

# Handbuch

# Password Depot Enterprise

# Server 15

Zuletzt aktualisiert: 25.11.2020

---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*

# Inhaltsverzeichnis

Einführung .....	3
Installation und Betrieb .....	4
Migration .....	6
Server-Manager .....	7
Server-Manager .....	7
Verwalten .....	8
Verwalten .....	8
Serveroptionen .....	9
Server-Lizenz .....	13
Server-Richtlinien .....	14
Server-Richtlinien .....	14
Rechte .....	15
Sicherheit .....	16
Einträge .....	17
Client-Sicherheitsrichtlinien .....	18
Programmooptionen .....	19
Extras .....	20
Anmeldung der Benutzer am AD .....	20
Active-Directory-Synchronisation .....	21
Berichte .....	22
Datenbanken .....	23
Datenbanken .....	23
Hinzufügen .....	24
Berechtigungen .....	25
Eigenschaften einer Datenbank .....	29
Benutzer .....	30
Benutzer .....	30
Hinzufügen .....	31
Eigenschaften .....	33
Rechte für Benutzer .....	34
Datenbank zuweisen .....	35
Gruppen .....	36
Gruppen .....	36
Hinzufügen .....	37
Benachrichtigungen .....	38
Benachrichtigungen .....	38
Hinzufügen .....	39
Eigenschaften .....	40
Protokoll .....	41

# Einführung

**Password Depot Enterprise Server** ist eine Erweiterung für **Password Depot**. Mit Hilfe des Enterprise Servers können Clients eine oder mehrere im Netzwerk auf einem **Server** befindliche Datenbank gemeinsam nutzen. Als Client dient das Password Depot-Hauptprogramm.

Der **Password Depot Enterprise Server** wird auf einem Computer im lokalen Netzwerk installiert. Dort richtet der Administrator über den Server-Manager die Benutzer ein und weist ihnen für die gewünschten Datenbanken oder aber auch nur für bestimmte Elemente innerhalb einer Datenbank Zugriffsrecht zu.

Die zugelassenen Benutzer können mit dem **Password Depot-Hauptprogramm (Client)** auf die Datenbanken auf dem Server zugreifen, für die sie zugelassen sind. Hierzu wird die IP-Adresse und der Port des Servers benötigt sowie die vom Administrator eingerichteten Zugangsdaten (Benutzername und Kennwort). Eine Anmeldung am Server kann außerdem auch per Integrierter Windows-Authentifizierung (SSO) erfolgen.

**HINWEIS:** Die Datenbank wird vom Server geöffnet und den Benutzern zur Verfügung gestellt. Wenn Sie also eine bereits vorhandene Datenbank über den Server zur Verfügung stellen wollen, geben Sie deren Master-Kennwort im Server-Manager ein.

Ein Benutzer, der auf eine Datenbank, die vom Server bereitgestellt wird, zugreifen möchte, tut dies nicht durch das Master-Kennwort einer Datenbank, sondern durch den Benutzernamen und das Kennwort, welche er vom Administrator für diesen Server erhalten hat. Der Administrator gibt außerdem vor, welche Datenbanken ein Benutzer aufrufen kann und welche Zugriffsrechte er besitzt.

Die **Clients** können die Datenbanken über den Server öffnen und die darin enthaltenen Daten verwenden. Clients können auch Änderungen an den Einträgen vornehmen, wenn Sie die entsprechenden Rechte dafür besitzen. **Password Depot Enterprise Server** sperrt in diesem Fall den Eintrag, der gerade bearbeitet wird, sodass gleichzeitig keine anderen Änderungen von anderen Benutzern vorgenommen werden können, also Konflikte vermieden werden. Es ist jedoch möglich, dass mehrere Benutzer an ein und derselben Datenbank gleichzeitig arbeiten.

Die Anzahl der Benutzer, die Sie am Server anlegen können, ist über Ihre Lizenz definiert. Haben Sie beispielsweise eine 25-Benutzer-Lizenz erworben, so können Sie **maximal** 25 Benutzer anlegen usw.

**HINWEIS:** Für die Verwendung des Enterprise Servers von bis zu **drei Benutzern** ist keine Lizenz erforderlich. Sie können ihn in diesem Fall ohne Lizenz einsetzen.

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Installation und Betrieb

Der **Password Depot Enterprise Server** wird idealerweise vom Netzwerk-Administrator auf dem Server-PC des lokalen Netzwerks installiert. Optional kann es aber auf jedem beliebigen Computer installiert werden, der im Netzwerk erreichbar ist. Voraussetzung ist, dass der Computer über eine fest zugeordnete IP-Adresse im lokalen Netzwerk verfügt.

**HINWEIS:** Sie können den Enterprise Server (z. B. zu Testzwecken) auch auf Ihrem lokalen Computer installieren. Um in diesem Falle mit **Password Depot** auf den Server zuzugreifen, geben Sie als Server-Adresse 127.0.0.1 bzw. localhost an.

## Installation als Windows-Dienst oder als Windows-Anwendung

**Password Depot Enterprise Server kann in zwei Modi betrieben werden: Als normale Windows-Anwendung oder als NT-Dienst (empfohlen).** Per Vorgabe wird der Server während der Installation als NT-Dienst installiert. Um ihn als Windows-Anwendung zu installieren, wählen Sie bei der Installation entsprechend diese Option.

**WICHTIG:** Sie müssen sich vor der Installation für eine Option entscheiden. Wenn Sie sich für die Ausführung als Dienst entscheiden, wird der Dienst bei der Installation gleich eingerichtet. Die Installation als Dienst wird empfohlen.

Bei der Installation als Dienst wird der Server als **Password Depot Enterprise Server 15** aufgeführt. Um ihn zu starten oder zu stoppen, verwenden Sie die Windows-Systemsteuerung.

Falls Sie den Server als Anwendung installiert haben, finden Sie ihn im Programmverzeichnis (standardmäßig ist das C:\Program Files\AceBIT>Password Depot Server 15 unter Vista, Windows 7,8 und Windows 10 bzw. C:\Programme\AceBIT>Password Depot Server 15 unter XP).

Mit Version 14 und höher wurde für den Password Depot Enterprise Server die 64-Bit-Architektur implementiert.

## Server-Manager

Der Server-Manager ist ein separates Verwaltungsprogramm für **Password Depot Enterprise Server**. Es erlaubt die Administration des Servers und die Einstellung diverser Optionen. Sie können den Server-Manager nur von dem Computer aufrufen, auf dem der Server ausgeführt wird.

Um ihn aufzurufen, klicken Sie auf **Start** und wählen Sie im Startmenü **AceBIT -> Password Depot Server Manager 15** aus.

Der Server wird mit den folgenden Standardvorgaben für Login und Kennwort installiert:

**Benutzername:** Admin

**Kennwort:** admin

**WICHTIG:** Es wird dringend empfohlen, nach der Installation diese Standard-Zugangsdaten für den Administrator (also das Konto *Admin*) im Server-Manager zu ändern. Gehen Sie dazu im Server-Manager auf **Benutzer -> admin -> Konto** und ändern Sie hier die Zugangsdaten unter "Password Depot-Authentifizierung verwenden" ab.

In der Regel wird **Password Depot Enterprise Server** automatisch beim Start von Windows gestartet und läuft im Hintergrund auf dem PC. Wenn Sie den Server so konfigurieren, dass er als NT-Dienst läuft, startet er unter dem **SYSTEM-Konto** und benötigt für den Start keine Benutzeranmeldung.

## Update-Manager

Seit Version 14 gibt es im **Password Depot Enterprise Server** einen integrierten Update-Manager. Somit erhalten Sie

über den Server-Manager eine Benachrichtigung, sobald neue Versionen verfügbar sind. Die Funktion steht Ihnen unter **Hilfe -> Nach Updates** suchen zur Verfügung.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Migration

Haben Sie zuvor mit einer Vorgängerversion des **Enterprise Servers** gearbeitet, so können Sie diesen sehr einfach auf die aktuelle Version migrieren.

Beachten Sie dazu, dass der Server immer nur mit Clients der **gleichen Hauptversion** arbeiten kann. Sie können also **nicht** mit einem Client der Version 10x auf einen Server der Version 14x zugreifen. Aus diesem Grunde müssen Sie immer Ihre Clients und den Enterprise Server gleichzeitig auf die neue Version aktualisieren.

Die [Durchführung der Migration des Enterprise Servers](#) wird in der Knowledgebase erläutert.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Server-Manager

Der **Server-Manager** ist die zentrale Steuerung für den schnellen und unkomplizierten Zugriff auf alle Funktionen für die Wartung und Konfiguration von **Password Depot Enterprise Server**. Sie müssen sich zunächst mit dem [Server verbinden](#), um die nachfolgend beschriebenen Funktionen zu sehen.

Die Navigationsbereich des Server-Managers besteht aus fünf Bereichen:

- **Datenbanken:** Dieser Bereich dient dem Anlegen und Verwalten von Datenbanken auf dem Server.
- **Benutzer:** Dieser Bereich enthält Funktionen zur Verwaltung der Clients (Benutzer).
- **Gruppen:** Hier können Benutzer in Gruppen zusammengefasst werden.
- **Benachrichtigungen:** Hier können Benachrichtigungen für bestimmte Ereignisse erstellt werden, die dann per E-Mail versandt werden.
- **Protokoll:** Hier wird das Protokoll der Serveraktivitäten angezeigt.

Wenn Sie im Navigationsbereich des Server-Managers auf die IP-Adresse klicken, werden Ihnen grundlegende Informationen zum Enterprise Server angezeigt:

- **Status:** Zeigt an, ob der Server aktuell läuft oder angehalten ist.
- **Server-Adresse:** Zeigt die IP-Adresse des Servers an.
- **Server-Port:** Zeigt den Standard-Port für die Verbindung zum Enterprise Server an.
- **Läuft seit:** Gibt an, wann der Server erstmalig in Betrieb genommen wurde.
- **Server-Version:** Zeigt die aktuelle Serverversion bzw. den aktuellen Build einer Hauptversion an.
- **Verfügbare Updates:** Zeigt an, ob es ein neues Update für den Server innerhalb der gleichen Hauptversion gibt.
- **Installierte Lizenzen:** Zeigt an, für wie viele Lizenzen der Enterprise Server aktuell freigeschaltet ist (Servergröße).
- **Registrierte Benutzer:** Gibt an, wie viele Benutzer insgesamt auf dem Server-Manager angelegt sind.
- **Verbundene Benutzer:** Zeigt an, wie viele Benutzer aktuell mit dem Server verbunden sind.
- **Installierte Datenbanken:** Zeigt an, wie viele Datenbanken auf dem Server insgesamt installiert sind.

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Verwalten

Dieser Menüpunkt beinhaltet folgende Elemente:

- **Serveroptionen:** Hier können grundlegende Einstellungen am Server vorgenommen und z.B. festgelegt werden, wo und wie oft Sicherungskopien angelegt werden sollen.
- **Server-Lizenz:** Erlaubt die Eingabe eines Lizenzschlüssels, um die Anzahl der erlaubten Clients zu erhöhen.
- **Serverrichtlinien:** Hier können Standard-Rechte für Datenbanken festgelegt werden. Die Berechtigungen für einzelne Datenbanken können trotzdem individuell vorgenommen werden.
- **Client-Sicherheitsrichtlinien:** Ändert die lokalen Sicherheitsrichtlinien für Corporate-Clients.
- **Anhalten:** Unterbricht die Verfügbarkeit des Servers für alle Clients. Der Server bleibt jedoch weiterhin verfügbar, damit Wartungsarbeiten durchgeführt werden können.
- **Fortsetzen:** Setzt einen angehaltenen Server fort und macht ihn somit wieder für die Clients im Netzwerk verfügbar.
- **Neustarten:** Nutzen Sie diese Option, um den Server gegebenenfalls neu zu starten.
- **Programmooptionen:** Ermöglicht das Einstellen der Programmooptionen (nicht zu verwechseln mit den **Serveroptionen**).
- **Beenden:** Beendet den Server-Manager. Der Dienst oder die Server-Anwendung sind davon nicht betroffen.

