

User Manual



Password Vault Manager

Version 8.0

Your all-in-one solution platform for password management
for your entire organization.

Table of Contents

Foreword	0
Part I Getting Started	9
1 What is Password Vault Manager?	10
2 System Requirements	10
3 Creating a New Entry	10
4 Configuring an Entry	12
5 Viewing an Entry	14
6 Opening a Url	15
7 Group/Folder Management	16
Part II Installation	20
1 Client	21
Configuration File Location	21
Portable (USB)	22
Custom Installer Service	23
Create an Installation Package	23
Download Package From Web	29
Installer File Generation	29
Option Selection Dialog	31
Registration	34
Register Enterprise Edition	34
Register Free Edition	34
2 Database Upgrade	37
3 Uninstall	38
Part III Commands	39
1 File	40
Lock Application	41
My Data Source Information	42
Cloud Account	46
Refresh	48
Manage Password	48
Backup	50
Settings	50
Restore	53
Data Sources	54
Import	56
Import Login Wizard	58
Export	59
Encrypted Html	62
Options	64
General	64
Application Start	65
Application Close	67

Notification	68
Proxy	68
User Interface.....	70
Dashboard	71
Filter	72
Keyboard	73
Navigation Pane	76
Title Bar	77
Trayicon/Taskbar.....	78
Tree View	80
Custom Variables.....	81
Reports	82
Browser Extensions.....	83
Key Agent.....	83
Security	84
Cloud	87
Advanced.....	88
Import Options.....	89
Export Options.....	92
Search Property.....	95
My Account Settings	96
My Personal Credentials.....	97
Templates	98
2 Home.....	102
Information	102
Macros	103
Clipboard	103
View	106
Details	107
Information.....	107
Attachments.....	113
Logs	113
Password History.....	114
Entry History.....	116
Tools	119
Favorites.....	120
3 Edit.....	123
Add	123
Shortcut/Linked Entries.....	124
Edit	127
Setting Overrides	127
User Specific Settings.....	128
Credential Entry Overriding.....	131
Credentials	132
Local Specific Settings.....	133
Batch Edit	135
Batch Actions.....	140
Export	142
4 View.....	142
Panels	143
All Entries.....	143
Private Vault.....	149
Favorite Entries.....	150

Most Recently Used Entries.....	151
View	152
Advanced Search.....	153
View Credential Entries.....	155
Search/Filter.....	156
Notification.....	160
Logs	161
Usage Logs (Local).....	161
Usage Logs (Global).....	162
Layout	165
Footer	165
5 Administration.....	166
Settings	166
Data Source Settings.....	166
General	168
Password Policy.....	172
Password Complexity.....	174
Forbidden Password.....	176
Allow password for external system.....	177
Version Management.....	179
Serial	181
System Message.....	182
Types	182
Paths	183
Custom Variables.....	184
Security Providers.....	185
Management	189
Users	190
Integrated Security.....	197
Permissions	199
Security Groups.....	200
Roles	203
Other	209
View Deleted.....	210
Reports	211
General	212
Duplicate Entries.....	213
Entry List	215
Entry Information.....	216
Entry Status	217
Expired	218
Expiration Schedule.....	219
Expired Entry List.....	220
Expired Passports.....	220
Expired Softwares.....	221
Expired Warranties.....	221
Security	222
Password Analyzer.....	222
Password Complexity.....	223
Password Usage.....	224
Security Group.....	224
Export Report	225
Change Current User Password.....	228
Clean up	228

Deleted History.....	229
Entries History.....	232
Logs	233
6 Refactoring.....	234
Extract	235
Convert To	236
Sub Connection	237
7 Tools.....	238
Extensions Manager	238
Translation Manager	239
Password Generator	241
Certificate Generator	247
Password Analyzer	249
Key Agent Manager	250
8 Window.....	254
Reset Layout	255
9 Help.....	256
Help	257
Support	258
View Application Log.....	259
Diagnostic.....	262
Profiler	264
Follow Us	268
About	268
10 Tray Icon.....	269

Part IV Data Sources 271

1 Data Sources Types.....	274
Choosing the data source type	278
Amazon S3	279
Dropbox	281
FTP	284
Microsoft Access	288
Online Drive	291
SFTP	294
SQLite	298
Web	303
XML	304
Advanced Data Sources	307
Devolutions Server.....	308
MariaDB	311
MySQL	314
Devolutions Online Database.....	317
Activate Subscription (Register).....	320
Activate Online Data Source Trial.....	320
SQL Azure.....	320
SQL Server.....	324
2 2-Factor Authentication.....	328
Google Authenticator	331
Yubikey	334
Duo	335

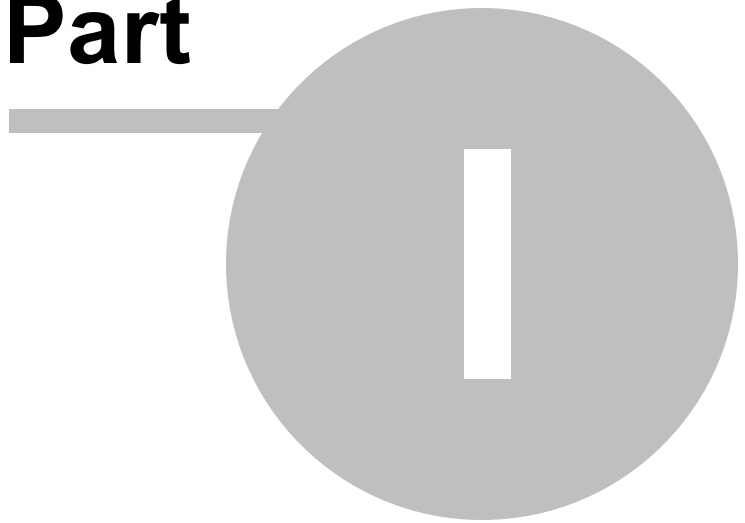
AuthAnvil	340
3 Offline Mode.....	341
Offline Read/Write	343
4 Caching.....	344
5 Lock Data Source.....	346
6 Import/Export Data Source.....	347
Part V Entry Types	348
1 Settings.....	350
General	351
Display Mode.....	352
Security	355
More	356
Description.....	357
Typing macro.....	361
Keywords/Tags.....	365
Security	367
Information	368
General	369
Hardware.....	371
Contact	372
Purchase.....	373
Notes	374
Custom Fields.....	375
Statistics	376
Attachments	376
Events	377
Auto Typing Macro.....	381
Logs	384
View Logs.....	386
Log Details.....	387
Advanced	391
2 Information.....	393
Alarm Codes	394
Bank Information	395
Credit Card	396
Email Account	398
Login (Account)	401
Login (Web)	402
Note/Secure Note	404
Other (Custom)	405
Passport	407
Safety Deposit	408
Software / Serials	408
Wallet	410
Auto Fill	411
Chrome Extension.....	412
Firefox Extension.....	416
IE Extension.....	421
3 Contact.....	422
4 Documents.....	424

Certificate	425
Default	426
Image	427
Microsoft Office (Word, Excel, PowerPoint, Visio and OneNote)	428
PDF	429
Phonebook	430
Rich Text Editor	431
Spreadsheet Editor	433
Text	435
Video	437
5 Groups.....	438
Company	441
Customer	442
Database	443
Device (router, switch, firewall)	444
Domain	445
Group/Folder	446
Identity	447
Printer	448
Server	448
Site	449
Software	450
Workstation	451
6 Credentials.....	452
Connection String	454
Private Key	454
Username/Password	456
Windows Credential Manager	457
7 Variables.....	459
8 Macro/Script/Tools.....	469
AuthoHotKey	471
Autolt	472
Jitbit Macro Recorder	474
Typing Macro	476
Part VI Support/Resources	477
1 Keyboard Shortcuts.....	478
2 Command Line Arguments.....	480
3 Lexicon.....	481
4 Technical Support.....	482
5 Follow Us.....	482
6 Troubleshooting.....	483
Clipboard	483
2-Factor Authentication	484
Data Sources	484
Performance	487
Diagnostic.....	487
Refresh	491
Startup	492
Unable to uninstall	493

General	493
SQL Server	494
Welcome Page	494
7 Knowledge Base.....	495
Internet outbound access	495
Free Edition to Enterprise	496
8 Best Practices.....	496
Backups	497
Credential Management for Teams	498
9 Tutorials.....	499
Overview	500
Getting Started	500
Spotlight On...	500
10 Tips and Tricks.....	501
Create a list of Credentials	501
Data Migration	504
Index	0

Getting Started

Part



1 Getting Started

1.1 What is Password Vault Manager?

Description



Password Vault Manager for Mac is a product used to manage all of your passwords and sensitive information.

Keep your credit card numbers, bank accounts, serial numbers or your alarm codes in an organized and secure database. Reveal with your team members what they need to know, and keep your data safe.

The following types can be stored on Password Vault Manager for Mac:

- Web Sites
- Credentials
- Banking information
- Credit card information
- Email accounts
- Alarm codes
- Note/Secure Note

1.2 System Requirements

Minimum Requirements

- Windows 8, 8.1 and 10
- Windows Server 2012 and 2012 R2
- Microsoft .Net Framework 4.0
- 800Mhz processor
- 512MB RAM
- 1024 x 768 screen resolution
- 200+ MB hard drive space

Terminal Services and Thin Client Support

Password Vault Manager can be installed on a Terminal Server machine, as well as a thin client and Windows XP Embedded.

1.3 Creating a New Entry

Overview

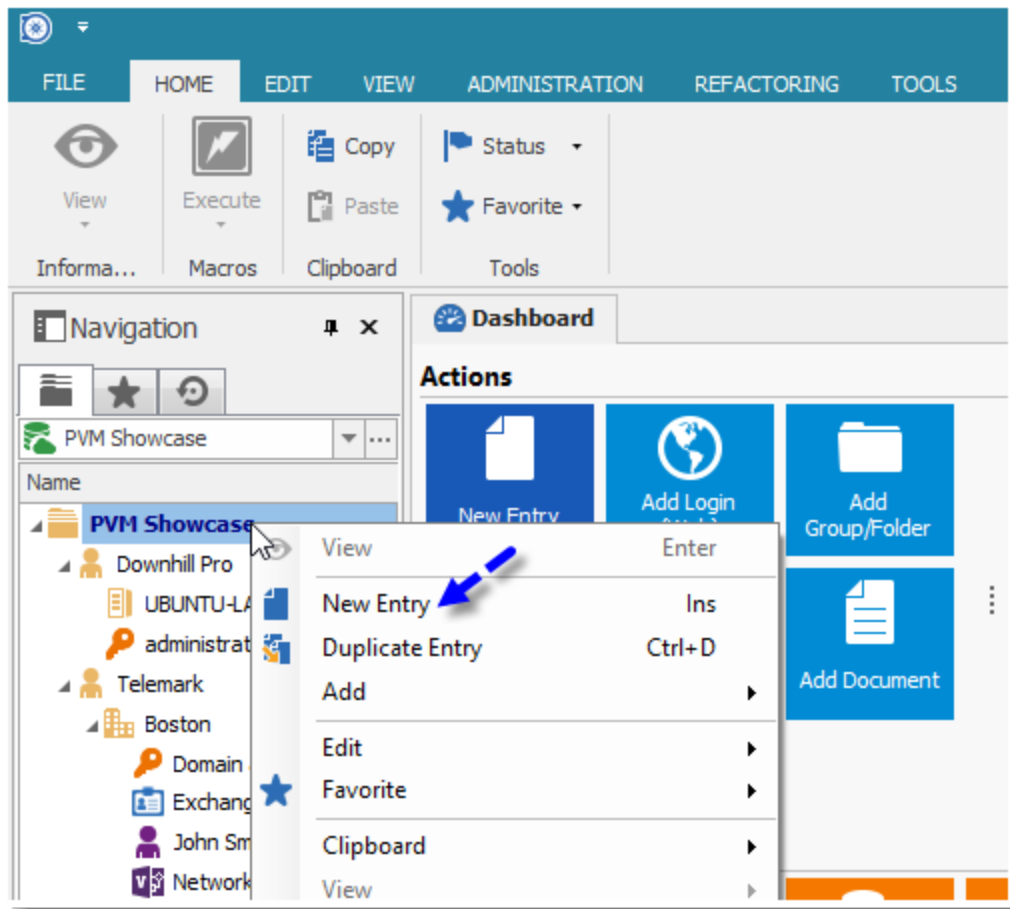
The first step in using Password Vault Manager is to configure an entry. There are several entry types. One should be familiar of which entry type(s) you intend to configure. Password Vault Manager supports the following entry types:

- [Information](#)
- [Contact](#)

- [Documents](#)
- [Groups](#)
- [Credentials](#)

Creating an Entry from the Context Menu

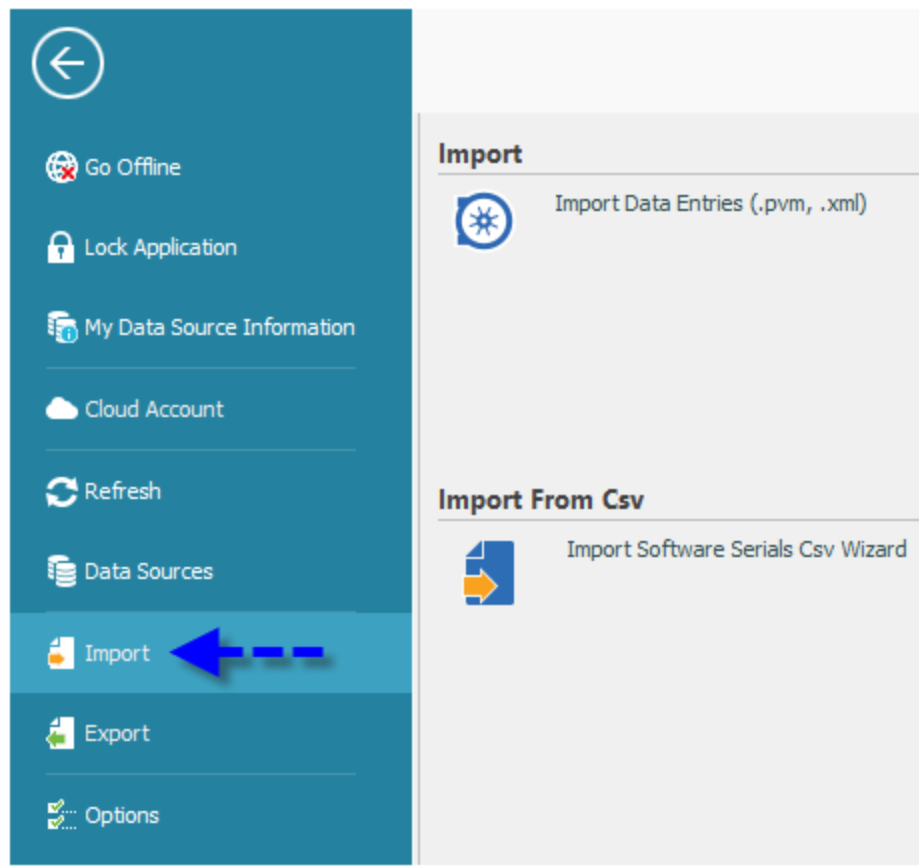
The simplest way to create a new entry is by using the **New Entry** key or from the Context Menu. Right-click on your folder and select **New Entry** from the menu in the main application window. The new entry window will prompt you to select the entry type you wish to create. Fill out the entry property to customize your settings.



Adding a New Entry

Creating an Entry by Importing its Configuration

An entry can be imported by selecting **File - Import**, or by importing its configuration directly from any compatible applications supported by our importing tools. To learn more about importing, refer to the [Import](#) topic.



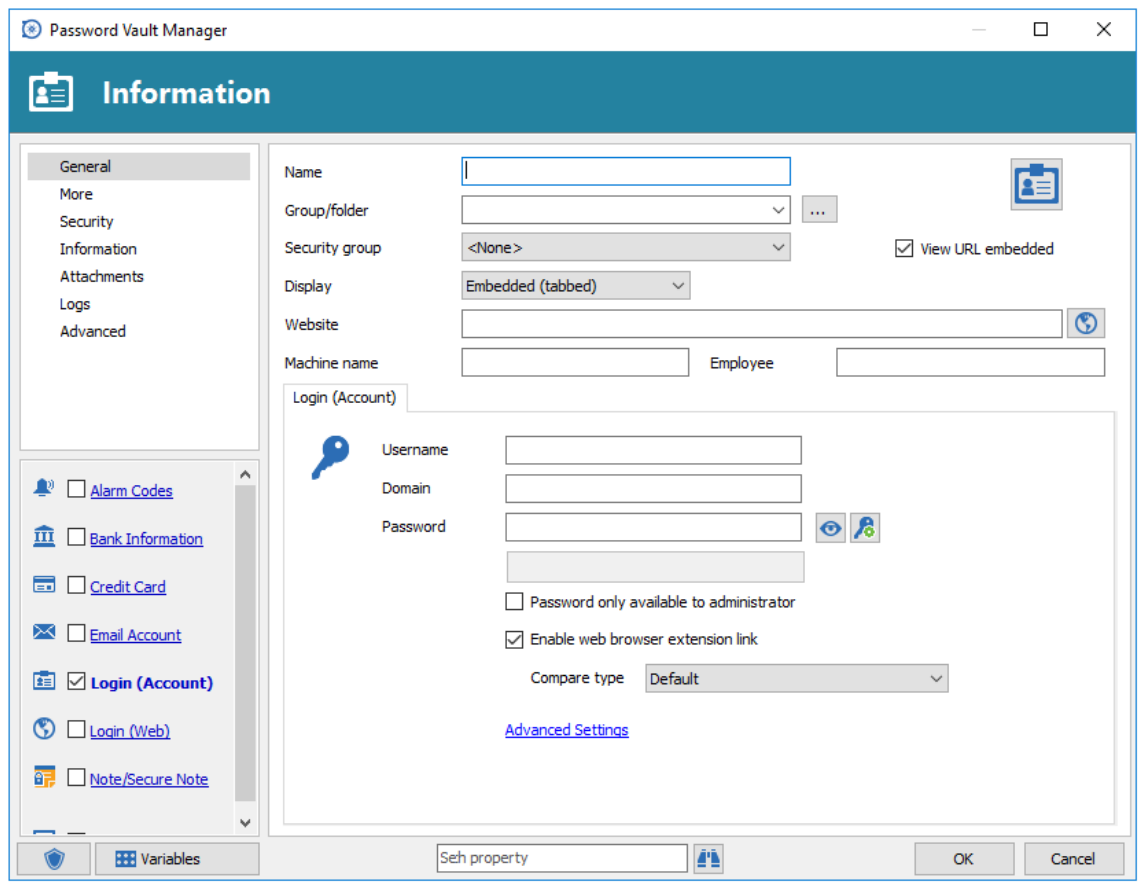
Import Entries

1.4 Configuring an Entry

Description

Each entry type contains its own unique settings. However, there are a few exceptions where common settings are shared.

Settings



Entry edition dialog

Description	
Name	The name of the entry displayed in the entry list.
Group/Folder	Useful to organize your session in different folders, either in the tray icon context menu or in the tree view. Learn more here .
Security Group	In the Enterprise edition, allows the Administrator to assign a security group to an entry, and therefore limit a subset of users in viewing this entry. See User Management for more information.
View URL embedded	View the the entry Url web page. The Url will be used to navigate directly to the web site.
Display	External: External mode sessions are opened as an external process. Embedded/Tabbed mode: Runs within the parameters of the Password Vault Manager window, and displays the tabs at the top of the window. Undocked: Launches a new window containing tabbed session. An Undocked browser allows the user to move beyond the confinements of the Password Vault Manager.
Open in modal window	When the display mode is in External mode you have the option of opening the browser in a modal window.
Primary monitor	If you have selected the Undocked or External mode in the display option you will be able to choose on which monitor to open your window:

	<p>Primary monitor: This is the monitor that is marked as "main display" in Window.</p> <p>Secondary monitor: The other non-primary monitor, obsolete, use Monitor #1, 2, 3, 4 instead.</p> <p>Current monitor: The monitor that Password Vault Manager is running in.</p> <p>Configured: See Systems Options.</p> <p>Default: Will not move the application, it will be Windows default mode.</p> <p>Monitor #1: Monitor #1 is primary.</p> <p>Monitor #2: Monitor #2 is primary.</p> <p>Monitor #3: Monitor #3 is primary.</p> <p>Monitor #4: Monitor #4 is primary.</p>
Website	Enter the Url web page for this entry. The Url will be used to navigate to the web site.
Machine name	Enter the machine name. Used to store the host name vs the DNS name.
Employee	Enter the employee name.

As well as the fields described above, additional tab pages contain many data fields and options for your sessions that are common to multiple entry.

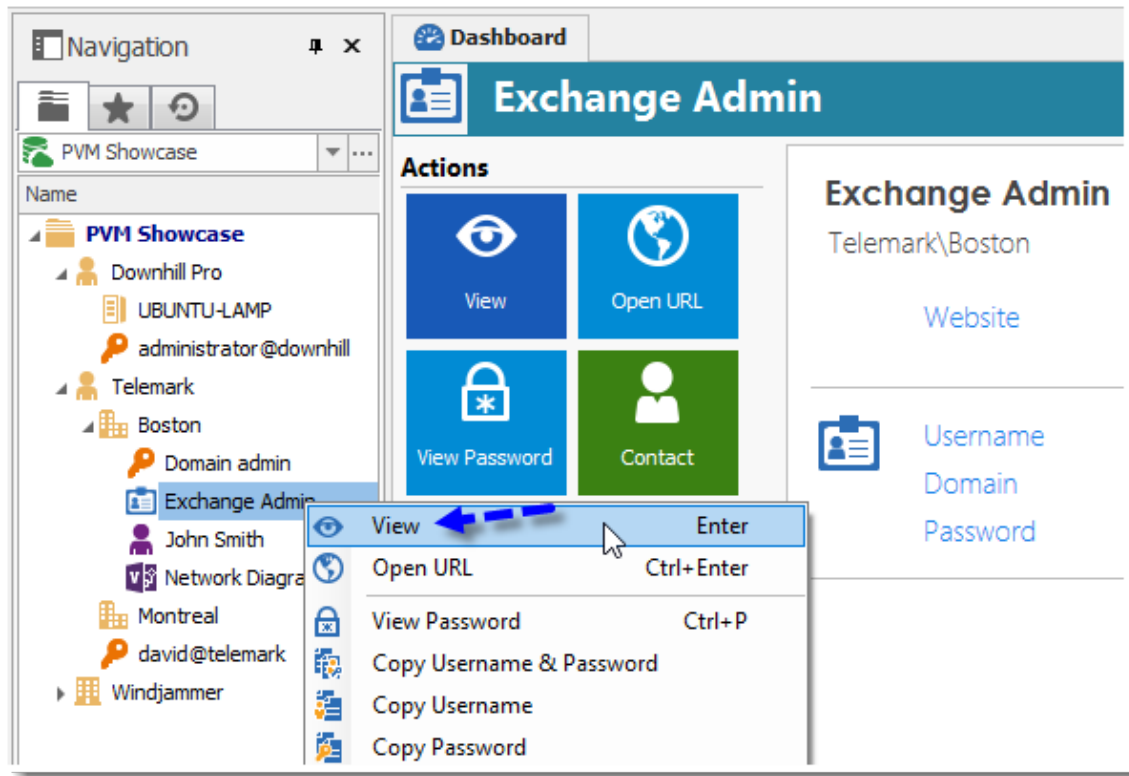
Description	
More	Contains the following sections: Description , Other and Keywords/Tags . The entry description can be in plain text, in rich text format, or a website link.
Security	The security tab is used to determine whether passwords must meet predetermined complexity requirements that has been configured. Password Complexity requirements are enforced when passwords are changed or a new entry is created.
Information	Contains different type of information related to the entry, such as the machine specifications, Computer , Contact , Custom Fields or some useful notes. Custom information can also be added.
Attachments	Manages the entry's attachments. Used to add, edit and delete the linked files. Please see Attachments Overview
Logs	Contains the session logs and other related options. For example, entering a comment when opening a session can be made mandatory. Please see Log Options
Advanced	Contains advanced settings related to the entry, such as the internal data source ID and session ID. These values can be used to invoke Password Vault Manager from a command line to open the entry, or to run a batch modification.

1.5 Viewing an Entry

Description

An entry can be accessed by double clicking the data entries list or by using the context menu.

If the **View embedded** option is selected, the view will open in the embedded mode within Password Vault Manager.

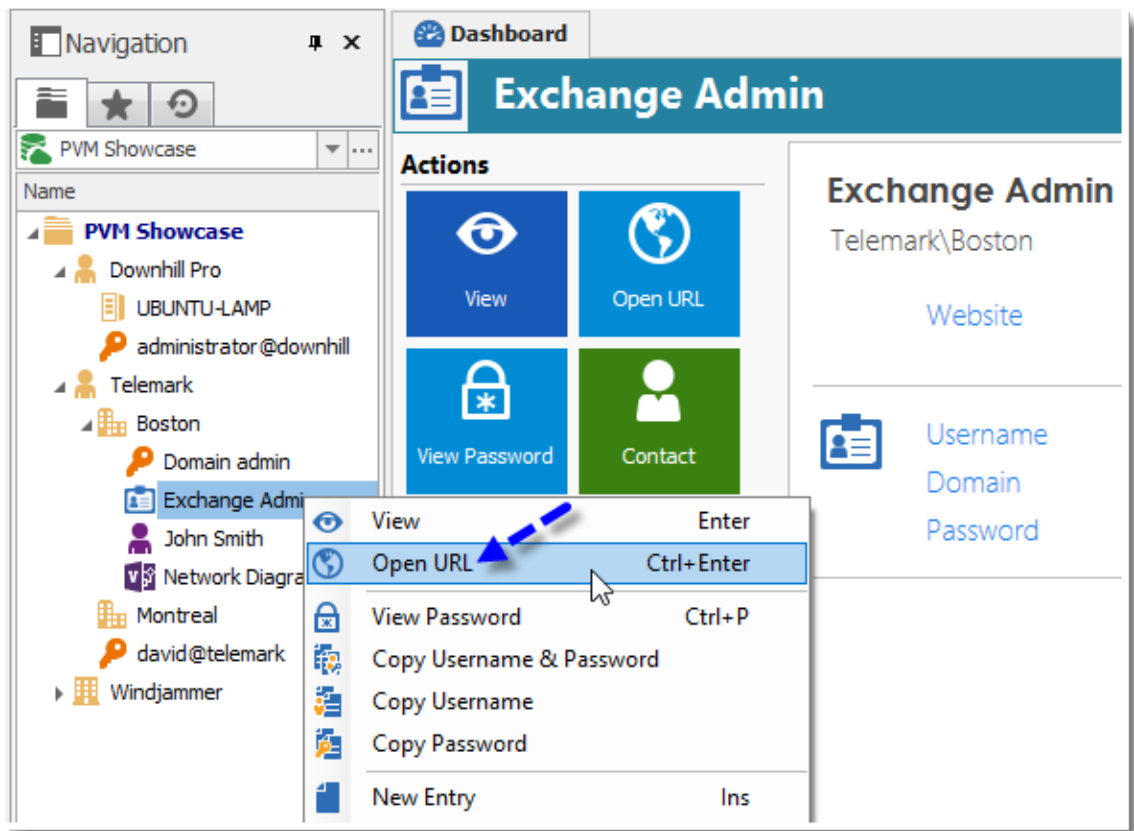


View existing entry

1.6 Opening a Url

Description

A Web Site can be opened by accessing the context menu **Open Url**, or by selecting **Ctrl+Enter** while the item is selected.



Open URL

Auto Fill

An Auto fill of username and password is supported on most web sites and in browsers. Plugins/Add-Ons/Extensions need to be installed in order to support this feature.

To learn more, please visit [Auto Fill](#).

1.7 Group/Folder Management

Description

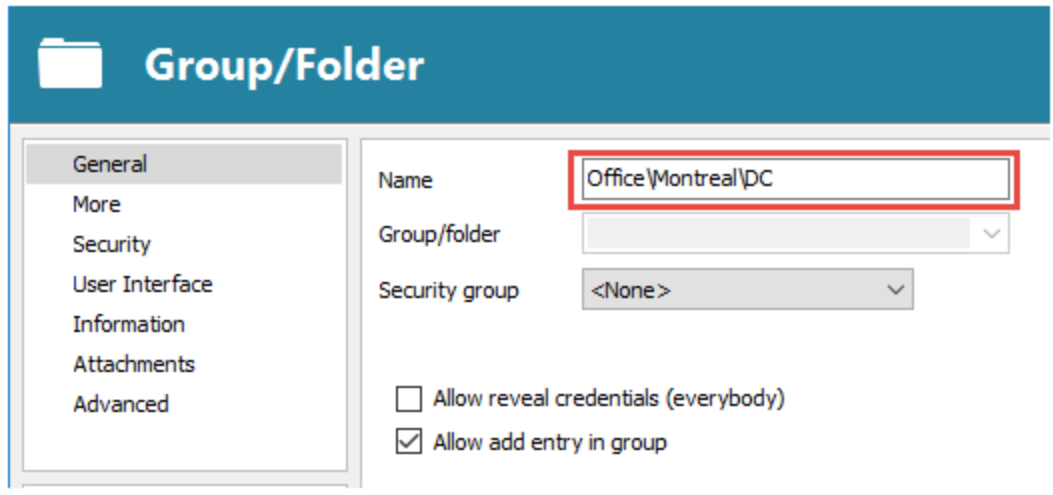
Groups or folders are used to logically organize your data entries. Password Vault Manager can create groups and sub groups that will automatically be sorted alphabetically.

Groups are created in two different ways:

- Via the entry properties
- From the entry tree view

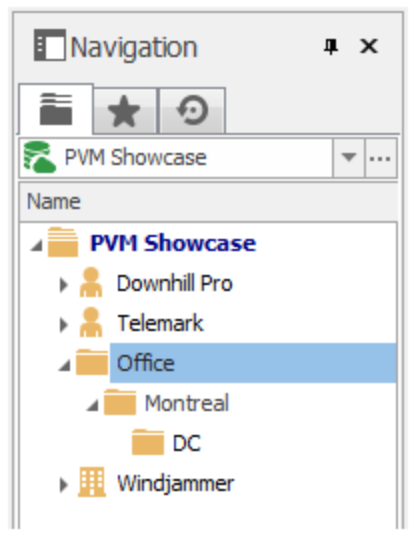
Creating Groups via the Data Entry Properties

Groups can be specified in the session properties. Simply fill in the field with the desired group name and Password Vault Manager will generate the corresponding tree structure. Use the backslash (\) to create a sub group.



The screenshot shows the 'Group/Folder' configuration window. The 'Name' field is highlighted with a red border and contains the text 'Office\Montreal\DC'. Below it, the 'Group/folder' dropdown is empty, and the 'Security group' dropdown is set to '<None>'. At the bottom, there are two checkboxes: 'Allow reveal credentials (everybody)' which is unchecked, and 'Allow add entry in group' which is checked.

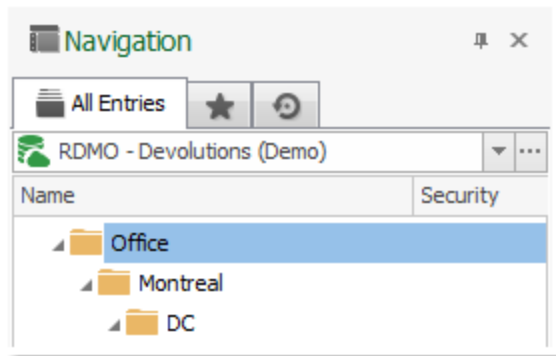
Creating Group/Folder



Basic group structure

For example, "Office\Montreal\DC" will create three nodes in the tree:

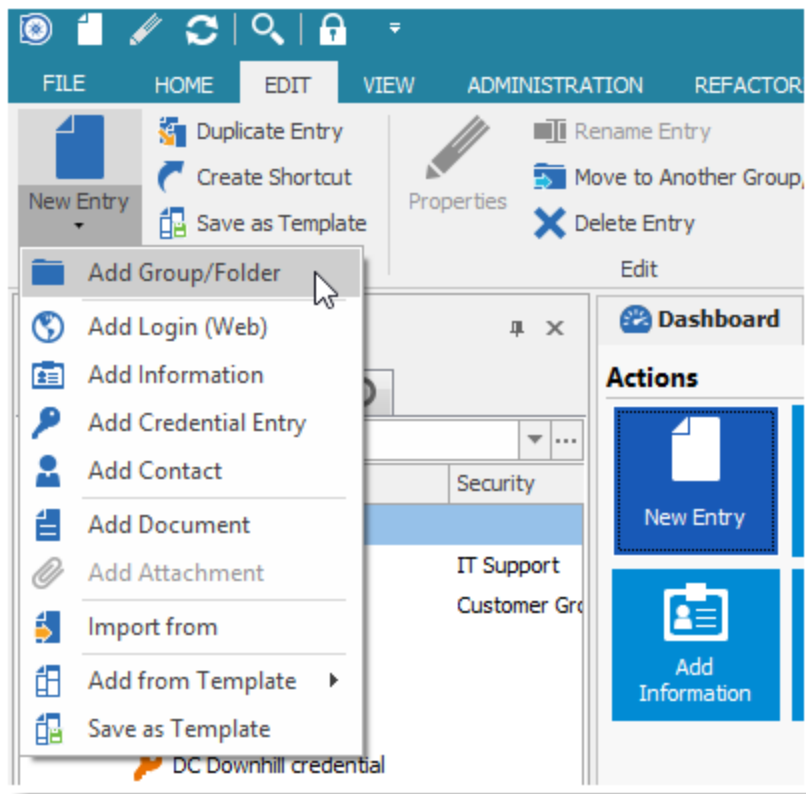
- Office
- Montreal
- DC



Modified group structure with a new node

Creating Groups

In the menu **Edit - New Entry**, select **Group/Folder** from the drop down menu.



Add Group/Folder

The **Add Group** dialog box will then prompt you to enter the name of the group and apply a Security Group on it.

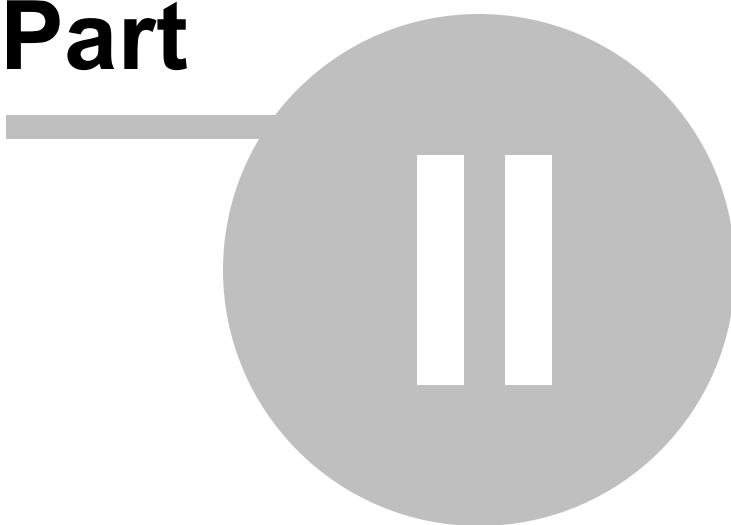
The screenshot shows a 'Group/Folder' configuration window. On the left is a sidebar with a tree view containing nodes: Company, Customer, Database, Device (router, switch, firewall), Domain, and Group/Folder (which is selected). The main area is divided into 'General' and 'Details' tabs. The 'General' tab contains fields for Name, Group/folder, and Security group, along with checkboxes for 'Allow reveal credentials (everybody)' and 'Allow add entry in group'. The 'Details' tab contains fields for Username, Domain, and Password, with a 'Show/Hide' icon next to the password field.

Group edition dialog

Once a group is created, you can add a data entry by using the menu, or by dragging its node directly to the content of the group.

Installation

Part



2 Installation

2.1 Client

Description

Password Vault Manager can either be downloaded as setup files, or as a compressed (zip) file containing the binaries.

Installation

Depending on the downloaded media, either run the setup, or extract the files from the archive in any folder and launch the executable.

Licence

You have a 30 day trial of the Enterprise edition. If you possess a purchased license of the Enterprise Edition, please follow the instructions at [Register Enterprise Edition](#).

Data Source

By default, a local data source has been created beforehand using the SQLite format. You may add as many data sources as needed. Please refer to [Data Sources](#) for more information.

Terminal Services

Password Vault Manager can also be installed on a Terminal Server, but to prevent loss of user settings, we recommend that you install the application in any folder except "**Program Files**" or "**Program Files (x86)**". The configuration and the default data source are created in this folder instead of the "**Local Application Settings**" folder.

Please see [Configuration File Location](#) for more information.

2.1.1 Configuration File Location

Default Location

Password Vault Manager saves its configuration in a file named **RemoteDesktopManager.cfg**. This file contains all application settings and configured data sources. All of the data source settings are encrypted for security reasons.

If Password Vault Manager is installed in a sub folder of "**Program Files**" and is not running on a Terminal Server, the configuration is saved in "**%LocalAppData%\Devolutions\RemoteDesktopManager"**

If the application is running on a Terminal Server, the configuration will be saved in "**%AppData%\Devolutions\RemoteDesktopManager"** It uses the roaming profile to avoid multi-user conflicts.

In any other case, the configuration is saved in the installation folder. This allows you to install multiple versions of the application side-by-side, as long as you don't install it in a sub folder of "**Program**

Files" (For more information on why -- this is because of the **"Program Files"** virtualization introduced with Windows Vista: <http://support.microsoft.com/kb/927387>.)

Override the Default Path

There are two ways to change the default option path:

1. Create a file named **"Override.cfg"** in the application folder. Password Vault Manager opens this file and reads the first line. It should contain the desired installation folder (without the option filename). If you wish to use the current installation path, place a dot in the file. Here are two examples:

Example	
c:\pvm	The config file is saved in a specific folder.
.	The dot is used to specify the Password Vault Manager installation folder.
%AppData%\Devolutions \RemoteDesktopManager	Specify the application roaming data folder.



Having the configuration file in the installation folder allows you to run multiple versions of the application side-by-side.

2. By adding a key in the registry: **CurrentUser\SOFTWARE\RemoteDesktopManager, OptionPath**. Set the desired path in the key **OptionPath**. Do not forget to exclude the option file name in the key.

Default Configuration

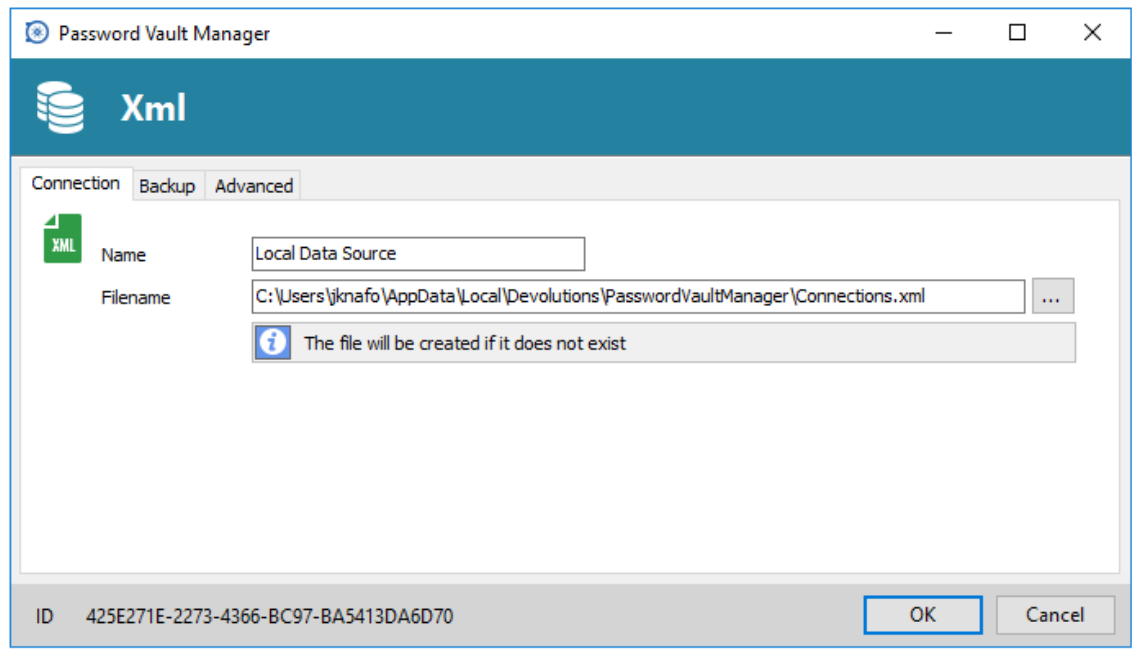
If Password Vault Manager can not locate the configuration file for a new user, it will automatically copy the file found in the application installation folder. This is useful in deploying the configuration in a Terminal Server environment. Moreover, the application will update the license key if a newer serial is found in the default configuration.

2.1.2 Portable (USB)

Description

Password Vault Manager can be used as a portable application. The following steps are required to ensure the process runs correctly:

1. Unzip Password Vault Manager on the portable device.
2. Open Password Vault Manager and configure the data source relative to the portable device: **.\Connections.xml**



Data Source saved on the portable device

2.1.3 Custom Installer Service

Description

The Custom Installer Service is offered through Devolutions Cloud Services. Please consult [Custom Installer Service](#) for an overview.

2.1.3.1 Create an Installation Package

Description



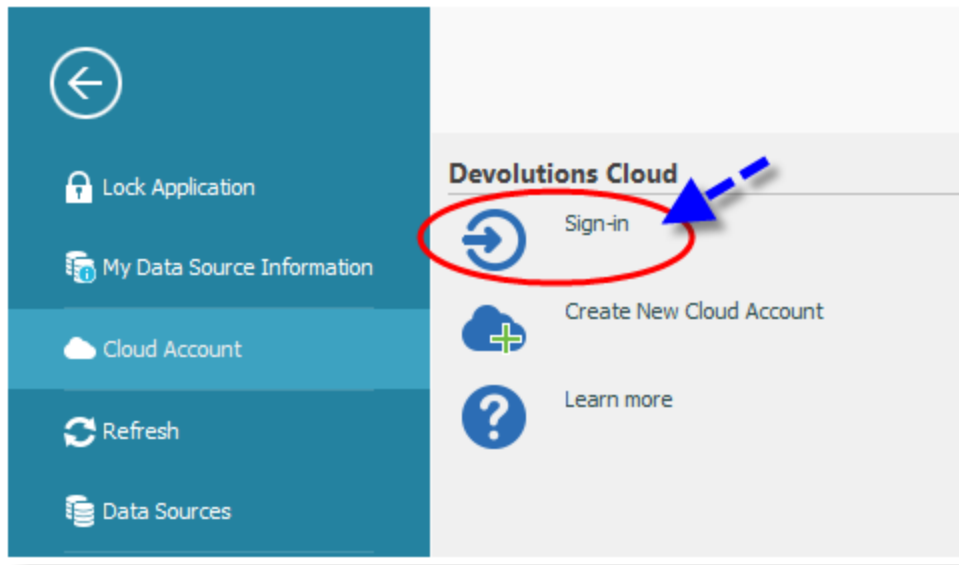
For stability reasons in large installation base, the latest official release isn't available for the Custom Installer Service until a period or varying length during which we ensure that no major issues are present. This will allow your organization the time to perform integration testing on a few workstations before upgrading your entire team.



Please ensure you have read and understood the content of the [Custom Installer Service](#) topic prior to subscribing to the service.

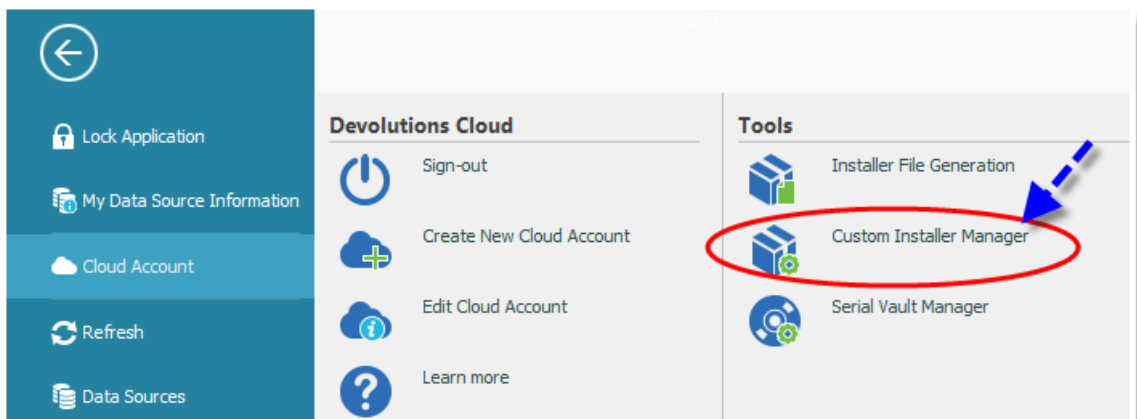
Settings

1. Click on **File - Cloud Account - Sign-in** to connect to your Devolutions Cloud account.



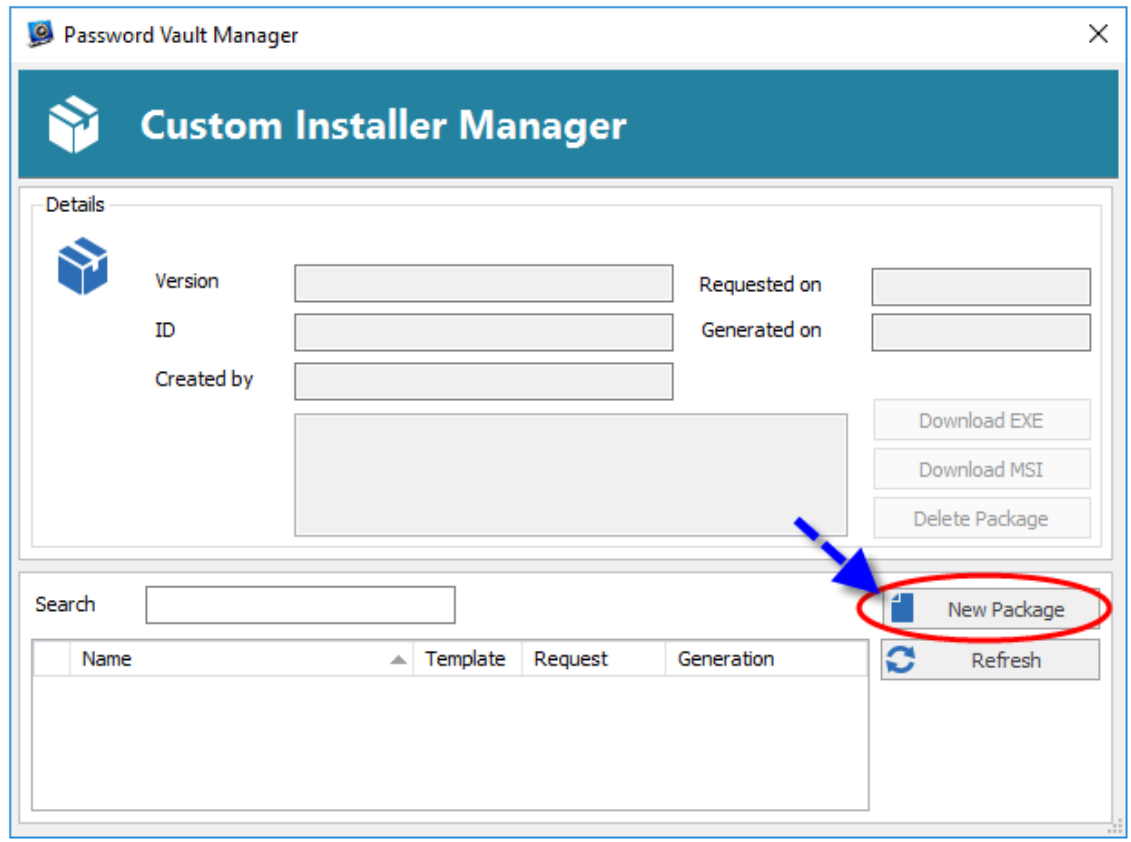
Sign-in Devolutions Cloud account

2. Click on **Custom Installer Manager** to create a new custom installer with specific settings.



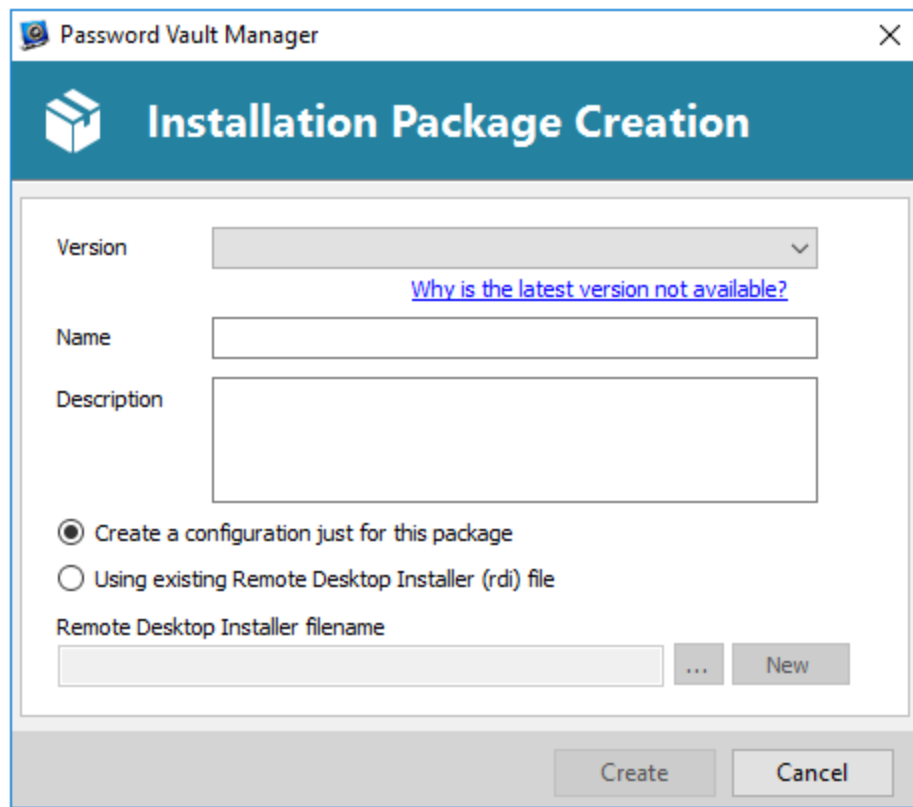
Custom Installer Manager

3. Click on **New Package**.



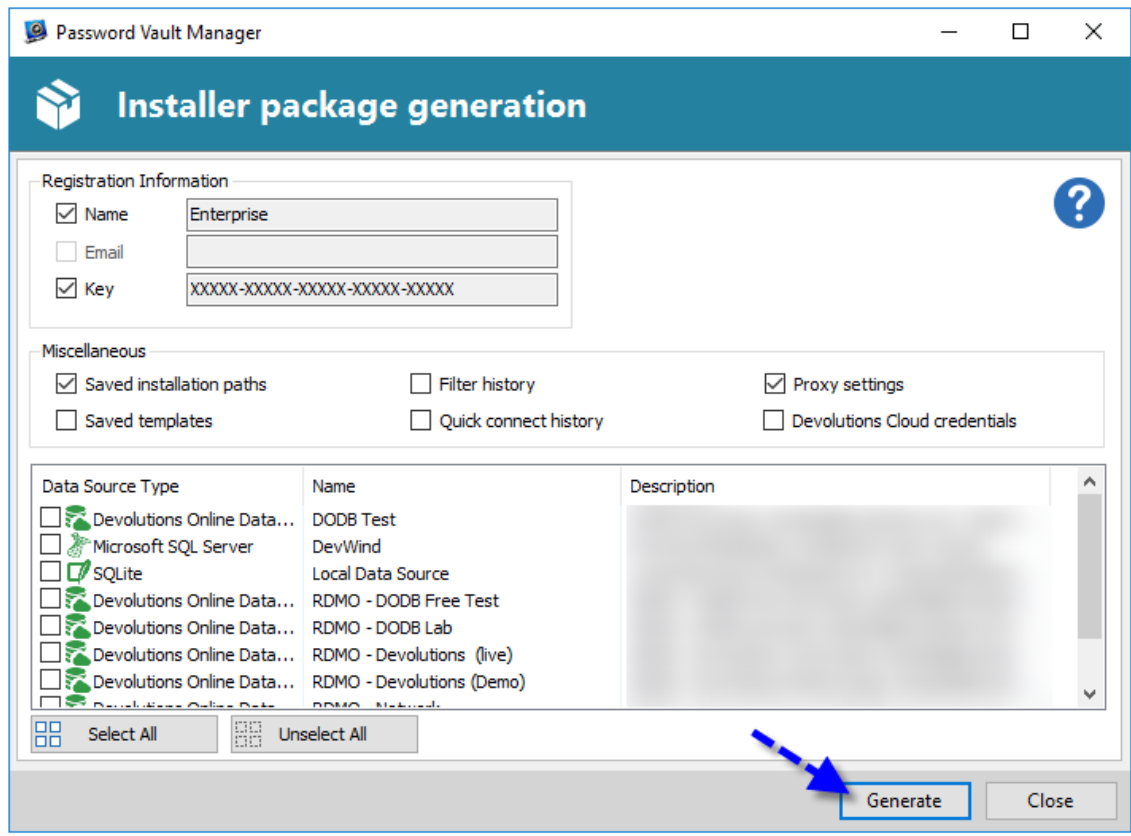
Custom Installer Manager - New Package

4. Select the application version and enter a name for your installation package. By default, the data source and option selection is performed while you go through the installation wizard. You have the option of choosing an existing Remote Desktop Installer (rdi) file as described in [Installer File Generation](#). The file selection controls will be enabled when selecting **Using existing Remote Desktop Installer (rdi) file**. Click on **Create** to create your Installation Package.



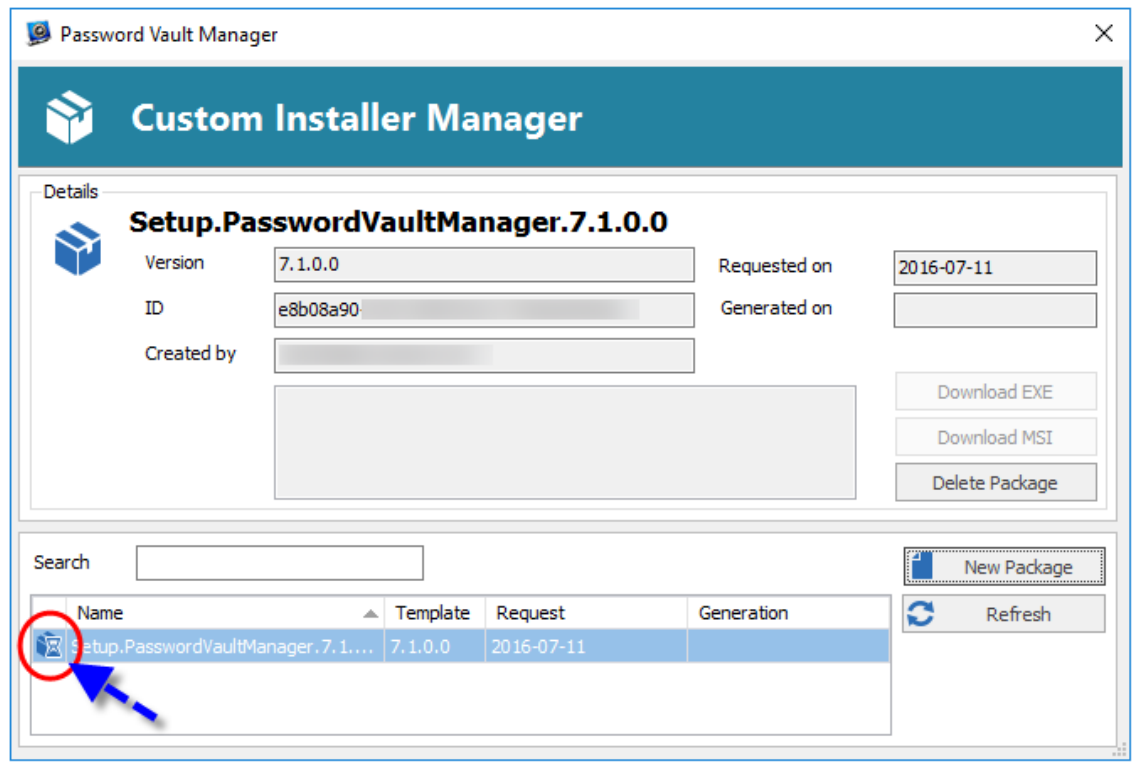
Installation Package Creation

5. When creating a new configuration, you can specify what to include in your custom installer. Click on **Generate** once your selection is made.



Installer Package Generation - Select your options

6. The request is submitted to our online services. Expect a brief waiting time while the request is being processed. You will receive a confirmation dialog once the package has been successfully submitted which is reflected by a display a clock icon indicating indicates that the package is being processed.



Custom Installer Manager

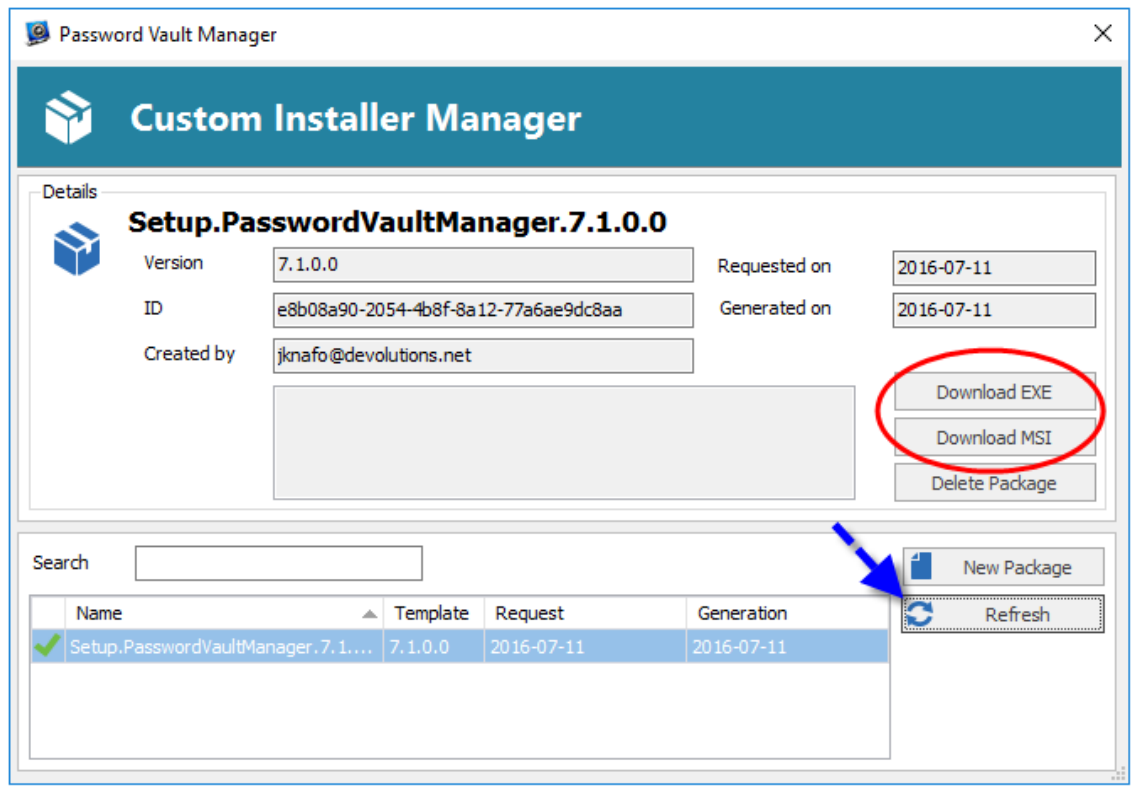
Downloading an Installation Package

Upon completion, you will receive a confirmation email. Click the **Refresh** button and the Custom Installer Manager form will display a green check mark indicating that the package has been successfully generated.

You can choose to download the installer as a Windows Installer (MSI file) or an Executable (EXE file). If you prefer to download the installation package from our web site, please refer to [Download Package From Web](#).



setup.exe is referred to as a **bootstrapper**. It ensures that the installer runs with the required privileges. Use the msi if certain that you are running all rights and process elevation.



Package downloaded

After you have downloaded your package, simply redistribute it for easy installation throughout your organization.

2.1.3.2 Download Package From Web

Description

Please consult topic [Download Package From Web](#) for more information on this service.

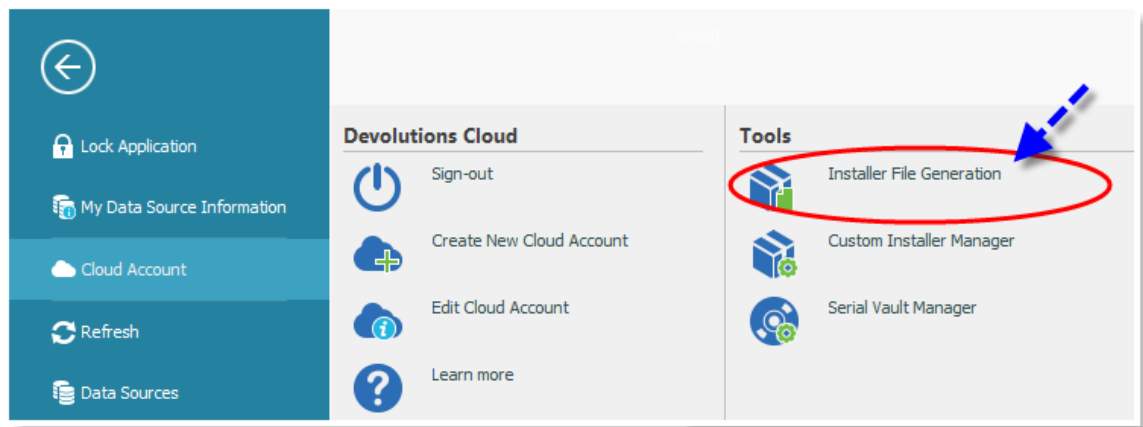
2.1.3.3 Installer File Generation

Description

When creating an installation package using the Custom Installer Manager, users must select which data sources to distribute. Instead of having to perform the same selections for all future updates, which can create a bevy of errors, you can simply perform the action once and reuse the appropriate file.

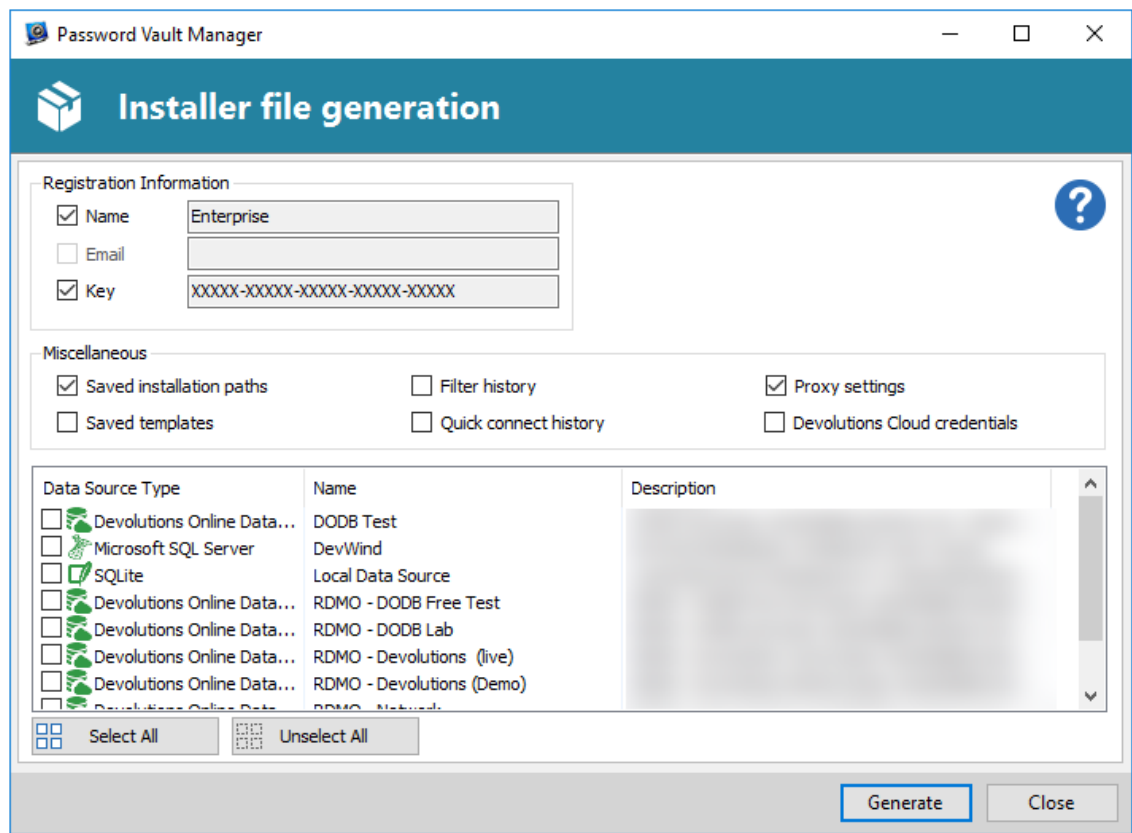
Settings

1. Click on **File - Cloud Account - Installer File Generation**.



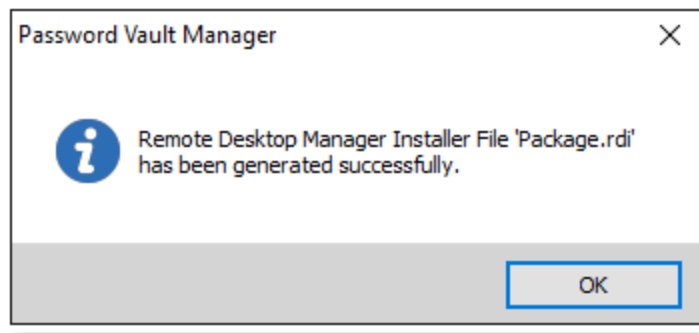
Installer File Generation

2. Select the data sources to be included. You can also include the name and serial key for the registration.



Installer file generation

3. Click on **Generate** to save your .rdi package.



Package.rdi

This file can be used in the Custom Installer Manager when creating an installation package.

Please consult the [Create an Installation Package](#) topic for more information on how to create a Custom Installer package.

2.1.3.4 Option Selection Dialog

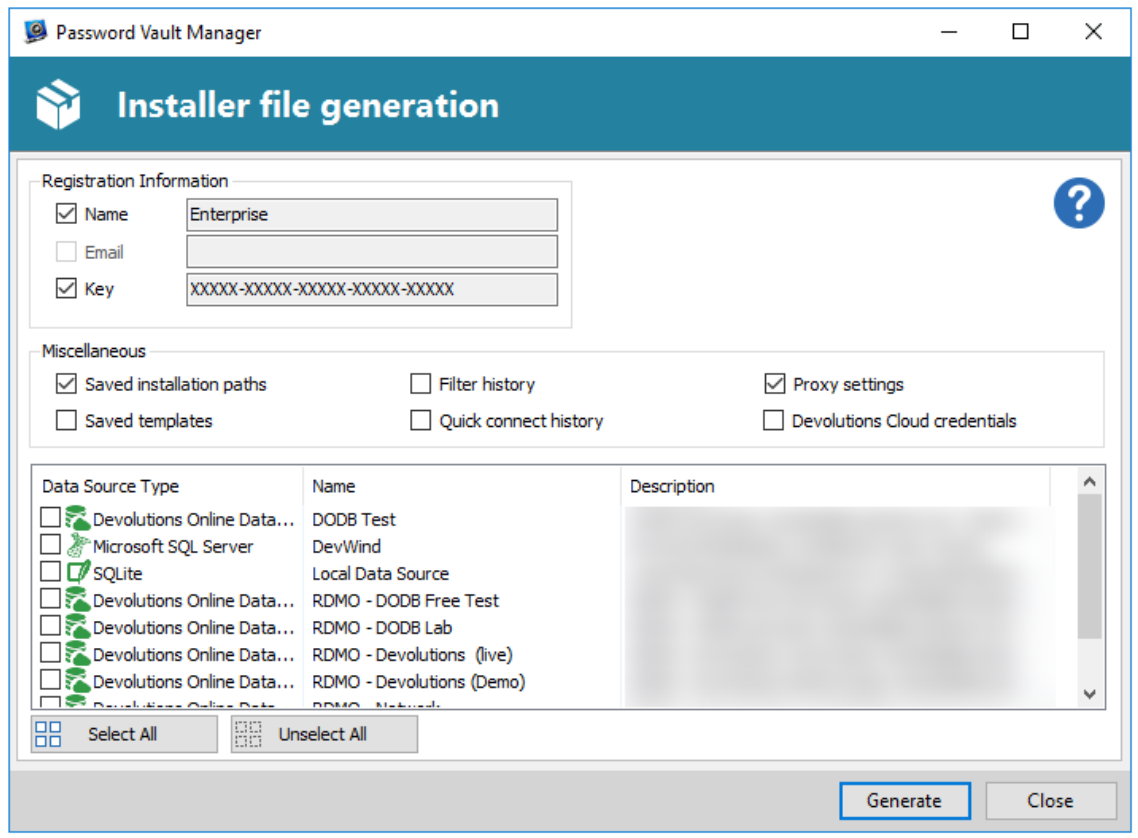
Description



The same dialog is used for the Custom Installer and for exporting Password Vault Manager options. Some options must NOT be used for the Custom Installer Service as it will mean sharing credentials. Please read the documentation carefully.

From the Password Vault Manager instance you are physically using, select the settings that will be bundled in the custom installer package. For security reasons, all settings that contain credentials have been unchecked by default.

Settings



Installer file generation

Registration information

Option	Description
Name	Enter the company registration name
Email	Enter the registration email if using a generic address
Key	License key

Miscellaneous



Do not redistribute the Devolutions Cloud credentials, doing so would result in **ALL** of your users to have access to the online account used to create the installer package.



Local templates will be included in bulk, if any template contains credential it may cause a security risk. Ensure you are sharing only what is required.

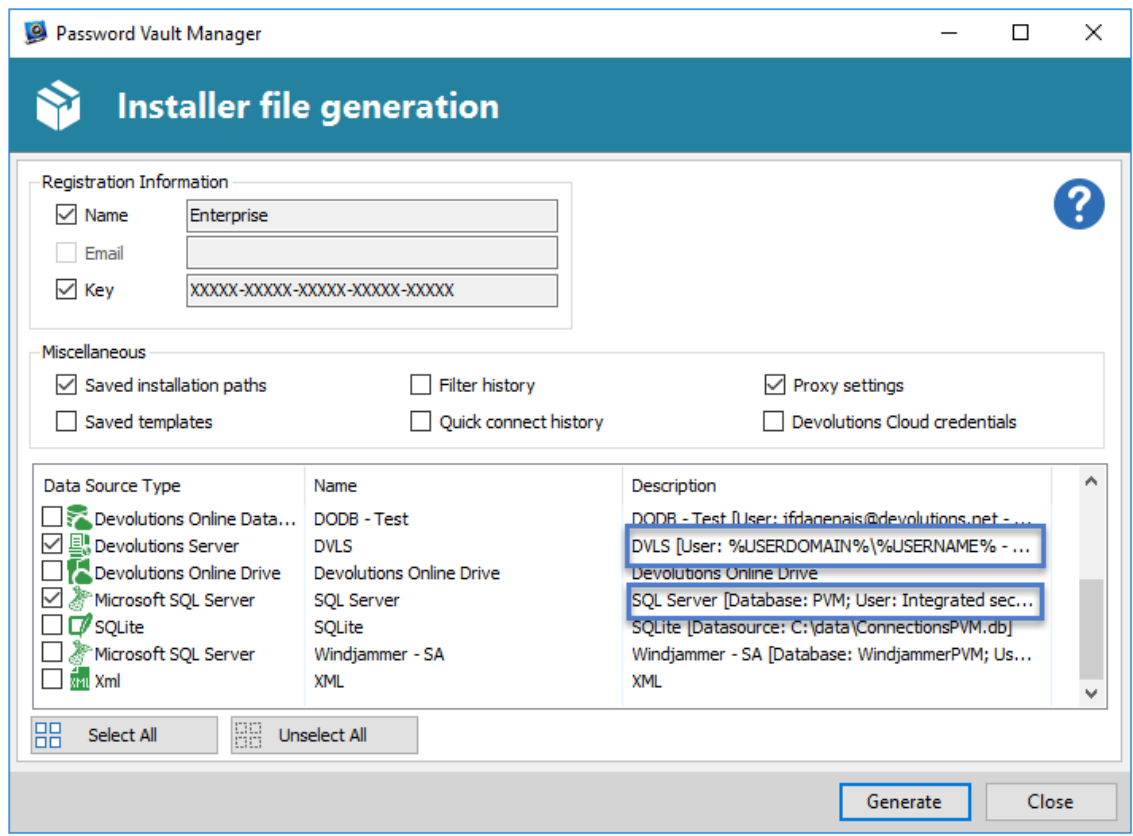
Option	Description
Saved installation paths	Preserve your installation paths configured for external third party applications. Use this only when all of machine's user has the same paths.

Saved templates	Include your local templates in the custom installer. Shared templates are stored in the data source and may be a better option in you need to share them.
Filter history	Preserve your search/filter history
Quick connect history	Preserve your Quick connect history
Proxy settings	Include your Internet proxy settings
Devolutions Cloud credential	Include your Devolutions Cloud credentials, please consult security warning above.

Data sources



The data sources you decide to redistribute should **NOT** contain identifiable credentials. Use of integrated security is highly recommended. You can also use environment variables for the user name.



Installer file generation

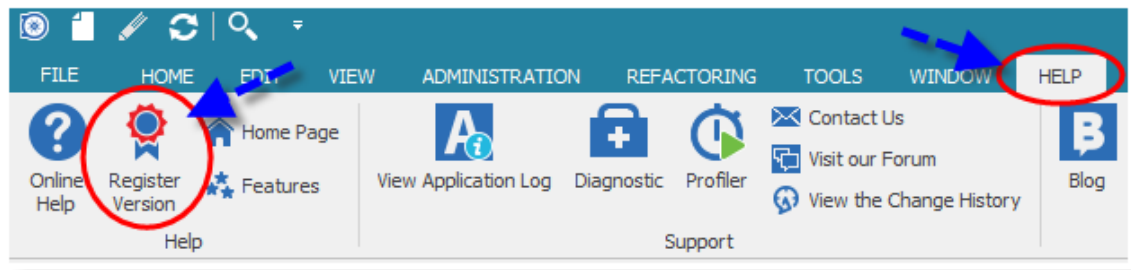
In the description column you will see details contained in the data source definitions, you must share **ONLY** data sources that are either using **Integrated Security** or that are using environment variables for the user name. Password for accessing Password Vault Manager's data source should **NEVER** be shared.

2.1.4 Registration

2.1.4.1 Register Enterprise Edition

Description

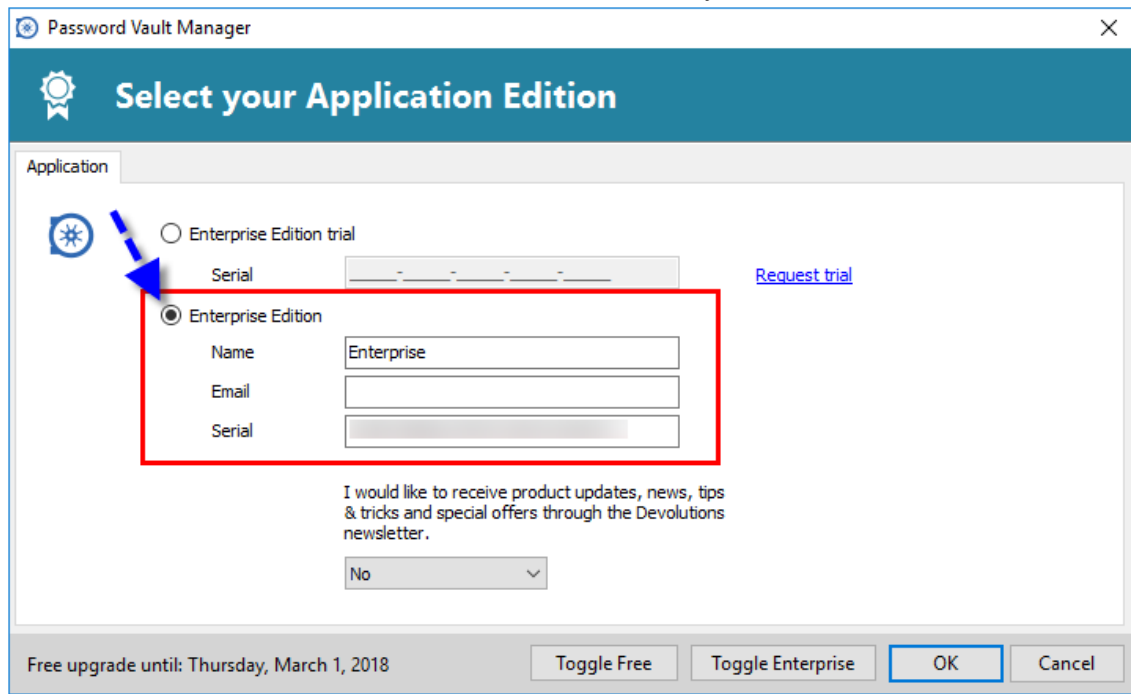
After receiving Devolution's registration email containing your serial license, you will be able to register the application. To enter your license go in **Help - Register Version**.



Register Version

Settings

Select the **Enterprise Edition** or the **Enterprise Edition trial**, depending on which kind of subscription you have, and then enter the user name and serial number exactly as noted in the email.

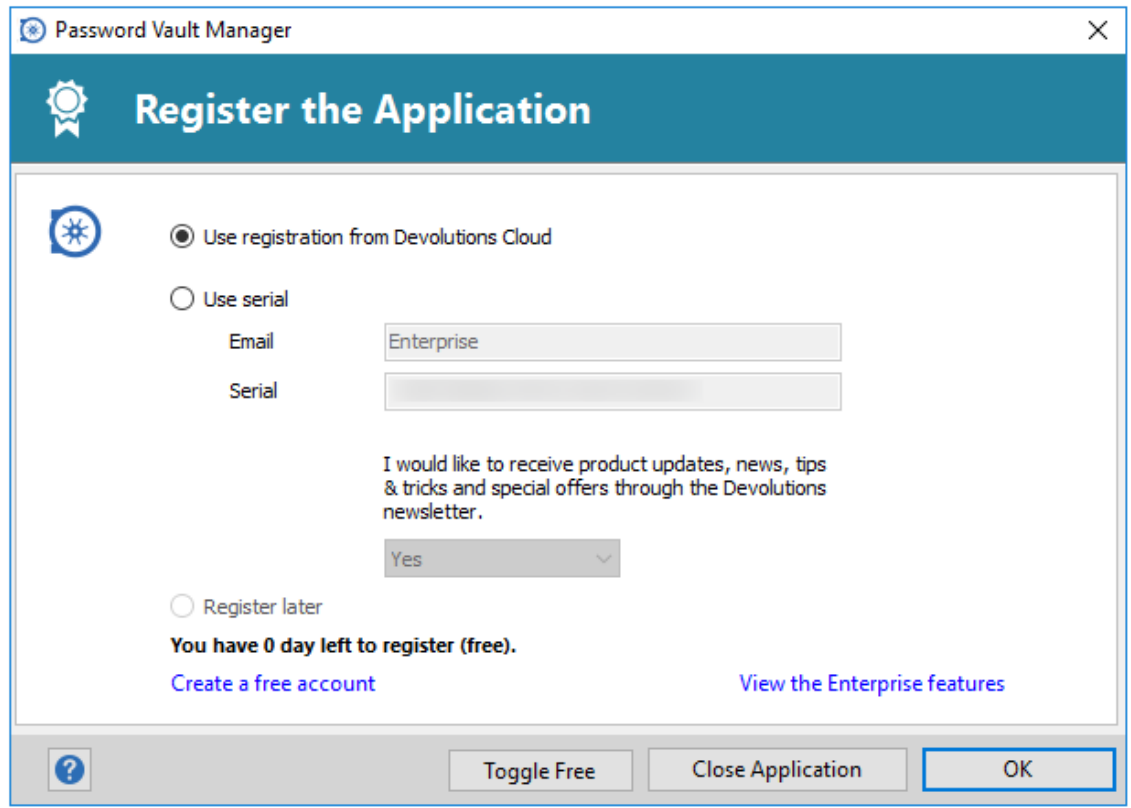


2.1.4.2 Register Free Edition

Description

The Free Edition of Password Vault Manager is indeed free, but does require registration in order to use it. To allow you to test it fully before having to divulge us your email address, we have granted a 30 day grace period during which no registration is necessary.

Upon every application launch, this dialog will appear. It presents the number of days left in the grace period, and the choice of source for the registration.



Register the Application

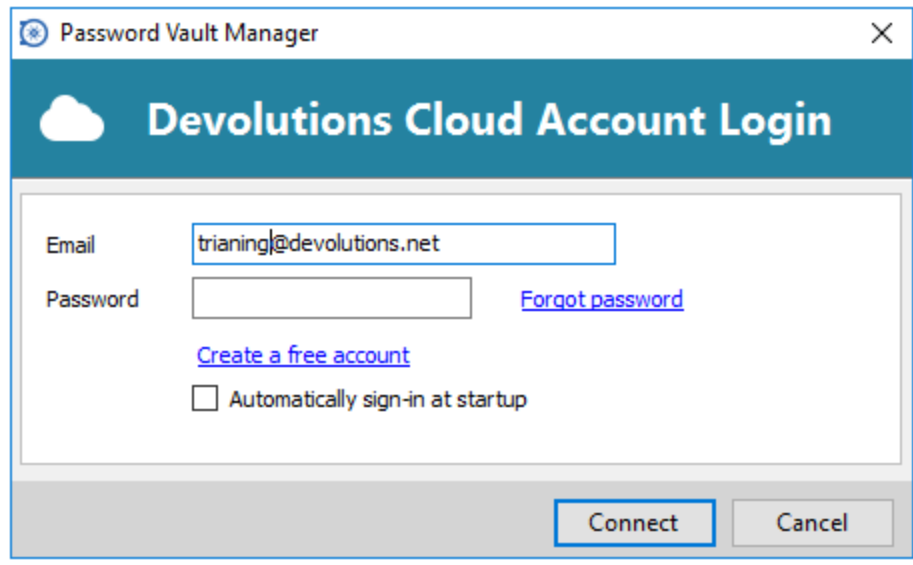
Settings

Use registration from Devolutions Cloud

Every holder of a [Cloud Account](#) (which are also free) has been assigned licence keys for all of our free products. If you select that option, upon pressing OK a dialog will appear prompting for your login information. The license key will automatically be obtained. You can also use the hyperlink to create your free account.

Use an existing cloud account

As you can see in this image, you can enable **Automatically sign-in at startup**, this will be important if you use an [Online Drive](#) data source and/or our [Online Backup Service](#). Enter you account information and we will obtain the serial automatically.



The image shows a dialog box titled "Password Vault Manager" with a close button (X) in the top right corner. The main heading is "Devolutions Cloud Account Login" with a cloud icon to the left. Below the heading, there is a form with the following elements:

- An "Email" label followed by a text input field containing "trianing@devolutions.net".
- A "Password" label followed by a text input field and a blue hyperlink "Forgot password".
- A blue hyperlink "Create a free account".
- A checkbox labeled "Automatically sign-in at startup".

At the bottom right of the dialog box, there are two buttons: "Connect" and "Cancel".

Devolutions Cloud Account Login

Create a new cloud account

Click on the ***Create a free account*** hyperlink in either of the above forms to display the following registration form.



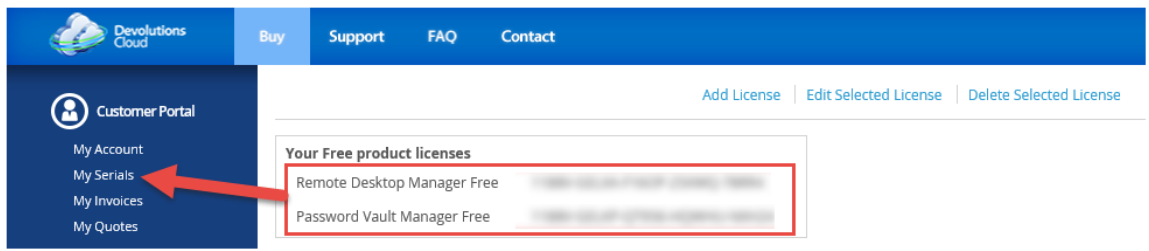
Cloud Account registration is not complete until you have received the activation email and clicked on the ***Activate*** link. Attempting to complete the Password Vault Manager Free registration process will fail until you have confirmed your email address!

Create Devolutions Cloud Account

Manually entering registration information

If you have received a license key through our support or sales channel, or if you need to register the product on a **computer that does not have internet access**; you will then need to manually enter the information.

You can view your serial license from your cloud account, simply login to <https://cloud.devolutions.net/> and click on **My Serials** side menu. This will display your serials for the **Free Editions** of both **Remote Desktop Manager** and **Password Vault Manager**.



My Serials

2.2 Database Upgrade

Description

This topic applies to installations with data sources that are using a database as their data store.

Some releases must modify the database structure. These are performed automatically for you but it is a best practice to perform a backup of your data source beforehand. Additionally if you are in a team environment you must be the sole user connected to the database during the upgrade.

Follow these steps for a successful version upgrade:

1. Ensure you are the sole user of the database during the upgrade process.
2. Backup your database using the DBMS tools.
3. Open RDM while logged in as a user with administrative rights. Please note that you must also be SYSDBA or DB_OWNER.
4. You may be prompted with an upgrade message when your data source is accessed. If so accept the upgrade.
5. Update the client software on all workstations.

2.3 Uninstall

Instructions

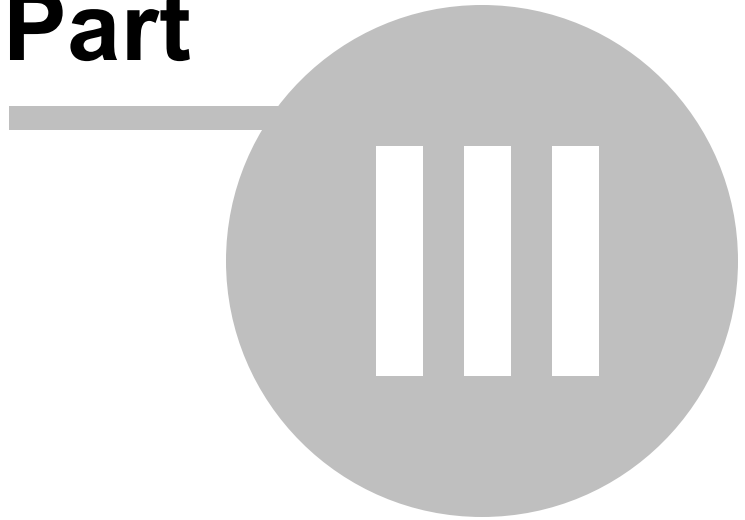
Password Vault Manager doesn't install anything in the Windows directory, and the only registry settings created are for the auto run and the installation path. As a result, Password Vault Manager can be uninstalled easily.

You can run the uninstaller if it was installed with the default setup file, or delete the installation folder directly if it was installed from the binaries.

You can also manually delete the content of "**%LocalAppData%\Devolutions
\RemoteDesktopManager**" or "**%AppData%\Devolutions\RemoteDesktopManager**"

Commands

Part

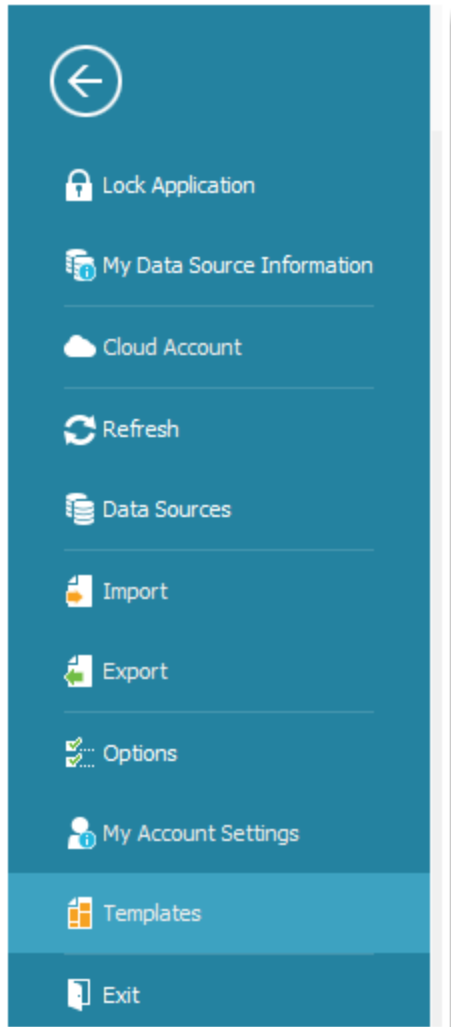


3 Commands

3.1 File

Description

The **File** menu contains several actions available to you regarding your data source. The options will change depending on the type of data source you are currently using.



File

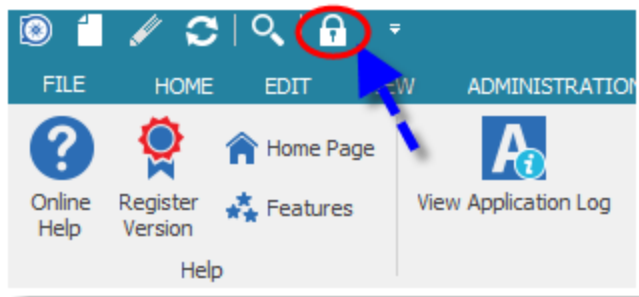
See the following topics for more information:

- [Lock Application](#)
- [My Data Source Information](#)
- [Cloud Account](#)
- [Refresh](#)
- [Manage Password](#)

- [Backup](#)
- [Import](#)
- [Export](#)
- [Options](#)
- [My Account Settings](#)
- [Templates](#)

3.1.1 Lock Application

You can manually lock the application by clicking on **File - Lock Application** or by pressing the **Lock Application** button in the Quick Toolbar. Once locked the application will automatically close and be locked by your application password.



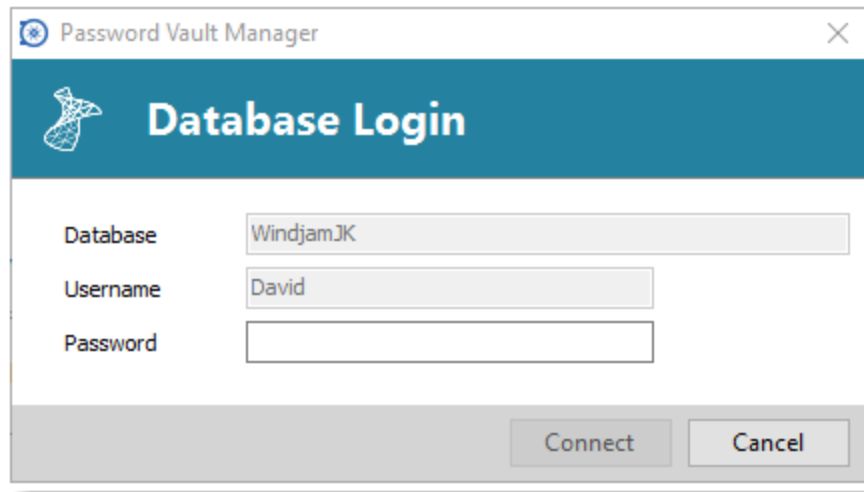
Lock Application button

The Lock Application button can be hidden in the configuration by checking the Disable lock in quick toolbar option.



The Lock Application button can be hidden in the configuration by checking the **Disable lock** in the quick toolbar option.

When reopening the application after it has been locked you will be prompted with the application login screen, enter your password to be granted access again.



Database Login

3.1.2 My Data Source Information

Description

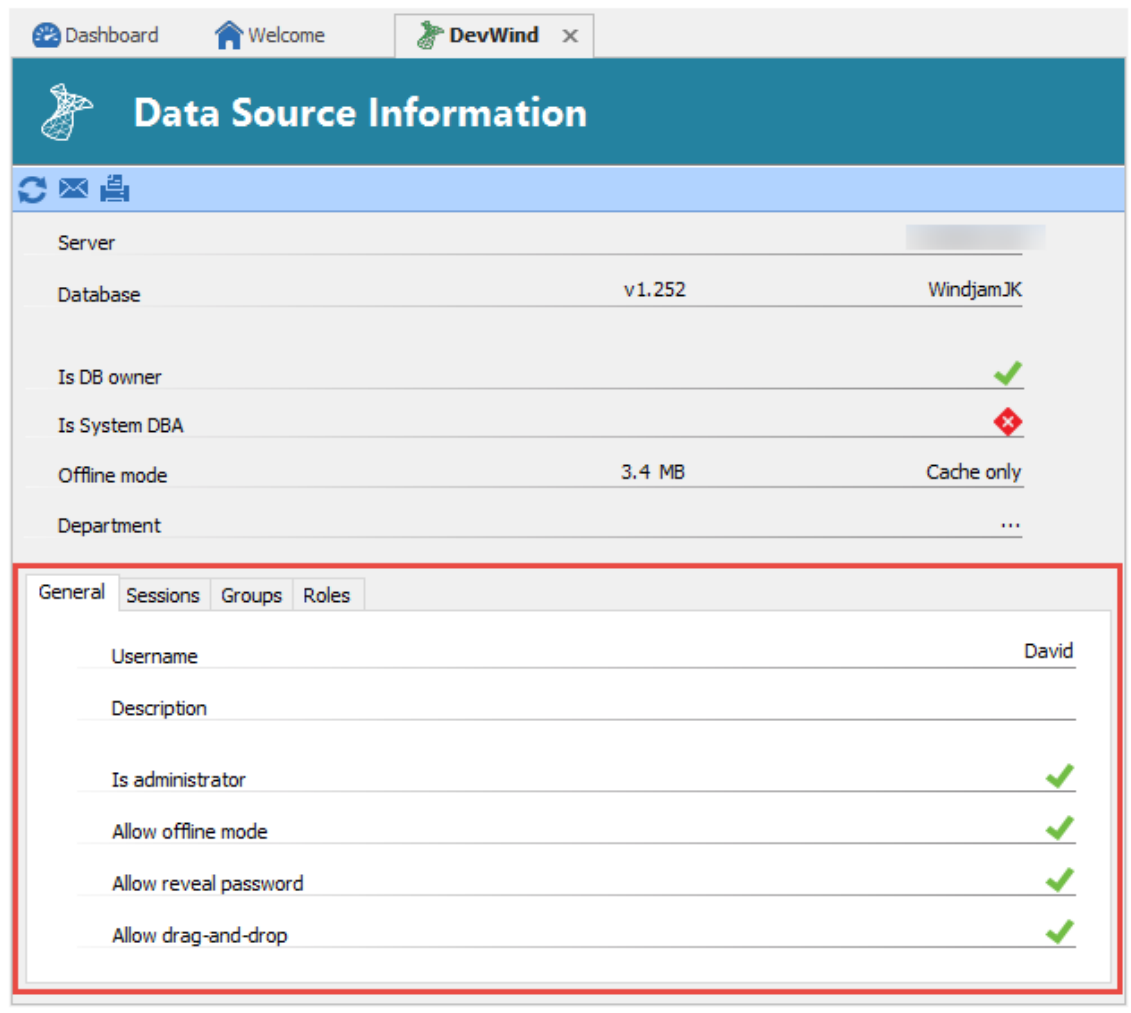
Use the **File - My Data Source Information** to display the data source information details like the current username and security access. The **My Data Source Information** screen will also give you the data source configuration information such as database version and the effective [Offline Mode](#).



The display of **My Data Source Information** can differ depending on the [Data Sources](#) type.

Settings

General



The screenshot shows the 'Data Source Information' window in DevWind. The window has a title bar with 'Dashboard', 'Welcome', and 'DevWind x'. Below the title bar is a blue header with a gear icon and the text 'Data Source Information'. Underneath the header is a light blue bar with icons for refresh, mail, and print. The main content area is a table with the following rows:

Server		
Database	v1.252	WindjamJK
Is DB owner		✓
Is System DBA		✗
Offline mode	3.4 MB	Cache only
Department		...

Below the table is a tabbed interface with four tabs: 'General', 'Sessions', 'Groups', and 'Roles'. The 'General' tab is selected and highlighted with a red border. It contains the following fields:

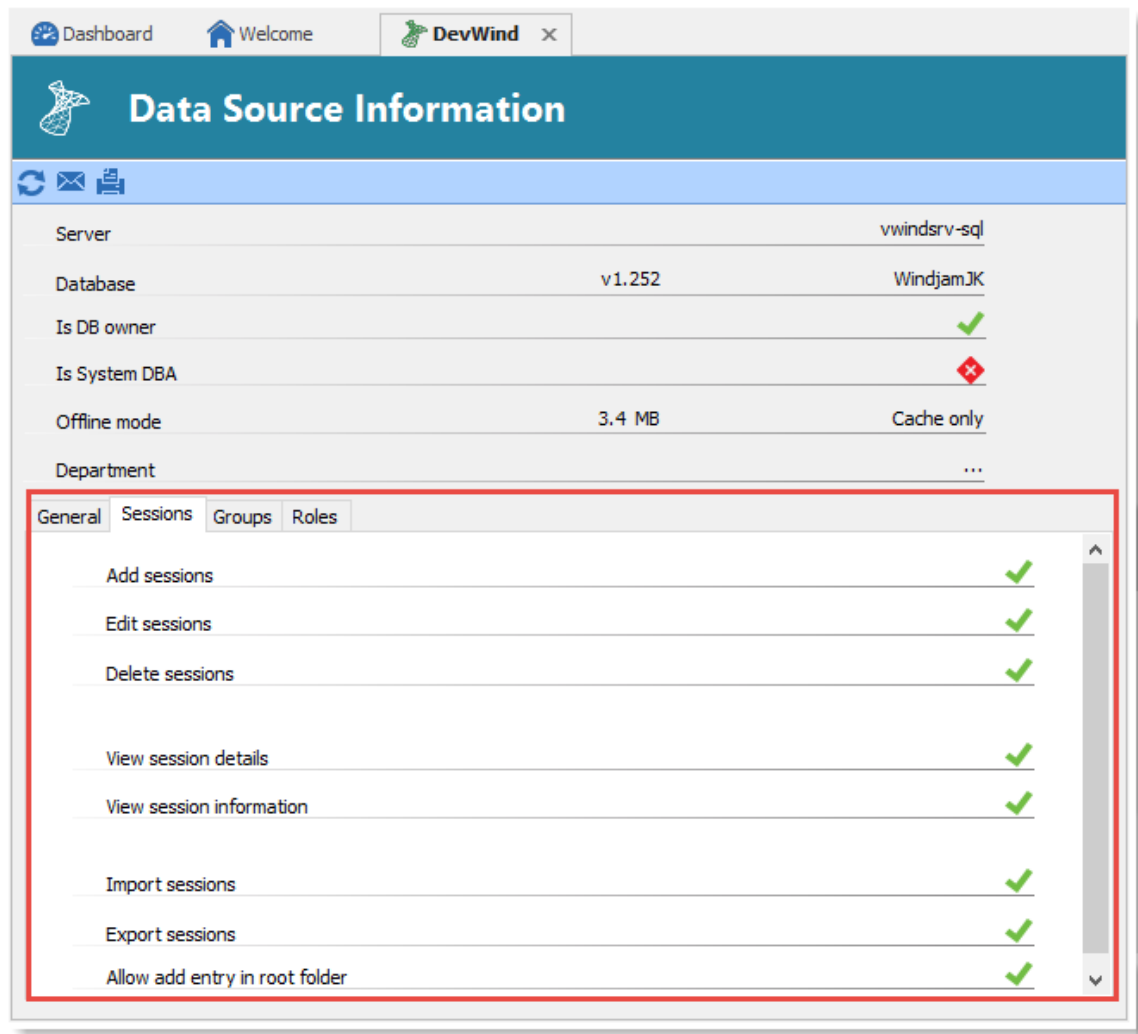
Username	David
Description	
Is administrator	✓
Allow offline mode	✓
Allow reveal password	✓
Allow drag-and-drop	✓

Data Source Information - General tab

The **General** tab displays information on the data source such as:

- Username
- Description
- Administrator rights
- Availability of the offline mode
- Reveal password rights
- Drag-and-drop rights

Sessions



The screenshot shows the 'Data Source Information' page in the Password Vault Manager. The 'Sessions' tab is selected, displaying a list of permissions for sessions. All permissions are granted, indicated by green checkmarks.

Permission	Status
Add sessions	✓
Edit sessions	✓
Delete sessions	✓
View session details	✓
View session information	✓
Import sessions	✓
Export sessions	✓
Allow add entry in root folder	✓

Data Source Information - Session tab

The **Sessions** tab will display user rights on the sessions such as the:

- Add sessions rights
- Edit sessions rights
- Delete sessions rights
- View session details rights
- View session information rights
- Import sessions rights
- Export sessions rights
- Allow add entry in root folder rights

Groups

The screenshot shows the 'Data Source Information' page in DevWind. The page has a blue header with a logo and the title 'Data Source Information'. Below the header is a navigation bar with icons for refresh, email, and print. The main content area is divided into two sections. The top section is a table with the following data:

Server		
Database	v1.252	WindjamJK
Is DB owner		
Is System DBA		
Offline mode	52.0 KB	Cache only
Department		...

Below this table is a tabbed interface with four tabs: 'General', 'Sessions', 'Groups', and 'Roles'. The 'Groups' tab is selected, showing a table with the following data:

Group Name	Rights
Customer Group	View, Add, Edit, Delete
Windjamm Group	View

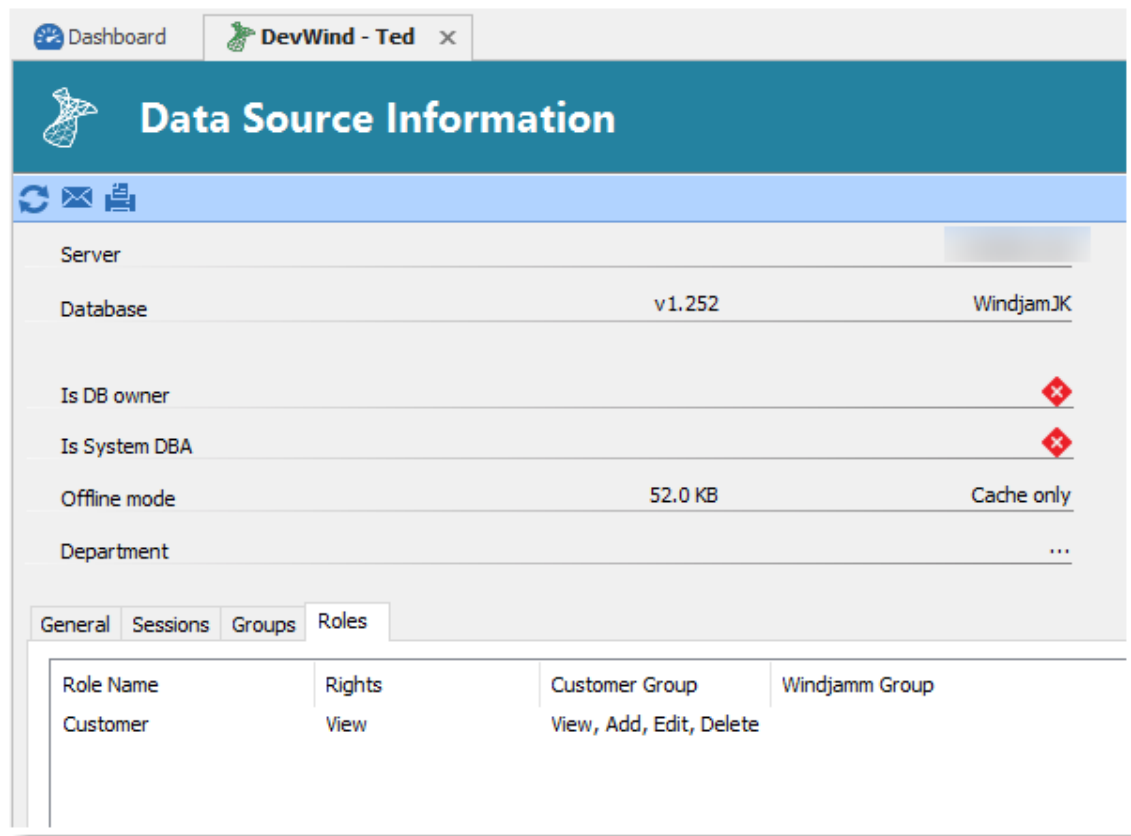
Data Source Information - Groups tab

The **Groups** tab displays the user's rights on each security groups.

Roles



This feature is only available with an [SQL Server](#), [SQL Azure](#) and [Devolutions Server](#) data source.



The screenshot shows the 'Data Source Information' page in the Password Vault Manager. The page has a blue header with the title 'Data Source Information' and a DevWind logo. Below the header is a navigation bar with icons for refresh, email, and print. The main content area is divided into several sections:

- Server:** A greyed-out field.
- Database:** v1.252, WindjamJK
- Is DB owner:** Indicated by a red 'X' icon.
- Is System DBA:** Indicated by a red 'X' icon.
- Offline mode:** 52.0 KB, Cache only
- Department:** ...

Below these sections are tabs for 'General', 'Sessions', 'Groups', and 'Roles'. The 'Roles' tab is active, showing a table with the following data:

Role Name	Rights	Customer Group	Windjamm Group
Customer	View	View, Add, Edit, Delete	

Data Source Information - Roles tab

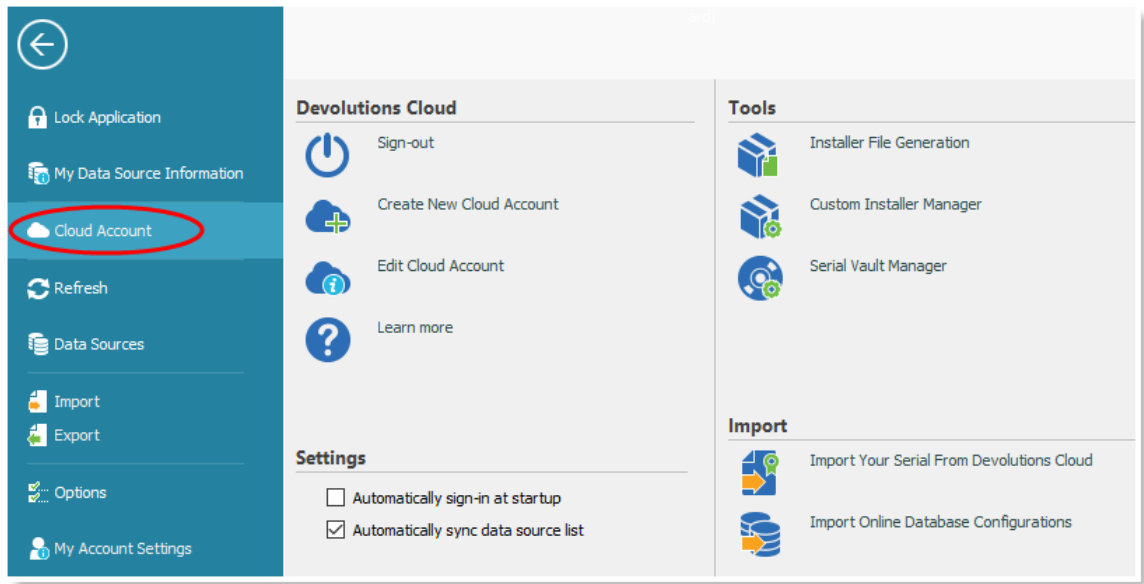
The **Roles** tab displays which roles the user is a member of and the rights defined by those roles.

