PASSWORD DEPOT
BY AceBIT

User Manual Password Depot Enterprise Server 17

Introduction

Password Depot Enterprise Server is an extension for Password Depot. With the Enterprise Server users can share databases stored to a server. The desktop client for Windows is the main program which is also used for Enterprise Server connection. Apart from that, you can also access the Enterprise Server with our macOS edition or mobile apps (Android & iOS). In addition, you can also utilize our web interface, which provides you with a convenient and straightforward access to the Enterprise Server, regardless of the device or operating system you're using. Server databases can be opened and modified using one of these clients.

Password Depot Enterprise Server is installed on a computer within the local network or in the cloud via Azure. The server administrator is mainly working with the Server Manager, a separate tool for Enterprise Server management and configuration. In the Server Manager the administrator can create new databases, add users and groups to the server and assign them databases. Users can get access to entire databases or parts of it only.

In general, you can provide access to a server database to multiple users and define different access rights for your users within the same database. In this case, every user will have a different view of the provided database.

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 user's access data is defined by the administrator. Login to the Enterprise Server can either be performed with a local user (username & password), through Integrated Windows Authentication (SSO) or Azure AD Authentication.

Apart from that, the administrator can define further server settings in the Server Manager, for example installing a certificate if an SSL connection is required, activate 2 Factor-Authentication, set up notifications for specific events and define global server policies etc.

All transferred data is always 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 is an On-premises software.

Watch our video to learn more about Password Depot Enterprise Server and how it can help and 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

Installation and Running

Ideally, the network administrator will install Password Depot Enterprise Server on the server computer of the local network. However, it is also possible to install the Enterprise Server 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 (for testing purposes, for example) also on your local computer. To access the server using the Password Depot desktop client, you can use the server addresses 127.0.0.1 or localhost (in any case you can also enter the server's IP address).

Installation as Windows Service or Windows Application

You can run Password Depot Enterprise Server in two modes:

- as Windows Service
- as Windows Application Server

By default, the installation is performed as Windows Service. Select the option Windows Application Server if you would like the server to be installed as Windows Application Server.

NOTE: We recommend performing the Windows Service installation since the Password Depot server service will be set up automatically in the background during installation.

If you have installed the Enterprise Server as Windows Service, the server will be listed as Password Depot Enterprise Server. The service is then always running in the background and normally Password Depot Enterprise Server starts automatically upon Windows startup. If you set up the server to run as 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 server service in the Windows services dialog window.

If you have installed the server as 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 onwards Password Depot Enterprise Server supports the 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, for example. The server's installation setup will install the Server Manager automatically. Thus it will be accessible on the same machine the server service is running, too.

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

User name: Admin

Password: admin

NOTE: We strongly recommend changing the administrator's default access credentials (that is the Super Administrator's 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 (Password Depot credentials).

For the Server Manager login the server's IP address is required (the IP address of the server on which the Enterprise Server is running) as well as the correct port number. In version 16 the correct port number is 25016 by default.

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

Updates

If you launch the Server Manager and go to Help → Search for updates you can check if any updates for the Enterprise Server and Server Manager are available. If you can see here that a new build has been released, we recommend installing it as soon as possible to keep the software up to date at all times. In this context, please take into consideration the following:

The Server Manager does not contain an integrated update manager. You can only check here if new updates within the same main version are available but cannot download them right away. New server updates can therefore only be downloaded from our website. After download you can launch the installation wizard to start the installation. When installing smaller updates within the same main version you do not need to stop the server service.

Migration

If you have already worked with an older Enterprise Server version and would now like to upgrade it to a new main version, you can easily migrate the server. Please note the following:

The Enterprise Server can only communicate with Windows clients of the same main version. This means that you cannot access the Enterprise Server of version 15x using a Windows client of version 12x and vice versa. Therefore, you always need to upgrade both, your Windows clients and the Enterprise Server to the new main version at the same time.

This is different concerning the macOS, Android and iOS editions. From version 15 onwards you can also connect to older Enterprise Server versions (for example, connecting with the iOS app of version 16 to the Enterprise Server of version 15, 14 or 12). To do so, upon connect you have to select the correct main version in the login dialog window. The port will then be changed automatically according to the selected main version.

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 instructions on how to migrate the Enterprise Server step by step and we recommend, following the instructions carefully to avoid problems. If you carry out the migration step by step, the whole process should only take some minutes. You can find the detailed instructions here:

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

NOTE: You can also follow the instructions in our knowledge base if you want to move your current server installation to another machine/server. The procedure is the same as when migrating the server to a new main version. The only difference is that you will have to install your current main version of the server on the new machine, too. The directories on the new server will then correspond to the directories on the old server

(provided you use the default directories). Basically, you only have to install the Enterprise Server of the same main version on the new machine and afterwards, copy your databases and the cfg file to the new server as described in our knowledge base.

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

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

Running Password Depot on a Terminal Server

In general, you can also run Password Depot on a terminal server. It is not recommended in general, however, it is possible though.

The installation of Password Depot on a terminal server is the same as installing it on a physical server. We recommend, following the instructions of the installation wizard carefully. If so, the installation should take a few minutes only.

As far as licensing is concerned, there is also no difference but it is the same either using Password Depot on a terminal or physical server. You can find detailed information about our licensing in the knowledge base:

Licensing and Maintenance

What do you have to know when running Password Depot on a terminal server and activating the browser add-on?

If multiple users have access to Password Depot on a terminal server and the browser add-on is activated, too it is mandatory or, at least, strongly recommended assigning individual port numbers to the users. If this, however, is not the case it may happen that user A receives the login data of user B since the browser add-on does not "know" which user is requesting the data. This may be a serious security issue because data may be sent to users who should not see or know about it at all. The socket port number for browser add-on communication is not a virtual but physical parameter and thus, cannot be shared by multiple instances of the Password Depot client.

How to assign individual port numbers to the users?

You have two options to choose from:

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 the corresponding user next. Open the user properties by double clicking on the user and go to the **Advanced** tab. You can see here the **WebSockets port for browser add-ons section**. Check the option **Use custom port number** and define a custom value for each user.

The users can see their individual port numbers (either automatically generated ones or manually assigned by the administrator) in the client by going to **Edit → Options → Browsers**. To complete the process, users finally have to change the port number in the browser, too since this cannot be changed automatically. They can enter here the custom port number which is displayed in their client. To do so, click the add-on icon in the browser and go to **Settings**. Afterwards they can 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?

Server Manager

The Server Manager is a separate tool which provides quick and easy access to all features for maintenance and configuration of Password Depot Enterprise Server. You first have to connect to the Server Manager with the super administrator's access data to see the features described below and start with the server configuration.

WARNING: Only the super administrator or other people authorized to access the Server Manager and perform server configuration should know the admin password. Please note that anyone knowing the adminstrator's password will have access to the Server Manager which means that they will also have access to the server administration!

The Server Manager's navigation area is divided into five sections:

- Databases: This section is used for creating new databases on the server. Besides, you can manage new databases as well as already existing ones.
- Users: This section includes features for managing the users on the server. You can add new users to the server here or manage already existing users.
- Groups: In this section you can create new groups and add new users to these groups. Besides, you can manage already existing ones.
- Notifications: In this section you can set up email notifications for certain events.
- Log: This section displays any server activity of the users and groups.

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

- Status: You can see here if the server is running or if it has been paused.
- Server address: Displays the server's IP address.

- Server port: Displays the default port number which is used for Enterprise Server connection.
- Running since: Displays the date the server has been put into operation for the first time.
- Server version: Displays the latest server version or server build of the current main version.
- Updates available: You can see here if new updates within the same main version are available for installation.
- Installed licenses: Displays the number of users allowed on the server at maximum (server size).
- Registered users: Displays the number of users already registered on the server.
- Connected users: You can see here 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 activated server mirroring in the Manage area the state of server mirroring is displayed in the Server Manager's main view.

NOTE: In case you may forget the password for the Server Manager login you will have to perform a workaround to get access again. Should this case arise, please read the following instructions carefully: How can I "reset" the administrator's password in Password Depot Enterprise Server?

Manage

This menu item can be found at the top on the right in the main view of the Server Manager. It contains the following features:

- Server settings: You can define basic server settings here, for example when to create backup files and where to store them, supported authentications or if Two Factor-Authentication should be mandatory for a client to server connection etc.
- Server license: Here, you can enter a new license key, for example if you would like to increase the total number of users on the server. Apart from that, you can also see here the current server license and version.
- Server policies: Here, you can set global default server policies that will be applied to the entire server. The global server policies have an impact on the assignment of user permissions in general, the password policy as well as supported types of entries. Please note that all server policies are global permissions that will always be applied to the entire server and all users. Thus, any policies set here cannot be changed in the database permissions afterwards. For example, if you deactivate specific policies in the Permissions tab, you cannot activate them for single users afterwards. Therefore, please be careful when using the server policies since they have restrictive effects. In general, we recommend setting them to Enabled or Not defined.
- Client security policies: The Client security policies are deployed if the Corporate Client is used. In this case, administrators can define even more settings and permissions and deploy them to all users which is not possible with the standard client. For more information about the Corporate Client and the Client security policies please click here.
- Mirroring: Select this option to activate server mirroring of your Password Depot Enterprise Server.
- Pause: Here, you can pause/stop the server service. With the service stopped, clients cannot connect to the server anymore. The Server Manager, however, is still available so that administrators can do maintenance.
- Continue: If the server service was stopped, you can start it again by clicking this button. Afterwards, the server will be available again for all clients within the same network.

- Restart: Select this option to restart the server if necessary.
- Program options: Here, you can define the program options (please note that the program options are different from the server settings). The program options refer to the Server Manager only, for example you can define here the language of the Server Manager's user interface.
- Exit: You can exit and shut down the Server Manager. The service or server application, however, is not affected. Thus, users will still have access to the server and its databases.

NOTE: Some changes on the Enterprise Server may require a server restart in order to save changes. With version 15 a command for restarting the server has been implemented. The prompt will be displayed automatically if needed. If so, we recommend carrying out the restart subsequently.

Server Settings

The Server settings dialog box can be found in the menu item Manage. It includes the following tabs: General, Connections, Logging, Backups, Additional, Email, 2FA Settings, Active Directory and Azure AD. In general, you can use the server settings for server configuration and defining settings that will affect the entire server and all users. The content of the single tabs available in the server settings is explained in detail below.