**HINWEIS:** Bei manchen Änderungen am Enterprise Server kann ein Neustart des Servers erforderlich sein, damit die Änderungen greifen. Mit Version 15 wurde ein entsprechender Befehl zum Neustarten des Servers implementiert. Dieser erscheint von Seiten des Programmes automatisch, sollte ein Neustart des Servers erforderlich sein.

---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*



# Serveroptionen

Das Dialogfeld **Serveroptionen** finden Sie unter dem Menüpunkt **Verwalten**. Es verfügt über sieben Registerkarten: **Allgemein, Verbindungen, Protokollierung, Sicherungsdateien, Erweitert, E-Mail** und **2FA-Einstellungen**.

## Allgemein

### Server

Hier können Sie grundlegende Einstellungen des Servers vornehmen:

**Sprache des Servers:** Erlaubt es, die Sprache festzulegen.

**Server-Port:** Legt den Port standardmäßig fest.

**SSL/TLS verwenden:** Nutzung einer SSL/TLS-Verbindung zu den Clients aktivieren.

**SSL/TLS für die REST-Server-Verbindung verwenden:** Nutzung einer SSL/TLS-Verbindung bei der REST-Server-Verbindung. Durch die REST-Server-Implementierung kann auf den Enterprise Server jetzt über eine REST-API zugegriffen werden. Zu Demonstrationszwecken oder für den produktiven Einsatz steht eine neue Web-Schnittstelle im Quellcode zur Verfügung. Es handelt sich grundsätzlich um einen Web-Server, der sowohl das HTTP- als auch das HTTPS-Protokoll (empfohlen) verwenden kann. Um HTTPS verwenden zu können, müssen Sie ein gültiges SSL-Zertifikat installieren.

**Zertifikat installieren:** Erlaubt die Installation eines SSL-Zertifikats. Es öffnet sich ein Dialogfeld, in dem Sie ferner Ihre **Zertifikatsdatei** und deren Schlüssel erfassen können.

### Datenbanken

**Speicherort:** Definiert den Pfad, unter dem standardmäßig die Datenbanken abgelegt werden.

## Verbindungen

### Unterstützte Authentifizierungen

Legen Sie fest, welche Authentifizierungen Sie für Ihren Server zulassen möchten. Dabei können Sie die Optionen **Zugangsdaten (Konto und Kennwort)** und/oder **Integrierte Windows-Authentifizierung (Single Sign On)** verwenden.

### Unterstützte Clients

Legen Sie fest, welche Clients sich mit Ihrem Server verbinden dürfen. Folgende Optionen stehen hier zur Auswahl:

- **Standard-Edition für Windows**
- **Corporate-Edition für Windows**
- **Mobile-Editionen (iOS und Android)**
- **macOS**
- **Web-Client**

**HINWEIS:** Über den Server-Manager müssen alle Clients, mit denen eine Verbindung erfolgen soll, aktiviert sein, ansonsten ist eine Verbindung nicht möglich.

### Neue Verbindung von anderem Gerät:

Wählen Sie hier unter einer der drei verfügbaren Optionen aus, um festzulegen, wie mit Verbindungen des gleichen Benutzers von weiteren Geräten verfahren werden soll.

### Inaktive Sitzungen

Legen Sie fest, wie Password Depot Enterprise Server mit inaktiven Verbindungen verfahren soll.

## Fehlgeschlagene Anmeldungen

Geben Sie an, nach wie vielen fehlgeschlagenen Anmeldungen ein Benutzerkonto vorläufig gesperrt werden soll. Wurde ein Benutzerkonto gesperrt, so kann es im Server-Manager unter **Benutzer -> <BENUTZERNAME> -> Konto** wieder aktiviert werden, indem Sie bei "Konto deaktiviert" das Häkchen entfernen.

## Protokollierung

Hier befinden sich alle Einstellungen zu den Protokollen, die der **Password Depot Enterprise Server** anlegt. Folgende Optionen können Sie in dieser Registerkarte individuell einstellen:

### Lokales Protokoll

- **Protokollordner:** Hier können Sie sehen, in welchem Verzeichnis die Protokolle des Enterprise Servers lokal auf diesem abgespeichert werden. Über die Schaltfläche "Durchsuchen" können Sie dieses anpassen.
- **Max. Dateigröße:** Definieren Sie hier, wie groß die Protokolldatei des Servers maximal in KB sein soll.
- **Neue Protokolldatei erzeugen:** Wählen Sie hier aus wie oft eine Protokolldatei erzeugt werden soll.
- **Protokolle löschen:** Definieren Sie hier die Einstellungen zum Löschen von bereits existierenden Protokollen. So können Sie entweder einstellen, dass diese nie gelöscht werden sollen oder aber Sie legen eine bestimmte Anzahl fest, die behalten werden soll, beispielsweise 30 (standardmäßig voreingestellt): Dies bedeutet dann, dass die letzten 30 Protokolle behalten und alle älteren gelöscht werden.
- **Protokolle versenden:** Setzen Sie ein Häkchen bei "Protokoll-Inhalte an einen Remote-Server senden", wenn Sie möchten, dass diese Option aktiviert wird und Protokolldateien des Enterprise Servers automatisch an einen externen Protokoll-Server gesendet werden. Sie können anschließend die Serveradresse und den Port des Servers eingeben, an den die Protokolle gesendet werden sollen. Dadurch können Sie sicherstellen, dass die Protokolle des Servers nicht durch unbefugten Zugriff manipuliert werden.

## Sicherungsdateien

In dieser Registerkarte können Sie Einstellungen zu Ihren Sicherungsdateien vornehmen:

### Datensicherung

- **Sicherungsordner:** Hier können Sie festlegen, wo die Sicherungskopien gespeichert werden sollen. Über die Schaltfläche **Durchsuchen** rechts daneben können Sie ein anderes Verzeichnis auswählen.
- **Datenbanken bei jedem Programmstart sichern:** Markieren Sie diese Option, damit das Programm bei jedem Start eine Sicherungskopie der vorhandenen Datenbanken anfertigt.
- **Datenbanken sichern alle:** Legen Sie hier eine Anzahl an Stunden fest, nach denen **Password Depot Enterprise Server** automatisch eine Sicherungskopie der vorhandenen Datenbanken anfertigt.

**HINWEIS:** Standardmäßig sind hier beide Optionen ausgewählt und wir empfehlen darüber hinaus auch, beide Optionen aktiviert zu lassen.

- **Protokolle sichern in Datei:** Wenn Sie diese Option markieren, erstellt das Programm ein Protokoll der vorgenommenen Sicherungen und speichert es in der angegebenen Datei ab, damit später nachverfolgt werden kann, zu welchem Zeitpunkt die Datenbanken gesichert wurden.

## Erweitert

In dieser Registerkarte stehen Ihnen erweiterte Einstellungen wie folgt zur Verfügung:

## Active Directory

- Legen Sie fest, ob die AD-Synchronisation automatisch und in welchen Zyklen durchgeführt werden soll und was mit Benutzern und Gruppen passieren soll, die nicht (mehr) im AD gefunden werden. Sie können solche Benutzer entweder **ignorieren**, **deaktivieren** oder **löschen** lassen.

**HINWEIS:** Vorzugsweise sollte die Synchronisation vom Administrator zu gegebenem Anlass manuell angestoßen werden. Falls Sie eine automatische Synchronisation benötigen, sollten die Zyklen vorzugsweise zu Zeiten, in denen die Serverlast gering ist und beispielsweise alle 24 Stunden (1140 Minuten) erfolgen.

## Einträge bearbeiten

- Legen Sie eine bestimmte Zeit (in Minuten) fest, nach deren Ablauf sich ein Eintrag automatisch sperren soll, wenn ein Benutzer einen Eintrag geöffnet hat, diesen aber gerade nicht nutzt. Standardmäßig sind hier fünf Minuten vorgegeben, diesen Zeitraum können Sie sowohl verringern als auch erhöhen.

## Private Datenbanken

- Legen Sie fest, ob für jeden neuen Benutzer am Enterprise Server, der hinzugefügt wird, automatisch auch eine private Datenbank erstellt werden soll. Diese Datenbank wird dann ebenfalls auf dem Enterprise Server abgespeichert und ein Benutzer kann hier private Daten ablegen, die nicht Inhalt der Unternehmensdatenbank sein sollen. Im Bereich **Datenbank** werden private Datenbanken dann mit folgender Bezeichnung versehen: **Privat\_DB\_<BENUTZER>.pswe**.
- Sie können auch festlegen, ob private Datenbanken beim Löschen eines Benutzers vom Server ebenfalls automatisch gelöscht werden sollen. Ist diese Option aktiviert und wird ein Benutzer vom Server gelöscht, so wird gleichzeitig auch automatisch seine private Datenbank entfernt und diese ist anschließend dann nicht mehr als Datenbank auf dem Server zu sehen bzw. verfügbar.

Bitte beachten Sie, dass standardmäßig beide Optionen **deaktiviert** sind.

## WebSockets-Port für Clients

- **Standard-Portnummer verwenden:** Die Standard-Portnummer lautet **25109** und ist standardmäßig aktiviert. Wenn das Browser-Add-On verwendet wird, erfolgt die Kommunikation standardmäßig über diesen Port und Benutzer müssen dabei keine Änderungen mehr vornehmen, da der Port **25109** auch bereits standardmäßig im Browser voreingestellt ist.
- **Automatisches Generieren der Portnummern (empfohlen für Terminal-Server):** Wie der Beschreibung zu entnehmen ist, empfiehlt sich diese Option dringend bei Verwendung von Password Depot auf einem Terminal-Server. Da bei einem Terminal-Server alle Benutzer am gleichen PC arbeiten, muss sichergestellt werden, dass bei der Nutzung des Add-Ons jedem Benutzer auch eine eigene Portnummer für die Kommunikation mit dem Add-On zugewiesen wird. Die Socket-Portnummer ist kein virtueller, sondern ein physikalischer Parameter und kann daher nicht von mehreren Instanzen der Password Depot-Clients gemeinsam genutzt werden.

Werden keine **eindeutigen** Portnummern für jeden Client verwendet, so sind Probleme vorprogrammiert, da Password Depot dann nicht wissen kann, an welchen Client es vom Add-On angeforderte Zugangsdaten senden soll. Es kann dann beispielsweise passieren, dass Benutzer A die Login-Daten von Benutzer B erhält, obwohl er nicht für diese Zugangsdaten berechtigt ist. Es ist deshalb **zwingend erforderlich**, bei Nutzung eines Terminal-Servers jedem Benutzer eine individuelle Portnummer zuzuweisen. In den Serveroptionen können Sie die Option **Automatisches Generieren der Portnummern (empfohlen für Terminal-Server)** nun bei Verwendung eines Terminal-Servers standardmäßig für den Enterprise Server aktivieren, sodass für jeden Benutzer am Server eine eigene Portnummer automatisch generiert wird und der Administrator dies nicht mehr manuell, für jeden Benutzer einzeln, einstellen muss.

