

Manual

Password Depot Enterprise

Server 15

Last updated: 09.09.20

Return to the [Password Depot homepage](#) (leave this help)

Table of Contents

| | |
|--|----|
| Introduction | 3 |
| Installation and running | 4 |
| Migration | 6 |
| Server Manager | 7 |
| Server Manager | 7 |
| Manage | 8 |
| Manage | 8 |
| Server Settings | 9 |
| Server License | 12 |
| Server Policies | 13 |
| Server Policies | 13 |
| Permissions | 14 |
| Security | 15 |
| Client Security Policies | 16 |
| Program Options | 17 |
| Tools | 18 |
| User login to AD | 18 |
| Active Directory Synchronization | 20 |
| Reports | 21 |
| Databases | 22 |
| Databases | 22 |
| Add Databases | 23 |
| Properties | 24 |
| Users | 26 |
| Users | 26 |
| Add User | 27 |
| Properties | 29 |
| Permissions for users | 30 |
| Assign Database | 31 |
| Groups | 32 |
| Groups | 32 |
| New Group | 33 |
| Notifications | 34 |
| Notifications | 34 |
| New Notification | 35 |
| Properties | 36 |
| Log | 37 |

Introduction

Password Depot Enterprise Server is an extension for **Password Depot**. Using the Enterprise Server, clients (i.e. the main program Password Depot) can share one or more databases located on a server in a network. The main Password Depot program serves as client.

Password Depot Enterprise Server is installed on a computer in the local network. There, the administrator sets up the users with the Server Manager and assigns them access rights for desired databases or elements within the databases.

Authorized users can use the **Password Depot main program (client)** to access databases on the server which they are authorized to. This requires the IP address and the port of the server as well as login data (user name and password) set up by the administrator. Apart from that, Integrated Windows Authentication (SSO) is also possible.

NOTE: The database is opened by the server and made available to users. If you want to make an already existing database available on the server, enter its master password in the Server Manager.

A user who wants to access a database provided by the server does not do so by using the master password of this database, but by using the user name and password he has received from the server administrator. The administrator also determines which databases a user can retrieve and also sets the access rights.

Clients can open databases through the server and use the data they contain. Clients can also modify entries if they have the appropriate permissions to. In this case, **Password Depot Enterprise Server** locks the entry which is currently being edited so that no other changes can be made by other users at the same time, thus avoiding conflicts. However, it is possible for several users to simultaneously work on the same database.

The number of users you can set up on the server is defined by your license. For example, if you have purchased a license for 25 users, you can set up 25 users **at maximum** etc.

NOTE: No license is required for the use of the Enterprise Server **up to three users**. In this case, you can use it without a license.

Return to the [Password Depot homepage](#) (leave this help)

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 order to do so, the computer must be assigned a fixed IP address in the local network.

NOTE: You may install the Enterprise Server (e. g. for testing purposes) on your local computer. In this case, to access the server using **Password Depot**, specify the server address 127.0.0.1 or localhost.

Installation as Windows Service or Windows Application

Password Depot Enterprise Server can run in two modes: As normal Windows application or NT Service. By default, the server is installed as NT Service during installation. To install it as Windows application, select the according option while installing.

IMPORTANT: Upon installation you must decide whether you want to install Password Depot Enterprise Server as service or application. If you select the service option the service will be set up during installation. It is recommended to install the server as service.

If installed as service, the server will be listed as **Password Depot Enterprise Server 15**. Please use the Windows control panel to start or stop the service.

If you have installed the server as application, you will find it in the program folder (by default this is C:\Program Databases \AceBIT\Password Depot Server 15 in Vista, Windows 7, 8 and 10 and C:\Programs\AceBIT\Password Depot Server 15 in XP).

Since version 14 onwards the Password Depot Enterprise Server supports 64-bit architecture.

Server Manager

The Server Manager is a separate managing tool for **Password Depot Enterprise Server**. It allows administration of the server. Further, many different options can be set up with this tool. You can access the Server Manager only from the computer the server is executed on.

To open, click **Start** and choose from the start menu **AceBIT -> Password Depot Server Manager 15**.

The server will be installed with the following default login credentials:

User name: Admin

Password: admin

IMPORTANT: It is highly recommended to change these default credentials (for the user *admin*) in the Server Manager following installation. To do so, go to **Users -> admin -> Account** in the Server Manager and change login credentials under "Use Password Depot authentication".

Normally, **Password Depot Enterprise Server** starts automatically on Windows start-up and runs in the background on your computer. 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.

Update Manager

Since version 14, **Password Depot Enterprise Server** works with an integrated update manager. Hence, the server administrator will receive a notification as soon as a new version is available for download. This feature is available under **Help -> Search for updates**.

Return to the [Password Depot homepage](#) (leave this help)

Migration

If you have already worked with a previous version of the **Enterprise Server**, you can easily migrate to the current one.

Please note that the server can only work with clients of the **same main version**. This means that you can't access a server of version 14x with a client of version 10x. Therefore, you always need to update both, your clients and the Enterprise Server to the new version.

Migration of the Enterprise Server is explained in the knowledgebase.

Return to the [Password Depot homepage](#) (leave this help)

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 must first [connect to the server](#) to see the features described below.

The Server Manager's navigation area includes five tabs:

- **Databases:** This tab is used for creating and managing databases on the server.
- **Users:** This tab contains commands for managing clients (users).
- **Groups:** Using this tab you can divide users in groups.
- **Notifications:** With this tab you can set up email notifications for certain events.
- **Log:** This tab displays the server activity log.

