Password DEPOT

Manual

Password Depot

Enterprise Server 17

Last updated: 01.12.22

AceBIT

Every Bit an Ace!

Table of Contents

Introduction

Password Depot Enterprise Server is an extension to Password Depot. With the Enterprise Server, users can share databases stored on a central server. The desktop client for Windows is the main program that is used to connect to the Enterprise Server. In addition, you can also access the Enterprise Server with our macOS edition or our mobile apps for Android or iOS.

Password Depot Enterprise Server is installed on a computer in your local network. The server administrator mainly works with the Server Manager, a separate tool for Enterprise Server management. In the Server Manager, the administrator can create new databases, add users and groups to the server and configure their access to databases on the server.

Users with access to server databases can open them in the client. For Enterprise Server connection, the following data is needed:

- Server address
- Port
- Access data (username & password)

The access dater of a user is defined by the administrator. Login to the Enterprise Server can be either performed with a local user via username and password, by Integrated Windows Authentication (SSO) or by Azure AD Authentication. In addition to that, the administrator can define further settings, for example activating 2 Factor-Authentication or setting up notifications for specific events.

All transferred data is encrypted with ephemeral keys using the AES 265-bit algorithm. Clients communicate with the server through TCP/IP protocol (IPv4/IPv6). This way, you can ensure GDPR (General Data Protection Regulation) compliance.

Summary

With Password Depot Enterprise Server,

- your data is centrally managed and your employees can securely share databases within your company.
- you can either access your data within the local network only or, if required, you can also access it through the internet from anywhere.
- you can create your own database tree and define the user permissions within the database yourself.
- you can decide where to store your sensitive data since Password Depot Enterprise Server is an on-premises software.

Watch our video to learn more about Password Depot Enterprise Server and how it can support companies in their everyday work:

How companies can benefit from Password Depot Enterprise Server

Or get to know Password Depot Enterprise Server during one of our free webinars:

Password Depot webinar

If you want to learn more about the Password Depot and Password Depot Enterprise Server system requirements, please have a look at our website using the link below:

Password Depot & Password Depot Enterprise Server - System requirements

Licensing

The required Enterprise Server license depends on the total number of users you would like to add to the server. It defines how many users can be added to the server at maximum. Purchased licenses are named licenses. They can be used by only one user, but on an unlimited number of devices. Furthermore, a license can be used in all available localized languages.

Adding a maximum of three users to the Enterprise Server does not require a license. In this case, the server can be downloaded and used for free. Please note, however, that you will still need licenses for the clients in this case.

When purchasing Password Depot Enterprise Server, all clients for all supported operating systems as well as the web interface are included. The Enterprise Server and the client (i.e. the main program) are sold as a bundle.

All server sizes and prices as well as further information on licensing can be found on our website:

Purchase Password Depot Enterprise Server

Installation and Running

While it is recommended to install Password Depot Enterprise Server on the server computer of the local network, it is also possible to install it on any computer accessible in the network. In this case, the computer must be assigned a fixed IP address within the local network.

> Note: You may install the Enterprise Server on your local computer as well, for example for testing purposes. To access the server using the Password Depot desktop client, you can use the server addresses 127.0.0.1 or local host, or the IP address of the server.

Installation as a Windows Service or as a Windows Application

You can run Password Depot Enterprise Server either as a Windows Service or as a Windows Application Server. By default, the installation is performed as a Windows Service. We recommend this mode since the Password Depot server service will be set up automatically in the background during installation.

If you have installed the Enterprise Server as a Windows Service, the server will be listed as Password Depot Enterprise Server. The service is always running in the background. Normally, Password Depot Enterprise Server starts automatically upon Windows startup. If you have set up the server to run as an NT service, it will start under the SYSTEM account and does not require a user to be logged in. You can manually start or stop the service in the Windows services dialog window.

If you have installed the server as a Windows Application Server, you will find it in the program directory. By default, this is *C:\Program Files\AceBIT\Password Depot Server x* in Vista, Windows 7, 8 and 10 or *C:\Programs\AceBIT\Password Depot Server x* in Windows XP.

Since version 14 onward, Password Depot Enterprise Server supports tge 64-bit architecture.

Server Manager

The Server Manager is the separate managing tool of Password Depot Enterprise Server. Administrators use it for general server configuration such as creating new databases. It is installed automatically along with the server. Thus, it will be accessible on the same machine the server is running on.

To open the Server Manager, either click on the Windows key → AceBIT → Password Depot Server Manager x or double click on the Server Manager desktop icon. The Server Manager is installed with the following default login credentials:

- User name: Admin
- Password: admin

NOTE: We highly recommend changing the administrator's default access credentials in the Server Manager after installation and first login. To do so, open the Server Manager, go to *Users* → *admin* → *Account* and change the login credentials.

For the Server Manager login, the IP address of the server on which the Enterprise Server is running is required, as well as the correct port number.

NOTE: The addresses 'localhost' and '127.0.0.1' always work. This way, administrators can still access the Server Manager in case of incorrect settings in order to correct them.

Updates

You can check for updates by launching the Server Manager and going to *Help* → *Search for updates*. If a newly released build is displayed here, we recommend installing it as soon as possible to keep the software up to date.

Please note that the Server Manager does not contain an integrated update manager. You can only check if new updates within the same main version are available here. New server updates can only be downloaded from our website. After download, you can launch the installation wizard ot start the installation. When installing smaller updates within the same main version, you do not need to stop the server service.

Running Password Depot on a Terminal Server

While it is generally not recommended, Password Depot can also be run on a terminal server.

The installation of Password Depot on a terminal server is the same as installing it on a physical server. As far as licensing concerned, there is no difference, either. You can find detailed information on our licensing model in the knowledge base:

Licensing and Maintenance

Using the Password Depot browser add-on on a terminal server

If multiple users have access to Password Depot on a terminal server and the browser add-on is activated, it is strongly recommended to assign individual port numbers to the users. Since the socket port number is for the browser add-on is not a virtual parameter but rather a physical one, it cannot be shared by multiple instances of the Password Depot client. Otherwise, users may receive login data they are not meant to see, since the browser add-on does not know which user is requesting the data. This can be a grave security issue.

How to assign individual port numbers to users

You can choose from two options:

1. Open the Server Manager and go to *Manage → Server settings → Additional*. Check the option Auto-generate unique port numbers (recommended for Terminal Servers). Every client automatically receives a specific port number afterwards.
2. Open the Server Manager and go to the *Users* area. Select a user next. Open the user properties by double clicking on the user and go to the Advanced tab. You can see the *WebSockets port for browser add-ons* section here. Check the option *Use custom port number* and define a custom value for each user.

Users can see their individual port numbers in the client by going to *Edit → Options → Browsers*. To complete the process, they have to manuall change the port number in the browser, since this cannot be changed automatically. To do so, click the add-on icon in the browser and go to Settings. Afterwards, change the value accordingly.

NOTE: If you do not want to assign individual port numbers to the users, we strongly recommend disabling the permissions for using the browser add-on in the Server Manager in order to avoid the above mentioned issues.

For more information, please visit our knowledge base:

How do I change the port number when working with the add-on and running Password Depot on a terminal server?

Migration

If you are already working with an older version of the Enterprise Server and would like to upgrade it to a new main version, you can easily migrate the server.

Please note that the Enterprise Server can only communicate with Windows clients of the same main version. For instance, you cannot access the Enterprise Server of version 17x using a Windows client of version 12x and vice versa. However, this does not apply to the macOS, iOS or Android editions, which are downward compatible to an extent.

