Password DEPOT

Handbuch

Password Depot Enterprise Server 17

Zuletzt aktualisiert: 01.12.22

Inhalt

Einführung
- Lizenzierung

Installation und Betrieb
- Migration
- Nutzung auf einem Terminal-Server

Server-Manager
- Verwalten
  - Serveroptionen
  - Server-Lizenz
  - Serverrichtlinien
  - Client-Sicherheitsrichtlinien
  - Serverspiegelung
  - Programmoptionen
- Extras
  - Active Directory-Synchronisation
  - Azure AD-Synchronisation
  - Berichte
  - SSL-Zertifikat
- Datenbanken
  - Datenbank dem Server hinzufügen
  - Berechtigungen
  - Eigenschaften
- Benutzer
  - Benutzer hinzufügen
  - Benutzereigenschaften
  - Datenbank zuweisen
- Gruppen
  - Gruppen hinzufügen
  - Gruppeneigenschaften
- Benachrichtigungen
  - Neue Benachrichtigung
  - Benachrichtigungseigenschaften
- Protokoll
  - Ereignis-IDs

Rechte für Benutzer

Einführung

Mithilfe 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 sowie die Clients für macOS und die Apps für iOS und Android. Über sie können Sie die Server-Datenbanken öffnen und die darin gespeicherten Daten verwenden.

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 nur auf bestimmte Objekte innerhalb einer Datenbank Zugriffsrechte erhalten.

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

- Adresse des Servers
- Port
- Zugangsdaten

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

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 kurz und bündig erklärt

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

Zum 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

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. 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.

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 müssen.

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 also im Paket verkauft.

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

Enterprise Server kaufen

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 auch auf Ihrem lokalen Computer installieren, beispielsweise zu Testzwecken. 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, was wir auch empfehlen. Dabei wird der Dienst während der Installation im Hintergrund gleich eingerichtet. Er läuft im Hintergrund immer automatisch mit, startet also automatisch beim Start von Windows. 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-BitArchitektur 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 Super-Administrator 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 17 lautet die Portnummer standardmäßig 25017.

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.

Bitte beachten Sie, dass der Server-Manager über keinen integrierten Update-Manager verfügt. Im Server-Manager wird Ihnen nur angezeigt, ob eine neue Version verfügbar ist. Diese müssen Sie über unsere Website herunterladen und manuell installieren. Das Update kann dabei über die bestehende Installation "drüber" installiert werden. Wenn es sich um kleinere Updates innerhalb der gleichen Hauptversion handelt, muss dabei der Server-Dienst nicht angehalten werden.

Migration

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

Bitte beachten Sie, dass der Enterprise Server und der Windows-Client immer nur in der gleichen Hauptversion miteinander kommunizieren können. So können Sie beispielsweise nicht mit einem Windows-Client der Version 15 auf einen Server der Version 17 zugreifen. Anders verhält es sich mit unseren Editionen für macOS, iOS und Android, die ab Version 15 und höher bis zu einem gewissen Grad abwärtskompatibel sind.

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:

Wie migriere ich den Enterprise Server auf Version 17?

Wir empfehlen, die Anleitung genau zu befolgen. Dann ist die Migration in wenigen Minuten vollzogen.

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

HINWEIS: Bei gespiegelten Servern läuft die Migration genauso ab wie bei nicht gespiegelten. Es spielt keine Rolle, in welcher Reihenfolge Sie Prinzipal und Spiegel upgraden. Sie müssen lediglich die in der Knowledge Base beschriebenen Schritte sowohl für Prinzipal und Spiegel befolgen.

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.

Nutzung auf einem Terminal-Server

Wenngleich wir nicht explizit empfehlen, Password Depot Enterprise Server auf einem Terminal-Server zu betreiben, ist es grundsätzlich möglich.

Hinsichtlich der Installation müssen Sie dabei nichts weiter beachten. Sie läuft auf einem Terminal-Server genauso ab wie auf einem physischen Server. 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. Anderenfalls kann das Browser-Add-On nicht erkennen, von welchem Benutzer eine Anfrage kommt, und ihm möglicherweise Daten zusenden, auf die er eigentlich keinen Zugriff haben soll.

Wie werden den Benutzern individuelle Portnummern zugewiesen?

Hier gibt es zewi Möglichkeiten:

- 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 Terminal-Server)*. So wird jedem einzelnen Client autmatisch eine individuelle Portnummer zugewiesen.
- Gehen Sie alternativ im Server-Manager in den Bereich *Benutzer* und wählen Sie den gewünschen Benutzer aus. Öffnen Sie seine Eigenschaften 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 für jeden Benutzer einen anderen Wert ein.

Die individuellen Portnummern können Benutzer anschließend selbst im Client selbst unter *Bearbeiten* → *Optionen* → *Browser* einsehen. Im Browser müssen die Benutzer die Portnummer entsprechend anpassen, indem sie auf das Add-On-Symbol klicken und unter *Einstellungen* ihre individuelle Portnummer eingeben.

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

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

Server-Manager

Der Server-Manager ist das separate Verwaltungstool des Enterprise Servers. Hierüber findet die zentrale Steuerung des Servers statt. Er erlaubt einen schnellen und unkomplizierten Zugriff auf alle Funktionen des Servers, um ihn zu warten und zu konfigurieren. Um die nachfolgend beschriebenen Funktionen nutzen zu können, müssen Sie sich zunächst einmal mit den Zugangsdaten des Administrators am Server-Manager anmelden.

WARNUNG: Das Administrator-Kennwort sollte grundsätzlich nur dem Administrator 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
- Benutzer
- Gruppen
- Benachrichtigungen
- Protokoll

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 (d.h. die 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, können Sie hier nachlesen, welchen Workaround es gibt:

Wie kann ich das Administrator-Kennwort im Password Depot-Server "zurücksetzen"?

Verwalten

Das Menü *Verwalten* befindet sich oben rechts im Server-Manager. Es beinhaltet folgende Funktionen:

- Serveroptionen: Hier können grundlegende Einstellungen am Server vorgenommen werden.
- 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.
- Client-Sicherheitsrichtlinien: Diese kommen bei Verwendung des Corporate Client zum Einsatz. In diesem Fall können Sie als Admin Ihren Benutzern umfassende, verbindliche Richtlinien mitgeben, 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 für den Server-Manager
- Beenden: Beendet den Server-Manager. Der Dienst oder die Server-Anwendung sind davon nicht betroffen.

HINWEIS: Bei manchen Änderungen am Enterprise Server kann ein Neustart des Servers erforderlich sein, damit die Änderungen greifen. Mit Version 15 wurde ein entsprechender Befehl zum Neustarten des Servers implementiert. Dieser erscheint von Seiten des Programms automatisch, sollte ein Neustart des Servers erforderlich sein. Wenn der Password Depot Enterprise Server diesen vorschlägt, empfehlen wir, ihn sogleich durchzuführen.

Serveroptionen

Die Serveroptionen finden Sie im Menü *Verwalten*. Folgende Registerkarten stehen Ihnen hier zur Verfügung:

- Allgemein
- Verbindungen
- Protokollierung
- Sicherungsdateien
- Erweitert
- E-Mail
- 2FA-Einstellungen
- Active Directory
- Azure AD

Allgemein

Server

- Sprache des Servers: Legt die Sprache des Servers (nicht der Benutzeroberfläche!) fest. Sie können hier zwischen Deutsch und Englisch wählen.
- Server-Port: Legt den Port für die Verbindung fest. Wenn Sie den Port anpassen, achten Sie darauf, dass anschließend auch im Client der korrekte Port für die Verbindung zum Server angegeben wird.
- Internet-Protokoll: Sie können ein bestimmtes Internet-Protokoll festlegen, das standardmäßig für die Verbindung zum Server verwendet werden soll. Sie können hier zwischen *IPv4 + IPv6*, *IPv4* oder *IPv6* wählen. Der Server meldet den Clients per UDP, welches Protokoll verwendet wird, sodass die Clients automatisch das Richtige wählen.
- **SSL/TLS verwenden:** Erlaubt die Nutzung einer SSL/TLS-Verbindung zwischen Server und Client. Klicken Sie auf *Zertifikat installieren*, um das entsprechende Zertifikat am Server zu hinterlegen.
- Keep-Alive aktivieren: Die Keep-Alive-Funktion 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.
- Portnummer: Geben Sie die Portnummer für die Verbindung zwischen Web-Client und Server ein.
- **SSL/TLS für REST-Server verwenden:** Aktivieren Sie die Nutzung einer SSL/TLSVerbindung bei der REST-Server-Verbindung.