3.1.3 Cloud Account

Description

Use **File - Cloud Account** to create/connect Password Vault Manager to your Devolutions Online Database account.

Settings



Cloud Account

Devolutions Cloud

Option	Description
Sign-in or Sign-out	Sign-in with your 'previously created Devolutions Cloud account. Sign-out of your Devolutions Cloud account.
Create a New Cloud Account	Create a new cloud account.
Edit Cloud Account	Edit your cloud account.
Learn More	Open Devolutions Cloud Online Help in your browser.

Settings

Option	Description
Automatically sign-in at startup	Automatically sign-in to your cloud account when opening the application.
Automatically sync data source list	Automatically sync the data source list from your cloud account to the application.

Tools

Option	Description
Installer File Generation	Create a Password Vault Manager Installer File (.rdi). Consult topic Installer File Generation for more information.
Custom Installer Manager	Please consult topic Custom Installer Service for more information.
Serial Vault Manager	Add your licenses in the Serial Vault to centralize your license key and to have them in your cloud account.

Import

Option	Description
Import your Serial from Devolutions Cloud	Import the serial from your cloud account.
Import Online Database Configurations	Import Online database configuration in the application.

3.1.4 Refresh

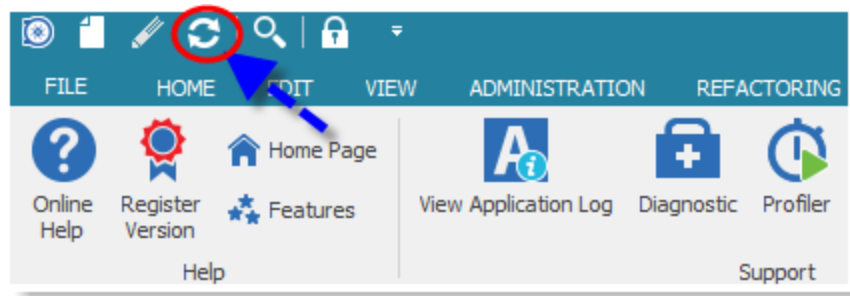
Description

Use **File - Refresh** to refresh your data source information. Performing a refresh will assure you that your data source is up to date.

A **Refresh** may also help when experiencing Cache issues.

Settings

You may also perform a refresh of your data source by holding the CTRL key + the refresh button.



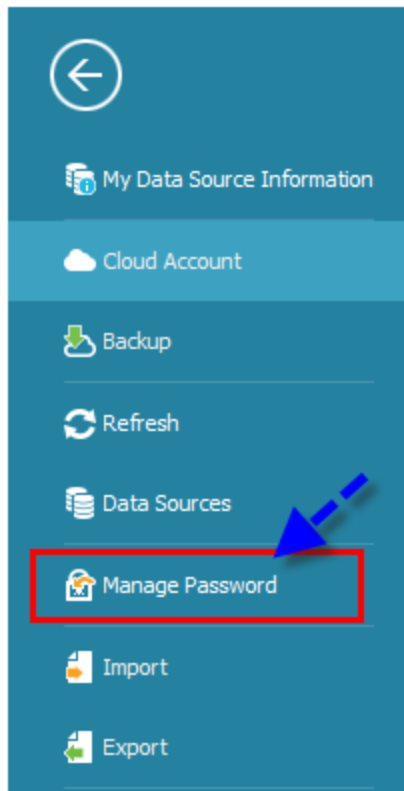
Refresh Account

3.1.5 Manage Password

Description

Use **File - Manage Password** to apply a Master Key or Encryption key to these types of data source:

- [XML](#)
- [FTP](#)
- [Devolutions Online Drive](#)
- [Dropbox](#)



Manage Password

It is generally a good idea to apply a Master Key to your data source, as it adds another layer of security protecting your Remote Sessions. It is highly advisable to implement the Master Key functionality if you're using Password Vault Manager in a portable environment (i.e. USB Flash Drive, USB Hard Drive), or if the data source is the portable portion of the application.

The use of the Master Key function will stop unauthorized users from being able to easily see/access the stored Sessions within your Data Source.

Password Vault Manager

Data Source Password

Password

Re-enter

We won't be able to recover your data if you lose your password. Please ensure that you remember or backup your password in a safe place.

No Password Save Cancel

Data Source Password

3.1.6 Backup

Description



The **Online Backup** is available only for your Devolutions Online Drive, SQLite, XML or Microsoft Access data sources.

Please consult topic [Online Backup](#) for information on this service.

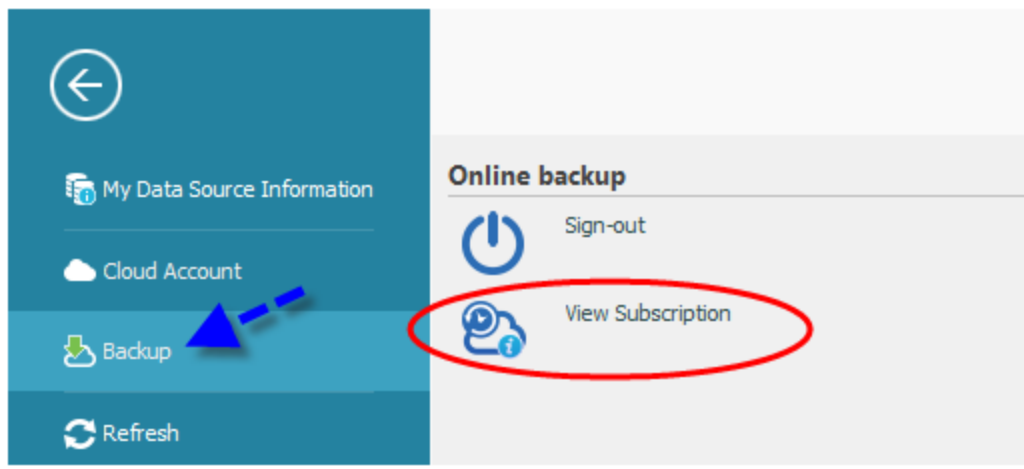
3.1.6.1 Settings

Description

The [Online Backup](#) allows you to backup your [Devolutions Online Drive](#), [SQLite](#), [XML](#) or [Microsoft Access](#) data sources in a safe online storage. The backup option is available through **File - Backup** menu.

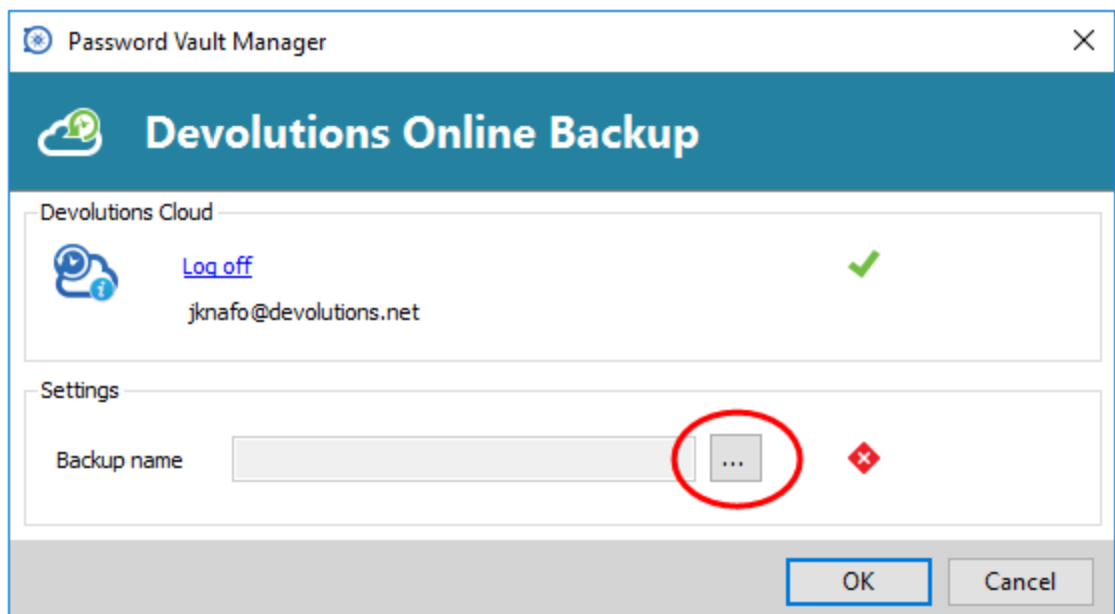
Settings

1. Click on **File - Backup** to Sign-in with your Devolutions Cloud account.
2. Click on **View Subscription**,



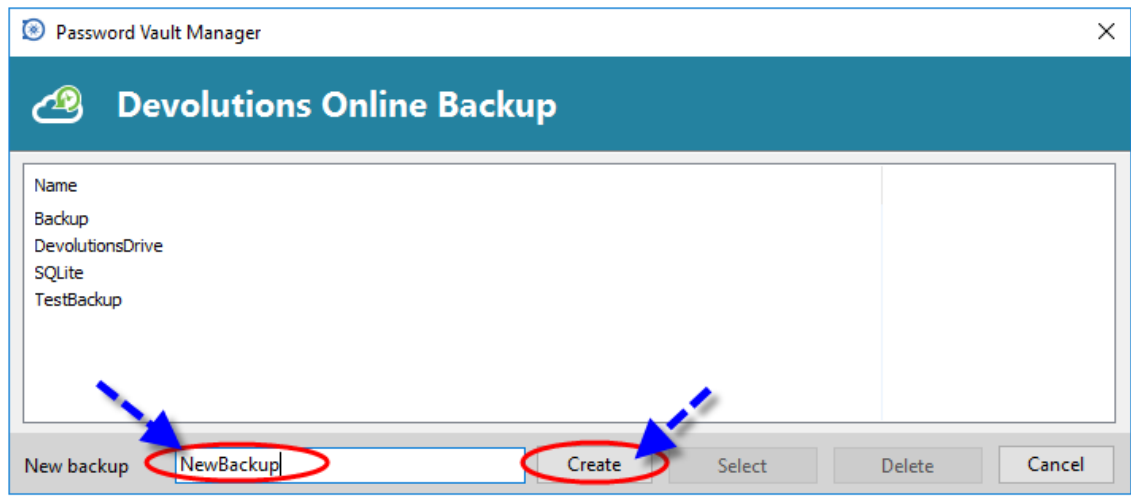
Backup - View Subscription

3. Click on the ellipsis to enter your Backup name.



Devolutions Online Backup

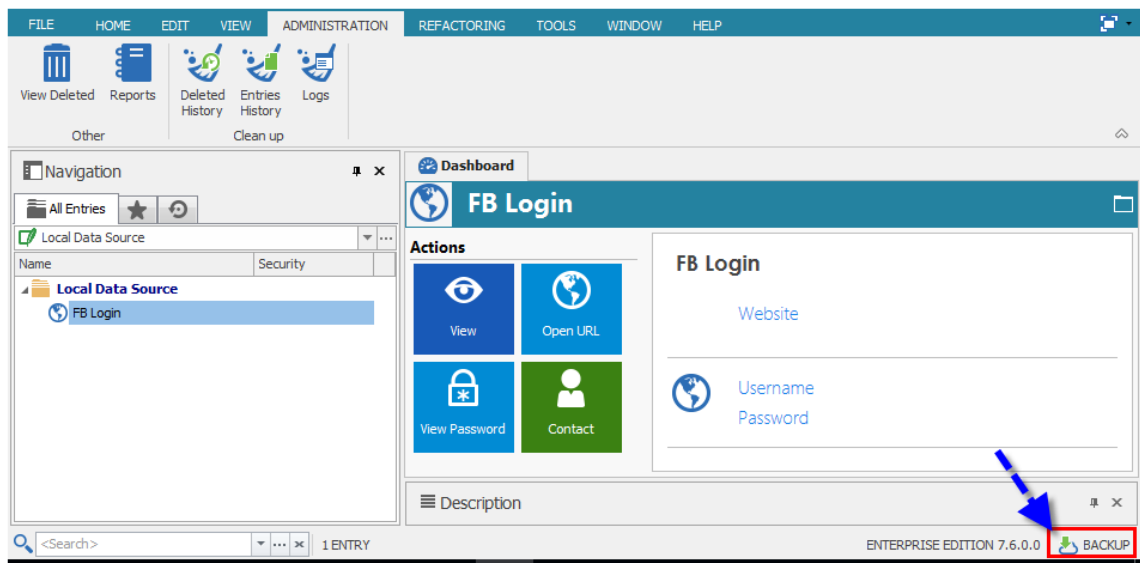
4. You will need to specify a unique backup name in the field **New backup** for each of your data source which will then be used to backup and restore the data source. Click on **Create** to automatically create your Online backup.



Devolutions Online Backup

5. Once you've completed all the steps, perform a change in the data source to properly activate the Online Backup.

6. The backup logo will display a green arrow meaning your backup is now enabled.



Backup Activated

You must perform this for all your Devolutions Online Drive, SQLite, XML or Microsoft Access data sources in order to be fully protected.

The automatic backup is executed in the background 30 seconds after any modification is made to the data source content.

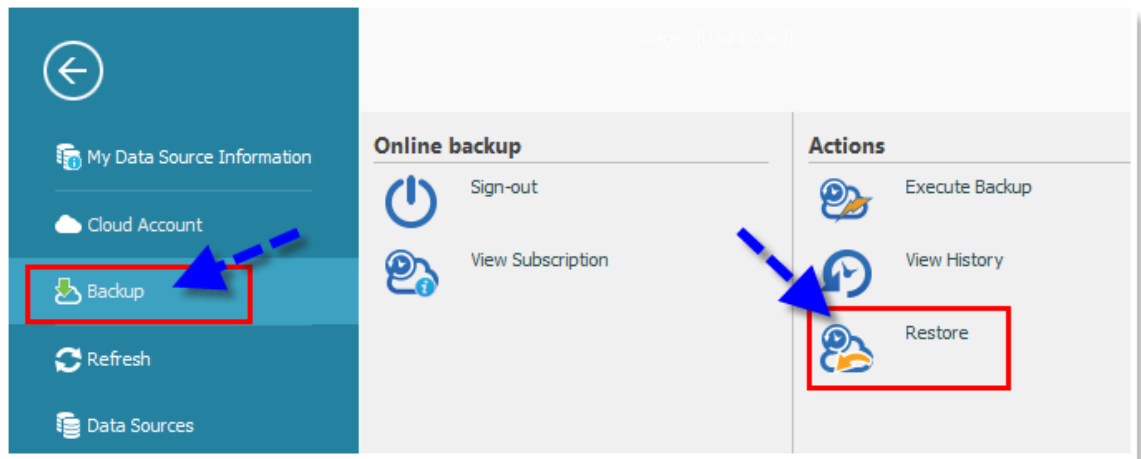
3.1.6.2 Restore

Description

At some point, you may need to restore a backup of your [Devolutions Online Drive](#), [SQLite](#), [XML](#) or [Microsoft Access](#) data sources. The restore option is accessible from the menu **File - Backup - Restore**.

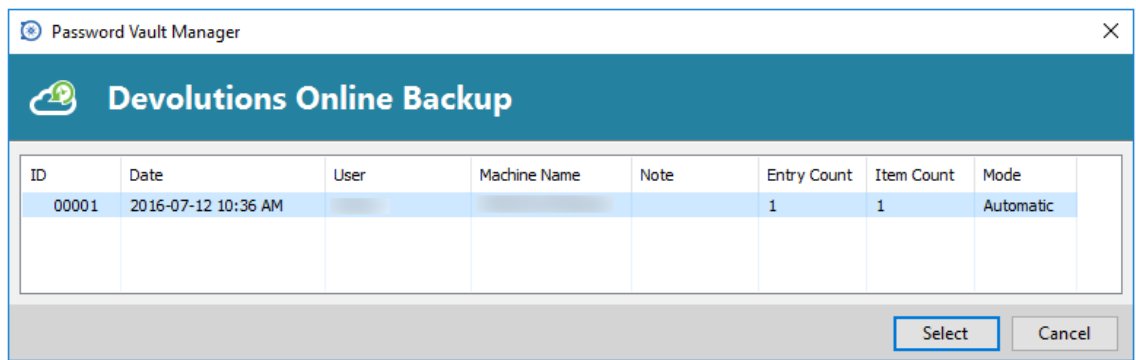
Settings

1. To restore a data source from a backup, select it as the current data source.
2. Click on **File - Backup - Restore**.



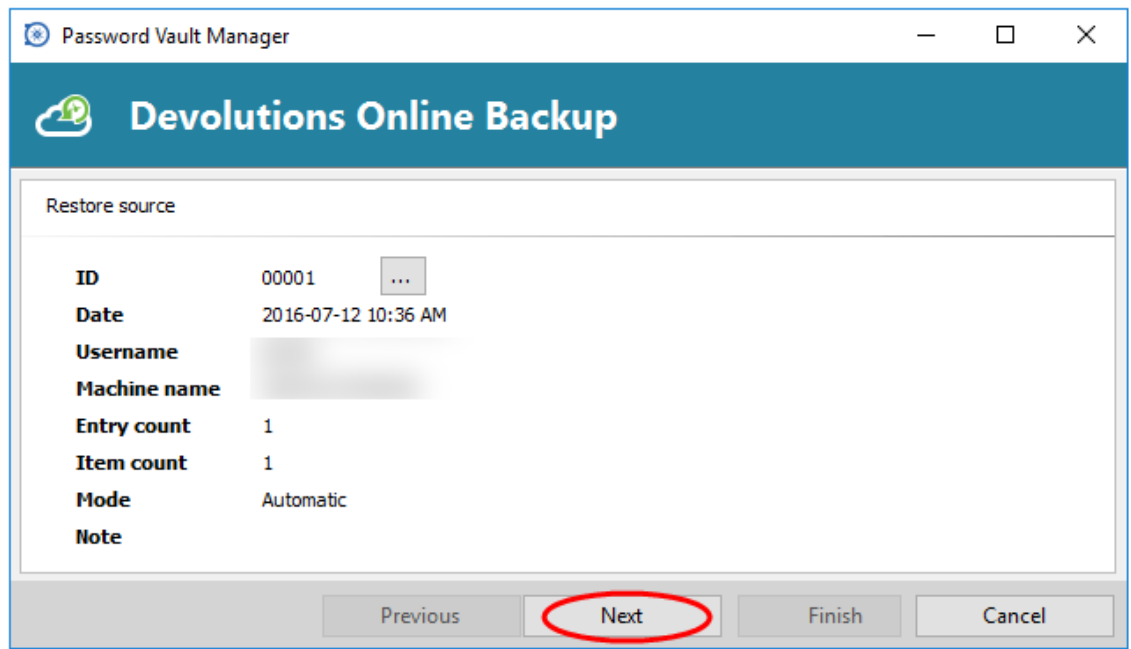
Restore Backup

3. Select the backup that you wish to restore from the list and click on Select.



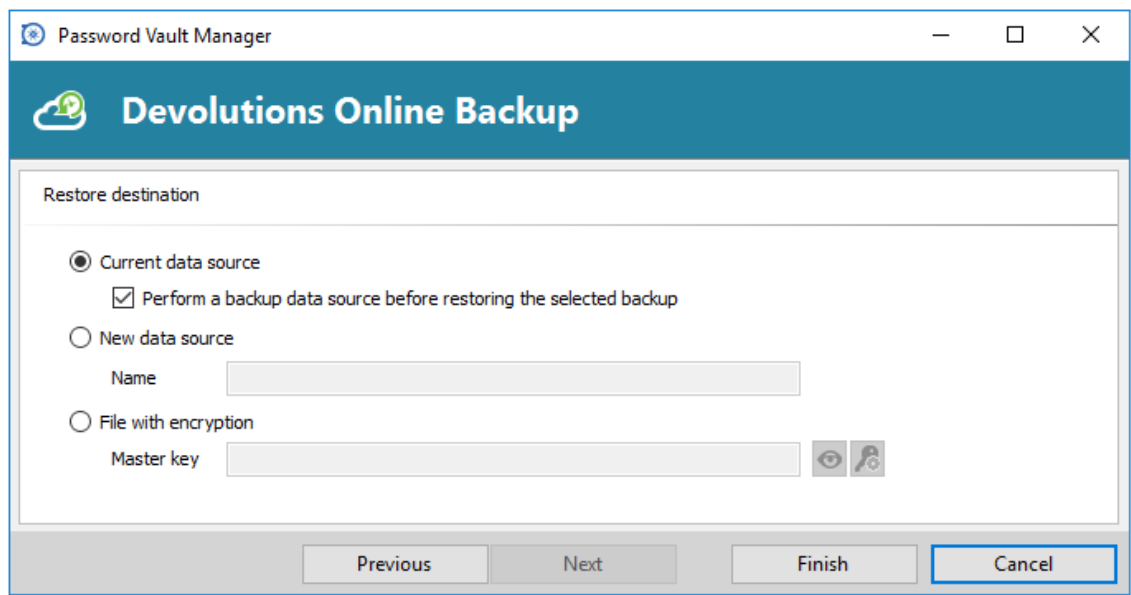
Select your Backup

4. The Online Backup wizard will display a brief description of the backup. Click on Next.



Backup Wizard

5. Select the destination to restore your backup.



Restore destination

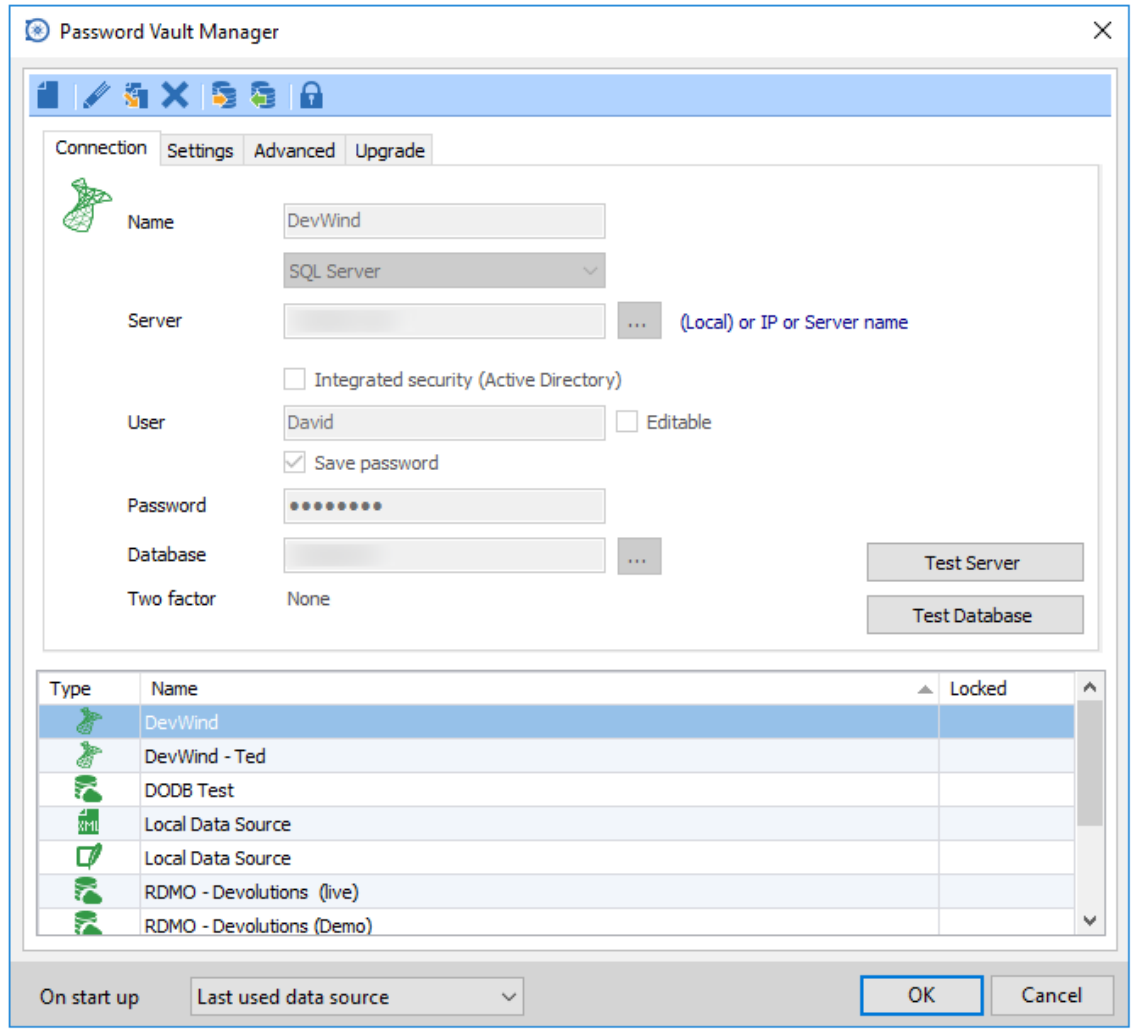
6. Click on **Finish** to perform your backup restore.

3.1.7 Data Sources

Description

Use **File - Data Sources** to manage your data sources. Remote Desktop Manager supports multiple types of data source. Some will only be available with a Remote Desktop Manager Enterprise edition.

Please refer to the topic [Data Source Types](#) for more information on all types of supported data sources.



Data Sources

Settings

Add a new data source

Use the add button to create a new data source configuration.

Edit/Duplicate/Delete data source

Use buttons to edit, duplicate or delete a data source configuration.



Only the configuration will be deleted but the actual file or database will still be available.

Import/Export data source configuration

Use buttons to import or export data source configuration. The configuration will be exported in a .RDD file making it easy to configure Password Vault Manager on another workstation.

Lock data source

Use the Lock button to lock the data source with a password to prevent any modification to a data source configuration. This is useful when having sensitive credentials that you wish to protect from other users.

Unlock data source

Use the Unlock button to unlock a data source locked with a password.

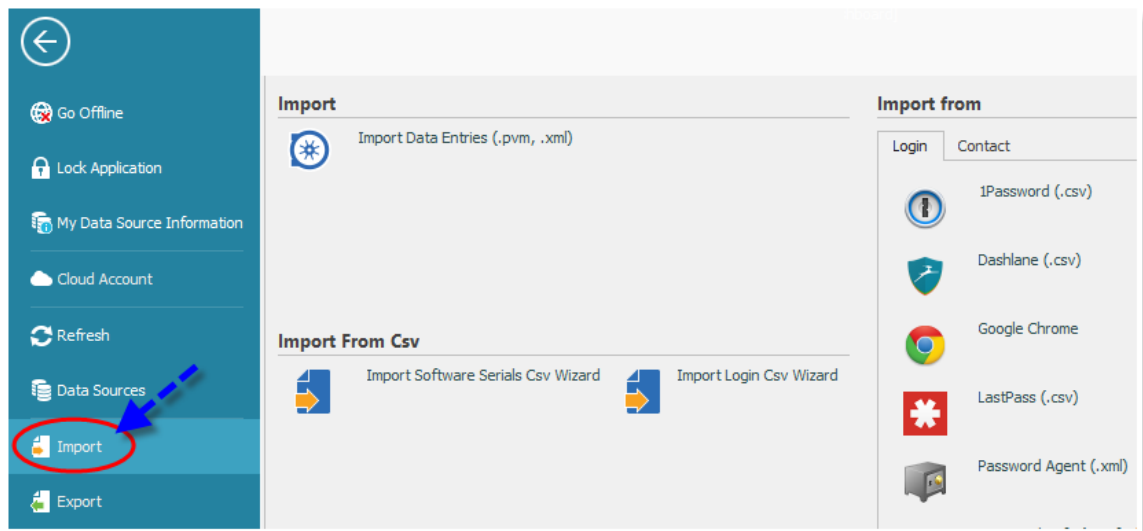
On start up

Option	Description
Use default data source	Set the data source that you wish to automatically open at start up.
Last used data source	Automatically open the last used data source at start up.
Prompt for data source	Prompt for the data source selection at start up.

3.1.8 Import

Description

Password Vault Manager can import from various sources. It can use its own export files, but also many other applications data. If your preferred application is not supported natively, an import wizard is provided to allow you to perform a massive import rapidly.



File - Import

Import Logins

You can also import your logins from an existing application. Your configuration file data must not be encrypted in order to allow Password Vault Manager to parse the content.

The list of the supported applications includes:

- 1Password
- Aurora Password Manager
- Dashlane
- DataVault
- Google Chrome
- KeePass
- LastPass
- Passpack
- Password Agent
- Password Depot
- Password Safe
- RoboForm
- SplashID
- Sticky Password

Using the Import Wizard

Please see the [Import Login Wizard](#) topic.

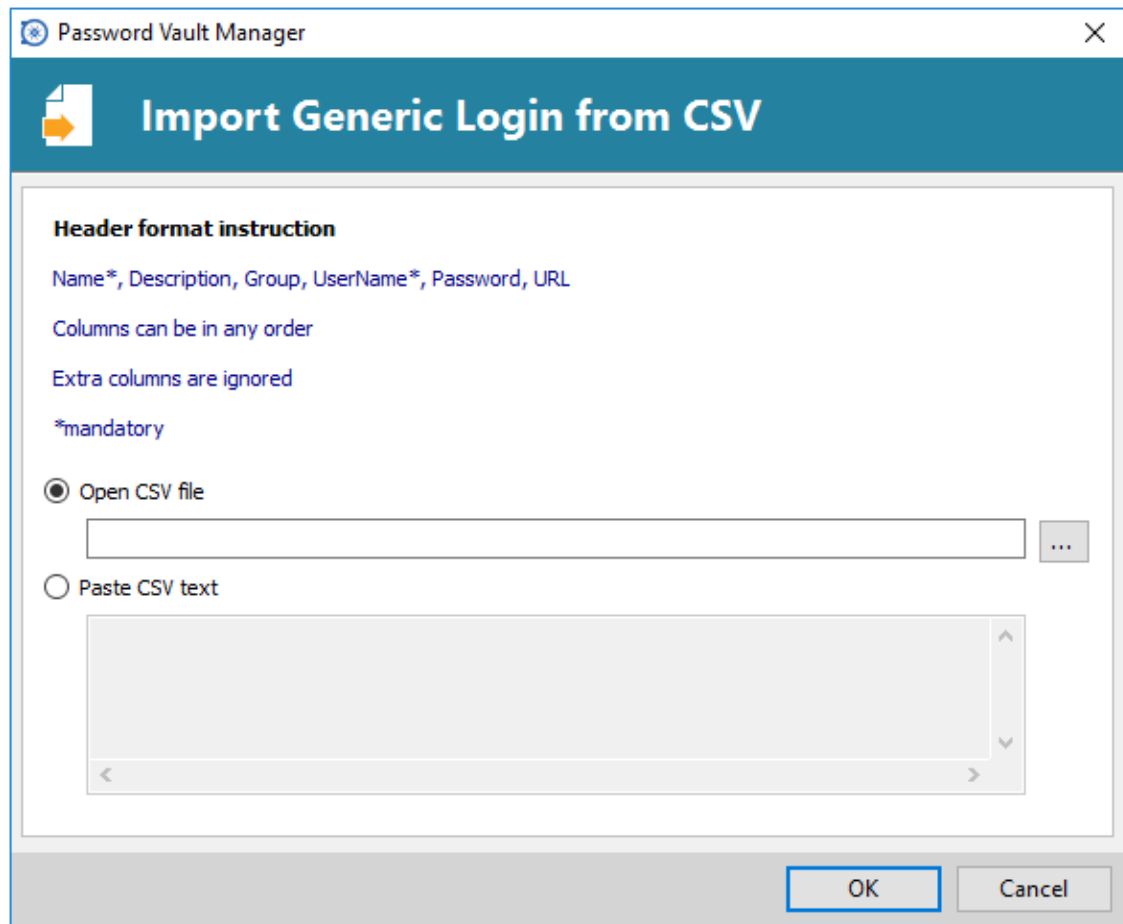
Import Data Entries

When your file was first generated using Password Vault Manager in its native format, it should have the contained a .pvm extension. Simply select the appropriate **Import Data Entry** menu to perform the operation.

3.1.8.1 Import Login Wizard

Description

When your application data file format is not natively supported by Password Vault Manager, you can use a plain csv file to create your data entries. This would be extremely useful when you wish to restructure the unsupported data file into a compatible csv file.



Import Login Wizard

Prerequisites

Our csv format has the following pre-requisites:

- The column separator must be a comma
- The string escape character is the double quote. You must use this if one of your fields contain commas.
- The following columns are mandatory : Name, UserName.
- The following columns are optional but imported when present : Description, Group, Password and URL.

Notes

- All other columns are simply ignored.
- The columns are accessed by name, therefore the order is unimportant.
- Instead of using a file, you can paste the content directly in the form.

3.1.9 Export

Description

Use the **File - Export** to export entries from Remote Desktop Manager. Below is a list of export options:

- Export All Entries (.pvm)
- Export All Entries (.csv)
- Export All Entries (.html)
- Export All Entries (.xml) (It's exactly the same content as a .rdm file but with the XML extension)
- Export All Documents

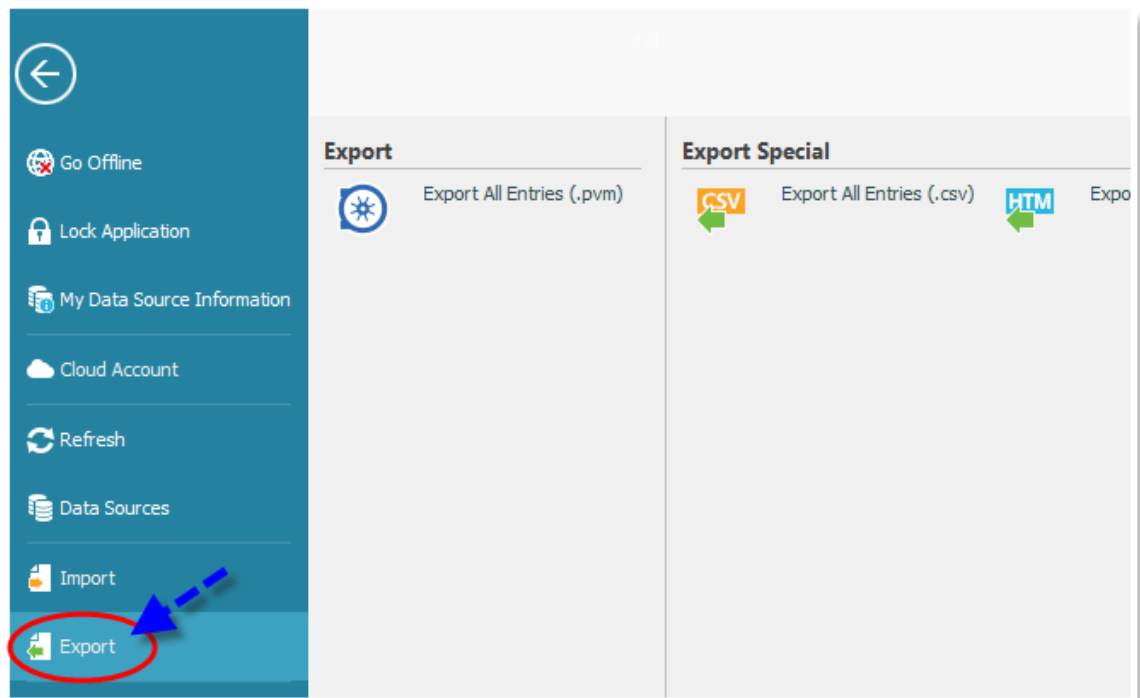


The export feature is only active if the import [Permission](#) has been enabled inside the user account.



The only appropriate format to import the entries back into Password Vault Manager is the .pvm format.

Settings



File - Export



When using an [Advanced Data Source](#), export capabilities can be disabled via security policies at the data source level (no one can export) or at a user level (particular users can't export). See [Security Group Management](#) for more information.

Export All Entries (.pvm)

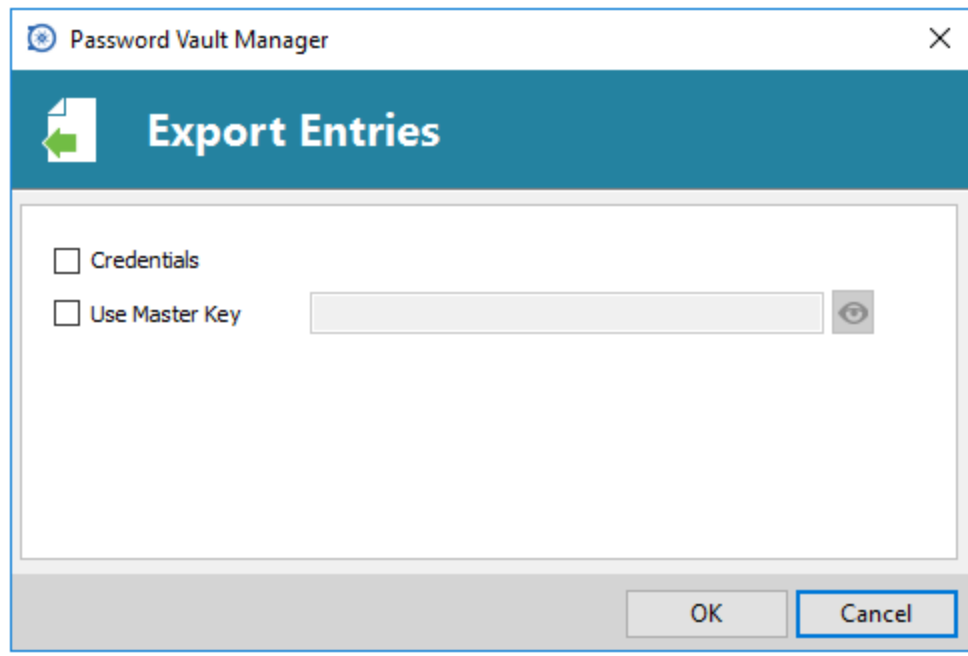
Export all entries in a .pvm file that can be imported into any Password Vault Manager data source. You can secure your file with a master key.



By default the credentials are NOT included. It's critical to check the Credentials option in order for the exported data to include the credentials.



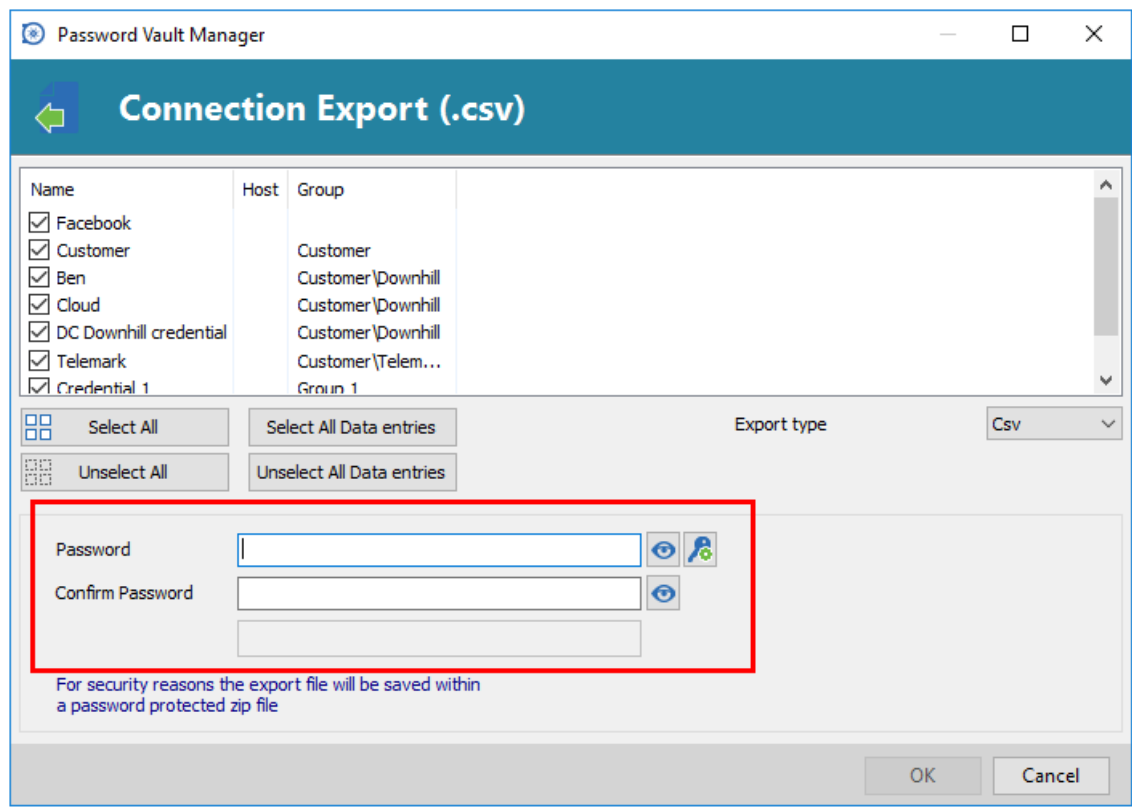
Specifying a master key will encrypt the whole content of the .pvm file to protect its content. It is highly recommended as a backup measure, but the key is absolutely necessary for decryption. Preserve this as well in a separate storage device for safekeeping.



Export Entries

Export All Entries (.csv)

Export all entries using the .csv format file. For security reasons the .csv file will be contained within a password encrypted zip file. This type of security can be hacked using brute force attacks, it should be used only when the zip file is under your exclusive control.



Connection Export

Export All Entries (.html)

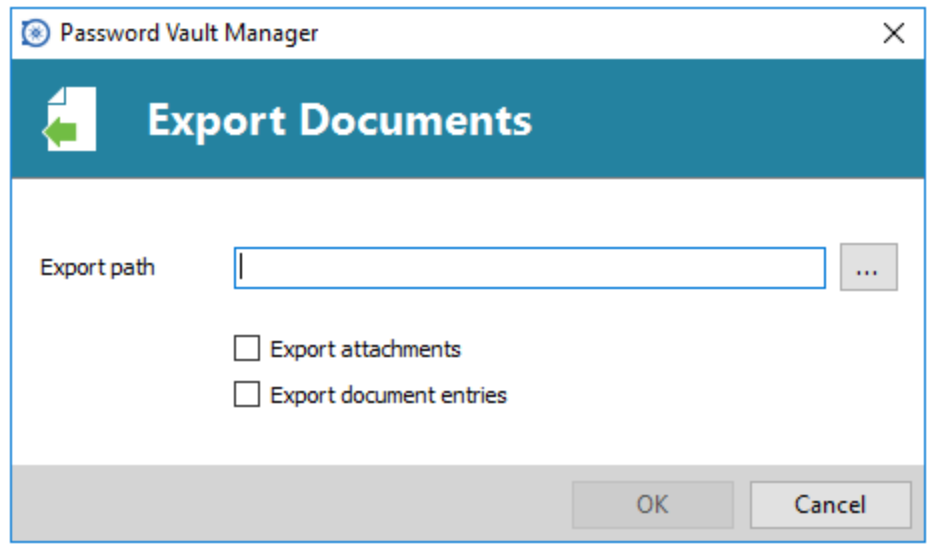
Exports all data entries within a AES-256 to encrypt self contained html file. See [Export Html Encrypted](#) for more information.

Export All Entries (.xml)

Based on prior issues, this export format has been converted to perform the exact same export as the "Export all entries" but sets the file extension to .xml instead.

Export All Documents

Export all attachments or all document entries that are linked to your data source.



Export Documents

¹ - only available via Right-Click menu of the tree view or hot key.

3.1.9.1 Encrypted Html

Overview

Export Html Encrypted was design to allow for simple & secure exports of data entry type sessions. It allows for an .html export of the session information while using symmetric encryption (AES-256) to encrypt sensitive information such as passwords. The file is an ultra portable self contained html file that requires no external script files or installs. As long as you have a web browser with JavaScript enabled you can get to your encrypted data.

Why?

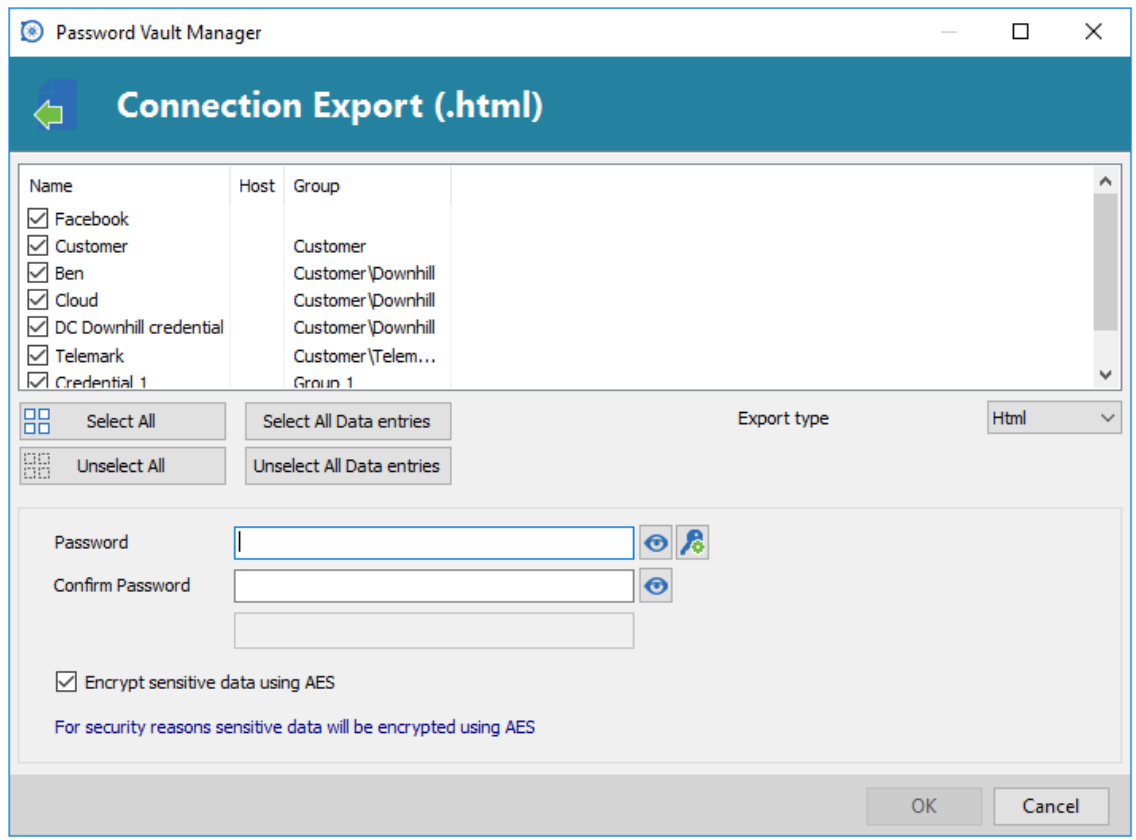
With a secure encrypted document you can freely send the information via email or any other protocol without compromising the sensitive data. Use the export as means of sharing or as a backup for sensitive information.

How To

Select the sessions to export or export all data entries. Right-click **Import/Export - Export Entry - Export Entry (.html)** or use **File - Export - Export All Entries (.html)**. You will be prompted for a password for the symmetric encryption of sensitive information. Select the file name for the new document. Once the export complete the file will open in your default browser.



Make sure you don't forget the password as you will not be able to decrypt the data without it.



Password for symmetric encryption

When exporting multiple entries they will all be contained within the same file. At decrypt time, each encrypted value must be decrypted individually for security reasons. Once you're done with the sensitive data simply hit F5 to refresh the file or simply close it. Your data is now safe from prying eyes.

AES-256

We use AES-256 to encrypt/decrypt your sensitive data. Since the decryption is done entirely in the browser, there's no need for external tools, downloads or installs.

```

▼<tr>
  <td class="label Password">Password</td>
  ▼<td class="value Password">
    ▼<span id="dff570b2-5fb1-459b-af38-0fcb4f677484" data="U2FsdGVkX1/TAub+TpB+UrMU2m1RSVdiU8FP7tPnXAaBLZdvSV9IiM2AKdIv0Siv">
      <a class="encrypted" onclick="javascript:decryptText('dff570b2-5fb1-459b-af38-0fcb4f677484')">*****</a>
    </span>
  </td>

```

Encrypted value

Safe & Smart Virtual Backup

In addition, HTML Export using symmetric encryption is a great way to securely – and virtually – backup your passwords and other sensitive information. It allows you to share information via email, or simply send the file to your personal email account as a backup.

3.1.10 Options

Description

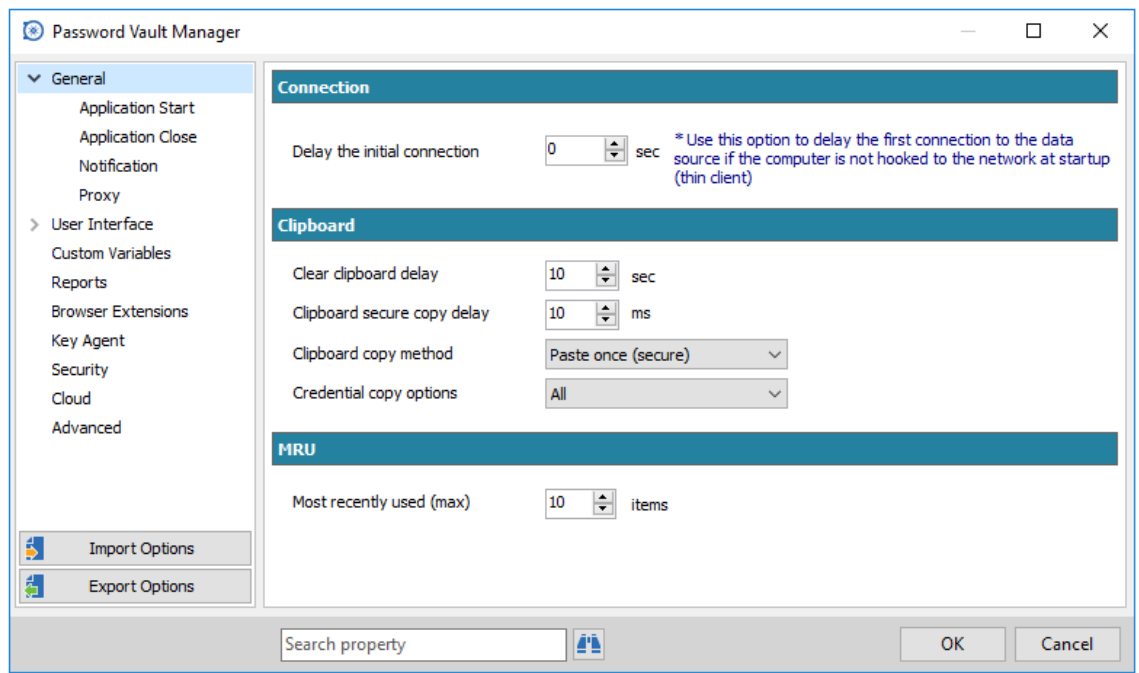
Password Vault Manager contains several options which are explained in detail in the following subtopics.

- [General](#)
- [User Interface](#)
- [Custom Variables](#)
- [Reports](#)
- [Browser Extensions](#)
- [Key Agent](#)
- [Security](#)
- [Cloud](#)
- [Advanced](#)

3.1.10.1 General

Description

Use the **File - Options - General** to control application behaviour as it pertains to Startup, application close, notification and proxy settings.



Options - General

Settings

Connection

Option	Description
--------	-------------

Delay the initial connection	Use this option to delay the first connection to the data source if the computer is not hooked to the network at startup (thin client).
------------------------------	---

Clipboard

Option	Description
Clear clipboard delay	Set the delay to empty the clipboard after a copy of a remote information.
Clipboard secure copy delay	Set the delay before Password Vault Manager clears the clipboard. When experiencing issue with the copy/paste the delay for the clipboard might be to short, you can change it to allow more time to proceed with the copy/paste.
Clipboard copy method	Select your copy method between: <ul style="list-style-type: none"> • Paste once (secure): This is our default method used for the clipboard, it is more secure allowing you to copy once, paste two (copy the credentials, paste the username, paste the password) without having to actually copy twice. For more information please follow this link. • Legacy: Some application has been knows to cause issues with the Paste once (secure) method, if experiencing problems you can revert to the legacy copy/paste method.
Credential copy options	Select which Copy/Paste button options you wish to see in your ribbon. <ul style="list-style-type: none"> • All: See the Copy Username/Password, the Copy Username and the Copy Password buttons. • Single action: Only see the Copy Username/Password button (single action). • Dual action: Only see the Copy Username button and the Copy Password button (dual action).

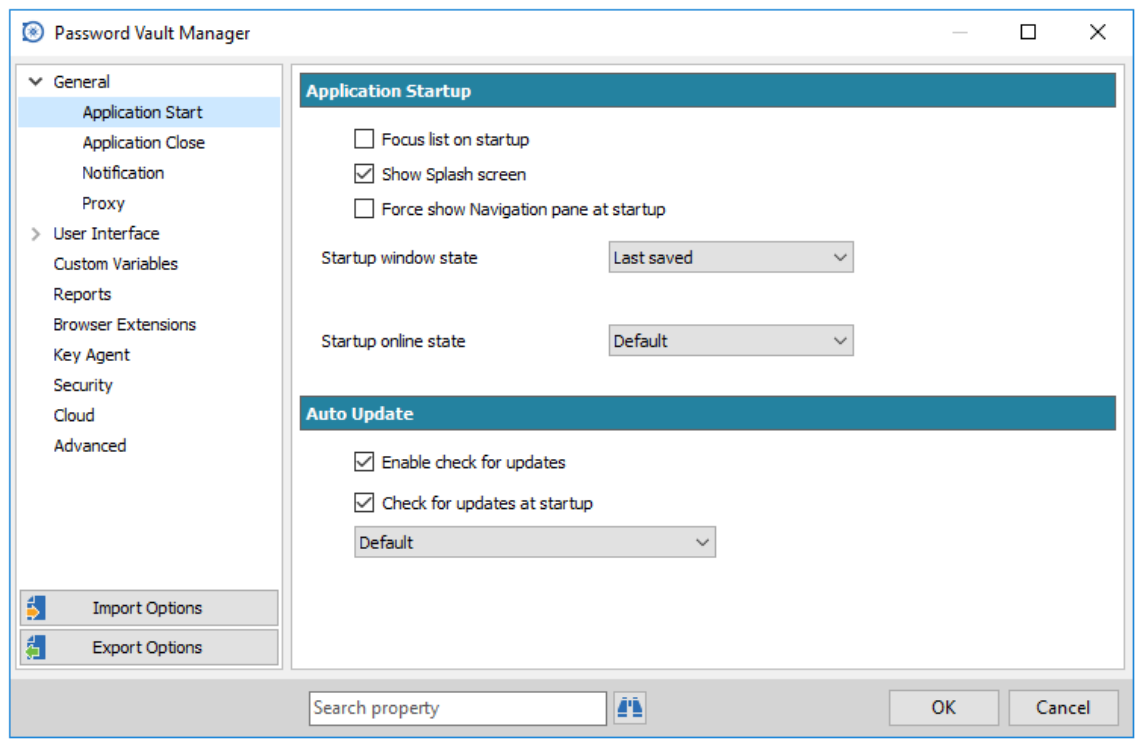
MRU

Option	Description
Most recently used (max)	Indicate the maximum number of items to display in the list view. The maximum MRU limit is of 200 items. See MRU topic for more information on Most Recently Used.

3.1.10.1.1 Application Start

Description

Use the **File - Options - General - Application Start** to control application startup settings.



General - Application Start

Settings

Application startup

Option	Description
Focus list on startup	The focus will be set on the entry list when application starts.
Show Splash screen	Application will display the splash screen on startup.
Force show Navigation pane at startup	The Navigation pane list will be shown on start, even if it was hidden when the application was closed.
Startup window state	Indicate the display of the windows state at startup: <ul style="list-style-type: none"> • Last saved • Minimized • Maximized
Startup online state	Select your startup online state between: <ul style="list-style-type: none"> • Default: By default Password Vault Manager will open in online mode. • Automatically go offline: Automatically go in offline mode at startup

Auto update

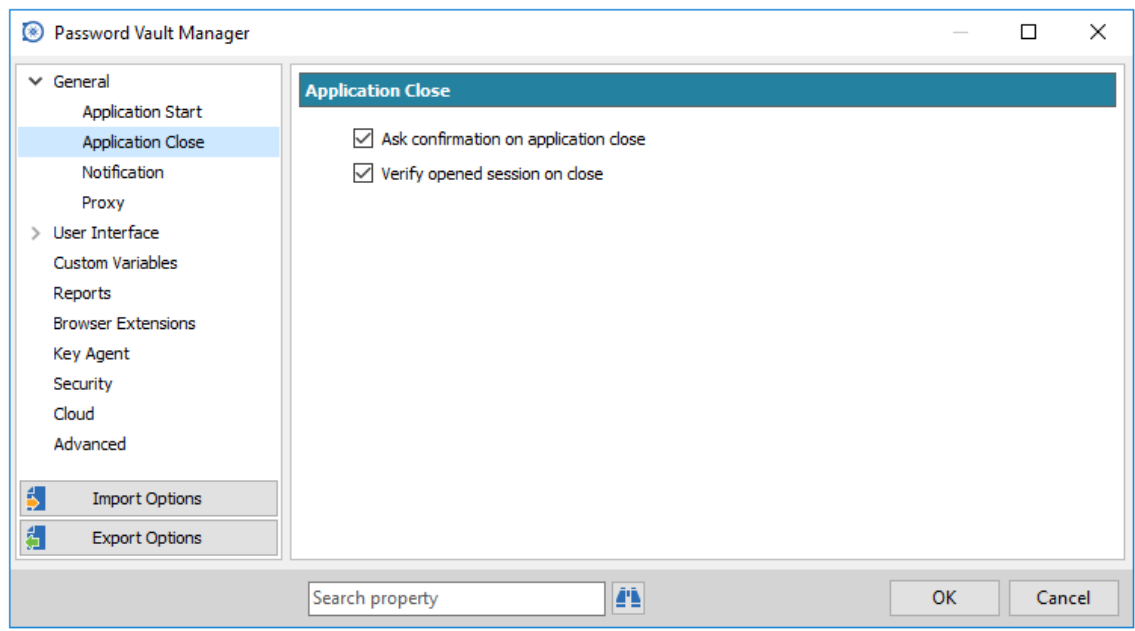
Option	Description
Enable check for updates	Enable the automatic update verification for the whole data source.

Check for update at startup	Application will perform a verification for new releases availability.
Default	Default setting, currently equals to All (Major and Minor Updates) .
Important Updates Only (Major)	Application will only update the important new releases. (9.2, 10.6, 11.0, 11.1)
All (Major and Minor Updates)	Application will update to all new releases. Usually occurs once per month (11.0.7, 11.0.15, etc)
All Updates Including Beta	Application will update to all new releases, including ones tagged as Beta .

3.1.10.1.2 Application Close

Description

Use the **File - Options - General - Application Close** to control the application close settings.



General - Application Close

Settings

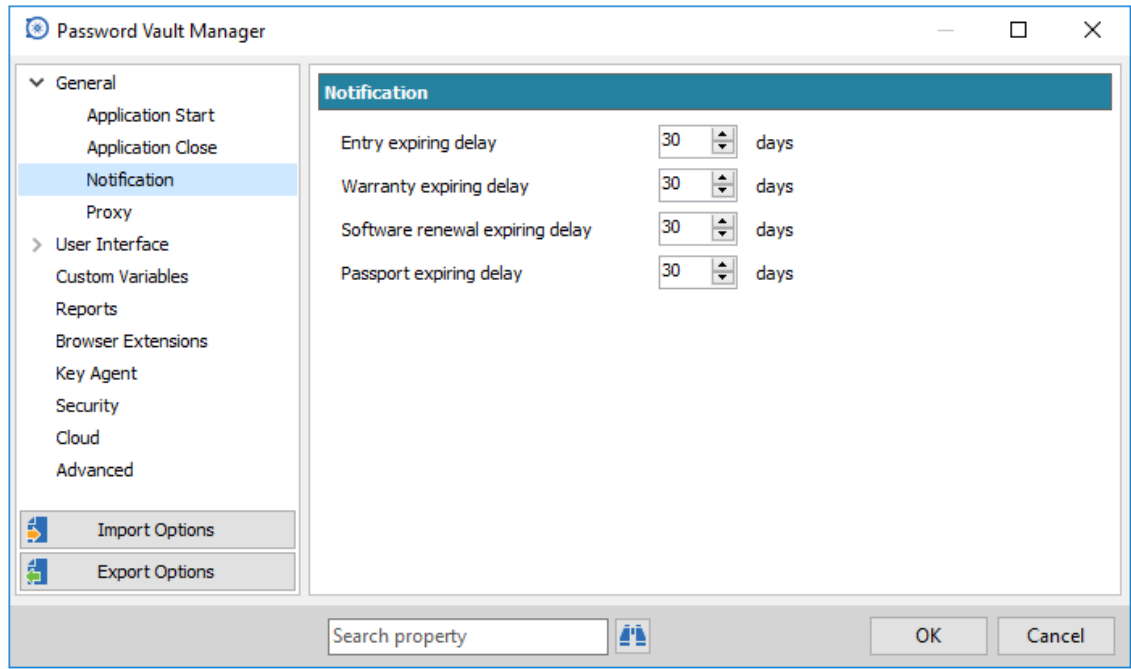
Application Close

Option	Description
Ask confirmation on application close	Application will prompt you for confirmation when attempting to close Password Vault Manager.
Verify opened session on close	Application will warn you about running sessions when attempting to close it.

3.1.10.1.3 Notification

Description

Use the **File - Options - General - Notification** to control application notification settings.



General - Notification

Settings

Notification

Option	Description
Entry expiring delay	Set the number of days to receive a notification before an entry expires.
Warranty expiring delay	Set the number of days to receive a notification before a warranty expires.
Software renewal expiring delay	Set the number of days to receive a notification to renew a software.
Passport expiring delay	Set the number of days to receive a notification before your passport expires.

3.1.10.1.4 Proxy

Description

Use the **File - Options - General - Proxy** to control application proxy settings.

Proxy Configuration

Settings

Proxy

Option	Description
No Proxy	Do not use any proxy.
Bypass proxy server for local addresses	For local addresses, the proxy server will not be used.
System Default	Use the system default proxy.
Custom	Use a custom proxy by selecting the address and port. It's possible to build a list of exceptions with this option.

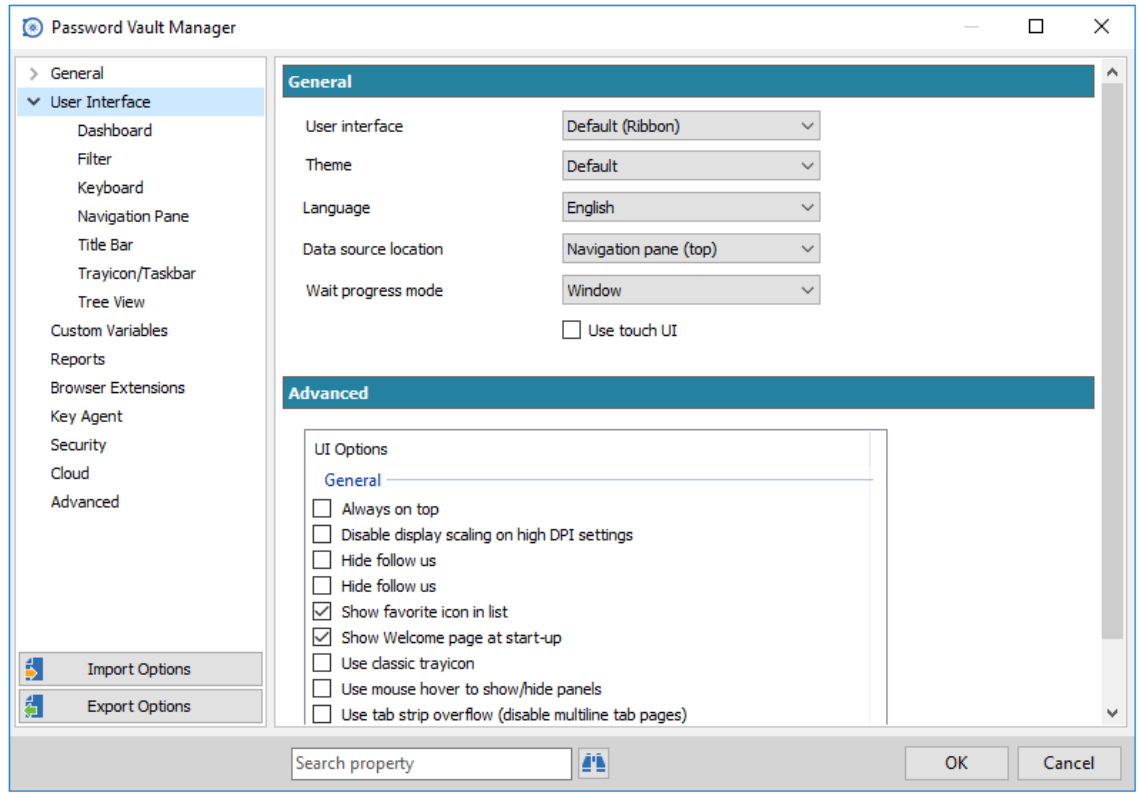
Credentials

Option	Description
Use specific credentials	Use specific credentials when custom is selected.

3.1.10.2 User Interface

Description

Use the **File - Options - User Interface** to customize the display of the Password Vault Manager User Interface.



Options - User Interface

Settings

General

Options	Description
User Interface	Indicate the user interface mode: <ul style="list-style-type: none"> • Default (Ribbon) • Default (Menu)
Theme	Select between different theme for the user interface: <ul style="list-style-type: none"> • Default • Legacy • Office 2013 • Office 2016 • Office 2016 (Dark)
Language	Select your preferred language for the user interface.
Data source location	Select the position of your data source selection drop down: <ul style="list-style-type: none"> • Status bar

	<ul style="list-style-type: none"> • Navigation Pane (top) • Navigation Pane (bottom) • None
Wait progress mode	Display the wait progress information in a Window or Status bar. You can disable the wait progress by selecting None.
Use touch UI	Password Vault Manager will be display and can be use with a touch User Interface.



The Data Source Location **None** setting is not supported in the Classic UI mode.

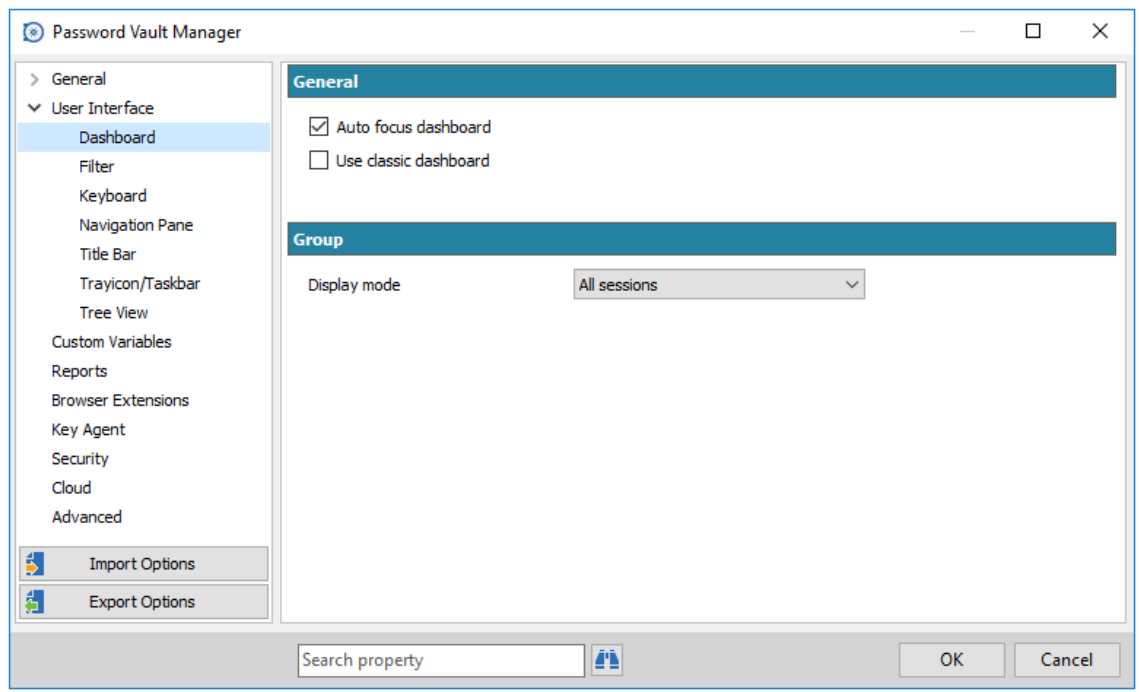
Advanced

Option	Description
Always on top	Keeps the application on top of all others.
Disable display scaling on high DPI settings	Disable scaling on high DPI in Password Vault Manager
Hide follow us	Hide the Follow Us section in the Help menu (Help - Follow Us).
Show favorite icon in list	Favorite icon is overlaid on your session icon.
Show welcome page at start up	Show the welcome page when opening Password Vault Manager.
Use classic tray icon	Use the classic trayicon even if chosen the Ribbon or Menu User Interface.
Use mouse hover to show/hide panels	Use the mouse to show panel when hovering over it.
Use tab strip overflow (disable multiline tab pages)	When there are too many active tabs for the width of the application, having this option checked will result in a new line of tabs to appear. If unchecked then arrows will appear to indicate more tabs are present.

3.1.10.2.1 Dashboard

Description

Use the **File - Options - User Interface - Dashboard** to control how the application displays sessions in the Dashboard.



User Interface - Dashboard

Settings

General

Option	Description
Auto focus dashboard	When an entry is selected in the tree view, the corresponding dashboard will be displayed and focus will immediately be set on it.
Use classic dashboard	The classic dashboard will be displayed instead of the new dashboard with larger buttons.

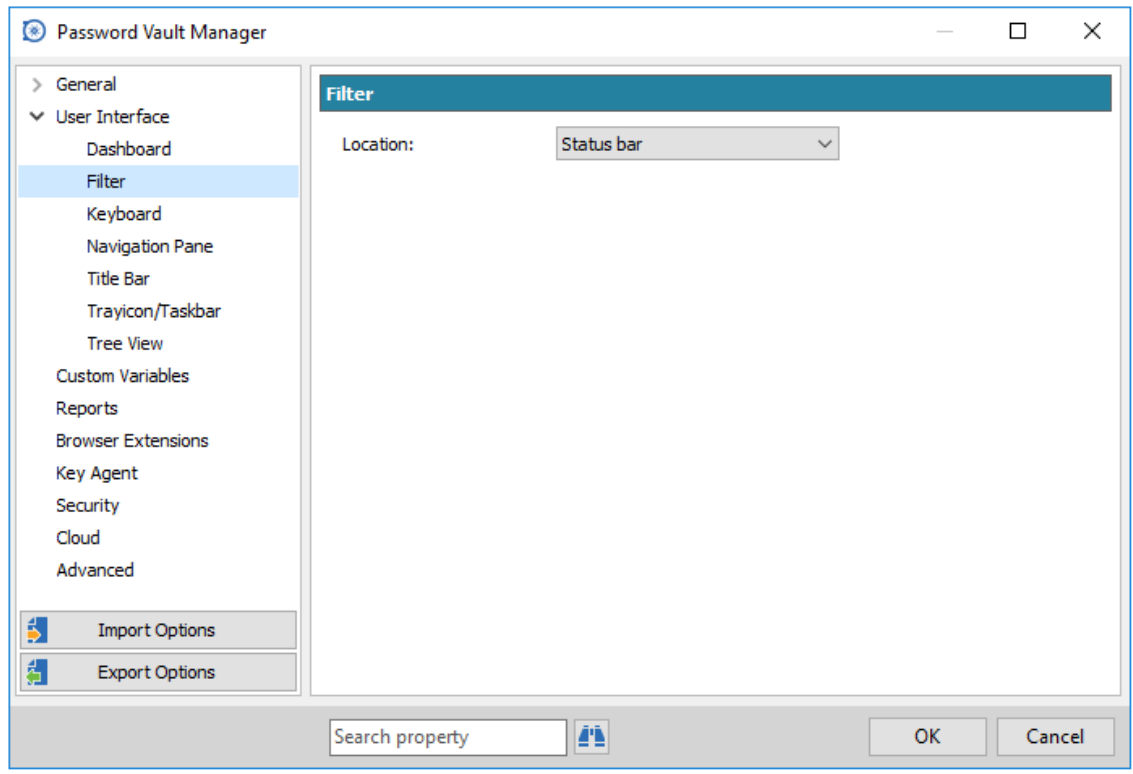
Group

Option	Description
Display mode	Select how the entries are displayed in the group dashboard. Choose between: <ul style="list-style-type: none"> • First level only: only the entries and the groups located directly in the selected group are listed. • All sessions: all the entries are listed including those contained in the sub-folders. • Default (all if not more than...): All entries will be displayed if not more than the selected number when the Default option is active.

3.1.10.2.2 Filter

Description

Use the **File - Options - User Interface - Filter** to control application filter box and settings. See topic [Search/Filter](#) for more information.



User Interface - Filter

Settings

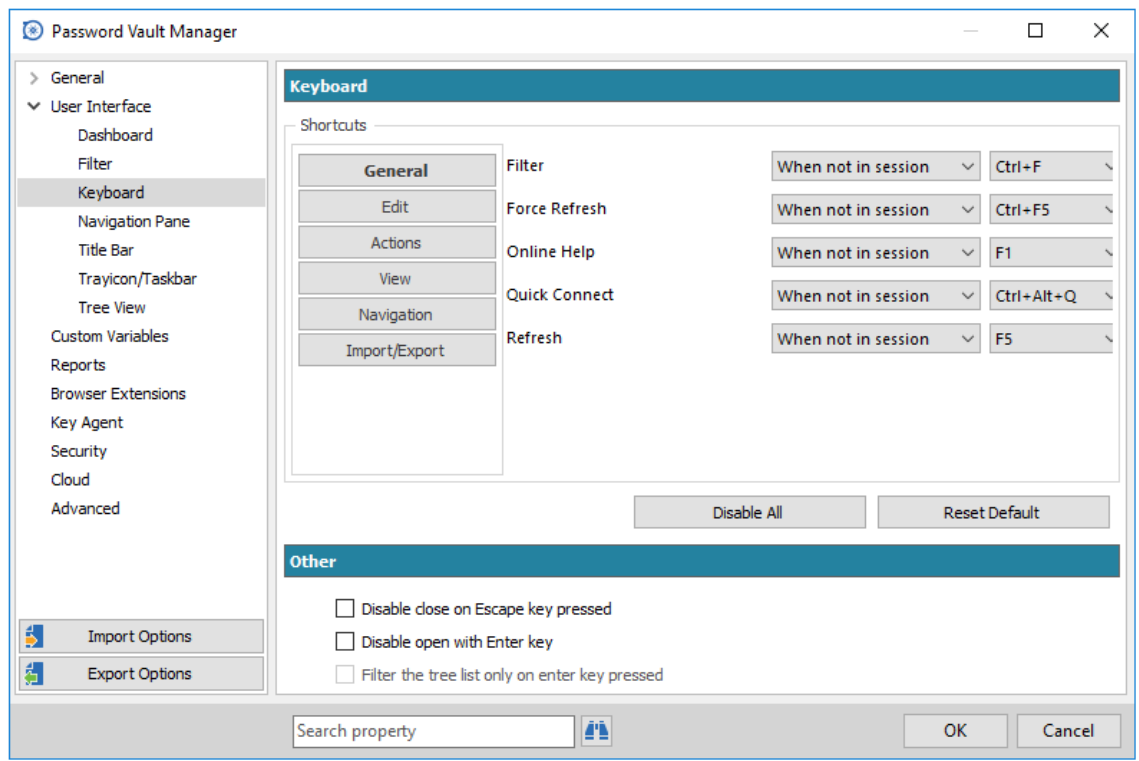
Filter

Option	Description
Location	For the location of the filter box, you can choose between: <ul style="list-style-type: none"> • Status bar • Navigation pane (bottom) • Navigation pane (top) • None When None is selected, a dialog will appear when the shortcut is press.

3.1.10.2.3 Keyboard

Description

Use the **File - Options - User Interface - Keyboard** to control how the application handles keyboard input.



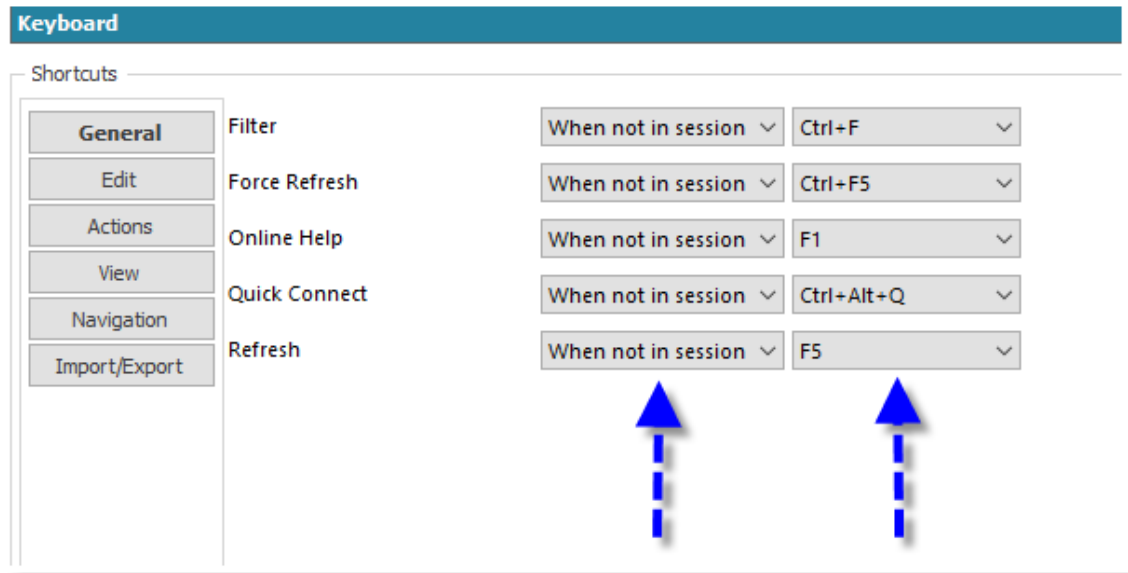
Options - User Interface - Keyboard

Settings

Keyboard

On the left there are different shortcut categories. This lightens the screen and allows you to focus on less shortcuts at the same time.

To configure a keyboard shortcut for an action, two controls are provided.




Keyboard shortcuts

The first drop down is for the scope of the keyboard shortcut.

Option	Description
Default	Use default shortcut keys. Use the magnet in the status bar to disable the shortcut.
When not in session	Use the shortcut keys when the focus is not in a session.
Global hotkey	This create global window hot key. For example, you can use it to execute a macro when Password Vault Manager is not loaded.
None	Select the None item to remove any hot key for the corresponding action.

The second drop down is to determine the shortcut key combination.



Currently no validation is performed as to your usage of the same key combination for two actions.

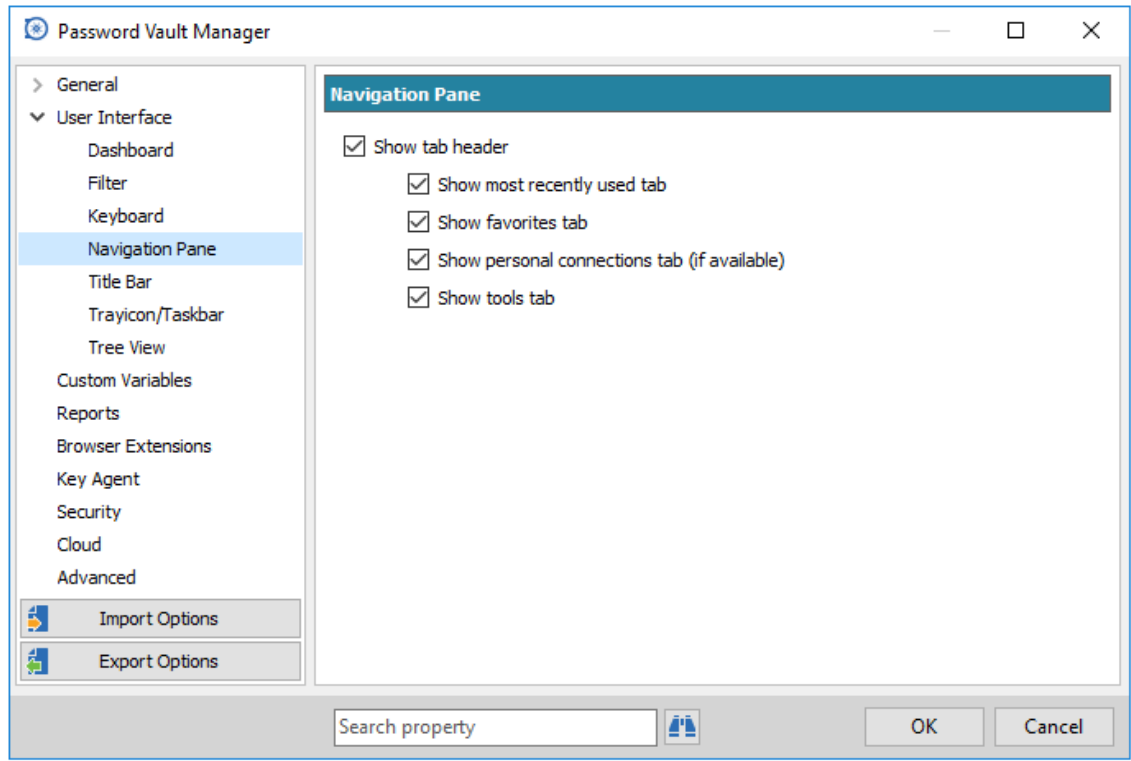
Other

Option	Description
Disable close on Escape key pressed	Pressing the Escape key while in a running session will not close it.
Disable open with Enter key	Pressing the Enter key while an entry is selected will not open it.
Filter the tree list only on enter key pressed	When typing in the tree list filter box, only apply the filter when the Enter key is pressed.

3.1.10.2.4 Navigation Pane

Description

Use the **File - Options - User Interface - Navigation Pane** to control the application Navigation Pane display.



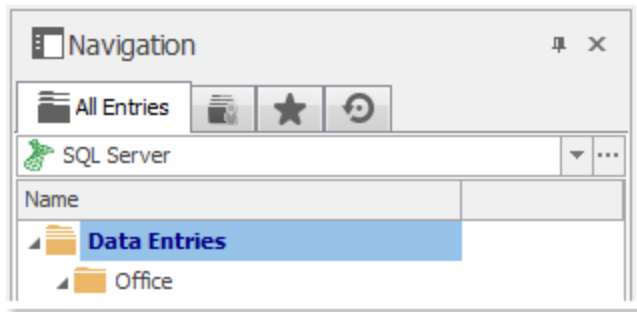
User Interface - Navigation Pane

Settings

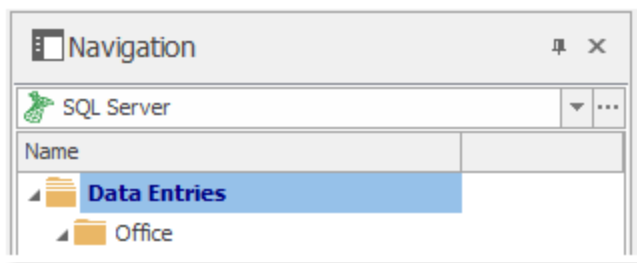
Navigation Pane

Option	Description
Show tab header	Display the tabs header in the Navigation Pane.
Show most recently used tab	Display the Most Recently Used tab in the Navigation Pane.
Show favorites tab	Display the Favorites tab in the Navigation Pane.
Show personal connections tab (if available)	Display the Private Vault tab in the Navigation Pane.
Show tools tab	Display the Tools tab in the Navigation Pane.

With Header



With Header

Without Header

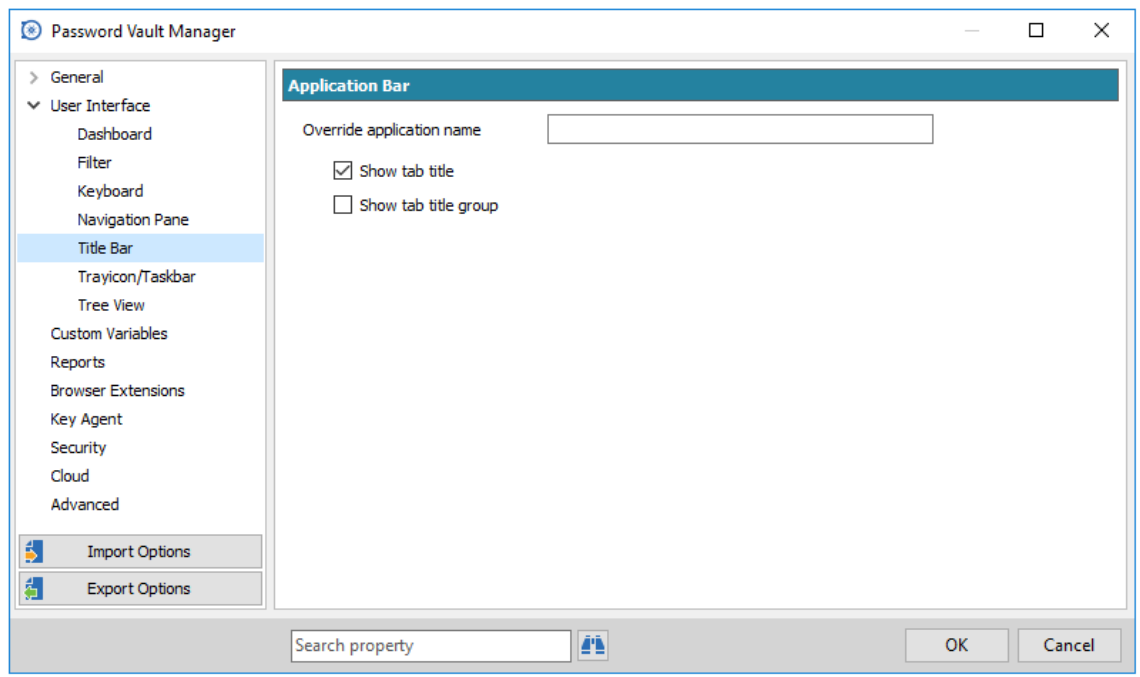
Without Header

You can reset your Navigation Pane to its default settings in Windows - [Reset Layout](#).

3.1.10.2.5 Title Bar

Description

Use the **File - Options - User Interface - Title bar** to control application title bar.



User Interface - Title Bar

Settings

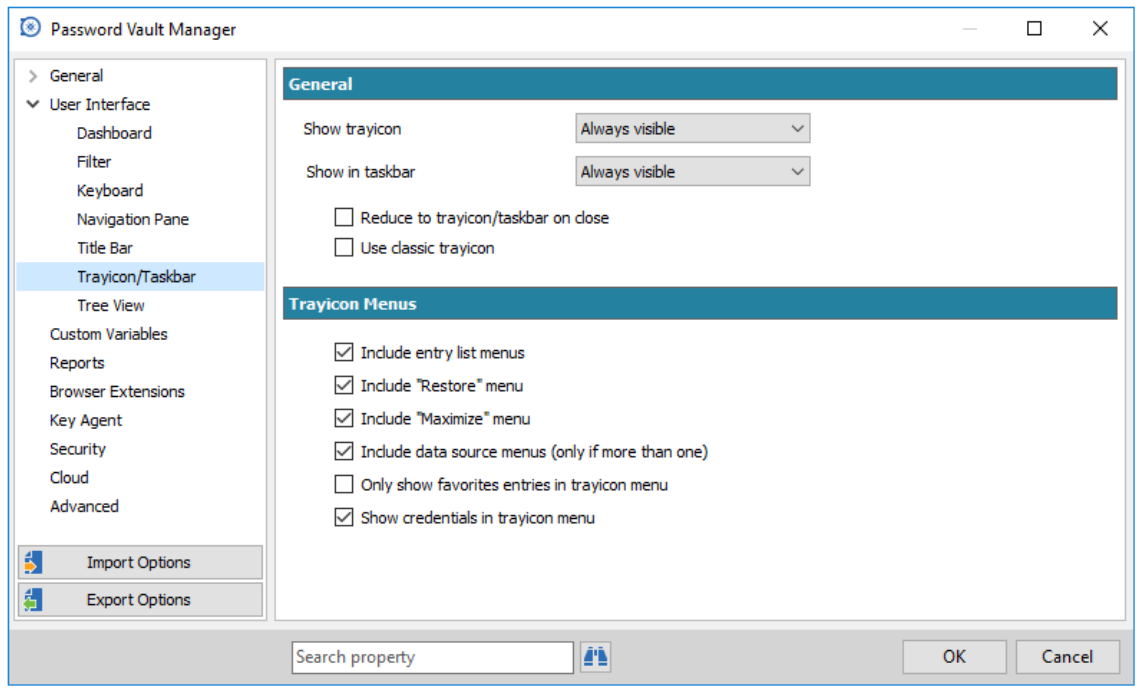
Application bar

Option	Description
Override application name	Display a custom title for the application title bar. Use this setting to get a unique identifier when having multiple instances opened or when using multiple versions side by side.
Show tab title	The application bar will append the caption of the current tab to the name to the title bar.
Show tab title group	This will prefix the tab title name with the session group name. It will also appear in the application title bar.

3.1.10.2.6 Trayicon/Taskbar

Description

Use the **File - Options - User Interface - Trayicon/Taskbar** tab to control the application tray icon and taskbar.



User Interface - Trayicon/Taskbar

Settings

General

Option	Description
Show Tray Icon	Indicates if the Tray Icon is enabled. Select between: <ul style="list-style-type: none"> • When not minimized • Always visible • Never visible
Show in taskbar	Indicates if the application is visible in the Windows taskbar. Select between: <ul style="list-style-type: none"> • When not minimized • Always visible • Never visible
Reduce to trayicon/taskbar on close	Clicking on the X will minimize Password Vault Manager instead of close it.
Use classic trayicon	Use the classic trayicon even if the Ribbon or Menu User Interface has been chosen.

Trayicon Menus

These options control the popup menu of the tray icon.

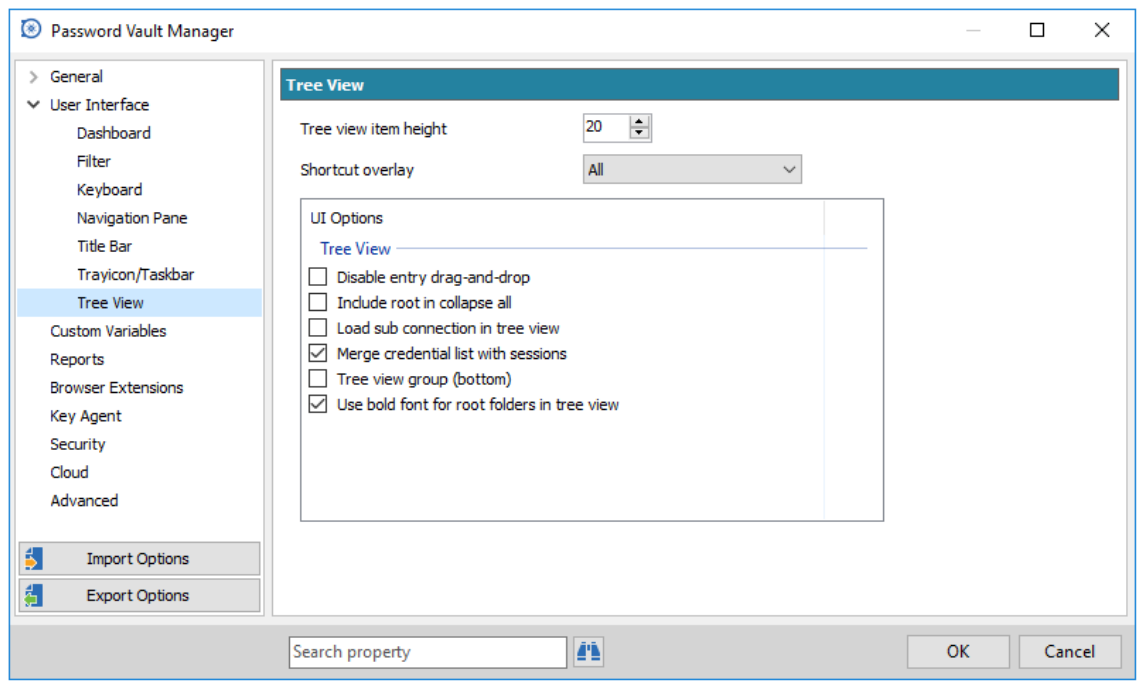
Option	Description
Include entry list menus	Includes the entries in the Tray Icon menu.

Include "Restore" menu	Includes a menu to restore application when it has been minimized.
Include "Maximize" menu	Includes a menu to maximize the application window to take the full area of the screen.
Include data source menus (only if more than one)	Includes a sub-menu for the data sources. This requires more than one data source to function.
Only show favorites entries in trayicon menu	Only the Favorite Entries will appear in the tray icon menu.
Show credentials in trayicon menu	Indicates if the credentials are listed in the tray icon menu.

3.1.10.2.7 Tree View

Description

Use the **File - Options - User Interface - Tree View** to control application tree view.



User Interface - Tree View

Settings

Tree View

Option	Description
Tree view item height	Specify the height of individual items in the Tree view. Valid values are between 16 and 32.
Shortcut overlay	Select on which items the shortcut icon is visible. Choose between: <ul style="list-style-type: none"> • All

- **None**
- **All except original**

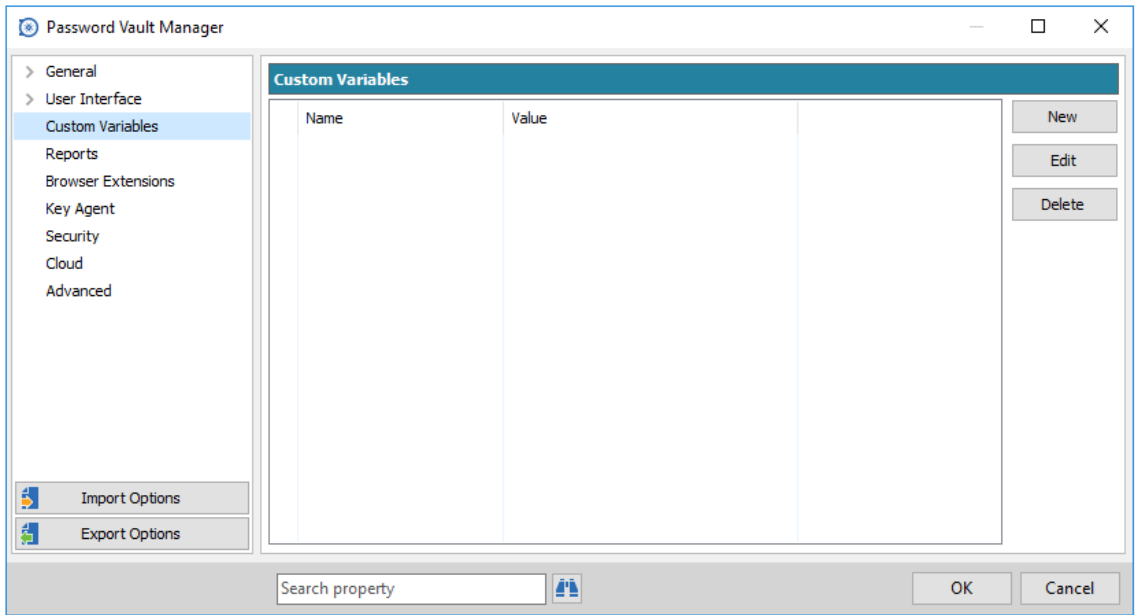
UI Options

Option	Description
Disable entry drag-and-drop	This setting disables moving entries with drag-and-drop. Enable this option to avoid any unwanted session created by drag-and-drop by mistake. If you do use the drag-and-drop a confirmation window will pop up every time making sure the move is wanted.
Include root in collapse all	By default the application has many root nodes in the tree view. i.e. Sessions, Credentials, Macros/Scripts/Tools. Collapsing the tree view will also collapse every root nodes if this option is enabled. Only the children of the current root are affected by the command when this option is not enabled.
Load sub-connection in tree view	Indicate if the sub connections appear under their parent in the tree view. You can use the sub-connection pane if you don't want them listed in the tree.
Merge credential list with sessions	Use this option if you want the credentials to appear within the list of Sessions instead of in their own root.
Tree view group (bottom)	This setting indicates if the Group/Folder entries are at the bottom of the list instead of appearing first under their parent.
Use bold font in tree view	Indicate if the root level items are displayed using the bold attribute.

3.1.10.3 Custom Variables

Description

Use the **File - Options - Custom Variables** to manage your own variable.



Options - Custom Variables

Settings

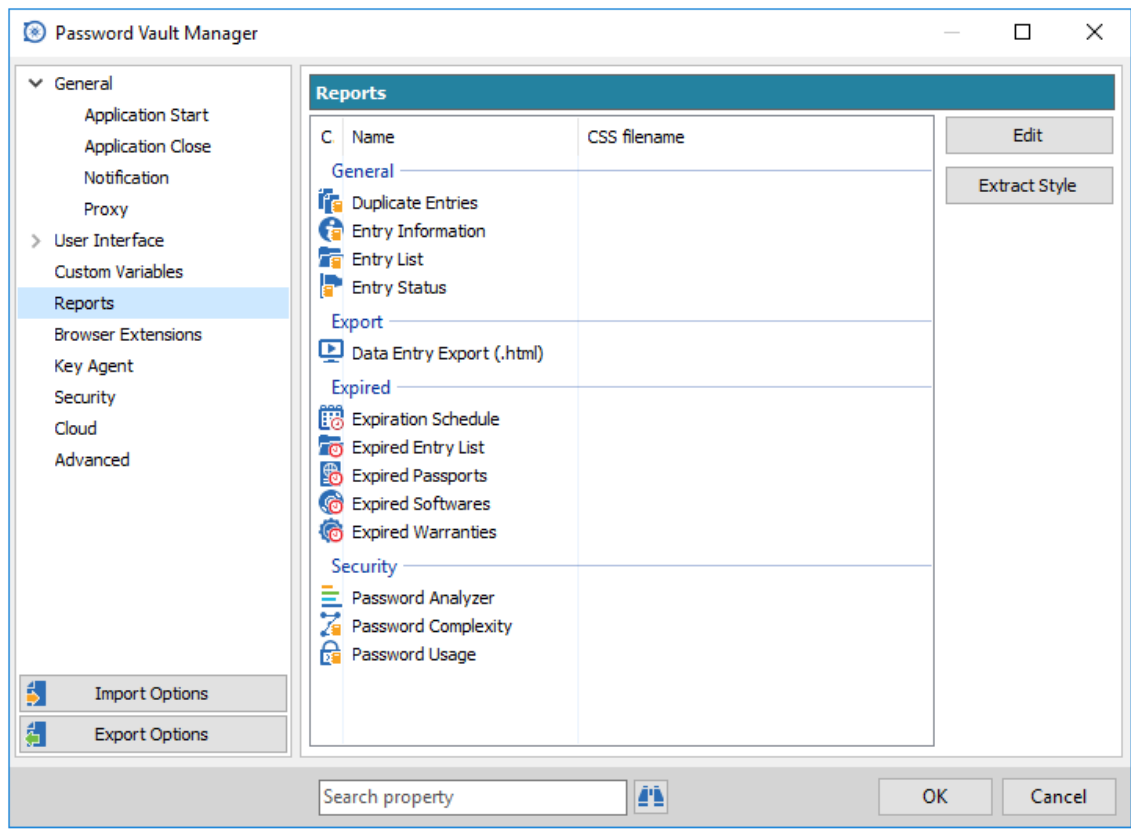
Custom variables

The custom variables option has been implemented to customize your very own variables in the application. Click on **New** to create a new variable.

3.1.10.4 Reports

Description

Use the **File - Options - Reports** to customize the style of your reports.



File - Option - Reports

Settings

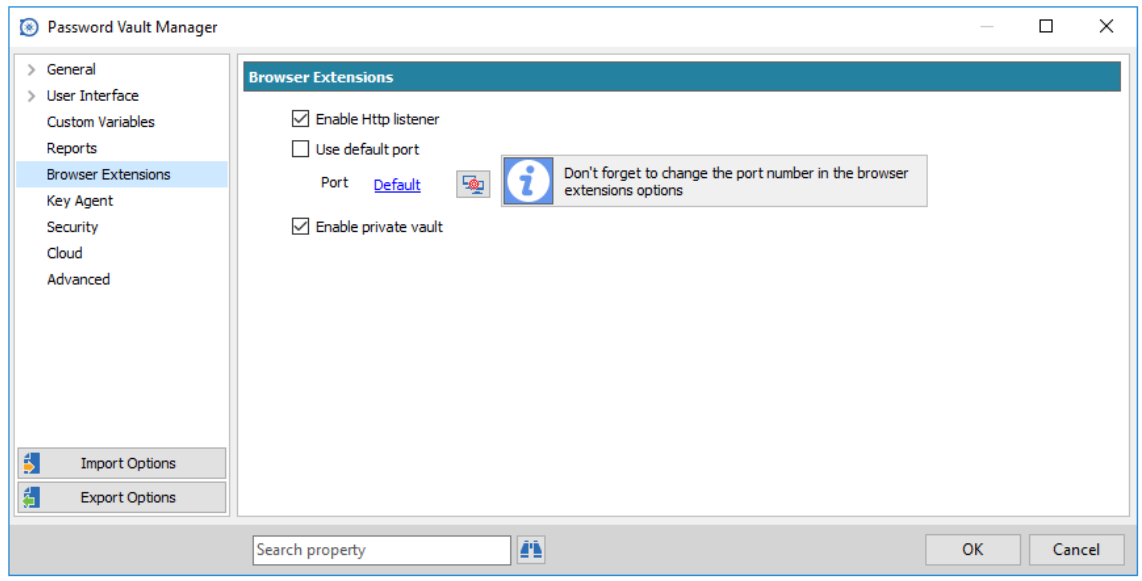
Reports

Option	Description
Edit	Select the proper CSS file to customize the report display. A CSS file is a plain text format that contain all the display settings.
Extract Style	Extract the style of a report in a CSS file.

3.1.10.5 Browser Extensions

Description

Use the **File - Options - Browser Extensions** to control specific settings in the browser extension such as the default port.



Options - Browser Extensions

Settings

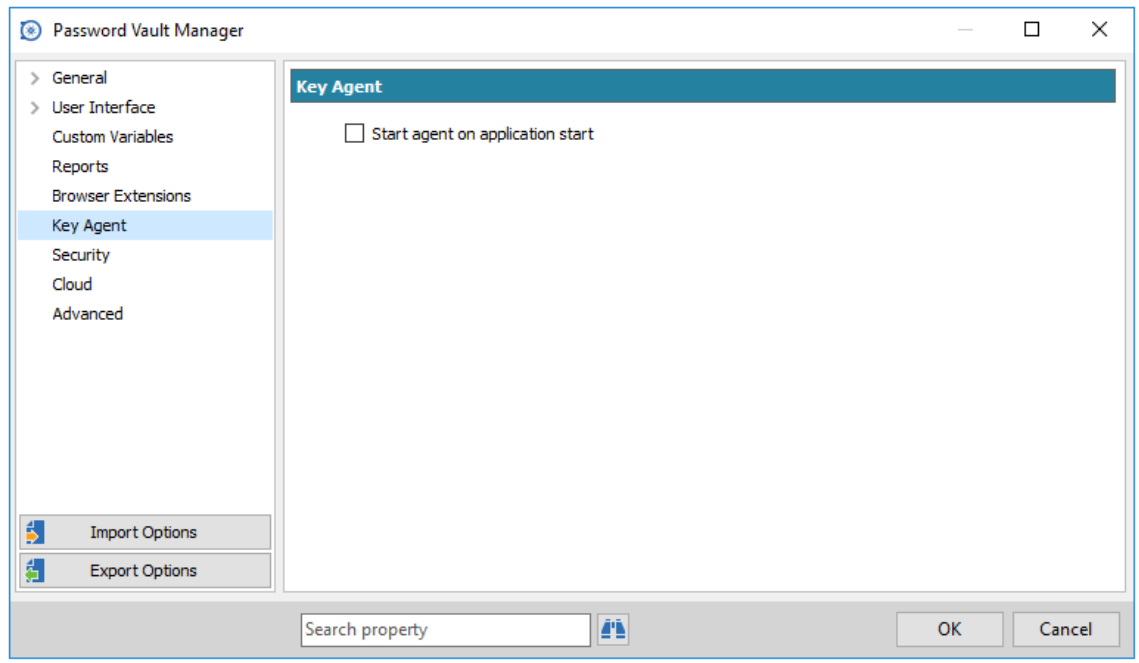
Browser Extensions

Option	Description
Enable Http listener	Enable a programmatically controlled HTTP protocol listener.
Use default port	Indicates the default port that you wish to use in your browser extension. Don't forget to change the port number in the browser extensions options.
Enable private vault	Enable the browser extensions to be use with the Private Vault..

3.1.10.6 Key Agent

Description

The Key Agent is used to hold all your SSH Keys in memory already decoded and ready for them to be used. Fore more information see [Key Agent Manager](#).



Options - Key Agent

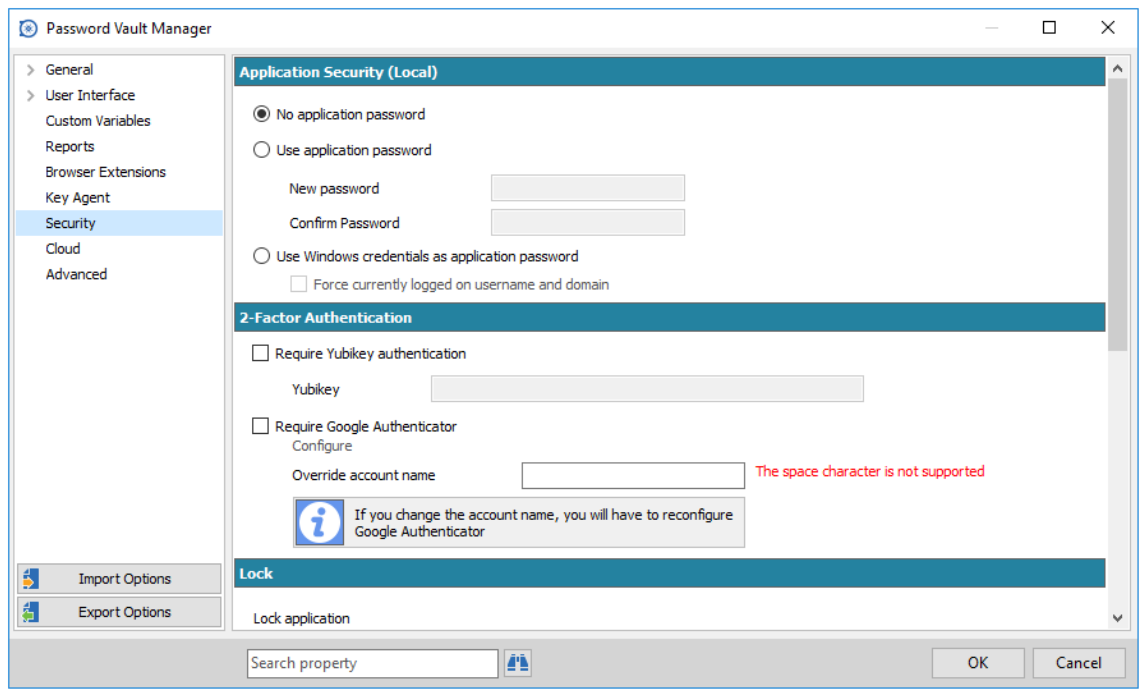
Settings

Option	Description
Start agent on application start	Automatically start the Key Agent when opening Remote Desktop Manager.