When upgrading to a new main version, you can migrate all databases as well as your users and server settings. In our knowledge base, you can find step-by-step instructions on how to migrate the Enterprise Server:

How to migrate Password Depot Enterprise Server to a new main version

We recommend following these instructions carefully to avoid problems. The process should only take a few minutes.

If you migrate from a very old version to a newer one, please have a look at the knowledge base article below first:

How to migrate from a previous version to Password Depot Enterprise Server 12

Note that the migration process for mirrored servers does not differ from that for non-mirrored ones. It does not matter in which order principal and mirror are upgraded. You only need to follow the instructions outlined above for both the principal and the mirror.

NOTE: You can follow these instructions if you would like to move your current server installation to another machine as well. The steps are the same as for an upgrade; the only difference is that you remain within the same version and use the same directories as on the old server, provided you use the default directories.

Server Manager

The Server Manager is a separate tool that allows for maintenance and configuration of Password Depot Enterprise Server. To do so, you will have to connect to the server with the super administrator's access data initially.

WARNING: Only the super administrator or other people authorized to access the Server Manager should know the admin password. Anyone with access to the admin password will have access to the Server Manager and thus server administration.

The navigation area of the Server Manager is divided into five sections:

- Databases
- Users
- Groups
- Notifications
- Log

If you click on the server's IP address in the navigation area, basic information about the Enterprise Server will be displayed:

- Status: Here, you can see if the server is running or if it has been paused.
- Server address: Displays the IP address of the server.
- Server port: Displays the default port number that is used to connect to the server.
- Running since: Displays the date the server has been put into operation for the first time.
- Server version: Displays the server build you are currently running.
- Updates available: Here, you can see if new updates within the same main version are available.
- Installed licenses: Displays the number of users allowed on the server at maximum.
- Registered users: Displays the number of users already registered on the server.
- Connected users: Here, you can see how many users are connected to the server at the moment.
- Installed databases: Displays how many databases are installed on the server in total.
- Mirroring: If you have activated server mirroring, the state of server mirroring is displayed here.

NOTE: In case you forget the password for the Server Manager login, you will have to perform a workaround to get access again. Please follow these instructions carefully: How can I "reset" the administrator's password in Password Depot Enterprise Server?

Manage

This menu item is found in the top right in the main view of the Server Manager. It contains the following options:

- Server settings: You can define basic server settings here.
- Server license: Here, you can enter a new license key.
- Server policies: Here, you can set global default server policies that will be applied to the entire server. Note that permissions that are disabled here cannot be enabled individually, while permissions that are enabled or left undefined here can still be disabled on an individual level. Our recommendation is therefore to enable them or leave them undefined.
- Client security policies: The Client security policies are applied to the Corporate Client. In this case, administrators can define even more settings and permissions that apply to all users even without an active connection to the server. Please click here for more information.
- Mirroring: Select this option to activate server mirroring.
- Pause: Here, you can pause the server. While clients are not able to connect to the server anymore, the Server Manager still is.
- Continue: If the server was paused, you can restart it here.
- Program options: Here, you can define the program options (note that they are different from the server settings). The program options refer to the Server Manager only.
- Exit: You can exit and shut down the Server Manager here. This does not affect the server itself.

NOTE: Some changes on the Enterprise Server may require a server restart. In version 15, a command for restarting the server has been implemented. The prompt will be displayed automatically if needed. If so, we recommend restarting the server immediately.

Server Settings

The server settings can be found in the menu *Manage*. The following tabs are available here:

- General
- Connections
- Logging
- Backups
- Additional
- Email
- 2FA Settings
- Active Directory
- Azure AD

General

Server

- Server language: You can select German or English as the server language here. Note that this is not the language for the for the Server Manager interface.
- Server port: You can define the port number for the client to server connection here. Usually, the default port is displayed, but you can change the value if required. Please make sure to change it in the client as well if you use a custom port number.
- Internet Protocol: Here, you can specify an Internet protocol version that should be used by default. The options are IPv4+IPv6, IPv4 and IPv6.
- Use SSL/TLS for TCP Server: You can activate the SSL/TLS connection when connecting clients to the Enterprise Server. Click Install Certificate to install the certificate in the Server Manager.
- Keepalive enabled: You can activate the Keepalive feature if clients connect to a server that is not part of the same local network.

REST Server

- Origin URL: Enter the correct URL of your Password Depot web server, which is used to access the server with the Password Depot web interface.
- Use SSL/TLS for REST Server: You can activate the SSL/TLS connection during REST Server connection. This allows for server access via a REST API. Essentially, it is a web server using both the HTTP and the HTTPs protocol, the latter of which we recommend. In order to use HTTPS, install a valid SSL certificate by clicking the button on the right.

> TIP: For more information on SSL connections on the Enterprise Server, please have a look at the following knowledge base article:

How does the SSL connection in Password Depot Enterprise Server work and which settings are required?

Databases

Here, you can see and edit the location where Password Depot Enterprise Server saves its databases by default.

Connections

Supported authentications

Here, you can define the supported authentication methods on your server. You can choose between *User credentials (account and password)*, *Integrated Windows Authentication (Single Sign On)* and/or *Azure Active Directory*. You can select multiple authentication methods at once.

TIP: For more information on the Integrated Windows Authentication as well as the required settings, please check the following knowledge base article:
How do I log on to the Enterprise Server using the Integrated Windows Authentication (SSO)?

Supported clients

Select which clients may connect to the server. The following options are available:

- Standard Edition for Windows
- Corporate Edition for Windows
- Android Edition
- iOS Edition
- macOS Edition
- Web Client

New connection from different device

Here, you can choose how to proceed with connections by the same user from multiple devices.

- Deny new connection when user is already logged on
- Close existing connection and allow new one
- Allow multiple connections from different IP addresses

NOTE: It is not recommended to allow multiple connections by the same user. This feature was implemented to allow for simultaneous connections from a desktop client and a mobile app. In this scenario, simultaneous connections would not cause any issues because mobile devices are not synchronized with the server in real time. However, connections by one user across more than one Windows client at a time may cause issues.

Inactive sessions

Specify here if Password Depot Enterprise Server should disconnect inactive users and, if so, when. Additionally, you can also choose to close the database and sign out the client.

Logging

Local log

- Logs folder: You can see the directory for the Enterprise Server logs here. By default, this is *C:\Program Files\AceBIT\Password Depot Server x\Logs* in Password Depot Enterprise Server 15 or newer. You can change the location using the browse button. However, we recommend using a local directory, if possible.
- Max. file size (KB): Determine the maximum size of the server log file.
- Create new log file: Select a time when to create a new log file.
- Delete logs: Define settings for deleting existing logs.

Remote log

- Send log messages to a remote server: Check this box if you wish to activate the option and send the Enterprise Server log files to external log servers. By specifying the address and the port of the external server, you can ensure that protocols are not manipulated.

Backups

Backup

- Backup folder: Here, you can specify where backup copies of your server database should be stored. By default, this is *C:\Program Files\AceBIT\Password Depot Server x\Backups\* in Password Depot 15 or newer. You can change it using the Browse button. However, we always recommend using a local directory. In addition to the databases themselves, the backup files include server logs and configuration files.
- Backup databases on every startup
- Backup databases every: Set a time for Password Depot Enterprise Server to automatically create a new backup file. We recommend creating new backup files at least once a day.
- Delete backup files older than: Activate this option if you would like to automatically delete backup files older than a period of time that you determine.