Datenbanken

Hier können Sie den Speicherort sehen und bearbeiten, an dem Password Depot Enterprise Server standardmäßig seine Datenbanken ablegt.

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 erlauben.

TIPP: Ausführliche Informationen zur Integrierten Windows-Authentifizierung 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

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 in Zusammenhang mit den mobilen Apps eingeführt, da es vorkommen kann, dass ein Nutzer sowohl von seinem PC als auch von seinem Smartphone auf eine Datenbank zugreifen muss. Das funktioniert, weil mobile Geräte nicht in Echtzeit synchronisiert werden. Wenn ein Nutzer allerdings von zwei Windows-Clients gleichzeitig auf den Server zugreifen möchte, kann das zu Problemen führen.

Inaktive Sitzungen

Hier können Sie festlegen, ob ein inaktiver Client automatisch getrennt werden soll und wenn ja, wann. Außerdem können Sie entscheiden, ob dabei die Datenbank geschlossen und der Client vom Server abgemeldet wird.

Protokollierung

Lokales Protokoll:

Hier können sie festlegen, in welchem Verzeichnis das Protokoll gespeichert werden soll, wie groß die Datei maximal sein darf, ob Sie immer dieselbe Protokolldatei benutzen oder ob und wann Sie neue Dateien erstellen, und ob Sie alte Protokolle löschen.

Remote-Protokoll

Hier können Sie, wenn gewünscht, einstellen, dass Password Depot Enterprise Server Protokolle an einen externen Server sendet. Geben Sie dafür das Übertragungsprotokoll, die Adresse des Remote-Servers und das Format des Server-Protokolls an.

Sicherungsdateien

- Sicherungsordner: Hier können Sie sehen und ändern, in welchem Verzeichnis die Sicherungsdateien gespeichert werden.
- Datenbanken bei jedem Programmstart sichern
- Datenbanken sichern alle: Hier können Sie einstellen, in welchen Intervallen Password Depot Enterprise automatisch Sicherungskopien erstellt.
- Sicherungsdateien löschen, die älter sind als: Hier können Sie festlegen, dass veraltete Sicherungsdateien automatisch gelöscht werden, um unnötigen Ballast zu vermeiden.
- Protokolle sichern in Datei: Hier können Sie den Namen der Protokolldatei sehen und ändern.

Erweitert

Einträge bearbeiten

Hier können Sie einstellen, wieviel Zeit Nutzer haben, bis ein Eintrag, der bearbeitet wird, gesperrt wird.

Private Datenbanken

Hier können Sie festlegen, ob für neue Nutzer automatisch private Datenbanken angelegt werden und ob diese Datenbanken automatisch gelöscht werden, wenn der entsprechende Nutzer gelöscht wird.

WebSockets-Port für Clients

Stellen sie hier ein, ob alle Clients die Standard-Portnummer verwenden sollen und wenn ja, wie diese lautet, oder ob für jeden Client eine individuelle Portnummer für die Kommunikation zwischen Client und Browser-Add-On verwendet werden soll.

Fehlgeschlagene Anmeldungen

Legen Sie fest, wie viele Anmeldeversuche ein Nutzer hat, bevor er am Server gesperrt wird. Bitte beachten Sie, dass fehlgeschlagene Anmeldeversuche nicht nach einer bestimmten Zeit zurückgesetzt werden, sondern nach einer erfolgreichen Anmeldung.

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

Auf dieser Registerkarte können Sie einstellen, ob Sie für Ihren Server eine Zwei-Faktor-Authentifizierung aktivieren möchten. Sie wird sowohl bei der Anmeldung mit Benutzernamen und Kennwort als auch bei der Integrierten Windows-Authentifizierung unterstützt. Wenn Sie sie für einzelne Benutzer deaktivieren möchten, können Sie das in den Eigenschaften des jeweiligen Benutzers tun.

Betriebsart

Legen Sie hier fest, ob die Codes, die für die Zwei-Faktor-Authentifizierung verwendet werden, über eine mobile Authenticator-App generiert oder per E-Mail an die Benutzer gesendet werden. Außerdem können Sie einstellen, ob und wie lange die Geräte der Benutzer gemerkt werden sollen, sodass in dieser Zeit kein neuer Code eingegeben werden muss, und wie lange die gesendeten Codes gültig sind.

Besuchen Sie auch unsere Knowledge Base für mehr Informationen zur Zwei-Faktor-Authentifizierung:

Was ist die Zwei-Faktor-Authentifizierung (2FA) in Password Depot und wie stelle ich diese ein?

Active Directory

Hier können Sie einstellen, ob und in welchen Intervallen eine automatische Active Directory-Synchronisation stattfindet, und wie mit Benutzern und Gruppen verfahren werden soll, die bei der Synchronisation nicht in Active Directory gefunden wurden. Hier haben Sie die Wahl, ob sie ignoriert, deaktiviert oder vom Server gelöscht werden sollen.

Azure AD

Mandanten

Verwalten Sie hier die Organisationen auf dem Enterprise Server. Sie können eine neue Organisation hinzufügen, indem Sie auf *Neu* klicken, einen Microsoft-Account wählen, sich als Admin anmelden und anschließend über *Extras → Azure AD-Synchronisation* eine Synchronisation durchführen. Außerdem können Sie bestehende Organisationen aktualisieren oder Löschen.

Weitere Informationen finden Sie im Kapitel Azure AD-Synchronisation.

Synchronisation

Legen Sie hier fest, ob und in welchen Intervallen eine automatische Azure AD-Synchronisation durchgeführt wird, und wie mit Benutzern und Gruppen verfahren werden soll, die bei der Synchronisation nicht gefunden wurden. Sie haben die Wahl, ob sie ignoriert, deaktiviert oder vom Server gelöscht werden sollen.

Server-Lizenz

Im Menü *Verwalten* → *Server-Lizenz* können Sie neue Lizenzen hinzufügen sowie 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 erhöhen.

Mehr Informationen zur Lizenzierung des Enterprise Server finden Sie hier.

Serverrichtlinien

Die Serverrichtlinien finden Sie im Menü *Verwalten*. Hier können Sie einige globale Einstellungen vornehmen, die die Rechtevergabe an die Benutzer, die Sicherheit der Kennwörter und die unterstützten Einträge betreffen.

HINWEIS: Auf allen Registerkarten können die Einstellungen über die Schaltfläche *Einstellungen wiederherstellen* auf die Standardeinstellungen zurücksetzen.

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 die entsprechende Berechtigung für jede Datenbank und für jeden Benutzer im Einzelnen nachträglich 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): Die entsprechende Berechtigung ist allen Benutzern für alle Datenbanken auf dem Server verwehrt. Der Status kann nachträglich nicht mehr geändert ewrden.

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, sodass Sie im weiteren Verlauf auf Datenbank-Ebene oder auch für einzelne Ordner oder Einträge Änderungen vornehmen können.

Da Berechtigungen, die an dieser Stelle auf *Deaktiviert* gesetzt werden, nachträglich Datenbank- oder Ordner-Ebene nicht mehr erteilt werden können, empfehlen wir, nur solche Berechtigungen zu deaktivieren, von denen Sie sicher sind, dass Sie sie nicht erlauben möchten.

Sicherheit

In dieser Registerkarte können Sie bestimmte Kennwortrichtlinien für die Clients definieren. So können Sie festlegen, dass Kennwörter auf Sicherheit gegenüber Wörterbuchangriffen geprüft werden. Außerdem können Sie Regeln bezüglich Mindestlänge und Zusammensetzung neuer oder bearbeiteter Kennwörter definieren. Bitte beachten Sie, dass diese Richtlinien nur für Kennwörter verbindlich sind, die von Password Depot generiert werden.

Zudem können Sie bestimmen, dass berechtigte Benutzer ein zweites Passwort festlegen müssen.

Einträge

Hier können Sie festlegen, welche Eintragstypen Benutzer anlegen dürfen. Zur Verfügung stehen:

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

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. Doppelklicken Sie auf eine Richtlinie, um sie zu bearbeiten.