3.1.10.7 Security

Description

Use the **File - Options - Security** to configure the security settings of Password Vault Manager.



Options - Security

Settings

Application security (local)

Option	Description
No application password	The application will have no security enabled. However it's recommended to use the default Windows lock workstation feature.
Use application password	Enable the application level security and define a specific password to access the application.
Use Windows credentials as application password	Enable the application level security and use the same password as your Windows password. The application needs an access to the domain to authenticate the user.

2-Factor authentication

Option	Description
Require Yubikey authentication	Use a Yubikey device to get access to the application when opening it or when it's locked.
Require Google Authenticator	Use Google Authenticator to get access to the application when opening it or when it's locked.

Consult the [Yubikey](#) authentication topic or the [Google Authenticator](#) topic to learn how to configure a [2-Factor Authentication](#).

Lock

Option	Description
Lock application when minimized	Lock application when minimized in the taskbar.
Lock on idle	Automatically lock the application when it's not used after a determined number of time. The value is in minute.

Offline security

This section contains the global offline security settings.

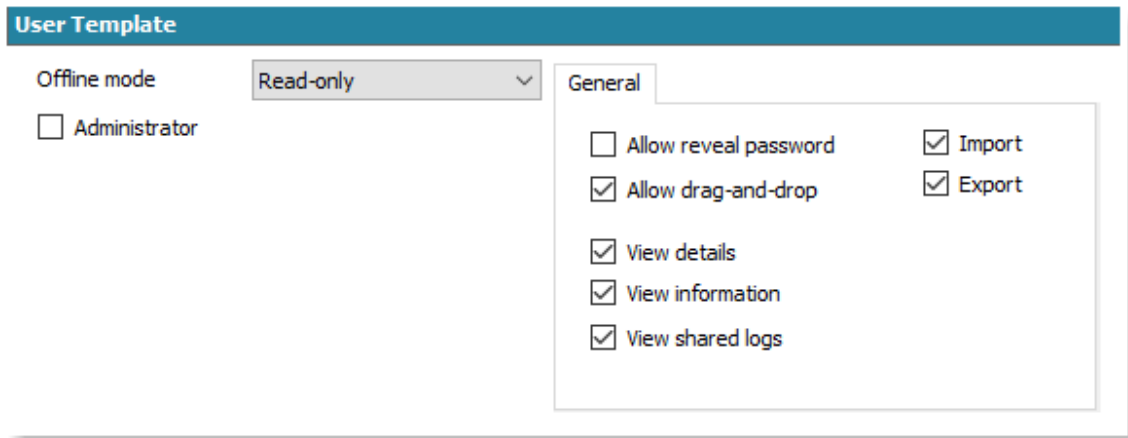
Security - Offline Security

Option	Description
Default security	The application uses an offline file that is encrypted with a non-portable computed key hash.
Enhanced security	The application uses an offline file that is encrypted with a hash of the non-portable computed key plus user specific password. This password is saved internally by default.
Prompt for offline access	Selecting this option forces the user to enter the password prior to accessing the offline data.

User Template

This section contains the default values used when a new user is created in a data source. It is used as a template to simplify the batch creation process.

See the [User Permissions](#) section for more details about the different fields.

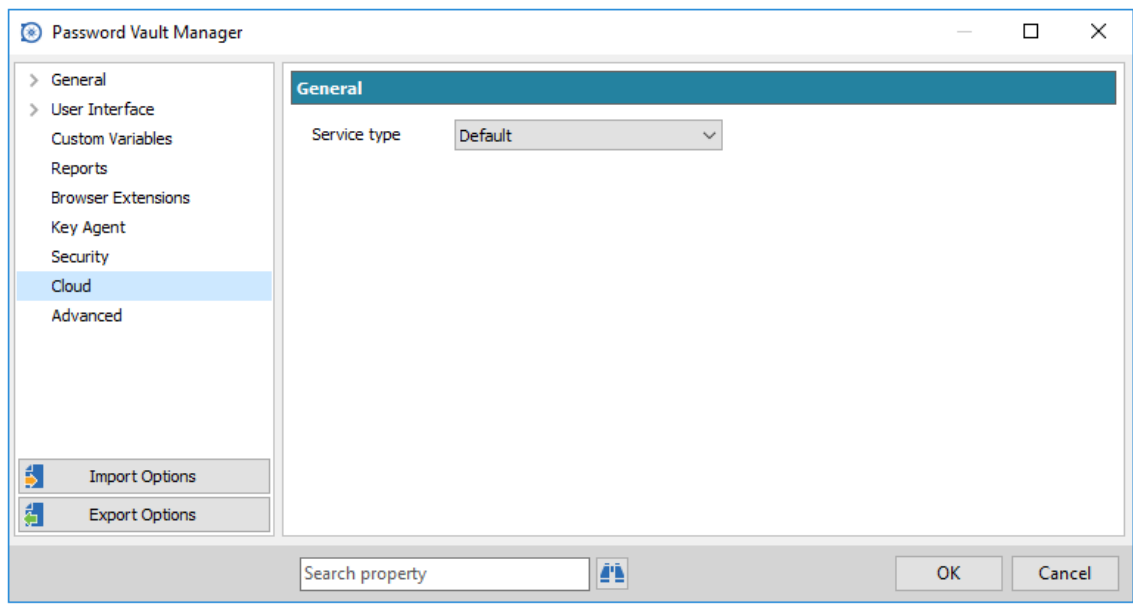


Security - User Template

3.1.10.8 Cloud

Description

Use **File - Options - Cloud** to define your Service type for your Devolutions Online Database data source.



Options Cloud

Settings

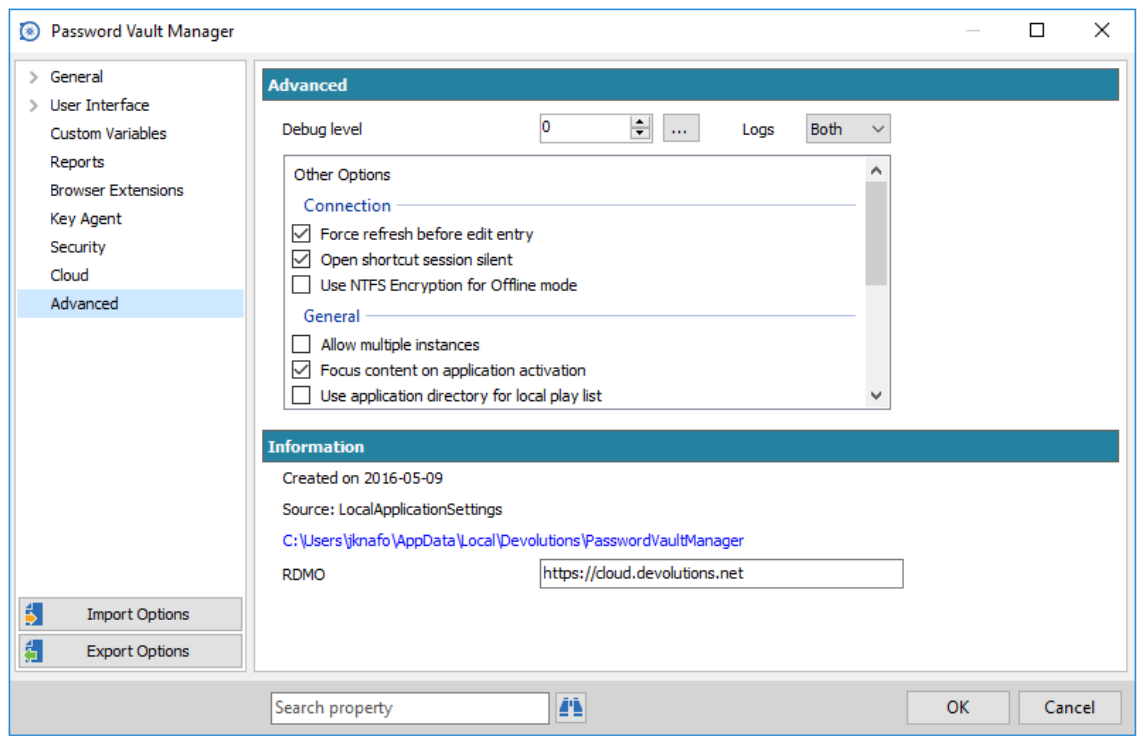
Option	Description
Service type	Select your service type for your Devolutions Online Database between:

- **Default.** The Default setting is the application default setting, at the moment the default is Web Service Client but will shortly be changed to Web API Client.
- **Web API Client**
- **Web Service Client**

3.1.10.9 Advanced

Description

Use the **File - Options - Advanced** tab to control application behavior as it pertains to low level settings.



Options - Advanced

Settings

Advanced

Option	Description
Debug level	Set the level of debugging information that Password Vault Manager captures. This should only be modified when requested from a Devolutions support technician as it might slow down your system.
Logs	The logs can be saved in a file or in a database file. Select between: <ul style="list-style-type: none"> • Both: Logs will be saved in a text file and in a database file. • Database: Logs will be saved in a file named RemoteDesktopManager.log.db. The file is located in the installation folder of the application.

- **File:** Logs will be saved in a file named RemoteDesktopManager.log. The file is located in the installation folder of the application.

Other Options - Connections

Option	Description
Force refresh before edit entry	This will perform a refresh of the entry just before entering in edit mode. This is useful in a multi-user environment with a shared data source. This ensure that you are editing the most recent version of the entry.
Open shortcut session silent	Disable the command line warning message when using a shortcut.
Use NTFS Encryption for Offline mode	When using Offline Mode, a local file is created to hold a copy of the data source. If this is enabled the local file is encrypted using the built-in NTFS encryption of Windows. This setting may cause delays when accessing the data source because the local file is refreshed on every access.

Other Options - General

Option	Description
Allow multiple instances	Allows more than one instance of Password Vault Manager to run concurrently. This is not recommended.
Focus content on application activation	This will set focus on the last embedded session when the application is activated.
Use application directory for local play list	Use the installation folder to save the local play list that has been created.
Use application directory for offline cache	Use the installation folder to save the offline cache file.

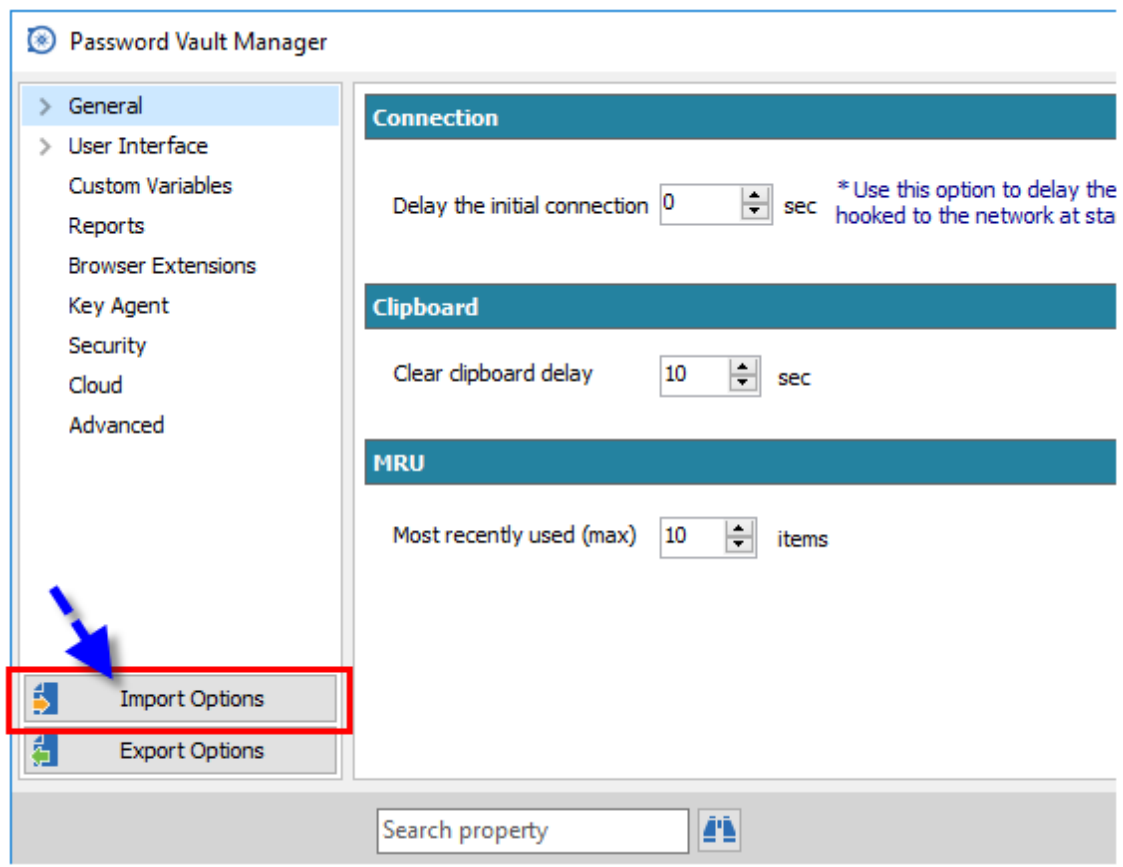
Other Options - UI Options

Option	Description
Always show "Go Offline" button	It will always display the "Go Offline" button in the status bar when using the Offline Mode .
Disable custom images	Disable the loading of any custom images in the tree view. Too many custom images could dramatically increase the size of the data source thus increasing the load time.
Hide version label	Hide the version label of Password Vault Manager.
Use old entry sort	Use the old entry sort from previous version of Password Vault Manager.

3.1.10.10 Import Options

Description

Use **File - Options - Import Options** to import your application configuration file.

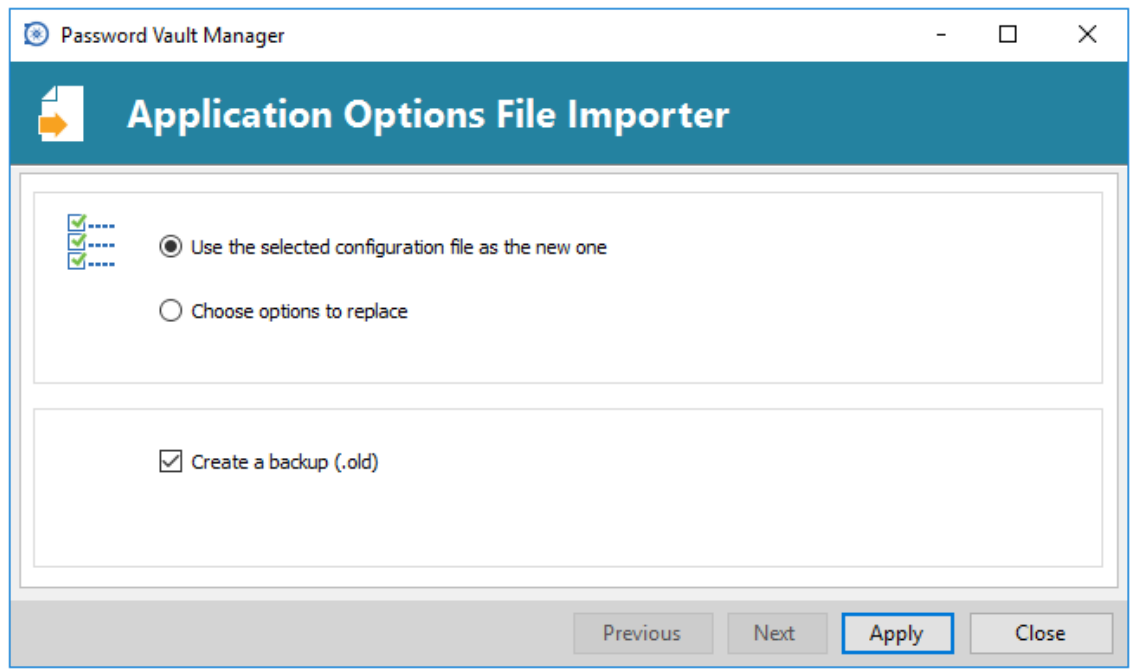


Import Options

Settings

Select the [Configuration File](#) to import in Password Vault Manager and click on Open.

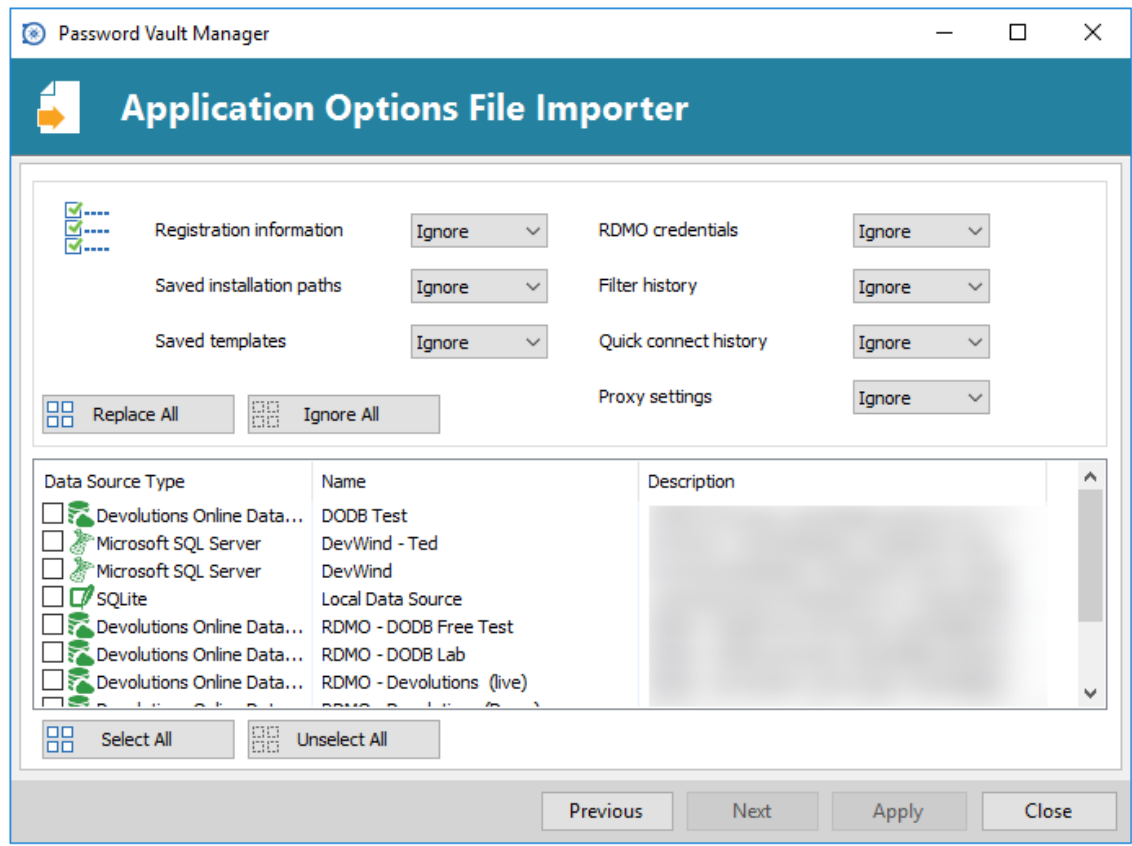
Remote Desktop Manager options file importer



Application Options File Importer

Option	Description
Use the selected configuration file as the new one	Use the PasswordVaultManager.cfg file as the new configuration file for your application.
Choose option to replace	Select which options to replace in your actual PasswordVaultManager.cfg file. See below for more information.
Create a backup (.old)	Create a backup of your old PasswordVaultManager.cfg.

Choose options to replace



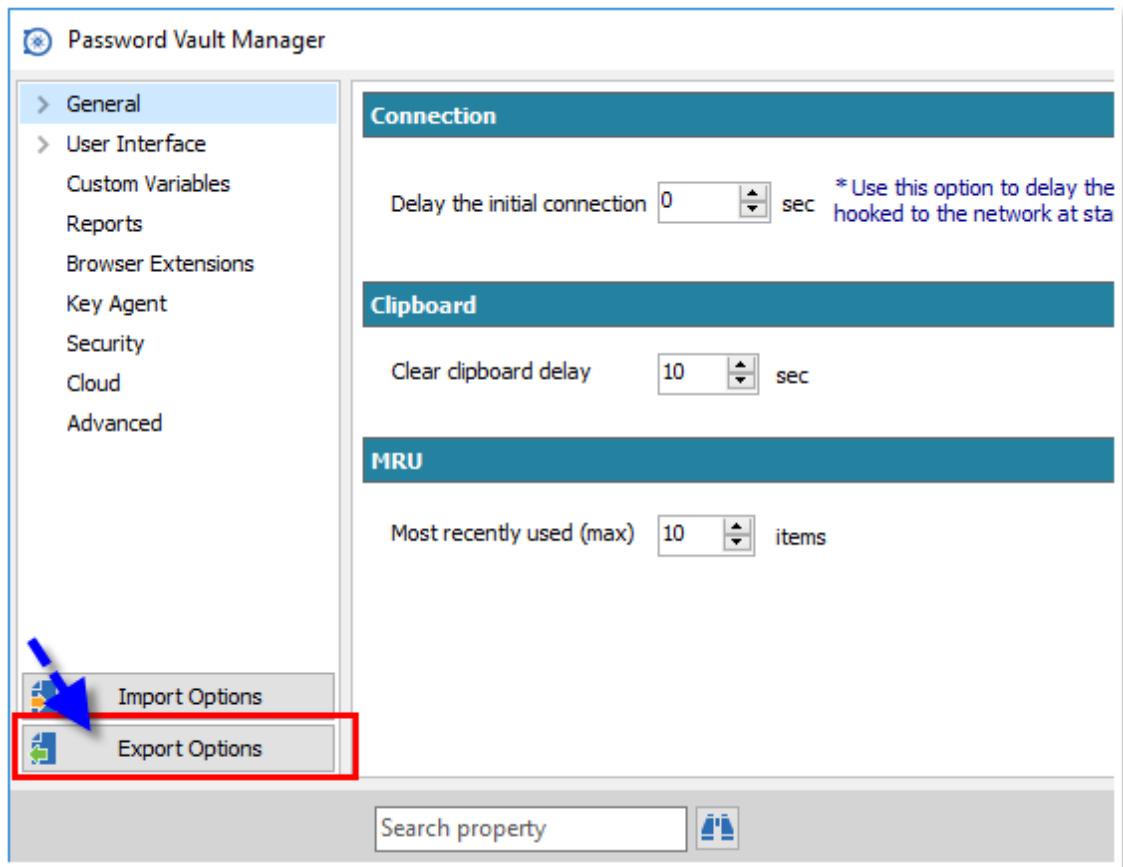
Application Options File Importer

Decide which options to replace with the one from PasswordVaultManager.cfg that you wish to import. Select **Replace** to replace an existing setting with a new one or select **Ignore** if you want to keep the setting that you already have.


3.1.10.11 Export Options

Description

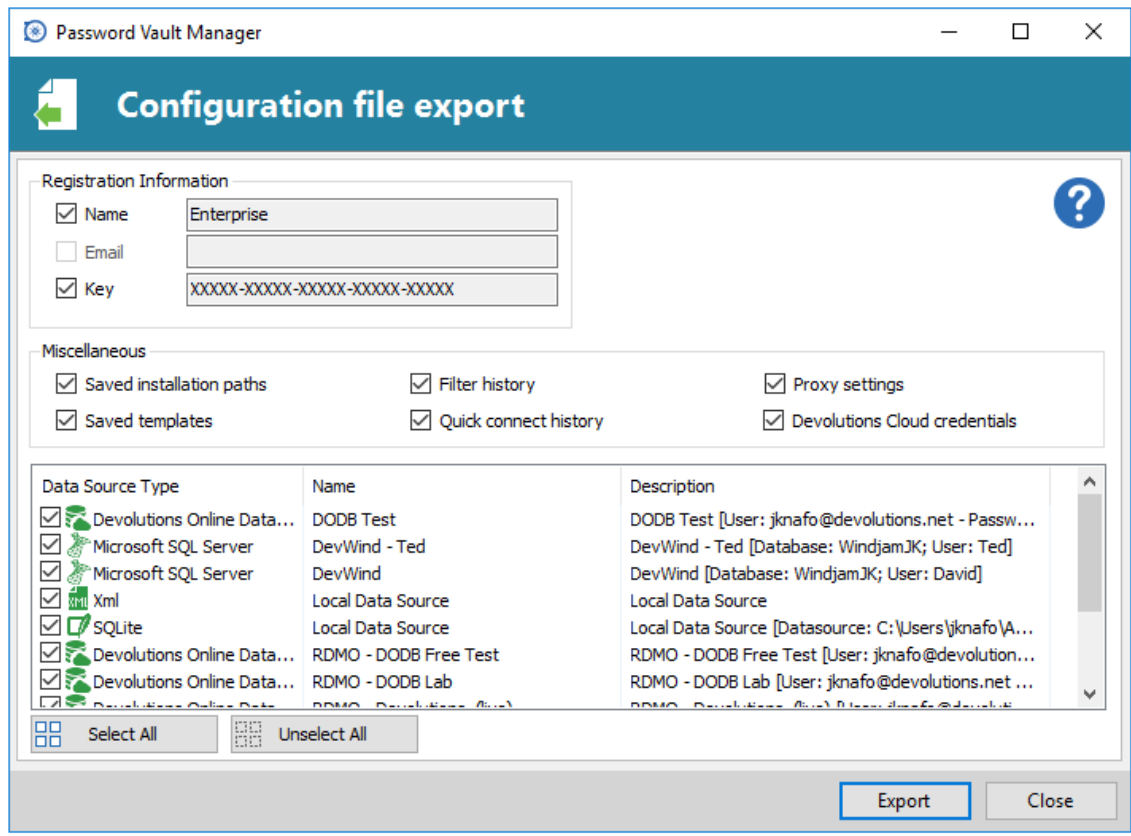
Use **File - Options - Export Options** to control the options to export from your application's configuration. Use this to easily transfer settings to another machine.



Export Options

 Sharing the exported file with a colleague would effectively give that person whatever credentials you have set in your data source definitions, including credentials set in your Devolutions Cloud. **Devolutions does not recommend sharing any credential to a team data source.**

Settings



Configure file export

Registration Information

Option	Description
Name	Company registration name
Email	Registration email
Key	Serial license key

Miscellaneous



The local templates may contain credentials, ensure you do not share the exported file.

Option	Description
Saved installation paths	Preserve your installation paths configured for the external application paths
Saved templates	Include your local templates in the export.
Filter history	Preserve your filter history
Quick connect history	Preserve your Quick connect history
Proxy Settings	Includes your proxy settings

Devolutions Cloud credentials	Includes your Devolutions Cloud account credentials.
-------------------------------	--

Data Source Type



The data source configurations you select will be exported with the username/password as they are currently configured. If you are creating a file to quickly set up new employees, you must be careful not to give away your credentials. Using the [Custom Installer Service](#) is recommended for this case.

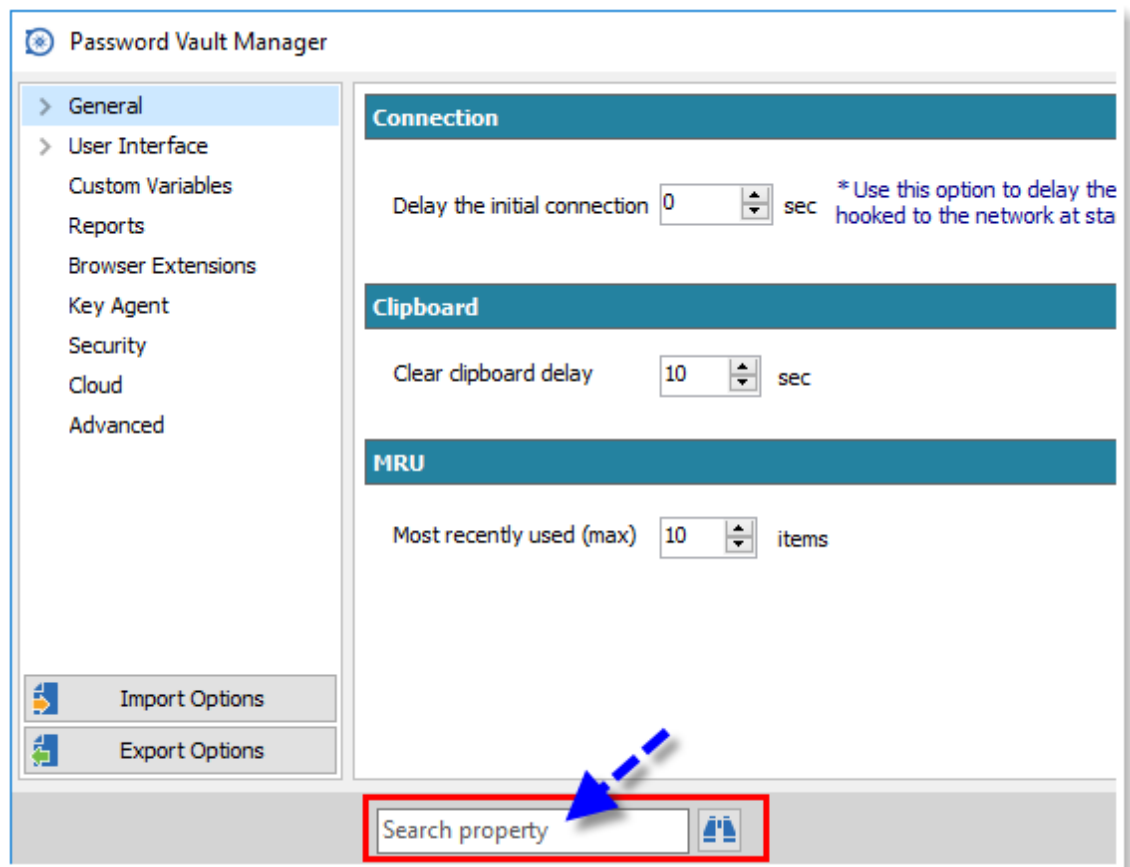
All your configured data sources will be displayed in this section. Select the one(s) that you wish to include in the export. Please note that the content of the data source is not exported.

When your settings are customized to your liking, click on **Export**. You will be prompted to save your settings in a PasswordVaultManager.cfg file.

3.1.10.12 Search Property

Description

Use **File - Options - Search** option property to search any option that you wish to retrieve from the option dialog of Password Vault Manager.



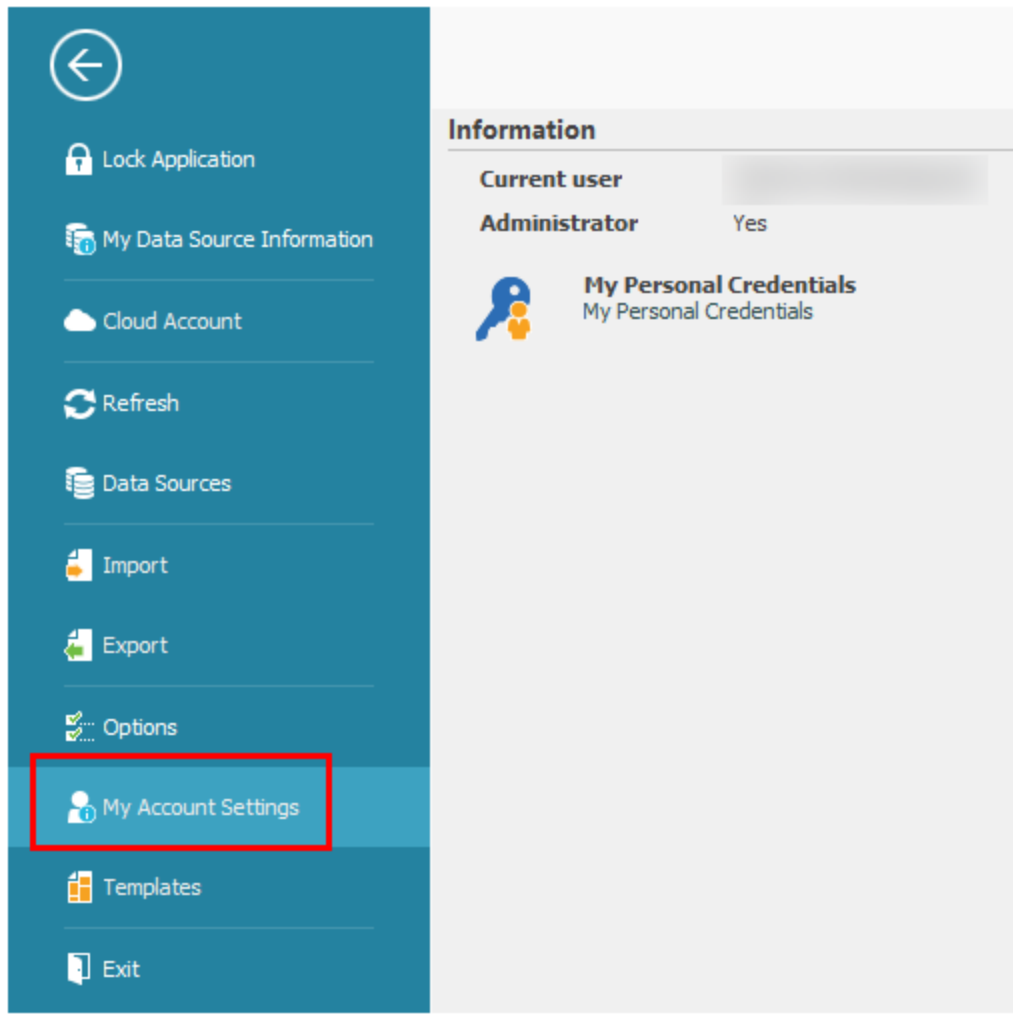
Search Property

3.1.11 My Account Settings

Description

Use **File - My Account Settings** to configure accounts to connect on different web platforms. This allows you to setup your account settings one time and use it in the creation of your entries as many time as you want.

Settings



File - My Account Settings

Information

Option	Description
Current user	Indicates the current user connected to the application.
Administrator	Indicate if the current user is administrator or not.
My Personal Credentials	Please consult My Personal Credentials topic for more information.

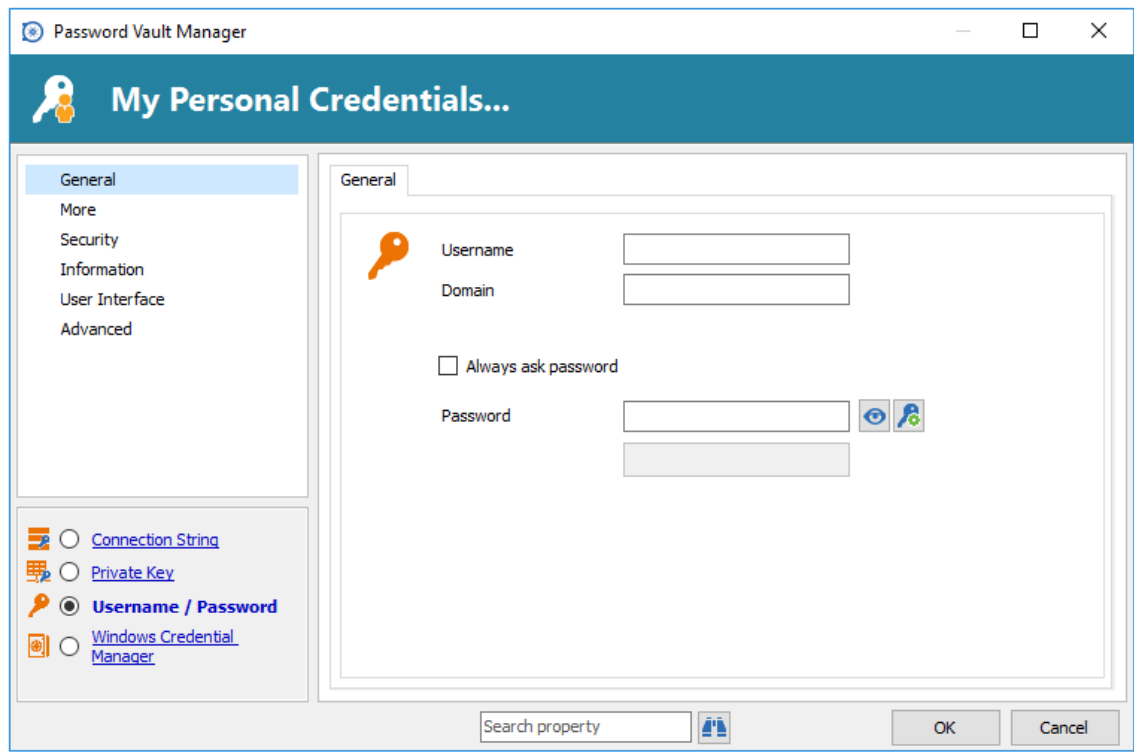
3.1.11.1 My Personal Credentials

Description

The *My Personal Credentials* feature is a single credential entry which is locally stored on your computer in your Windows profile.

It is typically used to hold the Windows credentials for your running sessions because Password Vault Manager can't access them. If you can't use integrated security then you must store your credentials in ***My Personal Credentials***.

This allows you to centralize one special credential to replace or emulate the ones for your Windows session. When a password change is needed you simply need to change it once in ***My Personal Credentials***.



My Personal Credentials...

3.1.12 Templates

Description

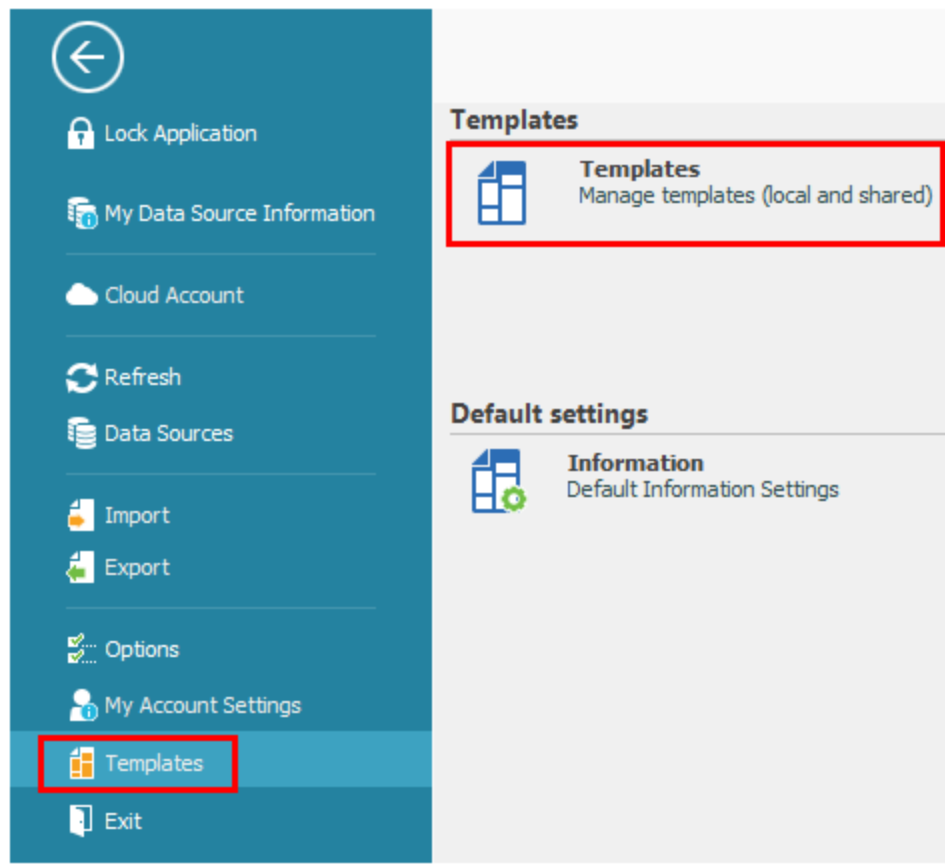
Templates allow you to create predefined configuration available such as:

- Create a new entry
- Quickly connect
- Open as a template
- Create an import wizard

Templates can be useful to have predefined values when creating a specific entry. It's possible to create Local templates and/or Shared templates.

Templates are available in the options dialog or via the menu ***File - Templates - Templates***.

This allows you to create predefined templates available with the quick connect toolbar or when creating or importing a new session.

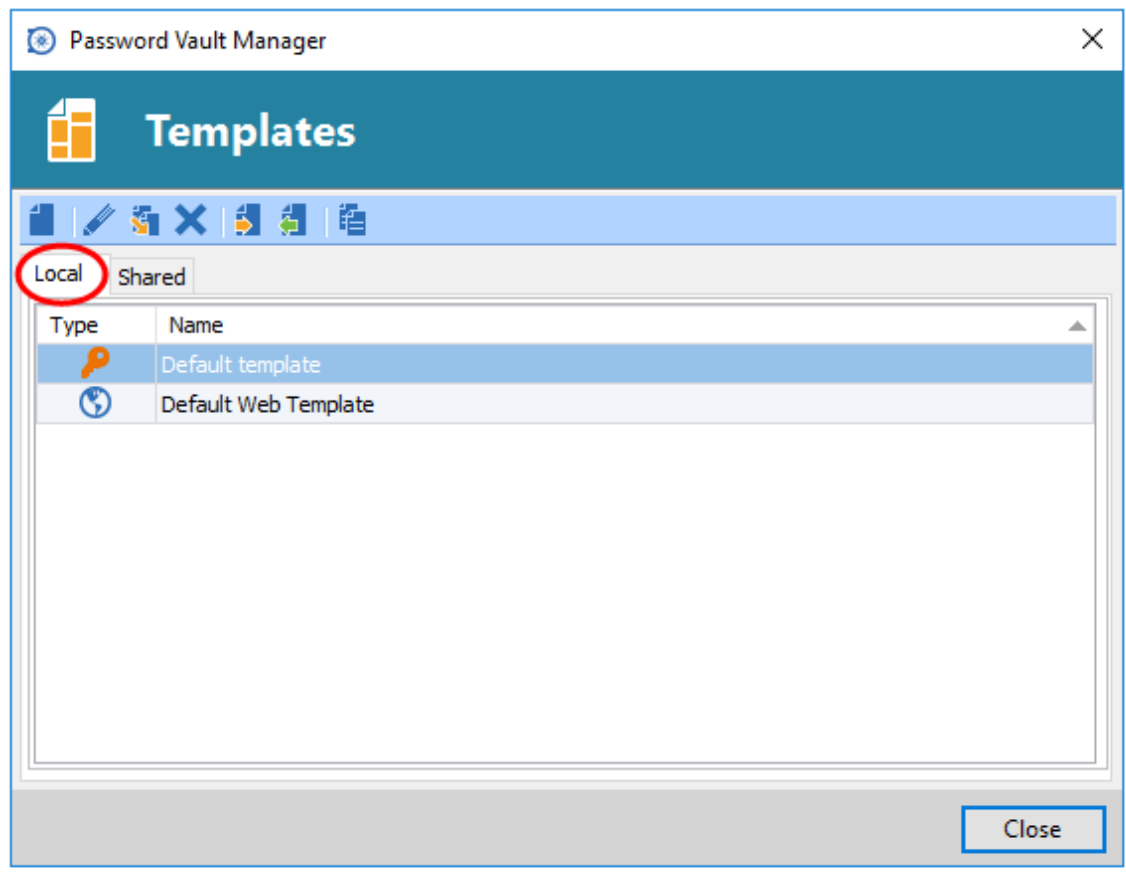


File - Templates

Settings

Local Templates

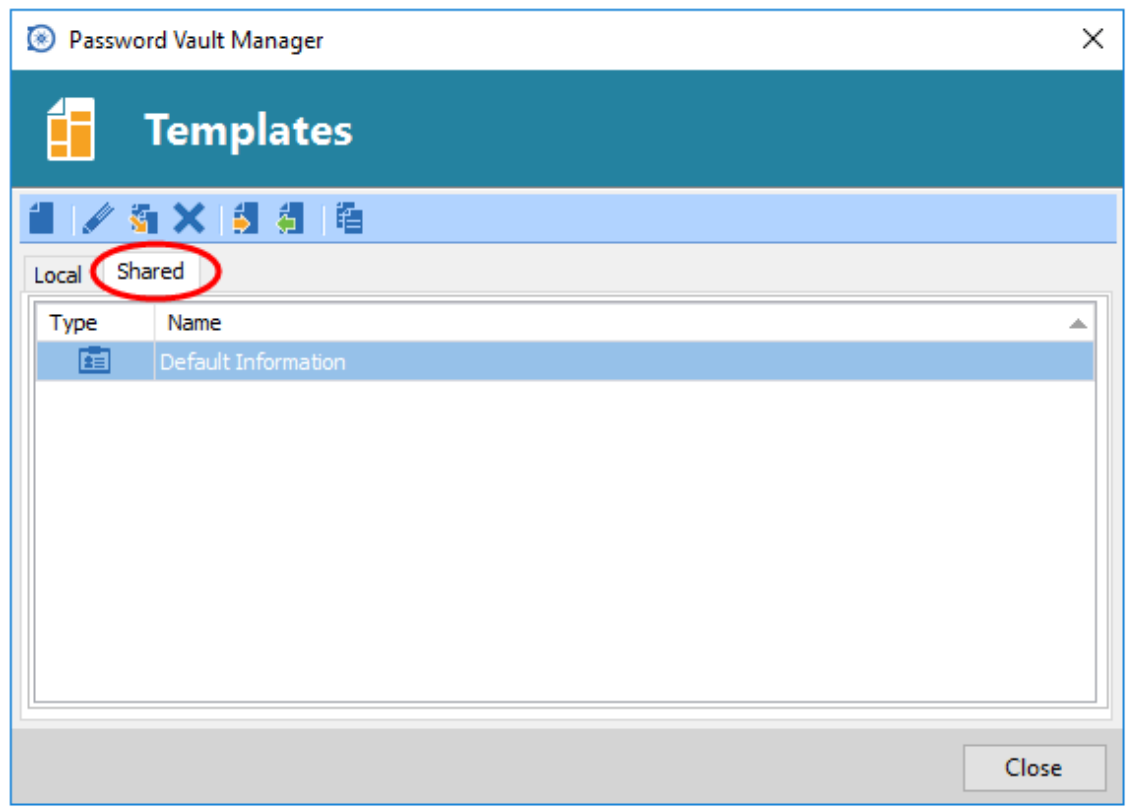
Local templates are saved on the local computer and are not available to other users.



Local Templates

Shared Template

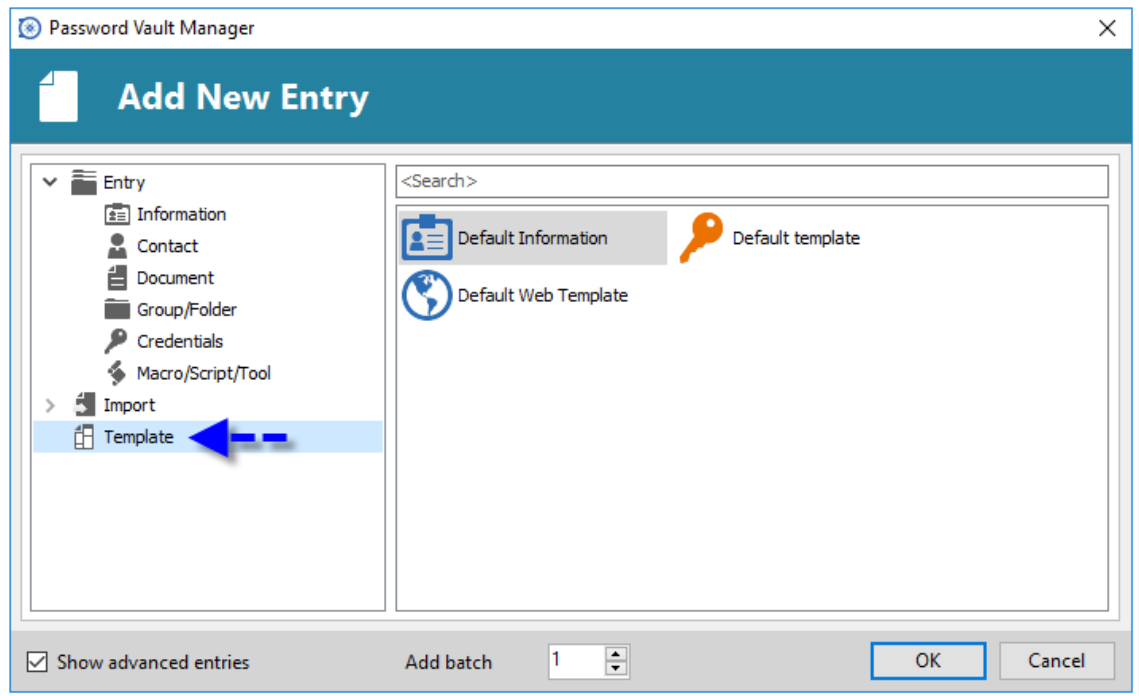
Shared templates are saved in the database and can be accessed by all users.



Shared Templates

Usage

The template can be used when creating a new entry.

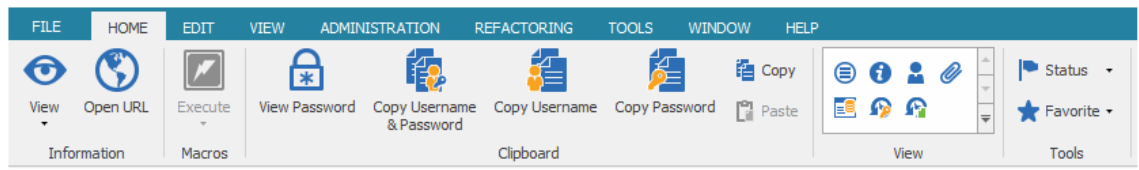


Add New Entry

3.2 Home

Description

The **Home** ribbon allows you to apply an action on the currently selected session. The options available to you will depend on the type of entry that is selected.



Home - Ribbon

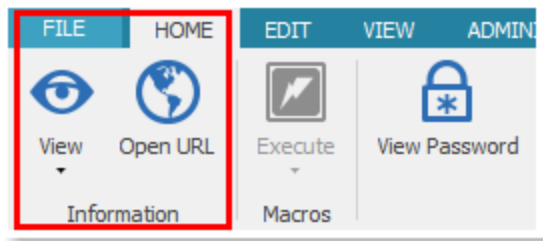
Consult the following topics for more information on each sections:

- [Information](#)
- [Macros](#)
- [Clipboard](#)
- [View](#)
- [Tools](#)

3.2.1 Information

Description

The **Information** section in **Home** tab allows you to view your entry or directly open the URL of the selected entry.



Home - Information

Settings

View

The **View** opens your selected entry either externally or embedded.

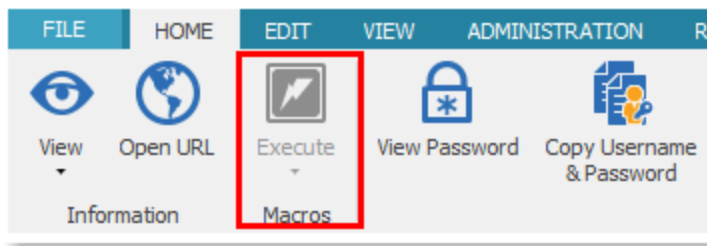
Open URL

If there is a URL defined in the selected entry, it will automatically open the URL.

3.2.2 Macros

Description

The **Macros** section in the **Home** tab allows you to execute scripts or macros of the selected entry. Please see Macros for more information.



Home Macros

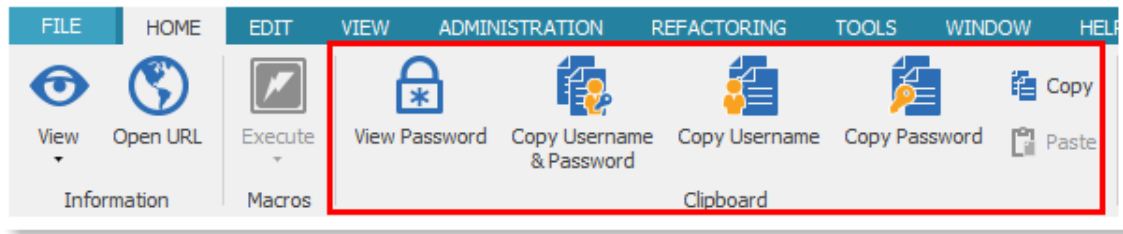
3.2.3 Clipboard

Description

With the Clipboard you can quickly copy entries value such as the username and the password.

- Username
- Password
- Data Entry (used to copy entries from one data source to another)

You can access the clipboard action via the **Home - Clipboard** ribbon bar or via the right-click menu **Clipboard - ...**



Home - Clipboard

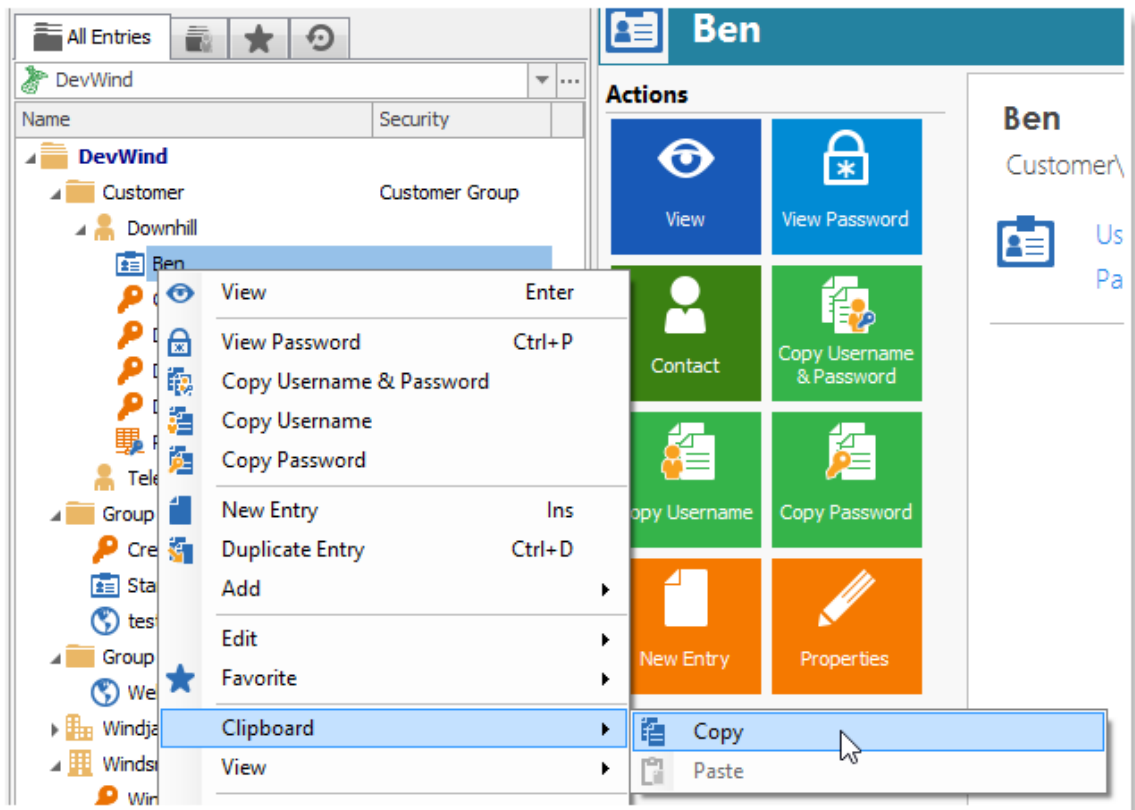
To access the User name and the Password from the clipboard, you must have entered the information in your session.



For security reasons, the clipboard will be cleared after **10** seconds when you copy a password. The delay can be configured via the system options, see [Options](#) for more information.

Copy/Paste entries

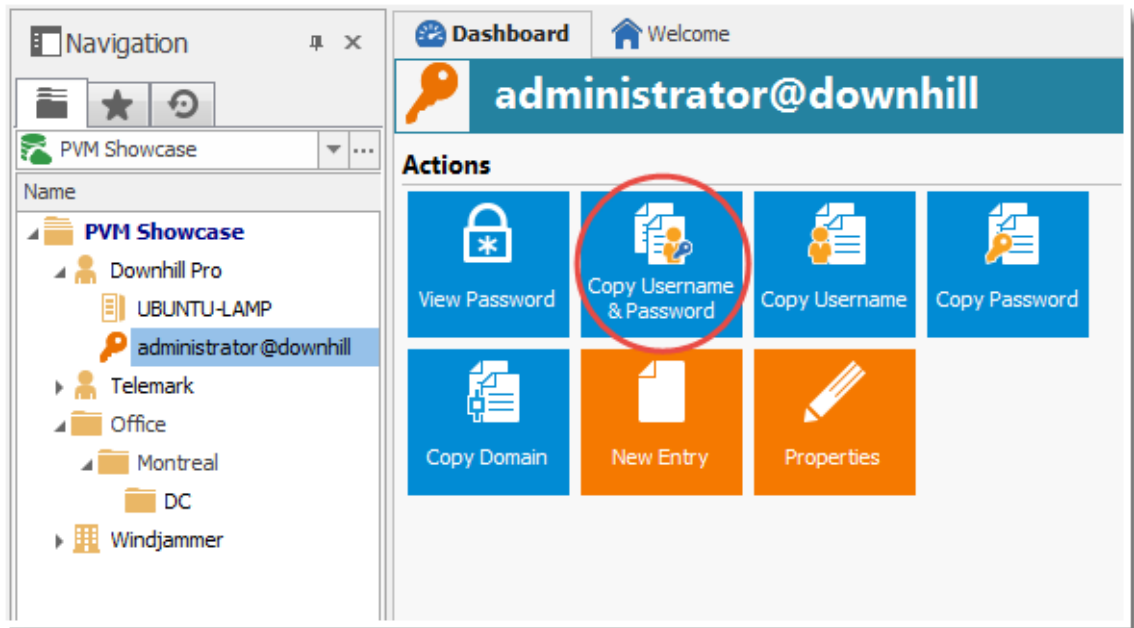
The Copy/Paste of an entry is also possible. Right-click on your entry and select **Clipboard - Copy**. Paste into a different data source or simply create a copy of an entry. It is a quick way to move/duplicate an item.



Copy/Paste an Entry

Copy Username and Password

The Copy Username and Password allows you to copy both the username and the password in a single action, pasting first the username and then the password by using our Paste once (secure) clipboard copy method. It is considerably more secure way to copy and paste your credential since your information will never be sitting in the internal copy buffer of the clipboard. You will only be able to paste once since the value will then be blocked from any further request.



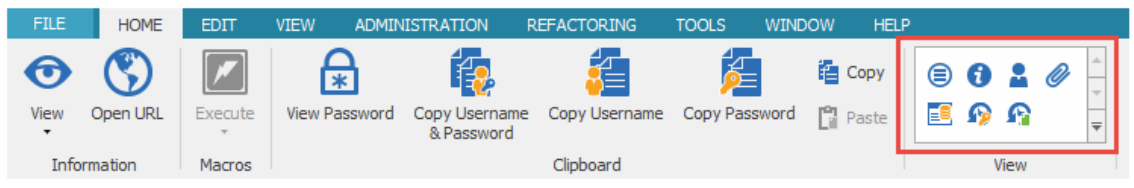
Copy Username & Password in a Single Action

3.2.4 View

Description

The **View** section in the **Home** tab displays multiple information on your selected entry.

Settings



Home - View

Option	Description
Details	Display the connection details. See Details topic for more information.
Information	Display several information on the entry. See Information topic for more information.
Contact	Display the contact information. See Contact topic for more information.
Attachments	Display the attachments file. See Attachments topics for more information.
Logs	Display remote computer logs. See Logs topic for more information.
Password History	Display the password history of a session. See Password History topic for more information.
Entry History	Allows you to compare two entries and manage history revisions. See Entry History topic for more information.

3.2.4.1 Details

Description

The connection details can be found on the dashboard, it is a simple grid that lists complete session information. The grid supports the copy/paste feature but the exporting is not available.

Description	Value
Connection Type	DataEntry
Data Source ID	0fbea4e0-cf5d-4222-bfd8-566bf934563
Description	
Group	Group 2
ID	58abd77f-0e0c-4783-a361-b1cc197d6147
Name	WebEntry

Connection detail grid from the dashboard

3.2.4.2 Information

Description

The information tab contains a wide assortment of information on the entry. Some purely informative and some of operational nature. It contains multiple tabs in order to present as much information as possible.

Settings

General

The **General** tab allows you to specify the computer specific information such as operating system, MAC address and the hardware description.

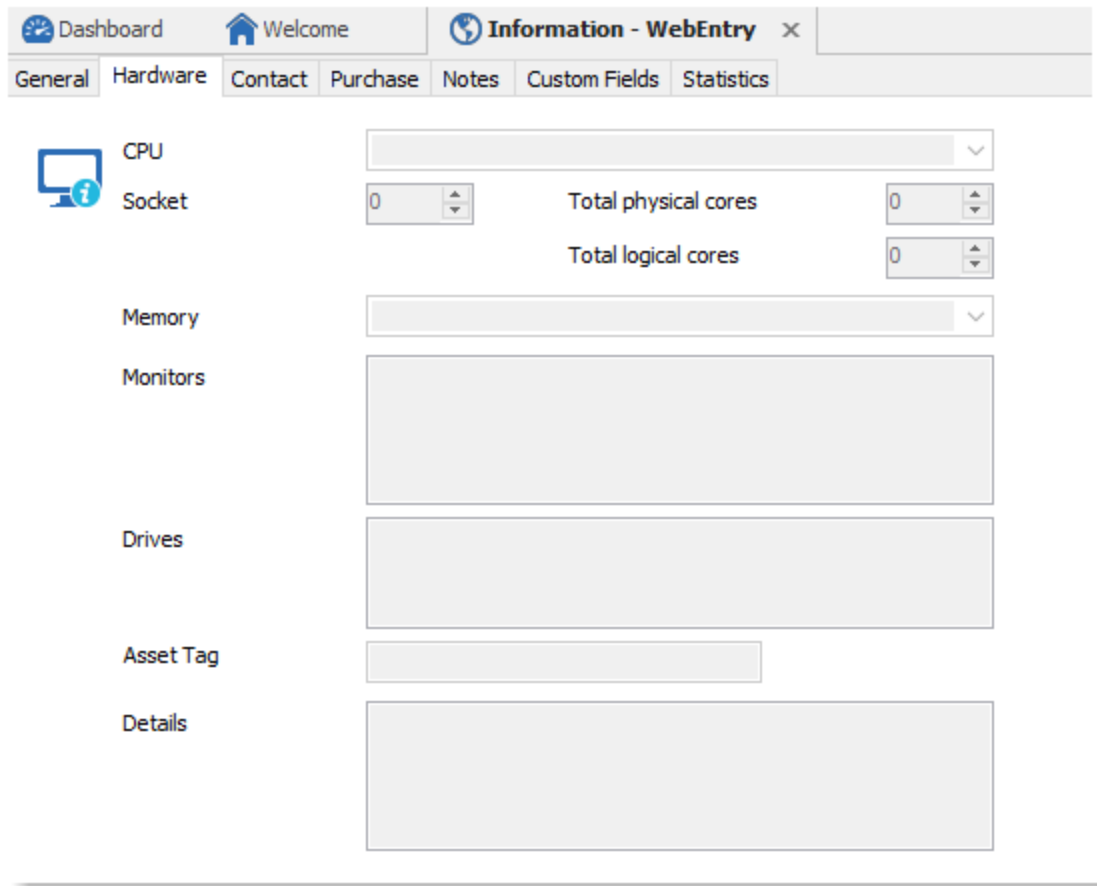
The screenshot displays the 'Information - WebEntry' form in Password Vault Manager. The interface includes a navigation bar with 'Dashboard', 'Welcome', and 'Information - WebEntry' tabs. Below this is a sub-navigation bar with tabs for 'General', 'Hardware', 'Contact', 'Purchase', 'Notes', 'Custom Fields', and 'Statistics'. The 'General' tab is active, showing a form with the following fields:

- OS: A dropdown menu.
- IP: A text input field.
- MAC: A text input field.
- Domain: A text input field.
- Architecture: A dropdown menu.
- Site: A text input field.
- Blade: A text input field.
- Rack: A text input field.
- Details: A text input field.
- Software: A large text area.
- Is Hyper-V server: A checkbox.
- Is Terminal server: A checkbox.
- Is virtual machine: A checkbox.
- Is VMware server: A checkbox.
- Is XenServer server: A checkbox.
- Server: A dropdown menu.
- Type: A dropdown menu.

Information - General tab

Hardware

The **Hardware** tab allows you to specify the hardware information of the remote computer.



Information - Hardware tab

Contact

The **Contact** tab displays information on a person that has a link to the entry.

Dashboard Welcome x Information - WebEntry x

General Hardware Contact Purchase Notes Custom Fields Statistics

Contact Default

First name Last name

Middle name Prefix

Gender Unspecified Job title

[Credentials](#) Customer #

Company Email

Address Home phone

City Work phone

State Mobile

Zip code Fax

Country Skype

Website

Information - Contact tab

Purchase

The **Purchase** tab allows you to enter information related to the invoice or the purchase of the equipment.

The screenshot shows a web application interface for 'Information - WebEntry'. The top navigation bar includes 'Dashboard', 'Welcome', and 'Information - WebEntry'. Below this, a series of tabs are visible: 'General', 'Hardware', 'Contact', 'Purchase', 'Notes', 'Custom Fields', and 'Statistics'. The 'Purchase' tab is active, displaying a form with the following fields:

- Date:** A date picker set to '2016-07-13' with a calendar icon and a dropdown arrow. To its right is the label 'Age'.
- Vendor:** A dropdown menu currently showing 'Default' and an empty text input field to its right.
- Serial number:** An empty text input field.

Below the 'Purchase' section is the 'Warranty' section, which contains:

- Expiration:** A date picker set to '2016-07-13' with a calendar icon and a dropdown arrow. To its right is a calendar icon and the label 'Remaining'.
- Service tag:** An empty text input field.
- Service level:** An empty text input field.

Information - Purchase tab

Notes

The **Notes** tab contains only one control. A text area where you can enter any information you require.

Custom Fields

The **Custom** tab contains five custom fields. The reason behind having discrete fields is that they are available via Field Variables and can therefore be accessed in sub-connections while being defined in the parent connection.

For ease of use, the labels can be modified to reflect the information you intend to store in them. Clicking on the label allows you to enter any caption you desire.

Information - Custom Fields tab

Statistics

The **Statistics** tab simply displays some information on the creation and last modification of the entry.

Information	
Created by	VDEVOLUTIONS56\jknaf0
Creation date	2016-07-11 11:05 AM
Last update by	VDEVOLUTIONS56\jknaf0
Last update date	2016-07-13 2:32 PM

Information - Statistics tab

3.2.4.3 Attachments

Description

Allows you to add an attachment to an entry. The file is stored directly in the database.



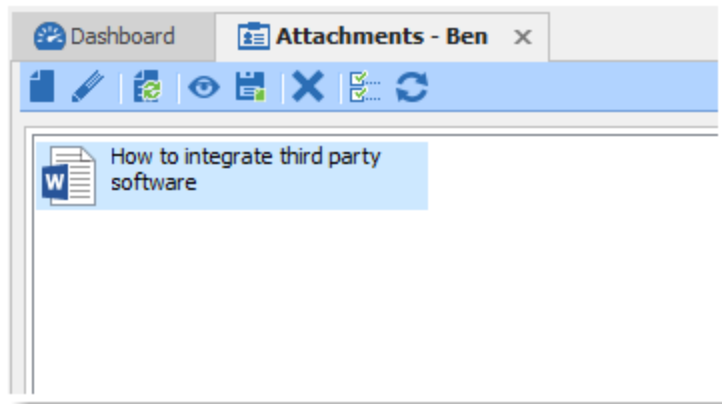
This feature is only available when using an [Advanced Data Source](#).



The file will not be available in the offline mode.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, they cannot be restored. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.



Attachment

The attachment can be any type and size, depending on your bandwidth and on the data source. You can also view a saved attachment from:

- the session context menu;
- the session properties; or
- directly on the dashboard.

The refresh button will directly update your selected document. Use it to save your local modifications after an edit.

3.2.4.4 Logs

Description

This pane displays the [Usage Logs \(Global\)](#) saved in the database, filtered to only show the selected entry's log.



This feature is only available when using an [Advanced Data Source](#).

Message	On Open Comment	Log Date	End Date...	Active Time
Copied password to clipboard		2016-07-13 3:31:27 ...		
Copied user name to clipboard		2016-07-13 3:31:27 ...		
Exported entry (Csv)		2016-07-13 2:24:58 ...		
Exported entry (Native)		2016-07-12 2:23:36 ...		
Viewed the data entry		2016-07-11 3:30:18 ...		
Entry edited		2016-07-11 3:22:52 ...		
Entry edited		2016-07-11 3:22:31 ...		

Global Usage Log

3.2.4.5 Password History

Description

Password History feature allows for viewing of the password history for an entry. The number of historical passwords to save is set in **Administration - Data Source Settings - Password Policy - Password history X items**.



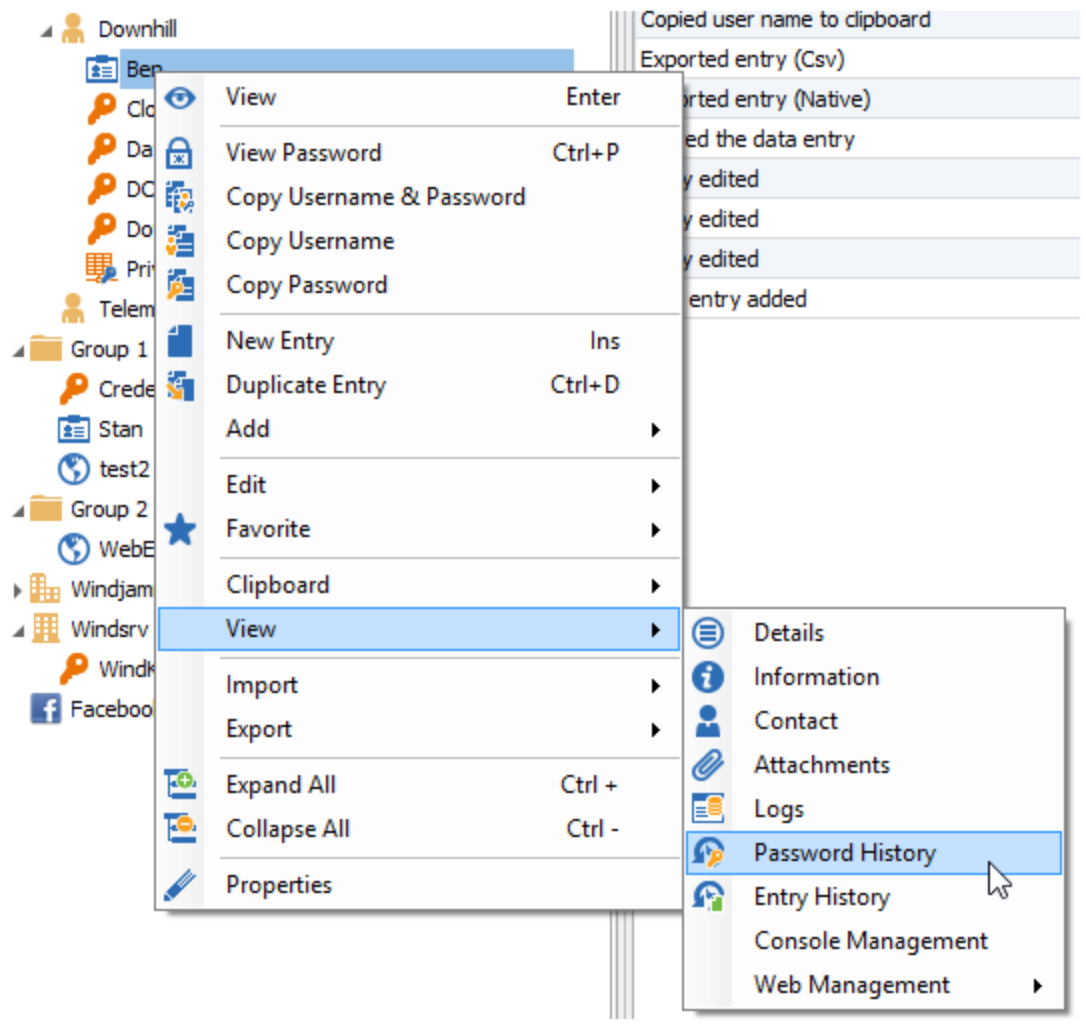
You must be an administrator of the data source to perform this action.



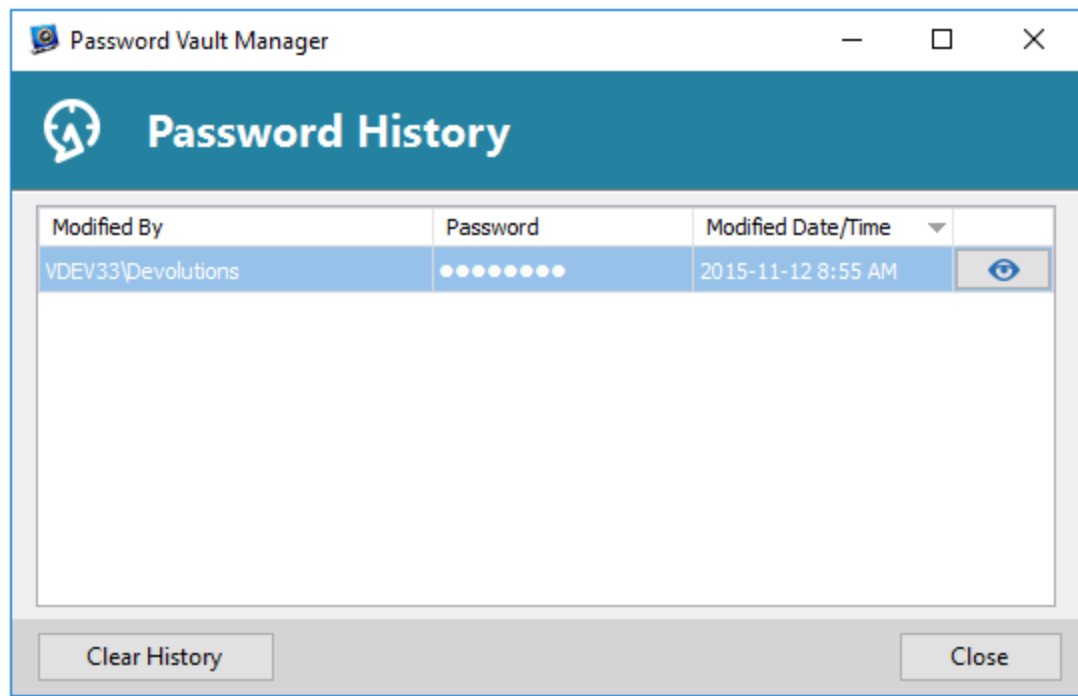
This feature requires an [Advanced Data Sources](#).

Settings

To display the password history you could also right-click on an entry and select **View - Password History**.



The password history of the entry will pop up, you will then be able to view the different passwords that were used and the date they were modified. You can delete the whole password history by clicking on **Clear History**.



Password History

3.2.4.6 Entry History

Description

Entry History feature allows you to view details regarding different version of your sessions and also gives you the option of performing compares between different versions.



This feature requires an [Advanced Data Sources](#).



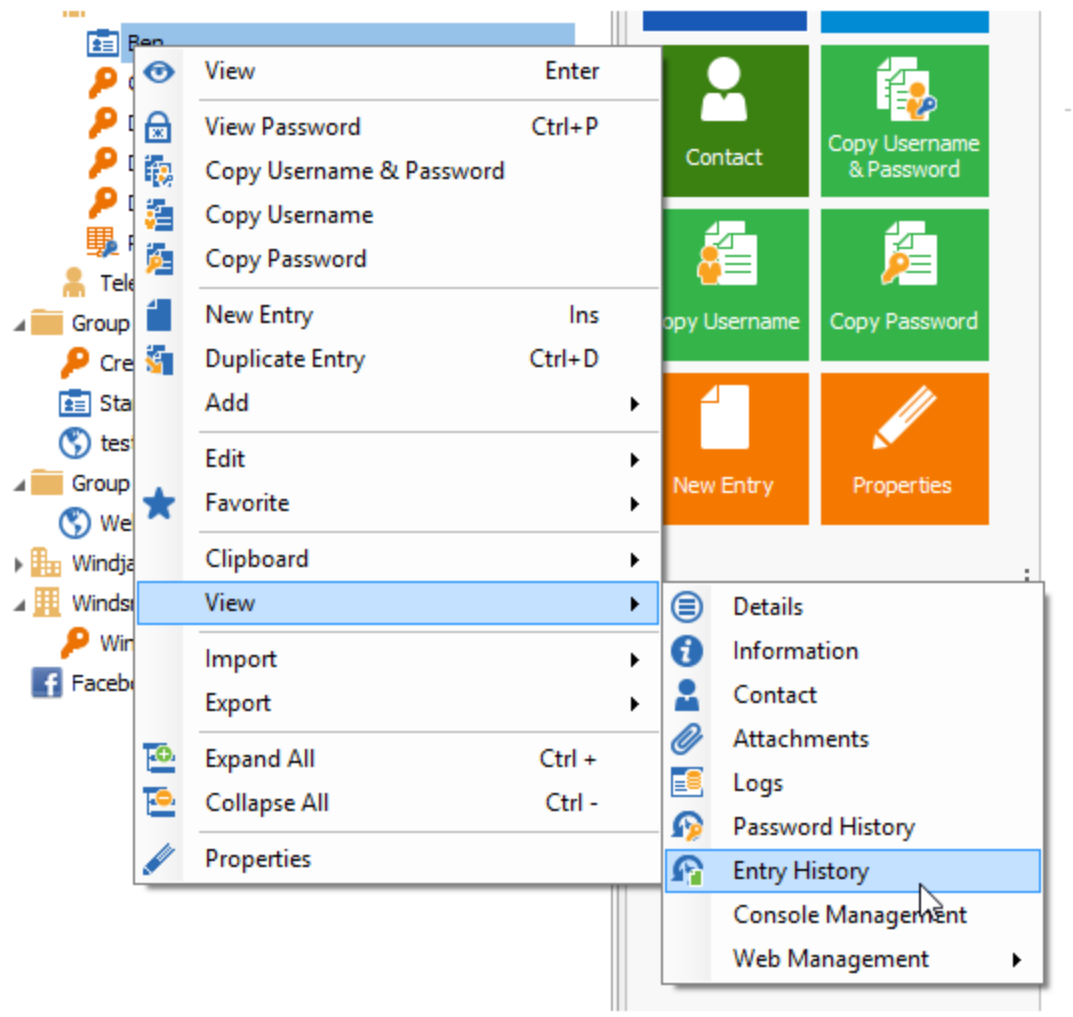
You must be an administrator of the data source to perform this action.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from modifications. Once they are modified, the previous version **cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

To display the entry history, **right-click** on an entry and select **View - Entry History**.

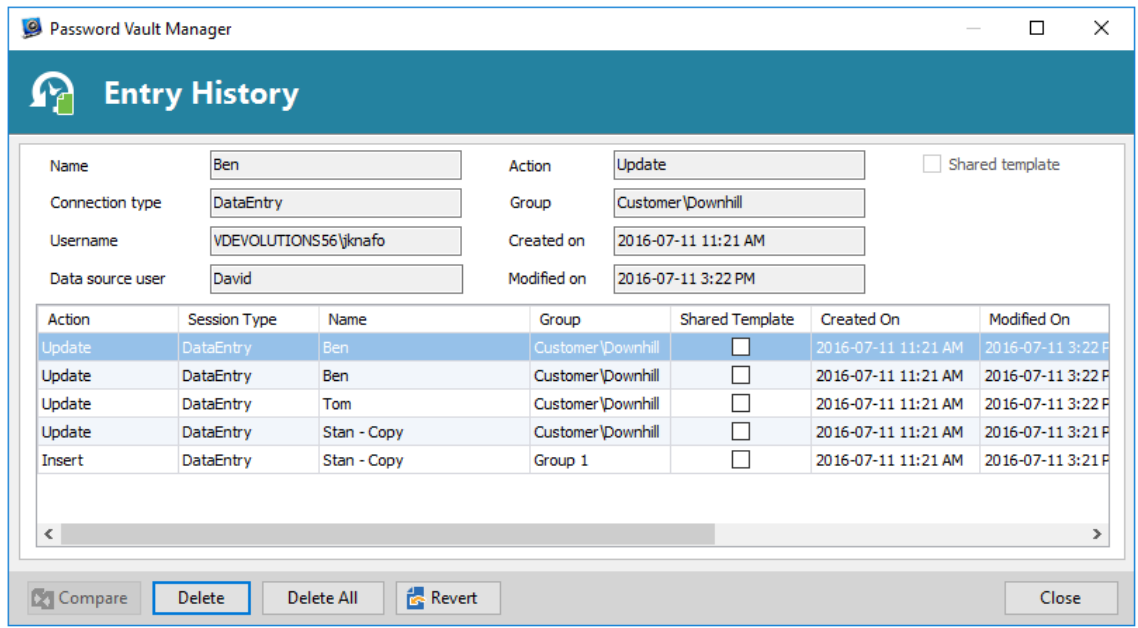


Entry History

Entry History view

The entry history view dialog allows you to compare two entries and manage history revisions. To compare simply select any two entries then use the **Compare** button.

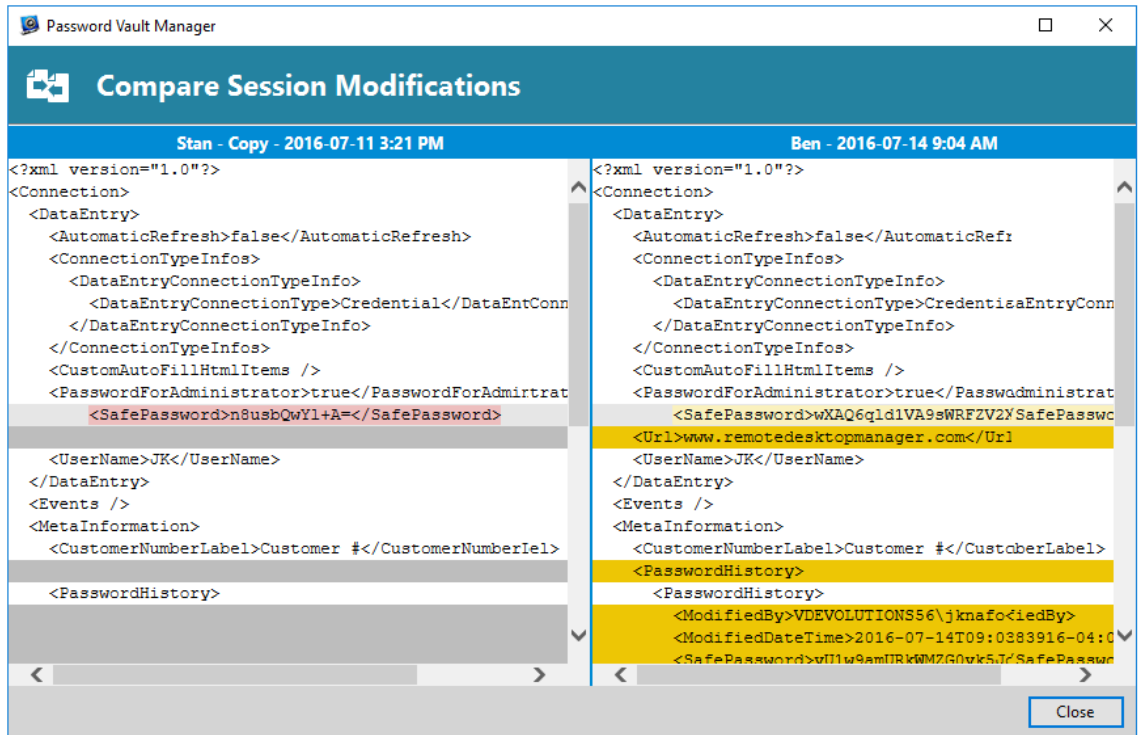
You can delete any history revision or the entire history using the **Delete** and **Delete All** buttons.



Entry History View

Compare

You can compare two entries to verify the changes that were made. Just select the entries (Ctrl+click) in your Entry History View and then click on **Compare**.



Compare Session Modifications

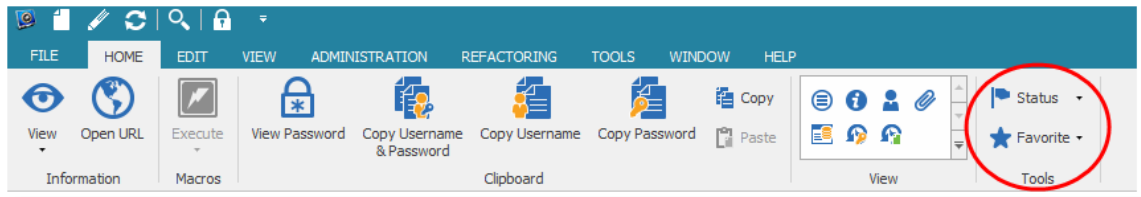
View Deleted Entries

Use the [View Deleted](#) to manage and resurrect deleted entries.

3.2.5 Tools

Description

The **Tools** section in the **Home** tab allows you to change the status of a session, create/delete favorite, create a Play List and Insert Log Comment.



Home - Tools

Status

You can modify the status of your selected entry to apply different actions to it.



Status

Edit Message

Write a session status message that will be displayed every time a user open a session.

Default

Set the status back to its default setting.

Locked

Lock other users out of a session, to prevent usage of a session by anyone else you must enable it. However, the holder of the lock can still use it.

Disabled

A disabled session can't be opened. It's mostly used when you don't want to delete a session but wish to avoid any unattended connection. It's also useful to disable an account for one of your former customer.

Warning

The session will be functional, but a message will be displayed to other users before opening it.

Expired

An expired session can't be opened. It can be set manually or automatically if the session expiration date is set in his property.

Favorites

For more information please see [Favorites](#).

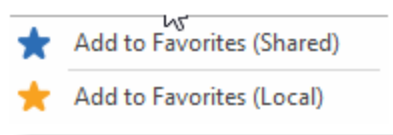
3.2.5.1 Favorites

Description

A feature to tag entries as favorites is provided. This is useful when the number of managed entries becomes too great or if you must maintain a strict directory structure to hold your entries.

Settings

There are two types of favorite sessions, the Shared and the Local. The blue star is for Share and the yellow star is for Local.



Favorite colors

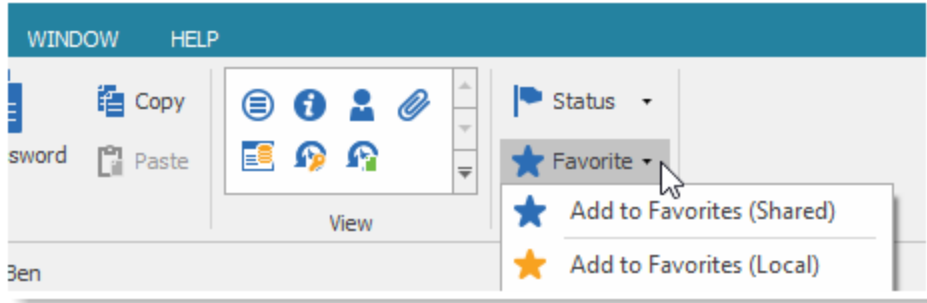
Adding a Session to the Local Favorites

Select your entry and do a right-click and select **Favorites - Add to Favorites** or from the menu **Home - Favorites**.




Local favorites are flagged locally on the current machine by the current user. These local favorites are saved in a file named **PasswordVaultManager.ext**. By default, this file is located in **%localappdata%\Devolutions\PasswordVaultManager**.

You can use the context menu to include or remove a session from your favorites by right-clicking on the session and select **Favorites** or you can do it by clicking on **Home - Favorite - Add to Favorites (Local)** in the Tools section.

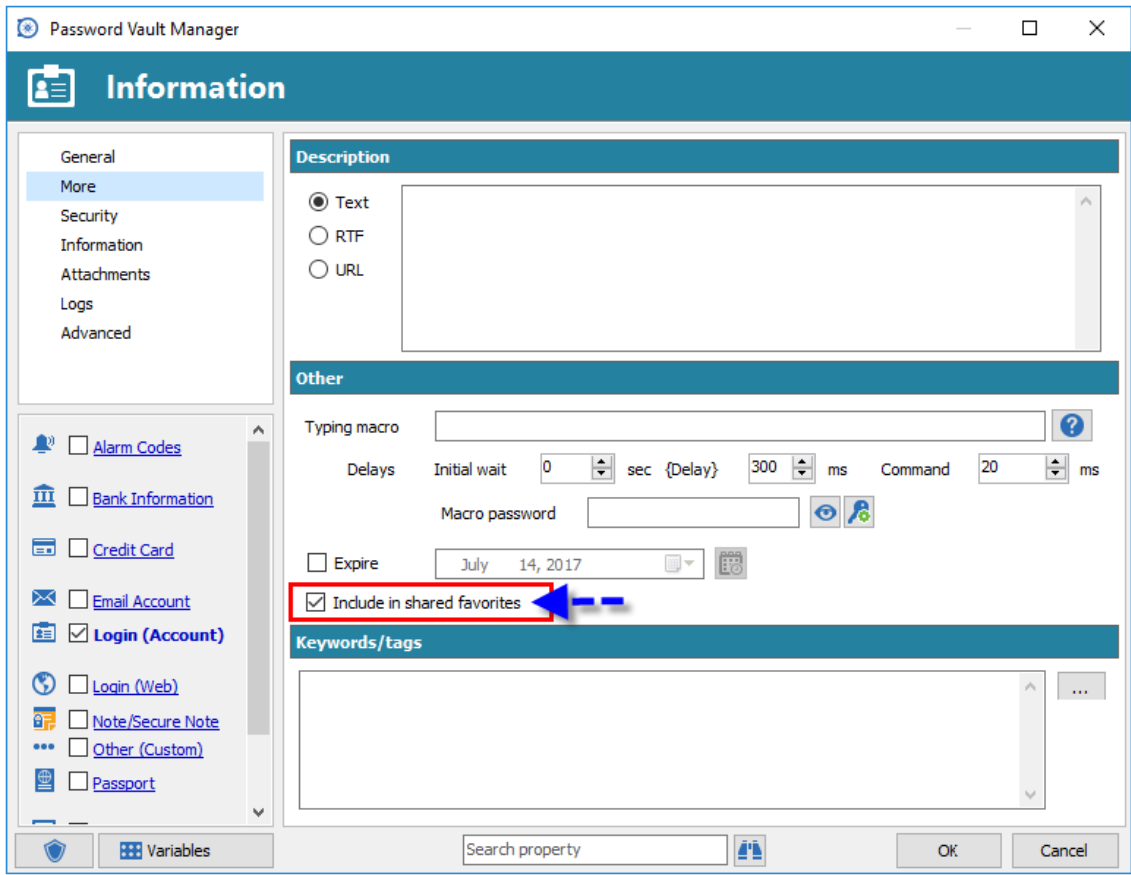


Setting an entry as a favorite

Adding a Session to the Shared Favorites

 **Shared favorites** are shared by all users who are connected to the data source and are directly configured from the session.

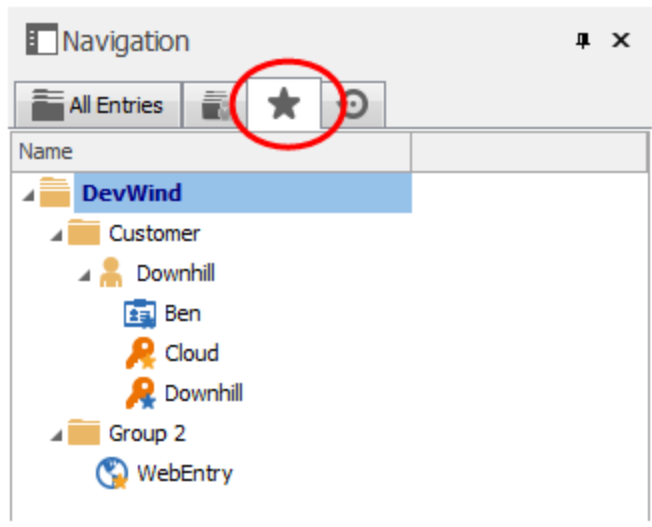
You can add an entry to your Shared favorites by clicking on **Home - Favorite - Add to Favorites (Shared)** in the Tools section. You could also Edit your session and enable the Include in shared favorites.



Information entry - More tab

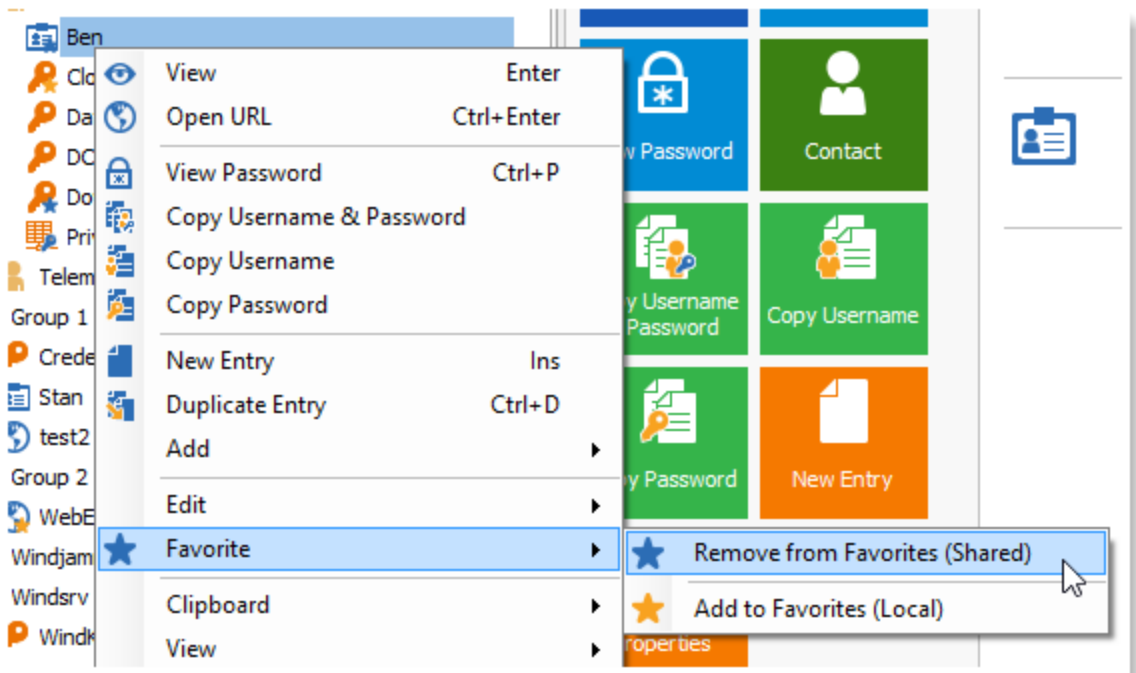
View your Favorites

You can view all your favorite entries that have been configured in the current data source in the **Favorite** tab of your **Navigation Pane**.



Favorites Tab

To remove an entry from your favorites use the **Home - Favorites** menu or do a right-click on your entry and select **Favorite - Remove from Favorites**.

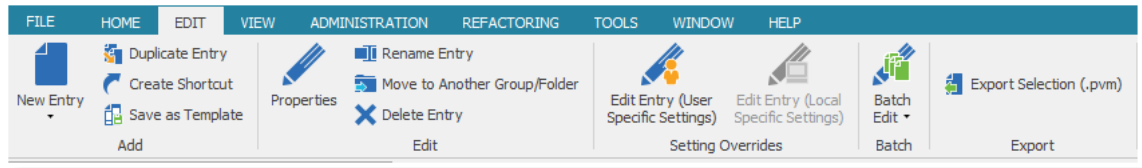


Remove from Favorites

3.3 Edit

Description

The **Edit** ribbon contains operations to rapidly Add, Edit, Overrides, Batch Edit or Export entries.



Edit Ribbon

For more information on the different sections please see:

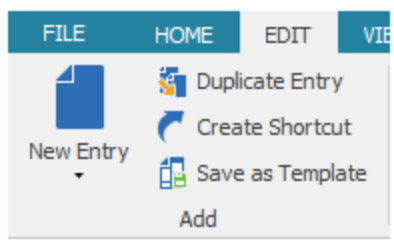
- [Add](#)
- [Edit](#)
- [Setting Overrides](#)
- [Batch](#)
- [Export](#)

3.3.1 Add

Description

The **Add** lets you quickly create new entries, duplicate them, create shortcut or rapidly save your entry as a template.

Settings



Edit - Add

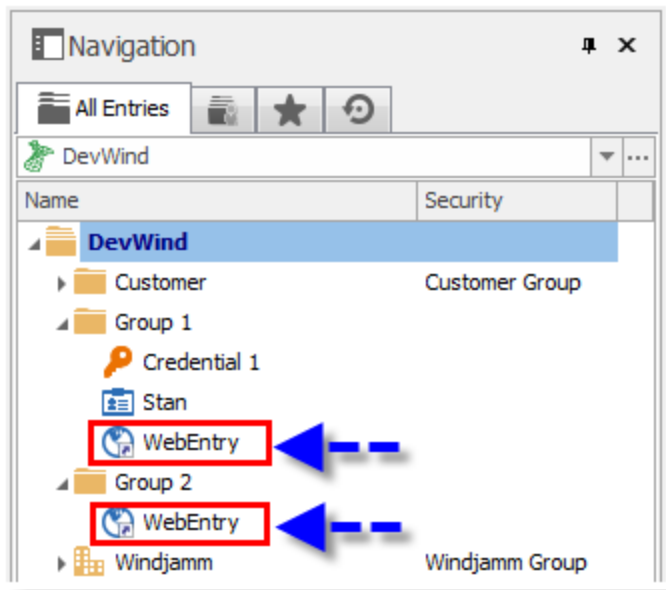
Option	Description
New Entry	Create a new entry (credential entry, group/folder, web login, information, etc...).
Duplicate Entry	Create a duplicate of your entry.
Create Shortcut	Link your entry to more than one group. See Shortcut/Linked Entries for more information.
Save as Template	Save your selected entry as a local or shared template.

3.3.1.1 Shortcut/Linked Entries

Description

There are a many scenarios where it makes sense for an entry to appear more than once in the User Interface. For example, you might want to:

- assign different access to the folder
- create a favorite folder with everything centralized
- reuse a document for different scenario.

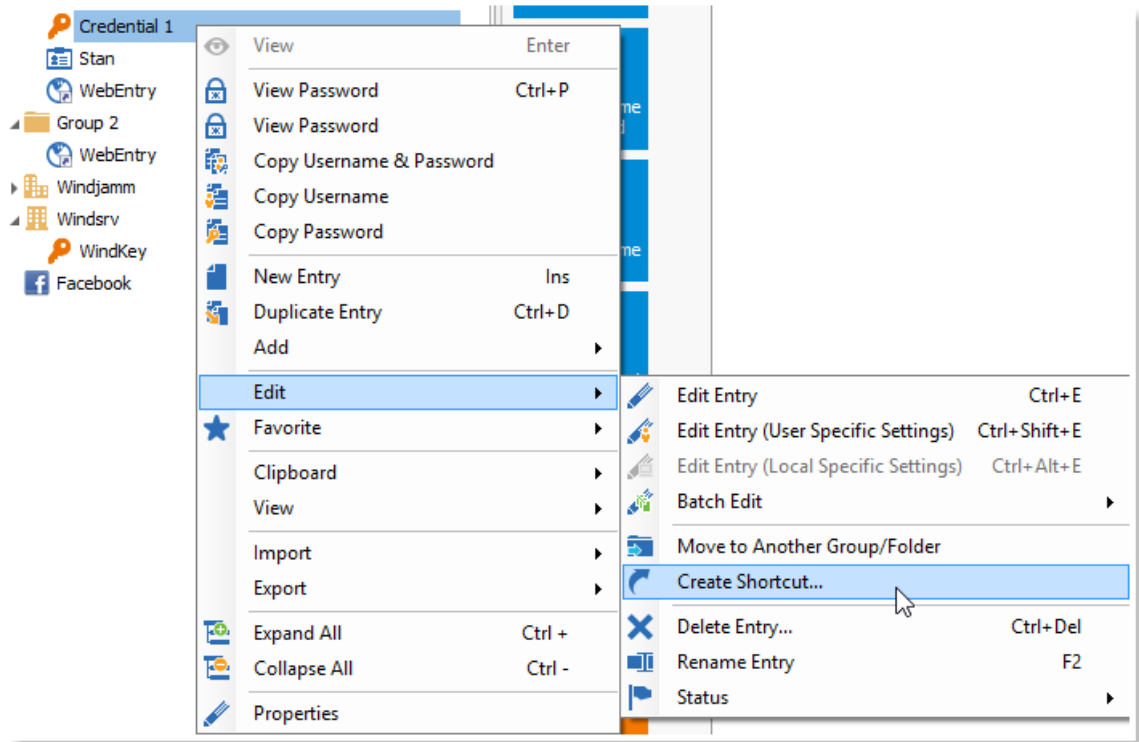


Shortcuts created

Creating shortcuts is simplified by saving the entry once in the database, while linking it to more than one group. So when the application loads the data, it automatically creates a link to the original entry.

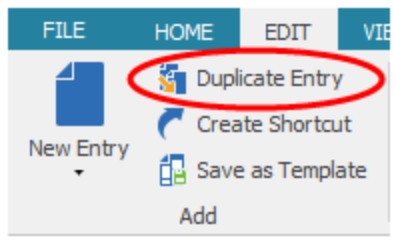
Creating a Shortcut: Option 1

One way to create a shortcut is by using the menu **Edit - Create Shortcut**.



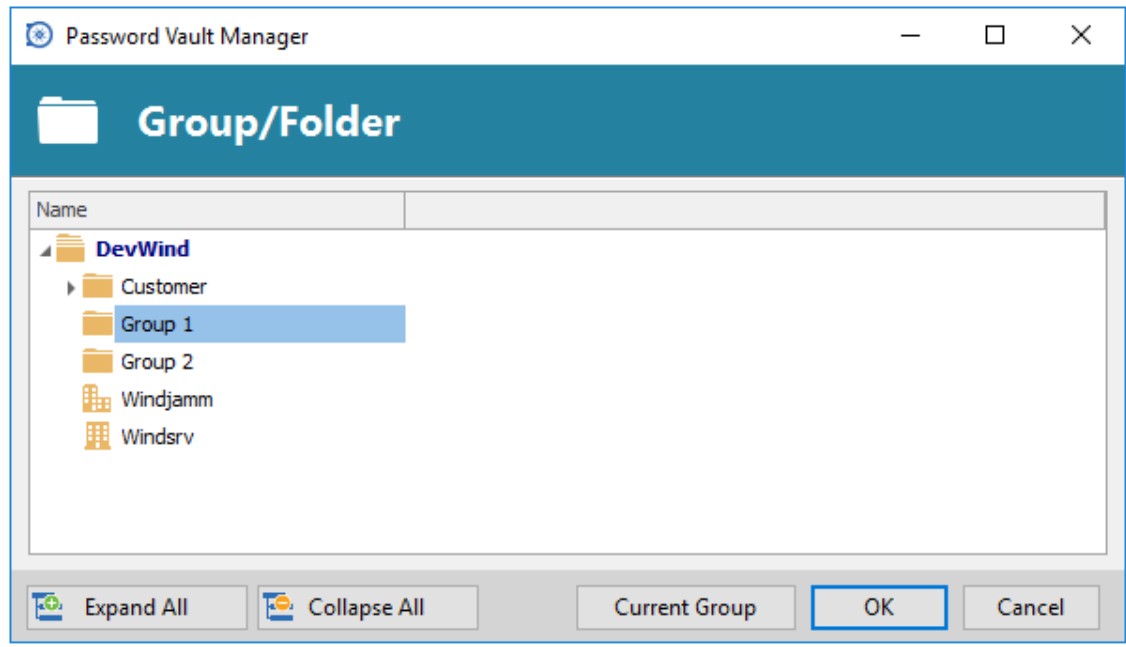
Edit - Create Shortcut

You could also select your entry and then click on **Create Shortcut** from your **Edit** menu.



Duplicate Entry

Select the destination folder for your newly created shortcut and click on **OK**.



Select destination folder

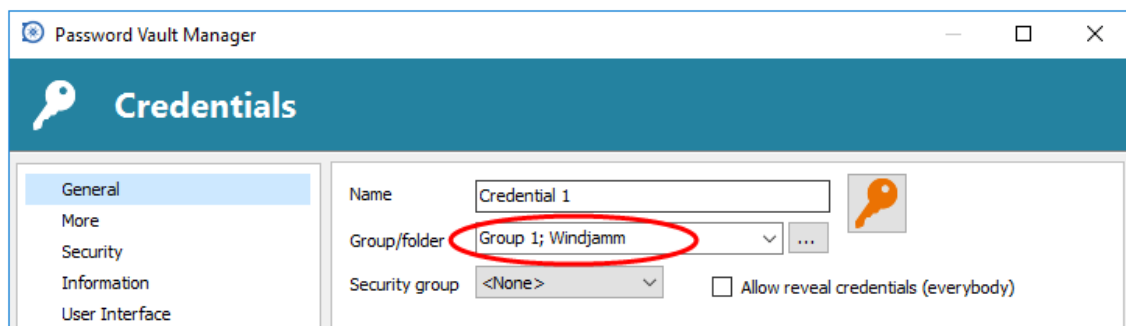
The application will automatically refresh and display the new shortcut in the list.



There is no visual difference between the shortcut and the original entry. Therefore, you'll need to delete all entries to completely remove them.

Creating a Shortcut: Option 2

A second way to create a shortcut is via the session properties. Since the shortcut is based on a group list, simply add a session in multiple groups by setting two or more destinations, which are separated by “;”. You can also use the browse button (...) and select more than one group by holding the Ctrl key while clicking on the tree node.



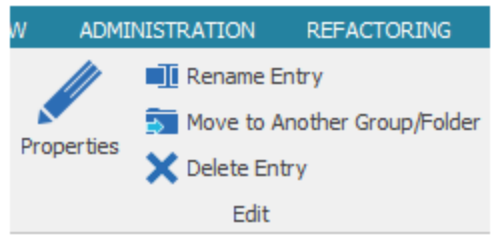
Group/folder

3.3.2 Edit

Description

The **Edit** menu is used to Edit one of your entry. You may edit the properties, rename your entry or quickly delete your entry.

