Password DEPOT

Handbuch

Password Depot Enterprise Server 16

Zuletzt aktualisiert: 02.02.22

AceBIT
Every Bit an Ace!

Einführung

Password Depot Enterprise Server ist eine Erweiterung für Password Depot. Mit Hilfe des Enterprise Servers können Benutzer über den Client auf einem Server gespeicherte Datenbanken gemeinsam nutzen. Als Client dient dabei das Password Depot-Hauptprogramm für Windows. Zusätzlich stehen Ihnen auch ein macOS-Client sowie unsere mobilen Apps für Android und iOS zur Verfügung, über die Sie ebenfalls eine Verbindung zum Enterprise Server herstellen können. Über die Clients können die Server-Datenbanken geöffnet und die darin gespeicherten Daten verwendet werden.

Der Password Depot Enterprise Server wird auf einem Computer im lokalen Netzwerk installiert. Über den Server-Manager, dem Verwaltungstool des Enterprise Servers, erstellt der Administrator Server-Datenbanken, legt Benutzer und Gruppen an und weist diesen die gewünschten Datenbanken zu. Benutzer können dabei auf die gesamte Datenbank oder aber auch nur auf bestimmte Objekte innerhalb einer Datenbank Zugriffsrechte erhalten.

Grundsätzlich können Sie Ihre Server-Datenbank so strukturieren, dass viele Benutzer darauf zugreifen können, je nach Zugriffsrechten aber eine andere Ansicht der Server-Datenbank haben.

Die zugelassenen Benutzer können über einen Client die Server-Datenbanken empfangen. Zur Anmeldung wird Folgendes benötigt:

- Adresse des Servers
- **Port**
- Zugangsdaten (Benutzername & Kennwort)

Die Zugangsdaten werden vom Administrator festgelegt. Die Anmeldung kann entweder über einen **lokalen Benutzer (Benutzername und Kennwort),** per Integrierter Windows-Authentifizierung (SSO) oder Azure AD-Authentifizierung erfolgen.

Zudem kann der Administrator über den Server-Manager weitere Serveroptionen, wie beispielsweise die Nutzung eines SSL-Zertifikats oder die Zwei-Faktor-Authentifizierung, bestimmen, Benachrichtigungen für bestimmte Ereignisse generieren lassen und allgemein geltende Serverrichtlinien etc. festlegen.

Der Datenaustausch zwischen dem Enterprise Server und den Clients wird durch AES-265-Bit verschlüsselt - die Client-Server-Verbindung erfolgt über TCP/IP (IPv4/IPv6). Dadurch können Sie sicherstellen, den Vorgaben der Datenschutz-Grundverordnung (DSGVO) zu entsprechen.

Fazit:

Mit dem Password Depot Enterprise Server können Sie

- im Unternehmen Daten zentral nutzen und gemeinsam mit allen Mitarbeitern sicher teilen.
- Ihre Daten nur im lokalen Netzwerk oder auch weltweit, über das Internet, zur Verfügung stellen.
- die Struktur Ihrer Datenbanken und die Zugriffsrechte Ihrer Benutzer selbst bestimmen.
- selbst entscheiden, wo Sie Ihre sensiblen Daten speichern, da Password Depot eine On-Premises-Lösung ist.

Erfahren Sie in unserem Erklärvideo, was Password Depot Enterprise Server für Ihr Unternehmen tun und wie es Sie bei der täglichen Arbeit unterstützen kann:

Password Depot Enterprise Server kurz & bündig erklärt

Oder lernen Sie Password Depot Enterprise Server in einem persönlichen und kostenlosen Webinar kennen:

Password Depot-Webinar

Die Systemanforderungen für Password Depot und **Password Depot Enterprise Server** können Sie im Detail hier einsehen:

Password Depot & Password Depot Enterprise Server - Systemanforderungen

---

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 er aber auch auf jedem beliebigen Computer installiert werden, der im Netzwerk erreichbar ist, vorausgesetzt der Computer verfügt über eine fest zugeordnete IP-Adresse im lokalen Netzwerk.

HINWEIS: Sie können den Enterprise Server (zum Beispiel zu Testzwecken) auch auf Ihrem lokalen Computer installieren. Um in diesem Fall mit dem Password Depot-Client auf den Server zuzugreifen, geben Sie als Server-Adresse 127.0.0.1 bzw. localhost an (oder alternativ auch die Adresse des Servers).

Installation als Windows-Dienst oder als Windows-Anwendung

Password Depot Enterprise Server kann in zwei Modi betrieben werden:

- als Windows-Systemdienst
- als Windows-Anwendung

Standardmäßig wird der Server als Windows-Systemdienst installiert. Um ihn als Windows-Anwendung zu installieren, wählen Sie im Installations-Setup die entsprechende Option.

HINWEIS: Es wird empfohlen, die Installation als Windows-Systemdienst durchzuführen. Hierbei wird der Dienst während der Installation im Hintergrund gleich eingerichtet.

Bei der Installation als Dienst wird der Server als Password Depot Enterprise Server aufgeführt und eingerichtet. Der Dienst läuft dann im Hintergrund immer automatisch mit, das heißt, in der Regel wird Password Depot Enterprise Server automatisch beim Start von Windows gestartet. 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. Unter den Windows-Diensten können Sie den Dienst des Password Depot Enterprise Servers bei Bedarf auch manuell starten oder stoppen.

Falls Sie den Server als Anwendung installiert haben, finden Sie ihn im Programmverzeichnis (standardmäßig ist das *C:\Program Files\AceBIT\Password Depot Server x* unter Vista, Windows 7,8 und Windows 10 bzw. *C:\Programme\AceBIT\Password Depot Server x* 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 das separate Verwaltungstool für Password Depot Enterprise Server. Es ermöglicht die Administration des Servers und die Einstellung diverser Optionen, zum Beispiel das Erstellen neuer Datenbanken. Bei Installation wird der Server-Manager automatisch mitinstalliert und ist dann auf dem System verfügbar, auf dem auch der Server läuft.

Um den Server-Manager aufzurufen, klicken Sie entweder auf Start -> **AceBIT -> Password** Depot Server Manager x oder doppelklicken Sie auf das entsprechende Desktop-Symbol. Der Server-Manager wird mit folgenden Standard-Zugangsdaten für den Login installiert:

Benutzername: Admin

Kennwort: admin

HINWEIS: Es wird dringend empfohlen, nach Installation und erstmaliger Anmeldung diese Standard-Zugangsdaten für den Administrator (also für das Konto des Super-Admins) im Server-Manager zu ändern. Gehen Sie dazu im Server-Manager auf **Benutzer -> admin ->** Konto und ändern Sie hier die Zugangsdaten unter Password Depot-Zugangsdaten.

Zur Anmeldung am Server-Manager wird zudem die IP-Adresse des Servers, auf dem der Enterprise Server läuft, sowie die entsprechende Portnummer benötigt. In Version 16 lautet die Portnummer standardmäßig 25016.

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

Updates

Im Server-Manager können Sie unter Hilfe -> Nach Updates suchen überprüfen, ob für den Password Depot Enterprise Server und Server-Manager Updates vorliegen. Wenn Ihnen hier angezeigt wird, dass eine neue Version zur Verfügung steht, dann empfehlen wir Ihnen, diese zu installieren, damit Ihre Software auf dem aktuellen Stand ist. Folgendes ist dabei zu beachten:

Der Server-Manager verfügt nicht über einen integrierten Update-Manager, das heißt, im Server-Manager selbst wird Ihnen nur angezeigt, ob eine neue Version verfügbar ist - Sie können diese im Anschluss allerdings nicht direkt herunterladen, sondern müssen hierzu auf unsere Webseite gehen. Starten Sie im Anschluss das Installations-Setup neu - das Update kann dann über die bestehende

Installation "drüber" installiert werden. Wenn es sich um kleinere Updates innerhalb der gleichen Hauptversion handelt, dann muss dabei der Dienst des Servers nicht angehalten werden.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Migration

Wenn Sie bereits mit einer Vorgängerversion des Enterprise Servers gearbeitet und nun eine neue Hauptversion erworben haben, so können Sie den gesamten Server sehr einfach auf die aktuelle Version migrieren. Bitte beachten Sie dabei Folgendes:

Enterprise Server und Windows-Clients können immer nur in der gleichen Hauptversion miteinander kommunizieren. Sie können also nicht mit einem Windows-Client der Version 12x auf einen Server der Version 15x zugreifen und umgekehrt. Aus diesem Grund müssen Sie die Windows-Clients und den Enterprise Server immer gleichzeitig auf eine neue Hauptversion aktualisieren.

Anders gestaltet sich dies bei unseren Editionen für macOS, iOS und Android. Ab Version 15 und höher können Sie mit diesen auch eine Verbindung zu Servern älterer Versionen herstellen (aktuell zu den Vorgängerversionen 15, 14 sowie 12). Hierzu ist es notwendig, im Anmeldefenster die entsprechende Hauptversion anzuklicken. Der Port wird automatisch angepasst.

Beim Wechsel auf eine neue Hauptversion können Sie alle Datenbanken sowie die Benutzer und Einstellungen übernehmen. In unserer Knowledge Base erläutern wir die Durchführung der Migration des Enterprise Servers Schritt für Schritt und wir empfehlen Ihnen, die Anleitung genau zu befolgen, denn dann ist die Migration in wenigen Minuten vollzogen. Zur Anleitung gelangen Sie hier:

Wie migriere ich den Enterprise Server auf eine neue Hauptversion?

HINWEIS: Die Anleitung in der Knowledge Base können Sie auch heranziehen, wenn Sie Ihre aktuelle Server-Installation auf einen anderen Server umziehen möchten. Die Schritte sind dabei genau gleich wie bei einem Wechsel auf eine neue Hauptversion; der einzige Unterschied ist, dass Sie in der gleichen Version bleiben und hier dann auf dem neuen Server die gleichen Verzeichnisse wie auf dem alten Server verwenden (sofern Sie die Standard-Verzeichnisse nutzen). Grundsätzlich können Sie Password Depot Enterprise Server ganz einfach auf dem neuen Server "frisch" installieren und im Anschluss, wie in der Anleitung beschrieben, die Datenbanken und cfg-Datei auf den neuen Server kopieren.

Zu Referenzzwecken (insbesondere dann, wenn Sie von einer sehr alten Version migrieren) können Sie auch folgenden Knowledge Base-Artikel heranziehen:

Migration des Enterprise Servers auf Version 12

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Nutzung auf einem Terminal-Server

Grundsätzlich ist es möglich, Password Depot auch auf einem Terminal-Server zu betreiben. Die Nutzung eines Terminal-Servers wird dabei nicht explizit empfohlen, sie ist jedoch möglich.

Hinsichtlich der Installation müssen Sie nichts weiter beachten, diese gestaltet sich auf einem Terminalserver genauso wie auf einem physischen Server. Wir empfehlen Ihnen, stets den Anweisungen des Installationsassistenten zu folgen, dann sollte die Installation in wenigen Minuten durchführbar sein.

Auch die Lizenzierung von Password Depot und Password Depot Enterprise Server ist bei Nutzung eines Terminalservers gleich. Ausführliche Informationen zu unserem Lizenzmodell finden Sie hier:

Lizenzierung und Softwarewartung

Was ist auf einem Terminal-Server bei aktiviertem Browser-Add-On zu beachten?

Wenn Sie Password Depot mit mehreren Benutzern auf einem Terminalserver verwenden und gleichzeitig das Browser-Add-On aktiviert haben, dann ist es zwingend erforderlich, dass Sie jedem Benutzer eine eigene Portnummer zur Kommunikation mit dem Add-On zuweisen. Wenn Sie dies nicht tun, dann kann es vorkommen, dass Benutzer A die Zugangsdaten von Benutzer B zugesendet bekommt, da das Browser-Add-On in dem Moment nicht wissen kann, welcher Benutzer die Daten anfragt - Sie laufen also Gefahr, dass Benutzer Daten zugesandt bekommen, die sie gar nicht sehen können sollen oder dürfen. Die Socket-Portnummer zur Kommunikation mit dem Browser-Add-On ist nämlich kein virtueller, sondern ein physikalischer Parameter und kann daher nicht von mehreren Instanzen der Password Depot-Clients gemeinsam genutzt werden.

Wie werden den Benutzern individuelle Portnummern zugewiesen?

Es gibt hier zwei Möglichkeiten:

1. Gehen Sie im Server-Manager auf Verwalten -> Serveroptionen -> Erweitert und aktivieren Sie unter WebSockets Port für Clients die Option Automatisches Generieren der Portnummern (empfohlen für Terminalserver). Im Anschluss wird jedem einzelnen Client automatisch eine individuelle Portnummer zugewiesen.

2. Gehen Sie im Server-Manager in den Bereich Benutzer und wählen Sie den gewünschten Benutzer aus. Öffnen Sie dessen Eigenschaften durch einen Doppelklick und gehen Sie im Anschluss zur Registerkarte Erweitert. Unter WebSockets-Port für Browser-Add-Ons wählen Sie die Option Benutzerdefinierte Portnummer verwenden und stellen hier pro Benutzer einen anderen Wert ein.

Die benutzerdefinierten Portnummern (entweder automatisch generiert oder aber durch den Administrator individuell zugewiesen) können Benutzer im Anschluss im Client selbst unter Bearbeiten -> Optionen -> Browser einsehen. Abschließend ist es dann noch notwendig, dass Benutzer diese individuelle Portnummer im Browser selbst abändern, was leider nicht automatisiert erfolgen kann. Hierzu muss der Benutzer auf das Add-On-Symbol im Browser klicken und dann unter Einstellungen die Portnummer entsprechend abändern.

HINWEIS: Wenn Sie Ihren Benutzern keine individuellen Portnummern zuweisen möchten, so empfehlen wir dringend, die Nutzung des Browser-Add-Ons im Server-Manager für Ihre Benutzer zu deaktivieren, um den oben beschriebenen Problemen vorzubeugen bzw. solche Probleme grundsätzlich zu vermeiden.

Weitere Informationen zu diesem Thema stehen Ihnen auch in folgendem Knowledge Base-Artikel zur Verfügung: Wie ändere ich die Portnummer bei Verwendung des Add-Ons, wenn Password Depot auf einem Terminal-Server läuft?

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Server-Manager

Der Server-Manager ist das separate Verwaltungstool des Enterprise Servers. Hierüber findet die zentrale Steuerung des Servers statt, das heißt, über den Server-Manager haben Sie schnellen und unkomplizierten Zugriff auf alle Funktionen des Servers, können diesen hierüber warten und konfigurieren. Sie müssen sich zunächst am Server-Manager mit den Zugangsdaten des Administrators anmelden, um die nachfolgend beschriebenen Funktionen sehen und die Konfiguration des Servers vornehmen zu können.

WARNUNG: Das Administrator-Kennwort sollte grundsätzlich nur dem Adminstrator selbst bekannt sein bzw. solchen Personen, die dazu authorisiert sind, den Enterprise Server zu verwalten. Bedenken Sie, dass jeder, der das Administrator-Kennwort kennt, Zugriff auf den Server-Manager und somit auf die komplette Verwaltung des Servers erhält!

Der Navigationsbereich des Server-Managers besteht aus fünf Bereichen:

- Datenbanken: Dieser Bereich dient dem Anlegen und Verwalten von neuen sowie bereits existierenden Server-Datenbanken.
- Benutzer: Dieser Bereich enthält Funktionen zur Verwaltung der Benutzer. Unter anderem können Sie hier dem Server neue Benutzer hinzufügen oder bereits bestehende Benutzer bearbeiten.
- Gruppen: Hier können Gruppen erstellt und Benutzer diesen Gruppen zugewiesen werden. Außerdem können Sie hier bestehende Gruppen verwalten.
- Benachrichtigungen: Hier können Benachrichtigungen für bestimmte Ereignisse erstellt werden, die dann per E-Mail versandt werden.
- Protokoll: Hier werden Ihnen die Serveraktivitäten Ihrer Benutzer und Gruppen angezeigt.

Wenn Sie im Navigationsbereich des Server-Managers auf die IP-Adresse klicken, können Sie grundlegende Informationen zum Enterprise Server einsehen:

- Status: Zeigt an, ob der Server aktuell läuft oder angehalten ist.
- Server-Adresse: Zeigt die IP-Adresse des Servers an.
- Server-Port: Zeigt den verwendeten 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 der jeweiligen 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.
- Spiegelung: Wenn Sie unter Verwalten -> Serverspiegelung die Spiegelung Ihres Enterprise Servers eingerichtet haben, dann wird Ihnen hier der Status der Serverspiegelung angezeigt.

HINWEIS: Sollten Sie das Kennwort zur Anmeldung am Server-Manager vergessen haben, so gibt es einen Workaround, den Sie durchführen müssen, um wieder Zugriff auf die Server-Konsole zu erhalten. Was genau in diesem Fall zu tun ist, können Sie hier nachlesen: Wie kann ich das Administrator-Kennwort im Password Depot-Server "zurücksetzen"?

