der Verwendung von **Apache** das Modul: **proxy_wstunnel** nachinstallieren. Beim **IIS** wird das **WebSocket Protocol** nötig. Infos hierzu sind auch im Kapitel Systemanforderung WebClient zu finden. Dies gilt für

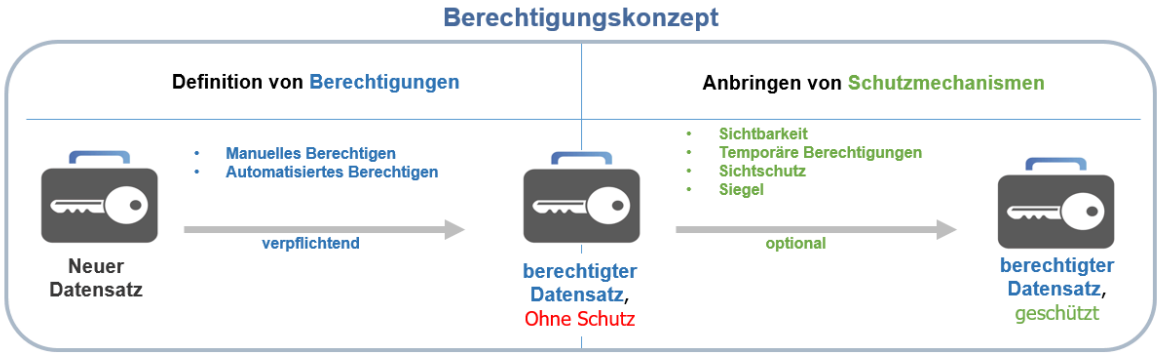
alle Updates auf 8.5.0.14896 oder neuer.

Berechtigungskonzept und Schutzmechanismen

Was ist das Berechtigungskonzept?

Die Stärke von Password Safe ist das Konzept der Berechtigungen. Benutzern wird dabei erlaubt, bei Datensätzen gewisse Aktionen durchzuführen. Um den Aufwand hier möglichst gering zu halten, bietet sich die Zusammenfassung mehrerer Benutzer in Rollen an. Diese Rollen können dann entweder manuell oder automatisiert auf Datensätze berechtigt werden. Dafür existieren mehrere Varianten, die folgend genauer erläutert werden.

Neben der Definition von manuellen und automatischen Berechtigungen ist das (optionale) Anbringen von Schutzmechanismen Teil des Berechtigungskonzeptes. Diese Schutzmechanismen sind – wie man in der folgenden Grafik erkennen kann – den Berechtigungen nachgelagert.



Berechtigungen auf Datensätze ist verpflichtend, Schutzmechanismen sind optional.

Die Sichtbarkeit ist technisch gesehen eine Berechtigung, besitzt aber einen “Schutzcharakter” und wird daher als Schutzmechanismus aufgeführt.

Das Berechtigungskonzept basiert auf drei Grundpfeilern, die Einfluss auf jede Art von Berechtigungen haben. Die Funktionsweise wird nachfolgend erklärt. Auf das manuelle und automatische Berechtigen sowie die möglichen Schutzmechanismen wird in den nächsten Kapiteln eingegangen.

Die drei Grundpfeiler des Berechtigungskonzeptes

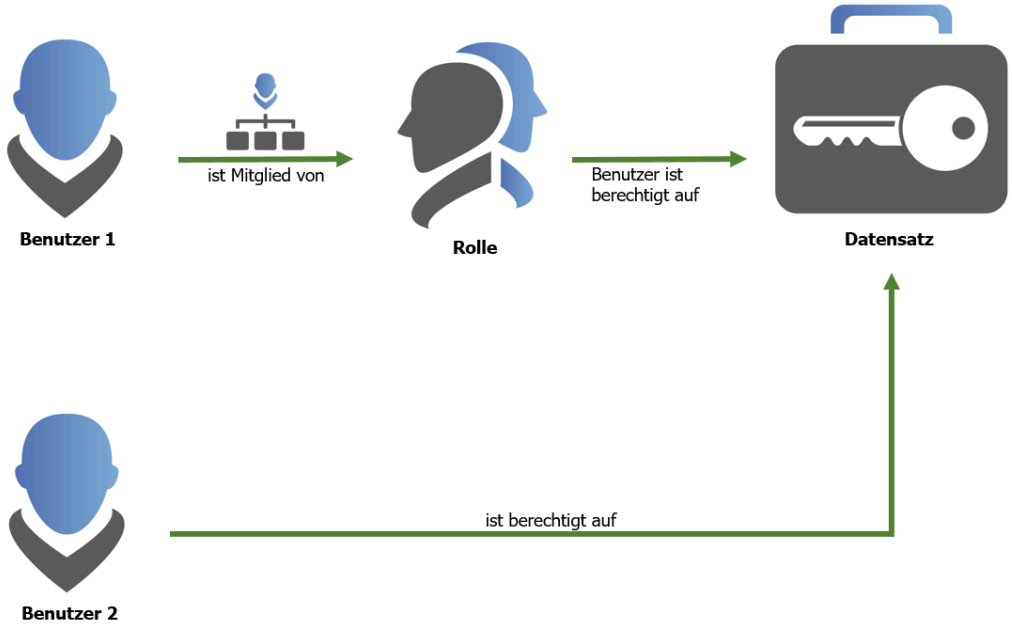
Egal ob kleine Arbeitsgruppe oder international agierender Konzern – in Password Safe sind alle gleich. Es gibt einige wenige Regeln, die trotz der unzähligen, individuellen Stellschrauben immer und ohne Ausnahme gelten.

1. Berechtigungen nur für Benutzer oder Rollen

Es gibt zwei Möglichkeiten, die Berechtigung für einen Datensatz festzulegen:

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

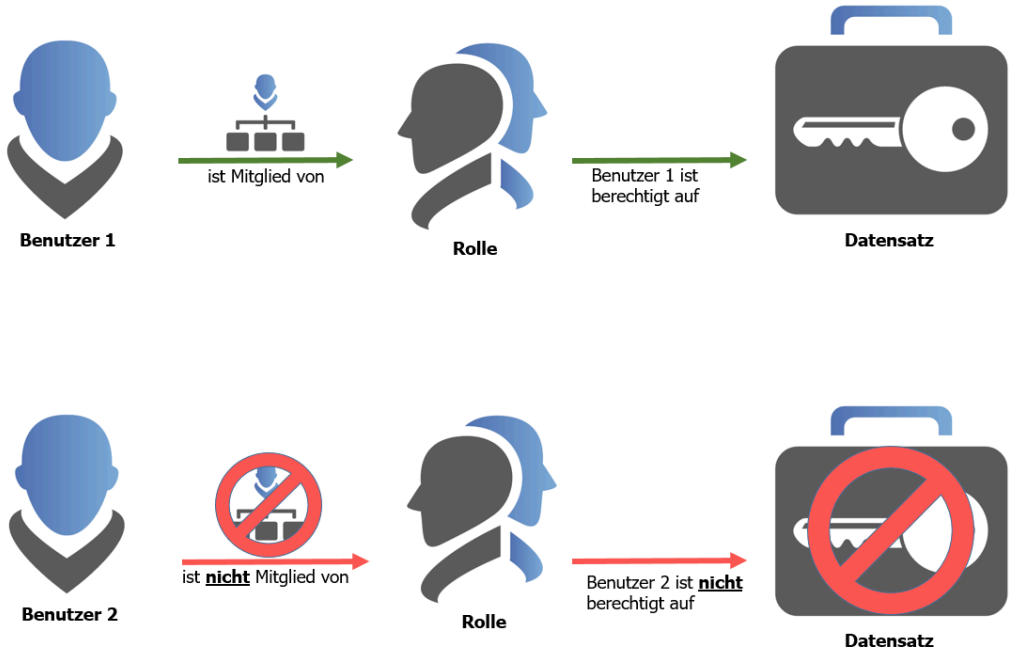
Eine Rolle ist technisch nichts anderes als eine Zusammenfassung mehrerer Benutzer mit gleichen Berechtigungen. Es bietet sich hier an, Benutzer entsprechend Ihrer Position oder Abteilung im Unternehmen in Rollen zu verwalten. Die Rolle “Administratoren” kann demnach mit weitläufigeren Berechtigungen versehen werden als z.B. die Rolle “Vertriebsassistenz”. Die rollenbasierte Vererbung der Berechtigungen ermöglicht eine bessere Übersicht bei größeren Unternehmensstrukturen sowie das einfache Hinzufügen neuer Mitarbeiter. Denn statt den Mitarbeiter einzeln berechtigen zu müssen, fügt man diesen einfach seiner ihm angedachten Rolle zu. Die Berechtigung für einen einzelnen Benutzer macht nur in Ausnahmesituationen Sinn.



Berechtigungen werden stets nur einem Benutzer oder einer Rolle gewährt!

2. Mitgliedschaft in Rollen

Soll ein Mitarbeiter die Berechtigungen gemäß der für ihn vorgesehenen Rolle nutzen können, **muss er zwingend Mitglied dieser Rolle sein**. Nur Mitglieder sehen die Datensätze, auf die eine Rolle berechtigt wurde.

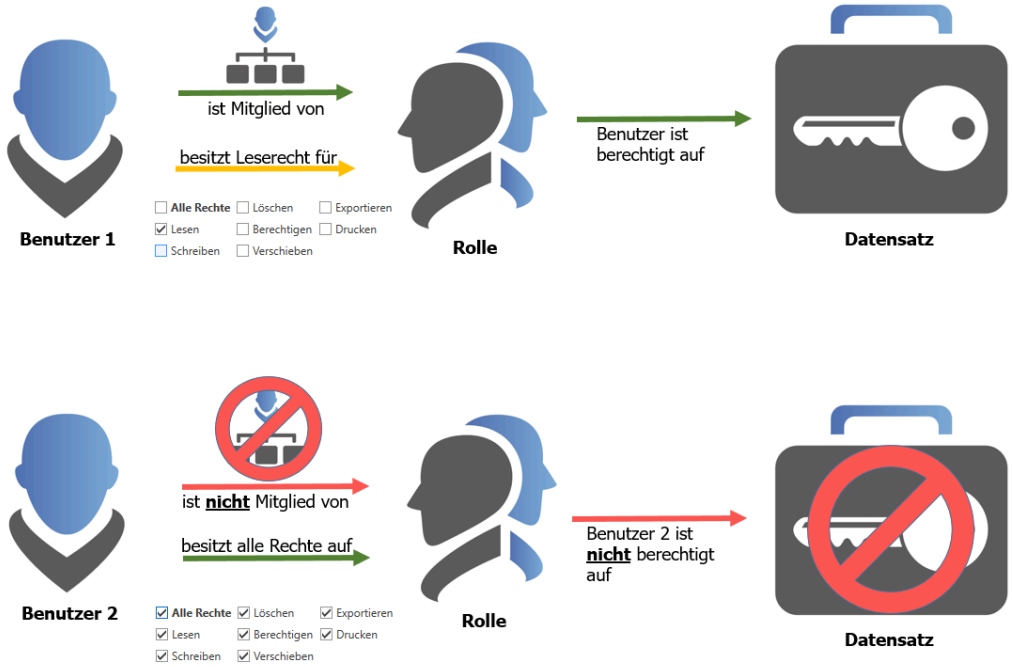


Ein kleiner technischer Exkurs in die Verschlüsselung von Datensätzen. Jede Rolle besitzt ein Schlüsselpaar. Mit dem ersten Schlüssel werden Daten verschlüsselt. Zugang zu diesen Informationen erhält man nur mit dem zweiten Schlüssel. Bei der Berechtigung einer Rolle auf einen Datensatz entspricht die Mitgliedschaft in dieser Rolle dem zweiten Schlüssel.

Die Mitgliedschaft in einer Rolle kann nur von denjenigen Benutzern vergeben werden, die selbst Mitglied sind!

3. Mitgliedschaft vs. Rechte auf Rollen

Das Wechselspiel zwischen Benutzern und Rollen ist ein Thema, bei dem es schnell zu Missverständnissen kommen kann. Daher muss man bei der Anwendung des Berechtigungskonzeptes an die eigene Unternehmensstruktur sehr aufmerksam sein. Das folgende Schaubild veranschaulicht den Unterschied anhand zweier Benutzer.



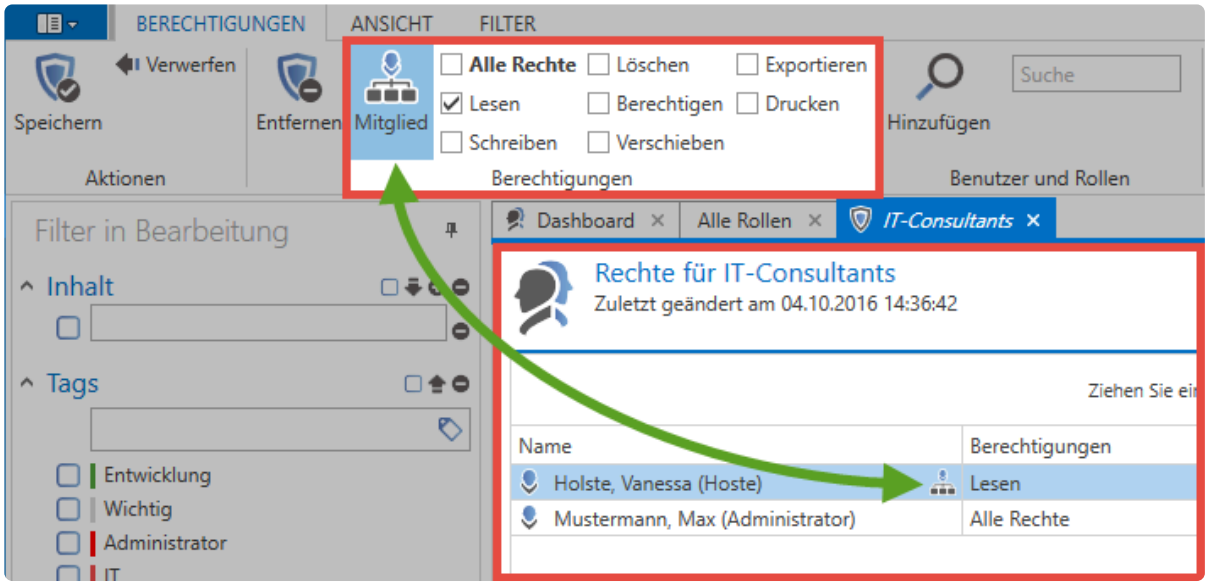
- **Benutzer 1** ist Mitglied der Rolle und dementsprechend berechtigt auf alle Datensätze, die der Rolle angedacht sind. Auf die Rolle an sich besitzt er jedoch nur “Leserecht”. Das bedeutet, er kann die Rolle sehen, jedoch nicht “bearbeiten, verschieben oder gar löschen”.
- **Benutzer 2** besitzt alle 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 die die Rolle berechtigt.

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

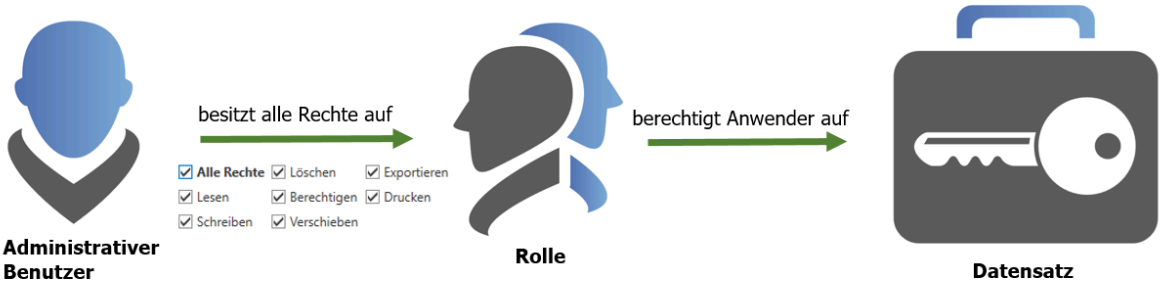
> Als Mitglied einer Rolle muss mindestens das Recht “Lesen” auf die Rolle gewährt werden!

Konkretes Beispiel und Konfiguration

Analog zum vorherigen Abschnitt (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 Beispiel-Rolle “IT-Consultants” in der Listenansicht wird die Detailansicht geöffnet



- Der Benutzer “Holste” ist Mitglied der Rolle und kann auf die Datensätze zugreifen, auf die die Rolle berechtigt ist. Er besitzt das obligatorische Leserecht auf die Rolle – Grundvoraussetzung für die Mitgliedschaft. Welche exakten Rechte er auf den Datensatz besitzt, wird nicht innerhalb der Rolle definiert! Dies geschieht durch manuelles oder automatisches Berechtigen.
- Der Benutzer “Administrator” besitzt alle Rechte auf die Rolle, ist **jedoch kein Mitglied**! Er kann demnach **keine** Datensätze sehen, auf die die Rolle berechtigt ist Er kann zwar weitere Benutzer auf die Rolle berechtigen und auch löschen aber er kann **nicht** die Mitgliedschaft an andere Benutzer weitergeben.



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 in Password Safe beliebig definierbar.

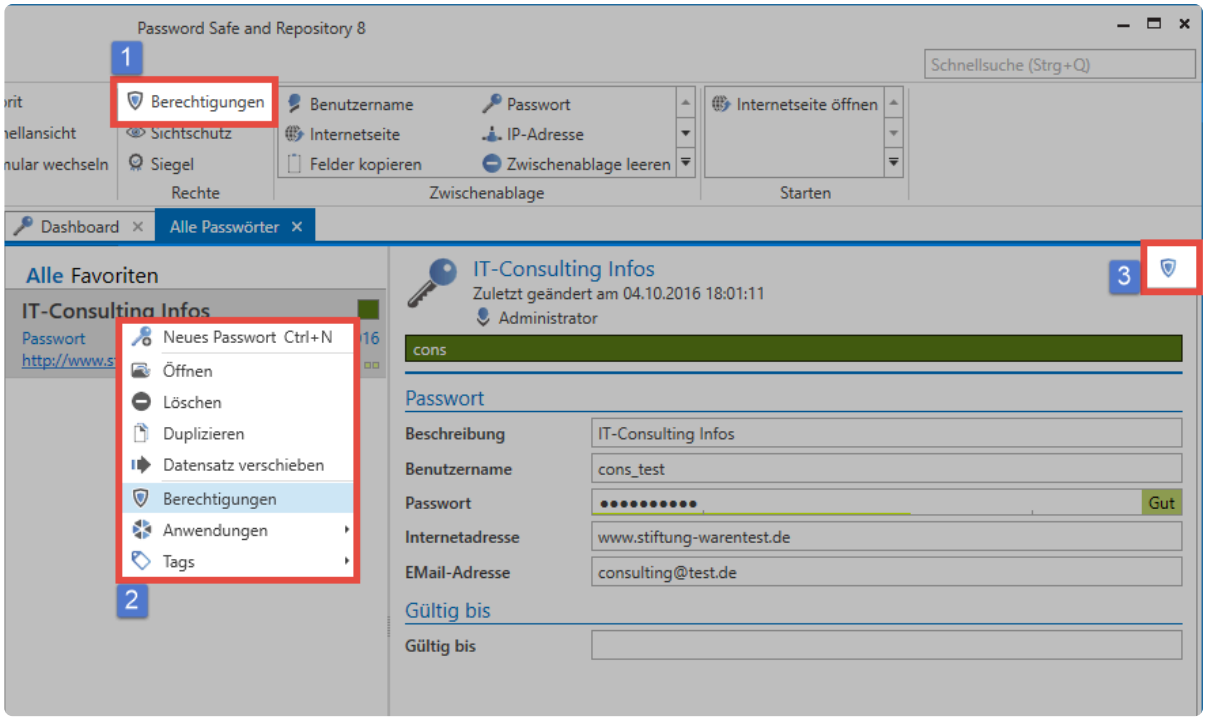
Manuelles Berechtigen

Hier werden die Berechtigungen auf einen Datensatz manuell zugewiesen. Das geschieht in der Regel bei bereits bestehenden Datensätzen. Für die Neuanlage von Datensätzen ist dieser Prozess wenig zielführend da unter Umständen sehr zeitaufwendig. Wir empfehlen in diesem Fall das automatisierten Berechtigen.

Hinzufügen von weiteren Berechtigten

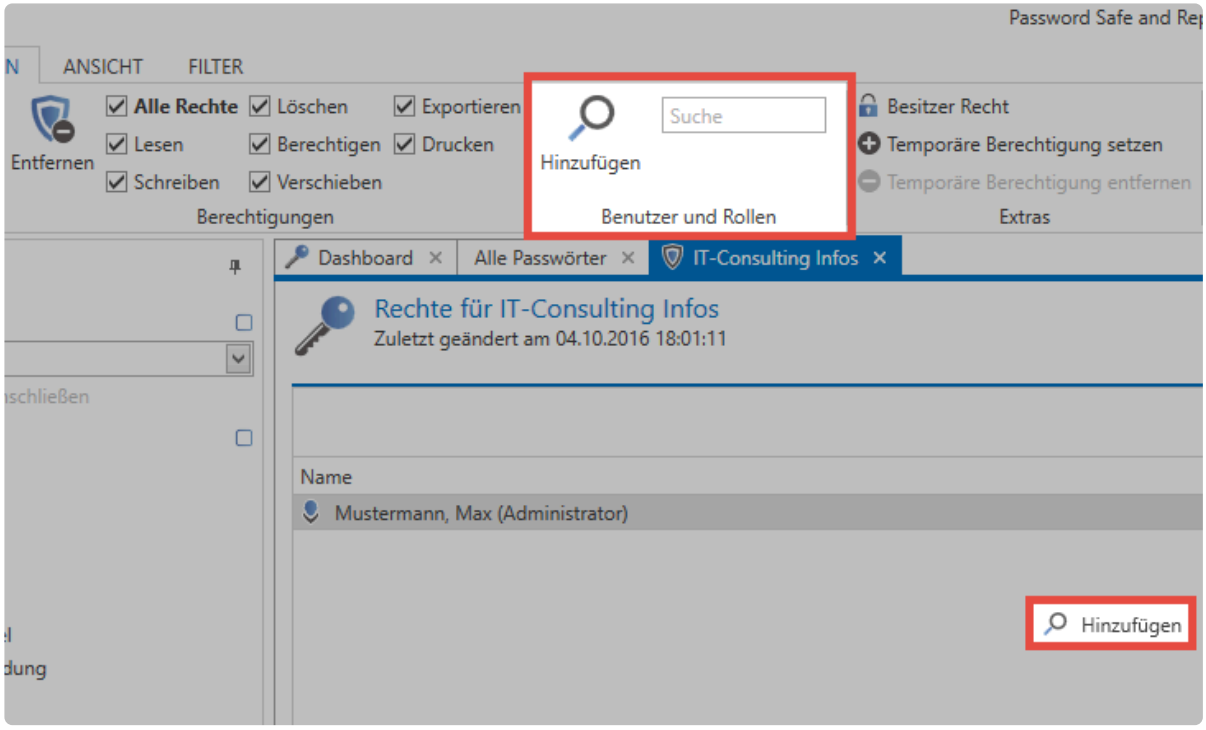
Im vorherigen Kapitel wurde geklärt, dass einzelne Benutzer direkt oder in Rollen zusammengefasst auf Datensätze berechtigt werden können. Dafür gibt es im Client Modul Passwörter drei verschiedene Möglichkeiten:

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

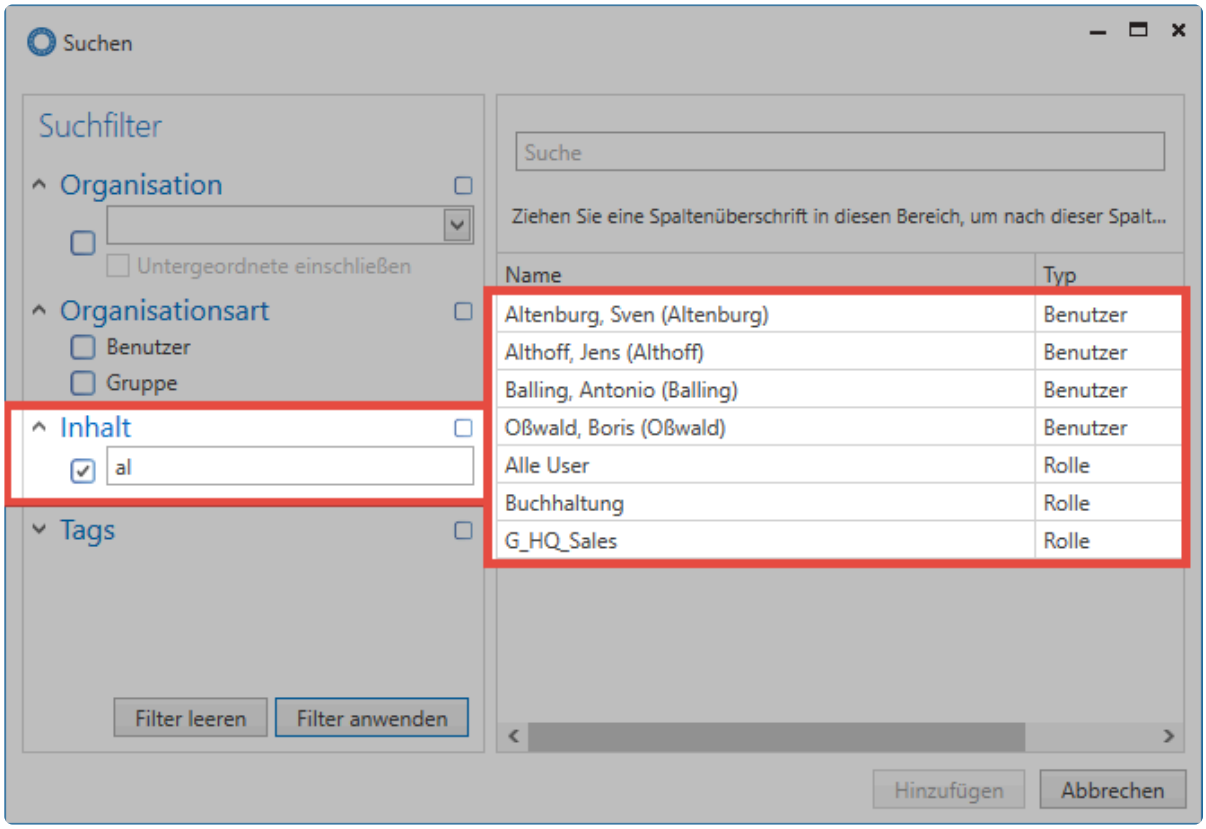


> Links neben dem Icon im Lesebereich wird angezeigt, ob der Datensatz persönlich oder öffentlich ist. Bei einem persönlichen Datensatz ist nur der angemeldete Benutzer auf diesen berechtigt!

Der Ersteller wird mit allen Rechten auf den Datensatz angelegt. Wie im Berechtigungskonzept beschrieben, können sowohl Rollen als auch weitere Benutzer hinzugefügt werden. Mittels Rechtsklick im Tab oder über das entsprechende Icon in der Ribbon gelangt man zum Suchfilter um nach den Benutzern oder Rollen zu suchen, die auf den Datensatz berechtigt werden sollen.



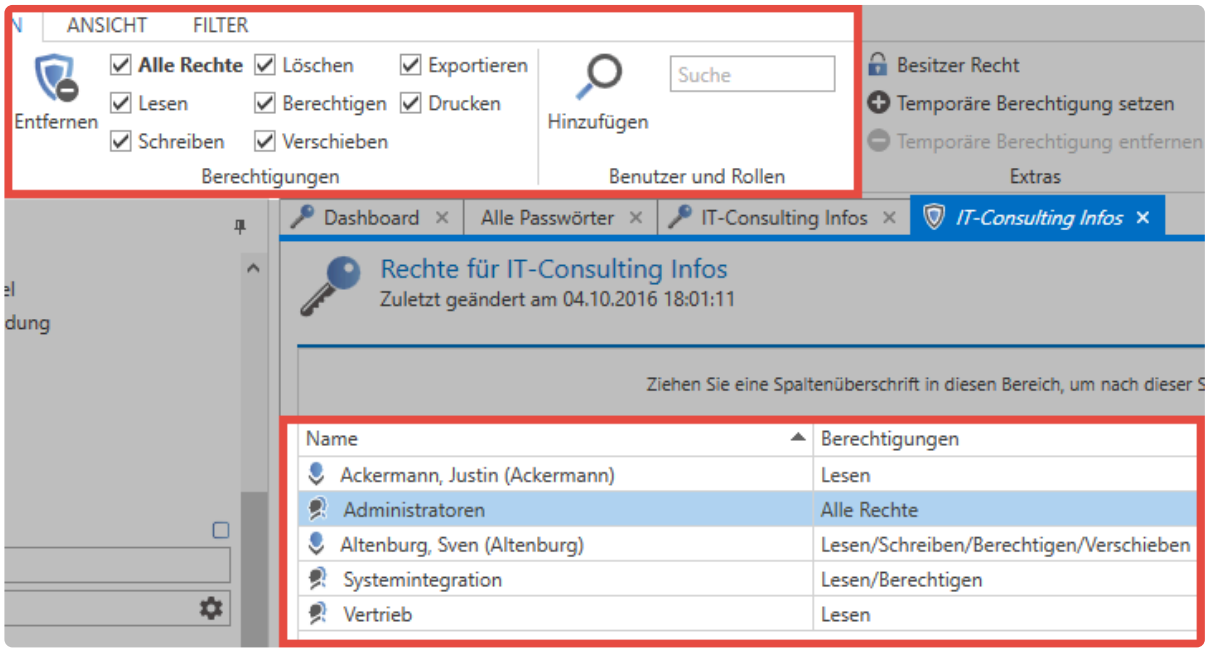
Der Suchfilter öffnet sich in einem separaten Tab. Der Filter lässt sich wie bekannt konfigurieren. Die Suche verhält sich analog zur Suche in der Listenansicht.



Dank **Mehrfachauswahl** mittels **Strg/Shift + linke Maustaste** können auch mehrere Benutzer gleichzeitig hinzugefügt werden.

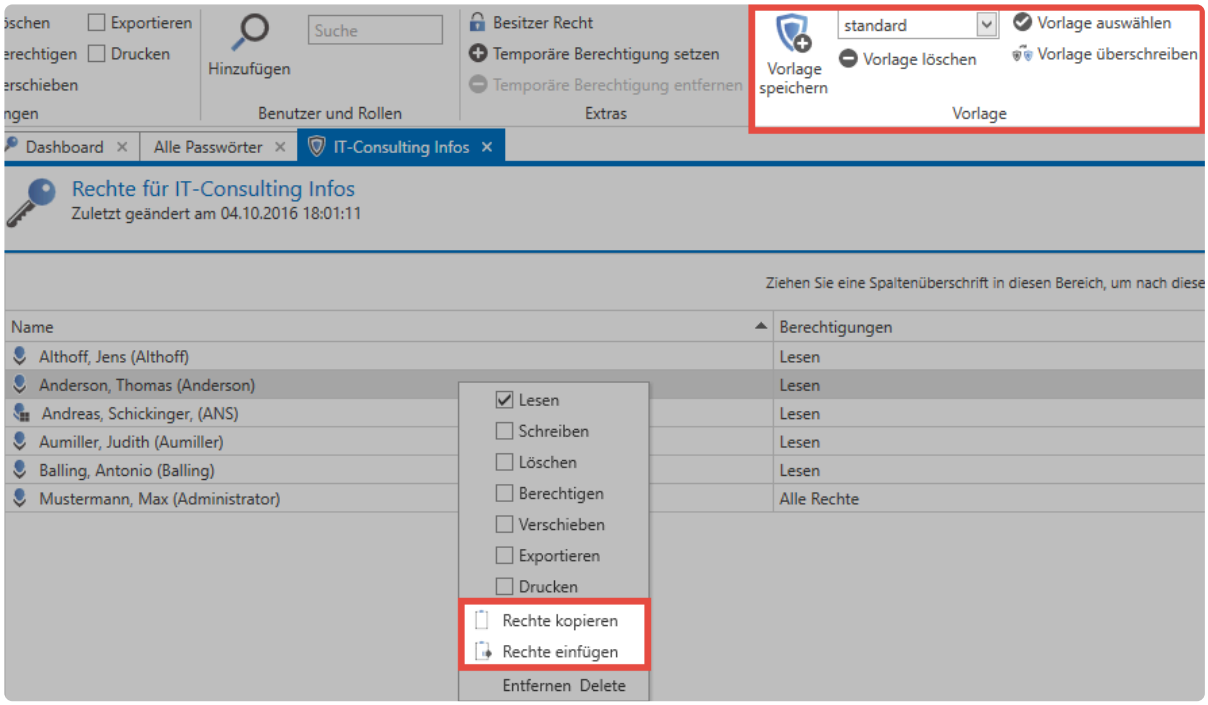
Setzen und Entfernen von Berechtigungen

Standardmäßig erhalten alle hinzugefügten Benutzer oder Rollen lediglich das Recht “Lesen” auf den Datensatz. Das ist ausreichend, um die Felder des Datensatzes einzusehen und das Passwort auch nutzen zu können. Zum Bearbeiten eines Datensatzes ist das Recht “Schreiben” notwendig. **Das Recht “Berechtigen” ist nötig, um einerseits andere Benutzer auf den Datensatz zu berechtigen** und andererseits Siegel zu konfigurieren.



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.



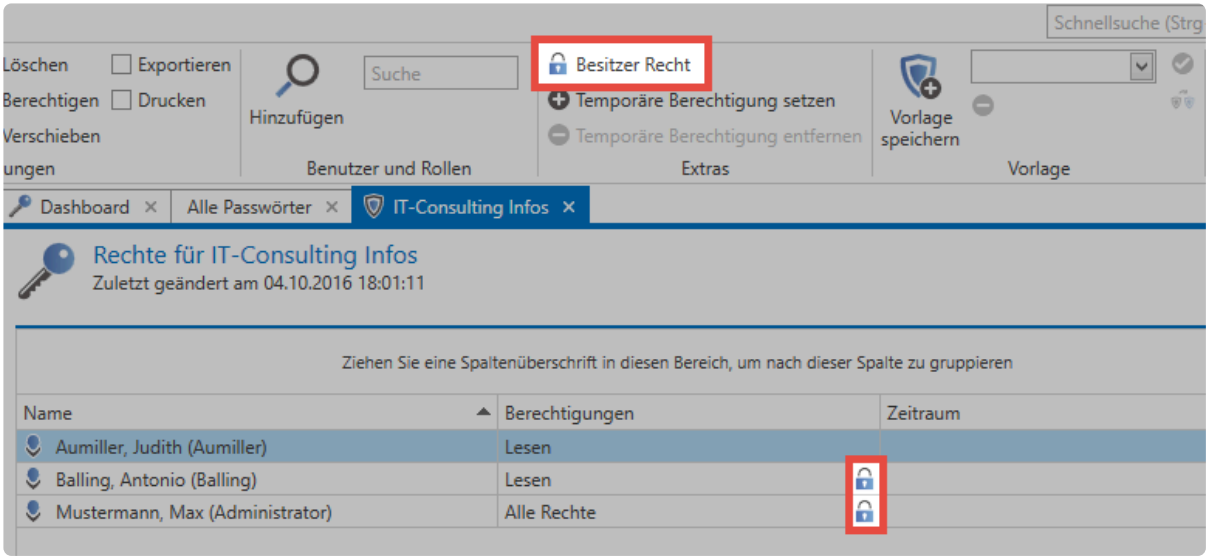
Das Übertragen von Rechten und die Wiederverwendung von Rechtevorlagen hilft bei der Berechtigungsintegrität und der Minimierung von Fehlkonfigurationen, auch wenn diese damit nicht 100%ig ausgeschlossen werden.

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 etwa einen neuen Datensatz erstellen darf. Dieses Recht kann daher nur im Modul Organisationsstrukturen zugewiesen werden. Mehr…

Besitzer Recht

Jedem Benutzer kann das Besitzerrecht zugewiesen werden. Einmal zugewiesen besteht keine Möglichkeit mehr, Benutzer oder Rollen mit Besitzerrecht aus den Berechtigungen eines Datensatzes zu entfernen. Dies ist nur noch durch den erstellenden Benutzer bzw. Rolle selbst oder durch Benutzer mit dem Recht “Ist Datenbank Administrator” möglich.

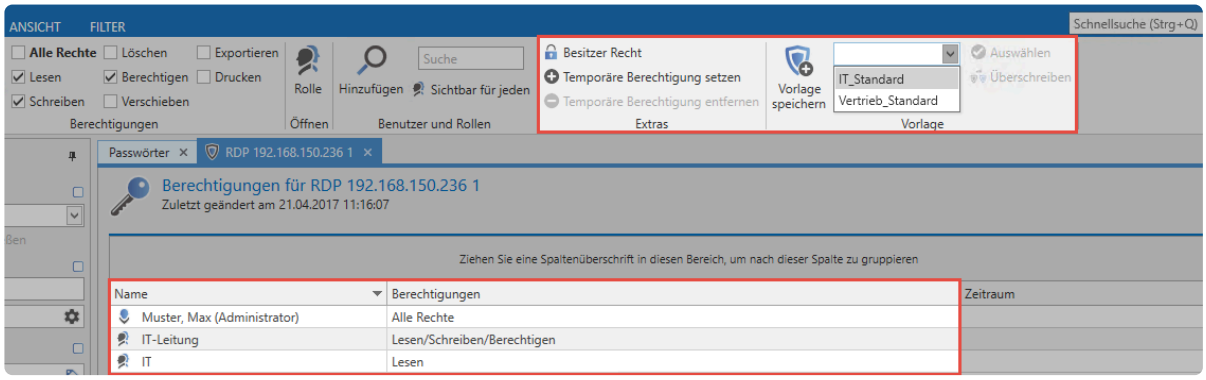


Das Besitzerrecht schützt somit vor dem Fall, dass andere Benutzer mit dem Recht “Berechtigen” wiederum andere Benutzer aus dem Datensatz entfernen wollen.

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

Nutzung von Rechtevorlagen

Einmal konfigurierte Berechtigungen können immer wieder verwendet werden. Hierfür nutzt man die in der Ribbon zur Verfügung gestellte Funktion **Vorlage speichern**. Diese Funktion steht dann global zur Verfügung und kann auch auf andere Datensätze angewandt werden.



> Verwenden Sie beim Speichern von Vorlagen aussagekräftige Namen um auch bei einer größeren Anzahl den Überblick zu behalten.

Wir empfehlen, die manuelle Rechtevergabe mittels Vorlagen nur in Ausnahmefällen zu nutzen. Verwenden Sie statt dessen Automatismen, die in den Kapiteln Rechte vordefinieren, und Vererbung aus Organisationsstrukturen erklärt werden..

Mehrfachbearbeitung von Berechtigungen

Es ist möglich, mehrere Datensätze zu markieren und deren Berechtigungen manuell anzupassen. Dazu können die Datensätze entweder durch eine selektive Auswahl in der Listenansicht als auch über die Nutzung des Filter markiert werden. Beide Szenarien sind nachfolgend beschrieben. Diese Option ist standardmäßig deaktiviert und muss für die entsprechenden Benutzer zunächst aktiviert werden.

Benutzerrecht

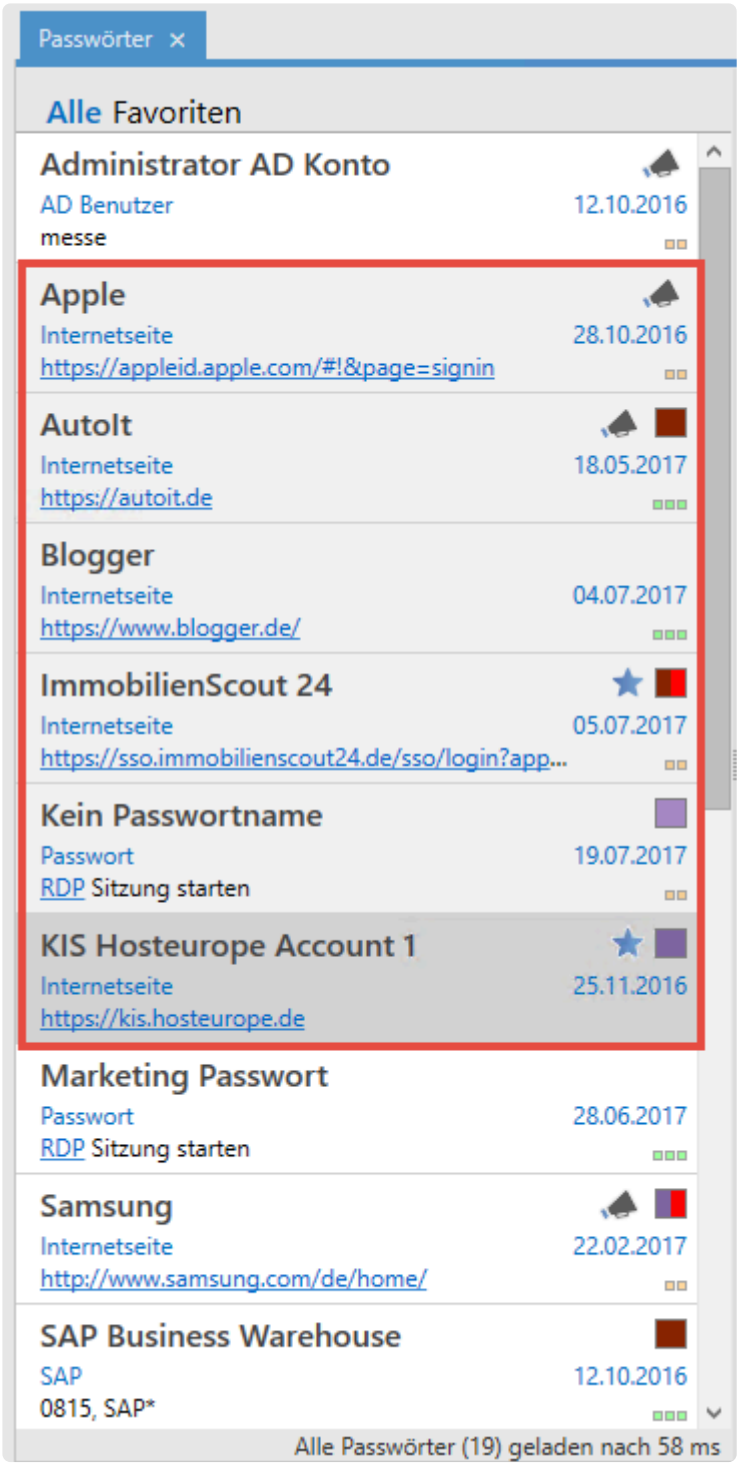
- Kann Stapelverarbeitung bei Berechtigungen anhand eines Filters durchführen

Mehrfachbearbeitung über die Listenansicht

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

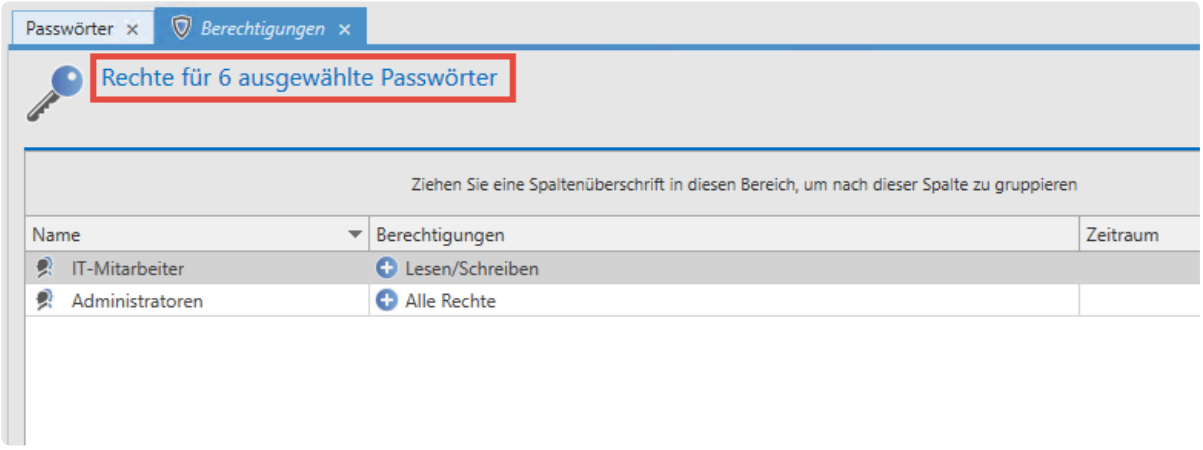
Selektion der Datensätze

Innerhalb der Listenansicht können mittels Shift, bzw. **Strg + Mausklick** mehrere Datensätze selektiert werden. Änderungen der Berechtigungen wirken sich dann auf alle diese Datensätze aus. 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 dem die zu vergebenden Rechte konfiguriert werden. Dort wird auch die Anzahl der Datensätze angezeigt, die von den 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.

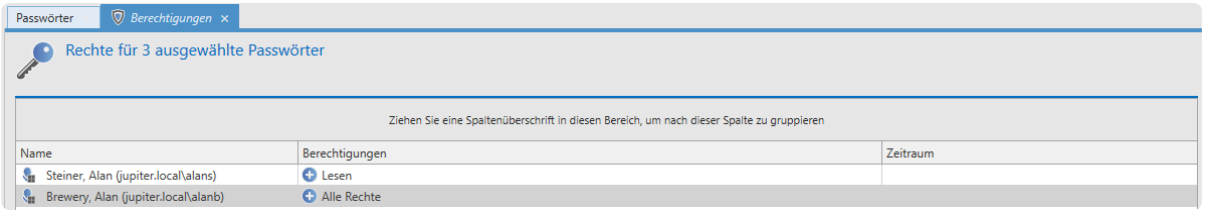
Rechte reduzieren / Benutzer und Rollen aus der Berechtigung entfernen

Sollen Rechte entfernt werden, muss ebenfalls zunächst der zu bearbeitende Benutzer, bzw. die gewünschte Rollen hinzugefügt werden. Über einen Klick auf **Rechte reduzieren** wird 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.

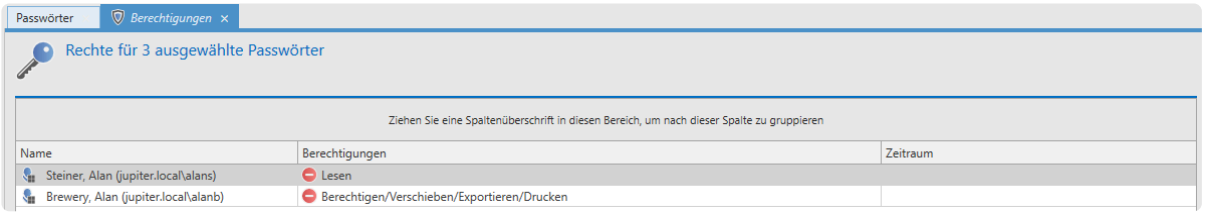
Beispiele

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



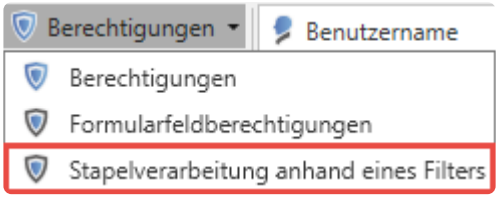
Hier wird Hr. Steiner das Leserecht entzogen. Da ohne das Leserecht keine anderen Rechte auf die Datensätze bestehen können, wird Hr. Steiner komplett aus den Berechtigungen entfernt. Hr. Brewery

werden die Rechte Berechtigen, Verschieben, Exportieren und Drucken entzogen. Davon ausgehend, dass er zuvor alle Rechte hatte, bleiben anschließend also noch die Rechte Lesen, Schreiben und Löschen übrig:



Stapelverarbeitung anhand eines Filters

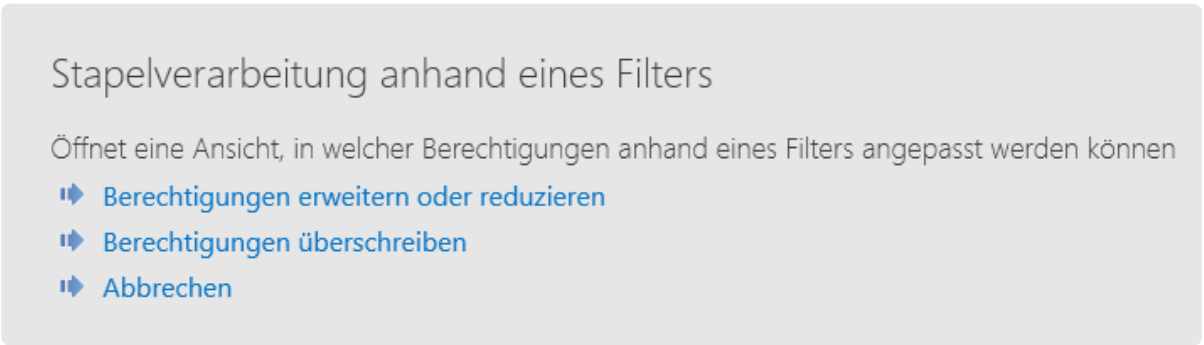
In manchen Fällen ist die Bearbeitung von Berechtigungen sehr viele Datensätze notwendig. Einerseits existiert die Restriktion auf maximal 1000 Datensätze, andererseits ist die Handhabung bei sehr vielen Datensätzen über die Listenansicht nicht immer die beste Wahl. Hierzu ist der Modus “Stapelverarbeitung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



Anschließend können Sie, ob vorhandene Berechtigungen erweitert, reduziert oder komplett überschrieben werden sollen. Bei **Erweitern bzw. Reduzieren** greift die gleiche Logik wie beim **Bearbeiten über die Listenansicht**: Es werden also keine bestehenden Rechte überschrieben.

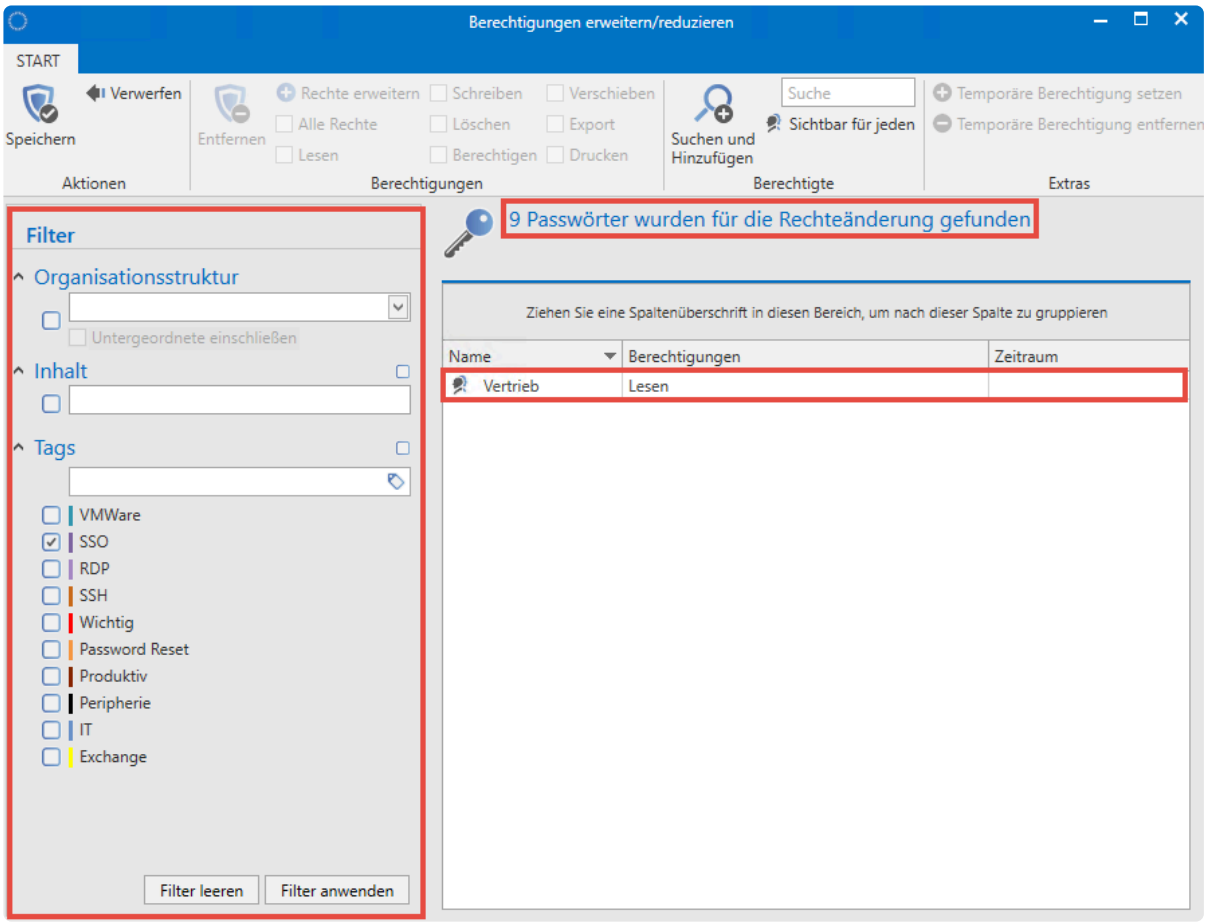
Bei **Berechtigungen überschreiben** werden zunächst alle bestehenden Rechte entfernt und durch die neu definierten Rechte ersetzt.

> ! Bitte beachten Sie, dass durch das Überschreiben der Rechte schnell eine große Anzahl an Datensätzen unbrauchbar gemacht werden kann.



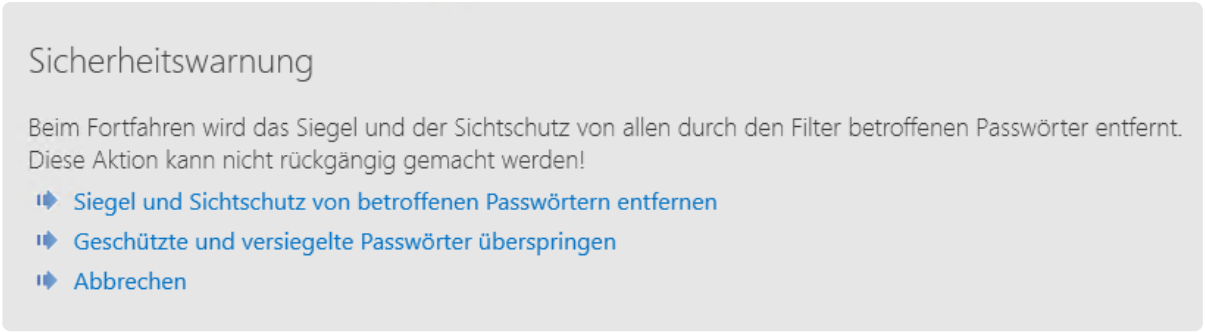
Die Auswahl der Datensätze, die bearbeitet werden sollen, wird durch den Filter selbst definiert. Als Default wird der derzeit konfigurierte Filter übernommen. Welche Datensätze von den Änderungen betroffen sein werden, wird in dieser Ansicht ebenso nicht aufgezeigt, sondern lediglich die Anzahl. Im 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 Sichtschutz nicht bearbeitet werden. Wenn derartige Passwörter selektiert sind, erscheint beim Ausführen der Stapelverarbeitung ein Dialog, in dem festgelegt wird, wie mit den Datensätzen umgegangen werden soll.



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

! Das Entfernen von Siegel und Sichtschutz 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. Nach Abschluss erhalten Sie einen entsprechenden Hinweis.

Automatisiertes Berechtigen

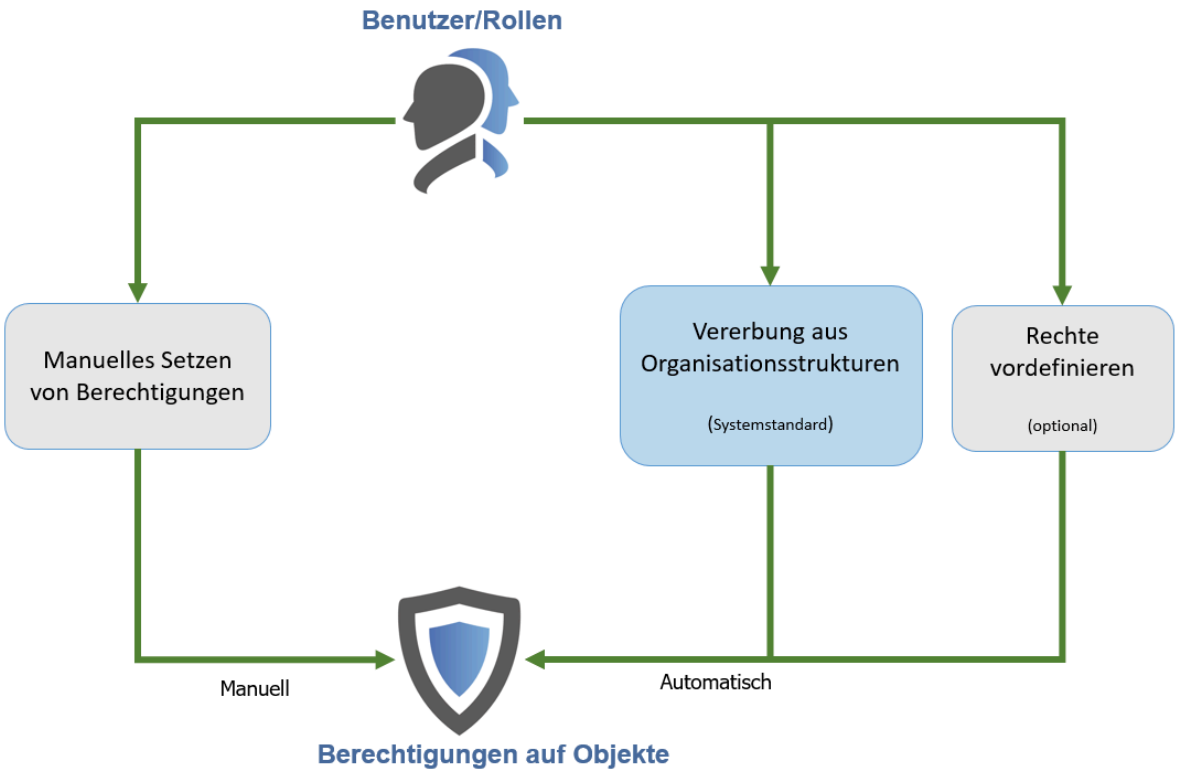
Wiederverwendung von Berechtigungen

Grundsätzlich unterscheidet Password Safe zwischen verschiedenen 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 konfigurieren Sie direkt für jeden Datensatz die gewünschten Berechtigungen. 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 mit der Frage: **Wie erhalten Benutzer oder Rollen die Ihnen angedachten Berechtigungen?**



Die Vererbung aus Organisationsstrukturen ist systemseitig als **Standard** definiert. Dies können Sie in den Einstellungen unter “Berechtigungen vererben auf neue Objekte (ohne Rechtevorlage) anpassen. **Weitere Infos…**

Berechtigung des Erstellers

Grundsätzlich wird immer derjenige Benutzer, der einen Datensatz erstellt, mit Vollzugriff berechtigt. Hierbei ist es irrelevant, ob weitere Rechte vergeben oder vererbt werden. Über die Einstellung **Ersteller aus den Berechtigungen bei neuen Objekten entfernen, wenn der erstellende Benutzer über eine Rolle berechtigt wird** kann dieses Verhalten geändert werden. Ist diese Einstellung aktiv, wird der erstellenden Benutzer nicht explizit in den Rechten mit aufgenommen, wenn er über eine Rolle zumindest Leserechte erhält.

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 finden Sie im Kapitel **Berechtigungen auf Organisationsstrukturen**". 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.

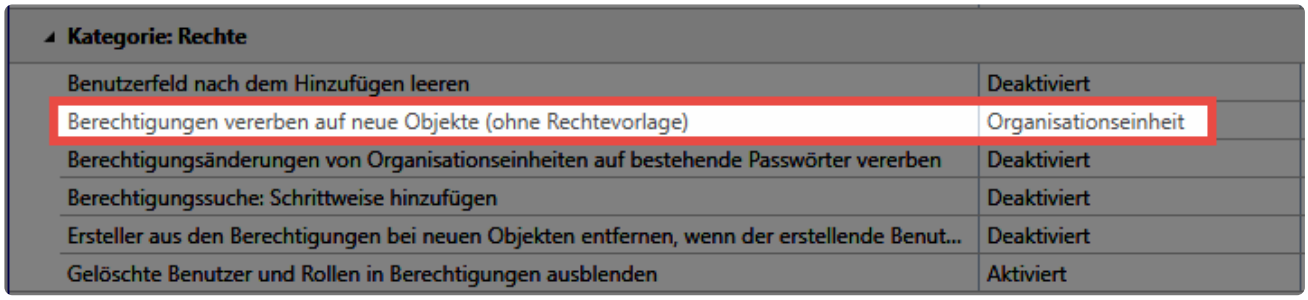
Relevante Benutzereinstellungen

Ob die genannte Form der Vererbung angewandt werden soll, definieren Sie über die **Einstellungen** in der Ribbon. Diese konfigurieren Sie über zwei Einstellungen näher.

> ! Ist ein **vordefiniertes Recht** vorhanden, überschreibt dieses stets Vererbungen aus Organisationsstrukturen.

Berechtigung vererben auf neue Objekte (ohne Rechtevorlage)

Diese Einstellung wirkt sich auf **neu erstellte** Datensätze aus.

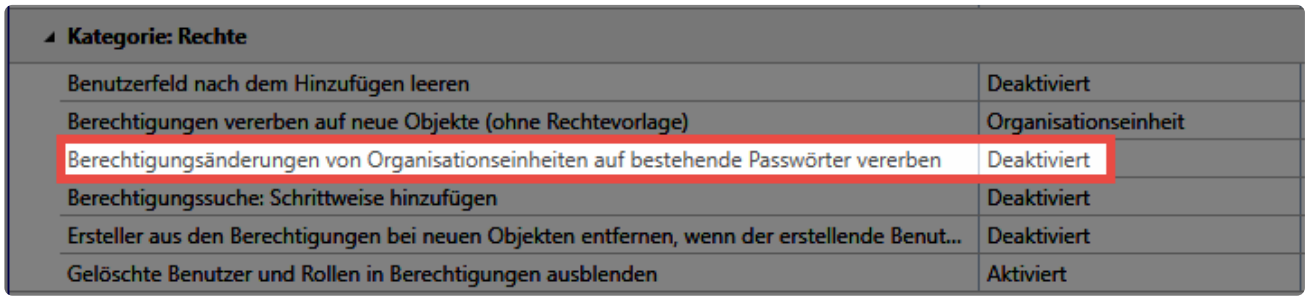


Folgende Werte können Sie konfigurieren:

- **Aus**: Berechtigungen auf OUs werden nicht vererbt.
- **Organisationseinheit**: Berechtigungen beim Erstellen neuer Objekte werden gemäß den in der Ziel-Organisationseinheit definierten Rechten gesetzt. Die Einstellung ist **standardmäßig aktiv**.
- **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 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.

Berechtigungsänderungen von Organisationseinheiten auf bestehende Passwörter vererben



Diese Option bedingt, dass Änderungen der Rechte einer Organisationseinheit auf alle darin befindlichen Passwörter vererbt werden. Die Einstellung ist **standardmäßig aktiv**. Beim Vererben wird ein Dialog eingeblendet, welcher folgende Möglichkeiten bietet:

- **Berechtigungen erweitern oder reduzieren**: Die Rechte der Passwörter bleiben bestehen und werden nur durch die Änderung ergänzt bzw. reduziert.
- **Berechtigungen überschreiben**: Die Rechte der Passwörter werden komplett überschrieben. Es werden also zunächst alle Rechte vom Passwort entfernt und anschließend die neu gesetzten Rechte der Organisationseinheit platziert.
- **Vererbung abbrechen**: Die Rechte werden nicht vererbt, sondern nur in der Organisationseinheit geändert.

> Die Vererbung auf bestehende Passwörter greift nur innerhalb der Organisationseinheit.

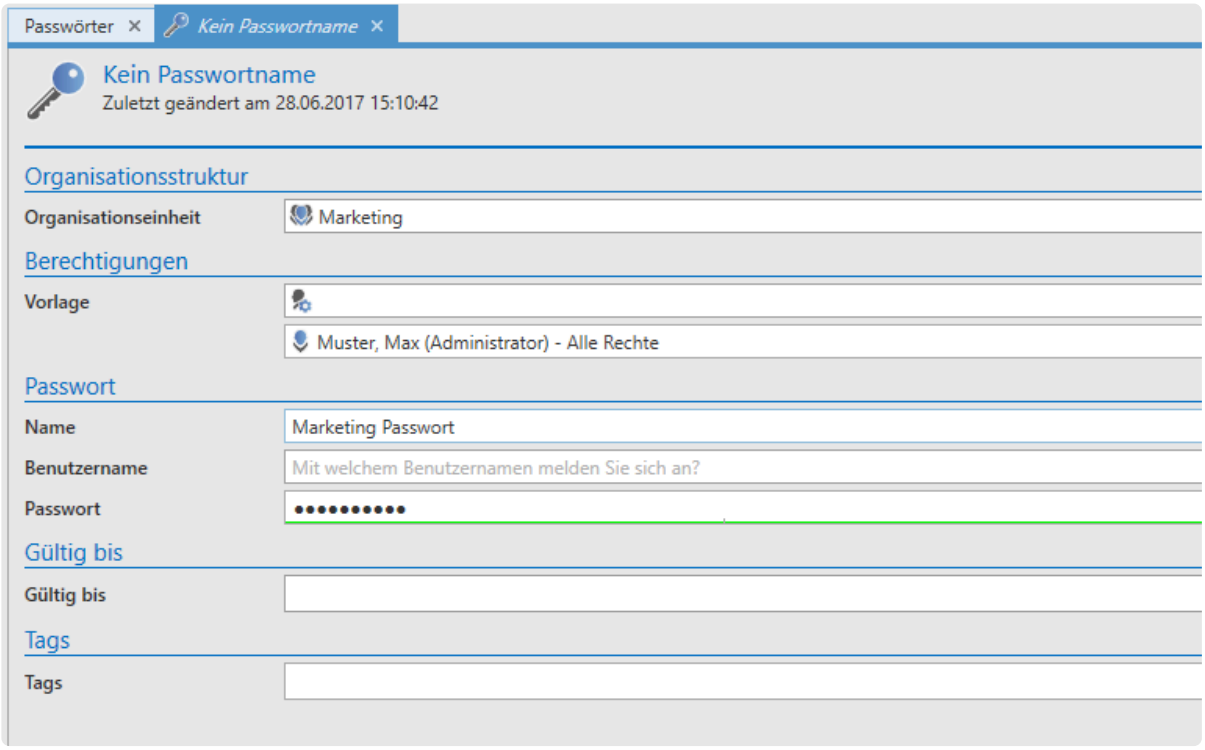
Es wird also nicht über die komplette Struktur nach unten durch vererbt.

Fallbeispiel

Betrachtet wird 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.



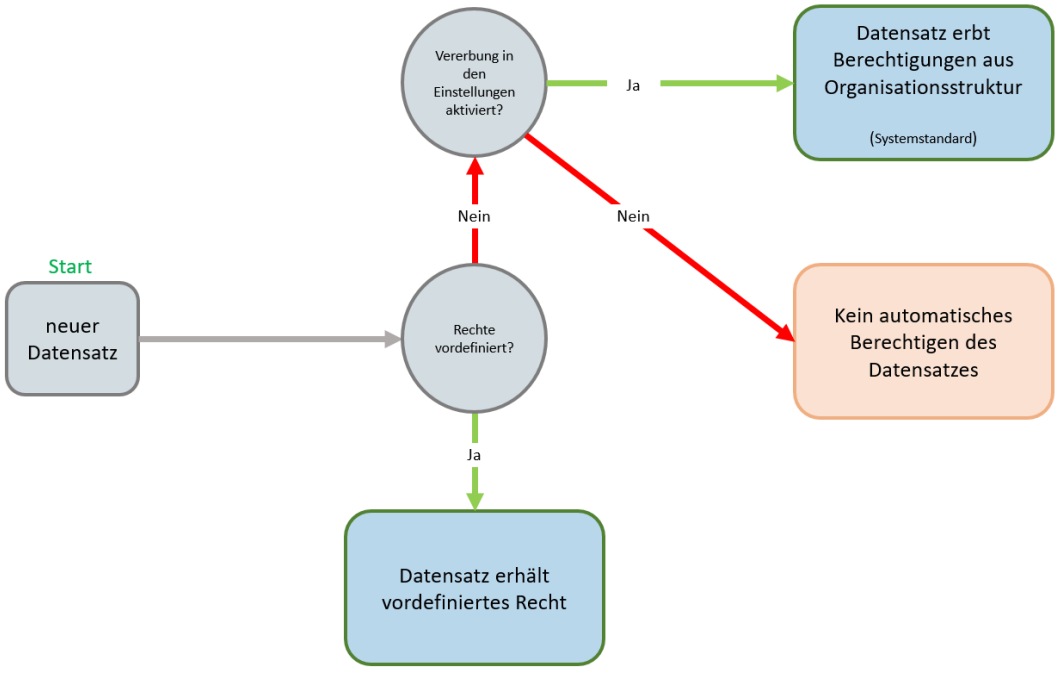
Wichtig ist, dass für diese Organisationseinheit **kein** Preset definiert ist. Betrachtet werden sollen nun die Berechtigungen auf den soeben erstellten Datensatz.

Fazit

Nutzen Sie beim Anlegen neuer Objekte die Berechtigung des “Ablageortes”. 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 für jeden Datensatz separat erfolgen. Obwohl Sie auf diese Art und Weise sehr granular jede angedachte Berechtigungsstruktur abdecken können, ist dies nicht wirklich effizient, da der Konfigurationsaufwand zu hoch ist.
Rechte vordefinieren ist eine Funktion, die, durch die Nutzung von Automatismen, Ihnen die Vergabe von Berechtigungen erleichtert . Nach deren Konfiguration widmen sich separate Kapitel dem **Arbeiten mit vordefinierten Rechten** sowie deren **Geltungsbereich**.

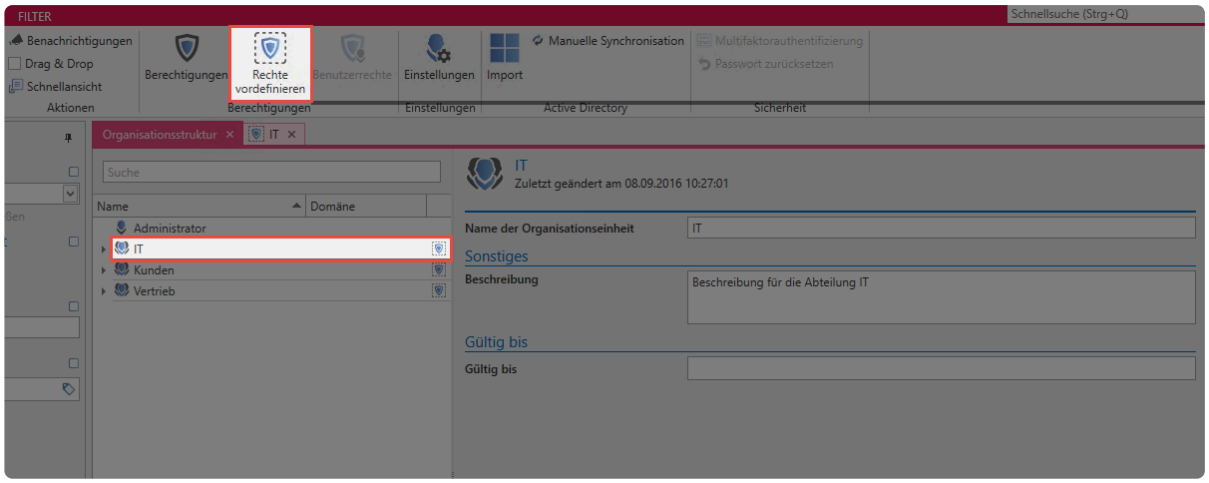
Organisationsstrukturen als Basis

Organisationsstrukturen sind in Password Safe in vielerlei Hinsicht sehr nützlich. Im vorliegenden Beispiel erstellen Sie das Grundgerüst, auf dem die automatische Rechtevergabe fußt. Im weitesten Sinne sollten Sie diese Organisationsstrukturen stets gemäß der vorhandenen Abteilungen in einem Unternehmen anlegen. Im nachfolgenden Beispiel wird im Speziellen eine IT-Abteilung betrachtet.. Innerhalb dieser IT-Abteilung sind folgende 3 Hierarchien (**Rollen**) gegeben:

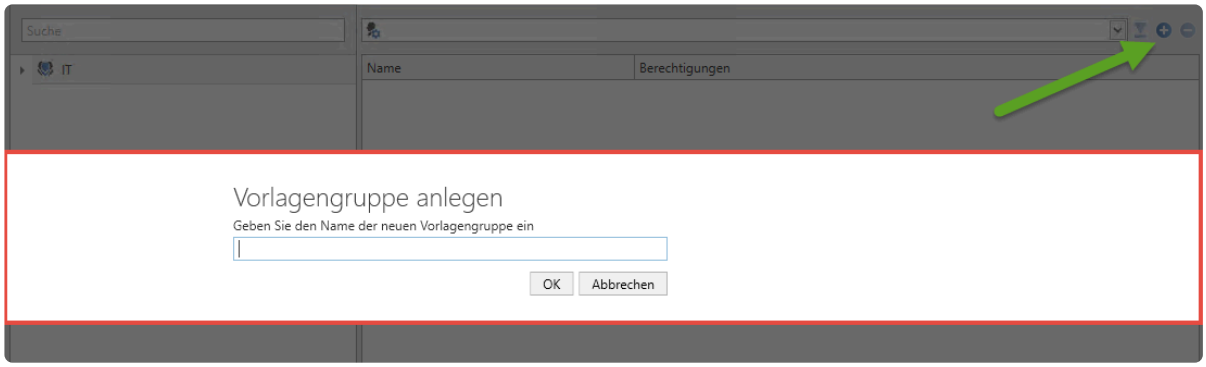
- **IT-Mitarbeiter**
- **IT-Leitung**
- **Administratoren**

Rechte vordefinieren

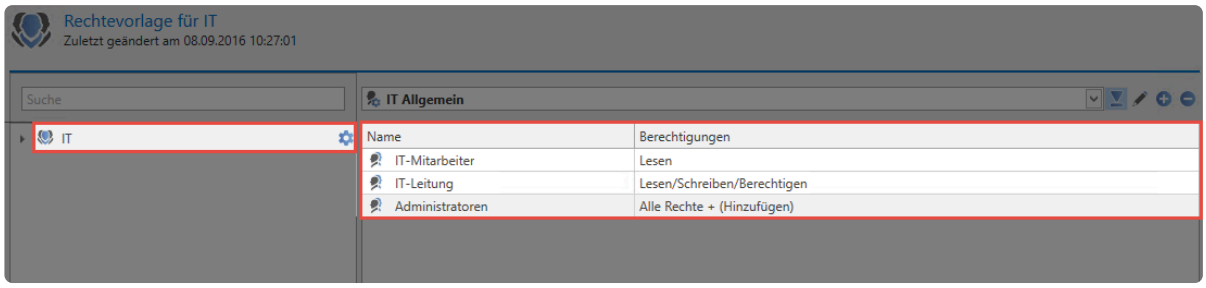
In der Regel ist ein höher gestellter, leitender Angestellter mit umfangreicheren Rechten ausgestattet. Diese Hierarchie und die damit verbundenen Berechtigungsstrukturen können Sie vordefinieren. Im Modul **Organisationsstruktur** wählen Sie nun die OU (Abteilung) aus, für welche die Rechte vordefiniert werden sollen. Nun klicken Sie auf **Rechte vordefinieren** in der Ribbon.



Erstellen der ersten Vorlagengruppe: Über das “**+**”-Icon zum Hinzufügen neuer Vorlagengruppen (grüner Pfeil) erscheint ein Fenster, bei dem Sie einen Namen für die Vorlagengruppe definieren.

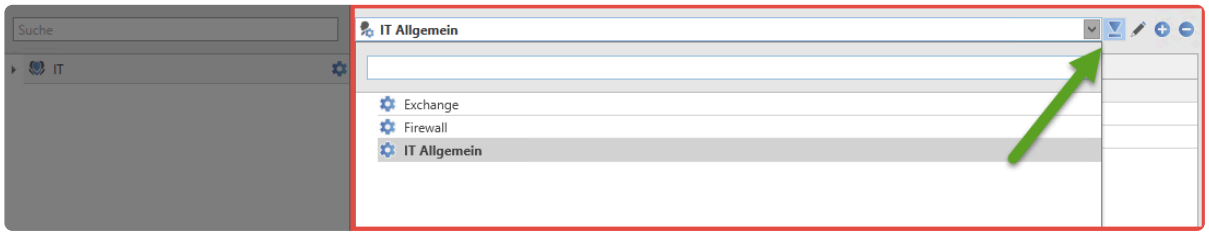


Sowohl über die Ribbon als auch über das Kontextmenü (rechte Maustaste) können Sie nun Rollen und Benutzer in diese Vorlage übernehmen. Dies wurde im nächsten Schritt bereits durchgeführt. Die Rolle **IT-Mitarbeiter** ist lediglich lesend berechtigt, die **IT-Leitung** besitzt zudem Schreibrechte, sowie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



Hinzufügen weiterer Vorlagengruppen

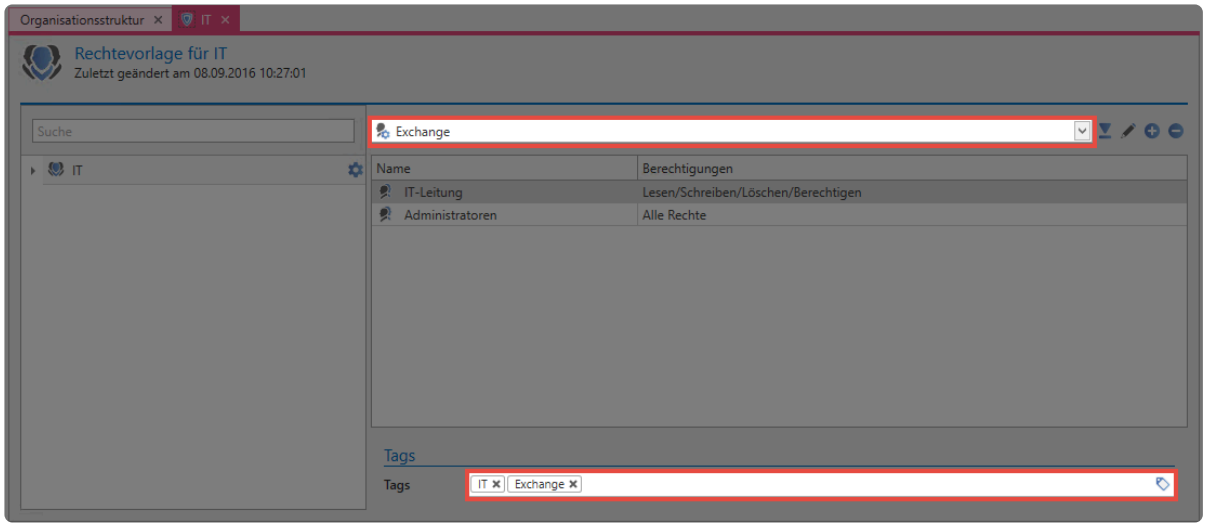
Auch innerhalb einer Abteilung können mehrere, unterschiedliche Rechtevorlagen konfiguriert werden. Nachfolgend sind neben dem Bereich **IT-Allgemein** noch die Vorlagengruppen **Exchange** sowie **Firewall** definiert.



Direkt neben dem Dropdown Menü für die Auswahl der Vorlagengruppe können Sie eine **Standard-Vorlagengruppe** definieren (grüner Pfeil). Das bedeutet, dass diese immer angewendet wird, wenn die OU “IT” ausgewählt wird.

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.

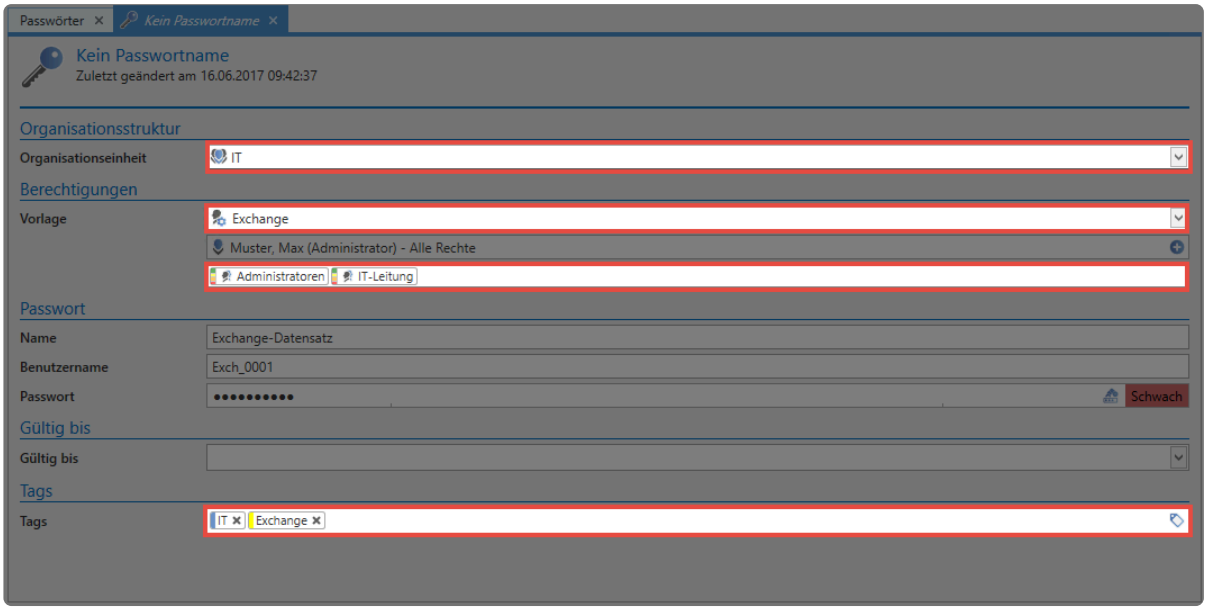
Arbeiten mit vordefinierten Rechten

Nutzung von vordefinierten Rechten beim Erstellen von Passwörtern

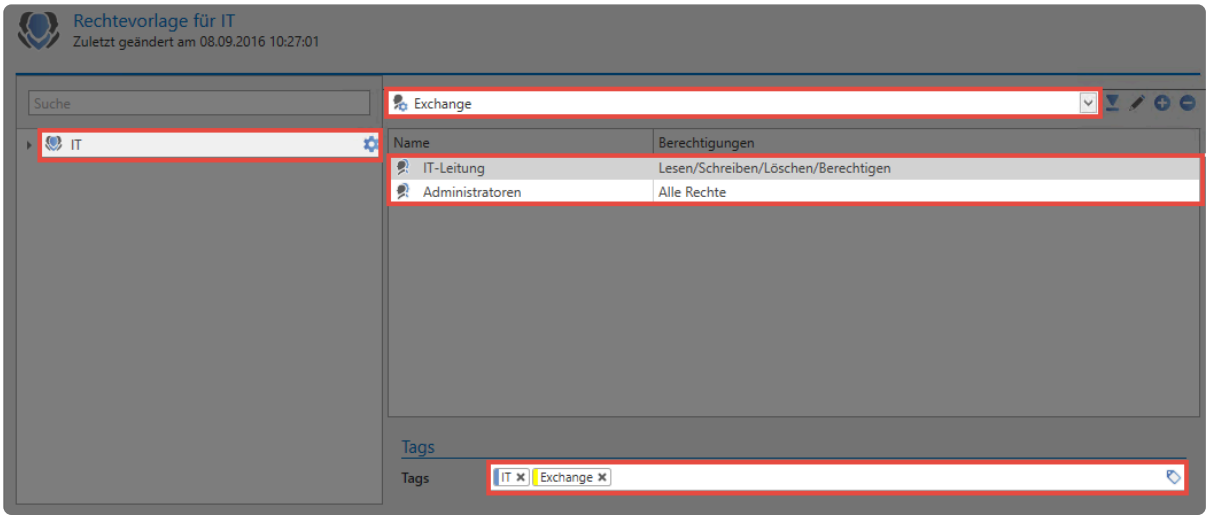
Nachdem Sie Rechte vorkonfiguriert haben, können diese beim Erstellen von neuen Datensätzen ausgewählt werden. Gehen Sie dazu wie folgt vor:

- Wählen Sie das Modul “Passwörter” aus
- Klicken Sie in der Ribbon auf “Neu” bzw. “NEU Formular auswählen”
- Wählen Sie dann ggf. ein Formular aus

In unserem Beispiel wurde daraufhin die Organisationseinheit “IT” sowie die Berechtigungsvorlage “Exchange” ausgewählt.



Zum Vergleich hier die hinterlegte Rechtevorlage:



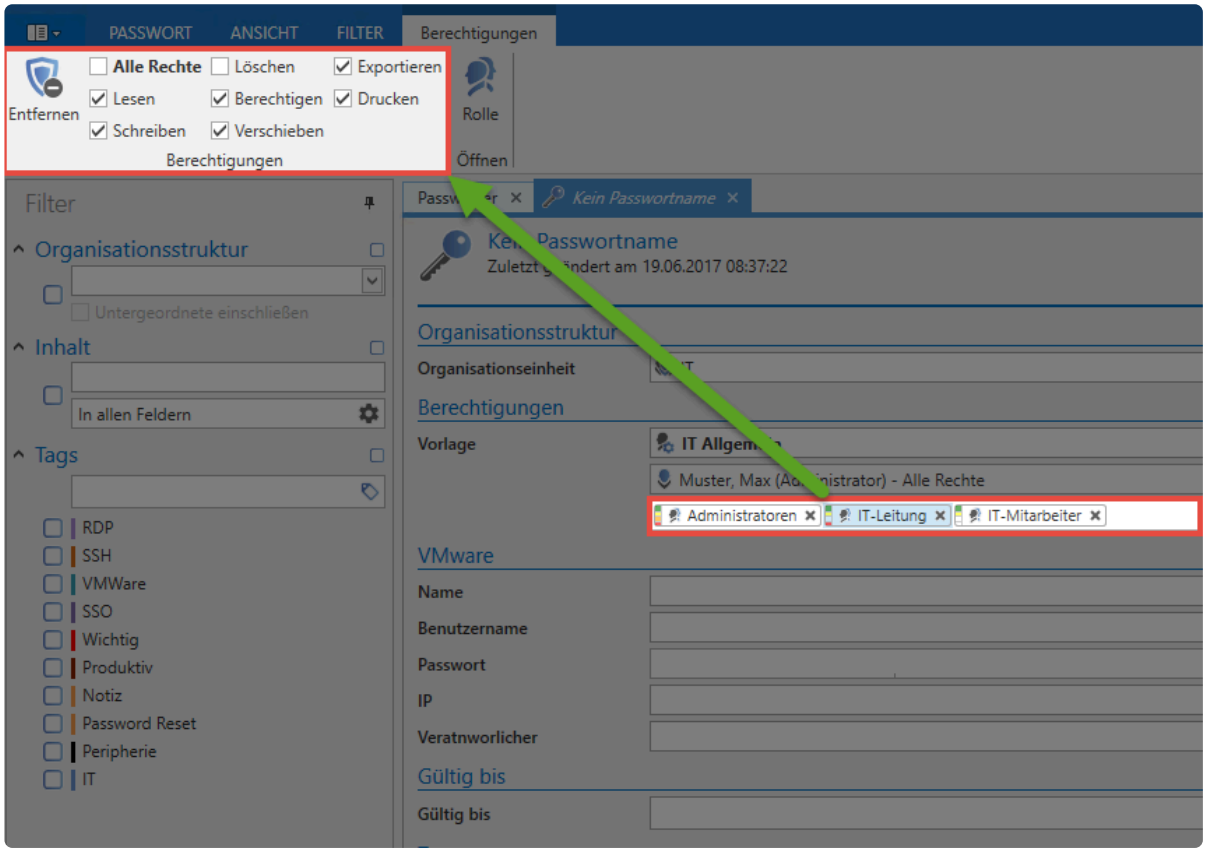
Es ist ersichtlich, dass durch das Auswählen der Organisationseinheit “IT”, gemäß den in der Rechtevorlage konfigurierten Rechten, die Rollen “IT-Leitung” und “Administratoren” berechtigt werden. **Ebenso werden die hinterlegten Tags “IT” und “Exchange” gesetzt**.

Vorschau auf zu setzende Berechtigungen

Beim Einsatz von Rechtevorlagen können Sie mit Hilfe einer **Farbtabelle** die zu erteilenden Berechtigungen sehr schnell erkennen. Die tatsächlichen Berechtigungen können Sie wie gewohnt zusätzlich über die Ribbon einsehen. Nachfolgend die Aufschlüsselung der Farben mit den zugehörigen Berechtigungen:

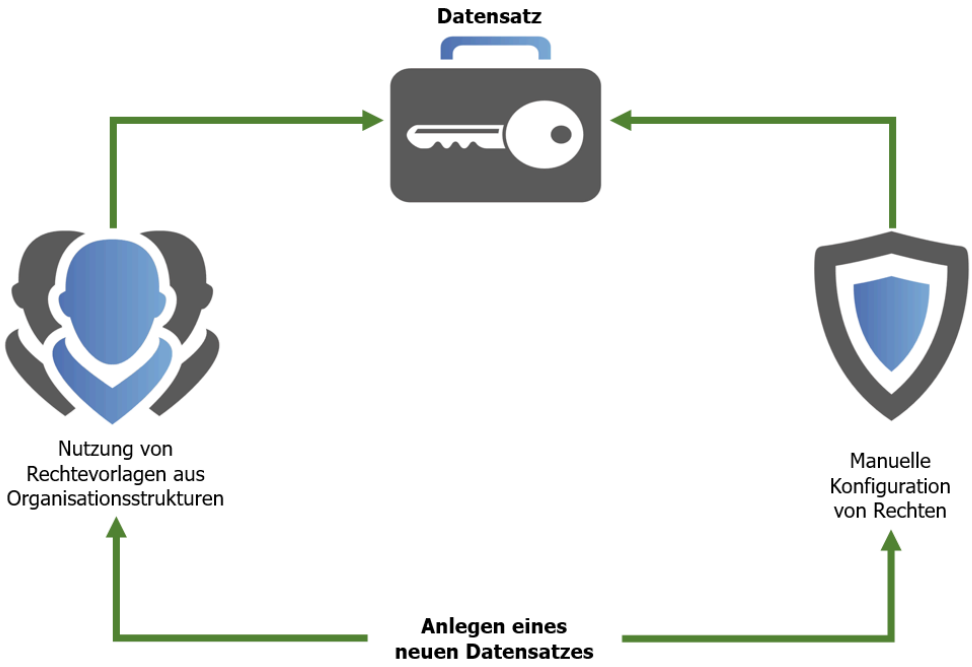
Farbe	Berechtigung
Grün	Lesen
Gelb	Schreiben
Orange	Löschen
Rot	Berechtigen

Darüber hinaus gibt es noch weitere Rechte, welche jedoch nicht separat mit einer Farbe versehen sind. Ob die Rechte “Verschieben”, “Exportieren” und “Drucken” gesetzt sind oder nicht, können Sie direkt in der Übersicht in der Ribbon einsehen. 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 Ihnen die Konfiguration von Rechten sowohl auf bestehende als auch auf neue Datensätze. Die Möglichkeit Rechte vorzudefinieren bietet hier einen sehr praktischen Automatismus. Statt für jeden Datensatz Berechtigungen separat zu vergeben, definieren Sie für jede Organisationsstruktur einmalig ein “Preset”. Wählen Sie zukünftig lediglich die Organisationsstruktur beim Erstellen eines Datensatz aus. Die Berechtigungen werden automatisch gesetzt. Besonders vorteilhaft ist dieses Vorgehen dann, wenn Benutzer die Berechtigungen nicht selbst setzen sollen.

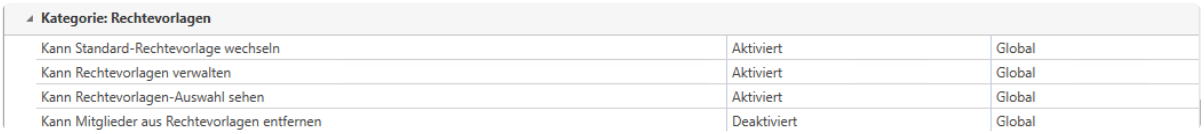


! Die Konfiguration von Berechtigungen für neue Passwörter kann entweder automatisch oder manuell erfolgen. Bereits gesetzte Berechtigungen können nur manuell geändert werden.

Relevante Benutzerrechte

Benutzerrechte für vordefinierte Rechte

Im Kapitel Benutzerrechte wurde der Umgang mit Benutzerrechten grundlegend erläutert. Nachfolgend wird auch noch auf die vier im Zusammenhang mit “Rechte vordefinieren” existierenden Benutzerrechte eingegangen.



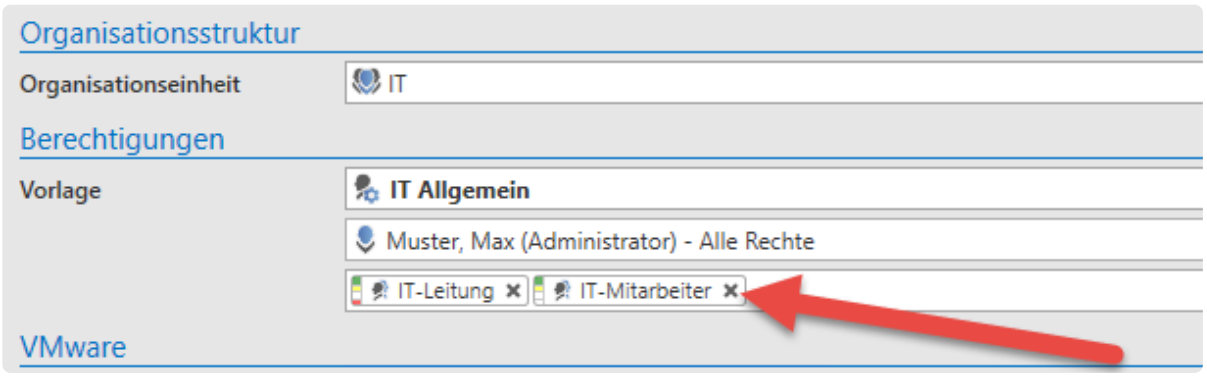
Kategorie: Rechtevorlagen		
Kann Standard-Rechtevorlage wechseln	Aktiviert	Global
Kann Rechtevorlagen verwalten	Aktiviert	Global
Kann Rechtevorlagen-Auswahl sehen	Aktiviert	Global
Kann Mitglieder aus Rechtevorlagen entfernen	Deaktiviert	Global

- **Kann Standard-Rechtevorlagen wechseln:** Bei der Auswahl der Rechtevorlage können Sie diverse Rechtevorlagegruppen auswählen. Um hier abweichend von der Standard-Vorlage andere Vorlagen auswählen zu können, benötigen Sie das Recht “Kann Standard-Rechtevorlagen wechseln”. Ohne dieses Recht kann nur die Standard-Vorlage verwendet werden.

- **Kann Rechtevorlagen verwalten:** Hier kann der Benutzer 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.

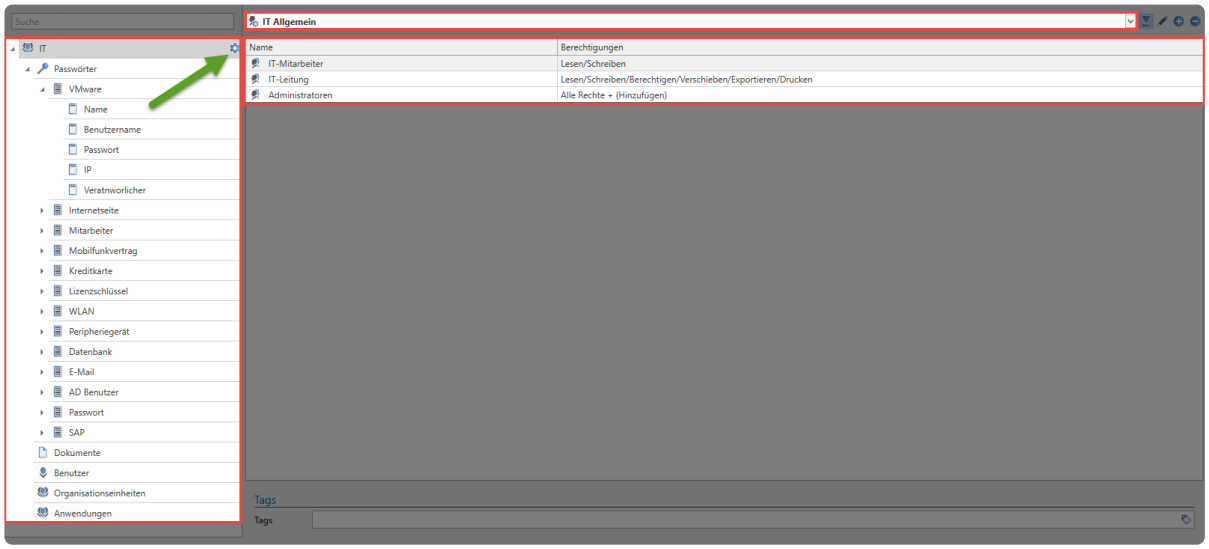
- **Kann Rechtevorlagen-Auswahl sehen:** Dieses Recht bestimmt, ob beim Erstellen neuer Datensätze die Rechtevorlagen-Auswahl angezeigt wird oder nicht. Ohne das Recht ist nicht ersichtlich, für welche Rollen und Benutzer Benutzerrechte definiert werden.

- **Kann Mitglieder aus Rechtevorlagen entfernen:** Ohne dieses Recht können die innerhalb von Rechtevorlagen definierten Rollen nicht entfernt werden. Diese sind dann stets auf Datensätze dieser Organisationsstruktur berechtigt. Mit aktiviertem Benutzerrecht: Man kann Rollen nun über das x-Icon entfernen:



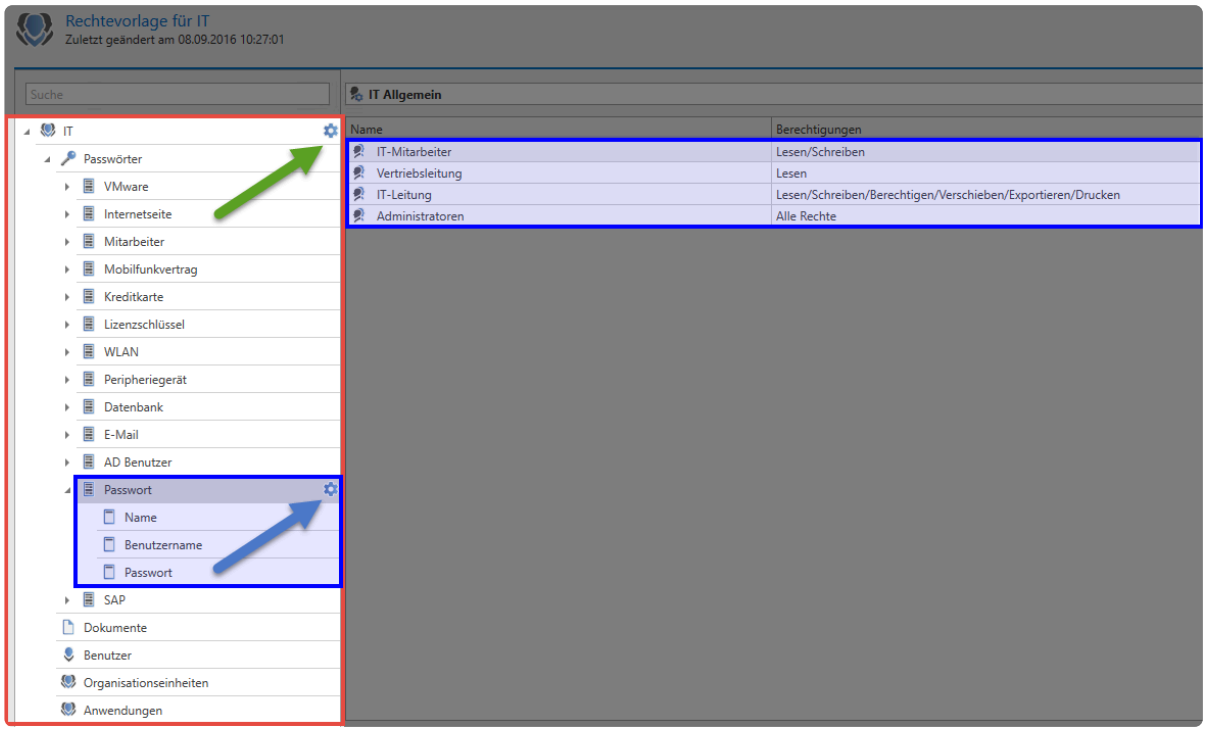
Geltungsbereich vordefinierter Rechte

Alle für eine Organisationsstruktur vordefinierten Berechtigungen werden auf alle darunterliegenden Objekte angewandt. Das 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 bei der entsprechenden Organisationseinheit ein stilisiertes Zahnrad(= grüner Pfeil). Da unterhalb dieser Ebene keine weiteren Icons existieren, gilt das “Preset” auch für alle darunterliegenden Objekte.

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



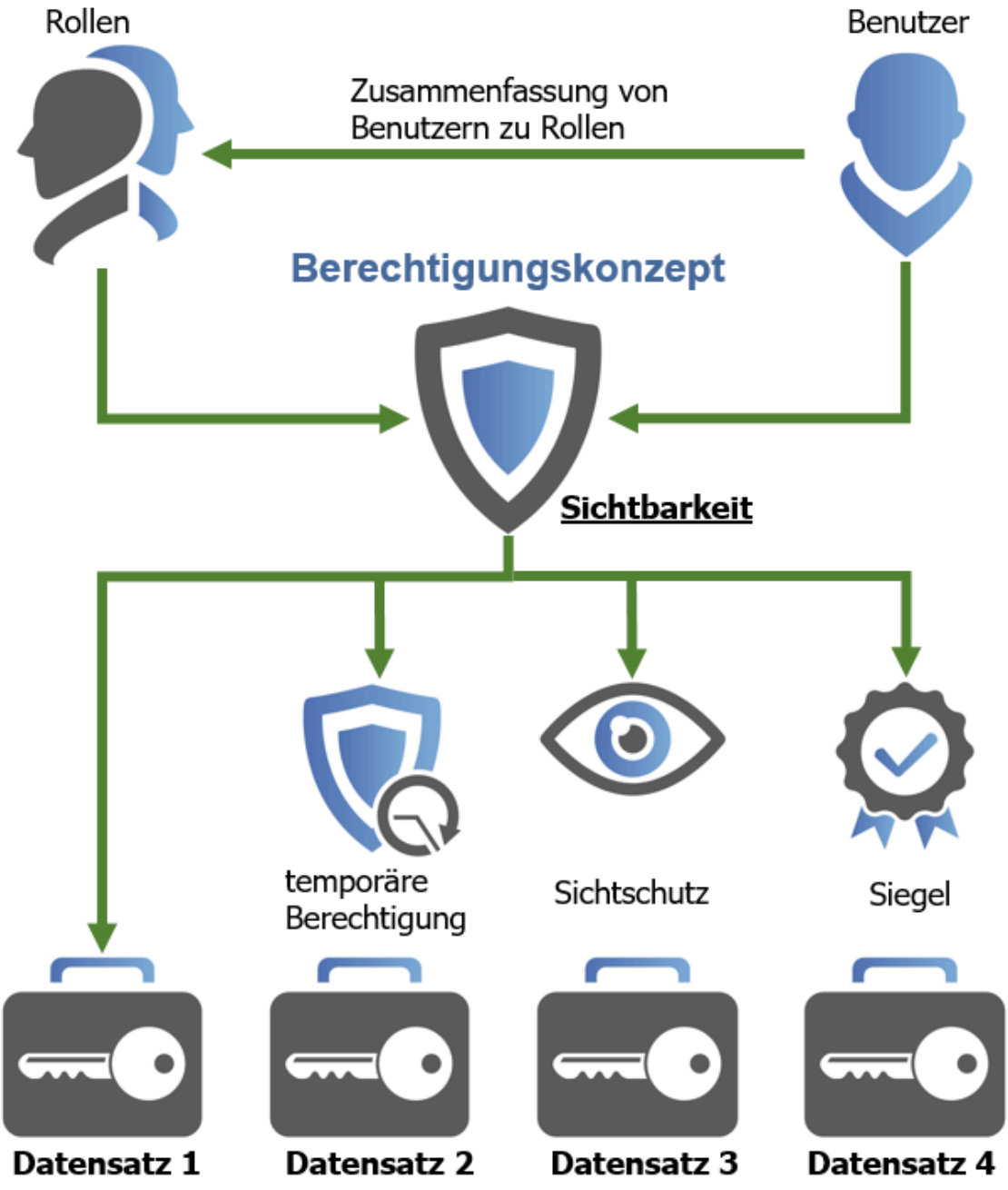
Das Preset “IT Allgemein” behält für alle Objekte weiterhin seine Gültigkeit. Eine Ausnahme bildet das Formular “Passwort”. Für dieses wurde ein eigenes Preset definiert (blauer Pfeil). Alle mit dem Formular “Passwort” erstellten Datensätze werden daher wie definiert berechtigt (inkl. der Vertriebsleitung).

Schutzmechanismen

Was sind Schutzmechanismen?

Die Sicherheit Ihrer Daten ist das oberste Ziel von Password Safe. Neben dem **Berechtigungskonzept** als wichtigste Komponente, bei dem Benutzer auf Datensätze berechtigt werden, gibt es auch noch weitere Schutzmechanismen.

- Legen Sie mittels dem Leserecht die **Sichtbarkeit** eines Datensatzes für bestimmte Benutzer fest.
- Dank **temporärer Berechtigungen** erhalten Benutzer oder Rollen nur zeitlich befristet Zugriff auf Datensätze.
- Dank des **Sichtschutzes** bleiben Passwörter verborgen und können nicht eingesehen werden.
- Mehr-Augen-Prinzip zur Freigabe von Datensätzen mittels **Siegel**.



Kombination mehrerer Schutzmechanismen

Sie können mehrere Schutzmechanismen miteinander kombinieren. Dafür muss der Datensatz für den Benutzer sichtbar sein. Beispielsweise ist ein temporär gewährter Zugriff auf einen sichtgeschützten Datensatz genauso möglich, wie ein sichtgeschützter Datensatz, der zusätzlich durch ein Mehr-Augen-Prinzip gesichert wird. **Bitte beachten Sie, dass temporäre Freigaben in Kombination mit Siegeln stets eine Gefahr darstellen**. Wenn für die Freigabe von Siegeln die Zustimmung einer Person notwendig ist, die nur temporäre Berechtigungen besitzt oder besessen hat, kann dies mit konfigurierten Freigabekriterien kollidieren.

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

Sichtbarkeit

Sichtbarkeit von Daten

In der Regel werden Datensätze über den **Filter** dargestellt. Dabei sehen Sie nur die Datensätze, auf welche Sie **mindestens lesend berechtigt** sind.

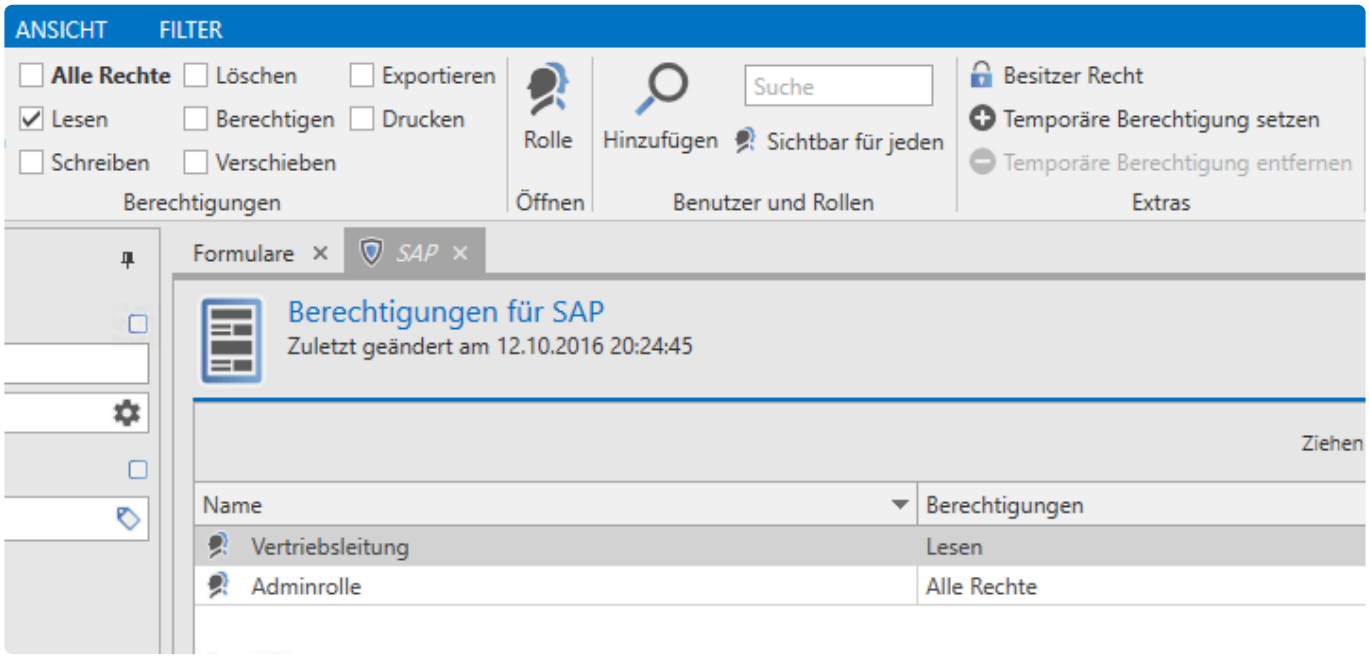
Tags unterliegen keinen Berechtigungen. Diese können von allen Benutzern als Filterkriterium verwendet werden. Aber auch hier sehen Sie nur die Datensätze, auf die Sie berechtigt sind.

Beispiel
Es gibt einen Tag **persönlicher Datensatz**, der für jeden Benutzer verfügbar ist. Jeder Benutzer kann seine eigenen Datensätze damit markieren. Über den Filter werden dem Benutzer aber nur seine eigenen persönlichen Datensätze angezeigt.

Eigenständige Arbeitsumgebungen

Ganz egal ob Datensätze, Dokumente, Organisationsstrukturen oder Rollen und Formulare: Sie können stets definieren, welcher Benutzer oder Rolle auf ein Objekt Leserechte besitzen. Jedes dieser Objekte kann über den Berechtigungsdialog in der Ribbon separat berechtigt werden. Diese ermöglicht die Erstellung von eigenständigen Arbeitsumgebungen innerhalb einer Datenbank. Sie können also Abteilungen, Teams, Standort usw. abbilden – ganz nach Ihren Anforderungen.

Beispiel
Hier ist die Berechtigungsstruktur des Formulars SAP zu sehen. Dieses Formular kann ausschließlich durch die Vertriebsleitung und die Administratoren eingesehen und verwendet werden, um neue Datensätze vom Typ SAP zu erstellen. Die Administratoren können das Formular zudem in vollem Umfang bearbeiten.



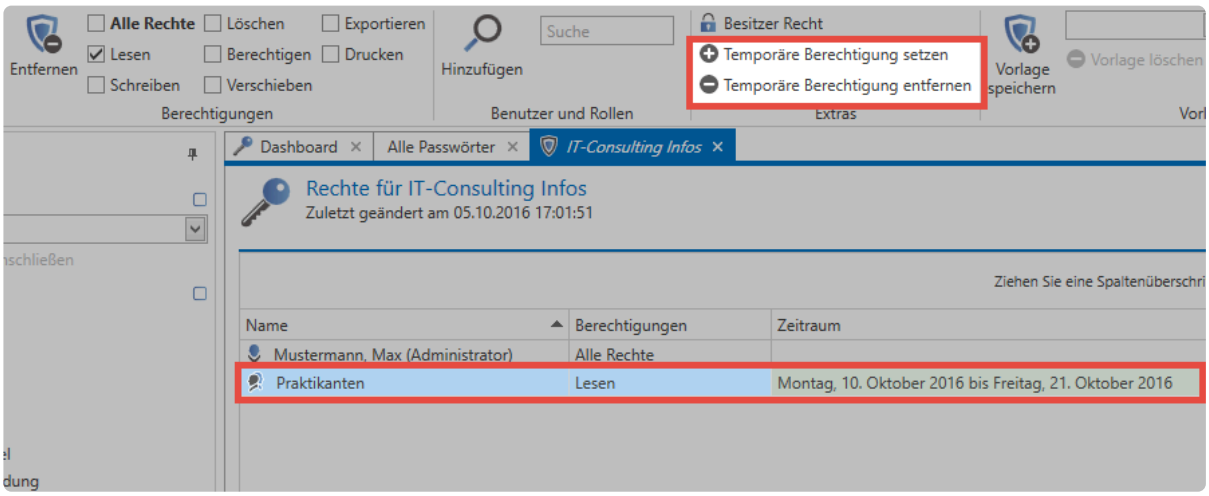
Grundsätzlich kann auf diese Art und Weise jede Abteilung eigenständig Formulare nutzen, Passwörter erstellen und Hierarchien verwalten. Besonders in sehr sensiblen Unternehmensbereichen ist eine derartige Abschottung oftmals erforderlich und auch erwünscht.

Eine Alternative wäre es, für jede Abteilung eine eigene Datenbank zu erstellen. Die physikalische Trennung der Daten ist jedoch deutlich aufwändiger zu verwalten.

Temporäre Berechtigungen

Konfiguration

Die **Berechtigungen auf Datensätze** lassen sich für jeden Benutzer oder Rolle zeitlich begrenzen. Klicken Sie in der Ribbon im Bereich “Extras” auf “Temporäre Berechtigungen setzen” und legen Sie anschließend ein Startdatum und ein Enddatum fest.



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 in der Zukunft.
- **Grün:** Die temporäre Berechtigung ist aktiv.
- **Rot:** Die temporäre Berechtigung ist bereits abgelaufen. Der Zeitraum liegt in der Vergangenheit

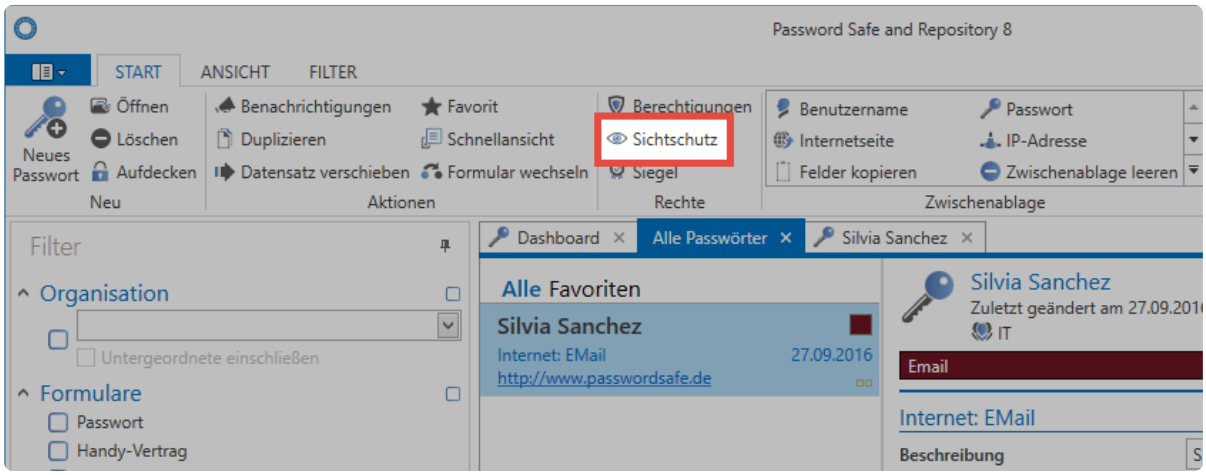
Vergeben Sie temporäre Berechtigungen auch auf mehrere Rollen und Benutzer gleichzeitig mittels Strg/Shift + linke Maustaste.

Es muss immer mindestens ein Benutzer das Recht “Berechtigen” auf einen Datensatz besitzen, ohne dass die Berechtigung nur temporär ist.

Sichtschutz

Was ist der Sichtschutz?

Die sichersten Passwörter sind diejenigen, die man nicht kennt. Genau diesen Ansatz verfolgt der Sichtschutz. Er verhindert, dass ein Passwort aufgedeckt – sprich sichtbar – wird. Dennoch kann es Dank automatischer Eintragungen verwendet werden.



Relevante Rechte

Sie benötigen folgende Optionen zum Anbringen des Sichtschutzes:

Benutzerrecht

- Kann Sichtschutz anbringen

Benötigte Berechtigungen

Analog zur Siegelkonfiguration ist das Recht **Berechtigen** auf den Datensatz Voraussetzung, um den Sichtschutz anbringen bzw. wieder entfernen zu können. Nach Anbringen können alle Benutzer mit diesem Recht den Datensatz trotz Sichtschutz weiter normal verwenden. Nur Benutzer ohne das Recht können das Passwort nicht mehr einsehen.

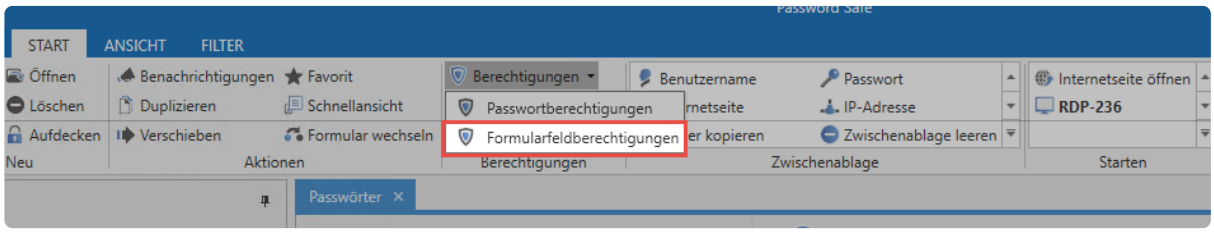
> Ein Sichtschutz kann nur auf Datensätze mit vorhandenem Passwort angewendet werden!

Anbringen des Sichtschutzes

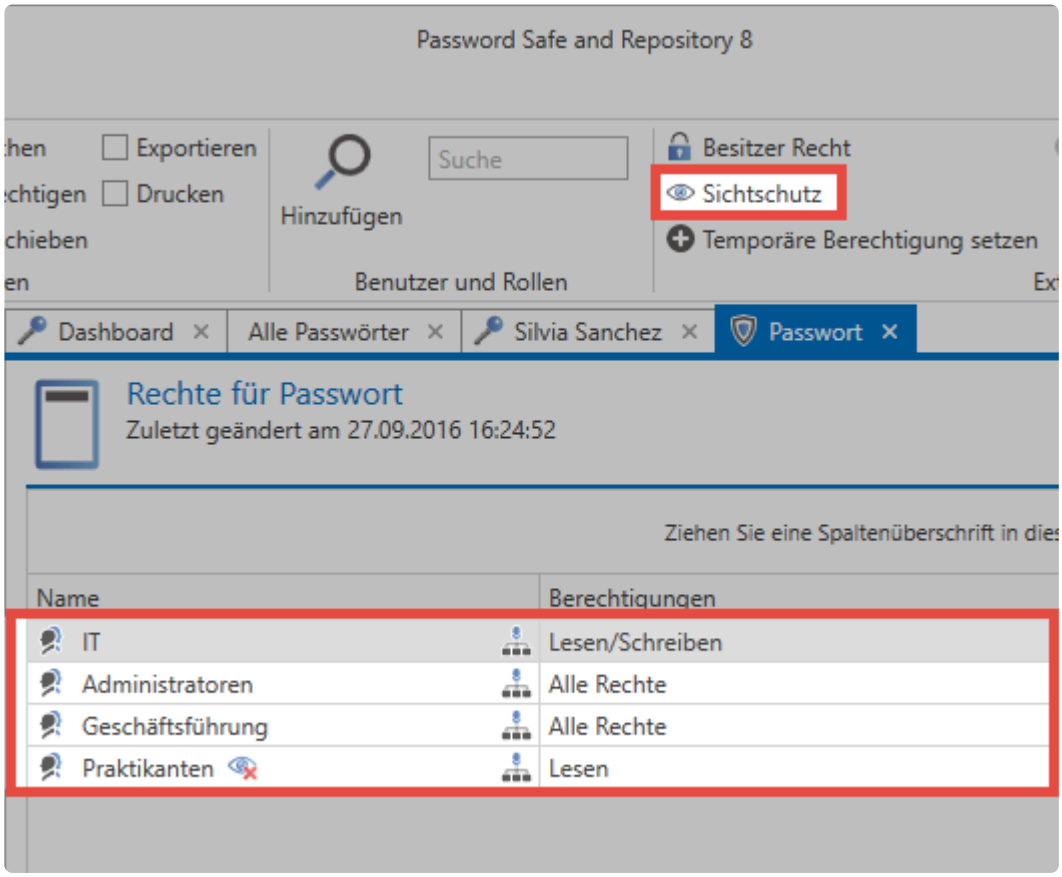
Über das Icon in der Ribbon können Berechtigte den Sichtschutz nach einer Sicherheitsabfrage anbringen. Standardmäßig gilt der Sichtschutz für all diejenigen, die mindestens Leseberechtigung besitzen, jedoch nicht das Recht **Berechtigen**.

Sichtschutz über Formularfeldberechtigungen

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



Beim Setzen oder Bearbeiten des Sichtschutzes über die Formularfeldberechtigungen können Sie individuell entscheiden, für wen der Sichtschutz gelten soll. Im folgenden Beispiel wurde der Sichtschutz nur für die Rolle “Praktikanten* definiert, obwohl die Rolle “IT” das Recht **Berechtigen** ebenfalls nicht besitzt. Neben dem Namen der Rolle oder des Benutzers symbolisiert ein Icon, dass für Praktikanten der Sichtschutz gilt.



> Über das Icon in der Ribbon wird der Sichtschutz auf alle Benutzer mit Leseberechtigung jedoch ohne das Recht **Berechtigen** auf den Datensatz angewandt. Wollen Sie genauer definieren, für wen der Sichtschutz gelten soll, ist dies zusätzlich über die **Formularfeldberechtigungen** möglich.

Beachten Sie, dass die Anmeldemaske bei Datensätzen mit Sichtschutz **automatisch abgesendet wird**, auch wenn die Einstellung „**Browser Addons: Loginmaske automatisch absenden**“ **deaktiviert** ist.

Der Sichtschutz gilt nur für die Benutzer, die zum Zeitpunkt der Anbringung auf den Datensatz berechtigt sind. Ist ein Datensatz sichtgeschützt und ein weiterer Benutzer wird **ohne** das **Berechtigen Recht** darauf berechtigt, so ist der Datensatz für diesen Benutzer **nicht geschützt**. Der Sichtschutz sollte dann also entfernt und neu gesetzt werden.

Siegel

Ein Siegel ist Schutzmechanismus, bei dem Passwörter mittels Mehr-Augen-Prinzip geschützt sind. Erst nach Freigabe durch berechtigte Personen kann ein Passwort eingesehen werden. Neben dem Berechtigungskonzept es ist eine zusätzliche wirksame Methode, sensible Passwörter vor unberechtigtem Zugriff zu schützen.

Relevante Rechte

Folgende Optionen werden benötigt, um ein Siegel einzurichten.

Benutzerrecht

- Kann Siegel anlegen

Benötigte Berechtigungen

Um ein Siegel einzurichten benötigen Sie zwingend das Recht **Berechtigen** auf den Datensatz. Darüber benötigt man das Leserecht auf alle Benutzer und Rollen, die vom Siegel betroffen sind. Die Konfiguration von Sichtbarkeit und Berechtigungen auf Datensätze wird im Kapitel Berechtigungskonzept erklärt.

Was wird genau versiegelt?

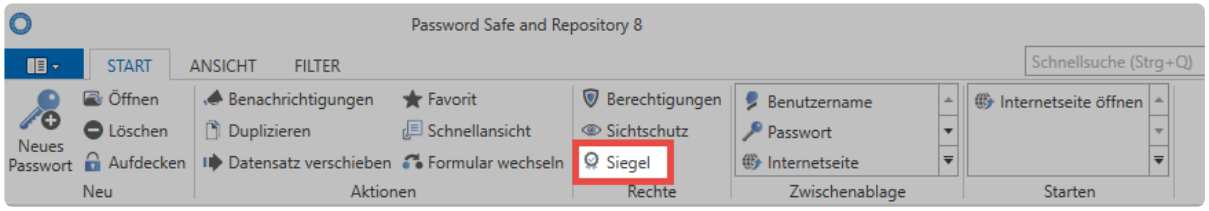
Technisch gesehen wird nicht das Passwort selbst versiegelt. Es ist das Recht, ein Passwortfeld einzusehen, das durch ein Siegel geschützt wird. Damit ist es beispielsweise möglich, dass eine Gruppe das Passwort ohne Einschränkungen benutzen kann, während für die andere Benutzergruppe das Passwort versiegelt ist. Der Assistent unterstützt Benutzer beim Einrichten von Siegeln.

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

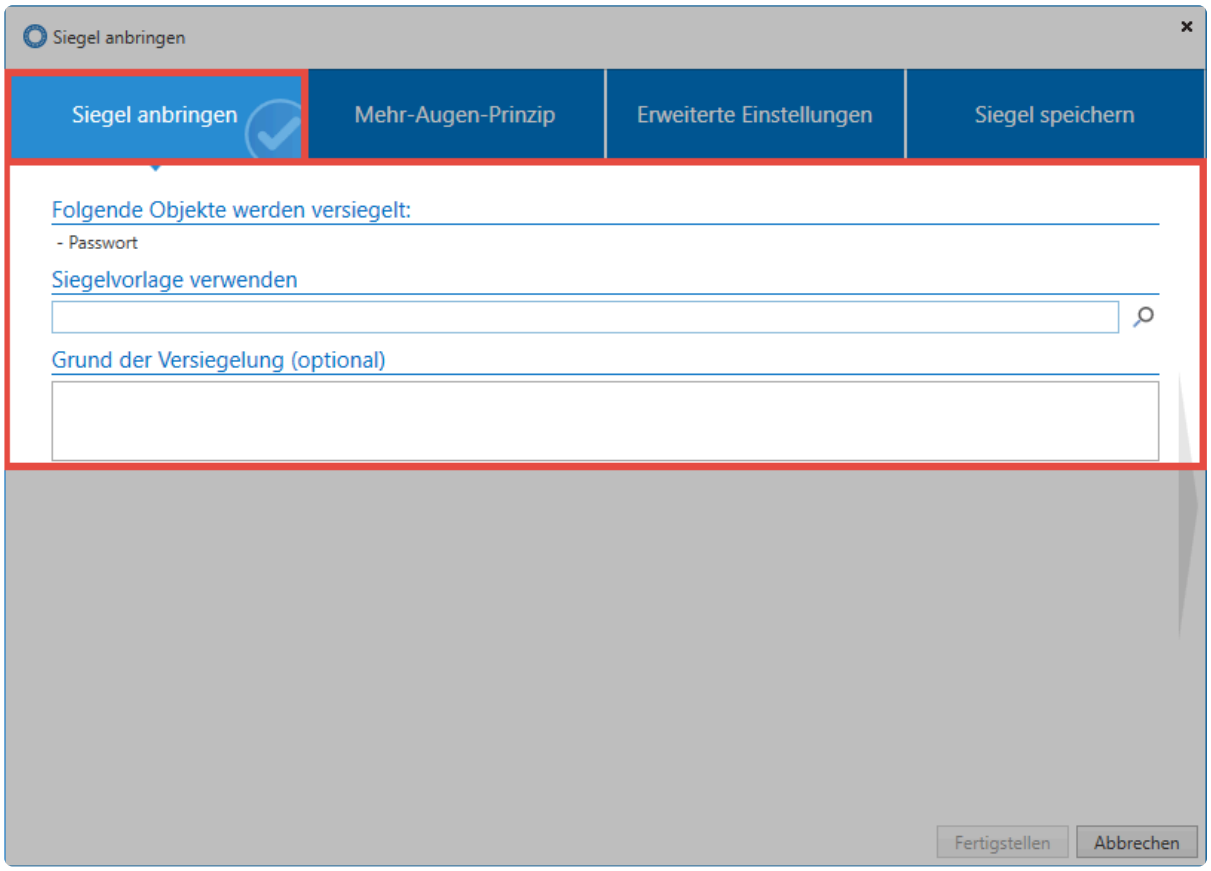
> ! Nur Datensätze mit einem Passwort können versiegelt werden!

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



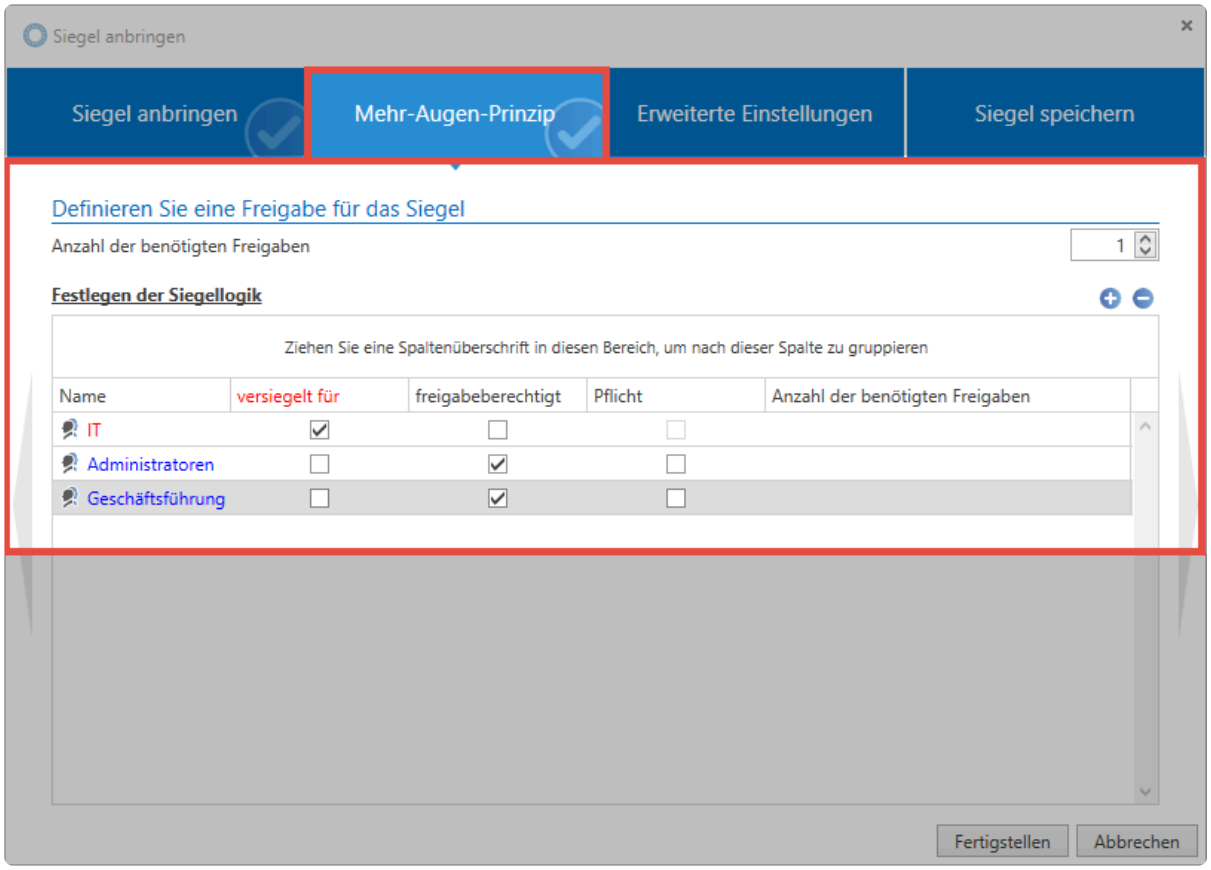
1. Siegel anbringen



Zuerst werden alle Objekte angezeigt, die versiegelt werden sollen. Das können je nach Datensatz ein oder auch mehrere Passwortfelder sein. Hier können Sie auch auf bereits bestehende Siegelvorlagen zurückgreifen. Optional kann für jedes Siegel eine Begründung eingegeben werden.

2. Mehr-Augen-Prinzip

Hier wird definiert, welche Benutzer oder Rollen zukünftig den Datensatz versiegelt vorfinden und wer für die Freigabe berechtigt ist. Dabei werden alle Benutzer / Rollen, für die der Datensatz versiegelt ist, 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.

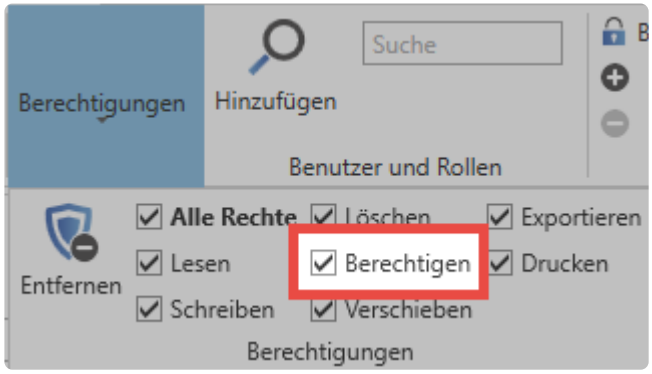
Um nicht jede Konfiguration manuell durchführen zu müssen, werden Rollen und Benutzer direkt aus den Berechtigungen des Datensatzes übernommen. Zum Vergleich die **“Berechtigungen”** für den Datensatz (einsehbar über die Ribbon).

Im Regelfall ist es gewünscht, dass Vorgesetzte die Freigaben für ihre Mitarbeiter vergeben. Daher folgt die Siegellogik auch den vorhandenen Berechtigungen und folgendes **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

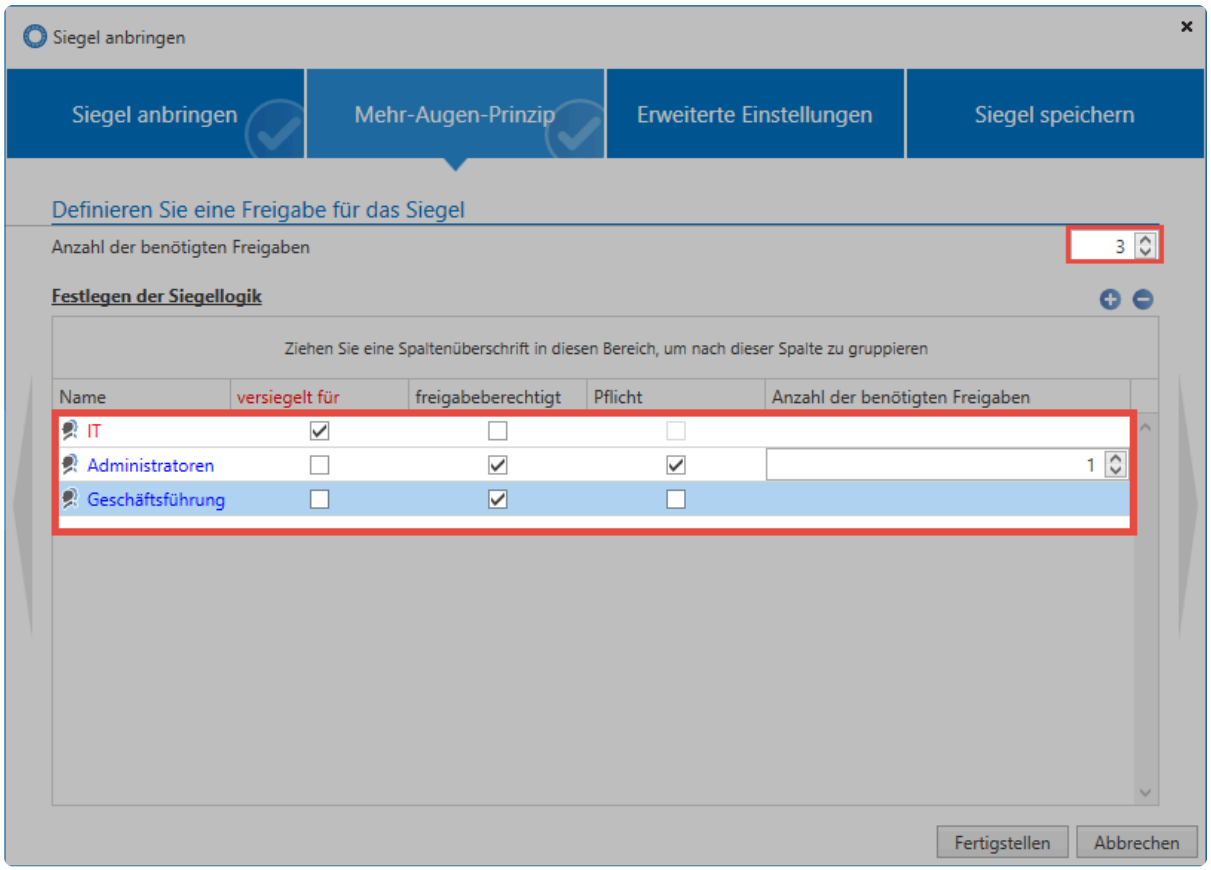
> das Recht “Berechtigen” auf den Datensatz nicht besitzen, werden direkt in der Spalte **“versiegelt für”** übernommen.

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

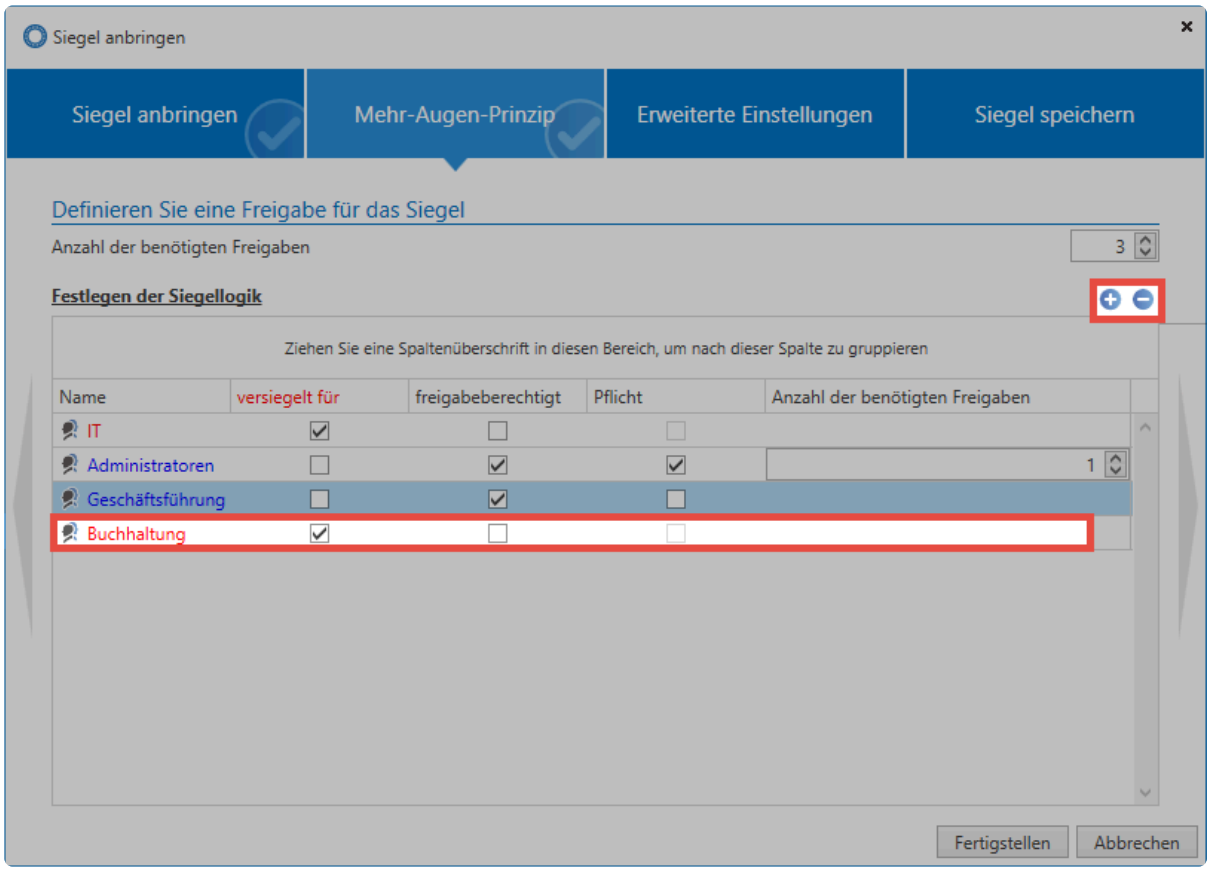


Anpassungen der Siegellogik

Bei Bedarf können Sie die Siegellogik auch anpassen. 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 das Siegel brechen zu können **(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 von bestehenden Berechtigungen auf den Datensatz abhängig zu sein, können Sie auch weitere Benutzer dem Siegel hinzufügen. Nachfolgend wurde die Rolle Buchhaltung unter “versiegelt für” hinzugefügt.



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

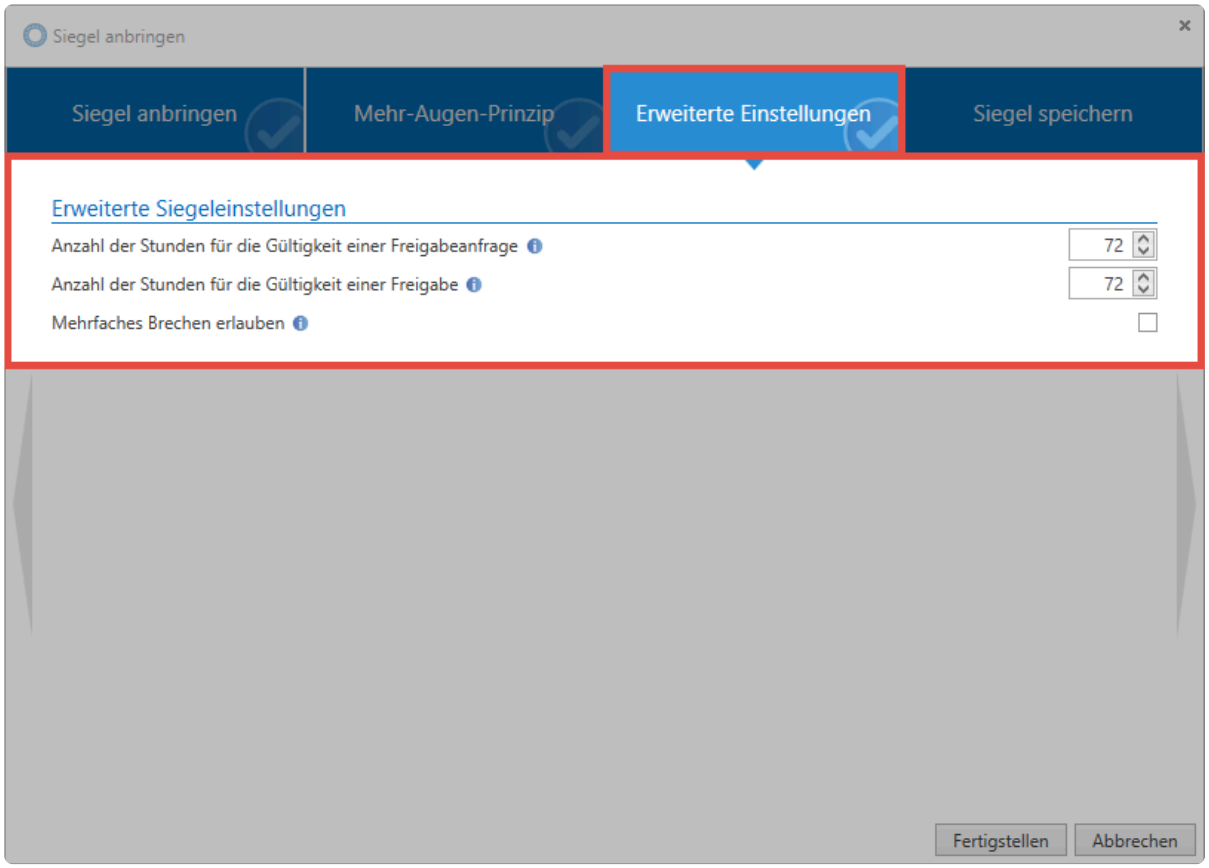
Alle Rollen, die einmal dem Siegel hinzugefügt wurden, können nicht mehr über die Siegellogik entfernt werden. Dies ist nur noch direkt über die Berechtigungen des Datensatzes möglich!

Es ist möglich, Datensätze für einen Benutzer zu versiegeln, der gleichzeitig freigabeberechtigt ist. Beachten Sie, dass in dieser Konstellation mindestens ein weiterer Benutzer freigabeberechtigt sein muss. Prinzipiell gilt, dass man eine Freigabe niemals für sich selbst erteilen kann.

3. Erweiterte Einstellungen

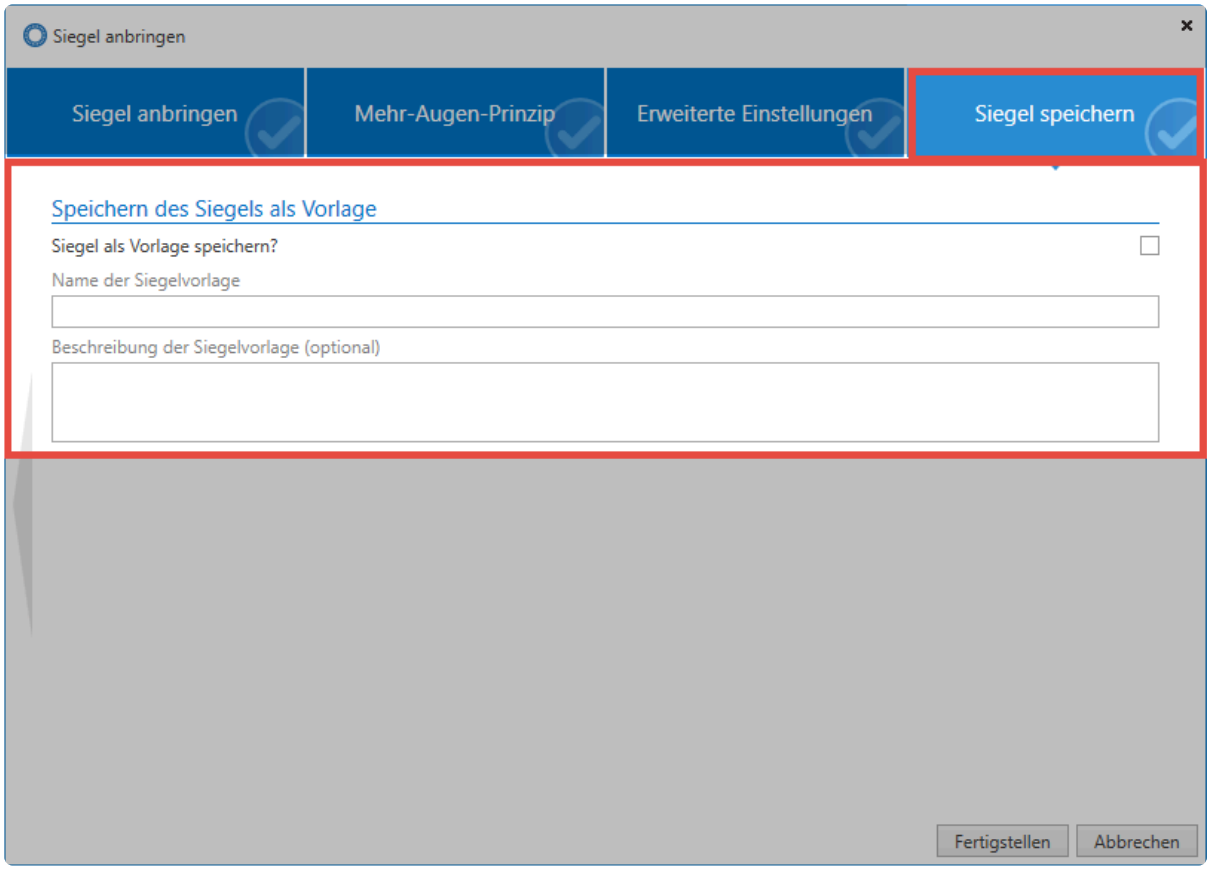
Erweiterte Siegeleinstellungen ermöglichen Ihnen weitere Anpassung des Mehr-Augen-Prinzips. Sowohl die zeitliche Gültigkeit einer Anfrage als auch einer gewährten Freigabe können konfiguriert werden.

Mehrfaches Brechen definiert, ob nach dem Brechen eines Siegels durch einen Benutzer auch weitere User dieses noch brechen dürfen.



4. Siegel Speichern

Vor dem Abschließen des Assistenten haben Sie 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.



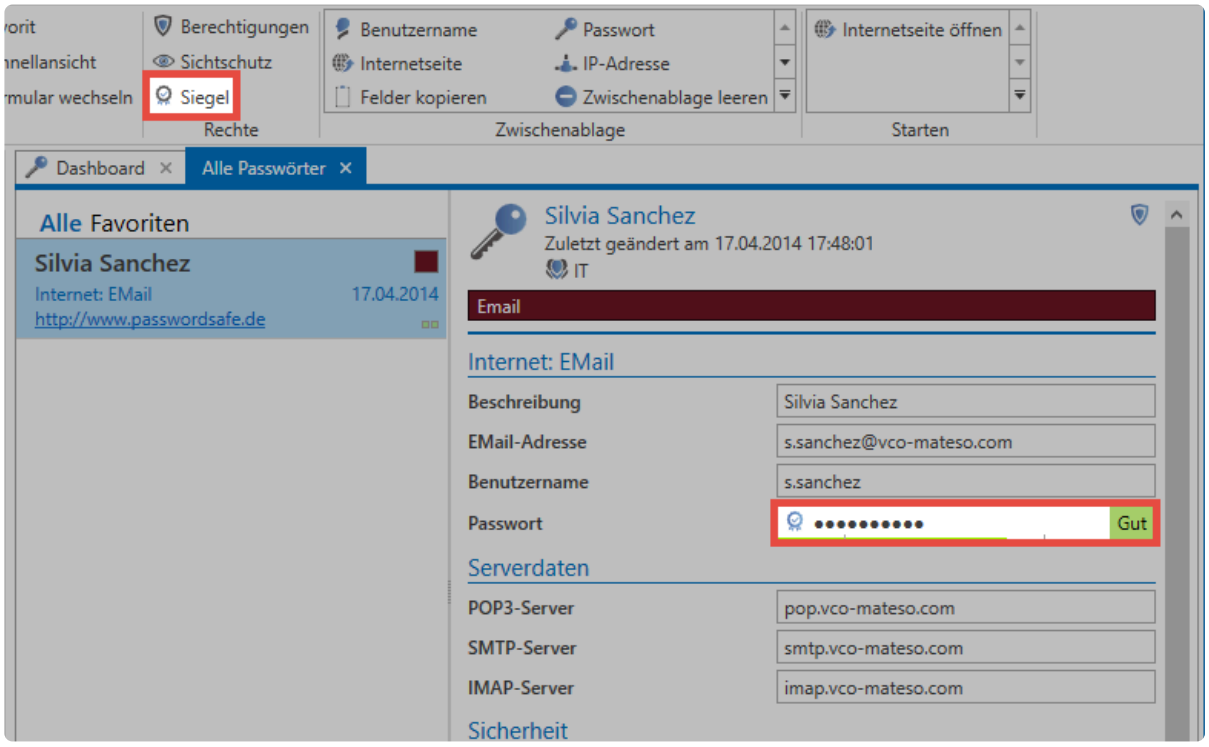
Zusammenfassung

Die für einen Datensatz vergebenen Rechte sind die Basis für beliebig komplexe Siegelkonfigurationen. Sie können sowohl konfigurieren, welche Benutzer und Rollen einen Freigabeprozess durchlaufen müssen als auch festlegen, welche Benutzer oder Rollen die Freigabe erteilen dürfen. Die Siegelübersicht ermöglicht allen Freigabeberechtigten Einsicht in 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

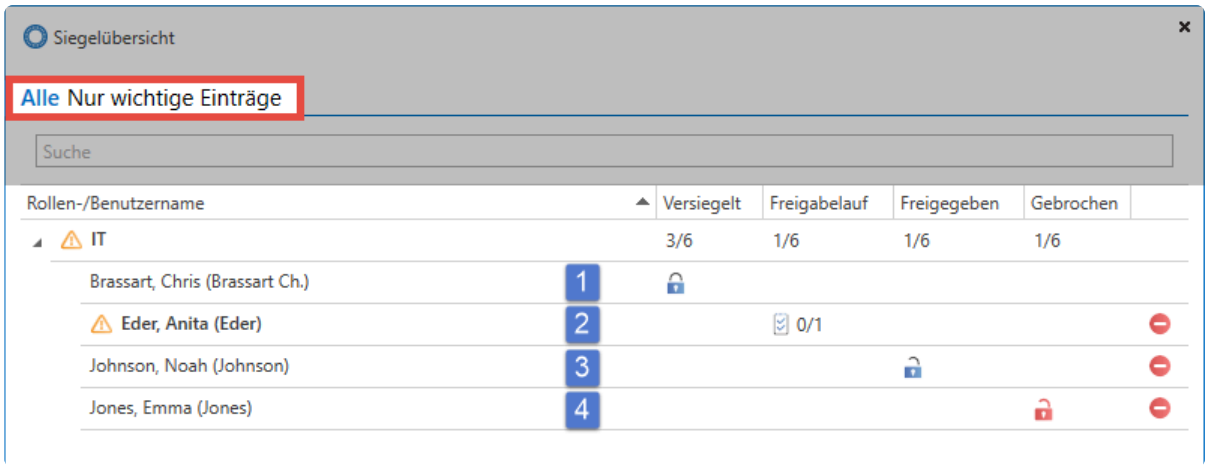
Siegelübersicht

Die Siegelübersicht zeigt alle Benutzer, die entweder direkt oder über eine Rolle auf einen versiegelten Datensatz berechtigt sind. Zudem zeigt eine Freigabematrix den aktuellen Zustand der Versiegelung Hier kann bei Bedarf auch ein Siegel bearbeitet oder gelöscht werden. Die Siegelübersicht erreicht man sowohl über die Ribbon, als auch über das Icon im Passwortfeld des Lesebereichs.



Zustand eines Siegels

Es existieren insgesamt **vier Zustände**, in denen sich ein Siegel befinden kann:



1. Versiegelt

Wenn Sie ein Siegel neu anbringen, ist dessen Zustand automatisch “versiegelt”. Der Benutzer hier keine Möglichkeit, das Passwort einzusehen. Durch das Zurücksetzen einer Anfrage über das Icon am rechten Bildschirmrand werden aktuelle Anfragen einzelner Benutzer ebenfalls wieder in diesen Zustand

versetzt.

2. Freigabelauf

Hat ein Benutzer die Freigabe angefragt, befindet er sich im **Freigabelauf**. Dieser Zustand wird durch ein dementsprechendes Icon neben dem Benutzernamen angezeigt. Jetzt kann eine mögliche Freigabe durch Freigabeberechtigte gewährt werden. Nach diesen sog. **wichtigen Einträgen** können Sie in der Kopfzeile der Siegelübersicht im gleichnamigen Reiter filtern. Die maximale Gültigkeit einer Freigabeanfrage können Sie in den erweiterten Siegeleinstellungen konfigurieren. Ist die Frist abgelaufen, ohne dass genug Freigaben erzielt wurden, wird die Anfrage gelöscht und der Zustand “versiegelt” wieder hergestellt.

3. Freigegeben

Wurde eine Freigabe gewährt, gilt ein Siegel als **freigegeben**. Die maximale Gültigkeit einer gewährten Freigabe können Sie in den erweiterten Siegeleinstellungen festlegen. 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 ein Benutzer nach einer Sicherheitsabfrage das Siegel aktiv bricht. Das Einsehen des Passwortes ist hierbei unerheblich. Einmal gebrochene Siegel können Sie manuell durch das Icon rechts neben der Spalte für gebrochene Siegel zurücksetzen. Hierbei wird der Zustand “Versiegelt” wiederhergestellt.

> ! Es macht keinen Sinn, bereits eingesehene Passwörter wieder neu zu versiegeln. Es ist nicht nachvollziehbar, ob ein Benutzer das Passwort z.B. per Screenshot gesichert hat. In solchen Fällen ist die Vergabe eines neuen Passwortes die einzige Möglichkeit, um die Passwortsicherheit zu 100% zu gewährleisten!

Freigabemechanismus

Was ist der Freigabemechanismus?

Ein versiegeltes Passwort wird erst dann freigegeben (gebrochen), wenn die im Siegel festgelegte Anzahl von Freigaben gewährt wurde. Freigaben können die Benutzer erteilen, die im Siegel als Freigabeberechtigte definiert wurden.

Benutzer und Rollen im Freigabemechanismus

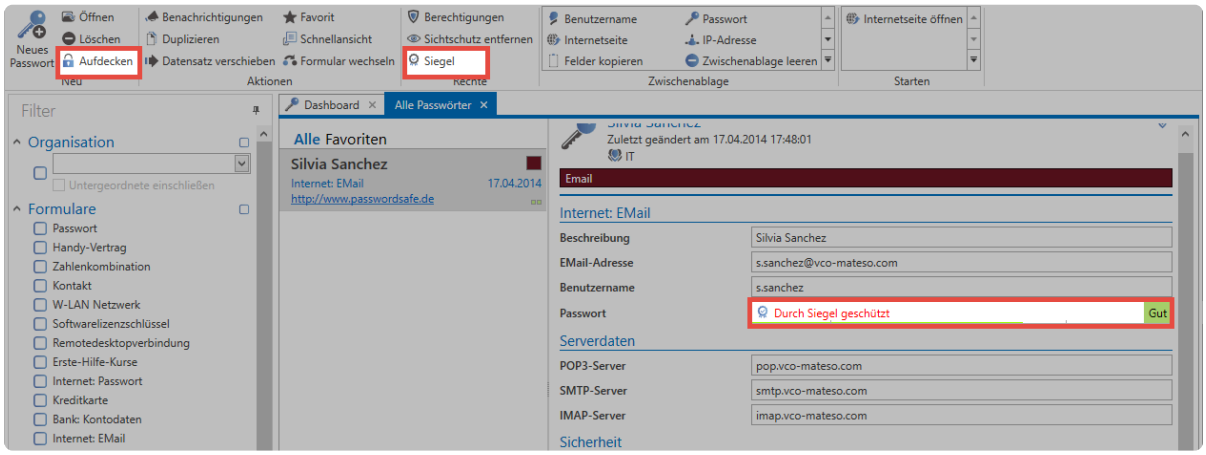
Wie bereits in den vorherigen Kapiteln erwähnt, schränken Siegel stets das Recht eines Benutzers ein, ein bestimmtes Passwort einzusehen. Das ist auch der Fall, wenn ein Sigel für eine Rolle konfiguriert wurde. Auch hier muss jedes Mitglied der Rolle den Freigabeprozess durchlaufen, da technisch gesehen für jeden Benutzer ein eigenes Siegel erstellt wurde.

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

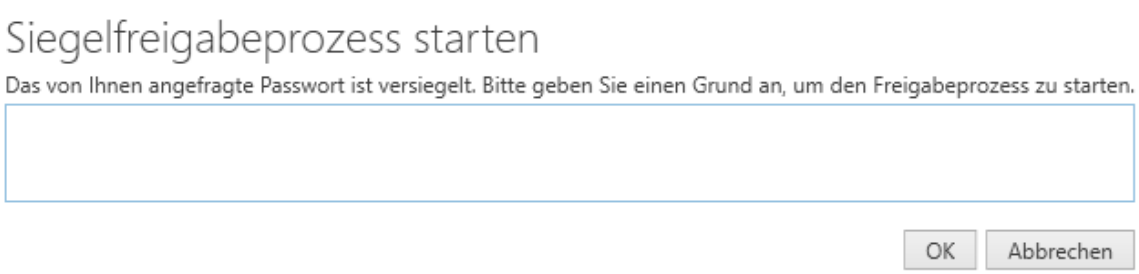
! Ist ein Benutzer in mehreren Rollen eines Siegels Mitglied, wird stets das “stärkere” Recht angewendet. Freigaberecht überwiegt Leserecht.

1. Freigaben anfragen

Freigaben für versiegelte Passwörter müssen bei den Freigabeberechtigten angefragt werden. Das ist sowohl über die Buttons **Aufdecken** und **Siegel** in der Ribbon als auch über das **Icon im Passwortfeld** des Datensatzes im Lesebereich möglich.



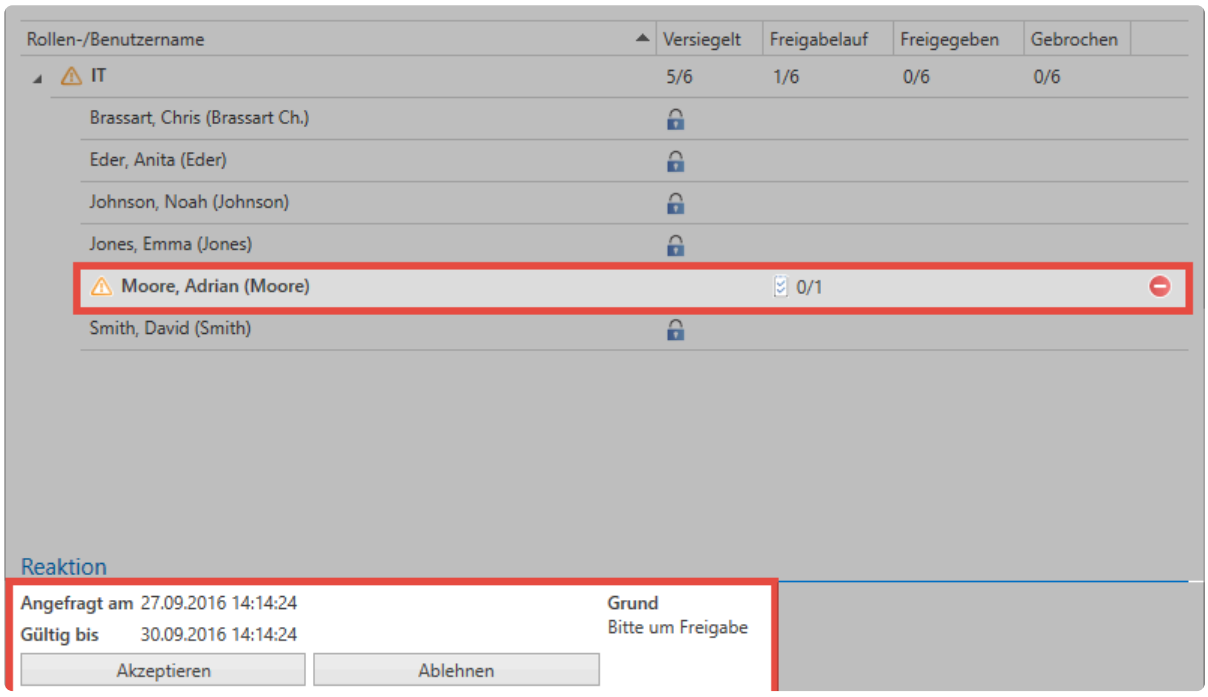
Es öffnet sich ein Fenster um den Freigabeprozess zu starten. Die eingegebene Begründung wird den Berechtigten angezeigt.



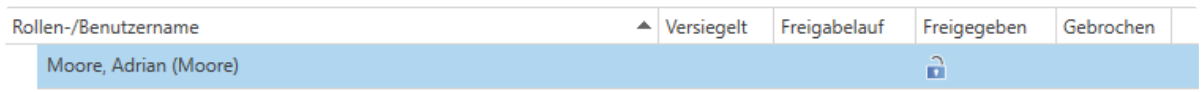
Alle Freigabeberechtigten erhalten die Benachrichtigung, dass ein Benutzer die Freigabe angefragt hat – erkennbar im Modul Benachrichtigungen als auch in der Siegelübersicht.

2. Freigaben gewähren

Klicken Sie im Modul Benachrichtigung in der Ribbon das Siegelsymbol um die Siegelübersicht zu öffnen. Alle für eine Freigabe relevanten Daten werden innerhalb der Siegelübersicht angezeigt – inklusive dem Grund für die Freigabe.

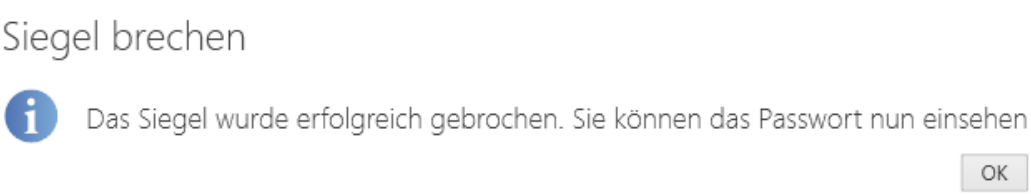


Nach gewährter Freigabe wird der Anfragende Im **Modul Benachrichtigungen** informiert. Er kann hier auch direkt das Siegel über die Ribbon öffnen und den aktuellen Stand des Freigabeprozesses einsehen.



3. Siegel brechen

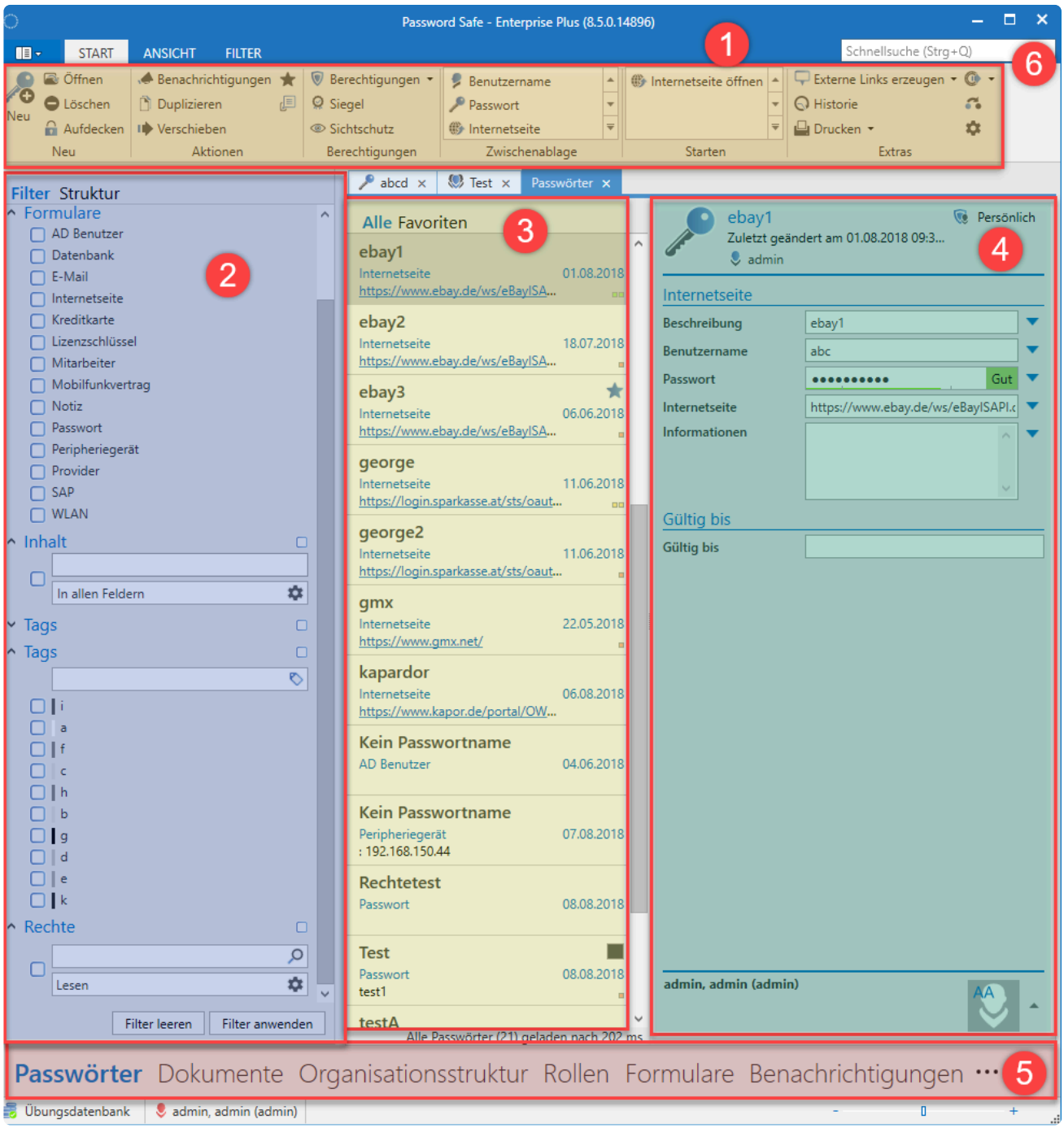
Sobald der anfragende Benutzer die Anzahl der benötigten Freigaben erhalten hat, wird er informiert. Er kann das Siegel nun brechen. Ab diesem Zeitpunkt ist das Passwort durch den Benutzer einsehbar.

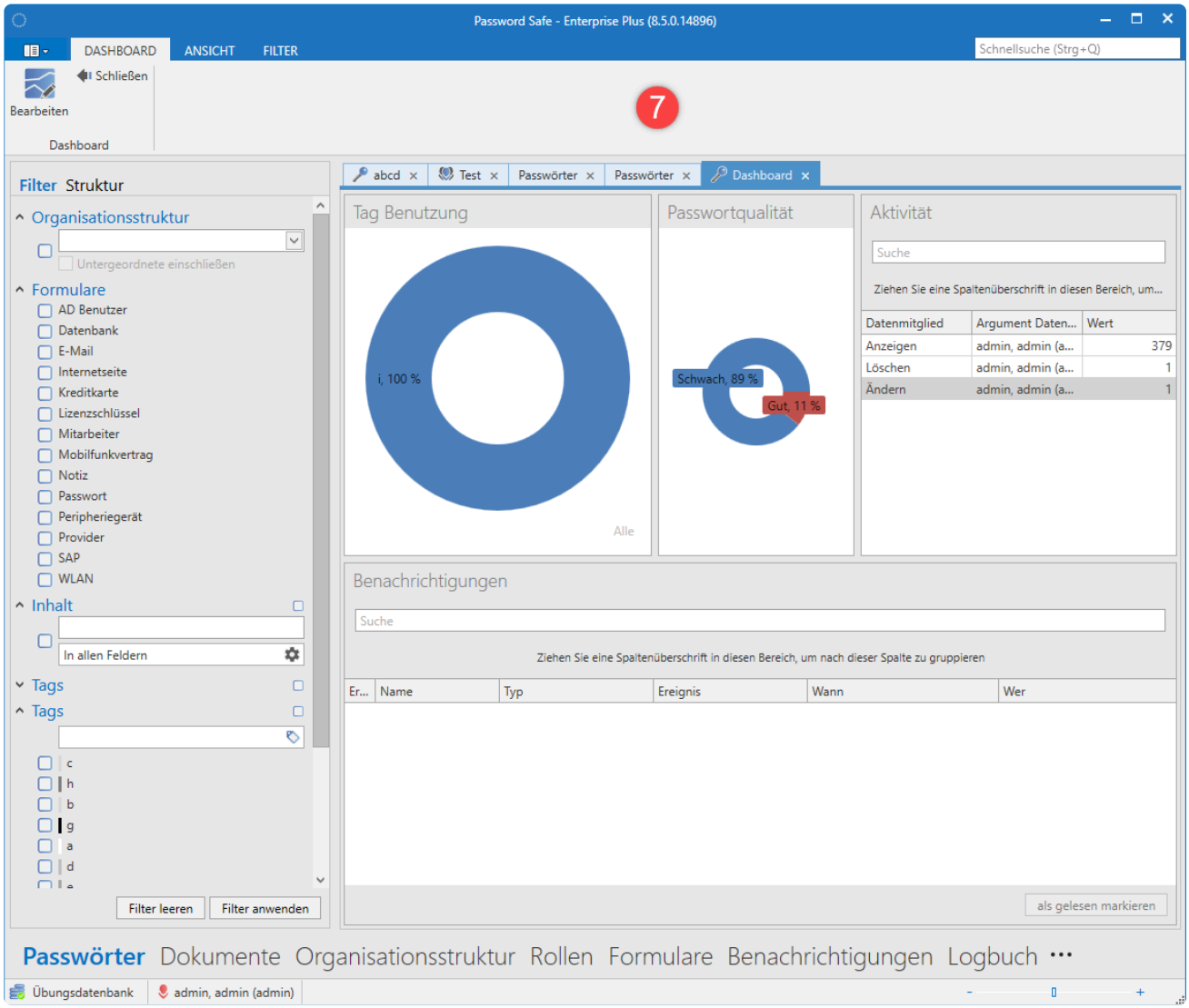

Siegel brechen
Das Siegel wurde erfolgreich gebrochen. Sie können das Passwort nun einsehen
OK

Bedienung und Aufbau

Clientaufbau

Durch den strukturierten und modularen Aufbau des Clients finden Sie regelmäßig benötigte Funktionen modulübergreifend immer an derselben Stelle.





[1. Ribbon]

[2. Filter]

[3. Listenansicht]

[4. Lesebereich]

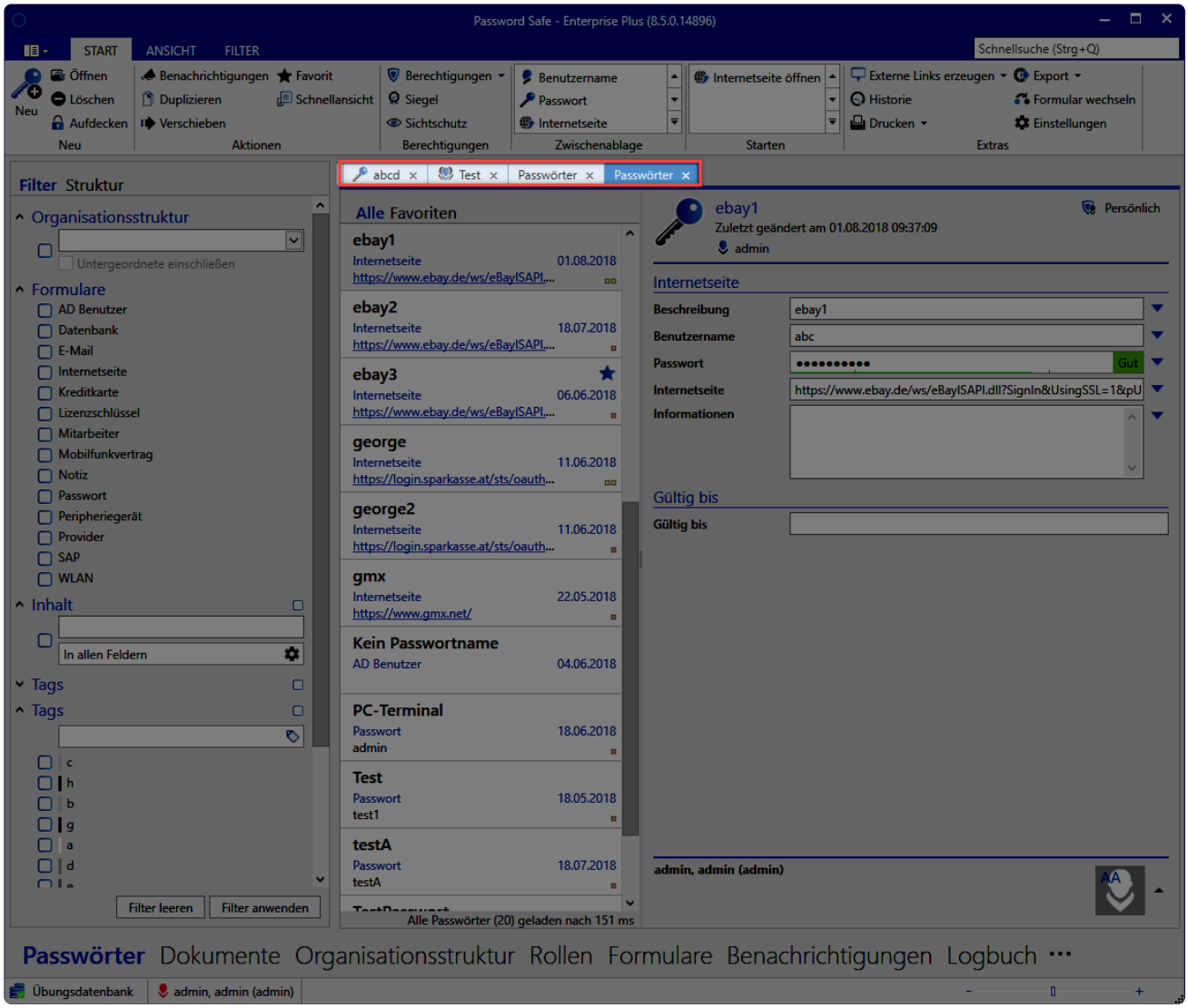
[5. Module]

[6. Suche]

[7. Dashboard und Widgets]

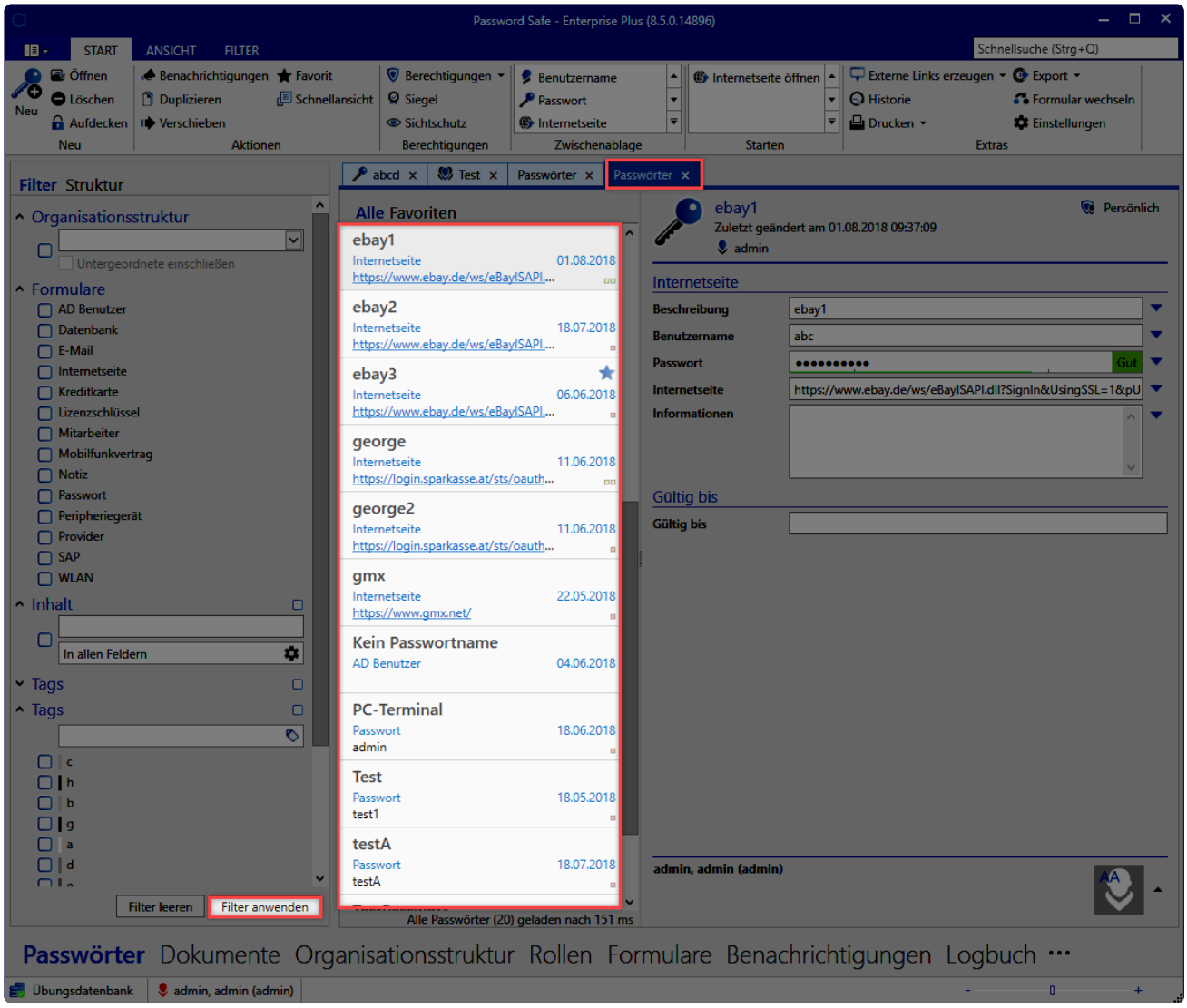
Tabs

Tabs bilden zusammengehörige Informationen in einem separaten Bereich ab. Diese Navigation ermöglicht die Darstellung sowie den schnellen Zugriff und Wechsel zwischen relevanten Informationen. Sie können beispielsweise das Ergebnis eines Filters festgehalten, ohne dass ein erneutes Filtern das ursprüngliche Ergebnis überschreibt. Parallel können Sie sich auch Detailinformationen zu Datensätzen in eigenen Tabs anzeigen lassen. Die Reihenfolge der Tabs kann per Drag & Drop angepasst werden.



Standard-Tab

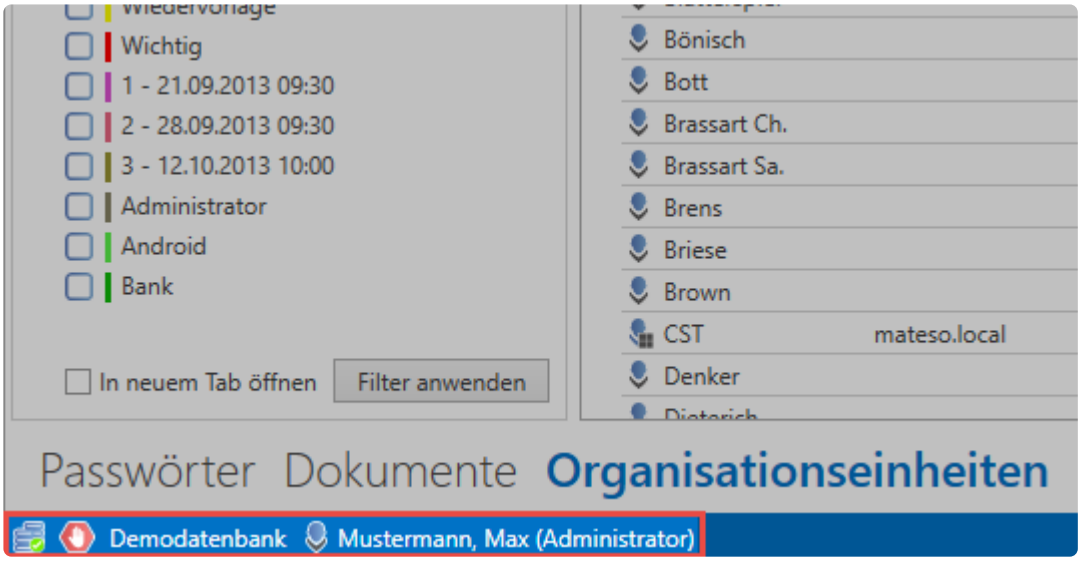
Rufen Sie ein Modul initial auf, wird Ihnen der Standard-Tab angezeigt. Dieser trägt immer den Namen des Moduls.



Der Tab lässt sich schließen und kann durch eine erneute Anwendung des Filters wiederhergestellt werden.

Client Footer Informationen

Unabhängig vom ausgewählten Modul werden im Footer-Bereich des Clients verschiedene Informationen angezeigt. Fahren Sie für weiterführende Informationen mit der Maus über die Icons.



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

Ausrichtung

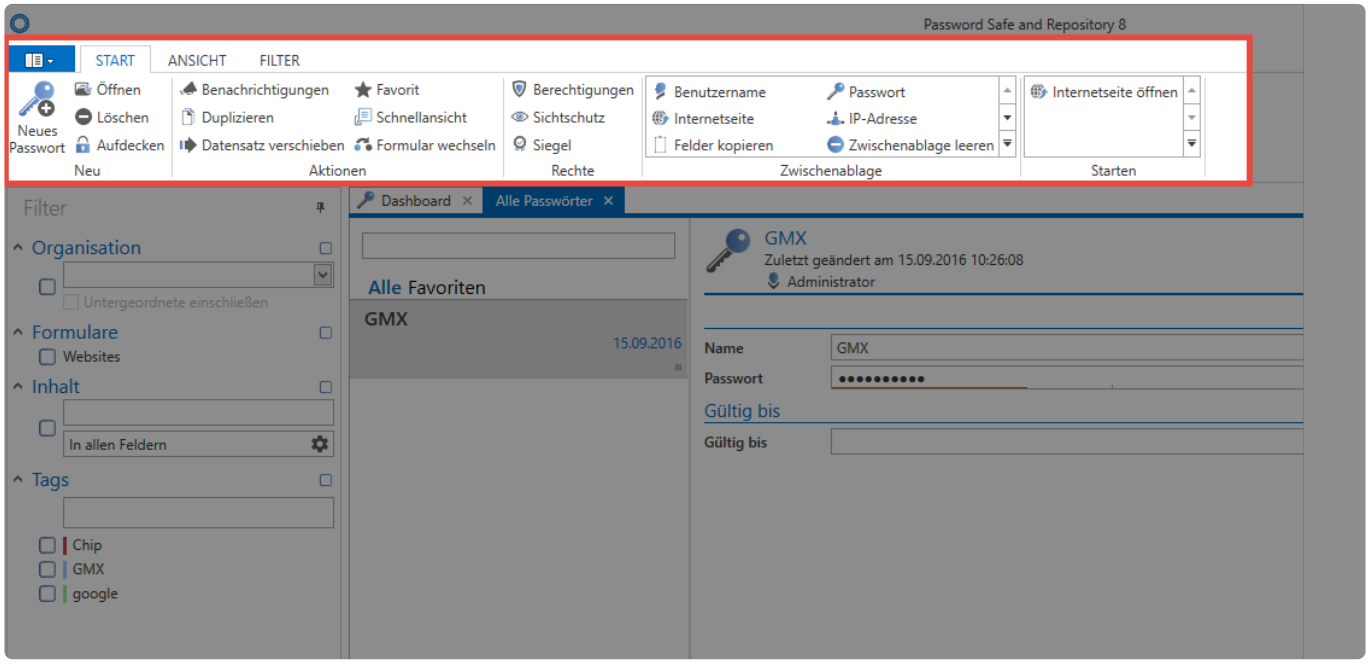
Bei folgenden Objekten können Sie – über die Einstellungen – die Ausrichtung ändern:

- Active Directory
- Anwendungen
- Benachrichtigungen
- Berichte
- Dokumente
- Formular
- Logbuch
- Organisationsstruktur
- Password Reset
- Richtlinie
- Rollen
- Siegelvorlagen
- System Tasks
- Weiterleitungsregeln
- Profilbildgröße im Lesebereich

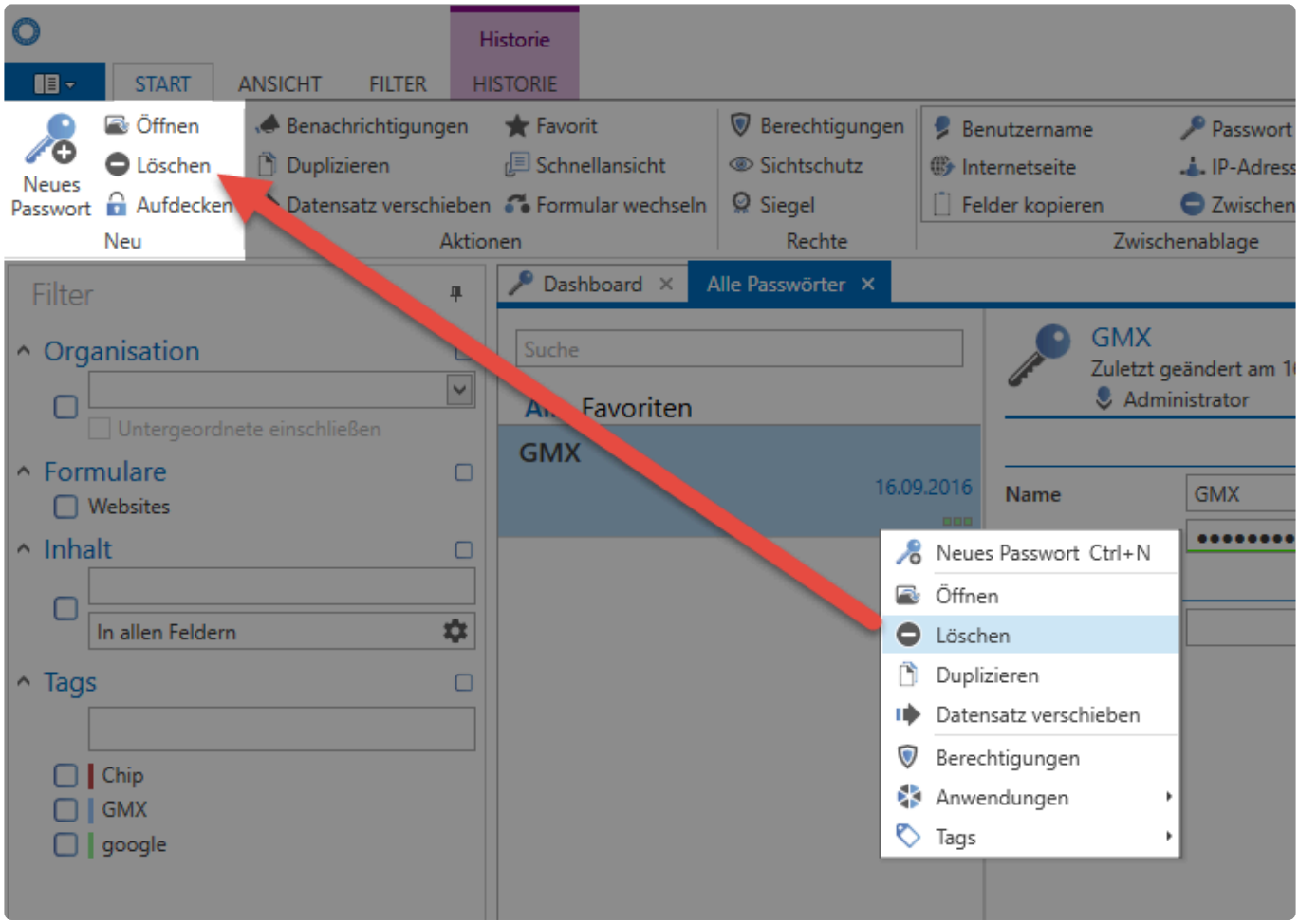
Ribbon

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.



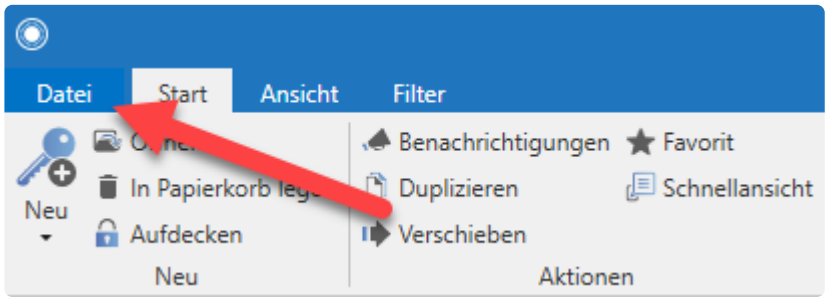
Die Ribbon stellt verschiedene Funktionalitäten dynamisch bereit. Je nachdem, welches Objekt Sie markiert haben, können Sie unterschiedliche Aktionen durchführen. Auch die Auswahl des Moduls hat Auswirkungen auf die Features, welche die Ribbon anbietet. Natürlich können Sie – darüber hinaus – die wichtigsten Aktionen per Kontextmenü (rechte Maustaste) steuern.



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

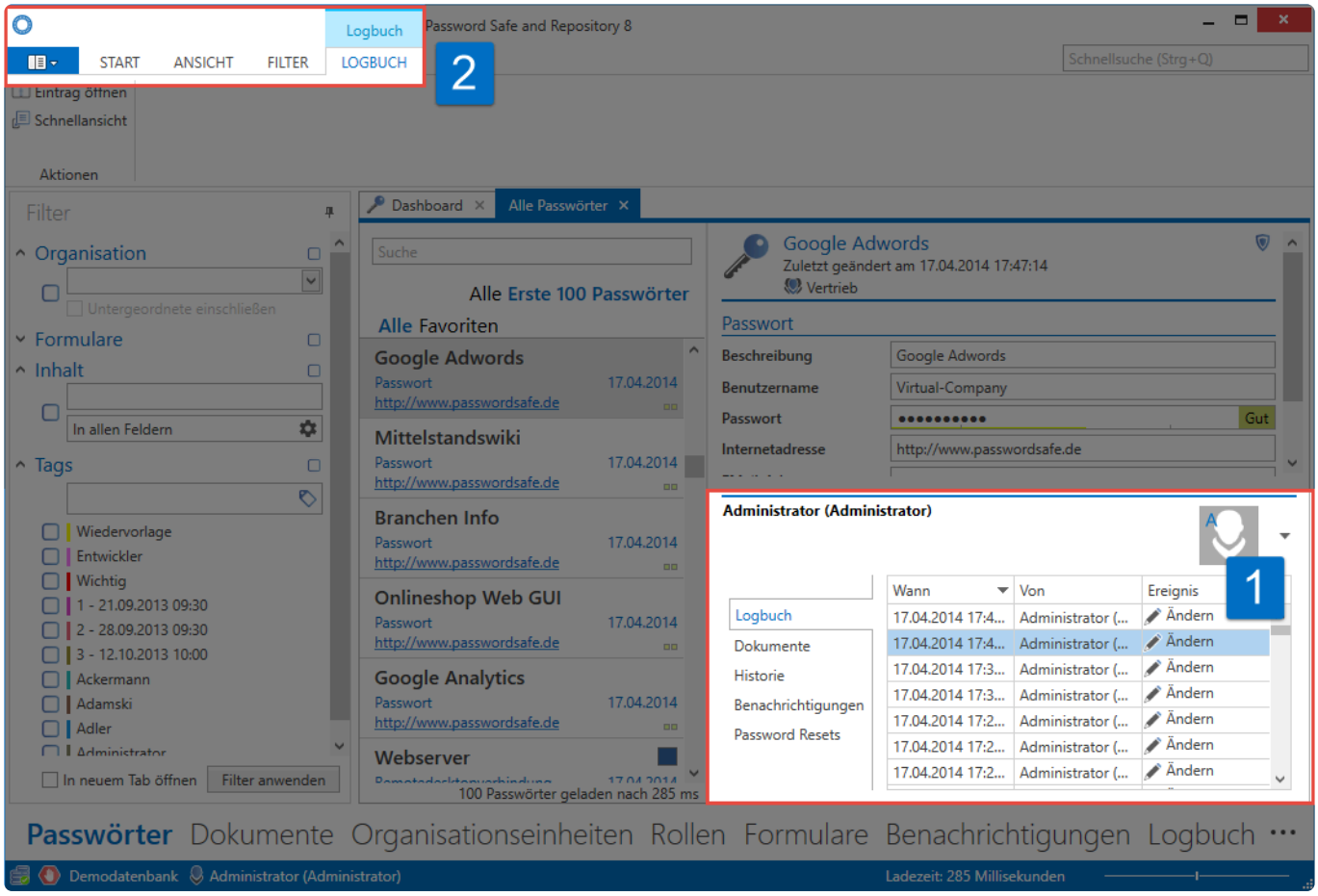
Zugang zum Hauptmenü (Backstage)

Über den Reiter “Datei” links oben in der Ribbon erreichen Sie das **Hauptmenü**:



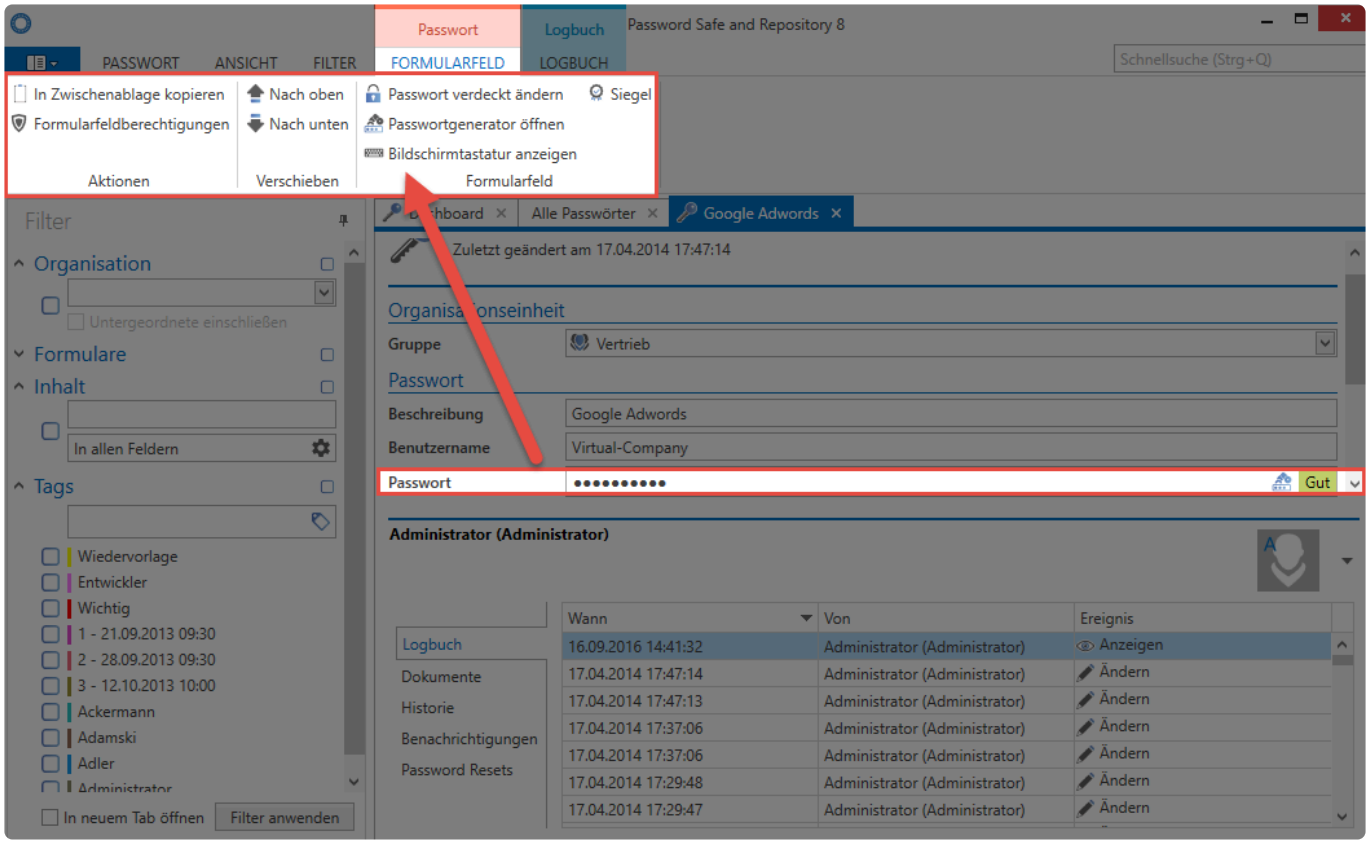
Ribbon-Tabs

Im Header Bereich der Ribbon finden Sie Tabs, welche alle verfügbaren Operationen zusammenfassen. Sie finden in jedem Modul **Start**, **Ansicht** und **Filter**. Wenn der Footer des **Lesebereichs** geöffnet ist **(1)**, werden 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 Sie markiert haben, öffnet sich in der Ribbon der dementsprechende Content-Tab.



Je nach markiertem Formularfeld stellt Ihnen der Content-Tab weitere Aktionen zur Verfügung. 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?

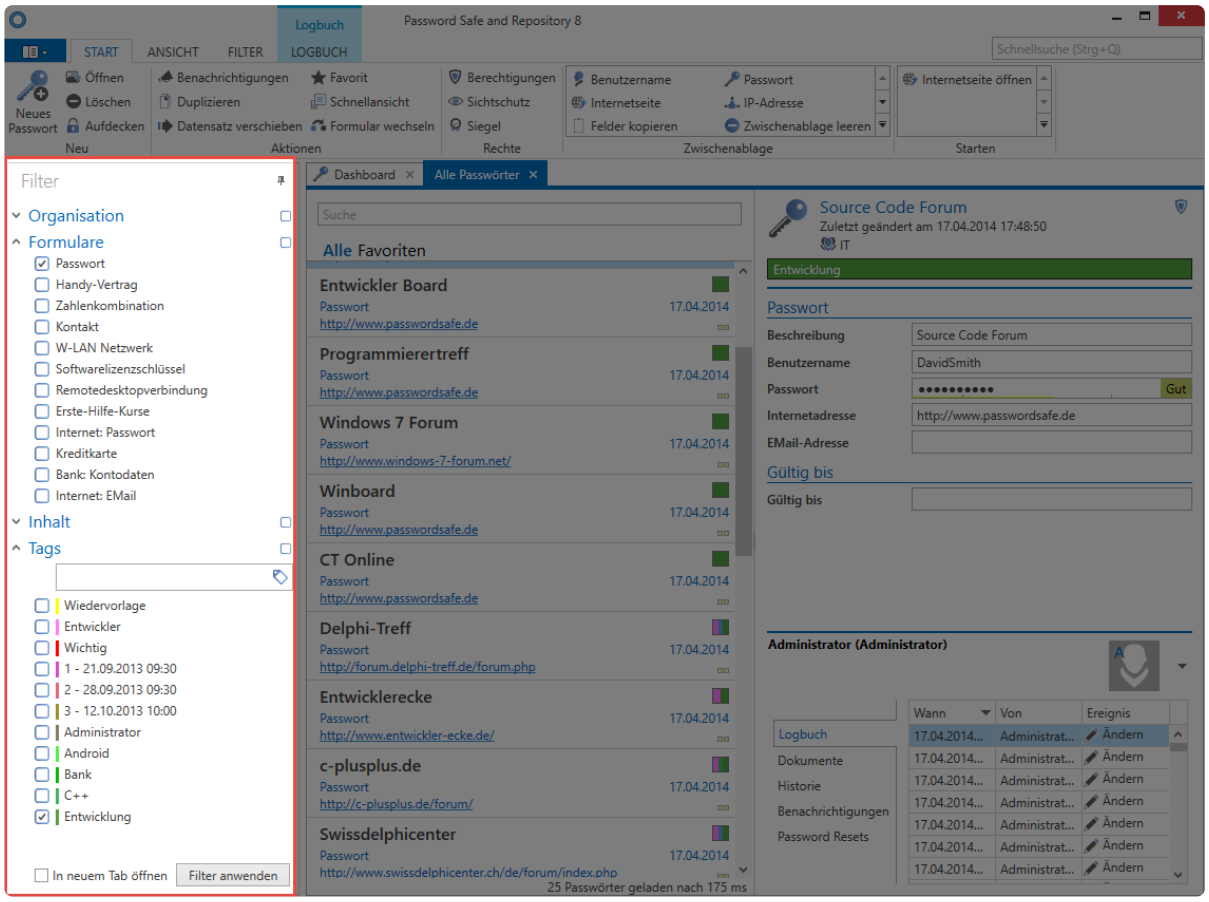
Mit den frei konfigurierbaren Filter des FullClient und WebClient können alle gespeicherten Daten gefunden werden. Die Filterkriterien werden dabei dem jeweiligen Modul angepasst, in dem man sich aktuell befindet. Durch die Auswahl einer oder auch mehrerer Suchkriterien und einem Klick auf „Filter anwenden“, wird die Ergebnismenge in der Listenansicht angezeigt.

Relevante Rechte

Es wird zum Bearbeiten von Filtern folgende Option benötigt:

Benutzerrecht

- Kann Filter bearbeiten



Wer kann den Filter benutzen?

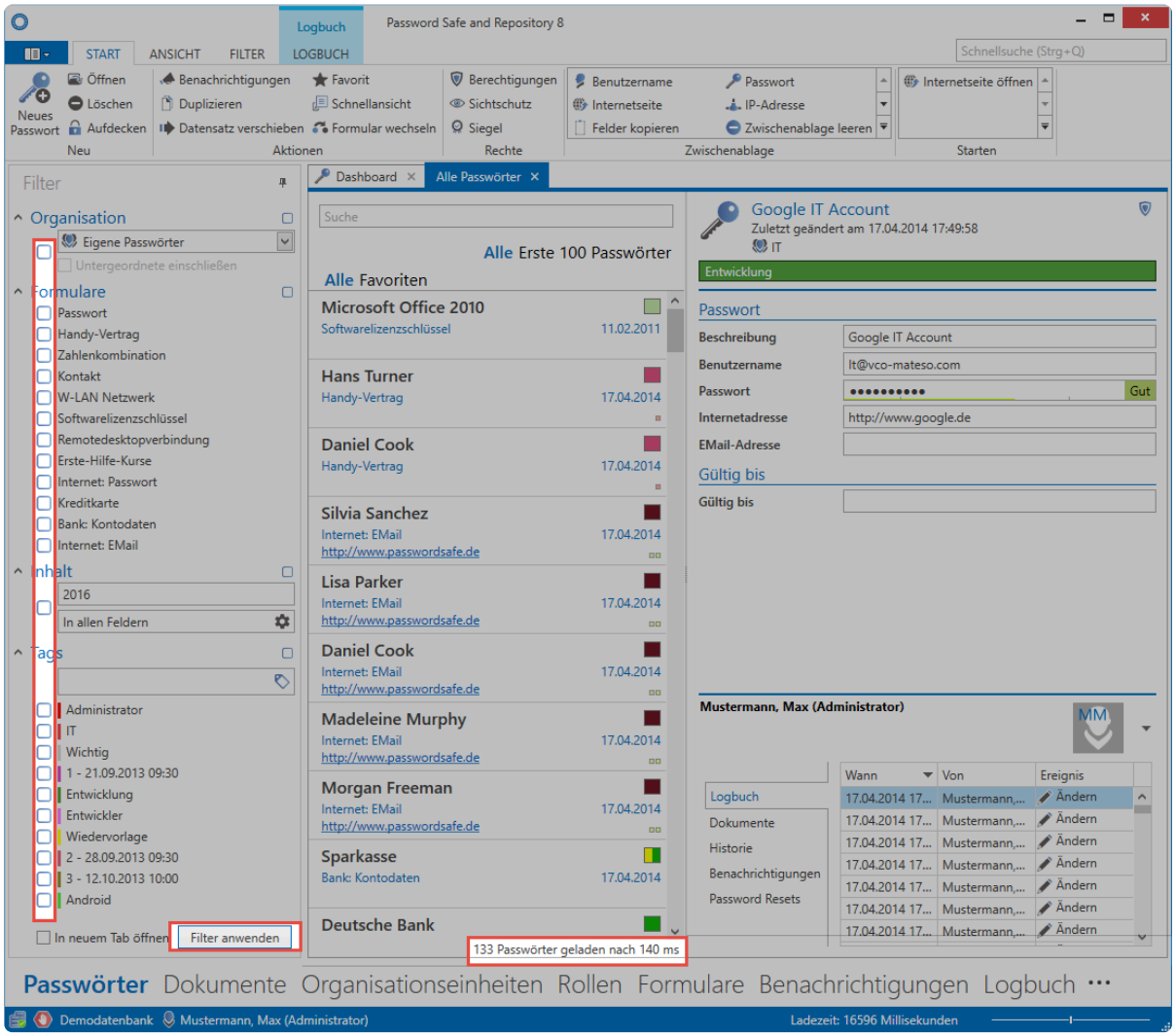
Alle Benutzern können den Filter nutzen. Es können jedoch durch Berechtigungen die möglichen Filterkriterien für einzelne Mitarbeiter eingeschränkt werden. Ein Mitarbeiter kann z.B. nur dann nach dem Formular **Passwort** filtern, wenn er Leseberechtigung auf das Formular besitzt.

> **!** 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 werden alle den Kriterien entsprechenden Datensätze in der Listenansicht angezeigt. Ist **kein Kriterium** ausgewählt, erhält man eine Auflistung aller Datensätze, auf die man berechtigt ist.



Wie man sehen kann, ist die Menge der Datensätze mit 133 nicht wirklich effizient verwaltbar. Hier macht es Sinn, durch das Hinzufügen von Filtern die Anzahl der Datensätze zu reduzieren.

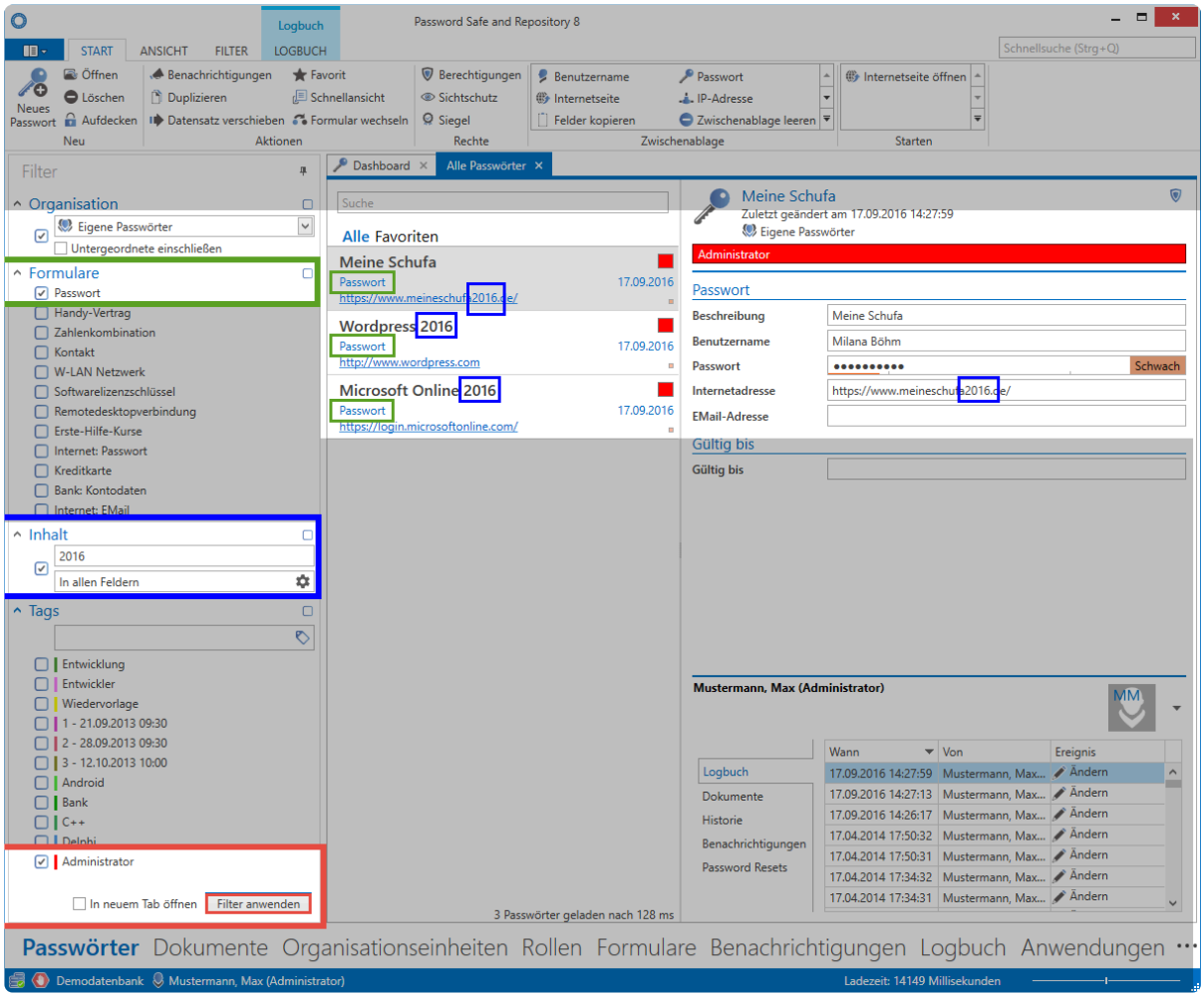
Hinzufügen von Filterkriterien

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”.

Folgend sehen sie das Ergebnis der Filterung. Inwiefern die Filterkriterien mit den drei übrig gebliebenen Datensätzen übereinstimmen, ist farblich zugeordnet.

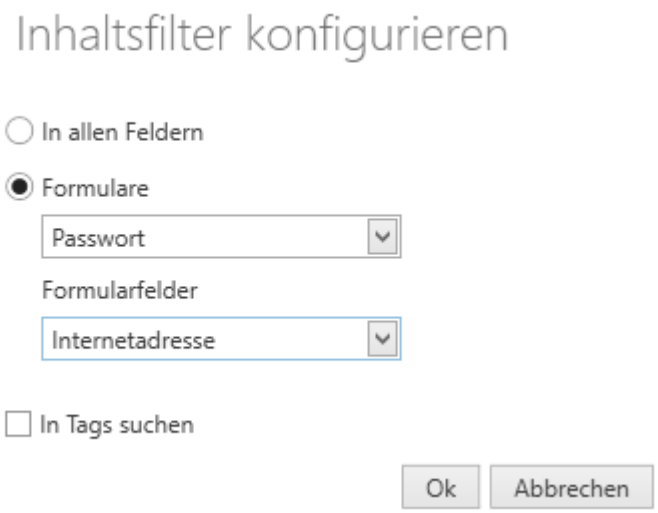


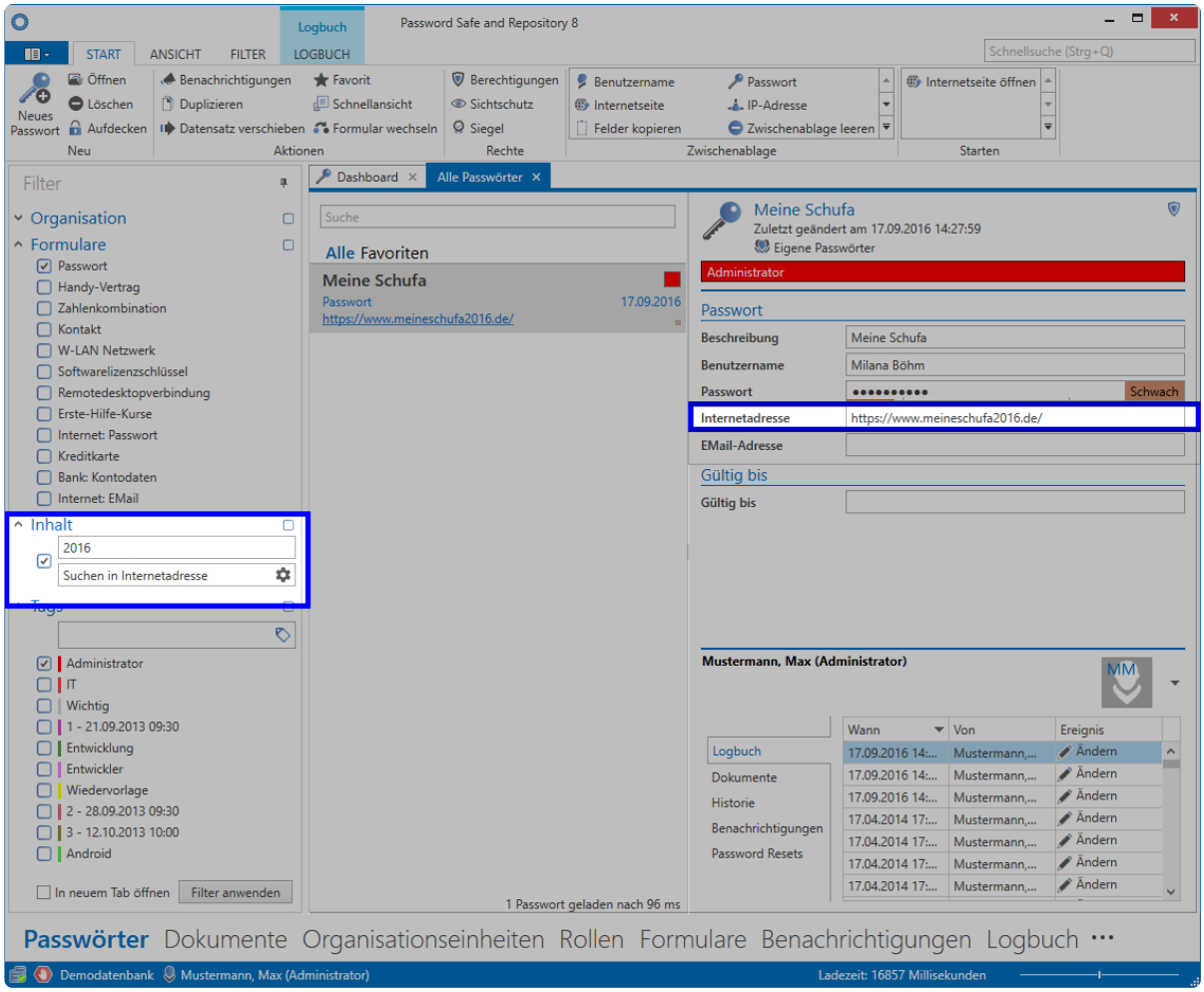
> ! Beim Filtern mit mehreren Kriterien, wie z.B. Formulare, Inhalt und Tags, müssen zwingend alle Filterkriterien erfüllt werden. Es handelt sich demnach um eine logische “Und-Verknüpfung”. Weitere mögliche Verknüpfungsarten sind in den Erweiterten Filtereinstellungen detailliert beschrieben.

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 so 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 Fenster. Man erkennt hier, dass der Inhaltsfilter lediglich noch das Formular **Passwort** und in diesem nur das Formularfeld **Internetadresse** berücksichtigen soll:





Anhand des Beispiels ist erkennbar, dass der Filter an jede persönliche Anforderung anpassbar ist. Er ist somit das wichtigste Werkzeug, um in der Datenbank abgelegte Daten wiederfinden zu können.

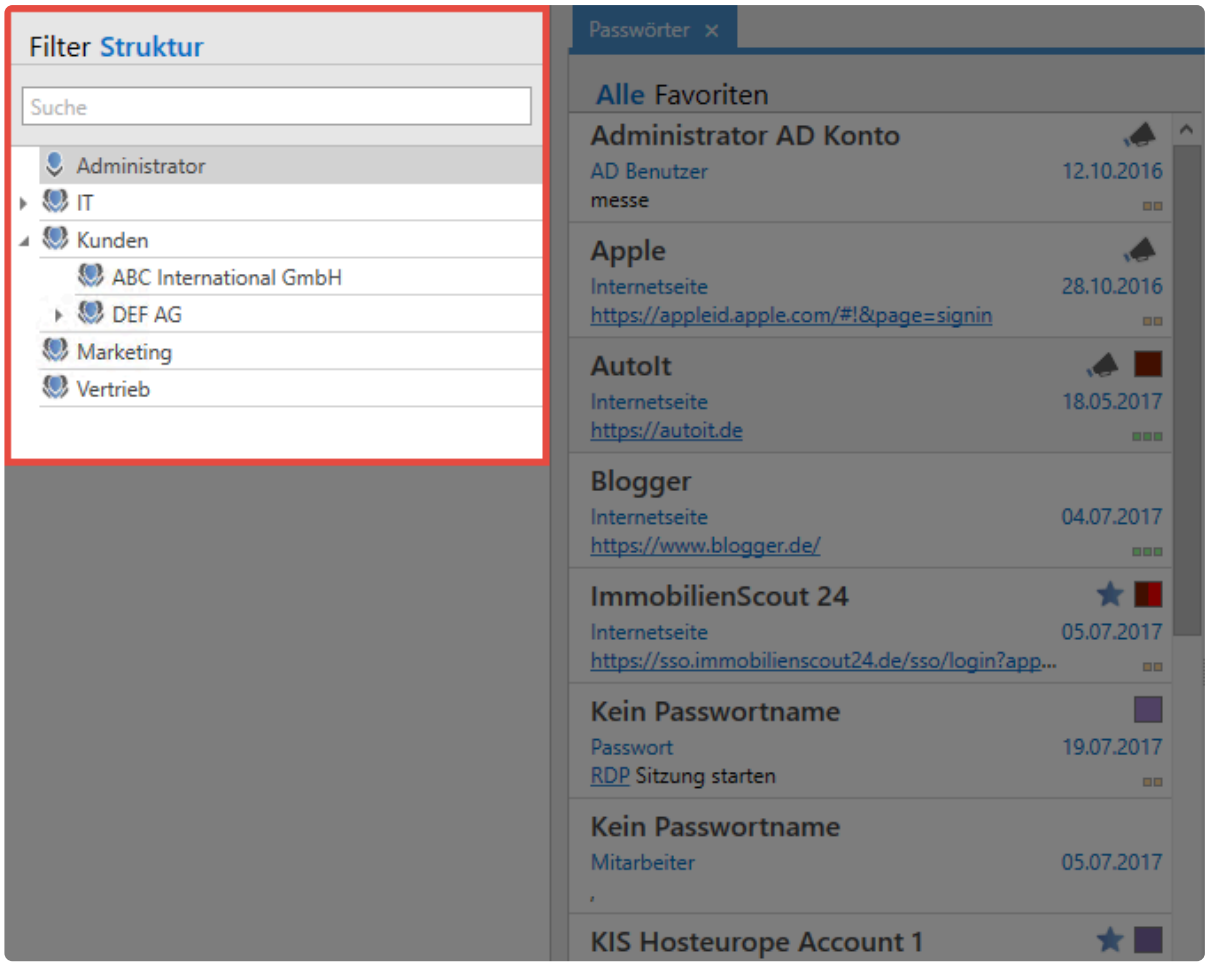
! Die Effektivität des Filters ist eng mit der Datenintegrität verbunden. Nur, wenn Daten sauber gepflegt vorliegen, ist effizientes Arbeiten mit dem Filter gewährleistet. Es ist wichtig, dass Mitarbeiter im richtigen Umgang mit dem Filterwerkzeug, als auch beim Anlegen der Datensätze, geschult werden. 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. Hier kann einzig auf Basis der Organisationsstruktur gefiltert werden, wobei die komplette Organisationsstruktur direkt einsehbar ist – ein Vorteil im Vergleich zur standardmäßigen Filteransicht.

> 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 – ein Vorteil für Benutzern, die stark strukturbasiert arbeiten möchten.

Relevante Einstellungen

Im Zusammenhang mit dem Anzeigemodus existieren relevante Einstellungen:

- **Anzeigemodus** – Auswahl ob Filter- und/oder Strukuransicht

- **Auf Filter springen bei Schnellsuche** – Springt bei der Schnellsuche auf den Filter, dabei spielt es keine Rolle in welcher Ansicht Sie sich befinden
- **Letzten Filter automatisch anwenden** – Wendet beim Neustart des Clients des letzten Filter an
- **Zustand des Anzeigemodus beim Programmstart** – Auswahlmöglichkeit zwischen Filter, Struktur oder letzter Zustand

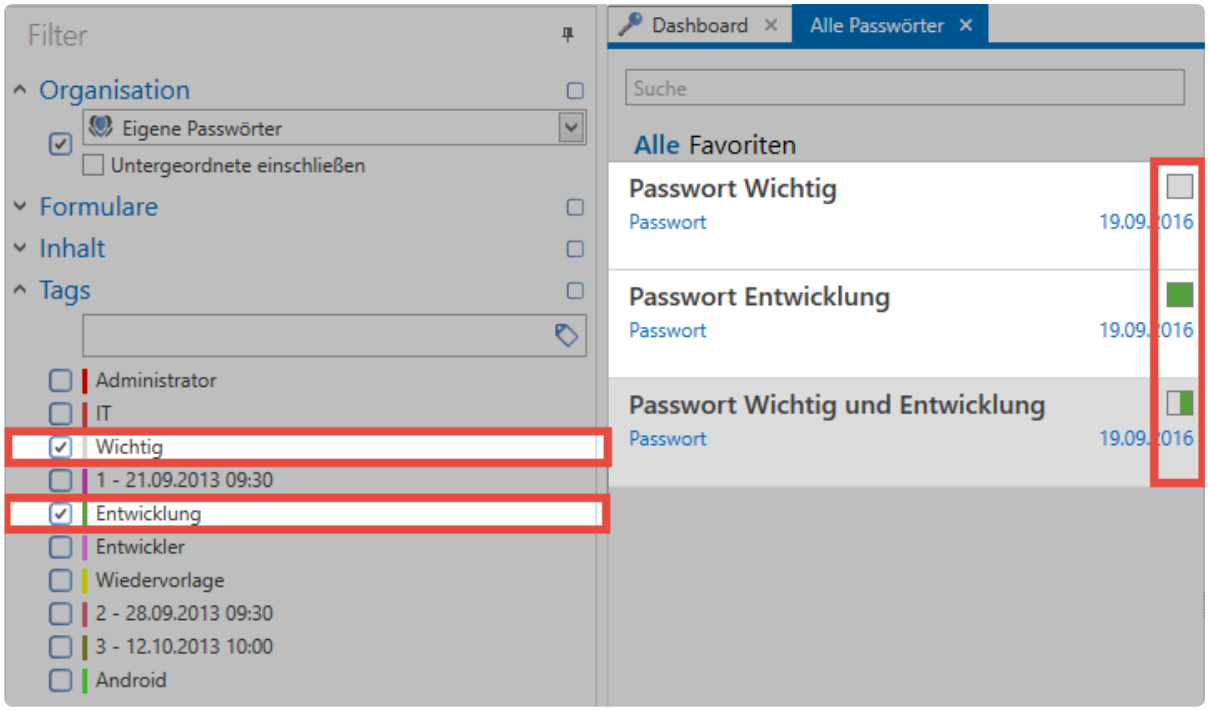
Erweiterte Filtereinstellungen

Verknüpfung von Filtern

Hier sehen Sie am Beispiel von Tags, wie Filterkriterien miteinander verknüpft werden können.

1. Logische “Oder-Verknüpfung”

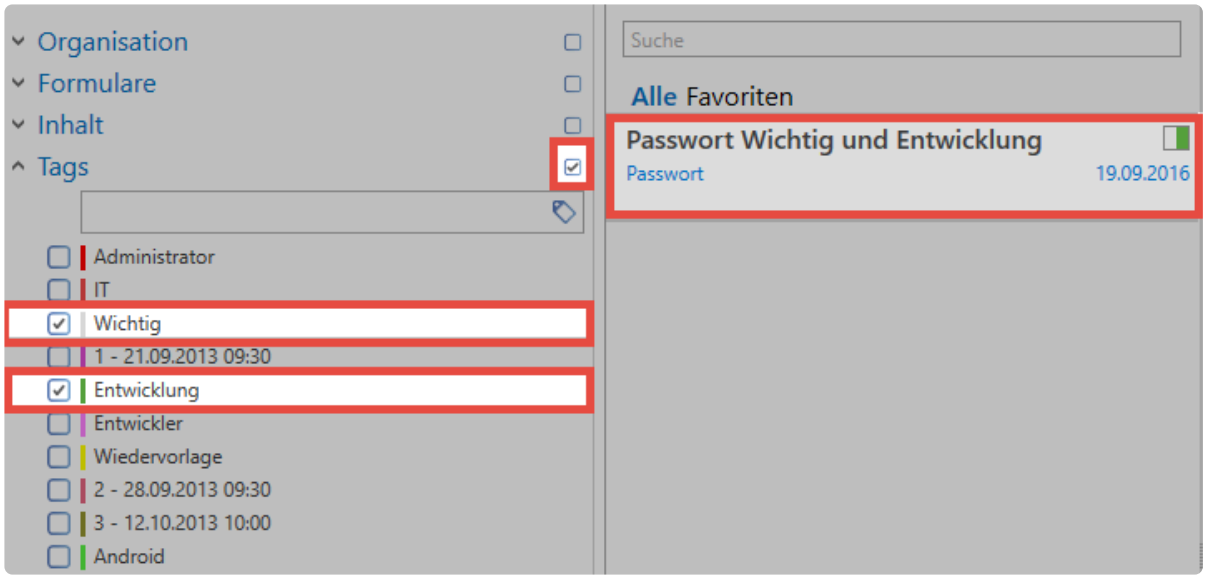
Das ist der Standardmodus für den Filter. Im folgendem Beispiel sollen alle Datensätze gefunden werden, die mindestens einen der Tags **“Wichtig”** oder **“Entwicklung”** besitzen. Es werden aber auch Datensätze angezeigt, die beide Tags besitzen.



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

2. Logische “Und-Verknüpfung”

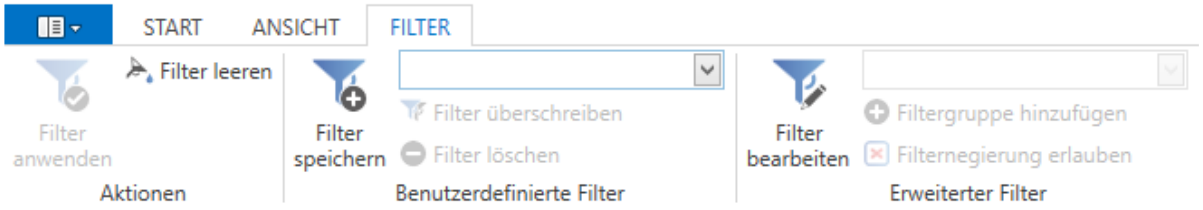
Aktiviert wird dieser Modus direkt durch die Checkbox im Filter. Jedes Filterkriterium besitzt seine eigene Checkbox.



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

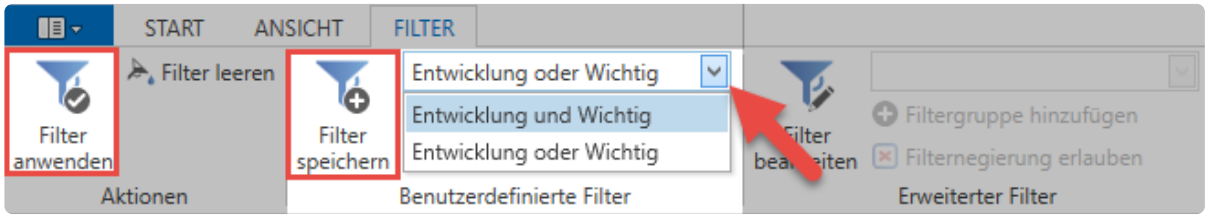
Filter-Tab in der Ribbon

In der Ribbon findet man die Filterverwaltung. Hier kann man z.B. die aktuell konfigurierten Filterkriterien erweitern oder eigene Filter speichern.



Filter speichern, bearbeiten und löschen

Es bietet sich in vielen Fällen an, einmal definierte Filter zu speichern. Durch den Button "**Filter speichern**" wird man direkt aufgefordert, für einen Filter einen entsprechenden Namen zu vergeben. Gespeichert wird der Filter gemäß der aktuell im Filter konfigurierten Kriterien. Der Filter kann zukünftig über das Auswahlmenü ausgewählt werden. Beachten Sie, dass eine getroffene Filterauswahl zwar sofort in den Filter übernommen, jedoch nicht automatisch durchgeführt wird. Der Filter muss erst angewendet werden, um die entsprechenden Ergebnisse zu erhalten. Verwenden Sie dazu den Button in der Ribbon, oder im Filter selbst.

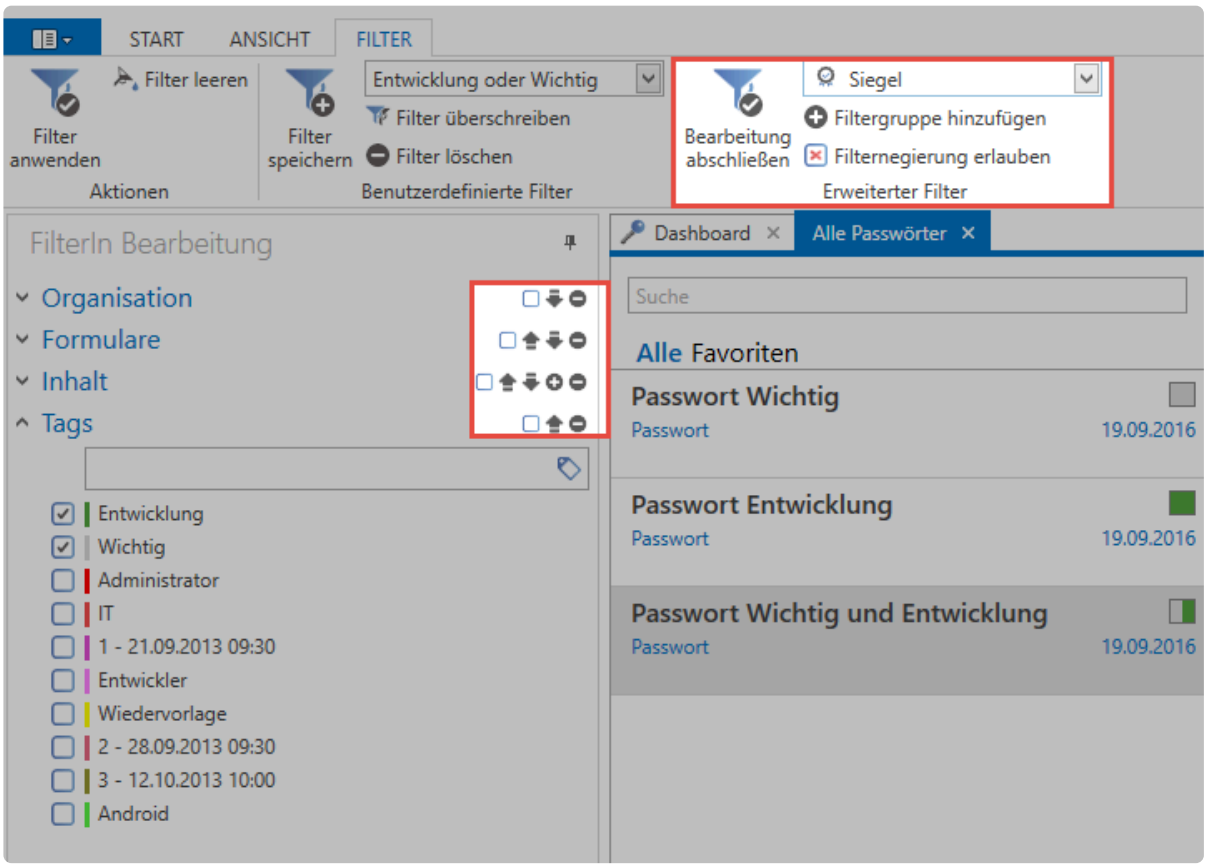


Das Löschen oder das Überschreiben vorhandener Filter ist in beiden Fällen gleich. Gelöscht wird stets

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.

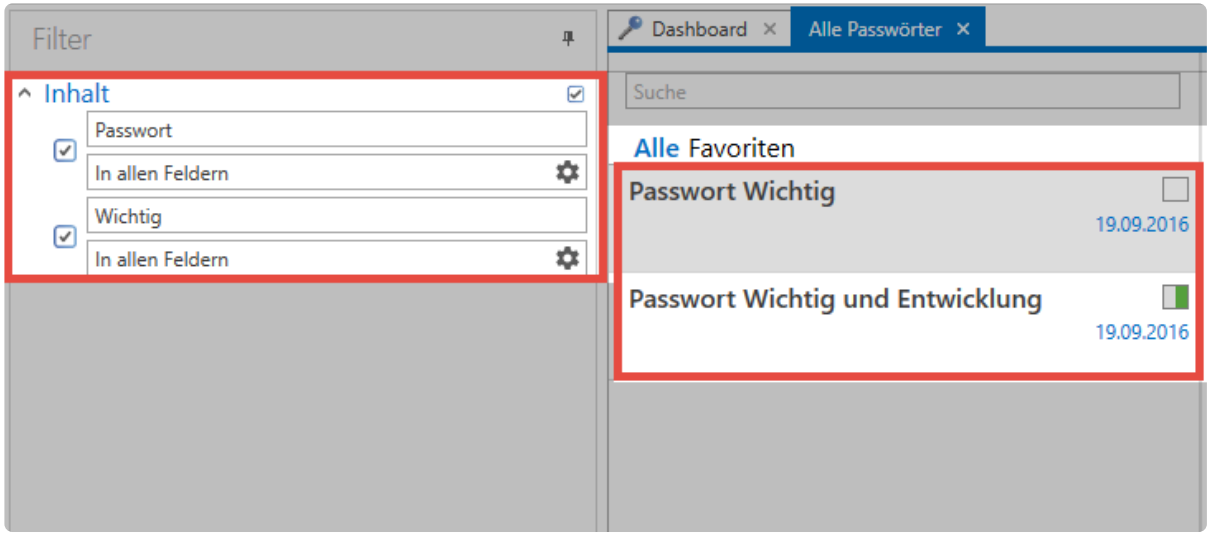
Erweiterter Filter

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”** beendet.



Über das Auswahlfeld können nun neue Filtergruppen hinzugefügt werden. Wählen Sie die gewünschte Filterart aus (im Beispiel ist das die Filtergruppe “Siegel”). Mittels **“Filtergruppe hinzufügen”** wird diese Filtergruppe im Filter ganz unten eingereiht.

Im **Bearbeiten Modus** ändert sich, neben den möglichen Aktionen in der Ribbon, auch die Ansicht im Filter. Durch die Pfeiltasten kann die Reihenfolge der Filtergruppen angepasst werden. 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

Oftmals ist es wichtig den Filter zu negieren.

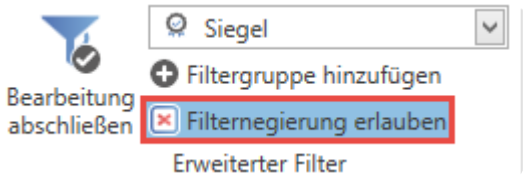
Relevante Einstellungen

Folgende Option ist zu beachten:

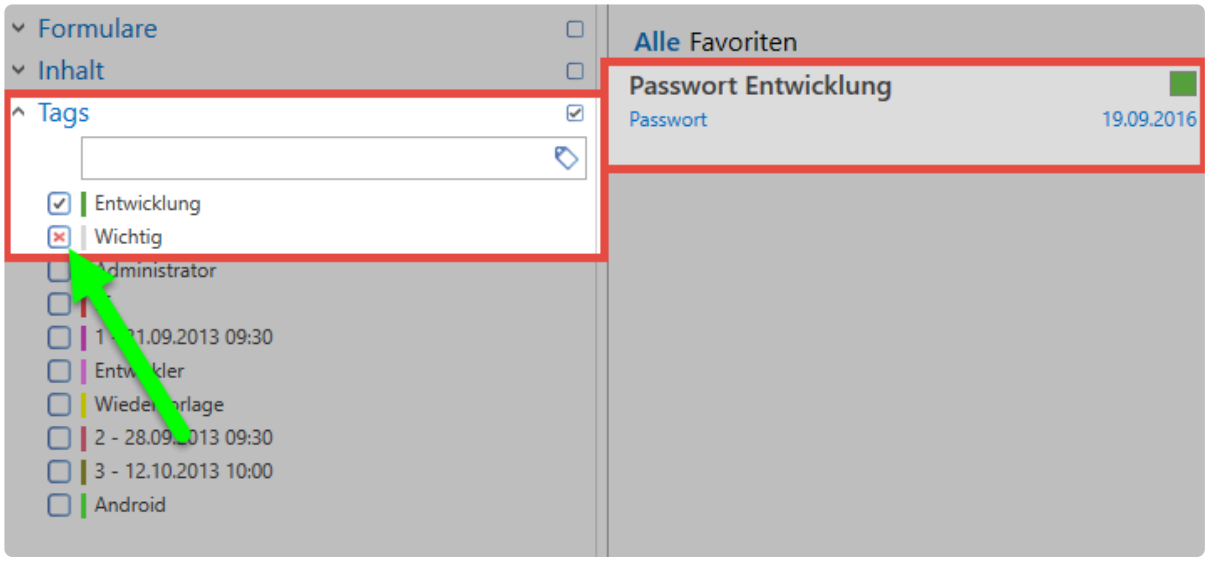
Einstellung

- Kann Filter-Negierung verwenden

Die Negierung können Sie im **Bearbeiten-Modus** aktivieren.



Somit können Sie die Ergebnisse 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 nicht 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.

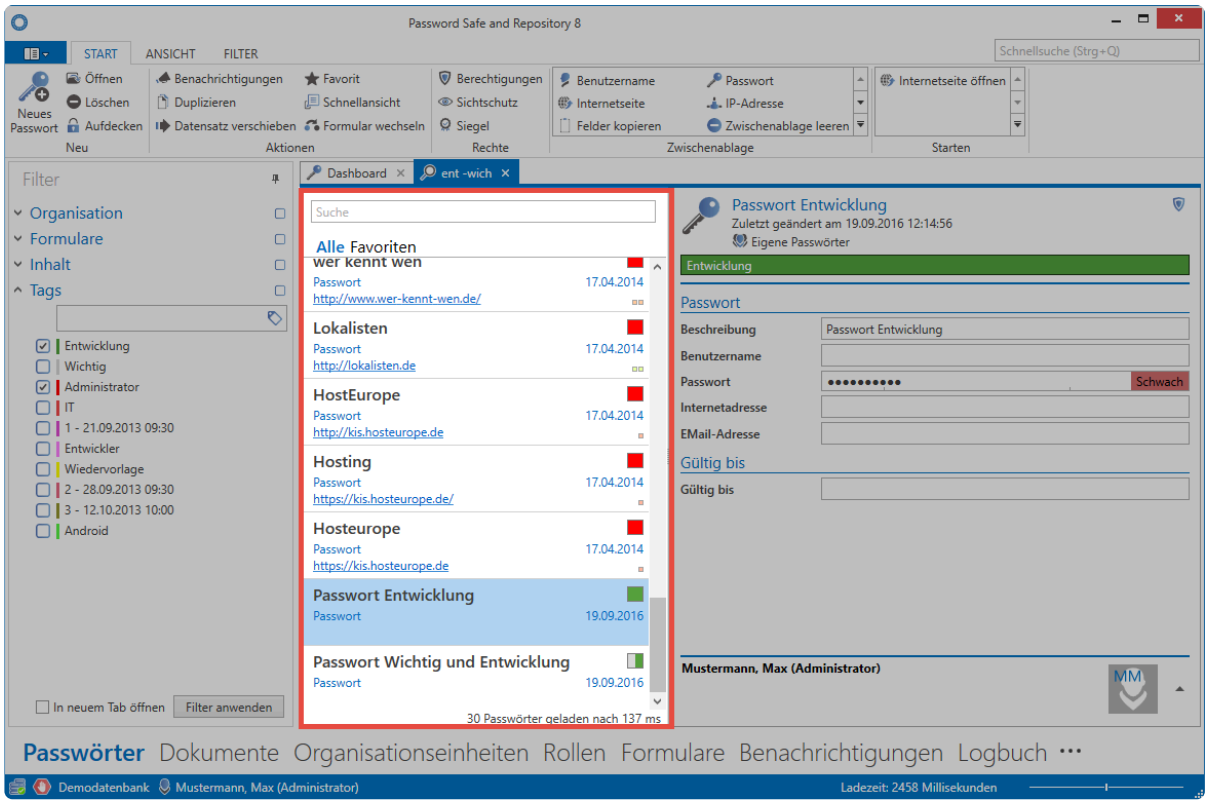
Listenansicht

Was ist die Listenansicht?

Die Listenansicht ist ein wesentlicher Bestandteil beim täglichen Arbeiten. Der Inhalt wird durch den aktuell angewendeten Filter definiert. **Die Listenansicht ist das Ergebnis eines durchgeführten Filters.** Zu dem in der Listenansicht aktuell markierten Datensatz werden im Lesebereich alle vorhandenen Formularfelder angezeigt.

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.