- Log backups to file: If activated, Password Depot Enterprise Server will create a log of all generated backups and save it to the specified file.

Additional

Edit entries

Here, you can set a time limit after which an opened entry should be locked.

Private databases

Here, you can choose to automatically create a private database for each new user and, if so, to automatically delete this database if the user is deleted.

WebSockets port for clients

Here, you can define whether all clients should use the default port number and, if so, what this number is, or whether each client should use an individual port number for the communication between client and browser add-on.

Failed logins

Define after how many failed login attempts a user will be deactivated on the server. Please note that failed login attempts do not reset after some period of time but rather after a successful login.

Email

On this tab, you can define settings for an email server:

- Sender: Here, you can define the name and the email address of the sender.
- Outgoing Mail Server: Configure the outgoing mail server here.
- Test Connection: You can enter the email address of a mail recipient here and send a test email to check if the settings are correct.

2FA Settings

Operation mode

- TOTP - codes are generated by mobile Authenticator apps: Users will receive the second factor for the login o their smartphone in their external authenticator app.
- Email - codes are sent by Server to user's default address: Users will receive the second factor by a separate email to their individual email address.
- Users may choose to remember their devices (days): You can specify a certain time period in which users can trust connections to a specific device. If this option is activated and users enable the option Trust this computer when connecting to the server for the first time, they will not need to enter the second factor for the specified period.
- Email code expiration time (minutes): This option determines the validity of a TOTP code sent by email. By default, this is ten minutes.

Both the Integrated Windows Authentication and Password Depot credentials authentication support Two-Factor Authentication. In the User area, you can deactivate or reset 2FA for individual users.

For more information on Two-Factor Authentication, please visit our knowledge base.

Active Directory

Synchronization

- Automatically run synchronization with AD every: Specify whether to perform AD synchronization automatically and, if so, at what intervals. Note that we recommend performing AD synchronization manually; however, if automatic synchronization is necessary, synchronization should preferably be performed when the server load is low.

Azure AD

Tenants

Here, you can add a new organization to Password Depot Enterprise Server and the Server Manager. Once a new organization has been added, you can use it to perform Azure AD synchronization.

- New: Click New to launch the process. You will be asked to select a Microsoft account and log in with the administrator's access data. After login, you can see the organization in the Tenants area. Select Tools → Azure AD Synchronization in the Server Manager to automatically synchronize Azure AD users with the Enterprise Server. You can select the organization in the synchronization wizard.

TIP: You can also add an organization directly under Tools → Azure AD Synchronization. The button New is available here, as well.

- Update: Update an organization that has already been added to the Server Manager and the data related to it.
- Delete: Delete organizations from the Server Manager. After deletion, you can add another organization to the Server Manager by clicking New.

Synchronization

- Automatically run synchronization with AD every: Here, you can define if Azure AD is synchronized automatically and, if so, at what intervals.

NOTE: Found out more about Azure AD synchronization in the chapter Azure AD Synchronization.

Server License

Under *Manage → Server* license, you can enter a new license key. Additionally, you can also see the current server license and version here. If you have increased the total number of users on the server by purchasing a new license, you can enter the new key here.

Licensing

The required Enterprise Server license depends on the total number of users you would like to add to the server. Please note that from version 12 onward, concurrent connections are not relevant anymore.

If you only want to work with a maximum of three users, you do not need to purchase a license for the Password Depot Enterprise Server. In this case, you can download the Enterprise Server from our website for free. However, please note that you will have to purchase the appropriate number of clients nonetheless.

If more than three users are required, you will have to purchase a server license. When purchasing Enterprise Server licenses, the price includes all clients on all platforms as well as the web interface as a bundle. We offer a scale of licenses, starting with five up to unlimited users.

All purchased licenses are Named Licenses. One license may only be used by one user at a time. However, one user may install and use their license on an unlimited number of devices. Furthermore, one license may be used with all additional language packs currently available.

You can find out more about server sizes and prices as well as licensing on our website:

Purchasing Enterprise Server licenses

Server Policies

The server policies can be found in the menu *Manage*. Here, you can adjust global settings, user permissions, password security and supported entry types.

NOTE: In all available tabs, you can reset any changes you have made by clicking *Restore default settings*.

Permissions

In this tab, you can define global user permissions, which will be applied to all users and databases on the server. You can choose from the following options:

- Not defined: When setting a permission to Not defined, you can still change its state for individual users and groups in the database permissions afterwards.
- Enabled: By default, enabled permissions are activated for all databases and users available on the server. However, you can still change its state for individual users and databases in the database permissions afterwards.
- Disabled: This state is the most restrictive. A disabled permission is deactivated for all users and databases on the server. You cannot enable it for individual users and databases in the database permissions afterwards.

By default, all permissions are set to *Not defined* or *Enabled*. Since permissions that are disabled at a global level cannot be enabled at an individual level, you should only disable those permissions you are certain you do not want to grant to any user on the server. Generally, we recommend setting permissions to *Enabled* or leaving them *Not defined*.

Security

In this tab, you can set a password policy that will be mandatory for all clients. For instance, you can ensure that passwords are examined for their resistance against dictionary attacks. Additionally, you can define policies regarding minimum length and complexity of new or edited passwords. Please note that these policies are only obligatory for passwords generated by Password Depot. Furthermore, you can enforce the use of a second password for authorized users.

Entries

In the *Entries* tab, administrators can select the types of entries that should be available in the client. The following types are available:

- Password
- Credit Card
- Software License
- Identity
- Information
- Banking
- Encrypted File
- Document
- Remote Desktop Connection
- PuTTY
- TeamViewer
- Certificate

NOTE: By clicking Restore default settings, you can reset any changes you have made to the settings in the Security tab.

Client Security Policies

By using the Client Security Policies, you can centrally define specific features of the Corporate client with the Server Manager. To do so, go to Manage → Client Security Policies to activate them and set the permissions as required. Note that the Client Security Policies are applied to all users on the server and cannot be changed for individual users or groups.

> NOTE: The Client Security Policies set in the Server Manager can only be applied if the Corporate edition client is used. The standard edition of the Password Depot Windows client, which is also available for download on our website, does not support these policies.

For more information on the Password Depot Client Corporate edition, please visit our knowledge base:

Password Depot Client Corporate edition and Client Security Policies

Password Policy

- Enforce password history: Define a specific number of new passwords users will have to use/create before reusing an old password.
- Maximum password age: Define a specific time span a password can be used before forcing users to change it.
- Minimum password age: Define a specific time span a password must be used before being able to change it.
- Password must meet complexity requirements: Define how many and which different types of characters (lowercase, uppercase, numbers and special characters) a password must contain at minimum.

Allowed Storage Policy

If you enable users to create and save databases outside of Password Depot Enterprise Server, you can determine here which locations users can save their databases to. Locations that have been deactivated in the Client Security Policies will not be visible in the client at all. Password Depot offers the following locations:

- Local System
- Enterprise Server
- USB Removable Devices
- Internet Servers
- Dropbox
- Google Drive
- OneDrive/OneDrive for Business

- HiDrive
- Box

Save for the Enterprise Server, all of these locations can be disabled, if desired.