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Verwalten

Dieser Menüpunkt befindet sich in der Hauptansicht des Server-Managers oben rechts. Er beinhaltet folgende Funktionen:

- Serveroptionen: Hier können grundlegende Einstellungen am Server vorgenommen werden, so z. B. wo und wie oft Sicherungskopien angelegt werden sollen, welche Methoden der Authentifizierung unterstützt werden sollen oder auch ob zur Anmeldung am Enterprise Server über die Clients die Zwei-Faktor-Authentifizierung verwendet werden soll etc.
- Server-Lizenz: Ermöglicht die Eingabe eines neuen Lizenzschlüssels, um die Anzahl der erlaubten Clients zu erhöhen. Außerdem können Sie hier Ihre aktuelle Lizenz sowie die aktuell eingesetzte Serverversion einsehen.
- Serverrichtlinien: Hier können globale Standard-Rechte für den gesamten Server festgelegt werden. Dies betrifft die allgemeine Rechtevergabe auf dem Server, die Kennwortrichtlinien sowie die unterstützen Eintragstypen. Bitte beachten Sie, dass sich alle Serverrichtlinien immer auf den gesamten Server und alle Benutzer beziehen, das heißt, auf untergeordneter Ebene können solche Rechte nicht mehr geändert werden. Deaktivieren Sie z.B. hier im Reiter "Rechte" bestimmte Rechte auf dem Server, so können diese im Anschluss nicht mehr für einzelne Benutzer aktiviert werden. Die Serverrichtlinien sind daher sehr restriktiv und sollten mit Vorsicht behandelt werden. Grundsätzlich empfehlen wir hier den Status Aktiviert oder Nicht definiert zu verwenden.
- Client-Sicherheitsrichtlinien: Diese kommen bei Verwendung des Corporate Client zum Einsatz. In diesem Fall können Sie als Admin Ihren Benutzern umfassende Richtlinien mitgeben und das Programm noch detaillierter konfigurieren, was mit dem Standard-Client so nicht möglich ist. Mehr zum Corporate Client und den Client-Sicherheitsrichtlinien erfahren Sie hier.
- Serverspiegelung: Hierüber können Sie die Spiegelung Ihres Servers einrichten und somit dessen Hochverfügbarkeit gewährleisten.
- Anhalten: Unterbricht die Verfügbarkeit des Servers für alle Clients. Der Server-Manager ist 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.
- Programmoptionen: Ermöglicht das Einstellen der Programmoptionen (nicht zu verwechseln mit den Serveroptionen). Die Programmoptionen beziehen sich dabei ausschließlich auf den Server-Manager, so z.B. in welcher Sprache dessen Benutzeroberfläche angezeigt werden soll.
- Beenden: Beendet den Server-Manager. Der Dienst oder die Server-Anwendung sind davon nicht betroffen, sodass Benutzer nach wie vor Zugriff auf die Server-Datenbanken erhalten.

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 Programms automatisch, sollte ein Neustart des Servers erforderlich sein. Wenn der Password Depot Enterprise Server diesen vorschlägt, empfehlen wir, ihn sogleich durchzuführen.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Serveroptionen

Die Serveroptionen sind das erste Dialogfeld im Menüpunkt Verwalten. Es stehen Ihnen hier folgende Registerkarten zur Verfügung: Allgemein, Verbindungen, Protokollierung, Sicherungsdateien, Erweitert, E-Mail, 2FA-Einstellungen, Active Directory sowie Azure-AD. Über die Serveroptionen können Sie den Enterprise Server allgemein konfigurieren und dabei Einstellungen vornehmen, die den gesamten Server und alle Benutzer betreffen. Im Folgenden werden die einzelnen Registerkarten sowie deren Inhalt erläutert.

Allgemein

Server

Hier können Sie folgende Einstellungen des Servers vornehmen:

- Sprache des Servers: Erlaubt es, die Sprache des Servers (nicht der Benutzeroberfläche!) festzulegen. Sie können hier zwischen Deutsch und Englisch wählen.
- Server-Port: Legt den Port für die Verbindung fest. Grundsätzlich wird hier der von Password Depot vorgegebene Standardport gezeigt, der auf Wunsch aber angepasst werden kann. Beachten Sie bei Anpassung des Ports, dass anschließend auch im Client für die Serververbindung der korrekte Port angegeben wird.
- Internet-Protokoll: Sie können hier zur Verbindung ein bestimmtes Internet-Protokoll festlegen, das standardmäßig genutzt werden soll. Folgende Optionen stehen zur Verfügung: **IPv4+IPv6**, IPv4, IPv6. Je nach entsprechender Netzwerk-Konfiguration können Administratoren daher festlegen, welche Internet-Protokoll-Versionen der Server grundsätzlich unterstützen soll. Der Server sendet dann per UDP an die Clients eine Info-Nachricht zur unterstützten Internet-Protokoll-Version, sodass die Clients im Anschluss dann automatisch die richtige Version für die Haupt-TCP-Verbindung wählen.
- SSL/TLS verwenden: Aktivieren Sie die Nutzung einer SSL/TLS-Verbindung zwischen Enterprise Server und den Clients. Klicken Sie auf Zertifikat installlieren, um das entsprechende Zertifikat am Server zu hinterlegen. Es öffnet sich im Anschluss ein neues Fenster, in dem Sie den Pfad zu Ihrer Zertifikatsdatei sowie deren Schlüssel erfassen können. Außerdem erfolgt hier auch die Eingabe eines Kennworts.
- Keepalive aktivieren: Die Keepalive-Option wird verwendet, wenn der Client mit einem Server kommuniziert, der sich nicht im gleichen Netzwerk befindet.

REST-Server

- Ursprungs-URL: Geben Sie hier die korrekte URL Ihres Password Depot-Web-Servers ein, das heißt, die genaue URL, über die Ihr Enterprise Server in Verbindung mit dem Web-Client erreichbar ist.

- SSL/TLS für REST-Server verwenden: Aktivieren Sie die Nutzung einer SSL/TLS-Verbindung bei der REST-Server-Verbindung. Durch die REST-Server-Implementierung kann auf den Enterprise Server nun 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. Die Installation des Zertifikats für REST-Server erfolgt dann in diesem Fall über die Schaltfläche Zertifikat installieren rechts daneben.

TIPP: Weitere Informationen zur Nutzung eines SSL-Zertifikats am Enterprise Server finden Sie hier: Wie funktioniert die SSL-Verbindung am Enterprise Server und wie richte ich diese ein?

Datenbanken

- Speicherort: Gibt den Pfad an, unter dem standardmäßig die Server-Datenbanken abgelegt werden. Per Vorgabe ist dies bei Password Depot 15 *C:\Program Files\AceBIT\Password Depot Server 15\Data\DB*. Auf Wunsch können Sie diesen Pfad anpassen, jedoch empfehlen wir, in jedem Falle ein lokales und keine gemappten Laufwerke für das Abspeichern der Server-Datenbanken zu wählen, da es bei Letzeren zu Zugriffsproblemen kommen kann. Sofern der Password Depot Enterprise Server während des Abspeicherns den in den Serveroptionen angegebenen Pfad nicht finden kann, springt er zurück auf die Standardeinstellungen und speichert die Datenbanken im entsprechenden Standard-Ordner ab.

Verbindungen

Unterstützte Authentifizierungen

Legen Sie fest, welche Arten der Authentifizierung Sie auf Ihrem Server zulassen möchten. Dabei können Sie zwischen den Optionen Zugangsdaten (Konto und Kennwort), Integrierte **Windows-Authentifizierung (Single Sign On)** sowie Azure Active Directory wählen. Sie können verschiedene Arten der Authentifizierung auf Ihrem Server gleichzeitig aktiviert haben.

TIPP: Ausführliche Informationen zur Nutzung der Integrierten Windows-Authentifizierung und der hierfür notwendigen Einstellungen finden Sie in unserer Knowledge Base unter: Wie erfolgt die Anmeldung am Enterprise Server per Single Sign-On (SSO)? .

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
- Android Edition
- iOS Edition
- macOS Edition
- 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:

Bestimmen Sie hier wie mit Verbindungen des gleichen Benutzers auf weiteren Geräten verfahren werden soll. Sie können hier zwischen den folgenden Optionen wählen:

- Neue Verbindungen verweigern, wenn Benutzer bereits angemeldet ist
- Bestehende Verbindung beenden und neue erlauben
- Mehrere Verbindungen von verschiedenen IP-Adressen erlauben

HINWEIS: Der Enterprise Server ist, wie die meisten anderen ähnlichen Server, nicht dafür vorgesehen, mehrere Verbindungen desselben Benutzers zuzulassen. Diese Option wurde eingeführt, weil es durchaus vorkommen kann, dass Benutzer gleichzeitig eine Verbindung von einem Client und einem mobilen Gerät aus benötigen. Das funktioniert immer noch, weil mobile Geräte nicht in Echtzeit synchronisiert werden. Wenn sich ein Benutzer aber mit seinem Account gleichzeitig über zwei Windows-Clients verbinden möchten, kann das ein Problem verursachen und es kommt zur Trennung einer der beiden bestehenden Verbindungen.

Inaktive Sitzungen

Legen Sie fest, wie Password Depot Enterprise Server mit inaktiven Verbindungen verfahren soll. Sie können hier zum Beispiel bestimmen, dass der Client vom Server nach x Minuten der Inaktivität getrennt werden soll. Zusätzlich können Sie dann bei Aktivierung der Option veranlassen, dass die geöffnete Datenbank geschlossen und der entsprechende Client abgemeldet wird.

Fehlgeschlagene Anmeldungen

Geben Sie an, nach wie vielen fehlgeschlagenen Anmeldeversuchen 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.

HINWEIS: Fehlgeschlagene Anmeldeversuche über den Client am Enterprise Server werden nicht nach x Stunden oder Tagen wieder zurückgesetzt werden - das heißt also im Umkehrschluss, der Password Depot Server-Manager "merkt" sich immer die Anzahl der fehlgeschlagenen Versuche und addiert diese dann entsprechend. Wenn der Benutzer allerdings nach 2 fehlgeschlagenen Anmeldeversuchen das Kennwort beim dritten Mal korrekt eingibt (sofern in den Serveroptionen die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen auf 3 gestellt ist), dann wird die Gesamtanzahl wieder auf 0 gesetzt. In diesem Fall werden also die vorherigen Fehlversuche gelöscht und der Benutzer hat dann von neuem wieder 3 Anmeldeversuche, bis er wieder gesperrt wird usw.

Protokollierung

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

Lokales Protokoll

- Protokollordner: Bestimmen Sie, in welchem Verzeichnis die Protokolle des Enterprise Servers abgespeichert werden sollen. Standardmäßig lautet das Verzeichnis hierfür *C:\Program Files\AceBIT\Password Depot Server 15\Logs*. Über die Schaltfläche Durchsuchen können Sie dieses anpassen, wir empfehlen Ihnen jedoch, nach Möglichkeit hier immer ein lokales Verzeichnis zu verwenden.
- Max. Dateigröße: Definieren Sie, wie groß die Protokolldatei des Servers (KB) maximal sein soll.
- Neue Protokolldatei erstellen: Legen Sie fest, wann die Protokolldatei jeweils erzeugt werden soll.
- Protokolle löschen: Definieren Sie die Einstellungen zum Löschen von bereits existierenden Protokollen. So können Sie entweder einstellen, dass Server-Protokolle nie gelöscht werden sollen oder aber Sie legen eine bestimmte Anzahl an Protokollen fest, die behalten werden sollen, beispielsweise 30 (standardmäßig voreingestellt). Dies bedeutet, dass die letzten 30 Protokolle behalten und alle älteren automatisch gelöscht werden.

Remote Protokoll

- Protokollmeldungen an einen Remote-Server senden: Setzen Sie hier ein Häkchen, wenn Sie möchten, dass die Protokolldateien des Enterprise Servers automatisch an einen externen Remote-Server gesendet werden. Dadurch können Sie sicherstellen, dass die Protokolle des Servers nicht durch unbefugten Zugriff manipuliert werden.

Sicherungsdateien

In dieser Registerkarte können Sie Einstellungen zu Ihrer Datensicherung im Allgemeinen vornehmen. Folgendes kann dabei von Ihnen festgelegt werden:

Datensicherung

- Sicherungsordner: Hier können Sie festlegen, wo die Sicherungsdateien des Servers gespeichert werden sollen. Standardmäßig lautet das Verzeichnis hierfür *C:\Program Files\AceBIT\Password Depot Server 15\Backups*. Über die Schaltfläche Durchsuchen können Sie dieses anpassen, wir empfehlen Ihnen jedoch, auch hier nach Möglichkeit immer ein lokales Verzeichnis zu verwenden. Es werden dabei Sicherungen Ihrer Datenbanken, Logs sowie der cfg-Datei (*pwd_srv.cfg*), in der Ihre Benutzer und Einstellungen gespeichert sind, angelegt.
- Datenbanken bei jedem Programmstart sichern: Markieren Sie diese Option, damit Password Depot Enterprise Server bei jedem Start eine neue Sicherungskopie anfertigt.
- Datenbanken sichern alle: Legen Sie einen Zeitpunkt fest, wann Password Depot Enterprise Server automatisch eine Sicherungskopie anfertigen soll. Wir empfehlen, dies mindestens einmal am Tag (also alle 24 Stunden) zu tun.
- Sicherungsdateien löschen, die älter sind als: Aktivieren Sie diese Option und bestimmen Sie einen Zeitraum, wenn Sie möchten, dass Sicherungsdateien älter als x Monate automatisch aus dem Backup-Verzeichnis des Servers gelöscht werden.

HINWEIS: Standardmäßig sind die beiden Optionen Datenbanken bei jedem Programmstart sichern und Datenbanken sichern alle x Stunden 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:

Einträge bearbeiten

- Zeit, bis der Eintrag gesperrt wird (Min.): Legen Sie eine Zeit (in Minuten) fest, nach deren Ablauf sich ein Eintrag automatisch sperren soll, wenn ein Benutzer diesen Eintrag geöffnet hat, ihn gerade jedoch nicht nutzt. Standardmäßig sind hier fünf Minuten vorgegeben, diesen Zeitraum können Sie sowohl verringern als auch erhöhen.

Private Datenbanken

- Private Datenbanken für neue Benutzer automatisch erzeugen: Legen Sie fest, ob für jeden neuen Benutzer, der dem Enterprise Server 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: Private_DB_<BENUTZER>.pswe.
- Private Datenbanken von gelöschten Benutzern automatisch löschen: Umgekehrt können Sie mit dieser Option festlegen, ob private Datenbanken beim Löschen eines Server-Benutzers 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.

HINWEIS: Bitte beachten Sie, dass standardmäßig beide Optionen deaktiviert sind.

WebSockets-Port für Clients

- Standard-Portnummer verwenden: Die Standard-Portnummer für das Add-On 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. Auf Wunsch bzw. wenn notwendig, kann die Portnummer jedoch manuell geändert werden. Bitte beachten Sie in diesem Fall, dass dies sowohl im Client selbst (Bearbeiten -> Optionen -> Browser -> WebSockets-Port) als auch im Browser selbst in den Add-On-Einstellungen geändert werden muss.
- 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 Browser-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 bei Einsatz eines Terminal-Servers 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) daher 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. Die Benutzer können im Anschluss die eigens zugewiesene Portnummer über die Client-Optionen auslesen und müssen diese danach nur noch im Browser selbst anpassen.

TIPP: Mehr zu diesem Thema erfahren Sie hier: Wie ändere ich die Portnummer bei Verwendeung des Add-Ons, wenn Password Depot auf einem Terminal-Server läuft?

E-Mail

In dieser Registerkarte können Sie Einstellungen zu einem E-Mail-Server vornehmen:

- Absender: Hier können Sie die E-Mail-Adresse des Absenders sowie 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 zuvor vorgenommenen Einstellungen zu überprüfen.

2FA-Einstellungen

Hier können Sie einstellen, ob Sie eine Zwei-Faktor-Authentifizierung Ihrer Benutzer am Server wünschen und diese aktivieren möchten.

Betriebsart

- TOTP - Codes werden von mobilen Authenticator-Apps generiert: Um für die Anmeldung den zweiten Faktor zu erhalten, ist die Nutzung einer Authenticator-App notwendig.
- E-Mail - Codes werden vom Server an die Standardadresse des Benutzers gesendet: Der zweite Faktor wird hier per E-Mail an den entsprechenden Benutzer und die jeweils hinterlegte E-Mail-Adresse gesendet.
- Benutzer dürfen sich die Geräte merken lassen (Tage): Der Administrator hat hier 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 auch die Option Diesem Computer vertrauen ausgewählt hat.
- Ablaufzeit des E-Mail-Codes (Minuten): Der Admin kann für einen per E-Mail versandten Code einen Zeitraum der Gültigkeit standardmäßig festlegen. Gibt ein Benutzer den Code nicht rechtzeitig ein, so läuft dieser ab und verliert im Anschluss seine Gültigkeit.

In diesem Fall muss für eine korrekte Authentifizierung sodann ein neuer Code angefordert werden.

TIPP: In unserer Knowledge Base 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; außerdem können Sie im Benutzerbereich die 2FA für Ihre Benutzer auch zurücksetzen, falls es zu Problemen kommen sollte. Mehr dazu können Sie auch im Bereich Benutzer lesen.

Active Directory

Synchronisation

- Automatische AD-Synchronisation alle: Aktivieren Sie die automatische Active Directory-Synchronisation und in welchen Abständen diese durchgeführt werden soll. Zusätzlich können Sie einstellen, was während der automatischen Synchronisation mit Benutzern und Gruppen passieren soll, die nicht (mehr) in Active Directory gefunden werden. Sie können solche Benutzer entweder ignorieren, deaktivieren oder löschen lassen. Beachten Sie bitte jedoch, dass sich diese Optionen ausschließlich auf den Enterprise Server beziehen, nicht aber auf die Active Directory an sich - hier werden grundsätzlich keine Änderungen durchgeführt.

HINWEIS: Vorzugsweise sollte die Synchronisation vom Administrator zu gegebenem Anlass manuell angestoßen werden. Falls Sie eine automatische Synchronisation benötigen, sollte diese nach Möglichkeit zu Zeiten, in denen die Serverlast gering ist und dann beispielsweise alle 24 Stunden erfolgen.

Azure-AD

Mandanten

Hier können Sie dem Server-Manager und Enterprise Server eine neue Organisation hinzufügen, über die Sie im Anschluss die Azure AD-Synchronisation durchführen möchten.

- Neu: Klicken Sie auf Neu, um den Vorgang zu starten. Im Anschluss müssen Sie einen Microsoft-Account wählen und sich mit Ihren Admin-Zugangsdaten hier anmelden. Nach erfolgreicher Anmeldung können Sie im Mandanten-Bereich die hinzugefügte Organisation sehen. Gehen Sie nun im Server-Manager auf Extras -> Azure AD-Synchronisation, um Azure AD-Benutzer dem Server per automatischer Synchronisation hinzuzufügen. Im entsprechenden Synchronisationsassistenten können Sie nun die zuvor hinzugefügte Organisation auswählen.

TIPP: Alternativ können Sie diesen Vorgang auch direkt über Extras -> Azure AD-Synchronisation starten. Auch hier finden Sie die Schaltfläche Neu, um eine Organisation für die Azure AD-Synchronisation auszuwählen und dem Server hinzuzufügen.