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

- **Status:** Shows if the server is running currently or if it has been paused.
- **Server address:** Shows the server's IP address.
- **Server port:** Shows the port which is used by default for connecting to the Enterprise Server.
- **Running since:** Shows the exact date the server has been put into operation for the first time.
- **Server version:** Shows the latest server version or server build of a main version.
- **Updates available:** Shows if any new updates within the same main version are available for installation.
- **Installed licenses:** Shows how many licenses are allowed on the server (server size).
- **Registered users:** Shows the number of users registered on the server.
- **Connected users:** Shows how many users are connected to the server currently.
- **Installed databases:** Shows how many databases are installed on the server in total.

Return to the [Password Depot homepage](#) (leave this help)

Manage

This menu item includes the following elements:

- **Server settings:** You can set up basic server configurations and, among other things, define, for example, where backups should be stored and how often they should be created.
- **Server license:** You can enter a license key in order to increase the number of allowed clients.
- **Server policies:** You can define default permissions for databases. Permissions for single databases can still be set up *individually*.
- **Client security policies:** You can change local security policy for corporate clients.
- **Pause:** Pauses the availability of the server for all clients. The server will still be available though, so that any maintenance work can be carried out.
- **Continue:** Continues a paused server, so that it will be available again for all clients in a network.
- **Restart:** Select this option to restart the server if and when necessary.
- **Program options:** This option allows you to adjust program options (not to be mixed up with [Server settings](#)).
- **Exit:** Exits the Server Manager. The service or server application is not affected.

NOTE: Some changes made on the Enterprise Server require a server restart in order to save changes. With version 15 a command for restarting the server has been implemented. When it is needed, the prompt will be shown automatically by the program itself.

Return to the [Password Depot homepage](#) (leave this help)

Server Settings

The **Server settings** dialog box can be found in the menu item **Manage**. It includes six tabs: **General, Connections, Logging, Additional, Email** and **2FA Settings**.

General

Server

Here you can make basic settings on the server:

Server language: Allows you to select the language.

Server port: Specifies the port by default.

Use SSL/TLS: Enables the use of an SSL/TLS connection between client and server.

Use SSL/TLS for REST Server: Enables the use of an SSL/TLS connection for REST Server connection. With the REST server implementation, the Enterprise Server can now be accessed via REST API. A new web interface is made available in the source code for demonstration purposes or for productive use. Internally it is a web server which can use HTTP or HTTPS (recommended) protocol. In order to use HTTPS, you need to install a valid SSL certificate.

Install certificate: Allows you to [install an SSL certificate](#). If you wish to use this option, a dialog box will open where you can enter your certificate file and its key.

Databases

Storage folder: You can define the path where databases should be stored by default.

Connections

Supported authentications

Specify which authentication you would like to allow on your server. You can use either authentication with **User credentials (account and password)** and/or **Integrated Windows Authentication (Single Sign On)** here.

Supported clients

Specify which clients should be supported for connection to the server. The following options are available here:

- **Standard Edition for Windows**
- **Corporate Edition for Windows**
- **Mobile Edition**
- **macOS Edition**
- **Web Client**

NOTE: All clients that should be able to connect to the Enterprise Server need to be activated in the Server Manager. If a client is unchecked here, users won't be able to connect to the Enterprise Server with this edition.

New connection from different device

Select one of the three available options here to specify how connections from other devices should be handled if carried out by the same user.

Inactive sessions

Specify how Password Depot Enterprise Server should handle inactive connections.

Failed logins

Specify the number of failed login attempts a user can carry out before his account will be temporarily blocked. If a user account has been 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".

Logging

In this tab you can adjust the settings referring to the **Password Depot Enterprise Server's** logs. The following options are available here:

Local log

- **Logs folder:** You can see here the local directory for storing the Enterprise Server's logs by default. You can adjust it by using the "Browse" button.
- **Max. file size (KB):** Determine the maximum size (KB) of the server's log file.
- **Create new log file:** Here, you can define the interval for creating new log files.
- **Delete logs:** Define the settings for deleting already existing logs. You can either select to never delete any log files created or determine a specific number of log files that should be kept, 30, for example (this number is set by default): This means that the latest 30 files will be saved and older log files will be deleted.
- **Remote log:** Check the box "Send log messages to a remote server" if you wish to activate this option and send the Enterprise Server's log files to external log servers. You can further adjust the server address and port of the external server where logs of the Enterprise Server should be sent to. Thus, you can ensure that protocols are not being manipulated.

Additional

In this tab, you can specify your settings for backup copies, among others:

Backup

- **Backup folder:** You can specify where backup copies should be saved to. Use the **Browse button** on the right to select a different directory.
- **Backup databases on every startup:** Select this option in order to create a backup copy of existing databases each time the program is started.
- **Backup databases every:** Determine a specific number of hours after which **Password Depot Enterprise Server** will automatically create a backup copy of existing databases.

NOTE: By default, both options for creating backups are checked and we further recommend to keep both options activated while working with the server.

- **Log backups to file:** If you select this option, the program will create a log of backups generated and will save it to the specified file so that you will be able to track when backups of databases were created at a later point of time.

Active Directory:

- Specify whether to perform AD synchronization automatically. If so, you will also be able to determine the time interval automatic AD synchronization should take place. Furthermore, you can also specify what to do with users and groups not (no longer) found in AD. Those users can be **ignored**, **deactivated** or **deleted** by the Server Manager.