Action Policy

The following actions can be disabled or enabled:

- Copy data to clipboard
- Decrypt external files
- Encrypt external files
- Erase external files
- Export
- Print
- Set Second Passwords
- Synchronize (databases)
- Use TANs

Program Options

- Auto save database on every change: This policy refers to databases stored outside of the Enterprise Server. If this option is activated, a database will be saved automatically on every change.
- Automatic cleaning of clipboard: You can define a specific time for Password Depot to automatically delete any data that has been copied to the clipboard.
- Automatic updates mode: If this option is activated, clients automatically look for updates.
- Automatically delete local copy after closing remote file: If users can save local copies of server databases to their local system, those local copies will be deleted as soon as the file is closed if this option is activated.
- Check for updates interval (days): If automatic searching for updates is enabled, you can define a specific interval for searches here.
- Close database and lock program: Always when the program is minimized
- Close database and lock program: When the computer enters standby/hibernate mode
- Close database and lock program: When the computer is idle
- Close database and lock program: When the current user (session) changes
- Close database and lock program: When the program is auto-minimized
- Create a backup copy on database saving: This policy also refers to databases stored outside of the Enterprise Server. If this policy is activated, a new backup copy is created and saved to a user's local system every time they save their database.
- Default authentication mode: Define a default authentication mode for all users. You can choose from Undefined (Client can use any value), Integrated Windows Authentication (SSO), Sign in with user name and password, and Azure AD authentication.

- Default expiration period for passwords: Define a default expiration period for all passwords within the server databases.
- Hide clipboard changes from external viewers
- Internet Protocol version: If you want to set a default Internet protocol version to be used by the clients, you can either choose between IPv4 or IPv6.
- Number of stored backup copies: This policy refers to databases stored outside of the Enterprise Server.
- Open last used password file at program start: If this policy is activated, the last used database is launched upon the client's next program start.
- Show passwords in the list view: You can define if the client's main view should include the Password column. However, passwords are never displayed in plain text but rather as asterisks.
- Store list of recent databases: This policy refers to databases stored outside of the Enterprise Server. If this option is activated, clients can go to the Database Manager → Recent Files and easily open databases they recently worked with.
- Store local copy of files from Password Depot Enterprise Server: If this policy is enabled, a local copy of the server database is stored to a user's local system. Note that local copies only include the data a user is able to access during active server connection.

TIP: If you have any questions about the client security policies or server configuration in general, please email us at info@acebit.de and we will be happy to help.

Server Mirroring

The Server Mirroring dialog box can be found in the menu item Manage.

Server mirroring is used in network management to create an exact replica of a server. This replica is created and continuously updated in real time. With the server mirroring feature in Password Depot Enterprise Server, administrators can duplicate the content of their entire server on another remote or in-house server. This way, you can restore your data in case the primary server fails.

In Password Depot Enterprise Server, server mirroring is implemented as follows:

In order to mirror a server, you will need two machines on which Password Depot Enterprise Server is installed and running. One server will be the principal server, which runs as usual, meaning that users connect to this server to access shared server databases. The other server will be the mirror server. Users will be able to connect to the mirror server as well, but they can only use it in read-only mode. The principal server updates and synchronizes the data with the mirror in real time. In case the principal server fails, administrators can activate the mirror server as principal server so that users can continue to work with the data stored to Enterprise Server databases.

To set server mirroring in the Server Manager, please proceed as follows:

Server role

Select a server role first.

- No mirroring if you do not want to mirror your server
- Principal if the server you are currently connected to should be the main server
- Mirror if the server you are currently connected to should be the mirror server

Server network addresses

Here, you can define the server addresses and ports of both the principal and mirror server.

Status

Here, you can see the current status of server mirroring along with additional information on the general configuration of your current server mirroring in Password Depot Enterprise Server.

Program Options

The Program options can be found under the menu item Manage. They refer to the Server Manager only and include the following options:

- Application language: Select the language of the Server Manager's user interface. Choose between English and German.
- SSL/TLS: Activate this option if you would like to log in to the Server Manager using an SSL connection. Please note that this is only possible if SSL connections have been generally activated in the Server Manager. If the settings are correct, the option Use SSL/TLS is checked by default in the login window of the Server Manager.

Tools

The menu item Tools includes further options for server configuration. The following features are available here:

- System log: This option allows you to generate a server log, which will then be displayed in the Windows Event Viewer. This may be helpful when combating errors.
- Active Directory Synchronization
- Azure AD Synchronization
- Databases report
- Users report
- Groups report
- SSL certificate

The following chapters include further information on the Active Directory and Azure AD synchronization as well as on creating and using the available reports.

Active Directory Synchronization

In the menu *Tools*, you can open the synchronization wizard by selecting *Active Directory Synchronization*. Active Directory synchronization is necessary if you would like your users to log in on the Enterprise Server using their Windows NT/Active Directory credentials.

NOTE: In version 14, the Windows NT provider was replaced with a more efficient LDAP provider.

When launching the wizard, you will need to provide the following information on the domain from which you would like to import users or groups:

LDAP Path

If the domain is not listed yet, enter its name here.

Sign in

- Sign in as current user: Select this option if you would like to sign in with the account you signed into windows previously.
- Use this account: Enter the user name and password of another user who is also authorized to read data

Additional options

- Explorer mode: In this mode, you can browse the existing folders in Active Directory. The Active Directory structure will be shown in a new window, from which you can select users or groups to synchronize.
- Search mode: In this mode, you can search users or groups in Active Directory.
- Recursively scan all containers: Use this option if you would like the synchronization wizard to scan the entire Active Directory. Please note that this process may take some time in some cases. Therefore, you should only use this option the very first time after migrating from an older version to the current one since it will reliably replace all WinNT with LDAP paths.
- Check deleted objects: With this option, any deleted objects, such as users or groups, are scanned both in Active Directory and Password Depot Enterprise Server and merged afterwards.
- Use SSL: Check this option if your Active Directory requires SSL.

Click *Sign in* when you have entered all necessary data. If the login was successful, you will see the Active Directory tree in the next window. Here, you can select the users and/or groups that you would like to import or update in Password Depot Enterprise Server. If you have a large number of entries, you can filter the entry using the button *Filter* in the bottom left. Click *Synchronize* to begin the synchronization. The results will be displayed in the next window.

TIP: You can synchronize individual users or groups with Active Directory as well. To do so, select the desired user or group and click *Synchronize* on the right.

NOTE: Find out here which settings are required for the Integrated Windows Authentication (SSO) in the Server Manager as well as the client:
How do I log on to the Enterprise Server using Single Sign On (SSO)?
Please note that the PC used for Signle sign-on has to be an Active Directory member.

Azure AD Synchronization

If you would like your users to be able to log in on the Enterprise Server using their Microsoft credentials, you will need to perform an Azure AD synchronization. To open the synchronization wizard, go to *Tools → Azure AD Synchronization.*

Organization

Select an organization from which you would like to import users, or add a new organization by clicking *New*. Select a Microsoft account to store as an organization. Please note that you can only use an admin account to do so.

Enter the admin user name, the admin password and the second factor from your Authenticator app. The two-factor Authentication is mandatory here as it is part of Microsoft's security policies. After logging in successfully, you will see the Azure AD users and groups available for synchronization. Select the objects you would like to import and click *Synchronize*. Afterwards, the synchronization results will be displayed.

Additional options

- Check deleted objects: With this option, any deleted objects are scanned both in Azure AD and Password Depot Enterprise Server and merged afterwards.

NOTE: Find out how Azure AD users can sign in on the server via the client in our Password Depot Windows Client manual.

Reports

The menu item *Tools* includes options for generating databases or users reports. By creating these reports, you can get a quick overview of your server users and databases. To create a report, select the desired type in the *Tools* area and click *Generate*. The report will be displayed in your browser upon generation. You can save the reports in the .html format by clicking *Save as*.