- Aktualisieren: Über die Schaltfläche Aktualisieren können Sie eine bereits hinzugefügte Organisation im Server-Manager aktualisieren.
- Löschen: Über die Schaltfläche Löschen können Sie Organisationen wieder aus dem Server-Manager löschen, sollten Sie diese beispielsweise nicht mehr benötigen. Anschließend können Sie über die Schaltfläche Neu eine andere Organisation zur Azure AD-Synchronisation auswählen.

HINWEIS: Weitere Informationen zur Azure AD-Synchronisation im Server-Manager erhalten Sie auch im Kapitel Azure AD-Synchronisation im Bereich Extras.

Synchronisation

- Automatische AD-Synchronisation alle: Hier können Sie, wie bei der normalen automatischen Active Directory-Synchronisation auch, die automatische Azure AD-Synchronisation alle x Minuten aktivieren. Die Azure AD-Benutzer und ihre Attribute werden dann zu dem festgelegten Intervall immer automatisch synchronisiert und aktualisiert. Die Option Benutzer und Gruppen nicht im AD gefunden funktioniert hier gleichermaßen wie bei der normalen automatischen Active Directory-Synchronisation, mit dem einzigen Unterschied, dass sie sich eben auf die Azure AD bezieht.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Server-Lizenz

Wenn Sie im Menü oben rechts auf **Verwalten ->** Server-Lizenz klicken, öffnet sich das Dialogfeld zum Hinzufügen einer neuen Lizenz. Darüber hinaus können Sie hier auch die aktuell verwendete Server-Lizenz bzw. Server-Version einsehen.

Wenn Sie die Anzahl an Lizenzen erweitert haben, können Sie hier Ihren neuen Freigabecode eingeben und damit die Anzahl an erlaubten Clients auf dem Server erhöhren.

Lizenzierung

Sie benötigen eine Lizenz des Enterprise Servers in der gewünschten Benutzeranzahl. Diese definiert die Anzahl der Benutzer, die Sie am Server maximal anlegen können (Hinweis: Es zählen seit Version 12 nicht mehr die gleichzeitigen Verbindungen).

Das Einrichten von maximal drei Benutzern am Enterprise Server erfordert keine Lizenz. In diesem Falle kann der Server kostenlos heruntergeladen und eingesetzt werden. Bitte beachten Sie, dass in diesem Fall aber trotzdem die entsprechende Anzahl an Clients lizenziert werden (zwischen einer und drei Client-Lizenzen, je nachdem wie viele letztendlich benötigt werden). Bei mehr als drei Benutzern ist auch der Erwerb einer Serverlizenz erforderlich. Diese Lizenz wird staffelweise angeboten: Sie beginnt bei fünf Benutzern und endet bei einer unbegrenzten Benutzeranzahl.

Mit dem Erwerb des Enterprise Servers in der gewünschten Benutzeranzahl erhalten Sie alle Clients **für alle unterstützten Betriebssysteme** sowie das Web-Interface. Enterprise Server und Client (Hauptprogramm) werden daher im Paket verkauft.

Erworbene Lizenzen sind Named Licences, die immer nur von einem Benutzer, jedoch auf beliebig vielen **Computern** installiert und verwendet werden dürfen. Darüber hinaus kann eine Lizenz in allen verfügbaren lokalisierten Sprachen genutzt werden.

Alle Servergrößen und Preise sowie weitere Informationen zur Lizenzierung können Sie unserer Webseite entnehmen:

Enterprise Server kaufen

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Serverrichtlinien

Die Serverrichtlinien erreichen Sie über das Menü Verwalten.

Über die Serverrichtlinien können Sie einige globale Einstellungen vornehmen, die unter anderem die Rechtevergabe an die Clients betreffen. Darüber hinaus können Sie hier die allgemeinen Kennwortrichtlinien konfigurieren und bestimmen, welche Eintragstypen in den Clients standardmäßig zur Verfügung stehen sollen. Das Dialogfeld ist dabei unterteilt in die Registerkarten Rechte, Sicherheit und Einträge.

Rechte

In dieser Registerkarte können Sie für Ihre Benutzer globale Richtlinien bestimmen, die standardmäßig für alle Benutzer und Datenbanken auf dem Server gelten. Hierzu können Sie zwischen den folgenden Status wählen:

- Nicht definiert (neutral): Sie können das entsprechende Recht für jede Datenbank und jeden Benutzer in den Datenbank-Berechtigungen nachträglich noch individuell einstellen.
- Aktiviert (erlaubt): Das entsprechende Recht wird für alle Datenbanken und Benutzer auf dem Server standardmäßig erlaubt. Sie können den Status für einzelne Benutzer/ Datenbanken jedoch in den Datenbank-Berechtigungen nachträglich noch ändern.
- Deaktiviert (nicht erlaubt): Dieser Status ist sehr restriktiv. Wenn Sie diesen wählen, so ist das entsprechende Recht für alle Datenbanken und Benutzer auf dem Server grundsätzlich verweigert. Es kann nachträglich in den Datenbank-Berechtigungen nicht mehr für einzelne Datenbanken/Benutzer geändert werden.

Standardmäßig sind alle Richtlinien hier entweder auf Nicht definiert oder Aktiviert gesetzt. Dies bedeutet, dass diese Richtlinien auf globaler (Server-) Ebene erlaubt bzw. nicht näher definiert sind. Dieser Status ermöglicht Ihnen, die Rechte im weiteren Verlauf auf Datenbank-Ebene oder auch für einzelne Ordner und Einträge innerhalb der Datenbanken näher zu spezifizieren. Dies ist allerdings nicht möglich, wenn Sie in den Serverrichtlinien den Status Deaktiviert einstellen, denn in den Serverrichtlinien einmal deaktivierte Rechte können nachträglich auf Datenbank-Ebene oder auch für einzelne Ordner und Einträge nicht mehr aktiviert werden. Es handelt sich dabei also um ein sehr restriktives Recht, was nur verwendet werden sollte, wenn Sie ein bestimmtes Recht für den gesamten Server sowie alle Benutzer deaktivieren möchten.

BEISPIEL: Das Exportieren von Einträgen soll grundsätzlich für keinen Benutzer ermöglicht werden und daher auf dem Server gar nicht erst möglich sein. In diesem Fall bietet es sich an, das entsprechende Recht in den Severrichtlinien auf "Deaktiviert" zu setzen - auf diese Weise kann der Status dieses Rechts nachträglich nicht mehr geändert werden und Sie können sicher sein, dass der Export von Daten über den Client gar nicht erst als Option angeboten wird.

TIPP: Wir empfehlen Ihnen, die Rechte grundsätzlich entweder auf Nicht definiert oder Aktiviert zu belassen. Auf diese Weise haben Sie im Nachhinein genug Spielraum und Möglichkeiten, die Rechte detaillierter zu vergeben und dabei vor allen Dingen auch benutzer- oder gruppenspezifische Rechte zu vergeben. Die detaillierte Rechtevergabe findet im Anschluss dann unter Datenbanken -> Berechtigungen statt.

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.

Sicherheit

In dieser Registerkarte können Sie bestimmte Kennwortrichtlinien für die Clients definieren.

So können Sie zum Beispiel eine Mindestlänge für Kennwörter bestimmen und festlegen, welche Zeichenarten ein Kennwort standardmäßig haben sollte. Diese Kennwortrichtlinien werden dann an die Clients weiter- und hier als Standard vorgegeben. Beim Generieren eines neuen Kennworts haben Benutzer dann zwar dennoch die Möglichkeit, diese Einstellungen abzuändern, aber, wenn für die Kennwörter im Server-Manager eine Mindestlänge bestimmt wurde, dann kann diese in keinem Fall unterschritten werden - hingegen kann ein Kennwort aber durchaus mehr Zeichen besitzen.

HINWEIS: Die Kennwortrichtlinien werden nur bei generierten Kennwörtern (über den integrierten Kennwort-Generator im Client) strikt angewendet. Erstellt sich ein Benutzer beispielsweise selbst ein Kennwort, das eigentlich nicht den gesetzten Kennwort-Richtlinien entspricht, dann werden Benutzer auf die Einhaltung der Richtlinien zwar hingewiesen, jedoch nicht dazu gezwungen, diese einzuhalten, um mögliche Konflikte mit Voraussetzungen Dritter (beispielsweise Webseiten) zu vermeiden.

BEISPIEL: Setzen Sie ein Häkchen bei Kennwortqualität auf Anfälligkeit gegen Wörterbuchangriffe prüfen, damit jedes Mal eine Warnung ausgegeben wird, wenn ein Benutzer ein Kennwort oder eine Zeichenkette verwendet, die in einem Wörterbuch enthalten sind.

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.

Einträge

In dieser Registerkarte haben Sie als Server-Administrator die Möglichkeit, die verschiedenen Eintragstypen zentral über den Server-Manager festzulegen. Standardmäßig werden alle Eintragstypen unterstützt, daher sind auch alle in den Serverrichtlinien angehakt. Insgesamt können Sie zwischen 11 verschiedenen Eintragstypen wählen:

- Kennwort
- Kreditkarte
- Softwarelizenz
- Identität
- Information
- Banking
- Verschlüsselte Datei
- Dokument
- Remote-Desktopverbindung
- PuTTY
- TeamViewer

BEISPIEL: Wenn Sie nicht möchten, dass Ihre Benutzer den Eintragstypen "Kreditkarte" verwenden, so können Sie in den Serverrichtlinien den Haken für diesen Eintragstypen entfernen. Dies bewirkt, dass dieser gar nicht erst im Client angezeigt wird und Benutzer dementsprechend auch keine Kreditkarten-Daten in der Server-Datenbank speichern können.

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

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 und eingestellt werden. Über die Client-Sicherheitsrichtlinien können Sie die Clients detaillierter konfigurieren und dadurch erzwingen, dass alle Clients diese Einstellungen befolgen müssen.

HINWEIS: Die Client-Sicherheitsrichtlinien greifen im Client selbst nur, wenn die Corporate Edition des Windows-Clients verwendet wird. Die Standardversion des Password Depot Clients, die ebenfalls im Download-Bereich zur Verfügung steht, unterstützt diese Richtlinien NICHT.

Weitere Informationen zur Corporate-Edition von Password Depot finden Sie hier:

Corporate Edition von Password Depot und Client-Sicherheitsrichtlinien

Richtlinie für Master-Kennwort

In diesem Bereich können Sie bestimmte Kennwortrichtlinien festlegen, die standardmäßig für alle Benutzer obligatorisch sind. Diese Kennwortrichtlinien werden dann strikt auf alle neuen Kennwörter angewendet, die innerhalb einer Server-Datenbank erstellt werden. Solche neuen Kennwörter müssen dann den im Server-Manager gesetzten Anforderungen entsprechen.

- **Kennwort muss Komplexitätsanforderungen entsprechen:** Neue Kennwörter müssen mindestens die angegebenen Zeichentypen enthalten (Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen).
- **Kennwortverlauf erzwingen:** Bestimmt die Anzahl der eindeutigen neuen Kennwörter, die verwendet werden müssen, bevor ein altes Kennwort wiederverwendet werden kann.
- **Maximales Alter für Kennwörter:** Bestimmt die Zeitspanne (in Tagen), die ein Kennwort verwendet werden kann, bevor das System den Benutzer auffordert, es zu ändern.
- **Mindestalter für Kennwörter:** Legt die Zeitspanne (in Tagen) fest, die ein Kennwort verwendet werden muss, bevor der Benutzer es ändern kann.
- **Kennwortlänge mindestens:** Legt fest, wie lange ein Kennwort mindestens sein muss.

Richtlinie für erlaubte Speicherorte

Ermöglicht es, festzulegen, welche Speicherorte (wie z.B. Lokales System, Cloud-Dienste etc.) die Clients zusätzlich zum Enterprise Server verwenden dürfen. Alle Speicherorte, die Sie hier deaktivieren, werden erst gar nicht im Client angezeigt und können daher von den Benutzern zum Speichern von Datenbanken außerhalb des Enterprise Servers gar nicht genutzt werden. Folgende Speicherorte stehen in Password Depot im Allgemeinen zur Verfügung:

- Lokales System
- Enterprise Server
- USB-Speicher-/Wechselmedium
- Internetserver
- Dropbox
- Google Drive
- OneDrive/OneDrive for Business
- HiDrive
- Box

Richtlinie für Aktionen

Ermöglicht es, festzulegen, ob bestimmte Aktionen wie z.B. das Drucken oder Exportieren von Einträgen auf dem Server grundsätzlich erlaubt sind. Dazu gehören:

- Daten in die Zwischenablage kopieren
- Drucken
- Exportieren
- Externe Dateien entschlüsseln
- Externe Dateien verschlüsseln
- Externe Dateien vollständig löschen
- Synchronisieren (von Datenbanken)
- TANs verwenden
- Zweite Passwörter einstellen

Programmoptionen

Ermöglicht die Definition relevanter sowie sicherheitstechnischer Programmoptionen. Dazu gehören:

- Anzahl der gespeicherten Sicherungskopien: Bezieht sich auf Datenbanken, die außerhalb des Enterprise Servers gespeichert werden (sofern erlaubt). Die Sicherungsdateien werden dann auf dem lokalen System des Benutzers gespeichert.

- Automatische Reinigung der Zwischenablage: Definieren Sie eine bestimmte Zeit (in Sekunden) nach der mit Password Depot in die Zwischenablage kopierte Kennwörter aus dieser wieder herausgelöscht werden.
- Automatischer Update-Modus: Legen Sie fest, ob die Clients automatisch nach neuen Updates suchen sollen oder nicht.
- Datenbank nach jeder Änderung automatisch speichern: Bezieht sich auf Datenbanken, die außerhalb des Enterprise Servers gespeichert werden (sofern erlaubt). Ist diese Option aktiviert, so wird die Datenbank nach jeder Änderung automatisch gespeichert.
- Datenbank schließen und Programm sperren: Bei Nichtbenutzung des Computers
- Datenbank schließen und Programm sperren: Immer, wenn das Programm minimiert wird
- Datenbank schließen und Programm sperren: Wenn sich das Programm automatisch minimiert
- Datenbank schließen und Programm sperren: Wenn sich der Computer in den Standby- oder Ruhezustand begibt
- Datenbank schließen und Programm sperren: Wenn sich die aktuelle Sitzung ändert
- Internetprotokollversion: Wählen Sie zwischen IPv4 und IPv6, wenn Sie eines der beiden grundsätzlich festlegen möchten.
- Kennwörter in der Listenansicht anzeigen: Legen Sie fest, ob die Hauptansicht des Clients die Spalte "Kennwort" enthalten soll. Die Kennwörter werden allerdings auch hier aus Sicherheitsgründen immer nur verdeckt angezeigt.
- Liste zuletzt verwendeter Datenbanken speichern: Bezieht sich auf Datenbanken, die außerhalb des Enterprise Servers gespeichert werden (sofern erlaubt). Ist diese Option aktiviert, so können im Client über den Datenbank-Manager -> Zuletzt verwendet kürzlich geöffnete Datenbanken leicht abgerufen werden.
- Lokale Kopie beim Schließen der Remote-Datei automatisch löschen: Wenn Benutzer lokale Kopien der Server-Datenbank auf ihrem System lokal speichern dürfen, dann können Sie diese Option aktivieren, um sicherzustellen, dass diese lokale Kopie sofort wieder gelöscht wird, wenn die Verbindung zum Enterprise Server gestoppt und die Server-Datenbank geschlossen wird.
- Lokale Kopie der Dateien von Password Depot Enterprise Server speichern: Erlaubt das lokale Speichern von Server-Datenbanken, z.B. für die Nutzung des Offline-Modus. Dabei ist zu beachten, dass jeder Benutzer immer nur die Ansicht der Server-Datenbank lokal speichert, die er auch bei aktiver Server-Verbindung sieht.
- Nach Updates suchen (Tage): Wenn die Clients automatisch nach Updates suchen sollen, dann können Sie hier ein bestimmtes Zeitintervall einstellen.
- Sicherungskopie beim Speichern einer Datenbank erzeugen: Bezieht sich auf Datenbanken, die außerhalb des Enterprise Servers gespeichert werden (sofern erlaubt). Die Sicherungsdateien werden dann auf dem lokalen System des Benutzers gespeichert. Ist die Option aktiviert, so wird bei jedem Speichern der Datenbank ebenfalls eine neue Sicherungsdatei erzeugt.
- Sicherungskopie beim Öffnen einer Datenbank erzeugen: Auch dies bezieht sich auf Datenbanken, die außerhalb des Enterprise Servers gespeichert werden (sofern erlaubt). Ist die Option aktiviert, so wird bei jedem Öffnen der Datenbank automatisch auch eine neue Sicherungsdatei erstellt.
- Standard-Authentifizierungsmodus: Legen Sie fest, wie sich Ihre Benutzer am Enterprise Server standardmäßig anmelden sollen. Folgende Optionen stehen hier zur Auswahl: Nicht definiert (Client kann beliebigen Wert verwenden), Integrierte

Windows-Authentifizierung (SSO), Mit Benutzername und Passwort anmelden sowie Azure AD-Authentifizierung.

- Standard-Gültigkeitsdauer für Kennwörter: Definieren Sie eine Standard-Gültigkeitsdauer für alle Kennwörter der Server-Datenbank.
- Zuletzt verwendete Kennwörterdatei beim Programmstart laden: Ist die Option aktiviert, wird standardmäßig beim Neustart von Password Depot-Client die zuletzt verwendete Datenbank geladen.
- Änderungen der Zwischenablage vor externen Viewern verbergen

TIPP: Falls Sie Fragen zu den einzelnen Programmoptionen der Client-Sicherheitsrichtlinien oder anderen Konfigurationen haben, schreiben Sie uns eine E-Mail an info@acebit.de und wir helfen Ihnen gerne weiter!

HINWEIS: Die Einstellungen der Client-Sicherheitsrichtlinien werden immer auf den gesamten Server und alle Benutzer angewendet. Das heißt, alle Einstellungen, die Sie hier definieren, können Sie nachträglich auf Datenbank-Ebene für einzelne Benutzer oder Gruppen nicht mehr ändern oder anders definieren. Über die Schaltfläche Einstellungen wiederherstellen können Sie die vorgenommenen Einstellungen wieder zurücksetzen, sodass Sie hier anschließend wieder zu den Standardeinstellungen gelangen.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Serverspiegelung

Die Serverspiegelung erreichen Sie über das Menü Verwalten.