Mehr zur Portnummer bei Verwendung des Add-Ons erfahren Sie [hier](#).

## E - Mail

In dieser Registerkarte können Sie die Einstellungen für die E-Mail-Warnungen festlegen:

- **Absender:** Hier können Sie die E-Mail-Adresse des Absenders und seinen Namen eintragen.
- **Postausgangsserver:** Hier können Sie den Postausgangsserver konfigurieren.
- **Verbindung testen:** Hier können Sie die E-Mail-Adresse eines Empfängers einfügen und eine Test-Mail verschicken, um die oben vorgenommenen Einstellungen zu überprüfen.

## 2 - FA - Einstellungen

Hier können Sie einstellen, ob Sie eine **Zwei-Faktor-Authentifizierung** Ihrer Benutzer am Server wünschen und diese aktivieren möchten. Hierbei können Sie wählen, ob Sie die Zwei-Faktor Authentifizierung mittels **TOTP** oder **E-Mail** veranlassen wollen. Mit der Option **Benutzer dürfen sich die Geräte merken lassen (Tage)** hat der Administrator die Möglichkeit, eine bestimmte Anzahl an Tagen festzulegen, während derer die Benutzer einer Verbindung zu einem bestimmten Gerät vertrauen können. Für den Fall der Zwei-Faktor-Authentifizierung bedeutet dies, dass für den gewählten Zeitraum x nicht bei jeder Anmeldung am gleichen Gerät erneut ein Code eingegeben werden muss, sondern nur beim erstmaligen Verbinden, sofern der entsprechende Benutzer beim Anmelden dann die Option **Diesem Computer vertrauen** auswählt.

Mit der Option **Ablaufzeit des E-Mail-Codes (Minuten)** kann der Admin die Gültigkeit eines per E-Mail versandten Codes zur Zwei-Faktor-Authentifizierung standardmäßig festlegen. Gibt ein Benutzer den Code nicht rechtzeitig ein und dieser läuft ab, muss für eine korrekte Authentifizierung ein neuer Code angefordert werden.

In unserer Knowledgebase finden Sie [weitere Informationen zur Zwei-Faktor-Authentifizierung](#).

**HINWEIS:** Sowohl die Integrierte Windows-Authentifizierung als auch die Anmeldung am Server per Benutzername und Kennwort unterstützen die Zwei-Faktor-Authentifizierung. Unter **Benutzer -> <BENUTZERNAME> -> Konto** können Sie für einzelne Benutzer die Zwei-Faktor-Authentifizierung deaktivieren. Mehr dazu können Sie im Bereich [Benutzer hinzufügen](#) lesen.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Server-Lizenz

Wenn Sie im Menü Verwalten auf **Server-Lizenz** klicken, öffnet sich das Dialogfeld zum Hinzufügen einer neuen Lizenz. Es zeigt die aktuell installierte Lizenz an und erlaubt es, einen neuen Freigabecode einzugeben, um so die Anzahl an erlaubten Clients zu erhöhen. Außerdem können Sie hier auch einsehen, welche Version des Servers aktuell installiert ist.

**HINWEIS:** Die Anzahl an Clients bezieht sich immer auf die Anzahl an Benutzern, **die am Server angelegt werden können.**

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Serverrichtlinien

Das Dialogfeld **Serverrichtlinien** erreichen Sie über das Menü **Verwalten**.

Hier können Sie Einstellungen vornehmen, welche die Rechtevergabe an die Clients und die Einstellungen der Clients selbst betreffen.

Das Dialogfeld ist unterteilt in die drei Registerkarten: **Rechte**, **Sicherheit** und **Einträge**.

**Siehe auch: [Rechteverwaltung in Password Depot Enterprise Server](#).**

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Serverrichtlinien - Rechte

In der Registerkarte **Rechte** der Serverrichtlinien können Sie die Voreinstellungen vornehmen, die Sie standardmäßig für alle Benutzer und Datenbanken verwenden möchten.

1. Wenn Sie den Zustand auf **Nicht definiert** setzen, können Sie das entsprechende Recht für jeden Benutzer und jede Datenbank in den Datenbankeigenschaften einzeln einstellen.
2. Wenn Sie **Aktiviert** wählen, ist das entsprechende Recht für alle Benutzer als aktiviert voreingestellt. Sie können es jedoch für einzelne Benutzer/Datenbanken ändern.
3. Wenn Sie die restriktivste Option **Deaktiviert** auswählen, so ist das entsprechende Recht für alle Benutzer als verweigert eingestellt. Sie können dieses Recht anschließend nicht mehr für einzelne Benutzer/Datenbanken ändern.

**HINWEIS:** Über die Schaltfläche **Einstellungen wiederherstellen** können Sie die vorgenommenen Einstellungen der Serverrichtlinien in der Registerkarte **Rechte** zurücksetzen, sodass Sie hier anschließend wieder zu den Standardeinstellungen gelangen.

**Siehe auch:** [Rechteverwaltung in Password Depot Enterprise Server](#)

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Serverrichtlinien - Sicherheit

In der Registerkarte **Sicherheit** der Serverrichtlinien können Sie Sicherheitseinstellungen für die Clients festlegen:

- Setzen Sie ein Häkchen bei **Kennwortqualität auf Anfälligkeit gegen Wörterbuchangriffe prüfen**, damit jedes Mal eine Warnung ausgegeben wird, wenn ein Benutzer ein Kennwort verwendet, das in einem Wörterbuch enthalten ist.
- Darunter können Sie **Kennwortrichtlinien** festlegen, denen neu angelegte Kennwörter (auch das Master-Kennwort) entsprechen sollten: Sie können eine Mindestanzahl an Zeichen bestimmen und außerdem festlegen, welche Symboltypen (Klein- und Großbuchstaben, Zahlen, Sonderzeichen) in einem Kennwort enthalten sein sollen.

**HINWEIS:** Über die Schaltfläche **Einstellungen wiederherstellen** können Sie die vorgenommenen Einstellungen der Sicherheitsrichtlinien in der Registerkarte **Sicherheit** zurücksetzen, sodass Sie hier anschließend wieder zu den Standardeinstellungen gelangen.

---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*



# Serverrichtlinien - Einträge

In der Registerkarte **Einträge** hat der Server-Administrator die Möglichkeit, die **verschiedenen Eintragstypen zentral über den Server-Manager festzulegen**. Hier können Sie einstellen, welche Eintragstypen benötigt bzw. nicht benötigt werden, indem Sie diese entsprechend aktivieren oder deaktivieren.

1. **Setzen Sie ein Häkchen** bei allen Eintragstypen, die Sie **verwenden möchten**. Alle aktivierten Eintragstypen stehen dann standardmäßig bei allen Clients zur Verfügung.
2. **Entfernen Sie das Häkchen** bei allen Eintragstypen, die **nicht benötigt** werden bzw. grundsätzlich nicht zur Auswahl stehen sollen. Clients sehen dann die deaktivierten Eintragstypen erst gar nicht, sodass diese beim Arbeiten mit Password Depot auch nicht verwendet werden können.

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Client-Sicherheitsrichtlinien

Die Client-Sicherheitsrichtlinien erlauben Ihnen, diverse Merkmale der Corporate-Clients aus dem Server-Manager heraus zu definieren. Damit die Client-Sicherheitsrichtlinien greifen, müssen diese zunächst über den entsprechenden Schalter aktiviert werden. Weitere Informationen zur Corporate-Edition von Password Depot finden Sie [hier](#).

## Richtlinie für Master-Kennwort

Erlaubt es, festzulegen, welche Anforderungen das Master-Kennwort beim Client erfüllen muss, wenn damit lokale Datenbanken erzeugt werden.

**Kennwortverlauf erzwingen:** Bestimmt die Anzahl der eindeutigen neuen Passwörter, die verwendet werden müssen, bevor ein altes Passwort wiederverwendet werden kann.

**Maximales Alter für Kennwörter:** Bestimmt die Zeitspanne (in Tagen), die ein Passwort verwendet werden kann, bevor das System den Benutzer auffordert, es zu ändern.

**Mindestalter für Kennwörter:** Legt die Zeitspanne (in Tagen) fest, die ein Passwort verwendet werden muss, bevor der Benutzer es ändern kann.

**Kennwortlänge mindestens:** Legt fest, wie lange das Master-Kennwort mindestens sein muss.

**Kennwort muss Komplexitätsanforderungen entsprechen:** Das Master-Passwort muss mindestens die angegebenen Zeichentypen enthalten (Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen).

**HINWEIS:** Diese Einstellungen beziehen sich nur auf das Master-Kennwort, nicht auf die Einträge innerhalb einer Datenbank selbst!

## Richtlinie für erlaubte Speicherorte

Ermöglicht es, festzulegen, welche Speicherorte (wie z.B. lokales System, Cloud-Dienste etc.) die Clients nutzen dürfen.

## Richtlinie für Aktionen

Ermöglicht es, festzulegen, ob Aktionen wie z.B. Drucken oder Exportieren erlaubt sind.

Neue Optionen in Version **15** sind:

- **TANs verwenden**
- **Zweite Passwörter einstellen**

## Programmoptionen

Ermöglicht die Definition sicherheitsrelevanter Programmoptionen.

# Programmoptionen

Die Programmoptionen beziehen sich auf die Einstellungen des Server-Managers.

Unter **Sprache der Anwendung** können Sie die Sprache für die Oberfläche auswählen.

Im Bereich **SSL/TLS-Optionen** legen Sie fest, ob sich der Server-Manager mit dem Server-Dienst über SSL/TLS verbinden soll.

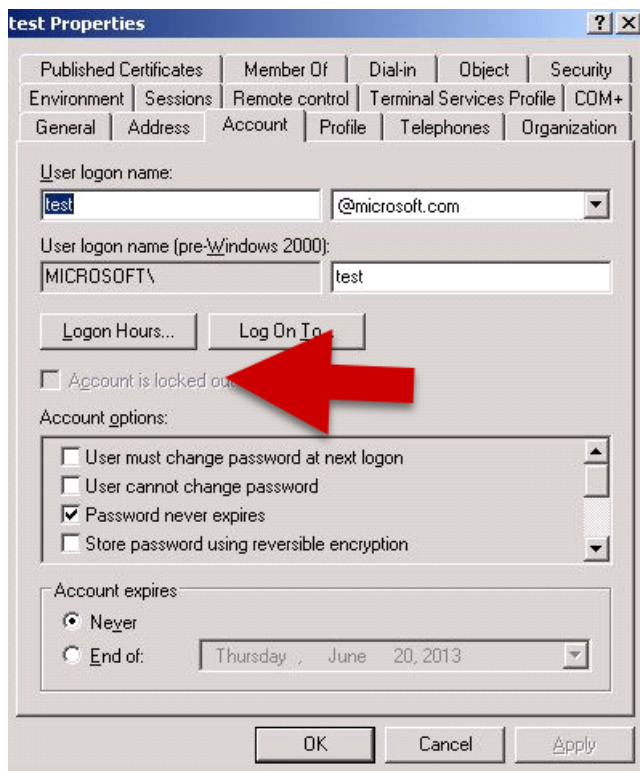
---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*

# Anmeldung der Benutzer am AD

Password Depot verwendet LDAP (anstelle von WinNT). Benutzer-UPNs (User Principal Name) können aus dem Active Directory abgerufen werden. Dieses Attribut ist jedoch erst nach einer manuellen oder automatischen Synchronisation mit AD über den Server-Manager verfügbar.