NOTE: Synchronization should preferably be initiated by the administrator manually for a given reason. If automatic synchronization is required, synchronization cycles should preferably be at times when server load is low and, for

example, every 24 hours (1140 minutes).

Edit entries

- The administrator 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 desired. 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.

Email

In this tab you can define your settings for email notifications:

- **Sender:** You can enter here the sender's email address and name.
- **Outgoing Mail Server:** You can configure the outgoing mail server here.
- **Test Connection:** You can enter the email address of a recipient here and send a test email to check the settings previously made.

2FA Settings

You can select here whether you would like users to log in on the server with **Two-Factor Authentication**. You can choose Two-Factor Authentication with two options: **TOTP** and **email**. By activating the option **Users may choose to remember their devices (days)** the administrator can determine 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 in x days if provided that the user enables the option **Trust this computer** when connecting for the first time and entering the required code once.

The option **Email code expiration time (minutes)** determines the validity of a code sent by email for Two-Factor Authentication. By default, this is ten minutes. However, this time can be adjusted here by the server administrator. If a user does not enter the required code in time, the latter expires. A new code will then be necessary in order to authenticate successfully.

Please visit our knowledgebase in order to get [more information about Two-Factor Authentication](#).

HINT: Both Integrated Windows Authentication and Password Depot authentication support support Two-Factor Authentication. Under **Users -> <USERNAME> -> Accounts** Two-Factor Authentication can be deactivated for single users individually, if necessary. Read more about this option in the chapter [Add User](#).

Return to the [Password Depot homepage](#) (leave this help)

Server License

Click on **Manage -> Server license** to add a server license of more users.

You will see a dialog window where you will find information about the currently used server licence and in the empty field below you can enter a new unlock code to increase the number of supported clients on the server. Besides, you can also see here which server version is currently installed.

NOTE: The number of supported clients always refers to the number of users **that can be created on the server.**

Return to the [Password Depot homepage](#) (leave this help)

Server Policies

The **Server policies** dialog box can be accessed by clicking the **Manage** menu item.

You can set default permissions for users here which are referring to rights management of clients. Besides, you can also determine different security related settings for all clients here.

The dialog box is divided into three different tabs: **Permissions**, **Security** and **Entries**.

See also: [Rights management in Password Depot Enterprise Server](#).

Return to the [Password Depot homepage](#) (leave this help)

Server Policies - Permissions

You can adjust the settings to be used by default in the **Permissions** tab of the Server policies. These default settings will apply for all users and databases.

1. If you select **Not defined**, you can set the appropriate permission for each user and database individually in the database's properties.
2. If you select **Enabled**, the corresponding permission is set as enabled for all users by default. However, you can still change it for individual users/databases.
3. If you select the most restrictive option **Disabled**, the corresponding permission won't be available by any user. You won't be able to adjust this permission for individual users/databases later.

NOTE: By clicking on the button **Restore default settings** you can restore the settings of the Server Policies' **permissions** tab and get back to the server's default settings.

See also: [Rights management in Password Depot Enterprise Server.](#)

Return to the [Password Depot homepage](#) (leave this help)

Server Policies - Security

You can define different security related settings for your clients in the **Security** tab of the Server policies' dialog box:

- Select the option **Check passwords quality against dictionary attacks** if users should receive a warning every time they are using a password which is not secure against dictionary attacks.
- Below, you can determine **preferred rules for passwords** which you want users to follow when adding new passwords (does also apply for master password): You can define the minimum length passwords should have by default and decide further, which kind of symbol types (lower case, upper case, numbers, special characters) you want to be used.

NOTE: By clicking on the button **Restore default settings** you can restore the settings of the Server Policies' **security** tab and get back to the server's default settings.

Return to the [Password Depot homepage](#) (leave this help)

Client Security Policies

The **Client security policies** allow you to define various features for all Corporate Clients through the Server Manager. In order to take effect, Client security policies must be activated first in the Server Manager. For more information about the Corporate Edition of Password Depot, please click [here](#).

Master Password Policy

Allows you to specify requirements the master password needs to fulfill when creating local databases with the client.

Enforce Password History: Determine the number of new master passwords a user is forced to use or create before an old or previous password can be reused.

Maximum Password Age: Determine a special period of time (days) a master password can be used by a user before he will be asked by the program to change it.

Minimum Password Age: Determine a special period of time (days) a master password must be used by a user before changing it.

Minimum Password Length: Determine how many characters a master password needs to have at minimum.

Password must meet: Determine how many different character types a master password must include at least (Lowercase, Uppercase, Special, Numbers).

NOTE: These settings refer to the master password only, but not to any entries within a database!

Allowed Storage Policy

You can determine here which locations (e.g. local system, cloud services etc.) clients should be allowed to use for storing databases.

Actions Policy

Specify whether actions such as printing or exporting should be allowed.

New options in version **15** are:

- **Use TANs**
- **Set Second Passwords**

Program Options

Allows definition of security relevant program options.

Return to the [Password Depot homepage](#) (leave this help)

Program Options

The **Program options** refer to the Server Manager's settings.

By going to the section **Application language**, you can select the language of the interface.