General

Server

You can define basic server settings here:

- Server language: You can select the language of the server (not the language for Server Manager's user interface!). You can choose between English, German, French, Spanish and Dutch.
- Server port: You can define the port number for the client to server connection. In general, the default port number is always displayed here but you can change the value if required. When changing the port number, please make sure to also change it in the client and use the correct port for your server connection.
- Internet Protocol: Here, you can specify a specific Internet protocol version that should be used by default. The following options are available: IPv4+IPv6, IPv4, IPv6. So, depending on the network configuration administrators can define which Internet protocol versions the server should support. The server will then send via UDP an info message to the clients about the supported Internet protocol version. Afterwards, the clients will automatically choose the correct version for the main TCP connection.
- 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. A new dialog window will open where you will have to specify the correct path for your certificate file and its private key. Besides, you will also have to enter the certificate's password here.
- Keepalive enabled: You can activate the Keepalive feature if clients connect to a server which is not part of the same local network.

WARNING: In case you decide to change the default port, make sure that it is not used by any other application.

REST Server

- Origin URL: Enter the correct URL of your Password Depot web server. It should be the exact URL which is used for addressing your Enterprise Server through the Password Depot web interface.
- Use SSL/TLS for REST Server: You can activate the SSL/TLS connection during REST Server connection. Because of the REST Server implementation you can now also access the Enterprise Server via REST API. A new web interface is available in the source code for the purpose of demonstration or productive use. It is basically a web server which can use both the HTTP and HTTPS (recommended) protocol. To use HTTPS a valid certificate is required on the server. Please click Install Certificate for installation.

HINT: For more information about 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

- Storage folder: You can specify the path where server databases are stored to by default. This is C:\Program Files\AceBIT\Password Depot Server 15\Data\DB in Password Depot 15. You can change the path, however, we always recommend storing the databases to the local drive instead of using a network share or mapped drive since the latter may not be accessible at all times. If, during the process of saving the database, Password Depot Enterprise Server cannot find or access the path specified in the server settings it will switch back to the default settings and save the databases to the default folder.

Connections

Supported authentications

Here, you can define the supported authentications on your server. You can choose between the following options: User credentials (account and password), Integrated

Windows Authentication (Single Sign On) and/or Azure Active Directory. The server supports activating more than one authentication mode at the same time.

HINT: For more information about 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

Check all the clients that should support the Enterprise Server connection. The following options are available here:

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

NOTE: All clients supposed to be used for Enterprise Server connection need to be activated in the Server Manager. If a client is deactivated here, users won't be able to use the disabled edition to connect to the Enterprise Server

New connection from different device

You can decide how you would like to proceed with connections carried out by the same user but from other devices. You can choose between the following:

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

NOTE: As is the case with many other similar servers, it is not recommended with the Enterprise Server either to allow multiple connections carried out by the same user at the same time. This feature was implemented since it may happen that users need to connect with their desktop client and a mobile device simultaneously. This works

because mobile devices are not synchronized with the server in real time. However, if a user tries to establish a server connection using their account on two different Windows clients at the same time, this may cause problems. It may happen that the user will get disconnected from one device at least.

Inactive sessions

Specify how Password Depot Enterprise Server should handle inactive connections. For example, you can define that clients should be disconnected from the server after a specific time of inactivity. In addition to that, that is if you activate this option, you can also specify that the database should be closed and users should be logged out.

Logging

In this tab you can define anything referring to the logs of Password Depot Enterprise Server. The following options are available here:

Local log

- Logs folder: You can see here the default directory for storing the Enterprise Server's logs which is C:\Program Files\AceBIT\Password Depot Server 15\Logs. You can change the location using the browse button. In any case, we recommend always using a local directory, if possible.
- Max. file size (KB): Determine the maximum size (KB) of the server's log file.
- Create new log file: Select a time when to create a new log file.
- Delete logs: Define the settings for deleting already existing logs. You can either select never deleting any log files or determine a maximum number of log files to be kept, 30 for example (this is the default value). This means that the latest 30 files will be saved and older log files will be deleted automatically.

Remote log

- Send log messages to a remote server: Check this box if you wish to activate the option and send the Enterprise Server's log files to external log servers. You can specify the server address and port of the external server where the log files should be sent to. Thus, you can ensure that protocols are not being manipulated.

Backup databases and settings

In this tab you can specify the settings of your backup files in general. The following options are available:

Backup

- Backup folder: You can specify where backup copies of your server database should be saved to. By default, they are stored to the directory C:\Program Files\AceBIT\Password Depot Server 15\Backups\. Use the browse button to change it. However, as is the case with the server's log files too we also recommend always using a local directory for storing the backup files, if possible. The server backup files include your databases, logs and the server's configuration file (pwd_srv.cfg) where the users, permissions and server configurations are saved to.
- On every startup: Select this option in order to create a new backup copy 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 (that is once in 24 hours). Since version 17.0.5 you also have the option to choose between the following options: Monthly, Weekly, Daily, Hourly (this option allows you to specify an interval within a certain time frame).

Delete old backups

- Limit number of stored backups to: This option allows you to set the maximum number of backups.
- Delete backup files older than: Activate this option if you would like to automatically delete backup files older than x months from the server's backup directory. You can determine a specific period of time for this deletion to take place.

NOTE: By default, the options Backup databases on every startup and Backup databases every x hours are checked and we strongly recommend to keep both options activated at all times.

Backup log

- Log backups to file: If you activate this option, Password Depot Enterprise Server will create a log of all generated backups and save it to the specified file. At a later point of time, this will help you to track the times server backups were created.

Additional

The Additional tab contains more options including the following:

Editing entries

- Lock entry timeout (min.): You can determine a specific lock entry timeout (min.) here. By default this is five minutes, however, you can increase or decrease the lock entry timeout, if required. If a user has opened an entry but is not working with it, this specific entry will then be locked automatically if the timeout set up in the Server Manager has expired.

Private databases

- Automatically create private databases for new users: You can determine whether a private database should be created automatically for every new user on the Enterprise Server. Those private databases will then also be stored to the server and users can add their own private entries there which are not supposed to be part of the company's server database. Private databases will be displayed as Private_DB_<USER→.pswe in the Database area.
- Automatically delete private databases for deleted users: You can further determine whether private databases should be deleted automatically from the server once the user a private database has been assigned to is removed from the Enterprise Server. If this option is activated and a user is deleted in the Server Manager, their private database will be deleted from the server, too and thus will no longer be available on the server.

NOTE: By default both options are deactivated.

WebSockets port for clients

- Use default port number: The add-on's default port number is 25109. It is checked in the server settings by default. If the browser add-on is activated, port 25109 is used for communication and users do not need to adjust their settings since port 25109 is also set in the browser by default. However, if required, this port can be changed. In any case, please note that users will then have to change the port number in the client (Edit -→ Options -→ Browsers -→ WebSockets port) and the browser itself.
- Auto-generate unique port numbers (recommended for Terminal Servers): As you can see from the description, this option is strongly recommended when using Password Depot on a terminal server. Since all users work on the same system when using a terminal server it must be ensured that each user is assigned a unique port number for the communication with the add-on. The socket port number is not a virtual but moreover physical parameter and therefore it cannot be shared by different instances of the Password Depot client. If you do not use individual port numbers for each client, problems will definitely occur since Password Depot can not know where to send the access data requested by the add-on. It may happen, in this case, that User A receives access data from User B even though he has no access rights for such entries. Therefore, when using a terminal server, it is mandatory, in any case, assigning individual port numbers to each user who is to work with Password Depot on the terminal server. For best practice, you can check the option Auto-generate unique port numbers (recommended for Terminal Servers) in the server settings and use it by default on the Enterprise Server. In this case, each user on the server will be assigned a separate port number automatically and it will not be necessary to adjust the port number for each user individually.

HINT: For additional information please have a look at the following knowledge base article: How do I change the port number when working with the add-on and using Password Depot on a terminal server?

Failed logins

Here, you can determine a maximum of failed login attempts a user can carry out before his server account will be blocked temporarily. If a user account was blocked, it can be re-activated again by the server administrator. To do so, open the Server Manager and go to Users → <USERNAME→ → Accounts and uncheck the box Account deactivated.

NOTE: A user's failed login attempts will not be reset after some hours or days but the Password Depot Server Manager will remember the number of failed login attempts and add them up. However, if a user enters the correct password after two failed login attempts (provided the maximum number of failed login attempts is set to 3 in the Server Manager) the previous failed attempts will be deleted and everything will be reset to 0. Next time the same user wants to login on the Enterprise Server again he will have another 3 new login attempts until his account will be blocked again etc.

Email

In this tab you can define email server settings:

- Sender: Here, you can enter the sender's email address and name.
- Outgoing Mail Server: You can configure the outgoing mail server.
- 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

In this tab, you can activate Two-Factor Authentication on the server for the users.

Operation mode

- TOTP - codes are generated by mobile Authenticator apps: Users will receive the second factor for the login on their smartphone in their authenticator app.
- Email - codes are sent by Server to user's default address: Users will receive the second factor by separate email to their individual email address.
- Users may choose to remember their devices (days): You can specify a certain period of time during which users can trust connections to a specific device. In this case, regarding Two-Factor Authentication, it will not be necessary for users to always enter a new code each time they want to connect to the same device (=server) in x days provided that users enable the option Trust this computer when connecting for the first time and entering the required code once.
- Email code expiration time (minutes): This option determines the validity of a code sent by email for Two-Factor Authentication. By default, this is ten minutes. However, this time can be changed here by the server administrator. If a user does not enter

the required code in time, it expires. For authentication, a new code will then be required.

HINT: Please visit our knowledge base to get more information about the Two-Factor Authentication.

NOTE: Both the Integrated Windows Authentication and Password Depot credentials authentication support Two-Factor Authentication. Go to Users → <USERNAME> → Account if you want to deactivate the Two-Factor Authentication for single users, if required. Besides, you can also reset 2FA for single users in the user area if problems occur. Read more about this feature in the chapter Users.

Active Directory

Synchronization

- Automatically run synchronization with AD every: Specify whether to perform AD synchronization automatically. If so, you can also determine the time interval automatic AD synchronization should be carried out. Furthermore, you can also specify what to do with users and groups not (or no longer) found in AD. Those users can be ignored, deactivated or deleted in the Server Manager. Please note that this option does only affect the users on the Enterprise Server but not in the Active Directory in general since Password Depot Enterprise Server cannot change anything in Active Directory.