Das heißt, dass Windows-Domänenbenutzer auf dem Password Depot-Server authentifiziert werden können, indem beide Formen des "User logon name / Benutzeranmeldenamens" verwendet werden:



1) <NetBIOS-Domain-Name>\<sAMAccountName> - dies ist die traditionelle WinNT-Form (vor Windows 2000)

**Beispiel:** MICROSOFT\Test

2) Benutzer-Hauptname (der normalerweise die Form <sAMAccountName>@<DNS-Domänenname> hat)

**Beispiel:** test@microsoft.com

3) Wenn es im Netzwerk nicht mehrere Benutzer mit den gleichen Namen aus verschiedenen vertrauenswürdigen Domänen gibt, kann ein Benutzer das einfache Formular <sAMAccountName> verwenden.

**Beispiel:** Test

Zusammengefasst bedeutet dies, dass ein AD-Benutzer zum Anmelden am Enterprise Server genau die gleichen Anmeldedaten wie für die Anmeldung an einem Windows-Domänenkonto verwenden kann.

# Active Directory-Synchronisation

Im Menü **Extras** finden Sie den Eintrag **Active Directory-Synchronisation**, über den Sie den gleichnamigen Assistenten starten.

Mit Version 14 wurde der WinNT Provider durch einen leistungsfähigeren LDAP Provider ersetzt. Außerdem wurde die Funktionalität der Active Directory-Synchronisation erweitert.

Auf der Startseite des Assistenten müssen Sie zunächst Angaben zur Domain machen, aus der Sie die Benutzer importieren möchten:

- **Name der Domain:** Sofern die Domain noch nicht in der Liste enthalten ist, geben Sie hier den Namen der Domain ein.
- **Anmelden als aktueller Benutzer:** Wählen Sie diese Option, wenn Sie sich mit dem aktuellen Benutzer anmelden möchten, um die Active Directory-Synchronisation durchzuführen.
- **Dieses Konto verwenden:** Geben Sie hier den Benutzernamen und das Kennwort eines Benutzers ein, der die Berechtigung besitzt, Daten aus dem Active Directory der Domain auszulesen. Normalerweise ist dies der Domain-Administrator.

Im Bereich **Optionen** können Sie ferner auswählen, ob **alle Container rekursiv gescannt** und ob **gelöschte Objekte** während der Synchronisation **überprüft werden sollen**. Wenn die Option **Alle Container rekursiv scannen** markiert ist, liest der Assistent das gesamte Verzeichnis ein. Dies kann in manchen Fällen sehr viel Zeit in Anspruch nehmen. Diese Option sollte nur beim allerersten Mal nach der Portierung von Daten aus einer älteren Version des Password Depot-Servers verwendet werden, um alle WinNT-Pfade durch LDAP-Pfade zu ersetzen. Wenn diese Option nicht aktiviert ist, arbeitet der Assistent wie ein normaler Active Directory-Explorer, d.h., er öffnet nur das angegebene Objekt oder den Container und scannt dann den Container, wenn Sie den Knoten erweitern.

Klicken Sie anschließend auf **Anmelden**.

Wenn Sie sich erfolgreich angemeldet haben, sehen Sie im nächsten Fenster den Active Directory-Baum.

Hier können Sie Benutzer und/oder Gruppen auswählen, die in **Password Depot Enterprise Server** importiert oder aktualisiert werden sollen.

Falls Sie sehr viele Einträge haben, können Sie die Einträge unten links im Feld **Filter** filtern.

Wenn Sie in den Active Directory-Baum mit der Maus rechts klicken, stehen Ihnen Funktionen zur Verfügung, um die Auswahl zu beschleunigen.

Wählen Sie die gewünschten Benutzer und/oder Gruppen aus, indem Sie die entsprechenden Kontrollkästchen markieren. Darüber hinaus werden Ihnen in diesem Fenster weitere Merkmale der Benutzer in der Active Directory sowie deren Wert angezeigt.

Klicken Sie abschließend auf **Synchronisieren** und es werden Ihnen im nächsten Fenster die Ergebnisse der Synchronisation angezeigt.

**HINWEIS:** Alle importierten Benutzer aus dem Active-Directory können sich per Standard mit Ihren Konten und Kennwörtern aus Windows NT anmelden. Dies können Sie in den Eigenschaften eines Benutzers ändern.

**TIPP:** Mit **Version 15** können Benutzer und Gruppen nun auch einzeln mit dem Active Directory synchronisiert werden.

---

[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)

# Berichte

Im Menü **Extras** können Sie Berichte generieren, um eine Übersicht über Benutzer und Datenbanken am Server zu erhalten.

Diese Berichte können sowohl ausgedruckt als auch in verschiedenen Formaten (.html, .mht, .txt) abgespeichert werden.

## Datenbanken - Bericht

Unter **Datenbanken-Bericht** wird ein Bericht erstellt, der die Datenbanken des Password Depot Enterprise Servers auflistet. Zusätzlich erhält man hier eine Übersicht, welche Benutzer Zugriff auf welche Datenbank haben und welche Berechtigungen genau sie besitzen. Dieser Bericht kann gespeichert und ausgedruckt werden.

Die **gewährten** Berechtigungen sind in der jeweiligen Spalte mit einem ✓ markiert, während die **verweigerten** Berechtigungen mit einem **leeren Feld** dargestellt werden. Die Anordnung der Spalten mit den Berechtigungen ist die gleiche wie die aus den erweiterten Berechtigungen in den Datenbankeigenschaften.

## Benutzerbericht

Unter **Benutzerbericht** wird ein Bericht erstellt, der die Benutzerkonten von Password Depot Enterprise Server auflistet. Zusätzlich erhält man hier eine Übersicht auf welche Datenbanken die einzelnen Benutzer Zugriff haben und welche Berechtigungen sie für die einzelnen Datenbanken besitzen. Dieser Bericht kann ebenfalls gespeichert und ausgedruckt werden.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Datenbanken

Im Bereich **Datenbanken** sind die vom Server verwalteten Datenbanken aufgeführt. Hier können Sie neue Datenbanken hinzufügen oder bestehende löschen. Darüber hinaus weisen Sie hier den vorhandenen Benutzern oder Gruppen Zugriffsrechte auf die einzelnen Datenbanken zu.

In der **Listenansicht** des Bereichs Datenbanken erhalten Sie einen Überblick über die vorhandenen Datenbanken, deren Größe, Änderungsdatum und der Anzahl der Datenbankinträge.

Darüber hinaus können Sie sehen, wie viele Benutzer aktuell mit einer Datenbank verbunden sind.

Wenn Sie sehr viele Datenbanken verwenden, können Sie im oberen Bereich einen **Filter** eingeben, um die Anzeige einzugrenzen. Geben Sie dazu einen Datenbanknamen oder einen Teil davon ein.

Folgende Funktionen stehen hier zur Verfügung:

- **Neue Datenbank:** Mit dieser Schaltfläche öffnen Sie das Dialogfeld **Datenbank dem Server hinzufügen**.
- **Berechtigungen:** Über diese Option können Sie die Rechteverwaltung vornehmen. Sie sehen zunächst alle Benutzer, die aktuell auf die Datenbank zugriffsberechtigt sind. Darüber hinaus werden Ihnen im unteren Abschnitt die effektiven Berechtigungen eines Benutzers angezeigt. Um die detaillierte Rechteverwaltung vorzunehmen, klicken Sie in diesem Bereich zunächst auf einen Benutzer oder eine Gruppe und anschließend auf **Eigenschaften**.
- **Eigenschaften:** Ruft ein Dialogfeld auf, in dem Sie nähere Informationen zu einer Datenbank einsehen können. Es werden Ihnen hier die Benutzer angezeigt, die aktuell mit der entsprechenden Datenbank verbunden sind, außerdem erhalten Sie weitere Informationen zu Dateityp, Größe sowie dem letzten Änderungsdatum der Datenbank.
- **Löschen:** Mit dieser Schaltfläche können Sie Datenbanken aus dem Arbeitsverzeichnis des Servers löschen. Falls die Datenbank zu diesem Zeitpunkt von einem Benutzer verwendet wird, erhält dieser beim nächsten Speichern einen Hinweis.
- **Umbenennen:** Benennt eine markierte Datenbank um.
- **Alle auswählen:** Markiert alle Datenbanken der Liste.

**TIPP:** Diese Funktionen können Sie auch durch einen Rechtsklick auf eine Datenbank aus der Liste aufrufen.

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Datenbank dem Server hinzufügen

Dieses Dialogfeld verfügt über zwei Register:

- **Vorhandene Datenbank hinzufügen**
- **Neue Datenbank erzeugen**

## Vorhandene Datenbank hinzufügen

Wählen Sie diese Registerkarte, um eine vorhandene Datenbank dem Server hinzuzufügen.

- Klicken Sie dort auf die Schaltfläche **Durchsuchen**, um die entsprechende Datenbank auszuwählen.
- Im Feld **Master-Kennwort** geben Sie das Master-Kennwort dieser Datenbank ein.
- Aktivieren Sie das Kästchen **Verbergen**, um die Zeichen Ihres Kennworts als Punkte darstellen zu lassen.

**HINWEIS:** Nachdem eine vorhandene Datenbank dem Server hinzugefügt wurde, wird Sie in das Datenbank-Verzeichnis des Servers kopiert und das Master-Kennwort so geändert, dass es dem Kennwort des Admin-Kontos entspricht.

## Neue Datenbank erzeugen

Wählen Sie diesen Tab, um eine neue, leere Datenbank zu erzeugen. Geben Sie den gewünschten Datenbanknamen und, falls erwünscht, zusätzliche Anmerkungen ein.

**HINWEIS:** Als Master-Kennwort wird das Administrator-Kennwort verwendet. Die Clients verwenden zum Öffnen der Datenbank jedoch ihr vom Administrator zugewiesenes Kennwort.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*



# Berechtigungen

In den **Berechtigungen** definieren Sie die Zugriffsrechte Ihrer Benutzer und Gruppen im Detail.

Im Hauptfenster werden Ihnen zunächst alle Benutzer/Gruppen angezeigt, die auf die entsprechende Datenbank zugriffsberechtigt sind. Darunter sehen Sie für jeden Benutzer dessen effektive Berechtigungen. Um diese genau einsehen zu können, klicken Sie auf einen bestimmten Benutzer bzw. eine bestimmte Gruppe aus der Liste.

## Neu

Klicken Sie auf **Neu**, um der ausgewählten Datenbank neue Benutzer/Gruppen hinzuzufügen. Diese können Sie nun aus der Liste auf der linken Seite auswählen und die Rechte im Bereich **Berechtigungen** genauer zuweisen. Die hier gesetzten Berechtigungen beziehen sich auf die **gesamte Datenbank**. Nähere Berechtigungen für **Einträge und Ordner** können Sie im gleichnamigen Reiter vornehmen. Im Reiter **Versiegelter Zugang** können Sie den Status eines versiegelten Eintrags ändern. Die Rechtevergabe sowie die Versiegelung von Einträgen wird nachstehend näher erläutert.

## Eigenschaften

Im Bereich **Datenbanken -> Berechtigungen -> Eigenschaften** erfolgt die detaillierte Rechteverwaltung auf dem Enterprise Server. Wählen Sie einen Benutzer aus und klicken Sie anschließend auf **Eigenschaften**. Diese können Sie auch per Doppelklick auf einen Benutzer, der bereits auf die entsprechende Datenbank zugreifen kann, aufrufen. Außerdem können Sie hier auch Benutzer oder Gruppen löschen, wenn diese keinen Zugriff mehr auf die ausgewählte Datenbank erhalten sollen.