Find more information on the reports below.

Databases report

You can create a Databases Report for individual or multiple Password Depot Enterprise Server databases at a time. This way, administrators can get a quick overview about their users and which server databases they can access. Additionally, user permissions in the selected databases are displayed. Granted permissions are always displayed with a check mark, while denied permissions are displayed as a "-". Note that databases reports only display user permissions at a database level.

Users report

Under *Users report*, a report will be generated containing a list of the previously selected user accounts as well as the following information:

- Account: Displays the user name.
- Type: Here, you can see if a user is a standard user or if they have been assigned additional server roles.
- Full Name
- Email
- Disabled: Here, you can see if an account has been deactivated. Deactivated users cannot connect to the Enterprise Server anymore. To reactivate an account, open the user properties and go to the Account tab.
- Assigned Databases
- Access Rights: Displays a user's access rights on every server database.

Groups report

Under *Groups report*, a report will be generated containing a list of the previously selected groups as well as the following information:

- Account: Displays the name of the group.
- Type: Here, you can see if a group is a standard group, an Active Directory group or an Azure AD group.
- Full Name

- Email
- Disabled
- Assigned Databases
- Access Rights: Displays a group's access rights on every server database.

SSL Certificate

Password Depot Enterprise Server allows for the installation and use of an SSL certificate. It supports X.509 SSL certificates in the PEM or DER format. With a certificate, users can verify the identity of a server before they send confidential data.

> WARNING: This installation should only be carried out by an experienced admin.

Before you decide on the use of SSL connections, please consider the following:

- SSL does not encrypt any data sent from the client to the server. These data are always encrypted with AES-256-Bit via the internal protocol via TCP/IP. Therefore, using SSL in local and internal networks is not recommended. However, validating the Enterprise Server using SSL can help prevent man-in-the-middle attacks, which may be helpful if you would like clients to be able to connect to the Enterprise Server from outside of your local network.
- For reasons of cross-platform compatibility, the OpenSSL library, which has some weaknesses and is not recommended for macOS or iOS devices by Apple, has to be used.
- The use of a self-signed certificate is not supported. While you can create a dummy certificate for testing purposes, it is pointless as it can easily be falsified by third parties. Only certificates signed by a known Certificate Authority (CA) can be used to validate the Enterprise Server. If you already run a web server that uses HTTPS, using the SSL certificate of this web server may be an adequate solution.
- When using SSL, please make sure that all clients use SSL! Mixed connections, i.e. part SSL and part standard TCP/IP, are not permitted.

To install a SSL certificate, please proceed as follows:

- Enter the path to the certificate file on the server.
- If you use a separate private key file, add the path in the field below. If the certificate file already contains a private key, leave the field empty.
- Enter the password for access to the private key.
- Restart the server to load the certificate and launch the SSL connection.

Creating a server certificate

Since version 16.0.6, Enterprise Server offers a wizard to create self-signed server certificates. To do so, a valid root certificate of the Certificate Authority (CA) is required. Open the wizard via *Tools → Server certificate*. Here, you have the following options:

- Create a self-signed root certificate
- Use an existing root certificate (recommended)

Create a self-signed root certificate

To create a self-signed certificate for testing purposes, enter all necessary information on the root certificate. Click *Next* and enter all required information on the server certificate. Click *Next* again and enter the domain name and IP address of the server computer. Then, click *Generate* to create the certificate.

Use an existing root certificate

To use an existing certificate, enter the paths to the public and private key files on the server as well as the password, and click *Next*. In the window *Server certificate properties*, enter all required data. Click *Next* and enter the domain name and IP address of the server computer. Then, click *Generate* to create the certificate.

Databases

The Databases area contains all databases available in the Server Manager. Here, you can add new databases to the server, manage or delete existing ones and assign databases to users or groups.

In the main view, you can see all existing server databases as well as their size, the time and date of the last access, the total number of entries and how many users are currently connected to each database.

On the right, the following options are available:

- New database
- Permissions: For more information on permission management, please see the chapter Permissions.
- Properties: This dialog window contains detailed information about a selected database.
- Delete
- Rename
- Select all

TIP: You can also access these options by right clicking a database from the list. Additionally, you can filter the main view. To do so, enter the database name or parts of it to start the search.

Add Database to Server

Databases can be added to the Enterprise Server by going to the Databases area and clicking New database on the right. The dialog window contains the following tabs:

- Add existing database
- Create new database

Add Existing Database

Select this tab to add an already existing database to the server.

- Click the Browse button to find the database.
- Enter the database's correct master password into the Master password field.
- Finally, click OK to finish the process.

NOTE: If you add an already existing database to the server, it will be copied to the server's database directory. The master password of the database is automatically converted to the Server Manager's admin password.

Create New Database

Select this tab to create a new, empty database and save it to Password Depot Enterprise Server. Enter a database name and, if desired, additional comments.

NOTE: Server databases are always encrypted with the administrator password. The clients, however, always use the authentication assigned to them by the administrator to open databases on the server.

Permissions

In the *Permissions* tab, you can manage access rights of users or groups.

In the main window, all users or groups authorized to access a selected database are listed. Below, you can see the effective rights of individual users or groups. If you want to see the effective rights in detail, select a user or group from the list.

If you want to remove database access for a user or group, select the account/group and click *Delete* on the right. Users and groups that have been removed from a database cannot access it anymore. However, they are still available on the server.

Click *Select All* to select all users/groups with access to a database. You can then perform further actions that will be applied to all selected users/groups.

New

Select *New* to add new users or groups to the selected database. Choose a user/ group from the list on the left. Lastly, click *OK* to finish.

Properties

In the main view, double click a user or group. Alternatively, you can also select the user/group and click *Properties* on the right. A new dialog window opens, where you can set permissions at database level as well as for individual folders and entries. The following tabs are available here:

- General
- Entries and folders
- Sealed access

General

The permissions set in the General tab are applied to the entire database. You can see the selected user or group in the upper left corner. If desired, you can add a time limit to a granted access by setting start and end dates using *Valid from* and *Valid to*. On the right, you can see the rights of a selected user/group. The following permissions are available on this tab:

- Access to database
- Read entries
- Modify entries
- Add entries
- Delete entries
- Use the function "Auto-Complete"

- Auto-fill web forms using browser add-ons
- Accept new entries from browser add-ons
- Print entries
- Export entries
- Save local copy
- Synchronize database
- Grant access to other users
- Seal entries
- Set second password
- Grant admin rights

To see the effective permissions of a group or user, click *View effective rights*.

NOTE: Permissions set in this tab apply to the entire database. As is the case with the server policies, undefined or activated rights can be changed on entry or folder level, whereas deactivated rights cannot.

Entries and folders

In the *Entries and folders* tab, you can assign users and groups access rights to individual folders and entries within a database. To do so, select entries or folders on the left. The *Entries and folders* tab includes the following permissions:

- Access to entries
- Read entries
- Modify entries
- Add entries
- Delete entries
- Grant access to other users
- Seal entries

Here, too, you can see the effective permission by clicking *View effective rights.*

TIP: Both on the tab *General* and the tab *Entries and folders*, activated permissions are marked green and deactivated permissions are marked red. Permissions that deviate from the global policies are marked bold.

Sealed access

If a user grants another user access to an entry, they have the additional option to seal this entry. This way, the other user can only access the entry after receiving permission from an authorized person.