In der Netzwerkverwaltung wird die Serverspiegelung eingesetzt, um ein Replikat eines Servers auf einer anderen Maschine zu erstellen. Dieses Replikat wird in Echtzeit erstellt und aktualisiert. Mit der Funktion der Serverspiegelung in Password Depot Enterprise Server können Administratoren den gesamten Inhalt ihres Servers auf einem Remote- oder auch internen Server spiegeln/duplizieren. Somit können Sie Ihre Daten jederzeit wiederherstellen, sollte der Haupt-Server einmal ausfallen. Anhand der Serverspiegelung in Password Depot Enterprise Server können Sie Ihre Daten, die auf dem primären Server gespeichert sind, mit einem Backup-Server synchronisieren und dadurch zusätzlich sichern.

In Password Depot Enterprise Server ist die Serverspiegelung wie folgt umgesetzt:

Wenn Sie zwei Maschinen haben, auf denen Password Depot Enterprise Server derzeit installiert ist und läuft, dann können Sie eine Serverspiegelung einrichten. Einer der beiden Server ist dabei der primäre oder Haupt-Server (Prinzipal), der wie gewohnt läuft, das heißt, Benutzer verbinden sich mit diesem Server um gemeinsam genutzte Datenbanken zu empfangen und öffnen. Die andere Maschine wird dann als gespiegelter Server genutzt. Benutzer können dabei zwar auch eine Verbindung zum gespiegelten Server herstellen, diesen aber ausschließlich im Lese-Modus nutzen. Der Haupt-Server aktualisiert und synchronisiert dann Ihre Daten im Hintergrund auf den gespiegelten Server in Echtzeit. Sollte der Haupt-Server einmal ausfallen, können Administratoren so den gespiegelten Server aktivieren und diesen dadurch als neuen Haupt-Server einstellen, sodass Benutzer weiterhin Zugriff auf die Daten in Password Depot Enterprise Server-Datenbanken haben und dadurch Ihre Arbeit fortsetzen können.

Um die Serverspiegelung im Server-Manager einzurichten, gehen Sie bitte wie folgt vor:

Serverrolle

Wählen Sie eine Serverrolle aus.

- Keine Spiegelung, wenn Sie für Ihre aktuelle Enterprise Server-Installation grundsätzlich keine Spiegelung wünschen
- Prinzipal, wenn der Server, mit dem Sie gerade verbunden sind, der Haupt- oder primäre Server sein soll
- Spiegel, wenn der Server, mit dem Sie gerade verbunden sind, der gespiegelte Server sein soll

Server-Netzwerkadressen

Hier können Sie jeweils die Netzwerk-Adresse des primären bzw. gespiegelten Servers sowie den entsprechenden Port zur Verbindung eingeben.

Status

In diesem Feld können Sie immer den aktuellen Status der eingerichteten Serverspiegelung einsehen, beispielsweise wird hier angezeigt, ob der Prozess der Spiegelung erfolgreich durchgeführt werden konnte oder währenddessen ein Fehler aufgetreten ist. Sollte Letzteres der Fall sein, wird Ihnen im Status-Feld eine Fehlermeldung angezeigt. Darüber hinaus können Sie diesem Feld auch zusätzliche, allgemeine Informationen über die aktuelle Serverspiegelung in Ihrem Password Depot Enterprise Server entnehmen.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Programmoptionen

Die Programmoptionen können Sie unter dem Menüpunkt Verwalten aufrufen. Sie beziehen sich ausschließlich auf den Server-Manager. Folgendes können Sie über die Programmoptionen festlegen:

- **Sprache der Anwendung:** Bestimmen Sie, in welcher Sprache die Benutzeroberfläche des Server-Managers angezeigt werden soll. Sie können hier zwischen Englisch und Deutsch wählen.

- SSL/TLS-Optionen: Legen Sie fest, ob Sie zur Anmeldung am Server-Manager eine SSL/TLS-Verbindung verwenden möchten. Bitte beachten Sie, dass dies nur möglich ist, wenn im Server-Manager allgemein die Verwendung eines SSL-Zertifikats aktiviert wurde. Sind alle Einstellungen korrekt gesetzt, so ist im Anmeldefenster des Server-Managers standardmäßig die Option SSL/TLS verwenden angehakt und bei jeder Anmeldung wird das entsprechende Zertifikat im Hintergrund geprüft.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Extras

Der Menüpunkt Extras beinhaltet zusätzliche Optionen der Server-Konfiguration, und zwar wie folgt:

- Systemprotokoll
- Active Directory-Synchronisation
- Azure AD-Synchronisation
- Datenbanken-Bericht
- Benutzerbericht

Der Menüpunkt ist daher einerseits von Relevanz, wenn Sie Active Directory- oder Azure AD-Benutzer dem Enterprise Server hinzufügen möchten, damit sich diese entweder über ihre Windows NT- oder Azure AD-Zugangsdaten auch am Enterprise Server zum Öffnen von Server-Datenbanken anmelden können. Hierzu ist vorab, damit diese Funktionen überhaupt genutzt werden können, jeweils eine entsprechende Synchronisation der Benutzer über den integrierten Synchronisationsassistenten notwendig.

Über die Schaltfläche Systemprotokoll können Sie sich ein solches generieren lassen, um über die Windows-Ereignisanzeige ein detailliertes Protokoll angezeigt zu bekommen. Treten am Enterprise Server beispielsweise Fehler auf, so können Sie diese über das Systemprotokoll gezielt einsehen und untersuchen.

Über die Berichte können Sie sich sowohl Datenbanken- als auch Benutzerberichte erzeugen lassen, um eine bessere Übersicht über Ihre Datenbanken und Benutzer auf dem Server zu erhalten.

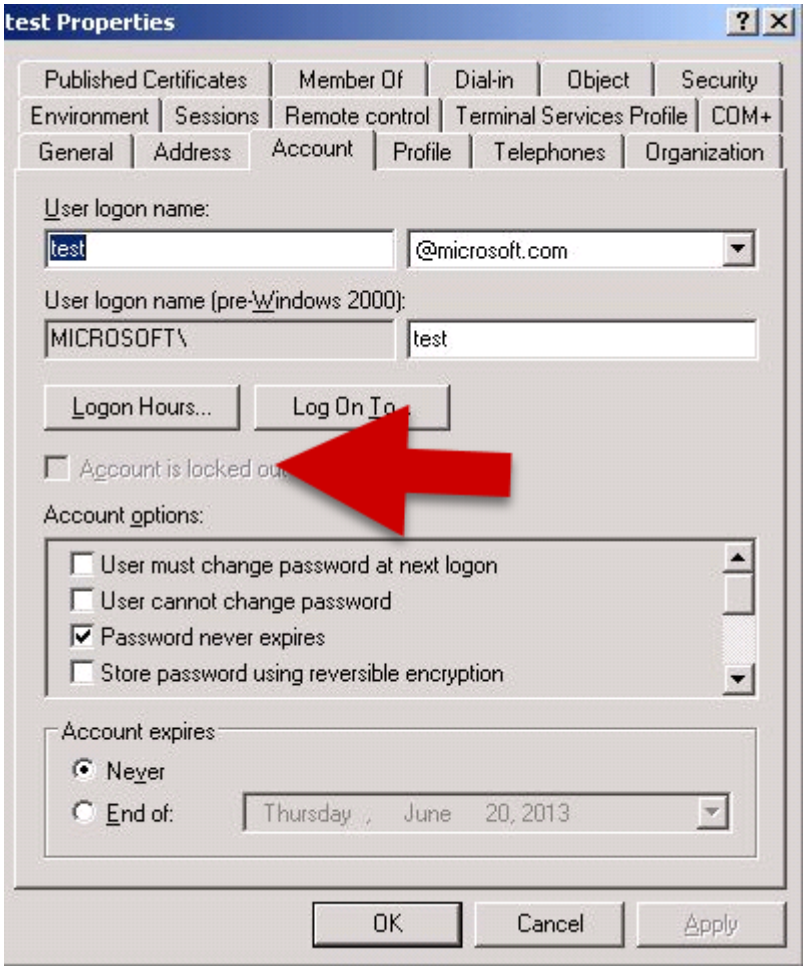
Die Active Directory- sowie Azure AD-Synchronisation sowie das Erstellen und Nutzen der jeweiligen Berichte wird in den nachfolgenden Kapiteln näher und detailliert erläutert.

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.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Active Directory-Synchronisation

Im Menü Extras finden Sie die Option **Active Directory-Synchronisation**, über die Sie den gleichnamigen Assistenten starten können. Die Active Directory-Synchronisation ist erforderlich, wenn Sie möchten, dass sich Ihre Benutzer per Single Sign-On (SSO) am Enterprise Server anmelden sollen. In diesem Fall verwendet ein Benutzer für den Login dann seine Windows NT-Zugangsdaten. Zuvor ist allerdings die korrekte Active Directory-Synchronisation zwingend erforderlich.

HINWEIS: 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 Domäne machen, aus der Sie die Benutzer/Gruppen importieren möchten:

LDAP-Pfad

Sofern die Domäne noch nicht in der Liste enthalten ist, geben Sie hier ihren Namen ein.

Anmelden

- Anmelden als aktueller Benutzer: Wählen Sie diese Option, wenn Sie sich mit dem aktuellen Benutzer anmelden möchten, um die Active Directory-Synchronisation durchzuführen. Der aktuelle Benutzer ist dabei der, mit dem Sie sich zuvor an Windows angemeldet haben.
- Dieses Konto verwenden: Geben Sie hier den Benutzernamen und das Kennwort eines anderen Benutzers ein, der ebenfalls die Berechtigung besitzt, Daten aus Active Directory Ihrer bzw. der zuvor gewählten Domäne auszulesen. Normalerweise ist dies der Domänen-Administrator. Bitte denken Sie daran, dass der Password Depot Server standardmäßig das SYSTEM-Konto des Rechners verwendet, auf dem der Server installiert ist und läuft. Stellen Sie daher bitte sicher, dass das Konto, das zur AD-Synchronisation verwendet wird (insbesondere dann, wenn es nicht das aktuelle Benutzerkonto ist), vollen Lesezugriff auf AD Ihrer Domäne hat, da ansonsten die Synchronisation nicht korrekt erfolgen kann.

Zusätzliche Optionen

- Explorer-Modus: Mit diesem Modus können Sie die vorhandenen Ordner im Active Directory durchsuchen. Im Anschluss wird Ihnen in einem neuen Dialogfenster die Active Directory-Struktur angezeigt, aus der Sie dann die entsprechenden Benutzer/Gruppen zur Synchronisation auswählen können.
- Suchen-Modus: Mit diesem Modus können Sie in Active Directory nach Benutzern und Gruppen suchen.
- Alle Container rekursiv scannen: Hierbei liest/scannt der Assistent das gesamte Active Directory-Verzeichnis. Dies kann in manchen Fällen sehr viel Zeit in Anspruch nehmen. Die Option sollte daher nur beim allerersten Mal nach dem Import von Daten aus älteren Versionen des Password Depot Enterprise Servers verwendet werden, um alle WinNT-Pfade zuverlässig durch LDAP-Pfade zu ersetzen. Ist die Option nicht aktiviert, arbeitet der Assistent wie ein normaler Active Directory-Explorer, das heißt, er öffnet nur das angegebene Objekt und scannt im Anschluss den Container, sofern Sie diesen erweitern.
- Gelöschte Objekte überprüfen: Mit dieser Option werden gelöschte Objekte (zum Beispiel Benutzer oder Gruppen) in Active Directory und Password Depot Enterprise Server überprüft bzw. miteinander abgeglichen.
- SSL verwenden: Diese Option sollten Sie anhaken, sofern Sie in Active Directory mit SSL arbeiten.

Klicken Sie auf Anmelden, sobald Sie alle notwendigen Einstellungen gesetzt haben. Wenn Die Anmeldung erfolgreich war, sehen Sie im nächsten Fenster den passenden 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. Wählen Sie die gewünschten Benutzer und/oder Gruppen aus, indem Sie die entsprechenden Kontrollkästchen markieren. Klicken Sie abschließend auf Synchronisieren und es werden Ihnen im nächsten Fenster die Ergebnisse der Synchronisation angezeigt.

HINWEIS: Grundsätzlich ist es so, dass Password Depot Server im Allgemeinen nicht mit OUs arbeiten kann. Diese werden zwar im Synchronisations-Assistenten der Einfachheit halber angezeigt, es werden prinzipiell aber nur AD-Objekte wie "Benutzer" oder "Gruppen" mit dem Server synchronisiert.

TIPP: Sie können Benutzer und Gruppen nun auch einzeln mit Active Directory synchronisieren. Wählen Sie hierzu den entsprechenden Benutzer oder die entsprechende Gruppe aus und klicken Sie im Anschluss im Server-Manager rechts auf Synchronisieren.

HINWEIS: Welche Einstellungen für die Anmeldung am Enterprise Server per Integrierter Windows-Authentifizierung (SSO) sowohl im Server-Manager als auch im Client notwendig sind, erfahren Sie hier: Anmeldung des Clients am Server per Single Sign-On (SSO). Bitte beachten Sie zudem, dass der PC, von dem die Anmeldung stattfinden soll, Mitglied im AD sein muss, ansonsten kann die Anmeldung nicht erfolgen. Ein Computer muss im AD sein, damit die

Authentifizierung überhaupt stattfinden kann. Wenn Sie nämlich AD-Benutzer mit dem Enterprise Server synchronisieren, dann "kennt" Password Depot die Kennwörter der Benutzer nicht und speichert diese auch nicht auf dem Server ab, sondern bei Authentifizierung wird das vom Benutzer eingegebene Kennwort an AD gesendet und Password Depot erhält ein richtig oder falsch zurück. Deshalb ist es erforderlich, dass der Computer im AD angemeldet ist.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Azure AD-Synchronisation

Neben der klassischen Active Directory-Synchronisation können Sie im Server-Manager auch die Azure AD-Synchronisation durchführen. Um hierfür den entsprechenden Assistenten zu starten, gehen Sie ebenfalls auf Extras und wählen hier dann die **Azure AD-Synchronisation** aus. Die Azure AD-Synchronisation ist erforderlich, wenn Sie möchten, dass sich Ihre Benutzer mit ihren Microsoft-Zugangsdaten am Enterprise Server anmelden können sollen. Wie schon bei der Anmeldung per Integrierter Windows-Authentifizierung (SSO) ist es auch bei der Verbindung per Azure AD notwendig, zuvor eine korrekte Synchronisation durchzuführen, denn nur so können Azure AD-Benutzer dem Server hinzugefügt werden (dies ist nicht! manuell möglich).

Um die Azure AD-Synchronisation starten zu können, müssen Sie im Synchronisationsassistenten bestimmte Angaben machen:

Organisation

Auf der Startseite des Assistenten müssen Sie zunächst eine Organisation auswählen, aus der die Azure AD-Benutzer importiert werden sollen. Sofern Sie im Drop-Down-Menü noch keine Organisation sehen können, klicken Sie rechts daneben auf Neu... Im Anschluss müssen Sie einen Microsoft-Account auswählen, der als Organisation hinterlegt werden soll.

HINWEIS: Bitte beachten Sie, dass für die Anmeldung einer Organisation nur das Benutzerkonto des Administrators verwendet werden kann!

Nach Eingabe des Admin-Benutzernamens sowie -Kennworts werden Sie als Administrator zunächst noch aufgefordert, den zweiten Faktor aus Ihrer Authenticator-App einzugeben. Die 2-Faktor-Authentifizierung ist an dieser Stelle notwendig und kann nicht umgangen werden, da sie Teil der Microsoft-Sicherheitsrichtlinien ist. Nach erfolgreicher Anmeldung werden Ihnen im Synchronisationsassistenten die Azure AD-Benutzer/-Gruppen angezeigt, die zur Synchronisation zur Verfügung stehen. Klicken Sie die einzelnen Objekte an, die Sie importieren möchten. Danach klicken Sie auf Synchronisieren. Im nächsten Fenster werden Ihnen die Ergebnisse angezeigt. Wenn hier alle gewünschten Benutzer/Gruppen angezeigt werden, können Sie den Synchronisationsassistenten schließen.

Zusätzliche Optionen

Gelöschte Objekte überprüfen: Mit dieser Option werden gelöschte Objekte (zum Beispiel Benutzer oder Gruppen) in Azure AD und Password Depot Enterprise Server überprüft bzw. miteinander abgeglichen.

TIPP: Sobald ein Benutzer per Azure AD-Synchronisation dem Server-Manager hinzugefügt wurde, können Sie in den Eigenschaften des Benutzers in der Registerkarte Konto sehen, dass als Authentifizierung automatisch die Option Azure Active Directory angehakt wurde. Zudem können Sie weitere Azure AD-Attribute eines Benutzers, der während der Synchronisation automatisch hinzugefügt wurde, in der Registerkarte Azure AD einsehen.

Wie sich Azure AD-Benutzer anschließend über den Client am Enterprise Server anmelden können, erklären wir in unserem Handbuch zum Password Depot-Windows-Client.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Berichte

Im Menü Extras können Sie Berichte generieren. Folgende Optionen stehen Ihnen hier zur Verfügung:

- Datenbanken-Bericht
- Benutzerbericht

Anhand dieser Berichte können Sie eine Übersicht über Ihre Benutzer und Datenbanken auf dem Server erhalten. Über die Schaltfläche Generieren, können Sie sich den entsprechenden Bericht direkt erstellen und im Standardbrowser anzeigen lassen. Über Speichern unter können Sie diesen auch im *.html-Format abspeichern, wenn Sie ihn erst später oder zukünftig benötigen. Im Folgenden wird kurz erläutert, wie die einzelnen Berichte zu verstehen sind.

Datenbanken-Bericht

Unter Datenbanken-Bericht können Sie Berichte über eine oder mehrere Datenbanken des Password Depot Enterprise Servers erstellen. Sie erhalten dabei eine Übersicht, welche Benutzer Zugriff auf welche Datenbanken haben und welche Berechtigungen sie hierfür besitzen. Die erlaubten Rechte sind in der jeweiligen Spalte mit einem "✓" markiert, während die verweigerten Rechte mit einem "-" dargestellt werden. Der Datenbanken-Bericht zeigt immer ausschließlich die Berechtigungen eines Benutzers auf Datenbank-Ebene.