Settings



Edit - Edit

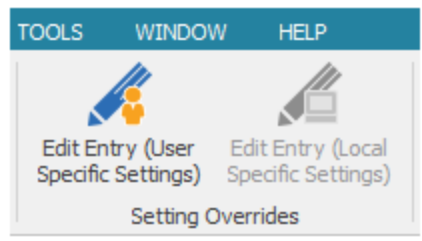
Option	Description
Properties	Automatically opens the property window of your selected entry.
Rename Entry	Rename your selected entry.
Move to Another Group/Folder	Move your selected entry to another Group or Folder.
Delete Entry	Delete your selected entry. A confirmation window will appear to confirm the deletion of the entry.

3.3.3 Setting Overrides

Description

Setting Overrides is used to override the user specific settings or the local specific settings of a session.

Settings



Setting Overrides

Option	Description
Edit Entry (User Specific Settings)	Allows session setting override for a user. Please consult User Specific Settings for more information.

Edit Entry (Local Specific Settings)	Allow session setting override for the local machine. Please consult Local Specific Settings for more information.
--------------------------------------	--

3.3.3.1 User Specific Settings

Description

The User Specific Settings allows session setting to be override for a user.

Settings

User Specific Settings

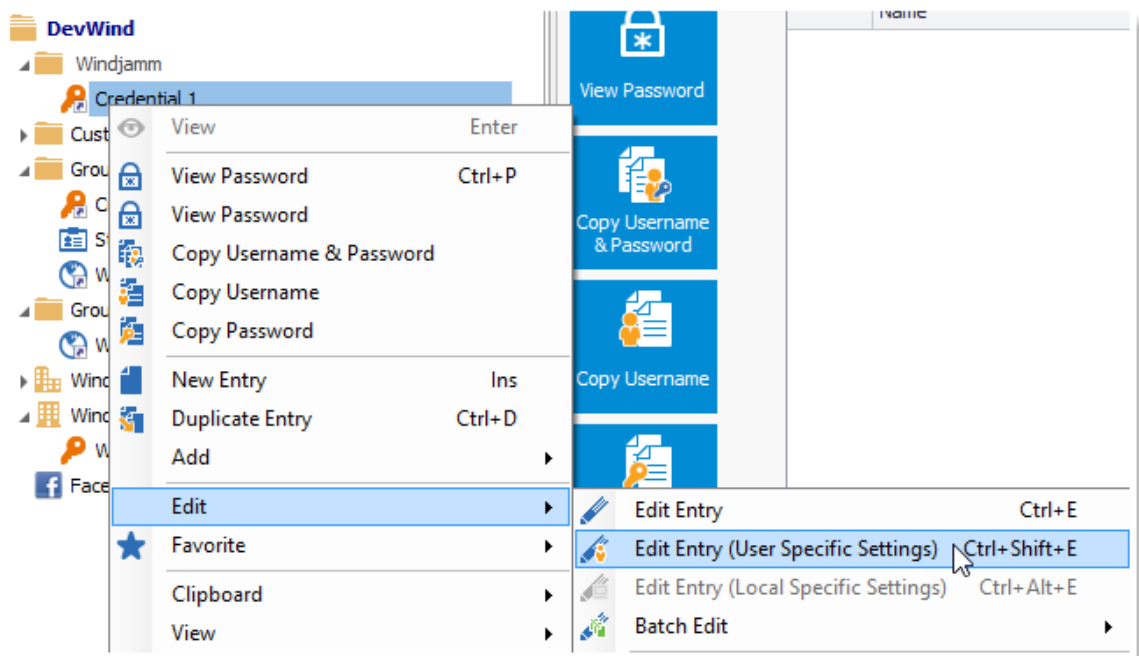


This feature requires an [Advanced Data Sources](#).



If both User Specific settings and [Local Specific Settings](#) are defined on the same entry, [Local Specific Settings](#) have priority.

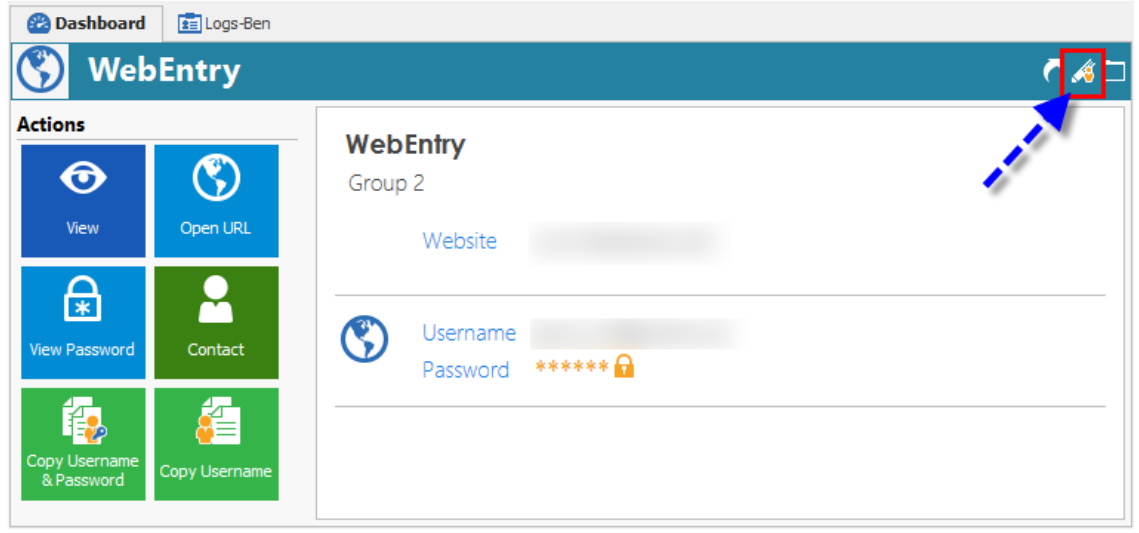
Do a right-click on your selected entry and select **Edit - Edit Entry (User Specific Settings)** or go in the menu **Edit - User Specific Settings**.



Edit Entry (User Specific Settings)

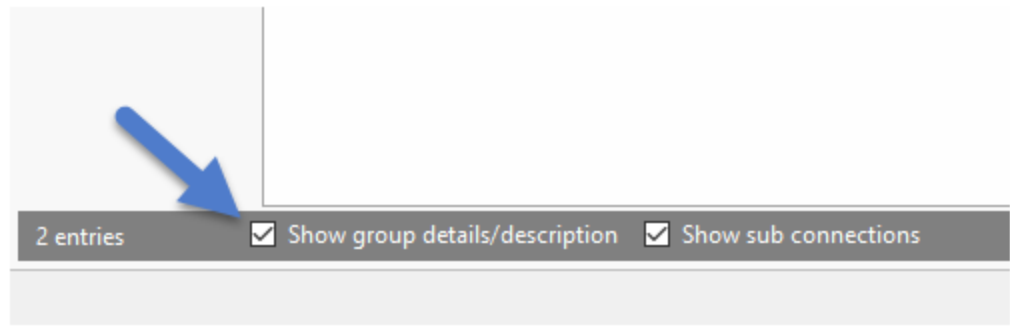
User Specific settings indicator

For entries with defined **User Specific Settings**, an indicator appears in the dashboard when you select the entry. You can simply click on the indicator to go to the **Edit Entry (User specific settings)** dialog.



User Specific Settings

For Groups/Folders you must have enabled the **Show group details/description** option to see the indicator.

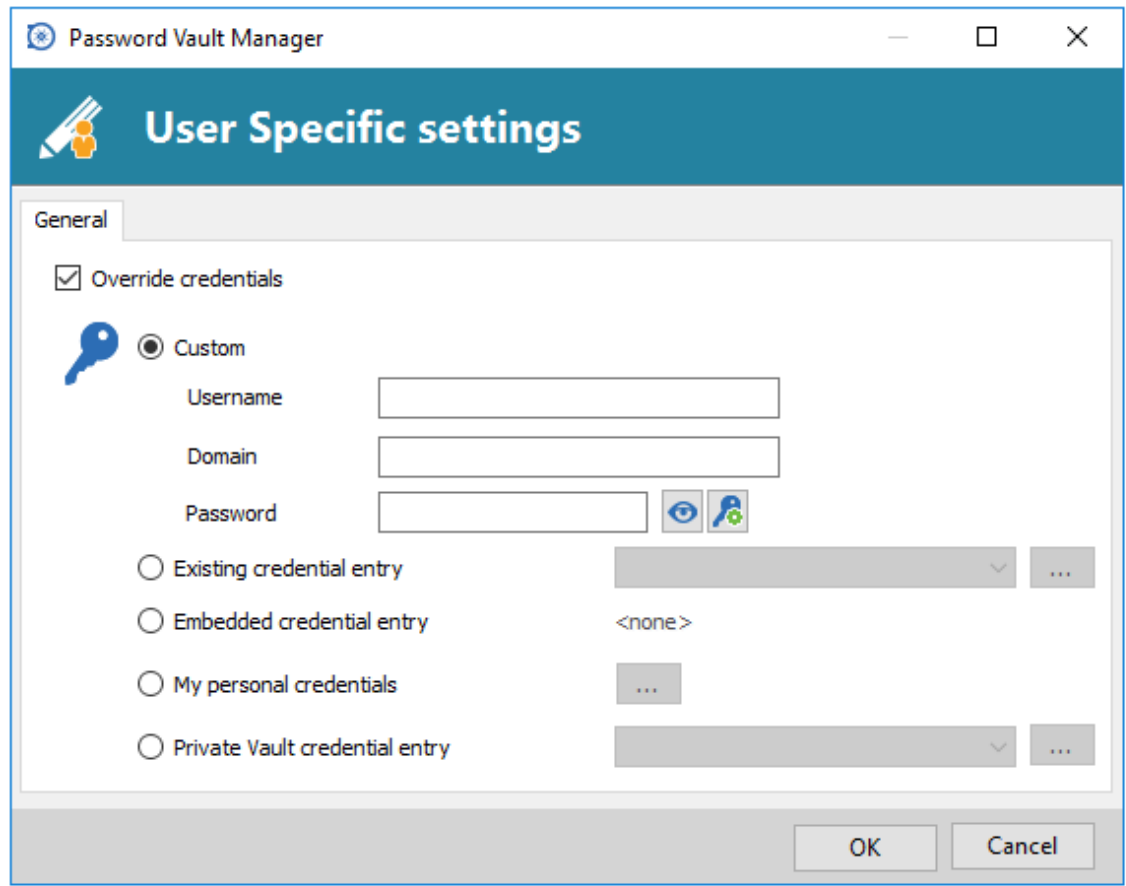


Show Group Details/Description

Workflow

Sessions and Groups/Folders

Right-click on your entry and select **Edit - Edit Entry (User Specific Settings)**



User Specific Settings

Please consult each specific override topics for more information:

- [Credential Entry Overriding](#)
- [Credentials](#)

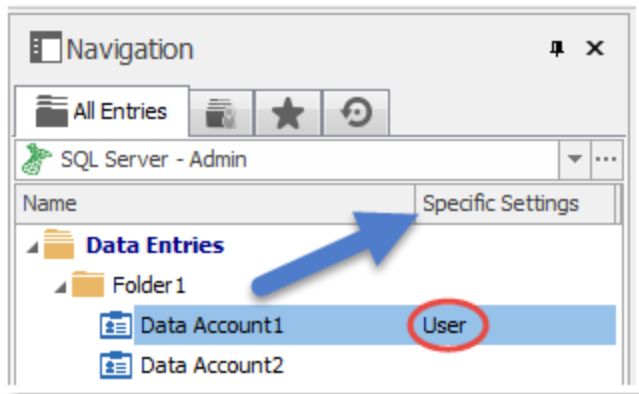
Credentials Entries

In the case of credential entries, please refer to [Credential Entry Overriding](#).

Navigation tree view column

A Specific Settings column can be added in the Navigation Pane by **right-clicking** on the **column Name** in the Navigation Pane and selecting **Column Chooser**.

Double-Click on **Specific Settings** and the column Specific Settings will be added. You will now be able to see if there is a specific setting applied to your entry.

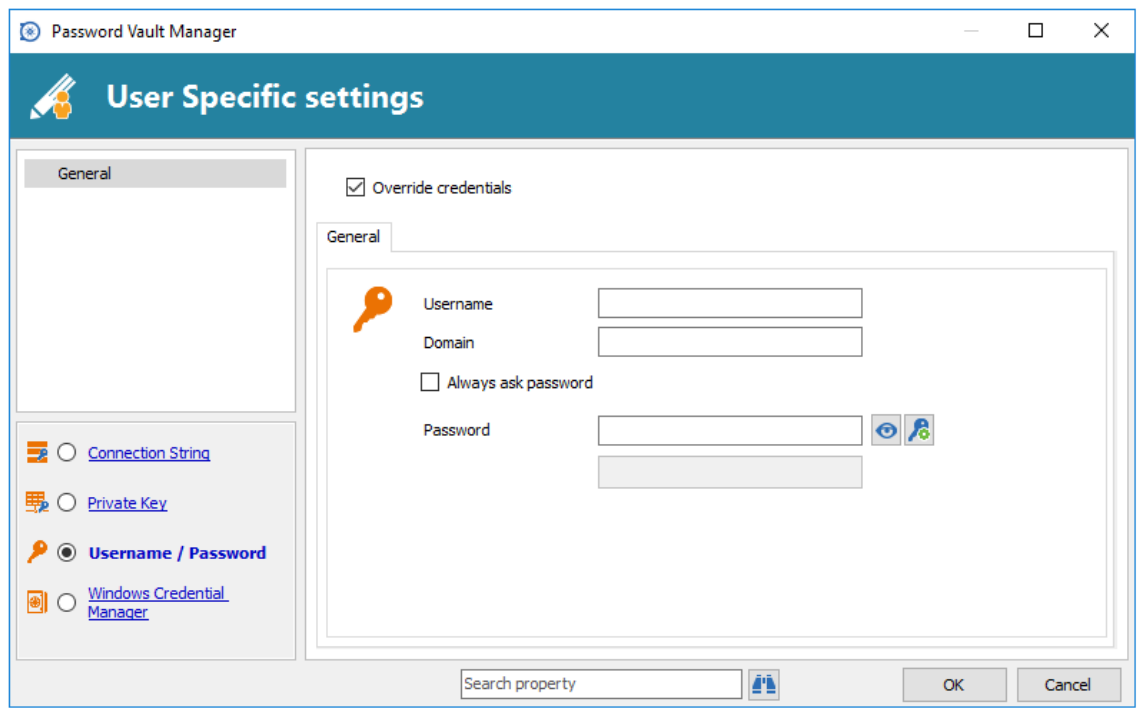


Specific Settings Column

3.3.3.1.1 Credential Entry Overriding

Description

The Credential Entry override is a special case. When overriding using either [User Specific Settings](#) or [Local Specific Settings](#), a specialized dialog appears to allow you to override the original credentials.



User Specific settings

Settings

To override the credentials you must first check the **Override credentials** option. Then you enter the new credentials in the area below.

To stop overriding credentials uncheck the **Override credentials** option.

3.3.3.1.2 Credentials

Description

Override Credentials allows you to specify other credentials than the ones that are stored in an entry. You can choose from multiple sources according to your security practices and policies.



The Credentials override is available on all entry types.

Settings

Credentials User Specific Settings

Depending on the type of entry being selected, the following choices are offered.

Option	Description
Custom	Use a specific User name, Domain and Password
Existing credential entry	Use an existing credential entry

Embedded credential entry	Use an Embedded credentials
My personal credentials	Use the credentials stored in My Personal Credentials
Private Vault credential entry	Use an entry from your Private Vault (Note 1)

Notes

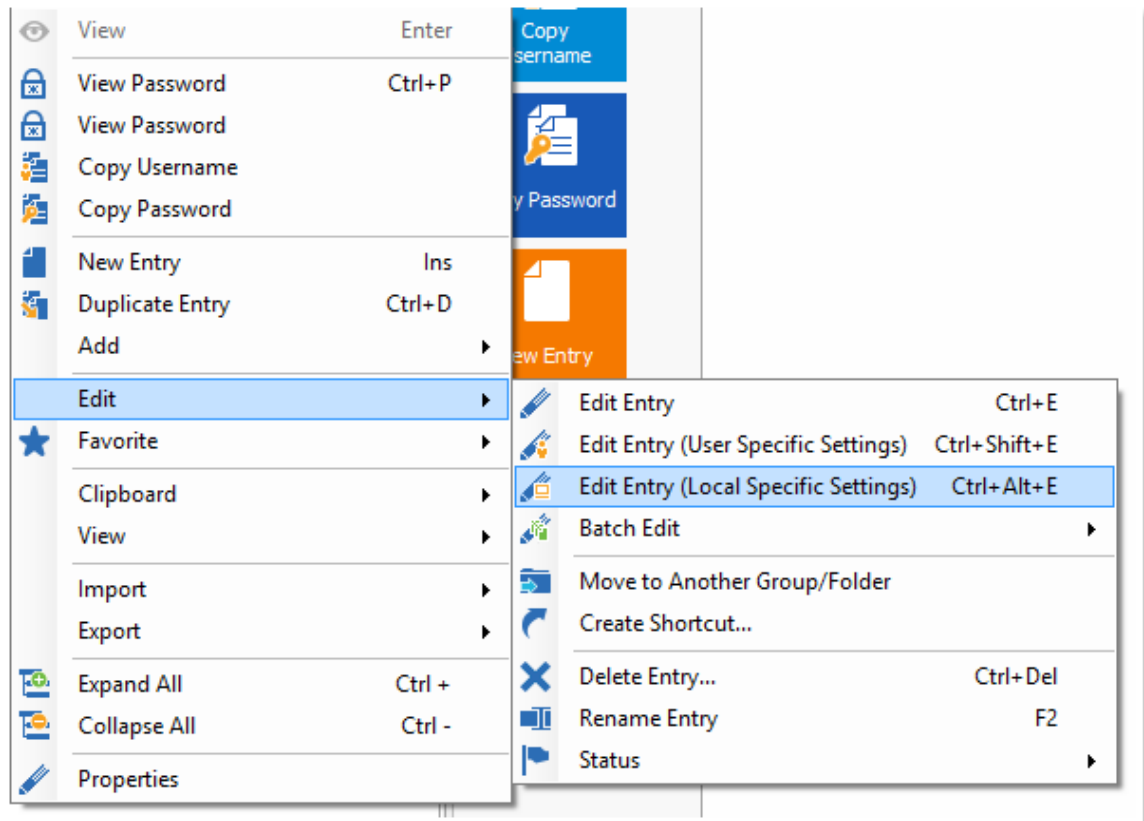
1. The Private Vault credential entry is only available under the following conditions:
 - 1.1. The Private Vault is available for your data source, please consult [Private Vault](#);
 - 1.2. You are overriding at the folder level;
 - 1.3. You are overriding a session that is itself in the Private Vault.

3.3.3.2 Local Specific Settings

Description

Allow session setting override for the local machine. Several settings can be overridden such as user name, password and display.

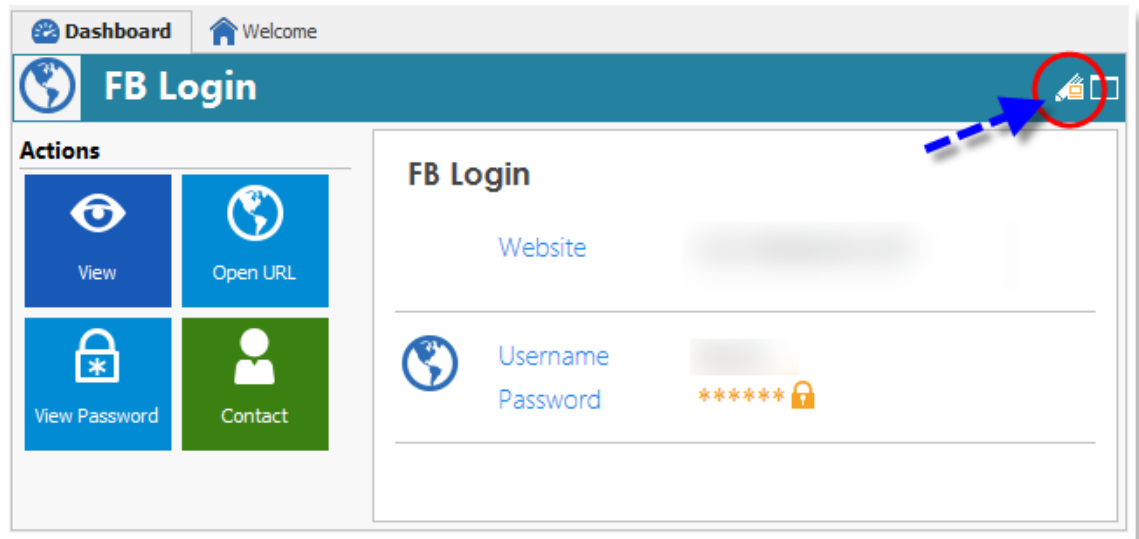
Local Machine Specific Settings



Context Menu

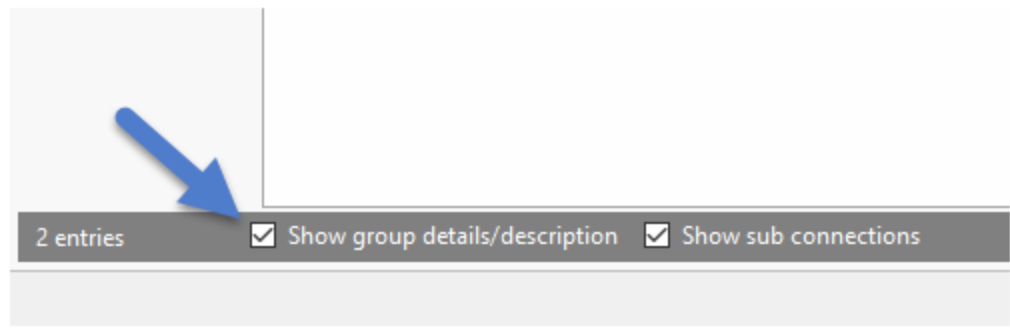
Local Machine Specific settings indicator

For entries with defined **Local Machine Specific Settings** an indicator appears in the dashboard when you select the entry. You can simply click on the indicator to go to the **Edit Entry (Local Machine specific settings)** dialog.



Local Machine Specific Settings

For Groups/Folders, you must have enabled the **Show group details/description** option to see the indicator.

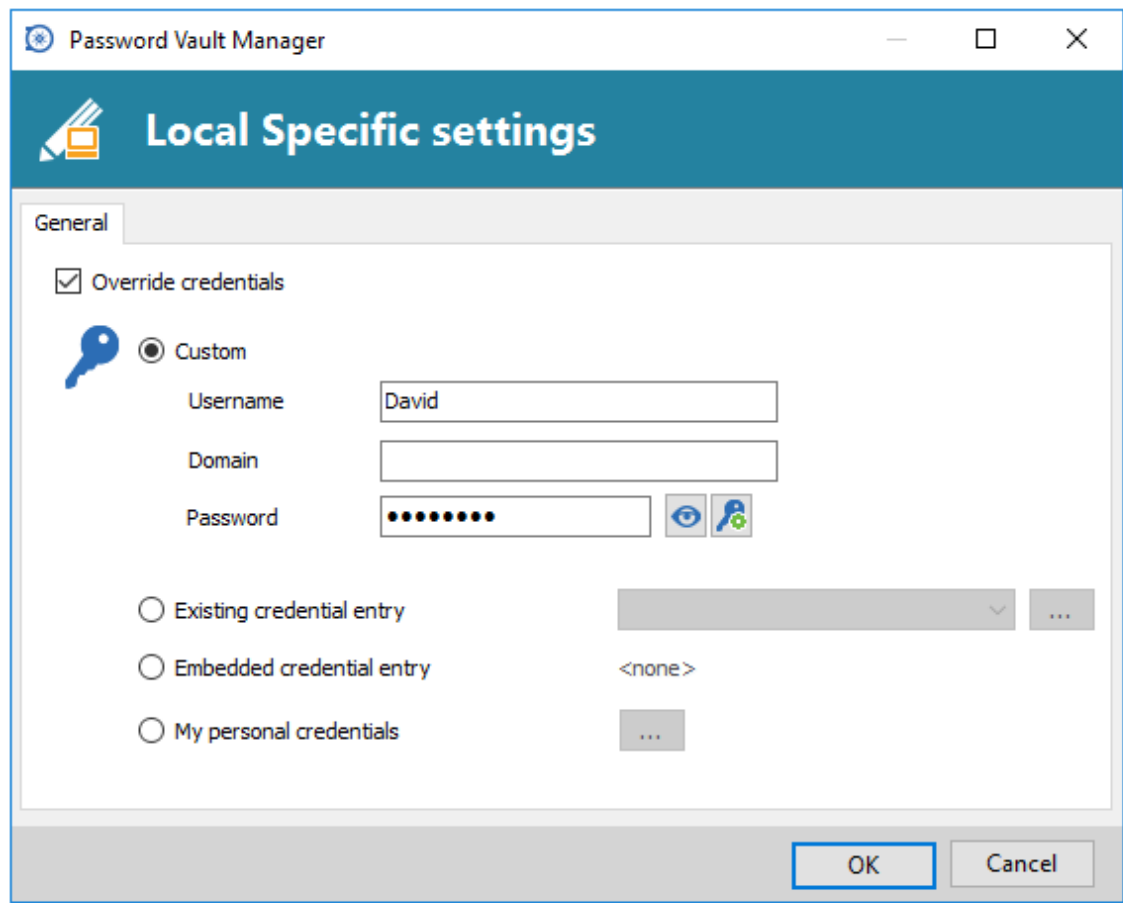


Show Group Details/Description

Workflow

Sessions and Groups/Folders

This dialog will appear.



Local Specific settings

Please consult each specific override topics for more information:

- [Credential Entry Overriding](#)
- [Credentials](#)

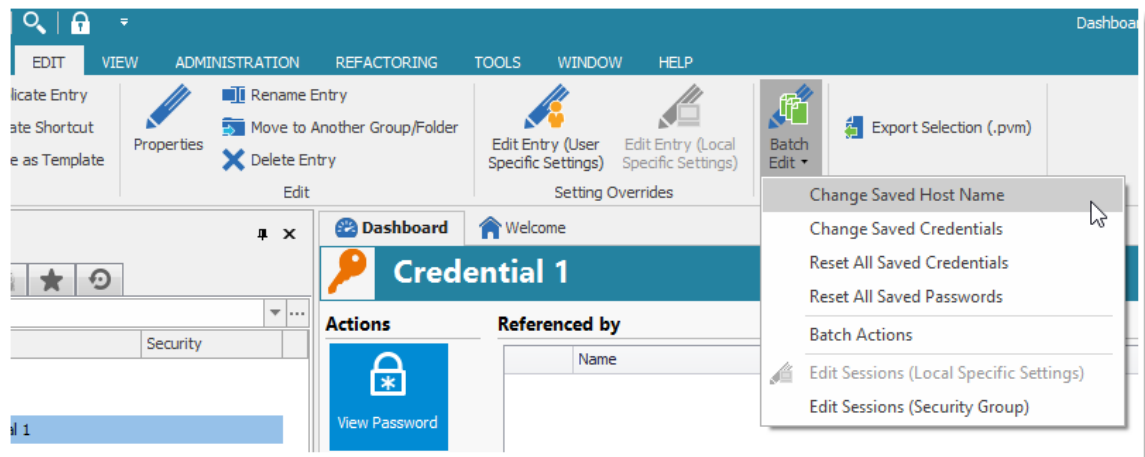
Credentials Entries

In the case of credential entries, please refer to [Credential Entry Overriding](#).

3.3.4 Batch Edit

Description

Batch Edit is used to change the settings of multiple entries in one operation. This option can be found in the entry context menu and in the Edit ribbon. It can be used for example to remove or update all of the credentials of a group of sessions.



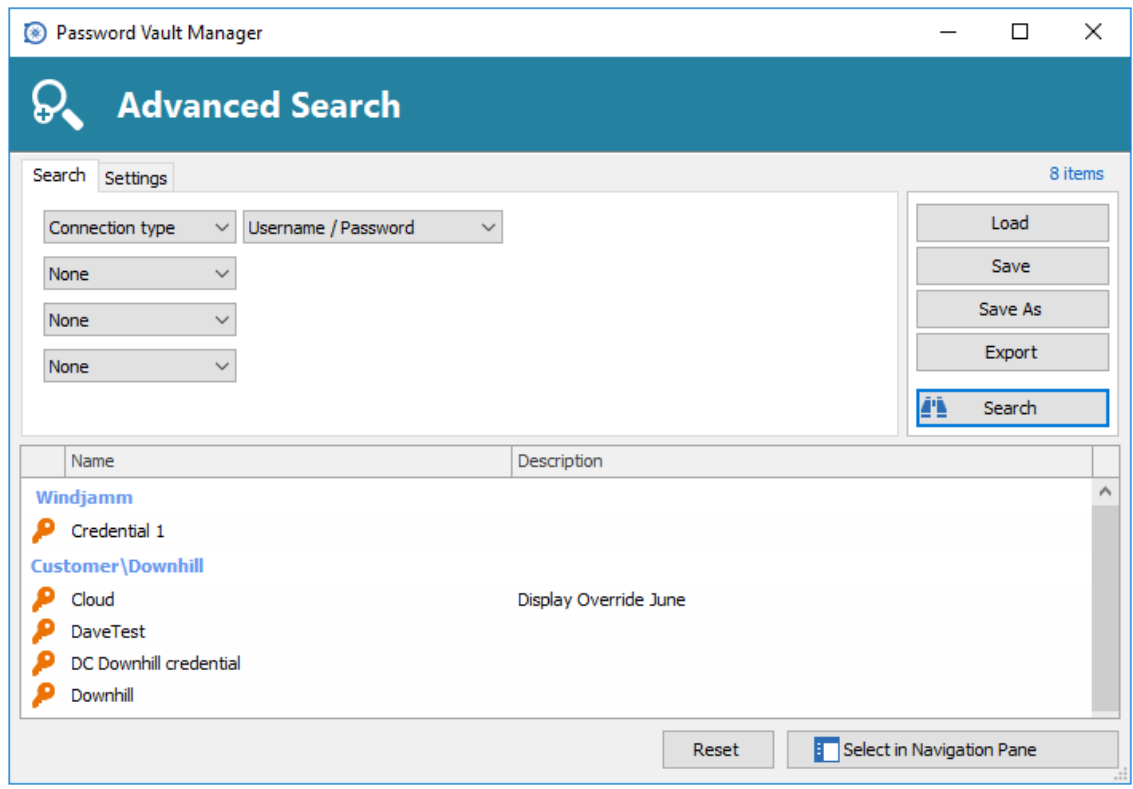
Edit - Batch Edit

You can change:

- the Host name;
- the credentials;
- reset passwords;
- the local specific settings (if using a local data source); or
- the assigned security group (if using an advanced data source)

Simple, yet effective

You can multi-select entries by using the usual CTRL, SHIFT, mouse clicks, etc. For a method with a little more power, use our Advanced Search dialog, accessible from View - Advanced Search. The **Advanced Search** allows you to select multiple criteria at once.



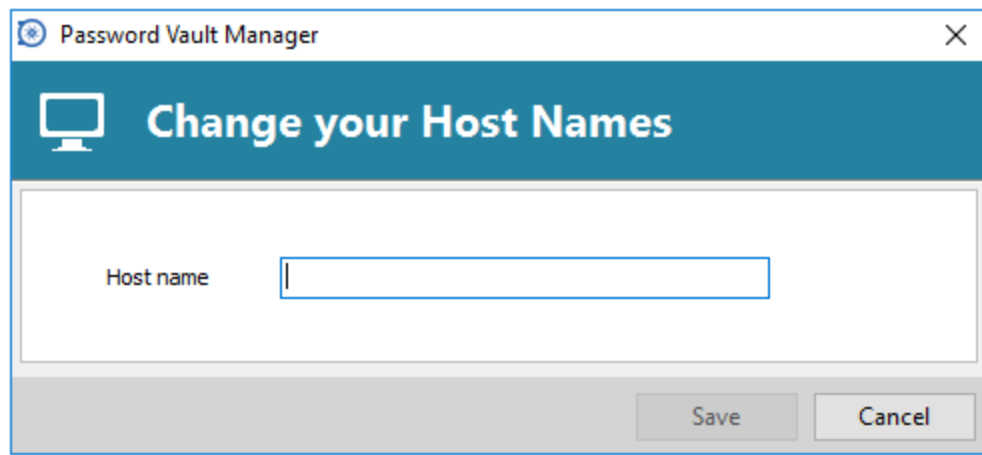
Advanced Search

After you have tweaked your criteria to get the results you want, press on **Select in Navigation Pane** and then **Edit - Batch Edit**.

Settings

Change Saved Host Name

Change Saved Host name is used to change multiple host names simultaneously.



Batch Edit - Change Host Names

Change Saved Credentials

You can change the configured credentials for multiple sessions in a batch.

Batch Edit - Change your credentials

Option	Description
Use specified credentials	Use a specific user name, password and domain.
Use credential repository	Use a Credential entry linked entry which can be external credentials like KeePass for example. This is very useful for sharing or reusing existing credentials among entries.
Use inherited	Inherit the credentials of the parent entry or group.
Use my personal credentials	This allows you to use one set of credentials to replace or emulate the ones from your Windows session. See My Personal Credentials topic.
Use private vault search	Enter the search string of your private vault .
None	No credential will be define for the entry, you will be prompted for credentials every time you connect.

Reset All Saved Credentials

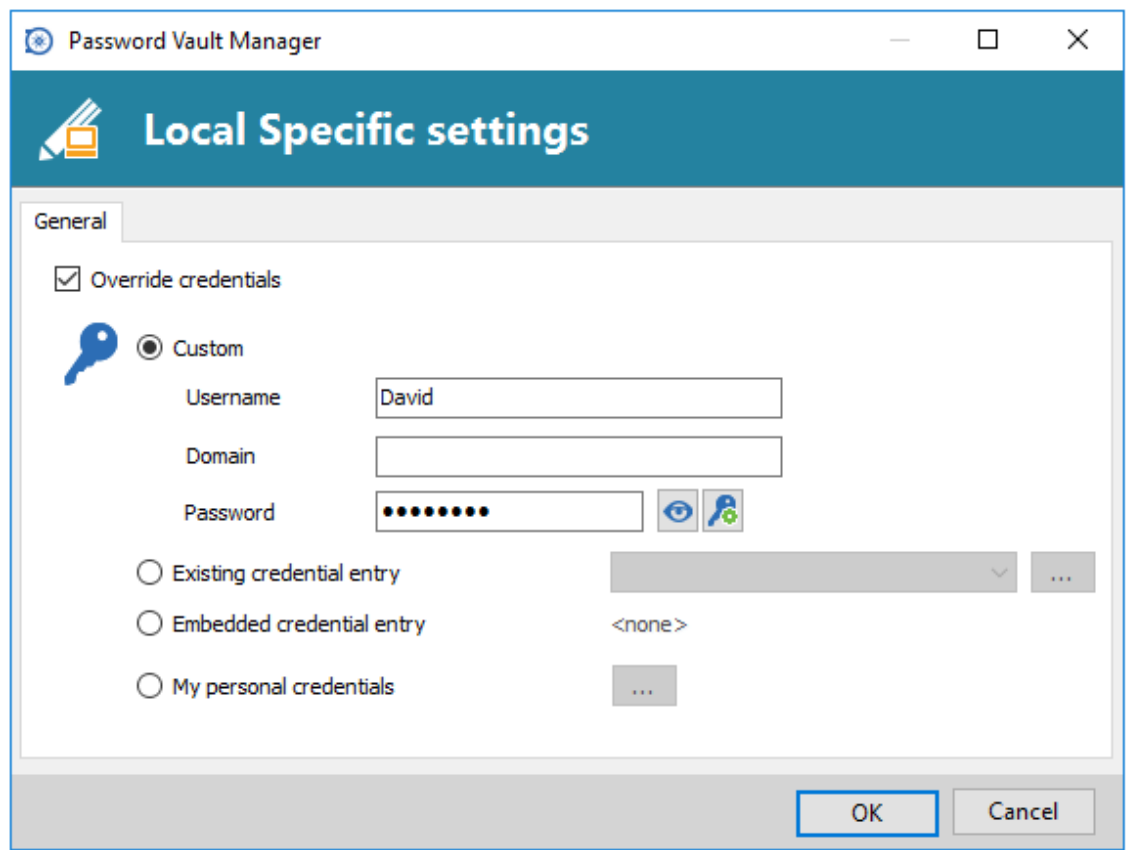
This will clear the existing credentials for all the selected sessions.

Reset All Saved Passwords

This will clear the existing passwords for all the selected sessions.

User-specific Settings

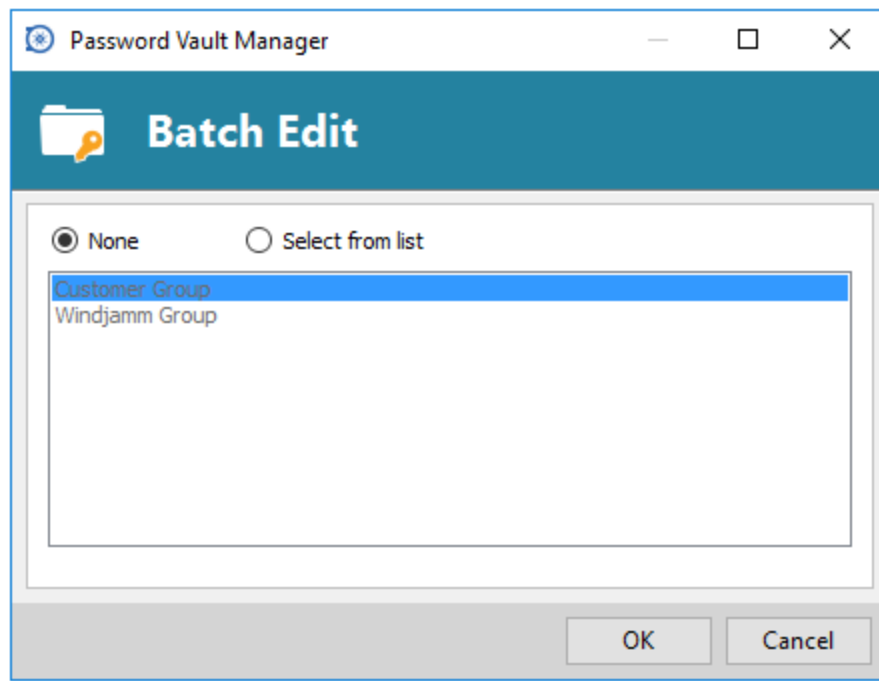
User-specific settings can be modified in a batch if they're supported by the type of session. To change user-specific sessions go to ***Batch Edit - Edit Sessions (User Settings)...***



Batch edit - User specific settings

Security Group

To apply a new security group to multiple sessions, use the menu ***Batch Edit - Edit Sessions (Security Group)...***



Batch Edit - Security Group

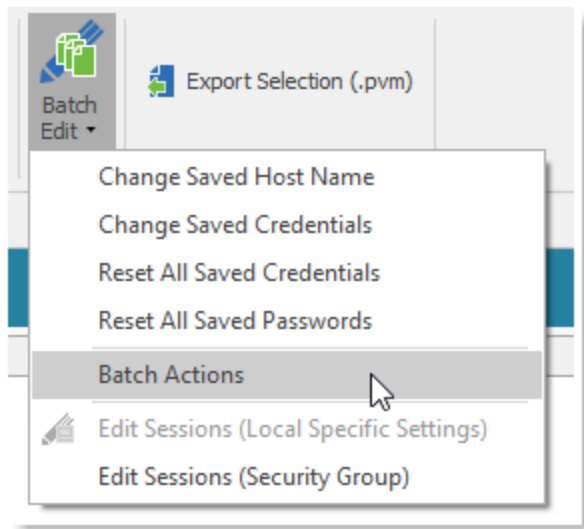
Batch Actions

For more information on the Batch Actions please follow this [link](#).

3.3.4.1 Batch Actions

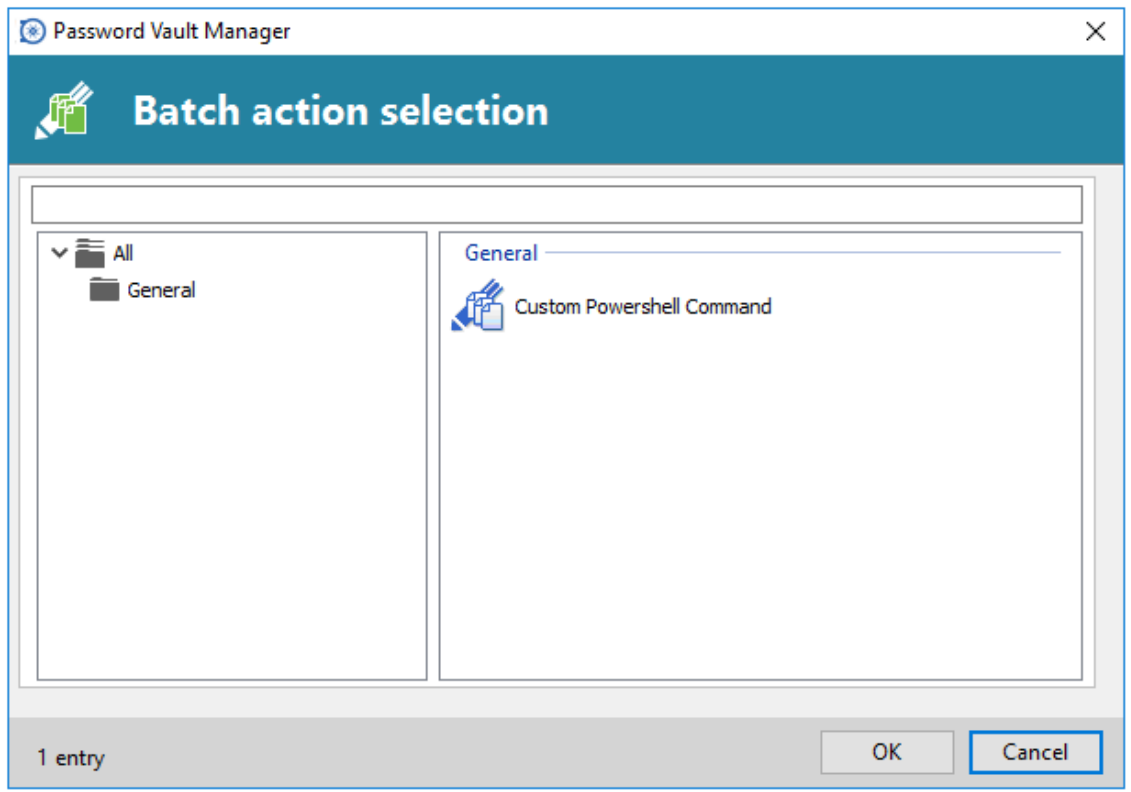
Description

Use the ***Edit - Batch Edit - Batch Actions*** to change the settings of multiple sessions in one operation. It can be used for a batch action command on a group of sessions.



Batch Actions

Settings



Batch Edit - Batch Action

Custom Powershell Command

Run a custom Powershell command on multiple selected sessions all at once to update the properties.

3.3.5 Export

Description

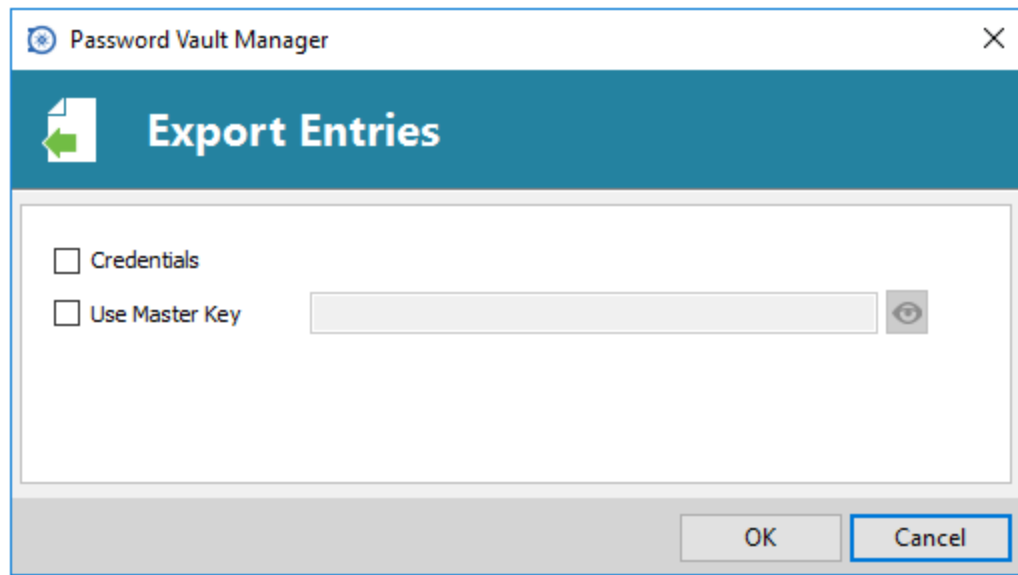
Use the **Export** options to export selected entries from Remote Desktop Manager.



Edit - Export selection

Settings

Use the **Export Selection (.pvm)** to export your selected entries in a .pvm file that can then be imported into any Password Vault Manager data source. You can elect to include your entries credentials in your export format and secure your file with a Master Key.

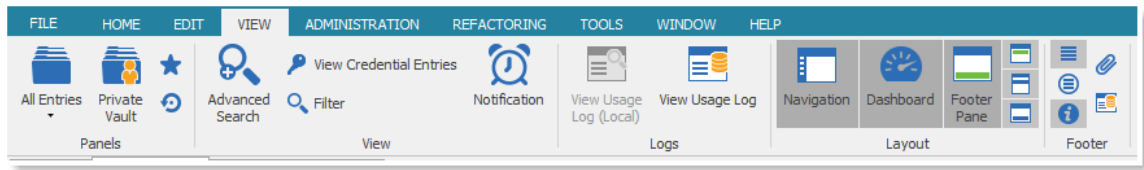


Export Entries

3.4 View

Description

The **View** ribbon is used to control multiple features regarding the views, layout and logs for Password Vault Manager.



Ribbon menu - View

Refer to the following topics for more information:

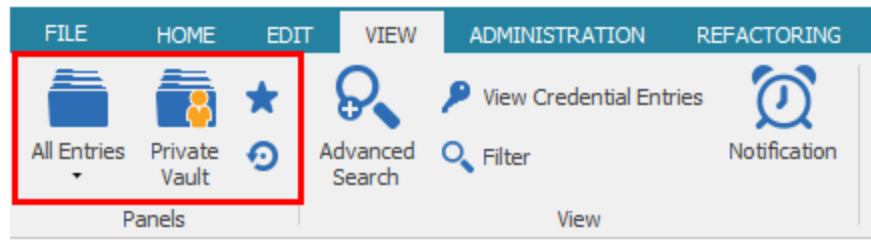
- [Panels](#)
- [View](#)
- [Logs](#)
- [Layout](#)
- [Footer](#)

3.4.1 Panels

Description

That section of the ribbon controls the state of the Navigation Pane.

Settings



View - Panels

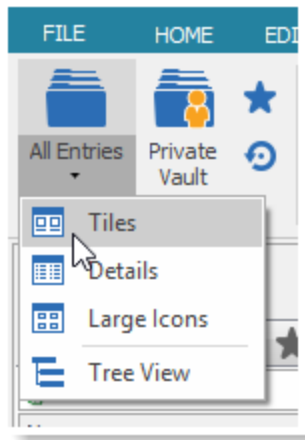
Refer to the following topics for more information:

- [All Entries](#)
- [Private Vault](#)
- [Favorite Entries](#)
- [Most Recently Used Entries](#)

3.4.1.1 All Entries

Description

All Entries is the default view and lists all existing entries. The visual structure can be in a list format or tree view.



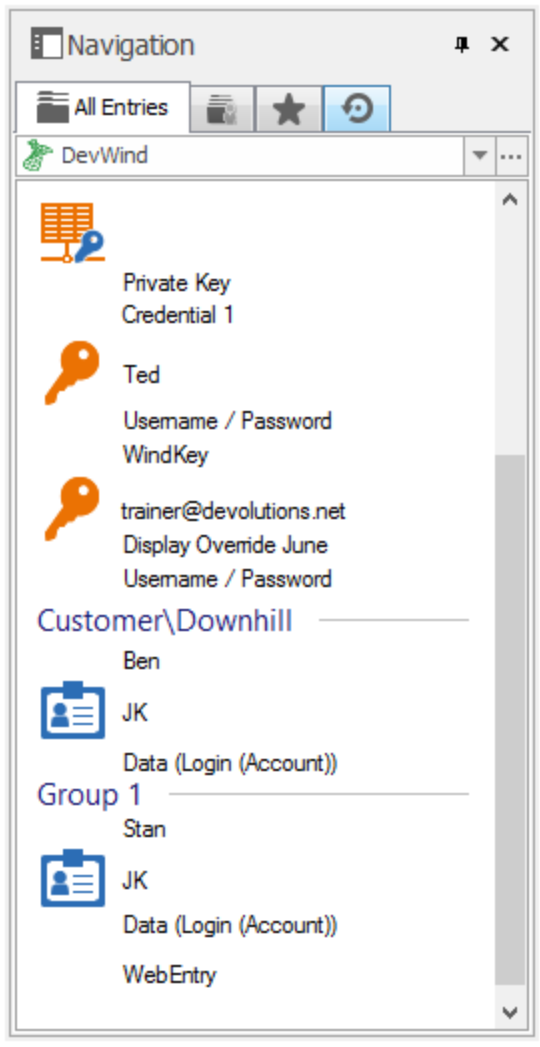
Session views

The list contains a large number of entry configurations. Use the filter box at the bottom of the screen to help you find what you need. Learn more about this feature [here](#).

Settings

Tiles

The Tiles view displays the sessions to see all of them next to one another.



Tiles view

Details

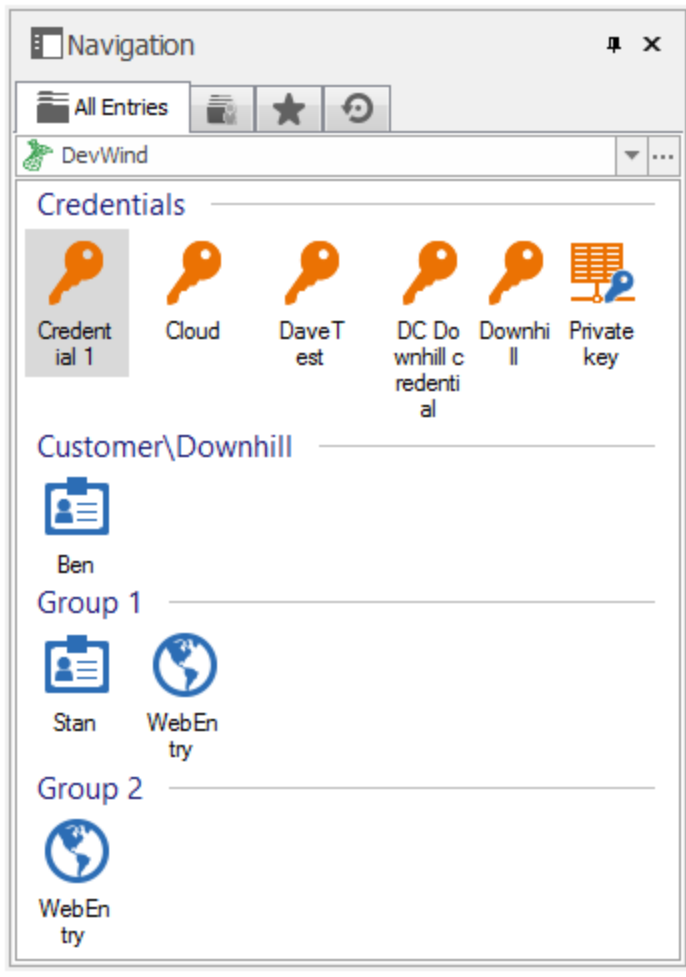
The Details view displays multiple details on each sessions.

Name	Parameter	User	Description	Type
Credentials				
Credential 1		Test		Username / Password
Cloud		jknafo@devoluti...	Display Override June	Username / Password
Dave Test		David		Username / Password
Downhill		David		Username / Password
Privatekey				Private Key
Credential 1		Test		Username / Password
Ted		Ted		Username / Password
Customer\Downhill				
Ben		JK		Data (Login (Account))
Group 1				
Stan		JK		Data (Login (Account))
WebEntry				Data (Login (Web))
Group 2				
WebEntry				Data (Login (Web))

Details view


Large Icons

The Large Icon view displays sessions with large icons.

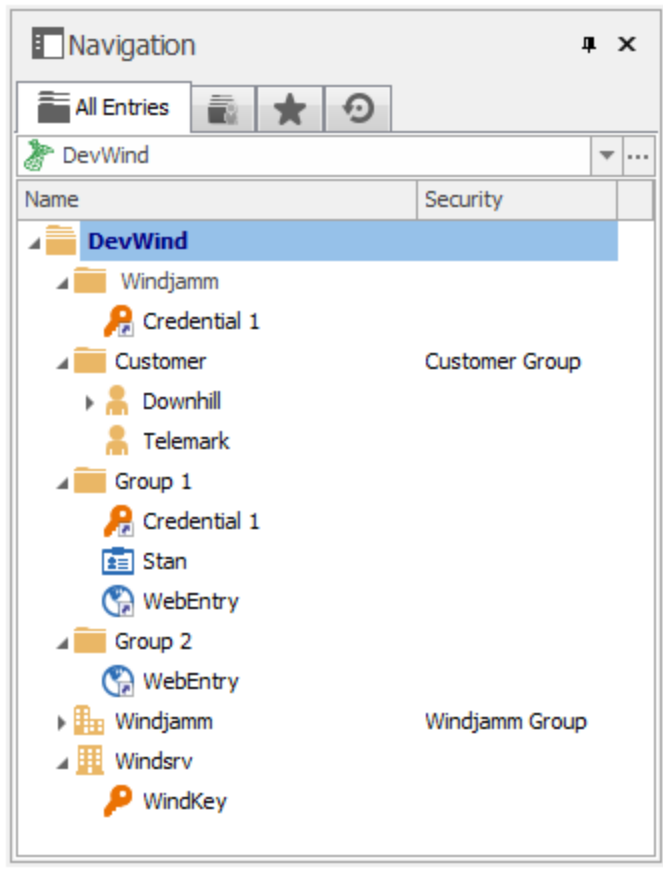


Large Icons view

Tree View

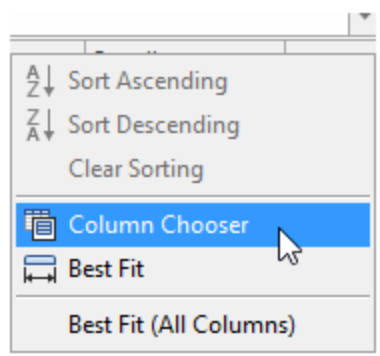

Use the F7 shortcut (default shortcut) to change the entry view to tree view

The tree view offers the most flexible display mode. By focusing the control, you can activate the incremental search by typing letters and numbers. Use **Ctrl+Up/Down** to move to the next or previous matching entry and **Backspace** to delete the current incremental search.



All Entries - Tree View

It's possible to specify the visible columns in the tree view. Columns can be added in the Navigation Pane by right-clicking on the column **Name** in the **Navigation Pane** and selecting **Column Chooser**.



Column Chooser

The following columns can be added:

- Description
- Expiration
- Host
- Ping

- Security
- Status
- Status Message
- Type
- Username

3.4.1.2 Private Vault

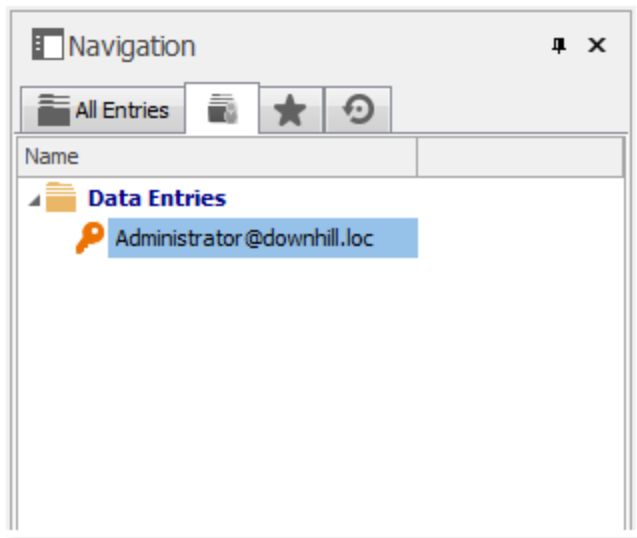
Description

The **Private Vault** is a user centric repository for entries of any type. It allows each user to create entries that only them can access and use the [User Specific Settings](#) to use link your Private Vault credential to an entry.



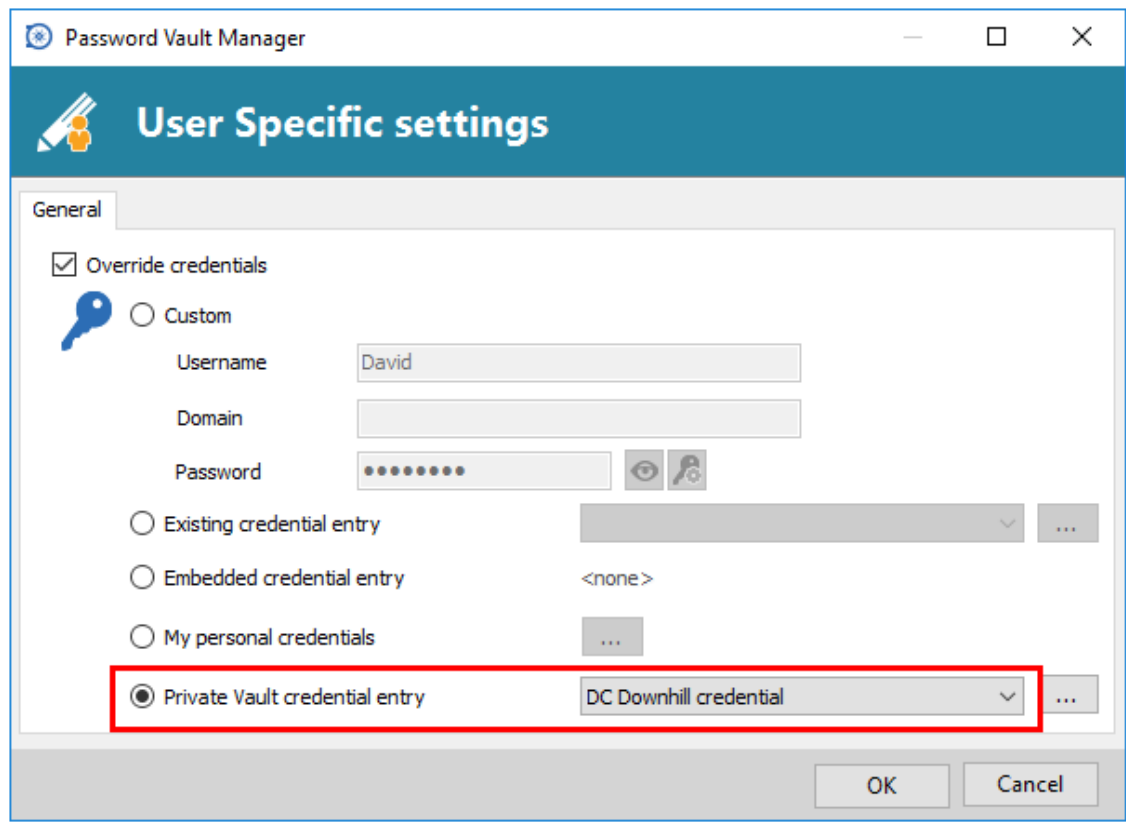
This feature requires an [Advanced Data Sources](#).

1. Create your Credential entry in your Private Vault.



Private Vault

2. Edit your entry using the **User Specific Settings** and select **Private Vault** and then select your Private Vault credential from the drop down.



User Specific Settings - Private Vault credential entry

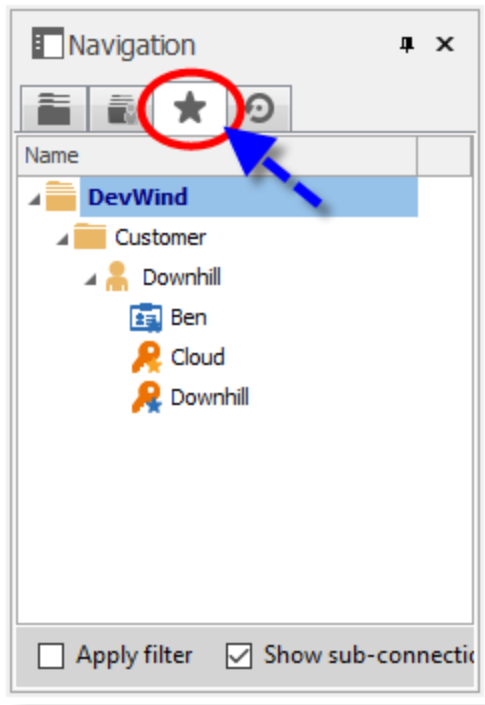
Keep in mind that the Private Vault is in fact contained in the user area of the database. It must be used from within itself, or by using our extension mechanism that is user specific.

3.4.1.3 Favorite Entries

Description

Favorite Entries view contains all of your favorite entries that have been configured in the current data source.

This is useful when the number of managed entries becomes too great or if you must maintain a strict directory structure to hold your entries. To learn more please see [Favorites](#).

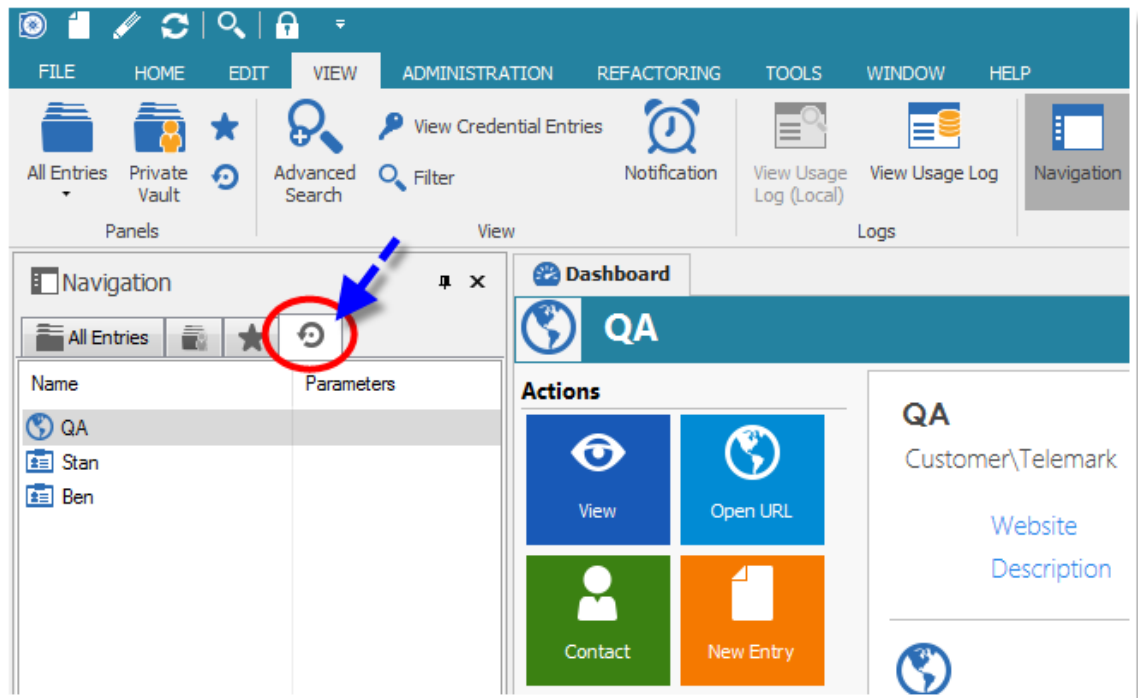


Favorite Entries

3.4.1.4 Most Recently Used Entries

Description

This view show the most recently used entries for a specific data source on the local computer.

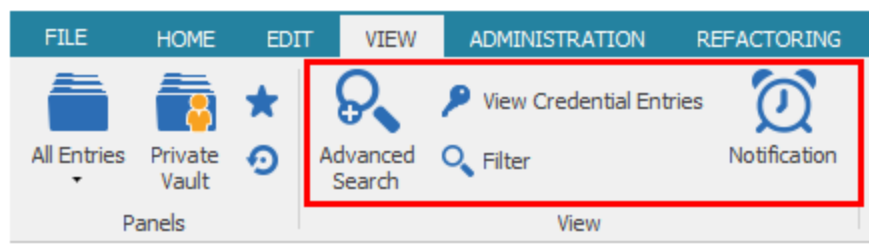


Most recently used entries

3.4.2 View

Description

The **View** section allows access to specialized screens that show only a subset of your entries. These are useful mainly for installations with a great number of entries.



Ribbon View - View

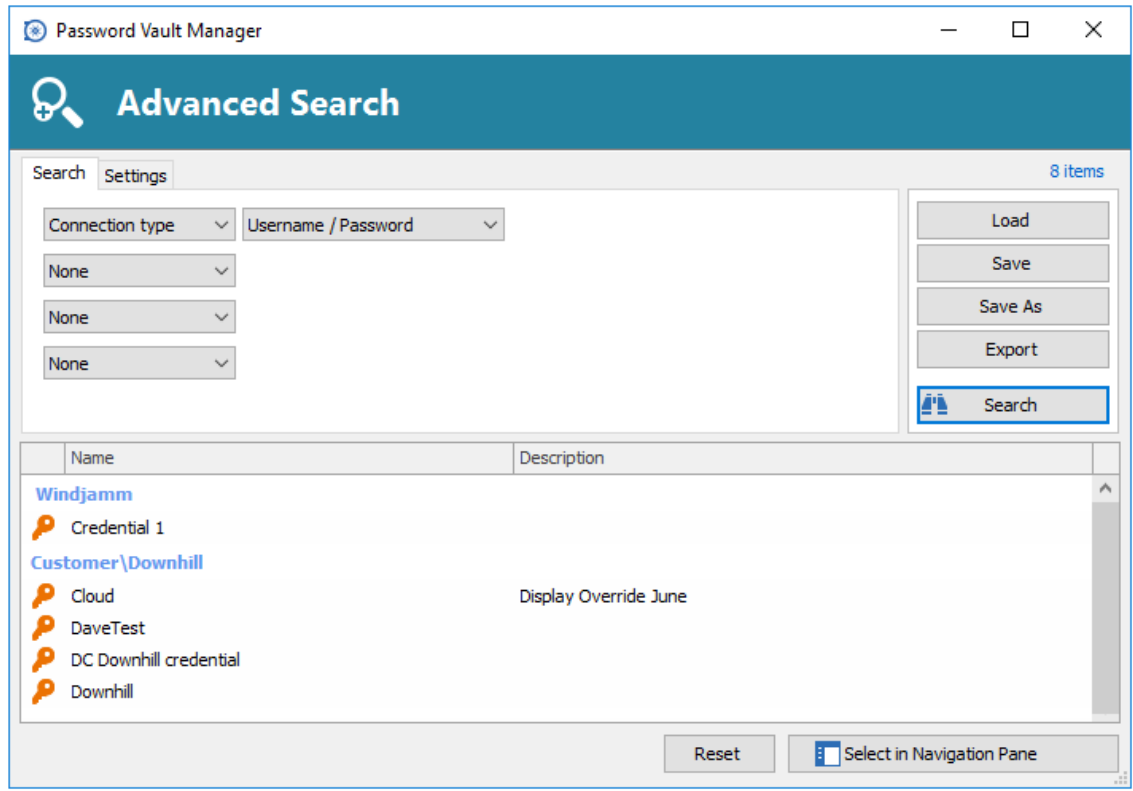
Refer to the following topics for more information:

- [Advanced Search](#)
- [View Credential Entries](#)
- [Filter](#)
- [Notification](#)

3.4.2.1 Advanced Search

Description

The **Advanced Search** feature allows you to search for multiple criteria at once.



Advanced Search - Search tab

Settings

Search

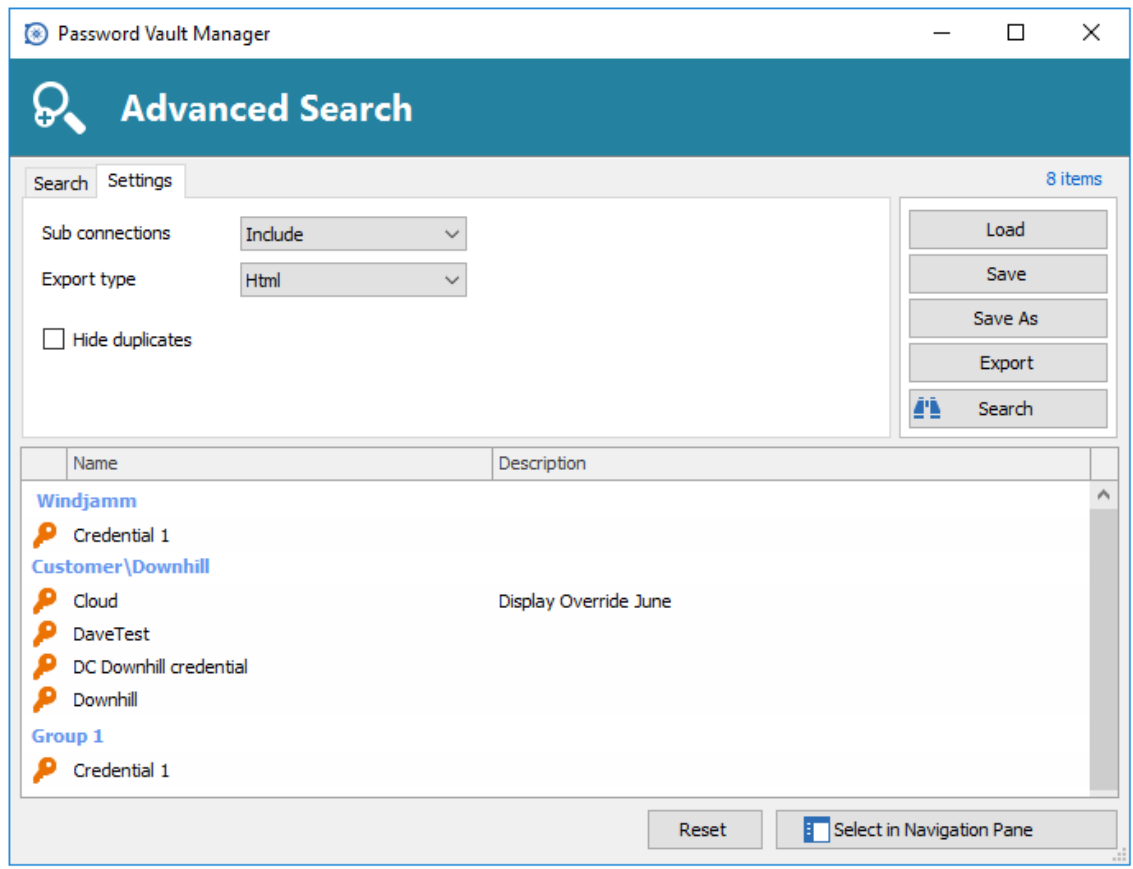
Option	Description
Search option	<p>You can select between different criteria to tweak your search:</p> <ul style="list-style-type: none"> • Connection type • Contact Reference • Creation date • Custom field • Description • Domain • Group • Host • Is favourite • Keywords/tags • Last update date • Name • OS

	<ul style="list-style-type: none"> • Password strength • Security group • Status • Username
Load	Load searches that has been previously saved.
Save	Allows you to save your search locally and reuse it.
Save as	Use to save a previously saved search but under another name.
Export	Export the entries of your search result as a Csv, Html, Xls or Xml file. Sensitive information will be encrypted using AES.
Search	Once you have selected your search criteria click on Search to display the search result.
Reset	Reset all your fields to proceed with a new Search.
Select in Navigation Pane	Select your search result in your Navigation Pane. This option can be used in combination with a Batch Edit .

There will be a drop-down list next to certain Search options (ex: **Name**) to give you more define search options.

Option	Description
Contains	Find any name that includes the characters you have entered, anywhere in the field name.
Starts with	Find any name beginning with the characters you have entered.
Ends with	Find any name ending with the characters you have entered.
Exact Expression	Find names that matches every character you have entered, exactly as entered.

Settings



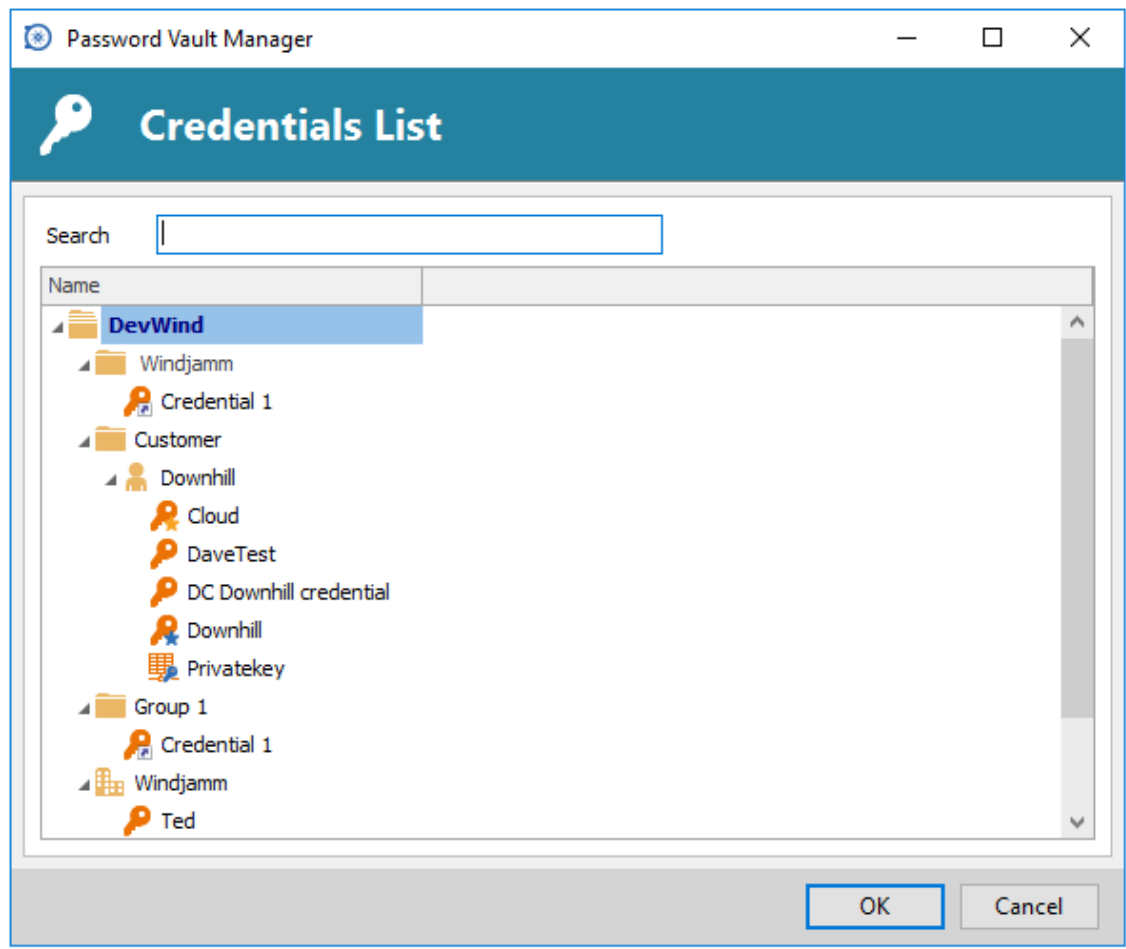
Advanced Search - Settings tab

Option	Description
Sub connections	Select if you wish for the sub connections to be included in the search, the options are: <ul style="list-style-type: none"> • Include (include sub connections in your search result) • Ignore (ignore all sub connections in your search result) • Exact match (only include the sub connections if exact match to the search)
Export type	Select your export type between: <ul style="list-style-type: none"> • Csv • Html • Xls • Xml
Hide duplicates	Hide duplicates in your search result.

3.4.2.2 View Credential Entries

Description

The **View Credential Entries** allows you to quickly generate a list including every credential entry held in your data source.

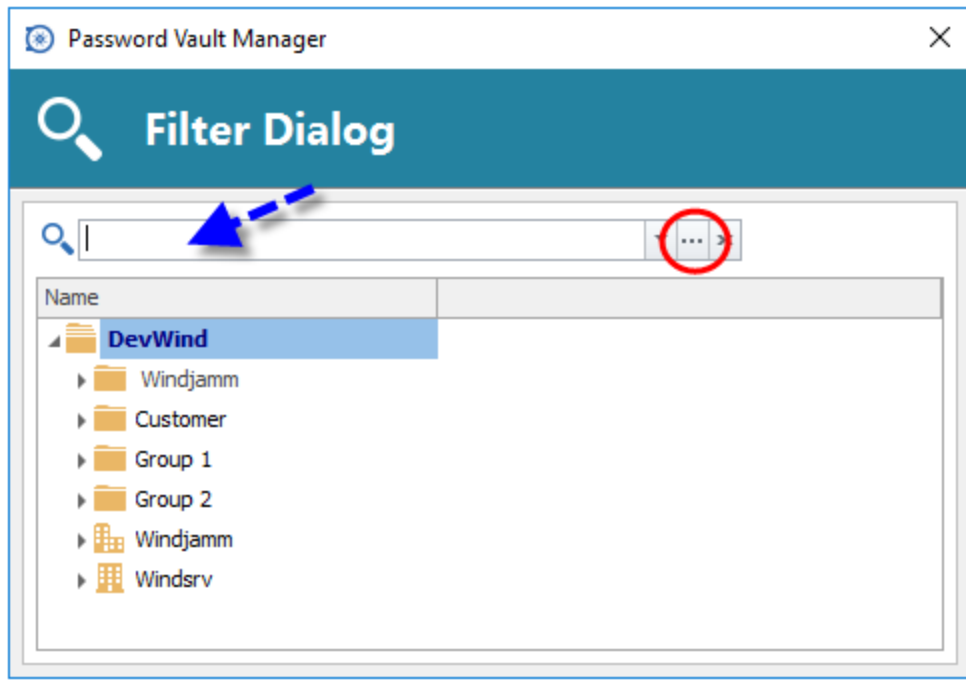


Credential List

3.4.2.3 Search/Filter

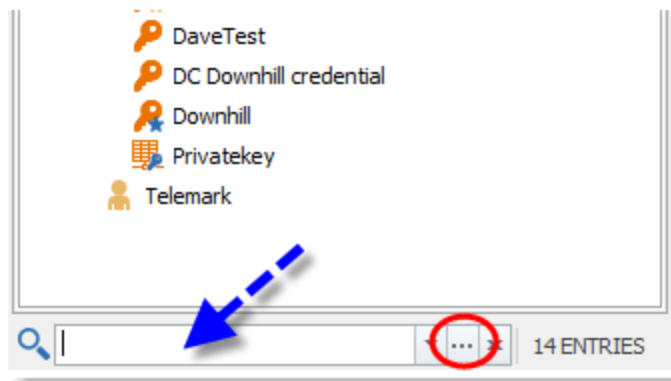
Description

The **Filter** allows you to type in the Filter Dialog thus making an easy and quick search throughout your Navigation Pane. Select the **ellipsis** button to display the options.



Filter Dialog

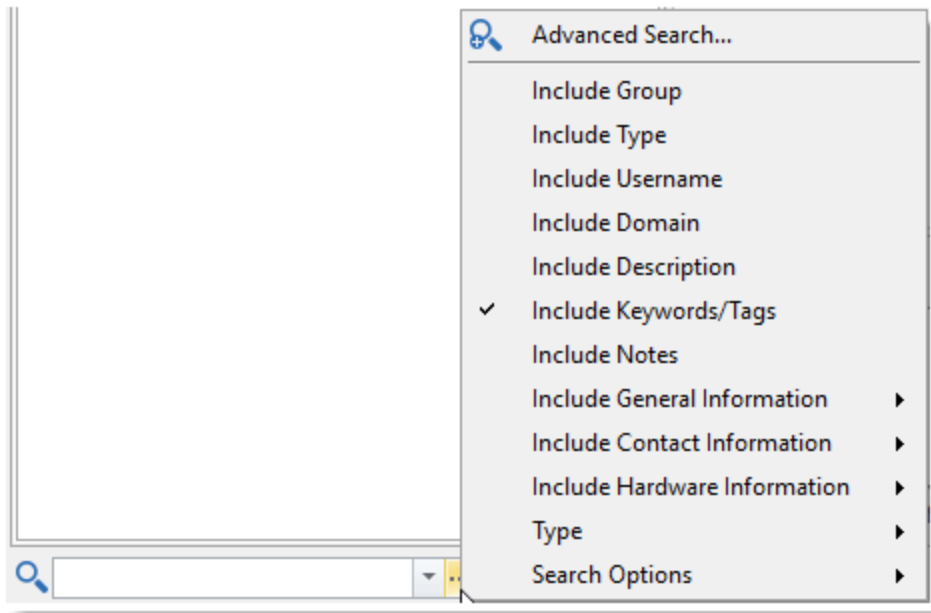
The **Search/filter** below the entry list will also filter your entries in the Navigation Pane. Select the **ellipsis** button to display the options.



Search/Filter

Settings

Select the ellipsis button to display the options.

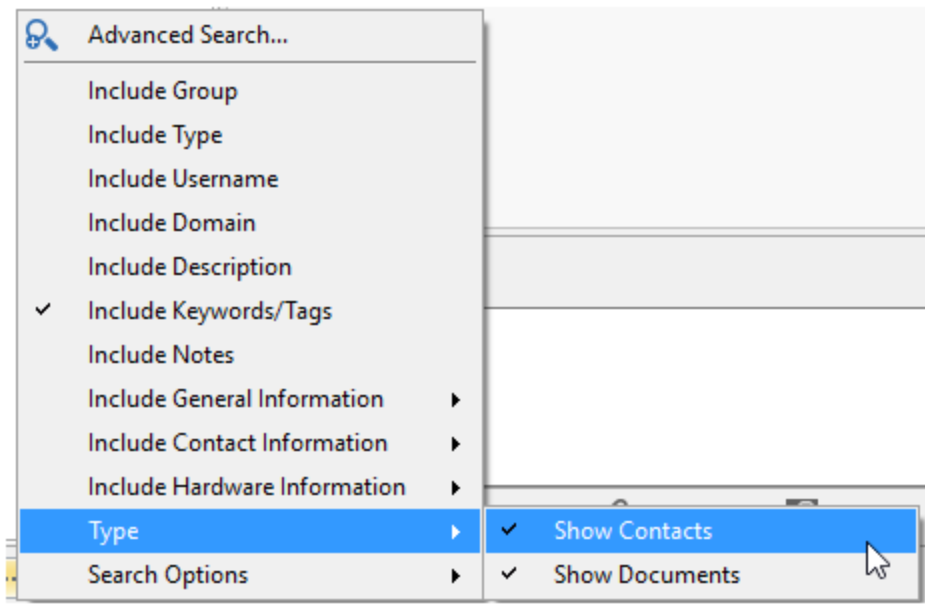


Search/Filter options

The filter expression is matched against fields as selected in the filter options such as:

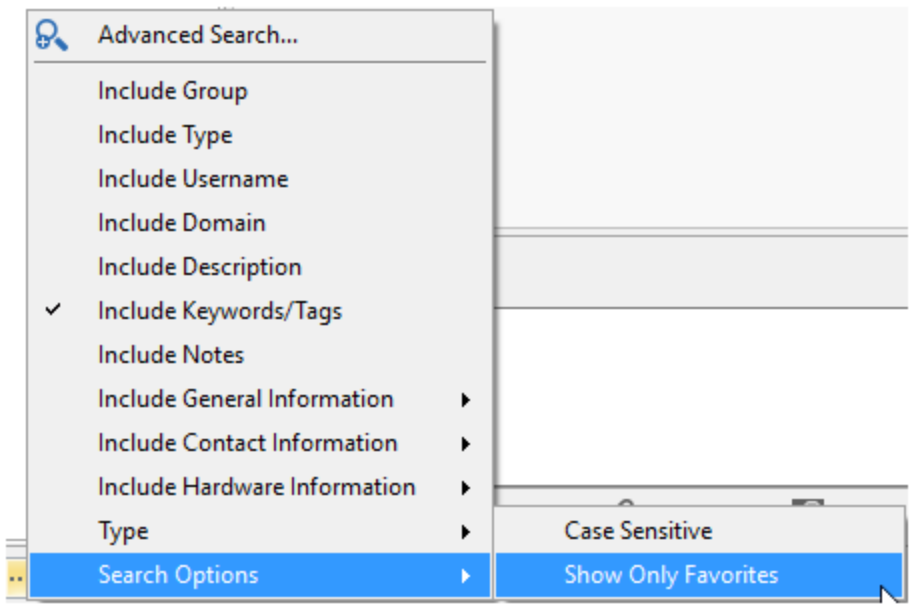
- Group
- Type
- Username
- Domain
- Description
- Keywords/Tags
- Notes
- General Reference
- Contact Information
- Hardware Information
- Sub Connections
- Various Contact information fields (choose them in the sub menu)

A **Search Type** can be executed to include Contacts and Documents.



Search Type

The **Search Options** will offer you the possibility to show only the favorites and/or make the search case sensitive.



Search Options

Keyboard Shortcut

Use the keyboard shortcut CTRL+F to quickly have access to the Search/Filter control. This can be disabled in **File - Options - User Interface - Keyboard**.

You can set the focus back on the Navigation Pane by using the keyboard shortcut Ctrl+L, this also can be disabled in the options.

Boolean Filter

Here a few implementation notes for the Boolean filter:

- We use the C# nomenclature (&& for AND, || for OR)
- Evaluated left-to-right
- No parentheses matching
- Double-quotes (") are not required or removed, they are part of the text filter, do not use them unless you are looking for a double-quote.
- Leading/trailing white-spaces are trimmed

Examples (this will work)

- Boise && Laptop
- Boise&&Laptop
- Boise && Laptop
- Baton Rouge || Boise && Laptop
- Laptop && Baton Rouge

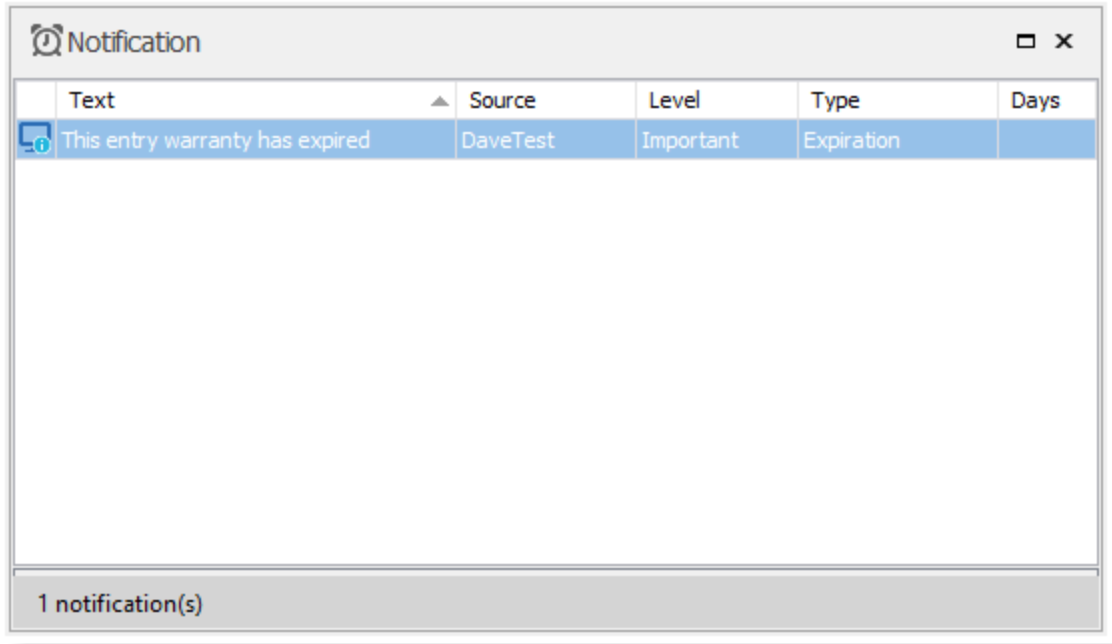
Examples (this will not work as expected)

- Laptop && "Baton Rouge"
 - Will work but filter for the string "Baton Rouge" and not the string Baton Rouge
- Laptop && (Baton Rouge || Boise)
 - Will work but filter for Laptop and the string (Baton Rouge || Boise)

3.4.2.4 Notification

Description

If you have defined an expiration date for an entry (example: a warranty expiration date), the **Notification** quickly generates a list including all notification of expiration from your data source.



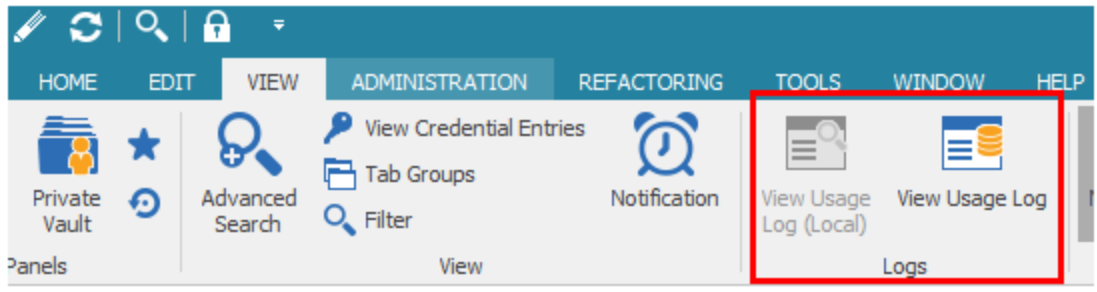
Notification

3.4.3 Logs

Description

Password Vault Manager supports two types of logs: the Local Usage log, which is a file based log, and the Usage log, which is in a database.

Settings



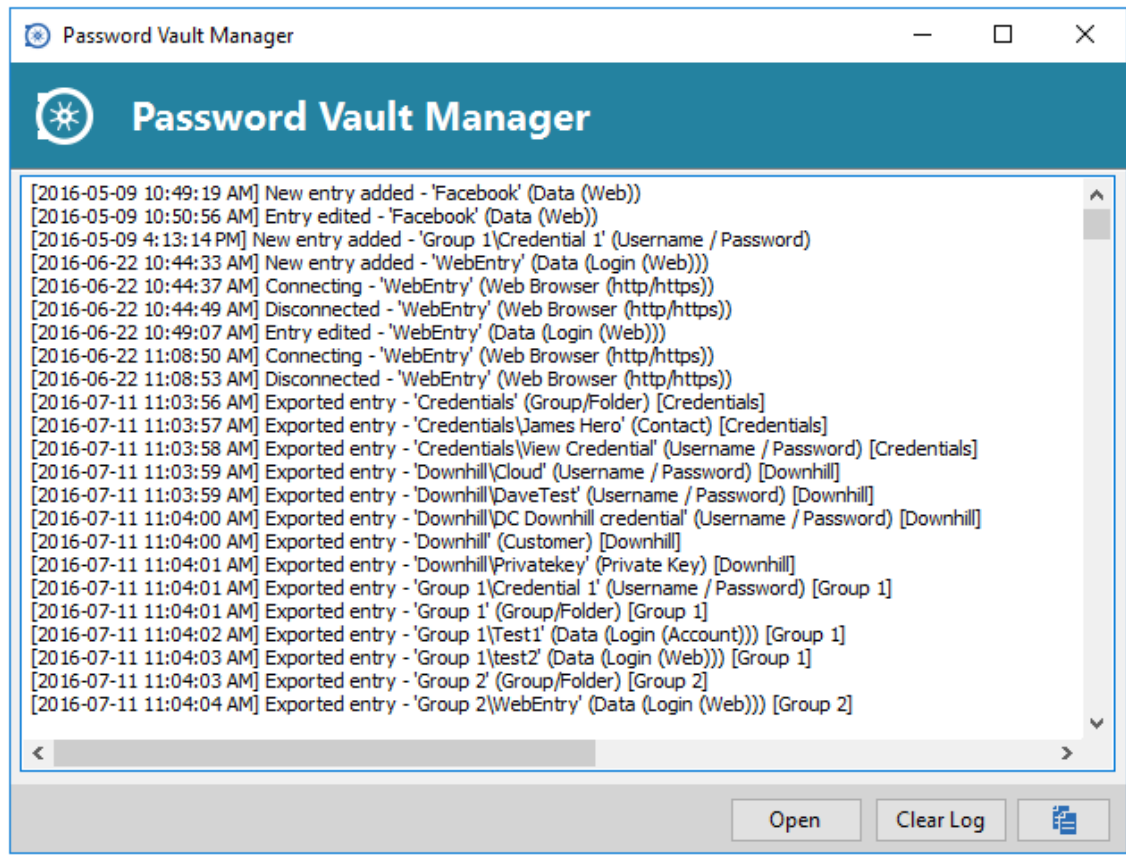
Logs

3.4.3.1 Usage Logs (Local)

Description

A basic local logging system is automatically available by default. This allows the system administrator to view the log file for all entry activities on the current machine. It's available on the local machine only via the menu **View Usage Log Local**. The Usage Logs (Local) is only available for Local data sources (ex: XML)

The log is written directly in a file in the settings folder and/or in the database.



Local connection log

3.4.3.2 Usage Logs (Global)

Description

The shared entry log offers a more robust solution. Through it, it's possible to monitor an opened entry for all users by using the [SQL Server](#) or the [Online Database](#). The logs are available for a specific entry in the context menu **View - Logs**, in the entry configuration (Log tab page), and in the dashboard.

Settings

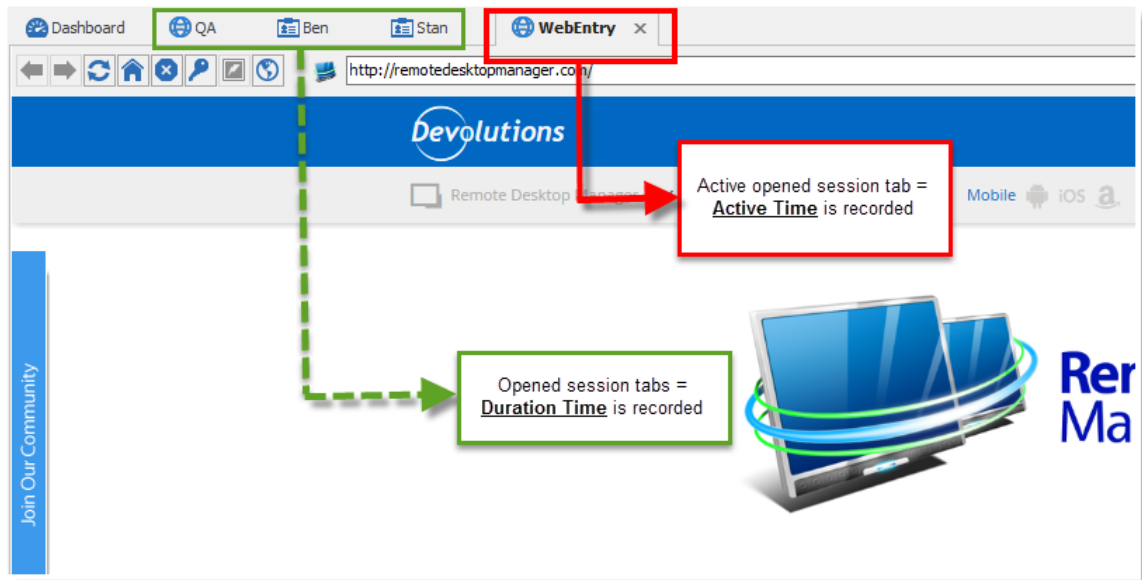
The log contains all the CRUD (add, edit and delete) operations, including the time and the username. It also contains all the details about the open/closed entries.

Group	Connection	Message	On Open Comment	On Close Comment	Log Date	End Date/Time	Active Time	Duration	User	Database User...	Connection User	Machine	Connection Type
Customer'D...	DaveTest	Entry edited			2016-07-18 3:5...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Group 1; Win...	Credential 1	Entry edited			2016-07-14 1:5...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Group 2;Gro...	WebEntry	New entry shortcut added			2016-07-14 1:4...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Group 2;Gro...	WebEntry	Entry edited			2016-07-14 1:4...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Group 1	test2	Entry deleted			2016-07-14 1:4...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Customer'D...	Downhill	Entry edited			2016-07-14 10:...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Customer'D...	Ben	Entry edited			2016-07-14 10:...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Customer'D...	Ben	Entry edited			2016-07-14 9:0...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Customer'D...	Ben	Entry edited			2016-07-14 9:0...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Customer'D...	Ben	Copied password to clipboard			2016-07-13 3:3...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Customer'D...	Ben	Copied user name to clipboard			2016-07-13 3:3...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Group 1	test2	Viewed the data entry			2016-07-13 2:3...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
WebEntry	Open session	Open session			2016-07-13 2:3...	2016-07-13 2:3...	5 sec	4 sec	VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Web Browser (Http/Http...)
WebEntry	Open session	Open session			2016-07-13 2:3...	2016-07-13 2:3...	8 sec	9 sec	VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Web Browser (Http/Http...)
Group 2	WebEntry	Entry edited			2016-07-13 2:3...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Group 2	WebEntry	Entry edited			2016-07-13 2:3...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Windsrv	Windsrv	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Company
Windsrv	WindKey	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Windjam	Windjam	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Site
Windjam	Ted	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Group 2	WebEntry	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Group 2	Group 2	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Group/Folder
Group 1	test2	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Web))
Group 1	Stan	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Data (Login (Account))
Group 1	Group 1	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Group/Folder
Group 1	Credential 1	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Username / Password
Customer'Te...	Telemark	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Customer
Customer'D...	PrivateKey	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Private Key
Customer'D...	Downhill	Exported entry (Csv)			2016-07-13 2:2...				VDEVOLUTIONS56\jinafo	David		VDEVOLUTIONS56	Private Key

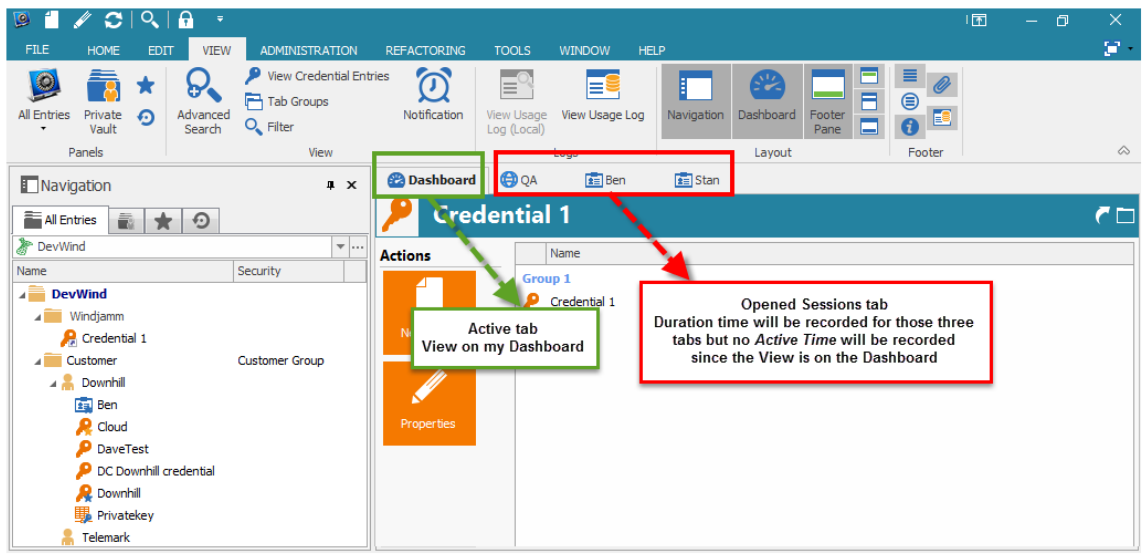
Usage Logs

Option	Description
Group	The Group/Folder where your entry is situated.
Connection	The connection being used to open your entry.
Message	Indicate the action that was done on your entry or session.
On Open Comment	The Open Comment is defined in the Log tab of your session.
On Close Comment	The Close Comment is defined in the Log tab of your session.
Log Date	Indicate the date and time your session was opened or your entry was edited.
End Date/Time	Indicate the date and time when the session or entry was closed.
Active Time	Only available for sessions in embedded mode. It will record your session active time, meaning the time your session was opened in embedded mode and you were active in your session. If your session is opened but your view is on your Dashboard tab and not on your session tab, no Active Time will be recorded. (Please see Note 1)
Duration	Only available for sessions in embedded mode. When sessions are opened in embedded mode the Duration time will be recorded, meaning that even if your view is on your Dashboard and you are not actively working in your session but your session tab is opened, Duration will record how long it was opened for. (Please see Note 1)
User	Indicate the Windows user name and domain.
Database username	Indicate the Windows user name and domain.
Connection user	Indicate the Connection user.
Machine	Indicate the machine name.
Connection Type	Indicate the connection type that was used.

Note 1



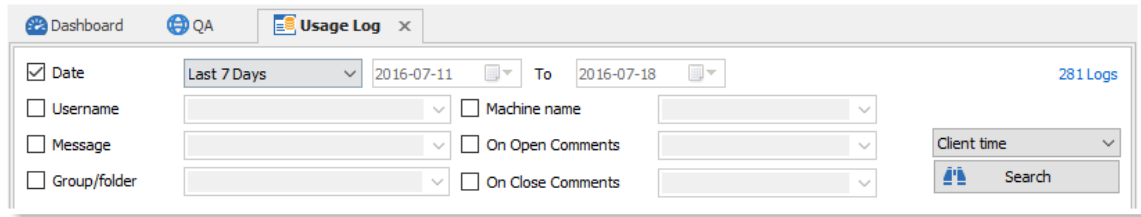
Web Entry Active Tab



Dashboard Active tab

Filter Usage Log

Some criteria's can be applied to filter the content of the grid like the machine name, the time period, the message, etc...

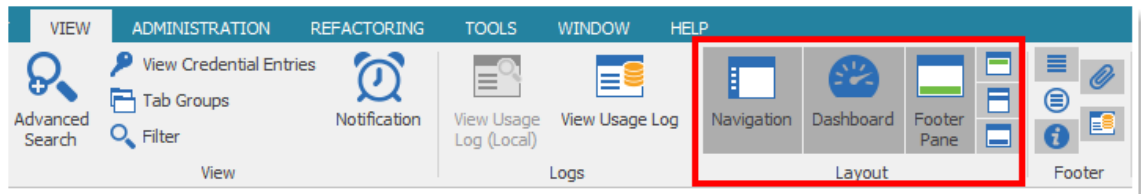


Usage


3.4.4 Layout

Description

The **Layout** section holds commands to control the layout of various Remote Desktop Manager components.



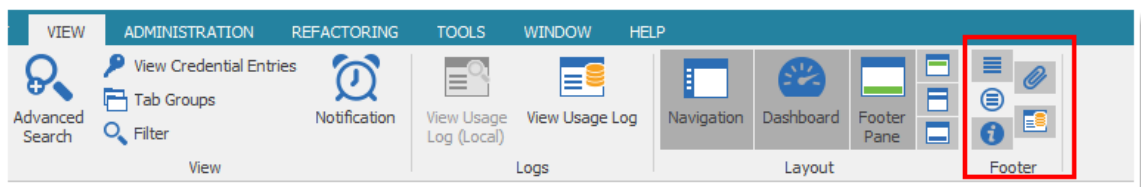
View - Layout

 If you hide the Top Pane and wish to restore it, using the keyboard shortcut ALT+F11 will toggle it's visibility.

3.4.5 Footer

Description

The **Footer** section allows you to show or hide the various panes that are provided with Remote Desktop Manager.



View - Footer

 Although they are by default displayed in the footer, all those panes can be dragged and docked anywhere within Remote Desktop Manager.

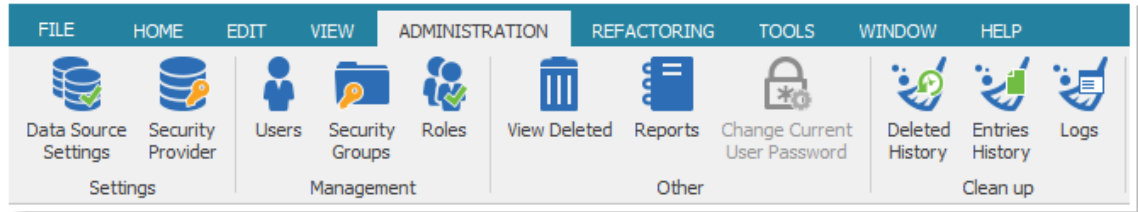
For more information please see the [View](#) topic.

3.5 Administration

Description

The **Administration** ribbon is **only available for Administrator of the data source** since it is mostly used to manage settings and users of a data source . If the options are grayed out contact your administrator.

Also most features contained in the Administration menu requires an [Advanced Data Sources](#).



Administration ribbon

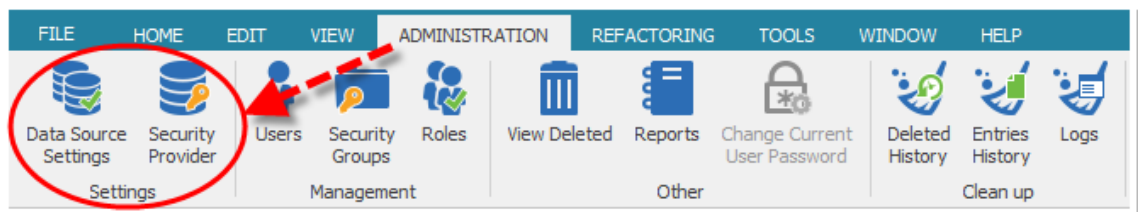
Refer to the following topics for more information:

- [Settings](#)
- [Management](#)
- [Other](#)
- [Clean up](#)

3.5.1 Settings

Description

The **Settings** menu includes the [Data Source Settings](#), which allows you to control many global aspects of the data source. This section also includes the [Security Providers](#), which is responsible for encrypting the data in your database.



Administration - Settings



These feature requires an [Advanced Data Sources](#).

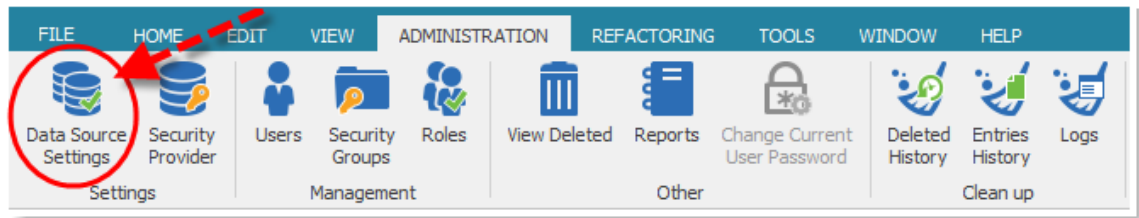
3.5.1.1 Data Source Settings

Description

The **Data source settings** allows you to control many global aspects of the data source, settings such as Offline Mode, password policies and version management are available. You can define general policies applicable for the whole data source.