NOTE: The administrator should perform AD synchronization manually, if required. However, if automatic synchronization is necessary, synchronization cycles should preferably be at times when the server load is low, for example once in 24 hours.

NOTE:The server option Automatically run synchronization with AD every is limited to 60 minutes and uses the server's own SYSTEM account.

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 next and login with the administrator's access data. After the login you can see the organization in the Tenants area which means that it has been added to the Server Manager successfully. Now, select Tools → Azure AD Synchronization in the Server Manager to automatically synchronize Azure AD users with the Enterprise Server. You can select the desired organization to perform Azure AD synchronization from the corresponding synchronization wizard.

HINT: You can launch the same process directly by going to Tools → Azure AD Synchronization. The button New for adding a new organization to the Server Manager is also available here.

- 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 if you do not need them anymore, for example. You can then add new or other organizations for Azure AD synchronization to the Server Manager by clicking the button New.

NOTE: Find out more about Azure AD synchronization in the Server Manager in the chapter Azure AD Synchronization which can be found under Tools.

Synchronization

- Automatically run synchronization with AD every: As is the case with the Active Directory synchronization, you can determine here too if Azure AD synchronization should be performed automatically every x minutes. Azure AD users and their attributes will then be synchronized and updated automatically according to the specified time interval. The option User and groups not found in AD does work in

the same way it does during Active Directory synchronization. The only difference is that it actually refers to Azure AD and not the Active Directory.

Server License

If you open the Server Manager and go to Manage → Server license a new dialog window opens where you can enter a new license key. Apart from that, you can also see here the current server license and version. If you have increased the total number of users on the server by purchasing a new license, you can also enter the new unlock code here and increase the number of supported clients accordingly.

Licensing

You can find all server sizes and prices as well as further information about our licensing on our website by clicking the link below:

Purchasing and licensing information

Server Policies

The **Server Policies** can be accessed through the **Manage** menu.

Through the server policies, you can make some **global settings** that among other things affect the **granting of rights to the clients**. In addition, you can configure the general password policies here and determine which entry types should be available to clients by default. The dialog box is divided into the tabs **Default permissions**, **Security**, **Entries** and **Passwords policy**.

The following tabs are available:

- Default permissions
- Security
- Entries
- Passwords policy

Client Security Policies

By using the **Client Security Policies** you can define specific features of the Corporate client with the Server Manager. Go to **Manage → Client Security Policies** to activate them and set the permissions as required. With the Client Security Policies more options for client configuration are available and you can enforce the Corporate edition clients to strictly follow them.

NOTE: The Client Security Policies set in the Server Manager can only be applied if the **Client Coporate edition** 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 about the Password Depot Client Corporate edition please visit our knowledge base using the link below:

Password Depot Client Corporate edition and Client Security Policies

Master Password Policy

Password policies can be configured to enforce security standards for both local databases and Server Manager users. For local databases, users must create passwords that comply with the defined policies during database creation. For Server Manager users, administrators are encouraged to follow these policies when setting passwords for Enterprise Server users. However, compliance is not mandatory during user creation to avoid conflicts with third-party requirements.

- **Enforce password history:** Define a specific number of new passwords users will be enforced to use/create before reusing an old password again.
- **Maximum password age:** Define a specific time span (days) a password can be used before enforcing users to change it in any case.
- **Minimum password age:** Define a specific time span (days) a password must be used before changing it.
- **Minimum password length:** Define how many characters a password needs to have at minimum.

- Password must meet complexity requirements: Define how many and which different types of characters a password must contain at least (Lowercase, Uppercase, Special, Numbers).

Allowed Storage Policy

If you enable users to also create and save databases outside Password Depot Enterprise Server you can determine here wich locations should be displayed for server users (for example the local system or cloud etc.). Locations that have been deactivated in the Client Security Policies will then not be visible in the client at all, thus users cannot select them for storing databases outside Password Depot Enterprise Server. In general, Password Depot offers the following locations for storing databases (all of them can be deactivated except the Enterprise Server, of course):

- Box
- Dropbox
- Google Drive
- HiDrive
- Internet Servers
- Local System
- OneDrive/OneDrive for Business
- Password Depot Enterprise Server
- USB Removeable Devices

Action Policy

Specify whether actions such as printing or exporting entries for example, should be enabled in general. This includes the following actions:

- Copy data to clipboard
- Decrypt external files
- Encrypt external files
- Erase external files
- Export

- Install Password Depot on USB devices
- Print
- Read TOTP secrets
- Set Second passwords
- Synchronize (databases)
- Use TANs

Program Options

Here, you can define relevant and safety-related program options. This includes the following:

- Auto save database on every change: This policy refers to databases stored outside Password Depot Enterprise Server (if this option is enabled in general). If so, a database will be saved automatically on every change.
- Automatic cleaning of clipboard: You can define a specific time (in seconds) for Password Depot to automatically delete any data that has been copied to the clipboard before.
- Automatic updates mode: You can define here, if clients should automatically search for new updates or not.
- Automatically delete local copy after closing remote file: If users can save local copies of server databases to their local system, you can check this option if you want those local copies to be deleted immediately as soon as the remote file is closed.
- Check for updates interval (days): If searching for updates is enabled, you can define a specific time span clients should automatically search for updates.
- 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 Password Depot Enterprise Server (if this option is enabled in general). If this policy is activated, a new backup copy is created and saved to a user's local system upon every database saving.
- Create a backup copy when opening a database: A new backup copy is created and saved to a user's local system every time a user opens a database. This policy also refers to database stored outside Password Depot Enterprise Server.
- Default authentication mode: Define a default authentication mode for all clients. You can choose from the following: 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 also refers to databases stored outside Password Depot Enterprise Server (if this option is enabled in general). Those backup copies will then be saved to a user's local system. Administrators can define a maximum number of backup copies to be stored.
- Open last used password file at program start: If this policy is activated, by default the last used database is launched upon the client's next program start.
- Protect access with a password: Specify whether the clients must additionally secure the connection to the browser add-on with a password.
- Show passwords in the list view: You can define, if the client's main view should include the "Password" column. However, please note that passwords are never displayed in plain text. Therefore the main view shows small stars only.
- Store list of recent databases: This policy also refers to databases stored outside Password Depot Enterprise Server (if this option is enabled in general). If activated, clients can go to the Database Manager → Recent Files and easily open databases they just 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, for

example if working in offline mode is required. However, please note that local copies do only include the data a user is able to also access during active server connection.

HINT: 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!

NOTE: The settings of the Client Security Policies are always applied to the entire server and all users. Therefore, the settings defined in the Client Security Policies cannot be changed for single users or groups at database level afterwards. By clicking Restore default settings you can reset the default settings and thus discard changes.

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 continuously created on run time. With the server mirroring feature in Password Depot Enterprise Server administrators can duplicate the entire content of their server on another remote or in-house server. This way, you can restore your data in case the primary server fails. Through server mirroring in Password Depot Enterprise Server you can synchronize and backup your data from the primary server to a backup server.

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

If you have two machines running Password Depot Enterprise Server (the software must be installed on both machines accordingly), you can organise server mirroring. One server must be the Principal server which runs as usual, that is users connect to this server to open shared server databases. The other server will be the mirror server. Users will be able to connect to the mirror server too but they can only use it in read-only mode. The Principal server updates and synchronizes the data on the mirror server in the background on run time. In case the main or principal server should fail, administrators can activate the mirror server as principal server so that users can continue to work and still access the data stored to Password Depot 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 use server mirroring at all
- Principal if the server you are currently connected to should be the main server
- Mirror if the server you are currently connected to should only 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 always see the current status of server mirroring, for example if the process was carried out successfully or if it failed. In case server mirroring should fail, an error message will be displayed in the status box. It also contains additional information about the general configuration of your current server mirroring in Password Depot Enterprise Server.

NOTES

- Both servers must be configured with identical settings. The Enterprise Server should be run as a Windows service. Ensure that the same keyboard layouts are in use on both Server A and Server B.
- Grant full read and write access to the specific program directory of the Enterprise Server, limited to only those user or service accounts required for operation.
- Check the firewall settings on both servers. It's essential to allow incoming and outgoing TCP/UDP connections over Port 25017 (the default port for Version 17).
- Log in to both servers using identical user credentials.
- Ensure that the roles of "Principal" and "Mirror" are correctly distributed between the two servers. The Principal server is generally responsible for the primary data processing, while the Mirror server acts as a backup.

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. English, German, French, Spanish and Dutch are available here.
- SSL/TLS Settings: Activate this option if you would like to login to the Server Manager using an SSL connection. Please note, that an SSL connection for the Server Manager login is only possible, if SSL connections have been activated in the Server Manager in general. If the settings are correct, you can see in the Server Manager's login window that the option Use SSL/TLS is always checked by default. This means that the installed certificate is verified in the background each time you log on to the Server Manager.

Tools

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

- System log
- Active Directory Synchronization
- Azure AD Synchronization
- Databases report
- Users report

The menu item Tools therefore is of importance if you would like to add Active Directory or Azure AD users to the Enterprise Server so that they can log on on the server either using their Windows NT or Azure AD access credentials to open server databases. To do so it is required in any case to perform Active Directory or Azure AD synchronization using the integrated synchronization wizard to import users to the server.

With the System log button you can generate the server log which will then be displayed in the Windows Event Viewer. For example, should you notice any errors occurring on the Enterprise Server you can have a look at the system log and explicitly search for errors here.

Creating a databases and users report may help you to get a better overview about your server databases and users.

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

User login to AD

Password Depot uses LDAP (instead of WinNT). A user UPN (User Principal Name) can be retrieved from the Active Directory. However, this feature is only available after manual or automatic synchronization with AD in the Server Manager.

This means that Windows domain users can be authenticated on the Password Depot Server by using both forms of "User logon name":

1) <NetBIOS domain name>\<sAMAccountName> - this is the classic WinNT form (before Windows 2000)

EXAMPLE: MICROSOFT\Test

2) Main user name (which normally is shown as <sAMAccountName>@<DNS domain name>)

EXAMPLE: test@microsoft.com

3) If you do not have multiple users with the same names from different trusted domains in the network, a user can use the simple form <sAMAccountName→.

EXAMPLE: Test

This means that a user from AD can use exactly the same credentials for logon on the Enterprise Server he also uses when logging on to a Windows domain account.

Active Directory Synchronization

In the Tools menu, choose Active Directory Synchronization to start the wizard of the same name. The Active Directory synchronization is required if you would like your users to log in on the Enterprise Server through Single sign-on (SSO). In this case, users will log in on the server using their Windows NT credentials. To do so, however, the Active Directory synchronization is mandatory in any case.