Relevante Einstellungen

Konfiguration der Anzahl angezeigter Datensätze (max. 500)

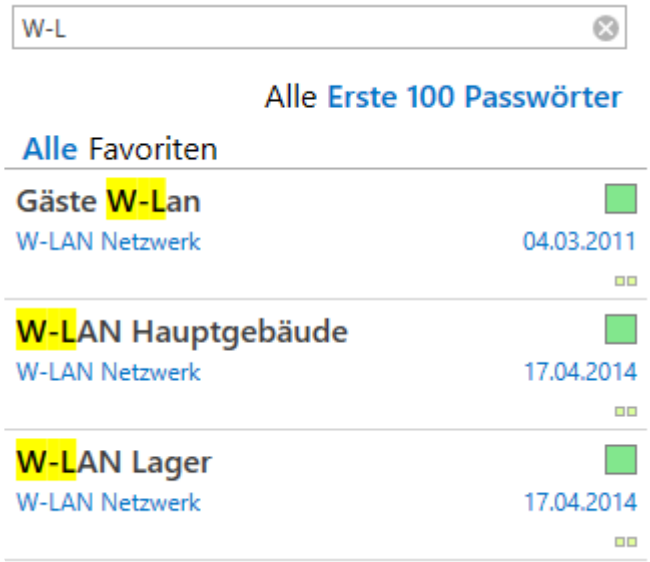
- **Anzahl der initial geladenen Datensätze**

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.

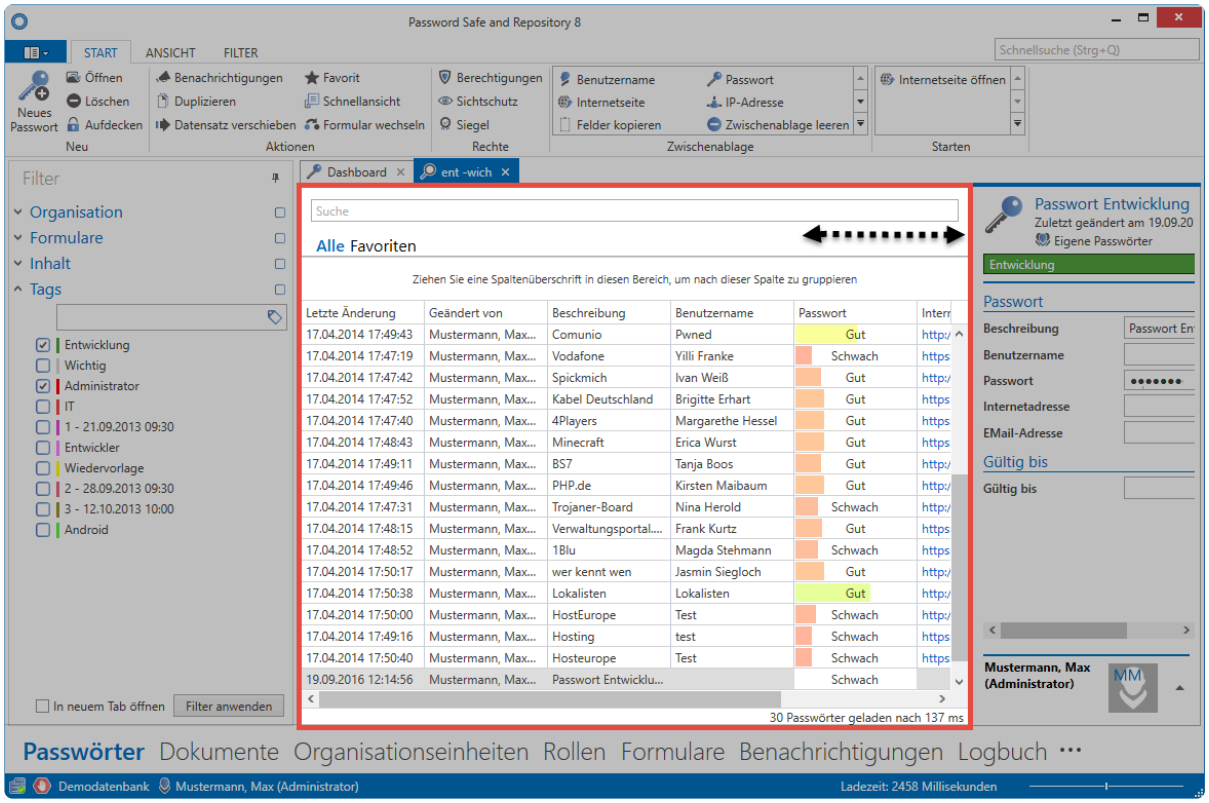
Suche in der Listenansicht

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



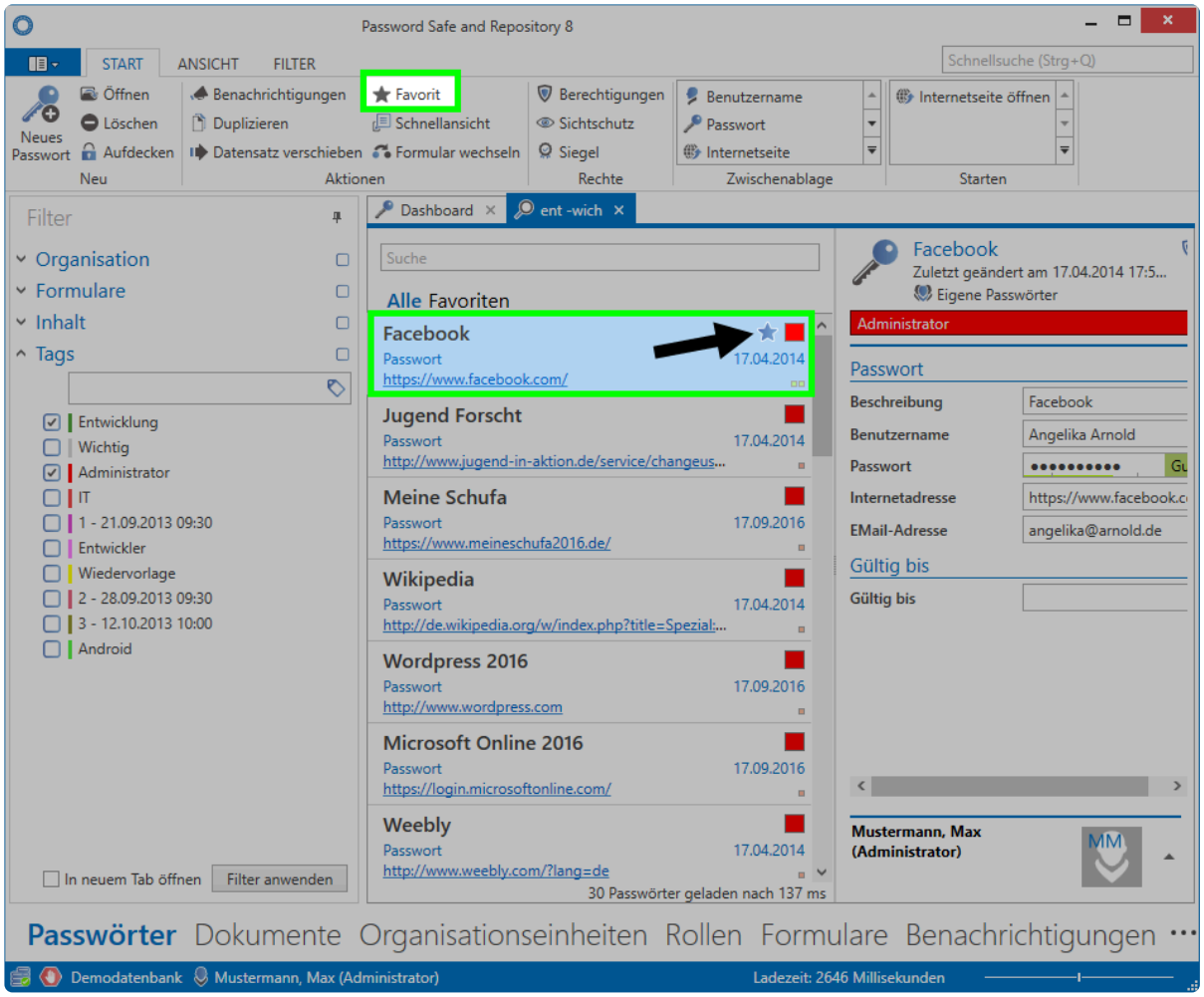
Detaillierte Listenansicht

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

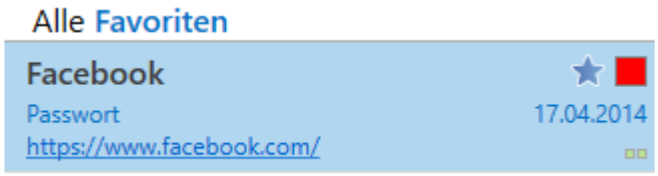


Favoriten

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 gekennzeichnet.



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



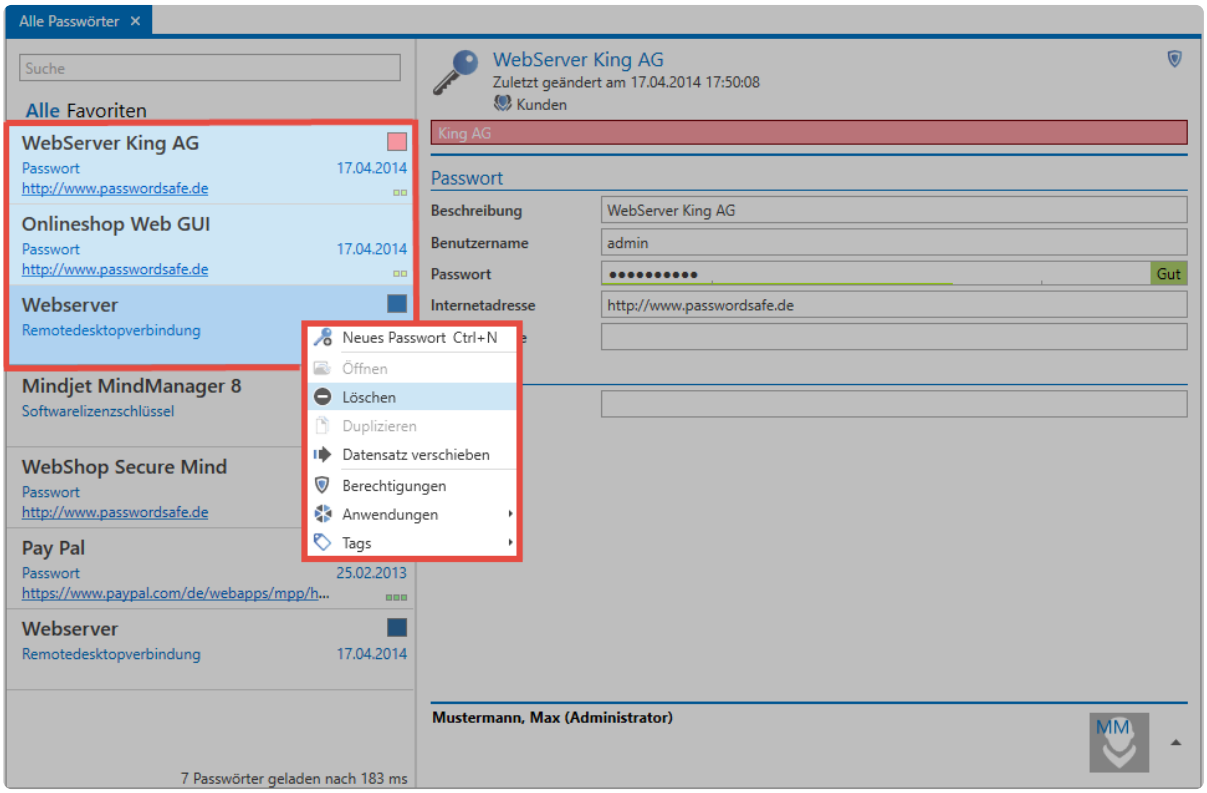
Weitere Symbole

Jeder in der Listenansicht angezeigte Datensatz besitzt rechtsbündig mehrere Symbole. Diese geben farblich Rückmeldung über die Passwortqualität, als auch die genutzten Tags. Mittels Mouseover-Tooltips erhalten Sie weitere Informationen.

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

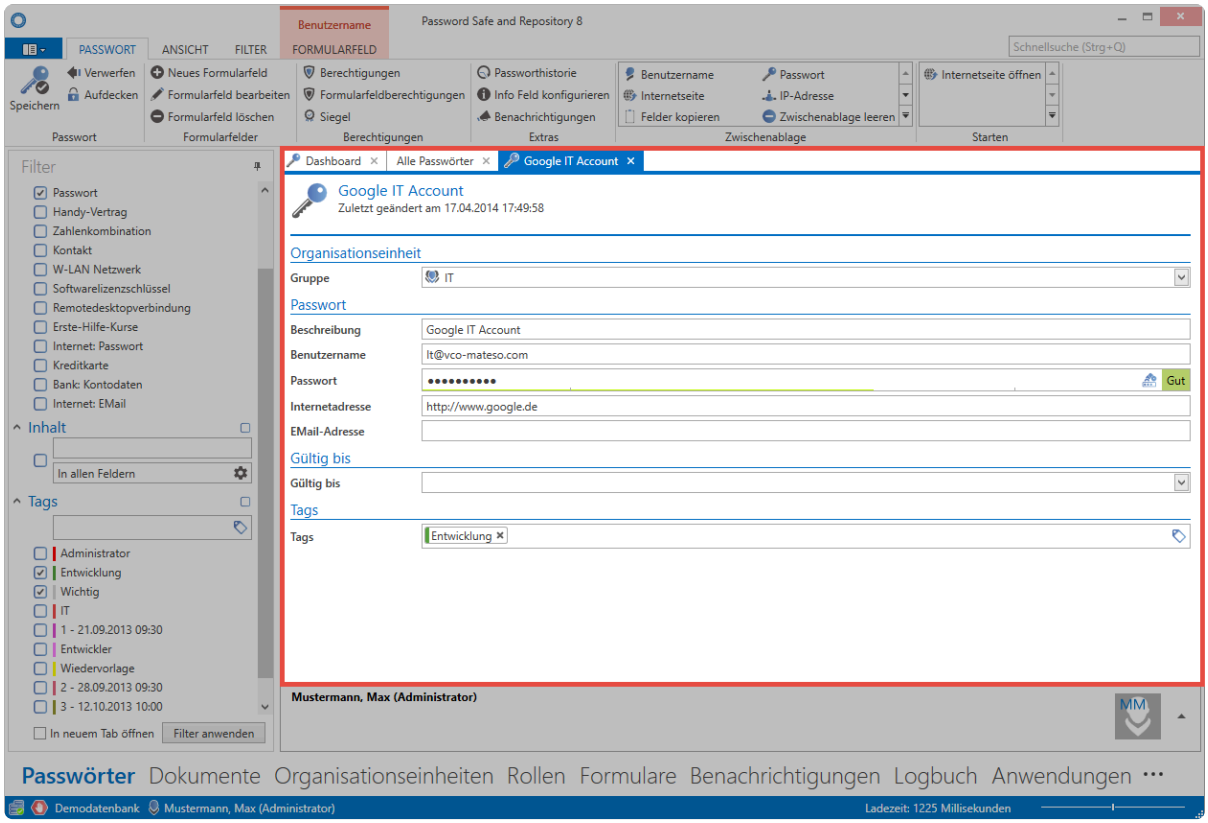
Arbeiten mit Datensätzen

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. Mittels Mausklick bei gedrückter Strg-Taste auf Datensätze ist auch eine Mehrfachauswahl möglich.



Öffnen und Bearbeiten von Datensätzen

Durch Doppelklick oder 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. Dabei wird die Listenansicht komplett verdeckt.

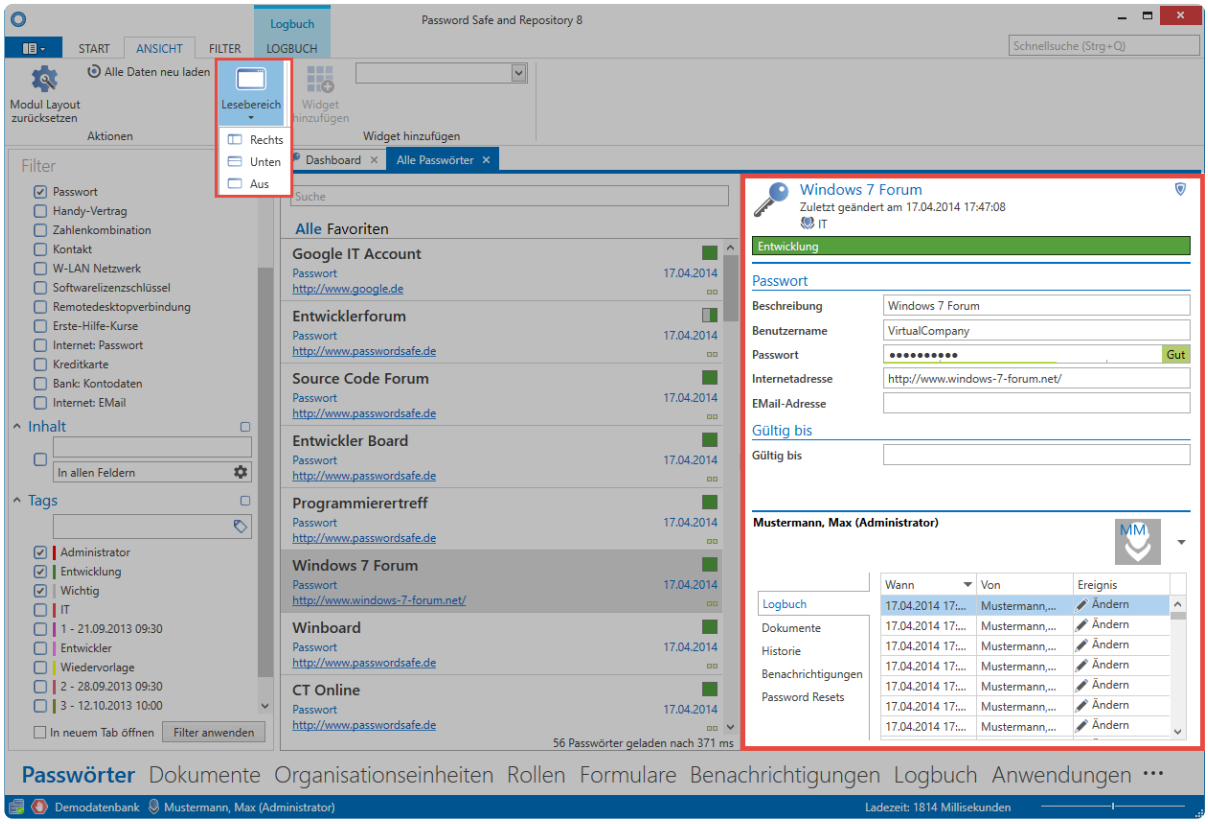


Das Arbeiten mit Datensätzen richtet sich natürlich stark nach der Art des Datensatzes. Egal ob Passwörter, Dokumente oder Organisationsstrukturen: Die Handhabe ist teils sehr unterschiedlich. Mehr Informationen hierzu entnehmen Sie deshalb bitte aus den jeweiligen Kapiteln über die einzelnen Module.

Lesebereich

Was ist der Lesebereich?

Der Lesebereich entspricht der Detailansicht einer in der Listenansicht ausgewählten Datensatzes Über die Ribbon kann der Lesebereich komplett deaktiviert oder die Position rechts oder unterhalb der Listenansicht festgelegt werden.



Vorraussetzungen

Die Sichtbarkeiten der einzelnen Reiter innerhalb des Footer-Bereichs sind über separate Benutzerrechte und Einstellungen gesichert.

Benutzerrechte

- Kann in Fußbereich Historie sehen
- Kann in Fußbereich Logbuch sehen
- Kann in Fußbereich Dokumente sehen
- Kann in Fußbereich die Metadaten von Dokumenten sehen
- Kann in Fußbereich Benachrichigungen sehen
- Kann in Fußbereich Password Reset sehen
- Kann in Fußbereich Mitgliedschaften sehen

Einstellungen

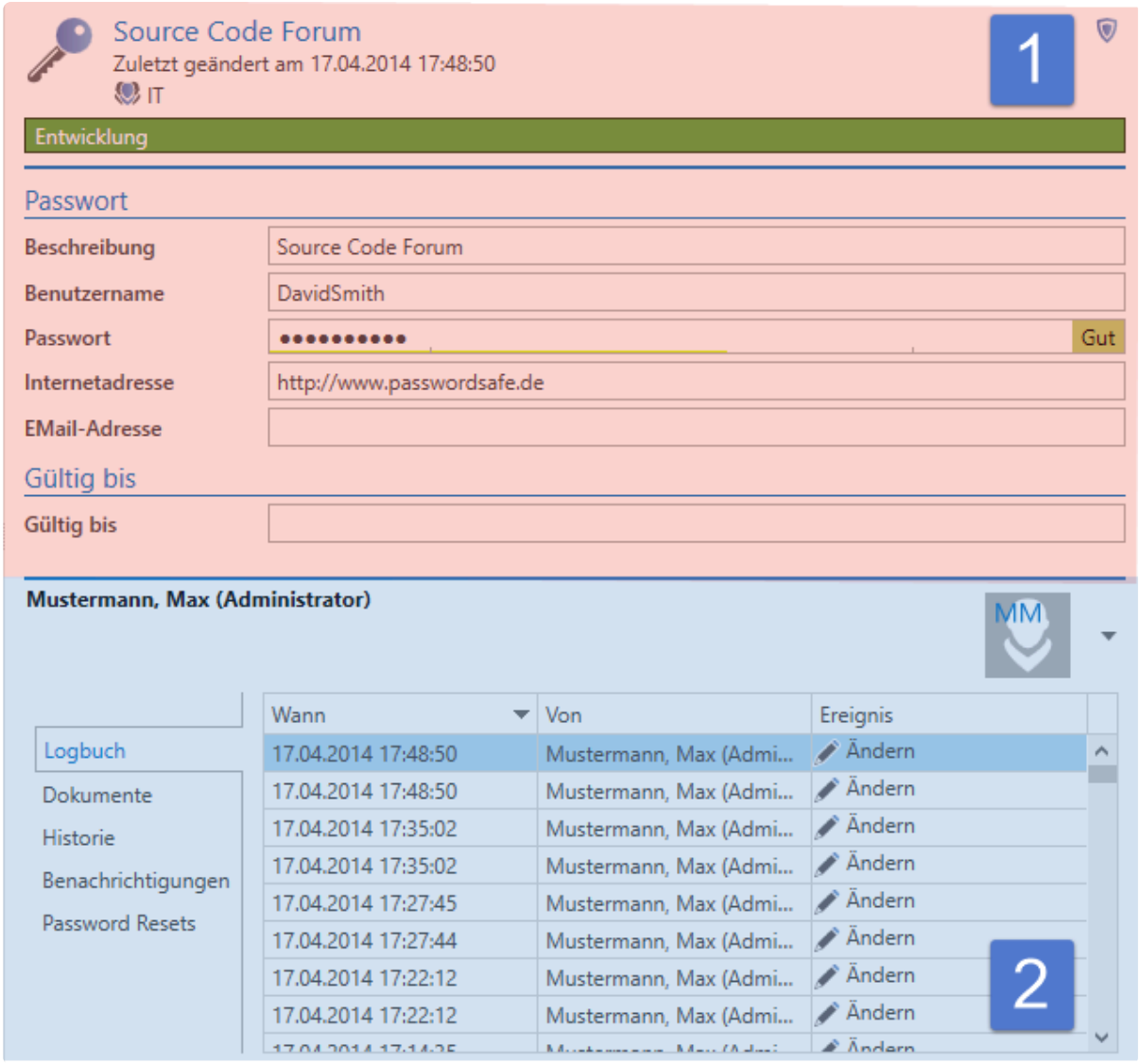
- Historie im Fußbereich anzeigen
- Logbuch im Fußbereich anzeigen

- Dokumente im Fußbereich anzeigen
- Metadaten im Fußbereich anzeigen
- Benachrichtigungen im Fußbereich anzeigen
- Password Resets im Fußbereich anzeigen
- Fußbereich anzeigen

Unterteilung des Lesebereichs

Der Lesebereich ist in zwei Bereiche unterteilt:

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



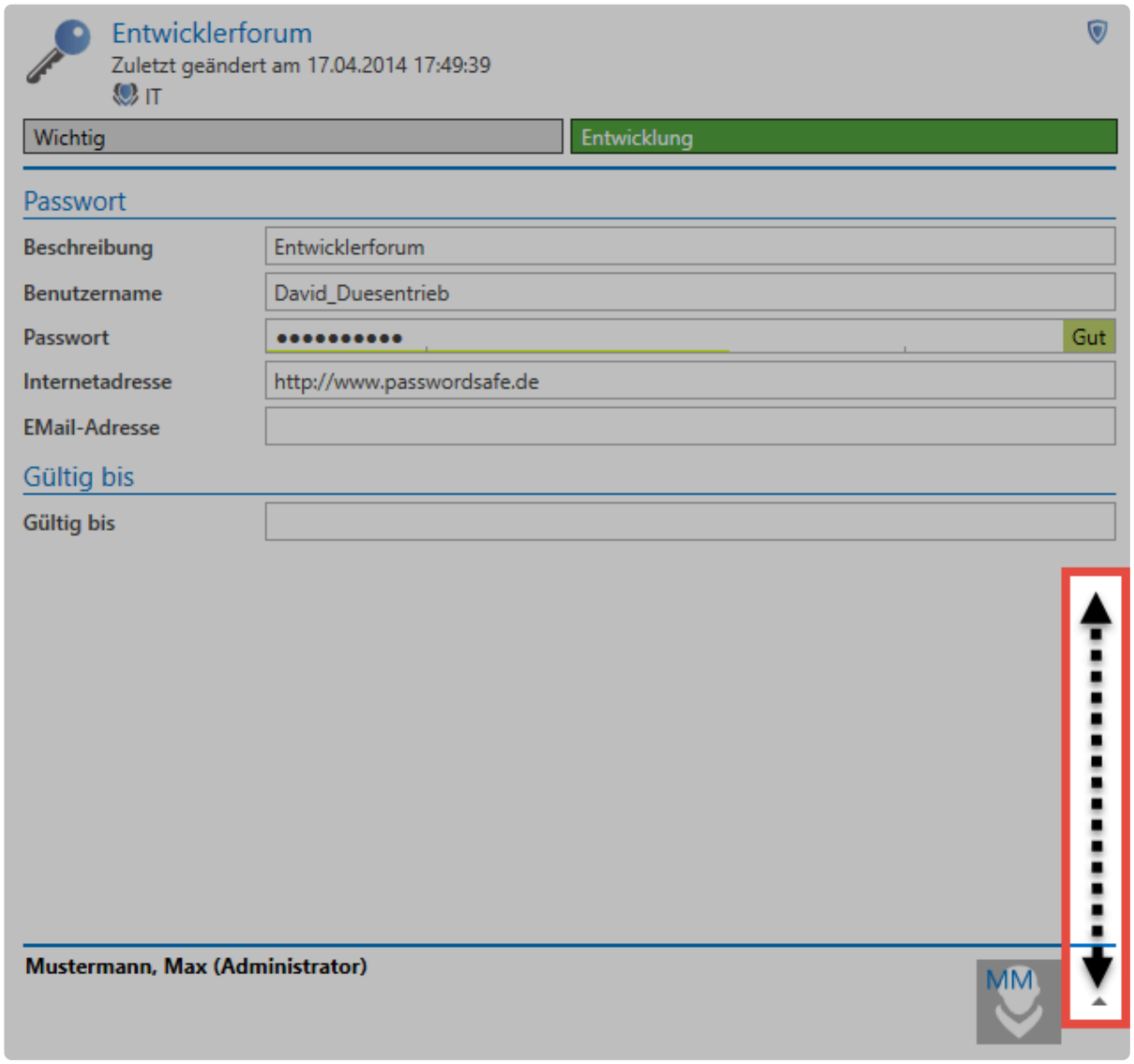
1. Detailbereich

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.

> ! Bitte beachten Sie, 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 können für den aktuell ausgewählten Datensatz diverse Informationen angezeigt werden können. Diese sind per default deaktiviert und lassen sich über den hierfür vorgesehenen Button anzeigen.



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.

Tags

Was sind Tags?

Fast jedes Objekt in Password Safe klassifizieren oder beschreiben Sie mittels des Tag-Systems. Dabei kann ein Objekt mehrere solcher Tags besitzen. Diese werden immer im Kopfbereich des Datensatzes angezeigt. Optional können Sie Tags mit Farben oder einem Beschreibungstext versehen. Sie prägen das Erscheinungsbild des Password Safe und sind optisch eine große Hilfe, um auch in großen Datenmengen nicht den Überblick zu verlieren.

Für Tags benötigt man keine Rechte – Jeder Benutzer kann alle Tags sehen!

Relevante Rechte

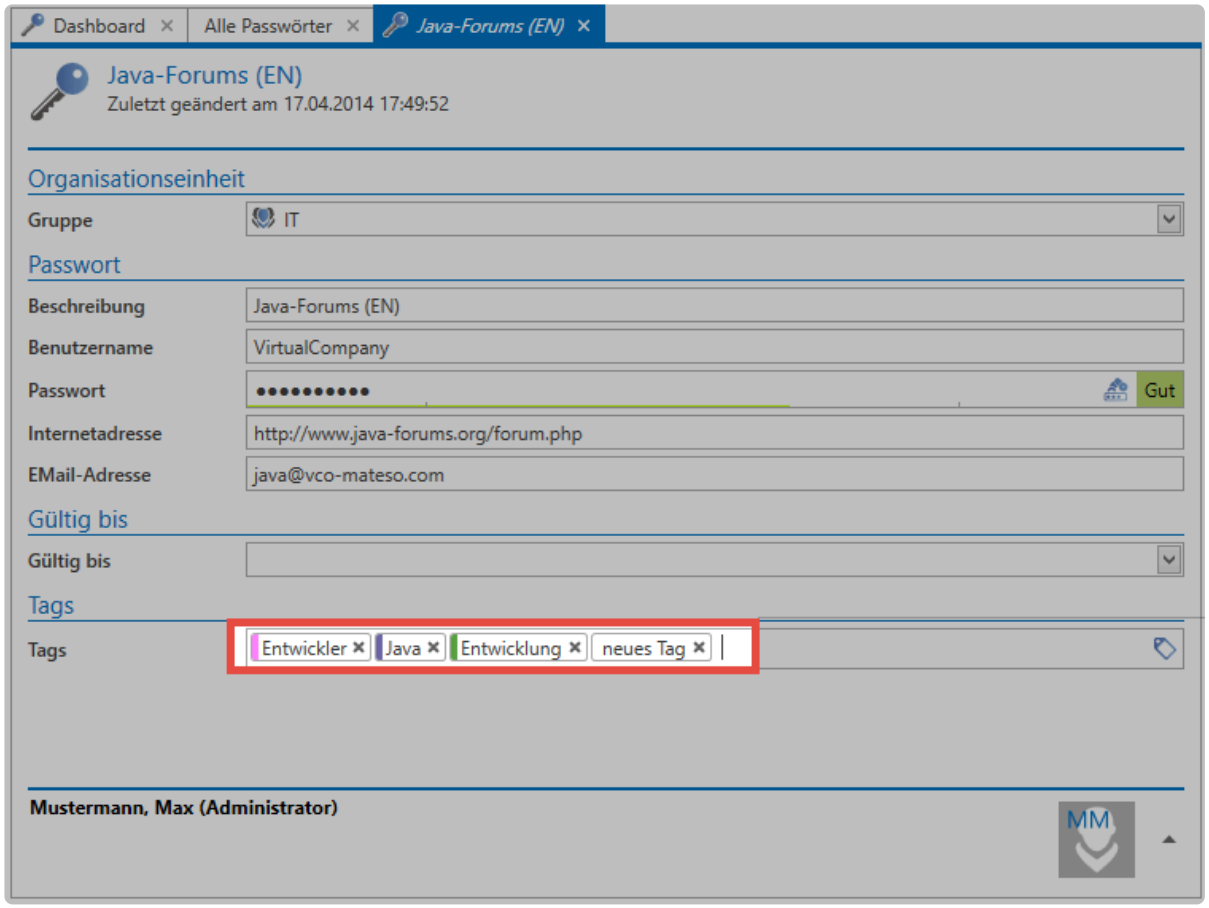
Zum Erstellen neuer Tags benötigen Sie folgende Option:

Benutzerrechte

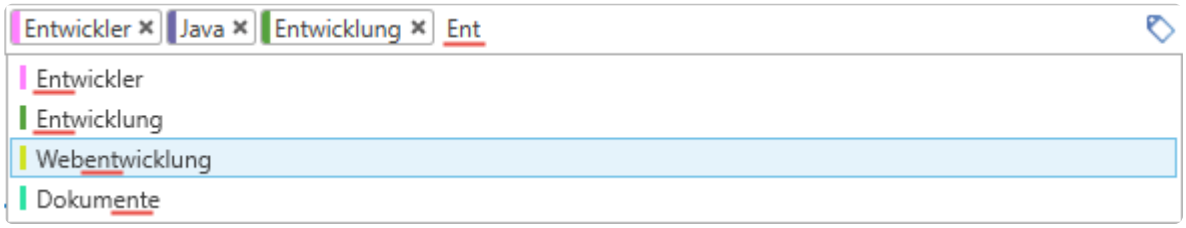
- Kann neue Tags anlegen

Hinzufügen von Tags zu Datensätzen

Tags fügen Sie einerseits direkt bei der Erstellung neuer, andererseits auch beim Bearbeiten existierender Datensätzen hinzu. Das Vorgehen ist dabei gleich. Im Bearbeiten Modus befinden sich die Tags stets an unterster Stelle.

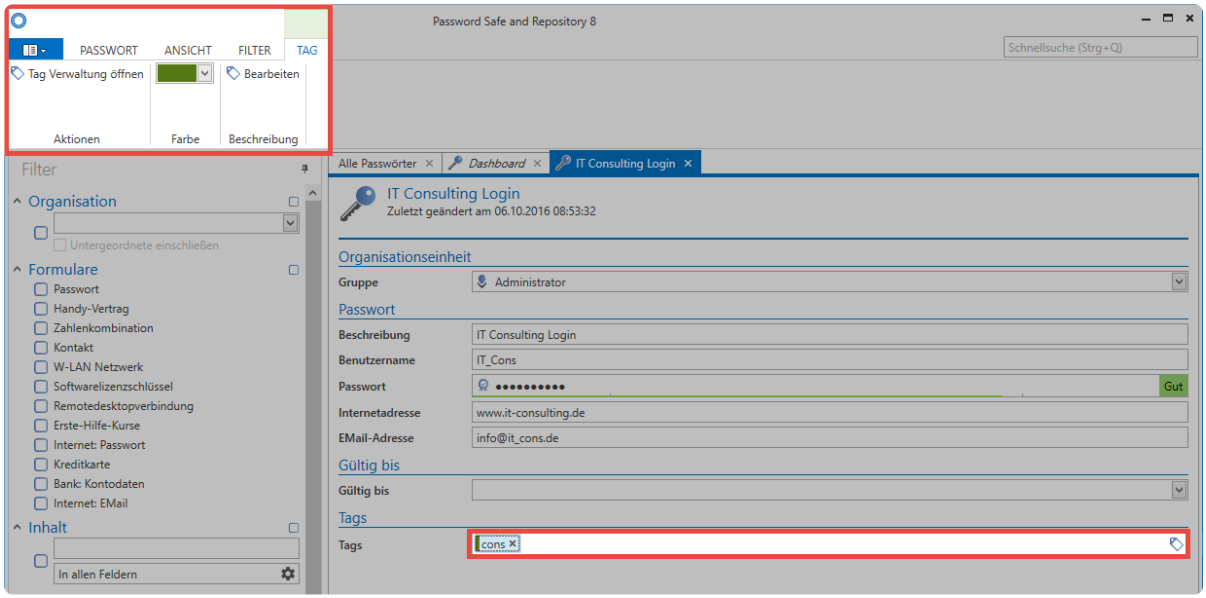


Die Bedienung ist hierbei intuitiv. Ab dem dritten eingegebenen Buchstaben werden bereits vorhandene Tags nach Volltext durchsucht. Fügen Sie den gewünschten Tag anschließend hinzu. Sowohl die Navigation mit der Maus als auch mit der Tastatur ist möglich. Mittels “Return”-Taste legen Sie einen neuen Tag direkt an.



Tags in der Ribbon

Bearbeiten Sie einen Datensatz und markieren Sie hierbei einen vorhandenen oder auch neuen Tag, erscheint in der Ribbon ein dementsprechender Content Tab. Hier öffnen Sie die Tagverwaltung oder passen die Farbe und Beschreibung des Tags direkt an.



Verwaltung von Tags

In den Extras im FullClient als auch im WebClient finden Sie zudem die Tagverwaltung zur Bearbeitung aller vorhandenen Tags.

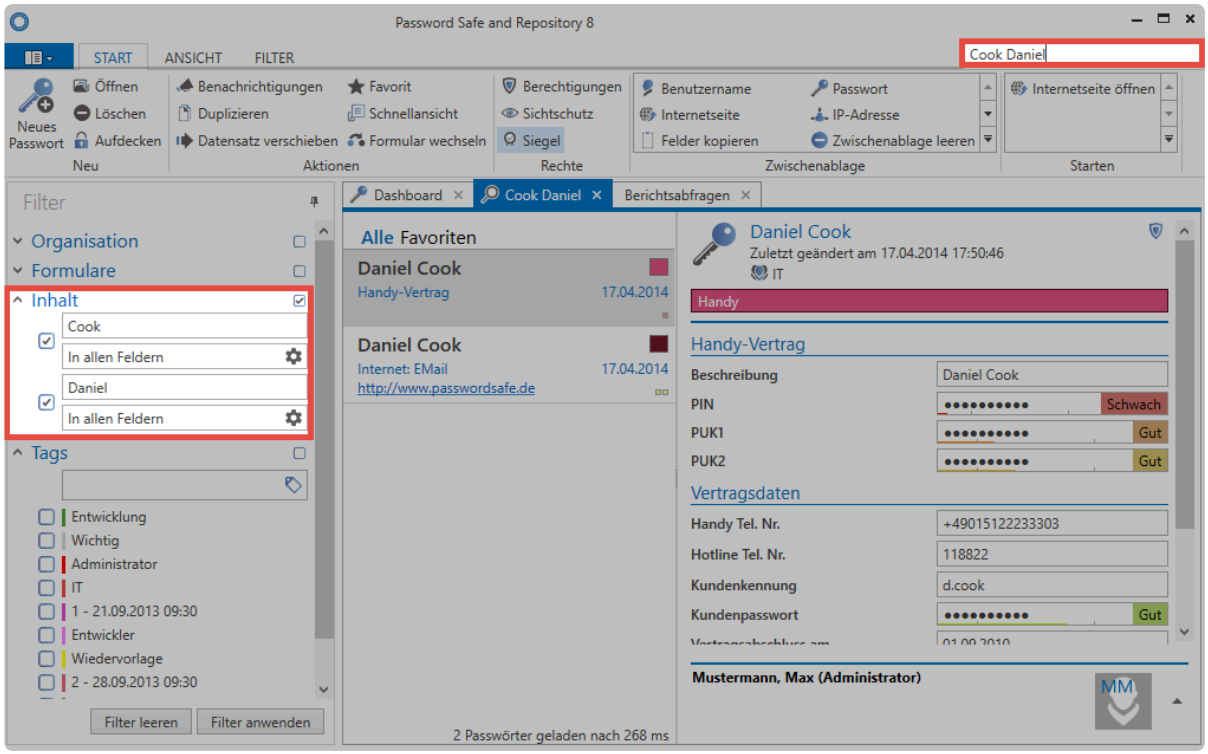
Suche

Was ist die Suche?

Mit Hilfe der Suche können Sie in der Datenbank gespeicherte Daten anhand gewählter Kriterien finden. Es existieren grundsätzlich zwei Suchmodi:

1. Schnellsuche

Rechts oben in der Ribbon steht Ihnen jederzeit ein Suchfeld zur Verfügung. Es handelt sich hierbei um eine Volltextsuche, die alle Felder und Tags außer dem Passwortfeld im gerade geöffneten Modul durchsucht.



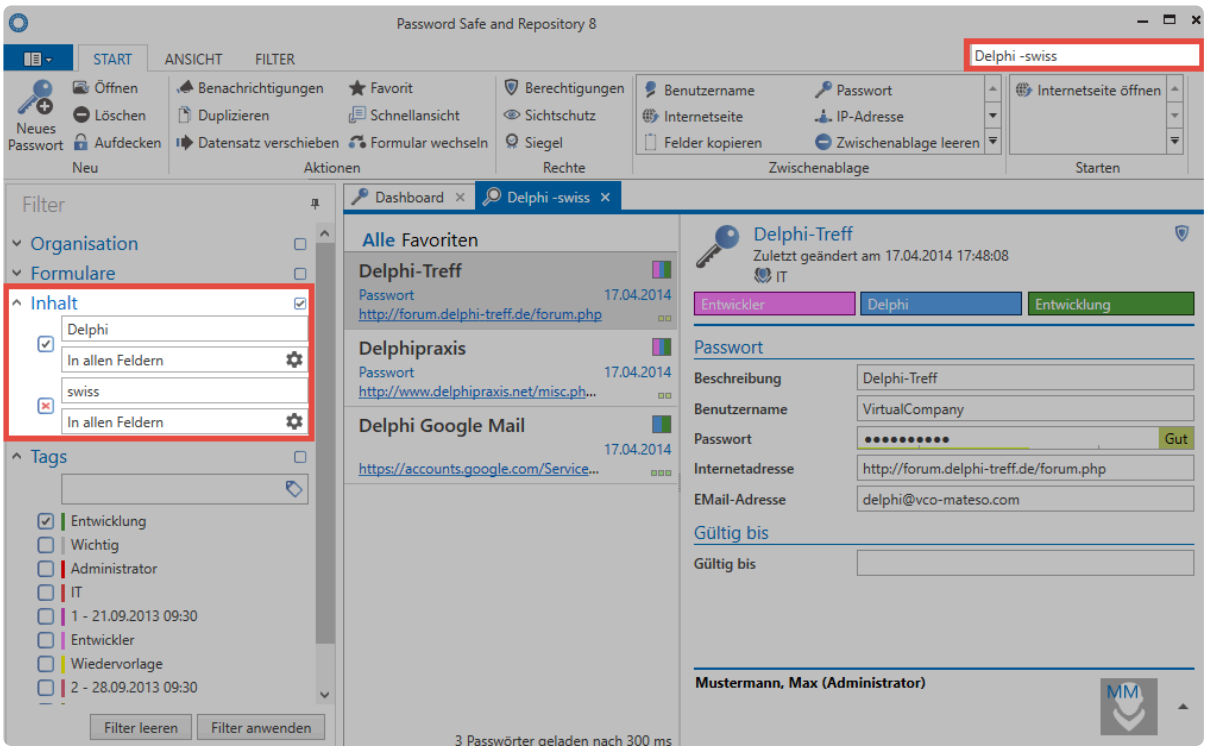
Die Schnellsuche ist eng mit dem Filter verbunden, da die Suchanfragen direkt in einen oder mehrere Inhaltsfilter umgewandelt werden. Eine Suche können Sie auch mit durch Leerzeichen getrennten Begriffen durchführen, wie beispielsweise **Cook Daniel**. Dabei werden zwei getrennte Inhaltsfilter erstellt, die 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, müssen Sie den Ausdruck in Anführungszeichen setzen: **“Cook Daniel”**. Die Suche ist nicht „case sensitiv“.

> Über **Strg + Q** können Sie direkt auf die Schnellsuche zugreifen!

Negierungen in der Schnellsuche

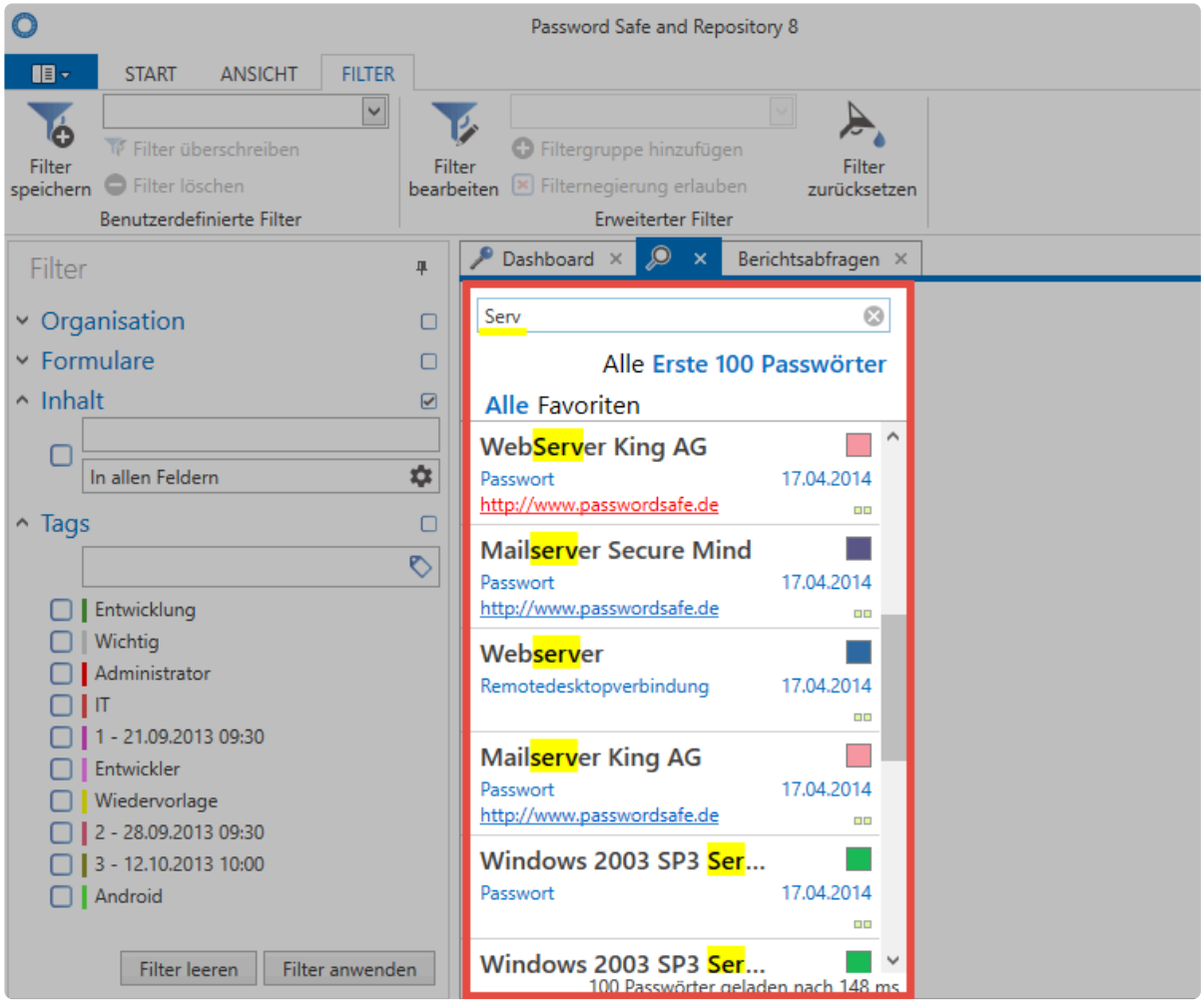
Negierungen schränken die Ergebnismenge so ein, dass bestimmte Kriterien nicht erfüllt sein dürfen. Im nachfolgenden Beispiel werden alle Datensätze gesucht, die zwar den Ausdruck **Delphi** beinhalten, jedoch nicht den Ausdruck **swiss**. Die Notation, welche Sie in der Schnellsuche eingegeben müssen,

lautet hierzu: **Delphi -swiss**



2. Listensuche

Mit der Listensuche im Header der Listenansicht können Sie die Ergebnismenge des Filters weiter durchsuchen. 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.



Bei der Suche mittels Filter wird eine direkte Datenbankabfrage durchgeführt. Die Listensuche sucht lediglich innerhalb einer bereits getätigten Abfrage.

> Die Listensuche ist standardmäßig ausgeblendet. Sie können sie mit “**Strg + F**” aktivieren.

Drucken

Was bietet die Druckfunktion?

Gelegentlich ist es sinnvoll, in **Password Safe** gespeichert Daten zur Dokumentation auszudrucken. Sie können Datensätze wie z.B. Passwörter oder auch Informationen zu Organisationseinheiten und vieles mehr ausdrucken.

Relevante Rechte

Folgende Rechte sind relevant.

Datensatz Rechte

- Es wird jeweils das Recht **Drucken** auf den jeweiligen Datensatz benötigt.

Benutzerrecht

- Kann drucken

Verfügbarkeit

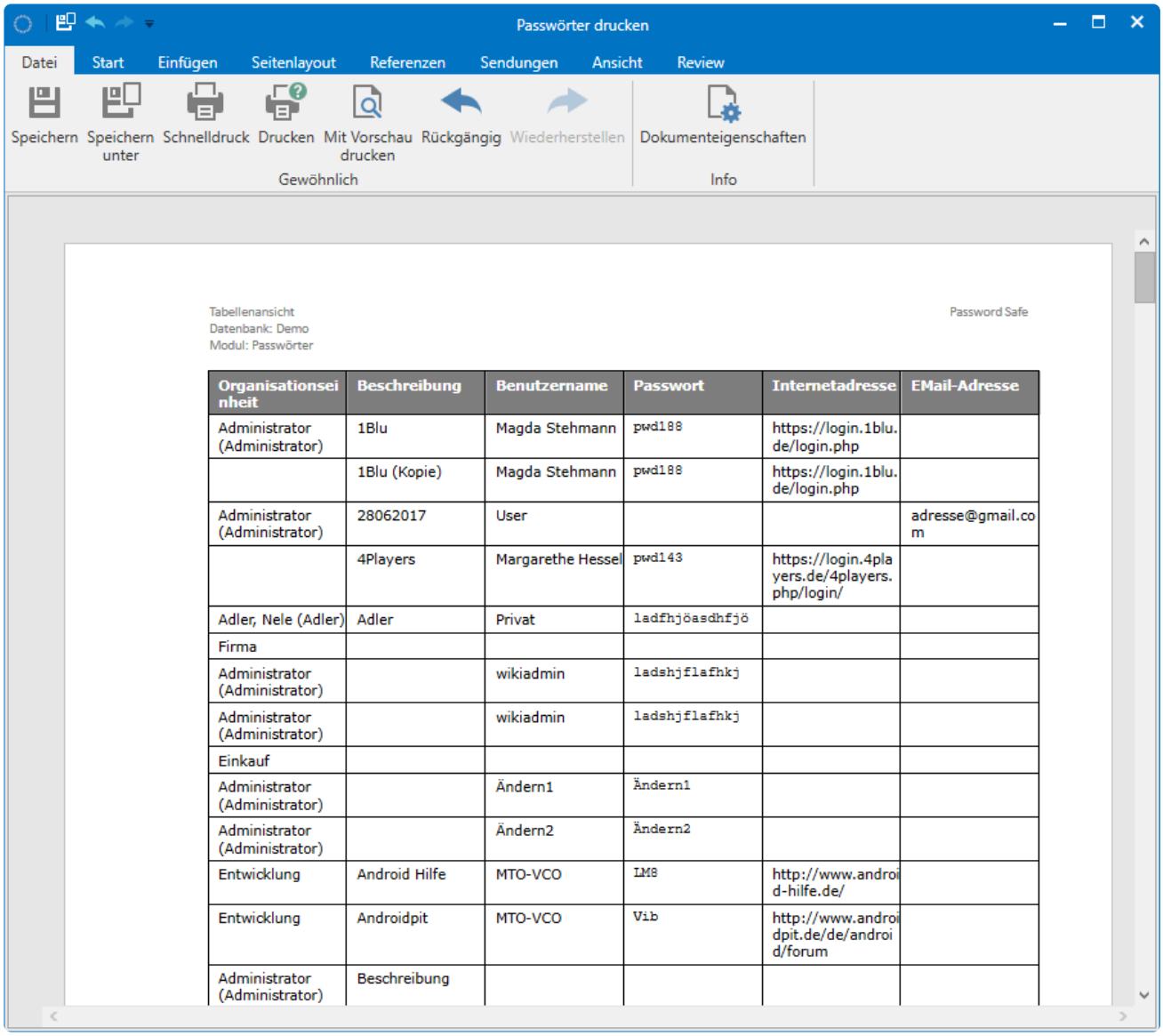
Die Druckfunktion steht Ihnen in folgenden Modulen zur Verfügung:

- Passwörter
- Dokumente
- Organisationsstruktur
- Rollen
- Formulare

Bedienung der Druckfunktion

Die Druckfunktion können Sie über die Ribbon aufrufen.

Selektieren Sie zunächst, ob in einer Tabelle oder detaillierten Ansicht gedruckt werden soll. Auch die Datenmenge können Sie festlegen. Die einzelnen Menüpunkte werden weiter unten im Kapitel ausführlich erläutert. Nach der Selektion werden zunächst die Daten zum Drucken vorbereitet. Je nach Datenmenge kann dies einige Minuten in Anspruch nehmen. Anschließend öffnet sich die **Druckvorschau**.



Organisationseinheit	Beschreibung	Benutzername	Passwort	Internetadresse	EMail-Adresse
Administrator (Administrator)	1Blu	Magda Stehmann	pwd188	https://login.1blu.de/login.php	
	1Blu (Kopie)	Magda Stehmann	pwd188	https://login.1blu.de/login.php	
Administrator (Administrator)	28062017	User			adresse@gmail.com
	4Players	Margarethe Hessel	pwd143	https://login.4players.de/4players.php/login/	
Adler, Nele (Adler)	Adler	Privat	ladfhjöasdhfjö		
Firma					
Administrator (Administrator)		wikiadmin	ladshjflafhkj		
Administrator (Administrator)		wikiadmin	ladshjflafhkj		
Einkauf					
Administrator (Administrator)		Ändern1	Ändern1		
Administrator (Administrator)		Ändern2	Ändern2		
Entwicklung	Android Hilfe	MTO-VCO	LM8	http://www.android-hilfe.de/	
Entwicklung	Androidpit	MTO-VCO	Vib	http://www.androidpit.de/de/android/forum	
Administrator (Administrator)	Beschreibung				

> Die **Druckvorschau** greift auf Funktionen des Druckertreibers zu. Je nach verwendetem Drucker bzw. Treiber kann die **Druckvorschau** daher sowohl optisch als auch vom Funktionsumfang her variieren. Auf die einzelnen Funktionen wird daher nicht näher eingegangen.

Über die **Druckvorschau** lösen Sie den Druck schlussendlich aus. Sie haben auch die Möglichkeit, die Ansicht zu speichern oder das Layout vor dem Druck anzupassen.

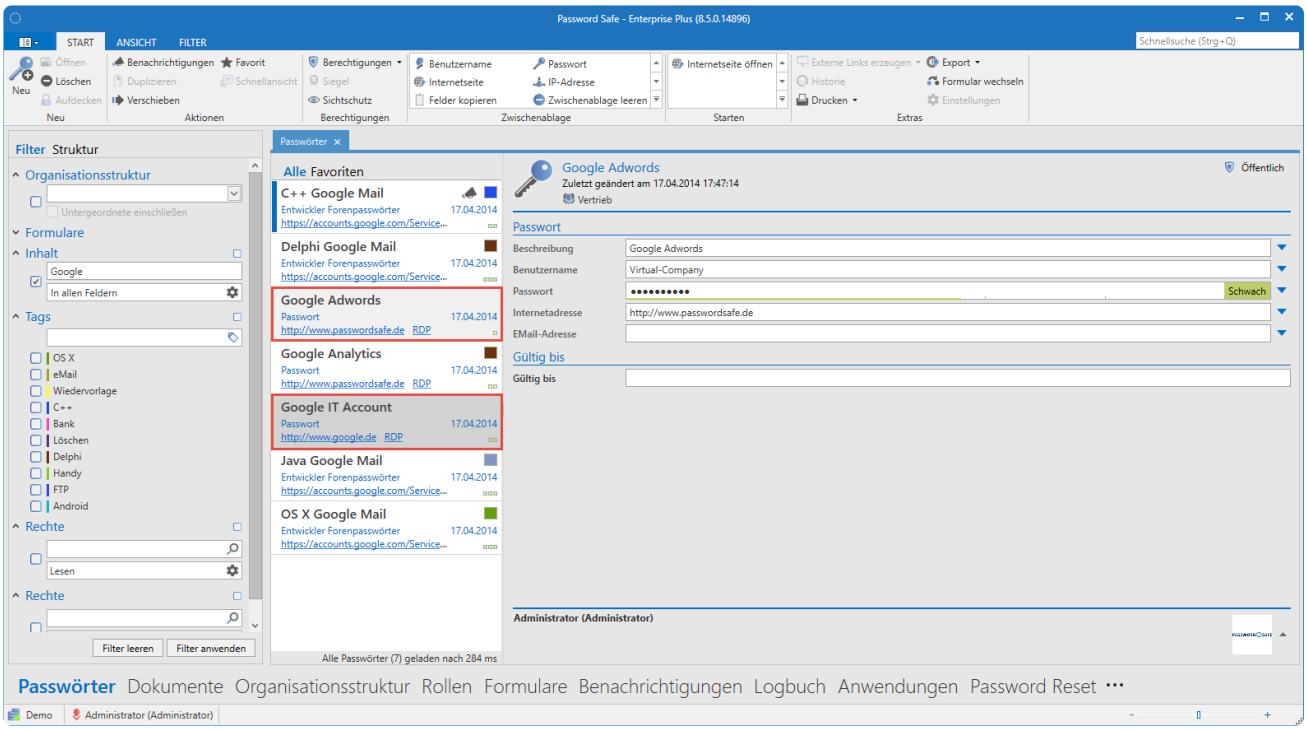
Selektion der zu druckenden Daten

Es stehen Ihnen mehrere Möglichkeiten zur Verfügung, um das Druckergebnis an die persönlichen Bedürfnisse anzupassen. Die einzelnen Menüpunkte werden folgend am Beispiel des Druckes von Passwörtern erläutert.

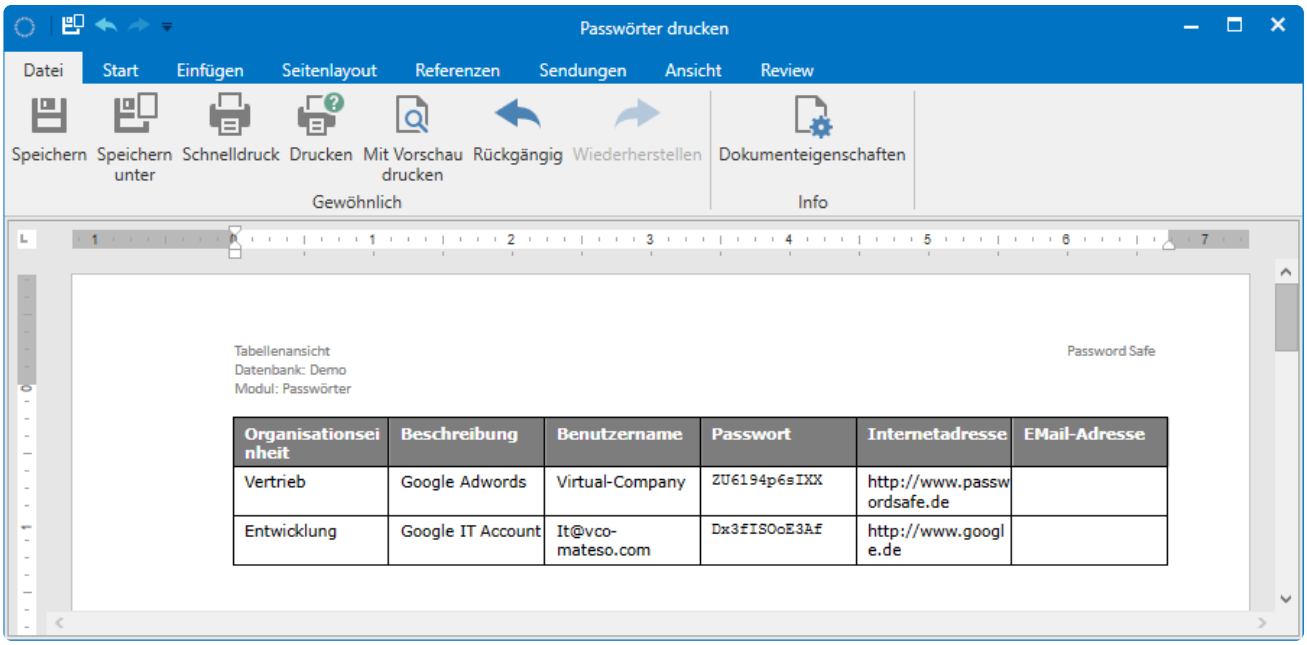
Tabellarische Ansicht (Aktuelle Auswahl)

Gedruckt werden alle **selektierten** Datensätze. In folgendem Beispiel also **Google Adwords** und

Google IT Account.



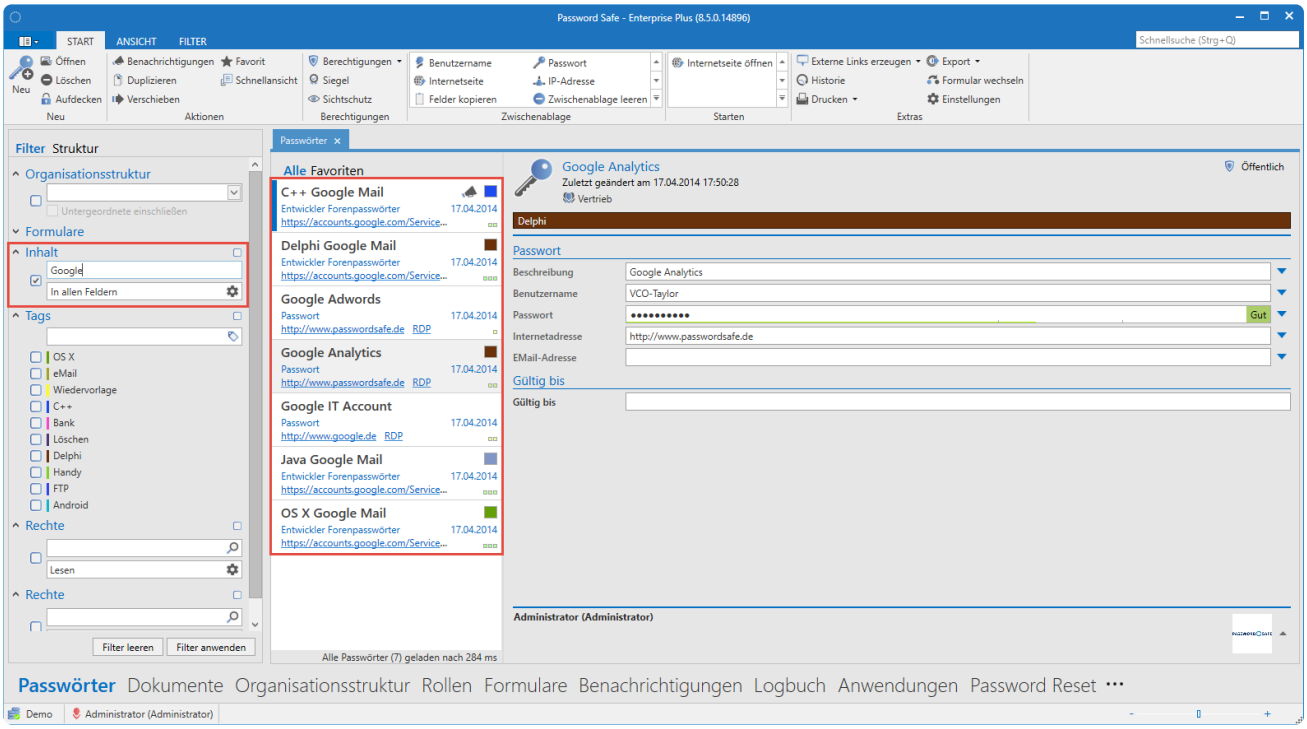
Die Daten werden hierbei in einer Tabelle gedruckt.



Organisationseinheit	Beschreibung	Benutzername	Passwort	Internetadresse	EMail-Adresse
Vertrieb	Google Adwords	Virtual-Company	ZU6194p6sIXX	http://www.passwordsafe.de	
Entwicklung	Google IT Account	It@vco-mateso.com	Dx3fISOoE3Af	http://www.google.de	

Tabellarische Ansicht (Aktuelle Filter)

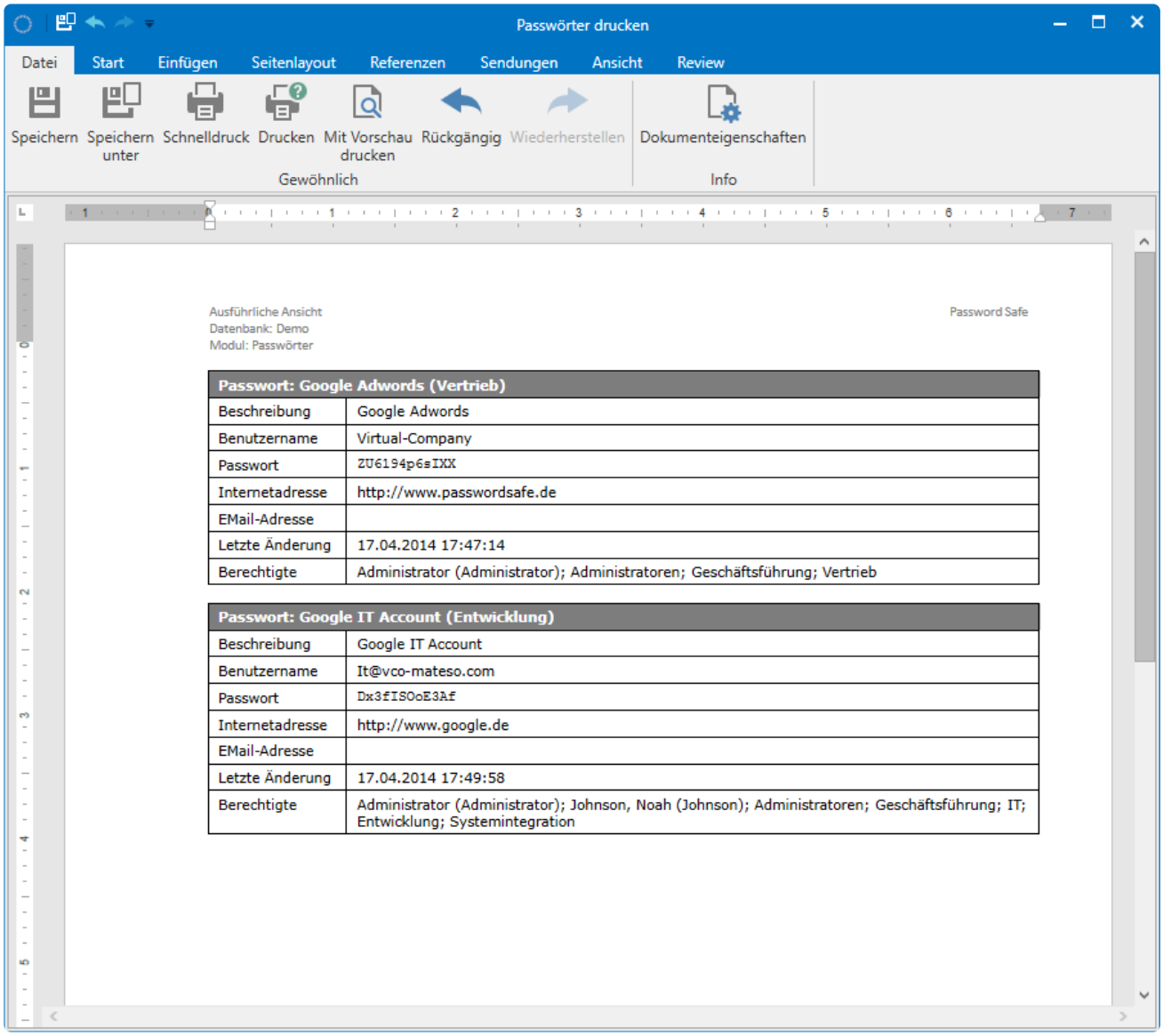
Hier werden alle aktuell **gefilterten** Datensätze gedruckt. In diesem Beispiel also alle sieben Datensätze.



Gedruckt wird – wie oben bereits beschrieben – in eine Tabelle.

Detaillierte Ansicht (Aktuelle Auswahl)

Diese Option druckt ebenfalls die aktuell selektieren Datensätze. Allerdings erfolgt der Druck in einer detaillierten Ansicht.



Detaillierte Ansicht (Aktuelle Filter)

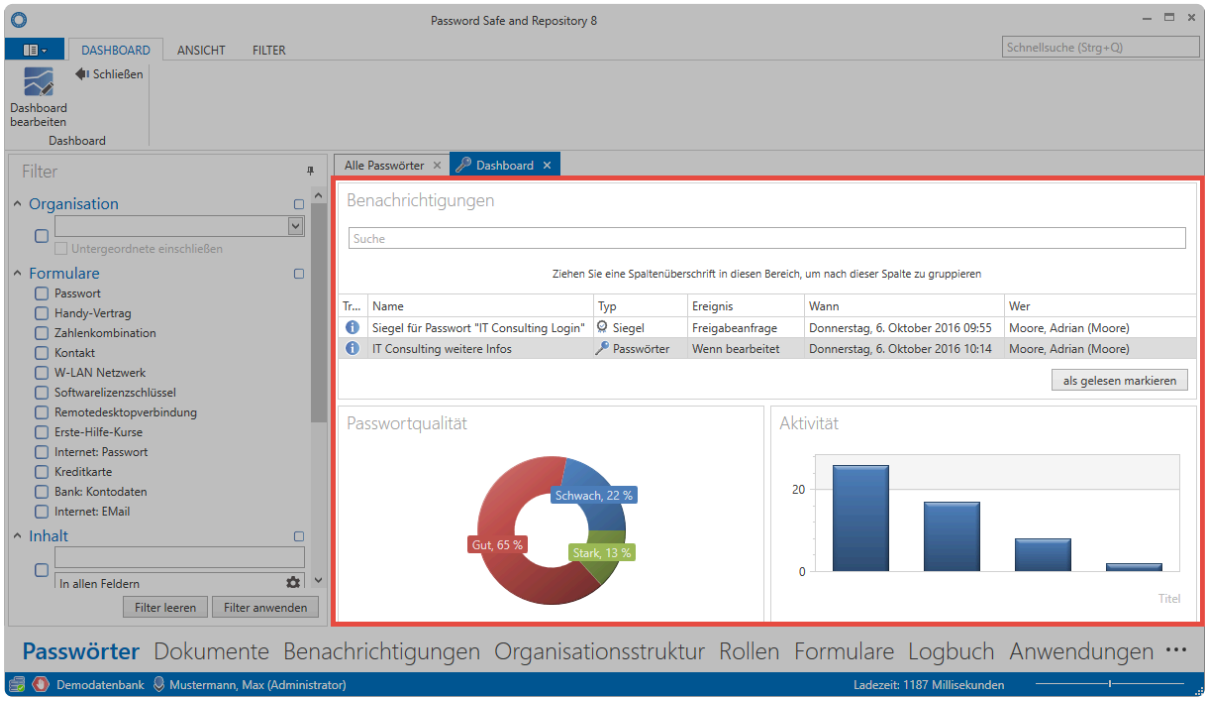
Über diese Funktion können alle gefilterten Datensätze in der oben beschriebenen Detailansicht gedruckt werden.

Bitte beachten Sie, dass die Datenmenge über diese Funktion schnell sehr groß werden kann.

Dashboard und Widgets

Was sind Dashboard und Widgets?

Dashboards erweitern die vorhandenen Filtermöglichkeiten um einen beliebig anpassbaren Info-Bereich, der visuell wichtige Ereignisse oder Fakten aufbereitet.



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

> Das Dashboard können Sie über den Button im Tab schließen. Erneut angezeigt wird es 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.

Relevante Einstellungen

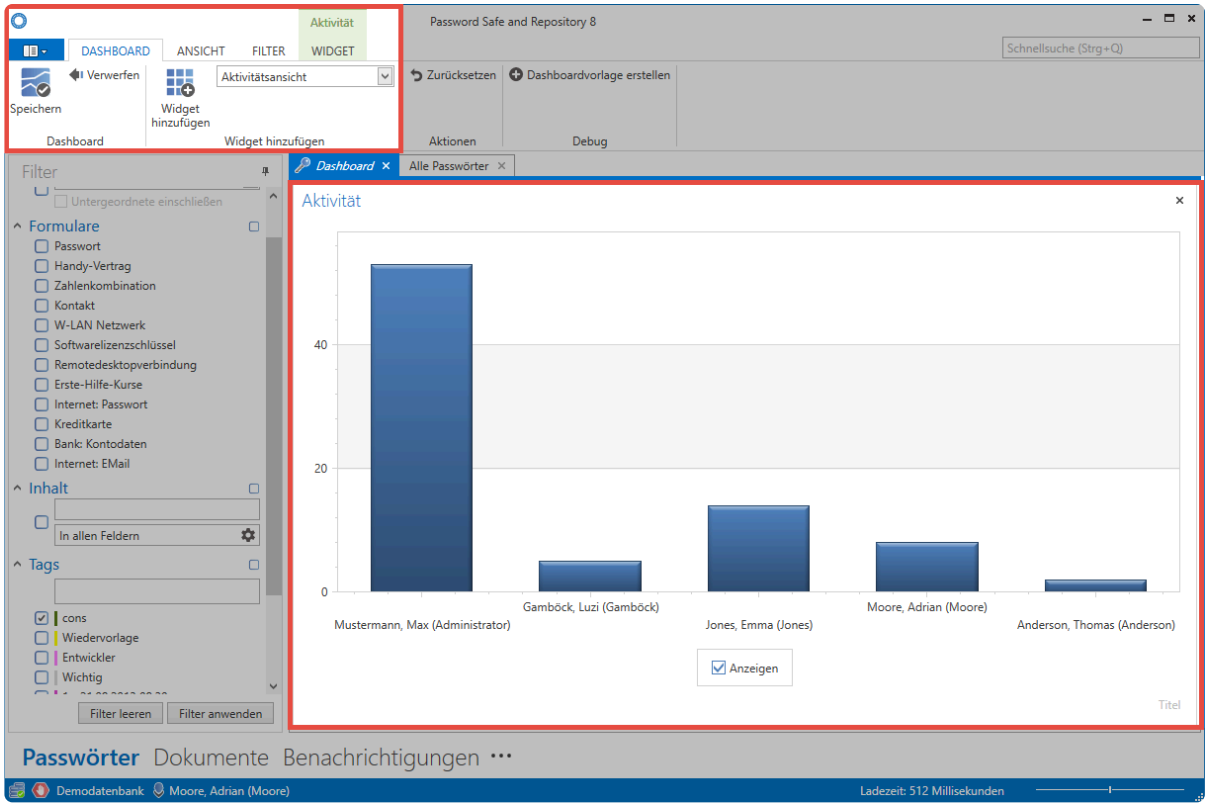
Folgende Optionen stehen im Zusammenhang mit Dashboard und Widgets zur Verfügung.

Einstellungen

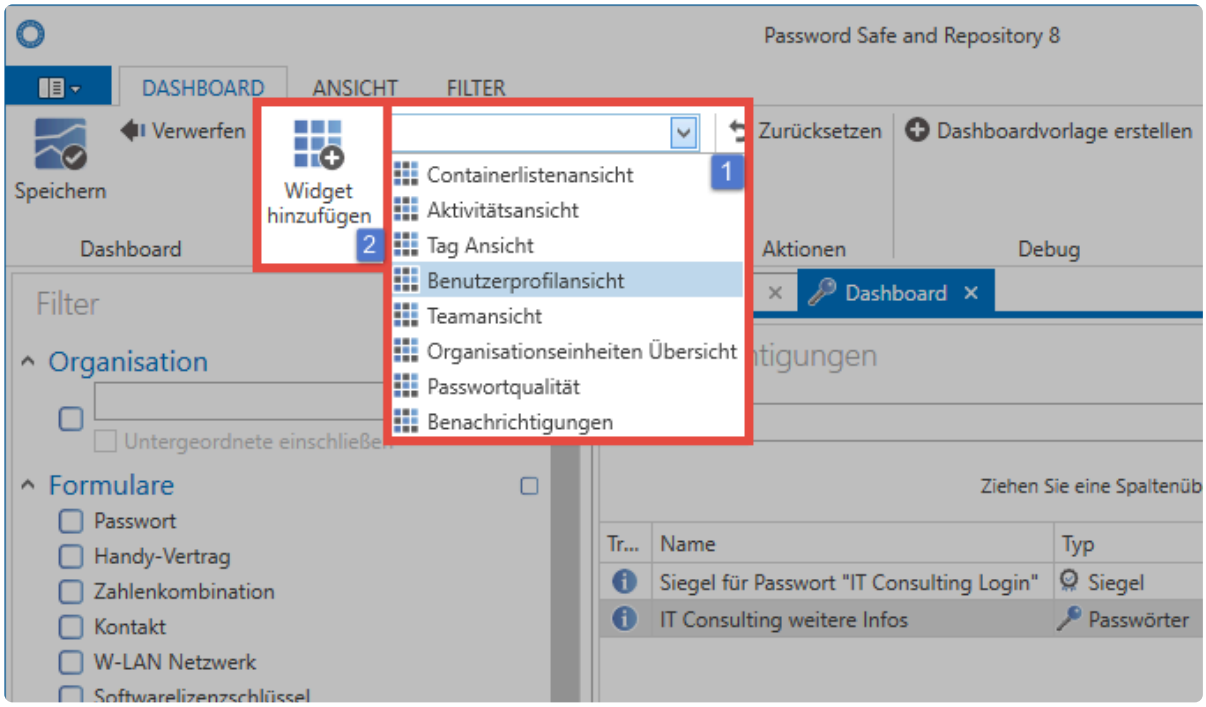
- Dashboard beim Start anzeigen
- Modulnamen in Dashboard anzeigen
- Anzahl der erlaubten Widgets
- Restanzahl der Daten im Widget anzeigen

Hinzufügen und Entfernen von Widgets

Bei aktiviertem Dashboard-Tab können Sie über die Ribbon den Bearbeitungsmodus für Dashboards aktivieren. Hier können Sie Widgets hinzufügen sowie bearbeiten.

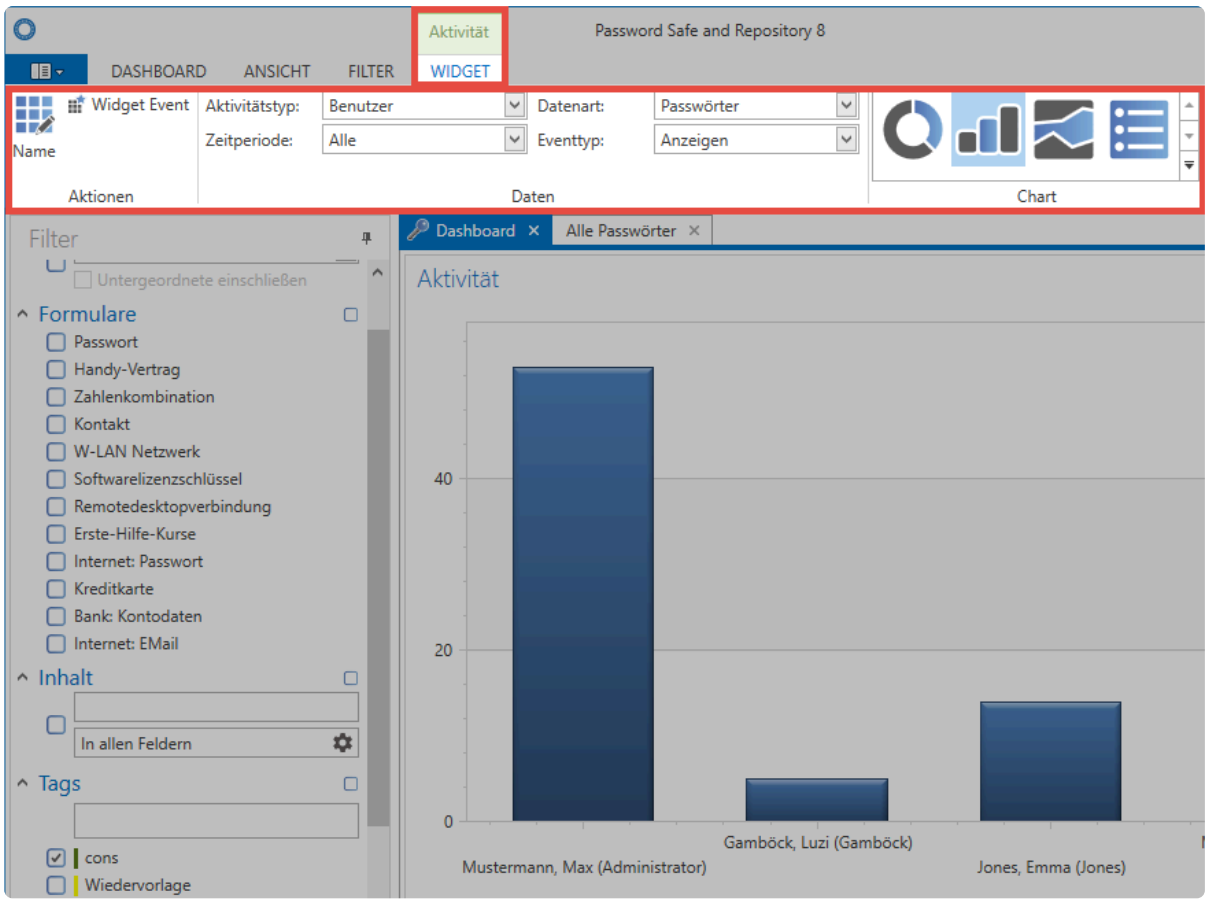


Über das Dropdown Menü wählen Sie ein Widget aus. **(1)**. Über den entsprechenden Button in der Ribbon **(2)** wird daraufhin das Widget dem Dashboard hinzugefügt. Die maximale Anzahl an Widgets, die hinzugefügt werden können, können Sie in den Benutzereinstellungen konfigurieren. Im Bearbeitungsmodus können Sie jedes Widget auch wieder über die Schaltfläche am rechten oberen Rand entfernen. Beendet wird der Bearbeitungsmodus durch Speichern über die Ribbon.



Anpassen von Widgets

Im Bearbeitungsmodus können Sie jedes Widget separat anpassen. Markieren Sie hierfür das Widget und wechseln Sie in der Ribbon in das sich öffnende **Widget-Content-Tab**.

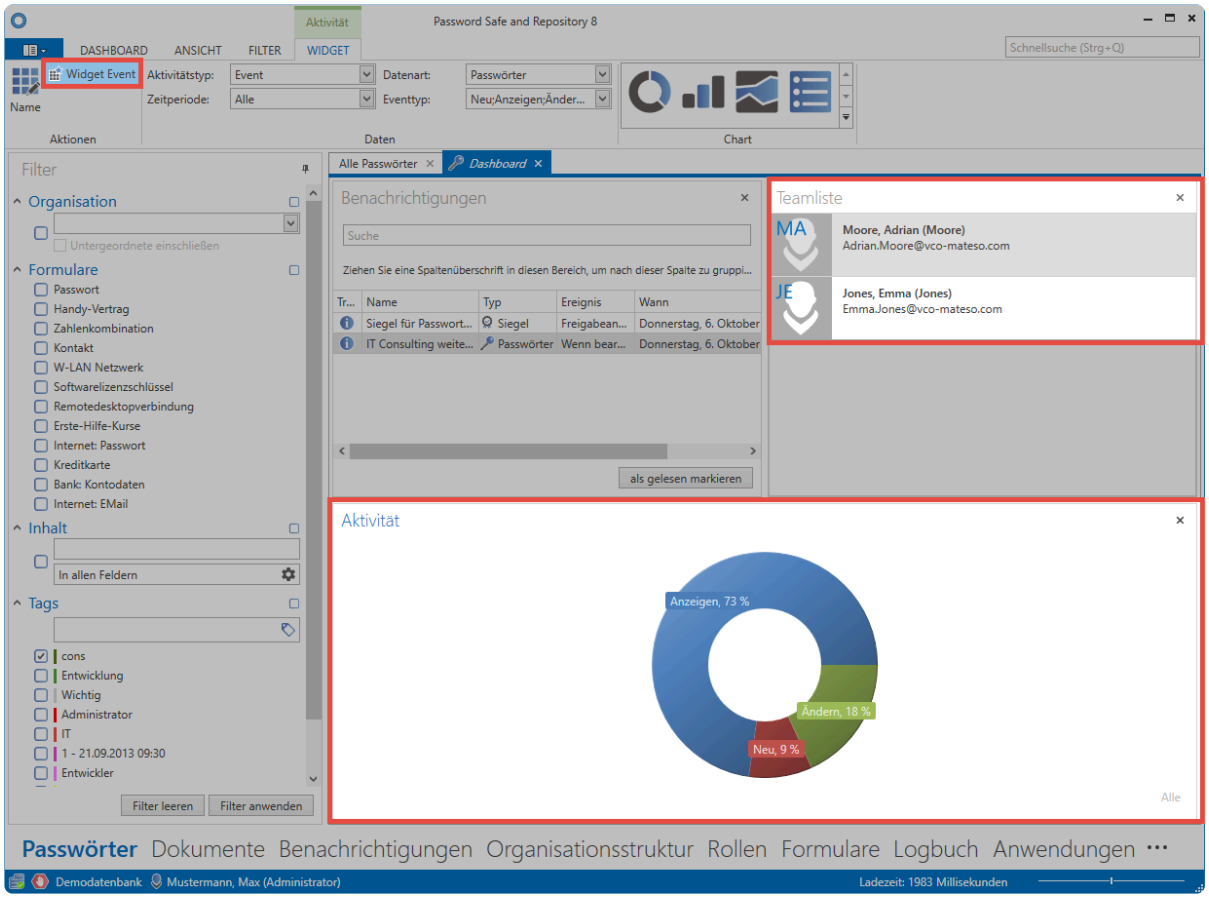


Für jedes Widget sind hier separate Variablen anpassbar. Im vorliegenden Beispiel wird angezeigt, wie oft sich Benutzer Passwörter angezeigt haben. Die Variablen sind natürlich je Widget individuell, da

jeweils andere Informationen relevant sein können.

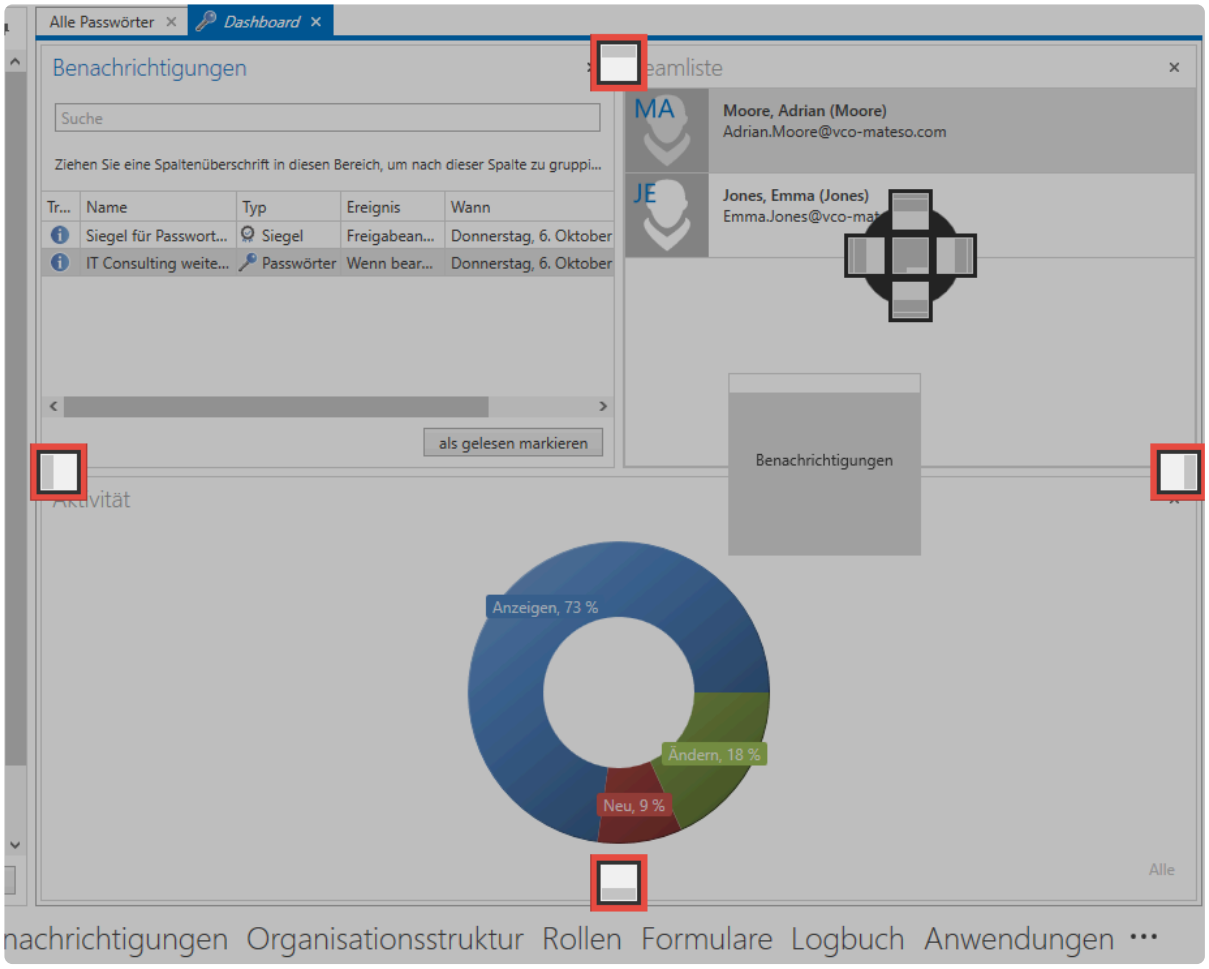
Widget Event

In der Ribbon können Sie die Option **Widget Event** auswählen. Hierdurch aktivieren Sie die Interaktion der Widgets untereinander. 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 angezeigt.



Anordnung der Widgets

Im Bearbeitungsmodus ist die Anordnung der Widgets frei definierbar. Durch Drag & Drop können Sie 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
MA
Moore, Adrian (Moore)
Adrian.Moore@vco-mateso.com
JE
Jones, Emma (Jones)
Benachrichtigungen
Aktivität
Anzeigen, 73 %
Ändern, 18 %
Neu, 9 %
Alle
nachrichtigungen
Organisationsstruktur
Rollen
Formulare
Logbuch
Anwendungen

Tastaturkürzel

Tastaturkürzel für Skripte

Einige Aktionen bzw. Skripte können Sie in Form von Tastaturkürzeln (Shortcuts) ausführen. Diese werden im gleichnamigen Bereich innerhalb der globalen Benutzereinstellungen konfiguriert.

> ✻ Bitte beachten Sie, dass diese Tastaturkürzel nur dann bei externen Anwendungen funktionieren, wenn diese direkt aus Password Safe heraus geöffnet werden!

Tastaturkürzel	Aktion
STRG+ ALT + U	übergibt den Benutzernamen aus dem selektierten Datensatz per Skript an das aktive Fenster
STRG+ ALT + U	übergibt den Benutzernamen aus dem selektierten Datensatz per Skript an das aktive Fenster
STRG+ ALT + S	startet ein Skript, das 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

Allgemeine Tastaturkürzel

Tastaturkürzel	Aktion
STRG + Q	Schnellsuche fokusieren
STRG + Shift + K	Bildschirmtastatur öffnen
STRG + Shift + P	Passwortgenerator öffnen
STRG + A	Alle auswählen
STRG + Space	Steuerung aufheben
STRG + N	Neues Objekt erstellen
STRG + C	Kopieren
STRG + V	Einfügen
ENTF/DEL	Löschen

Leertaste	Schnellansicht aufrufen
Enter/Return	Öffnen von selektierten Objekten
F5	Refresh
STRG + F5	Alle Daten neu laden
STRG + W	Aktuellen Tab in LighClient schließen
ESC	Bearbeiten Modus verlassen/Änderungen verwerfen
STRG + S	Speichern
STRG + F	Suchfeld fokusieren

Tastaturkürzel beim Erstellen von Dokumenten

Tastaturkürzel	Aktion
STRG + DEL	Alle Dokumente aus der Liste entfernen
STRG + F	Suchfenster für die Dateiauswahl öffnen

Tastaturkürzel zum Formulare bearbeiten

Tastaturkürzel	Aktion
STRG + N	Neues Formularfeld hinzufügen

Tastaturkürzel zum Passwörter bearbeiten

Tastaturkürzel	Aktion
STRG + U	URL Formularfeld hinzufügen
STRG + M	Memo Formularfeld hinzufügen
STRG + O	Berichtsabfrage öffnen

Tastaturkürzel Berechtigen von Datensätzen

Tastaturkürzel	Aktion
Enter/Return	Suchen und Hinzufügen
ENTF/DEL	Rolle bzw. Benutzer entfernen

Tastaturkürzel in den Siegelvorlagen

Tastaturkürzel	Aktion
STRG + O	Siegelvorlage öffnen

Tastaturkürzel im Passwort-Modul

Tastaturkürzel	Aktion
F12	Passwort aufdecken

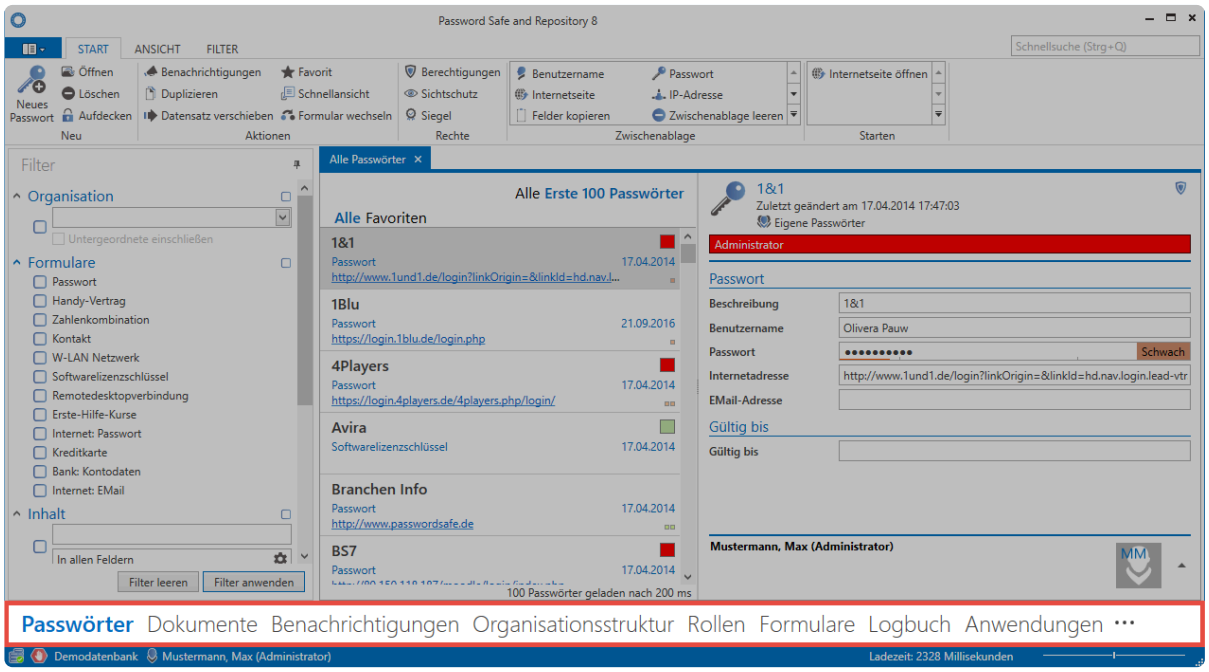
Tastaturkürzel im Anwendungs-Modul

Tastaturkürzel	Aktion
STRG + O	Anwendung im neuen Tab öffnen

Client Module

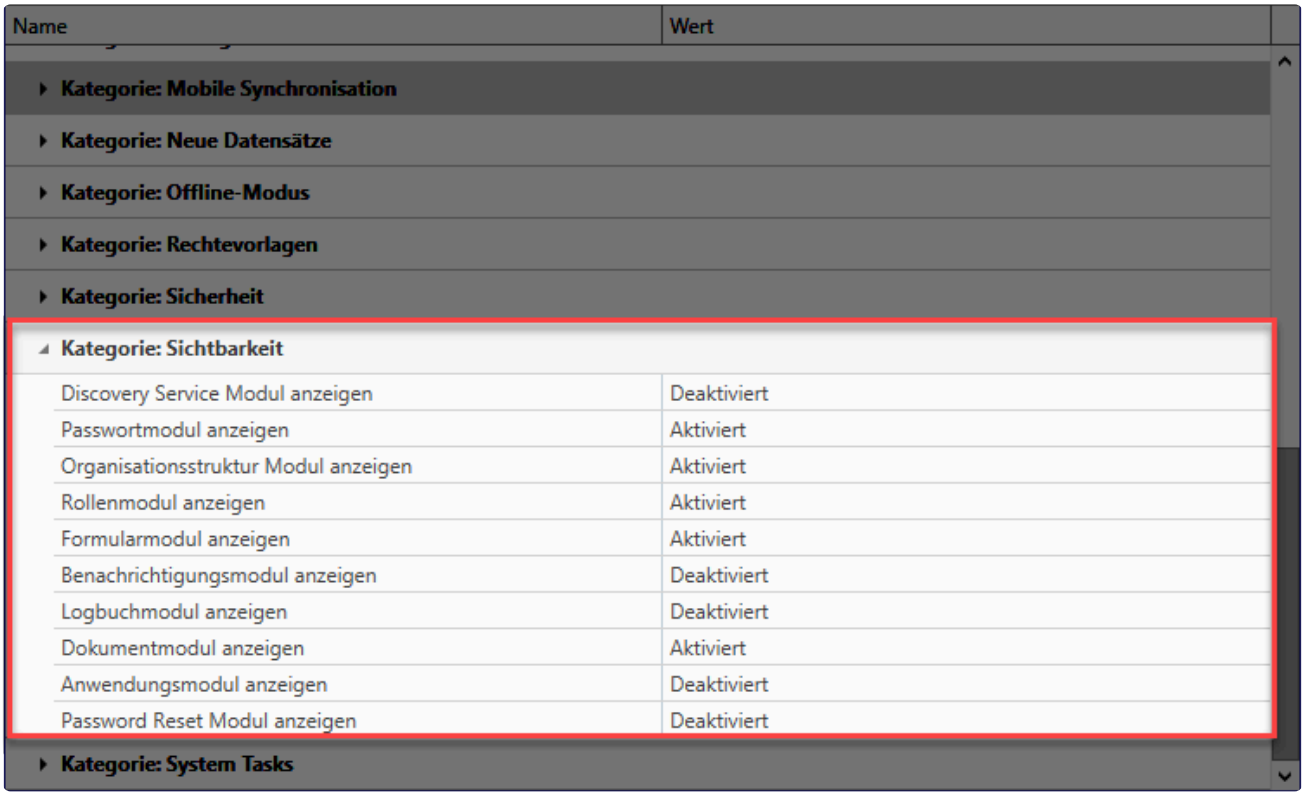
Was sind Module?

Password Safe verfolgt den Ansatz des modularen Aufbaus. Dabei ist jeder Funktionsbereich in sich geschlossen. Je nach Aufgabengebiet können einem Benutzer die entsprechenden Module zugewiesen werden. Nur diese sind dann sichtbar und können verwendet werden.



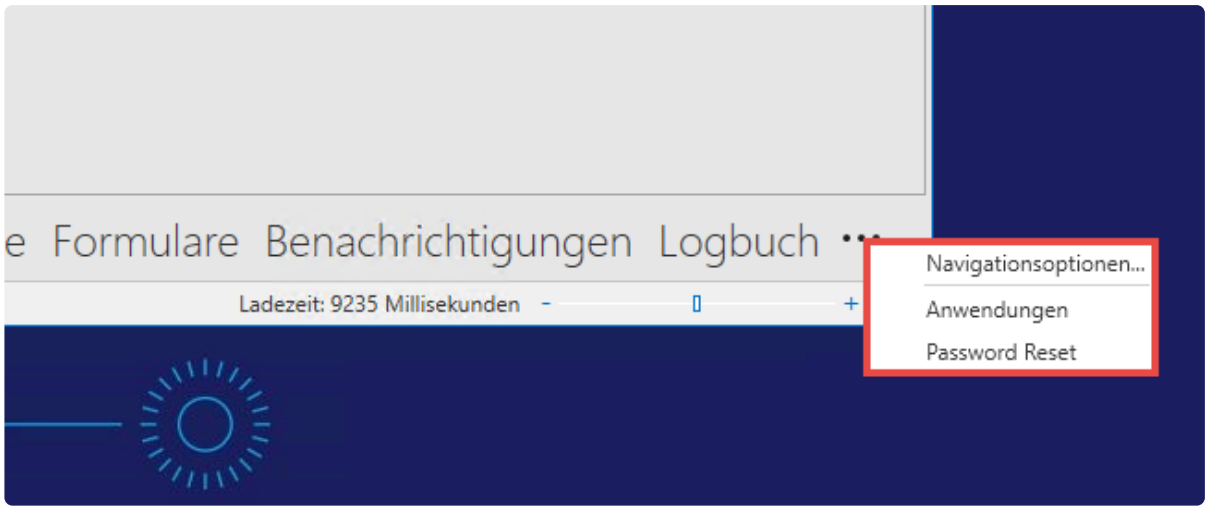
Sichtbarkeit von Modulen

Die Sichtbarkeit können Sie in den **Benutzerrechten** einstellen. Suchen Sie dazu die Kategorie **Sichtbarkeit** und aktivieren bzw. deaktivieren Sie die entsprechenden Module. Das ist sowohl für alle Benutzer (global), als auch einzelne Organisationseinheiten bzw. Benutzer möglich.

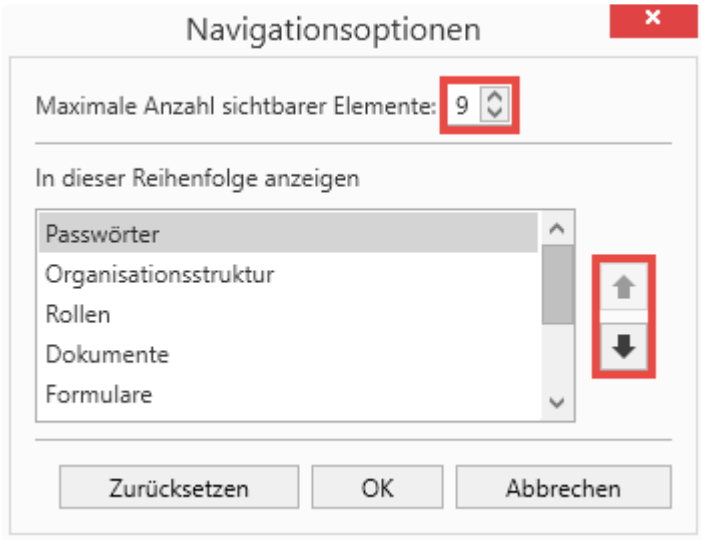


Sortierung der Module

Klicken Sie am rechten unteren Ende der im FullClient dargestellten Module auf die drei Punkte und dort auf “**Navigationsoptionen**”



Es öffnet sich ein kleines Fenster, in dem Sie die maximale Anzahl der sichtbaren Module sowie die Sortierung festgelegt werden kann. Markieren Sie dazu ein Modul und verschieben es mittels der Pfeiltasten nach oben oder unten.

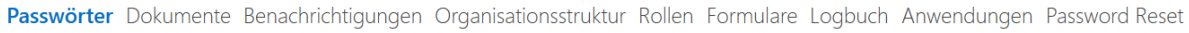


Sie können immer nur die für Sie freigegebenen Module sehen und sortieren.

Passwörter

Was sind Passwörter?

In Password Safe v8 stellt der Datensatz mit den darin enthaltenen Passwörtern das zentrale Datenobjekt dar. Über das Modul **Passwörter** erhalten Administratoren und Endbenutzer den zentralen Zugang zu den sensiblen und schützenswerten Daten. Frei definierbare Suchfilter im Zusammenspiel mit Tag-Markierungen auf Datensätzen ermöglichen zielführendes Arbeiten. Mithilfe diverser Ansätze kann die gewünschte Form der Berechtigung an Objekten angebracht werden. Die Konfiguration der Sichtbarkeit ist analog zu den anderen Modulen an zentraler Stelle erläutert.



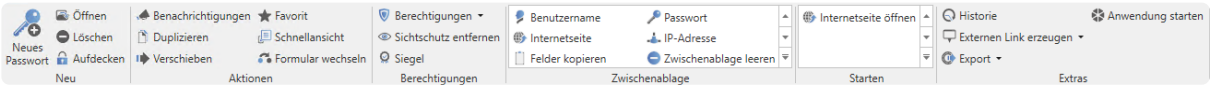
Voraussetzung

Sie benötigen folgendes recht, um neue Passwörtern anzulegen:

- **Kann neue Passwörter anlegen**

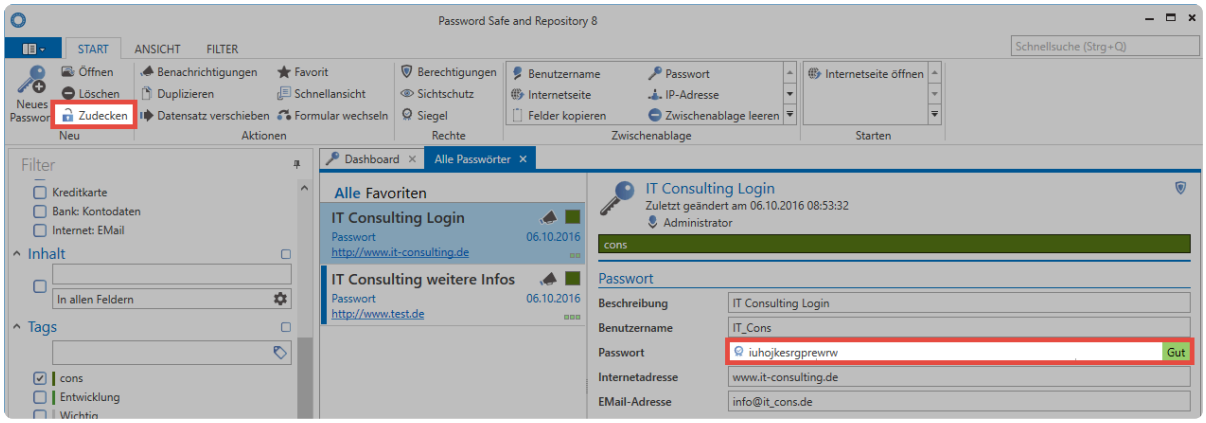
Modulspezifische Ribbonfunktionen

Die Ribbon bietet innerhalb des Moduls **Passwörter** eine Vielzahl an modulspezifischen Funktionen an. Allgemeine Informationen zum Thema Ribbon gibt es im hierfür vorgesehenen Kapitel. Im Folgenden wird auf die modulspezifischen Ribbonfunktionen eingegangen.



Neu

- **Neues Passwort:** Sowohl über dieses Icon in der Ribbon als auch über das Kontextmenü der rechten Maustaste sowie per Shortcut (STRG + N) können neue Datensätze angelegt werden. Im nächsten Schritt wählen Sie ein geeigneten Formular aus.
- **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. Sie verdecken das Passwort wieder über den Button **Zudecken**.



Aktionen

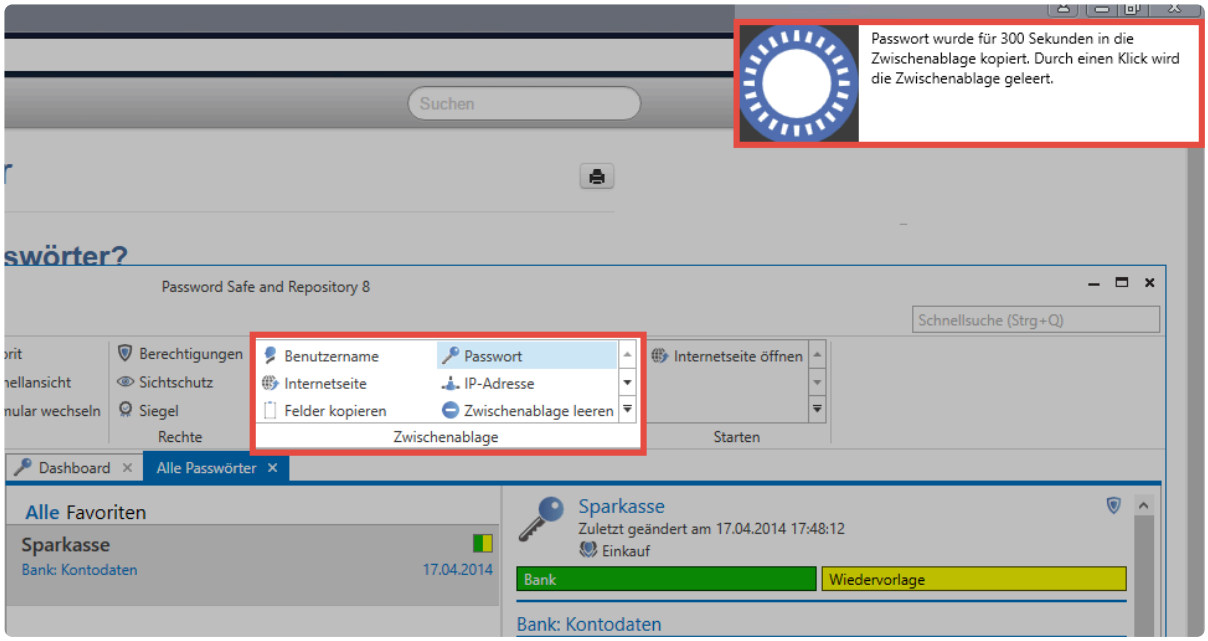
- **Benachrichtigungen**: Die Definition von Benachrichtigungen ermöglicht den stetigen Informationsfluss bei jedweder Form von Datensatz-Änderungen. Die Ausgabe der Benachrichtigungen erfolgt in dem hierfür vorgesehenen Modul.
- **Duplizieren**: Beim Duplizieren wird eine exakte Kopie des Datensatzes in einem neuen Tab erstellt. Hier haben Sie dann die Möglichkeit den Datensatz weiter zu bearbeiten.
- **Verschieben**: Verschiebt den in der Listenansicht markierten Datensatz in eine andere Organisationsstruktur. Weitere Informationen hierzu finden Sie in einem eignen Kapitel.
- **Favorit**: Der ausgewählte Datensatz wird als Favorit markiert. Wählen Sie oberhalb der Listenansicht jederzeit zwischen allen Datensätzen und Favoriten.
- **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 nehmen Sie direkt im sich öffnenden, modalen Fenster vor.

Berechtigungen

- **Berechtigungen**: Sowohl Passwortberechtigungen als auch Formularfeldberechtigungen setzen Sie über das sich öffnende Drop-Down Menü. 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 in 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”. Ein **Mausklick auf das gewünschte Formularfeld eines Datensatzes in der Ribbon** kopiert dieses in die Zwischenablage.



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

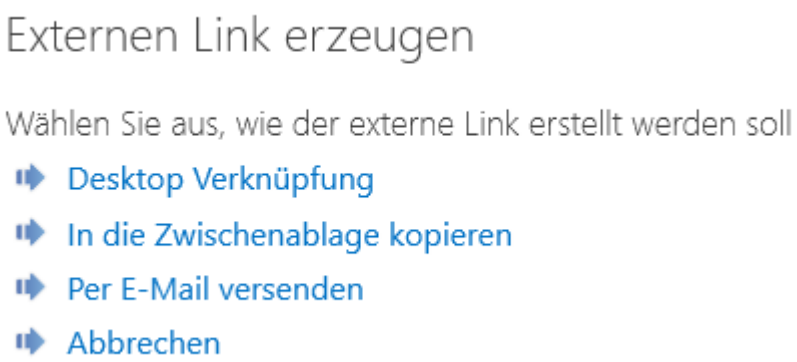
Starten

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

- **Internetseite öffnen**: Ist im Datensatz eine URL hinterlegt, öffnen Sie diese hiermit direkt.
- **Anwendungen**: Verknüpfen Sie Anwendungen direkt mit Datensätzen, öffnen Sie diese direkt über das “Starten-Menü”.

Extras

- **Externen Link erzeugen**: Ermöglicht, für den in der Listenansicht markierten Datensatz, einen externen Link zu erzeugen. Hierfür stehen mehrere Möglichkeiten zur Auswahl:



> ! Sind an einem Client mehrere Sessions geöffnet, wird ein externer Link immer in der ersten Session aufgerufen.

- **Historie**: Über das Icon öffnen Sie die Historie des in der Listenansicht ausgewählten Datensatzes in einem neuen Tab. Durch die lückenlose Erfassung historischer Versionsstände von Passwörtern können Sie mehrere Stände miteinander vergleichen. Weitere Informationen zu dieser Thematik sind in einem eigenen Kapitel erfasst.
- **Drucken**: Hierüber kann die Druckfunktion geöffnet werden.
- **Export**: Es ist möglich, sowohl alle selektierten Datensätze als auch durch den Filter definierte Daten in eine .csv Datei zu exportieren. Mehr…
- **Formular wechseln**: Hierüber weisen Sie den selektierten Passwörtern ein neues Formular zu.
- **Einstellungen**: Die Passworteinstellungen werden in einem gesonderten Kapitel beschrieben.

> ✻ Das Modul **Passwort** orientiert sich am gleichnamigen Modul, das sich im WebClient befindet. Beide Module unterscheiden sich im Umfang und Design. Hinsichtlich der Bedienung sind sie allerdings nahezu identisch.

Erstellen neuer Passwörter

Was versteht man unter dem Erstellen neuer Passwörter/ Datensätze?

Das Speichern eines Datensatzes/Passwortes hat zum Ziel, Informationen in der MSSQL-Datenbank abzulegen. Gestartet wird dieser Vorgang im **Client Modul Passwörter**. Entweder nutzen Sie 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, welches sich in einem neuen Fenster öffnet.

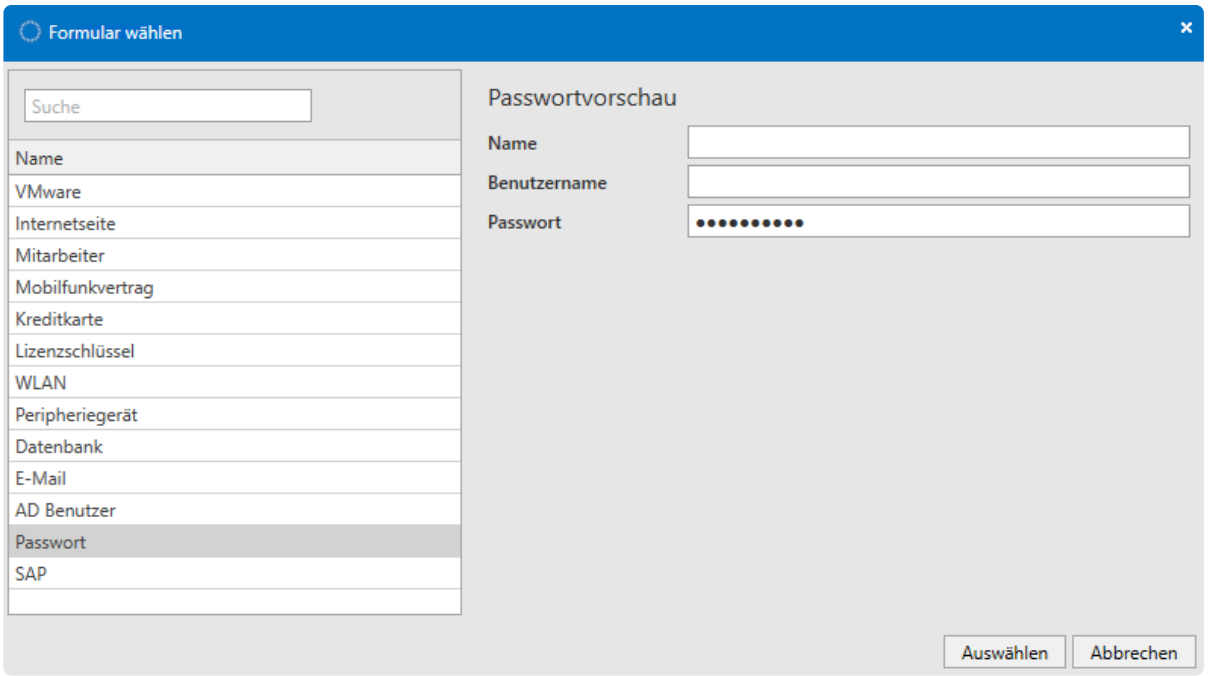
Voraussetzungen

Sie benötigen folgende 2 Benutzerrechte:

- **Kann neue Passwörter anlegen**
- **Passwortmodul anzeigen**

Formularauswahl

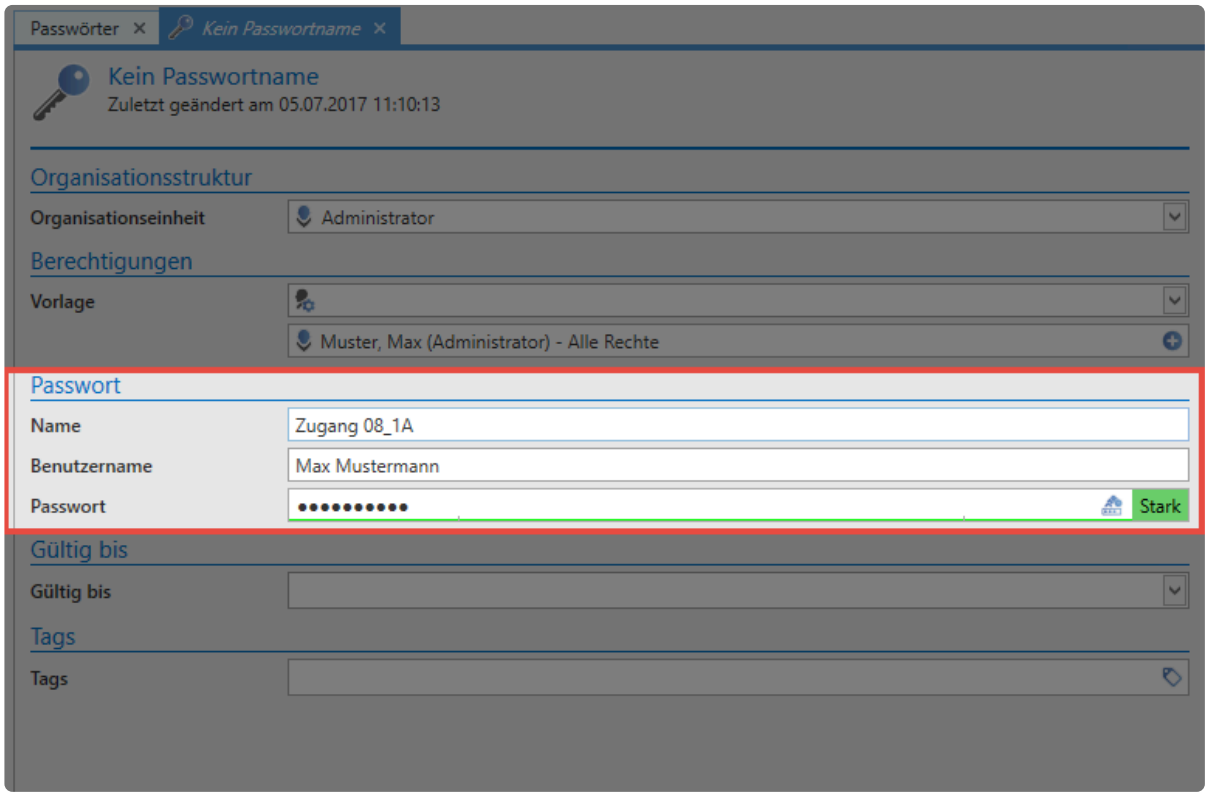
Bei der Erstellung eines neuen Datensatzes können Sie unter all denjenigen Formularen auswählen, auf welche der angemeldete Benutzer **berechtigt** ist. Um die Auswahl so einfach wie möglich zu gestalten, ist auf der rechten Seite eine Vorschau zu sehen.



Im vorliegenden 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).

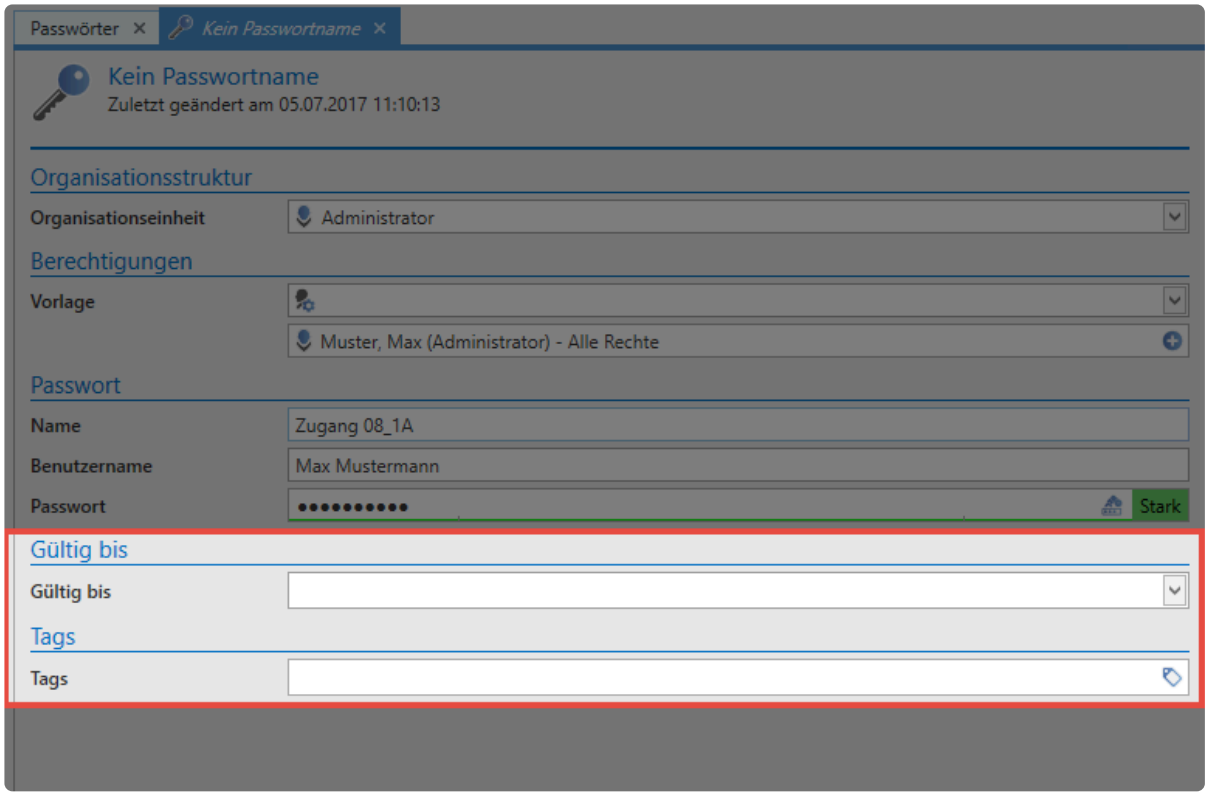
Eintragen der Daten

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



Gültigkeit und Tags

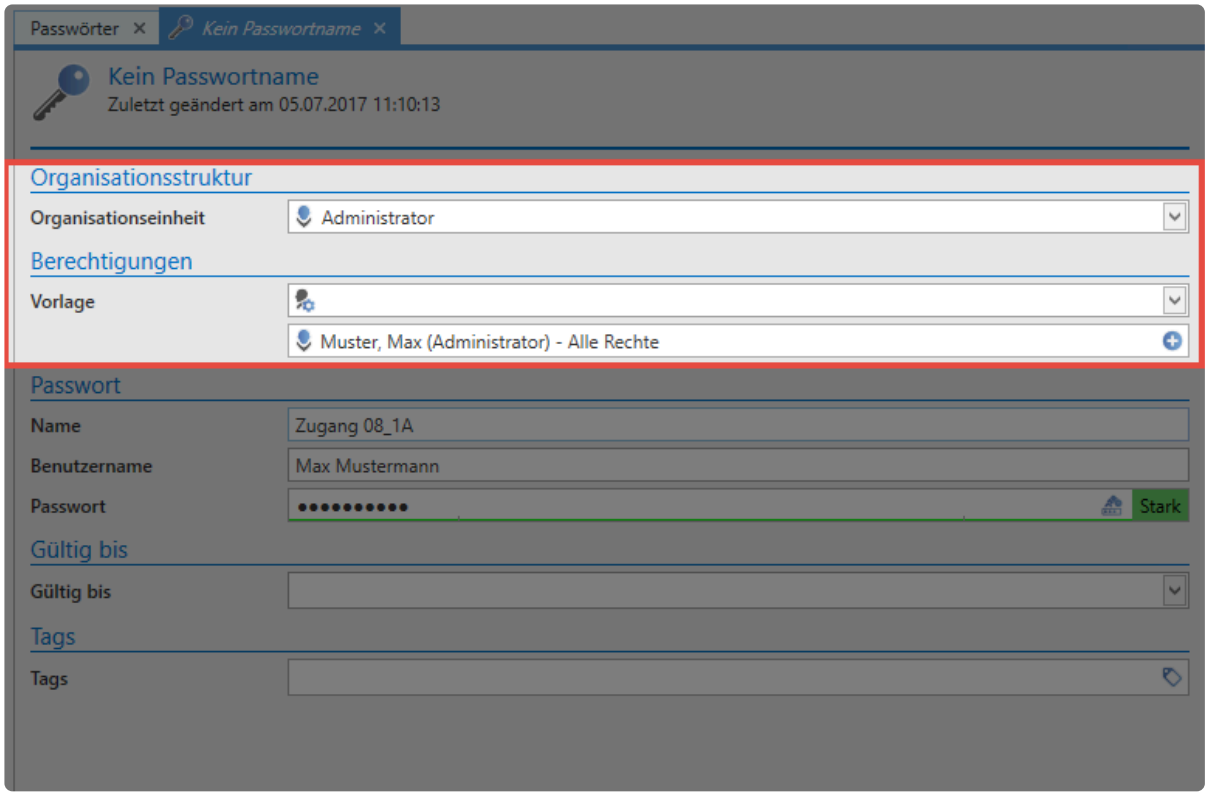
Unabhängig vom ausgewählten Formular definieren Sie für jeden Datensatz stets eine Gültigkeit und Tags. Beide Werte sind optional.



- Die **Gültigkeit** legt ein Enddatum fest, bis zu welchem 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 können Sie die Nutzbarkeit abgelaufener Passwörter aus Sicherheitsgründen **nicht** eingeschränken.
- **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…**

Festlegen 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 hierbei ist, dass das **manuelle Berechtigen erst nach dem Speichern** eines Datensatzes möglich ist. Die automatisch festzulegenden Berechtigungen definieren Sie vor dem Speichern. Wichtig ist in diesem Zusammenhang die Auswahl der Organisationsstruktur sowie die Berechtigungen eines Datensatzes.



- **Manuelles Berechtigen**: Wählen Sie beim manuellen Berechtigen die Organisationsstruktur aus, in die der Datensatz abgelegt werden soll. **Nach dem Speichern** können Sie **über den Reiter Berechtigungen in der Ribbon** manuell die Berechtigungen anpassen. Falls Sie einen persönlichen Datensatz erstellen, auf den kein weiterer Benutzer berechtigt sein soll, wählen Sie die eigene Organisationsstruktur aus.

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.

Über das Benutzerrecht **Kann andere Benutzer auf persönliche Passwörter berechtigen** können Sie definieren, dass persönliche Passwörter nicht für andere Benutzer freigegeben werden können.

- **Automatisches Berechtigen**: Das **automatische Berechtigen** von Datensätzen geschieht vor dem Speichern. Egal ob Sie vordefinierte Rechte oder Rechtevererbung nutzen: 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.

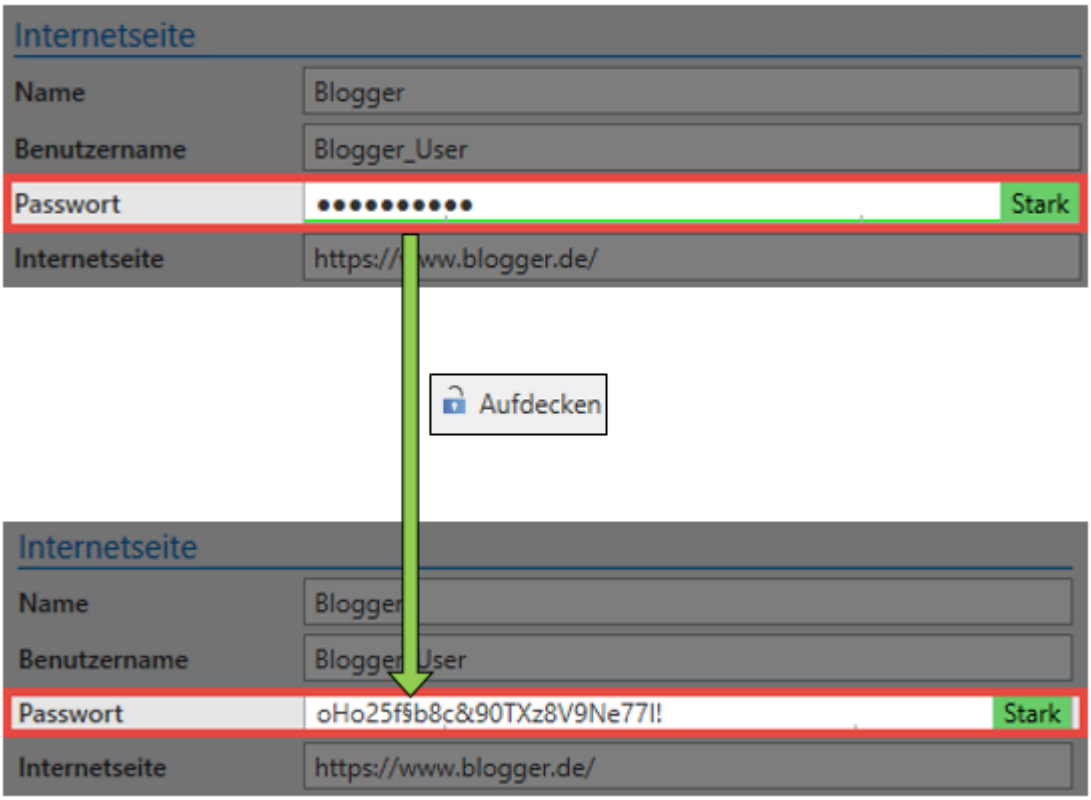
Aufdecken von Passwörtern

Worum geht es beim Aufdecken von Passwörtern?

Das Aufdecken von Passwörtern beschreibt den Mechanismus, bei dem ein Passwort im Client dem Benutzer sichtbar gemacht wird. Aus Performanzgründen wird lediglich das Passwort selbst (=secret) mit Hilfe der genutzten Verschlüsselungsalgorithmen im Client 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**. Nachfolgend wird die Funktionsweise detailliert beschrieben.

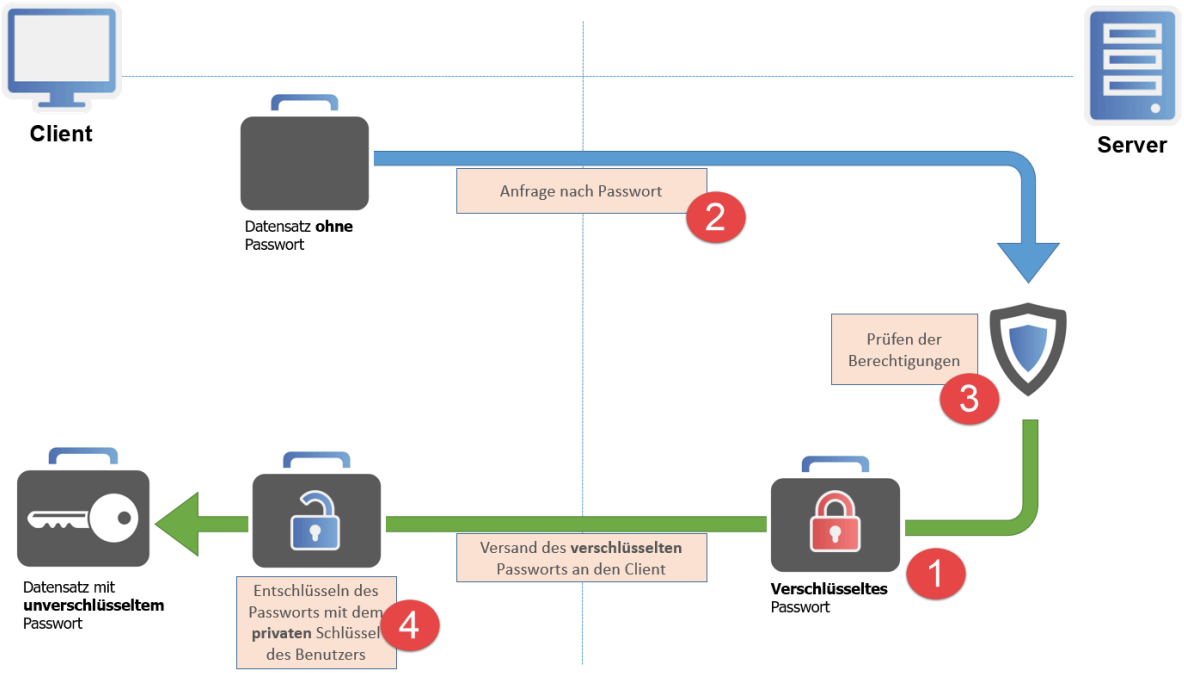
Fallbeispiel

Der Datensatz “Blogger” ist in der Datenbank gespeichert und vom angemeldeten Benutzer einsehbar. Der Benutzer ist somit zumindest lesend auf den Datensatz berechtigt. Gemäß Berechtigungskonzept hat der Benutzer somit auch Leserecht auf das Passwort selbst. Dies bedeutet, er kann über die Funktion “Aufdecken” das Passwort im Klartext sehen.



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 angezeigt werden muss. Der im Hintergrund ablaufende Prozess bis zum Anzeigen des Passwortes ist jedoch bei weitem komplexer.



1. Aufbewahrung des Passwortes am Server

Auch wenn Sie es vermuten…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** wird das Passwort **hybridverschlüsselt** in der MSSQL-Datenbank aufbewahrt. 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 eine Anfrage 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

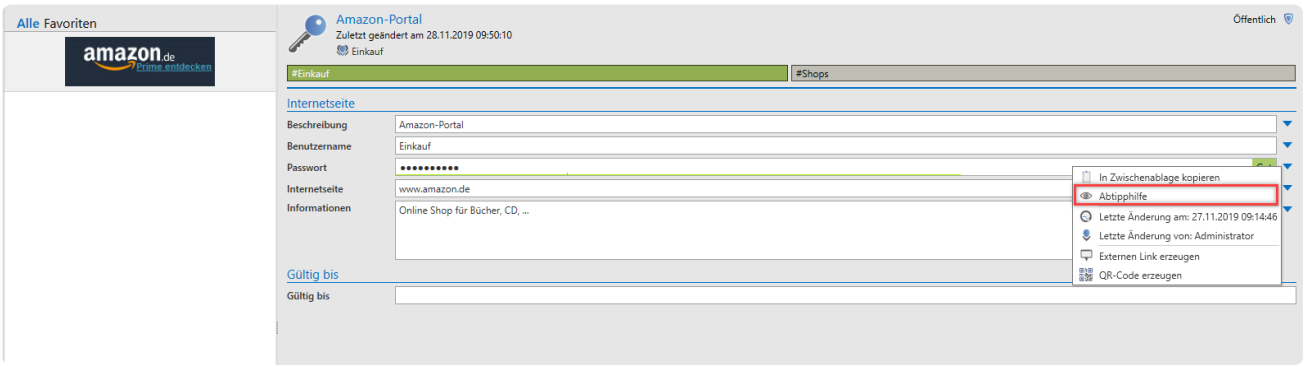
Ob eine wie unter 2. gestellte Anfrage eine Freigabe erhält, wird im Berechtigungskonzept definiert. Nach dem Eingang der Anfrage prüft der Server, ob der Benutzer die nötigen Rechte besitzt. Auch das Vorhandensein eventuell angebrachter Sicherheitsmechanismen, wie zum Beispiel eines Siegels oder dem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

4. Entschlüsseln des Passwortes am Client

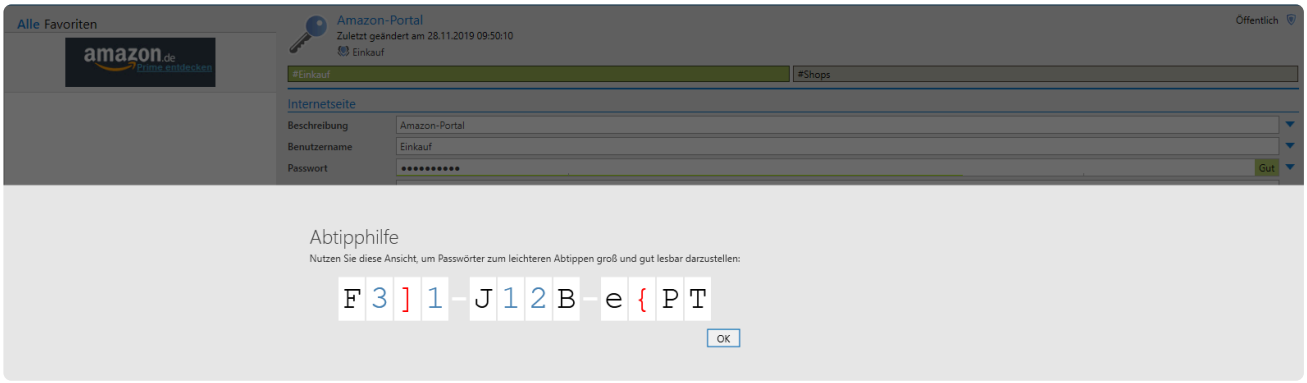
Der Benutzer besitzt nun das verschlüsselte Passwort, welches vom Server geliefert wurde. Der Benutzer selbst ist im Besitz des zur Entschlüsselung notwendigen **privaten Schlüssels** und kann nun den tatsächlichen Wert des Passwortes einsehen.

Abtipphilfe

Um ein Passwortfeld besser einsehen bzw. abtippen zu können, müssen Sie den Pfeil hinten am Passwortfeld aufklappen. Daraufhin können Sie die Abtipphilfe öffnen:



Dadurch werden Passwörter groß und gut lesbar dargestellt:



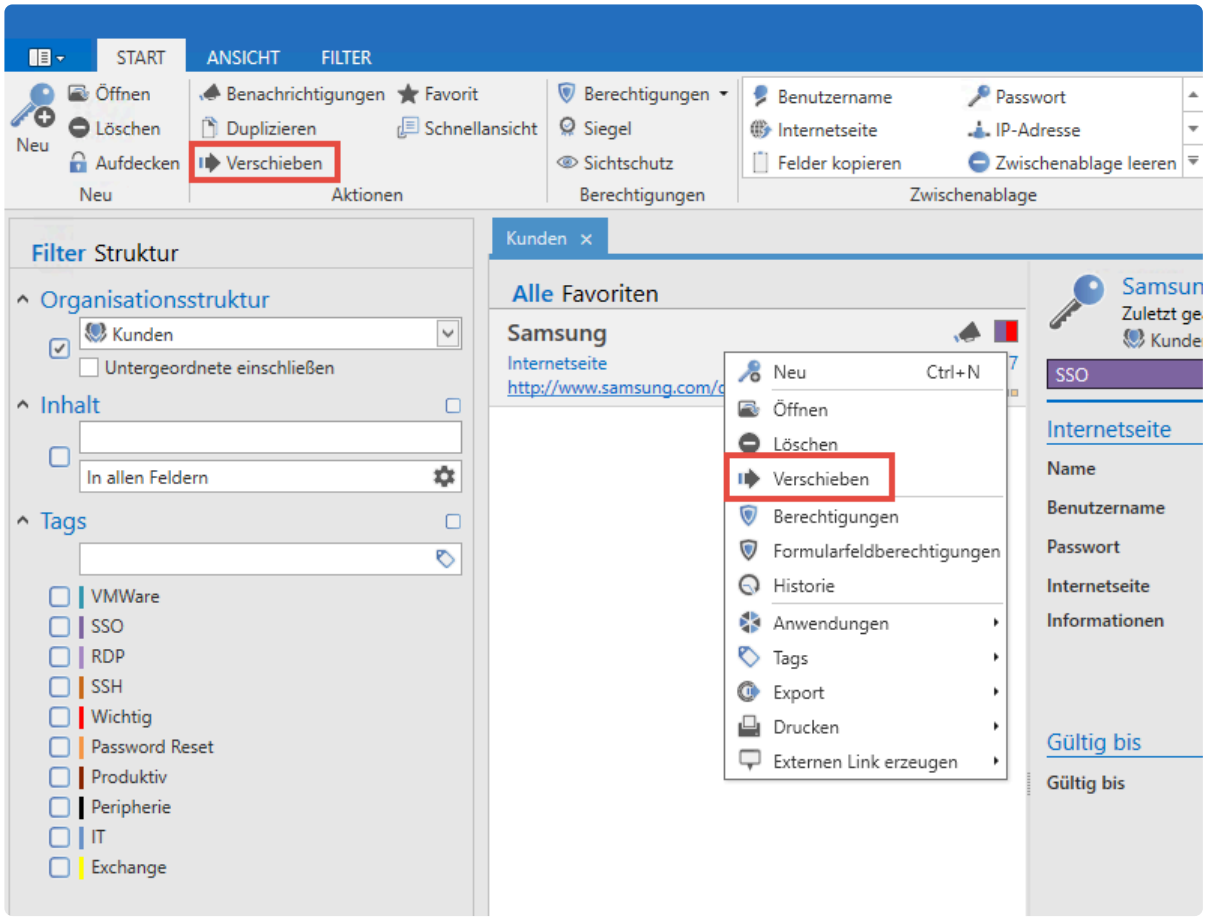
Verschieben von Passwörtern

Was passiert beim Verschieben des Datensatzes?

Datensätze können in Password Safe in andere Organisationsstrukturen verschoben werden. Hat eine die Organisationsstruktur, in die ein Datensatz verschoben wird, andere Berechtigungen, so werden diese auch auf den Datensatz angewendet. Das Verschieben ohne Änderungen der Berechtigungen hat hauptsächlich Auswirkungen auf die Filterung, bzw. die Suche nach Datensätzen.

Wie verschiebt man Datensätze?

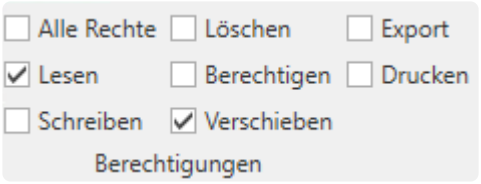
Das Verschieben von (markierten) Datensätzen erfolgt entweder in der Ribbon oder über das Kontextmenü der rechten Maustaste.



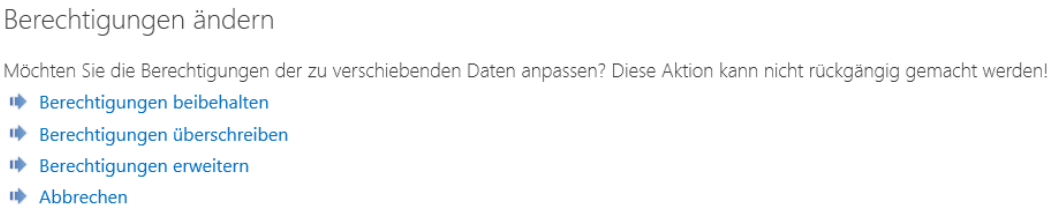
Es können auch mehrere Datensätze markiert und verschoben werden. Hier ändern sich ggf. auch die Berechtigungen für alle Datensätze.

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 Berechtigungen der Ziel-OU überschrieben
- **Berechtigungen erweitern**: Die vorhandenen Berechtigungen werden um die Berechtigungen der Ziel-OU erweitert

! Beim Überschreiben der Berechtigungen werden – technisch gesehen – zunächst alle Rechte auf dem Datensatz entfernt. Anschließend werden die Berechtigungen entsprechend der **Vererbung aus Organisationsstrukturen** bzw. der **Rechte Vorlage** auf den Datensatz angewandt. Bitte beachten Sie, dass man sich theoretisch die eigenen Rechte auf den Datensatz entziehen kann! Die Rechteänderung wird nur dann ausgeführt, wenn dadurch zumindest ein Benutzer das Recht zum Berechtigen erhält. Ansonsten bricht die Rechteänderung mit einer entsprechenden Meldung ab.

Formularfeldberechtigungen

Was sind Formularfeldberechtigungen?

Gemäß Berechtigungskonzept kann jedes Objekt – Datensätze, Formulare oder Benutzer – für sich berechtigt werden. Password Safe geht hierbei noch einen Schritt weiter. Jedes einzelne Formularfeld eines Datensatzes kann separat berechtigt werden. Es ist somit möglich, dass das Passwortfeld eines Datensatzes anders berechtigt ist als die anderen Formularfelder oder der Datensatz selbst.

Relevante Rechte

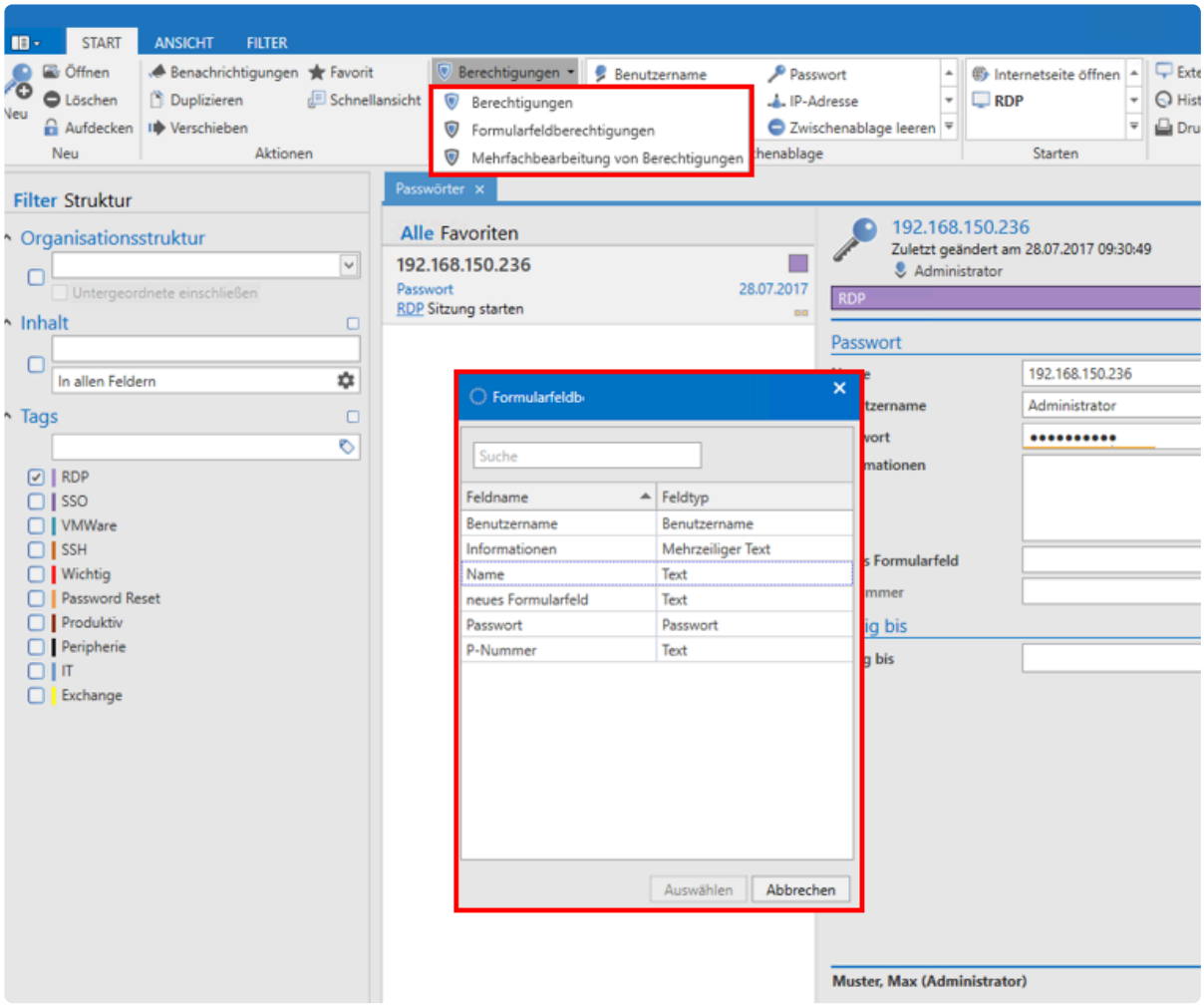
Folgende Optionen werden benötigt, um die Icons **“Vererben”** und **“Überschreiben”** sehen zu können.

Benutzerrecht

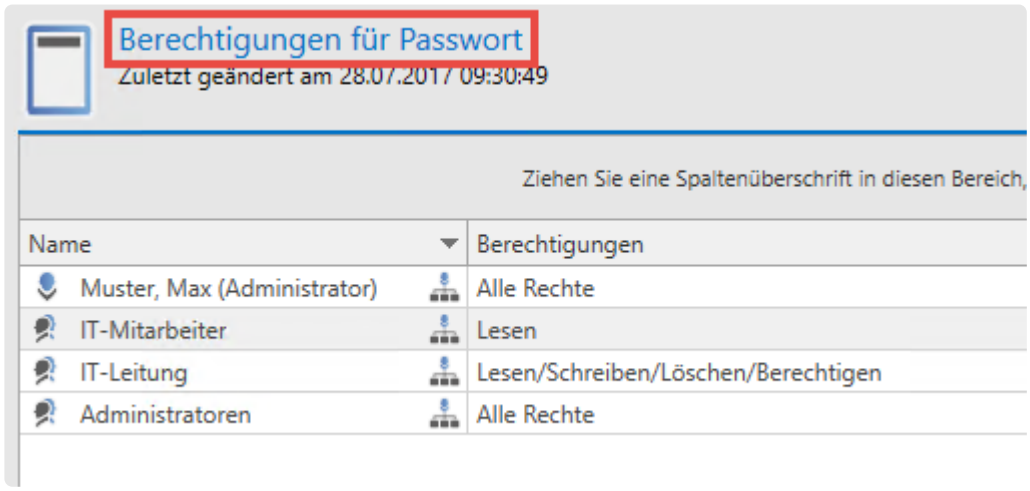
- Kann Berechtigungen überschreiben
- Kann Berechtigungen vererben

Konfiguration

Markieren Sie einen Datensatz und öffnen in der Ribbon im Bereich “Berechtigungen” über ein Dropdown Menü die Formularfeldberechtigungen.



In dem sich öffnenden Fenster können die Formularfelder bei Bedarf individuell berechtigt werden – hier beispielhaft am Passwortfeld gezeigt.

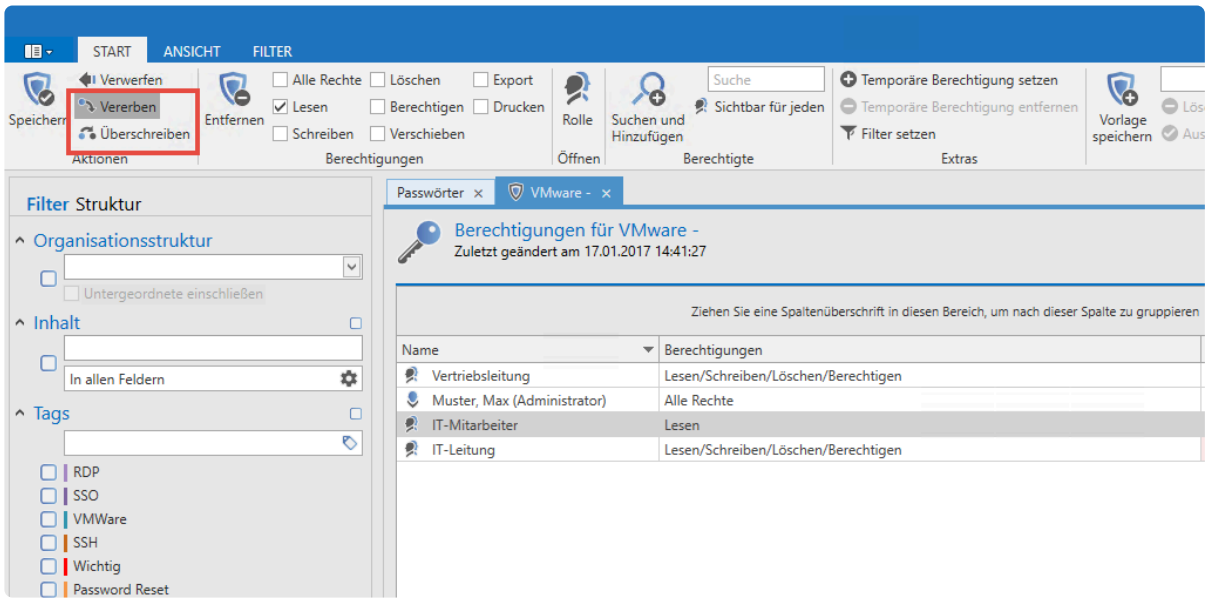


Die konfigurierten Berechtigungen betreffen ausschließlich das Passwortfeld. Die anderen Formularfelder bleiben unberührt.

Vererbung von Berechtigungen innerhalb von Datensätzen

Änderungen an Datensatzberechtigungen werden im Regelfall automatisch auf alle Formularfelder

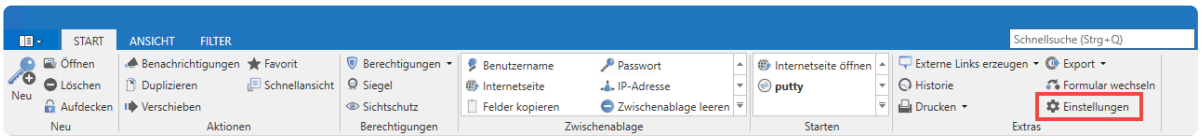
vererbt und überschreiben individuelle Berechtigungen einzelner Formularfelder. Öffnet man die Berechtigungen eines Datensatzes über die Ribbon, gelten die konfigurierten Rechte für alle Formularfelder. Um das zu verhindern, können die beiden Buttons “Vererben” und “Überschreiben” in der Ribbon an- und ausgeschaltet werden.



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

Passworteinstellungen

Klicken Sie in der Ribbon im Unterauswahlpunkt **Extras** auf **Einstellungen**. Es öffnet sich ein neuer Tab, in dem Sie einige Einstellungen zur Verwendung von Passwörtern vornehmen können.



Kategorie: Browser

- **Standardbrowser**: Hier können Sie für jeden Datensatz separat ein Standardbrowser festlegen. Dabei können Sie zwischen den lokal installierten Browsern wählen.

Kategorie: Passwort Reset

- **Zeitspanne, nach der Anmeldedaten von verbundenen Passwörtern überprüft werden**: Hier legen Sie pro Passwort den Intervall fest, in welchem der **Passwort Reset** das Passwort prüft.

Kategorie: SSO

- **Browser Addons: Exakte Domainprüfung**: Hier können Sie festlegen, ob die Domain für die Darstellung der Datensätze exakt geprüft werden soll oder nicht. Unter Browser-Erweiterungen finden Sie weitere Infos zu diesem Thema.

- **Browser Addons: Loginmasken automatisch befüllen**: Hier legen Sie fest, ob bei Anmeldungen über SSO die Loginmasken automatisch befüllt werden sollen. Ist ein Datensatz für eine Login Seite hinterlegt, werden die Anmeldeinformationen bei aktivierter Option direkt in die entsprechenden Felder eingetragen. Ohne diese Option wählen Sie den Datensatz über die Browser-Erweiterung aus und tragen ihn ein. Genauso verhält es sich bei mehreren hinterlegten Datensätzen für eine Login Seite. Hier müssen Sie über die Browser-Erweiterung den richtigen Datensatz auswählen.

- **Browser Addons: Loginmasken automatisch absenden**: Bei aktivierter Option wird nach dem Befüllen der Anmeldeinformationen der Anmeldebutton automatisch betätigt.

- **Browser Addons: Passwort anzeigen**: Ist diese Option aktiviert, wird das Passwort in der Browser-Erweiterung angezeigt.

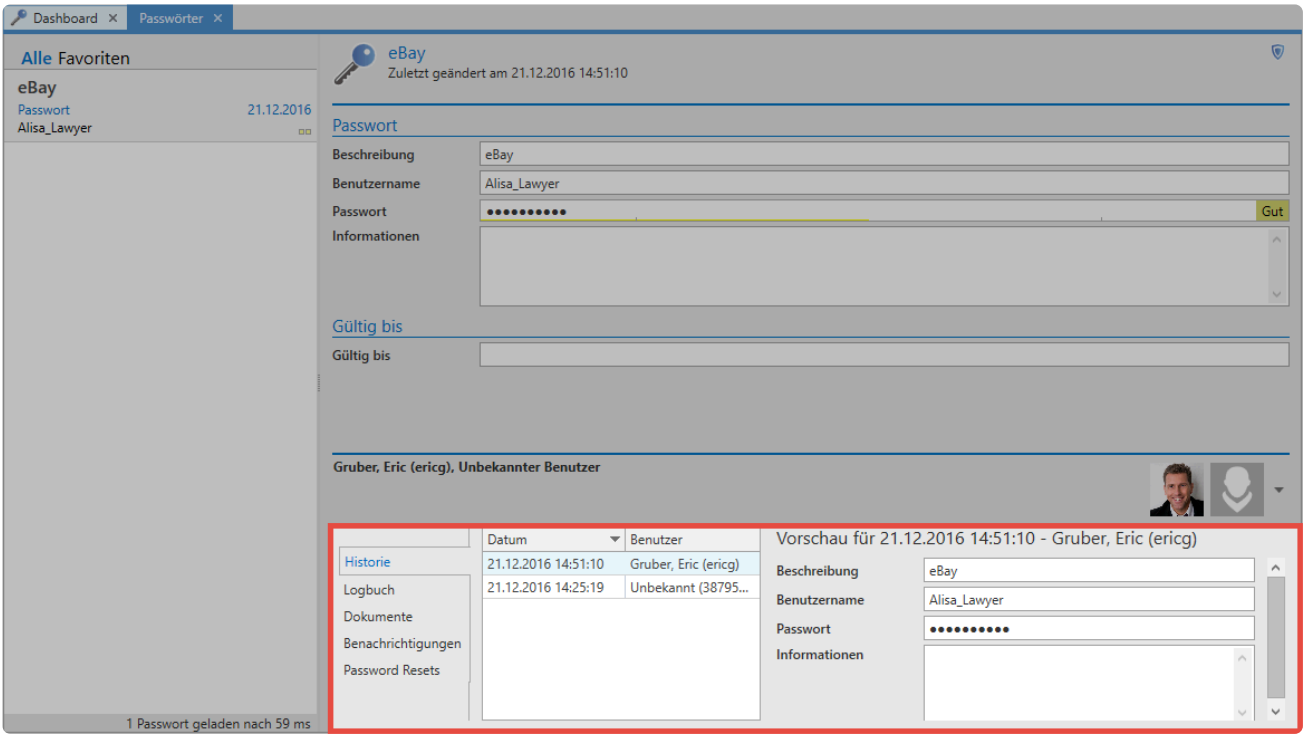
Historie

Was ist die Historie?

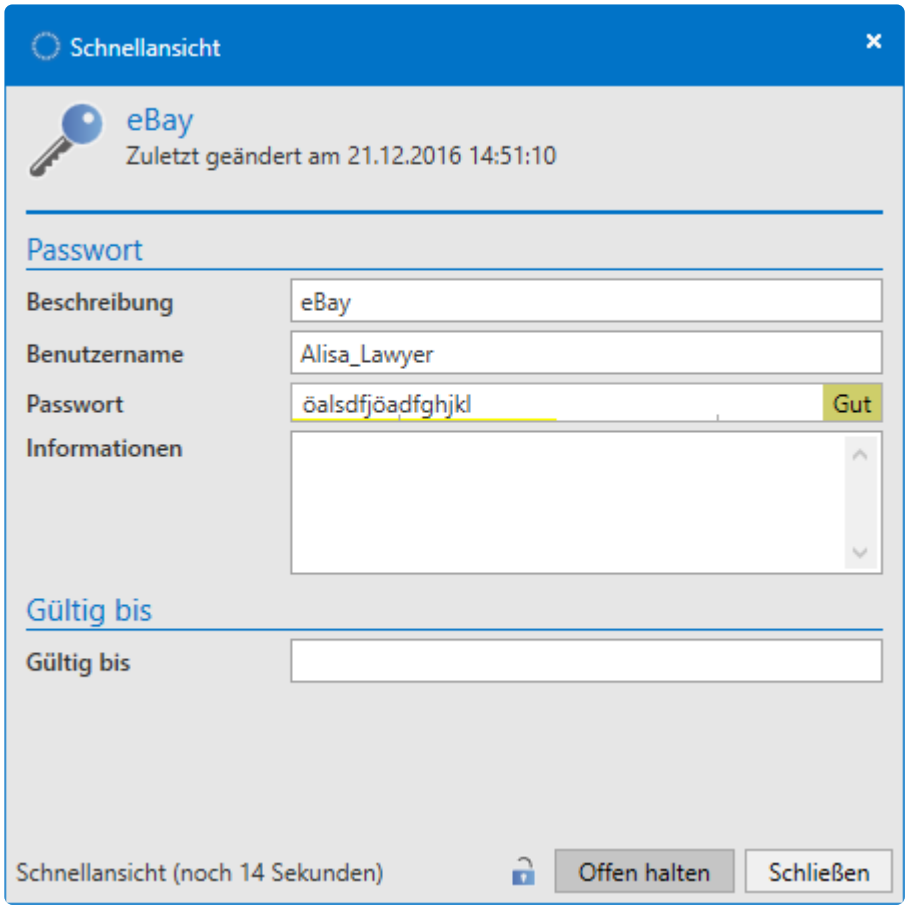
Die Historie ermöglicht die lückenlose Versionierung aller Formularfelder eines Datensatzes. Jede Veränderung von Datensätzen wird separat erfasst, gespeichert und kann auch wiederhergestellt werden. Darüber hinaus ergibt sich die Möglichkeit, stets historische Werte mit dem aktuellen Stand zu vergleichen. Die Historie ist ein unverzichtbarer Bestandteil in jedem Sicherheitskonzept.

Die Historie im Lesebereich

Über den optional aufrufbaren Footerbereich können Sie die Historie im Lesebereich einsehen. Alle historischen Einträge sind chronologisch sortiert aufgelistet.

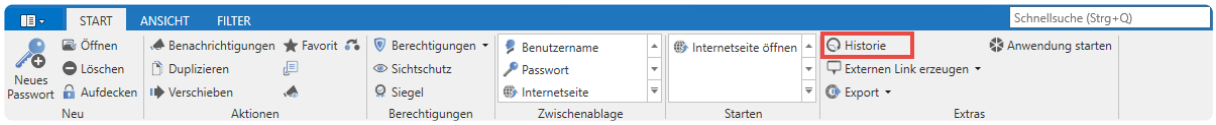


Links werden die verschiedenen Versionsstände untereinander angezeigt. Rechts daneben sind die Infos zur jeweiligen Version zu sehen. In der Ribbon unter **Historie** oder per Doppelklick lässt sich eine Schnellansicht einblenden.

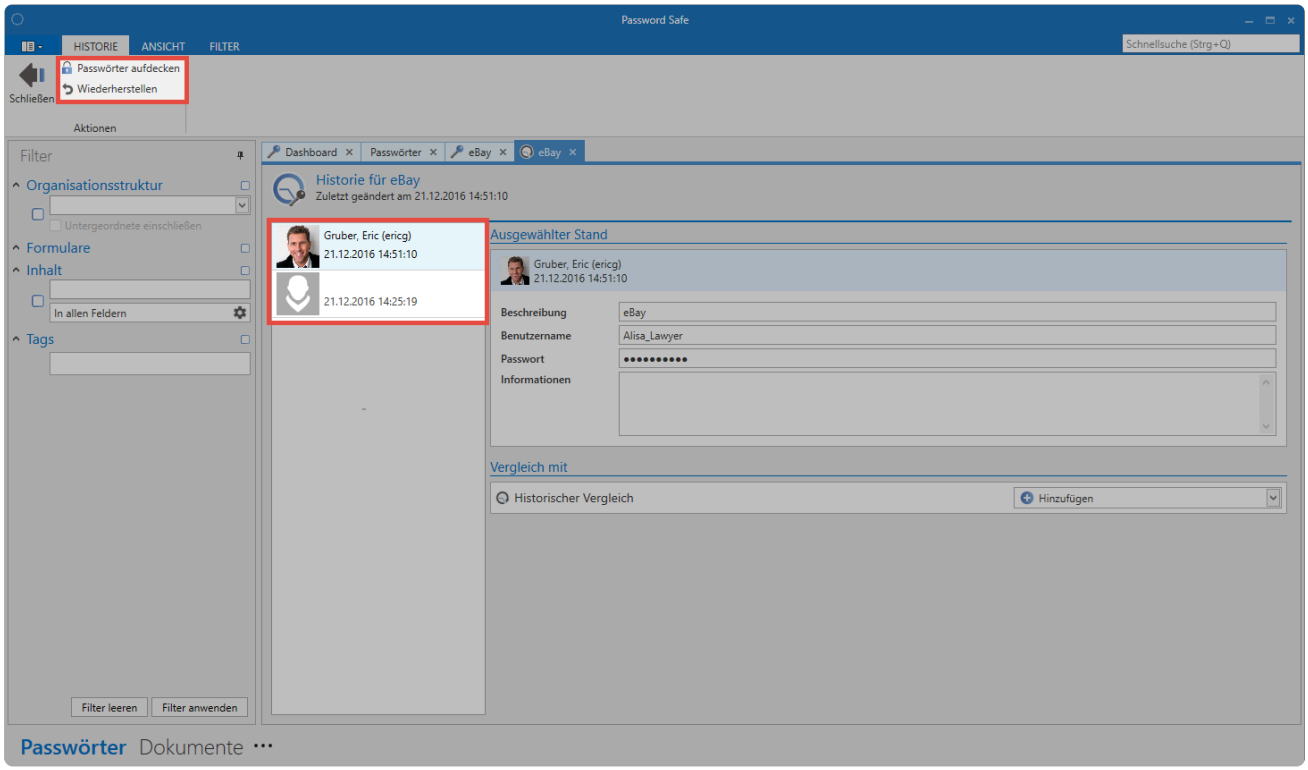


Detaillierte Historie in den Extras

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

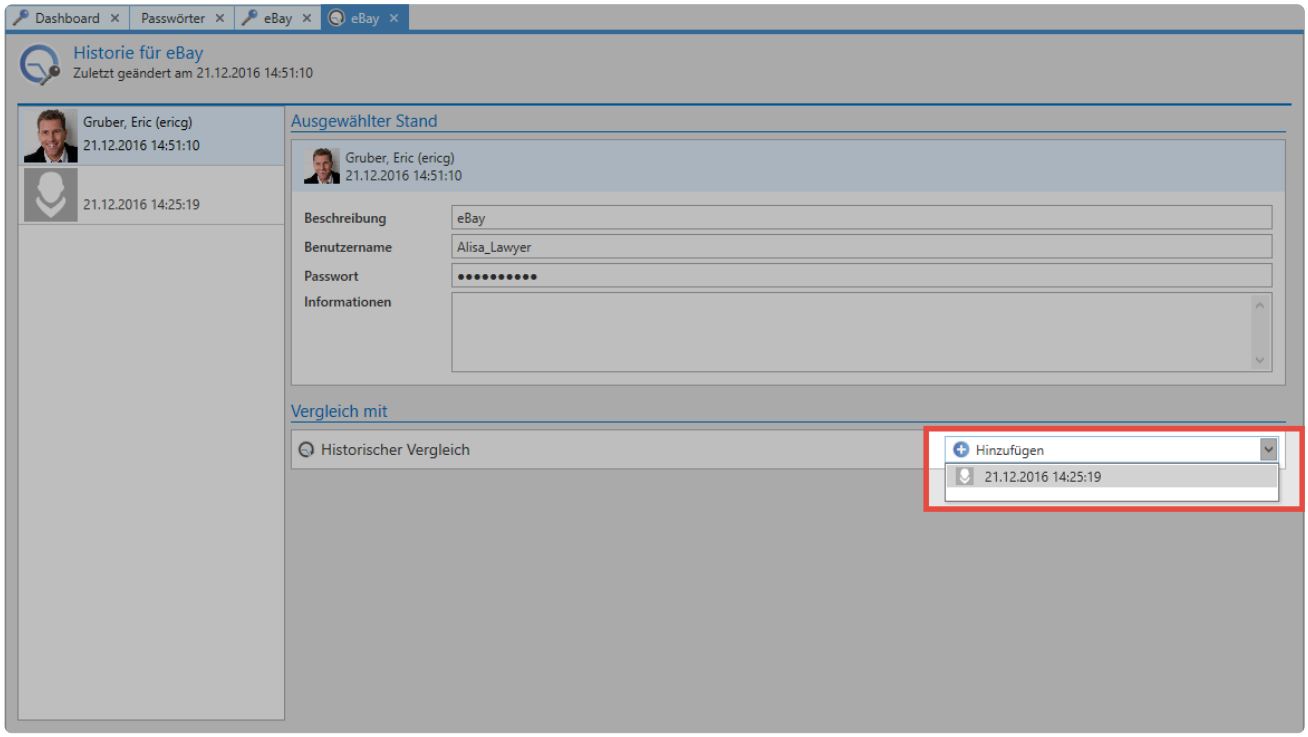


Die Historie des markierten Datensatzes öffnet sich in einem separaten Tab. In der Listenansicht sind nun alle verfügbaren Versionsstände mit Datum und Uhrzeit der letzten Änderung chronologisch sortiert aufgeführt.

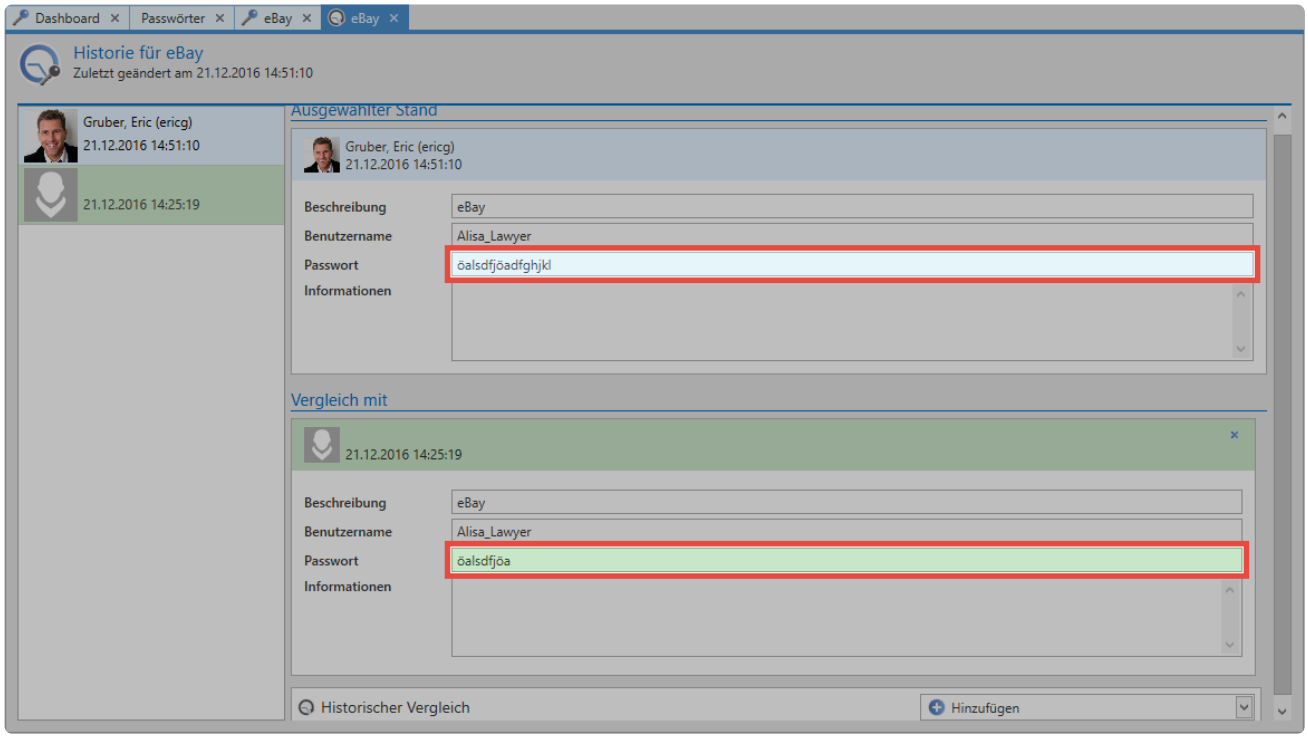


Vergleich von Versionsständen

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



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



Versionen wiederherstellen

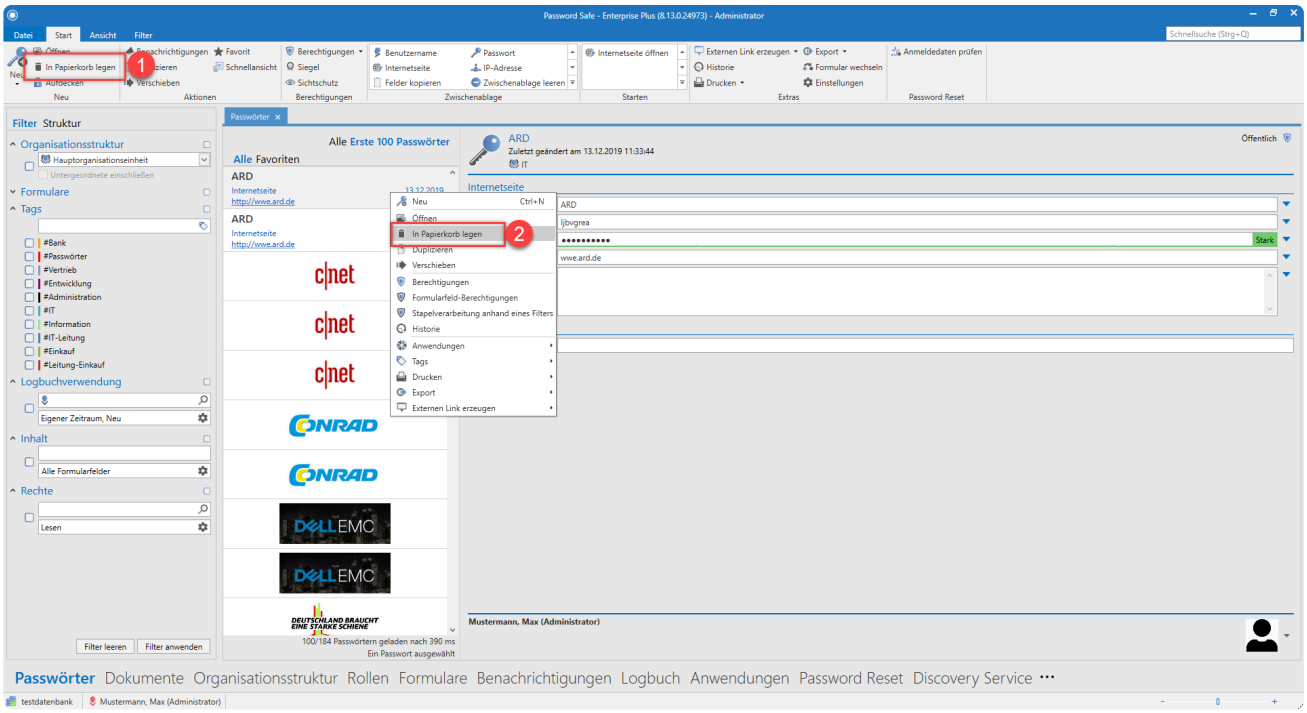
Über die Ribbon kann ein selektierter Stand wiederhergestellt werden. Der aktuelle Stand wird überschrieben und der Historie hinzugefügt

Papierkorb

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

Vorgehensweise beim Löschen von Passwörter

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



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

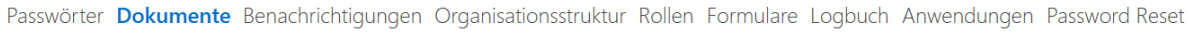
Verwalten des Papierkorbs

Die Verwaltung des Papierkorbs finden Sie hier

Dokumente

Was sind Dokumente?

Sicherheitskritische Daten müssen nicht zwingend in Form von Passwörtern vorliegen. Durch die Möglichkeit, Dokumente gemäß der Berechtigungen mit anderen zu teilen, erhält man stets den aktuellen Stand eines Dokuments und vermeidet Redundanzen. Zudem haben Sie die Möglichkeit sämtliche, in der Vergangenheit gespeicherten Versionen eines Dokumentsauf den historischen Wert zurückzusetzen. Die Konfiguration der **Sichtbarkeit** ist analog zu den anderen Modulen an zentraler Stelle erläutert..



Relevante Rechte

Um neue Dokumente anlegen zu können, benötigt man folgende Option.

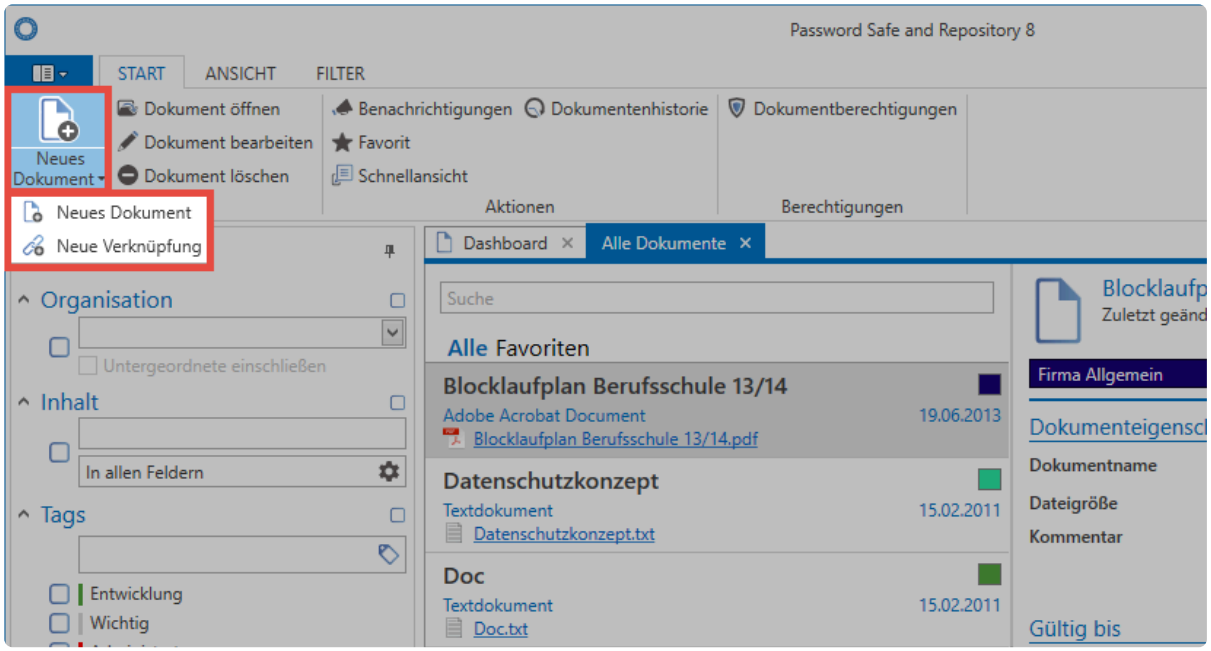
Benutzerrecht

- Kann neue Dokumente anlegen

Hinzufügen von Dokumenten

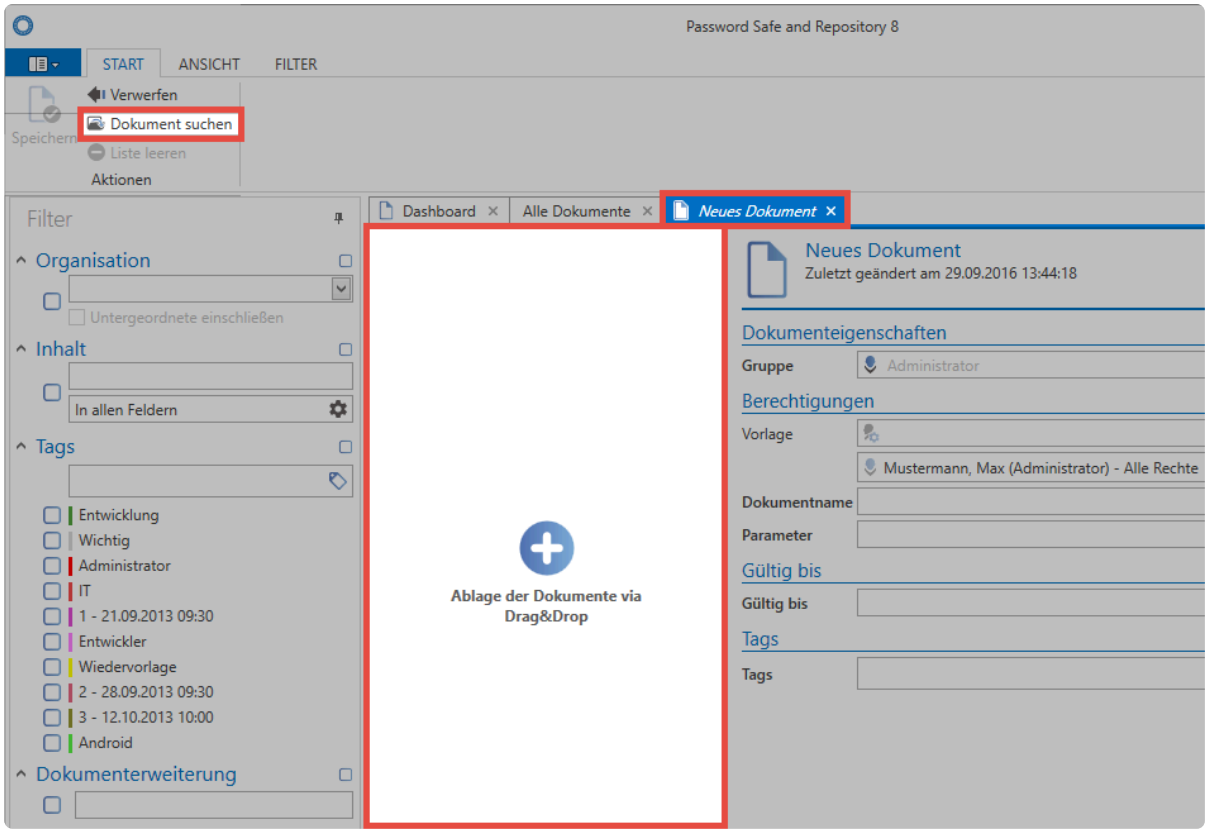
Es gibt zwei Arten, Dokumente und Dateien in Password Safe zu verwalten:

1. **Erstellen einer Verknüpfung:** Hierbei wird lediglich auf eine Datei verwiesen, die 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 berechtigten 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, mehrere Dokumente in einem Schritt zu importieren.



Versionsverwaltung

Sämtliche Versionen eines Dokuments 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 Dokuments zur Verfügung. Diese ist analog zur Historie von Passwörtern anwendbar. Mit der Versionsverwaltung lassen sich beliebige historische Versionen eines Dokuments wiederherstellen.

> ✻ Die Dateigröße eines **verknüpften Dokuments** kann nur dann aktualisiert werden, wenn das Dokument aus Password Safe heraus geöffnet wird.

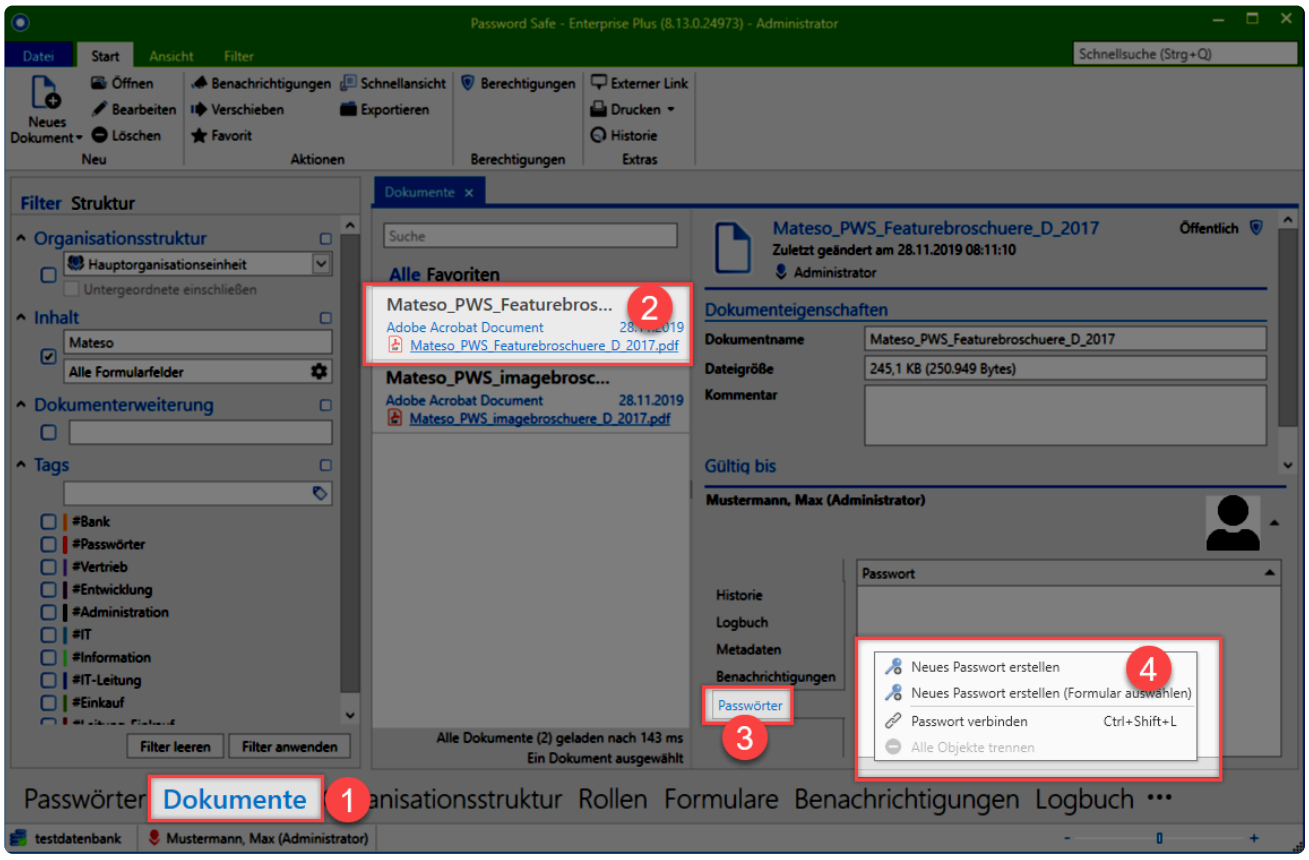
> ✻ Falls gewünscht kann die Dokumenthistorie automatisch bereinigt werden. Diese Option wird am **AdminClient** konfiguriert. Weitere Informationen finden Sie im Kapitel **Verwaltung von Datenbanken**.

Dokumente mit Passwort verknüpfen

Für die Verknüpfung eines Dokuments mit einem Passwort haben Sie 2 Möglichkeiten.

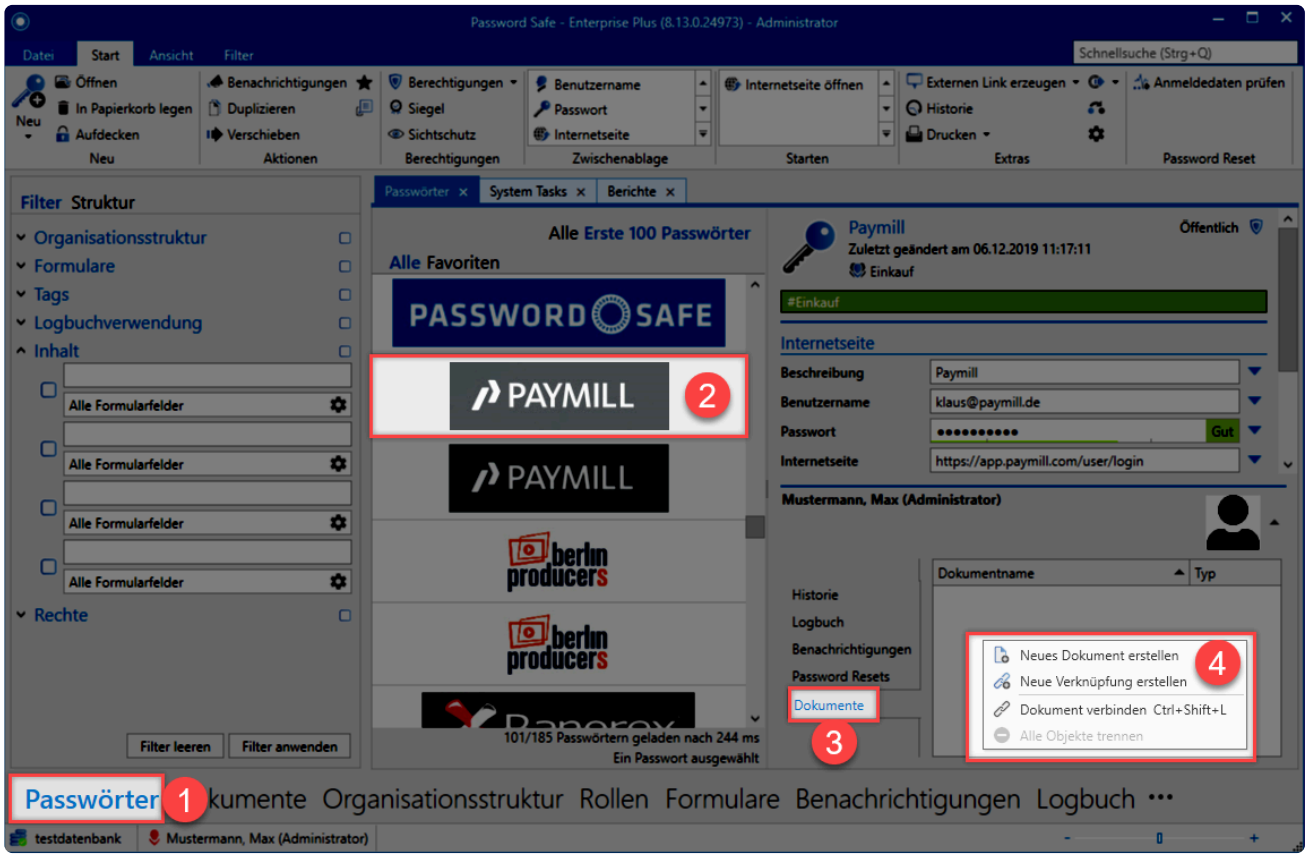
1. Dokument über das Dokumente-Modul verknüpfen

Öffnen Sie dafür im entsprechenden Dokument den Fußbereich. Im Reiter Passwörter können Sie mit Rechtsklick dem entsprechenden Dokument ein Passwort zuordnen.



2. Dokument über das Passwort-Modul verknüpfen

Öffnen Sie dafür im entsprechende Passwort den Fußbereich. Im Reiter Dokumente können Sie mit Rechtsklick dem Passwort ein Dokument zuordnen.



Benachrichtigungen

Was sind Benachrichtigungen?

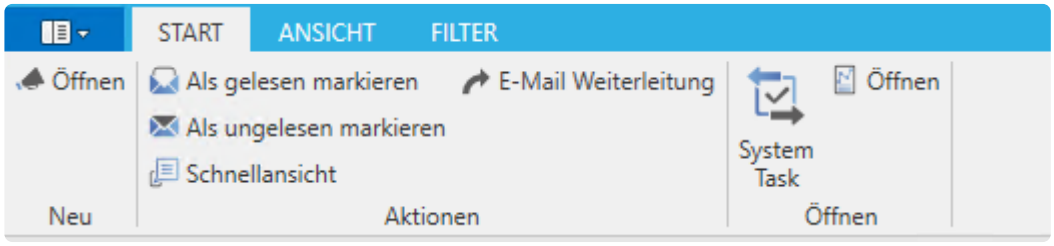
In nahezu allen Modulen können Benutzer individuell konfigurieren, wann Sie Benachrichtigungen über Ereignisse, die Sie für wichtig erachten, erhalten wollen. Jeder Benutzer kann definieren, welche Passwörter, welche Auslöser sowie Änderungen für Ihn wichtig sind. Alle konfigurierten Meldungen werden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

Passwörter Dokumente **Benachrichtigungen** Organisationsstruktur Rollen Formulare Logbuch Anwendungen Password Reset

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

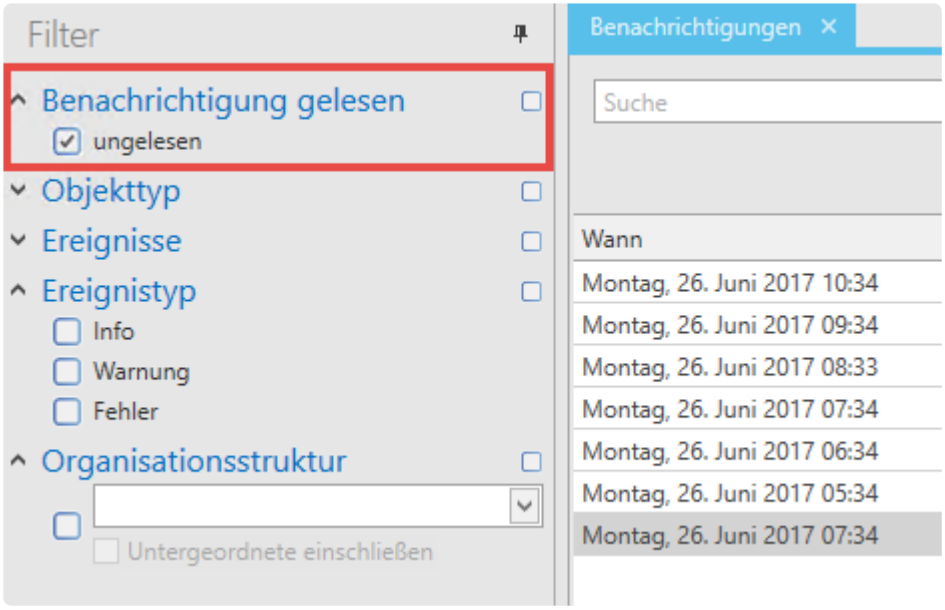
Modulspezifische Ribbonfunktionen

Auch in den Benachrichtigungen existieren einige Ribbon-Funktionen, die ausschließlich in diesem Modul zur Verfügung stehen. Besonders das **Weiterleiten von wichtigen Mitteilungen an Email-Adressen** ermöglicht Kontrolle und Transparenz.



Benachrichtigungen als gelesen markieren

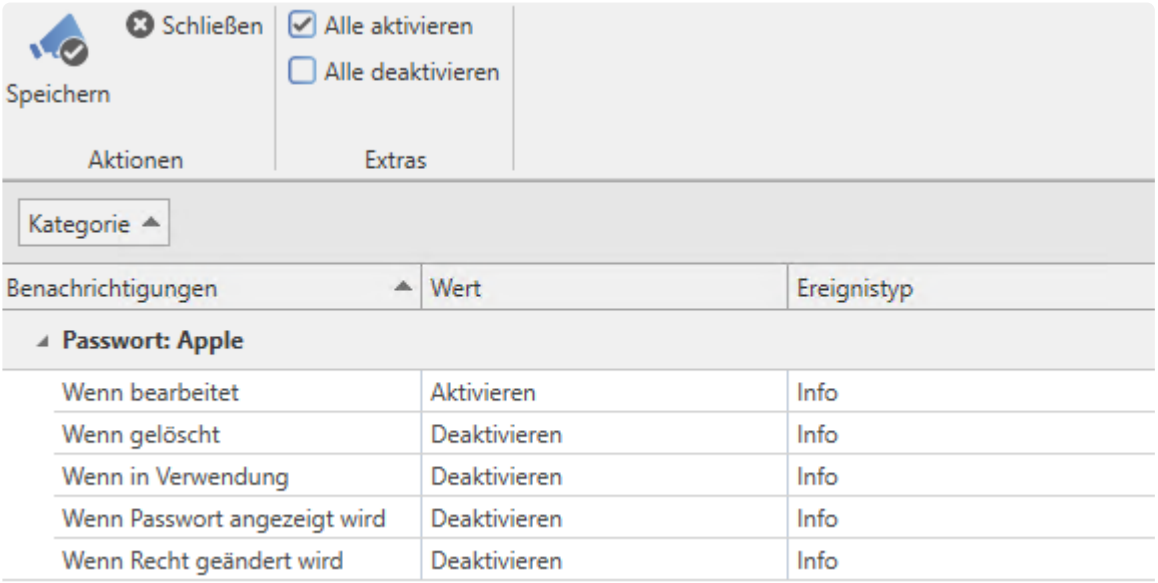
Über die beiden Buttons in der Ribbon ist es möglich, Benachrichtigungen als gelesen/ungelesen zu markieren. Besonders das in diesem Zusammenhang stehende Filterkriterium (s. nachfolgender Screenshot) ermöglicht das rasche Sortieren nach sowohl aktuellen als auch historischen Benachrichtigungen.



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.

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:

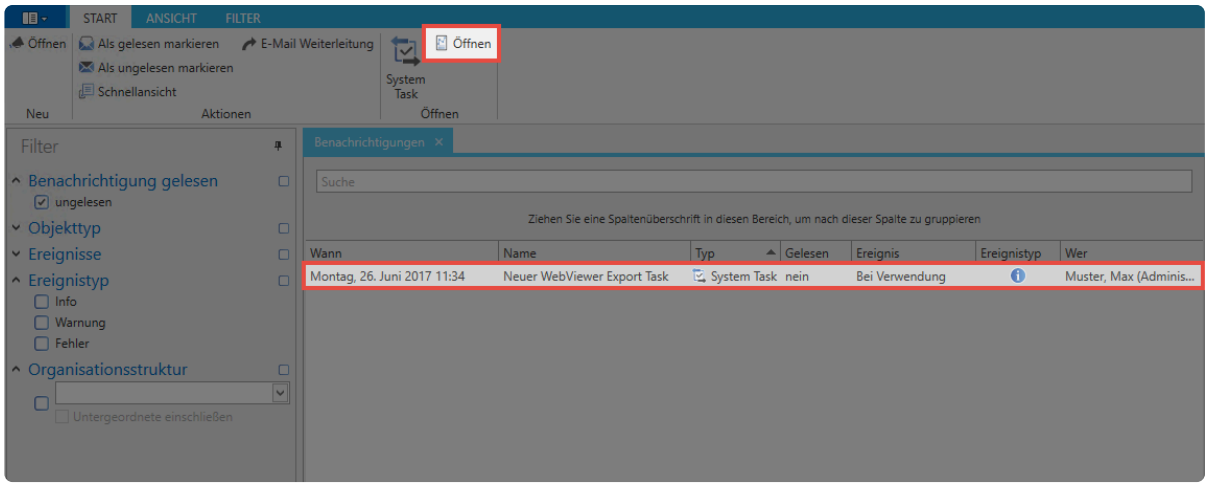


- **Benachrichtigung**: Definition des Auslösers
- **Wert**: Bestimmt, ob für den zuvor definierten Auslöser eine Benachrichtigung erzeugt wird. Im vorliegenden Datensatz “Apple” erfolgt diese nur, wenn der Datensatz bearbeitet wird.
- **Ereignistyp**: Bei erzeugten Benachrichtigungen kann zwischen “Info”,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

Weitere Auslöser von Benachrichtigungen

Zusätzlich zu den manuell konfigurierbaren Benachrichtigungen existieren im Password Safe weitere Auslöser für Benachrichtigungen.

- **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.



Automatisches Löschen alter Benachrichtigungen

Falls Sie wünschen, können Benachrichtigungen automatisch bereinigt werden. Diese Option wird am **AdminClient** konfiguriert. Weitere Informationen finden Sie im Kapitel **Verwaltung von Datenbanken**.

Organisationsstruktur

Was ist eine Organisationsstruktur?

In Anlehnung an bereits vorhandene Organigramme eines Unternehmens oder Abteilungen ist eine Organisationsstruktur die Abbildung eben dieser hierarchischen Strukturen in Password Safe. Natürlich ist es auch möglich, andere Kriterien – wie z.B. die ausgeübte Funktion/Tätigkeit – als Grundlage für die Erstellung von Hierarchien heranzuziehen. Es bleibt dabei Ihnen überlassen, welche Struktur für den Einsatzzweck am sinnvollsten ist. Der Zugriff auf Passwörter oder Dokumenten erfolgt entsprechend den jeweiligen Berechtigungen in den einzelnen Hierarchie-Ebenen. Die Konfiguration der **Sichtbarkeit** des Moduls wird analog zu den anderen Modulen an **zentraler Stelle erläutert.**

Passwörter Dokumente Benachrichtigungen **Organisationsstruktur** Rollen Formulare Logbuch Anwendungen Password Reset

Relevante Rechte

Sie benötigen folgende Option zum Anlegen neuer Organisationsstrukturen:

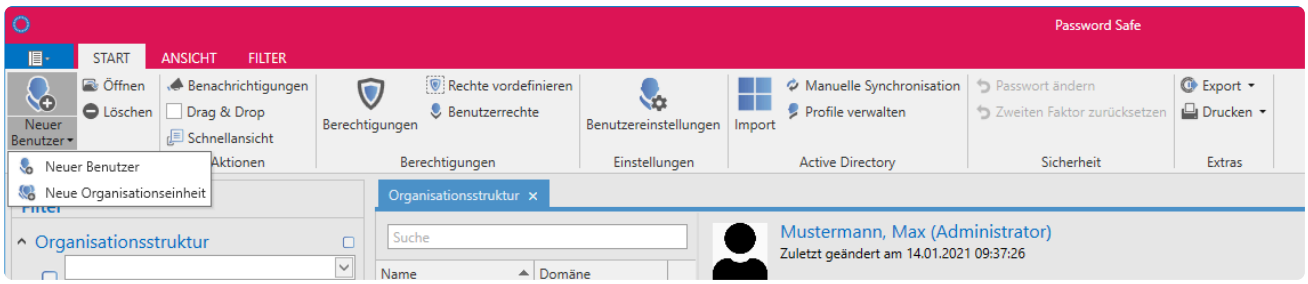
Benutzerrechte

- Kann neue Organisationseinheiten anlegen
- Kann neue Benutzer anlegen
- Organisationsstruktur Modul anzeigen

> Mit der Benutzereinstellung **Standard-Organisationseinheit** werden alle neu erstellten Datensätze dieser Organisationseinheit zugewiesen.

Modulspezifische Ribbonfunktionen

Die Bedienung der Ribbon unterscheidet sich in ein paar Punkten von der Handhabung in anderen Modulen. Diese werden hier erklärt. Die restlichen Aktionen sind im Modul Passwörter bereits erläutert.



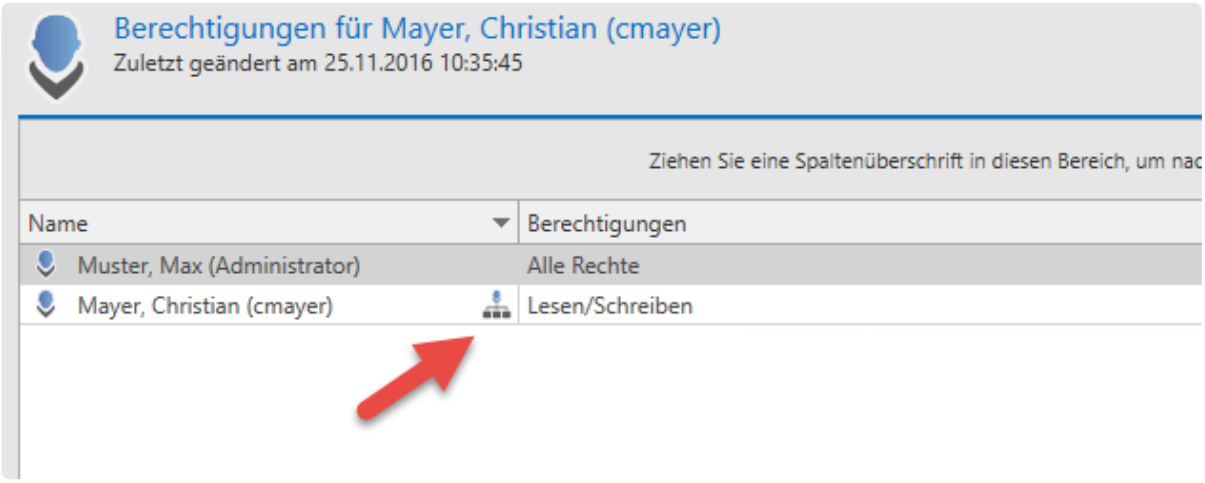
- **Neue Organisationseinheit/Benutzer**: Sowohl über die Ribbon, über den Shortcut “STRG + N” als auch über das Kontextmenü können Sie neue Organisationseinheiten bzw. neue Benutzer anlegen. Aufgrund der Komplexität existieren für diesen Unterpunkt separate Kapitel: neue Organisationsstrukturen / neue Benutzer.
- **Drag & Drop**: Mit dieser Option können Sie Benutzer oder Organisationseinheiten in der

Listenansicht per Drag & Drop verschieben.

- **Berechtigungen**: Legen Sie fest, wer die Organisationsstruktur in welcher Form administrieren darf.
- **Einstellungen**: Können Sie sowohl auf Benutzer als auch auf Organisationseinheiten konfigurieren. Näheres zu den Benutzereinstellungen finden Sie im Kapitel globale Einstellungen.
- **Active Directory**: Die Anbindung an das Active Directory, die ab der Enterprise Edition möglich ist, wird in einem eigenen Kapitel erläutert.
- **Multifaktor-Authentifizierung**: Die Anmeldung nach erfolgreicher Authentifizierung durch einen weiteren Faktor schafft zusätzlich Sicherheit.
- **Passwort zurücksetzen**: Administratoren können die Passwörter, mit denen sich Benutzer am Password Safe anmelden, auf einen definierbaren Wert zurücksetzen, sofern Sie die Active Directory Anbindung über die Ende zu Ende Verschlüsselung konfigurieren. Im alternativen Master Key Modus ist die Authentifizierung an die korrekte Eingabe des AD-Passwortes gekoppelt.

✻ Für das Zurücksetzen eines Benutzerpasswortes benötigen Sie das Schlüsselmaterial des Benutzers, dessen Besitz mit dem Mitgliedschaftsicon symbolisiert wird.

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



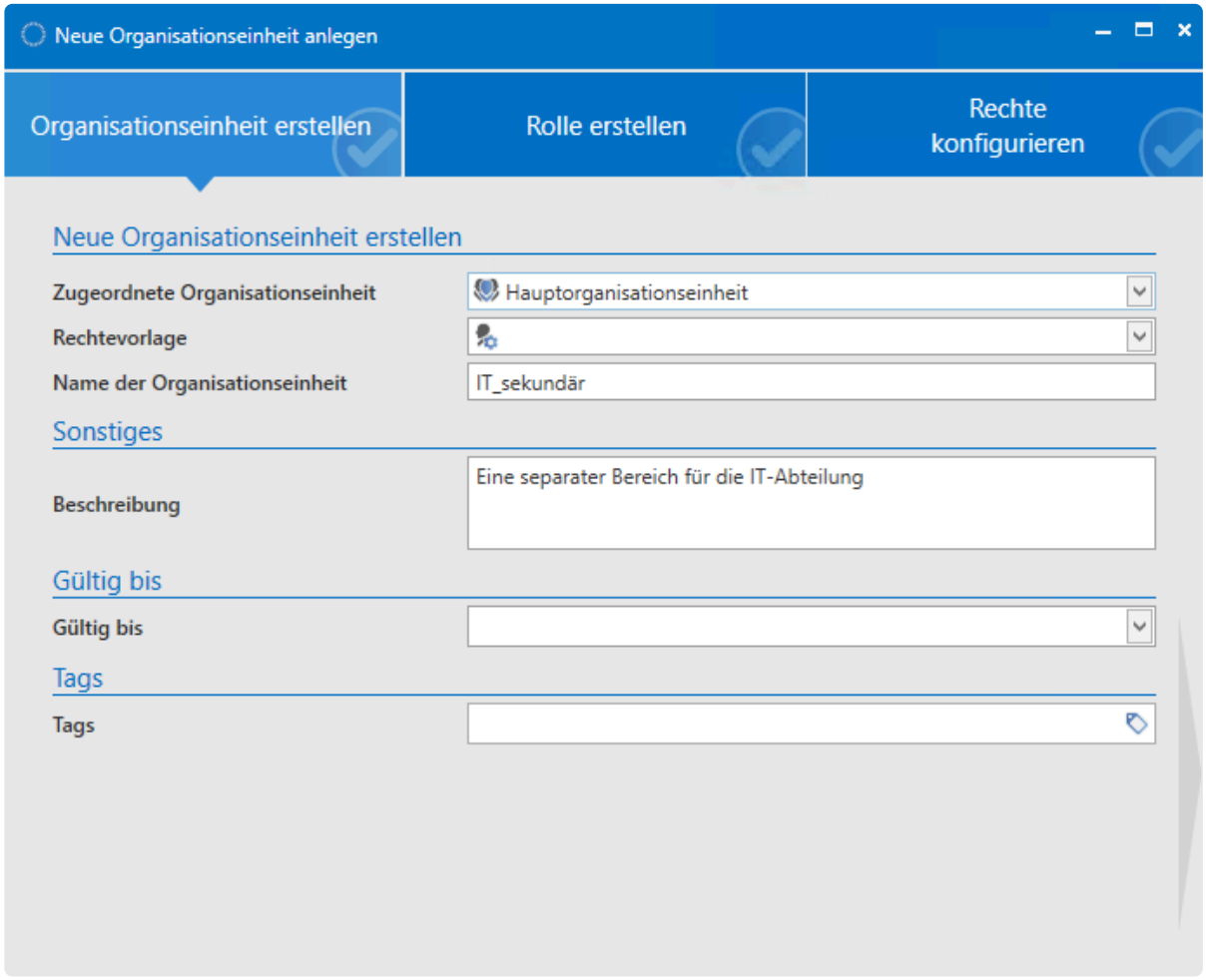
Durch diese Konfiguration kann das Benutzerpasswort nicht durch Administratoren zurückgesetzt werden. Bei Verlust des Passwortes besteht daher technisch keine Möglichkeit, das Passwort systemseitig zu “resetten”.

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

Anlegen lokaler Organisationseinheiten

Sowohl Benutzer als auch Organisationseinheiten selbst können Sie wie gewohnt über die Ribbon (Alternativ über Ctrl. + N oder Kontextmenü) anlegen. Dabei öffnet sich ein Assistent, der Sie unterstützt. Nachfolgend wird eine neue Organisationseinheit erstellt:

Organisationseinheit erstellen

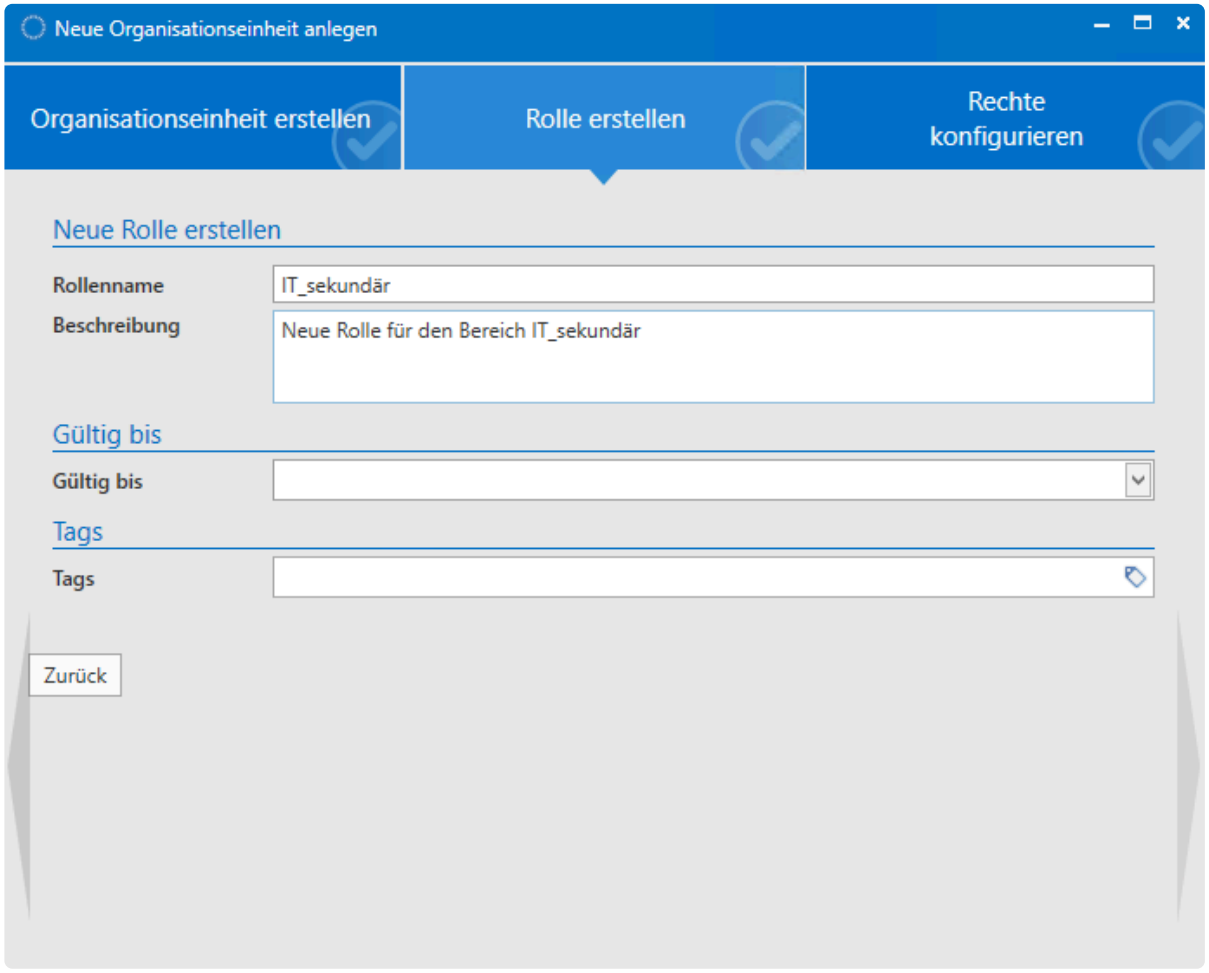


- **Zugeordnete Organisationseinheit**: Sobald Sie hier die **Hauptorganisationseinheit** festlegen, erhält das neue Objekt keine Zuordnung zu einer bereits bestehenden Organisationseinheit.

- **Rechtevorlagengruppe**: Haben Sie unter “zugeordneter Organisationseinheit” eine bereits bestehende ausgewählt, können Sie hier eine der dort möglicherweise vorhandenen Rechtevorlagengruppen auswählen.

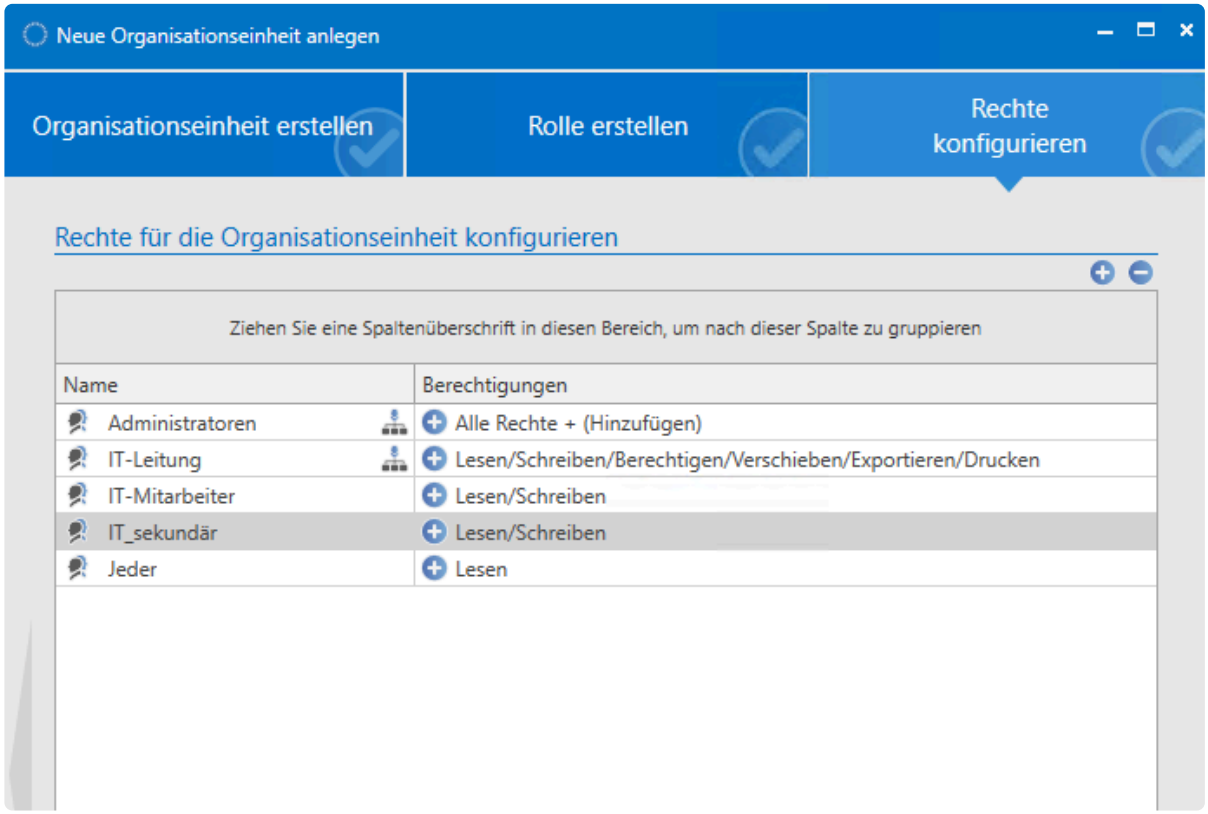
Als Default wird die in der Listenansicht markierte Organisationseinheit verwendet. Dies betrifft die Felder “zugeordnete Organisationseinheit” und “Rechtevorlage”.

Rolle erstellen



Über den zweiten Reiter im Assistenten legen Sie neue Rollen an. Diese Rolle wird automatisch mit “lesend” auf die neu erstellte Organisationseinheit berechtigt.

Rechte konfigurieren



Im dritten Reiter des Assistenten definieren Sie die Berechtigungen auf die neue Organisationseinheit. Haben Sie im ersten Reiter eine zugeordnete Organisationseinheit, bzw. eine Rechtevorlagengruppe, definiert, so erbt die neue Organisationseinheit deren Rechte. Passen Sie diese Berechtigungen bei Bedarf an.

> ✻ Das Modul **Organisationsstruktur** orientiert sich am gleichnamigen WebClient-Modul. Beide Module unterscheiden sich in Umfang und Design, sind aber hinsichtlich der Bedienung trotzdem nahezu identisch.

Benutzerverwaltung

Wie werden im Password Safe Benutzer verwaltet?

Die Art der Benutzerverwaltung hängt stark davon ab, ob Sie das Active Directory angebunden haben oder nicht. Im Master Key Modus ist das Active Directory das führende System, da dort die Benutzerverwaltung erfolgt. Falls der Password Safe das führende System ist – wie z.B. beim Ende zu Ende Modus – erfolgt die Benutzerverwaltung im Modul Organisationsstrukturen. Dieser Fall wird folgend beschrieben.

Relevante Rechte

Zum Anlegen lokaler Benutzer werden folgende Rechte benötigt.

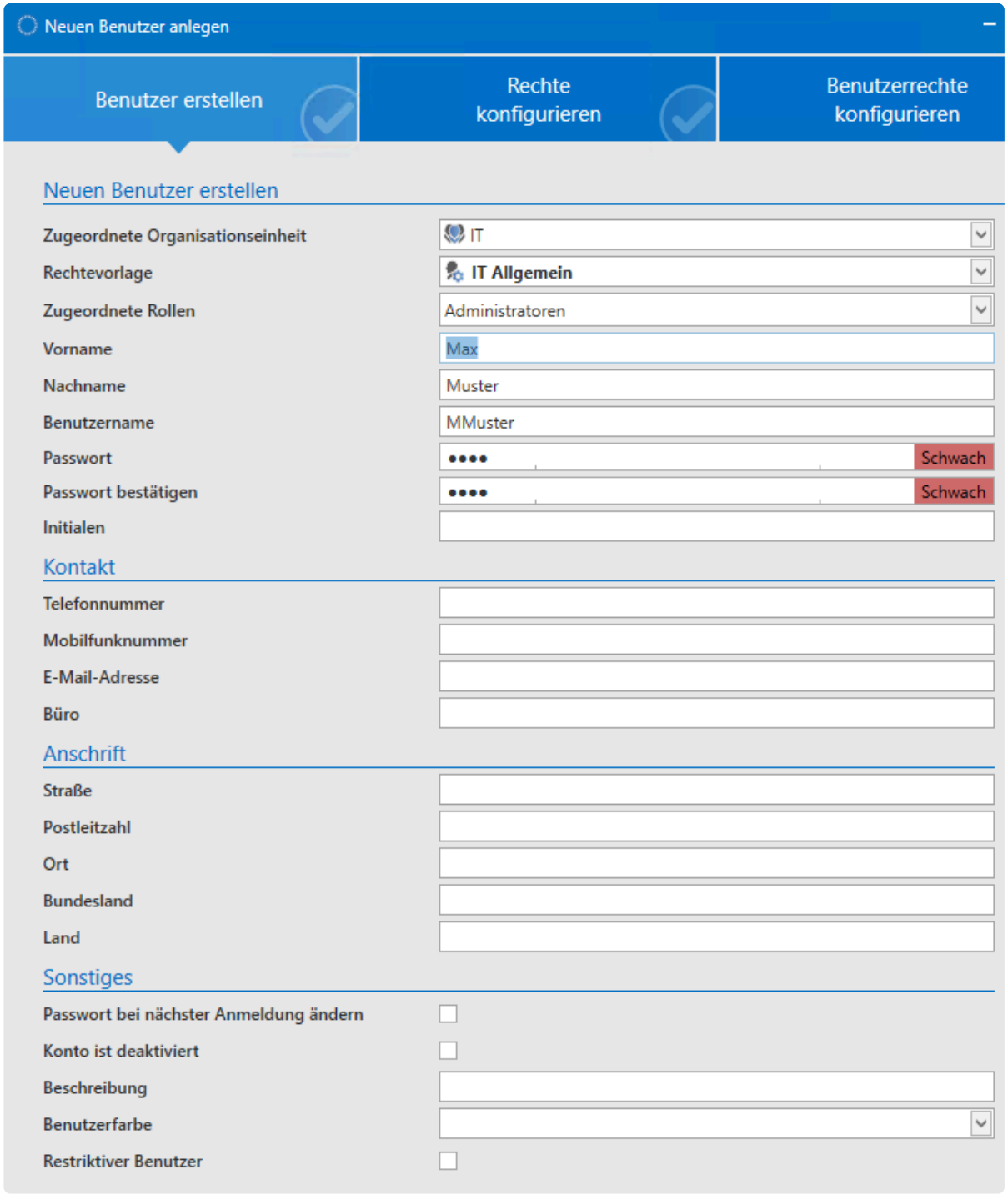
Benutzerrechte

- Kann neuen Benutzer anlegen
- Organisationsstruktur Modul anzeigen

Anlegen lokaler Benutzer

Grundsätzlich werden neue Benutzer wie lokale Organisationseinheiten angelegt. Daher wird hier nur auf die Unterschiede eingegangen.

Benutzer erstellen



- **Zugeordnete Rollen**: Neuen Benutzern können Sie direkt beim Erstellen eine oder mehrere Rollen zuweisen.
- **Passwort bei der nächsten Anmeldung ändern**: Der Benutzer wird bei der nächsten Anmeldung aufgefordert, sein Benutzerpasswort zu ändern (obligatorisch).
- **Konto ist deaktiviert**: Sie erstellen den Benutzer im Zustand “deaktiviert”. Das Konto ist nicht nutzbar. Er kann aber von Benutzern mit Schreibrechten jederzeit aktiviert werden.
- **restriktiver Benutzer**: In vielen Unternehmen existieren Kontrollinstanzen, die nur die Integrität und Hierarchien der Informationen zueinander überprüfen, jedoch nicht selbst produktiv damit arbeiten sollen. Ein Datenschutzbeauftragter könnte eine solche Person sein. Das Merkmal **restriktiver Benutzer** bezieht sich auf die Einschränkung im Hinblick der Einsicht auf das Passwortfeld, das er nie sehen kann.

Ein restriktiver Benutzer kann keine Passwörter einsehen

Rechte konfigurieren

Im zweiten Reiter des Assistenten können Sie die Berechtigungen auf den neu zu erstellenden Benutzer definieren. Haben Sie im ersten Reiter eine zugeordnete Organisationseinheit, bzw. Rechtevorlagengruppe definiert, so erbt der Benutzer diese Rechte. Bei Bedarf können Sie diese Berechtigungen auch noch anpassen.

Benutzerrechte konfigurieren

Benutzer erhalten Benutzerrechte stets über eine Rolle, benutzerspezifisch oder global (vergl. Benutzerrechte). Haben Sie 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, die in einem separaten Kapitel beschrieben werden.

Benutzerlizenzen

In der **Enterprise Plus** gibt es zwei verschiedene Arten von Lizenzen. Dabei handelt es sich um **FullClient- und LightClient-Lizenzen.** In allen weiteren Editionen können Sie ausschließlich FullClient-Lizenzen erwerben.
Beachten Sie, dass lizenzierte LightClient-Benutzer nicht in der Lage sind, den FullClient zu nutzen. FullClient Benutzer hingegen können auch auf den LightClient umschalten.

Aus lizenztechnischen Gründen ist es nicht vorgesehen, von einem FullClient-Benutzer in einen LightClient-Benutzer zu wechseln!

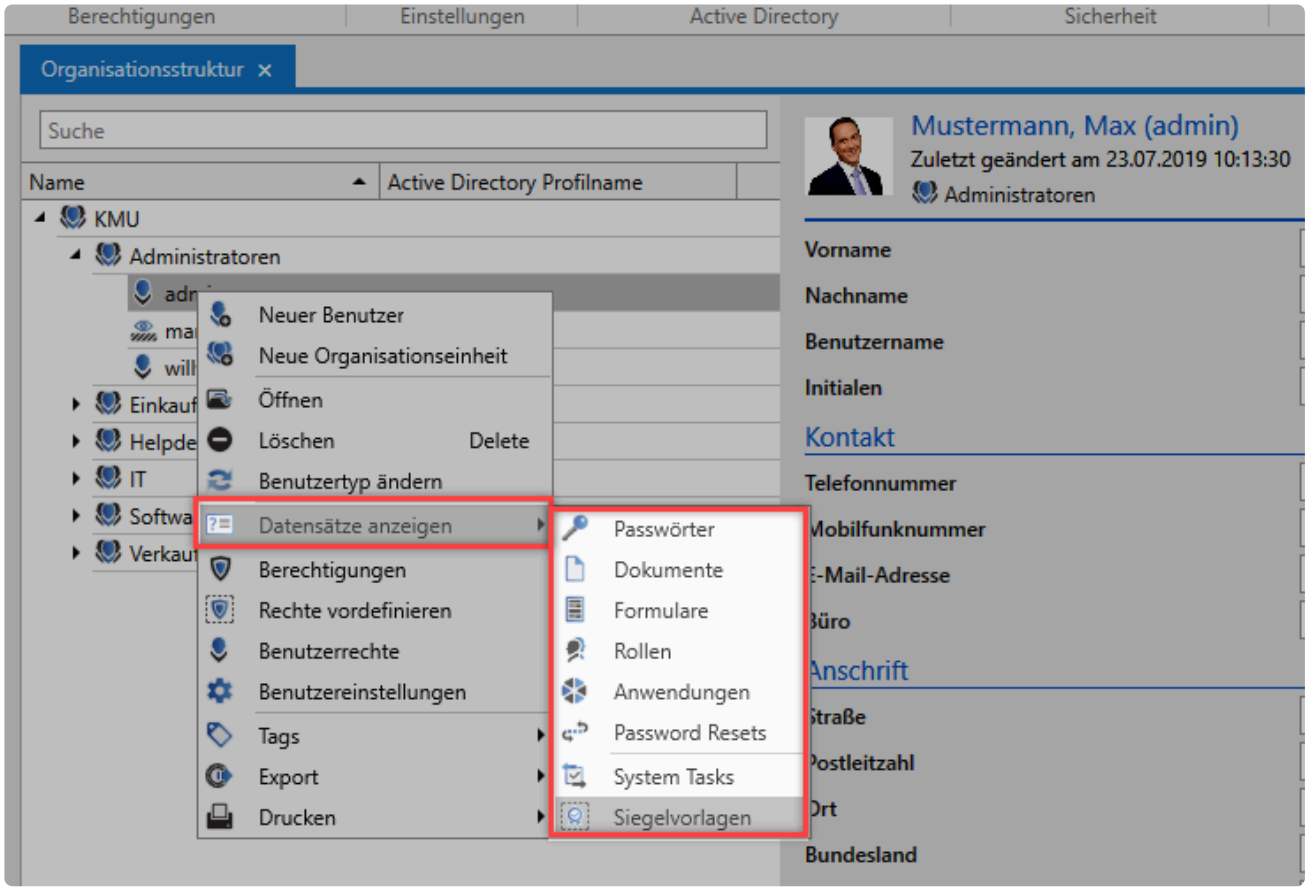
Bei Fragen zur Lizenzierung steht Ihnen unser Vertriebsteam gerne zur Verfügung.

Daten anzeigen, auf die ein Benutzer berechtigt ist

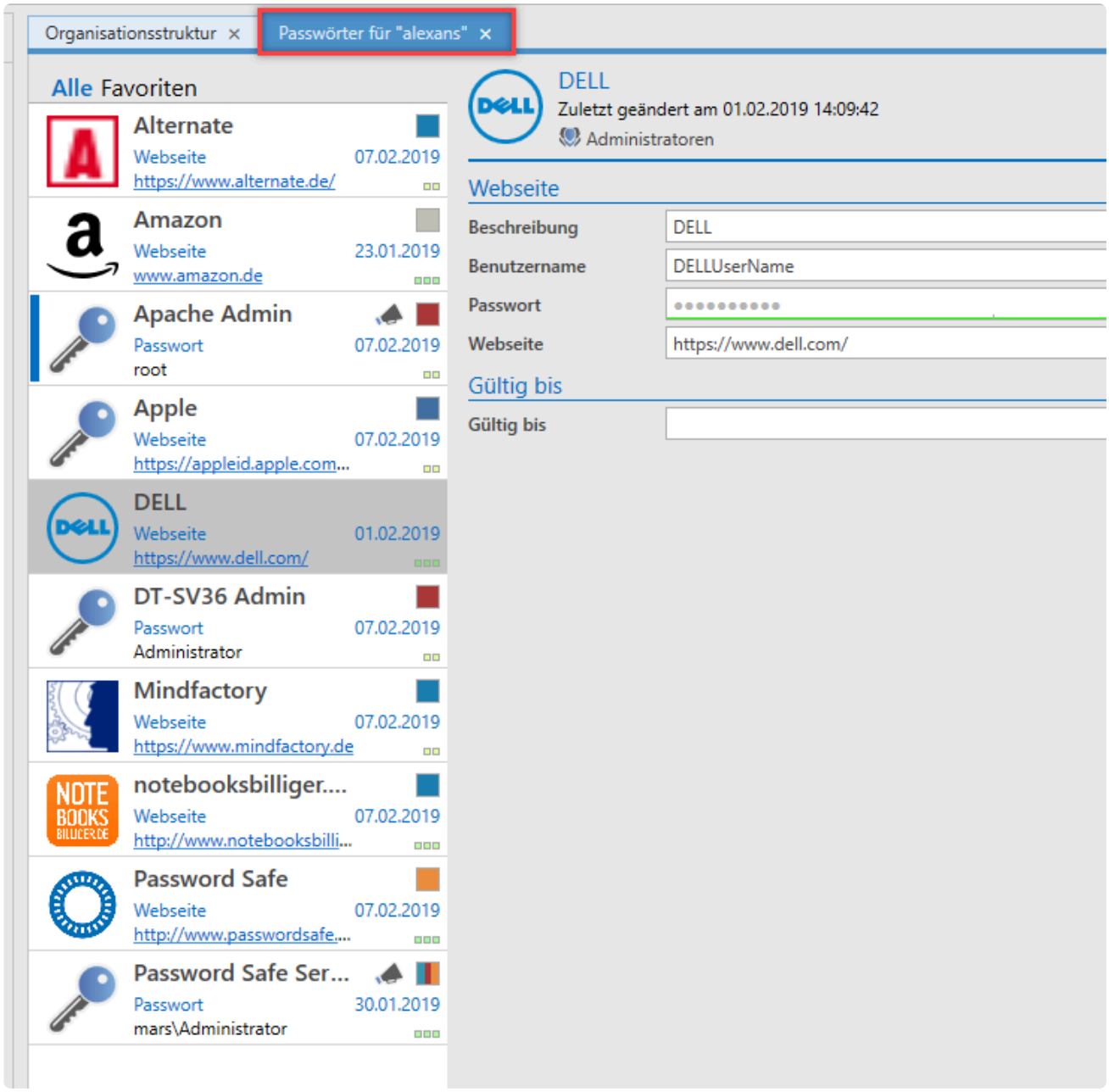
Öffnen Sie in der Organisationsstruktur mittels Rechtsklick auf den Benutzer das Kontextmenü. Hier finden Sie bei **Datensätze anzeigen** folgende Auswahlmöglichkeiten:

- Passwort
- Dokumente
- Formulare
- Rollen
- Anwendungen
- Password Reset

- System Tasks
- Siegelvorlagen



Es werden alle Berechtigungen auf einen Datensatz berücksichtigt, egal ob der Benutzer über eine Rolle oder direkt berechtigt wird.


Organisationsstruktur
Passwörter für "alexans"
Alle Favoriten
Alternate
Webseite
07.02.2019
https://www.alternate.de/
Amazon
Webseite
23.01.2019
www.amazon.de
Apache Admin
Passwort
07.02.2019
root
Apple
Webseite
07.02.2019
https://appleid.apple.com...
DELL
Webseite
01.02.2019
https://www.dell.com/
DT-SV36 Admin
Passwort
07.02.2019
Administrator
Mindfactory
Webseite
07.02.2019
https://www.mindfactory.de
notebooksbilliger....
Webseite
07.02.2019
http://www.notebooksbilli...
Password Safe
Webseite
07.02.2019
http://www.passwordsafe....
Password Safe Ser...
Passwort
30.01.2019
mars\Administrator
DELL
Zuletzt geändert am 01.02.2019 14:09:42
Administratoren
Webseite
Beschreibung
DELL
Benutzername
DELLUserName
Passwort
Webseite
https://www.dell.com/
Gültig bis
Gültig bis

Benutzer Passwörter / Anmeldung am Client

Benutzer Passwörter

Benutzer erhalten je nach verwendeter Verschlüsselung ihre Zugangsdaten aus Password Safe selbst oder aus dem Active Directory. Dementsprechend unterscheidet sich auch die Anmeldung an Password Safe selbst.

Unterschiede bei den Benutzern und Passwörtern

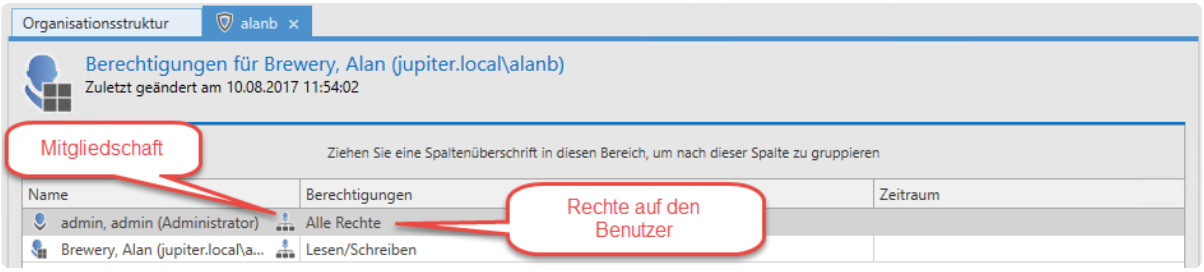
- **Lokale Benutzer**
  werden direkt in Password Safe erstellt und gepflegt. Diesen Benutzern muss direkt beim Anlegen ein Passwort zugewiesen werden. Bei der Migration lokaler Benutzer aus Password Safe V7 bekommen diese ein zufällig generiertes Passwort per E-Mail.

- **AD Benutzer im Ende zu Ende Modus**
  erhalten ebenfalls ein Passwort direkt in Password Safe. Bei einer Migration aus Password Safe V7 erhalten auch diese Benutzer per E-Mail ein neues Passwort.

- **AD Benutzer im Master key Modus**
  melden sich direkt mit ihren Zugangsdaten der Domäne an. Da sich diese Benutzer direkt gegenüber dem Active Directory authentifizieren, gilt immer das dort aktuell hinterlegte Passwort. Nach einer Migration können sich diese Benutzer direkt mit dem bekannten Passwort anmelden

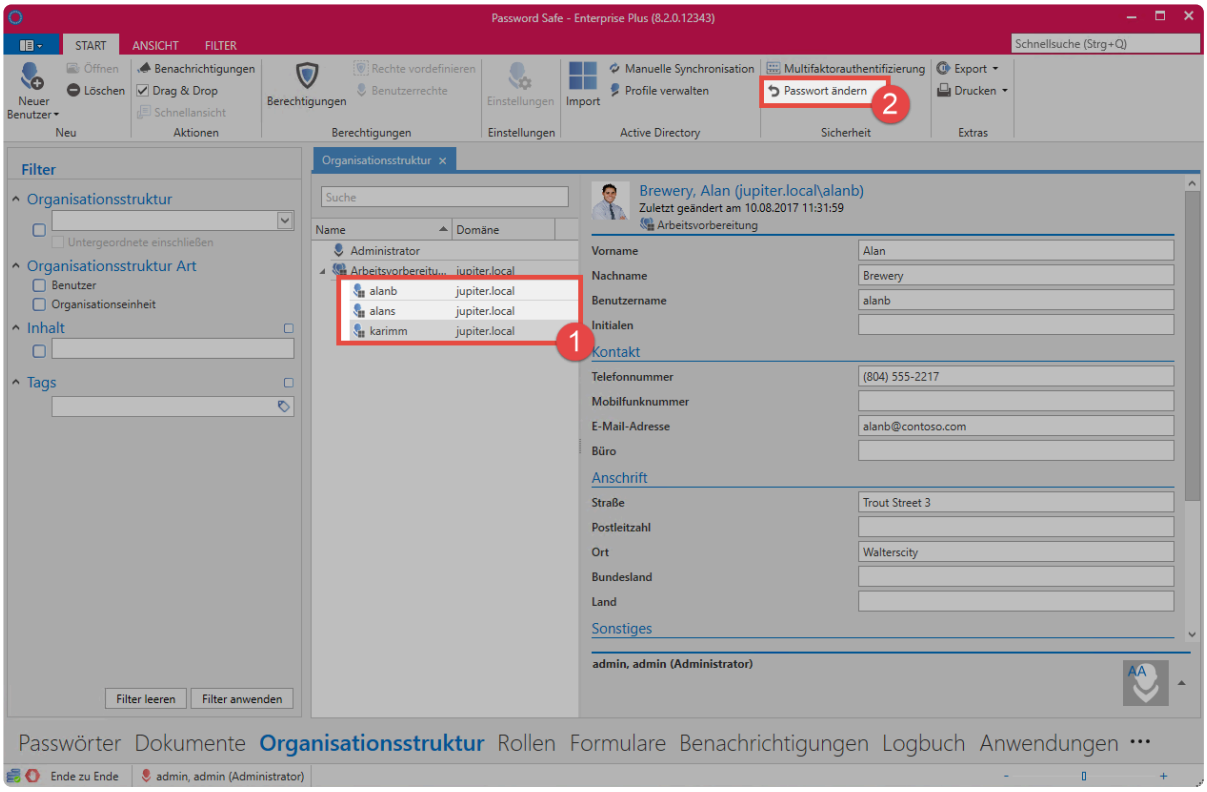
Benötigte Rechte

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, das Passwort zu ändern.



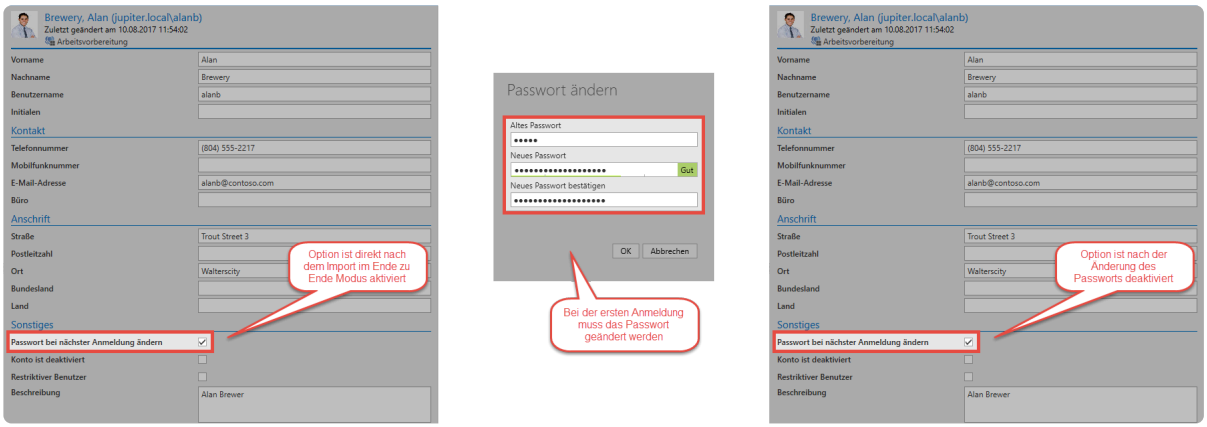
Zuweisen und Ändern von Passwörtern

Lokalen Benutzern wird das initiale Passwort direkt beim Erstellen zugewiesen. Benutzern, die im Ende zu Ende Modus importiert werden erhalten, muss nach dem Import ebenfalls ein Passwort zugewiesen werden. Dies geschieht direkt über die Ribbon. Hier ist auch eine Multiselektion möglich, falls beispielsweise mehreren importierten Benutzern das gleiche Passwort zugewiesen 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** aktivieren Sie diese während des Erstellens des Benutzers. 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 legen Sie die Passwortrichtlinie noch als Benutzer Passwortrichtlinie fest.