HINWEIS: Die Client-Sicherheitsrichtlinien greifen nur in der Corporate Edition des Windows-Clients. In der Standardversion des Windows-Clients, die ebenfalls im Download-Bereich zur Verfügung steht, werden diese Richtlinien nicht unterstützt.

Kennwortrichtlinien

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. Folgende Optionen haben Sie:

- Kennwort muss den Komplexitätsanforderungen entsprechen: Legen Sie hier fest, ob generierte Kennwörter die hier von Ihnen definierten Zeichen enthalten müssen.
- Kennwortlänge mindestens
- Kennwortverlauf erzwingen: Hier können Sie einstellen, wie viele eindeutig neuen Kennwörter verwendet werden müssen, bevor ein altes wiederverwendet werden kann.
- Maximales Alter für Kennwörter: Bestimmt, wie lange ein Kennwort verwendet werden kann, bevor der Benutzer aufgefordert wird, es zu ändern.
- Mindestalter für Kennwörter: Legt fest, wie lange ein Kennwort verwendet werden muss, bevor es geändert werden darf.

Richtlinien für erlaubte Speicherorte

Hier können Sie festlegen, welche Speicherorte die Clients neben dem Enterprise Server verwenden dürfen. Sie haben folgende Auswahl:

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

Richtlinien für Aktionen

Hier können Sie festlegen, ob die folgenden Aktionen grundsätzlich erlaubt sind:

- 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
- Automatische Reinigung der Zwischenablage
- Automatischer Update-Modus
- Datenbank nach jeder Änderung automatisch speichern
- 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
- Kennwörter in der Listenansicht anzeigen
- Liste zuletzt verwendeter Datenbanken speichern
- Lokale Kopie beim Schließen der Remote-Datei automatisch löschen
- Lokale Kopie der Dateien von Password Depot Enterprise Server speichern
- Nach Updates suchen (Tage): Wenn Sie festgelegt haben, dass die Password Depot-Clients automatisch nach Updates suchen, können Sie hier einstellen, in welchen Abständen das geschehen soll.
- Sicherungskopie beim Speichern einer Datenbank erzeugen
- Sicherungskopie beim Öffnen einer Datenbank erzeugen
- Standard-Authentifizierungsmodus
- Standard-Gültigkeitsdauer für Kennwörter
- Zuletzt verwendete Kennwörterdatei beim Programmstart laden
- Änderungen der Zwischenablage vor externen Viewern verbergen

HINWEIS: Die Einstellungen der Client-Sicherheitsrichtlinien werden immer auf den gesamten Server und alle Benutzer angewendet. Sie können nachträglich auf Benutzer- oder Datenbank-Ebene nicht geändert werden. Über die Schaltfläche *Einstellungen wiederherstellen* können Sie die Client-Sicherheitsrichtlinien wieder auf die Standard-Einstellungen zurücksetzen.

Serverspiegelung

Die Serverspiegelung finden Sie im 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.

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

Sie benötigen zwei Maschinen, auf denen Password Depot Enterprise Server läuft. Einer der beiden Server ist der Haupt-Server bzw. *Prinzipal*, der wie gewohnt läuft. Mit ihm verbinden sich die Benutzer, um Datenbanken zu empfangen und benutzen. Die andere Maschine wird als gespiegelter Server genutzt. Benutzer können sich zwar auch mit ihm verbinden, ihn aber ausschließlich im Lese-Modus benutzen. Der Haupt-Server synchronisiert Ihre Daten im Hintergrund in Echtzeit auf den gespiegelten Server. Wenn der Haupt-Server einmal ausfällt, können Administratoren den gespiegelten Server als neuen Haupt-Server einstellen, sodass Benutzer weiterhin Zugriff auf ihre Daten haben.

Um die Serverspiegelung einzurichten, wählen Sie für Ihre Server eine Serverrolle aus: *Keine Spiegelung*, wenn sie grundsätzlich keine Spiegelung wünschen, *Prinzipal*, wenn der Server, mit dem Sie gerade verbunden sind, der Haupt-Server sein soll, oder *Spiegel*, wenn der aktuelle Server der gespiegelte Server sein soll. Geben Sie jeweils die Netzwerk-Adresse des primären bzw. gespiegelten Servers sowie den Port für die Verbindung ein. Im Feld *Status* können Sie den Stand der eingerichteten Serverspiegelung überblicken.

Programmoptionen

Die Programmoptionen finden Sie im Menü *Verwalten*. Sie beziehen sich ausschließlich auf den Server-Manager. Folgendes können Sie über die Programmoptionen festlegen:

- Sprache der Anwendungen: Sie können zwischen Englisch und Deutsch als Anzeigesprache für die Benutzeroberfläche 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.

Extras

Das Menü *Extras* befindet sich oben rechts im Server-Manager. Hier haben Sie die folgenden Optionen:

- Systemprotokoll: Hier können Sie sich ein Systemprotokoll 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.
- Active Directory-Synchronisierung
- Azure AD-Synchronisierung
- Datenbank-Bericht
- Benutzer-Bericht
- Gruppen-Bericht
- Serverzertifikat erstellen

Auf die Active Directory-Synchronisierung, die Azure AD-Synchronisierung sowie die Berichte werden die folgenden Kapitel näher eingehen.

Active Directory-Synchronisation

Im Menü *Extras* können Sie über die Option *Active Directory-Synchronisation* den Synchronisationsassistenten starten. 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 seine Windows NT- bzw. Active Directory-Zugangsdaten.

HINWEIS: Mit Version 14 wurde der WinNT-Provide durch einen leistungsfähigeren LDAP-Provider ersetzt.

Auf der Startseite des Assistenten müssen Sie zunächst einige 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 Benutzer anmelden möchten, mit dem Sie sich zuvor an Windows angemeldet haben.
- Diese Konto verwenden: Geben Sie hier den Benutzernamen und das Kennwort eines anderen Benutzers ein, der ebenfalls die Berechtigung besitzt, Daten aus Active Directory der zuvor gewählten Domäne auszulesen.

Bitte beachten Sie, dass der Password Depot Server standardmäßig das SYSTEM-Konto des Rechners verwendet, auf dem der Server läuft. Stellen Sie daher bitte sicher, dass das Konto, das zur AD-Synchronisation verwendet wird, vollen Lesezugriff auf AD Ihrer Domäne hat.

Zusätzliche Informationen

- 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 scannt der Assistent das gesamte Active Directory-Verzeichnis. Dies kann in manchen Fällen sehr viel Zeit in Anspruch nehmen. Die Option sollte daher nur bei der ersten Synchronisierung 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.
- Gelöschte Objekte überprüfen: Mit dieser Option werden gelöschte Objekte, zum Beispiel Benutzer oder Gruppen, in Active Directory und Password Depot Enterprise Server miteinander abgeglichen.

- SSL verwenden: Diese Option sollten Sie anhaken, wenn 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 und klicken Sie abschließend auf *Synchronisieren*. Die Ergebnisse der Synchronisierung werden Ihnen im nächsten Fenster angezeigt.

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, damit die Anmeldung erfolgen kann.

Azure AD-Synchronisation

Im Menü *Extras* können Sie über die Option *Azure AD-Synchronisation* den Synchronisationsassistenten starten. Sie ist notwendig, wenn Sie möchten, dass die Benutzer sich mit ihren Microsoft-Zugangsdaten am Enterprise Server anmelden können.

Organisation

Wählen Sie eine Organisation aus, aus der Sie Azure AD-Benutzer importieren, oder fügen Sie über *Neu* eine neue Organisation hinzu. Wählen Sie einen Microsoft-Account aus, der als Organisation hinterlegt werden soll. Bitte beachten Sie, dass für die Anmeldung einer Organisation nur das Benutzerkonto des Administrators verwendet werden kann.

Geben Sie den Admin-Benutzernamen, das Admin-Kennwort und den zweiten Faktor aus Ihrer Authenticator-App ein. Die 2-Faktor-Authentifizierung ist an dieser Stelle unumgänglich, da Sie Teil der Microsoft-Sicherheitsrichtlinien sind. 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, und klicken Sie auf *Synchronisieren*. Anschließend werden Ihnen die Ergebnisse der Synchronisierung angezeigt.