This authorized person is chosen by the user sharing the entry. They have to be a user with admin rights on the Enterprise Server. Under *Databases → Permissions*, they can see that the new user has been granted access to an entry, how long this access is valid, and if this entry has been sealed. The status of the seal can be changed under *Properties → Sealed access*. The following statuses are available:

- Sealed: There has been no attempt to access the entry yet.
- Unsealed: The seal has been removed.
- Waiting for approval: The user who has been granted access is asking for permission to open the entry.
- Approval granted: An authorized person has granted permission to access the entry.
- Broken: The entry has been accessed.

Authorized persons can change the seal status at any time. Additionally, they can add other authorized persons who may change the seal status by using *Add*.

For more information on sealed entries, visit our Knowledge Base:
How can I grant access to other users in Password Depot and seal entries?

Database Properties

You can access the database properties by selecting a database in the databases area and clicking *Properties* on the right. Here, you can see the following tabs:

- General
- Advanced

General

Here, you can edit the name of the database. Additionally, you can see the file type, its size, when it was last modified and who is connected to it. You can update this list by clicking *Refresh* or disconnecting selected users by clicking *disconnect*.

Advanced

The *Advanced* tab includes additional features for monitoring user access and activity. Here, you can add a custom password to encrypt the database with. If a database is encrypted with an additional password, its properties and permission can only be accessed by users who know the additional password. To add a custom password, click *Change Settings*. In the dialog window *Change Database encryption settings*, open the drop down menu and select the option Custom password (Permissions management requires verification). You will be asked to enter a new password and confirm it next. Lastly, click *OK* to finish.

If you want to change the custom password, enter the current custom password and open the database properties. In the Advanced tab, click Change settings. Enter the old custom password first and then enter a new password. Click OK to save the new password.

If you would like to delete the custom password and allow for access to the database properties and permissions without an additional password, select the option Administrator password (Automatic access to permissions management) from the drop-down menu. Enter the current custom password. Lastly, click OK.

WARNING: We recommend only setting an additional custom password for a database if it is truly necessary. If the custom password is forgotten, the database will be inaccessible.

Additionally, you can elect to monitor and log all cases of user access to entries in the Advanced tab, as well as force users to specify a reason for deleting an entry.

Users

Administrators can add new users to the server or edit already existing ones in the Users area. However, a user's permissions need to be defined in the Database area by clicking Permissions.

The main view of the Users area displays the following:

- Account
- Authentication
- User Principal Name: Displays a user's UPN in case they have been added to the server by Azure AD synchronization.
- State: Shows whether the selected user account is activated or deactivated, and whether the user is currently connected to the server.
- Roles: For more information on server roles, please click here.
- Address: Displays a user's IP address if they are currently connected to the server.
- Full name
- Email
- Department
- Open database: If a user is connected to the server, this column shows the database a user is working with.

The following options are available on the right:

- New user: Add new, local users here.
- Properties: Open the User properties here.
- Delete
- Disconnect
- Synchronize: You can synchronize selected users with Active Directory or Azure AD individually without launching a synchronization for the entire server. Note that this option can only be used if the user was added via Active Directory or Azure AD in the first place.
- Assign database: Here, you can assign a database to individual or multiple users at a time. Additionally, you can also create a new server database here and assign it to one or more users. In the Permissions tab, you can assign user rights at database level immediately. You can also create private databases for your users here. For more information, see the chapter Assign Database.
- Reset 2FA: If Two-Factor Authentication for the server login is generally enabled, you can choose this option to reset the 2FA settings for one or more users. In this case, the selected users will have to enter the second factor again next time they try to connect to the server.
- Select all

TIP: You can also access these options by right-clicking a user from the list. Additionally, you can filter the main view. To do so, enter a user name or part of it to start the search.

Add users

In Password Depot Enterprise Server, you can add new users to the Server using one of the following options:

- The button *New user*
- Active Directory Synchronization
- Azure AD Synchronization

Add new users manually

You can add new, local users to the Server Manager manually by using the *New user* button available in the *Users* area on the right. These users will connect to the Enterprise Server using their Password Depot credentials. Go to the *Account* tab and select the *Password Depot credentials* authentication. Enter the user name and the password of the user. Click OK to finish.

For the Enterprise Server login, local users will choose the option *Sign in with user name and password* in the Database Manager of the desktop client. They have to enter their credentials, the server IP address and the correct port number in order to access the server.

Add new users via Active Directory synchronization

If you want users to log in on the enterprise Server via the Integrated Windows Authentication (SSO), you have to add them by performing an Active Directory synchronization. You can launch the synchronization wizard by going to *Tools → Active Directory Synchronization.* The user objects will then be imported into the Server Manager from Active Directory. If synchronization was successful, you can see all imported objects in the *Users* area.

In the user properties of Active Directory users, the option On-Premises Active Directory is already checked by default in the Account tab. In the Active Directory DS tab, you can see other Active Directory attributes of a selected user.

For the Enterprise Server login, Active Directory users will choose the option *Integrated Windows Authentication* in the Database Manager of the desktop client.

During authentication, a user's user name and password will be sent to the Active Directory. Depending on whether the data Active Directory is correct or incorrect, login on the Enterprise Server will be successful or unsuccessful. It is therefore important that the user data available in the Server Manager corresponds to the user data in the Active Directory. We recommend performing Active Directory synchronization regularly.

TIP: Find out more about Active Directory synchronization here.

Add new users via Azure AD synchronization

Adding new users to the server via synchronization is required if you want to use Azure AD authentication as well. To do so, go to *Tools → Azure AD Synchronization*. The user objects from Azure AD will then be imported into the Server Manager. If synchronization was successful, all imported objects will be displayed in the *User* area.

In the user properties of Azure AD users, the option Azure Active Directory will already be checked by default in the Account tab. In the *Azure AD* tab, you can see other Azure AD attributes of a selected user.

For the Enterprise Server login, Azure AD users will choose the option *Azure AD* in the Database Manager of the desktop client.

TIP: Find out more about Azure AD synchronization here.

NOTE: You should not enter or edit data in the Active Directory DS or Azure AD tab of the user properties. These attributes are always entered automatically during synchronization, and are only useful if they were added automatically. If a user's Active Directory or Azure AD data has changed, please run the Active Directory or Azure AD synchronization to update their data in the Server Manager.

User Properties

The *User properties* dialog window is available for every user in the Server Manager. You can access the user properties by double clicking or right clicking a user or by clicking *Properties* on the right.

The following tabs are available here:

- General
- Account
- Roles
- Member of
- Advanced
- Azure AD
- Active Directory DS

General

The *General* tab includes the following information:

- Full name
- Email
- Phone
- Department
- Description

Account

Authentication

Here, you can see the different types of authentication available for the server users:

- Password Depot credentials
- On-Premises Active Directory
- Azure Active Directory

If you select the authentication via Password Depot credentials, administrators have to define a specific user name and password for each user, which they will then have to share with their users. If enabled in the Server Manager, users can change their user names and passwords afterwards. For more information, please visit the following knowledge base article:

How to change the password for the Enterprise Server login

The On-Premises Active Directory authentication is the so-called Integrated Windows Authentication (SSO). It requires a full Active Directory synchronization with the Server Manager. For more information, please see this chapter.

When using the Azure Active Directory authentication, users log on to the Enterprise Server with their Microsoft credentials. This authentication requires a full Azure AD synchronization. For more information, please see this chapter.