Benutzerbericht

Unter Benutzerbericht wird ein Bericht erstellt, der die Benutzerkonten von Password Depot Enterprise Server auflistet. Es werden Ihnen hier also alle auf dem Server verfügbaren Benutzer und in dem Zusammenhang zusätzlich noch folgende Übersicht angezeigt:

- Konto: Zeigt das entsprechende Benutzerkonto bzw. den Namen eines Benutzers an.
- Typ: Zeigt an, ob der Benutzer ein "normaler" Server-Benutzer ist oder zusätzlich eine Serverrolle besitzt (zum Beispiel die des Datenbankadministrators).
- Vollständiger Name: Zeigt den vollständigen Namen des Benutzers an, der ihm unter Eigenschaften -> Allgemein zugeordnet ist.
- E-Mail: Zeigt, ob für diesen Benutzer eine E-Mail-Adresse hinterlegt ist.
- Deaktiviert: Zeigt, ob das entsprechende Benutzerkonto aktuell deaktiviert ist. In diesem Fall kann sich der entsprechende Benutzer nicht mehr am Enterprise Server anmelden. Öffnen Sie die Eigenschaften des Benutzers und gehen Sie zur Registerkarte Konto, um das Konto wieder zu aktivieren.

- Zugeordnete Datenbanken: Zeigt an, auf welche Server-Datenbanken ein Benutzer Zugriff hat.
- Zugriffsrechte: Zeigt pro Datenbank die entsprechenden Zugriffsrechte eines Benutzers an.

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 sowie bestehende löschen oder verwalten. Darüber hinaus weisen Sie hier den vorhandenen Benutzern oder Gruppen die Rechte auf einzelne Datenbanken zu.

In der Listenansicht des Bereichs Datenbanken erhalten Sie einen Überblick über alle vorhandenen Server-Datenbanken, deren Größe, über das letzte Änderungsdatum und der Gesamtanzahl der Datenbankeinträge. Darüber hinaus können Sie unter Verbindungen sehen, wie viele Benutzer aktuell mit einer Datenbank verbunden sind. Wenn Sie mit sehr vielen einzelnen Datenbanken arbeiten, können Sie im oberen Bereich der Hauptansicht einen Filter verwenden, um die Anzeige einzugrenzen. Geben Sie dazu beispielsweise den Datenbanknamen oder einen Teil davon ein.

Auf der rechten Seite der Hauptansicht stehen Ihnen zudem die folgenden Optionen zur Verfügung:

- Neue Datenbank: Mit dieser Schaltfläche können Sie eine neue Datenbank erstellen. Es öffnet sich im Anschluss das Dialogfenster **Datenbank dem Server hinzufügen**.
- Berechtigungen: Hierüber nehmen Sie die Rechteverwaltung vor. Durch einfachen Klick auf die gleichnamige Schaltfläche sehen Sie zunächst alle Benutzer/Gruppen, 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, doppelklicken Sie auf einen Benutzer oder eine Gruppe. Es öffnet sich ein neues Fenster, in dem Sie die Berechtigungen einstellen können. Alternativ können Sie auch einen Benutzer/eine Gruppe aus der Liste anklicken und anschließend rechts auf Eigenschaften gehen.
- 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. Weitere Informationen zu den Eigenschaften einer Datenbank erhalten Sie hier.
- Löschen: Mit dieser Schaltfläche können Sie vorhandene Datenbanken vom Server löschen. Falls die Datenbank zu diesem Zeitpunkt von einem Benutzer verwendet wird, erhält dieser beim nächsten Speichern einen Hinweis darüber. Gelöschte Datenbanken werden auch aus dem entsprechenden Arbeitsverzeichnis des Servers gelöscht.
- Umbenennen: Benennen Sie eine markierte Datenbank um.
- Alle auswählen: Markiert alle vorhandenen Server-Datenbanken, um anschließend weitere Aktionen auszuführen, die sich dann auf alle Datenbanken beziehen.

TIPP: Obige Funktionen können Sie auch durch einen Rechtsklick auf eine Datenbank aus der Liste aufrufen. Zudem können Sie die Anzeige der Hauptansicht auch filtern, um

beispielsweise nach einer bestimmten Datenbank zu suchen. Geben Sie dazu einen Datenbanknamen oder einen Teil davon ein, um die Suche zu starten.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Datenbank dem Server hinzufügen

Dieses Dialogfenster erreichen Sie, indem Sie im Bereich Datenbanken auf Neue Datenbank klicken. Sie können hierüber also dem Server neue Datenbanken hinzufügen. Folgende Registerkarten stehen Ihnen hier zur Verfügung:

- Vorhandene Datenbank hinzufügen
- Neue Datenbank erzeugen

Vorhandene Datenbank hinzufügen

Wählen Sie diese Registerkarte, um eine bereits vorhandene Datenbank dem Server hinzuzufügen. Dabei kann es sich beispielsweise um Datenbanken handeln, die bereits auf dem lokalen System eines Benutzers existieren, etc.

- Klicken Sie auf die Schaltfläche Durchsuchen, um die entsprechende Datenbank auszuwählen.
- Im Feld Master-Kennwort geben Sie das aktuelle Master-Kennwort dieser Datenbank ein. Standardmäßig wird dieses verdeckt angezeigt. Klicken Sie auf das Augen-Symbol im gleichen Feld, um das Master-Kennwort im Klartext anzeigen zu lassen.
- Klicken Sie abschließend auf OK, um den Vorgang abzuschließen.

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

Neue Datenbank erzeugen

Wählen Sie diese Registerkarte, um eine neue und leere Datenbank direkt auf dem Password Depot Server zu erzeugen. Geben Sie unter Dateiname den gewünschten Datenbanknamen und, falls erwünscht, zusätzliche Anmerkungen im Feld darunter ein.

HINWEIS: Das Master-Kennwort von Server-Datenbanken entspricht immer dem Administrator-Kennwort (Super-Administrator). Die Clients verwenden zum Öffnen der Server-Datenbanken jedoch immer ihre vom Administrator zugewiesenen Zugangsdaten (je nach eingestellter Methode der Authentifizierung).

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 bereits 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.

Über die Schaltfläche Löschen können Sie Benutzern und Gruppen den Zugriff auf die ausgewählte Datenbank wieder entziehen. Der Benutzer oder die Gruppe können dann nicht mehr auf diese Datenbank zugreifen, auf dem Server sind Sie dennoch verfügbar. Über Alle auswählen, können Sie alle Benutzer/Gruppen, die auf die ausgewählte Datenbank zugreifen können, gleichzeitig markieren, um anschließend weitere Aktionen auszuführen, die sich dann auf alle markierten Benutzer/Gruppen beziehen.

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. Klicken Sie abschließend auf OK, um den Vorgang abzuschließen.

Doppelklicken Sie im Anschluss in der Hauptansicht auf den zuvor neu hinzugefügten Benutzer oder die Gruppe, um die Rechte zu setzen. Alternativ können Sie auch den Benutzer/die Gruppe aus der Liste auswählen und rechts auf Eigenschaften gehen. Es öffnet sich ein neues Fenster, über das Sie die detaillierte Rechteverwaltung auf dem Enterprise Server vornehmen können. Es stehen Ihnen hier drei Registerkarten zur Verfügung:

- Datenbank
- Einträge und Ordner
- Versiegelter Zugang

In der Registerkarte Datenbank setzen Sie die Berechtigungen für die gesamte Datenbank. Weitere Berechtigungen für einzelne 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

Datenbank

In der Registerkarte Datenbank werden Rechte für die gesamte Datenbank vergeben. 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 Optionen Gültig ab / 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.

HINWEIS: Alle Rechte, die Sie hier erlauben, gelten global für die gesamte Datenbank. Wenn Sie Benutzern/Gruppen hier auf Datenbank-Ebene also das Lesen / Ändern / Hinzufügen / Löschen von Einträgen erlauben, dann können sie alle Einträge innerhalb der gesamten Datenbank standardmäßig sehen und verwalten. Wenn Sie Benutzern/Gruppen innerhalb der Datenbank nur Zugriff auf einzelne Ordner und/oder Einträge gewähren möchten, dann sollten Sie die Rechte Lesen / Ändern / Hinzufügen / Löschen auf Datenbank-Ebene nicht gewähren

und das Häkchen entsprechend rausnehmen, nicht jedoch verweigern! Wie Sie sicherstellen können, dass unbefugte Benutzer keine Einträge lesen können, erläutern wir genauer im Kapitel Rechte für Benutzer.

Einträge und Ordner

In dieser Registerkarte können Sie Benutzern/Gruppen Rechte auf einzelne Ordner und/oder Einträge innerhalb der Datenbank zuweisen. Auf diese Weise ist es möglich, die Zugriffe verschiedener Benutzer/Gruppen innerhalb der gleichen Datenbank so zu gestalten, dass jeder nur tatsächlich das sehen kann, was er auch sehen können darf bzw. soll.

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.

HINWEIS: In den beiden Registerkarten Datenbank und Einträge und Ordner können Sie verschiedene Formatierungen sehen, die die Rechtevergabe erleichtern sollen. Standardmäßig sind 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, beispielsweise während einer Urlaubsvertretung.

Benutzer können anderen Benutzern 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 Eintrag teilen möchte, 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 autorisierte Benutzer mit seinen Zugangsdaten am Server-Manager 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 auch tatsächlich 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 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. 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.

TIPP: Besuchen Sie gerne auch unsere Knowledge Base, um weitere Informationen zu dieser Funktion zu erhalten: Wie kann ich anderen Benutzern in Password Depot Zugriff gewähren und Einträge versiegeln?

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Eigenschaften einer Datenbank

In diesem Dialogfenster werden Ihnen allgemeine Informationen zur ausgewählten Datenbank angezeigt. Sie erreichen es über den Bereich Datenbanken durch einfaches Klicken auf die gewünschte Datenbank und der Schaltfläche Eigenschaften.

Allgemein

In der Registerkarte Allgemein sehen Sie grundlegende Informationen zur ausgewählten Datenbank, z.B. die Benutzer, die die Datenbank derzeit geöffnet haben, sowie die Größe und den Dateityp etc. Über die Schaltfläche Aktualisieren können Sie die derzeitige Ansicht aktualisieren.

Erweitert

In der Registerkarte Erweitert können Sie optional einstellen, ob Sie alle Zugriffe von Benutzern auf Einträge in Server-Datenbanken überwachen und protokollieren möchten und ob Benutzer für das Löschen eines Eintrages zwingend Gründe angeben müssen. Wenn Sie alle Zugriffe Ihrer Benutzer überwachen und protokollieren möchten, dann verschwindet im Client im Detail-Bereich auf der rechten Seite das Augen-Symbol zum Anzeigen eines Kennworts im Klartext. Hintergrund: Nur so können Sie als Server-Administrator sicherstellen, auch wirklich alle Zugriffe genauestens überwachen zu können. Weitere Informationen zu dieser Option stehen Ihnen auch in unserer Knowledge Base zur Verfügung:

Wo finde ich das "Augen"-Symbol zur Anzeige des Kennworts im Klartext?

HINWEIS: Die Eigenschaften **einer** Datenbank sind eher informativer Natur; die eigentlichen Zugriffsrechte werden in den Berechtigungen definiert.

Sicherheit

Datenbank am Server verschlüsseln mit

Hier können Sie Ihre Datenbanken auf dem Server mit einem zusätzlichen Kennwort verschlüsseln. Grundsätzlich werden alle Datenbanken auf dem Server mit dem Kennwort des Super-Administrators standardmäßig verschlüsselt. Das bedeutet, sobald der Super-Administrator Zugriff zum Server-Manager hat, kann er automatisch auch die vorhandenen Server-Datenbanken verwalten.

Es kann allerdings durchaus vorkommen, dass der Super-Administrator oder ein anderer Server-Administrator nicht grundsätzlich Zugriff auf alle am Server verfügbaren Datenbanken haben und diese verwalten können soll. Für einen solchen Fall ist eine detailliertere Konfiguration notwendig und

erfordert dann die Nutzung eines zusätzlichen Kennworts. Über die Schaltfläche Einstellungen ändern können Sie den Vorgang starten:

Es öffnet sich das Dialogfenster Datenbankverschlüsselung ändern. Wählen Sie unter Datenbank am Server verschlüsseln die Option Benutzerdefiniertes Kennwort (Berechtigungsverwaltung erfordert Verifizierung) aus. Im Anschluss werden Sie aufgefordert ein neues Kennwort einzugeben und dieses im Feld darunter zu wiederholen. Klicken Sie abschließend auf OK, um den Vorgang abzuschließen.

Nachdem die ausgewählte Datenbank erfolgreich verschlüsselt und abgespeichert wurde, kann im weiteren Verlauf ein Zugriff auf die Eigenschaften/Berechtigungen der Datenbank und damit Ihre Verwaltung nur erfolgen, wenn das benutzerdefinierte Kennwort korrekt eingegeben wird. Darüber hinaus wird es anderen Benutzern, die ebenfalls über den Server-Manager Zugriff auf diese Datenbank haben, nur möglich sein, deren Eigenschaften zu öffnen, sofern Sie das korrekte zusätzliche Kennwort eingeben.

Wenn Sie das benutzerdefinierte Kennwort im Nachhinein ändern möchten, geben Sie zunächst das aktuelle benutzerdefinierte Kennwort ein, um zu den Datenbank-Eigenschaften zu gelangen. Gehen Sie im Anschluss ebenfalls auf Einstellungen ändern und geben Sie zunächst das bisherige und im Anschluss das neue Kennwort ein. Über die Schaltfläche OK können Sie das neue Kennwort speichern. Wenn Sie das zusätzliche Kennwort entfernen möchten, wählen Sie im Fenster Datenbankverschlüsselung ändern die Option Administrator-Kennwort (Automatischer Zugriff auf die Berechtigungsverwaltung) aus und geben danach noch das aktuell verwendete benutzerdefinierte Kennwort im entsprechenden Feld ein. Klicken Sie danach auf OK. Das Kennwort zur Verschlüsselung wird dann wieder in das Kennwort des Super-Administrators geändert, sodass fortan zum Verwalten der Berechtigungen und Eigenschaften der Datenbank kein weiteres Kennwort mehr eingegeben werden muss.

WARNUNG: Diese Funktion sollte mit äußerster Vorsicht genutzt werden! Bitte nutzen Sie sie daher nur, wenn es zwingend erforderlich ist, denn es besteht nicht die Möglichkeit, ein solches benutzerdefiniertes zusätzliches Kennwort für Datenbanken zurückzusetzen oder wiederherzustellen, sollte es vergessen werden. Daher ist es bei Verlust dieses Passworts im Anschluss nicht mehr möglich, die Eigenschaften und Berechtigungen der betroffenen Datenbank zu öffnen und diese somit zu verwalten. Bewahren Sie daher dieses zusätzliche Kennwort sorgfältig auf und verwenden Sie die Funktion nur, sofern erforderlich.

HINWEIS: Weitere Informationen zu dieser Funktion erhalten Sie über unsere Knowledge Base und folgenden Artikel: Datenbanken auf dem Password Depot Server vor unberechtigtem Zugriff durch den Administrator schützen.

Benutzer

Der Bereich Benutzer ermöglicht dem Administrator, neue Benutzer hinzuzufügen und bestehende zu verwalten. Die Zugriffsrechte der Benutzer werden jedoch im Bereich Datenbanken -> Berechtigungen zugewiesen.

In der Hauptansicht werden Ihnen zu einem Benutzer folgende Spalten angezeigt:

- Konto: Zeigt das entsprechende Benutzerkonto an.
- Authentifizierung: Gibt an, welche Art der Anmeldung am Enterprise Server ein Benutzer verwendet (Password Depot-Authentifizierung oder Integrierte Windows-Authentifizierung).
- Benutzerprinzipalname: Zeigt den Benutzerprinzipalnamen eines Benutzers an, sofern dieser dem Server-Manager per Azure AD-Synchronisation hinzugefügt wurde.
- Status: Zeigt, ob das entsprechende Benutzerkonto aktiviert oder deaktiviert und ob der Benutzer aktuell mit dem Server verbunden ist.
- Rollen: Zeigt, ob der ausgewählte Benutzer eine zusätzliche Rolle am Server besitzt. Mehr zu den Rollen am Server erfahren Sie hier.
- Adresse: Gibt die IP-Adresse des jeweiligen Benutzers an, sofern dieser aktuell mit dem Server verbunden ist.
- Vollständiger Name: Gibt den vollständigen Namen eines Benutzers an, so wie dieser im Server-Manager hinterlegt wurde (siehe auch die Eigenschaften eines Benutzers).
- E-Mail: Zeigt die E-Mail-Adresse eines Benutzers an, sofern diese im Server-Manager hinterlegt wurde.
- Abteilung: Zeigt die Abteilung eines Benutzers an, sofern diese im Server-Manager hinterlegt wurde.
- Geöffnete Datenbank: Gibt an, welche Datenbank ein Benutzer gerade geöffnet hat, sofern er aktiv mit dem Server verbunden ist.

Auf der rechten Seite der Hauptansicht stehen Ihnen zudem die folgenden Optionen zur Verfügung:

- Neuer Benutzer: Über diese Schaltfläche können Sie dem Server neue, lokale Benutzer hinzufügen. Es öffnet sich im Anschluss das Dialogfenster Benutzer hinzufügen. Hier können Sie für neue Benutzer den entsprechenden Benutzernamen und das Kennwort einstellen (Anmelde-Option Password Depot-Zugangsdaten).
- Eigenschaften: Öffnet die Eigenschaften eines Benutzers.
- Löschen: Löscht einen markierten Benutzer aus dem Server-Manager.
- Trennen: Trennt die Verbindung der ausgewählten Benutzer zum Password Depot Enterprise Server.
- Synchronisieren: Mit dieser Option können Sie den markierten/ausgewählten Benutzer einzeln über AD bzw. Azure AD synchronisieren, ohne dabei den Active Directory- bzw. Azure AD-Synchronisationsassistenten erneut aufrufen und den Benutzer hieraus importieren zu müssen. Bitte beachten Sie jedoch, dass der jeweilige Benutzer zuvor bereits per AD-/Azure 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-/Azure AD-Daten geändert haben. Hierfür muss dann nicht erneut eine komplette AD-/Azure AD-Synchronisation erfolgen.