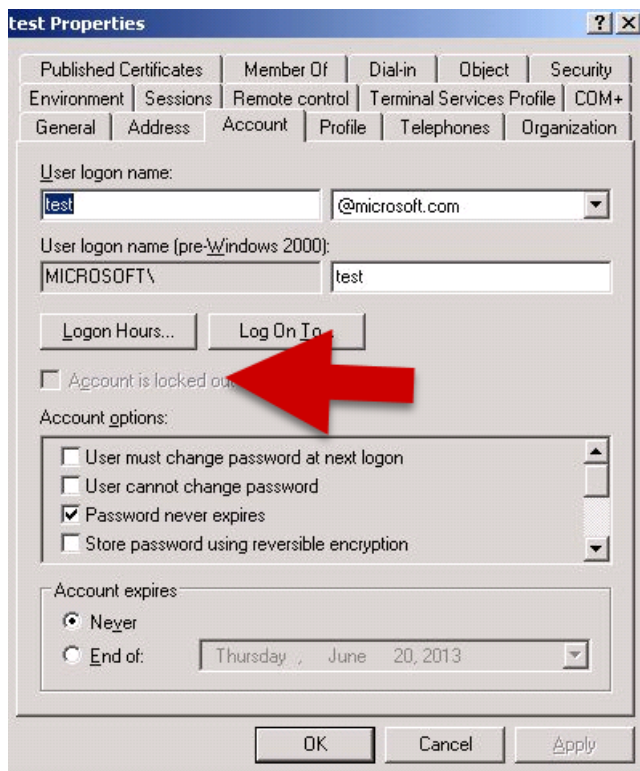
In the **SSL/TLS Settings** section, you can select if the Server Manager should connect to the server service via SSL/TLS.

Return to the [Password Depot homepage](#) (leave this help)

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.

Return to the [Password Depot homepage](#) (leave this help)

Active Directory Synchronization

In the **Tools** menu, choose **Active Directory Synchronization** to start the wizard of the same name.

The WinNT provider has been replaced by a more powerful LDAP provider since version 14. Furthermore, extended functionality for Active Directory synchronization has been implemented.

When opening the wizard, please enter the following information in a first step:

- **Domain name:** Type in or select a domain name from the list.
- **Sign in as current user:** Select this option if you wish to login with the current user in order to start Active Directory synchronization.
- **Use this account:** Enter user name and password of a user who has permission to read data from the Active Directory of the domain. Usually, this should be the domain administrator.

Regarding Active Directory synchronization, you will also be able to choose from further different options here, that is **Recursively scan all containers** and **Check deleted objects**. If the option **Recursively scan all containers** is checked the wizard will read the entire directory. In some cases, this may take some time. We recommend to only use this option the first time after porting data from an older version of Password Depot Server in order to replace all WinNT paths with LDAP paths. However, if this option is not selected, the wizard works like a usual Active Directory explorer, i.e. it only opens the specified object or container and scans the container when you expand the node afterwards.

Then, click **Sign In** to continue.

If login was successful, the Active Directory tree will be listed next.

Check users and/or groups here that should be imported or updated in **Password Depot Enterprise Server**.

If you have a large number of entries, you can filter them by using the **Filter** option at the bottom on the left.

If you right-click on the Active Directory tree, different features will be available in order to speed up selection.

Select desired users and/or groups by checking the boxes. In addition to that, you can also see in this dialog window further attributes of users in the Active Directory as well as their value.

Afterwards, click **Synchronize** and results of synchronization will be displayed in a new dialog window.

NOTE: All imported users from Active Directory can log in with their accounts and passwords from Windows NT by default. You can change this in the user's properties.

HINT: With **version 15**, users and groups can also be synchronized individually with the Active Directory.

Return to the [Password Depot homepage](#) (leave this help)

Reports

In order to get a better overview of users and databases on the server you can generate reports in the **Tools** menu. You can either print these reports or save them using various formats (.html, .mht, .txt).

Databases Report

By using the option **Databases report** you can generate a report which lists all databases from Password Depot Enterprise Server. Furthermore, with the databases report, you will also get an overview of users and their individual permissions and you can see which user has access to which database. This report can be saved and printed.

Granted permissions are shown by a ✓ in the corresponding column, whereas **Denied** permissions are represented by an **empty field**. The columns are arranged the same way as they are in the advanced tab in the database's properties.

Users Report

By using the option **Users report** you can generate a report which lists all user accounts from Password Depot Enterprise Server. In addition to that, you will also see which databases are assigned to which user and the users report also shows individual access rights of every user for every database. This report can also be saved or printed.

Return to the [Password Depot homepage](#) (leave this help)

Databases

The **Databases** section lists all databases on the server. You can add new databases here or delete existing ones. Apart from that, this is the section where you assign access rights to existing users or groups for individual databases.

The **list view** in the databases section gives you an overview of already existing databases, their size, modification date as well as the number of database entries.

Besides, you can also see how many users are currently connected to a database.

If you are working with a large number of databases, you can enter a **filter** at the top in the corresponding field in order to narrow the display. To do this, enter a whole database name or part of it.

The following features are available here:

- **New database:** With this button you can open the dialog box [Add database to server](#).
- **Properties:** A dialog box will open where you can have a look at the **Properties** of a database and edit them. In addition to that, you can assign different rights to users and groups for the corresponding database.
- **Delete:** With this button you can delete databases from the server's working directory. If a client is simultaneously using a database, they will receive a note when trying to save it.
- **Rename:** Rename a selected database.
- **Select all:** Select all databases from the list view.

HINT: You can also access these options by right-clicking on a database in the list.

Return to the [Password Depot homepage](#) (leave this help)

Add Database to Server

This dialog box has two tabs:

- **Add existing database**
- **Create new database**

Add Existing Database

Choose this option to add an already existing database to the server.