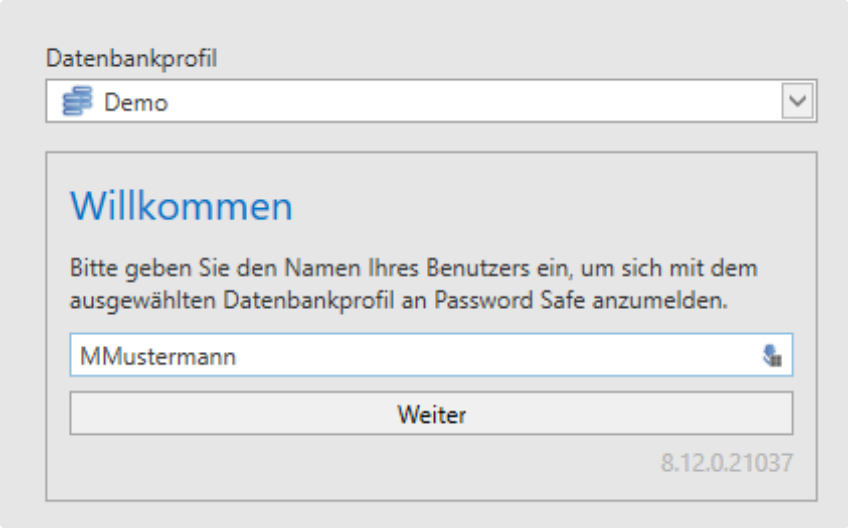
Anmeldung an der Datenbank

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

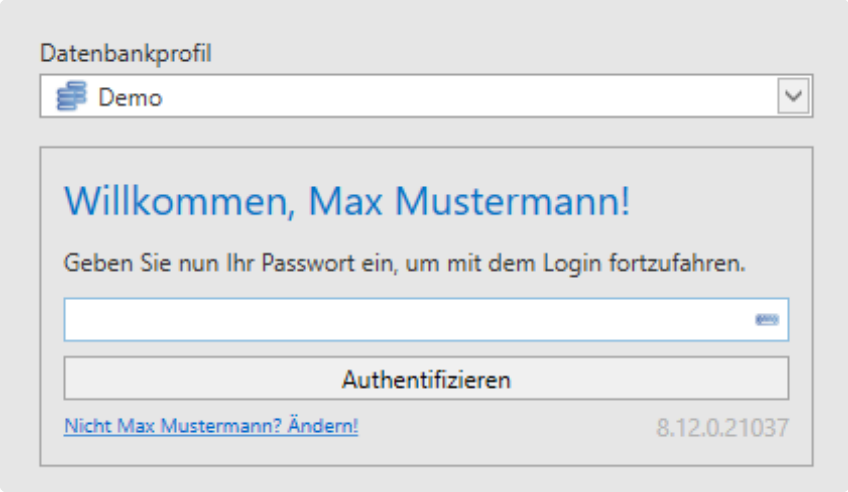
Lokaler Benutzer

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

Zuerst geben Sie dabei den Benutzernamen an:

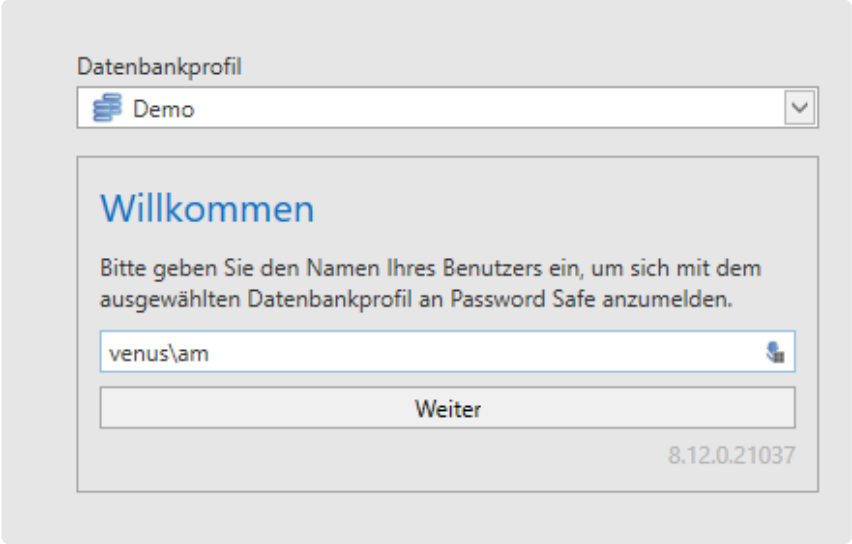


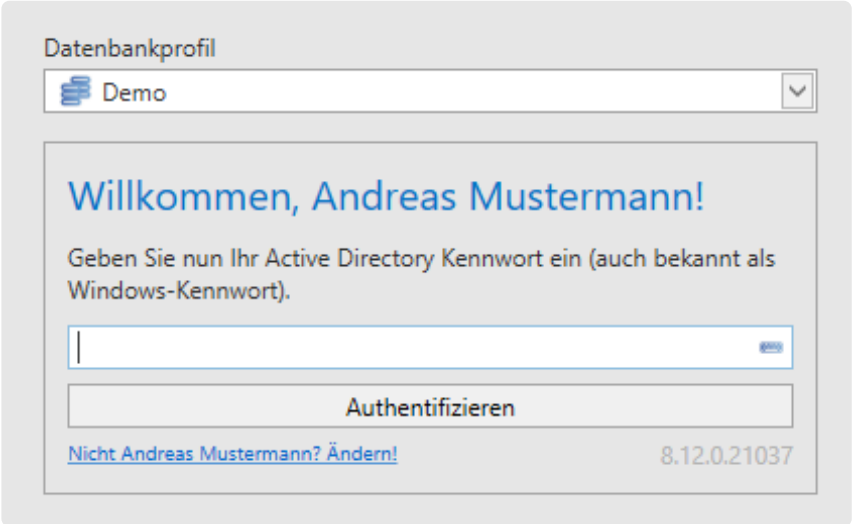
Wird ein Benutzer gefunden erfolgt die Passwortabfrage:



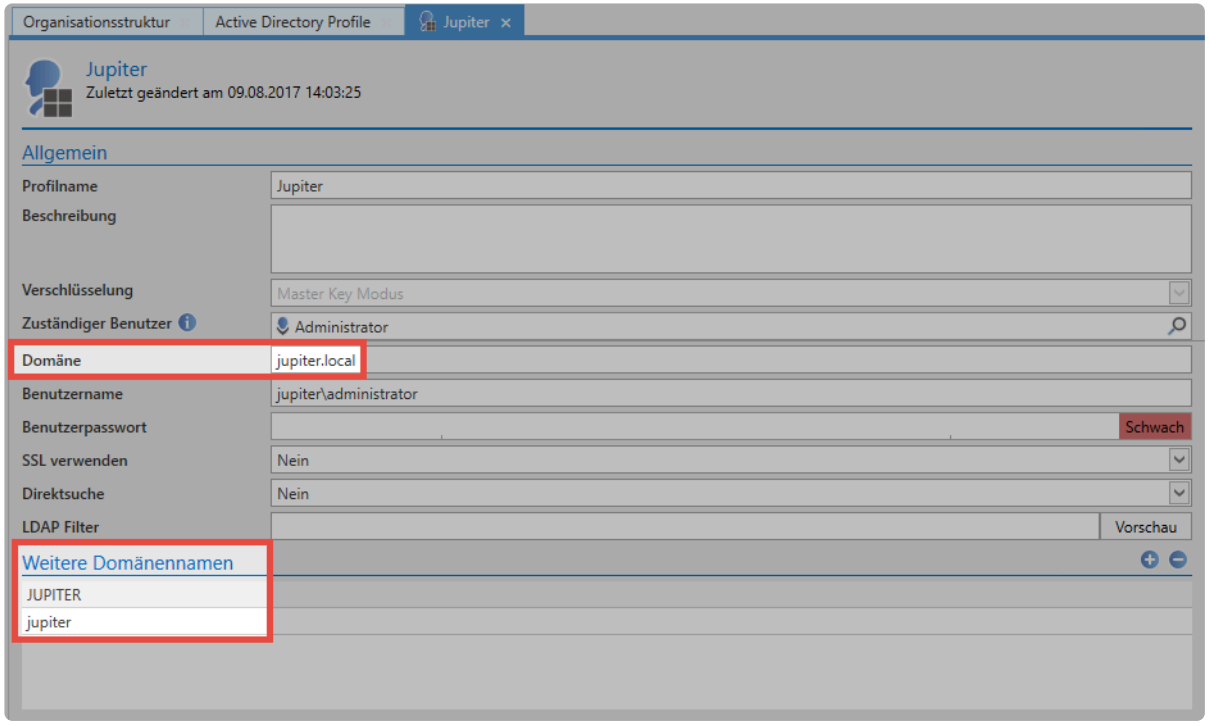
AD Benutzer

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





Geben Sie die Domäne hierbei so an, wie sie im AD Profil unter **Domäne** konfiguriert ist. Unter **Weitere Domänennamen** können andere Versionen der Domäne hinterlegt werden.



Die Anmeldung am Client wird automatisch an den den SSO Agent und weitere Clients auf dem gleichen Rechner weitergereicht. Das gilt auch für die Anmeldung am SSO Agent.

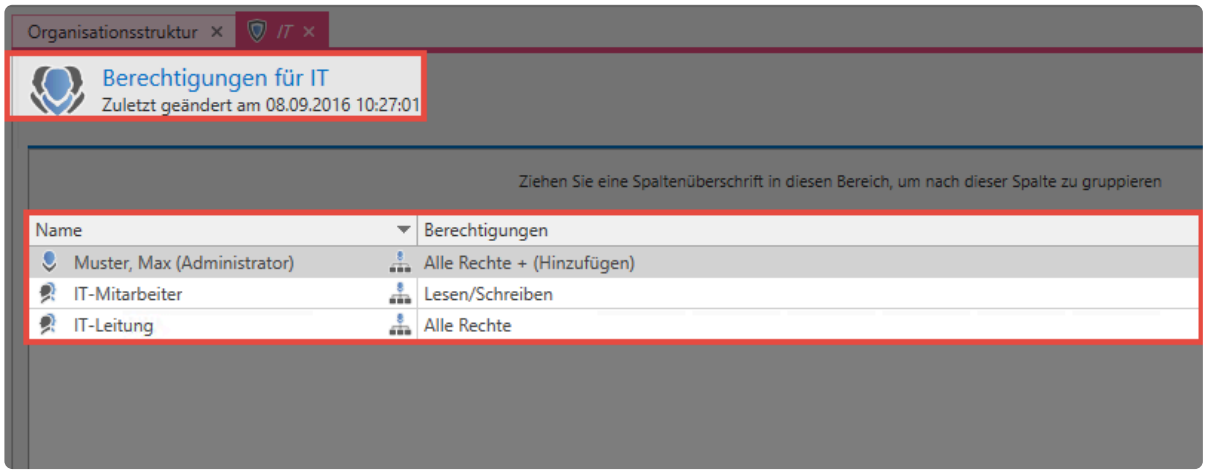
Berechtigungen auf Organisationsstrukturen

Auswirkung der Berechtigungen

Die Berechtigungen auf Organisationsstrukturen haben zweierlei Auswirkungen. Zum einen definieren Sie darüber, durch wen – und in welchem Umfang – eine Organisationseinheit gesehen, bzw. bearbeitet werden darf. Zusätzlich ist als Standard die **Vererbung aus Organisationsstrukturen** aktiviert. Diejenigen Berechtigungen, welche auf die Organisationseinheit konfiguriert sind, werden also auf alle neuen Elemente innerhalb der Organisationseinheit übertragen. Dies bedeutet, dass zwischen den Berechtigungen auf eine Organisationsstruktur sowie den Berechtigungen auf Daten, welche in diesen Organisationsstrukturen liegen, **nicht** unterschieden wird.

Berechtigungen auf Organisationsstrukturen

Die Berechtigungen können Sie entweder über den entsprechenden Button in der Ribbon, oder über das Kontextmenü der rechten Maustaste verwalten:



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

Wichtig ist, dass Sie die angezeigten Berechtigungen richtig deuten. Das obige Beispiel zeigt die

Berechtigungen auf die Organisationsstruktur **IT**. Der Benutzer Max Muster besitzt alle Rechte auf diese Organisationsstruktur und kann demnach diese Organisationsstruktur bearbeiten, löschen und auch Berechtigungen setzen.

Das Hinzufügen-Recht

Das Recht **Hinzufügen** steuert welcher Benutzer innerhalb einer Organisationseinheit neue Elemente – wie z.B. Datensätze, Benutzer, usw. – erstellen darf. Im obigen Beispiel wäre das Hinzufügen neuer Datensätze lediglich dem Administrator gestattet. Auch die IT-Leitung, welche alle anderen Rechte auf die Organisationsstruktur **IT** hat, besitzen nicht das Recht, neue Datensätze anzulegen. Die IT-Leitung kann also die Organisationseinheit selbst in vollem Umfang bearbeiten obwohl Sie darin keinen neuen Daten anlegen kann.

> ! Über das **Hinzufügen Recht** wird festgelegt wer in einer Organisationsstruktur neue Elemente anlegen darf. Dies betrifft **Passwörter, Dokumente, Anwendungen, Password Resets, Benutzer und Organisationseinheiten**.

Vererbung von Berechtigungen

Was wird vererbt und wie?

Die Berechtigungen, welche Sie auf eine Organisationseinheit gesetzt haben, können Sie auf die darunter liegenden Organisationseinheiten vererben. Vererbt wird immer durch die komplette Struktur hindurch bis auf die unterste Ebene.

> ✻ Die in diesem Kapitel beschriebene Vererbung wirkt sich **nur auf untergeordnete Organisationseinheiten** und nicht auf die darin befindlichen Passwörter, Dokumente, usw. aus. Im Kapitel **Vererbung aus Organisationsstrukturen** wird beschrieben, wie Sie Berechtigungen auch auf Datensätze vererben können.

Relevante Rechte

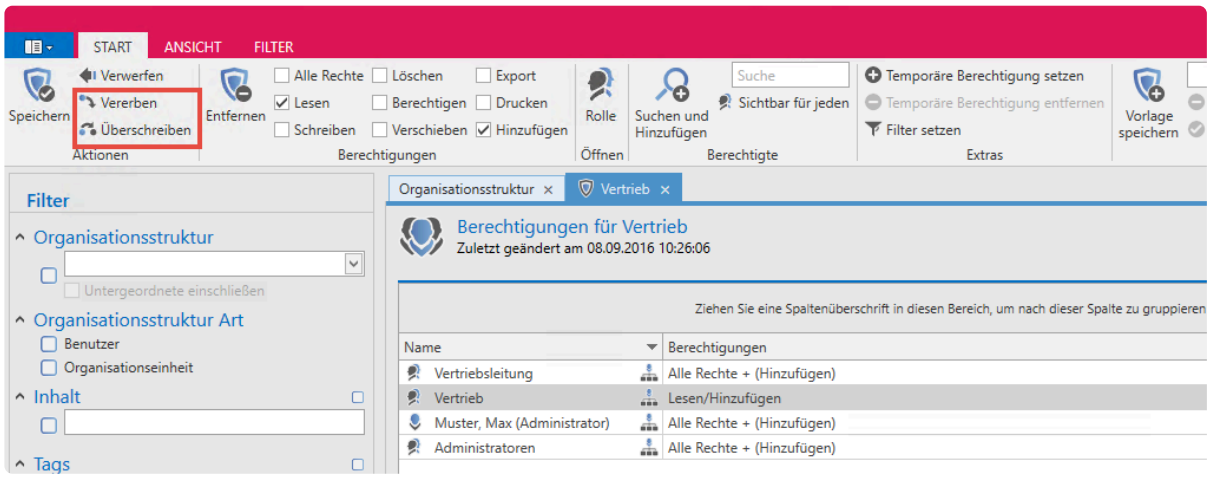
Sie benötigen folgende Optionen um die Icons **Vererben** und **Überschreiben** sehen zu können.

Benutzerrecht

- Kann Berechtigungen überschreiben
- Kann Berechtigungen vererben

Vererbung

Nachdem Sie dem gewünschten Benutzer die oben genannten Rechte gegeben haben, sieht er in der Ribbon stehen die beiden markierte Optionen.



Nach einer Anpassung der Rechte können Sie – vor dem endgültigen Speichern – über die Buttons definieren, ob und wie die Änderung vererbt werden soll.

- **Vererben**: Hierbei werden beim Speichern alle in der aktuellen Berechtigungsmaske definierten Konfigurationen auf darunterliegende Organisationsstrukturen vererbt. Bestehende und neue Berechtigungen werden hierbei addiert.

- **Überschreiben**: Es werden beim Speichern alle definierten Konfigurationen auf darunterliegende Organisationsstrukturen angewendet. Die bisherigen (alten) 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**. Sie benötigen 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 gewährleistet. Diese enthalten alle notwendigen Informationen für den Verbindungsaufbau und ermöglichen den Import sowie die Synchronisation von Benutzern, Organisationseinheiten und 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, die sich signifikant unterscheiden.

- **Ende zu Ende Verschlüsselung**
- **Master Key Modus**

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 (hierbei handelt es sich um ein Zertifikat, siehe auch **Master Key Zertifikate**) erstellt. Dieser Schlüssel wird auf alle Benutzer, Organisationseinheiten und Rollen voll berechtigt. Dies stellt einen zusätzlichen Angriffsvektor dar, der im Ende zu Ende Modus nicht gegeben ist. Im Gegenzug können Sie jedoch im Master Key Modus die Benutzer über die Synchronisation mit dem Active Directory aktualisieren. Ebenso werden Zugehörigkeiten zu Organisationseinheiten und Rollen importiert. Im sichereren Ende zu Ende Modus müssen Sie den Abgleich solcher Änderungen manuell durchführen.

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

Vergleich der Modi	Ende zu Ende Modus	Master Key Modus
Ende zu Ende Verschlüsselung*	+	-
Import von Benutzerinformationn	+	+
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	-	+
Autologin	+	+

Wie man sieht, bietet **E2EE die höchstmögliche Sicherheit**. Das Ziel ist der Import von Benutzern, Organisationseinheiten und Rollen. Deren Verwaltung und Konfiguration erfolgt komplett im Password Safe. Im Gegensatz hierzu ermöglicht Ihnen die Anbindung im **Master Key Modus den größtmöglichen Komfort**. Sie können darüber nicht nur Benutzer, Organisationseinheiten und Rollen, sondern auch deren Verknüpfungen bzw. Zugehörigkeiten importieren. 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 ebenso als Benutzer in Password Safe angelegt. Auch die Organisationseinheiten werden in Password Safe als solche verwendet.

Um Password Safe schnell in eine bestehende Struktur zu integrieren, können Sie auch Rollen aus dem Active Directory importieren. Hier gilt, dass **Active Directory Gruppen** zu **Password Safe Rollen** werden.

✻ Gruppen in Gruppen Mitgliedschaften, welche im Active Directory vorkommen können, werden in Password Safes nicht abgebildet. Es werden beide Gruppen als Rollen importiert. Diese sind jedoch eigenständig und nicht miteinander verknüpft.

! Wurde beim Active Directory Profil der **Master Key Modus** gewählt, gilt das **AD als führendes System**. Importierte Rollen 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 Ihnen die **höchstmögliche Sicherheit**. Benutzer, Organisationseinheiten sowie Rollen werden lediglich importiert. Die Berechtigungen und das Verhältnis der einzelnen Objekte zueinander muss in Password Safe konfiguriert werden. Der Vorteiil der Ende zu Ende Verschlüsselung besteht darin, dass das Active Directory als mögliches Einfallstor entschärft wird. Im Master Key Modus können Benutzer, welche Zugriff auf das Active Directory haben, kompletten Zugriff auf alle Passwörter erlangen, da das Zurücksetzen eines Windows-Benutzernamens die Anmeldung in fremdem Namen ermöglicht. **Mit aktiver E2EE benötigen Benutzer für den Password Safe ein eigenes Passwort**. Eine Anmeldung mit Benutzerdaten aus dem Active Directory ist nicht möglich.

Relevante Rechte

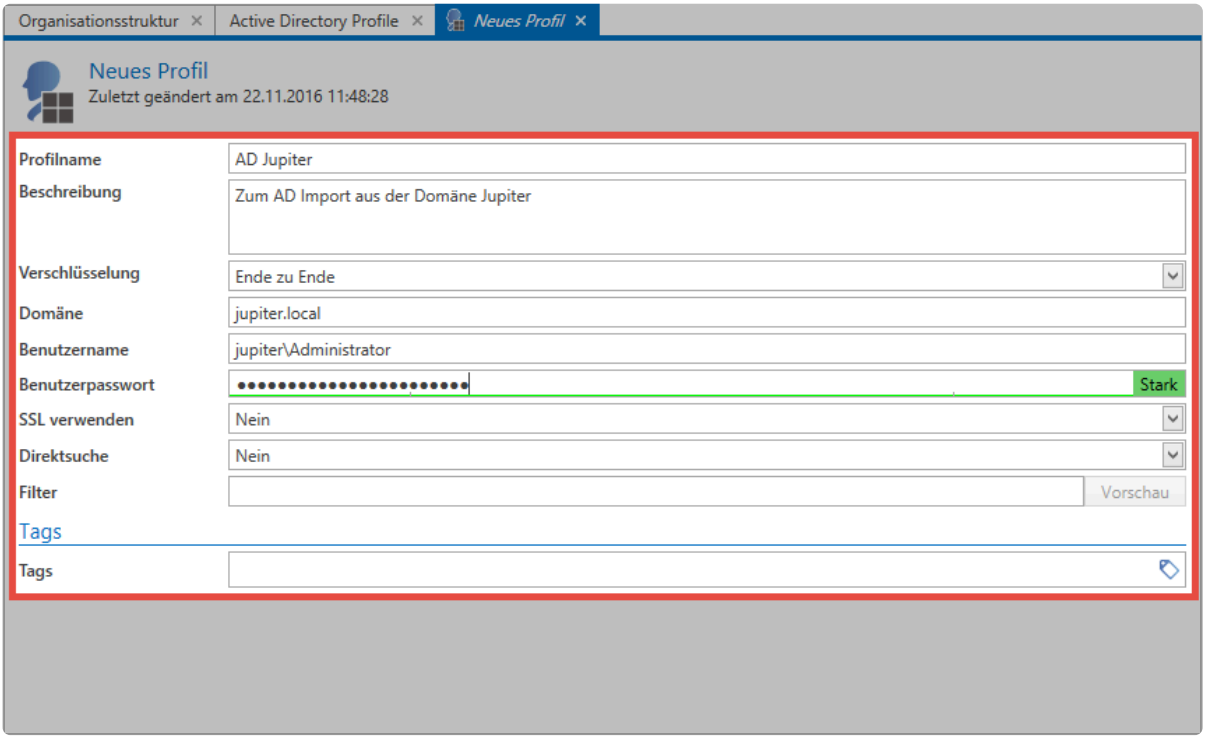
Um ein neues Profil anlegen zu können, benötigen Sie folgende Rechte:

Benutzerrecht

- Kann neue Active Directory Profile anlegen
- Organisationsstruktur Modul anzeigen
- Rollenmodul anzeigen

Erstellen des Profils

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

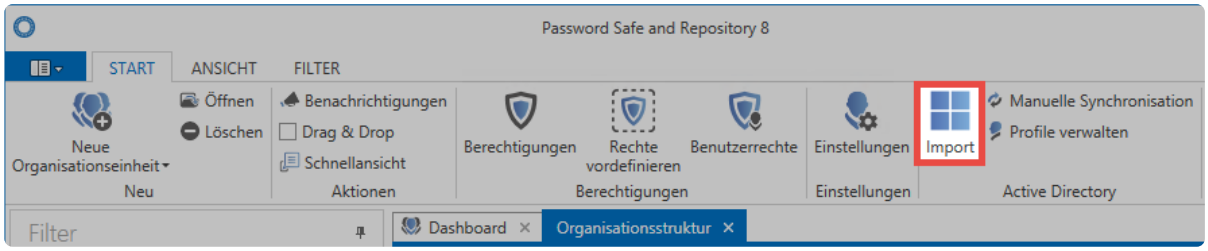


Im Feld **Verschlüsselung** aktivieren Sie **Ende zu Ende**.

- Zum Zugriff auf das AD ist ein **Benutzer** nötig. Dieser wird im Format **Domäne\Benutzer** angegeben.
- Zum oben angegebenen Benutzer ist das zugehörige **Benutzerpasswort** (Domänenkennwort) nötig.
- Die **Direktsuche** ist bei sehr großen Strukturen zu empfehlen. Die Darstellung der Baumstruktur entfällt. Alle Elemente können nur über die Suche gefunden und selektiert werden.
- Über den **Filter** kann mit einer LDAP Query direkt ein AD-Pfad als Einstiegspunkt angeben werden.
- Für die Anbindung des AD an Password Safe können verschiedene Sicherheitsoptionen – sogenannte AuthenticationTypes Enumeration – ausgewählt werden.
    - Secure
    - SecureSocketsLayer
    - ReadOnlyServer
    - Signing
    - Sealing

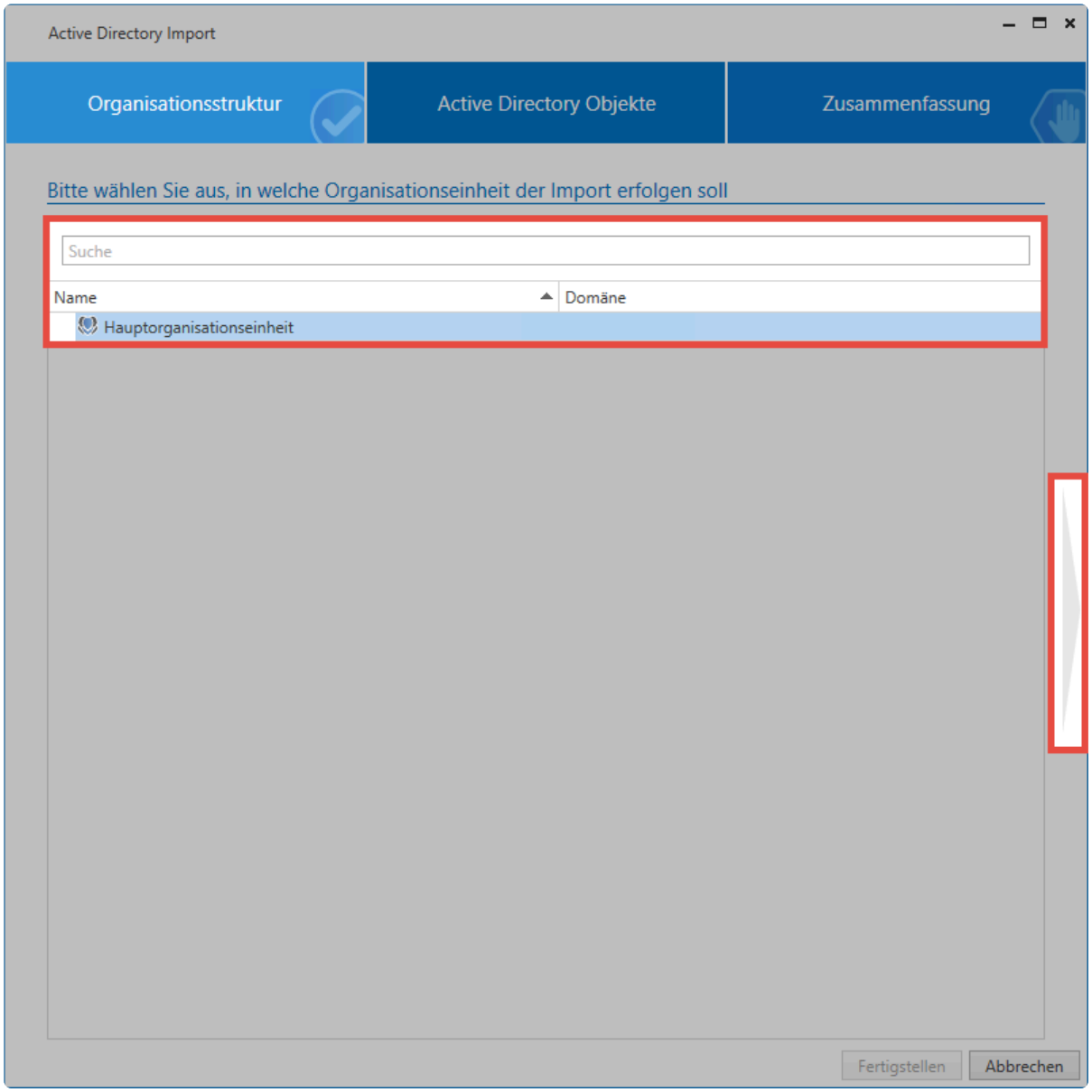
Import

Den Import starten Sie direkt in der Ribbon. Ein Assistent führt Sie durch den Vorgang.



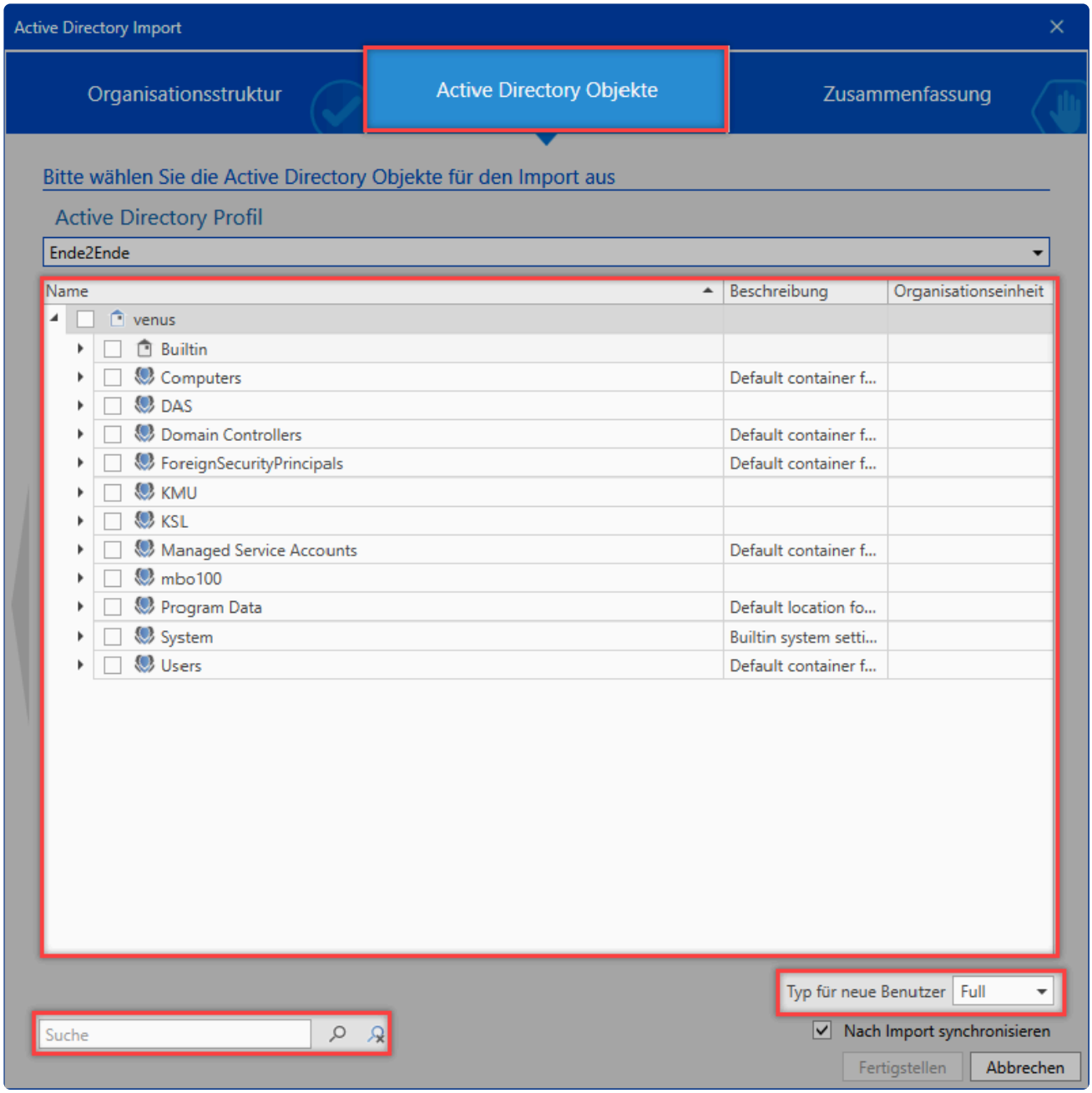
Organisationsstruktur

Zunächst wählen Sie die Organisationseinheit in die der Import erfolgen soll. Existieren – wie in diesem Beispiel – keine Organisationseinheiten in der Datenbank, erfolgt der Import in die **Hauptorganisationseinheit**.



Active Directory Objekte

Im nächsten Schritt selektieren Sie das Profil, mit dem importiert werden soll. Anschließend wählen Sie die Organisationseinheiten und/oder Benutzer zum Import aus. Hierfür steht eine Suche bereit.

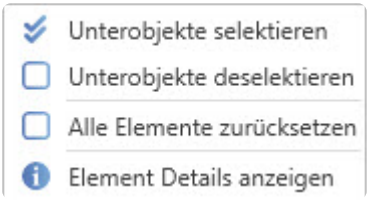


Hier ist ersichtlich, dass die Organisationseinheiten **Jupiter** und **Contoso** Elemente beinhalten, die importiert werden. Die Organisationseinheiten selbst werden nicht importiert. Die Markierung der Gruppe **Accounting** zeigt an, dass sowohl die Gruppe selbst als auch ein Teil der Unterelemente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

Es gibt verschiedene Symbole, die 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, die importiert werden.

Innerhalb der Liste können Sie über die rechte Maustaste ein Kontextmenü mit hilfreichen Funktionen zur Selektion der einzelnen Elemente aufrufen.



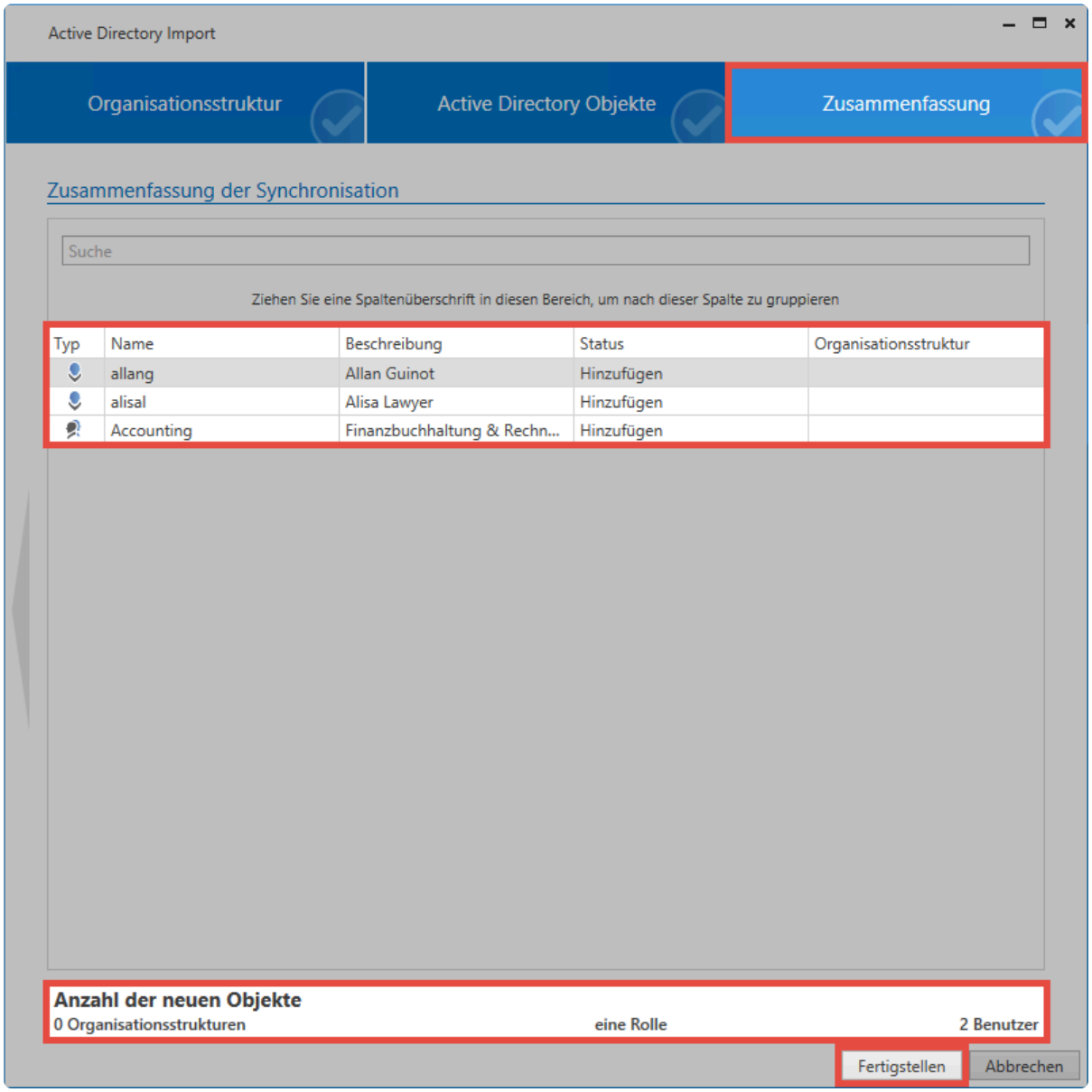
- **Unterobjekte selektieren** markiert alle Unterobjekte, die **direkt** unter dem aktuellen Objekt liegen.
- **Unterobjekte deselektieren** entfernt die Markierungen bei allen Unterobjekten, die **direkt** unter dem aktuellen Objekt liegen.
- **Alle Elemente zurücksetzen** entfernt alle bisher gesetzten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

Im unteren Bereich können Sie festlegen, ob die soeben zum Import selektieren Benutzer als **Light** oder **Full** Benutzer angelegt werden sollen.

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

Zusammenfassung

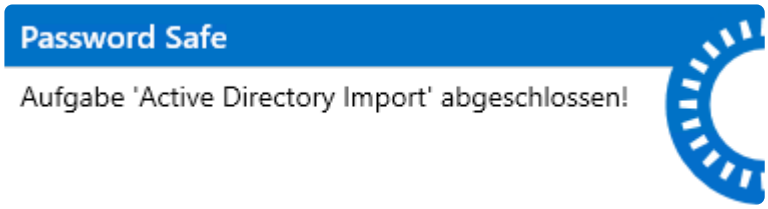
Die letzte Seite fasst zusammen, welche Objekte in welcher Form bearbeitet werden. In der Spalte **Status** sehen Sie, ob das Objekt neu hinzugefügt, aktualisiert oder deaktiviert wird. In der letzten Spalte ist ersichtlich, in welche Organisationseinheit das Element importiert wird. Ganz unten wird 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 ausgeführt. Die einzelnen Elemente tauchen nach und nach in der Liste auf. Je nach Menge der importierenden Daten kann dies längere Zeit in Anspruch nehmen. Wurde der Import beendet, erhalten Sie 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 nicht statt**. Ebenso können Sie keine Mitgliedschaften importieren. Nach dem Import müssen Sie die Benutzer manuell den entsprechenden Organisationseinheiten und Rollen zuweisen.

Importierte Benutzer und Organisationseinheiten

Im Ende zu Ende Modus verhalten sich die importierten Benutzer wie lokale Benutzer. Die Benutzer können/müssen Sie in Password Safe manuell bearbeiten. Die Zugehörigkeiten zu Organisationseinheiten und/oder Rollen müssen Sie ebenfalls manuell anpassen.

Rechte

Beim Import bzw. der Synchronisation werden die Rechte wie folgt vergeben:

Neue Objekte

	Benutzer	Gruppen	Rollen
Werden Rechte von der OU vererbt?	wenn kein Preset hinterlegt ist	wenn kein Preset hinterlegt ist	Nein
Werden Rechte aus einem Preset angewandt?	wenn Preset hinterlegt ist	wenn Preset hinterlegt ist	Nein
Wird das “Hinzufügen” Recht vergeben?	Nein	Ja	Nein
Wer bekommt den Rechte Schlüssel?	Importierter Benutzer und alle mit “Berechtigen” Recht	Alle	Importierte Rolle und alle mit “Berechtigen” Recht

Geänderte Objekte

	Benutzer	Gruppen	Rollen
Werden Rechte von der OU vererbt?	Nein	Nein	Nein
Werden Rechte aus einem Preset angewandt?	Nein	Nein	Nein
Wird das “Hinzufügen” Recht vergeben?	Nein	Nein	Nein
Wer bekommt den Rechte Schlüssel?	Keiner	Keine	Keine

✻ Im Ende zu Ende Modus wird durch den Import bzw. die Synchronisation **keine Rollenzugehörigkeit** vergeben.

Anmeldung an Password Safe

Benutzer, die in diesem Modus importiert werden, können sich **nicht mit dem Domänenkennwort anmelden**. Es wird beim Import ein Passwort generiert. Dieses wird den Benutzern per E-Mail zugeschickt. Hat ein Benutzer keine E-Mail-Adresse hinterlegt, wird der Benutzername als Passwort hinterlegt. Das Initialpasswort kann durch den Administrator oder den Benutzer selbst bei der ersten Anmeldung geändert werden.

Masterkey-Modus

Maximaler Komfort

Im Gegensatz zum Ende-zu-Ende-Modus, der die Sicherheit an erste Stelle stellt, bietet der Masterkey-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**.

Relevante Rechte

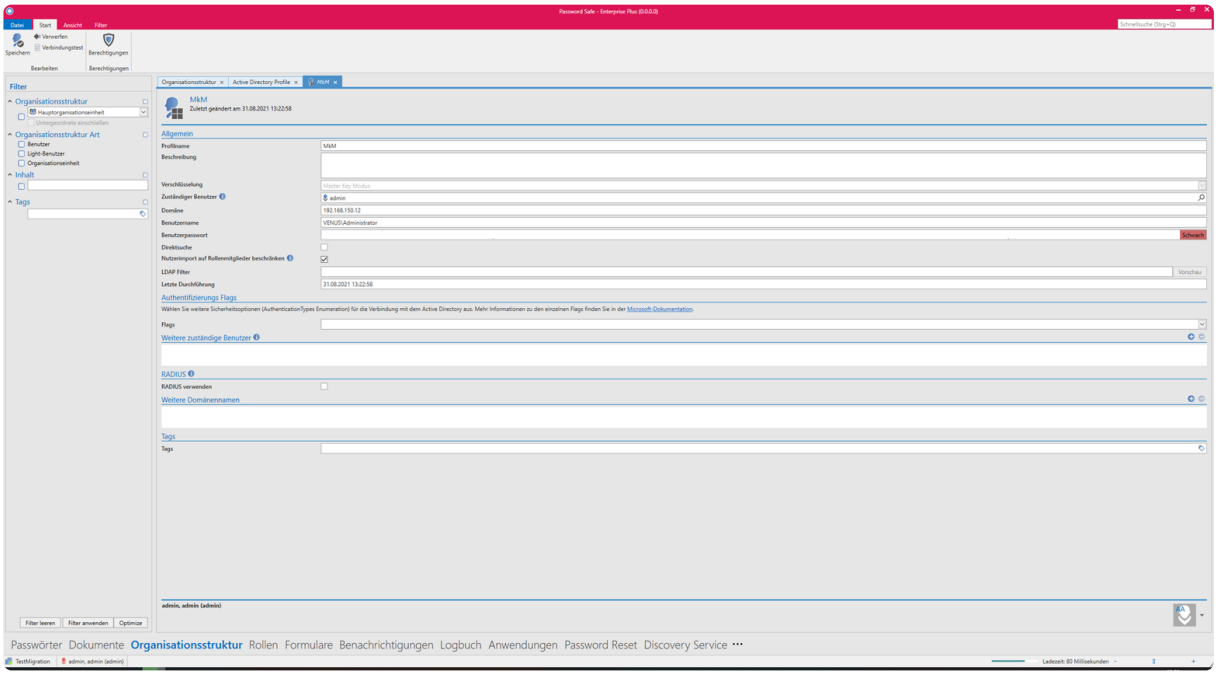
Um ein neues Profil anzulegen, benötigen Sie folgende Rechte.

Benutzerrecht

- Kann neue Active Directory Profile anlegen.
- Organisationsstruktur Modul anzeigen.
- Rollenmodul anzeigen.

Erstellen des Profils

Die Profilverwaltung starten Sie über das gleichnamige Icon in der Ribbon.



Im Profil geben Sie folgende Informationen an:

- **Profilname**
- Eine optionale **Beschreibung**
- Bei der **Verschlüsselung** wählen Sie den Masterkey-Modus aus.

Bei bereits erstellten Profilen können Sie die Verschlüsselung nicht mehr ändern.

- Unter **Domäne** legen Sie fest, welche Domäne ausgelesen wird. Der hier hinterlegte Wert wird auch zur Authentifizierung verwendet. Alternative Schreibweisen können sie unter **Weitere Domänennamen** hinterlegen.
- Es muss ein **Benutzer** (beispielsweise der Administrator) angegeben werden, welcher den Import durchführt. Aus technischen Gründen können Sie hierfür nur **lokale Benutzer** verwenden.
- Zum oben angegebenen Benutzer ist das zugehörige **Benutzerpasswort** (Domänenkennwort) nötig.
- Die **Direktsuche** ist bei sehr großen Strukturen zu empfehlen. Die Baumstruktur entfällt. Sie finden und selektieren Elemente dann nur über die Suche.
- Mit Aktivierung der Checkbox **Nutzerimport auf Rollenmitglieder beschränken** wird ein vereinfachter Modus aktiviert. In diesem werden nur AD Benutzer importiert, die Mitglied einer mindestens einer Rolle sind. Soblad sie kein Mitglied mindestens einer Rolle mehr sind, werden sie in Password Safe gelöscht.
- Mit Aktivierung der Checkbox **Update bei nächster Synchronisation erzwingen** werden **ALLE** Datensätze bei der nächsten Synchronisation aktualisiert, egal ob sich der Datensatz im Active Directory geändert hat oder nicht. (Diese Checkbox aktiviert sich automatisch wenn man die weiteren zuständigen Benutzer bearbeitet hat und wird wieder deaktiviert nach der nächsten Synchronisation)
- Mit dem **LDAP Filter** können Sie über eine LDAP-Query direkt einen AD-Pfad als Einstiegspunkt angeben.
- Für die Anbindung des AD an Password Safe können verschiedene Sicherheitsoptionen (**Flags**) – sogenannte AuthenticationTypes Enumeration – ausgewählt werden.
    - Secure
    - SecureSocketsLayer
    - ReadOnlyServer
    - Signing
    - Sealing

Die beiden ersten Optionen sind bei Neuanlage per default bereits aktiviert. Sollte eine Verbindung damit nicht möglich sein, deaktivieren Sie ggf. SecureSocketsLayer.

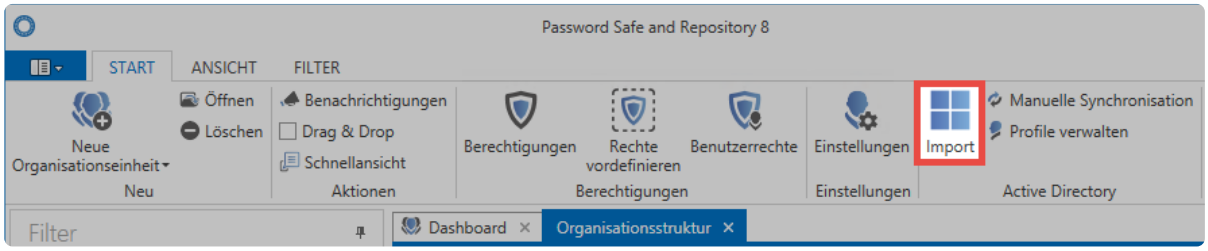
- Über **Weitere Zuständige Benutzer oder Rollen** definieren Sie, wer alles die Synchronisation durchführen darf.
- Unter **Weitere Domänennamen** können Sie alternative Schreibweisen der Anmeldedomäne hinterlegen. Diese müssen der Schreibweise im Loginfenster entsprechen. Wird die Domäne beispielsweise mit **jupiter.local** oder einer IP-Adresse angesprochen, kann die Anmeldung nur mit **jupiter\benutzer** erfolgen, wenn **jupiter** hinterlegt ist.

Der Masterkey wird als Zertifikat angelegt. Dieses Zertifikat müssen Sie **unbedingt sichern**! Möchten Sie die Datenbank auf einen anderen Server verschieben, müssen Sie das Zertifikat mit übertragen! Weitere Infos finden Sie im Kapitel **Zertifikate**.

Sie können die Authentifizierung auch über einen RADIUS-Server realisieren. Mehr dazu im Kapitel **Radius Server**

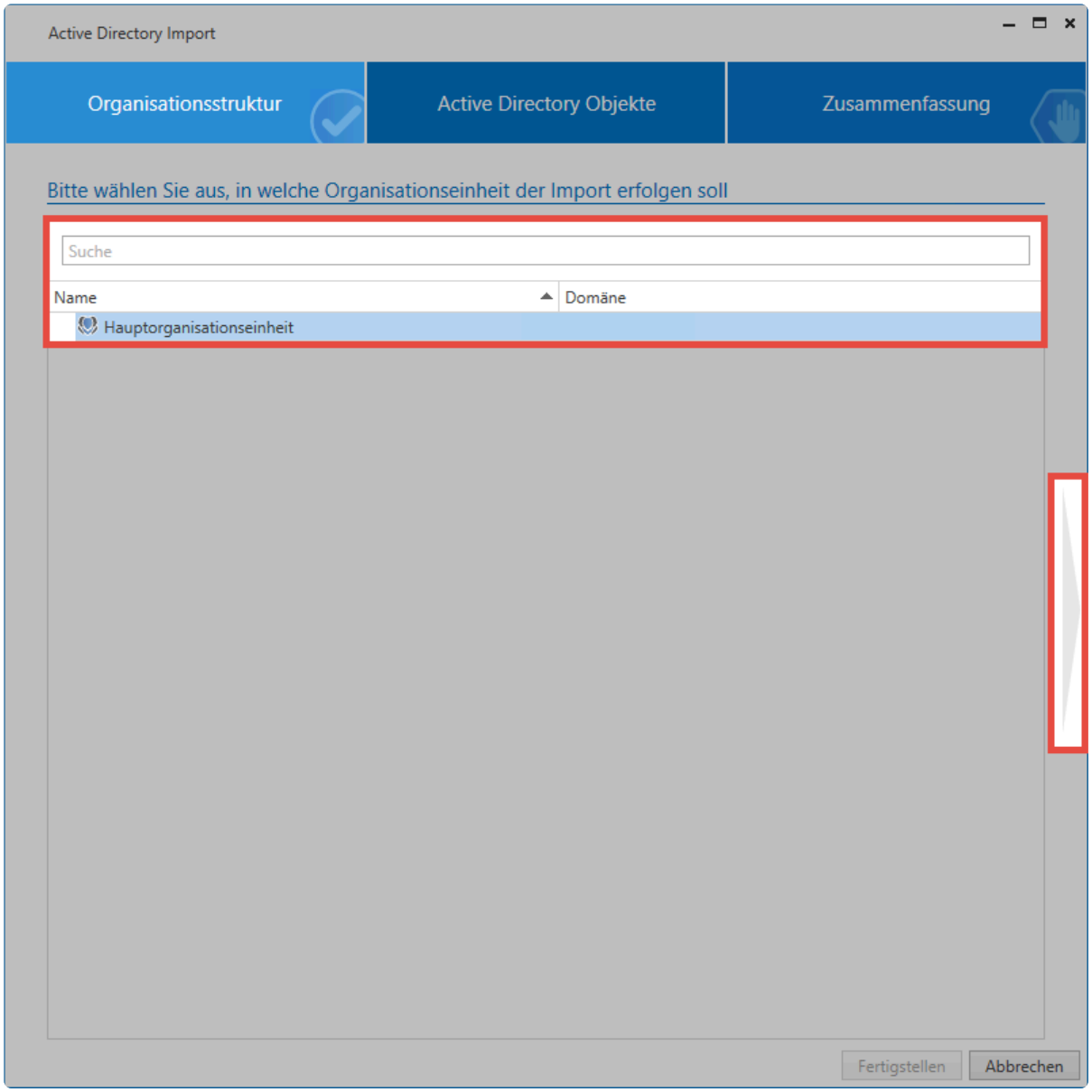
Import

Den Import starten Sie direkt in der Ribbon. Ein Assistent begleitet Sie durch den Vorgang.



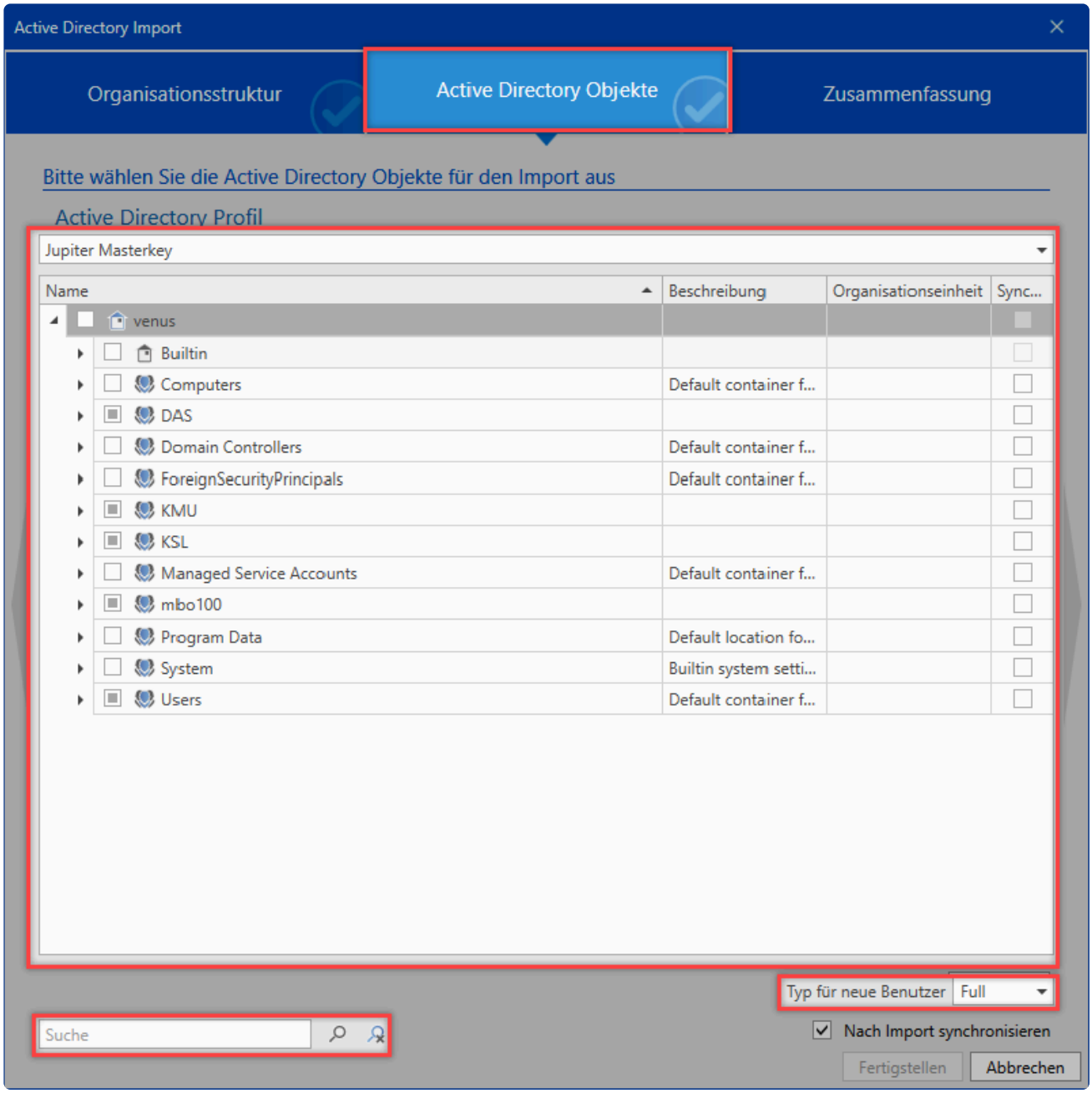
Organisationsstruktur

Zunächst legen Sie fest, in welche Organisationseinheit der Import erfolgen soll. Existiert – wie in diesem Beispiel – noch keine Organisationseinheit, erfolgt der Import in die **Hauptorganisationseinheit**.



Active Directory Objekte

Im nächsten Schritt wählen Sie das Profil, mit welchem Sie importieren wollen. Anschließend wählen Sie die Organisationseinheiten und/oder Benutzer zum Import aus. Hier können Sie auf die Suche zurückgreifen.

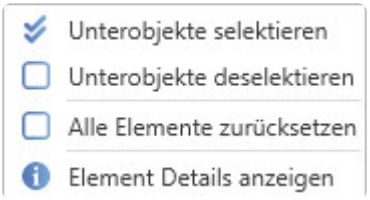


Hier sehen Sie, dass die Organisationseinheiten **Jupiter** und **Contoso** Elemente beinhalten, die importiert werden. Die Organisationseinheiten selbst werden nicht importiert. Die Gruppe **1099 Contractor** wird inklusive aller Unterelemente importiert. Die Markierung der Gruppe **Accounting** zeigt, dass hier die Gruppe selbst als auch ein Teil der Unterelemente importiert werden. Die Haken in der letzten Spalte sorgen dafür, dass die Elemente bei der zukünfigen Synchronisation beachtet werden.

Die zu importierenden Elemente werden mittels verschiedener Symbole gekennzeichnet.

☑ 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, die importiert werden.

Über einen Rechtsklick in die Liste gelangen Sie in ein Kontextmenü zur Selektion der einzelnen Elemente.



Im unteren Bereich legen Sie fest, ob die soeben für den Import selektieren Benutzer als **Light** oder **Full** Benutzer angelegt werden sollen.

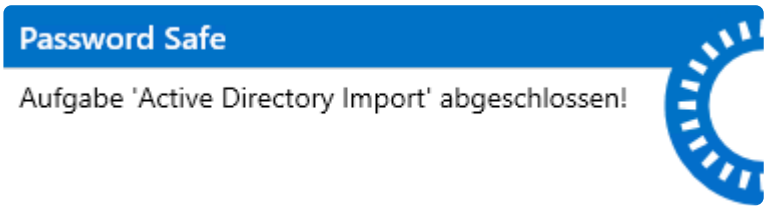
> Lassen sich einzelne Benutzer nicht zum Import markieren, wurden sie bereits über ein Ende-zu-Ende-verschlüsseltes Profil importiert.

Zusammenfassung

Hier sehen Sie, welche Objekte in welcher Form bearbeitet werden. 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 durch den Server im Hintergrund durchgeführt. Die einzelnen Elemente tauchen daher nach und nach in der Liste auf. Je nach Menge der importierenden Daten kann dies längere Zeit in Anspruch nehmen. Wurde der Import beendet, wird ein entsprechender Hinweis angezeigt.



Importierte Benutzer und Organisationseinheiten

Die im Masterkey-Modus importierten Benutzer und Organisationseinheiten können in Password Safe nicht bearbeitet werden. Änderungen müssen im AD vorgenommen und synchronisiert werden. **Somit ist das AD das führende System**. Zugehörigkeiten in Rollen werden synchronisiert und müssen im AD gesetzt werden. Die User können aber in Organisationseinheiten oder Rollen, die in direkt in Password Safe angelegt wurden, aufgenommen werden.

Rechte

Beim Import bzw. der Synchronisation werden die Rechte wie folgt vergeben.

Neue Objekte

	Benutzer	Gruppen	Rollen

Werden Rechte von der OU vererbt?	Wenn kein Preset hinterlegt ist	Wenn kein Preset hinterlegt ist	Nein
Werden Rechte aus einem Preset angewandt?	Wenn Preset hinterlegt ist	Wenn Preset hinterlegt ist	Nein
Wird das “Hinzufügen” Recht vergeben?	Nein	Ja	Nein
Wer bekommt den Rechte Schlüssel?	Importierter Benutzer und alle mit “Berechtigen” Recht	Alle	Alle mit “Berechtigen” Recht

Geänderte Objekte

	Benutzer	Gruppen	Rollen
Werden Rechte von der OU vererbt?	Wenn kein Preset hinterlegt ist	Nein	Nein
Werden Rechte aus einem Preset angewandt?	Wenn Preset hinterlegt ist	Nein	Nein
Wird das “Hinzufügen”-Recht vergeben?	Nein	Nein	Nein
Wer bekommt den Rechte-Schlüssel?	Alle mit “Berechtigen”-Recht	Keine	Alle mit “Berechtigen”-Recht

Wenn Sie einen Benutzer importieren, wird er in die Rollen aus dem AD aufgenommen. Voraussetzung ist dabei, dass diese Rollen in Password Safe bereits existieren oder mit importiert werden.

Anmeldung an Password Safe

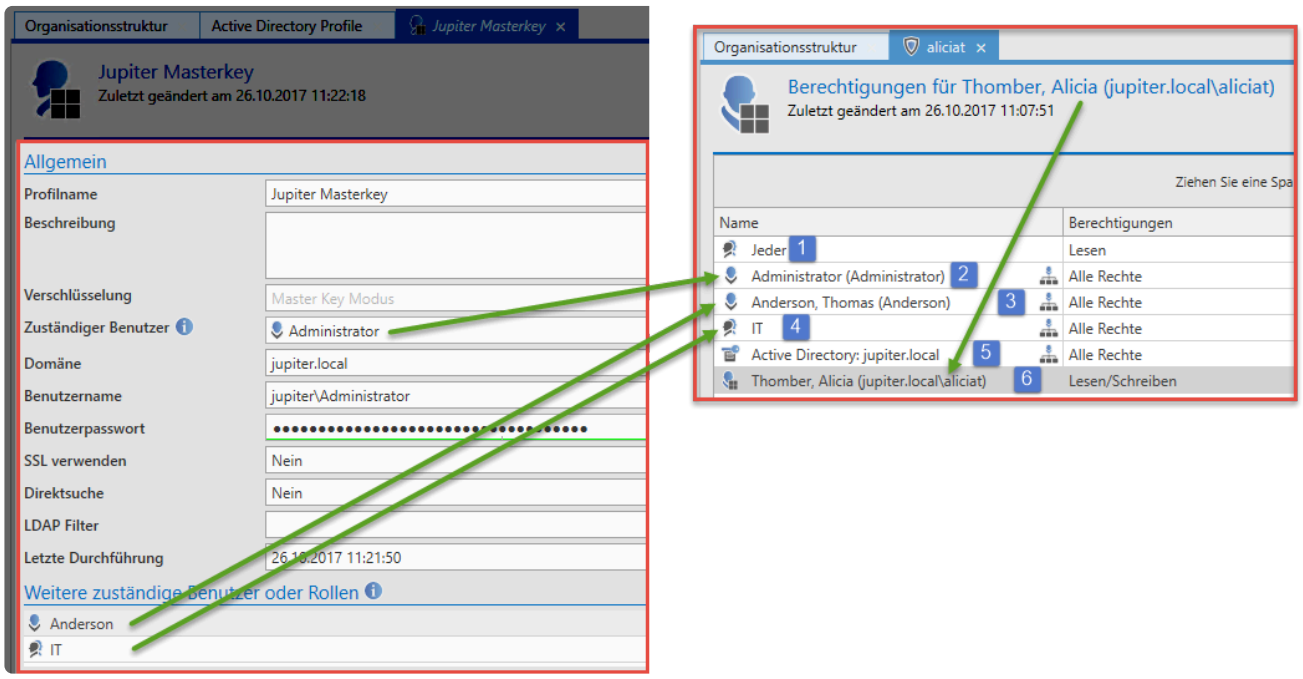
Benutzer, die Sie in diesem Modus importieren, können sich mit dem Domänenkennwort anmelden. Bei der Anmeldung muss keine Domäne angegeben werden. Die Anmeldung kann zusätzlich durch die **Multi-Faktor-Authentifizierung** ergänzt werden.

Die Anmeldung mittels Kerberos funktioniert „automatisch“. Solang der entsprechende Kerberos-Server erreichbar ist, authentifizieren sich die Benutzer in der Domäne mittels Kerberos unter Verwendung seines Domänenkennwortes. Sollte die Anmeldung via Kerberos – z.B. aufgrund fehlerhafter Konfiguration des Domain Controllers – nicht funktionieren, wird die Anmeldung über das NTLM Protokoll versucht. Dies sind jedoch alles Einstellungen, die auf dem Domain Controller vorgenommen werden müssen und haben nichts mit Password Safe zu tun.

> ! Die Anmeldung an Password Safe mittels SSO über Kerberos ist aktuell nicht möglich.

Berechtigungen auf importierte Objekte

Folgendes Beispiel veranschaulicht die Rechte, die auf die importierten Benutzer vergeben werden:



1. Im Masterkey-Modus wird immer **Jeder** auf den Benutzer **lesend** berechtigt.
2. Der *zuständige Benutzer" wird mit allen Rechten und dem Schlüssel berechtigt. Hierdurch ist gewährleistet, dass er den Benutzer zukünftig auch synchronisieren bzw. ändern kann.
3. Die **weiteren zuständigen Benutzer** werden wie der **zuständige Benutzer** berechtigt.
4. Der **Masterkey** des **Active Directory** Profils wird ebenfalls mit allen Rechten und Schlüsseln berechtigt, da hierüber synchronisiert wird.
5. Schlussendlich wird der Benutzer auf sich selbst berechtigt.

> ✻ Alle Benutzer und Rollen, die mit **Berechtigen** auf das importierte Objekt berechtigt werden, erhalten auch dessen Rechteschlüssel.

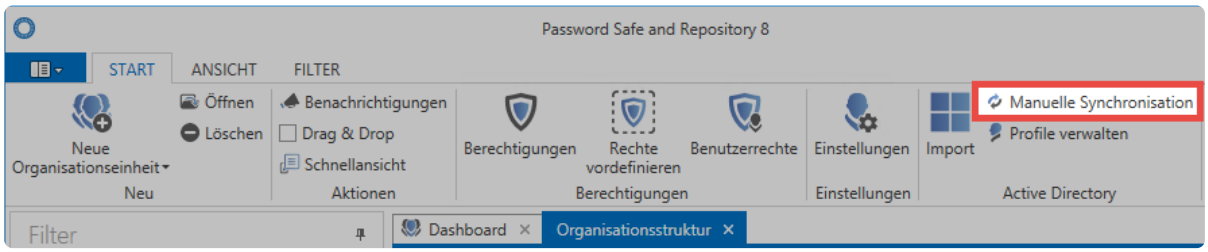
Synchronisation

Bei einer Synchronisation werden alle relevanten Informationen der Benutzer, Organisationseinheiten und Rollen (Namen, E-Mail, usw.) aktualisiert. Geänderte Zugehörigkeiten zu Rollen werden angepasst. Ebenso werden Benutzer entsprechend den Einstellungen im AD aktiviert bzw. deaktiviert. Wechseln Sie die Zugehörigkeit von Organisationseinheiten wechseln mittels **Drag & Drop**. Neue Benutzer und entsprechend definierte Rollen werden importiert.

Haben Sie beim Import eines Benutzers den Haken in der Spalte **Synchronisation** nicht gesetzt, finden keine Änderungen statt.

Manuelle Synchronisation

Über die entsprechende Schaltfläche in der Ribbon können Sie die Synchronisation manuell starten.



Anschließend wählen Sie das gewünschte Profil aus und starten die Synchronisation. Wie auch der initiale Import läuft die Synchronisation im Hintergrund. Wurde die Synchronisation beendet, wird ein entsprechender Hinweis angezeigt.

Synchronisation über System Tasks

Die Synchronisation kann mittels **System Tasks** automatisiert werden.

Löschen bzw. Entfernen von Benutzern

Wird ein Benutzer im Active Directory entfernt, so wird er in Password Safe beim nächsten Sync ebenfalls gelöscht. Voraussetzung hierfür ist, dass der Benutzer als **synchronisationsfähig** importiert wurde.

Wollen Sie den Benutzer nur aus Password Safe, aber nicht aus dem AD löschen, so müssen Sie ihn aus der Datenbank heraus synchronisieren. Rufen Sie hierfür über **Import** den Assistenten auf. Im ersten Schritt wählen Sie eine Organisationseinheit aus. Diese hat beim reinen Löschen keine Auswirkung. Im zweiten Schritt suchen Sie dann den Benutzer, um beide Haken zu entfernen.

Nach dem Prüfen der Zusammenfassung schließen Sie den Vorgang ab. Der Benutzer wird aus der Datenbank synchronisiert.

RADIUS-Authentifizierung

Was ist die RADIUS-Authentifizierung

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das der Authentifizierung von Benutzern dient. Password Safe kann an einen RADIUS-Servers angebunden werden um beispielsweise die Multi-Faktor-Authentifizierung zu nutzen. Aber auch alle weiteren RADIUS-typischen Funktionen können verwendet werden. Weitere Informationen finden Sie beispielsweise bei **Wikipedia**.

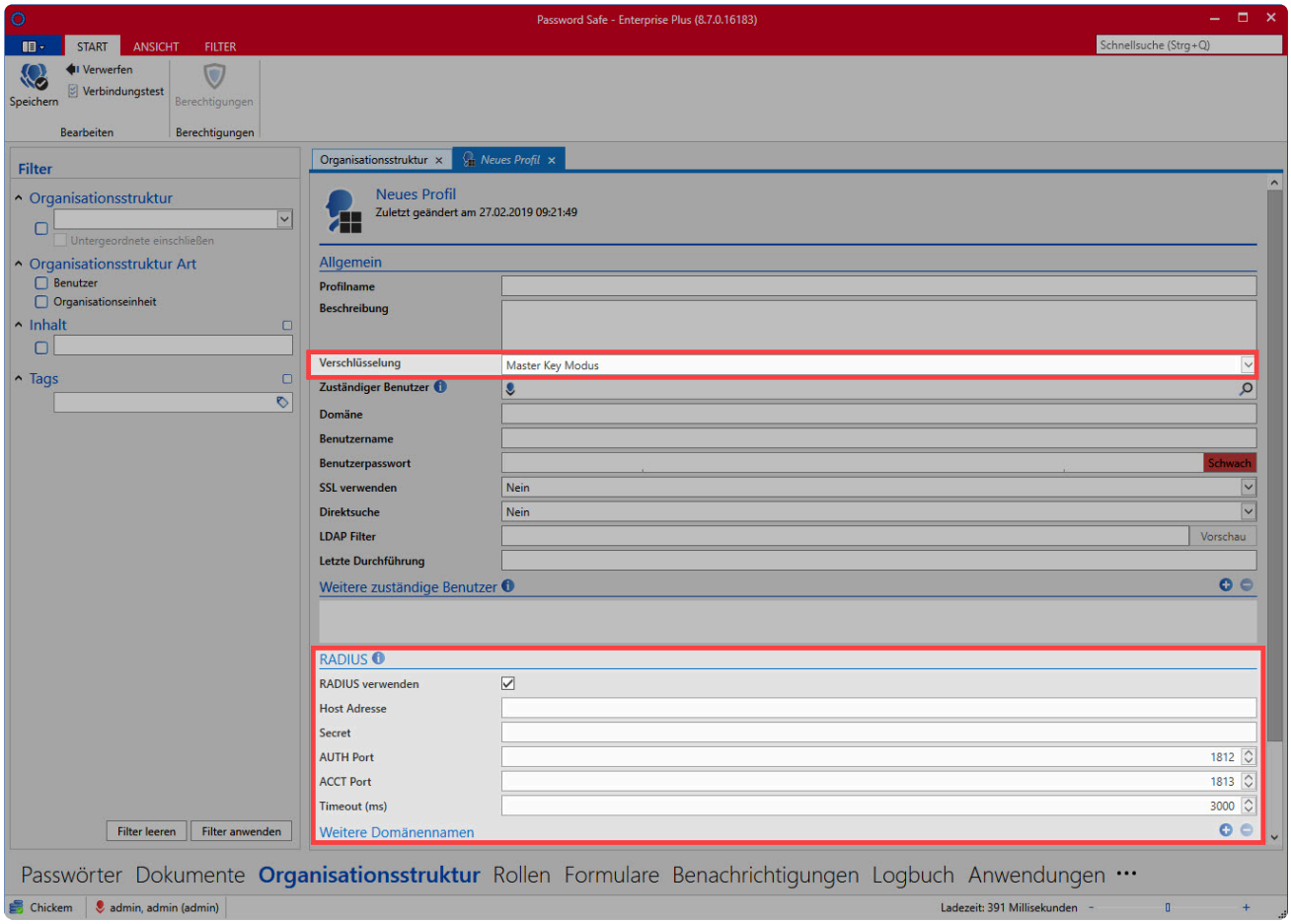
Voraussetzungen

Damit Password Safe einen RADIUS-Server ansprechen kann, müssen folgende Voraussetzungen gegeben sein:

- Ein RADIUS-Server muss bereitstehen und über das Netzwerk erreichbar sein.
- Es muss am RADIUS-Server ein Zugang für den Password Safe AdminClient eingerichtet sein.
- Für den Zugang muss ein entsprechendes Secret konfiguriert sein.
- In Password Safe müssen Benutzer im Masterkey-Modus aus dem AD importiert worden sein.

Konfiguration

Die eigentliche Anbindung des RADIUS-Servers ist sehr einfach:



- **RADIUS verwenden** Zunächst aktivieren Sie die Verwendung.
- **Host Adresse** Hier hinterlegen Sie die Adresse unter der Ihr RADIUS Server erreichbar ist.
- **Secret** Verweist auf das Secret, das für den Password Safe AdminClient hinterlegt wurde.
- **AUTH Port** Hier geben Sie den sogenannte AUTH Port des RADIUS-Servers an.
- **ACCT Port** Hier können Sie – bei Bedarf – den ACCT Port des RADIUS-Servers hinterlegen.
- **Timeout** Geben Sie hier an, wie viel Zeit der RADIUS-Server zum Reagieren hat.

! Stellen Sie bei der Radius Anbindung sicher, dass auch die Authentifizierung gegenüber dem Active Directory über Radius abgewickelt wird. Password Safe kann diesem Fall nicht selbst gegenüber dem AD authentifizieren.

Azure AD Anbindung

Warum Azure AD?

Immer mehr Unternehmen setzen auf Cloud-Dienste. Dabei wird auch die Verwaltung der Benutzer ausgelagert. Anstatt eines konventionellen Active Directory via LDAP wird immer häufiger ein Azure AD verwendet. Hierfür bietet Password Safe die Möglichkeit, Benutzer und Rollen aus Azure zu übernehmen. Um Benutzer und Rollen aus mehreren Azure ADs anzubinden, können mehrere Profile angelegt werden.

Unterschiede zur LDAP-Anbindung

Die Anbindung zum Azure AD unterscheidet sich in einem speziellen Punkt von der Anbindung an konventionelles Active Directory. Während sich beim konventionellen AD Password Safe aktiv die Informationen über Benutzer, Gruppen und Rollen abfragt, überträgt das Azure AD diese automatisch an den Password Safe Server. Hierfür wird ein so genannter SCIM-Service verwendet.

Um sich an Password Safe anzumelden, öffnet sich nach der Eingabe des Benutzernamens ein Popup für die Anmeldung mit dem angegebenen Microsoft-Konto. Hier wird auch ein gegebenenfalls konfigurierter zweiter Faktor abgefragt. Die Anmeldung wird über das Open ID Connect-Protokoll durchgeführt.

Azure AD Anbindung

Im Folgenden finden Sie eine Anleitung, wie Azure AD an Password Safe angebunden werden kann. Besuchen Sie im Azure-Portal die Verwaltung Ihres Azure Active Directory. Verwenden Sie hierfür ein Konto mit administrativen Berechtigungen. Melden Sie sich parallel in Password Safe mit einem Konto an, dessen Benutzerrechte “Organisationsstruktur Modul anzeigen”, “Kann Azure AD Profile verwalten” sowie “Kann neue Azure AD Profile anlegen“ aktiv sind.

Vorbereitungen im Azure-Portal

1. Notieren Sie sich die “Mandanten-ID” des Azure AD – diese benötigen Sie später zur Konfiguration innerhalb von Password Safe
2. Navigieren Sie in Ihrem Azure AD zu den “Unternehmensanwendungen”
3. Fügen Sie eine neue eigene Anwendung hinzu, die nicht in der Azure Gallery zu finden ist – in unserem Beispiel nennen wir sie “MATESO Password Safe”
   Anmerkung: Ein wesentliches Feature von Password Safe ist, dass es bei unseren Kunden selbst gehostet ist. Um in der Azure Gallery gelistet zu werden, wird jedoch ein SaaS Modell vorausgesetzt. Deshalb ist Password Safe nicht in der Azure Gallery verfügbar.
4. Sobald die Anwendung erfolgreich erstellt wurde, werden Sie automatisch zu dieser weitergeleitet
5. Notieren Sie sich die “Anwendungs-ID” – auch diese wird gleich benötigt
6. Klicken Sie in der Navigation auf “Benutzer und Gruppen”
7. Fügen Sie die Benutzer und Gruppen hinzu, die in Password Safe verfügbar sein sollen
8. Navigieren Sie zu dem Punkt “Bereitstellung”
9. Stellen Sie den Bereitstellungsmodus auf “Automatisch”

10. Lassen Sie das Browser-Tab geöffnet und wechseln Sie zu Password Safe

> ! Der Import einer Azure-Gruppe als Password Safe Rolle ist nur möglich, wenn Sie das Azure-Paket **Azure AD Premium P2** gebucht haben!

Erstellen eines Azure AD-Profils in Password Safe

1. Navigieren Sie in das Modul “Organisationsstruktur” oder “Rollen”
2. Klicken Sie in der Toolbar auf “Profile verwalten” in der Kategorie “Azure AD“
3. Legen Sie ein Profil mit den gewünschten Informationen an
4. Fügen Sie die Mandanten-ID und Anwendungs-ID an, die in Azure angezeigt wurden
5. Sobald das Profil gespeichert wurde, öffnet sich ein Popup zur Generierung eines Tokens
6. Wählen Sie ein gewünschtes Ablaufdatum (max. 10 Jahre) und klicken Sie auf “Token generieren”
7. Notieren Sie die Werte der Felder “Mandanten-URL” und “Geheimes Token”
8. Wechseln Sie zurück zum Azure-Portal

Konfiguration der Bereitstellung

1. Füllen Sie die Felder “Mandanten-URL” und “Geheimes Token” mit den Informationen aus Password Safe
2. Klicken Sie auf “Verbindung testen”
3. Wenn der Test erfolgreich abgeschlossen wurde, klicken Sie oben auf “Speichern”
4. Zurück auf der “Bereitstellung”-Seite klicken Sie auf “Bereitstellung starten”
5. Prüfen Sie in den Einstellungen der Bereitstellung, ob der “Bereitstellungsstatus” auf “Ein” konfiguriert ist
6. Alle zugeordneten Benutzer und Gruppen werden nun in Password Safe angelegt

> * Der Standard-Bereitstellungsintervall beträgt 40 Minuten. Es kann also etwas dauern, bis die Benutzer und Rollen in Password Safe erscheinen.

> ! Beachten Sie, dass Azure die Verbindung zu Password Safe herstellt. Hierfür muss die Mandanten-URL von einem externen Netzwerk erreichbar sein und ein ggf. verwendetes SSL-Zertifikat gültig sein!
> Falls die Benutzer in Password Safe nicht angelegt werden, finden Sie weitere Informationen im **Bereitstellungsprotokoll** der Azure Unternehmensanwendung.

Konfiguration des Logins

1. Damit sich die Azure-Benutzer in Password Safe anmelden können, sind ein paar weitere Konfigurationen notwendig.
2. Navigieren Sie in Azure auf die Übersichtsseite Ihres Azure ADs
3. Navigieren Sie weiter zu “App-Registrierungen”
4. Falls keine Anwendung angezeigt wird, klicken Sie den Button “Alle Anwendungen anzeigen”
5. Klicken Sie auf “MATESO Password Safe” und navigieren Sie dann zu “Authentifizierung“
6. Klicken Sie hier auf “Plattform hinzufügen”, wählen Sie “Mobilgerät- und Desktopanwendungen“

und konfigurieren Sie die benötigten URLs

Für welchen Client?	Welche URL ist benötigt?
WebClient	**Benutzerdefinierte URL:** https://WEBCLIENT_URL/authentication/login-via-oidc
FullClient & SSO Agent	https://login.microsoftonline.com/common/oauth2/nativeclient
iOS & Android	**Benutzerdefinierte URL:** psrmobile://auth
Google Chrome Extension	**Benutzerdefinierte URL:** https://bpjfchmapbmjeklgmlkabfepflgfckip.chromiumapp.org
Microsoft Edge Extension	**Benutzerdefinierte URL:** https://ahdfobpkkckhdhbmnpjehdkepaddfhek.chromiumapp.org
Firefox Extension	**Benutzerdefinierte URL:** https://28c91153e2d5b36394cfb1543c897e447d0f1017.extensions.allizom.org/

! Damit Ihre Nutzer sich am FullClient am Desktop mit den importierten Usern anmelden können, muss zusätzlich auf jedem Endgerät WebView2 von Microsoft installiert werden. Dies wird benötigt um allgemein Websiten (Azure-Loginseite) im FullClient anzeigen zu können.

API-Berechtigungen setzen

Zuletzt müssen noch die API-Berechtigungen für die Azure-API gesetzt werden, damit die Anmeldung an Password Safe vollständig durchgeführt werden kann.

1. Navigieren Sie zu “API-Berechtigungen“ und klicken Sie “Berechtigung hinzufügen”
2. Wählen Sie “Microsoft Graph” und dann “Delegierte Berechtigungen”
3. Setzen Sie unter “OpenId-Berechtigungen“ die Haken bei “openid” und “profile”
4. Klicken Sie auf “Berechtigungen hinzufügen”
5. Klicken Sie auf “Administratorzustimmung für ‘IHR_AD_NAME’ erteilen”

Häufig gestellte Fragen

Ist eine Migration von LDAP zu Azure AD möglich?

Eine automatische Migration von LDAP-Benutzern (sowohl E2E als auch Master Key) zu Azure AD-Benutzern ist zum aktuellen Zeitpunkt **nicht möglich**!

Welcher Port wird für den SCIM-Endpunkt für die Bereitstellung von Benutzern/ Gruppen von Azure AD zu Password Safe Application Server verwendet?

11015 ist der Port, der für die Kommunikation von Azure AD zu Password Safe verwendet wird.

Unterstützt die Password Safe Azure AD Anbindung verschachtelte Gruppen?

Aufgrund technischer Einschränkungen von Azure unterstützt Password Safe keine verschachtelten Gruppen.

Funktioniert Azure AD auf Servern, die nur intern erreichbar sind?

Auf Servern, auf die von extern nicht zugegriffen werden kann, ist eine Integration von Azure AD ebenfalls möglich. Verwenden Sie hierfür den Bereitstellungs-Agent. Dieser kann auf allen oder nur auf einem Anwendungsserver installiert werden. Dabei muss beachtet werden, dass die IP oder der DNS-Name der in der später erstellten Unternehmensanwendung angegebenen “Mandanten-URL” in den alternativen Antragstellernamen im Serverzertifikat vorhanden ist.
Tipp: als “Mandanten-URL” kann auch “https://127.0.0.1:11015/scim” angegeben werden, dabei muss 127.0.0.1 wiederum in den alternativen Antragstellernamen im Serverzertifikat vorhanden sein.

1. Laden Sie den Provisioning Agent herunter von hier
2. Installieren Sie den Provisioning Agent auf dem Server mit dem Password Safe Server.
3. Starten Sie den “AAD Connect Provisioning Agent Wizard”.
4. Wählen Sie “On-premises application provisioning Azure AD to application”, klicken Sie auf “Next”.
5. Klicken Sie auf “Authenticate” und authentifizieren Sie sich mit einem Benutzer, der ein Hybrid-Administrator oder ein globaler Administrator sein sollte.
6. Klicken Sie auf “Bestätigen”.
7. Warten Sie, bis die Anwendung die Registrierung in Azure abgeschlossen hat.
8. Wechseln Sie zum Azure-Portal.
9. Klicken Sie auf “Azure Active Directory”.
10. Klicken Sie auf “Unternehmensanwendungen”.
11. Klicken Sie auf “Neue Anwendung”.
12. Suchen Sie nach “On-premises SCIM app”.
13. Klicken Sie auf “On-premises SCIM app”.
14. Passen Sie den Namen an.
15. Klicken Sie auf “Erstellen”.
16. Warten Sie, bis der Vorgang abgeschlossen ist.
17. Klicken Sie auf die erstellte Anwendung in der Übersicht der “Unternehmensanwendungen”.
18. Klicken Sie auf “Provisioning”.
19. Klicken Sie auf “Get started”.
20. Stellen Sie den Bereitstellungsmodus “Automatisch” ein.
21. Blenden Sie “On-Premises Connectivity” ein.
22. Weisen Sie den soeben installierten Agenten dieser Anwendung zu, indem Sie ihn auswählen und auf “Assign Agent(s)” klicken.
23. Es dauert circa 20 Minuten bis der Agent korrekt mit Ihrer Anwendung verbunden ist und Sie weitermachen können
24. Weiter mit “Provisioning configuration” auf dieser Hilfeseite oben

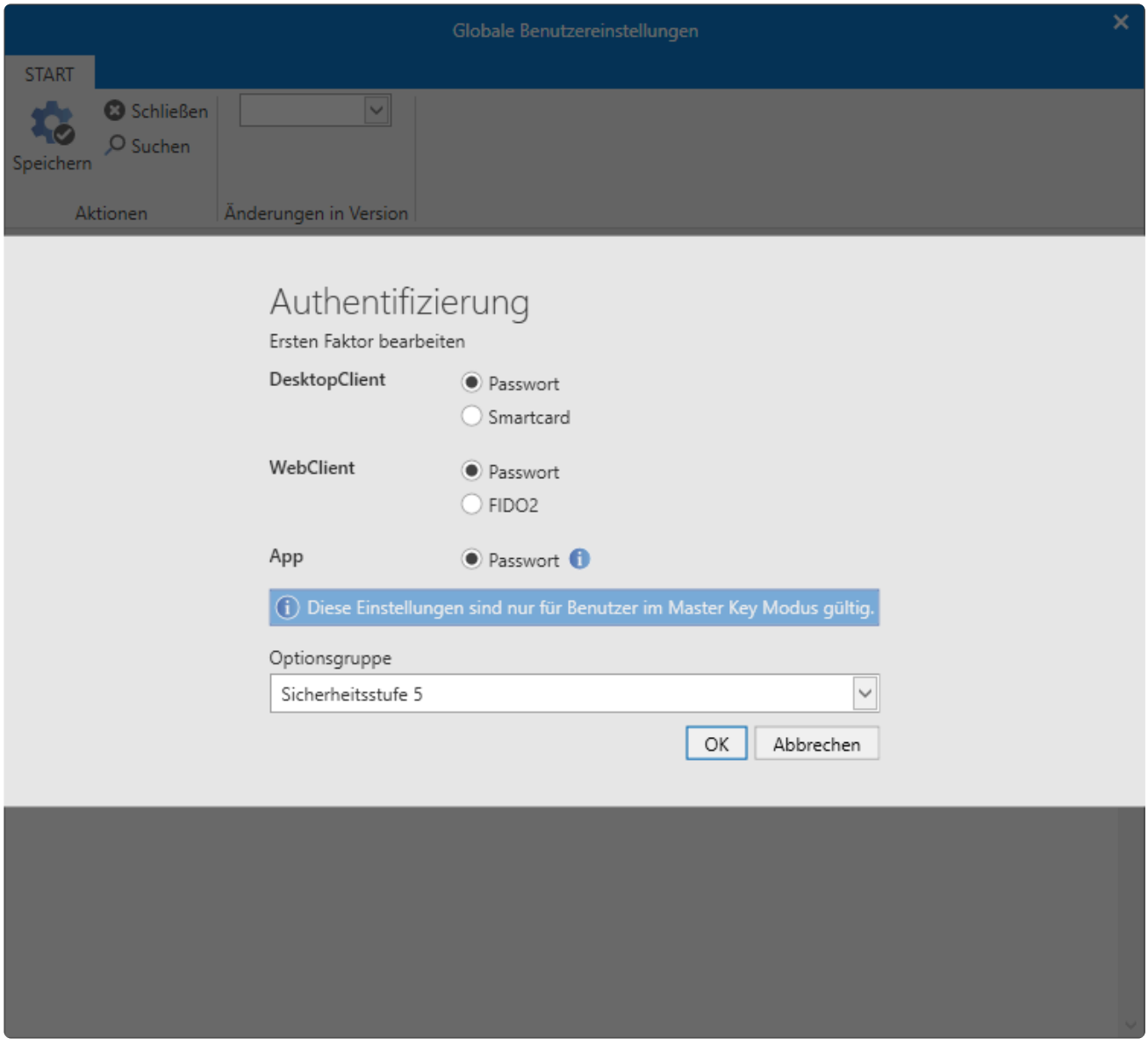
Erster Faktor

Was versteht man unter Erster Faktor?

Es handelt sich hier um einen Prozess, der den Zugriff auf unser System reguliert.

Voraussetzungen

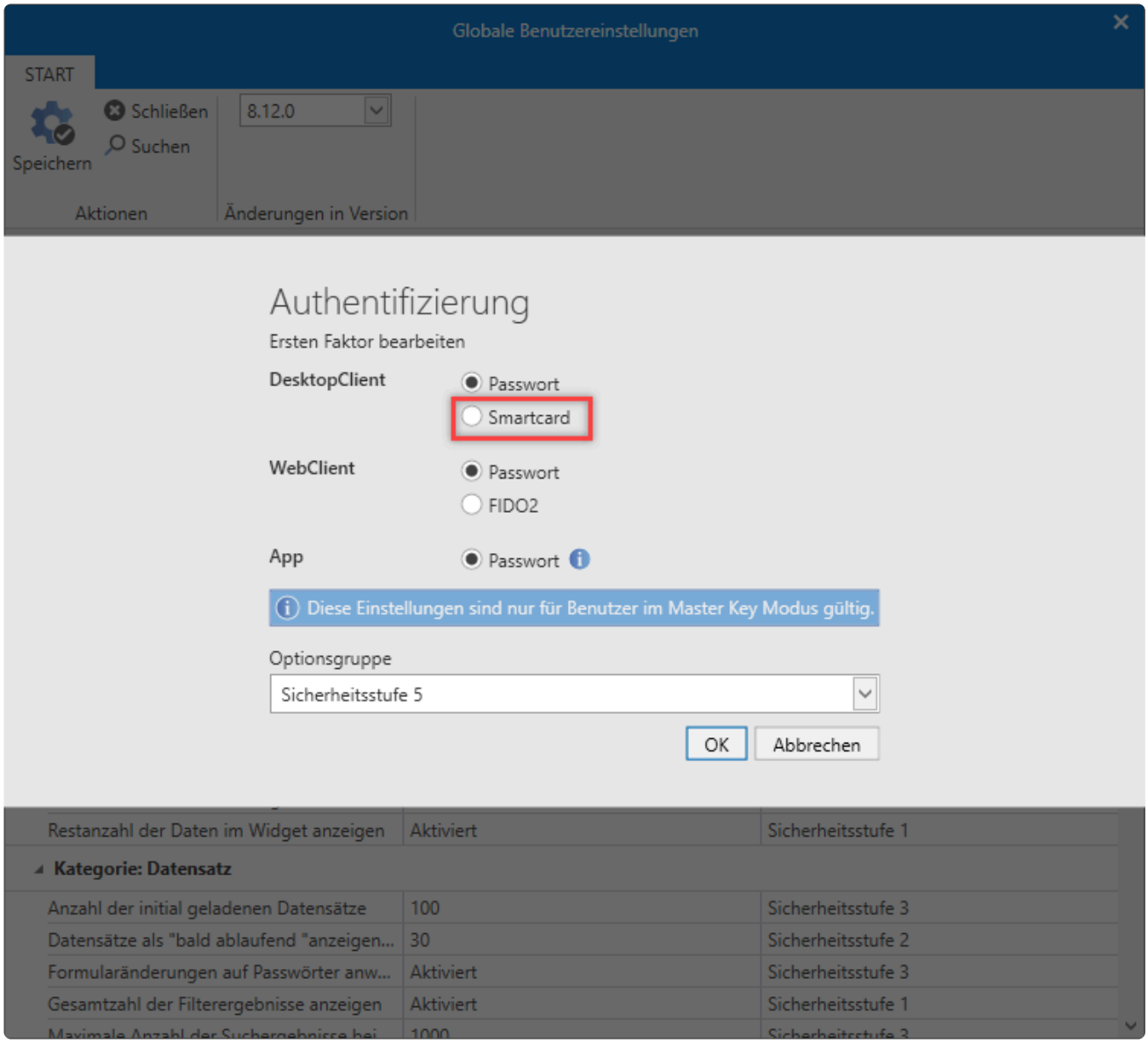
Mit der Benutzereinstellung **Ersten Faktor bearbeiten** haben Sie die Möglichkeit, einen anderen Faktor zu Authentifizierung, als das Standard-Passwort, zu definieren.



Faktoren

Smartcard (nur am FullClient)

Die Konfiguration erfolgt über die Benutzereinstellung **Ersten Faktor**.



Diese Option ist nur für Benutzer im Master Key Modus gültig

Die Smartcardanmeldung versucht anhand des Antragsteller im Smartcardzertifikat festzustellen, ob das Zertifikat zu dem anzumeldenden User gehört. Dies passiert mithilfe von Regex, die Standardregex “^{username}[.@\\\/-_:]({domain})$” oder “^({domain})[.@\\\/-_:]({username})$” wird dabei auf den Antragsteller angewendet. Dabei wird {username} mit dem anzumeldenden User und {domain} mit der im AD-Profil befindlichen Domain im Regex ersetzt und falls die Regexabfrage positiv ist, wird der User angemeldet. Falls das Format Ihres Antragstellers in Ihren Zertifikaten nicht mit diesen beiden Regexabfragen kompatibel ist, so müssen Sie im Admin-Client eine benutzerdefinierte Regexabfrage einstellen. Bitte beachten Sie dass “{username}” für Username und “{domain}” für die AD-Domain in der Regexabfrage vorhanden sein SOLLTE. Falls die Domain explizit angegeben werden muss, muss diese in Großbuchstaben geschrieben werden.

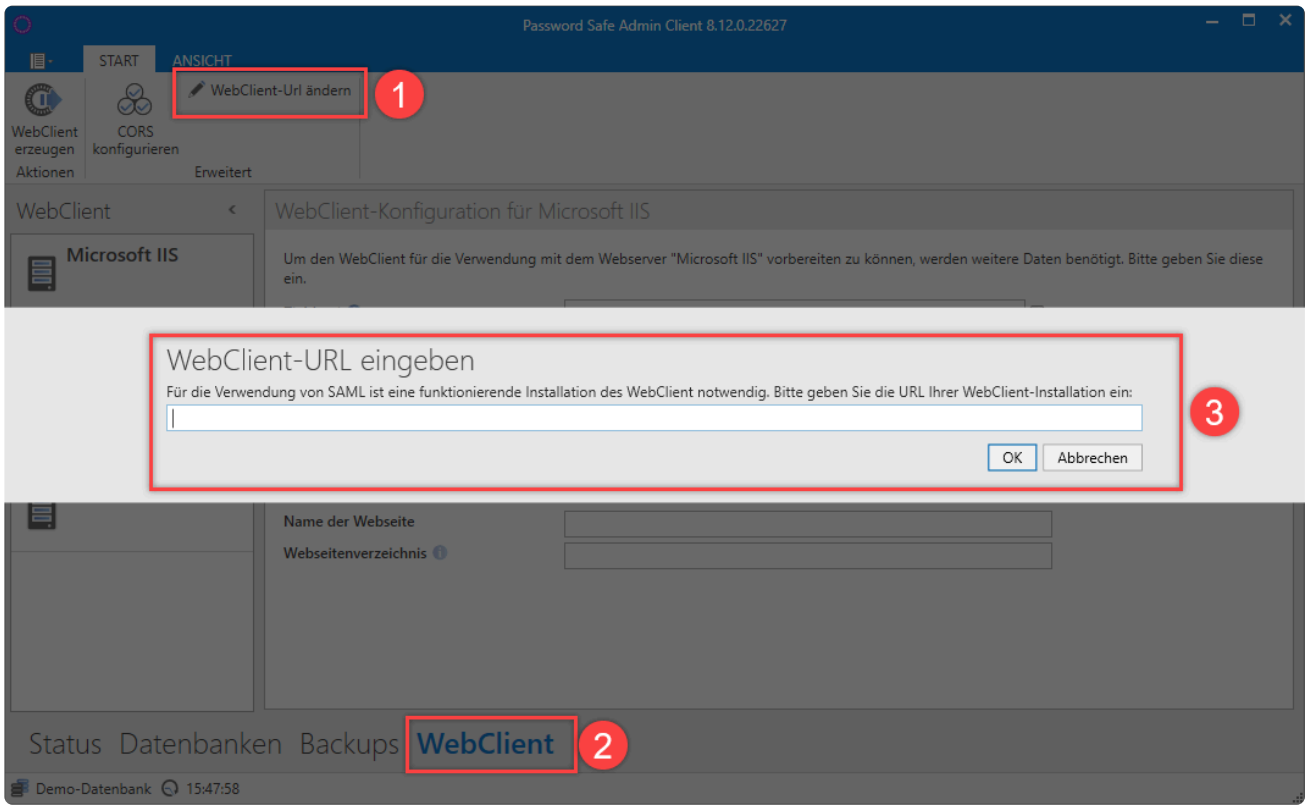
Zusätzlich muss das Smartcardzertifikat natürlich auch am Server gültig sein!

Fido2 (nur am WebClient)

Voraussetzung

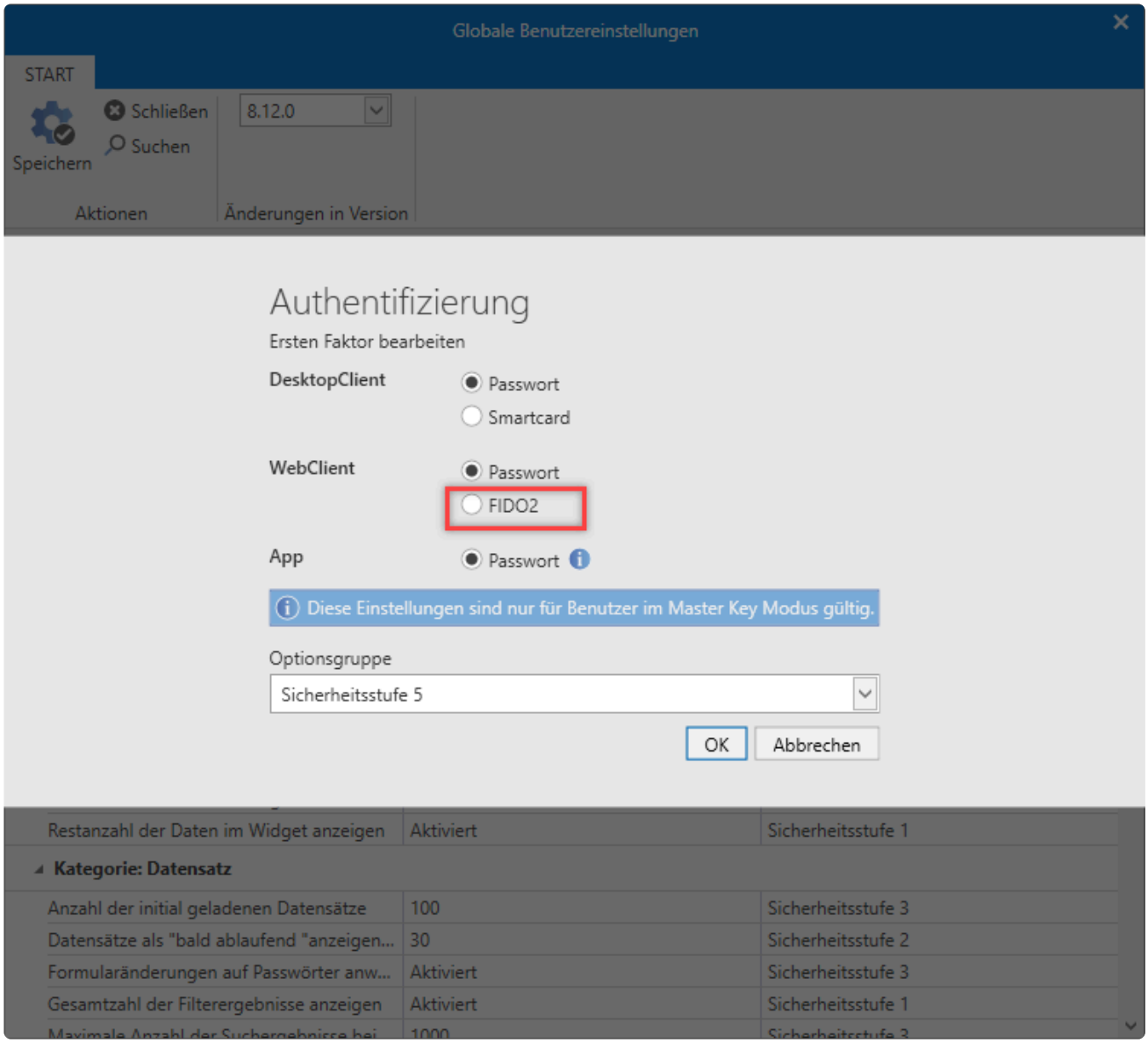
Für Fido2 muss zwingend SMTP konfiguriert sein. Zusätzlich muss bei den AD-Benutzern eine E-Mail-Adresse hinterlegt sein.

Zudem muss die URL des WebClients im Admin Client hinterlegt sein:

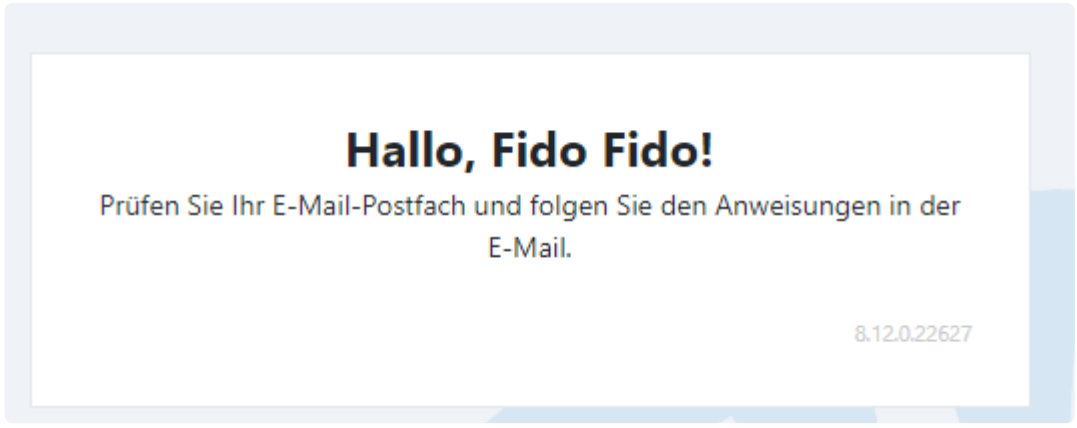


Konfiguration

Die Konfiguration erfolgt über die Benutzereinstellung **Ersten Faktor**.



Sobald sich dann ein AD-Benutzer am WebClient anmeldet, bekommt er folgende Aufforderung:



Im E-Mailfach des entsprechenden Benutzers erfolgt die weitere Konfiguration:

MATESO
PASSWORD SAFE
FIDO2-Zugang einrichten
Hallo Fido Fido,
mit dieser E-Mail erhalten Sie den Link zur Einrichtung Ihres FIDO2-Zugangs im Password Safe WebClient.
Um den Einrichtungsprozess des FIDO2-Zugangs zu starten, klicken Sie auf den folgenden Link:
FIDO2-Zugang einrichten
Dieser Link ist für 10 Minuten gültig.
Dies ist eine automatisch erstellte E-Mail. Bitte antworten Sie nicht auf diese E-Mail, da die Antwort nicht zugestellt werden kann.

Multifaktor-Authentifizierung

Was ist Multifaktor-Authentifizierung?

Über die Multifaktor-Authentifizierung wird die Anmeldung an Password Safe durch einen weiteren Faktor abgesichert.

Voraussetzungen

Um die Multifaktor-Authentifizierung nutzen zu können, müssen Sie diese zuvor im AdminClient aktivieren. Die eigentliche Einrichtung kann durch den Administrator oder den Benutzer selbst erfolgen.

> ✻ Ein **“vorkonfigurieren”** der Multifaktor-Authentifizierung für andere Benutzer durch den Administrator ist nicht möglich. Der Administrator gibt am AdminClient die zu benutzenden Multifaktor-Authentifizierungen vor. Mit aktivierter Benutzereinstellung **Benötigt zweiten Faktor** muss der Benutzer, bei der nächsten Anmeldung, eine der vordefinierten Multifaktor-Authentifizierung einrichten

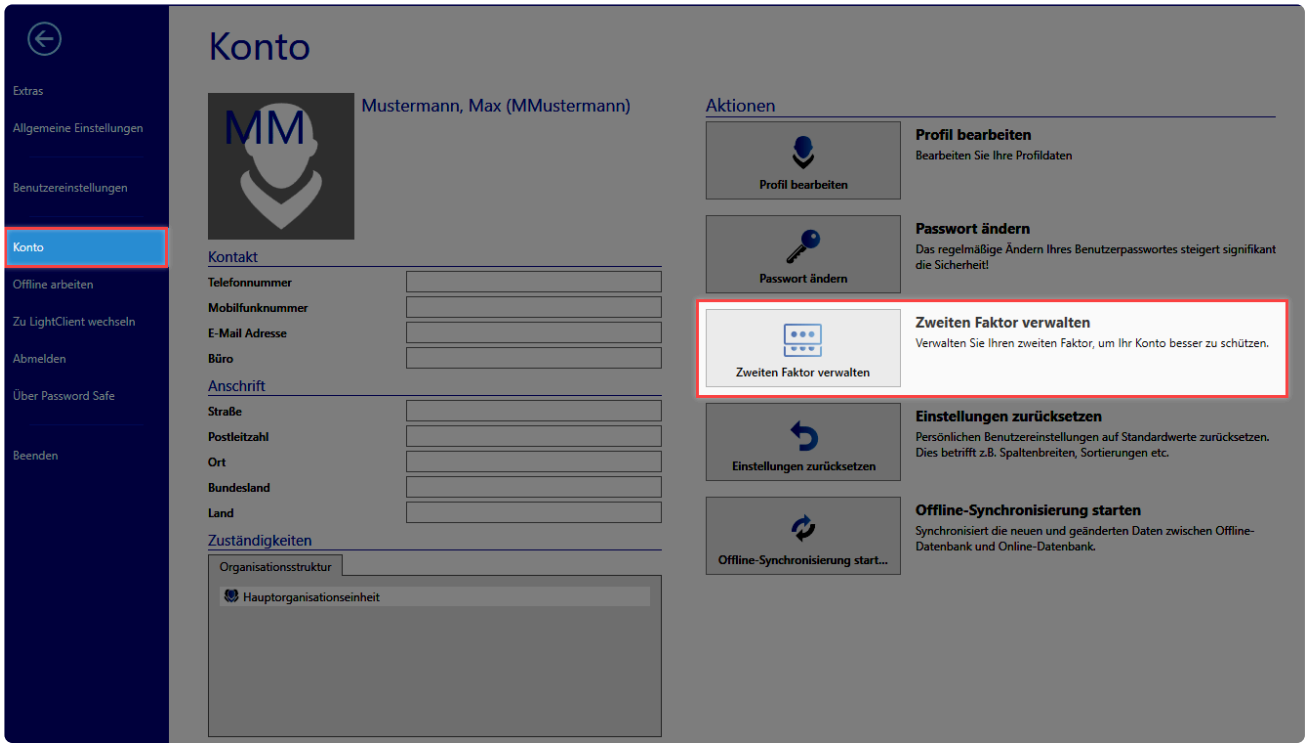
Konfiguration der Multifaktor-Authentifizierung

Für die Konfiguration der Multifaktor-Authentifizierung bleiben Ihnen zwei Möglichkeiten:

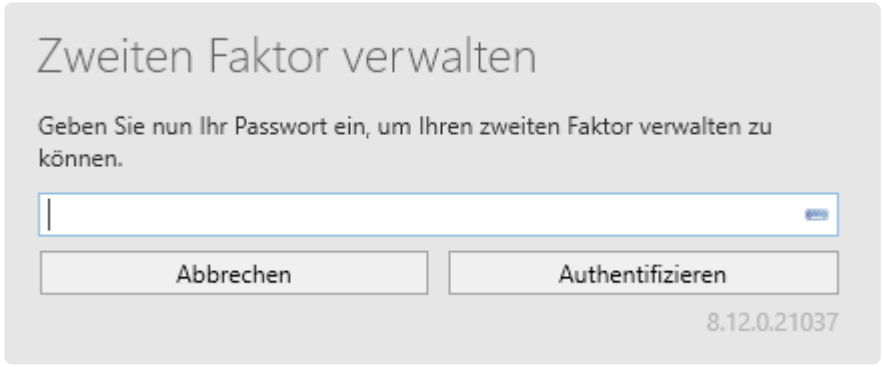
1. Multifaktor-Authentifizierung-Einrichtung vorgeben
Sie geben dem User vor eine Multifaktor-Authentifizierung zu nutzen, indem Sie entweder **global** oder dem **Benutzer** selbst die Benutzereinstellung **Benötigt zweiten Faktor** aktivieren.
Dadurch wird der User “gezwungen” bei der nächsten Anmeldung eine Multifaktor-Authentifizierung einzurichten.

2. selbstständige Einrichtung des Benutzers
Um eine Multifaktor-Authentifizierung einzurichten gehen Sie bitte wie folgt vor:

- Begeben Sie sich in das Hauptmenü -> Konto und klicken auf **Zweiten Faktor verwalten**



- Authentifizieren Sie sich um die Multifaktor-Authentifizierungen zu verwalten



- Konfigurieren Sie eine der vordefinierten Multifaktor-Authentifizierungen

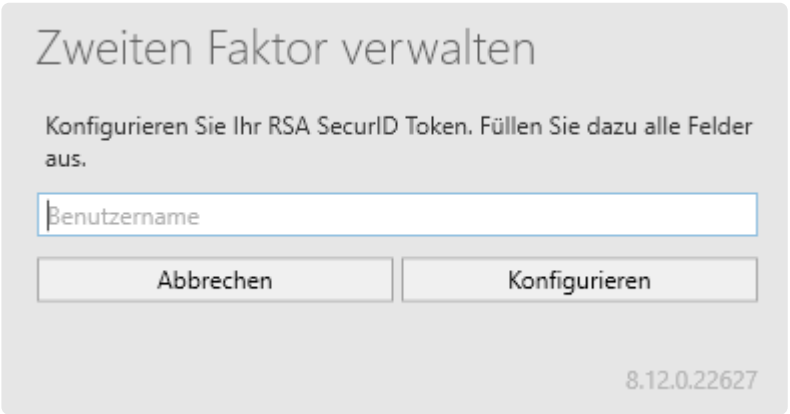
Authenticator App (TOTP)

Voraussetzung ist, dass die entsprechende App auf einem Smartphone gestartet ist. Sobald der Benutzer auf **Authenticator App (TOTP)** geklickt hat, wird ein QR-Code angezeigt, der mit der Authenticator App des Smartphones gescannt werden muss.

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

RSA SecurID Token

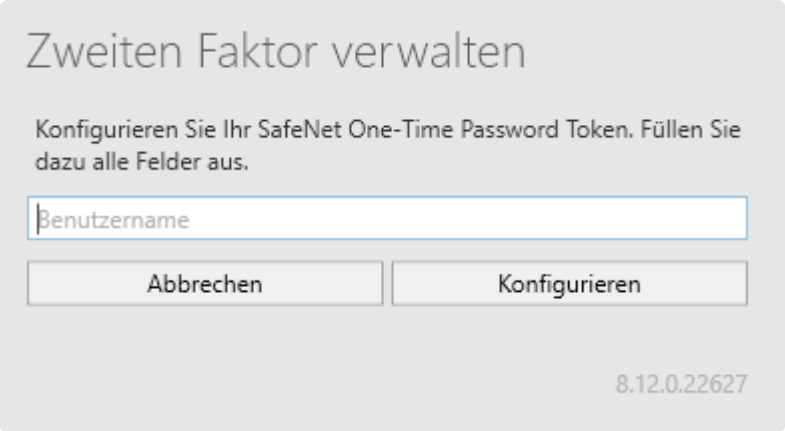
Um die Multifaktor-Authentifizierung mittels RSA SecurID anzulegen, gibt man den RSA Benutzernamen an und klickt direkt in der Ribbon auf **Konfigurieren**.



Voraussetzung für die Verwendung von RSA SecurID Token ist, dass am AdminClient in den 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 Sie am AdminClient in Datenbank Einstellungen die Zugangsdaten hinterlegen.

Public-Key-Infrastruktur

Für die Einrichtung von PKI suchen Sie über die **Lupe** nach dem infrage kommenden Zertifikat und wählen dieses dann aus.

Sollte Ihr Zertifikat nicht erkannt werden, deaktivieren Sie im AdminClient die Checkbox “Key-Encipherment” und versuchen es anschließend erneut.

Yubico One Time Password

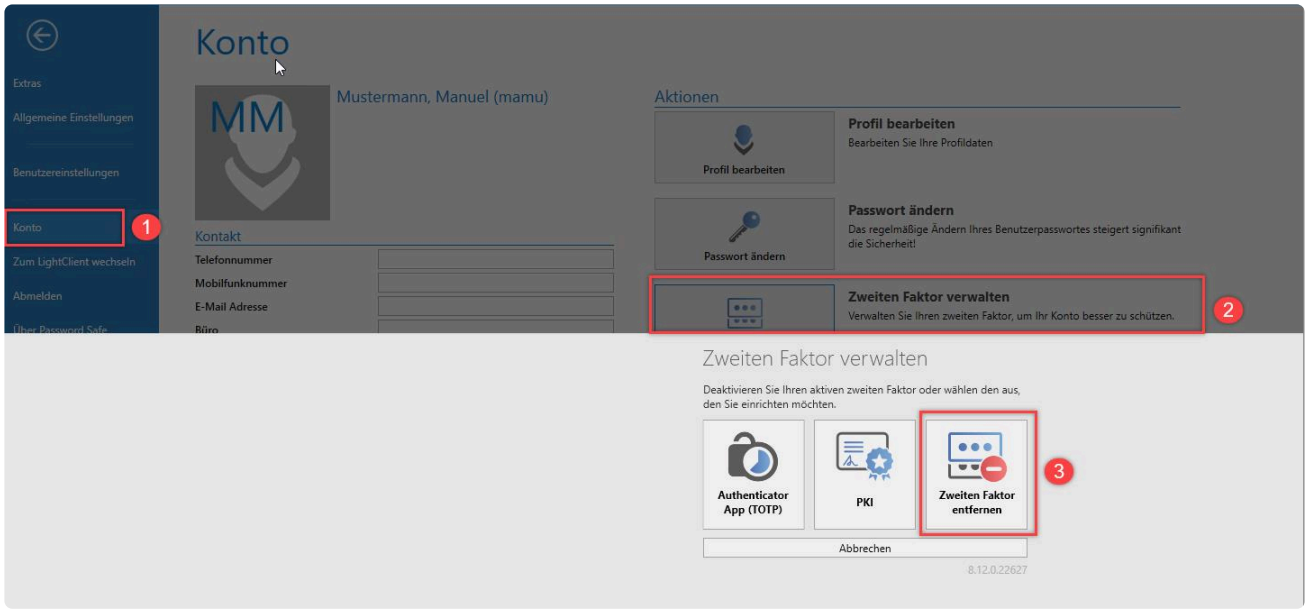
Die Konfiguration der Multifaktor-Authentifizierung mittels Yubico One Time Password wird in einem gesonderten Kapitel beschrieben.

Löschen der Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung kann durch den Benutzer selbst oder einen ausreichend berechtigten anderen Benutzer gelöscht werden.

Die Löschung durch den Benutzer selber erfolgt im Hauptmenü.

Unter **Konto** finden Sie den Punkt **Zweiten Faktor verwalten**. Nachdem Sie sich hier authentifiziert haben, besteht die Möglichkeit die Multifaktor-Authentifizierung zu ändern oder zu löschen.



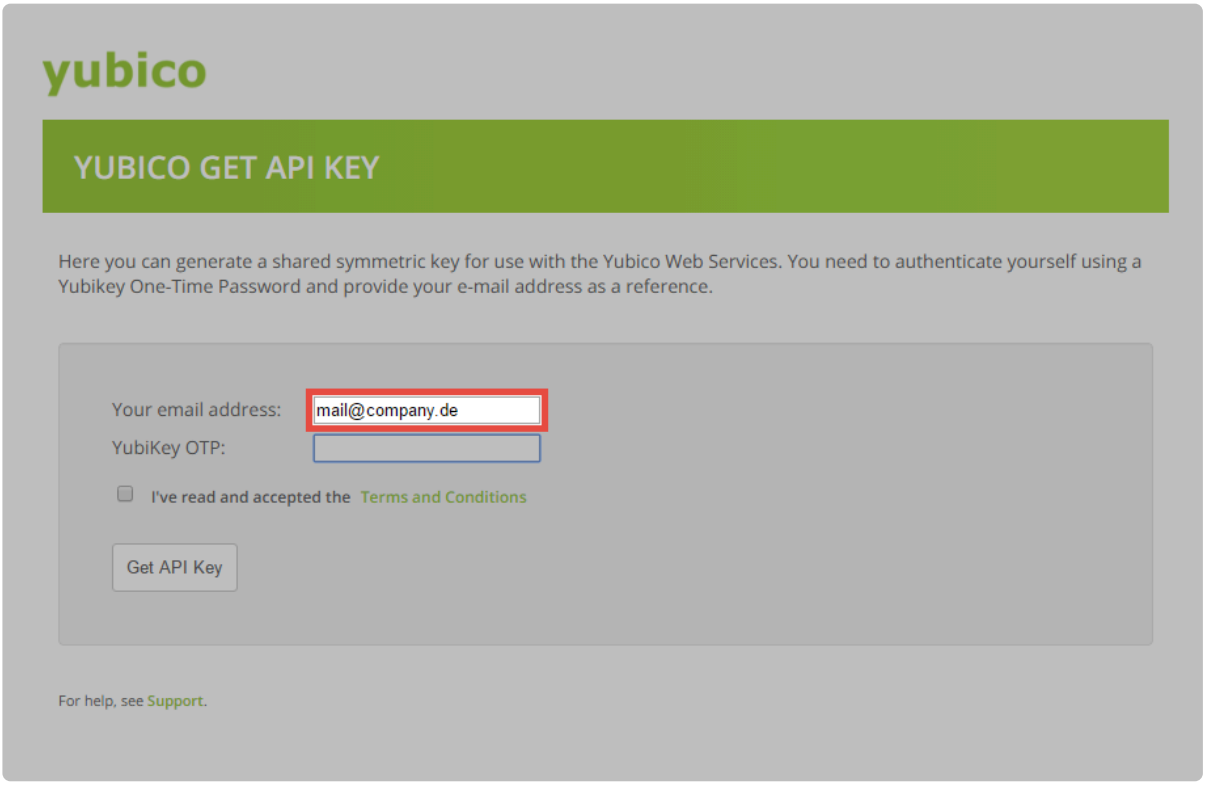
Damit ein anderer Benutzer die Löschung vornehmen kann, werden die Rechte **Lesen**, **Schreiben**, **Berechtigen** und **Löschen** benötigt.

Yubico / Yubikey

Einrichtung der Multifaktor-Authentifizierung

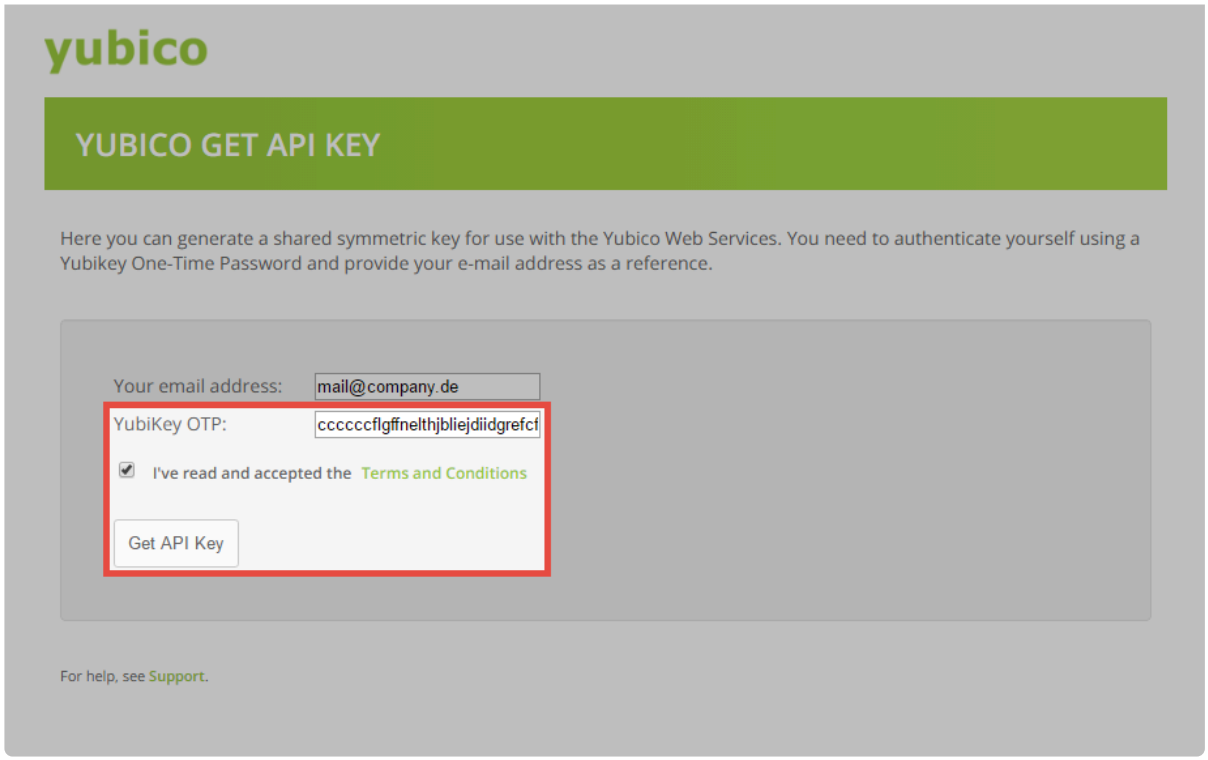
Anfordern des Yubico API Keys

Zur Konfiguration fordern Sie einen API Key an. Rufen Sie hierzu den folgenden Link auf und geben Sie eine E-Mailadresse an: https://upgrade.yubico.com/getapikey/

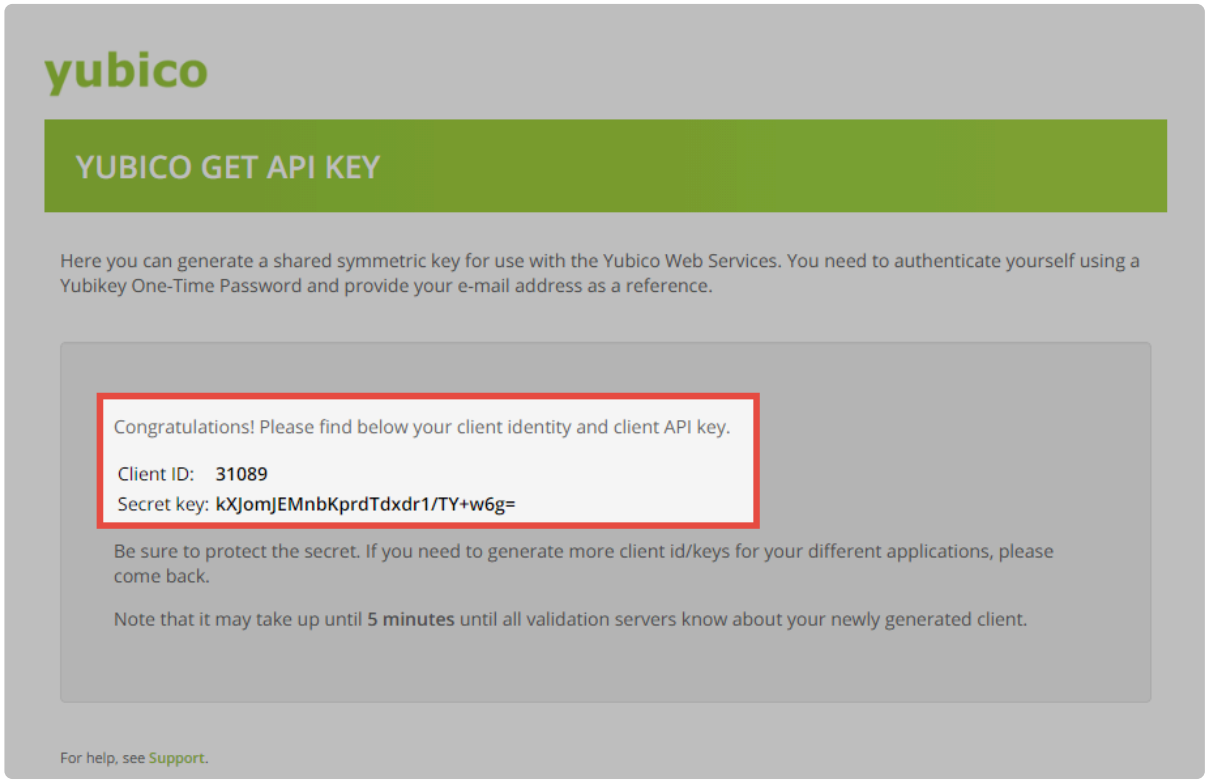


Erzeugen Sie anschließend über den Yubikey ein **One Time Password**.

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

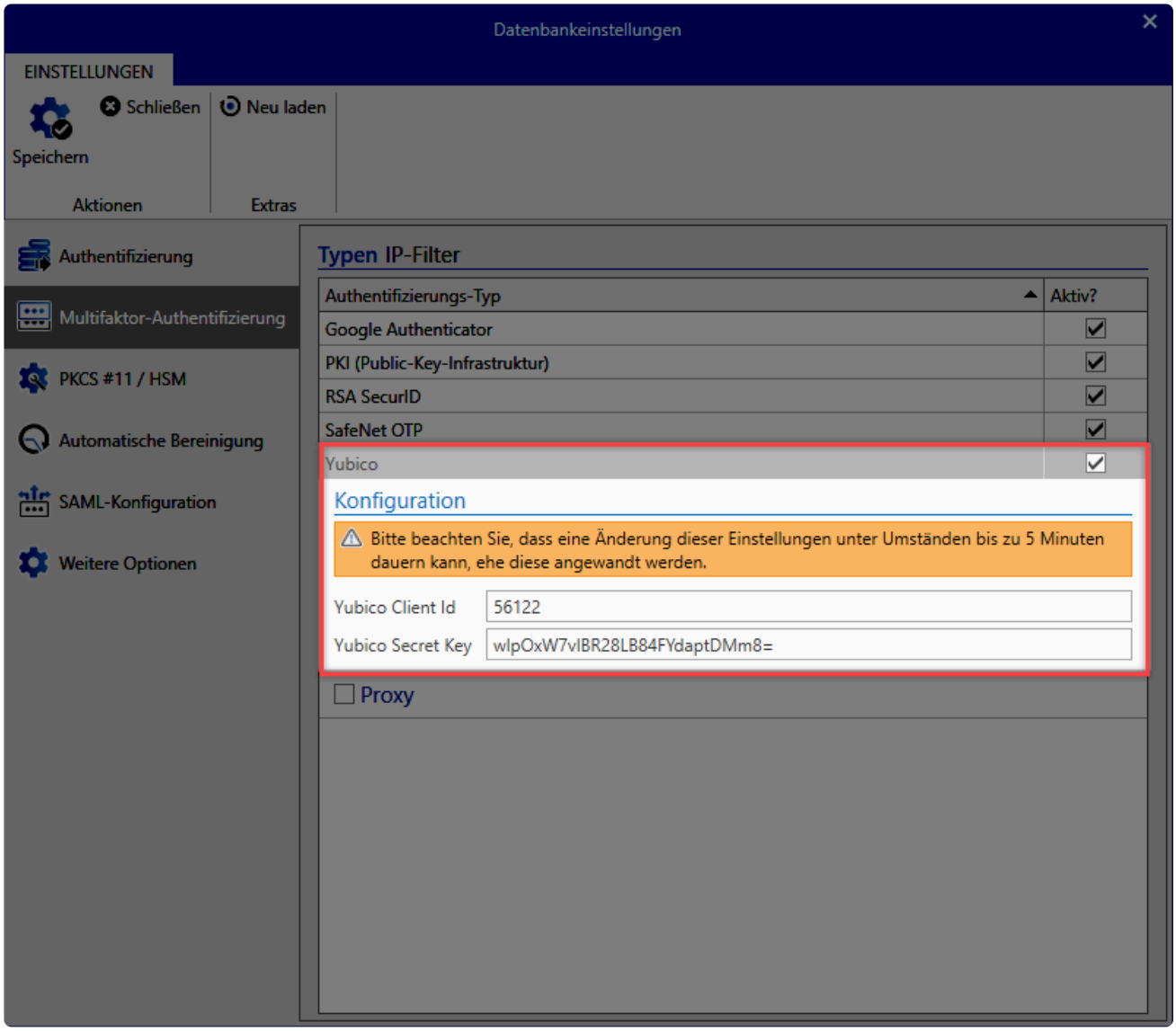


Nachdem Sie den allgemeinen Geschäftsbedingungen zugestimmt haben, können Sie den API Key anfordern.



Konfiguration der Yubikey API

Die Einrichtung der Multifaktor-Authentifizierung erfolgt am Admin Client im Modul **Datenbanken**.
Selektieren Sie zunächst die gewünschte Datenbank und rufen Sie dann in der Ribbon die **Eigenschaften** auf.
Tragen Sie anschließend die **Yubico Client ID** sowie den **Yubico Secret Key** ein und speichern Sie.

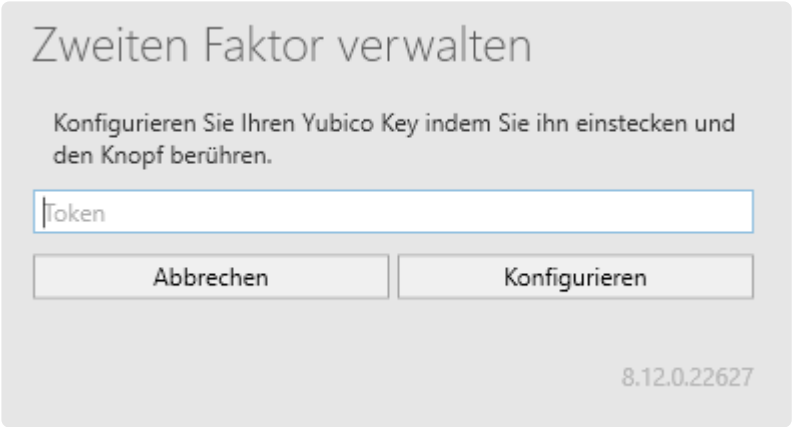


Die Schnittstelle ist nun fertig eingerichtet.

> Zur Kommunikation mit Yubico wird der HTTPS Endpoint “https://api.yubico.com/wsapi/2.0/verify” verwendet. Stellen Sie bitte sicher, dass der Password Safe Server eine Verbindung mit diesem Endpoint aufbauen kann.

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.

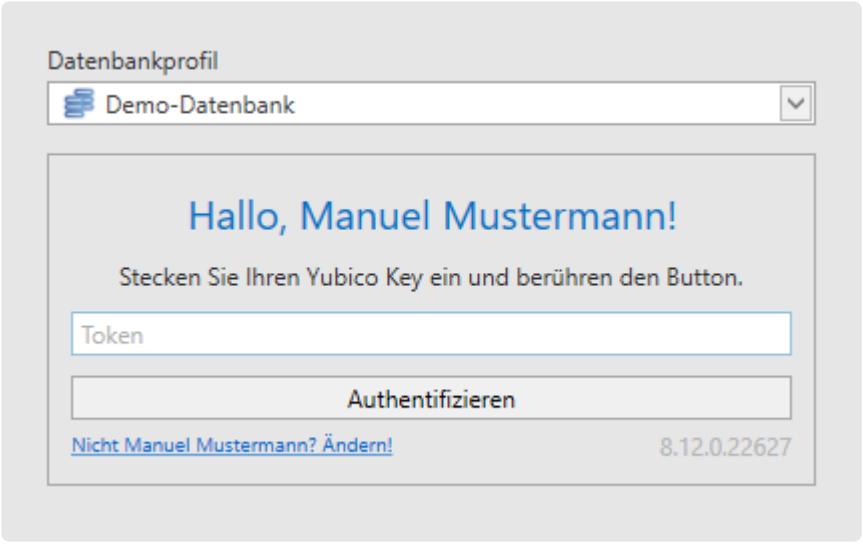


Sobald Sie sie den Token eintragen haben lassen ist die Konfiguration abgeschlossen. Beim **Yubikey NEO** genügt hierfür das Berühren des Touchfelds. Der **Yubikey Nano** muss ebenfalls lediglich “berührt” werden.

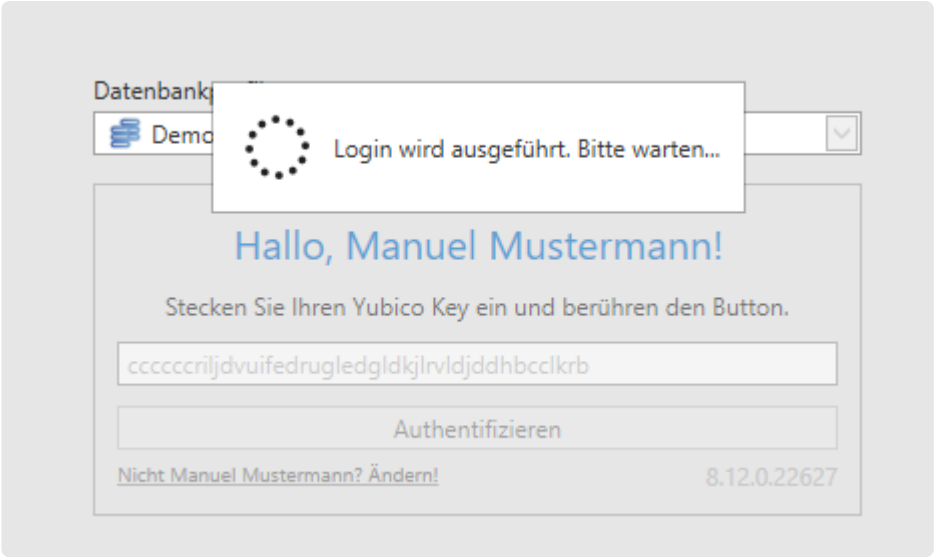
Anmeldung mit dem Yubikey

Zur Anmeldung mit Multifaktor-Authentifizierung wählen Sie zunächst die Datenbank aus, geben Sie anschließend **Benutzername** und das **Passwort** ein und bestätigen Sie den Vorgang.

Nach der erfolgreicher Eingabe vom Benutzernamen und Passwort wird in einem weiteren Fenster der **Yubikey Token** abgefragt.



Klicken Sie in das Feld. Durch das Berühren des Yubikeys wird das **One Time Password** eingetragen.



Der Benutzer wird angemeldet.

OTP (One-Time-Password)

Verwendung von OTP in Password Safe

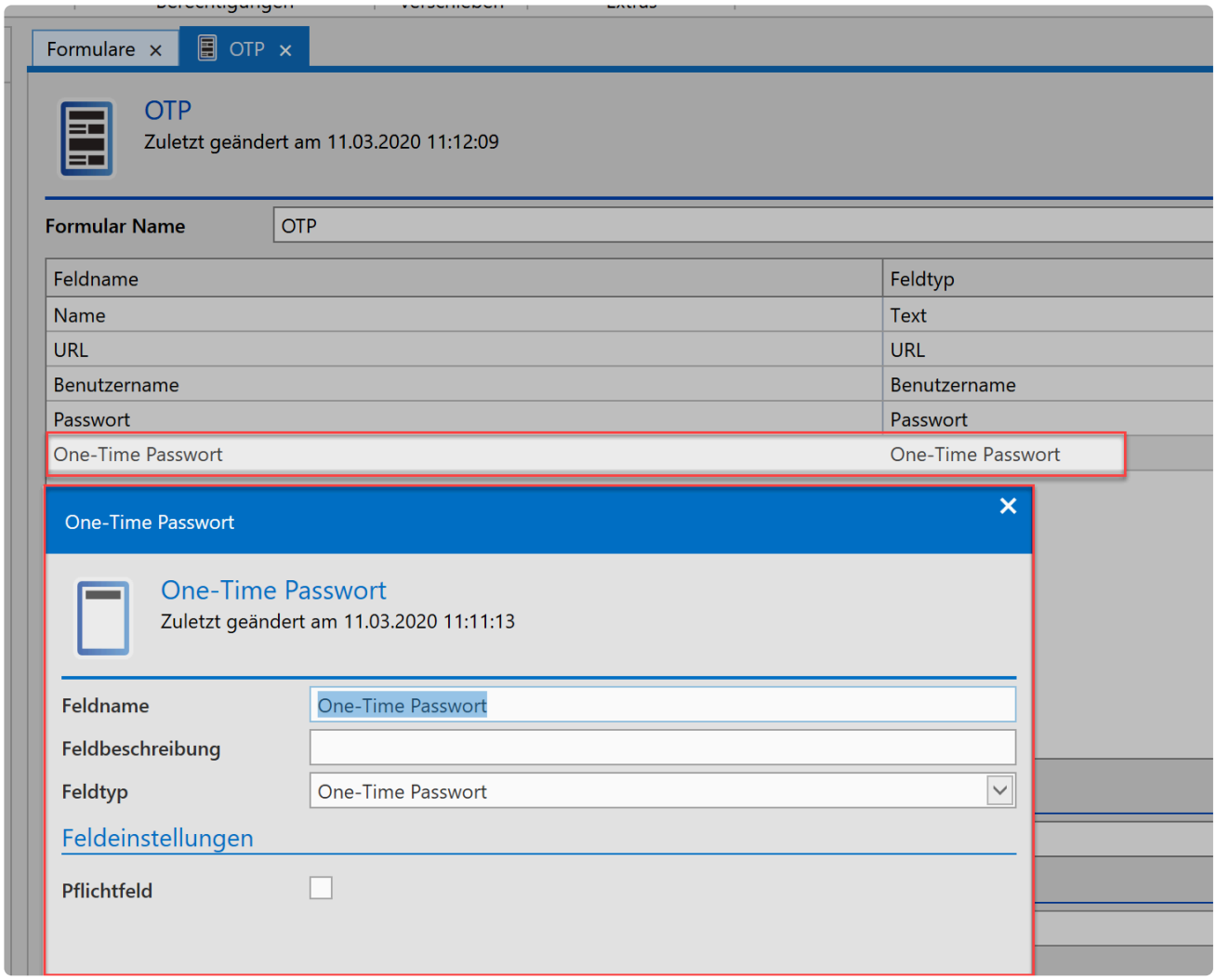
Ein One-Time-Password ist ein einmal gültiges Passwort, welches sich für Transaktionen oder die Authentifizierung verwenden lässt. Entsprechend erfordert jede weitere Authentifizierung oder Autorisierung ein neues Einmalkennwort.

Einrichtung

Um OTP im Password Safe einzurichten, gehen Sie wie folgt vor:

1. Formular mit OTP-Feld erstellen

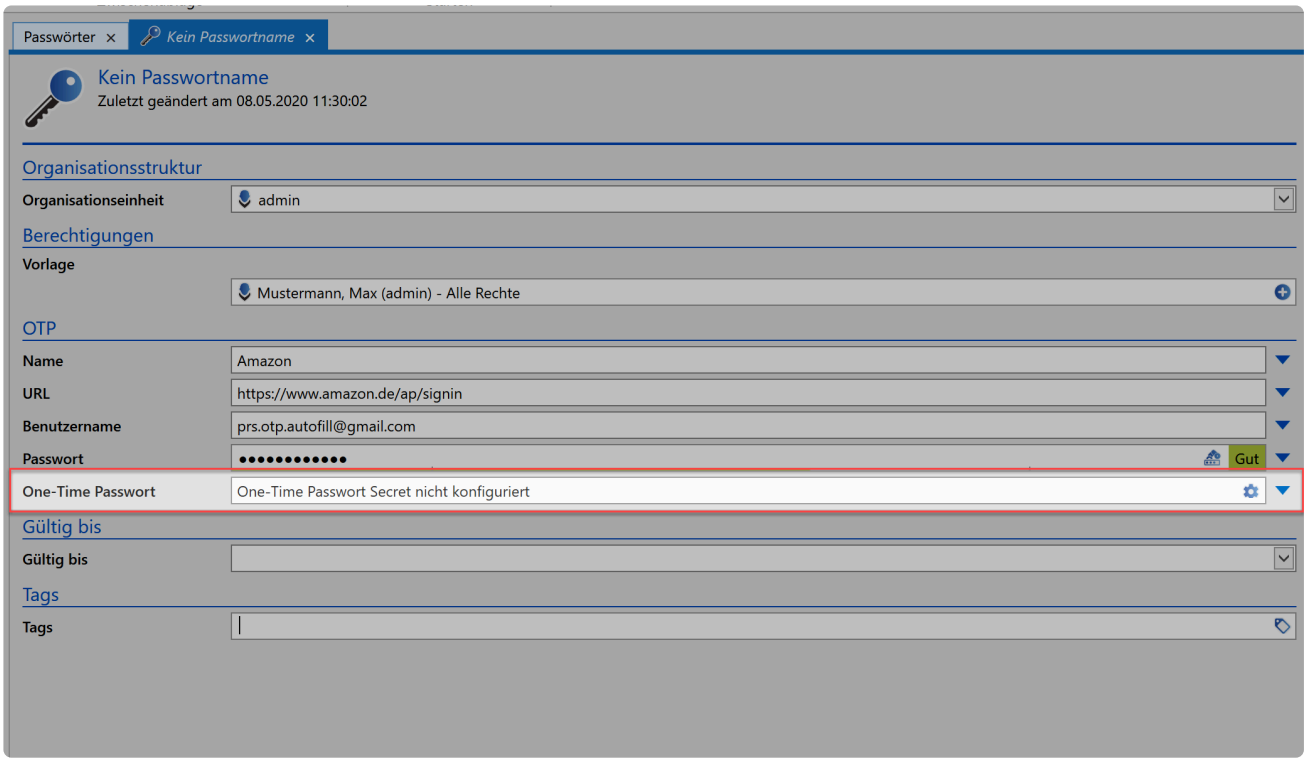
Sie erstellen ein neues Formular oder ergänzen ein bestehendes Formular mit einem One-Time Passwort Feld:



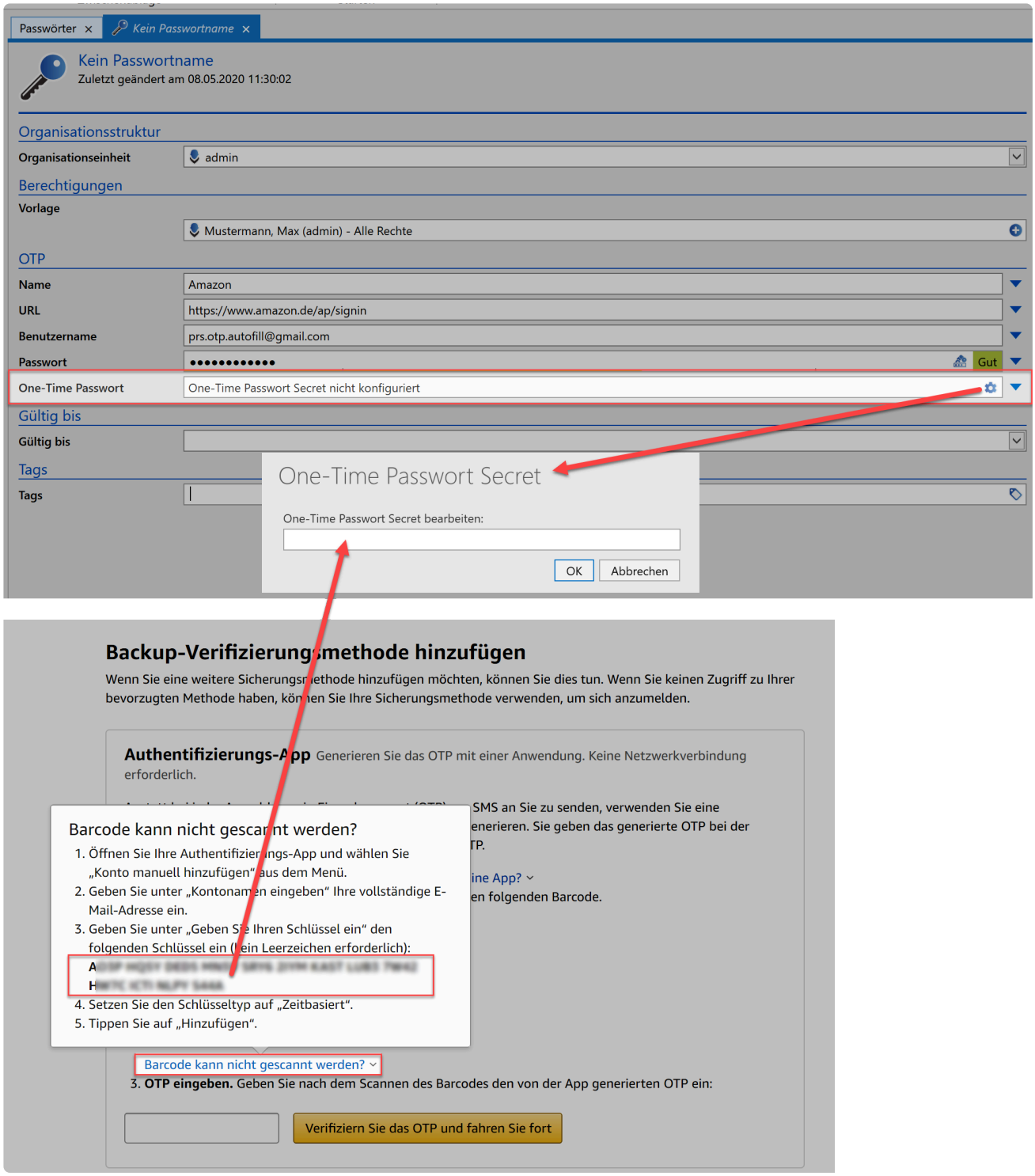
2. Passwort anlegen

Weisen Sie das neue Formular bestehenden Passwörtern zu oder erstellen Sie mit dem neuen Formular

ein neues Passwort.



Als nächstes konfigurieren Sie das OTP-Feld. Hierfür hinterlegen Sie den Schlüssel (Secret) der gewünschten Webseite/Anwendung im Password Safe:

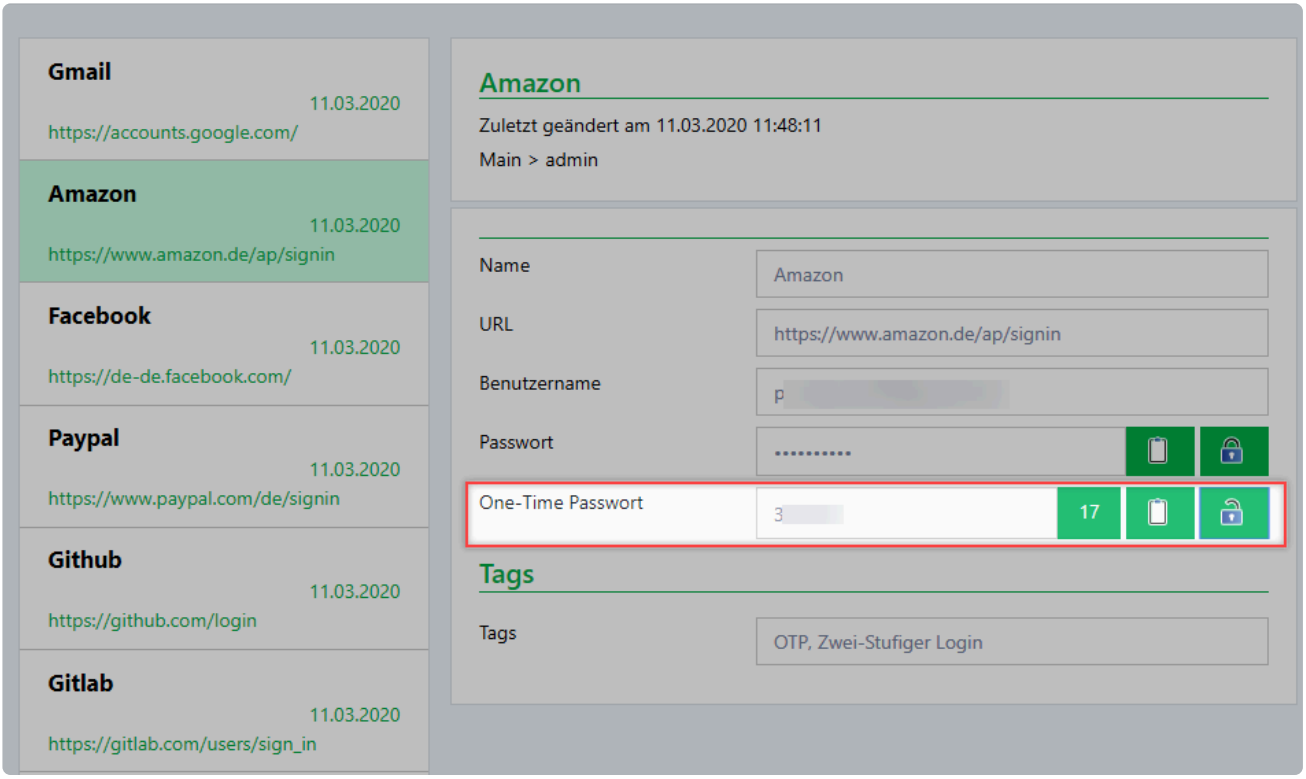


Sobald Sie das Secret hinterlegt haben und das Passwort abgespeichert haben, ist die Einrichtung abgeschlossen.

OTP im HTML WebViewer und Notfall WebViewer

OTP im HTML WebViewer

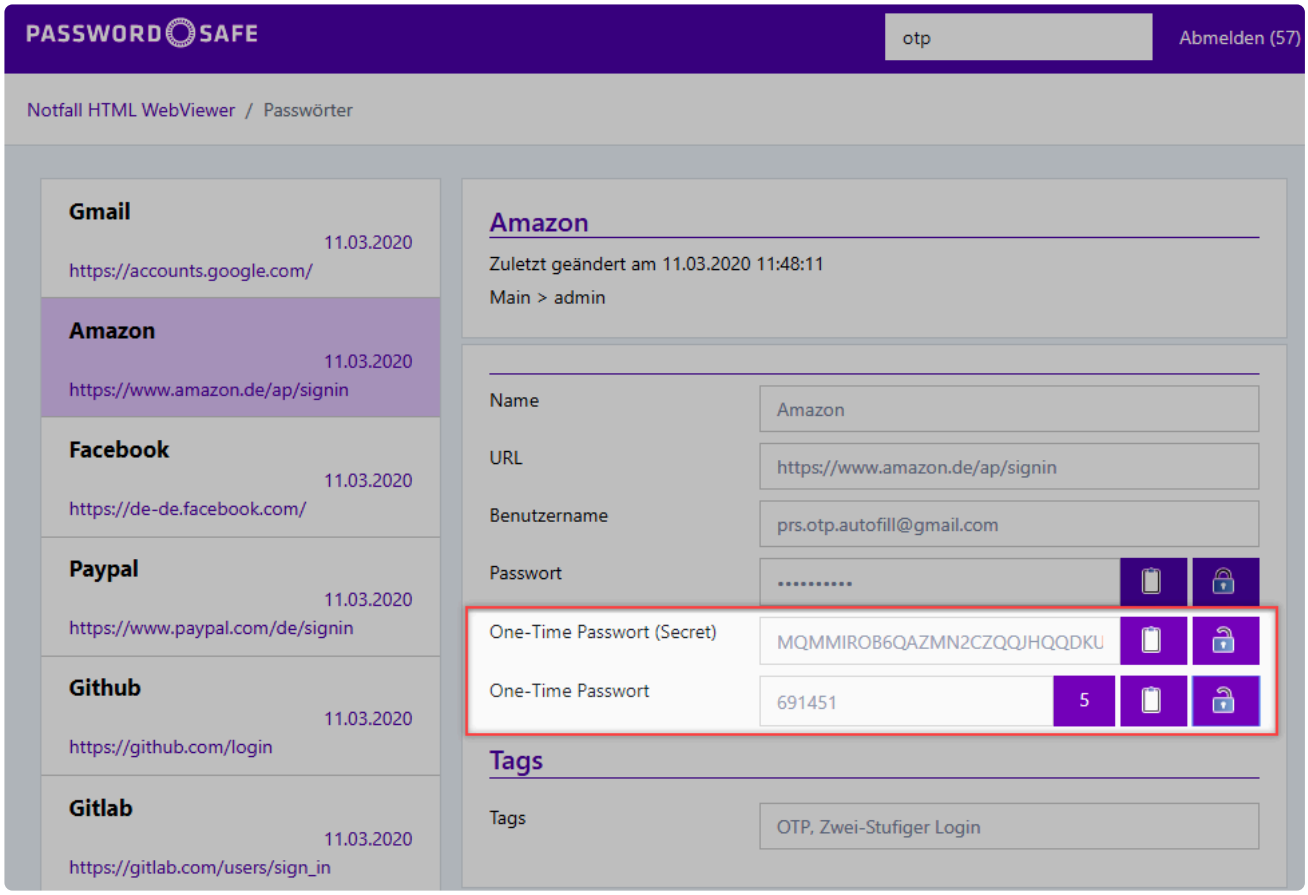
- 1. OTP einrichten
- 2. HTML WebViewer erstellen
- 3. Öffnen des erstellten HTML WebViewers



Wie Sie den HTML WebViewer nutzt, können Sie im gleichnamigen Kapitel nachlesen.

OTP im Notall WebViewer

Die Besonderheit beim Notfall WebViewer ist, dass das hinterlegte OTP Secret mit ausgegeben wird.



Um das One-Time-Password im Notfall WebViewer nutzen zu können, müssen Sie wie folgt vorgehen:

- 1. OTP einrichten
- 2. Notfall-HTML WebViewer Export Task erstellen
- 3. Öffnen des erstellten Notfall WebViewer

Rollen

Was sind Rollen?

Jeder Mitarbeiter in einem Unternehmen ist Mitglied einer Abteilung und / oder Teil einer bestimmten Funktionsebene. Diese Hierarchien können Sie innerhalb von Password Safe mittels Rollen abbilden. Mehrere Mitarbeiter einer Abteilung sind dabei Mitglied einer Rolle. Eine Rolle hat dann wiederum Berechtigungen auf Passwörter. Dadurch haben automatisch alle Mitglieder dieser Rolle auch die Berechtigungen auf die Passwörter.

Aufgrund der Komplexität des Rollenkonzeptes bietet es sich an, das Modul **Rollen** nur administrativ tätigen Benutzern zur Verfügung zu stellen. Das Berechtigungskonzept gewährleistet, dass Benutzern lediglich Zugriff auf diejenigen Rollen gewährt wird, auf die sie auch berechtigt sind. Hier finden Sie weitere Informationen zur Konfiguration der **Sichtbarkeit**.

Passwörter Dokumente Benachrichtigungen Organisationsstruktur **Rollen** Formulare Logbuch Anwendungen Password Reset

Relevante Rechte

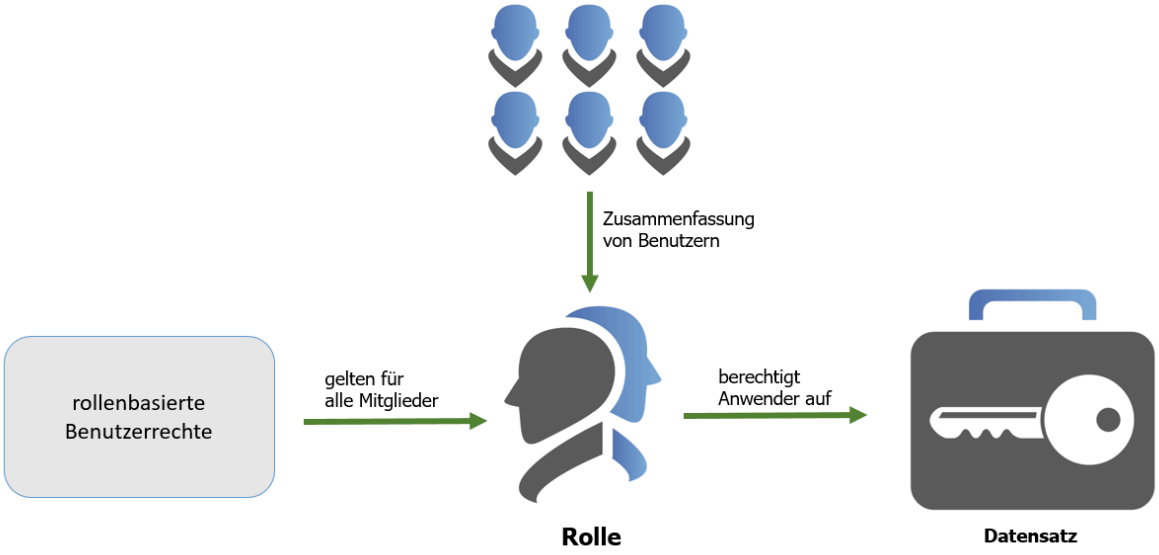
Folgende Rechte kommen hier zum Tragen.

Benutzerrecht

- Kann neue Rollen anlegen
- Rollenmodul anzeigen

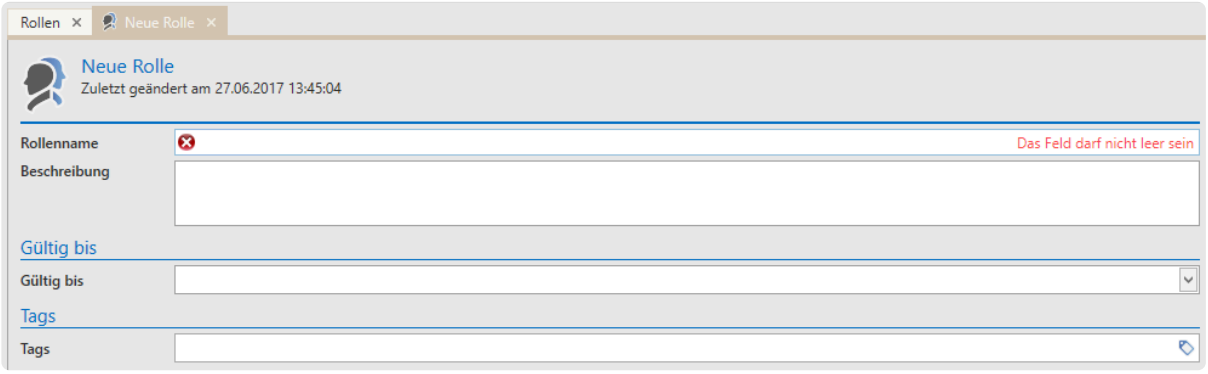
Rollen im Fokus

Die Konfiguration von Rollen ist die Basis für das **Berechtigungskonzept**. Die Berechtigung auf Daten ist auch auf Benutzerebene möglich. Durch die Nutzung von Rollenzugehörigkeiten lässt sich jedoch der administrative Aufwand reduzieren. Sie können ebenso Benutzerrechte über Rollen abbilden.



Erstellung und Berechtigen neuer Rollen

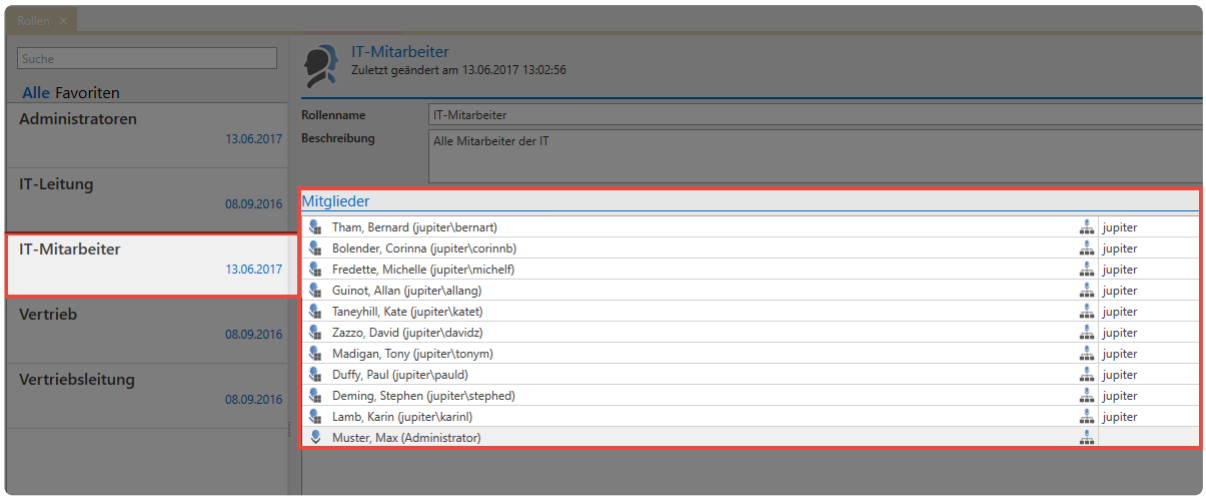
Das Erstellen neuer Rollen entspricht dem **Erstellen neuer Datensätze**. Sowohl über die Ribbon, als auch über das Kontextmenü der rechten Maustaste können Sie Rollen anlegen.



Weitere Informationen zu Rollen und den Berechtigungen finden Sie im Kapitel **Berechtigungskontzept**.

Übersicht auf Rollenmitglieder

Zusätzlich zur Ansicht im Berechtigungsdialog, ist auch im **Lesebereich** eine Auflistung aller **Mitglieder** einer Rolle möglich. Alle anderen Berechtigten ohne Mitgliedschaft in der Rolle werden in dieser Ansicht nicht berücksichtigt.



> Das Modul **Rollen** ähnelt dem gleichnamigen **WebClient-Modul**. Beide Module sind hinsichtlich der Bedienung nahezu identisch. Sie unterscheiden sich allerdings in Umfang und Design.

Formulare

Was sind Formulare?

Im **Formular** definieren Sie die Felder, die zum Anlegen eines Passworts befüllt werden müssen. **Formulare** stellen also die **“Schablonen” der zu speichernden Informationen** dar. Zudem dienen **Formulare** auch als Filterkriterium. Die Konfiguration der **Sichtbarkeit** wird hier erläutert: **Sichtbarkeit der Module**

Passwörter Dokumente Benachrichtigungen Organisationsstruktur Rollen **Formulare** Logbuch Anwendungen Password Reset

Relevante Rechte

Sie benötigen folgende Optionen um ein neues Formular anzulegen:

Benutzerrecht

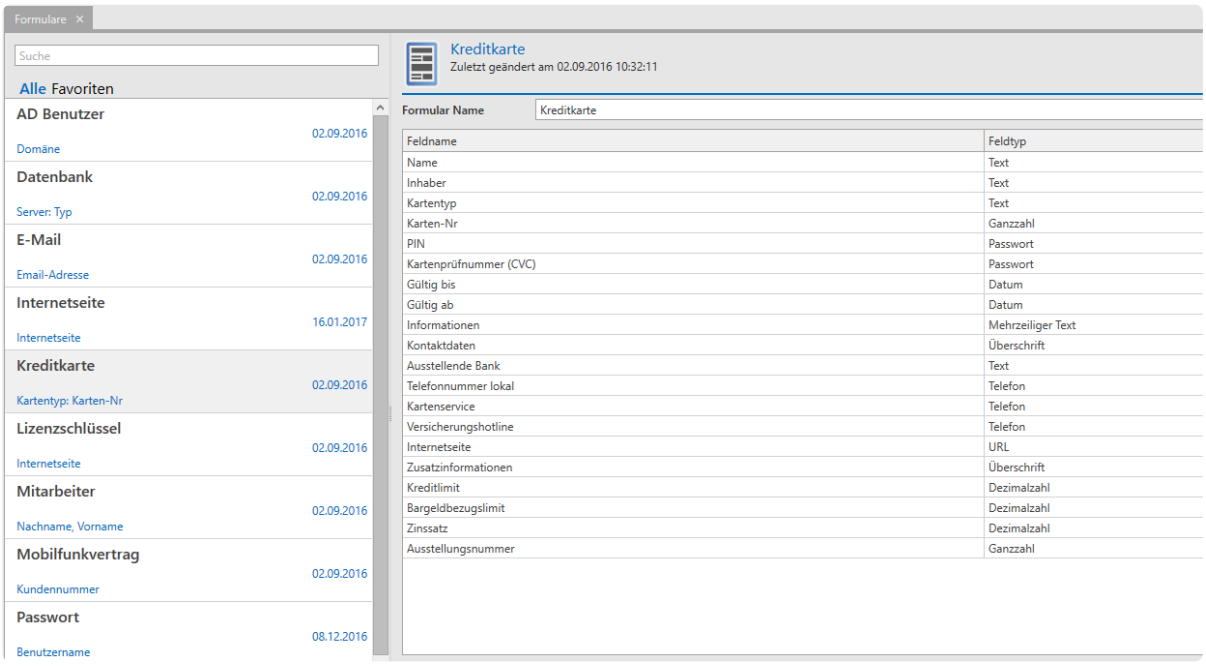
- Kann neue Formulare anlegen
- Formularmodul anzeigen

Benutzereinstellung

- Standard-Formular

Mitgelieferte Formulare

Password Safe wird mit einer Reihe von Formularen ausgeliefert. Diese decken in der Regel alle gängigen Anforderungen ab. Selbstverständlich können Sie diese Formulare an Ihre Anforderungen anpassen.



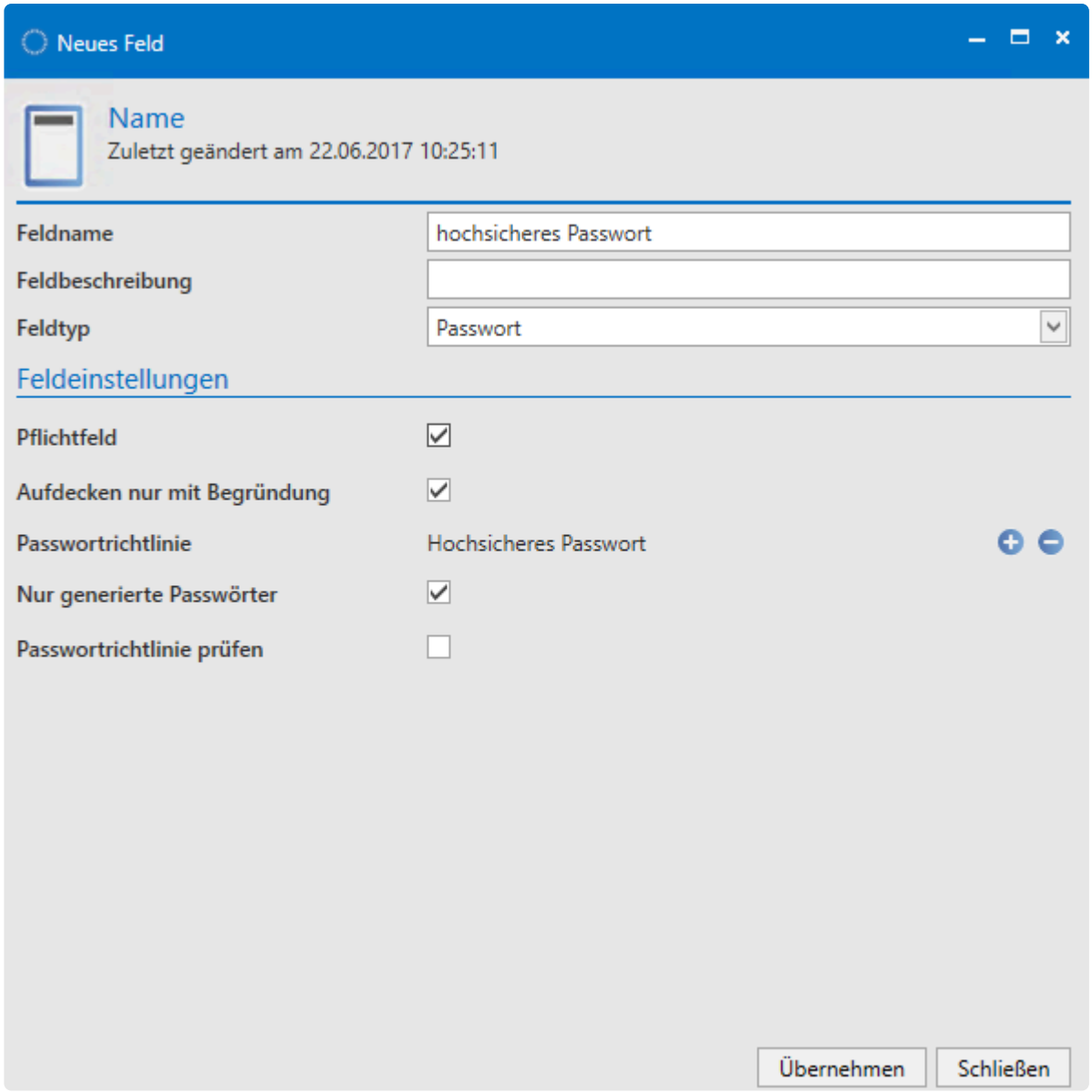
Wählen Sie in der **Listenansicht** ein Formular aus, erscheint im **Lesebereich** die zugehörige Vorschau. Sowohl Feldname als auch Feldtyp sind einsehbar.

Erstellen neuer Formulare

Den Assistenten zum Erstellen neuer Formulare starten Sie über die Ribbon, den Shortcut **Strg + N** oder über das Kontextmenü der rechten Maustaste. Im Assistenten legen Sie über die gleichen Mechanismen neue Formularfelder an. Je nach ausgewähltem Feldtyp ergeben sich für den Bereich **Feldeinstellungen** andere Optionen.

Beispiel

In diesem Beispiel wird ein Feld vom Typ **Passwort** erstellt.



Für den Feldtyp **Passwort** stehen Ihnen die Feldeinstellungen **Pflichtfeld**, **Aufdecken nur mit Begründung**, **nur generierte Passwörter und Passwortrichtlinie prüfen** zur Verfügung. Diese sind frei definierbar.

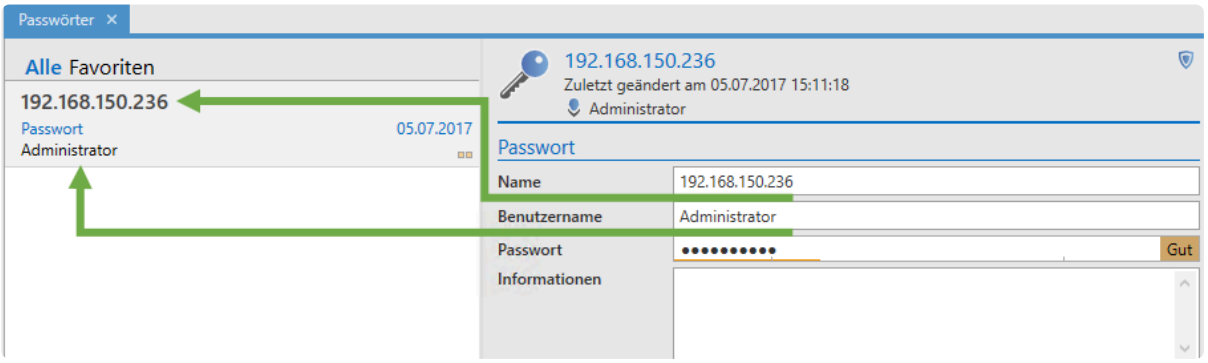
> ! Ist ein Formular angelegt, kann dieses beim Erstellen neuer Datensätze ausgewählt werden. Voraussetzung hierfür ist, dass der angemeldete Benutzer auf das Formular mindestens Leseberechtigung besitzt.

Berechtigungen auf Formulare

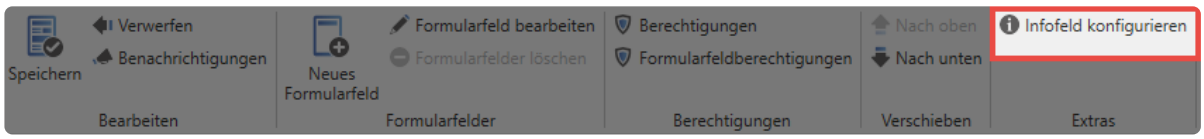
Informationen zu den Rechten finden Sie im Kapitel: **Berechtigungskonzept**. Dies stellt sicher, dass einerseits nicht jeder Formulare bearbeiten kann, andererseits stellen Sie die Formulare auf diese Art und Weise den unterschiedlichen Benutzergruppen zur Verfügung. Somit wird die Übersichtlichkeit gewahrt. Die Benutzer sehen also keine Formulare, die sie nicht benötigen. Das Formular **Kreditkarte** wird beispielsweise in der Buchhaltung benötigt. Administratoren sollten dieses in der Regel eher nicht brauchen.

Infofeld konfigurieren

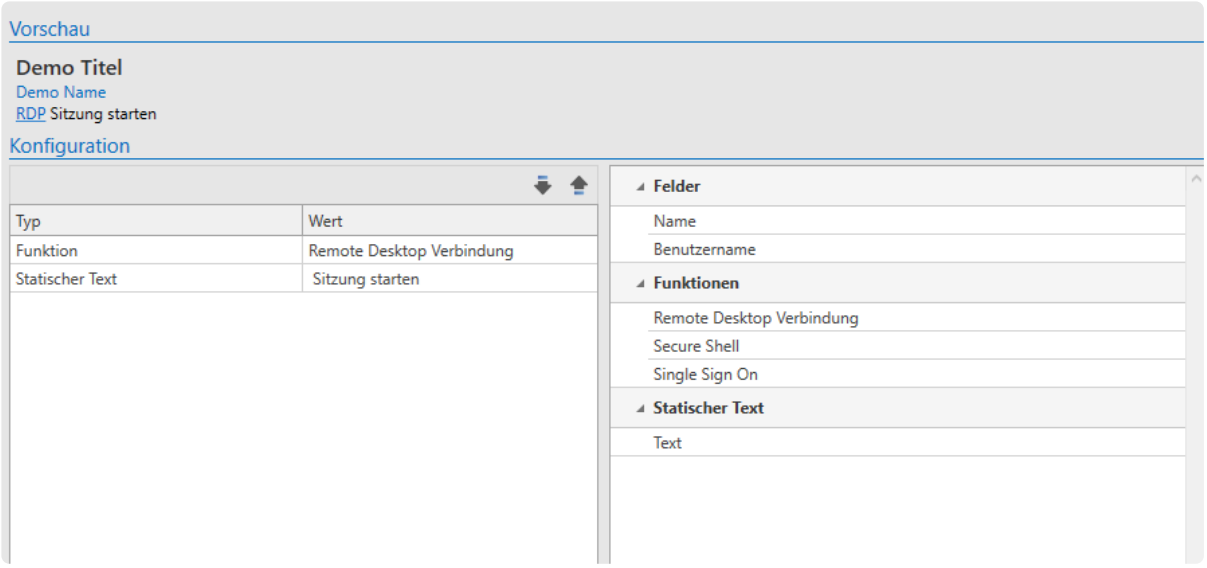
Jeder Datensatz besitzt in der Listenansicht den Datensatznamen, sowie weitere Informationen. Diese können Sie frei definieren. Im nachfolgenden Beispiel wird zusätzlich zum Namen des Passworts noch der Benutzername angezeigt. Dazwischen finden Sie in blauer Schrift den Name des Formulars.



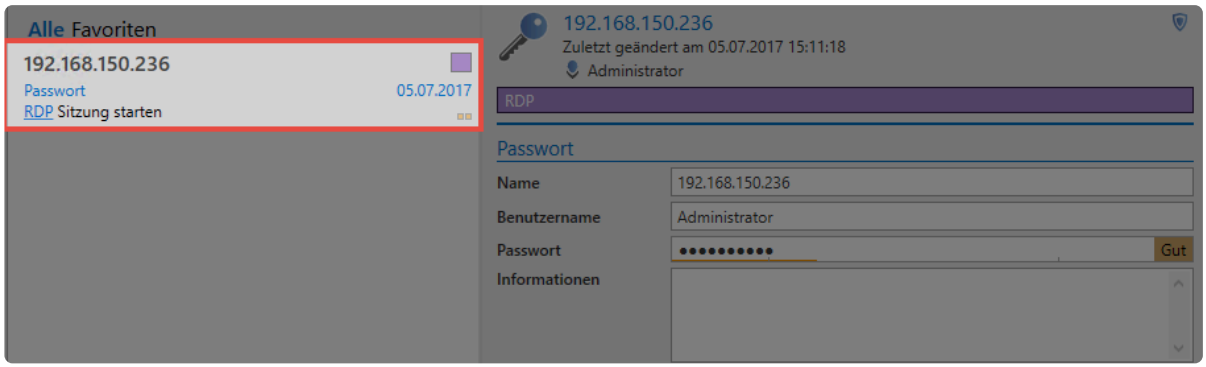
Der Name des Datensatzes (192.168.150.236) sowie des Formulars (Passwort) können nicht angepasst werden. Diese werden also immer angezeigt. Aktuell wird der im Datensatz hinterlegte Benutzer angezeigt. Dies können Sie im **Infofeld** des Formulars anpassen. Definieren Sie dadruch für jedes Formular, welche Informationen innerhalb der Listenansicht dargestellt werden. Um das Infofeld zu konfigurieren, öffnen Sie zunächst das Formulare mit einem Doppelklick. Anschließend starten Sie über die Schaltfläche **Infofeld konfigurieren** in der Ribbon die Konfiguration.



Es öffnet sich ein Tab, welches Ihnen per Drag & Drop die Gestaltung des Infobereichs ermöglicht. Die rechts verfügbaren Felder können Sie in das linke Konfigurationsfenster ziehen. 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.

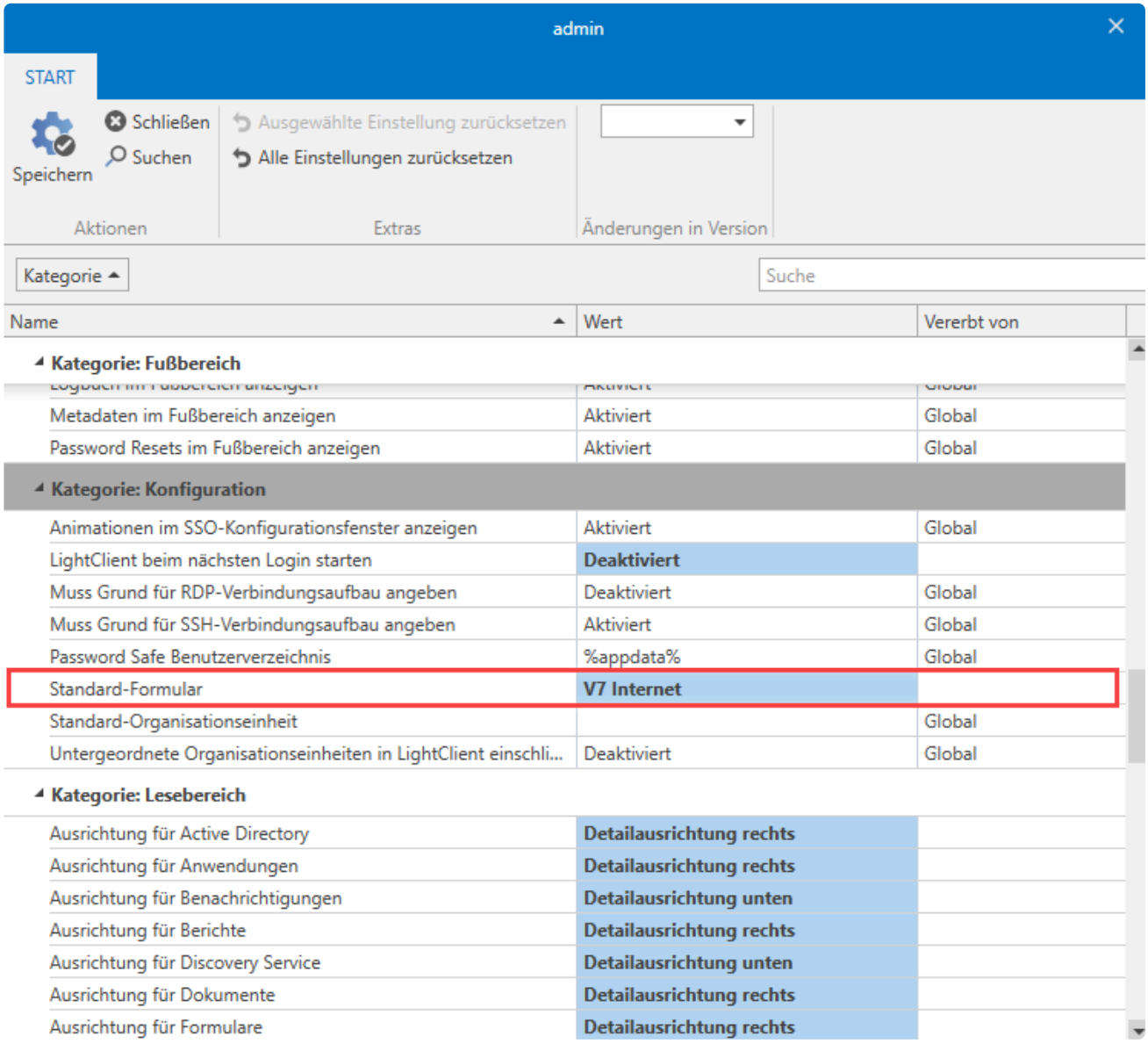


> Das Modul **Formulare** ähnelt dem gleichnamigen WebClient-Modul. Beide Module unterscheiden sich in Umfang und Design. Hinsichtlich der Bedienung sie sie jedoch nahezu identisch.

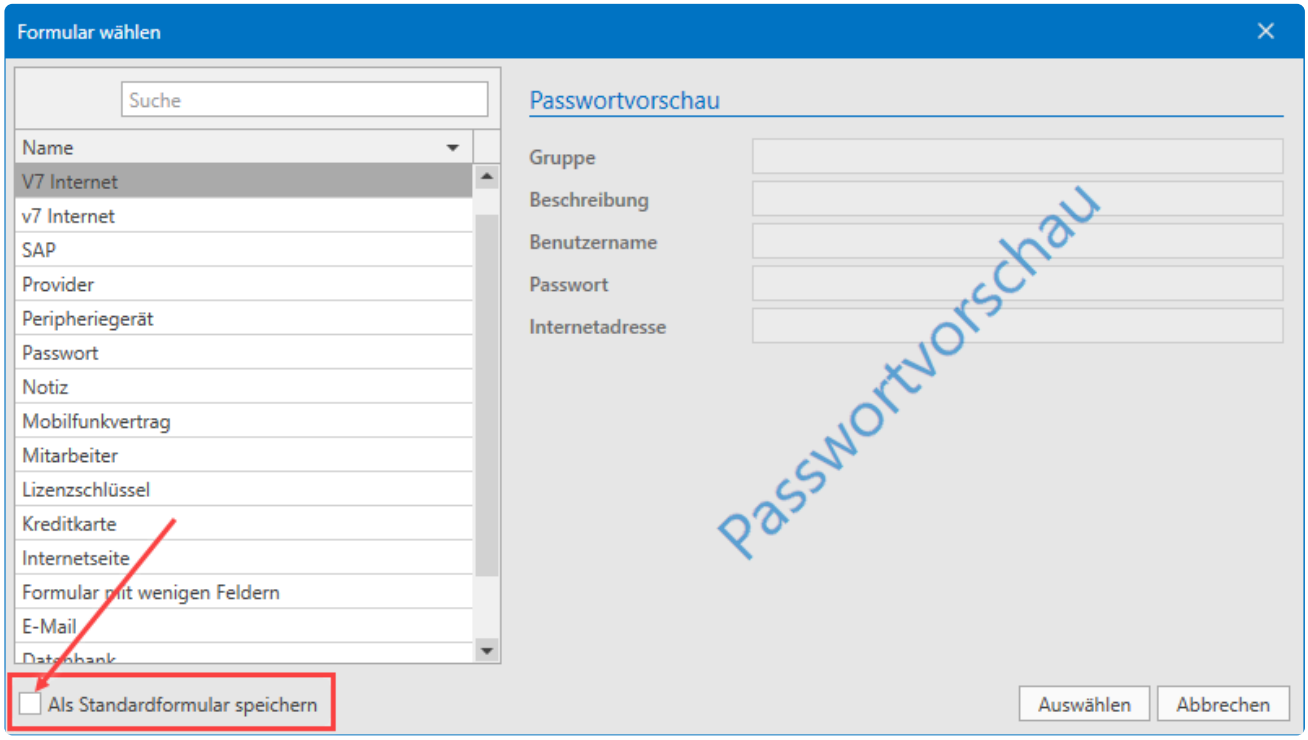
Standard-Formular

Das Standard-Formular hat zwei Funktionen. Zum einen werden im **LightClient** alle neuen Datensätze über dieses Formular erstellt. Im FullClient wird beim Erstellen eines neuen Passworts ebenfalls das Standard-Formular verwendet. Hier können Sie jedoch – über die Schaltfläche unter dem **Neu** Button – auch ein anderes Formular auswählen.

1. Über die Benutzereinstellung Standard-Fomular



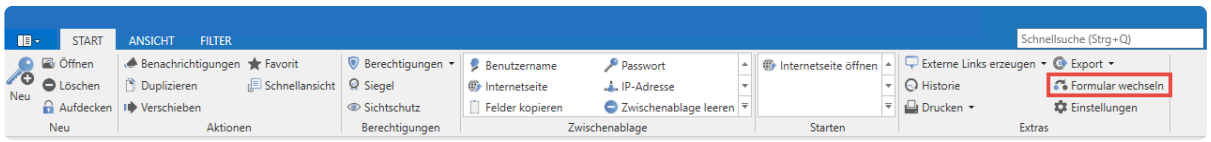
2. Über die Formularauswahl:



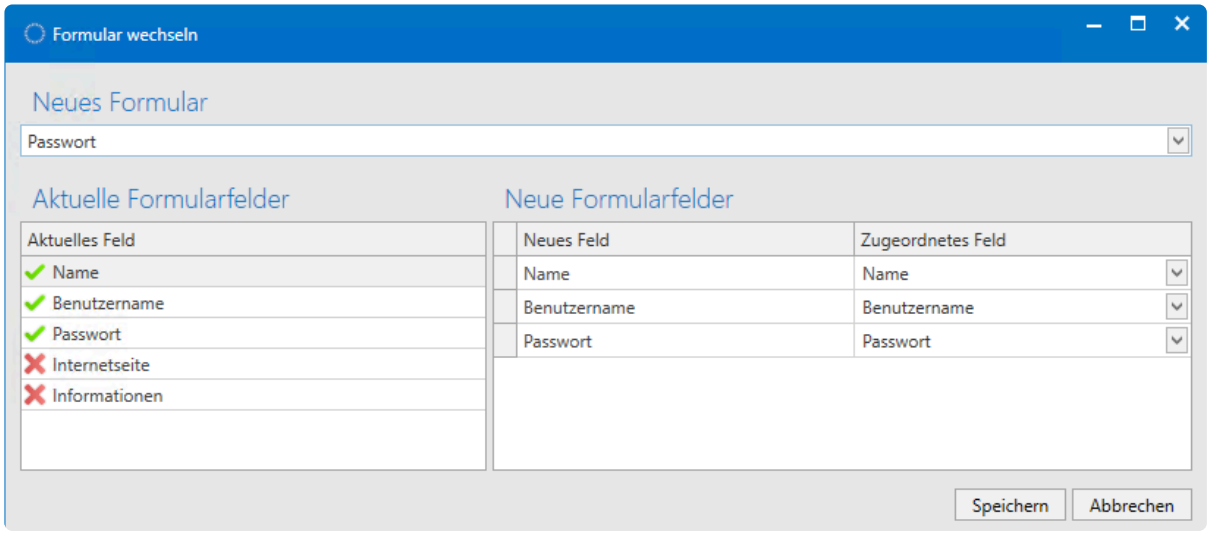
Formulare wechseln

Das Wechseln von Formularen

In manchen Fällen kann es notwendig sein, dass Sie das Formular eines Datensatzes wechseln. Die Funktionalität finden Sie in der Ribbon unter **Extras/Einstellungen** verfügbar.



Der Wechsel eines Formulars macht es nötig, die Felder des alten Formulars denen des neuen Formulars zuzuweisen. Hier wird beispielhaft versucht, einen Datensatz basierend auf dem Formular **Internetseite**, auf das Formular **Passwort**" (rechts) zu "mappen". Dies geschieht über folgenden Dialog.



Wählen sim im Dropdown das Ziel-Formular aus. 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

Relevante Rechte

Sie benötigen folgende Optionen um Formular zu wechseln.

Benutzerrecht

- Kann Formular eines Passworts wechseln

! Bitte beachten Sie, dass dabei Informationen dauerhaft verloren gehen können! Im

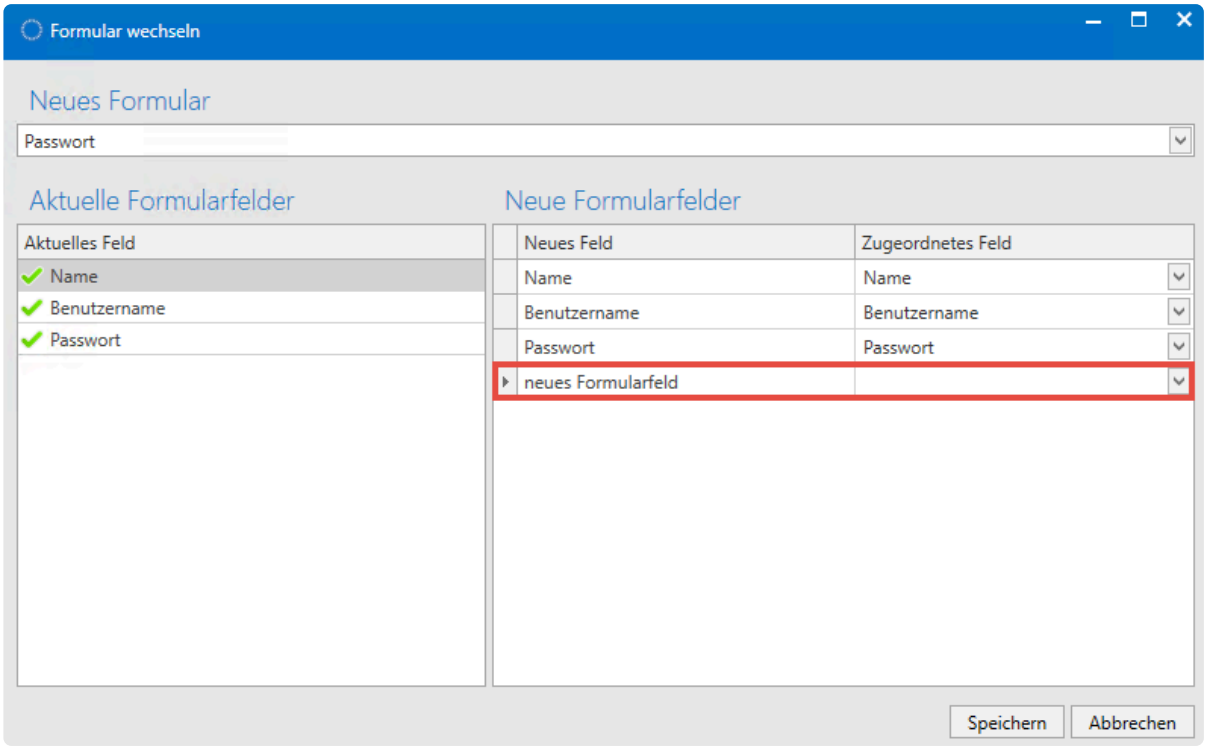
Beispiel wären dies die Felder **Internetseite** sowie **Informationen**.

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 nicht geändert wird. Dennoch gibt es Methoden, wie Anpassungen an Formularen auch in bereits bestehende Datensätze übernommen werden können:

Formular wechseln

Sie können über den Button **Formular wechseln** den Datensätzen das geänderte Formular einfach zuweisen.



Formularänderungen auf Passwörter anwenden

Die Einstellung **Formularänderungen auf Passwörter anwenden** ermöglicht, dass Änderungen an Formularen erzwungen werden. Dies geschieht beim Bearbeiten des Datensatzes. Es ist hierbei unerheblich, ob am Datensatz Veränderungen vorgenommen wurden. Sobald Sie den Datensatzes speichern wird ihm das neue Formular zugewiesen.

Folgende Berechtigungen/Konfigurationen müssen gegeben sein:

- Der Benutzer, welche die Änderung vornehmen will, benötigt Leserecht auf das Formular
- Auf den Datensatz (sowie die anzupassenden Formularfelder) sind die Rechte “Lesen”, “Schreiben”, “Löschen” und “Berechtigen” nötig.

- Versiegelte und sichtgeschützte Datensätze bleiben unangetastet

Fazit

In beiden Varianten werden Anpassungen an Formularen **nicht automatisiert herbeigeführt**. Bereits bestehende Datensätze werden nicht automatisch angepasst. Die Änderungen müssen manuell 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

Revisionssicherheit durch das Logbuch

Password Safe protokolliert alle Aktionen aller Benutzer im sogenannten Logbuch. Dabei wird gespeichert, welcher Benutzer wann welche Änderungen vorgenommen hat. Dabei kann jeder Benutzer nur auf die Logbucheinträge der Objekte zugreifen, auf die er auch tatsächliche berechtigt ist. Zudem muss der Benutzer die Berechtigung haben, das Modul “Logbuch” sehen zu können, was **hier** konfiguriert werden kann.

Password Safe verfolgt bei der Handhabung des Logbuchs einen kompromisslosen Weg: Jede Zustandsänderung wird erfasst und in der Datenbank abgelegt. Es kann nicht festgelegt werden, dass nur bestimmte Aktionen gespeichert werden sollen. Denn nur diese Herangehensweise ermöglicht, dass Änderungen revisionssicher und dadurch unverfälschbar nachvollzogen werden können.

Relevante Rechte

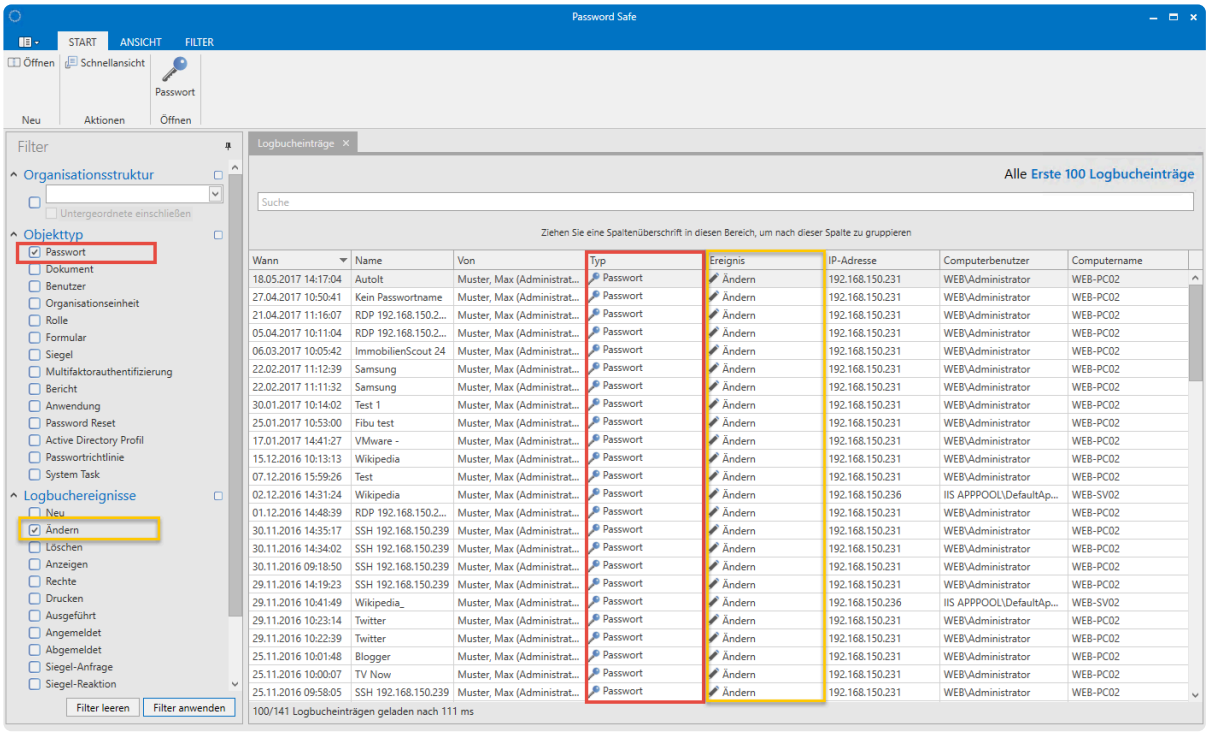
Folgende Optionen werden benötigt:

Benutzerrecht

- Logbuch-Modul anzeigen

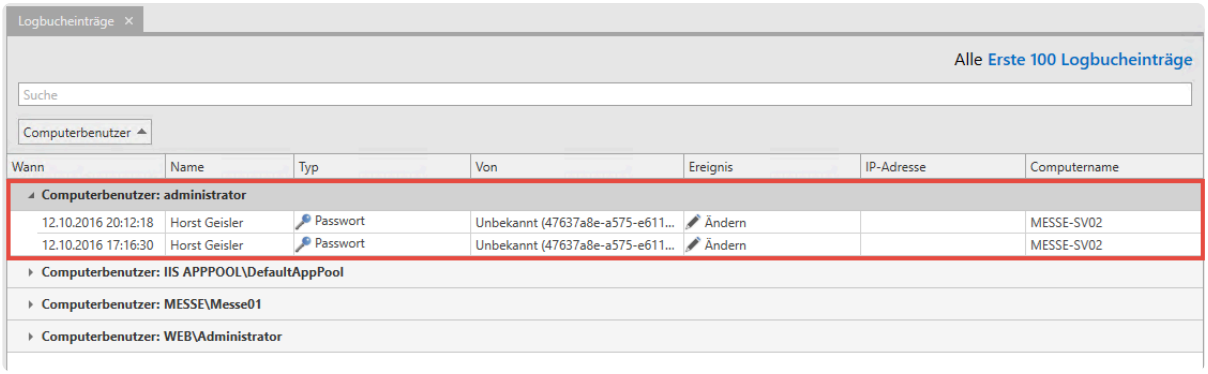
Einsatz des Filters im Logbuch

Wie in allen anderen Modulen können Sie auch im Logbuch den Filter nutzen um die Anzahl der angezeigten Elemente einzugrenzen. Im nachfolgenden Beispiel wird nach Logbucheinträgen gesucht, die den Objekttyp **Passwort** betreffen und dem Ereignis “Ändern” entsprechen. Kurz gesagt: Es wird nach Änderungen an Passwörtern gefiltert.



Gruppierungen im Logbuch

Durch Drag & Drop der Spaltenüberschriften können Sie diese Auflistung gruppieren. Die gefilterten Informationen zeigen nun alle Ergebnisse, die Änderungen an Passwörtern durch den Computerbenutzer **Administrator** entsprechen.



Automatische Bereinigung

Falls gewünscht, kann das Logbuch automatisch bereinigt werden. Diese Option wird am **AdminClient** konfiguriert. Weitere Informationen finden Sie im Kapitel Verwaltung von Datenbanken.

Übertragen an einen Syslog-Server

Falls gewünscht, können Sie das Logbuch komplett an einen Syslog-Server übertragen. Weitere Informationen finden Sie dazu im Kapitel Syslog.

Anwendungen

Was sind Anwendungen?

Mithilfe von Anwendungen können Sie die automatisierte Anmeldung an verschiedenen Systemen konfigurieren. In Kombination mit zusätzlichen Schutzmechanismen steigern Sie hierdurch nicht nur den Komfort, sondern auch die Sicherheit: Komplexe Passwörter werden automatisiert und für den Benutzer verdeckt in Anmeldemasken eingefügt. Es stehen verschiedene Anwendungstypen zur Verfügung.

Passwörter Dokumente Benachrichtigungen Organisationsstruktur Rollen Formulare Logbuch **Anwendungen** Password Reset

Das automatisierte Anmelden an Websites erfolgt über den SSO-Agent.

Relevante Rechte

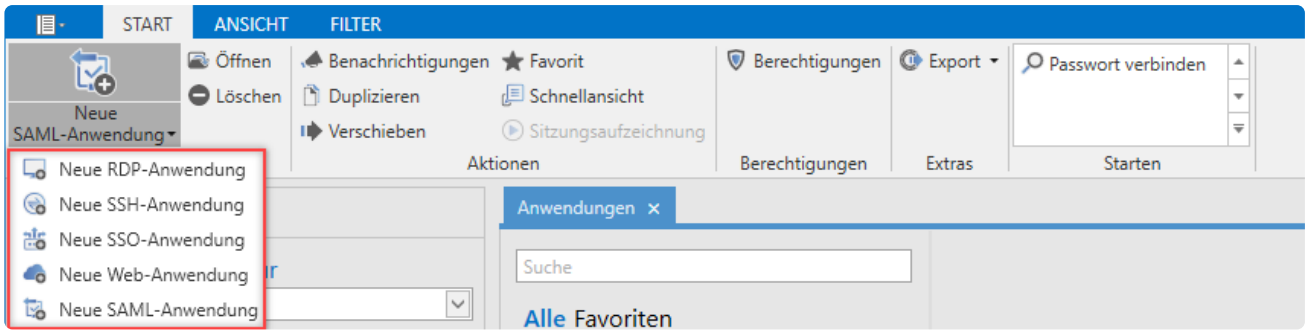
Sie benötigen folgende Optionen.

Benutzerrecht

- Kann neue Anwendungen vom Typ RDP anlegen
- Kann neue Anwendungen vom Typ SSH anlegen
- Kann neue Anwendungen vom Typ SSO anlegen
- Kann neue Anwendungen vom Typ Web anlegen
- Kann neue Anwendungen vom Typ SAML anlegen

Die fünf Anwendungsarten

Password Safe unterscheidet zwischen fünf verschiedene Anwendungsarten: RDP, SSH, SSO, Web & SAML-Anwendungen.



Informationen zu den unterschiedlichen Anwendungen finden Sie in den folgenden Kapiteln:

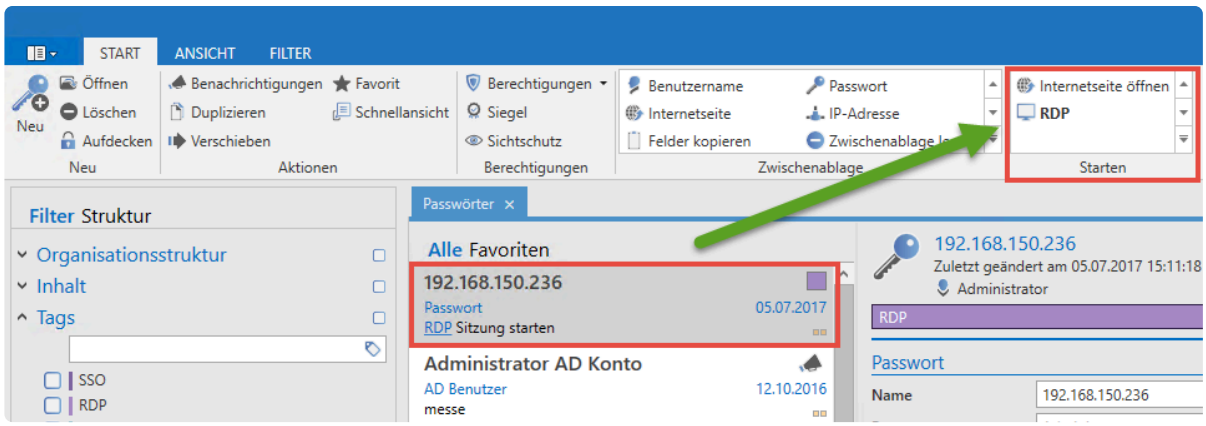
- SSO Anwendungen
- RDP und SSH Anwendungen
- SAML Anwendungen
- Web Anwendungen

Unter folgendem Kapitel finden Sie einige Konfigurationsbeisipele:

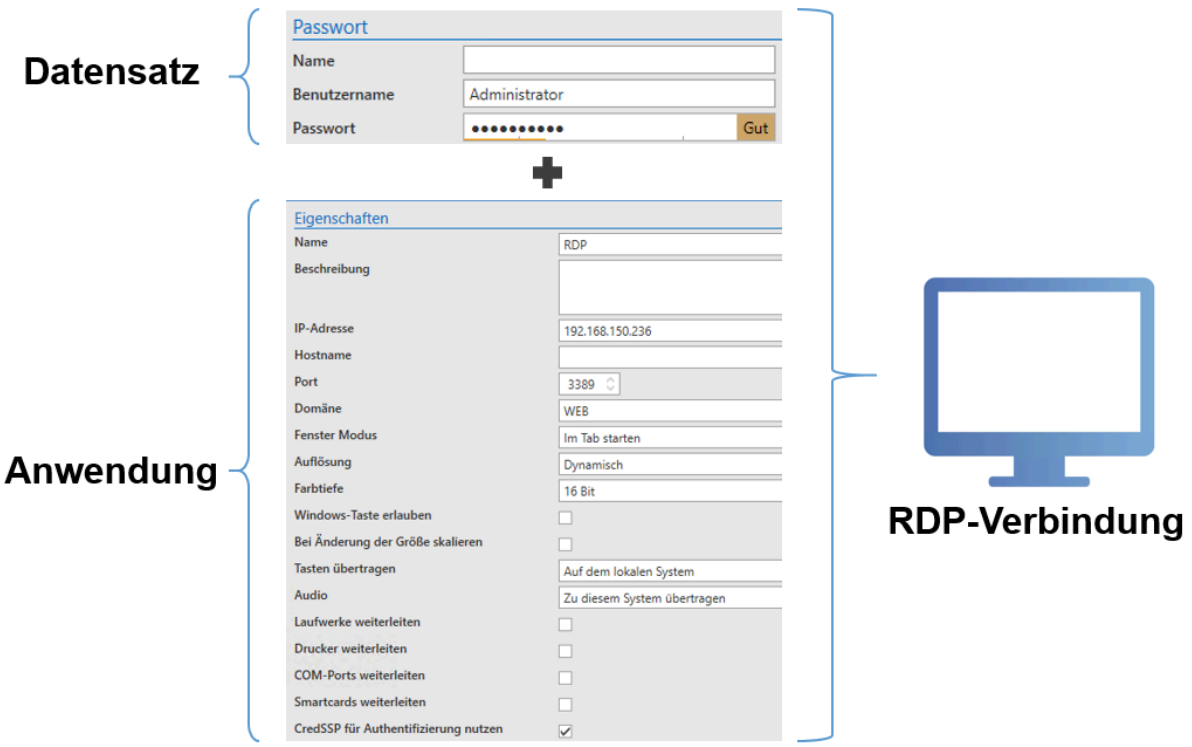
- **Beispiele für Anwendungen**

Verbindung von Datensätzen und Anwendungen

Durch das Verbinden von Datensätzen mit Anwendungen kann die komplette Anmeldung automatisiert abgebildet werden. Verknüpfen Sie 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.

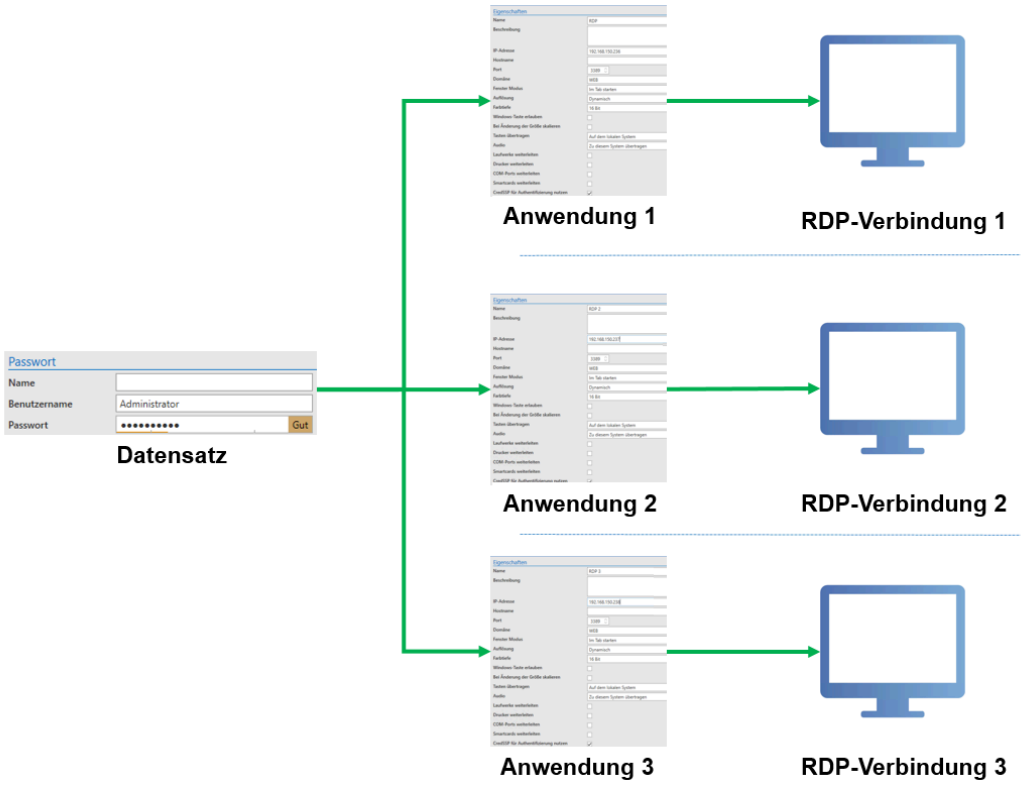


Das nachfolgende Beispiel soll dies anhand einer RDP-Verbindung veranschaulichen:



Auf diese Art können Sie auch einen Datensatz mit mehreren Zielsystemen verknüpfen. Benutzername und Datensatz werden aus dem Datensatz gespeist. Alle verbleibenden, für die Anmeldung erforderlichen Informationen kommen aus den unterschiedlichen Anwendungen. Im nachfolgenden

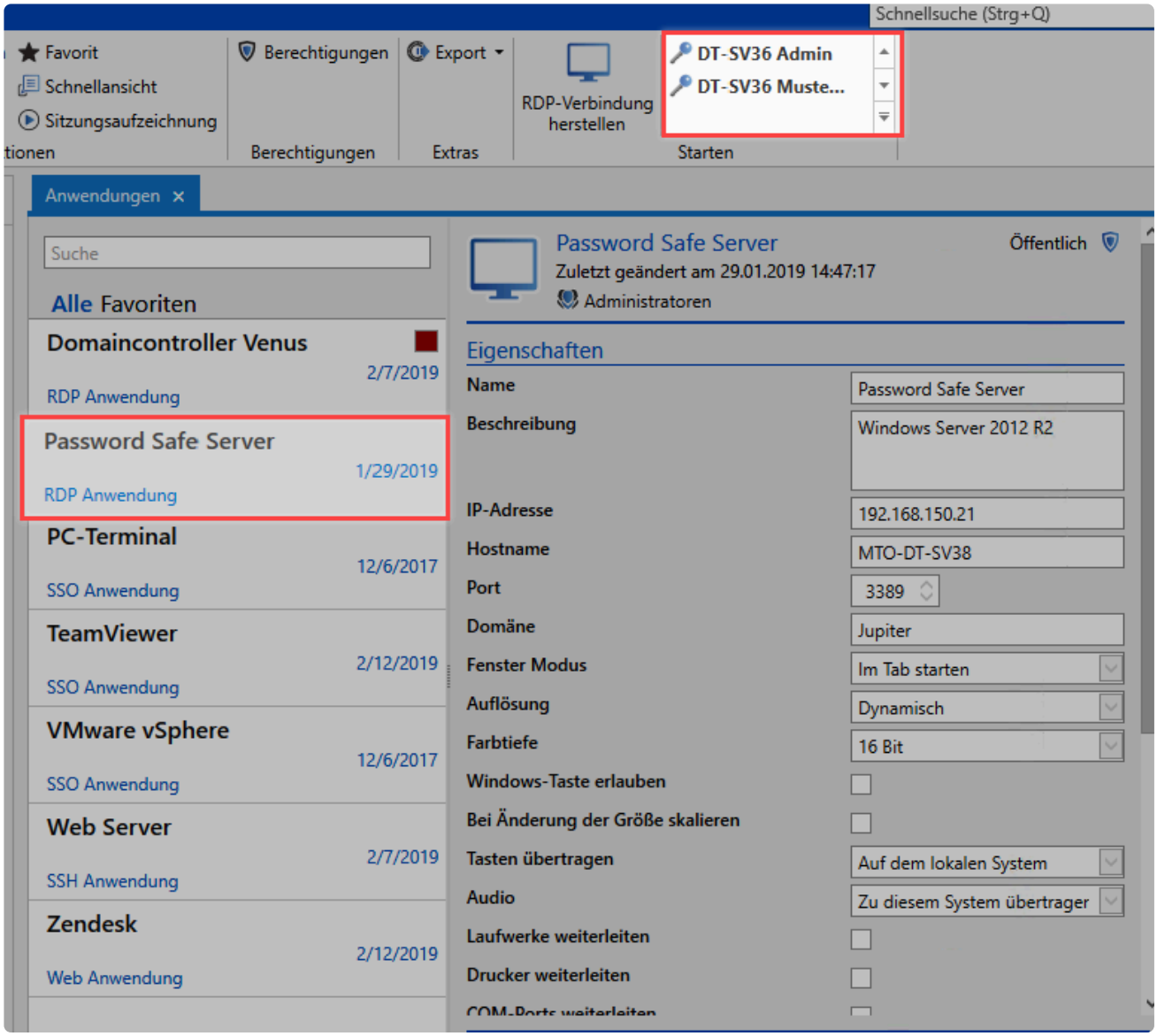
Beispiel ist ein Datensatz (Benutzername und Passwort) mit mehreren Zugängen verknüpft.



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

> Das Feld **IP-Adresse** kann in einer Anwendung auch leer gelassen werden. Wenn im verknüpften Datensatz das Feld **IP-Adresse** existiert, wird die darin enthaltene Adresse verwendet. Wenn das Feld leer ist, erscheint ein Pop-up, in welchem Sie die gewünschte IP manuell eintragen.

Sie haben auch die Möglichkeit, mehrere Datensätze mit einer RDP-Anwendung zu verbinden. Auf diese Art und Weise können mehrere Benutzer mit einer RDP-Verbindung verknüpft werden.



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

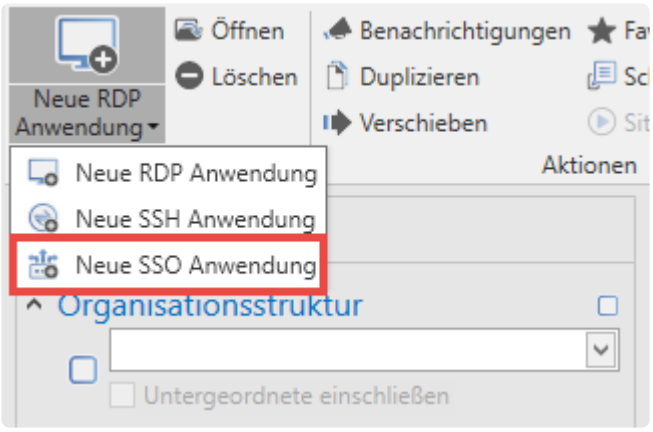
SSO Anwendungen

Was passiert beim Anlernen?

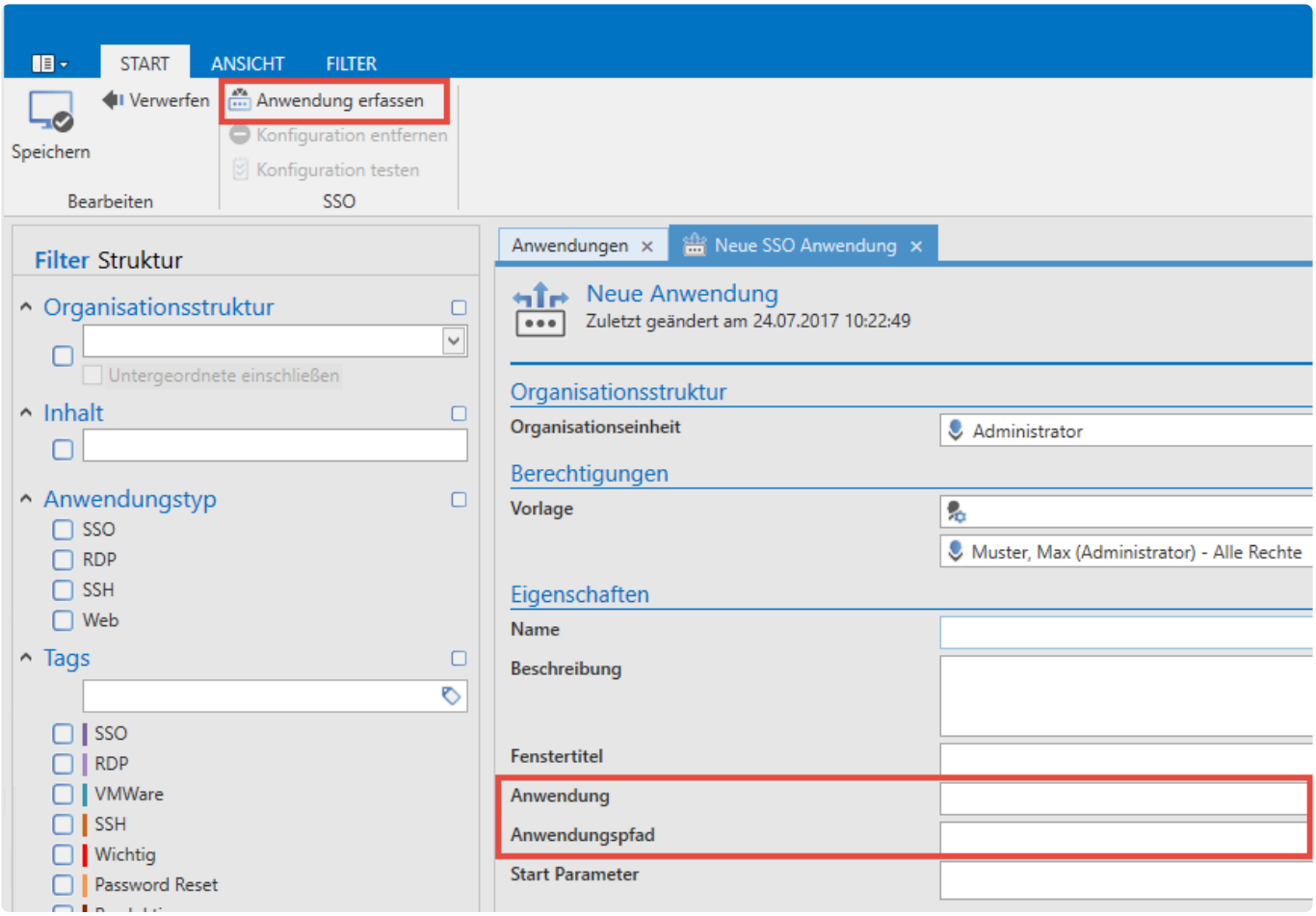
Beim Anlernen einer Anwendung werden die Schritte festgelegt, die nötig sind, um Benutzername und Passwort automatisch in eine Anwendung einzutragen. Das Ergebnis ist eine Art Skript, das definiert, wo genau die Anmeldedaten eingetragen werden sollen. In Password Safe wird die fertiggestellte Arbeitsanweisung **Anwendung** genannt.

Konfiguration

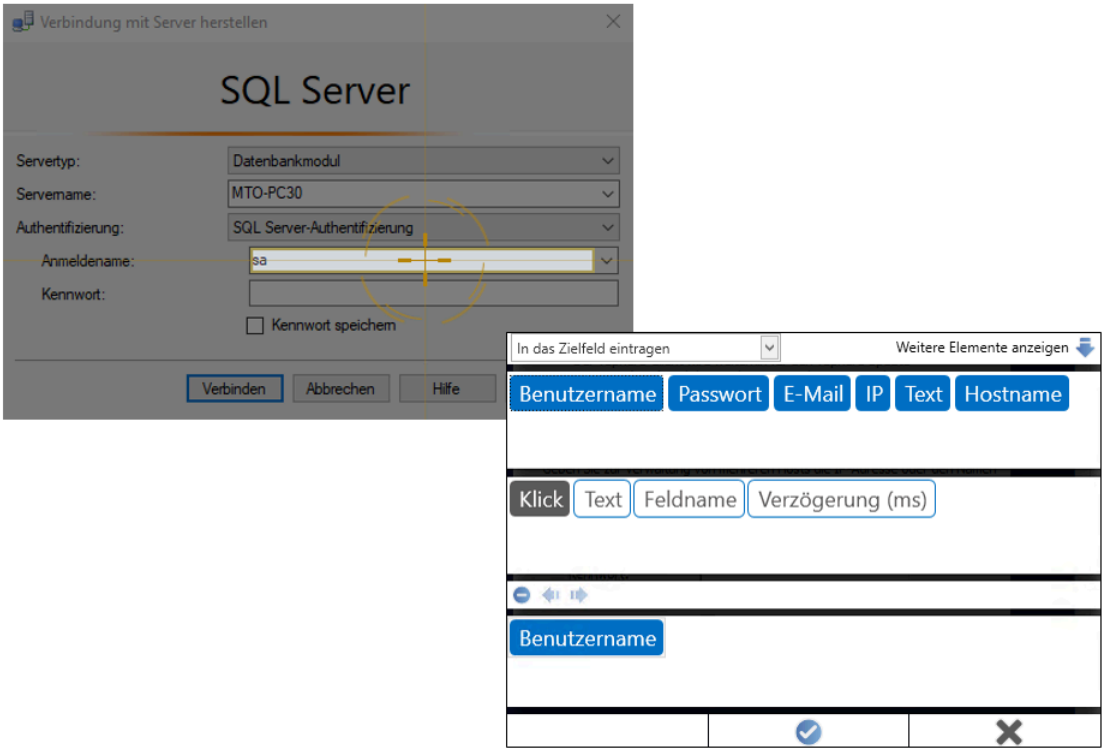
Im ersten Schritt erstellen Sie über die Ribbon eine neue SSO Anwendung.



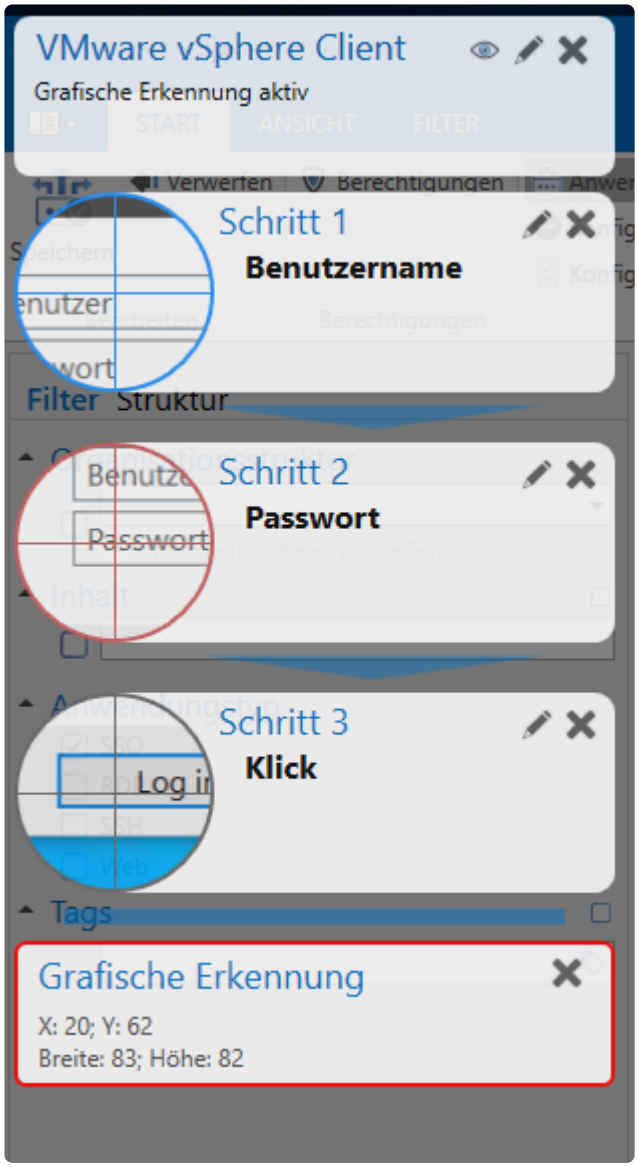
Zunächst definieren Sie die verschiedenen Eigenschaften für die Anwendung. Die Felder **Fenstertitel**, **Anwendung** sowie **Anwendungspfad** können Sie nicht manuell befüllen. Dies erfolgt über den Button **Anwendung erfassen** in der Ribbon:



Nun können Sie über ein Fadenkreuz die Zuweisung der Zielfelder vornehmen. Nachfolgend ist zu sehen, wie die Feldzuweisung für den Benutzernamen am Beispiel der Anmeldung an SQL Server abläuft. Alle weiteren Felder werden über den gleichen Weg zugeordnet. Die Vorgehensweise ist immer dieselbe: Sie wählen das Feld aus welches befüllt werden soll und entscheiden dann, mit welchen Information.

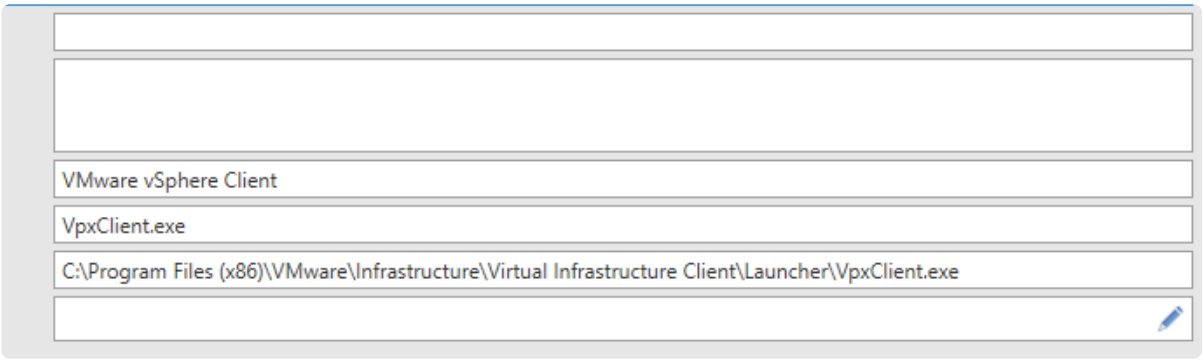


Parallel zum vorherigen Arbeitsschritt wird am rechten Bildschirmrand jede bereits getätigte Zuweisung angezeigt. In diesem Beispiel wurden dem VMware vSphere Client drei Anweisungen gegeben: Benutzername, Passwort sowie das Klicken des Buttons für die abschließende Anmeldung.



Grafische Erkennung:
Die Grafische Erkennung ist ein **zusätzlicher Schutz**. Sie können darüber weitere Faktoren für den SSO bestimmen. Hierfür legen Sie einen Bereich fest, der dann als Ausgang für den Abgleich dient (z.B. bei Anmeldemasken mit Bild). Um die Grafische Erkennung zu aktivieren, klicken Sie – nach der Zuweisung der Felder – auf das Auge rechts oben. Daraufhin markieren Sie den gewünschten Bereich.

Haben Sie alle Felder zugewiesen, verlassen Sie mit der Eingabetaste die Anwendungserfassung. Es werden nun die Felder “Fenstertitel”, “Anwendung” und “Anwendungspfad” automatisch befüllt.



Hier ist zu sehen, dass direkt auf die .exe Datei verwiesen wird. Wenn das entsprechende Tool oder Programm bei allen Anwendern am selben Ablageort gespeichert ist, kann diese Anwendung auch von allen Benutzern angesprochen werden.

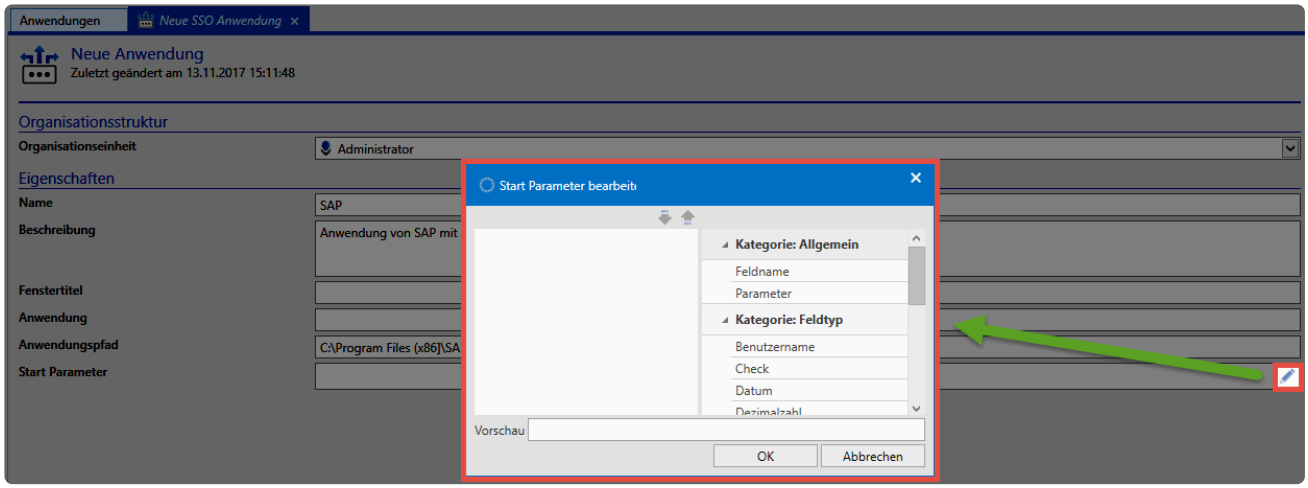
Startparameter für SSO Anwendungen

Startparameter für SSO Anwendungen

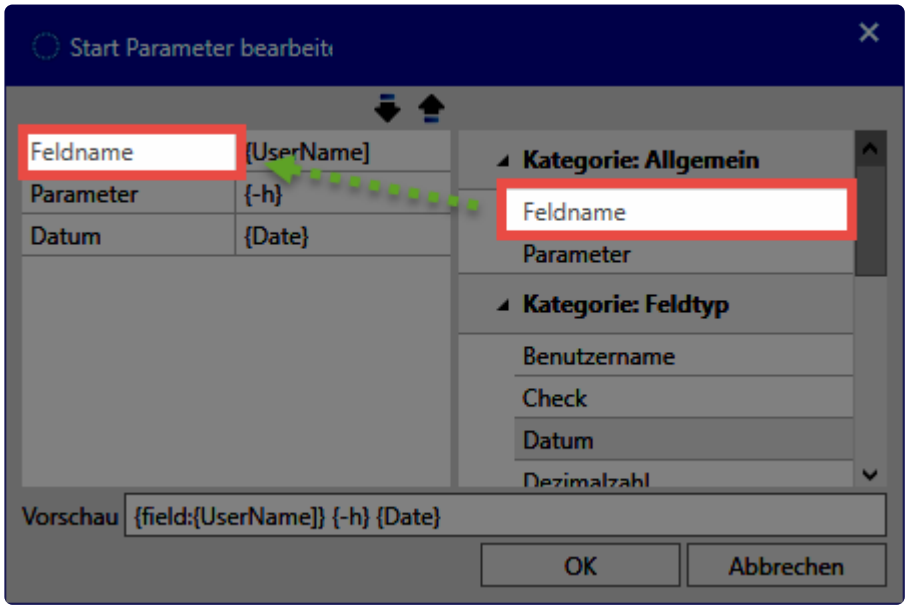
Beim Erstellen bzw. Bearbeiten einer SSO Anwendung können Startparameter definiert werden. Diese werden dann beim Start der Anwendung direkt mit übergeben – beispielsweise um das Programm direkt mit diversen Grundeinstellungen zu starten. Die entsprechenden Parameter sind direkt beim Hersteller der Software 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 Sie die benötigten Elemente per Drag&Drop von der rechten auf die linke Seite ziehen.



Hier stehen verschiedene Kategorien zur Verfügung:

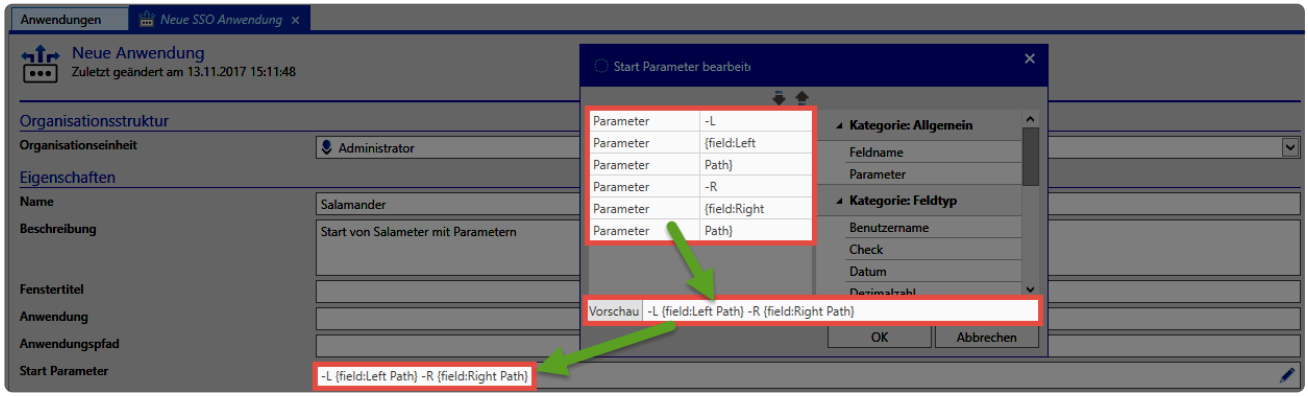
- Über **Parameter** werden lediglich die Parameterbezeichnungen **Feldname** oder **Parameter** vorgegeben. Diese müssen dann manuell ergänzt werden.
- über die Parameter der Kategorie **Feldname** können Felder direkt angesprochen und so direkt die Feldnamen übergeben werden.

Beispiel

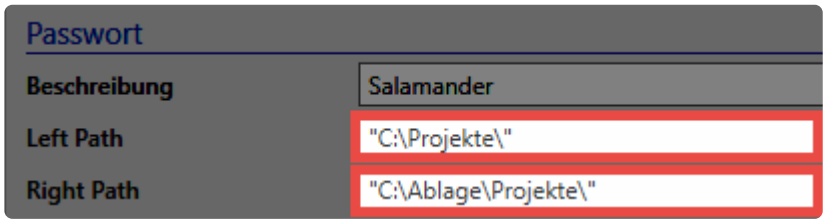
In diesem Beispiel wurden für die Anwendung Salamander folgende Startparameter definiert:

- -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

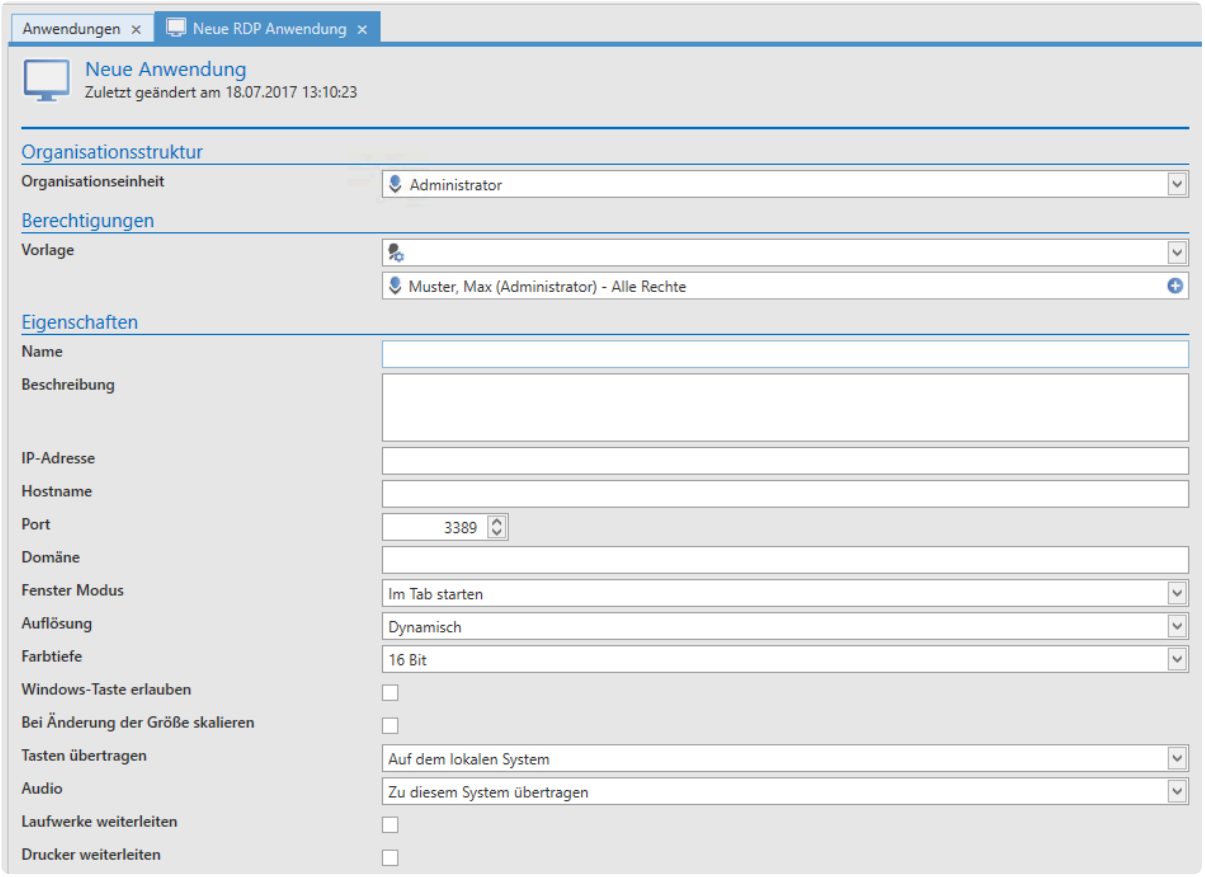
Text	{Text}
Passwort	{Password}
Datum	{Date}
Check	{Check}
URL	{Url}
E-Mail	{Email}
Telefon	{Phone}
Liste	{List}
Überschrift	{Header}
Mehrzeiliger Text	{Memo}
Mehrzeiliger Passwort Text	{PasswordMemo}
Ganzzahl	{Int}
Gleitkommazahl	{Decimal}
Benutzername	{UserName}
IP-Adresse	{Ip}
Feldname eingeben	{field:name}

RDP und SSH Anwendungen

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

Erstellen von RDP und SSH Anwendungen

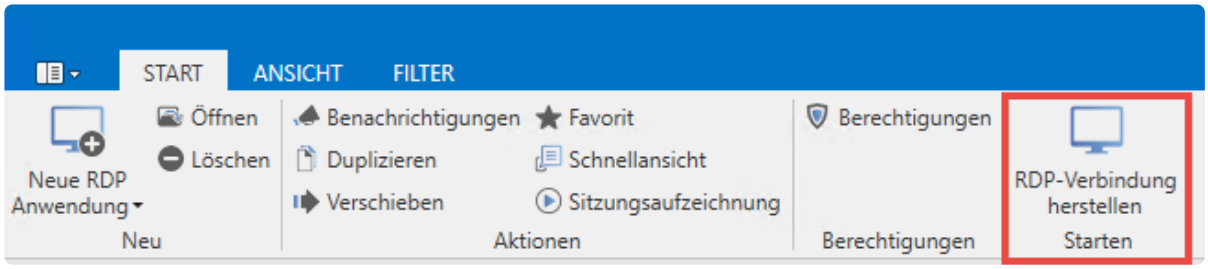
Eine neue RDP- oder SSH- Anwendung kann über die Ribbon oder das Kontextmenü der rechten Maustaste erstellt. Es erscheint das entsprechende Formular, in dem Sie die Variablen für eine Verbindung definieren.



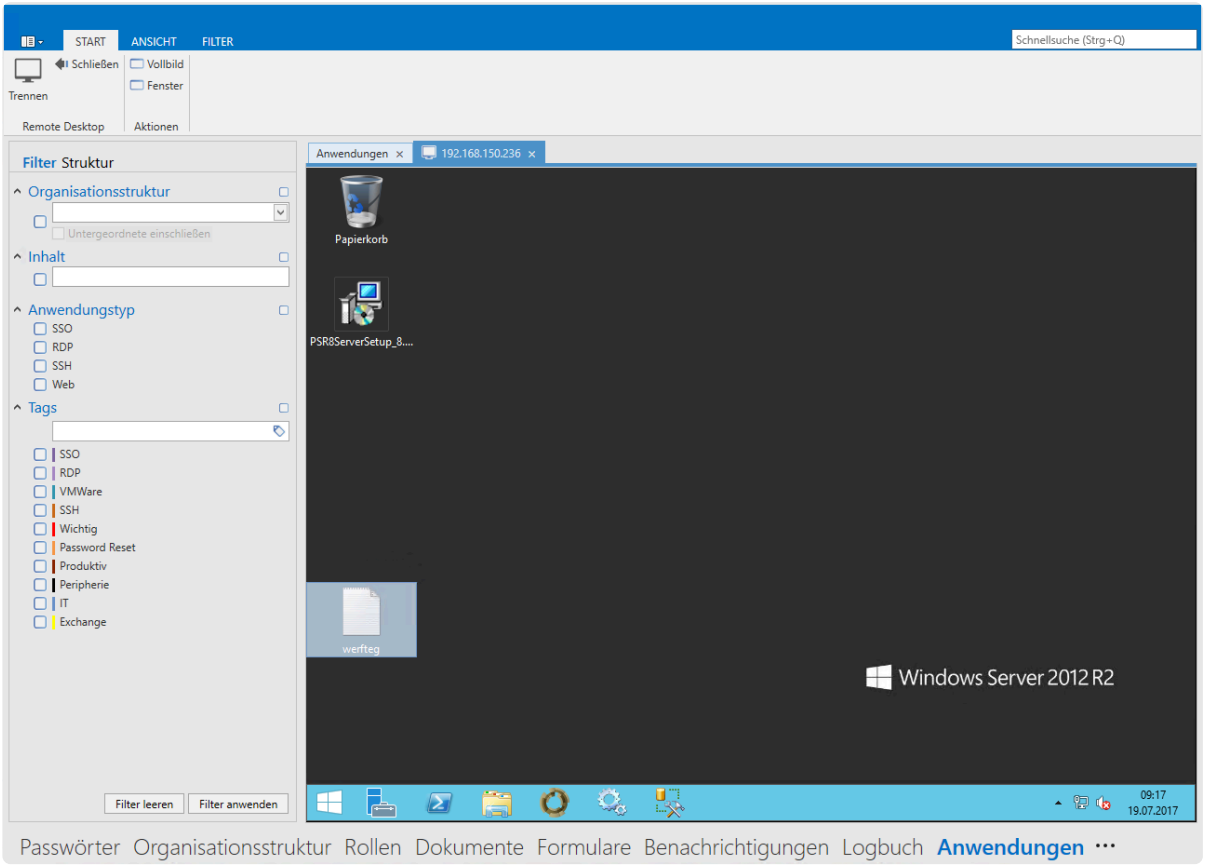
Diese Variablen entsprechen genau denjenigen, die man (hier am Beispiel RDP) bei der Erstellung einer RDP-Verbindung über “mstsc” konfigurieren kann. Im **Fenstermodus** wird definiert, ob die Verbindung in einem Tab, im Vollbildmodus oder in einem separaten Fenster gestartet werden soll.