Zusätzliche Optionen

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

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

Berichte

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

- Datenbanken-Bericht
- Benutzer-Bericht
- Gruppe-Bericht

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 benötigen. Im Folgenden wird kurz erläutert, wie die einzelnen Berichte zu verstehen sind.

Datenbank-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 der Benutzer und Gruppen auf Datenbank-Ebene.

Benutzer-Bericht

Unter *Benutzer-Bericht* wird ein Bericht erstellt, der Ihnen zu den ausgewählten Benutzerkonten folgende Informationen anzeigt:

- Konto: Zeigt den Benutzernamen an.
- Typ: Zeigt an, ob ein Benutzer ein normaler Server-Benutzer ist oder eine zusätzliche Serverrolle besitzt.
- Vollständiger Name
- E-Mail
- Deaktiviert
- Zugeordnete Datenbanken
- Zugriffsrechte: Zeigt die Zugriffsrechte auf die jeweiligen Datenbanken in Kurzform an.

Gruppen-Bericht

Unter *Gruppen-Bericht* wird ein Bericht erstellt, der Ihnen zu den augewählten Gruppen folgende Informationen anzeigt:

- Konto: Zeigt den Namen der Gruppe an.
- Typ: Zeigt an, ob es sich um eine Standard-Gruppe, eine Active Directory-Gruppe oder eine Azure AD-Gruppe handelt.
- Beschreibung
- E-Mail
- Deaktiviert
- Zugeordnete Datenbanken
- Zugriffsrechte: Zeigt die Zugriffsrechte auf die jeweiligen Datenbanken in Kurzform an.

SSL-Zertifikat

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

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

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

- 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. In den lokalen und internen Netzwerken wird die Verwendung von SSL nicht empfohlen, da jegliche Datenübertragung zwischen dem S Clients bereits stark verschlüsselt ist. Die Verwendung von SSL ermöglicht die Validierung des Servers und hilft, Mar in-the-Middle-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.
- 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.
- Die Verwendung von selbstsignierten Zertifikaten wird nicht unterstützt. Sie können sich zwar zu Testzwecken ein Dummy-Zertifikat erstellen lassen, aber da es leicht von Dritten zu fälschen ist, ist es ansonsten nutzlos. 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.
- Wenn Sie sich für eine SSL-Verbindung entscheiden, stellen Sie bitte sicher, dass alle Ihre Clients SSL verwenden! Gemischte Verbindungen, d.h. teilweise SSL und teilweise Standard-TCP/IP, sind nicht erlaubt.

Um ein SSL-Zertifikat zu erstellen, gehen Sie wie folgt vor:

- Geben Sie den Pfad zur Zertifikatsdatei auf dem Server an.
- Wenn Sie eine separate private Schlüsseldatei verwenden, geben Sie ihren Pfad im Feld darunter ein. Wenn die Zertifikatsdatei bereits den privaten Schlüssel enthält, lassen Sie das Feld leer.
- Geben Sie das Kennwort für den Zugriff auf den privaten Schlüssel ein.
- Starten Sie den Server neu, um das Zertifikat zu laden und SSL-Verbindungen zu starten.

Serverzertifikat erstellen

Seit Version 16.0.6 bietet Enterprise Server einen Assistenten zum Erstellen von selbstsignierten Serverzertifikaten. Dazu ist ein gültiges Stammzertifikat der Zertifizierungsstelle (CA) erforderlich. Öffnen Sie den Installationsassistenten über *Extras → Serverzertifikat erstellen*. Hier haben Sie folgende Möglichkeiten:

- Ein selbstsigniertes Stammzertifikat erstellen
- Ein bestehendes Stammzertifikat verwenden (empfohlen)

Ein selbstsigniertes Stammzertifikat erstellen

Um zu Testzwecken ein selbstsigniertes Zertifikat zu erstellen, geben Sie alle erforderlichen Informationen für das Root-CA-Zertifikat ein. Klicken Sie auf *Weiter*. Geben Sie nun die erforderlichen Informationen zum Serverzertifikat ein und klicken Sie erneut auf *Weiter*. Geben Sie danach die Domänennamen und IP-Adressen, die der Server-Computer verwendet. Klicken Sie anschließend auf *Generieren*, um das Zertifikat zu erstellen.

Ein bestehendes Stammzertifikat verwenden

Um ein bestehendes Zertifikat zu verwenden, geben Sie die Dateipfade zu der öffentlichen und der privaten Schlüsseldatei auf dem Server sowie das Kennwort an und klicken Sie auf *Weiter*. Im daraufhin angezeigten Dialogfeld Eigenschaften des Serverzertifikats geben Sie die erforderlichen Eigenschaften für das Serverzertifikat ein. Klicken Sie anschließend auf *Weiter*. Danach geben Sie im Dialogfeld *Domänennamen und IP-Adressen* die vom Servercomputer verwendeten Domänennamen und IP-Adressen an. Klicken Sie dann auf *Generieren*, um das Zertifikat zu generieren.

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 Datenbank

In der Listenansicht des Bereichs *Datenbanken* erhalten Sie einen Überblick über alle vorhandenen Server-Datenbanken, ihre Größe, über das letzte Änderungsdatum und die Gesamtanzahl der Datenbankeinträge. Unter *Verbindungen* sehen Sie, wie viele Benutzer aktuell mit einer Datenbank Sie mit sehr vielen einzelnen Datenbanken arbeiten, können Sie im oberen Bereich der Hauptansicht einen Filter verwenden, um die Anzeige einzugrenzen.

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

- Neue Datenbank
- Berechtigungen
- Eigenschaften
- Löschen
- Umbenennen
- Alle auswählen

Datenbank dem Server hinzufügen

Dieses Dialogfenster erreichen Sie, indem Sie im Bereich Datenbanken auf *Neue Datenbank* klicken. 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. Klicken Sie dazu auf die Schaltfläche *Durchsuchen*, um die gewünschte Datenbank auszuwählen. Geben Sie das aktuelle Master-Kennwort dieser Datenbank ein. Über das Augen-Symbol können Sie es im Klartext anzeigen oder verbergen. Klicken Sie zum Abschluss auf *OK.*

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. Die Clients verwenden zum Öffnen der Server-Datenbanken jedoch immer ihre vom Administrator zugewiesenen Zugangsdaten.

Berechtigungen

Dieses Dialogfenster erreichen Sie, indem Sie im Bereich Datenbanken auf *Berechtigungen* klicken.

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.

Über die Schaltfläche *Löschen* können Sie Benutzern und Gruppen den Zugriff auf die ausgewählte Datenbank wieder entziehen. Sie können dann nicht mehr auf die Datenbank zugreifen, sind allerdings noch am Server verfügbar. Über *Alle auswählen* können Sie alle Benutzer/Gruppen, die auf die ausgewählte Datenbank zugreifen können, gleichzeitig markieren.

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. Auf der rechten Seite können Sie die Berechtigungen der neuen Benutzer/Gruppen festlegen. Dies können Sie in den jeweiligen Registerkarten auf Datenbank-, Ordner- oder Eintragsebene tun. Klicken Sie abschließend auf *OK*.

Eigenschaften

Markieren Sie einen Nutzer/eine Gruppe und öffnen Sie per Doppelklick oder über die Schaltfläche rechts die Eigenschaften. Hier sehen Sie folgende Registerkarten:

Datenbank

In der Registerkarte Datenbank werden Rechte für die gesamte Datenbank vergeben. Sie sehen hier oben links den ausgewählten Benutzer bzw. die ausgewählte Gruppe. Der Zugriff auf die Datenbank kann, wenn gewünscht, über *Gültig ab* und *Gültig bis* zeitlich begrenzt werden. Auf der rechten Seite sehen Sie die Berechtigungen des ausgeählten Benutzers/der ausgewählten Gruppe. Folgende Berechtigungen können Sie hier erteilen:

- 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
- Synchronisieren der Datenbank
- Anderen Benutzern Zugriff gewähren
- Einträge versiegeln
- Zweites Kennwort setzen
- Admin-Rechte gewähren

Unter *Effektive Berechtigungen anzeigen* können Sie die effektiven Berechtigungen eines Benutzers oder einer Gruppe gesondert ansehen.

HINWEIS: Die Rechte, die Sie hier erlauben, gelten für die gesamte Datenbank. Wie auch bei den Serverrichtlinien können Sie hier aktivierte oder nicht definierte Berechtigungen auf Eintrags- oder Ordner-Ebene bearbeiten, deaktivierte Berechtigungen dagegen nicht.