NOTE: In version 14 the WinNT provider was replaced by a more powerful LDAP provider. In addition to that, the functionality of the Active Directory synchronization was improved and more features have been added to the synchronization wizard.

Password Depot also supports nested AD security groups.

WARNING: If group A is a member of group B and group A is imported via the built-in AD synchronization wizard, group B and its users will also be imported (if not unchecked manually). If any users get unselected, Password Depot will not import the coresponding group but only the selected users.

When you launch the wizard you will first have to provide information about the domain you would like to use for importing users/groups to Password Depot Enterprise Server:

LDAP Path

Enter the LDAP path, domain name or IPv4 address of your AD server to synchronize AD users.

Sign In

- Sign in as current user: Select this option if you would like to sign in with the current user to start the Active Directory synchronization. The current user is the one you also used for the Windows login.
- Use this account: Enter the user name and password of another user who can also read data from the Active Directory of your domain or the domain selected. Usually, it is the domain administrator. Please note that by default the Password Depot server uses the SYSTEM account of the computer/machine it has been installed to (the machine running the Enterprise Server). Therefore, please make sure that any

account used for Active Directory synchronization (especially if it is not the current user account) has full read access to the Active Directory of your domain. Otherwise the synchronization cannot be carried out properly.

Additional Options

- Explorer mode: Using this mode you can browse the existing folders in the Active Directory. A new dialog window will open afterwards and your the Active Directory tree will be displayed. Select the users/groups you would like to import into Password Depot Enterprise Server.
- Search mode: Use this mode if you would like to search for specific users and groups in the 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. If, however, this option is not checked, the wizard will work like a standard Active Directory explorer which means that it will only open the specified object and scan the container afterwards, if expanded.
- Check deleted objects: If you activate this option, any deleted objects (for example deleted users or groups) are scanned in both the Active Directory and Password Depot Enterprise Server and merged afterwards.
- Use SSL: You should check this option, if your Active Directory requires SSL.

Click Sign In once all settings are done. If the login was carried out correctly a new dialog window opens displaying the Active Directory tree. Please select all users and/or groups you would like to import to or update in Password Depot Enterprise Server. If there are a lot of objects you can filter the view using the corresponding box at the bottom on the left.

HINT: If the filter does not find any users or groups, go back, enable the option Recursively scan all containers and try again.

Next, check the desired users and/or groups and finally, click Synchronize. A new dialog window will open subsequently displaying the synchronization results.

NOTE: In general, Password Depot server cannot work with OUs. Although those groups are displayed in the synchronization wizard only Active Directory objects such as "Users" or "Groups" can be used for server synchronization.

HINT: You can now synchronize users and groups individually with Active Directory. To do so, select the corresponding user or group and click Synchronize in the Server Manager on the right afterwards.

NOTE: If you would like to know which settings are required for both the Server Manager and client in order to use the Integrated Windows Authentication (SSO) to log in on the Enterprise Server, please read the following knowledge base article carefully: Single sign-on (SSO) for Enterprise Server login. Please also note, that the computer which is used for Single sign-on has to be an Active Directory member, otherwise the login will fail. A computer has to be an Active Directory member in order to carry out the Integrated Windows Authentication at all. When synchronizing Active Directory users with the Enterprise Server, Password Depot does not "know" and save the user passwords to the server but moreover, during authentication, the password which is entered by a user is sent to the Active Directory and Password Depot will get a notification if the entered password is either valid or wrong. Therefore it is mandatory in any case that the computer which is used for login is also a domain member.

Azure AD Synchronization

The Enterprise Server does not only include the standard Active Directory synchronization but also Azure AD synchronization. To launch the Azure AD synchronization wizard open the Server Manager and go to **Tools → Azure AD Synchronization**. The latter is required if you would like your users to use their **Microsoft credentials** to access their databases. As is the case with the AD synchronization you need to make sure to run the Azure AD synchronization wizard correctly. Azure AD users cannot be added to the Server Manager manually -this is the only way to do it.

WARNING: To initiate Azure AD synchronization, you must first read: Adding Password Depot Enterprise Server as an Enterprise Application in Azure Active Directory. Afterward, you can proceed with the following steps:

Organization

When launching the wizard you first have to choose an organization which should be used for the import of Azure AD users. If you cannot select an organization from the drop down-menu, click **New...** right next to it. Afterwards you will have to select a Microsoft account that is supposed to be stored as organization.

NOTE: Only the **administrator's user account** can be used to sign in to an organization!

Enter the administrator's user name and password to login. Next, you will be asked to also enter the second factor displayed in your authenticator app. Two-Factor Authentication is always required in this case because it is part of the Microsoft security policies. If you have logged in successfully, the Azure AD users/groups that are available for synchronization will be displayed in the wizard accordingly. Select the objects you would like to import. Afterwards, click **Synchronize** to start the actual synchronization process. The synchronization results will be shown subsequently. If you can see here all users/groups you would like to import you can close the wizard.

Additional options

Check deleted objects: If you activate this option, the synchronization wizard will check and compare any deleted objects (users and groups, for example) in both, the Azure AD and Password Depot Enterprise Server.

HINT: If a user has been added to the Server Manager through Azure AD synchronisation, you can open the user properties, go to the tab Account and see that the option Azure Active Directory has already been checked automatically as the default type of authentication. Besides, you can find more Azure AD attributes of a user in the Azure AD tab of the user properties. All those attributes are entered automatically during Azure AD synchronisation and you should not insert any data here manually.

Please have a look at our Password Depot desktop client manual to learn how Azure AD users can log on to the Enterprise Server.

Import Users and Groups from Azure AD

After establishing the connection to Azure AD, you can search for specific users or groups to add. If you leave the Search users and groups field empty and click on Search now" all entries from Azure will be displayed for selection.

You can now check the box for individual entries to select them, or right-click and choose Select all.

Once you have completed your selection, click on Synchronize to finalize the import.

Reports

The menu item Tools includes options for generating specific reports. You can generate the following:

- Databases report
- Users report
- Groups report

By creating these reports you can get a quick overview of your server users and databases. To create a report, select the desired one in the Tools area and click Generate. The corresponding report will be generated immediately and displayed in your browser. You can save the reports to the *.html format by clicking Save as, for example if a report will be needed at a later point of time. Below, more details are provided about the Databases, Users and Groups report.

Databases Report

You can create a Databases Report for single or multiple Password Depot Enterprise Server databases at the same time. This way, administrators can get a quick overview about their users and which server databases they can access. In addition to that, a user's access rights on the selected databases are displayed in detail. Allowed permissions are always displayed with a "✓" in the corresponding column, rights that have been denied by the administrator are displayed with a "-". The databases report shows a user's permissions at database level only.

Users Report

Generating a Users report will create a list of all user accounts currently available on Password Depot Enterprise Server. The following information is displayed about every server user:

- Account: Displays the corresponding user account or user name.
- Type: You can see here if a user is just a "standard" user or if they have been assigned additional server roles (for example Database Administrator).
- Full Name: Displays a user's full name that has been saved in the user properties in the General tab.

- Email: Displays a user's email address if it has been saved in the user properties in the General tab.
- Disabled: You can see here if a user account has been deactivated. If so, the corresponding user cannot connect to the Enterprise Server anymore. Open the user properties and go to the Account tab to activate the account again.
- Assigned Databases: You can see here all databases a user has been assigned access to.
- Access Rights: Displays a user's access rights on every server database in detail.

Groups Report

Generating a Groups report will create a list of all groups currently available on Password Depot Enterprise Server. The report includes the following information (in columns):

- Account: Displays the corresponding user account or user name.
- Type: You can see here if a user is just a "standard" user or if they have been assigned additional server roles (for example Database Administrator).
- Description: Displays a groups description if it has been saved in the user properties in the General tab.
- E-Mail: Displays a user's email address if it has been saved in the user properties in the General tab.
- Disabled: You can see here if a user account has been deactivated. If so, the corresponding user cannot connect to the Enterprise Server anymore. Open the user properties and go to the Account tab to activate the account again.
- Assigned Databases: You can see here all databases a user has been assigned access to.
- Access Rights:Displays a user's access rights on every server database in detail.

Databases

The Databases area contains all databases available in the Server Manager. Here, you can add new databases to the server or manage and delete already existing ones. Apart from that, users and groups are assigned general and detailed access to server databases in this tab.

In the main view of the Databases area you can see all existing server databases, their size, the time and date of the last access as well as the total number of entries. Besides, the main view also displays a Connections column where you can see how many users are currently connected to each database available. If many single databases are available on the server you can filter the main view by using the filter box at the top. To do so, enter a database name or parts of it, for example.

Besides, more options are available on the right:

- New database: Using this button you can create a new or add an existing database to the Enterprise Server. A new dialog window called Add database to server opens subsequently.
- Permissions: In the Server Manager, rights management is done in the permissions tab. By clicking the button of the same name you will be forwarded to the main view where you can see a list of all users/groups who have already been granted access to the selected database. Apart from that you can see a user's effective rights at database level as well as for single folders and entries at the bottom of the main view. For specific rights management, please select a user or group from the list and double click it. A new dialog window opens where you can set individual user/group permissions. To open the Permissions tab you can also select a user from the list in the main view and click the Properties button on the right.
- Properties: A new dialog window opens where detailed information about a database is displayed. For example, you can see here all users currently connected to the corresponding database. Besides you can get further information about the file type and size and you can see the exact date and time the database was last modified. For more information about a database's properties please click here.
- Delete: Use this button to delete already existing server databases. If another user is working with the corresponding database at the same time, they will receive a notification about the deletion upon database saving. Databases deleted in the

Server Manager are also removed from Password Depot Enterprise Server's working directory.

- **Rename:** Rename a selected database.
- **Select all:** Select all databases displayed in the Server Manager's main view. You can then perform further actions which will be applied to all server databases.

HINT: You can also access these options by **right-clicking a database** from the list. Apart from that, you can also filter the main view, for example if you would like to search for a specific database. To do so, enter the database name or parts of it to start search.

Add Databases

You can open this dialog window if you go to the Databases area and click New database on the right. This way you can create new databases on the server. 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. You may need this option, for example, if you would like to add a database to the server that has been saved to a user's local system so far.

- Click the Browse button to find the corresponding database.
- Enter the database's correct master password into the Master password field. By default, it is hidden and not displayed in plain text. Click the eye icon to reveal it, if required.
- Finally, click OK to finish.