Account options

- Account deactivated: If this box is checked, the account of this user has been locked temporarily. Uncheck the box to reactivate the account so the user can access the server again.
- User may not change password: Check this box if you do not want local users to change their password. Please note that this can only be used if a user accesses the Enterprise Server via Password Depot credentials.
- User must change password at next logon: Check this box if you want to force local users to change their password next time they want to connect to the Enterprise Server. Note that this can only be used if a user accesses the Enterprise Server via Password Depot credentials.
- 2-Factor Authentication deactivated: Check this box if you want to deactivate 2-Factor authentication for a specific user.

Roles

With version 15, additional server roles were implemented. This way, you can assign specific server roles to one or more users. Thus, server administration can be carried out by multiple users. Users with additional roles can access both the Server Manager and the Enterprise Server using a client. The following server roles are available:

- Server Administrator: This role grants full access to the server and Server Manager.
- Database Administrator: A database Administrator can create and manage databases as well as users' access rights.
- Account Administrator: An Account Administrator can add and manage users and groups.
- Active Directory Operator: An Active Directory Operator can perform Active Directory or Azure AD synchronization in the Server Manager. Please note that this server role additionally requires the Database or Account Administrator role.
- Event Log Reader: An Event Log Reader can access the server logs.

NOTE: The introduction of different server roles in the Server Manager meant that the super administrator is now only used for server administration in the Server Manager. Thus, the super administrator is not a classic user account anymore. They can only log into the Server Manager, but not into the client. Therefore, they are not part of the total number of users available on the server.

Member of

Here, you can find a list of groups a user is a member of. In addition to their names you can see their types and descriptions. By clicking *Add group*, you can add new groups to this list. By clicking *Delete,* you can remove groups from this list.

Advanced

Web Sockets port for browser add-ons

Here, administrators can define the web sockets port settings for the browser add-ons. The following options are available:

- Use global settings [25109]: If you select this option, all clients will use this port number to communicate with the browser add-on.
- Auto-generate unique port number: Activate this option if you want to automatically assign individual port numbers to each user on the server. Users can then see their port number in the desktop client by going to *Edit* → *Options* → *Browser*.
- Use custom port number: Administrators can assign custom port numbers to their users and define specific port numbers themselves. Users can see the custom port number in the desktop client by going to *Edit* → *Options* → *Browser* in this case as well.

IP address verification

Here, you can assign a fixed IP address to a user. Every connection attempt of this user with a different IP address will then be rejected. This can increase security, but it requires using static IP addresses.

Azure AD

This tab contains all Azure AD attributes of a user who has been added to the Server Manager via Azure AD synchronization.

- User Principal Name: Here, you can see the User Principal Name if the user has been added via Azure AD synchronization.
- Object ID: Every Azure AD user is assigned a specific object ID. It will be displayed here after Azure AD synchronization.
- User Type: You can see the user type of a user who was imported from Azure AD here. Azure AD has two types of users: members and guests. Members belong to your own organization. A guest can be invited to your organization temporarily.

Active Directory DS

This tab contains all Active Directory attributes of a user who has been added to the Server Manager via Active Directory synchronization.

- Logon Name: Displays a user's user name that is used for the domain login.
- User Principal Name: The User Principal Name displays the name of the Active Directory system user in email format.
- ADs Path: Displays a user's path in the Active Directory.
- Object GUID: Displays the ID of an Active Directory user, which is generated automatically.

NOTE: The information in the tabs *Azure AD* and *Active Directory DS* is only relevant if users have been added via Azure AD or Active Directory synchronization. During synchronization, the users' attributes will be added to the Server Manager automatically. Please do not enter any data manually.

Assign Database

The *Assign database* option is located in the *Users* and *Groups* area on the right. Here, you can assign a database directly to users or groups and manage their permissions. You can either use an existing database or create a new one.

The following tabs are available here:

- Database
- Permissions

Database

- Selected accounts: Displays the users or groups you would like to assign a database to.
- Select an existing database
- Create a new database
- Create a private database: Here, you can create private databases for each of the selected users or groups. They indclude the name of the user or group they belong to and are only accessible to this user or group.

Permissions

Here, you can manage the permissions for the databases that you want to assign to users or groups. In this case, all selected users or groups are granted the same permissions. For a more detailed permission management, use the *Permissions* **option of a database**.

Groups

In the *Groups* area, administrators can add new groups and manage existing ones. A group consists of one or more members (i.e. users). Creating groups can make permission management easier by allowing you to grant rights to entire groups instead of individual users.

In the main view, you can see the following information on each group:

- Name
- Type: Password Depot Enterprise Server distinguishes between standard, i.e. manually added local groups, Azure AD groups and Active Directory groups.
- Domain: Displays the Root Domain Name of the domain that was selected during server configuration and that is used for Active Directory synchronization.
- Description

Additionally, the following options are available on the right:

- New group
- Properties
- Delete
- Synchronize: Allows the synchronization of individual groups with Active Directory or Azure AD without having to start a synchronization for the entire server.
- Assign database
- Select all

Adding Groups

There are three ways in which you can add groups to the Enterprise Server:

- by using the button *New Group*
- via Active Directory synchronization
- via Azure AD synchronization

Adding new groups manually

You can add new groups to the Server via *Groups* → *New group*. Name it and add, if desired, additional properties. Please note that the type of manually added groups is always *Standard*, which cannot be changed. Add users to the group on the tab *Members*. On the tab *Member of*, you can turn this group to a subgroup of another group.

Via Active Directory synchronization

Password Depot Enterprise Server allows you to import existing groups from Active Directory. With Password Depot 17, nested groups are supported as well. Go to *Tools* → *Active Directory synchronization* to launch the synchronization. If it was successful, you will see all imported objects in the *Groups* area afterwards.

Groups that were added by Active Directory synchronization automatically include the corresponding Active Directory members. If a group receives access to a database on the server, the members of this Active Directory group can log in on the Enterprise Server using the Integrated Windows Authentication (SSO).

Find out more on the Active Directory synchronization here.

Via Azure AD Synchronization

In order to import group objects from Azure AD, launch the synchronization under *Tools* → *Azure AD synchronization.* If it was successful, you will see all imported Azure AD objects in the *Groups* area afterwards.

Groups that were added by Azure AD synchronization automatically contain the corresponding Azure AD users. If an Azure AD group receives access to a database, the members of this Azure AD group can log in on the Enterprise Server using the Azure AD authentication.

Find out more on the Azure AD synchronization here.

Group Properties

You can open the properties of a group by double-clicking it or selecting it and clicking *Properties* on the right. The following tabs are available here:

- General
- Members
- Member of

General

Here, you can see the following information:

- Name
- Email
- Description
- Type: Password Depot Enterprise Server distinguishes between standard, i.e. manually created local groups, Active Directory groups and Azure AD groups. This is the only property that cannot be changed.
- Disabled: Deactivates a group, for example if it is not needed for a while.

Members

Here, you can see and manage members of a group. By clicking *Add...*, you can add users or subgroups to the group. If you select the arrow button, you can add users by department. If you select a member and click *Delete*, the member will be removed from the group. Note that they will not be deleted from the server, only from the group.

Member of

Here, you can turn a group into a subgroup of another group. By clicking *Add...*, you can choose a super-group. By clicking *Delete*, you can remove a super-group from this list. Note that this super-group will not be removed from the server. It is only no longer the super-group of this group.

Notifications

In the *Notifications* area, you can define which server events you would like to be notified of. In the main view, the following information is available:

- ID: Each notification has its own ID. They are numbered according to the order in which you added them.
- Type: Describes the event in which the notification is sent.
- Notes
- Recipients

On the right, you have the following options:

- New notification
- Properties
- Delete
- Select all

New notification

You can add new notifications to the Server Manager under *Notifications* → *New notification*.