Arbeiten mit RDP- und SSH-Anwendungen

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



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



Anmeldung über SSH-Zertifikate

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

Tastaturkürzel

Password Safe unterstützt verschiedene Tastaturkürzel zum Übertragen von – beispielsweise – Benutzernamen und Passwort in die entsprechende Anwendung. Hierbei ist jedoch zu beachten, dass

dies nur funktioniert, wenn die Anwendung direkt aus Password Safe heraus geöffnet wird.

RDP und SSH 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 und anschließend anzusehen und auszuwerten. Hierbei ist es auch möglich diese so einzuschränken, dass nur der Benutzer selbst oder eine zugewiesene Person, wie z.B. ein Sicherheitsbeauftragter, Zugriff auf diese Aufzeichnungen hat.

Passwörter Dokumente Benachrichtigungen Organisationsstruktur Rollen Formulare Logbuch **Anwendungen** Password Reset

Relevante Rechte

Folgende Optionen werden benötigt um Sitzungen von Anwendung verwalten zu können.

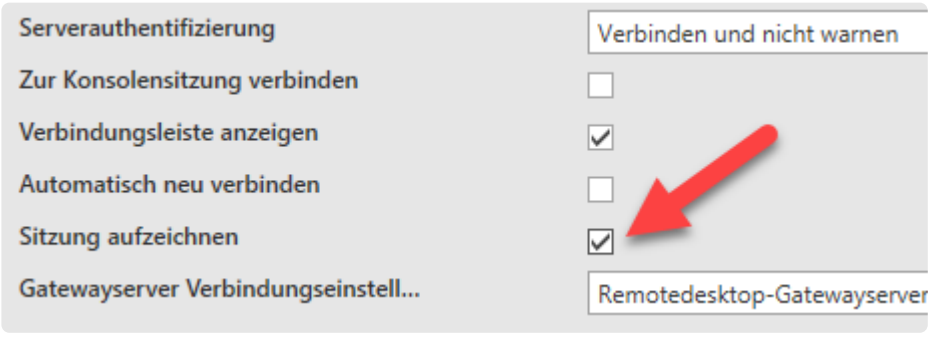
Benutzerrecht

- kann Aufzeichnungen einer Anwendung verwalten

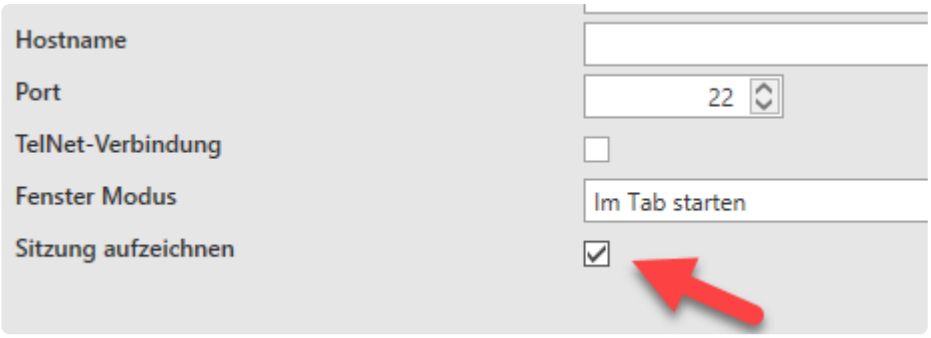
> Beachten Sie, dass die Sitzungsaufzeichnung Speicherplatz innerhalb der Datenbank benötigt. Die Aufnahmen werden zwar Ressourcensparend abgelegt, jedoch variiert die Speichergröße sehr stark mit dem Inhalt. Je mehr in der aufgezeichneten Sitzung passiert, umso höher ist auch der Speicherverbrauch.

Die Sitzungaufzeichnungen müssen bei der jeweiligen RDP- oder SSH-Anwendung erst aktiviert werden.

RDP



SSH

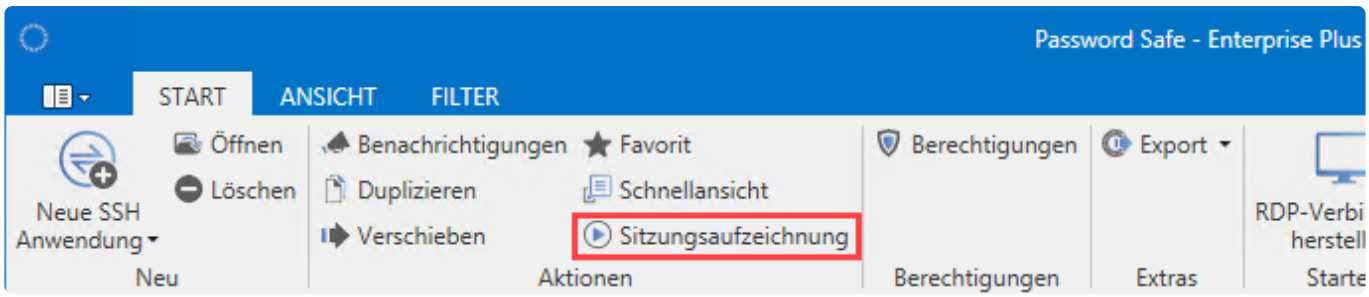


Ist die Einstellung aktiviert, so wird beim nächsten Verbindungsaufbau die Aufzeichnung automatisch gestartet.

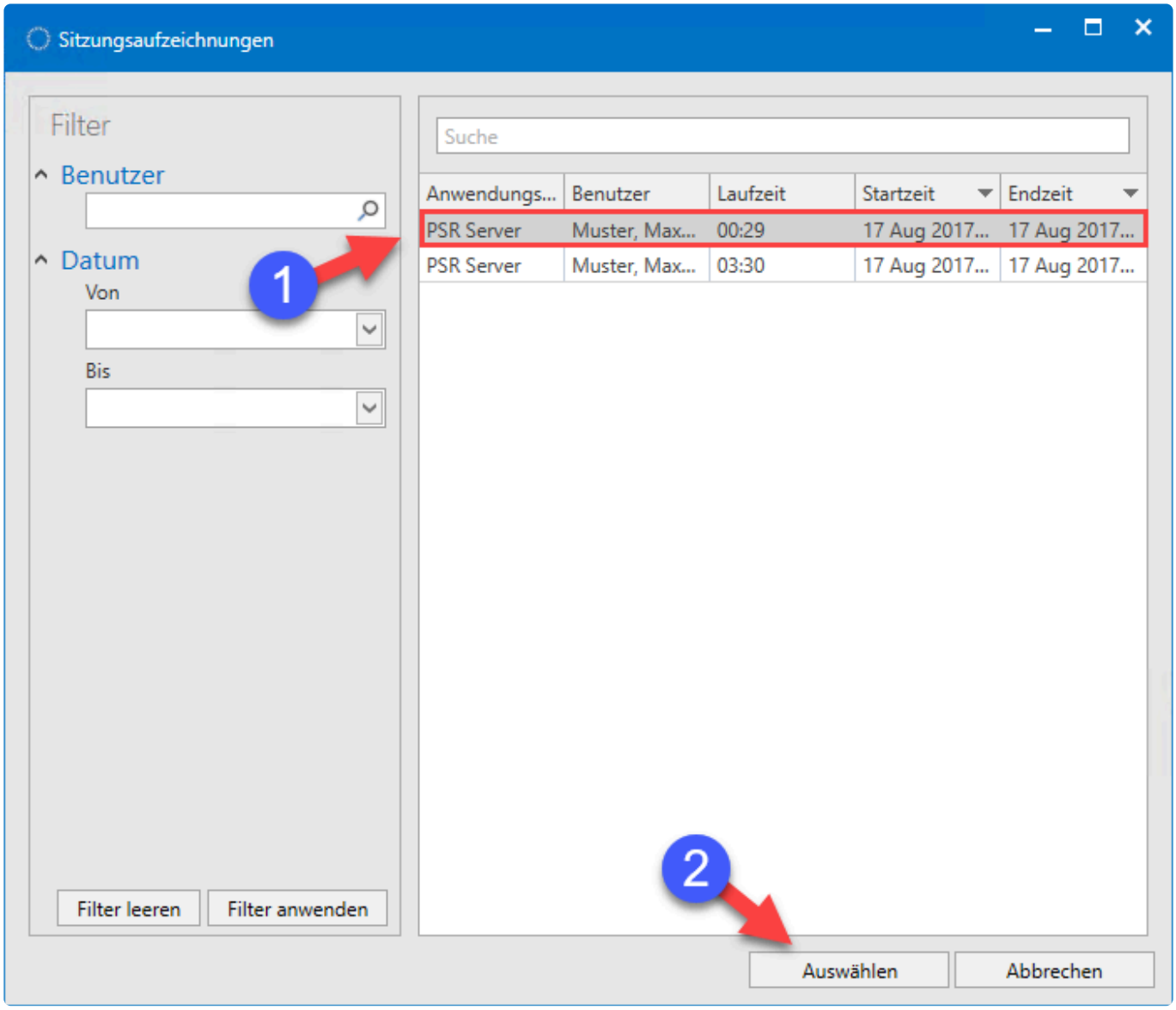
> Die Aufzeichnungen werden bereits während der Aufnahme zum Server und in die Datenbank gestreamt. Somit gehen auch bei einem Verbindungsabbruch keine Aufzeichnungen verloren und sind bis zu einem Verbindungsabbruch oder Ende der Sitzung sofort gespeichert.

Sitzungsaufzeichnungen ansehen

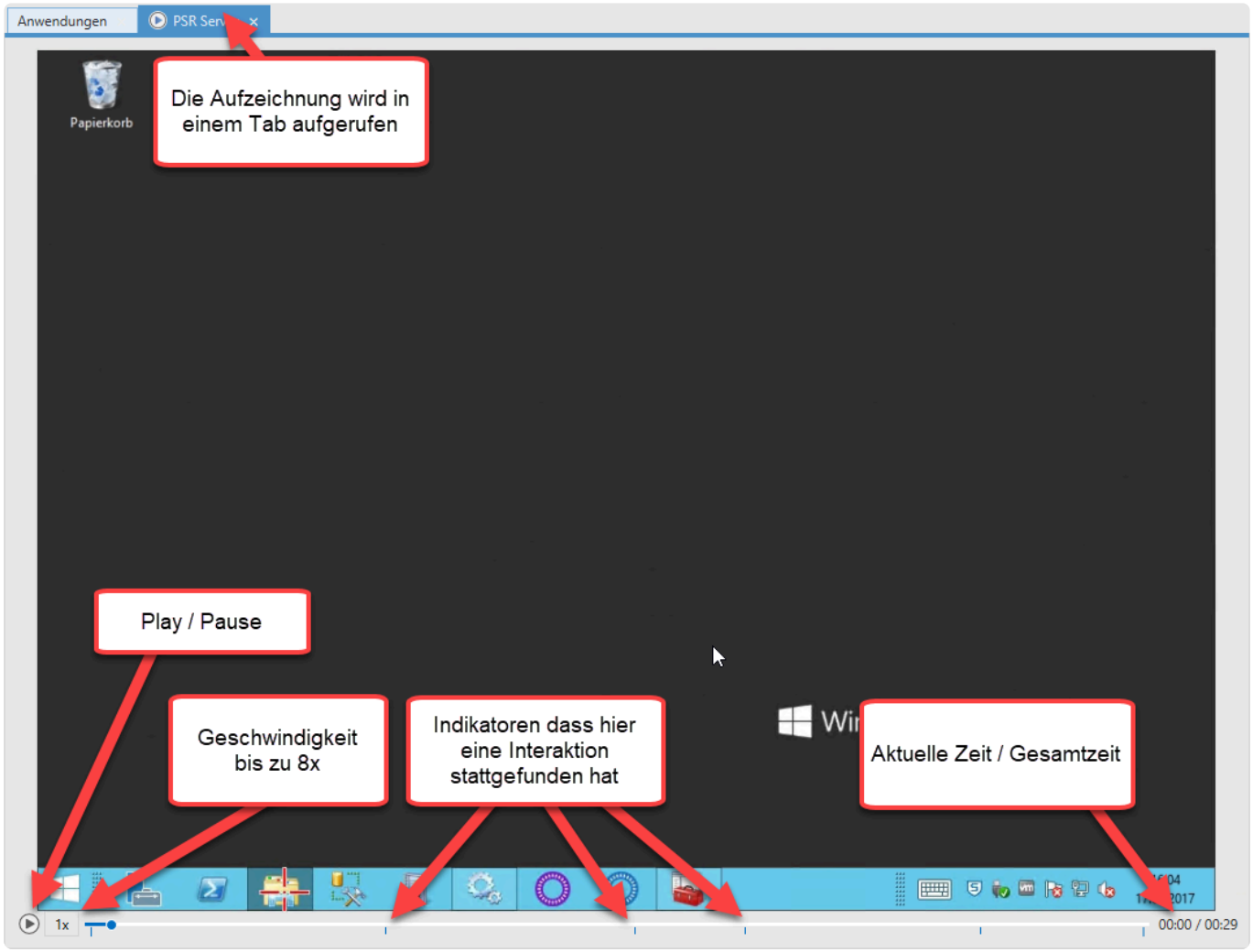
Sind Aufzeichnungen für eine Anwendung vorhanden, so können diese im Modul Anwendungen aufgerufen und angesehen werden.



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 schnell vorgespult werden, um nur die relevanten Aktionen zu sehen.



Wann werden Indikatoren gesetzt?

- Mausklick
- Tastaturbefehle

Automatisches Löschen alter Aufzeichnungen

Falls gewünscht können Aufzeichnungen automatisch gelöscht werden. Diese Option wird am **AdminClient** konfiguriert. Weitere Informationen finden Sie sind im Kapitel Verwaltung von Datenbanken.

SAML Anwendungen

Was ist SAML?

Die Security Assertion Markup Language (SAML) ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.
Das bedeutet, dass man sich mit einen Satz von Anmeldeinformationen bei vielen verschiedenen Webseiten anmelden kann. Es ist viel einfacher, eine Anmeldung pro Benutzer zu verwalten, als separate Anmeldungen für E-Mail, Customer Relationship Management- (CRM) Software, das Active Directory usw.

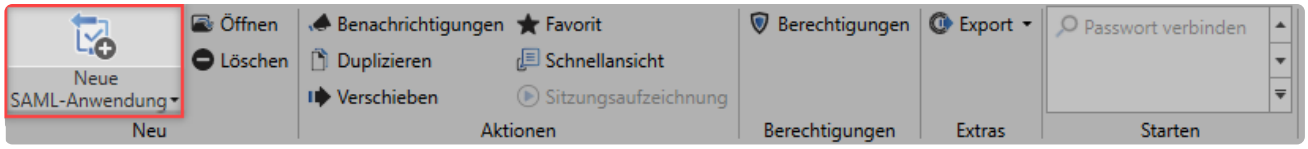
Voraussetzungen

Damit die Benutzer SAML nutzen können, muss SMTP eingerichtet und bei den entsprechenden Benutzern eine E-Mailadresse hinterlegt sein.
Außerdem ist der WebClient zwingend erforderlich. Daher muss der WebClient bereits eingerichtet bzw. installiert sein.

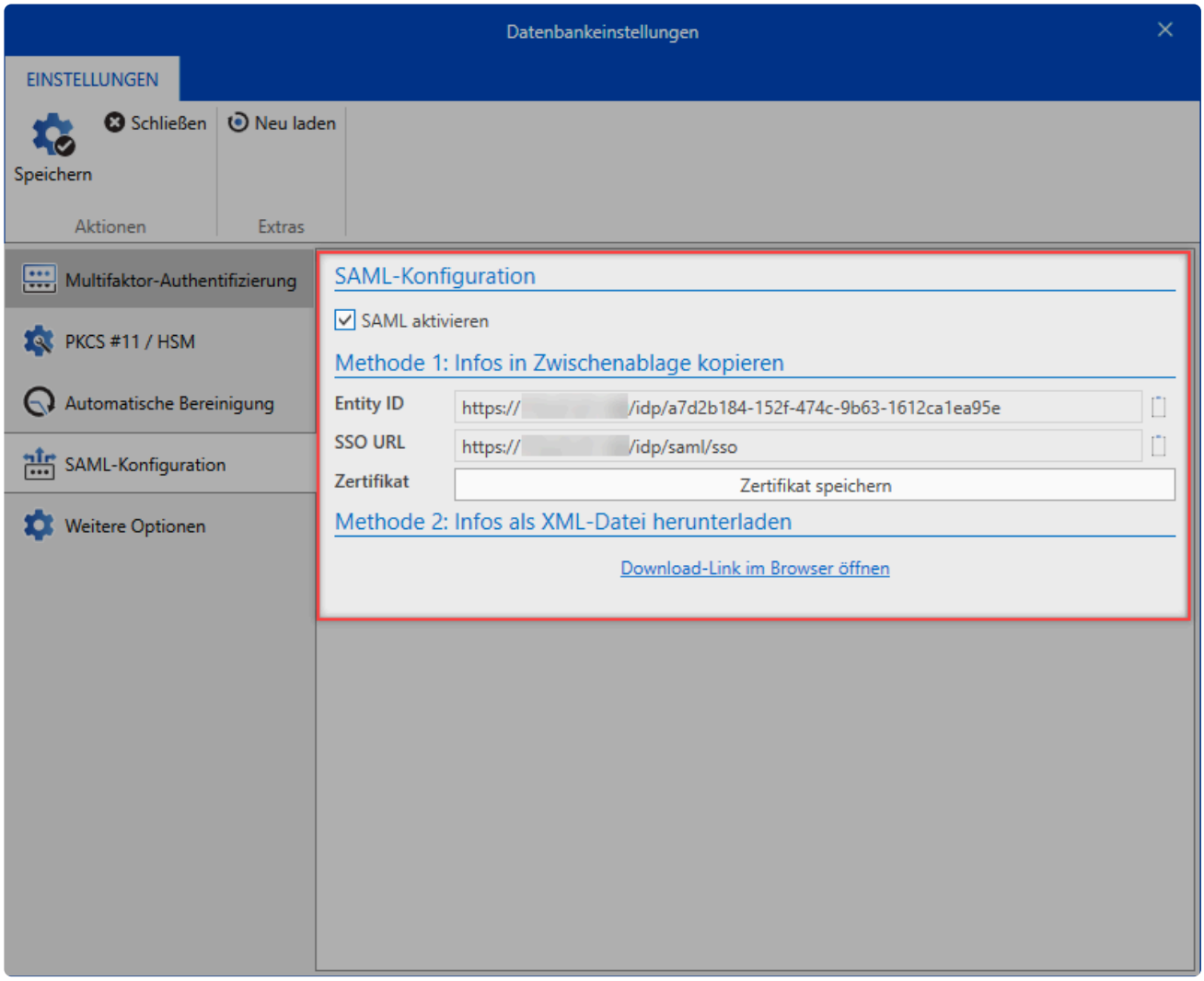
Konfiguration

Damit Sie **SAML Anwendungen** angelegen können, muss SAML zunächst einmal aktiviert werden.

Das geschieht über die Einstellungen der Datenbank im Admin Client:

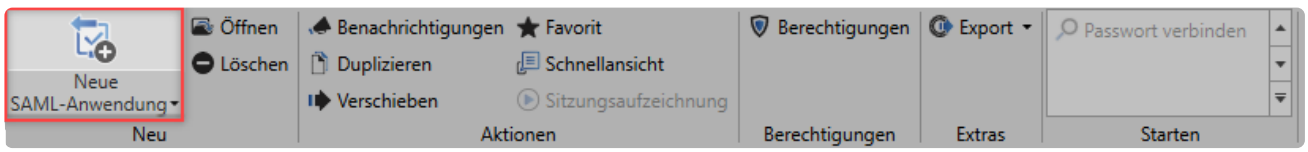


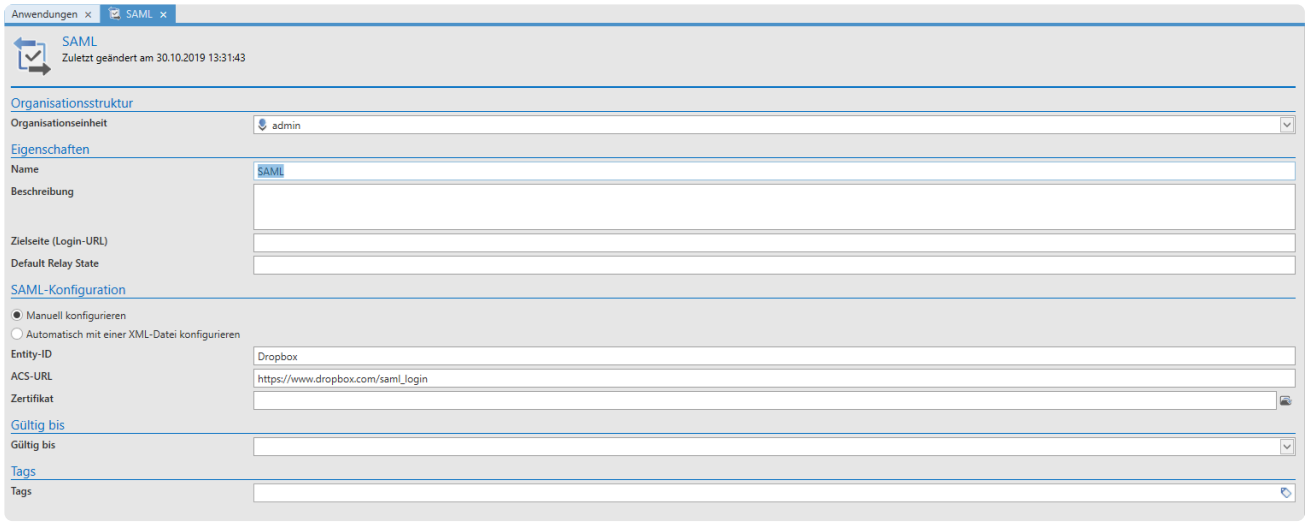
Sobald Sie die Checkbox angehakt haben muss als nächster Schritt die URL des WebClients hinterlegt werden. Daraufhin sollte das SAML-Konfigurationsfenster in etwa wie folgt aussehen:



Das Fenster wird offen gelassen und die Konfiguration wird am FullClient fortgesetzt.
Melden sich wie gewohnt am Client an und wechseln auf das Modul **Anwendungen**. Wählen Sie eine **neue SAML-Anwendung** aus und befüllen diese mit den relevanten Daten des Service Providers.

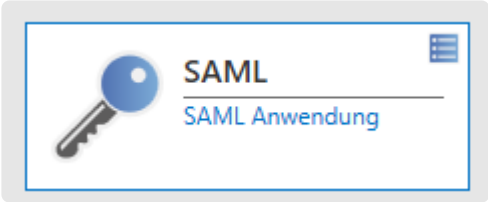
> Die Daten des Service Providers, die in den FullClient eingetragen werden, finden Sie beim jeweiligen Provider. Die Daten unterscheiden sich im Regelfall von Provider zu Provider.





Zusätzlich müssen die Daten im **Admin Client** beim Service Provider hinterlegt werden.

Als letzter notwendiger Schritt muss der Benutzer noch verifiziert werden. Dies erfolgt durch einen Klick auf die Kachel. Dadurch erhält der Benutzer eine E-Mail mit der er sich verifizieren kann.



Nach der Verifizierung kann die **SAML-Anwendung** über die LightClient-Ansicht gestartet werden.

! Da es sich hierbei um eine passwortlose Authentifizierung handelt, ist auch keine Verknüpfung der **SAML-Anwendung** mit einem Passwort nötig.

✻ Beispielhaft zeigen wir Ihnen die Einrichtung und Konfiguration für **Dropbox** oder **Postman**.

Beispiele für Anwendungen

Folgend finden Sie Beispiele aus Praxis zum Erstellen von Anwendungen:

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

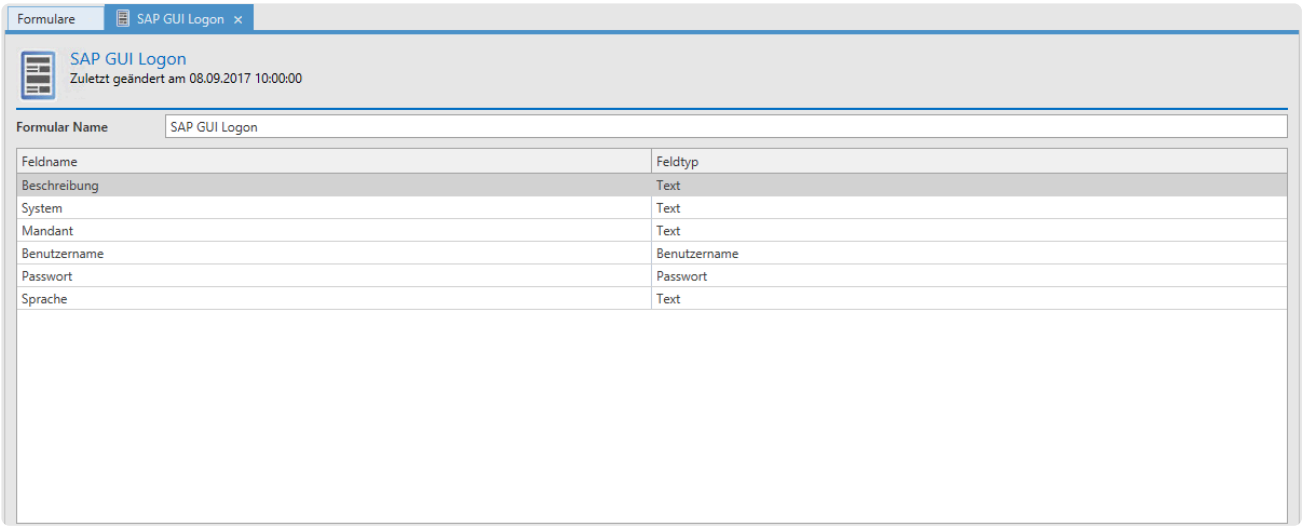
SSO-Anwendung für SAP GUI Logon

Grundlegende Informationen

Die Anmeldung an SAP kann über Startparameter realisiert werden. Dafür muss die Anmeldung über “SAPshortcut” ausgeführt werden.
Unter SAP Wiki werden alle verfügbaren Parameter gelistet.

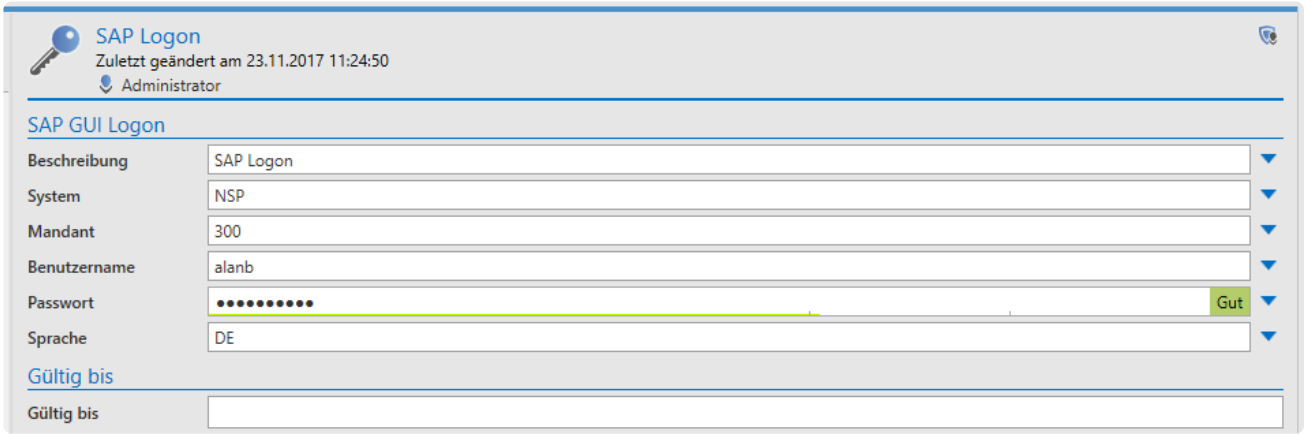
Formular

Erzeugen Sie zunächst ein Formular mit den benötigten Feldern. Dies könnte wie folgt aussehen:



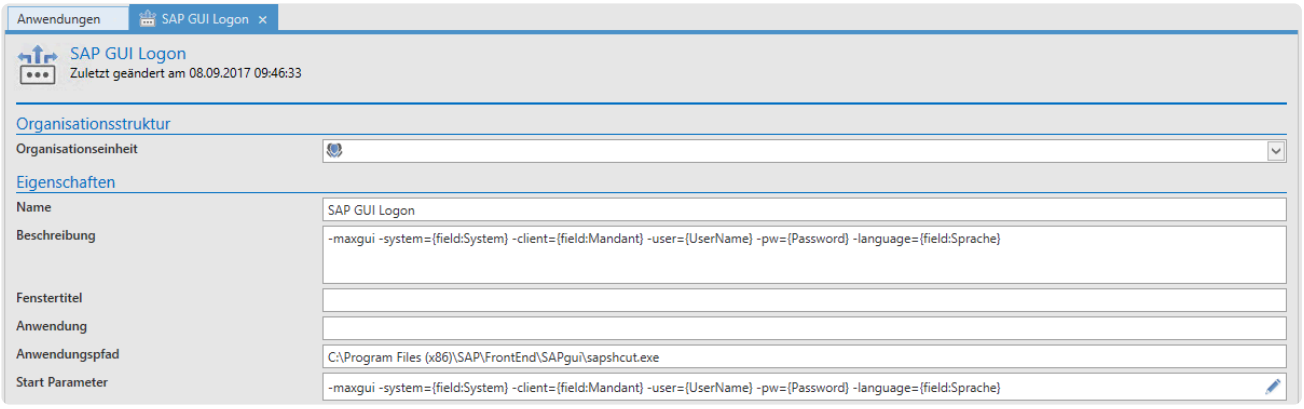
Datensatz

Über das Formular wird dann ein entsprechender Datensatz erstellt:



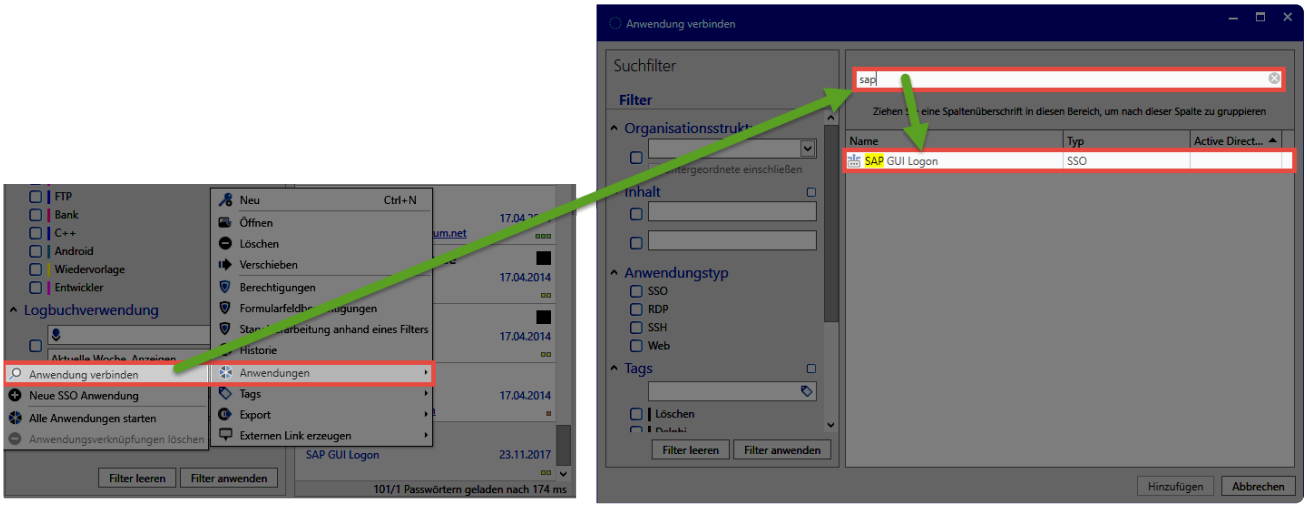
Anwendung

Nun müssen Sie eine entsprechende SSO Anwendung erstellen.



Verknüpfung

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



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

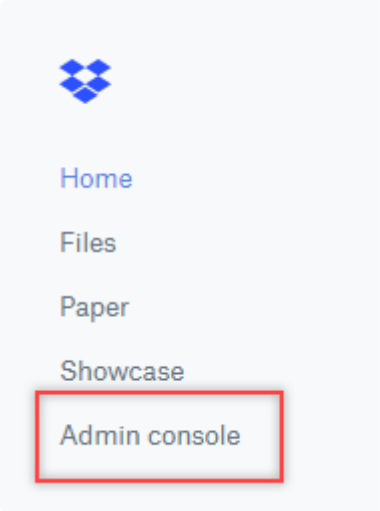
SAML-Anwendung für Dropbox

SAML-Konfigurationsbeispiel für Dropbox

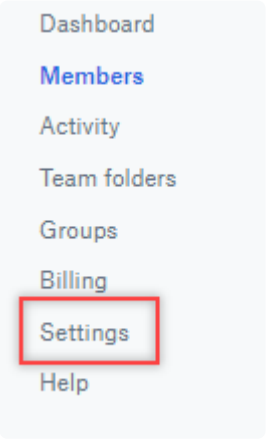
Zur Konfiguration muss SAML bereits am Admin Client aktiviert sein..

1. Als Administrator an der **Dropbox** anmelden

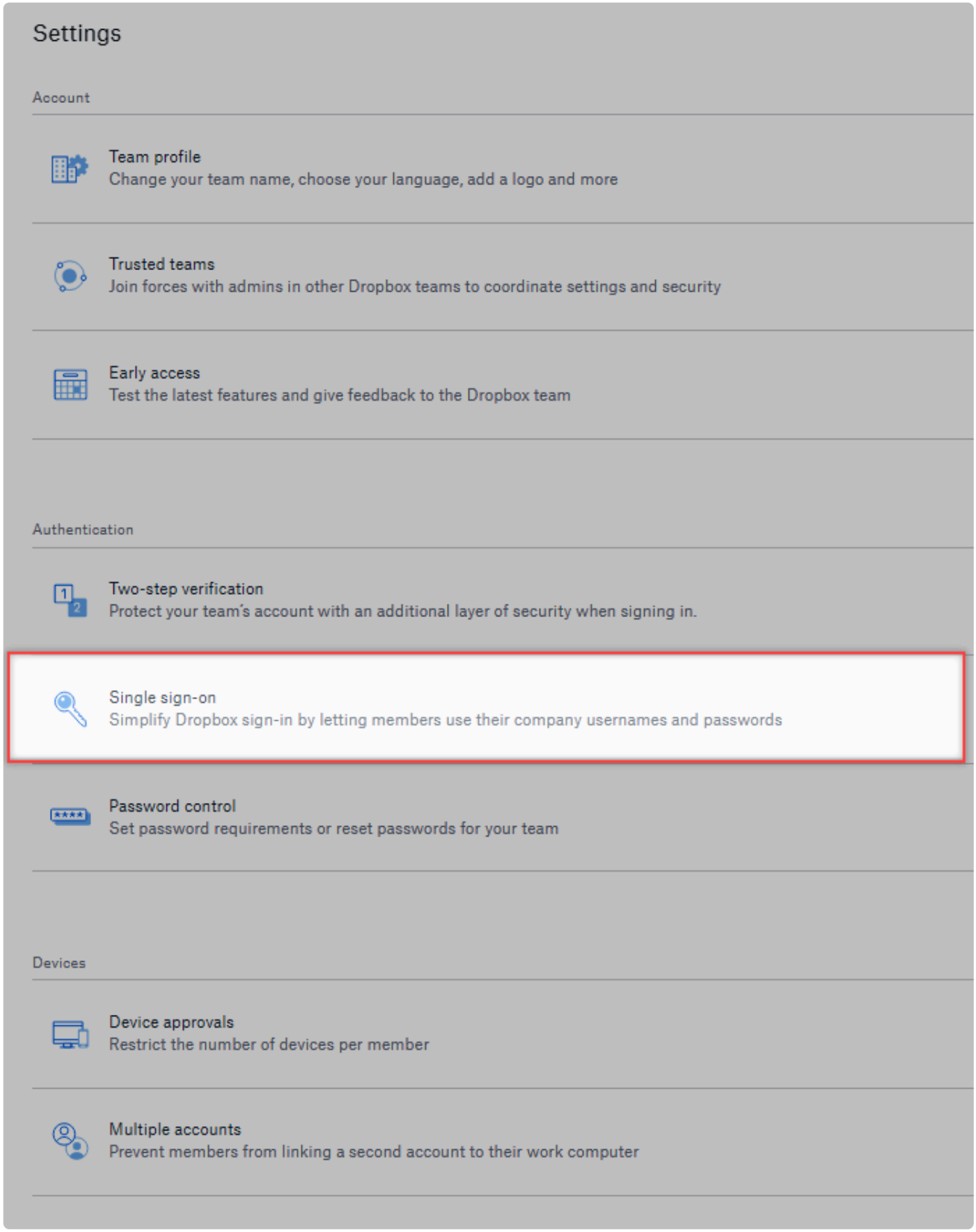
2. Die Admin Console öffnen



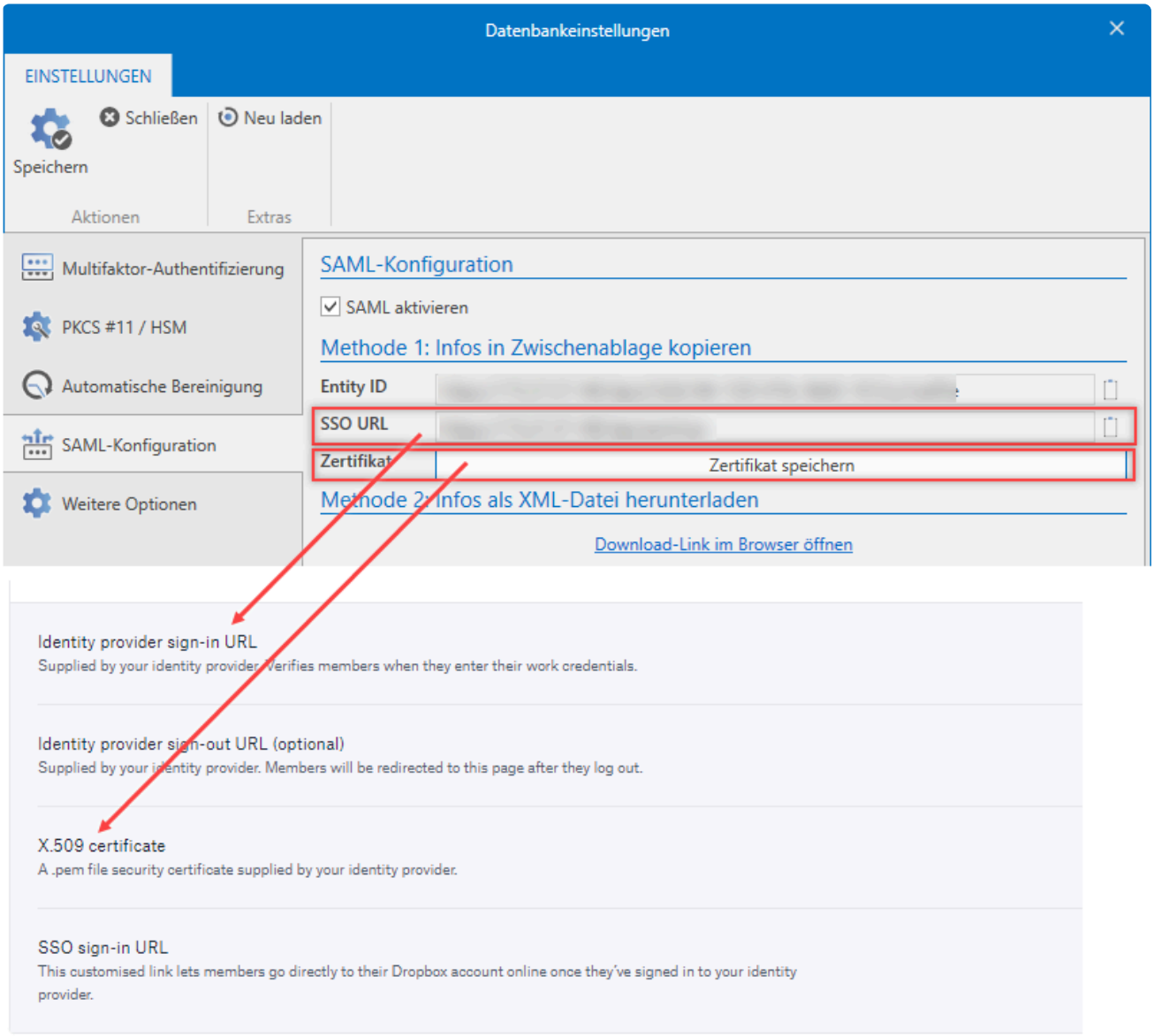
3. Settings öffnen



4.Single Sign On

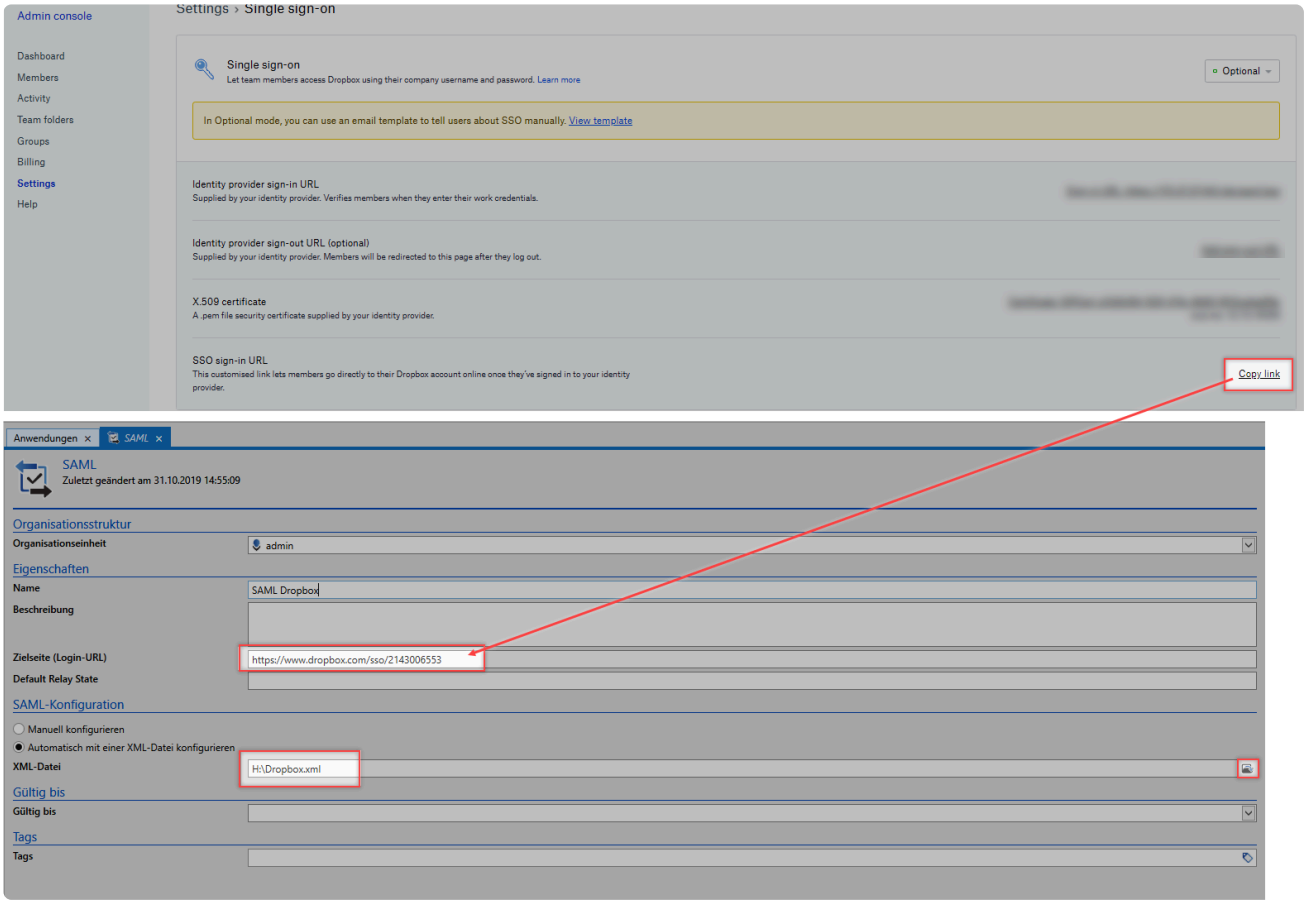


5. Die Daten **SSO URL** und das **Zertifikat** aus dem Admin Client hinterlegen.



6. Im FullClient muss beim Modul Anwendungen eine neue **SAML-Anwendung** erstellen.

7. Die Zielseite (Login-URL) und die XML-Datei in der Anwendung hinterlegen.



Die XML-Datei muss wie folgt aussehen.

8. Die Anwendung kann nun über den LightClient ausgeführt werden.

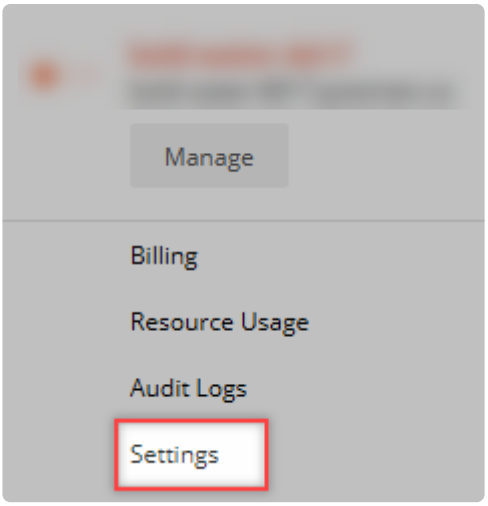
SAML-Anwendung für Postman

SAML-Konfigurationsbeispiel für Postman

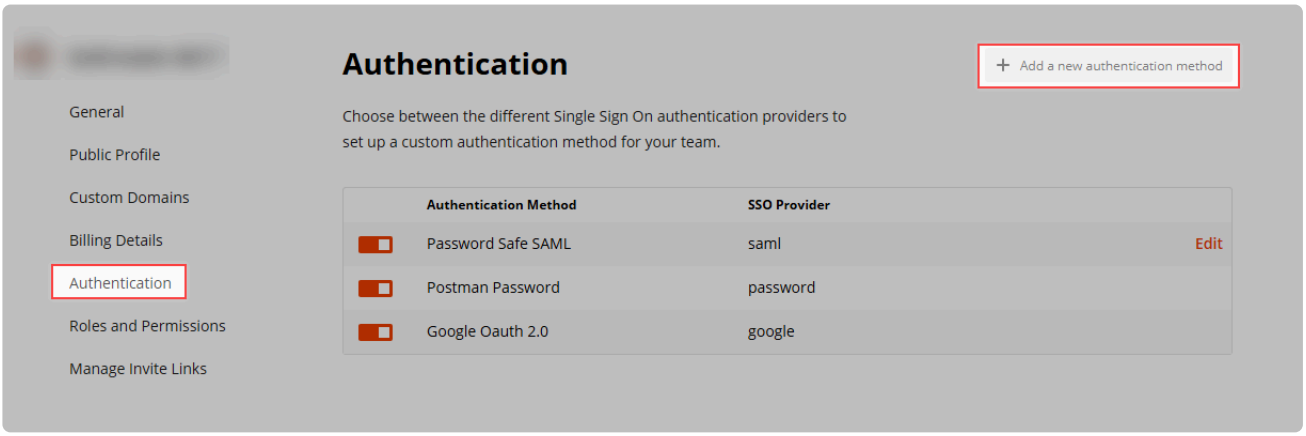
Zur Konfiguration muss SAML bereits am Admin Client aktiviert sein..

1. Bei Postman anmelden.

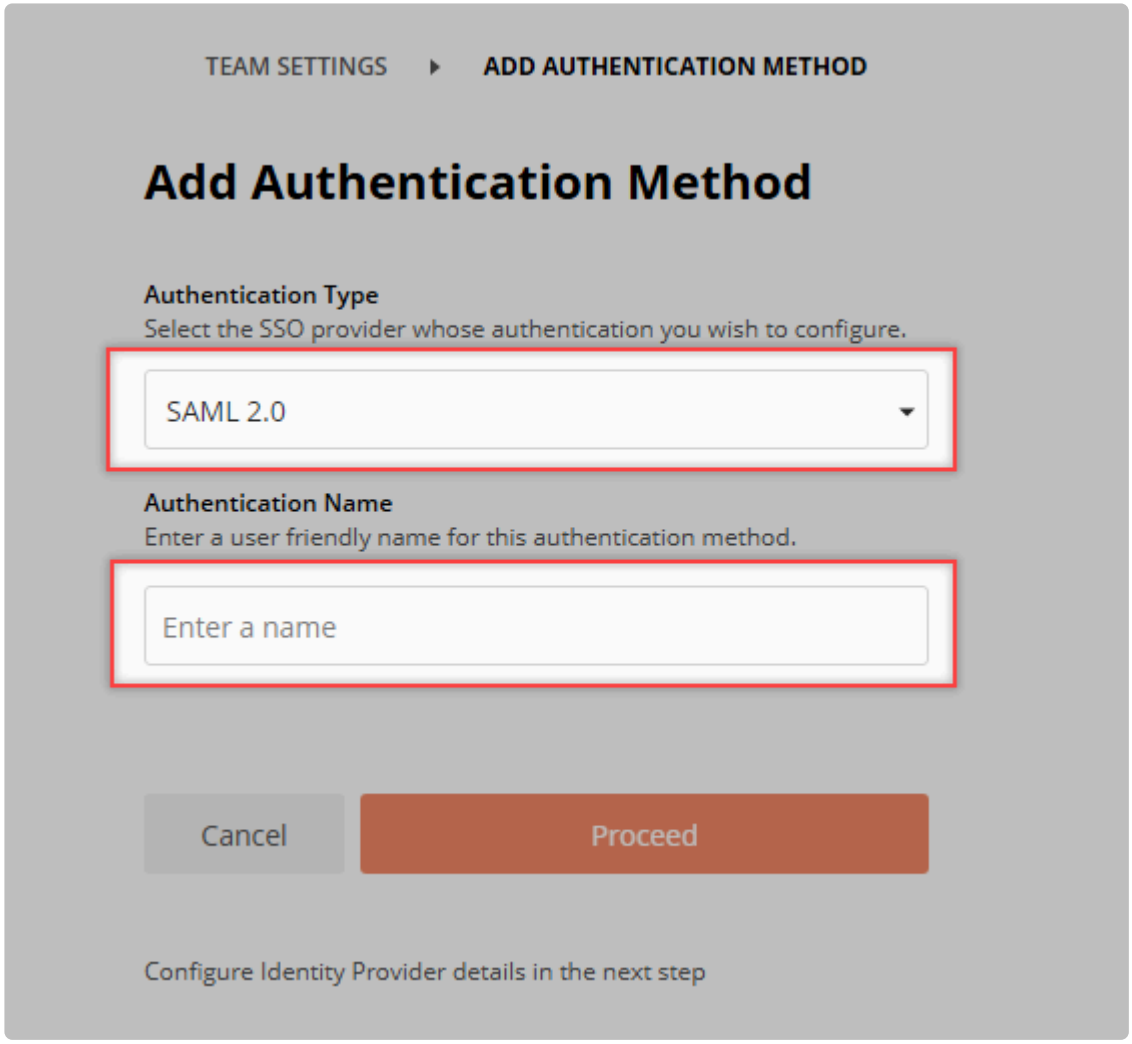
2. Auf den Avatar klicken und **“Settings”** auswählen .



3. Bei **Authentication** eine neue Methode auswählen.



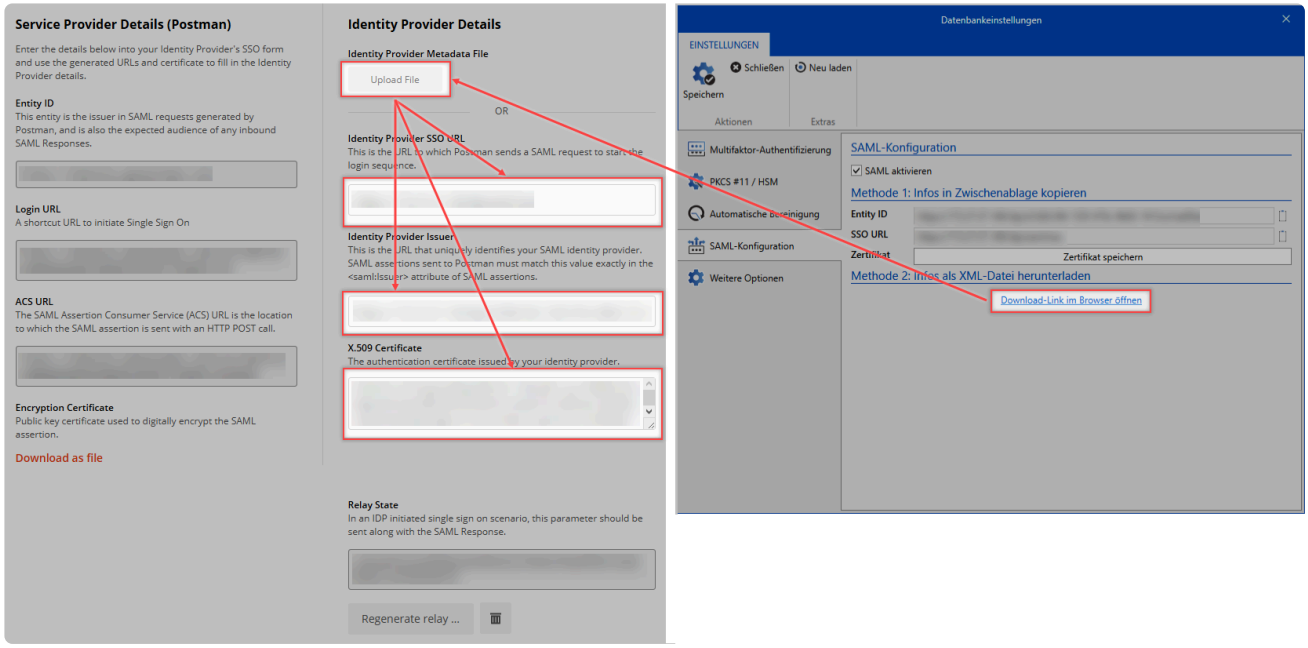
4. Authentication Type **SAML 2.0** auswählen und beliebigen, sinnvollen Authentication Namen festlegen.



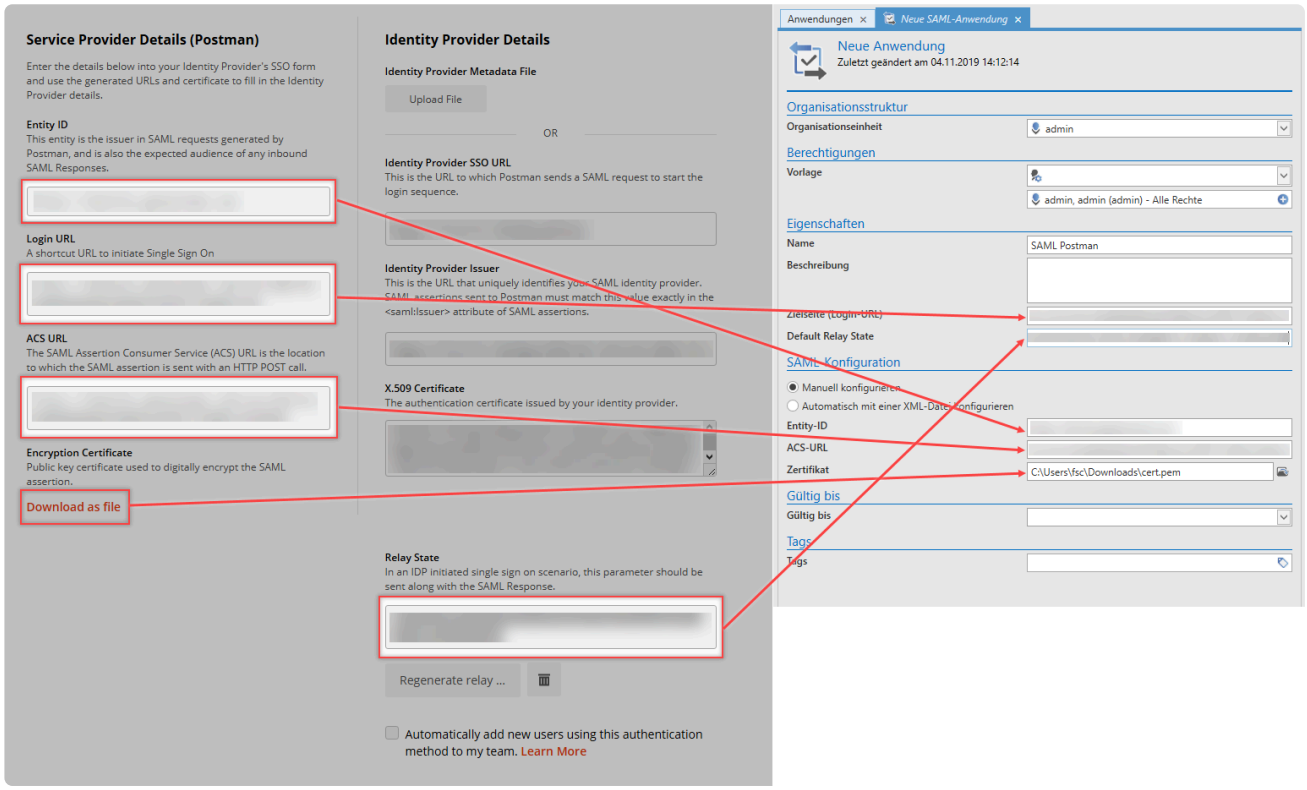
Daraufhin kommt man zur eigentlichen Konfiguration.

5. Provider Details hinterlegen

- **5.1 Identity Provider Details**
  Die Daten aus dem Admin Client werden als XML hochgeladen oder manuell hinterlegt.



- **5.2 Service Provider Details**
  Die Service Provider Details werden nun in die Anwendung im Password Safe Client kopiert

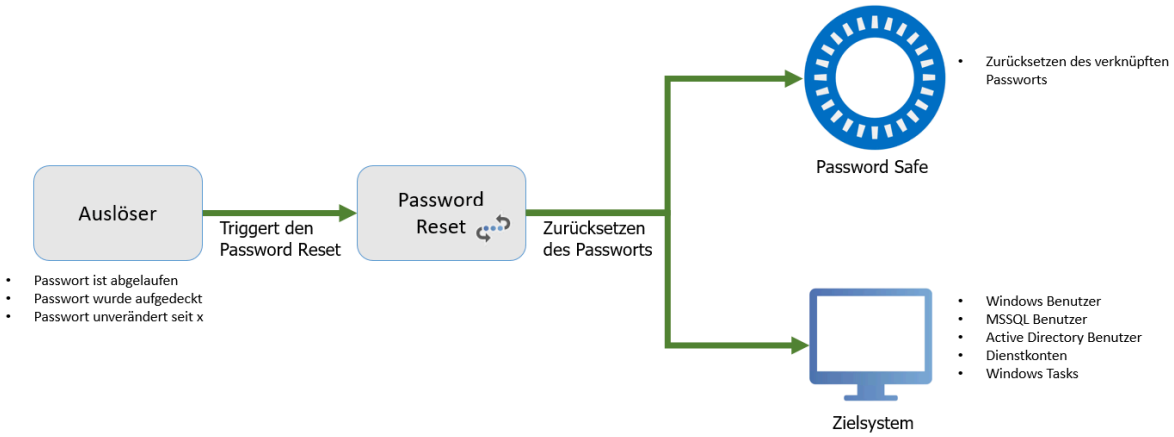


Es wird ein **Relay State** benötigt. Dieser Wert kann in der **Configure Identity Provider Details-View** erzeugt werden.

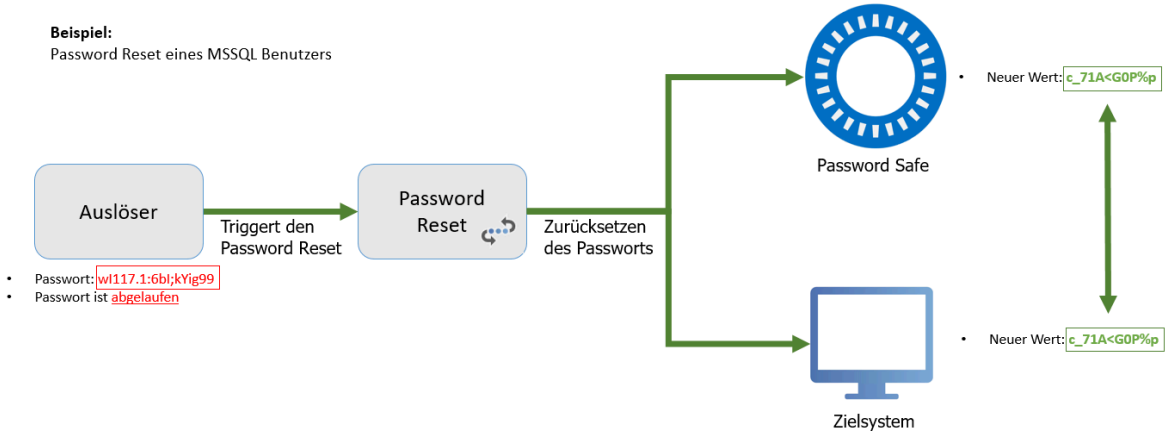
Password Reset

Was ist der 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.



Kommt es bei der Ausführung eines Password Resets zu einem Fehler, wird der betroffene Reset mit allen verbundenen Passwörtern blockiert. Dies wird im Logbuch mit einem Eintrag “blockiert” vermerkt. Weitere Informationen finden Sie im Kapitel **Logbucheinträge unter Passwort Reset**.

Aufgrund der Komplexität wird dringend empfohlen, dass der Password Reset **in Zusammenarbeit mit zertifizierten Partnern** konfiguriert wird. Die angestrebte

Arbeitserleichterung durch die Nutzung genannter Automatismen geht einher mit einer Vielzahl von Risiken.

Voraussetzungen

Verfügbarkeit

Das **Password Reset** ist ausschließlich in der **Enterprise Plus Edition** verfügbar.

Relevante Rechte

Für die Erstellung eines Password Resets werden folgende Optionen benötigt.

Benutzerrechte

- Kann neue Password Resets anlegen
- Password Reset Modul anzeigen

Voraussetzungen

- In Password Safe muss ein Datensatz hinterlegt sein, der auf dem jeweiligen Zielsystem administrative Rechte hat.
- Die Microsoft Remote Admin Tools müssen auf den Zielsystemen installiert sein.
- Das Zielsystem muss über das Netzwerk erreichbar sein.

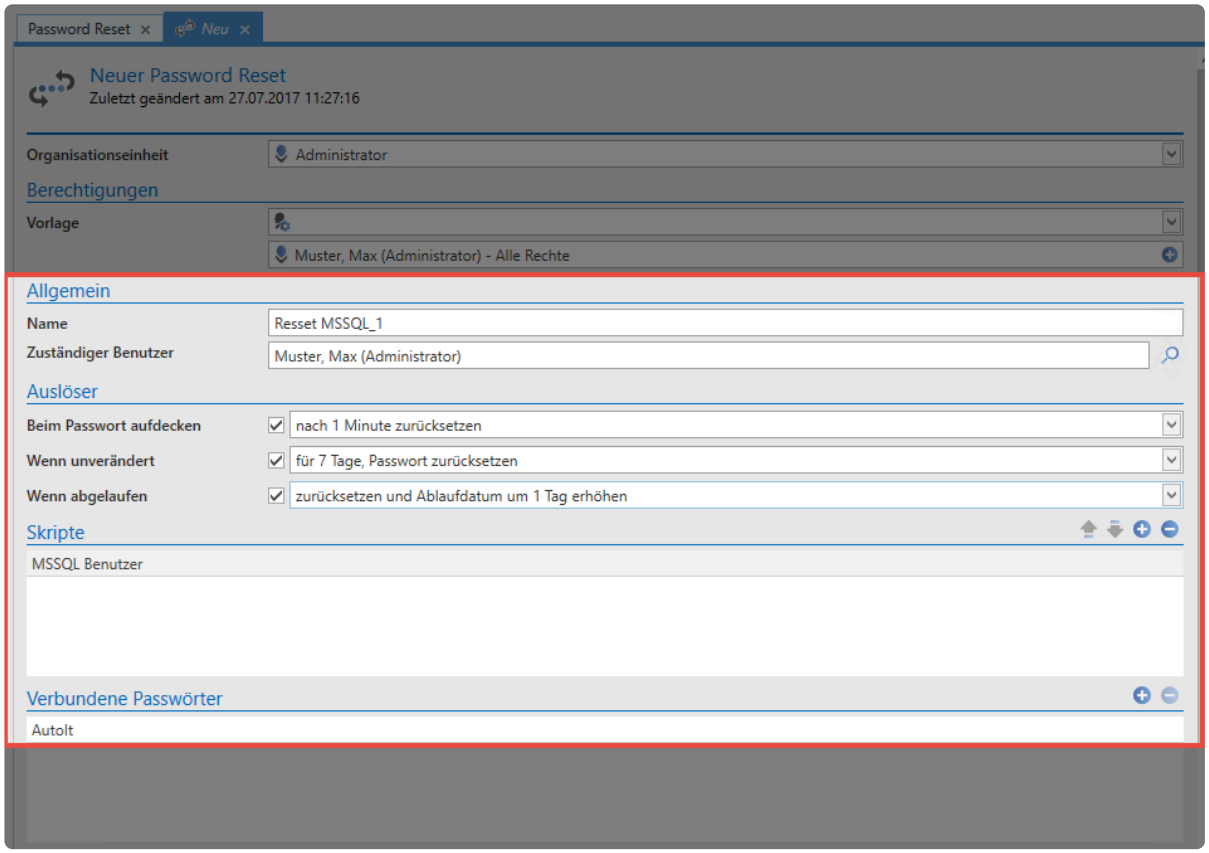
Konfiguration

Erstellen eines Password Resets

Ein neuer Password Reset kann über die Ribbon oder über das Tastenkürzel “Strg + N” im entsprechenden Modul angelegt werden.

Konfiguration

Die Konfiguration erfolgt in vier Schritten. In den Bereichen “Allgemein”, “Auslöser”, “Skripte” sowie “Verbundene Passwörter” werden alle notwendigen Bedingungen und Variablen definiert.



Allgemein

- **Name**: Bezeichnung für den Password Reset.
- **Zuständiger Benutzer**: Alle durchgeführten Password Resets werden protokolliert (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.

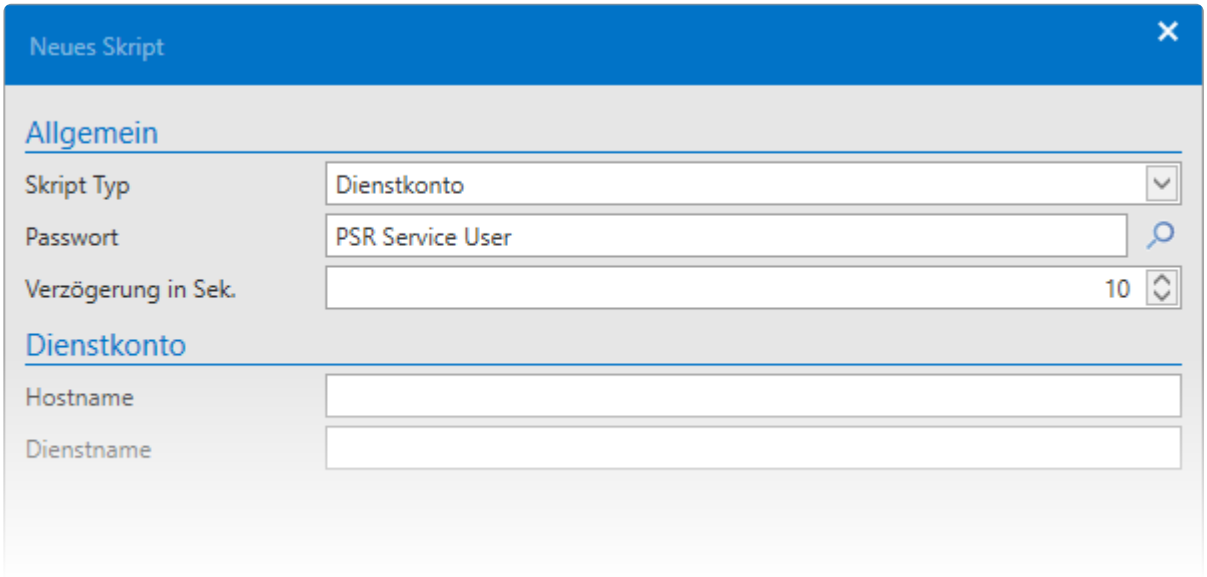
- Zurücksetzen des Passworts, wenn es seit x Tagen abgelaufen ist.

Es muss mindestens ein Auslöser aktiviert sein, damit das Password Reset aktiv ist. Es können alle drei Auslöser unabhängig voneinander ein- und ausgeschaltet werden. Sind alle Auslöser deaktiviert, ist auch der Password Reset deaktiviert.

> Innerhalb von Password Safe prüft ein separater System Task minütlich, ob ein Auslöser zutrifft.

Skripte

Nach der Auswahl erscheint ein neuer Dialog, bei dem die Auswahl über den Typ des Systems getroffen wird, bei dem das Passwort zurückgesetzt werden soll.



- **Skript Typ**: Wählen Sie ihr eigenes oder aus einer Auswahl vorgegebener Skripte das gewünschte aus.
- **Passwort**: Das in Password Safe gespeicherte Passwort, dass zurückgesetzt werden soll.

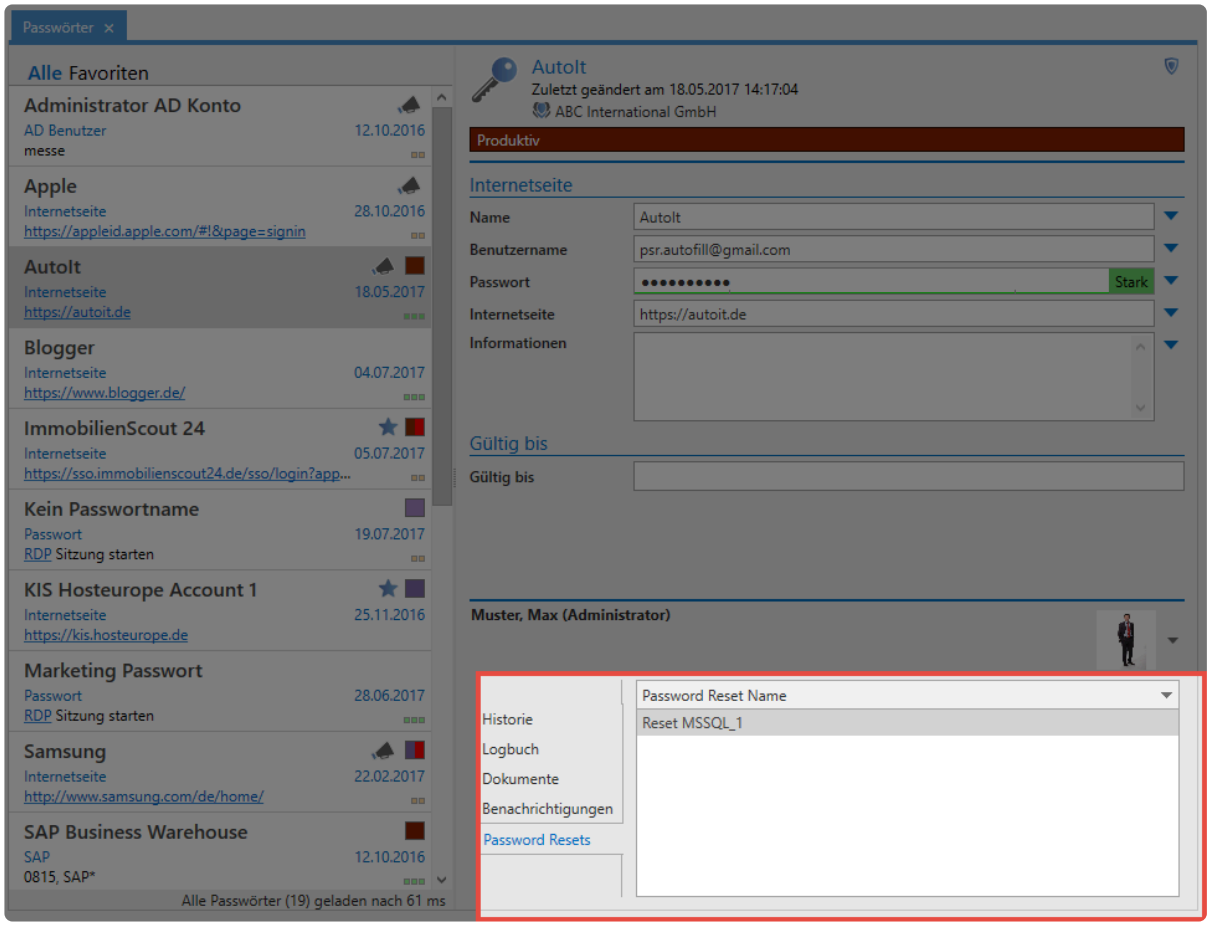
Je nach Skript werden anschließend die jeweils benötigten Informationen abgefragt – bei einem MSSQL-Benutzer beispielsweise die MSSQL-Instanz sowie den genutzten Port.

Die Funktionen und die Konfiguration werden im Kapitel Skripte näher erläutert.

> Es ist nicht möglich, ein Password Reset ohne ein zugehöriges Skript zu erstellen.

Verbundene Passwörter

Unter “Verbundene Passwörter” werden alle Passwörter aufgelistet, die mit dem Password Reset zurückgesetzt werden sollen. Mit einem Passwort verknüpfte Password Resets werden im Lesebereich im Footer des entsprechenden Passworts angezeigt.

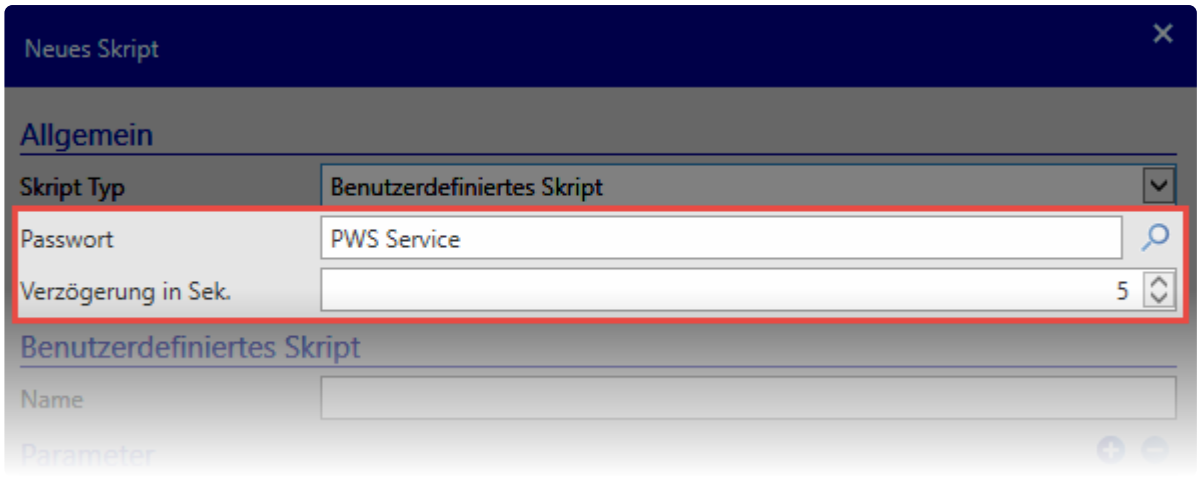

Passwörter
Alle Favoriten
Administrator AD Konto
AD Benutzer 12.10.2016
messe
Apple
Internetseite 28.10.2016
https://appleid.apple.com/#!&page=signin
AutoIt
Internetseite 18.05.2017
https://autoit.de
Blogger
Internetseite 04.07.2017
https://www.blogger.de/
ImmobilienScout 24
Internetseite 05.07.2017
https://sso.immobilienscout24.de/sso/login?app...
Kein Passwortname
Passwort 19.07.2017
RDP Sitzung starten
KIS Hosteurope Account 1
Internetseite 25.11.2016
https://kis.hosteurope.de
Marketing Passwort
Passwort 28.06.2017
RDP Sitzung starten
Samsung
Internetseite 22.02.2017
http://www.samsung.com/de/home/
SAP Business Warehouse
SAP 12.10.2016
0815, SAP*
Alle Passwörter (19) geladen nach 61 ms
AutoIt
Zuletzt geändert am 18.05.2017 14:17:04
ABC International GmbH
Produktiv
Internetseite
Name AutoIt
Benutzername psr.autofill@gmail.com
Passwort Stark
Internetseite https://autoit.de
Informationen
Gültig bis
Gültig bis
Muster, Max (Administrator)
Historie
Logbuch
Dokumente
Benachrichtigungen
Password Resets
Password Reset Name
Reset MSSQL_1

Password Safe Skripte

Verfügbare Skripte

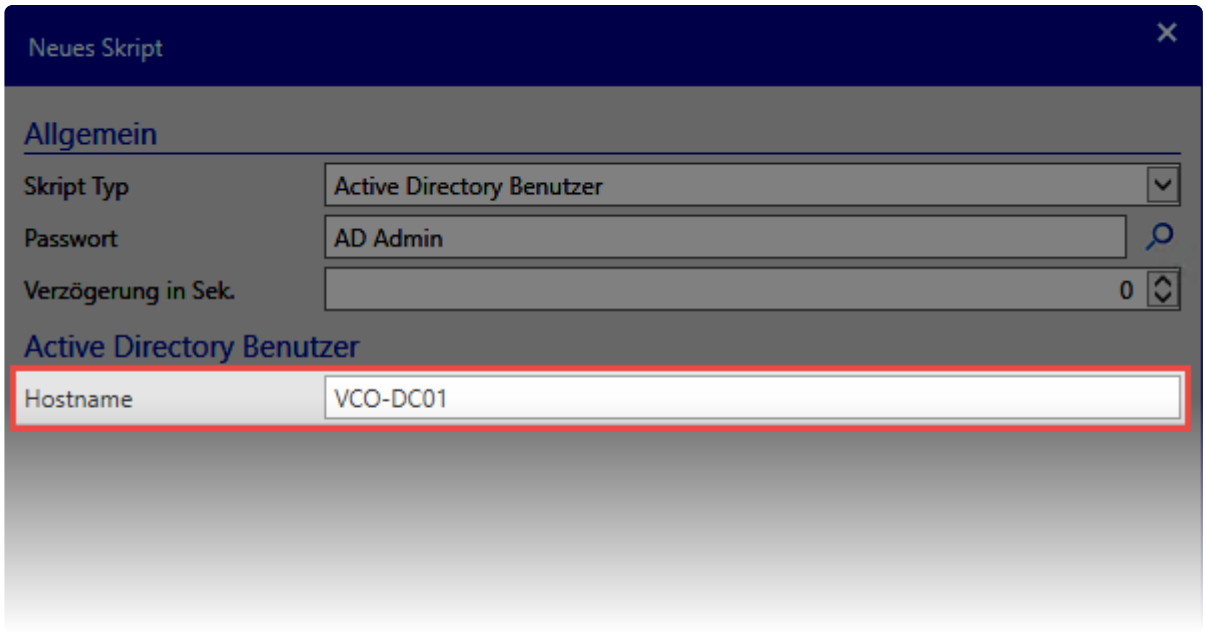
Die folgenden Skripte werden mit ausgeliefert und können direkt verwendet werden. Wählen Sie in allen Skripten im oberen Bereich zunächst ein Passwort aus. Hierbei handelt es sich **nicht** um das Passwort, das auf dem Zielsystem neu gesetzt wird. Vielmehr wird hier der Benutzer angegeben, der den Rest auf dem Zielsystem durchführt. Dieses Passwort benötigt daher administrative Rechte auf dem Zielsystem.

Ebenso können Sie in jedem Skript eine Verzögerung konfigurieren. Dies kann beispielsweise nötig sein, wenn sich im AD ein Passwort ändert, das zunächst auf andere Controller verteilt wird.



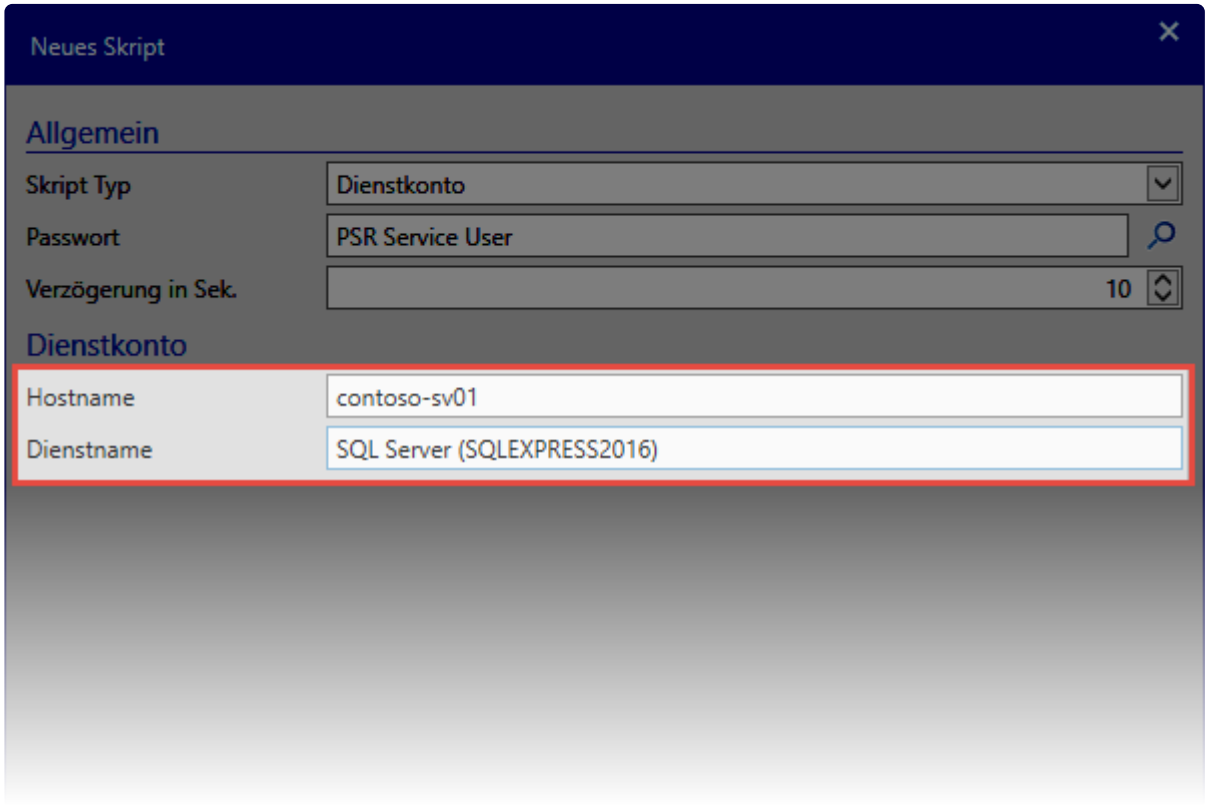
Active Directory Benutzer

Zum Ändern der Passwörter von Active Directory Benutzern (Domänenbenutzern) ist dieses Skript zuständig. Hier wird unter **Hostname** der Zugang zum Active Directory konfiguriert.

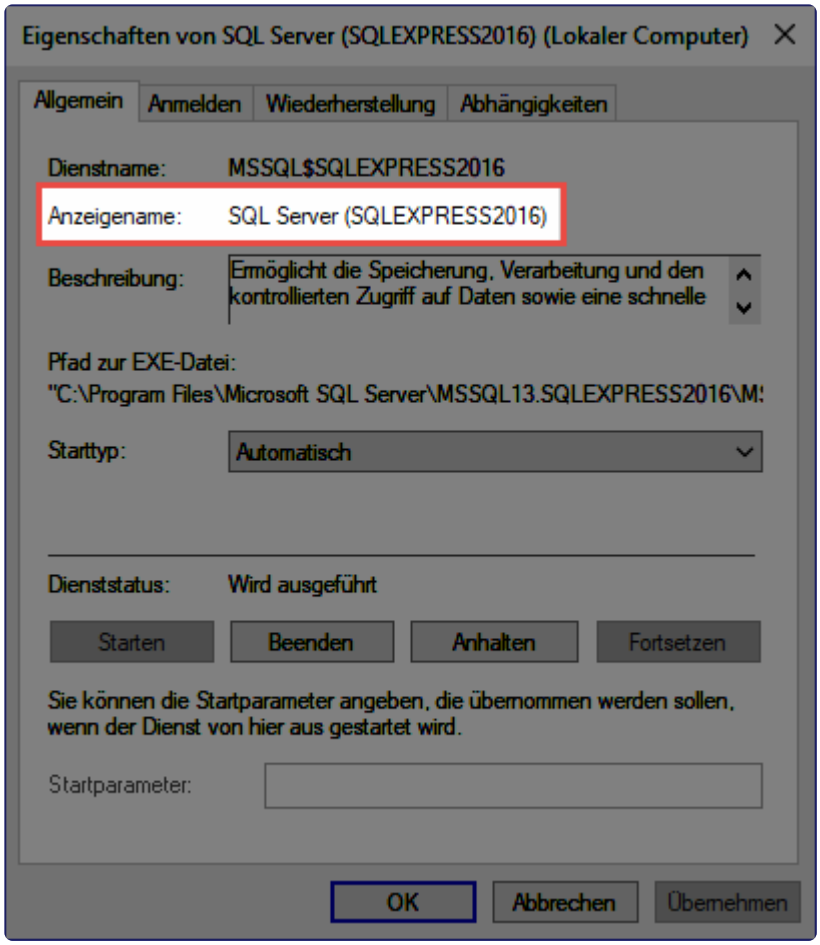


Dienstkonten

Dieses Skript ändert die Zugangsdaten innerhalb eines Dienstes. Sowohl der Benutzer als auch das Passwort können geändert werden. Hierbei wird der **Hostname** – also der Zielrechner – sowie der **Dienstname** hinterlegt.



Es gilt zu beachten, dass aus dem **Dienst** der **Anzeigename** verwendet werden muss.



Die Zugangsdaten in den verbundenen Passwörtern können wie folgt hinterlegt sein:

Lokaler Benutzer

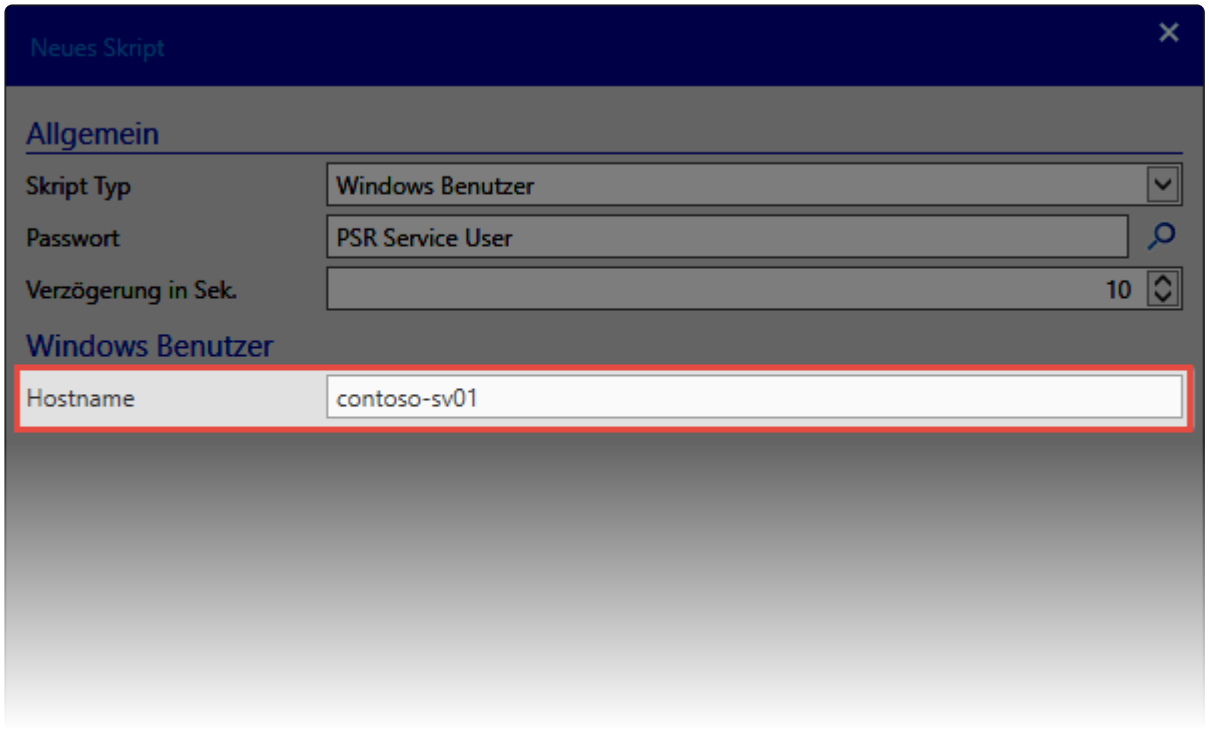
[Username]
\[Username]
.\[Username]
[Computer]\[Username]

Active Directory Benutzer

[Domain]\[Username]

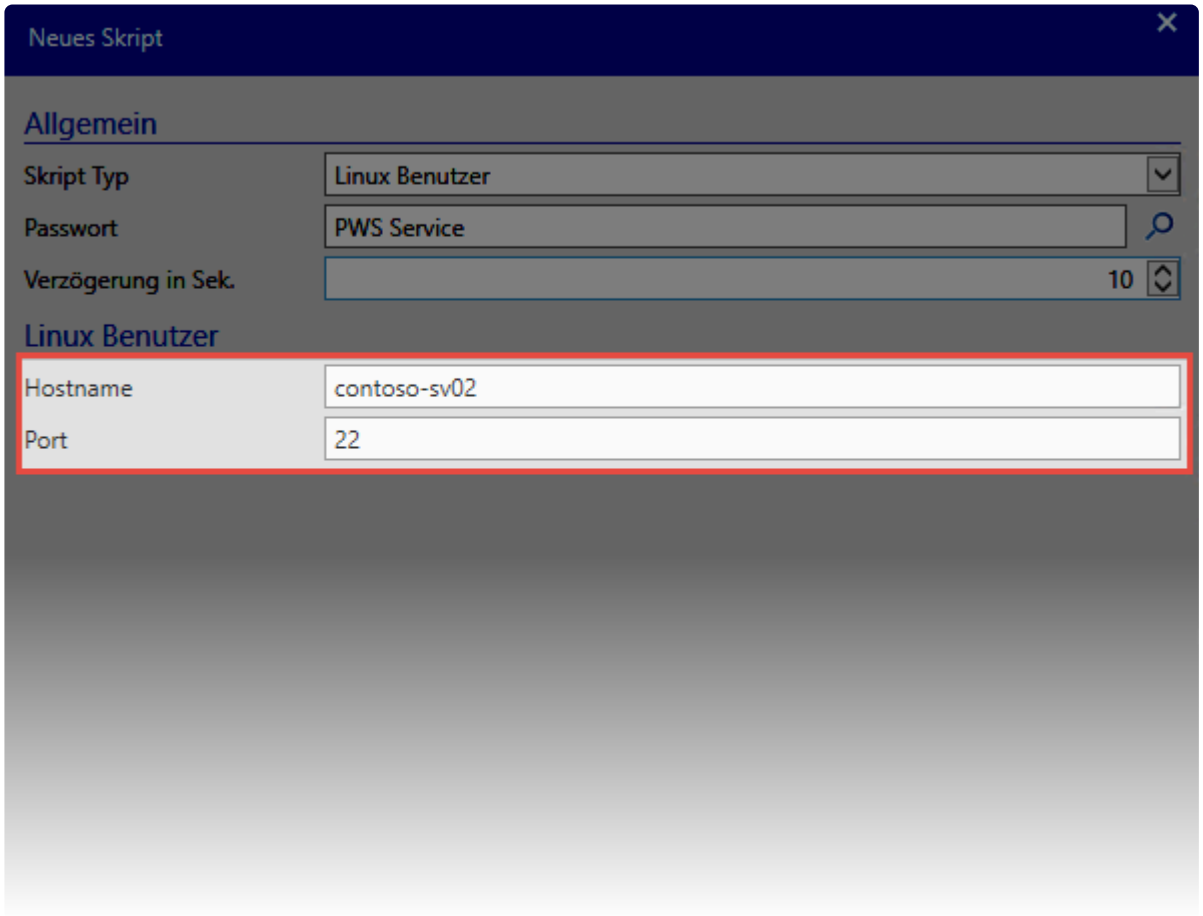
Windows Benutzer

Über dieses Skript setzen Sie die Passwörter von lokalen Windows-Benutzern zurück. Sie hinterlegen hier lediglich den **Hostnamen**.



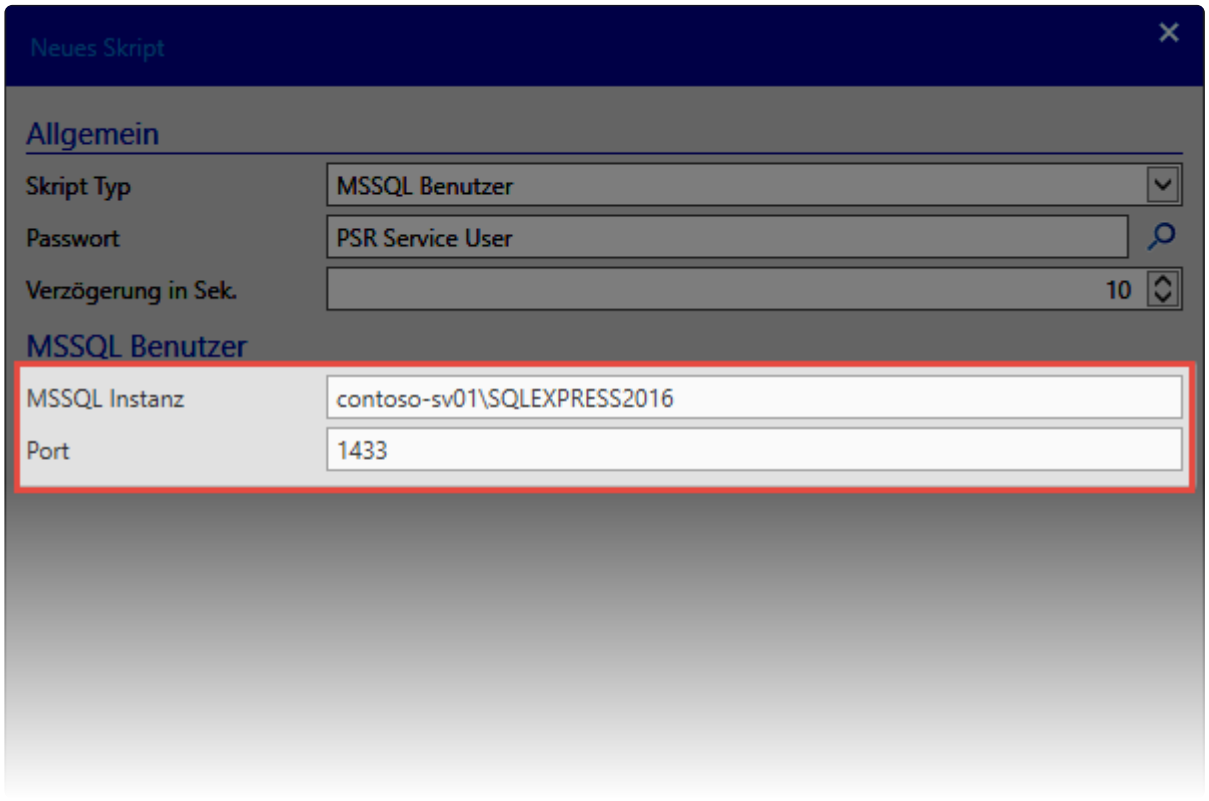
Linux Benutzer

Analog zu den Windows-Benutzern können auch Linux-Benutzer zurückgesetzt werden. Hier müssen Sie ebenfalls nur den **Hostname** sowie den **Port** angeben.

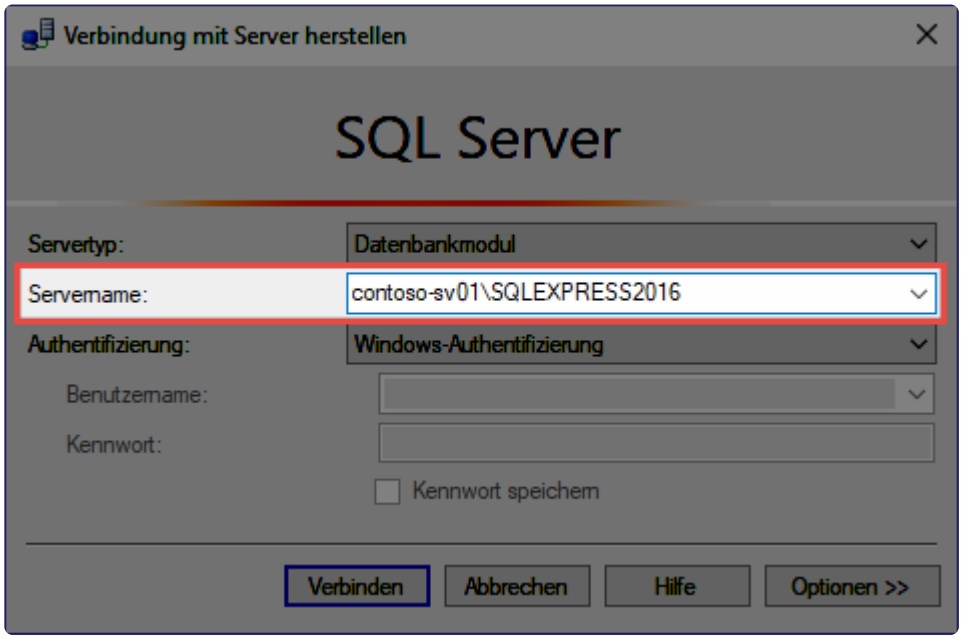


MSSQL Benutzer

Dieses Skript setzt Passwörter von lokalen MSSQL Benutzern zurück. Sie müssen hier die **MSSQL-Instanz** sowie der **Port** angeben.



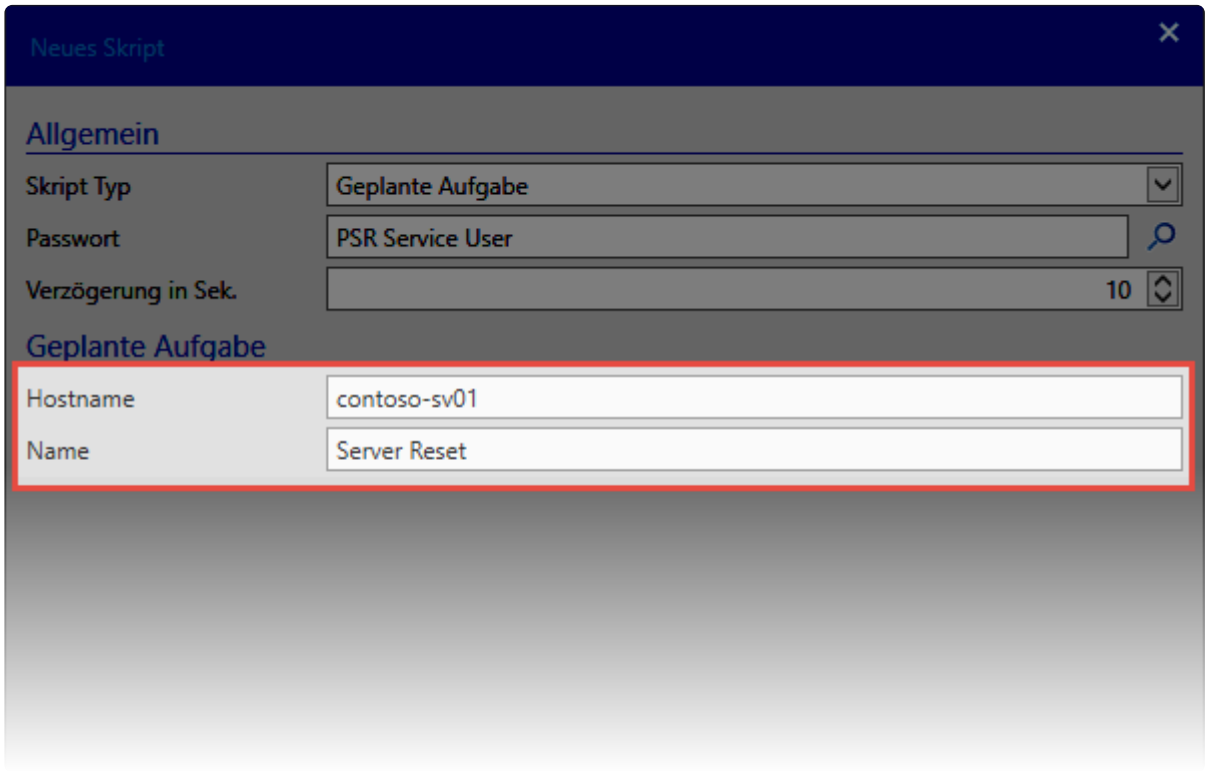
Den Namen der MSSQL-Instanz entnehmen Sie dem Anmeldefenster des SQL Management Studios.



Sollte für die Anmeldung am SQL-Server ein Domänen-Benutzer verwendet werden, so müssen Sie diesen über das Skript **Active Directory Benutzer** verwalten.

Geplante Aufgabe

Die Passwörter der Benutzer der Windows-Aufgabenplanung ändern Sie über dieses Skript. Geben Sie den **Hostname** des Rechners, auf dem die Aufgabe läuft, sowie den **Namen** der Aufgabe selbst an.



Benutzerdefinierte Skripte

Individuelle Lösungen durch eigene Skripte

Als Ergänzung zu den **frei verfügbaren Skripten** können bei Bedarf auch eigene Powershell-Skripte erstellt werden. Folgend werden die benötigten Anforderungen beschrieben, um sie in Password Safe verwendet werden zu können.

Speicherort und Name

Speichern Sie die Skripte im Verzeichnis:
C:\ProgramData\MATESO\Password Safe and Repository Service\System\PowerShell

Speichern Sie die Skripte im **Format .ps1**.

Aufbau der Skripte

Die PowerShell-Skripte müssen wie folgt aufgebaut sein:

RunScript-Funktion

Password Safe ruft immer die RunScript-Funktion auf.

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

Dafür können folgende Standard-Parameter verwendet werden:

- **UserName:** Benutzername, dessen Passwort geändert werden soll.
- **Password:** Passwort, das neu gesetzt werden soll.
- **CredentialsUserName:** Benutzername des Berechtigen, der den Reset durchführen kann (z.B. Administrator).
- **CredentialsPassword:** Passwort des Berechtigten.

scriptBlock

Der **scriptBlock** kann verwendet werden, wenn das Skript im Kontext eines anderen Benutzers laufen soll. Im **scriptBlock** wird dann die eigentliche Änderung durchgeführt.

Wichtig ist an dieser Stelle, dass man Password Safe über einen **Write-Output** ein Feedback über den

Erfolgt übergibt. In folgendem Beispiel wird einfach mit **true** oder **false** gearbeitet. Denkbar wäre allerdings auch eine Fehlermeldung oder ähnliches.

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

Selbstverständlich können CredentialsUserName und CredentialsPassword auch direkt im Skript (also ohne scriptBlock) verwendet werden. Als Beispiel kann hier das mitgelieferte MSSQL Skript dienen.

Invoke

Abschließend muss noch ein Credential erstellt werden. Dieses wird dann per **Invoke** an den **scriptBlock** übergeben. Auch hier ist darauf zu achten, dass alle Fehler per **Write-Output** oder **throw [System.Exeption]** an Passwordsafe zurückgemeldet werden.

Heartbeat

Was ist der Heartbeat?

Der Heartbeat prüft, ob im Password Safe gespeicherte Passwörter mit den Anmeldedaten auf den jeweiligen Systemen übereinstimmen. Dadurch wird gewährleistet, dass die Passwörter nicht voneinander abweichen.

Voraussetzungen

Der Heartbeat steht nur bei Passwörtern zur Verfügung, die mit einem eingerichteten und aktiven Passwort Reset verknüpft sind.

Unterstützte Skripttypen

Es können die Passwörter folgender Skripttypen getestet werden:

- Windows Benutzer
- MSSQL Benutzer
- Active Directory Benutzer
- Linux Benutzer

Weitere Informationen sind im Kapitel Skripte zu finden.

Prüfung mittels Heartbeat

Die Prüfung kann über mehrere Methoden erfolgen.

Prüfung über Passwort Reset

Der Heartbeat wird immer vor dem ersten Passwort Reset ausgeführt. Nachdem das Skriptes durchgelaufen ist,findet die Prüfung erneut statt. Weitere Informationen dazu sind auch im Kapitel Rollback zu finden.

Manuelle Prüfung

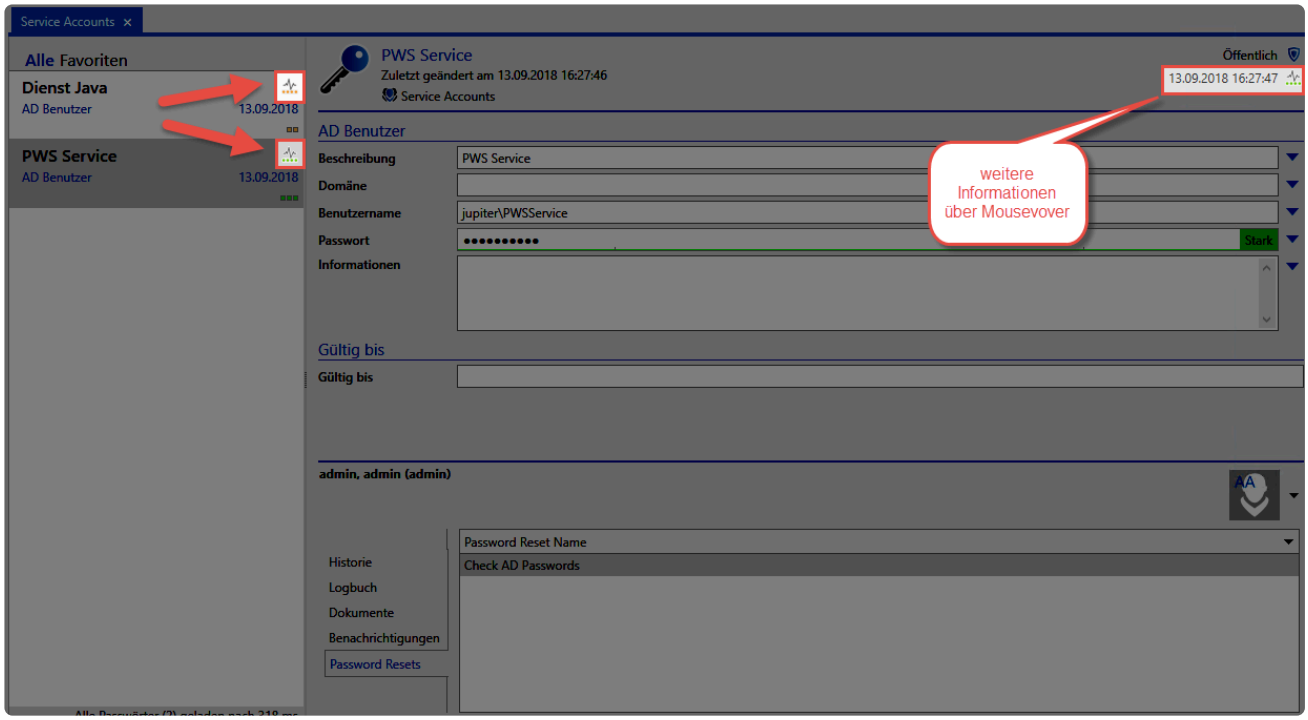
Im Passwort Modul wird der Heartbeat in der Ribbon über einen Klick auf **Anmeldedaten prüfen** ausgeführt. Geprüft wird immer das aktuell markierte Passwort.

Automatisch über Passwort Einstellungen

Sie können auch konfigurieren, dass der Heartbeat zyklisch verläuft. Dies kann entweder über die globalen Einstellungen oder direkt in den Passworteinstellungen erfolgen.

Ergebnis der Prüfungen

Die Ergebnisse der Prüfung sind im **Modul Passwörter** einsehbar.



Oben im Lesebereich ist das Datum der letzten Ausführung zu sehen. Daneben wird der Erfolg über ein farbliches Icon dargestellt. Durch ein Mouseover auf das Icon werden weitere Informationen eingeblendet.

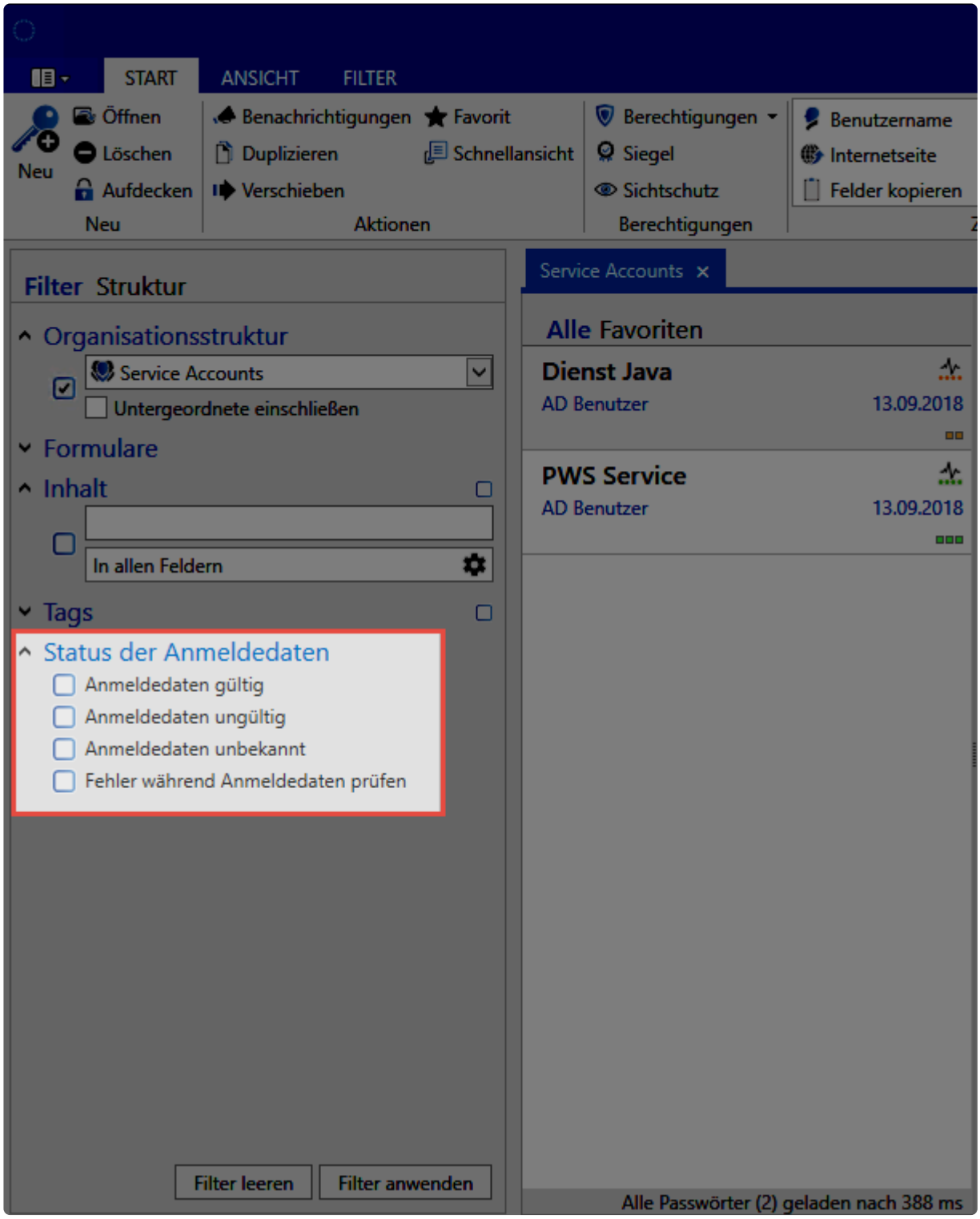
Die letzte Prüfung war erfolgreich. Das Passwort ist korrekt

Die Prüfung konnte nicht durchgeführt werden. Etwa, weil das Zielsystem nicht erreicht werden konnte.

Die letzte Prüfung fand statt. Das Passwort weicht aber von dem des Zielsytems ab.

Filtern der Ergebnisse

Über die Filtergruppe **Status der Anmeldedaten** kann ein Filter konfiguriert werden, um die geprüften Datensätze zu selektieren.


START
ANSICHT
FILTER
Neu
Öffnen
Löschen
Aufdecken
Neu
Benachrichtigungen
Favorit
Duplizieren
Schnellansicht
Verschieben
Aktionen
Berechtigungen
Siegel
Sichtschutz
Berechtigungen
Benutzername
Internetseite
Felder kopieren
Filter Struktur
Organisationsstruktur
Service Accounts
Untergeordnete einschließen
Formulare
Inhalt
In allen Feldern
Tags
Status der Anmeldedaten
Anmeldedaten gültig
Anmeldedaten ungültig
Anmeldedaten unbekannt
Fehler während Anmeldedaten prüfen
Filter leeren
Filter anwenden
Service Accounts
Alle Favoriten
Dienst Java
AD Benutzer
13.09.2018
PWS Service
AD Benutzer
13.09.2018
Alle Passwörter (2) geladen nach 388 ms

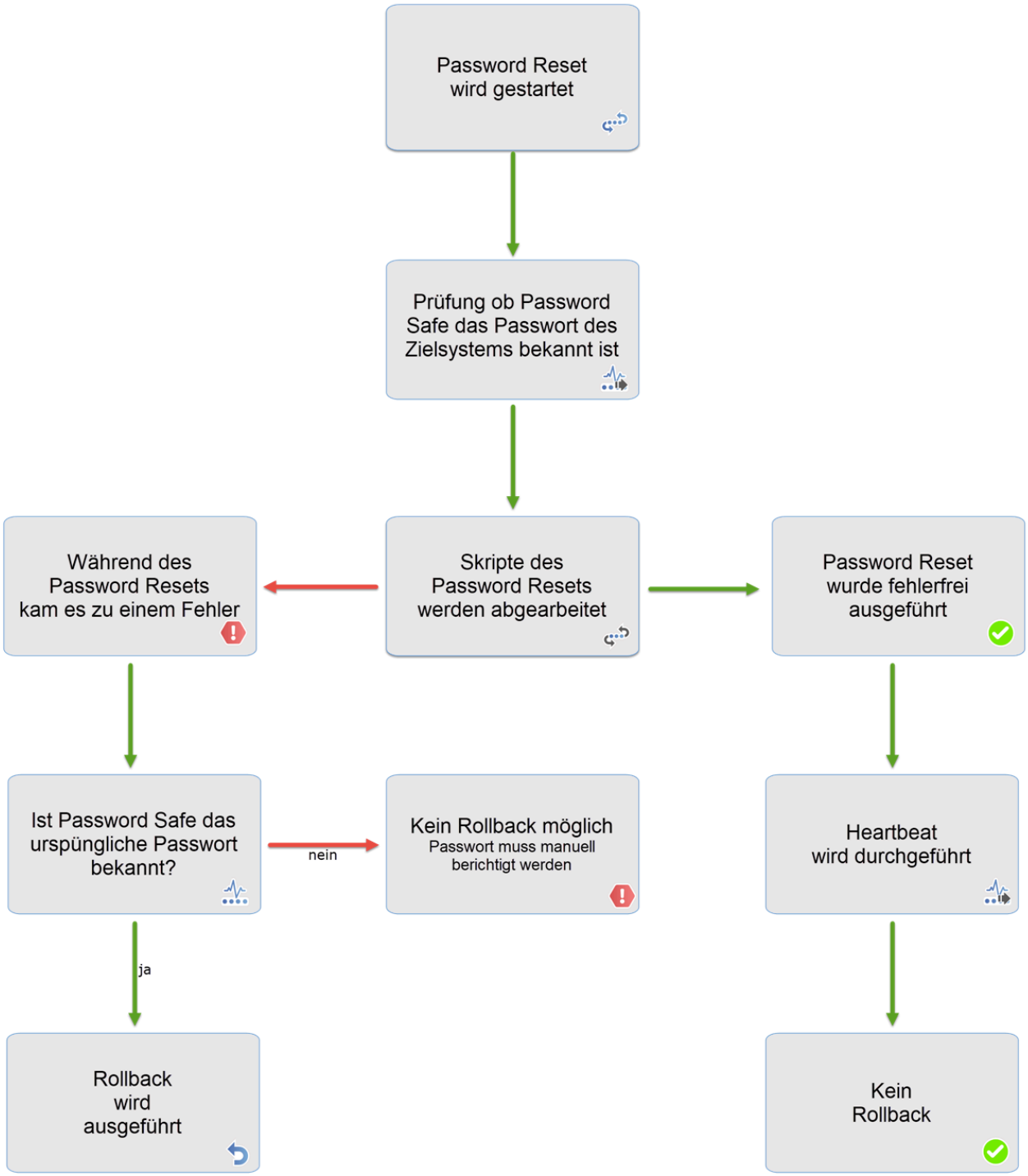
Rollback

Was ist der Rollback?

Wenn beim Ausführen eines Skriptes ein Fehler auftritt, wird wieder das ursprüngliche Passwort gesetzt.

Wann läuft der Rollback?

Das folgende Diagramm zeigt, wann, bzw. nach welchen Kriterien der Rollback angestoßen wird.



Ablauf

Muss der Rollback ausgeführt werden, so laufen alle Skripte des Resets noch einmal durch. Hierbei wird das letzte Passwort der Historie verwendet.
Nach dem Rollback wird kein neuer Historischer Eintrag erstellt.

Logbuch

Im Logbuch wird protokolliert, ob ein Rollback gelaufen ist und ober er erfolgreich war. Nach einem Rollback sollten Sie das Passwort sicherheitshalber nochmals prüfen.

Logbucheinträge unter Password Reset

Nachfolgend werden alle möglichen Logbucheinträge aufgeführt die im Zusammenhang mit Password Reset stehen

Der Password Reset prüft zuerst anhand des ersten Scriptes (über den Heartbeat), ob das Passwort korrekt ist. Dabei können folgende Logbucheinträge geschrieben werden:

Logbuch Typ	Logbuch Datensatz
Anmeldedaten gültig	Container
Anmeldedaten ungültig	Container
Fehler während Anmeldedaten prüfen	Container

Anschließend werden alle Scripte des Password Resets nacheinander ausgeführt. Dabei werden folgende Logbucheinträge geschrieben:

Logbuch Typ	Logbuch Datensatz
Ausführen	Password Reset
Rollback ausführen	Password Reset
Fehler bei der Ausführung	Password Reset
Fehler bei der Ausführung des Rollbacks	Password Reset

Wenn ein Rollback nicht durchgeführt werden kann, weil das alte Passwort vor dem Reset falsch war oder das erste Script vom Typ “Benutzerdefiniert” ist, wird folgender Logbucheintrag geschrieben:

Logbuch Typ	Logbuch Datensatz
Fehler bei der Ausführung des Rollbacks	Password Reset

Falls ein Password Reset fehlgeschlagen ist und versucht wird ein Rollback durchzuführen, wird der Password Reset für einen Tag blockiert und folgender Logbucheintrag geschrieben: (Dabei ist es egal ob der Rollback funktioniert hat oder nicht)

Logbuch Typ	Logbuch Datensatz
Password Reset blockiert	Password Reset

Discovery Service

Das Problem

In den meisten Netzwerken kommen sogenannte **Service Accounts** zum Einsatz. Diese werden beispielsweise verwendet, um Dienste auszuführen. Nicht selten wird hierbei für mehrere Accounts **ein und dasselbe Passwort** verwendet. Das manuelle Ändern dieser Passwörter gestaltet sich als extrem aufwendig. Deswegen wird aus Bequemlichkeit oft darauf verzichtet.

Das Resultat ist, dass oftmals für viele **sicherheitskritische Zugänge** die gleichen veralteten Passwörter verwendet werden. Dies stellt natürlich ein **extremes Sicherheitsrisiko** dar. Einem Angreifer sind Tür und Tor geöffnet, wenn er an nur eines der Passwörter gelangt!

Die Lösung

Mit Hilfe des **Discovery Service** kann das komplette Netzwerk gescannt werden. Dabei wird sowohl nach lokalen Benutzerkonten als auch nach Active Directory Benutzern gesucht. Zudem werden auch Password Resets ermittelt, über die die Passwörter der gefundenen Accounts zurückgesetzt werden können.

Funktionsweise

Der **Discovery Service** kann in drei logische Schritte aufgeteilt werden:

1. Es wird ein **Discovery Service Task** angelegt, der die Daten im Netzwerk ermittelt. Dieser kann einmalig oder auch zyklisch ausgeführt werden und läuft im Hintergrund.
2. Die gefundenen Daten werden nach erfolgreichem Lauf im **Discovery Service Modul** angezeigt (z.B. Windows Benutzer, Dienste, etc.).
3. Aus den gefundenen Daten können schlussendlich **Passwörter** oder **Password Resets** erzeugt werden.

Voraussetzungen

Verfügbarkeit

Der **Discovery Service** ist ausschließlich in der **Enterprise Plus Edition** verfügbar.

Relevante Rechte

Um den Discovery Service nutzen zu können, werden folgende Optionen benötigt:

Benutzerrechte

- Discovery Service Modul anzeigen
- Kann Discovery Service System Task verwalten

Voraussetzungen

Eine Voraussetzung für **Discovery Service** sind Daten von **Active Directory Benutzern, Benutzerkonto und Dienstkonten.** Diese werden über einen **Netzwerk Scan** im Netzwerk gescannt und erfasst. Dafür müssen Sie vor der Konfiguration des **Netzwerk Scan** ein **Passwort** anlegen, das **Zugriff** auf die entsprechenden **Server/Clients** und **Dienste eines Netzwerks** hat, um Daten zu erfassen. Dieser Benutzer sollte, der Domänengruppe entsprechend, Admin-Mitglied sein. Sonst verwendet man einen Domänen-Administrator.

> ! Vor dem Anlegen eines **Netzwerk Scan** muss ein entsprechendes **Passwort** mit **Rechten** für die **Domäne** vorhanden sein!

Passwort:

1. Wird für die **Authentifizierung** gegenüber dem **Active Directory Computer** benötigt.
2. Wird für die **Authentifizierung** gegenüber der **WMI (Windows Management Instrumentation)** der zu scannenden Computer benötigt.

Anforderungen an die Netzwerkinfrastruktur:

1. Die zu scannenden Computer und der Ad-Controller müssen über das Netzwerk erreichbar sein.
2. Auf den zu scannenden Computern muss der Dienst: “Windows-Verwaltungsinstrumentation” gestartet werden (standardmäßig wird er von Windows ausgeführt).
3. Hilfe zum Starten des Dienstes: https://msdn.microsoft.com/de-de/library/aa826517(v=vs.85).aspx
4. Firewall darf WMI-Anfragen nicht blockieren (wird standardmäßig nicht blockiert).
5. Hilfe zur Konfiguration der Firewall: https://msdn.microsoft.com/de-de/library/aa822854(v=vs.85).aspx

> ✻ Aktuell können nur **IPv4-Adressen** gescannt werden.

Offene Ports für den Scan (Notwendig):

1. LDAP: Port 389(TCP,UDP)
2. RPC/WMI: Port 135(TCP)
3. (Windows Server 2008, Windows Vista und höhere Versionen) – Port 49152-65535 (TCP) oder statischer WMI Port
4. (Windows 2000, Windows XP und Windows Server 2003) – Port 1025-5000 (TCP) oder statischer WMI Port

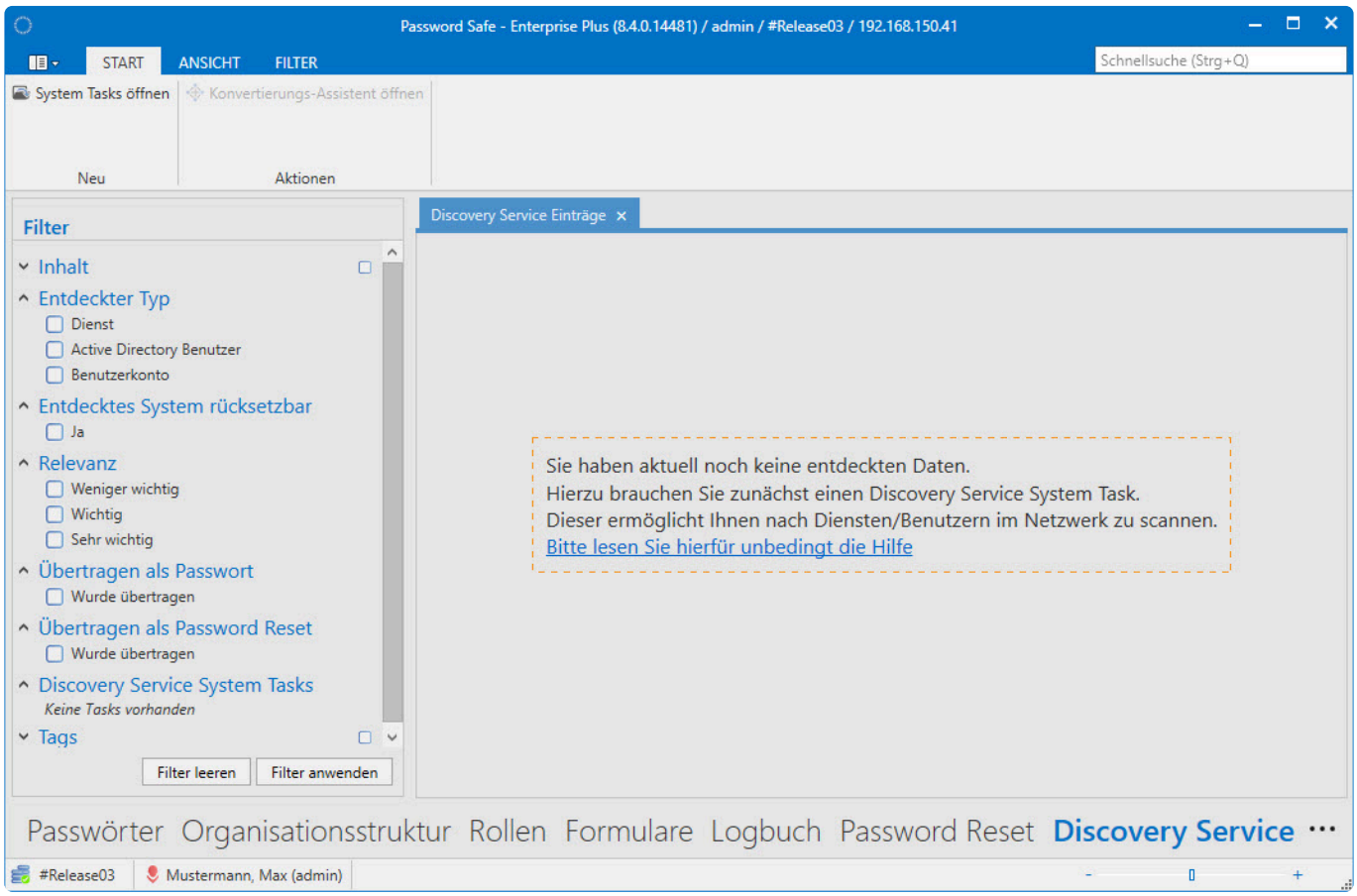
Computername (Hostname):

1. IP-Adresse:
   Gibt die IP-Adresse des gefundenen Elements an, bzw., wo das Element gefunden wurde (im Falle eines Active Directory Benutzers die IP-Adresse des Domaincontrollers).
2. Computername und passende IP-Adresse:
   Zunächst wird am **DNS-Server** der Domäne der Computername angefragt. Der zurückgegebene Computer-Name enthält zusätzlich als Postfix den Domänen-Namen (z.B. Client01.domain.local). Gibt es keinen Eintrag in der Domäne zu der angefragten IP-Adresse, wird der Computername über **NetBIOS** ermittelt. Der Domänen-Name wird dann am Computer nicht angezeigt (z.B. Client01).
   Für die Ermittlung des Computer-Namens wird im **Password Safe V8** die **DNS-Anfrage** bevorzugt. Wird hier kein Ergebnis geliefert, erfolgt die Abfrage über **NetBIOS**.

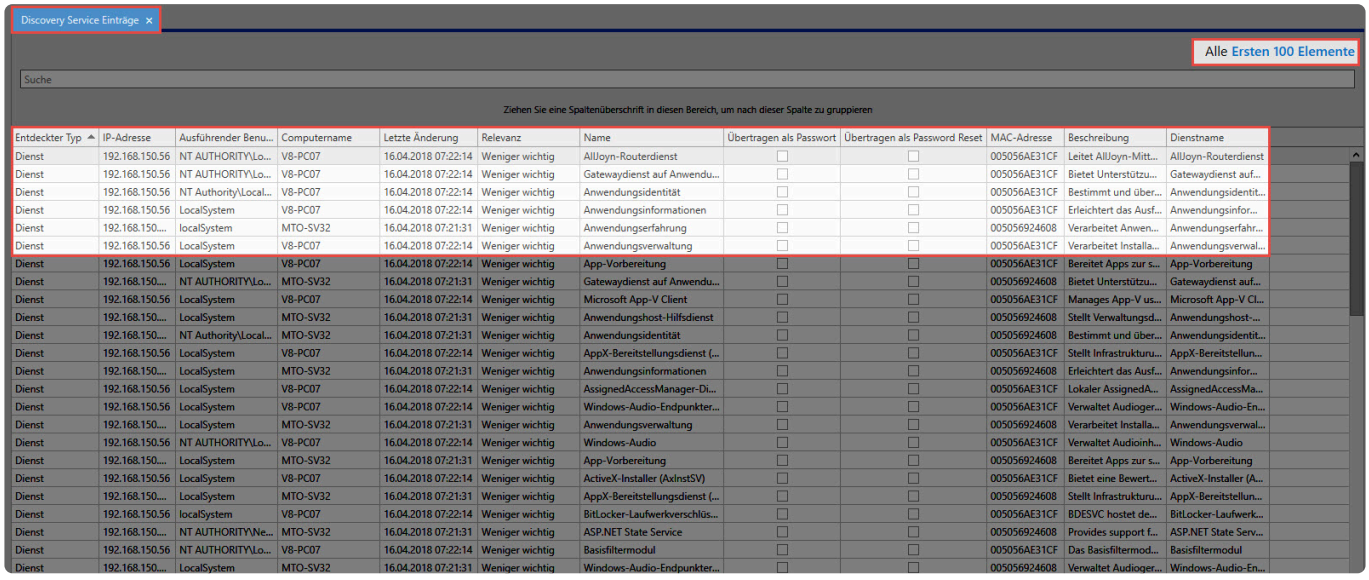
Konfiguration

Das Discovery Service Modul

Öffnet man das Modul in **Password Safe**, sind dort erst einmal **Discovery Service** keine Einträge vorhanden. Diese müssen über einen **System Task** erzeugt werden.



Nach Abschluss eines **System Task** werden die gefundenen Daten tabellarisch dargestellt:



Eine Gruppierung der Informationen können Sie über den Spalten-Editor vornehmen.

Netzwerk Scan

Über einen **Discovery Service Task** wird ein neuer **Discovery Service** angelegt und für einen **Netzwerk Scan** konfiguriert. Gefunden werden entsprechend der Konfiguration des **Netzwerk Scans** folgende Typen:

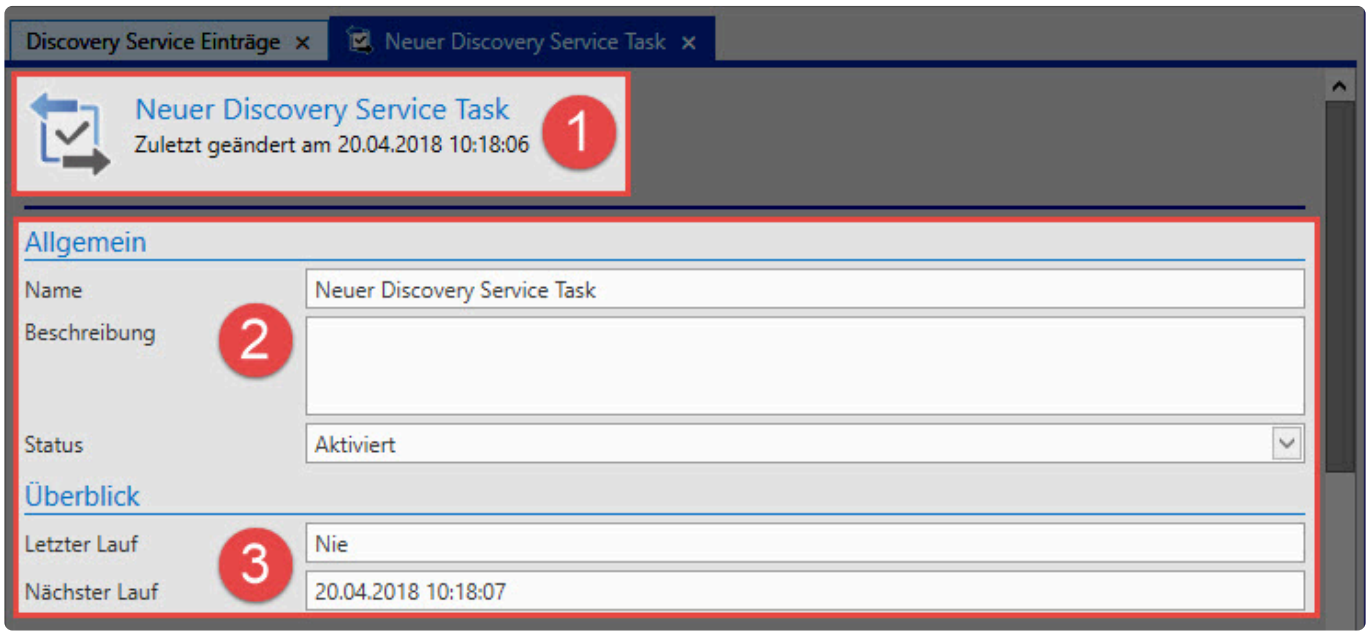
- Dienstkonten
- Active Directory Benutzer
- Benutzerkonto

Konfiguration eines Discovery Service Task

Um Daten für den **Discovery Service** zu erfassen, muss der **Discovery Service Task** für einen **Netzwerk Scan** entsprechend konfiguriert werden.

Allgemein und Überblick

Das folgende Bild zeigt einen neu anzulegenden **Discovery Service Task**.

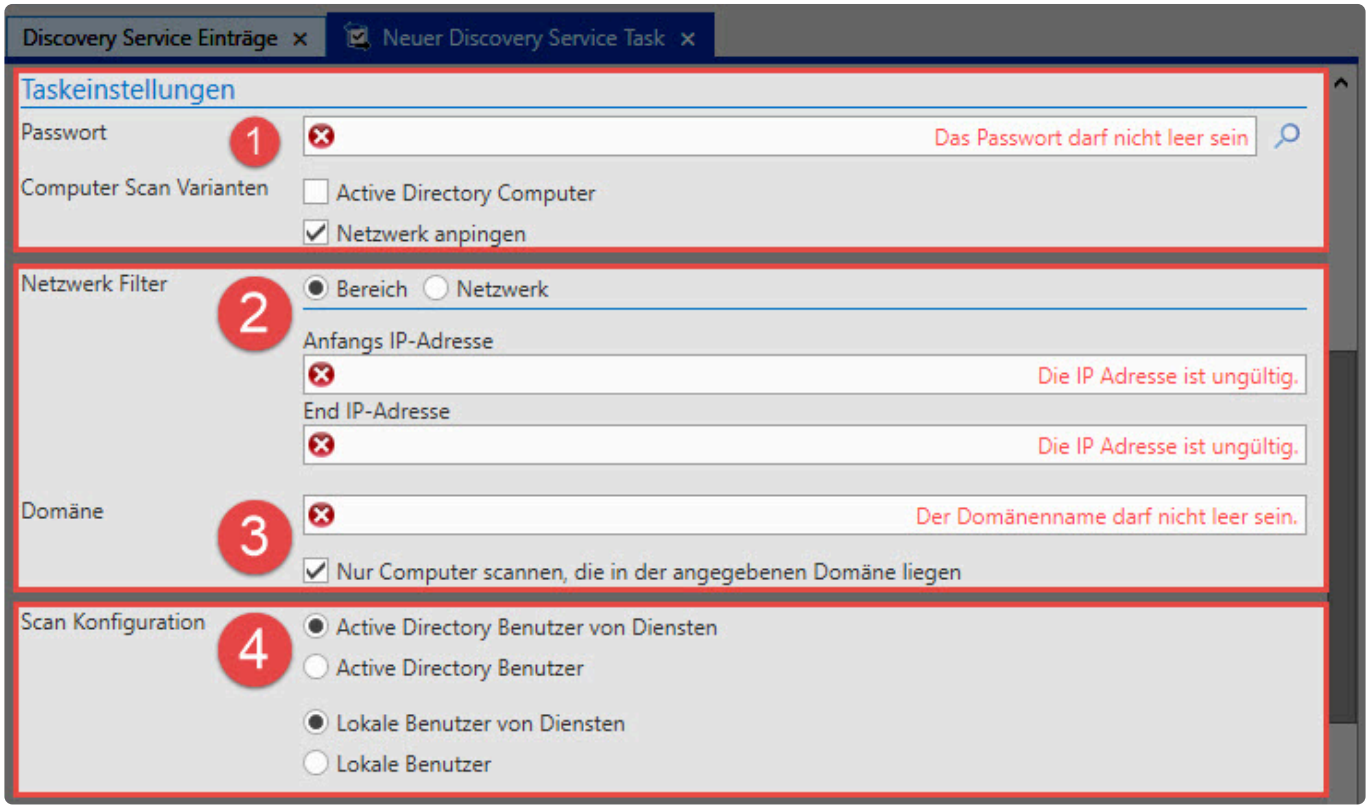


1. Zeigt Informationen über den **Discovery Service Task** an.
2. Im Bereich **Allgemein** wird der Name des **Discovery Service Task** (optional mit Beschreibung) eingetragen.
   Der **Status** ist standardmäßig immer auf **Aktiviert**, kann aber in der Konfiguration auf **Deaktiviert** gesetzt werden.
3. Der **Überblick** zeigt die Aktivität des **Discovery Service Task** an:
   Letzter Lauf: Zeigt das Datum des letzten Laufes an.
   Nächster Lauf: Zeigt den zukünftigen Lauf an.

Task-Einstellungen

Passwort:
1. Feld Benutzername: Typ
2. Feld Passwort: Typ
Mehrere Passwortfelder —> 1. Feld wird verwendet.

In diesem Bereich werden spezielle Eingaben für den **Discovery Service Task** getroffen. Ein **Netzwerk Scan** scannt nach Fertigstellung das **Netzwerk** nach diesen Vorgaben.

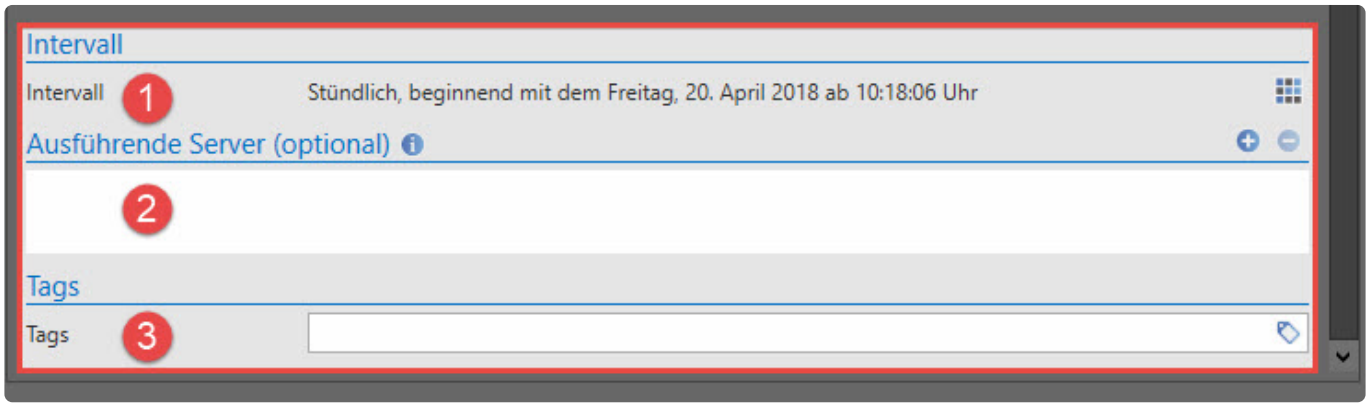


1. **Passwort** und **Computer Scan Varianten:** Das benötigte Passwort muss schon angelegt sein und benötigt entsprechende Rechte für die Domäne.
   Active Directory Computer: Es werden nur die Computer gescannt, die sich im Active Directory befinden (kann als Option auch einzeln oder mit Netzwerk anpingen verwendet werden).
   Netzwerk anpingen: Es wird ein Netzwerk-Filter für die Konfiguration des Netzwerks eingeblendet.
2. **Netzwerk Filter**: Es wird festgelegt, wie das Netzwerk gescannt werden soll: entweder über einen IP-Bereich oder über eine IP-Netzwerk-Adresse.
   Bereich: Eingabe der Anfangs-IP-Adresse und End-IP-Adresse des Bereichs im Netzwerk
   Netzwerk: Eingabe der Netzwerk-Adresse und entsprechenden Subnetz-Maske des Netzwerks
3. **Domäne:** Hier wird die Domäne angegeben, die für den **Netzwerk-Scan** verwendet wird. Zusätzlich können Sie auswählen, dass nur Computer in der angegebenen Domäne gescannt werden. Eine Namensauflösung sollte dahingehend funktionieren.
4. **Scan-Konfiguration**:
   Hier wird der Netzwerk Scan für die Konfiguration des Active Directory festgelegt. Entweder **Active Directory Benutzer von Diensten** oder **Active Directory Benutzer**.
   Der zweite Bereich legt die Scan-Konfiguration für lokale Computer fest. Entweder **Lokale Benutzer von Diensten** oder **Lokale Benutzer**.

Das ausführende System, auf dem der AdminClient installiert ist, wird nicht gescannt!

Intervall / Ausführende Server / Tags

In diesem Bereich werden Informationen über den Start und weitere zusätzliche Informationen eingetragen.



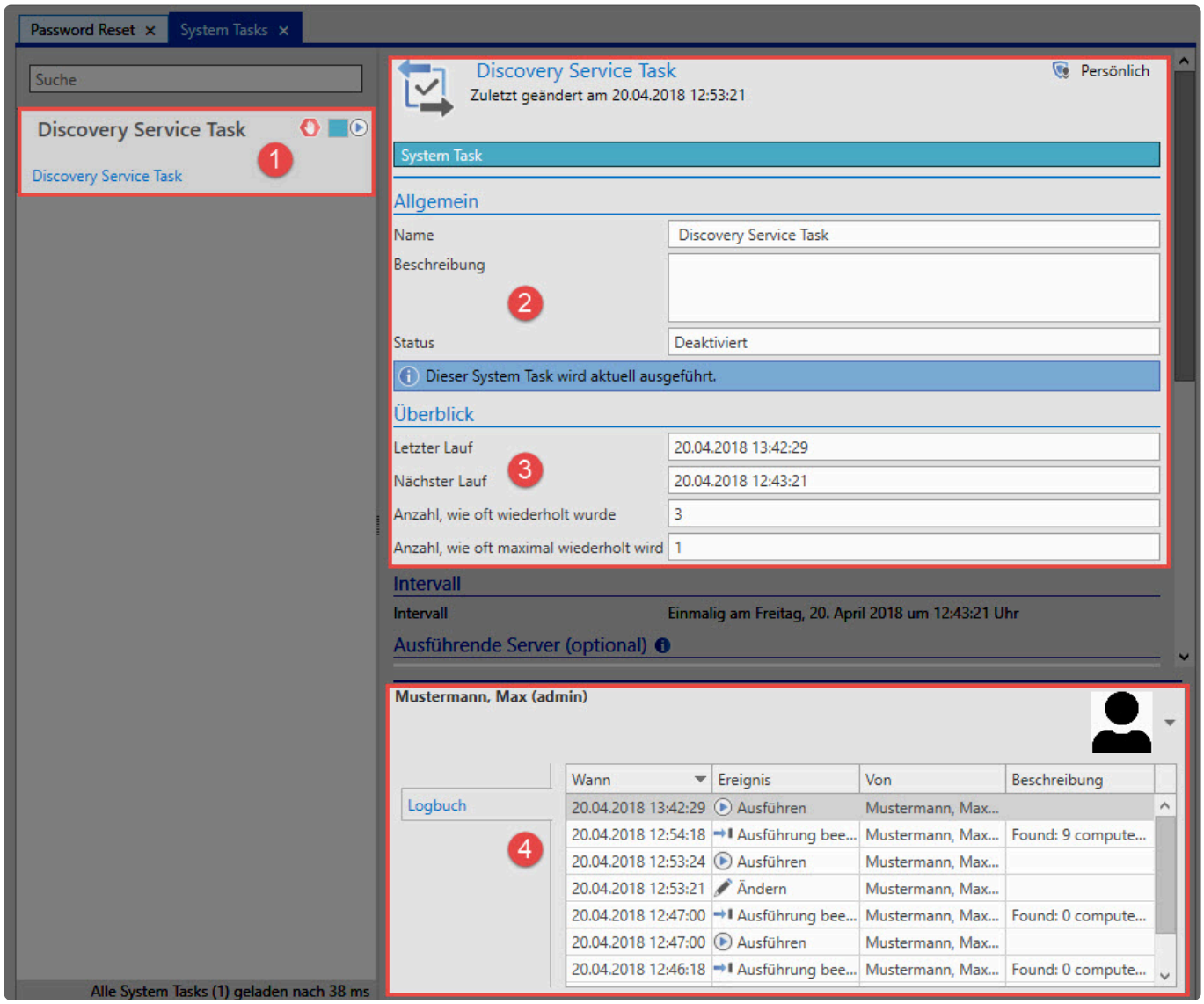
1. **Intervall:** Es wird definiert, in welchem Intervall der **Discovery Service Task** ablaufen soll. Die Standardeinstellung ist stündlich ein Jahr lang ab dem Anlegen des **Discovery Service Task**. Im Intervall kann eine Abstufung zwischen minütlich und einmalig (optional mit Enddatum) eingestellt werden.
2. **Ausführende Server (optional):** Hier können Server mit einem **AdminClient** eingetragen werden, auf den der **Discovery Service Task** bei Ausfall des Hauptservers ausgeführt werden kann. Es wird automatisch der **Discovery Service Task** von den in der Liste erreichbaren Servern übernommen und ausgeführt. Es wird von oben nach unten nach erreichbaren Servern gesucht.
3. **Tags:** Die Verwendung von Tags ist im Kapitel Tagverwaltung genauer beschrieben. Hier kann ein spezieller Tag für den **Discovery Service Task** vergeben werden.

Nach der Konfiguration des **Discovery Service Task wird beim Speichern ein *Verbindungstest** durchgeführt. Daraufhin wird eine korrekte oder fehlerhafte Konfiguration angezeigt. Entsprechend dieser Meldung muss der **Discovery Service Task** angepasst werden.

Standardeinstellung des **Discovery Service Task** nach dem Speicher ist **Aktiviert**! Es wird **sofort aktiv** im Netzwerk nach Daten **gescannt.** Diese werden **ausgelesen, aber nicht verändert!**

Gefundene Einträge

Die Einträge für den **Discovery Service** werden über einen **Discovery Service Task** gefunden. Es kann eine bestimmte Zeit in Anspruch nehmen, um alle Daten der Systeme im angegebenen IP-Netzwerk zu erfassen. Das Symbol **Blauer Pfeil** am **Discovery Service Task** sowie eine entsprechende Meldung in der Anzeige **Allgemein** weisen darauf hin. Nach Beenden des **Discovery Service Task** werden die Daten im **Discovery Service Modul** angezeigt.

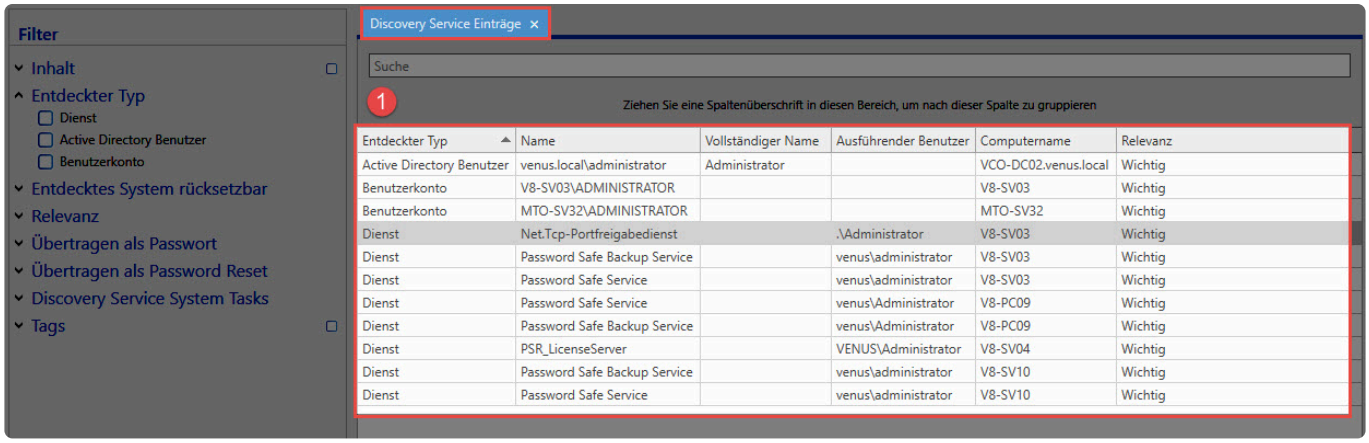


1. **Discovery Service Task**: Anzeige des Status: mit der **Taste F5** kann dieser in der Preview und im Logbuch aktualisiert werden.
   Rote Hand: Deaktiviert
   Blauer Pfeil: Aktiviert und wird ausgeführt
   farbiges Kästen: Entsprechend zugeordneter Tag
2. **Allgemein:** Hier werden aktuelle Angaben zum **Discovery Service Task** angezeigt. Bei aktiven **Discovery Service Task** wird hier ein **Hinweistext** angezeigt.
3. **Überblick:** Aktuelle Daten des **Discovery Service Task** über die Läufe sowie Wiederholungen werden hier angezeigt.
4. **Logbuch:** Am **Discovery Service Task** befindet sich im **Footer** das **Logbuch**. Hier werden die letzten Aktivitäten des **Discovery Service Task** angezeigt.

> Die **Daten** werden **nicht zur Laufzeit aktuell gehalten** und zeigen nicht immer den aktuellen Stand an. Eine **Aktualisierung** der Daten sollte daher regelmäßig mit der **Taste F5** erfolgen!

Verwenden der Discovery Service-Einträge

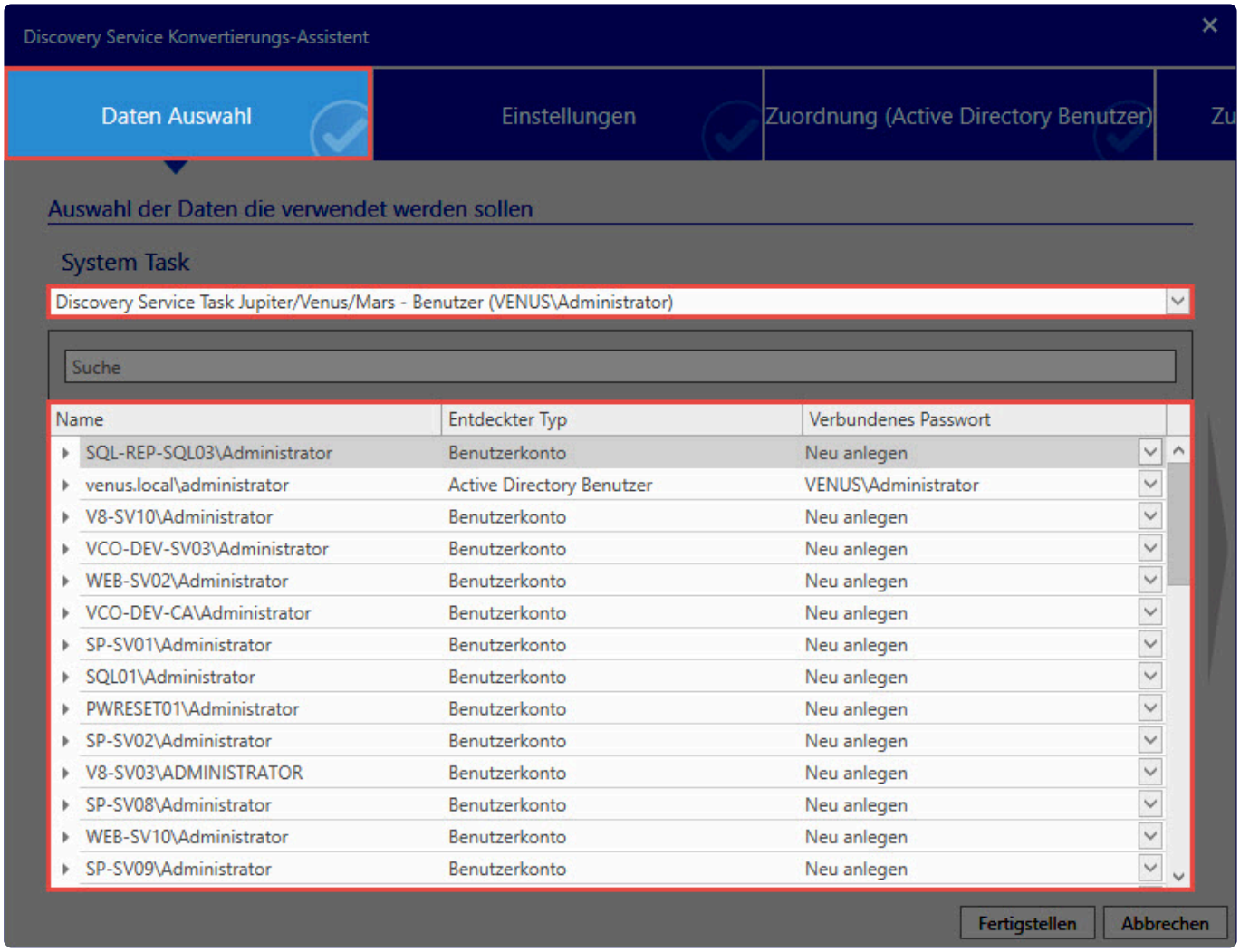
Das erfolgreiche Ausführen eines **Discovery Service Task** ist Voraussetzung für die **Discovery Service Einträge**. Die gefundenen Daten werden im **Modul Discovery Service** tabellarisch angezeigt und können über den Filter **Discovery Service System Task** entsprechend zugeordnet werden.



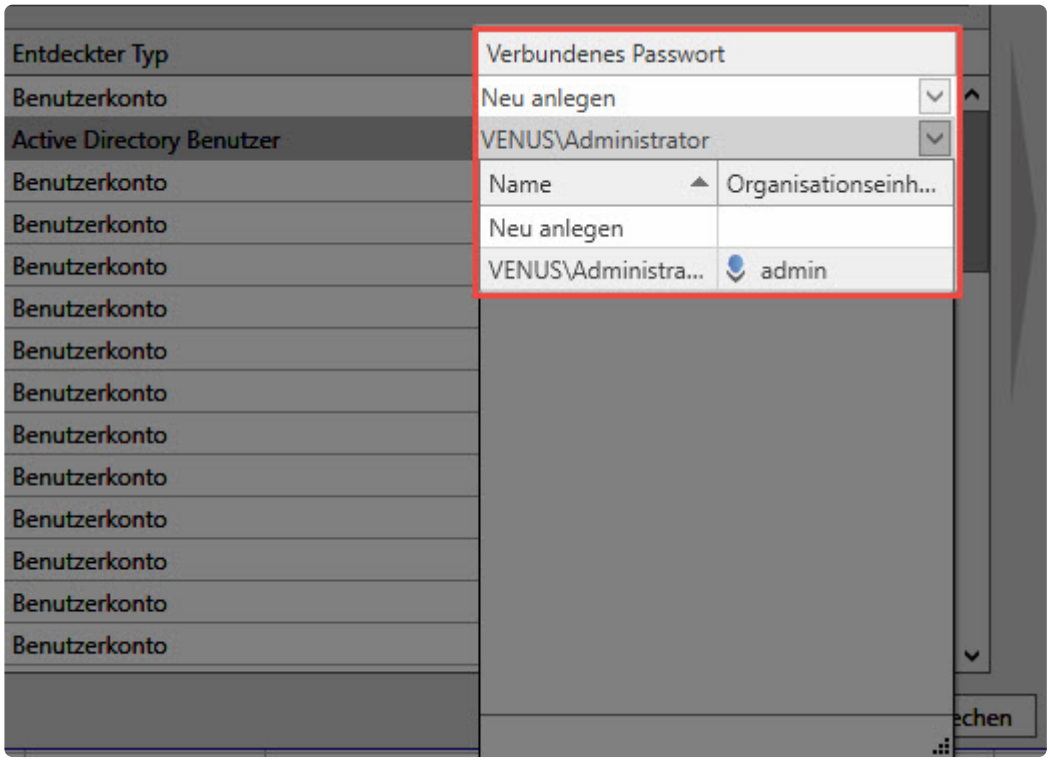
1. In diesem Bereich werden die **Discovery Service Einträge** angezeigt, die durch den **Discovery Service Task** gefunden wurden und für den **Konvertierungs-Assistent** ausgewählt.

Mehrfachauswahl Discovery Service Einträge

Werden mehrere Einträge für ein **Password Reset** ausgewählt, müssen Sie im **Konvertierungs-Assistent** entsprechend mehrere **Passwörter** und **Password Resets** anlegen. Je nach Auswahl der Einträge **(Dienst, Active Directory Benutzer, Benutzerkonto)** müssen entsprechende **Zuordnungen** im **Konvertierungs-Assistent** für die **Passwörter** durchgeführt werden.



Jede Zeile muss am Ende mit einem **Passwort** verbunden sein. Somit muss für jeden Eintrag eine Zuordnung im **Konvertierungs-Assistent** durchgeführt werden.

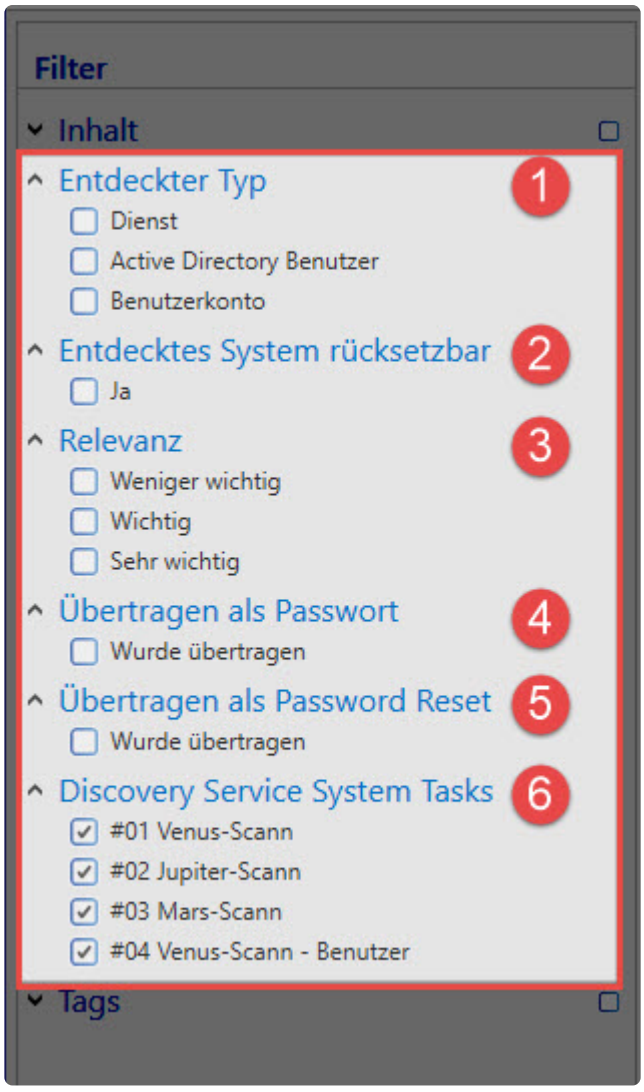


Bei **Active Directory Benutzern** besteht die Möglichkeit, die Zuordnung zu einem vorhandenen **Passwort** durchzuführen.

> ✻ Das weitere Vorgehen erfolgt analog zur Durchführung mit nur einem ausgewählten **Discovery Service Eintrag.**

Filtereinstellungen

Für die Verarbeitung der gefundenen Daten können Sie den im **Discovery Service Modul** entsprechend **angepasstern Filter** verwenden.



Beschreibung des **Filters mit den speziellen Optionen für die Discovery Service Einträge:**

1. **Entdeckter Typ**: Hier kann man die gefundenen Einträge nach Typ filtern.
2. **Entdecktes System rücksetzbar:** Gibt an, ob aus den gefundenen Daten ein Password Reset erstellt werden kann.
3. **Relevanz:** Stuft die Wichtigkeit des gefundenen Systems ein.
   Hohe Relevanz bedeutet, dass bei einem Active Directory Benutzer oder Benutzerkonto mehrere Dienste gefunden wurden.

Weniger wichtig: Genau ein Dienst wurde gefunden.
Wichtig: Zwei bis neun Dienste wurden gefunden.
Sehr wichtig: 10 oder mehr Dienste wurden gefunden.
Wenn bereits ein Password Reset erzeugt worden ist, wird die Relevanz auf Weniger wichtig abgestuft.

4. **Übertragen als Passwort:** Gibt an, ob über den Konvertierungs-Assistent ein Passwort erstellt wurde.
5. **Übertragen als Passwort Reset:** Gibt an, ob über den Konvertierungs-Assistent ein Password Reset erstellt wurde.
6. **Discovery Service System Tasks:** Hier befindet sich eine Filterung der Einträge nach dem System Task.

Konvertierung von Einträgen

Ein wichtiges Element für den **Discovery Service** ist der **Konvertierungs-Assistent**. Er verarbeitet **Einträge** und legt dementsprechend **Passwörter und Password Resets** an.

Starten Sie den **Konvertierungs-Assistent** in der Ribbon über das Register “Start”. Von dort aus wechseln Sie auch zu den **System Tasks**.

Nach einem erfolgreichen Lauf des **Discovery Service Task**, sind Einträge im **Discovery Service** vorhanden. Anschließend werden sie mit dem **Konvertierungs-Assistent** weiterverarbeitet. Für die Verarbeitung im **Konvertierungs-Assistent** wird das Netzwerk nach folgenden Typen gescannt:

1. Entdeckter Typ: Dienst
2. Entdeckter Typ: Active Directory Benutzer
3. Entdeckter Typ: Benutzerkonto

> Es werden nur **Dienste aufgenommen**, denen mindestens ein **AD-Benutzer** oder **Benutzerkonto** zugeordnet werden kann! Es werden nur **AD-Benutzer** und **Benutzerkonten** aufgenommen, denen **mindestens ein Dienst** zugeordnet werden kann.

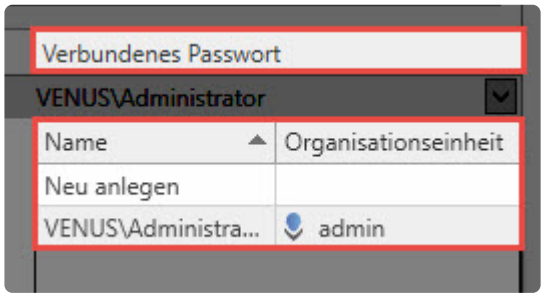
Ausführung

In der Tabelle des **Discovery Service** selektieren Sie die Einträge, für die Sie ein **Password Reset** oder **Passwort** anlegen möchten. Anschließend klicken Sie auf den **Konvertierungs-Assistent** und der **Discovery Service Konvertierungs-Assistent** öffnet sich für die weitere Bearbeitung.

1. Wählen Sie zunächst einen **Discovery Service Task** aus. Dadurch bestimmen Sie, in welchem Kontext die neuen Daten erzeugt werden (Für neue **Password Reset** wird als ausführender Benutzer das **Passwort des Domänenadministrators** des Tasks verwendet. Außerdem werden nur noch **Discovery Service Task Einträge** zur Konvertierung verwendet, die auch von dem angegebenen **Discovery Service Task** gefunden wurden.).
2. In diese Spalte werden die gefundenen Einträge mit den **Diensten** angezeigt, für die der Benutzer eingetragen ist.
3. Diese Spalte zeigt an, um welchen **entdeckten Typ** es sich handelt.
4. Diese Spalte zeigt bereits existierende Passwörter in Password Safe an, die zu dem gefundenen **Active Directory Benutzer** oder **Benutzerkonto** passen. Hier wählen Sie aus, welches Passwort bei der Erzeugung eines **Password Reset** verwendet werden soll (es wird als einziges verbundenes Passwort für den Password Reset verwendet.). Alternativ können Sie diese Passwörter auch neu erstellen.

Jeder Wurzelknoten entspricht logisch gesehen **einem Benutzer** mit all seinen zugeordneten Daten (wie z.B. Dienste). Für **jeden Benutzer** mit seinen zugeordneten Daten wird später ein **Password Reset** erstellt.

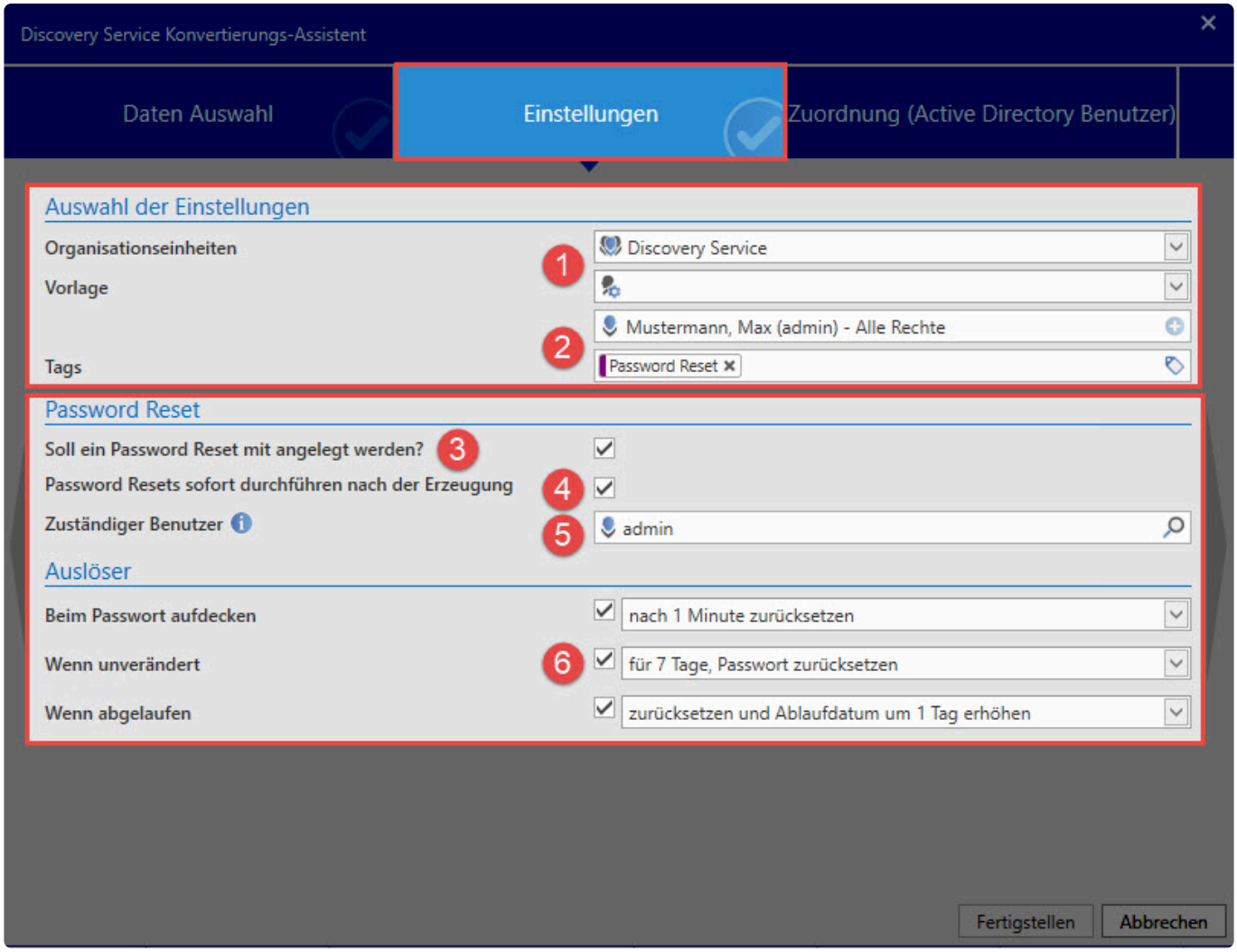
Folgendes Bild zeigt die Option ein **neues Passwort anlegen** oder **vorhandenes Passwort beibehalten** an.



Außerdem wird angezeigt, in welcher **Organisationseinheit** sich das vorhandene Passwort befindet.

Einstellungen

Im Ribbon **Einstellungen** konfigurieren Sie das **Password Reset**.

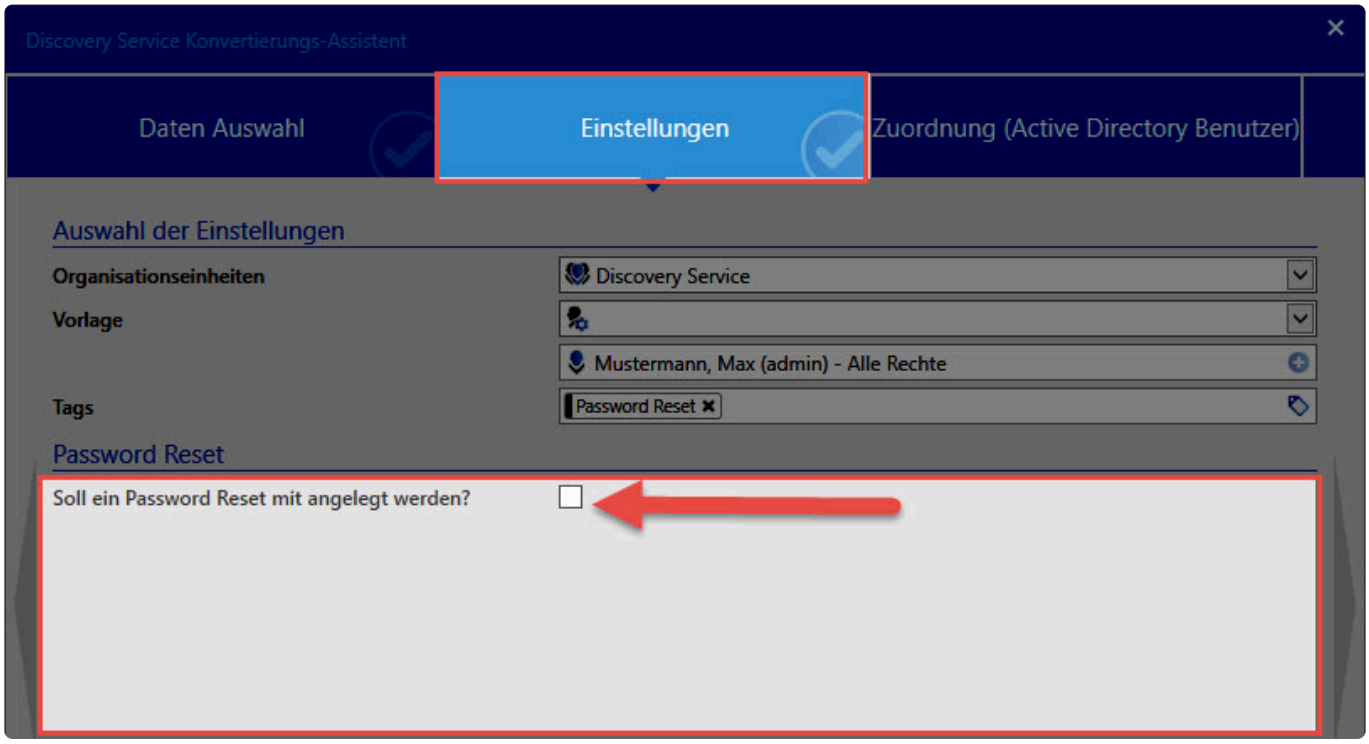


Nachfolgend werden die **Einstellungen** genauer beschrieben:

1. Hier tragen Sie die Organisationseinheit ein, in der das **Password Reset** angelegt werden soll. Zusätzlich können Sie hier eine Vorlage für die Rechtevererbung eintragen.
2. Hier tragen Sie den **Verantwortliche** für das **Passwort** (optional mit speziellem Tag) ein.
3. Anlegen eines **Password Reset**
   Option 1: **Soll ein Password Reset mit angelegt werden?** legt ein* Password Reset* an. Wählen Sie **Option 1** nicht aus, werden nachfolgende Optionen nicht angezeigt.
4. Einstellung der Durchführung eines **Password Reset**
   Option 2: **Password Resets sofort nach der Erzeugung durchführen** führt nach dem Klick auf **Fertigstellen** sofort ein **Password Reset** durch.
5. Hier tragen Sie den **Verantwortliche für das Password Reset** ein.
6. Hier wählen Sie verschiedene **Auslöser für das Password Reset** aus.

> ! Nachdem Sie auf **Fertigstellen** geklickt haben, werden die **Password Resets sofort ausgeführt** und die **Passwörter geändert!**. Dies betrifft auch die **Windows-Passwörter!**

Wählen Sie die Option 1 “**Soll ein Password Reset mit angelegt werden?**” nicht aus, werden die **Schritte 4, 5 und 6** nicht zur Konfiguration angezeigt.

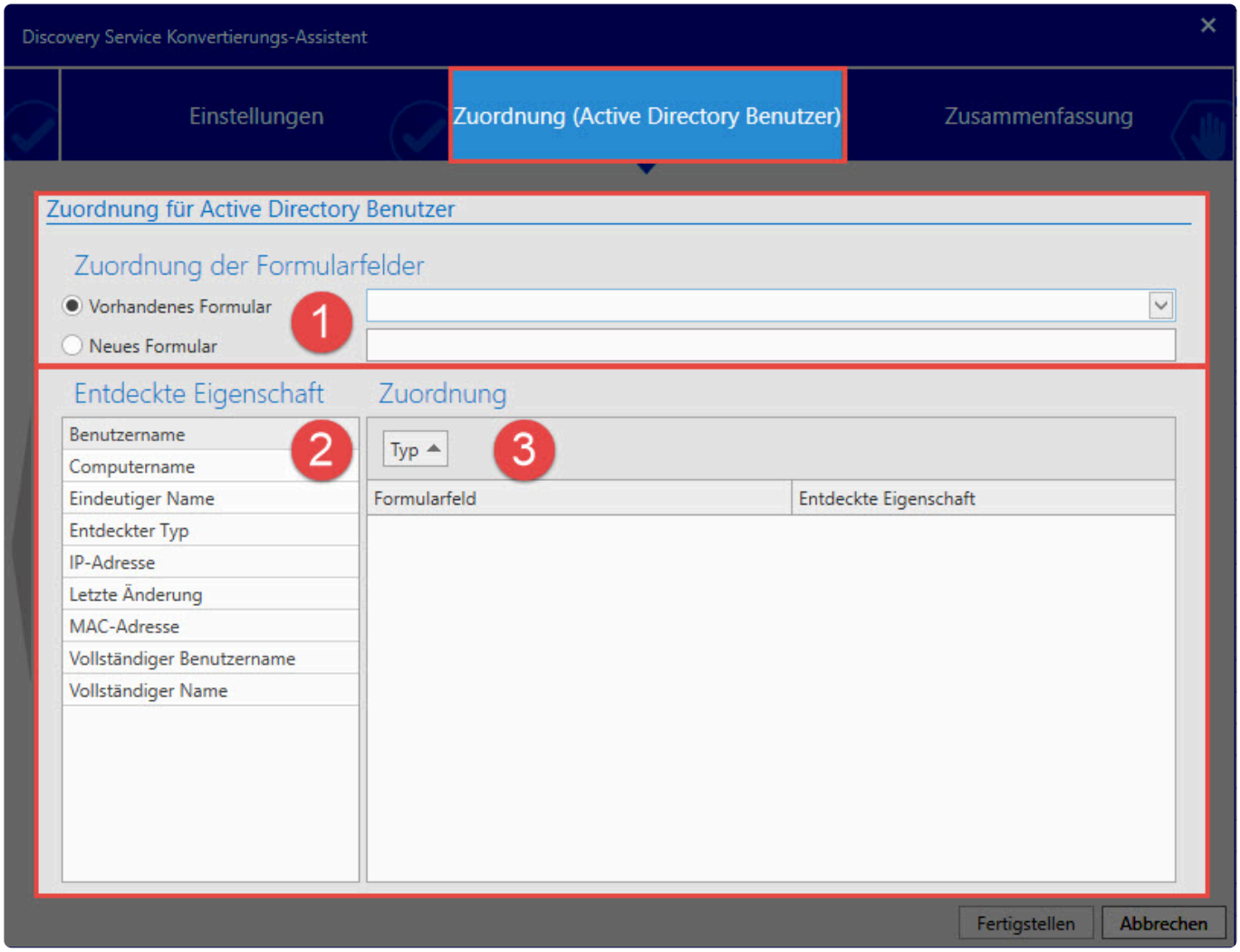


> ! Nach dem Klick auf **Fertigstellen**, werden ein oder mehrere **Passwörter angelegt**, aber **keine entsprechenden Password Resets!**

Zuordnung (Active Directory Benutzer)

In Ribbon **Zuordnung (Active Directory Benutzer)** werden die gefundenen Daten der **Discovery Service Einträge** auf ein Password-Formular übertragen.

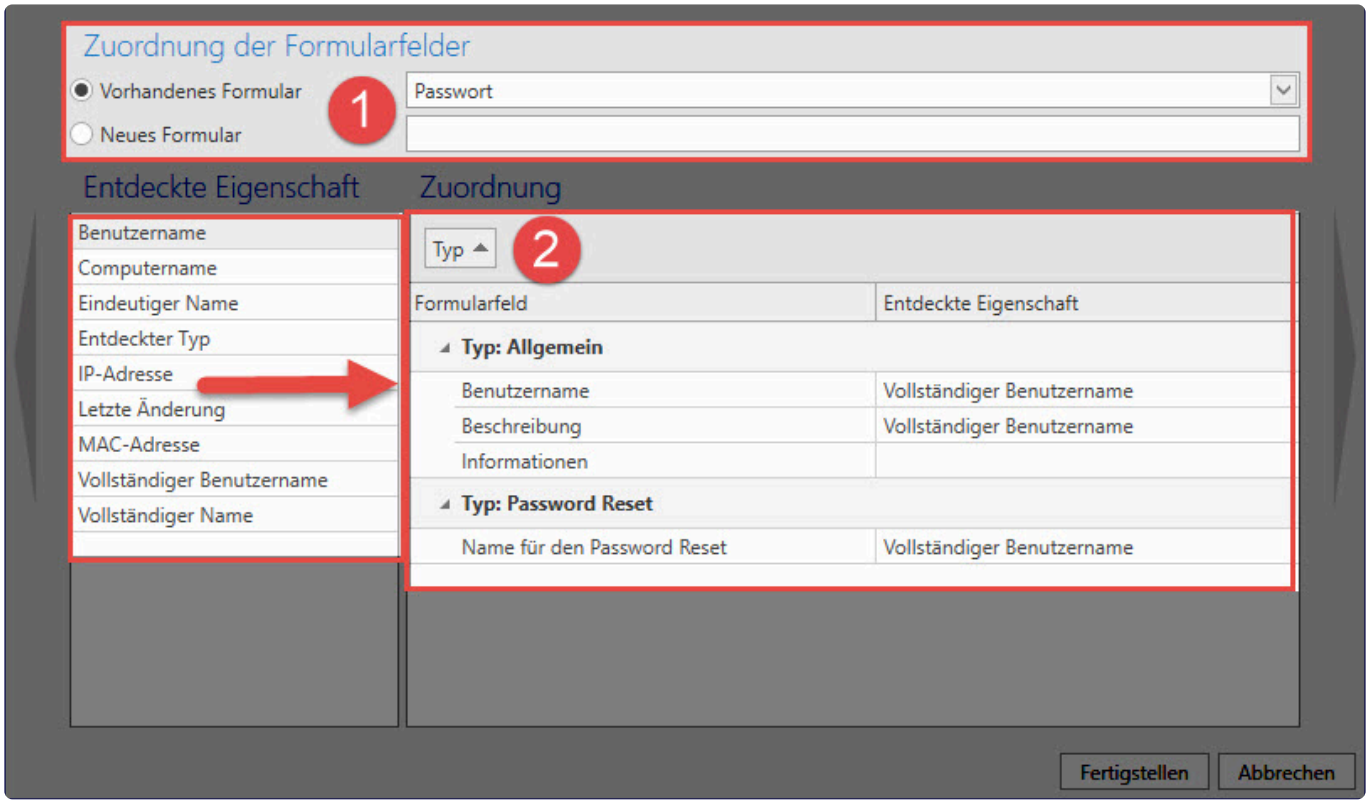
Folgendes Bild zeigt das Ribbon **Zuordnung (Active Directory Benutzer)**:



Beschreibung

1. Hier wählen Sie ein **Vorhandenes Formular** aus oder legen ein **Neues Formular** mit Namen an.
2. Die **Entdeckten Eigenschaften** werden hier angezeigt.
3. Hier erfolgt die **Zuordnung** der **Eigenschaften** zu den Formularfeldern.

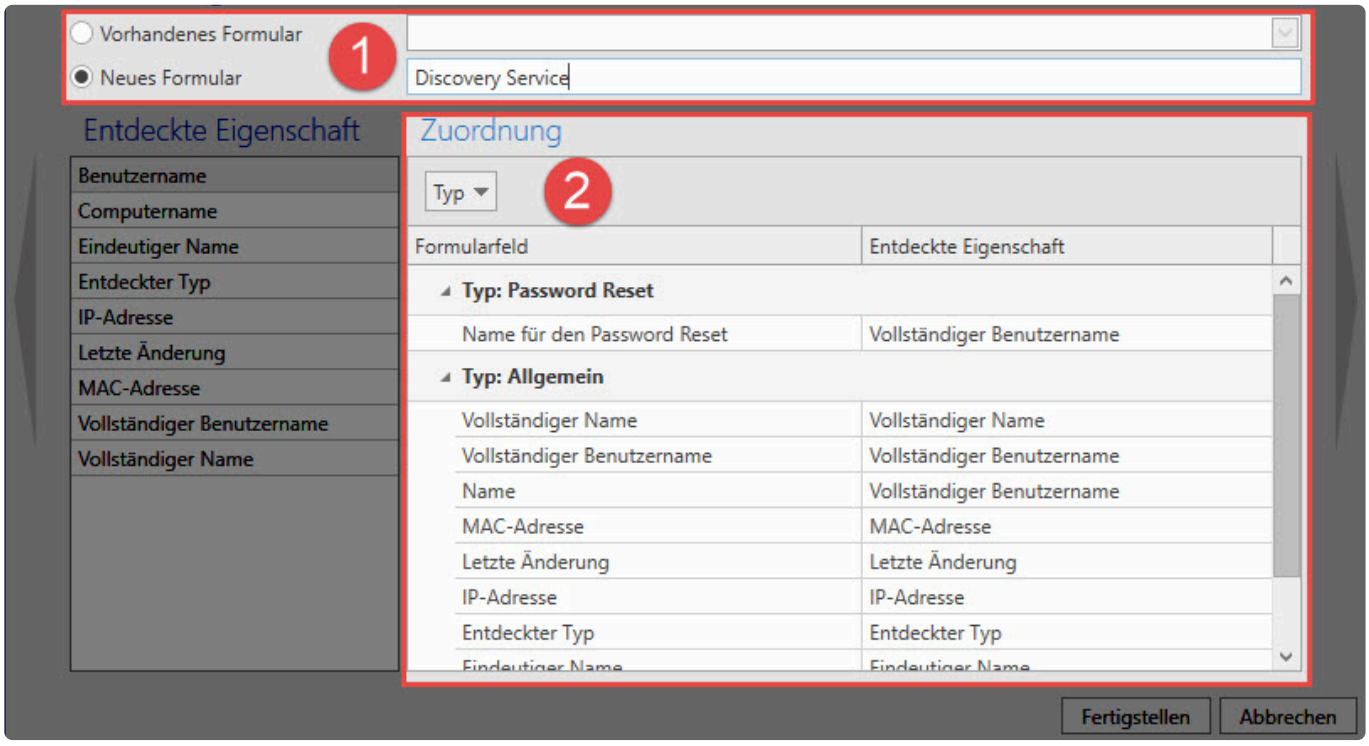
Auswahl “Vorhandenes Formular”



Vorgehensweise:

1. Wählen Sie hier ein **Vorhandenes Formular** aus.
2. Nehmen Sie hier die **Zuordnung** der Felder vor.
   Wichtig ist die Zuordnung des **Typ: Allgemein** und **Typ: Password Reset**. Eine Anpassung führen Sie Sie durch.

Auswahl “Neues Formular”

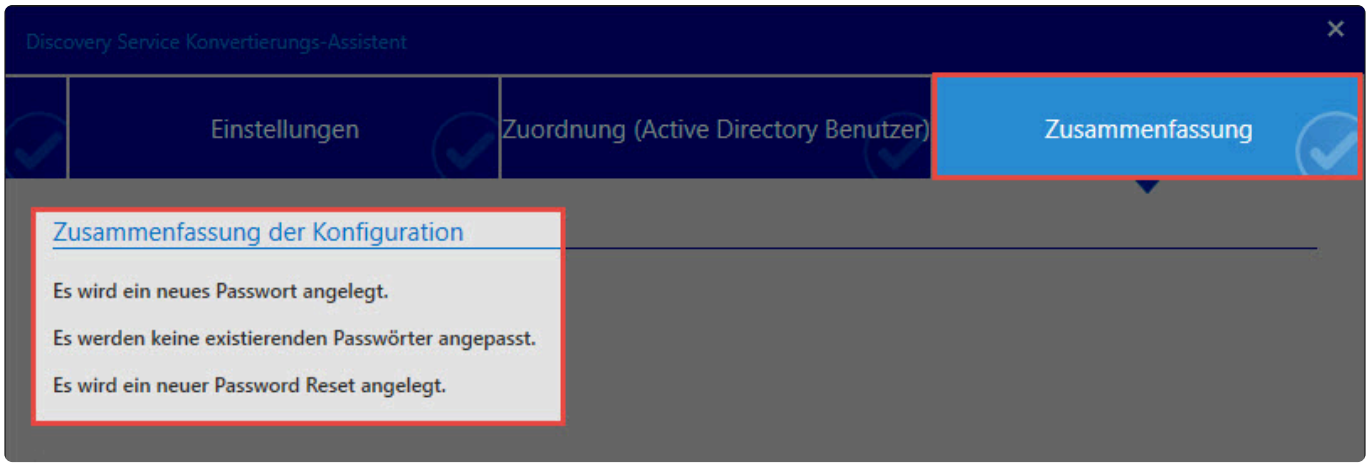


Vorgehensweise:

1. Hier tragen Sie einen Name für das **Neue Formular** ein.
2. Standardmäßig werden die gefundenen Einträge **automatisch** zugeordnet.
   Wichtig ist die Zuordnung des **Typ: Allgemein** und **Typ: Password Reset**. Eine Anpassung führen Sie hier durch.

Zusammenfassung

Im Ribbon **Zusammenfassung** wird eine kurze Übersicht angezeigt, welche Aktionen mit der angelegten Konfiguration durchgeführt werden. Durch den Klick auf **Fertigstellen**, werden diese ausgeführt.



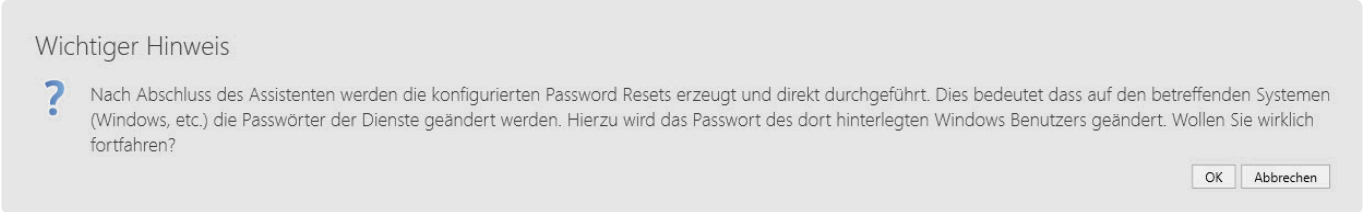
Sicherheitsabfrage

Ein wichtiger Aspekt bei **Password Safe V8** ist die **Sicherheit** der Passwörter von Systemen. Im **Discovery Service** wurde daher für den **letzten Schritt** bei der Erstellung des **Password Resets** eine **Sicherheitsvorkehrung** getroffen.
Verwenden Sie bei der **Konfiguration** die Option “**Password Resets sofort nach der Erzeugung durchführen**”, werden nach dem **Fertigstellen** die **ausgewählten Passwörter** sofort geändert. Bei **Unachtsamkeit** kann das unangenehme Folgen nach sich ziehen.

Sicherheitsstufe 1:
Es wird in der **Zusammenfassung** nach dem Klick auf **Fertigstellen** ein **Wichtiger Hinweis** angezeigt.

> ! **Beachten Sie den Hinweis und lesen Sie sich diesen genau durch!**

Mit diesem **Hinweis** wird Ihnen eine **Übersicht** angezeigt, welche Aktionen durchgeführt werden. Hier können Sie sich noch für einen **Abbruch** entscheiden.
Klicken Sie auf **OK**, wird eine **weitere Sicherheitswarnung** angezeigt.



Sicherheitsstufe 2:

Eine weitere **Sicherheitsabfrage** verdeutlicht, wie wichtig es ist, zu wissen, was Sie tun. Danach ist keine Rückkehr mehr möglich!

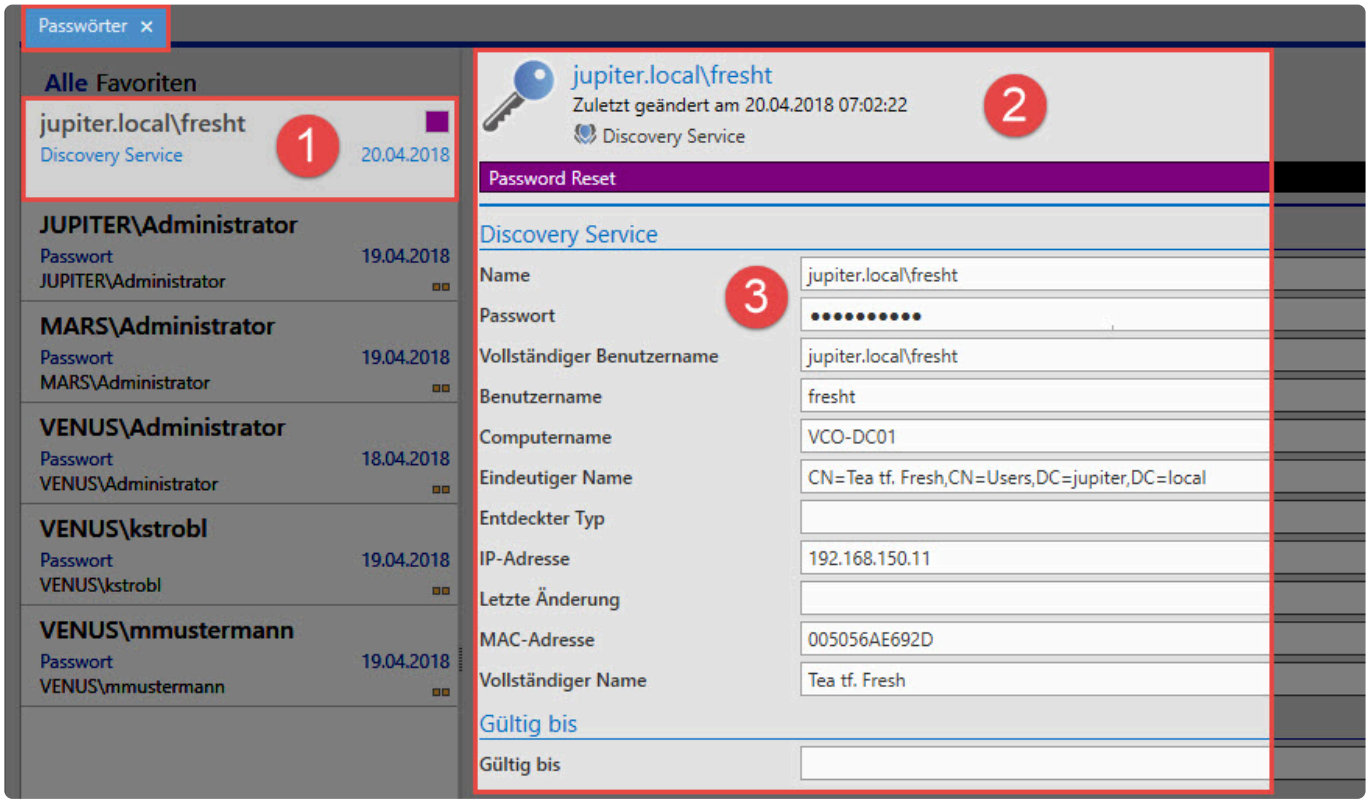
Dies ist die letzte Möglichkeit, eine Ausführung abzubrechen!

Mit der **Eingabe der angezeigten Zahl** und der Bestätigung des **OKs** wird die **Ausführung sofort gestartet** und die **Password Resets** ausgeführt sowie die **dazugehörigen Passwörter geändert**.

Erstellte Passwörter

Nach der **Fertigstellung** werden **Passwörter** und den Optionen entsprechend **Password Resets** für die Einträge erstellt.
Folgendes Beispiel erklärt das **Passwort** sowie den **Password Reset**.

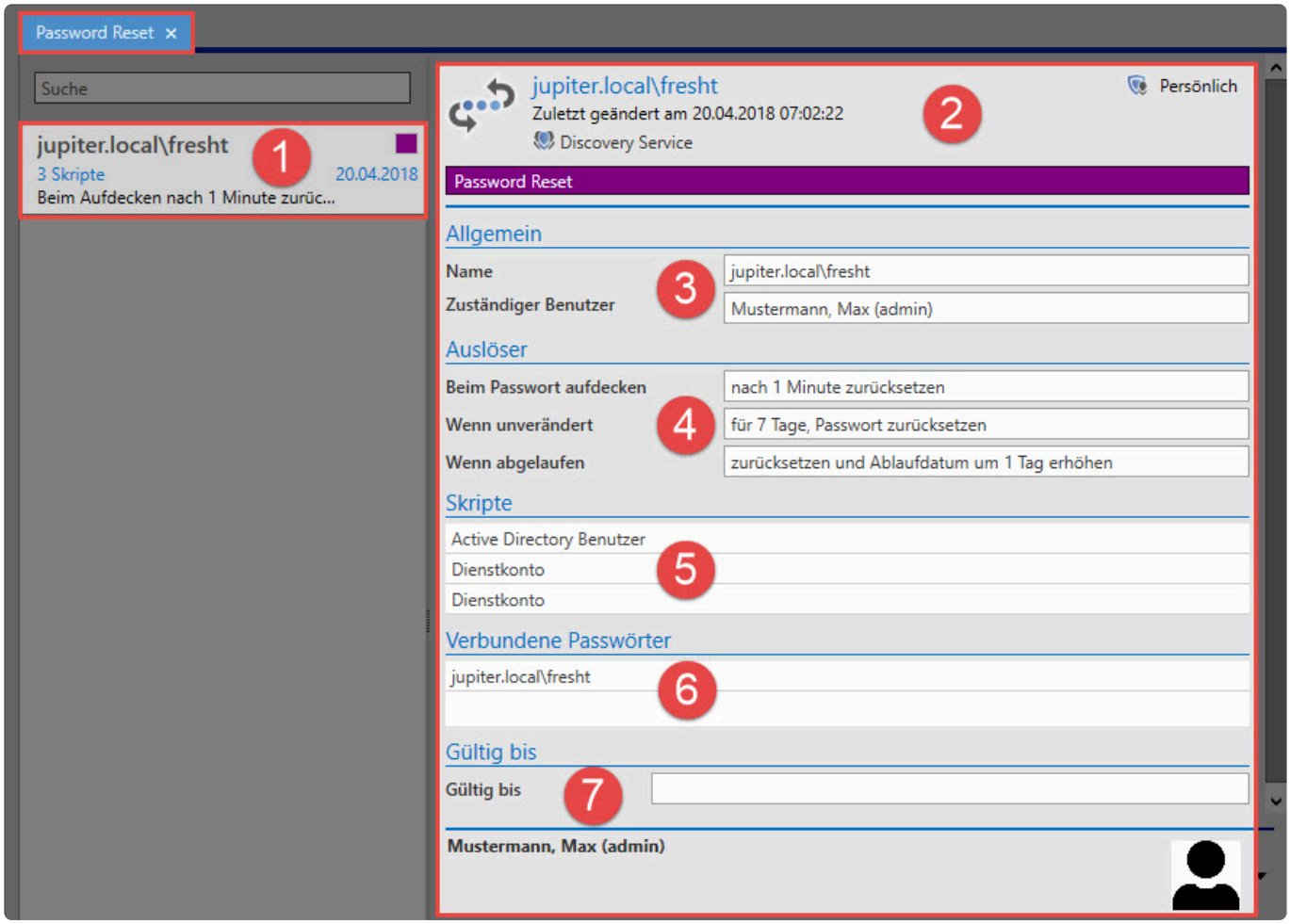
Passwort



1. der Name des erstellten Passwortes
2. allgemeine Daten des Passwortes
3. Daten des Passwortes erstellt aus dem Formular (Vorhandenes oder Neues)

Password Reset

Ein weiteres Passwort wird im **Password Reset Modul** erzeugt und für einen entsprechenden Password Reset benötigt.



Nachfolgend sind die Punkte 1-7 beschrieben:

1. der Name des Password Reset
2. Überblick des Passworts
3. Allgemein
4. Hier werden die Daten für den Auslöser angezeigt.
5. Hier werden die Skripte für die zu ändernden Passwörter angezeigt.
6. das verbundene Passwort, das über den Password Reset zurückgesetzt wird
7. Hier wird die Gültigkeit angezeigt (wenn vergeben).

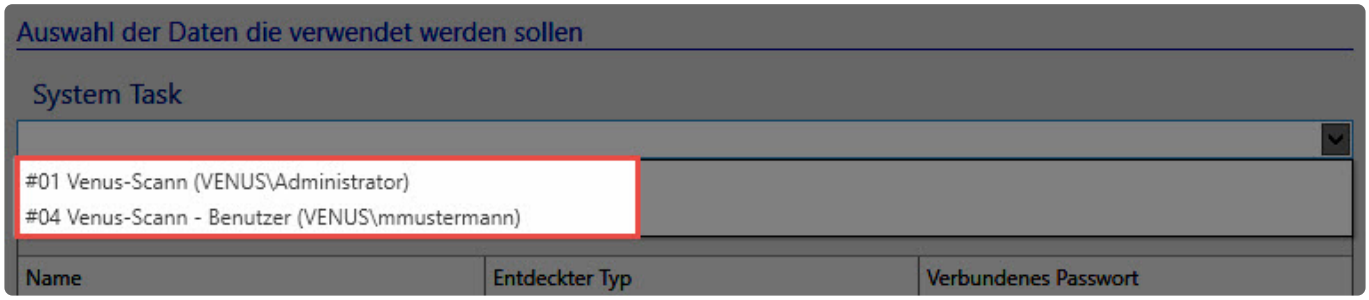
Mit diesen Daten kann nun für den gefundenen **Discovery Service Eintrag** ein **Password Reset** für den Benutzer erstellt werden.
Aktiviert wird das **Password Reset** über die entsprechend eingestellten Auslöser.

Löschen von Einträgen

Nach dem Anlegen eines automatischen **Password Reset** über den **Konvertierungs-Assistent** werden die Daten nicht mehr benötigt und können gelöscht werden. Die gefundenen Einträge haben eine **Bindung** mit dem jeweiligen ausgeführten **Discovery Service Task**. Sie können über die Filterfunktion gefunden und angezeigt werden.

Löschvorgang

Gefundene Einträge im **Discovery Service** können nicht einfach gelöscht und aus den **Discovery Service-Einträgen** entfernt werden. Daher müssen Sie die gefundenen Einträge zuerst über die **erstellten Discovery Service Tasks** löschen.
Wenn aber Einträge über einen **gemeinsamen Discovery Service Task** gefunden wurden, müssen Sie diese auf anderem Weg löschen. Dies passiert, wenn zwei verschiedene Benutzer im gleichen Bereich einen Scan durchgeführt haben. Löscht man nun einen der beiden **Discovery Service Tasks**, so wird nur der Eintrag, der alleinig eine Bindung zu diesem **Discovery Service Task** hatte, gelöscht. Die Einträge des anderen **Discovery Service Task** bleiben erhalten und müssen über den zugehörigen **Discovery Service Task** gelöscht werden. Über den **Konvertierungs-Assistent** ist durch Auswählen eines Eintrags ersichtlich, von welchem **Discovery Service Task** dieser gefunden wurde.



Löschen von Einträgen durch Änderung der Einstellungen im System Task

Wird bei einem vorhandenen **Discovery Service Task** die IP-Range geändert und anschließend der **Discovery Service Task** in dieser neuen IP-Range ausgeführt, so werden die vorher gefundenen Einträge des vorhergehenden **Discovery Service Task** aus dem **Discovery Service** gelöscht. Möchten Sie in einer anderen IP-Range einen **Discovery Service Task** durchführen, sollten Sie einen neuen **Discovery Service Task** anlegen. Dadurch wird verhindert, dass die bereits gefundenen Einträge gelöscht werden. Sollten jedoch die vorhandenen Einträge nicht mehr benötigt werden, so können diese durch den gleichen **Discovery Service Task** mit veränderter IP-Range gelöscht werden.

1. Task A scannt nur IP-Adresse: 192.168.150.1
2. Es werden nur Einträge der IP-Adresse 192.168.150.1 gefunden.
3. Task A wird geändert und scannt nun die IP-Adresse:192.168.150.2
4. Ergebnis:
5. Die Einträge sind nur von der IP-Adresse 192.168.150.2
6. Einträge der IP-Adresse 192.168.150.1 sind gelöscht.
7. Ausnahme:
8. Task B scannt die IP-Adresse: 192.168.150.1
9. Es werden die gleichen Einträge der IP-Adresse 192.168.150.1 gefunden wie bei 1.

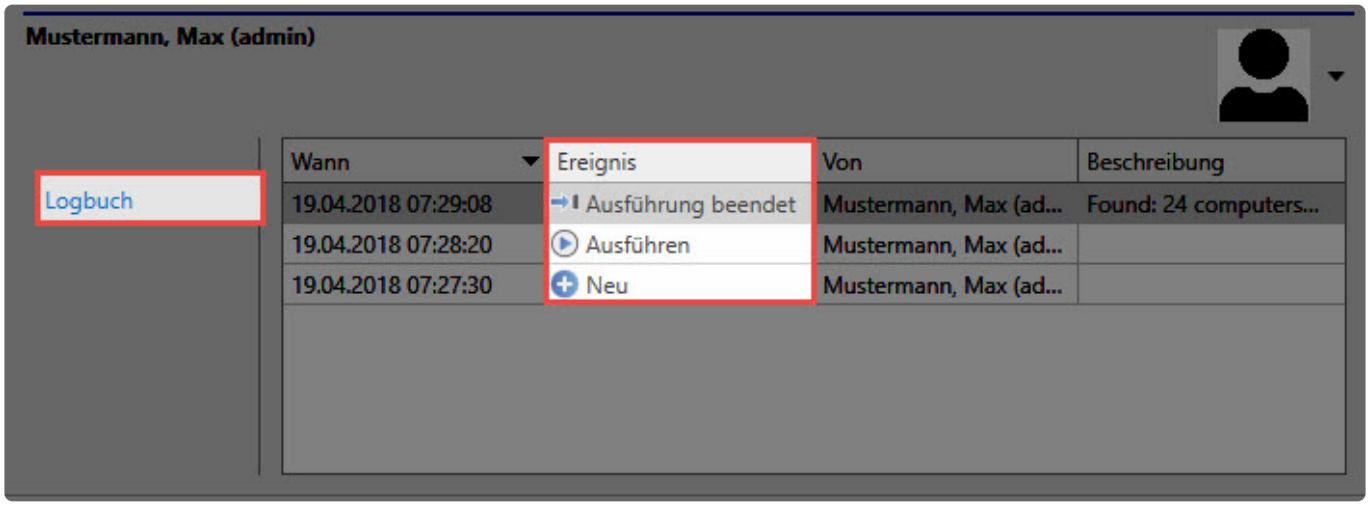
10. Ein erneuter Scan des Task A mit anderer IP-Adresse 192.168.150.2 löscht die Daten vom Task B nicht.

Durch das Löschen der **Discovery Service Tasks** werden die erzeugten **Password Resets** und angelegte **Passwörter** mittels **Konvertierungs-Assistent** nicht gelöscht.

Logbuch

Für die Überprüfung der **Discovery Service Task** ist das **Logbuch im Footer** des **Discovery Service Task** enorm hilfreich. Hier werden die Informationen über den Vorgang des **Discovery Service Task** angezeigt. Dies passiert sowohl im **Footer** als auch ausführlicher im **Logbuch-Modul**. Für die Anzeige des Footers benötigt der Benutzer das Benutzerrecht in den Benutzereinstellungen der **Kategorie: Fußbereich: Logbuch im Fußbereich anzeigen (Aktiviert)**.

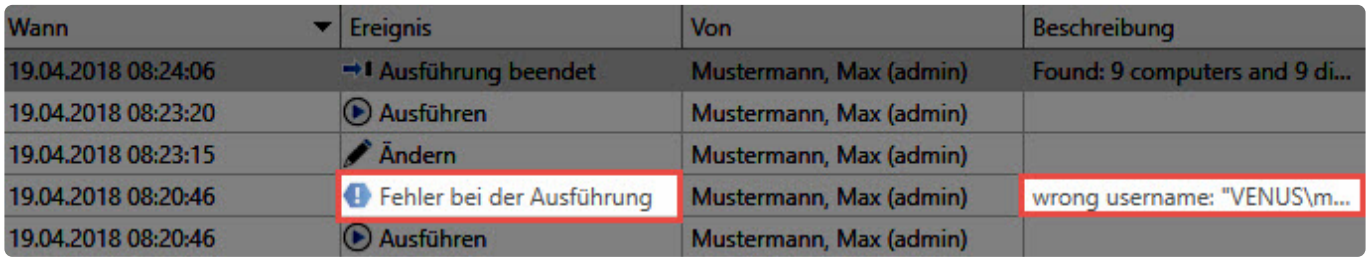
Anzeige im Footer



Folgende **Ereignisse** werden im **Logbuch des Footers** und im **Logbuch-Modul** angezeigt:

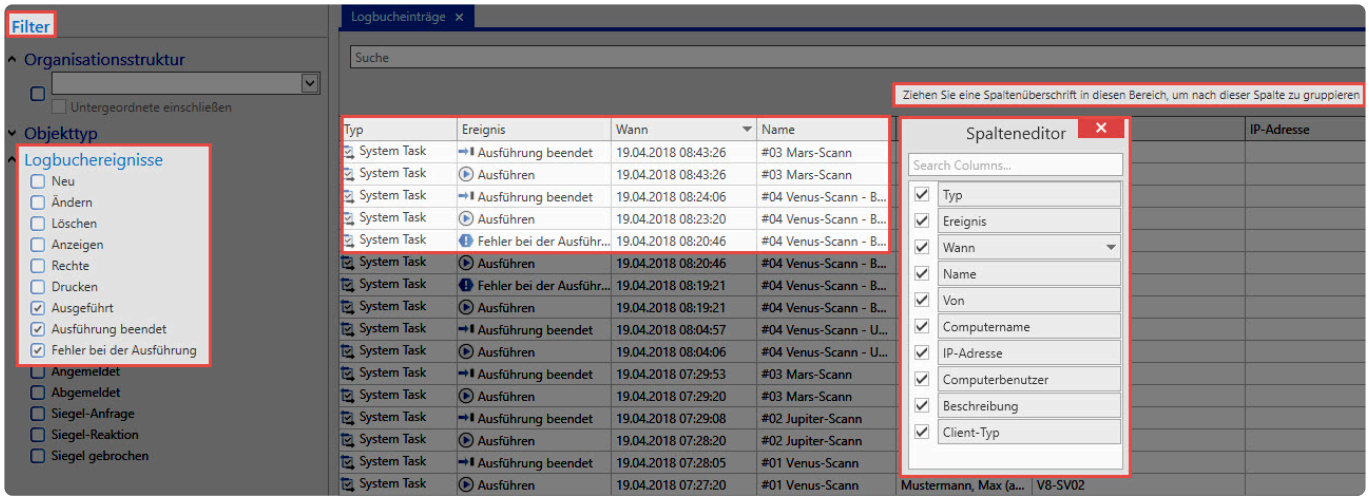
1. Neu
2. Ändern
3. Ausführen
4. Ausführung beendet
5. Fehler bei der Ausführung

Tritt im **Discovery Service Task** ein Fehler bei der Ausführung auf, wird dieser ebenfalls im **Logbuch des Footers** mit **zusätzlicher Information** angezeigt.



Anzeige im Logbuch

Allgemein werden im **Logbuch-Modul** genauere Informationen über den **Discovery Service Task** angezeigt. Die Auswahl der anzuzeigenden Daten erfolgt über den Filter. Ebenso werden hier die gleichen **Ereignisse** verwendet wie im Footer des **Discovery Service Task**.

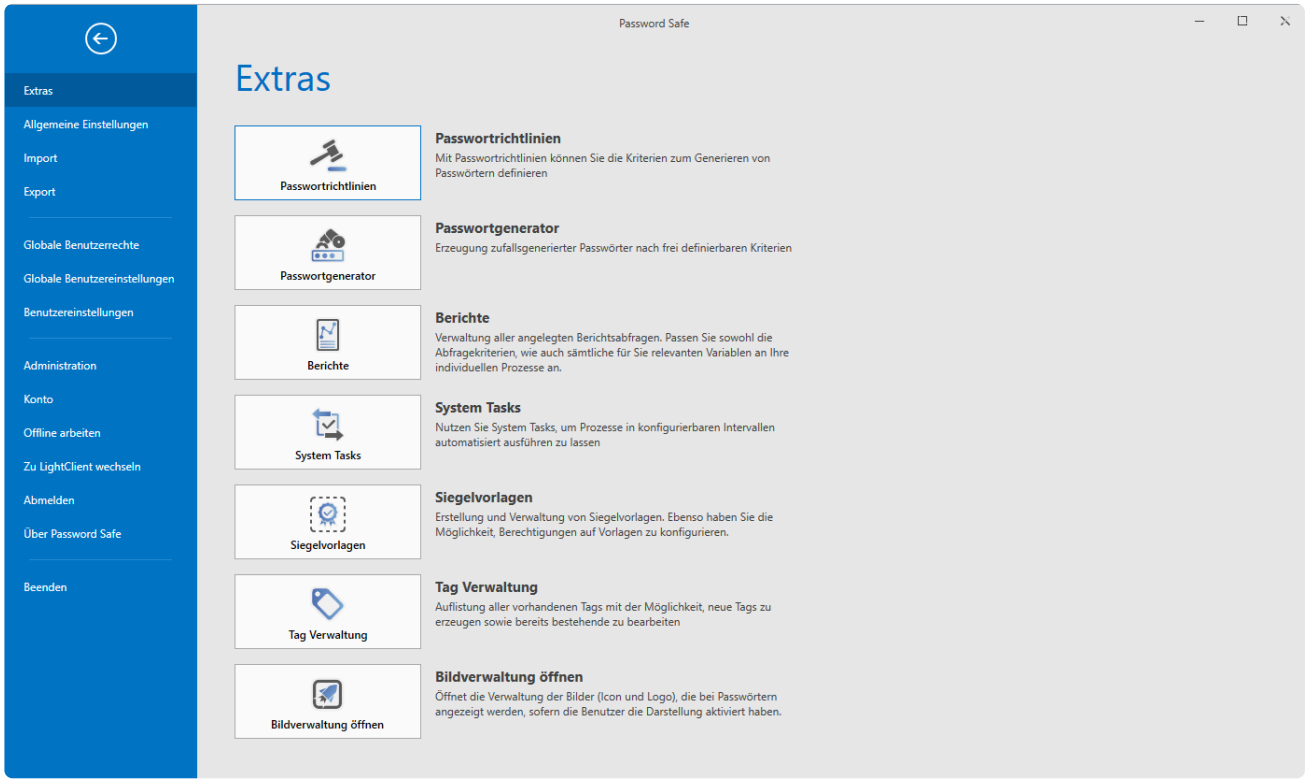


Mit dem Spalteneditor können Sie Ihre Daten in der Tabelle nach Priorität anordnen und anzeigen lassen.

Hauptmenü

Was ist das Hauptmenü/Backstage?

Alle Einstellungen, welche nicht an ein bestimmtes Modul gebunden sind, definieren Sie im **Backstage**. Dadurch sind die Einstellungen jederzeit und in jedem Modul komfortabel erreichbar.



- **Extras**
- **Allgemeine Einstellungen**
- **Import**
- **Export**
- **Benutzerrechte**
- **Benutzereinstellungen**
- **Administration**
- **Konto**

Import

Was ist der Import?

Über den Import können Sie Daten aus anderen Tools in den Password Safe übertragen. Unterstützt werden die Formate .csv sowie im Speziellen Keepass (.xml). Gestartet wird der Import im **Hauptmenü** unter **Import**

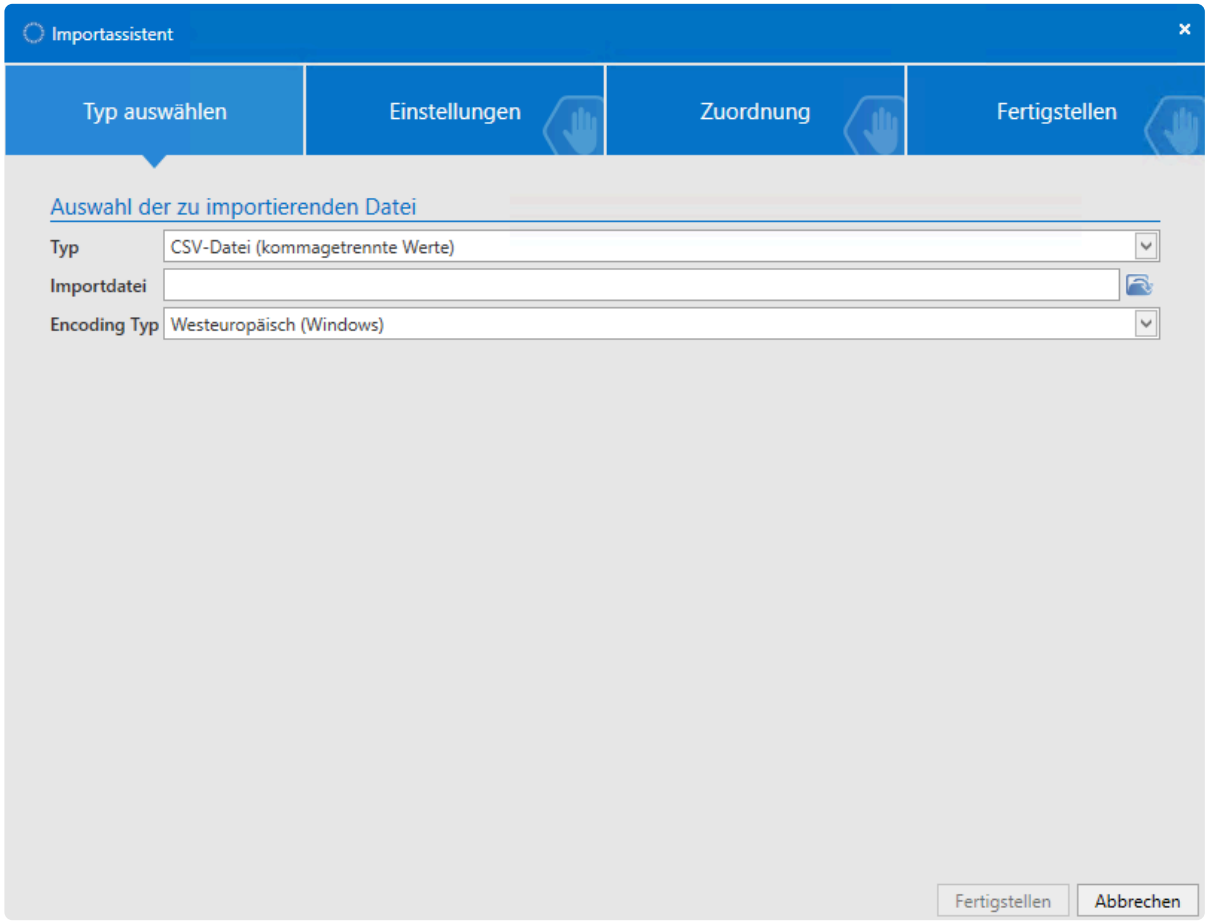
Relevantes Recht

Zum Import von Daten benötigen Sie das Benutzerrecht **Kann importieren**.

Der Importassistent

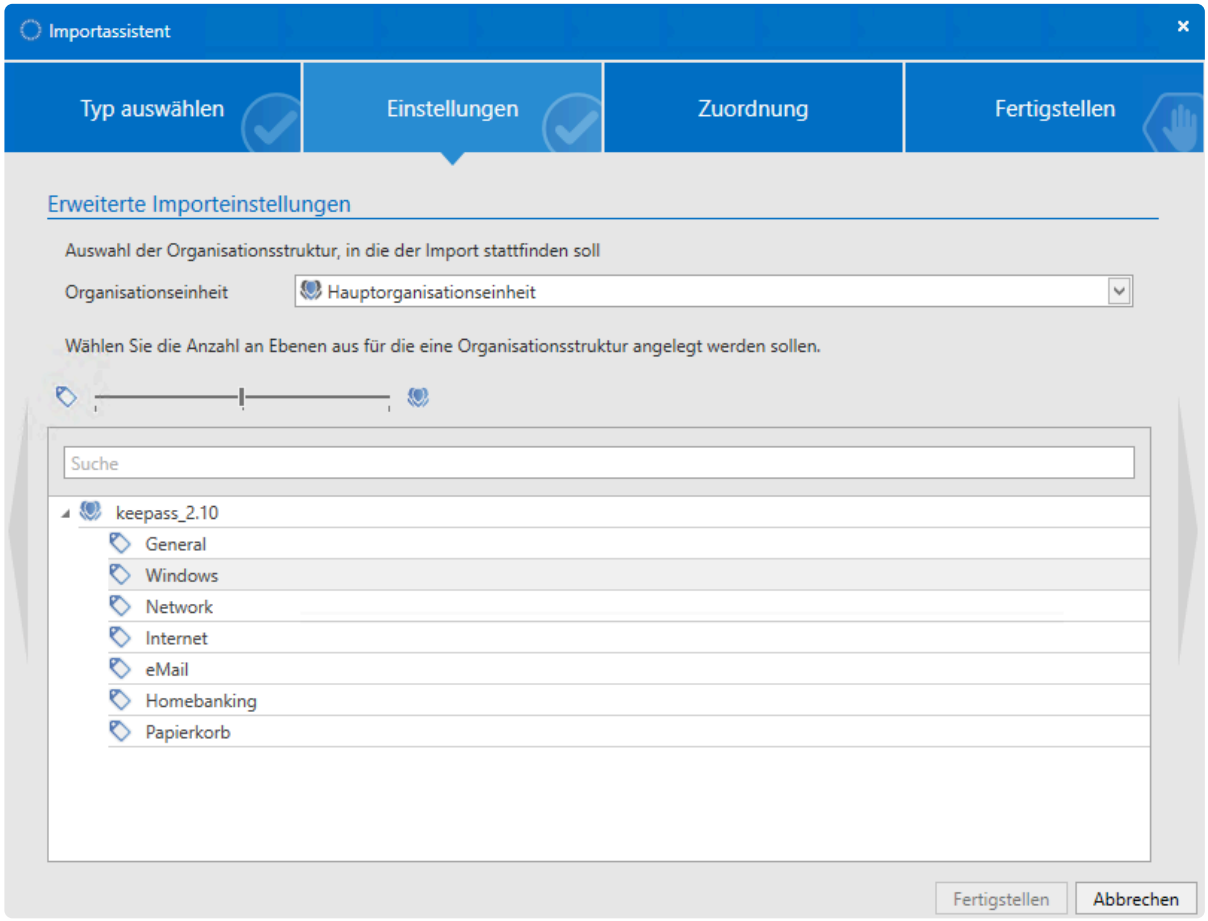
Der Assistent unterstützt Sie in vier Schritten

Typ auswählen



Im ersten Schritt wählen Sie die Datei aus, aus welcher der Import erfolgen soll.

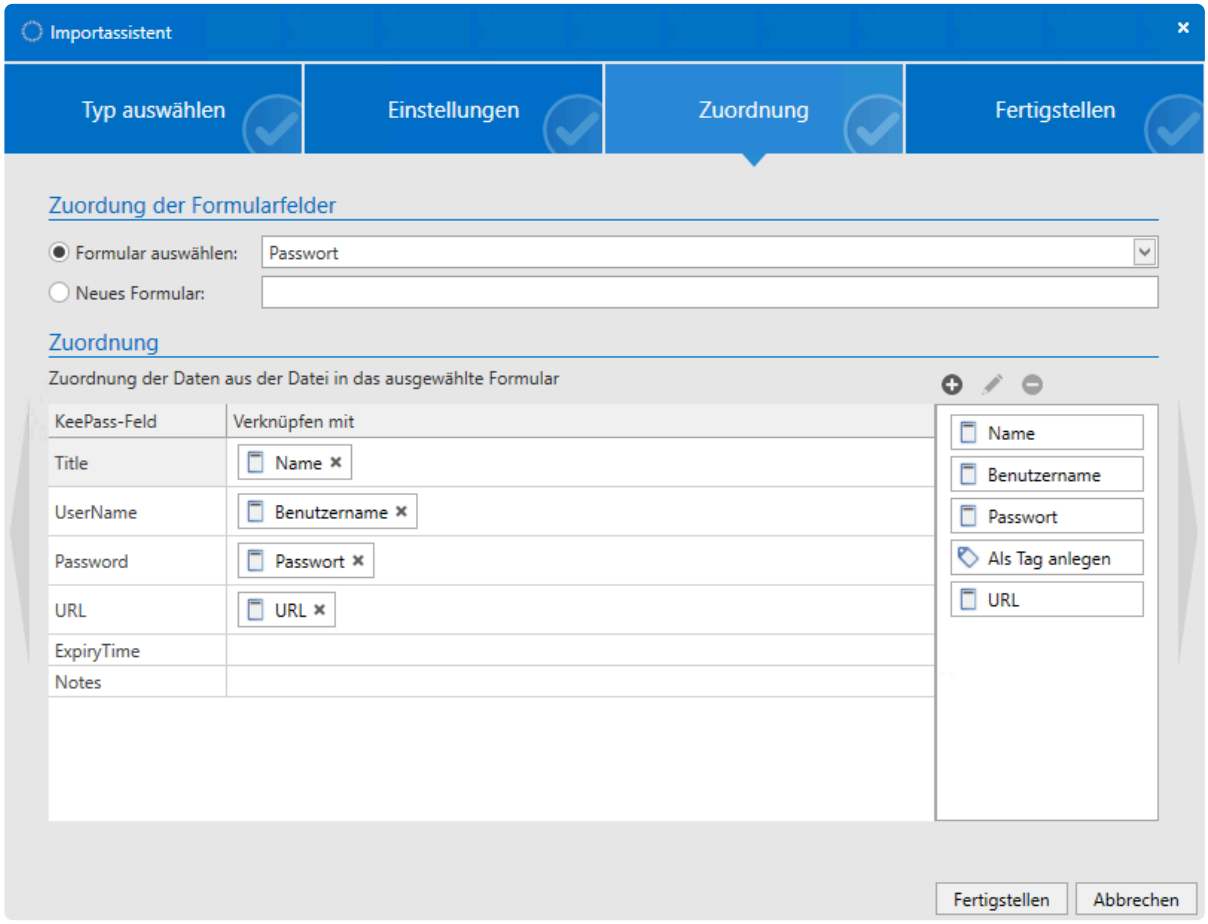
Einstellungen



1. In den Einstellungen legen Sie fest, wo die zu importierende Struktur gespeichert werden soll. In diesem Beispiel wird in die Hauptorganisationseinheit importiert. Über ein Dropdown-Menü kann auch eine der bestehenden Organisationseinheiten gewählt werden.
2. Über den Schieberegler legen Sie fest, ob die zu importierenden Strukturen als Organisationseinheit oder als Tag importiert werden sollen. Schieben Sie den Regler nach links, werden lediglich Tags erstellt. Befindet sich der Regler rechts, werden alle Objekte als Organisationsstruktur angelegt. Darüber hinaus konfigurieren Sie über das Kontextmenü der rechten Maustaste jedes Objekt separat. Auch das Ignorieren von Ordnern ist möglich.

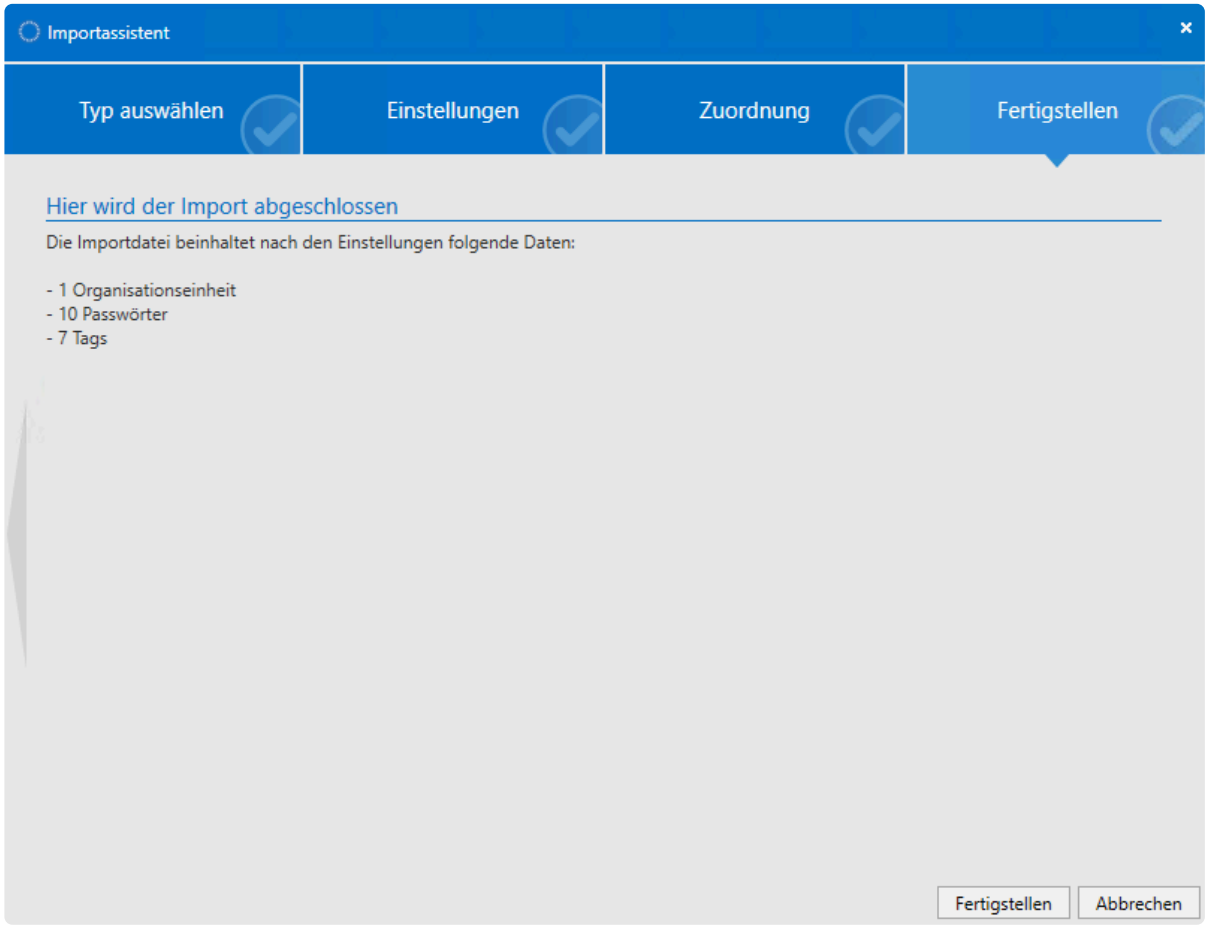
> Da es in Password Safe keine Ordner gibt, muss beim Import festgelegt werden, ob ein Ordner als Organisationsstruktur oder als Tag angelegt werden soll.

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 Sie in der obersten Zeile ausgewählt haben, ordnen Sie Formularfelder aus der Liste rechts nun per Drag & Drop den zu importierenden Formularfeldern zu. Auch die Erstellung von neuen Formularen ist möglich.

Fertigstellen



Im abschließenden Arbeitsschritt werden die getroffenen Einstellungen zusammengefasst. Über **Fertigstellen** schließen Sie den Assistenten und startet den Import.

Export

Was ist der Export?

Über den Export können Sie verschiedene Daten aus der Datenbank in entsprechenden Dateien speichern. Dies kann sowohl manuell, als auch über einen automatisiertem **System Task** erfolgen.

> ! Bitte beachten Sie, dass das Extrahieren von Passwörtern stets kritisch zu betrachten ist. Sind die Daten exportiert, kann über das **Logbuchs** nicht mehr nachvollzogen werden, was mit ihnen geschieht, da jene Daten nicht mehr der Revision unterliegen können.

Aufgerufen wird der Export im **Hauptmenü** unter **Export**. Sie finden hier zwei Arten von Export. Den **HTML-WebViewer Export** sowie den **Export Assistenten**. Letzterer unterteilt sich in vier Unterkategorien.

HTML WebViewer-Export

Was ist der WebViewer-Export?

Mit dem **WebViewer** hat **Password Safe** eine Möglichkeit geschaffen, **Passwörter** in eine verschlüsselte **HTML-Datei** zu exportieren. Die Auswahl der Datensätze erfolgt über den **Filter**. Es werden die Passwörter exportiert, auf welche der Benutzer entsprechend berechtigt ist. Die Anzeige erfolgt in einem aktuellen Browser mit **aktiviertem JavaScript.**

Datensicherheit

Selbstverständlich ist die HTML WebViewer Datei **verschlüsselt**

- Der Export selbst, wird über ein entsprechendes **Benutzerrecht** geschützt
- Auf die Passwörter benötigt der Benutzer das **Export-Recht**

Nötige Rechte

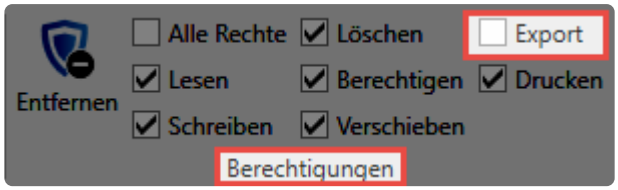
Zum Erstellen eines WebViewer benötigen Sie folgende Rechte.

Benutzerrecht

Kann HTML WebViewer exportieren

Export-Recht auf die Passwörter

Wird wie gewohnt über die Ribbon konfiguriert:



Export einer HTML-Datei

Die Erstellung der **HTML-Datei** wird im **Hauptmenü** über **Export WebViewer** gestartet.

Der **HTML WebViewer-Assistent** führt durch den **WebViewer-Export**.

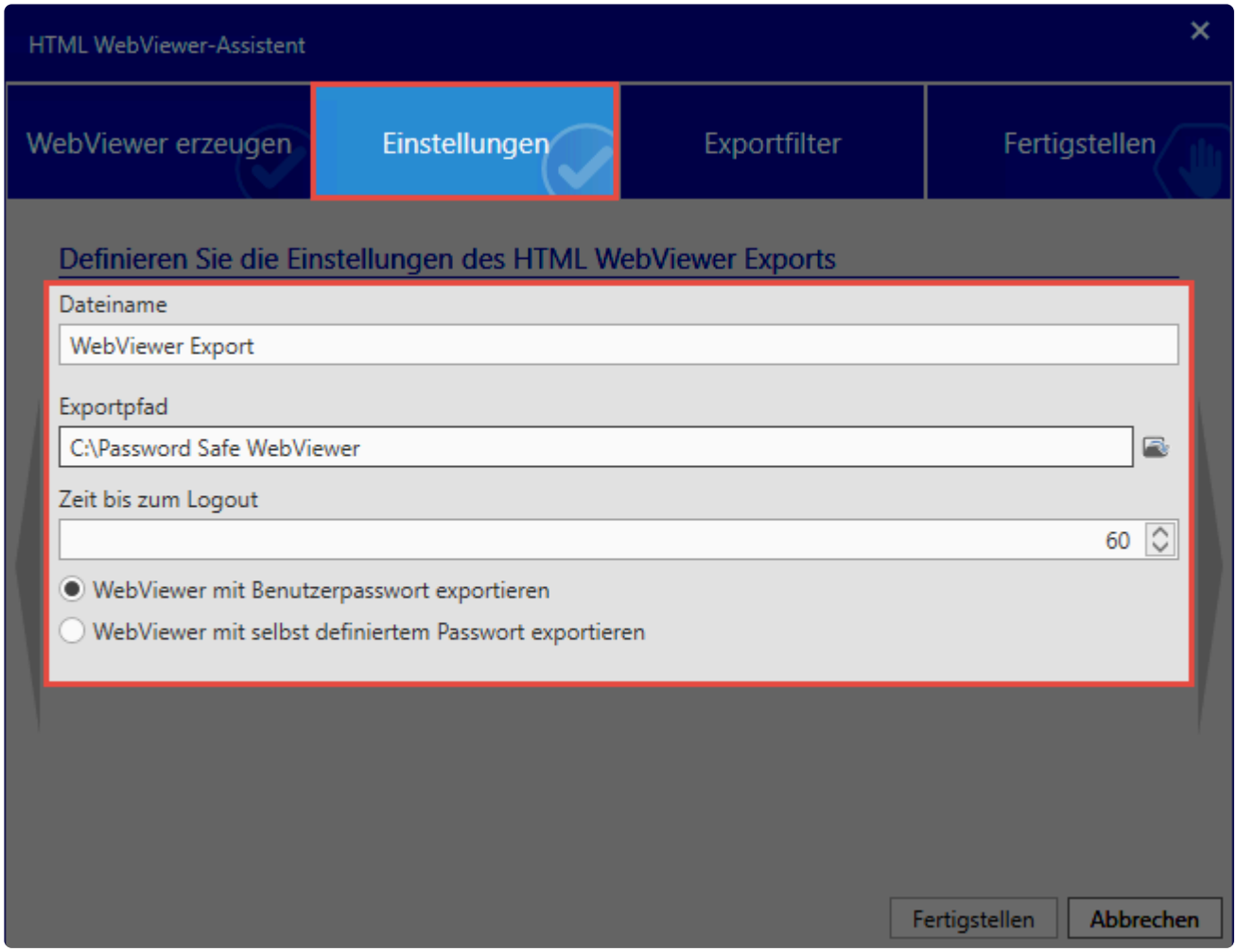
WebViewer erzeugen

Unter **WebViewer erzeugen** werden allgemeine Informationen und Hinweise zum Export angezeigt.

Einstellungen

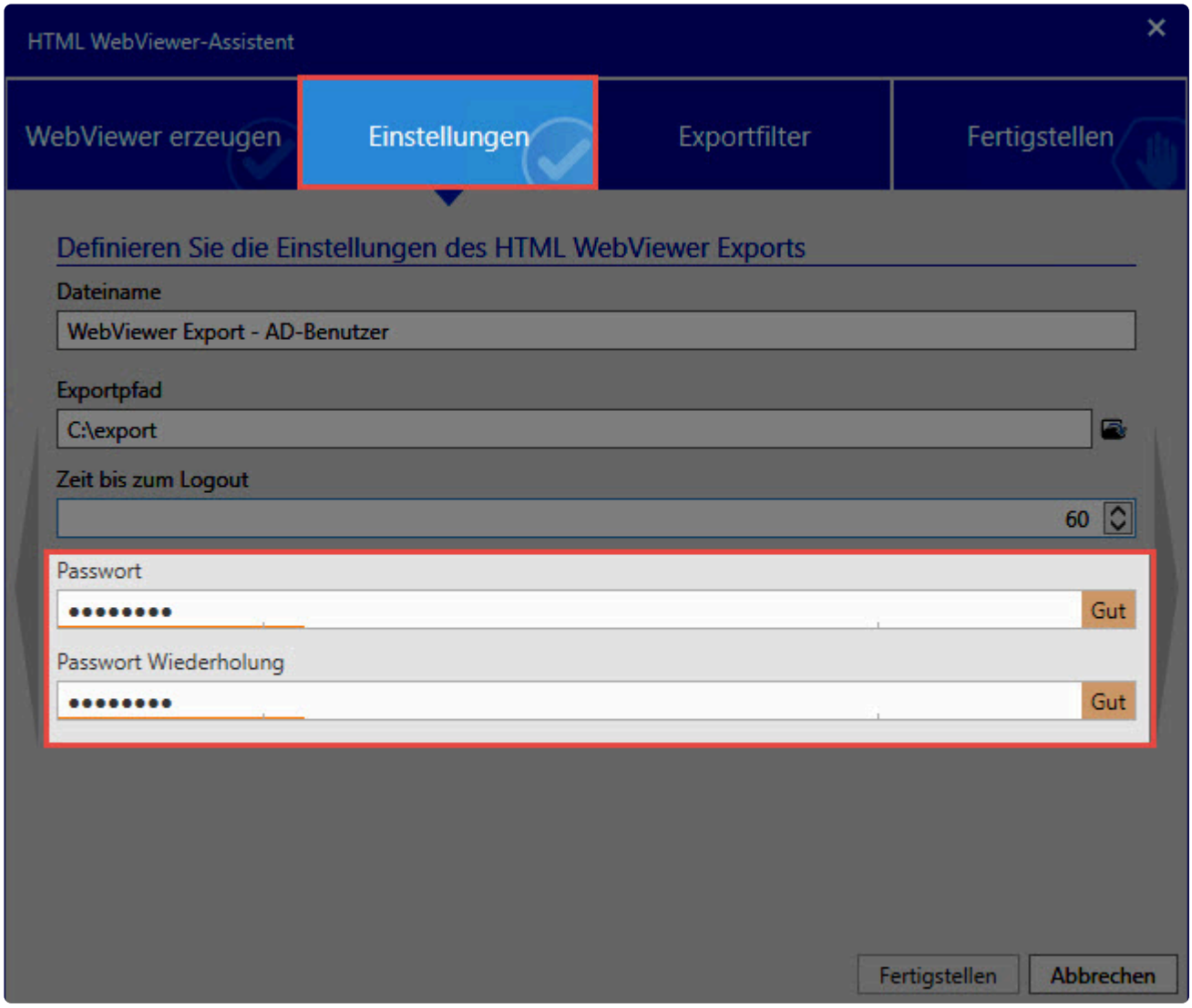
Hier geben Sie allgemeine Informationen wie **Name** und **Exportpfad** für die **HTML-Datei** an.

Dateiname: Name frei wählbar
Exportpfad: Speicherort der Datei auf dem Client
Zeit bis zum Logout: Zeit in Sekunden, wie lange das Fenster ohne Aktivität offen bleibt
Standardwert: 60 Sekunden, Benutzer kann Zeit vorgeben
WebViewer mit **Benutzerpasswort** oder neuem, frei **definiertem Passwort** exportieren: Hier kann entschieden werden, ob ein neues Passwort für den Export vergeben werden soll.



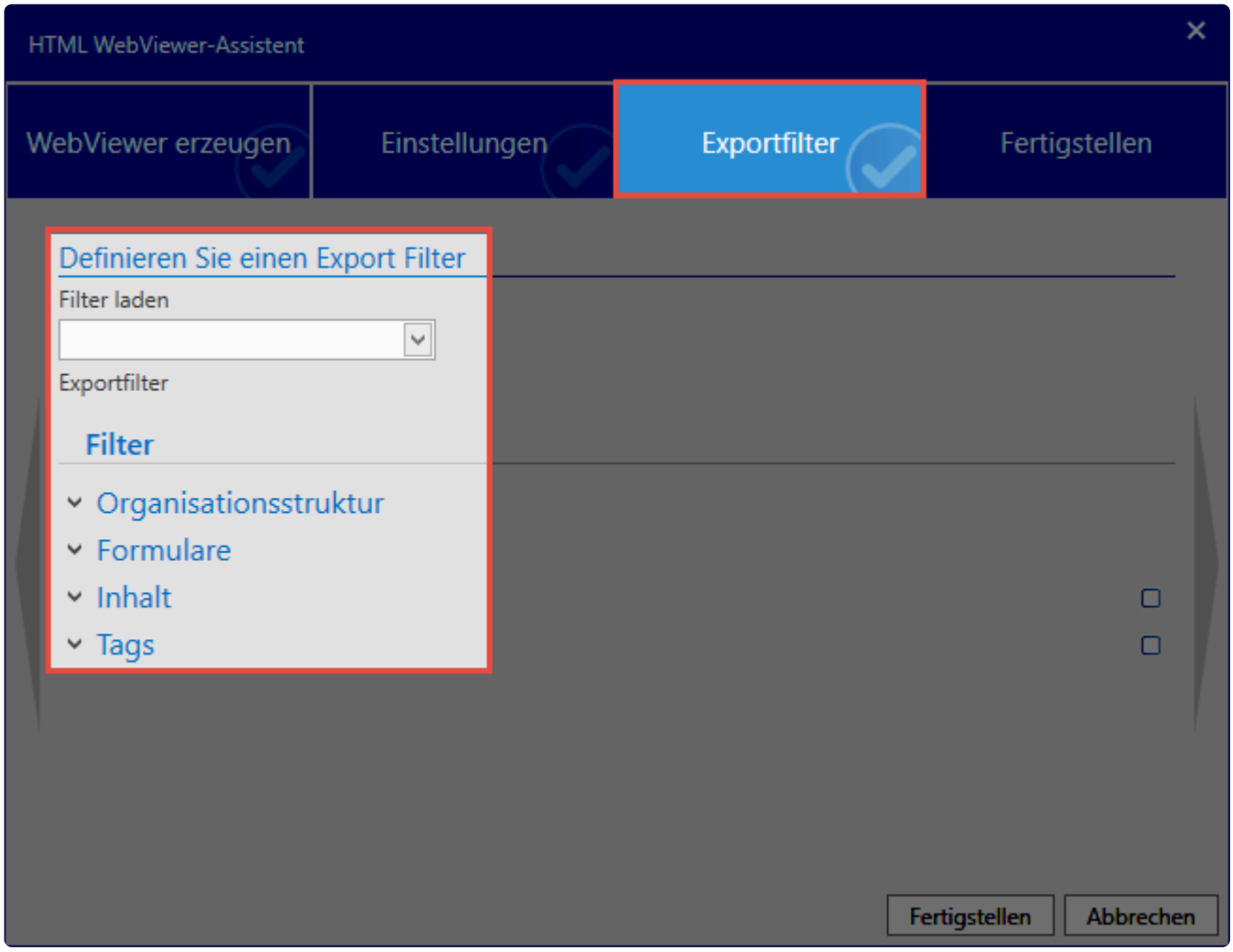
WebViewer Export mit einem Active Directory Benutzer

Bei Verwendung eines **Active Directory Benutzers** für den **WebViewer Export** müssen Sie explizit ein **Passwort** angeben.