- Click on the **Browse** button in order to select the corresponding database.
- Enter the master password of this database in the corresponding field named **Master password**.
- Activate the **Hide** option in order to mask your master password's characters.

NOTE: After having added an already existing database to the server, it will be copied to the server's database directory and the master password is changed so that it will correspond with the password of the admin account.

Create New Database

Select this tab to create a new, empty database. Enter the desired database name and, if required, also add a comment.

NOTE: The administrator's password will be used as master password for newly created databases. However, to open a database on the server, clients will use the password which has been assigned to them by the administrator.

Return to the [Password Depot homepage](#) (leave this help)

Database Properties

In the **Properties** of a database you assign access rights to users and groups.

General

In the **General** tab you can have a look at basic information about the selected database. For example, you can see here how many users are currently connected to it.

Security

In the **Security** tab you can **add** users or groups to the database so that they will be able to access it afterwards or you can **delete** users or groups if you do not want them to have access to the selected database anymore.

In the bottom area of the dialog window you will find the **Permissions on the database** and **Permissions on entries and folders** tabs.

Permissions on the database

Highlight a user or group in the upper section of the security tab in order to define **permissions on the database** for the selected element.

Please find more information about this topic in [Rights administration in Password Depot Enterprise Server](#).

Permissions on entries and folders

In general, permissions of a user or group should apply for the whole database. However, if you wish to grant special access rights also within a database, you can do this in the permissions on entries and folders tab. You can define access rights for individual folders or entries here.

Different permissions are available here and you can choose from the following:

1. **Access to entries**
2. **Read entries**
3. **Modify entries**
4. **Add entries**
5. **Delete entries**
6. **Access expired entries**

The permission **Add entries** is new in version 14 in this tab. With this option, the administrator can decide whether users/groups should also be able to add/create new entries in folders and sub folders of a database, too.

For more information about this topic, please read our article [Rights administration in Password Depot Enterprise Server](#).

NOTE: Both tabs **Permissions on the database** and **Permissions on entries and folders** include different formatting since version 14. By default, all options/permissions are depicted in **green** and bold letters. This means that all these permissions are allowed to users. Apart from that, all denied options/permissions are depicted in **red** and bold letters as well. This way, the administrator is able to recognize from the start which permissions have been allowed or denied to different users and groups.

Advanced

In the **Advanced** tab you can define whether you want to monitor and log all cases of user access to entries and whether users must specify a reason for deleting any entries.

NOTE: You can adjust default settings for these permissions in the server manager using the option **Server Policies**.

Return to the [Password Depot homepage](#) (leave this help)

Users

The **Users** area allows the administrator to add new users and edit or delete existing ones. However, users' access rights are granted in the **Databases** area by selecting the desired database.

Different features are available here. These are the following:

- **New user:** Open the **Add user** dialog box.
- **Properties:** Open the **User properties** dialog box.
- **Delete:** Delete selected users.
- **Duplicate:** Create a copy of selected users.
- **Disconnect:** Disconnect selected users from Password Depot Enterprise Server.
- **Assign database:** Allows you to assign databases to multiple users or groups simultaneously or to create new databases.
- **Reset 2FA:** If you are using **Two-Factor Authentication** for login on the server, you can choose this option in order to reset 2FA settings for one or several users. In this case, selected users will need to enter a new code next time they want to connect to the server. So, the option "Trust this computer" will be reset and all trusted devices for selected users will be deleted.
- **Select all:** Select all users.

TIP: You can also access these options by right-clicking on a user in the list.

Return to the [Password Depot homepage](#) (leave this help)

Add User

The **New user** button in the toolbar of the Users area allows you to create new users. By clicking the corresponding button, the **Add user** dialog box will open. You will find the following tabs here:

General

The **General** tab provides following options:

- **UPN:** You can enter the user's user UPN (User Principal Name) from the Active Directory here.
- **Full name:** Enter the user's first and last name.
- **E-mail:** Enter the user's e-mail address.
- **Department:** Enter the user's department.
- **Description:** Here you may add additional information about the user, if necessary.
- **ADs Path:** Enter the user's full Active Directory path.
- **GUID:**

Account

Settings can be adjusted as follows in the **Account** tab:

Log on to the server: You can define here if a new user should use their **Windows NT credentials** to log in on the server or if you would like to determine a user name and password for them yourself.

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, for example. Uncheck the box to activate the account again and thus enable a user to access and log on on the server again.

User may not change password: Check this box if you do not want to allow users to change their password for login on the Enterprise Server.

User must change password at next logon: Check this box if you want users to be forced to change their password for login on the Enterprise Server next time they want to login.

2-Factor Authentication deactivated: Check this box if you want to deactivate 2-Factor Authentication for one or several special users. Thus, you can activate 2-Factor Authentication for login on the server in general for all users but still deactivate it for special users, if and when necessary.

Roles

In this tab you can assign different server roles to individual users additionally. Role based access to the Server Manager can be guaranteed this way. The following roles are available:

- **Server Administrator:** This role grants full access to the server and the Server Manager. In general, a server administrator has full access to all databases and entries. In addition to that, he 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 adjust access rights of users and groups to 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.
- **Active Directory Operator:** An Active Directory Operator can manage the process of Active Directory Synchronization.
- **Event Log Reader:** An Event Log Reader has access to the server's logs.

Member of

You can determine here, if a selected user should be member of any groups and, if so, also decide which groups he should be a member of.