Einträge und Ordner

In dieser Registerkarte können Sie Benutzern/Gruppen Rechte auf einzelne Ordner und/oder Einträge innerhalb der Datenbank zuweisen. Wählen Sie dazu links einzelne Ordner oder Einträge aus. Auf der rechten Seite können Sie folgende Berechtigungen erteilen:

- Zugriff auf Einträge
- Lesen von Einträgen
- Ändern von Einträgen
- Hinzufügen von Einträgen
- Einträge löschen
- Anderen Benutzern Zugriff gewähren
- Einträge versiegeln
- Zweites Kennwort setzen

Auch hier können Sie sich die *effektiven Berechtigungen anzeigen* lassen.

TIPP: Sowohl auf der Registerkarte *Datenbank* als auch auf der Registerkarte *Einträge und Ordner* werden alle erlaubten Berechtigungen grün und alle deaktivierten Berechtigungen rot markiert. Berechtigungen, die von den globalen Richtlinien abweichen, werden dabei fett markiert.

Einträge versiegeln

Wenn ein Benutzer einem anderen Benutzer Zugriff auf einen Eintrag gewährt, hat er zusätzlich die Möglichkeit, diesen Eintrag zu versiegeln. Dadurch hat der andere Nutzer erst Zugriff auf diesen Eintrag, wenn er sich von einer autorisierten Person die Erlaubnis dafür eingeholt hat.

Diese autorisierte Person wird von dem Benutzer, der den Eintrag teilt, ausgewählt. Dabei muss es sich um jemanden handeln, der Admin-Rechte am Enterprise Server hat. Dieser autorisierte Benutzer kann im Bereich *Datenbanken → Berechtigungen* sehen, dass dem neuen Benutzer Zugriff auf einen Eintrag gewährt wurde, wie lange der Zugriff gültig ist und ob der Eintrag versiegelt wurde. Über *Eigenschaften → Versiegelter Zugang* kann der Siegelstatus geändert werden. Zur Verfügung stehen folgende Status:

- Versiegelt: Wenn der Eintrag versiegelt ist, wurde noch nicht versucht, auf ihn zurückzugreifen.
- Unversiegelt: Die Versiegelung wurde aufgehoben.
- Warten auf Genehmigung: Der Nutzer, dem der Zugriff gewährt wurde, hat versucht, den Eintrag zu öffnen und wartet nun auf die Genehmigung.
- Genehmigung erteilt: Eine autorisierte Person hat die Genehmigung gewährt. Der neue Benutzer kann auf den Eintrag zugreifen.
- Gebrochen: Wenn das Siegel gebrochen ist, wurde auf den Eintrag zugegriffen.

Autorisierte Personen können den Status jederzeit ändern. Außerdem können sie über *Hinzufügen* weitere autorisierte Personen hinzufügen, die den Status eines Siegels ebenfalls bearbeiten können.

Weitere Informationen zu versiegelten Einträgen finden Sie in unserer Knowledge Base: Wie kann ich anderen Benutzern in Password Depot Zugriff gewähren und Einträge versiegeln?

Eigenschaften

Dieses Dialogfenster erreichen Sie, indem Sie im Bereich Datenbanken auf *Eigenschaften* klicken.

Hier sehen Sie folgende Registerkarten:

- Allgemein
- Erweitert

Allgemein

Hier können Sie den Namen der Datenbank bearbeiten. Außerdem sehen Sie den Dateitypen, die Größe, den Zeitpunkt der letzten Änderung und eine Liste der Nutzer, die gerade mit dieser Datenbank verbunden sind. Über die Schaltfläche *Aktualisieren* können Sie die Ansicht aktualisieren. Über *Trennen* können Sie ausgewählte Nutzer von der Datenbank trennen.

Erweitert

Hier können Sie für die Verschlüsselung der Datenbank ein benutzerdefiniertes Kennwort festlegen, alle Zugriffe von Benutzern auf Einträge protokollieren lassen und einstellen, dass Benutzer für die Löschung von Einträgen einen Grund angeben müssen.

Das Kennwort der Datenbank dient ihrer Verschlüsselung. Standardmäßig wird eine Datenbank mit dem Admin-Kennwort verschlüsselt. Über *Einstellungen ändern* können Sie allerdings ein eigenes Kennwort festlegen, was hilfreich sein kann, wenn Administratoren nicht grundsätzlich auf alle Datenbanken am Server zugreifen sollen.

Im Dialogfenster *Datenbankverschlüsselung ändern* wählen Sie die Option *Benutzerdefiniertes Kennwort (Berechtigungsverwaltung erfordert Verifizierung)*. Geben Sie ein neues Kennwort ein und wiederholen sie es. Klicken Sie zum Abschluss auf *OK.* 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.

Um das benutzerdefinierte Kennwort zu ändern, gehen Sie auf *Einstellungen ändern* und geben Sie erst das aktuelle, dann das neue Kennwort ein. Wiederholen Sie das neue Password und klicken Sie zum Abschluss auf *OK*. Wenn Sie das benutzerdefinierte Kennwort entfernen möchten, gehen Sie auf *Einstellungen ändern* und wählen Sie *Administrator-Kennwort (Automatischer Zugriff auf die Berechtigungsverwaltung)* aus. Geben Sie das aktuelle Kennwort ein und klicken Sie zum Abschluss auf *OK*. Dadurch wird das Administrator- Kennwort wieder zum Kennwort zur Verschlüsselung, sodass zur Verwaltung der Datenbank kein weiteres Kennwort mehr nötig ist.

WARNUNG: Diese Funktion sollte mit äußerster Vorsicht genutzt werden! Bitte nutzen Sie sie nur, wenn es zwingend erforderlich ist. Es besteht keine Möglichkeit, ein solches benutzerdefiniertes Kennwort für Datenbanken zurückzusetzen oder wiederherzustellen, sollte es vergessen werden. In diesem Fall wäre die Verwaltung der Datenbank nicht mehr möglich.

Benutzer

Der Bereich Benutzer ermöglicht dem Administrator, neue Benutzer hinzuzufügen und bestehende zu verwalten.

In der Hauptansicht ewrden Ihnen folgende Spalten angezeigt:

- Konto: Zeigt den Benutzernamen an.
- Authentifizierung
- Benutzerprinzipalname: Zeigt den Benutzerprinzipalnamen von Nutzern an, die dem Server über Active Directory oder Azure AD hinzugefügt wurden.
- Status: Zeigt an, ob der Benutzer deaktiviert, aktiviert oder verbunden ist.
- Rollen: Zeigt an, ob der Benutzer zusätzliche Serverrollen innehat.
- Adresse: Zeigt die IP-Adresse des Benutzers an, wenn er mit dem Server verbunden ist.
- Vollständiger Name
- E-Mail
- Abteilung
- Geöffnete Datenbank

Auf der rechten Seite stehen Ihnen folgende Optionen zur Verfügung:

- Neuer Benutzer
- Eigenschaften
- Löschen
- Trennen: Trennt den Benutzer vom Server.
- Synchronisieren: Erlaubt die Synchronisierung einzelner Benutzer mit Active Directory bzw. Azure AD.
- Datenbank zuweisen
- 2FA zurücksetzen: Ermöglicht dem Administrator bei Nutzung der Zwei-Faktor-Authentifizierung am Server, für einzelne Benutzer die 2FA zurückzusetzen, sodass sie bei der nächsten Anmeldung am Server erneut den zweiten Faktor eingeben müssen.
- Alle auswählen

Benutzer hinzufügen

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

- Über die Schaltfläche *Neuer Benutzer*
- Per Active Directory-Synchronisation
- Per Azure AD-Synchronisation

Neue Benutzer manuell anlegen

Im Bereich *Benutzer* können Sie über die Schaltfläche *Neuer Benutzer* manuell neue, lokale Benutzer hinzufügen. Solche Benutzer melden sich mit Benutzernamen und Kennwort am Server an. Wählen Sie dazu beim Anlegen des Benutzers in der Registerkarte *Konto* die Option *Password Depot-Zugangsdaten* aus und legen Sie einen Benutzernamen und ein Kennwort fest.

Außerdem können Sie beim Anlegen eines neuen Nutzers gleich seine Eigenschaften definieren.