### Datenbank

Sie sehen hier oben links den ausgewählten Benutzer bzw. die ausgewählte Gruppe. Administratoren haben hier die Möglichkeit, den Zugriff von Benutzern und Gruppen auf eine Datenbank zeitlich zu beschränken oder aber diesen ohne zeitliche Limitierung zuzulassen. Um den Zeitraum zu definieren, müssen Sie unter **Gültig ab** das Startdatum und unter **Gültig bis** das Enddatum des Zugriffs festlegen. Wünschen Sie einen zeitlich unbegrenzten Zugriff für den entsprechenden Benutzer/die entsprechende Gruppe, so müssen Sie die Option **Gültig bis** nicht beachten und nur das Startdatum festlegen (standardmäßig ist hier der Tag gesetzt, an dem Sie den Zugriff erlauben und die Rechteverwaltung festlegen).

### Berechtigungen

Hier können Sie die Berechtigungen auf Datenbank-Ebene einstellen, das bedeutet, alle Rechte, die Sie hier setzen, gelten für die **gesamte** Datenbank. Folgende Berechtigungen stehen Ihnen hier zur Verfügung:

- **Zugriff auf die Datenbank**
- **Lesen von Einträgen**
- **Ändern von Einträgen**
- **Hinzufügen von Einträgen**
- **Löschen von Einträgen**
- **Nutzen der Funktion "Automatisches Ausfüllen"**
- **Autom. Ausfüllen über Browser Add-Ons**
- **Neue Einträge aus Browser Add-Ons übernehmen**
- **Drucken von Einträgen**
- **Exportieren von Einträgen**
- **Lokales Speichern der Datenbank**

- **Anderen Benutzern Zugriff gewähren**
- **Einträge versiegeln**
- **Admin-Rechte gewähren**

**TIPP:** Unter **Effektive Berechtigungen anzeigen** können Sie sich die effektiven Berechtigungen eines Benutzers oder einer Gruppe nochmal gesondert anzeigen lassen.

## Einträge und Ordner

Grundsätzlich sollten sich die Rechte eines Benutzers oder einer Gruppe auf die gesamte Datenbank beziehen. Falls Sie aber Rechte auch innerhalb der Datenbank vergeben möchten, z. B. auf einzelne Ordner oder Einträge, so können Sie dies in dieser Registerkarte durchführen.

Folgende Berechtigungen stehen Ihnen unter Einträge und Ordner zur Verfügung:

- **Zugriff auf Einträge**
- **Lesen von Einträgen**
- **Ändern von Einträgen**
- **Hinzufügen von Einträgen**
- **Einträge löschen**
- **Anderen Benutzern Zugriff gewähren**
- **Einträge versiegeln**

Wählen Sie links einzelne Ordner oder Einträge aus und setzen Sie anschließend unter **Berechtigungen** die Zugriffsrechte wie gewünscht.

**TIPP:** Auch hier können Sie sich unter **Effektive Berechtigungen anzeigen** die effektiven Berechtigungen eines Benutzers oder einer Gruppe auf einzelne Einträge und Ordner innerhalb der Datenbank nochmal gesondert anzeigen lassen.

Mehr dazu erfahren Sie unter [Rechteverwaltung in Password Depot Enterprise Server](#).

Wie Sie außerdem sicherstellen, dass unbefugte Benutzer keine Einträge lesen können erfahren Sie [hier](#).

**HINWEIS:** In den beiden Registerkarten **Datenbank** und **Einträge und Ordner** können Sie verschiedene Formatierungen sehen, die die Rechtevergabe erleichtern sollen. Standardmäßig sind nun zunächst alle Optionen/Funktionen **grün** und in Fettdruck gesetzt, was bedeutet, dass diese **Rechte gewährt werden**. Alle verweigerten Optionen/Funktionen sind **rot** und in Fettdruck dargestellt. Somit kann der Administrator hier von Beginn an sehr gut erkennen, welche Rechte dem jeweiligen Benutzer oder der jeweiligen Gruppe gewährt sind bzw. verwehrt wurden.

## Anderen Benutzern Zugriff gewähren

Dieses Recht steht Ihnen sowohl auf Datenbank-Ebene als auch für einzelne Einträge und Ordner innerhalb einer Datenbank zur Verfügung. Erlaubt der Administrator einem Benutzer, anderen Benutzern Zugriff gewähren zu dürfen, so kann dieser über den Client Daten mit anderen Server-Benutzern teilen, ohne, dass der Server-Administrator hierzu jedes Mal die Rechteverwaltung ändern muss. Dies ist beispielsweise hilfreich, wenn ein Benutzer einem anderen Benutzer temporär Zugriff auf einen seiner Einträge gewähren muss bzw. möchte.

Benutzer können anderen Benutzern/Gruppen über den Client Zugriff gewähren. Der genaue Vorgang wird in unserem

[Handbuch für den Windows-Client](#) beschrieben.

## Einträge versiegeln

Wird einem Benutzer der Zugriff auf einen Eintrag gewährt, so kann der Eintrag, der geteilt werden soll, zusätzlich versiegelt werden. Ein Zugriff ist dabei erst dann möglich, wenn das Siegel durch eine autorisierte Person im Server-Manager aufgehoben bzw. der Zugriff gewährt wurde.

**HINWEIS:** Nur Benutzer mit **Admin-Rechten** im Server-Manager können den Zugriff auf einen versiegelten Eintrag gewähren.

Der versiegelte Zugriff auf einen Eintrag wird ebenfalls über den Client eingestellt, und zwar steht diese Option zusätzlich zur Verfügung, wenn ein Benutzer einem anderen Benutzer Zugriff auf einen Eintrag gewährt. Dabei kann der Benutzer, der den Zugriff gewähren will, dann entscheiden, ob eine zusätzliche Versiegelung erforderlich ist oder nicht.

Das Einstellen eines Siegels für einen Eintrag wird ebenfalls detailliert im [Handbuch für den Windows-Client](#) beschrieben.

## Versiegelter Zugang

Wurde der Zugriff auf einen Eintrag in der Datenbank durch Benutzer A Benutzer B gewährt und eine Versiegelung des Eintrags erstellt, so ist es zunächst erforderlich, dass ein Benutzer mit Admin-Rechten am Enterprise Server den Zugriff auf den ausgewählten Eintrag erlaubt, damit der Zugriff auch erfolgen kann. Der Benutzer, der den Zugriff gewährt, bestimmt dabei, von welchem Benutzer am Server eine Genehmigung erforderlich ist.

Hierzu meldet sich der entsprechende Benutzer mit seinen Zugangsdaten am Enterprise Server an. Im Bereich **Datenbanken -> Berechtigungen** ist nun zu sehen, dass Benutzer B auf einen Eintrag in der ausgewählten Datenbank Zugriff gewährt wurde. Dabei wird der festgelegte Zeitraum des Zugriffs angezeigt, wer den Zugriff erstellt hat und ob der Eintrag versiegelt wurde. Per Doppelklick können die Berechtigungen geöffnet werden. Die Genehmigung wird dabei im Reiter **Versiegelter Zugang** erteilt.

Zu sehen ist hier der Status des Eintrags, der zum Beispiel auf Versiegelt gesetzt ist, wenn der entsprechende Eintrag versiegelt wurde. Über **Siegelstatus ändern** kann der entsprechende Status geändert werden. Folgende Optionen stehen nun hier als Status zur Verfügung:

- **Versiegelt:** Ein Eintrag ist nach wie vor versiegelt und es wurde noch nicht versucht, auf den entsprechenden Eintrag zuzugreifen.
- **Unversiegelt:** Die Versiegelung für einen Eintrag wurde aufgehoben.
- **Warten auf Genehmigung:** Der Benutzer, dem der Zugriff gewährt wurde, bittet konkret um eine Zugriffsgenehmigung. In diesem Fall hat er den entsprechenden Eintrag bereits öffnen wollen und fragt nun um Erlaubnis, den Eintrag öffnen zu können.
- **Genehmigung erteilt:** Eine autorisierte Person hat die Genehmigung für den Zugriff entsprechend erteilt.
- **Gebrochen:** Ein Siegel wurde gebrochen und damit auf einen Eintrag zugegriffen.

Nachdem der Status geändert wurde, kann in den Berechtigungen der Datenbank der neue Status eingesehen werden. Wurde eine Genehmigung erteilt, so kann der Benutzer, dem der Zugriff gewährt wurde, nun den Eintrag öffnen und das Siegel brechen.

Autorisierte Personen haben darüber hinaus die Möglichkeit, den Status des Siegels für einen Eintrag jederzeit zu ändern. Außerdem können Server-Administratoren auch weitere autorisierte Personen hinzufügen, die dann ebenfalls dazu berechtigt sind, den Status des Siegels zu ändern. Dies erfolgt im Reiter **Versiegelter Zugang** über die Schaltfläche **Hinzufügen**.

**Beispiel:** Der Benutzer Test1 gewährt Benutzer Test2 Zugriff auf einen Eintrag innerhalb der Datenbank für insgesamt 2 Wochen und versiegelt diesen Eintrag. Nach erteilter Genehmigung kann der Benutzer Test2 das Siegel brechen und auf den Eintrag zugreifen. Er sieht dann innerhalb der Datenbank nur den einzelnen Eintrag, auf dem ihm der Zugriff gewährt wurde - andere Daten sind für ihn innerhalb der Datenbank nicht einsehbar. Sofern erforderlich, kann ein Server-Administrator den Status des Siegels erneut ändern; so kann er den Eintrag beispielsweise erneut versiegeln, sodass Benutzer Test2 erneut um Genehmigung bitten muss, wenn er auf den entsprechenden Eintrag zugreifen möchte etc.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Eigenschaften einer Datenbank

In diesem Dialogfenster werden Ihnen allgemeine Informationen zur ausgewählten Datenbank angezeigt.

## Allgemein

Im Register **Allgemein** sehen Sie grundlegende Informationen zur ausgewählten Datenbank, z.B. die Benutzer, die die Datenbank derzeit geöffnet haben sowie Größe und Dateityp etc.

## Erweitert

Im Register **Erweitert** können Sie optional einstellen, ob Sie Zugriffe von Benutzern auf Einträgen in Serverdatenbanken überwachen und protokollieren möchten und ob Benutzer für das Löschen eines Eintrages Gründe angeben müssen.

**HINWEIS:** Die **Eigenschaften** im Bereich **Datenbanken** sind eher informativer Natur; die eigentlichen Zugriffsrechte werden in den **Berechtigungen** definiert.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Benutzer

Der Bereich **Benutzer** ermöglicht es dem Administrator, neue Benutzer hinzuzufügen und bestehende zu bearbeiten oder zu löschen. Die Zugriffsrechte der Benutzer werden jedoch im Bereich **Datenbanken** auf ausgewählte Datenbanken zugewiesen.