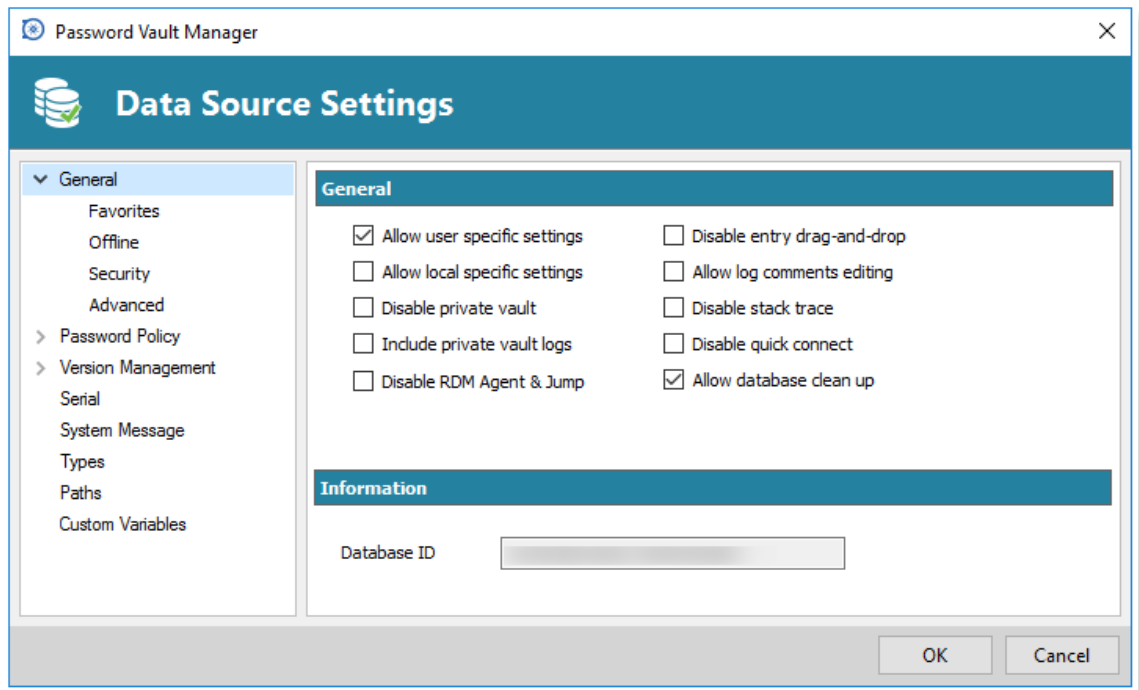
 This feature requires an [Advanced Data Sources](#).

Accessible from the menu **Administration - Data Source Settings**



Administration - Data Source Settings

Settings



Data Source Settings

For more information on the different options held in the Data Source settings please see:

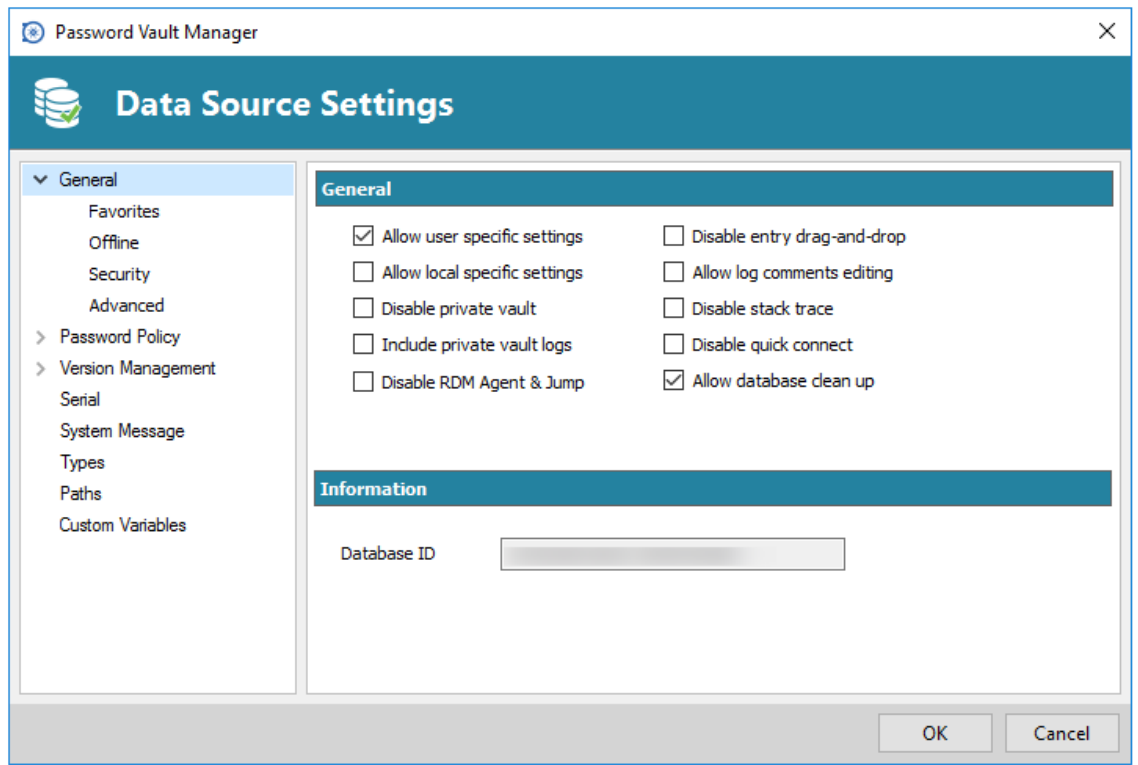
- [General](#)
- [Password Policy](#)
- [Version Management](#)
- [Serial](#)

- [System Message](#)
- [Types](#)
- [Paths](#)
- [Custom Variables](#)

3.5.1.1.1 General

Description

In the **General** side menu, you will be able to manage different access rights specific to the data source.



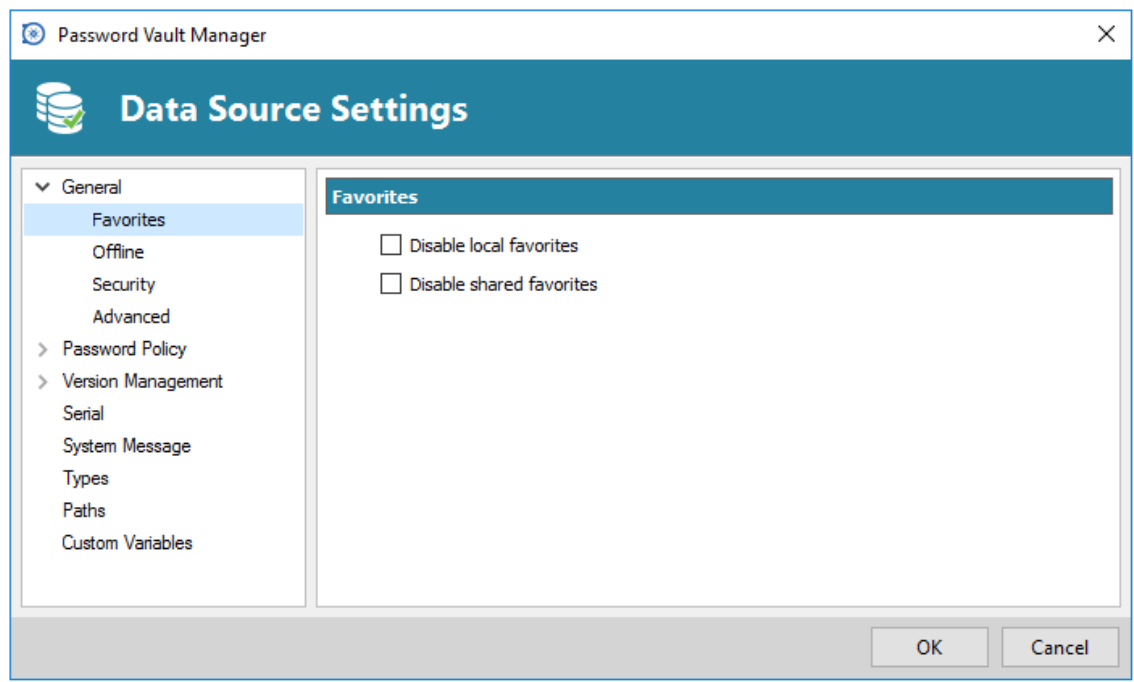
Data Source Settings - General

General

Option	Description
Allow user specific settings	Enables the use of User Specific Settings. See User Specific Settings for more information.
Allow local specific settings	Enables the use of Local Machine Specific Settings . See Local Machine Specific Settings for more information.
Disable private vault	Disable the usage of the Private Vault for all users of the data source.
Include private vault logs	Include the logs for the Private Vault for all users of the data source.
Disable RDM Agent and Jump	The option to activate a session as an RDM Agent or Jump will be disabled.

Disable entry drag-and-drop	Entry group modification using the drag and drop feature will be disabled. Use this setting to avoid accidental drag and drop.
Allow log comments editing	Enable the log comment editing for all users.
Disable stack trace	Disable the stack trace details when an error appears during the execution of the application.
Disable quick connect	Disable the usage of Quick Connect for all users of the data source.
Allow database clean up	Enable the use of the Clean up logs. See Clean up logs for more information.

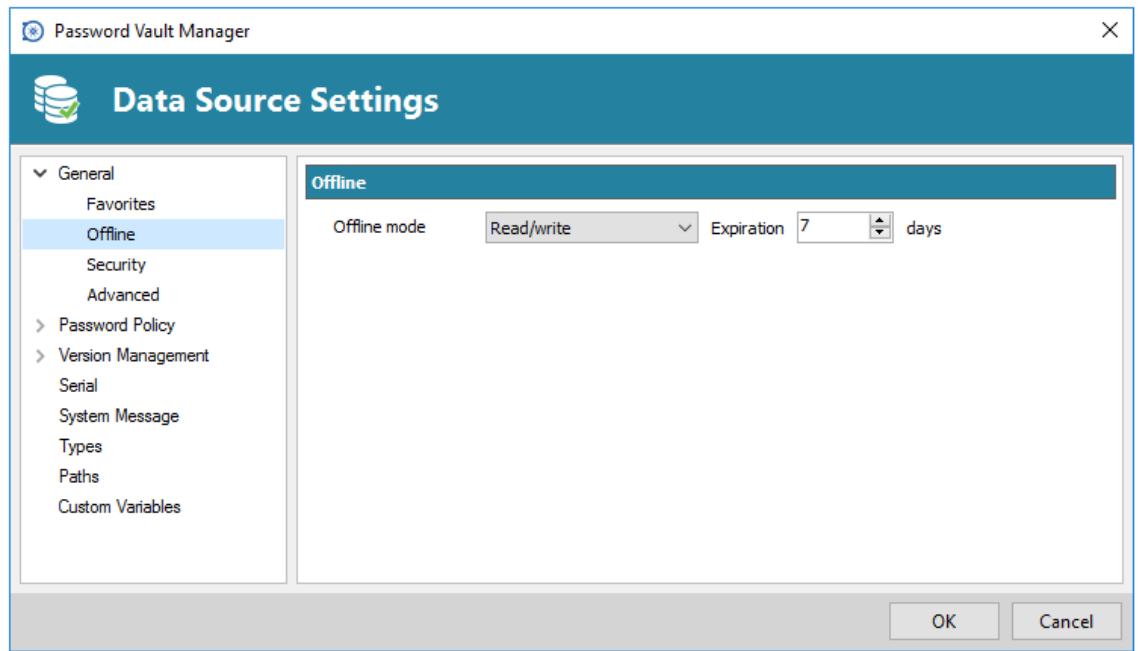
General - Favorites



Data Source Settings - General - Favorites

Option	Description
Disable local favorites	Disable the local Favorites and make them invisible for all users of the data source.
Disable shared favorites	Disable the shared Favorites and make them invisible for all users of the data source.

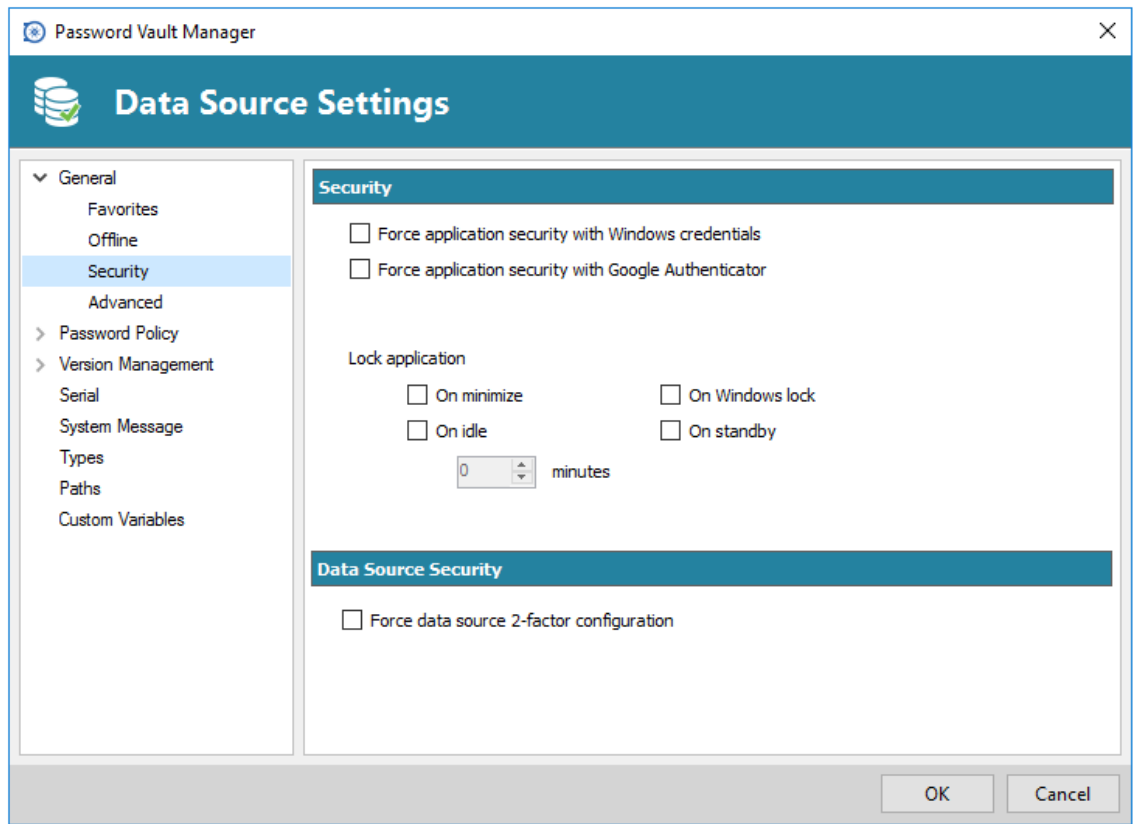
General - Offline




Data Source Settings - General - Offline

Option	Description
Offline mode	Set the global data source support for Offline Mode . Useful when using a VPN connection that makes using local network impossible.
Expiration	Number of days that the local copy will be considered valid for the offline cache. You should go online prior to the end of that period to re-validate the data.

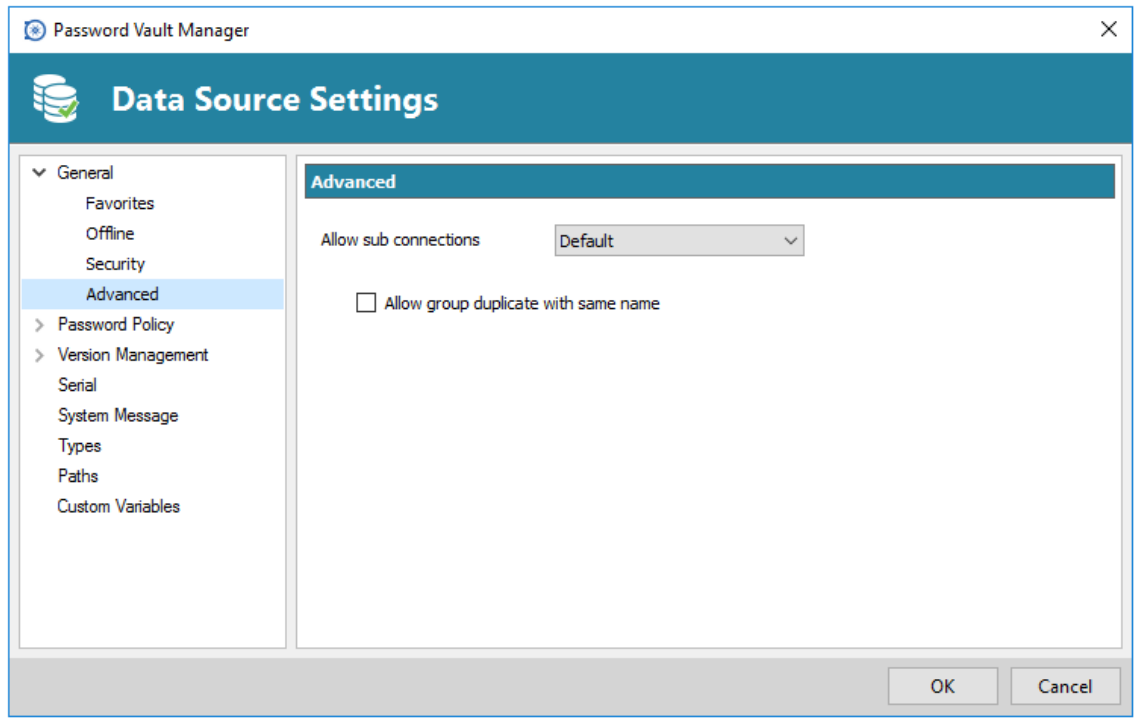
General - Security



Data Source Settings - General - Security

 Note that this setting applies security when **launching** Remote Desktop Manager, it is independent of the security that is required for data sources.

Option	Description
Force application security with Windows credentials	Require the users to authenticate with their Windows credentials at application startup.
Force application security with Google Authenticator	Require the users to authenticate with Google Authenticator at Remote Desktop Manager startup.
Lock application	You can apply on automatic lock of the application on: On Minimize: Lock application when minimized in the taskbar for all users of the data source. On Idle: Automatically lock the application when it is not used after a determined number of time. On Windows lock: Lock the application on Windows lock. On standby: Lock the application when on standby.
Force data source 2-factor configuration	Require the users to have the 2-factor configuration applied on the data source.

General - Advanced**Data Source Settings - General - Advanced**

Option	Description
Allow sub connections	Select True if you wish to allow users of the data source to create sub connections.
Allow group duplicate with same name	Enable if you wish to allow group duplicate using the same name.

3.5.1.1.2 Password Policy

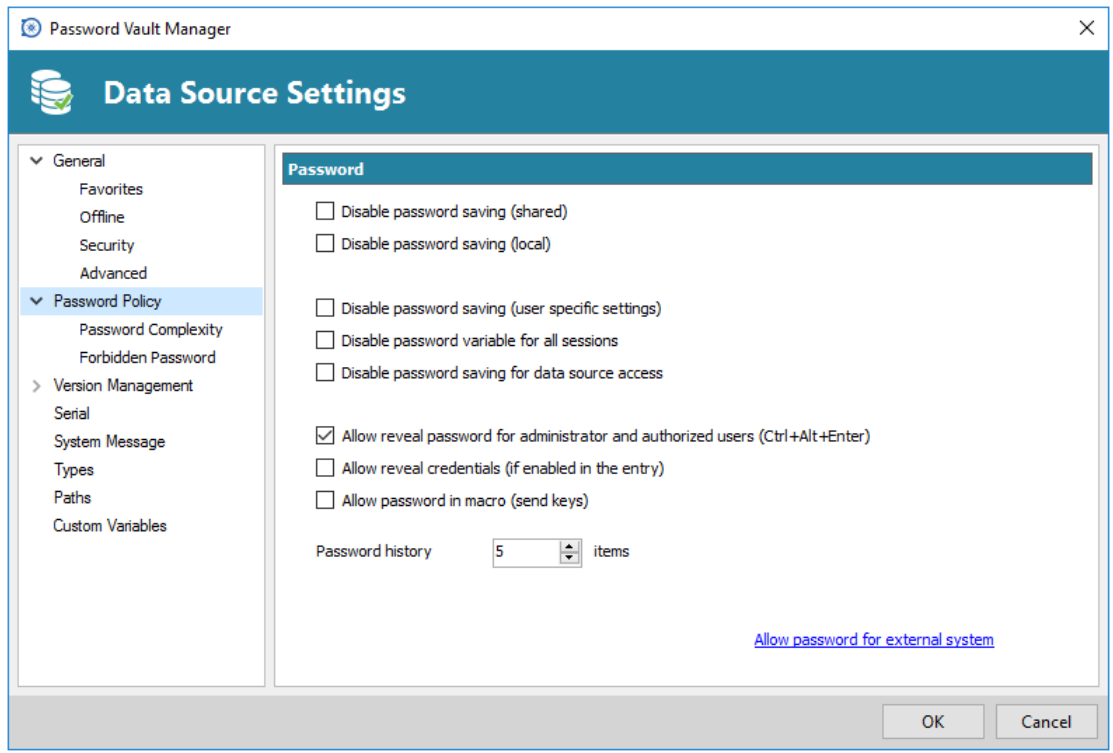
Definition

Password Policy will allow you to manage the different password policy and settings for your data source. For more information regarding the Password Complexity or Forbidden Password follow these links:

- [Password Complexity](#)
- [Forbidden Password](#)
- [Allow password for external system](#)

Some of these settings could be overridden using Group Policies. For more information see How to modify Group Policy Templates.

Settings**Password Policy**



Data Source Settings - Password Policy

Option	Description
Disable password saving (shared)	Users will not be able to save passwords within an entry.
Disable password saving (local)	Users will not be able to save passwords using Windows credential vault.
Disable password saving (user specific settings)	Users will not be able to save password in the User Specific Settings .
Disable password variable for all sessions	Renders \$PASSWORD\$ variable unusable for this data source.
Disable password saving for data source access	Users will not be able to save a new password to access the data source.
Allow reveal password for administrator and authorized users (Ctrl+Alt+Enter)	Controls if reveal password is enabled for authorized users.
Allow reveal credentials (if enabled in the entry)	Shows the credentials if the box " Allow show credentials (everybody) " is check inside the entry.
Allow password in macro (send keys)	Renders \$MACRO_PASSWORD\$ variable useless for this data source.
Password history	Indicates the maximum saved password history count. See Password History for more information.
Allow password for external system	Please see Allow password for external system for more information.

3.5.1.1.2.1 Password Complexity

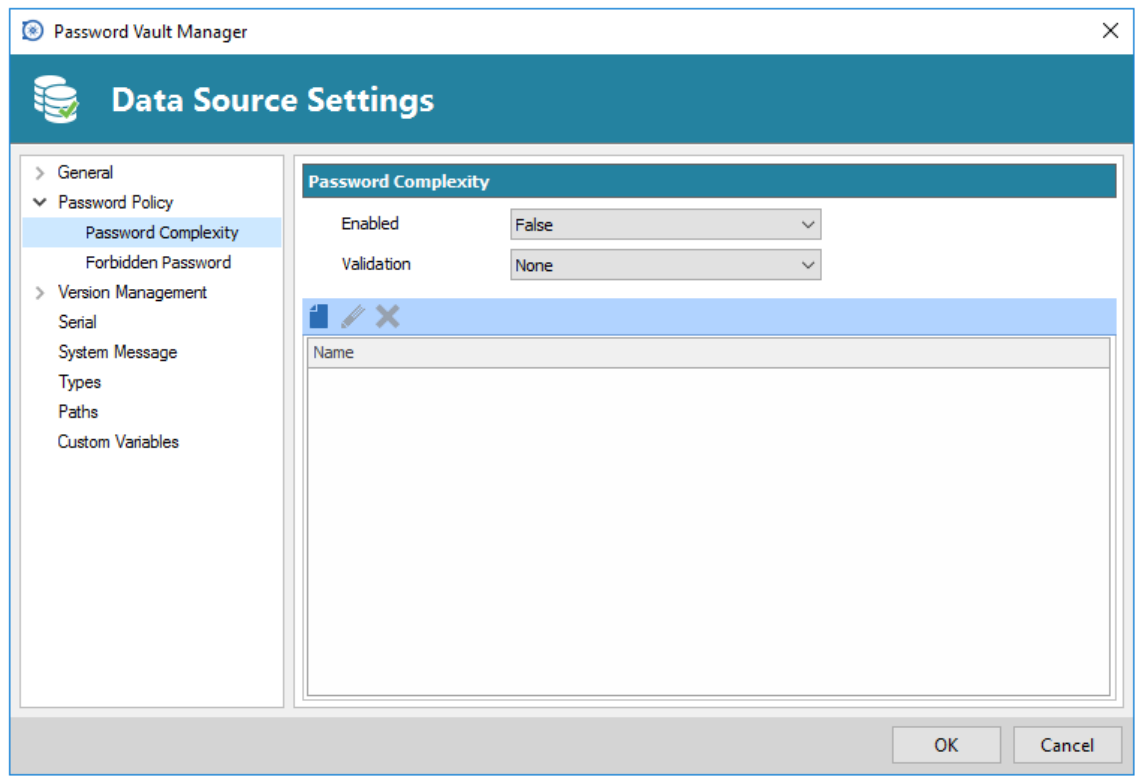
Definition

This security setting determines whether passwords must meet predetermined complexity requirements that has been configured in your Data source settings. Complexity requirements are enforced when passwords are changed or a new entry is created. If this policy is enabled then new passwords must meet some of the following minimum requirements:

- Minimum length
- Minimum lowercase characters
- Minimum uppercase characters
- Minimum numeric characters
- Minimum symbols

Settings

The settings set in the Password Complexity Data source will determine what is the Default value of the Session settings.



Data Source Settings - Password Policy - Password Complexity

Enabled

The **Enabled** option determined in the data source settings will determine the Default option of your Password Complexity entry.

Option	Description
True	Enable the use of the Password Complexity requirements, doing so will force users of the data source to meet the password requirement set by the administrator of the data source.
False	Disable the Password Complexity requirements.
Inherited	Inherit the usage set in the parent folder. When using Inherited you will have to set a password to use as Inherited in the top folder of the entry.


Validation

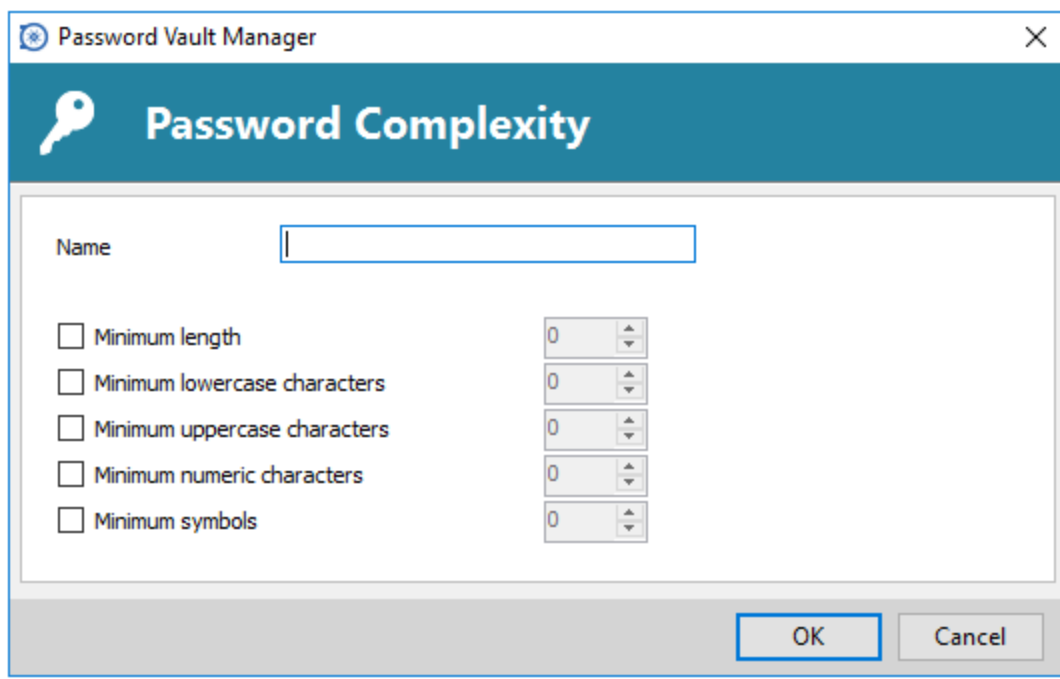
If the Password Complexity is enabled and you then try to change or create a new password for one of your entry, the reaction will depend on the chosen Validation mode.

The validation option determined in the data source settings will determine the Validation Default option of your Password Complexity entry.

Option	Description
None	Will not use any kind of validation when changing or creating a new password.
Warn	Will warn you that your password does not comply with the Password Complexity requirements but will allow you to continue with that password or to edit it.
Required	The requirements of the Password Complexity will be mandatory to change or create a new password.
Inherited	Inherit the usage set in the validation folder. When using Inherited you will have to set a password to use as Inherited in the top folder of the entry.

How-to

You must create your own Password Complexity requirements template to then apply them to your sessions. Click on the New Entry button  to create your Password Complexity template, enter a name and the desired requirements.

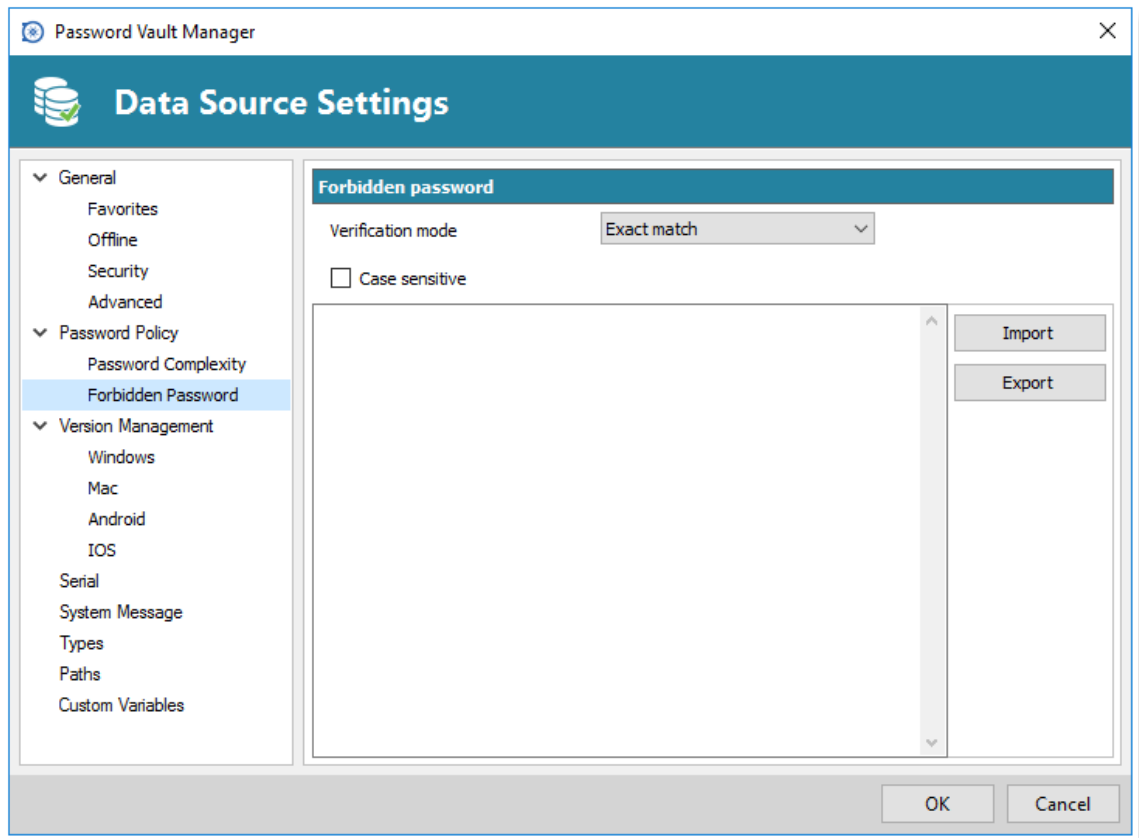


Password Complexity

3.5.1.1.2.2 Forbidden Password

Description

You can create a blacklist of Forbidden password, those passwords will never be allowed to be used once added to this list.



Forbidden password

Option	Description
Verification mode	Select your verification mode between: Exact match: the password will be forbidden if it is the exact match of the one entered in your blacklist. Contains: the password will be forbidden if it contains one of the word entered in your blacklist.
Case sensitive	Enable if you wish the verification mode to be case sensitive.
Import	Import a list of forbidden password from your computer.
Export	Export your Forbidden Password list. By default the list will be exported in a Password Files format (.pwd).

3.5.1.1.2.3 Allow password for external system

Description



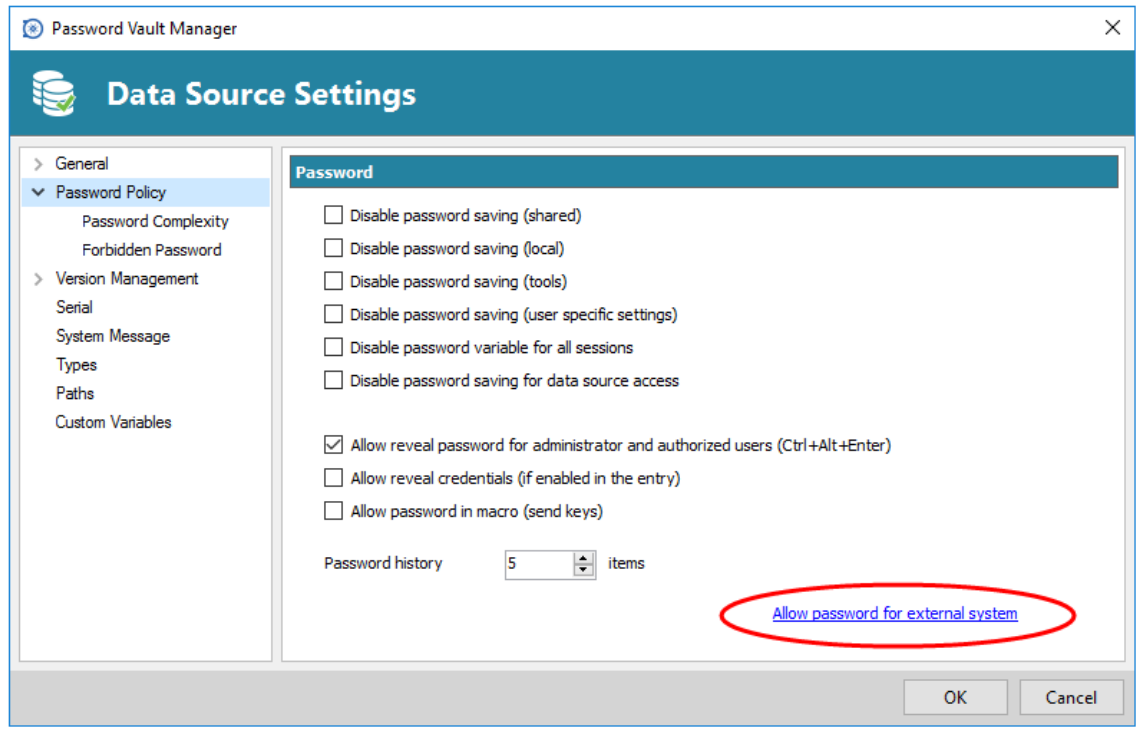
This feature requires an [Advanced Data Sources](#).

Accessing passwords stored in your data source by querying the underlying database is not possible because of the encryption we apply on the passwords. For those of you that need to access passwords directly in the database, for example by a CRM system, we have created a way to achieve this.

Settings

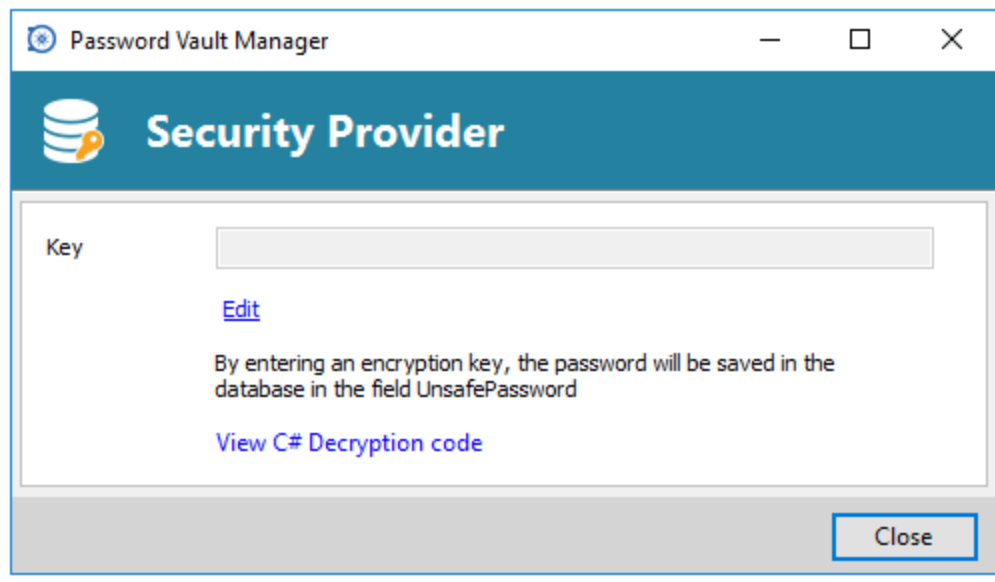
The session information, which is an XML structure, is stored in the **Data** field of the **Connections** table in the underlying database.

However, getting the encrypted password from the database requires that the **Allow password for external system** be configured.



Password Policy - Allow password for external system

Enter an encryption key in the **Key** field. Once a key is provided it will cause the system to extract a copy of the password from our XML structure, this will then be re-encrypted using the **key** you have provided and stored back into the **UnsafePassword** field of the **Connections** table.



Security Provider

Decryption Code

Use the following .net code to decrypt your passwords.

```
public static string Decrypt(string encryptedString, string key)
{
    if (string.IsNullOrEmpty(encryptedString))
    {
        return encryptedString;
    }

    try
    {
        TripleDESCryptoServiceProvider tripleDesCryptoServiceProvider = new TripleDESCryptoServiceProvider();
        MD5CryptoServiceProvider cryptoServiceProvider = new MD5CryptoServiceProvider();

        string strTempKey = key;

        byte[] byteHash = cryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(strTempKey));

        tripleDesCryptoServiceProvider.Key = byteHash;

        tripleDesCryptoServiceProvider.Mode = CipherMode.ECB;

        byte[] byteBuff = Convert.FromBase64String(encryptedString);

        string strDecrypted =
            Encoding.UTF8.GetString(
                tripleDesCryptoServiceProvider.CreateDecryptor().TransformFinalBlock(
                    byteBuff, 0, byteBuff.Length));

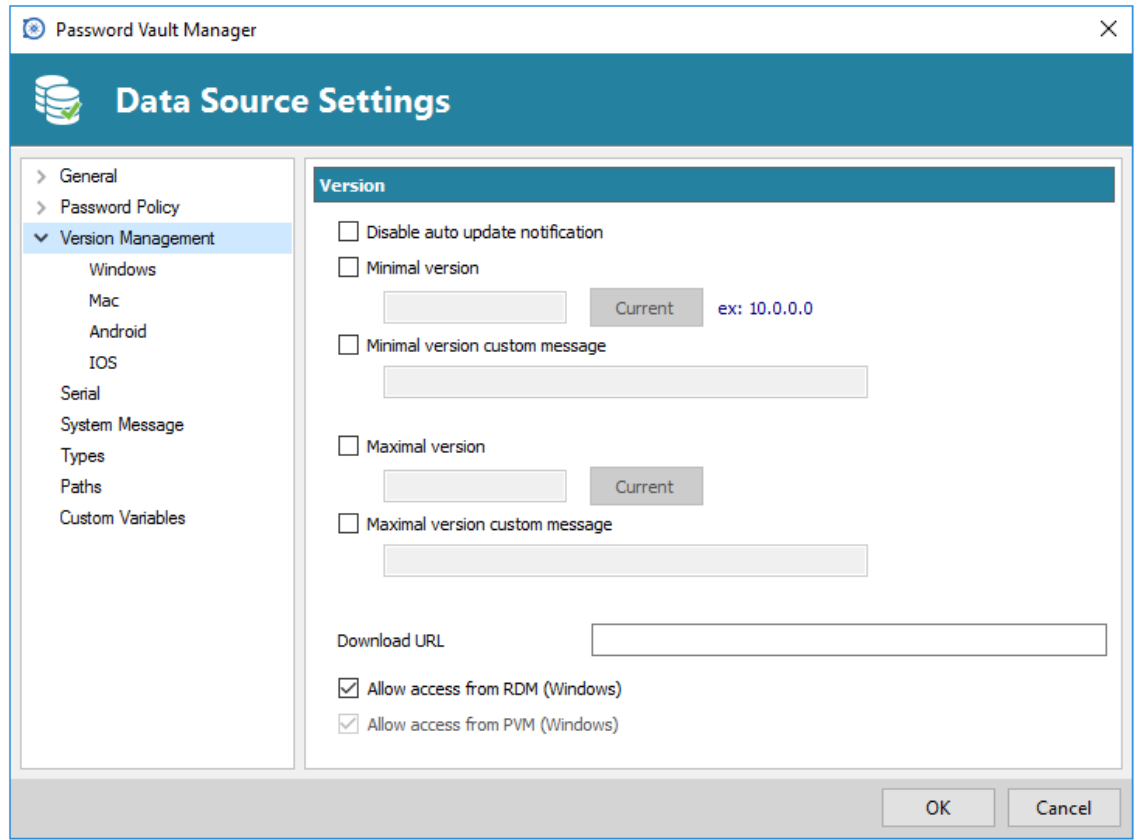
        return strDecrypted;
    }
    catch (Exception)
    {
        return null;
    }
}
```

3.5.1.1.3 Version Management

Description

You can manage your Remote Desktop Manager versions for Windows, Mac, Android or IOS.

Settings



Data Source Settings - Version Management

Option	Description
Disable auto update notification	Disable the auto update notification message. Use this when you want to manually update the application and not get notify when new versions are available.
Minimal version	Forces users of the data source to use a minimal version of Remote Desktop Manager. Enter the entire version number (7.9.10.0) to force a specific version or use partial number to force a subset version (7.9). Use this to disable connecting to the data source with an older version.
Minimal version custom message	Enter a custom message for the minimal version notification.
Maximal version	Forces users of the data source to use a maximal version. Enter the entire version number (7.9.10.0) to force a specific version or use partial number to force a subset version (7.9). Use this to disable connecting to the data source with a newer version.
Maximal version custom message	Enter a custom message for the maximal version notification.
Download URL	Used in conjunction with the minimal or maximal version, once a minimal or maximal version requirement is not met the system will

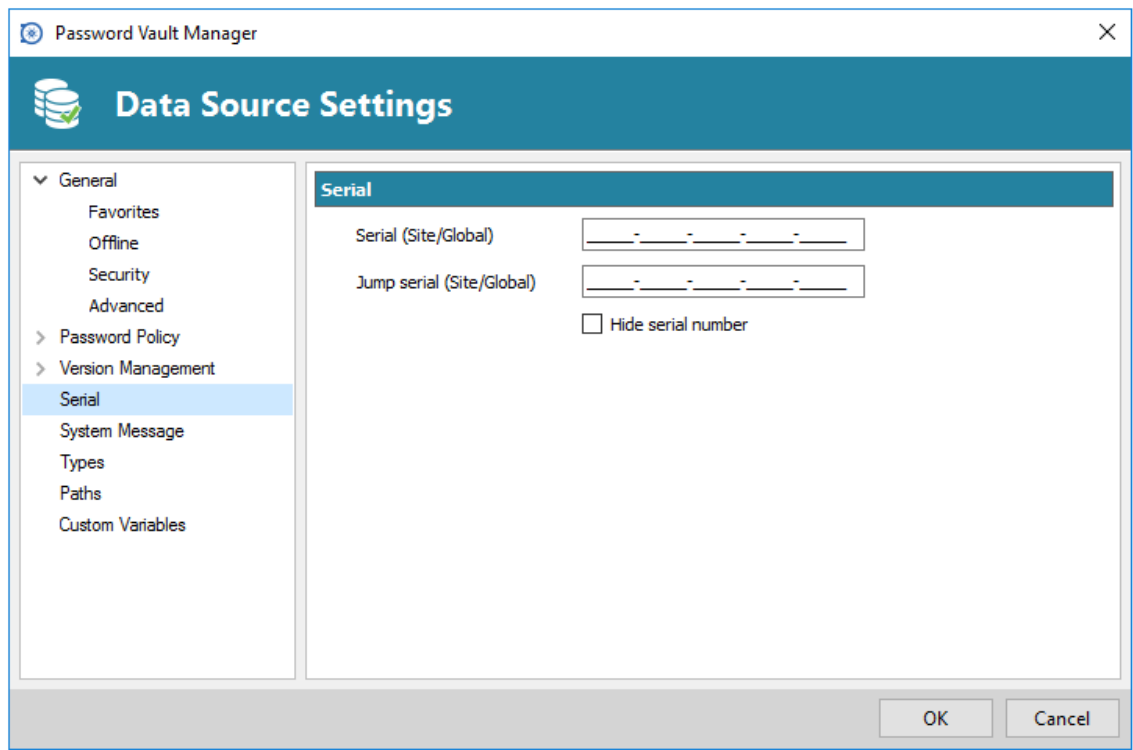
	prompt the user that the version is no longer valid and it will open the link (path/URL) to download the newer or older version.
Allow access from RDM (Windows)	Disable option to exclude some client on different platform like Windows, Mac, IOS or Android.
Allow access from PVM (Windows)	Disable option to deny access to your data source from PVM.

3.5.1.1.4 Serial

Description

Centralize your Serial in the same place for easy access and managing.

Settings



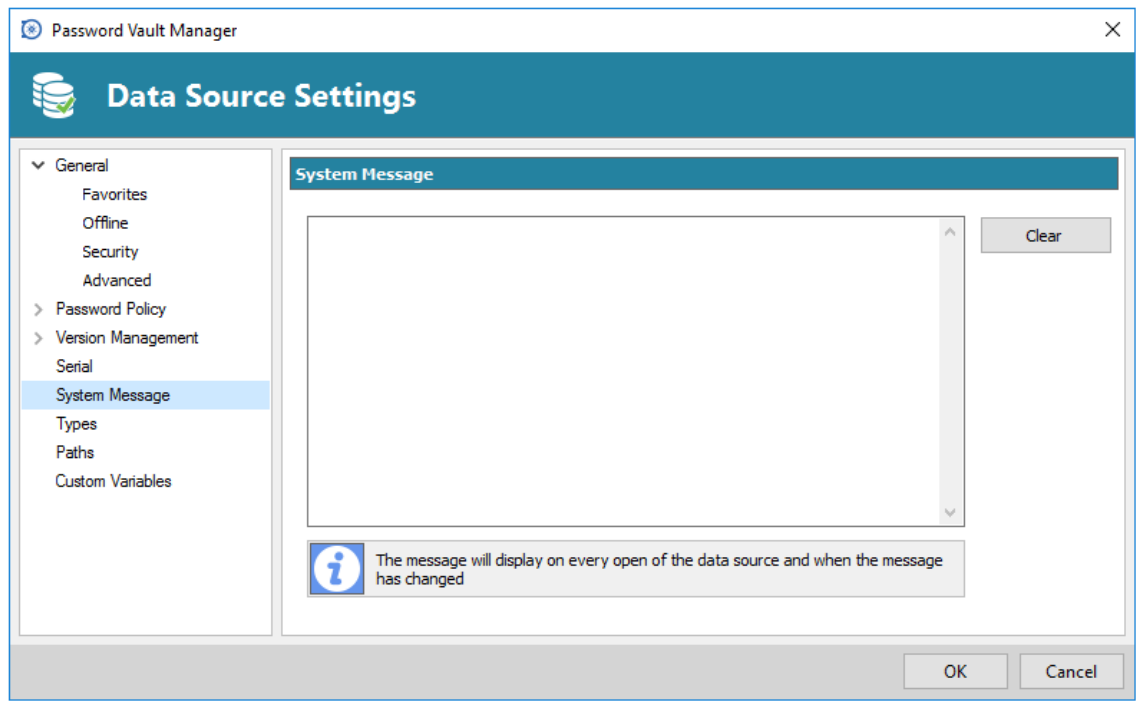
Data Source Settings - Serial

Option	Description
Serial (Site/Global)	Easily distribute Site/Global serials to the entire organization. The application is updated with the license if it's newer than the registered one.
Jump serial (Site/Global)	Easily distribute Jump Site/Global serials to the entire organization. The application is updated with the license if it's newer than the registered one.
Hide serial number	The serial number will be hidden by default for every user connected to the data source.

3.5.1.1.5 System Message

Definition

Enter a system message for other users of the same data source to see when opening Remote Desktop Manager.

Settings

Data Source Settings - System Message

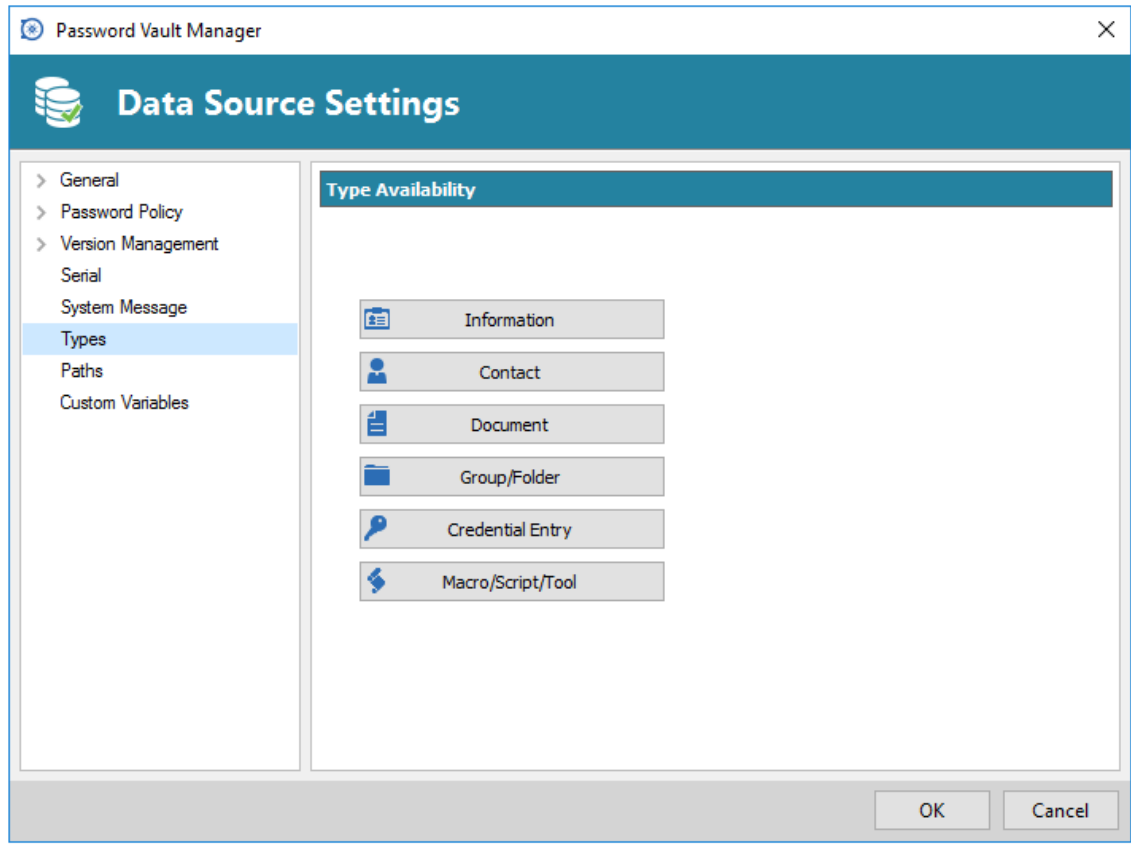
Option	Description
Serial (Site/Global)	Easily distribute Site/Global serials to the entire organization. The application is updated with the license if it's newer than the registered one.
Jump serial (Site/Global)	Easily distribute Jump Site/Global serials to the entire organization. The application is updated with the license if it's newer than the registered one.
Hide serial number	The serial number will be hidden by default for every user connected to the data source.

3.5.1.1.6 Types

Definition

You can select the availability for each type of entry. For example you could choose to exclude credit card from your list of available Information.

Settings



Data Source Settings - Types

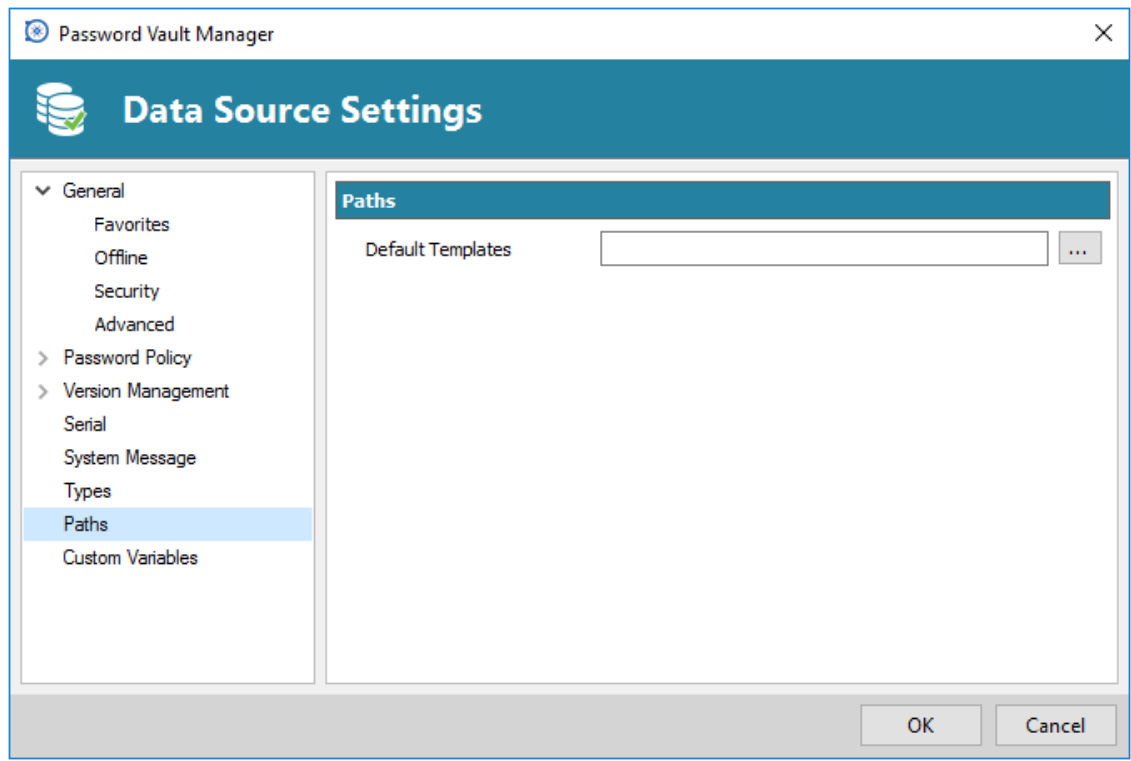
Option	Description
Type Availability	You have the possibility to hide/exclude Information, Contact, Document, Group/Folder, Credential Entry, and Macro/Script/Tool types for all users of the data source.

3.5.1.1.7 Paths

Definition

You can define a default path to save your default templates.

Settings



Data Source Settings - Paths

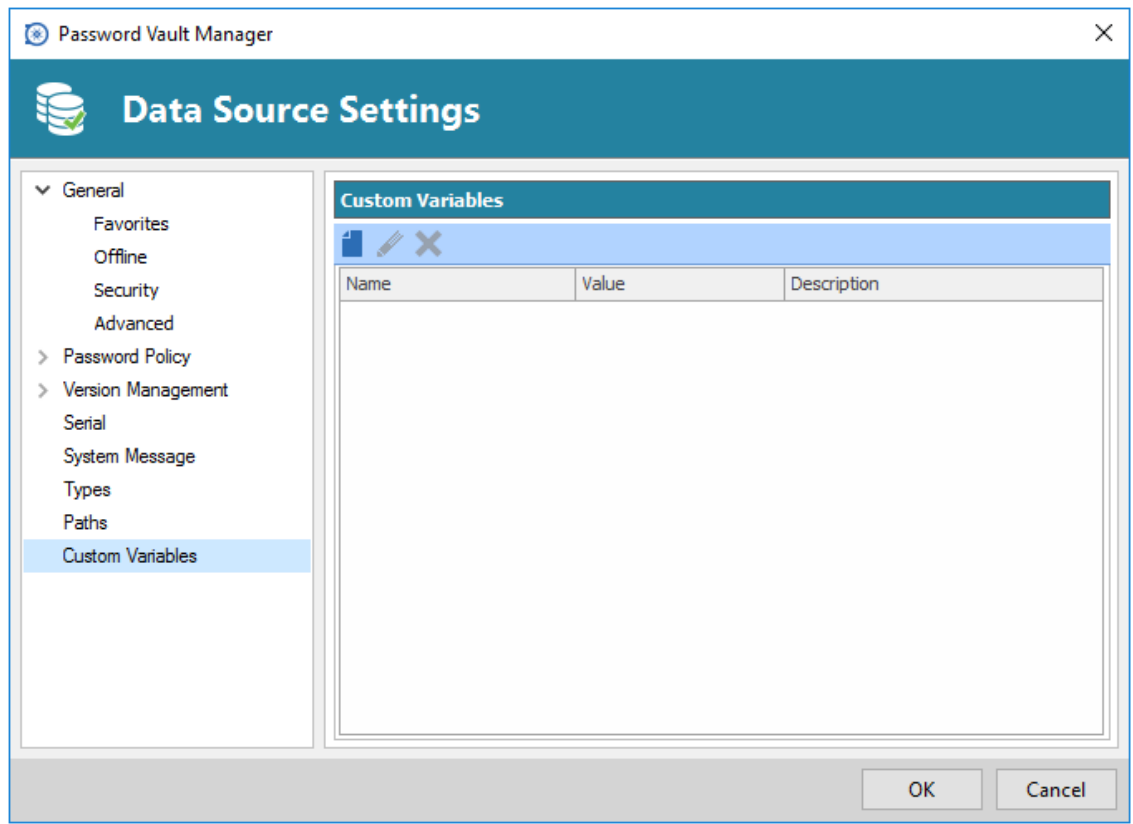
Option	Description
Default Templates	Indicate the default path to save shared templates.

3.5.1.1.8 Custom Variables

Definition

You can define your own custom variables to use in your data source configuration.

Settings



Data Source Settings - Custom Variables

Option	Description
Custom Variables	Add a new custom variable to use in your data source configuration or with any templates. Please view Custom Variables for more information.


3.5.1.2 Security Providers

Description



This feature requires an [Advanced Data Sources](#).

The security provider is available from Administration - Security Provider. The security provider is responsible for encrypting the data in the database.



Regardless of the security provider you've selected, the passwords are stored in the database are **ALWAYS** encrypted using AES 256 bit encryption.



By using a Security Provider, you ensure that nobody can read your entry configuration data, even when people have a direct access to your database(s) or a backup. You should always use this when you use a data source that is not local, especially when using Devolutions Online Database.

Settings

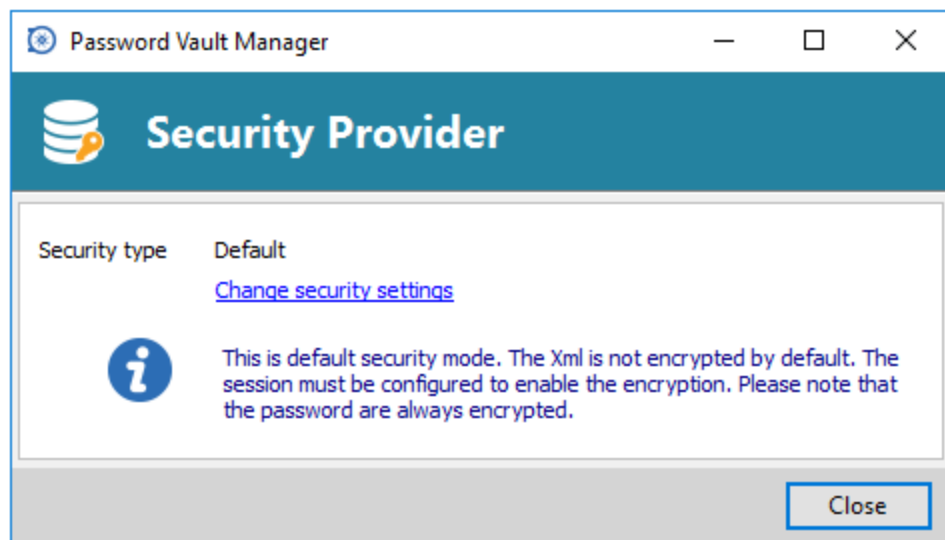


Please note that changing a security provider on a data source with a great number of entries is a lengthy operation.



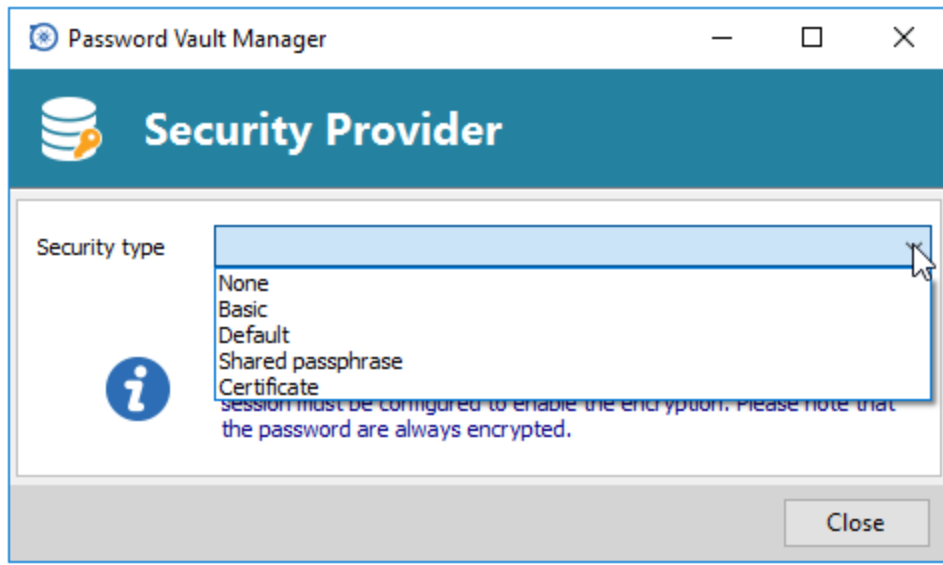
Applying a new security provider does process the whole database, therefore we advise you to create a backup prior to this operation.

1. Click on **Change the security settings** to change the security provider.



Security Provider

2. Select your new security type from the drop down menu.



Security Provider

Option	Description
None	The session data is not encrypted at all (it will still be encrypted using AES 256 bit encryption).
Basic	All of the data is encrypted in the database, and it's impossible for an external system to access it.
Default	This is the legacy security provider. The data is encrypted if the session configuration is set accordingly in the advanced settings.
Shared passphrase	All of the data is encrypted with a mix of our key, a salt and the passphrase. This is the most secure encryption, but if the passphrase is lost, there is nothing that can be done to recover the data.
Certificate	See Certificate below for more information.

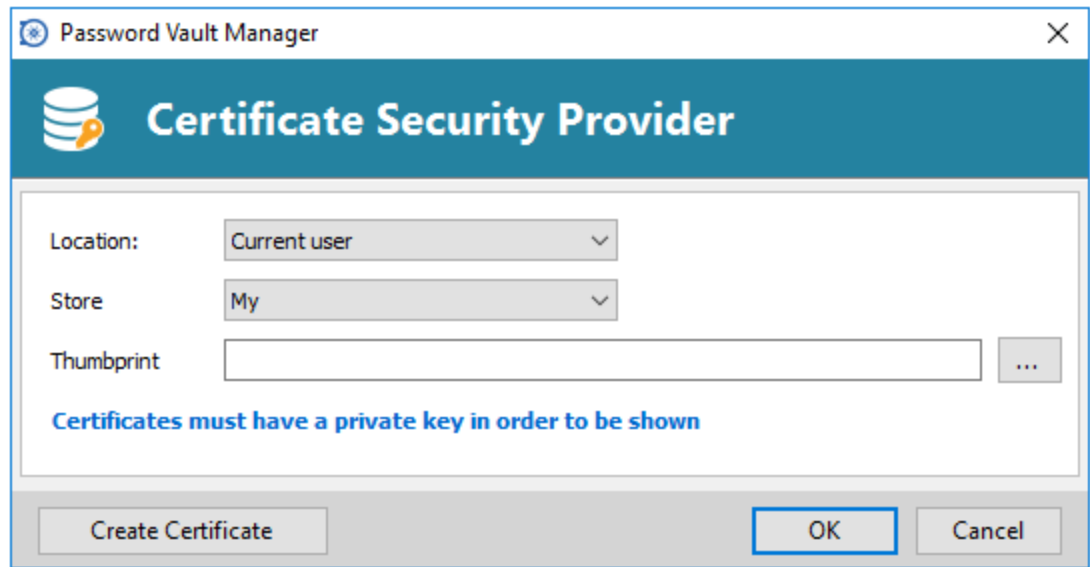
Shared Passphrase

If the passphrase is lost, there is **nothing** that can be done to recover the data. Always copy it to a secure location when putting it in place.

All of the entries configuration data is encrypted with a mix of key stored in Remote Desktop Manager and the passphrase you've entered. The passphrase is required only when configuring the data source.

Certificate

If you have chosen Certificate as your Security Provider, it will encrypt the entry configuration data with a mix of key stored in Remote Desktop Manager and the private key contained in the certificate.



Certificate Security Provider

Option	Description
Location	Indicate the certificate location. Select between: <ul style="list-style-type: none"> • Current user • Local machine
Store	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none"> • Address book • Authorization root • Certificate authority • Disallowed • My • Root • Trusted people • Trusted publisher
Thumbprint	Select a certificate that already exist to use for the encryption.

Create Certificate

You can choose to create your own Self Signed certificate by clicking on **Create Certificate**.

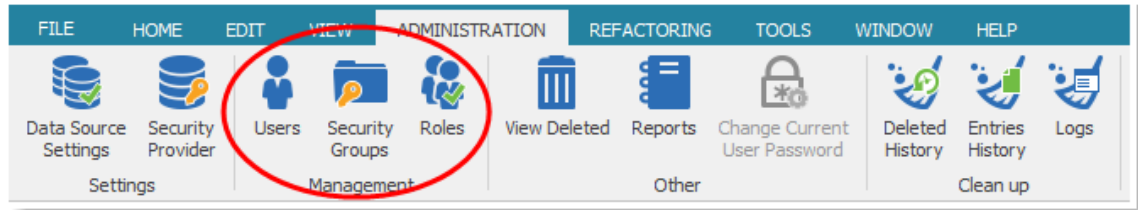
Self Signed Certificate

Option	Description
Common name	Name of the certificate.
Key size (bits)	Indicates the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"> • 384 • 512 • 1024 • 2048 • 4096 • 8192 • 16384
Valid from	Starting date of the certificate.
Valid to	Ending date of the certificate.
Save to file (pfx)	Save the certificate into a pfx file and secure this certificate with a password.
Save to certificate store	Indicate the location and the store to save the certificate.

3.5.2 Management

Description

The **Management** menu is for managing your Users, Security Groups and Roles. You have to be an administrator of the data source to enable those options, if the menu is grayed out contact your administrator.



Management

Refer to the following topics for more information:

- [Users](#)
- [Security Groups](#)
- [Roles](#)

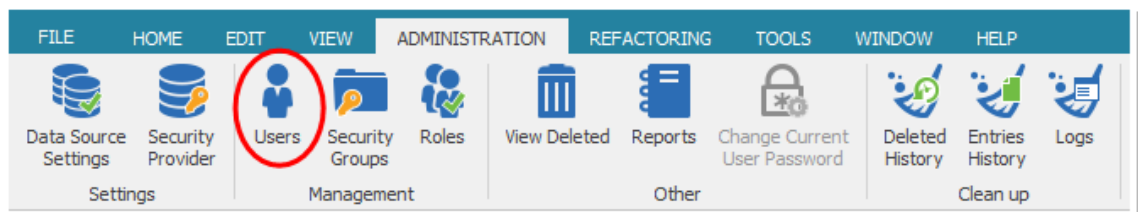
3.5.2.1 Users

Description

The Users administration is available from the menu **Administration - Users**. Users management allows you to create, manage and assign rights to a user.

Remote Desktop Manager allows for advanced user rights management, letting you control how a session is employed by each user. Note that some visibility control will depend on the active data source.

However, there is currently no way to inherit security rights from a group. They must be assigned individually for each user.




Administration - Users



This feature requires an [Advanced Data Sources](#).



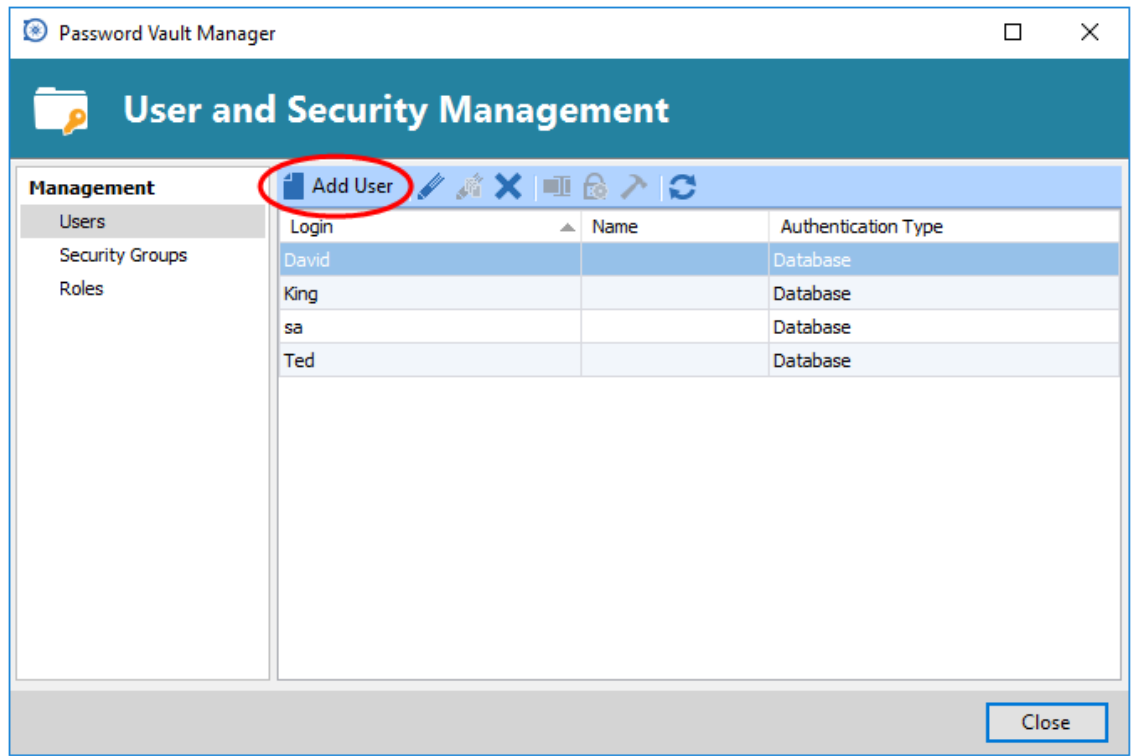
Not all [Advanced Data Sources](#) support the use of [Integrated Security](#). [SQL Server](#) supports it natively and [MySQL](#) supports integrated security via [Windows Authentication Plugin](#) which is a commercial extension of MySQL.

 In order to create users and assign rights, you must be administrator of not only Password Vault Manager, but also of the underlying database.

Settings

Create Users

To create a new user in your data source click on **Add User**. You can create a user using a default security (specify the password) or [Integrated Security](#).



Users - Add User

User Management Settings

General

The screenshot shows the 'User Management' dialog box in Password Vault Manager. The 'General' tab is selected in the left-hand navigation pane. The main area contains the following fields and options:

- ID:** A text input field.
- Login:** A text input field with a blue border.
- Integrated security (Active Directory):** An unchecked checkbox.
- Password:** A text input field.
- Create SQL Server Login and User:** A checked checkbox.
- Email:** A text input field.
- Administrator:** An unchecked checkbox.

At the bottom right, there are 'OK' and 'Cancel' buttons.

User Management - General

Option	Description
Login	Login name for the user. When using Integrated Security you must select the user in the directory.
Integrated Security (Active Directory)	Specifies to use the Windows Integrated Authentication to authenticate to the data source. Applies only to SQL Server and Devolutions Server , depending on their configuration. When checked, an ellipsis button appears to allow you to browse for the user account in the directory. Consult Integrated Security topic for more information.
Create SQL Server Login and User	Automatically create the user in the SQL Server when using the Integrated Security .
Password	Enter the user Password. This field is disabled when using Integrated Security .
Email	Insert the user's email address.
Administrator	Grants full administrative rights to the user for the whole system.

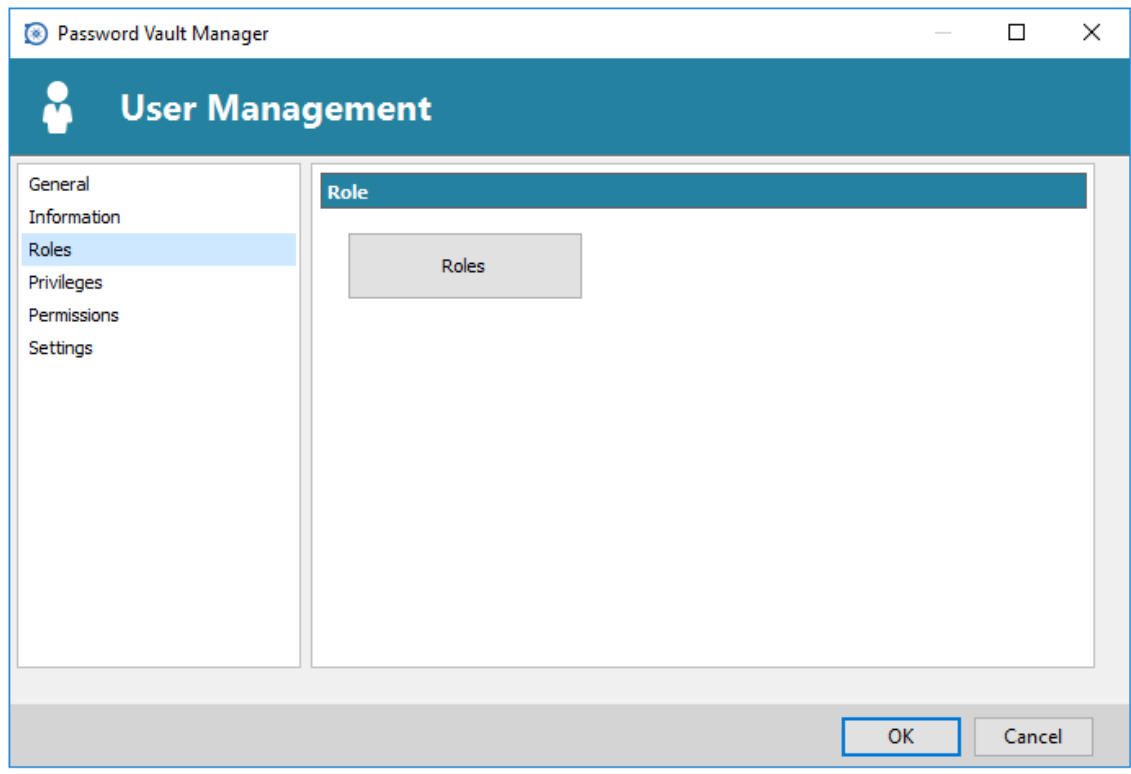
Information

Enter all necessary information regarding your new user.

The image shows a screenshot of the 'Password Vault Manager' application window. The title bar reads 'Password Vault Manager'. The main content area is titled 'User Management' and features a sidebar on the left with a list of options: 'General', 'Information' (which is selected and highlighted in blue), 'Roles', 'Privileges', 'Permissions', and 'Settings'. The main area is divided into three sections: 'Information', 'Address', and 'Phone'. Each section contains several text input fields. The 'Information' section includes fields for 'First name', 'Last name', 'Company', and 'Gravatar email'. The 'Address' section includes fields for 'Address', 'State', and 'Country'. The 'Phone' section includes fields for 'Phone', 'Work', 'Mobile', and 'Fax'. At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons.

User Management - Information

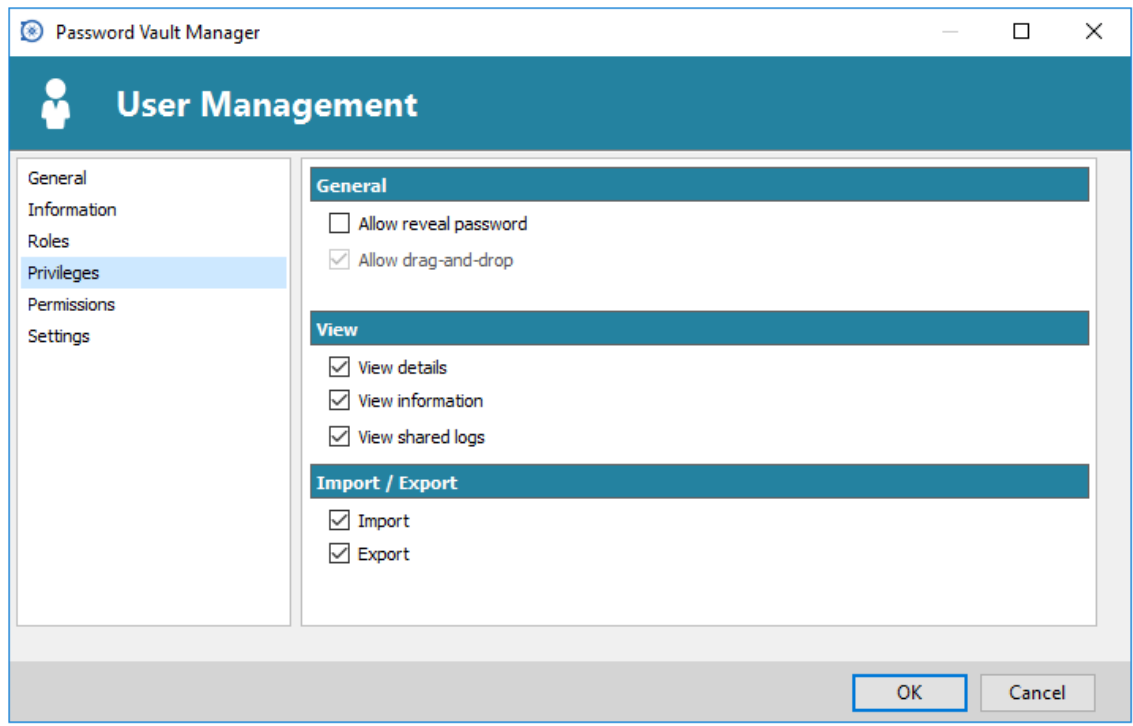
Roles



User Management - Roles

Option	Description
Roles	Consult Role Management topic for more information. When a role needs to be added to a user, a description column will help you to select the proper role.

Privileges



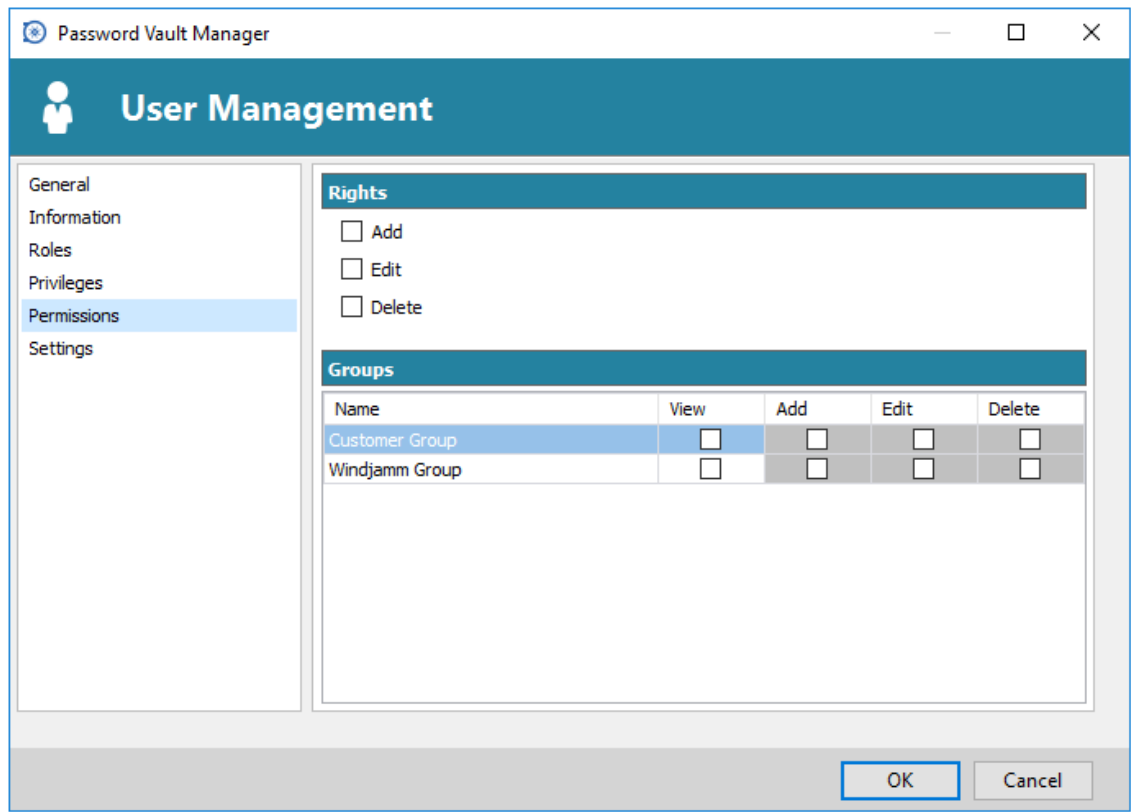
User Management - Privileges

Option	Description
Allow reveal password	Allows the user to use the Reveal Password command.
Allow drag-and-drop	Allows the user to move the sessions using drag-and-drop from other applications.
View details	Allows the user to see the content of the Details tab for all sessions.
View information	Allows the user to see the content of the Information tab for all sessions.
View shared logs	Allows the user to see the content of the Logs that applies to a session.
Import	Allows the user to Import sessions (Clipboard - Paste as well). The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.
Export	Allows the user to Export sessions (Clipboard - Copy as well). The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.

Permissions

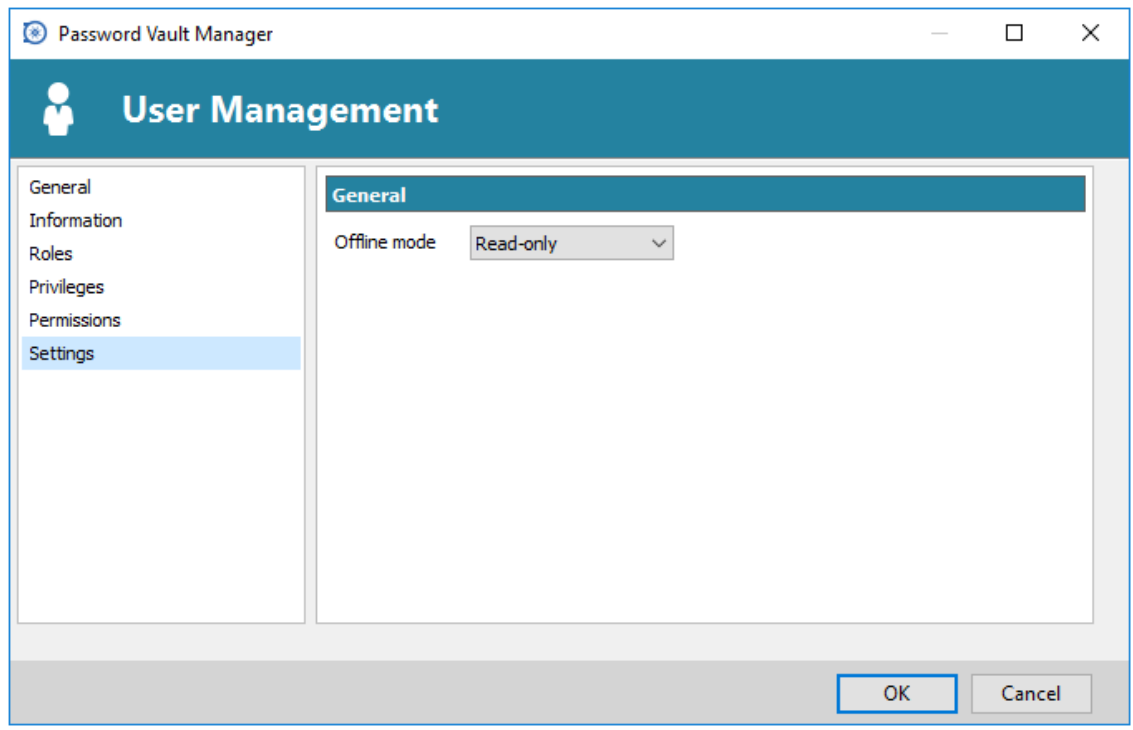
The Permissions section allows you to assign permissions. Controls are sometimes hidden depending on the data source or the state of other controls.

Consult the [Permissions](#) topic for more information on rights that can be added to a user.



User Management - Permissions

Settings



User Management - Settings


Allow the user to enable the [Offline Mode](#) on the data sources. This also depends on the data source being configured to allow it. You can choose between:

Option	Description
Disabled	Offline mode is disabled for that user.
Read-Only	A Read-only cache is allowed for the user (an Advanced Data Source is required).
Read/Write	An advanced cache, with change synchronization is allowed for the user (an Advanced Data Source is required).

3.5.2.1.1 Integrated Security

Description

Integrated Security is the name Microsoft gives to the technology that uses the credentials of your current running session and passes them automatically to the remote resources for authentication.



This feature requires an [SQL Server](#), [MySQL](#) or a [Devolutions Server](#) data source.

Settings

When activating the **Integrated Security** checkbox in the User Management window, the password field will be disabled because the operating system will provide a cached copy automatically.

The screenshot shows the 'User Management' window in Password Vault Manager. The 'General' tab is active. The 'Password' field is highlighted with a red rectangle. A blue dashed arrow points to the 'Integrated security (Active Directory)' checkbox, which is checked. The 'Create SQL Server Login and User' checkbox is also checked. The 'Administrator' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

User Management - Integrated Security

When the option is activated, an ellipsis button will either appear or be enabled. Clicking this button will display the Select User dialog.

The screenshot shows the 'Select User' dialog box. The 'Object Types' field is set to 'User'. The 'Locations' field is set to 'VDEV'. The 'Check Names' button is visible. The 'OK' and 'Cancel' buttons are at the bottom right.

Integrated Security - Select User



Ensure the appropriate domain is displayed in the **From this location** field because sometime the location defaults to the local computer. Click the **Locations** button to be able to browse for the domain instead.

Consult the [Permissions](#) topic for information on the rights that can be given to a user.

3.5.2.1.2 Permissions

Description

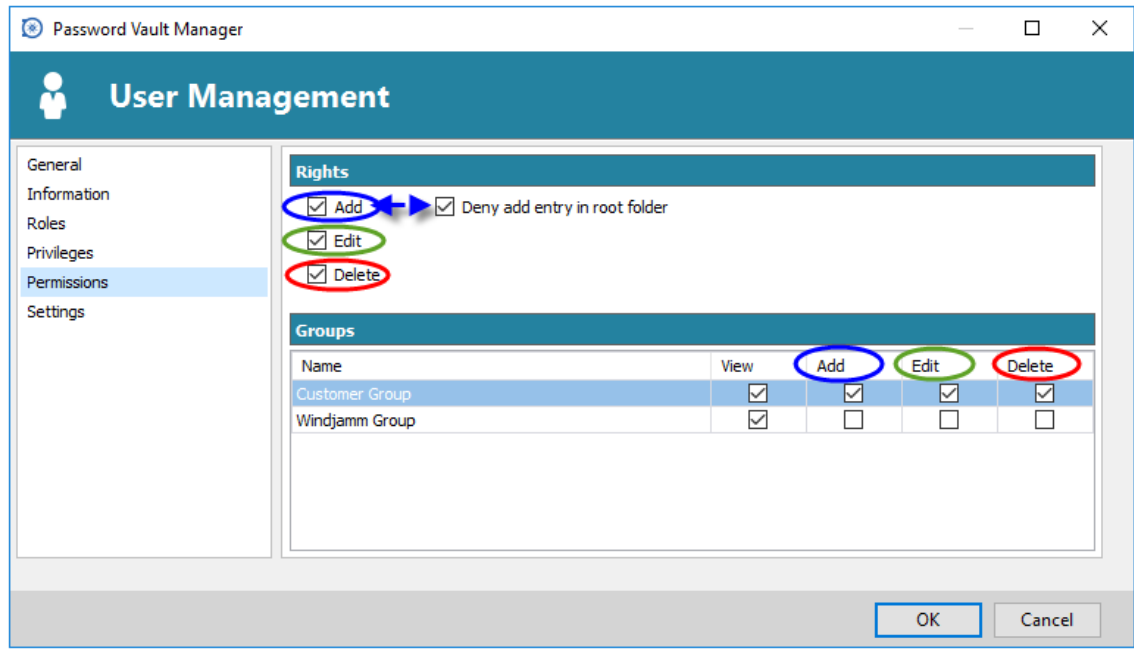
The Permissions section allows you to assign permissions. Controls are sometimes hidden depending on the data source or the state of other controls.

Settings

Permissions

The options directly above the grid are for **public** folders, meaning any folder that hasn't been assigned a security group will be assigned those rights. They also act as the most basic permission you can assign because they are needed in order to allow permissions for each of the security group listed below, when they are not checked the corresponding column of the grid is grayed out.

The public **Add** permission also displays the **Deny add entry in root folder**. This folder is named Sessions in your tree view and is in fact virtual, we created this option so you could control which users could create entries at the root.



User Management - Permissions

Option	Description
Add	Grant the Add privileges for public groups. Also controls the visibility of the Add column in the Groups grid. The Add privilege needs to be checked if the user needs to add sessions in the Private Vault.
Edit	Grant the Edit privileges for public groups. Also controls the visibility of the Edit column in the Groups grid. The Edit privilege needs to be checked if the user needs

	to edit sessions in the Private Vault.
Delete	Grant the Delete privilege for public groups. Also controls the visibility of the Delete column in the Groups grid. The Delete privilege need to be check if the user need to delete sessions in the Private Vault.



For higher security, it is a best practice to set security groups on **all** root level folders. This ensures that there are no public folders and that you have good control over the activity in your system.

All security groups are listed in the grid and you can assign permission using the corresponding columns.



Granting the View permission does allow the right to also launch/open sessions of that group.

Option	Description
View	Allows the user to View AND USE the entries for that security group.
Add	Allows the user to Add entries in groups/folders for that security group.
Edit	Allows the user to Edit the entries for that security group.
Delete	Allows the user to Delete the entries for that security group.

3.5.2.2 Security Groups

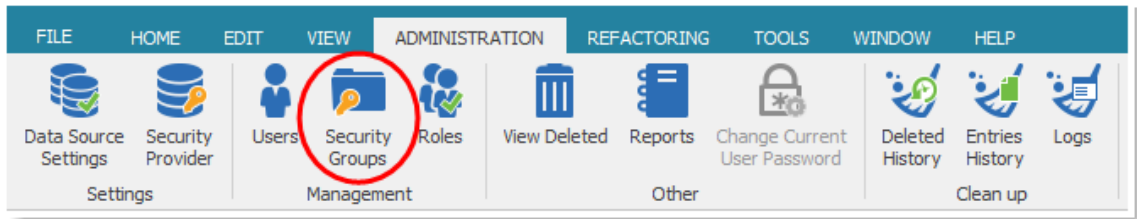
Description

The Security Group Management is available from the menu **Administration - Security Groups**.

Security groups are used to protect sessions from a subset of system users. Assign sessions to security groups then control who has access and how much control they have on each security group.


Security groups are used to classify sessions and restrict access to certain users. There is no direct relationship between Active Directory and Security Groups. By default, every session is created without an assigned security group, and therefore is visible to all connected users.

Each entry in the navigation pane can be assigned to a single security group. Best practices dictates that you assign security groups to groups/folders that way all the entries they contain will inherit the same security group.



Administration - Security Groups

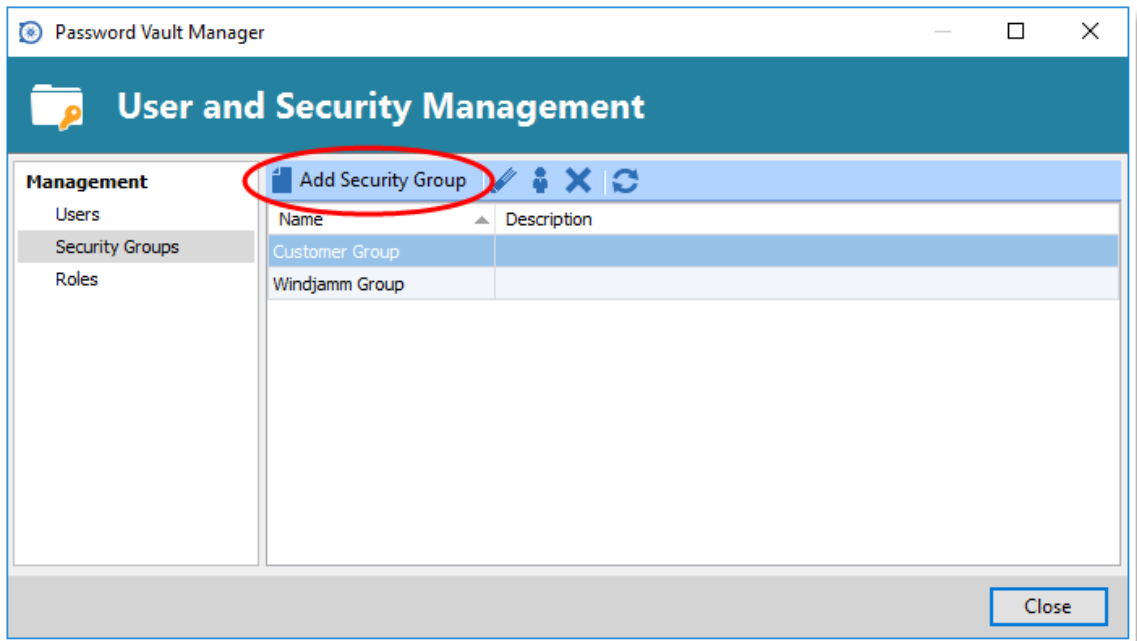
 This feature requires an [Advanced Data Sources](#).

 **All sessions without security groups are considered public, which means that it will be available to all your data source users.**

Settings

Create a security group

Security groups are created from the menu **Administration - Security Group - Add Security Group**.



Security Group - Add Security Group

A Security Group Management dialog will appear. Enter a name and a short description of your new Security Group.

Password Vault Manager

Security Management

General

ID: 778F6699-E7AC-4CC6-BB39-FFD3A607E9F1

Name:

Description:

OK Cancel

Security Group

Manage the proper rights applied to each user to define your Security Group.

Password Vault Manager

Security Group Rights

Name: IT Support

Users

Name	Administrator	View	Add	Edit	Delete
David	✓	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
King		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sa	✓	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ted		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add Rights
View Only
Remove Rights

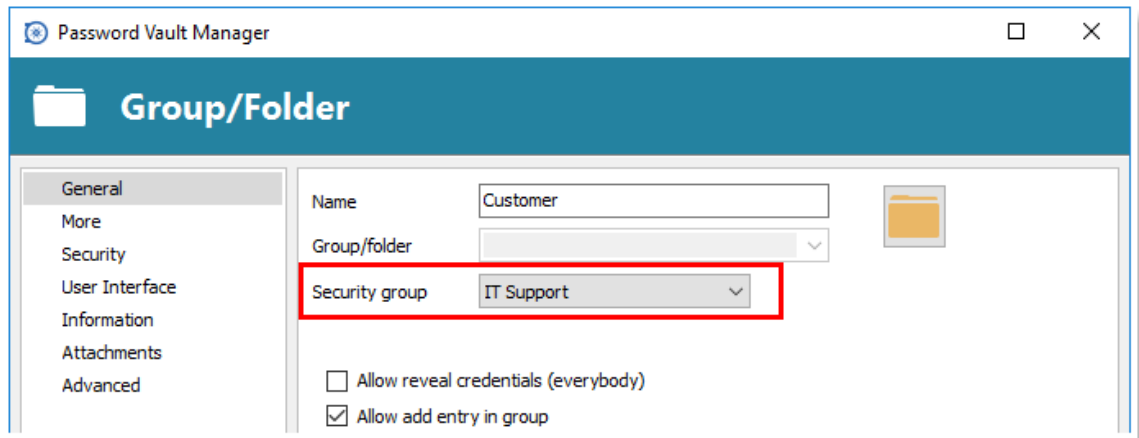
778f6699-e7ac-4cc6-bb39-ffd3a607e9f1

Save Cancel

Security Group Rights

Assign a security group to the session

Security groups can be assigned to entries using the property window. Each entry can only have one security group assigned. For easy maintenance, we recommend assigning security groups to groups/folders which will result in the child entries to inherit the security group.

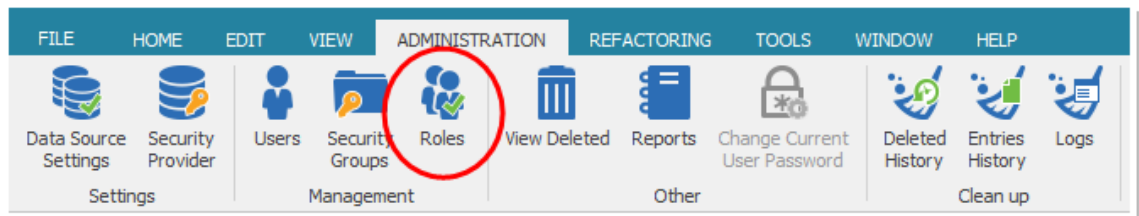


Assign a Security Group


3.5.2.3 Roles

Description

Roles in Remote Desktop Manager are mainly used to reduce the time taken to manage users. The management of permissions granted to roles are quite similar to the corresponding notions for users, but instead of a single user, they apply to all users to which you've assigned the role.



Administration - Roles

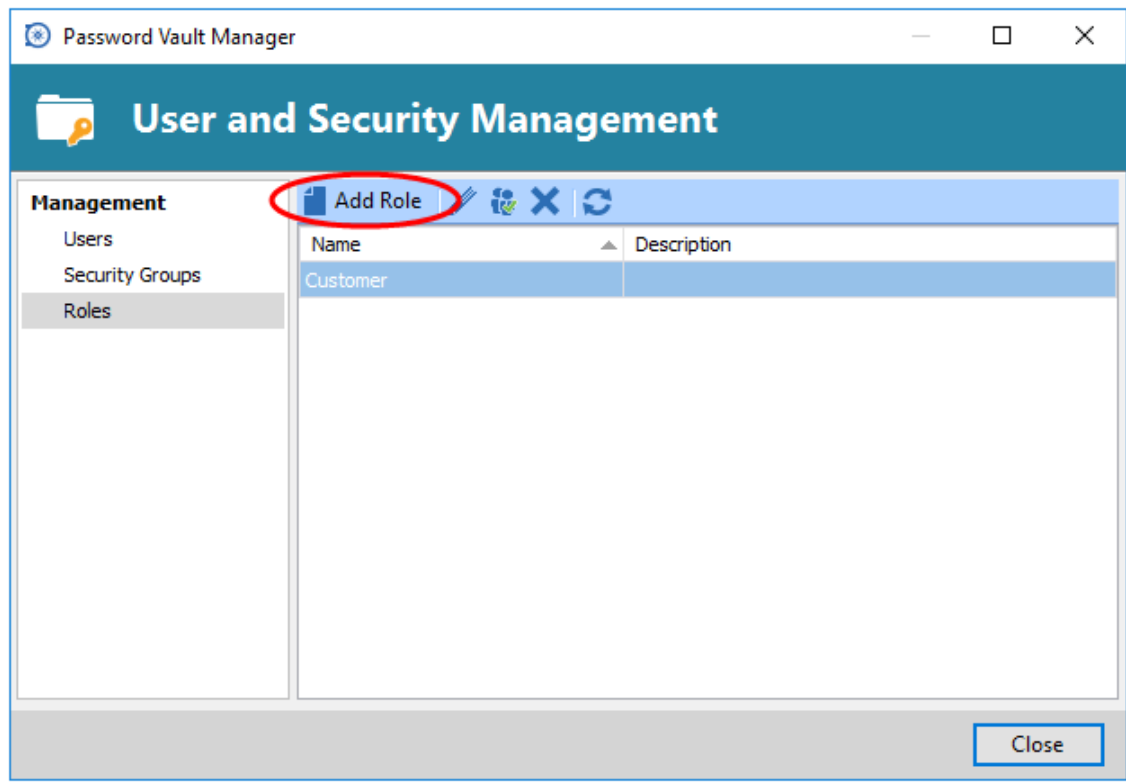


This feature is only available with an [SQL Server](#), [SQL Azure](#) and a [Devolutions Server](#) data source.

Roles in Remote Desktop Manager

Roles in Remote Desktop Manager are simply permission sets that you assign to a user. You can assign multiple roles to each user and the end result is the union of all permissions.

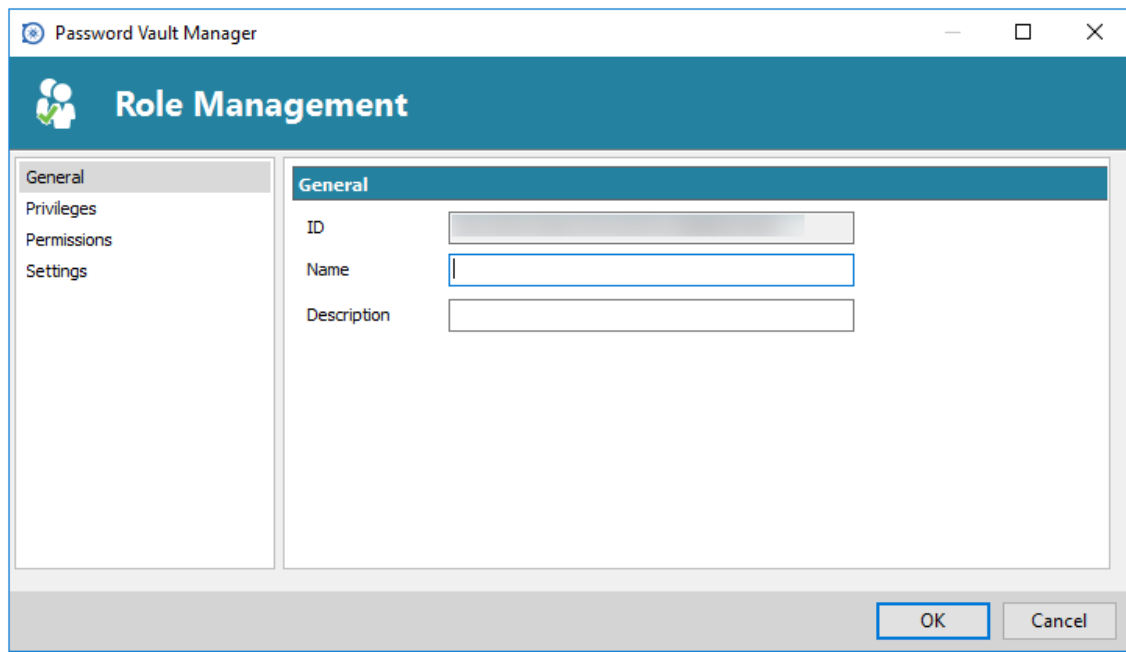
To create a role you need to go in **Administration - Roles - Add Role**.



Roles - Add Role

Role Management

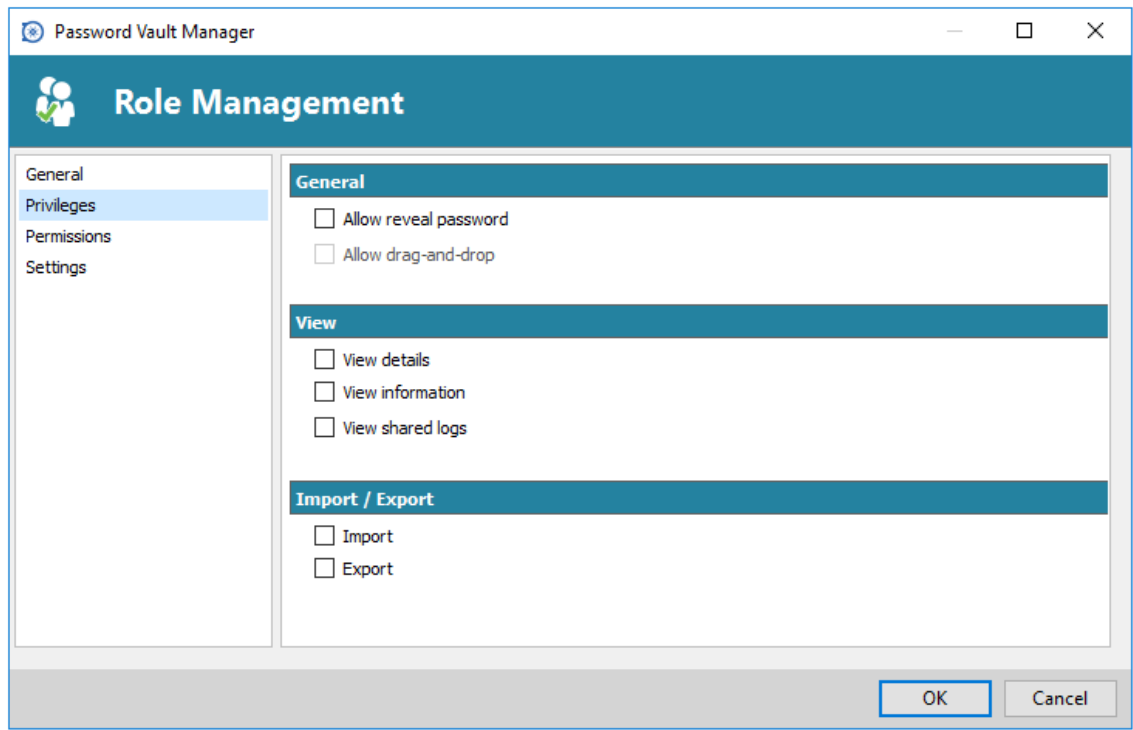
General



Role Management - General

Option	Description
Name	Enter a name for your new Role.
Description	Enter a short description of your new Role.