NOTE: Local databases protected by a key file or master password and a key file are not supported. To change the authentication of your local database, please read the following article: How can I change database authentication in Password Depot?

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

Create New Database

Select this tab to create a new, empty database and save it to Password Depot server. Enter a database name first. You can also add additional comments to the Comments field, if required.

NOTE: Server databases are always encrypted with the super administrator's password, thus the master password of server databases always corresponds to the super administrator's password. To access server databases, however, clients will use the access credentials assigned to them by the administrator (depending on the authentication set by the server administrator).

Databases - Permissions

In the Permissions tab you can do the rights management and assign access rights to users and groups in detail.

In the main window you can see all users/groups authorized to access the corresponding database. Below you can see the effective rights of single users and groups. If you want to see the effective rights in detail, select the desired user or group from the list.

If you want to remove database access for single users or groups, select the corresponding account and click Delete on the right. Users and groups that have been removed from a database cannot access it anymore, however, those users and groups are still available on the server. Click Select All to select all users/groups with access to the corresponding database. You can then perform further actions which will be applied to all highlighted user/group objects.

New

Select New to add new users/groups to the selected database. Choose a user/group form the list on the left. Finally, click OK to finish.

In the main view, double click the user or group you just added to the database in order to perform detailed rights management. Alternatively, you can also select the user/group form the list and click Properties on the right. A new dialog window opens where you can set the permissions at database level as well as for single folders and entries. Three tabs are available here:

- General
- Entries and folders
- Sealed access

The permissions set in the General tab are applied to the entire database. Further permissions for single entries and folders can be set in the tab of the same name. The sealed access tab is used for changing the status of sealed entries. Detailed rights management as well as the process of sealing entries is explained more precisely below.

Properties

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. Below the user name, administrators can either limit the access of users and groups to a database or grant access without time limitation. If you want to enable limited access only, enter a start date in the Valid from box and define the date of end in the Valid to box. If you want to allow unlimited access for the corresponding user/group, you can uncheck the boxes Valid from/to and define a start date only (by default, the date is set to the day you grant a user or group access to a database and set the permissions).

Permissions

Here, you can define the access rights at database level, that is, those permissions are applied to the entire database. The following permissions are available:

- 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

HINT: If you click View effective rights you can see a user's or group's effective rights in a separate window more precisely.

NOTE: Enabled permissions in the General tab are global rights and applied to the entire database. If you enable users/groups to Read/Modify/Add/Delete entries at database level, they can see and edit all entries within the corresponding database by default. If you want users/groups to only access specific folders and/or entries within the database, you should not enable the rights Read/Modify/Add/Delete at database level and thus remove the Allow tick accordingly. Attention: Only remove the tick but do not disable those rights! In the Permissions for Users chapter you can learn more about correct rights management and how to ensure that unauthorized users do not see entries they are not allowed to.

Entries and Folders

In the Entries and folders tab you can assign users and groups access rights on single folders and/or entries within a database. This way, administrators can define the user and group access rights in a way that each user/group can only see those objects they should actually be allowed to access.

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
- Set second password

Select single entries or folders on the left and assign rights in the permissions area afterwards.

HINT: If you click View effective rights you can see a user's or group's effective rights for single entries and folders in a separate window more precisely.

NOTE: Both the General and Entries and Folders tabs inlcude special formatting to make rights management easier. By default, all permissions are depicted in green and bold letters. This means that these permissions are enabled to users. On the other hand, denied permissions are depicted in red and bold letters as well. This way, the administrator can recognize from the start which permissions have been enabled or denied for single users and groups.

Grant access to other users

This permission can be enabled either for the entire database or for single entries and folders within a database only. If the server administrator enables the permission to grant access to entries and folders to other users, a user can share data with other Enterprise Server users in the client. In this case, the administrator does not need to change the access rights in the Server Manager. This is useful, for example, if a user wants to share data with another Enterprise Server user temporarily.

Users can grant access to other users in the client only. The exact procedure is described in our Windows client manual.

Seal Entries

If a user has been granted access to an entry, the entry to be shared may be sealed. In this case, accessing the entry will only be possible if the access has been approved or the seal removed by an authorized person in the Server Manager.

NOTE: Only users with admin rights in the Server Manager can change an entry's seal state.

Sealed access to an entry is also set in the client. This feature is available when granting access to an entry to another user. The issuer who would like share an entry can decide whether it should additionally be sealed or not.

The process of sealing entries is also described in detail in our Windows client manual.

Sealed access

If access to an entry in the database has been granted by user A to user B and the entry has been sealed by user A, it is first necessary that a user with admin rights on the Enterprise Server allows access to the selected entry so that access can be granted. The user who grants access determines which user on the server is required to grant access.

To do this, the corresponding user logs on to the Enterprise Server with his access data. In the area Databases → Permissions you can now see that user B has been granted access to an entry in the selected database. This shows the defined period of access, who created the access and whether the entry has been sealed. The permissions can be opened with a double click. The permission is granted in the Sealed Access tab.

Here you can see the state of the entry, which may be set to Sealed, for example, provided the entry has been sealed. The corresponding state can be changed by clicking the Change Seal Status button. You can choose from the following states:

- Sealed: An entry is still sealed and no attempt has been made to access the corresponding entry.
- Unsealed: The seal has been removed.
- Waiting for approval: The user who has been granted access is specifically asking for access permission. In this case, the user would like to open the corresponding entry and asks for permission to do so.
- Approval granted: An authorized person has granted permission for accessing an entry accordingly.
- Broken: A seal has been broken and thus, an entry has been accessed.

After changing the seal state, the new state is displayed in the database permissions. If permission has been granted, the user who was granted access can now open the entry and break the seal.

Authorized persons can change an entry's seal state at any time. Server administrators can also add other authorized persons to change the seal state. This is done in the Sealed Access tab by clicking the Add button.

EXAMPLE: The user Test1 grants access to an entry to user Test2 for 2 weeks in total and seals this entry. If the approval is granted, user Test2 can break the seal and access the entry. If necessary, a server administrator can change the seal state again; for

example, the admin can reseal the record so that user Test2 must ask for approval again if they want to access the record, etc.

HINT: For more information about this feature feel free to visit our knowledge base: How to grant access to other users and seal entries in Password Depot.

Database Properties

The Database - Properties dialog window contains general information about a selected database. You can access it by selecting a database in the databases area and clicking Properties on the right afterwards.

General

In the General tab you can find basic information about the selected database. For example, you can see here the users currently connected to the corresponding database as well as the database's size and file type. By clicking the Refresh button you can update the current view.

Advanced

The Advanced tab includes additional features for monitoring the user accesses and activity. You can activate monitoring and logging all cases of user accesses to entries and define whether users must specify a reason when deleting an entry. If you would like to monitor and log all cases of user accesses to entries and activate the option of the same name, the eye icon for revealing a password in plain text will disappear in the client's details area on the right. Background: This is the only way for server administrators to monitor and log every access on server entries in detail. For more information about this feature, please visit our knowledge base using the link below:

Where can I find the "eye" icon for revealing passwords in plain text?

NOTE: The Database Properties are supposed to provide basic information about a database in general. Detailed rights management, however, can only be carried out in the Permissions area.

Security

Encrypt Database on Server with

Here you can encrypt your server databases with an additional password. By default all server databases are encrypted with the super administrator's password which means that the super administrator can automatically manage all databases available on the server as soon as they access the Server Manager.

In some cases, however, the super administrator or other server administrators should not be allowed to access and manage all server databases by default. If so, further configuration is needed and we therefore recommend encrypting the server databases with an additional password. Click Change settings to start:

The dialog window Change Database encryption settings opens. Open the drop down-menu Encrypt Database on Server with and select the option Custom password (Permissions management requires verification). You will be asked to enter a new password and confirm it next. Finally, click OK to finish.

If you save changes, the selected database is encrypted with an additional password. From this point onwards, accessing the database properties and permissions and thus, database management in general will only be possible if the custom password is known and entered correctly. Other users with additional server roles who may also have access to the Server Manager can only access such databases and their properties if they know about the additional password.

If you would like to change the custom password at a later point in time, enter the database's current custom password to open its properties. In the Advanced tab click Change settings next. Enter the old custom password first and enter a new password afterwards. Click OK to save the new custom password. If you would like to delete the custom password, select the option Administrator password (Automatic access to permissions management) from the drop down-menu and enter the current custom password into the corresponding field afterwards. Finally, click OK to finish. The additional custom password for further database encryption is then restored to the super administrator's password which means that from this point onwards no custom password is needed or has to be entered if server administrators would like to manage the database's permissions or properties.

WARNING: Caution when using this feature! Please only set an additional custom password for database encryption if it is really needed because there is no option of resetting or restoring those additional custom passwords if server administrators forget them. As a consequence, you cannot open the properties and permissions of the affected database and database management will not be possible anymore if the custom password gets lost. Therefore, please only use this feature if really needed and if so, please keep the additional custom password safe.

NOTE: For more information about this feature, please visit our knowledge base: How to protect Enterprise Server databases from unauthorized access by the server administrator.

Monitor and log all cases of user access to entries

This option allows you to track and log every instance of user access to the entries in Password Depot Enterprise Server. By enabling this feature, you can maintain a detailed record of user activities, which can help enhance security and accountability within your organization.

Users must specify a reason when deleting an entry

Enabling this option requires users to provide a reason for deleting an entry in the Password Depot Enterprise Server. This added layer of accountability can help prevent unauthorized or accidental deletions, as well as provide valuable information for auditing and tracking changes within the system.

Users

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

The main view of the **Users** area displays the following columns:

- **Account:** Displays the corresponding user account.
- **Authentication:** Displays a user's type of authentication on the Enterprise Server (Password Depot credentials or Integrated Windows Authentication)
- **User Principal Name:** Displays a user's user principal name in case a user has been added to the server through Azure AD synchronization.
- **State:** Displays if the corresponding user account is enabled or deactivated and if the user is currently connected to the server.
- **Roles:** Displays if the selected users has been assigned an additional server role. If you would like to find out more about the server roles, please click here.
- **Address:** Displays a user's IP address if the user is currently connected to the server.
- **Full name:** Displays a user's full name which can be entered and defined in the **General** tab of the user properties.
- **Email:** Displays a user's email address provided it has been added to the Server Manager.
- **Department:** Displays a user's department provided it has been added to the Server Manager.
- **Open database:** If a user is connected to the server this column shows the database a user is working with.