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Neuer Benutzer:** Öffnet das Dialogfeld **Benutzer hinzufügen**.
- **Eigenschaften:** Öffnet das Dialogfeld **Eigenschaften des Benutzers**.
- **Löschen:** Löscht die markierten Benutzer.
- **Trennen:** Trennt die Verbindung der markierten Benutzer zum Password Depot Enterprise Server.
- **Synchronisieren:** Mit dieser Option können Sie den markierten/ausgewählten Benutzer einzeln über AD synchronisieren, ohne dabei den Active Directory-Synchronisationsassistenten erneut aufrufen und den Benutzer hieraus importieren zu müssen. Bitte beachten Sie aber, dass der jeweilige Benutzer zuvor bereits per AD-Synchronisation über den entsprechenden Assistenten dem Enterprise Server hinzugefügt worden sein muss. Die Option **Synchronisieren** im Bereich **Benutzer** dient also beispielsweise dazu, einen am Server bereits angelegten Benutzer einzeln zu aktualisieren, wenn sich seine Active Directory-Daten geändert haben. Hierfür muss dann nicht erneut eine komplette AD-Synchronisation erfolgen.
- **Datenbank zuweisen:** Ermöglicht es, Datenbanken gleichzeitig mehreren Benutzern oder Gruppen zuzuweisen bzw. neue zu erzeugen. Außerdem können hier für die Benutzer private Datenbanken erzeugt werden.
- **2FA zurücksetzen:** Ermöglicht es Ihnen, bei Nutzung der **Zwei-Faktor-Authentifizierung** am Server, für einen oder mehrere Benutzer die Optionen der 2FA zurückzusetzen, sodass die ausgewählten Benutzer beim nächsten Anmelden am Server erneut einen Code angeben müssen. Die Option "Diesem Computer vertrauen" wird hiermit also zurückgesetzt und alle vertrauten Geräte des ausgewählten Benutzers werden gelöscht.
- **Alle auswählen:** Wählt alle Benutzer aus.

This command allows to synchronize with AD only the selected user without calling that Import from AD Wizard

**TIPP:** Diese Funktionen können Sie auch durch einen Rechtsklick auf einen Benutzer aus der Liste aufrufen.

---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*

# Benutzer hinzufügen

Die Schaltfläche **Neuer Benutzer** in der Symbolleiste des Bereichs **Benutzer** erlaubt das Anlegen eines neuen Benutzers und öffnet das Dialogfeld **Benutzer hinzufügen**. Folgende Registerkarten stehen Ihnen hier zur Verfügung:

## Allgemein

In der Registerkarte **Allgemein** sind folgende Angaben möglich:

- **UPN:** Hier können Sie den Benutzer-UPN (User Principal Name) des Benutzers aus dem Active Directory angeben.
- **Vollständiger Name:** Geben Sie den Vor- und Nachnamen des Benutzers.
- **E-Mail:** Geben Sie die E-Mail-Adresse des Benutzers an.
- **Abteilung:** Geben Sie die Abteilung des Benutzers an.
- **Beschreibung:** Hier können Sie, wenn nötig, weitere Angaben zum Benutzer hinterlegen.
- **ADs-Pfad:** Geben Sie hier den korrekten Active Directory-Pfad eines Benutzers an.
- GUID:

## Konto

In der Registerkarte **Konto** können Sie Folgendes einstellen:

### Am Server anmelden

Hier können Sie auswählen, ob ein Benutzer sich mit seinen **Windows NT-Zugangsdaten (SSO)** anmelden soll oder ob Sie als Administrator einen Benutzernamen und ein Kennwort selbst festlegen möchten.

### Konto-Optionen

**Konto deaktiviert:** Wenn hier ein Häkchen gesetzt ist, so ist der Account des betroffenen Benutzers aktuell gesperrt, beispielsweise, weil er die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen am Server erreicht hat. Entfernen Sie hier das Häkchen, um das Konto wieder zu aktivieren und dem Benutzer den Zugriff auf den Server wieder zu ermöglichen.

**Benutzer darf Kennwort nicht ändern:** Setzen Sie hier ein Häkchen, wenn Sie nicht möchten, dass ein Benutzer sein Kennwort für die Anmeldung am Enterprise Server ändern können soll.

**Benutzer muss Kennwort bei der nächsten Anmeldung ändern:** Setzen Sie hier ein Häkchen, wenn Sie möchten, dass ein Benutzer sein Kennwort für die Anmeldung am Enterprise Server bei seiner nächsten Anmeldung ändern soll.

**2-Faktor-Authentifizierung deaktiviert:** Setzen Sie hier ein Häkchen, wenn Sie möchten, dass für einen oder mehrere spezielle Benutzer die Anmeldung am Server per Zwei-Faktor-Authentifizierung deaktiviert sein soll. Dadurch können Sie die Anmeldung per 2FA im Server grundsätzlich für alle einstellen, im Nachgang aber für bestimmte Benutzer deaktivieren, wenn gewünscht oder erforderlich.

## Rollen

In dieser Registerkarte können Sie einem Benutzer zusätzlich verschiedene weitere Server-Rollen zuweisen, wodurch der Zugriff auf den Server-Manager rollenbasiert definiert werden kann. Folgende Server-Rollen stehen Ihnen hier zur Auswahl zur Verfügung:

- **Server-Administrator:** Vollzugriff auf den Enterprise Server und den Server-Manager. Ein Server-Administrator hat auf alle Datenbanken und Einträge des Servers Zugriff. Außerdem kann er über den Server-Manager den Server verwalten und konfigurieren.
- **Datenbank-Administrator:** Dieser kann neue Datenbanken auf dem Server erstellen und bereits bestehende Datenbanken bearbeiten, beispielsweise kann er bei bereits existierenden Datenbanken die Zugriffsrechte einzelner Benutzer und Gruppen anpassen.
- **Konto-Administrator:** Dieser kann Benutzer und Gruppen auf dem Server verwalten und in diesem Zusammenhang beispielsweise dem Server auch neue Benutzer und Gruppen zuweisen.
- **Active Directory-Verwalter:** Diese Server-Rolle ermöglicht es Benutzern, zusätzlich Vorgänge hinsichtlich der AD-Synchronisation durchzuführen.
- **Ereignisprotokoll-Leser:** Diese Server-Rolle ermöglicht Benutzern Zugriff auf die Protokolle des Servers.

## Mitglied von

Hier legen Sie fest, ob und in welchen Gruppen der Benutzer Mitglied ist.

**Gruppe hinzufügen:** Klicken Sie auf diese Schaltfläche, um den/die Benutzer/in einer neuen Gruppe zuzuweisen.

**Löschen:** Klicken Sie hier, um den/die Benutzer/in aus einer Gruppe zu entfernen.

## Erweitert

Die Registerkarte **Erweitert** ist in zwei Abschnitte unterteilt:

- **WebSockets-Port für Browser-Add-Ons**
- **Überprüfung IP-Adresse**

### WebSockets-Port für Browser-Add-Ons:

Hier kann der Admin über den Server-Manager die **benutzerdefinierte Verteilung der Portnummern für das Add-On** manuell festlegen. Verschiedene Optionen stehen hier zur Verfügung:

1. Globale Einstellungen verwenden [25109]
2. Automatisches Generieren der Portnummer
3. Benutzerdefinierte Portnummer verwenden

Wenn der Administrator die Portnummer eines Benutzers also direkt über den Server-Manager definiert, so muss der Benutzer dann nur noch im Client seine Portnummer selbst anpassen. Dies ist insbesondere bei Nutzung von Password Depot auf einem Terminal-Server notwendig.

### Überprüfung IP-Adresse:

Hier können Sie dem Benutzer eine feste IP-Adresse zuweisen, sodass ein Verbindungsversuch dieses Benutzers mit einer anderen als der hier angegebenen IP-Adresse abgewiesen wird. Dies kann die Sicherheit erhöhen, setzt jedoch voraus, dass statische IP-Adressen verwendet werden.

**HINWEIS:** Die Adressen 'localhost' und '127.0.0.1' sind **immer erlaubt**, sodass der Administrator falsche Einstellungen am Server korrigieren kann.



# Eigenschaften eines Benutzers

Das Dialogfeld **Eigenschaften** auf der Registerkarte **Benutzer** erlaubt es, die Eigenschaften eines Benutzers einzusehen und zu bearbeiten. Nähere Informationen zum Inhalt dieses Dialogfeldes finden Sie unter **Benutzer hinzufügen**.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Rechte für Benutzer

Wählen Sie im Bereich **Datenbanken** eine Datenbank aus und klicken Sie anschließend in der Symbolleiste auf **Eigenschaften**, um die Rechte für Benutzer im Dialogfeld **Eigenschaften einer Datenbank** zu setzen.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Datenbank zuweisen

Die Funktion **Datenbank zuweisen**, die Sie in der Symbolleiste **Benutzer** und **Gruppen** finden, ermöglicht es Ihnen, Datenbanken gleichzeitig mehreren Benutzern oder Gruppen zuzuweisen bzw. neue Datenbanken zu erzeugen.

Wählen Sie einen oder mehrere Benutzer/Gruppen aus und klicken Sie dann auf **Datenbank zuweisen**.

Im Dialogfeld **Datenbank zuweisen** stehen Ihnen zwei Register zur Verfügung:

## Datenbank

### Vorhandene Datenbank auswählen

Wählen Sie aus dem Dropdown-Menü eine vorhandene Datenbank aus, die Sie gleichzeitig allen, links unter **Ausgewählte Konten** markierten Elementen zuweisen. Im Register **Rechte** können Sie darüber hinaus die Zugriffsrechte setzen.

### Neue Datenbank erzeugen

Erzeugt eine neue, leere Datenbank, die Sie gleichzeitig allen, links unter **Ausgewählte Konten** markierten Einträgen zuweisen können. Im Register **Rechte** können Sie darüber hinaus die Zugriffsrechte setzen.

### Private Datenbank erzeugen

Erzeugt eine neue, **private** Datenbank für jeden, links unter **Ausgewählte Konten** markierten Eintrag. Im Register **Rechte** können Sie darüber hinaus die Zugriffsrechte setzen.

Diese Funktion ist hilfreich, wenn Sie viele Benutzer haben und Sie diesen (zusätzlich) auch private Datenbanken bereitstellen müssen.

## Rechte

Geben Sie hier die **Rechte** für die zuvor ausgewählten Datenbanken an.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Gruppen

Der Bereich **Gruppen** ermöglicht dem Administrator, neue Gruppen hinzuzufügen und bestehende zu bearbeiten oder zu löschen. Die Zugriffsrechte der Gruppen werden jedoch im Bereich **Datenbanken** ausgewählten Datenbanken zugewiesen.

Im oberen Bereich können Sie die Anzeige filtern. Geben Sie dazu einen Gruppennamen oder einen Teil davon ein, um nach einer bestimmten Gruppe aus der Liste zu suchen.

## Allgemeine Informationen zu Gruppen

Eine Gruppe besteht aus einem oder mehreren Mitgliedern (Benutzern). Um Benutzer einer Gruppe hinzuzufügen, öffnen Sie die Registerkarte **Benutzer**.

Durch das Erzeugen von Gruppen können Sie die Verwaltung vereinfachen, indem Sie später die Rechte für Datenbanken ganzen Gruppen zuweisen anstatt einzelnen Benutzern.

## Verfügbare Funktionen

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Neue Gruppe:** Erlaubt es, eine **neue Gruppe** zu erzeugen.
- **Eigenschaften:** Zeigt die Eigenschaften einer vorhandenen Gruppe an und erlaubt es, diese zu ändern.
- **Löschen:** Löscht eine Gruppe.
- **Synchronisieren:** Mit dieser Option können Sie die markierte/ausgewählte Gruppe einzeln über AD synchronisieren, ohne dabei den Active Directory-Synchronisationsassistenten erneut aufrufen und die Gruppe hieraus importieren zu müssen. Bitte beachten Sie aber, dass die jeweilige Gruppe zuvor bereits per AD-Synchronisation über den entsprechenden Assistenten dem Enterprise Server hinzugefügt worden sein muss. Die Option **Synchronisieren** im Bereich **Gruppen** dient also beispielsweise dazu, eine am Server bereits angelegte Gruppe einzeln zu aktualisieren, wenn sich bestimmte Active Directory-Daten geändert haben. Hierfür muss dann nicht erneut eine komplette AD-Synchronisation erfolgen.
- **Datenbank zuweisen:** Ermöglicht es, Datenbanken gleichzeitig mehreren Benutzern oder Gruppen zuzuweisen bzw. neue Datenbanken zu erzeugen.
- **Alle auswählen:** Wählt alle Gruppen aus.