To do so, select an event you would like to be notified of first. Add notes if desired.

Then, define a recipient of the notification. To add a recipient, enter an email address in the field on the bottom left and click *Add*. To replace a recipient with another, select the recipient you would like to replace, enter a new email address on the bottom left and click *Replace*. To remove a recipient, select them and click *Delete.* Click *OK* to finish the process.

Notification properties

Here, the following tabs are available:

- General
- Advanced

General

- Event
- Notes to include in notification
- Send email notification to recipients

Advanced

Depending on which event the notification was created for, you may have further options available on this tab.

Users and groups

- All users and groups: Select this option if you want the notification to be triggered by all users and groups on the server.
- Selected users and groups: Here, you can choose individual users and groups to trigger the notification.

Objects

- All databases: Select this option if you want the notification to apply to all databases on the server.
- Selected databases: Here, you can choose individual databases the notification applies to.
- Selected entries: Here, you can choose individual entries the notification applies to.

Log

Here, you can view a log of the activities on the server.

The sever logs have a standard format according to RFC 5424 for ease of processing in external log analyzers. Server logs can optionally be sent to external log servers for revision-proof processing and saving in real time via UDP. You can make further adjustments to the log settings in the server settings.

In the main view of the *Log* area, you can see the following information:

- Severity: Here, you can see the type of the log entry.
- Date and time: Displays the exact point in time when a server activity was registered.
- User name: Displays which user performed a server activity.
- Address: Displays the IP address from which an activity was performed.
- Event ID: Each registered event has a unique event ID.
- Event description: Here, you can see what activity was performed.
- Database: Displays the database in which an activity was registered.
- Object: Displays which entry or folder was accessed.
- New Object: If an object was updated, you can see the results here.
- Reason: If an error is registered, the reason why it occurred is listed here. Additionally, if you enforce the naming of a reason for deleting entries or folders, these reasons will be displayed here as well.

On the right, you have the following options:

- Open log: Allows you to open a log file directly in the Server Manager.
- Export log: Allows you to export the server log into an XML or CSV file.
- Advanced filter: Allows the detailed filtering of the log entries.

By using the search function in the top left, you can search the log for specific events.

Event IDs

In the server log, different events are tagged with IDs. You can learn what each ID means in this article.

IDs starting with 1 concern the client.

- 101: Log on with a client application.
- 102: Log out of a client application.
- 103: A list of available databases was sent.
- 104: A user password was changed.
- 105: Connecting to the server.

IDs starting with 2 concern databases.

- 201: A database was sent to a user.
- 202: A database was closed by a user.
- 203: A database was opened by a user.
- 204: A database was exported.
- 205: A database was printed.
- 206: A database was updated.

IDs starting with 3 concern entries.

- 301: An entry was locked.
- 302: An entry was unlocked.
- 303: An entry was updated.
- 304: A new entry was created.
- 305: An entry was accessed.
- 306: An entry was deleted.
- 307: An entry was moved.
- 308: Approval was requested for a sealed entry.
- 309: The seal on an entry was broken.

IDs starting with 4 concern folders.

- 403: A folder was updated.
- 404: A folder was created.
- 405: A folder was deleted.

IDs starting with 5 concern documents.

- 501: The content of a document was received by a user.
- 502: The content of a document was sent to a user.
- 503: A document was deleted.

IDs starting with 6 concern server management.

- 601: Log on from the Server Manager.
- 602: Log out of the Server Manager.
- 603: A new database was installed on the server.

- 604: The default server policies were modified.
- 605: The database properties were modified.
- 606: A group was created or modified.
- 607: A notification was created or modified.
- 608: A user was created or modified.
- 609: A database was deleted from the server.
- 610: A user was deleted from the server.
- 611: A group was deleted from the server.
- 612: A notification was deleted.
- 613: A user disconnected from the server.
- 614: The server was paused.
- 615: The server was continued.
- 616: A license key was installed.
- 617: The server options were modified.
- 618: The database was read by the admin.
- 619: The Active Directory was read by the admin.
- 620: The two-factor authentication of a user was reset.
- 621: The server was restarted.
- 622: A permission was deleted.
- 623: A user or group was added to a database.
- 624: The password of a database was changed.
- 625: A list of users was sent to the admin.
- 626: A list of groups was sent to the admin.
- 627: Information on the server was sent to the admin.
- 628: The server log was sent to the admin.
- 629: A list of databases was sent to the admin.
- 630: A list of notifications was sent to the admin.
- 631: The server policies were sent to the admin.
- 635: Information on the mirror was sent to the admin.
- 636: A mirror was set.
- 640: A tenant was updated.
- 641: A tenant was added.
- 642: A tenant was deleted.
- 643: A certificate was generated.

IDs starting with 7 concern Active Directory.

- 701: The Active Directory synchronization was started.
- 702: The Active Directory synchronization was stopped.
- 703: An error occurred while synchronizing with Active Directory.
- 704: An object was disabled by synchronizing with Active Directory.
- 705: An object was deleted by synchronizing with Active Directory.
- 706: An object was added by synchronizing with Active Directory.
- 707: An error occurred while adding a user by synchronizing with Active Directory.
- 708: An object was updated by synchronizing with Active Directory.

IDs starting with 8 concern backups.

- 801: The backup status was sent to the admin.
- 802: A database was updated from a backup.
- 803: A database backup was sent to the admin.

User permissions

In addition to using multiple databases, Password Depot Enterprise Server allows for the use of one central database accessible to all users. By managing user permissions, administrators can structure this database in such a way that each user can only view and access what they are meant to.

NOTE: Permissions for users can also be applied to groups in the same manner as described in this chapter.

How does permission management work on the Enterprise Server?

On the Enterprise Server, you can set permissions on three levels:

- on a server-wide level
- on a database level
- on an entry and folder level

Users only have rights that were explicitly granted to them. If a permission is undefined or deactivated, it does not apply. The principle of inheritance applies here: Settings defined at a higher level are also valid at a lower level. Activated or undefined permissions can be changed at a lower level, whereas deactivated permissions cannot.

The following sections will explain permission management on each level in more detail.

Permission management on a server-wide level

Under *Manage → Server policies*, you can define global permissions that apply to all users on the entire server. You can set the permissions to *Enabled, Disabled* or *Not defined*. Since permissions that were disabled on this level cannot be enabled on a database, entry or folder level, we recommend keeping the default settings for the server policies and managing user permissions primarily in the *Databases → Permissions* area.

Permission management within a database

Under *Databases → Permissions*, you can grant detailed rights to users and groups.

If you have multiple users or groups that have access to the same database, but are supposed to have different views of its contents, you should

- remove the checkmarks from the permissions *Read/Modify/Add/Delete* in the *General* tab
- select precisely those objects you would like to grant users or groups access to in the *Entries and folders* tab

NOTE: Please do not deny the *Read/Modify/Add/Delete* permissions in the *General* tab if a selected user/group is meant to have access to entries or folders in this database, but only remove the checkmark for *Allow*. Otherwise, the user/group will be able to access the database, but not to view or edit its contents.

In permission management on a database, folder or entry level, allowed permissions are marked green, while denied permissions are marked red. Additionally, you can view the effective permissions of a user or group.

For further information on permission management on the Enterprise Server, along with examples, please visit our knowledge base:

How do I have to set the user permissions to ensure they can only see those objects they are allowed to access?