Besides, more options are available on the right:

- **New user:** Use this button if you would like to add new, local users to the Server Manager. The dialog window Add user will be displayed afterwards. You can enter here the user name and password of new, local users (**Password Depot credentials** type of authentication).
- **Properties:** Open the User properties dialog box.

- **Delete:** You can delete selected users in the Server Manager.
- **Disconnect:** You can disconnect selected users from Password Depot Enterprise Server.
- **Synchronize:** You can use this option to synchronize selected users with Active Directory or Azure AD separately without launching the Active Directory or Azure AD wizard and start the whole synchronization process all over again. In any case, however, please note that this option can only be used if the respective user was added to the Server Manager through Active Directory or Azure AD synchronization before. Therefore, the **Synchronize** option in the **Users** area can be used, for example, for updating an already existing user in the Server Manager separately if their Active Directory/Azure AD data has changed. In this case, it will not be required to perform AD/Azure AD synchronization again for all users if individual users need to be updated only.
- **Assign database:** Administrators can assign single databases to single or multiple users at the same time. Besides, they can also create new server databases here and assign them to single or multiple users at the same time subsequently. In the **Permissions** tab administrators can assign user rights at database level right away. You can also create **private databases** for your users here. Those private databases are also stored to the company's server. You can find out more about private databases in the chapter Assign Database.
- **Reset 2FA:** If **Two-Factor Authentication** for the server login is enabled in general, you can choose this option to reset the 2FA settings for single or multiple users. In this case, the selected users will have to start the 2FA process all over again, that is, next time they want to connect to the server they will have to scan the QR code again and enter the 6-digit code.
- **Select all:** Select all users available in the Server Manager. You can then perform further actions which will be applied to all server users.

NOTE: The **Synchronize** option uses by default the server's own **SYSTEM account**.

HINT: You can also access these options by **right-clicking a user** from the list. Apart from that, you can also filter the main view, for example if you would like to search for a specific user. To do so, enter the username or a part of it to start search.

Add Users

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

1. The button New user
2. Through Active Directory Synchronization
3. Through Azure AD Synchronization

Add new users manually

You can add new, local users to the Server Manager manually using the New user button available in the Users area on the right. Those users will then connect to the Enterprise Server using their Password Depot credentials. To do so, go to the Account tab and select the Password Depot credentials authentication. Enter the user's user name and password. Click OK to finish. The new user will be displayed in the main view of the Users area subsequently and you can start giving them access to databases and assign permissions to entries and folders within those databases.

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

Add new users through Active Directory synchronization

If users should login on the Enterprise Server through the Integrated Windows Authentication (SSO) you cannot add them to the server manually but have to perform Active Directory synchronization first. You can launch the corresponding wizard by going to Tools → Active Directory Synchronization. The user objects will then be imported into the Server Manager from Active Directory. If synchronization could be completed successfully, you can see all objects that were imported from Active Directory in the Users area afterwards.

In the user properties of Active Directory users you can see in the Account tab that the option On-Premises Active Directory is already checked by default. In the Active Directory

DS tab you can furthermore check other Active Direvtory attributes of the selected user. Those attributes too were inserted automatically during synchronization.

For the Enterprise Server login, Active Directory users will choose in the desktop client's Database Manager the option Integrated Windows Authentication. During authentication a user's user name and password will be sent to the Active Directory. A message will then be sent back to Password Depot saying that the data sent is either correct or wrong. Based on this information the login will either be completed (if the data sent is correct) or denied (if it is wrong). Therefore, it is important that the user data available in the Server Manager corresponds to the user data in the Active Directory. Thus, we recommend performing Active Directory synchronization on a regular basis in order to transfer changes from the Active Directory into the Server Manager, too.

HINT: Find out more about Active Directory synchronization in the chapter of the same name.

Add new users through Azure AD synchronization

Adding new users to the server through synchronization is also required if you want to use Azure AD autentication on the server. To start the synchronization process, open the Server Manager and go to Tools → Azure AD Synchronization. The user objects from Azure AD will then be synchronized with the Server Manager. If synchronization could be completed successfully, you can see all objects that were imported from Azure AD in the Users area afterwards.

In the user properties of Azure AD users you can see in the Account tab that the option Azure Active Directory is already checked by default. In the Azure AD tab you can furthermore check other Azure AD attributes of the selected user. Those attributes too were inserted automatically during synchronization.

For the Enterprise Server login, Azure AD users will choose in the desktop client's Database Manager the option Azure AD authentication.

NOTE: You should not manually enter or edit any data in the Active Directory DS or Azure AD tab of the user properties because those attributes are always entered automatically during synchronization. Besides, those attributes are only useful if added automatically. Therefore, please note the following: If a user's Active Directory or Azure AD data have changed, do not manually enter those changes in the Server Manager.

Moreover, run the Active Directory or Azure AD synchronization again in order to update a user's data.

HINT: Find out more about Azure AD synchronization in the chapter of the same name.

See also: Add Groups, Add users by department

User Properties

The User properties dialog window is available for every user in the Server Manager. You can access the user properties either by double- or right-clicking a user in the Users area.

Administrators can edit the users in the user properties dialog window. The following tabs are available here:

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

The content of each tab is explained below.

General

The General tab includes the following options:

- Full name: Enter the user's first and last name here if different from the actual user name on the server.
- Email: Enter the user's email address.
- Phone: Enter the user's phone number.
- Department: Enter the user's department.
- Description: Here you may add additional information about the user, if required.

Account

In the Account tab you can set the following:

Authentication

You can see here 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 specifc user name and password for each user. Afterwards, they have to share the data with their users. Users can or may change the password for the Enterprise Server login afterwards, if this option is enabled in the Server Manager. Please have a look at the following knowledge base article to learn about how to change the password:

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 in the Server Manager so that the users can connect to the Enterprise Server using their Windows credentials. Find detailed information about the Active Directory Synchronization in the Server Manager here.

Using the **Azure Active Directory** authentication users will have to logon on the Enterprise Server with their Microsoft credentials. This authentication also requires a full Azure AD synchronization in the Server Manager prior to the login of a user. Azure AD users can only be added to the Server Manager through synchronization and not manually. Find detailed information about the Azure AD synchronization in the Server Manager here.

Two-Factor Authentication

- **Operation Mode:** With this setting you can change the 2FA operation mode individually depending on the user's requirements (this setting was implemented in v17.0.5).

Account options

- **Account deactivated:** If this box is checked, the user's account has been locked temporarily. This may occur if a user has reached the maximum failed login attempts allowed on the server. Uncheck the box to activate the account again and thus, enable the user affected to access and log on on the server again.
- **User may not change password:** Check this box if you do not want to enable **local users** changing their password for login on the Enterprise Server. Please note that

his option can only be used if a user is accessing Password Depot Enterprise Server via Password Depot credentials authentication.

- User must change password at next logon: Check this box if you want users to be forced changing their password for login on the Enterprise Server next time they want to connect. Changing the password will then be mandatory for the user at the next login in any case. Again, please note that his feature can only be activated for local users but not for Active Directory or Azure AD users that have been imported to the Server Manager.

Roles

With version 15, additional server roles were implemented. This way, you can assign specific server roles to single or multiple server users and thus, server administration can now be carried out by multiple users instead of having only one person being responsible for server configuration and administration. Users being assigned an additional server role can access both the Server Manager as well as 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. In general, a server administrator has full access to all databases and entries. In addition to that, they can manage and configure the server and its settings by accessing the Server Manager.
- Database Administrator: A Database Administrator can create new databases on the server and edit already existing ones. This server role enables a user, for example, to change a user's or groups' permissions for databases and entries.
- Account Administrator: An Account Administrator can manage users and groups on the server and, in this context, also add new users and groups to the server, for example.
- Group administrator: The Group Administrator role allows users to access the Server Manager and manage groups and their users for which they have been granted authorizations under Groups → <Group> → Properties → Administrators.
- Active Directory Operator: An Active Directory Operator can perform Active Directory or Azure AD synchronization in the Server Manager. Please note: This server role requires additional server roles, that is, either Database or Account Administrator. If a user is an Active Directory Operator only, they will not be able to

perform Active Directory or Azure AD synchronization in the Server Manager or change any other server settings.

- Event Log Reader: An Event Log Reader can access the server's logs.

NOTE: Introducing different server roles in the Server Manager with version 15 did also have an impact on the super administrator's account: The latter is now only used for server administration in the Server Manager and thus, the super administrator can only login to the Server Manager but not to the Enterprise Server to access databases. In general, the super administrator's account is not a classic user account anymore and is therefore not a part of the total number of users available on the server.

Member of

You can check here, if the user selected is a group member of one or several server groups. In addition to that, you can add single users to new or other server groups , provided those groups are already available in the Server Manager.

- Add group: Click this button to add a user to a new or other group.
- Delete: Select a group from the list and click Delete afterwards to remove the selected user from the corresponding group.

Active Directory DS

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

- Logon Name: Displays a user's user name which 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 correct path in the Active Directory.
- Object GUID: Displays the ID of an Active Directory user which is generated automatically.

NOTE: The information displayed in the tabs called Azure AD or Active Directory DS is of importance only if Active Directory or Azure AD synchronization is performed in the Server Manager thus, enabling users to login to the server through Integrated

Windows Authentication (SSO) or using their Azure AD access data. During synchronization the users' Active Directory or Azure AD attributes will be added to the Server Manager automatically. Therefore, please do not enter here any data manually but instead please let Password Depot Enterprise Server do so during the process of synchronization.

Azure AD

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

- User Principal Name: You can see here a user's User Principal Name if the user has been added to the Server Manager through Azure AD synchronization.
- Object ID: Every Azure AD user is assigned a specific object ID. A user's object ID is also displayed in the Server Manager once the Azure AD synchronization has been completed.
- User Type: You can see here the user type of a user who was imported from Azure AD into the Server Manager. Azure Active Directory has two types of users: members and guests. Members belong to your own organization. A guest can be invited to your organization temporarily, for example if temporary collaboration is required.

Advanced

The Advanced tab is divided into two parts:

- WebSockets port for browser add-ons
- IP address verification

Web Sockets port for browser add-ons

Here, administrators can define the web sockets port settings for the browser add-ons. You can choose between the following:

1. Use global settings [25109]: If you select this option, by default all clients will use the port number 25109 to communicate with the browser add-on.