**TIPP:** Diese Funktionen können Sie auch durch einen Rechtsklick auf eine Gruppe aus der Liste aufrufen.

# Neue Gruppe

Das Dialogfeld **Neue Gruppe** hat zwei Register:

## Allgemein

- **Gruppenbezeichnung:** Geben Sie den Namen der Gruppe ein.
- **Typ:** Bezeichnet den Typ der Gruppe, z.B. AD-Gruppe oder Standard, falls die Gruppe im Password Depot Server-Manager erzeugt wurde.
- **AD-Pfad:** Falls es eine AD-Gruppe ist, wird hier deren Pfad angezeigt, z.B. WinNT://WORKGROUP/TEAMSERVER/Benutzer.
- **Beschreibung:** Hier können Sie optional eine Beschreibung der Gruppe hinzufügen. Falls die Gruppe aus Active Directory synchronisiert wurde, wird die Beschreibung von dort übernommen.

Sie können diese Gruppe **aktivieren** oder **deaktivieren**, indem Sie das entsprechende Kontrollkästchen **Deaktiviert** im unteren linken Bereich anklicken oder nicht.

## Mitglieder

In der Registerkarte **Mitglieder** können Sie Benutzer einer Gruppe einsehen, Benutzer zu einer Gruppe hinzufügen sowie aus einer Gruppe entfernen ( **Löschen**).

Zum Hinzufügen von Mitgliedern einer Gruppe stehen Ihnen diese Möglichkeiten zur Verfügung:

- **Benutzer hinzufügen**
- **Benutzer über Abteilung hinzufügen**

---

Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)

# Benachrichtigungen

In diesem Bereich können Sie Benachrichtigungen verwalten, die bei bestimmten Ereignissen an ausgewählte Personen per E-Mail verschickt werden sollen.

Folgende Schaltflächen stehen Ihnen in der Symbolleiste der Benachrichtigungen zur Verfügung:

- **Neue Benachrichtigung:** Fügt eine neue Benachrichtigung hinzu.
- **Eigenschaften:** Öffnet die Eigenschaften einer bereits angelegten Benachrichtigung.
- **Löschen:** Löscht die ausgewählte Benachrichtigung.
- **Alle auswählen:** Wählt alle Benachrichtigungen aus.

**TIPP:** Diese Funktionen können Sie auch durch einen Rechtsklick auf eine Benachrichtigung aufrufen.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Neue Benachrichtigung

Die Schaltfläche **Neue Benachrichtigung** in der Symbolleiste der Benachrichtigungen öffnet das Dialogfeld **Neue Benachrichtigung**, in dem Sie eine neue Benachrichtigung anlegen können. Dieses Dialogfeld besteht aus zwei Registerkarten: **Allgemein** und **Erweitert**.

## Allgemein

Hier können Sie folgende Einstellungen vornehmen:

- **Ereignis:** Wählen Sie das Ereignis aus, über das Sie informiert werden möchten. Es stehen Ihnen hier viele verschiedene Ereignisse zur Verfügung, beispielsweise ein fehlgeschlagener Anmeldeversuch eines Benutzers oder das Hinzufügen einer neuen Datenbank. Mit Version 14 wurden drei weitere Ereignisse hinzugefügt, nämlich: **Ablauf der Einträge, Massentilgung von Einträgen und Kritische Änderung der Datenbankgröße**. Beim Ereignis **Ablauf der Einträge** erhalten Admins und Clients nun eine Benachrichtigung, wenn Einträge bald ablaufen oder bereits abgelaufen sind.
- **Der Benachrichtigung diese Anmerkungen hinzufügen:** Wenn Sie der E-Mail mit der Benachrichtigung Anmerkungen hinzufügen möchten, so können Sie diese hier eingeben.
- **Benachrichtigung an diese Empfänger senden:** Hier sehen Sie die Empfängerliste mit den E-Mail-Adressen, an die die Benachrichtigung verschickt wird.

Im Drop-Down Feld unten links können Sie die **E-Mail-Adresse** eingeben oder eine bestehende aus der Liste auswählen. Klicken Sie dann auf **Hinzufügen**, um die angegebene Adresse der Liste hinzuzufügen.

Wenn Sie eine E-Mail-Adresse ersetzen möchten, so markieren Sie die bisherige, geben im linken Feld die neue E-Mail-Adresse ein und klicken auf **Ersetzen**.

Um eine E-Mail-Adresse aus der Liste zu löschen, markieren Sie diese in der Liste und klicken Sie anschließend auf **Löschen**.

## Erweitert

Hier können Sie einstellen, dass die Benachrichtigung für bestimmte Ereignisse auf ausgewählte Datenbanken, Datenbankinträge oder Nutzer beschränkt werden soll.

Zwei Bereiche stehen dafür zur Auswahl:

### Benutzer und Gruppen

**Alle Benutzer und Gruppen:** Wenden Sie diese Option an, wenn die Benachrichtigung bei allen Benutzern und Gruppen ausgelöst werden soll.

**Ausgewählte Benutzer und Gruppen:** Hier können Sie einzelne Benutzer und Gruppen hinzufügen, die denen Sie diese Benachrichtigung erhalten möchten.

### Objekte

**Alle Datenbanken:** Wendet die Benachrichtigung für alle Datenbanken an.

**Ausgewählte Datenbanken:** Ermöglicht Ihnen, bestimmte Datenbanken auszuwählen, für die die Benachrichtigung gelten soll.

**Ausgewählte Einträge:** Falls Sie eine Benachrichtigung einstellen, die sich auf einzelne Einträge bezieht, steht Ihnen diese Option ebenfalls zur Verfügung, damit Sie aus einer Datenbank einen speziellen Eintrag auswählen können, für den die Benachrichtigung gelten soll.

# Eigenschaften einer Benachrichtigung

Die Schaltfläche **Eigenschaften** aus der Symbolleiste der Benachrichtigungen öffnet das Dialogfeld **Benachrichtigungs-Eigenschaften**, wo Sie die Eigenschaften der Benachrichtigung noch einmal überprüfen und ändern können. Nähere Informationen zu diesem Dialogfeld finden Sie unter [Benachrichtigung hinzufügen](#).

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*



# Protokoll

In dieser Ansicht wird das **Protokoll** der Serveraktivitäten angezeigt.

Sie haben im oberen Bereich die Möglichkeit, die Anzeige der Ereignisse zu filtern.

In der Symbolleiste des Bereichs Protokoll stehen Ihnen folgende Funktionen zur Verfügung:

- **Protokoll öffnen:** Ermöglicht Ihnen, eine Protokolldatei (\*.logx) zu öffnen.
- **Protokoll exportieren:** Ermöglicht Ihnen, das Protokoll in das XML- oder CSV-Format zu exportieren.
- **Erweiterter Filter:** Erlaubt die detaillierte [Filterung](#) der Datensätze des Protokolls.

**HINWEIS:** Die Sprache des Protokolls können Sie ändern, indem Sie in den Serveroptionen die Sprache des Servers ändern.

Die Serverprotokolle haben ein Standardformat nach RFC 5424 für die einfache Verarbeitung in externen Log-Analysern. Optional können alle Protokollaufzeichnungen im Echtzeitmodus per UDP an externe Protokollserver zur revisionssicheren Verarbeitung und Speicherung gesendet werden.

---

[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)

# Verbinden

Um den Server-Manager mit dem Dienst zu verbinden, klicken Sie auf **Server** -> **Status** -> **Verbinden**.

Geben Sie im sich öffnenden Dialogfeld die erforderlichen Daten ein, um sich am Server anzumelden.

- **Benutzername:** Geben Sie den Benutzernamen ein (voreingestellt: *admin*).
- **Kennwort:** Geben Sie das Kennwort ein (voreingestellt: *admin*).

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# SSL-Zertifikat

Password Depot Enterprise Server ermöglicht die Installation und Verwendung eines **SSL-Zertifikats**.

**WARNUNG:** Diese Installation sollte nur von einem erfahrenen Administrator durchgeführt werden.

Password Depot Enterprise Server unterstützt **X.509** SSL-Zertifikate im **PEM**- und **DER**-Format. Mit einem Zertifikat können Benutzer die Identität eines Servers überprüfen, bevor sie vertrauliche Informationen an diesen senden.

Bevor Sie sich für die Verwendung von SSL-Verbindungen entscheiden, beachten Sie bitte folgende Punkte:

- 1) SSL verschlüsselt **keine Daten**, die von Clients an den Server übertragen werden. Diese Daten werden vom internen Protokoll, das über TCP/IP implementiert ist, **immer** mit AES-256-Bit verschlüsselt.
- 2) Aus Gründen der plattformübergreifenden Kompatibilität muss die **OpenSSL**-Bibliothek verwendet werden, die einige Einschränkungen aufweist und von **Apple** nicht für die Verwendung auf Systemen wie iOS und macOS empfohlen wird.
- 3) Die Verwendung von selbstsignierten Zertifikaten ist **zwecklos** und wird nicht unterstützt. Nur Zertifikate, die von einer bekannten **Zertifizierungsstelle** (CA) signiert sind, können für die Validierung des Password Depot Enterprise Servers verwendet werden. Wenn Sie bereits einen Webserver besitzen, der auf HTTPS läuft, dann ist die Verwendung eines SSL-Zertifikats dieses Webservers eine geeignete Lösung. Andernfalls müssen Sie unter Umständen ein neues SSL-Zertifikat bei einer der anerkannten Zertifizierungsstellen bestellen.
- 4) Wenn Sie SSL-Verbindungen verwenden wollen, müssen Sie ein gültiges SSL-Zertifikat installieren, das von einer anerkannten Zertifizierungsstelle ausgestellt wurde. Der Enterprise Server kann ein **Dummy-Zertifikat** generieren, um die Verwendung der SSL-Verbindung zu testen, wenn kein anderes Zertifikat verfügbar ist. In der Praxis ist das Dummy-Zertifikat jedoch nutzlos, da es leicht von Dritten gefälscht werden kann.
- 5) In den **lokalen und internen Netzwerken** wird die Verwendung von SSL **nicht empfohlen**, da jegliche Datenübertragung zwischen dem Server und den Clients bereits stark verschlüsselt ist. Die Verwendung von SSL erhöht in dem Falle die Sicherheit der Datenübertragung nicht wesentlich, sondern ermöglicht die Validierung des Servers und hilft, **Man-in-the-Middle-Angriffe** (*MITM-Angriffe*) zu verhindern. Diese Funktion kann in externen Netzwerken nützlich sein, wenn sich Clients von jedem beliebigen Ort aus mit dem Server verbinden können sollen.
- 6) Wenn Sie sich für eine SSL-Verbindung entscheiden, stellen Sie bitte sicher, dass **alle** Ihre Clients (Windows, Mac OS X, Android und iOS) SSL verwenden! Gemischte Verbindungen (teilweise SSL und teilweise Standard-TCP/IP) sind **nicht erlaubt**.
- 7) Um ein SSL-Zertifikat zu **installieren**, müssen Sie Folgendes eingeben:
  1. Den vollqualifizierten Pfad zur Zertifikatsdatei auf dem Server.
  2. Wenn das obige Zertifikat sowohl öffentliche als auch private Schlüssel enthält, lassen Sie das Feld leer. Wenn der private Schlüssel in einer separaten Datei gespeichert ist, geben Sie den vollständigen Pfad zum privaten Schlüssel an.
  3. Das Passwort für den Zugriff auf den privaten Schlüssel.