Add group: Click this button to add a user to a new group.

Delete: Select this option to remove a user from a group.

Advanced

The **Advanced** tab is divided into two sections:

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

WebSockets port for browser add-ons:

The administrator can determine the custom distribution of port numbers for the users' add-on in the Server Manager. Different options are available here:

1. Use the default port number (recommended)
2. Auto-generate unique port number
3. Use custom port number

If the administrator determines the default port number of a user in the Server Manager, then each user only needs to adjust the port number in the client accordingly.

IP address verification:

You can assign a fixed IP address to a user here, so that every connection attempt of this user with another IP address will be rejected. This can increase security, but it also requires using static IP addresses.

NOTE: The addresses 'localhost' and '127.0.0.1' are **always allowed**, so that the administrator is able to adjust wrong settings on the server.

Return to the [Password Depot homepage](#) (leave this help)

User Properties

The **User properties** dialog window in the **Users** area allows you to see and edit the user's properties. For more information about the content of this dialog window see [Add user](#).

Return to the [Password Depot homepage](#) (leave this help)

Permissions for Users

In the **Databases** area, select a database and then go to **Properties** in the toolbar to set rights for users in the **Database Properties** dialog box.

Return to the [Password Depot homepage](#) (leave this help)

Assign Database

The option **Assign database**, located in the **Users** and **Groups** toolbar, allows you to simultaneously assign databases to multiple users or groups or to create new databases and directly assign them to selected users.

Select one or many users/groups. Afterwards, click **Assign database**.

Two tabs are available in the **Assign database** dialog box:

Database

Select an existing database

From the drop-down menu, select an already existing database which you would like to simultaneously assign to selected elements listed on the left under **Selected accounts**. Apart from that, you can also adjust permissions for the corresponding database in the **Permissions** tab optionally.

Create a new database

You can create a new database and assign permissions to selected elements listed on the left under **Selected accounts**. Apart from that, you can also adjust permissions for the new database in the **Permissions** tab optionally.

Create a private database

You can create a new **private** database for each selected element listed on the left under **Selected accounts**. Apart from that, you can also adjust permissions for the new database in the **Permissions** tab optionally.

This feature is useful if you have many accounts on the server and need or wish to provide private databases for your users.

Permissions

Specify **permissions** for previously selected databases here.

Return to the [Password Depot homepage](#) (leave this help)

Groups

The **Groups** area allows the administrator to add new groups to the server and edit or delete existing ones. However, access rights of groups are assigned to selected databases in the **Databases** area.

You can filter the displayed list of groups by using the corresponding field in the upper section of the dialog box. To do so, enter a group name or part of a group name to search for a specific group from the list.

General Information about Groups

A group consists of one or several members (users). In order to assign users to a group, open the **Users** tab.

By creating groups, you will be able to simplify management of the server because you can assign rights and permissions to whole groups instead of separately assigning them to single users.

Available Options

In the **Groups** area you can choose from the options below:

- **New group:** Allows you to create a **new group**.
- **Properties:** You are able to look at the properties of an existing group.
- **Delete:** Delete a group.
- **Duplicate:** Duplicate selected groups.
- **Assign database:** Allows you to simultaneously assign databases to multiple users or groups or to create new databases and directly assign them to selected users.
- **Select all:** Select all existing groups.

TIP: All of these features can also be accessed by right-clicking a group from the list.

Return to the [Password Depot homepage](#) (leave this help)

New Group

The **New group** dialog box consists of two tabs:

General

- **Group name:** Enter the name of a group.
- **Type:** Describes the type of group, e.g. AD group or standard, if it was created in Password Depot Server Manager.
- **AD path:** If a new group is an AD group, its path will be displayed here, e.g. WinNT://WORKGROUP/TEAMSERVER/User.
- **Description:** You can add a description of the group here optionally. If the group has been synchronized from Active Directory, the description is taken from there.

You can **enable** or **disable** the group by selecting the **Disabled** check box or not at the bottom edge of the dialog window.

Members

You can use the **Members** tab to either see which users are members of a group or you can add here single users to a group as well as remove users from a group (**Delete**).

In order to add members to a group you can choose from one of the two options available:

- **Add users**
- **Add users by Department**

Return to the [Password Depot homepage](#) (leave this help)

Notifications

In this area you can manage notifications which are to be sent by email to selected users if certain events occur.

In the notification toolbar, the following buttons are available:

- **New notification:** Add a new notification.
- **Properties:** Open properties of an already existing notification.
- **Delete:** Delete selected notifications.
- **Select all:** Select all notifications.

TIP: You can also access these options by right-clicking an already existing notification.

Return to the [Password Depot homepage](#) (leave this help)

New Notification

You can open the **New notification** dialog box by clicking the **New notification** button in the notification toolbar. This way, you are able to create a new notification. In total, this dialog box consists of two tabs: **General** and **Advanced**.

General

Here, you can adjust settings as follows:

- **Event:** Select an event which you would like to receive a notification for. You can select here from many different events available, such as a failed login attempt by a user or a new database has been installed. Three more events will be available with the release of version 14: **Expiration of entries, Bulk deletion of entries and Critical change of database size**. With the event **Expiration of entries** administrators and clients will now receive a notification if an entry has expired or if it is about to expire soon.
- **Notes to include in notification:** You can insert comments into this empty field which then will also be sent by email together with the corresponding notification.
- **Send email notification to recipients:** You can see the list of all recipients who will get an email when the selected event occurs.