Exportfilter

Der **Exportfilter** funktioniert analog zu den Filtern in den Modulen.



Fertigstellen

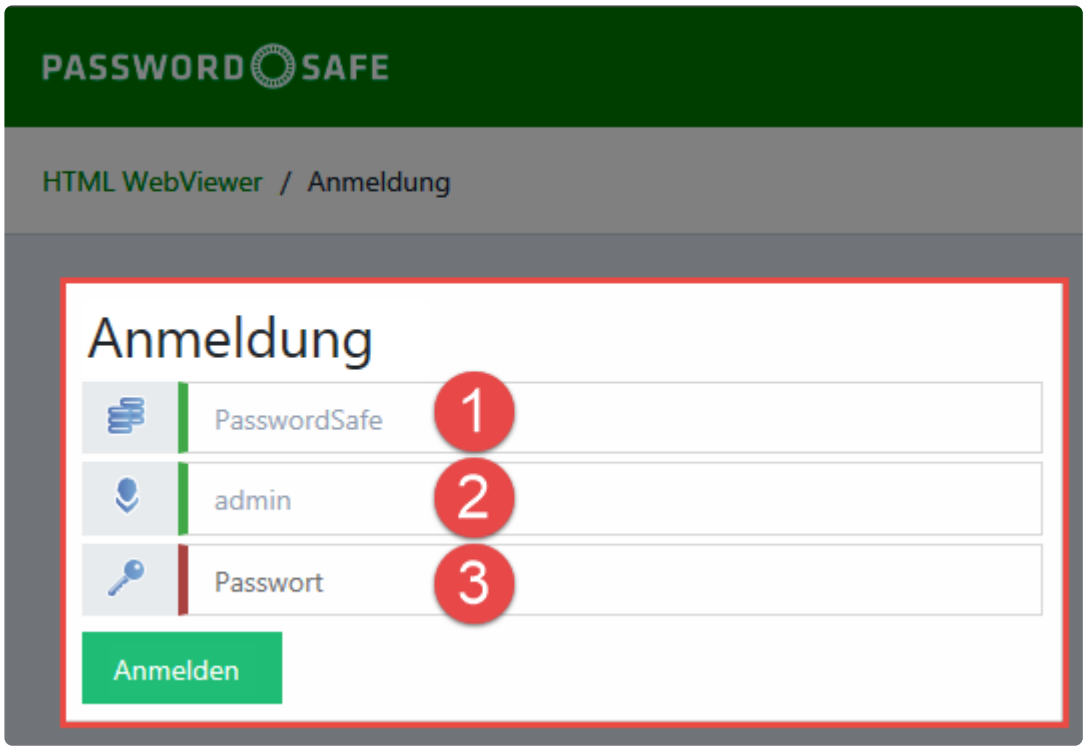
Unter **Fertigstellen** wird Ihnen angezeigt wie viele Passwörter exportiert werden. Hier schließen Sie den Vorgang ab.

Ein Hinweis informiert Sie über den Exportvorgang.

Verwendung der HTML WebViewer Datei

Hben Sie die **HTML-Datei** im Exportpfad erstellt, können Sie sie direkt verwenden. Ein Anwendungsfall ist auch die Datei auf einen mobilen Datenträger zu kopieren. Somit können Sie auch unterwegs auf Ihre Passwörter zugreifen. Das Benutzen der **HTML-Datei** erfolgt in einem Standardbrowser und zeigt beim Start die **Password Safe – HTML WebViewer / Anmeldung** an. Vorgegeben ist die **Datenbank** und der **Benutzername**. Die Anmeldung erfolgt mit dem **Passwort** des Benutzers.

Bei falscher Eingabe des Passwortes wird das Anmelden zeitlich gesperrt!



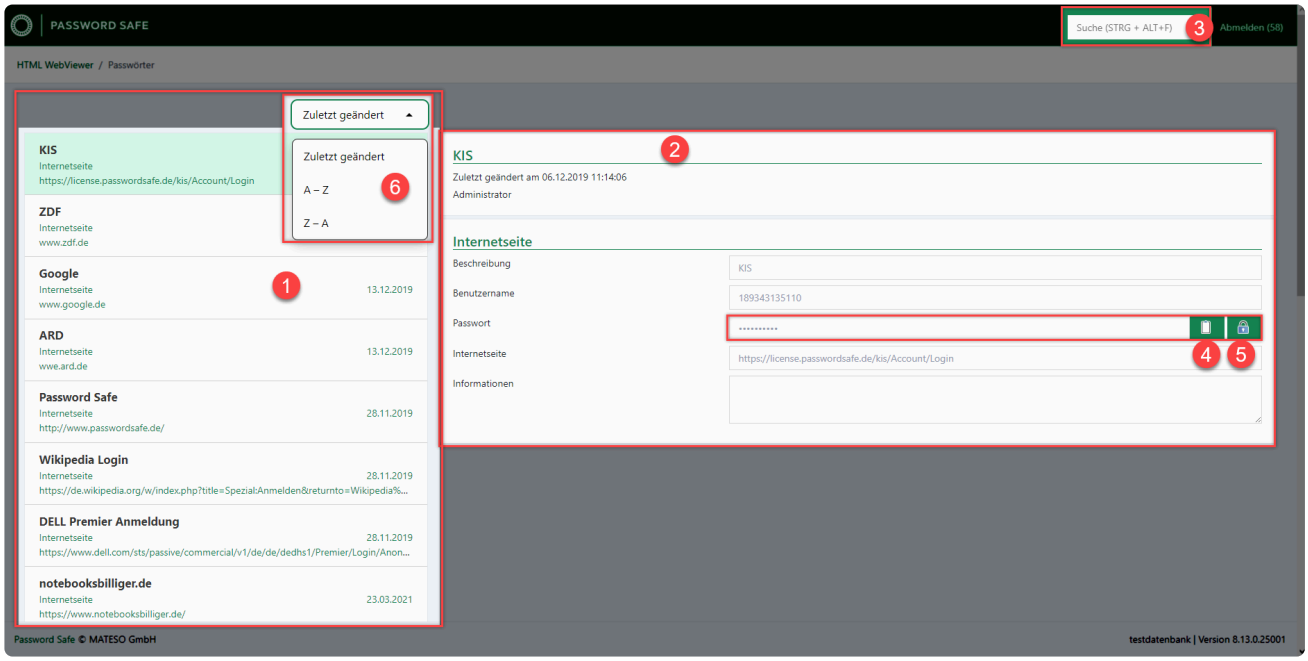
Übersicht

Nach dem Anmelden am **Passwort Safe** wird die Übersichtsseite des **HTML-WebViewer** mit den Passwörtern angezeigt.

Bei mehr als 20 Passwörtern können Sie auf die Suche zurück greifen.

1. Anzeige der Datensätze (max. 20)

2. Detailinformation des ausgewählten Datensatzes
3. Suche, Abmelden, Timeout
4. In Zwischenablage kopieren
5. Aufdecken
6. Filtermöglichkeit (A-Z, Z-A, zuletzt geändert)



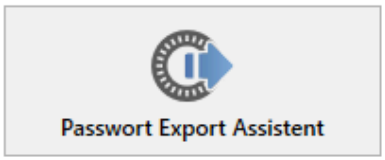
Schließen der HTML WebViewer Übersicht

Das Abmelden erfolgt durch einen Klick auf **Abmelden**. Bei längerer **Inaktivität** werden Sie **automatisch** nach Ablauf der eingestellten Zeit abgemeldet. Der Browser zeigt anschließend wieder die **Password Safe – HTML WebViewer / Anmeldung** an und zusätzlich den Grund der Abmeldung.Sie können sich direkt wieder anmelden.

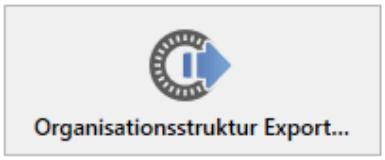
Export Assistent

Für jeden Anwendungsfall der richtige Assistent

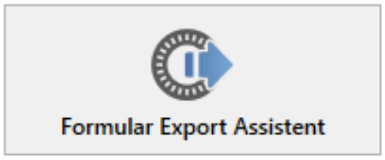
Es gibt vier verschiedene Exportassistenten.



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, wird hier nur der Passwort Export Assistent betrachtet**.

Der Passwort Export Assistent

Der Assistent ermöglicht es Ihnen Datensätzen in das gängige .csv Format zu exportieren. Im Gegensatz zum WebViewer Export ist die Exportdatei nicht durch ein Passwort geschützt. Aus diesem Grund gehen Sie mit diesem Feature bitte behutsam um.

Starten des Passwort Export Assistenten

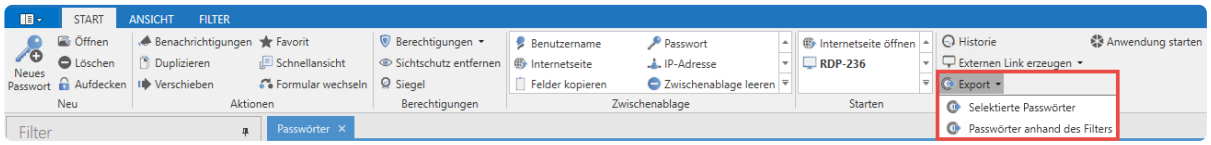
Den Export Assistenten können Sie über unterschiedliche Wege starten:

Start über das Hauptmenü

Sie können den Assistenten im **Hauptmenü** unter **Extras** aufrufen. Es werden dann stets **alle Passwörter** exportiert, auf die der angemeldete Benutzer berechtigt ist.

Start über die Ribbon

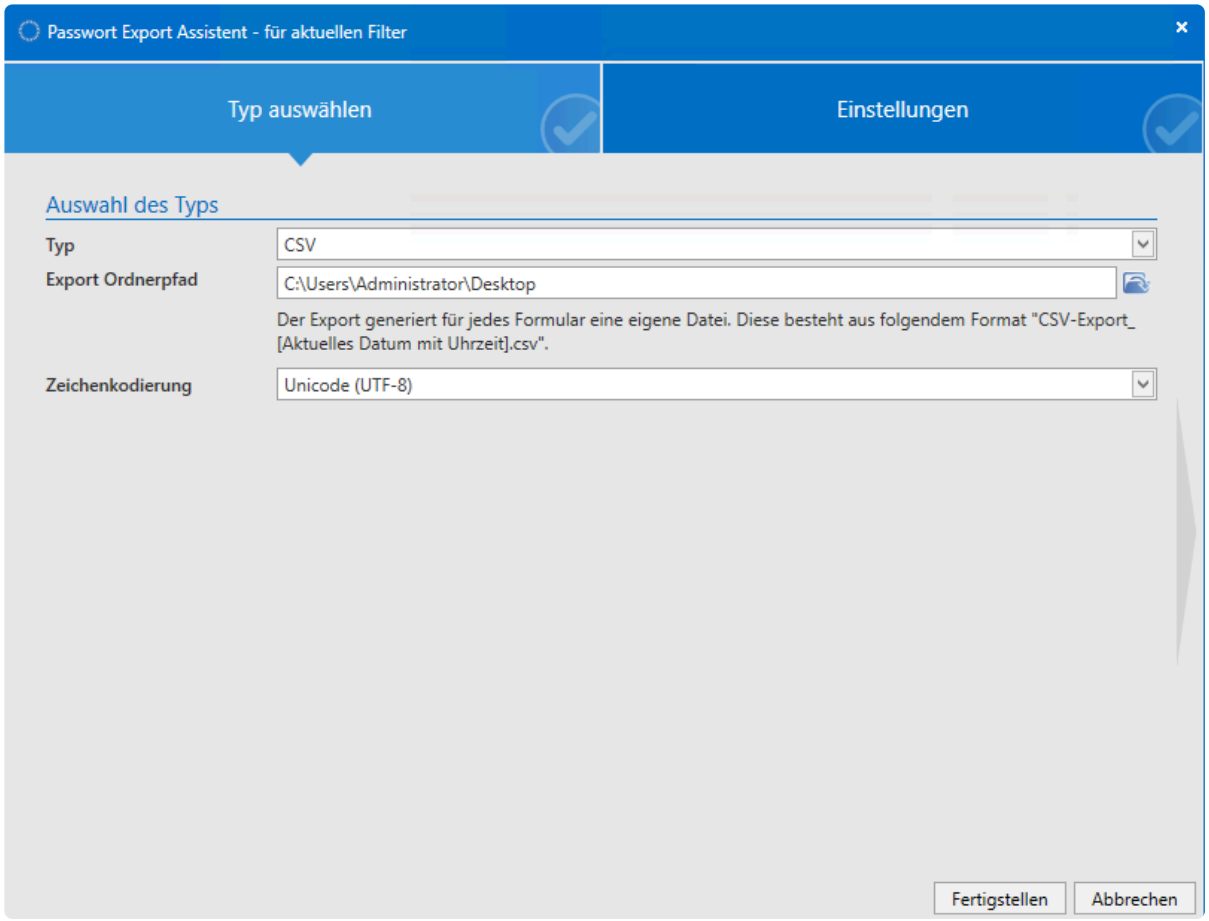
Auch über die **Ribbon** im **Modul Passwörter** können Sie den Export anstoßen.



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.



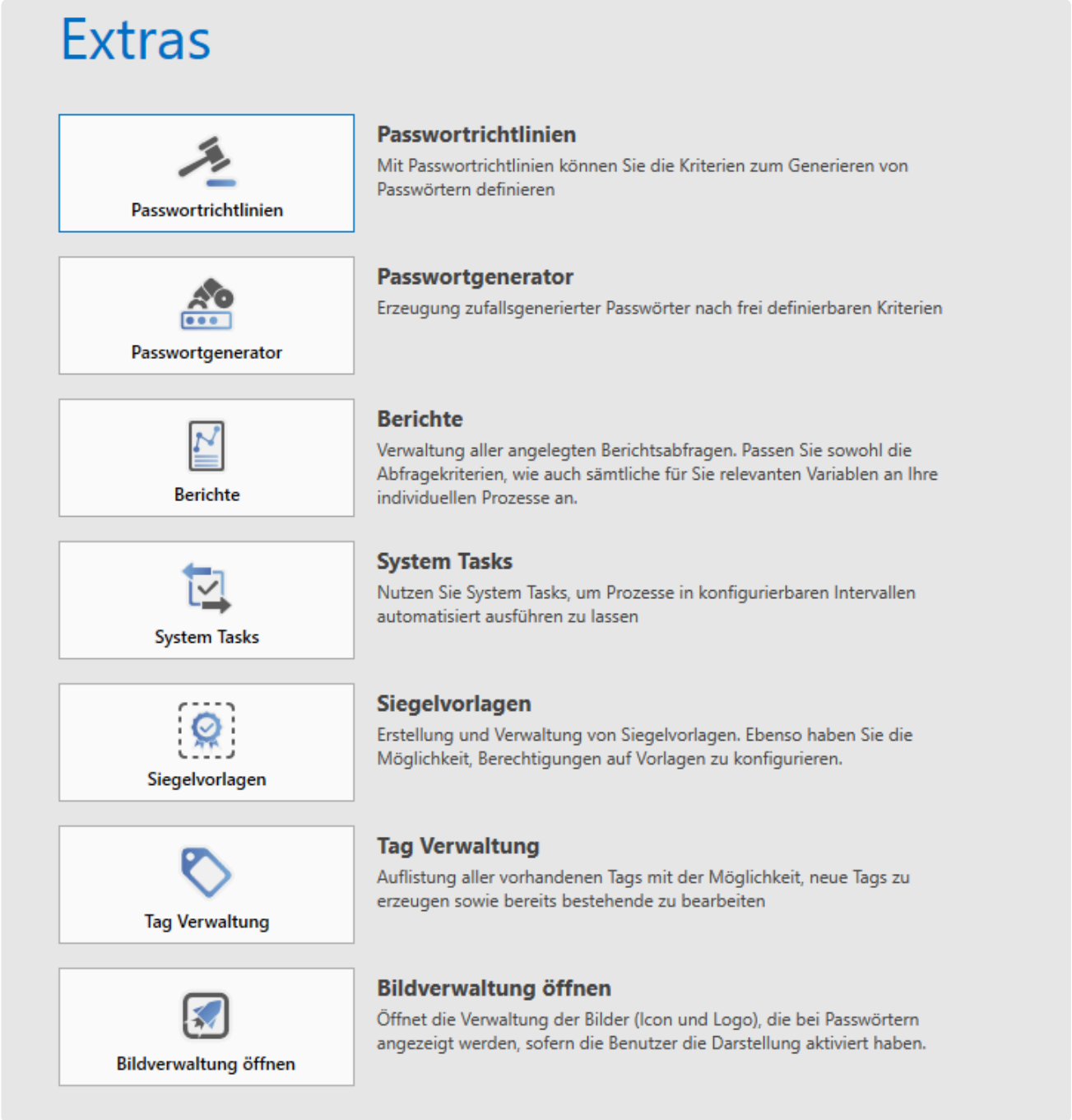
Nach Fertigstellung des Assistenten wird der gewünschte Export erzeugt und gespeichert.

> ! Beachten Sie bitte, dass diese Funktion sicherheitskritisch ist. Die **nötigen Berechtigungen** sollten daher nur denjenigen Benutzern gegeben werden, welche sie auch wirklich benötigen.

Extras

Was sind Extras?

Es geht um Funktionen, welche in der Summe das Arbeiten mit dem Password Safe erleichtern.

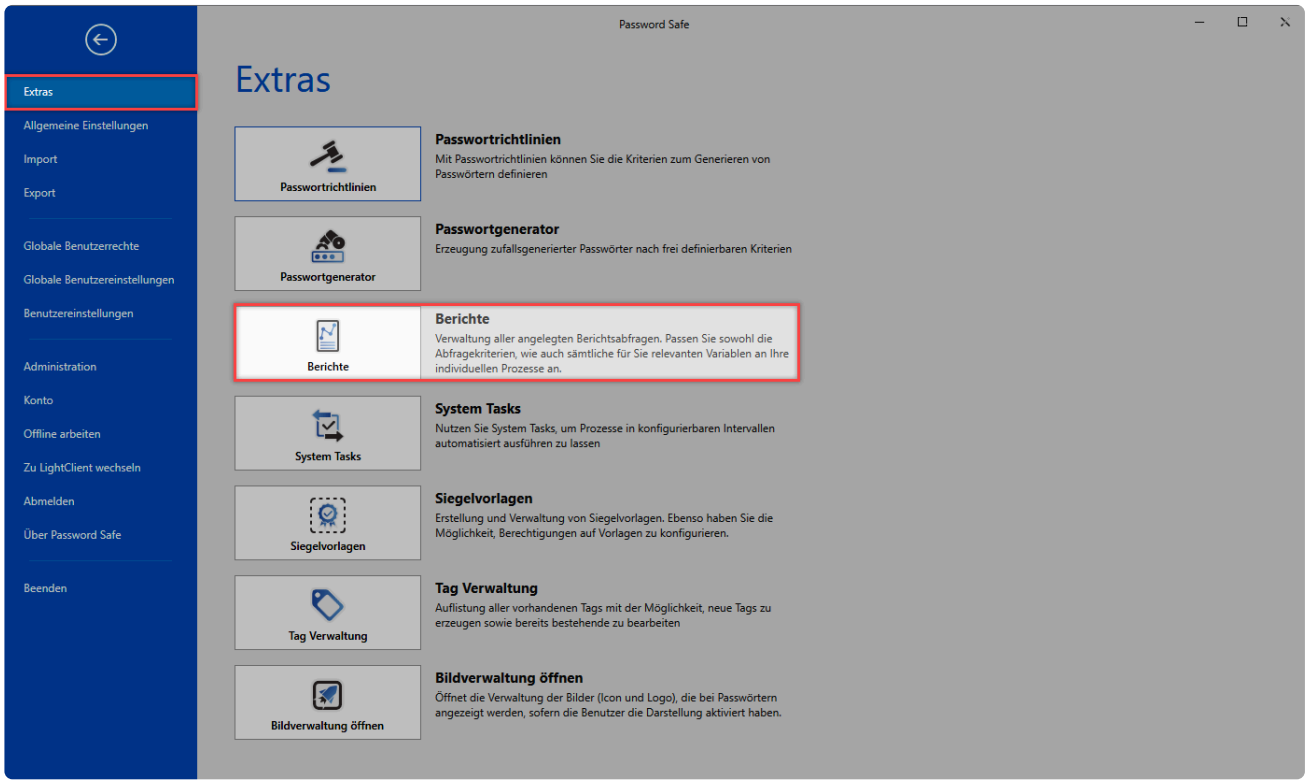


- Passwortrichtlinien
- Passwortgenerator
- Berichte
- System Tasks
- Siegelvorlagen
- Tagverwaltung
- Bildverwaltung

Berichte

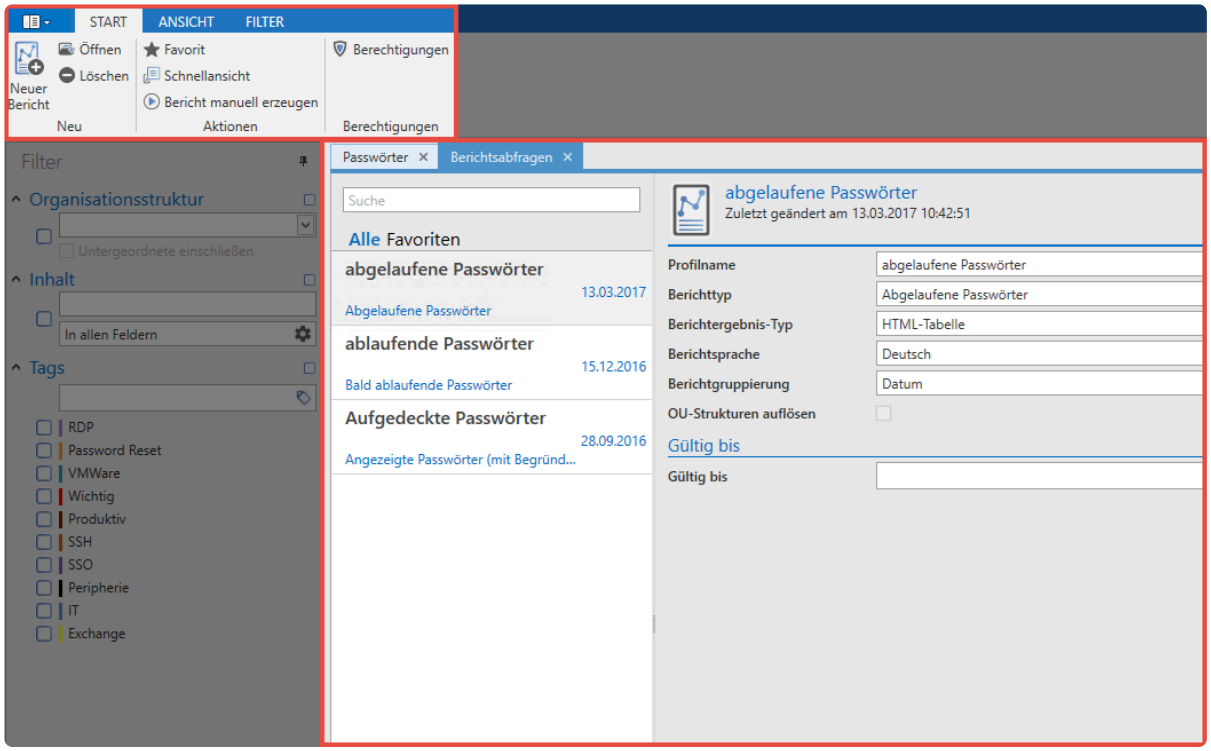
Was sind Berichte?

Berichte ermöglichen die tabellarische Auflistung frei definierbarer Aktionen zu einem selbst wählbaren Zeitpunkt. Der Auslöser ist das Erstellen eines Berichtes.
Dieser Vorgang können Sie weiterhin über **System Tasks** automatisieren.



Berichte enthalten stets nur diejenigen Informationen, auf die Sie auch berechtigt sind.

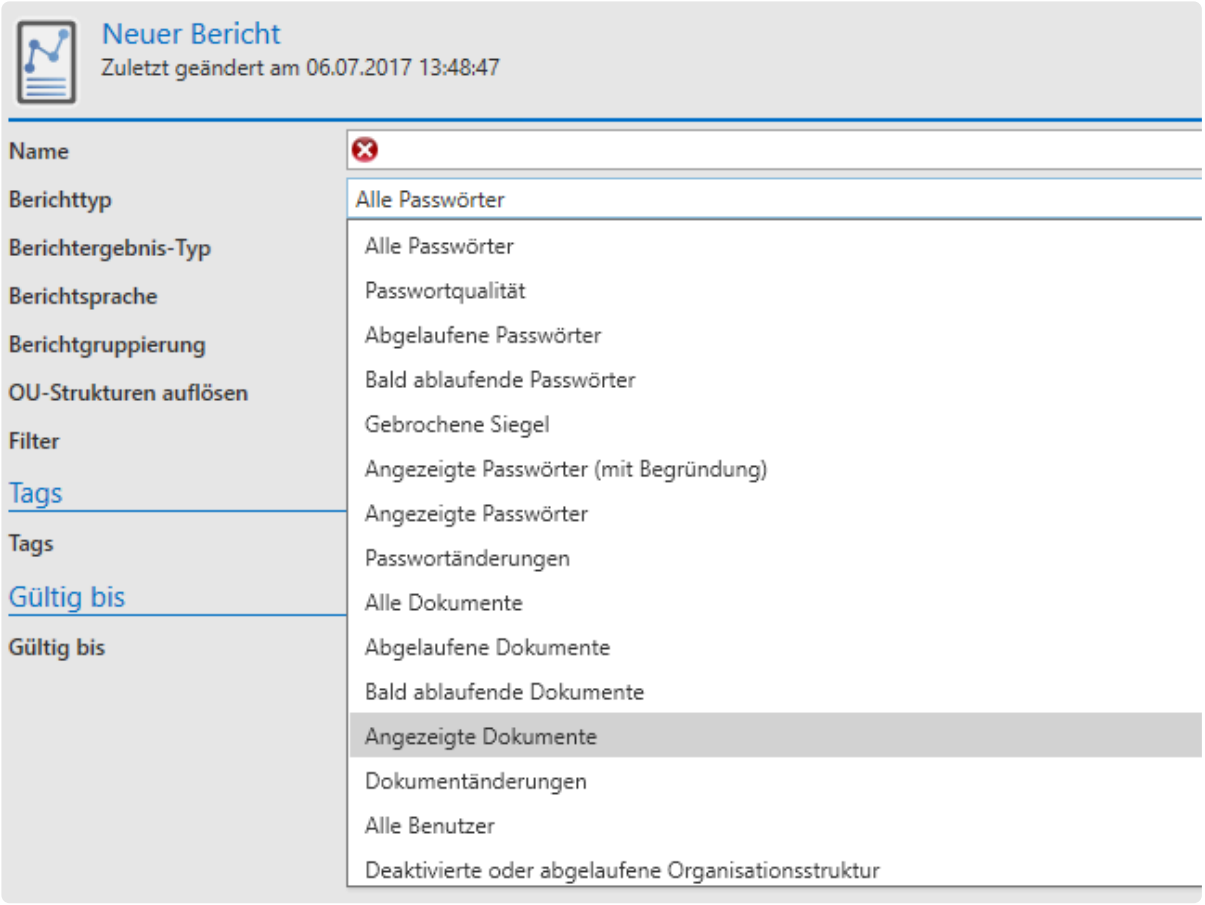
Über **Hauptmenü/Extras/Berichte** öffnen Sie im aktuellen Modul einen separaten Tab zum Verwalten der Berichte. Es ist irrelevant, in welchem Modul Sie die Berichte öffnen, der Inhalt ist stets der gleiche.



Der Filter besitzt im Zuge der Berichte keinerlei Relevanz. Obwohl Berichte “getagt” werden können, wirkt sich das Filtern nicht auf die Berichte aus.

Erstellen von Berichtsabfragen

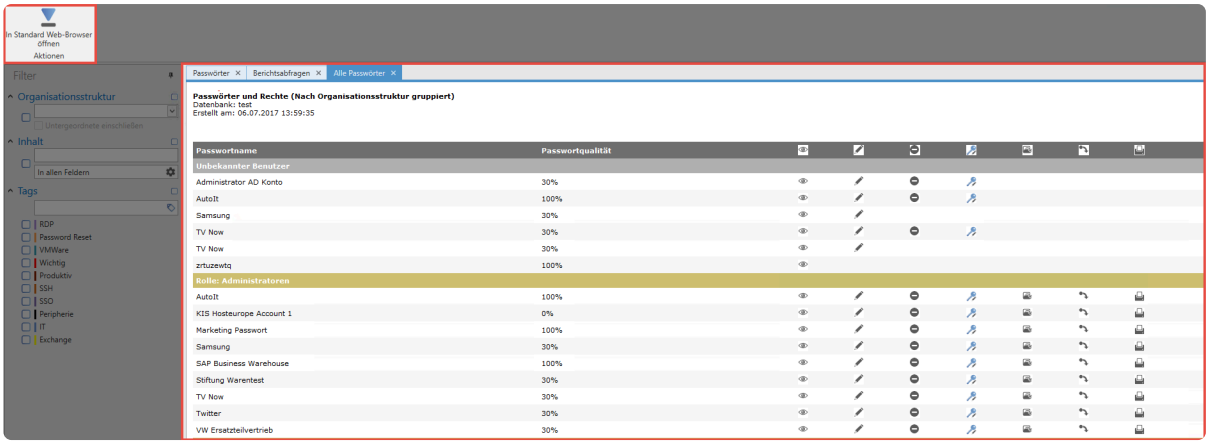
Über die Ribbon, wie auch über das Kontextmenü der rechten Maustaste, können Sie in der Listenansicht neue Berichtsabfragen erstellen. Es öffnet sich ein Formular zum Erstellen der Abfrage. Neben diversen Variablen legen Sie hier den Berichtstyp per Dropdown-Liste fest.



Per **Filter setzen** legen Sie den Wirkungsbereich des Berichts, beispielsweise auf eine bestimmte OU oder lediglich eine Auswahl an Tags, fest. Nach dem Speichern wird der Bericht nun in der Liste der Berichtsabfragen angezeigt.

Berichte manuell erzeugen

Über die Ribbon erzeugen Sie einen manueller Bericht. Dieser öffnet sich in einem separaten Tab und kann auf Wunsch im Web-Browser dargestellt werden.



Automatischer Versand über System Tasks

In der Regel erzeugen Sie Berichte nicht manuell, sondern sie werden automatisch an definierbare

Adressaten versandt. Dies wird im Zuge der **System Tasks** möglich, welche Vorgänge dieser Natur zeitgesteuert ablaufen lassen.

Relevante Berichte

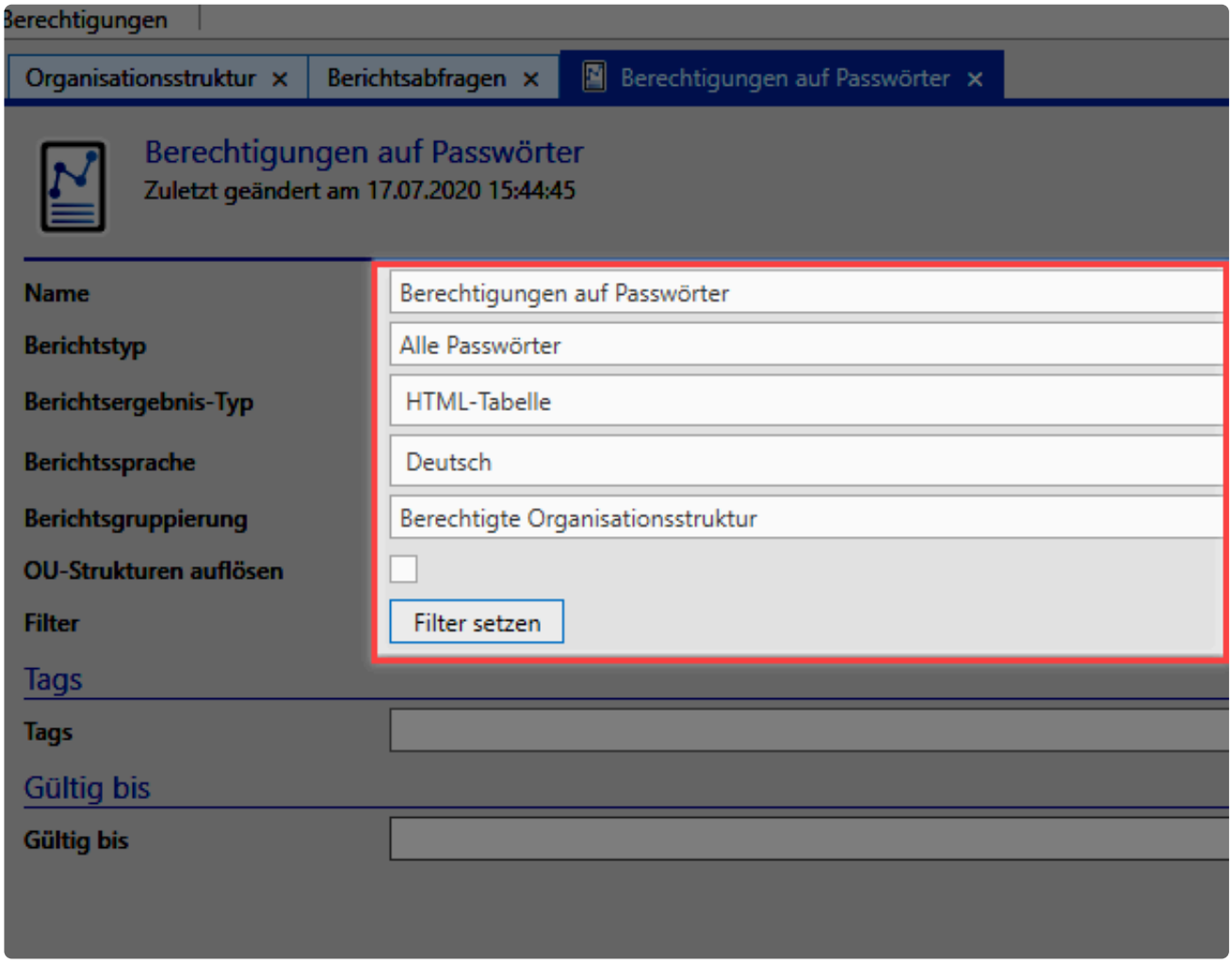
In diesem Kapitel finden Sie häufig verwendete Berichte und wie Sie diese konfigurieren.

Berechtigungen auf Passwörter

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

Bericht:

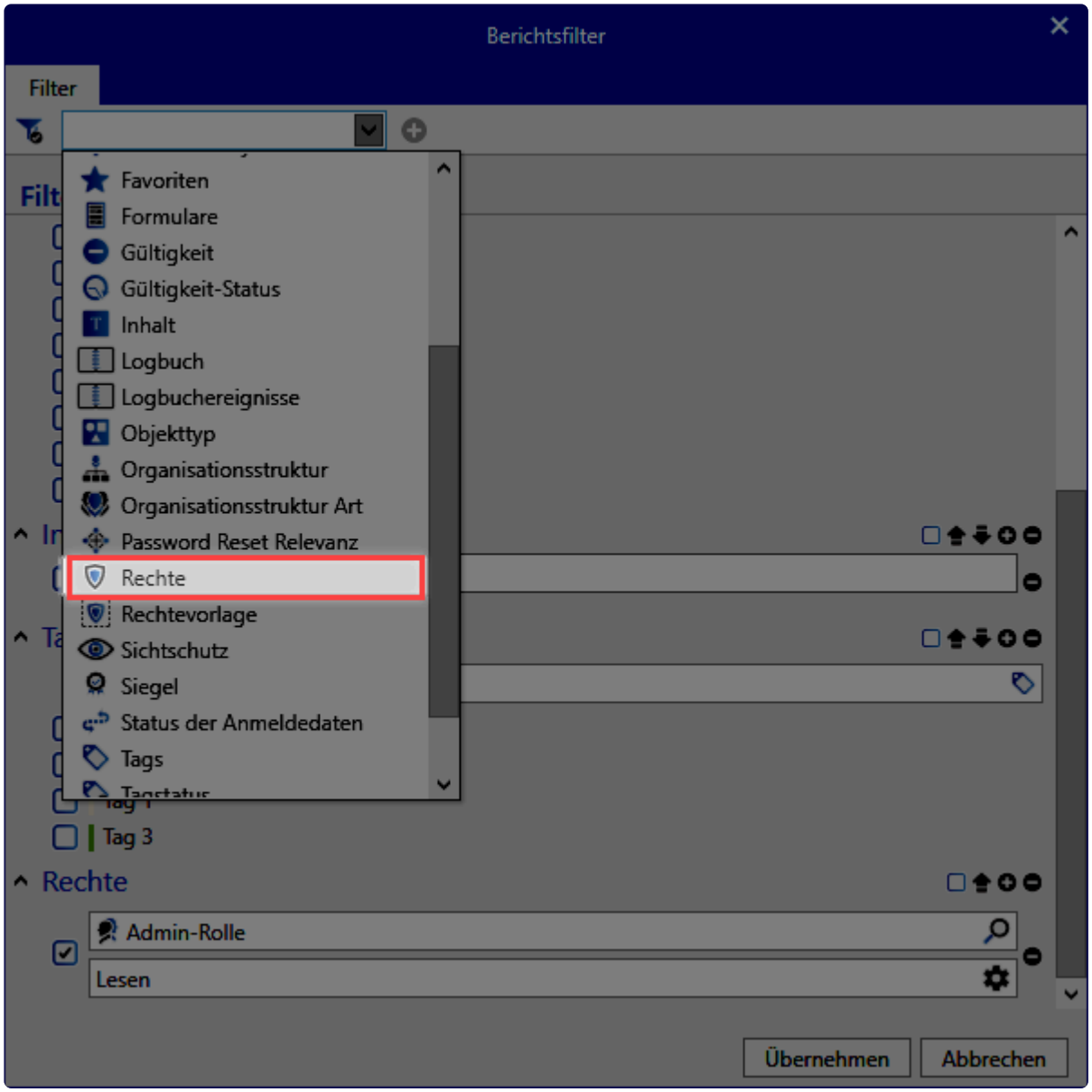
- **Berichtstyp**: Alle Passwörter
- **Berichtsergebnis-Typ**: HTML-Tabelle
- **Berichtsgruppierungen**: Berechtigte Organisationsstruktur



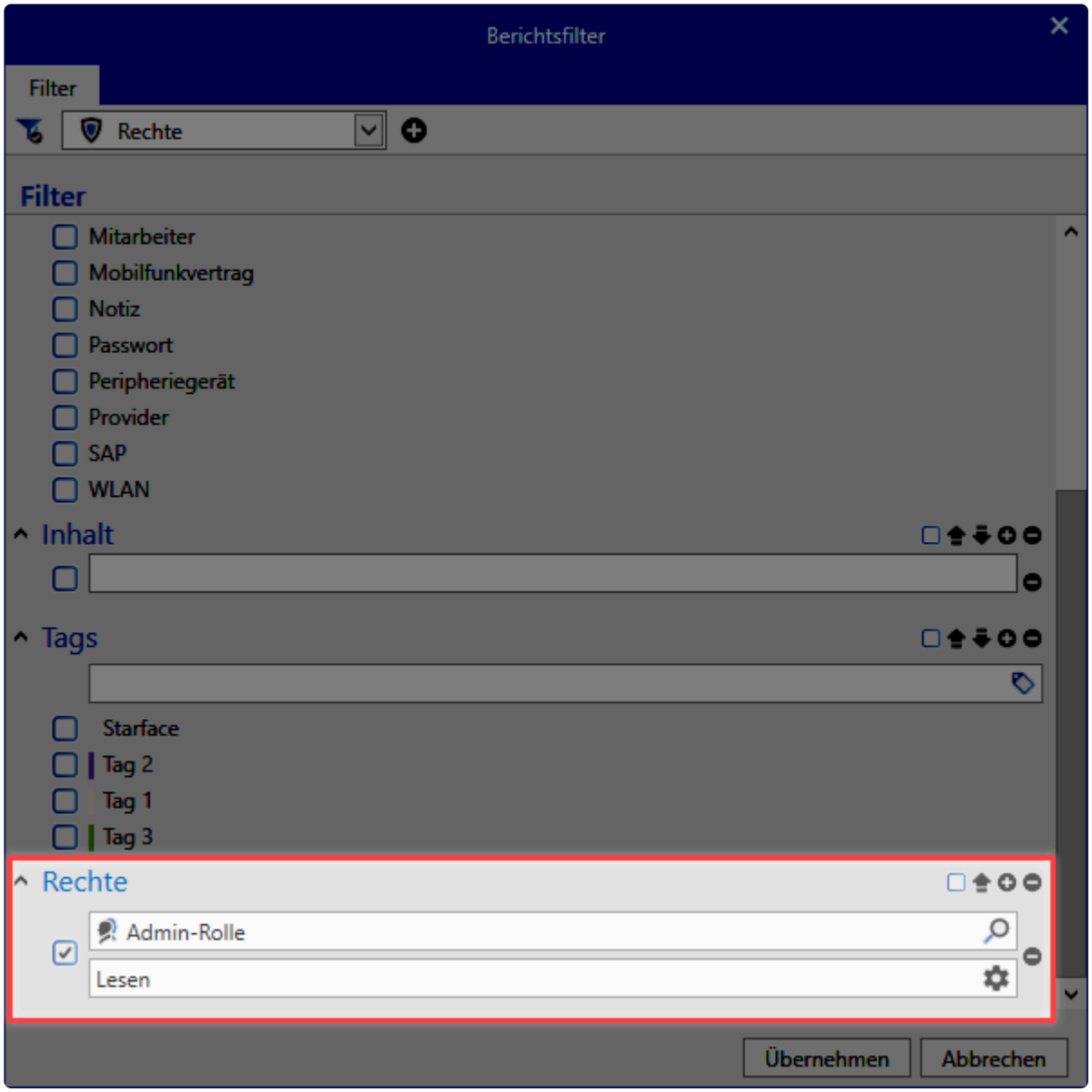
Filter

Beim Filter müssen Sie ein weiteres Filterattribut hinzufügen.

- Filter **Rechte** hinzufügen



- entsprechende Rolle oder Benutzer im neuen Filter auswählen



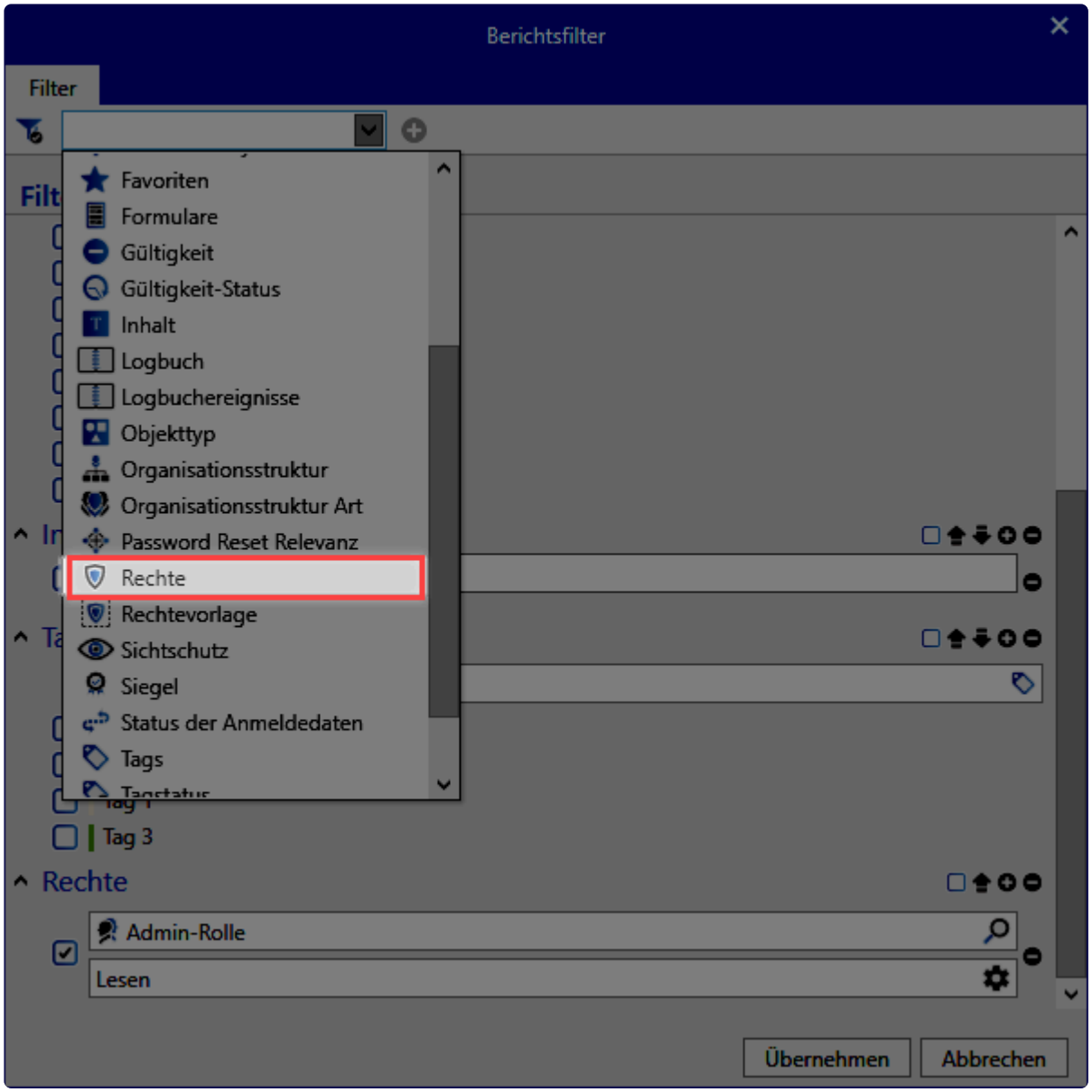
Nach dem definieren des Filter kann der Bericht erzeugt werden.

Zugriffe auf die Passwörter

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

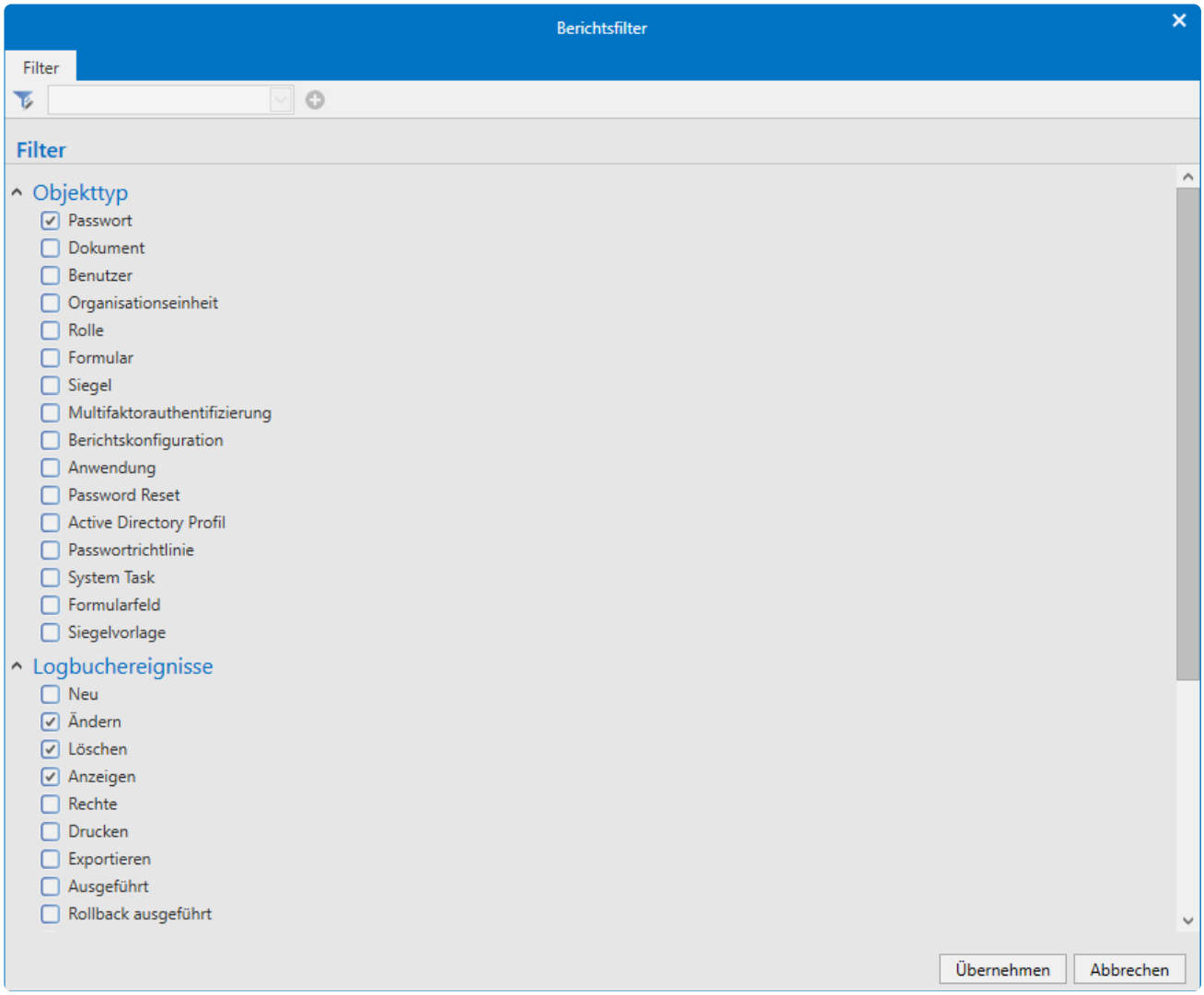
Bericht

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



Filter

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



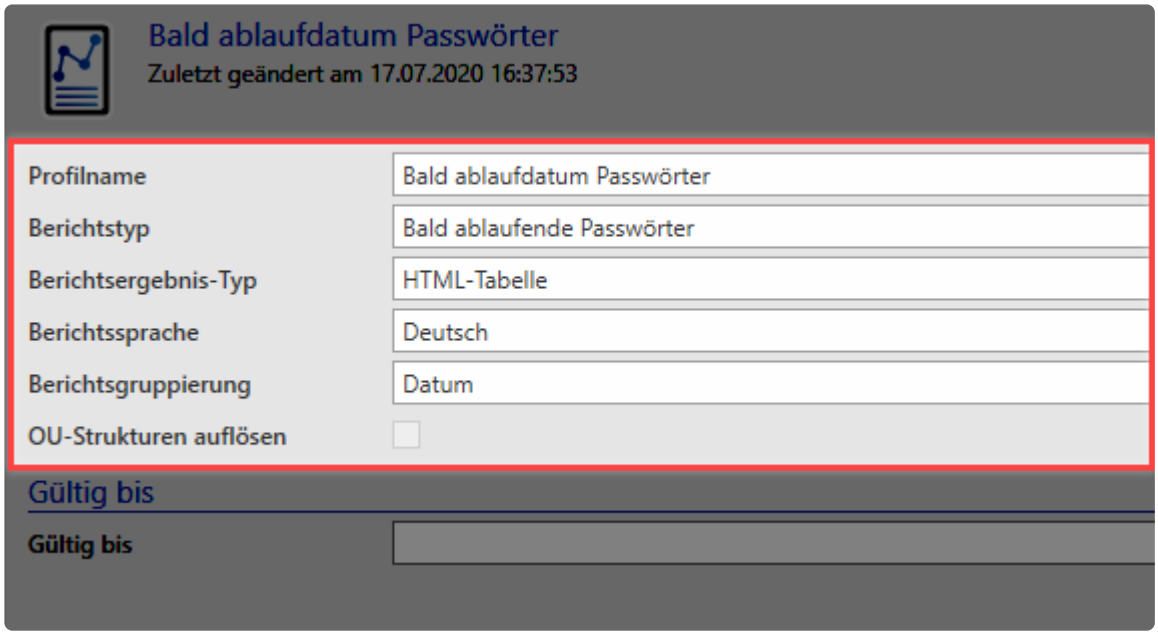
Nachdem der gewünschte Filter eingestellt ist, muss der Bericht nur noch erzeugt werden.

Bald ablaufende Passwörter

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

Bericht

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



Filter

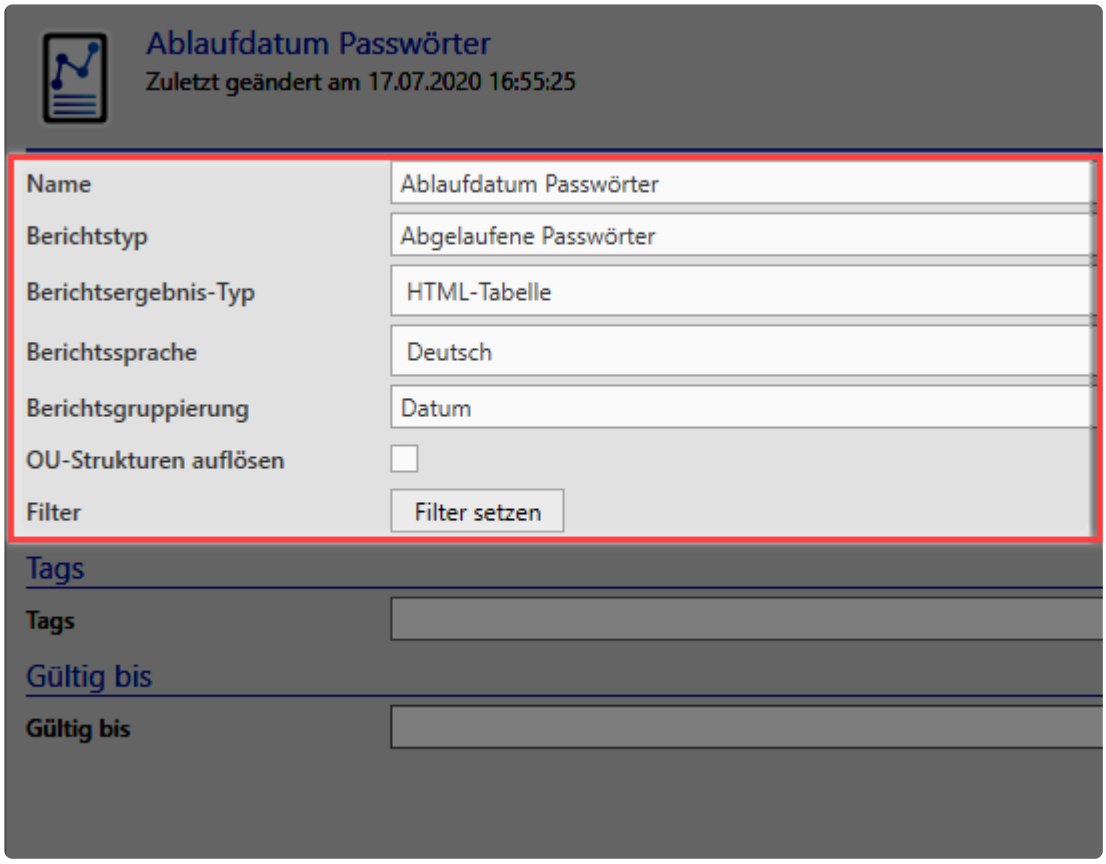
Ein Filter muss bei dieser Abfrage nicht definiert werden

Abgelaufene Passwörter

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

Bericht

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



Filter

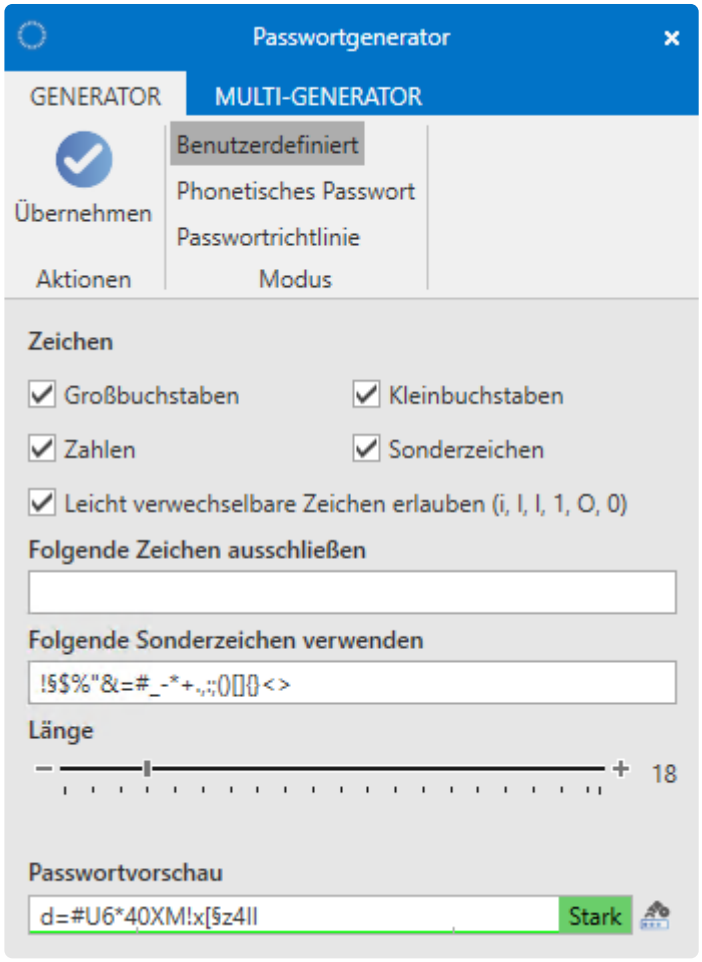
Ein Filter muss bei dieser Abfrage nicht definiert werden

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

Passwortgenerator

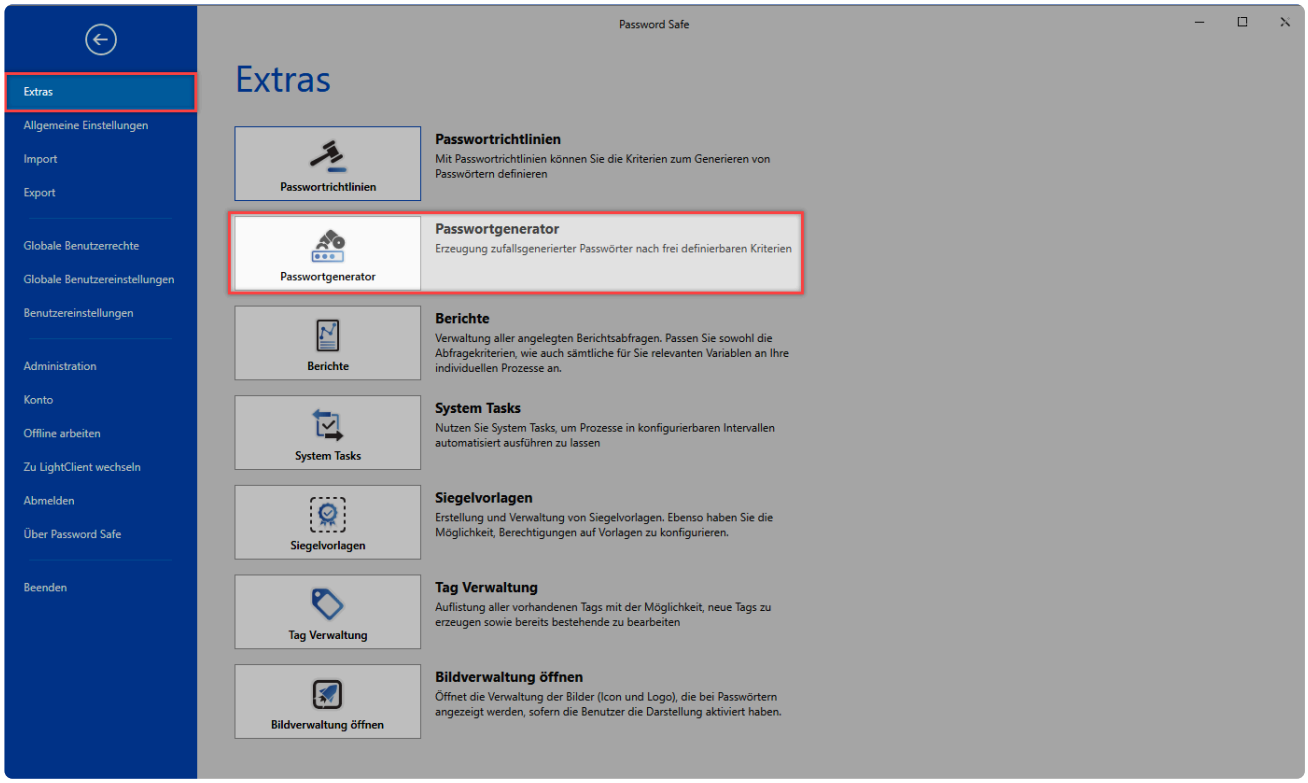
Was ist der Passwortgenerator?

Der Passwortgenerator ist ein in komplett die Software eingebundener Algorithmus zum Erstellen von Passwörtern. Die Komplexität von Passwörtern wird grundsätzlich durch die Zufälligkeit und Anzahl der verwendeten Zeichen bestimmt. Dies können Sie im Passwortgenerator einstellen und sich wirklich sichere Passwörter generieren lassen.



Öffnen des Passwortgenerators

- **Hauptmenü/Extras/Passwortgenerator**: Hierbei wird der Passwortgenerator direkt aufgerufen. Dort kreierte Passwörter können in die Zwischenablage kopiert werden.



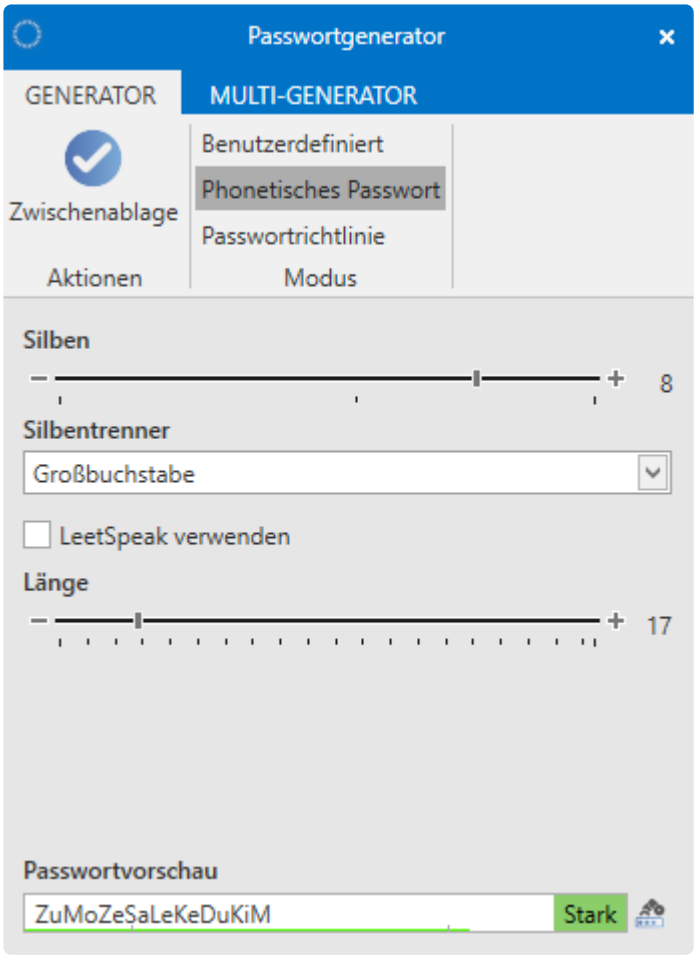
- **Beim Erstellen neuer Datensätze**: Am Ende vom Passwortfeld befindet sich eine kleine Schaltfläche. Hier kann der Generator geöffnet werden. Dann können die Kriterien definiert und das Passwort übernommen werden.

Funktionsweise

Unter **Zeichen** definiert man die Zeichengruppen. Analog können auf diese Art und Weise auch Zeichen ausgeschlossen werden. Nachdem die Passwortlänge bestimmt wurde, existiert am unteren Rand des Passwortgenerators eine Vorschau auf ein 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 – dem Ersetzen von Buchstaben durch ähnliche aussehende Ziffern oder Sonderzeichen – verwendet werden.



Passwortrichtlinie

Bereits definierte **Passwortrichtlinien** können für das automatische Erzeugen neuer Passwörter herangezogen werden

Multi-Generator

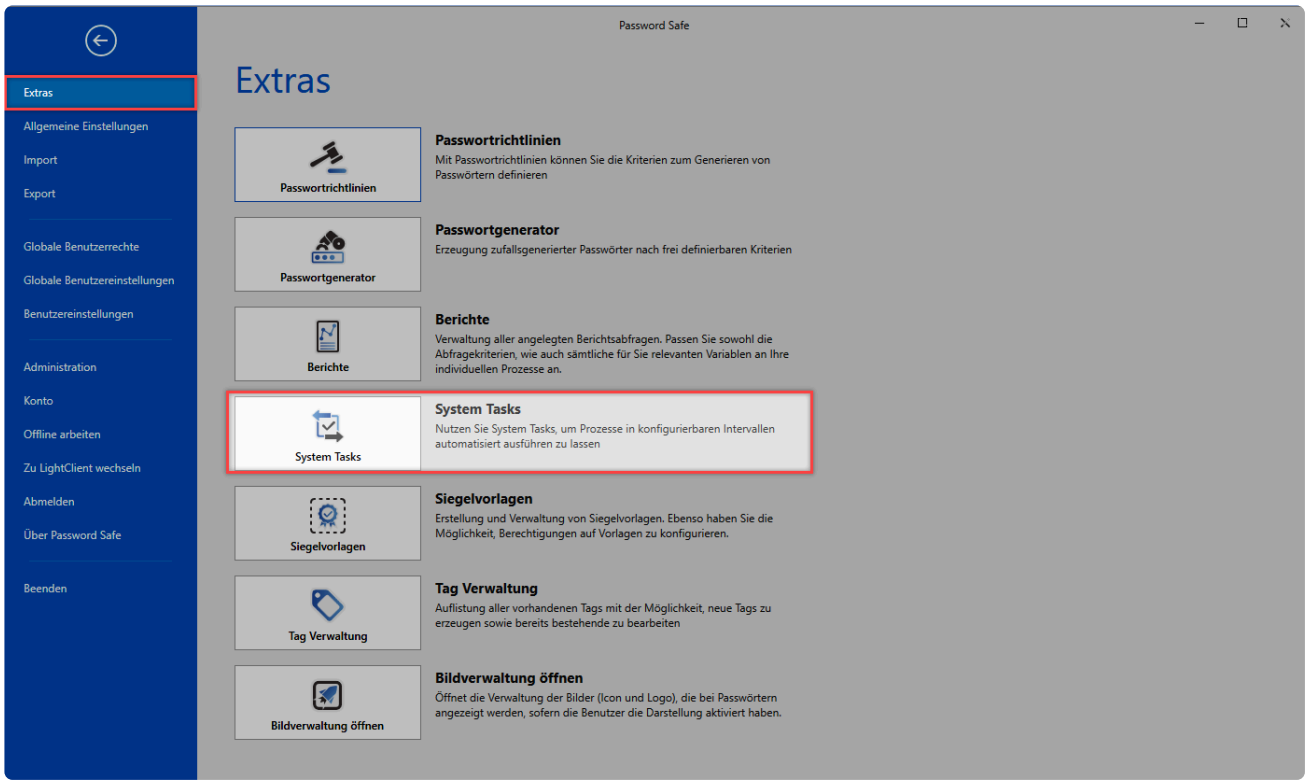
Der Multigenerator ermöglicht das automatische Erstellen von bis zu 200 Passwörtern. Die Konvention, nach der diese Passwörter erzeugt werden, entspricht stets den vorher definierten Vorgaben. Diese können sein

- Benutzerdefiniert
- Phonetische Passwörter
- Passwortrichtlinien

Die erzeugten Passwörter werden im lokalen Benutzerverzeichnis in einer Textdatei gespeichert.

System Tasks

System Tasks sind vordefinierte Aufgaben mit frei konfigurierbaren Intervallen, welche automatisch durchgeführt werden.



Relevante Rechte

Für die Verwaltung von System Tasks werden folgende Rechte benötigt.

Benutzerrecht

- Kann Active Directory System Tasks verwalten
- Kann Berichte System Tasks verwalten
- Kann Discovery Service System Tasks verwalten
- Kann Notfall-WebViewer-Export System Tasks verwalten
- Kann WebViewer Export System Tasks verwalten

Was kann automatisiert werden?

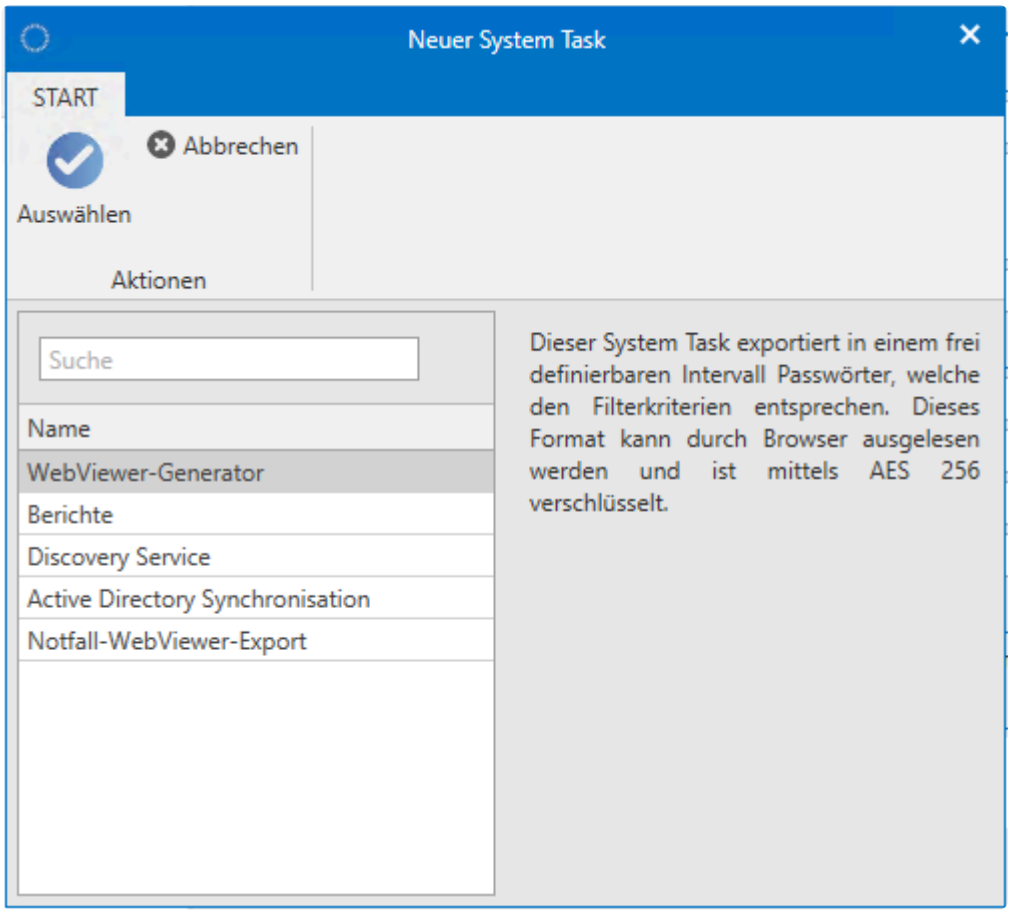
Aktuell gibt es fünf verschiedene Aufgaben, die durch System Tasks automatisiert werden können:

- **WebViewer-Generator**: Exportiert eine mittels AES 256 verschlüsselte HTML-Datei. Die Datei wird Ihnen über eine Benachrichtigungen zugestellt.
- **Berichte**: Erstellt automatisiert einen Bericht, welcher in den Benachrichtigungen ausgegeben wird. Erstellen Sie zuvor eine **Berichtsabfrage**.
- **Discovery Service**: Sucht in definierbaren Zyklen nach Dienstkonten im Netzwerk. Im Kapitel **Discovery Service** finden Sie weiterführende Informationen.

- **Active Directory Synchronisation**: Der Abgleich mit dem Active Directory kann über System Tasks automatisiert werden. Erstellen Sie vorab das **Active Directory Profil**. Bitte beachten Sie, dass nur **Masterkey Profile** automatisch abgeglichen werden können.
- **Notfall WebViewer**: Erstellt einen Notfall WebViewer zum Zugriff auf die Daten beim Ausfall der Systeme.

Erstellen von System Tasks

System Tasks können Sie entweder über die Ribbon oder über das Kontextmenü der rechten Maustaste anlegen..



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 Sie den System Task hier deaktiviert haben, 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 Sie diesen schon erstellt haben und nun bearbeiten).
- **Intervall**: Definieren Sie, 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.

WebViewer-Generator

- **Filter**: Per **Filter** definieren Sie, welche Passwörter exportiert werden sollen.
- **Passwort**: Der HTML-WebViewer erstellt eine verschlüsselte HTML Datei. Definieren und Bestätigen Sie das Passwort.

Berichte

- **Berichtsabfrage**: Die unter **Berichte** definierten Berichtsabfragen stehen Ihnen zur Auswahl.

Discovery Service

- Der **Discovery Service** durchsucht das Netzwerk und listet alle Dienste auf, bei welchen ein Service User hinterlegt ist. Diese können Sie dann mittels Password Safe pflegen. Hierzu übergeben Sie die gesammelten Information direkt an den **Password Reset**.

Active Directory Synchronisierung

- Wählen Sie das zu synchronisierende **Active Directory Profil** aus den vorhandenen aus.
- Sollten **Light-User-Lizenzen** vorhanden sein, ist es möglich bei der Acive Directory Synchronisation zu definieren, ob die Benutzer als **Full** oder **Light** Benutzer importiert werden sollen.

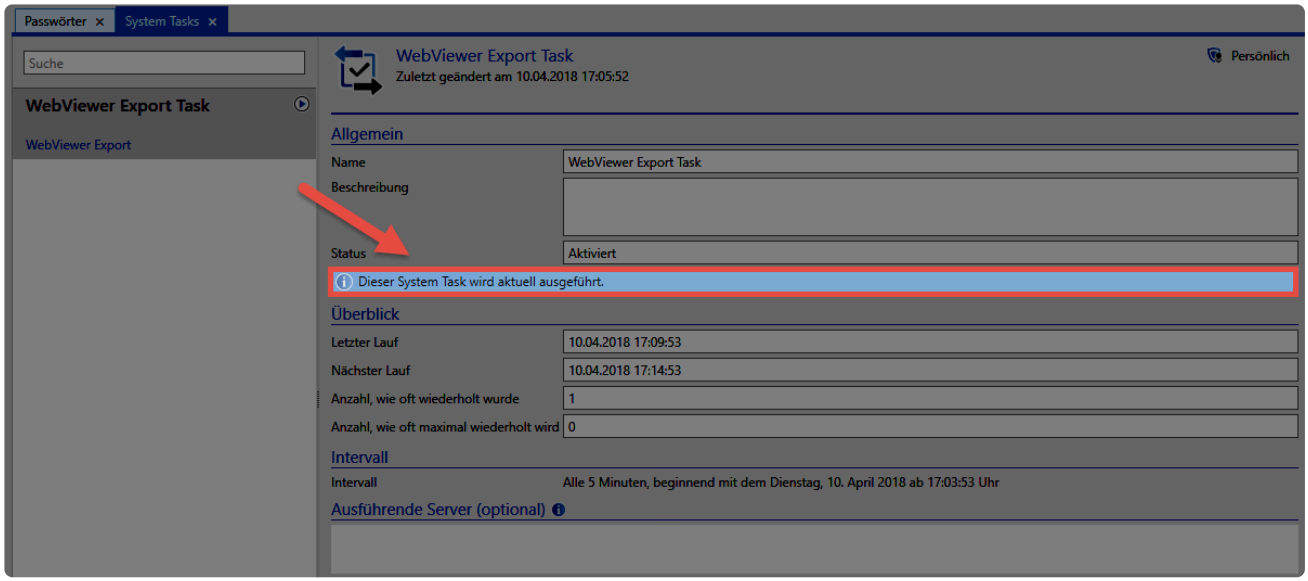
Notfall-WebViewer-Export

- Der Notfall-WebViewer-Export erstellt eine verschlüsselte HTML-Datei, welche alle Passwörter beinhaltet. Im Notfall kann über diese Datei auf die Daten zugegriffen werden um die Systeme wieder zum Laufen zu bringen.

> 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.

Status

Wenn ein Task aktuell läuft, wird dies über einen entsprechenden Hinweis dargestellt.


Passwörter
System Tasks
Suche
WebViewer Export Task
WebViewer Export
WebViewer Export Task
Zuletzt geändert am 10.04.2018 17:05:52
Persönlich
Allgemein
Name
WebViewer Export Task
Beschreibung
Status
Aktiviert
Dieser System Task wird aktuell ausgeführt.
Überblick
Letzter Lauf
10.04.2018 17:09:53
Nächster Lauf
10.04.2018 17:14:53
Anzahl, wie oft wiederholt wurde
1
Anzahl, wie oft maximal wiederholt wird
0
Intervall
Intervall
Alle 5 Minuten, beginnend mit dem Dienstag, 10. April 2018 ab 17:03:53 Uhr
Ausführende Server (optional)

Notfall WebViewer

Was versteht man unter Notfall-WebViewer-Export?

Der Schutz der Daten ist essential und sollte über Backups erfolgen. In manchen Fällen ist ein Backup jedoch nicht ausreichend, beispielsweise, wenn Sie aufgrund von Hardwareproblemen ein Backup nicht direkt zurückgespielen können. **Password Safe** bietet für derartige Fälle das Sicherheitsfeature **Notfall-WebViewer-Export** an.

Der **Notfall-WebViewer-Export** setzt auf eine verschlüsselte **HTML-Datei**, welche mit einem entsprechenden **Key** entschlüsselt werden kann. Beide Dateien sind für die Ansicht der Passwörter im Browser notwendig und bilden das Kernsystem des Sicherheitsmechanismus.

Voraussetzungen

Der Notfall WebViewer ist in der **Enterprise** und **Enterprise Plus** Edition enthalten.

Erstellung von Datei und Key

Legen Sie den **Notfall-WebViewer-Export** im Password Safe als **System Task** an. Durch die Einrichtung eines **Intervalls** wird eine **regelmäßige Sicherung** der Datensätze (Passwörter) gewährleistet. Bei der Konfiguration des System Task legen Sie fest, in welchem Zyklus die **Desaster WebViewer.html-Datei** auf dem AdminClient erzeugt werden soll. Dabei wird im **eingestellten Intervall** die jeweils vorhandene Datei mit der aktuell erstellten überschrieben. Der zugehörige **Key** wird bei der Erstellung einmalig erzeugt und muss gespeichert werden. Nur dieser **Key** entschlüsselt die jeweils aktuell vorhandene **HTML-Datei**.

> ! Der Key (PrivateKey.prvkey) und die Datei (Desaster WebViewer.html) müssen Sie auf einem sicheren Medium (USB-Stick, HDD, CD/DVD, …) und an einem sicheren Ort aufbewahren!

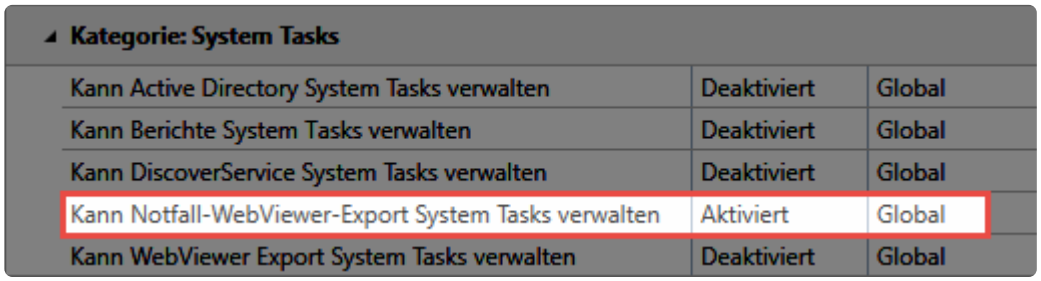
Datensicherheit

- Selbstverständlich ist die HTML WebViewer Datei verschlüsselt.
- Der Export der Datei wird über ein entsprechendes Benutzerrecht geschützt.
- Die Datei kann nur mittels der **PrivateKey.prvkey** Datei entschlüsselt werden.

> ! Das **Export-Recht** auf die Passwörter wird beim **Notfall-WebViewer-Export nicht benötigt!**

Benötigte Rechte

Sie benötigen für das Erstellen eines **Notfall-WebViewer-Export System Tasks** folgendes Recht:



! Beachten Sie, dass nur Passwörter exportiert werden, auf die der Benutzer, der den Export einrichtet, mit mindestens **Lesen** berechtigt ist.

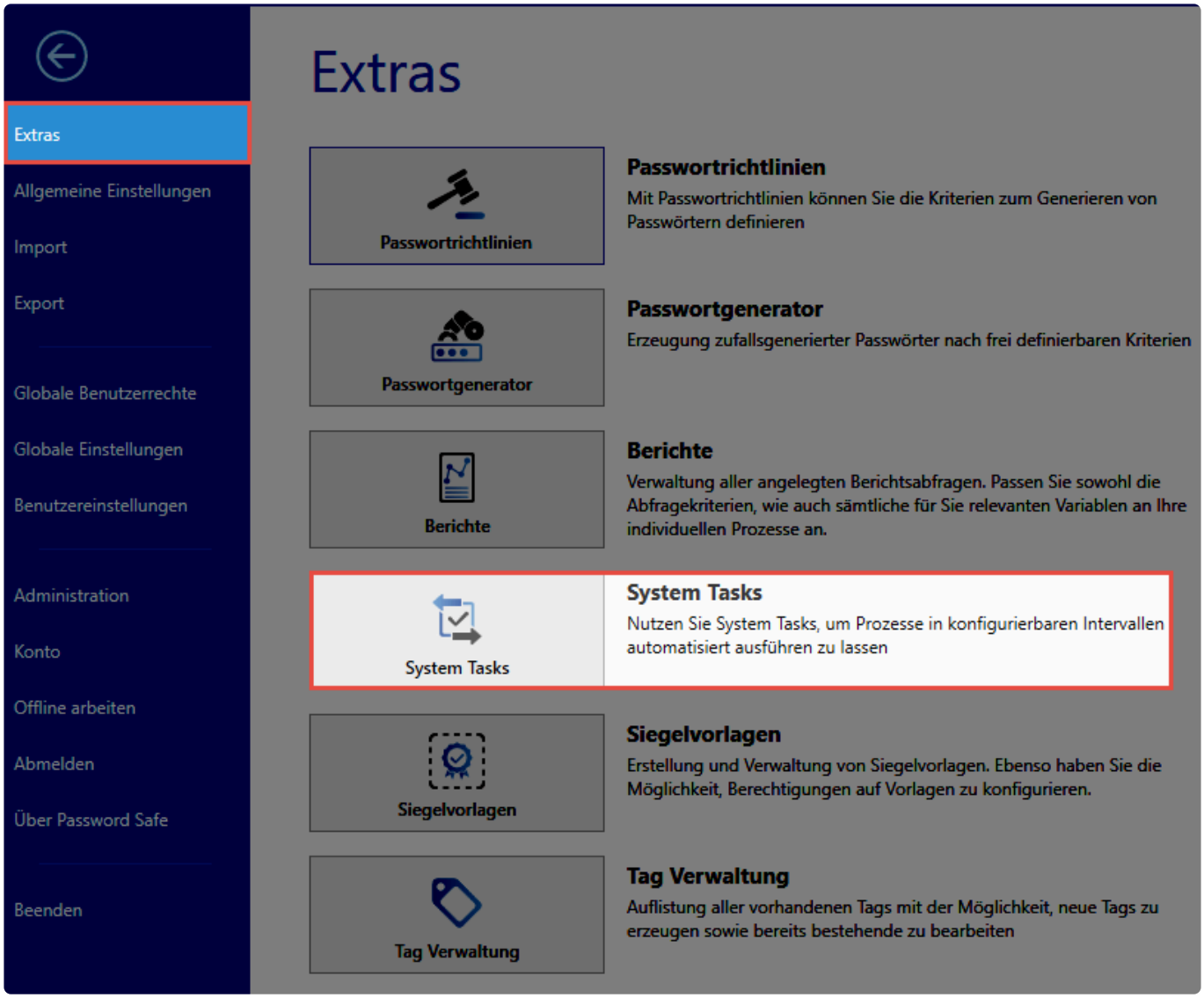
Desaster WebViewer.html und PrivateKey.prvkey

Der **Notfall-WebViewer-Export** erstellt zwei zusammengehörende Dateien.

1. Auf dem ausführenden Server wird die Datei **Desaster WebViewer.html** erzeugt.
2. Auf dem Client wird der zugehörige Key **PrivateKey.prvkey** erzeugt.

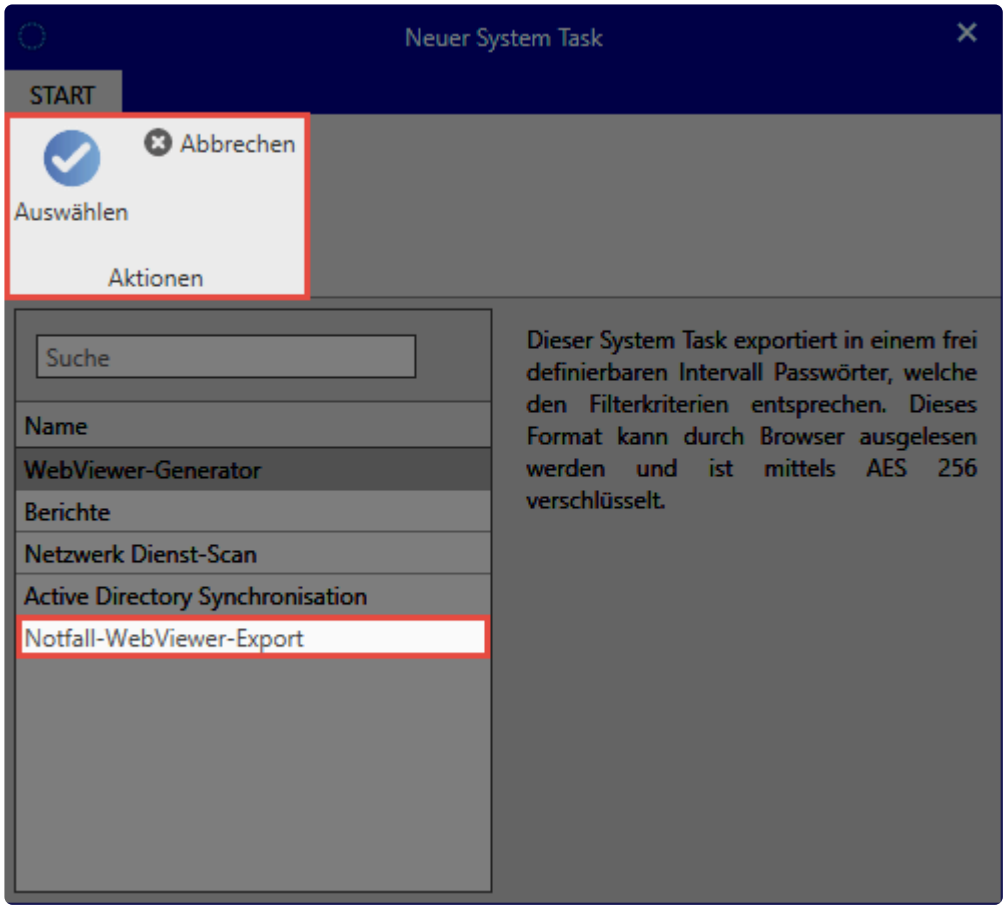
Aufruf des Notfall-WebViewer-Export

Der Notfall-WebViewer-Export wird als **System Task** eingerichtet. Rufen Sie diesen im Hauptmenü unter **Extras** -> **System Tasks** auf.

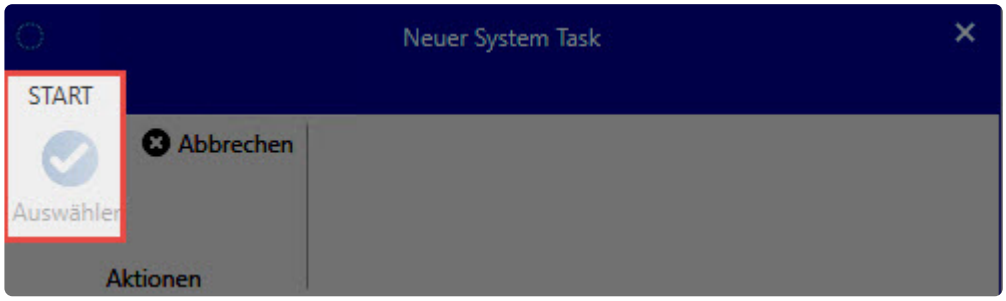


Erstellen einer Notfall-WebViewer-Export-Datei

Ein Klick auf **Neu** öffnet ein neues Fenster. Wählen Sie den **Notfall-WebViewer-Export** aus. Anschließend wird die **Konfigurationsseite** angezeigt.

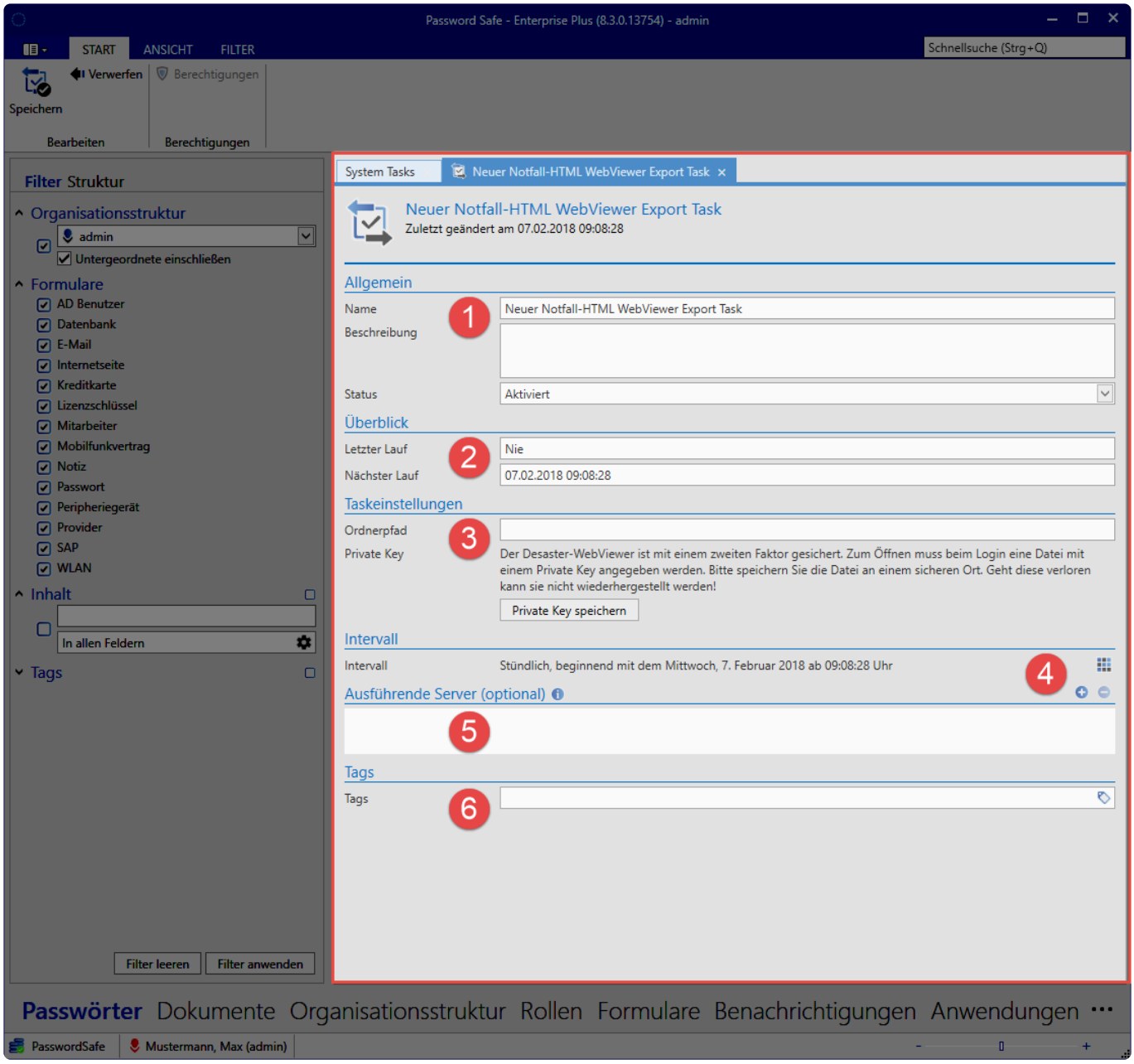


Die Verwendung des **Notfall-WebViewer-Export** mit einen **Active Directory Benutzer** ist nicht möglich.



Konfigurationsseite des Notfall-WebViewer-Export Tasks

Es wird ein neuer Tab angezeigt: **Neuer Notfall-HTML WebViewer Export Task.** Diesen konfigurieren Sie nun entsprechend den Anforderungen.

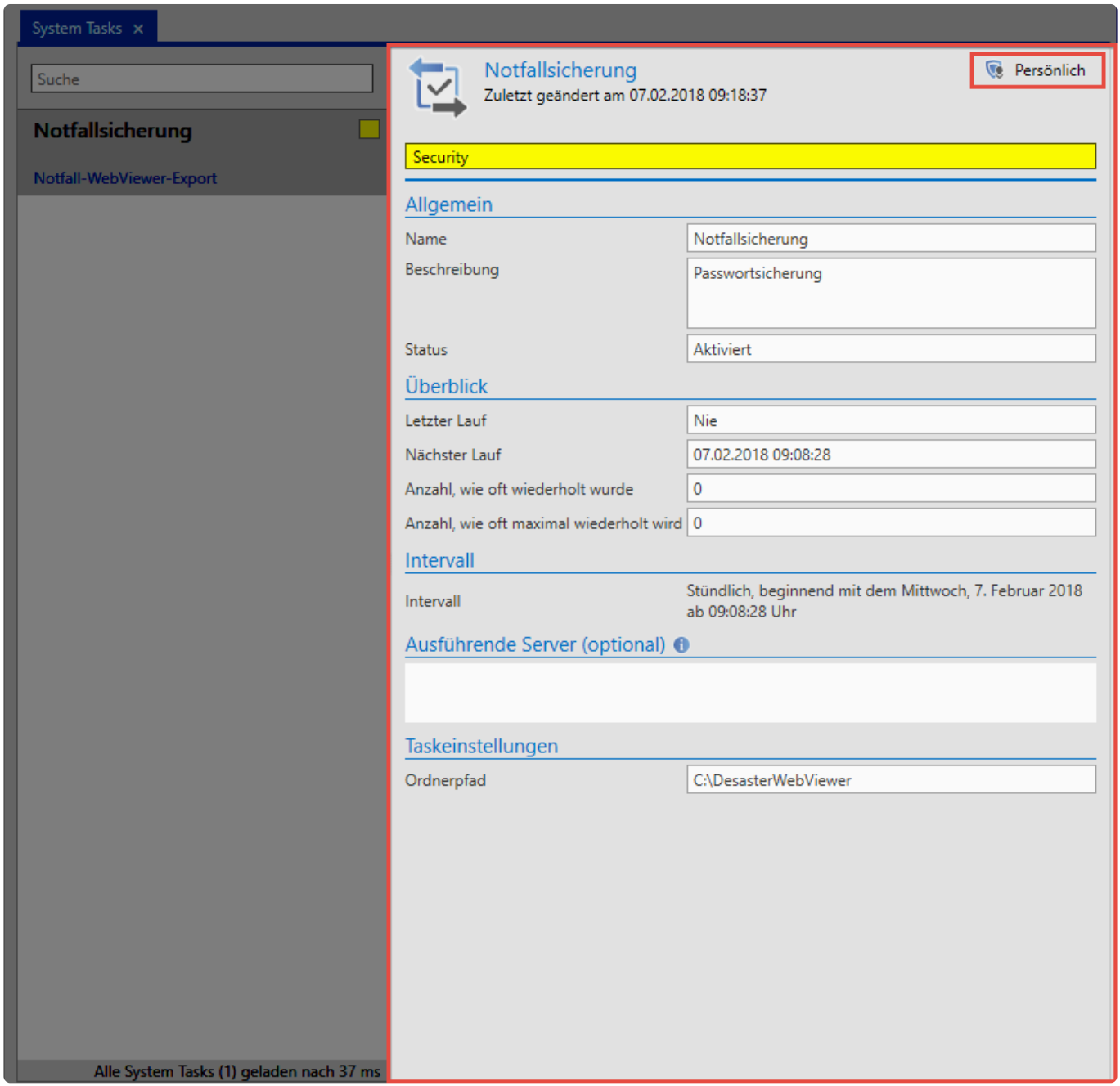


1. **Allgemein**
   Name: Eindeutig zu vergebender Name
   Beschreibung: Eingabe zusätzlicher Informationen
   Status: Ausführung: *Aktiviert*/Deaktiviert
2. **Überblick**
   Letzter Lauf: Informationsanzeige
   Nächster Lauf: Informationsanzeige
3. **Taskeinstellung**
   Ordnerpfad: Eintrag aus Sicht des Servers
   Private Key: muss gespeichert werden
4. **Intervall**
   Ausführungseinstellung des System Tasks
5. **Ausführende Server(optional)**
   Adresse (IP) der zusätzlichen Server
6. **Tags**
   Frei definierbare Merkmale von Datensätzen

> ! Der **Private Key** für Desaster-WebViewer muss **gespeichert** werden, bevor der System Task gespeichert werden kann!

Anzeige der Notfall-WebViewer-Export Tasks

Nach Beendigung der Konfiguration wird der **System Task** im aktuellen Modul im Reiter **System Tasks** angezeigt. Sie haben hier die Möglichkeit, die Daten zu überprüfen.



Bedienung der Desaster WebViewer.html Datei

Nach erfolgreicher Ausführung des **System Tasks** sind für die Passwortsicherheit **zwei Dateien** erstellt worden.

1. **Desaster WebViewer.html**
2. **PrivateKey.prvkey**

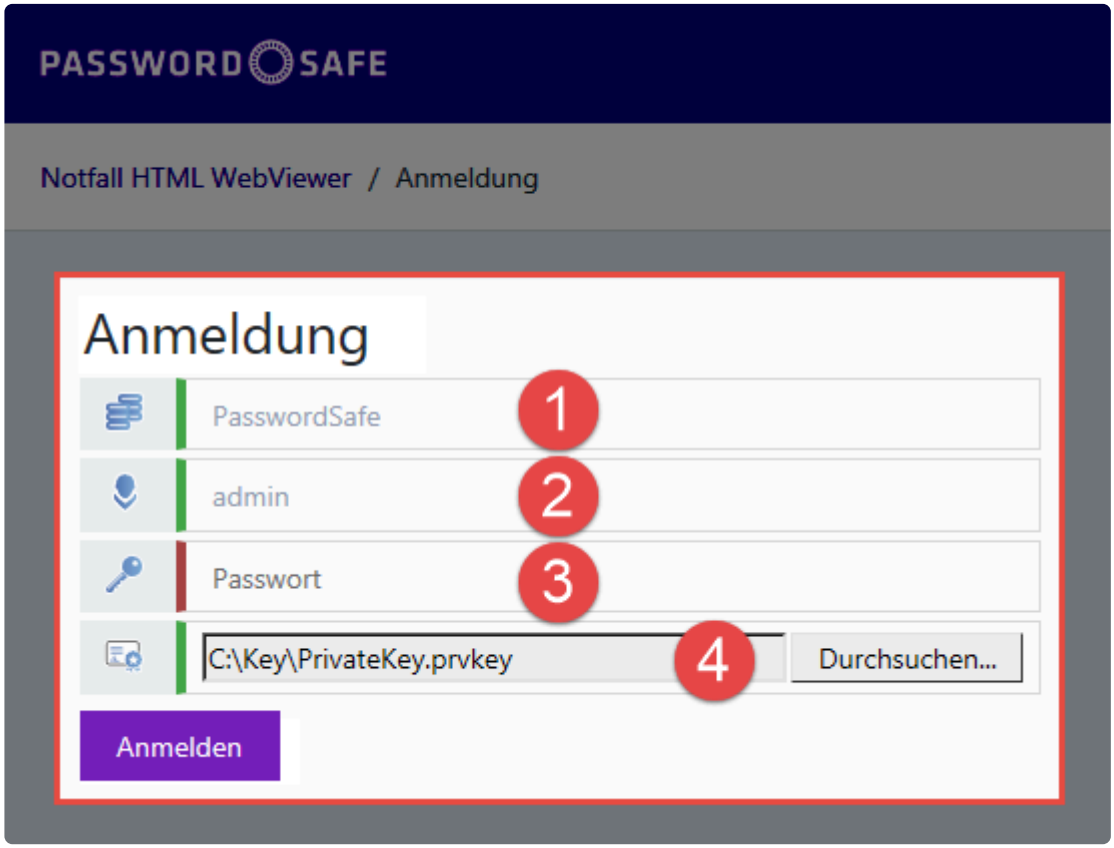
> ! Die Datei **Desaster WebViewer.html** ist auf dem ausführenden **Server gespeichert.** Der Key **PrivateKey.prvkey** muss vom **Benutzer** sicher **gespeichert werden!**

Die Anwendung des **Notfall-WebViewer-Export** erfolgt analog zum **WebViewer-Export.** Die **Passwörter** werden in einem aktuellen Browser angezeigt. Der Zugang erfolgt im **Notfall-WebViewer-Export** über das **Benutzerpasswort** und den gespeicherten **Key** des Benutzers. Mit Durchsuchen wird der **Key (PrivateKey.prvkey)** ausgewählt und zusätzlich auf **Gültigkeit** überprüft. Sind alle Daten korrekt eingetragen, ist eine Anmeldung möglich.

> ✻ Der eingetragene Benutzer muss sich mit seinem Passwort anmelden. Wird ein falsches Passwort eingegeben, wird der Zugang temporär gesperrt.

Anmeldedaten

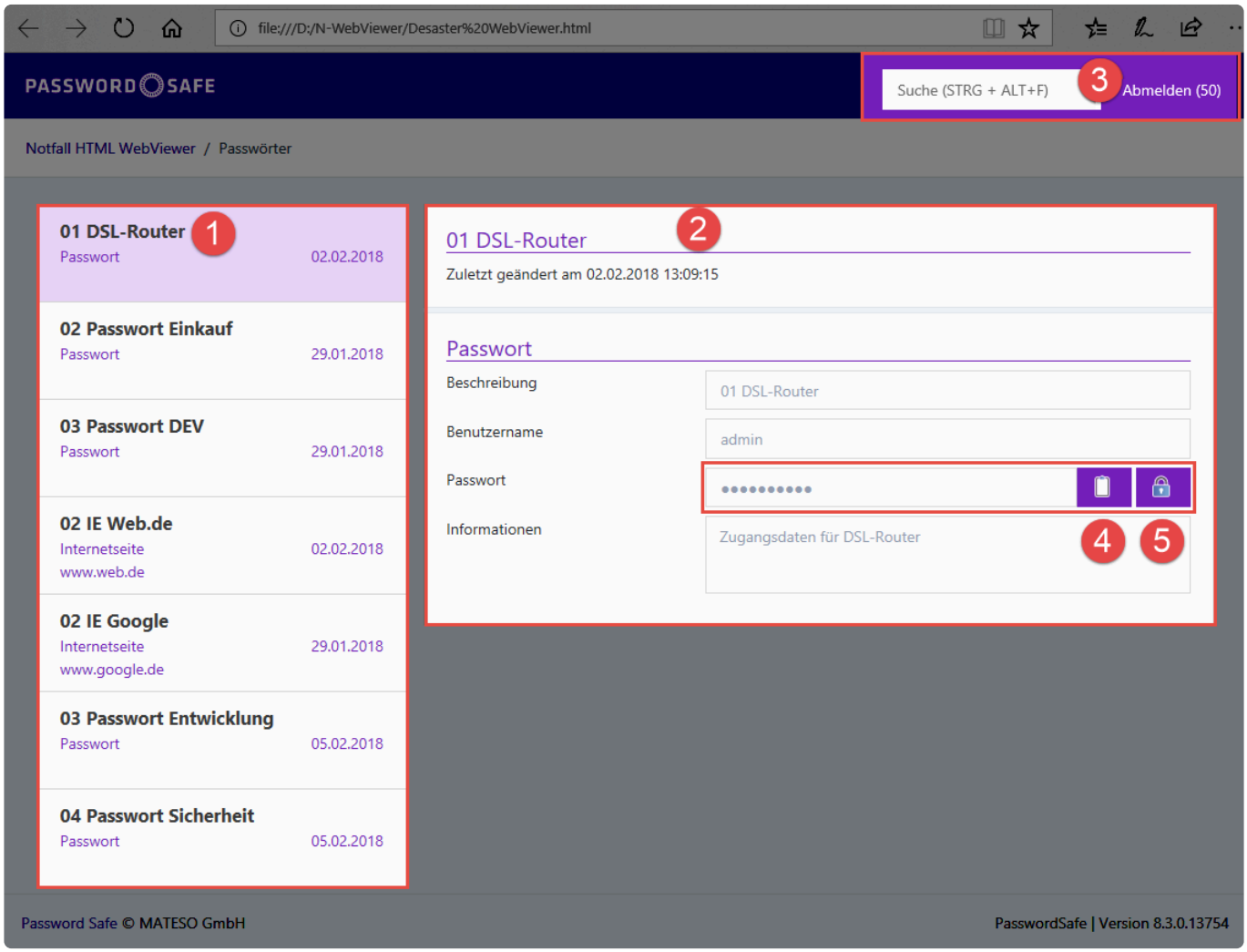
1. Datenbank: Vorgegeben
2. Benutzer: Vorgegeben
3. Passwort: **Benutzerpasswort (muss vom Benutzer eingegeben werden)**
4. Key: **PrivateKey.prvkey**



Übersicht

Nach erfolgreicher Anmeldung wird die **Übersichtsseite** des **Notfall-WebViewer-Export** angezeigt. Hier werden Ihnen die Informationen über die gespeicherten **Passwörter** analog zum WebViewer-Export dargestellt. Sie stehen nun dem Benutzer zur Verfügung.

Übersicht: Notfall HTML WebViewer / Passwörter



In der Übersicht werden folgende Daten angezeigt:

Übersichtsdaten:

1. Anzeige der aktuell vorhandenen Datensätze
2. Detailinformation des ausgewählten Datensatzes
3. Suche, Abmelden, Timeout bis zur Abmeldung
4. Passwort in die Zwischenablage kopieren
5. Passwort aufdecken

Sicherheitshinweis

Dem Benutzer stehen die vorhandenen **Passwörter** zur weiteren Verarbeitung zur Verfügung. Das

Schließen der HTML-Seite erfolgt über **Abmelden.**
Bei einer **Inaktivität** des Benutzers von **60 Sekunden** wird dieser automatisch **abgemeldet** und es wird die **Anmeldung** angezeigt mit zusätzlicher Information.

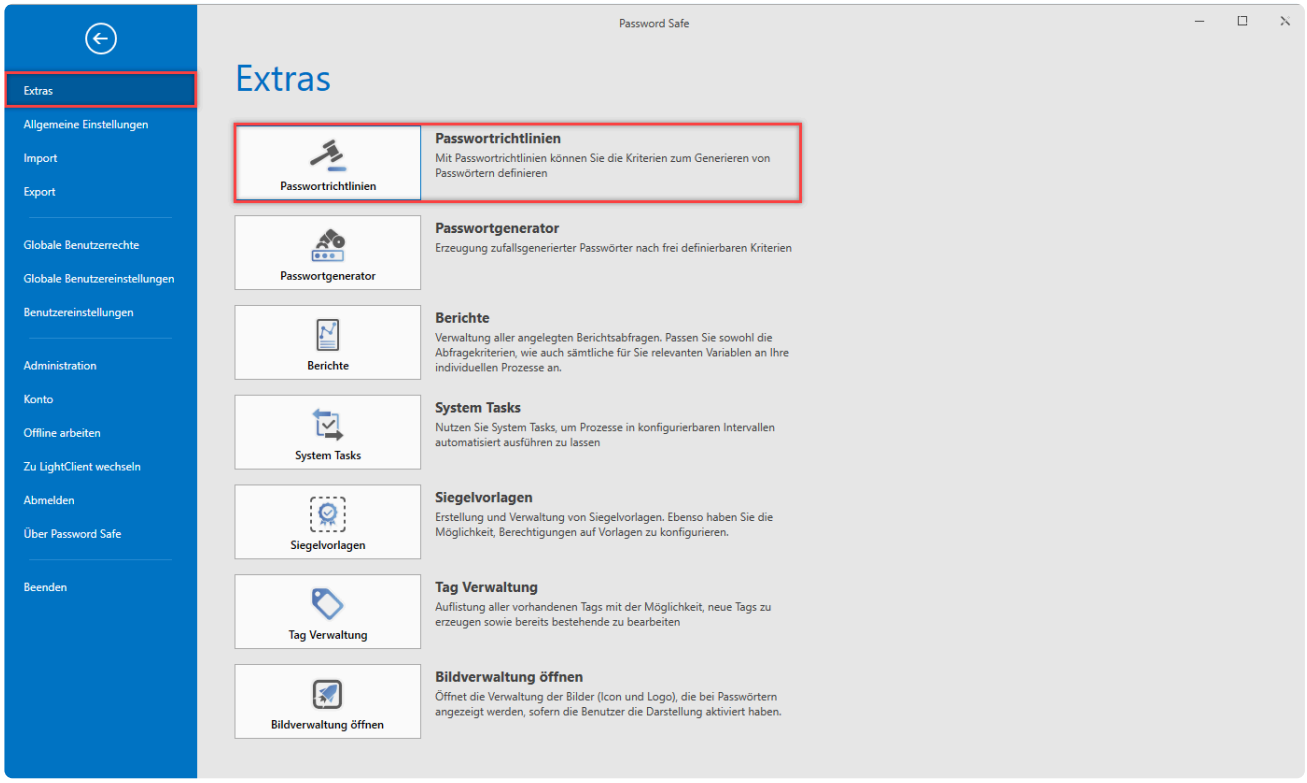
Sie wurden aufgrund von Inaktivität automatisch abgemeldet.

Eine erneute Anmeldung des Benutzers erfolgt wieder mit **Passwort** und **Key** wie oben beschrieben.
Nach erfolgreicher Anmeldung wird wieder die **Notfall-WebViewer-Export-Übersicht** angezeigt.

Passwortrichtlinien

Was sind Passwortrichtlinien?

Richtlinien bieten die Möglichkeit Benutzer an bestimmte Vorgaben zu binden. Somit erzwingen Sie den Einsatz von Passwörtern einer bestimmten Komplexität.



Relevantes Recht

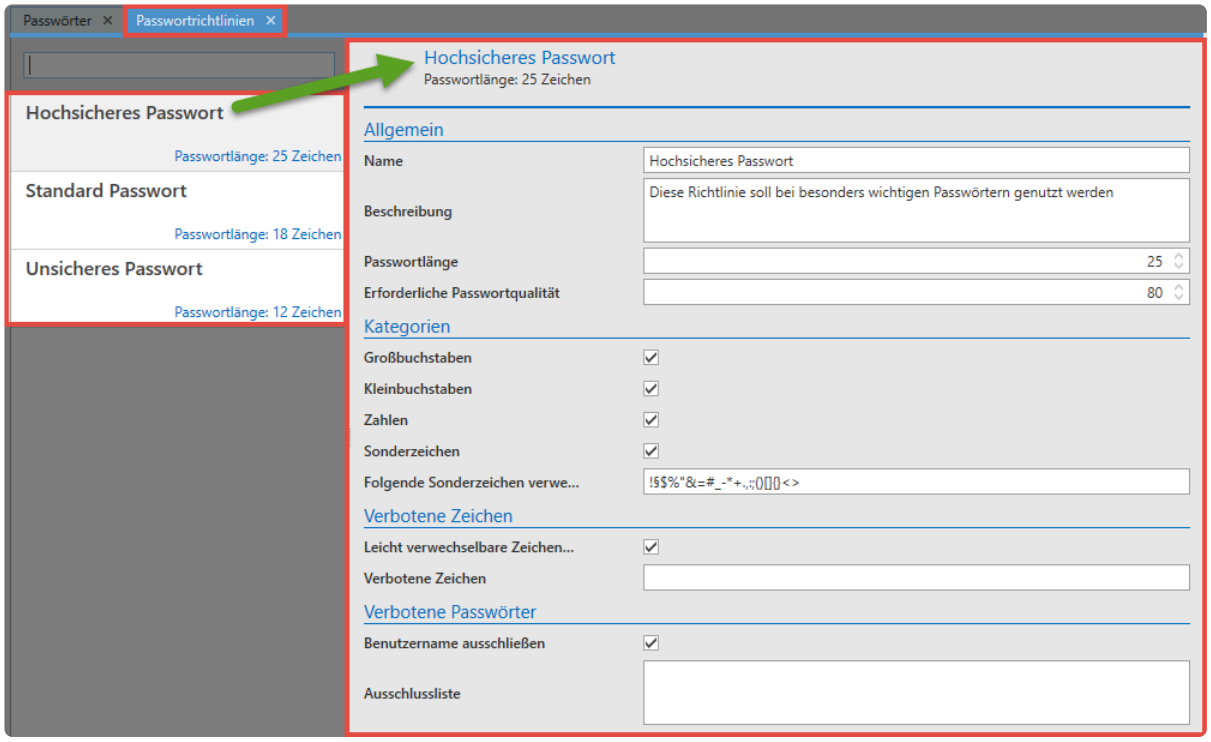
Folgende Option benötigen Sie um Passwortrichtlinien zu verwalten.

Benutzerrecht

- Kann Passwortrichtlinien verwalten

Verwaltung von Passwortrichtlinien

Wählen Sie unter Hauptmenü > Extras “**Passwortrichtlinien**” aus, erscheinen die verfügbaren Möglichkeiten 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:

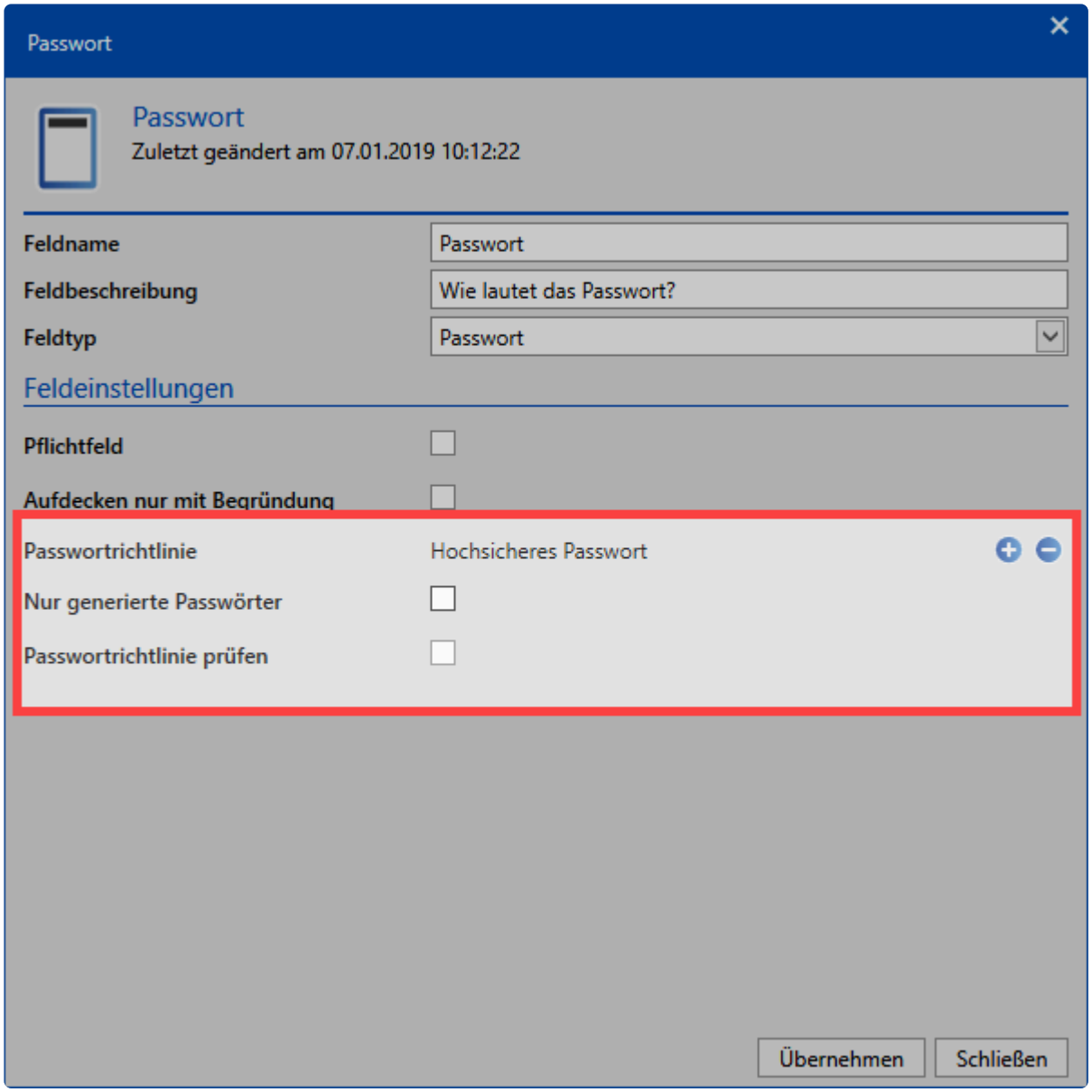
- **Allgemein**: Die Passwortlänge gibt die minimale Anzahl von Zeichen an, welche ein Passwort gemäß der vorliegenden Richtlinie erfüllen muss. Die erforderliche **Passwortqualität** ist ein internes Maß an Sicherheit, welche für diese Richtlinie errechnet wurde. Dieser Wert liegt immer zwischen 1 (sehr unsicher) und 100 (maximale Sicherheit).
- **Kategorien**: Es gibt insgesamt vier Kategorien, aus denen ein Passwort bestehen kann.
- **Verbotene Zeichen**: Auch das Ausschließen von manchen Sonderzeichen ist möglich. Diese tragen Sie ohne Trennzeichen in der Liste ein.
- **Verbotene Passwörter**: Bestimmte Passwörter sowie der Benutzername können Sie ebenso auf die Liste der verbotenen Passwörter aufführen.
- **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:

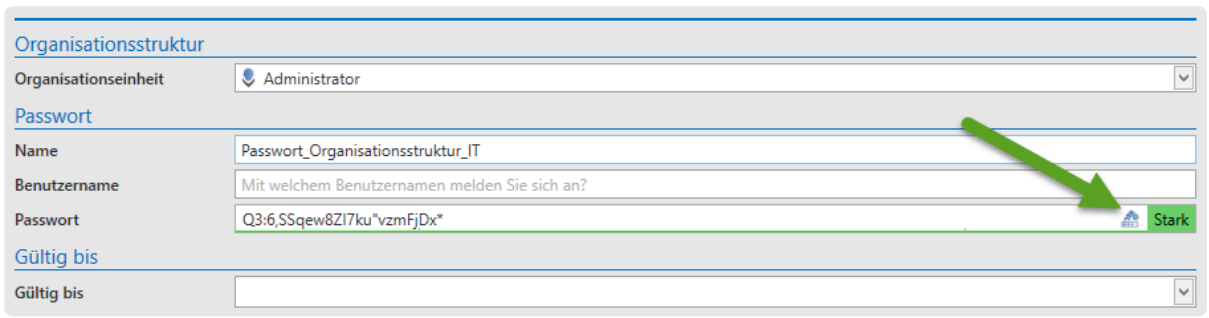
- Nutzung innerhalb des **Passwortgenerators**
- Vorgabe im Passwortfeld eines Formulars:

Definieren Sie in Formularen ein Passwortfeld, können Sie eine der definierten Passwortrichtlinien als Vorgabe setzen. Dies hat zur Folge, dass bei der Erstellung eines neuen Passwortes stets diese Vorlage genutzt wird. Auf diese Art und Weise stellen Sie sicher, dass für bestimmte Passwörter stets die geforderte Komplexität erreicht wird.



Ist auf einem Formular nun eine solche Richtlinie definiert, definieren Sie bei der Erstellung eines neuen Passwortes lediglich einen neuen Zufallswert für das Passwort. Nutzen Sie hierzu das Icon am rechten Ende des Passwortfeldes.

Ebenfalls schränken Sie mit der Funktion **nur generierte Passwörter** das Passwortfeld ein, sodass nur Passwörter aus dem Generator verwendet werden dürfen.
Die Funktion **Passwortrichtlinie prüfen** erlaubt bei manueller Eingabe eines Passwortes nur solche, welche der Richtlinie entsprechen.



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. Weitere Informationen hierzu finden Sie in einem **separaten Kapitel**.

Sichtbarkeit

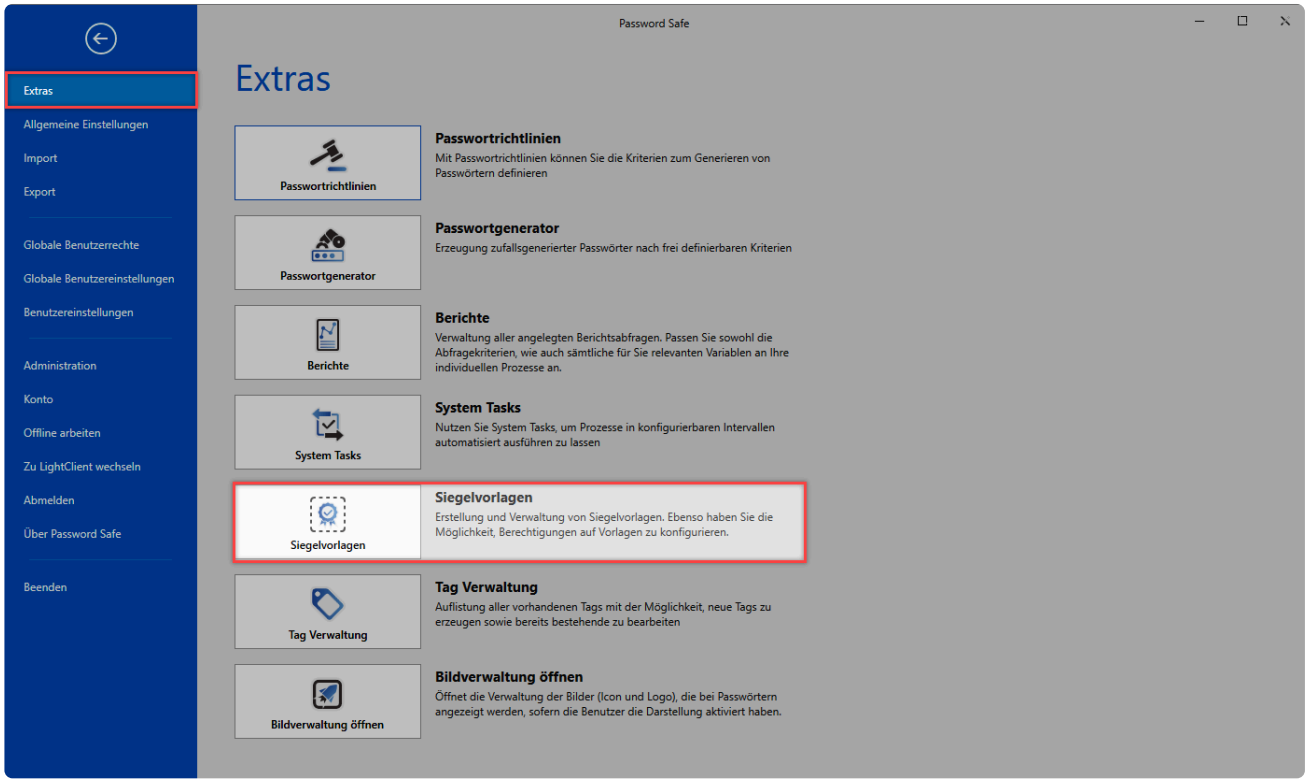
Passwortrichtlinien selbst unterliegen keinerlei Berechtigungen. Alle erstellten Richtlinien stehen somit allen Benutzern zur Verfügung. Die Richtlinien verwalten Sie über das Hauptmenü.

> Die Verwaltung der Richtlinien ist nur möglich, wenn der Benutzer das entsprechende Benutzerrecht besitzt.

Siegelvorlagen

Was sind Siegelvorlagen?

Die **Konfiguration von Siegeln** muss gut durchdacht und fehlerfrei sein. Es bietet sich an Siegelvorlagen abzuspeichern. Einmal definiert können Sie die Vorlagen mit wenigen Handgriffen an Datensätzen anbringen. Auch die Anpassung bereits erstellter Siegelvorlagen gestaltet sich übersichtlich und simpel.



> Die Bearbeitung der Standardvorlagen öffnet sich in einem eigenen Tab im aktiven Modul.

Relevante Rechte

Zum Verwalten der Siegelvorlagen benötigen Sie folgende Option:

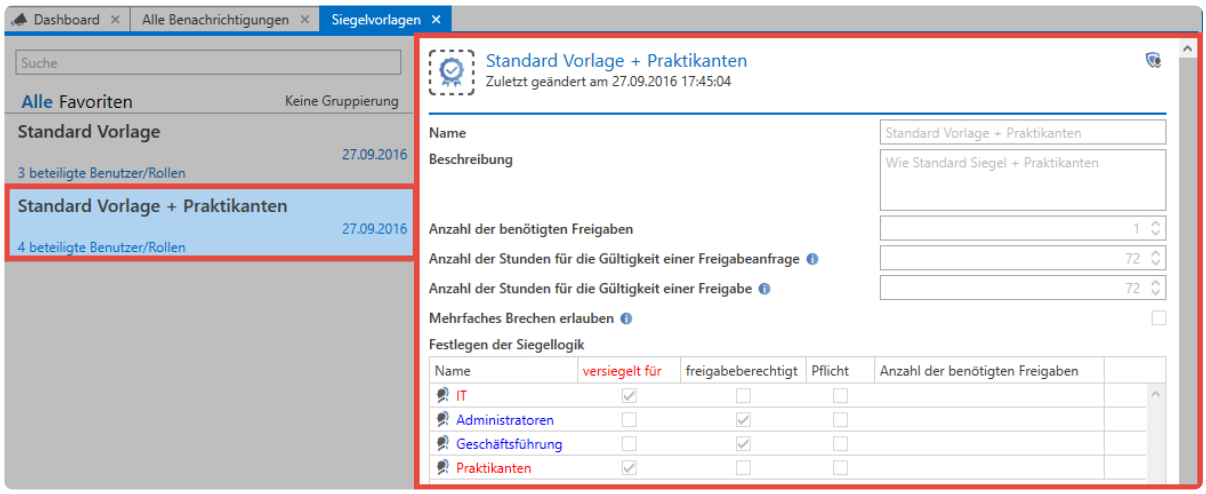
Benutzerrecht

- Kann Siegelvorlagen verwalten

Erstellung von Vorlagen

Bei der Erstellung von Siegeln speichern Sie über den Assistenten das Siegel **als Vorlage**. Diese werden in der Übersicht der Siegelvorlagen aufgelistet. Weiterhin haben Sie hier die Möglichkeit bestehende Vorlagen direkt zu bearbeiten. Dies geschieht analog zur Vorgehensweise im

Siegelassistenten.

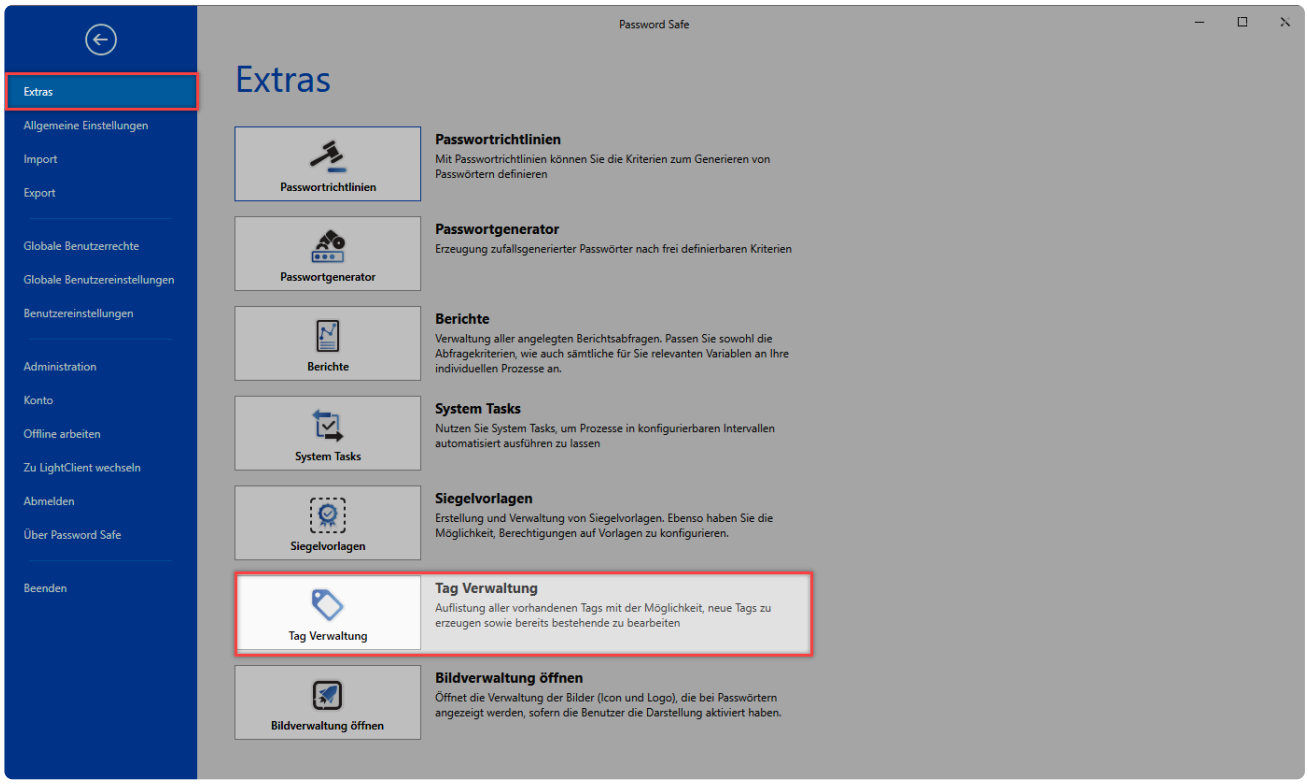


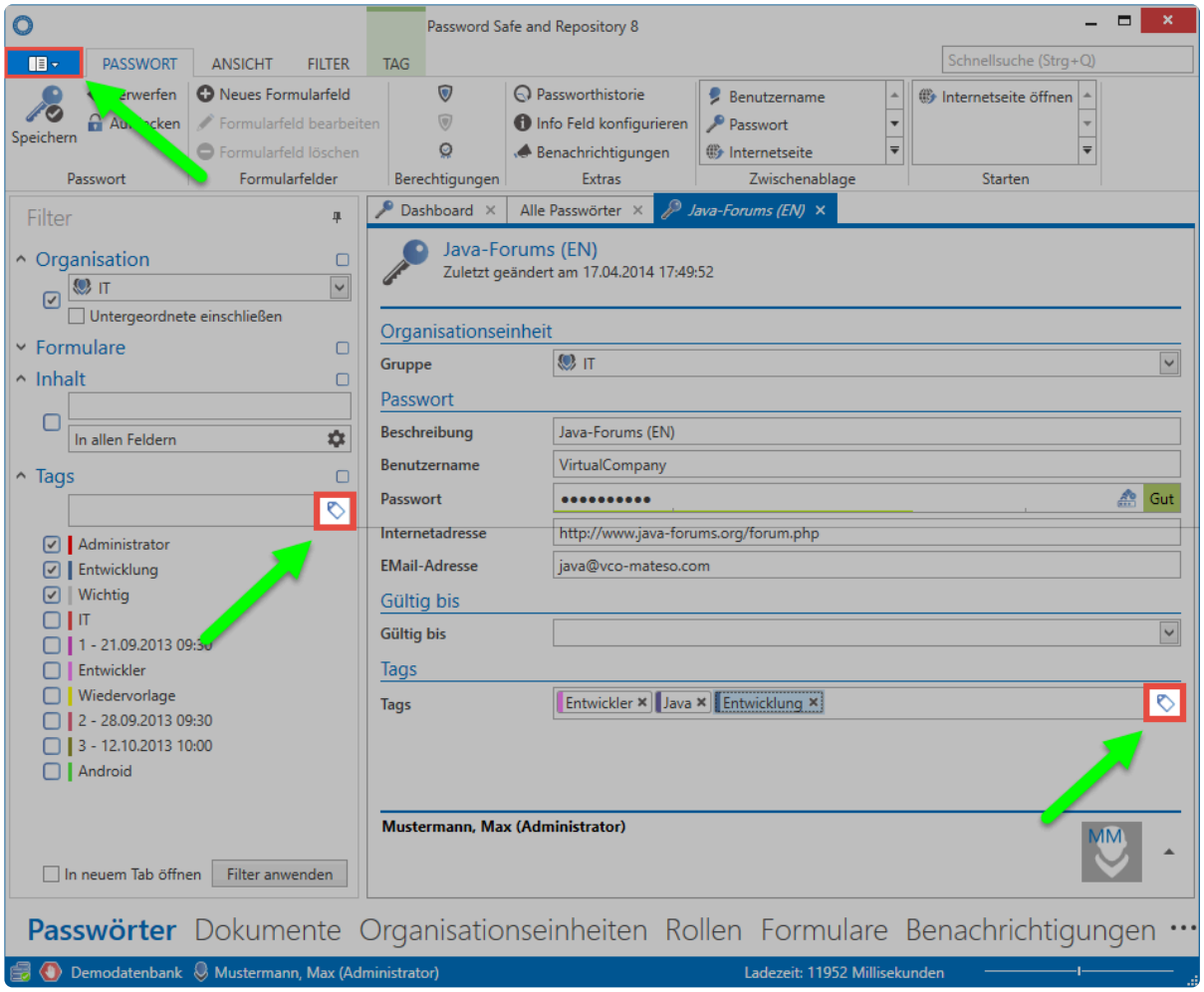
Sind Vorlagen einmal angelegt, können Sie diese bei der Erstellung neuer Siegel direkt auswählen.

Tagverwaltung

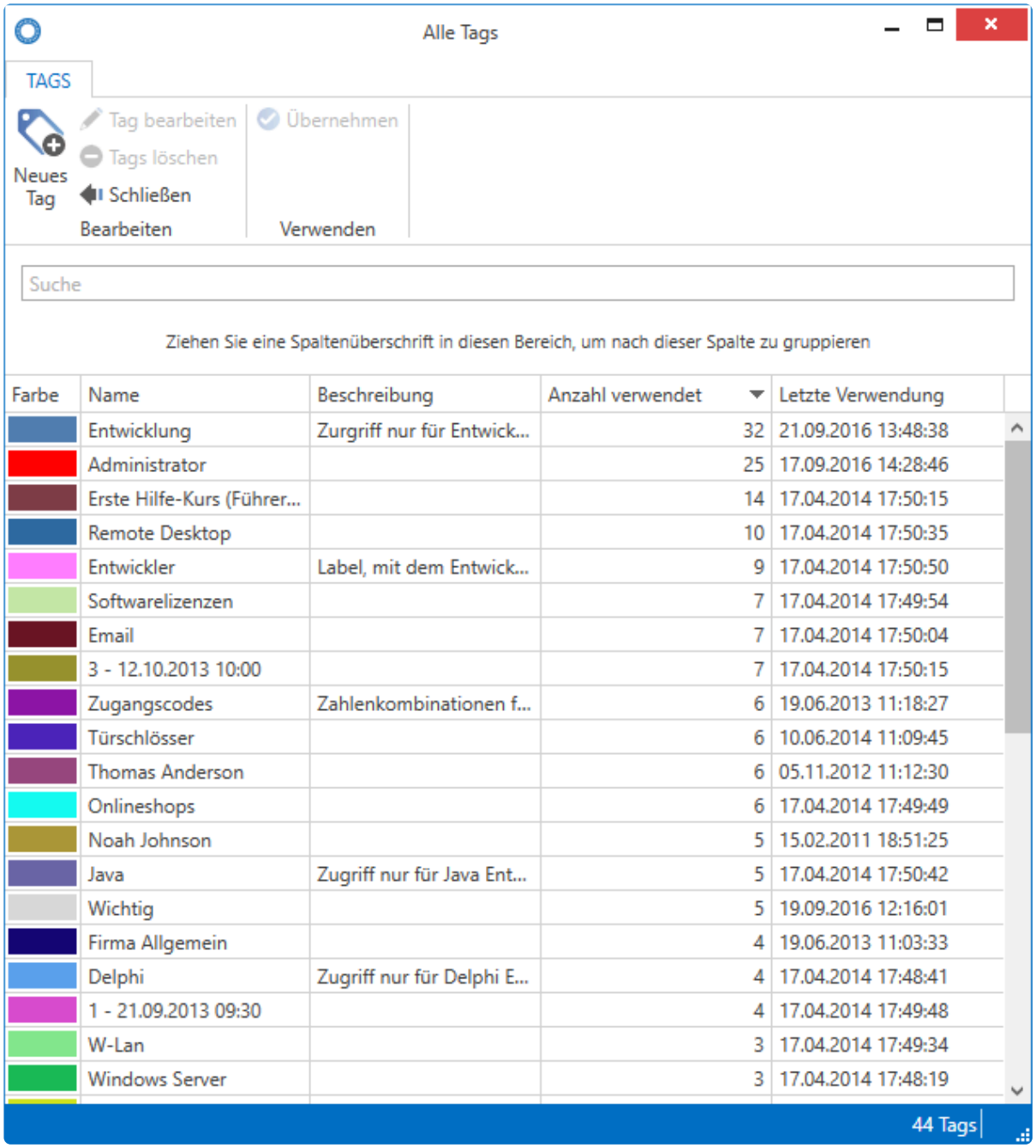
Was ist die Tagverwaltung?

Alle existierenden Tags können Sie direkt in der Tagverwaltung einsehen, bearbeiten und löschen. Sie erreichen 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 Sie alle relevanten Informationen einsehen und bearbeiten können. Auch die Zuweisung der Farben nehmen Sie hier vor. Die Spalte “Anzahl verwendet” zeigt hierbei an, wie oft ein Objekt mit dem jeweiligen Tag versehen wurde. Auf diese Art und Weise behalten Sie den Überblick und können nicht mehr benötigte Tags entfernen.



Relevante Rechte

Zum Verwalten von Tags ist folgende Option erforderlich:

Benutzerrecht

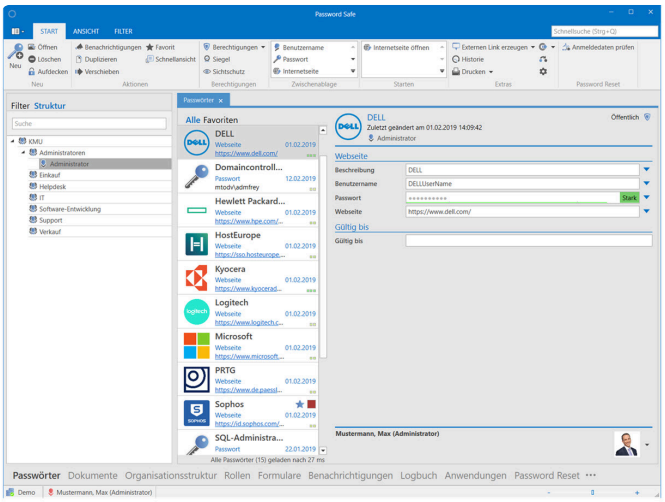
- Tags verwalten

> ! Das Löschen von Tags ist nur dann möglich, wenn diese mit keinerlei Daten mehr verknüpft sind.

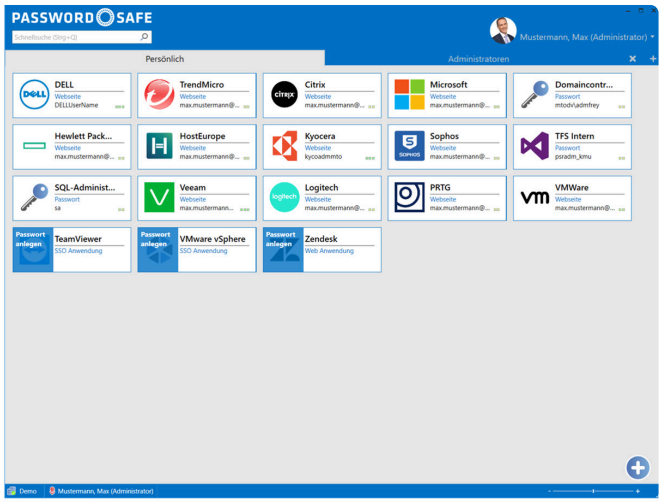
Bildverwaltung

Was ist die Bildverwaltung?

In der Bildverwaltung verwalten Sie alle Logos und Icons. Diese verbinden Sie dann mit den entsprechenden Datensätzen. Die Bilder werden sowohl im LightClient als auch im Client in der Listenansicht dargestellt.



Windows Client



Light Client

Relevante Rechte

Sie benötigen folgende Rechte:

- Kann neue Passwort-Bilder hochladen
- Kann Passwort-Bilder verwalten

> Wichtig ist hierbei, dass die Einstellung **“Nach Favicon-Download fragen”** nur greift, wenn das Recht **“Kann neue Passwort-Bilder hochladen”** aktiviert ist!

Verwalten von Icons / Logos

Sie haben zwei Möglichkeiten, Icons hochzuladen.

1. Mit Anlegen bzw. Speichern des Datensatzes

Um Favicons direkt beim Speichern des Datensatzes zu importieren, müssen Sie folgende Voraussetzungen erfüllen:

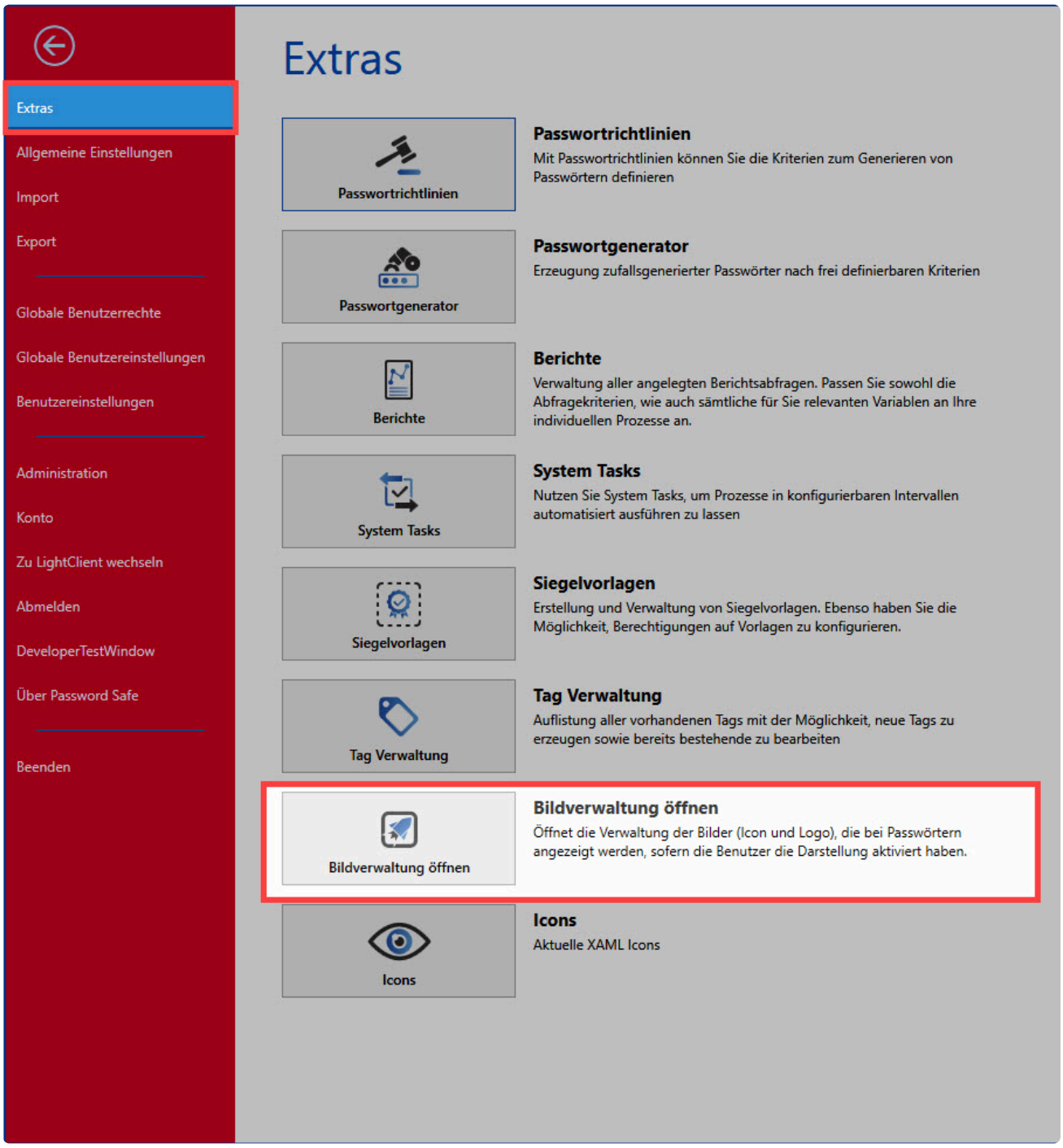
- Die Einstellung **“Favicon-Download fragen”** ist aktiviert.
- Im Datensatz ist eine URL hinterlegt.

Sind diese Voraussetzungen gegeben, wird beim Speichern des Datensatzes die hinterlegte URL auf das Favicon hin geprüft. Wird ein Favicon gefunden, wird es in die Datenbank importiert und zukünftig beim Datensatz angezeigt.

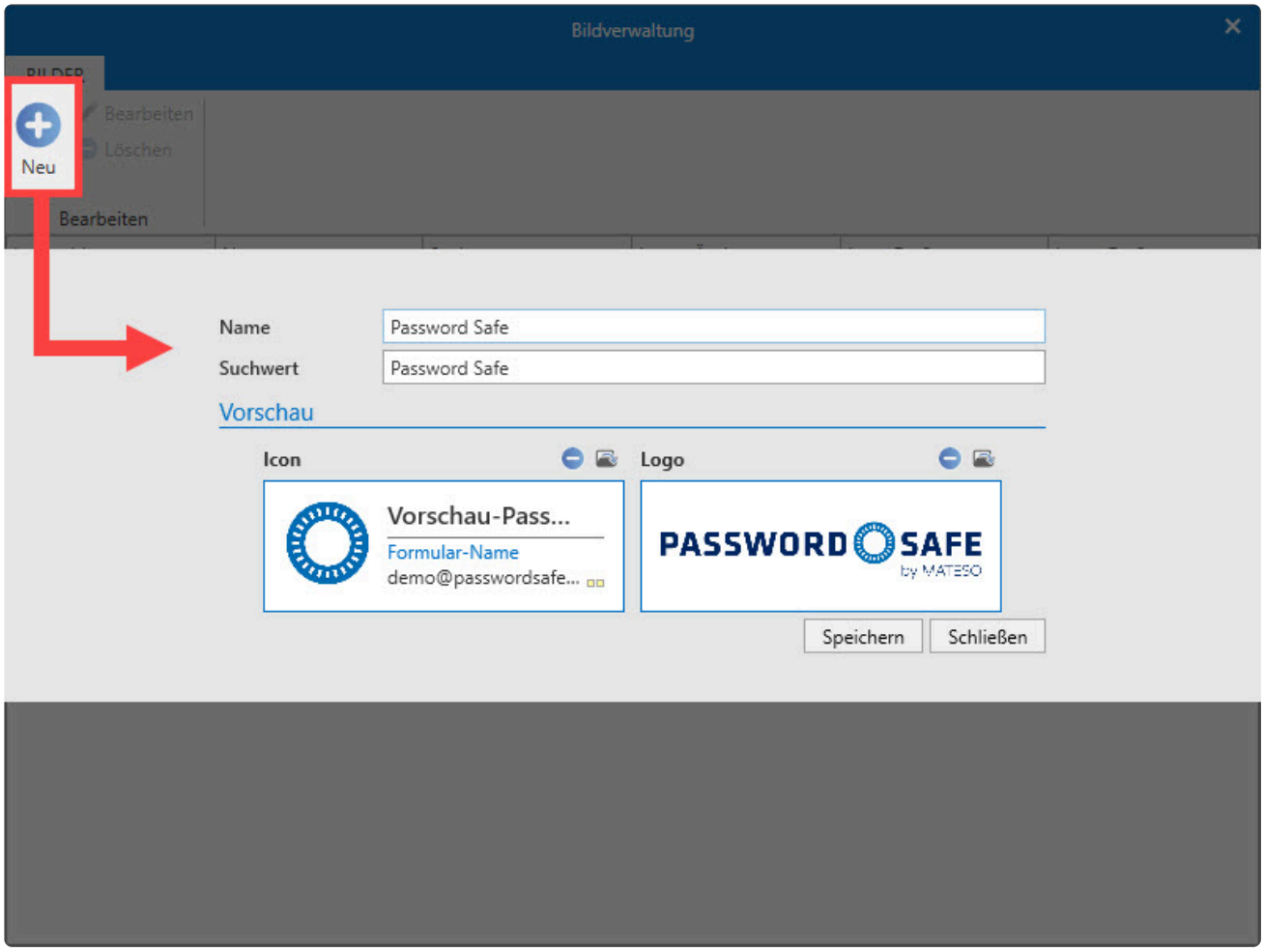
> Bei mehreren hinterlegten URLs wird immer die erste URL beachtet.

2. Manuelles Hinterlegen

Sie finden die Bildverwaltung im Hauptmenü bei den Extras. Hier besteht die Möglichkeit, Icons und Logos manuell zu hinterlegen.



Durch einen Klick auf das **+** -Symbol öffnet sich die Maske zum Anlegen von Bildern.



- **Name**: Hier benennen Sie die Bilder.
- **Suchwert**: Beachten Sie folgende Priorität:
  - **Passwörter**: Erste URL im Passwort (falls mehrere URLs hinterlegt sein sollten) -> angehängte Tags -> Passwortname -> Namen von verbundenen Anwendungen
  - **Anwendungen**: In der Anwendung hinterlegte URL -> angehängte Tags -> Anwendungsname
- : Über dieses Symbol laden Sie lokal gespeicherte Icons und Logos hoch.

Beachten Sie, dass die Icons und Logos nicht lokal, sondern in der Datenbank abgespeichert werden.

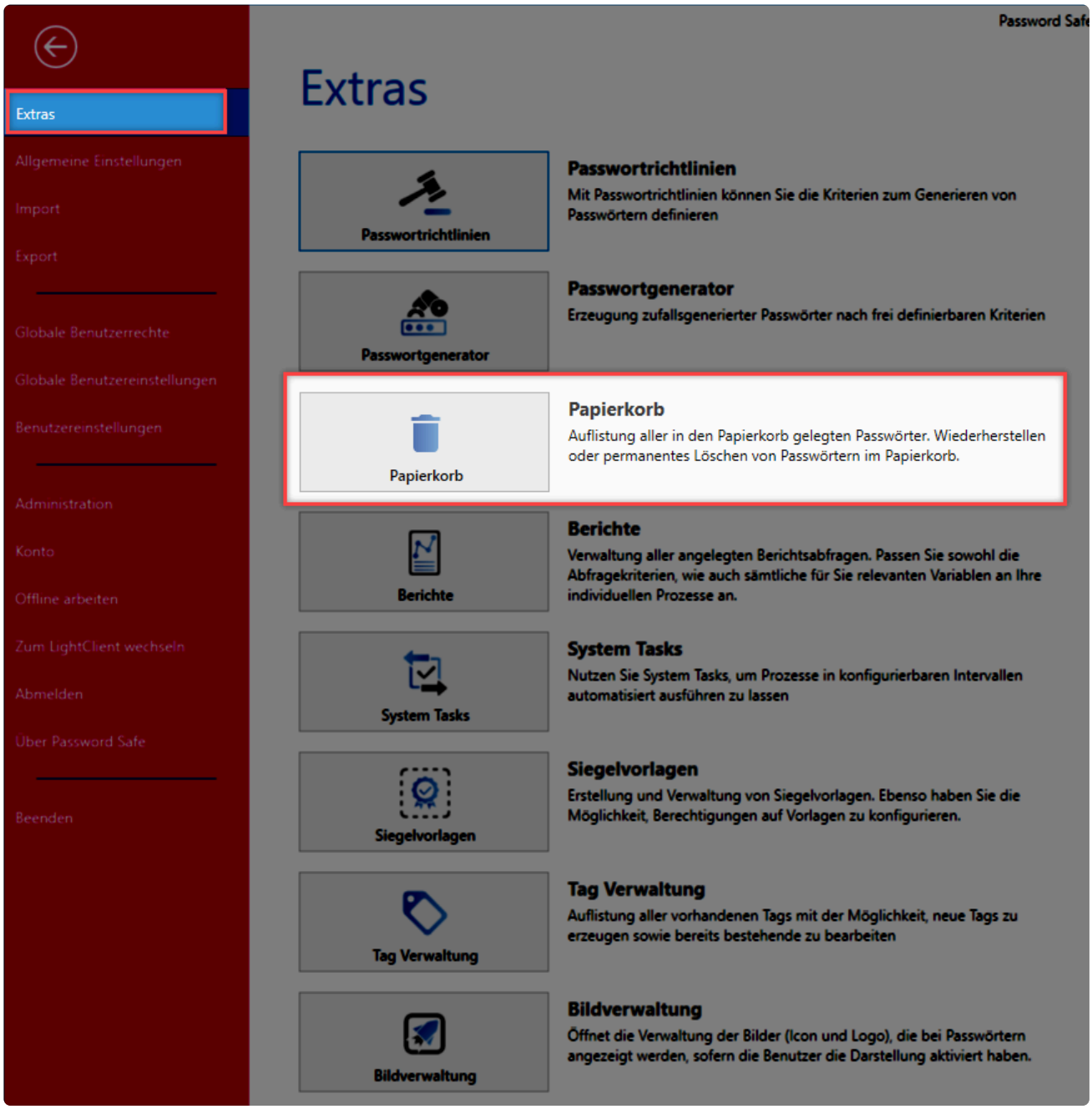
Bedingungen

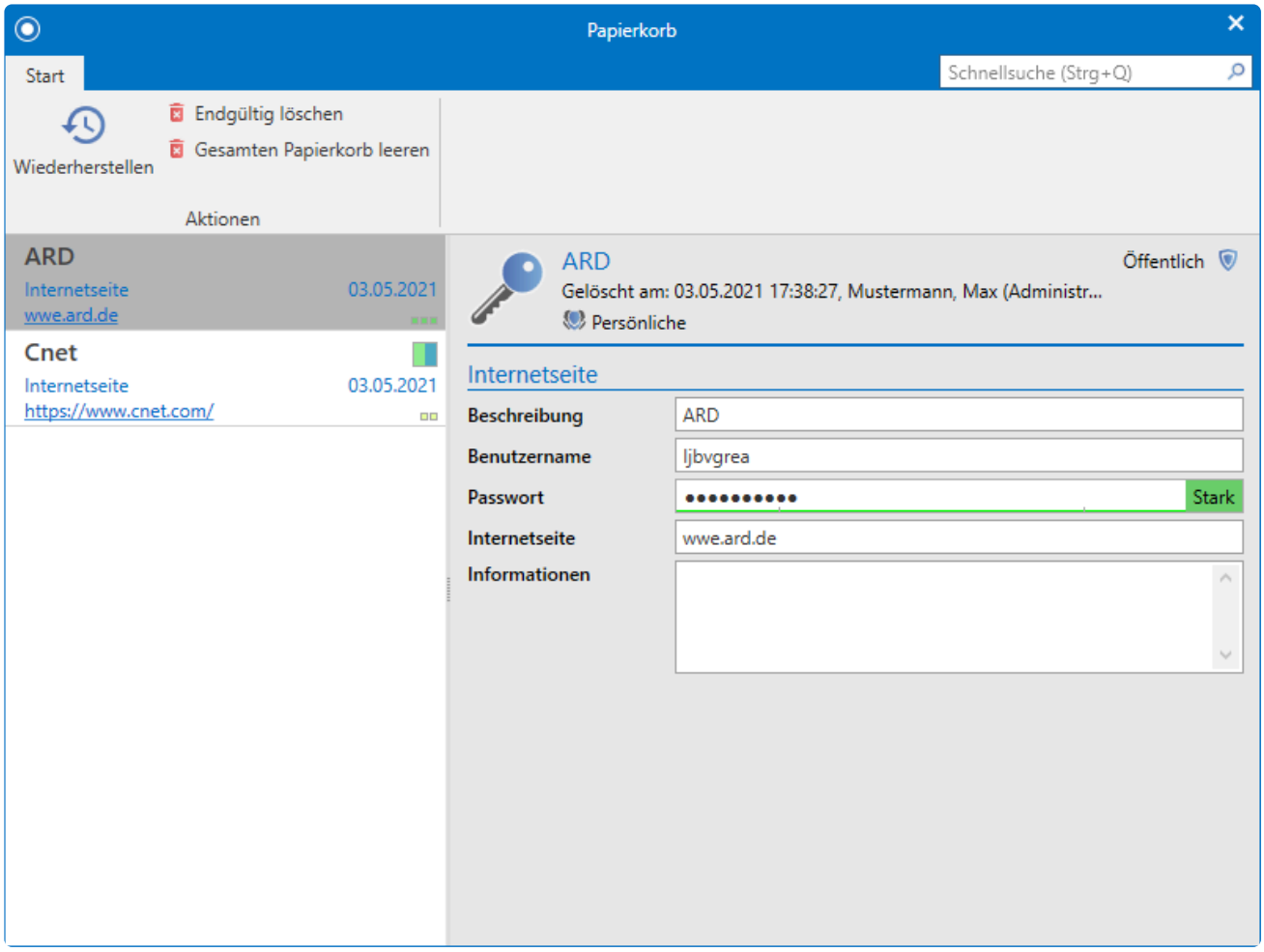
Damit Sie Icons / Logos dementsprechend hochladen und abspeichern können, müssen Sie folgende Bedingungen erfüllen:

- Die maximale Größe einer Bilddatei beläuft sich auf 100 MB.
- Unterstützte Formate sind png, jpg, bmp, ico und svg.
- Mehrere Suchwerte sind durch ein Komma getrennt möglich (“Netflix.de, Netflix.com”).

Papierkorbverwaltung

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

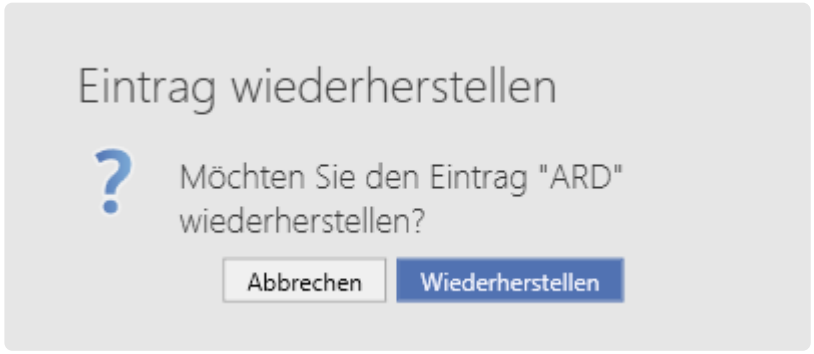




Funktionen

Folgende Funktionen stehen Ihnen zur Verfügung:

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



- **Endgültig löschen**: Die ausgewählten Passwörter werden endgültig gelöscht. Damit können diese nicht mehr wiederhergestellt werden.

- **Papierkorb leeren**: Der komplette Papierkorb wird endgültig gelöscht, somit kann keines dieser Passwörter wiederhergestellt werden.

Allgemeine Einstellungen

Was sind die allgemeine Einstellungen?

Die **Allgemeinen Einstellungen** sind benutzerbezogen. Somit kann jeder Benutzer die Software auf die eigenen Bedürfnisse anpassen. Sie können folgende Optionen konfigurieren:

Farbschema

Es stehen Ihnen mehrere Windows Farbschemata zur Auswahl. Das Farbschema **Colorful** stellt z.B. verschiedene Farben bereit, welche das unterscheiden der Module in der Software erleichtern. Der Client muss bei einer Änderung des Farbschemas neu gestartet werden.

Sprache

Wählen Sie zwischen Deutsch und Englisch. Nach dem Ändern der Sprache muss der Client neu gestartet werden.

Starte Anwendung minimiert im Benachrichtigungsbereich

Minimieren Sie den Client, um Password Safe im Hintergrund zu betreiben. 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.

Mit Windows starten

Selbstverständlich können Sie den Password Safe Client auch direkt mit Windows starten.

Client-übergreifende Anmeldung

Die Client-übergreifende Anmeldung betrifft nur den FullClient und den SSO-Agent. Achten Sie bei der ersten Einrichtung darauf, dass nur einer der beiden Clients geöffnet ist. Sobald Sie den den Haken setzen, werden Sie, nach der erfolgreichen Anmeldung an einem Client, mit dem angemeldeten Benutzer auch am anderen Client eingeloggt.

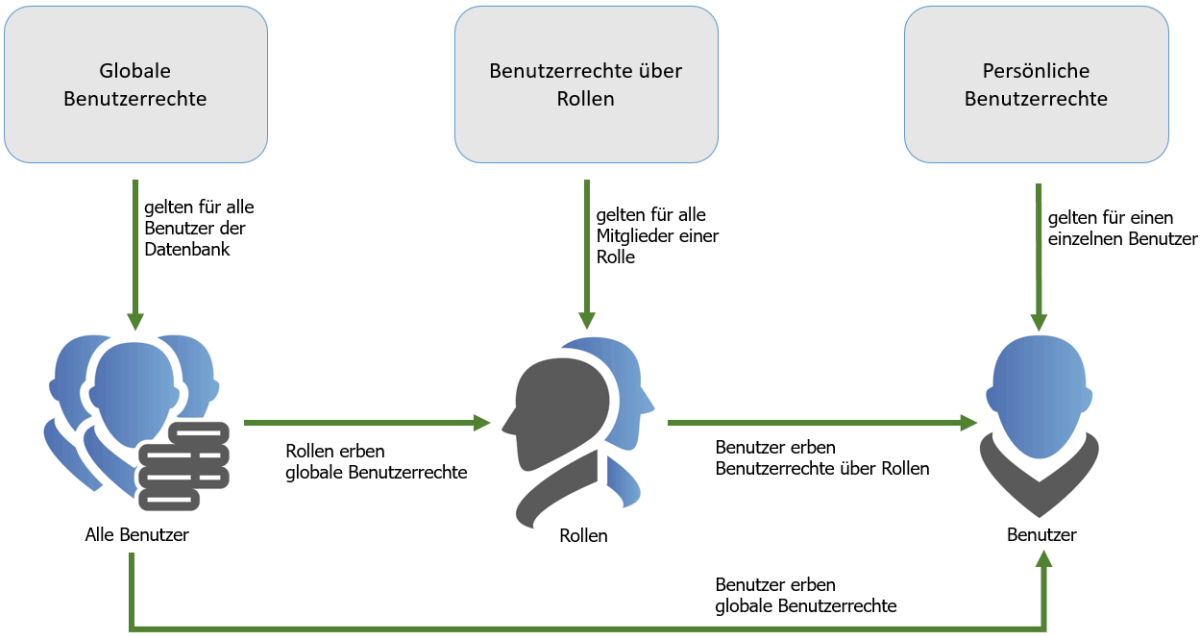
Benutzerrechte

Was sind Benutzerrechte?

Über die Benutzerrechte konfigurieren Sie den Zugang zu Funktionalitäten. Sie können beispielsweise die Sichtbarkeit einzelner **Module** oder auch die Nutzung von Import und Export erlauben bzw. untersagen. Eine vollständige Auflistung ist direkt in den Benutzerrechten einsehbar.

Verwaltung von Benutzerrechten

Alle Benutzerrechte können Sie über ein dreistufiges Konzept konfigurieren. Sie können Funktionalitäten allgemein zur Verfügung stellen. Analog zum Berechtigungskonzept können auch für die Benutzerrechte mehrere Benutzer zusammengefasst werden. Es ist auch möglich auf individuelle Anforderungen einzelner Benutzer einzugehen.

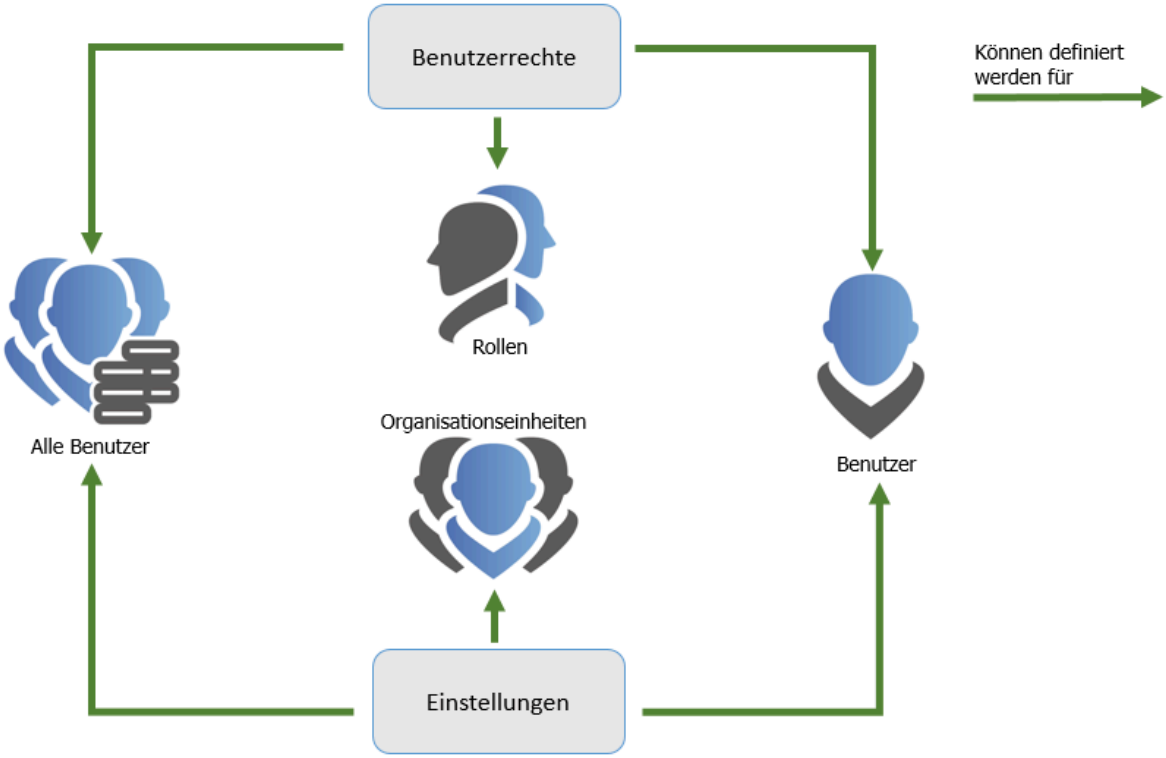


Am Ende der Benutzerrechte steht immer der jeweilige Benutzer. Dieser erhält die Benutzerrechte immer auf einem der drei folgenden Wege:

1. Das **persönliche Benutzerrecht** gilt immer nur für einen bestimmten Benutzer. Konfiguriert wird es 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 können Sie in den **Einstellungen** vornehmen.

! Zusätzlich zu persönlichen und globalen Benutzerrechten werden (im Gegensatz zu den **Einstellungen**) Benutzerrechte nicht über Organisationseinheiten, sondern über Rollen vergeben.

Sie können nur diejenigen Benutzerrechte vergeben, welche Sie selbst haben. Entziehen können Sie jedoch alle Rechte.



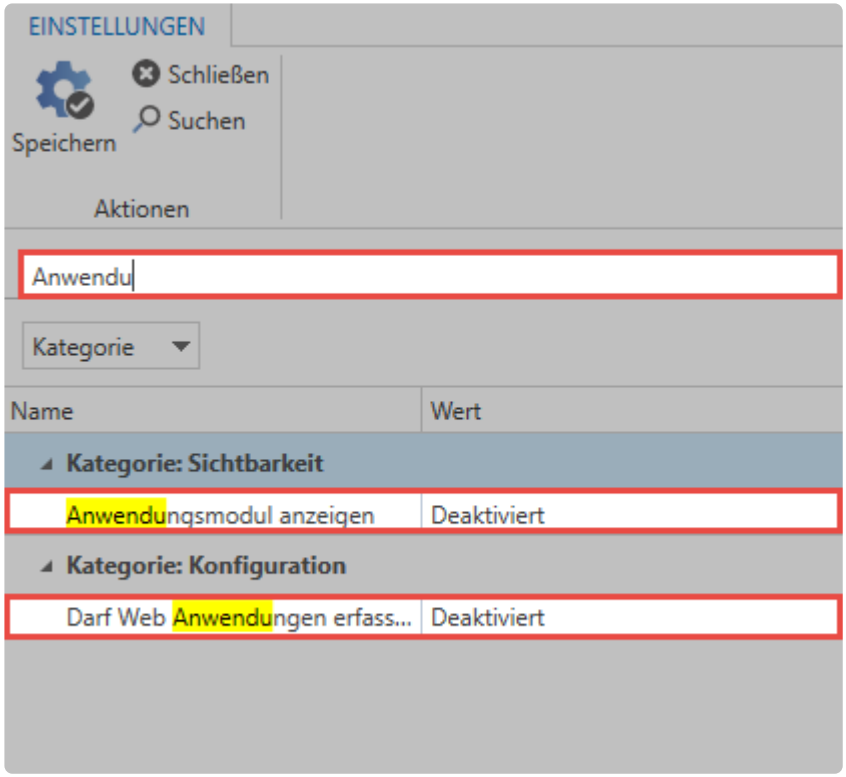
Konfiguration der Sicherheitsstufe

In den Benutzerrechten können Sie auch die **Sicherheitsstufe** festlegen. 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

Über die Suche können Sie die gewünschte Option schnell auffinden. Funktionell orientiert sich diese an der **Listensuche**.



Datenbank Administrator

Besonderes Augenmerk sollten Sie auf das Recht **Ist Datenbank Administrator** legen. Dieses Recht hat folgende Auswirkungen:

- Der Benutzer kann auch Rechte vergeben, welche er selbst nicht hat.
- Der Benutzer kann ausschließlich durch andere Datenbank Administratoren aus Rechten entfernt werden.
- Der Benutzer kann am AdminClient andere Benutzer entsperren.
- Der Benutzer kann andere Benutzer auch aus den Rechten entfernen wenn diese das Besitzer Recht haben.

Übersicht aller Benutzerrechte

In diesem Kapitel werden alle vorhandenen Benutzerrechte aufgeführt. Wird ein Recht in einem anderen Kapitel weiter erläutert, so können Sie über den Link in der Spalte **Kapitel** direkt dorthin gelangen. Für eine bessere Übersicht werden die Rechte hier nach Kategorien gruppiert.

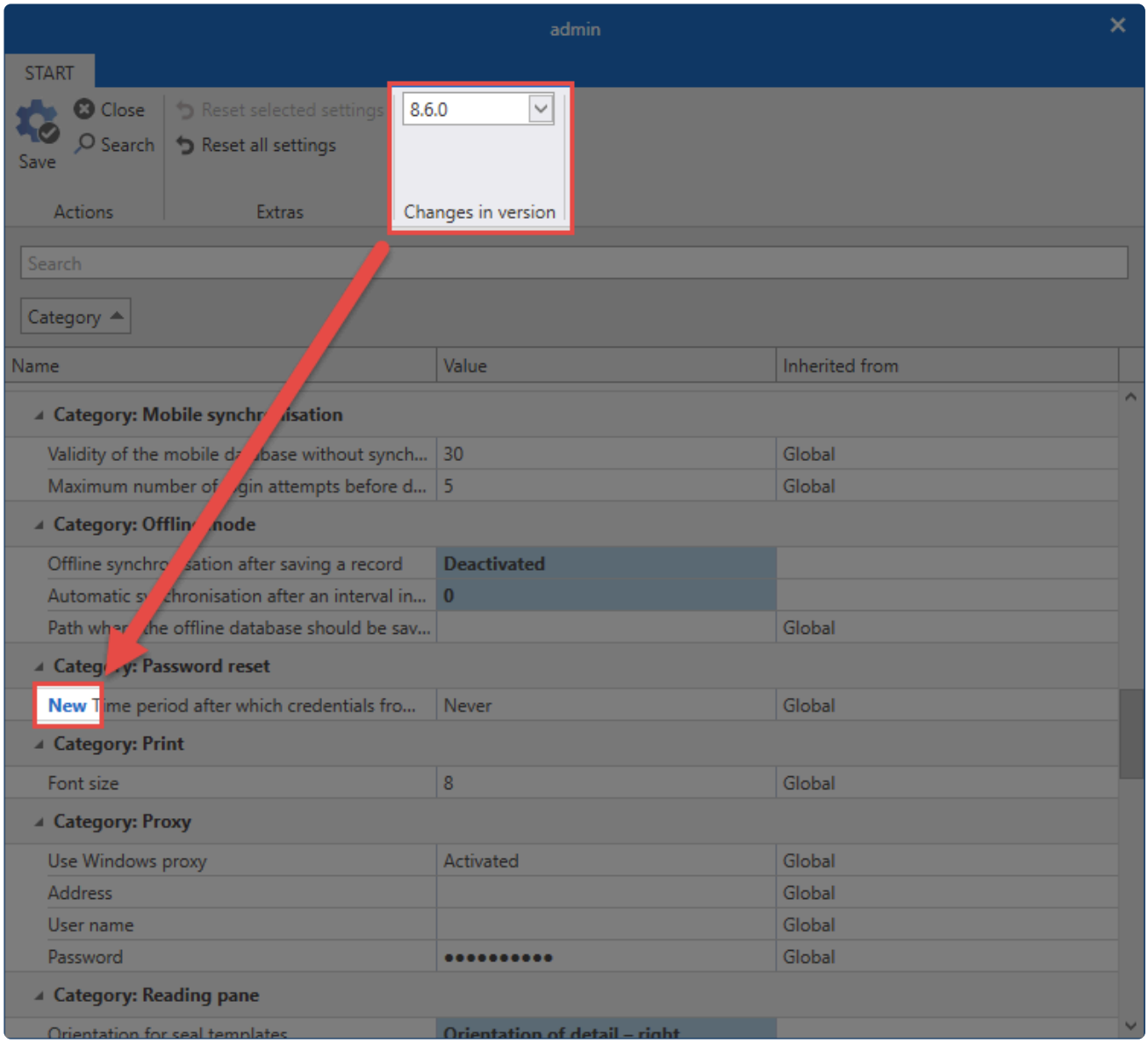
Kategorie: Allgemein	**Kapitel**	**neu**
Kann Berechtigungen überschreiben	Formularfeldberechtigungen	
Kann Berechtigungen vererben	Formularfeldberechtigungen	
Kategorie: Fußbereich	**Kapitel**	**neu**
Kann in Fußbereich Benachrichtigungen sehen	Lesebereich	
Kann in Fußbereich die Metadaten von Dokumenten sehen	Lesebereich	
Kann in Fußbereich Dokumente sehen	Lesebereich	
Kann in Fußbereich Historie sehen	Lesebereich	
Kann in Fußbereich Logbuch sehen	Lesebereich	
Kann in Fußbereich Password Reset sehen	Lesebereich	
Kategorie: Konfiguration	**Kapitel**	**neu**
Kann drucken	Drucken	
Kann exportieren	Export	
Kann Filter bearbeiten	Filter	
Kann Formular eines Passworts wechseln	Formular wechseln	
Kann importieren	Import	
Kann Passwortformularfelder verwalten		
Kann Sichtschutz anbringen	Sichtschutz	
Kann Siegel anbringen	Siegel	
Kann Siegelvorlagen verwalten	Siegelvorlagen	
Kann Tags verwalten	Tags	
Kann Tab der eigenen Organisationseinheit im LightClient schließen		
Kategorie: Mobile Synchronisation	**Kapitel**	**neu**
Kann mit mobilen Geräten synchronisieren	Mobile Geräte	
Kategorie: Neue Datensätze	**Kapitel**	**neu**
Kann neue Active Directory Profile anlegen	Ende-zu Ende / Master Key	

Kann neue Anwendungen vom Typ RDP anlegen	RDP Anwendungen	
Kann neue Anwendungen vom Typ SSH anlegen	SSH Anwendungen	
Kann neue Anwendungen vom Typ SSO anlegen	SSO Anwendungen	
Kann neue Anwendungen vom Typ Web anlegen	Web Anwendungen	
Kann neue Benutzer anlegen	Benutzerverwaltung	
Kann neue Dokumente anlegen	Dokumente	
Kann neue Anwendungen vom Typ SAML anlegen		
Kann neue Formulare anlegen	Formulare	
Kann neue Organisationseinheiten anlegen	Organisationsstruktur / Benutzerverwaltung	
Kann neue Password Resets anlegen	Password Reset	
Kann neue Passwörter anlegen	Passwörter / Erstellen neuer Passwörter	
Kann neue Rollen anlegen	Rollen	
Kann neue Tags anlegen	Tags	
Kann neue Passwort-Bilder hochladen		
Kann individuelle Passwörter im LightClient anlegen		
Kategorie: Offline-Modus	**Kapitel**	**neu**
Offline-Modus	Einrichten und Synchronisieren	
Zeitspanne, wie lange der Offline-Modus ohne Serververbindung benutzt werden kann	Einrichten und Synchronisieren	
Kategorie: Rechte	**Kapitel**	**neu**
Wenn Nicht-Administratoren beim Verschieben von Datensätzen die Aktion “Berechtigungen überschreiben” wählen, bleiben die aktuellen Berechtigungen für Administratoren erhalten		✔
Kategorie: Rechtevorlagen	**Kapitel**	**neu**
Kann Mitglieder beim Verwenden einer Rechtevorlage bearbeiten		
Kann Rechtevorlagen verwalten	Relevante Benutzerrechte	
Kann Rechtevorlagen-Auswahl sehen	Relevante Benutzerrechte	
Kann Standard-Rechtevorlage wechseln	Relevante Benutzerrechte	
Kategorie: Sicherheit	**Kapitel**	**neu**
Ist Datenbank-Administrator		

Kann Active Directory Profile verwalten		
Kann andere Benutzer auf persönliche Passwörter berechtigen		
Kann Aufzeichnungen einer Anwendung verwalten	Sitzung aufzeichnen	
Kann Autologin verwalten	Konto	
Kann Besitzrecht setzen		
Kann Datenabanksitzungen verwalten		
Kann gelöschte Benutzer endgültig löschen		
Kann gelöschte Organisationsstrukturen endgültig löschen		
Kann gelöschte Organisationsstrukturen sehen		
Kann gelöschte Rollen endgültig löschen		
Kann gelöschte Rollen sehen		
Kann gesperrte Benutzer verwalten		
Kann globale Einstellungen bearbeiten		
Kann HTML WebViewer exportieren	HTML WebViewer	
Kann Optionen der Sicherheitsstufe ändern		
Kann Passwortrichtlinien verwalten	Passwortrichtlinien	
Kann persönliche Datensätze erstellen		
Kann Standard-Passwortrichtlinien konfigurieren	Administration	
Kann Stapelverarbeitung bei Berechtigungen anhand eines Filters durchführen	Mehrfachbearbeitung von Berechtigungen	
Kann Passwort-Bilder verwalten		
Kategorie: Sichtbarkeit	**Kapitel**	**neu**
Anwendungs-Modul anzeigen	Client Module	
Benachrichtigungs-Modul anzeigen	Client Module	
Discovery Service Modul anzeigen	Client Module / Discovery Service	
Dokument-Modul anzeigen	Client Module	
Formular-Modul anzeigen	Client Module / Formulare	
Logbuch-Modul anzeigen	Client Module / Logbuch	
Organisationsstruktur-Modul anzeigen	Client Module / Organisationsstruktur	
Password Reset Modul anzeigen	Client Module / Password	

	Reset	
Passwort-Modul anzeigen	Client Module / Erstellen neuer Passwörter	
Rollen-Modul anzeigen	Client Module / Ende-zu-Ende / Master Key / Rollen	
Kategorie: System Tasks	**Kapitel**	**neu**
Kann Active Directory System Tasks verwalten	System Task	
Kann Berichte System Tasks verwalten	System Task	
Kann Discovery Service System Tasks verwalten	System Task / Discovery Service	
Kann Notfall WebViewer Export System Tasks verwalten	System Task	
Kann WebViewer Export System Tasks verwalten	System Task	

In den Benutzerrechten gibt es eine Versions-Auswahlbox. Die Optionen, die in der ausgewählten Version neu hinzugefügt wurden, werden der Liste entsprechend markiert.



Das macht es den Administratoren leichter, neue Optionen korrekt zu konfigurieren, bevor sie das Update für alle Mitarbeiter freigeben.

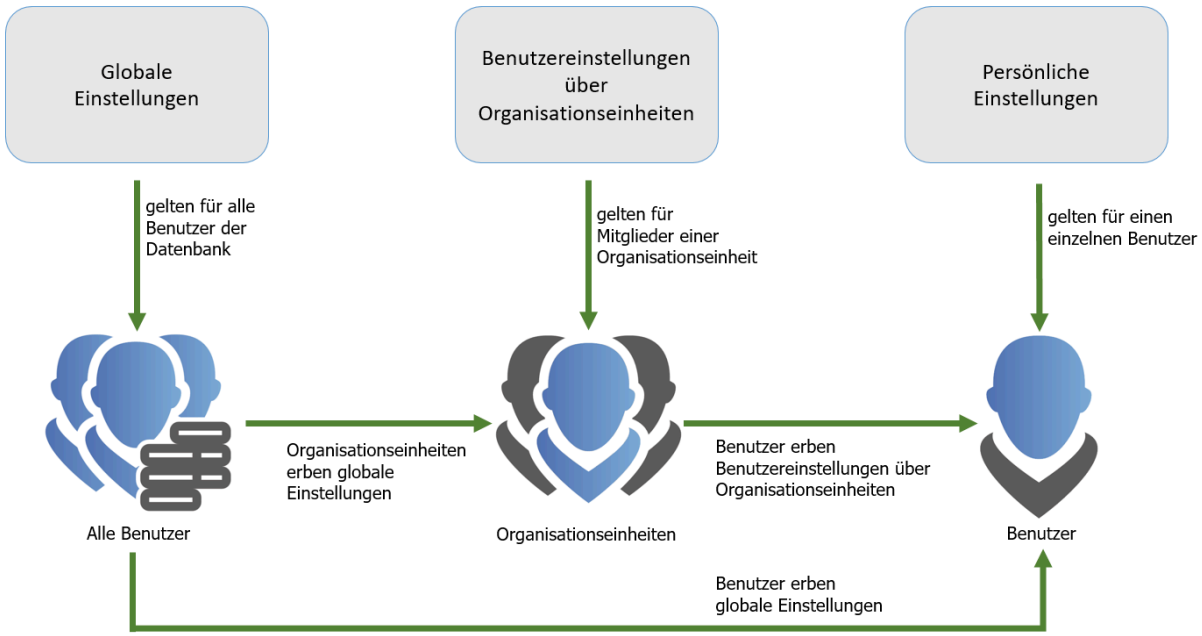
Benutzereinstellungen

Was sind Benutzereinstellungen

Sie können in Password Safe zahlreiche Funktionen an die Bedürfnisse von Benutzern anpassen. Auch die Darstellungen der Software kann konfiguriert werden. Diese Einstellungen können in mehreren Stufen vererbt werden. Darüber hinaus gibt es das **Konzept von Sicherheitsstufen**, über welches Sie Benutzer in fünf verschiedene Kategorien einordnen können. Die Verwaltung von Einstellungen kann somit granular definiert werden.

Verwaltung von Benutzereinstellungen

Die Konfiguration der Benutzereinstellungen ähnelt dem Vorgehen bei den **Benutzerrechten**. Auch hier gibt es drei Möglichkeiten, mit denen ein Benutzer seine Einstellungen definieren kann, bzw. von anderer Stelle konfiguriert bekommt. Es bietet sich an die User nicht einzeln zu konfigurieren, sondern mehrere gleichberechtigte Benutzer zusammenfassend mit Einstellungen zu versehen.

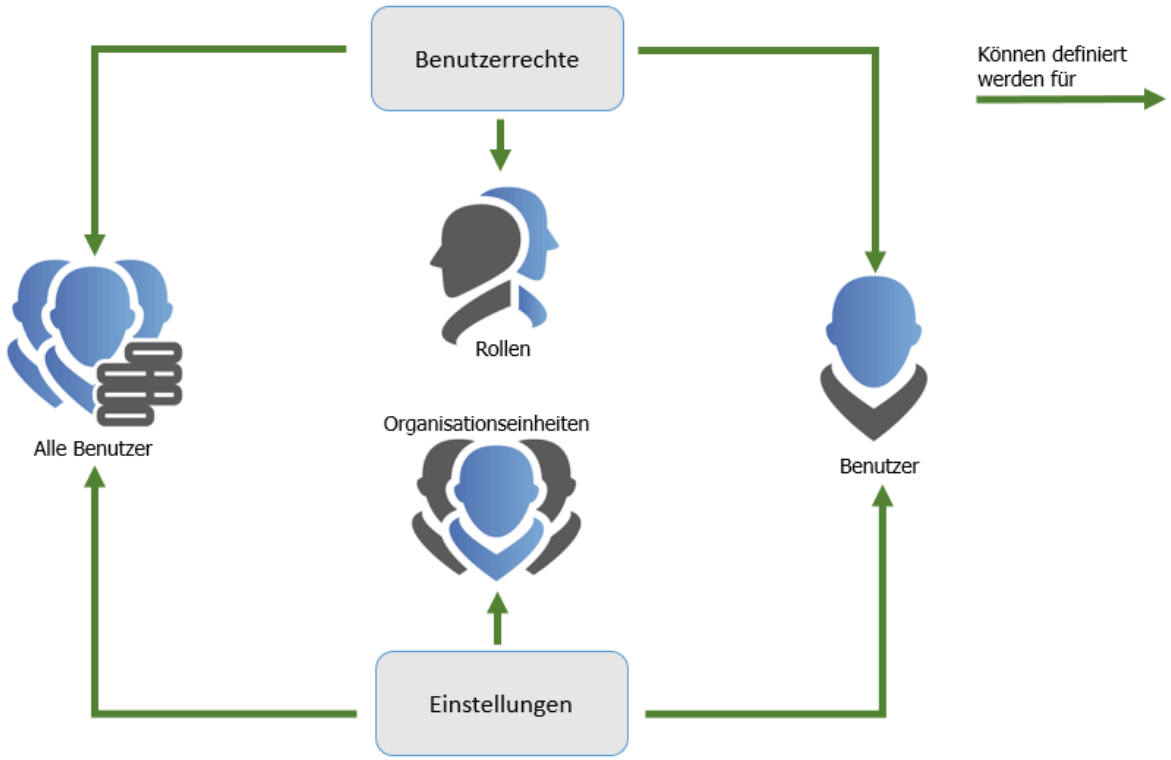


Der Benutzer erhält seine Einstellungen über einen der drei folgenden Wege:

1. **Persönliche Einstellungen** gelten immer nur für einen bestimmten Benutzer. Sie konfigurieren diese über das Modul Organisationsstruktur.
2. **Einstellungen über Organisationseinheiten** gelten für alle Mitglieder einer Organisationseinheit und werden im Modul Organisationsstruktur definiert.
3. **Globale Einstellungen** gelten für alle Benutzer einer Datenbank. Die Konfiguration hierfür wird in den * Einstellungen* vorgenommen.

! Zusätzlich zu persönlichen und globalen Einstellungen werden, im Gegensatz zu Berechtigungen, Einstellungen nicht über Rollen, sondern über Organisationseinheiten

vergeben!

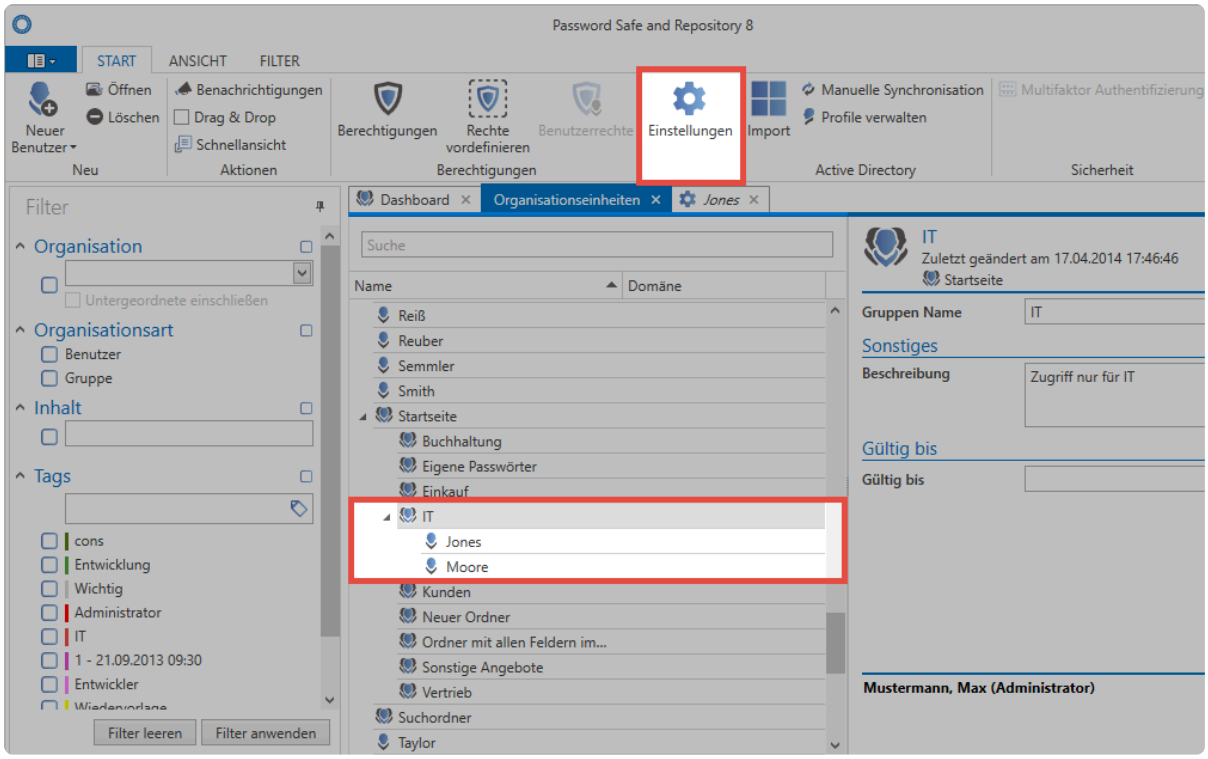


Vererbung von Benutzereinstellungen

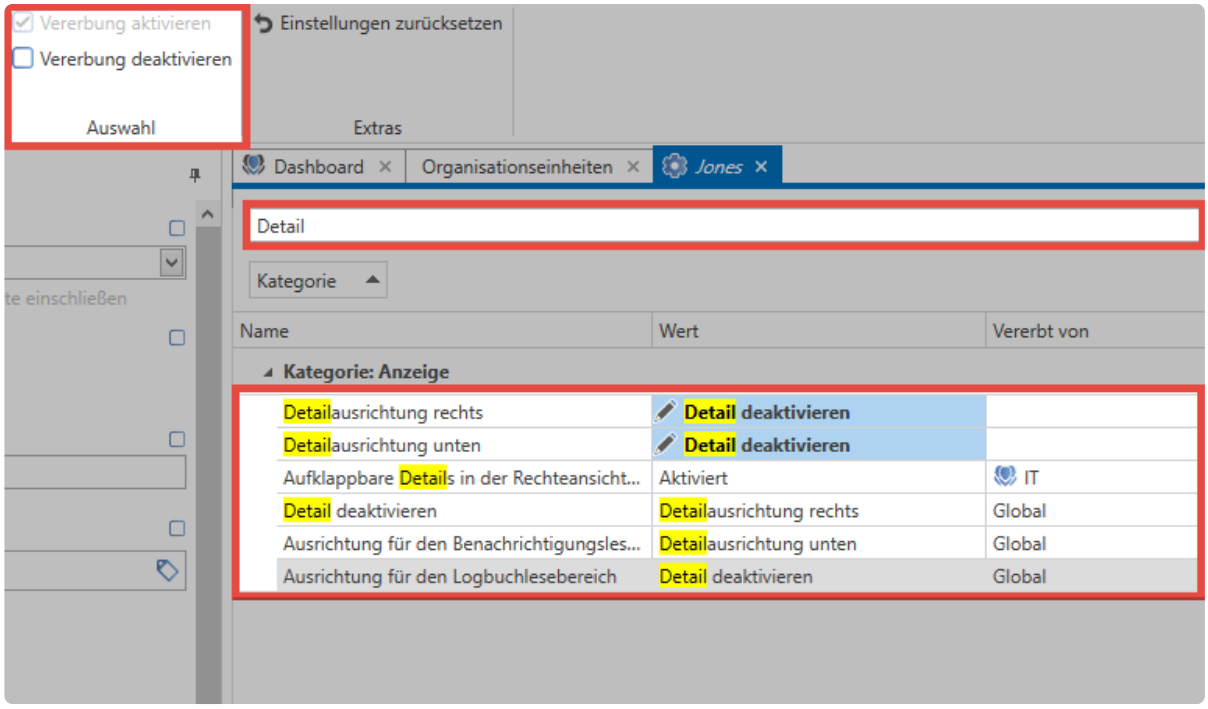
Lässt man die personenbezogenen Einstellungen außen vor, bleiben zwei Möglichkeiten zur Vererbung von Einstellungen:

1. globale Vererbung
2. Vererbung auf Basis von Mitgliedschaft in Organisationseinheiten (OU)

Globale Einstellungen konfigurieren Sie in den **Client Einstellungen**. 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** die Einstellungen aus der Organisationseinheit **IT**:



Über den Button **Einstellungen** in der Ribbon können Sie sowohl für Organisationseinheiten, als auch für Benutzer die Einstellungen einsehen. Die Vielzahl der Einstellungsmöglichkeiten können Sie durch die bekannten **Suchmechanismen** einschränken.

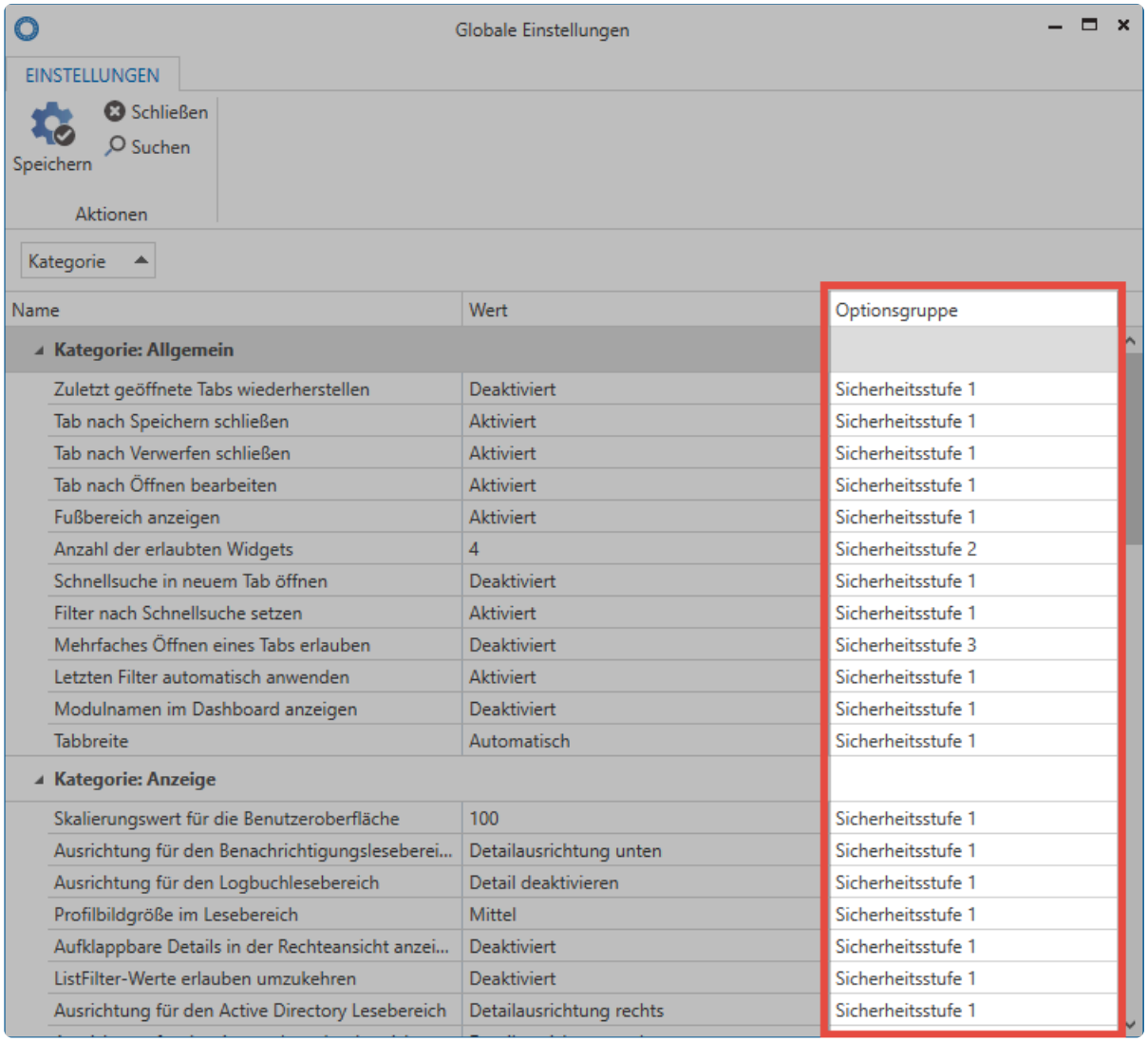


Hier sind die Benutzereinstellung des Users **Jones** zu sehen. Es wurde nach dem Suchbegriff **Detail** gefiltert. In der Spalte **Vererbt von** ist ersichtlich, dass einige Einstellungen global, bzw. von der Organisationseinheit **IT**, geerbt wurden. Die beiden obersten Optionen weisen keinen Wert in der Spalte auf. Diese Parameter wurden also nicht vererbt, sondern direkt auf Benutzerebene definiert.

In der Ribbon können Sie die Vererbung für einzelne Einstellungen gezielt deaktivieren.

Sicherheitsstufen

Über die **Sicherheitsstufen** können Sie festlegen, dass Benutzer nur **bestimmte Einstellungen** selbst beeinflussen können. Hierfür wird in den **globalen Einstellungen** eine Einteilung in Optionsgruppen vorgenommen. Den einzelnen Einstellungen weißen Sie hierfür eine Sicherheitsstufe von 1 bis 5 zu.



Welcher Benutzer Einstellungen aus welchen Sicherheitsstufen ändern darf, legen Sie in den **Benutzerrechten** fest. Dieses Recht definieren Sie wiederum über die globale Vererbung, über eine Rolle oder direkt beim Benutzer.

Übersicht aller Einstellungen

In diesem Kapitel werden alle vorhandenen Einstellungen aufgeführt. Wird eine Einstellung in einem anderen Kapitel weiter erläutert, so können Sie über den Link in der Spalte **Kapitel** direkt dorthin gelangen. Für eine bessere Übersicht werden die Einstellungen hier nach Kategorien gruppiert.

Kategorie: Allgemein	**Kapitel**	**neu**
Anzahl der erlaubten Widgets	Dashboard & Widgets	
Benachrichtigungen beim Öffnen als gelesen markieren		
Kann nach Updates suchen		
Mehrfaches Öffnen eines Tabs erlauben		
Modulname in Dashboard anzeigen	Dashboard & Widgets	
Schnellsuche in neuem Tab öffnen		
Tab nach Öffnen bearbeiten		
Tab nach Speichern schließen		
Tab nach Verwerfen schließen		
Tabbreite		
Zuletzt geöffnete Tabs wiederherstellen		
Nach Favicon-Download fragen		
Kategorie: Anzeige	**Kapitel**	**neu**
Anpassbarer Fenstertitel		
Aufklappbare Details in der Berechtigungenansicht anzeigen		
Listen beim Verbreitern in Tabellenansicht umschalten		
Pfad der Organisationssturktur im Header anzeigen		
Skalierungswert für die Benutzeroberfläche		
Darstellung der Passwörter im LightClient		
Darstellung der Passwörter im Vollclient		
Logo-Ansicht bei MouseOver im LightClient umschalten		
Kategorie: Browser	**Kapitel**	**neu**
Standardbrowser		
Kategorie: Dashboard	**Kapitel**	**neu**
Dashboard beim Start anzeigen	Dashboard & Widgets	
Restanzahl der Daten im Widget anzeigen		

Kategorie: Datensatz	Kapitel	neu
Anzahl der initial geladenen Datensätze		
Datensätze als “bald ablaufend” anzeigen, wenn deren Resttage kleiner sind als		
Formularänderungen auf Passwörter anwenden		
Gesamtzahl der Filterergebnisse anzeigen		
Maximale Anzahl der Suchergebnisse bei **Alle**		
Kategorie: Desktop Benachrichtigungen	**Kapitel**	**neu**
Bei externen Links		
Bei konfigurierten Links		
Beim Anzeigen von Zusammenfassungen		
Beim automatischen Login		
Beim Discovery Service		
Beim Erzeugen von Berichten		
Beim Export		
Beim Importieren		
Beim Kopieren in die Zwischenablage		
Beim Minimieren		
Beim Modifizieren von Datensätzen		
Beim Nachladen des Icons für Favoriten		
Beim Prüfen der Anmeldedaten		
Beim Synchronisieren		
Beim Transfer von Dokumenten		
Kategorie: Dokumente	**Kapitel**	**neu**
Dokumentenhistorie		
Erlaubte Dokumenterweiterungen		
Maximale Größe in MB		
Kategorie: Drucken	**Kapitel**	**neu**
Schriftgröße		
Kategorie: Echtzeitaktualisierung	**Kapitel**	**neu**
Benachrichtigungen in Echtzeit aktualisieren		

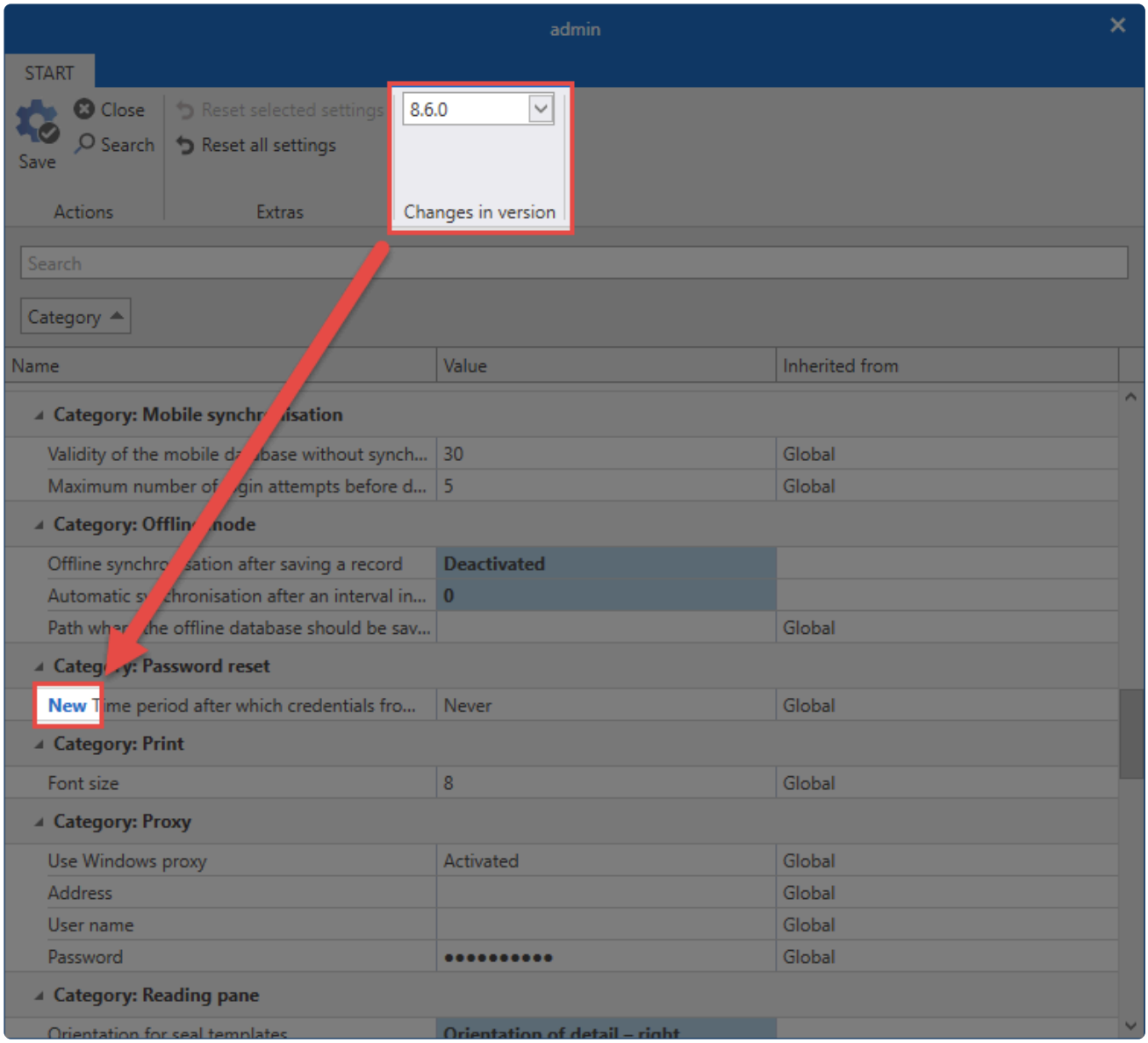
Kategorie: Filter	Kapitel	neu
Anzeigemodus	Anzeigemodus	
Auf Filter springen bei Schnellsuche	Anzeigemodus	
Kann Filter-Negierung verwenden	Erweiterte Filtereinstellungen	
Letzten Filter automatisch anwenden	Anzeigemodus	
Zustand des Anzeigemodus beim Programmstart	Anzeigemodus	
Kategorie: Fußbereich	**Kapitel**	**neu**
Benachrichtigungen im Fußbereich anzeigen	Lesebereich	
Dokumente im Fußbereich anzeigen	Lesebereich	
Fußbereich anzeigen	Lesebereich	
Historie im Fußbereich anzeigen	Lesebereich	
Logbuch im Fußbereich anzeigen	Lesebereich	
Metadaten im Fußbereich anzeigen	Lesebereich	
Password Resets im Fußbereich anzeigen	Lesebereich	
Kategorie: Konfiguration	**Kapitel**	**neu**
Animation im SSO-Konfigurationsfenster anzeigen		
Muss Grund für RDP-Verbindungsaufbau angeben	Bedienung & Aufbau	
Muss Grund für SSH-Verbindungsaufbau angeben		
Password Safe Benutzerverzeichnis		
Standard-Formular		
LightClient beim nächsten Login starten		
Untergeordnete Organisationseinheiten in LightClient einschließen		
Standard-Organisationseinheit		
Kategorie: Lesebereich	**Kapitel**	**neu**
Ausrichtung für Active Directory	Bedienung & Aufbau	
Ausrichtung für Anwendungen	Bedienung & Aufbau	
Ausrichtung für Benachrichtigungen	Bedienung & Aufbau	
Ausrichtung für Berichte	Bedienung & Aufbau	
Ausrichtung für Dokumente	Bedienung & Aufbau	
Ausrichtung für Formulare	Bedienung & Aufbau	

Ausrichtung für Logbuch	Bedienung & Aufbau	
Ausrichtung für Organisationsstruktur	Bedienung & Aufbau	
Ausrichtung für Password Reset	Bedienung & Aufbau	
Ausrichtung für Passwörter	Bedienung & Aufbau	
Ausrichtung für Richtlinie	Bedienung & Aufbau	
Ausrichtung für Rollen	Bedienung & Aufbau	
Ausrichtung für Siegelvorlagen	Bedienung & Aufbau	
Ausrichtung für System Tasks	Bedienung & Aufbau	
Ausrichtung für Weiterleitungsregeln	Bedienung & Aufbau	
Profilbildgröße im Lesebereich	Bedienung & Aufbau	
Kategorie: Mobile Synchronisation	**Kapitel**	**neu**
Gültigkeit der mobilen Datenbank ohne Synchronisation in Tagen (0 = keine Gültigkeitsbegrenzung)	Mobile Geräte	
Maximale Anzahl an Loginversuchen vor dem Löschen der Datenbank (0 = unbegrenzt)	Mobile Geräte	
Kategorie: Offline Modus	**Kapitel**	**neu**
Automatische Synchronisation nach Intervall in Minuten (0 für Deaktiviert)	Einrichten und Synchronisieren	
Offline Synchronisation nach dem Speichern eines Datensatzes	Einrichten und Synchronisieren	
Pfad, an dem die Offline-Datenbank abgelegt werden soll (Leer für Standard)	Einrichten und Synchronisieren	
Offline-Synchronisation nach dem Login		
Kategorie: Proxy	**Kapitel**	**neu**
Adresse		
Benutzername		
Passwort		
Windows-Proxy verwenden		
Kategorie: Rechte	**Kapitel**	**neu**
Benutzerfeld nach Hinzufügen leeren		
Berechtigungen vererben auf neue Objekte (ohne Rechtevorlage)	Vererbung aus Organisationsstrukturen	
Berechtigungesänderungen von Organisationseinheiten auf	Vererbung aus	

bestehende Passwörter vererben	Organisationsstruktur	
Berechtigungssuche: Schrittweise hinzufügen		
Ersteller aus den Berechtigungen bei neuen Objekten entfernen, wenn der erstellende Benutzer über eine Rolle berechtigt wird		
Gelöschte Benutzer und Rollen in Berechtigungen ausblenden		
Kategorie: Sicherheit	**Kapitel**	**neu**
Änderungsrichtlinie des Benutzerpassworts		
Datenbankverbindung trennen bei Inaktivität nach		
Deaktivierung inaktiver Benutzer		
Echtheitsbestätigung beim Login		
Gültigkeitsdauer eines Multifaktorauthentifizierungs-Tokens (Minuten)		
Mindestpunktzahl für Passwort Qualitätsstufe “Gut”		
Mindestpunktzahl für Passwort Qualitätsstufe “Stark”		
Passwort in Schnellansicht anziegen		
PKI: Zertifikat-Gültigkeit erzwingen		
PKI: Zertifikat-Hash-Methode		
PKI: Zertifikatketten-Prüfmodus		
Zeitspanne, nach der inaktive Sitzungen vom Server gelöscht werden		
Kategorie: Authentifizierung	**Kapitel**	**neu**
Benötigt zweiten Faktor		
Ersten Faktor bearbeiten		
Kategorie: SSO	**Kapitel**	**neu**
Browser Addons: Exakte Domainprüfung	Addons	
Browser Addons: Loginmaske automatisch absenden	Addons	
Browser Addons: Loginmaske automatisch befüllen	Addons	
Browser Addons: Passwort anzeigen		
Kategorie: Tastaturkürzel	**Kapitel**	**neu**
Skript ausführen, um das Passwort in das ausgewählte Fenster einzutragen		
Skript ausführen, um den Benutzernamen in das ausgewählte Fenster einzutragen		
Skript ausführen, um den Benutzernamen und das Passwort in das		

ausgewählte Fenster einzutragen		
Skript ausführen, um den Benutzernamen und das Passwort mittels Eingabetaste in das ausgewählte Fenster einzutragen		
Kategorie: Zwischenablage	**Kapitel**	**neu**
Bereinigung der Zwischenablage		
Zwischenablage beim Beenden löschen		
Zwischenablage beim Minimieren löschen		
Zwischenablage-Galerie		
Zwischenablage-Historie von Windows umgehen (Windows 10 Version 1809 und später)		

In den Einstellungen gibt es eine Versions-Auswahlbox. Die in der ausgewählten Version neu hinzugefügten Optionen werden der Liste entsprechend markiert. Sie können so nach einem Update alle neuen Einstellung direkt auffinden.



Abspeichern in die Windows-Zwischenablage-Historie vermeiden

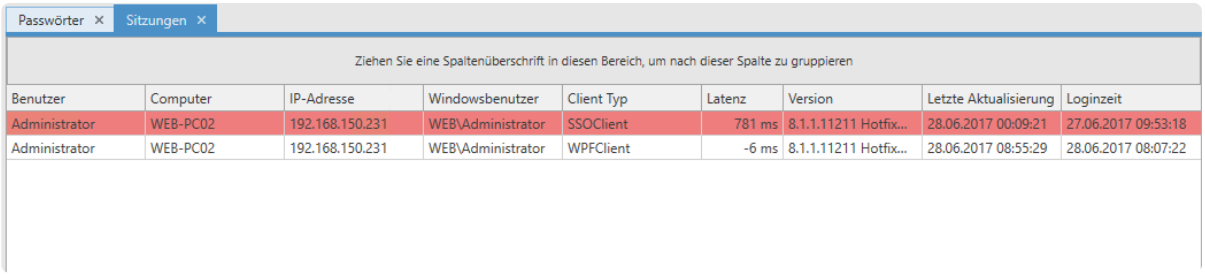
Mit der Option **Zwischenablage-Historie von Windows umgehen (Windows 10 Version 1809 und später)** können Sie verhindern, dass die kopierten Werte in der Zwischenablagen-Historie von Windows erscheinen.

> Von dieser Einstellung sind nur diejenigen Werte betroffen, welche Sie direkt über den Client kopieren. Beispielsweise wenn Sie ein Passwort über die Ribbon kopieren. Die Option hat keine Auswirkung, wenn das Passwort aufgedeckt und mittels STRG + C kopiert wird.

Administration

Sitzungen

Über den Menüpunkt **Sitzungen** werden alle Benutzer angezeigt, welche aktuell mit der Datenbank verbunden sind. Diese Seite hat einen rein informativen Charakter, Sie können hier keine Konfigurationen vornehmen.



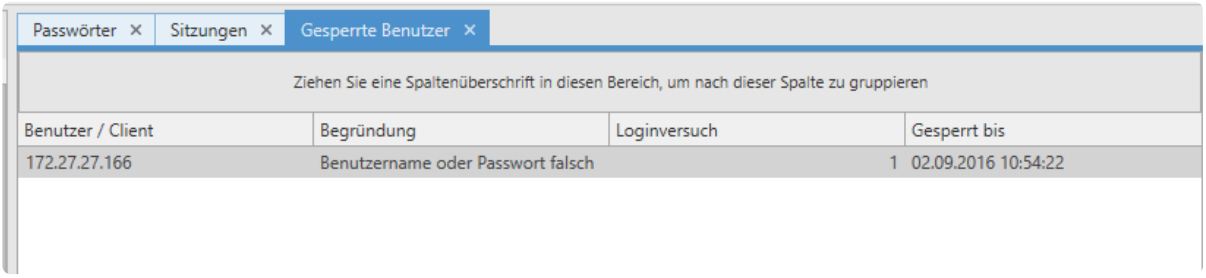
Die Sitzungsansicht startet in einem separaten Tab in dem derzeit aktiven Modul.

Gesperrte Benutzer

Rufen Sie alle derzeit gesperrten Benutzer ab. Es gibt hierfür zwei Szenarien:

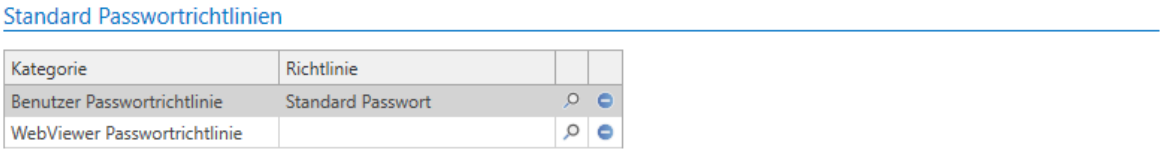
1. **Benutzername korrekt, Passwort falsch**: Der Benutzername wird angezeigt.
2. **Benutzername falsch**: Der Client wird angezeigt.

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 definieren Sie **Passwortrichtlinien**, welche dann eingehalten werden müssen. Im folgenden Fall muss ein Benutzerpasswort mindestens der Richtlinie “Standard Passwort” entsprechen, um valide zu sein.



Relevantes Recht

Um Die **Passwortrichtlinien** für genannte Passwörter zu definieren, existiert ein separate Option.

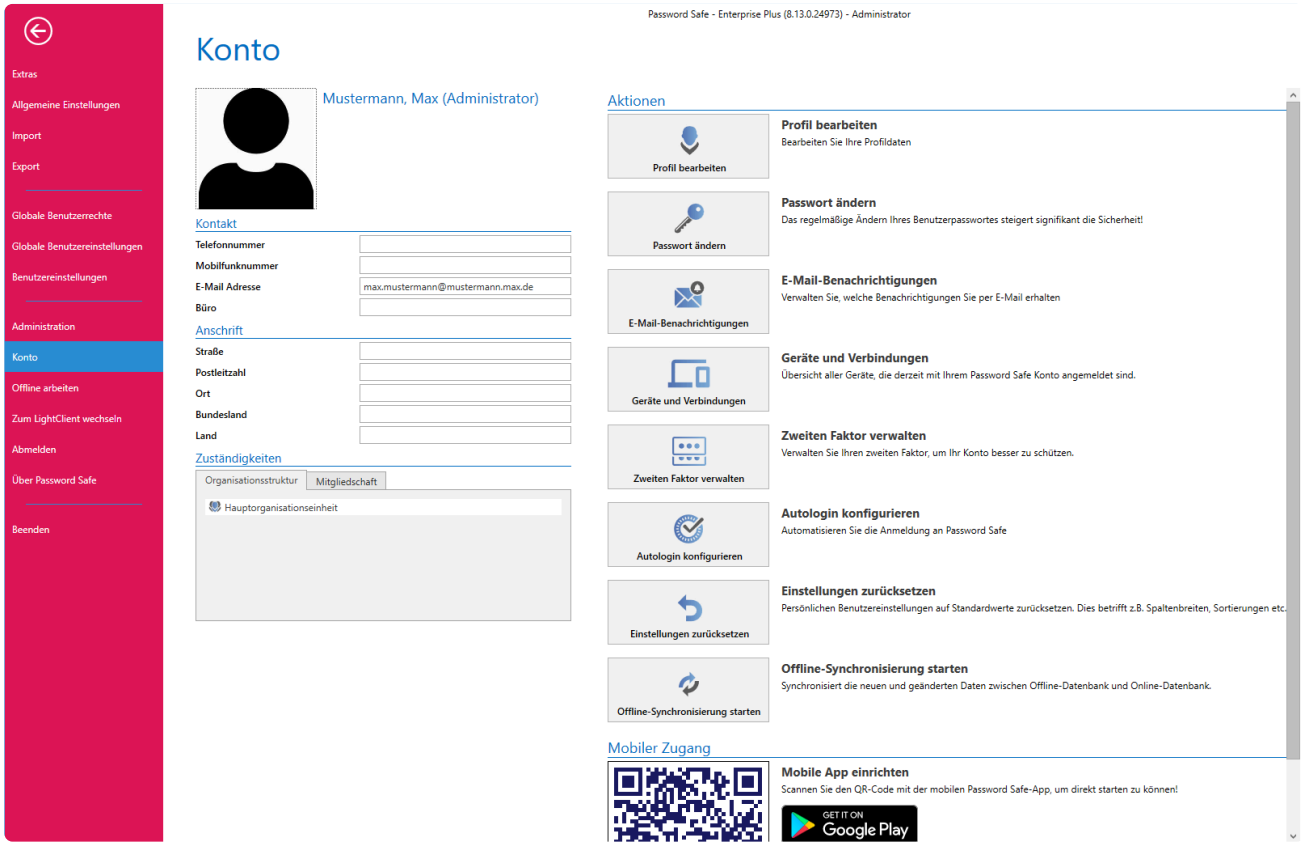
Benutzerrecht

- Kann Standard-Passwortrichtlinien konfigurieren

Konto

Was ist das Konto?

Im Konto können Sie die Konfiguration benutzerspezifischer Information einsehen und Änderungen vornehmen.



Profil bearbeiten

Alle in den Rubriken “Kontakt” und “Anschrift” geführten Informationen definieren Sie unter **Profil bearbeiten**. Manche Bereiche des Profils überschneiden sich thematisch mit der **Benutzerverwaltung**. Diese Informationen sind in einem **separaten Kapitel** erläutert.

Passwort ändern

Es wird empfohlen, regelmäßig das Benutzerpasswort zu ändern. Geben Sie das bisherige Passwort ein, um ein neues Passwort nutzen zu können. Die Stärke des Passwortes wird direkt dargestellt.

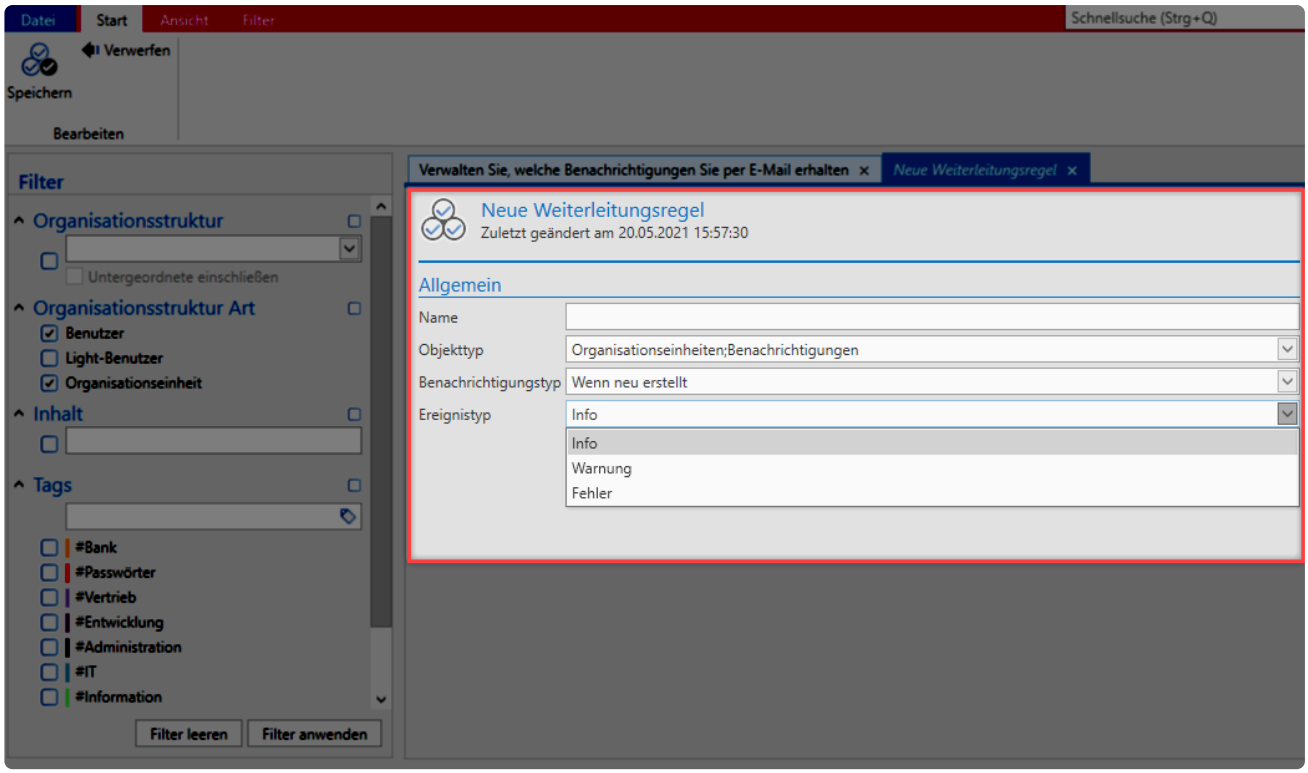
> Benutzer, welche mit Hilfe des Master Key Modus aus dem AD importiert wurden, melden sich mit dem Domänenkennwort an. Daher kann hier kein Passwort konfiguriert werden.

Die Stärke des Benutzerpasswortes kann durch die Administration durch die Vorgabe von **Passwortrichtlinie** vorgegeben werden.

Wenn ein Benutzer sein Passwort ändert, werden alle noch offenen Sessions automatisch beendet.

E-Mail-Benachrichtigungen

Hier können Sie Weiterleitungsregeln definieren. Eine Regel bestimmt, wann eine Benachrichtigung an das E-Mail-Postfach des angemeldeten Benutzers weitergeleitet werden soll.

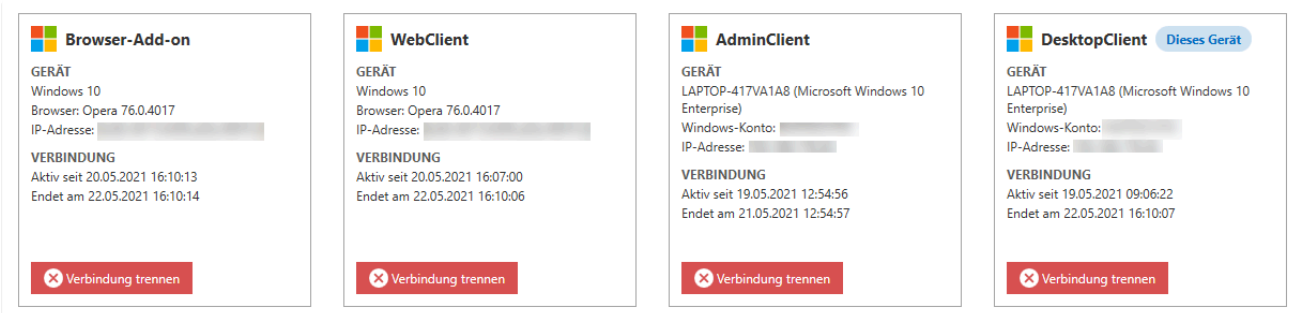


Im vorliegenden Fall werden alle Benachrichtigungen weitergeleitet, die dem genannten Objekttyp (Organisationseinheiten, Benachrichtigungen) sowie dem Benachrichtigungstyp (Wenn neu erstellt) entsprechen. Zusätzlich kann noch nach dem Nachrichtentyp (=Ereignistyp) gefiltert werden.

Voraussetzung für eine Weiterleitung ist, dass für den angemeldeten Benutzer eine E-Mail Adresse hinterlegt ist.

Geräte und Verbindungen

Sie können sich hier alle aktiven Sitzungen des angemeldeten Benutzer anzeigen lassen.



Zweiter Faktor verwalten

Die **Multifaktor Authentifizierung** bietet zusätzlichen Schutz durch einen zweiten Sicherheitsfaktor bei der Anmeldung.

Autologin konfigurieren

Über diese Option automatisieren Sie die Anmeldung an Password Safe. Zum Einrichten genügt es das Passwort zweimal einzugeben und zu speichern.

> ✻ Der Autologin wird an die Hardware gebunden und funktioniert somit nicht auf einem anderen Rechner. Ändert sich die Hardware bzw. Hardware Ids, so müssen Sie einen bestehenden Autologin neu erstellen.

Relevantes Recht

Option um den Autologin zu verwalten

Benutzerrecht

- Kann Autologin verwalten

> ! Die automatische Anmeldung ist als *sicherheitskritisch *einzustufen. Bedenken Sie hierbei, dass dadurch auf alle Daten zugegriffen werden kann, wenn beispielsweise vergessen wurde den Rechner zu sperren.

> ✻ **Aus Sicherheitsgründen ist ein eingerichteter Autologin nur für 180 Tage gültig. Sie müssen diesen nach Ablauf der Frist erneut einrichten.**

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

Starten Sie die **Offline** manuell, falls Sie Änderungen am Datenbestand unmittelbar nach der Änderung einsehen möchten. Die Synchronisation läuft hierbei im Hintergrund und wird über einen Statusbalken im Footer sowie im Icon dargestellt.

Benutzerbild bearbeiten

Durch Klicken auf das Profilbild fügen Sie ein neues Bild hinz oder ersetzen bzw. löschen ein vorhandenes.

> Bei Benutzern, welche im Master Key Modus aus dem AD importiert wurden, können keine Änderungen vorgenommen werden. Alle Informationen inkl. Profilbilder werden hier aus dem AD übernommen.

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 des Passworts, durchgeführt werden. Im Zusammenspiel mit dem Sichtschutz kann das ein wertvolles Werkzeug sein. Sie legen über das Berechtigungskonzept fest, welche Benutzer einen Zugang nutzen. 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 von Usern dann (ausreichend Berechtigungen vorausgesetzt) verwendet. Eine separate Installation ist demnach nicht nötig. Es wird sowohl für den Client wie auch für den SSO Agent eine eigene Desktop Verknüpfung erstellt.

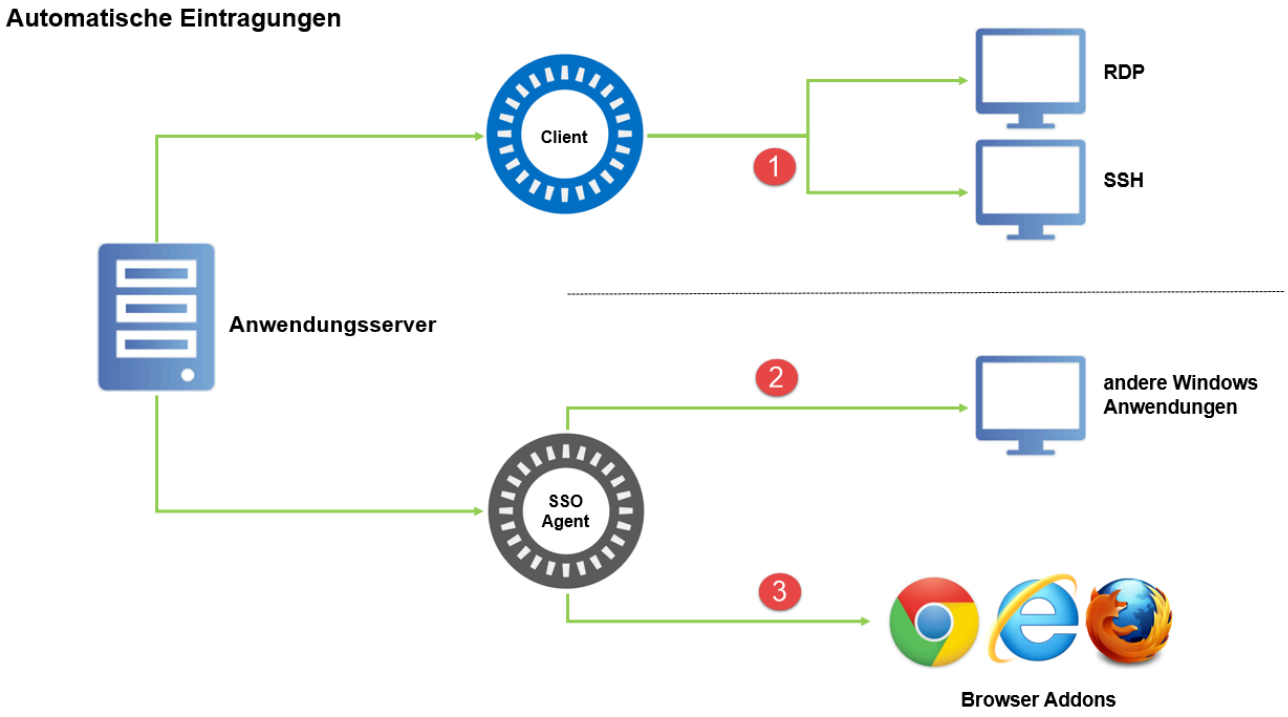
Benutzerrechte

Für das Erfassen von neuen Webanwendungen benötigen Sie das Recht **Kann Webanwendungen erfassen**.

> ✻ Der Agent kann mehrere Datenbanken gleichzeitig ansteuern.

Funktionsweise

Die Funktionsweise des SSO Agents wird im nachfolgendem Schaubild erläutert.



Das automatisierte Starten von RDP- und SSH-Sessions (1) starten Sie nicht über den SSO Agent. Hierfür erstellen Sie Anwendungen im Password Safe Client. Die Erstellung und Nutzung dieser Verbindungen wird im entsprechenden 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 haben Sie die Möglichkeit auch andere Windows Anwendungen zu automatisieren (2). Ein wesentlicher Unterschied ist, dass Sie die beiden genannten Verbindungen innerhalb eines separaten Tabs “embedded” errichten. Andere Anwendungen, wie z.B. VMware, werden wie gewohnt direkt gestartet. Mehr zu diesem Thema finden Sie in einem separaten Kapitel. 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 automatisch vornehmen. Das bedeutet, dass Sie über die Addons die gewünschte Anmeldung einmal konfigurieren und zukünftig effizient nutzen. Der SSO Agent bildet hierbei die **Schnittstelle** (3) zwischen dem Anwendungsserver und den verfügbaren Browser Addons (Google Chrome, Edge und Mozilla Firefox).

Zur Eintragung in Webseiten muss der Datensatz mindestens folgende Felder haben: **Benutzername**, **Passwort**, **URL**.

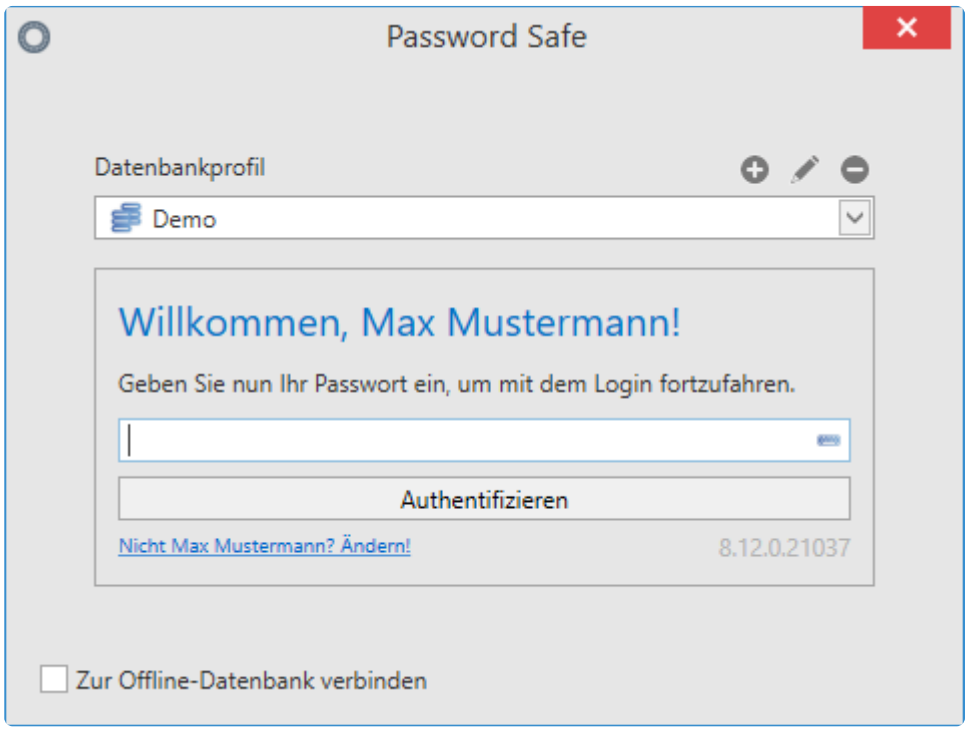
Fazit

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 eine schlanke Alternative für die Nutzung des Clients mit den beiden angesprochenen Einschränkungen. Selbstverständlich sind 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, können Sie den SSO Agent direkt starten. Die Anmeldedaten entsprechen den regulären Benutzerdaten des Clients.



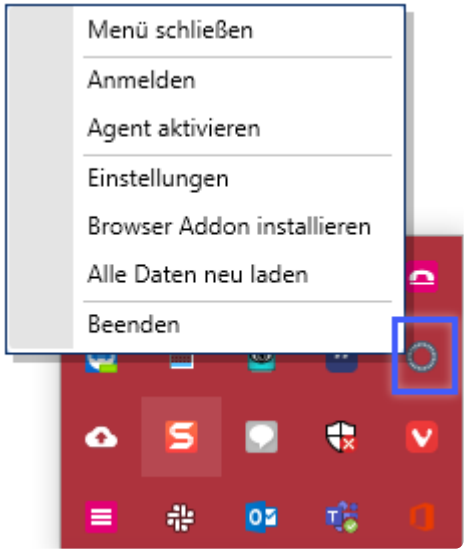
Wählen Sie zur Anmeldung zunächst die gewünschte Datenbank sowie die zugehörigen Anmeldedaten aus. Der SSO Agent stellt alle am Client konfigurierten Datenbanken zur Verfügung. Auch die Erstellung von Profilen ist wie gewohnt möglich, um die Verbindungsdaten zu bestimmten Datenbanken zukünftig effizient zu nutzen.

> 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 Sie somit auch über den SSO Agent erstellen.

> Um die Eintragung auf Webseiten zu gewährleisten wird folgendes benötigt: **Benutzername**, **Passwort**, **URL**.

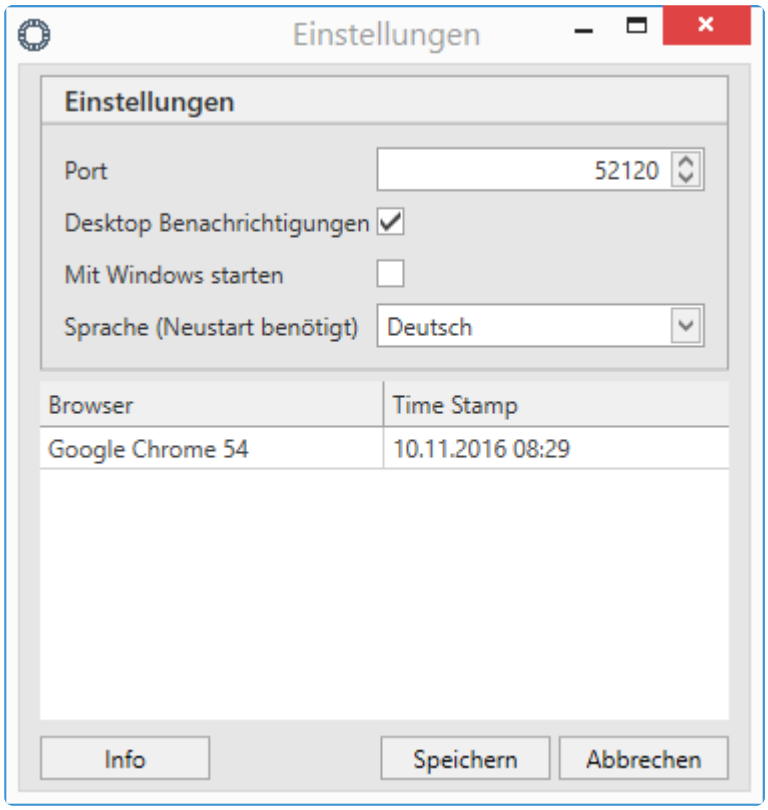
Funktionen über das Kontextmenü

Nach der erfolgreichen Anmeldung läuft der SSO Agent vorerst im Hintergrund. Ein Kontextmenü öffnen Sie über einen Rechtsklick auf das Icon im System-Tray.



- **Menü schließen**: Das Menü wird geschlossen und muss wieder über die System Tray geöffnet werden.
- **Anmelden**: ermöglicht die Anmeldung an einer weiteren Datenbank.
- **Agent deaktivieren / aktivieren**: bietet die Möglichkeit, die automatische Eintragung temporär abzuschalten.
- Über die **Einstellungen** definieren Sie diverse Variablen.
- **Browser Addon installieren**: startet die Installation des Google Chrome oder Mozilla Firefox Addons.
- **Alle Daten neu laden**: alle möglichen Änderung werden aktualisiert.
- **Mit Addon verbinden**: ermöglicht die Kopplung von Addon und Agent (steht nur im Terminalserver Betrieb zur Verfügung).

Einstellungen



- Den **Port** zur Verbindung mit der Datenbank müssen Sie in der Regel nicht ändern. Sollte er anderweitig belegt sein, können Sie ihn hier neu definieren. Passen Sie den Port hier an, müssen Sie ihn im Addon ebenso ändern.
- Im Terminalserver Betrieb definieren Sie über **Terminal Server Ports** eine Range, aus welcher sich der Terminalserver zur Verbindung bedient. Der Standard ist hier 1000. Hier ist in der Regel keine Anpassung nötig. Ebenso können Sie im Terminalserver Betrieb die sogenannte **Terminal Server Kennung** auslesen. Es handelt sich hier um eine einzigartige ID, welche den Agent am Addon einwandfrei ausweist. Geben Sie die Kennung bei der ersten Verbindung im Addon an.
- 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

Stellen Sie vor dem Pairing sicher, dass das gewünschte Addon installiert ist. Weiterhin muss der Terminalserver Dienst installiert sein. Dieser wird zusammen mit dem Client installiert.

Pairing

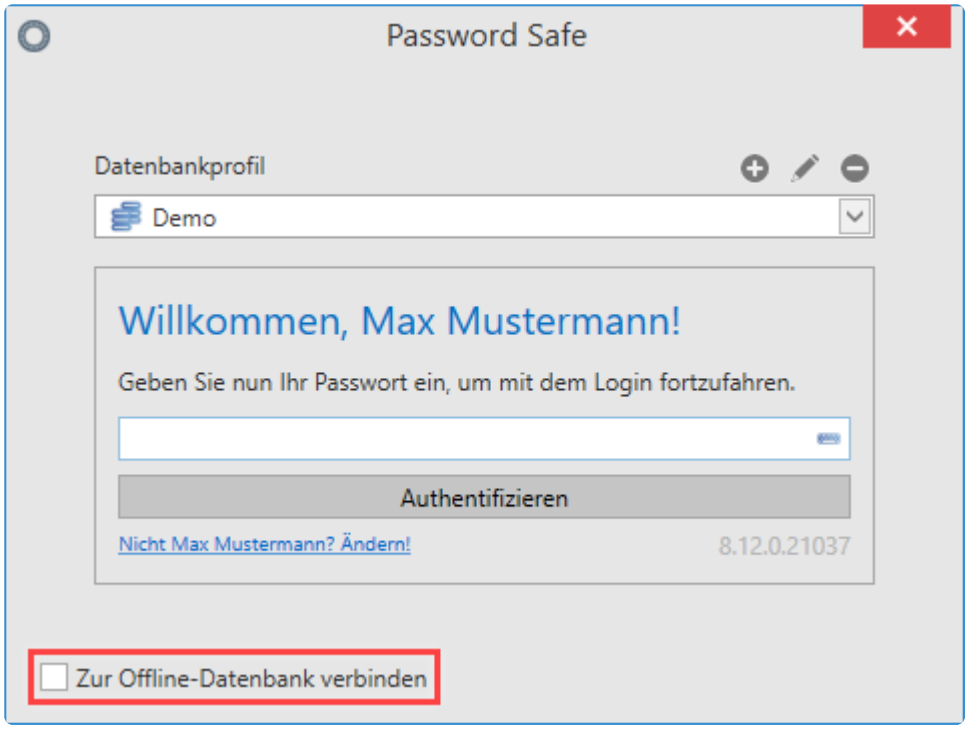
Zunächst klicken Sie am Agent im Kontextmenü auf den Punkt **Mit Addon verbinden**. Im nächsten Fenster wählen Sie dann den gewünschten Browser aus, welcher sich daraufhin öffnet.
Nun erscheinen die Einstellungen des Addons. Hier ist in der Regel bereits die Terminalserver Kennung eingetragen. Sie müssen diese nur noch bestätigen.