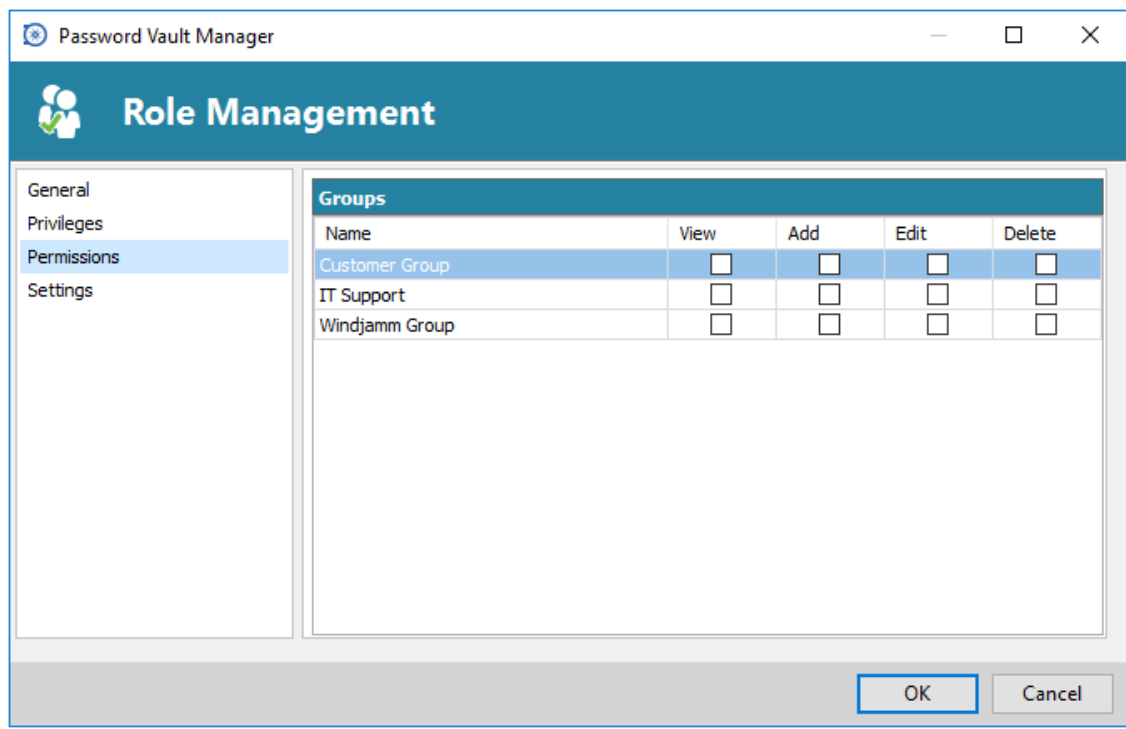
Privileges



Role Management - Privileges

Option	Description
Allow reveal password	Allows the user to use the Reveal Password command.
Allow drag-and-drop	Allows the user to move the sessions using drag-and-drop from other applications.
View details	Allows the user to see the content of the Details tab for all sessions.
View information	Allows the user to see the content of the Information tab for all sessions.
View shared logs	Allows the user to see the content of the Logs that applies to a session.
Import	Allows the user to Import sessions (Clipboard - Paste as well). The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.
Export	Allows the user to Export sessions (Clipboard - Copy as well). The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.

Permissions

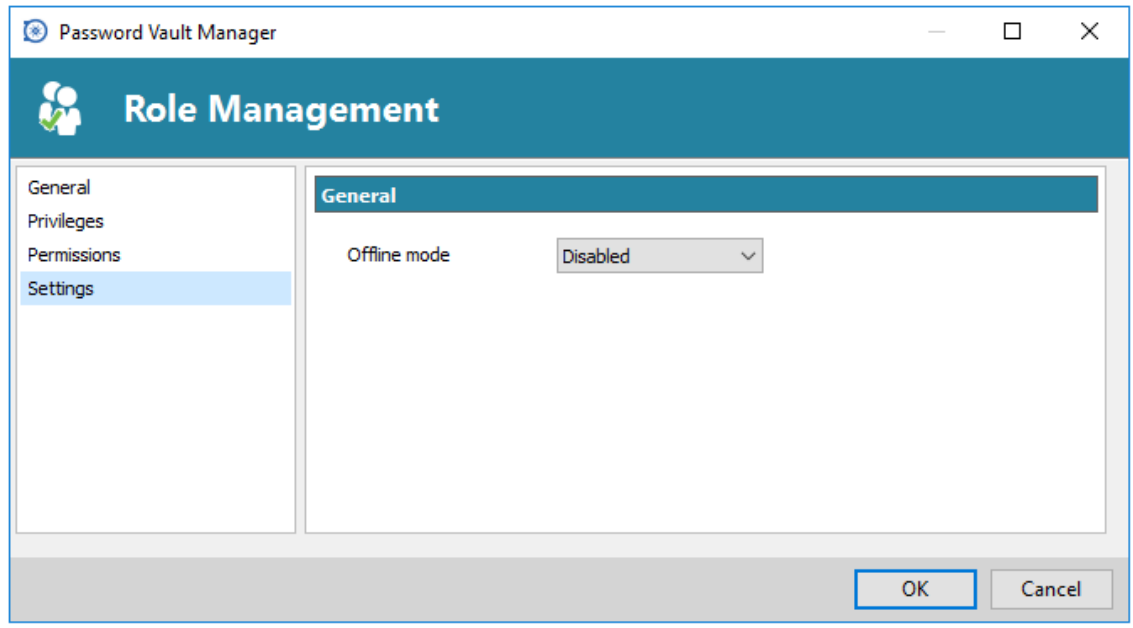


Role Management - Permissions

To learn more about Permissions please see the [Permissions](#) topic.

Settings

Allow the user to enable the [Offline Mode](#) on the data sources. This also depends on the data source being configured to allow it.



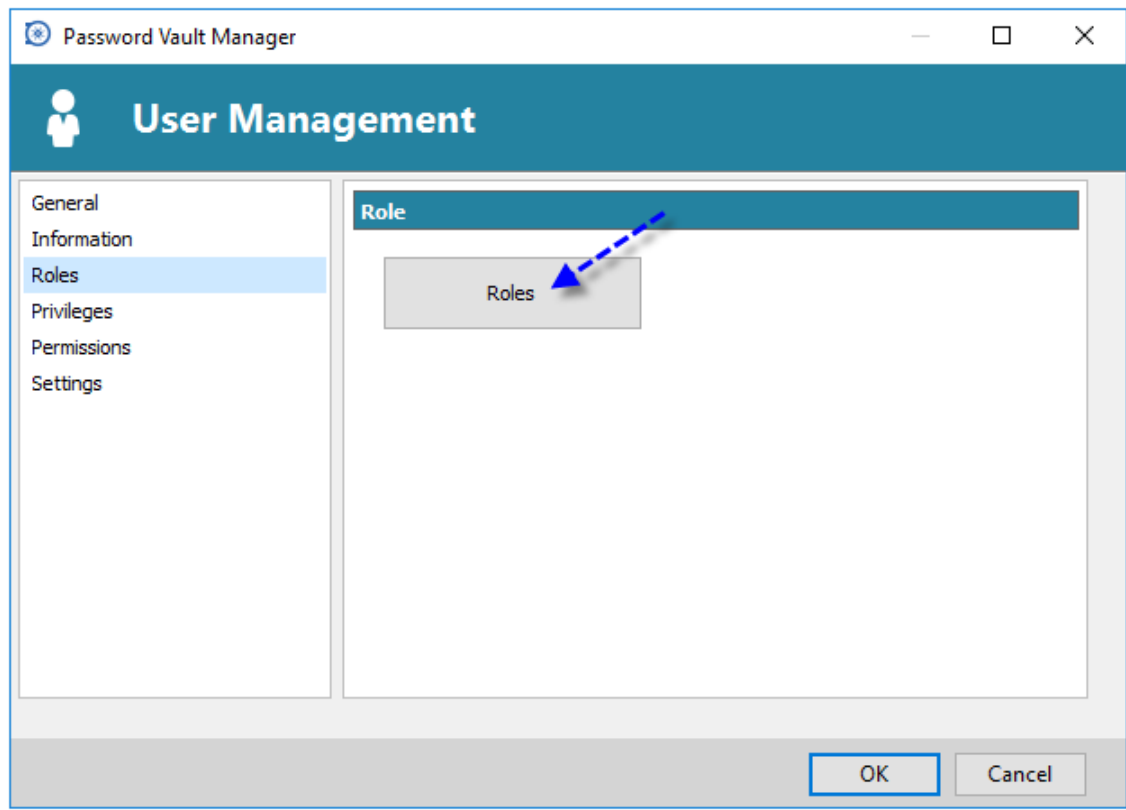
Role Management - Settings

Your can choose your Offline Mode between:

Option	Description
Disabled	Offline mode is disabled for that user.
Read-Only	A Read-only cache is allowed for the user (an Advanced Data Source is required).
Read/Write	An advanced cache, with change synchronization is allowed for the user (an Advanced Data Source is required).

Assign a Roles

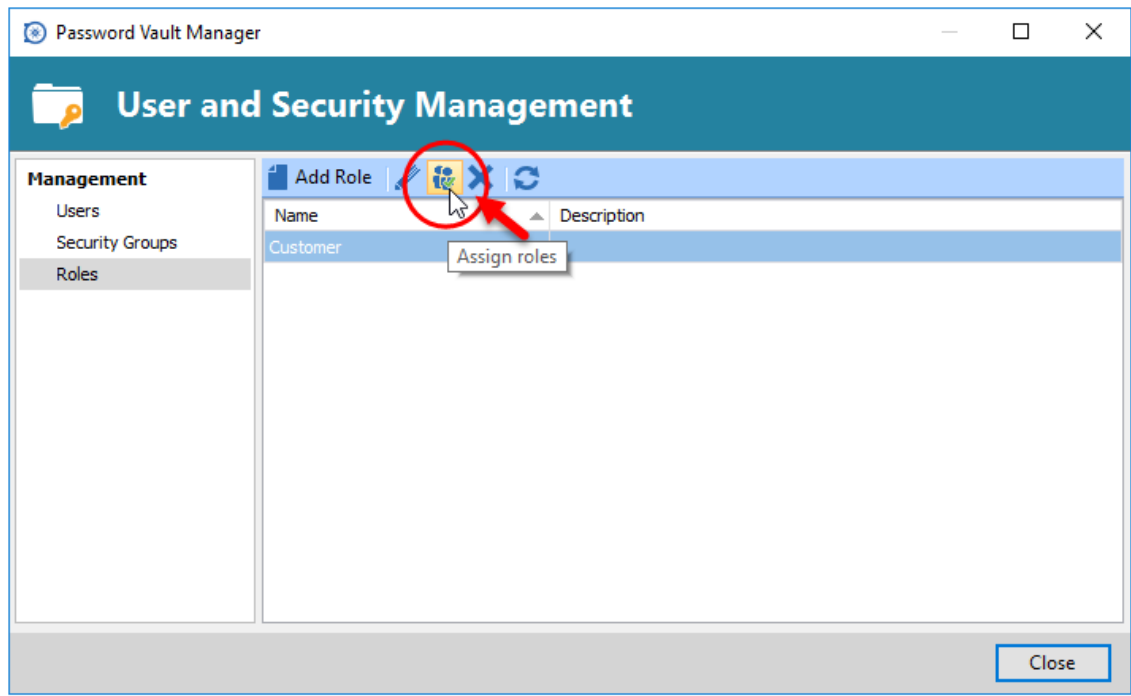
To assign role(s) to a user or to manage roles(s) for a user, you must go in **Administration - Users - Add or Edit user** - click the **Roles** button.



User Management - Roles

Assign role to multiple users

It's possible to assign a role to multiple users at the same time. In ***Administration - Roles***, click the button ***Assign Roles*** and select the users to apply the selected role. You can also click ***Select All*** or ***Unselect All***.



Roles - Assign Roles

Roles in Devolutions Server

Roles in Devolutions Server are in fact links to Active Directory groups. By leveraging Active Directory integration you can easily define access rights for all domain users in your organization. Once a domain user log in the Devolutions Server data source, their user account will be created if needed and users rights will be controlled by the defined groups.



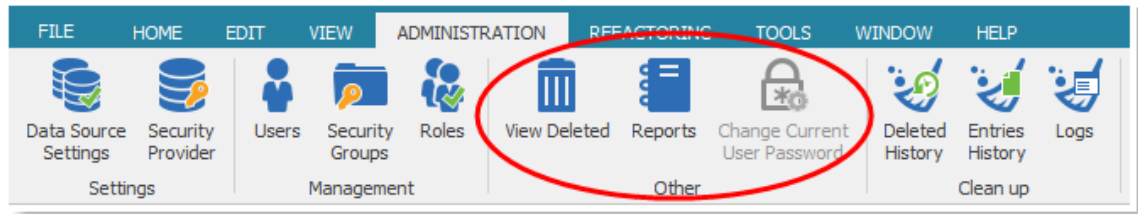
Please note that the Unsecured group permissions (the ones above the grid) are ignored. You must set them on each user individually.

For more information please see [Devolutions Server Role Management](#).

3.5.3 Other

Description

The **Other** menu is used to view your deleted entries, generate reports and will allow your users to change their current password. You have to be an administrator of the data source for some of those options to be available to you, if the menu is grayed out contact your administrator.



Administration - Other

Refer to the following topics for more information:

- [View Deleted](#)
- [Reports](#)
- [Change Current User Password](#)

3.5.3.1 View Deleted

Description

The **Administration - View deleted** option allows you to view the deleted entries as well as restore them.



This feature requires an [Advanced Data Source](#).



Administrators can permanently delete some or all deleted entries.

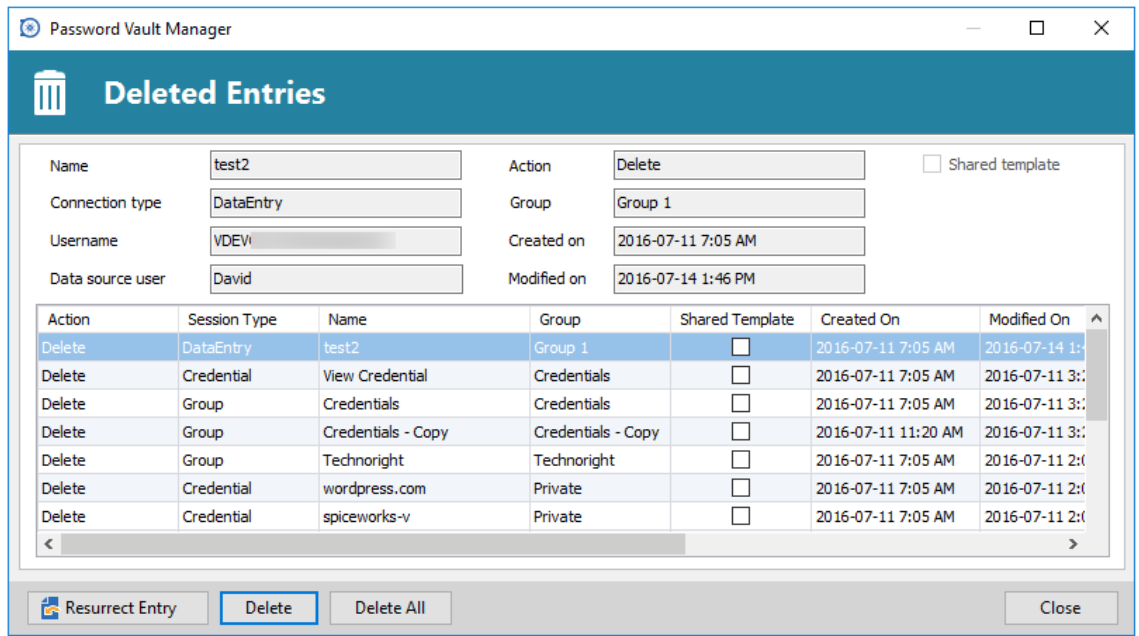


For architectural reasons, the documents stored in our Advanced Data sources are NOT protected from deletions. Once they are deleted, they cannot be restored. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings


Manage Deleted Entries

The **View deleted** generates a list containing all the entries previously deleted from your data source. You may resurrect an entry, meaning it will become an active entry again and will be shown in your data source. You may also choose to permanently delete your entries, once you have permanently deleted your entries you won't be able to resurrect them afterward.



Deleted Entries

Option	Description
Resurrect Entry	Restore a deleted entry.
Delete	Permanently delete the selected entry.
Delete All	Permanently delete all deleted entries.



Deleted entries can be resurrected as long as the Security Provider has not been changed since the deleted action.

Export deleted entries

You can use a Right-Click button on one or several lines to export them in CSV, HTML or XML format.

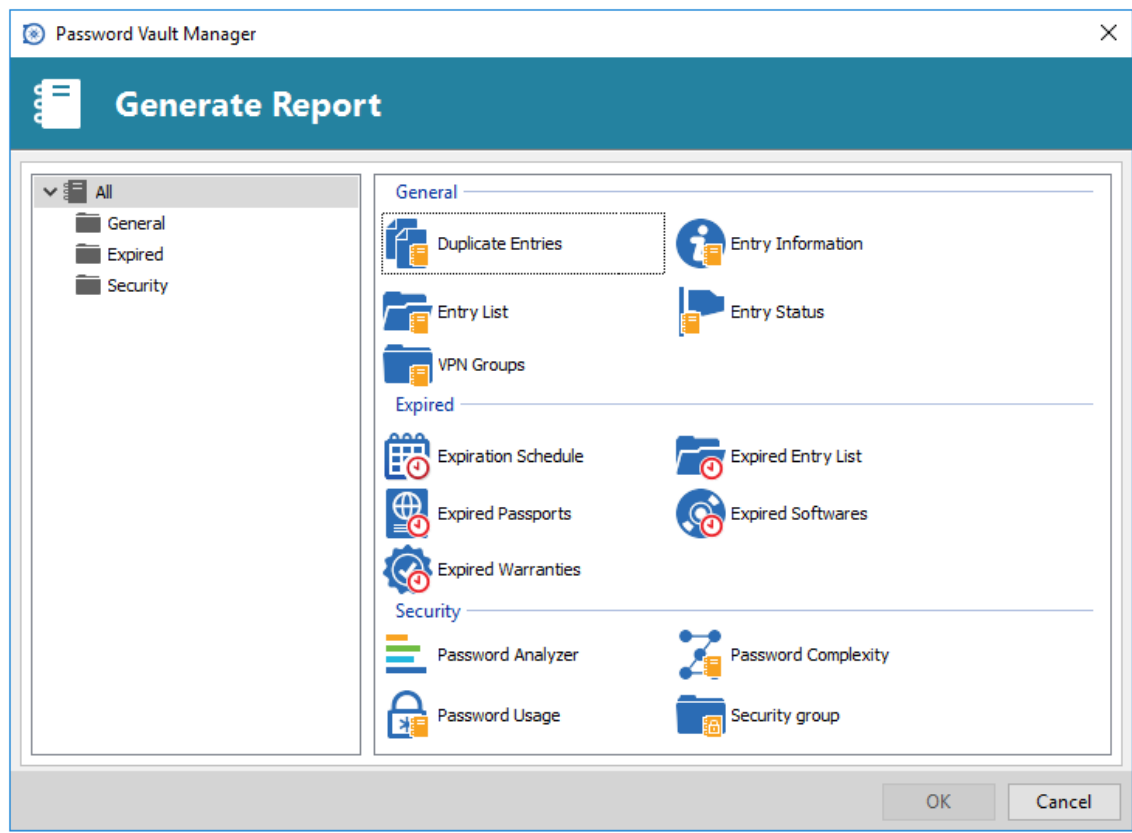
3.5.3.2 Reports

Description

The Reports section automatically generate reports regarding your credentials, entries, logs and security. You will also have the option to export your generated report which is a way to execute and export reports through a command line.

They are separated in three groups:

- [General](#)
- [Expired](#)
- [Security](#)



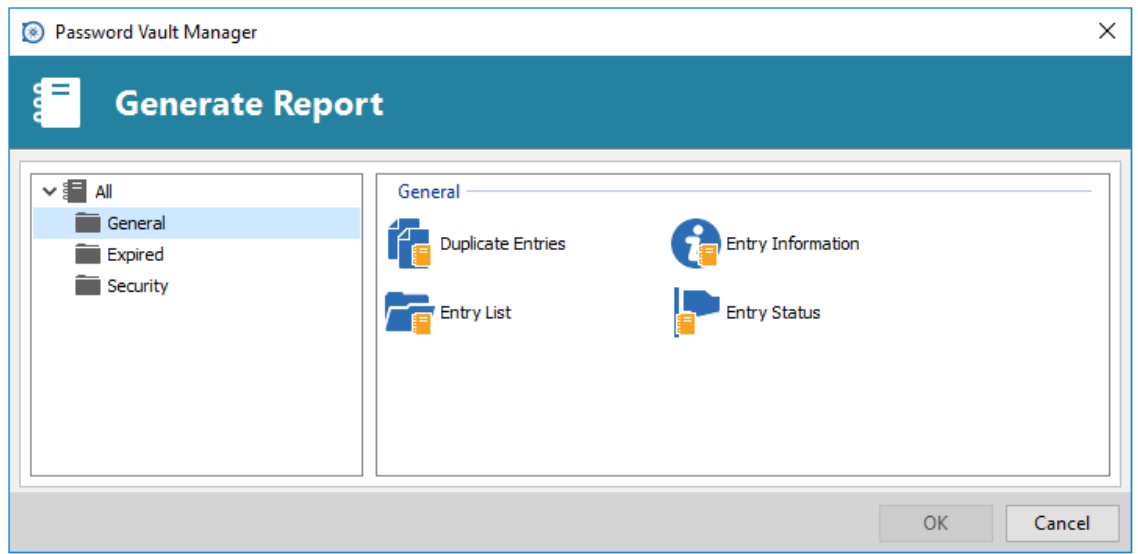
Report - Generate Report

3.5.3.2.1 General

Description

The **General** tab is used to generate reports regarding entries general information.

- [Duplicate Entries](#)
- [Entry List](#)
- [Entry Information](#)
- [Entry Status](#)



General Reports

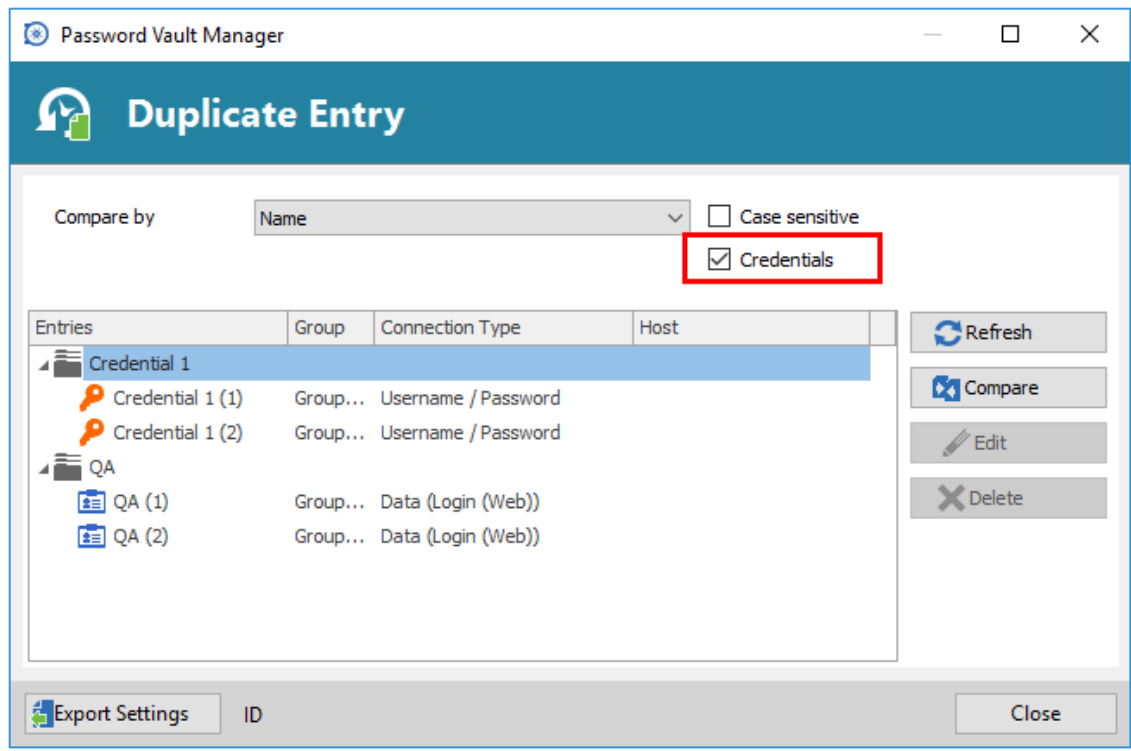
3.5.3.2.1.1 Duplicate Entries

Description

Generate a report of all duplicated entries in your data source, allowing you to compare same entries to verify if there is any difference between them.



To include **Credentials duplicate** in your Duplicate Entry Report you must enabled the **Credentials box**.

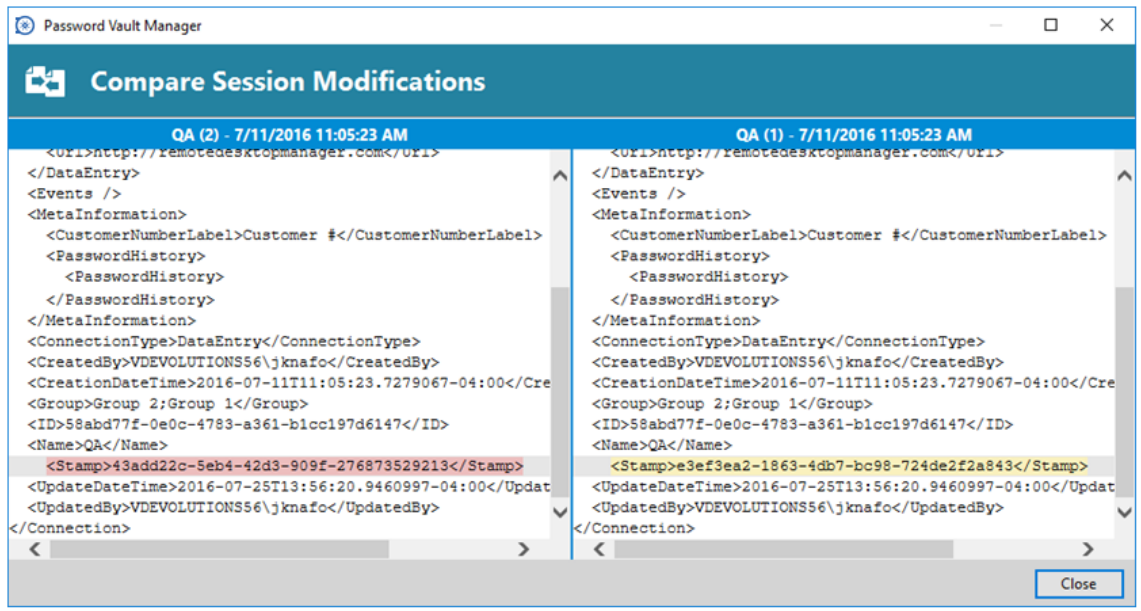


You can compare them by:

Option	Description
Name	Compare entries with the same entry name.
Connection type and host	Compare entries with the same connection type and host.

You also have the options to:

Option	Description
Refresh	Refresh your duplicate entry report.
Compare	When selecting two entries in your compare result, it will show you the differences and similarity between those two entries.
Edit	When selecting an entry in your compare result it will let you edit your entry.
Delete	When selecting an entry in your compare result it will let your delete your entry.

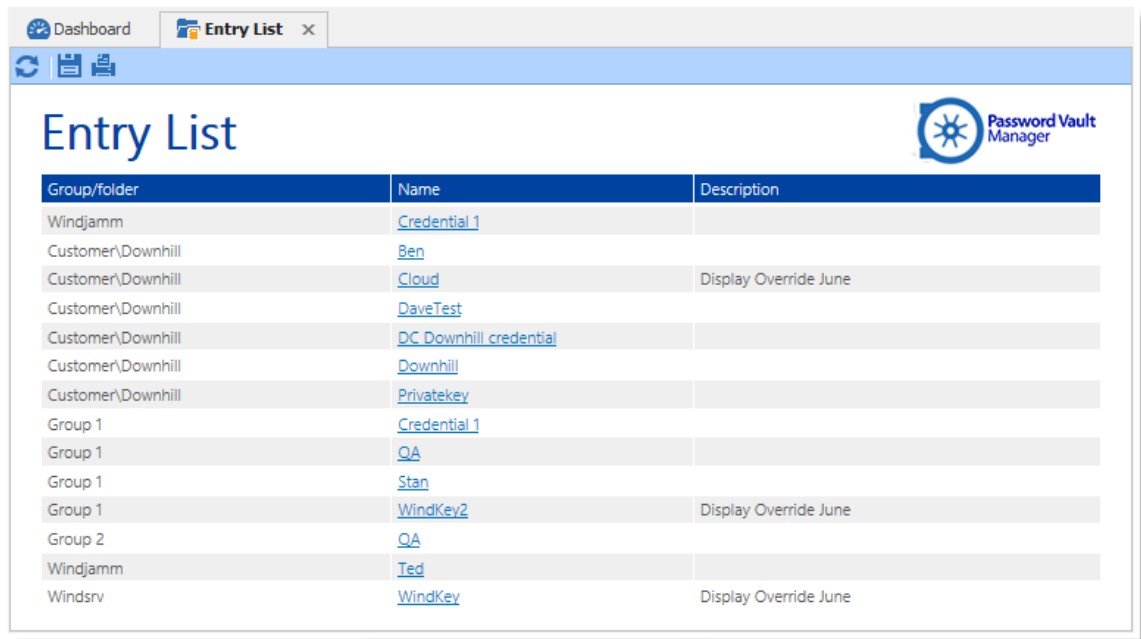


Compare Session Modifications

3.5.3.2.1.2 Entry List

Description

This report shows a simplified list of all your entries. Entry names are in fact hyperlinks to drill down directly to the entry.



Entry List Report

3.5.3.2.1.3 Entry Information

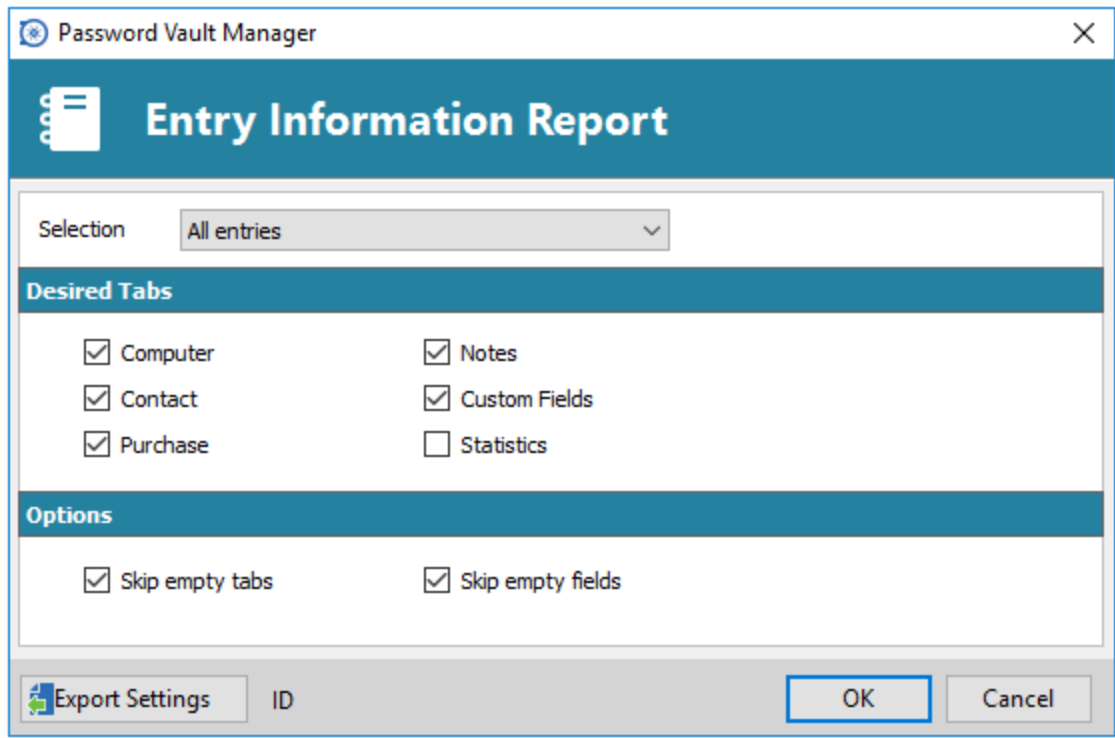
Description

Generate a report displaying the Information pane fields regarding entries. If the fields are empty the entries will not appear in the report. If you wish to have information on all your entries regarding the date it was created and by whom, enable the **Statistic** field in the **Desired Tabs** section.

Entry Information - Monday, July 25, 2016 2:19:55 PM	
Apple VPN	
Created by	VDEV
Creation date	2016-05-06 - 10:45 AM
Last update by	VDEV
Last update date	2016-06-02 - 4:03 PM
Blog	
Created by	VDEV
Creation date	2016-05-06 - 10:45 AM
Last update by	VDEV
Last update date	2016-06-02 - 4:03 PM
Chrome	
Created by	VDEV
Creation date	2016-05-06 - 10:45 AM
Last update by	VDEV
Last update date	2016-05-30 - 2:32 PM
Client 1	

Entry Information Report

Settings



Entry Information Report Settings

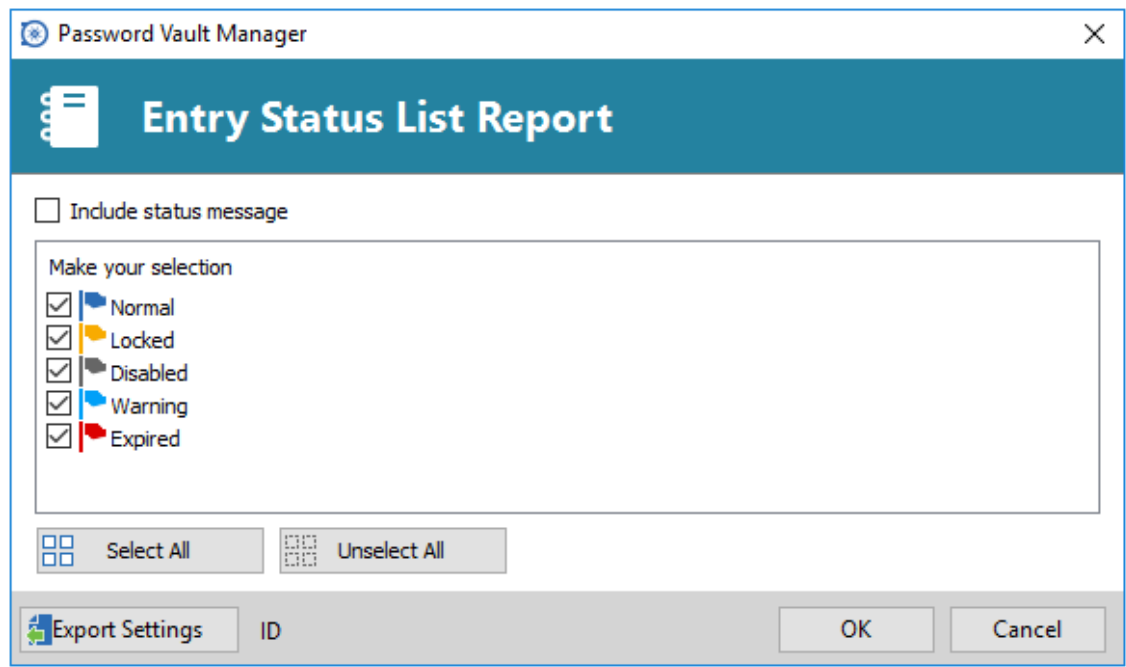
Option	Description
Selection	You can run a report on all your entries or only on currently selected entries in the navigation pane.
Desired Tabs	Choose which sub-tabs are selected for the report.
Options	You can choose between: Skip empty tabs: empty tabs do not appear in the report. Skip empty fields: empty fields do not appear in the report.

3.5.3.2.1.4 Entry Status

Description

Generate a report showing the list of all entries with an assigned status.

Select which status you wish to generate a report for. You may choose all status and may also include the [status](#) message in your report.



Entry List Status Report

Once you have done your selection you can generate your Entry Status report.

Group/folder	Name	Status
Customer/Downhill	DaveTest	Expired
Group 1	QA	Warning
Group 2	QA	Warning
Windjamm	Ted	Disabled

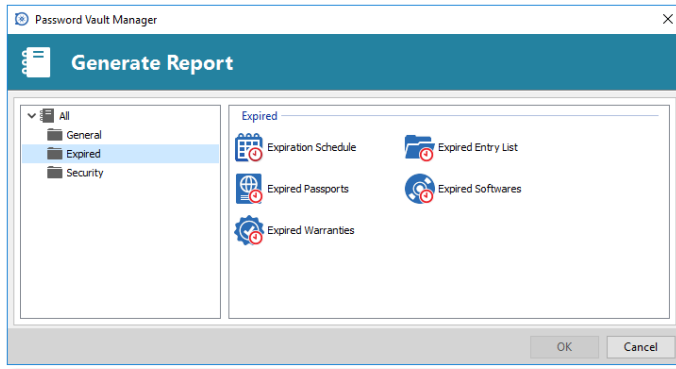
Entry Status Report

3.5.3.2.2 Expired

Description

The **Expired** tab is useful to generate reports regarding any sessions or entries with an expiration date.

- [Expiration Schedule](#)
- [Expired Entry List](#)
- [Expired Passports](#)
- [Expired Softwares](#)
- [Expired Warranties](#)



Expired Reports

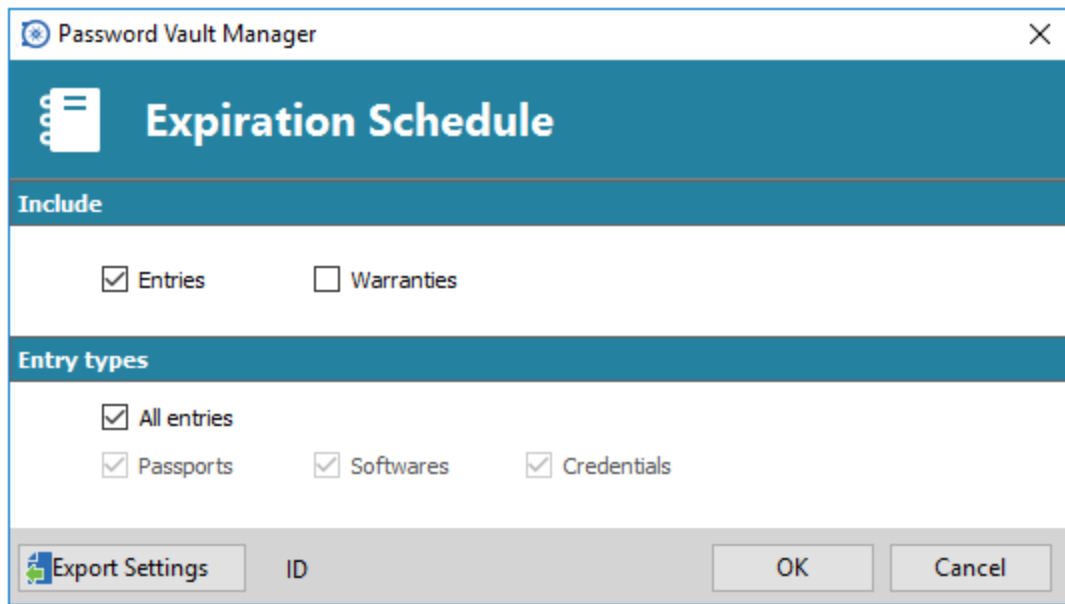
3.5.3.2.2.1 Expiration Schedule

Description

Expiration Schedule generates a calendar report on every entry that has an expiration date that is either linked to the entry or to the warranty of your entry.

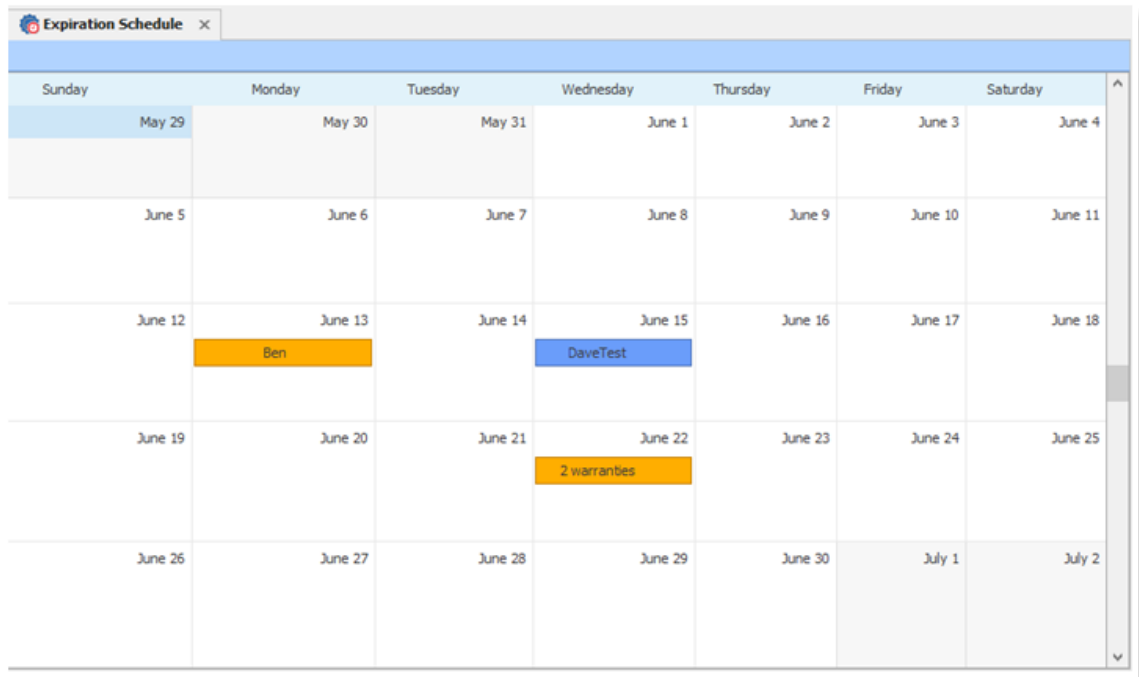
Settings

You can generate a calendar report only for Entries (select which type of entry), only for Warranties or for both.



Expiration Shedule

Expiration related to Entries appear in blue and expiration related to Warranties appear in yellow.



Expiration Calendar

3.5.3.2.2 Expired Entry List

Description

Generate a report with all the expired entries with an expiration date. Before running the report, you can select to run the report for only expired entries or only expiring entries or for both.

Group/folder	Name	Expiration	Status
Customer\Downhill	DaveTest	2016-06-15	Expired
Group 1	Expired Software	2016-06-22	Expired

Expired Entry List report

3.5.3.2.3 Expired Passports

Description

Generate a report with all the expired passport entry with an expiration date. You can select to run the report for all the expired passports, all the one that are about to expire or both.

Group/folder	Name	Expiration	Status
	Passport A1	2016-07-29	3 days remaining
	Passport B-12	2016-06-14	This passport has expired

Expired Passports Report

3.5.3.2.2.4 Expired Softw ares

Description

Generate a report with all the expired software entry with an expiration date. You can select to run the report for all the expired software, all the one that are about to expire or both.

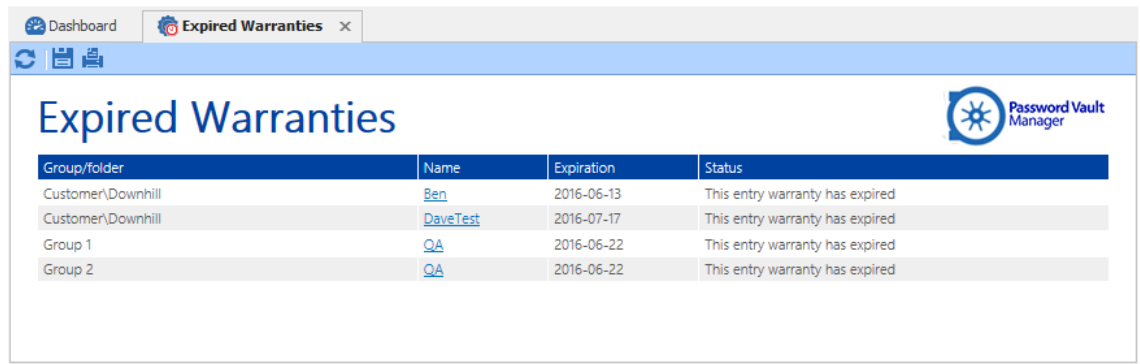
Group/folder	Name	Expiration	Status
	Computer1	2016-06-22	This software entry renewal has expired
	Laptop	2016-08-10	15 days remaining
Group 1	Expired Software	2016-06-22	This software entry renewal has expired

Expired Softwares report

3.5.3.2.2.5 Expired Warranties

Description

Generate a report including all the expired warranties of all your entries with an expiration date. You can select to run the report for all the expired entries, all the one that are about to expire or both.



Group/folder	Name	Expiration	Status
Customer\Downhill	Ben	2016-06-13	This entry warranty has expired
Customer\Downhill	DaveTest	2016-07-17	This entry warranty has expired
Group 1	QA	2016-06-22	This entry warranty has expired
Group 2	QA	2016-06-22	This entry warranty has expired

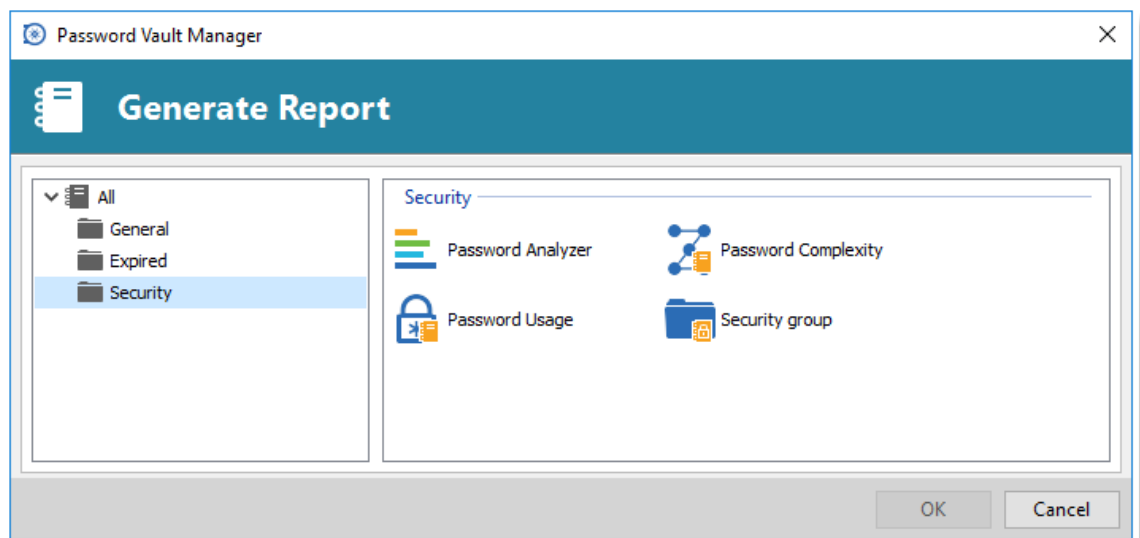
Expired Warranties report

3.5.3.2.3 Security

Description

The Security tab allows for generating reports of entries using password or linked to a security groups.

- [Password Analyzer](#)
- [Password Complexity](#)
- [Password Usage](#)
- [Security Group](#)



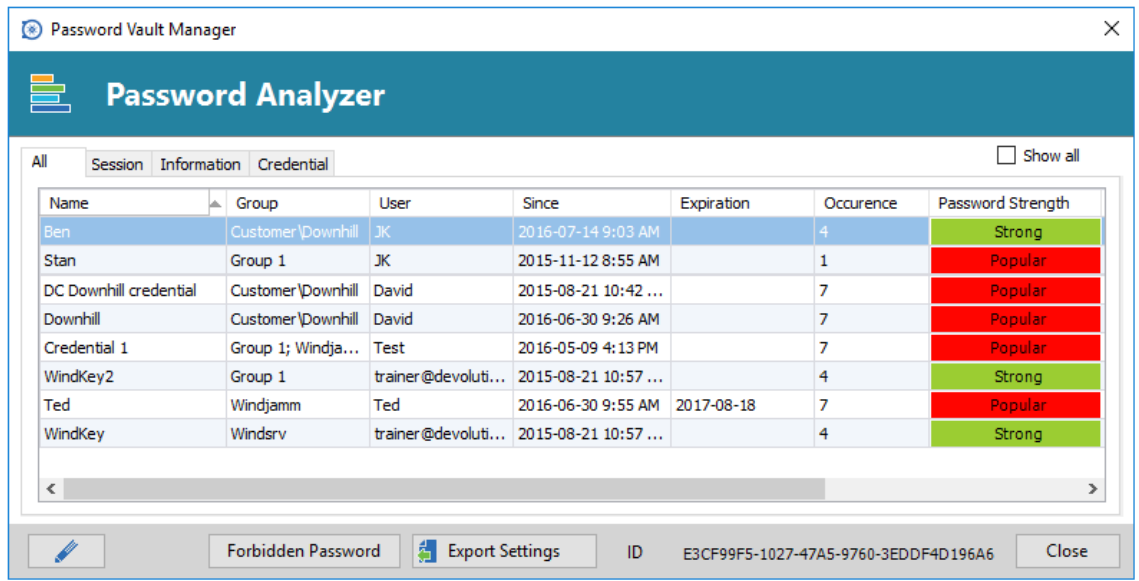
Generate Security Report

3.5.3.2.3.1 Password Analyzer

Description

Password Analyzer generates a report detailing your passwords strength and occurrences for your entries and credentials.

You can also add passwords to your [Forbidden Password](#) list, once added to the Forbidden list they will never be allowed to be used.

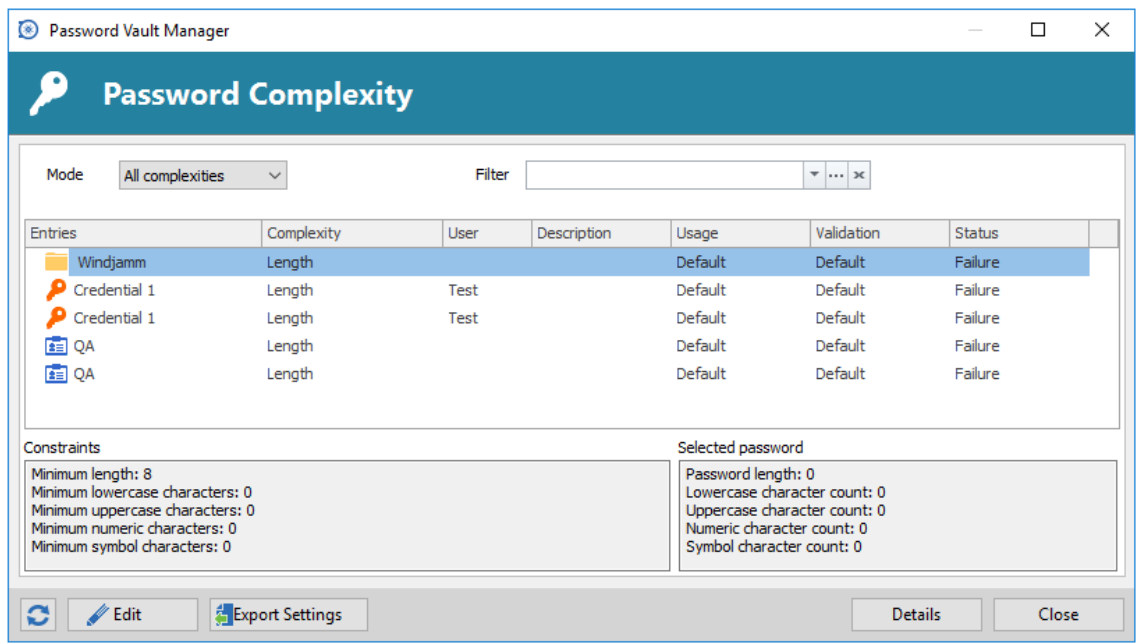


Password Analyzer report

3.5.3.2.3.2 Password Complexity

Description

Password Complexity generates a report list with every entry containing a [Password complexity](#) setting configured in the security settings.

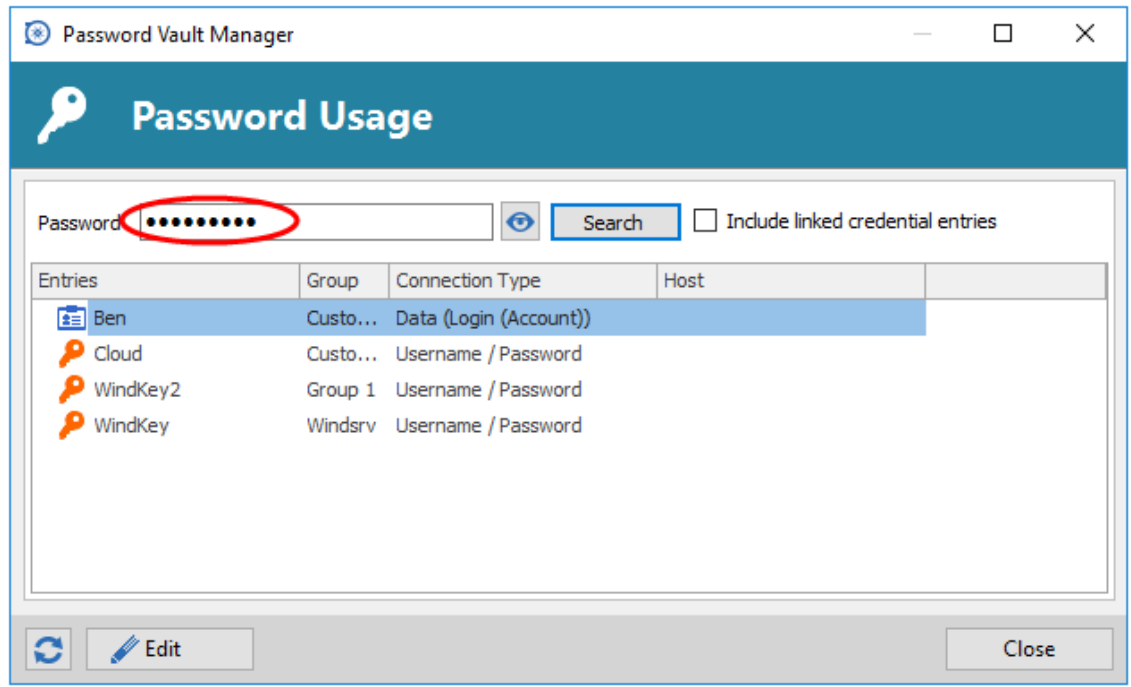


Password Complexity report

3.5.3.2.3.3 Password Usage

Description

Password Usage generates a report list with all the entries using the password you have entered in the Search field.



Password Usage report

3.5.3.2.3.4 Security Group

Description

The Security Group report displays the assigned security groups for all the entries. It's not an HTML report like the other reports.



This feature requires an [Advanced Data Source](#).

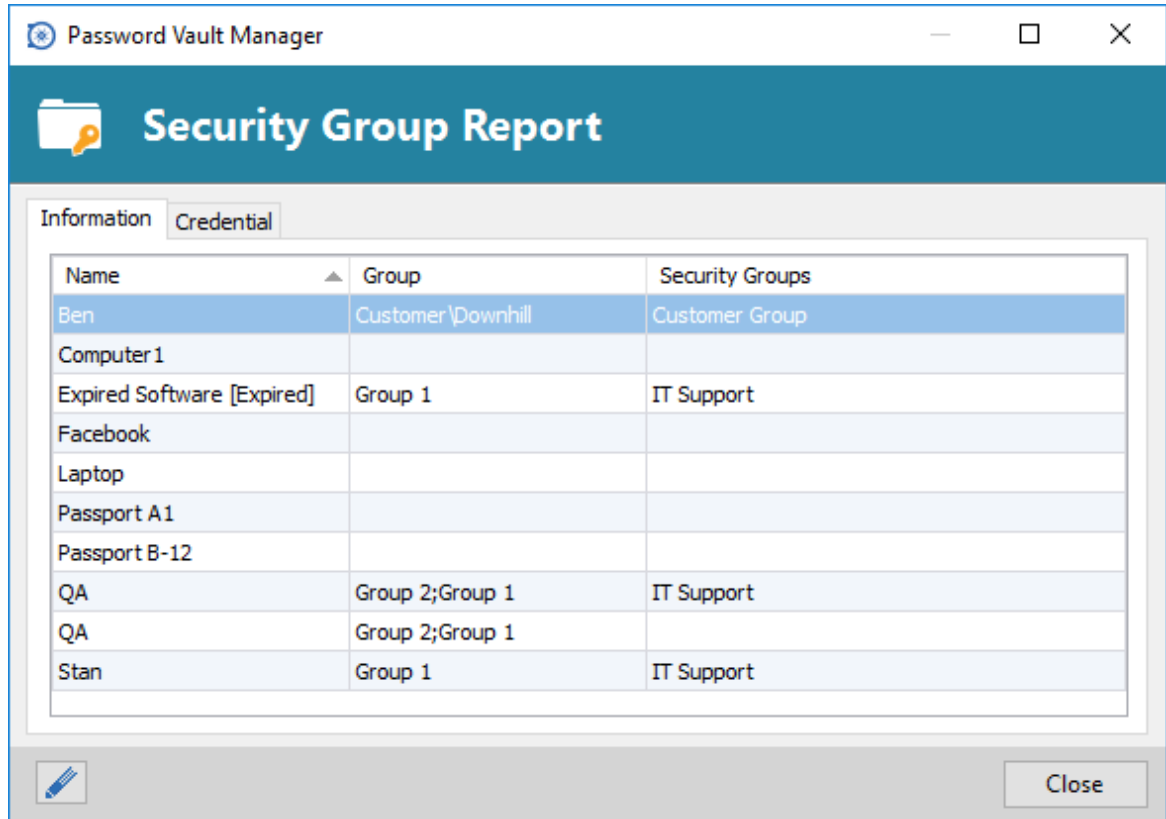


It is a best practice to run this report every time you change a security group or assign any user permissions.



Any entry without a security group is public, any user can use/edit/delete public sessions. In a typical team environment no entries should be without a security group.

The dialog has tabs that organizes entries by types: Information and Credential. Sub-connections are also included in this report and are prefixed with their parent's name. You can use the edit button to quickly edit a selected entry.



Security Group report

3.5.3.2.4 Export Report

Description

The Export Reports is a way to execute and export reports through a command line. You can use this feature in a shortcut or in a batch file and use the Windows task scheduler to execute it.

You will be able to export your report for every report except for the Entry List, Password Usage and Security Group.

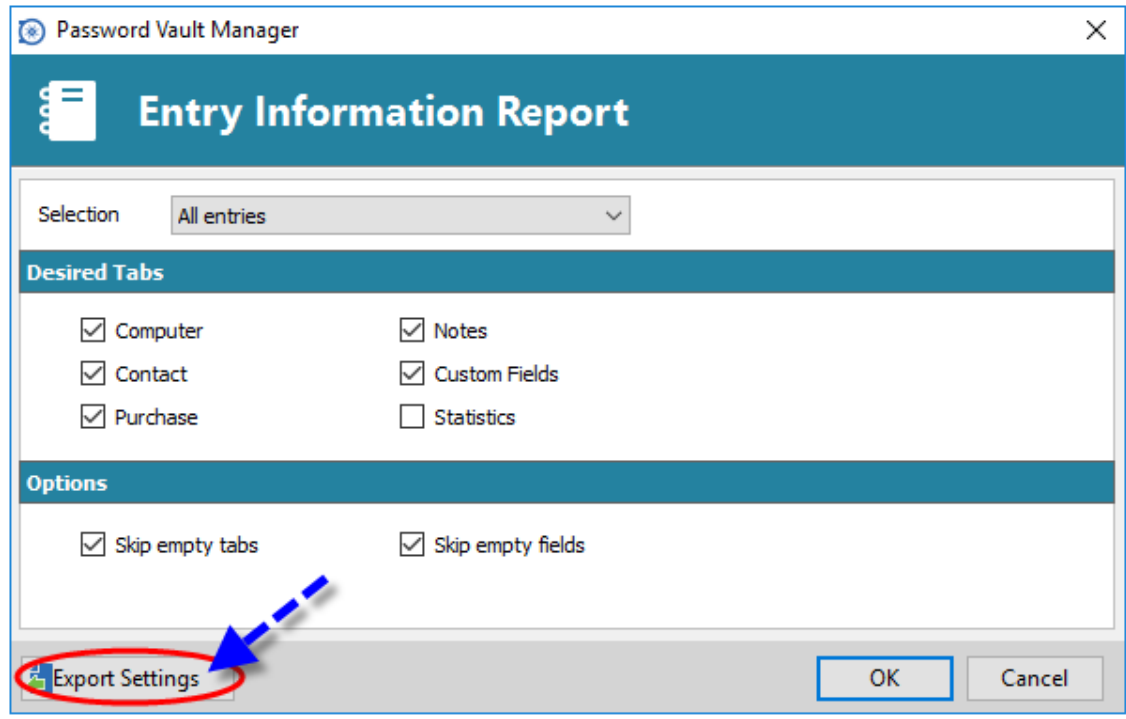


You must have the rights to run report in Remote Desktop Manager to use this feature.

Settings

You will have to start with exporting your report settings to create the .rdr file that the command line use to generate the reports.

1. Select your Report in **Administrations - Report** and then select the option **Export Settings**. It will create an .rdr file containing all your report settings.



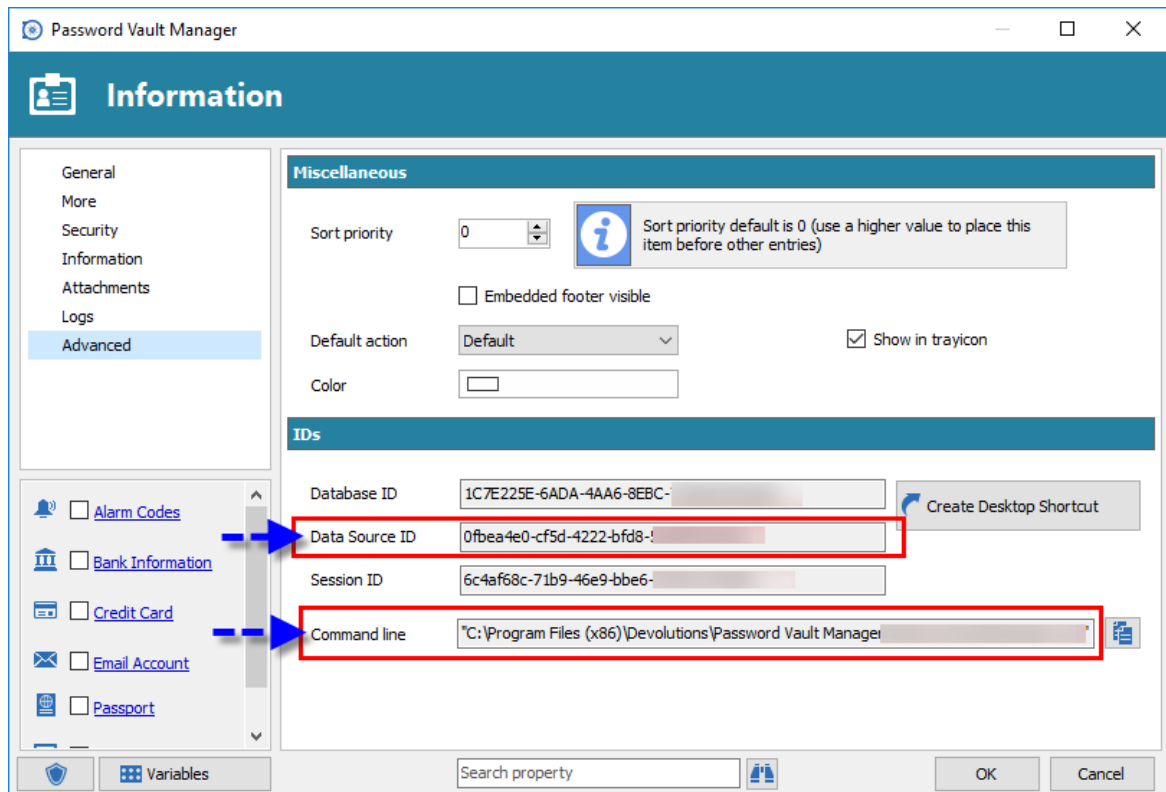
Export Settings

2. In your Windows Command Prompt enter the following command line:

```
C:\*** /DataSource:*** /report:***/reportoutput:"***" /reportsettings:"***.rdr" /closeapp
```

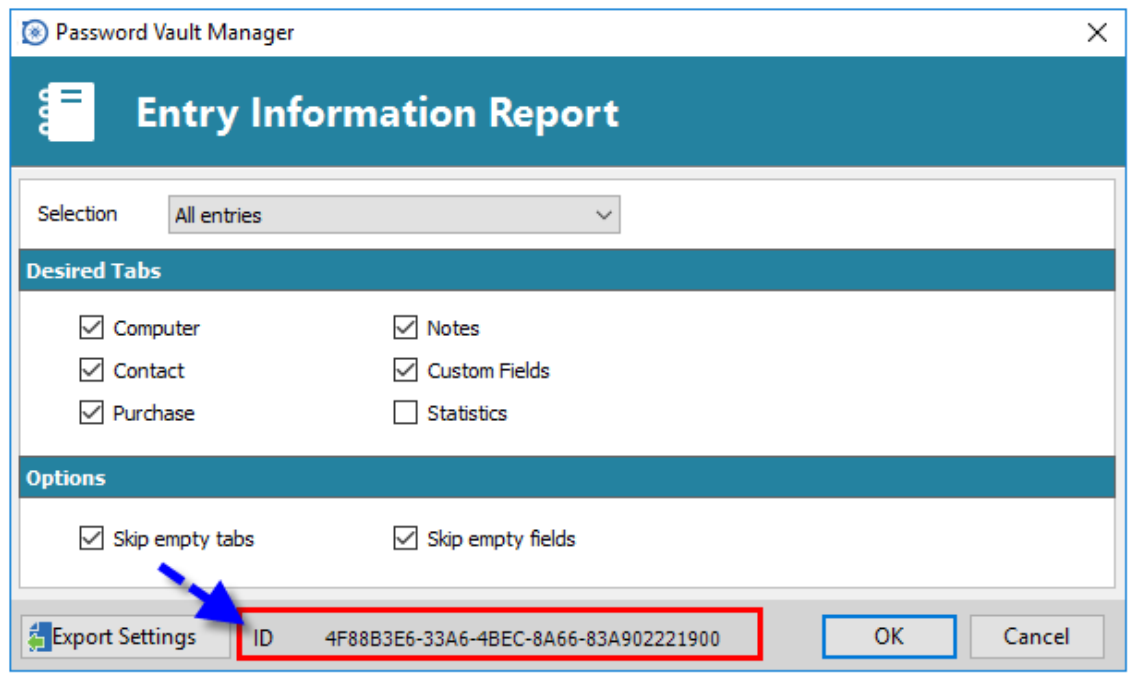
Parameters	Description
C:\	Enter the path used to start your Remote Desktop Manager application (path of the RemoteDesktopManager.exe file)
/DataSource	Specify the data source ID.
/report	Specify the type of report to generate or the report ID.
/reportoutput	Specify the path to save your report and the name for the newly generated report.
/reportsettings	Specify the path of your report settings file (.rdr).
/closeapp	This command will close the Remote Desktop Manager if the application was started from a command line. If Remote Desktop Manager was already open before launching the command it won't close the application.

To find your Data Source ID and the Command Line use to start Remote Desktop Manager you must edit one of your entry and select the **Advanced** side menu.



Entry Advanced side menu

To find your Report ID go in **Administration - Report** and select the report to generate. Clicking on the ID will automatically copy the ID number.



Entry Information Report ID

Here is a list of types of Reports you can find in Remote Desktop Manager and the name to enter in the command line to generate the report:

Report type in Remote Desktop Manager	Report name (type) to insert in the Command line
Entry Information	EntryInformation
Entry Status	ConnectionStatus
Duplicate Entries	DuplicateEntry
Expiration Schedule	CalendarExpiredEntry
Expired Entry List	ConnectionExpiredEntry
Expired Passports	ConnectionExpiredPassports
Expired Softwares	ConnectionExpiredSoftwares
Expired Warranties	ConnectionExpiredWarranties
Password Complexity	PasswordComplexity
Password Analyzer	PasswordAnalyzer

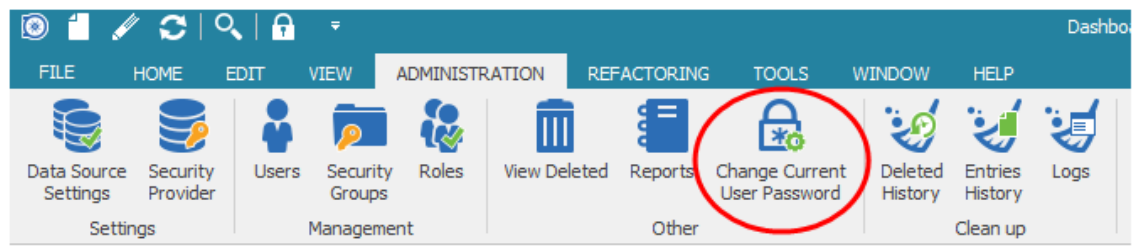
Here is an example of a command line for an Entry Information Report:

```
C:\Program Files (x86)\Devolutions\Remote Desktop Manager\RemoteDesktopManager.exe /D
/reportoutput:C:\dev\devolutions\Rapport\rapportEntry /reportsettings:C:\dev\devoluti
```

3.5.3.3 Change Current User Password

Description

If you are a data source User and wish to change the password that the Administrator has assigned you to access the data source you will find the option in **Administration - Change Current User Password**.

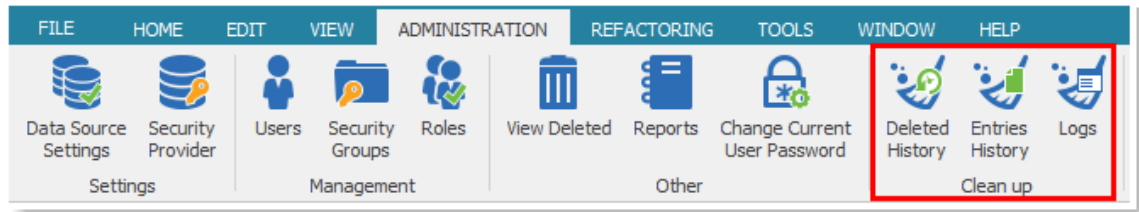


Administration - Change Current User Password

3.5.4 Clean up

Description

In **Administration - Clean up** you will have the option to manage your deleted history, your entries history or your logs.



Clean up

Refer to the following topics for more information:


- [Deleted History](#)
- [Entries History](#)
- [Logs](#)

3.5.4.1 Deleted History

Description

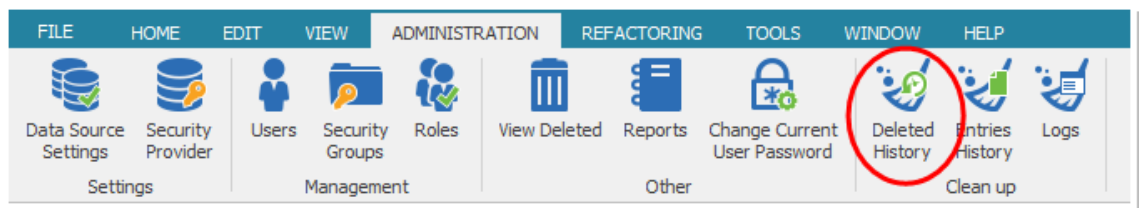
The **Deleted History** permanently deletes entries that had been previously deleted. Full history is always preserved because every entry "version" is kept in historical tables.

 This feature requires an [Advanced Data Source](#).

 You must be an administrator of the data source to perform this action.

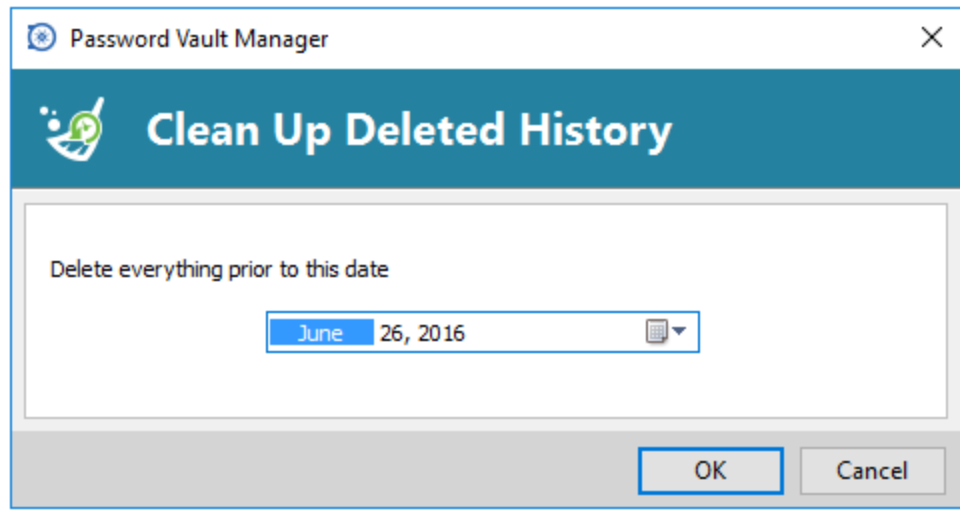
Settings

1. To permanently delete entries history go in **Administration - Clean up - Deleted History**.



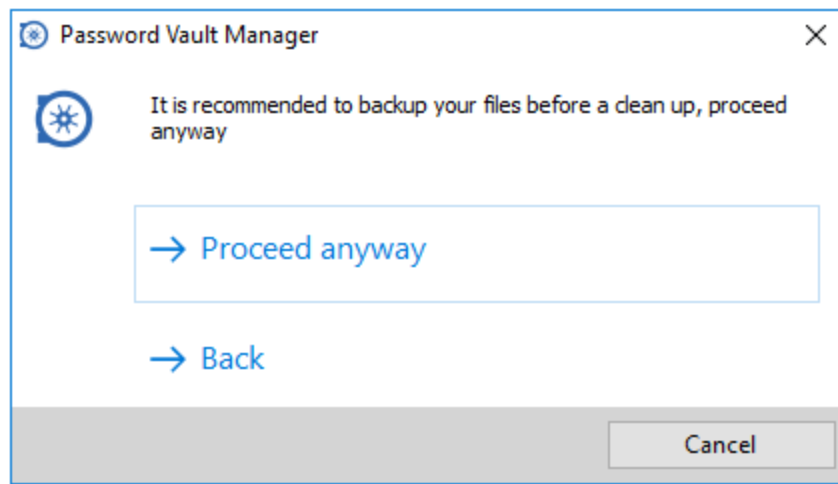
Administration - Deleted History

2. Select prior to which date you wish to permanently delete your deleted entries history.



Clean up Deleted History

3. Confirm your choice prior to permanently delete your deleted entries history.



Confirmation window

There is no History backup, hence we strongly recommend to do a backup before proceeding.


The **Administration - View deleted** option allows you to view the deleted entries as well as restoring them.



This feature requires an [Advanced Data Sources](#).



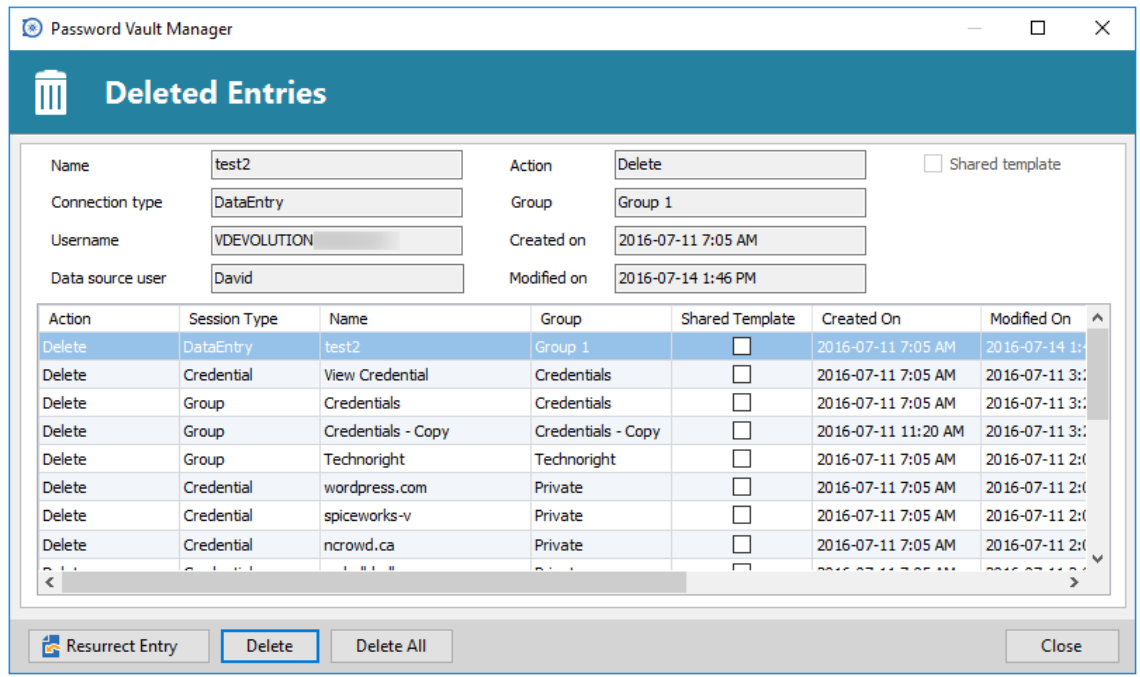
Only Administrators of the data source can permanently delete some or all deleted entries.

 For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update of our products.

Settings


Manage Deleted Entries

The **View deleted** will generate a list containing all the entries previously deleted from your data source. You may resurrect an entry, meaning it will become active entry again and will be shown in your data source. You may also chose to permanently delete your entries, once you have permanently deleted your entries you won't be able to resurrect them afterward.



Deleted Entries

Option	Description
Resurrect Entry	Use this button to restore an entry.
Delete	Permanently delete the selected entry.
Delete All	Permanently delete all the deleted entries.

 Deleted entries can be resurrected as long as the [Security Provider](#) has not been changed since the delete action.

Export deleted entries list

You can use the **Right-click** button on one or several lines to export them in CSV, HTML, XLS or XML format.

3.5.4.2 Entries History

Description

The Entry History deletes the history attached to your entry, you can find the history by right clicking on your entry and selecting **View - Entry history**.



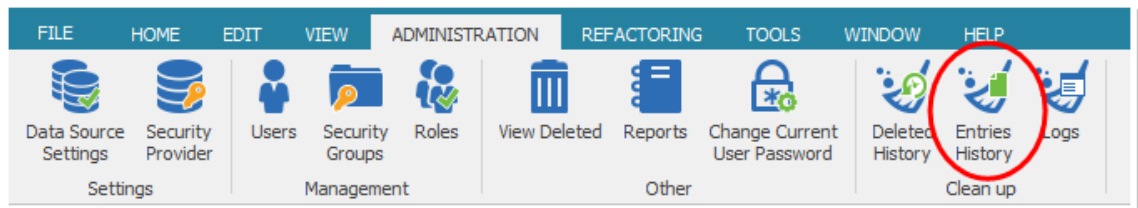
This feature requires an [Advanced Data Source](#).



You must be an administrator of the data source to perform this action.

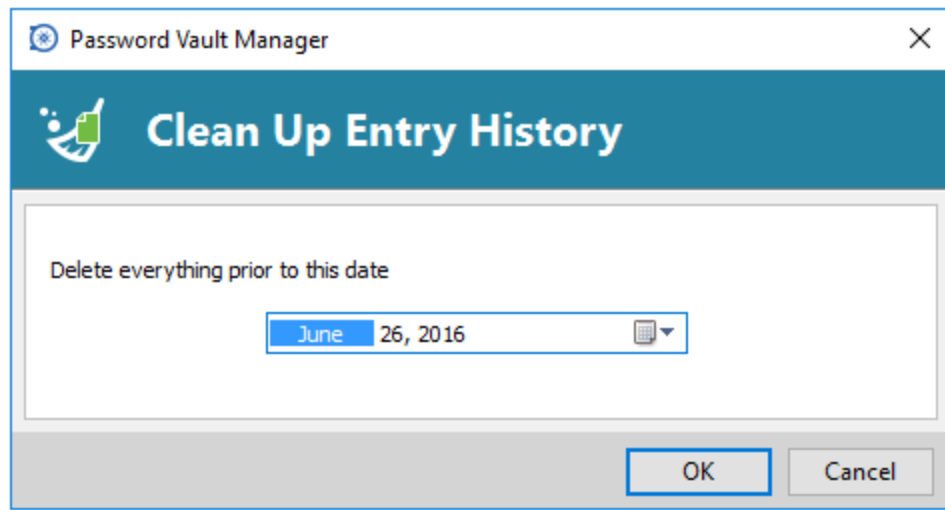
Settings

1. To Delete the **Entry History** go in **Administration - Clean up - Entry History**.



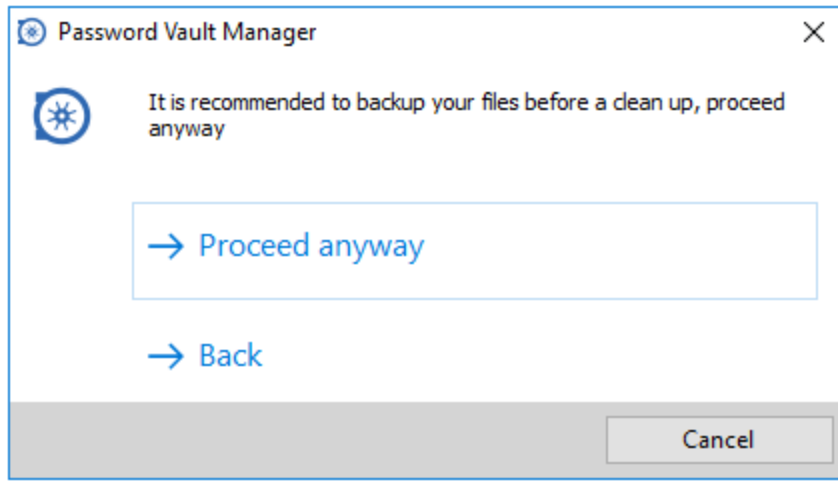
Administration - Entries History

2. Confirm your choice prior to permanently delete your entry history.

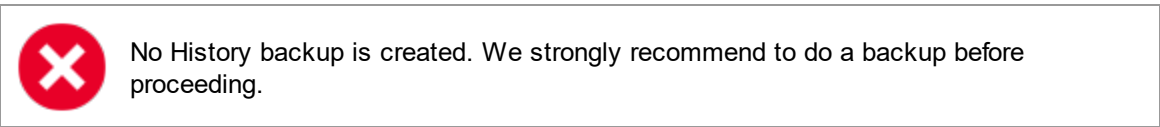


Clean Up Entry History

3. Another window will appear to confirm your choice of deleting all the history prior to the chosen date.



Confirmation window



3.5.4.3 Logs

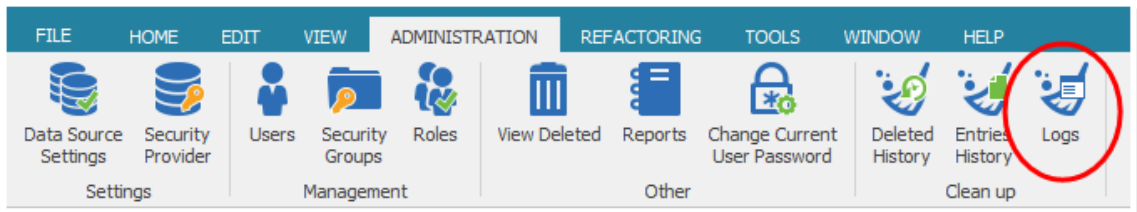
Description

The **Logs** would delete all of your data source logs.



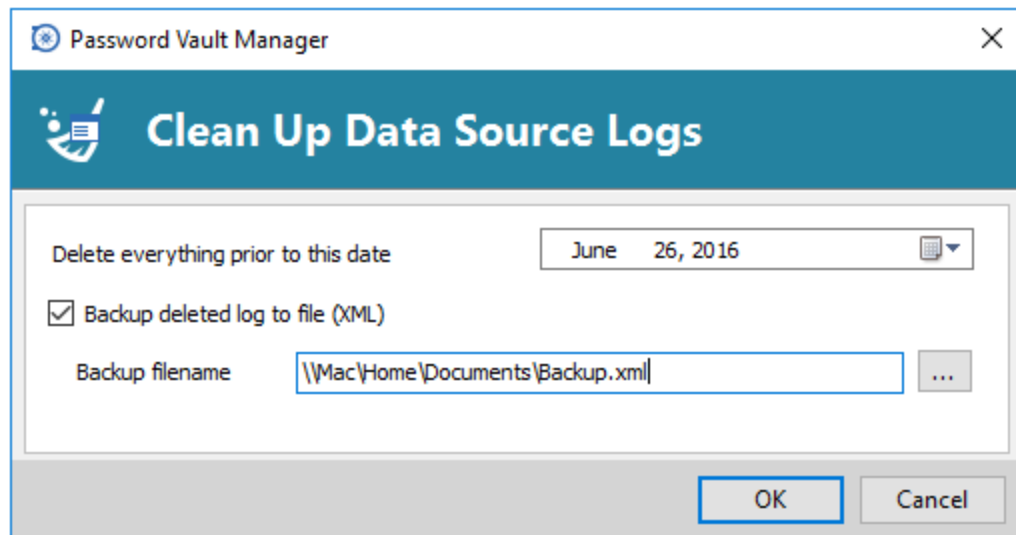
Settings

1. To delete your data source logs go under **Administration - Clean up - Logs**.



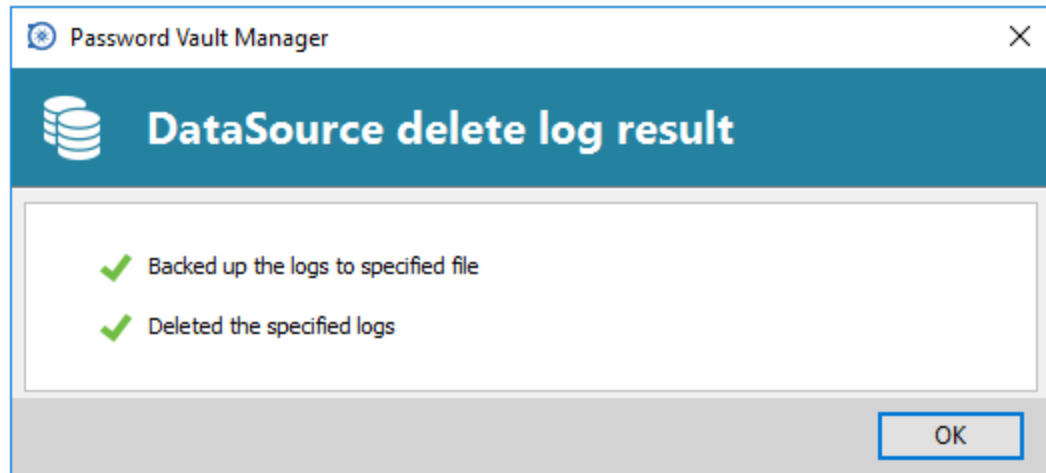
2. Confirm prior to which date you wish to delete your logs. We strongly suggest to do a backup of your logs, just enabled the **Backup deleted log to file** option and enter a your backup filename and path (ex:

\\C:\Home\Documents\Backup.xml). A backup of your log will be created as an XML file although it will then be impossible to import this file in Remote Desktop Manager.



Clean Up Data Source Logs

3. Once you have entered your Backup file name and proceeded with the clean up a delete log result window will appear.

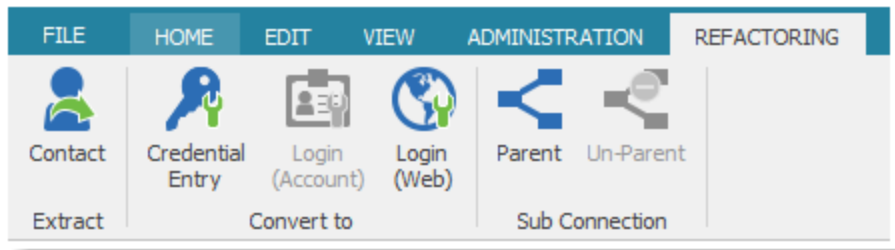


Data Source Delete Log Result

3.6 Refactoring

Description

The **Refactoring** ribbon is used to modify the structure of your sessions, create new entry or to convert an entry in another entry type.



Refactoring

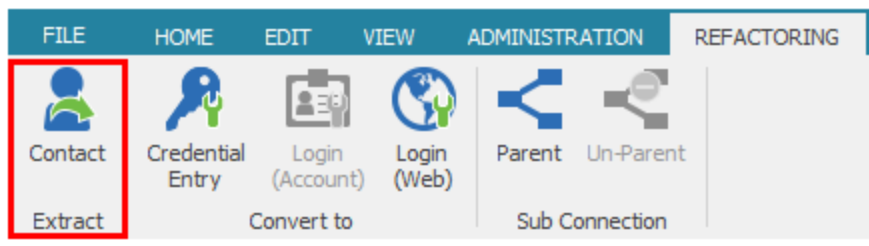
Please consult the following topics for more information:

- [Extract](#)
- [Convert To](#)
- [Sub Connection](#)

3.6.1 Extract

Description

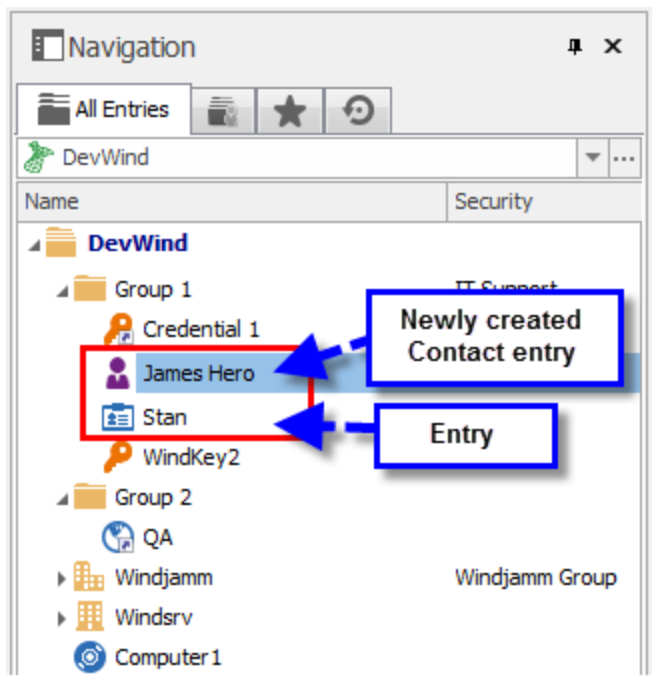
Use the **Refactoring - Extract** to extract the contact information held in an entry.



Refactoring - Extract

Settings

The **Contact** extract the contact information of the selected entry. It will then automatically create a new Contact entry with the extracted information and link it to the current session.



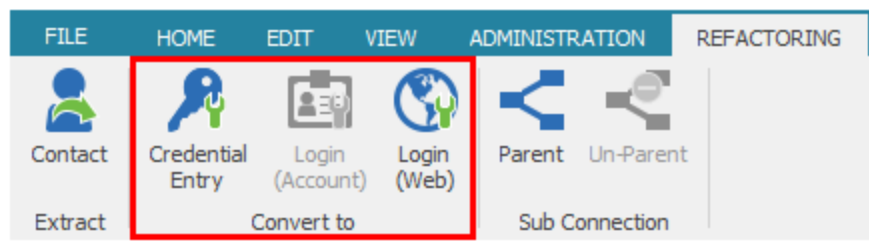
Newly created Contact entry

3.6.2 Convert To

Description

Use the **Refactoring - Convert to** to convert the current entry into another type.

Settings



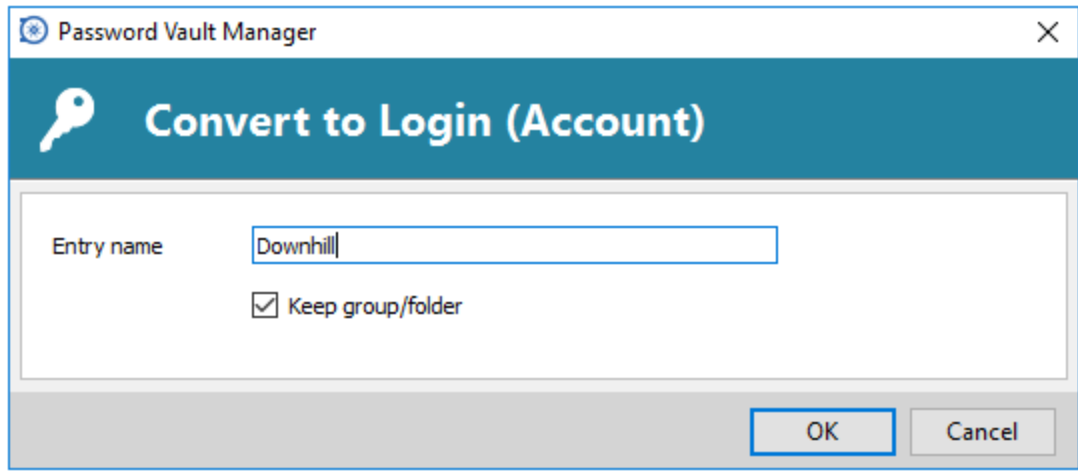
Convert to

There are currently three **Convert to** types and their actions are enabled only when the source entry is compatible with the destination.

Option	Description
Credential Entry	Convert your selected entry in a Credential entry.
Login (Account)	Convert your selected entry in a Login (Account) entry.

Login (Web)	Convert your selected entry in a Login (Web) entry.
-------------	---

When converting one of your entry you will be presented with a dialog to enter a name for the new entry. You can also specify to keep the entry in the same folder. The dialogs are mostly the same for all three Convert to.



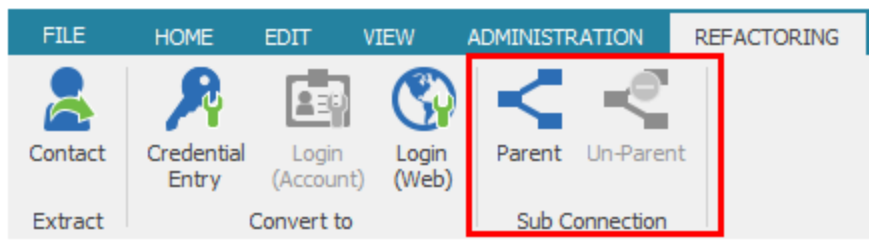
Convert to a Login (Account)

3.6.3 Sub Connection

Description

The **Refactoring - Sub Connection** allows you to set a connection under a parent connection or reverse the process.

Settings



Refactoring - Sub Connection

Option	Description
Parent	Available for connections that are not parents themselves, this allows you to move a connection under a parent connection.
Un-Parent	Available only for sub connections, this allows you to move a connection out from under a parent connection.

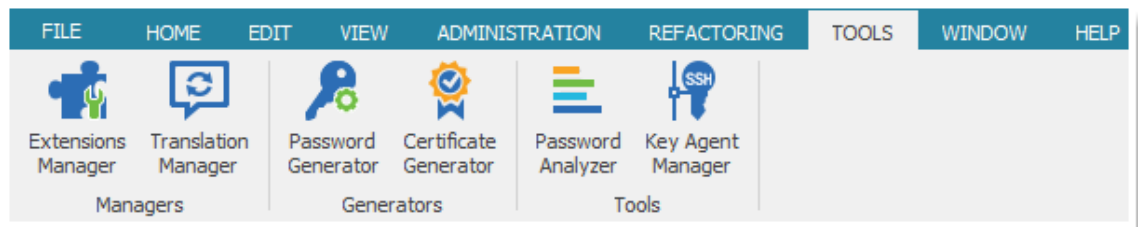


If you want to move a sub connection under a new parent it can't be performed in a single action. You must first Un-parent it to be a standalone connection and then use the Parent command.

3.7 Tools

Description

The **Tool** ribbon is used to manage extensions, generate password or certificate and holds your Key Agent Manager and your Password Analyzer.



Tools

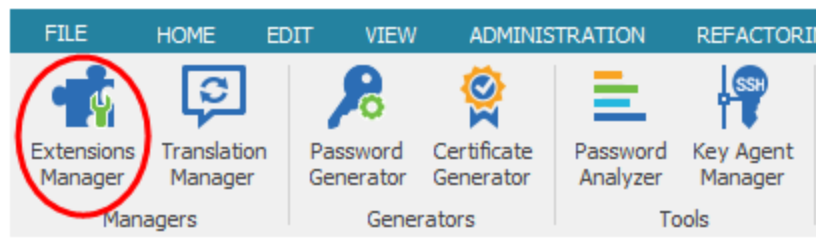
Please consult the following topics for more information:

- [Extensions Manager](#)
- [Translation Manager](#)
- [Password Generator](#)
- [Certificate Generator](#)
- [Password Analyzer](#)
- [Key Agent Manager](#)

3.7.1 Extensions Manager

Description

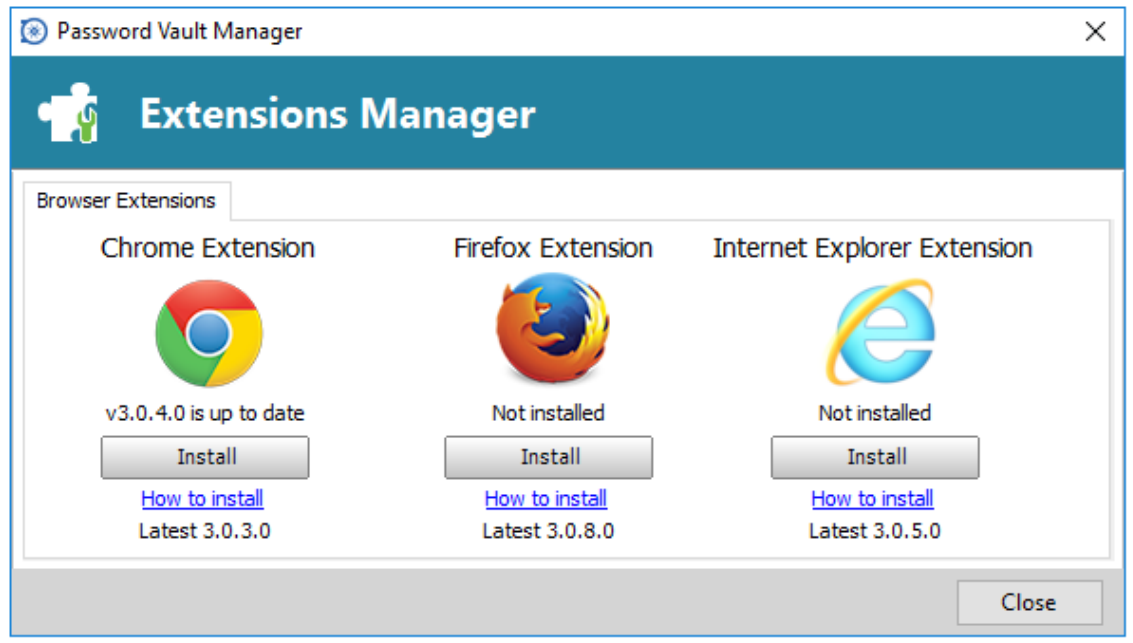
The **Extensions Manager** is available in the **Tools - Extensions Manager** menu. It's use to simplified the installation of extensions in Remote Desktop Manager.



Tools - Extensions Manager

Settings

Browser Extensions



Browser Extensions

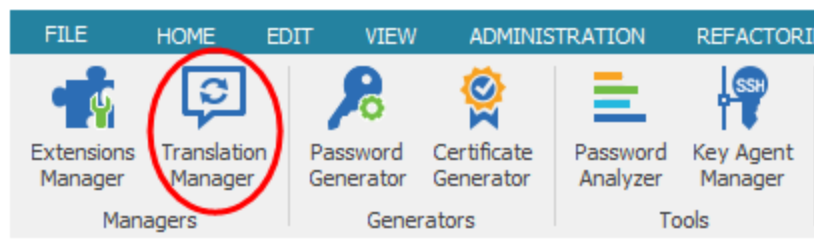
Option	Description
Chrome Extension	You can install the Chrome Extension directly by clicking Install or follow the steps indicated in Chrome Extension topic.
Firefox Extension	You can install the Firefox Extension directly by clicking Install or follow the steps indicated in Firefox Extension topic.
Internet Explorer Extension	You can install the Internet Explorer Extension directly by clicking Install or follow the steps indicated in Internet Explorer Extension topic.

3.7.2 Translation Manager

Description

Use the **Tools - Translation Manager** to easily translate resources used by our products.

The translation manager is in fact a cloud based translation repository that is managed by an external application named *Devolutions Localizer*, developed by our team at Devolutions.

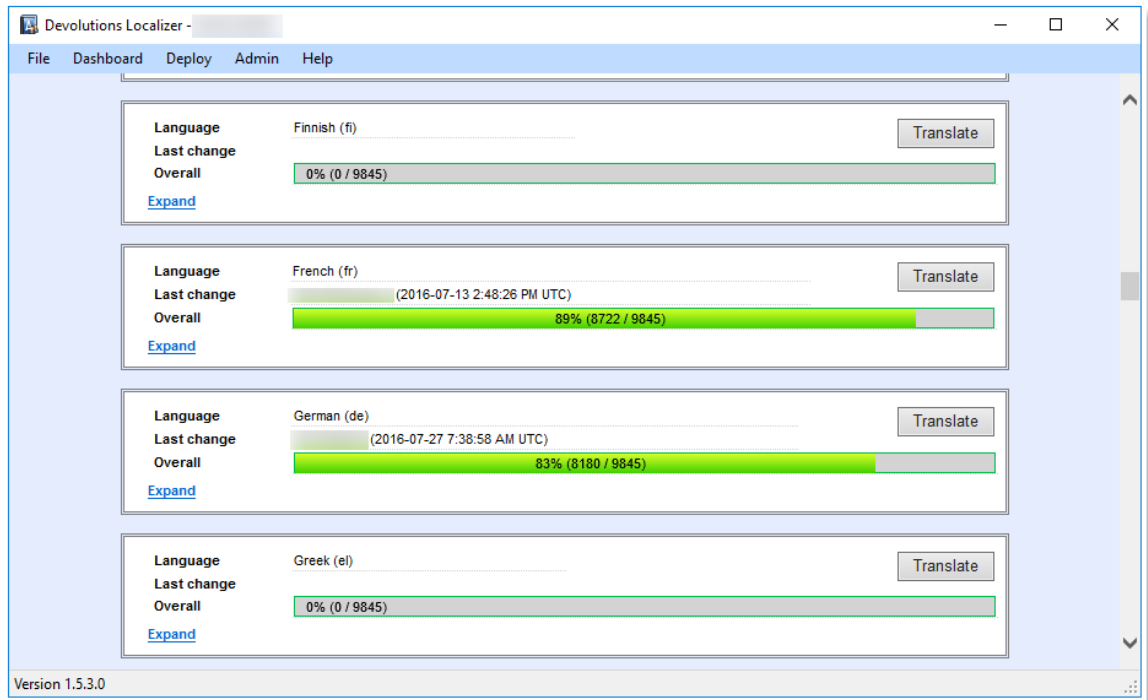


Tools - Translation Manager

Settings

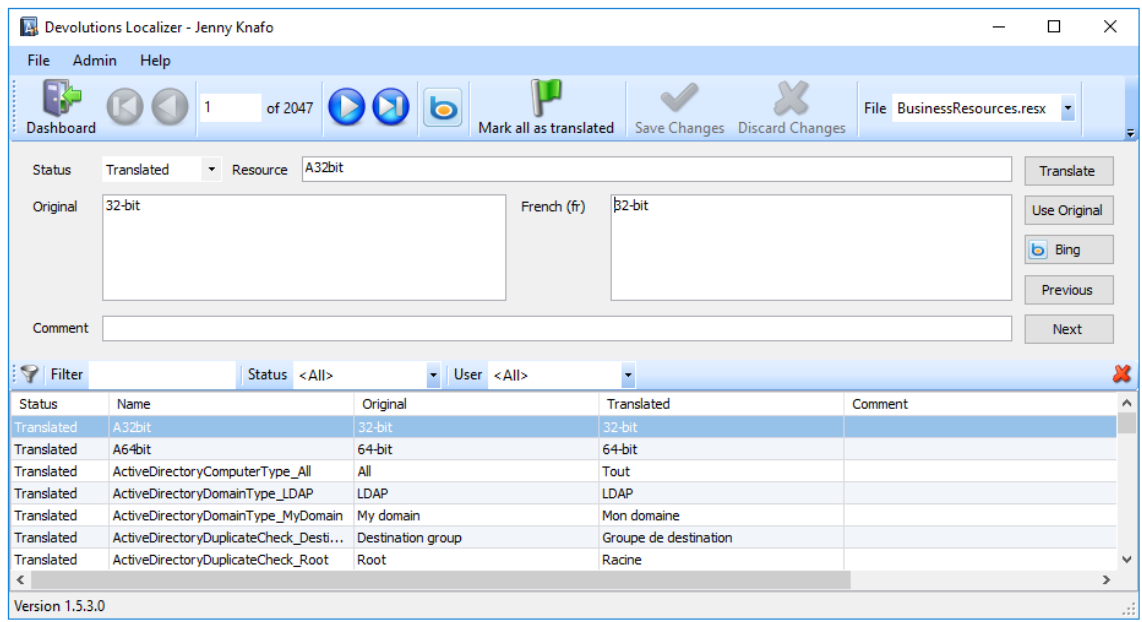
The **Devolutions Localizer** requires an account that you can create [here](#). Enter the requested information, submit the form and you will receive a confirmation email within 24 hours.

It is a click once application that will be installed within your application data folder and will automatically verify for any updates. It is used to manipulate the cloud based translation repository.