Neue Benutzer per Active Directory-Synchronisation hinzufügen

Wenn Sie möchten, dass Ihre Benutzer sich über die Integrierte Windows-Authentifizierung (SSO) am Server anmelden können, müssen Sie sie über *Extras → Active Directory-Synchronisation* hinzufügen. Dadurch werden Benutzer von Active Directory importiert.

Auf der Registerkarte *Eigenschaften → Konto* wird bei solchen Benutzern automatisch *Active Directory Domain Services* als Authentifizierung ausgewählt. Im Client wählen Benutzer, die per Active Directory-Synchronisation hinzugefügt wurden, für die Anmeldung am Server *Integrierte Windows-Authentifizierung* aus.

Mehr zur Active Directory-Synchronisation erfahren Sie hier.

Neue Benutzer per Azure AD-Synchronisation hinzufügen

Wenn Sie möchten, dass Ihre Benutzer sich über Azure AD am Server anmelden können, müssen Sie sie über *Extras → Azure AD-Synchronisation* hinzufügen. Dadurch werden Benutzer von Azure AD importiert.

Auf der Registerkarte *Eigenschaften → Konto* wird bei solchen Benutzern automatisch *Azure Active Directory* als Authentifizierung ausgewählt. Im Client wählen Benutzer, die per Active Directory-Synchronisation hinzugeügt wurden, für die Anmeldung am Server entsprechend *Azure AD-Authentifizierung* aus.

Mehr zur Azure AD-Synchronisation erfahren Sie hier.

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.

Benutzereigenschaften

Die Eigenschaften eines Benutzers können Sie im Bereich *Benutzer* aufrufen, indem Sie auf einen Benutzer doppelklicken oder ihn markieren und rechts auf die Schaltfläche *Eigenschaften* klicken.

Folgende Registerkarten stehen Ihnen in den Eigenschaften zur Verfügung:

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

Allgemein

In der Registerkarte *Allgemein* sind folgende Angaben möglich:

- Vollständiger Name
- E-Mail
- Telefon
- Abteilung
- Beschreibung

Konto

Authentifizierung

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

- Password Depot-Zugangsdaten
- Active Directory Domain Services
- 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, erfahren Sie hier:

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). Um sie zu nutzen, muss vorher eine Active Directory-Synchronisation durchgeführt werden. Mehr Informationen dazu finden Sie hier.

Bei der Option *Azure Active Directory* melden sich Ihre Benutzer mit ihren Microsoft-Zugangsdaten am Server an. Dafür ist vorab eine Azure AD-Synchronisation notwendig. Mehr Informationen dazu finden Sie hier.

Konto-Optionen

- Konto deaktiviert: Wenn ein Benutzer aufgrund zu vieler fehlgeschlagener Anmeldeversuche gesperrt ist, ist hier ein Häkchen gesetzt. Entfernen Sie es, um den Benutzer zu entsperren.
- **Benutzer darf Kennwort nicht ändern:** Wählen Sie diese Option, wenn ein lokaler Benutzer sein Kennwort nicht ändern können soll. Beachten Sie, dass diese Option nur bei einer Anmeldung mit Nutzernamen und Kennwort sinnvoll ist.
- Benutzer muss Kennwort bei der nächsten Anmeldung ändern: Wählen Sie diese Option, wenn Sie eine Kennwortänderung für einen lokalen Benutzer erzwingen möchten. Bitte beachten Sie, dass diese Option nur bei der Anmeldung mit Nutzernamen und Kennwort sinnvoll ist.
- **2-Faktor-Authentifizierung deaktiviert:** Deaktiviert die Zwei-Faktor-Authentifizierung für diesen einen Benutzer.

Rollen

Mit Version 15 wurde ein rollenbasiertes Server-Modell eingeführt, um die Verwaltung des Servers grundsätzlich auch auf mehrere verschiedene Personen aufteilen zu können. Folgende Server-Rollen stehen Ihnen hier zur Auswahl:

- Server-Administrator: Ein Server-Administrator hat Vollzugriff auf den Enterprise Server und den Server-Manager. Seine Rechte entsprechen denen des Super-Administrators.
- Datenbank-Administrator: Der Datenbank-Administrator kann neue Datenbanken auf dem Server erstellen und bestehende Datenbanken bearbeiten.
- Konto-Administrator: Der Konto-Administrator kann neue Benutzer und Gruppen dem Server hinzufügen und bestehende Benutzer und Gruppen verwalten.
- Active Directory-Operator: Der Active Directory-Operator kann im Server-Manager die Active Directory- oder Azure AD-Synchronisation durchführen. Bitte beachten Sie, dass er dazu zusätzlich auch die Rolle des Datenbank- oder Konto-Administrators innehaben muss.
- Ereignisprotokoll-Leser: Der Ereignisprotokoll-Leser hat Zugriff auf die Protokolle des Servers.

HINWEIS: Durch die Einführung der Server-Rollen in Version 15 ist das Konto des Super-Administrators nun ausschließlich für die Verwaltung des Servers vorgesehen. Mit dem Konto des Super-Administrators kann man sich nur am Server-Manager anmelden, nicht jedoch über den Client am Server. Da der Super-Administrator kein eigentlicher Benutzer mehr ist, spielt sein Konto auch bei der Lizenzierung keine Rolle.

Mitglied von

Hier werden die Gruppen aufgelistet, deren Mitglied ein Benutzer ist. Neben ihrem Namen können Sie ihren Typen und ihre Beschreibung sehen. Über *Gruppe hinzufügen* können Sie dem Benutzer weitere Gruppen zuweisen. Über *Löschen* können Sie Gruppen aus der Liste entfernen.

Erweitert

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 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. 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.

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 an, mit dem der Benutzer sich an der Domäne anmeldet.
- Benutzerprinzipalname: Gibt den Namen des Systembenutzers im Active Directory im E-Mail-Format wieder.
- ADs-Pfad: Zeigt den Active Directory-Pfad eines Benutzers an.
- GUID: Zeigt die automatisch generierte ID eines Active Directory-Benutzers.

Azure AD

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

- Benutzerprinzipalname
- Objekt-ID
- Benutzertyp: Hier wird Ihnen der Benutzertyp des synchronisierten Azure AD-Benutzers angezeigt. Es wird grundsätzlich zwischen einem *Gast* und einem *Mitglied* unterschieden.

HINWEIS: Bitte tragen Sie in den Registerkarten *Active Directory DS* und *Azure AD* keine Daten manuell ein. Die Attribute der Benutzer werden während der Synchronisation automatisch hinzugefügt und sind auch nur dann brauchbar.

Datenbank zuweisen

Die Funktion *Datenbank zuweisen* finden Sie in den Ansichten *Benutzer* und *Gruppen* an der rechten Seite. Hierüber können Sie Benutzern oder Gruppen direkt eine Datenbank zuweisen und ihre Berechtigungen darin verwalten. Sie können eine bereits bestehende Datenbank verwenden oder eine neue erstellen.

Folgende Registerkarten stehen Ihnen dabei zur Verfügung:

- Datenbank
- Rechte

Datenbank

- Ausgewählte Konten: Zeigt die Benutzer oder Gruppen an, denen eine Datenbank zugewiesen werden soll.
- Vorhandene Datenbank auswählen
- Neue Datenbank erzeugen
- Private Datenbank erzeugen: Hier können Sie private Datenbanken für jeden der ausgewählten Benutzer bzw. Gruppen erstellen. Sie werden zwecks Zuordnung mit dem jeweiligen Benutzernamen versehen und sind nur für die entsprechenden Benutzer oder Gruppen zugänglich.

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.