Ändern des Ports

Sollte es nötig sein, den Port zu ändern, so melden Sie sich zunächst am **SSO Agent** an. Ändern Sie in den **Einstellungen** nun den Port und speichern Sie diesen Vorgang. Nun wird der **SSO Agent** beendet. Um die Änderungen für den Dienst zu übernehmen, wird nun der Windows Dienst **Password Safe V8 Terminal SSO Service** neu gestartet. Starten Sie nun den*SSO Agent* neu. Ändern Sie abschließend den Port im gewünschten **Browser Addon**.

Zusammenspiel mit Offline Datenbanken

Der SSO Agent kann auch Verbindungen zu Offline Datenbanken herstellen. Beim Login verbinden Sie direkt auf die Offline Datenbank, sofern eine existiert. Besteht keine Serververbindung, wird direkt das Verbinden zur Offline Datenbank vorgeschlagen.


Password Safe
Datenbankprofil
Demo
Willkommen, Max Mustermann!
Geben Sie nun Ihr Passwort ein, um mit dem Login fortzufahren.
Authentifizieren
Nicht Max Mustermann? Ändern!
8.12.0.21037
Zur Offline-Datenbank verbinden

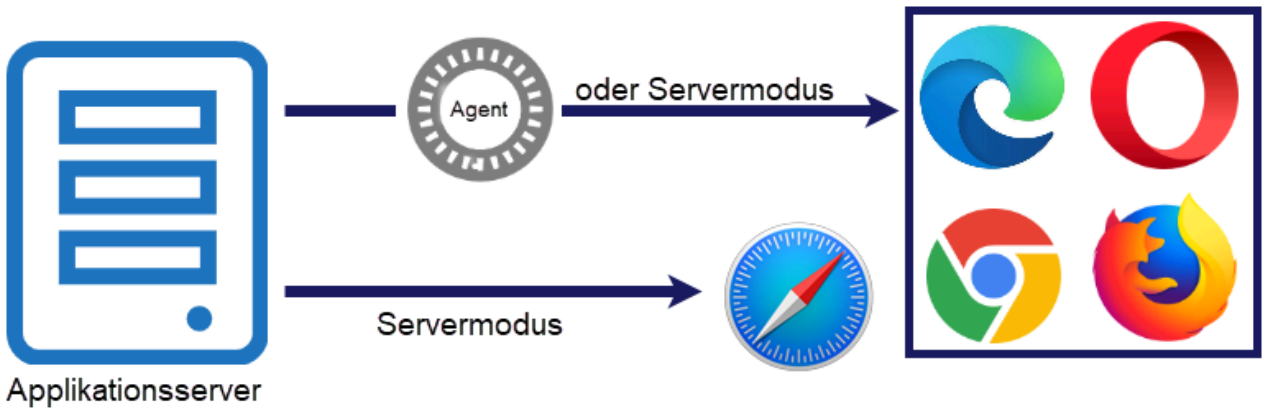
Browser-Erweiterungen

Was versteht man unter Browser-Erweiterungen?

Über Browser-Erweiterungen können Passwörter auch im Browser verwendet werden. Sie können in der Browser-Erweiterung nach Passwörtern suchen, sie in die Zwischenablage übernehmen oder automatisch in die Eingabemaske der Webseite eintragen lassen. Für die automatische Eintragung sind unter Umständen Anwendungen nötig.

Um die Daten über die Browser-Erweiterung bereitstellen zu können, wird eine Verbindung zur Datenbank benötigt. Die Verbindung kann entweder über den **SSO Agent** oder direkt im **Server-Modus** erfolgen.

Aktuell sind Browser-Erweiterungen für folgende Browser verfügbar: **Microsoft Edge**, **Google Chrome**, **Mozilla Firefox** und **Safari**.



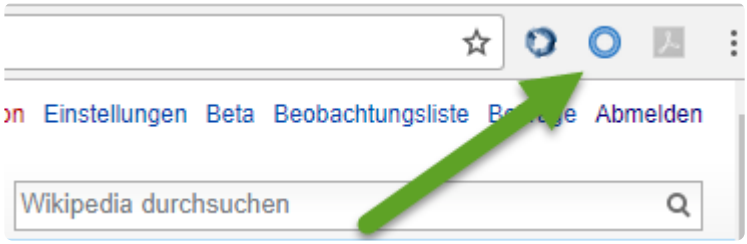
Installation

Die Installation der Browser-Erweiterungen wird im Kapitel Installation Browser-Erweiterungen beschrieben.

Bitte beachte, dass die Browserversion aktuell gehalten wird.

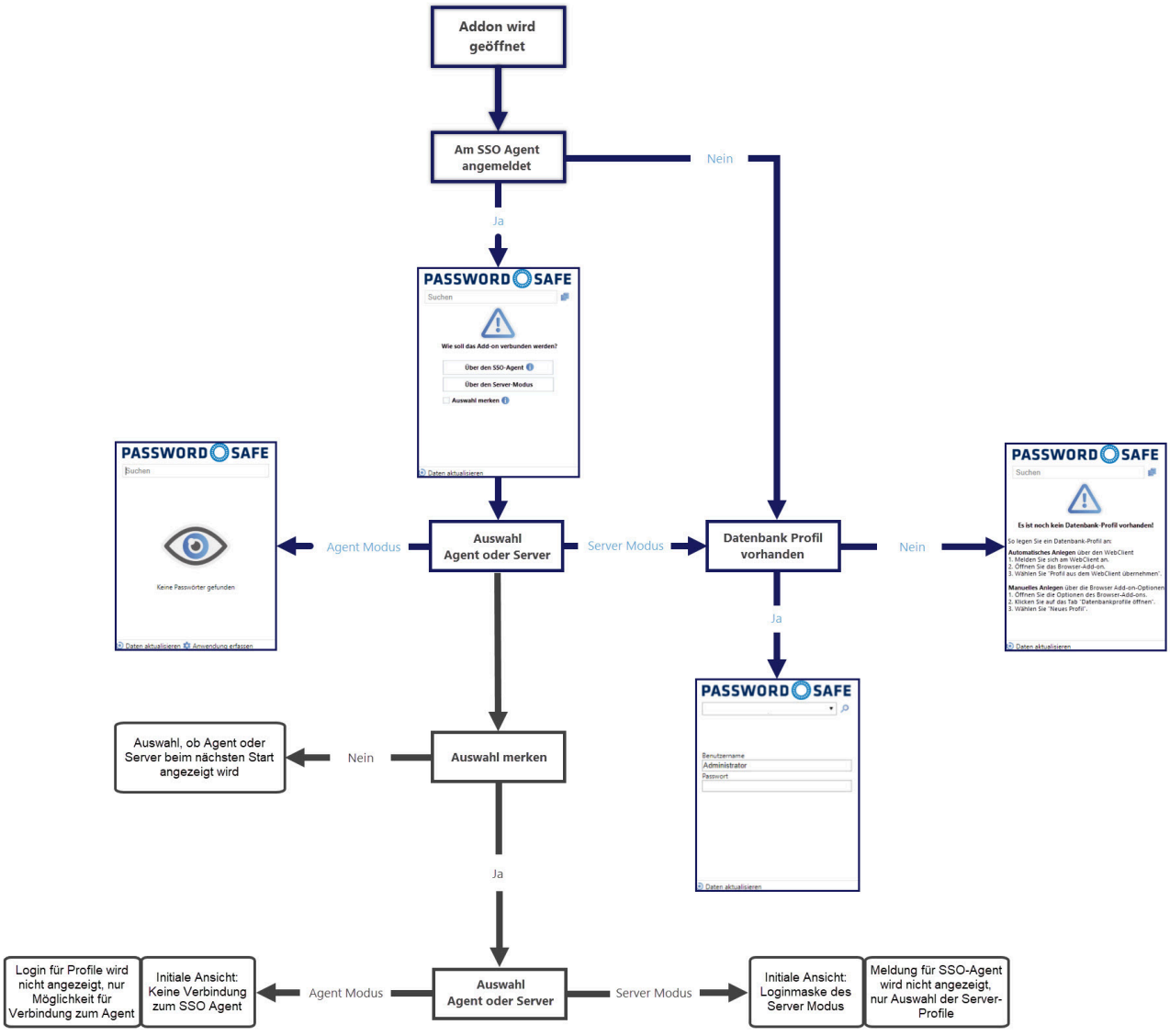
Verbindung mit dem SSO-Agent oder Server-Modus

Ist der Punkt Installation der Browser-Erweiterung abgeschlossen, öffnen Sie den gewünschten Browser. Es erscheint ein Fenster, in dem Sie die Sicherheit der Verbindung bestätigen müssen. Über einen einfachen Klick erfolgt das Pairing. Die Browser-Erweiterung ist ab diesem Zeitpunkt berechtigt, Daten vom SSO Agent abzufragen. Ab diesem Zeitpunkt ist dann im gewünschten Browser ein **neues Icon** sichtbar:

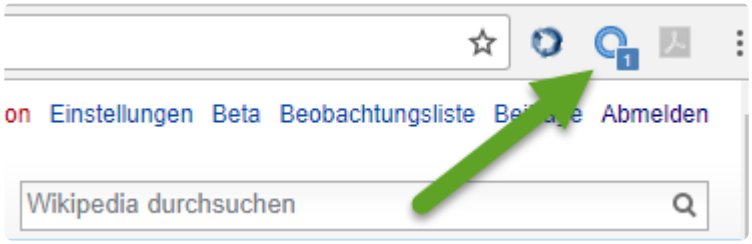


Wird das Icon in dieser Form dargestellt, bedeutet dies, dass die Erweiterung zwar installiert ist, jedoch aktuell noch keine Verbindung besteht. Diese Verbindung, ob zum SSO-Agent oder im Server-Modus, können Sie mit einem Klick auf die Erweiterung ermöglichen.

Im nachfolgenden Bild wird die genaue Vorgehensweise beim Verbinden genauer erläutert:



Nach erfolgreicher Verbindung wird am Icon die **Anzahl der Datensätze angezeigt, die für die aktuelle Internetseite verfügbar sind**.

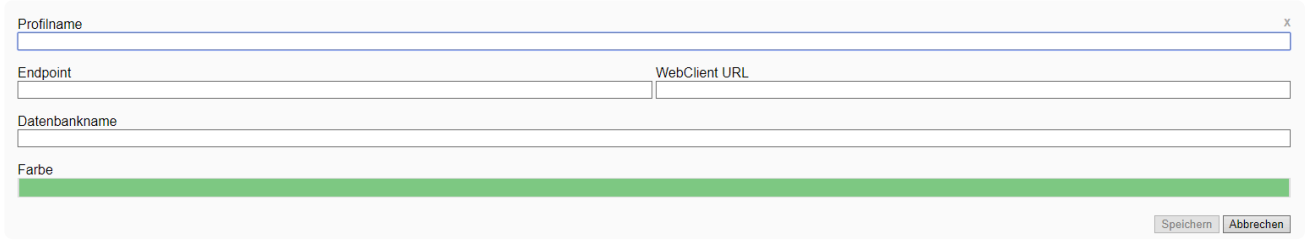


Eine tiefgestellte “0” bedeutet, dass eine Verbindung zur Datenbank besteht.

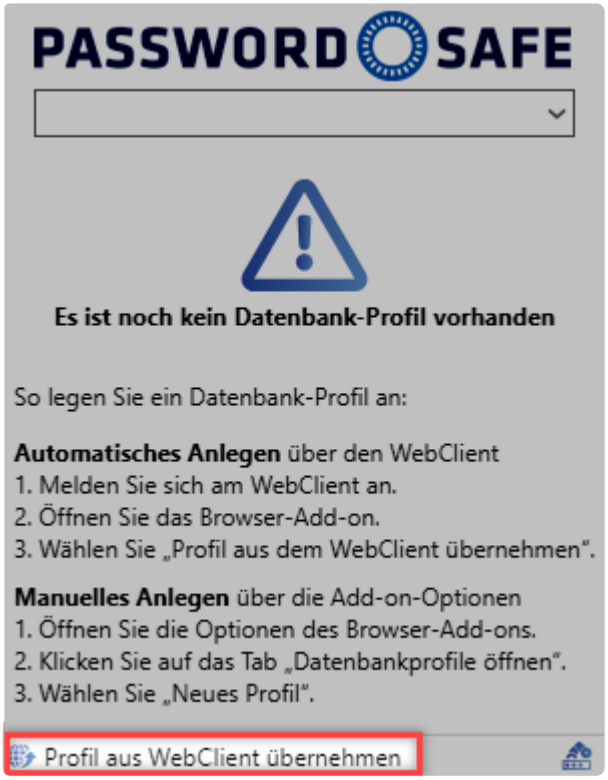
Datenbankprofile

Der Server-Modus muss wissen, mit welchem Datenbankprofil er verbunden ist. Es gibt zwei Möglichkeiten, ein Datenbankprofil einzurichten:

- Zum einen kann das Datenbankprofil manuell erstellt werden. Hierfür werden folgende Angaben benötigt: IP-Adresse, WebClient URL und Datenbankname. Beachten Sie, dass **/api** am Ende der IP-Adresse angehängt wird.



- Zum anderen besteht die Möglichkeit, das Ausfüllen des Datenbankprofils automatisch durchführen zu lassen. Dafür reicht es, sich mit dem WebClient an einer Datenbank anzumelden. Durch Klick auf die Erweiterung im WebClient wird dessen Profil übernommen. Dadurch werden alle nötigen Informationen wie Profilname, IP-Adresse, WebClient und Datenbankname übergeben.



> Das Kapitel WebClient beschreibt, wie Sie den Datenbanknamen und den Namen in die URL des WebClients überführen.

Vorteile des Server-Modus

Der Server-Modus bietet folgende Vorteile:

- im Terminalserverbetrieb wird kein Terminalserverdienst benötigt.
- Der SSO-Agent wird nicht mehr benötigt.

> SSO-Anwendungen sind nur nur mit dem SSO-Agent möglich. Im Server-Modus mit nicht gestartetem SSO-Agent funktionieren SSO-Anwendungen nicht!

Einstellungen

Alle Einstellungen, die die Browser-Erweiterungen betreffen, bearbeiten Sie zentral am Client. Über das System Benutzereinstellungen setzen Sie diese global, pro Organisationseinheit oder pro Benutzer. In der Kategorie **SSO** finden Sie folgende Optionen, die sich direkt auf die Browser-Erweiterungen auswirken:

- **Browser-Add-ons: Loginmasken automatisch absenden** sorgt dafür, dass nach dem Eintragen der Zugangsdaten direkt eine Anmeldung erfolgt. Es ist also kein manueller Klick nötig.
- Über **Browser-Add-ons: Loginmasken automatisch befüllen** wird erreicht, dass die Zugangsdaten ohne Rückfrage eingetragen werden, wenn eine Website erkannt wird.

Ebenso wirkt sich die Option **Standardbrowser** auf die Erweiterungen aus. Hier legen Sie fest, in welchem Browser die Websites aus dem Client heraus geöffnet werden.

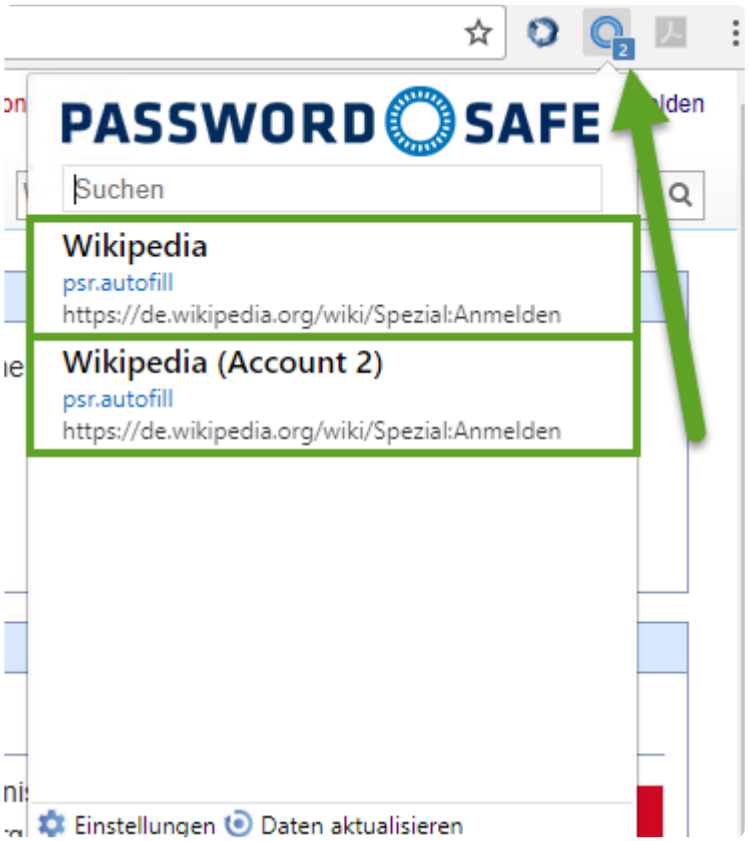
Die oben genannten Einstellungen können auch pro Datensatz gesetzt werden. Weiterführende Infos hierzu finden Sie in einem separaten Kapitel.

> Bitte beachten Sie: auch wenn die Einstellung „**Browser-Add-ons: Loginmaske automatisch absenden**“ **deaktiviert** wurde, wird die Anmeldemaske bei Datensätzen mit Sichtschutz **automatisch abgesendet**.

Arbeiten mit den Browser-Erweiterungen

> Ein Datensatz kann nur dann für Eintragungen genutzt werden, wenn dieser ein Formularfeld vom Typ “URL” besitzt.

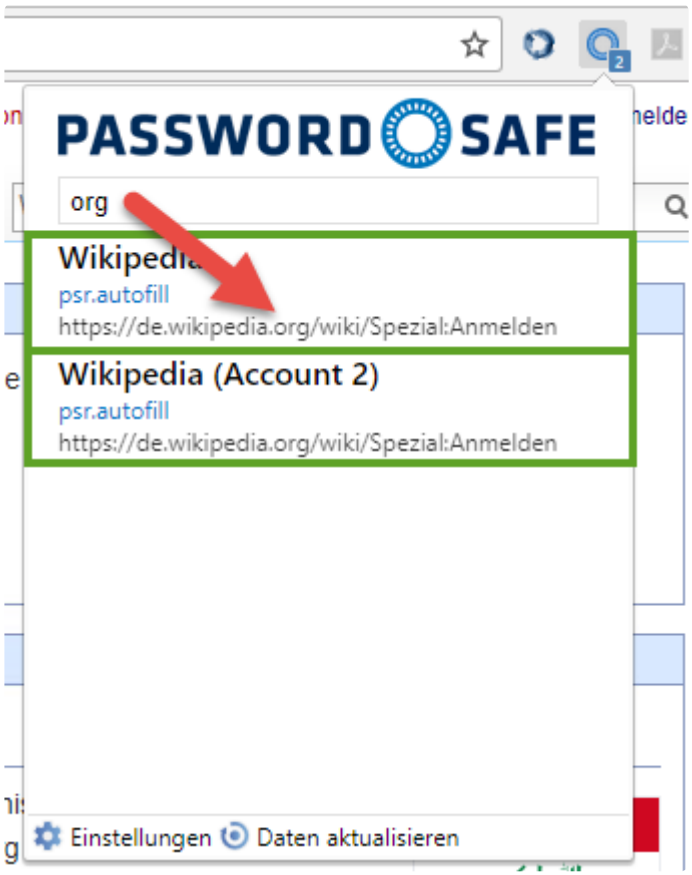
Die im vorherigen Kapitel erwähnte, tiefgestellte Zahl ist einerseits nur bei einer aktiven Anmeldung verfügbar, andererseits sagt diese bereits viel über die **Anzahl der möglichen Eintragungen** aus. Wenn hier z.B. eine “2” angezeigt wird, können Sie über das Icon direkt den Account auswählen, mit dem Sie sich anmelden möchten.



Voraussetzung war bisher immer, dass man manuell über den Browser genau zu der Website navigiert, welche man auch nutzen möchte. Diese Navigation kann auch durch Password Safe übernommen werden (siehe nachfolgendes Kapitel).

Suche und Navigation

Aktuell wurde immer davon ausgegangen, dass Sie manuell zu der Seite navigieren, für die er eine automatische Eintragung nutzen möchte. Diese Art zu arbeiten ist möglich, jedoch nicht ausreichend komfortabel. Die Browser-Erweiterung ist analog zur Vorgehensweise bei Lesezeichen nutzbar. Über das Suchfeld können Sie direkt auf Basis der Datensätze in der Datenbank suchen. Voraussetzung ist nach wie vor, dass der Datensatz eine URL besitzt.



Im Bild ist ebenso ersichtlich, dass neben dem Namen des Datensatzes (Wikipedia) die URL durchsucht wird. Die den Suchkriterien entsprechenden Treffer werden angezeigt und Sie können diese direkt über die Pfeiltasten oder die Maus selektieren. Die gewählte Internetseite wird in einem separaten Tab geöffnet.

Dargestellte Passwörter

Welche Passwörter zu einer erkannten Website dargestellt werden, hängt davon ab, wie der Datensatz bzw. die Datensätze konfiguriert sind. Hierfür definieren Sie pro Passwort, wie granular die URL überprüft wird. Weitere Infos dazu finden Sie im Kapitel **Passworteinstellungen**.

Ein **Beispiel** zur Veranschaulichung:

Für folgende Websites wird jeweils ein eigenes Passwort erstellt:

- www.passwordsafe.de
- help.passwordsafe.de
- license.passwordsafe.de

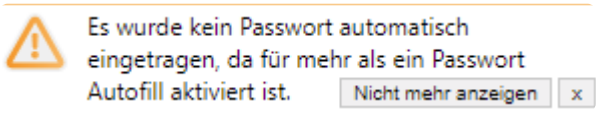
Die **Exakte Domainprüfung** wird bei allen drei Passwörtern deaktiviert:
Auf **www.passwordsafe.de** werden in der Browser-Erweiterungen auch die Passwörter der Subdomains angezeigt, also **www.passwordsafe.de**, **help.passwordsafe.de** und **license.passwordsafe.de**

Die **Exakte Domainprüfung** ist bei allen drei Passwörtern aktiviert:
Auf **www.passwordsafe.de** werden in der Browser-Erweiterung keine Passwörter von Subdomains angezeigt. Dargestellt wird also nur **www.passwordsafe.de**

Die **Exakte Domainprüfung** ist bei allen Passwörtern außer bei **license.passwordsafe.de** aktiviert:
Auf **www.passwordsafe.de** werden in der Browser-Erweiterung **www.passwordsafe.de** sowie **license.passwordsafe.de** angezeigt.

Mehrere Passwörter für eine Webseite

Falls Sie eine Seite ansteuern und mehrere Passwörter mit Autofill für diese Webseite in Frage kommen, wird nicht mehr, wie in den alten Versionen, ein Datensatz ausomatisch eingetragen. Stattdessen erscheint dann im Pop-up folgende Meldung:



Ist jedoch nur für ein Passwort Autofill aktiviert, aber mehrere Passwörter würden in Frage kommen, wird das Passwort eingetragen, das mit Autofill versehen ist.
Klicken Sie im Pop-up auf einen Datensatz, wird dieser (wie bisher auch) normal eingetragen.

Web Anwendungen

Was sind Anwendungen?

Viele Webseiten können ohne weitere Konfiguration befüllt werden. Auf den 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, müssen Sie manuell eine Anwendung erstellen. 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 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 dann 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.

Relevantes Recht

Sie benötigen folgende Optionen, um Web-Anwendungen anzulegen

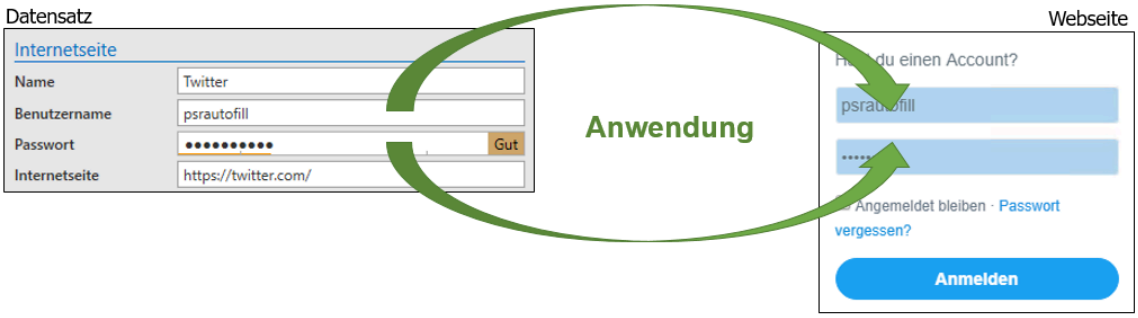
Benutzerrecht

- Kann neue Anwendungen vom Typ Web anlegen

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

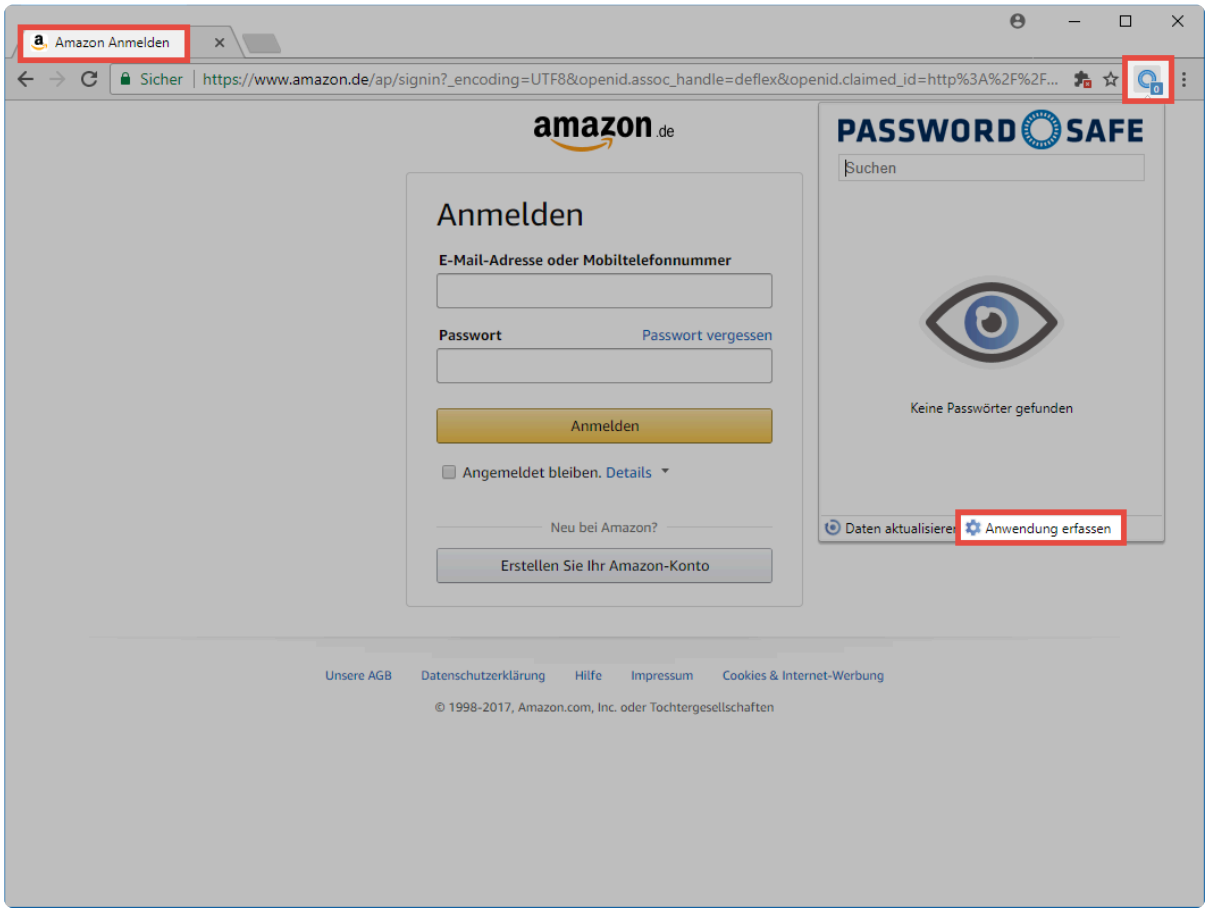
Zuweisung von Feldern aus dem Datensatz zu dem zugehörigen Feld auf der Webseite. Dieses Mapping muss nur einmal konfiguriert werden. Die Anwendung ist fortan für die Eintragung der Daten in die Felder der Webseite zuständig. Im nachfolgenden Beispiel wird die Eintragung aus dem Client heraus vorgenommen. Dies ist natürlich auch über die Browser Addons analog möglich. Die Vorgehensweise bleibt die gleiche.



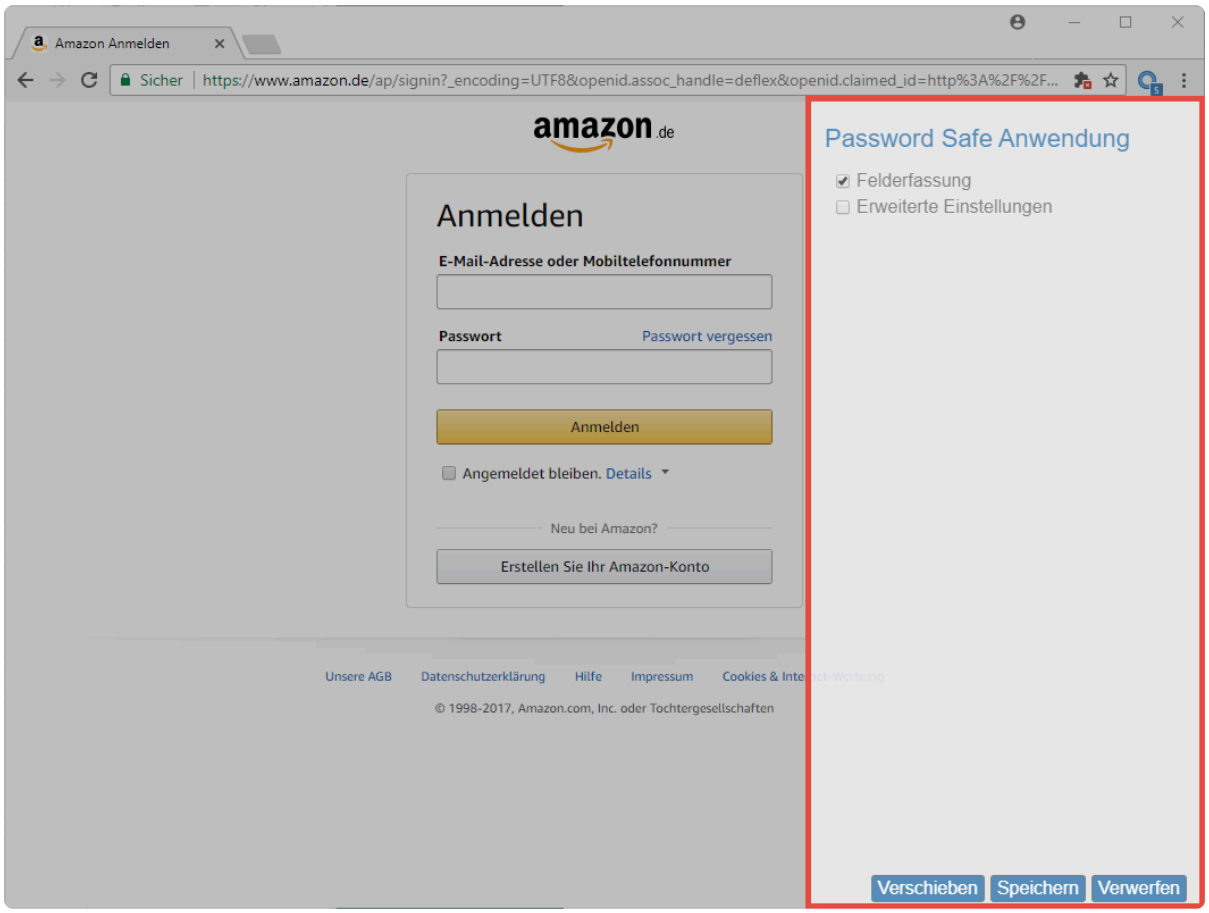
Technisch wird anhand der URL geprüft, ob der Datensatz zur Seite passt. Lediglich der Hostname inkl. Endung (“.de” und “.com”) muss hierbei übereinstimmen.

Anwendungen erfassen

Falls die Anmeldemaske einer Webseite nicht automatisch befüllt werden kann, müssen Sie eine Anwendung manuell erfassen. Zum Erfassen wird zunächst die gewünschte Webseite aufgerufen. Anschließend wird über das Icon das Addon aufgerufen. Die finden hier den Menüpunkt **Anwendung erfassen**.



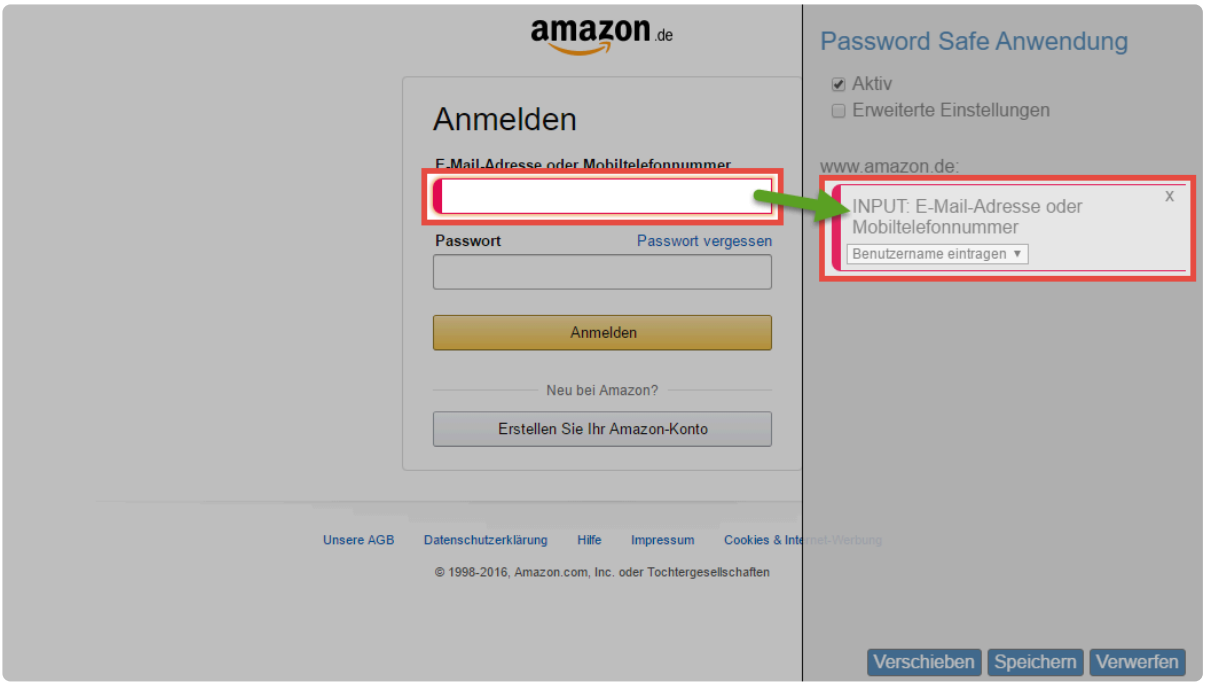
Nun öffnet sich ein modales Fenster. Hier legen Sie nun die eigentliche Anwendung an.



Folgende Optionen stehen Ihnen 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** ändern Sie die Position des modalen Fensters, wenn durch dieses das Anmeldefenster verdeckt ist.

Zum Erfassen klicken Sie in der Webseite in das erste auszufüllende Feld. 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 können Sie die Aktion selbstverständlich anpassen. Sind alle Felder erfasst, wird nochmals geprüft ob die Aktionen korrekt sind. Abschließend speichern Sie dann die Anwendung.

Die gespeicherte Anwendung steht nun zur Benutzung bereit und kann über das Addon genutzt werden.

Passwörter speichern

Speichern von Passwörtern über die Browser-Erweiterung

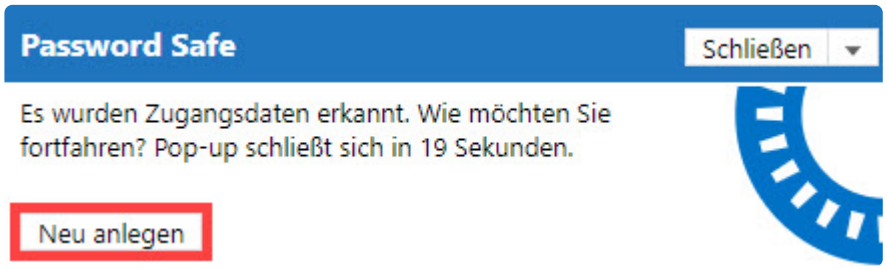
In diesem Kapitel wird das Speichern von Passwörtern über die Browser-Erweiterung näher ausgeführt.

> ! Das Speichern funktioniert nur im Server-Modus. Lesen Sie hier, wie man den Server-Modus auswählt.

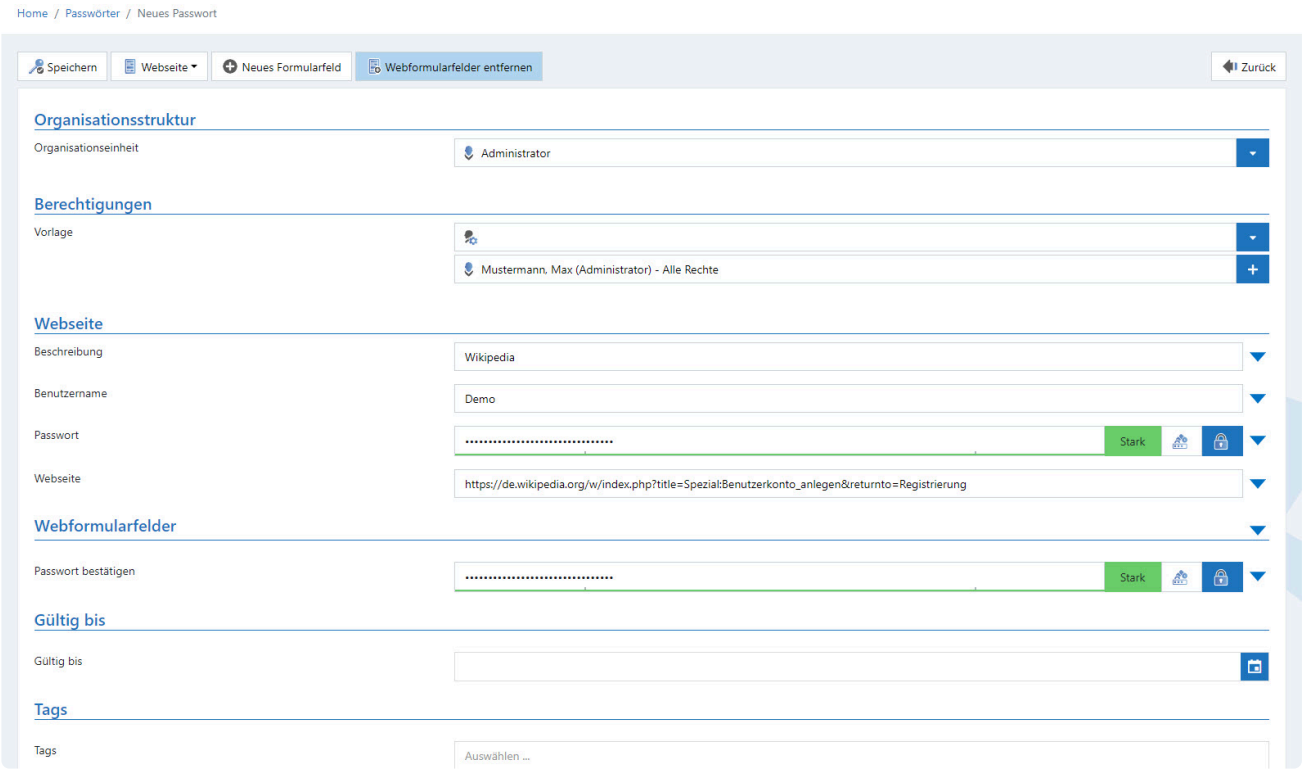
Abspeichern von Passwörtern

Neue Zugangsdaten

Mit der Einrichtung und Anmeldung über den Server-Modus können Zugangsdaten jetzt automatisiert hinzugefügt werden. Bei dem Besuch einer Website, deren Anmeldedaten bis dato nicht in Password Safe hinterlegt waren, fragt Password Safe automatisch, ob Sie die neu erkannten Zugangsdaten anlegen wollen.



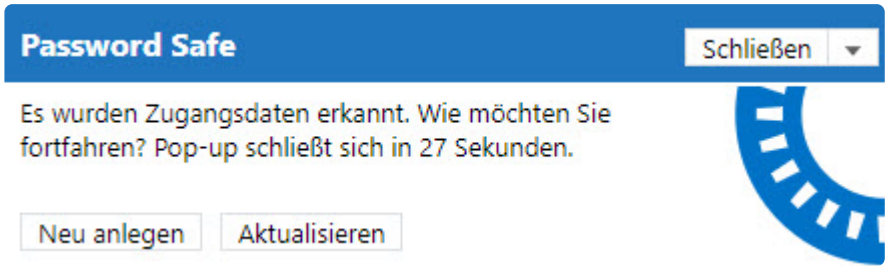
Bei Bestätigung dieser Meldung werden Sie direkt zum WebClient weitergeleitet und dort angemeldet. Wenn bei dem hinterlegten bzw. ausgewählten Formular weniger Felder als in der Anmeldemaske vorhanden sein sollten, werden die fehlenden Felder per default automatisch als Webformularfelder angelegt.



> Das Recht **“Kann Passwortformularfelder verwalten”** muss aktiviert sein, damit Webformularfelder überhaupt angelegt werden können.

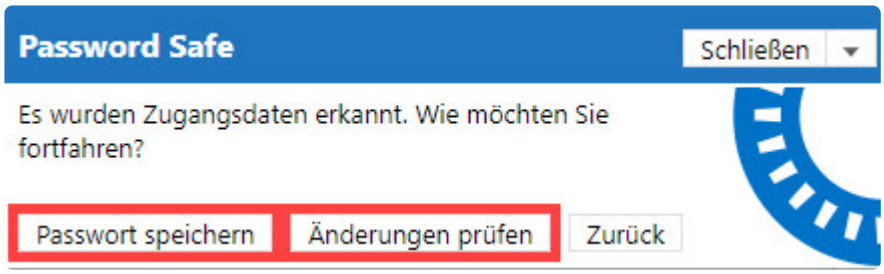
Bekannte Zugangsdaten

Falls Sie sich an einer Anmeldemaske mit geänderten Zugangsdaten anmelden, können Sie diese automatisch aktualisieren. Dafür melden Sie sich wie gewohnt an der Anmeldemaske der geänderten Seite an. Daraufhin erscheint eine Meldung, dass neue Zugangsdaten erkannt wurden. Nun können Sie optional entscheiden, einen neuen Datensatz anzulegen oder einen bereits bekannten Datensatz zu aktualisieren.



- **Passwort speichern**: Das Passwort wird dabei ausgetauscht, ohne dass der WebClient geöffnet wird.
- **Änderungen prüfen**: Der WebClient wird geöffnet und Sie werden angemeldet. Das bisherige Passwort wurde durch das neue ersetzt. Die Speicherung muss aber manuell vorgenommen

werden.



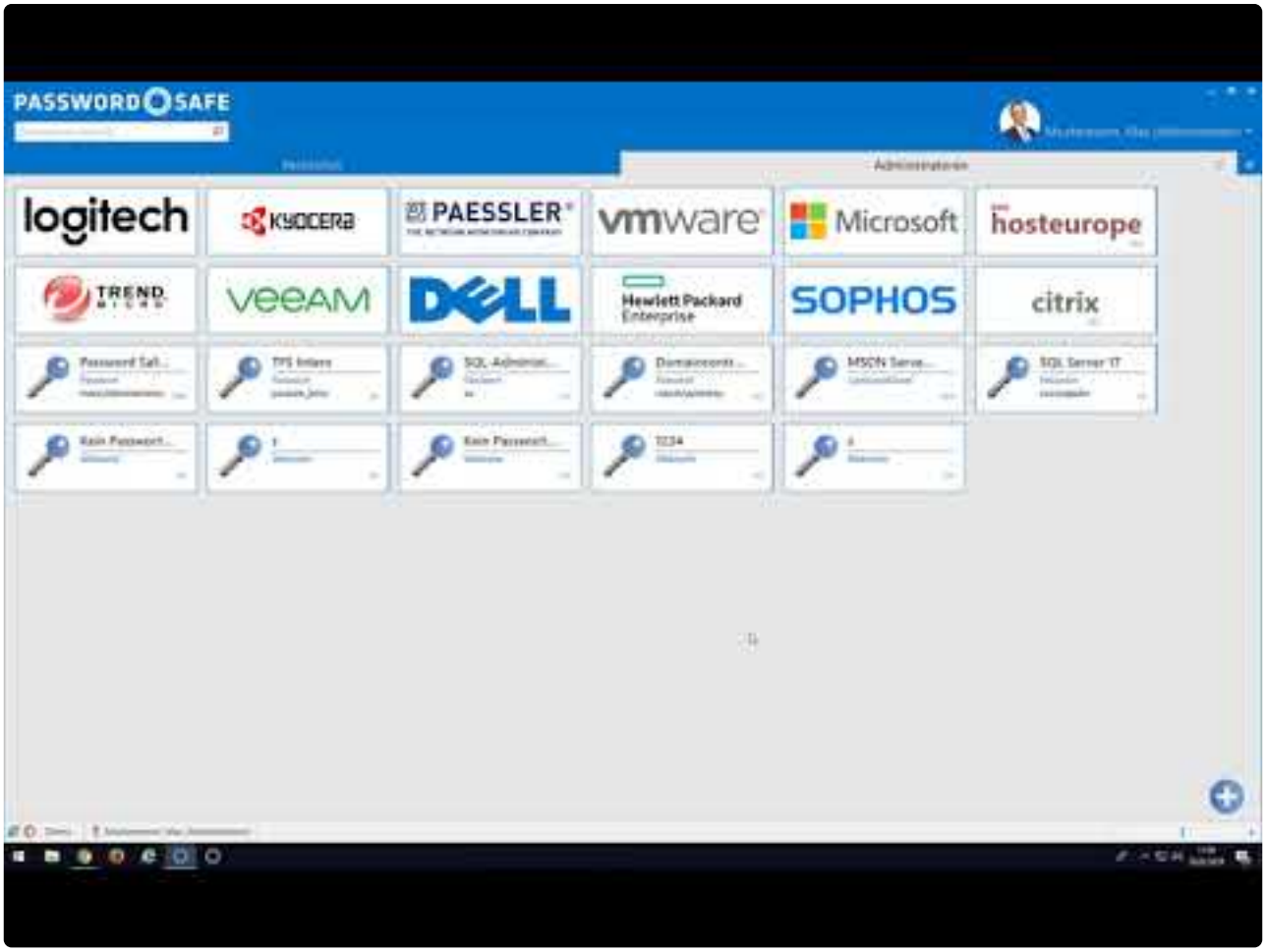
Damit ein Datensatz als bereits vorhanden gilt, gelten folgende Voraussetzungen:

- Die URL muss identisch sein.
- Der Benutzername muss identisch sein.
- Die Eintragung muss von der Browser-Erweiterung erfolgen und die Änderung darf nur das Passwort betreffen.

LightClient

Was ist der LightClient?

Der LightClient ist ein schlanker Client für den Endanwender, der einen schnellen Zugriff auf die täglich benötigten Passwörter ermöglicht. Obwohl der LightClient einen eingeschränkten Funktionsumfang hat, kann er intuitiv und ohne Vorkenntnisse von jedem Mitarbeiter bedient werden. Der LightClient stellt nicht nur den Einstieg in das professionelle Password Management dar. Er ist auch das ideale Werkzeug für den täglichen Umgang mit Passwörtern.



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

Voraussetzungen & benötigte Rechte

Für die Verwendung des LightClients sind keine speziellen Rechte nötig. Dennoch kann die Handhabung des LightClients über Rechte und Einstellungen konfiguriert werden. Alle nötigen Infos hierzu gibt es im Kapitel **To do für die Administration**

Installation

Der LightClient wird direkt mit dem FullClient installiert. Weiterführende Informationen finden Sie im Kapitel **Installation Client**.

Funktionen

Die Funktion und auch die Bedienung des LightClients werden in der Hilfe beschrieben.

To do für die Administration

Voraussetzungen für den Betrieb des LightClients

Der LightClient soll einen angenehmen und mühelosen Umgang mit Passwörtern ermöglichen. Um den einwandfreien Betrieb zu gewährleisten, sollten durch die Administration gewisse Vorbereitungen getroffen werden. Auf diese wir im Folgenden eingegangen.

> ✻ Um den Übergang zum LightClient für die Benutzer so einfach und reibungslos wie möglich zu gestalten, gibt es eine **Checkliste** für die Administration, an welcher Sie sich orientieren können.

Relevante Rechte und Einstellungen

In diesem Abschnitt werden die **Rechte und Einstellungen** aufgezählt, die der Benutzer zum Arbeiten mit dem LightClient benötigt. Diese müssen von Ihrer Administration nach eigenem Ermessen angepasst und konfiguriert werden.

Rechte

Benutzerrecht	Kapitel	Neu
Kann individuelle Passwörter im LightClient anlegen		✔
Kann neue Passwort-Bilder hochladen		✔
Kann Passwort-Bilder verwalten		✔
Kann Tab der eigenen Organisationseinheit im LightClient schließen		✔

Einstellungen

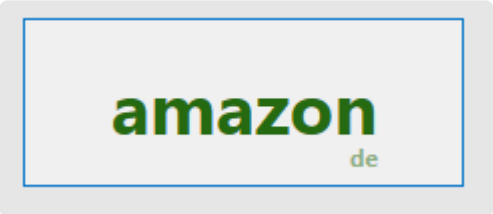
Einstellungen	Kapitel	Neu
Nach Favicon-Download fragen		✔
Darstellung der Passwörter im LightClient		✔
Darstellung der Passwörter im Vollclient		✔
Logo-Ansicht bei MouseOver im LightClient umschalten		✔
Standard-Formular (für LightClient)		✔
LightClient beim nächsten Login starten		✔
Untergeordnete Organisationseinheiten in LightClient einschließen		✔

Umgang mit Passwörtern im LightClient

Sie haben mehrere Möglichkeiten Passwörter im LightClient zur Verfügung zu stellen bzw. anzulegen.

Vorgegebene Passwörter

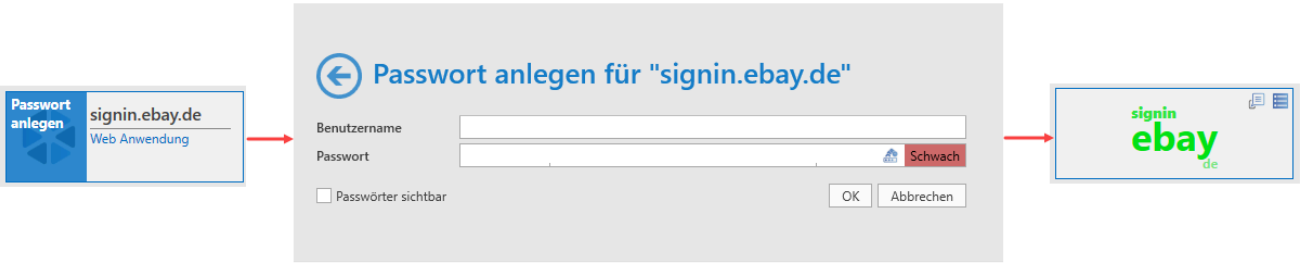
Bei vorgegeben Passwörtern handelt es sich um Passwörter, die bereits am FullClient angelegt worden sind. Achten Sie darauf, dass Sie die Berechtigungen so anpassen, dass die Benutzer die Passwörter auch im LightClient nutzen können. Der Benutzer muss mit **mindestens lesend** auf den Datensatz berechtigt ist.



Über Anwendung selbst erstellte Passwörter

Es gibt die Möglichkeit, durch den Administrator am FullClient Anwendungen zu erstellen. Diese werden dann am LightClient zur Verfügung gestellt. Durch einen Klick auf die Anwendung kann der Endanwender dann schnell und einfach ein entsprechendes Passwort dazu erstellen. Dabei ist es wichtig, dass nicht nur die Anwendung für sich erstellt wurde, sondern dass die Berechtigungen für den entsprechenden Benutzer genauso gegeben sind. Der Benutzer der die Anwendung nutzen soll, muss mit **mindestens lesend** auf die Anwendung berechtigt sein.

Weitere Informationen zu diesem Thema finden Sie im Kapitel Anwendungen.



Selbst erstellte Passwörter ohne Anwendung

Damit ein LightClient-Benutzer neue Passwörter anlegen kann, müssen Sie folgende **Rechte und Einstellungen** berücksichtigen.

Benutzerrecht:

- **Kann individuelle Passwörter im LightClient anlegen**

Einstellung:

- **Standard-Formular (für LightClient)**, ansonsten kann dem neu zu erstellendem Passwort kein

Formular zugeordnet werden
- **Hinzufügen-Recht** auf die Organisationseinheit des Benutzers

Passwortverwaltung am LightClient

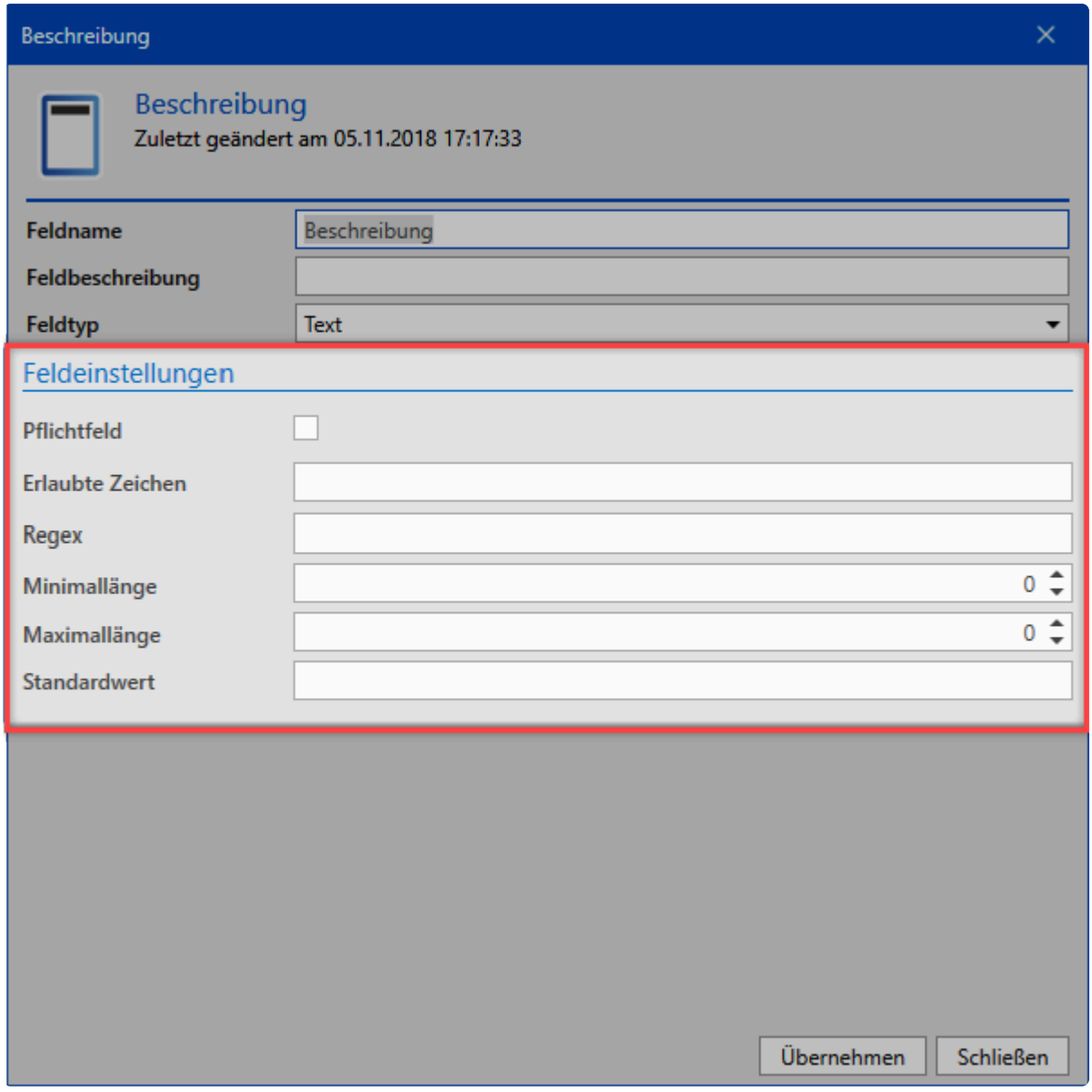
Errorcodes des LightClients

Errorcodes für die Administration

Treten am LightClient Probleme auf, werden diese durch Errorcodes klassifiziert. Diese Codes helfen der Administration, Probleme einzugrenzen und schlussendlich zu beheben. Es gibt 7 verschiedene Errorcodes:

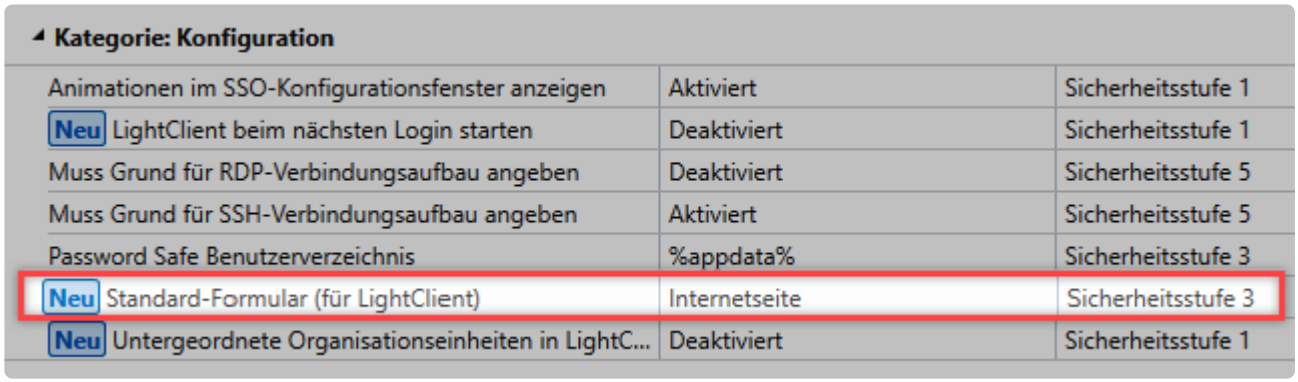
SavePasswordUnknown
Es ist ein unerwarteter Fehler aufgetreten. In der Ereignisanzeige des Anwendungsservers sind weitere Hinweise zu finden.

SavePasswordPlausibilityField
Beim Speichern eines Passworts wurde die Plausibilität nicht erfüllt. Prüfen Sie die Pflichtfelder des hinterlegten Formulars.



NoDefaultForm

Es wurde kein Standardformular ausgewählt. Dieses können Sie in den Einstellungen unter **Standard-Formular (für den LightClient)** hinterlegen.



DefaultFormNotFound
Überprüfen Sie die Rechte des Formulars. Der Benutzer muss mindestens **lesend** auf das Formular berechtigt sein.

DefaultFormMissingFields
Das Formular wurde richtig konfiguriert. Sie müssen die Feldtypen im Formular prüfen. Mindestens benötigt werden: Text, Benutzername, Passwort, URL.

DefaultFormImpossiblePlausibility
Beim Anlegen eines Passworts für eine Anwendung gibt es ein Feld, das nicht angezeigt wird. Prüfen Sie daher die Plausibilitäten in Feldern.

NoValidOrganisation
Ist nur für die Webansicht im LightClient relevant. Der Fehler wird ausgelöst, wenn Sie über die Browser-Erweiterung ein Passwort anlegen möchte und Sie keine OU haben, in der Sie es anlegen können.

Checkliste LightClient

Checkliste zum Einrichten/Konfigurieren des LightClients

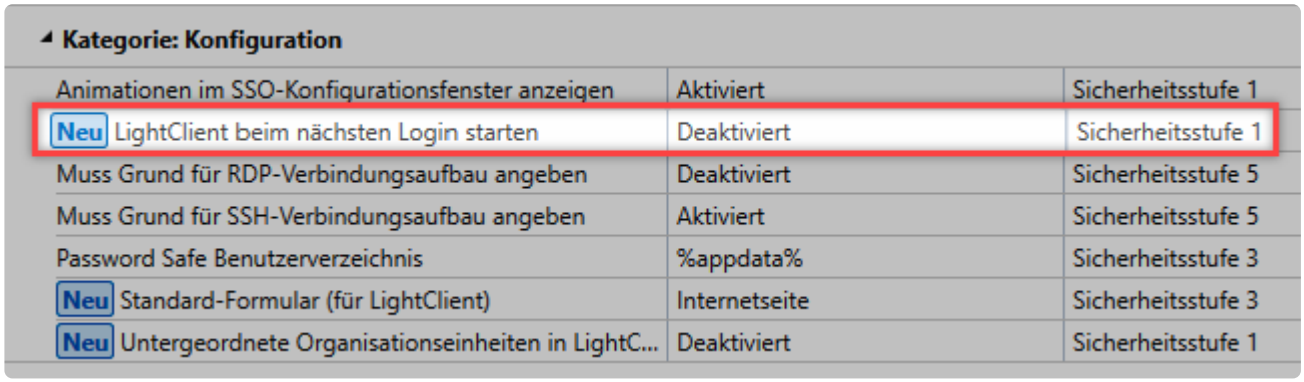
Diese Checkliste unterstützt den Administrator bei der Konfiguration des LightClients. Für ein reibungsloses Arbeiten mit dem LightClient gilt es, folgende Punkte zu beachten:

1. Formular auswählen
Das hinterlegte Formular muss alle benötigten Feldtypen abdecken. Mindestens benötigt werden: **Text, Benutzername, Passwort, URL**

2. Darstellung des LightClient bzw. des FullClient einstellen
Die Einstellung **Darstellung der Passwörter im LightClient & Darstellung der Passwörter im FullClient** ermöglicht Ihnen, die Darstellung der beiden Clients zu konfigurieren. Dabei können Sie die Passwörter mit einem Icon, einem Logo oder in Textform darstellen.

3. Benutzer in der richtigen Organisationseinheit?
Prüfen Sie, ob sich der Benutzer in der richtigen Organisationseinheit befindet. Außerdem wird das **Hinzufügen-Recht** auf die Organisationseinheit benötigt, damit die Benutzer Passwörter im LightClient anlegen können.

4. Benutzer als LightClient-Benutzer definieren
Sie können den Benutzer direkt als LightClient-Benutzer definieren. Dies funktioniert, indem Sie den Benutzertyp entsprechend ändern bzw. gleich definieren.
Alternativ können Sie die Einstellung **LightClient beim nächsten Login starten** aktivieren. Damit ist der Benutzer dazu angehalten, sich am LightClient anzumelden.

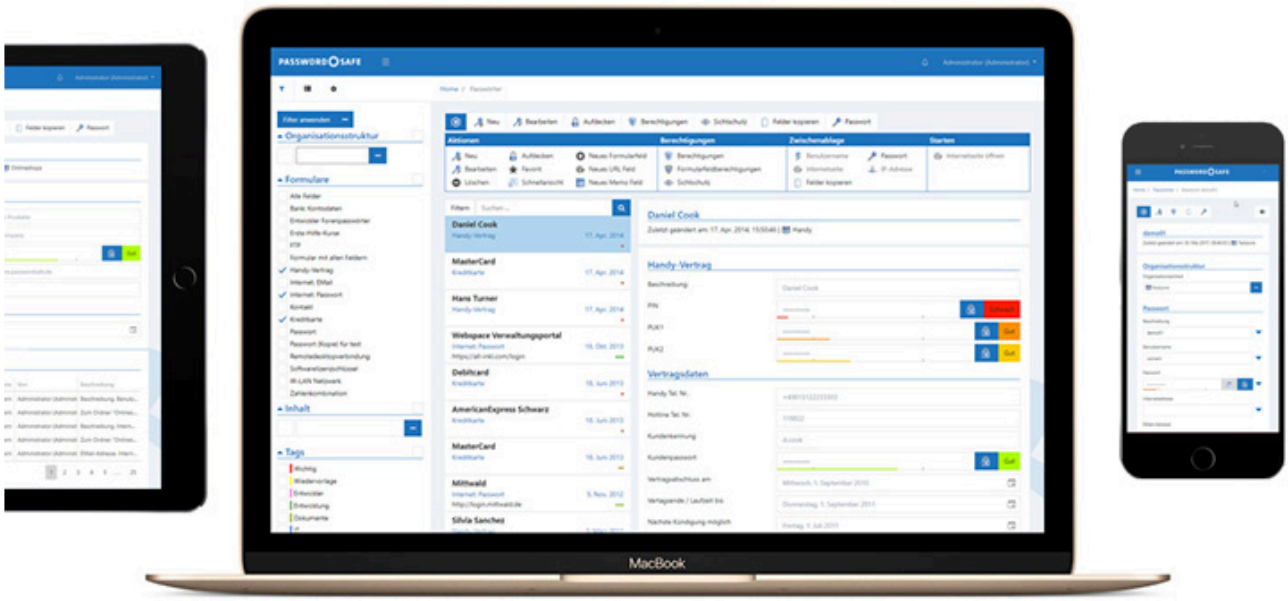


5. Standardanwendungen hinzufügen (optional)
Es wird geraten, die Anwendungen, die als Passwörter hinterlegt werden sollen, vorab anzulegen.

WebClient

Was ist der WebClient

Mit der Password Safe Version 8.3.0 wird der bisherige WebAccess durch den **WebClient** mit einem stetig wachsenden Funktionsumfang ersetzt. Das Ziel ist es, im WebClient die gleichen Funktionen wie im WPF-Client zur Verfügung zu stellen. Der **WebClient** wird daher ständig erweitert.
Alle aktuell verfügbaren Funktionen finden Sie im Kapitel **Funktionsumfang**.



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, können Sie ihn zudem auch auf allen mobilen Geräten wie Tablets und Smartphones benutzen.

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, auf die sie auch berechtigt sind. Die Installation wird im Kapitel **Installation WebClient** beschrieben.

Funktionsumfang

Durch den **WebClient** wurde die Basis für eine stetige Erweiterung gesetzt. Der jeweils aktuelle Funktionsumfang wird an dieser Stelle erläutert. Um eine bessere Übersicht zu schaffen, werden die einzelnen Module in eigenen Unterkapiteln behandelt.

Allgemeine Funktionen

- Globale Einstellungen und Benutzereinstellungen
- Globale Benutzerrechte

Funktionen in den einzelnen Modulen

- Passwörter
- Tag System
- Organisationsstruktur
- Rollen
- Formulare
- Benachrichtigungen
- Logbuch
- Anwendung
- Dokumente

Tag System

Das **Tag System** stellt aktuell folgende Funktionen bereit:

- Anlegen
- Löschen
- Editieren

Passwörter

Im **Passwort Modul** stehen Ihnen 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
- Sichtschutz
- Siegel
- Drucken
- Externen Link erzeugen
- Historie
- Formular wechseln
- Exportieren
- WebViewer Export

Das WebClient Modul **Passwort** Modul orientiert sich am gleichnamigen Modul, das sich im Client befindet. Beide Module unterscheiden sich in Umfang und Design, sind aber hinsichtlich der Bedienung trotzdem nahezu identisch.

Organisationsstruktur

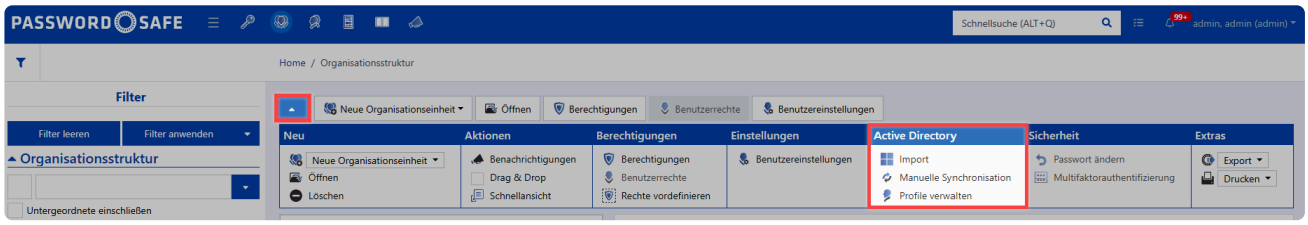
Im **Organisationsstrukturen-Modul** gibt es aktuell folgende Funktionen:

- Benutzer/Organisationsstruktur anlegen/editieren/löschen/berechtigen
- Benachrichtigungen
- Drag & Drop
- Filter
- Schnellansicht
- Benutzereinstellungen
- Benutzerrechte
- Rechte vordefinieren
- Passwortänderung
- Drucken
- AD-Anbindung
- Exportieren
- Drucken

> Das WebClient-Modul **Organisationsstruktur** orientiert sich am gleichnamigen Client Modul. Beide Module unterscheiden sich in Umfang und Design. Die Bedienung ist jedoch nahezu identisch.

AD-Anbindung im WebClient

Die Active Directory Anbindung am WebClient funkioniert ähnlich wie am Client. Nähere Informationen finden Sie hier

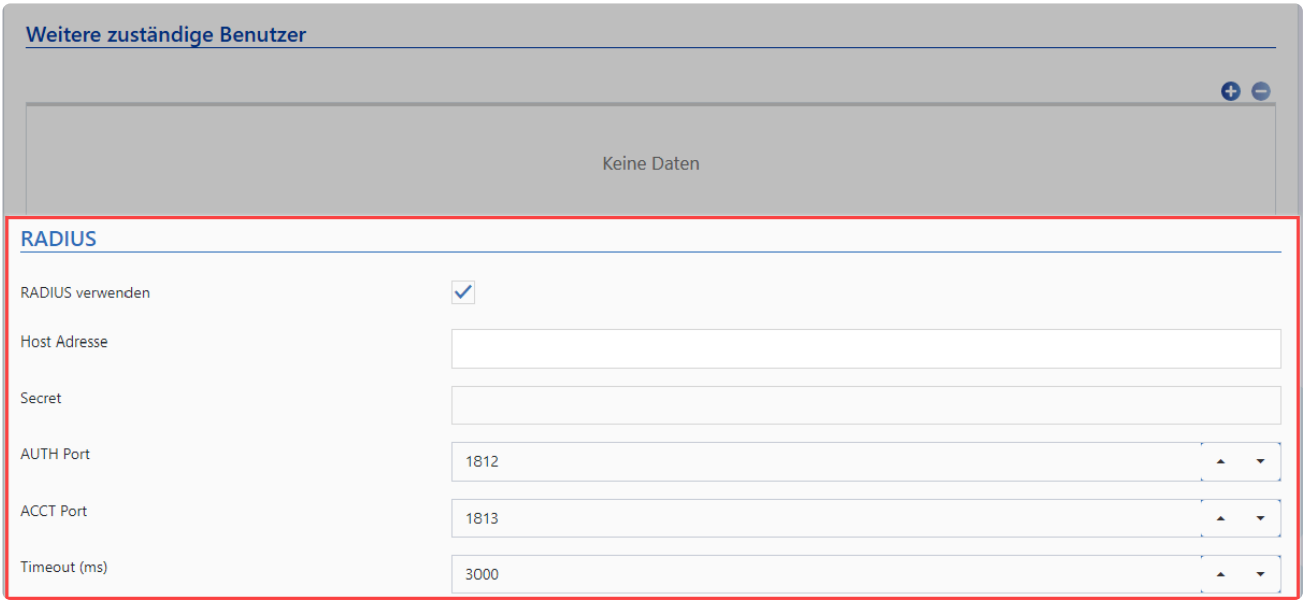


Der WebClient bietet folgende Funktionen:

- Import
- Manuelle Synchronisation
- Profile verwalten

Radius

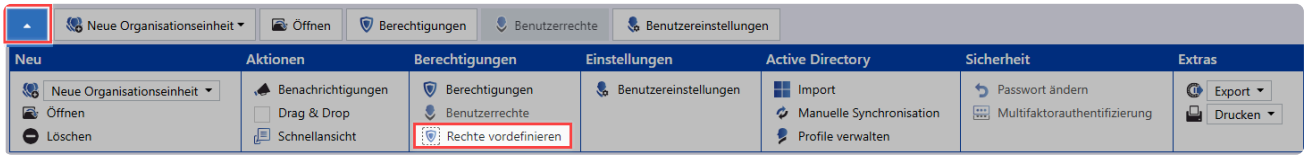
Findet der Import im Masterkey-Modus statt, kann ein Radius-Server angesprochen werden. Dieser wird direkt im Activ Directory Profil hinterlegt und übergibt dann zukünftig die möglichen Authentifzierungs-Methoden. Weitere Infos finden Sie im Kapitel **Radius Server**.



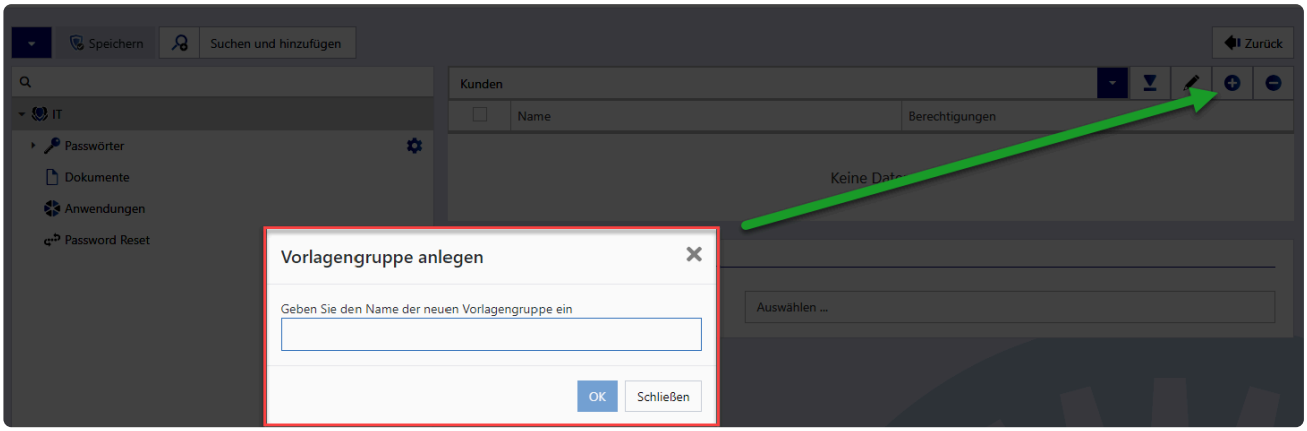
Vordefinieren von Rechten

Beim **Rechte vordefinieren** im WebClient ist die Vorgehensweise genau dieselbe wie im Client. Mehr dazu erfahren Sie hier.

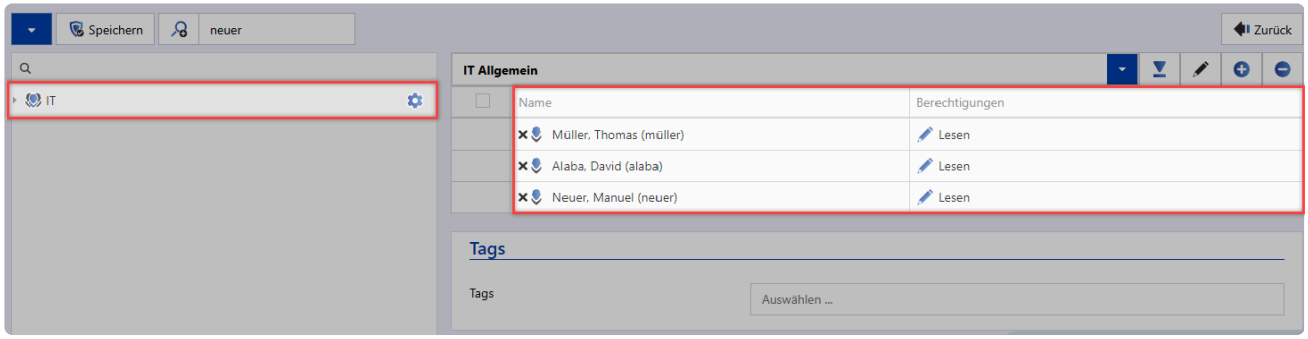
Im Modul Organisationsstruktur wählen Sie die Organisationseinheit aus, für die die Rechte vordefiniert werden. Wählen Sie anschließend in der Menüleiste **Rechte vordefinieren** aus.



Erstellen der ersten Vorlagengruppe: Durch einem Klick auf das Icon zum Hinzufügen neuer Vorlagengruppen (grüner Pfeil) erscheint ein modales Fenster. Wählen Sie für die Vorlagengruppe einen möglichst aussagekräftigen Namen.

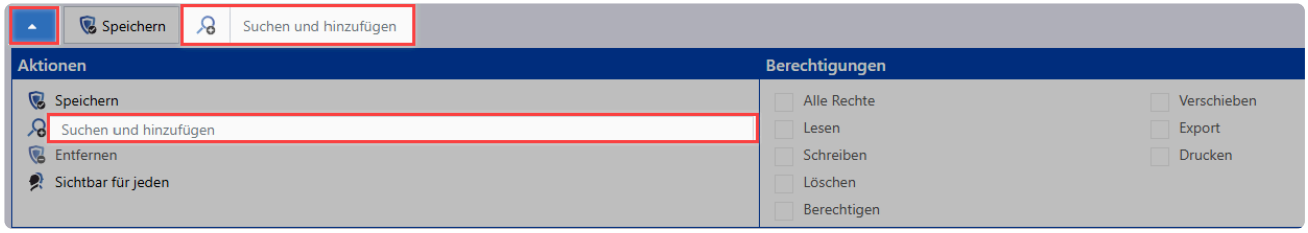


Fügen Sie die entsprechenden Rollen und Benutzer hinzu.



Das Hinzufügen von Benutzern und Rollen ist auf verschiedene Weisen möglich:

- Fügen Sie in der Toolbar bei **Suchen und hinzufügen** die entsprechenden Benutzer und Rollen hinzu.
- Durch einen Klick auf die Lupe werden alle verfügbaren Benutzer und Rollen einsehbar.



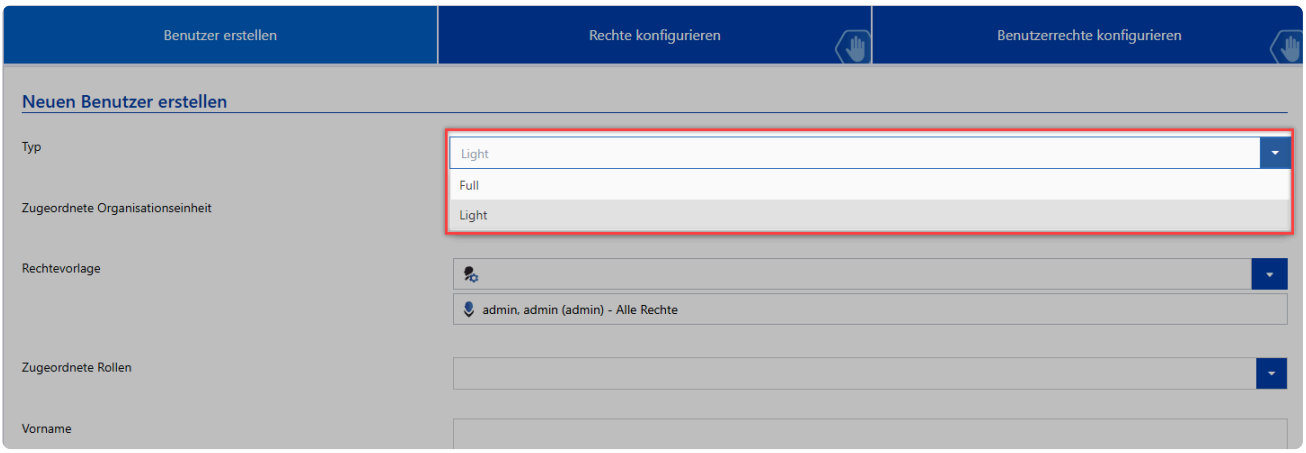
Benutzerverwaltung

Wie werden die Benutzer im WebClient 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. In allen anderen Modi erfolgt die Benutzerverwaltung über das Modul Organisationsstruktur.

Anlegen lokaler Benutzer

Achten Sie beim ANlegen neuer Benutzer drauf, ob es sich bei dem Benutzer um einen **Light-Benutzer** oder einen **Voll-Benutzer** handelt.



Rollen

Im **Rollen Modul** stehen Ihnen aktuell folgende Funktionen zur Verfügung:

- Anlegen
- Löschen
- Benachrichtigungen
- Favoriten
- Schnellansicht
- Berechtigungen
- Benutzerrecht
- Drucken

> Das WebClient Modul **Rollen** orientiert sich am gleichnamigen Client-Modul. Beide Module unterscheiden sich in Umfang und Design, sind aber hinsichtlich der Bedienung trotzdem nahezu identisch.

Formulare

Im **Formulare Modul** stehen aktuell folgende Funktionen bereit:

- Anlegen
- Öffnen
- Löschen
- Benachrichtigungen
- Duplizieren
- Favorit
- Schnellansicht
- Berechtigungen
- Drucken
- Exportieren

Das WebClient Modul **Formulare** orientiert sich am gleichnamigen Client-Modul. Beide Module unterscheiden sich in Umfang und Design, sind aber hinsichtlich der Bedienung trotzdem nahezu identisch.

Benachrichtigungen

Im **Benachrichtigungs-Modul** stehen Ihnen folgende Funktionen zur Verfügung:

- Filterfunktionaltiät
- Siegelfunktionalität
- Nachrichten als ungelesen/gelesen markieren
- Schnellansicht (über Button und Leertaste möglich)
- E-Mail-Weiterleitung

> Das WebClient-Modul **Benachrichtigungen** orientiert sich am gleichnamigen Client-Modul Benachrichtigungen. Beide Module unterscheiden sich in Umfang und Design, die Bedienung ist jedoch nahezu identisch.

Anwendung

Im **Anwendungs-Modul** sind aktuell folgende Funktionen verfügbar:

Web- & SAML Anwendungen:

- Anlegen
- Verwalten
- Löschen

> Eine ausführliche Erläuterung wie Sie SAML konfigurieren können, finden Sie im Kapitel Konfiguration von SAML

allgemeine Funktionen:

- Benachrichtigungen
- Duplizieren
- Verschieben
- Favorit
- Schnellansicht
- Passwort verbinden

> Das WebClient-Modul **Anwendungen** orientiert sich am gleichnamigen Client-Modul Anwendungen. Beide Module unterscheiden sich in Umfang und Design, die Bedienung ist jedoch nahezu identisch.

Logbuch

Im **Logbuch-Modul** sind aktuell folgende Funktionen vorhanden:

- Filterfunktionalität
- Schnellansicht

> Das WebClient-Modul **Logbuch** orientiert sich am gleichnamigen Logbuch. Beide Module unterscheiden sich in Umfang und Design, die Bedienung ist jedoch nahezu identisch.

Dokumente

Im **Dokumenten-Modul** gibt es aktuell folgende Funktionen:

- Neu
  Neues Dokument fügen Sie auf folgende Arten hinzu:
  - Rechtsklick -> Suchen
  - Suchen über die Navigationsleiste
  - per Drag & Drop (indem man das Dokument in das Fenster zieht)
- Eigenschaften öffnen
- Dokument aktualisieren
- Benachrichtigungen
- Verschieben
- Favorit
- Schnellansicht
- Export
- Berechtigungen
- Externen Link erzeugen
- Drucken
- Historie

Das WebClient-Modul **Dokumente** orientiert sich am gleichnamigen Client-Modul Dokumente. Beide Module unterscheiden sich in Umfang und Design, die Bedienung ist jedoch nahezu identisch.

Bedienung

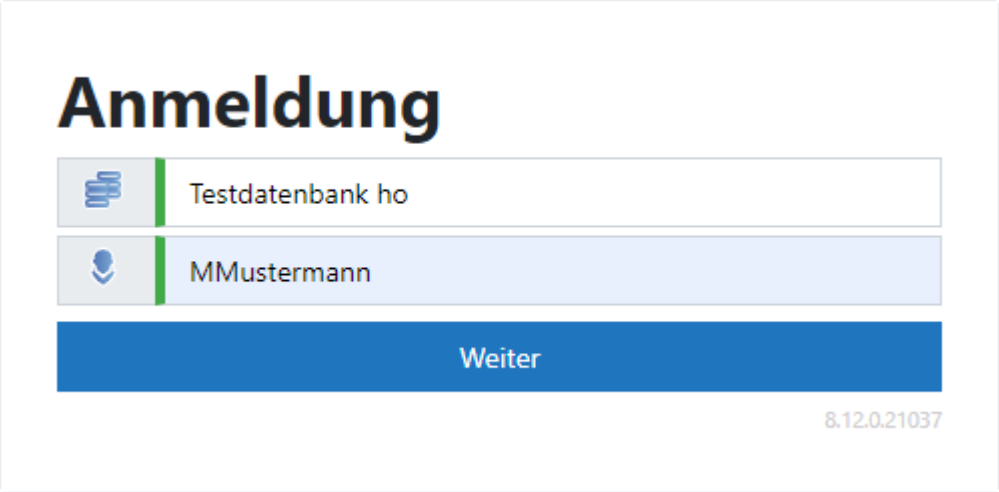
Die Bedienung des WebClients wurde soweit als möglich an die Bedienung des Password Safe Clients angelehnt. Dennoch gibt es einige Unterschiede zu beachten, welche hier geschildert werden.

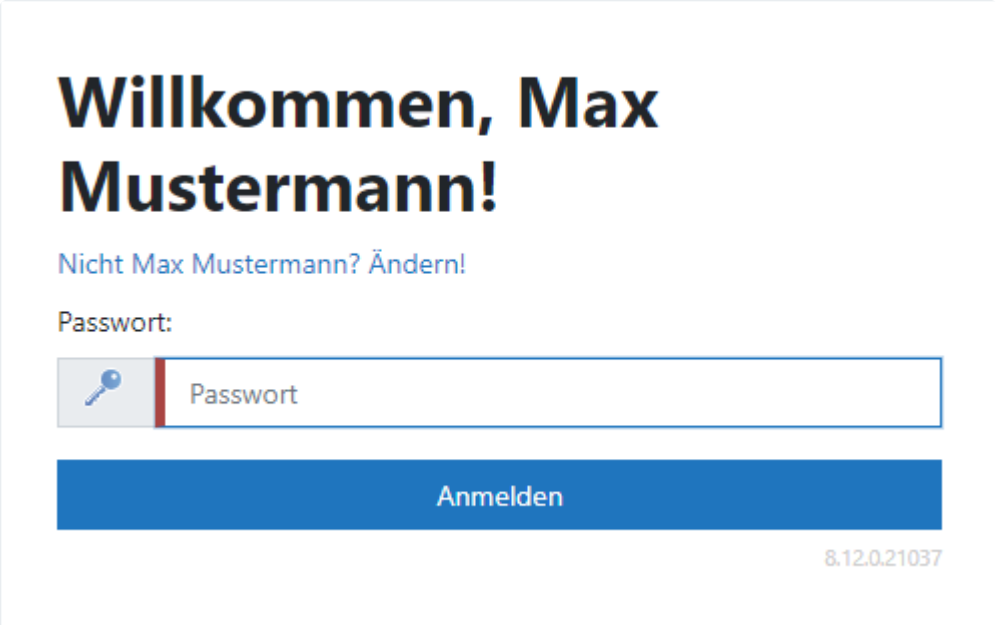
> Auch im WebClient gibt es einen LightClient. Alles wissenswerte hierzu finden Sie unter folgendem Link: Webansicht Light Client

Login

Am WebClient gibt es keine Datenbank Profile. Es stehen alle Datenbanken zur Verfügung, welche für den WebClient freigegeben wurden. Zum Login müssen Sie also folgende Infos eingeben:

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.

Übergabe der Anmeldedaten per URL

Über die URL können direkt der **Datenbankname** und der **Benutzername** übergeben werden. Hierbei werden folgende Parameter verwendet:

- **database** zum Übergeben des Datenbanknamens
- **username** übergibt den Benutzernamen

Die Parameter werden einfach an die URL des WebClients angehängt und mittels **&** voneinander getrennt.

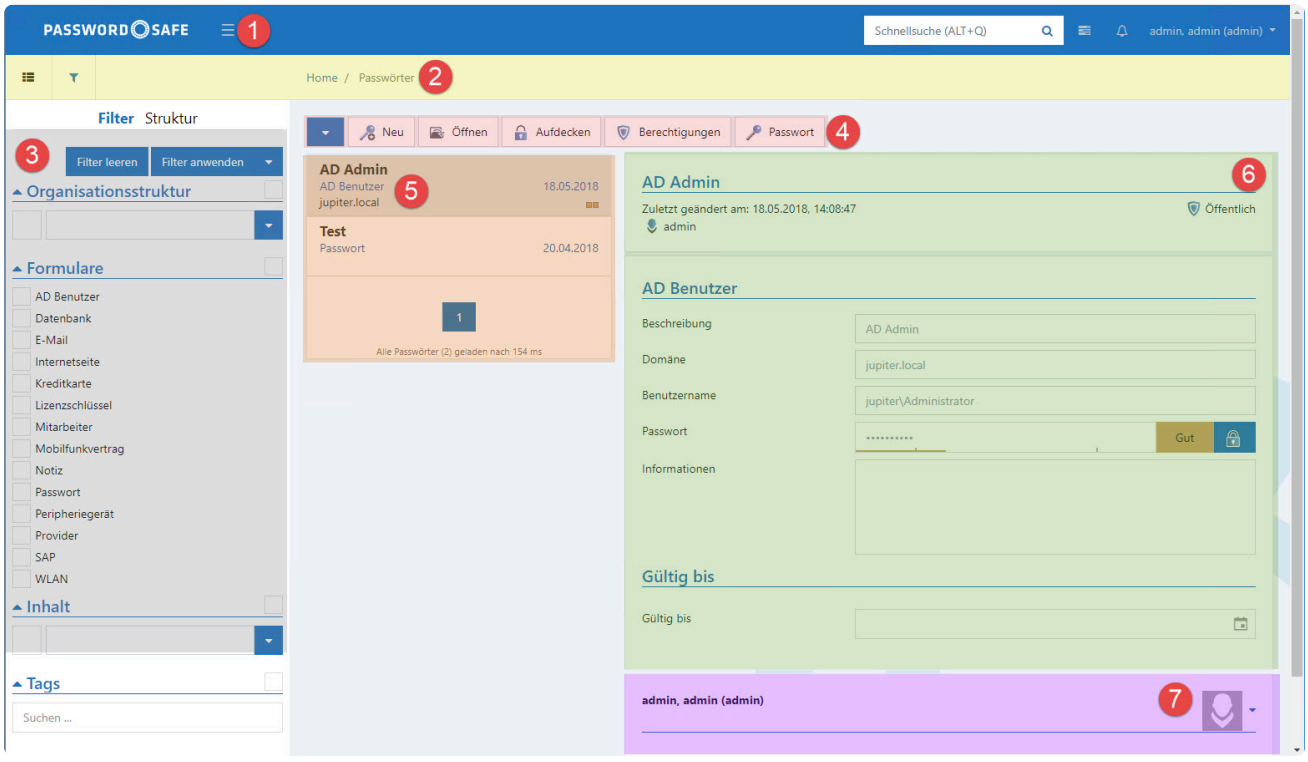
Beispiel

Der WebClient soll unter **https://psr_webclient.firma.com** aufgerufen werden. Hierbei soll die Loginmaske direkt mit der Datenbank **Passwords**, sowie dem Benutzernamen **Anderson** befüllt werden. Verwenden Sie dann folgende URL: **https://psr_webclient.firma.com/authentication/login?database=Passwords&username=Anderson**

> Es ist möglich nur die Datenbank zu übergeben. Der Benutzername ist nicht zwingend nötig.

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 schalten Sie zwischen der Modul- und der Filteransicht um.

3. Filter bzw. Strukturbereich

Wie auch am Client wählen Sie zwischen Filter und Struktur.

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.

7. Footer

Im Footer werden diverse Informationen zum Datensatz angezeigt. Beispielsweise Logbucheinträge oder die Historie.

Filter- bzw. Strukturbereich

Wie auch am Client, können Sie zwischen Filter und Struktur wechseln. Hierfür stehen Ihnen in der Navigationsleiste folgende Buttons bereit:

1. Filter

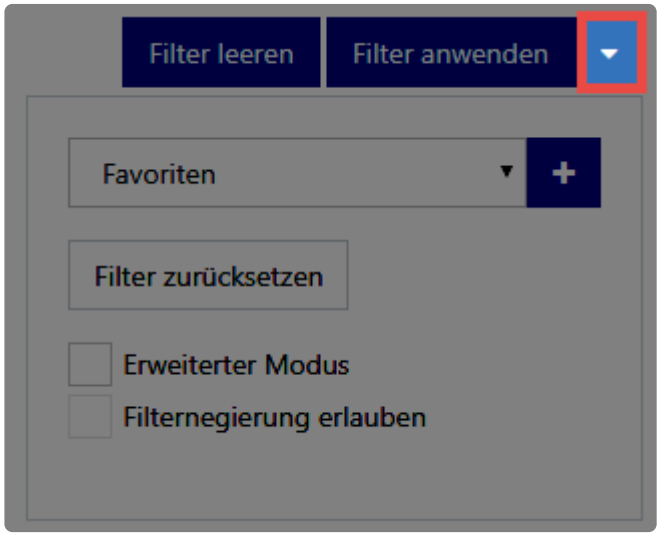
Der Filter im WebClient ist an den Filter der Clients angelehnt. Daher soll hier lediglich auf die WebClient-spezifischen Eigenschaften eingegangen werden.

Bedienung des Filters

Die Bedienung des **WebClient Filters** unterscheidet sich kaum von der des **Client Filters**. Beachten Sie nur, dass die Schaltflächen **Filter leeren** und **Filter anwenden** über dem Filter stehen.
Ebenso finden Sie direkt über dem **WebClient Filter** die Möglichkeit diesen zu konfigurieren.

Konfiguration des Filters

Blenden Sie die Konfiguration des Filters über folgende Schaltfläche ein:



Hier können Sie sowohl neue **Filtergruppen hinzufügen** als auch den aktuellen **Filter zurücksetzen**. Über den **erweiterten Modus** erhalten Sie die Möglichkeit einzelne Filtergruppen zu löschen oder zu verschieben. Ebenso kann die **Filternegierung erlaubt** werden.

2. Struktur

Die Struktur bedienen Sie genau so wie die des Clients.

Header

Der Header beinhaltet folgende Funktionen:

1. Logo

Das Logo entspricht einem Home-Button. Dadurch gelangen Sie immer wieder auf die standardmäßige Ansicht.

2. Filter ein- und ausblenden

Wie auch am Client können Sie den Filter, bzw. Strukturbereich ein- und ausblenden.

3. Module

Wie auch am Client besteht hier die Möglichkeit, die Module Passwörter, Organisationsstruktur, Rollen und Formulare zu verwalten.

4. Schnellsuche

Die Schnellsuche bietet die gleichen Funktionen wie die Schnellsuche des Clients. Sie durchsucht die komplette Datenbank in allen Feldern, außer dem Passwortfeld. Weiterhin werden die Tags durchsucht.

5. Aufgaben

Hier werden bevorstehende Aufgaben wie z.B. Export, Import, Drucken, etc. angezeigt.

6. Benachrichtigungen

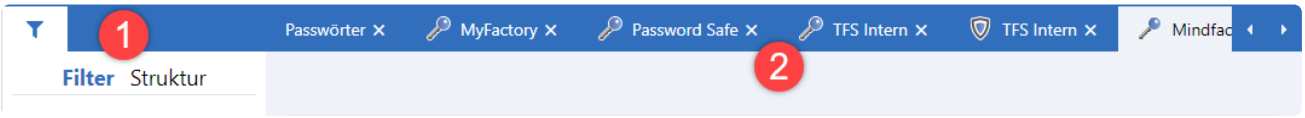
Hier werden Sie über eingehende Nachrichten informiert. Rufen Sie die nachricht über einen Klick ab.

7. Account

Unter dem Account ist der aktuell angemeldete Benutzer zu sehen. Über einen Klick darauf melden Sie sich ab. Blenden Sie hier ebenso die Einstellungen ein.

Navigationsleiste

Die Navigationsleiste stellt folgende Funktionen bereit.



1. Filter und Struktur

Hierüber können Sie im linken Bereich die Ansicht auf den Filter oder auf die Struktur umgeschalten.

2. Tabsystem

Das aus dem Client bekannte Tabsystem ist auch im WebClient verfügbar. Öffnen Sie mehrere Datensätze, so werden diese in Tabs dargestellt. Sollten die geöffneten Tabs die Seitenränder überschreiten, werden zwei Pfeile angezeigt, mit welchen Sie nach links oder rechts navigieren können.

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 Sie sich gerade befinden, sind unterschiedliche Aktionen möglich.

Menüleiste

Das Menü kann zwei Ausprägungen annehmen. In der Regel wird die **Menüleiste** angezeigt, die die **wichtigsten Funktionen** darstellt. Exemplarisch soll das am Beispiel des Passwort Moduls verdeutlicht werden.

1. Menü erweitern

Über diese Schaltfläche maximieren Sie das Menü.

2. Neu

Hierüber rufen Sie den Assistent zum Anlegen eines neuen Datensatzes auf.

3. Öffnen

Diese Funktion stellt das selektierte Passwort im Lesebereich mit allen Details dar.

4. Aufdecken

Hier wird das Passwort eingeblendet.

5. Berechtigungen

Über diesen Button konfigurieren Sie die Rechte des Datensatzes.

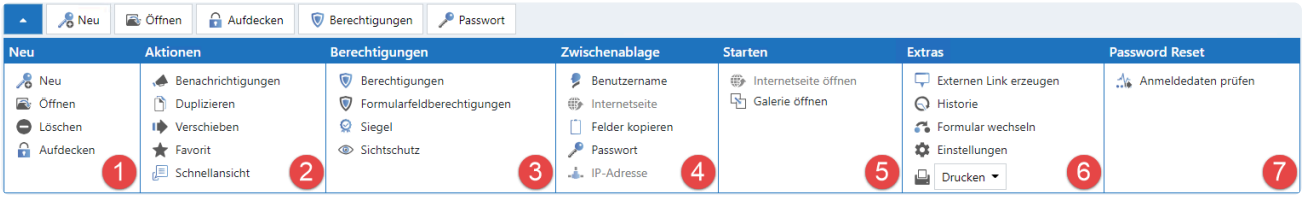
6. Passwort

Hierüber übernehmen Sie das Passwort in die Zwischenablage.

Erweitertes Menü

Wird das Menü – wie oben bereits erläutert – **maximiert**, stehen Ihnen **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 Ihnen weitere Aktionen zum Bearbeiten von Passwörtern. Beispielsweise **Öffnen** oder auch **Löschen**.

2. Aktionen

Über Aktionen markieren Sie das Passwort beispielsweise als **Favorit** oder **duplizieren** dieses.

3. Berechtigungen

Dieser Bereich bietet keine weiteren Funktionen als das Öffnen der Berechtigungen.

4. Zwischenablage

In diesem Bereich übernehmen Sie alle verfügbaren Felder in die Zwischenablage.

5. Starten

Hier rufen Sie eine Website auf.

> Wie bereits geschildert ist das Menü dynamisch und tritt somit in verschiedensten Ausprägungen auf. Die Grundfunktion ist jedoch immer gleich: In der Menüleiste finden Sie die Grundfunktionen, im erweiterten Menü dann alle Funktionen.

6. Extras

Über “Extras” finden Sie etliche Zusatzfunktionen. Deren Funktionen entsprechen dem HauptClient und werden in folgendem Kapitel beschrieben:
Passwort Extras

7. Password Reset

Die Funktionen des Password Resets finden Sie hier.

Listenansicht

Was versteht man unter Listenansicht?

Das Zentrale Element zur Navigation im WebClient ist die Listenansicht, welche die gefilterten Elemente übersichtlich darstellt. Da die Listenansicht des WebClients die gleichen Funktionen wie die Listenansicht des Clients zur Verfügung stellt, wird an dieser Stelle auf das Kapitel **Listenansicht** verwiesen.

Besonderheiten

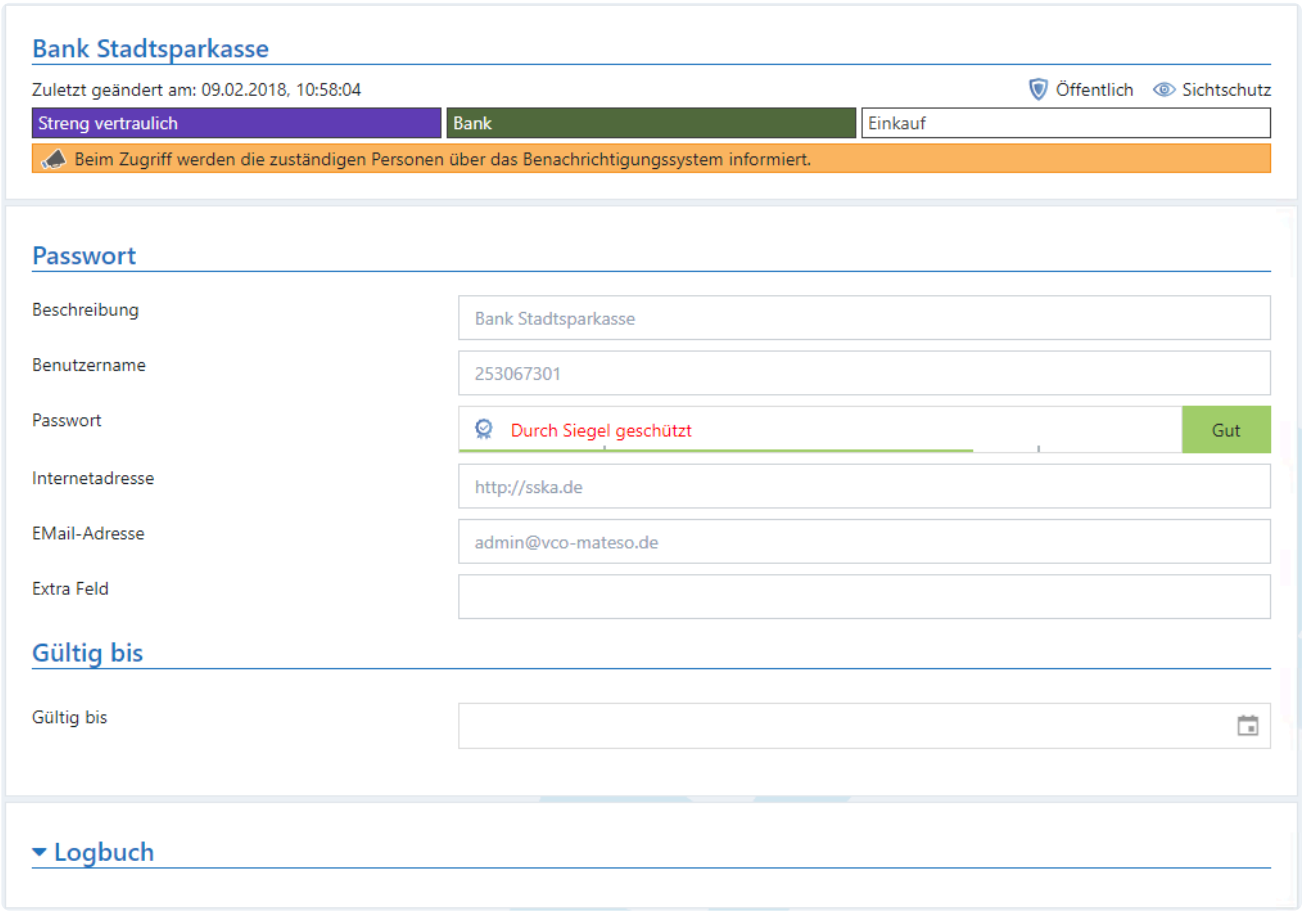
In folgenden Punkten unterscheidet sich die Listenansicht des WebClients von der des Clients:

- Die Listenansicht können Sie nicht individuell anpassen.

Lesebereich

Was versteht man unter Lesebereich?

Wie auch die Listenansicht, ist der Lesebereich des WebClients nahezu mit dem des Clients identisch. Deshalb wird auch hier auf das entsprechende Kapitel Lesebereich verwiesen.

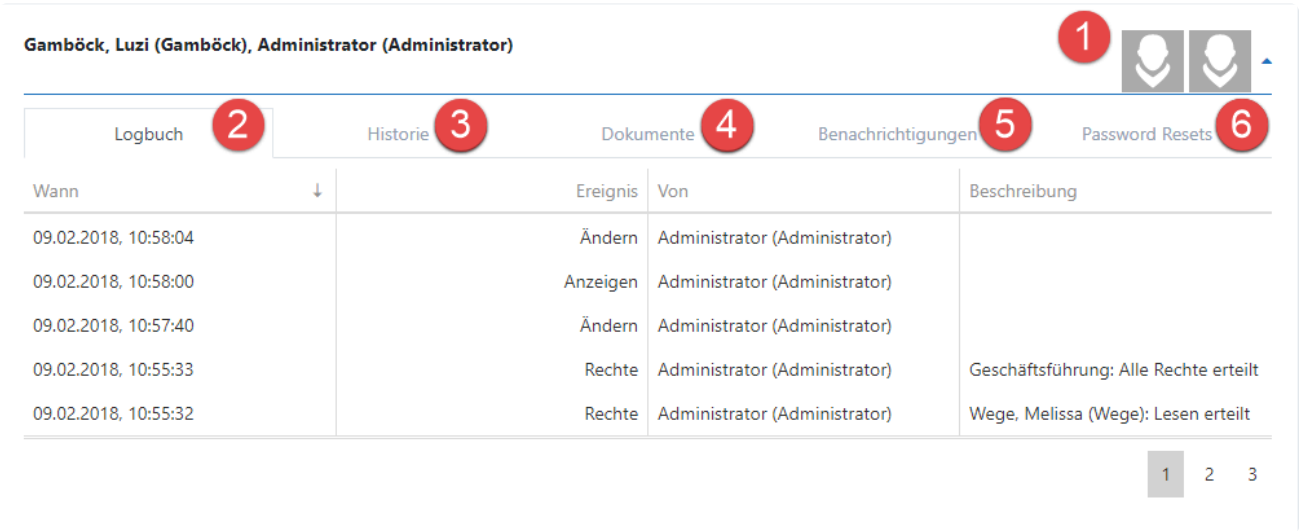


Im Header werden – wie vom Client gewohnt – diverse Informationen dargestellt. Beispielsweise die Tags des Datensatzes, oder Hinweise, ob der Datensatz öffentlich oder privat ist. Der Sichtschutz wird hier ebenso symbolisiert.

Es gibt – wie im Browser üblich – kein Kontextmenü.

Footer

Im Footer werden über mehrere Reiter verschiedenste Informationen zum aktuell ausgewählten Datensatz dargestellt. Über den kleinen Pfeil rechts aktivieren bzw deaktivieren Sie diesen.



1. Infobereich

Im Informationsbereich sehen Sie, wer auf den Datensatz zuletzt Zugriff hatte. Die Benutzer werden durch entsprechende Icons bzw. Ihre Avatare dargestellt. Durch einen Klick auf den User werden Ihnen seine Rechte angezeigt.

2. Logbuch

Im Reiter Logbuch sehen Sie die letzten Logeinträge zum Datensatz.

3. Historie

Die Historie können Sie ebenfalls über einen entsprechenden Reiter darstellen.

4. Dokumente

Über den Reiter Dokumente können Sie auf alle verknüpften Dokumente zugreifen.

5. Benachrichtigungen

Hier ist ersichtlich, wer die Benachrichtigungen zum Datensatz aktiviert hat.

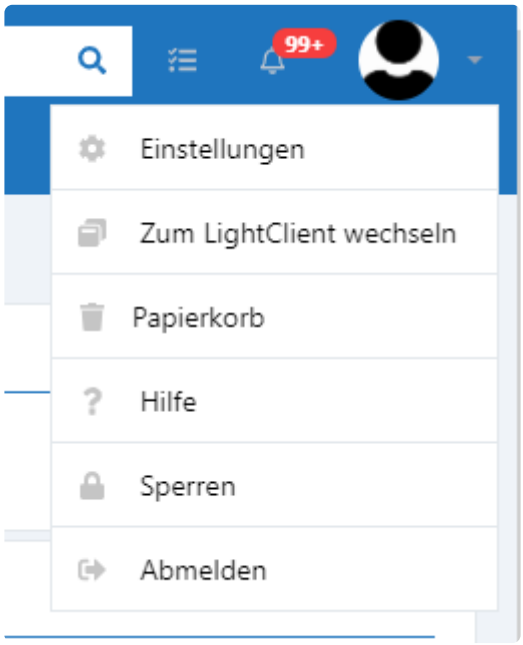
6. Password Resets

Es können auch getätigte Password Resets aufgelistet werden.

Benutzermenü

Das Benutzermenü finden Sie rechts oben im WebClient. Mit einem Rechtsklick auf den angemeldeten Benutzer wird dieses geöffnet.

Optionen im Benutzermenü



Einstellungen

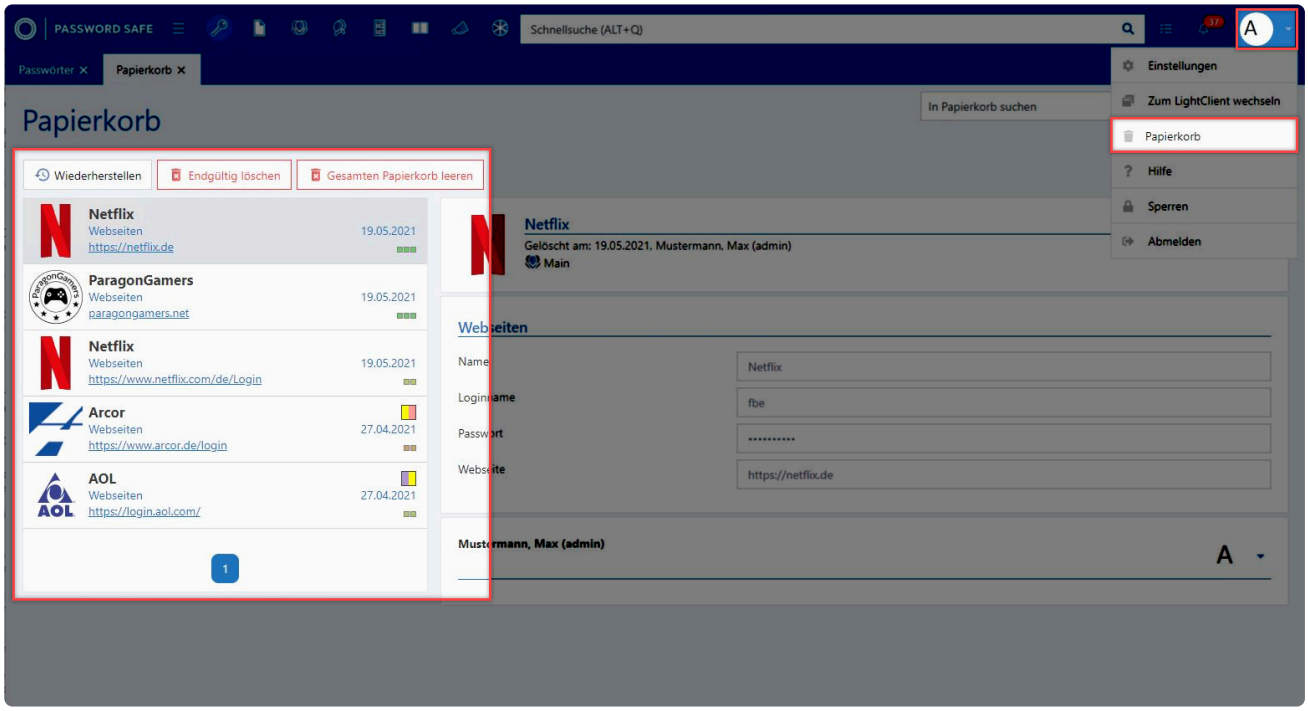
Alle möglichen Einstellungen können Sie in dem Kapitel **Einstellungen** einsehen.

Zu LightClient wechseln

Was der LightClient in der Webansicht zu leisten imstande ist, können Sie **hier** in Erfahrung bringen.

Papierkorb

Im Papierkorb werden alle gelöschten Passwörter angezeigt auf die der angemeldete Benutzer berechtigt ist



Hilfe

Mit einem Klick auf **Hilfe** werden Sie direkt auf die Dokumentationsseite von Password Safe weitergeleitet.

Sperren

Hierdurch wird der momentan angemeldet Benutzer gesperrt und muss, zum erneuten Nutzen des Webclients, lediglich sein Passwort eingeben.

Abmelden

Der angemeldet Benutzer wird abgemeldet. Zur Anmeldung sind nun wieder alle relevanten Informationen nötig.

Einstellungen

Die Einstellungen werden über das **Benutzermenü** aufgerufen. Es stehen Ihnen folgende Optionen zur Verfügung:

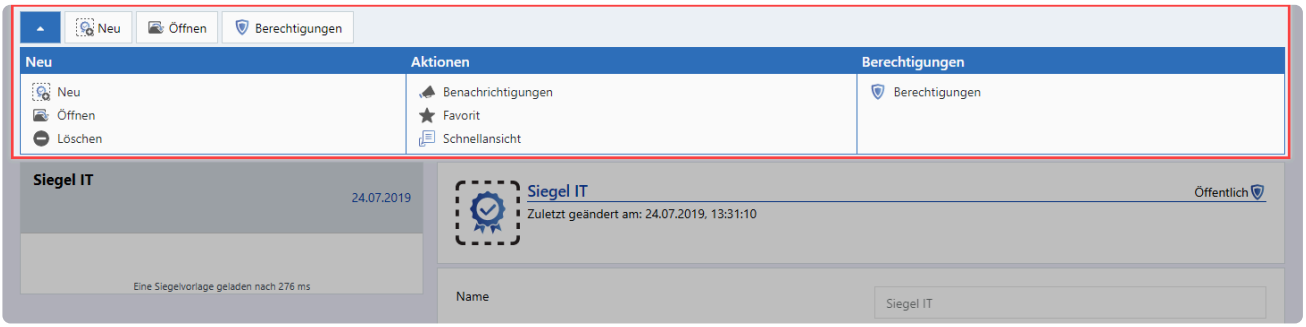
Sprache

Hier können Sie durch einen Klick **Deutsch** bzw. **Englisch** auswählen. Die Änderung erfolgt direkt und benötigt keinen Neustart des Browsers.

Extras

Siegelverwaltung

Hier verwalten Sie die Vorlagen für Siegel.

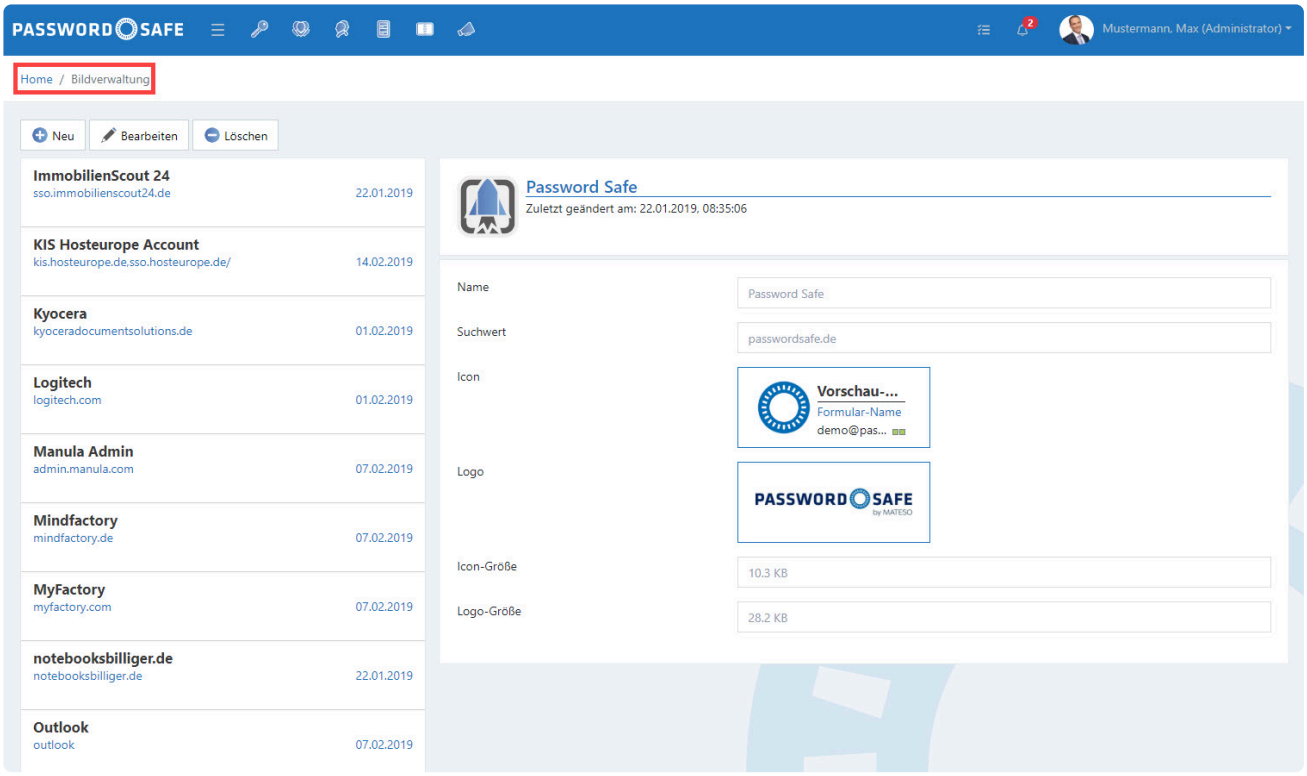


Tagverwaltung

Hier haben Sie die Möglichkeit die Tags zu verwalten.

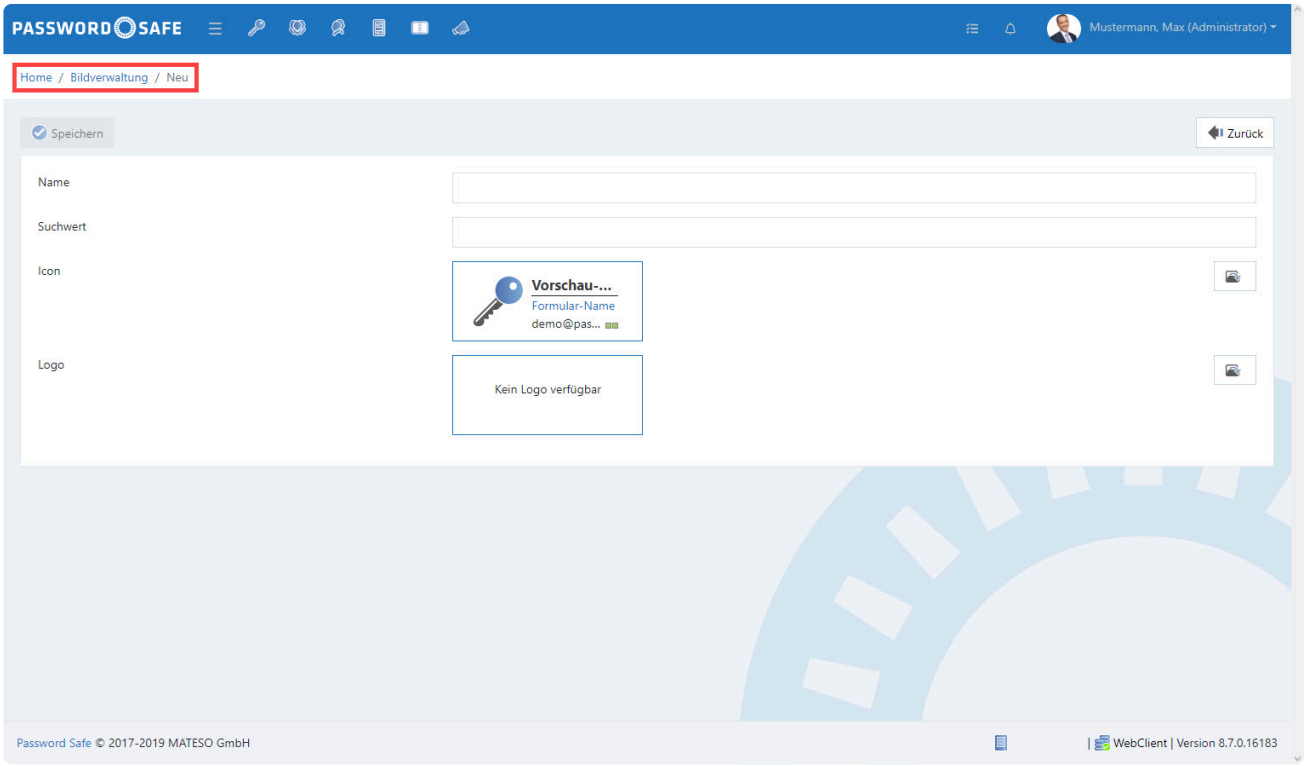
Bildverwaltung

Mit der Bildverwaltung können Sie die Icons und Logos verwalten.

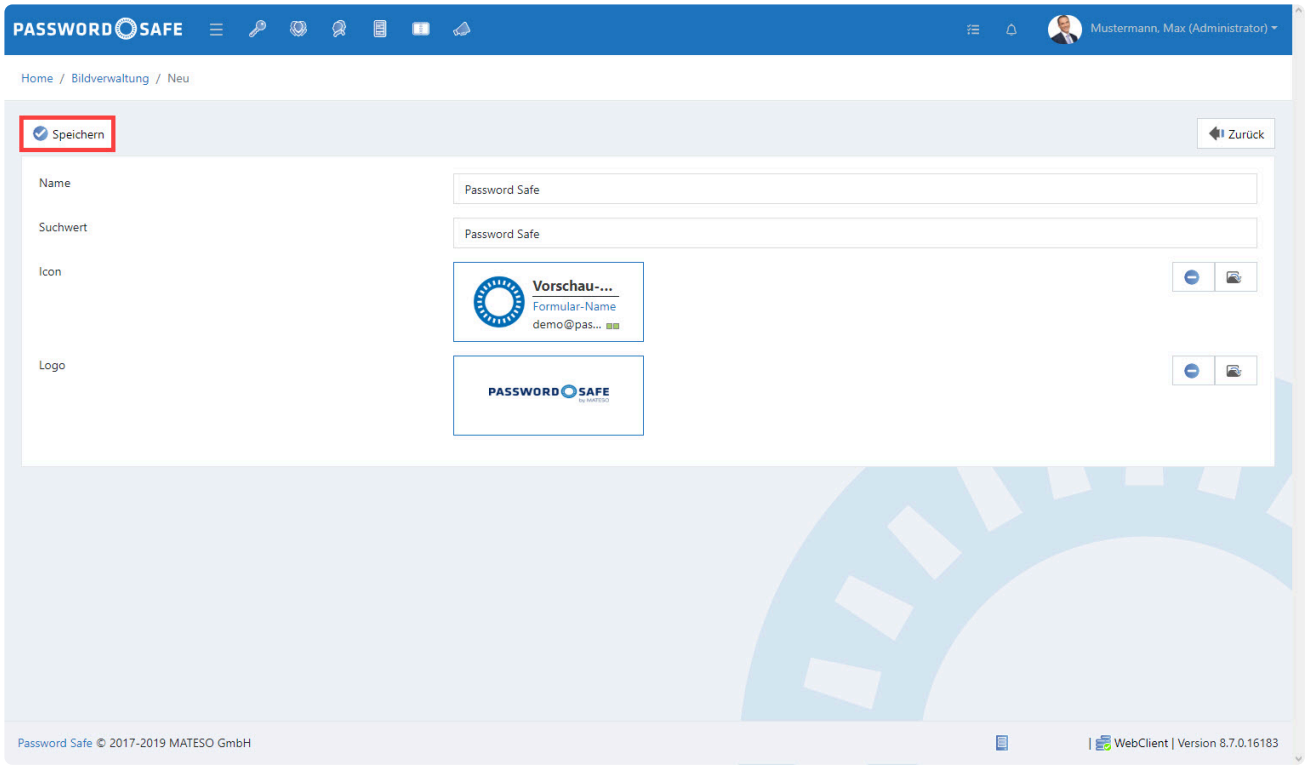


Hinzufügen von Icons und Logos

Mit einem Klick auf den **Neu-Button** öffnet sich eine Eingabemaske.

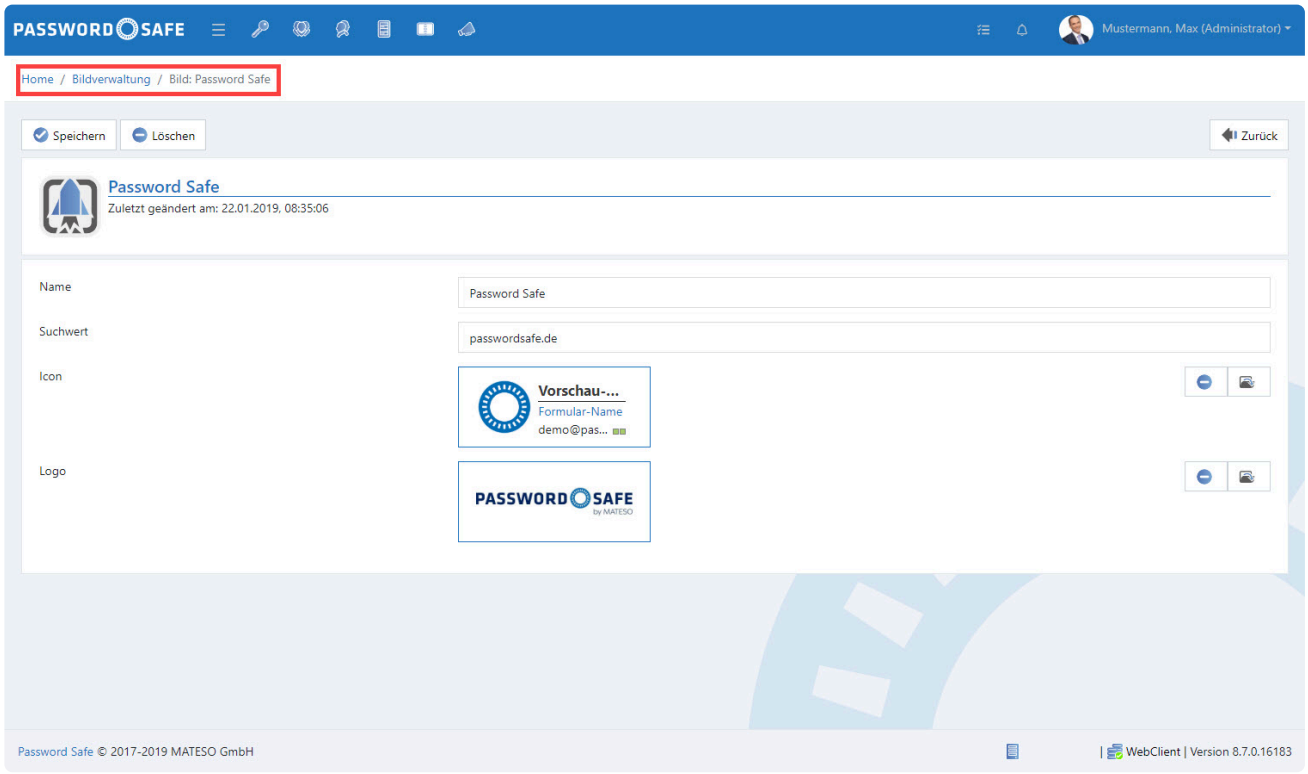


Speichern Sie nach dem Ausfüllen und Hochladen des Icons / Logos den Vorgang.



Bearbeiten / Löschen von Icons und Logos

Veraltete Icons / Logos können Sie bearbeiten oder sogar löschen.



Einstellungen

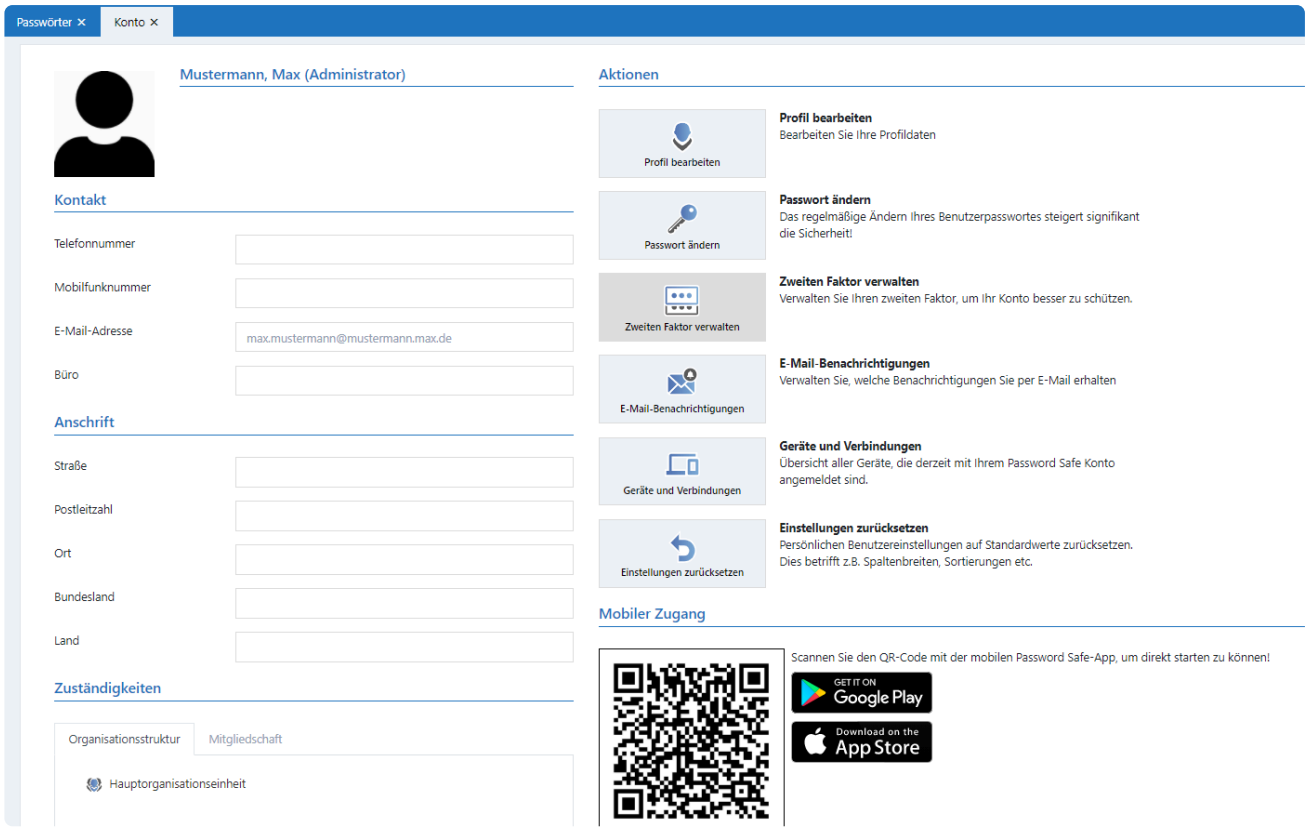
Unter diesem Menüpunkt verwalten Sie folgende Optionen:

- Globale Benutzerrechte
- Globale Einstellungen
- Benutzereinstellungen

Das Handling lehnt sich an das des Clients an. Weitere Informationen können Sie unter Globale Benutzerrechte bzw. Globale Einstellungen finden.
Folgende Einstellungen stehen am WebClient nicht zur Verfügung:

- Anpassbarer Fenstertitel
- Erlaubte Dokumentenerweiterungen
- Zwischenablage-Galerie
- Kategorie: Proxy

Kontoeinstellungen



Profil bearbeiten.

Diese Option ermöglicht Ihnen das Anpassen bzw Ändern der Benutzerinformationen.

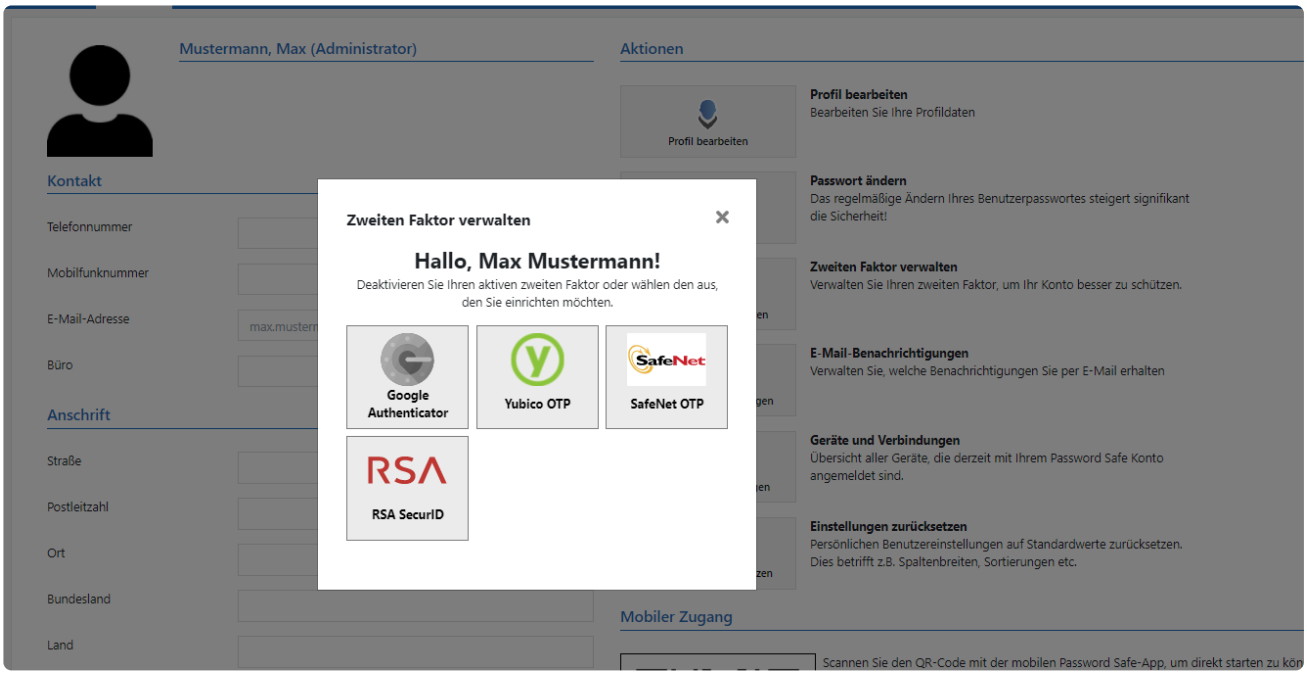
Passwort ändern

Sie ändern hier das Passwort des eingeloggten Benutzers.

Zweiten Faktor verwalten

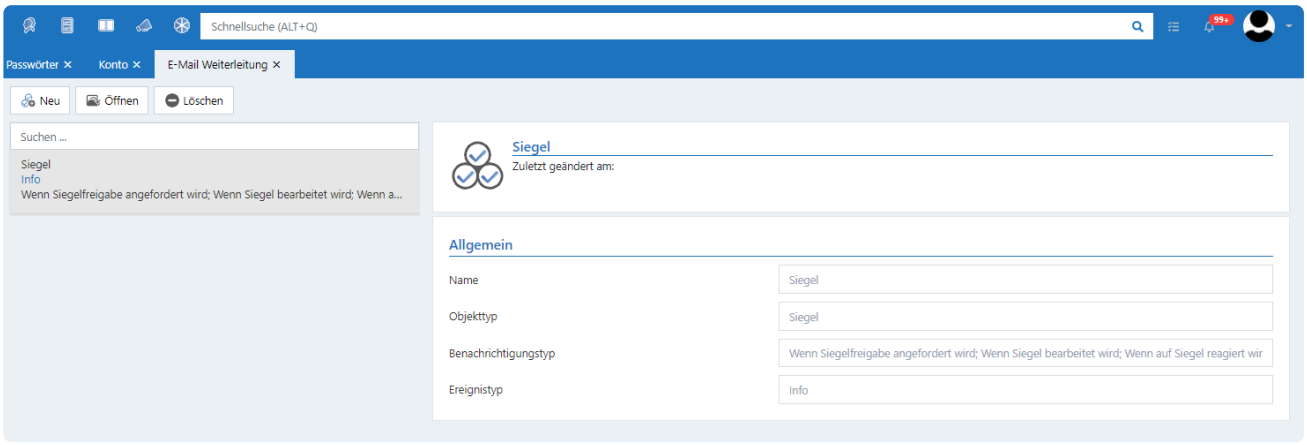
Die **Multifaktor Authentifizierung** bietet zusätzlichen Schutz durch einen zweiten Sicherheitsfaktor bei

der Anmeldung.



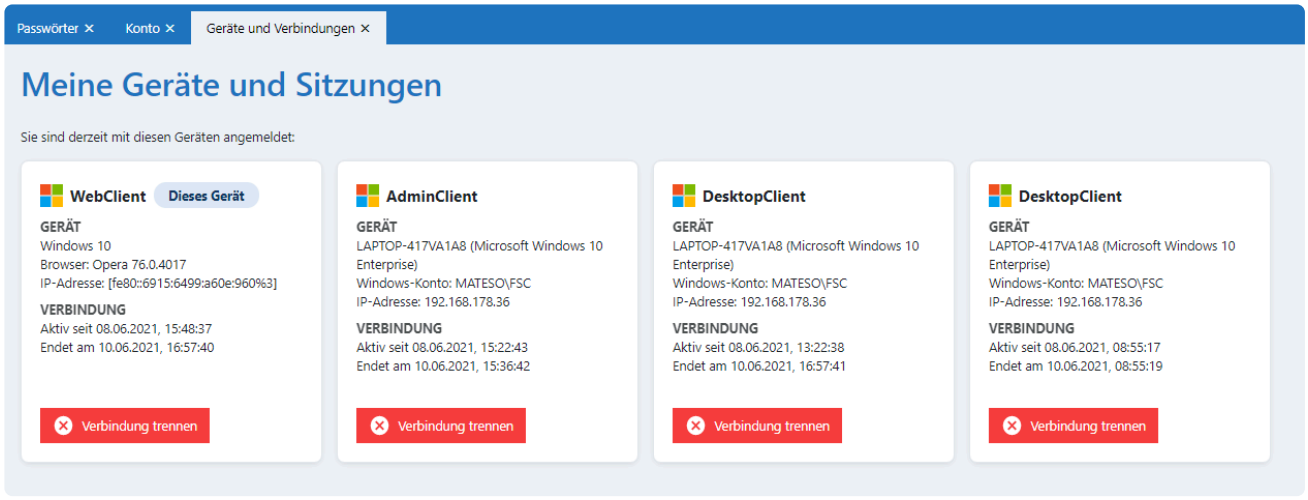
E-Mail-Benachrichtigungen

Hier können Sie Weiterleitungsregeln definieren. Eine Regel bestimmt, wann eine Benachrichtigung an das E-Mail-Postfach des angemeldeten Benutzers weitergeleitet werden soll.



Geräte und Verbindungen

Sie können sich hier alle aktiven Sitzungen des angemeldeten Benutzer anzeigen lassen.



Einstellungen zurücksetzen.

Hierüber werden alle Benutzereinstellungen zurückgesetzt.

Mobiler Zugang

Stellen Sie hier die Verknüpfung mit der App für die Version 8 her. Detaillierte Informationen findet Sie in der dazugehörigen **Dokumentation**.

Berechtigungs- und Schutzmechanismen

Sicherheit und Schutz am WebClient

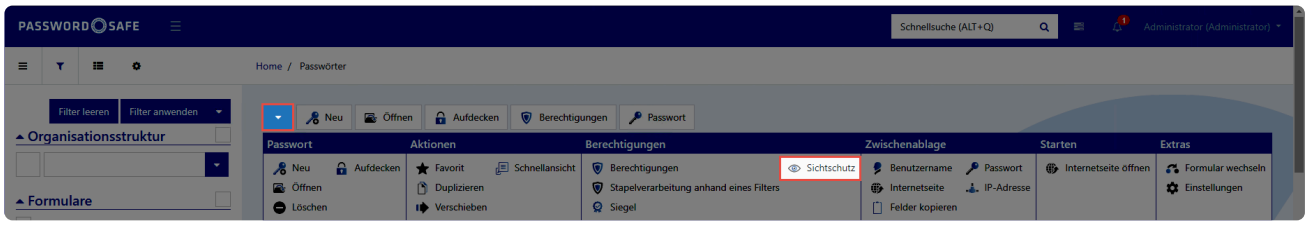
Wie auch am Client, können Sie am WebClient die Datensätze mit verschiedenen Mechanismen schützen. Auch die Berechtigungen auf Datensätze können Sie im WebClient verwalten. Bei der Entwicklung des WebClients wurde stets darauf geachtet, die Bedienung an die des Clients anzulehnen. Da der WebClient auf HTML basiert, ist es leider nicht möglich, den Client zu 100% identisch abzubilden. Daher kann sich die Bedienung dezent unterscheiden. Diese Abweichungen werden in diesem Kapitel verdeutlicht.

Berechtigungen und Rechtekonzept

Schutzmechanismen

Sichtschutz

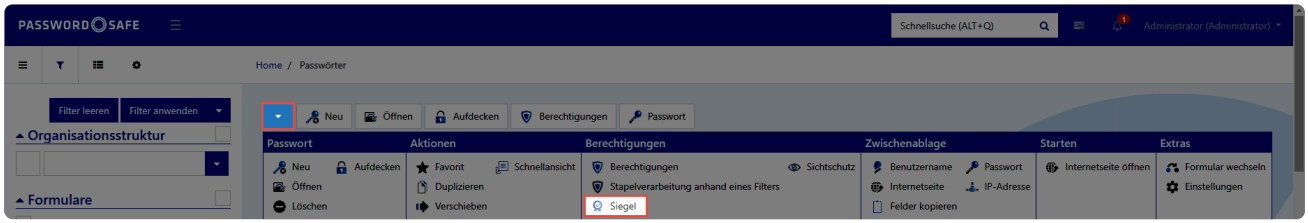
Der Sichtschutz folgt der bekannten Logik des Clients. Bezüglich der Funktion soll an dieser Stelle auf das Kapitel **Sichtschutz** verwiesen werden.
Marginale Unterschiede gibt es in der Bedienung. Bearbeiten Sie oder bringen Sie den Sichtschutz über einen Button im **erweiterten Menü** an.



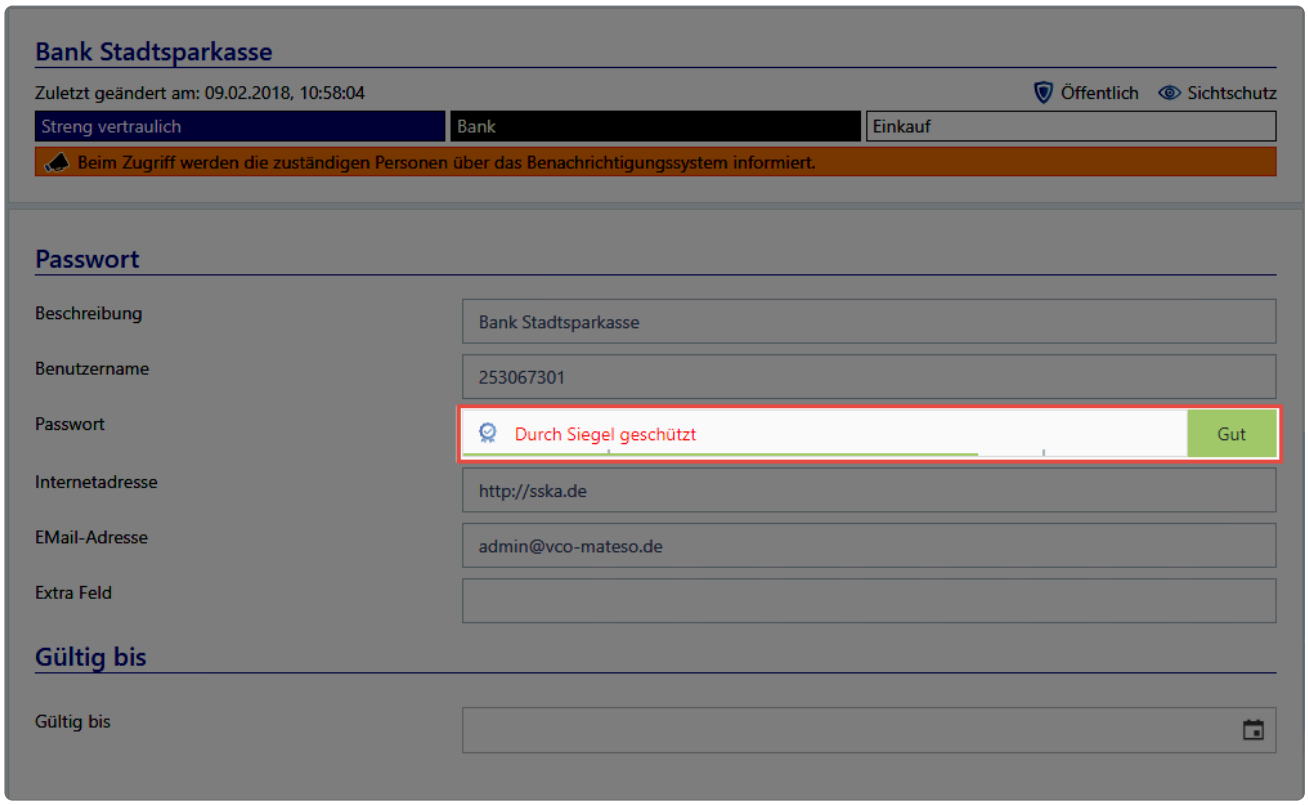
Der entsprechende Button wird nur dann dargestellt, wenn der angemeldete Benutzer ausreichende Rechte dafür hat.
Ist ein Datensatz mit einem Sichtschutz versehen, so wird das im Header des Passworts dargestellt.

Siegel

Auch die Siegel entsprechen bezüglich der Funktion der bekannten Logik des Clients. Im Kapitel **Siegel** finden Sie weitere Erläuterungen. Konfigurieren Sie die Siegel über eine Schaltfläche im **erweiterten Menü**.



Der Button wird nur für die User dargestellt, welche auch die Rechte zum Bearbeiten von Siegeln haben. Ist ein Datensatz versiegelt, so wird dies im Passwortfeld dargestellt.



Probleme mit der Serververbindung

Kann vom WebClient aus keine Verbindung aufgebaut werden, so kommen mehrere Ursachen in Frage:

Server nicht gestartet

Prüfen Sie zunächst ob der Anwendungsserver läuft.

Dienst nicht gestartet

Über die Diensteverwaltung von Windows prüfen Sie, ob der Dienst **Password Safe Service** gestartet ist.

Port nicht freigegeben

Geben Sie am Anwendungsserver den Port 11016 TCP frei.

CORS nicht konfiguriert

Stellen Sie sicher, dass die CORS Konfiguration durchgeführt wurde. Weitere Informationen dazu finden Sie im Kapitel Installation WebClient.

Mobile Geräte

Die neue Password Safe Mobile App – Mobil und einfach!

Mit der Version 8.10 haben wir die perfekte Ergänzung zum Client geschaffen: **Die Password Safe Mobile App**!
Die Password Safe Mobile App ermöglicht es jedem Benutzer sich durch ihre **komfortablen** Oberfläche zurechtzufinden.

Zur detaillierten Dokumentation der **Password Safe Mobile App**

Beachten Sie, dass ab der Version 8.10.0 die bisherige Version 7 App nicht mehr kompatibel ist.

Sicherheit ist unser Bestreben

Ganz egal, ob Sie mit einem Smartphone oder Tablet arbeiten, Sie profitieren auf allen iOS und Android Geräten von der höchstmöglichen Sicherheit. Alle Passwörter stehen Ihnen nicht nur auf dem mobilen Gerät zur Verfügung, sondern können auch automatisch in Webseiten übernommen werden. Sie können also hochkomplexe und somit sichere Passwörter verwenden und müssen sich diese nicht mehr merken. Die Password Safe Mobile App verbindet Sicherheit und Komfort. Zudem wird durch die Verwendung einer lokalen Datenbank sichergestellt, dass Sie auch dann auf Passwörter zugreifen können, wenn keine Internetverbindung vorhanden ist.

Funktionen

Die Funktionalitäten von **Passwortverwaltung**, **SSO**, **Synchronisation** und **Tabsystem** finden Sie noch umfangreicher und detaillierter in der dafür eigens geschaffenen **Dokumentation**.

Passwort Verwaltung

In der neuen **Password Safe mobile App** sind alle **Passwörter** sicher aufgehoben. Sie können nicht nur sicher verwahrt, sondern auch komfortabel strukturiert werden.

SSO

Das wichtigste Komfortmerkmal der Password Safe Mobile App ist die Möglichkeit, Passwörter direkt in Anmeldemasken anderer Apps bzw. Browserseiten einzutragen. Die Konfiguration und die richtige Verwendung finden Sie in den entsprechenden Kapiteln für **iOS** bzw. **Android**.

Synchronisation

Da der Datenaustausch zwischen mobiler Datenbank und der Server Datenbank automatisch im Hintergrund geschieht, müssen Sie sich um die Aktualität der Daten nicht mehr sorgen. Genauere Informationen zur Synchronisation erhalten Sie **hier**.

Tabsystem

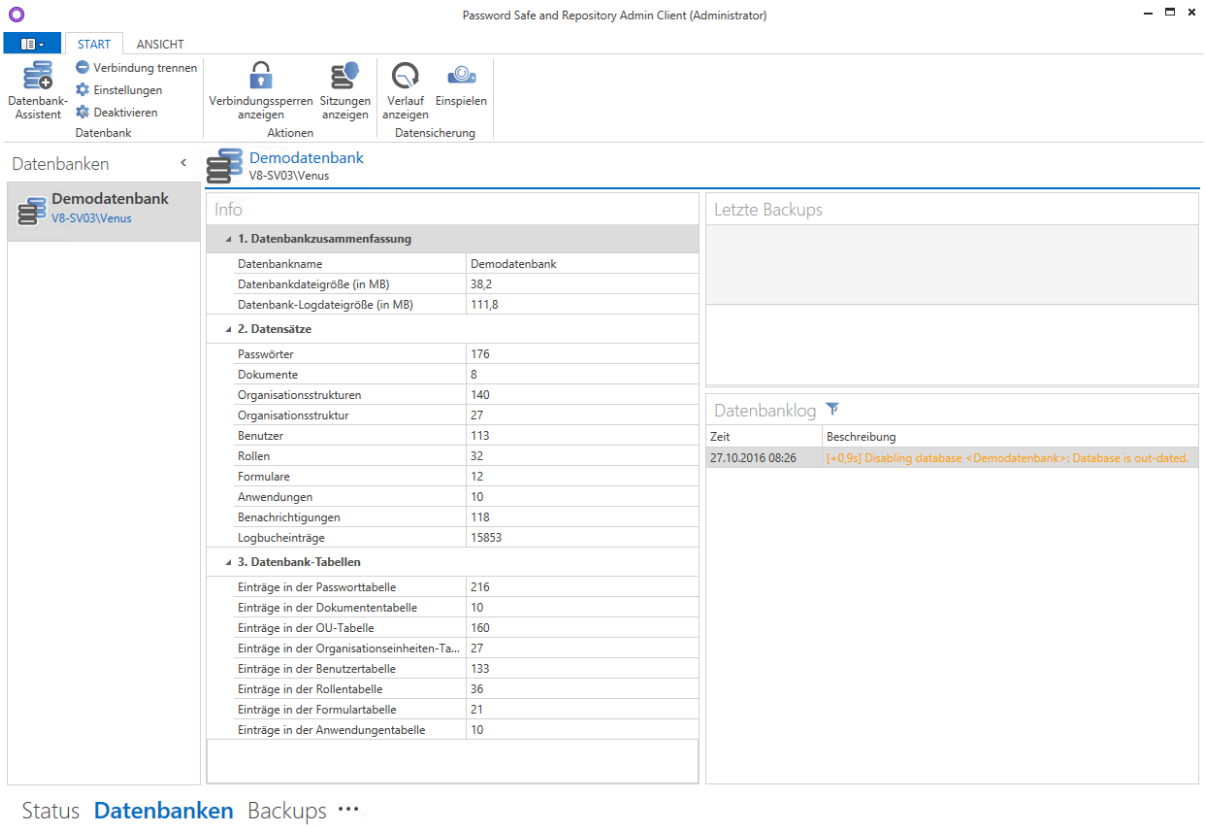
Mit dem neuen und vereinfachten Tabsystem ist die Handhabung für den einzelnen Benutzer unkompliziert und übersichtlich gestaltet worden. Die die Zugehörigkeit der Passwörter ist auf einen Blick ersichtlich. Den genauen Umgang mit dem Tabsystem finden Sie im Kapitel **Tabs**.

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. Nähere Informationen zur Installation des Admin Clients finden Sie in einem separaten Kapitel.

> Das Initialpasswort für den Admin Client lautet “admin”

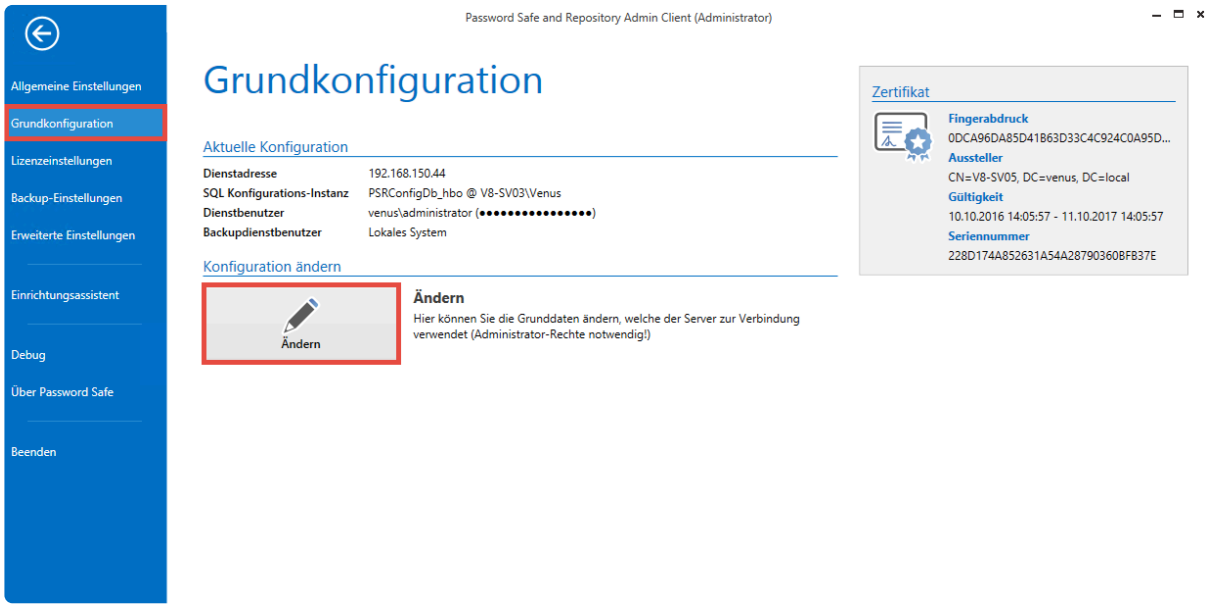


Der Serverdienst stellt die Schnittstelle zwischen dem Client und dem SQL-Server dar. Der Admin Client ist hierbei für die Konfiguration des Serverdienstes zuständig. Er ermöglicht die zentrale Verwaltung der Datenbanken, ohne auf den SQL-Server Zugriff zu haben. Dies ist in Bezug auf Organisation und Berechtigungen ein immenser Vorteil.

Grundkonfiguration

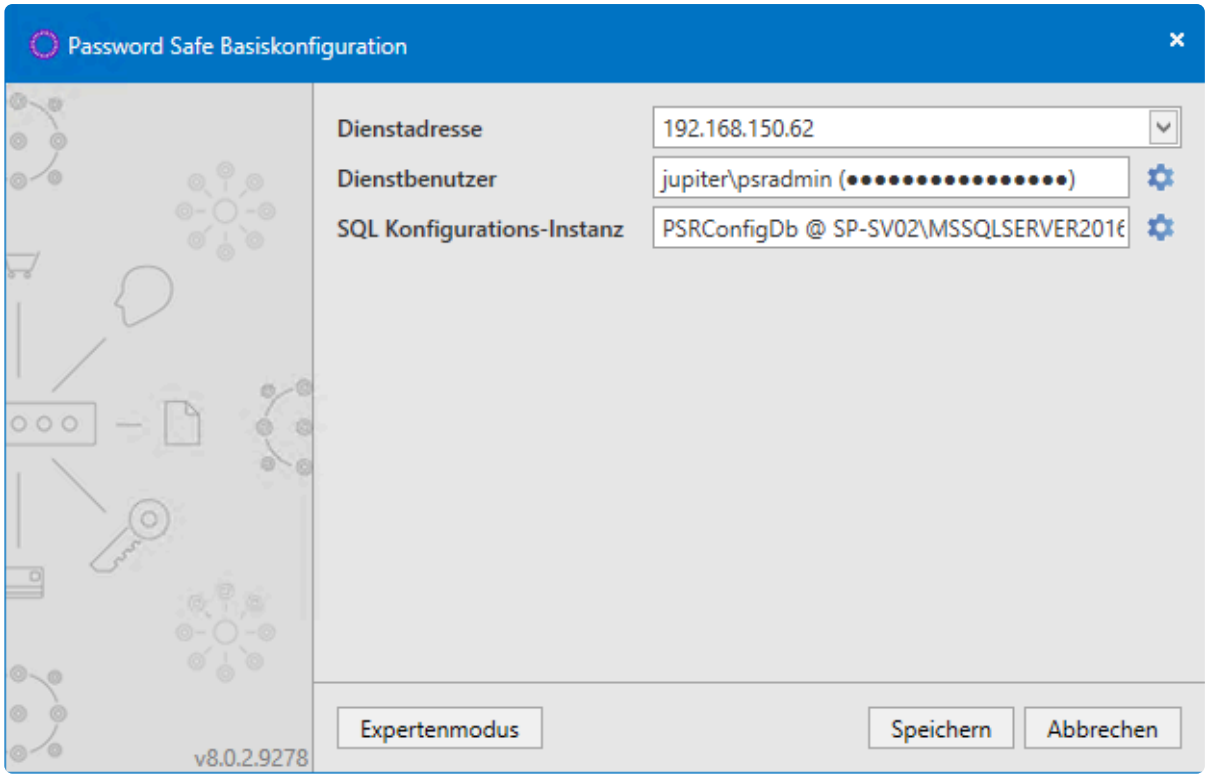
Was ist die Grundkonfiguration?

Innerhalb der Grundkonfiguration definieren Sie die Verbindung zum SQL-Server, bzw. zu den Datenbanken. Die Grundkonfiguration erscheint beim ersten Start des AdminClient und kann im Hauptmenü jederzeit wieder aufgerufen werden.



Die Grundkonfiguration

Zur Konfiguration steht ein eigener Assistent bereit:



Dienstadresse

Die Dienstadresse des SQL-Servers wählen Sie über das Drop Down Menü aus. Wählen Sie zwingend den Adapter aus, über den der Admin Client den SQL-Server auch ansprechen kann.

> ✻ Die Loopback Adresse 127.0.0.1 sollte hier nicht verwendet werden.

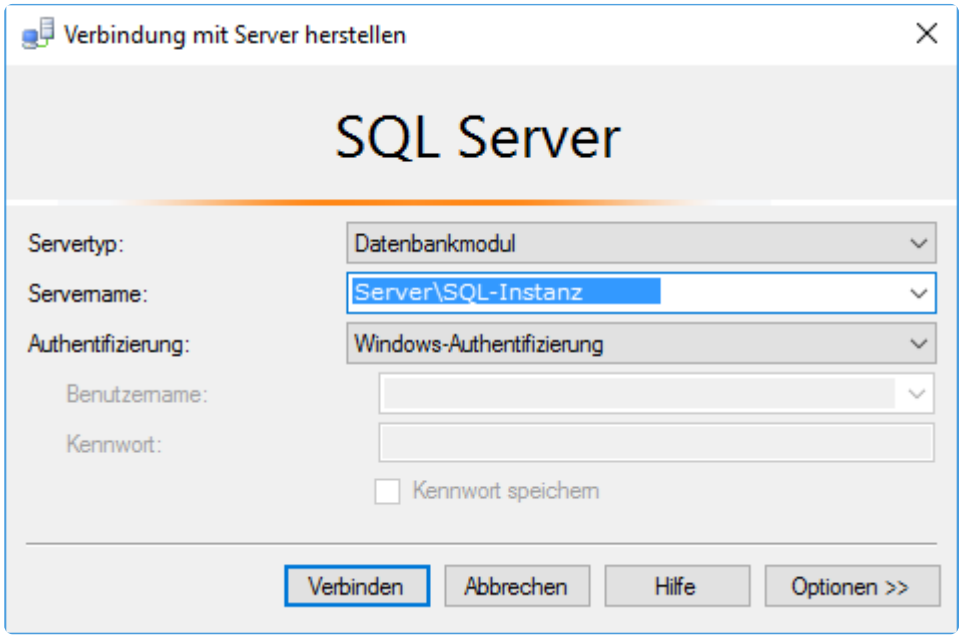
Dienstbenutzer

Legen Sie den Dienstbenutzer fest, der für den Start des Serverdienstes sowie des Backupdienstes vorgesehen ist. Über die Option “Lokales System verwenden” starten die Dienste mit dem Lokalen Systemkonto.

> ! Der hinterlegte Dienstbenutzer benötigt **lokale Administratorenrechte**, um den Server korrekt zu konfigurieren und Datenbanken zu erstellen.

SQL-Konfigurations-Instanz

Unter “SQL-Server Instanz” geben Sie den Datenbankserver inklusive der SQL-Instanz an. Der Einfachheit halber können Sie den Servernamen aus dem Loginfenster des SQL-Servers kopieren.



Selektieren Sie die Option “Dienstbenutzer”, geben Sie den User an, der sich am SQL Server anmeldet. Beachten Sie, 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” geben Sie den Name der Konfigurationsdatenbank an.

> ✻ Weitere Informationen über die verwendeten Benutzer finden Sie im Kapitel

Systemanforderungen Server.

Expertenmodus

Der Expertenmodus blendet zusätzliche Menüpunkte zur erweiterten Konfiguration ein:

Backupdienstbenutzer

Hier können Sie einen eigenen Benutzer zum Ausführen der Backups verwenden. Als Standard wird der Dienstbenutzer verwendet.

SQL Konfigurations-Instanz

Dieser Menüpunkt konfigurieren Sie im **Expertenmodus** über einen sogenannten **Connection String**.

Zertifikat

Unter diesem Punkt konfigurieren Sie das SSL-Verbindungszertifikat zum Schutz der Client Server Verbindung. Standardmäßig wird durch den AdminClient ein Zertifikat erzeugt. Sie haben aber auch die Möglichkeit ein eigenes auszuwählen. Nähere Informationen hierzu finden Sie im hierfür vorgesehenen Kapitel.

! 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.

Hostmodus erlauben

Der Hostmodus wird seit Version 8.13 nicht mehr unterstützt.

Caching aktivieren

Zur Verbesserung der Performance ist das Caching standardmäßig aktiv. Hierdurch wird am SQL Server für die Datenbanken der sogenannte SqlBroker registriert. Es wird folgendes gecached:

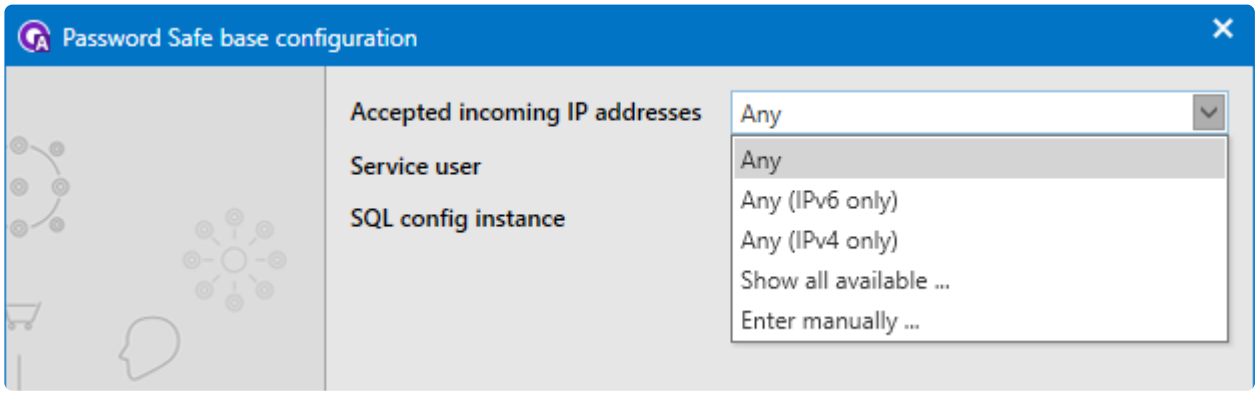
- die Rollen der einzelnen Benutzer
- die Struktur der Organisationseinheiten
- sämtliche Einstellungen

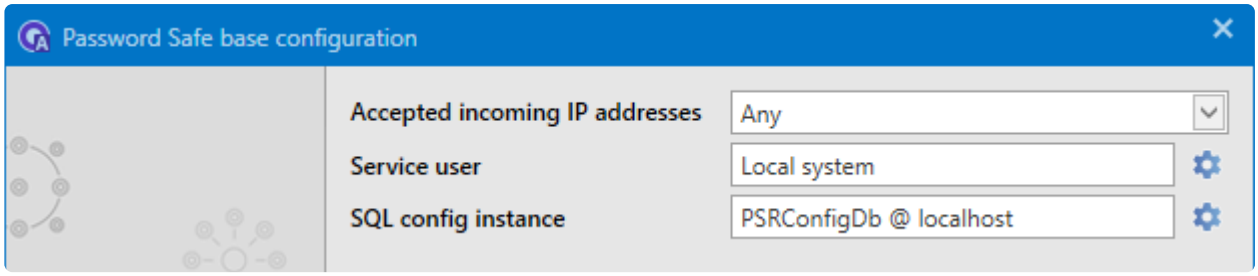
✻ Ändern Sie diese Option, müssen Sie den Serverdienst neu starten, damit die Änderung greifen kann.

Hier geht´s zurück zum Kapitel Erste Schritte

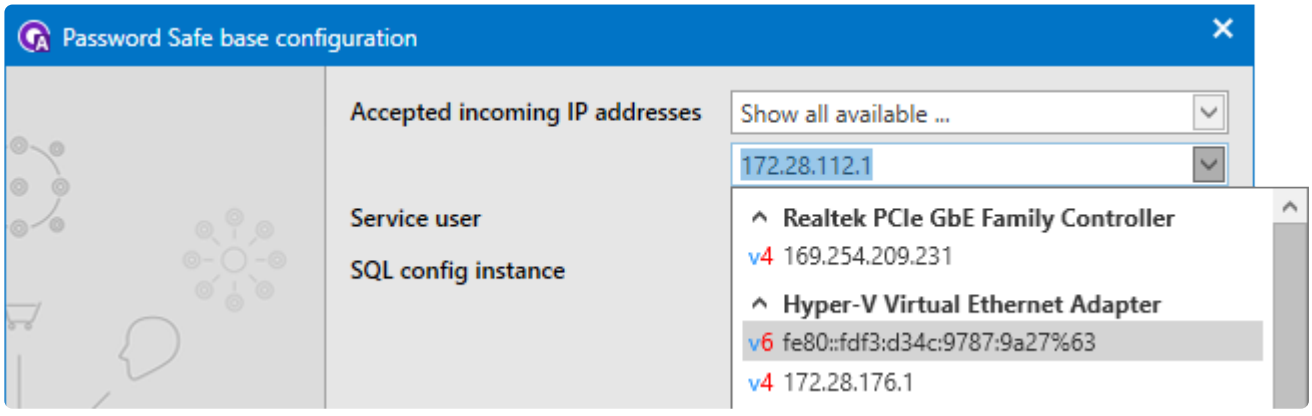
DualStack IP aktivieren (IPv4 + IPv6)

Wir haben jetzt eine DropBox-Steuerung für die IP-Adresskonfiguration. Der Standardwert für diese Konfiguration ist “Any”, diese Einstellung aktiviert auch den DualStack-IP-Modus. Die Einstellungen “Any (IPv6 only)” und “Any (IPv4 only)” setzen das ForceIpAddress-Attribut auf die jeweiligen ANY-Adressen “[::]” (für IPv6) und “0.0.0.0” (für IPv4).

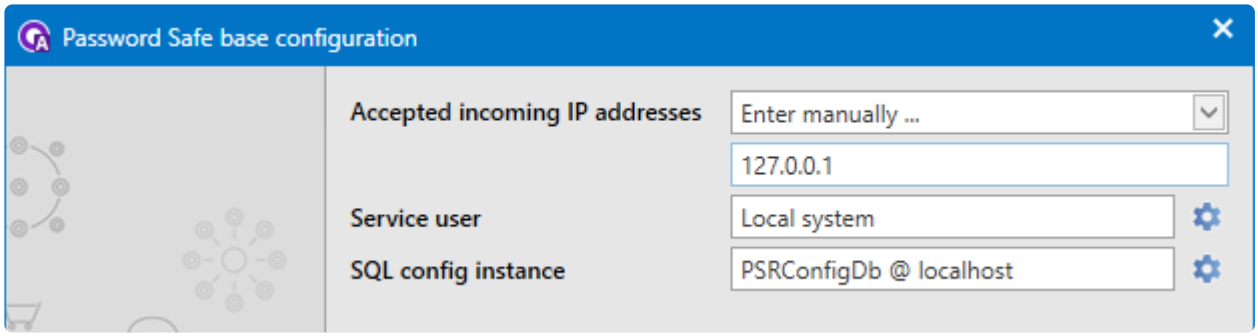


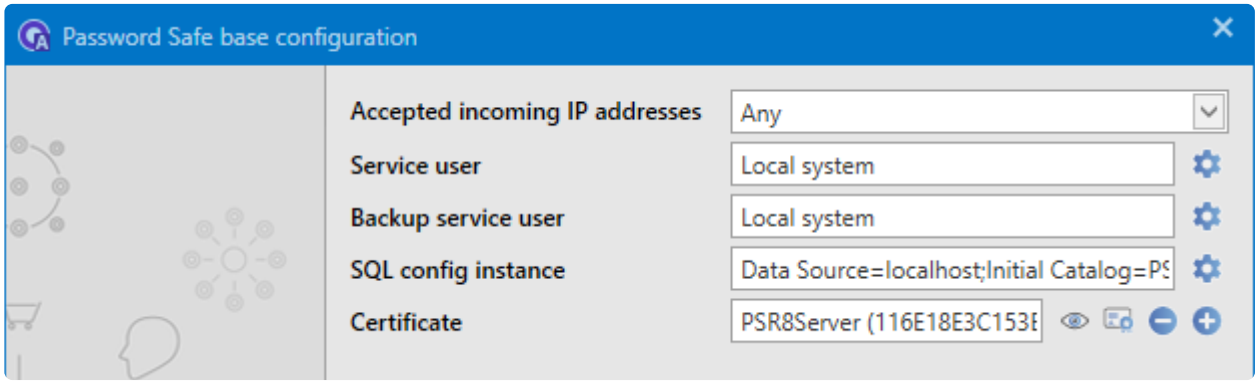


Die Option “Show all available …” fügt die bekannte DropDown-Steuerung hinzu, um eine der IP-Adressen des Systems auszuwählen.



Die Option “Manuell eingeben …” fügt das TextBox-Steuerelement für die bisher bekannte Konfiguration “Statische Dienstadresse” hinzu. Folgerichtig wurde das Feld “Statische Dienstadresse” aus den “Expertenoptionen” entfernt und die entsprechende Warnung ist ebenfalls verschwunden.


Password Safe base configuration
Accepted incoming IP addresses
Enter manually ...
127.0.0.1
Service user
Local system
SQL config instance
PSRConfigDb @ localhost


Password Safe base configuration
Accepted incoming IP addresses
Any
Service user
Local system
Backup service user
Local system
SQL config instance
Data Source=localhost;Initial Catalog=PS
Certificate
PSR8Server (116E18E3C153E

Zertifikate

Um die Sicherheit in Password Safe zu garantieren, kommen verschiedene Zertifikate zum Einsatz. Die Zertifikate sind für den reibungslosen Betrieb von Password Safe essentiell. Dementsprechend sollten Sie diese sorgfältig sichern.

Welche Zertifikate kommen zum Einsatz?

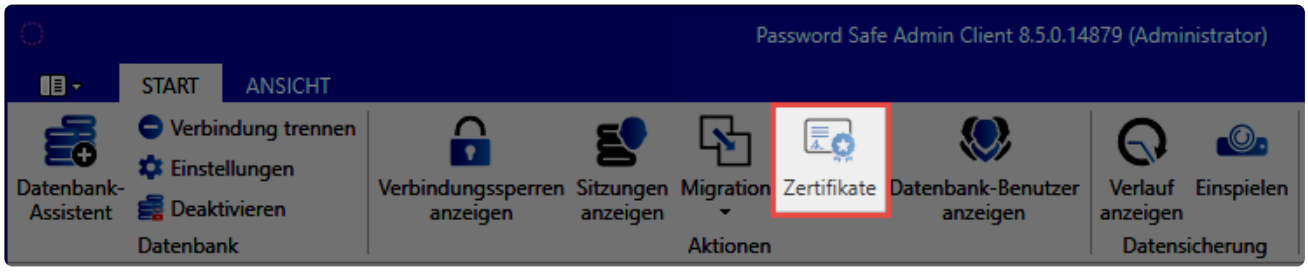
Auf die einzelnen Zertifikate wird in folgenden Kapiteln eingegangen:

- SSL Verbindungszertifikate
- Datenbank Zertifikate
- Master Key Zertifikate
- Discovery Service Zertifikate
- Passwort Reset Zertifikate

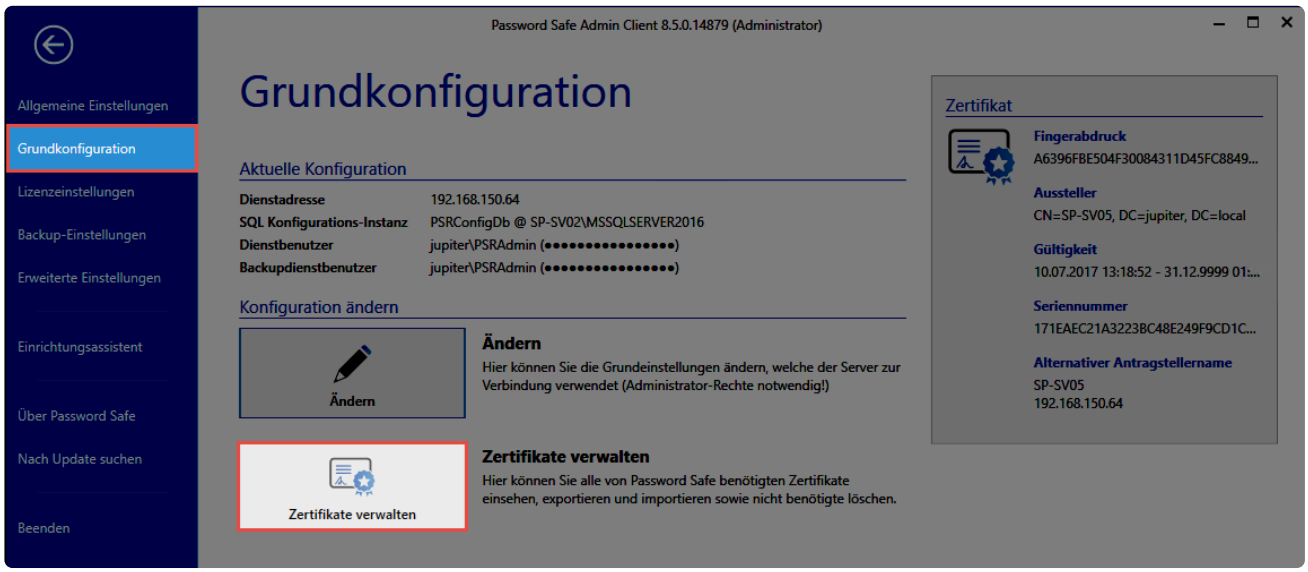
Aufruf Zertifikatsverwaltung

Sie öffnen die Zertifikatsverwaltung über zwei Wege.

Über die Ribbon verwalten Sie die Zertifikate datenbankspezifisch:



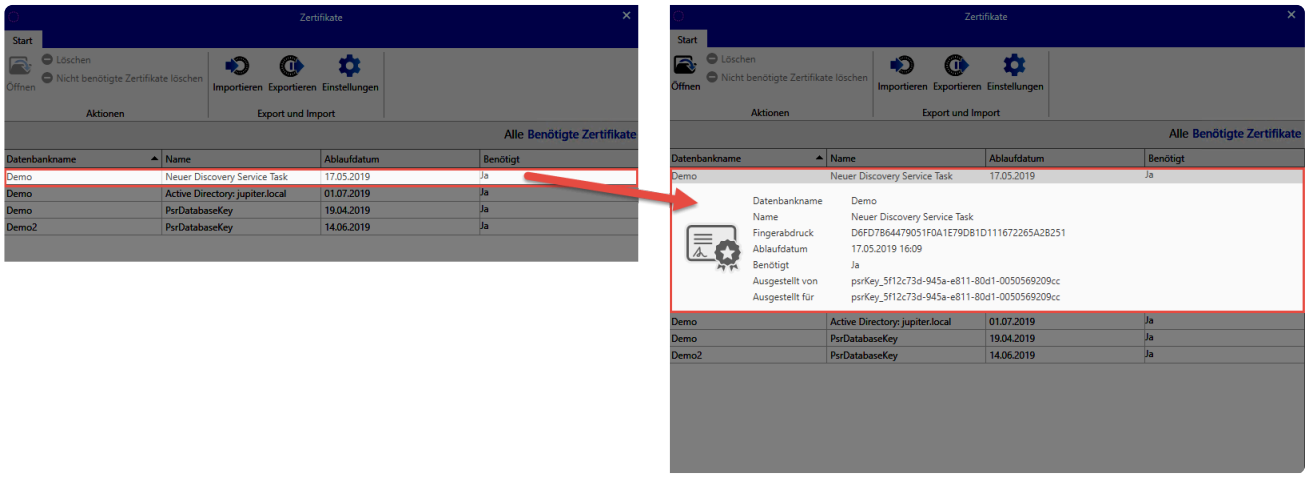
Im **Hauptmenü** starten Sie unter **Grundkonfiguration** die Zertifikatsverwaltung Datenbank-übergreifend:



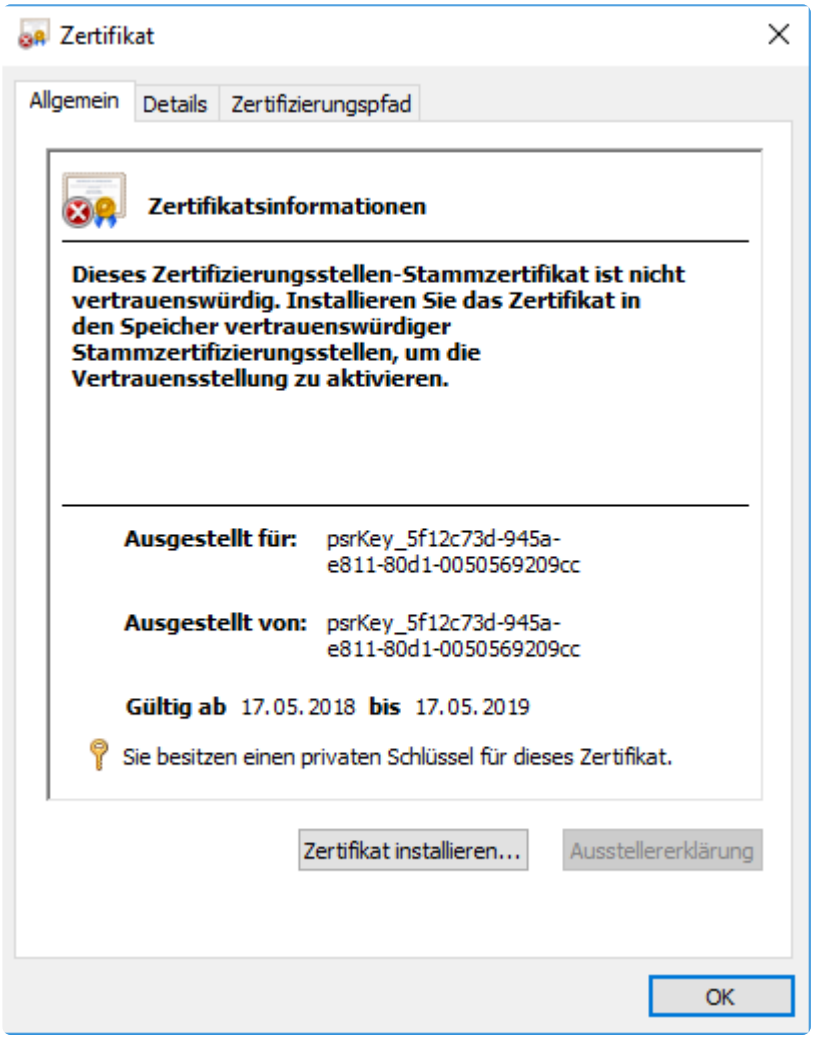
Die Bedienung der Zertifikatsverwaltung ist immer gleich. Der Unterschied liegt alleine darin, ob die Zertifikate pro Datenbank oder für alle Datenbanken angezeigt werden.

Prüfen vorhandener Zertifikate

Nach dem Öffnen der Zertifikatsverwaltung werden alle Password Safe spezifischen Zertifikate angezeigt. Durch einen Klick auf ein Zertifikat werden weiterführende Informationen dargestellt.

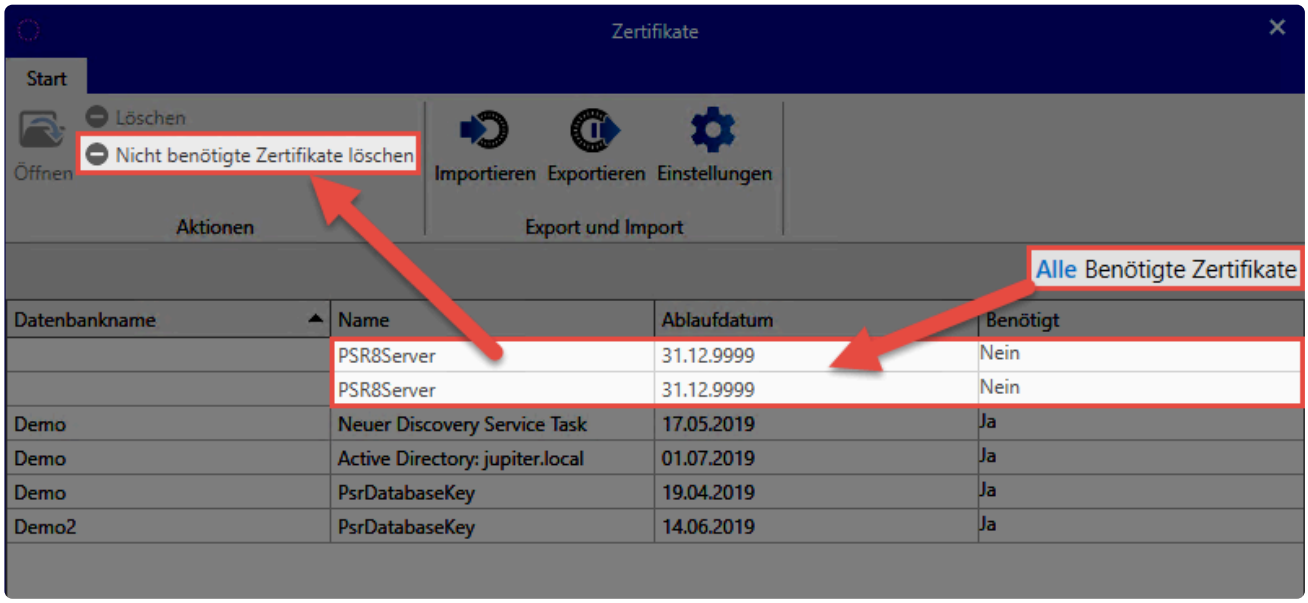


Durch einen Doppelklick auf ein Zertifikat öffnet sich die Windows Zertifikatsverwaltung für noch detailliertere Informationen.



Benötigte Zertifikate / Löschen nicht benötigter Zertifikate

In der Übersicht werden zunächst nur die Zertifikate angezeigt, die in Verwendung sind und somit benötigt werden. Über einen Klick auf **Alle** werden zusätzlich auch nicht benötigte Zertifikate eingeblendet. Beispielsweise durch Testinstallationen kann es dazu kommen, dass auf der Maschine veraltete Zertifikate liegen. Diese löschen Sie über den entsprechenden Button in der Ribbon.



Import von Zertifikaten

Über den *Import*-Button binden Sie zuvor gesicherte Zertifikate in die Installation ein. Hierfür geben Sie lediglich die gewünschte .pfx-Datei sowie deren Passwort an.

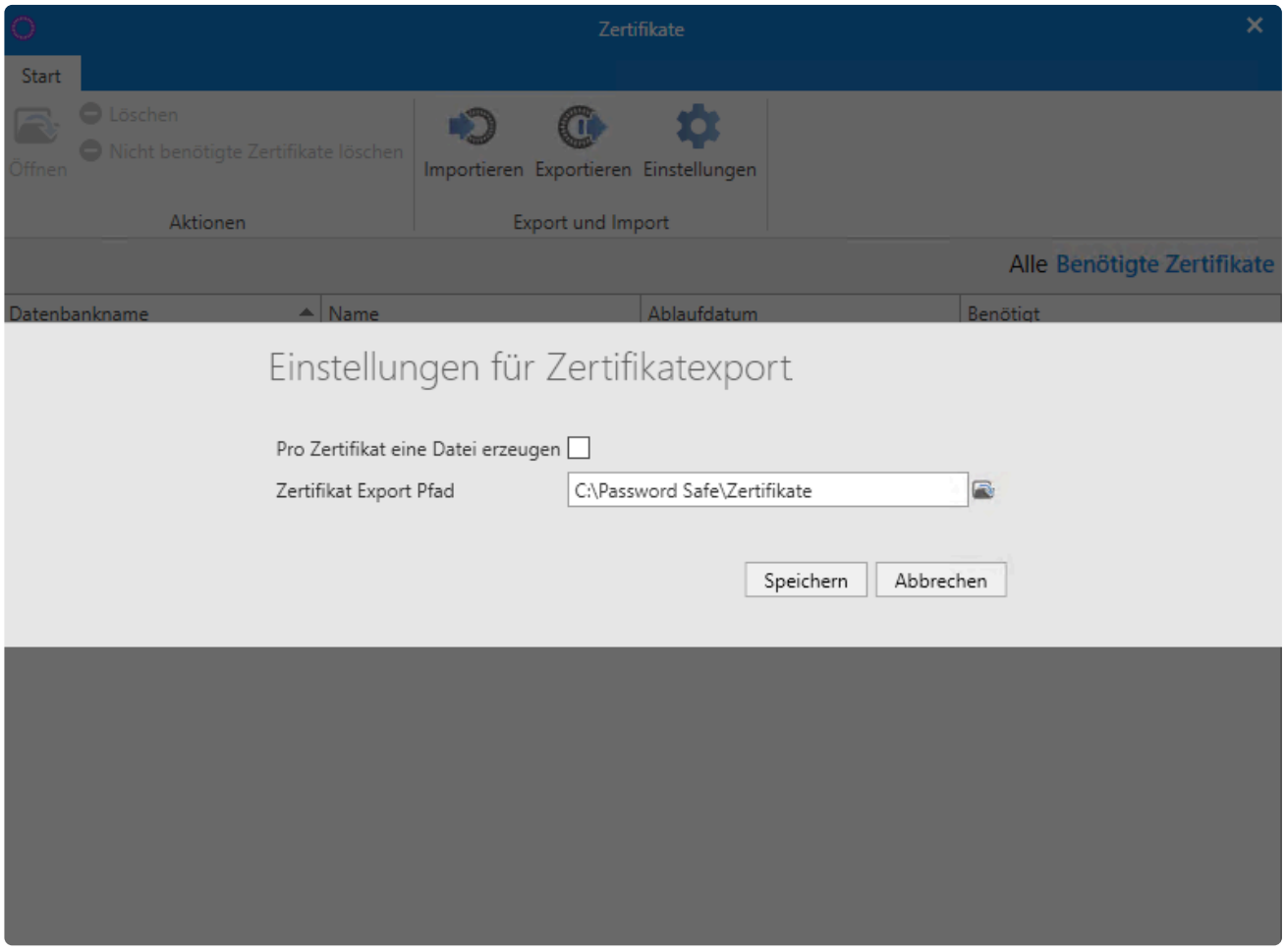
Export von Zertifikaten

Über einen Klick auf **Exportieren** sichern Sie die relevanten Zertifikate. Vergeben Sie hierfür zunächst ein Passwort. Haben Sie über **Einstellungen** noch keinen Speicherort hinterlegt, wird dieser vorab abgefragt.

> SSL-Verbindungszertifikate werden nicht mit aufgeführt und auch nicht gesichert. Diese können Sie bei Bedarf neu erstellen.

Einstellungen

In den **Einstellungen** legen Sie fest, ob jedes Zertifikat in einer eigenen Datei gespeichert werden soll. Ist diese Option nicht aktiv, werden alle relevanten Zertifikate in einer Datei gesichert. Zusätzlich wird in den Einstellungen der Speicherort festgelegt.



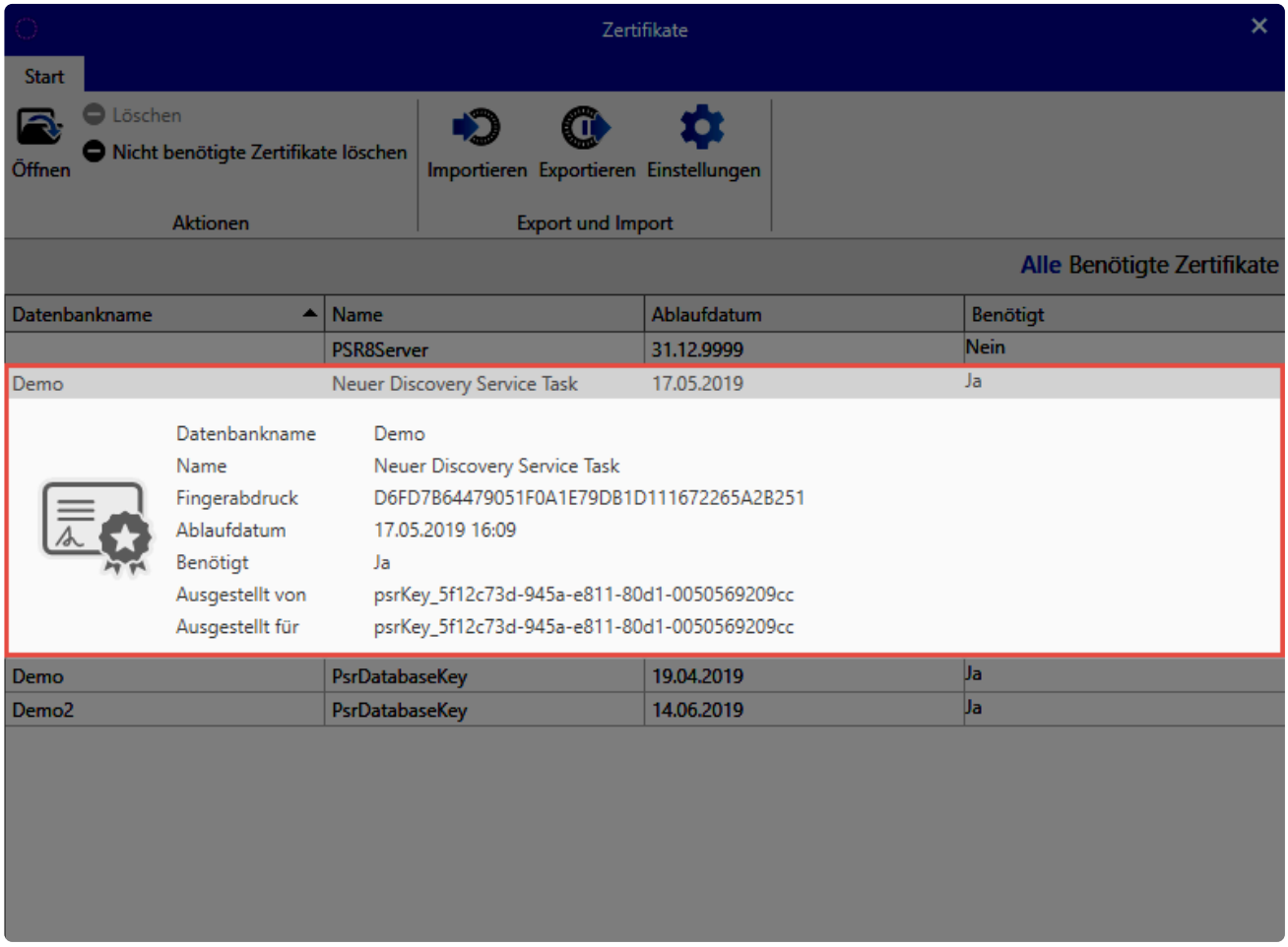
Sicherung von Zertifikaten über Backups

Sollen die Zertifikate zyklisch und automatisch gesichert werden, so ist das über das Backup System möglich. Weiterführende Informationen finden Sie im Kapitel Backup Verwaltung.

Discovery Service Zertifikate

Was ist das Discovery Service Zertifikat?

Wird ein Discovery Service erstellt, wird ein zugehöriges Zertifikat erzeugt:



✻ Das Discovery Service Zertifikat können Sie **nicht** durch ein eigenes Zertifikat ersetzen.

✻ Die **Zertifikate für den Discovery Service** haben ein Ablaufdatum. Dies wird jedoch nicht geprüft. Diese Zertifikate müssen also nicht erneuert werden.

! Verschieben Sie die Datenbank auf einen anderen Server, müssen Sie das Discovery Service Zertifikat **zwingend mit übertragen**!

Export und Import des Zertifikats

Wie Sie das Zertifikat sichern und wieder einbinden, erfahren Sie im Kapitel Zertifikate.

SSL Verbindungszertifikate

Was ist das SSL Verbindungszertifikat?

Die Verbindung zwischen den Clients und dem Server wird mittels SSL-Zertifikaten gesichert. Hier wird auf die **aktuellsten Verschlüsselungsstandards TLS 1.2 und TLS 1.3** zurückgegriffen. Sie können über den Server ein Zertifikat erstellen, aber auch über eine CA ein bereits bestehendes Zertifikat 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 erstellen Sie die Datenbanken. Währenddessen wird pro Datenbank ebenfalls ein eigenes Zertifikat erzeugt. Daher muss der **Dienstbenutzer lokaler Administrator** oder **Domänenadministrator** sein, da die Rechte zum Speichern in den Zertifikatsstore fehlen.

Aufbau der Zertifikate

Folgende Informationen gelten sowohl für das **Password Safe Zertifikat** als auch für **eigene Zertifikate**:

Alternativer Antragsteller

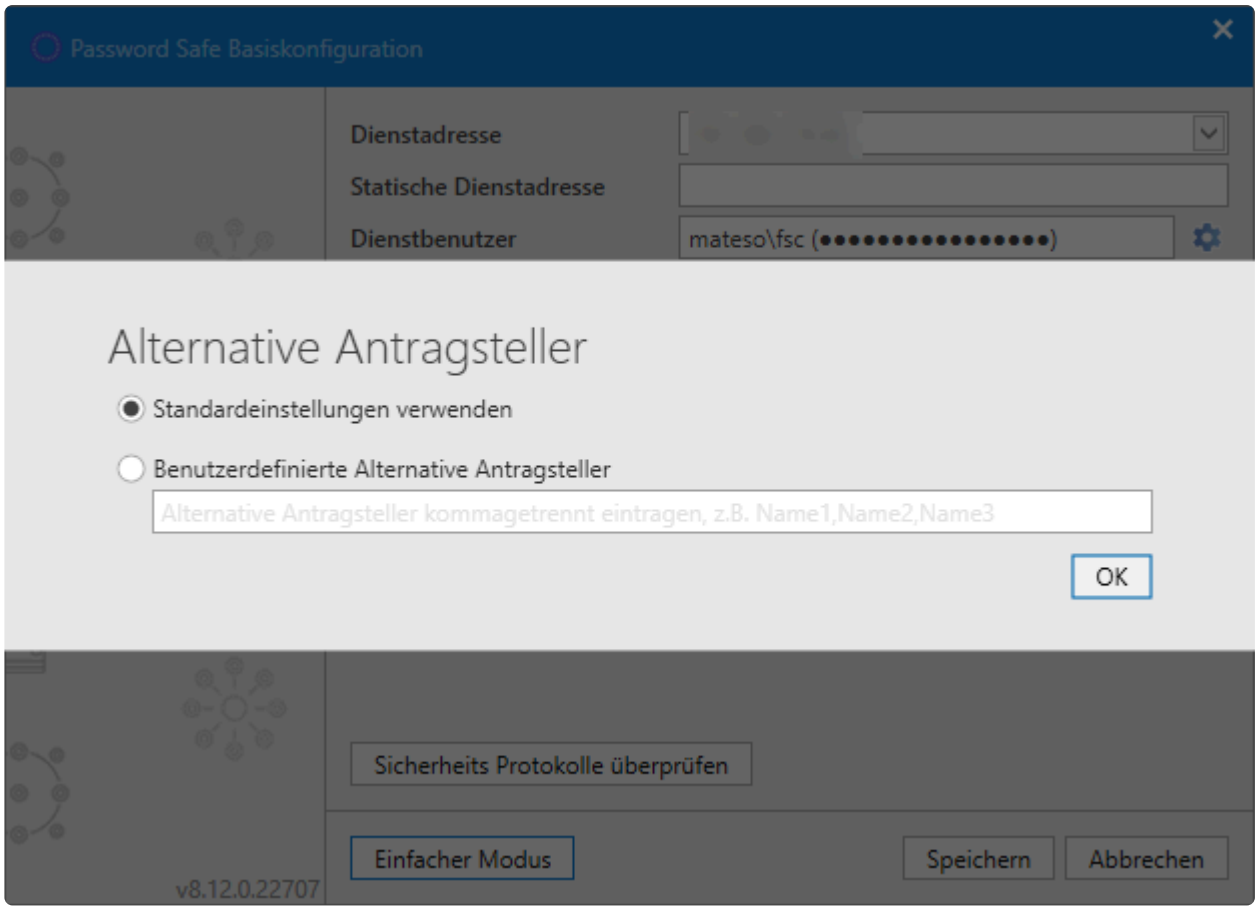
Die Kommunikation zwischen Client und Server kann nur auf dem Weg erfolgen, welcher im Zertifikat beim alternativen Antragsteller hinterlegt ist. Das Password Safe Zertifikat nimmt daher alle IP-Adressen des Servers sowie den Hostname auf. Beim Erstellen eines eigenen Zertifikats sollten Sie also ebenso diese Informationen unter dem alternativen Antragsteller hinterlegen.

Alle Informationen, auch die IP Adresse, werden als DNS-Name hinterlegt.

Nutzung des Password Safe Zertifikats

Die Bezeichnung des PSR Zertifikats ist **PSR8Server**. Erstellen können Sie dies über die Grundkonfiguration in der AdminConsole. Das Zertifikat liegt lokal unter:
lokaler Computer -> eigene Zertifikate -> Zertifikate

Beim Erstellen eines neuen Zertifikates haben Sie die Möglichkeit die Standardeinstellungen zu verwenden oder weitere alternative Antragsteller zu hinterlegen:



Das Zertifikat ist nach Erstellung bis zum Jahr 9999 – und somit endlos gültig. Aus diesem Grund gibt es kein Ablaufdatum zu beachten.

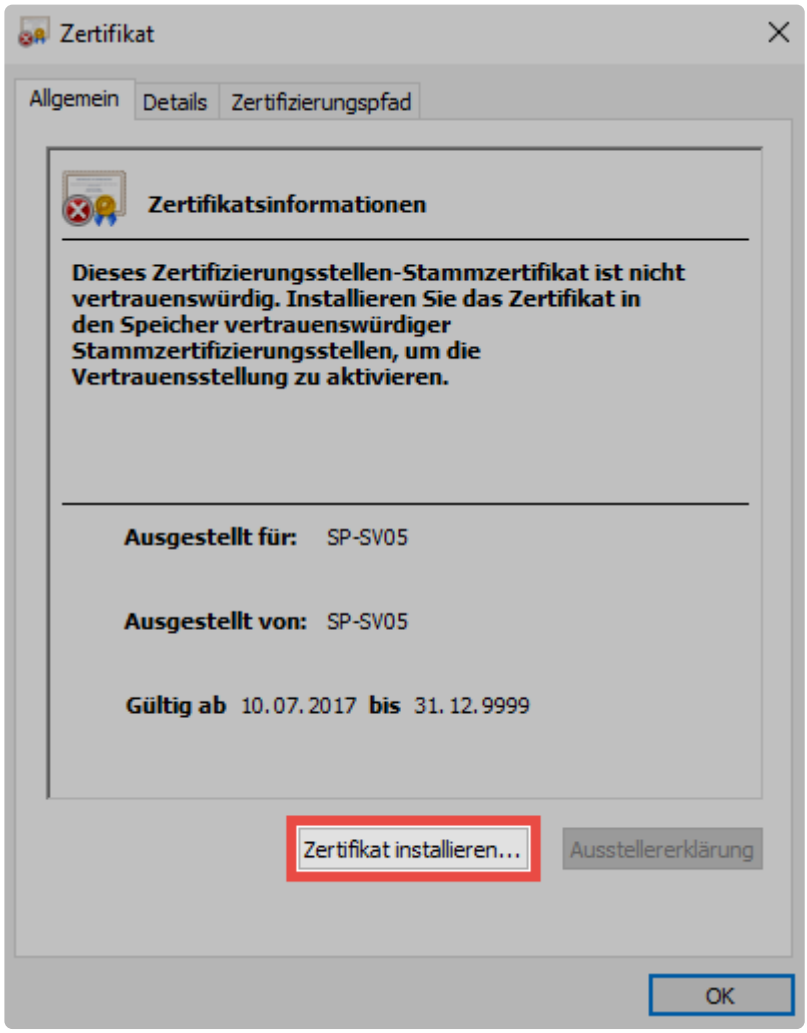
Verteilen des Password Safe Zertifikats

Um dem Zertifikat zu trauen, exportieren Sie dieses am Server und importieren Sie dieses danach den den Clients. Wählen Sie hier folgenden Speicher aus:
lokaler Computer > vertrauenswürdige Stammzertifizierungsstellen -> Zertifikate

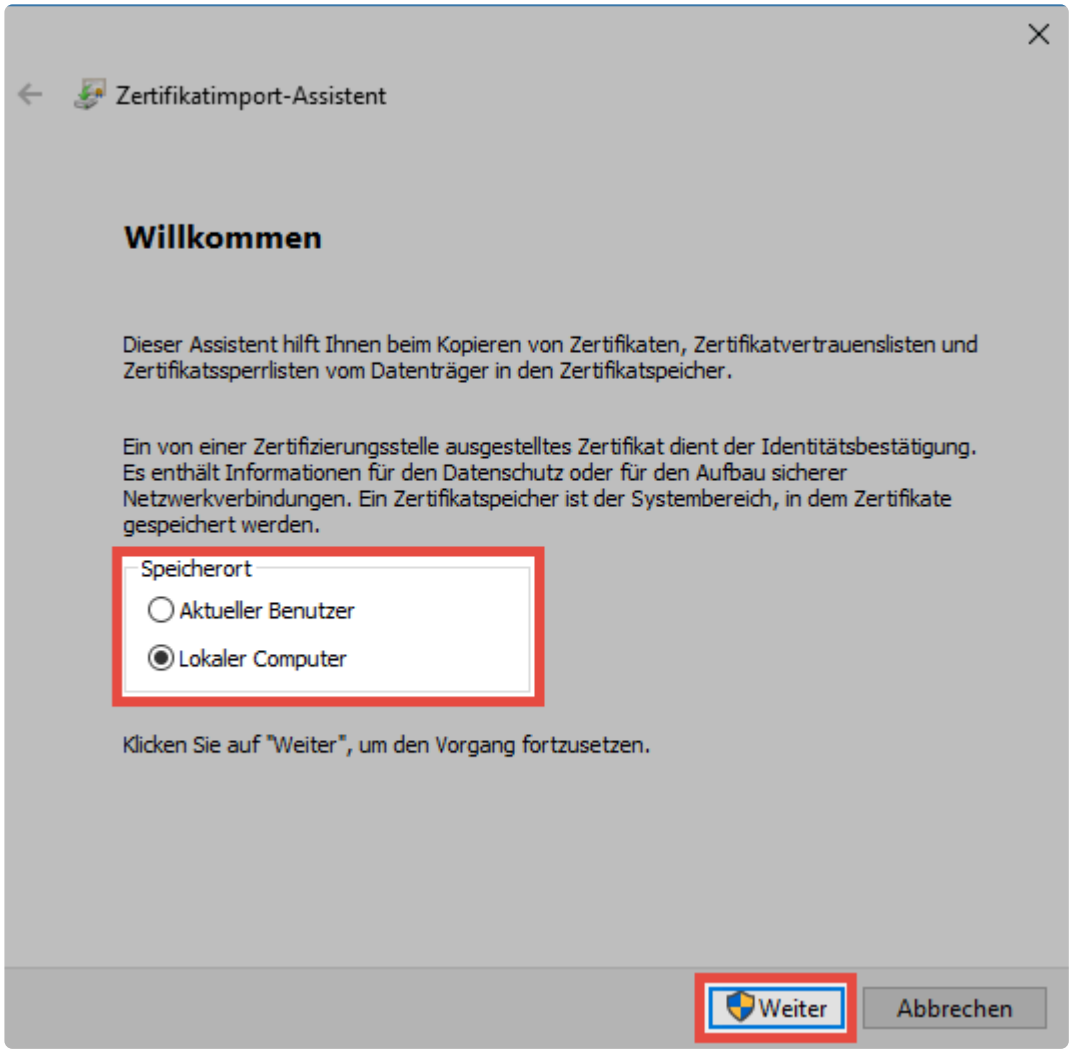
Das Zertifikat können Sie sowohl über Gruppenrichtlinien verteilen als auch ausrollen.

Manuelles Importieren des Password Safe Zertifikats

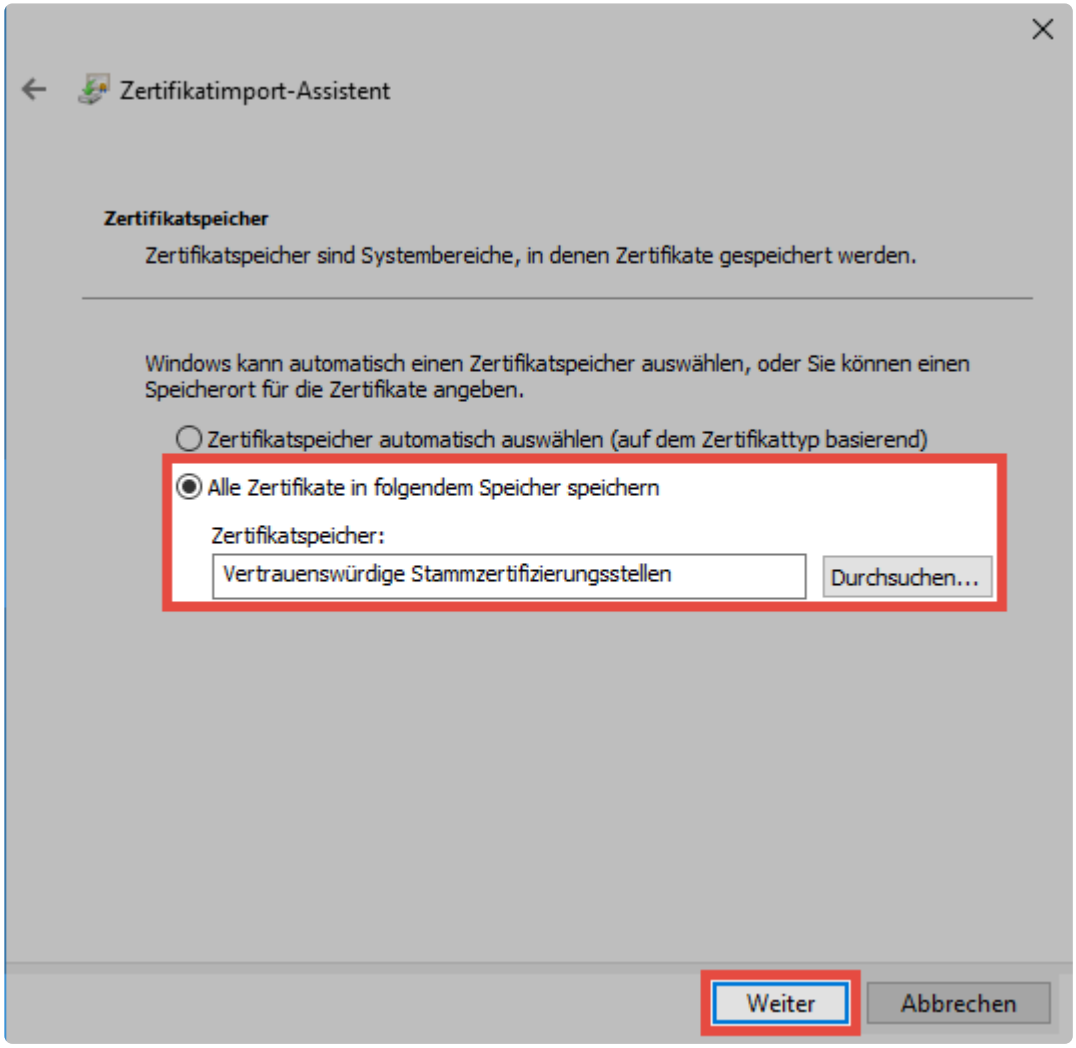
Wird das Password Safe Zertifikat nicht ausgerollt, so besteht auch die Möglichkeit, das Zertifikat manuell zu importieren. Öffnen Sie die Zertifikatsinformationen. In der Warnmeldung steht hierfür die Schaltfläche **Show server certificate** bereit. Wählen Sie im folgenden Dialog die Option **Zertifikat installieren…**.



Es öffnet sich der **Zertifikatimport-Assistent** in welchem Sie zunächst **Lokaler Computer** auswählen.



Im nächsten Schritt wählen Sie den Speicher “Vertrauenswürdige Stammzertifizierungsstellen” manuell aus.



Abschließend bestätigen Sie die Installation nochmals.

> Der am Betriebssystem angemeldete Benutzer benötigt Rechte, um Zertifikate erstellen zu können.

Nutzung eines eigenen Zertifikats

Ist bereits eine CA vorhanden, können Sie auch ein eigenes Zertifikat nutzen. Wählen Sie dieses innerhalb der Grundkonfiguration aus. Beachten Sie, dass hier ein Server-Zertifikat zur SSL-Verschlüsselung verwendet wird. Konfigurieren Sie die CA so, dass alle Clients dem Zertifikat trauen. Halten Sie daher den Zertifizierungspfad ein.

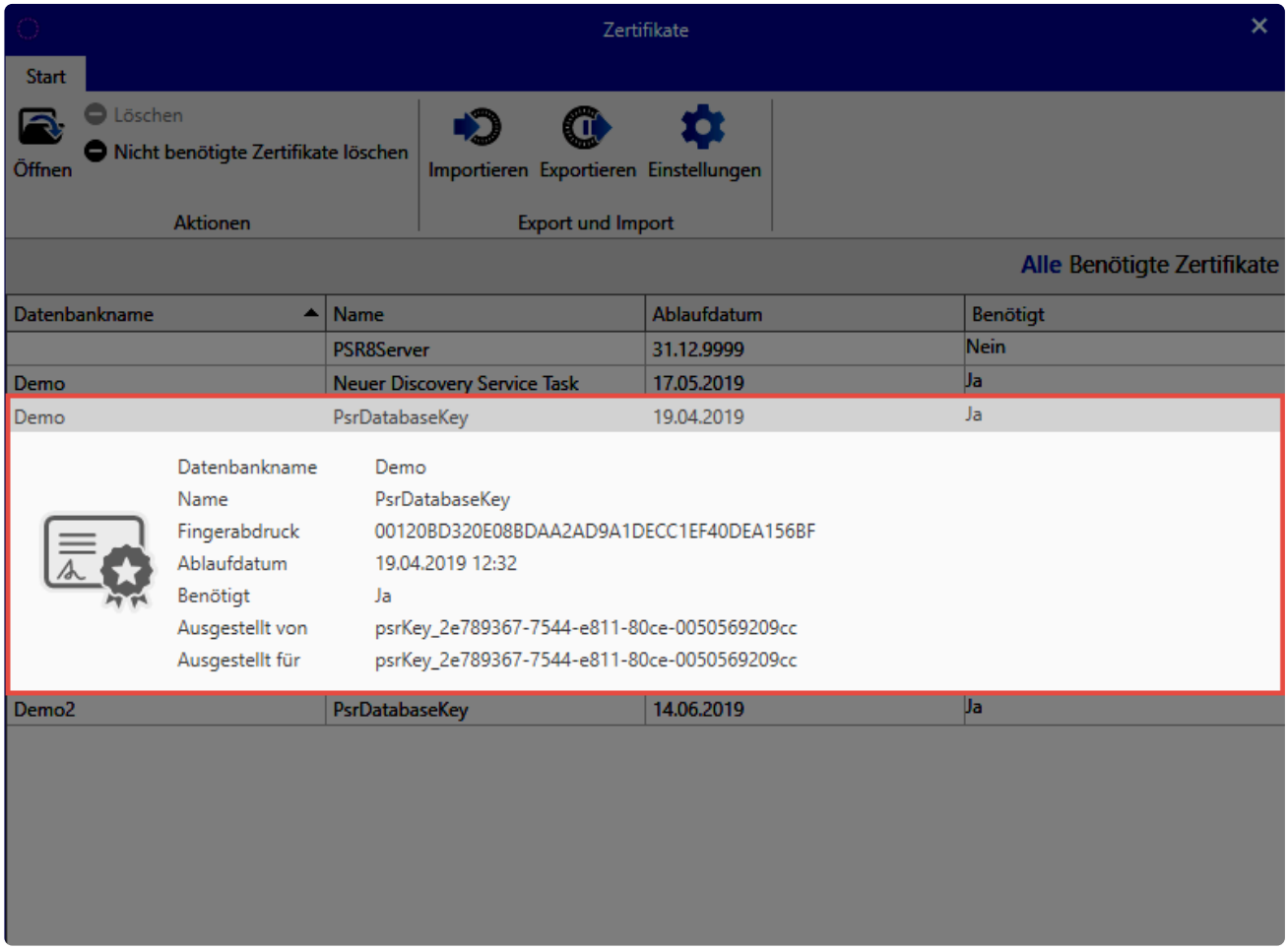
Wildcard Zertifikate

Wildcard Zertifikate werden leider nicht unterstützt. Theoretisch wäre die Verwendung zwar möglich, wir können jedoch bei der Konfiguration keine Hilfestellung bieten. Daher erfolgt der Einsatz von Wildcard Zertifikaten auf Ihre Verantwortung.

Datenbank Zertifikate

Was ist das Datenbank Zertifikat?

Pro Datenbank wird ein eigenes Zertifikat erstellt. Dieses trägt den Namen **psrDatabaseKey**:



Das Datenbank Zertifikat **verschlüsselt nicht die Datenbank**. Vielmehr wird es verwendet, um in folgenden Fällen Passwörter verschlüsselt vom Client zum Server zu übertragen:

- Erstellung eines WebViewers per Task
- Erstellen eines Masterkey-geschützen AD Profils
- Login von Benutzern, welche im Masterkey Modus aus dem AD importiert wurden

Das Datenbank Zertifikat können Sie **nicht** durch ein eigenes Zertifikat ersetzen.

Das Ablaufdatum des Datenbank Zertifikats wird nicht geprüft. Sie müssen das Zertifikat nicht erneuern.

> ! Soll die Datenbank auf einen anderen Server verschoben werden, müssen Sie das Zertifikat **zwingend mit übertragen**!

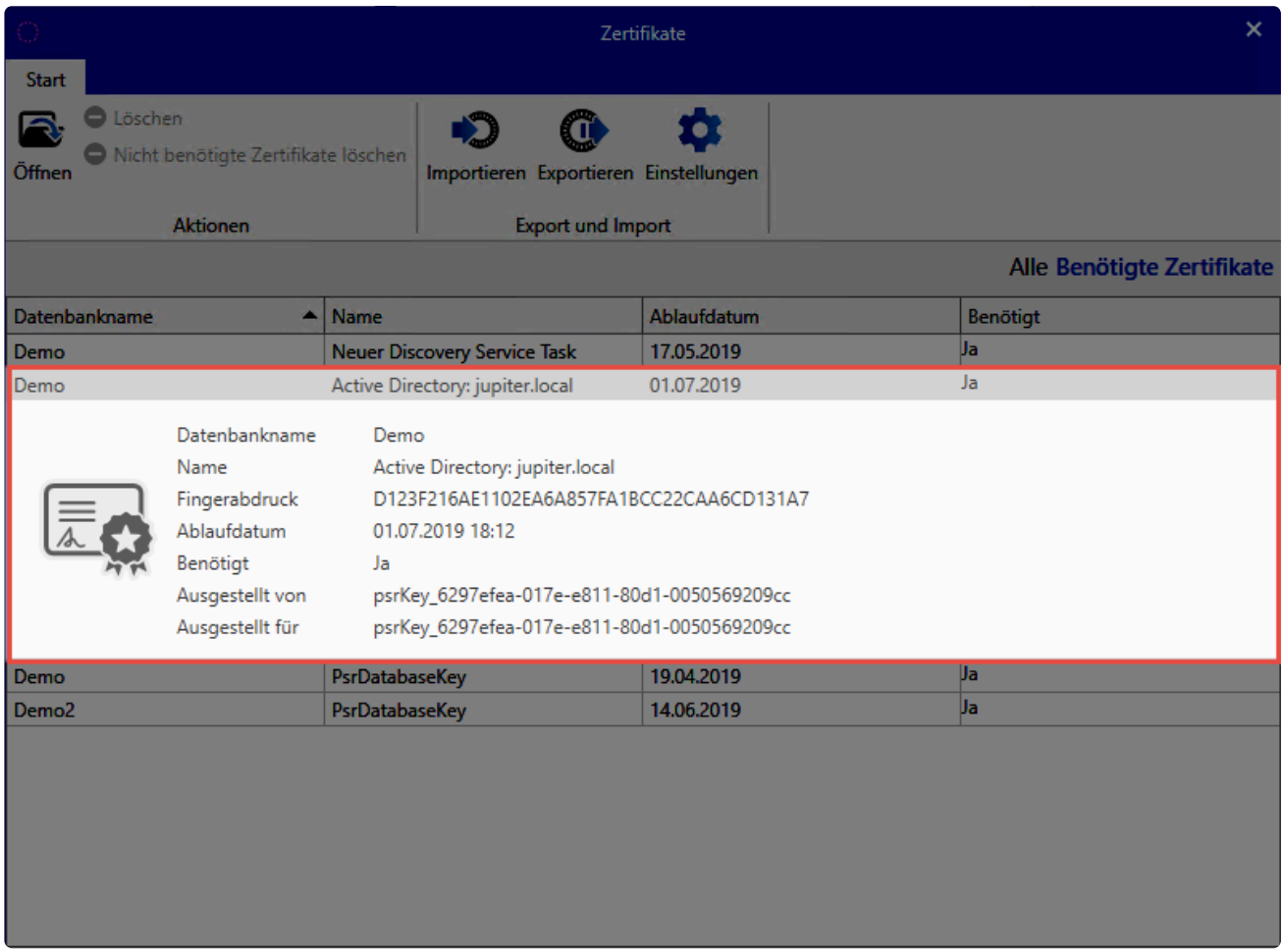
Export und Import des Zertifikats

Wie Sie das Zertifikat sichern und wieder einbinden, erfahren Sie im Kapitel Zertifikate.

Master Key Zertifikate

Was ist das Masterkey Zertifikat?

Wird ein Active Directory über den **Masterkey Modus** angesprochen, wird hierfür ein Zertifikat erstellt. Dieses trägt den Namen **Active Directory: Domain**:



Das Masterkey Zertifikat können Sie **nicht** durch ein eigenes Zertifikat ersetzen.

Die **Zertifikate für den Masterkey Modus** haben ein Ablaufdatum. Dies wird jedoch nicht geprüft. Diese Zertifikate müssen also nicht erneuert werden.

Verschieben Sie die Datenbank auf einen anderen Server, müssen Sie das Masterkey Zertifikat **zwingend mit übertragen**!

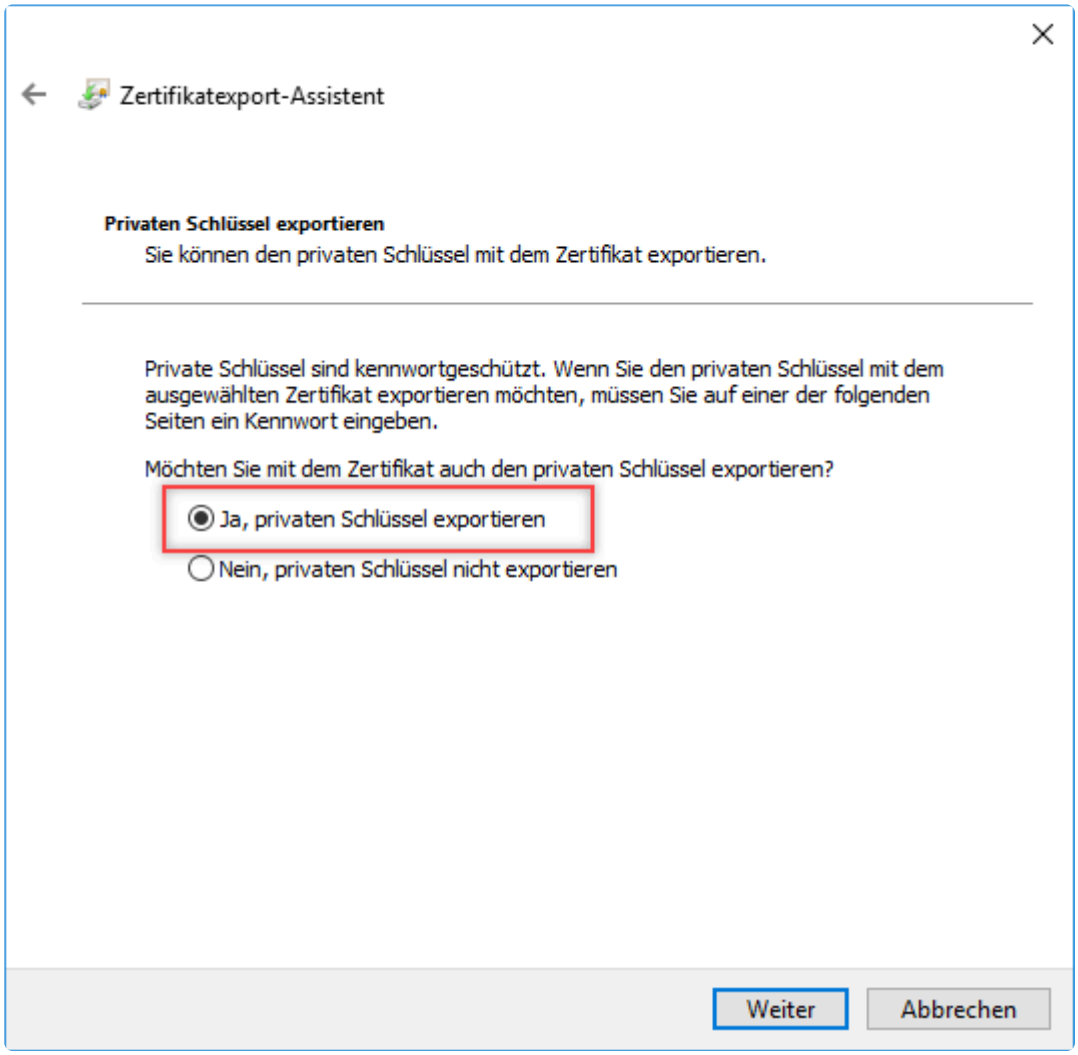
Zertifikat sicher verwahren

Da über das Masterkey Zertifikat alle Benutzeraccounts gesichert werden, ist es nötig dieses Zertifikat

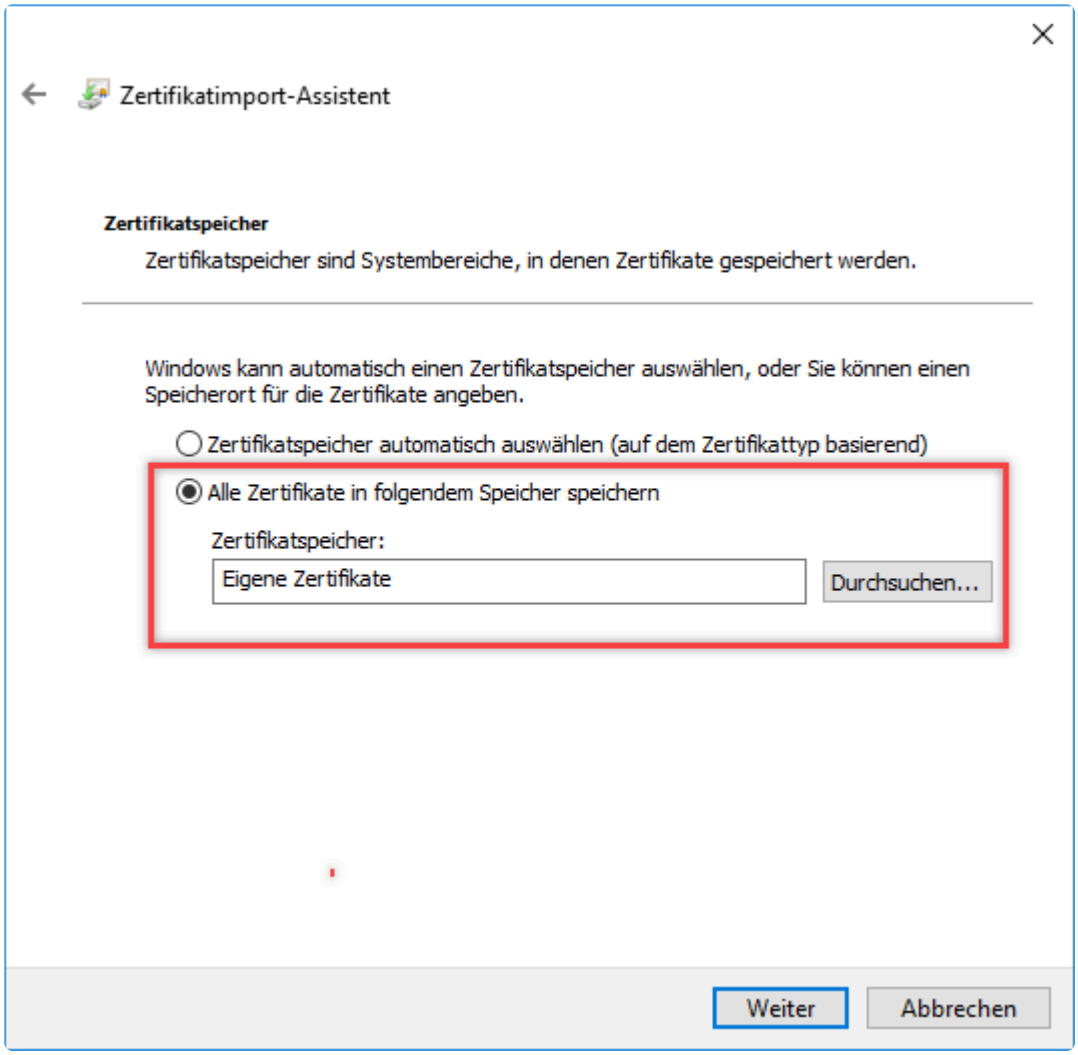
besonders zu sichern und zu schützen. Zunächst müssen Sie das Zertifikat mitsamt Private Key exportieren und an einem sicheren Ablageort aufbewahren (z. B. Tresor, o.ä.).

Gehen Sie dabei folgendermaßen vor:

- Exportieren Sie das Master Key Zertifikat mitsamt Private Key.



- Löschen Sie das Zertifikat aus **Eigene Zertifikaten**.
- Importieren Sie das exportierte Zertifikat in die **Eigene Zertifikat**. Achten Sie darauf, dass Sie den Privat Key ohne Exportrechte importieren.



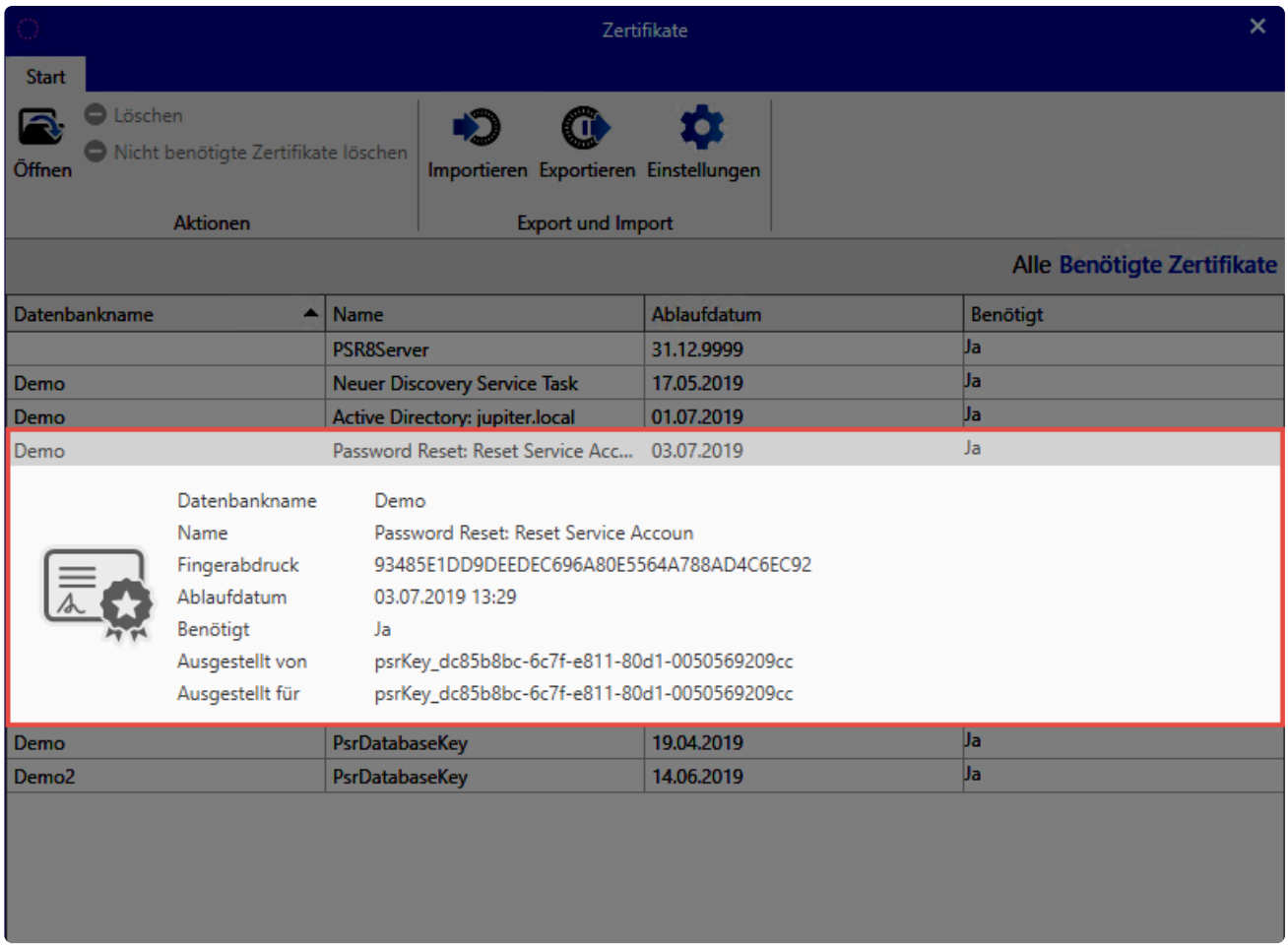
- Speichern Sie das exportierte Zertifikat auf einem Stick und verwahren Sie es sicher.

Zusätzlich erfahren Sie im Kapitel Zertifikate detaillierte Informationen zum Im- und Export von Zertifikaten.

Passwort Reset Zertifikate

Was ist das Passwort Reset Zertifikat?

Erstellen Sie einen Passwort Reset, so wird ein zugehöriges Zertifikat erzeugt. Dieses dient dazu, die Passwörter verschlüsselt zu übertragen.



Das Passwort Reset Zertifikat können Sie **nicht** durch ein eigenes Zertifikat ersetzen.

Die **Zertifikate für den Passwort Reset** haben ein Ablaufdatum. Dies wird jedoch nicht geprüft. Sie müssen diese Zertifikate daher nicht erneuern.

Verschieben Sie die Datenbank auf einen anderen Server, müssen Sie alle Passwort Reset Zertifikate **zwingend mit übertragen**!

Export und Import des Zertifikats

Wie Sie das Zertifikat sichern und wieder einbinden, erfahren Sie im Kapitel Zertifikate.

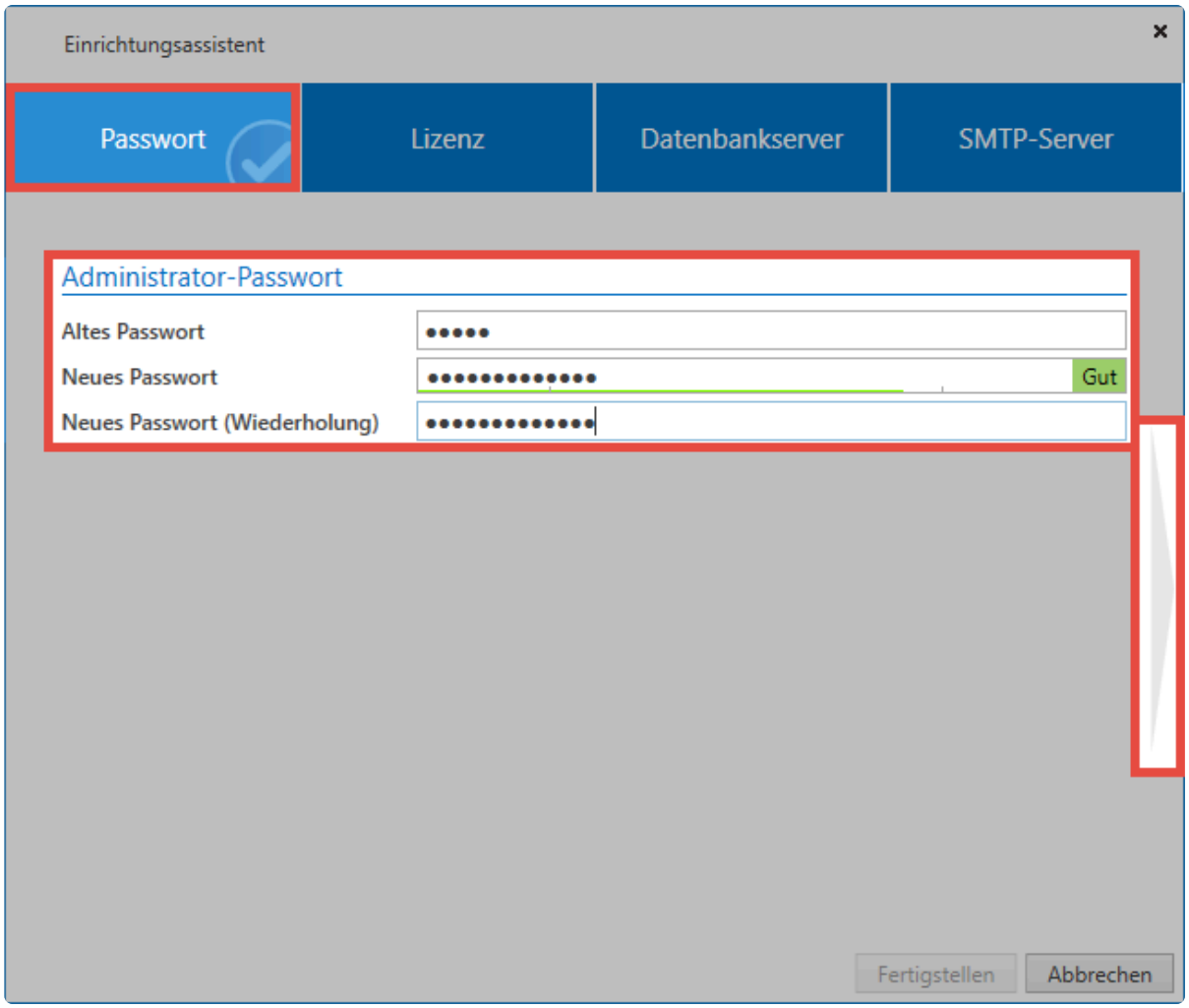
Einrichtungsassistent

Was ist der Einrichtungsassistent?

Der Einrichtungsassistent beinhaltet alle relevanten Einstellungen im Zuge der Einrichtung von Password Safe. Die einzelnen Punkte können Sie ebenso im Nachhinein ändern. Hierzu existieren jeweils separate Kapitel.

Administrator-Passwort definieren

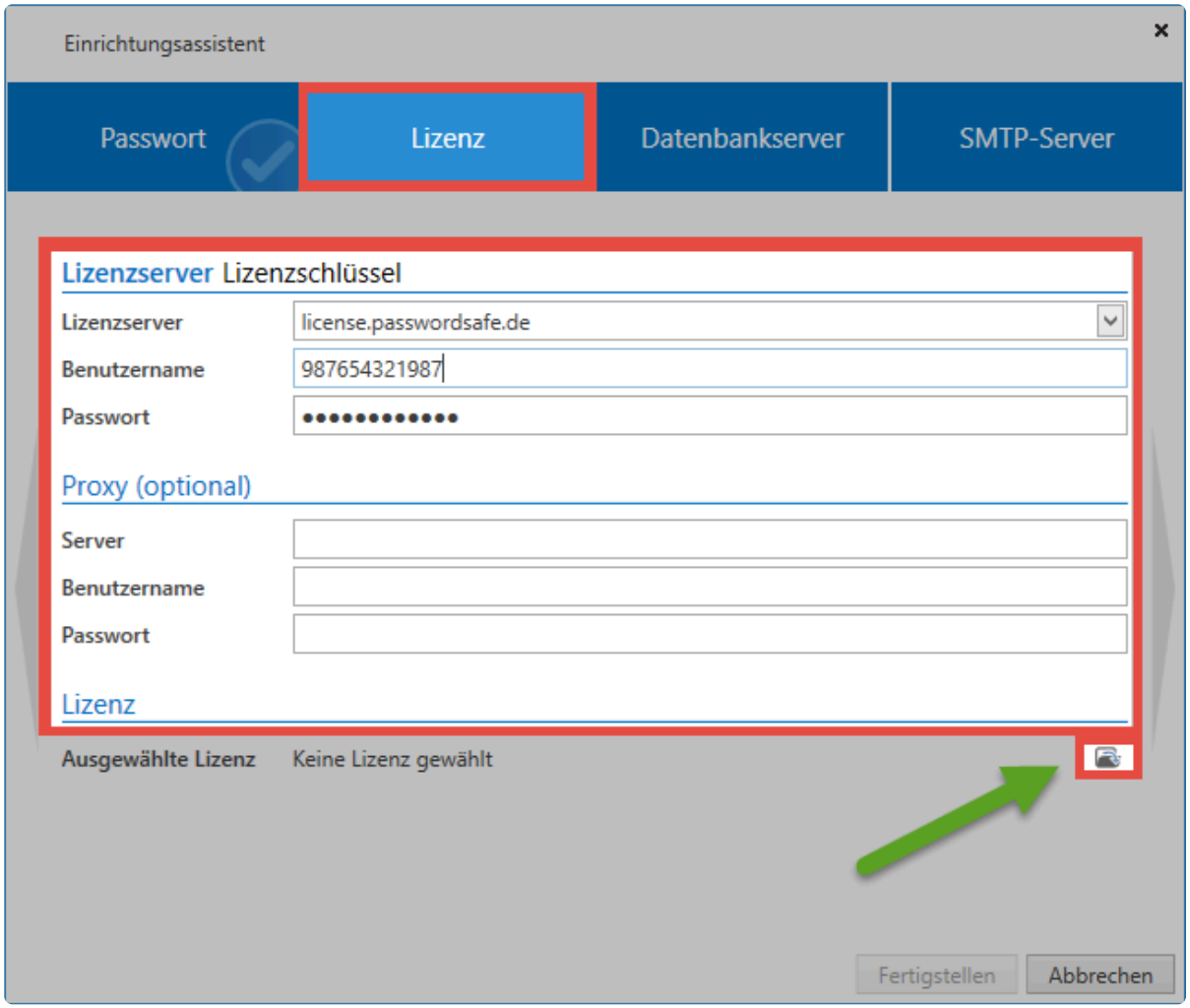
Das Initialpasswort lautet “admin”. Im ersten Schritt legen Sie dann das Authentifizierungspasswort für den Admin Client fest. Dieses vergeben Sie beim Start neu – das neue Passwort ist sicher und wohl dokumentiert aufzubewahren. Im Nachhinein können Sie dies in den allgemeinen Einstellungen ändern.