In the drop-down menu on the left at the bottom edge of the dialog box, you can enter the **email address** or select an already existing one from the list. Then, click **Add** in order to add the specified email address to the list.

If you wish to replace an email address, select the one which had been used so far, then, enter the new email address in the empty field down on the left and click **Replace**.

In order to delete an email address, select it from the displayed list and click **Delete**.

Advanced

You can define here whether you want a notification for certain events to be limited to specified databases, database entries or users.

There are two options available here:

Users and Groups

All users and groups: Select this option if you wish the notification to apply to all users and groups.

Selected users and groups: You can choose this option in order to select individual users and groups which you want to receive this notification for.

Objects

All databases: Apply the notification to all databases.

Selected databases: Allows you to select specific databases which you want the notification to apply for.

Selected entries: If you set up a notification which refers to individual entries, this option is available, too, so that you will be able to select a specific entry from a database this notification should be sent for.

Return to the [Password Depot homepage](#) (leave this help)

Notification Properties

The button **Properties** in the notification toolbar will open the **Notification properties** dialog box. You can review them once again or adjust the notification's properties here, if necessary. For more information about this dialog box, see [Add Notification](#).

Return to the [Password Depot homepage](#) (leave this help)

Log

This view displays the **log** of server activity.

You can filter the displayed list of events in the upper area using the corresponding field.

In the log's toolbar, you can choose from the following options available:

- **Open log:** Allows you to open a log file (*.logx).
- **Export log:** Allows you to export the log to the XML or CSV format.
- **Advanced filter:** Allows detailed [filtering](#) of the protocol's records.

NOTE: You can change the log's language by changing the language of the server in the server settings.

The server logs have a standard format according to RFC 5424 for easy processing in external log analyzers. Optionally, all log recordings can be sent in real-time mode via UDP to external log servers for audit-proof processing and storage.

Return to the [Password Depot homepage](#) (leave this help)

Connect

In order to connect the Server Manager to the service, click **Server** -> **Status** -> **Connect**.

A new dialog window will open. Enter all necessary data in order to connect to the server.

- **User name:** Enter the user name (by default *admin*).
- **Password:** Enter the password (by default *admin*).

Return to the [Password Depot homepage](#) (leave this help)

Using an SSL Certificate

Password Depot Enterprise Server allows the installation and use of an **SSL certificate**.

WARNING: The installation procedure should be performed by an experienced administrator only.

Password Depot Enterprise Server supports **X.509** SSL certificates in **PEM** and **DER** format. Using a certificate allows users to validate the identity of a server before sending any confidential information.

Before deciding to use SSL connections, please consider the following:

- 1) SSL does **not** encrypt **data** transferred from the clients to the server. All data is **always** encrypted with AES 256-bit encryption by the internal protocol which is implemented through TCP/IP.
- 2) Due to cross-platform compatibility reasons, the **OpenSSL** library must be used which has some limitations and which is further not recommended by **Apple** for using it on their systems iOS and macOS.
- 3) Using self-signed certificates is **pointless** and also not supported. Certificates signed by a well-known **Certificate Authority** (CA) can be used for validation of Password Depot Enterprise Server only. If you already own a web server running on HTTPS, using its SSL certificate would be an appropriate solution. Otherwise, you may need to order a new SSL certificate from one of the recognized Certificate Authorities.
- 4) If you are going to use SSL connections you need to install a valid SSL certificate issued by a recognized Certificate Authority. The Enterprise Server can generate a **dummy certificate** to test the use of SSL connection if no other certificate is available. However, in practice, a dummy certificate is useless as it can easily be faked by third parties.
- 5) Using SSL in **local and internal networks** is **not recommended** as all data transferred between server and client is already strongly encrypted. In this case, using SSL does not increase the security of data transfer significantly but allows validation of the server and further helps to prevent **Man-in-the-middle attacks (MITM)**. This feature might be useful in external networks when clients should be able or need to connect to the server from any location.
- 6) If you decide to use an SSL connection, please make sure **all** clients (Windows, Mac OS X, Android and iOS) will use SSL! Mixed connections (that is, both SSL and standard TCP/IP) are **not allowed**.
- 7) In order to **install** an SSL certificate, you will need to enter the following:
 1. The fully qualified path of the certificate file on the server.
 2. If the above certificate contains both public and private keys, leave the field empty. If the private key is stored to a separate file, enter the full path of the private key here.
 3. The password for accessing the private key.

Restart the server to load the certificate and start SSL connections.

Return to the [Password Depot homepage](#) (leave this help)

Server Policies - Entries

In the **Entries** tab of the Server Policies the administrator can determine **different types of entries through the Server Manager centrally**. The admin can decide which types of entries are required or not by checking or unchecking the corresponding boxes.

1. **Select** all different types of entries you **would like your users to work with**. All activated types of entries will then be available in the client by default.
2. **Uncheck the boxes** of all types of entries you **do not want your users to work with** and should therefore not be available in the client at all. Client users then won't be able to see the deactivated types of entries by default and therefore also won't be able to select them when working with Password Depot.

Return to the [Password Depot homepage](#) (leave this help)

Add Users by Department

This dialog box allows you to add users to a group by department.

Return to the [Password Depot homepage](#) (leave this help)

Log Filter Entries

You can filter the log display to get the information you need more quickly.

To do this, click **Advanced filter** in the **Log** toolbar.

If you activate filtering, you will have numerous options for reducing the display of log entries to the desired ones.