- Datenbank zuweisen: Ermöglicht dem Administrator, einzelne Datenbanken einem oder mehreren Benutzern gleichzeitig zuzuweisen bzw. auch, neue Datenbanken zu erzeugen und diese direkt den markierten Benutzern zuzuordnen. Über die Registerkarte Rechte kann der Administrator für die Benutzer gleich die entsprechenden Rechte auf Datenbank-Ebene definieren. Außerdem können hier für Benutzer private Datenbanken erzeugt werden, die ebenfalls auf dem Enterprise Server abgespeichert sind. Mehr zu den privaten Datenbanken erfahren Sie im Kapitel Datenbank zuweisen.
- 2FA zurücksetzen: Ermöglicht dem Administrator bei Nutzung der Zwei-Faktor-Authentifizierung (2FA) am Server, für einen oder gleich mehrere Benutzer die Optionen der 2FA zurückzusetzen, um den gesamten Vorgang hier von Neuem zu starten. Die ausgewählten Benutzer müssen dann beim nächsten Anmelden am Server erneut den QR-Code scannen und den übermittelten Zahlencode eingeben.
- Alle auswählen: Markiert alle am Server verfügbaren Benutzer, um anschließend weitere Aktionen auszuführen, die sich dann auf alle Benutzer beziehen.

TIPP: Diese Funktionen können Sie auch durch einen Rechtsklick auf einen Benutzer aus der Liste aufrufen. Zudem können Sie die Anzeige der Hauptansicht auch filtern, um beispielsweise nach einem bestimmten Benutzer zu suchen. Geben Sie dazu einen Benutzernamen oder einen Teil davon ein, um die Suche zu starten.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Benutzer hinzufügen

In Password Depot Enterprise Server gibt es drei Möglichkeiten, über die Sie dem Server-Manager Benutzer hinzufügen können:

1. Über die Schaltfläche Neuer Benutzer
2. Per Active Directory-Synchronisation
3. Per Azure AD-Synchronisation

Neue Benutzer manuell anlegen

Über die Schaltfläche Neuer Benutzer, die Ihnen im Bereich Benutzer auf der rechten Seite zur Verfügung steht, können Sie dem Server-Manager neue, lokale Benutzer manuell hinzufügen. Solche Benutzer melden sich dann über die Password Depot-Authentifizierung am Enterprise Server an. Wählen Sie hierfür in der Registerkarte Konto die Anmeldeoption Password Depot-Authentifizierung verwenden aus und erstellen Sie für den Benutzer einen Benutzernamen und Kennwort. Klicken Sie abschließend auf OK, um den Vorgang zu beenden. Der neu hinzugefügte Benutzer wird im Anschluss in der Hauptansicht angezeigt und Sie können nun beginnen, ihm Zugriff auf Datenbanken zu gewähren und innerhalb dieser die passenden Rechte zu vergeben.

Lokal angelegte Benutzer wählen dann im Datenbank-Manager des Client für die Anmeldung am Enterprise Server die Option Melden Sie sich mit Benutzername und Kennwort an aus. Nach Eingabe der korrekten Zugangsdaten, der IP-Adresse des Servers sowie des korrekten Ports kann dann der Zugriff auf den Server erfolgen.

Neue Benutzer per Active Directory-Synchronisation hinzufügen

Wenn sich Ihre Benutzer per Integrierter Windows-Authentifizierung (SSO) am Enterprise Server anmelden können sollen, dann können Sie diese Benutzer nicht manuell am Server anlegen, sondern müssen über Extras -> Active Directory-Synchronisation eine entsprechende Synchronisation durchführen. Die Benutzerobjekte werden dann entsprechend aus Active Directory mit dem Server-Manager synchronisiert. Sofern der Vorgang erfolgreich war, können Sie im Anschluss im Bereich Benutzer alle aus Active Directory importierten Objekte sehen.

In den Eigenschaften solcher Benutzer können Sie dann in der Registerkarte Konto sehen, dass die Anmeldeoption Active Directory Domain Services bereits ausgewählt ist. In der Registerkarte

Active Directory DS können Sie zudem für Ihre Benutzer weitere Active Directory-Attribute sehen, die hier während der Synchronisation automatisch eingetragen werden.

Benutzer, die per Active Directory-Synchronisation dem Server-Manager hinzugefügt wurden, wählen im Datenbank-Manager des Client für die Anmeldung am Enterprise Server die Option Integrierte Windows-Authentifizierung aus. Bei Authentifizierung wird das vom Benutzer eingegebene Kennwort an Active Directory gesendet und Password Depot erhält ein richtig oder falsch zurück und vollzieht auf Grundlage dessen die Anmeldung oder verweigert diese bei falschen Zugangsdaten. Daher ist es wichtig, dass die im Server-Manager hinterlegten Daten den Benutzerdaten aus Active Directory entsprechen. Aus diesem Grund empfiehlt es sich, regelmäßig eine Synchronisation durchzuführen, um Änderungen in der Active Directory auch in den Server-Manager zu übernehmen.

TIPP: Mehr zur Active Directory-Synchronisation erfahren Sie im gleichnamigen Kapitel.

Neue Benutzer per Azure AD-Synchronisation hinzufügen

Auch bei dieser Form der Anmeldung müssen Sie als Administrator Ihre Benutzer per Synchronisation dem Server hinzufügen. Um die Synchronisation zu starten, gehen Sie auf Extras -> Azure AD-Synchronisation. Die Benutzerobjekte werden dann entsprechend aus Ihrem Azure-AD mit dem Server-Manager synchronisiert. Sofern der Vorgang erfolgreich war, können Sie im Anschluss im Bereich Benutzer alle aus Azure-AD importierten Objekte sehen.

In den Eigenschaften solcher Benutzer können Sie dann in der Registerkarte Konto sehen, dass die Anmeldeoption Azure Active Directory bereits ausgewählt ist. In der Registerkarte Azure AD können Sie zudem für Ihre Benutzer weitere Azure AD-Attribute sehen, die hier während der Synchronisation automatisch eingetragen werden.

Benutzer, die per Azure AD-Synchronisation dem Server-Manager hinzugefügt wurden, wählen im Datenbank-Manager des Client für die Anmeldung am Enterprise Server die Option Azure AD-Authentifizierung aus.

HINWEIS: Sie sollten in den Eigenschaften eines Benutzers in den Registerkarten Active Directory DS sowie Azure AD bewusst keine Daten eintragen, da diese über die Active Directory- oder Azure AD-Synchronisation automatisch eingefügt werden und auch nur dann sinnvoll sind. Wenn sich also die Active Directory- bzw. Azure AD-Daten eines Benutzers geändert haben, so können Sie die Änderungen nicht manuell in den Server-Manager übertragen, sondern müssen dies über die erneute Synchronisation durchführen, um somit die Daten zu aktualisieren.

TIPP: Mehr zur Azure AD-Synchronisation erfahren Sie im gleichnamigen Kapitel.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Eigenschaften eines Benutzers

Jeder am Server-Manager angelegte Benutzer hat eigene Eigenschaften. Diese können Sie aufrufen, indem Sie im Bereich Benutzer entweder auf einen Benutzer doppelklicken oder einen Benutzer auswählen und per Rechtsklick dessen Eigenschaften öffnen.

Die Eigenschaften eines Benutzers ermöglichen Ihnen, Ihre Benutzer zu verwalten. Es stehen Ihnen die folgenden Registerkarten zur Verfügung:

- Allgemein
- Konto
- Rollen
- Mitglied von
- Erweitert
- Azure AD
- Active Directory DS

Was Sie in den einzelnen Registerkarten verwalten können, wird nachfolgend näher erläutert.

Allgemein

In der Registerkarte Allgemein sind folgende Angaben möglich:

- Vollständiger Name: Geben Sie den Vor- und Nachnamen des Benutzers ein, sofern dieser vom eigentlichen Benutzernamen abweicht.
- E-Mail: Geben Sie die E-Mail-Adresse des Benutzers an.
- Telefon: Geben Sie die entsprechende Telefonnummer des Benutzers ein.
- Abteilung: Geben Sie die Abteilung des Benutzers an.
- Beschreibung: Hier können Sie, sofern nötig und erwünscht, weitere Angaben zu einem Benutzer hinterlegen.

Konto

In der Registerkarte Konto können Sie Folgendes einstellen:

Authentifizierung

Hier können Sie sehen, welche Art der Authentifizierungen am Server für Ihre Benutzer möglich ist:

- Password Depot-Zugangsdaten
- Active Directory Domain Services

und

- Azure Active Directory

Bei der Option Password-Depot-Zugangsdaten definiert der Administrator für jeden Benutzer den entsprechenden Benutzernamen und das Kennwort selbst und teilt den Benutzern die Zugangsdaten im Anschluss mit. Sofern es erlaubt ist, können Benutzer das Kennwort zur Anmeldung am Enterprise Server nachträglich noch ändern. Wie sie dabei vorgehen müssen, wird in folgendem Knowledge Base-Artikel erläutert:

Wie ändere ich das Kennwort zur Anmeldung am Enterprise Server?

Bei der Option Active Directory Domain Services handelt es sich um die Integrierte Windows-Authentifizierung (SSO) und es muss zuvor im Server-Manager eine korrekte Active Directory-Synchronisation durchgeführt werden, damit sich die Benutzer mit Ihren Windows-Anmeldedaten am Enterprise Server anmelden können. Detaillierte Informationen zur Active Directory-Synchronisation im Server-Manager erhalten Sie auch hier.

Bei der Option Azure Active Directory melden sich Ihre Benutzer mit ihren Microsoft-Zugangsdaten über den Client am Enterprise Server an. Auch hier ist es zwingend notwendig, dass zuvor im Server-Manager die korrekte Azure AD-Synchronisation durchgeführt wird, denn nur dadurch können die Azure AD-Benutzer auch dem Server-Manager und somit auch dem Enterprise Server hinzugefügt werden. Detaillierte Informationen zur Azure AD-Synchronisation im Server-Manager erhalten Sie auch hier.

Konto-Optionen

- Konto deaktiviert: Wenn hier ein Häkchen gesetzt ist, so ist der Account des betroffenen Benutzers aktuell gesperrt, 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 dadurch wieder den Zugriff auf den Server zu ermöglichen.
- Benutzer darf Kennwort nicht ändern: Setzen Sie hier ein Häkchen, wenn Sie nicht möchten, dass ein lokaler Benutzer sein Kennwort für die Anmeldung am Enterprise Server ändern können soll. Beachten Sie, dass diese Option nur Auswirkungen hat bzw. verwendet werden kann, wenn ein Benutzer die Anmeldeoption Password Depot-Zugangsdaten nutzt.

- Benutzer muss Kennwort bei der nächsten Anmeldung ändern: Setzen Sie hier ein Häkchen, wenn Sie erzwingen möchten, dass ein Benutzer sein Kennwort für die Anmeldung am Enterprise Server bei seiner nächsten Anmeldung ändern muss. Auch diese Einstellung ist nur dann von Bedeutung, wenn es sich um lokal angelegte Benutzer und nicht aus Active Directory oder Azure Active Directory synchronisierte Benutzer handelt.
- 2-Faktor-Authentifizierung deaktiviert: Setzen Sie hier ein Häkchen, wenn Sie möchten, dass für einen speziellen Benutzer die Anmeldung am Enterprise Server per Zwei-Faktor-Authentifizierung (2FA) deaktiviert sein soll. Dadurch können Sie die Anmeldung per 2FA am Server grundsätzlich für alle einstellen, im Nachgang aber für bestimmte Benutzer deaktivieren, wenn gewünscht oder erforderlich.

Rollen

Mit Version 15 wurde ein rollenbasiertes Server-Modell eingeführt, um die Verwaltung des Servers grundsätzlich auch auf mehrere verschiedene Personen aufteilen zu können. Der Zugriff auf den Server-Manager kann dadurch rollenbasiert erfolgen und obliegt auf Wunsch nicht mehr nur ausschließlich einer einzigen Person. Folgende Server-Rollen stehen Ihnen hier zur Auswahl:

- Server-Administrator: Ein Server-Administrator hat Vollzugriff auf den Enterprise Server und den Server-Manager. Über den Server-Manager kann er den Server verwalten und konfigurieren, er kann zudem neue Datenbanken und Benutzer erstellen. Die Rechte eines Server-Administrators entsprechen denen des Super-Administrators.
- 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 etc.
- Konto-Administrator: Dieser kann Benutzer und Gruppen auf dem Server verwalten und in diesem Zusammenhang beispielsweise dem Server auch neue Benutzer und Gruppen hinzufügen.
- Active Directory-Operator: Diese Server-Rolle ermöglicht Benutzern, im Server-Manager die Active Directory- oder Azure AD-Synchronisation durchzuführen. Bitte beachten Sie in diesem Zusammenhang Folgendes: Die Server-Rolle Active Directory Operator ist nur von Bedeutung, wenn der entsprechende Benutzer zusätzlich entweder auch noch die Server-Rolle Datenbank- oder Konto-Administrator besitzt. Ist ein Benutzer nur Active Directory Operator, dann kann er weder die Active Directory-/Azure AD-Synchronisation durchführen noch andere Server-Einstellungen tätigen.
- Ereignisprotokoll-Leser: Diese Server-Rolle ermöglicht Benutzern, über den Server-Manager Zugriff auf die Protokolle des Servers zu erhalten und diese einzusehen.

HINWEIS: Durch die Einführung der unterschiedlichen Server-Rollen wurde mit Version 15 auch die Rolle des vordefinierten Admin-Kontos geändert: Das Konto des Super-Administrators ist von nun an ausschließlich für die Verwaltung des Servers vorgesehen und nicht mehr zusätzlich auch als Benutzerkonto. Das heißt, mit dem Konto des Super-Administrators können Sie sich nur noch am Server-Manager anmelden, aber nicht mehr über den Client am Server. Daher zählt das

Konto des Super-Administrators auch nicht mehr als Benutzerkonto, sondern dieses kann zusätzlich zu der bestehenden Anzahl an Benutzerlizenzen dazugerechnet werden.

Mitglied von

Hier können Sie einsehen, in welchen Gruppen der entsprechende Benutzer Mitglied ist. Außerdem können Sie einzelne Benutzer hier weiteren Gruppen hinzufügen. Voraussetzung hierfür ist, dass die entsprechende Gruppe bereits im Server-Manager existiert.

- Gruppe hinzufügen: Klicken Sie auf diese Schaltfläche, um den Benutzer in eine neue bzw. weitere Gruppe aufzunehmen.
- Löschen: Wählen Sie eine bestehende Gruppe aus der Liste aus und klicken Sie auf Löschen, um den Benutzer aus der entsprechenden 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 können Sie als Administrator über den Server-Manager die Einstellungen zum WebSockets-Port für die Browser-Add-Ons definieren. Folgende Optionen stehen hier zur Verfügung:

- **Globale Einstellungen verwenden [25109]:** Mit dieser Einstellung verwenden alle Clients für die Kommunikation mit dem Browser-Add-On standardmäßig die Portnummer 25109.
- Automatisches Generieren der Portnummer: Aktivieren Sie diese Option, wenn Sie möchten, dass jedem einzelnen Benutzer eine eigene, spezifische Portnummer automatisch zugewiesen wird. Die individuelle Portnummer können Benutzer dann im Client unter Bearbeiten -> Optionen -> Browser einsehen.
- Benutzerdefinierte Portnummer verwenden: Hier können Sie als Administrator Ihren Benutzern benutzerdefinierte Portnummern zuweisen und die entsprechenden Portnummer selbst definieren. Auch in diesem Fall können Benutzer dann die benutzerdefinierte Portnummer im Client unter Bearbeiten -> Optionen -> Browser einsehen.

Überprüfung IP-Adresse

Hier können Sie einem 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.

Azure AD

In dieser Registerkarte werden die Azure AD-Attribute eines Benutzers, der per Azure AD-Synchronisation dem Server-Manager hinzugefügt wurde, aufgeführt.

- Benutzerprinzipalname: Zeigt den Benutzerprinzipalnamen eines Benutzers an, sofern dieser dem Server-Manager per Azure AD-Synchronisation hinzugefügt wurde.
- **Objekt-ID:** Jedem Azure AD-Benutzer wird eine spezifische Objekt-ID zugeordnet, die auch im Server-Manager nach korrekter Azure AD-Synchronisation angezeigt wird.
- Benutzertyp: Hier wird Ihnen der Benutzertyp des synchronisierten Azure AD-Benutzers angezeigt. Es wird grundsätzlich zwischen einem Gast und einem Mitglied unterschieden. Bei Mitgliedern handelt es sich um Benutzer, die Ihrer eigenen Organisation angehören, Gäste sind Benutzer, die Sie beispielsweise zur temporären Zusammenarbeit zu Ihrer Organisation einladen können.

Active Directory DS

In dieser Registerkarte werden die Active Directory-Attribute eines Benutzers, der per Active Directory-Synchronisation dem Server-Manager hinzugefügt wurde, aufgeführt.

- Anmeldename: Zeigt den Benutzernamen des Benutzers an, mit dem er sich an der Domäne anmeldet.
- Benutzerprinzipalname: Der Benutzerprinzipalname gibt den Namen des Systembenutzers im Active Directory im E-Mail-Format wieder.
- ADs-Pfad: Hier wird der korrekte Active Directory-Pfad eines Benutzers angezeigt.
- GUID: Die automatisch generierte ID eines Active Directory-Benutzers.