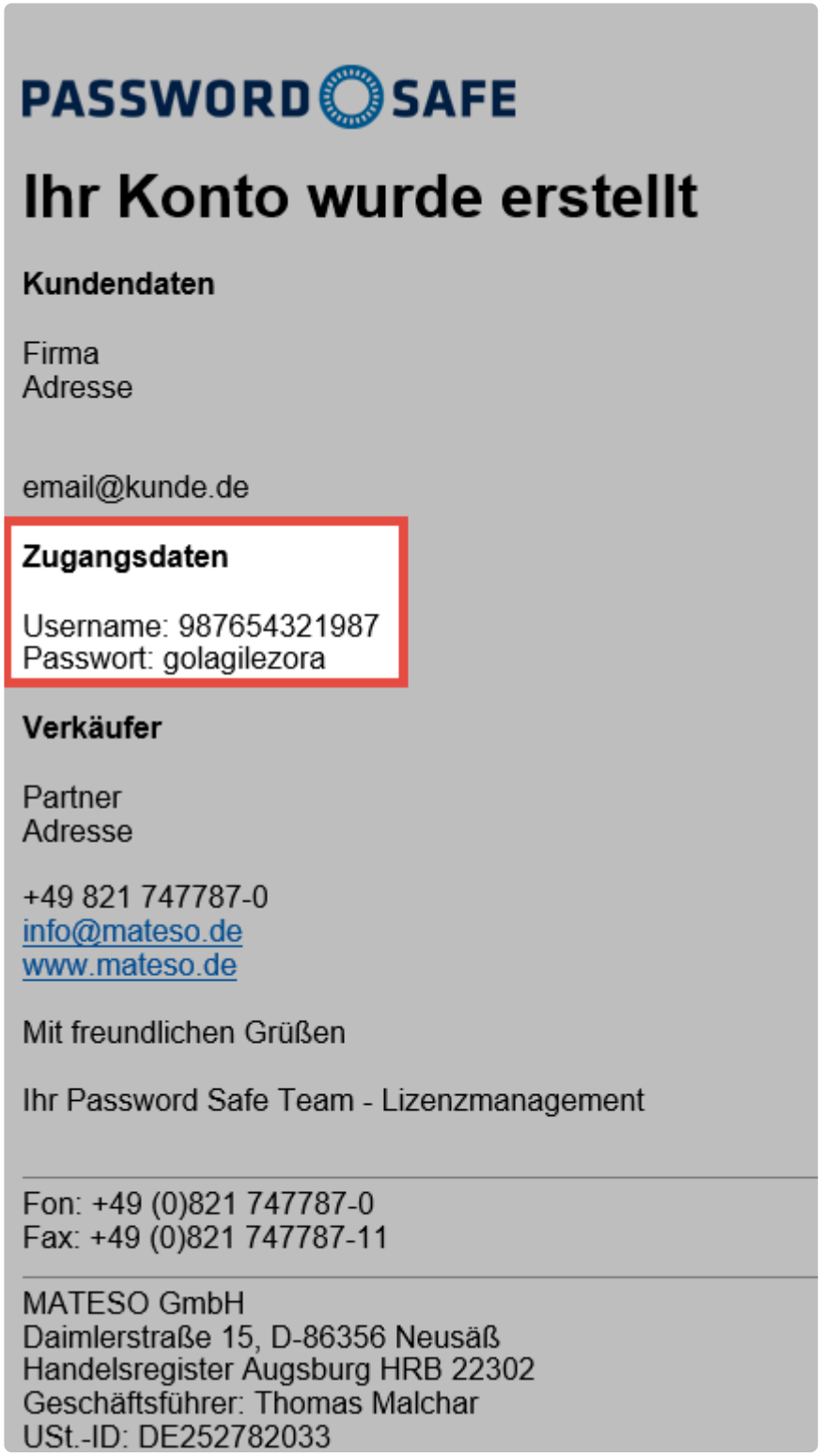
Das Initialpasswort lautet “admin”.

Lizenzeinstellungen

Im zweiten Schritt konfigurieren Sie die erfolgreiche Anbindung an den Lizenzserver. In den Lizenzeinstellungen können Sie dies auch im Nachhinein durchführen.



Im Feld Lizenzserver hinterlegen Sie “license.passwordsafe.de”. Die weiteren Zugangsdaten (Benutzername und Passwort zum Lizenzserver) werden Ihnen 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

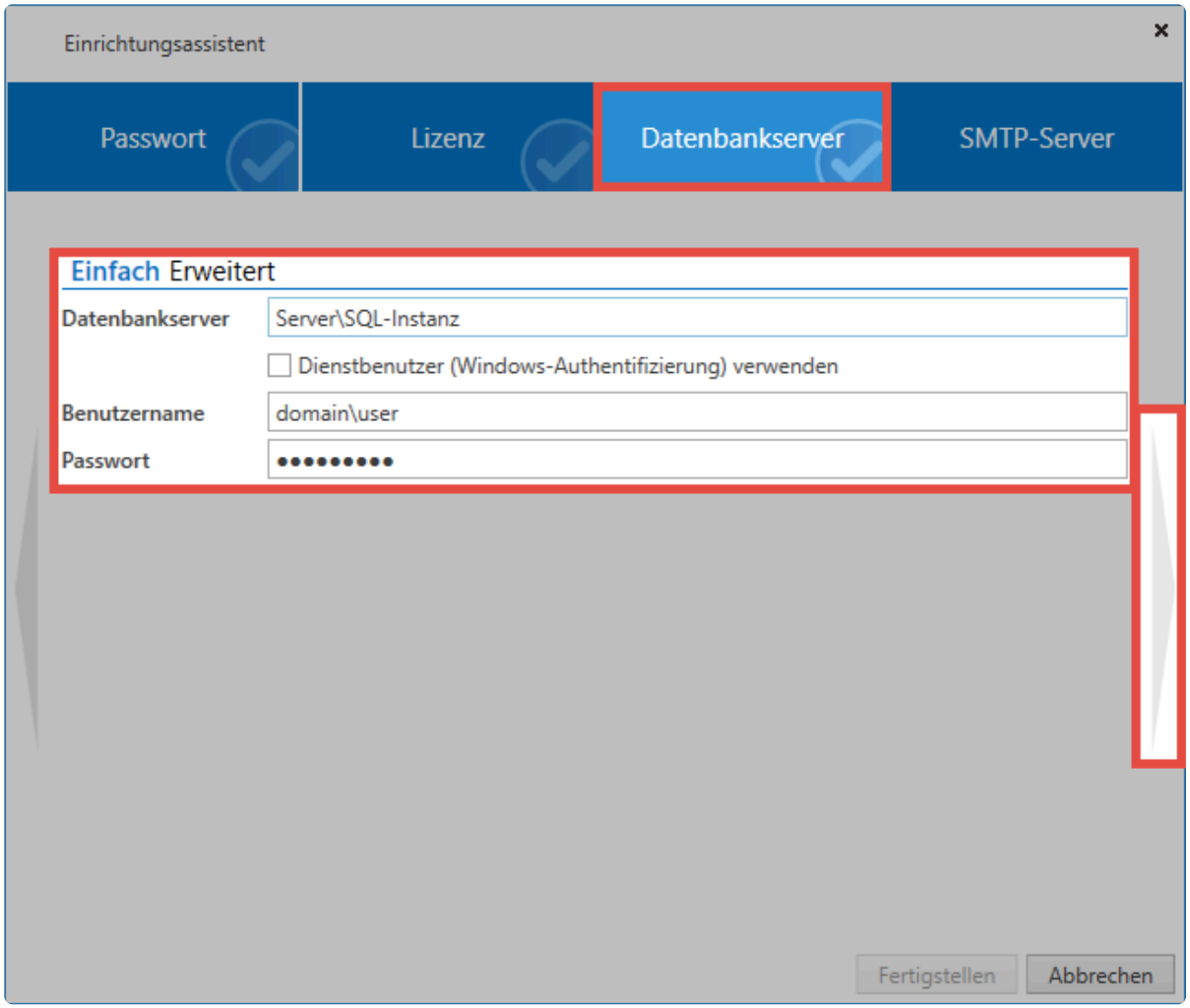
Fon: +49 (0)821 747787-0
Fax: +49 (0)821 747787-11

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Handelsregister Augsburg HRB 22302
Geschäftsführer: Thomas Malchar
USt.-ID: DE252782033

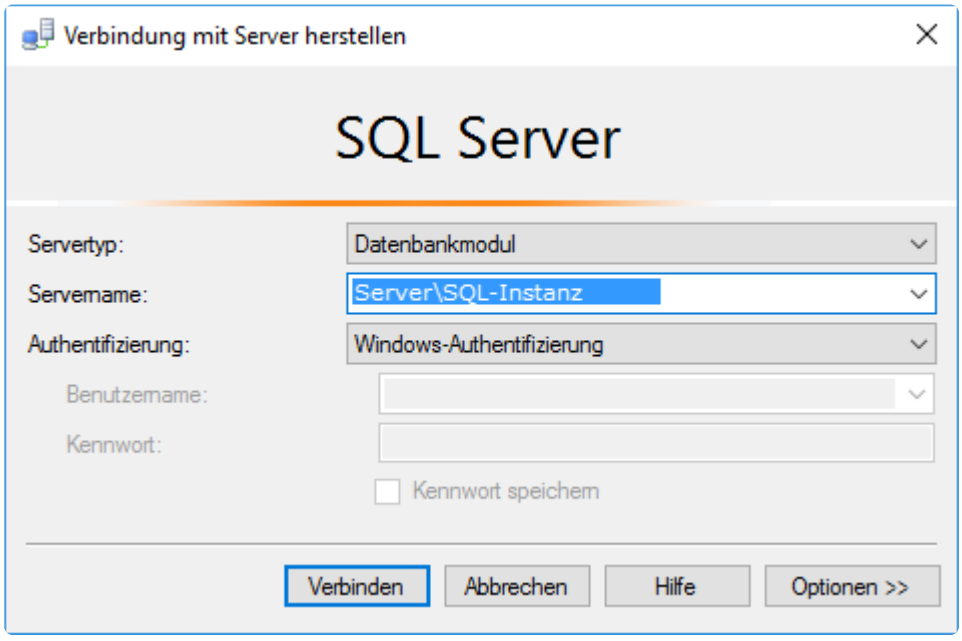
Falls nötig, können Sie ebenso Zugangsdaten für einen etwaigen Proxy angeben – ansonsten wird der im Betriebssystem hinterlegte Proxy verwendet. Über die entsprechende Schaltfläche können Sie dann die gewünschte Lizenz auswählen und aktivieren.

Datenbankserver

Die Konfiguration des Datenbankservers ist ebenso Teil der erweiterten Einstellungen und kann dort von Ihnen im Nachhinein geändert werden.



Geben Sie den Datenbankserver inklusive der zugehörigen SQL Instanz an. Der Einfachheit halber können Sie den Servernamen aus dem Loginfenster des SQL-Servers kopieren.

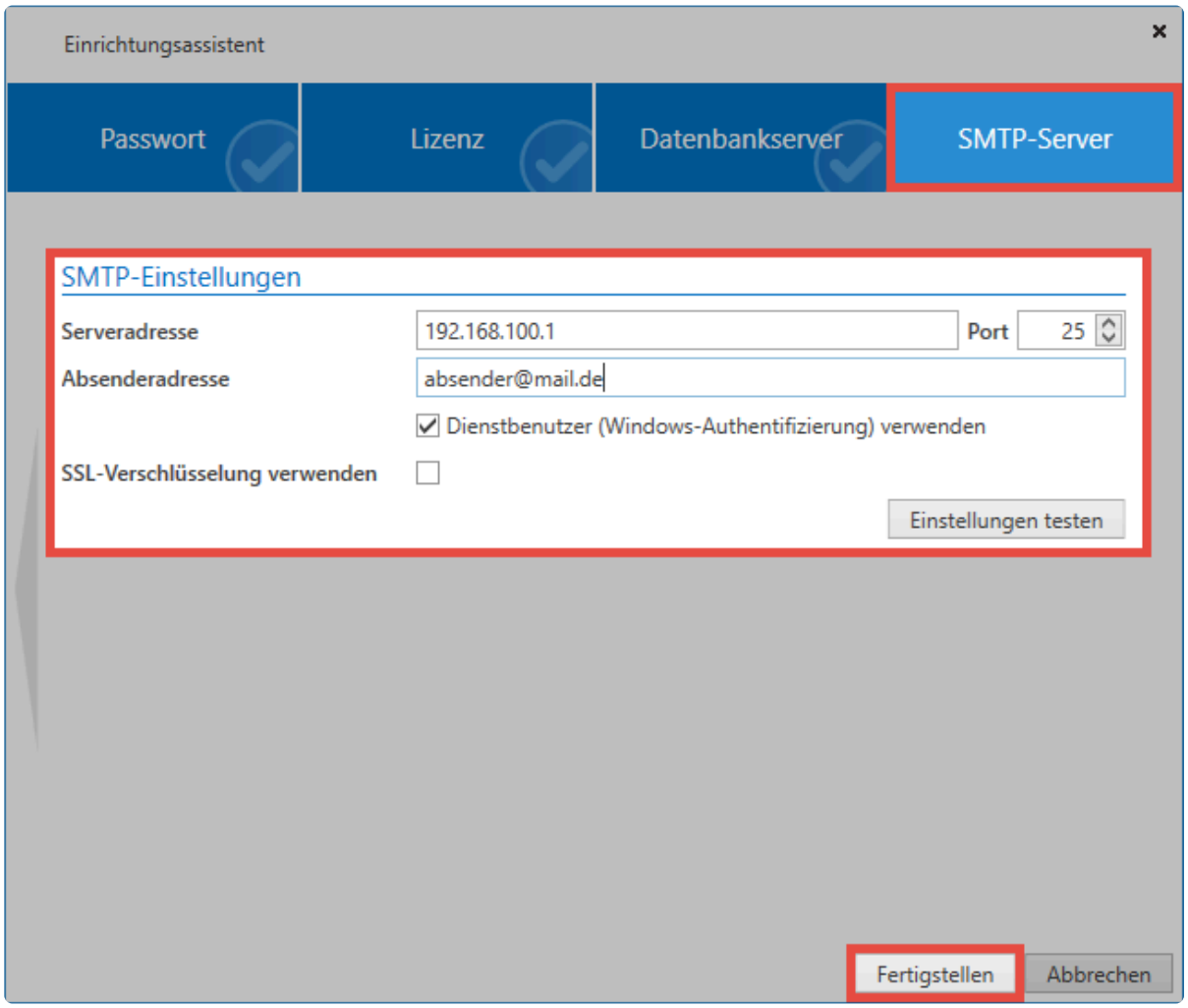


Weiterhin geben Sie den Benutzer an, in dessen Kontext Sie am SQL-Server die Datenbank erstellen. Sie benötigen Der Benutzer benötigt **dbCreator** Rechte. Alternativ besteht hier auch die Möglichkeit den Dienstbenutzer zu verwenden. Über die Schaltfläche “Erweitert” erhalten Sie die Möglichkeit einen

Connection String anzugeben.

SMTP-Server

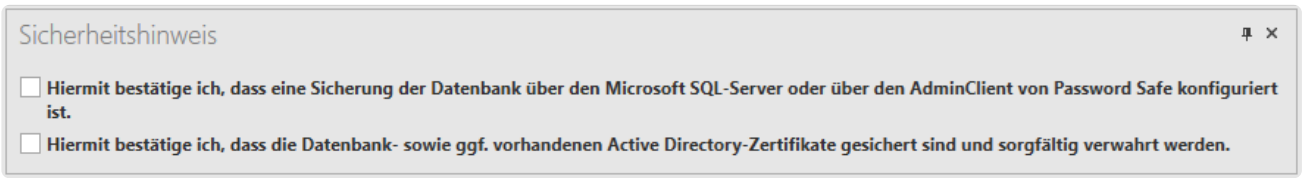
Im letzten Schritt konfigurieren Sie den SMTP-Server, über welchen alle E-Mails verschickt werden. Auch dies ist Teil der erweiterten Einstellungen, falls im Nachhinein Änderungen vorgenommen werden müssen.



Sobald Sie die Daten eingegeben haben und diese erfolgreich getestet wurden, können Sie den Assistenten über einen Klick auf “Fertigstellen” schließen.

Sicherheitshinweise

Ist der Einrichtungsassistent eingerichtet, werden im Modul **Status** zwei Sicherheitshinweise eingeblendet, welche von Ihnen bestätigt werden müssen:



! Es wird empfohlen die Sicherheitshinweise erst dann zu bestätigen, wenn Sie die entsprechenden Punkte tatsächlich erledigt haben. Sie sollten unbedingt darauf achten, dass regelmäßige Backups erstellt und die Zertifikate gesichert werden.

Hier geht´s zurück zum Kapitel Erste Schritte.

Erstellen von Datenbanken

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

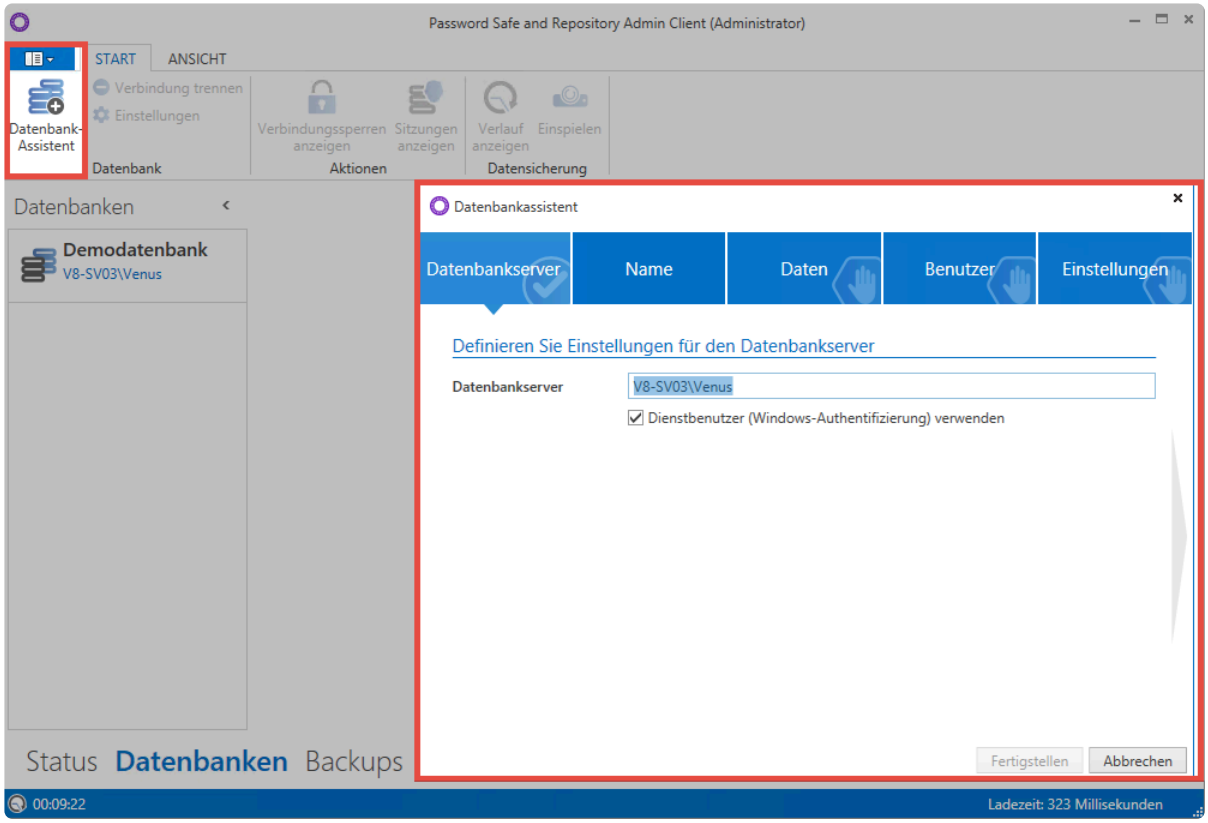
https://www.youtube.com/embed/md7_VEdVuWM?rel=0

Was sind Datenbanken?

Datenbanken beinhalten alle Informationen zu Benutzern, Datensätzen, Dokumenten, Rollen – sprich von allen Objekten in Password Safe. Alle Änderungen von Objekten werden ebenfalls in der Datenbank gespeichert. Password Safe verwendet hierzu eine MSSQL Datenbank. Um den Verlust dieser Informationen zu vermeiden empfehlen wir die Erstellung regelmäßiger Backups, um die Daten zu sichern.

Erstellen von Datenbanken

Zum Erstellen einer Datenbank starten Sie den Datenbankassistenten über die Ribbon. Er leitet Sie durch die einzelnen Schritte.



Datenbankserver

Die Auswahl des Datenbankservers können Sie im ersten Reiter manuell definieren. Standardmäßig ist der in den erweiterten Einstellungen definierte Wert voreingestellt. Sie können darüber hinaus einen Benutzer hinterlegen oder auf den Dienstbenutzer zurückgreifen.

Name

Hier wird der Name der neuen Datenbank angegeben. Alternativ können Sie auch eine bestehende Datenbank selektierten. Ein aussagekräftiger Name erleichtert besonders im Zusammenspiel mehrerer Datenbanken die Unterscheidung.

Daten

Sie können auswählen, ob eine Vorlage verwendet werden soll. Über die Vorlage erhält die Datenbank vorgefertigte Formulare und Dashboard-Einstellungen, welche den Einstieg erleichtern. Sie haben die Möglichkeit zwischen der deutschen und der englischen Vorlage auszuwählen. Es ist jedoch auch möglich, ohne Vorlage fortzufahren. So erhalten Sie eine komplett leere Datenbank. Haben Sie ein Backup aus einer Password Safe Version 7, kann dieses migriert werden.

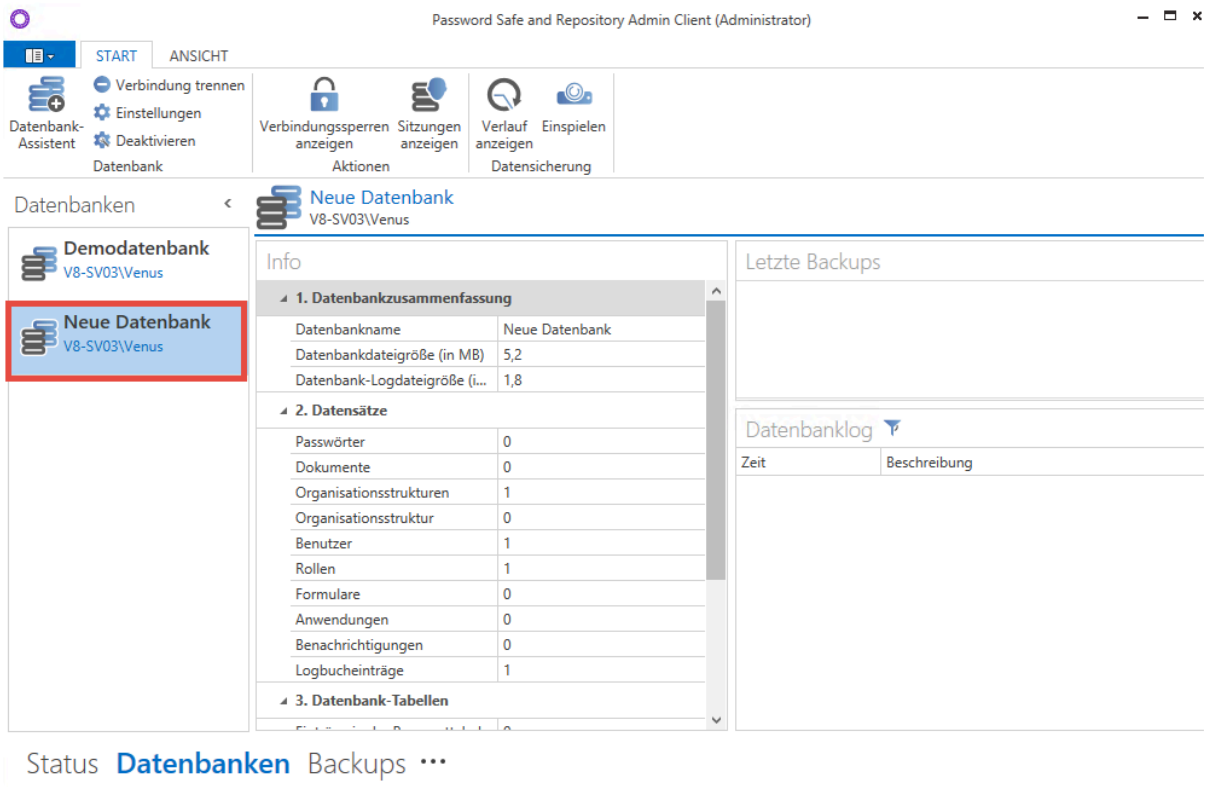
Benutzer

Legen Sie einen sogenannten Datenbank-Benutzer an – üblicherweise ist dies der Administrator. Ist die Migration aktiv, können Sie den User nach der Migration wieder löschen.

Abschließen des Datenbankassistenten

Nach der erfolgreichen Erstellung einer Datenbank startet die Datenbankmigration, sofern diese

ausgewählt wurde. Ohne Migration wird die neue Datenbank direkt angelegt und in der Datenbankübersicht angezeigt.

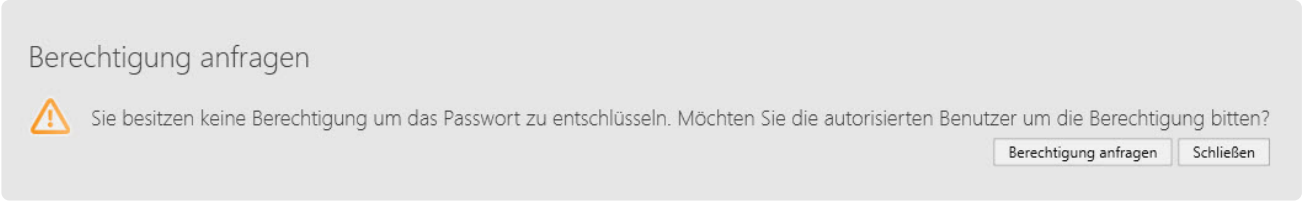


Hier geht´s zurück zum Kapitel Erste Schritte

Bereinigung Rechteschlüssel

Problembeschreibung

In Version 8.3.0.13378 konnten Passwörter angelegt werden, welche für andere Benutzer nicht entschlüsselt werden können. Hierbei fehlt einzelnen oder auch allen Benutzern der nötige Rechteschlüssel. Möchte ein Benutzer ein betroffenes Passwort aufdecken wird folgende Meldung angezeigt:



Bugfix

Der Bug wurde mit Version **8.3.0.14422 Hotfix 1** behoben. Sollte ein ältere Version im Einsatz sein, sollte unbedingt auf die aktuelle Version **8.4.0.14576** aktualisiert werden.

Prüfung und Bereinigung der Datensätze

Beim Update auf Version **8.4.0.14576** wird am AdminClient auf betroffene Datensätze geprüft.

Prüfung über den AdminClient

In den Ergebnissen der Abfrage ist zu sehen, welche Passwörter von welchem Benutzer repariert werden können. (In diesem Beispiel, werden die Einträge farblich hervorgehoben).

Blau = Passwortname
Gelb = Reparierbar/Irreparabel
Orange = Benutzer/Rollen, welche das Passwort reparieren können

Reparable Datensätze

Passwörter, bei welchen Benutzer/Rollen vorhanden sind mit Berechtigen-Recht und Rechteschlüssel:

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

Irreparable Datensätze

Passwörter, bei welchen Benutzer/Rollen vorhanden sind ohne Rechteschlüssel oder mit Rechteschlüssel jedoch ohne Berechtigen-Recht:

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

Bereinigung reparabler Datensätze

Beschädigte Passwörter werden mit den unter ‘repairable with’ angegebenen Benutzern/Rollen automatisch beim Anmelden am Client oder WebClient korrigiert.

Geprüft werden kann der Rechteschlüssel über die Formularfeldberechtigungen von Passwortfeldern. Besitzt mindestens ein Benutzer den Rechteschlüssel, kann das Passwort repariert werden. Im folgenden Beispiel besitzt lediglich der Benutzer ‘chno’ den Rechteschlüssel und somit kann nur dieser Benutzer das Passwort aufdecken und korrigieren.

Name	Berechtigungen
Mustermann, Max (admin)	Lesen
Norred, Chris (chno)	Lesen/Berechtigen
Tane, Kate (kata)	Lesen/Schreiben/Löschen/Verschieben/Exportieren/Drucken

Beim Anmelden an der Datenbank über den Client wird automatisch ein Bereinigungs-Task gestartet. Dieser Task wird immer mit dem angemeldeten Benutzer ausgeführt. Dabei werden – soweit es mit dem Benutzer möglich ist – alle betroffenen Passwörter korrigiert. Sobald sich also alle Benutzer einmalig angemeldet haben, sollten alle betroffenen Passwörter bereinigt sein.

Irreparable Datensätze (not repairable)

Irreparable Passwörter können nicht automatisch korrigiert werden. Dennoch kann es vorkommen, dass als irreparable markierte Passwörter manuell korrigiert werden können.

Erster Fall

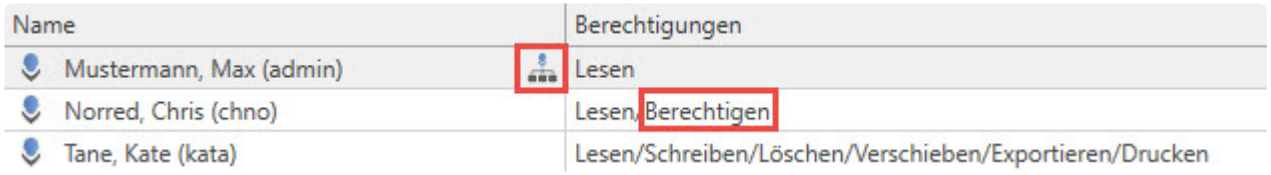
Im ersten Fall besitzt kein Benutzer/Rolle den Rechteschlüssel auf das Passwort, somit kann auch kein Benutzer das Passwort entschlüsseln oder korrigieren.

Name	Berechtigungen
Mustermann, Max (admin)	Lesen
Tane, Kate (kata)	Lesen/Schreiben/Löschen/Verschieben/Exportieren/Drucken

Die betroffenen Passwörter müssen neu angelegt werden. Zur Sicherheit kann eine neue Datenbank mit einen älteren Backup eingebunden werden. Aus dieser Datenbank können die betroffenen Passwörter/ Daten in die akutelle Datenbank erneut übernommen werden.

Zweiter Fall

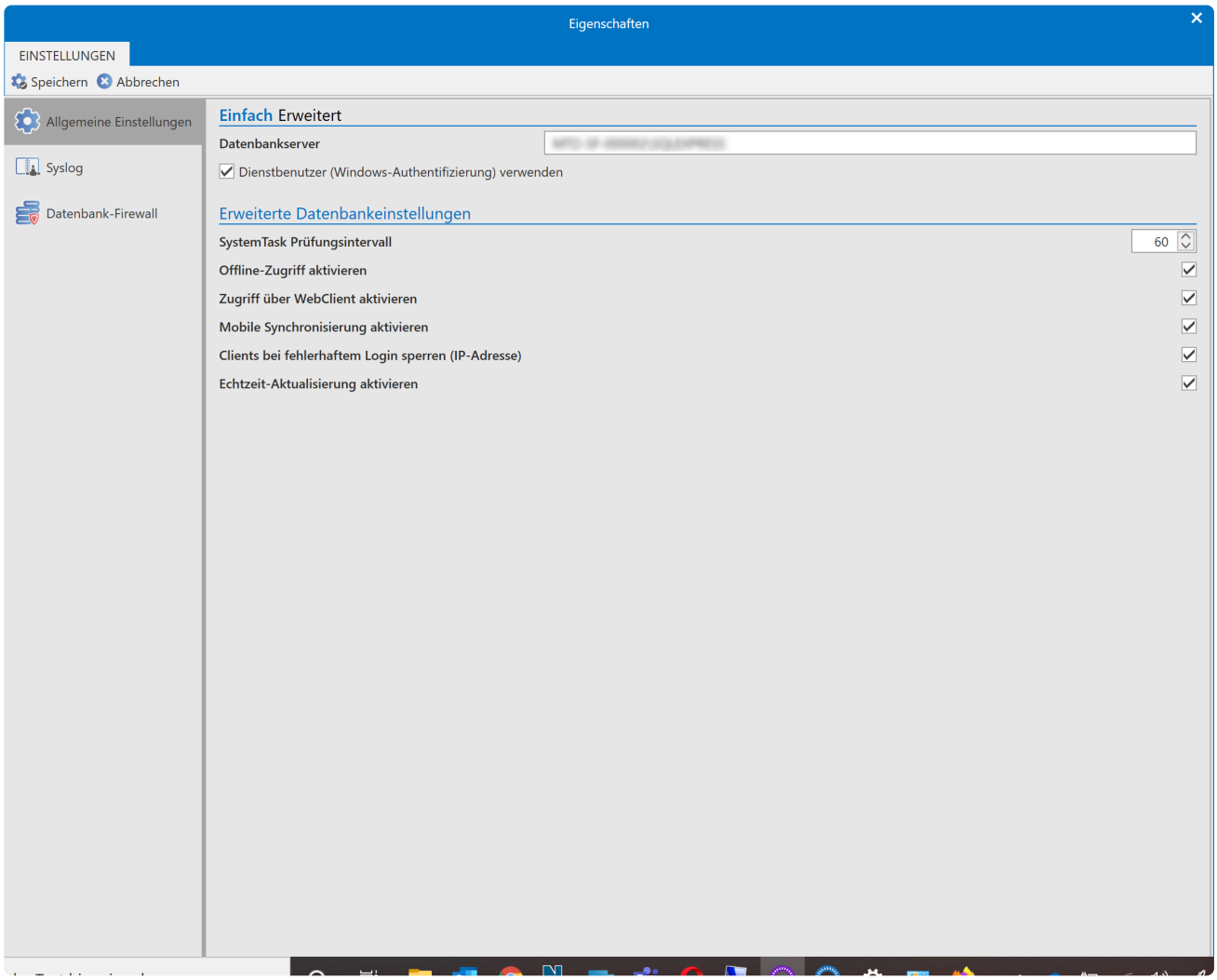
Im zweiten Fall gibt es Benutzer/Rolle, welche zwar den Rechteschlüssel besitzen jedoch nicht das Berechtigen-Recht. Insofern sich die Anzahl von irreparablen Passwörtern in Grenzen hält, können bei diesen die Formularfeldberechtigungen manuell geprüft werden.



Bei den betroffenen Passwörtern muss dem Benutzer mit dem Rechteschlüssel vorübergehend zum Korrigieren das Berechtigen-Recht gegeben werden. Hat der entsprechende Benutzer das Berechtigen-Recht, kann dieser die Rechteschlüssel neu setzen, dies erfolgt entweder automatisch beim Anmelden oder manuell beim Speichern der Berechtigungen.

Datenbankeigenschaften

Die Eigenschaften einer Datenbank öffnen Sie, in dem Sie einen Doppelklick auf die Datenbank durchführen. Hierbei wird keine Anmeldung an der Datenbank vorausgesetzt.



Eigenschaften

Folgende Optionen stehen Ihnen zur Bearbeitung zur Verfügung:

- **Allgemeine Einstellungen**
- **Syslog**
- **Datenbank-Firewall**

Allgemeine Einstellungen

Bei den **Allgemeinen Einstellungen** können Sie folgendes definieren:

- **Datenbankserver** – hier können Sie die SQL Instanz neu angeben.
- **SystemTask Prüfungsintervall** – gibt vor in welcher Zeitspanne der Prüfungsintervall für System Tasks laufen soll (**standardmäßig auf 60 Minuten gesetzt**).
- **Offline-Zugriff aktivieren** – Aktivierung/Deaktivierung des Offline Clients.

- **Zugriff über Webclient aktivieren** – Aktivierung/Deaktivierung des WebClients (**standardmäßig aktiv**).
- **Mobile Synchronisation erlauben** – Aktivierung/Deaktivierung der Synchronisation mit mobilen Geräten.
- **Clients bei fehlerhaftem Login sperren (IP-Adresse)** – Sperrung der IP bei fehlerhafter Anmeldung .
- **Echtzeit-Aktualisierung aktivieren** – Aktivierung/Deaktivierung der Echtzeit-Aktualisierung zwischen den Clients (**standardmäßig aktiv**).

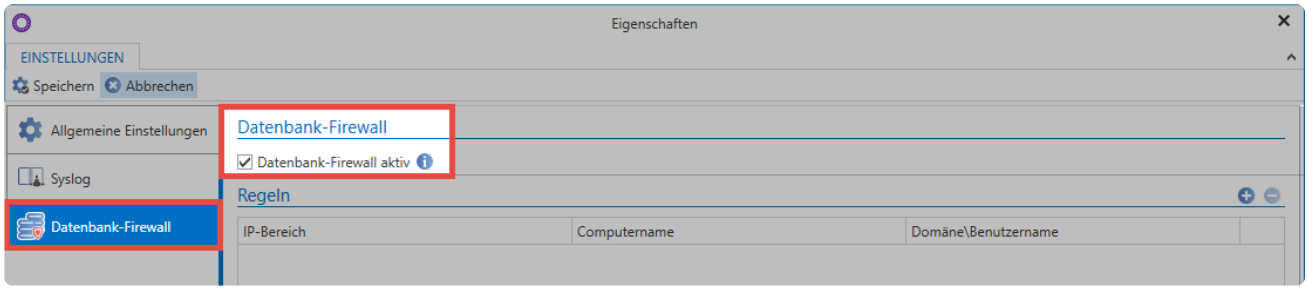
Datenbank Firewall

Was ist die Datenbank Firewall?

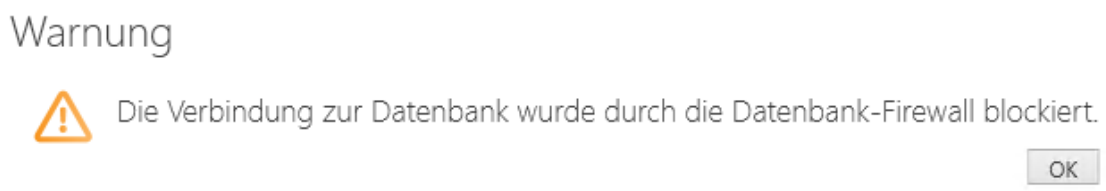
Die Datenbank Firewall ermöglicht es Ihnen den Zugriff auf die Datenbank zu reglementieren. Über Firewall Regeln geben Sie dann einzelne Zugriffe frei.

Aktivieren der Firewall

Die Firewall aktivieren Sie direkt in den Datenbank Einstellungen.



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 fügen Sie Regeln hinzu oder löschen Sie sie. Über einen Doppelklick bearbeiten Sie Regeln.

Es stehen folgende Möglichkeiten bereit:

- Über die **IP-Adresse** wird der Zugriff von einem einzelnen Rechner aus erlaubt.
- Optional wählen Sie auch ein **Bereich** für mehrere **IP-Adressen** aus.
- Ebenso ist es möglich die Freigabe über den **Computernamen** zu regeln.
- Schlussendlich können Sie auch den Zugriff für einen bestimmten Windowsbenutzer freigeben. Beispielsweise um den Administrator unabhängig vom Rechner zu berechtigen.
- Über **Zugriff gewähren** legen Sie fest, ob der Zugriff erlaubt oder blockiert wird. Dies wird über entsprechende Icons symbolisiert.

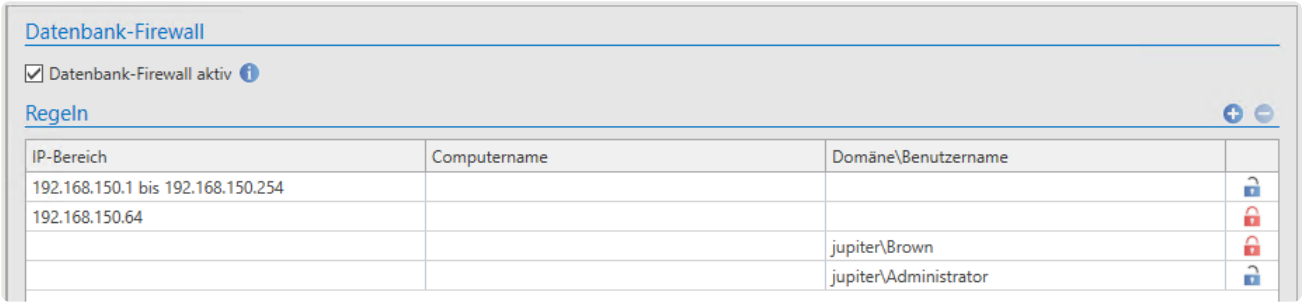
Selbstverständlich können Sie die Regeln auch kombinieren. Somit können Sie z.B. festlegen, dass sich von einer bestimmten IP Adresse aus nur ein definierter Benutzer anmelden kann.

> Die Kombination von Bedingungen erfolgt immer über **UND-Verknüpfungen**.

Überschneiden sich zwei bzw. mehrere Regeln, so überwiegt immer die Regel mit den geringeren Rechten. 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)

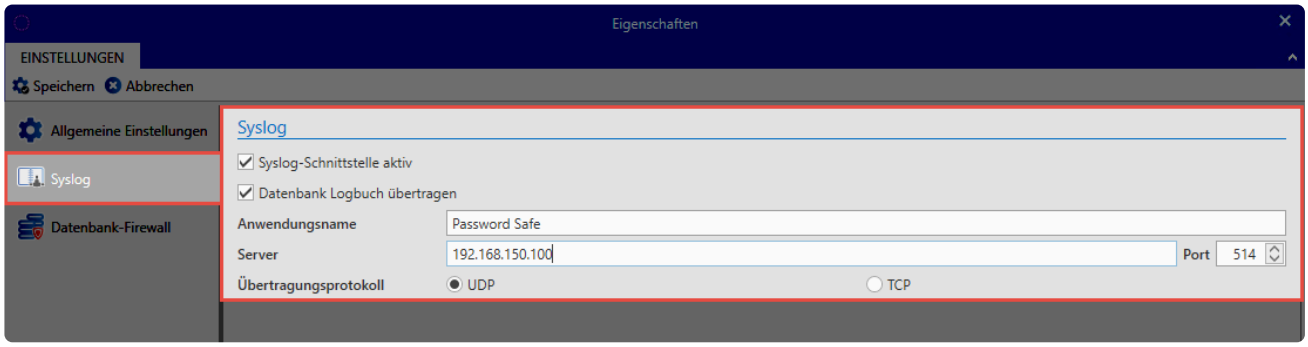
Ebenso können Sie auch einen bestimmten Benutzer, beispielsweise weil dieser die Firma verlassen hat.

Rechnerunabhängige Freigabe eines Benutzers (Regel 4)

Über diese Regel bekommt der Administrator den Zugriff gewährt. Hierbei ist es egal, von welchem Rechner aus er sich anmelden möchte.

Syslog

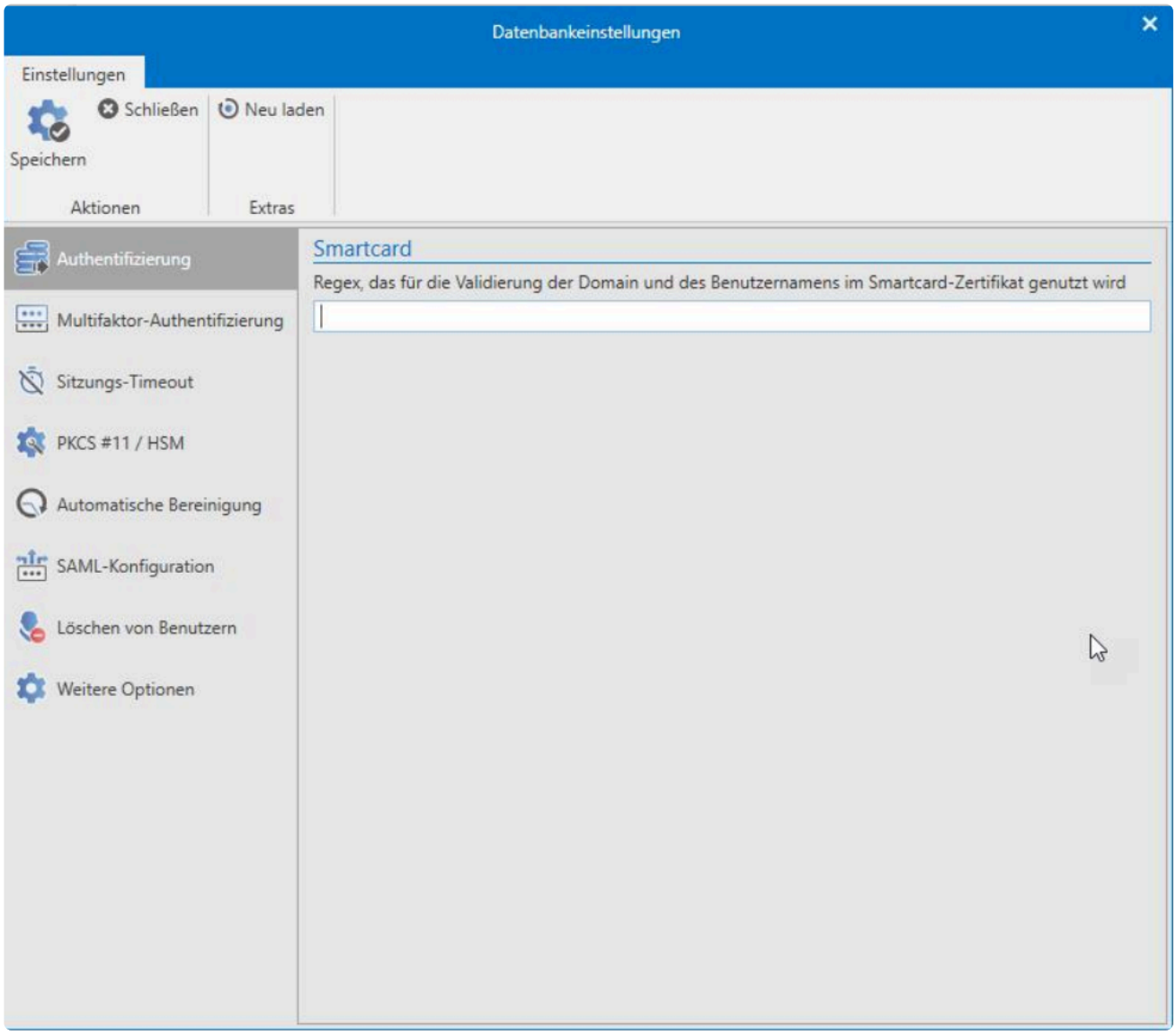
Auf Wunsch können Sie die Serverlogs und auch das Logbuch an einen Syslog-Server übertragen. Durch einen Doppelklick auf eine Datenbank gelangen Sie in deren Eigenschaften. Dort finden Sie den entsprechende Menüpunkt.



Konfigurieren Sie den Syslog-Server, nachdem Sie die Syslog-Schnittstelle über die entsprechende Option aktiviert haben. Falls gewünscht haben Sie auch die Möglichkeit das Datenbank Logbuch übertragen zu lassen.

Datenbankeinstellungen

Zum Öffnen der Einstellungen einer Datenbank selektieren Sie diese und klicken in der Ribbon auf “Einstellungen”. Alternativ können Sie mit der rechten Maustaste das Kontextmenü öfnnen und dort auf “Eigenschaften” klicken. Im nächsten Schritt werden Sie aufgefordert, Ihr Admin-Passwort einzugeben. Danach öffnet sich ein Fenster mit den Einstellungen.



Einstellungen

Folgende Einstellungen können Sie jetzt vornehmen:

- Authentifizierung
- **Multifaktor-Authentifizierung**
- **Sitzungs-Timeout**
- PKSC #11/ HSM
- Automatische Bereinigung
- SAML-Konfiguration
- Löschen von Benutzern

- Weitere Optionen

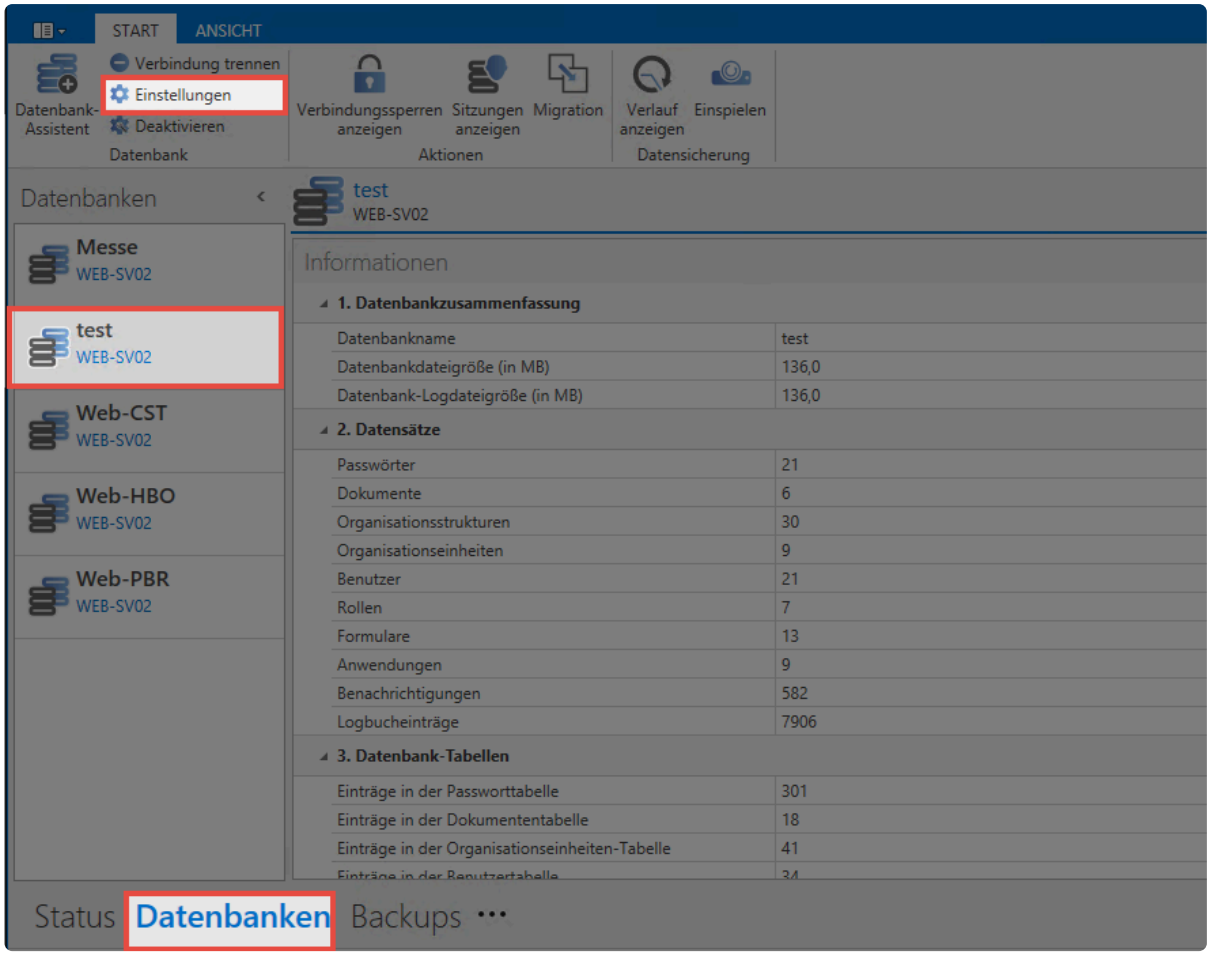
Multifaktor-Authentifizierung

Was ist Multifaktor-Authentifizierung?

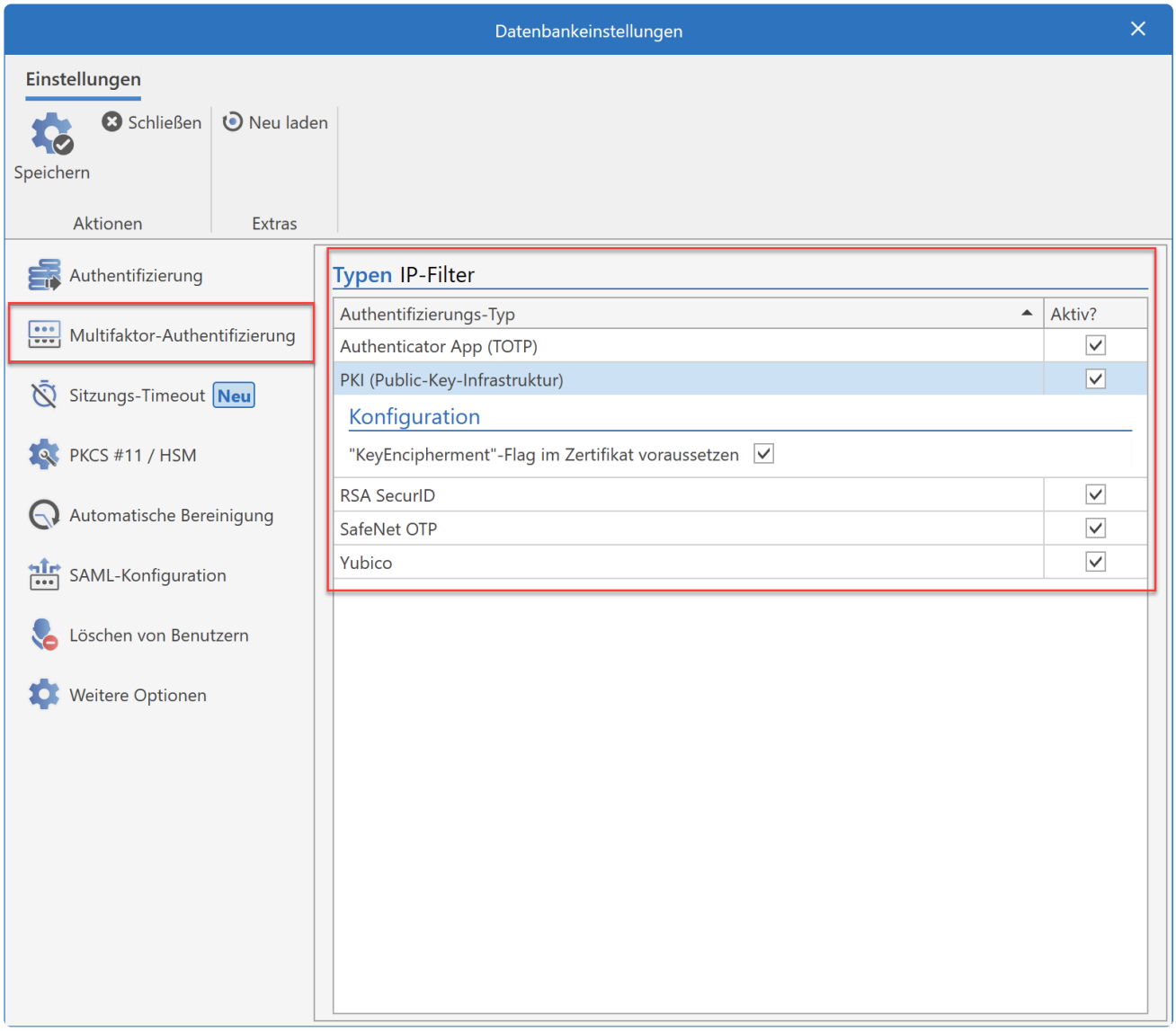
Über die Multifaktor-Authentifizierung wird die Anmeldung am Password Safe durch einen weiteren Faktor abgesichert. Die eigentliche Einrichtung findet im Client statt. Die konfigurierten Multifaktor-Authentifizierungen können anschließend von jedem Benutzer verwendet werden

Aktivierung verschiedener Faktoren

Wählen Sie im Modul **Datenbanken** eine Datenbank aus und öffnen deren Einstellungen über die Ribbon..



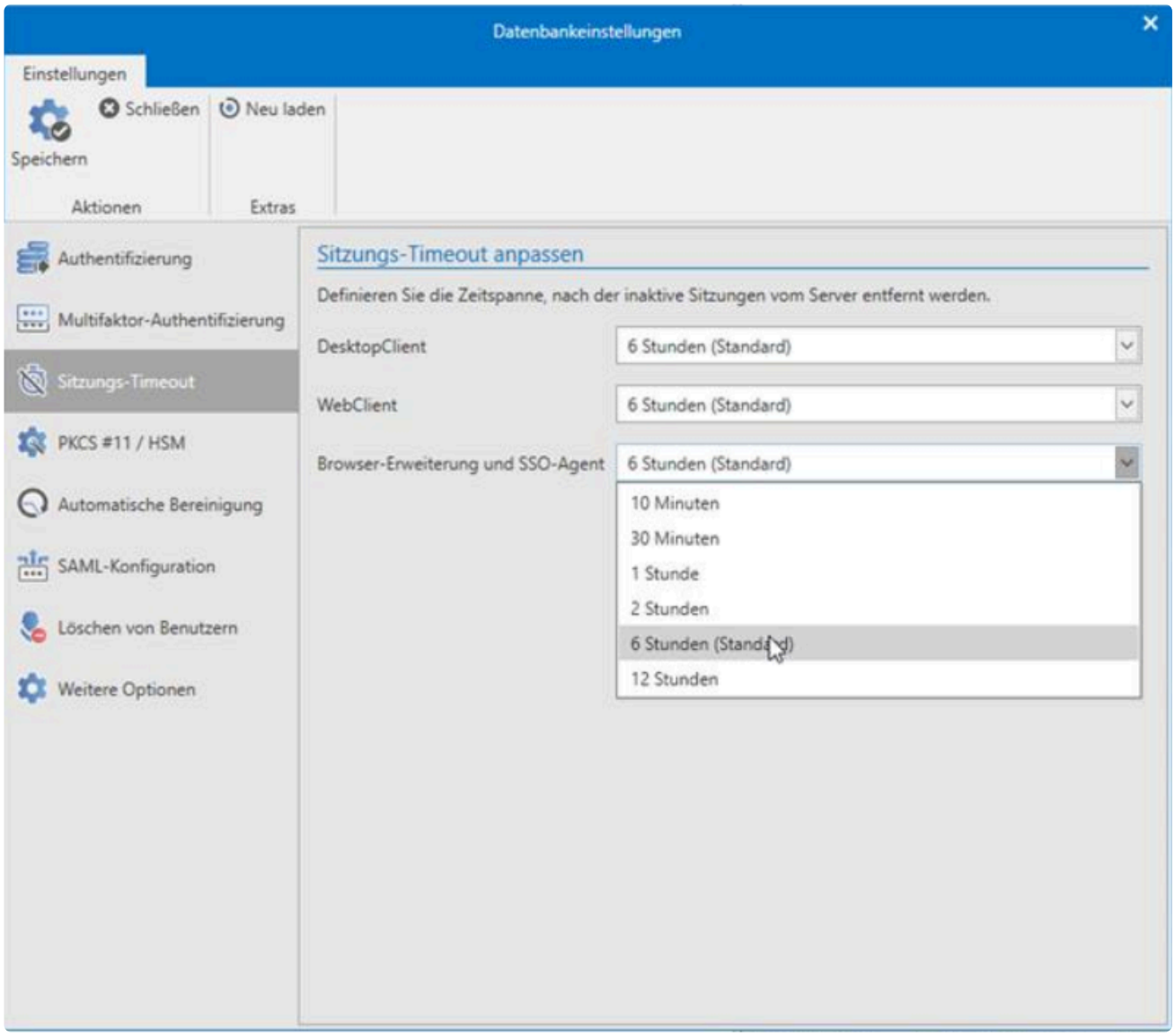
In den Einstellungen legen Sie fest, welche zweiten Faktoren verwenden werden können.



Sofern Sie für PKI Zertifikate ohne KeyUsageFlag “Verschlüsselung (Encipherment)” verwenden wollen, deaktivieren Sie die entsprechende Checkbox.

Sitzungs-Timeout

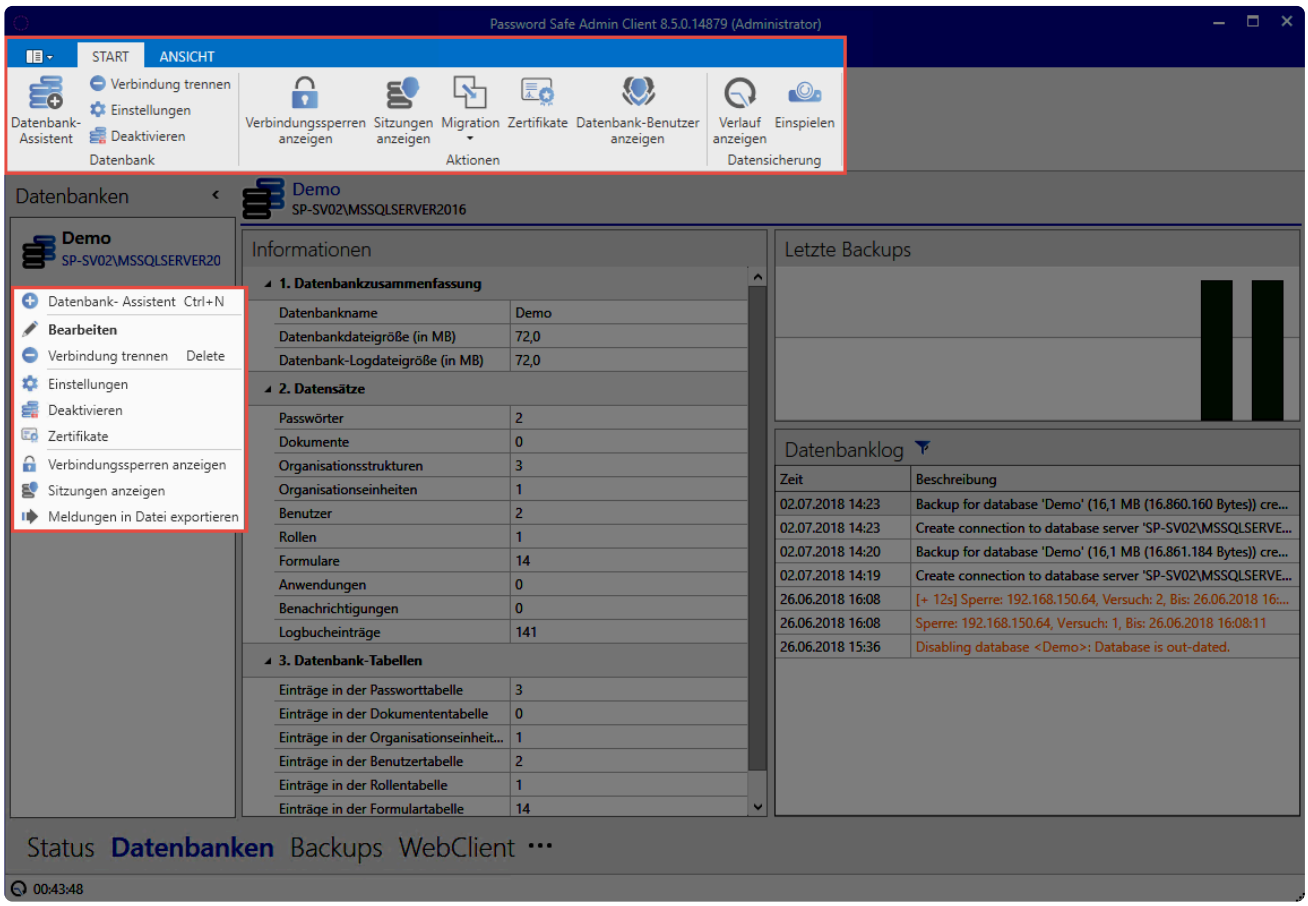
Hier können Sie individuell für die einzelnen Clients einstellen, wann eine inaktive Verbindung zum Anwendungsserver automatisch beendet wird. Wählen Sie dazu im Dropdown die gewünschte Zeitspanne aus und Speichern die Einstellung mittels klick auf “Speichern



Verwaltung von Datenbanken

Datenbank verwalten

Sowohl über das Kontextmenü der rechten Maustaste als auch über die Ribbon können Sie die zur Verfügung stehenden Aktionen selektieren.



Datenbankeinstellungen

Sämtliche Datenbankeinstellungen sind in der Datenbank hinterlegt. Melden Sie sich an, um die Einstellungen zu bearbeiten. Hierfür kann jeder beliebige, in der Datenbank existente Benutzer, verwendet werden. Dies ist auch mit konfigurierter Multifaktor-Authentifizierung möglich. Über die Ribbon können Sie stets die globalen Einstellungen wiederherstellen.

> ! Bei Datenbankadministratoren wird bei der Anmeldung aus sicherheitstechnischen Gründen eine konfigurierte Multifaktor-Authentifizierung ignoriert. Dadurch wird gewährleistet, dass bei einem möglichen defekt der Multifaktor-Authentifizierung die Datenbankadministratoren nicht ausgesperrt werden.

Multifaktor-Authentifizierung

In diesem Bereich konfigurieren Sie, welche Dienste für eine Multifaktor-Authentifizierung verwendet werden sollen. Verfügbar sind **RSA Secure ID**, **SafeNet** sowie **YubiKey NEO** und **YubiKey Nano**. Nach

der Selektion des gewünschten Dienstes geben Sie die jeweiligen Zugangsdaten an. Sie können auch mehrere Dienste konfigurieren. In diesem Fall kann dann am Client ausgewählt werden, welches Verfahren die einzelnen Benutzer verwenden.

Weiterführende Informationen zu diesem Thema finden Sie im Kapitel **Multifaktor-Authentifizierung**.

PKCS#11

Schützen Sie die Serverschlüssel über die PKCS#11 Schnittstelle mithilfe eines Hardwaresicherheitsmoduls (HSM). Hier konfigurieren Sie die Schnittstelle.

Automatische Bereinigung

Auf Wunsch können Sie hier das **Logbuch**, **Benachrichtigungen**, **Sitzungsaufzeichnungen** und auch **historische Dokumente** automatisiert bereinigen. Hierfür müssen Sie lediglich angeben, wie alt die Daten sein müssen, bevor sie entfernt werden. Logbucheinträge können Sie vor dem Löschen noch exportieren.

> ! Beachten Sie, dass das Logbuch auch für die Filterfunktion verwendet wird. Wird das Logbuch regelmäßig bereinigt, so ist es möglich, dass der Filter nicht mehr den vollständigen Funktionsumfang hat.

Datenbankaktionen

Verbindungssperren anzeigen

In der Ribbon werden alle Verbindungssperren angezeigt. Hierfür melden Sie sich zunächst an der Datenbank an. In einer Liste werden dann alle gesperrten User angezeigt:

- Benutzername (sofern bekannt)
- Grund der Sperre
- Anzahl der Loginversuche
- Ablauf der Sperre. Über einen Rechtsklick auf einen Eintrag entsperren Sie den Benutzer.

Über die entsprechende Schaltfläche sperren Sie einen User manuell. Wählen Sie den User aus, konfigurieren Sie den Ablauf der Sperre und geben Sie einen Grund an.

Sitzungen anzeigen / trennen

Über die entsprechende Schaltfläche können Sie sich alle aktuell verbundenen Clients anzeigen lassen. Nach der Selektion einer Sitzung können Sie die Verbindung trennen.

Migration

Starten Sie, nach dem Auswählen einer Datenbank über die Ribbon, die Migration. Über diesen Weg können Sie auch mehrere Version 7 Datenbanken zu einer zusammenführen.

> ! 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, sodass die Benutzer direkt weiterarbeiten können, sobald die Migration beendet ist.

Zertifikate

Extrem wichtig ist die Verwaltung der Zertifikate, welche im Kapitel Zertifikate beschrieben wird.

Datenbank-Benutzer anzeigen

Über diese Schaltfläche rufen Sie eine Statistik über die Benutzer in den jeweiligen Datenbanken aus. Es wird dargestellt, welcher Benutzer sich in welcher Datenbank befindet. Die Liste können Sie selbstverständlich auch exportieren.

Datensicherung

Lassen Sie sich hier den Verlauf aller getätigten Backups anzeigen oder spielen Sie ein Backup ein.

Verlauf anzeigen

Alle Backups der Datenbank werden hierarchisch in einer sortierbaren Liste dargestellt.

Einspielen

Hierüber spielen Sie ein Backup ein. Dies können Sie über eine Datei oder aus der Historie herstellen. Beschrieben wird der Vorgang unter Backupverwaltung.

HSM Anbindung über PKCS#11

Was ist die HSM Anbindung?

Über die HSM Anbindung erreichen Sie, dass die Serverschlüssel auf die HSM ausgelagert werden. Dies führt schlussendlich zu einem erhöhten Schutz, da die Schlüssel nicht direkt im Zugriff des Servers sind. Die Anbindung erfolgt über PKCS#11.

Voraussetzungen

Um eine HSM anbinden zu können, müssen Sie folgende Voraussetzungen schaffen:

- Eine lauffähige HSM muss vorhanden sein.
- Die PKCS#11 Treiber müssen am Anwendungsserver installiert sein.
- Die Enterprise Plus Edition muss lizenziert sein.
- Die Einrichtung erfolgt über den Datenbank Administrator am AdminClient.

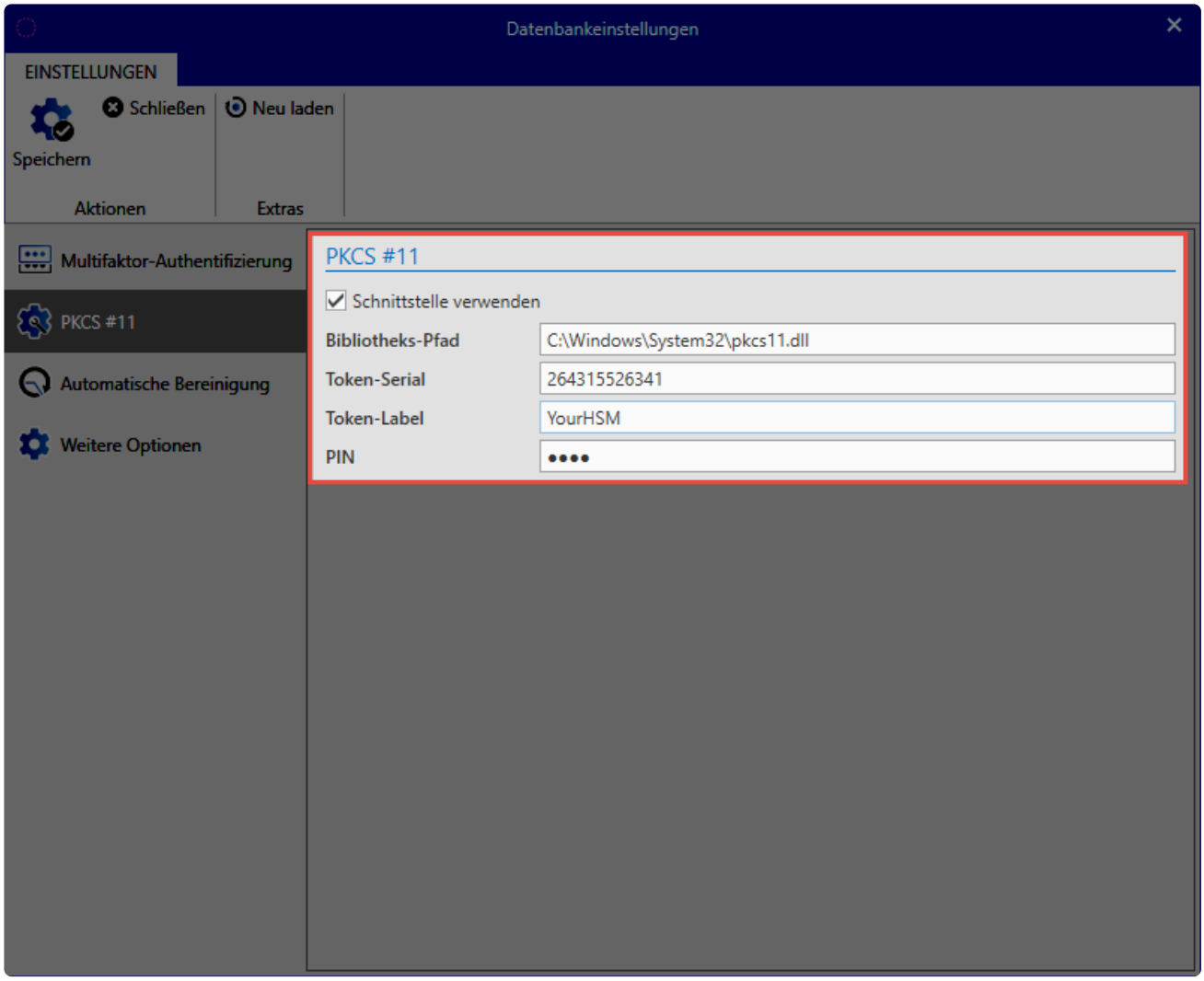
> ! Bitte beachten Sie: wenn eine HSM eingesetzt werden soll, müssen Sie auch die Datenbank von Grund auf damit einrichten. Es ist aktuell **nicht** möglich, eine bestehende Datenbank in eine HSM zu überführen.

Hardware Kompatibilität

Grundsätzlich sollte jede HSM mit der PKCS#11 Schnittstelle funktionieren. Es ist jedoch zu empfehlen, dies vorher in einer Teststellung oder einem POC auszuprobieren

Einrichtung

Die Einrichtung erfolgt am AdminClient über die **Datenbank Einstellungen**



- **Bibliotheks-Pfad**: Hier wird auf den installierten PKCS#11 Treiber der HSM verwiesen.
- **Token-Serial**: Geben Sie hier die Seriennummer des Tokens an.
- **Token-Label**: Dies ist der Name des Tokens.
- **PIN**: Abschließend geben Sie die PIN zur Authentifizierung am Token an.

Verwendung durch Password Safe

Sobald Sie die HSM angebunden haben, werden alle Serverschlüssel an die HSM übertragen. Hierbei handelt es sich um das **Datenbank Zertifikat**. Falls Sie das AD im Masterkey Modus angebunden haben, wird auch der **Masterkey** an die HSM übergeben. Die Zertifikate werden dann nicht mehr im Zertifikatsstore des Anwendungsservers hinterlegt, sondern zentral durch die HSM verwaltet. Alle anderen Schlüssel werden nicht auf der HSM abgelegt, sondern von den Masterschlüsseln abgeleitet. Daher greift Password Safe nur selten auf die HSM zu. Beispielsweise beim Serverstart oder beim AD Sync. Hierdurch kann die Last auf die HSM gering gehalten werden.

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. 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. Die aus der Version 7 bekannten Ordner wurden hierbei durch Organisationseinheiten ersetzt, welche durch Tags ergänzt werden. Die Datensätze werden nicht mehr in Ordner einsortiert, sondern kategorisiert.

Vorteile

Durch das neue Bedienkonzept ergeben sich etliche Vorteile gegenüber der Version 7. Über die Ordner konnten Sie einem Datensatz nur jeweils eine einzige Kategorie zuweisen. In der Version 8 können Sie einen Datensatz sowohl über die Zugehörigkeit zu einer Organisationseinheit als auch mit beliebig vielen Tags kategorisieren. Dies biete Ihnen eine viel flexiblere Möglichkeit der Einteilung. In der Version 7 gab es oftmals die Situation, dass in zahlreichen Ordnern genau die gleichen Unterordner verwendet wurden. Hier kommen nun die **Tags** ins Spiel. Diese können übergreifend zur Klassifizierung verwendet werden, um unnötige Redundanzen zu vermeiden.

Organisationseinheiten in der Strukturansicht

Um den Umstieg von der Version 7 zu erleichtern, können Sie die Organisationseinheiten auch als Struktur anzeigen lassen. In diesem Fall werden die Organisationseinheiten also ähnlich der bisherigen Ordner verwendet.

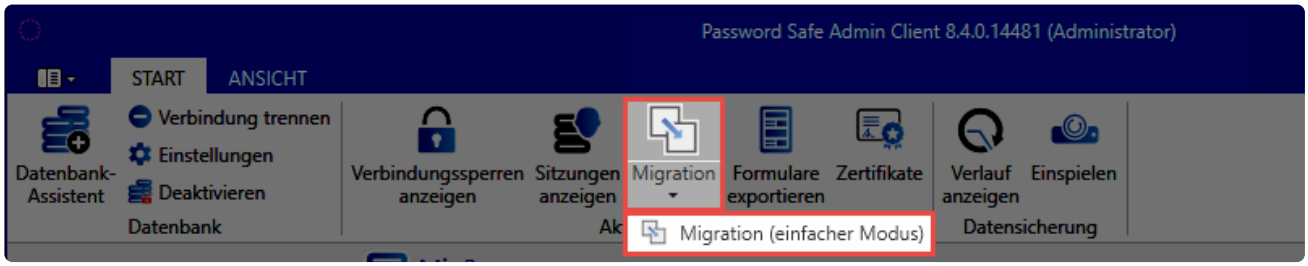
Kategorisierung während der Migration

Während der Migration können Sie festlegen, wie mit den, in ehemals Ordnern befindlichen, Datensätze umgegangen werden soll. Es erfolgt also ein “Mapping”, welches festlegt, wie diese Datensätze eingeteilt werden sollen. Sie können im Zuge der Migration für jeden Ordner separat festlegen, ob dieser als Organisationseinheit oder als Tag abgebildet werden soll. Ebenso können Sie einzelne Ordner von der Migration herausnehmen. Natürlich bleibt Ihnen auch die Möglichkeit die komplette Struktur aus der Version 7 zu übernehmen. Um die Arbeit zu erleichtern steht Ihnen ein entsprechender Assistent bereit, welcher in einem eigenen 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.

Einfache Migration – Die Verwendung der Struktur aus Version 7

Möchten Sie in der Password Safe Version 8 weiterhin mit der Struktur aus der Version 7 arbeiten, so steht Ihnen hierfür der **einfache Migrationsmodus** zur Verfügung. Diesen starten Sie ausschließlich über die Ribbon, nicht über den Datenbank Assistenten.



Im einfachen Migrationsmodus erfolgt keine Zuordnung von Tags und Organisationseinheiten. Vielmehr werden alle Ordner als Organisationseinheiten übernommen. Die Datenbank wird im Client auch direkt in der Strukturansicht gestartet. Somit erhalten Sie die von der Version 7 gewohnte Struktur.

Parallelbetrieb von Version 7 und 8

Technisch gesehen ist es möglich die 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

Stellen Sie vor der Migration sicher, dass sowohl der Server als auch der Client der Version 8 installiert sind. Informationen hierzu finden Sie im Kapitel Erste Schritte. Weiterhin sollten Sie **vor** der Migration festlegen, ob Active Directory Benutzer im Master Key Modus oder Ende zu Ende verschlüsselt importiert werden sollen. Das Kapitel Active Directory Anbindung hilft Ihnen bei der Entscheidungsfindung.

> ! Der Master Key Modus und die Ende zu Ende Verschlüsselung unterscheiden sich erheblich voneinander. Daher sollten Sie diese Entscheidung sorgfältig prüfen und treffen. Weitere Infos erhalten Sie in einem separaten Kapitel.

Vorbereitungen Version 7

E-Mail Adressen

In der v7 Datenbank müssen Sie bei allen lokalen Benutzern sowie allen Usern, welche im **Ende zu Ende Modus** migriert werden sollen, eine E-Mail Adresse hinterlegen. 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 Sie hierfür keine E-Mail Adressen hinterlegen. In diesem Fall müssen Sie den einzelnen Benutzern manuell Passwörter zuweisen. 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 benötigen Sie den zugehörigen **private key** mit der Endung .prvkey.
- Sie benötigen das **Datenbankpasswort** (bei Single- und Multiuser-Datenbanken).

Offline Modus und USB-Sticks

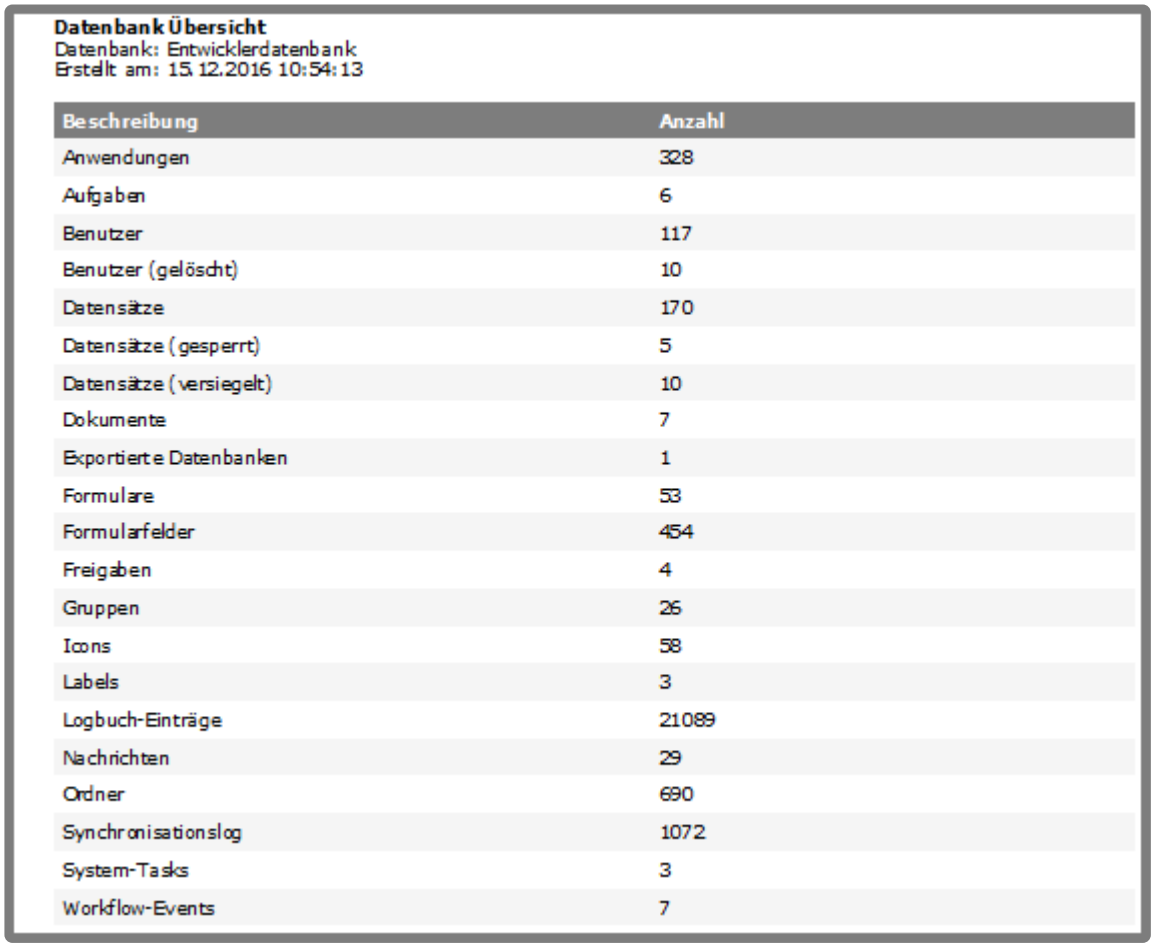
- Synchronisieren Sie alle Offline-Datenbanken vor der Migration.
- Alle USB-Sticks müssen Sie vor der Migration synchronisieren.

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 Ihnen das “Zurechtfinden” in der Version 8. Die Datenbankübersicht rufen Sie in der Version 7 über **Bearbeiten -> Reports -> Datenbankübersicht** aus. Dies 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

- Löschen Sie nicht mehr benötigte Datensätze, Dokumente, Ordner oder Anwendungen. Die Bereinigung persönlicher Datensätze und Dokumente muss durch den Benutzer selbst durchgeführt werden.
- Es bietet sich an, dass Sie Ordnerstrukturen mit Ausblick auf die Migration schon im Vorfeld anpassen.
- 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, löschen Sie ihn. 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, können Sie mit Labels Datensätze „Taggen“ und so einen bestimmten Bereich 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.

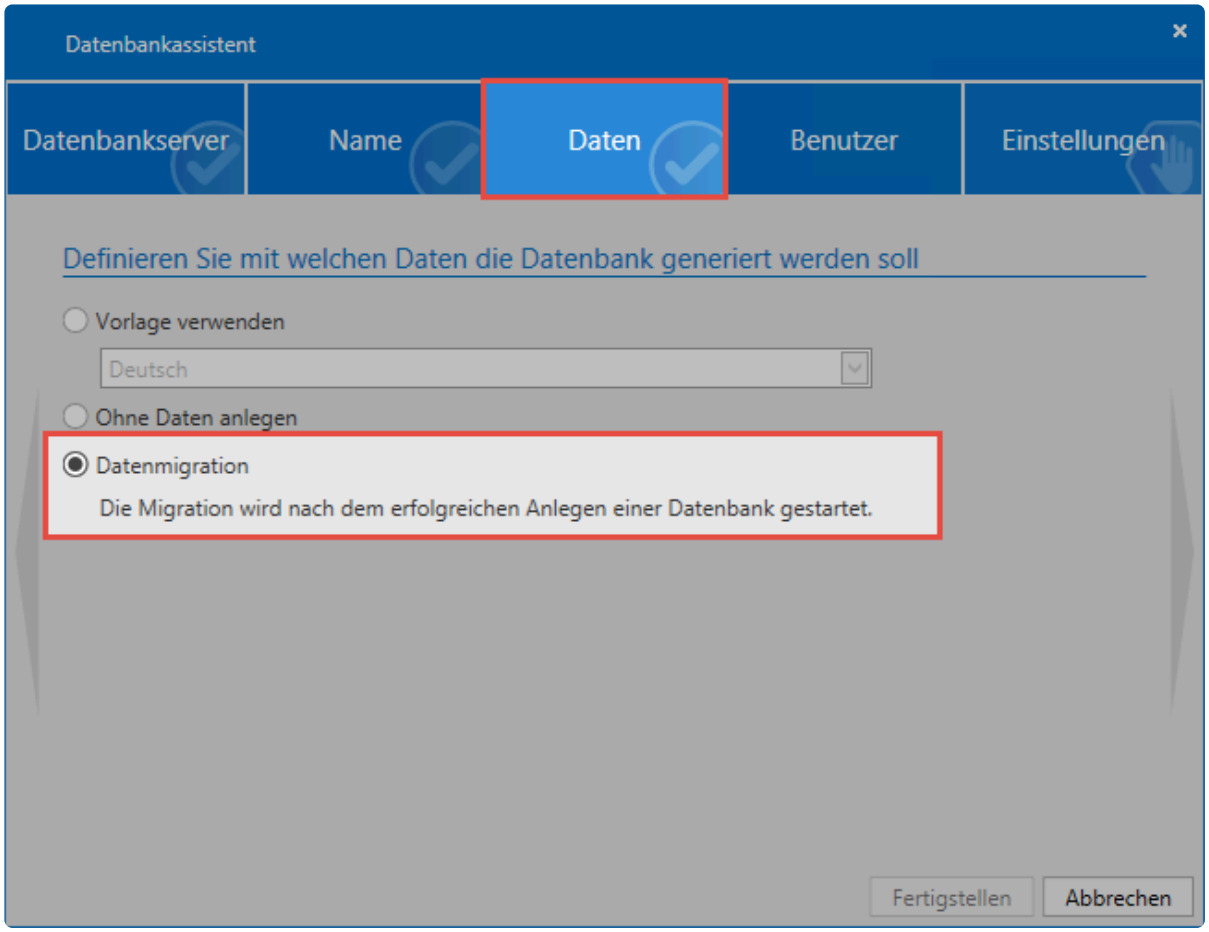
Starten des Migrationslaufs

Was ist der Migrationslauf?

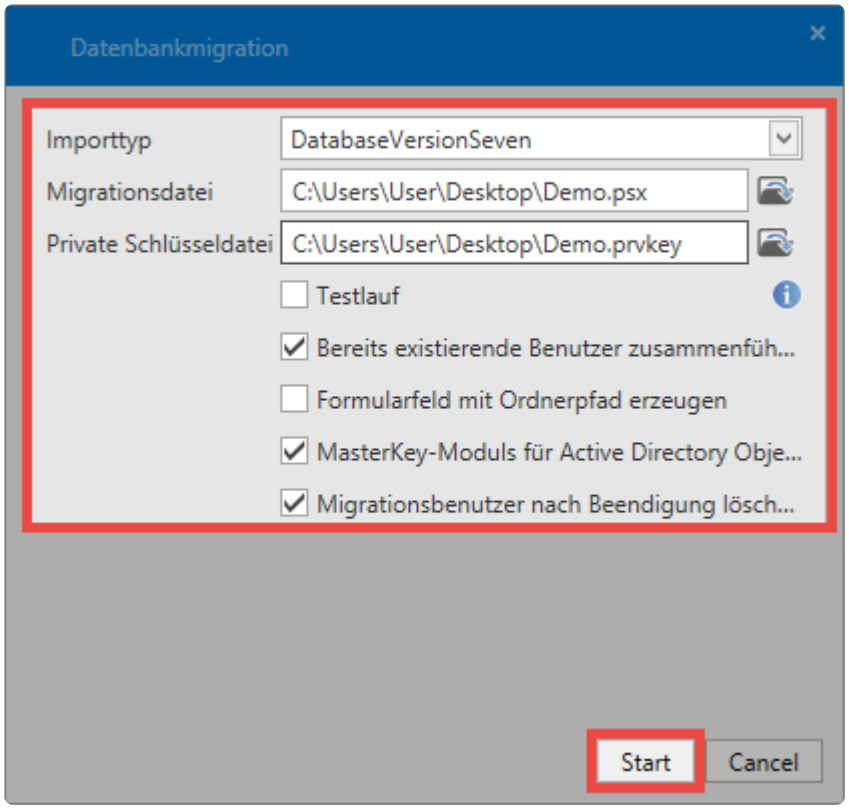
Der Migrationslauf beschreibt die tatsächliche Durchführung der Portierung, bei der alle Daten aus einer Datenbank der Version 7 in eine neue / vorhandene Datenbank der Version 8 umgewandelt werden. Ebenso werden die aufgrund der Umgestaltung des Berechtigungskonzeptes notwendigen Anpassungen am Datenbestand durchgeführt.

Starten der Migration

Zunächst wird wie im Kapitel Erstellen und Verwaltung von Datenbanken beschrieben eine neue Datenbank erstellt. Im dritten Schritt des Assistenten aktivieren Sie die Datenmigration.



Nach Abschluss des Datenbankassistenten gelangen Sie direkt in den Migrationsassistenten.



- Wählen Sie den gewünschten **Importtyp** aus.

> Momentan wird nur ein Import aus Password Safe v7 unterstützt. Falls Sie Migrationen älterer Datenbankversionen anstreben, müssen Sie den Zwischenschritt über die Version 7 nehmen.

- Unter **Migrationsdatei** wählen Sie das zuvor erstellte Password Safe v7-Backup im Format **.psx** aus.
- Sie müssen bei der Migration einer Serverdatenbank die zugehörige **private Schlüsseldatei** im Format .prvkey auswählen. Bei Single- und Multiuser Datenbanken werden Sie 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. bei deaktiviertem Masterkey Modus, können Sie **zufällige Passwörter erzeugen**. 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**: Migrieren Sie eine bestehende Datenbank, werden eventuell 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 dann “**” 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**: Sie entscheiden, ob die AD-Benutzer im Master Key Modus oder Ende zu Ende verschlüsselt importiert werden. Beachten Sie, dass im

Master Key Modus ein entsprechendes Zertifikat erstellt wird.
- Falls Sie in der Version 7 eine eigene Ordnerstruktur für die Dokumente haben, so können die **Dokumentordner als Organisationseinheit angelegt** werden.
- Es wird empfohlen, das Sie den **Migrationsbenutzer löschen**, da dieser durch die Migration auf alle Datensätze der Datenbank berechtigt wird! In der Regel benötigen Sie diesen nach der Migration nicht mehr, da der Administrator aus dem migrierten Backup als Benutzer übernommen und zukünftig genutzt wird.

! Sie sollten vor dem Import genau abwägen, ob Sie 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.

✻ Beachten Sie, dass alle lokalen Benutzer sowie jene, welche mit der Ende zu Ende Verschlüsselung migriert werden, eine E-Mail mit einem zufallsgeneriertem 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 Datenbankgröße kann dieser Schritt mehrere Stunden beanspruchen.

✻ Sollte ein Fehler auftreten, erzeugt der Assistent einen Logfile-Eintrag. Diesen finden Sie im Pfad **C:\Users\User\AppData\Roaming\MATESO\Migration**.

Migration in eine bestehende Datenbank

Über die Ribbon können Sie die Migration auch in eine bestehende Datenbank durchführen. Der Ablauf der Migration bleibt gleich. Durch diese Funktion können Sie mehrere Datenbanken zusammenführen. 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 währenddessen mit der Datenbank verbunden, können sie die Datenbank nicht verwenden.

! Migrieren Sie mehrere Datenbanken in eine, so muss dies mit dem gleichen Migrationsbenutzer geschehen. Dieser User dürfen Sie erst bei der Migration der letzten Datenbank löschen .

Zuordnung von Tags und OUs

> Haben Sie den **einfachen Migrationsmodus** gewählt, erfolgt keine Zuordnung. Vielmehr werden dann alle Order als Organisationseinheit klassifiziert um die Struktur der Version 7 abzubilden.

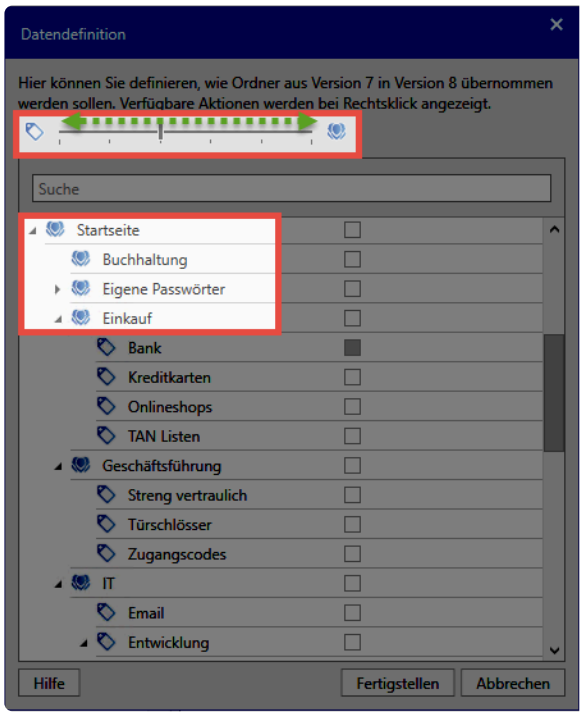
Warum eine Zuordnung von Tags und OUs?

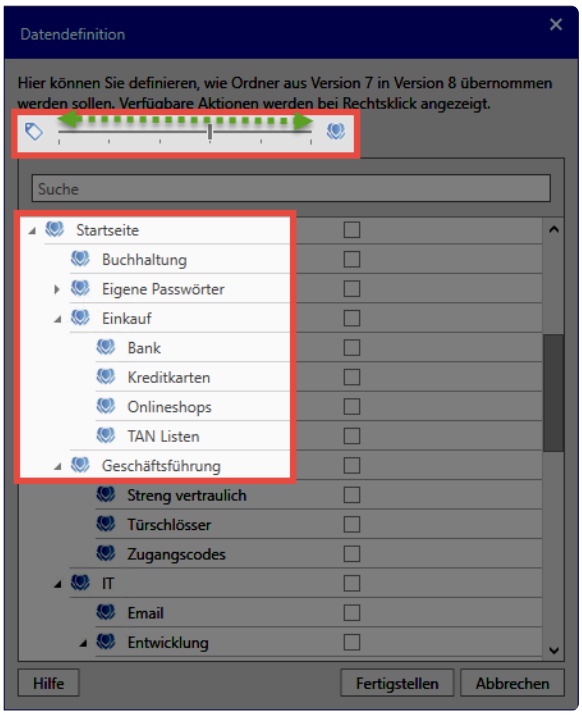
An den vorherigen Arbeitsschritt anschließend wird nun die Ordnerstruktur der Version 7 dargestellt. Aufgrund der bereits genannten Änderungen am Bedienkonzept der Version 8 legen Sie nun fest, wie die Daten zukünftig kategorisiert werden sollen. Hierbei legen Sie fest, welcher Ordner aus der Version 7 in der Version 8 in eine Organisationseinheit, bzw. ein Tag, umgewandelt werden soll. Die Bedeutung der Icons in der Ansicht ist 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 legen Sie fest, bis in welche Ebene, im Zuge der Migration, Ordner in Organisationseinheit umgewandelt werden sollen – alle darunterliegenden Ordner werden zu Tags. So können Sie eine gewisse Vorauswahl treffen, welche dann noch manuell verfeinert werden kann. Durch wiederholtes “Klicken” wechseln Sie zwischen Tag, Organisationseinheit und Ordnern ohne Zuordnung.

> Wird der Schieberegler ganz nach rechts verschoben, werden alle Ordner als Organisationseinheiten migriert. Es wird die komplette Struktur der Version 7 übernommen.

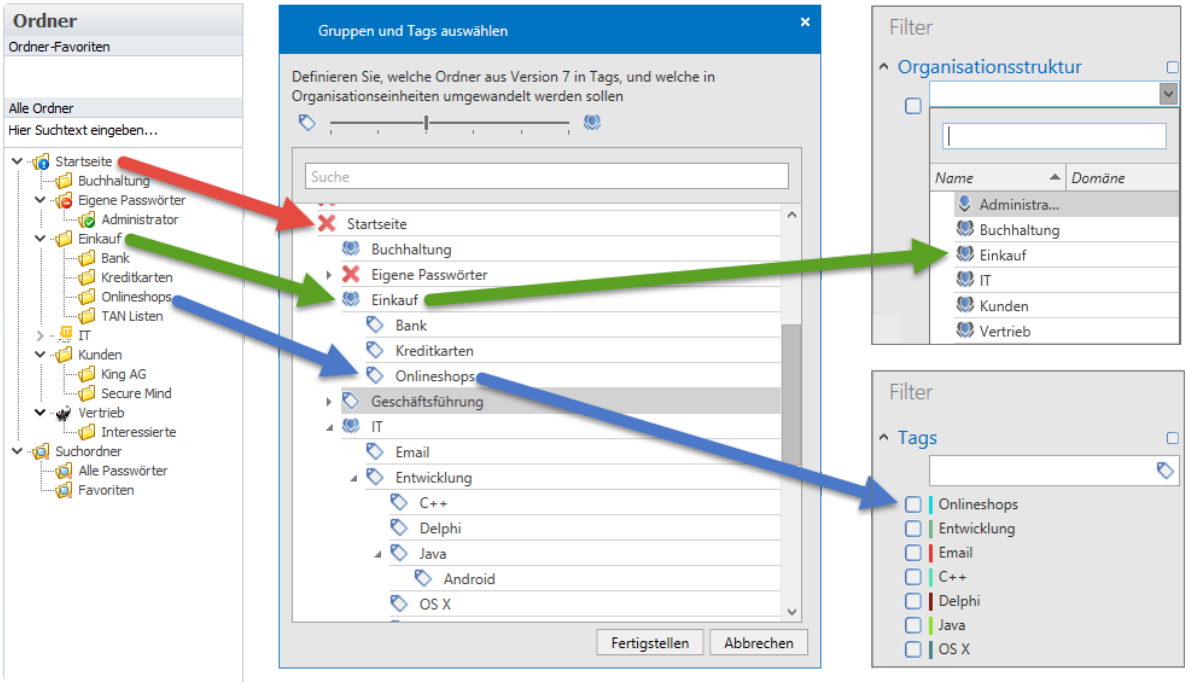




Über das Kontextmenü (rechte Maustaste) eröffnen sich weitere Optionen:

- Kategorisierung aller Unterobjekte als Organisationseinheit
- Kategorisierung aller Unterobjekte als Tag
- Alle Unterobjekte ignorieren
- Löschen aller zuvor gesetzten Markierungen

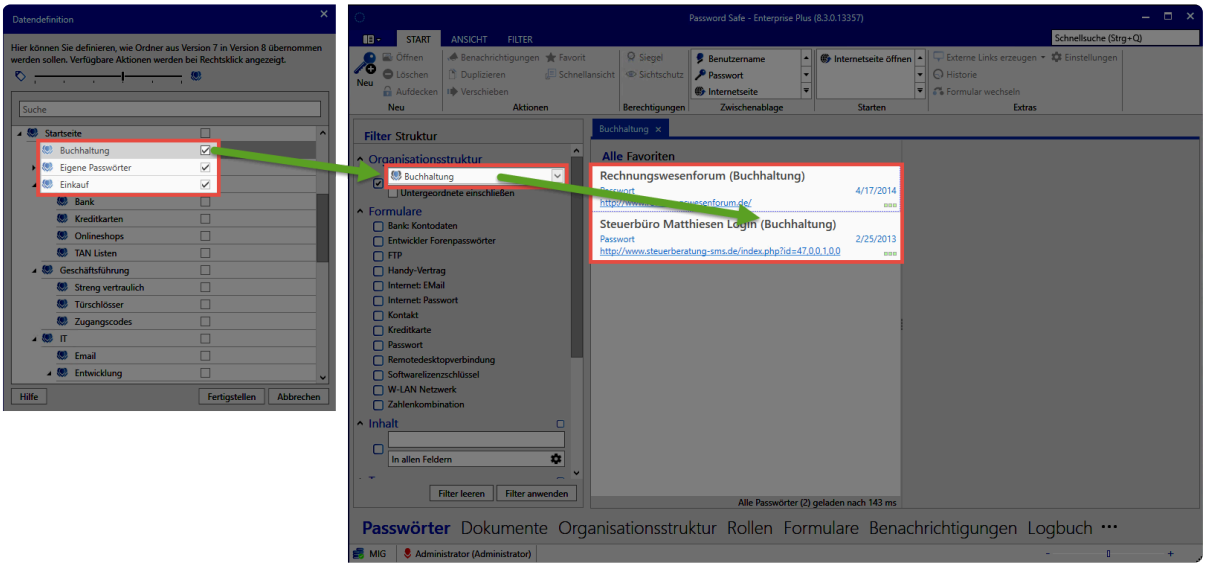
Im nachfolgenden **Schaubild** ist ein mögliches Vorgehen bei der Zuweisung von Ordnern zu Organisationseinheiten und Tags abgebildet:



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.

Sie haben auch die Möglichkeit die Ordnernamen in die Datensatzbeschreibung aufzunehmen. Hierfür steht bei jedem Ordner eine entsprechende Schaltfläche bereit.



Über das Kontextmenü können Sie die Option für alle Ordner setzen.

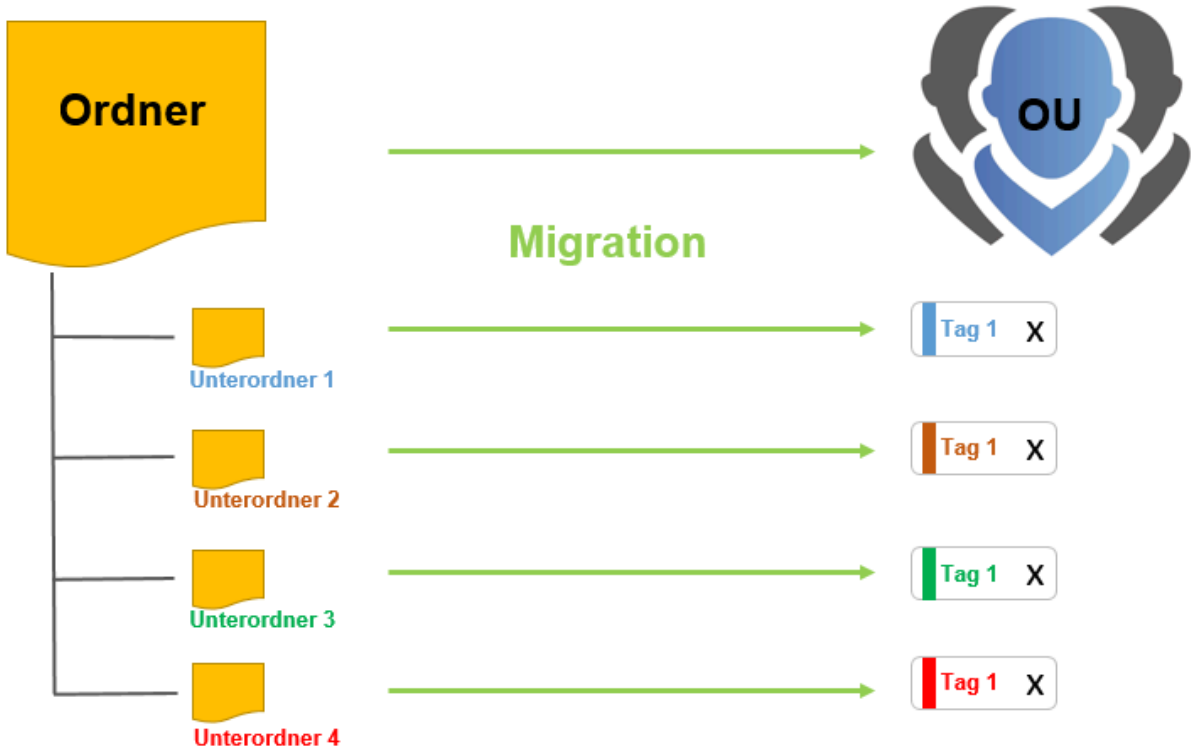
Abschließen der Migration

Über **Fertigstellen** werden die Daten in die Datenbank übertragen. **Die Migration kann – je nach Umfang – durchaus mehrere Stunden dauern**. Falls Sie keinen Master Key Modus gewählt haben, bekommen die importierten Benutzer per E-Mail zufallsgenerierte Passwörter und können sich direkt anmelden. Beim ersten Anmelden müssen diese Passwörter geändert werden. Der Benutzer, mit dem Sie die Migration durchgeführt haben, wir direkt gelöscht, falls Sie dies so konfiguriert haben.

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. Erstellen Sie einen Datensatz in einem Ordner, so wurde der Datensatz analog zu den Berechtigungen des zugehörigen Ordners berechtigt. Solange Sie nur vereinzelte Ordner aus der Version 7 im Rahmen der Migration auf Organisationseinheiten in der Version 8 “mappen”, ändert sich dieses Vorgehen nicht. Es wird für die Organisationseinheit automatisch ein Rechtepreset definiert (**vordefinierte Rechte**), welches bei zukünftigen Datensätzen automatisch die vorgesehenen Rechte gibt. Da bei der Zuordnung von Tags aus Unterordnern nun Tags werden können, müssen Sie einen neuen Mechanismus anwenden, da Tags keine Rechte besitzen. Um ein einheitliches System verfolgen zu können, helfen hier die den vordefinierten Rechten zugehörigen Rechtevorlagengruppen weiter.

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 die Datenbankzusammenfassung 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 wird nachfolgend eingegangen.

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 Sie unter „Alle Passwörter“ all diejenigen Passwörter einsehen, auf welche ein Benutzer berechtigt ist. Dies können Sie in der Version 8 ggf. nicht immer überprüfen, da die Version 8 maximal 1000 Passwörter ausgeben kann. Ist ein Benutzer auf mehr als 1000 Datensätze berechtigt, müssen Sie den Filter dementsprechend anpassen.

> ! In Version 7 konnten Sie über eine Rechtevorlage konfigurieren, dass auf Datensätze kein Benutzer das Berechtigen Recht hat. Dies wurde gerne bei persönlichen Datensätzen angewandt, damit diese nicht geteilt werden können. In Version 8 steuern Sie das Teilen von persönlichen Datensätzen über ein Benutzerrecht. Es ist jedoch zwingend nötig, dass auf jeden Datensatz mindestens ein Benutzer das Berechtigen Recht hat. Aus diesem Grund werden bei der Migration die Rechte angepasst. Zunächst wird geprüft, ob auf die betroffenen Datensätze jemanden mit Löschen berechtigt ist. In diesem Fall erhalten diese Nutzer oder Rollen zusätzlich das Berechtigen Recht. Ist niemanden zum Löschen berechtigt, werden alle gesetzten Rechte um das Berechtigen Recht erweitert.

Siegel

Siegel werden – je nach Ausprägung in der Version 7 – unterschiedlich migriert. Sicherheitshalber sollten Sie die Anzahl der versiegelten Datensätze ebenso abgleichen.

- **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 zu brechen.
- **Begründungen für den Siegelbruch** aus der Version 7 werden übernommen.
- Eine Abweichung existiert 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 entsprechende 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 Sie einzelne Anwendungen nochmals neu anlernen 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. Sollten Sie dies nicht wünschen, 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. Mithilfe des Filters können Sie diese schnell identifizieren.

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. 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 Sie dies überprüfen und nach Bedarf anpassen.

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 können Sie, vor der Migration, mit Labels 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 Sie nun über das gleichnamige Modul abbilden.

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.

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 eventuell übergeordnete 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.

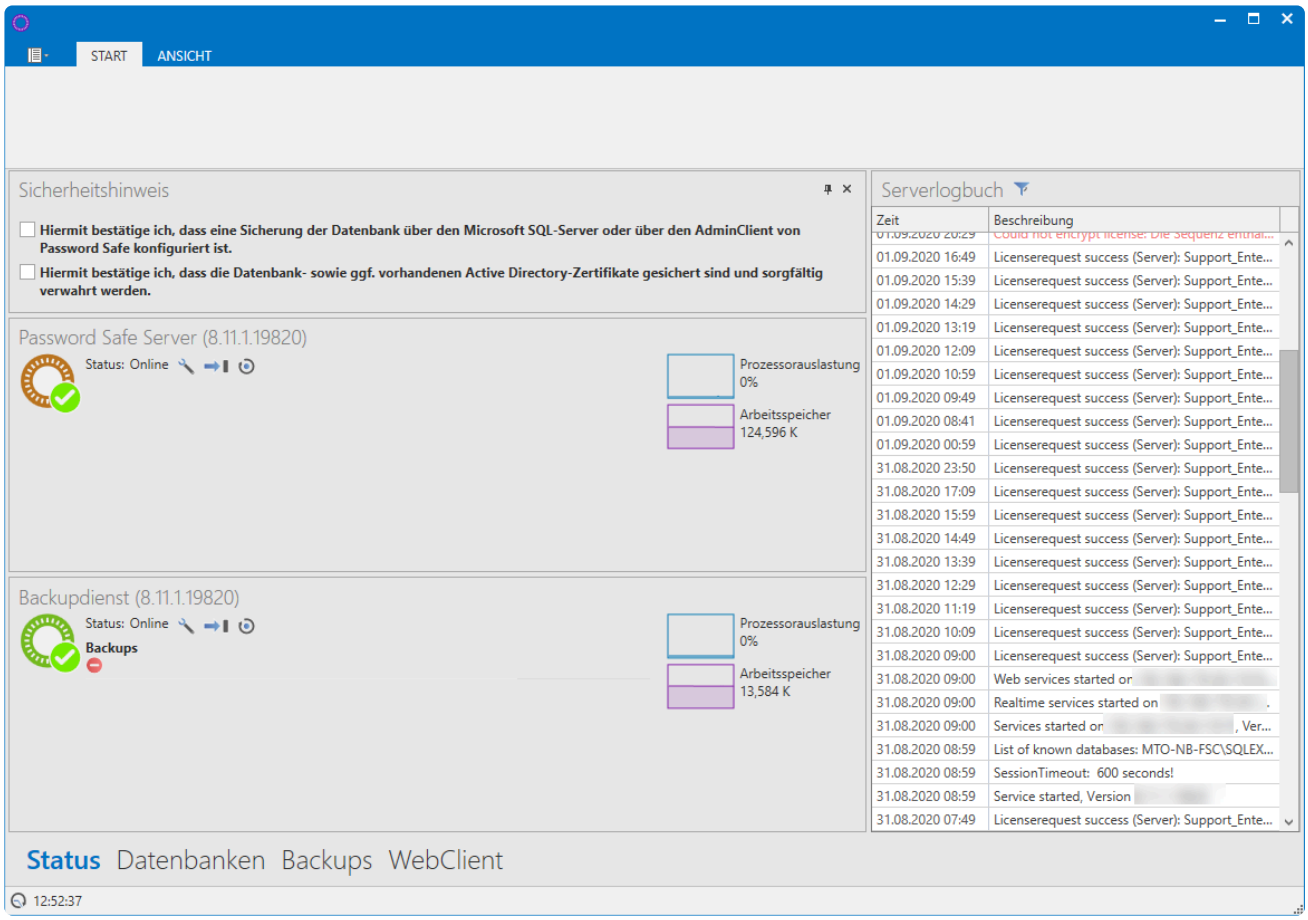
Bedienung und Aufbau

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 benötigen Sie ein Initialpasswort. Dieses lautet “admin”. Direkt nach der Anmeldung sollten Sie es ändern und sauber dokumentieren.

Das Modul Status



1. Ribbon

Wie gewohnt finden Sie oben die Ribbon. Da das Modul ein rein informatives ist, gibt es in der Ribbon keine Funktionen, außer dem Aktualisieren der Ansicht.

2. Infobereich

- Der Infobereich bereich links zeigt den Status der einzelnen Dienste an. Über das Icon können Sie die Dienste konfigurieren. Standardmäßig wird die Konfiguration aus der Basiskonfiguration

verwendet. Falls nötig ersetzen Sie einzelne Parameter bzw. passen diese auf die persönlichen Bedürfnisse an.

- Über stoppen bzw. starten Sie den jeweiligen Dienst.
- 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. Mithilfe des Mouseovers 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:

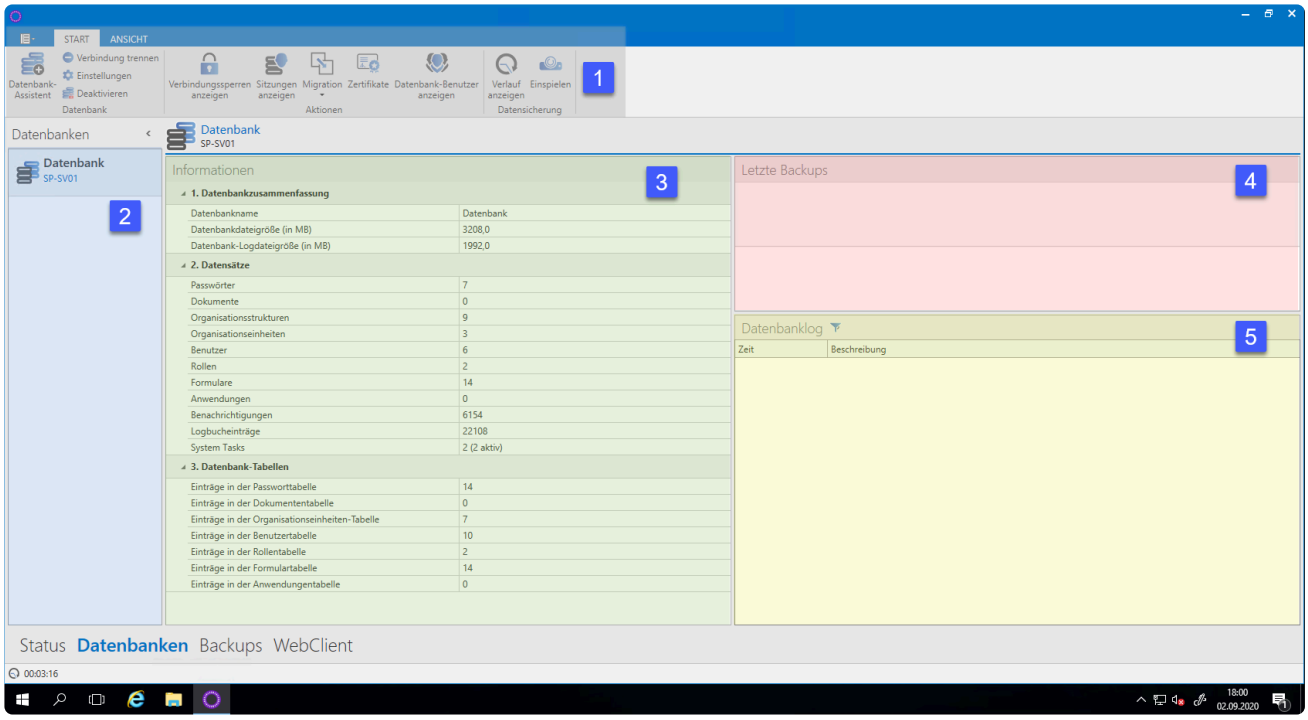
Erwartete Aktionen	schwarz
Ereignisse, welche Aufmerksamkeit fordern	orange
Probleme und Abbrüche	rot

- 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 können Sie über die Spaltenüberschriften nach Datum und Beschreibung auf- und absteigend sortieren. Über schränken Sie den dargestellten Zeitraum ein.

Das Modul Datenbanken

Datenbanken verwalten Sie in einem eigenen Modul. Ebenso können Sie alle relevanten Informationen zu den vorhandenen Datenbanken abrufen, ohne Zugriff auf den SQL-Server.



1. Ribbon

2. Datenbankenübersicht

In der Datenbankenübersicht werden alle Datenbanken alphabetisch sortiert aufgeführt. Diesen Bereich minimieren Sie über das Pfeilsymbol am oberen, linken Rand. Über einen Rechtsklick auf eine der Datenbanken, wird ein Kontextmenü mit allen verfügbaren Funktionen eingeblendet.

3. Infobereich

Im Infobereich werden alle Informationen zur aktuell in der Datenbankenübersicht selektierten Datenbank dargestellt. Diese sind in die drei Unterbereiche “Datenbankzusammenfassung, Datensätze und Datenbank-Tabellen “ unterteilt.

4. Letzte Backups

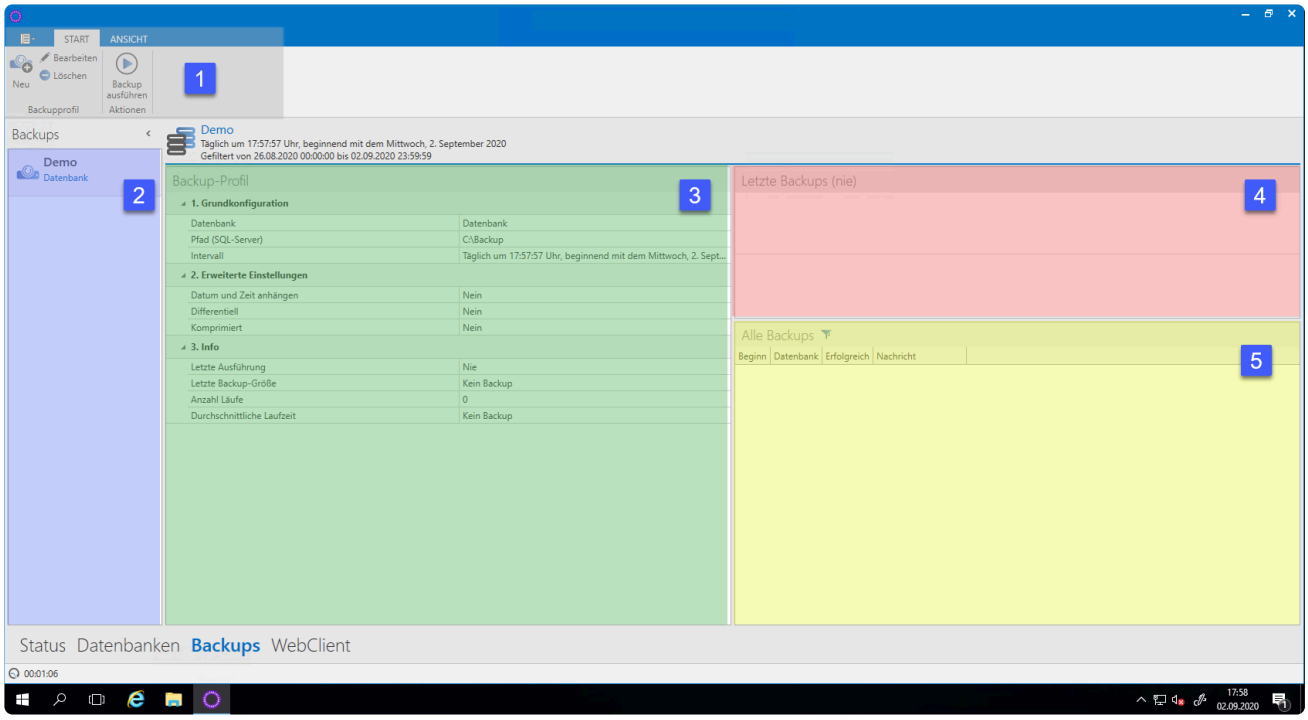
Hier finden Sie eine Liste der zuletzt gelaufenen Backups, welche Sie nach Datum sortieren können.

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 Sie sämtliche Backups direkt im Admin Client konfigurieren und verwalten.



1. Ribbon

2. Backupübersicht

Hier werden alle konfigurierten Backups aufgeführt. Sie können die Ansicht nach links minimieren. Weitere Funktionen finden Sie indem Sie einen Rechtsklick ausführen.

3. Infobereich

Der Infobereich ist in drei Bereiche aufgeteilt. Sie können zwischen “Grundeinstellungen, erweiterte Einstellungen sowie Infos” zur ausgewählten Datenbank wählen.

4. Letzte Backups

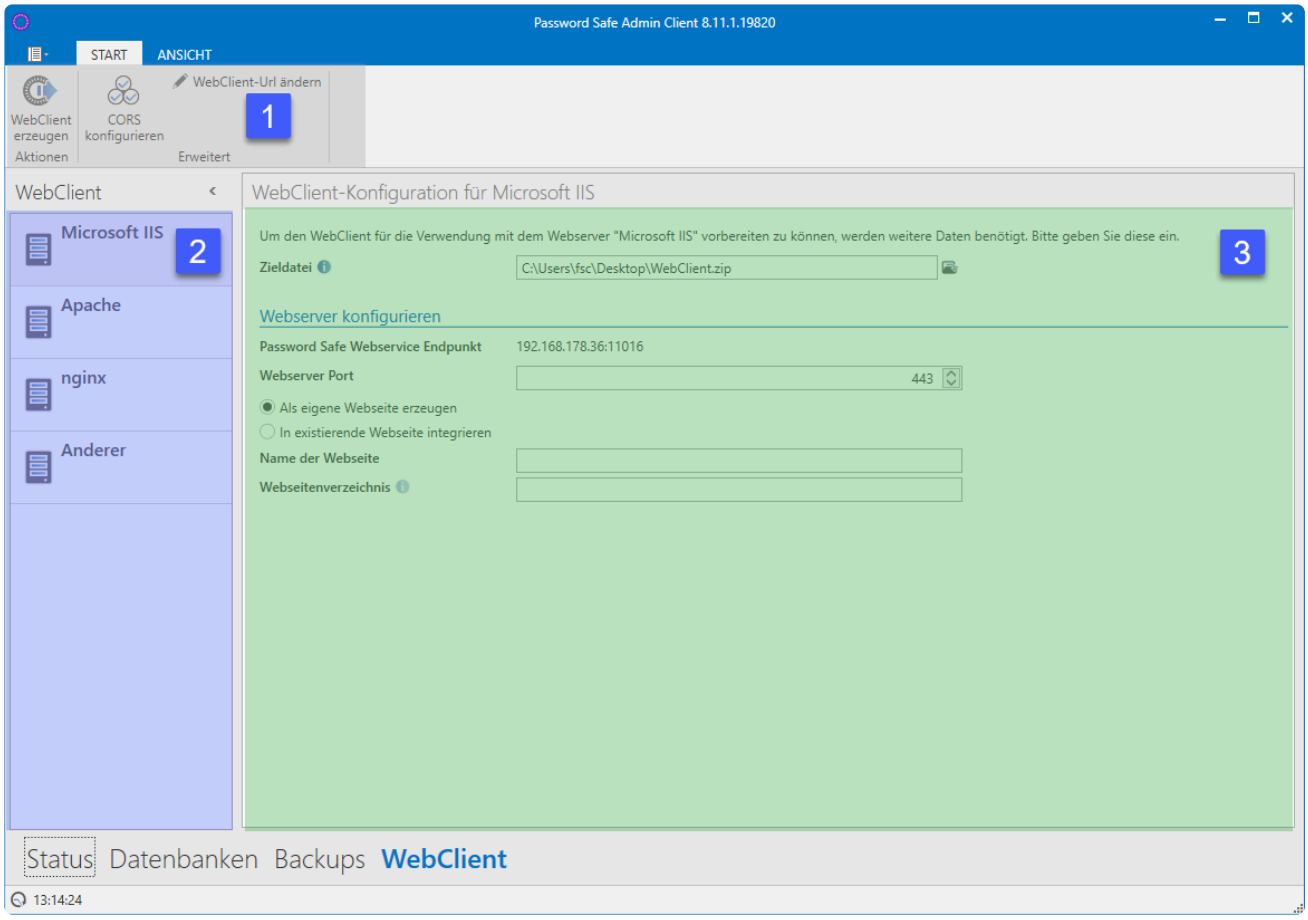
Rechts werden in einer Liste die zuletzt gelaufenen Backups dargestellt.

5. Alle Backups

Eine tabellarische Übersicht stellt alle bisherigen Backups dar. Sie haben die Möglichkeit diese Ansicht zu sortieren. Hier sehen Sie auf einen Blick, wann welche Datenbank gesichert wurde und ob das Backup erfolgreich war.

Das WebClient Modul

In diesem Modul konfigurieren Sie den WebClient. Die Installation des WebClients wird Ihnen in einem separaten Kapitel beschrieben.



1. Ribbon

Den WebClient erzeugen Sie hier. Außerdem haben Sie die Gelegenheit **CORS** zu definieren.

2. Webserver

Den gewünschten Webserver wählen Sie auf der rechten Seite aus.

3. WebClient-Konfiguration

Damit der WebClient ordnungsgemäß funktioniert, muss dieser von Ihnen entsprechend konfiguriert werden.

Hauptmenü

Was ist das Hauptmenü

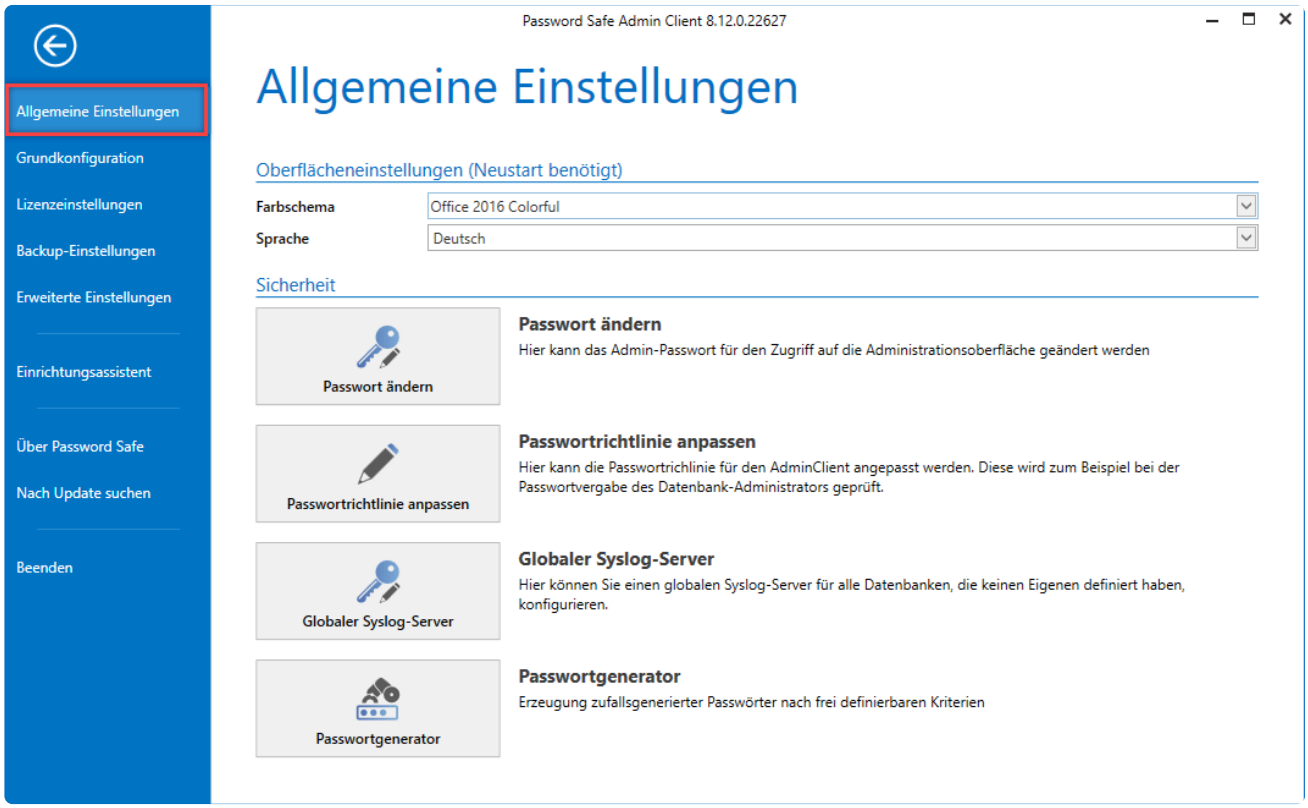
Analog zum Hauptmenü des Clients erfolgt die Bedienung und der Aufbau des Hauptmenüs/Backstage-Menüs. Dieser Bereich ist unabhängig vom aktuell ausgewählten Modul nutzbar.

- Allgemeine Einstellungen
- Backup-Einstellungen
- Lizenzeinstellungen
- Erweiterte Einstellungen

Allgemeine Einstellungen

Was sind die allgemeinen Einstellungen?

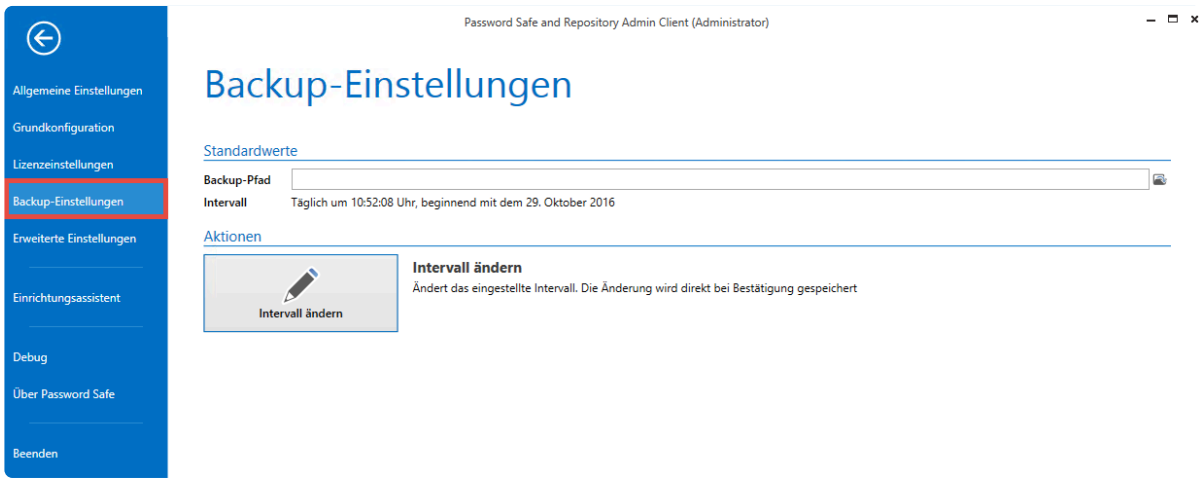
Innerhalb der allgemeinen Einstellungen konfigurieren Sie die Oberflächeneinstellungen, zum Beispiel das Farbschemas oder die genutzte Sprache. Ebenso ändern Sie hier das Passwort für die Anmeldung am Admin Client.



Backup-Einstellungen

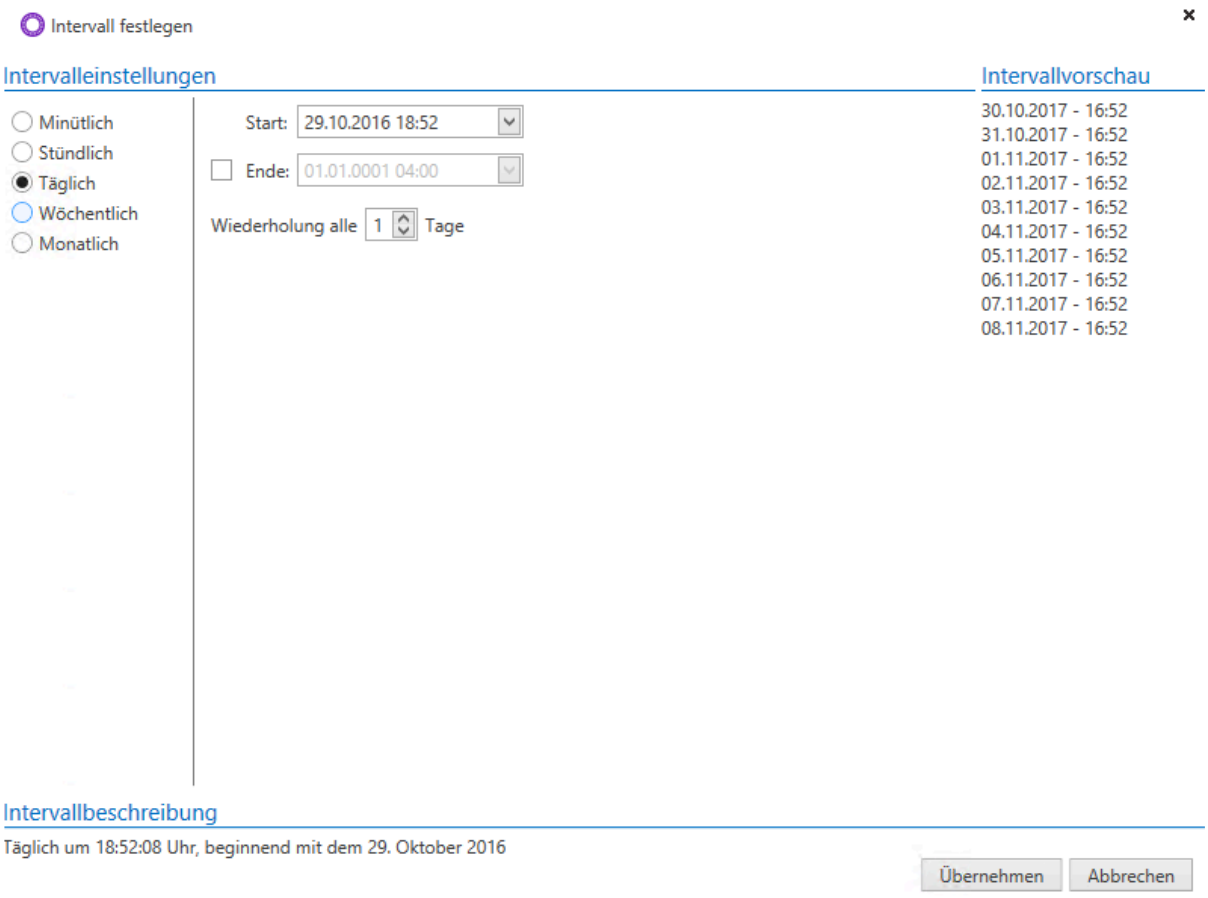
Was sind Backup-Einstellungen?

Innerhalb der Backup-Einstellungen können Sie die Standardwerte für die Durchführung von Datensicherungen festlegen.



Intervalleinstellungen

Das Intervall für Backups lässt sich beliebig definieren. Hierfür steht Ihnen eigens ein Assistent zur Verfügung.



Backupverwaltung

Einleitung

Das regelmäßige Sichern von Daten in Form von Backups sollte stets Teil eines jeden Sicherheitskonzepts sein. Erstellen Sie am SQL Server zentral Backups, empfiehlt es sich die Password Safe Datenbanken hier ebenso aufzunehmen. Werden keine zentralen Backups auf SQL-Ebene verwendet, können Sie über den Admin Client Backup-Profile erstellen. 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 anfangs erstellten Backup gesichert. Hierdurch kann sowohl Zeit als auch Speicherplatz gespart werden.

> Bitte beachten Sie, dass das differentielle Backup in das letzte vorhandene Vollbackup geschrieben wird!

Backupkonzept

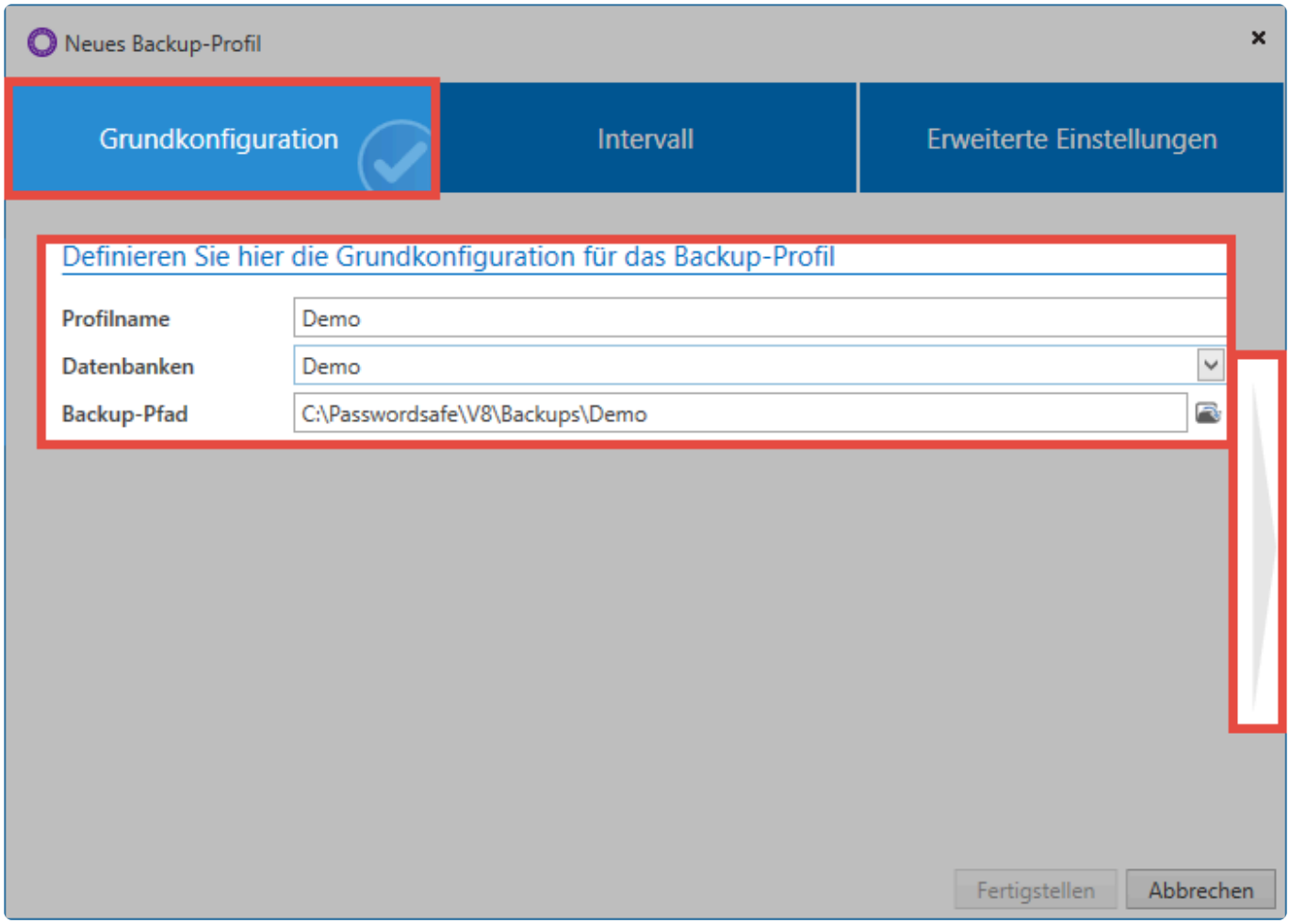
Empfohlen wird, stündlich ein differentielles Backup zu erstellen. Zusätzlich sollten Sie einmal in der Woche ein komplettes Backup erzeugen.

Backup Zeitpläne verwalten

Backup Zeitplan erstellen

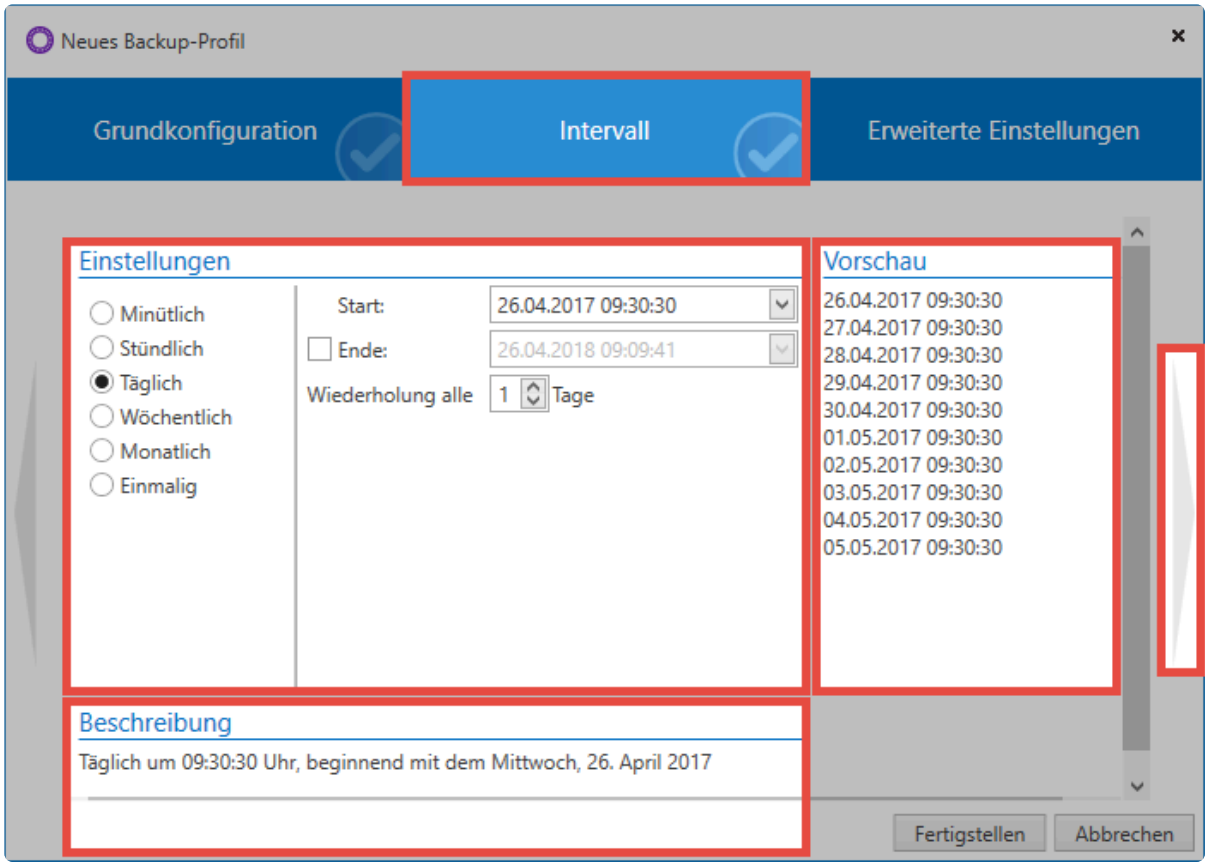
Über die Ribbon erzeugen Sie ein neuen Zeitplan. Dies wird durch einen Assistenten erleichtert. Alle unter Backup-Einstellungen definierten Angaben, werden als Standard herangezogen.

Zunächst vergeben Sie einen Profilname, wählen Sie dann die gewünschten Datenbanken aus und legen Sie fest, in welchem Verzeichnis die Backups erzeugt werden sollen.

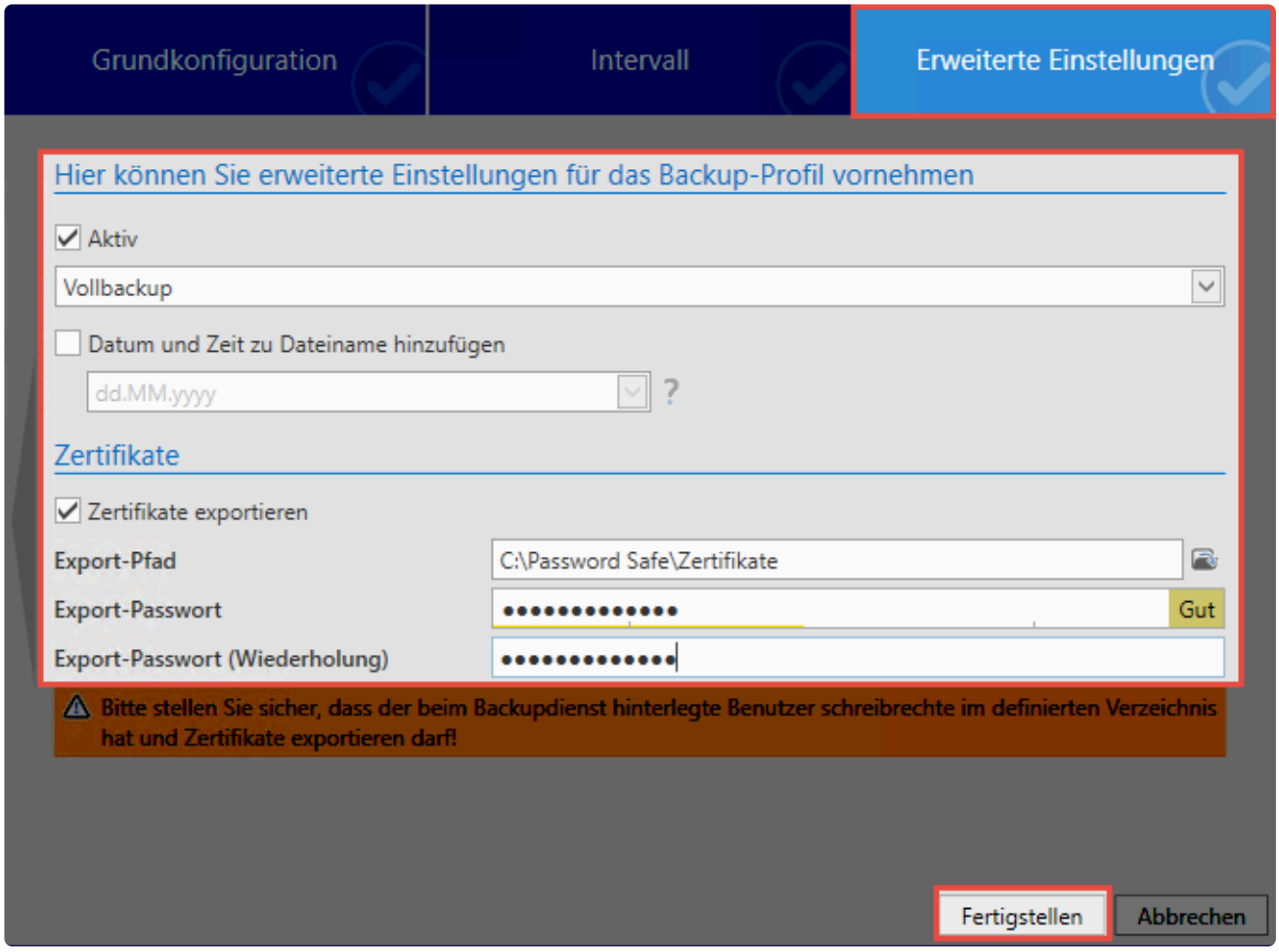


Es handelt sich hier um ein Verzeichnis direkt auf dem SQL-Server.

Im nächsten Schritt legen Sie das Intervall fest, in welchem die Backups erzeugt werden sollen. Rechts wird Ihnen in einer Vorschau dargestellt, wann die Backups zukünftig erstellt werden. Geben Sie optional ein Enddatum an.



In den erweiterten Einstellungen konfigurieren Sie zunächst, ob das Backup direkt aktiv geschaltet werden soll. Zudem können Sie hier festlegen, ob differentielle Backups erzeugt werden sollen. Fügen Sie dem Dateinamen Datum und Uhrzeit hinzu, so wird mit jedem Lauf ein neues Backup erzeugt. Geschieht dies nicht, wird immer das letzte Backup überschrieben. Zum Erstellen des Backups nutzen Sie den Dienstbenutzer oder geben Sie einen Servicebenutzer mit Namen und Passwort an. Weiterhin können Sie hier angeben, ob die benötigten Zertifikate durch den Backup Task mitgesichert werden sollen. Weitere Infos finden Sie im Kapitel Zertifikate.



Lauf der Backups

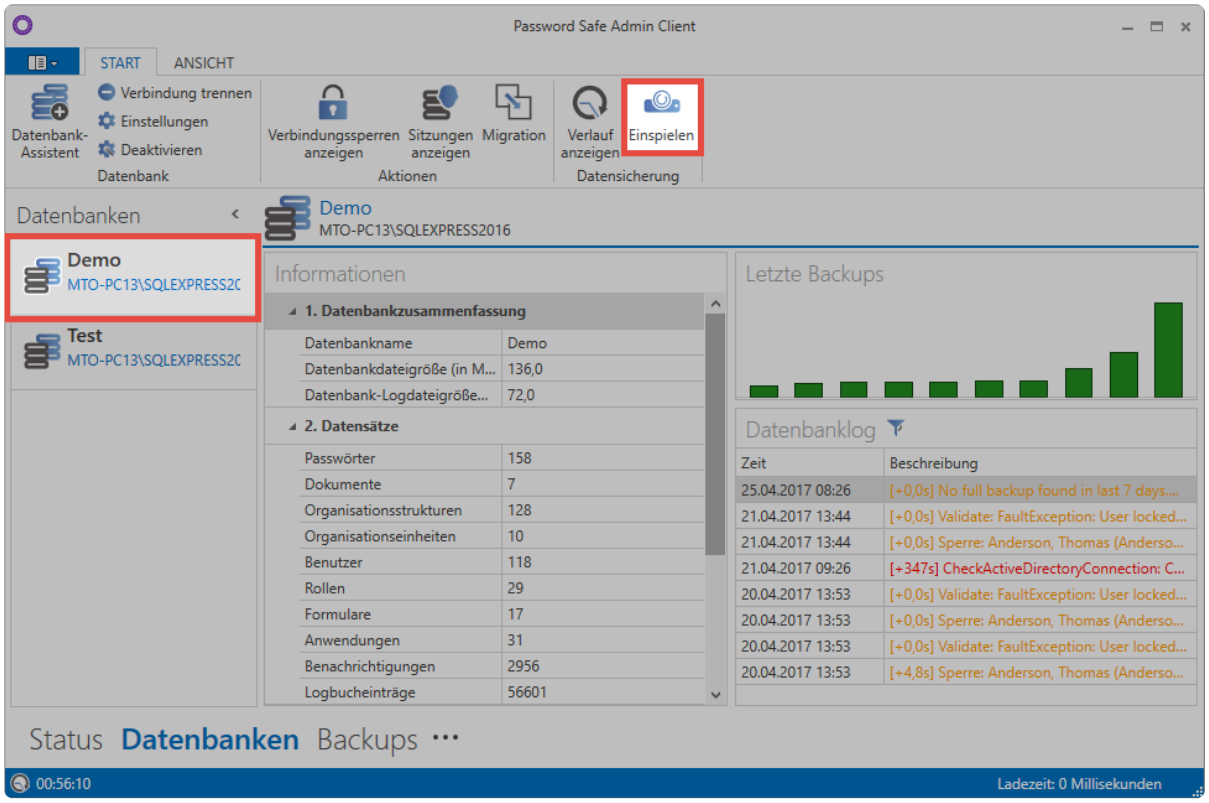
Die Backups werden durch den SQL-Server im Hintergrund ausgeführt. Wenn ein Fehler auftritt, wird dies in der Backupliste “orange” dargestellt. Unter allen Backups werden Informationen zum Fehler angezeigt, sofern der SQL-Server welche ausgibt. Läuft ein Backup 5x in Folge nicht, wird es automatisch deaktiviert. Dies wird in der Liste “rot” dargestellt. Den Zeitplan können Sie nicht direkt reaktivieren. Öffnen Sie ihn und passen Sie ihn direkt an.

Weitere Backup Aktionen

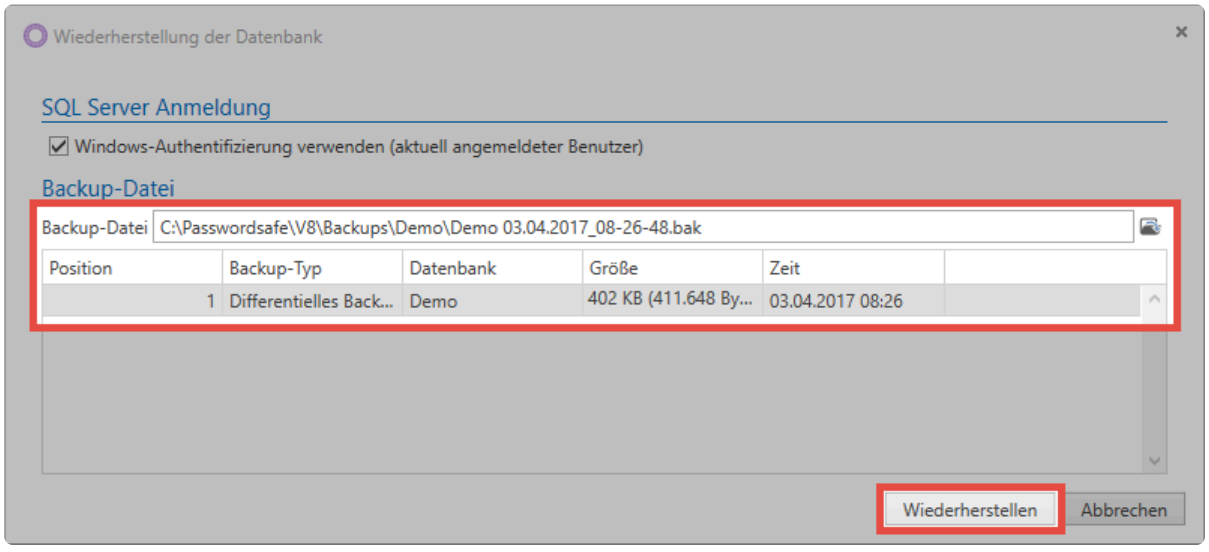
Über die Ribbon haben Sie die Möglichkeit einen selektierten Zeitplan zu löschen. Über einen Doppelklick rufen Sie den Assistenten eines Zeitplans auf, um diesen zu ändern. Das Backup können Sie auch über die Ribbon starten. Hierfür muss der Backupdienst laufen. Sie können das im Verlauf einsehen.

Backup rücksichern

Das Rücksichern von Backups geschieht im Modul Datenbanken. Sie können nur in bestehende Datenbanken sichern. Zunächst wählen Sie die gewünschte Datenbank aus. Daraufhin klicken Sie in der Ribbon auf **Einspielen**.

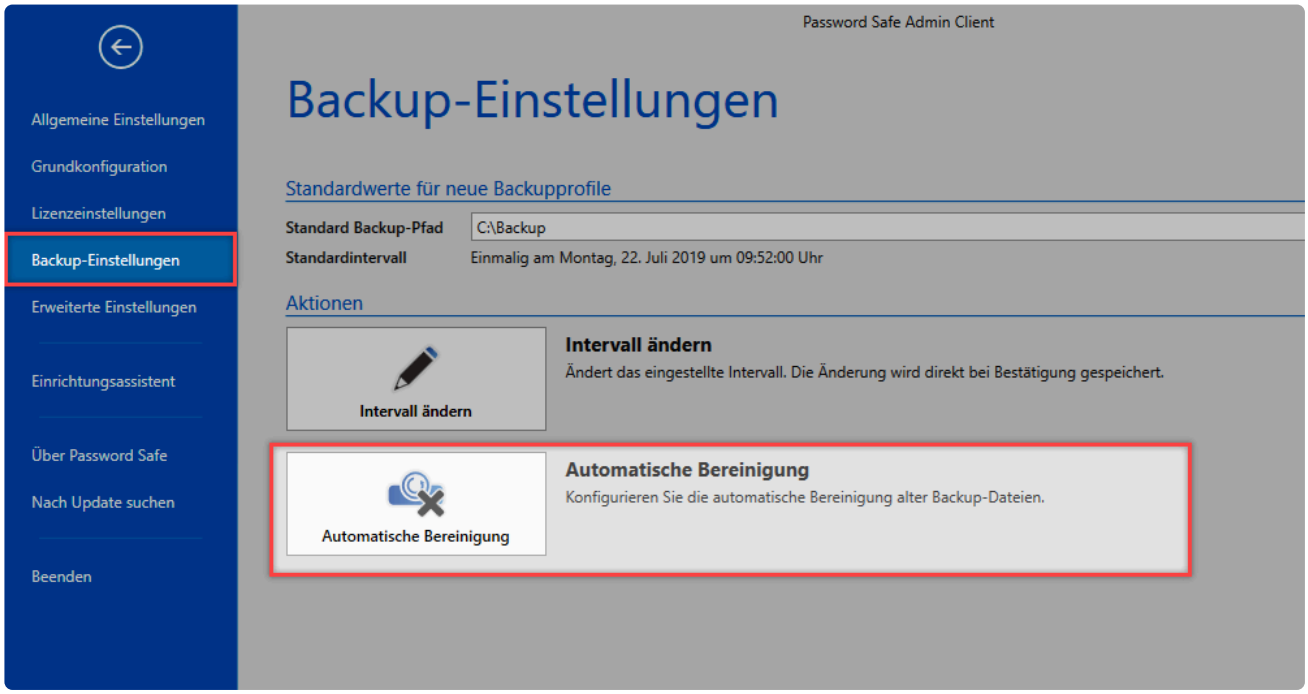


Geben Sie, flls nötig, zunächst den Benutzer an, welcher sich am SQL-Server anmeldet. Wählen Sie nun die Backup-Datei aus. Anschließend werden alle in der Datei enthaltenen Backups dargestellt. Es genügt nun ein Klick auf **Wiederherstellen**, um das Backup in die bestehende Datenbank zurückzuspielen.



Automatisiertes Löschen von Backups

Sie haben die Möglichkeit, Backups nach einem bestimmten Zeitraum automatisiert löschen zu lassen. Es empfiehlt sich, dass Sie an die Backups Datum und Uhrzeit anhängen und somit täglich neue Files generieren.

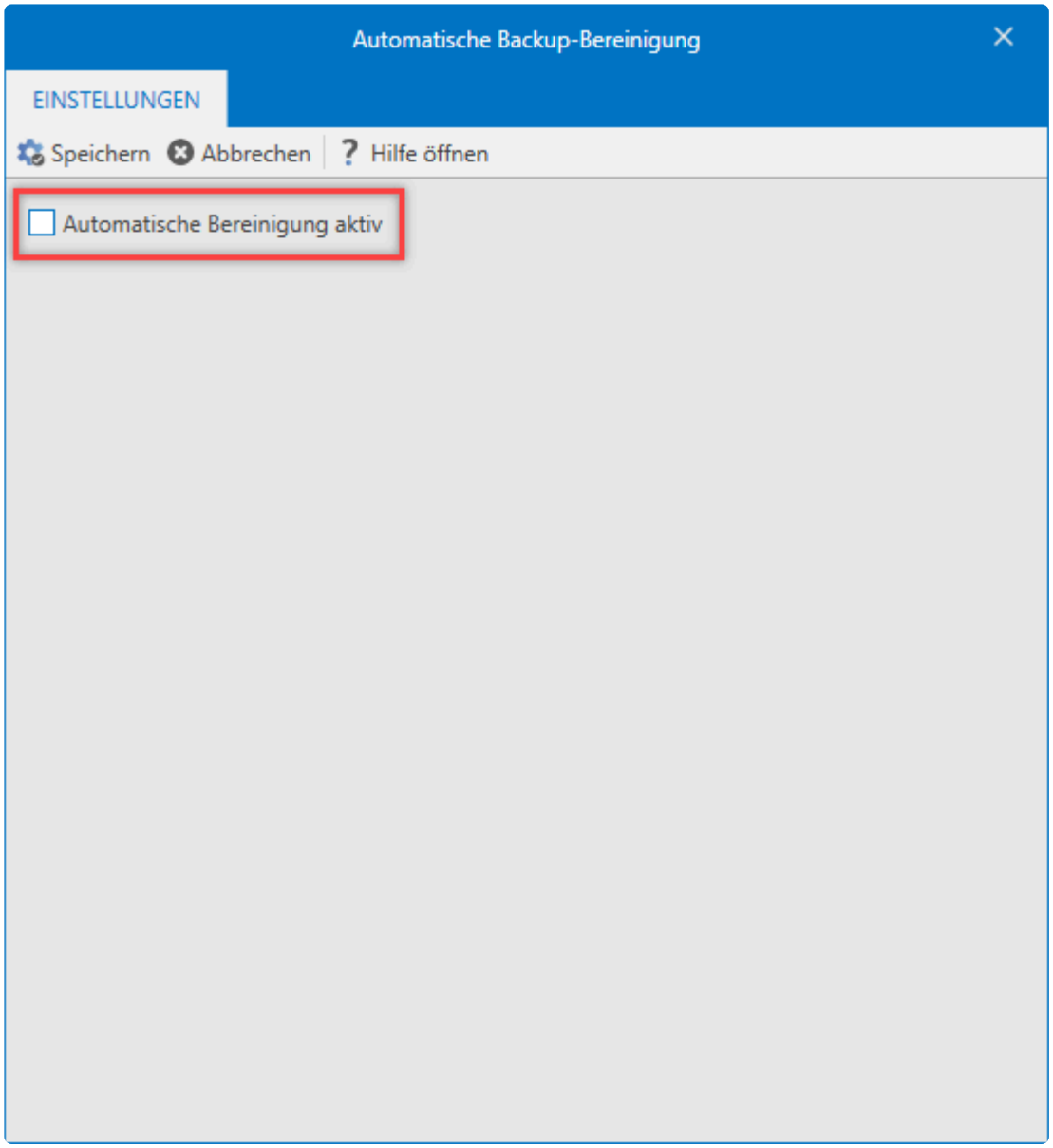


Voraussetzung

Achten Sie darauf, dass der Benutzer, welcher die automatisierte Löschung einrichtet, **sysadmin-Rechte** am SQL-Server hat.

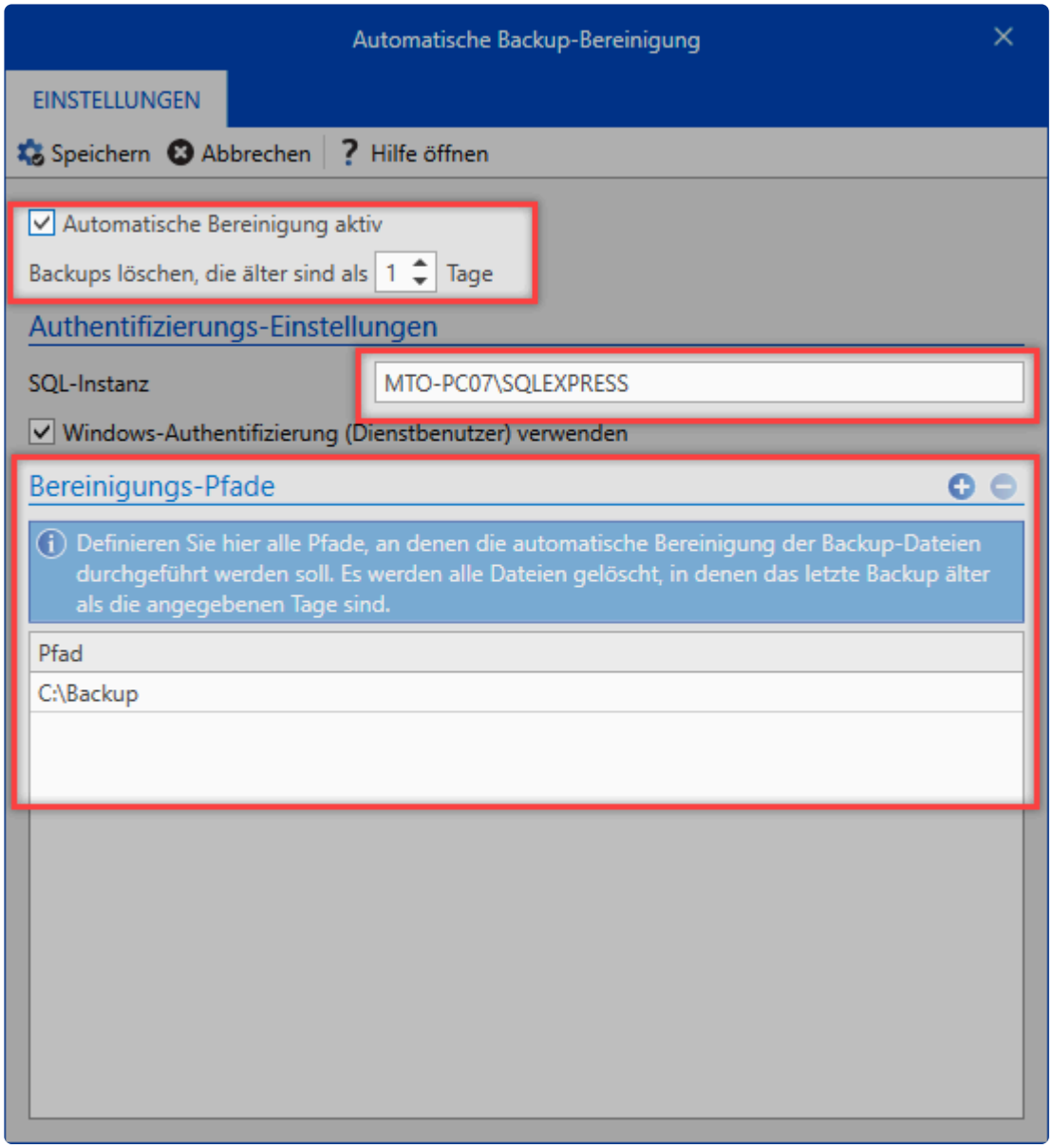
Einrichtung

Um die automatische Bereinigung nutzen zu können, müssen Sie diese zu allererst aktivieren.



Damit die automatische Löschung nun funktionsgemäß läuft, müssen Sie folgendes definieren:

- das Alter der zu löschenden Backups
- die SQL-Instanz
- alle Pfade, an denn die automatische Bereinigung der Backup-Dateien durchgeführt werden soll


Automatische Backup-Bereinigung
EINSTELLUNGEN
Speichern
Abbrechen
Hilfe öffnen
Automatische Bereinigung aktiv
Backups löschen, die älter sind als 1 Tage
Authentifizierungs-Einstellungen
SQL-Instanz
MTO-PC07\SQLEXPRESS
Windows-Authentifizierung (Dienstbenutzer) verwenden
Bereinigungs-Pfade
Definieren Sie hier alle Pfade, an denen die automatische Bereinigung der Backup-Dateien durchgeführt werden soll. Es werden alle Dateien gelöscht, in denen das letzte Backup älter als die angegebenen Tage sind.
Pfad
C:\Backup

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, müssen Sie so schnell wie möglich wieder Zugriff auf die Passwörter haben. Dieses Kapitel soll Ihnen 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. Berücksichtigen Sie dabei folgende Punkte:

Erzeugen von Backups

Essentiell ist natürlich im Desasterfall auf ein möglichst aktuelles Backup zugreifen zu können. Erzeugen Sie daher regelmäßig Backups.

Sichern der Zertifikate

Wichtig ist auch, dass Sie die Zertifikate sichern. Zu nennen sind hier vor allem das Datenbank Zertifikat als auch das Zertifikat für den Masterkey. Ohne diese kann die Datenbank nicht mehr fehlerfrei verwendet bzw. wiederhergestellt werden. Das Verbindungszertifikat muss nicht unbedingt gesichert werden. Sie können es jederzeit wieder erzeugen. Gerade im Desasterfall ist es hilfreich, wenn Sie auf eine Sicherung zurückgreifen können. Weitere Infos zu diesem Thema finden Sie im Kapitel Zertifikate.

Wer ist im Desasterfall zuständig?

Betrachten Sie zunächst wer im Desasterfall eingreifen kann. Legen Sie daher auch entsprechende Stellvertreter fest. 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?

- das Domänenkennwort, um sich an den einzelnen Rechner anmelden zu können
- das Passwort für den Admin Client
- die Zugangsdaten des Dienstbenutzers
- die Zugangsdaten des SQL Nutzers
- das Passwort zur Anmeldung an Password Safe

Stellen Sie sicher, 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

*Zyklisches Erstellen einer Notfall-WebViewer Datei

Desaster Szenarien

Folgend sollen verschieden Desaster Szenarien inklusive möglicher Recovery Möglichkeiten beleuchtet werden.

Szenario 1

Problem:
Datenbank korrupt.

Lösung:
Stellen Sie die Datenbank aus einem Backup wieder her.

Szenario 2

Problem:
Datenbank-Server defekt.

Lösung:
Installieren Sie den Datenbank Server auf einer neuen Hardware. Ändert sich dadurch der Servername, müssen Sie die Lizenz neu aktivieren. Haben Sie die Lizenz bereits mehrfach aktiviert, kann es sein, dass diese durch die MATESO wieder freigegeben werden muss. Ändert sich der SQL Instanz Name, müssen Sie am Anwendungsserver die Verbindung zum Datenbankserver neu konfigurieren. Dies gelingt über die Grundkonfiguration.
Eventuell vorhandene Offline Datenbanken funktionieren weiterhin.

Szenario 3

Problem:
Applikationsserver defekt.

Lösung:
Führen Sie eine Neuinstallation auf einer neuen Hardware aus. Aktivieren Sie die Lizenz neu. Ändert sich der Servername kann es sein, dass die Lizenz durch die MATESO wieder freigegeben werden muss. Die Grundkonfiguration muss von Ihnen durchgeführt werden, um die Anbindung an den Datenbankserver wiederherzustellen. Ändert sich der Servername, müssen Sie die Datenbankprofile an den Clients anpassen.
Eventuell vorhandene Offline Datenbanken müssen neu erstellt werden!

Szenario 4

Problem:
Beide Server defekt, Passwörter aus dem Password Safe werden aber dringend benötigt.

Lösung:
Installieren Sie den Datenbank Server und den Anwendungsserver wird auf einer neuen Hardware. Sie müssen die Lizenz neu aktivieren. Spielen Sie ein Backup in eine leere Datenbank ein. Die Grundkonfiguration muss von Ihnen erneut durchgeführt werden, um die Anbindung an den Datenbankserver wiederherzustellen. Haben Sie 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

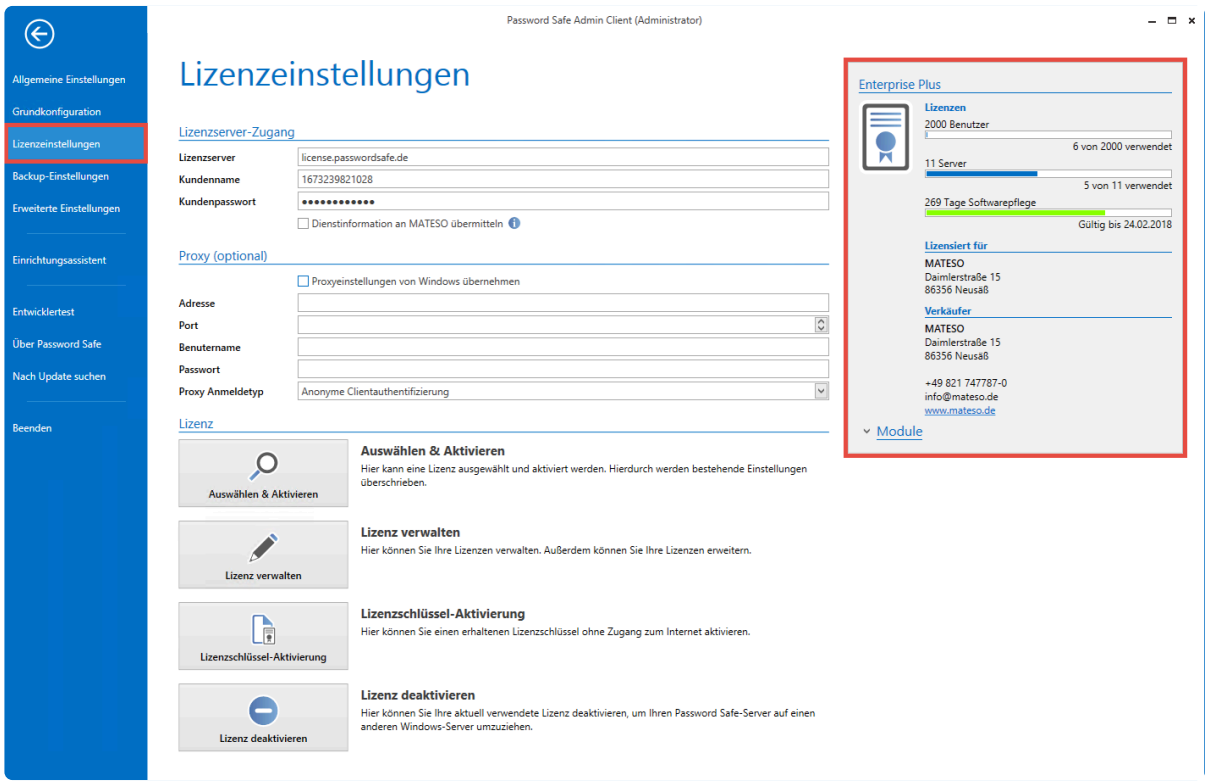
Problem:
Wie Szenario 4, aber zusätzlich ist auch Active Directory nicht verfügbar.

Lösung:
Gehen Sie wie beim Szenario 4 vor. Haben Sie die User im Ende zu Ende Modus importiert, können sie sich auch ohne AD Anbindung anmelden. User, welche im Masterkey Modus importiert wurden, können sich nicht anmelden. Erstellen Sie daher spezielle, lokale Notfall User für solche Fälle.

Lizenzeinstellungen

Was sind Lizenzeinstellungen?

Innerhalb der Lizenzeinstellungen verwalten Sie die Lizenzen für den Password Safe. 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 bezüglich der Ausstellung einer Version 8 Lizenz.

Angebunden werden die Lizenzinformationen über den MATESO Lizenzserver. Nachfolgend die Details:

- license.passwordsafe.de
- IP: 13.74.32.103
- Port 443 TCP (Standard HTTPS-Port)

Sie müssen dafür Sorge tragen, dass dieser Server erreichbar ist. Optional können Sie Proxy Server verwenden. 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, können Sie demnach noch 30 Tage weiterarbeiten. 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 konfigurieren Sie direkt im Bereich **Lizenzserver-Zugang**. 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.

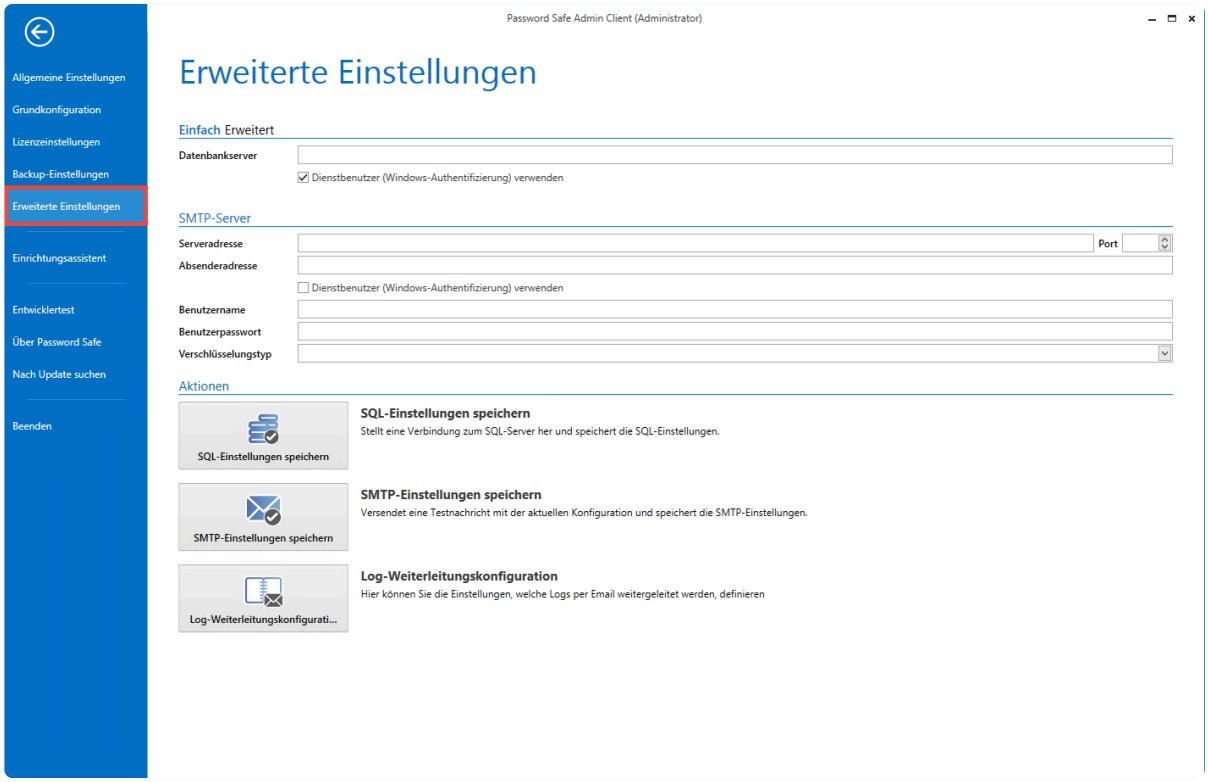
✻ Optional können Sie Proxy angeben. Standardmäßig wird der im Betriebssystem hinterlegte Proxy verwendet.

! 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 definieren Sie globale Standardwerte.



Datenbankserver

Der hier hinterlegte Datenbankserver wird beim Neuerstellen von Datenbanken als Standardwert verwendet. Hierbei existieren 2 Modi:

Einfacher Modus

Im einfachen Modus geben Sie den Pfad zum Datenbankserver inklusive dem Benutzer und dem zugehörigen Passwort an. Alternativ können Sie ebenso den Dienstbenutzer verwenden.

Erweiterter Modus

Im erweiterten Modus geben Sie den Connection String an, welcher sowohl den Server, den User als auch das Passwort enthält.

SMTP-Server

Durch die Konfiguration des SMTP-Servers definieren Sie 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.

Hochverfügbarkeit

Was ist Hochverfügbarkeit?

Durch Hochverfügbarkeit soll der weitere Betrieb des Password Safe im Schadensfall gewährleistet werden. Damit dieses Feature genutzt werden kann, müssen Sie **im Vorfeld** eine Reihe von Voraussetzungen erfüllen.

> ! 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

Beachten Sie bei der Konfiguration folgende Punkte:

- Für die Replikation der Datenbank müssen Sie zwingend die MSSQL Enterprise Version nutzen (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, können Sie vor die Applikationsserver einen Load Balancer schalten.
- Verwenden Sie keinen Load Balancer, erfolgt die Verteilung des Datenbankprofils bei den Benutzern generell über die Registry.

Wurde die Datenbank in “Standort A” inkl. AD-Profil erstellt, so müssen Sie diese Zertifikate dort exportieren und auf dem Server Standort B importieren. Replizieren Sie die Datenbank mittels MSSQL Technologie und binden Sie sie als bestehende Datenbank im Password Safe am Standort B ein. Fällt der Applikationsserver in Standort A aus, tauschen Sie den Server in der Registry ausgetauscht (Standort B) und rollen ihn an die Benutzer mittels Gruppenrichtlinien (GPO) neu aus.

> ✻ Es wurde ausschließlich die **Peer-to-Peer Transaktionsreplikation** getestet. Möchten Sie eine andere Art der Replikation verwenden, so sollten Sie dies vorab testen.

LoadBalancerModus

Was bewirkt der LoadBalancerModus?

Wenn Sie mehrere Password Safe Server verwenden möchten, müssen Sie einen dedizierten Load

Balancer einsetzen, der die RPC-Aufrufe von den Clients an eine Reihe von Password Safe Application Servern weiterleitet. Um korrekt zu arbeiten, muss der Load Balancer die .NET WCF TCP-Verbindungen im Auge behalten, was nicht jeder Load Balancer unterstützte oder in einigen Fällen zu einer hohen CPU-Last auf den WCF-Clients führte, weil der Load Balancer z.B. das TCP Close Flag manipulierte.

Für diesen Fall haben wir nun den LoadBalancerModus. Mit dieser Einstellung teilen wir allen WCF-basierten Clients mit, dass sie auf Basis einer Sitzung pro Aufruf arbeiten. Bei jedem RPC-Aufruf legt der WCF-Client also eine neue TCP-Verbindung an, ruft die RPC-Funktion auf und schließt die Verbindung direkt danach. Der LoadBalancer muss also nicht den Überblick über die Client-Verbindungen behalten.

Vor- und Nachteile von aktiviertem LoadBalancerMode?

+ Der Load Balancer muss die TCP-Verbindungen nicht im Auge behalten.

+ WCF-basierte Clients fallen nicht in hohe CPU-Last

- WCF basierte Clients sind langsamer, da bei jedem RPC-Aufruf neue Verbindungen aufgebaut werden

- Mehr Last für den Load Balancer und den Application Server, aufgrund neuer Verbindungen (SSL Handshake, etc) für jeden RPC-Aufruf

Um den LoadBalancerModus zu aktivieren oder zu deaktivieren, müssen Sie die folgende Reg-Datei auf allen Password Safe Application Servern ausführen:

Aktivieren – LoadBalancerModus
Deaktiveren – LoadBalancerModus

Supportkontext: Bei der Verwendung der Hochverfügbarkeit oder beispielweise Datenbank-Clustering ist zusätzliches technisches Wissen notwendig. Zudem betrifft die Konfiguration und Einrichtung nicht direkt Password Safe, sondern dies wird extern, bspw. auf dem MS SQL Server, durchgeführt werden. Aus diesem Grund können wir hierzu keinen direkten Support gewährleisten. Weiterführend erfolgt die Verwendung eines Clusters oder beispielsweise eines Loadbalancers auf eigene Verantwortung. Wir empfehlen hier die Verwendung unserer Solution Architects. Gerne erstellen wir dir ein individuelles Consulting-Angebot. Oder Du nutzt eines unserer Consulting-Pakete, die praktisch nach Stunden abgerechnet werden. Wende dich hierzu einfach an unser Vertriebsteam.

Offline Client

Was ist der Offline Client?

Der Offline Client ermöglicht das Arbeiten ohne aktive Verbindung zum Password Safe Server. Sollten Sie es an entsprechender Stelle konfiguriert haben, synchronisiert sich die lokale Replikation der Serverdatenbank in frei definierbaren Zyklen selbstständig. Damit wird sichergestellt, dass die Stände nahezu aktuell sind.
h4. 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.
- Hier erfahren Sie mehr zu diesem Thema.

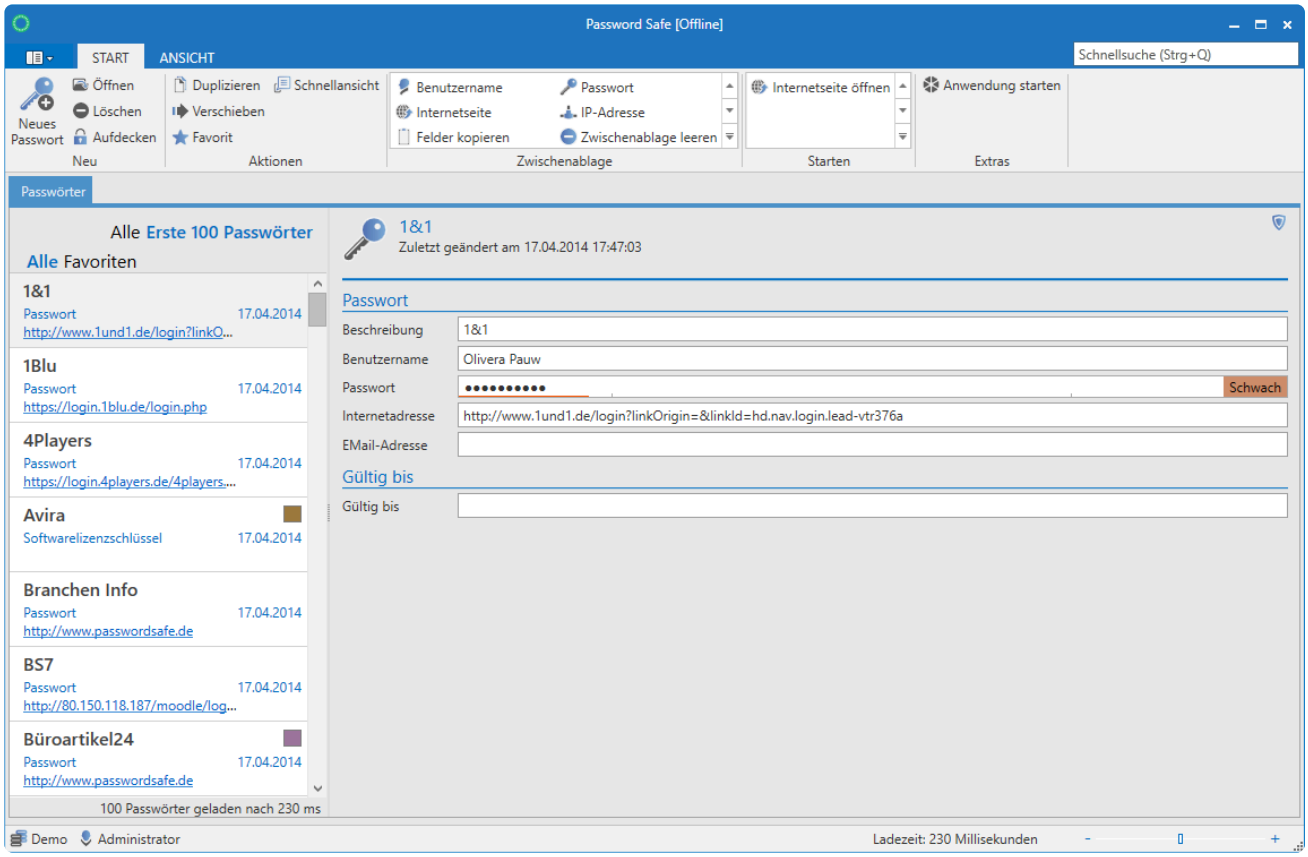
Installation

Der Offline Client wird automatisch zusammen mit dem Haupt Client installiert. Sie müssen keine Datenbankprofile erstellten. Diese Aufgabe übernimmt der Client bei der ersten Synchronisation zusammen mit der Erstellung 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.



Welche Daten werden synchronisiert?

Siegel erweitern das Sicherheitskonzept des Password Safe um ein 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 nicht einholbar, wenn keine Server-Verbindung besteht. Aus diesem Grund werden versiegelte Datensätze nicht synchronisiert und sind demnach auch nicht Bestandteil der Offline Datenbanken.

Ansonsten werden alle Datensätze synchronisiert, auf welche der Benutzer das **Export Recht** hat.

Datensätze mit **Sichtschutz** werden in die Offline Datenbank übernommen und Sie können diese wie gewohnt verwenden.

Einrichten und Synchronisieren

Einrichten der Offline Datenbank

Für die Einrichtung des Offline Clients gilt es im Vorfeld die richtigen Voraussetzungen zu schaffen. Führen Sie sowohl am Admin Client selbst als auch in den Benutzerrechten / Benutzereinstellungen die nachfolgend aufgeführten Konfigurationen durch.

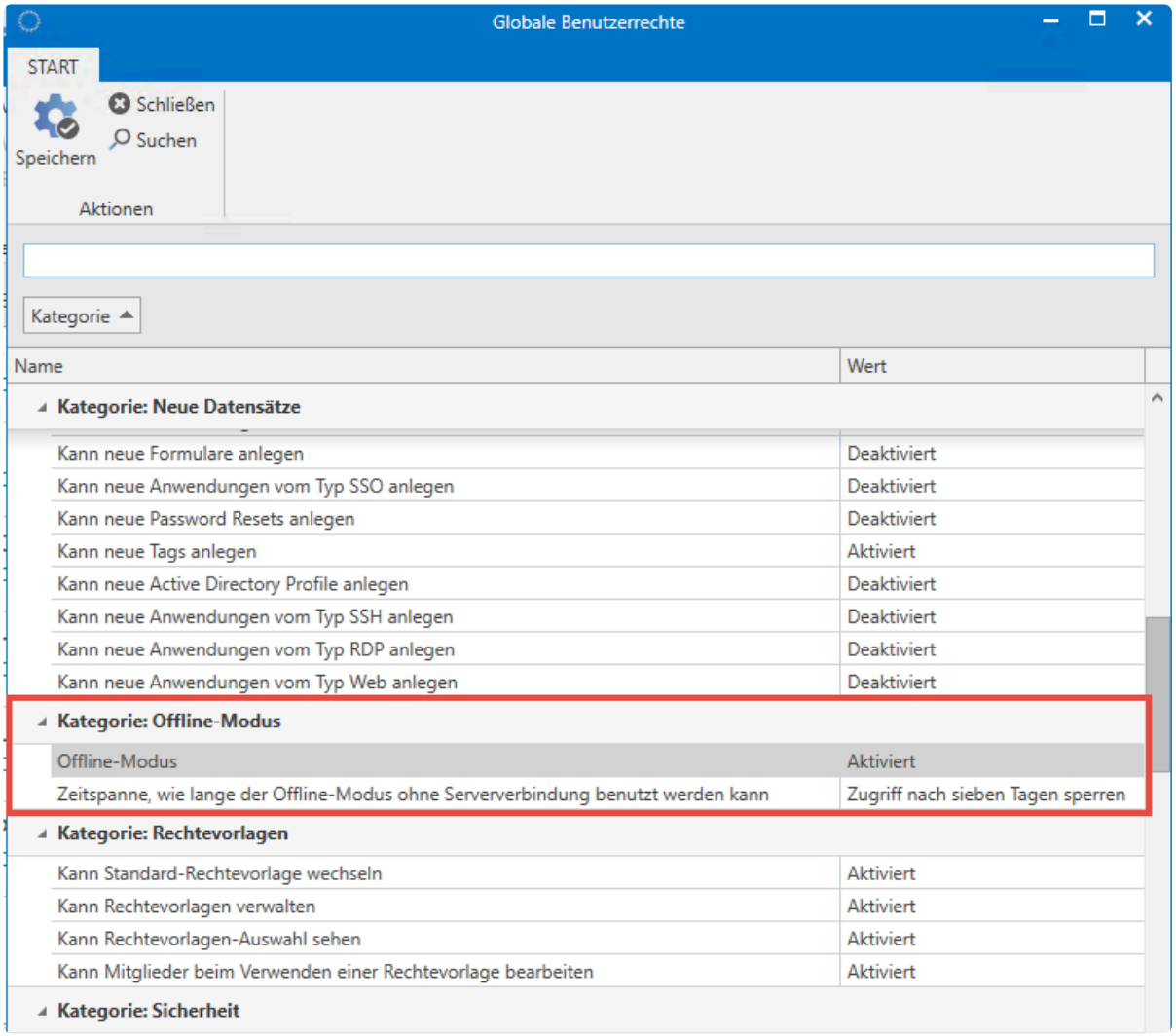
Voraussetzungen

Um Offline Datenbanken einrichten zu können, müssen Sie die Funktion am Admin Client aktivieren. Dies wird in der Datenbankübersicht am Admin Client für jede Datenbank separat in den “Allgemeinen Einstellungen” (Rechtsklick auf die Datenbank) durchgeführt. Ebenso können Sie die Option bereits beim initialen Erstellen der Datenbank auswählen.

Weitere Infos zu diesem Thema finden Sie in den Kapiteln Erstellen von Datenbanken und Verwaltung von Datenbanken.

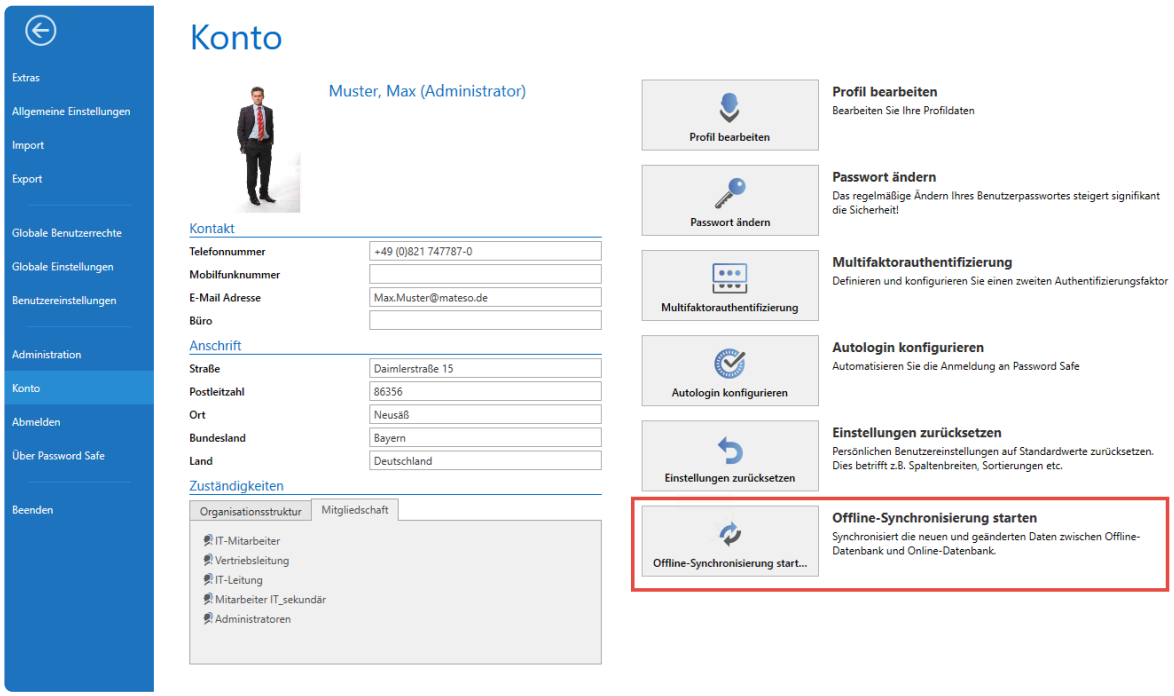
Benutzerrechte

Der Benutzer benötigt das Recht “Offline-Modus”. Zudem können Sie in den Benutzerrechten die Zeitspanne definieren, wie lange der Offline-Modus ohne Serververbindung genutzt werden kann.



Einrichten einer Offline Datenbank

Grundlegend erfolgt die Synchronisation mit der Offline Datenbank automatisch. Dennoch müssen Sie **das erste Mal** manuell anstoßen. Initiieren Sie hierzu unter Hauptmenü / Konto die Synchronisation.



> Gespeichert werden die Offline Datenbanken lokal unter folgendem Pfad: %appdata%\MATESO\Password Safe and Repository Client\OfflineDB

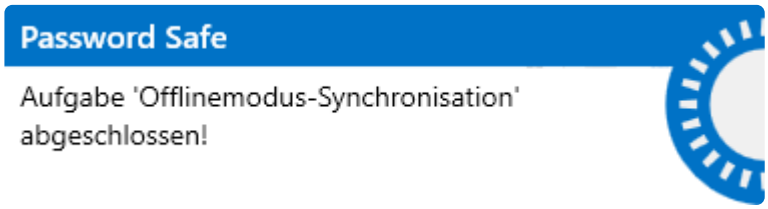
Sie müssen pro Benutzer und Client für jede Online Datenbank eine Offline Datenbank erstellen. Somit ist es möglich, mit einem Offline Client mehrere Offline Datenbanken zu verwenden.

Synchronisation

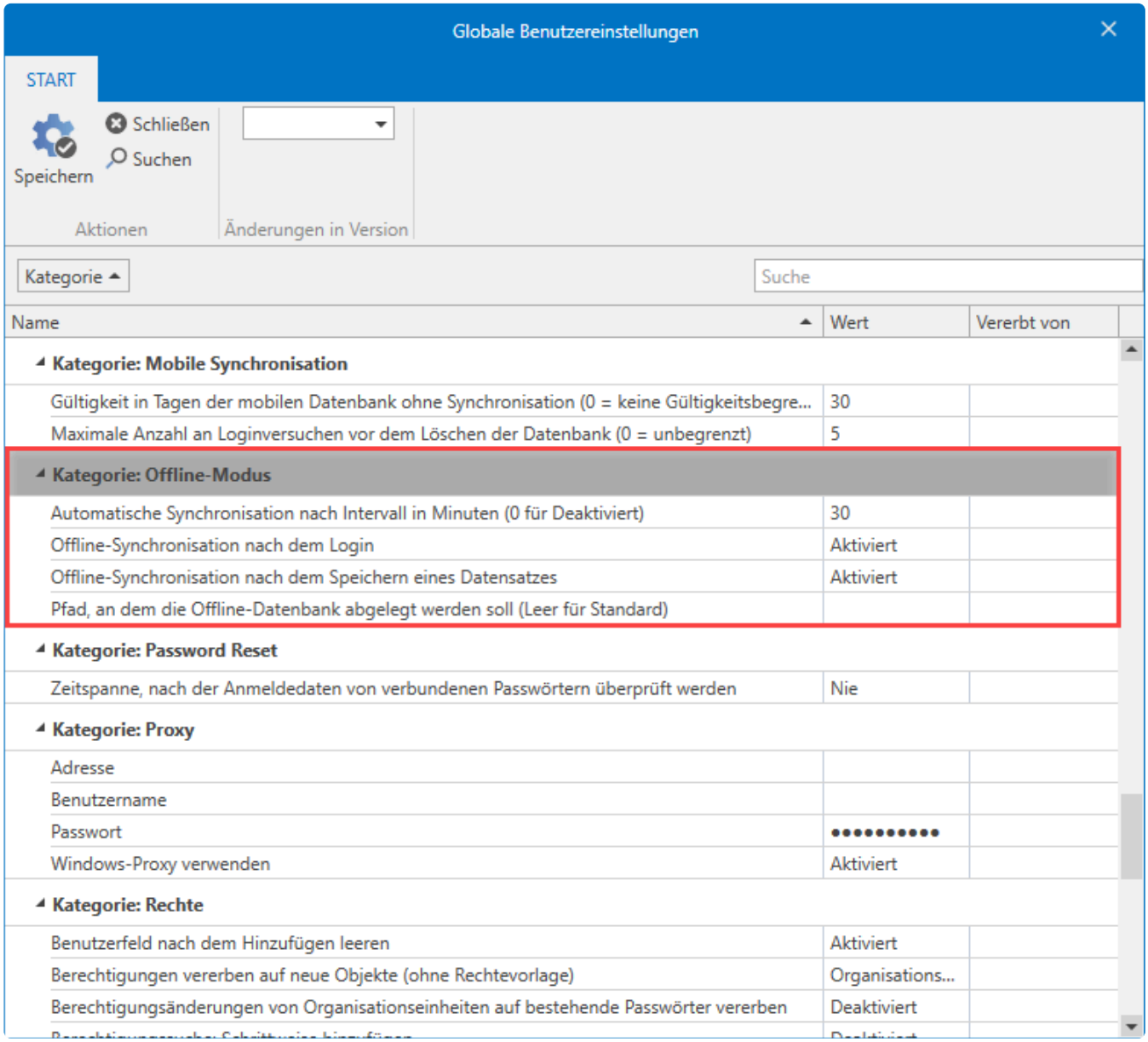
Um die Daten immer konsistent zu halten, müssen Sie die Offline Datenbank regelmäßig synchronisieren. Die Synchronisation wird durch den Client automatisch im Hintergrund ausgeführt. Konfigurieren Sie das Intervall hierfür in den Einstellungen. Standardmäßig wird alle 30 Minuten synchronisiert. Beim Anlegen und Bearbeiten von Datensätzen, sowie beim Starten des FullClient kann auch azyklisch synchronisiert werden, damit die Änderungen direkt offline verfügbar sind. Starten Sie darüber hinaus im Backstage über “Konto” die Synchronisation manuell.

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 können Sie den Offline Modus konfigurieren und personalisieren:

- **Offline Synchronisation nach dem Speichern eines Datensatzes**: Die Synchronisation der Offline Datenbank erfolgt direkt nach dem Speichern eines Datensatzes. Beachten Sie bitte, dass dies nur diejenigen Datensätze betrifft, welche vom angemeldeten Benutzer gespeichert werden. Änderungen anderer Benutzer lösen **keine** Synchronisation aus!
- **Offline-Synchronisation nach dem Login**: Wenn diese Option aktiv ist, erfolgt die Synchronisation der Offline Datenbank nach jedem Neustart des Clients.
- **Automatische Synchronisation nach Intervall**: Definieren Sie das Intervall, das zyklisch zu einer Synchronisation der Offline Datenbank führt. Der Standard beträgt 30 Minuten.
- **Pfad, an dem die Offline Datenbank abgelegt werden soll**: Lassen Sie dieses Feld leer, wird der Systemstandard genutzt. Anderweitig können Sie auch direkt den Ablageort der Offline Datenbank angeben.

How-to

Um die Bedienung von Password Safe zu erleichtern, werden hier How-to’s zu häufig angefragten Themen zur Verfügung gestellt. Sie schildern Lösungen zu bestimmten Aufgaben und Anforderungen. Die How-to’s richten sich hauptsächlich an die Endanwender. Aber auch Administratoren finden hier sicherlich wertvolle Informationen.

Die Sammlung an Anleitungen wird ständig erweitert. Aktuell sind folgende How-to’s verfügbar:

- Wechseln eines SSL Verbindungszertifikats
- WebViewer automatisiert per Mail erhalten
- Felder kopieren
- Rechte auf den Datensatz aber nicht auf das Passwortfeld
- Anzeigen von Passwörtern mit möglicherweise falsch gesetzten Berechtigungen

Wechseln eines SSL Verbindungszertifikats

Anforderung

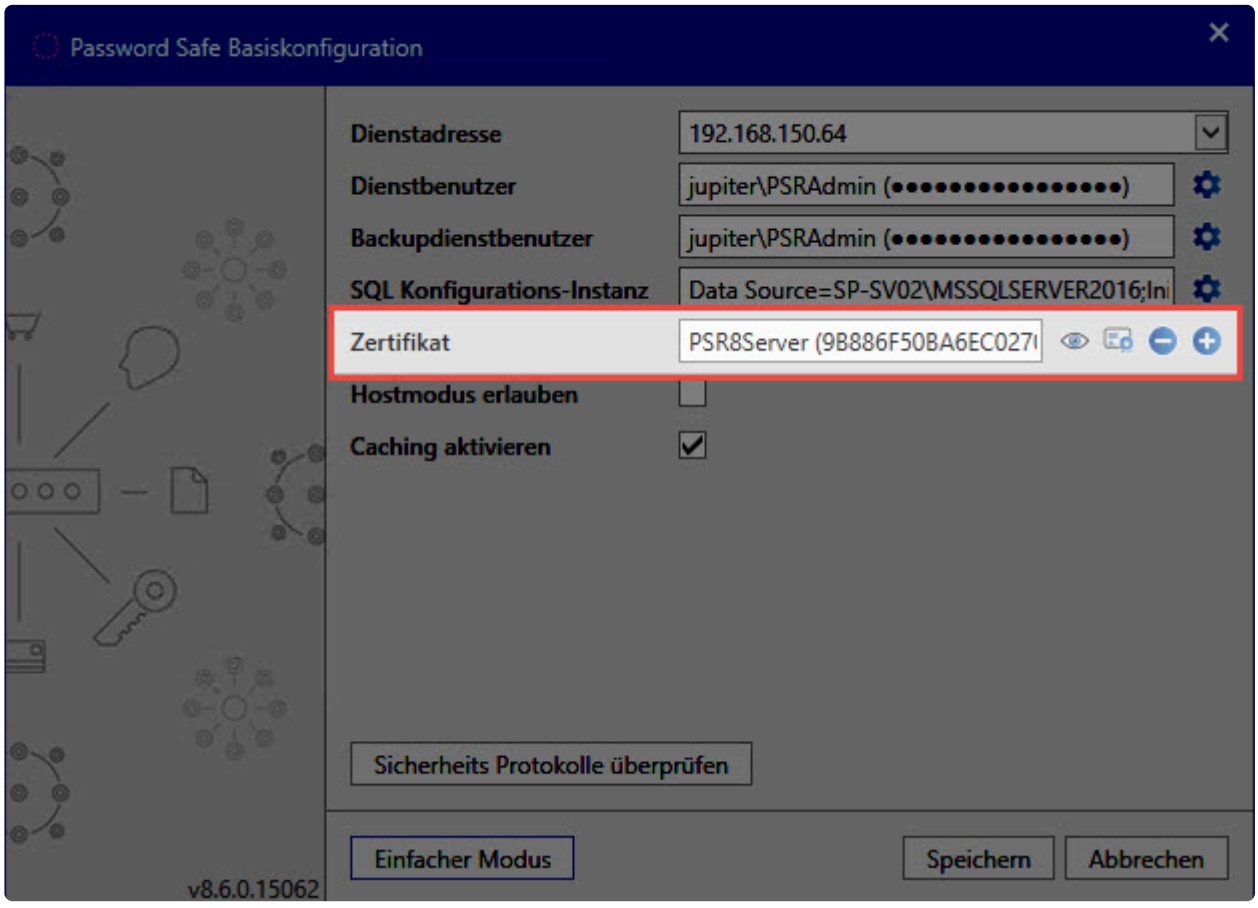
Ein **SSL Verbindungszertifikat** soll gewechselt werden, weil es zum Beispiel abgelaufen ist.

Voraussetzungen

Sie benötigen Zugriff auf **AdminClient**.

Wechsel des Zertifikats

Zunächst erfolgt die Anmeldung am AdminClient. Anschließend öffnen Sie die **Grundkonfiguration**. Über den Button **Ändern** rufen Sie das Konfigurationsmenü auf. Wählen Sie nun den **Expertenmodus** aus. Hier ist das aktuell hinterlegte Zertifikat sichtbar.



Die Buttons neben dem Zertifikat haben (von links nach rechts) folgende Funktionen:

- Informationen zum Zertifikat aufrufen
- bestehendes Zertifikat auswählen
- Zertifikat verwerfen
- neues selbstsigniertes Zertifikat erstellen

Hinweise zu den Zertifikaten

Bestehendes Zertifikat auswählen

Hier werden alle Zertifikate angezeigt, die von Password Safe verwendet werden können. Sie müssen den Anforderungen entsprechen, die unter **SSL Verbindungszertifikate** aufgeführt sind.

Neues selbstsigniertes Zertifikat erstellen

Ist keine CA verfügbar, können Sie auch ein selbstsigniertes Zertifikat verwenden.Beachten Sie, dass dieses nach dem Wechsel an die Clients verteilt werden muss. Nähere Informationen hierzu finden Sie im Kapitel **Zertifikate**.

> In den Versionen 8.0.0 bis 8.2.0 wurden die Zertifikate mit einer Gültigkeit von einem Jahr erzeugt und können somit ablaufen. Bitte aktualisieren Sie die Software auf die neues Version, wenn Sie ein abgelaufenes Zertifikat ersetzen möchten. Das Zertifikat wird dann mit einer Gültigkeit bis zum Jahr 9999 erstellt und ist somit quasi endlos gültig.

WebViewer automatisiert per Mail erhalten

Anforderung

Ein HTML WebViewer soll einmal täglich um 10:00 Uhr erzeugt werden. Sie möchten den WebViewer über Ihr E-Mail Postfach abrufen, damit Sie auch darauf zugreifen können, wenn Sie nicht im Büro sind.

Voraussetzungen

Der HTML WebViewer kann ab der Professional Edition aufwärts erzeugt werden. Richten Sie vorab den SMTP Server im Einrichtungsassistenten oder alternativ im Backstage, bei den Erweiterten Einstellungen ein.

Benötigte Benutzerrechte

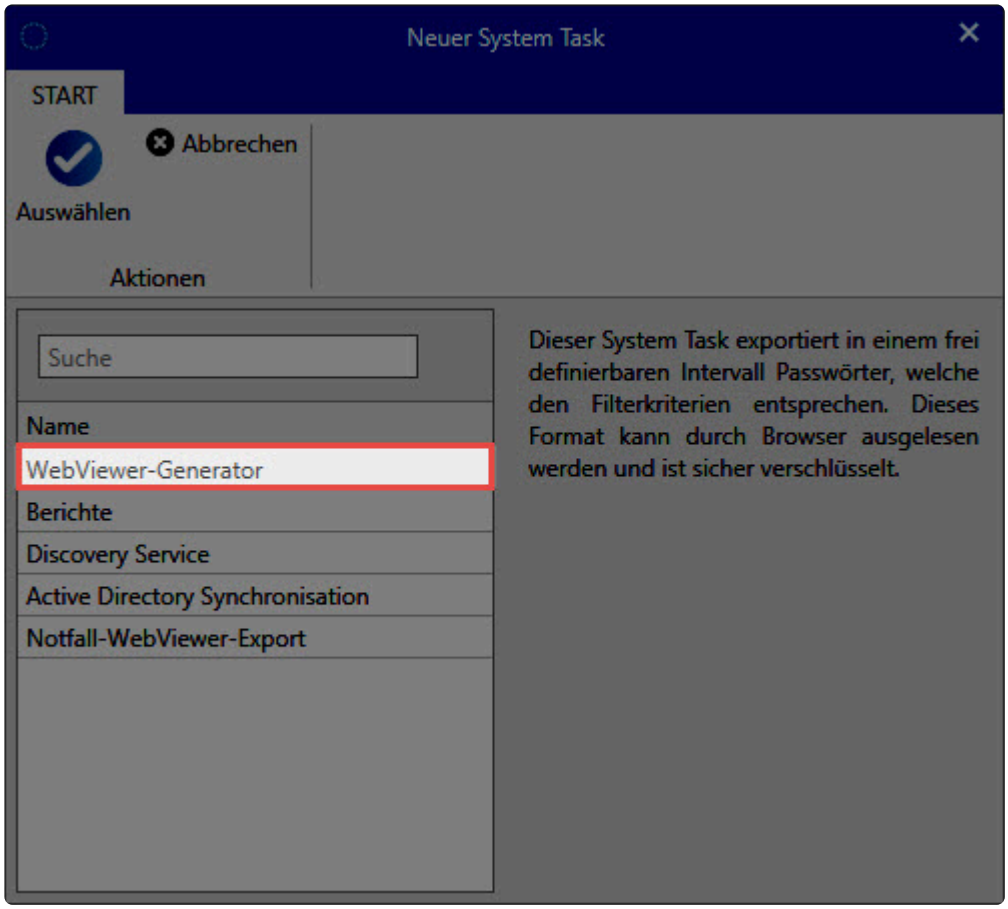
- Kann HTML WebViewer exportieren
- Kann WebViewer Export System Tasks verwalten
- Benachrichtigungsmodul anzeigen

Zudem benötigen Sie **Export Rechte** auf die gewünschten Passwörter.

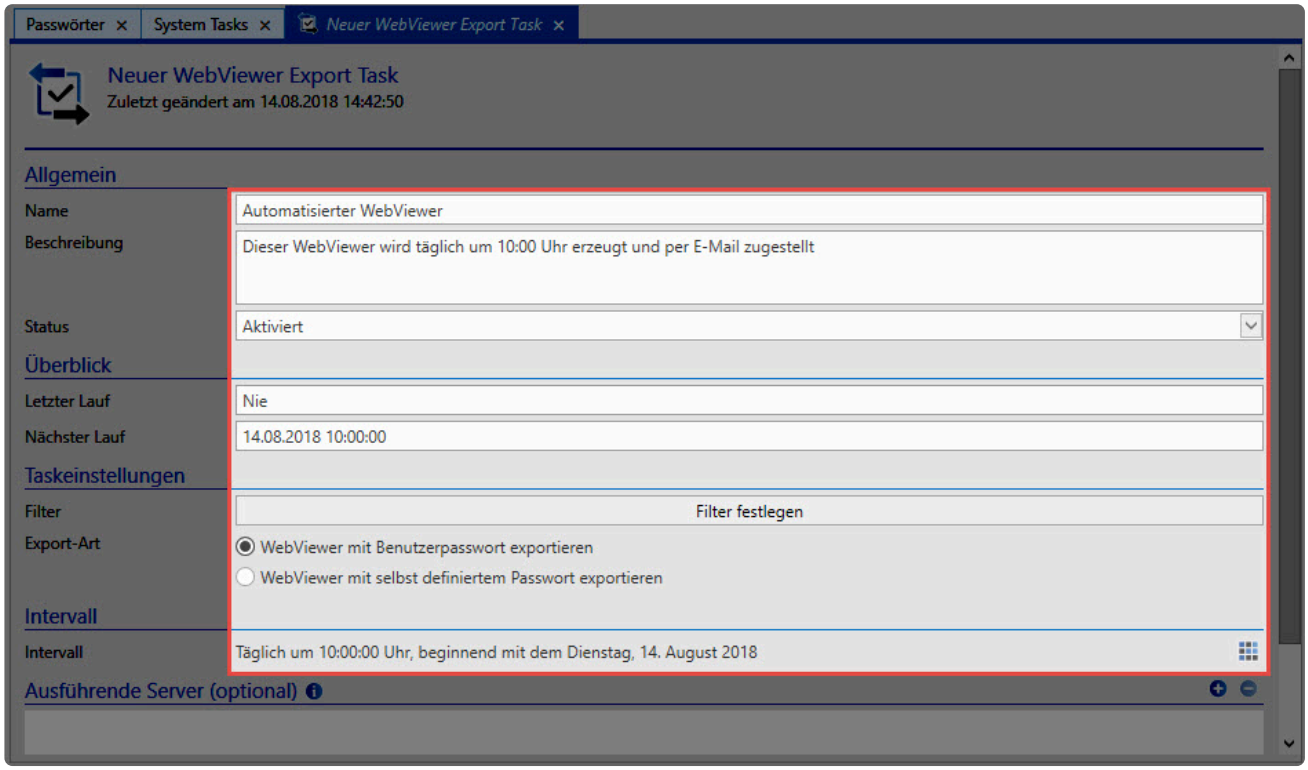
Konfiguration

Task einrichten

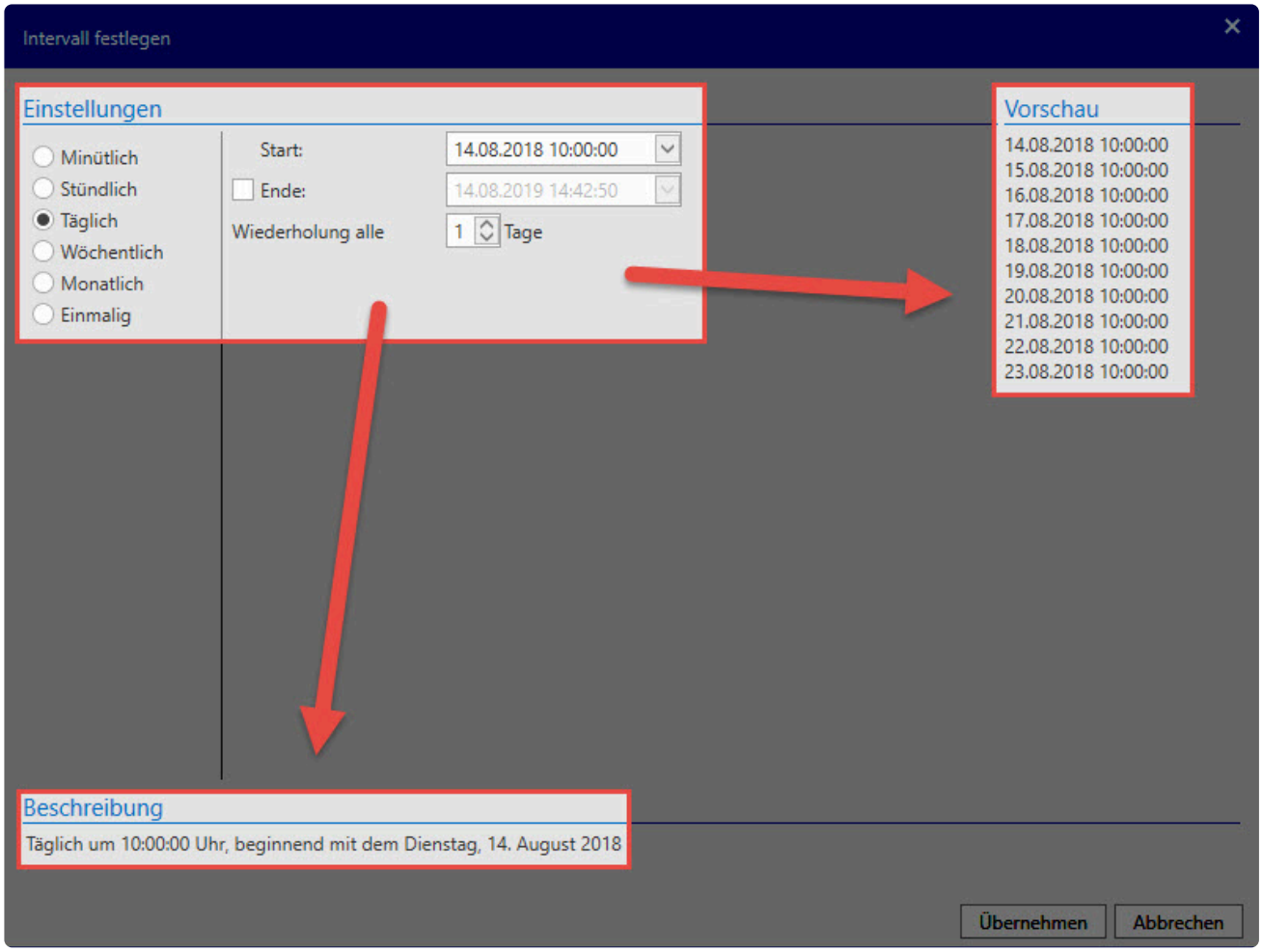
Öffnen Sie zunächst im Hauptmenü (Backstage) die Verwaltung der **System Tasks**. Erstellen Sie dann über den Button **Neu** einen neuen Task. Hier wählen Sie den **WebViewer-Generator** aus:



Konfigurieren Sie den WebViewer wie gewünscht.

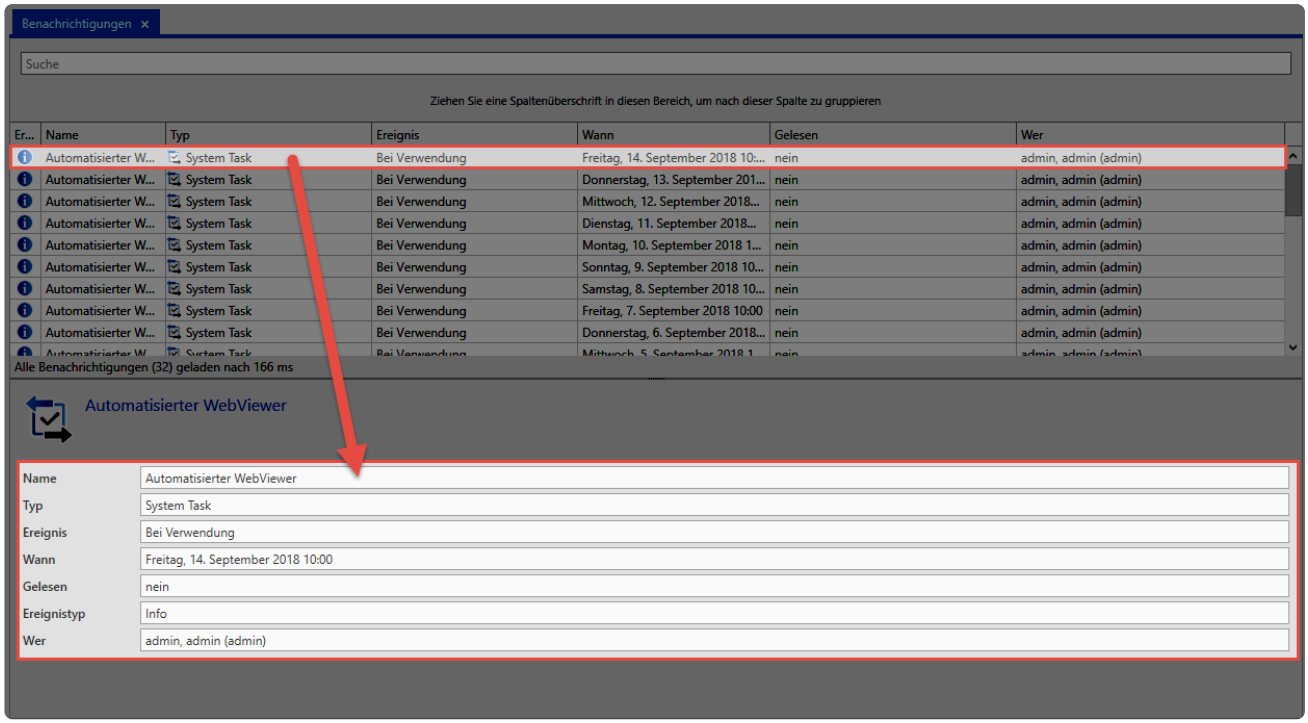


Hierbei wird das Intervall auf 10:00 Uhr täglich gestellt.



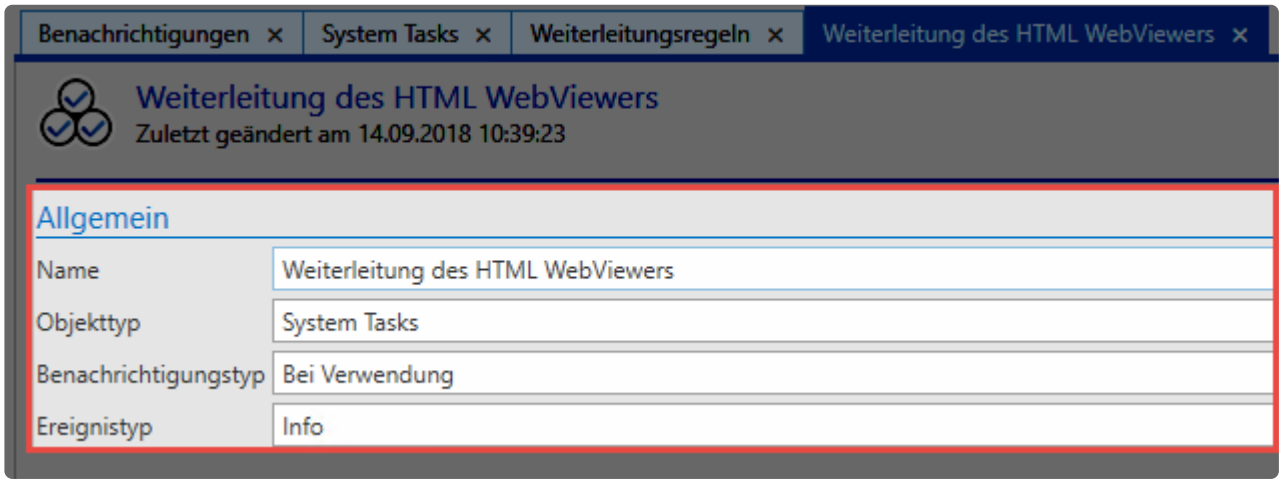
E-Mail Weiterleitung konfigurieren

Nachdem der Task gelaufen ist, wird der erstellte WebViewer im **Benachrichtigungsmodul** zugestellt.



Ebenfalls im Modul **Benachrichtigungen** richten Sie über die die Ribbon die **E-Mail Weiterleitung** ein.

Im nächsten Schritt erzeugen Sie über **Neu** eine neue Weiterleitungsregel. Die nötigen Einstellungen entnehmen Sie dem Screenshot.



Felder kopieren

Anforderung

- Es soll eine Kopie eines Datensatzes erstellt werden, diese soll aber andere Rechte besitzen oder ein anderes Formular nutzen.
- Nach einer erfolgreichen Migration sollen noch einzelne Datensätze von der Version 7 in die Version 8 übertragen werden.
- Einzelne Datensätze sollen von einer Datenbank in eine andere übernommen werden.

Voraussetzungen

Es wird ein bereits vollständiger Datensatz benötigt.

Benötigte Benutzerrechte

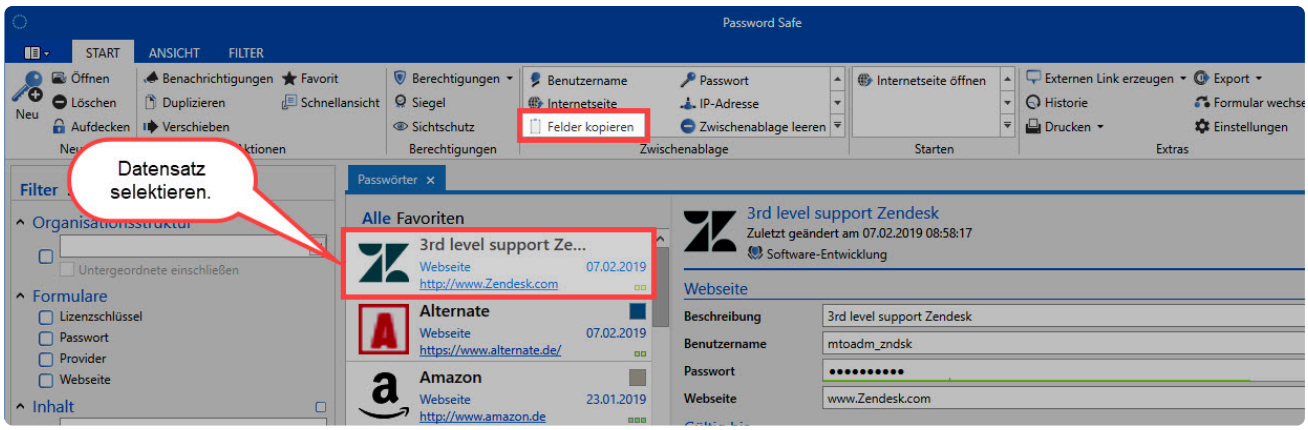
- Kann neue Passwörter anlegen
- Leserechte auf den Datensatz

Konfiguration

Vorgehensweise in der Version 8

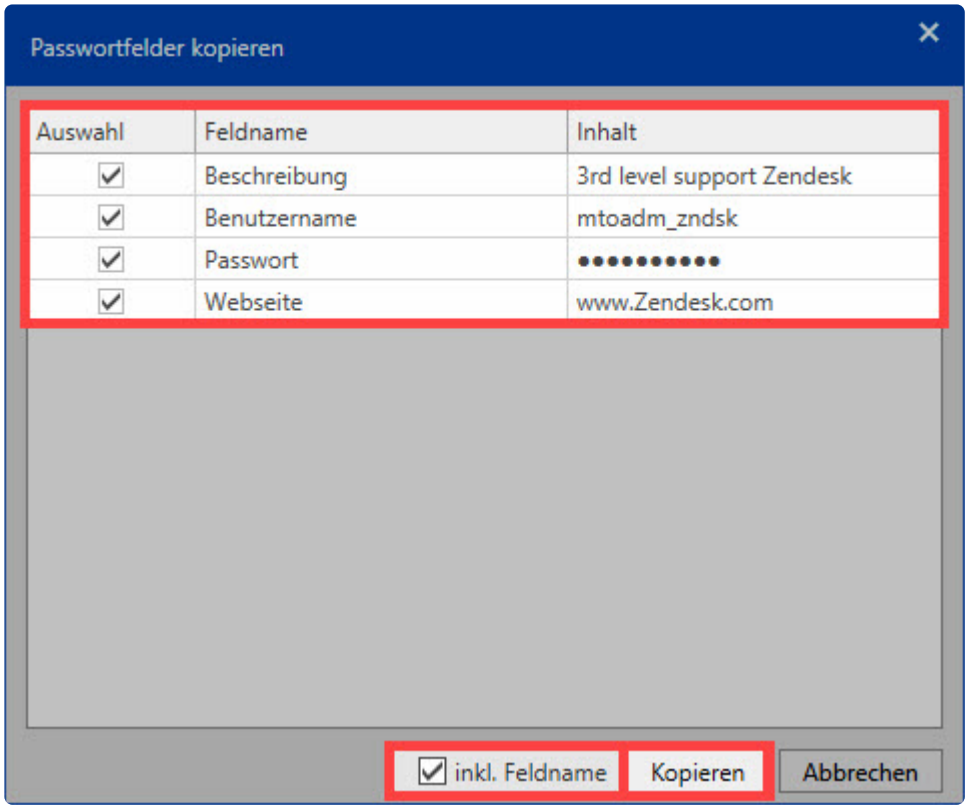
Selektieren Sie den gewünschten Datensatz, welchen Sie kopiert möchten.

Wählen Sie dann in der Ribbon **Felder kopieren** aus.

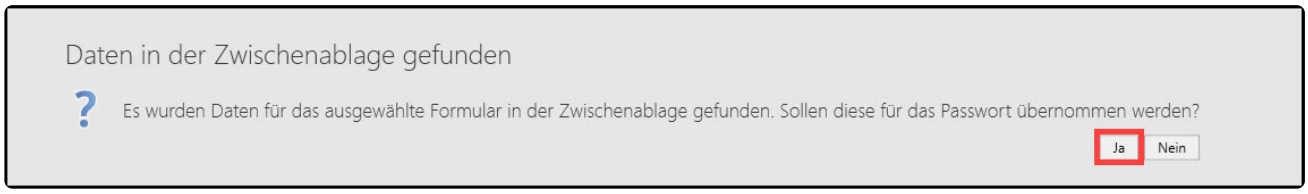


Es öffnet sich ein weiteres Fenster. Hier definieren Sie welche Felder genau kopiert werden sollen. Grundsätzlich sind alle Felder bereits ausgewählt. Ebenfalls entscheiden Sie, ob der Feldnamen auch kopiert werden sollen.

Achtung: Möchten Sie einen Datensatz **duplizieren**, muss dieser Haken gesetzt sein!

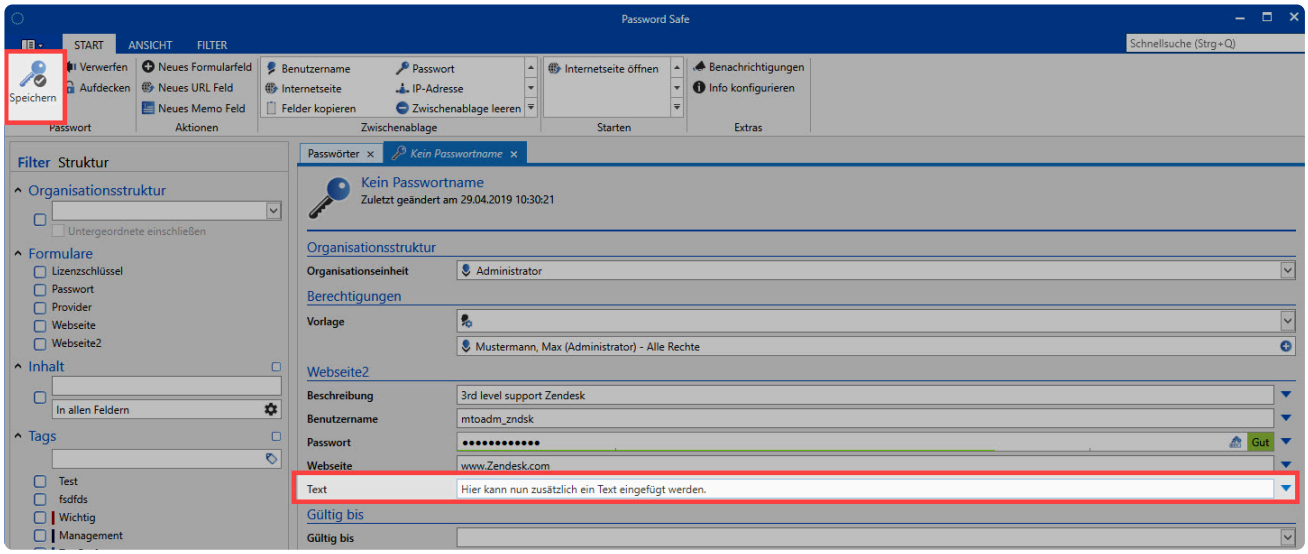


Wenn Sie einen neuen Datensatz angelegen, erscheint die Meldung, dass bereits Daten in der Zwischenablage gefunden wurden. Hier entscheiden Sie, ob diese übernommen werden sollen.



Wenn Sie die Meldung mit **Ja** bestätigen, werden die Daten mit dem **exakt** selben Feldnamen automatisch befüllt. Wenn die Feldnamen nicht gleich sind, werden hier auch keine Daten eingetragen.

Nun befüllen Sie die restlichen Felder (falls vorhanden) speichern den Datensatz ab. Danach setzen Sie die Rechte.

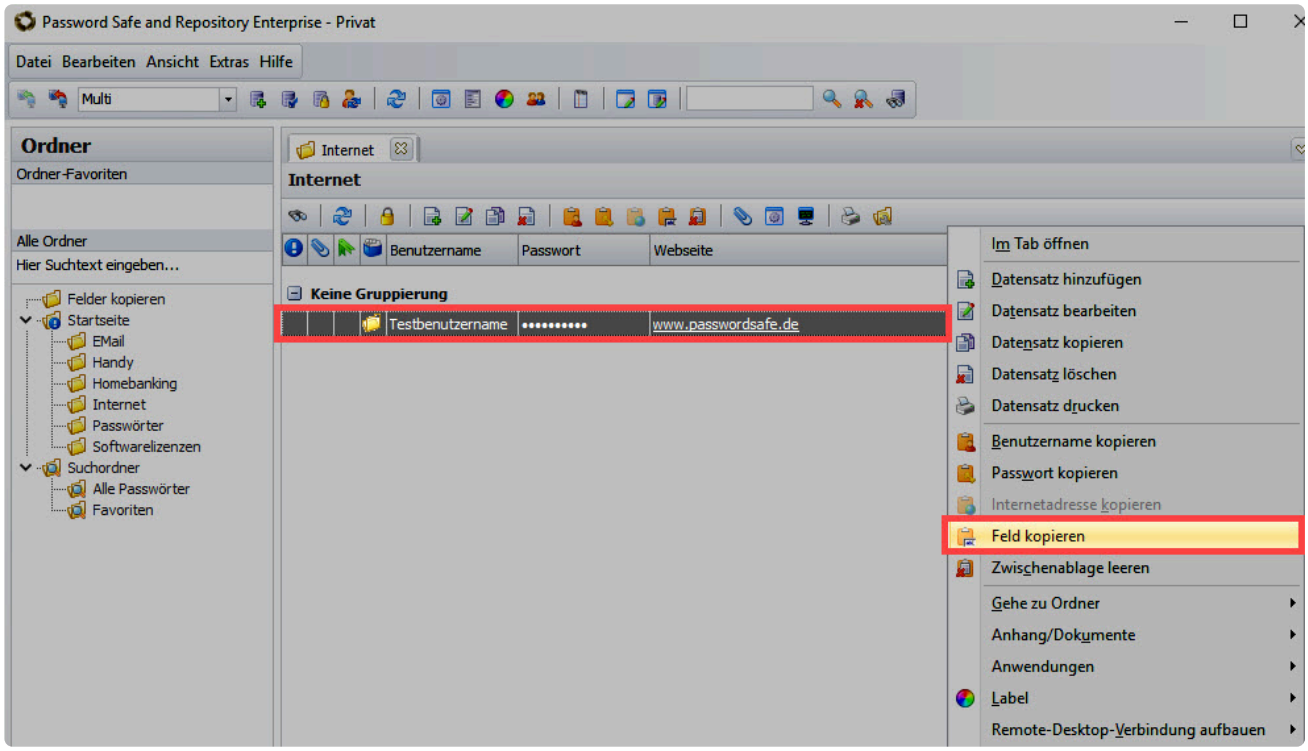


Vorgehensweise mit Daten aus Version 7

Um wenige Datensätze aus der Version 7 schnell und unkompliziert in die Version 8 zu übertragen, können Sie hier ebenfalls die Felder kopieren.

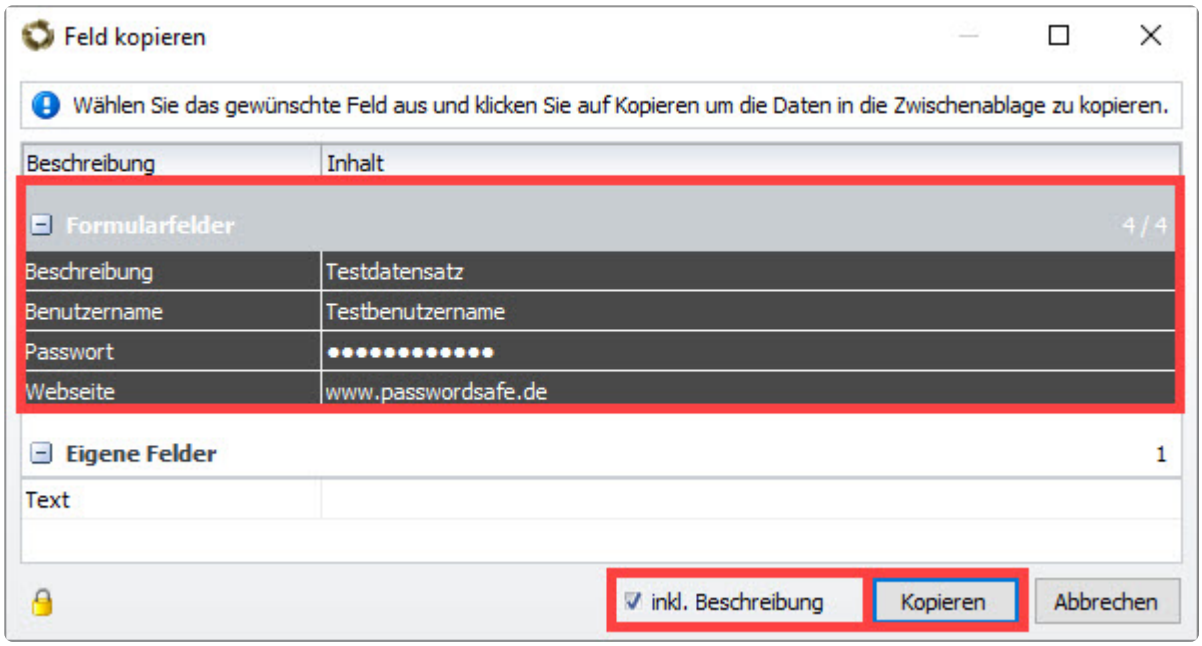
Beachten Sie hierbei folgende Schritte:

1. Wählen Sie den Datensatz aus, welcher in die Version 8 übertragen werden soll.
2. Führen Sie danach einen Rechtsklick auf den Datensatz aus und wählen Sie **Feld kopieren**.

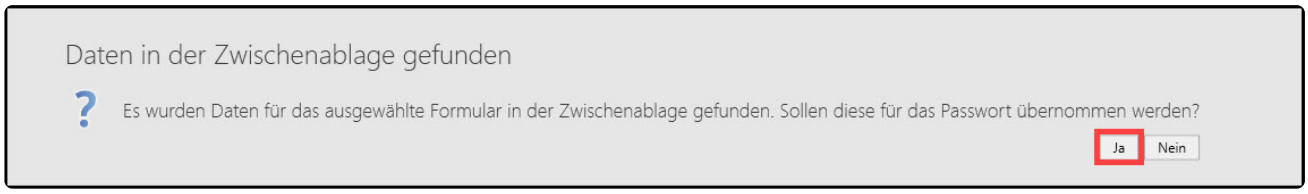


3. Wählen Sie dann per Multiselect die Felder aus, welche kopiert werden sollen und setzen Sie ebenfalls den Haken bei **inkl. Beschreibung**.

4. Bestätigen Sie den Vorgang mit **Kopieren**.



5. Wechseln Sie in die Version 8 und fügen Sie einen neuen Datensatz hinzu.
6. Nun erscheint wieder die selbe Meldung, dass Daten in der Zwischenablage gefunden wurden und ob diese eingetragen werden sollen.



7. Nach der Bestätigung der Meldung erfolgt die Eintragung.
8. Bestätigen Sie den Vorgang mit “Speichern”.
9. Nun können Sie zusätzlich die Rechte definieren.

Rechte auf den Datensatz aber nicht auf das Passwortfeld

Anforderung

Ein oder mehrere Benutzer sollen auf einen Datensatz Zugriff haben, aber nicht auf das Passwortfeld.

Voraussetzungen

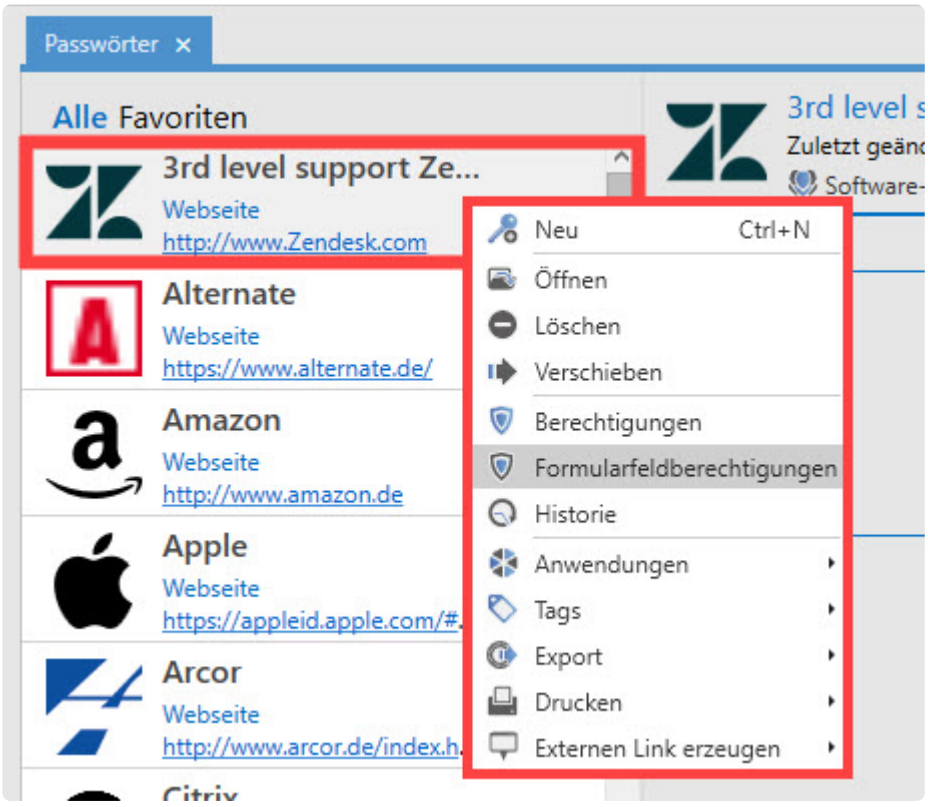
Es muss ein Datensatz vorhanden sein.

Benötigte Benutzerrechte

- Kann Passwortformularfelder verwalten
- Lese- und Berechtigen-recht auf den Datensatz

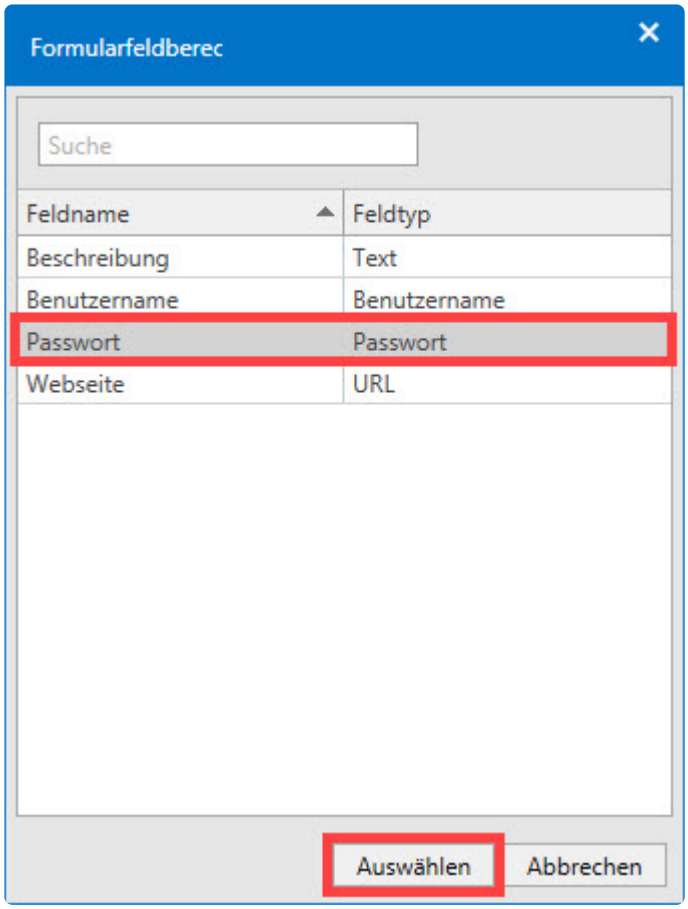
Konfiguration

Zuerst wählen Sie einen Datensatz aus. Danach öffnen Sie per Rechtsklick auf den Datensatz die Formularfeldberechtigungen.