2. Auto-generate unique port number: Activate this option if you want to automatically assign individual port numbers to every single user on the server. Users can then see their port number in the desktop client by going to Edit → Options → Browser.
3. Use custom port number: Administrators can assign custom port numbers to their users and define specific port numbers themselves. In this case, users can also see the custom port number in the desktop client by going to Edit → Options → Browser.

IP address verification

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

User Permissions

In general, you can use Password Depot Enterprise Server to create one single database only and enable your entire company including all employees accessing it. Administrators can perform detailed rights management in the Server Manager and thus, can ensure that server users can only see those objects within a database they are allowed to access. If rights management is carried out properly by the server administrator users and groups do not know about the entire database content. Therefore, they can only access and work with those entries and folders displayed in their client.

NOTE: The user permissions described in this chapter can be applied to groups accordingly.

Please note that you do not have to work with one single server database only. However, the idea behind all this is that you can basically work with one single server database only and still meet all the requirements even though working with a large number of users. If you prefer working with multiple databases though, this is also possible. Besides, you can also create private databases for individual server users and groups which can be used, for example, to store private data that should either not be part of the shared database but still stored to the server. If you would like to learn more about private databases, please click here.

How is rights management realised in Password Depot Enterprise Server?

In general, we recommend assigning user permissions in the Databases → Permissions area. Here you can assign users and groups individual rights

1. at database level
2. for single folders and entries

Apart from that, you can also find global policies by going to Manage → Server policies. The latter are applied on the entire server. This way, you can define specific permissions which will then be valid for all users/groups available on the server. Therefore, the server policies are global policies.

What to consider when working with the server policies?

The permissions that can be found in the server policies are the same permissions you can find in the **Databases → Permissions** area at database level. In general, the permissions of the server polices can have three different settings:

1. **Enabled**
2. **Not defined**
3. **Disabled**

When installing the Enterprise Server the server policies are either **enabled** or **not defined** by default. As best practice, we recommend not changing the default settings here and mainly carry out rights management in the **Databases → Permissions** area. However, please note the following: You can also change a permission's state in the server policies and set it to disabled, for example but if so, please take the following into consideration:

If a permission has been disabled in the server policies, you **cannot enable it** at database level or for single folders and entries later when performing rights mangement in detail! Disabled permissions in the server policies are valid for **ALL** users and groups (the super administrator included) as well as **ALL** server databases. Therefore, the disabled state is very restrictive and you should only use it if really required. Otherwise you may disable permissions at a global level you would like to enable for special users and groups at database level afterwards which, however, will then not be possible anymore.

HINT: Learn more about the Enterprise Server's server policies in the Permissions chapter or have a look at the following knowledge base article: How does rights management in Password Depot Enterprise Server work?

CONCLUSION: You should only disable global permissions in the **Manage → Server policies** area, if required.

EXAMPLE: You can disable the **export of entries** in the Server policies area. In this case, exporting entries will be disabled for all server users and databases, thus exporting entries in order to import them into a new database will not be possible at all. Therefore, the export will be deactivated on the entire server and cannot be performed by any server user.

Defining rights in a database's permissions dialog window

If you open a database's permissions dialog window, you can start assigning single users and groups individual permissions. Individual rights management is done in the General and Entries and folders tab.

If you would like to enable multiple users/groups to access the same database but see different database content at the same time you should

1. go to the General tab and remove the tick for Reading/Modifying/Adding and Deleting entries and
2. go to the Entries and folders tab afterwards and specifically select those objects you would like a user or group to access within the database.

WARNING: You should not use the deny flag in the General tab for the above permissions (Read/Modify/Add/Delete entries) at all because if so, you will enable a user or group to access the corresponding database in the first place, however, since the deny flag is the most restrictive, users and groups affected will not see the database content at all and thus, they will not be able to work with it or use it.

You should enable the Access to database permission if you want a user or group to access a database and work with its content. You can disable the other permissions available at database level (in the General tab). In this case, the selected user or group cannot perform the corresponding action within the selected database (permissions in the General tab refer to the entire database).

What is the point of removing the ticks for Reading/Modifying/Adding and Deleting entries?

If you remove the ticks for Reading/Modifying/Adding and Deleting entries in the General tab and enable the Access to database permission, users and groups will be able to receive a database and access it in general. At the same time, however, those users and groups cannot see any entries and folders within the database (or the database's root directory) in the first place because the ticks for Reading/Modifying/Adding and Deleting entries have been removed. These rights, however, are mandatory if users should work with entries and folders.

If you go to the Entries and folders tab afterwards, you can see that the entire database content is displayed in red colour which means that accessing entries and folders within the database is not allowed. In order to enable users and groups to see and access the

database content, in this tab you have to select the single folders and/or entries and define the permissions for accessing those objects accordingly. This way, you can assign users and groups specific rights and determine in detail which objects (entries and folders) should be accessed by which user or group. The colours will help you: Permissions displayed in red are denied, thus a user or group cannot access such objects. Permissions displayed in green, however, are enabled and users/groups can access such objects.

If you follow rights management as described above, you can organize your server databases and create a database tree which includes both shared and private folders/ entries ensuring at the same time that users and groups will only be able to access those objects they are allowed to.

NOTE: The permissions Read/Modify/Add/Delete entries are somehow dependent on each other. Thus, you should either enable or deny them all together, if possible. For example, if you enable the Add entries permission but disable the Modify entries permission at the same time, it will not work since adding a new entry also requires changing the database content in general. Therefore, there is no point in separating these four permissions from one another but you should always consider them as dependent from one another.

For more information about rights management in Password Depot Enterprise Server, please visit our knowledge base:

How to ensure users can only see those objects they are allowed to?

Assign Database

The Assign database option is located in the Users and Groups area on the right.

Select one or multiple users/groups. Afterwards, click Assign database. Two tabs are available in the Assign database to dialog box:

Database

In this tab you can assign databases to single users and/or groups. Furthermore, you can also use this feature to assign a database to multiple users and/or groups at the same time or to create a new database and immediately assign this one to users and/or groups, too.

Selected accounts

You can see here all users or groups that have been selected for database assignment. All users and groups that have been checked here will have access to the corresponding database once the database assignment process has been completed.

Select an existing database

Select an already existing server database from the drop down-menu. This database will then be assigned to all checked objects in the Selected accounts area.

Create a new database

You can create a new database and assign it to all checked objects in the Selected accounts area.

Create a private database

You can create a new private database for every checked object in the Selected accounts area. This feature is helpful if you have many server users and would like or have to additionally provide private databases to all these users. Those private databases include the corresponding user name of the user they were created for and thus can easily be detected. For example, a private database that was created for the user "John Smith" will be displayed in the Server Manager with the following description: Private_DB_John Smith.pswe. You can also create private databases and assign them to groups.

Permissions

In this tab you can set permissions at database level for the databases you would like to assign to single or multiple users/groups at the same time. All selected users/groups will then have the same rights at database level. However, we recommend performing detailed rights management for users and groups in the database permissions dialog box.

Groups

Administrators can add new groups to the server or edit already existing ones in the Groups area. However, access rights for groups should be defined in the Database area by clicking Permissions. A group consists of one or several members (users). By creating groups, you can simplify server management because you can assign rights and permissions to whole groups instead of assigning them to single users.

The main view of the Group area displays the following columns:

- Name: Displays the name of a group.
- Type: Displays the corresponding type of group. The Server Manager includes Standard groups (local group, manually created by the server administrator), Azure AD groups (groups that have been imported through Azure AD synchronization) and Active Directory groups (groups that have been imported through Active Directory synchronization).
- Domain: Displays the name of the root domain which is used for server configuration and Active Directory synchronization. Active Directory groups were imported into the Server Manager from this domain.
- Description: Displays the group description if added. You can add a description when creating the group or editing it at a later point of time.

Besides, more options are available on the right:

- New group: Use this button if you would like to add new, local standard groups to the Server Manager. The dialog window New group will be displayed afterwards. You can enter here the group name as well as a group description, if required.
- Properties: Open the group properties dialog box.
- Delete: You can delete selected groups in the Server Manager.
- Synchronize: You can use this option to synchronize selected groups with Active Directory or Azure AD separately without launching the Active Directory or Azure AD wizard and start the whole synchronization process all over again. In any case, however, please note that this option can only be used if the respective group was added to the Server Manager through Active Directory or Azure AD synchronization before. Therefore, the Synchronize option in the Groups area can be used, for example, for updating an already existing group in the Server Manager separately if

their Active Directory/Azure AD data has changed. In this case, it will not be required to perform AD/Azure AD synchronization in general, if individual groups need to be updated only.

- Assign database: Administrators can assign single databases to single or multiple groups at the same time. Besides, they can also create new server databases here and assign them to single or multiple groups at the same time subsequently. In the Permissions tab administrators can assign group rights at database level right away. You can also create private databases for your groups here. Those private databases are also stored to the company's server. You can find out more about private databases in the chapter Assign Database.
- Select all: Select all groups available in the Server Manager. You can then perform further actions with them which will be applied to all server groups.

HINT: You can also access these options by right-clicking a group from the list. Apart from that, you can also filter the main view, for example if you would like to search for a specific group. To do so, enter the group name or a part of it to start search.

New Group

As is the case with Password Depot Enterprise Server users, you can choose one of the following options to add new groups to the Server Manager:

1. Using the button **New group**
2. Through **Active Directory Synchronization**
3. Through **Azure AD Synchronization**

Add new groups manually

You can add **new, local standard groups** to the Server Manager manually using the **New group** button available in the **Groups** area on the right. Add a group name afterwards. If required, you can also add a detailed group description to the **Description** field. Manually created, local groups are **standard groups** always and you cannot change that. Using the **Members** tab you can add new users to a group afterwards. For more information, please also have a look at the chapter Group Properties.

HINT: You can add **local users** as well as **Active Directory** or **Azure AD users** to standard groups. Depending on the corresponding user type, the group members will choose the appropriate authentication type for the Enterprise Server login.

Add new groups through Active Directory synchronization

You can also add **Active Directory groups** to the Server Manager (through **Active Directory synchronization**). This may be helpful, for example, if you would like to use already existing Active Directory groups in the Server Manager also. To start synchronization, open the Server Manager and go to **Tools → Active Directory Synchronization**. The group objects will then be imported into the Server Manager from Active Directory. If synchronization could be completed successfully, you can see all objects that were imported from Active Directory in the **Groups** area afterwards.

Password Depot also supports nested AD security groups.