Return to the [Password Depot homepage](#) (leave this help)

Index

Access Rights

[Database Properties](#)

[Database Properties](#)

[Databases](#)

[Databases](#)

[Groups](#)

Account options

[Add Users](#)

Active Directory

[Active Directory Synchronization](#)

[Server Settings](#)

Active Directory Import

[Active Directory Synchronization](#)

Active Directory Synchronization

[Active Directory Synchronization](#)

Active Directory Tree

[Active Directory Synchronization](#)

Add database to server

[Add database to server](#)

Add existing database

[Add database to server](#)

Add User

[Add Users](#)

Adding new user

[Add Users](#)

[Add Users](#)

[Users](#)

[Users](#)

Admin

[Installation and running](#)

Android app

[Migration](#)

Assign Database

[Assign Database](#)

[Assign Database](#)

Assign Database dialog

[Assign Database](#)

Backup

[Server Settings](#)

Client Security Policies

[Client Security Policies](#)

[Client Security Policies](#)

Control Panel

[Manage](#)

[Server Manager](#)
Corporate Clients
[Client Security Policies](#)
Create new database
[Add database to server](#)
Create private database
[Assign Database](#)
[Assign Database](#)
Add existing
[Add database to server](#)
[Add database to server](#)
assign
[Assign Database](#)
Create new
[Add database to server](#)
[Add database to server](#)
[Assign Database](#)
create private
[Assign Database](#)
Create private
[Assign Database](#)
Permissions
[Database Properties](#)
Database assign
[Assign Database](#)
Database Properties
[Database Properties](#)
[Database Properties](#)
Databases
[Databases](#)
Report
[Reports](#)
Dictionary attacks
[Server Policies - Security](#)
Duplicate Groups
[Groups](#)
Duplicate user
[Users](#)
Email Settings
[Server Settings](#)
Permissions
[Database Properties](#)
Events
[New Notification](#)
Export log
[Log](#)
Groups

[Groups](#)
[Groups](#)
[New Group](#)
[New Group](#)
[Add](#)
[New Group](#)
[Inactive Sessions](#)
[Server Settings](#)
[Install a license](#)
[Server License](#)
[Server License](#)
[Installation](#)
[Installation and running](#)
[Installation and running](#)
[Introduction](#)
[Introduction](#)
[Introduction](#)
[IP restriction](#)
[Add Users](#)
[Localhost](#)
[Installation and running](#)
[Installation and running](#)
[Log view](#)
[Log](#)
[Log](#)
[Logging](#)
[Server Settings](#)
[Logins](#)
[Server Settings](#)
[Manage](#)
[Manage](#)
[Master Password Policy](#)
[Client Security Policies](#)
[Member of](#)
[Add Users](#)
[Menu Manage](#)
[Manage](#)
[Migration](#)
[Migration](#)
[New Group](#)
[New Group](#)
[New Notification](#)
[New Notification](#)
[New Notification](#)
[New User](#)
[Add Users](#)
[Add Users](#)

[Users](#)

[Users](#)

[new](#)

[New Notification](#)

[Notification properties](#)

[Notification Properties](#)

[Notifications](#)

[Notifications](#)

[NT Service](#)

[Installation and running](#)

[Installation and running](#)

[Open log](#)

[Log](#)

[Password Depot Server](#)

[Introduction](#)

[Password Files](#)

[Databases](#)

[Permissions](#)

[Assign Database](#)

[Database Properties](#)

[Permissions for users](#)

[Permissions for users](#)

[Server Policies](#)

[Server Policies - Permissions](#)

[Server Policies - Permissions](#)

[on database](#)

[Database Properties](#)

[on entries and folders](#)

[Database Properties](#)

[Permissions on entries and folders](#)

[Database Properties](#)

[Permissions on the database](#)

[Database Properties](#)

[Program Options](#)

[Program Options](#)

[Program Options](#)

[Properties dialog](#)

[User Properties](#)

[User Properties](#)

[Properties Notification](#)

[Notification Properties](#)

[Proxy](#)

[Program Options](#)

[R/O](#)

[Databases](#)

[Databases](#)

[R/W](#)

[Databases](#)

[Databases](#)

Databases

[Reports](#)

Users

[Reports](#)

Reports

[Reports](#)

Rights administration in Password Depot Enterprise Server

[Server Policies](#)

Client

[Client Security Policies](#)

Server License

[Server License](#)

[Server License](#)

Server Manager

[Installation and running](#)

[Server Manager](#)

Server Options

[Server Settings](#)

Server Policies

[Server Policies](#)

[Server Policies](#)

[Server Policies - Security](#)

[Server Policies - Security](#)

Server Port

[Server Settings](#)

Server Settings

[Server Settings](#)

[Server Settings](#)

Single-Sign On

[Server Settings](#)

Storage folder

[Server Settings](#)

Storage Folder

[Server Settings](#)

[Server Settings](#)

Supported authentications

[Server Settings](#)

[Server Settings](#)

Active Directory

[Active Directory Synchronization](#)

SYSTEM

[Installation and running](#)

Unlock

[Server License](#)

[Server License](#)

Duplicate

[Users](#)

User properties

[User Properties](#)

[User Properties](#)

Users

[Add Users](#)

[Add Users](#)

Groups

Users

[Users](#)

Users Report

[Reports](#)

Windows application

[Installation and running](#)

[Installation and running](#)

Windows Authentication

[Server Settings](#)

Glossary