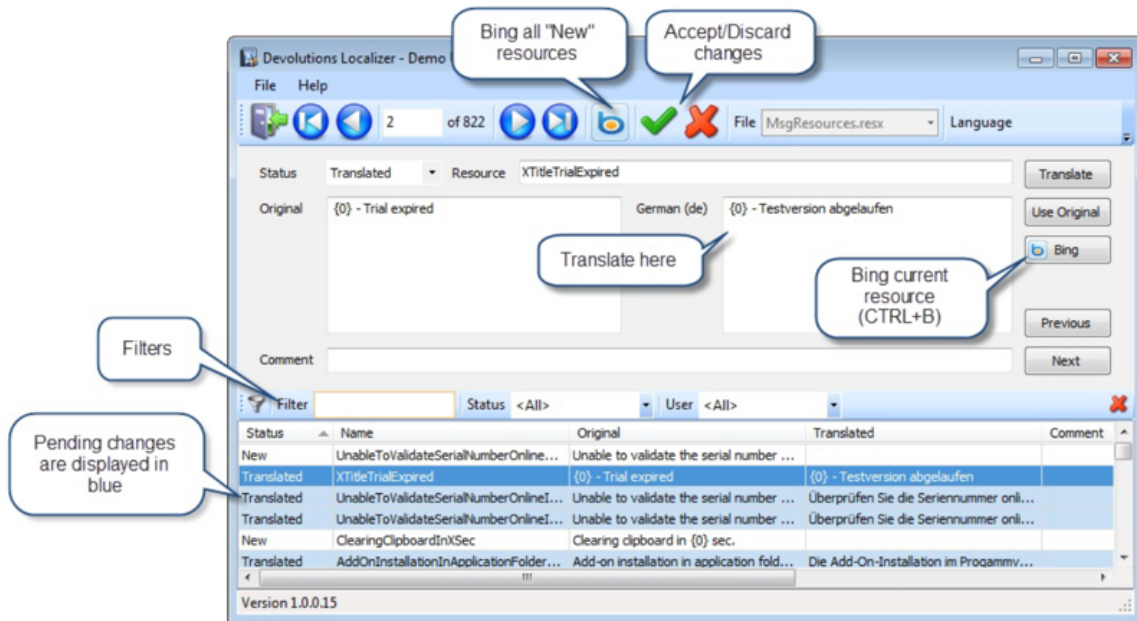
Workflow

From the dashboard view you get a quick progress overview for each Resource file used by the application, simply choose the file you plan to work on and click the **Translate** button. You'll be presented with the following screen.



Localizer translation form

Here is a visual overview of the main features.

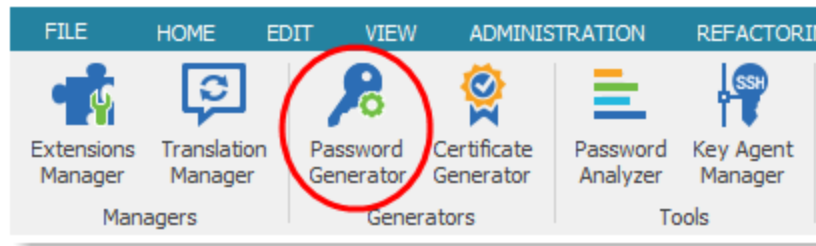


Localizer main features

3.7.3 Password Generator

Description

The **Password Generator** is available in the **Tools - Password Generator** menu. It enables you to create random passwords that are secure and difficult to interpret or predict, due to a mix of uppercase and lowercase letters, numbers and punctuation symbols.



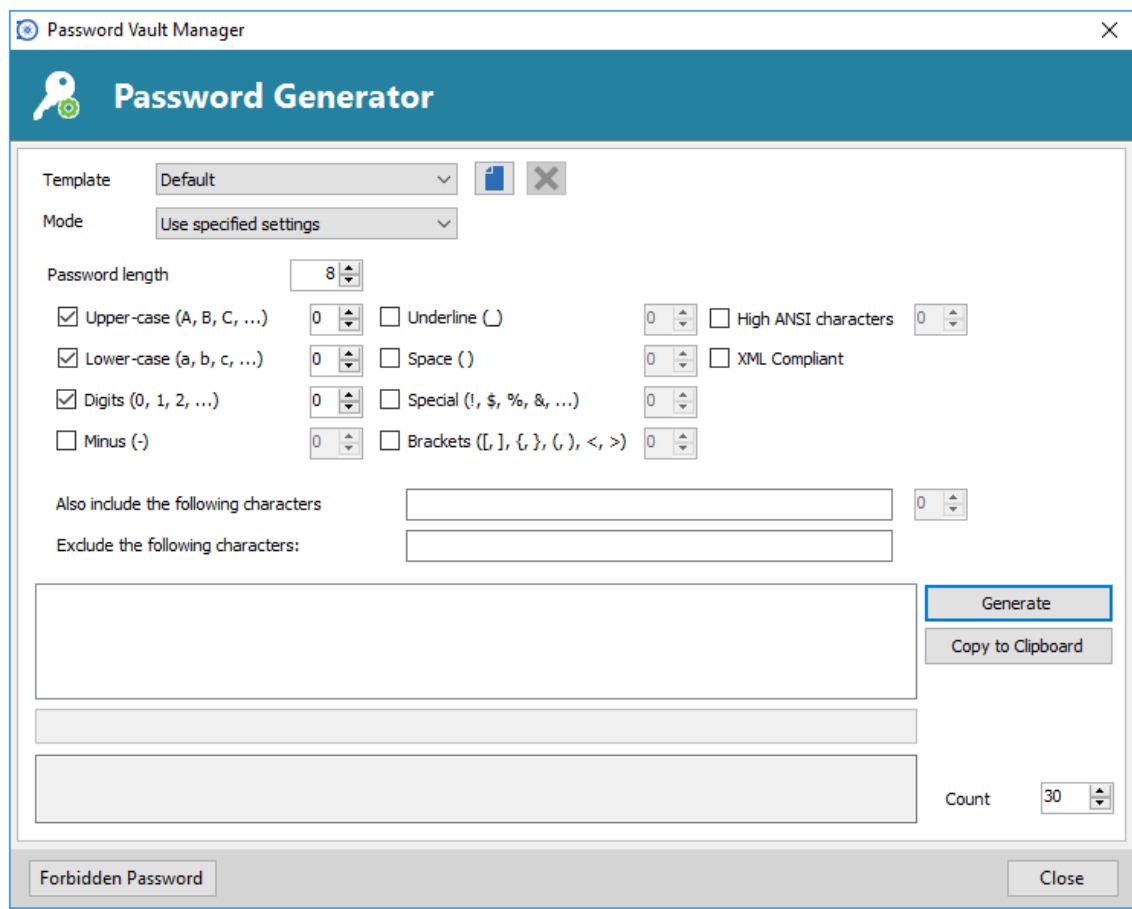
Password Generator

You can also create password generator templates to generate password more rapidly. After you have selected your mode and settings, you can then create your template.

Settings

Use the specified settings

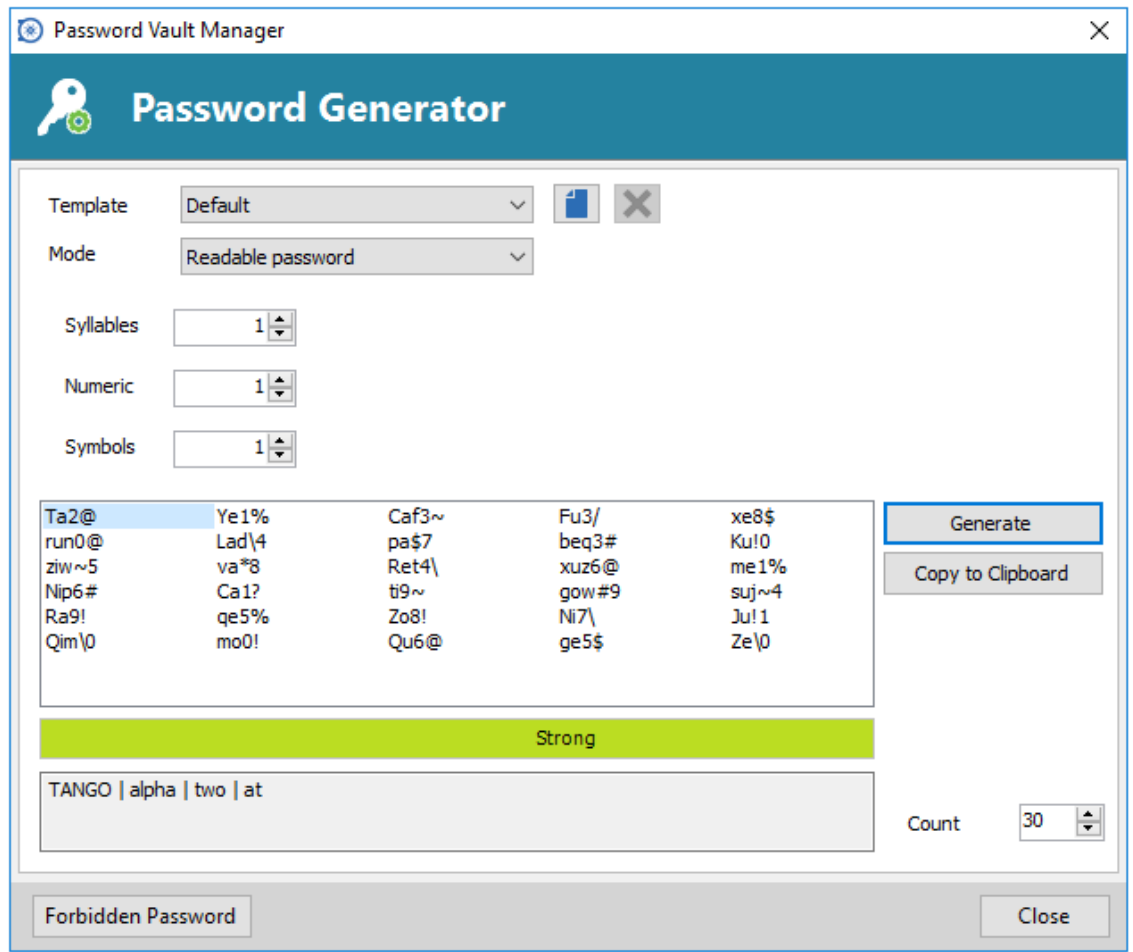
Choose all the character types you wish to use and generate your passwords.



Password Generator - Use specified settings


Readable Password

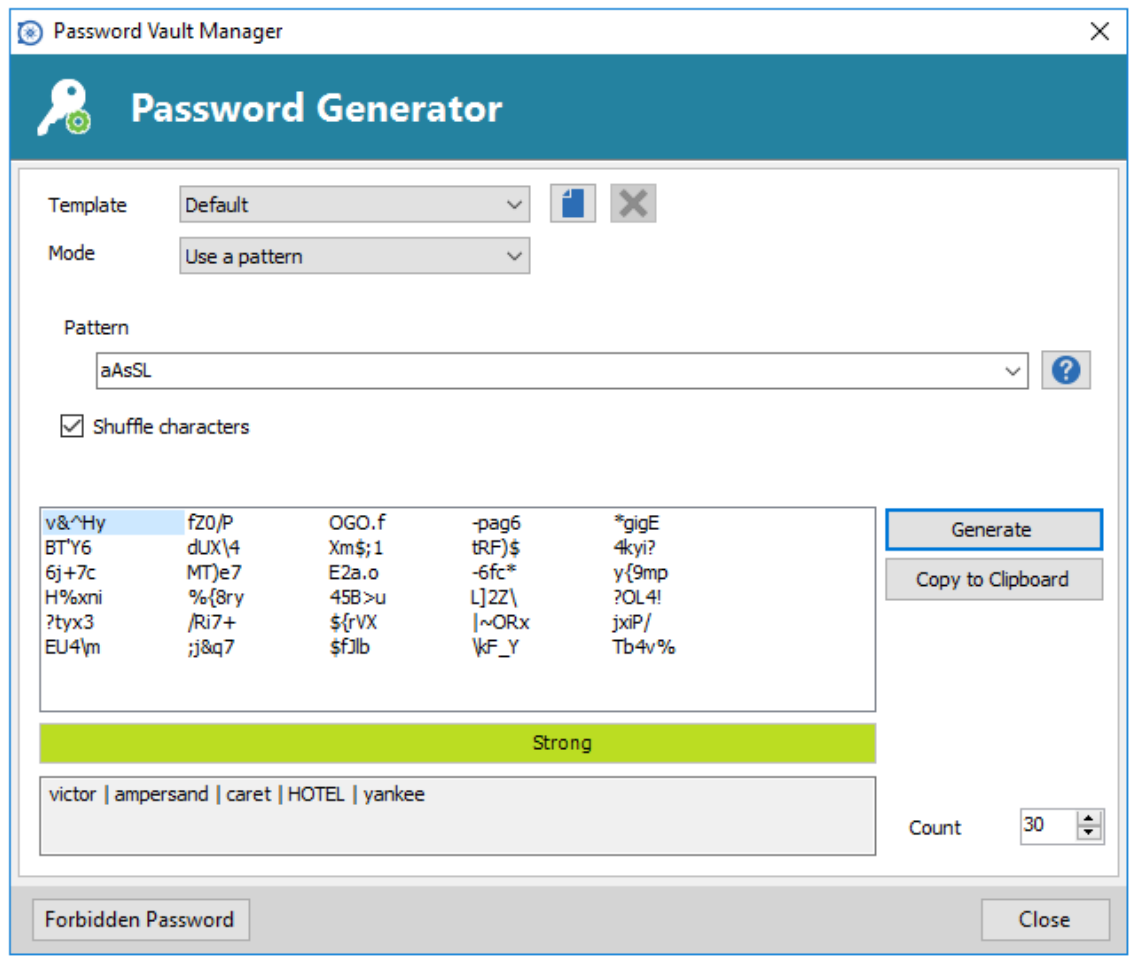
Each generated password will be readable but will not be a word in the dictionary.



Password Generator - Readable password

Use a pattern

Press the  button and select any pattern you need to create your passwords. A list of the most recent used pattern will also be created.



Password Generator - Use a pattern

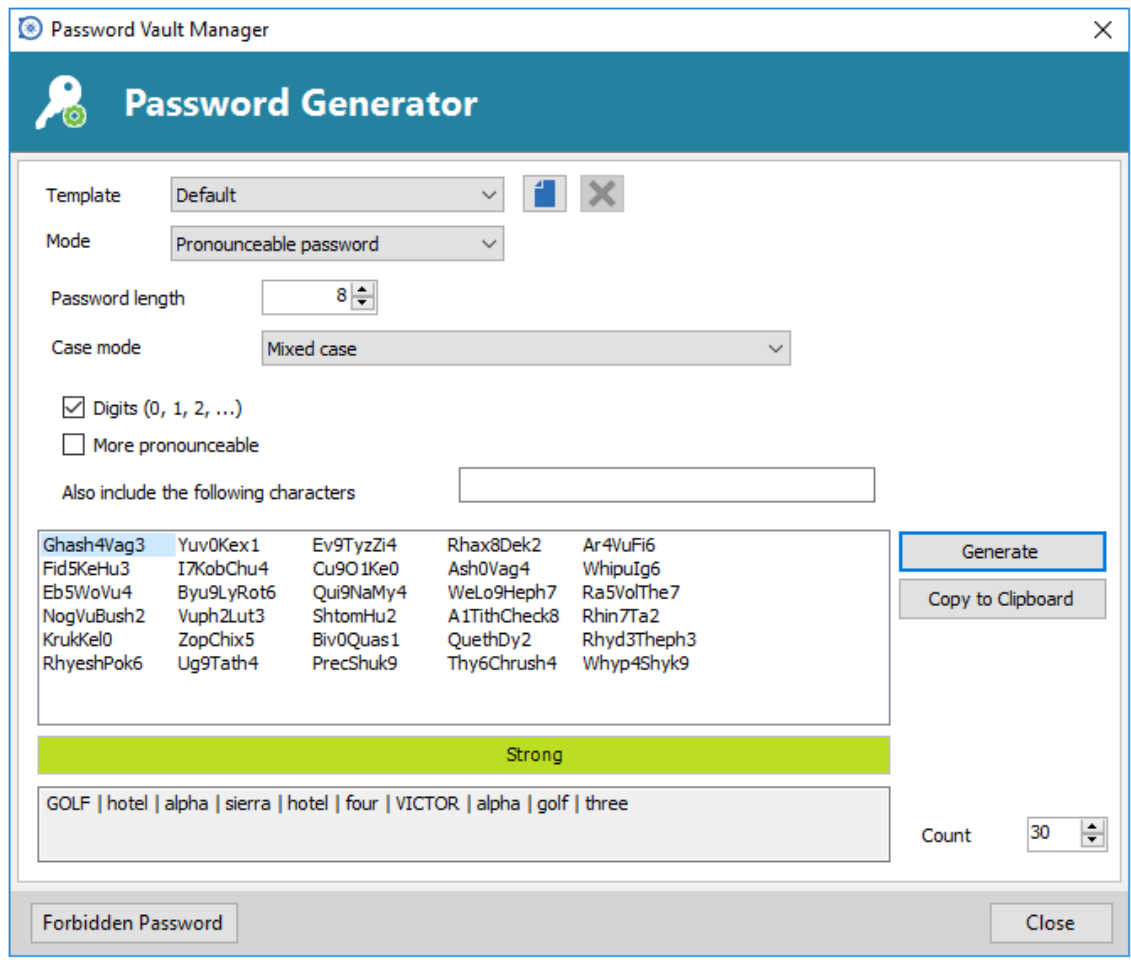
The following are the supported patterns:

Key	Description	Sample
a	Lower-Case Alphanumeric	abcdefghijklmnopqrstuvwxyz 0123456789
A	Mixed-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
b	Bracket	()[]{}<>
c	Lower-Case Consonant	bcdfghjklmnpqrstvwxyz
C	Mixed-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz
d	Digit	123456789
h	Lower-Case Hex Character	0123456789 abcdef
H	Upper-Case Hex Character	0123456789 ABCDEF
l	Lower-Case Letter	abcdefghijklmnopqrstuvwxyz
L	Mixed-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz

p	Punctuation	,.:;
s	Printable 7-Bit Special Character	!"#\$%&'()*+,-./:;<=>?[\]^_`{ }~
S	Printable 7-Bit ASCII	A-Z, a-z, 0-9, !"#%&'()*+,-./:;<=>?[\]^_`{ }~
u	Upper-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ
U	Upper-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
v	Lower-Case Vowel	aeiou
V	Mixed-Case Vowel	AEIOU aeiou
x	High ANSI	From '~' to U255 (excluding U255)
z	Upper-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ
Z	Upper-Case Vowel	AEIOU
\	Escape (Fixed Char)	Use following character as is
{n}	Escape (Repeat)	Repeats the previous character <i>n</i> times
[x]	Custom character	Define a custom character sequence

Pronounceable password

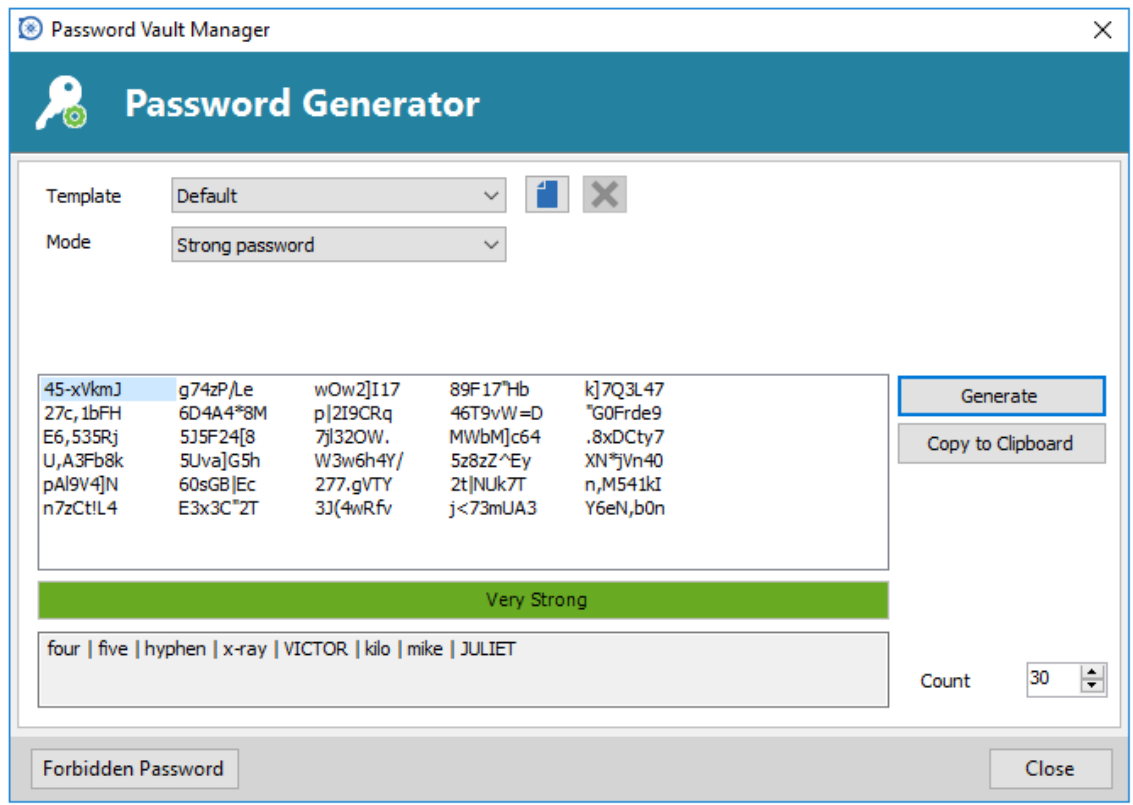
The application will generate a password that is pronounceable.



Password Generator - Pronounceable password

Strong password

Password Vault Manager generates an 8 characters password with mixed alphanumeric cases and special characters.

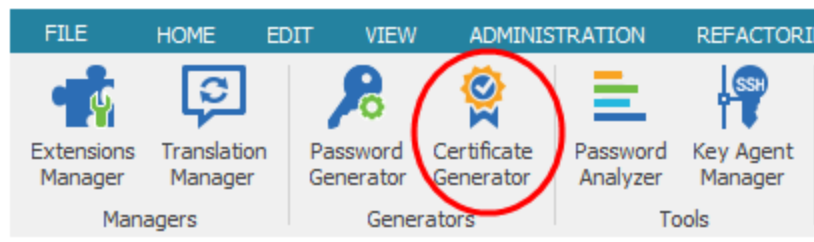


Password Generator - Strong password

3.7.4 Certificate Generator

Description

The **Certificate Generator** is available in the **Tools - Certificate Generator** menu. It allows you to create a self signed certificate which is an identity certificate that is signed by the same entity whose identity is certified.



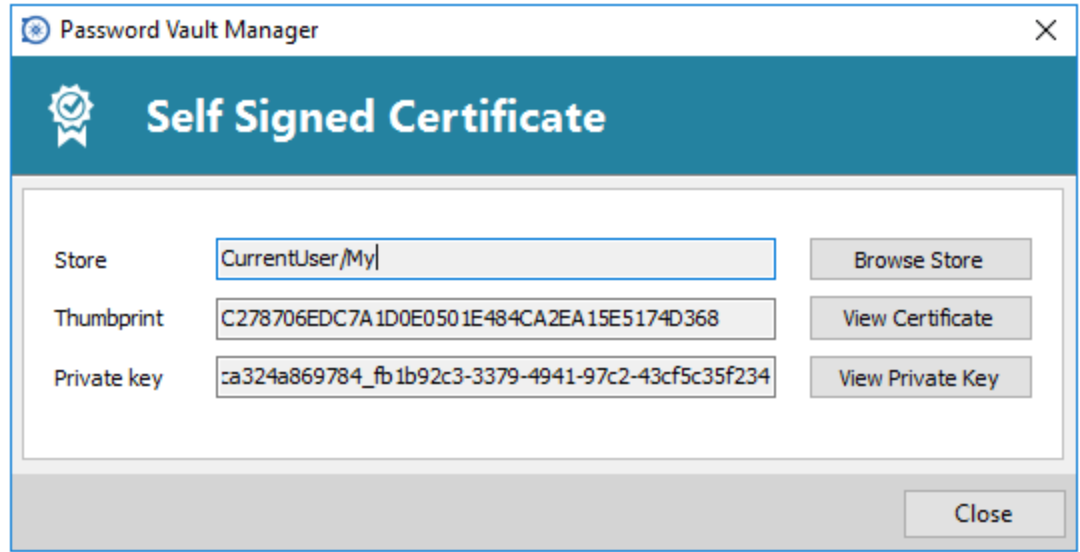
Tools - Certificate Generator

Settings

Self Signed Certificate

Option	Description
Common name	Name of the certificate.
Key size (bits)	Indicates the key size (bits) of the certificate. Select between: <ul style="list-style-type: none"> • 384 • 512 • 1024 • 2048 • 4096 • 8192 • 16384
Valid from	Start date of the certificate
Valid to	End date of the certificate
Save to file (pfx)	Save the certificate into a pfx file and secure this certificate with password.
Save to certificate store	Indicate the location and the store to save the certificate.
Location	Indicate the location of the certificate. Select between: <ul style="list-style-type: none"> • Current user • Local machine
Store	Indicate the store location of the certificate. Select between: <ul style="list-style-type: none"> • Address book • Authorization root

- **Certificate authority**
- **Disallowed**
- **My**
- **Root**
- **Trusted people**
- **Trusted publisher**



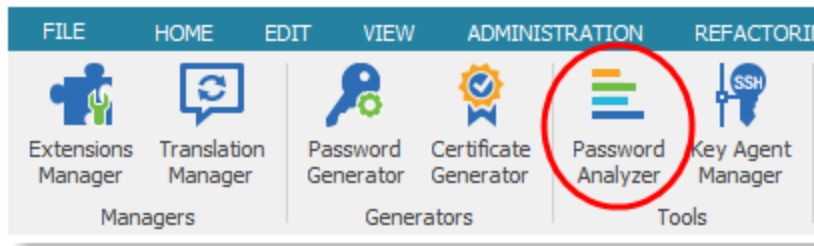
Self Signed Certificate

Option	Description
Store	Indicate the store where the certificate will be located.
Browse Store	Browse the store that is indicated in the store field.
Thumbprint	Display the certificate thumbprint.
View Certificate	Display the certificate that you have created.
Private key	Display the certificate private key.
View Private key	View the private key file on your computer.

3.7.5 Password Analyzer

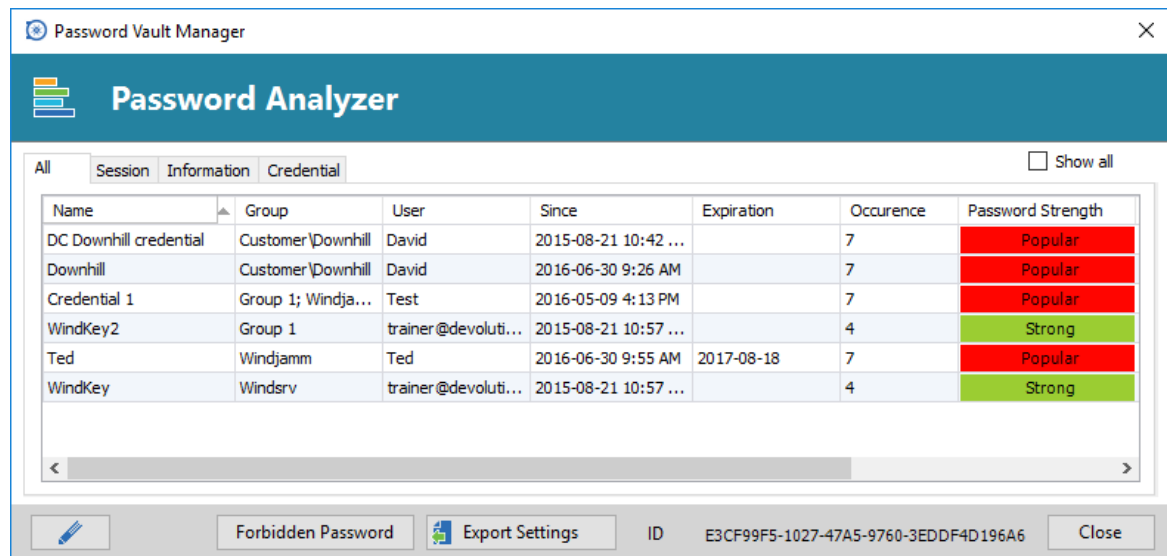
Description

The **Password Analyzer** is available in **Tools - Password Analyzer**. It will display a strength indicator for all passwords stored in your data source.



Tools - Password Analyzer

Settings



Password Analyzer

The dialog displays four tabs :

- All
- Session
- Information
- Credential

In a single glance you can see the strength ratings of your stored passwords.

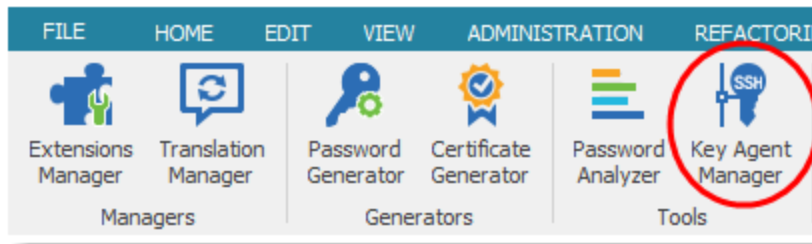
3.7.6 Key Agent Manager

Description

The **Key Agent Manager** is used to hold all your SSH Keys in memory, already decoded and ready for them to be used. It has the same use as Pageant (SSH Key Manager) has for Putty except that the Key Agent Manager is used with Password Vault Manager.

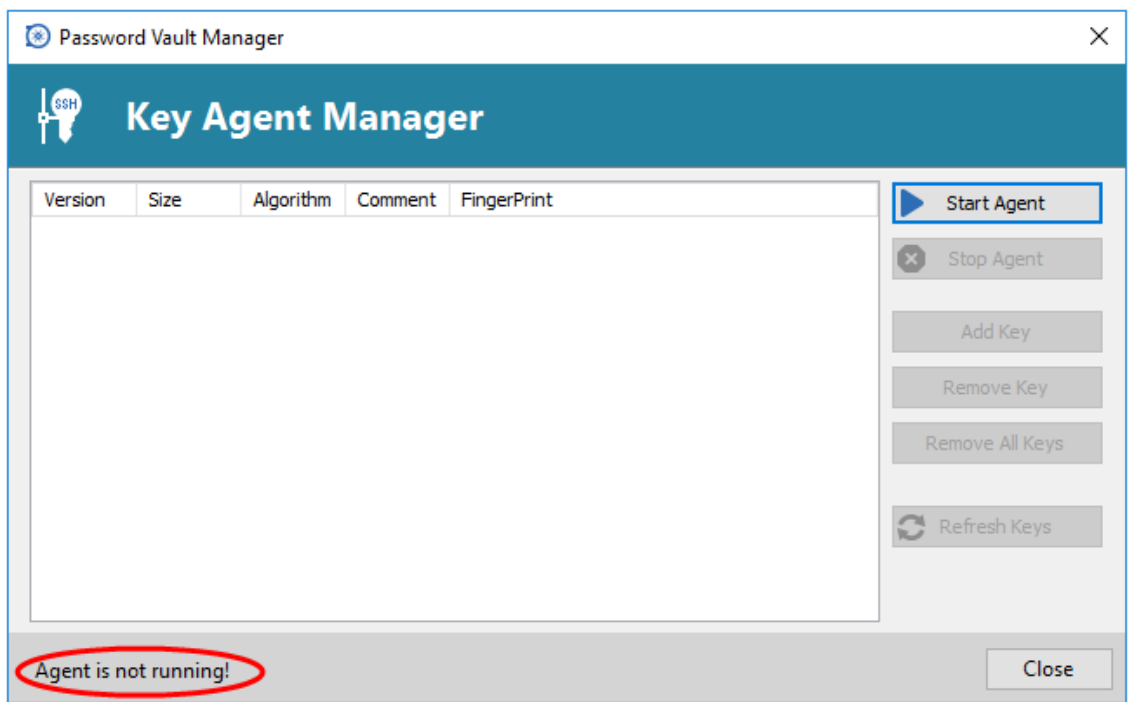
Settings

1. In **Tools** select the option **Key Agent Manager**



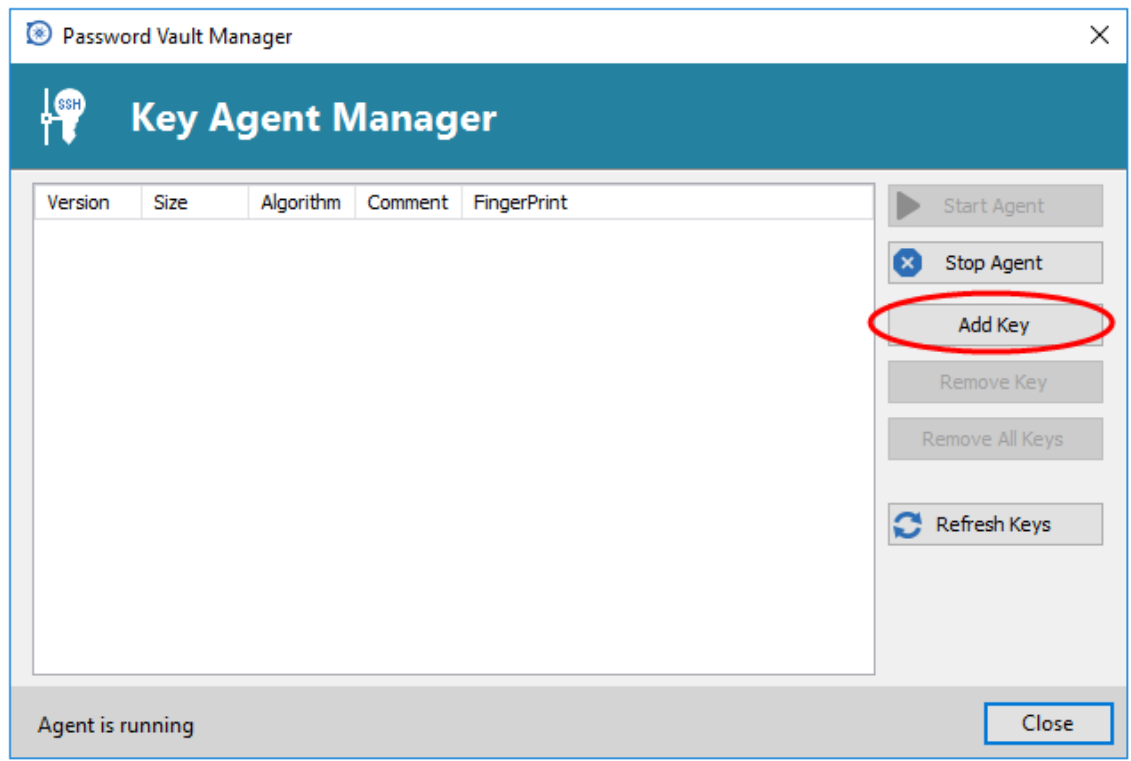
Key Agent Manager

2. When opening the **Key Agent Manager** you will notice at the bottom right that the **agent is not running** you will need to click on **Start Agent**. If you wish to always have your Key Agent running you can activate the option in **File - Option - Key Agent - Start agent on application start**.



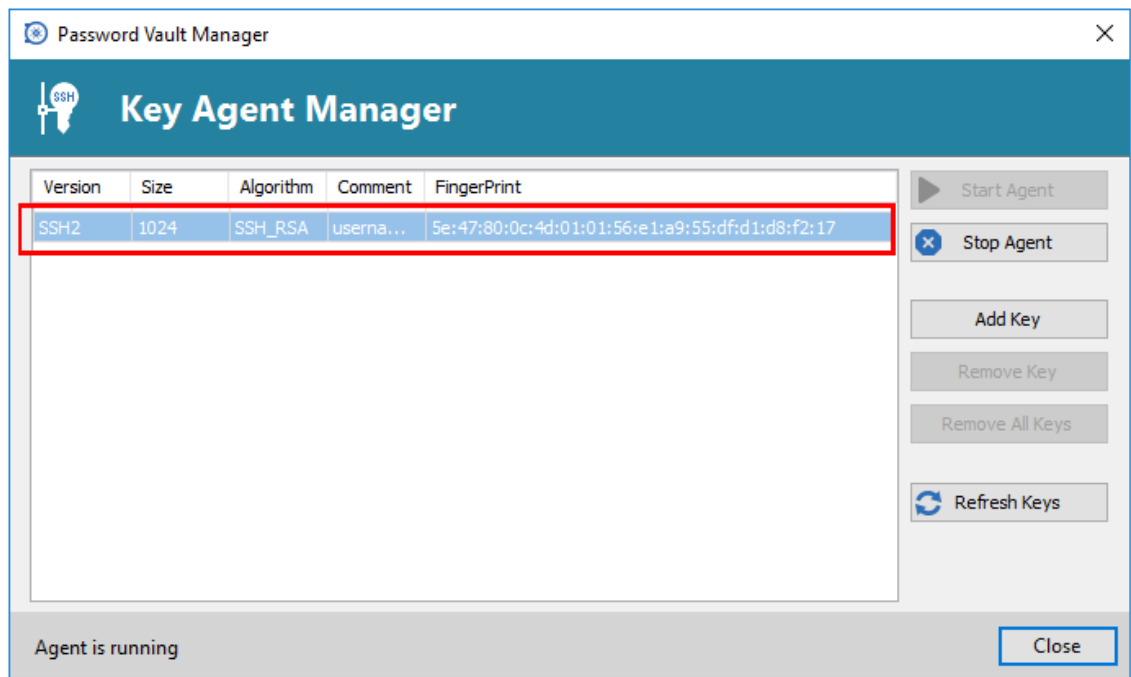
Key Agent Manager - Start Agent

3. Click on **Add key** and select the file to open your SSH key.



Key Agent Manager - Add Key

4. All your added SSH Key will appear in your *Key Agent Manager*.

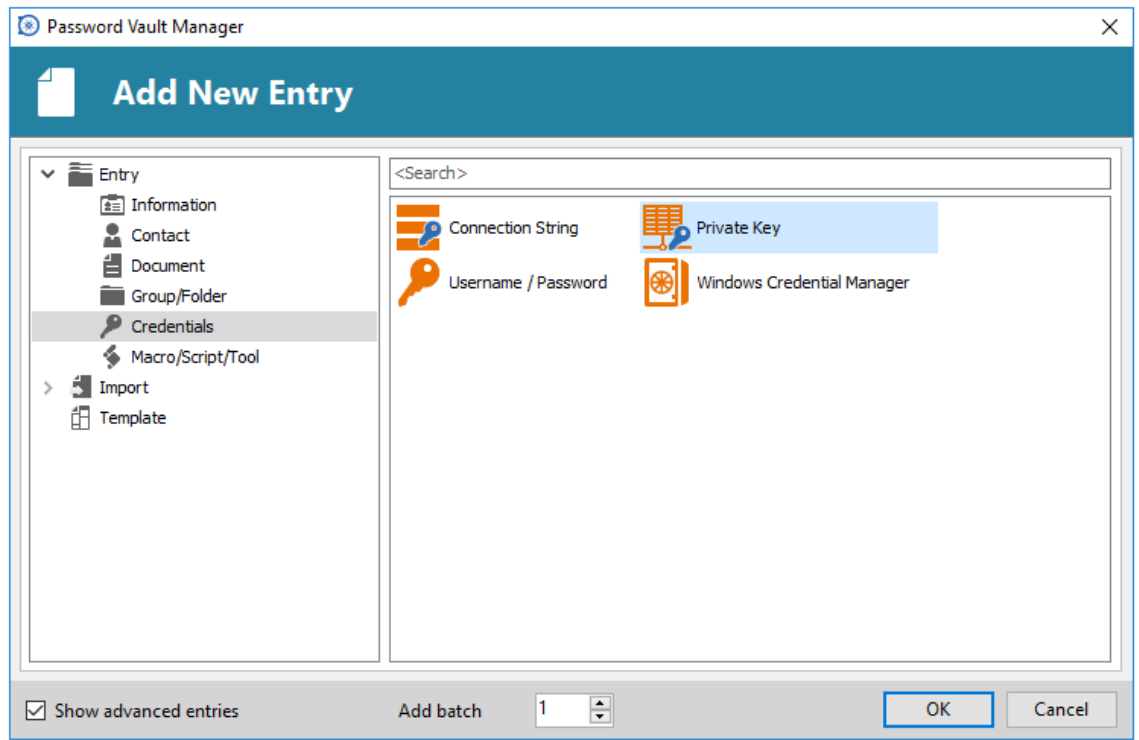


Key Agent Manager

Private Key Credential

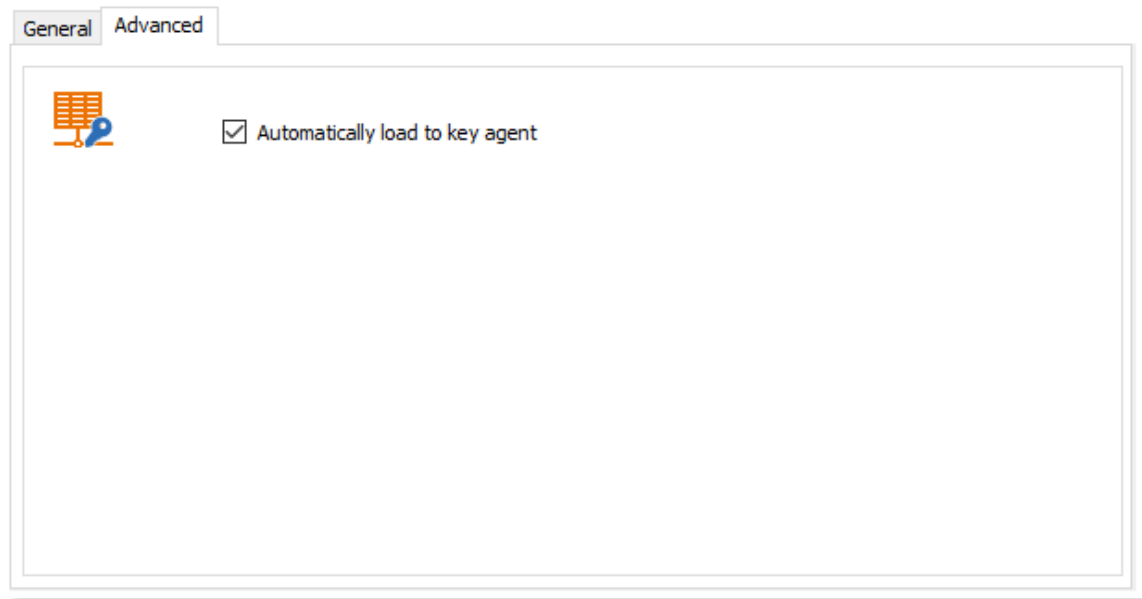
When creating new Private Key credential entry in Password Vault Manager you have the option of loading them automatically in your Key Agent Manager.

1. Create your new Private Key credential.



New Entry - Private Key

2. In the **Advanced** tab of your Private Key entry activate the option **Automatically load to key agent**.

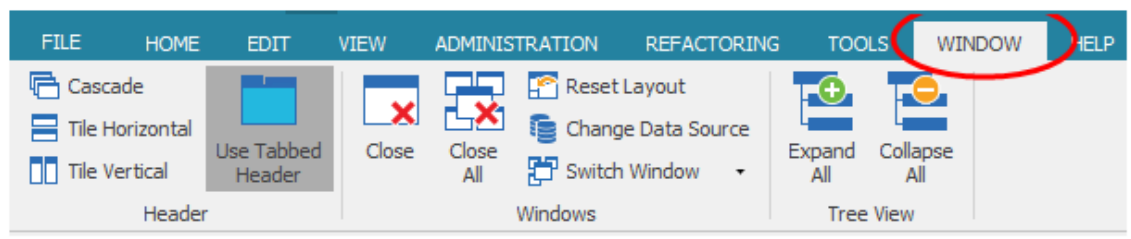


Private Key - Advanced tab

3.8 Window

Description

The **Window** ribbon manages the different windows layout in Password Vault Manager.



Window

Settings

Header

The **Header** section allows you to display your windows in different mode.

Option	Description
Cascade	Display the sessions in cascade mode.
Tile Horizontal	All sessions will be displayed one under an other.
Tile Vertical	All sessions will be displayed side by side.
Use Tabbed Header	Sessions are displayed in separate tabs instead of MDI windows.

Windows

The **Windows** section allows you to close your sessions, switch between them or **reset the application layout**.

Option	Description
Close	Close the active session tab.
Close All	Close all the opened session tabs.
Reset Layout	If getting lost with the View use the Reset Layout to reset it to its original layout. For more information see Reset Layout .
Change Data Source	Switch to another one of your data source.
Switch Window	Used to easily switch between the different opened sessions when you have multiple connections opened. All the tabs page, including the dashboard, will be listed in the drop down menu.

Tree View

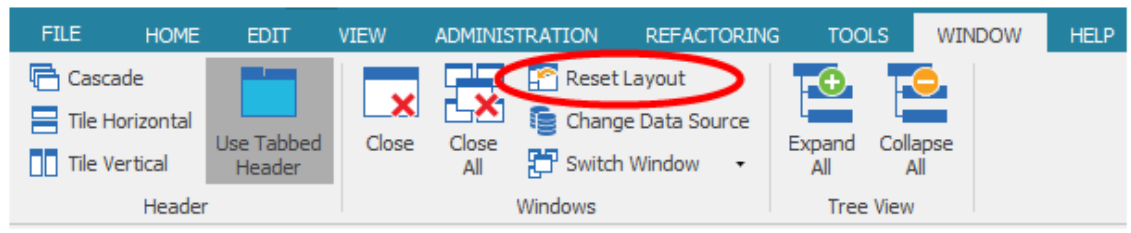
The Tree View section allows you to expand or collapse your entry groups in the navigation panel.

Option	Description
Expand All	Expand all the groups in the Navigation pane when the Tree view mode is used.
Collapse All	Collapse all the groups in the Navigation pane when the Tree view mode is used.

3.8.1 Reset Layout

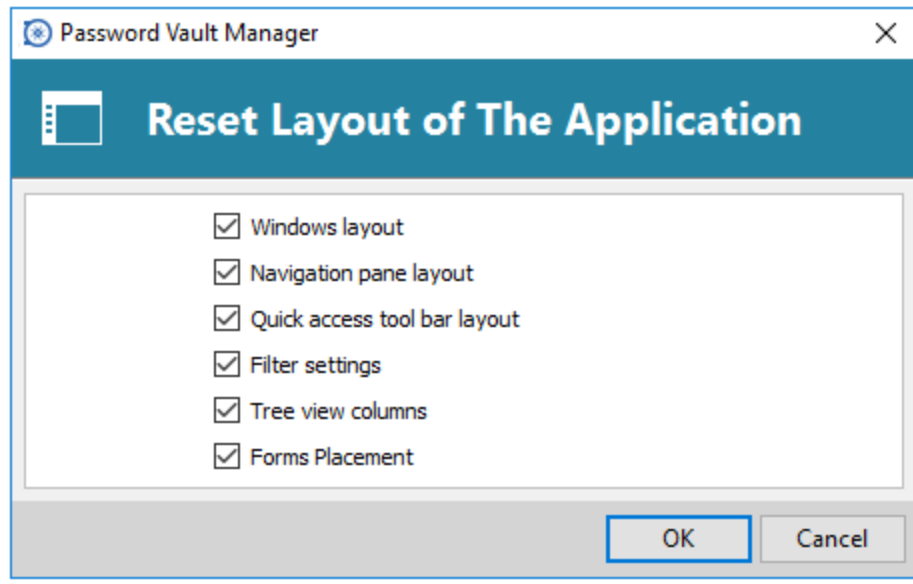
Description

Use the **Reset Layout** option to revert back to the default User Interface layout of Password Vault Manager.



Windows - Reset Layout

Settings



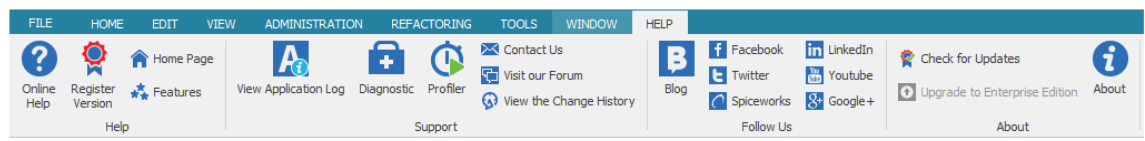
Reset Layout of the Application

Option	Description
Windows layout	Reset the windows layout to it's original state.
Navigation pane layout	Reset the Navigation pane layout and automatically switch to the tree view mode.
Quick access tool bar layout	Reset the Quick access tool bar buttons.
Filter settings	Reset the filter/search field.
Tree view columns	Remove all columns in the Navigation Pane except the name column.
Forms Placement	Reset the forms placement to its original state.

3.9 Help

Description

The **Help** tab contain links to our Devolutions web site and Online Help. It also includes all the links to follow us on different social media platform. Our Support team might also ask you to perform some operations that you will find in the Help ribbon.



Help

Refer to the following topics for more information:

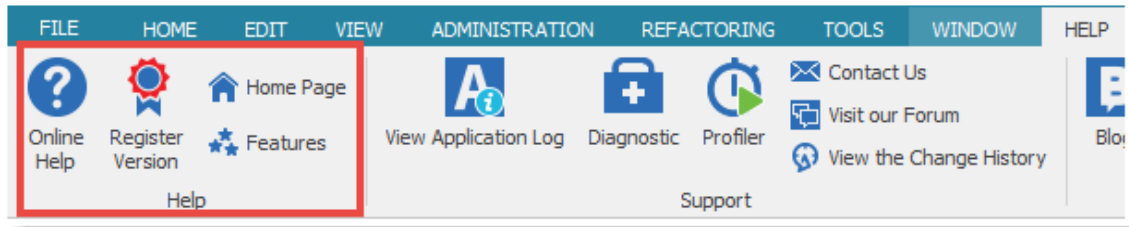
- [Help](#)
- [Support](#)
- [Follow Us](#)

- [About](#)

3.9.1 Help

Description

The **Help** section contains quick links to our different web sites and also contains the option to **Register your Password Vault Manager** trial or Enterprise Edition license.



Help

Settings

Online Help

Online Help is a direct link to our Windows Password Vault Manager [Online Help](#).

Register Version

Enter your Trial or Enterprise license to register your Password Vault Manager version. For more information about registering your version please see [Register Enterprise Edition](#), or [Register Free Edition](#).

Application

Enterprise Edition trial
Serial [Request trial](#)

Enterprise Edition
Name
Email
Serial

I would like to receive product updates, news, tips & tricks and special offers through the Devolutions newsletter.

Free upgrade until: Thursday, March 1, 2018

Select your Application Edition

Home Page

The Home Page is a direct link to our Devolutions web site [home page](#).

Features

Features is a direct link to our Password Vault Manager web page to view [features and highlights](#) for our products.

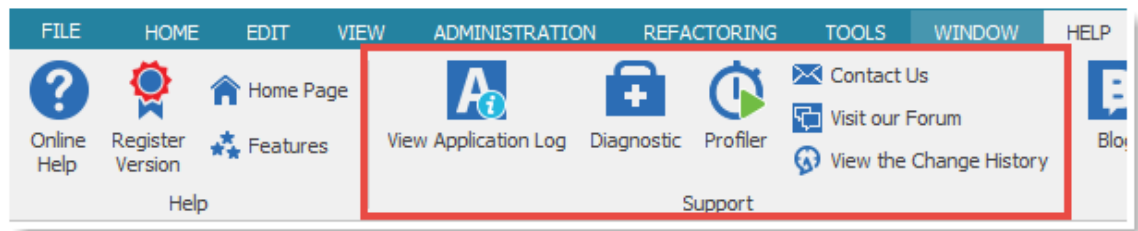
What's New

What's New is a direct link to our Password Vault Manager web page to view the [new features and enhancements](#) when a new version is release.

3.9.2 Support

Description

When experiencing issues with Password Vault Manager one of our Support team member might ask you to perform some action to help them resolve your issue.



Help - Support

Settings

Refer to the following topics for more information on:

- View Application Log
- Diagnostic
- Profiler

Contact Us

Contact Us will automatically open an email with our Support Devolutions email address ready to be sent to us.

Visit our Forum

Visit our Forum is a direct link to our [Forum](#).

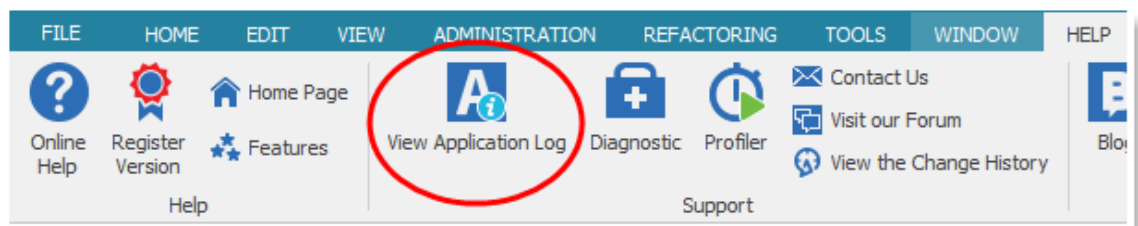
View the Change History

View the Change History shows you a detail list of every change history between your Password Vault Manager version and the latest available version of Password Vault Manager.

3.9.2.1 View Application Log

Description

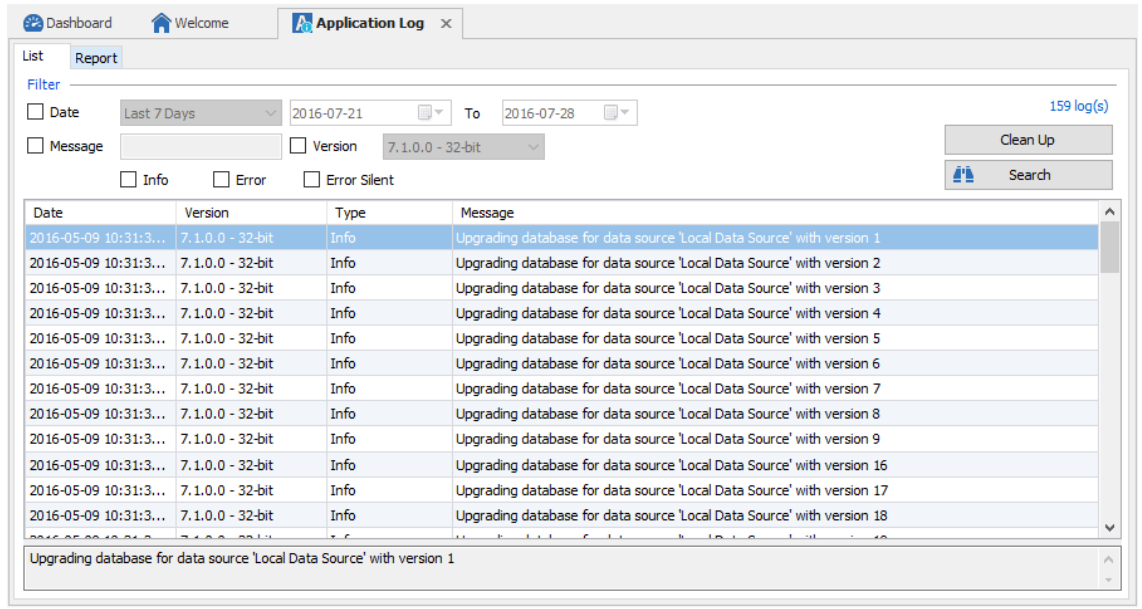
In case an error occurs, you can verify the local application log, which is available from the menu **Help - View Application Log**.



Help - View Application Log

Those logs are saved in `%LocalAppData%\Devolutions\PasswordVaultManager\PasswordVaultManager.cfg`. You could view it as a list which could then be filter by Date, Message, Version, Info, Error or Error Silent.

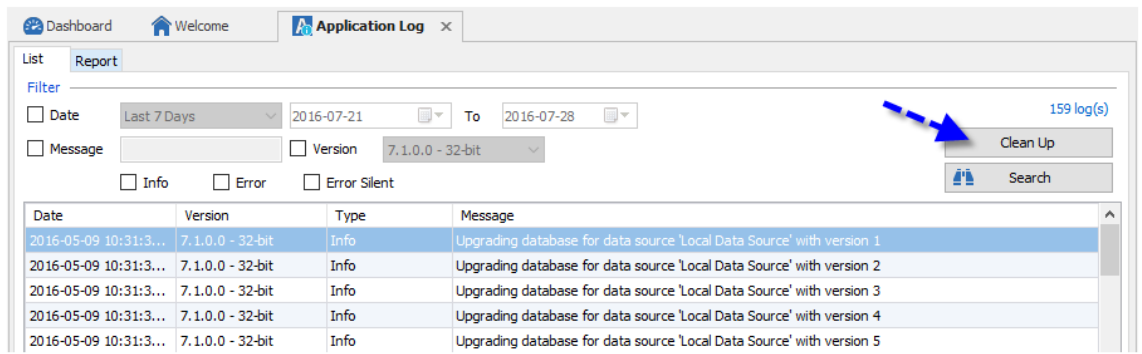
You could also generate a Report with the log which could be saved afterward.



View Application Log

Clean up

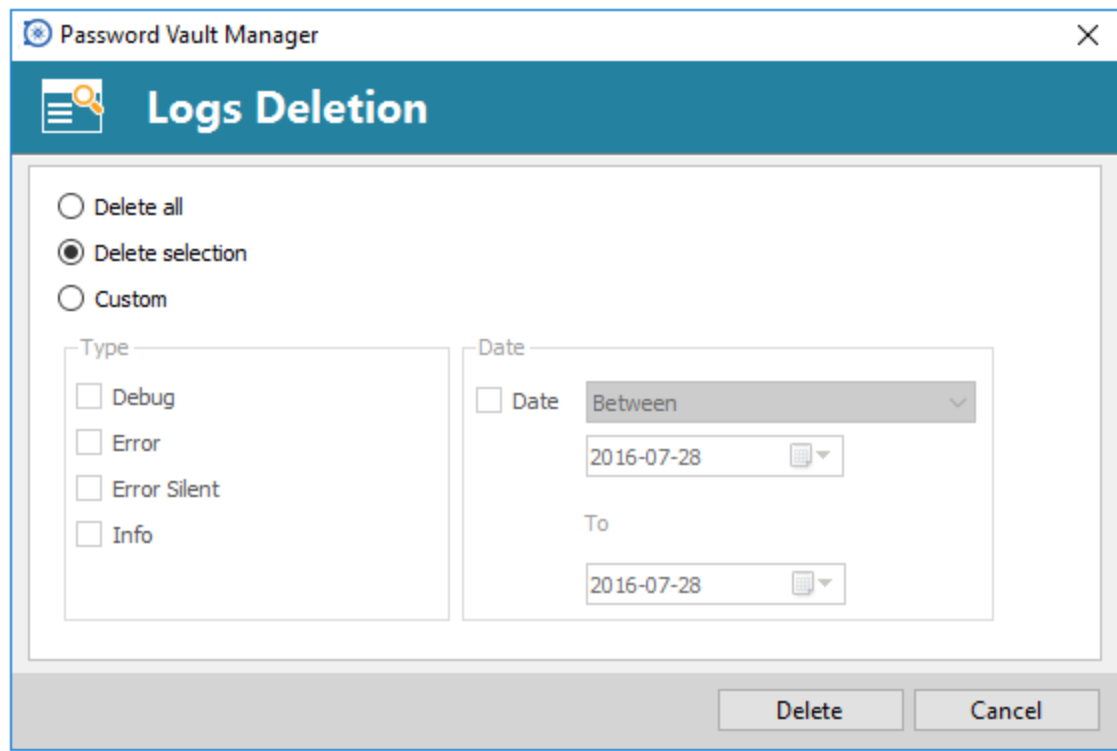
As a best practice we suggest cleaning up your local Application log once every month for security reason. To do so, in your Application Log select the option **Clean Up**.



Application Log - Clean Up

You can select to delete all your Log, or decide precisely what you wish to delete, from the exact date to a precise type.

We strongly suggest to do a **Delete all**.

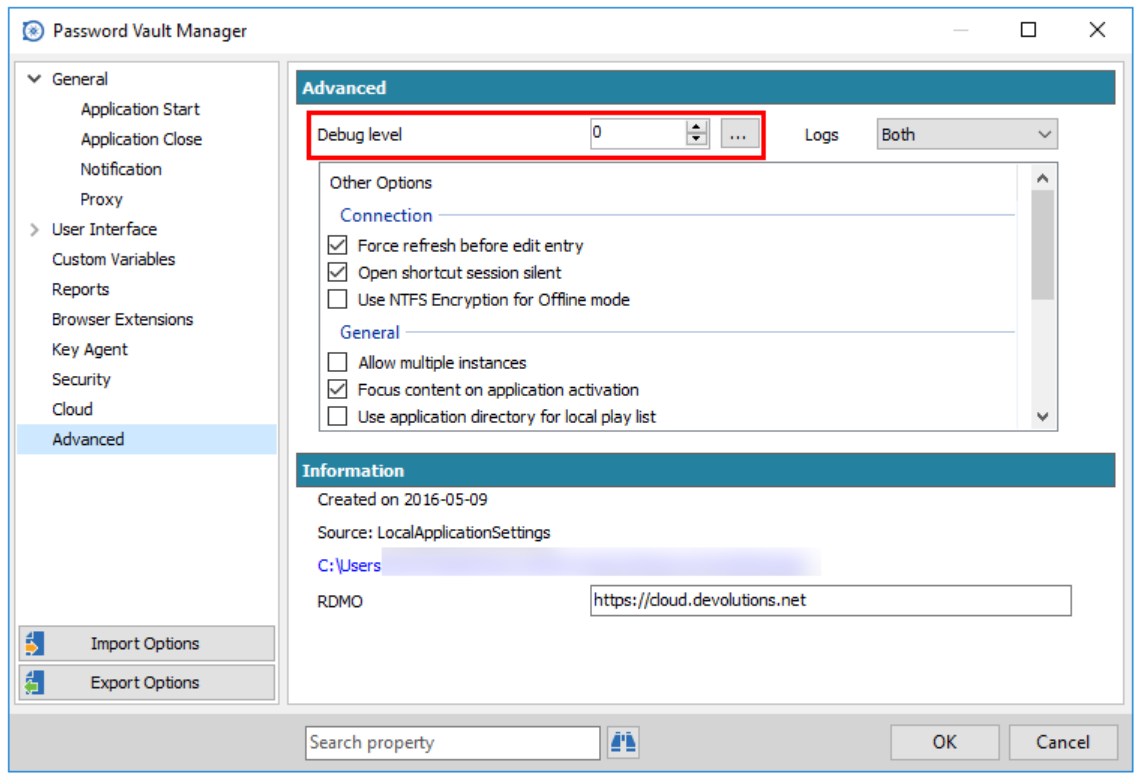


Logs Deletion

Increasing the Debug level

When experiencing issues with Password Vault Manager our Devolutions support team might ask you to increase the debug level of the application to a higher level during a support process. We strongly suggest to only increase the debug level when requested by our Support team.

You can increase the Debug level in ***File - Options - Advanced***.

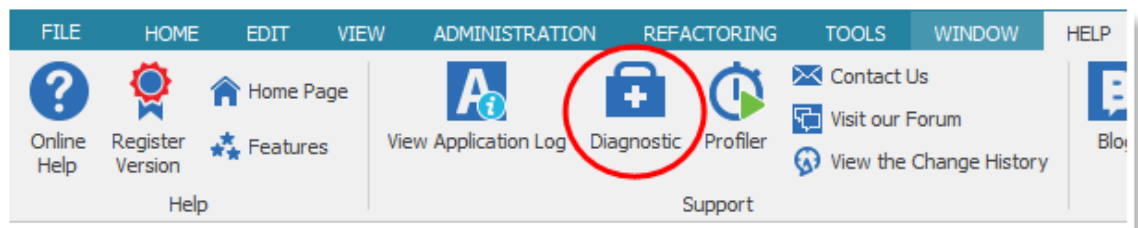


Options - Advanced - Debut level

3.9.2.2 Diagnostic

Description

If you encounter an issue with Password Vault Manager you can run a system diagnostic, which is available in **Help - Diagnostic**. This could help diagnose or give a pointer to what kind of issues you might be experiencing.



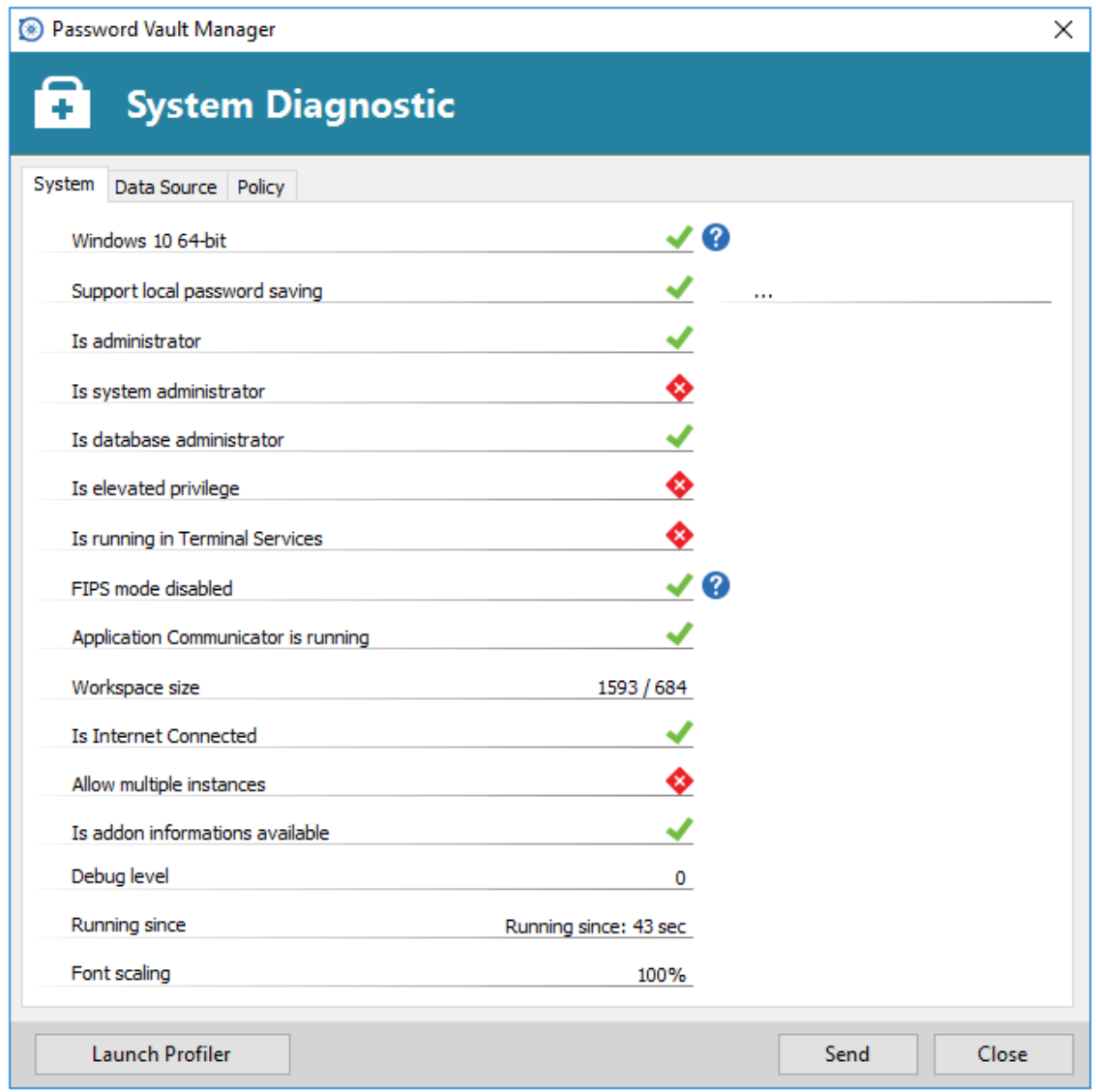
Help - Diagnostic

Settings

System

The administrator item could be the possible cause of a security problem. This happens often when a user has the SYSDBA or is DB_OWNER of the SQL Server database.


Some other issues could be related to the application running in Terminal Services. However Password Vault Manager is fully compatible with Terminal Services.



System Diagnostic

The administrator item could be the possible source for security problem. This happen often when a user has the SYSDBA or is DB_OWNER of the SQL Server database.

Some other issues could be related to the fact that the application is running in Terminal Services. However Password Vault Manager is fully compatible with Terminal Services.



Please read the [Troubleshooting](#) topic, it lists error messages and could contain the fix/workaround for your problem.

3.9.2.3 Profiler

Description



Displaying the Profiler window might slow down the operations on the data source. Proceed with care.

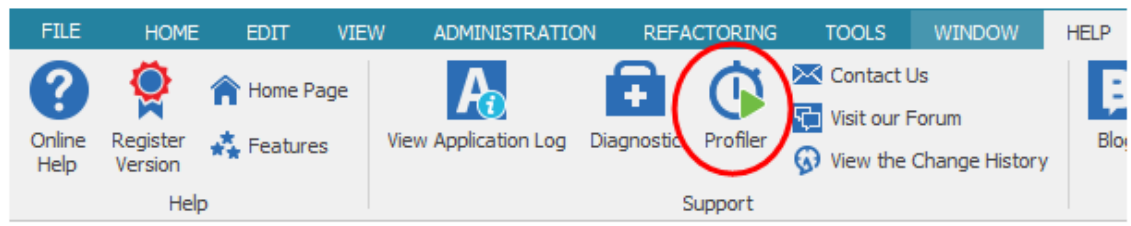


To diagnose startup issues, you can enable the profiler from the command line as described in [Command Line Arguments](#)

Procedure

Performance

1. Select **Help - Profiler**.

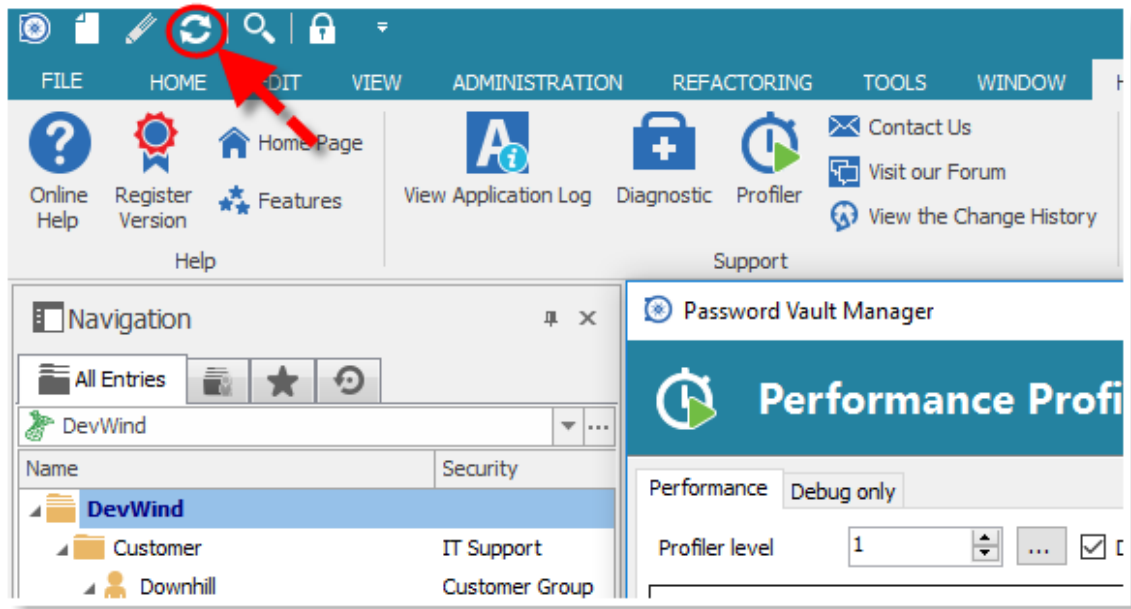


Help - Profiler

2. Move the window to the side in order to display the Password Vault Manager main window and refresh the data source by using the refresh button or by using **File - Refresh**.

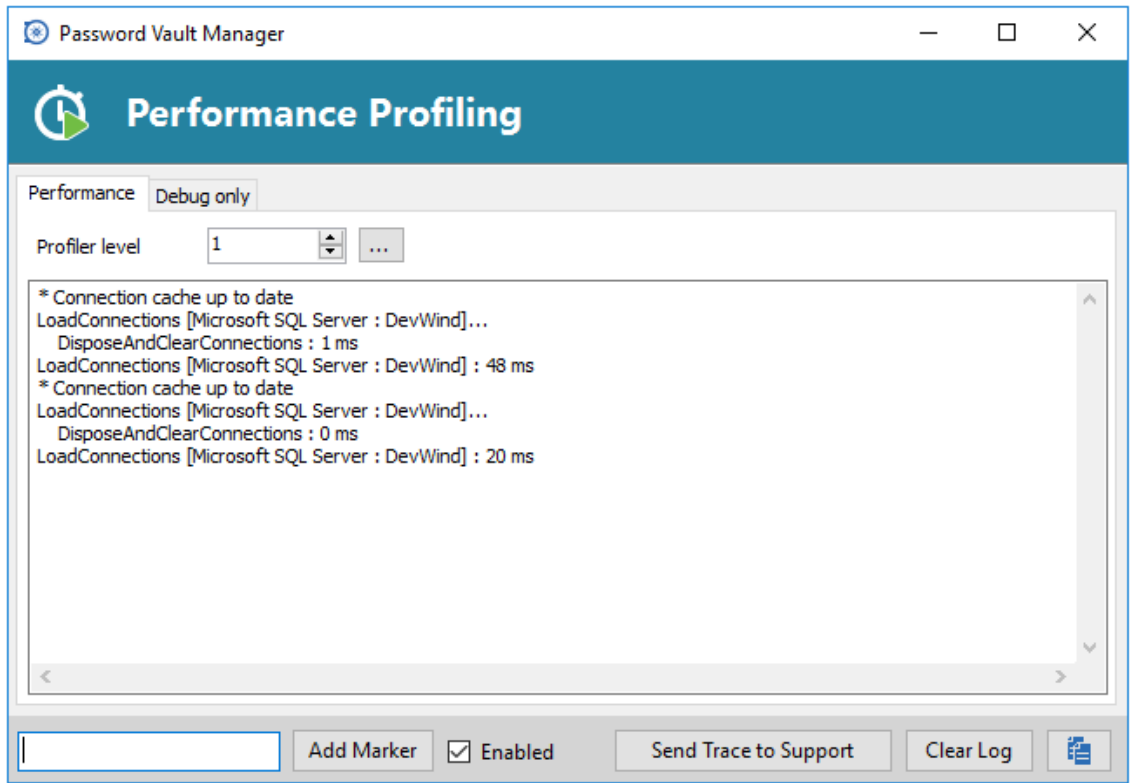


Holding the **CTRL** key while performing the refresh will force a full reload of the data source, thereby ignoring the cache.



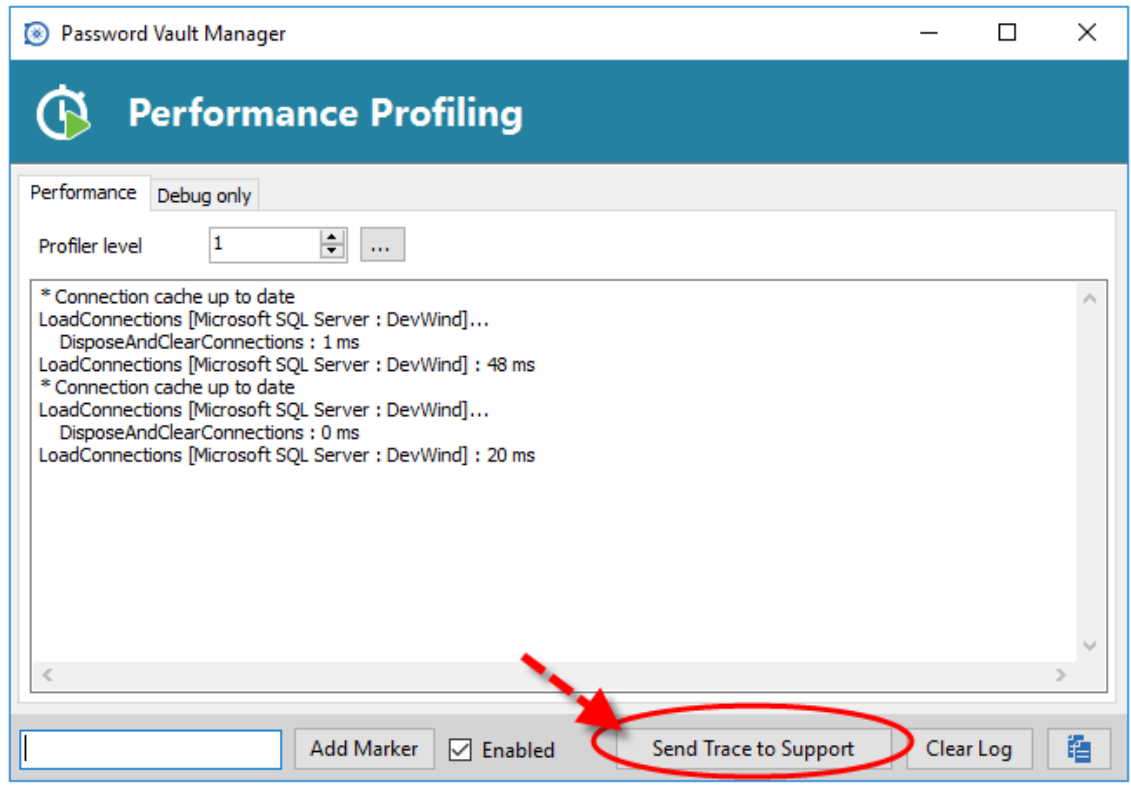
Refresh

3. The Profiler data will appear in the **Performance Profiler** window.



Performance Profiling

4. Click on **Send Trace to Support** in order to send the Profiler data logs to our Devolutions support team. You can add a Marker when running multiple tests to separate them.



Send Trace to Support

Debug only

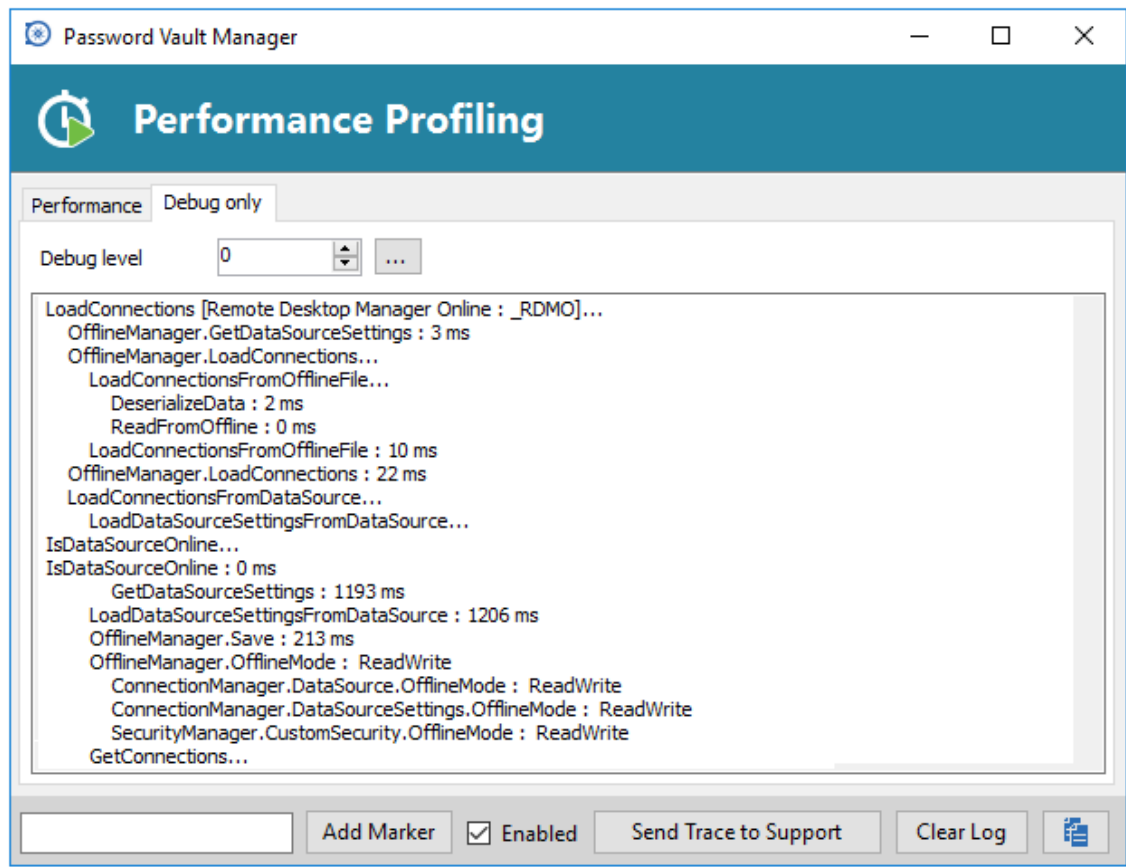
Sometimes when an issue occurs while using Password Vault Manager, the support personnel may ask you to turn on debugging and send the information back. Here are two procedures that you can follow.



Any debug level other than zero will slow down the application and write a lot of information in the application logs. As soon as you have completed the diagnostics you should revert back the debug level to zero.

Use the in-depth debugging method whenever you need to diagnose the startup or initial connection. the Ad-hoc debugging method is much easier to follow and is sufficient in most cases.

Ad-hoc debugging



Performance Profiling - Debug only tab

1. Open **Help - Profiler**, move the window aside to clear the main window of Password Vault Manager.
2. In the **Debug only** tab, click on the ellipsis button and activate the proper debug categories.
3. In Password Vault Manager, perform the action that is under investigation. You should see debug information appear in the profiler window.
4. Click on **Send trace to support**. In the following dialog, ensure you specify enough information to link the report to the appropriate ticket, if the process was started from the forum include your forum user name.

In-depth debugging

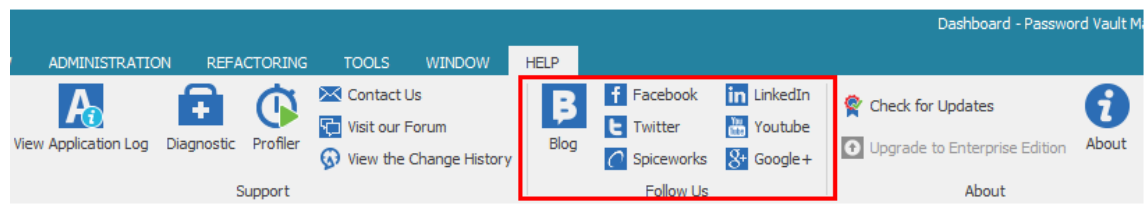
1. Open **File - Options - Advanced**, click on the **Debug level** ellipsis button and activate the proper debug categories.
2. In the Information section below, you will see a hyperlink to your configuration folder, press on it to have an explorer window opened in that folder.
3. Close Password Vault Manager.

4. As a preparatory phase, it would be best to clear existing logs to limit the scope of what will need to be analyzed. Delete or rename files named RemoteDesktopManager.log, %APPNAMECAMELCASE%.log.db and %APPNAMECAMELCASE%.debug from your configuration folder.
5. Start Password Vault Manager.
6. Perform the action that is under investigation.
7. Open **File - Options - Advanced**, set the **Debug level** to zero.
8. Close Password Vault Manager.
9. Package the .log, .log.db and .debug files from your configuration folder and send them to us.

3.9.3 Follow Us

Description

The Follow Us section include links to all of our Social Media Platform.



Help - Follow Us

You can follow us on:

- [Blog](#)
- [Facebook](#)
- [Twitter](#)
- [Spiceworks](#)
- [LinkedIn](#)
- [Youtube](#)
- [Google +](#)

3.9.4 About

Description

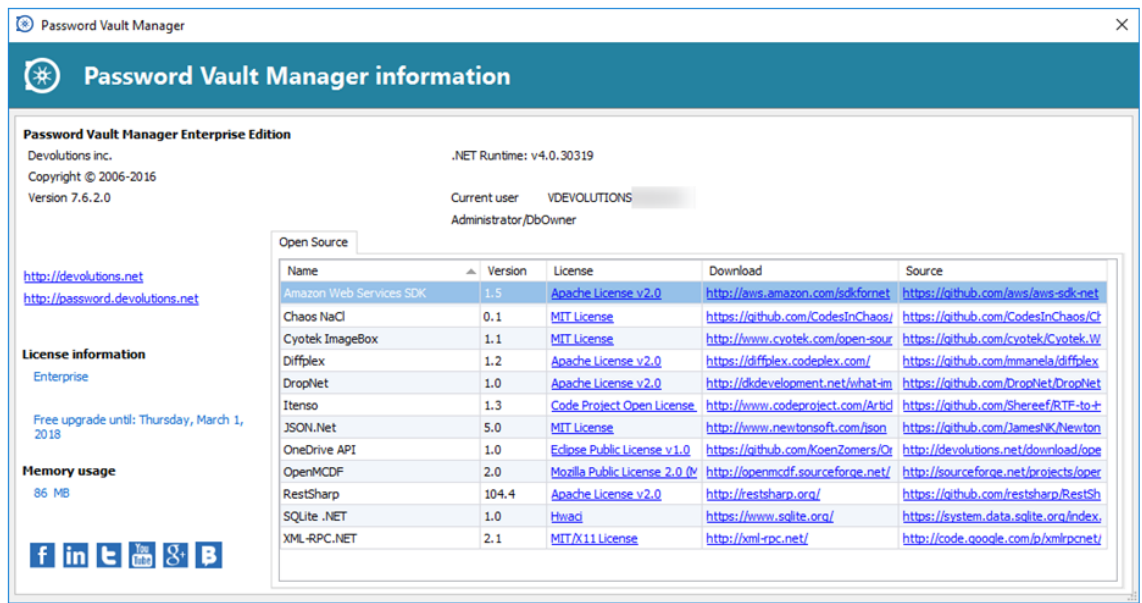
The **About** section contains Check for Upgrade options and also the About section.



Help - About

Option	Description
Check Version	Verify if your Password Vault Manager version is up-to-date.
Upgrade to Enterprise Edition	If you are using the Free edition and wish to upgrade to the Enterprise Edition.
About	Open a window containing multiple information regarding Password Vault Manager. It will display your Password Vault Manager version, your license information (if you are administrator) and also your open source.

About

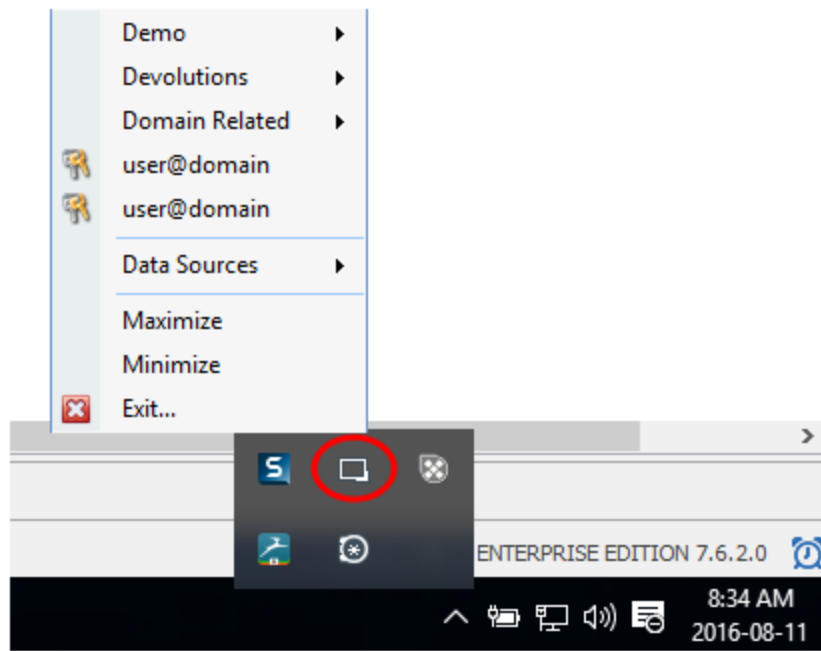


About - Password Vault Manager information

3.10 Tray Icon

Description

Password Vault Manager also lets you show the entry list and other useful information in the Windows system tray. You can also customize the content. To open an entry, click on it or use the context menu by right-clicking on the icon to access more options.

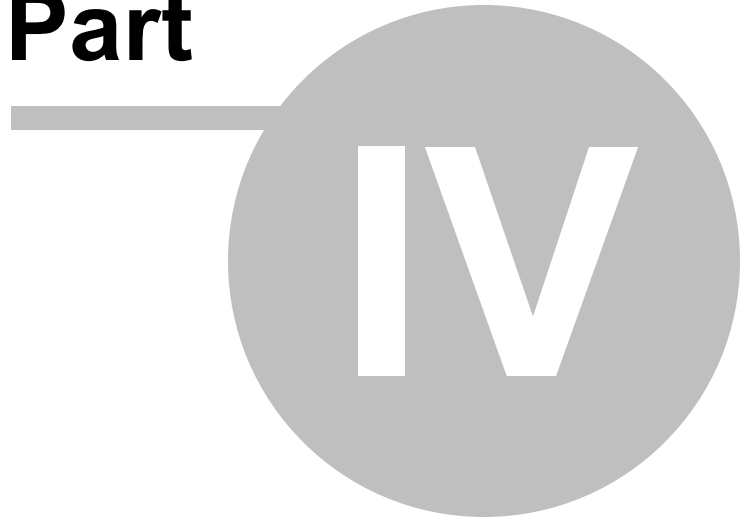


Trayicon View

The application's options window contains many settings that enable you to customize the system tray icon settings. You can also disable it from here, or change its default behavior.

Data Sources

Part



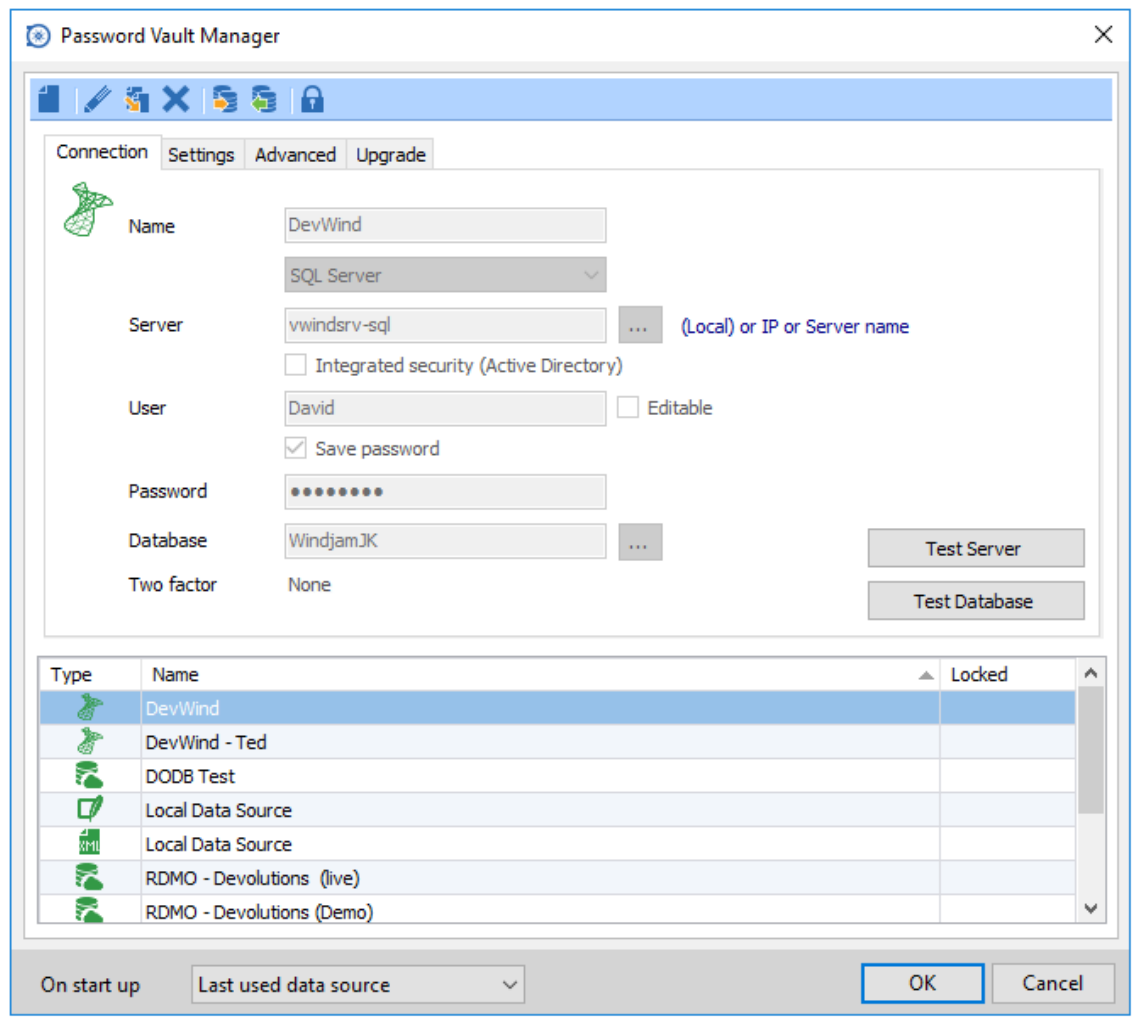
4 Data Sources

Description

The data source is at the heart of Password Vault Manager, it is the container that holds all entries.

Settings

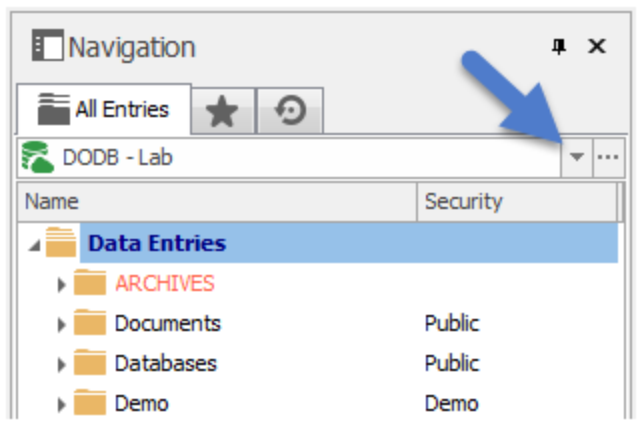
The data source can be a file or database and you can use multiple data sources at the same time as seen below. It needs to be configured on each workstations.



Data Sources

Multiple Data Sources

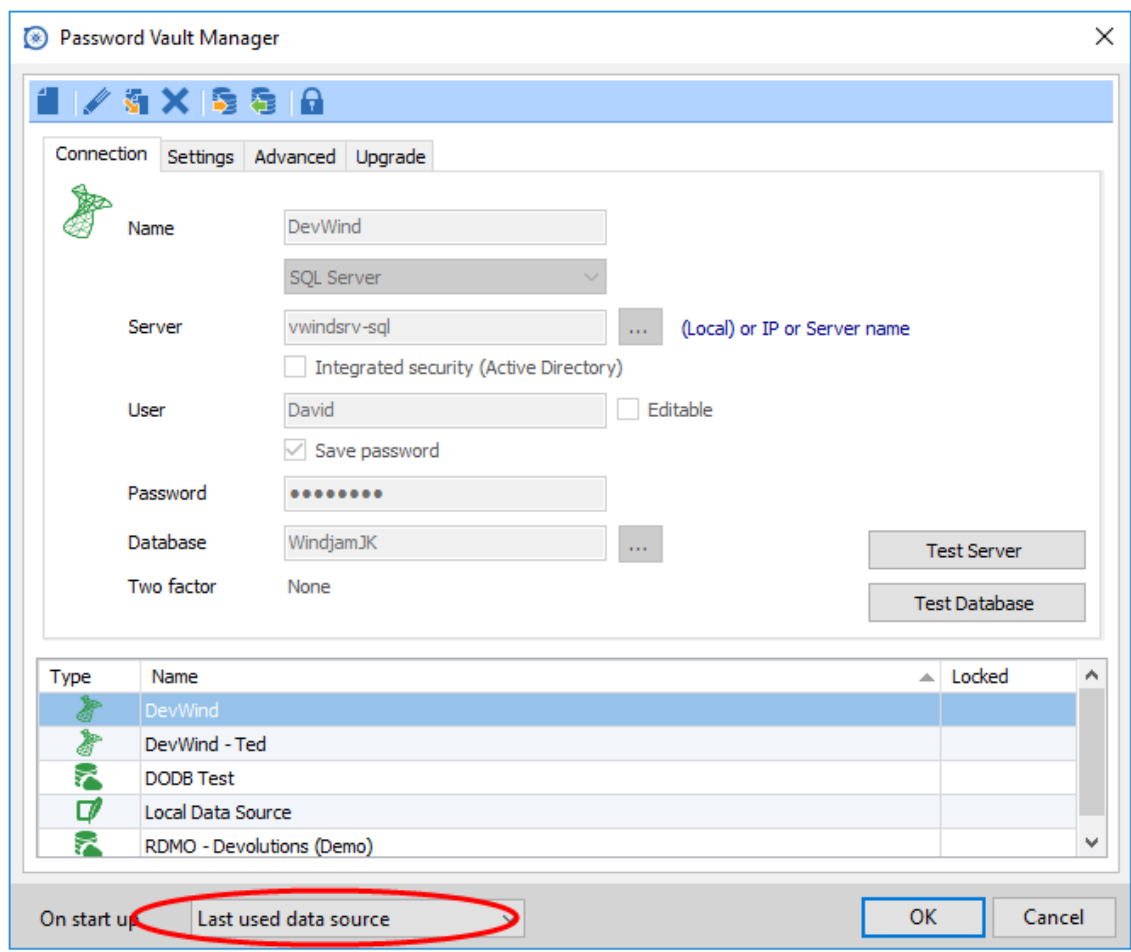
You can configure multiple data sources within the application. These data sources can be of mixed types but there is only one active at a time. It is possible to switch from one data source to another via the data source combo box.



Select Data Source

Open Data Source at Startup

You may assign a data source to open automatically when Password Vault Manager starts.



Option	Description
--------	-------------

Use default data source	Set the data source that you always want to open at start up.
Last used data source	Open with the last used data source.
Prompt for data source	A message box will open on startup for the data source selection.

Data Source Settings

The [Advanced Data Source](#) contains some specific settings or global policies. Those settings are saved directly in the database.


4.1 Data Sources Types






Description





Password Vault Manager supports multiple types of data source. To start, decide which data source you'll be using.








Upon initial installation, you will be running from a local data source which is an SQLite database.

Name	Description	Pros and cons
Amazon S3 storage 	<p>Password Vault Manager saves the settings in a file located in an Amazon S3 bucket.</p> <p>Amazon S3 is a storage service for the Internet. It's designed to make cloud computing accessible to everyone.</p> <p>Amazon S3 provides a simple web service interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. Password Vault Manager uses this API to persist your session settings.</p> <p>More details on cloud computing and Amazon S3 can be found at: http://aws.amazon.com/s3/</p> <p>For more information, please consult Amazon S3 topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Can be shared in read-only mode • Backups (by Amazon) are automatic <p>Cons:</p> <ul style="list-style-type: none"> • You must have an Amazon account and pay storage and transfer fees, although most would agree they are minimal. • No security management • There is a possibility of conflicts or data corruption to occur • Doesn't support all features, such as attachments, connection logs and Security Management
Devolutions Online Database	Password Vault Manager connects to Devolutions online repository.	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • Secure

	<p>Note that there are different subscription levels for that product.</p> <p>The Basic is appropriate for micro teams (up to 3 users), whereas the Professional and Enterprise editions are for larger teams.</p> <p>For more information, please consult Online Database topic.</p>	<ul style="list-style-type: none"> Depending on the subscription level, supports all features, such as attachments, connection logs, Offline Mode and Security Management <p>Cons:</p> <ul style="list-style-type: none"> Not hosted internally
<p>Devolutions Online Drive</p> 	<p>Password Vault Manager uses Devolutions Online Drive to store and synchronize your sessions. Access your sessions from anywhere using a simple Internet connection.</p> <p>For more information, please consult Online Drive topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Quick Reliable The service is free <p>Cons:</p> <ul style="list-style-type: none"> No possibility for sharing No security management
<p>Devolutions Server</p> 	<p>Password Vault Manager uses Devolutions Server to store session information.</p> <p>For more information, please consult Devolutions Server topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Quick Reliable Secure Supports all features, such as attachments, connection logs, Offline Mode and Security Management Active Directory integration
<p>Dropbox</p> 	<p>Password Vault Manager uses the Dropbox API to retrieve the XML file from the configured repository.</p> <p>For more information, please consult Dropbox topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Can be shared in read-only mode Backups (by Dropbox) are automatic Storage infrastructure is free (if within your free storage quota) <p>Cons:</p> <ul style="list-style-type: none"> No security management There is a possibility for conflict or data corruption to occur Doesn't support all features, such as attachments, connection logs and Security Management
<p>FTP</p> 	<p>Password Vault Manager uses an FTP connection to retrieve the XML file.</p> <p>For more information, please consult FTP topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> Can be shared in read-only mode Easy to deploy online <p>Cons:</p> <ul style="list-style-type: none"> No security management There is a possibility for conflict or data corruption to occur Doesn't support all features, such as attachments, connection logs and Security Management

<p>MariaDB</p> 	<p>Password Vault Manager uses MariaDB as a drop-in replacement for MySQL.</p> <p>For more information, please consult MariaDB topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • The database is free and can be installed on Linux • Supports all features, such as attachments, connection logs, Offline Mode and Security Management <p>Cons:</p> <ul style="list-style-type: none"> • MariaDB needs to be installed
<p>Microsoft Access</p> 	<p>Password Vault Manager saves the settings in a Microsoft Access database on the local machine, or on a network share.</p> <p>Microsoft Access is a pseudo relational database management system from Microsoft, which combines the relational Microsoft Jet Database Engine with a graphical user interface and software development tools.</p> <p>Access is no longer supported by Microsoft, this option is not possible on newer operating systems.</p> <p>For more information, please consult Microsoft Access topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Easy setup • Can be shared • Easy backup <p>Cons:</p> <ul style="list-style-type: none"> • Slower than SQL Server • No security management • There is a possibility for conflict or data corruption to occur • Doesn't support all features, such as attachments, connection logs and Security Management
<p>Microsoft SQL Azure</p> 	<p>Password Vault Manager uses the Microsoft cloud platform to save and manage all sessions.</p> <p>For more information, please consult SQL Azure topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • Secure • Supports all features, such as attachments, connection logs, Offline Mode and Security Management <p>Cons:</p> <ul style="list-style-type: none"> • Microsoft Azure needs to be configured
<p>Microsoft SQL Server</p> 	<p>Password Vault Manager uses the power of SQL Server to save and manage all sessions. This is the recommended data source for a multi-user environment.</p> <p>For more information, please consult SQL Server (MSSQL) topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • Secure • Supports all features, such as attachments, connection logs, Offline Mode and Security Management • SQL Server Express is free <p>Cons:</p> <ul style="list-style-type: none"> • SQL Server must be installed

<p>MySQL</p> 	<p>Password Vault Manager uses a MySQL database to store session information.</p> <p>For more information, please consult MySQL topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • The database is free and can be installed on Linux • Supports all features, such as attachments, connection logs, Offline Mode and Security Management <p>Cons:</p> <ul style="list-style-type: none"> • MySQL needs to be installed
<p>SFTP</p> 	<p>Password Vault Manager uses a Secure FTP connection to retrieve the XML file.</p> <p>For more information, please consult SFTP topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Can be shared in read-only mode • Easy to deploy online <p>Cons:</p> <ul style="list-style-type: none"> • No security management • There is a possibility for conflict or data corruption to occur • Doesn't support all features, such as attachments, connection logs and Security Management
<p>SQLite</p> 	<p>Password Vault Manager uses a SQLite database to store session information.</p> <p>For more information, please consult SQLite topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Quick • Reliable • The database is free • Supports all features, such as attachments, connection logs, Offline Mode and Security Management <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing • No security management
<p>Web</p> 	<p>Password Vault Manager uses a Web connection to retrieve the XML file.</p> <p>For more information, please consult Web topic.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Easy backup • Can be edited manually or by an external system • Nothing to install <p>Cons:</p> <ul style="list-style-type: none"> • No possibility for sharing • Read-only • Doesn't support all features, such as attachments, connection logs and Security Management
<p>XML</p> 	<p>Password Vault Manager saves the settings directly in a file with the XML format.</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Easy backup • Can be edited manually or by an external system • Nothing to install

	For more information, please consult XML topic.	<p>Cons:</p> <ul style="list-style-type: none"> • No possibility of sharing • No security management • There is a possibility for conflict or data corruption to occur • Doesn't support all features, such as attachments, connection logs and Security Management
--	---	--

4.1.1 Choosing the data source type

Description

To make things simple, we are presenting a set of concerns and the list of data sources that can serve in that context. If you have multiple concerns simply create the intersection of all sets to isolate a list of choices.

Concern	Devolutions Server	SQL Server	SQL Azure	MySQL/MariaDB	DODB Pro	DODB Ent
The database is not accessible to end users.	X	Note 1	Note 1	Note 1	Note 1	Note 1
AD accounts used for authentication	X	X				
AD group membership used to assign permissions	X					
The data is stored locally	X	X		X		
Activity Logs	X	X	X	X		
Data accessible globally	Note 2	Note 3	X	Note 3	X	X
Optional local cache of connections	X	X	X	X	X	X

Notes

Note 1

The administrators can create accounts for end users without divulging the passwords. A locked data source definition is imported for each end user. This obviously requires a lot of manual operations.

Note 2

You should not expose a Devolutions Server instance to the Internet without being able to protect it from DDoS attacks. Strong passwords must be used as well as obscure account names that are not easily inferred using social data mining.

Note 3

You can indeed expose a RDBMS to the Internet, but you must use SSL/TLS to encrypt traffic, you must also protect against DDoS attacks.

4.1.2 Amazon S3

Description



Password Vault Manager saves the settings in a file located in an Amazon S3 bucket. Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for everyone.

Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web and Password Vault Manager uses this API to persist your session settings.

More details on cloud computing and Amazon S3 can be found at: <http://aws.amazon.com/s3/>

Highlights

- This data source can be shared over the Internet between multiple locations.
- This is a file-based data source, based on the XML data source



Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues. This data source type is meant for a single user using multiple computers, not multiple users.


Settings

Connection

Password Vault Manager

Amazon S3

Connection **Advanced**


 Name

Access key ID

Secret access key

Bucket name

Key name (filename)

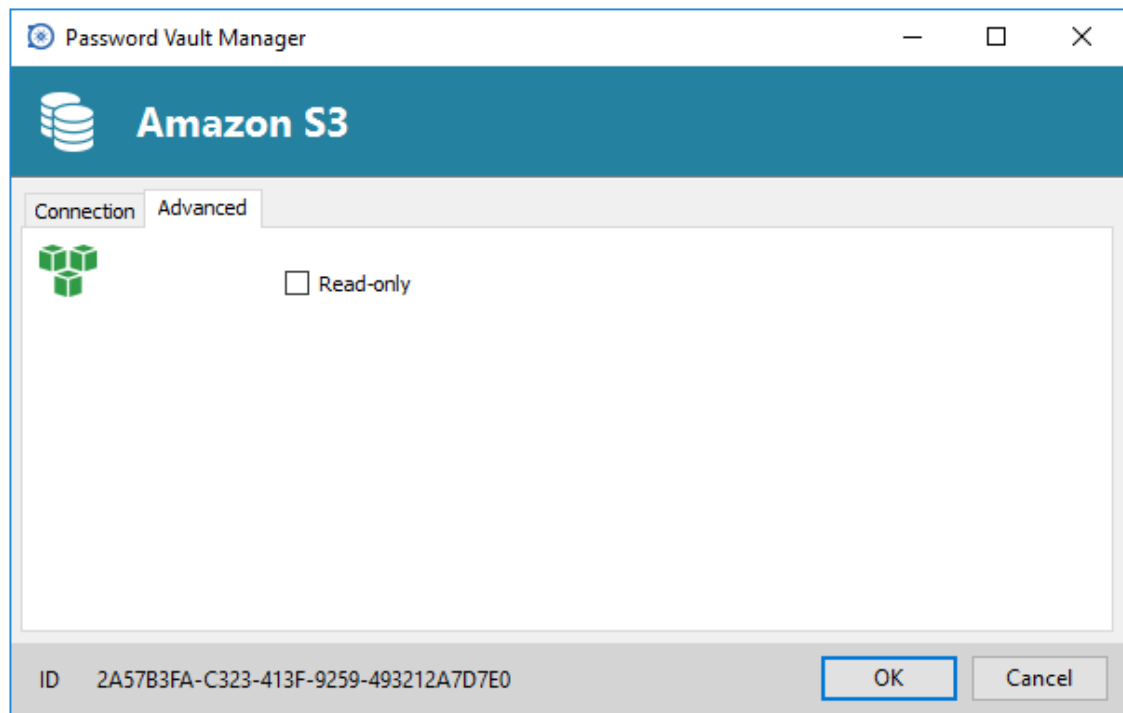
 The file will be created if it does not exist

ID 2A57B3FA-C323-413F-9259-493212A7D7E0

Amazon S3 - Connection tab

Option	Description
Name	Name of the data source.
Access key ID	Enter the Amazon S3 Access Key ID.
Secret access key	Enter the Amazon S3 Secret access ID.
Bucket name	Enter the bucket name created on Amazon S3 website and used by the application.
Key name (filename)	Enter the file name that will used be store the data on Amazon S3.