Gruppen

Der Bereich *Gruppen* ermöglicht dem Administrator, neue Gruppen hinzuzufügen und bestehende zu bearbeiten oder zu löschen. 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
- **Typ:** Es wird zwischen Standard-Gruppen, also manuell lokal angelegten Gruppen, Azure AD-Gruppen und Active Directory-Gruppen unterschieden.
- 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

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

- Neue Gruppe
- Eigenschaften
- Löschen
- Synchronisieren: Erlaubt es, einzelne Gruppen mit Active Directory oder Azure AD zu synchronisieren, ohne eine Synchronisierung für den gesamten Server starten zu müssen.
- Datenbank zuweisen
- Alle auswählen

Gruppen hinzufügen

Wie bei den Benutzern gibt es für Gruppen drei Wege, sie dem Enterprise Server hinzuzufügen:

- Über die Schaltfläche *Neue Gruppe*
- Per Active Directory-Synchronisation
- Per Azure AD-Synchronisation

Neue Gruppen manuell anlegen

Über *Gruppen → Neue Gruppe* können Sie dem Server neue, lokale Gruppen manuell hinzufügen. Geben Sie ihr einen Namen und tragen Sie, wenn gewünscht, weitere Eigenschaften ein. Bitte beachten Sie dabei, dass manuell hinzugefügte lokale Gruppen immer den Typen Standard haben, was nicht geändert werden kann. Fügen Sie auf der Registerkarte *Mitglieder* dieser Gruppe Benutzer hinzu. Auf der Registerkarte *Mitglied von* können Sie die neue Gruppe einer anderen Gruppe unterordnen.

Per Active Directory-Synchronisation

Password Depot Enterprise Server kann Gruppen, die in Active Directory bestehen, importieren. Seit Password Depot Enterprise Server 17 werden auch verschachtelte Gruppen unterstützt. Gehen Sie auf *Extras → Active Directory-Synchronisation*, um die Synchronisation zu starten. Wenn sie erfolgreich war, sehen Sie anschließend im Bereich *Gruppen* alle aus Active Directory importierten Objekte.

Gruppen, die per Active-Directory-Synchronisation hinzugefügt wurden, enthalten automatisch die entsprechenden Active Directory-Benutzer. Erhält eine Active Directory-Gruppe nun Zugriff auf eine Datenbank auf dem Server, können sich alle Mitglieder dieser Gruppe per Integrierter Windows-Authentifizierung (SSO) am Enterprise Server anmelden.

Mehr zur Active Directory-Synchronisation erfahren Sie hier.

Per Azure AD-Synchronisation

Um Gruppenobjekte aus Azure AD zu importieren, starten Sie unter *Extras → Azure AD-Synchronisation* die Synchronisation. Wenn sie erfolgreich war, sehen Sie im Anschluss im Bereich *Gruppen* alle aus Azure AD importierten Objekte.

Gruppen, die per Azure AD-Synchronisation hinzugefügt wurden, enthalten automatisch die entsprechenden Azure AD-Benutzer. Erhält eine Azure AD-Gruppe nun Zugriff auf eine Datenbank auf dem Server, können sich alle Mitglieder dieser Gruppe per Azure AD-Authentifizierung am Enterprise Server anmelden.

Mehr zur Azure AD-Synchronisation erfahren Sie hier.

Gruppeneigenschaften

Die Eigenschaften einer Gruppe können Sie aufrufen, indem Sie im Bereich *Gruppen* eine Gruppe markieren und doppelklicken oder rechts auf die Schaltfläche *Eigenschaften* klicken. Folgende Registerkarten stehen Ihnen hier zur Verfügung:

- Allgemein
- Mitglieder
- Mitglied von

Allgemein

Hier können Sie folgende Angaben machen:

- Name
- Typ: Zeigt an, ob es sich um eine Standard-Gruppe, also eine manuell angelegte lokale Gruppe, um eine Active Directory-Gruppe oder eine Azure AD-Gruppe handelt.
- Beschreibung
- Deaktiviert: Deaktiviert eine Gruppe, etwa wenn sie zeitweise nicht benötigt wird. Ihre Mitglieder können sich allerdings noch mit dem Server verbinden.

Mitglieder

Hier können Sie die Mitglieder einer Gruppe sehen und verwalten. Über *Hinzufügen* können Sie Benutzer einer Gruppe hinzufügen. Wenn Sie auf die Pfeil-Schaltfläche klicken, können Sie Benutzer auch über ihre Abteilung hinzufügen. Um einen Benutzer aus der Gruppe zu entfernen, markieren Sie ihn und klicken Sie auf *Löschen*. Bitte beachten Sie, dass die Benutzer dabei nicht vom Server gelöscht werden, sondern nur aus der Gruppe.

Mitglied von

Hier können Sie eine Gruppe anderen Gruppen unterordnen. Über *Hinzufügen* können Sie dabei Gruppen aussuchen, die dieser Gruppe übergeordnet sein sollen. Über *Entfernen* können Sie übergeordnete Gruppen entfernen. Bitte beachten Sie, dass entfernte Gruppen noch am Server verfügbar sind. Sie sind der aktuell bearbeiteten Gruppe nur nicht mehr übergeordnet.

Benachrichtigungen

Im Bereich *Benachrichtigungen* können Sie festlegen, über welche Ereignisse am Server sie benachrichtigt werden möchten. In der Hauptansicht sehen Sie folgende Spalten:

- ID: Jede Benachrichtigung besitzt eine eigene ID. Je nach Reihenfolge, in der Sie Benachrichtigungen hinzugefügt haben, werden sie durchnummeriert.
- Typ: Zeigt an, bei welchem Ereignis die Benachrichtigung verschickt werden soll.
- Anmerkungen
- Empfänger

An der rechten Seite haben Sie noch folgende Optionen:

- Neue Benachrichtigung
- Eigenschaften
- Löschen
- Alle auswählen

Neue Benachrichtigung

Sie können dem Server-Manager neue Benachrichtigungen über *Benachrichtigungen → Neue Benachrichtigung* hinzufügen.

Wählen Sie dazu zunächst aus, über welches Ereignis Sie informiert werden möchten. Fügen Sie, wenn gewünscht, eigene Anmerkungen hinzu.

Legen Sie anschließend die Empfänger der Benachrichtigung fest. Um einen Empfänger hinzuzufügen, geben Sie seine E-Mail-Adresse unten links ein und klicken Sie auf *Hinzufügen*. Um einen Empfänger durch einen anderen zu ersetzen, markieren Sie diesen Benutzer, geben unten links eine neue E-Mail-Adresse ein und klicken Sie auf *Ersetzen*. Um einen Empfänger zu entfernen, markieren Sie ihn und klicken Sie auf *Löschen*. Klicken Sie zum Abschluss auf *OK*.

Benachrichtigungseigenschaften

Hier haben Sie folgende Registerkarten zur Verfügung:

- Allgemein
- Erweitert

Allgemein

In der Registerkarte *Allgemein* können Sie folgende Eigenschaften bearbeiten:

- Ereignis: Wählen Sie aus, wann Sie eine Benachrichtigung erhalten.
- Der Benachrichtigung diese Anmerkungen hinzufügen
- Benachrichtigung an diese Empfänger senden: Hier können Sie Liste der Personen an, die über das entsprechende Ereignis benachrichtigt werden, sehen und bearbeiten.

Erweitert

Je nachdem, für welches Ereignis die Benachrichtigung erstellt wurde, können Sie auf der Registerkarte *Erweitert* für einige Benachrichtigungen zusätzliche Einstellungen vornehmen.

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.

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.
- Ausgewählte Einträge: Sie können die gewählte Benachrichtigung auch nur bei ausgewählten Einträgen verschicken lassen.

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.
- Datum und Uhrzeit: Zeigt den genauen Zeitpunkt an, zu der eine Serveraktivität registriert wurde.
- Benutzername: Zeigt den Benutzer an, der auf dem Server eine Aktivität durchgeführt hat.
- Adresse: Zeigt die IP-Adresse an, von der eine Aktivität ausgegangen ist.
- Ereignis-ID: Jede einzelne Aktivität auf dem Server wird mit einer spezifischen Ereignis-ID bezeichnet.
- Beschreibung: In dieser Spalte können Sie sehen, welche Aktivität durchgeführt wurde.
- 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, können Sie die Änderung hier sehen.
- Grund: Wird ein Fehler auf dem Server registriert, so wird Ihnen in dieser Spalte der Grund für diesen Fehler angezeigt. Wenn Sie von Ihren Nutzern die Angabe eines Grunds zum Löschen von Ordnern und Einträgen erzwingen, werden diese Gründe ebenfalls hier angezeigt.

Auf der rechten Seite stehen Ihnen zudem folgende Optionen zur Verfügung:

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

Über die Suchfunktion oben links können Sie außerdem das Protokoll gezielt nach bestimmten Ereignissen durchsuchen.