WARNING: If group A is a member of group B and group A is imported via the built-in AD synchronization wizard, group B and its users will also be imported (if not

unchecked manually). If any users get unselected Password Depot will not import the coresponding group but only the selected users.

When you launch the wizard you will first have to provide information about the domain you would like to use for importing users/groups to Password Depot Enterprise Server:

Groups that have been added to the Server Manager through Active Directory synchronization will also include the corresponding Active Directory users/members automatically. If a database is assigned to an Active Directory group afterwards, all group members (=AD users) can logon to the Enterprise Server through Integrated Windows Authentication (SSO). Again, please note the following in this case: During authentication a user's user name and password will be sent to the Active Directory. A message will then be sent back to Password Depot saying that the data sent is either correct or wrong. Based on this information the login will either be completed (if the data sent is correct) or denied (if it is wrong). Therefore, it is important that the user data available in the Server Manager corresponds to the user data in the Active Directory. Thus, we recommend performing Active Directory synchronization on a regular basis in order to transfer changes from the Active Directory into the Server Manager, too.

HINT: Find out more about Active Directory synchronization in the chapter of the same name.

Add new groups through Azure AD synchronization

If administrators want to work with Azure AD groups in the Server Manager, synchronization is required, too. To start synchronization, open the Server Manager and go to Tools → Azure AD Synchronization. The group objects will then be imported into the Server Manager from Azure AD. If synchronization could be completed successfully, you can see all objects that were imported from Azure AD in the Groups area afterwards.

As is the case with Active Directory groups all Azure AD groups, that have been added to the Server Manager through Azure AD synchronization, will also include the corresponding Azure AD users/members automatically. If a database is assigned to an Azure AD group afterwards, all group members (=Azure AD users) can logon to the Enterprise Server using the Azure AD Authentication.

HINT: Find out more about Azure AD synchronization in the chapter of the same name.

See also: Add Users, Add users by department

Group Properties

The Group properties dialog box is available for every group in the Server Manager. You can access the group properties either by double- or right-clicking a group in the Groups area.

Administrators can edit the groups in the user properties dialog window. The following tabs are available here:

- General
- Members
- Members Of
- Administrators

The content of both tabs is explained below.

General

In the General tab you can define the following settings:

- Name: Enter the name of a group.
- Type: Displays the type of group, fore xample an Active Directory or standard group if the latter was created manually in the Password Depot Server Manager.
- Description: Optionally, you can add a group description. If a group has been imported from Active Directory or Azure AD, the group description will also be imported into the Server Manager, too.

You can disable an existing group in the Server Manager by checking the Disabled box at the bottom on the left. Uncheck it to activate the corresponding group again (if disabled). This way you can disable server groups temporarily, for example, if you do not want to permanently delete them but also do not need them for some time. You can easily activate a group again by removing the checkmark and thus, enable it again in the Server Manager if required.

Members

In the Members tab you can do the following:

- See the members of a group
- Add new members to a group
- Remove members from a group

The members of a group

You can see all members of a group in the **Members** tab of the group properties. The following information about the members is displayed here:

- **Account:** Displays a member's user account (= the member's username).
- **Type:** You can see here if group members have been assigned additional server roles in the Server Manager, for example Database or Account Administrator. You can find out more about the server roles here.
- **Full name:** Displays a member's full name as it was entered in the user properties.
- **Department:** Displays a member's department provided it has been added to the Server Manager.
- **Description:** If you added a user description in the user properties it will be displayed here, too. If a group member has been imported from Active Directory or Azure AD, the user description will be imported too and displayed here in the **Members** tab.

Add new members to a group

Click the **Add users** button to add new users to a group.

- **Add users:** If you select this option, the dialog window **Users** will open. Afterwards you can see all users available on the server. You can select single users and click **OK** to add them as members to the corresponding group.

NOTE: You can also highlight multiple users in order to add them to a group at the same time. Besides, the dialog window **Users** also contains a search box. Enter a username to start searching for individual users you would like to add to the group.

- **Add users by Department:** If your users have been assigned different departments (you can check that in the **General** tab of the user properties), you can also add new users to groups by department. In the **Add users by Department** dialog window you can select the desired department first. On the left, you can see the **Department**

members in the Group box. It displays all the department members of the selected department who have already been added as members to the corresponding group. On the right, you can see the Other Department members box. It displays all other department members. Those users also belong to the selected department but have not been added as group members to the corresponding group (yet).

Remove members from a group

Use the Delete button to remove single users from a group.

> NOTE: Users who have been removed from a server group will not be automatically removed from the Server Manager too. Removing a member from a group does only mean that he is not a part or member of the corresponding gropu anymore. However, this user will then still be available in the Server Manager though and count as active user.

Administrators

In this tab, you can assign administrative group rights to users. Note that it is important to combine this with the Group Administrator server role, which can be assigned via Users → <User > → Properties → Roles, to grant the respective users, access to the Server Manager.

Notifications

In the Notifications area you can set and manage specific notifications which should be sent to selected persons by email if certain events occur.

The main view of the Notifications area displays the following columns:

- ID: Every notification created on the server contains a specifc ID, starting from 1. For example, if you have created 10 separate notifications on the server, they will be assigned the IDs 1-10. The first notification added to the server will be assigned the ID 1 and all other notifications will be assigned the corresponding ID depending on the order created on the server.
- Type: Displays the type of notification or moreover the event the corresponding notification should be sent to the recipients.
- Notes: You can add individual notes to be included in a notification. These notes will then also be displayed in the Notification areas main view.
- Recipients: Displays the recipient(s) (email address) of a particular notification.

Besides, more options are available on the right:

- New notification: Using this button, you can create a new notification on the server.
- Properties: Click this button to open the notification properties dialog box, for example to edit an already existing notification.
- Delete: Use this button to delete already existing notifications and remove them from the Server Manager.
- Select all: Select all notifications displayed in the main view. You can then perform further actions which will be applied to all notifications available in the Server Manager.

HINT: You can also access these options by right-clicking a notification from the list. Apart from that, you can also filter the main view, for example if you would like to search for a specific notification. To do so, enter parts of the corresponding notification type to start search.

New Notification

To add a new notification to the server go to the Notifications area and click New notification on the right.

The New notification dialog window will open afterwards.

Choose an event from the drop down-menu which should trigger a notification to be sent by email to individual recipients. You can add additional notes to be included in the notification email, if required.

Next, enter the recipients' email addresses. The corresponding notification will then be sent to all persons from the list. How to add a new recipient is explained in detail in the Notification Properties.

Finally, click OK to add the new notification to the server. It will be displayed in the Notification area's main view subsequently.

Notification Properties

The Notification properties dialog box is available for every notification in the Server Manager. You can access the notification properties either by double- or right-clicking a notification in the Notifications area.

You can use the Notification properties dialog box to manage already existing notifications. The following tabs are available here:

- General
- Advanced

The content of the single tabs is explained in detail below.

General

In the General tab you can set the following:

- Event: Choose an event you would like the Enterprise Server to send a notification. May different events can be selected here, for example "A failed login attempt by a user" or "A new database has been installed" etc.
- Notes to include in notification: Here, you can add individual notes to be included in the notification email
- Send email notification to recipients: You can see here all the recipients who will receive an email as soon as the corresponding event occurs.

You can enter a new email address in the drop down-menu at the bottom of the dialog box or select an already existing one from the list. Click Add afterwards, to save the corresponding email address and add a new recipient.

If you would like to replace an email address from the list, you can highlight it and enter a new email address in the drop down-menu (or choose another already existing address from the drop down-menu). Finally, click Replace.

If you would like to delete an email address from the list of recipients, select the correct one and click Delete afterwards.

Advanced

The Advanced tab cannot be used for all notifications available on the server. It is only important for specific ones. If it is activated, you can further specify here when to send the corresponding notification. For example, you can set that the notification should be limited to single databases, database entries, users or groups. If the specified event occurs on the server in general, a notification will not be sent by default and only if it is referred to a specific database or if it was triggered by a specific user etc.

Users and Groups

- All users and groups: Select this option if the notification should be triggered by all server users and groups.
- Selected users and groups: Select his option if the notification should be triggered by specific server users and/or groups only. Click Add to add individual users/ groups to the list or Remove to delete user/group objects from the list.

Objects

- All databases: Select this option to apply the notification to all server databases.
- Selected databases: Select this option to apply the notification to specific server databases only. In this case, a notification will only be sent if the event connected to it occurs within a specific database from the list. Click Add to add individual databases to the list or Remove to delete single databases.
- Selected entries: You can apply the notification to single entries also. In this case, the notification will only be triggered if the event connected to it can be referred to a single entry from the list. Click Add to add a single entry to the list or Remove to delete single entries.

Log

The Log area displays a detailed log of server activity.

The server logs have a standard format according to RFC 5424 for easy processing in external log analyzers. Optionally, you can also send all log recordings in real-time mode via UDP to external log servers for audit-proof processing and storage. You can find additional server log settings in the server's general server settings.

The main view of the Log area displays the following columns:

- Severity: You can see here which kind of log entry was registered. For example, log entries may be Informational or an error may be registered on the server which will then be displayed as Error, too.
- Date and time: Displays the exact date and time a server activity was logged.
- User name: Displays the user (with their user name) responsible for the corresponding server activity.
- Address: Displays a user's IP address or the IP address a server activity can be related to.
- Event ID: Every single event has a specific event ID.
- Event description: You can see here which kind of activity was carried out by a user/group and therefore logged, for example Database sent to the user, Exporting entries or Log on with a client application etc.
- Database: You can see here which databases were accessed and within which databases server activities were logged.
- Object: Displays the object (folder/entry) which was accessed within a specific database.
- New object: If an entry or folder is modified or moved, for example, the procedure is logged in the New object column. You can then see here which object was updated or replaced by something else, for example.
- Reason: In case an error is logged on the server, this column will show the reason for this error. Besides, it may be mandatory for server users to specify a reason when deleting folders and entries within server databases. If so, users must enter a

reason if they would like to delete objects. This reason will then also be displayed here.

Besides, more options are available on the right:

- Open log: Use this button to open an already existing log file (*.log) in the Server Manager.
- Export log: Here, you can export the server's log either to the XML or CSV format and save it accordingly.
- Advanced filter: Use this button if you would like to filter the log entries in more detail.

HINT: You can use the filter box in the upper left corner of the Log area's main view to search for specific events in the server log. For example, enter a server user's username to display all events related to the corresponding user.

-

S

U

W