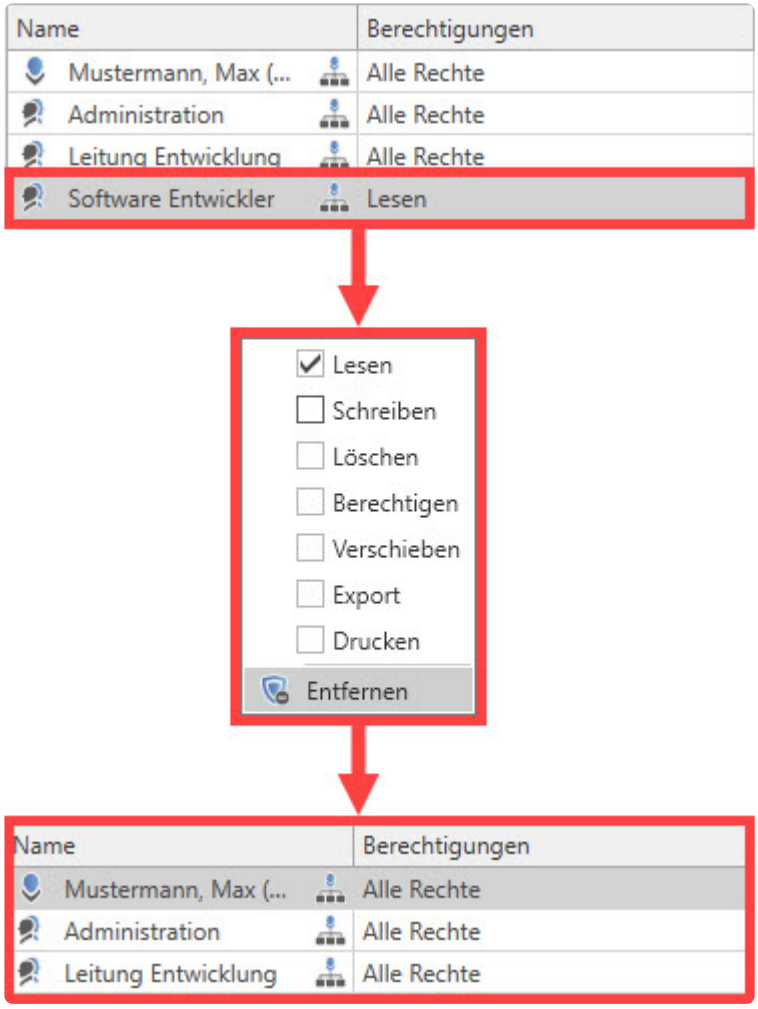
Nun wählen Sie das Formularfeld bzw die Formularfelder aus, für welche die Berechtigungen gelten sollen. Wenn diese für das Passwortfeld gelten sollen, müssen Sie dieses natürlich auch auswählem.

Tipp: Wählen Sie hier per Multiselect auch mehrere Felder gleichzeitig aus.

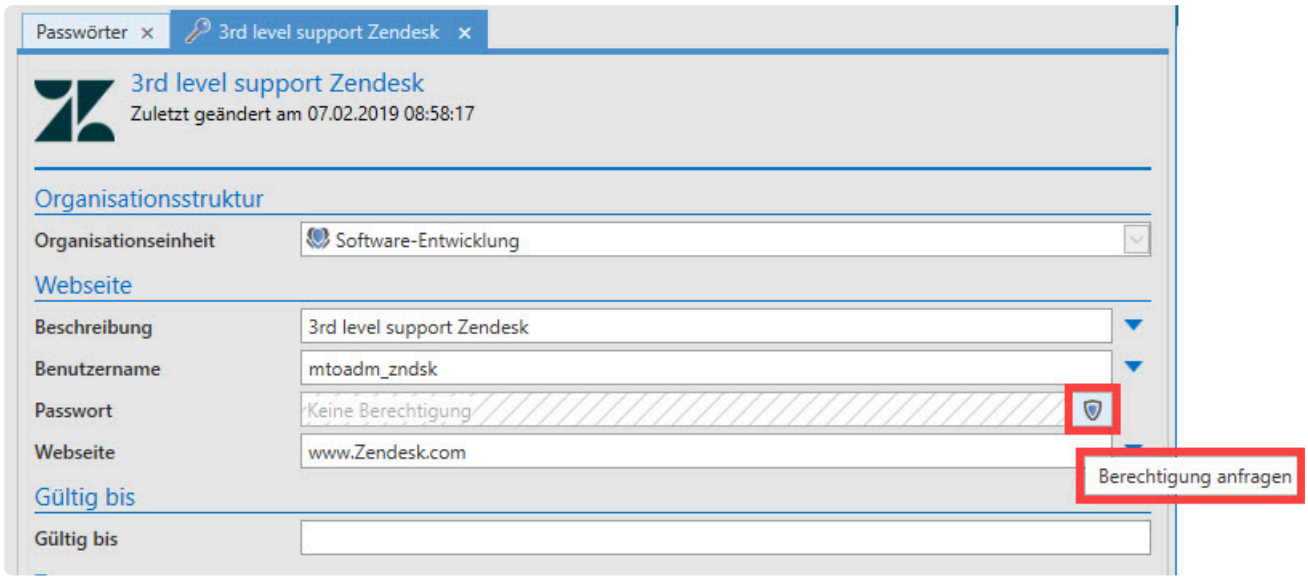


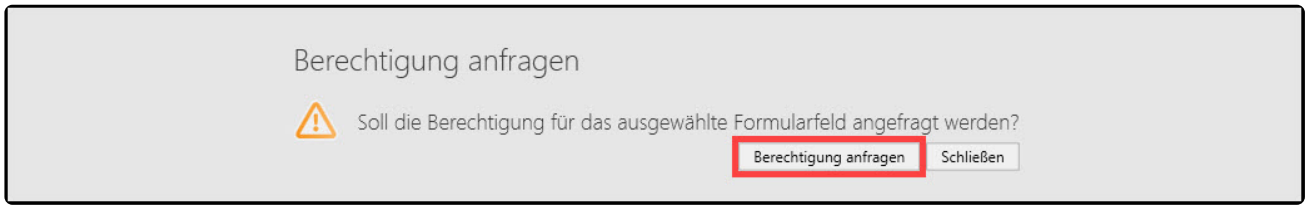
Als Nächstes setzen Sie die Berechtigungen wie gewünscht. Sollte ein Benutzer bereits auf den Datensatz mit dem Leserecht berechtigt sein, so ist er hier auch bereits vorhanden. Wenn Sie nun wünschen, dass der Benutzer das Passwortfeld nicht sehen darf, so entfernen Sie ihn aus den Berechtigungen. Nachdem die gewünschten Änderungen durchgeführt wurden, speichern Sie den Vorgang.

Bei erfolgreicher Konfiguration hat der Benutzer, welcher kein Zugriff auf das Passwortfeld haben darf, folgende Ansicht:

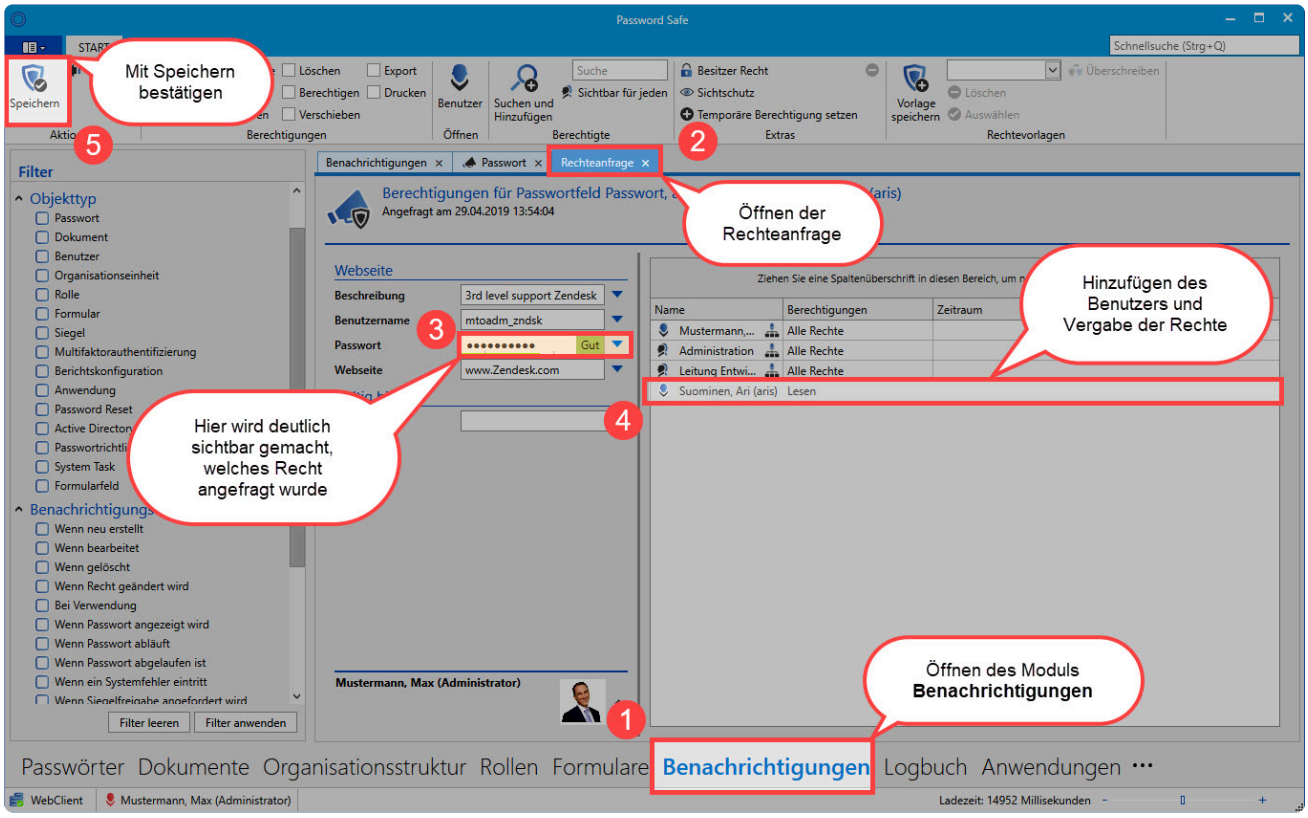


Nun hat der Benutzer die Möglichkeit das Recht anzufragen, indem er auf das Symbol im Formularfeld klickt. Danach können Sie die Berechtigungsanfrage bestätigen.





Diese Rechteanfrage kann nun von einem ausreichend berechtigten User bestätigt werden. Dies erfolgt über das Modul Berechtigungen. Hierauf wird daher auch die Berechtigung auf das Modul Benachrichtigungen benötigt.
Die Freigabe erfolgt dann über die Bestätigung der Rechteanfrage. Hierzu stellen Sie dem anfragendem Benutzer das Recht manuell aus.

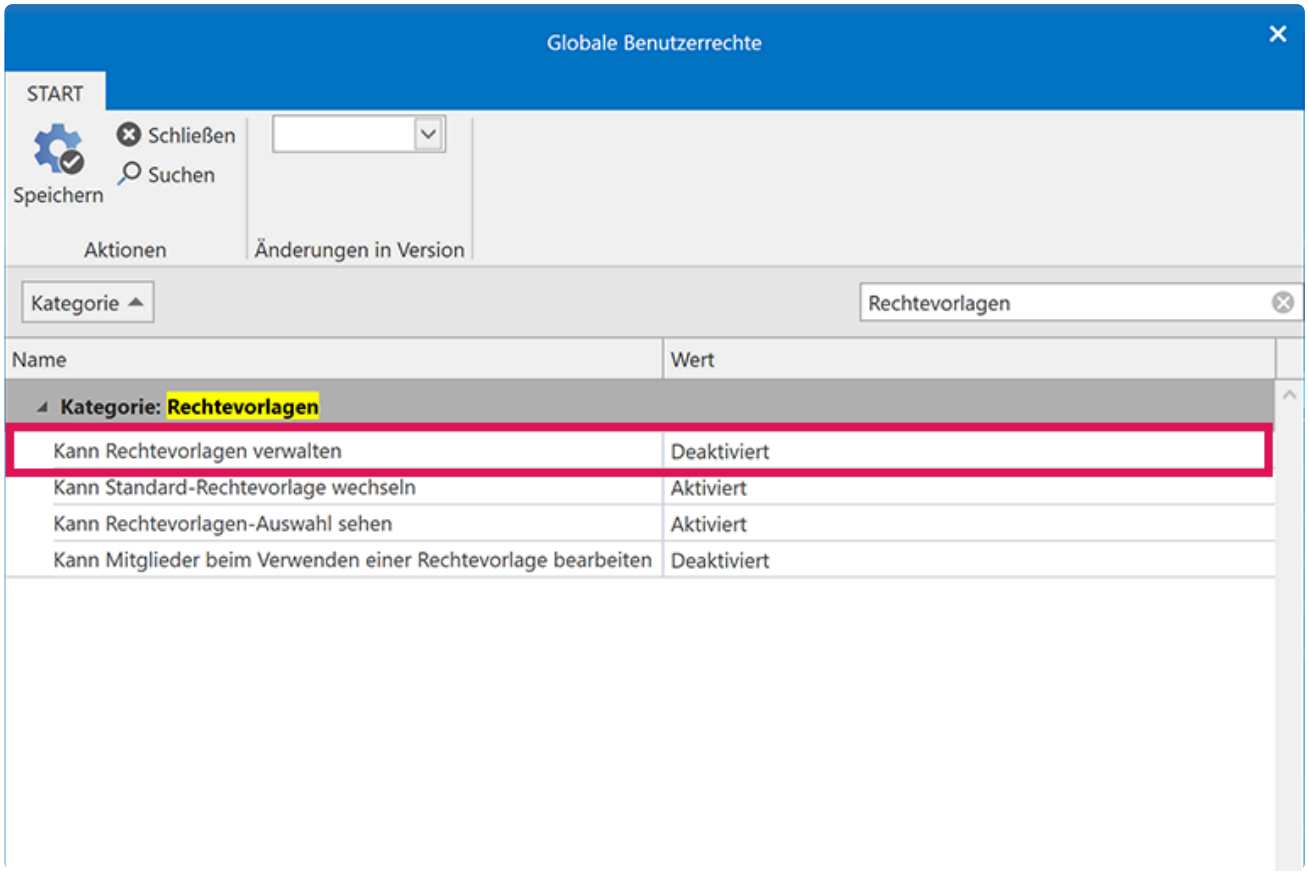


Somit hat der Benutzer nun auch Zugriff auf das Formularfeld **Passwort**.

Anzeigen von Passwörtern mit möglicherweise falsch gesetzten Berechtigungen

Erklärung zum Hotfix in Version 8.10

Aktuell gibt es einen kritischen Bug in Version **8.10**, der eventuell dazu führen könnte, dass Passwörter falsch berechtigt werden. Durch Prüfen eines falschen Rechtes konnten Benutzer eine andere Rechtevorlage auswählen. Beim Speichern vom Passwort wird jedoch immer nur die Standard-Rechtevorlage verwendet. Dies trifft nur für Benutzer zu, bei denen das (globale) Recht **“Kann Rechtvorlagen verwalten”** deaktiviert ist.



Deshalb haben wir nach ausführlicher Prüfung ein Hotfix veröffentlicht. Um kein unnötiges Risiko einzugehen, bitten wir Benutzer von Version 8.10, das aktuelle Hotfix zu installieren. Dieses können Sie über die Updatesuche in der Software oder das Kundeninformationssystem downloaden.

Wen es betrifft

Diese Anleitung betrifft ausschließlich Version **8.10**. Sollte in dieser Version Ihre Standard-Rechtevorlage mehr Rechte beinhalten als die optional ausgewählte, dann können Sie mithilfe dieser Anleitung überprüfen, ob Rechte falsch gesetzt wurden. Dieser Filter gibt die Passwörter aus, bei denen womöglich eine falsche Rechtevorlage ausgewählt wurde.

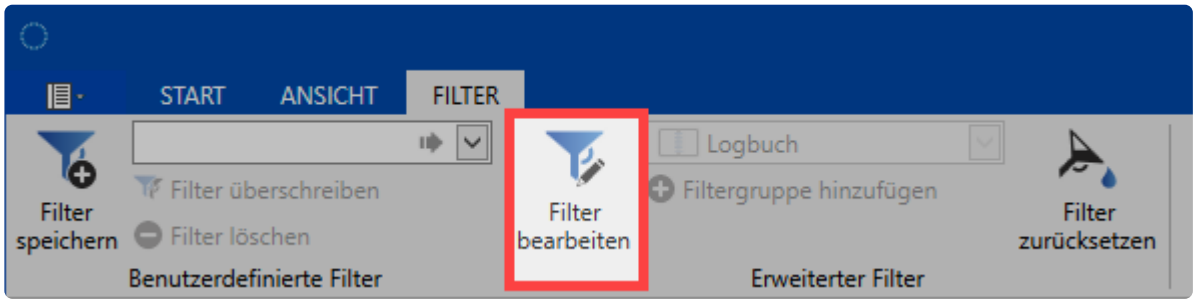
Benötigte Benutzerrechte

- Kann Filter bearbeiten
- Leserechte auf den Datensatz

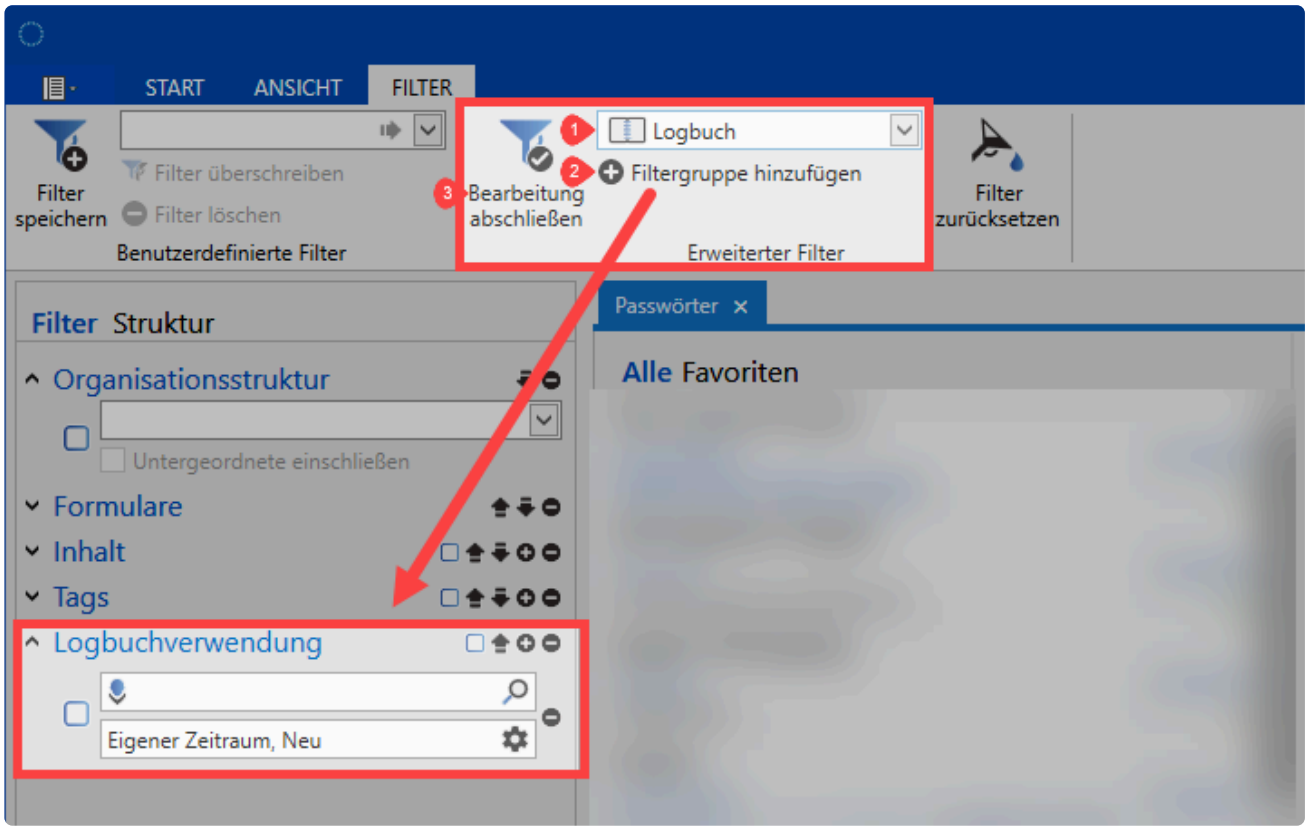
Vorgehensweise

Anleitung für den Administrator

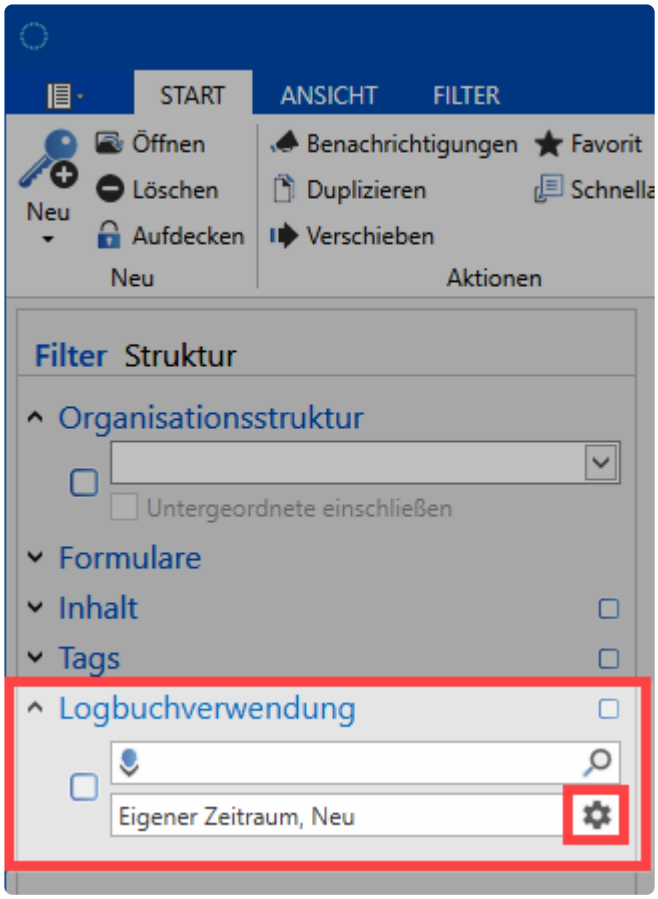
1. Password Safe öffnen
2. Das Modul **Passwörter** auswählen
3. Öffnen der Filteransicht und auf “Filter bearbeiten”



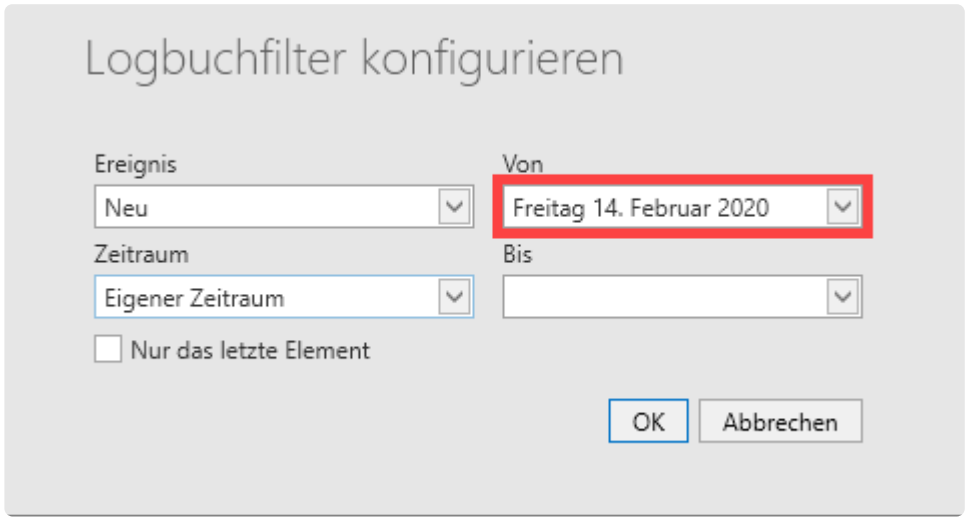
4. Fügen Sie die Filtergruppe “Logbuch” hinzu



5. Filter-Bearbeitung schließen
6. Öffnen Sie die Einstellungen für die Filtergruppe Logbuchverwendung via Klick auf das Zahnrad.



7. Tragen Sie als Startdatum bitte das Datum ein, an dem Sie auf die Version 8.10 upgedatet oder migriert haben. Sollte Ihnen das Datum nicht bekannt sein, verwenden Sie den 14.02.2020, das Datum des offiziellen Releases.



Als Enddatum tragen Sie den heutigen Tag ein. Als Ergebnis erhalten Sie eine Liste aller Passwörter, die von diesem Fehler **möglicherweise** betroffen sind, um sie zu überprüfen.

API

Die Enterprise Plus Edition verfügt über eine **API**: Über diese Schnittstelle ist es Ihnen möglich, Password Safe **von außen anzusprechen**, um beispielsweise Daten für andere Programme auszulesen. Die API ist ausschließlich über unsere Wrapper mit **C#** und **JavaScript** ansprechbar.

In der JavaScript Version der API finden Sie alle Enums unter dem globalen Objekt “PsrApiEnums”.

Voraussetzungen und Download

Die API ist ausschließlich in der Enterprise Plus Edition verfügbar. Im Kunden Informations System können Sie den API-Client für die gewünschte Programmiersprache herunterladen. Um die API nutzen zu können, aktivieren Sie im **AdminClient**, im Modul **WebClient**, die Webservices.

Verwendung der API

Das zentrale Objekt ist „PsrApi“. Dieses enthält diverse „Manager“, die die gesamte Business-Logik enthalten. Zunächst muss ein „PsrApi“-Objekt angelegt werden. Der einzige Übergabeparameter dieser Klasse ist der Endpoint der Password Safe WebServices. Falls Sie den WebClient einsetzen, können Sie “aufruf-des-webclient/api” als Endpoint verwenden. Andernfalls verwenden Sie direkt der Password Safe Server, also “ip-des-servers:11016”.

C#

```
var psrApi = new PsrApi(„passwordsafe.company.com/api“);
```

JavaScript

```
const psrApi = new PsrApi(„passwordsafe.company.com/api“)
```

Login

Ohne einen vorherigen Login ist die Verwendung der API nicht möglich. Der erste Parameter der Login-Methode ist die gewünschte Datenbank, gefolgt von Benutzername und dem Passwort. Beachten Sie, dass alle Methoden der API, die einen Server-Call nach sich ziehen, asynchron implementiert sind. In C# werden also Objekte des Typs „Task“ und in JavaScript Objekte des Typs „Promise“ zurückgegeben.

C#

```
await psrApi.AuthenticationManager.Login(„Company“, „username“, „password“);
```

JavaScript

```
await psrApi.authenticationManager.login(„Company“, „username“, „password“)
```

Methoden

Anschließend können Sie alle Methoden der API verwendet werden. So können Sie beispielsweise nach Datensätzen suchen und ein Passwort entschlüsseln:

C#

```
using System;
using System.Linq;
using System.Threading.Tasks;
using PsrApi.Data;
using PsrApi.Data.Enums;


namespace CSharpSDK
{
    class Program
    {
        static async Task Main(string[] args)
        {
            // Nach dem login können Sie alle Funktionen der API nutzen.
            // Setzen Sie an den mit # markierten Stellen Ihre Zugangsdaten ein.
            var psrApi = new PsrApi.PsrApi("#");
            await psrApi.AuthenticationManager.Login("#", "#", "#");

            // Passwörter sind im Kontext der API Container.
            // Für die Handhabung ist der ContainerManager notwendig.
            var conMan = psrApi.ContainerManager;

            // Um nach bestimmten Passwörtern filtern zu können, benötigen Sie
            // einen Filter vom Typ PsrListFilterGroupContent. Dazu müssen Sie
            // den Standard-Filter für Passwörter abrufen.
            var passwordListFilter = await conMan.GetContainerListFilter(
                PsrContainerType.Password, true);

            // In einem zweiten Schritt können Sie den Standardfilter nach einem
            // Filterobjekt vom Typ PsrListFilterGroupContent durchsuchen.
            var contentFilter = passwordListFilter.FilterGroups
                .OfType<PsrListFilterGroupContent>().FirstOrDefault()
                ?.SearchList.FirstOrDefault();

            if (contentFilter != null)
            {
                // Ersetzen Sie die Stelle # mit Ihrem Suchbegriff.
                // Zudem muss der Filter als Aktiv markiert werden.
                contentFilter.Search = "#";
                contentFilter.FilterActive = true;
```

```
            }

            // Jetzt können Ihre gesuchten Passwörter mit Hilfe des
            // vorher konfigurierten Filters abgerufen werden.
            var passwords = await conMan.GetContainerList(
                PsrContainerType.Password, passwordListFilter);

            var passwordContainer = passwords.FirstOrDefault();
            if (passwordContainer != null)
            {
                // Um Ihr gesuchtes Passwort im Klartext sichtbar machen zu können,
                // müssen Sie nach dem ersten Passwortfeld in der Liste
                // von ContainerItems in Ihrem Passwort suchen.
                var passwordItem = passwordContainer.Items
                    .FirstOrDefault(i => i.ContainerItemType == PsrContainerItemType.Co

                // Das gefundene ContainerItem kann dann entschlüsselt werden.
                var decryptedPasswordString = await conMan.DecryptContainerItem(passwor

                // Danach können Sie das Passwort im Klartext verwenden.
               Console.WriteLine("Your password is: " + decryptedPasswordString);
            }

            // Wird die API nicht mehr benötigt, müssen Sie sich wieder
            // von der aktuellen Sitzung abmelden.
            await psrApi.AuthenticationManager.Logout();
        }
    }
}
```

JavaScript

```
(async function() {

  const { PsrApi, PsrApiEnums } = require('./src/psrApi')
  const { PsrContainerType, PsrContainerItemType } = PsrApiEnums

  // Nach dem login können Sie alle Funktionen der API nutzen.
  // Setzen Sie an den mit # markierten Stellen Ihre Zugangsdaten ein.
  const psrApi = new PsrApi('#')
  await psrApi.authenticationManager.login('#', '#', '#')

  // Passwörter sind im Kontext der API Container.
  // Für die Handhabung ist der ContainerManager notwendig.
  const conMan = psrApi.containerManager
```

```
  // Um nach bestimmten Passwörtern filtern zu können, benötigen Sie
  // einen Filter vom Typ PsrListFilterGroupContent. Dazu müssen Sie
  // den Standard-Filter für Passwörter abrufen.
  const passwordListFilter = await conMan.getContainerListFilter(
    PsrContainerType.Password, true)

  // In einem zweiten Schritt können Sie den Standardfilter nach einem
  // Filterobjekt vom Typ PsrListFilterGroupContent durchsuchen.
  const contentFilter = passwordListFilter.FilterGroups
    .find(fg => 'SearchList' in fg).SearchList[0]

  if (contentFilter) {
    // Ersetzen Sie die Stelle # mit Ihrem Suchbegriff.
    // Zudem muss der Filter als Aktiv markiert werden.
    contentFilter.Search = '#'
    contentFilter.FilterActive = true
  }

  // Jetzt können Ihre gesuchten Passwörter mit Hilfe des
  // vorher konfigurierten Filters abgerufen werden.
  const passwords = await conMan.getContainerList(
    PsrContainerType.Password, passwordListFilter)

  const passwordContainer = passwords[0]
  if (passwordContainer) {
    // Um Ihr gesuchtes Passwort im Klartext sichtbar machen zu können,
    // müssen Sie nach dem ersten Passwortfeld in der Liste
    // von ContainerItems in Ihrem Passwort suchen.
    const passwordItem = passwordContainer.Items
      .find(i => i.ContainerItemType === PsrContainerItemType.ContainerItemPassword)

    // Das gefundene ContainerItem kann dann entschlüsselt werden.
    const decryptedPasswordString = await conMan.decryptContainerItem(passwordItem)

    // Danach können Sie das Passwort im Klartext verwenden.
    console.log('Your password is: ', decryptedPasswordString)
  }

  // Logout nach vollendeter Arbeit nicht vergessen, um tote Sitzungen zu verhindern
  await psrApi.authenticationManager.logout()

})()
```

Technische Dokumentation

Die komplette technische Dokumentation der API finden Sie unter folgendem Link: [Password Safe API]

Supportkontext: Bei der Verwendung der API-Schnittstelle ist zusätzliches technisches Wissen notwendig. Dies fällt nicht in den Zuständigkeitsbereich des Support.
Möchtest Du den Code durch unsere Entwickler überprüfen lassen, oder wünschst Dir Beratung zur API?
Gerne erstellt Dir unser Team ein individuelles Consulting-Angebot. Oder Du nutzt eines unserer Consulting-Pakete, die praktisch nach Stunden abgerechnet werden.

Beispiele C# SDK

> ! Alle folgenden Funktionen (außer Login und Logout) müssen in einem authentifizierten Kontext aufgerufen werden. Verwenden Sie also zuerst die Login-Funktion, bevor Sie eine der folgenden Funktionen ausführen.

Mit Benutzername und Passwort einloggen

```
private static async Task Login()
{
    // Accept invalid certificates - until .NET Framework 4.6
    // When using .NET Framework 4.7 or higher, you need to
    // create an own HttpClientHandler and set the callback there
    ServicePointManager.ServerCertificateValidationCallback += (sender, cert, chain, ss

    Console.Write("Enter your endpoint IP's to proceed (xxx.xxx.xxx.xxx): ");
    var endpointIp = Console.ReadLine();

    var psrApi = new PsrApi($"{endpointIp}:11016");

    Console.WriteLine($"Available databases: {string.Join(", ", await psrApi.GetActiveD

    Console.Write("Database: ");
    var database = Console.ReadLine();

    Console.Write("Username: ");
    var username = Console.ReadLine();

    Console.Write("Password: ");
    var password = ReadPassword();
    var mfaRequest = await psrApi.AuthenticationManager.Login(database, username, passw

    if (mfaRequest != null)
    {
        await PerformMultiFactorAuth(mfaRequest, psrApi, database, username, password);
    }

    psrApi.ServerStatusChanged += (sender, status) => Console.WriteLine(status);
    psrApi.SessionExpired += async (sender, e) =>
    {
        Console.WriteLine("Session has expired");
        //For example, you could relogin here...
    };
```

```
    Console.WriteLine($"Logged in; Session expiring at: { psrApi.SessionExpirationUtc?.

    psrApi.RealtimeEventManager.ServerMessageReceived += (sender, args) =>
        Console.WriteLine(args.ServerMessage.Message + $" was received ({args.ServerMes
    psrApi.RealtimeEventManager.ContainerChanged += (sender, args) =>
        Console.WriteLine(args.Container.DataName() + $" was changed ({args.EventType.T
    psrApi.RealtimeEventManager.RoleChanged += (sender, args) =>
        Console.WriteLine(args.Role.DataName() + $" was changed ({args.EventType.ToStri
    psrApi.RealtimeEventManager.UserChanged += (sender, args) =>
        Console.WriteLine(args.User.DataName() + $" was changed ({args.EventType.ToStri
    psrApi.RealtimeEventManager.GroupChanged += (sender, args) =>
        Console.WriteLine(args.Group.DataName() + $" was changed ({args.EventType.ToStr
    psrApi.RealtimeEventManager.DataBindingChanged += (sender, args) =>
        Console.WriteLine(args.DataBinding.DataId + $" was changed ({args.EventType.ToS

    _psrApi = psrApi;
}

private static async Task PerformMultiFactorAuth(PsrMultiFactorAuthenticationRequest mf
{
    if (mfaRequest.AuthenticatorType == PsrMultiFactorAuthType.Pki)
    {
        var pkiFields = GetCertificatePkiFields(mfaRequest);

        mfaRequest.RequiredFields.ToList().Find(f => f.Type == PsrMultiFactorField.Sign
        mfaRequest.RequiredFields.ToList().Find(f => f.Type == PsrMultiFactorField.Cert
    }
    else
    {
        foreach (var field in mfaRequest.RequiredFields)
        {
            Console.Write($"Enter 2nd factor '{mfaRequest.DisplayName}' ({field.Type.To
            var mfa = field.Type == PsrMultiFactorField.Pin || field.Type == PsrMultiFa
                ? ReadPassword()
                : Console.ReadLine();
            field.Value = mfa;
        }
    }

    await psrApi.AuthenticationManager.Login(database, username, password, mfaRequest.R
}

private static PkiFields GetCertificatePkiFields(PsrMultiFactorAuthenticationRequest mf
{
    Console.WriteLine("Select a certificate from the store");
    var store = new X509Store("MY", StoreLocation.CurrentUser);
    store.Open(OpenFlags.ReadOnly | OpenFlags.IncludeArchived);
```

```
    var collection = store.Certificates.Find(X509FindType.FindByKeyUsage, X509KeyUsageF
    var selectedCert = X509Certificate2UI.SelectFromCollection(collection, "Select a ce
        X509SelectionFlag.SingleSelection)[0];
    if (!(selectedCert.PrivateKey is RSACryptoServiceProvider csp))
    {
        throw new Exception();
    }

    string signedHash;
    using (var hashAlgo = HashAlgorithm.Create(HashAlgorithms.Sha1.ToString()))
    {
        if (hashAlgo == null)
        {
            throw new Exception();
        }

        var hash = hashAlgo.ComputeHash(mfaRequest.DataToSign);
        var oid = CryptoConfig.MapNameToOID(HashAlgorithms.Sha1.ToString());
        var bytes = csp.SignHash(hash, oid);
        signedHash = Convert.ToBase64String(bytes);
    }

    return new PkiFields()
    {
        SignedDataId = signedHash,
        CertificateThumbPrint = selectedCert.Thumbprint
    };
}

public class PkiFields
{
    public string SignedDataId;
    public string CertificateThumbPrint;
}
```

Ausloggen

```
await _psrApi.AuthenticationManager.Logout();
Console.WriteLine("PsrApi logged out")
```

Ein Passwort für den eigenen Benutzer erstellen

```
var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, PasswordGener
var passwordContainer = new PsrContainer
```

```
{
    ContainerType = PsrContainerType.Password,
    Items = new List<PsrContainerItem>
    {
        new PsrContainerItem
        {
            Name = "Name",
            ContainerItemType = PsrContainerItemType.ContainerItemText,
            Value = "MyPsrApiPassword_SIMPLE",
        },
        new PsrContainerItem
        {
            Name = "Password",
            ContainerItemType = PsrContainerItemType.ContainerItemPassword,
            PlainTextValue = "utlra secret password goes here",
        },
    }
};

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, _psr
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Ein Passwort für eine Organisationseinheit erstellen

```
var passwordContainer = new PsrContainer
{
    ContainerType = PsrContainerType.Password,
    Items = new List<PsrContainerItem>
    {
        new PsrContainerItem
        {
            Name = "Name",
            ContainerItemType = PsrContainerItemType.ContainerItemText,
            Value = "MyPsrApiPassword_SIMPLE",
        },
        new PsrContainerItem
        {
            Name = "Password",
            ContainerItemType = PsrContainerItemType.ContainerItemPassword,
            PlainTextValue = "utlra secret password goes here",
        },
    }
};

// find the organisational unit to put our new password (we take the most top ou)
```

```
var filter = new PsrListFilter
{
    DataStates = PsrDataStates.StateActive,
    FilterGroups = new List<PsrListFilterGroup>
    {
        new PsrListFilterGroupOrganisationUnitType
        {
            TypeFilters = new List<PsrListFilterObjectOrganisationUnitType>
            {
                new PsrListFilterObjectOrganisationUnitType
                {
                    FilterActive = true,
                    OrganisationUnitType = PsrFilterOrganisationUnitType.FilterOrganisa
                }
            }
        }
    }
};
var ouGroups = await _psrApi.OrganisationUnitManager.GetOrganisationUnitStructure(filte
var topLevelOu = ouGroups?.FirstOrDefault();
var targetOu = topLevelOu?.OrganisationUnit ?? _psrApi.CurrentUser;

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, targ
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Ein Passwort mittels einem bestimmten Formulars für den eigenen Benutzer erstellen

```
var formsFilter = await _psrApi.ContainerManager.GetContainerListFilter(PsrContainerTyp
var availableForms = await _psrApi.ContainerManager.GetContainerList(PsrContainerType.F

if (!availableForms.Any())
{
    Console.WriteLine("no forms found");
    return;
}

var passwordContainer = _psrApi.ContainerManager.CreateContainerFromBaseContainer(avail

var textField = passwordContainer.Items.FirstOrDefault(ci => ci.ContainerItemType == Ps
if (textField != null) textField.Value = "MyPsrApiPassword_FORM";

var urlField = passwordContainer.Items.FirstOrDefault(ci => ci.ContainerItemType == Psr
if (urlField != null) urlField.Value = "https://www.passwordsafe.de";
```

```
var passwordField = passwordContainer.Items.FirstOrDefault(ci => ci.IsPasswordItem());
if (passwordField != null)
{
    var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, PasswordG
    passwordField.PlainTextValue = newPassword;
}

var savedPassword = await _psrApi.ContainerManager.AddContainer(passwordContainer, _psr
Console.WriteLine($"Password {passwordContainer.DataName()} ({savedPassword.Id}) create
```

Passwörter mit Hilfe der Inhaltssuche finden

```
var filter = new PsrContainerListFilter
{
    DataStates = PsrDataStates.StateActive,
    FilterGroups = new List<PsrListFilterGroup>
    {
        new PsrListFilterGroupContent
        {
            SearchList = new List<PsrListFilterObjectContent>
            {
                new PsrListFilterObjectContent
                {
                    FilterActive = true,
                    Search = "MyPsrApiPassword_",
                }
            }
        }
    }
};

var passwords = await _psrApi.ContainerManager.GetContainerList(PsrContainerType.Passwo
Console.WriteLine($"{passwords.Count()} Passwords found with Content 'MyPsrApiPassword_
```

Ein Passwort mittels der ID finden

```
var password = await _psrApi.ContainerManager.GetContainer(id);
if (password != null) Console.WriteLine($"Password {password.DataName()} retrieved by G
```

Ein Passwort aktualisieren

```
private static async Task UpdatePassword(PsrContainer updatePassword)
{
```

```
    var textField = updatePassword.Items.FirstOrDefault(ci => ci.ContainerItemType == P
    if (textField != null) textField.Value = "MyPsrApiPassword_UPDATE";

    var passwordField = updatePassword.Items.FirstOrDefault(ci => ci.IsPasswordItem());
    if (passwordField != null)
    {
        var newPassword = _psrApi.PasswordManager.GeneratePhoneticPassword(20, 3, Passw
        passwordField.PlainTextValue = "UPDATED_SECRET_PASSWORD_" + newPassword;
    }

    await _psrApi.ContainerManager.UpdateContainer(updatePassword);
    Console.WriteLine($"Password {updatePassword.Id} updated");
}
```

Ein Passwort löschen

```
await _psrApi.ContainerManager.DeleteContainer(deletePassword);
Console.WriteLine($"Password {deletePassword.Id} deleted");
```

Benutzer zum Mitglied einer Rolle machen

```
private static async Task MakeUserRoleMember(Guid userId, Guid roleId)
{

    var role = await _psrApi.RoleManager.GetRole(roleId);
    var user = await _psrApi.OrganisationUnitManager.GetOrganisationUnitUser(userId);
    var rights = (await _psrApi.RightManager.GetLegitimateDataRightsWithTemporalRights(
    rights.Add(new PsrDataRight
    {
        DataId = roleId,
        LegitimateId = userId,
        Legitimate = user,
        IncludeDataRightKey = true,
        Rights = PsrRights.RightRead
    });
    await _psrApi.GenericRightManager.SaveRights(new List<PsrData> { role }, rights, fa
}
```

Eine Organisationseinheit anhand des Namens finden

```
private static async Task<IEnumerable<PsrOrganisationUnitStructure>> FindOrganisationUn
{
    var filterGroups = new List<PsrListFilterGroup>
```

```
    {
        new PsrListFilterGroupContent
        {
            SearchList = new List<PsrListFilterObjectContent>
            {
                new PsrListFilterObjectContent
                {
                    FilterActive = true,
                    Search = name,
                }
            }
        }
    };

    // if we should search in a specified parent, we have to add this as filter conditi
    if (parent != null)
    {
        filterGroups.Add(new PsrListFilterGroupOrganisationUnit
        {
            OrganisationUnitFilter = new PsrListFilterObjectOrganisationUnit
            {
                FilterActive = true,
                SelectedOrganisationUnitId = parent.Id
            }
        });
    }

    var ouContentFilter = new PsrListFilter
    {
        DataStates = PsrDataStates.StateActive,
        FilterGroups = filterGroups
    };

    return (await _psrApi.OrganisationUnitManager.GetOrganisationUnitStructure(ouConten
}
```

Erstellen einer Organisationseinheit unterhalb einer bereits existierenden

```
private static Task<PsrOrganisationUnitGroup> CreateOrgainsationUnitGroup(string name,
{
    var rsa = new PsrRsa();
    var group = new PsrOrganisationUnitGroup
    {
        GroupName = name,
```

```
        PublicKey = rsa.PublicKey,
    };

    var encryptedGroupKey = PsrEncryption.EncryptWithPublicKey(_psrApi.CurrentUser.Publ
    return _psrApi.OrganisationUnitManager.AddOrganisationUnitGroup(group, _psrApi.Curr
}
```

Überprüfen, ob eine Organisationseinheit unterhalb einer bestimmten Organisationseinheit existiert und wenn nicht Erstellen dieser.

```
private static async Task<PsrOrganisationUnit> CheckIfOuExists(string parentOuName, str
{
    var myParentOu = (await FindOrganisationUnitsByName(parentOuName)).FirstOrDefault()
    if (myParentOu == null)
    {
        Console.WriteLine("Parent-OU doesn't exist");
        return null;
    }

    var myChildOu = (await FindOrganisationUnitsByName(findOrCreateOuName, myParentOu.O
    if (myChildOu != null)
    {
        Console.WriteLine("ou found -> not creating anything");
        return myChildOu.OrganisationUnit;
    }

    Console.WriteLine("ou not found -> we create now the ou group");
    return await CreateOrgainsationUnitGroup(findOrCreateOuName, myParentOu.Organisatio
}
```

Alle Benutzer finden, die Datenbank-Administrator sind

```
private static async Task LoadAllDatabaseAdmins()
{
    var onlyUserOus = new PsrListFilter
    {
        FilterGroups = new List<PsrListFilterGroup>
        {
            new PsrListFilterGroupOrganisationUnitType
            {
                TypeFilters = new List<PsrListFilterObjectOrganisationUnitType>
                {
```

```
                    new PsrListFilterObjectOrganisationUnitType
                    {
                        FilterActive = true,
                        OrganisationUnitType = PsrFilterOrganisationUnitType.FilterOrga
                    }
                }
            }
        }
    };

    Console.WriteLine($"Following Users have the Database Admin Right:");
    var organisationUnitUsers = await _psrApi.OrganisationUnitManager.GetOrganisationUn
    foreach (var user in organisationUnitUsers.Select(ous => ous.OrganisationUnit as Ps
    {
        var rightsOfUsers = await _psrApi.OptionManager.GetOptions(new List<PsrOptionGr
        var dbAdminRight = rightsOfUsers.FirstOrDefault(r => r.Name == PsrUserRightDefa
        if (dbAdminRight is PsrOptionBoolean bDbAdminRight && bDbAdminRight.ValueBoolea
        {
            Console.WriteLine($"- {user.UserName}");
        }
    }
}
```

Beispiele Javascript SDK

> ! Alle folgenden Funktionen (außer Login und Logout) müssen in einem authentifizierten Kontext aufgerufen werden.

Benutzer hinzufügen

```
const { EncryptWithPassword, EncryptWithPublicKey } = require('../node/lib/MtoEncryptic
const { MtoPbkdf2GenerateSalt } = require('../node/lib/MtoPbkdf2');
const MtoRsa = require('../node/lib/MtoRsa');

const createUser = async (api, username, password, parentId) => {
  const encodedPassword = unescape(encodeURIComponent(password))
  const pwHash = MtoPbkdf2GenerateSalt(encodedPassword, 16, 100000, 32)
  const rsa = new MtoRsa()
  rsa.generateKeyPair()
  const encryptedPrivateKeyWithPassword = EncryptWithPassword(encodedPassword, rsa.priv

  // Membership of current API user
  const currentUserRsa = new MtoRsa()
  currentUserRsa.publicKeyFromXml(api.currentUser.PublicKey)
  const encryptedPrivateKeyWithPublicKey = EncryptWithPublicKey(currentUserRsa, rsa.pri

  const user = {
    UserName: username
  }

  await api.organisationUnitManager.addOrganisationUnitUser(
    user,
    pwHash.key,
    pwHash.salt,
    rsa.publicKeyToXml(),
    encryptedPrivateKeyWithPassword,
    encryptedPrivateKeyWithPublicKey,
    parentId
  )
}
```

Tag hinzufügen

```
// Data may be any PsrData like PsrContainer, PsrRole, PsrOrganisationUnitUser …
const addTag = async (api, data, tagId) => {
  const dataTags = data.DataTags
```

```
  dataTags.push({
    DataId: data.Id,
    TagId: tagId
  })

  await api.tagManager.setDataTags(dataTags, data.Id)
}
```

Versionshistorie

Die bisher veröffentlichten Versionen und die zugehörigen Changelogs sind unter den folgenden Kapiteln zu finden.

- Version 8.14.3.27962
- Version 8.14.2.27917
- Version 8.14.1.27830
- Version 8.14.0.27745
- Version 8.13.14.27679
- Version 8.13.13.27522
- Version 8.13.12.27427
- Version 8.13.11.27156
- Version 8.13.10.26901
- Version 8.13.9.26689
- Version 8.13.8.25983
- Version 8.13.7.25979
- Version 8.13.6.25933
- Version 8.13.5.25731
- Version 8.13.4.25228
- Version 8.13.3.25194
- Version 8.13.2.25151
- Version 8.13.1.25117
- Version 8.13.0.25027
- Version 8.12.1.22757
- Version 8.12.0.22707
- Version 8.11.1.19828 Hotfix 1
- Version 8.11.1.19823
- Version 8.11.0.19788
- Version 8.10.0.18473 Hotfix 2
- Version 8.10.0.18516 Hotfix 1
- Version 8.10.0.18472
- Version 8.9.0.17993 Hotfix 2
- Version 8.9.0.17702 Hotfix 1
- Version 8.9.0.17656
- Version 8.8.0.18002 Hotfix 3
- Version 8.8.0.17596 Hotfix 2
- Version 8.8.0.17168 Hotfix 1
- Version 8.8.0.17146
- Version 8.7.0.18000 Hotfix 3
- Version 8.7.0.16698 Hotfix 2
- Version 8.7.0.16387 Hotfix 1
- Version 8.7.0.16245
- Version 8.6.0.15386 Hotfix 1
- Version 8.6.0.15368
- Version 8.5.0.14896
- Version 8.4.0.14618

- Version 8.3.0.13378
- Version 8.2.0.12343
- Version 8.3.0.14422 Hotfix 1
- Version 8.2.0.12388 Hotfix 1
- Version 8.1.0.10812
- Version 8.1.1.11106
- Version 8.1.1.11211 Hotfix 1
- Version 8.0.2.9541 Hotfix 1
- Version 8.0.2.9978 Hotfix 2
- Version 8.0.1.9032
- Version 8.0.2.9278

Version 8.14.3.27962

Veröffentlichung

07.07.2022

Kompatibilität

Zum AdminClient der Version 8.14.3.27962 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.14.3.27962
- Windows Client Version 8.14.2.27917
- Windows Client Version 8.14.1.27830
- Windows Client Version 8.14.0.27745
- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.14.3.27962
- WebClient Version 8.14.2.27917
- WebClient Version 8.14.1.27830
- WebClient Version 8.14.0.27745
- WebClient Version 8.13.14.27679
- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.14.3.27962 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.11.1.19828 Hotfix 1, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Neu

LightClient in der Web-Ansicht

- Einträge können nun als Favoriten gesetzt und angezeigt werden.

Verbesserung

LightClient in der Web-Ansicht

- In der Kachelansicht der Liste an Datensätzen wurden die Kacheln vergrößert.

Behoben

FullClient

- KeePass-Datenbanken können auch mit deaktiviertem Benutzerrecht “Kann Tags hinzufügen” importiert werden.

LightClient in der Web-Ansicht

- Lange Titel von Anwendungen werden wieder korrekt angezeigt.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.8.14.3.27962-de.msi)
`876711ca2727b20680dbdb85db01f2e318b2e174e201380c7c177f32cc1012f4c5f02a90ad6f09c53c510`

Englisches Server Setup (pss8.8.14.3.27962-en.msi)
`7d1f0eeb44f01f49e855f5525fb06e84116a943255f06a4480ef6ff87acb29fd884ac43d269ee85030603`

Deutsches Client Setup (psc8.8.8.14.3.27962-de.msi)
`e0526e5932b985232cdb12cfb9ec6335654341367234932228c8c20a9906c8da93ebf2e9f0d0654248a14a`

Englisches Client Setup (psc8.8.8.14.3.27962-en.msi)
`5ba13e1fee9e2ac61c6720f927d259534718b7aaf94c88a5b2ae0eee0110c6aa854092fe6dda337de9515`

Version 8.14.2.27917

Veröffentlichung

22.06.2022

Kompatibilität

Zum AdminClient der Version 8.14.2.27917 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.14.2.27917
- Windows Client Version 8.14.1.27830
- Windows Client Version 8.14.0.27745
- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.14.2.27917
- WebClient Version 8.14.1.27830
- WebClient Version 8.14.0.27745
- WebClient Version 8.13.14.27679
- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Änderung

WebClient

- Der veraltete Produkttest-Banner wird nicht mehr angezeigt.

Verbesserung

Server

- In der Syslog-Ausgabe des Logbuchs wird der “ClientUser” nun zu “WindowsUser” umbenannt und der Name des betroffenen Password Safe Benutzers wird ebenfalls gelogt.

AdminClient

- Wenn die akzeptierten eingehenden IP-Adressen als “Alle” eingestellt sind, kann man den Endpunkt für einen lokalen Webserver als “Loopback” einstellen oder die IP-Adresse und Hostnamen selbst wählen.

Browser-Erweiterungen

- Die Performance beim Entschlüsseln von Passwörtern wurde verbessert.

Behoben

FullClient

- Das Tastenkürzel “Strg + Q” für die Schnellsuche funktioniert wieder.
- Beim Wählen einer bestimmten Backup-Intervall-Konfiguration stürzt das Programm nicht mehr ab.
- Wenn man bei einem Element einer Filtergruppe die “Entfernen”-Schaltfläche anklickt, wird nicht mehr die ganze Filtergruppe entfernt, sondern nur das Filterelement.

WebClient

- Die Baumstruktur im Organisationseinheiten-Modul kann normal gescrollt werden mit vielen OUs.
- Das Logbuchmodul kann in jeder Browsersprache geladen werden.
- Bei einer großen Anzahl verfügbarer Tags wird das Kontextmenü überschaubar angezeigt.
- Beim Anlegen eines Dokuments mit Rechtevorlage wird der Rechteschlüssel korrekt erzeugt.

LightClient in der Web-Ansicht

- Beim Wechseln der Sprache passen sich alle Beschriftungen und Texte sofort an.
- Passwörter können bei kleiner Display-Breite bearbeitet werden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.8.14.2.27917-de.msi)

99aed6b5e579dbbe19ff24efb7ece9e1b8918dc25db6b13a9e5c58045926002bd141ad4506360d752a35b

Englisches Server Setup (pss8.8.14.2.27917-en.msi)

7a00637b562db3d02d59edebeb681c4c1b940f7544daabf6e0c651ef598e1e95cb302f296c28d73a06f67

Deutsches Client Setup (psc8.8.14.2.279170-de.msi)

0c9b9f5f53050d8b009b23eec5ae548b9e2493e92f4872102be74700618fdce9e0cc71bc28c385962662b

Englisches Client Setup (psc8.8.14.2.27917-en.msi)

5780967bcfcdc0b431bd26bfec1f20190b52facbc074b1f2808a312e4c4cb619070a5c2e5a42248750246

Version 8.14.1.27830

Veröffentlichung

04.05.2022

Kompatibilität

Zum AdminClient der Version 8.14.1.27830 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.14.1.27830
- Windows Client Version 8.14.0.27745
- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.14.1.27830
- WebClient Version 8.14.0.27745
- WebClient Version 8.13.14.27679
- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✱ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Behoben

FullClient

- Das Zurücksetzen des Kennworts funktioniert wieder nach dem Überschreiben von Berechtigungen, wenn die Benutzereinstellung “Berechtigungsänderungen von Organisationseinheiten auf Kennwörter vererben” aktiviert ist und Sie die Berechtigungen der OU, die das Kennwort für die Anmeldeinformationen enthält, über das Skript “Kennwort zurücksetzen” geändert haben.
- Das Starten einer neuen WebViewer-Systemaufgabe und das Speichern erfordern immer ein Passwort, ein leeres Passwort ist nicht mehr möglich.
- Nach einem Export mit dem HTML WebViewer, werden zuverlässig alle Objekte wieder richtig dargestellt und alle Funktionen sind wieder aufrufbar.
- Ein Hinweis und Rückfrage zu Änderungen werden nur aktiviert, wenn auch wirklich Änderungen am Datensatz gemacht wurden.
- Benachrichtigungs-Mails können verschickt werden, sobald eine gültige Konfiguration im Admin-Client hinterlegt wurde.
- Nach Änderungen an Objekten und Berechtigungen kann die Offline-Synchronisation unbegrenzt häufig durchgeführt werden.

WebClient

- Das Zurücksetzen des Kennworts funktioniert wieder nach dem Überschreiben von Berechtigungen, wenn die Benutzereinstellung “Berechtigungsänderungen von Organisationseinheiten auf Kennwörter vererben” aktiviert ist und Sie die Berechtigungen der OU, die das Kennwort für die Anmeldeinformationen enthält, über das Skript “Kennwort zurücksetzen” geändert haben.
- Azure AD Import zeigt die Objektliste im WebClient wieder an.
- Ein Hinweis und Rückfrage zu Änderungen werden nur aktiviert, wenn auch wirklich Änderungen am Datensatz gemacht wurden.
- Benachrichtigungs-Mails können verschickt werden, sobald eine gültige Konfiguration im Admin-Client hinterlegt wurde.

AdminClient

- Benachrichtigungs-Mails können verschickt werden, sobald eine gültige Konfiguration im Admin-Client hinterlegt wurde.

Browser-Erweiterungen

- Wenn Sie beim erneuten Öffnen des Browsers mehrere Registerkarten geladen haben, können Sie sich im Addon anmelden, ohne dass alle Registerkarten vollständig geladen sind.

OfflineClient

- Nach Änderungen an Objekten und Berechtigungen kann die Offline-Synchronisation unbegrenzt häufig durchgeführt werden.

LightClient

- Ein Hinweis und Rückfrage zu Änderungen werden nur aktiviert, wenn auch wirklich Änderungen

am Datensatz gemacht wurden.

LightClient in der Web-Ansicht

- Das Kontextmenü erscheint wieder für Anwendungen im WebLight-Client für Anwendungen in der Kachel- und Listenansicht.
- Ein Hinweis und Rückfrage zu Änderungen werden nur aktiviert, wenn auch wirklich Änderungen am Datensatz gemacht wurden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.8.14.1.27830-de.msi)
`cbb2e08a2a967c2a10fc346fd065efd8fbafb5821d53e48bb613c95479aa2d2be9a114565bfbd933fffc7`

Englisches Server Setup (pss8.8.14.1.27830-en.msi)
`ee7132430fb77298f9d0bac645091bd9d254dda849721b2b65bf3aa2ffc0e87a36b2236709c5b000b9e90`

Deutsches Client Setup (psc8.8.14.1.27830-de.msi)
`6449f8c88546ea4b9ace2211dcb4fa401e4e265aba36873275b8e5d9815d6f6ea19888b77d8aa8c1a3a6d`

Englisches Client Setup (psc8.8.14.1.27830-en.msi)
`0aebbf7b3d4728a91c9ae57746609dce22a70a9505b9c03acb5d3bdb86779ca5e1a0fcbc76779d0903665`

Version 8.14.0.27745

Veröffentlichung

13.04.2022

Kompatibilität

Zum AdminClient der Version 8.14.0.27745 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.14.0.27745
- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.14.0.27745
- WebClient Version 8.13.14.27679
- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✻ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Neu

FullClient

- Password Safe unterstützt nun Azure Active Directory.

WebClient

- Password Safe unterstützt nun Azure Active Directory.

Server

- Password Safe unterstützt nun Azure Active Directory.

AdminClient

- Password Safe unterstützt nun Azure Active Directory.

Browser-Erweiterungen

- Password Safe unterstützt nun Azure Active Directory.

Android App

- Password Safe unterstützt nun Azure Active Directory.

iOS App

- Password Safe unterstützt nun Azure Active Directory.

SSO Client

- Password Safe unterstützt nun Azure Active Directory.

OfflineClient

- Password Safe unterstützt nun Azure Active Directory.

LightClient

- Password Safe unterstützt nun Azure Active Directory.

LightClient in der Web-Ansicht

- Password Safe unterstützt nun Azure Active Directory.

MSP

- Password Safe unterstützt nun Azure Active Directory.

Verbesserung

Server

- Wie bereits in der Konfiguration des System-Tasks und des WebViewer-Exports erwähnt, ist die

alte WebViewer-System-Task-Unterstützung mit dieser Version nicht mehr verfügbar. Wenn noch die alte WebViewer System Task Unterstützung verwendet wird um den WebViewer Export zu nutzen, muss ein neuer System Task erstellt werden.

Behoben

FullClient

- Es muss jetzt auch nach dem Nutzen eines Shortcuts (Default CTRL + ALT + P) ein Grund angegeben werden, wenn dieses Password genutzt wird.
  Keepass import bei korrupter Verfallszeit (ExpiryTime) funktioniert jetzt auch stabil.

Server

- Beim Setzen oder Löschen von temporären Berechtigungen wird nun ein Logeintrag geschrieben.

AdminClient

- Der Password Safe Service wird nun nicht mehr neu gestartet, wenn ein User den AdminClient über das Windows Startmenü ausführt, der diesen zuvor noch nicht gestartet hatte.

OfflineClient

- Nach dem Aktivieren und Deaktivieren der Exportberechtigung im Offline Client und der Synchronisierung wird die Exportberechtigung wie erwartet berücksichtigt.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.8.14.0.27745-de.msi)
`0ae527f62415a0ea9ada8c01b84e76d1a74ea9ba94d49ecc7abb24b1675fbd87fb455126cd4566c3549e4`

Englisches Server Setup (pss8.8.14.0.27745-en.msi)
`78248de00107ded061960780942519586c2326c829504c175cd60244a48f2a8d58f3af600ae5bf316306b`

Deutsches Client Setup (psc8.8.14.0.27745-de.msi)
`0aebbd3234be1691e23f68e0bb569d5430443e5323b2e1f34a849f2d5c1fa142c6d7d9cd5b2d84727e868`

Englisches Client Setup (psc8.8.14.0.27745-en.msi)
`184bc5d62fb3ef9b32a3cde09a0acfaef0d4de7455942ef26ca6ab45a852eaaecd311c2fd3b9cefb20d8c`

Version 8.13.14.27679

Veröffentlichung

29.03.2022

Kompatibilität

Zum AdminClient der Version 8.13.14.27679 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.14.27679
- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.14.27679
- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✱ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Neu

FullClient

- Die Lesbarkeit der Aktionsschaltflächen wurde zum besseren Verständnis in der Navigation / im Ribbon optimiert.

WebClient

- Die Lesbarkeit der Aktionsschaltflächen wurde zum besseren Verständnis in der Navigation / im Ribbon optimiert.

LightClient

- Die Lesbarkeit der Aktionsschaltflächen wurde zum besseren Verständnis in der Navigation / im Ribbon optimiert.

LightClient in der Web-Ansicht

- Die Lesbarkeit der Aktionsschaltflächen wurde zum besseren Verständnis in der Navigation / im Ribbon optimiert.

Änderung

FullClient

- Es wurde zum neuen Yubico-Endpunkt api.yubico.com gewechselt. Die alten APIs api(n).yubico.com werden von Yubico nicht mehr unterstützt.

LightClient

- Es wurde zum neuen Yubico-Endpunkt api.yubico.com gewechselt. Die alten APIs api(n).yubico.com werden von Yubico nicht mehr unterstützt.

Bitte stelle sicher, dass Password Safe Zugriff auf die neue API hat.

Verbesserung

FullClient

- Die Meldungen während eines Keepass-Imports wurden optimiert.

LightClient in der Web-Ansicht

- Das Erscheinungsbild von leeren Kacheln inklusive Text hinzugefügtem Schlüssellogo wurde verbessert.

Behoben

FullClient

- Benutzer können sich nun mit einem Smartcard-Zertifikat anmelden, wenn es nur den letzten Teil eines Benutzernamens enthält.

> Wir weisen darauf hin, bitte auf Version 8.13.14 upzudaten, wenn Smartcards im Gebrauch sind.

- Bei einer RDP-Sitzung wird bei der Rückkehr in den Fenstermodus das Fenster nicht mehr skaliert.

Server

- System Tasks werden beim Auftreten eines Fehlers angehalten.
- Es wird kein falscher SQL-Verbindungsstring mehr angezeigt, der eine Fehlermeldung erzeugte, wenn ein Backup durchgeführt wurde UND MARS aktiv war.
- Bei Verwendung einer Lizenz auf einem Standby-Rechner im Hybernate-Modus ist die Lizenz auch nach 30 Tagen im Hybernate-Modus wieder gültig.

LightClient

- Benutzer können sich nun mit einem Smartcard-Zertifikat anmelden, wenn es nur den letzten Teil eines Benutzernamens enthält.

LightClient in der Web-Ansicht

- Benutzer können das Benutzerrecht zum Anlegen von Passwörtern unter bestimmten Bedingungen wieder löschen, wenn die Benutzerrechte “Kann individuelle Passwörter über LightClient hinzufügen” UND “Kann persönliche Datensätze anlegen” erteilt wurden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.8.13.14.27679-de.msi)
`5335503d5d1d1ef0703d39a48224766de87d4099541cbe1030cd6af02bb24afa442c77402fb0ad33ddd8e`

Englisches Server Setup (pss8.8.13.14.27679-en.msi)
`a02bd2c7086208620b207c5d4eaf188c212d9839c73aa5817347af9ad664af704de81e5e4ee0bd02defc6`

Deutsches Client Setup (psc8.13.14.27679-de.msi)
`52a5539424440935e8f75eeba4a461183e232920ca30430e856c5c47a6e56becc3e5170f8571cb02fe977`

Englisches Client Setup (psc8.13.14.27679-en.msi)
`d44a00e384dcb1c9347a20c0aab5ef03b831af7b6db2ad08c633e8e7a588a13b8f484f46edb3b2d459b57`

Version 8.13.13.27522

Veröffentlichung

14.03.2022

Kompatibilität

Zum AdminClient der Version 8.13.13.27522 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.13.27522
- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.13.27522
- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✻ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Neu

LightClient in der Web-Ansicht

- Wenn noch keine Passwörter in Password Safe hinterlegt sind, erhalten neue Benutzer Hinweise zu weiteren Aktionen, um sich schneller zurechtzufinden.

Verbesserung

FullClient

- Aktualisierung der integrierten PuTTY-Version auf Version 0.76

LightClient

- Aktualisierung der integrierten PuTTY-Version auf Version 0.76

Behoben

Server

Benutzer von Professional- und MSP-Lizenzen können auch ohne Active Directory-Integration wieder gelöscht werden.

MSP

- Benutzer von Professional- und MSP-Lizenzen können auch ohne Active Directory-Integration wieder gelöscht werden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.13.27522-de.msi)
`02d44733b306c85708dd25fa8b745d3bf3b5e6d29db7e56ab2f1125cef1dc486d27c99249710dabc5514e`

Englisches Server Setup (pss8.13.13.27522-en.msi)
`4622dd0a3bd569ec439457789a6198b310c0703ead111d50857c0f42592328575b8638e8e4f7cf916a006`

Deutsches Client Setup (psc8.13.13.27522-de.msi)
`7f82e162b2fed7f06e682c9cecaf5c2f96c6606dbe1782b42d0bcaad74d4f493690f3381ff356aee5d87a`

Englisches Client Setup (psc8.13.13.27522-en.msi)
`abc3184c3fc65f16d49a41f8628b81cd2fc753897abf39813ea904dad341d8bdc15e11eebadeb67429f0c`

Version 8.13.12.27427

Veröffentlichung

28.02.2022

Kompatibilität

Zum AdminClient der Version 8.13.12.27427 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.12.27427
- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.12.27427
- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✻ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Neu

WebClient

- Im Web können LightClient-Benutzer nun auch die Sprache der Benutzeroberfläche wechseln, ohne hierfür in den FullClient wechseln zu müssen.

Verbesserung

FullClient

- Der RDP-Tab am Desktop zeigt nun auch Informationen wie den Host- und Passwortnamen sowie die IP-Adresse, wenn vorhanden.

Behoben

FullClient

- Beim CSV-Import funktioniert das Kontrollkästchen “Auswahl für die folgenden Passwörter merken” nun auch für die Auswahl “Neu erstellen”.
- Passwörter können wieder am Desktop gespeichert werden, wenn ein Benutzer über den SSO-Agent angemeldet ist.

WebClient

- Die Tag-Auswahl für ein Passwort – gerade bei mehreren hundert Tags – funktioniert jetzt schneller.
- Die Sicherheitsstufe der Einstellungen in den “Globalen Nutzereinstellungen” konnte nicht mehr geändert werden.

Server

- Ein Benutzer konnte keinen AD-Import / Sync mehr starten, auch wenn er weder der Masterkey-Benutzer noch der zusätzliche verantwortliche Benutzer eines AD-Profils war und es gibt keine Fehlermeldung mehr.
- Bei der Umstellung von der oder auf die Sommerzeit werden System Tasks wieder zum richtigen Zeitpunkt ausgeführt.

Android App

- Die Mobile App kann wieder synchronisieren, wenn bei der Verwendung von zwei Organisationseinheiten ein Passwort in eine Einheit verschoben und damit die Rechte überschrieben wurden.

iOS App

- Die Mobile App kann wieder synchronisieren, wenn bei der Verwendung von zwei Organisationseinheiten ein Passwort in eine Einheit verschoben und damit die Rechte überschrieben wurden.*

SSO Agent

- Passwörter können wieder im FullClient am Desktop gespeichert werden, wenn ein Benutzer über den SSO-Agent angemeldet ist.

LightClient in der Web-Ansicht

- Ein Tooltip für die Schaltfläche “Neues Passwort erstellen” wurde hinzugefügt.

- Ein Tooltip für die Listenansicht wurde hinzugefügt.

> Bei dem Update im AppStore handelt es sich um Version 1.26.3, obwohl hier noch Version 1.16.3 angegeben ist. Die Versionsnummer wird mit dem nächsten Update berichtigt.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.12.27427-de.msi)

```
5d6ac7c7b9a42eb09c6b11df33febf3d90140a16c82139abc140c88a31f7bb6b967fb81f28a657f8d96a6
```

Englisches Server Setup (pss8.13.12.27427-en.msi)

```
62894d51ccebb21ce45370628c8e858f322981ee2aeea734b73eb302dea64f6cc30f8ab7554d426766c86
```

Deutsches Client Setup (psc8.13.12.27427-de.msi)

```
65951207888d648d6be2f57a81e887f1a05e17a561a31c913118d228a14062d7334e0f9dee8ae5984ff50
```

Englisches Client Setup (psc8.13.12.27427-en.msi)

```
5d9a05048d2cc250dece4c9117449a32a3dbc76506be08fa986827566508ff7ac0d2aded2dbe1d7e9662c
```

Version 8.13.11.27156

Veröffentlichung

15.02.2022

Kompatibilität

Zum AdminClient der Version 8.13.11.27156 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.11.27156
- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.11.27156
- WebClient Version 8.13.10.26901
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.11 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.10.0.18473 Hotfix 3, sowie das OS **Android 9** bei der mobilen App eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

✻ Das Handling von AD-Profilen wird nur mit den jeweils neuesten Clients unterstützt

Verbesserung

FullClient

- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.

WebClient

- Verbesserte Anzeige des Nutzer-Avatars

- Anzeige einer Rückmeldung an die Nutzer, wenn sie ihren zweiten Faktor hinzufügen/entfernen
- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.
- Verbesserte Performance bei der Entschlüsselung von Passwörtern im WebClient

Server

- Verbesserte Geschwindigkeit des IP-Adressfilters

AdminClient

- Änderungen an der Webserver-Konfiguration sind für Administratoren jetzt besser erkennbar.

Android App

- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.

iOS App

- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.

OfflineClient

- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.

LightClient

- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.

LightClient in der Web-Ansicht

- Die Oberfläche der Kachelansicht wurde benutzerfreundlicher gestaltet.
- Anwendungen, die im WebLightClient nicht verwendet werden können, werden ausgeblendet.
- Verbesserte Anzeige des Nutzer-Avatars
- Vereinfachung der Verknüpfung von Anwendungen in der Ansicht “Bearbeiten/Erstellen”
- Anzeige einer Rückmeldung an die Nutzer, wenn sie ihren zweiten Faktor hinzufügen/entfernen
- Für die Anzeige von Passwörtern im Klartext wurde zur besseren Lesbarkeit die Schriftart „Monotype“ hinterlegt.
- Verbesserte Performance bei der Entschlüsselung von Passwörtern im WebClient

Behoben

FullClient

- Das Ausdrucken einer sehr großen Anzahl von Passwörtern ist jetzt wieder möglich.
- Der DesktopClient stürzt bei der Offline-Synchronisation unter bestimmten Umständen nicht mehr ab.
- Unter Windows 11 konnte der automatische Logout zu einem nicht reagierenden Client führen.

- Der YubiKey konnte im DesktopClient nicht konfiguriert werden, da der Autologout ausgelöst wurde.
- Im AD werden zusätzliche verantwortliche Benutzer beim Speichern nicht mehr gelöscht, wenn der aktuelle Benutzer keine Leseberechtigung dafür hat.
- Verantwortliche Benutzer, die in einem Active Directory-Profil hinterlegt sind, können jetzt nicht mehr gelöscht werden.
- Es wurde behoben, dass Passwörter unter speziellen Bedingungen nicht gespeichert werden konnten.

WebClient

- Das Ausdrucken einer sehr großen Anzahl von Passwörtern ist jetzt wieder möglich.
- Das Benutzerrecht “Kann exportieren” war unter besonderen Umständen für den WebClient nicht deaktiviert.
- Verantwortliche Benutzer, die in einem Active Directory Profil hinterlegt sind, konnten gelöscht werden.

Server

- Zusätzliche verantwortliche Benutzer werden nicht zu den Berechtigungen von Benutzern/Rollen aus diesem Profil hinzugefügt.
- Bei der Verwendung des Modus “Nutzerimport auf Rollenmitglieder beschränken” im AD-Import-Assistenten wird die Exclude List verwendet.
- Verantwortliche Benutzer, die in einem Active Directory Profil hinterlegt sind, konnten gelöscht werden.

Browser-Erweiterung

- Die Verbindung mit dem SSO Agent zur Nutzung der Browser-Erweiterung funktioniert wieder automatisch.

SSO Client

- Die Verbindung mit dem SSO Agent zur Nutzung der Browser-Erweiterung funktioniert wieder automatisch.

LightClient

- Der YubiKey konnte im DesktopClient nicht konfiguriert werden, da der Autologout ausgelöst wurde.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.11.27156-de.msi)

f8b93cebd2637e7409c18f627ea047898ff0bc36d60d62702d96cb9c9865deb019610f43dc8a71ec4ae6f

Englisches Server Setup (pss8.13.11.27156-en.msi)

46d5ac713707e847669e45e9e1a21606a88321be087b3949b73e6f6f3205b6886a8e4f1b81d1e62d6ea59

Deutsches Client Setup (psc8.13.11.27156-de.msi)

046324ebd35615f42f3ddd52d71d2ec9fb46cd07a4a8b69ac307c422853d6d3ba338f9721c756942d34ae

Englisches Client Setup (psc8.13.11.27156-en.msi)

8134cefc9ddc465a31851c0dd429e5c0b3ea44953692479a32f8a1cec85d05ad47217e347344e5d81fc45

Version 8.13.10.26901

Veröffentlichung

17.01.2022

Kompatibilität

Zum AdminClient der Version 8.13.10.26901sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.10.26901
- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.10.xxxxx
- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.9 wurde der Support für die Versionen 8.0.1.19032 bis Version Version 8.9.0.17993 Hotfix 2 eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

Server

- Die Installation des SAML Service ist jetzt optional.

! Kunden, die SAML in Verwendung haben, müssen bei Aktualisierung auf Version 8.13.10 die Installation des SAML Services aktivieren. Andernfalls funktioniert dieser Dienst nicht mehr. Sollte die Installation vergessen werden, erscheint ein entsprechender Hinweis im AdminClient.

AdminClient

Alle durch ein Update deaktivierten Datenbanken können gleichzeitig reaktiviert werden.

LightClient in der Web-Ansicht

- Passwörter können in einer Liste angezeigt werden.

Verbesserung

WebClient

- Die Auswahl von Tags wurde optimiert.

LightClient in der Web-Ansicht

- Der Button zum Anlegen eines neuen Passwortes wurde präsenter positioniert.
- Die Auswahl von Tags wurde optimiert.

Behoben

FullClient

- Der automatische Session Timeout trennt die Verbindung jetzt endgültig
- Eine angepasste Tabellen-Ansicht wird dauerhaft gespeichert.
- Der Filter für Logbuch Einträge zeigt bei einem Report die korrekten Ergebnisse an.
- Restriktive Benutzer können keine Passwörter ändern.
- Es werden Hinweise beim CSV Import eingeblendet, wenn ein Benutzer trotz fehlender Berechtigung Organisationseinheiten anlegen will.
- Es werden auch CSV Dateien, die Datensätze mit Anführungszeichen enthalten, importiert.
- Der Freigabeprozess für ein Siegel funktioniert auch, wenn zwei Benutzer das Siegel freigeben müssen.

WebClient

- Restriktive Benutzer können keine Passwörter ändern.
- Der Freigabeprozess für ein Siegel funktioniert auch, wenn zwei Benutzer das Siegel freigeben müssen.

AdminClient

- Nach dem Update auf Version 8.13.9 konnten Offline-Lizenzen nicht mehr aktiviert werden.

Browser-Erweiterungen

- Neu erkannte Zugangsdaten werden wieder korrekt in den WebClient übertragen.
- Wenn die Systemsprache nicht deutsch oder englisch ist, wird englisch verwendet.

LightClient

- Der automatische Session Timeout trennt die Verbindung jetzt endgültig

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.10.26901.msi)

feb423403492910afc57f774e788621177526bacec64f01ae100ffe77756fe7423846355893cd493ff361

Englisches Server Setup (pss8.13.10.26901-en.msi)

5120058ad9a6b6a44842fa2d59ae92e7d736e82fe078da77adb54dcd86a91ddb3093374c7effdd3323434

Deutsches Client Setup (psc8.13.10.26901-de.msi)

db66f4ef3d4874bc73e34d9f1ff664dcb446ef4f4f853beb6c3f9c7d65879f5e47d82f7039155794ba6c5

Englisches Client Setup (psc8.13.10.26901.msi)

fff957f3eff180cbdb7413ed8bdfaf6624999955d25ae1043acb0fd68f0c828755abd79f355d0331cf77d

Version 8.13.9.26689

Veröffentlichung

20.12.2021

Kompatibilität

Zum AdminClient der Version 8.13.9.26689 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.9.26689
- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.9.26689
- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.9 wird der Support für die Versionen 8.0.1.19032 bis Version Version 8.9.0.17993 Hotfix 2 eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient

- Bei aktiviertem Auto-Login wird nach erstmaliger Eingabe eines neuen Passwortes dieses automatisch gespeichert.

Server

- Die Installation ist auch ohne Konfiguration einer SMTP Verbindung möglich.

LightClient in der Web-Ansicht

- Benutzer können den Siegelfreigabeprozess starten und nach Bestätigung ein Siegel brechen.

Verbesserung

FullClient

- Das Wechseln eines Formulars bei mehreren, unterschiedlichen Passwörtern wurde verbessert.
- Die Bibliotheken für die Verwendung von Smartcards als erster Faktor wurden aktualisiert.

Server

- Die für die Verschlüsselung der Daten auf dem HSM verwendeten Bibliotheken wurden aktualisiert.

> ! Benutzer eines Hardware Sicherheitsmoduls werden gebeten, die aktuelle Version zuerst auf einem Testsystem zu installieren.

Browser-Erweiterungen

- Das Eintragen von Zugangsdaten in die entsprechenden Felder wurde verbessert.
- Der Standardwert für die (globale) Benutzereinstellung “Loginmasken automatisch absenden” wurde auf aktiviert gesetzt und die Sicherheitsstufe auf 3 erhöht. Dies betrifft nur Datenbanken, die zukünftig angelegt werden.

mobile Apps

- Es wurden Benachrichtigungen integriert, die den Benutzer daruf hinweisen, warum ein aktivierter zweite Faktor unter Umständen nicht abgefragt wird.

Behoben

FullClient

- Der Ordner „_archived“ im AD lässt sich wieder über den Import Assistenten aufrufen.
- Die Inhaltssuche wird auch auf E-Mail-Felder angewendet.
- Die Anzahl bei wievielen Passwörtern ein Tag verwendet wird beinhaltet auch die im Papierkorb befindlichen Passwörter.
- In der Historie eines Datensatzes wird auch der Benutzername eines Active Directory Benutzers statt nur dessen ID angezeigt.
- Mit einem Password verlinkte, lokal gespeicherte .ppk Schlüssel-Dateien können für SSH Verbindungen verwendet werden.

WebClient

- Der Ordner „_archived“ im AD lässt sich wieder über den Import Assistenten aufrufen.
- Die Inhaltssuche wird auch auf E-Mail-Felder angewendet.
- Die Anzahl bei wievielen Passwörtern ein Tag verwendet wird beinhaltet auch die im Papierkorb befindlichen Passwörter.
- In der Historie eines Datensatzes wird auch der Benutzername eines Active Directory Benutzers statt nur dessen ID angezeigt.

Server

- Die Meldungen an den Syslog Server werden auch übertragen, wenn dieser über TCP mit Password Safe verbunden ist.
- Der IP-Filter für Zweifaktorauthentifizierung funktioniert nun bei allen Clients, auch wenn bei einem Benutzer die Einstellung “Benötigt zweiten Faktor” aktiviert ist.
- Im Logbuch werden auch im WebClient vorgenommene Änderungen eines Objekts gespeichert

Browser-Erweiterungen

- Passwörter können – wenn diese Option aktiviert ist – nicht ohne Angabe eines Grundes in die Zwischenablage kopiert werden

SSO Client

- Bei aktivierter clientübergreifender Anmeldung wird nach dem Login im DesktopClient das verwendete Profil auch im SSO Agent angezeigt.

LightClient in der Web-Ansicht

- Beim Erstellen eines Passwortes können weitere Benutzer berechtigt werden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.9.26689-de.msi)
`c16c67d226a18f05fffcefa5681d64dba67fcbe86484667b6417ddf0f2d392ab4a200a35c0d12ed2af9b4`

Englisches Server Setup (pss8.13.9.26689-en.msi)
`11624ca1aeecffcdf02670d4361d2c7a4a4f175fe06acec299b2509667bd434a44ad86e1c3e12171e35ea`

Deutsches Client Setup (psc8.13.9.26689-de.msi)
`aa3ea99e70520eb77872e354f18b4fe5ef6c2424bb14fac25831d9c888b1f34f7c519158878d0d309ae7f`

Englisches Client Setup (psc8.13.9.26689-en.msi)
`5bd9fb8c456584b35c368ab0dca62df9f93f1246c0d53abe381e238b99d6898162f8bef03919b71a7a08d`

Version 8.13.8.25983

Veröffentlichung

02.12.2021

Kompatibilität

Zum AdminClient der Version 8.13.8.25983 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.8.25983
- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.8.25983
- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Behoben

Benutzer, die temporär auf ein Objekt berechtigt waren, konnten dieses Objekt nach Ende der Berechtigung weiterhin sehen jedoch nicht mehr auf die Inhalte zugreifen.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.8.25983-de.msi)

```
4de754247c1f22bea5e12ea4725bb0145d1d2864f1d5097d979e222b546da0adb7608406c3e3a6222f759
```

Englisches Server Setup (pss8.13.8.25983-en.msi)

```
59f2af1735b0e9ec51ed5ace144fb119ed08fc8c972603ba17ce37792576923d221d148d8ebd3ff420da2
```

Deutsches Client Setup (psc8.13.8.25983-de.msi)

```
7676b976e084d899ffce2eb5abc50321c49aa322e56f724f8af1f1cdc8551c53f4a1e14aef6c532bcc6d0
```

Englisches Client Setup (psc8.13.8.25983-en.msi)

```
425a99283fa667554ec1909a4b2a7783a49341ba5ffc24caeee980ea8df48f5fd16683f0f4133572f5461
```

Version 8.13.7.25979

Veröffentlichung

25.10.2021

Kompatibilität

Zum AdminClient der Version 8.13.7.25979sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.7.25979
- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.7.25979
- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

> ! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

LightClient und LightClient in der Web-Ansicht

- Benutzer können zusäzlich hinzugefügte Felder bearbeiten oder löschen.

Verbesserung

FullClient

- Beim Import einer CSV Datei wird diese automatisch auf die verwendete Kodierung überprüft.
- Passwörter können aus der Bearbeiten-Ansicht in den Papierkorb verschoben werden.

WebClient

- Passwörter können aus der Bearbeiten-Ansicht in den Papierkorb verschoben werden.

LightClient und LightClient in der Web-Ansicht

- Passwörter können aus der Bearbeiten-Ansicht in den Papierkorb verschoben werden.

AdminClient

- Es können jetzt auch PKI-Zertifikate ohne ‘KeyEncipherment’-Flag als zweiter Faktor verwendet

werden.

Behoben

FullClient

- Es können auch One-Time-Passwörter ohne Geheimnis angelegt werden.
- Die Berechtigungen können jetzt auch wieder mittels einer Vorlage reduziert werden.

Server

- Die Meldung im Fall einer fehlenden Verbindung zum SQL-Server wurde angepasst.

AdminClient

- Die Meldung im Fall einer fehlenden Verbindung zum SQL-Server wurde angepasst.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.7.25979-de.msi)
`6f30f9f0989ad541ecf0da2971ce3adbb0d474e06bc7ccc8c80220666a09a43ace40abd064598da438823`

Englisches Server Setup (pss8.13.7.25979-en.msi)
`ea6c16721fc2db12f88478783922e767dfaa463f88e7a55beaff4b3dc07391e995344627c31acb34e3124`

Deutsches Client Setup (psc8.13.7.25979-de.msi)
`fe1f4e7d331691a5683463550fc024c5e6e70a45b8a912befec4af822618485009117f5c45efda37badda`

Englisches Client Setup (psc8.13.7.25979-en.msi)
`fb7d6660a05d6550b980ee0214f4b7ad3ab3afea14fdf8de2904caade5009e4de3412cc9f9a75a7584b61`

Version 8.13.6.25933

Veröffentlichung

11.10.2021

Kompatibilität

Zum AdminClient der Version 8.13.6.25933 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.6.25933
- Windows Client Version 8.13.5.25731

- WebClient Version 8.13.6.25933
- WebClient Version 8.13.5.25731

> ! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient

- Deaktivierte Benutzer werden nur noch im Modul Organisationseinheiten angezeigt

WebClient

- Deaktivierte Benutzer werden nur noch im Modul Organisationseinheiten angezeigt

LightClient und LightClient in der Web-Ansicht

- Beim Anlegen eines Passworts können Benutzer aus verschiedenen Formularen auswählen und zusätzliche Felder hinzufügen.

MSP

- Der Datenbankname ist bei jedem Kunden dauerhaft sichtbar.
- Deaktivierte Benutzer werden ab dem Folgemonat nicht mehr berechnet.

Verbesserung

LightClient in der Web-Ansicht

- Das Suchfeld als auch die Suchergebnisse können über einen Button zurückgesetzt werden.
- Das Hinzufügen neuer Tabs wurde intuitiver gestaltet.

- Der Tab “alle Passwörter” wird per default immer angezeigt.

Behoben

FullClient

- Der Password Reset funktioniert auch mit dem https:// Protokoll.
- Active Directory Benutzer im Ende-zu-Ende Modus werden nur bei funktionierender SMTP Verbindung importiert.
- Das Versiegeln eines Passwortes wurde beschleunigt.
- Die Schnell- als auch die Filtersuche zeigt alle Objekte an, die den Suchbegriff enthalten
- Eine RDP Verbindung im separaten Fenster kann mittels des “Schließen” Buttons beendet werden.

WebClient

- Wenn ein Benutzer zum Ändern seines Passwortes aufgefordert wird, greift eine vorhandene Passwortrichtlinie.
- Bei deaktiverter Benutzereinstellung “Tab nach dem Öffnen bearbeiten” fehlten im Menü eines Passwortfeldes einige Optionen.
- Active Directory Benutzer im Ende-zu-Ende Modus werden nur bei funktionierender SMTP Verbindung importiert.
- Das Versiegeln eines Passwortes wurde beschleunigt.
- Die Schnell- als auch die Filtersuche zeigt alle Objekte an, die den Suchbegriff enthalten

Android App

- Die Synchronisation funktioniert jetzt auch ohne Realtime-Verbindung.

iOS App

- Die Synchronisation funktioniert jetzt auch ohne Realtime-Verbindung.

API

- Passwörter werden von dem JavaScript SDK verschlüsselt übertragen.

MSP

- Trotz aktivierter Option konnten keine Automatischen Reports erstellt werden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.6.25933-de.msi)
`15972f7ca3bd6f535599cc587c21b8132a3bab5171d4f05f7ad09e4a2c216d61aa87bf066a8316487efc3`

Englisches Server Setup (pss8.13.6.25933-en.msi)
`71beba69780646aead27a8e20315768dfb73c205493f4ed7a84214e13796fc877385acc4d9251625841a2`

Deutsches Client Setup (psc8.13.6.25933.msi)

1017e3e794bdc70f44492cc28d63a99a8175cc766c5e352ea6693eb9110f52ef575a6a4e3871abf57c925

Englisches Client Setup (psc8.13.6.25933-en.msi)

6a3db708f9e87ddc88a014dce6c6b15ed84b889b9672f3b1ebe9698188f6cebb8006940919190965bc59a

Version 8.13.5.25731

Veröffentlichung

13.09.2021

Kompatibilität

Zum AdminClient der Version 8.13.5.25731 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.5.25731
- WebClient Version 8.13.5.25731

> ! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient

- Es ist möglich, sich Berichte über die Änderungen durch Active Directory Importe generieren zu lassen.
- Die Funktion “Letzte X Passwörter ausschließen” wurde bei den Passwortrichtlinien entfernt.
- Der Loginprozess wurde angepasst, um es möglichen Angreifern zu erschweren, gültige Benutzernamen zu erraten.
- Benutzer können nur Passwörter duplizieren, wenn sie auch auf das entsprechende Formular berechtigt sind.
- Beim Anlegen eines neuen AD Profils sind die beiden Flags “Secure” und SecureSocketsLayer” per default aktiviert.
- Active Directory Objekte können jetzt einfach mittels Zugehörigkeit zu einer Gruppe in Password Safe angelegt oder gelöscht werden.
- In den Email-Benachrichtigungen wird die Organisationseinheit, in der sich das Secret befindet, mit angegeben.
- Der Tab mit der Listenansicht in jedem Modul kann nicht geschlossen werden.

WebClient

- Der Loginprozess wurde angepasst, um es möglichen Angreifern zu erschweren, gültige Benutzernamen zu erraten.
- Das Öffnen und Schließen des Filters wurde optimiert und die mobile Ansicht angepasst.
- Benutzer können nur Passwörter duplizieren, wenn sie auch auf das entsprechende Formular berechtigt sind.
- Es wurde eine Direktsuche nach Active Directory Objekten integriert

- Active Directory Objekte können jetzt einfach mittels Zugehörigkeit zu einer Gruppe in Password Safe angelegt oder gelöscht werden.
- In den Email-Benachrichtigungen wird die Organisationseinheit, in der sich das Secret befindet, mit angegeben.
- Der Tab mit der Listenansicht in jedem Modul kann nicht geschlossen werden.

Server

- TLS 1.2 und 1.3 sind die beiden Standardversionen für die verschlüsselte Übertragung.
- Wenn ein Benutzer sein Passwort ändert, werden alle noch offenen Sessions automatisch beendet.
- Der Discovery Service Scan wurde optimiert.
- Password Safe ist jetzt DualStack fähig.

AdminClient

- Die Länge einer aktiven Session kann jetzt für jeden Client individuell eingestellt werden.

LightClient

- Der Loginprozess wurde angepasst, um es möglichen Angreifern zu erschweren, gültige Benutzernamen zu erraten.

LightClient in der Web-Ansicht

- Der Loginprozess wurde angepasst, um es möglichen Angreifern zu erschweren, gültige Benutzernamen zu erraten.

Verbesserung

FullClient

- SSH Verbindungen mittels einer Schlüsseldatei sind einfacher zu konfigurieren.

Browser-Erweiterungen

- Bei aktiviertem IP Filter wird ein etwaiger zweiter Faktor nicht mehr abgefragt.

Behoben

FullClient

- Das Standardformular kann in den globalen Benutzereinstellungen zurückgesetzt werden.
- Der DesktopClient verhindert nur bei ungespeicherten Änderungen das Herunterfahren von Windows.
- Das Widget “Mein Team” zeigt im Dashboard alle Mitglieder der ausgewählten Organisationsheinheit an.
- Es wurde ein Übersetzungsfehler im Report “Logbucheinträge” korrigiert
- RDP Sessions im externen Fenster können auch in Fullscreen dargestellt werden.
- Beim Import von Passwörtern ist nur der Benutzer selbst auf die Passwörter berechtigt.
- Die Tastaturkürzel funktionieren wieder in RDP-Sessions.

- Die client-übergreifende Anmeldung funktioniert wieder.
- Die Authentifizierung mittels Kerberos ist wieder möglich.
- Benachrichtigungen können nur von dem Benutzer gesehen werden, der sie konfiguriert hat.

WebClient

- Das Standardformular kann in den globalen Benutzereinstellungen zurückgesetzt werden.
- Das Formular eines bestehenden Passwortes kann nur mit dem Recht “Berechtigen” oder “Löschen” gewechselt werden.
- Die Qualität eines Passwortes wird beim Wechsel des Formulares erneut überprüft.
- Der Export von Passwörtern oder Organisationseinheiten wurde optimiert.
- Bei der Auswahl möglicher Formulare zum Erstellen eines Passwords kann man mittels einer Scrollbar durch die Formulare navigieren.
- Beim AD Import werden bei der Selektion eines Objektes ebenfalls alle Unterobjekte selektiert und anschließend synchronisiert.
- Die Authentifizierung mittels Kerberos ist wieder möglich.
- Der Link zum Add-on Store des Firefox verwendet jetzt das https:// Protokoll
- Benachrichtigungen können nur von dem Benutzer gesehen werden, der sie konfiguriert hat.

AdminClient

- Der Name einer Datenbank kann auch einen Bindestrich enthalten.

AdminClient

- Im MSSQL Server Management Studio gelöschte Datenbanken werden im AdminClient deaktiviert.

Browser-Erweiterungen

- Die Anmeldung über den SSO Agent funktioniert bei entsprechender Konfiguration der Browser Erweiterung.
- Die automatische Eintragung über den SSO Agent wurde beschleunigt.

SSO Client

- Die client-übergreifende Anmeldung funktioniert wieder.
- Die automatische Eintragung über den SSO Agent wurde beschleunigt.

LightClient

- Die Authentifizierung mittels Kerberos ist wieder möglich.

LightClient in der Web-Ansicht

- Im Passwortgenerator stehen – sofern welche konfiguriert wurden – die entsprechenden Passwort-Richtlinien zur Auswahl.
- Benutzer mit exklusiver LightClient Lizenz können Passwörter in andere Organisationseinheiten verschieben
- Die Authentifizierung mittels Kerberos ist wieder möglich.
- Benutzer mit ausschließlicher LightClient Lizenz können Passwörter mit Tags versehen.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.5.25731-de.msi)

```
56cb7260d587d50afceca87ef53772c3106ec192de88695b247495022c768e03ac9a6a4e5e273f74c98d4
```

Englisches Server Setup (pss8.13.5.25731-en.msi)

```
05fb18e29549b94f8b238cbe1904d44240af7bcd48a802d64ea9bb50d6e9149daffc46ceae942771de772
```

Deutsches Client Setup (psc8.13.5.25731.msi)

```
cd4a82995f45d19d1d4aa306025e296b1142fbd74c0da1ffbd2b8a3078ffeb9a58bbcb86f732d9f411c5f
```

Englisches Client Setup (psc8.13.5.25731-en.msi)

```
473ef56a4d9f1cf12800437bdf869cbf7a5b4993079f9cd401206344c07285838c02e75d108f68fa62de1
```

Version 8.13.4.25228

Veröffentlichung

16.08.2021

Kompatibilität

Zum AdminClient der Version 8.13.4.25228 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.4.25228
- Windows Client Version 8.13.3.25194
- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.4.25228
- WebClient Version 8.13.3.25194
- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

> ! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

LightClient in der Web-Ansicht

- In der Schnellansicht werden auch die TAGs angezeigt.

Verbesserung

FullClient

- SSH Verbindungen mittels einer Schlüsseldatei sind einfacher zu konfigurieren.

Behoben

FullClient

- Siegel-Vorlagen können auch dann bearbeitet werden, wenn eine am Siegelprozess beteiligte Rolle gelöscht wurde.
- Die Suche sucht wieder nach dem exakten Begriff. Die unscharfe Suche nach ähnlich lautenden

Begriffen kann beim Filter aktiviert werden.

WebClient

- Mitglieder eine Rolle konnten ein Siegel nicht freigeben.
- Siegel-Vorlagen können auch dann bearbeitet werden, wenn eine am Siegelprozess beteiligte Rolle gelöscht wurde.
- Die Suche sucht wieder nach dem exakten Begriff. Die unscharfe Suche nach ähnlich lautenden Begriffen kann beim Filter aktiviert werden.

MSP

- Der Name einer Datenbank kann auch einen Bindestrich enthalten.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.4.25228-de.msi)
`90f932af037b681a321725bc3b94608dfd85e7df6f980cd223c66ef0f0499d08b88bbd41f352e81467002`

Englisches Server Setup (pss8.13.4.25228-en.msi)
`b66c1eebb79ca081239b0454f85310089d4ea98b5b96aa8c67eb65c7a831fd54b1f1933b3a55d30777113`

Deutsches Client Setup (psc8.13.4.25228.msi)
`57e088a311882770b1b71f561ac5b5712fc8e225a7d5b05beb29d894932089312718e1226c0084827eb06`

Englisches Client Setup (psc8.13.4.25228-en.msi)
`945e7f4c0a82a50fcb1d398a6039a67ea74b1382be49fb558737234ba697bbaff9d040f0387bc9060623f`

Version 8.13.3.25194

Veröffentlichung

02.08.2021

Kompatibilität

Zum AdminClient der Version 8.13.3.25194 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.3.25194
- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.3.25194
- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

> ! Mit Version 8.13.0 wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Behoben

FullClient

- Der QR Code für die Einrichtung des zweiten Faktors wird korrekt angezeigt.
- In der Übersicht des Active Directory Imports werden auch alle verschachtelten Gruppen angezeigt.
- Password Safe prüft die Gültigkeit des Server-Zertifikats wieder korrekt
- Die Überprüfung der Berechtigungen beim Bearbeiten von Passwörtern und Formularen wurde optimiert.

WebClient

- Beim Abwählen von Gruppen in der Übersicht des Active Directory Imports werden auch alle darunterliegenden Objekte abgewählt.
- In der Übersicht des Active Directory Imports werden auch alle verschachtelten Gruppen angezeigt.
- Der Doppelklick auf ein Dokument startet den Download dieses Dokuments.
- Die Überprüfung der Berechtigungen beim Bearbeiten von Passwörtern und Formularen wurde optimiert.

Server

- Der Anwendungsserver stürzt nicht ab, wenn der IDP Server nicht gestartet werden konnte.

Browser-Erweiterungen

- Bei aktivierter Browser Erweiterung wird der interne Passwordmanager des Browsers deaktiviert.

> ! Nach dem Update auf die aktuellste Version der Browser-Erweiterung erscheint der Hinweis “Akzeptieren Sie die neuen Berechtigungen, um die Erweiterung wieder zu aktivieren”. Durch Bestätigen wird der interne Passwordmanager deaktivert und die Browser-Erweiterung kann wieder genutzt werden.

mobile Apps

- Das Feld zum Eintragen eines OTP verschwindet nicht mehr beim Wechsel zu einer Authenticator App.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.3.25194-de.msi)
`763c7cc99f131083d74427c67b817aa867e7934c8620bc255efbc5682e6f6baf43b0050f2f3db26f59903`

Englisches Server Setup (pss8.13.3.25194-en.msi)
`fed9f56f15527aa0e7ba78be13c2a13b9fc32047bab78eeb64bb61656ee611e23ed23f6d8b2d8a8b3f8ad`

Deutsches Client Setup (psc8.13.3.25194.msi)
`1f339736e763fb50235aa4328110a3b022f4b22e9ad51c9894aca60fe10154f08f9242845ce6848474279`

Englisches Client Setup (psc8.13.3.25194-en.msi)
`af6c13f9910d5b6f5bc9bc499c1673878d5825cfed3dee953d8b05c2c3491a68f3b012948334416ead64d`

Version 8.13.2.25151

Veröffentlichung

05.07.2021

Kompatibilität

Zum AdminClient der Version 8.13.2.25151 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.2.25151
- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.2.25151
- WebClient Version 8.13.1.25117
- WebClient Version 8.13.0.25027

> ! Mit diesem Release wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient und WebClient

- Die Berechtigungen von DB-Admins auf ein Passwort bleiben bestehen, wenn das Passwort durch einen normalen Benutzer verschoben wird.

Behoben

FullClient

- Active Directory Benutzer können auch ohne hinterlegte E-Mail-Adresse imporiert werden.

WebClient

- Active Directory Benutzer können auch ohne hinterlegte E-Mail-Adresse imporiert werden.
- Nach der Anmeldung am WebClient über die Browser-Erweiterung konnte ein Benutzer sein Passwort nicht ändern.

Server

- Die clientübergreifende Anmeldung funktioniert wenn sowohl IP-Adressen als auch DNS Einträge als altenative Antragssteller im Verbindungszertifikat hinterlegt sind.

AdminClient

- Eine Datenbank kann auch aktiviert werden, wenn die Collation des SQL Server Groß- und Kleinschreibung beachtet.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.2.25151-de.msi)
`8c2d446692aaf2c42643aacfa930202adb12040c38d7c24a48ee6013346539e1058f40d48bee0ac89e0c2`

Englisches Server Setup (pss8.13.2.25151-en.msi)
`e06926d06dc961a100f524aa9be1f0923e47b03ec4e3ffa43baa7d43bdf9b4052a20bd317926f25a4574b`

Deutsches Client Setup (psc8.13.2.25151.msi)
`8b50af0a5250d18f3434f72a32c5daa0d51d4eeae0fba0031daf4c58d4b38c91f2b8503aa10aa10524283`

Englisches Client Setup (psc8.13.2.25151-en.msi)
`e06926d06dc961a100f524aa9be1f0923e47b03ec4e3ffa43baa7d43bdf9b4052a20bd317926f25a4574b`

Version 8.13.1.25117

Veröffentlichung

21.06.2021

Kompatibilität

Zum AdminClient der Version 8.13.1.25117 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.1.25117

- WebClient Version 8.13.1.25027
- WebClient Version 8.13.0.25117

> ! Mit diesem Release wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient und WebClient

- Für die Anbindung des Active Directory können weitere Verbindungseinstellungen (AuthenticationTypes Enumeration) verwendet werden
- Die vordefinierten Werte einiger Standardeinstellungen wurden angepasst. Folgende Änderungen werden nur bei neuen Datenbanken aktiv.
  - “Website-Icon automatisch herunterladen” wurde von inaktiv auf aktiv gesetzt.
  - “Dokumentenhistorie” wurde von inaktiv auf aktiv gesetzt.
  - “Untergeordnete Organisationseinheiten in LightClient einschließen” wurde von inaktiv auf aktiv gesetzt.
  - “Ersteller aus den Berechtigungen bei neuen Objekten entfernen, wenn der erstellende Benutzer über eine Rolle berechtigt wird” wurde von inaktiv auf aktiv gesetzt.
  - “Browser Addons: Exakte Domainprüfung” wurde von inaktiv auf aktiv gesetzt.
  - “Kann indivituelle Passwörter im LightClient anlegen” wurde von inaktiv auf aktiv gesetzt.
  - “Benachrichtigungsmodul anzeigen” wurde von inaktiv auf aktiv gesetzt.
  - Sicherheitsstufe für “Datensätze als bald ablaufend anzeigen, wenn deren Resttage kleiner sind als” wurde auf Stufe 1 gesenkt.
  - Sicherheitstufe für “Standard-Formular” wurde auf Stufe 1 gesenkt.
  - Sicherheitsstufe für “Anpassbarer Fenstertitel” wurde auf Stufe 5 erhöht.
  - Sicherheitsstufe aller Berechtigungen in der Kategorie “Fußbereich” wurde auf Stufe 5 erhöht.
  - “Gültigkeit in Tagen der mobilen Datenbank ohne Synchronisation” wurde auf 7 Tage reduziert.

    - “Maximale Größe in MB” wurde von 100 auf 10 reduziert.
- Die vordefinierten Werte einiger Standardeinstellungen wurden angepasst. Folgende Änderungen werden sowohl bei neuen als auch bei bestehenden Datenbanken aktiv.
    - “Kann Filter-Negierung verwenden” wurde von inaktiv auf aktiv gesetzt und aus den Einstellungen entfernt.
    - Das Modul “Fußbereich” wurde bei den globalen Benutzereinstellungen entfernt.
    - “Benutzerfeld nach dem Hinzufügen leeren” wurde von aktiv auf inaktiv gesetzt und aus den Einstellungen entfernt.
    - “Berechtigungssuche: Schrittweise hinzufügen” wurde von aktiv auf inaktiv gesetzt und aus den Einstellungen entfernt.
    - “Zwischenablage beim Minimieren löschen” wurde von aktiv auf inaktiv gesetzt und aus den Einstellungen entfernt.
    - Die Benutzereinstellung “Browser Addons: Passwort anzeigen” befindet sich jetzt bei den Passwort-Einstellungen

Behoben

FullClient

- Benutzer, die ihm aktivierten LDAP Filter nicht angezeigt werden, werden bei der Synchronisation automatisch gelöscht.
- Die Überprüfung von mit einem Password Reset verbundenen Passwörtern funktionierte aufgrund einer Code-Anpassung in Version 8.13 nicht mehr.
- Einige Benutzer konnten sich mit dem Verweis auf “Ein Element mit dem gleichen Schlüssel wurde bereits hinzugefügt” nicht anmelden.

WebClient

- Benutzer, die ihm aktivierten LDAP Filter nicht angezeigt werden, werden bei der Synchronisation automatisch gelöscht.
- Die Überprüfung von mit einem Password Reset verbundenen Passwörtern funktionierte aufgrund einer Code-Anpassung in Version 8.13 nicht mehr.

Server

- Benutzerdefinierte Skripte für den Password Reset verwenden jetzt SecureString als CredentialPassword.

AdminClient

- Der Login am AdminClient funktioniert auch, wenn ’0.0.0.0’ (IPv4) bzw. ‘::0’ (IPv6) als IP Adresse eingetragen wurde.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.1.25117-de.msi)
`eaad17bd5ff3639dd330e544d2c7e044c2efabdc3334ca3c3551f51e8fbb8574a8f2239e9fa5a4a64ef6f`

Englisches Server Setup (pss8.13.1.25117-en.msi)

0eb35d304cf446f910edec4c40bc709642d77149f191797eff8c5f7d2bf2f5065b140062b1c72fa968c21

Deutsches Client Setup (psc8.13.1.25117.msi)

32993a01592a56eb2be8c41690438c778aa28d14d4acdce00f447b2b5c9d1f42be3f67c235a957a321b13

Englisches Client Setup (psc8.13.1.25117-en.msi)

434d269289d730125026c1989799abdcc5d0b7eb6ea3c882f7956872c9059ccb215a1c0a711a582f3b11d

Version 8.13.0.25027

Veröffentlichung

14.06.2021

Kompatibilität

Zum AdminClient der Version 8.13.0.25027 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.13.0.25027
- WebClient Version 8.13.0.25027

> ! Mit diesem Release wird der Support für die Versionen 8.0.1.19032 bis Version 8.6.0.15386 Hotfix eingestellt. Wir bitten Kunden, die eine der genannten Versionen noch im Einsatz haben, diese zu aktualisieren. Nur so können wir für die nötige Sicherheit von Password Safe garantieren.

Neu

FullClient

- Es wurde eine neue grafische Oberfläche “Office 2019 Colorful” hinzugefügt.
- Mit einem Dokument verlinkte Passwörter werden im Footerbereich des Dokuments angezeigt.
- Es gab grafische Anpassungen an der Oberfläche.
- In den Papierkorb verschobene Passwörter können endgültig gelöscht werden.
- In den Papierkorb verschobene Passwörter können wieder hergestellt werden.
- Gelöschte Passwörter werden jetzt in einen Papierkorb verschoben.
- Die geöffneten Tabs werden jetzt eindeutiger gekennzeichnet.
- Dokumente können über das Modul “Dokumente” mit Passwörtern verlinkt werden.
- Der Benutzer kann in seinem Konto auf einen Blick sehen, mit welchen Geräten er angemeldet ist.
- Die Hinweismeldungen wurden verbessert.

WebClient

- Es wurden neue Config Headers für den Webserver implementiert.
- Die Benachrichtigungen im Siegelprozess verlinken zur Siegelansicht des betreffenden Passwortes.
- Wenn eine Notification ausgewählt wird, öffnet sich ein neuer Tab mit detaillierten Informationen.
- In der Listenansicht im Modul “Organisationseinheiten” wird die Anzahl der ausgewählten Datensätze angezeigt.
- Mit einem Dokument verlinkte Passwörter werden im Footerbereich des Dokuments angezeigt.
- Die Passwörter können im WebViewer alphabetisch und nach Änderungsdatum sortiert werden.
- Das Mailing für eine Siegelanfrage enthält einen Link zur Siegelübersicht.
- In den Papierkorb verschobene Passwörter können endgültig gelöscht werden.

- In den Papierkorb verschobene Passwörter können wieder hergestellt werden.
- Gelöschte Passwörter werden jetzt in einen Papierkorb verschoben.
- Die geöffneten Tabs werden jetzt eindeutiger gekennzeichnet.
- Dokumente können über das Modul “Dokumente” mit Passwörtern verlinkt werden.
- Der Benutzer kann in seinem Konto auf einen Blick sehen, mit welchen Geräten er angemeldet ist.
- Die Hinweismeldungen wurden verbessert.

Server

- Es wurden neue Config Headers für den Webserver implementiert.
- Benutzer, die im Active Directory gelöscht werden, werden bei der nächsten Synchronisation auch in Password Safe gelöscht.
- Active Directory Objekte, die nicht importiert werden können, sind bei der Konfiguration des Active Directory Imports ausgegraut.
- Active Directory Benutzer können sich auch mit ihrem “User Principal Name” an Password Safe anmelden.
- Es wurde ein neuer Logbucheintrag “wiederhergestellt” für Passwörter integriert.
- Beim Anlegen von neuen Benutzern muss eine Passwort-Richtlinie beachtet werden.
- Wird ein Benutzer deaktiviert oder gelöscht, werden alle noch etwaigen offenen Verbindungen geschlossen.
- Der Benutzername gelöschter Benutzer wird weiterhin im Logbuch angezeigt.
- QR Codes für MFA werden innerhalb von Password Safe generiert.

AdminClient

- In der Liste der Datenbankbenutzer wird beim Mouse over ein Tooltipp angezeigt, um welche Art von Benutzer es sich handelt.
- Beim Anlegen einer Datenbank muss für den Datenbank Administrator eine E-Mail-Adresse hinterlegt werden.

Browser-Erweitrung

- Das Icon der Browser-Erweiterung zeigt an, wenn der Benutzer abgemeldet ist.

Android App

- Die Log files können bei Problemen über andere Apps geteilt werden.

iOS App

- Die Log files können bei Problemen über andere Apps geteilt werden.

SSO Client

- Ist ein Benutzer bei einer Datenbank angemeldet und er wählt diese im Dropdown aus, erscheint keine Loginmaske sondern ein Hinweis, dass er bereits angemeldet ist.

OfflineClient

- Es kann nach Organisationseinheiten gesucht und sortiert werden.

LightClient

- In den Papierkorb verschobene Passwörter können endgültig gelöscht werden.
- In den Papierkorb verschobene Passwörter können wieder hergestellt werden.
- Gelöschte Passwörter werden jetzt in einen Papierkorb verschoben.
- Die Hinweismeldungen wurden verbessert.

LightClient in der Web-Ansicht

- Es können die Details eines Passwortes angezeigt werden.
- In den Papierkorb verschobene Passwörter können endgültig gelöscht werden.
- In den Papierkorb verschobene Passwörter können wieder hergestellt werden.
- Gelöschte Passwörter werden jetzt in einen Papierkorb verschoben.
- Die Hinweismeldungen wurden verbessert.

MSP

- Im AdminClient wurde eine Kundenverwaltung integriert.
- In der Kundenverwaltung können Testkunden angelegt, verwaltet, deaktiviert als auch gelöscht werden.
- Für jeden Kunden kann die Anzahl der verfügbaren Lizenzen individuell eingestellt werden.
- In der Kundenverwaltung können Kunden angelegt, verwaltet, deaktiviert als auch gelöscht werden.
- Für jeden Kunden können zusätzliche Optionen individuell hinzugefügt werden.
- Es wurde ein Dashboards integriert für Informationen über aktive Lizenzen und gebuchte Optionen inklusive der daraus resultierenden Kosten für jeden Kunden.

Verbesserung

FullClient

- Die Konfiguration der E-Mail Benachrichtigungen befindet sich jetzt in den Kontoeinstellungen.
- Wenn ein Benutzer nicht das Recht hat, ein Objekt in einer Organisationseinheit anzulegen, erscheint eine entsprechende Fehlermeldung.
- Die Option “Automatisch letzten Filter verwenden” wurde optimiert.
- Die Suche wurde optimiert: Es werden jetzt auch ähnlich klingende Werte angezeigt.
- Das Fehlerhandling beim Import von Passwörtern wurde optimiert.
- Die Suche nach Werten in den Benutzereinstellungen wurde optimiert.
- Der Verwendung von Smartcards für die passwortlose Anmeldung wurde optimiert.
- Die Verwendung der Assistenten wurde optimiert.
- Die Überprüfung der Werte in den Benutzereinstellungen wurde verbessert.

WebClient

- Die Konfiguration der E-Mail Benachrichtigungen befindet sich jetzt in den Kontoeinstellungen.
- Wenn ein Benutzer nicht das Recht hat, ein Objekt in einer Organisationseinheit anzulegen, erscheint eine entsprechende Fehlermeldung.
- Die Konfiguration des Ablaufdatums eines Passwortes wurde optimiert.
- Die Suche wurde optimiert: Es werden jetzt auch ähnlich klingende Werte angezeigt werden.
- Die Suche nach Werten in den Benutzereinstellungen wurde optimiert.

- Die Verwendung der Assistenten wurde optimiert.
- Die Überprüfung der Werte in den Benutzereinstellungen wurde verbessert.

Server

- Der Active Directory Import wurde verbessert. Beim Hinzufügen neuer Benutzer zu einer Rolle bleibt der Status quo der bereits zugehörigen Benutzer unangetastet.
- Wenn ein Benutzer nicht das Recht hat, ein Objekt in einer Organisationseinheit anzulegen, erscheint eine entsprechende Fehlermeldung.
- Die Option “Automatisch letzten Filter verwenden” wurde optimiert.

AdminClient

- Die Verwendung der Assistenten wurde optimiert.

LightClient

- Die Suche wurde optimiert: Es werden jetzt auch ähnlich klingende Werte angezeigt werden.

LightClient in der Web-Ansicht

- Die Suche wurde optimiert: Es werden jetzt auch ähnlich klingende Werte angezeigt werden.

Behoben

FullClient

- Es kann eine Benachrichtigung für abgelaufene bzw. bald ablaufende Passwörter verschickt werden.
- Der Fortschrittsbalken zeigt die noch verbleibende Zeit in Form eines farbigen Balken an.
- Der Import von Passwörtern wurde verbessert.
- Die Schnellsuche in der Strukturansicht wurde angepasst.
- Sehr lange Passwörter – beispielsweise RSA private Key – bringen den Client nicht mehr zum Absturz.

WebClient

- Beim Zurücksetzen einer Siegelanfrage wird der Benutzername des anfragenden Benutzers in der Bestätigung angezeigt.
- Die Schnellansicht kann mit “ESC” geschlossen werden.
- Die Unterscheidung zwischen aktiven und inaktiven Elementen während des AD Imports wurde verbessert.
- Die Schnellsuche in der Strukturansicht wurde angepasst.
- Eine Anmeldung ist auch bei aktivierter Datenbank Firewall mittels IPv6 Adressen möglich.
- Die Felder in einem Active Directory Profil sind nur mit entsprechenden Recht bearbeitbar.

Server

- Es kann eine Benachrichtigung für abgelaufene bzw. bald ablaufende Passwörter verschickt werden.
- Der Login mit Google Authenticator als zweiter Faktor funktioniert auch, wenn die erste Zahl des

Tokens eine Null ist.

AdminClient

- Der Datenbank Benchmark Test funktioniert auch für Datenbanken mit Sonderzeichen im Namen.

Add-ons

- Benutzer mit Sonderzeichen können sich am Addon anmelden.
- Passwörter mit Sichtschutz und Siegel werden in die entsprechenden Webseiten eingetragen wenn das Siegel gebrochen wurde.

Android App

- Passwörter können in andere Organisationseinheiten verschoben werden.
- Das Öffnen der Blacklist führt nicht mehr zum Absturz der Anwendung.

iOS App

- Der QR Code Scanner wurde angepasst.
- Passwörter können in andere Organisationseinheiten verschoben werden.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.13.0.25027-de.msi)
`ac00968bcd2bdbd339d990186ac1eaf3a74d74063714a43332204904e5d333920860d65d29859f1657f10`

Englisches Server Setup (pss8.13.0.25027-en.msi)
`e43f71a7587a9a5652d476dbf9321a367c85d2594fb9fdc7f99be653786a7341e400e4c67b52f40ea173a`

Deutsches Client Setup (psc8.13.0.25027.msi)
`65f2e2e90cbf5345473514b19ce3e7233c7c1fc8ce8286223fc30be55a1755cb28ed21706588c5e119ff6`

Englisches Client Setup (psc8.13.0.25027-en.msi)
`1df2729c4fc7aa8f4072ca342c289a548d205be1e7fa7f139a1859c44fe1c30e2e8ab483b0161f4cd5ab2`

Version 8.12.1.22757

Veröffentlichung

01.02.2021

Kompatibilität

Zum AdminClient der Version 8.12.1 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.12.1.22757
- Windows Client Version 8.12.0.22707

- WebClient Version 8.12.1.22757
- WebClient Version 8.12.0.22707

- Password Safe Mobile Apps 1.19

> ! Mit dem Update auf **Version 8.12.0** wird sowohl am Anwendungsserver als auch an den Clients die **.net Version 4.8.0** oder neuer voraus gesetzt. **Prüfen Sie** daher **vor der Installation** auf allen relevanten Geräten ob dies gegeben ist.

Neu

Add-ons

- Benutzer mit aktiviertem FIDO2 können sich mit ihrem Active Directory Passwort am Addon anmelden.

Behoben

FullClient

- Benutzer mit Sonderzeichen im Benutzernamen können einen beliebigen aktivierten zweiten Faktor konfigurieren.
- Benutzer, deren Profile über Registry-Einträge verteilt werden, können sich wieder anmelden.
- Ein Benutzer mit Smartcard als erster Faktor für die Anmeldung kann keinen automatischen Login konfigurieren.

WebClient

- Benutzer mit Sonderzeichen im Benutzernamen können einen beliebigen aktivierten zweiten Faktor konfigurieren.
- Die Strukturansicht im Modul “Passwörter“wird wieder angezeigt.
- Es können Benutzer mit Sonderzeichen im Namen als auch im Passwort angelegt werden.

AdminClient

- Benutzer, die ein selbst erstelltes Zertifikat nur mit dem Servernamen aber ohne dazugehörige IP Adresse verwenden, können die Datenbank-Einstellungen öffnen.

Setup Prüfhash (SHA-512 Hash)

Deutsches Server Setup (pss8.12.1.22757-de.msi)
967b6619cba45ba96f34405416271cf46696ef8512d29b74ae2bd122f4046c4d41c61fb15542e2cc6ae6d

Englisches Server Setup (pss8.12.1.22757-en.msi)
257a52762b5c6de6e7d9b75fe88746058ccfbafc1d71f9152c79b42f994ab5ce3aa106f702482d0e3da2f

Deutsches Client Setup (psc8.12.1.22757.msi)
25bbf824932b9876818083371db17af6a1303be54e79e6b3fbfd3b433fbc582c1db0c736c4eedd01863ca

Englisches Client Setup (psc8.12.1.22757-en.msi)
53d8a75b9d30d483687e564a31b5201675266976d916cdb9c577c3c137a4ee8e4d1054ecfc199ecc98bd6

Version 8.12.0.22707

Veröffentlichung

21.01.2021

Kompatibilität

Zum AdminClient der Version 8.12. sind folgende Client Versionen kompatibel:

- Windows Client Version 8.12.0.22707
- WebClient Version 8.12.0.22707
- Password Safe Mobile Apps 1.19

> ! Mit dem Update auf **Version 8.12.0** wird sowohl am Anwendungsserver als auch an den Clients die **.net Version 4.8.0** oder neuer voraus gesetzt. **Prüfen Sie** daher **vor der Installation** auf allen relevanten Geräten ob dies gegeben ist.

Neu

FullClient

- Nach dem endgültigen Löschen einer Organisationseinheit wird die Ansicht automatisch aktualisiert.
- Es wurde eine Abtipphilfe für Passwörter integriert.
- Bei der Konfiguration des Google Authenticators wird neben dem QR-Code auch das Secret angezeigt.
- Die Benutzereinstellungen wurden um die Auswahlmöglichkeiten für die passwortlose Anmeldung erweitert.
- Benutzer können sich nun mit Hilfe einer Smartcard anmelden.
- Nach Eingabe des Benutzernamens wird das dazugehörige Profilbild angezeigt – sofern hinterlegt.
- Bei Erstellung eines neuen Datenbank-Zertifikates werden alle damit verschlüsselten Anmelde-Faktoren zurückgesetzt.
- In der Session-Liste der verbundenen Geräte werden Android und iOS Apps inklusive der jeweiligen Version angezeigt.
- Das Recht “Hinzufügen” kann nur im Rechtefilter des Moduls “Organisationseinheiten” ausgewählt werden.
- Offene Tabs können mittels „STRG + W“ oder mittlerer Maustaste geschlossen werden.
- Datensätze können auch ohne das Recht “Kann persönliche Datensätze anlegen” dupliziert werden, solange das Ziel nicht der eigene Benutzer ist.
- Tooltipps beim Passwort-Import hinzugefügt
- Benutzereinstellungen können auch bei Active*Directory-Profilen vererbt werden.
- Die Filterung nach Organisationseinheiten wurde verbessert.

- In der Session Liste der verbundenen Geräte werden Android und iOS Apps inklusive der jeweiligen Version angezeigt.

WebClient

- Es wurde eine Abtipphilfe für Passwörter integriert.
- Benutzer können sich nun mit Hilfe eines FIDO2-Tokens anmelden.
- Die Benutzereinstellungen wurden um die Auswahlmöglichkeiten für die passwortlose Anmeldung erweitert.
- Nach Eingabe des Benutzernamens wird das dazugehörige Profilbild angezeigt – sofern hinterlegt.
- Das Secret bei Konfiguration des Google Authenticators kann in die Zwischenablage kopiert werden.
- Bei Erstellung eines neuen Datenbank*Zertifikates werden alle damit verschlüsselten Anmelde-Faktoren zurückgesetzt.
- Die Konfigurationsmöglichkeiten der Benachrichtigungen bei Passwörtern wurden angepasst.
- Wenn eine SAML-Anwendung gestartet wird, wird eine Benachrichtigung ausgelöst.
- Das Recht “Hinzufügen” kann nur im Rechtefilter des Moduls “Organisationseinheiten” ausgewählt werden.
- Benutzereinstellungen können auch bei Active-Directory-Profilen vererbt werden.

AdminClient

- Sollte ein Datenbank-Zertifikat nicht mehr vorhanden sein, so kann ein neues erstellt werden.
- Bei der Erstellung eines Verbindungs*Zertifikates während der Basiskonfiguration können mehrere alternative Antragsteller eingetragen werden.
- In der Session-Liste der verbundenen Geräte werden Android und iOS Apps inklusive der jeweiligen Version angezeigt.
- Es können Netzwerke festgelegt werden, in denen ein konfigurierter zweiter Faktor für die Anmeldung nicht benötigt wird.
- Es kann ein alternativer Crypto Service Provider für die Anmeldung mittels Smartcard angegeben werden.

OfflineClient

- Es kann nach Organisationseinheiten gesucht werden.

Add-ons

- Der Login-Prozess des Add-ons wurde angepasst.
- Die Fehlermeldung für Autofill bei mehreren Passwörtern für eine Webseite wurde angepasst.

Android App

- Es wurde eine Abtipphilfe für Passwörter integriert.
- Es wurde ein Passwort-Generator zum Erstellen besonders sicherer Passwörter integriert.
- Benutzer können im Tab “Alle Passwörter” neue Datensätze anlegen und sich selbst zuweisen.

iOS App

- Es wurde ein Passwort-Generator zum Erstellen besonders sicherer Passwörter integriert.
- Benutzer können im Tab “Alle Passwörter” neue Datensätze anlegen und sich selbst zuweisen.

LightClient in der Web-Ansicht
- Es wurde eine Abtipphilfe für Passwörter integriert.
- Der zweite Faktor kann auch im LightClient in der Web-Ansicht konfiguriert werden

Änderung

FullClient

- Der Standardwert für ein Session Timeout wurde auf eine Stunde gesetzt.

WebClient

- Der Standardwert für ein Session Timeout wurde auf eine Stunde gesetzt.

Verbesserung

Server

- Der Password Safe Server akzeptiert nur noch Verbindungen mit TLS Version 1.3 und 1.2.

h4, Add-ons

- Das automatische Ausfüllen der Anmeldemasken wurde optimiert.

FullClient

- Die Darstellung der Tags in der Listenansicht wurde optimiert.
- Der Prozess zum Zurücksetzen des zweiten Faktors – falls aktiviert – wurde optimiert.
- Wenn zwei AD-Profile mit derselben Domäne existieren und eines davon gelöscht wird, funktioniert das zweite auch weiterhin.
- Die Konfiguration des zweiten Faktors wurde – falls benötigt – optimiert.
- Wenn sich ein Benutzer authentifizieren möchte, wird eine konfiguriertes Session Timeout ignoriert.

WebClient

- Der Prozess zum Zurücksetzen des zweiten Faktors wurde – falls aktiviert – optimiert.
- Die Konfiguration des zweiten Faktors wurde – falls benötigt – optimiert

AdminClient

- Der Export von Datenbank-Zertifikaten wurde optimiert.

Add-ons

- Das automatische Ausfüllen der Anmeldemasken wurde optimiert.

LightClient

- Sucht ein Benutzer nach einer Organisationseinheit, die bereits geöffnet ist, so wechselt er direkt in den entsprechenden Tab.

LightClient in der Web-Ansicht

- Die Ansicht wurde für mobile Endgeräte optimiert

Behoben

FullClient

- Das Kontext-Menü in der Listenansicht wurde optimiert.
- Die Konfiguration von One*Time*Passwords wurde optimiert.
- Die Konfiguration von Password Resets optimiert.
- Die Konfiguration von Discovery Service Taks optimiert.
- In den Benutzerrechten wird die Version angezeigt, ab welcher eine Option verfügbar ist.
- Die Konfiguration des Filters wurde optimiert.
- Anpassung der Farbschemen Office 2019 Black, Dark Grey und Metropolis Dark
  Benachrichtigungen für Objekte anderer Benutzer können nur mit dem Recht “Schreiben” aktiviert werden.
- Nach erfolgreichem Import von Passwörtern wird die Ansicht automatisch aktualisiert.
- Die Zeit bis zum automatischen Logout des WebViewers wurde auf maximal einen Tag begrenzt.
- Jedes Mitglied einer Rolle kann andere Benutzer zu der Rolle hinzufügen, unabhängig von den Rechten, die das Mitglied für den Benutzer hat.
- Beim Wechsel in ein anderes Modul werden etwaige Filtereinstellungen nicht mehr übernommen.
- Die Siegelübersicht wurde optimiert.
- Die Zwischenablage-Aktionen in der Ribbon sind nur bei einem ausgewählten Passwort verfügbar.
- Die Konfiguration von System Tasks wurde optimiert.
- Die Buttons zum Überschreiben und Vererben von Berechtigungen werden nur angezeigt, wenn die Berechtigungen angepasst wurden.
- Beim Verschieben von Passwörtern in andere Organisationseinheiten bleiben die jeweiligen Besitzerrechte erhalten.
- Die Tagverwaltung in den Rechtevorlagen wurde angepasst.
- Wird mehr als eine Instanz geöffnet, bleiben alle weiteren Instanzen bis zur Abmeldung mit dem Anwendungsserver verbunden.
- Bei einer SSO-Anwendung mit mehreren damit verbundenen Passwörtern kann zwischen diesen ausgewählt werden.
- Der letzte aktive zweite Faktor kann nur dann deaktiviert werden, wenn auch bei allen Organisationseinheiten die Option “zweiter Faktor wird benötigt” deaktiviert ist.
- Im Modul “Rollen” wird die Listenansicht nach Bearbeitung einer Rolle automatisch aktualisiert.
- Wird ein in Password Safe gespeichertes Dokument bearbeitet und überschreitet dabei die maximal erlaubte Dateigröße, so erscheint beim Speichern eine entsprechende Fehlermeldung.
- Bei deaktivierter Option “Tab nach öffnen bearbeiten” werden die beiden Optionen “Konfiguration entfernen” und “Anwendung erfassen” in der Ribbon aktiviert, wenn im Modul “Anwendungen” auf “Bearbeiten” geklickt wird.
- Bei Skalierung des Hauptfensters wird auch der Footerbereich entsprechend skaliert.
- Beim Versuch, trotz Druckerecht ein versiegeltes Passwort zu drucken, erscheint eine entsprechende Fehlermeldung.
- Es ist nicht möglich, User oder Organisationseinheiten mittels Drag & Drop einem einzelnen User zuzuweisen.
- Beim Anlegen eines neuen Dokuments wird die Organisationseinheit des Erstellers vorausgefüllt.

- Für mehrzeilige Textfelder in Passwörtern können keine Passwortrichtlinien festgelegt werden.
- Die Ansicht der Zusammenfassung eines Importes wurde angepasst.
- Die Berichtsansicht im FullClient wurde angepasst
- Das Formularfeld für das Benutzerpasswort wurde angepasst.
- Wenn ein Benutzer versucht, bei einem anderen Benutzer dessen Rechteschlüssel bei “Berechtigungen” zu entfernen, erscheint eine Fehlermeldung, dass diese Aktion nicht möglich ist.
- Wenn keine Anwendung ausgewählt ist, ist der Button “Passwort verbinden” deaktiviert.
- Temporäre Berechtigungen für ‘Jeder’ werden in Berechtigungsvorlagen nun korrekt gespeichert.
- Ein Benutzer kann in der Schnellansicht ein versiegeltes Passwort sehen, wen er nicht vom Siegel betroffen ist.
- Die Namen der Filtergruppen im Modul “Discovery Service” wurden angepasst.
- Soll eine Auswahl von Formularen in der Listenansicht ausgedruckt werden, so wird die Anzahl der Formularfelder mit Druckrecht im Verhältnis zur Anzahl aller Felder mit Leserecht angezeigt.
- Bei aktiviertem Benutzerrecht “Kann Stapelverarbeitung bei Berechtigungen anhand eines Filters durchführen” werden die Rechte eines Benutzers bei allen gefilterten Passwörtern reduziert.
- Beim Import von Organisationseinheiten können diese nur anderen Organisationseinheiten untergeordnet werden.
- Das Verschieben von Objekten generiert einen neuen Logbucheintrag “Verschoben”.
- Bei Copy & Paste von Host* und Dienstname in einem Skript für einen Password Reset werden alle Leerzeichen entfernt.
- Der Tabname eines neu angelegten Objekts bleibt erhalten, wenn während der Neuanlage “alle Daten neu laden” geklickt wird.
- Beim Anlegen eines neuen Berichts wird der Tabname entsprechend benannt.
- Die Zählung der Benutzerlizenzen bei Verwendung von Active Directory wurde angepasst.
- Der Prozess zum Anlernen von Anwendungen wurde angepasst.
- Wird bei Passwörtern mit Sichtschutz und Siegel letzteres gebrochen, erscheint ein entsprechender Hinweis zum Sichtschutz.
- Das Kontextmenü im Modul “Passwörter” wurde angepasst.
- Benutzer ohne entsprechendes Recht können keine Rechte für eine Organisationseinheit vordefinieren.
- Die Listenansicht der System Tasks wurde um neue Spalten erweitert.
- Die Filtergruppe “Tags” wurde angepasst
- Bei Bearbeitung eines geöffneten Siegels kommt die Aufforderung, ein neues Passwort zu vergeben.
- Im Modul “Benachrichtigungen” können Siegelvorlagen via Button “Siegelvorlage” direkt geöffnet werden.
- Die Vorschau eines Dokuments kann nur bei entsprechendem Recht geöffnet werden.Das Kontexmenü bei den Benutzerrechten bzw. -einstellungen wurde angepasst.
- Die Konfiguration der Benachrichtung “Wenn in Verwendung” wurde erweitert.
- Die Zusammenfassung eines Active Directory Imports zeigt jetzt die korrekte Zuordnung der Benutzer zu den entsprechenden Organisationseinheiten an.
- Das Fehlerhandling beim endgültigen Löschen von Benutzern wurde angepasst.
- Dokumente können jetzt auch nach Dateinamenserweiterung gefiltert werden.
- Geänderte Formularfeldtypen werden jetzt auch bei einem Formularwechsel erkannt.
- Die Filtergruppe “Rechte” im Modul “Passwörter” wurde angepasst.
- Werden Benutzer im Active Directory in eine andere Organisationseinheit verschoben, so werden sie auch bei der nächsten Synchronisation entsprechend verschoben.
- Das Verhalten der Buttons in der Ribbon wurde in allen Modulen vereinheitlicht.

- Nur Benutzer mit dem Recht “Hinzufügen” können bei einem Active Directory Import neue Organisationseinheiten anlegen.
- Beim Import von leeren Gruppen aus dem Active Directory werden die entsprechenden Berechtigungen und Mitgliedschaften gesetzt.
- Ein Benutzer kann ohne entsprechende Rechte nicht die Mitgliedschaften anderer Benutzer in Rollen bearbeiten.
- Die Skalierungsmöglichkeiten der Fenstergröße von RDP-Anwendungen wurden angepasst.
- Beim Downgrade auf eine Edition mit geringerem Funktionsumfang werden Module, die diese Edition nicht enthält, nicht mehr angezeigt.
- Die Eingabemaske für neue Passwort-Richtlinien wurde angepasst.
- Wenn ein Passwort geöffnet wird, dessen Formular aber zwischenzeitlich geändert wurde, erscheint beim Schließen der Hinweis, ob die Änderungen verworfen werden sollen.
- In Formularen können jetzt neue Felder mit dem Namen von gelöschten Formularfeldern angelegt werden.
- Die in einer Filtergruppe angezeigten Objekte werden beim Aufruf eines gespeicherten Filters aktualisiert.
- Bei RDP Verbindungen kann auch der lokale Benutzer „.\Benutzer“ des Zielsystems für die Anmeldung verwendet werden.
- Ungültige Zeichen im Namen einer Multi-Faktor-Authentisierung werden herausgefiltert.
- Wenn eine Synchronisation des Active Directory nicht erfolgreich war, wird eine entsprechende Fehlermeldung angezeigt.
- Die Funktionalität beim Minimieren von RDP-Anwendungen in Password Safe wurde optimiert.
- Beim Import eines Active Directory Benutzers wird auch die hinterlegte Beschreibung importiert.
- Einer Anwendung können beliebig viele Passwörter zugeordnet werden, ohne dass der Client bei Anzeige der Passwörter einfriert.
- Wenn das Lizenzmodul fehlt, wird im Logbuch bei den entsprechenden System-Task eine Fehlermeldung angezeigt.
- Wenn ein Benutzer die Berechtigungen von mehreren Rollen gleichzeitig bearbeitet, bleibt sein Mitgliedsstatus so lange unverändert, bis er diesen explizit bearbeitet.
- Ein etwaiger aktiver Filter wird beim Anlegen eines neuen Berichts zurückgesetzt.
- Keepass Ordner können nur in Organisationseinheiten, nicht in Benutzer importiert werden.
- Bei Web-Anwendungen ist das URL-Feld ein Pflichtfeld.
- Beim Herunterfahren von Windows werden eventuell noch aktive SSO*Agent oder FullClient Sessions automatisch beendet.
- Die Filtergruppe “Gültigkeit-Status” wurde optimiert.
- Beim Anzeigen der Metadaten von verknüpften Dokumenten erscheint keine Fehlermeldung.
- Trotz mehrmaligen Doppelklicks auf eine/n Benachrichtigung / Logbucheintrag wird das Objekt nur einmal geöffnet.
- Beim Import von Anwendungen wird das korrekte Datum für “gültig bis” importiert.
- Ein Klick auf den blauen Pfeil öffnet das Kontextmenü zum Bearbeiten des Feldeinhaltes eines Passwortes unabhängig davon, ob der Tab sofort oder erst durch Klicken auf “Bearbeiten” in der Ribbon bearbeitet werden kann.
- Die Negierung eines Organisationseinheiten-Filters zeigt auch Benutzer außerhalb Organisationseinheiten an.
- Die Anzahl der Datensätze hat keinen Einfluss auf die Anmeldung beim WebViewer.
- Die Anpassung der Fenstergröße einer RDP- oder SSH-Verbindung verursacht keine Logbucheinträge mehr.
- Bei einem Bericht vorgenommene Filteranpassungen bleiben nach dem Speichern des Berichts

erhalten.
- Die Offline Synchronisation wird entsprechend der möglichen Einstellungen ausgeführt.
- Die Checkbox “Restriktiver Benutzer” ist bei fehlendem Recht “Bearbeiten” ausgegraut.
- Logbucheinträge können nach “Ausführung gestartet” oder “Ausführung beendet” gefiltert werden.
- Bei Änderung eines Feldtyps in einem Formular wird der entsprechende Standardwert angepasst.
- Der Import von CSV-Dateien wurde überarbeitet.
- Die Vorschau des Importassistenten wurde in allen Modulen angepasst.
- Die Hinweismeldungen in Formularfeldern wurden angepasst.
- Deaktivierte Benutzer mit aktiver MFA können sich nach Aktivierung mittels Synchronisation wieder an Password Safe anmelden.
- Offene RDP-Verbindungen brechen beim Wechsel in ein anderes Modul und zurück nicht mehr ab.
- Die Tastaturkürzel “STRG+ALT+S” und “STRG+ALT+V” tragen Benutzername und Passwort in die dazugehörigen Felder ein.
- Schalflächen zum Ändern von Passwörtern und zur Konfiguration von OTPs sind bei restriktiven Benutzern ausgegraut.
- Das Kontextmenü wurde systemweit angeglichen.
- Der Darstellungsfehler beim Read-only-Modus eines Discovery Service Tasks wurde behoben.
- Bei der Eingabe des Secrets für ein One*Time-Password wird der Fokus auf das Feld gesetzt.
- Mit entsprechendem Recht “Kann neue Anwendungen vom Typ RDP anlegen” können RDP-Anwendungen dupliziert werden.
- Der Spalteneditor funktioniert auch bei der Skalierung größer 100%.
- Der Hinweis auf ein bereits gebrochenes Siegel wird auch beim Bearbeiten eines betroffenen Passwortes angezeigt.
- Der Siegel-Freigabe-Prozess bei Verwendung kurzer Gültigkeits-Zeiträume wurde optimiert.
- Die client*übergreifende Anmeldung bleibt aktiv, wenn man den OfflineClient öffnet.
- Wenn ein Benutzer die Berechtigungen auf Passwörter über Gruppenberechtigungen anpasst, erscheint eine Fehlermeldung für die Passwörter, auf die er selbst nicht berechtigt ist.
- Beim Anlegen einer neuen Rolle mittels “CTRL+N” wird der Fokus im Tab auf das erste Eingabefeld gesetzt.
- Die Berechnung der Passwortqualität wurde optimiert.
- Passwörter können nur mit dem entsprechenden Recht “Kann Passwörter anlegen” dupliziert werden.
- Benutzer können auch ohne das Recht “Kann Tags verwalten” nach Tags suchen und diese Objekten zuweisen.

WebClient

- Der Siegelprozess wurde optimiert.
- Beim Verschieben von Passwörtern in andere Organisationseinheiten bleiben die jeweiligen Besitzerrechte erhalten.
- Benachrichtigungen werden auch in der mobilen Ansicht des Browsers angezeigt.
- Die Tagverwaltung in Rechtevorlagen wurde angepasst.
- Bei einer SSO-Anwendung mit mehreren damit verbundenen Passwörtern kann zwischen diesen ausgewählt werden.
- Grafische Anpassungen im Active Directory Profil
- Der letzte aktive zweite Faktor kann nur dann deaktiviert werden, wenn auch bei allen Organisationseinheiten die Option “zweiter Faktor wird benötigt” deaktiviert ist.
- Der WebClient kann mittels „F5“ neu geladen werden, auch wenn im Modul

“Organisationsstruktur” eine Organisationseinheit ausgewählt ist.
- Befinden sich in einer Liste Objekte, für die das Druckrecht nicht vorhanden ist, so erscheint eine entsprechende Fehlermeldung beim Versuch, die Liste auszudrucken.
- Fehlermeldungen sind nur sichtbar, wenn ein Benutzer angemeldet ist.
- Bei erteilter Siegelfreigabe werden im Benachrichtigungsmodul bei Klick auf den Buttons “Passwort” das entsprechende Passwort und bei “Siegel” die Siegelübersicht angezeigt.
- Wenn ein Benutzer versucht, bei einem anderen Benutzer dessen Rechteschlüssel bei “Berechtigungen” zu entfernen, erscheint eine Fehlermeldung, dass diese Aktion nicht möglich ist.
- Suchergebnisse im Modul “Organisationsstruktur” werden bereits angezeigt, wenn mit der Eingabe des Suchbegriffs begonnen wird.
- Es können nicht mehrere Tags gleichzeitig bearbeitet werden
- Freigabeberechtigte Benutzer können versiegelte Passwörter drucken.
- Wenn keine Anwendung ausgewählt ist, ist der Button “Passwort verbinden” deaktiviert.
- Bei aktivierter Benutzereinstellung “Benachrichtigungen beim Öffnen als gelesen markieren” werden in der Schnellansicht geöffnete Benachrichtigungen als gelesen markiert.
- In der Schnellansicht aller Elemente wird das Feld “Beschreibung” angezeigt.
- Die Schnellansicht von Benachrichtigungen zeigt das Datum und die Uhrzeit an.
- Das Verschieben von Objekten generiert einen neuen Logbucheintrag “Verschoben”.
- Das Kontextmenü im Modul “Benachrichtigungen” wurde angepasst.
- Die Schnellansicht wurde in allen Modulen verbessert.
- Der Button “Passwörter löschen” in der Ribbon im Modul “Anwendungen” ist nur dann aktiv, wenn es entsprechende verknüpfte Passwörter gibt.
- Bei verschachtelten Organisationseinheiten kann die oberste nicht in eine untergeordnete verschoben werden.
- Duplizierte Anwendungen werden der Organisationseinheit oder dem Benutzer zugewiesen, der sie dupliziert.
- Anwendungen können als öffentlich oder persönlich gekennzeichnet werden.
- Die farbliche Unterscheidung temporärer Berechtigungen wurde im WebClient angepasst.
- Die Sortierung der Toolbar*Gruppen wurde angepasst.
- Werden Benutzer im Active Directory in eine andere Organisationseinheit verschoben, so werden sie auch bei der nächsten Synchronisation entsprechend verschoben.
- Die Gruppierung von Passwörtern nach Datum wurde optimiert.
- Beim Downgrade auf eine Edition mit geringerem Funktionsumfang werden Module, die diese Edition nicht enthält, nicht mehr angezeigt.
- Beim Anlegen eines neuen Dokuments in einer Organisationseinheit soll * sofern es für diese OU eine Standard-Rechtevorlage gibt – diese ausgewählt und entsprechend eingetragen sein
- Das Protokoll „lns://“ wird jetzt unterstützt.
- Die Listenansicht im Modul Benachrichtigungen und im Logbuch wurde angepasst.
- Bei Neuanlage einer Organisationseinheit wird diese beim Wechsel ins Modul “Passwörter” im Strukturfilter angezeigt.
- Einer Anwendung können beliebig viele Passwörter zugeordnet werden, ohne dass der Client bei Anzeige der Passwörter einfriert.
- Das Verhalten bei Klick auf ein Benachrichtigungssymbol wurde in der mobilen Ansicht angepasst.
- Die Ansicht im Modul “Benachrichtigungen” wurde angepasst.
- Benutzer können die Einstellungen anderer Benutzer nur mit dem Recht “Berechtigen” sehen.
- Beim Speichern mittels „ALT + S“ werden alle Formularfelder gespeichert.
- Der Text über die Anzahl der ausgewählten Objekte in der Listenansicht wurde angepasst.
- Die Mehrfachselektion mittels „Shift“ und Pfeiltasten funktioniert in allen Modulen.

- Änderungen der Rechte wirken sich erst nach dem Speichern aus.
- Bei Web*Anwendungen ist das URL-Feld ein Pflichtfeld.
- Die Filtergruppe “Gültigkeit-Status” optimiert.
- Mit „ALT + S“ können im Modul “Organisationseinheiten” neue Objekte gespeichert werden.
- Neu angelegte Benutzer oder Organisationseinheiten werden nach dem Speichern in der Listenansicht markiert.
- Beim Anlegen eines Dokuments wird ein Logeintrag “Neu” geschrieben.
- Überlange Texte werden in der Löschbestätigung umgebrochen.
- Die Negierung eines Organisationseinheiten*Filters zeigt auch Benutzer außerhalb Organisationseinheiten an.
- Die Tooltipps beim Anlegen eines neuen Dokumentes wurden korrigiert.
- Schalflächen zum Ändern von Passwörtern und zur Konfiguration von OTPs sind bei restriktiven Benutzern ausgegraut.
- Die Breite der Schnellsuche angepasst.
- Die Berechnung der Passwortqualität wurde optimiert.
- Benutzer können auch ohne das Recht “Kann Tags verwalten” nach Tags suchen und Objekten zuweisen.
- Bei Skalierung des Hauptfensters wird auch der Footerbereich entsprechend skaliert.

Server

- Die Migration von V7 auf V8 wurde optimiert.
- LightClient-Lizenzen werden nur in der Enterprise Plus Edition gezählt.

*Verbesserte Lizenzprüfung für virtuelle Maschinen ohne Hardware-IDs
- Beim Import von Passwörtern, die Anführungszeichen enthalten, werden diese als solche erkannt.
- Beim Active Directory Import können nur noch Benutzer mit hinterlegter E-Mail importiert werden.
- Die “Admin-Rolle” wird beim Anlegen einer Datenbank unter Verwendung einer englischen Vorlage richtig übersetzt.
- Bei der Bearbeitung der Rechte mehrerer Rollen erscheint eine Fehlermeldung beim Hinzufügen neuer Benutzer, wenn der Bearbeiter selbst nicht Mitglied einer oder mehrerer dieser Rollen ist.
- Datenbankprofile können über die Registry an Benutzer verteilt werden.
- User, die im Active Directory deaktiviert wurden, werden jetzt nicht mehr mit Password Safe synchronisiert.
- Änderungen am Notfall-WebViewer sind sofort nach dem Speichern aktiv.
- Der Discovery Service scannt auch die Dienste auf dem Server, auf dem er gestartet wurde.

AdminClient

- Die “Admin-Rolle” wird beim Anlegen einer Datenbank unter Verwendung einer englischen Vorlage richtig übersetzt.
- Bei fehlender Berechtigung des Benutzers erscheint eine Fehlermeldung beim Versuch, ein Backup-Profil anzulegen.
- Ungültige Zeichen im Datenbanknamen werden beim Erstellen eines Backups durch einen Unterstrich ersetzt.
- IP-Sperren können in der Übersicht gesperrter Verbindungen bearbeitet werden.
- Die Konfigurationseinstellungen wurden für nginx Server aktualisiert.
- Benutzer werden in der Datenbank*Benutzer-Ansicht entsprechend ihres Status farbig markiert.
- Beim Einspielen eines Datenbank*Backups werden die eingegebenen Zugangsdaten für den Login

verwendet.
- Die Backup-Funktionalität optimiert.
- Der Dialog für die Migration von V7 auf V8 wurde angepasst.
- Das Kontextmenü wurde systemweit angeglichen.
- Die Fehlermeldung bei abgelaufenem Passwort eines AdminClient Benutzers wurde angepasst.
- Wenn die Prüfung der Lizenz für eine bestimmte Datenbank im Host*Modus fehlschlägt, wird in der Fehlermeldung der Datenbankname angezeigt.
- Die lokale Zeit wird korrekt angezeigt.

Add-ons

- Das Safari-Add-on wurde optimiert.
- Der Prozess beim Anlegen eines neuen Passwortes mittels Add-on wurde optimiert.

Android App

- Der automatische Logout wurde optimiert.
- Die Synchronisation mit dem Password Safe Server wurde optimiert.
- Die Abtipphilfe optimiert.
- Die Apps auf einer selbst definierten Blacklist sind vom Auto-Fill ausgeschlossen.
- Beim Anlegen eines Passwortes wird jedes Eingabefeld direkt validiert und eventuelle Fehler werden neben den Feldern, bzw. in den Feldern angezeigt.
- Das Scroll-Verhalten in der mobilen App wurde optimiert.
- Die Änderungen der Konfiguration durch Ein-Aus-Schalter werden gespeichert.

iOS App

- Der automatische Logout wurde optimiert.
- Die Synchronisation mit dem Password Server optimiert.
- Die Abtipphilfe wurde optimiert.
- Beim Anlegen eines Passwortes wird jedes Eingabefeld direkt validiert und eventuelle Fehler werden neben den Feldern bzw. in den Feldern angezeigt.
- Das Scroll*Verhalten in der mobilen App wurde optimiert.
- Die Performance der iOS App optimiert.

API-Schnittstelle

- Fehlermeldungen beim Aufruf von Funktionen über die API wurden angepasst.
- Die Änderung des Benutzerpasswortes ist nur durch vorherige Eingabe des alten Passwortes möglich.

SSO Agent

- Wenn der Agent minimiert gestartet wird, öffnet sich beim Klick auf “Login” ein Anmeldefenster.
- Daten aus der Offline*Datenbank können mithilfe des SSO-Agents in die entsprechenden Anwendungen eingetragen werden.
- Beim Herunterfahren von Windows werden eventuell noch aktive SSO-Agent* oder FullClient-Sessions automatisch beendet.
- Der Login beim SSO-Agent wurde optimiert.
- Beim erneuten Starten eines aktiven SSO-Agents wird die Anmeldemaske angezeigt.
- Das Kontextmenü wurde systemweit angeglichen.

OfflineClient

- Die Fehlermeldungen bei der Synchronisation wurden angepasst.
- Passwörter werden auch im OfflineClient entsprechend konfigurierter Richtlinien überprüft.
- Das Kontextmenü wurde systemweit angeglichen.

LightClient

- Das Kontextmenü wurde angepasst.
- Mögliche Fehlermeldungen beim Abmelden wurden angepasst.

LightClient in der Web-Ansicht

- Bei der Suche nach SAML-Anwendungen wird die Anzahl gefundener Anwendungen angezeigt.
- Die Tastaturkürzel zum Speichern eines Datensatzes funktionieren nun auch in der Web-Ansicht des LightClients.

Version 8.11.1.19828 Hotfix 1

Veröffentlichung

21.01.2021

Kompatibilität

Zum AdminClient der Version 8.11.1.19828 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.7.0.18000 Hotfix 3
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.8.0.18002 Hotfix 3
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.9.0.17993 Hotfix 2
- Windows Client Version 8.10.0.18472
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.10.0.184736 Hotfix 2
- Windows Client Version 8.11.0.19788
- Windows Client Version 8.11.1.19823
- Windows Client Version 8.11.1.19828 Hotfix1

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.7.0.18000 Hotfix 3
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.8.0.18002 Hotfix 3
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.9.0.17993 Hotfix 2
- WebClient Version 8.10.0.18472
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.10.0.184736 Hotfix 2
- WebClient Version 8.11.0.19788
- WebClient Version 8.11.1.19823
- WebClient Version 8.11.1.19828 Hotfix 1

- Password Safe Mobile Apps 1.19

! Behoben: API-Schnittstelle: Möglichen Umgehung eines aktivierten zweiten Faktors

Neu

FullClient

- Beim Kopieren des One-Time-Passwords (OTP) werden etwaige Leerzeichen entfernt.

OfflineClient

- Beim Kopieren des One-Time-Passwords (OTP) werden etwaige Leerzeichen entfernt.

Behoben

FullClient

- System Tasks mit einem wöchentlichen oder monatlichen Intervall angepasst.
- Benutzer können beim Anlegen von Passwörtern nur zwischen verschiedenen Rechtevorlagen wählen, wenn sie das Recht “Kann Rechtevorlagen-Auswahl sehen” besitzen.
- Passwörter werden jetzt auch gespeichert, wenn beim Anlegen weitere Formularfelder hinzugefügt werden.
- Änderungen der Rechte von Organisationseinheiten wirken sich direkt auf zugehörige Passwörter aus.

WebClient

- Der WebClient funktioniert auch im Internet Explorer.

AdminClient

- Der Migrationsprozess von Password Safe V7 auf V8 wurde optimiert.

Add-ons

- In einer Terminalserver Session verbindet sich das Addon für Google Chrome sich bei entsprechender Einstellung mit dem SSO Client.

API

- Die Bibliothek “web-socket-sharp.dll” wurde hinzugefügt.

OfflineClient

- Das Passwort kann über die Ribbon bzw. das Feldmenü in die Zwischenablage kopiert werden.

Version 8.11.1.19823

Veröffentlichung

06.07.2020

Kompatibilität

Zum AdminClient der Version 8.11.1.19823 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18472
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788
- Windows Client Version 8.11.1.19823

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.10.0.18472
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.11.0.19788
- WebClient Version 8.11.1.19823

- Password Safe Mobile Apps 1.19

Neu

FullClient

- Beim Kopieren des One-Time-Passwords (OTP) werden etwaige Leerzeichen entfernt.

OfflineClient

- Beim Kopieren des One-Time-Passwords (OTP) werden etwaige Leerzeichen entfernt.

Behoben

FullClient

- System Tasks mit einem wöchentlichen oder monatlichen Intervall angepasst.
- Benutzer können beim Anlegen von Passwörtern nur zwischen verschiedenen Rechtevorlagen wählen, wenn sie das Recht “Kann Rechtevorlagen-Auswahl sehen” besitzen.
- Passwörter werden jetzt auch gespeichert, wenn beim Anlegen weitere Formularfelder hinzugefügt werden.
- Änderungen der Rechte von Organisationseinheiten wirken sich direkt auf zugehörige Passwörter aus.

WebClient

- Der WebClient funktioniert auch im Internet Explorer.

AdminClient

- Der Migrationsprozess von Password Safe V7 auf V8 wurde optimiert.

Add-ons

- In einer Terminalserver Session verbindet sich das Addon für Google Chrome sich bei entsprechender Einstellung mit dem SSO Client.

API

- Die Bibliothek “web-socket-sharp.dll” wurde hinzugefügt.

OfflineClient

- Das Passwort kann über die Ribbon bzw. das Feldmenü in die Zwischenablage kopiert werden.

Version 8.11.0.19788

Veröffentlichung

15.05.2020

Kompatibilität

Zum AdminClient der Version 8.11.0.19788 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18472
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.11.0.19788

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.10.0.18472
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.11.0.19788

- Password Safe Mobile Apps 1.19

Achtung:
Da die Technik des **Internet Explorers** veraltet ist, sehen wir uns leider dazu gezwungen, den Support für die das Add-on einzustellen. Es wird seit Version 8.9.0 nicht mehr weiterentwickelt und seit Version 8.11.0 nicht mehr ausgeliefert. Beachten Sie bitte, dass hier keine Fehler mehr behoben werden und kein Support hierfür mehr stattfindet. Die Verwendung des Add-ons erfolgt folglich auf eigene Verantwortung.

Neu

FullClient

- Im Berichtstyp “Passwort-Alter” wird zusätzlich das Erstellungsdatum der Passwörter ausgegeben.
- Anstatt der Zahlen wird bei zugedeckten One-Time-Passwörtern die entsprechende Anzahl von Strichen angezeigt.
- Ein externer Link auf ein One-Time-Password-Feld kopiert das entsprechende Token in die Zwischenablage.

WebClient

- Beim Anlegen oder Bearbeiten von Passwörtern, Dokumenten, Organisationseinheiten, Rollen oder Formularen können neue Tags erstellt, bzw. vorhandene ausgewählt werden.
- Beim Anlegen neuer Passwörter können sowohl die Organisationseinheit als auch Rechtevorlagen ausgewählt werden. Beim Bearbeiten von Passwörtern kann dagegen nur die Organisationseinheit ausgewählt werden. Wechselt man die Organisationseinheit, überschreiben die Rechte einer etwaigen Rechtevorlage die existierenden Rechte des Passwortes.

LightClient in der Web-Ansicht

- Beim Anlegen oder Bearbeiten von Passwörtern, Dokumenten, Organisationseinheiten, Rollen oder Formularen können neue Tags erstellt, bzw. vorhandene ausgewählt werden.
- Befindet man sich im Tab der Hauptorganisationseinheit (alle Passwörter), können auch von dort aus neue Passwörter angelegt werden.
- In der Tag-Verwaltung können einem Passwort mehrere Tags gleichzeitig zugewiesen werden.
- Legt man in einem Tab ein neues Passwort an, so wird die Organisationseinheit des Tabs und – sofern vorhanden – die dazugehörige Rechtevorlage angezeigt. Wird das Passwort dann unter einer anderen Organisationseinheit als die des Tabs angelegt, so wird das Passwort nicht im Tab angezeigt.
- Der Tab “Hauptorganisationseinheit” wurde in “Alle Passwörter” umbenannt. In diesem können jetzt auch Passwörter über den aus anderen Tabs bekannten “+”-Button angelegt werden.
- Passwörter können in andere Organisationseinheiten verschoben werden. Dabei werden die Rechte der Passwörter von den Rechten überschrieben, die die Organisationseinheit aufgrund einer Rechtevorlage hat.
- Passwörter können in über einen Eintrag im Kontextmenü in andere Organisationseinheiten verschoben werden. Das Passwort wird danach nicht mehr in dem geöffneten Tab angezeigt.
- Werden Passwörter bearbeitet, können jetzt Organisationseinheiten ausgewählt werden, in die die Passwörter verschoben werden sollen.

AdminClient

- Damit eine Datenbank im Hostmodus in der Liste der verfügbaren Datenbanken bei der Einrichtung der iOS bzw. Android App auftaucht, muss die Checkbox “In Datenbankliste für mobile Geräte auflisten” in den Datenbankeinstellungen aktiviert werden.

Password Safe App

- Die Apps für Android und iOS unterstützen die One-Time-Password-Funktionalität.
- Beim Anlegen und Bearbeiten von Passwörtern über die iOS oder Android App können auch

Organisationseinheiten und Rechtevorlagen ausgewählt werden.

API

- Das One-Time-Password wurde auch in die API übernommen.

Server

- Alle Lizenzen werden zentral am Password Safe Server gezählt.
- Im Notfall WebViewer werden sowohl das One-Time-Password als auch das dazugehörige Secret angezeigt.

Verbesserung

FullClient

- Passwörter ohne Benutzer mit “Berechtigen-Recht” in einer V7-Datenbank erhalten bei der Migration auf V8 einen Benutzer mit “Berechtigen-Recht”.

WebClient

- Im WebClient kann ein WebViewer Export angestoßen werden.

Password Safe App

- Das One-Time-Password für eine Webseite wird beim Autofill automatisch in die Zwischenablage kopiert.

Add-on

- Ein zweistufiges Passwort über das Add-on wird auch eingetragen, wenn die Option “Loginmasken automatisch befüllen” deaktiviert ist.

Behoben

FullClient

- Es wurden unnötige Leerzeichen in den Konfigurationseinstellungen für Benachrichtigungen entfernt.
- Beim Anlegen eines neuen Formulars sind die Ribbon-Elemente “Berechtigungen”, “Formularfeldberechtigungen” und “Info konfigurieren” ausgeblendet.
- In den Benutzereinstellungen kann in der Kategorie “Konfiguration” die Hauptorganisationsstruktur nicht mehr als Standard-Organisationseinheit ausgewählt werden.
- Bei der Konfiguration von RDP-Anwendungen dürfen “Desktopbreite” und “Desktophöhe” nur bei aktivierter Option “Bei Änderung der Größe skalieren” editierbar sein.
- Springt man mittels der TAB-Taste in das Dropdown zur Auswahl des Feldtyps und ändert diesen mittels der Pfeiltasten, wird der Feldname automatisch entsprechend geändert.
- Beim Bearbeiten von Benutzern in der Organisationsstruktur zeigt das Sprachsymbol in der Ribbon die tatsächlich ausgewählte Sprache an.
- Will ein Benutzer ohne Berechtigung ein Passwortfeld aufdecken und ignoriert den Hinweis zur Bitte um Berechtigung bei autorisierten Benutzern, bleibt das Passwortfeld zugedeckt.

- Eventuell noch laufende Report-Tasks werden beim Abmelden des Benutzers abgebrochen und der Benutzer ausgeloggt.
- Wenn man sich mittels SSO-Agent am FullClient anmeldet, kann auch ein WebViewer-Export durchgeführt werden.
- Bei einer von V7 auf V8 migrierten Datenbank wird beim endgültigen Löschen einer Organisationseinheit nur diese gelöscht. Dies wird auch im Logbuch protokolliert. Alle untergeordneten Organisationseinheiten werden nicht gelöscht.
- Das Kontextmenü der Spaltenüberschriften in der Spaltenansicht wurde in allen Modulen vereinheitlicht.
- Beim Anlegen eines neuen Tags im FullClient passt sich die Größe des Formularfeldes nicht an die Zeichenlänge des Tags an.
- Die Fehlermeldung bei Objektbezeichnungen größer als 255 Zeichen wurde in allen Modulen vereinheitlicht.
- Wählt man mehrere Benutzer im Modul “Organisationseinheiten” aus, wird der Button “Multifaktorauthentifizierung” in der Ribbon ausgegraut.
- Benutzer mit Berechtigung auf ein Passwort, aber ohne Berechtigung auf darauf berechtigte Benutzer oder Rollen, erhalten eine Fehlermeldung, wenn sie versuchen, diese Benutzer oder Rollen zu öffnen.
- Eine ausgewählte Spalte in der User- / Rollensuche zeigt je nach Sortierung immer den ersten, bzw. letzten Wert der Spalte an.
- Beim Erfassen einer Anwendung kann immer nur ein Element ausgewählt und bearbeitet werden.
- Alle beteiligten Benutzer – aktiv als Ersteller bzw. passiv als Benutzer oder Rolle in einer Rechtevorlage – werden beim Anlegen eines Passworts im Logbuch korrekt gespeichert.
- Es können Dokumente mit einer Dateiendung größer als 10 Zeichen gespeichert werden.
- Sind alle Rechte ausgewählt, so wird beim Abwählen eines beliebigen Rechts die Checkbox “Alle Rechte” abgewählt.
- Der Tooltipp bei den Formularfeldern “Internetadresse” und “IP Adresse” wurde angepasst.
- Beim Anlegen von Passwörtern mit Rechtevorlage werden darin vergebene Berechtigungen sowohl auf das komplette Passwort als auch auf einzelne Formularfelder korrekt für den jeweiligen Benutzer gespeichert.
- Passwörter, in denen ungültige reguläre Ausdrücke eingetragen wurden, werden nicht gespeichert und dem Benutzer wird eine Fehlermeldung angezeigt.
- Die Progressbar der Offline-Synchronisation wird nicht mehr angezeigt, wenn sich ein Benutzer während der Synchronisation abmeldet und sich ein neuer Benutzer anmeldet. Nach automatischer Abmeldung eines Benutzers und darauffolgender Anmeldung eines neuen Benutzers wird dieser für die automatisch startende Offline-Synchronisation nicht erneut nach seinen Zugangsdaten gefragt.
- Erstellt ein Benutzer bei aktivierter Einstellung „Ersteller aus den Berechtigungen bei neuen Objekten entfernen, wenn der erstellende Benutzer über eine Rolle berechtigt wird” manuell einen Datensatz, so wird dieser Benutzer auf den Datensatz berechtigt.
- Bei einem Active Directory Import im “MasterKeyModus” werden auch verschachtelte Gruppen importiert.
- Sonderzeichen im Dateinamen von Dokumenten werden beim Export entfernt.
- Ergebnisse aus der Suche mittels Filter werden beim Wechsel in die Strukturansicht korrekt angezeigt.
- Verliert ein Client bei aktivierter clientübergreifender Anmeldung die Verbindung zum Server und stellt sie wieder her, so wird der aktive Benutzer automatisch wieder angemeldet
- In der Ribbon sind die Buttons “Vererben” und “Überschreiben” von Berechtigungen erst im

Bearbeiten-Modus verfügbar.
- Wenn die Einstellung „Tab nach Öffnen bearbeiten“ deaktiviert ist, können Berichte nicht bearbeitet werden.
- Änderungen der Berechtigungen von Organisationseinheiten werden korrekt an die dazugehörigen Passwörter vererbt.
- Passwörter mit Siegelschutz können nur durch berechtigte Benutzer gelöscht werden.
- Es können Intervalle festgelegt werden, in denen Berichte erstellt werden sollen.
- Das Password Reset wird nur bei entsprechender Lizenz durchgeführt.
- Der Autofill von Passwörtern mit Siegel oder Sichtschutz funktioniert auch über die iOS App.
- Benutzer mit dem Recht “Löschen” können auch Passwörter mit hinterlegten Tags löschen.
- Man kann temporäre Berechtigungen auf einen Datensatz, die in der Zukunft liegen, entfernen.
- Bei deaktivierter Benutzereinstellung “Tab nach Öffnen bearbeiten” wird nach dem Öffnen eines Datensatzes in der Ribbon der Button “Bearbeiten” angezeigt.
- Ein Passwort kann nur angelegt werden, wenn eine Organisationseinheit ausgewählt ist.
- Bei deaktivierter Einstellung “Tab nach Speichern schließen” wird immer nur eine Weiterleitungsregel im Modul “Benachrichtigungen” angelegt, wenn man diese Regel speichert.
- Im Logbuch wird ein Eintrag des Active Directory Profils bei Klick auf den Button “Öffnen” angezeigt.
- Beim Löschen einer Siegelvorlage wird eine Benachrichtigung verschickt.
- Beim Löschen eines Active Directory Profils werden auch die dazugehörigen Zertifikate gelöscht.
- Die Übersicht aller Benachrichtigungen wurde angepasst.
- Der aktuellste und damit aktive Stand eines Passwortes kann nicht wiederherstellt werden.
- Die Eintragung mittels SSO wurde für zahlreiche Anwendungen umgesetzt.
- Beim Wiederherstellen von Dokumenten werden auch die entsprechenden Metadaten wiederhergestellt.
- Beim Anlegen neuer Passwörter wird nur eine Benachrichtigung über das Anlegen erzeugt.
- One-Time-Passwörter werden im Full- als auch im WebClient gleichbehandelt.
- Die Listenansicht wurde in allen Modulen vereinheitlicht.
- Die Optionen der jeweiligen Password Safe Editionen wurden angepasst.
- Die Listenansicht für die Anzeige des Datums der letzten Änderung eines Datensatzes wurde in allen Modulen vereinheitlicht.
- Änderungen einer Formular-Info werden nach dem Speichern direkt in der Listenansicht angezeigt.
- Es können auch bei mehreren gleichzeitig selektierten Datensätzen Rechte hinzugefügt und entfernt werden.
- Bei der Bearbeitung eines Passworts mit einem One-Time-Password-Feld läuft weder der Countdown des OTPs noch wird der Ablaufbalken angezeigt.
- Nach dem Bearbeiten und Speichern eines Passwortes mit einem One-Time-Password-Feld wird das Secret des OTP nicht zurückgesetzt, sondern bleibt erhalten.
- In der Tabellenansicht im Modul „Passwörter” wird das One-Time-Password nicht angezeigt.
- Beim Duplizieren von Passwörtern wird das Feld zur Auswahl einer Rechtevorlage nicht angezeigt.
- Beim Versuch, ein gelöschtes Passwort anzuzeigen, wird eine entsprechende Fehlermeldung angezeigt.
- Restriktive Benutzer können bei einem WebViewer-Export keine Passwörter aufdecken.
- Benutzer ohne das Recht “Hinzufügen” können Dokumente keiner anderen Organisationseinheit zugewiesen werden.
- Passwörter mit einem One-Time-Passwort als Pflichtfeld können ohne konfiguriertes Secret nicht

gespeichert werden.
- Der Button “Entfernen” wird im Kontextmenü zum Konfigurieren neuer Rechte bei einer Organisationseinheit einmal angezeigt.
- Das Besitzerrecht für ein Objekt kann nur vom Besitzer selbst oder dem Datenbankadministrator entfernt werden.
- Beim Drucken von Passwörtern mit nicht konfiguriertem One-Time-Passwort sind die Felder für das One-Time-Password und / oder das dazugehörige Secret leer.
- Bei Skalierung des Hauptfensters wird auch der Footerbereich entsprechend skaliert.
- Beim Versuch, trotz Druckerecht ein versiegeltes Passwort zu drucken, erscheint eine entsprechende Fehlermeldung.
- Es ist nicht möglich, User oder Organisationseinheiten mittels Drag&Drop einem einzelnen User zuzuweisen.
- Beim Anlegen eines neuen Dokuments wird die Organisationseinheit des Erstellers vorausgefüllt.
- Beim Drucken von Passwörtern mit nicht konfiguriertem One-Time-Passwort sind die Felder für das One-Time-Password und / oder das dazugehörige Secret leer.
- Für mehrzeilige Textfelder in Passwörtern können keine Passwortrichtlinien festgelegt werden.
- Die Ansicht der Zusammenfassung eines Importes wurde angepasst.
- Die Berichtsansicht im FullClient wurde angepasst
- Das Formularfeld für das Benutzerpasswort wurde angepasst.
- Mit dem Recht “Kann Rechtevorlage verwalten” können auch andere Rechtevorlagen einer Organisationseinheit als die Standard-Rechtevorlage ausgewählt und zugewiesen werden.

WebClient

- Der Name “Account” von Formularvorlagen mit diesem Namen wird in der Vorlagenauswahl korrekt angezeigt.
- Bei vererbten Benutzereinstellungen wird angezeigt, von welcher Organisationseinheit die Einstellung vererbt wurde.
- Rollen aus einem Actice Directory im Master Key Modus können nicht gelöscht werden.
- Die Ansicht kann mittels „F5“ neu geladen werden, auch wenn im Modul “Organisationsstruktur” eine Organisationseinheit ausgewählt ist.
- In der Tag-Verwaltung werden alle Tags angezeigt.
- Befinden sich in einer Liste Objekte, für die das Druckrecht nicht vorhanden ist, so erscheint eine entsprechende Fehlermeldung beim Versuch, die Liste auszudrucken.
- Fehlermeldungen sind nur sichtbar, wenn ein Benutzer angemeldet ist.
- Suchergebnisse im Modul “Organisationsstruktur” werden bereits angezeigt, wenn mit der Eingabe des Suchbegriffs begonnen wird.

LightClient in der Web-Ansicht

- Es ist nicht möglich, ohne das Recht “Kann individuelle Passwörter im LightClient anlegen” Passwörter anzulegen.
- In der Tag-Verwaltung des WebClients werden alle Tags angezeigt.
- Der Name “Account” von Formularvorlagen mit diesem Namen wird in der Vorlagenauswahl korrekt angezeigt.
- Bei vererbten Benutzereinstellungen wird angezeigt, von welcher Organisationseinheit die Einstellung vererbt wurde.
- Es können nicht mehrere Tabs mit der gleichen Organisationseinheit angelegt werden.
- Fehlermeldungen sind nur sichtbar, wenn ein Benutzer angemeldet ist.

- Suchergebnisse im Modul “Organisationsstruktur” werden bereits angezeigt, wenn mit der Eingabe des Suchbegriffs begonnen wird.

OfflineClient

- Änderungen des Ablaufdatums einer Datenbank werden korrekt gespeichert und synchronisiert.
- Die Tabs mit den Ergebnissen aus der Schnellsuche können geschlossen werden.
- Ist die Anzahl der Datensätze kleiner als der Wert, der in der Option “Anzahl der initial geladenen Datensätze” definierte ist, so wird die tatsächliche Anzahl der Datensätze angezeigt. Ansonsten wird der definierte Wert angezeigt.
- Beim Öffnen eines Passwortes mit den entsprechenden Rechten wird keine Fehlermeldung angezeigt.

SSO-Agent

- Die Anmeldedaten aus der Offline-Datenbank werden automatisch in die entsprechenden Anwendungen eingefügt.
- Es kann immer nur ein Anmeldefenster gleichzeitig geöffnet sein.

AdminClient

- Bei der Erstinstallation wird beim Speichern der Grundkonfiguration überprüft, ob die notwendige Datenbank angelegt werden konnte. War das nicht möglich, wird die Grundkonfiguration nicht gespeichert und ein Fehler angezeigt und man kann die Einstellungen noch einmal überprüfen.
- Die “Admin-Rolle” wird beim Anlegen einer Datenbank unter Verwendung einer englischen Vorlage richtig übersetzt.
- Die Proxyeinstellungen für Yubico können geändert werden.
- Benutzer mit aktivierter Zwei-Faktor-Authentifizierung können sich nicht anmelden. Es erscheint eine entsprechende Fehlermeldung.
- Die Fehlermeldung, wenn sich der DB-Admin selbst aus einer Organisationseinheit entfernt und diese Änderungen speichern will, wurde angepasst.
- Es werden nur Logeinträge verschickt, die nach der Erstellung der Weiterleitungsregel angefallen sind.
- Im “Ende-zu-Ende”-Modus beim Active Directory Import werden die Rechte entsprechend der Organisationseinheit, in der sich ein importierte Benutzer befindet, korrekt vererbt.
- Eine deaktivierte, aber noch gültige Lizenz kann auch wieder über den Einrichtungsassistenten aktiviert werden.
- Bei einem erfolglosen Password Reset werden die entsprechenden Fehlermeldungen ausgegeben.

Password Safe Mobile App

- Bei der initialen Anmeldung wird bei Eingabe der falschen Zugangsdaten das Passwortfeld eine gewisse Zeit ausgegraut. Erst nach dieser Zeit kann das Passwort erneut eingetragen werden.
- Das Ändern des Passwortes nach Aufforderung verursachte einen Fehler, der die App abstürzen ließ. Das Passwort kann jetzt nach Aufforderung problemlos geändert werden.
- Neu angelegte Passwörter in der Organisationseinheit werden bei zwischenzeitlich deaktiviertem Recht “Kann persönliche Datensätze erstellen” nicht mit dem Server synchronisiert.
- Beim Anzeigen eines One-Time-Passwords werden die ersten und die letzten drei Ziffern mittels eines Leerzeichens getrennt.

- Die App für iOS unterstützt Datenbanken mit 20.000 Datensätzen und mehr.
- In der Password Safe App für iOS wird bei einer Webseite mit einem One-Time-Password keine Fehlermeldung angezeigt, wenn dieses nicht konfiguriert ist.
- Die Autofill-Funktion für die Password Safe App für Android wurde optimiert.
- Beim Anlegen eines neuen Datenbankprofils in der Password Safe App für Android werden alle bereits vorhandenen Passwörter korrekt synchronisiert. Beim Aufruf einer Webseite wird das entsprechende Passwort vorgeschlagen.
- In der Password Safe App für Android generierte und zum Password Safe Server synchronisierte Passwörter werden vom Autofill der App automatisch bei den entsprechenden Webseiten eingetragen.

Add-on

- Die zweistufige Eintragung für die Webseite “https://signin.techsmith.com” funktioniert jetzt auch mittels Browser-Add-on für Google Chrome und Safari.
- Auch wenn die Sitzung des WebClients abgelaufen ist, können Passwörter über das Browser-Add-on noch im WebClient angelegt werden.
- Eine zweistufiges Passwort wird über das Add-on eingetragen, wenn man über den SSO-Agent mit dem Add-on verbunden ist.
- Das Add-on für den Internet Explorer wird nicht mehr unterstützt und ist mit Version 8.11 auch nicht mehr verfügbar.

Version 8.10.0.18473 Hotfix 2

Veröffentlichung

21.01.2021

Kompatibilität

Zum AdminClient der Version 8.10.0.18473 Hotfix 2 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.7.0.18000 Hotfix 3
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.8.0.18002 Hotfix 3
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.9.0.17993 Hotfix 2
- Windows Client Version 8.10.0.18472
- Windows Client Version 8.10.0.18516 Hotfix 1
- Windows Client Version 8.10.0.184736 Hotfix 2

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.7.0.18000 Hotfix 3
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.8.0.18002 Hotfix 3
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.9.0.17993 Hotfix 2
- WebClient Version 8.10.0.18472
- WebClient Version 8.10.0.18516 Hotfix 1
- WebClient Version 8.10.0.184736 Hotfix 2

- Password Safe Mobile Apps 1.18

! Behoben: API-Schnittstelle: Möglichen Umgehung eines aktivierten zweiten Faktors p(banner tip). Es gilt zu beachten, dass es bei der Nutzung von älteren Clients zu Darstellungsfehler im Logbuch kommt. Die Funktionalität des Logbuchs ist aber im vollen Umfang gegeben. Mit einem Update des Clients auf die aktuellste Version tritt dieser Darstellungsfehler nicht mehr auf.

> **Achtung:**
> Da die Technik des **Internet Explorers** veraltet ist, sehen wir uns leider dazu gezwungen, den Support für die das Add-on einzustellen. Es wird seit Version 8.9. nicht mehr weiterentwickelt. Das bedeutet auch, dass keine Fehler mehr behoben werden und kein Support hierfür mehr stattfindet. Die Verwendung des Add-ons erfolgt folglich auf eigene Verantwortung. Ab Version 8.11 wird das Add-on nicht mehr ausgeliefert.

Hotfix 1

Durch die Prüfung eines falschen Rechtes konnten Benutzer zwar eine andere Rechtevorlage für ein OU auswählen, beim Speichern wurde aber immer nur die Standard-Rechtevorlage verwendet.
Hier finden Sie einen Beitrag für weitere Informationen

Neu seit 8.10.0.18464

WebClient

- Passwörter können nun auch mit Anwendungen verbunden werden. Dazu ist im Menü die neue Funktion Password verbinden beim Start hinzugefügt worden. So können Anwendungen verbunden, Internetseiten geöffnet sowie vorhandene Anwendungsverknüpfungen gelöscht werden.
- Für das Einrichten der Password Safe Mobile App wird in den Einstellungen des WebClients bei Kontoeinstellungen des Benutzers ein mobiler Zugang mittels QR-Code angezeigt. Mit der Mobile App kann der QR-Code gescannt werden, um eine Verknüpfung anzulegen und eine Anmeldung durchzuführen.
- Mit der neuen Funktion Einstellungen zurücksetzen können nun in den Kontoeinstellungen die persönlichen Benutzereinstellungen wieder auf den Standardwert zurückgesetzt werden.
- Das Benutzerbild kann nun auch im WebClient bearbeitet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Verbesserung seit 8.10.0.18464

Allgemein

- Active Directory Benutzer können sich nun mittels UPN (User Principal Name) an Password Safe authentifizieren.
- Ein Login auf die Datenbank wird bei abgelaufener Offline-Datenbank (Synchronisation ist nicht mehr möglich) verhindert.
- Wird der Admin aufgefordert, sein Passwort zu ändern, wird jetzt ein Fenster mit der Aufforderung angezeigt, hierfür in den Client zu wechseln.

- Die Auswahl der Add-on-Verbindung wird jetzt in den Optionen über Radio-Buttons eingestellt.
- Beim SSO-Agent wird durch Aktivieren der Option Starte Anwendung minimiert im Benachrichtigungsbereich beim Start nur noch das Symbol im Tray angezeigt.

FullClient

- Die Schnellsuche funktioniert jetzt auch in der Strukturansicht bei den Modulen Passwörter, Dokumente, Anwendungen und Password Reset.
- Meldet sich der Benutzer innerhalb des Ablauf-Zeitraums (180 Tage) nicht an, verlängert sich dieser automatisch wieder um 180 Tage.

WebClient

- Im Modul Anwendungen werden im Menü Starten die mit der Anwendung verbundenen Passwörter angezeigt.
- Im Modul Rolle kann ein Mitglied in der Preview ausgewählt werden und über die Schnellansicht die Daten angezeigt werden.
- Beim Neu-Anlegen eines Passworts in der Strukturansicht kann dieses einer Organisationseinheit zugewiesen werden.
- Es können nun mehrere Neuer Datensatz-Tabs in den Modulen Passwörter, Dokumente, Organisationsstruktur, Rollen und Anwendungen geöffnet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Änderungen seit 8.10.0.18464

FullClient

- Beim Anlegen einer neuen Organisationseinheit ist der Name dieser nun auf 255 Zeichen begrenzt.
- Beim Öffnen eines externen Links wird der Datensatz als Tab im Vordergrund geöffnet.

AdminClient

- In der Server-Exception werden nun zusätzlich die IP-Adresse und der Computername mit ausgegeben.

Behoben in 8.10.0.18464

Allgemein

- Das Datenbank-Timeout greift für SQL-Server nun auch bei Migrationen.
- Beim Client werden gelöschte Benutzer und Rollen beim Verwenden von Rechtevorlagen nicht mehr als Jeder interpretiert.

- Beim OfflineClient können die Tabs der Schnellsuche nun über das X am Passwort geschlossen werden.
- Beim AdminClient wird bei Aktivierung einer neuen Lizenz die vorhandene wieder korrekt deaktiviert.
- Im Web-Modus des LightClients können Passwörter über das Add-on wieder korrekt angelegt werden.
- Beim SSO-Agent wird bei Abbruch des Plausibilitätschecks bei Passwortänderung wird der Username nun wieder korrekt überprüft.

FullClient

- Im Formular-Modul kann man wieder über den Shortcut CTRL+N ein neues Formular anlegen.
- Passwörter können nun unabhängig vom Recht Kann Passwortformularfelder verwalten verdeckt geändert werden.
- Im Logbuch-Modul kann der Typ Active Directory Profil über den jeweiligen Button direkt geöffnet und angezeigt werden.
- Mit der Essential-Lizenz kann das Benachrichtigungsfenster wieder angezeigt werden.
- In der Strukturansicht der Module Passwörter, Dokumente, Anwendungen und Password Reset wird beim Anlegen eines Objekts die Organisationsstruktur korrekt eingetragen, wenn das Recht Kann persönliche Datensätze erstellen deaktiviert ist.
- Die Namen der Passwörter in einer Fehlermeldung beim CSV-Import werden nun wieder korrekt angezeigt.
- Die Passwortliste im Passwort-Modul behält nun auch beim Wechsel zwischen allen Passwörtern und Favoriten das eingestellte Format bei.
- Wenn die Benutzereinstellung Zuletzt geöffnete Tabs wiederherstellen aktiviert ist, werden beim Starten des Formular- und Rollen-Moduls keine zusätzlichen Listen-Tabs mehr hinzugefügt.
- Die Dokumente im Dokumenten-Modul (Office Dokumente Word, Excel und PowerPoint) können nur bearbeitet werden, wenn die dazugehörigen Programme nicht geöffnet sind.
- Im Benachrichtigungsmodul wird eine Siegel-Benachrichtigung mit Klick auf den Button Siegel wieder korrekt angezeigt.
- Die Fehlermeldung bei Siegelbruch-Anfragen für Passwörter mit mehr als einem Passwortfeld wird wieder korrekt angezeigt. Die Fehlermeldung bei Bestätigung für Siegelanfragen bei mehr als einer Bestätigung wurde ebenfalls korrigiert.
- Die benutzerdefinierten Shortcuts funktionieren auch bei geöffneten Datensätzen korrekt.
- Im Organisations-Wizzard wird der Ersteller der Organisationseinheit korrekt in Rechte konfigurieren angezeigt.
- Öffnet man ein Passwort über einen externen Link, können Passwortfelder nicht bearbeitet werden, da diese im Read-Only-Modus sind.
- Bei einer KeePass-Datei werden die importierten Organisationseinheiten unter der ausgewählten Organisationseinheit angelegt.
- Wird ein Benutzer über das Active Directory importiert, kann man beim Benutzer einen User-Typ angeben. Der User-Typ Full / Light wird beim Import wieder korrekt umgesetzt.
- Ein mehrfaches Anmelden mit Registry-Profilen ist nun nicht mehr möglich.
- Bei einer Migration (V7-Datenbank) werden Passwörter in der nächsthöheren Organisationseinheit angelegt, wenn der Ordner mit den Passwörtern beim Import ignoriert wird.
- In der Siegelübersicht werden Benutzer, die Mitglied einer Rolle und gleichzeitig freigabeberechtigt sind, nicht mehr als versiegelt angezeigt.
- Es wird ein erneutes Verbinden des SSO-Agents mit der Datenbank verhindert, wenn die

Anmeldedaten einmal ungültig waren. Außerdem löscht der SSO-Agent abgelaufene Sitzungen oder Anmeldedaten, die ungültig geworden sind. Eine entsprechende Meldung wird angezeigt.
- Bei einer KeePass-Datei werden beim Import die Rechtevorlagen auf importierte Organisationseinheiten korrekt angewendet.

WebClient

- Nach der Bearbeitung von Berechtigungen eines Passworts aktualisiert sich der Status Persönlich / Öffentlich automatisch.
- Ein neues Formular kann mit einem neuen Tag versehen werden. Der Tag wird nach dem Speichern der Vorlage in der Tagverwaltung nach einem Refresh angezeigt.
- In den Modulen kann die Navigation mit den Pfeiltasten durchgeführt und die Schnellsuche via Leertaste angezeigt werden.
- Die Informationen für die Softwarepflege werden bei der Benachrichtigung in der Menüleiste korrekt angezeigt.
- Die Kategorie Sicherheit ist in den Benutzerrechten und Globalen Rechten nicht mehr doppelt vorhanden.
- In der Schnellansicht sind die Checkboxen eines Passworts durch Read-Only vor Veränderungen geschützt.
- Die Fehlermeldung in der Siegelübersicht nach einer Siegelbruchanfrage wird wieder korrekt angezeigt.
- In der Strukturansicht des Passwort-Moduls funktioniert die Schnellsuche im Filter wieder korrekt.
- Ein automatischer Login über das Add-on am WebClient ist jetzt wieder verfügbar.

Add-on

- Der Benutzername wird wieder angezeigt.
- Bei einem fehlerhaften Login wird kein wiederholtes Eintragen der Login-Daten mehr ausgeführt.
- Bei Passwörtern ohne Login-Maske können die Passwörter nicht mehr aufgedeckt werden.

Version 8.10.0.18516 Hotfix 1

Veröffentlichung

30.04.2020

Kompatibilität

Zum AdminClient der Version 8.10.0.18516 Hotfix 1 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18472
- Windows Client Version 8.10.0.18516 Hotfix 1

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.10.0.18472
- WebClient Version 8.10.0.18516 Hotfix 1

- Password Safe Mobile Apps 1.18

✻ Es gilt zu beachten, dass es bei der Nutzung von älteren Clients zu Darstellungsfehler im Logbuch kommt. Die Funktionalität des Logbuchs ist aber im vollen Umfang gegeben. Mit einem Update des Clients auf die aktuellste Version tritt dieser Darstellungsfehler nicht mehr auf.

! **Achtung:**
Da die Technik des **Internet Explorers** veraltet ist, sehen wir uns leider dazu gezwungen, den Support für die das Add-on einzustellen. Es wird seit Version 8.9. nicht mehr weiterentwickelt. Das bedeutet auch, dass keine Fehler mehr behoben werden und kein Support hierfür mehr stattfindet. Die Verwendung des Add-ons erfolgt folglich auf eigene Verantwortung. Ab Version 8.11 wird das Add-on nicht mehr ausgeliefert.

Hotfix 1

Durch die Prüfung eines falschen Rechtes konnten Benutzer zwar eine andere Rechtevorlage für ein OU auswählen, beim Speichern wurde aber immer nur die Standard-Rechtevorlage verwendet.
Hier finden Sie einen Beitrag für weitere Informationen

Neu seit 8.10.0.18464

WebClient

- Passwörter können nun auch mit Anwendungen verbunden werden. Dazu ist im Menü die neue Funktion Password verbinden beim Start hinzugefügt worden. So können Anwendungen verbunden, Internetseiten geöffnet sowie vorhandene Anwendungsverknüpfungen gelöscht werden.
- Für das Einrichten der Password Safe Mobile App wird in den Einstellungen des WebClients bei Kontoeinstellungen des Benutzers ein mobiler Zugang mittels QR-Code angezeigt. Mit der Mobile App kann der QR-Code gescannt werden, um eine Verknüpfung anzulegen und eine Anmeldung durchzuführen.
- Mit der neuen Funktion Einstellungen zurücksetzen können nun in den Kontoeinstellungen die persönlichen Benutzereinstellungen wieder auf den Standardwert zurückgesetzt werden.
- Das Benutzerbild kann nun auch im WebClient bearbeitet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Verbesserung seit 8.10.0.18464

Allgemein

- Active Directory Benutzer können sich nun mittels UPN (User Principal Name) an Password Safe authentifizieren.
- Ein Login auf die Datenbank wird bei abgelaufener Offline-Datenbank (Synchronisation ist nicht mehr möglich) verhindert.
- Wird der Admin aufgefordert, sein Passwort zu ändern, wird jetzt ein Fenster mit der Aufforderung angezeigt, hierfür in den Client zu wechseln.
- Die Auswahl der Add-on-Verbindung wird jetzt in den Optionen über Radio-Buttons eingestellt.
- Beim SSO-Agent wird durch Aktivieren der Option Starte Anwendung minimiert im Benachrichtigungsbereich beim Start nur noch das Symbol im Tray angezeigt.

FullClient

- Die Schnellsuche funktioniert jetzt auch in der Strukturansicht bei den Modulen Passwörter, Dokumente, Anwendungen und Password Reset.

- Meldet sich der Benutzer innerhalb des Ablauf-Zeitraums (180 Tage) nicht an, verlängert sich dieser automatisch wieder um 180 Tage.

WebClient

- Im Modul Anwendungen werden im Menü Starten die mit der Anwendung verbundenen Passwörter angezeigt.
- Im Modul Rolle kann ein Mitglied in der Preview ausgewählt werden und über die Schnellansicht die Daten angezeigt werden.
- Beim Neu-Anlegen eines Passworts in der Strukturansicht kann dieses einer Organisationseinheit zugewiesen werden.
- Es können nun mehrere Neuer Datensatz-Tabs in den Modulen Passwörter, Dokumente, Organisationsstruktur, Rollen und Anwendungen geöffnet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Änderungen seit 8.10.0.18464

FullClient

- Beim Anlegen einer neuen Organisationseinheit ist der Name dieser nun auf 255 Zeichen begrenzt.
- Beim Öffnen eines externen Links wird der Datensatz als Tab im Vordergrund geöffnet.

AdminClient

- In der Server-Exception werden nun zusätzlich die IP-Adresse und der Computername mit ausgegeben.

Behoben in 8.10.0.18464

Allgemein

- Das Datenbank-Timeout greift für SQL-Server nun auch bei Migrationen.
- Beim Client werden gelöschte Benutzer und Rollen beim Verwenden von Rechtevorlagen nicht mehr als Jeder interpretiert.
- Beim OfflineClient können die Tabs der Schnellsuche nun über das X am Passwort geschlossen werden.
- Beim AdminClient wird bei Aktivierung einer neuen Lizenz die vorhandene wieder korrekt deaktiviert.
- Im Web-Modus des LightClients können Passwörter über das Add-on wieder korrekt angelegt werden.
- Beim SSO-Agent wird bei Abbruch des Plausibilitätschecks bei Passwortänderung wird der

Username nun wieder korrekt überprüft.

FullClient

- Im Formular-Modul kann man wieder über den Shortcut CTRL+N ein neues Formular anlegen.
- Passwörter können nun unabhängig vom Recht Kann Passwortformularfelder verwalten verdeckt geändert werden.
- Im Logbuch-Modul kann der Typ Active Directory Profil über den jeweiligen Button direkt geöffnet und angezeigt werden.
- Mit der Essential-Lizenz kann das Benachrichtigungsfenster wieder angezeigt werden.
- In der Strukturansicht der Module Passwörter, Dokumente, Anwendungen und Password Reset wird beim Anlegen eines Objekts die Organisationsstruktur korrekt eingetragen, wenn das Recht Kann persönliche Datensätze erstellen deaktiviert ist.
- Die Namen der Passwörter in einer Fehlermeldung beim CSV-Import werden nun wieder korrekt angezeigt.
- Die Passwortliste im Passwort-Modul behält nun auch beim Wechsel zwischen allen Passwörtern und Favoriten das eingestellte Format bei.
- Wenn die Benutzereinstellung Zuletzt geöffnete Tabs wiederherstellen aktiviert ist, werden beim Starten des Formular- und Rollen-Moduls keine zusätzlichen Listen-Tabs mehr hinzugefügt.
- Die Dokumente im Dokumenten-Modul (Office Dokumente Word, Excel und PowerPoint) können nur bearbeitet werden, wenn die dazugehörigen Programme nicht geöffnet sind.
- Im Benachrichtigungsmodul wird eine Siegel-Benachrichtigung mit Klick auf den Button Siegel wieder korrekt angezeigt.
- Die Fehlermeldung bei Siegelbruch-Anfragen für Passwörter mit mehr als einem Passwortfeld wird wieder korrekt angezeigt. Die Fehlermeldung bei Bestätigung für Siegelanfragen bei mehr als einer Bestätigung wurde ebenfalls korrigiert.
- Die benutzerdefinierten Shortcuts funktionieren auch bei geöffneten Datensätzen korrekt.
- Im Organisations-Wizzard wird der Ersteller der Organisationseinheit korrekt in Rechte konfigurieren angezeigt.
- Öffnet man ein Passwort über einen externen Link, können Passwortfelder nicht bearbeitet werden, da diese im Read-Only-Modus sind.
- Bei einer KeePass-Datei werden die importierten Organisationseinheiten unter der ausgewählten Organisationseinheit angelegt.
- Wird ein Benutzer über das Active Directory importiert, kann man beim Benutzer einen User-Typ angeben. Der User-Typ Full / Light wird beim Import wieder korrekt umgesetzt.
- Ein mehrfaches Anmelden mit Registry-Profilen ist nun nicht mehr möglich.
- Bei einer Migration (V7-Datenbank) werden Passwörter in der nächsthöheren Organisationseinheit angelegt, wenn der Ordner mit den Passwörtern beim Import ignoriert wird.
- In der Siegelübersicht werden Benutzer, die Mitglied einer Rolle und gleichzeitig freigabeberechtigt sind, nicht mehr als versiegelt angezeigt.
- Es wird ein erneutes Verbinden des SSO-Agents mit der Datenbank verhindert, wenn die Anmeldedaten einmal ungültig waren. Außerdem löscht der SSO-Agent abgelaufene Sitzungen oder Anmeldedaten, die ungültig geworden sind. Eine entsprechende Meldung wird angezeigt.
- Bei einer KeePass-Datei werden beim Import die Rechtevorlagen auf importierte Organisationseinheiten korrekt angewendet.

WebClient

- Nach der Bearbeitung von Berechtigungen eines Passworts aktualisiert sich der Status Persönlich

/ Öffentlich automatisch.
- Ein neues Formular kann mit einem neuen Tag versehen werden. Der Tag wird nach dem Speichern der Vorlage in der Tagverwaltung nach einem Refresh angezeigt.
- In den Modulen kann die Navigation mit den Pfeiltasten durchgeführt und die Schnellsuche via Leertaste angezeigt werden.
- Die Informationen für die Softwarepflege werden bei der Benachrichtigung in der Menüleiste korrekt angezeigt.
- Die Kategorie Sicherheit ist in den Benutzerrechten und Globalen Rechten nicht mehr doppelt vorhanden.
- In der Schnellansicht sind die Checkboxen eines Passworts durch Read-Only vor Veränderungen geschützt.
- Die Fehlermeldung in der Siegelübersicht nach einer Siegelbruchanfrage wird wieder korrekt angezeigt.
- In der Strukturansicht des Passwort-Moduls funktioniert die Schnellsuche im Filter wieder korrekt.
- Ein automatischer Login über das Add-on am WebClient ist jetzt wieder verfügbar.

Add-on

- Der Benutzername wird wieder angezeigt.
- Bei einem fehlerhaften Login wird kein wiederholtes Eintragen der Login-Daten mehr ausgeführt.
- Bei Passwörtern ohne Login-Maske können die Passwörter nicht mehr aufgedeckt werden.

Version 8.10.0.18472

Veröffentlichung

14.02.2020

Kompatibilität

Zum AdminClient der Version 8.10.0.18472 sind folgende Client Versionen kompatibel:

- Windows Client Version 8.7.0.16387 Hotfix 1
- Windows Client Version 8.7.0.16698 Hotfix 2
- Windows Client Version 8.8.0.17146
- Windows Client Version 8.8.0.17168 Hotfix 1
- Windows Client Version 8.8.0.17596 Hotfix 2
- Windows Client Version 8.9.0.17656
- Windows Client Version 8.9.0.17702 Hotfix 1
- Windows Client Version 8.10.0.18472

- WebClient Version 8.7.0.16387 Hotfix 1
- WebClient Version 8.7.0.16698 Hotfix 2
- WebClient Version 8.8.0.17146
- WebClient Version 8.8.0.17168 Hotfix 1
- WebClient Version 8.8.0.17596 Hotfix 2
- WebClient Version 8.9.0.17656
- WebClient Version 8.9.0.17702 Hotfix 1
- WebClient Version 8.10.0.18472

- Password Safe Mobile Apps 1.18

✻ Es gilt zu beachten, dass es bei der Nutzung von älteren Clients zu Darstellungsfehler im Logbuch kommt. Die Funktionalität des Logbuchs ist aber im vollen Umfang gegeben. Mit einem Update des Clients auf die aktuellste Version tritt dieser Darstellungsfehler nicht mehr auf.

! **Achtung:**
Da die Technik des **Internet Explorers** veraltet ist, sehen wir uns leider dazu gezwungen, den Support für die das Add-on einzustellen. Es wird seit Version 8.9. nicht mehr weiterentwickelt. Das bedeutet auch, dass keine Fehler mehr behoben werden und kein Support hierfür mehr stattfindet. Die Verwendung des Add-ons erfolgt folglich auf eigene Verantwortung. Ab Version 8.11 wird das Add-on nicht mehr ausgeliefert.

Neu

WebClient

- Passwörter können nun auch mit Anwendungen verbunden werden. Dazu ist im Menü die neue Funktion Password verbinden beim Start hinzugefügt worden. So können Anwendungen verbunden, Internetseiten geöffnet sowie vorhandene Anwendungsverknüpfungen gelöscht werden.
- Für das Einrichten der Password Safe Mobile App wird in den Einstellungen des WebClients bei Kontoeinstellungen des Benutzers ein mobiler Zugang mittels QR-Code angezeigt. Mit der Mobile App kann der QR-Code gescannt werden, um eine Verknüpfung anzulegen und eine Anmeldung durchzuführen.
- Mit der neuen Funktion Einstellungen zurücksetzen können nun in den Kontoeinstellungen die persönlichen Benutzereinstellungen wieder auf den Standardwert zurückgesetzt werden.
- Das Benutzerbild kann nun auch im WebClient bearbeitet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Verbesserung

Allgemein

- Active Directory Benutzer können sich nun mittels UPN (User Principal Name) an Password Safe authentifizieren.
- Ein Login auf die Datenbank wird bei abgelaufener Offline-Datenbank (Synchronisation ist nicht mehr möglich) verhindert.
- Wird der Admin aufgefordert, sein Passwort zu ändern, wird jetzt ein Fenster mit der Aufforderung angezeigt, hierfür in den Client zu wechseln.
- Die Auswahl der Add-on-Verbindung wird jetzt in den Optionen über Radio-Buttons eingestellt.
- Beim SSO-Agent wird durch Aktivieren der Option Starte Anwendung minimiert im Benachrichtigungsbereich beim Start nur noch das Symbol im Tray angezeigt.

FullClient

- Die Schnellsuche funktioniert jetzt auch in der Strukturansicht bei den Modulen Passwörter, Dokumente, Anwendungen und Password Reset.
- Meldet sich der Benutzer innerhalb des Ablauf-Zeitraums (180 Tage) nicht an, verlängert sich dieser automatisch wieder um 180 Tage.

WebClient

- Im Modul Anwendungen werden im Menü Starten die mit der Anwendung verbundenen Passwörter angezeigt.

- Im Modul Rolle kann ein Mitglied in der Preview ausgewählt werden und über die Schnellansicht die Daten angezeigt werden.
- Beim Neu-Anlegen eines Passworts in der Strukturansicht kann dieses einer Organisationseinheit zugewiesen werden.
- Es können nun mehrere Neuer Datensatz-Tabs in den Modulen Passwörter, Dokumente, Organisationsstruktur, Rollen und Anwendungen geöffnet werden.

LightClient

- Es kann nun Autologin aktiviert werden.
- Das Passwort kann nun geändert werden.
- Im Web-Modus können nun vorhandene Organisationseinheiten per mittlere Maustaste oder durch ALT+W geschlossen werden.
- Es kann nun auch im Web-Modus die Hauptorganisationseinheit hinzugefügt werden.

Änderungen

FullClient

- Beim Anlegen einer neuen Organisationseinheit ist der Name dieser nun auf 255 Zeichen begrenzt.
- Beim Öffnen eines externen Links wird der Datensatz als Tab im Vordergrund geöffnet.

AdminClient

- In der Server-Exception werden nun zusätzlich die IP-Adresse und der Computername mit ausgegeben.

Behoben

Allgemein

- Das Datenbank-Timeout greift für SQL-Server nun auch bei Migrationen.
- Beim Client werden gelöschte Benutzer und Rollen beim Verwenden von Rechtevorlagen nicht mehr als Jeder interpretiert.
- Beim OfflineClient können die Tabs der Schnellsuche nun über das X am Passwort geschlossen werden.
- Beim AdminClient wird bei Aktivierung einer neuen Lizenz die vorhandene wieder korrekt deaktiviert.
- Im Web-Modus des LightClients können Passwörter über das Add-on wieder korrekt angelegt werden.
- Beim SSO-Agent wird bei Abbruch des Plausibilitätschecks bei Passwortänderung wird der Username nun wieder korrekt überprüft.

FullClient

- Im Formular-Modul kann man wieder über den Shortcut CTRL+N ein neues Formular anlegen.
- Passwörter können nun unabhängig vom Recht Kann Passwortformularfelder verwalten verdeckt geändert werden.

- Im Logbuch-Modul kann der Typ Active Directory Profil über den jeweiligen Button direkt geöffnet und angezeigt werden.
- Mit der Essential-Lizenz kann das Benachrichtigungsfenster wieder angezeigt werden.
- In der Strukturansicht der Module Passwörter, Dokumente, Anwendungen und Password Reset wird beim Anlegen eines Objekts die Organisationsstruktur korrekt eingetragen, wenn das Recht Kann persönliche Datensätze erstellen deaktiviert ist.
- Die Namen der Passwörter in einer Fehlermeldung beim CSV-Import werden nun wieder korrekt angezeigt.
- Die Passwortliste im Passwort-Modul behält nun auch beim Wechsel zwischen allen Passwörtern und Favoriten das eingestellte Format bei.
- Wenn die Benutzereinstellung Zuletzt geöffnete Tabs wiederherstellen aktiviert ist, werden beim Starten des Formular- und Rollen-Moduls keine zusätzlichen Listen-Tabs mehr hinzugefügt.
- Die Dokumente im Dokumenten-Modul (Office Dokumente Word, Excel und PowerPoint) können nur bearbeitet werden, wenn die dazugehörigen Programme nicht geöffnet sind.
- Im Benachrichtigungsmodul wird eine Siegel-Benachrichtigung mit Klick auf den Button Siegel wieder korrekt angezeigt.
- Die Fehlermeldung bei Siegelbruch-Anfragen für Passwörter mit mehr als einem Passwortfeld wird wieder korrekt angezeigt. Die Fehlermeldung bei Bestätigung für Siegelanfragen bei mehr als einer Bestätigung wurde ebenfalls korrigiert.
- Die benutzerdefinierten Shortcuts funktionieren auch bei geöffneten Datensätzen korrekt.
- Im Organisations-Wizzard wird der Ersteller der Organisationseinheit korrekt in Rechte konfigurieren angezeigt.
- Öffnet man ein Passwort über einen externen Link, können Passwortfelder nicht bearbeitet werden, da diese im Read-Only-Modus sind.
- Bei einer KeePass-Datei werden die importierten Organisationseinheiten unter der ausgewählten Organisationseinheit angelegt.
- Wird ein Benutzer über das Active Directory importiert, kann man beim Benutzer einen User-Typ angeben. Der User-Typ Full / Light wird beim Import wieder korrekt umgesetzt.
- Ein mehrfaches Anmelden mit Registry-Profilen ist nun nicht mehr möglich.
- Bei einer Migration (V7-Datenbank) werden Passwörter in der nächsthöheren Organisationseinheit angelegt, wenn der Ordner mit den Passwörtern beim Import ignoriert wird.
- In der Siegelübersicht werden Benutzer, die Mitglied einer Rolle und gleichzeitig freigabeberechtigt sind, nicht mehr als versiegelt angezeigt.
- Es wird ein erneutes Verbinden des SSO-Agents mit der Datenbank verhindert, wenn die Anmeldedaten einmal ungültig waren. Außerdem löscht der SSO-Agent abgelaufene Sitzungen oder Anmeldedaten, die ungültig geworden sind. Eine entsprechende Meldung wird angezeigt.
- Bei einer KeePass-Datei werden beim Import die Rechtevorlagen auf importierte Organisationseinheiten korrekt angewendet.

WebClient

- Nach der Bearbeitung von Berechtigungen eines Passworts aktualisiert sich der Status Persönlich / Öffentlich automatisch.
- Ein neues Formular kann mit einem neuen Tag versehen werden. Der Tag wird nach dem Speichern der Vorlage in der Tagverwaltung nach einem Refresh angezeigt.
- In den Modulen kann die Navigation mit den Pfeiltasten durchgeführt und die Schnellsuche via Leertaste angezeigt werden.
- Die Informationen für die Softwarepflege werden bei der Benachrichtigung in der Menüleiste

korrekt angezeigt.
- Die Kategorie Sicherheit ist in den Benutzerrechten und Globalen Rechten nicht mehr doppelt vorhanden.
- In der Schnellansicht sind die Checkboxen eines Passworts durch Read-Only vor Veränderungen geschützt.
- Die Fehlermeldung in der Siegelübersicht nach einer Siegelbruchanfrage wird wieder korrekt angezeigt.
- In der Strukturansicht des Passwort-Moduls funktioniert die Schnellsuche im Filter wieder korrekt.
- Ein automatischer Login über das Add-on am WebClient ist jetzt wieder verfügbar.

Add-on

- Der Benutzername wird wieder angezeigt.
- Bei einem fehlerhaften Login wird kein wiederholtes Eintragen der Login-Daten mehr ausgeführt.
- Bei Passwörtern ohne Login-Maske können die Passwörter nicht mehr aufgedeckt werden.

Drittanbieter Lizenzen

Here you can find all used 3rd party libraries for MATESO Password Safe.

Table of Content

- Autofac.WebApi2 (Version: 6.1.0)
- Autofac (Version: 6.3.0)
- Castle.Core (Version: 4.4.1)
- CliWrap (Version: 3.4.1)
- DeepEqual (Version: 2.0.0)
- EntityFramework.SqlServerCompact (Version: 6.4.4)
- EntityFramework (Version: 6.4.4)
- Esprima (Version: 2.1.2)
- FaviconFetcher (Version: 1.2.0)
- Fido2 (Version: 2.0.2)
- Fleck (Version: 1.2.0)
- Hardcodet.NotifyIcon.Wpf (Version: 1.1.0)
- IPAddressRange (Version: 4.2.0)
- IdentityModel.OidcClient (Version: 5.0.0)
- IdentityModel (Version: 6.0.0)
- InputSimulator (Version: 1.0.4.0)
- LinqKit.Core (Version: 1.2.0)
- MailKit (Version: 3.1.1)
- MaxMind.GeoIP2 (Version: 5.1.0)
- MessagePack (Version: 2.3.85)
- Newtonsoft.Json (Version: 13.0.1)
- NoGit (Version: 0.1.0)
- Node.js (Version: 5.3.0)
- PCSC (Version: 5.1.0)
- PeterO.Cbor (Version: 4.5.2)
- Pkcs11Interop (Version: 5.1.2)
- Portable.BouncyCastle (Version: 1.9.0)
- PriorityQueue (Version: 0.1.0)
- PuTTY (Version: 0.76)
- QRCoder (Version: 1.4.3)
- Radius (Version: 2.0.0.2)
- SSH.NET (Version: 2020.0.1)
- SharpVectors.Reloaded (Version: 1.7.7)
- SuperSocket.ClientEngine.Core (Version: 0.10.0)
- Tanneryd.BulkOperations.EF6 (Version: 1.4.1)
- UAParser (Version: 3.1.47)
- WebSocket4Net (Version: 0.15.2)
- WebSocketSharp (Version: 1.0.3-rc11)
- Z.EntityFramework.Plus.EF6 (Version: 6.13.10)
- xxHash4net (Version: 1.2.0)

Licenses

Autofac.WebApi2 (Version: 6.1.0)
Authors: Autofac Contributors
URL: https://autofac.org/

The MIT License (MIT)

Copyright © 2014 Autofac Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

———————————————————————————————————————

Autofac (Version: 6.3.0)
Authors: Autofac Contributors
URL: https://autofac.org/

The MIT License (MIT)

Copyright © 2015 Autofac Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Castle.Core (Version: 4.4.1)
Authors: Castle Project Contributors
URL: http://www.castleproject.org/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of

Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty,

indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2004-2020 Castle Project – http://www.castleproject.org/ Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

CliWrap (Version: 3.4.1)
Authors: Tyrrrz
URL: https://github.com/Tyrrrz/CliWrap

The MIT License (MIT)

Copyright © Oleksii Holub

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DeepEqual (Version: 2.0.0)

Authors: James Foster
URL: http://github.com/jamesfoster/DeepEqual

The MIT License (MIT)

James Foster 2018

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

EntityFramework.SqlServerCompact (Version: 6.4.4)
Authors: Microsoft
URL: http://go.microsoft.com/fwlink/?LinkID=263480

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on

(or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with

Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. © Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

EntityFramework (Version: 6.4.4)
Authors: Microsoft
URL: http://go.microsoft.com/fwlink/?LinkID=263480

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii)

beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that

such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. © Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Esprima (Version: 2.1.2)
Authors: Sebastien Ros
URL: https://github.com/sebastienros/esprima-dotnet

BSD-3-Clause

Sebastien Ros

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation and/or
other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors
may be used to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FaviconFetcher (Version: 1.2.0)
Authors: Nathan Belue
URL: https://github.com/ComputerGhost/FaviconFetcher

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Fido2 (Version: 2.0.2)
Authors: Fido2
URL: https://github.com/abergs/fido2-net-lib

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Fleck (Version: 1.2.0)
Authors: statenjason
URL: https://github.com/statianzo/Fleck

The MIT License (MIT)

Copyright Jason Staten 2010-2018. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

———————————————————————————————————————

Hardcodet.NotifyIcon.Wpf (Version: 1.1.0)
Authors: Philipp Sumi, Robin Krom, Jan Karger
URL: https://github.com/hardcodet/wpf-notifyicon

The Code Project Open License (CPOL) 1.02

Copyright © 2009-2021 Philipp Sumi

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are: * Source Code and Executable Files can be used in commercial applications; * Source Code and Executable Files can be redistributed; and * Source Code can be modified to create derivative works. * No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is
provided “as-is”. * The Article accompanying the Work may not be distributed or republished without the Author’s
consent
This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License (“Author”).

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE
(“LICENSE”). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK
OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS
OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN

CONSIDERATION OF YOUR
ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF
THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK. 1. Definitions. 1. “Articles” means, collectively, all articles written by Author which describes how the Source
Code and Executable Files for the Work may be used by a user. 2. “Author” means the individual or entity that offers the Work under the terms of this License.

3. “Derivative Work” means a work based upon the Work or upon the Work and other pre-existing works. 4. “Executable Files” refer to the executables, binary files, configuration and any required data files included in the Work. 5. “Publisher” means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You. 6. “Source Code” refers to the collection of source code and configuration files used to create the Executable Files. 7. “Standard Version” refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author. 8. “Work” refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles. 9. “You” is you, an individual or entity wishing to use the Work and exercise your rights under this License. 2. Fair Use/ Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws. 3. License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below: 1. You may use the standard version of the Source Code or Executable Files in Your own applications. 2. You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License. 3. You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file. 4. You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution. 5. The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author’s consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author. Any subroutines or modules supplied by You and linked into the Source Code or Executable Files of this Work shall not be considered part of this Work and will not be subject to the terms of this License. 4. Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work. 5. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions: 1. You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files. 2. You agree not to advertise or in any way imply that this Work is a product of Your own. 3. The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author. 4. You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented. 5. You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code

agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License. 6. You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work. 6. Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS. 7. Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You. 8. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 9. Termination. 1. This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License. 2. If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically. 3. Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above. 10. Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice 11. Miscellaneous 1. This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author. 2. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable. 3. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in

writing and signed by the party to be charged with such waiver or consent. 4. This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

IPAddressRange (Version: 4.2.0)
Authors: J.Sakamoto
URL: https://github.com/jsakamoto/ipaddressrange/

Copyright © 2012-2021 J.Sakamoto, Mozilla Public License 2.0

Mozilla Public License Version 2.0

1. Definitions 1.1. “Contributor” means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software. 1.2. “Contributor Version” means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor’s Contribution. 1.3. “Contribution” means Covered Software of a particular Contributor. 1.4. “Covered Software” means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof. 1.5. “Incompatible With Secondary Licenses” means (a) that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or (b) that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License. 1.6. “Executable Form” means any form of the work other than Source Code Form. 1.7. “Larger Work” means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software. 1.8. “License” means this document. 1.9. “Licensable” means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License. 1.10. “Modifications” means any of the following: (a) any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or (b) any new file in Source Code Form that contains any Covered Software. 1.11. “Patent Claims” of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version. 1.12. “Secondary License” means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses. 1.13. “Source Code Form” means the form of the work preferred for making modifications. 1.14. “You” (or “Your”) means an individual or a legal entity exercising rights under this License. For legal entities, “You” includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity. 2. License Grants and Conditions 2.1. Grants Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license: (a) under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and (b) under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution. 2.3. Limitations on Grant Scope The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor: (a) for any code that a Contributor has removed from Covered Software; or (b) for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or © under Patent Claims infringed by Covered Software in the absence of its Contributions. This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4). 2.4. Subsequent Licenses No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3). 2.5. Representation Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License. 2.6. Fair Use This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents. 2.7. Conditions Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1. 3. Responsibilities 3.1. Distribution of Source Form All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form. 3.2. Distribution of Executable Form If You distribute Covered Software in Executable Form then: (a) such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and (b) You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License. 3.3. Distribution of a Larger Work You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s). 3.4. Notices You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies. 3.5. Application of Additional Terms You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction. 4. Inability to Comply Due to Statute or Regulation If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except

to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it. 5. Termination 5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice. 5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate. 5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination. 6. Disclaimer of Warranty Covered Software is provided under this License on an “as is” basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer. 7. Limitation of Liability Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party’s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You. 8. Litigation Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims. 9. Miscellaneous This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor. 10. Versions of the License 10.1. New Versions Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number. 10.2. Effect of New Versions You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward. 10.3. Modified Versions If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License). 10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the

License, the notice described in Exhibit B of this License must be attached. Exhibit A – Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B – “Incompatible With Secondary Licenses” Notice

This Source Code Form is “Incompatible With Secondary Licenses”, as defined by the Mozilla Public License, v. 2.0.

IdentityModel.OidcClient (Version: 5.0.0)
Authors: Dominick Baier, Brock Allen

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or

its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work

and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

IdentityModel (Version: 6.0.0)
Authors: Dominick Baier, Brock Allen
URL: https://github.com/IdentityModel/IdentityModel

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on

(or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with

Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

InputSimulator (Version: 1.0.4.0)
Authors: Michael Noonan
URL: http://inputsimulator.codeplex.com

The MIT License (MIT)

Copyright 2009-2013

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LinqKit.Core (Version: 1.2.0)
Authors: Joseph Albahari, Tomas Petricek, Scott Smith, Tuomas Hietanen, Stef Heyenrath
URL: https://github.com/scottksmith95/LINQKit

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MailKit (Version: 3.1.1)
Authors: Jeffrey Stedfast
URL: http://www.mimekit.net/

The MIT License (MIT)

.NET Foundation and Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MaxMind.GeoIP2 (Version: 5.1.0)
Authors: MaxMind.GeoIP2
URL: https://github.com/maxmind/GeoIP2-dotnet

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this

definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR

PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

MessagePack (Version: 2.3.85)
Authors: neuecc, aarnott
URL: https://github.com/neuecc/MessagePack-CSharp

The MIT License (MIT)

© Yoshifumi Kawai and contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Newtonsoft.Json (Version: 13.0.1)
Authors: James Newton-King
URL: https://www.newtonsoft.com/json

The MIT License (MIT)

Copyright © James Newton-King 2008

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NoGit (Version: 0.1.0)
Authors: Pavel Nezhencev
URL: https://github.com/whyleee/nogit

The MIT License (MIT)

© 2015 Pavel Nezhencev

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

———————————————————————————————————————

Node.js (Version: 5.3.0)
Authors: Node.js Foundation
URL: https://nodejs.org/

Node.js is licensed for use as follows:

“”“
Copyright Node.js contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.
“”“

This license applies to parts of Node.js originating from the
https://github.com/joyent/node repository:

“”“

Copyright Joyent, Inc. and other Node contributors. All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
“”“

The Node.js license applies to all parts of Node.js that are not externally maintained libraries.

The externally maintained libraries used by Node.js are:

- V8, located at deps/v8. V8’s license follows: “”“ This license applies to all parts of V8 that are not externally maintained libraries. The externally maintained libraries used by V8 are:

– PCRE test suite, located in test/mjsunit/third_party/regexp-pcre.js. This is based on the test suite from PCRE-7.3, which is copyrighted by the University of Cambridge and Google, Inc. The copyright notice and license are embedded in regexp-pcre.js. – Layout tests, located in test/mjsunit/third_party. These are based on layout tests from webkit.org which are copyrighted by Apple Computer, Inc. and released under a 3-clause BSD license. – Strongtalk assembler, the basis of the files assembler-arm-inl.h, assembler-arm.cc, assembler-arm.h, assembler-ia32-inl.h, assembler-ia32.cc, assembler-ia32.h, assembler-x64-inl.h, assembler-x64.cc, assembler-x64.h, assembler-mips-inl.h, assembler-mips.cc, assembler-mips.h, assembler.cc and assembler.h. This code is copyrighted by Sun Microsystems Inc. and released under a 3-clause BSD license. – Valgrind client API header, located at third_party/valgrind/valgrind.h This is release under the BSD license. These libraries have their own licenses; we recommend you read them, as their terms may differ from the terms below. Copyright 2006-2012, the V8 project authors. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- C-Ares, an asynchronous DNS client, located at deps/cares. C-Ares license follows: “”“ /* Copyright 1998 by the Massachusetts Institute of Technology. * * Permission to use, copy, modify, and distribute this * software and its documentation for any purpose and without * fee is hereby granted, provided that the above copyright * notice appear in all copies and that both that copyright * notice and this permission notice appear in supporting * documentation, and that the name of M.I.T. not be used in * advertising or publicity pertaining to distribution of the * software without specific, written prior permission. * M.I.T. makes no representations about the suitability of * this software for any purpose. It is provided “as is” * without express or implied warranty. “”“

- OpenSSL located at deps/openssl. OpenSSL is cryptographic software written by Eric Young (eay@cryptsoft.com) to provide SSL/TLS encryption. OpenSSL’s license follows: “”“ /* == * Copyright © 1998-2011 The OpenSSL Project. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in * the documentation and/or other materials provided with the * distribution. * * 3. All advertising materials mentioning features or use of this * software must display the following acknowledgment: * “This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit. (http://www.openssl.org/)” * * 4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to * endorse or promote products derived from this software without * prior written permission. For written permission, please contact * openssl-core@openssl.org. * * 5. Products derived from this software may not be called “OpenSSL” * nor may “OpenSSL” appear in their names without prior written * permission of the OpenSSL Project. * * 6. Redistributions of any form whatsoever must retain the following * acknowledgment: * “This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit (http://www.openssl.org/)” * * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS’‘ AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED * OF THE POSSIBILITY OF SUCH DAMAGE. * == * * This product includes cryptographic software written by Eric Young * (eay@cryptsoft.com). This product includes software written by Tim * Hudson (tjh@cryptsoft.com). * */ “”“

- HTTP Parser, located at deps/http_parser. HTTP Parser's license follows: “”“ http_parser.c is based on src/http/ngx_http_parse.c from NGINX copyright Igor Sysoev.

Additional changes are licensed under the same terms as NGINX and copyright Joyent, Inc. and other Node contributors. All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- ESLint is located at tools/eslint. ESLint's license follows: “”“ ESLint Copyright © 2013 Nicholas C. Zakas. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- tools/cpplint.py is a C++ linter. Its license follows: “”“ # Copyright © 2009 Google Inc. All rights reserved. # # Redistribution and use in source and binary forms, with or without # modification, are permitted provided that the following conditions are # met: # # * Redistributions of source code must retain the above copyright # notice, this list of conditions and the following disclaimer. # * Redistributions in binary form must reproduce the above # copyright notice, this list of conditions and the following disclaimer # in the documentation and/or other materials provided with the # distribution. # * Neither the name of Google Inc. nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR # A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT # OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, # SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT # LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, # DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY # THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE # OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- lib/punycode.js is copyright 2011 Mathias Bynens and released under the MIT license. “”“ * Punycode.js * Copyright 2011 Mathias Bynens * Available under MIT license “”“

- tools/gyp. GYP is a meta-build system. GYP’s license follows: “”“ Copyright © 2009 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. “”“

- Zlib at deps/zlib. zlib’s license follows: “”“ /* zlib.h — interface of the ‘zlib’ general purpose compression library version 1.2.8, April 28th, 2013

Copyright © 1995-2013 Jean-loup Gailly and Mark Adler This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu */ “”“

- npm is a package manager program located at deps/npm. npm’s license follows: “”“ Copyright © Isaac Z. Schlueter All rights reserved.

npm is released under the Artistic 2.0 License. The text of the License follows: ———— The Artistic License 2.0 Copyright © 2000-2006, The Perl Foundation. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. Preamble This license establishes the terms under which a given free software Package may be copied, modified, distributed, and/or redistributed. The intent is that the Copyright Holder maintains some artistic control over the development of that Package while still keeping the Package available as open source and free software. You are always permitted to make

arrangements wholly outside of this license directly with the Copyright Holder of a given Package. If the terms of this license do not permit the full use that you propose to make of the Package, you should contact the Copyright Holder and seek a different licensing arrangement. Definitions “Copyright Holder” means the individual(s) or organization(s) named in the copyright notice for the entire Package. “Contributor” means any party that has contributed code or other material to the Package, in accordance with the Copyright Holder’s procedures. “You” and “your” means any person who would like to copy, distribute, or modify the Package. “Package” means the collection of files distributed by the Copyright Holder, and derivatives of that collection and/or of those files. A given Package may consist of either the Standard Version, or a Modified Version. “Distribute” means providing a copy of the Package or making it accessible to anyone else, or in the case of a company or organization, to others outside of your company or organization. “Distributor Fee” means any fee that you charge for Distributing this Package or providing support for this Package to another party. It does not mean licensing fees. “Standard Version” refers to the Package if it has not been modified, or has been modified only in ways explicitly requested by the Copyright Holder. “Modified Version” means the Package, if it has been changed, and such changes were not explicitly requested by the Copyright Holder. “Original License” means this Artistic License as Distributed with the Standard Version of the Package, in its current version or as it may be modified by The Perl Foundation in the future. “Source” form means the source code, documentation source, and configuration files for the Package. “Compiled” form means the compiled bytecode, object code, binary, or any other form resulting from mechanical transformation or translation of the Source form. Permission for Use and Modification Without Distribution (1) You are permitted to use the Standard Version and create and use Modified Versions for any purpose without restriction, provided that you do not Distribute the Modified Version. Permissions for Redistribution of the Standard Version (2) You may Distribute verbatim copies of the Source form of the Standard Version of this Package in any medium without restriction, either gratis or for a Distributor Fee, provided that you duplicate all of the original copyright notices and associated disclaimers. At your discretion, such verbatim copies may or may not include a Compiled form of the Package. (3) You may apply any bug fixes, portability changes, and other modifications made available from the Copyright Holder. The resulting Package will still be considered the Standard Version, and as such will be subject to the Original License. Distribution of Modified Versions of the Package as Source (4) You may Distribute your Modified Version as Source (either gratis or for a Distributor Fee, and with or without a Compiled form of the Modified Version) provided that you clearly document how it differs from the Standard Version, including, but not limited to, documenting any non-standard features, executables, or modules, and provided that you do at least ONE of the following: (a) make the Modified Version available to the Copyright Holder of the Standard Version, under the Original License, so that the Copyright Holder may include your modifications in the Standard Version. (b) ensure that installation of your Modified Version does not prevent the user installing or running the Standard Version. In addition, the Modified Version must bear a name that is different from the name of the Standard Version. © allow anyone who receives a copy of the Modified Version to make the Source form of the Modified Version available to others under (i) the Original License or (ii) a license that permits the licensee to freely copy, modify and redistribute the Modified Version using the same licensing terms that apply to the copy that the licensee received, and requires that the Source form of the Modified Version, and of any works derived from it, be made freely available in that license fees are prohibited but Distributor Fees are allowed. Distribution of Compiled Forms of the Standard Version or Modified Versions without the Source (5) You may Distribute Compiled forms of the Standard Version without the Source, provided that you include complete instructions on how to get the Source of the Standard Version. Such instructions must be valid at the time of your distribution. If these instructions, at any time while you are carrying out such distribution, become invalid, you must provide new instructions on demand or cease further distribution. If you provide valid instructions or cease distribution within thirty days after you become aware that the instructions are invalid, then you do not forfeit any of your rights under this license. (6) You may Distribute a Modified Version in Compiled form without the Source, provided that you comply with Section 4 with respect to the Source of the Modified Version. Aggregating or Linking the Package (7) You may

aggregate the Package (either the Standard Version or Modified Version) with other packages and Distribute the resulting aggregation provided that you do not charge a licensing fee for the Package. Distributor Fees are permitted, and licensing fees for other components in the aggregation are permitted. The terms of this license apply to the use and Distribution of the Standard or Modified Versions as included in the aggregation. (8) You are permitted to link Modified and Standard Versions with other works, to embed the Package in a larger work of your own, or to build stand-alone binary or bytecode versions of applications that include the Package, and Distribute the result without restriction, provided the result does not expose a direct interface to the Package. Items That are Not Considered Part of a Modified Version (9) Works (including, but not limited to, modules and scripts) that merely extend or make use of the Package, do not, by themselves, cause the Package to be a Modified Version. In addition, such works are not considered parts of the Package itself, and are not subject to the terms of this license. General Provisions (10) Any use, modification, and distribution of the Standard or Modified Versions is governed by this Artistic License. By using, modifying or distributing the Package, you accept this license. Do not use, modify, or distribute the Package, if you do not accept this license. (11) If your Modified Version has been derived from a Modified Version made by someone other than you, you are nevertheless required to ensure that your Modified Version complies with the requirements of this license. (12) This license does not grant you the right to use any trademark, service mark, tradename, or logo of the Copyright Holder. (13) This license includes the non-exclusive, worldwide, free-of-charge patent license to make, have made, use, offer to sell, sell, import and otherwise transfer the Package with respect to any patent claims licensable by the Copyright Holder that are necessarily infringed by the Package. If you institute patent litigation (including a cross-claim or counterclaim) against any party alleging that the Package constitutes direct or contributory patent infringement, then this Artistic License to you shall terminate on the date that such litigation is filed. (14) Disclaimer of Warranty: THE PACKAGE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS “AS IS’ AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT ARE DISCLAIMED TO THE EXTENT PERMITTED BY YOUR LOCAL LAW. UNLESS REQUIRED BY LAW, NO COPYRIGHT HOLDER OR CONTRIBUTOR WILL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING IN ANY WAY OUT OF THE USE OF THE PACKAGE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ———— “Node.js” and “node” trademark Joyent, Inc. npm is not officially part of the Node.js project, and is neither owned by nor officially affiliated with Joyent, Inc. Packages published in the npm registry (other than the Software and its included dependencies) are not part of npm itself, are the sole property of their respective maintainers, and are not covered by this license. “npm Logo” created by Mathias Pettersson and Brian Hammond, used with permission. “Gubblebum Blocky” font Copyright © by Tjarda Koster, http://jelloween.deviantart.com included for use in the npm website and documentation, used with permission. This program uses several Node.js modules contained in the node_modules/ subdirectory, according to the terms of their respective licenses. “”“

- tools/doc/node_modules/marked. Marked is a Markdown parser. Marked’s license follows: “”“ Copyright © 2011-2012, Christopher Jeffrey (https://github.com/chjj/)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR

COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. “”“

- test/gc/node_modules/weak. Node-weak is a node.js addon that provides garbage collector notifications. Node-weak’s license follows: “”“ Copyright © 2011, Ben Noordhuis

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED “AS IS” AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. “”“

- ICU’s license follows: From http://source.icu-project.org/repos/icu/icu/trunk/license.html “”“ ICU License – ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE Copyright © 1995-2014 International Business Machines Corporation and others All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder. All trademarks and registered trademarks mentioned herein are the property of their respective owners. Third-Party Software Licenses This section contains third-party software notices and/or additional terms for licensed third-party software components included within ICU libraries. 1. Unicode Data Files and Software COPYRIGHT AND PERMISSION NOTICE Copyright © 1991-2014 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html. Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the “Data Files”) or Unicode software and any associated documentation (the “Software”) to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) this copyright and permission notice appear with all copies of the Data Files or Software, (b) this copyright and permission notice appear in associated documentation, and © there is clear notice in each modified Data File or in the Software

as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified. THE DATA FILES AND SOFTWARE ARE PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder. 2. Chinese/Japanese Word Break Dictionary Data (cjdict.txt) # The Google Chrome software developed by Google is licensed # under the BSD license. Other software included in this distribution # is provided under other licenses, as set forth below. # # The BSD License # http://opensource.org/licenses/bsd-license.php # Copyright © 2006-2008, Google Inc. # # All rights reserved. # # Redistribution and use in source and binary forms, with or # without modification, are permitted provided that the following # conditions are met: # # Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. # Redistributions in binary form must reproduce the above # copyright notice, this list of conditions and the following # disclaimer in the documentation and/or other materials provided with # the distribution. # Neither the name of Google Inc. nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. # # # The word list in cjdict.txt are generated by combining three word lists listed # below with further processing for compound word breaking. The frequency is generated # with an iterative training against Google web corpora. # # * Libtabe (Chinese) # – https://sourceforge.net/project/?group_id=1519 # – Its license terms and conditions are shown below. # # * IPADIC (Japanese) # – http://chasen.aist-nara.ac.jp/chasen/distribution.html # – Its license terms and conditions are shown below. # # ————-COPYING.libtabe —— BEGIN———————— # # /* # * Copyrighy © 1999 TaBE Project. # * Copyright © 1999 Pai-Hsiang Hsiao. # * All rights reserved. # * # * Redistribution and use in source and binary forms, with or without # * modification, are permitted provided that the following conditions # * are met: # * # * . Redistributions of source code must retain the above copyright # * notice, this list of conditions and the following disclaimer. # * . Redistributions in binary form must reproduce the above copyright # * notice, this list of conditions and the following disclaimer in # * the documentation and/or other materials provided with the # * distribution. # * . Neither the name of the TaBE Project nor the names of its # * contributors may be used to endorse or promote products derived # * from this software without specific prior written permission. # * # * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # * “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS # * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE # * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, # * INCIDENTAL, SPECIAL, EXEMPLARY,

OR CONSEQUENTIAL DAMAGES # * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR # * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) # * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, # * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) # * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED # * OF THE POSSIBILITY OF SUCH DAMAGE. # */ # # /* # * Copyright © 1999 Computer Systems and Communication Lab, # * Institute of Information Science, Academia Sinica. # * All rights reserved. # * # * Redistribution and use in source and binary forms, with or without # * modification, are permitted provided that the following conditions # * are met: # * # * . Redistributions of source code must retain the above copyright # * notice, this list of conditions and the following disclaimer. # * . Redistributions in binary form must reproduce the above copyright # * notice, this list of conditions and the following disclaimer in # * the documentation and/or other materials provided with the # * distribution. # * . Neither the name of the Computer Systems and Communication Lab # * nor the names of its contributors may be used to endorse or # * promote products derived from this software without specific # * prior written permission. # * # * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS # * “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT # * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS # * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE # * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, # * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR # * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) # * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, # * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) # * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED # * OF THE POSSIBILITY OF SUCH DAMAGE. # */ # # Copyright 1996 Chih-Hao Tsai

```
Beckman Institute, University of Illinois
    #         c-tsai4uiuc.edu http://casper.beckman.uiuc.edu/~c-tsai4 # #
```

————————-COPYING.libtabe——-END———————————————— # # # ————————-COPYING.ipadic——-BEGIN———————————————— # # Copyright 2000, 2001, 2002, 2003 Nara Institute of Science # and Technology. All Rights Reserved. # # Use, reproduction, and distribution of this software is permitted. # Any copy of this software, whether in its original form or modified, # must include both the above copyright notice and the following # paragraphs. # # Nara Institute of Science and Technology (NAIST), # the copyright holders, disclaims all warranties with regard to this # software, including all implied warranties of merchantability and # fitness, in no event shall NAIST be liable for # any special, indirect or consequential damages or any damages # whatsoever resulting from loss of use, data or profits, whether in an # action of contract, negligence or other tortuous action, arising out # of or in connection with the use or performance of this software. # # A large portion of the dictionary entries # originate from ICOT Free Software. The following conditions for ICOT # Free Software applies to the current dictionary as well. # # Each User may also freely distribute the Program, whether in its # original form or modified, to any third party or parties, PROVIDED # that the provisions of Section 3 (“NO WARRANTY”) will ALWAYS appear # on, or be attached to, the Program, which is distributed substantially # in the same form as set out herein and that such intended # distribution, if actually made, will neither violate or otherwise # contravene any of the laws and regulations of the countries having # jurisdiction over the User or the intended distribution itself. # # NO WARRANTY # # The program was produced on an experimental basis in the course of the # research and development conducted during the project and is provided # to users as so produced on an experimental basis. Accordingly, the # program is provided without any warranty whatsoever, whether express, # implied, statutory or otherwise. The term “warranty” used herein # includes, but is not limited to, any warranty of the quality, # performance, merchantability and fitness for a particular purpose of # the

program and the nonexistence of any infringement or violation of # any right of any third party. # # Each user of the program will agree and understand, and be deemed to # have agreed and understood, that there is no warranty whatsoever for # the program and, accordingly, the entire risk arising from or # otherwise connected with the program is assumed by the user. # # Therefore, neither ICOT, the copyright holder, or any other # organization that participated in or was otherwise related to the # development of the program and their respective officials, directors, # officers and other employees shall be held liable for any and all # damages, including, without limitation, general, special, incidental # and consequential damages, arising out of or otherwise in connection # with the use or inability to use the program or any product, material # or result produced or otherwise obtained by using the program, # regardless of whether they have been advised of, or otherwise had # knowledge of, the possibility of such damages at any time during the # project or thereafter. Each user will be deemed to have agreed to the # foregoing by his or her commencement of use of the program. The term # “use” as used herein includes, but is not limited to, the use, # modification, copying and distribution of the program and the # production of secondary products from the program. # # In the case where the program, whether in its original form or # modified, was distributed or delivered to or received by a user from # any person, organization or entity other than ICOT, unless it makes or # grants independently of ICOT any specific warranty to the user in # writing, such person, organization or entity, will also be exempted # from and not be held liable to the user for any such damages as noted # above as far as the program is concerned. # # ————————-COPYING.ipadic——-END——————————————————— 3. Lao Word Break Dictionary Data (laodict.txt) # Copyright © 2013 International Business Machines Corporation # and others. All Rights Reserved. # # Project: http://code.google.com/p/lao-dictionary/ # Dictionary: http://lao-dictionary.googlecode.com/git/Lao-Dictionary.txt # License: http://lao-dictionary.googlecode.com/git/Lao-Dictionary-LICENSE.txt # (copied below) # # This file is derived from the above dictionary, with slight modifications. # ——————————————————————————————————————— # Copyright © 2013 Brian Eugene Wilson, Robert Martin Campbell. # All rights reserved. # # Redistribution and use in source and binary forms, with or without modification, # are permitted provided that the following conditions are met: # # Redistributions of source code must retain the above copyright notice, this # list of conditions and the following disclaimer. Redistributions in binary # form must reproduce the above copyright notice, this list of conditions and # the following disclaimer in the documentation and/or other materials # provided with the distribution. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND # ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED # WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE # DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR # ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; # LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON # ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS # SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. # ——————————————————————————————————————— 4. Burmese Word Break Dictionary Data (burmesedict.txt) # Copyright © 2014 International Business Machines Corporation # and others. All Rights Reserved. # # This list is part of a project hosted at: # github.com/kanyawtech/myanmar-karen-word-lists # # ——————————————————————————————————————— # Copyright © 2013, LeRoy Benjamin Sharon # All rights reserved. # # Redistribution and use in source and binary forms, with or without modification, # are permitted provided that the following conditions are met: # # Redistributions of source code must retain the above copyright notice, this # list of conditions and the following disclaimer. # # Redistributions in binary form must reproduce the above copyright notice, this # list of conditions and the following disclaimer in the documentation and/or # other materials provided with the distribution. # # Neither

the name Myanmar Karen Word Lists, nor the names of its # contributors may be used to endorse or promote products derived from # this software without specific prior written permission. # # THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND # ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED # WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE # DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR # ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES # (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; # LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON # ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT # (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS # SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. #

——————————————————————————————————————— 5. Time Zone Database ICU uses the public domain data and code derived from Time Zone Database for its time zone support. The ownership of the TZ database is explained in BCP 175: Procedure for Maintaining the Time Zone Database section 7. 7. Database Ownership The TZ database itself is not an IETF Contribution or an IETF document. Rather it is a pre-existing and regularly updated work that is in the public domain, and is intended to remain in the public domain. Therefore, BCPs 78 [RFC5378] and 79 [RFC3979] do not apply to the TZ Database or contributions that individuals make to it. Should any claims be made and substantiated against the TZ Database, the organization that is providing the IANA Considerations defined in this RFC, under the memorandum of understanding with the IETF, currently ICANN, may act in accordance with all competent court orders. No ownership claims will be made by ICANN or the IETF Trust on the database or the code. Any person making a contribution to the database or code waives all rights to future claims in that contribution or in the TZ Database. “”“

———————————————————————————————————————

PCSC (Version: 5.1.0)
Authors: Daniel Mueller
URL: https://github.com/danm-de/pcsc-sharp

Copyright © 2007-2019 Daniel Mueller
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Changes to this license can be made only by the copyright author with
explicit written consent.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PeterO.Cbor (Version: 4.5.2)
Authors: Peter Occil
URL: https://github.com/peteroupc/CBOR

Creative Commons Legal Code

CC0 1.0 Universal CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN “AS-IS” BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY
FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS
PROVIDED HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an “owner”) of an original work of authorship and/or a database (each, a “Work”).

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works (“Commons”) that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the “Affirmer”), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and

publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

1. Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights (“Copyright and Related Rights”). Copyright and Related Rights include, but are not limited to, the following: i. the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work; ii. moral rights retained by the original author(s) and/or performer(s); iii. publicity and privacy rights pertaining to a person’s image or likeness depicted in a Work; iv. rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below; v. rights protecting the extraction, dissemination, use and reuse of data in a Work; vi. database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and vii. other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof. 2. Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer’s Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the “Waiver”). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer’s heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer’s express Statement of Purpose. 3. Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer’s express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer’s Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the “License”). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer’s express Statement of Purpose. 4. Limitations and Disclaimers. a. No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document. b. Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law. c. Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person’s Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work. d. Affirmer understands and acknowledges that Creative Commons is not a party to this

document and has no duty or obligation with respect to this CC0 or use of the Work.

Pkcs11Interop (Version: 5.1.2)
Authors: Jaroslav Imrich
URL: https://www.pkcs11interop.net/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or

counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields

enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2012-2021 The Pkcs11Interop Project Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Portable.BouncyCastle (Version: 1.9.0)
Authors: Claire Novotny
URL: https://www.bouncycastle.org/csharp/

The MIT License (MIT)

© 2000-2021 Legion of the Bouncy Castle Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PriorityQueue (Version: 0.1.0)
Authors: Denis Shulepov
URL: https://github.com/dshulepov/ConcurrentPriorityQueue

The MIT License (MIT)

Copyright 2015

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PuTTY (Version: 0.76)
Authors: Simon Tatham
URL: https://www.putty.org

PuTTY is copyright 1997-2021 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, Josh Dersch, Lars Brinkhoff, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

QRCoder (Version: 1.4.3)
Authors: Raffael Herrmann
URL: https://github.com/codebude/QRCoder/

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Radius (Version: 2.0.0.2)
Authors: Front Porch Inc.
URL: https://github.com/frontporch/Radius.NET

The MIT License (MIT)

Copyright 2016

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SSH.NET (Version: 2020.0.1)
Authors: Renci
URL: https://github.com/sshnet/SSH.NET/

The MIT License (MIT)

2012-2021, RENCI

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the “Software”), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SharpVectors.Reloaded (Version: 1.7.7)
Authors: Elinam LLC (Japan)
URL: https://github.com/ElinamLLC/SharpVectors

BSD-3-Clause

Copyright © 2010 – 2021 Elinam LLC

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

———————————————————————————————————————

SuperSocket.ClientEngine.Core (Version: 0.10.0)
Authors: Kerry Jiang
URL: http://www.supersocket.net/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the

Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing

herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

———————————————————————————————————

Tanneryd.BulkOperations.EF6 (Version: 1.4.1)
Authors: Måns Tånneryd

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii)

beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that

such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright © 2017-2021 Tånneryd IT AB Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

UAParser (Version: 3.1.47)
Authors: enemaerke
URL: https://github.com/ua-parser/uap-csharp

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute

must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Copyright 2020 Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

WebSocket4Net (Version: 0.15.2)
Authors: Kerry Jiang
URL: http://websocket4net.codeplex.com/

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that

Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and © You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or

class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives. Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

WebSocketSharp (Version: 1.0.3-rc11)
Authors: sta
URL: http://sta.github.io/websocket-sharp

The MIT License (MIT)

© 2010-2016 sta.blockhead

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Z.EntityFramework.Plus.EF6 (Version: 6.13.10)
Authors: ZZZ Projects
URL: https://entityframework-plus.net/

The MIT License (MIT)

Copyright © ZZZ Projects

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal

in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

---

xxHash4net (Version: 1.2.0)
Authors: ailen0ada
URL: https://github.com/ailen0ada/xxHash4net

BSD 2-Clause License (http://www.opensource.org/licenses/bsd-license.php)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.