Starten Sie den Server neu, um das Zertifikat zu laden und SSL-Verbindungen zu starten.

---

[Zur Homepage von Password Depot zurückkehren](#) (diese Hilfe verlassen)

# Benutzer über Abteilung hinzufügen

Dieses Dialogfeld ermöglicht es Ihnen, Benutzer über Abteilungen einer Gruppe hinzuzufügen.

---

*Zur [Homepage von Password Depot](#) zurückkehren (diese Hilfe verlassen)*

# Protokolleinträge filtern

Sie können die Anzeige des Protokolls filtern, um so die für Sie relevanten Informationen schneller abrufen zu können.

Klicken Sie dazu in der Symbolleiste des Bereichs **Protokoll** auf **Erweiterter Filter**.

Wenn Sie die Filterung aktivieren, stehen Ihnen zahlreiche Optionen zur Verfügung, um die Darstellung der Protokolleinträge auf die gewünschten zu reduzieren.

---

*[Zur Homepage von Password Depot zurückkehren \(diese Hilfe verlassen\)](#)*

# Index

Active Directory

[Serveroptionen](#)

Active Directory-Struktur

[Active-Directory-Synchronisation](#)

Active-Directory-Import

[Active-Directory-Synchronisation](#)

Active-Directory-Synchronisation

[Active-Directory-Synchronisation](#)

[Active-Directory-Synchronisation](#)

Administration

[Installation und Betrieb](#)

Administrator

[Serveroptionen](#)

Migration

[Migration](#)

Anwendung

[Programmoptionen](#)

Ausführung

[Installation und Betrieb](#)

Authentifizierung

[Serveroptionen](#)

Authentifizierungen

[Serveroptionen](#)

Benachrichtigung

[Eigenschaften einer Benachrichtigung](#)

neue

[Neue Benachrichtigung](#)

Benachrichtigungen

[Benachrichtigungen](#)

[Benachrichtigungen](#)

Benachrichtigungs-Eigenschaften

[Eigenschaften einer Benachrichtigung](#)

[Eigenschaften einer Benachrichtigung](#)

Benachrichtigung

[Neue Benachrichtigung](#)

Benutzer

[Benutzer](#)

[Benutzer](#)

[Eigenschaften eines Benutzers](#)

[Rechte für Benutzer](#)

[Rechte für Benutzer](#)

Benutzer duplizieren

[Benutzer](#)

Benutzer hinzufügen

[Benutzer hinzufügen](#)  
[Benutzer hinzufügen](#)  
Benutzer löschen  
[Benutzer](#)  
Benutzerbericht  
[Berichte](#)  
[Berichte](#)  
Benutzerkonto  
[Serveroptionen](#)  
Benutzers  
[Eigenschaften eines Benutzers](#)  
Berechtigungen  
[Benutzer hinzufügen](#)  
Bereich Benutzer  
[Benutzer](#)  
Bereich Gruppen  
[Gruppen](#)  
Benutzer  
[Berichte](#)  
Datenbank  
[Berichte](#)  
Berichte  
[Berichte](#)  
Betrieb  
[Installation und Betrieb](#)  
[Installation und Betrieb](#)  
Client-Sicherheitsrichtlinien  
[Client-Sicherheitsrichtlinien](#)  
[Client-Sicherheitsrichtlinien](#)  
Corporate Edition  
[Client-Sicherheitsrichtlinien](#)  
CSV  
[Protokoll](#)  
Datenbank  
[Berechtigungen](#)  
importieren  
[Datenbank dem Server hinzufügen](#)  
neu  
[Datenbank dem Server hinzufügen](#)  
Datenbank zum Server hinzufügen  
[Datenbank dem Server hinzufügen](#)  
Datenbank zuweisen  
[Datenbank zuweisen](#)  
benachrichtigen  
[Neue Benachrichtigung](#)  
Bereich  
[Datenbanken](#)

Eigenschaften

[Berechtigungen](#)

hinzufügen

[Datenbank dem Server hinzufügen](#)

Rechte

[Berechtigungen](#)

zuweisen

[Datenbank zuweisen](#)

Datenbanken hinzufügen

[Datenbanken](#)

Datenbanken löschen

[Datenbanken](#)

Datenbanken-Bericht

[Berichte](#)

[Berichte](#)

Datensicherung

[Serveroptionen](#)

[Serveroptionen](#)

Definition sicherheitsrelevanter Programmooptionen

[Client-Sicherheitsrichtlinien](#)

Benutzer hinzufügen

[Benutzer hinzufügen](#)

Dialogfeld Benutzer

[Benutzer hinzufügen](#)

Dialogfeld neue Gruppe

[Neue Gruppe](#)

[Neue Gruppe](#)

Dialogfeld neuer Benutzer

[Benutzer hinzufügen](#)

Dialogfeld Serveroptionen

[Serveroptionen](#)

Dialogfeld Serverrichtlinien

[Serverrichtlinien](#)

Server

[Installation und Betrieb](#)

Domäne

[Active-Directory-Synchronisation](#)

E-Mail Einstellungen

[Serveroptionen](#)

Eigenschaften

[Berechtigungen](#)

[Berechtigungen](#)

[Eigenschaften eines Benutzers](#)

[Eigenschaften eines Benutzers](#)

[Rechte für Benutzer](#)

Einführung

[Einführung](#)



[Einführung](#)

Server

[Serveroptionen](#)

Einstellungen am Client

[Client-Sicherheitsrichtlinien](#)

Erweiterter Filter

[Protokoll](#)

Fehlgeschlagene Anmeldungen

[Serveroptionen](#)

Freigabecode

[Server-Lizenz](#)

Großbuchstaben

[Serverrichtlinien - Sicherheit](#)

Gruppe

[Neue Gruppe](#)

Neu

[Neue Gruppe](#)

Gruppen

[Gruppen](#)

[Gruppen](#)

Datenbanken zuweisen

[Gruppen](#)

Duplizieren

[Gruppen](#)

[Gruppen](#)

Eigenschaften

[Gruppen](#)

Löschen

[Gruppen](#)

Installation

[Installation und Betrieb](#)

[Installation und Betrieb](#)

IP eingrenzen

[Benutzer hinzufügen](#)

Kennwortqualität

[Serverrichtlinien - Sicherheit](#)

Server

[Server-Lizenz](#)

Localhost

[Installation und Betrieb](#)

Mail Einstellungen

[Serveroptionen](#)

Mehrere Datenbanken zuweisen

[Datenbank zuweisen](#)

Menü Verwalten

[Verwalten](#)

Migration

[Migration](#)

Mitglied

[Benutzer hinzufügen](#)

Mitglied von

[Benutzer hinzufügen](#)

Neue Benachrichtigung

[Neue Benachrichtigung](#)

Neue Datenbank

[Datenbank dem Server hinzufügen](#)

[Datenbank zuweisen](#)

[Datenbank zuweisen](#)

[Datenbanken](#)

Neue Verbindung

[Serveroptionen](#)

Neuer Benutzer

[Benutzer](#)

[Benutzer hinzufügen](#)

Optionen

[Programmoptionen](#)

[Serveroptionen](#)

Server

[Serveroptionen](#)

Postausgangsserver

[Serveroptionen](#)

[Serveroptionen](#)

Private Datenbank

[Datenbank zuweisen](#)

Private Datenbanken

[Datenbank zuweisen](#)

Programmoptionen

[Programmoptionen](#)

[Programmoptionen](#)

[Verwalten](#)

Programmstart

[Serveroptionen](#)

Programmverzeichnis

[Installation und Betrieb](#)

Protokoll

[Protokoll](#)

[Protokoll](#)

Protokoll exportieren

[Protokoll](#)

Protokoll filtern

[Protokoll](#)

Protokoll öffnen

[Protokoll](#)

Protokolldatei

[Protokoll](#)

Protokollierung

[Serveroptionen](#)

Rechte

[Rechte für Benutzer](#)

Rechte für Benutzer

[Serverrichtlinien - Rechte](#)

[Serverrichtlinien - Rechte](#)

mehrere Datenbanken

[Datenbank zuweisen](#)

Rechte für Datenbank

[Berechtigungen](#)

Rechte für Einträge und Ordner

[Berechtigungen](#)

Rechte vergeben

[Berechtigungen](#)

Rechteverwaltung

[Berechtigungen](#)

Rechteverwaltung in Password Depot Enterprise Server

[Serverrichtlinien](#)

Richtlinie

[Client-Sicherheitsrichtlinien](#)

Richtlinien

[Serverrichtlinien - Sicherheit](#)

Schaltfläche Neue Benachrichtigung

[Neue Benachrichtigung](#)

Server hinzufügen

[Datenbank dem Server hinzufügen](#)

Server Lizenz

[Server-Lizenz](#)

Server-Lizenz

[Server-Lizenz](#)

Server-Manager

[Server-Manager](#)

[Server-Manager](#)

Server-Port

[Serveroptionen](#)

Server-Richtlinien

[Serverrichtlinien](#)

[Serverrichtlinien - Rechte](#)

[Serverrichtlinien - Sicherheit](#)

Server-Zertifikat

[Serveroptionen](#)

Serveraktivitäten

[Protokoll](#)

Serveroptionen

[Serveroptionen](#)

[Serveroptionen](#)  
Serverrichtlinien  
[Serverrichtlinien](#)  
[Serverrichtlinien](#)  
[Serverrichtlinien - Rechte](#)  
[Serverrichtlinien - Sicherheit](#)  
Sicherheit  
[Serverrichtlinien - Sicherheit](#)  
[Serverrichtlinien - Sicherheit](#)  
Sicherheitsrichtlinien  
[Verwalten](#)  
Client  
[Client-Sicherheitsrichtlinien](#)  
Sicherungen  
[Serveroptionen](#)  
Single-Sign On  
[Serveroptionen](#)  
Speicherort  
[Serveroptionen](#)  
[Serveroptionen](#)  
Sprache  
[Programmoptionen](#)  
[Serveroptionen](#)  
Sprache des Servers  
[Serveroptionen](#)  
SSL/TLS  
[Serveroptionen](#)  
SSL/TLS verwenden  
[Serveroptionen](#)  
SSL/TLS-Optionen  
[Programmoptionen](#)  
Status  
[Verwalten](#)  
Struktur  
[Active-Directory-Synchronisation](#)  
Symbolleiste  
[Server-Manager](#)  
Benachrichtigungen  
[Benachrichtigungen](#)  
Benutzer  
[Benutzer](#)  
Datenbanken  
[Datenbanken](#)  
Gruppen  
[Gruppen](#)  
Protokoll  
[Protokoll](#)

Server-Manager

[Server-Manager](#)

Synchronisation

[Active-Directory-Synchronisation](#)

[Serveroptionen](#)

Active Directory

[Active-Directory-Synchronisation](#)

Übersicht

[Einführung](#)

Upgrade

[Migration](#)

Verwalten

[Verwalten](#)

Verzeichnis

[Serveroptionen](#)

Voreinstellungen

[Serverrichtlinien - Rechte](#)

Vorhandene Datenbank

[Datenbank dem Server hinzufügen](#)

Windows-Anwendung

[Installation und Betrieb](#)

Wörterbuchangriffe

[Serverrichtlinien - Sicherheit](#)

XML

[Protokoll](#)

Zugangsdaten

[Installation und Betrieb](#)

Zugriffsrechte

[Benutzer](#)

[Berechtigungen](#)

[Berechtigungen](#)

# Glossar