HINWEIS: Die Informationen in den Registerkarten Azure AD sowie Active Directory DS sind nur von Bedeutung, wenn Sie im Server-Manager eine Active Directory- oder Azure AD-Synchronisation durchführen, damit sich Ihre Benutzer per Integrierter Windows-Authentifizierung (SSO) bzw. mit Ihren Azure AD-Zugangsdaten am Enterprise Server anmelden können. In diesem Fall werden hier bei der Synchronisation der Benutzer die entsprechenden Daten aus Active Directory/Azure AD automatisch erfasst und eingefügt. Bitte tragen Sie daher hier keine Daten manuell ein, sondern lassen Sie dies den Server-Manager, während der entsprechenden Synchronisation, automatisch übernehmen.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Rechte für Benutzer

Grundsätzlich können Sie Password Depot Enterprise Server so nutzen, dass Sie eine Server-Datenbank erstellen, auf die alle Ihre Mitarbeiter Zugriff haben. Die Rechteverwaltung im Server-Manager erlaubt es Administratoren, die Struktur der Datenbank so aufzubauen und die Zugriffsrechte so zu verteilen, dass jeder Benutzer tatsächlich nur das sieht, was er sehen und worauf er zugreifen können soll. Sind die Rechte korrekt gesetzt, so kennen Benutzer und Gruppen gar nicht den gesamten Inhalt einer Datenbank und können daher immer nur mit den Ordnern und Einträgen arbeiten, die ihnen angezeigt werden.

HINWEIS: Die Rechte für Benutzer, so wie sie in diesem Kapitel beschrieben werden, können gleichermaßen auch auf Gruppen angewendet werden.

Es besteht kein Zwang, auf dem Enterprise Server nur mit einer einzigen Datenbank zu arbeiten, der Gedanke dahinter ist aber, dass Sie grundsätzlich mit einer einzigen Datenbank auch bei sehr vielen Mitarbeitern allen Anforderungen entsprechen können. Sollten Sie mit mehreren Datenbanken arbeiten wollen, ist dies prinzipiell auch möglich und umsetzbar. Darüber hinaus können Sie Ihren Benutzern/Gruppen auf dem Server auch private Datenbanken zur Verfügung stellen, die immer getrennt von gemeinsamen Datenbanken zu betrachten sind. Mehr zu den privaten Datenbanken können Sie hier nachlesen.

Wie gestaltet sich die Rechteverwaltung am Enterprise Server?

Wir empfehlen grundsätzlich, die Rechtezuweisung für Benutzer im Bereich Datenbanken -> Berechtigungen vorzunehmen. Hier können Sie für jeden einzelnen Benutzer und jede einzelne Gruppe auf dem Server detailliert Rechte vergeben, und zwar

1. auf Datenbank-Ebene
2. auf Ebene der einzelnen Einträge und Ordner

Darüber hinaus gibt es noch eine globale und für den gesamten Server geltende Rechteverwaltung unter Verwalten -> Serverrichtlinien. Hier können Sie bereits bestimmte Rechte definieren, die dann aber für den gesamten Server und alle Benutzer/Gruppen gelten. Die Serverrichtlinien sind daher also globale Richtlinien.

Was ist bei den Serverrichtlinien zu beachten?

Die Rechte der Serverrichtlinien sind identisch mit den Rechten, die Sie im Bereich Datenbanken -> Berechtigungen auf Datenbank-Ebene vergeben können. In den Serverrichtlinien können die Rechte drei verschiedene Zustände haben:

1. Aktiviert
2. Nicht definiert
3. Deaktiviert

Bei Installation des Enterprise Servers sind die Serverrichtlinien standardmäßig entweder auf Aktiviert oder Nicht definiert gesetzt. Als Best Practice empfehlen wir, die Einstellungen hier so zu belassen und die Rechteverwaltung mehrheitlich über den Bereich Datenbanken -> Berechtigungen vorzunehmen. Dennoch gilt: Sie können den Status eines Rechts auch in den Serverrichtlinien ändern und diesen beispielsweise hier auf Deaktiviert setzen. In diesem Fall müssen Sie dann nur dringend Folgendes beachten:

Ist ein Recht in den Serverrichtlinien deaktiviert, so können Sie dieses Recht im weiteren Verlauf der Rechtevergabe auf Datenbank-Ebene und auf Ebene der Einträge und Ordner nicht mehr aktivieren! Deaktivierte Rechte in den Serverrichtlinien gelten daher für ALLE Benutzer/Gruppen (auch für Server-Administratoren) sowie ALLEN Datenbanken auf dem Server. Es handelt sich dabei also um einen sehr restriktiven Status, der tatsächlich nur verwendet werden sollte, wenn es zwingend erforderlich ist. Ansonsten laufen Sie eventuell Gefahr, Rechte global zu verwehren, die Sie im Nachhinein gerne für einzelne Benutzer/Gruppen doch noch aktivieren möchten.

TIPP: Mehr zu den Serverrichtlinien können Sie im Kapitel Berechtigungen nachlesen oder auch in folgendem Knowledge Base-Artikel: Wie erfolgt die Rechteverwaltung im Enterprise Server?

FAZIT: Globale Rechte unter Verwalten -> Serverrichtlinien sollten Sie tatsächlich nur deaktivieren, sofern es nicht anders möglich ist.

BEISPIEL: In den Serverrichtlinien deaktivieren Sie das Recht Exportieren von Einträgen. Dies bedeutet, dass im weiteren Verlauf kein einziger Server-Benutzer Einträge aus den Server-Datenbanken exportieren kann, um diese beispielsweise in eine andere Datenbank zu importieren. Der Export bleibt dann auf dem gesamten Server deaktiviert und ist daher für niemanden verfügbar.

Rechteverwaltung in den Berechtigungen einer Datenbank

Wenn Sie die Berechtigungen einer Datenbank öffnen, so können Sie hier beginnen, die Rechte für einzelne Benutzer und Gruppen detailliert zu vergeben. Die Rechte werden jeweils in den Registerkarten Datenbank sowie Einträge und Ordner vergeben.

Wenn Sie mehrere Benutzer/Gruppen haben, die auf die gleiche Datenbank zugreifen, dabei aber eine unterschiedliche Ansicht des Inhalts haben sollen, dann sollten sie

a. In der Registerkarte Datenbank bei den Rechten Lesen/Ändern/Hinzufügen/Löschen von Einträgen die Häkchen entfernen und
b. In der Registerkarte Einträge und Ordner genau die Objekte auswählen, auf die Sie einem Benutzer oder eine Gruppe explizit den Zugriff gewähren möchten.

WARNUNG: Sie sollten in der Registerkarte Datenbank bei den Rechten Lesen/Ändern/Hinzufügen/Löschen auf keinen Fall das Verweigern-Flag verwenden, denn dies hat zur Folge, dass Sie einem Benutzer zwar den Zugriff auf die Datenbank gewähren, sodass er sie empfangen kann - dadurch, dass das Verweigern-Flag aber sehr restriktiv in seinen Auswirkungen ist, kann der Benutzer innerhalb der entsprechenden Datenbank nichts sehen und somit auch nicht damit arbeiten.

Das Recht Zugriff auf die Datenbank sollten Sie einem Benutzer erlauben, sofern er mit der Datenbank und deren Inhalt arbeiten soll. Bei allen anderen Rechten auf Datenbank-Ebene (Registerkarte Datenbank) können Sie hier auch das Verweigern-Flag verwenden. Dies hat dann zur Folge, dass der ausgewählte Benutzer oder die ausgewählte Gruppe dieses bestimmte Recht innerhalb der ausgewählten Datenbank (das heißt also, auf die gesamte Datenbank bezogen) nicht ausüben kann.

Häkchen bei den Rechten Lesen/Ändern/Hinzufügen/Löschen von Einträgen entfernen - was hat dies zur Folge?

Wenn Sie in der Registerkarte Datenbank das Häkchen bei den zuvor genannten Rechten entfernen, gleichzeitig aber den Zugriff auf die entsprechende Datenbank erlauben, dann bedeutet dies, dass Sie einem Benutzer/einer Gruppe erlauben, eine Datenbank zu empfangen und auf diese (grundsätzlich) zuzugreifen. Gleichzeitig kann der jeweilige Benutzer erst einmal aber keine Einträge innerhalb der Datenbank und innerhalb ihres Stammverzeichnisses sehen, weil die Häkchen bei den Rechten Lesen/Ändern/Hinzufügen/Löschen von Einträgen entfernt wurden. Diese Rechte sind jedoch für das Arbeiten mit Einträgen und Ordnern erforderlich.

Wenn Sie nun zur Registerkarte Einträge und Ordner wechseln, so sehen Sie zunächst, dass der gesamte Datenbank-Inhalt rot markiert ist. Die Farbe Rot teilt in diesem Fall mit, dass der Zugriff auf Einträge und Ordner nicht erlaubt ist. Damit Ihre Benutzer/Gruppen nun auch tatsächlich Zugriff auf den Inhalt der Datenbank erhalten, müssen Sie als Administrator in dieser Registerkarte die einzelnen Ordner und Einträge aufrufen und die Berechtigungen entsprechend verteilen. Auf diese Weise können Sie für jeden Benutzer/jede Gruppe explizite Rechte definieren und genau festlegen, auf welchen Inhalt (=Einträge und Ordner) zugegriffen werden soll. Die farbliche Gestaltung unterstützt Sie dabei: Alles, was Rot ist, kann nicht geöffnet werden; auf alles, was Grün ist, kann wiederum zugegriffen werden.

Diese Vorgehensweise erlaubt Ihnen als Administrator auch, eine Struktur innerhalb der Datenbank aufzubauen, die beispielsweise gemeinsam genutzte und private Ordner/Einträge umfasst und dabei stets gewährleistet, dass jeder Benutzer/jede Gruppe tatsächlich immer nur das sieht, wozu er/sie berechtigt sind.

HINWEIS: Die Rechte Lesen / Ändern / Hinzufügen / Löschen von Einträgen besitzen eine gewisse Abhängigkeit voneinander und sollten nach Möglichkeit entweder alle zusammen erlaubt oder verweigert werden. Wenn Sie also beispielsweise das Hinzufügen eines neuen Eintrags erlauben, das Ändern eines bestehenden Eintrags aber verweigern möchten, dann wird dies nicht funktionieren, da das Hinzufügen eines Eintrags ebenso bedeutet, dass innerhalb der Datenbank etwas geändert wird. Es macht daher also keinen Sinn, diese vier Rechte getrennt voneinander zu betrachten, sondern diese sollten als zusammengehörig angesehen werden.

Weitere Informationen zur Rechteverwaltung im Enterprise Server mit anschaulichen Beispielen finden Sie in unserer Knowledge Base:

Wie vergebe ich die Rechte an die Benutzer, sodass diese nur das sehen können, wozu sie berechtigt sind?

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Datenbank zuweisen

Die Funktion **Datenbank** zuweisen, die Sie für Benutzer und Gruppen auf der rechten Seite des Server-Managers finden können, ermöglicht es Ihnen, Datenbanken einem Benutzer und/oder einer Gruppe direkt zuzuordnen. Darüber hinaus können Sie diese Funktion auch nutzen, um mehreren Benutzern und/oder Gruppen gleichzeitig eine Datenbank zuzuweisen bzw. neue Datenbanken zu erzeugen und diese ebenfalls gleich Benutzern und/oder Gruppen zuzuweisen.

Wählen Sie einen oder mehrere Benutzer/Gruppen aus und klicken Sie dann auf Datenbank zuweisen. Im Dialogfeld Datenbank zuweisen stehen Ihnen folgende Register zur Verfügung:

Datenbank

Ausgewählte Konten

Hier sehen Sie alle Benutzer bzw. Gruppen, die Sie zuvor für die explizite Datenbankzuweisung ausgewählt haben. Allen hier angehakten Objekten wird die entsprechende Datenbank im Anschluss zugewiesen.

Vorhandene Datenbank auswählen

Wählen Sie aus dem Drop-Down-Menü eine vorhandene Datenbank aus, die Sie gleichzeitig allen, links unter Ausgewählte Konten markierten Objekten zuweisen möchten.

Neue Datenbank erzeugen

Wählen Sie diese Option, wenn Sie eine neue, leere Datenbank erzeugen und diese gleichzeitig allen, links unter Ausgewählte Konten markierten Objekten zuweisen möchten.

Private Datenbank erzeugen

Hier können Sie eine neue, private Datenbank für jedes, links unter Ausgewählte Konten markierte Objekt erstellen lassen. Diese Funktion ist hilfreich, wenn Sie viele Benutzer haben und Sie diesen (zusätzlich) auch private Datenbanken auf dem Server bereitstellen möchten oder müssen. Die privaten Datenbanken werden jeweils mit dem Benutzernamen des Benutzers versehen, für den sie erstellt wurden. Somit lassen sich solche privaten Datenbanken genau zuordnen. Eine automatisch erzeugte private Datenbank für den Benutzer "Matthias Müller" erhält

dann beispielsweise folgende Bezeichnung: Private_DB_Matthias Müller.pswe. Auch für Gruppen können Sie gleichermaßen private Datenbanken erzeugen.

Rechte

Sie können hier vorab für die Datenbanken, die Sie einem oder mehreren Benutzern/Gruppen zuweisen möchten, die Rechte auf Datenbank-Ebene bestimmen. Alle ausgewählten Benutzer/Gruppen erhalten dann die gleichen Rechte. Die detaillierte Rechteverwaltung sollten Sie allerdings über die Berechtigungen einer Datenbank vornehmen.

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 **-> Berechtigungen** zugewiesen. Eine Gruppe besteht aus einem oder mehreren Mitgliedern (Benutzern). Durch das Erzeugen von Gruppen können Sie die Verwaltung vereinfachen, indem Sie später die Rechte für Datenbanken ganzen Gruppen zuweisen anstatt einzelnen Benutzern.

In der Hauptansicht werden Ihnen zu den einzelnen Gruppen folgende Spalten angezeigt:

- Name: Zeigt den Namen der entsprechenden Gruppe an.
- Typ: Zeigt an, um welchen Gruppentyp es sich handelt. Es gibt im Server-Manager Gruppen vom Typen Standard (manuell und lokal angelegte Gruppen), Azure AD (Gruppen, die per Azure AD-Synchronisation importiert wurden) sowie Active Directory-Gruppen (wenn diese per Active Directory-Synchronisation hinzugefügt wurden).
- Domain: Zeigt den Namen der Stammdomäne (Root Domain Name) an, die bei der Konfiguration des Servers festgelegt und für die Active Directory-Synchronisation verwendet wurde. Aus dieser Stammdomäne wurden die Gruppen aus Active Directory mit dem Server-Manager synchronisiert.
- Beschreibung: Zeigt die Beschreibung einer Gruppe an, sofern Sie beim Erstellen der Gruppe (oder auch im späteren Verlauf) der Gruppe eine Beschreibung hinzugefügt haben.

Auf der rechten Seite der Hauptansicht stehen Ihnen zudem die folgenden Optionen zur Verfügung:

- Neue Gruppe: Über diese Schaltfläche können Sie dem Server neue, lokale Gruppen hinzufügen. Es öffnet sich im Anschluss das Dialogfenster Neue Gruppe.
- Eigenschaften: Öffnet die Eigenschaften einer vorhandenen Gruppe und erlaubt dem Administrator, diese zu ändern.
- Löschen: Löscht eine markierte Gruppe vom Server-Manager.
- Synchronisieren: Mit dieser Option können Sie die markierte/ausgewählte Gruppe einzeln über AD bzw. Azure AD synchronisieren, ohne dabei den Active Directory- bzw. Azure AD-Synchronisationsassistenten erneut aufrufen und die Gruppe hieraus importieren zu müssen. Bitte beachten Sie aber, dass die jeweilige Gruppe zuvor bereits per AD-/Azure 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-/Azure AD-Daten geändert haben. Hierfür muss dann nicht erneut eine komplette AD-/Azure AD-Synchronisation erfolgen.
- Datenbank zuweisen: Ermöglicht dem Administrator, einzelne Datenbanken mehreren Gruppen gleichzeitig zuzuweisen bzw. auch, neue Datenbanken zu erzeugen und diese

direkt den markierten Gruppen zuzuordnen. Über die Registerkarte Rechte kann der Administrator für die Gruppen gleich die entsprechenden Rechte auf Datenbank-Ebene definieren. Außerdem können hier auch für Gruppen private Datenbanken erzeugt werden, die ebenfalls auf dem Enterprise Server abgespeichert sind. Mehr zu den privaten Datenbanken erfahren Sie im Kapitel Datenbank zuweisen.

- Alle auswählen: Markiert alle am Server verfügbaren Gruppen, um anschließend weitere Aktionen auszuführen, die sich dann auf alle Gruppen beziehen.

TIPP: Diese Funktionen können Sie auch durch einen Rechtsklick auf eine Gruppe aus der Liste aufrufen. Zudem können Sie die Anzeige der Hauptansicht auch filtern, um beispielsweise nach einer bestimmten Gruppe zu suchen. Geben Sie dazu einen Gruppennamen oder einen Teil davon ein, um die Suche zu starten.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Gruppen hinzufügen

Wie auch bei den Benutzern, gibt es ebenso für Gruppen drei unterschiedliche Wege, um diese im Password Depot Enterprise Server verfügbar zu machen.

1. Über die Schaltfläche Neue Gruppe
2. Per Active Directory-Synchronisation
3. Per Azure AD-Synchronisation

Neue Gruppen manuell anlegen

Über die Schaltfläche Neue Gruppe, die Ihnen im Bereich Gruppen auf der rechten Seite zur Verfügung steht, können Sie dem Server-Manager neue, lokale Gruppen manuell hinzufügen. Geben Sie solchen Gruppen einen Namen; auf Wunsch können Sie der Gruppe auch eine ausführlichere Beschreibung hinzufügen. Manuell angelegte Gruppen sind vom Typ her Standard-Gruppen und dies kann auch nicht geändert werden. Über die Registerkarte Mitglieder können Sie einer neuen Gruppe im Anschluss die gewünschten Mitglieder hinzufügen. Weitere Informationen hierzu erhalten Sie auch im nachfolgenden Kapitel Eigenschaften einer Gruppe.

TIPP: Sie können Standard-Gruppen sowohl lokal angelegte Benutzer als auch aus Active Directory oder Azure AD synchronisierte Benutzer hinzufügen. Je nachdem um welchen Benutzertypen es sich handelt, melden sich diese im Anschluss über die entsprechende Authentifizierungsmethode am Enterprise Server an.