Ereignis-IDs

Im Server-Protokoll werden die verschiedenen Ereignisse mit IDs gekennzeichnet. Was sich hinter welcher ID verbirgt, erfahren Sie im Folgenden:

IDs, die mit einer Eins beginnen, beschäftigen sich mit den Clients.

- 101: Anmeldung eines Clients.
- 102: Abmeldung eines Clients.
- 103: Eine Liste der verfügbaren Datenbanken wurde gesendet.
- 104: Das Benutzerpasswort wurde geändert.

IDs, die mit einer Zwei beginnen, beschäftigen sich mit Datenbanken.

- 201: Eine Datenbank wurde an einen Benutzer gesendet.
- 202: Eine Datenbank wurde von einem Benutzer geschlossen.
- 203: Eine Datenbank wurde von einem Benutzer geöffnet.
- 204: Eine Datenbank wurde exportiert.
- 205: Eine Datenbank wurde gedruckt.
- 206: Eine Datenbank wurde aktualisiert.

IDs, die mit einer Drei beginnen, beschäftigen sich mit einzelnen Einträgen.

- 301: Ein Eintrag wurde gesperrt.
- 302: Ein Eintrag wurde entsperrt.
- 303: Ein Eintrag wurde aktualisiert.
- 304: Ein neuer Eintrag wurde erzeugt.
- 305: Ein Eintrag wurde aufgerufen.
- 306: Ein Eintrag wurde gelöscht.
- 307: Ein Eintrag wurde verschoben.
- 308: Für einen versiegelten Eintrag wurde um Zugriffserlaubnis gebeten.
- 309: Das Siegel eines Eintrags wurde gebrochen.

IDs, die mit einer Vier beginnen, beschäftigen sich mit Ordnern.

- 403: Ein Ordner wurde aktualisiert.
- 404: Ein Ordner wurde erstellt.
- 405: Ein Ordner wurde gelöscht.

IDs, die mit einer Sechs beginnen, beschäftigen sich mit der Verwaltung des Servers.

- 601: Anmeldung am Server-Manager.
- 602: Abmeldung vom Server-Manager.
- 603: Eine neue Datenbank wurde am Server erstellt.
- 604: Die Server-Richtlinien wurden geändert.
- 605: Die Datenbank-Eigenschaften wurden bearbeitet.
- 606: Eine Gruppe wurde erstellt oder bearbeitet.
- 607: Eine Benachrichtigung wurde erstellt oder bearbeitet.
- 608: Ein Benutzer wurde erstellt oder bearbeitet.
- 609: Eine Datenbank wurde vom Server gelöscht.
- 610: Ein Benutzer wurde vom Server gelöscht.
- 611: Eine Gruppe wurde vom Server gelöscht.

- 612: Eine Benachrichtigung wurde gelöscht.
- 613: Ein Benutzer wurde vom Server getrennt.
- 614: Der Server wurde angehalten.
- 615: Der Server wurde fortgesetzt.
- 616: Eine Lizenz wurde installiert.
- 617: Die Serveroptionen wurden geändert.
- 618: Eine Datenbank wurde vom Admin gelesen.
- 619: Die Active Directory wurde vom Admin gelesen.
- 620: Bei einem Benutzer wurde die Zwei-Faktor-Authentifizierung zurückgesetzt.
- 621: Der Server wurde neugestartet.
- 622: Eine Berechtigung wurde gelöscht.
- 623: Ein Benutzer oder eine Gruppe wurde einer Datenbank hinzugefügt.
- 624: Das Passwort einer Datenbank wurde geändert. 625: Eine Liste der Nutzer wurde an den Admin gesendet.
- 626: Eine Liste der Gruppen wurde an den Admin gesendet.
- 627: Informationen über den Server wurden an den Admin gesendet.
- 628: Das Server-Protokoll wurde an den Admin gesendet.
- 629: Eine Liste der Datenbank wurde an den Admin gesendet.
- 630: Eine Liste der Benachrichtigungen wurde an den Admin gesendet.
- 631: Die Serverrichtlinien wurden an den Admin gesendet.
- 635: Eine Liste über den Spiegel wurde an den Admin gesendet.
- 636: Ein Spiegel wurde erstellt.
- 640: Ein Mandant wurde aktualisiert.
- 641: Ein Mandant wurde hinzugefügt.
- 642: Ein Mandant wurde gelöscht.
- 643: Ein Zertifikat wurde generiert.

IDs, die mit einer Sieben beginnen, beschäftigen sich mit Active Directory.

- 701: Die Active Directory-Synchronisation wurde begonnen.
- 702: Die Active Directory-Synchronisation wurde beendet.
- 703: Bei der Active Directory-Synchronisation ist ein Fehler aufgetreten.
- 704: Ein Objekt wurde bei der Active Directory-Synchronisation deaktiviert.
- 705: Ein Objekt wurde bei der Active Directory-Synchronisation gelöscht.
- 706: Ein Objekt wurde bei der Active Directory-Synchronisation hinzugefügt.
- 707: Ein Fehler ist aufgetreten, während ein Objekt bei der Active DirectorySynchronisation hinzugefügt wurde.
- 708: Ein Objekt wurde bei der Active Directory-Synchronisation aktualisiert.

IDs, die mit einer Acht beginnen, beschäftigen sich mit Sicherungsdateien.

- 801: Informationen über den Status des Backups wurden an den Admin gesendet.
- 802: Eine Datenbank wurde über ein Backup aktualisiert.
- 803: Das Backup einer Datenbank wurde an den Admin gesendet.

Rechte für Benutzer

Der Password Depot Enterprise Server erlaubt neben der Benutzung mehrer Datenbanken auch, eine zentrale Server-Datenbank zu erstellen, auf die alle Mitarbeiter Zugriff haben. Durch die Rechteverwaltung können Administratoren sie so strukturieren, dass jeder Benutzer tatsächlich nur das sieht, was er sehen soll, und auch nur darauf zugreifen kann.

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

Wie gestaltet sich die Rechtevergabe am Enterprise Server?

Am Enterprise Server können Sie Berechtigungen auf drei Ebenen festlegen:

- auf Server-Ebene
- auf Datenbank-Ebene
- auf Ebene der einzelnen Einträge und Ordner

Benutzer haben dabei nur die Rechte, die ihnen explizit erteilt wurden. Wenn eine Berechtigung nicht definiert oder verweigert ist, gilt sie also für Ihre Benutzer nicht. Dabei gilt das Prinzip der Vererbung: Die Einstellungen zu den Berechtigungen setzen sich von einer höheren Ebene auf eine tiefere Ebene fort. Dabei können erlaubte oder nicht definierte Berechtigungen in einer tieferen Ebene geändert werden, verweigerte Berechtigungen dagegen nicht.

Im Folgenden wird die Rechtevergabe auf den jeweiligen Ebenen genauer erklärt.

Rechtevergabe auf Server-Ebene

Unter *Verwalten → Serverrichtlinien* können Sie globale Rechte definieren, die global für alle Benutzer am gesamten Server gelten. Sie können die Berechtigungen auf *Aktiviert, Nicht aktiviert* oder *Nicht definiert* setzen. Da Berechtigungen, die auf dieser Ebene deaktiviert wurden, auf Datenbank-, Ordner oder Eintragsebene nicht mehr erlaubt werden können, empfehlen wir, bei den Serverrichtlinien die Standardeinstellungen beizubehalten und die Rechtevergabe hauptsächlich im Bereich *Datenbanken → Berechtigungen* vorzunehmen.

Rechteverwaltung in den Berechtigungen einer Datenbank

Über *Datenbanken → Berechtigungen* können Sie Berechtigungen detailliert für Benutzer und Gruppen 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

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

HINWEIS: Bitte setzen Sie auf der Registerkarte *Datenbank* kein Häkchen bei der Option *Verweigern* für *Lesen/Ändern/Hinzufügen/Löschen*, wenn ein Benutzer Zugriff auf die Ordner und Einträge einer Datenbank haben soll, sondern entfernen Sie nur das Häkchen bei *Erlauben*. Anderenfalls kann der Benutzer die Datenbank zwar empfangen, aber ihre Inhalte nicht sehen oder bearbeiten.

Bei der Rechtevergabe auf Datenbank-, Ordner- und Eintragsebene werden erlaubte Berechtigungen grün, verweigerte Berechtigungen rot markiert. Zudem können Sie sich die effektiven Berechtigungen ansehen.

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?