Neue Gruppen per Active Directory-Synchronisation dem Server hinzufügen

Sie können Gruppen auch aus Active Directory (per Active Directory-Synchronisation) auf dem Server-Manager verfügbar machen. Dies ist zum Beispiel sinnvoll, wenn Sie bereits existierende Active Directory-Gruppen genauso auch im Server-Manager abbilden und nutzen möchten. Gehen Sie im Server-Manager auf Extras -> Active Directory-Synchronisation, um die Synchronisation zu starten. Die Gruppenobjekte werden dann entsprechend aus Active Directory mit dem Server-Manager synchronisiert und importiert. Sofern der Vorgang erfolgreich war, können Sie im Anschluss im Bereich Gruppen alle aus Active Directory importierten Objekte sehen.

HINWEIS: Der Password Depot Enterprise Server unterstützt derzeit leider keine verschachtelten Sicherheitsgruppen.

Gruppen, die per Active Directory-Synchronisation dem Server-Manager hinzugefügt wurden, enthalten automatisch die entsprechenden Active Directory-Benutzer. Erhält eine AD-Gruppe nun Zugriff auf eine Datenbank auf dem Server, dann können sich alle Mitglieder dieser Gruppe (=AD-Benutzer) per Integrierter Windows-Authentifizierung (SSO) am Enterprise Server anmelden. Auch hier gilt Folgendes: Bei Authentifizierung wird das vom Benutzer eingegebene Kennwort an Active Directory gesendet und Password Depot erhält ein richtig oder falsch zurück und vollzieht auf Grundlage dessen die Anmeldung oder verweigert diese bei falschem Kennwort. Daher ist es wichtig, dass die im Server-Manager hinterlegten Daten den Benutzerdaten aus Active Directory entsprechen. Aus diesem Grund empfiehlt es sich, regelmäßig eine Synchronisation durchzuführen, um Änderungen in der Active Directory auch in den Server-Manager zu übernehmen.

TIPP: Mehr zur Active Directory-Synchronisation erfahren Sie im gleichnamigen Kapitel.

Neue Gruppen per Azure AD-Synchronisation dem Server hinzufügen

Azure AD-Gruppen müssen Sie als Administrator ebenfalls per Synchronisation dem Server hinzufügen. Um die Synchronisation zu starten, gehen Sie auf Extras -> Azure AD-Synchronisation. Die Gruppenobjekte werden dann entsprechend aus Ihrem Azure-AD mit dem Server-Manager synchronisiert. Sofern der Vorgang erfolgreich war, können Sie im Anschluss im Bereich **Gruppen** alle aus Azure-AD importierten Objekte sehen.

Wie bei der Active Directory-Synchronisation gilt auch für die Synchronisation aus Azure AD: Gruppen, die per Azure AD-Synchronisation dem Server-Manager hinzugefügt wurden, enthalten automatisch die entsprechenden Azure AD-Benutzer. Erhält eine Azure AD-Gruppe nun Zugriff auf eine Datenbank auf dem Server, dann können sich alle Mitglieder dieser Gruppe (=Azure AD-Benutzer) per Azure AD-Authentifizierung am Enterprise Server anmelden.

TIPP: Mehr zur Azure AD-Synchronisation erfahren Sie im gleichnamigen Kapitel.

Eigenschaften einer Gruppe

Jede am Server-Manager verfügbare Gruppe hat eigene Eigenschaften. Diese können Sie aufrufen, indem Sie im Bereich Gruppen entweder auf eine Gruppe **doppelklicken** oder aber eine **Gruppe auswählen** und per Rechtsklick deren Eigenschaften öffnen.

Über die Eigenschaften einer Gruppe können Sie diese verwalten. Es stehen Ihnen die folgenden Registerkarten zur Verfügung:

- Allgemein
- Mitglieder

Was Sie in den einzelnen Registerkarten verwalten können, wird nachfolgend näher erläutert.

Allgemein

Folgende Angaben können Sie in der Registerkarte Allgemein definieren:

- Name: Geben Sie den Namen der Gruppe ein.
- Typ: Bezeichnet den Typ der Gruppe, zum Beispiel Active Directory- oder Standard-Gruppe, falls diese im Password Depot Server-Manager manuell erzeugt wurde.
- Beschreibung: Hier können Sie optional der Gruppe noch eine Beschreibung hinzufügen. Falls die Gruppe aus Active Directory oder Azure AD synchronisiert wurde, wird die Beschreibung von dort übernommen.

Über das Kontrollkästchen Deaktiviert im unteren linken Bereich können Sie eine vorhandene Gruppe im Server-Manager deaktivieren (Häkchen setzen) und auch wieder aktivieren (Häkchen rausnehmen), sofern die Gruppe deaktiviert war. Somit können Sie Gruppen beispielsweise temporär deaktivieren, sollten diese eine Zeit lang nicht mehr benötigt werden, ohne diese vollständig löschen zu müssen. Sobald eine Gruppe dann wieder benötigt wird, können Sie diese durch Entfernen des Häkchens wieder aktivieren.

Mitglieder

In der Registerkarte Mitglieder können Sie Folgendes durchführen:

- Die Benutzer einer Gruppe einsehen
- Einer Gruppe neuer Benutzer hinzufügen
- Benutzer aus einer Gruppe entfernen bzw. löschen

Die Benutzer einer Gruppe einsehen

Falls die ausgewählte Gruppe bereits Mitglieder hat, werden diese in der gleichnamigen Registerkarte aufgelistet. Die hier angezeigten Informationen zu einem Benutzer teilen sich wie folgt auf:

- Konto: Zeigt das Benutzerkonto (= den Benutzernamen) eines Benutzers an.
- Typ: Zeigt, ob ein Benutzer eine zusätzliche Serverrolle hat, zum Beispiel Datenbank- oder Server-Administrator etc. Mehr zu den Serverrollen erfahren Sie hier.
- Vollständiger Name: Zeigt den vollständigen Namen eines Benutzers an, so wie dieser in den Eigenschaften des Benutzers hinterlegt wurde.
- Abteilung: Zeigt die Abteilung eines Benutzers an, sofern diese im Server-Manager hinterlegt wurde.
- Beschreibung: Sofern Sie einem Benutzer eine individuelle Beschreibung hinzugefügt haben oder die Beschreibung eines Benutzer per Active Directory-/Azure AD-Synchronisation dem Server-Manager hinzugefügt wurde, werden die entsprechenden Informationen hier angezeigt.

Einer Gruppe neuer Benutzer hinzufügen

Über die Schaltfläche Benutzer hinzufügen können Sie neue Mitglieder in eine Gruppe aufnehmen.

- Benutzer hinzufügen: Wenn Sie diese Option wählen, dann öffnet sich das Dialogfenster Benutzer. Hier werden Ihnen alle auf dem Server verfügbaren Benutzer angezeigt, sodass Sie einzelne Benutzer auswählen und per Klick auf OK einer Gruppe hinzufügen können.

HINWEIS: Sie können hier auch mehrere Benutzer markieren, wenn Sie diese einer bestimmten Gruppe gleichzeitig hinzufügen möchten. Außerdem sehen Sie im unteren Bereich des Dialogfensters eine Such-/Filteroption. In diesem Feld können Sie gezielt nach einzelnen Benutzern suchen.

- Benutzer über Abteilung hinzufügen: Wenn Sie Ihre Benutzer bestimmten Abteilungen zugewiesen haben (dies können Sie in den Eigenschaften eines Benutzers in der Registerkarte Allgemein einsehen), dann haben Sie auch die Möglichkeit, einer Gruppe neue Mitglieder über Abteilungen hinzuzufügen. Im Dialogfenster Benutzer über Abteilung hinzufügen können Sie dann ganz oben zunächst die gewünschte Abteilung auswählen. Unter Abteilungsmitglieder in der Gruppe können Sie sehen, welche Abteilungsmitglieder der zuvor gewählten Abteilung in der entsprechenden, geöffneten Gruppe Mitglieder sind. Unter Andere Abteilungsmitglieder sehen Sie alle anderen

Benutzer, die ebenfalls der zuvor gewählten Abteilung angehören, aber (noch) nicht der gerade geöffneten Gruppe hinzugefügt wurden.

Benutzer aus einer Gruppe entfernen bzw. löschen

Nutzen Sie die Schaltfläche Löschen um einzelne Mitglieder aus Gruppen zu entfernen bzw. zu löschen.

HINWEIS: Benutzer, die aus einer Gruppe entfernt wurden, werden nicht automatisch auch vom Server-Manager gelöscht, sondern Sie beenden dadurch nur deren Mitgliedschaft in der ausgewählten Gruppe. Auf dem Server-Manager sind solche Benutzer aber nach wie vor verfügbar und aktiv.

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.

Zu den Benachrichtigungen wird Ihnen in der Hauptansicht Folgendes angezeigt:

- ID: Jede Benachrichtigung besitzt ein eigene ID, beginnend bei 1. Wenn Sie also beispielsweise auf dem Server 10 Benachrichtigungen hinzugefügt haben, dann werden die IDs 1-10 vergeben. Die als erstes hinzugefügte Benachrichtigung erhält die 1 und alle weiteren Benachrichtigungen werden dann nach oben hin durchnummeriert.
- Typ: Zeigt den Typ der Benachrichtigung an bzw. bei welchem Ereignis eine Benachrichtigung verschickt werden soll.
- Anmerkungen: Sie können den einzelnen Benachrichtigungen noch individuelle Anmerkungen hinzufügen, die dann ebenfalls in der Hauptansicht angezeigt werden.
- Empfänger: Zeigt den/die Empfänger (E-Mail-Adresse) einer bestimmten Benachrichtigung an.

Auf der rechten Seite der Hauptansicht stehen Ihnen zudem die folgenden Optionen zur Verfügung:

- Neue Benachrichtigung: Über diese Schaltfläche können Sie dem Server eine neue Benachrichtigung hinzufügen.
- Eigenschaften: Öffnet die Eigenschaften einer bereits angelegten Benachrichtigung.
- Löschen: Löscht eine markierte Benachrichtigung vom Server-Manager.
- **Alle auswählen:** Markiert alle am Server verfügbaren Benachrichtigungen, um anschließend weitere Aktionen damit auszuführen, die sich dann auf alle Benachrichtigungen beziehen.

TIPP: Diese Funktionen können Sie auch durch einen Rechtsklick auf eine Benachrichtigung aufrufen. Zudem können Sie die Anzeige der Hauptansicht auch filtern, um beispielsweise nach einer bestimmten Benachrichtigung zu suchen. Geben Sie dazu den Benachrichtigungstypen oder einen Teil davon ein, um die Suche zu starten.

Benachrichtigung hinzufügen

Um dem Server-Manager eine neue Benachrichtigung hinzuzufügen, klicken Sie rechts im Navigationsbereich auf Benachrichtigungen und im Anschluss rechts im Server-Manager auf Neue Benachrichtigung.

Im Anschluss öffnet sich das Dialogfenster Neue Benachrichtigung.

Wählen Sie unter Ereignis das gewünschte Ereignis aus, zu dem eine Benachrichtigung an eine bestimmte Person verschickt werden soll. Auf Wunsch können Sie im Feld darunter individuelle Anmerkungen hinzufügen, die dann immer zusammen mit der entsprechenden Benachrichtigung verschickt werden.

Definieren Sie danach den Empfänger der Benachrichtigung. Wie Sie diesen genau hinzufügen, wird Ihnen in den Eigenschaften einer Benachrichtigung näher erläutert.

Klicken Sie abschließend auf OK, um die gewählte Benachrichtigung dem Server hinzuzufügen. Sie wird im Anschluss in der Hauptansicht aufgelistet.

Eigenschaften einer Benachrichtigung

Jede dem Server-Manager hinzugefügte Benachrichtigung besitzt eigene Eigenschaften. Diese können Sie aufrufen, indem Sie im Bereich Benachrichtigungen entweder auf eine Benachrichtigung **doppelklicken** oder aber eine **Benachrichtigung auswählen** und per Rechtsklick deren Eigenschaften öffnen.

Über die Eigenschaften einer Benachrichtigung können Sie diese verwalten. Es stehen Ihnen die folgenden Registerkarten zur Verfügung:

- Allgemein
- Erweitert

Was Sie in den einzelnen Registerkarten verwalten können, wird nachfolgend näher erläutert.

Allgemein

In dieser Registerkarte 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.
- Der Benachrichtigung diese Anmerkungen hinzufügen: Wenn Sie der E-Mail mit der Benachrichtigung individuelle 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 eine 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 bereits aufgelistete E-Mail-Adresse ersetzen möchten, so markieren Sie die bisherige, geben im Feld unten links die neue E-Mail-Adresse ein (oder wählen diese, sofern bereits vorhanden, aus dem Drop-Down-Menü aus) und klicken auf Ersetzen.

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

Erweitert

Die Registerkarte Erweitert greift nicht bei allen Ereignissen, sondern nur bei bestimmten. Wenn Sie greift, dann können Sie hier zusätzlich einstellen, dass die Benachrichtigung für das bestimmte Ereignis auf ausgewählte Datenbanken, Datenbankeinträge, Benutzer oder Gruppen beschränkt werden soll. In diesem Fall wird die Benachrichtigung dann nicht grundsätzlich verschickt, wenn auf dem Server das Ereignis eintritt, sondern beispielsweise nur, wenn es in einer bestimmten Datenbank eintritt oder von einem spezifischen Benutzer ausgelöst wurde etc.

Benutzer und Gruppen

- Alle Benutzer und Gruppen: Wählen Sie diese Option, wenn die Benachrichtigung durch alle Benutzer und Gruppen auf dem Server ausgelöst werden soll.
- Ausgewählte Benutzer und Gruppen: Hier können Sie definieren, ob die gewählte Benachrichtigung nur durch bestimmte Benutzer und/oder Gruppen ausgelöst werden soll. Über die Schaltfläche Hinzufügen können Sie einzelne Benutzer/Gruppen hinzufügen und über die Schaltfläche Entfernen solche Benutzer/Gruppen wieder aus der Liste löschen.

Objekte

- Alle Datenbanken: Wählen Sie diese Option, wenn die Benachrichtigung auf alle Server-Datenbanken angewendet werden soll.
- Ausgewählte Datenbanken: Hier können Sie festlegen, ob die gewählte Benachrichtigung nur auf einzelne Server-Datenbanken angewendet werden soll. In diesem Fall gilt die gewählte Benachrichtigung dann nur für die hier aufgelisteten Datenbanken auf dem Server. Über die Schaltfläche Hinzufügen können Sie einzelne Datenbanken hinzufügen und über die Schaltfläche Entfernen solche Datenbanken wieder aus der Liste löschen.
- Ausgewählte Einträge: Sie können die gewählte Benachrichtigung auch nur bei ausgewählten Einträgen verschicken lassen. In diesem Fall greift die Benachrichtigung dann nur für die hier aufgelisteten einzelnen Einträge auf dem Server. Über die Schaltfläche Hinzufügen können Sie einzelne Einträge hinzufügen und über die Schaltfläche Entfernen solche Einträge wieder aus der Liste löschen.

Zur Homepage von Password Depot zurückkehren (diese Hilfe verlassen)

Protokoll

In dieser Ansicht wird das Protokoll der Serveraktivitäten angezeigt.

Die Serverprotokolle haben ein Standardformat nach RFC 5424 für die einfache Verarbeitung in externen Log-Analyzern. Optional können alle Protokollaufzeichnungen im Echtzeitmodus per UDP an externe Protokollserver zur revisionssicheren Verarbeitung und Speicherung gesendet werden. Weitere Einstellungen zu den Protokollen des Enterprise Servers können Sie in den Serveroptionen vornehmen.

In der Hauptansicht des Protokoll-Bereichs werden Ihnen folgende Informationen angezeigt:

- Ebene: Hier können Sie sehen, um was für eine Art von Protokolleintrag es sich handelt, zum Beispiel Zur Information oder Fehler, wenn ein Fehler auf dem Server registriert wurde.
- Datum und Uhrzeit: Zeigt das genaue Datum und die exakte Uhrzeit an, zu der eine Serveraktivität registriert wurde.
- Benutzername: Zeigt den Benutzer (unter seinem Benutzernamen) an, der auf dem Server eine Aktivität durchgeführt hat.
- Adresse: Zeigt die IP-Adresse des Benutzers an bzw. von welcher IP-Adresse eine Aktivität ausgegangen ist.
- Ereignis-ID: Jede einzelne Aktivität auf dem Server erhält eine spezifische Ereignis-ID.
- Beschreibung: In dieser Spalte können Sie sehen, welche Aktivität durchgeführt wurde, zum Beispiel **Datenbank an Benutzer gesendet, Einträge exportiert** oder Anmeldung eines Clients usw.
- Datenbank: Zeigt an, in welcher Datenbank auf dem Server eine Aktivität durchgeführt wurde.
- Objekt: Zeigt an, auf welches Objekt (Ordner/Eintrag) in der entsprechenden Datenbank zugegriffen wurde.
- Neues Objekt: Wird ein Eintrag/Ordner aktualisiert oder beispielsweise verschoben, so gibt es einen Vermerk in der Spalte Neues Objekt. Sie können hier dann sehen, durch was ein Objekt ersetzt bzw. aktualisiert wurde.
- Grund: Wird ein Fehler auf dem Server registriert, so wird Ihnen in dieser Spalte der Grund für diesen Fehler angezeigt. Außerdem können Administratoren von Ihren Benutzern das Angeben eines Grunds zum Löschen von Ordnern und Einträgen auf dem Server erzwingen. Wird in diesem Fall ein Objekt gelöscht und muss dafür ein Grund definiert werden, so wird dieser ebenfalls in der Spalte Grund angezeigt.

Auf der rechten Seite der Hauptansicht stehen Ihnen zudem die folgenden Optionen zur Verfügung:

- Protokoll öffnen: Öffnen Sie eine vorhandene Protokolldatei (*.log) direkt im Server-Manager.

- Protokoll exportieren: Exportieren Sie das Protokoll des Servers entweder in das XML- oder CSV-Format und speichern Sie dieses ab.
- Erweiterter Filter: Erlaubt die detaillierte Filterung der Datensätze des Protokolls.

TIPP: Im oberen Bereich der Hauptansicht haben Sie die Möglichkeit im Protokoll des Servers gezielt nach Ereignissen zu suchen. Geben Sie als Filter zum Beispiel den Benutzernamen eines Server-Benutzers ein und Ihnen werden alle Ereignisse aufgelistet, die in Zusammenhang mit diesem Server-Benutzer stehen.

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)

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)