Advanced



Amazon S3 - Advanced tab

Option	Description
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.

4.1.3 Dropbox

Description



Password Vault Manager uses the Dropbox API to retrieve the XML file from the configured repository. There is no need to install the Dropbox client on the machine to open the data source. It is also possible to configure more than one Dropbox account on the same machine.

Highlights

- This data source can be shared over the Internet between multiple locations
- The data source supports auto refresh
- This is a file-based data source, based on the XML data source
- To avoid data corruption, the session list should be modified in one location at a time
- No need to have the Dropbox client installed to use the Dropbox data source
- Each Dropbox data source can use a different Dropbox account



Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues. This data source type is meant for a single user using multiple computers, not multiple users.

Settings

Connection

Dropbox - Connection

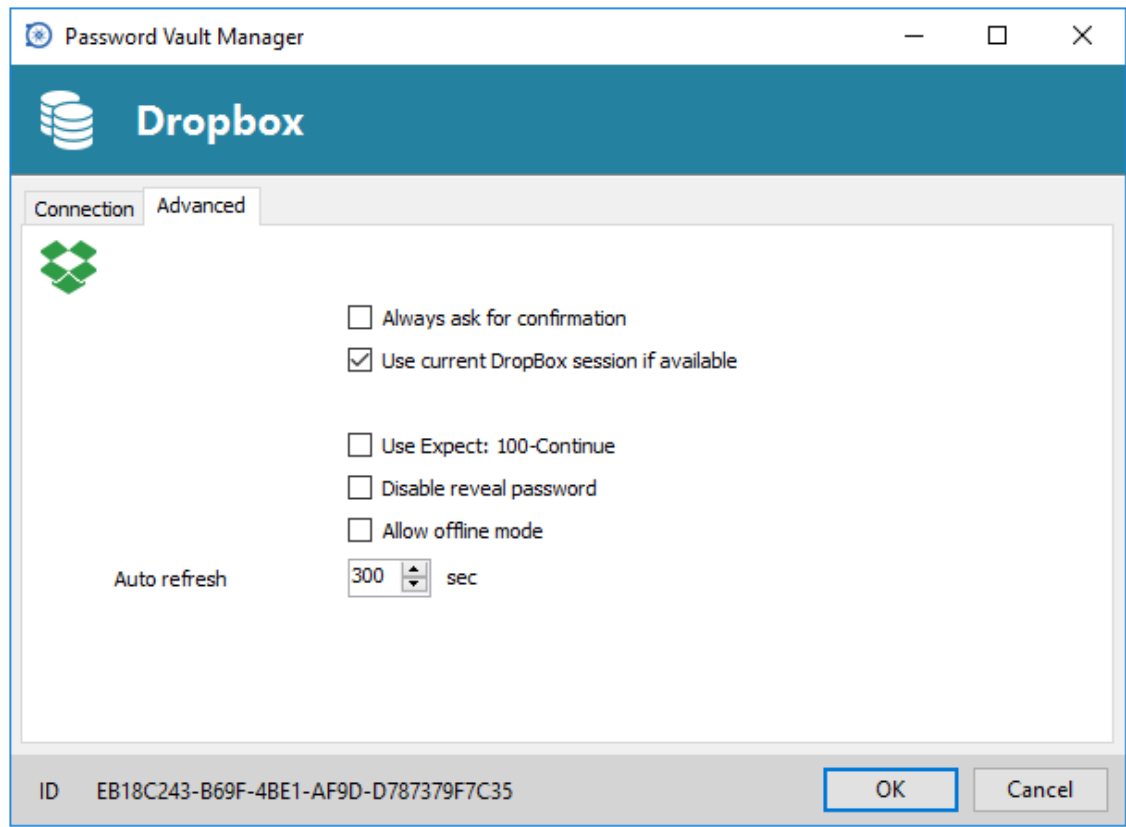


Password Vault Manager support the 2-Factor Authentication of Dropbox. When the button **Validate with Dropbox** is press and the 2-Factor Authentication is enabled in Dropbox, a first box will open and ask for the Dropbox account password. After, a second box will open to enter the security code. The security code can be receive by SMS or generate by Google Authenticator.

Option	Description
Name	Name of the data source.
Mode	Select the preferred mode to configure the data source. Select between: <ul style="list-style-type: none"> • Account • Local
Email	Contains the email address associated with the Dropbox account.
Validate with Dropbox	Button to validate the email address with the Dropbox account.

Dropbox directory	Indicate the folder in Dropbox. It should not contains any drive since it's stored online. Leave it empty to use the default Dropbox root.
Filename	Indicate the filename used to store the data on the data source.
Compress database file	Activate this option if you wish to compress your database file.

Advanced



Dropbox - Advanced tab

Option	Description
Always ask for password	Always ask for password when connecting to the data source.
Use current Dropbox session if available	This option will use the Dropbox account who has been already validated without any other validation.
Use Expect: 100-Continue	Use the HTTP response status codes.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allow the data source to be used in Offline Mode .
Auto refresh	Set the interval to use between each automatic refresh.

4.1.4 FTP

Description



Password Vault Manager downloads and uploads the session settings directly from file located on an FTP site.

Highlights

- This data source can be shared over the Internet between multiple locations
- This is a file-based data source, based on the XML data source



Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues.

Settings

Connection

Password Vault Manager



Ftp

Connection | Advanced | Security Settings | Proxy Settings | SSH Settings

Name


FTP path Port

Username

Password  

Filename

Passive mode

 The file will be created if it does not exist

ID FDF7CE62-562B-4029-AB1A-BC15BCEE7CCF

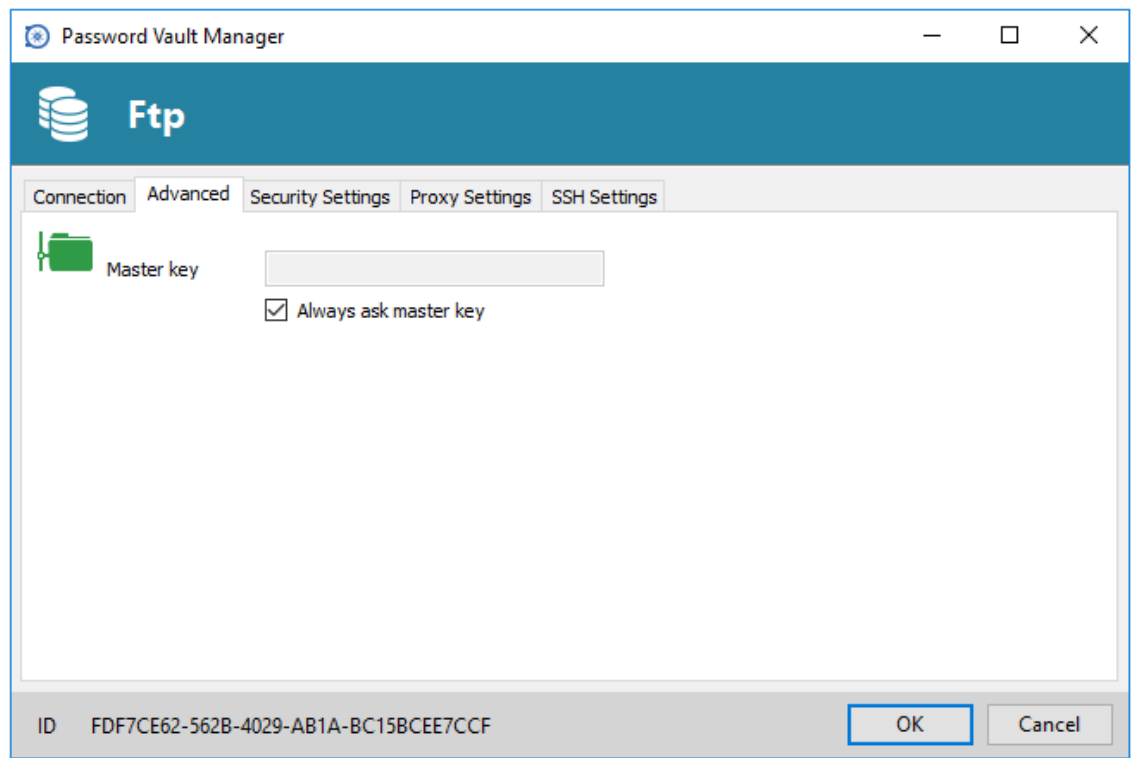
OK Cancel

FTP - Connection tab

Option	Description
Name	Name of the data source.
FTP Path	FTP server name to access the XML file.

Passive mode	Set the FTP mode to passive.
Username	Username used to access the FTP server.
Password	Password used to access the FTP server.
Filename	Indicate the remote folder and filename for data source XML.

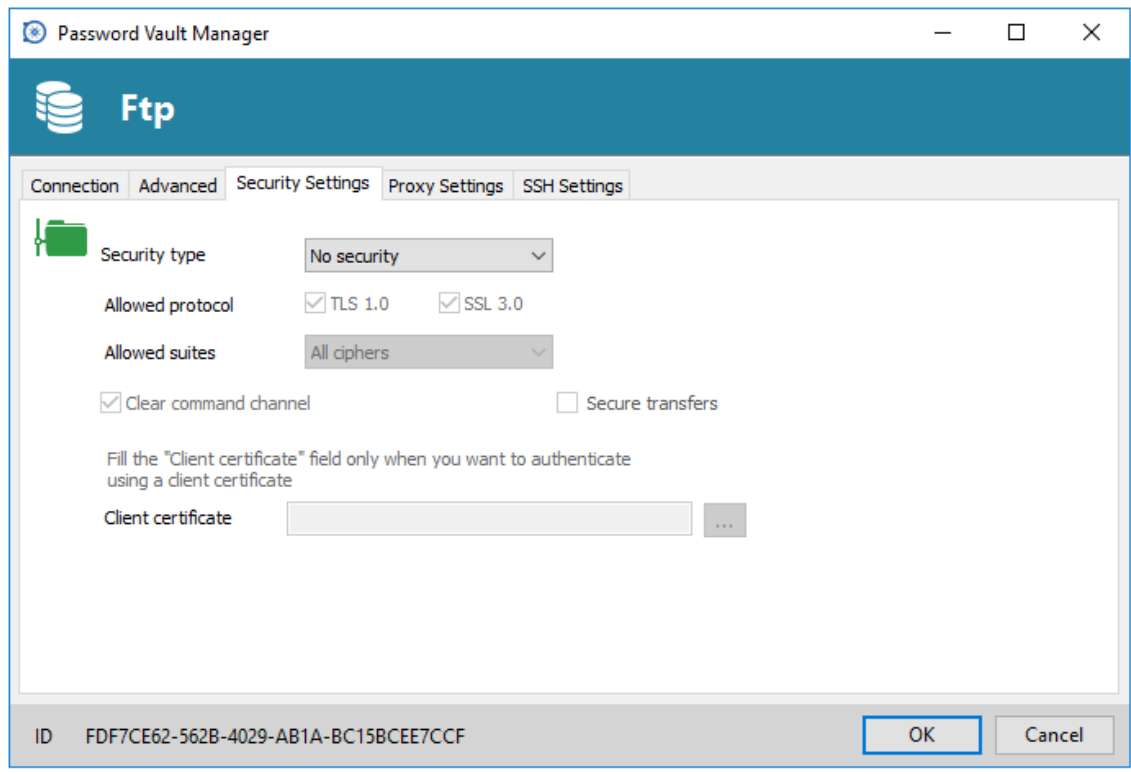
Advanced



FTP - Advanced tab

Option	Description
Always ask master key	Always ask the master key when connecting to the data source. The application will not store any password.

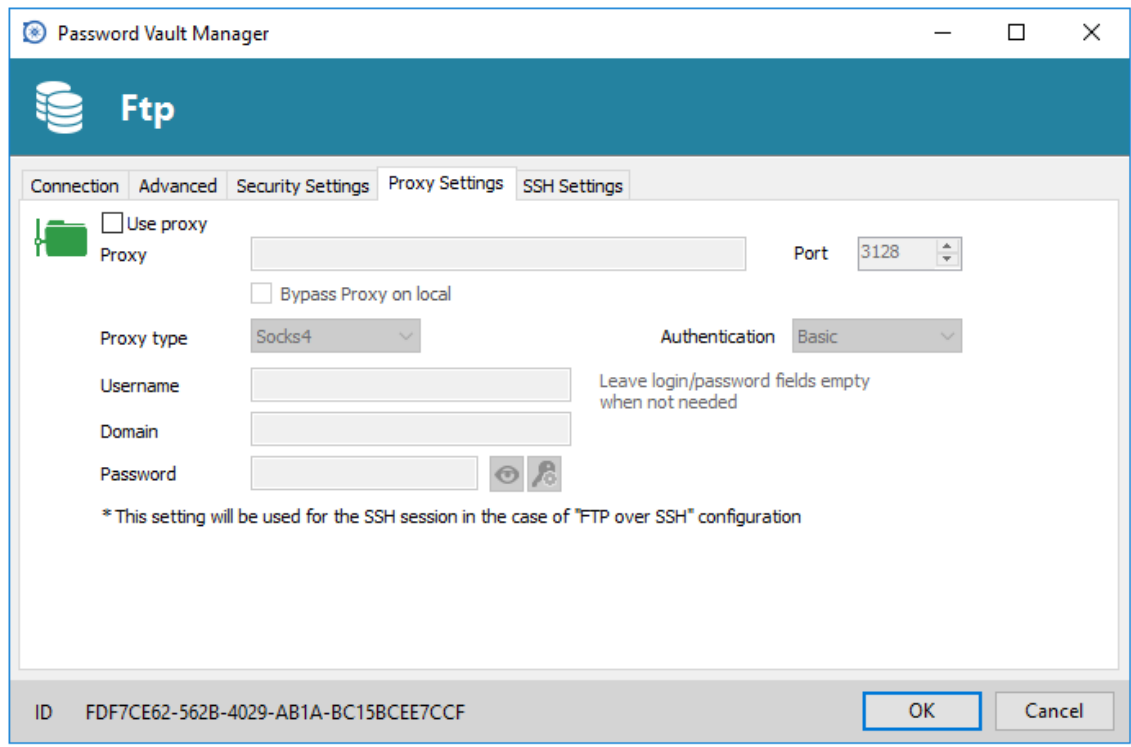
Security Settings



FTP - Security Settings

Option	Description
Security type	Specify the security type used for the FTP connection.
Allowed protocol	Indicate the allowed FTP protocol.
Allowed suites	Indicate the allowed cipher suites.
Clear command channel	If the Clear Control Connection (CCC) setting is enabled, the FTP client connects to the server, negotiates a secure connection, authenticates (sends user and password) and reverts back to plaintext.
Secure transfers	Enable the secure transfers.
Client certificate	Specify the client certificate used for the authentication.

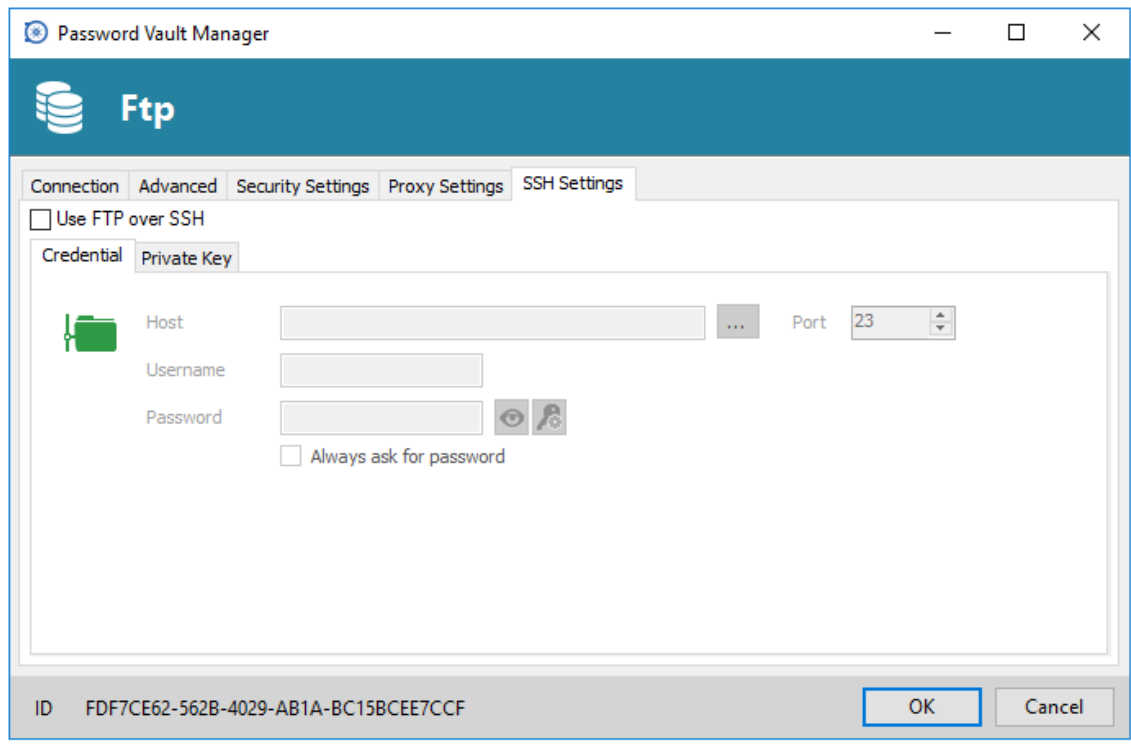
Proxy Settings



FTP - Proxy Settings

Option	Description
Use proxy	Enable this option if you wish to use a proxy server.
Proxy	Enter the name of the Proxy Server.
Bypass Proxy on local	For local addresses, the proxy server will not be used.
Proxy type	Specify the proxy type to use.
Authentication	Select the type of authentication mode used to connect on the proxy server such as Basic or NTLM.
Username	Username to access the Proxy server.
Domain	Domain to access the Proxy server.
Password	Password to access the Proxy server.

SSH Settings



FTP - SSH Settings

Option	Description
Use FTP over SSH	Use FTP over SSH connection.
Host	Name of the host to access the FTP over SSH.
Username	Username to access the FTP Server over SSH.
Password	Password to access the FTP Server over SSH.
Always ask for password	Will always prompt you for your password.
No private Key	Indicate that no private key is used.
Private key file	Specify the private key filename located on the local disk.
Private key data	Specify the private key data instead of the filename.

4.1.5 Microsoft Access

Description



Password Vault Manager saves the settings in a Microsoft Access database, located on the local machine or on a network share.

Microsoft Access is a pseudo relational database management system from Microsoft, which combines the relational Microsoft Jet Database Engine with a graphical user interface and software development tools.

Highlights

- This data source supports the native Access database password (Note that the password must be set using Microsoft Access directly. Password Vault Manager does not allow you to set or change the database, because it requires an exclusive connection to it)
- The [Offline Mode](#) is supported by this data source
- The database can be shared by multiple users on a network drive, but the performance and the data integrity can't be guaranteed
- The [Online Backup Service](#) is available for this data source



This data source is **not recommended** since Microsoft has stopped providing support in the newest Windows version.



Entering a database password when creating the physical file has no effect. You must use Microsoft Access to set the password in the database file.

Settings

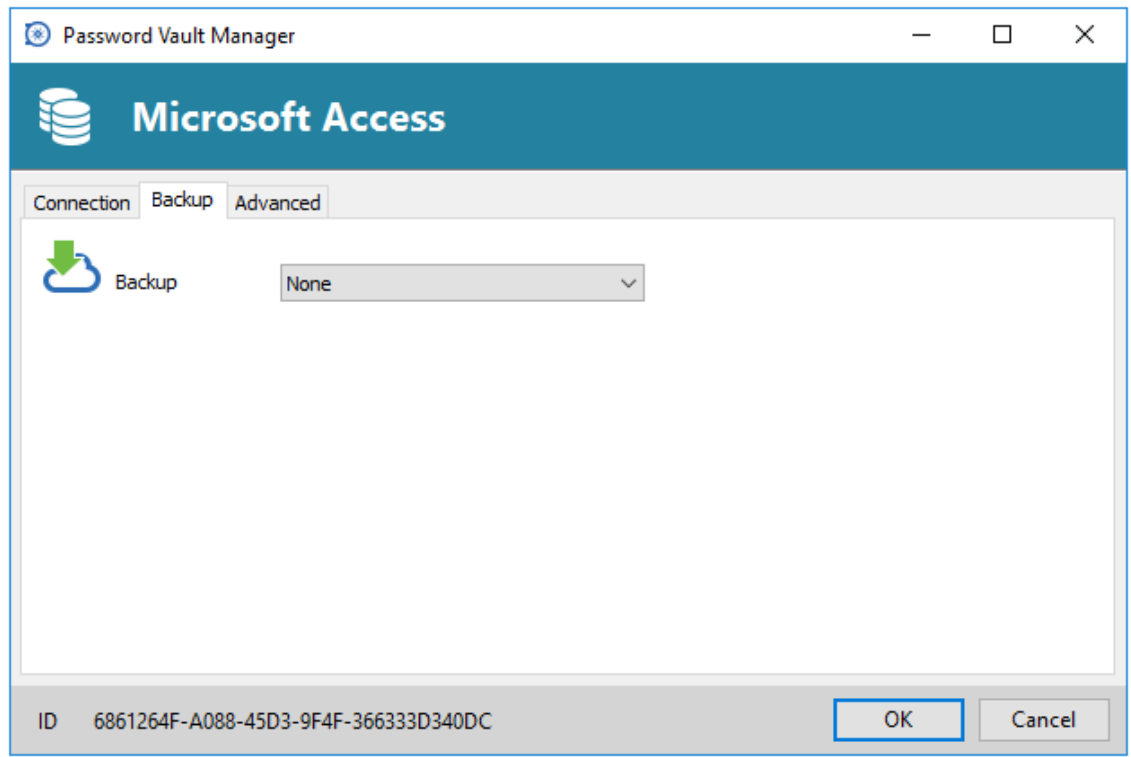
Connection

Microsoft Access - Connection tab

Option	Description
Name	Name of the data source.

Filename	Indicate the destination folder including the data source file name. This needs to be an .mdb file extension.
Database password	Password to open the database. The application will not set the password. It needs to be applied with another tool like Microsoft Access directly.
Always ask password	Always ask for password when connecting to the data source.
Two factor	Enable the 2-Factor Authentication to access your data source.

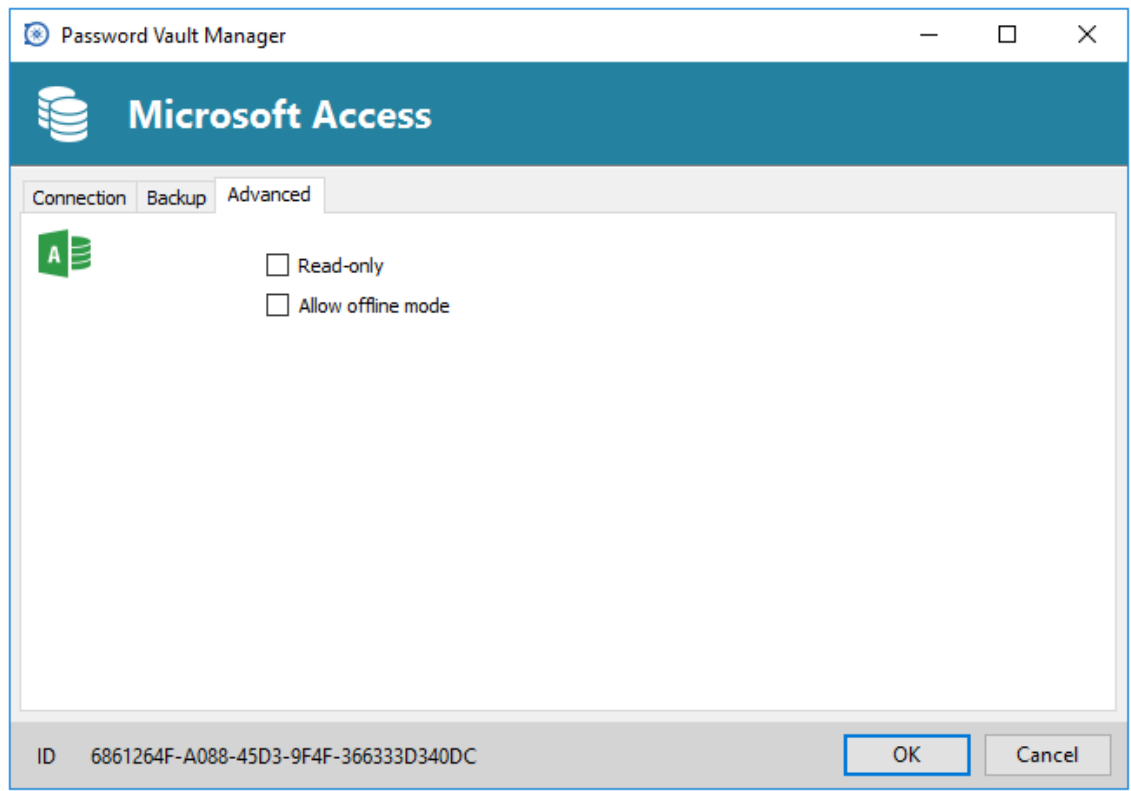
Backup



Microsoft Access - Backup

Option	Description
Backup	Select between: <ul style="list-style-type: none"> • None: No backup of your data source will be created. • Online Backup: An Online Backup (using Online Backup Service) will automatically be created. • Save to file: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.

Advanced



Microsoft Access - Advanced tab

Option	Description
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.
Allow offline mode	Allow the data source to be used in Offline Mode .

4.1.6 Online Drive

Description

Please consult topic [Online Drive](#) for information on this service.

Settings

Connections

Password Vault Manager

Devolutions Online Drive

Connection Backup Advanced

Name

Use default Devolutions Cloud credentials

Email

Password Always ask for password

[Create a free account](#) [Forgot password](#)

Filename ...

The file will be created if it does not exist

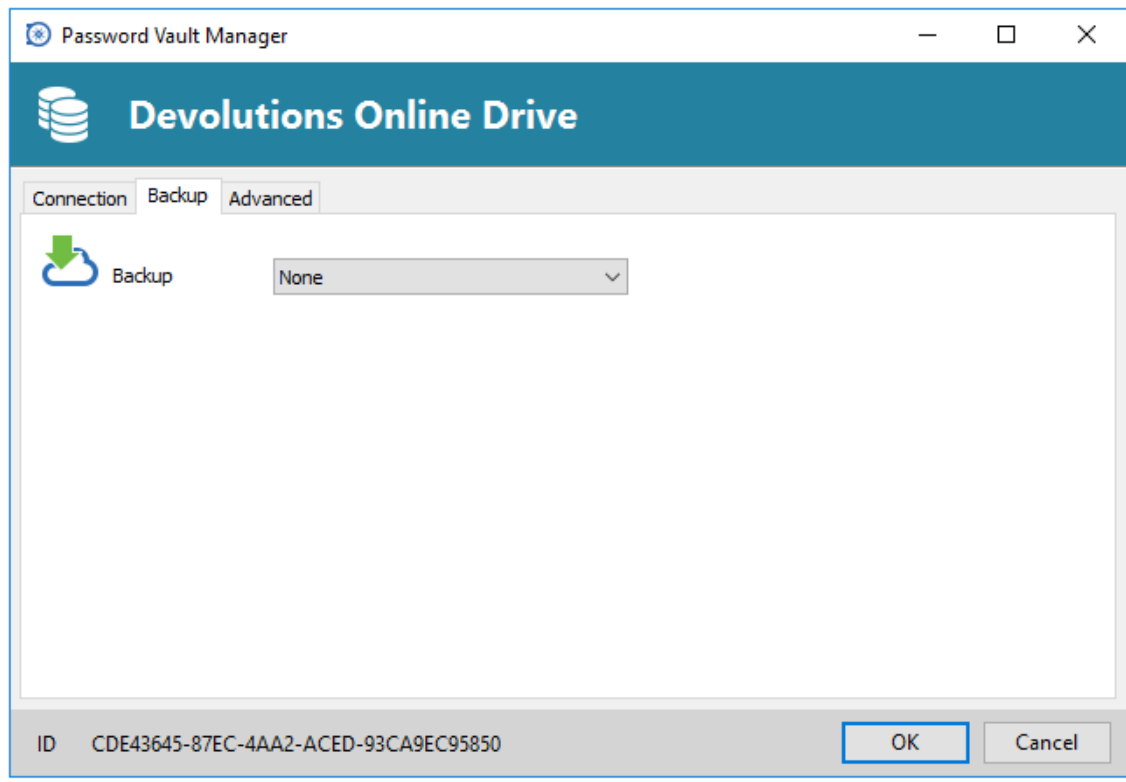
Server

ID CDE43645-87EC-4AA2-ACED-93CA9EC95850

Devolutions Online Drive - Connection tab

Option	Description
Name	Name of the data source.
Use default Remote Desktop Manager Online credentials	Use the credentials from your Devolutions Cloud account. You need to be connected with this account in File - Online Account .
Email	Contains the email address associated with the Devolutions Cloud account.
Password	Password used to access the Devolutions Cloud account.
Create a free account	Create a new Devolutions Cloud Online account.
Filename	Indicate the filename used to store the data on the data source.
Test Connection	Test the connection with Devolutions Online Drive to validate if the proper information has been provided.

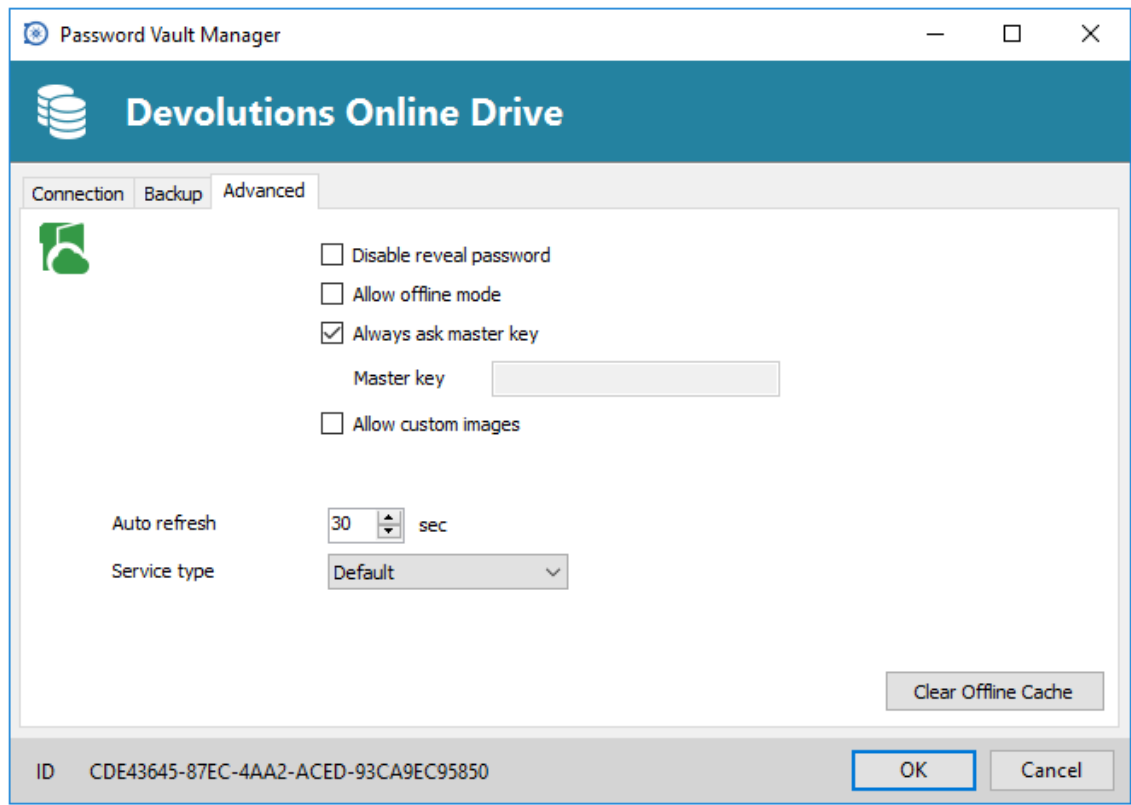
Backup



Devolutions Online Drive - Backup tab

Option	Description
Backup	Select between: <ul style="list-style-type: none">• None: No data source backup will be created.• Online Backup: An Online Backup (using Online Backup Service) will automatically be created.• Save to file: Your backup will be saved to a chosen file but will not automatically proceed with a backup every 30 seconds.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and easily restore it if encountering any issues.

Advanced



Devolutions Online Drive - Advanced tab

Option	Description
Disable reveal password	Disable the reveal password feature when a user access this data source.
Allow offline mode	Allows the data source to be used in Offline Mode .
Always ask master key	Always ask for the master key when connecting to the data source.
Allow custom images	Allows the user to use custom images.
Auto refresh	Set the interval to use between each automatic refresh.
Service type	Select your service type between: <ul style="list-style-type: none"> • Default (the default is the option defined in the File - Option - Cloud) • Web API client • Web service client
Clear Offline Cache	Clear the offline cache on your computer. This can be very helpful when encountering offline issues.

4.1.7 SFTP

Description



Password Vault Manager downloads and uploads the session settings directly from a XML file located on an Secure FTP.

Highlights

- This data source can be shared over the Internet between multiple users
- This is a file-based data source, based on the XML data source



Although it can be shared between multiple locations, there is no conflict management for the configuration. If you share with other users you may get update conflicts and run into issues. This data source type is meant for a single user using multiple computers, not multiple users.

Settings

Connection

The screenshot shows the 'SFTP' configuration window in Password Vault Manager. The window has a title bar 'Password Vault Manager' and a header 'SFTP'. Below the header are four tabs: 'Connection' (selected), 'Advanced', 'Proxy Settings', and 'Private Key'. The 'Connection' tab contains the following fields:

- Name:** SFTP
- FTP host:** (empty text box)
- Port:** 22 (dropdown menu)
- Username:** (empty text box)
- Password:** (empty text box with eye and key icons)
- Filename:** (empty text box)

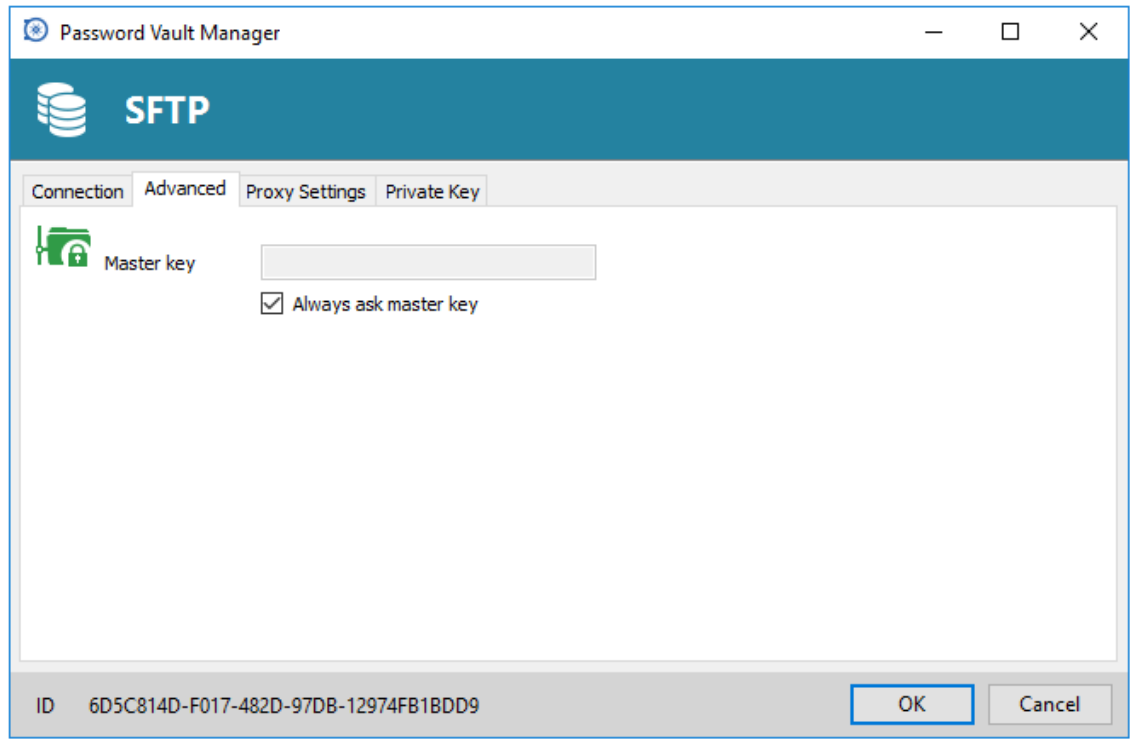
Below the fields is an information icon and the text: 'The file will be created if it does not exist'. At the bottom of the window, there is an ID field with the value '6D5C814D-F017-482D-97DB-12974FB1BDD9' and 'OK' and 'Cancel' buttons.

SFTP - Connection tab

Option	Description
Name	Name of the data source.
FTP Host	FTP server name to access the XML file.
Port	Select the port to connect on the FTP server.
Username	Username used to access the FTP server.

Password	Password used to access the FTP server.
Filename	Indicate the remote folder and filename for data source XML.

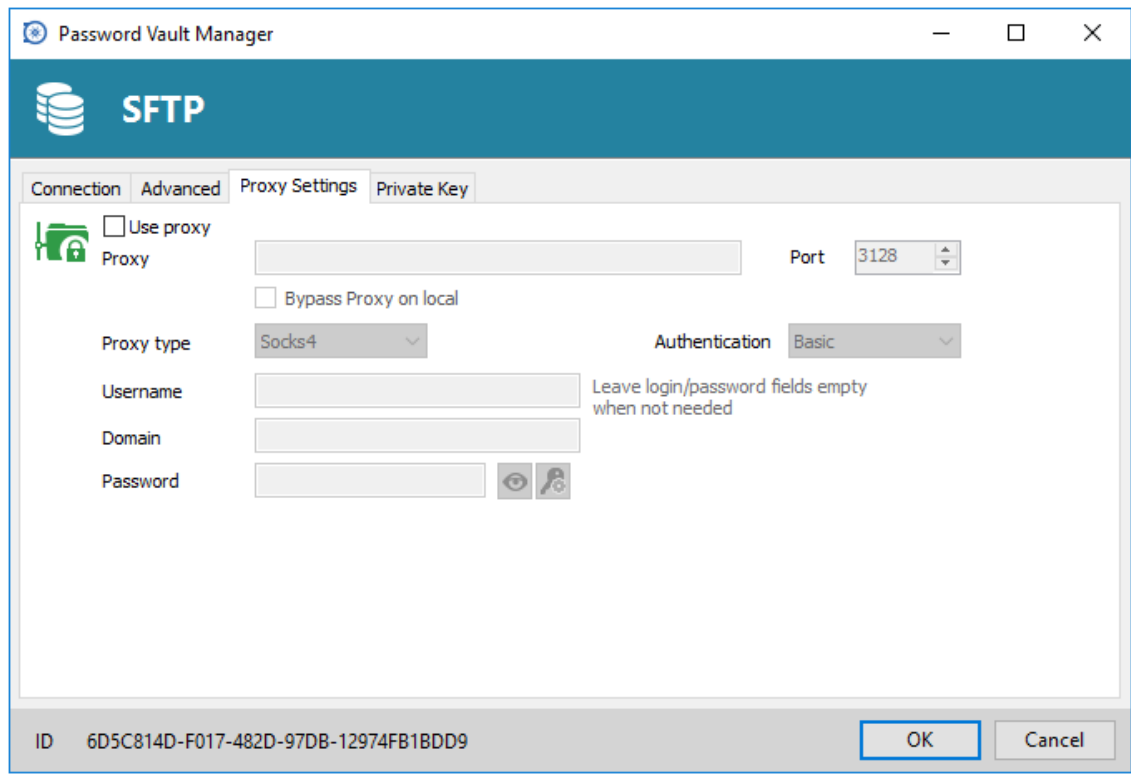
Advanced



SFTP - Advanced tab

Option	Description
Always ask master key	Always ask the Master key when connecting to the data source.

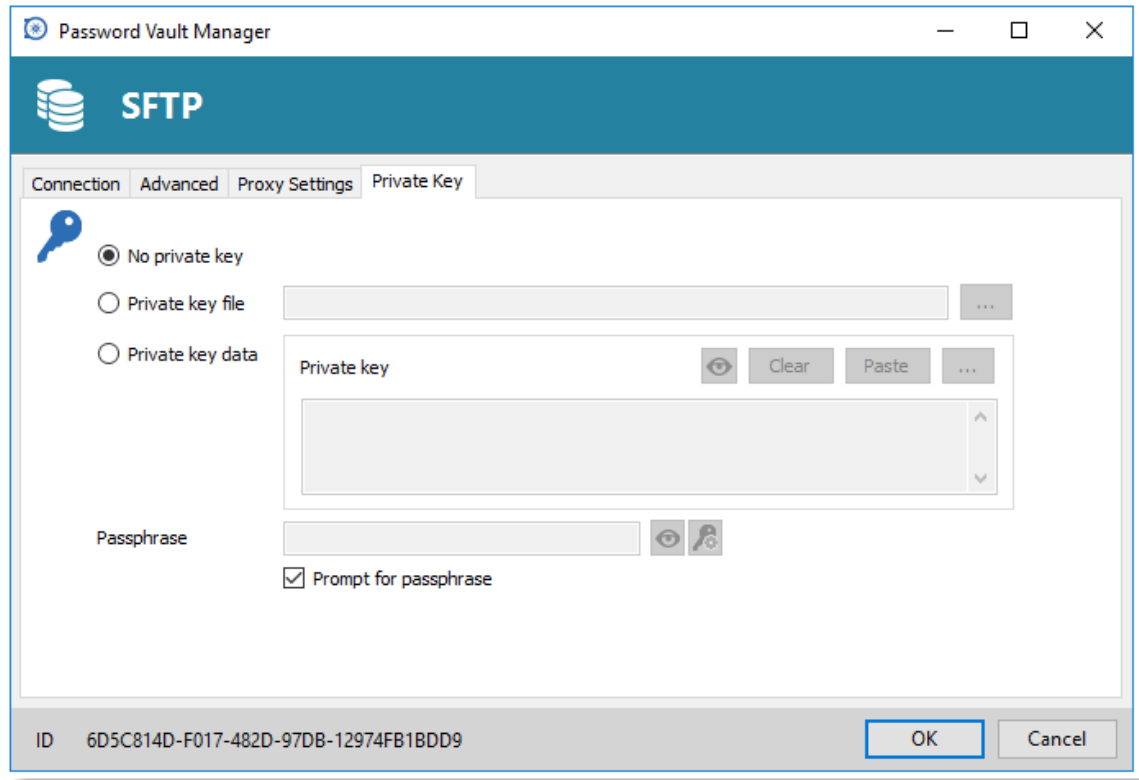
Proxy Settings



SFTP - Proxy Settings tab

Option	Description
Use proxy	Enable this option to set your proxy settings.
Proxy	Enter the name of the proxy Server.
Port	Enter the port of the proxy server
Bypass Proxy on local	For local addresses, the proxy server will not be used.
Proxy type	Specify the proxy type to use. Select between: <ul style="list-style-type: none"> • Socks4 • Socks4a • Socks5 • HttpConnect • FtpSite • FtpUser • FtpOpen
Authentication	Select the type of authentication mode used to connect on the proxy server. Select between: <ul style="list-style-type: none"> • Basic • NTLM
Username	Username to access the proxy server.
Domain	Domain to access the proxy server.
Password	Password to access the proxy server.

Private Key



SFTP - Private Key

Option	Description
No private Key	Indicate that no private key is used.
Private key file	Specify the private key filename located on the local disk.
Private key data	Specify the private key data instead of the filename.
Passphrase	Enter the passphrase to connect.
Prompt for passphrase	Always ask for the passphrase.

4.1.8 SQLite

Description



Password Vault Manager SQLite data source is ideal for single user stand alone situations. More powerful and more flexible than the XML file format, it also supports a few of the advanced data source options like Logs and Attachments.

Highlights

- Full connection log and attachments support
- The [Online Backup Service](#) is available for this data source



All passwords are encrypted by default by Password Vault Manager. You can specify a custom password to fully encrypt the content of the SQLite database.



Password recovery is not possible, the data will be unrecoverable if you cannot authenticate. Please ensure you backup the password in a safe place.

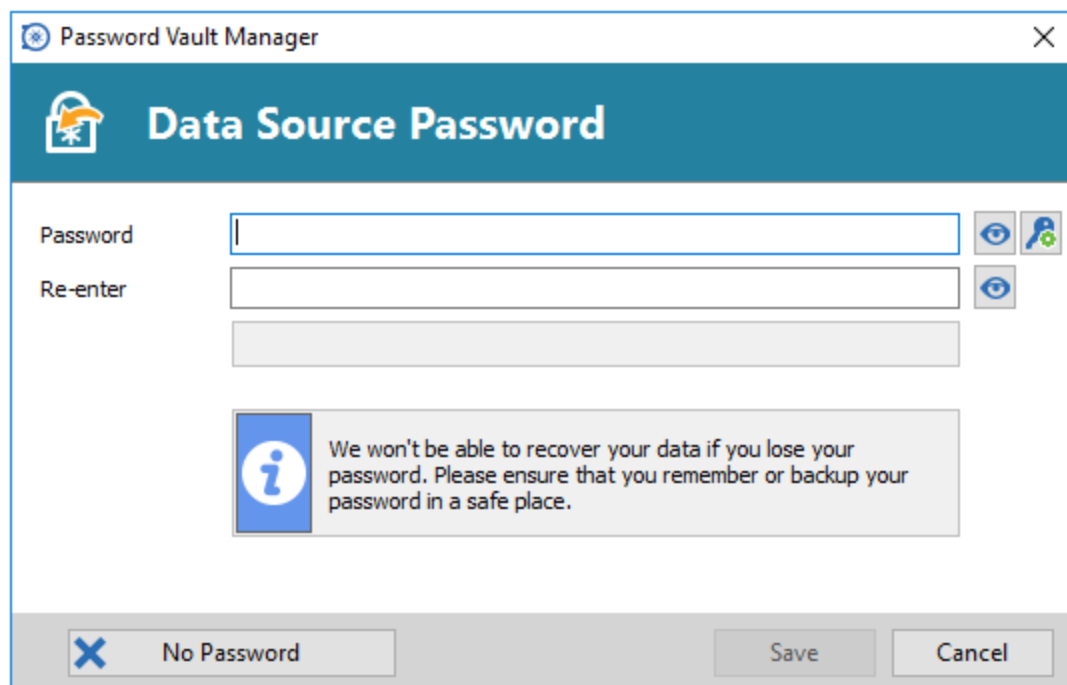


SQLite supports an unlimited number of simultaneous readers, but will only allow one writer at any instant in time. For this reason Password Vault Manager does not support sharing a SQLite data source between several users by storing it on a network drive. If you want to share your data and work in a team environment with your colleagues, please use one of the [Advanced Data Sources](#). Please consult [SQLite.org](#) for more information.

Password management

You can specify a password to further encrypt your data. Specify it at creation time. If the data source already exists you can modify the password by using the **File - Manage Password** dialog.

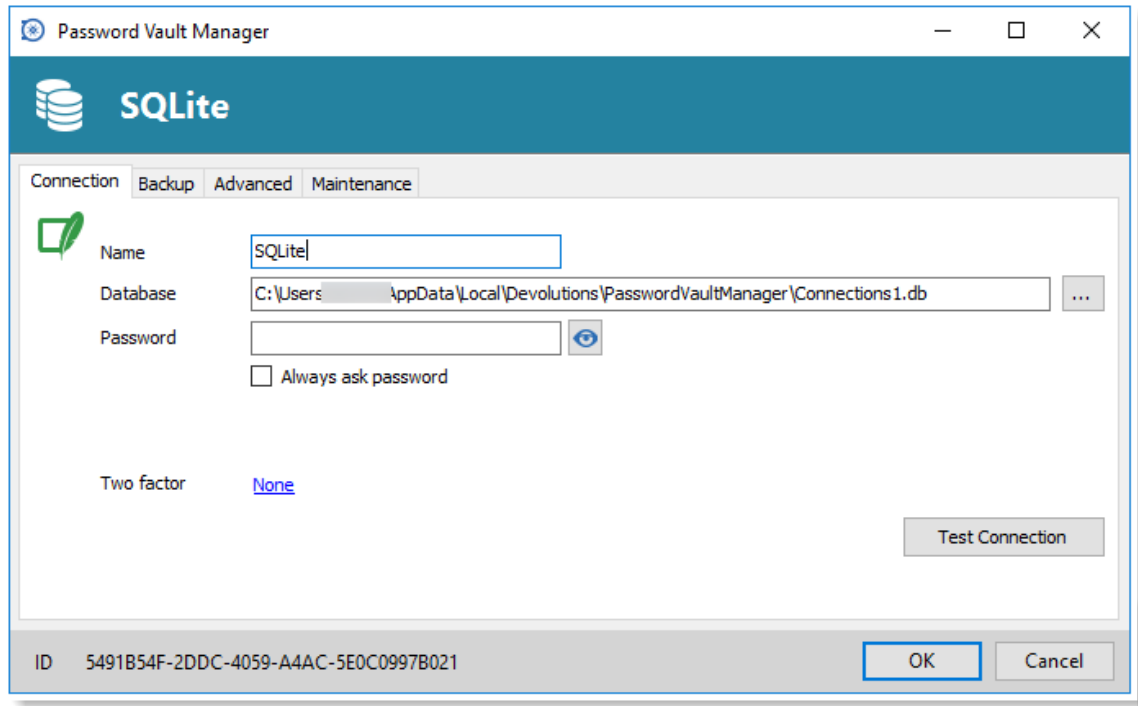
Change or clear the password of an SQLite data source.



Manage Data Source password

Settings

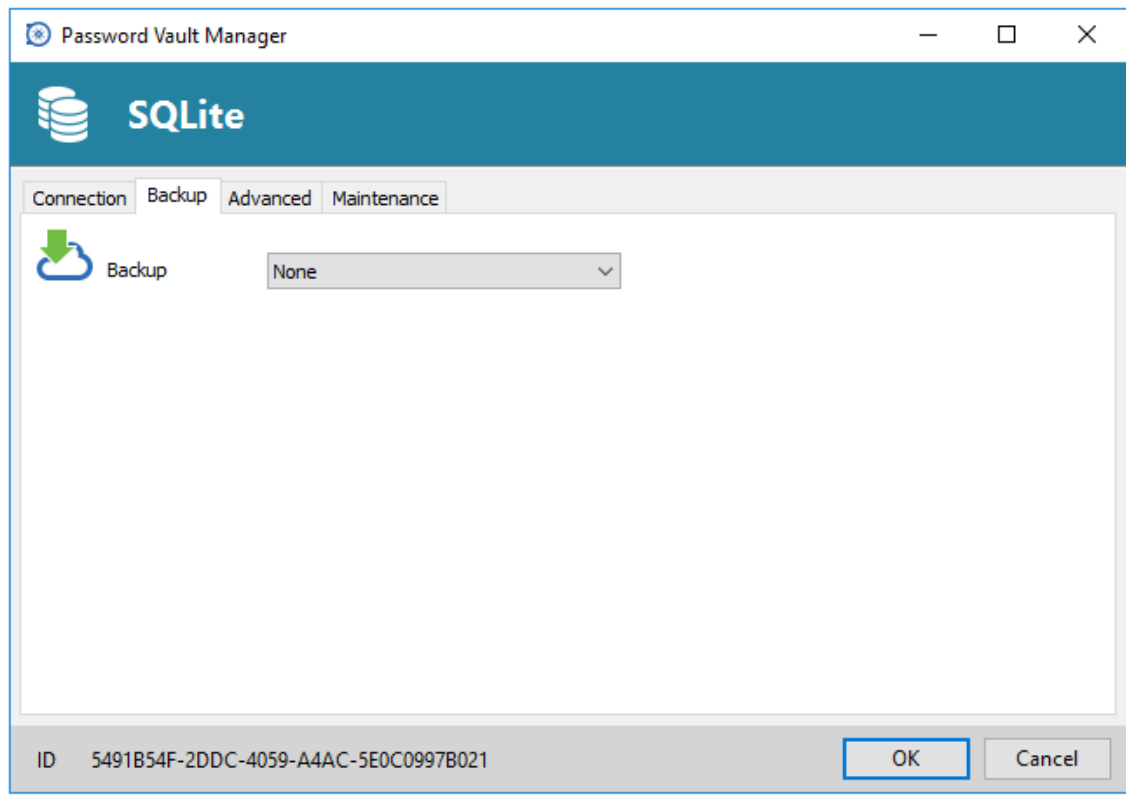
Connection



SQLite- Connection tab

Option	Description
Name	Name of the data source.
Database	Indicates the filename of the SQLite database (.db).
Password	Password used to access the data source.
Always ask password	Always ask for the password when connecting to the data source.
Two factor	Enable the 2-Factor Authentication to access your data source.

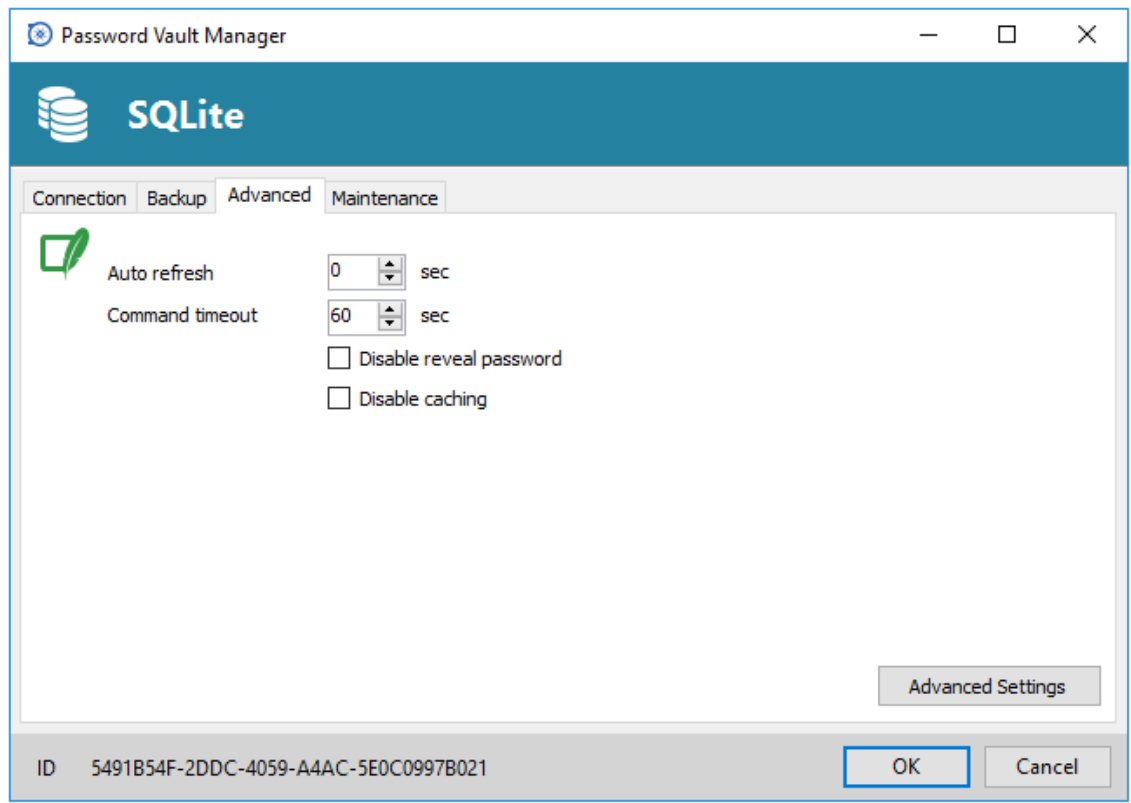
Backup



SQLite - Backup

Option	Description
Backup	Select between: <ul style="list-style-type: none"> • None: No data source backup will be created. • Online Backup: An Online Backup (using Online Backup Service) will automatically be created. • Save to file: Your backup will be saved to a chosen file but will not automatically proceed with a backup every 30 seconds.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and easily restore it if encountering any issues.

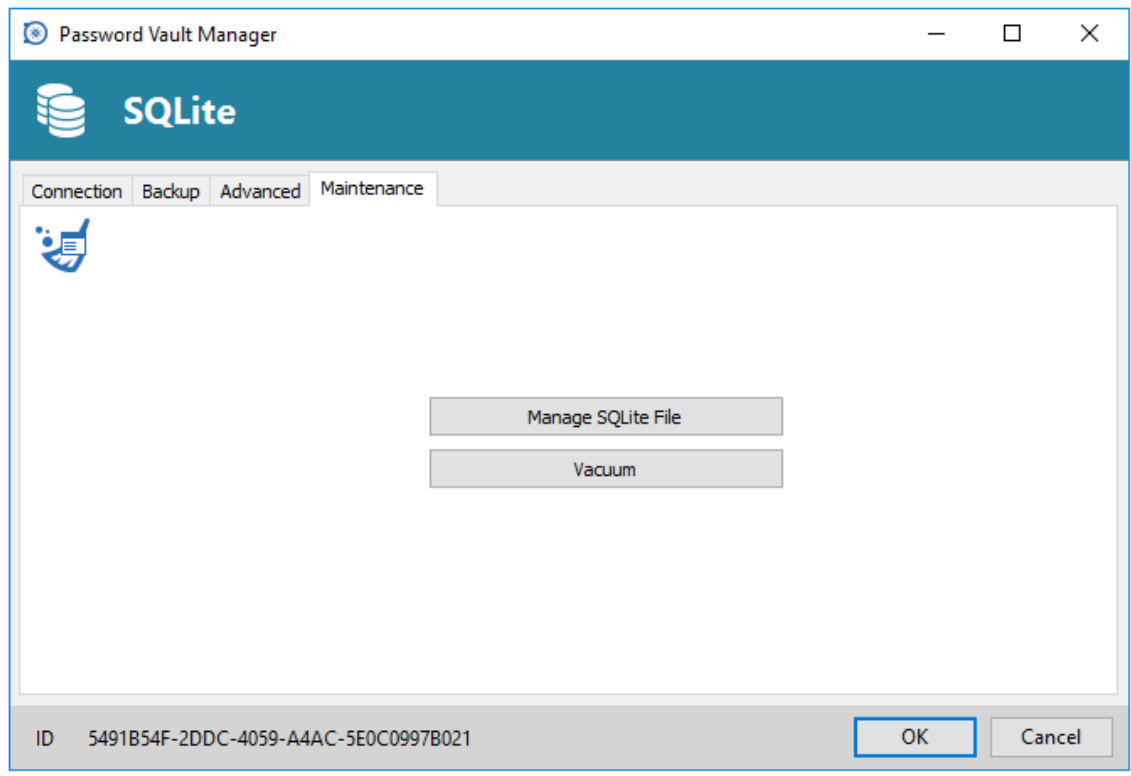
Advanced



SQLite - Advanced tab

Option	Description
Auto refresh	Set the interval for the automatic refresh.
Command timeout	Waiting time before a command timeout.
Disable reveal password	Disable the reveal password feature when a user access this data source.
Disable caching	Entries will be reloaded in Simple mode in the data source.
Advanced Settings	Use to directly modify the connection string value.

Maintenance



SQLite - Maintenance tab

Option	Description
Manage SQLite File	Allows you to analyze, clean or repair your SQLite file.
Vacuum	Used to compress and clean up the current database file.

4.1.9 Web

Description



Password Vault Manager reads the session settings directly from a file located on a web site.

Highlights

- This read-only data source can be shared over the Internet between multiple users
- This is a file-based data source, based on the XML data source
- Supports Windows authentication in IIS

Settings

Connection

Web - Connection tab

Option	Description
Name	Enter the data source name.
URL filename	Indicate the web location of the data source and the name of data source file.
Username	Username used to access the data source.
Password	Password used to access the data source.

4.1.10 XML

Description



Password Vault Manager saves the settings directly in a file with the XML format.

Highlights

- This is a very simple data source and it can be modified or generated by an external tool
- It's possible to configure auto refresh and share the file on a network share
- There is no locking mechanism -- therefore only one user at the time should modify the list
- This is a good replacement for the Access data source, or for users who have problems with their MDAC driver (Microsoft Access database connector)

- The [Online Backup](#) service is available for this data source



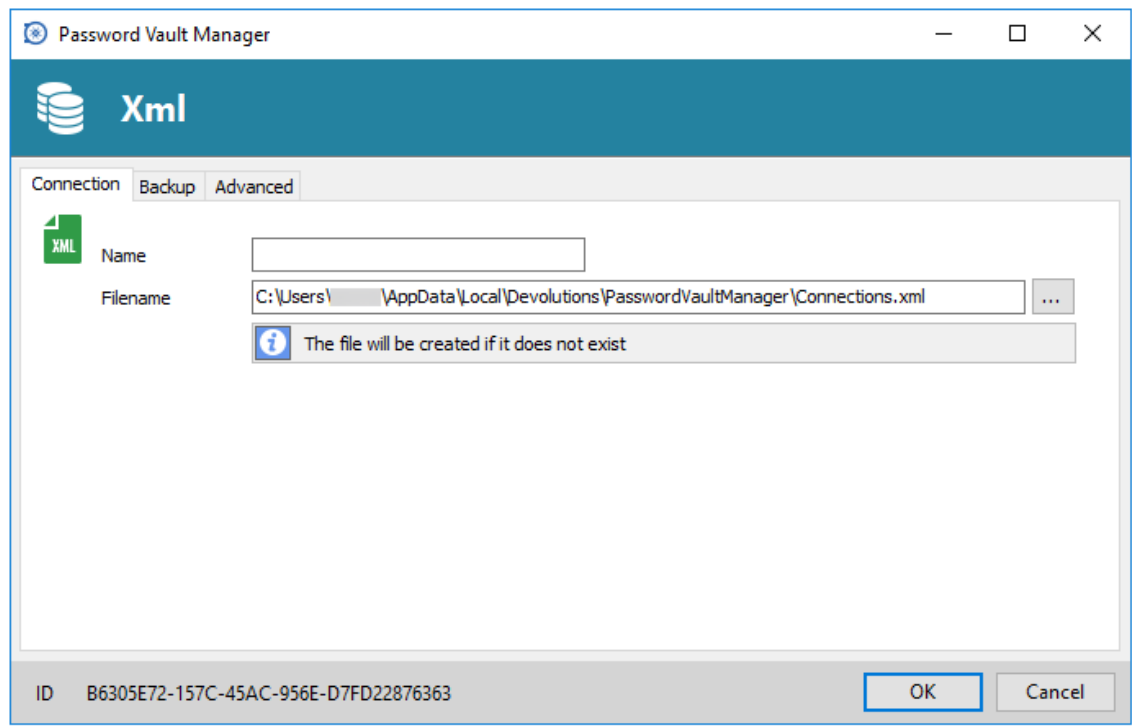
All passwords are encrypted by default. You can specify a custom password (master key) to fully encrypt the content of the file.



It's impossible to recover the data if the master key is lost. Please make sure to remember or backup the master key in a safe place.

Settings

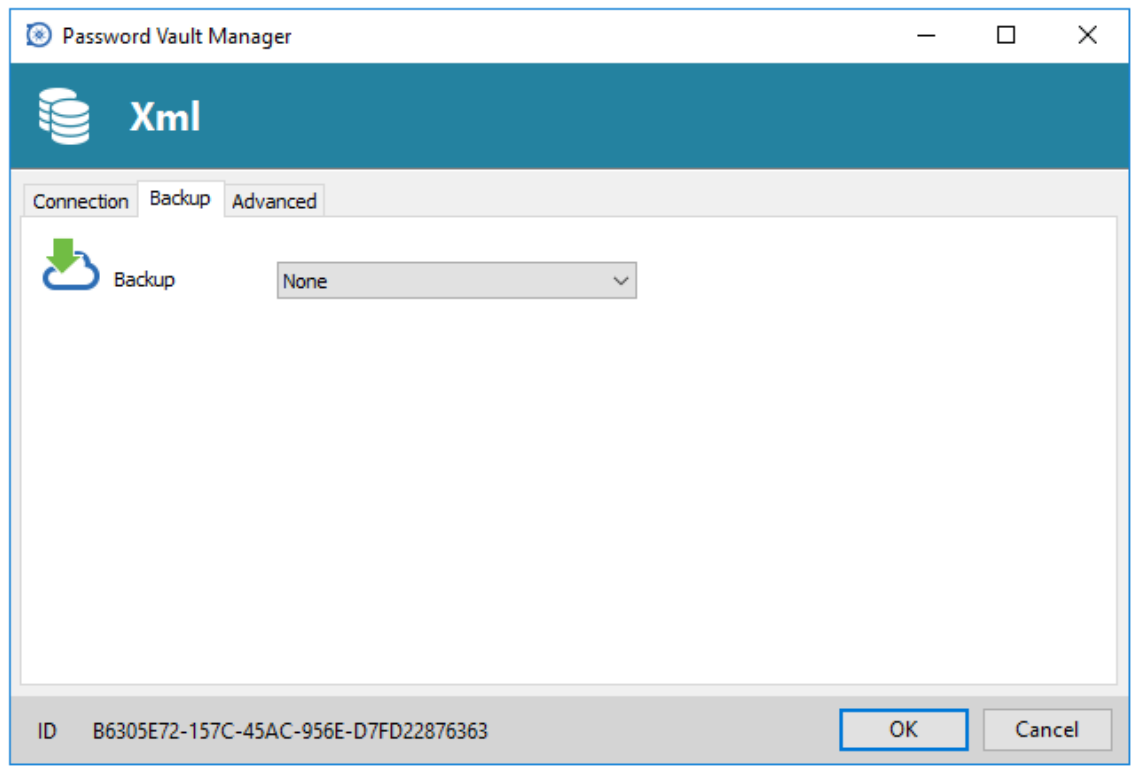
Connection



Xml - Connection tab

Option	Description
Name	Name of the data source.
Filename	Specify the full path of the XML file used to save the data. Relative paths and environment variables can be used as well.

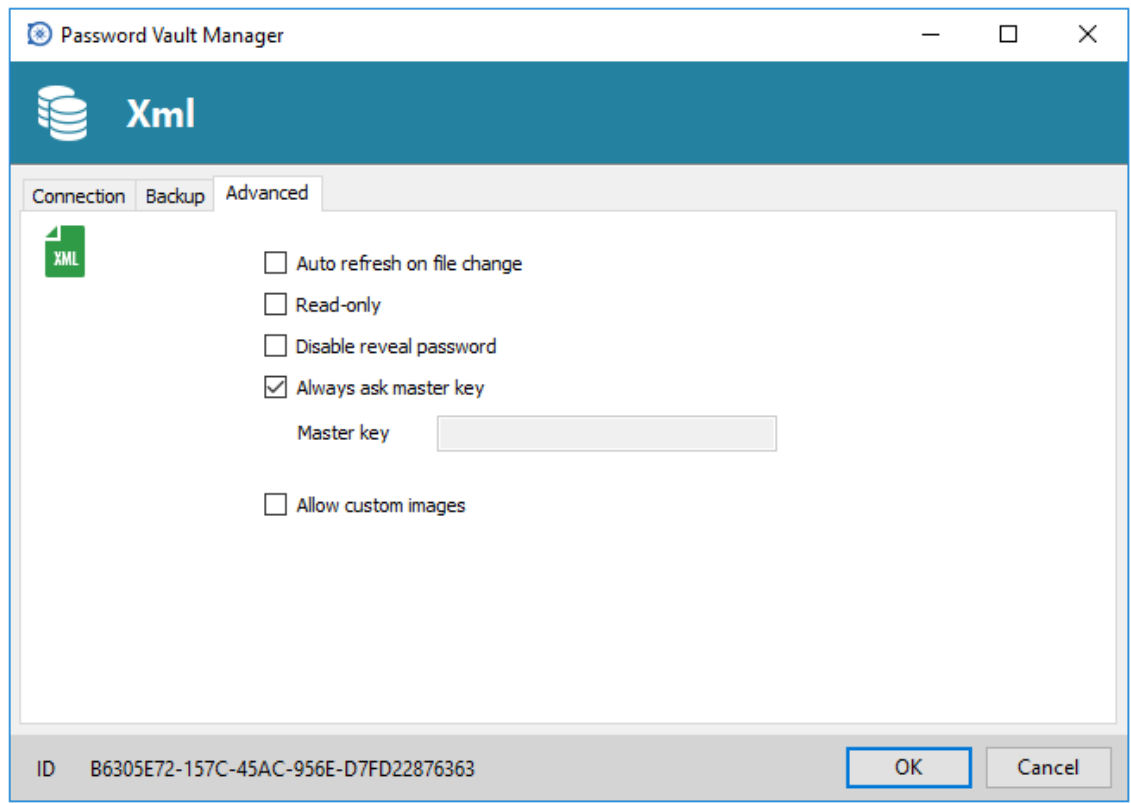
Backup



Xml - Backup tab

Option	Description
Backup	Select between: <ul style="list-style-type: none"> • None: No backup of your data source will be created. • Online Backup: An Online Backup (using Online Backup Service) will automatically be created. • Save to file: Your backup will be saved to a chosen file but will not automatically do backup every 30 seconds.
Backup name	Specify the backup name that will allow you to automatically save your sessions in a safe online storage space and restore them in the event of problems.

Advanced



Xml - Advanced tab

Option	Description
Auto refresh on file change	Indicate if the application monitor the file changes to automatically refresh the data source.
Read-only	Set the data source in read only. No new entry can be created and the existing data cannot be edit.
Disable reveal password	Disable the reveal password feature when a user accesses this data source.
Always ask master key	Always ask the Master key before opening the data source. This is used to encrypt the XML content and it could not be recovered if lost.
Master key	Enter the Master key that will be used before opening the data source.
Allow custom images	This will enable the loading of any custom images in the tree view.

4.1.11 Advanced Data Sources

Description

Advanced Data Sources are typically running on an advanced management system, either a Database Management System or our own Online Services.

This allows Password Vault Manager to support these features:

- Document uploads and Entry Attachments
- Audit and logging
- Advanced security with [User Management](#) and [Security Group Management](#)
- [Offline Mode](#)
- [2-Factor Authentication](#)



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Currently the Advanced Data Sources are:

- [Devolutions Server](#)
- [MariaDB](#)
- [MySQL](#)
- [Online Database \(Only the Professional and Enterprise subscriptions levels\)](#)
- [SQL Azure](#)
- [SQL Server \(MSSQL\)](#)

4.1.11.1 Devolutions Server

Description



Devolutions Server is a self-hosted repository for storing and sharing your remote connections and credentials. You can find more information on the product's web site [here](#).

Highlights

- High-end security server for your company
- Share your sessions with multiple users
- Can be deployed online
- Support Windows authentication and Active Directory group integration
- Client and server side caching optimization
- Requires the Remote Desktop Manager Enterprise client (included with the server license)



Devolutions Server supports only SQL Server as a data store at this time.

For more information, please consult these topics:

- [Devolutions Server installation instructions](#)
- [Devolutions Server Security Checklist](#)
- [Devolutions Server Automatic Account Creation](#)

Configure the server data source on all your client machines.

Enter a name of the data source and the URL for the server. Ensure you use the correct protocol if SSL is required by the server (https).

Alternatively, you can export the data source information and then import the file in your client workstations as described [Import/Export Data Source](#).

Settings

Connection

The screenshot shows a window titled "Password Vault Manager" with a sub-header "Devolutions Server". Below this, there are two tabs: "Connection" and "Advanced". The "Connection" tab is selected. It contains a green folder icon and the following fields:

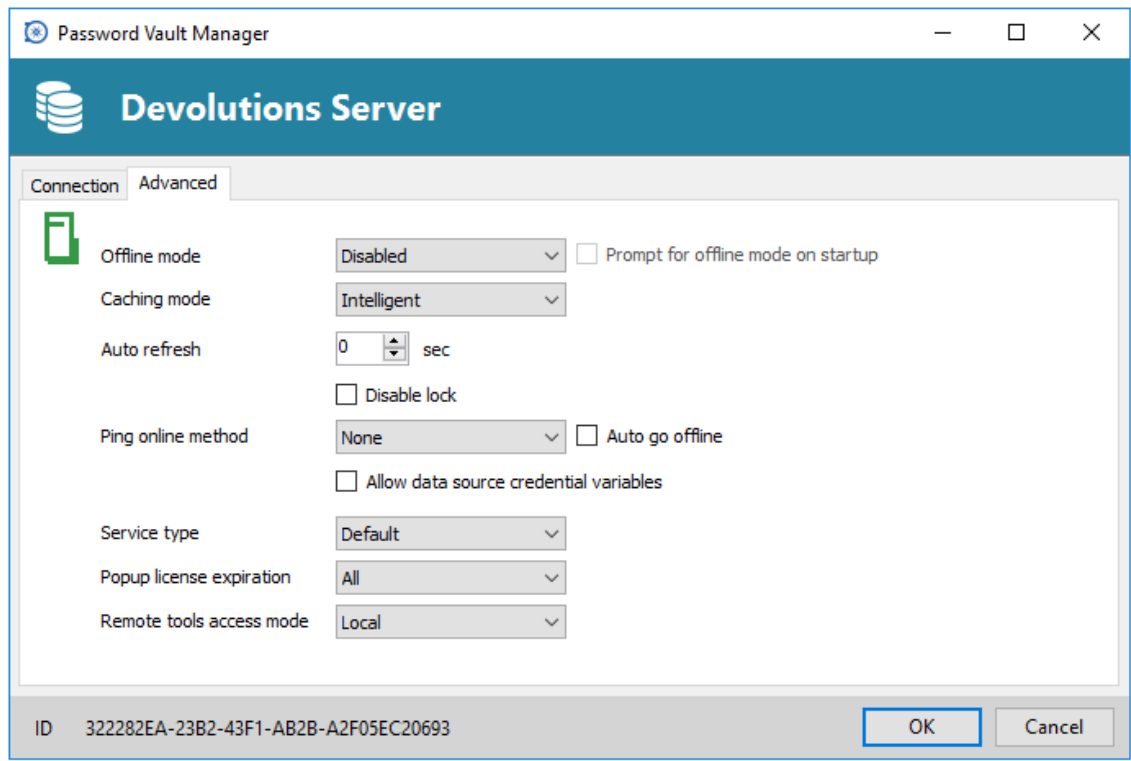
- Name:** A text box containing "DevServer".
- Server:** A dropdown menu showing "http://127..." with a globe icon to its right.
- Username:** A text box with a dropdown arrow, and a checkbox labeled "Always ask username".
- Password:** A text box with a dropdown arrow, and a checkbox labeled "Always ask password".

Below these fields is a blue link labeled "Test Connection". At the bottom of the dialog, there is an ID field containing "322282EA-23B2-43F1-AB2B-A2F05EC20693" and two buttons: "OK" and "Cancel".

Devolutions Server - Connection

Option	Description
Name	Name of the data source.
Server	Name of the Devolutions Server instance.
Username	Username to connect to the data source.
Password	Password to connect to the data source.
Always ask username	Always ask for the username when connecting to the data source.
Always ask password	Always ask for the password when connecting to the data source.
Test Connection	Test the connection with Devolutions Server to validate if the proper information has been provided.

Advanced



Devolutions Server - Advanced

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode . In Offline Mode , the data source can be available in Read Only or in Read/Write mode. Please consult Offline Read/Write topic for more information.
Prompt for offline mode on startup	Every time you will connect on your data source, you will be prompt to use the data source in offline mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh.
Disable lock	Disable the option to lock the data source.
Ping online method	Indicate the prefer ping online method. Select between: <ul style="list-style-type: none"> • None • Web request
Auto go offline	If the ping online method doesn't work it will automatically go offline.
Allow data source credential variables	Allow to use the data source credential to be use in variables.
Service type	Indicate the prefer Service type. Select between: <ul style="list-style-type: none"> • Default • Web API Client • Web service client
Popup license expiration	Determine how the application will advise you of the license expiration. Select between: <ul style="list-style-type: none"> • All

	<ul style="list-style-type: none"> • Disabled • Only Administrator(s)
Remote management mode	Remote Management mode. Select between: <ul style="list-style-type: none"> • Local • Via data source

4.1.11.2 MariaDB

Description



Password Vault Manager uses MariaDB as a drop-in replacement for MySQL. It is only supported in the Enterprise edition.

Highlights

- The data can be shared on a MariaDB database installed on any Operating System MySQL supports
- Full connection log and attachments support
- Integrated Security support.

Settings

Connection

The screenshot shows the 'MariaDB' connection configuration window in Password Vault Manager. The window has a title bar with the application name and standard window controls. Below the title bar is a blue header with the MariaDB logo and name. The main area contains several input fields and checkboxes:

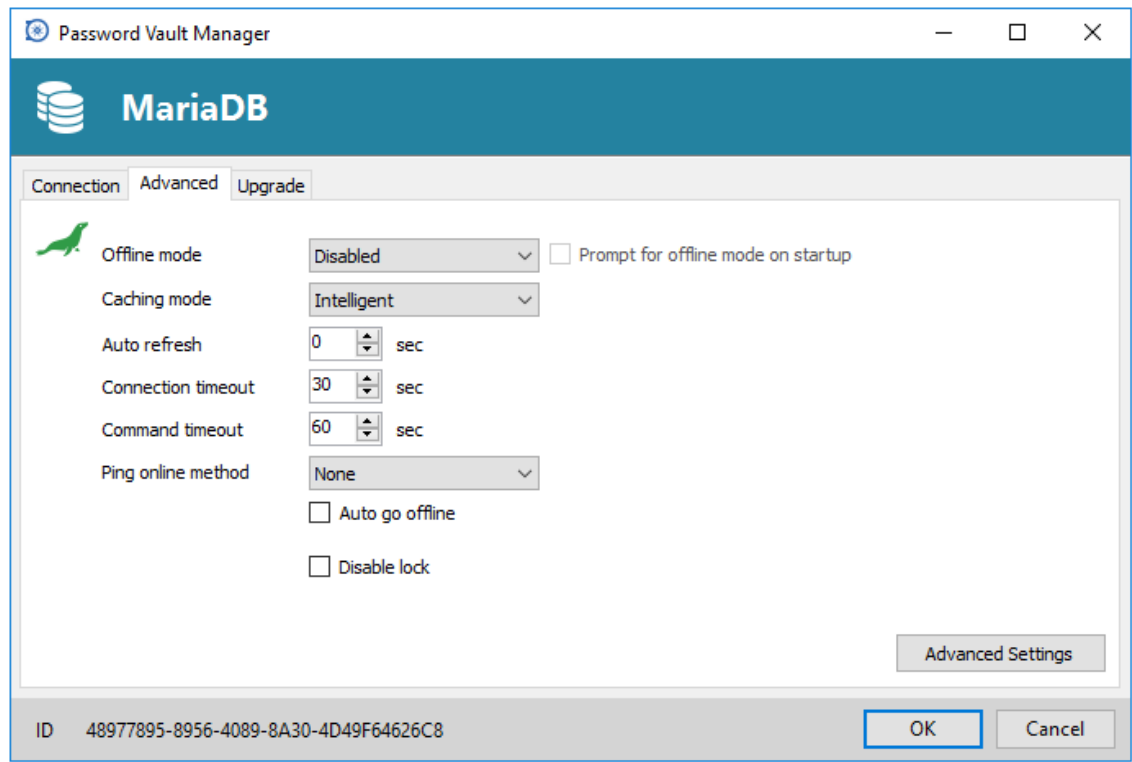
- Name:** MariaDB
- Host name:** (empty text box)
- Port:** 3306 (spin box)
- User:** (empty text box) with an Editable checkbox.
- Save password:**
- Password:** (empty text box)
- Schema:** (empty text box) with a dropdown arrow.
- Two factor:** [None](#)

At the bottom right, there are buttons for 'Test Host', 'Test Schema', 'OK', and 'Cancel'. At the bottom left, there is an ID field containing the value '48977895-8956-4089-8A30-4D49F64626C8'.

MariaDB - Connection tab

Option	Description
Name	Name of the data source.
Host name	Name of the host (server name) where the data source will be stored.
User	Username used to access the host server.
Password	Password used to access the host server.
Schema	Name of the schema (database) on the server.
Test Host	Test the connection with the host (server name) to validate if the proper information has been provided.
Test Schema	Test the connection with the schema to validate if the proper information has been provided.
Two factor	Enable the 2-Factor Authentication to access your data source.

Advanced

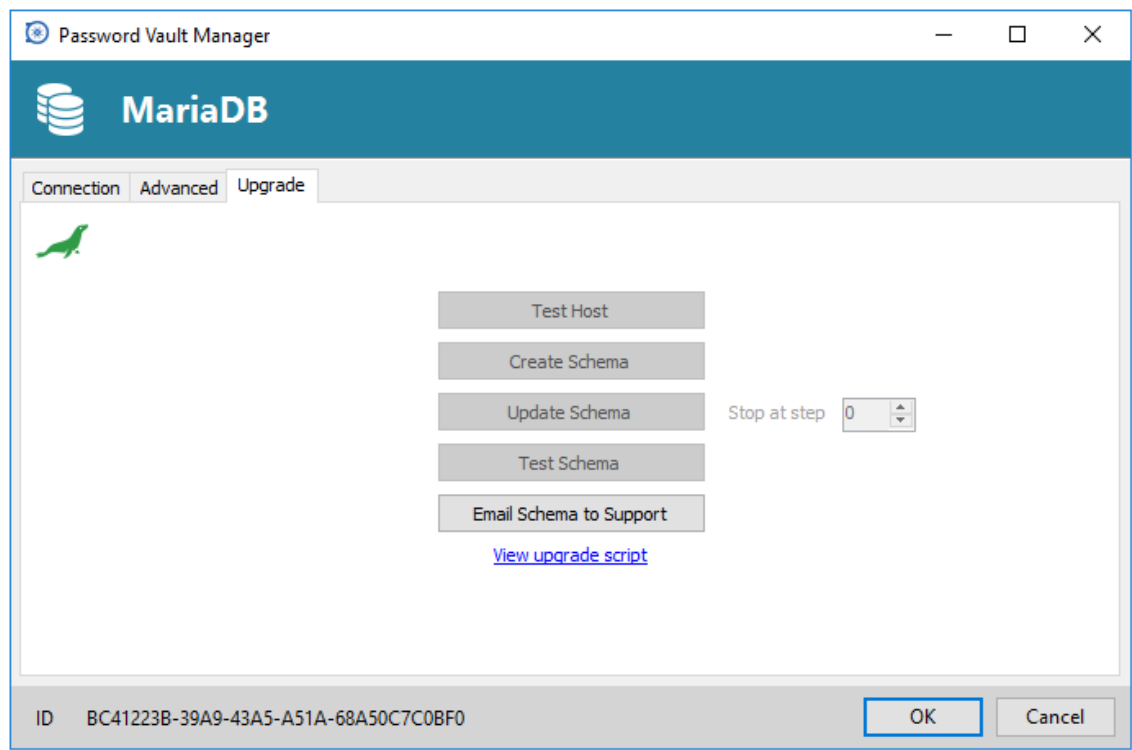


MariaDB - Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode . With this mode, the data source can be available in Read Only or in Read/Write mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh

Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> • None • Port Scan
Auto go offline	If the ping online method doesn't work it will automatically go offline.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.
Advanced Settings	Directly edit the connection string values.

Upgrade



MariaDB - Upgrade tab

Option	Description
Test Host	Test the connection with the Host (server name) to validate if the proper information has been provided.
Create Schema	Create the schema (database) on the MariaDB server to use Password Vault Manager.
Update Schema	Update the schema (database) on the MariaDB server, if required, to use Password Vault Manager.

Test Schema	Test the connection with the schema (database) to validate if the proper information has been provided.
Email Schema to Support	Send your schema (database) to the Devolutions Support team.

4.1.11.3 MySQL

Description



Password Vault Manager uses a MySQL database to store the session data. It is only supported in the Enterprise edition.

Highlights

- The data can be shared on a MySQL database installed on any Operating System MySQL supports.
- Full connection log and attachment support.
- Integrated Security support. (Requires a v5.5.16 commercial distribution of MySQL).

Settings

Connection

MySQL

Connection Advanced Upgrade

Name MySQL

Host name Port 3306

Integrated security (Active Directory)

User Editable

Save password

Password

Schema ...

Two factor [None](#)

Test Host

Test Schema

ID 09DC90A8-EDB3-4527-977F-AF03066378E4

OK Cancel

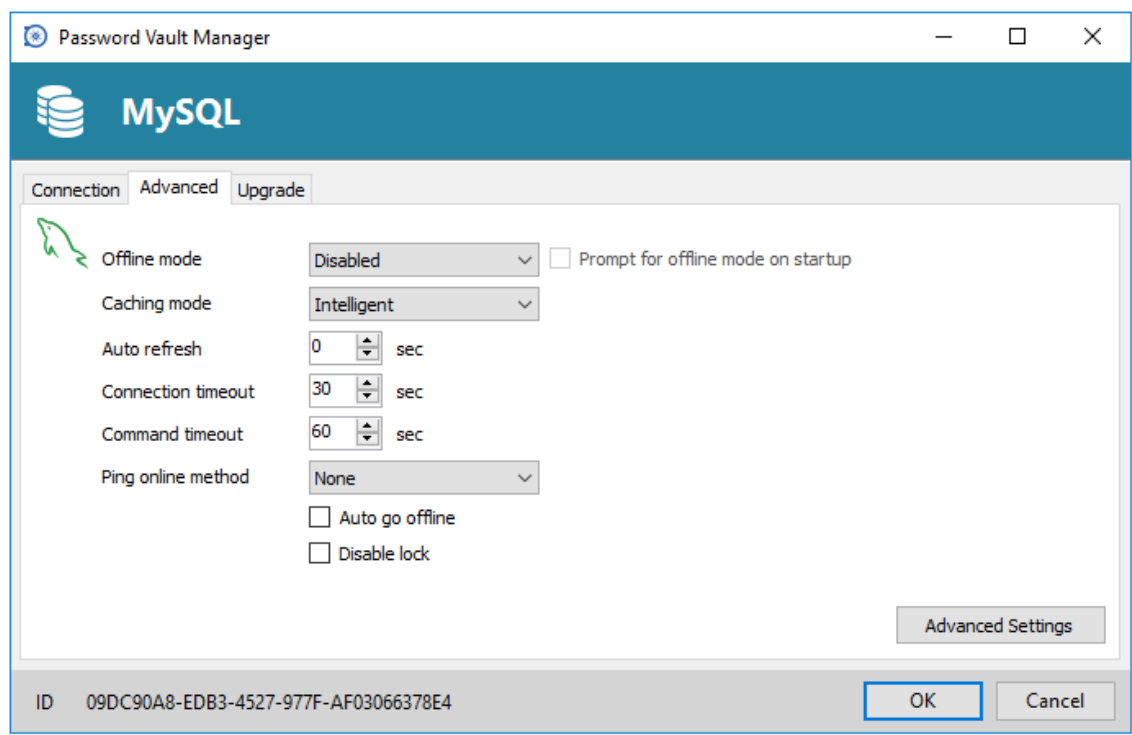
Requires: v5.5.16 commercial distributions of MySQL

MySQL - Connection tab

Option	Description
--------	-------------

Name	Name of the data source.
Host name	Name of the server where the data source will be store.
Integrated security (Active Directory)	Specify to use Windows Integrated Authentication for authenticating to the data source. Applies only to SQL Server and RDMS, depending on their configuration. When checked, an ellipsis button appears to allow you to browse for the user account in the directory. Consult Integrated Security topic for more information.
User	Username to access the MySQL server.
Password	Password to access the MySQL server.
Schema	Name of the schema on the MySQL server for the utilization of Password Vault Manager.
Two factor	Enable the 2-Factor Authentication to access your data source.
Test Host	Test the connection with the Host (server) to validate if the proper information has been provided.
Test Schema	Test the connection with the schema to validate if the proper information has been provided

Advanced

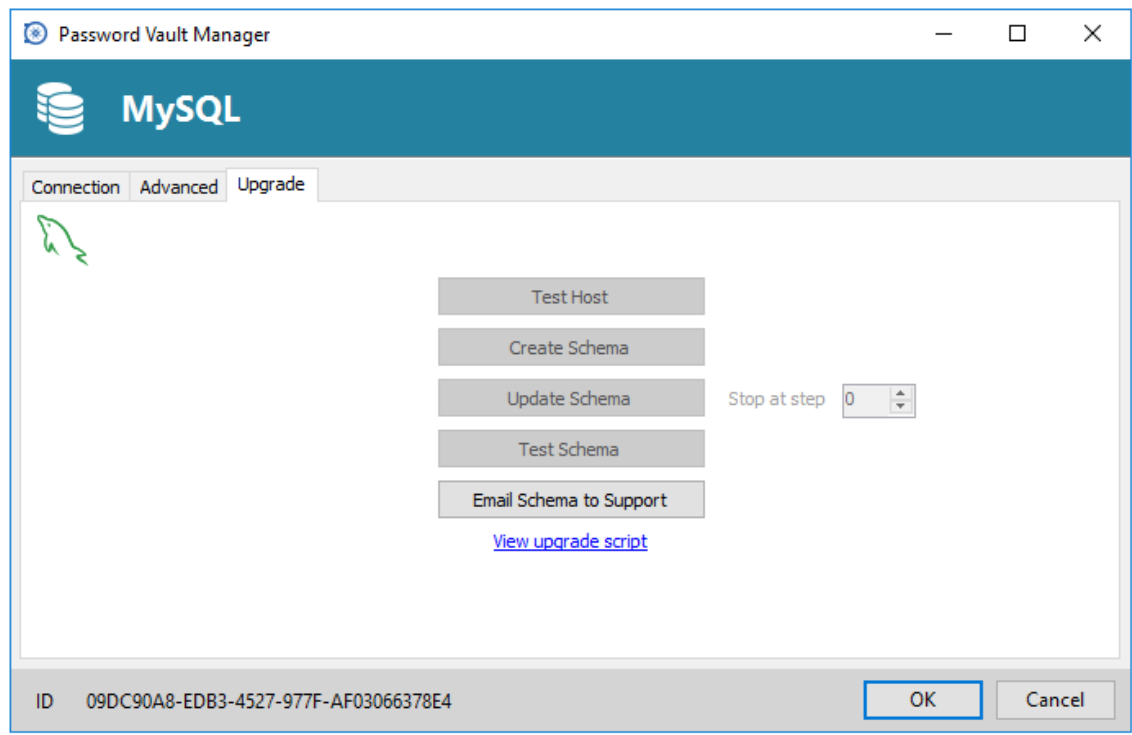


MySQL - Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode . In this mode, the data source can be available in Read Only or in Read/Write mode.
Prompt for offline mode on startup	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.

Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh.
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> • None • Port Scan
Auto go offline	If the ping online method doesn't respond it will automatically go offline.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.
Advanced Settings	Edit the connection string values directly.

Upgrade



MySQL - Upgrade tab

Option	Description
Test Host	Test the connection with the host (server) to validate if the proper information has been provided.
Create Schema	Create the schema on the MySQL server to use.
Update Schema	Update the schema on the MySQL server, if required, to use.
Test Schema	Test the connection with the schema to validate if the proper information has been provided.

Email Schema to Support	Send your schema to the Devolutions Support team.
-------------------------	---

4.1.11.4 Devolutions Online Database

Description



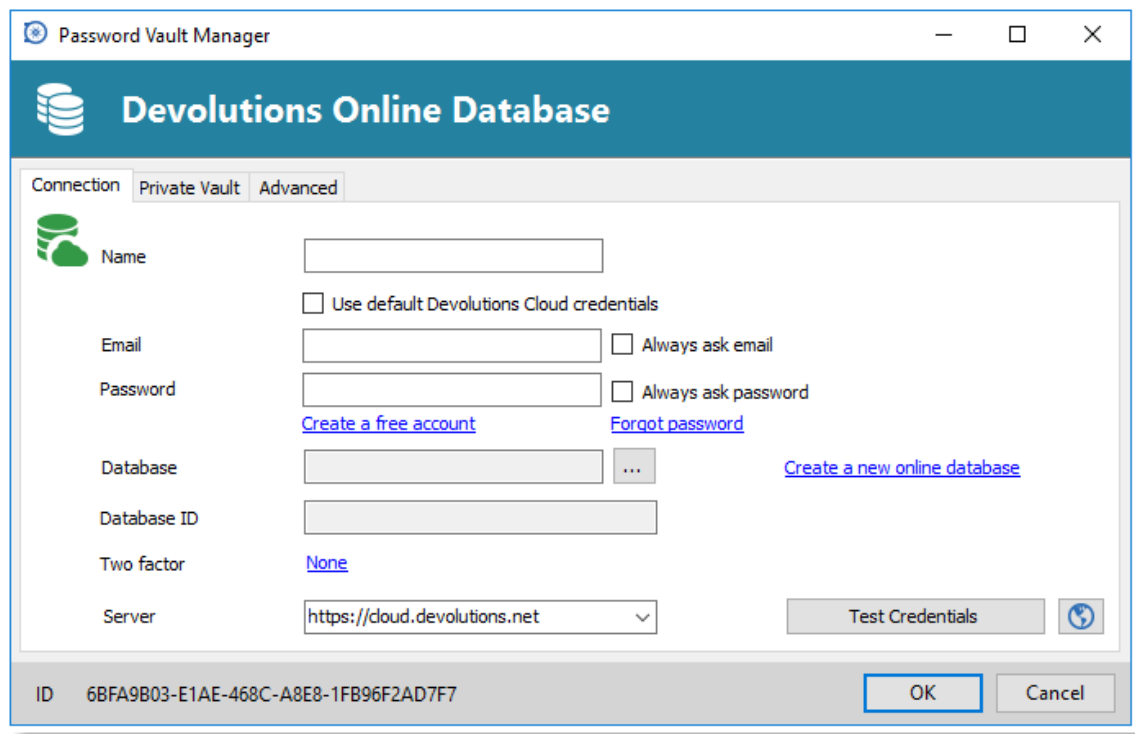
Remote Desktop Manager Online is a hosted repository managed by Devolutions. The Password Vault Manager client connects directly to the data source. For details on this service, please visit <https://online.remotedesktopmanager.com>.

Highlights

- No VPN required to access the data
- Full connection logs
- Hosted on Microsoft Windows Azure and Microsoft SQL Azure
- This data source allows user management with security groups
- The offline mode can be used when the server is unavailable, or when the user is on the road

Settings

Connection

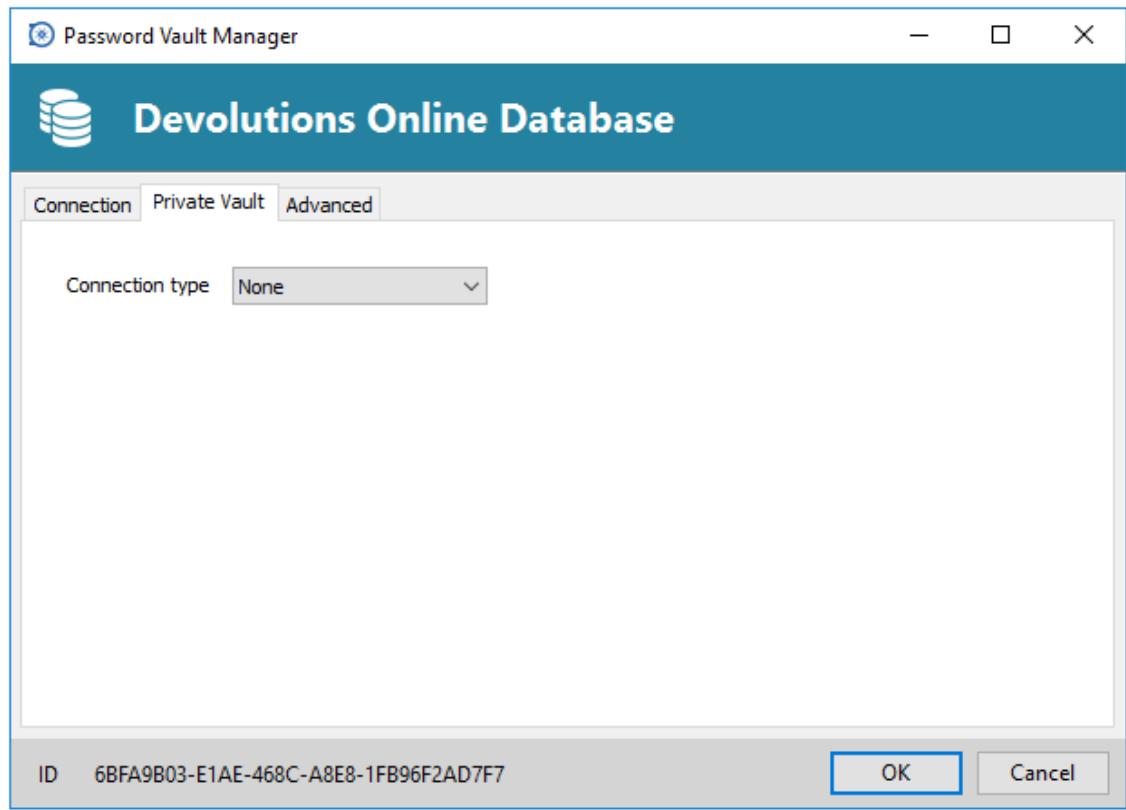


Devolutions Online Database - Connection tab

Option	Description
Name	Name of the data source.

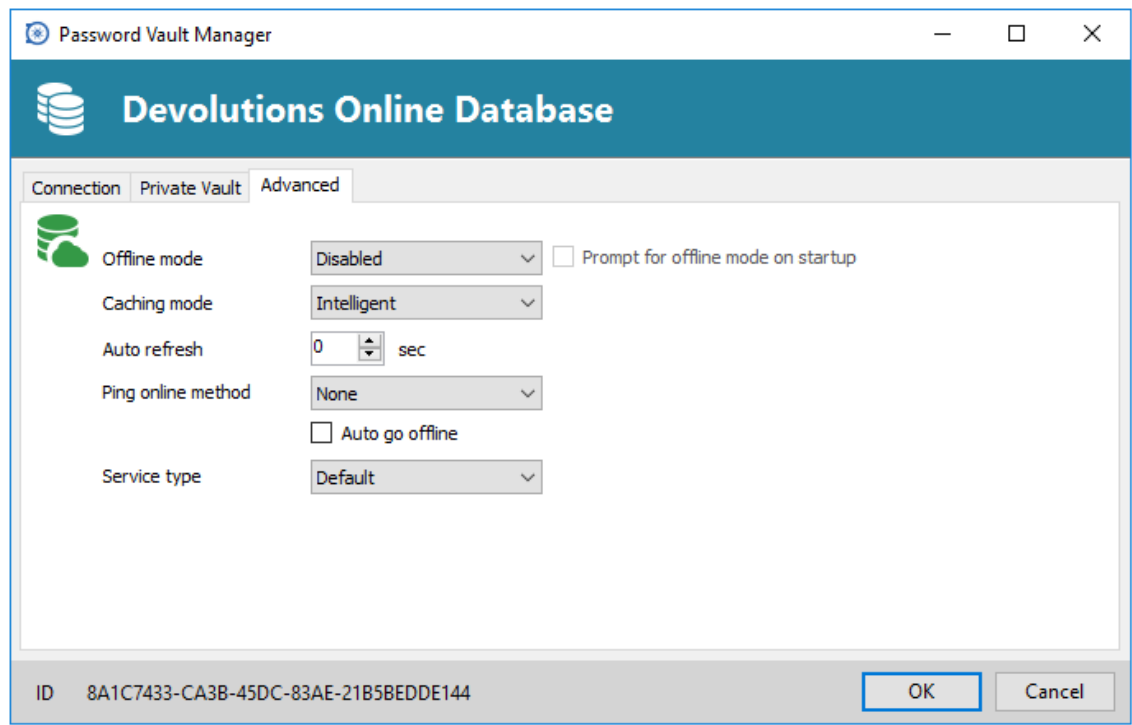
Email	Email address used to connect online.
Always ask email	Always ask for email when connecting to the data source.
Create a new account	Create a new Devolutions Cloud account.
Password	Password to connect to the data source.
Always ask password	Always ask for password when connecting to the data source.
Database	Name of the data source created online. You must use the ellipsis button to select it from the list of online data sources available to the entered email.
Create a new data source online	Create a new Password Vault Manager Online data source.
Database ID	Unique Key to identify the data source.
Two factor	Enable the 2-Factor Authentication to access your data source.
Test Credentials	Test the credentials that you have configured to connect on Password Vault Manager Online.

Private Vault



Devolutions Online Database - Private Vault tab

Option	Description
Connection type	The content of the Private Vault will be saved in a Online Drive file instead of directly in the database. Select between: <ul style="list-style-type: none"> • None • Online Drive

Advanced**Devolutions Online Database - Advanced**

Option	Description
Offline mode	Determine if you want to use this data source in offline mode. In offline mode, the data source can be available in Read Only or in Read/Write mode. Consult Offline Mode topic for more information.
Prompt for offline mode on startup	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Auto refresh	Set the interval for the automatic refresh.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> • None • Web request
Auto go offline	If the ping online method doesn't work it will automatically go offline.
Service Type	Indicate the preferred Service type. Select between: <ul style="list-style-type: none"> • Default • Web API Client • Web service client

4.1.11.4.1 Activate Subscription (Register)

Description

Please consult topic [Online Database Subscription Activation](#) for information on this service.

4.1.11.4.2 Activate Online Data Source Trial

Description

Please consult topic [Online Database Trial Subscription Activation](#) for information on this service.

4.1.11.5 SQL Azure

Description



Password Vault Manager uses the Microsoft's cloud platform to save and manage all sessions.

We also support the following features:

- ***Always on availability group***
- ***Clustering***
- ***Log Shipping***
- ***Database mirroring***

Highlights

- This data source allows user management with a superior security model
- The [Offline Mode](#) can be used when the server is unavailable, or when the user is on the road
- Full connection log and attachment support
- The data source supports an auto refresh at your preferred interval
- Microsoft SQL Azure can be used to create an online database. Get more detail on SQL Azure [here](#)



A proper database backup strategy should be implemented to minimize possible data loss.

Settings

Connection

The screenshot shows the 'Microsoft SQL Azure' connection configuration window in Password Vault Manager. The window title is 'Password Vault Manager' and the subtitle is 'Microsoft SQL Azure'. The 'Connection' tab is selected, showing the following fields and options:

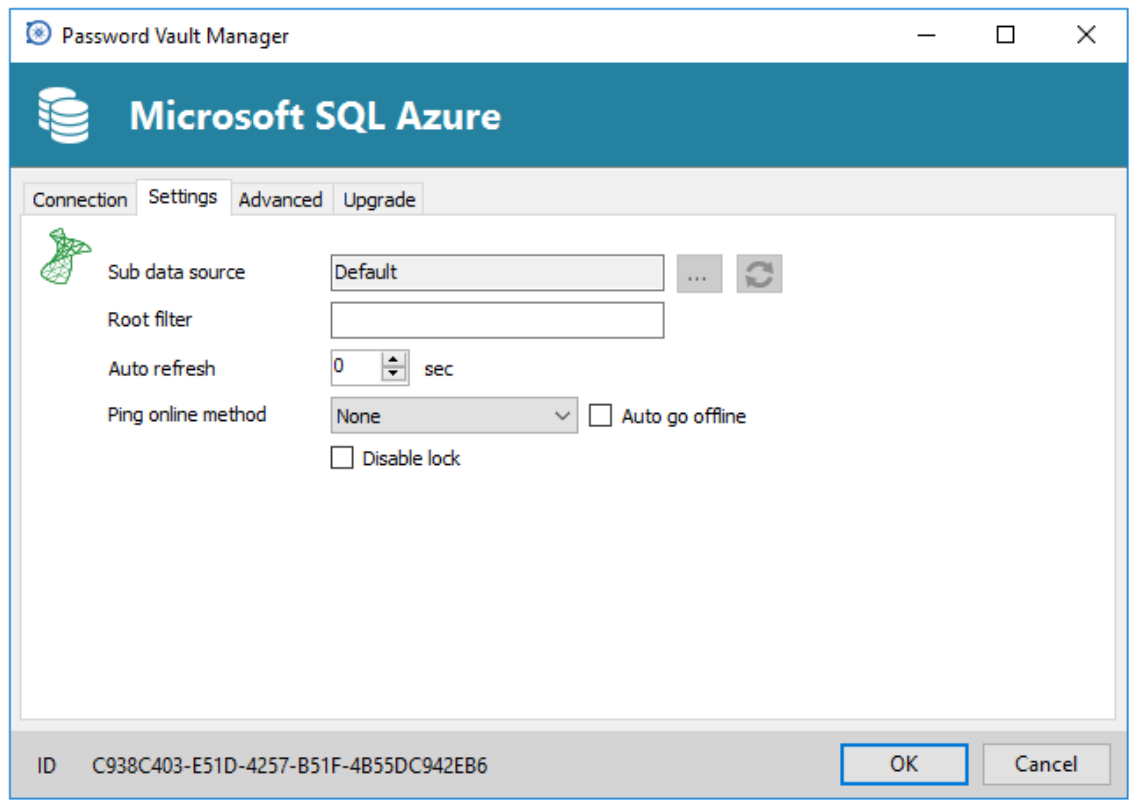
- Name:** SQL Azure
- Server:** SQL Azure (dropdown menu)
- User:** (text input field)
- Password:** (text input field)
- Database:** (text input field)
- Two factor:** None
- Integrated security (Active Directory)
- Save password
- Editable

Buttons include 'Test Database', 'OK', and 'Cancel'. The ID is C938C403-E51D-4257-B51F-4B55DC942EB6.

SQL Azure - Connection tab

Option	Description
Name	Name of the data source.
Server	Name of the server where the data source will be store.
Integrated security (Active Directory)	Specify to use Windows Integrated Authentication for authenticating to the data source. When checked, an ellipsis button appears to allow you to browse for the user account in the directory. Consult Integrated Security topic for more information.
User	Username to access the SQL server.
Password	Password used to access the SQL server.
Database	Name of the database on the SQL server for the utilization of Password Vault Manager.
Test Server	Test the connection with the server to validate if the proper information has been provided.
Two factor	Enable the 2-Factor Authentication to access your data source.
Test Database	Test the connection with the database to validate if the proper information has been provided.

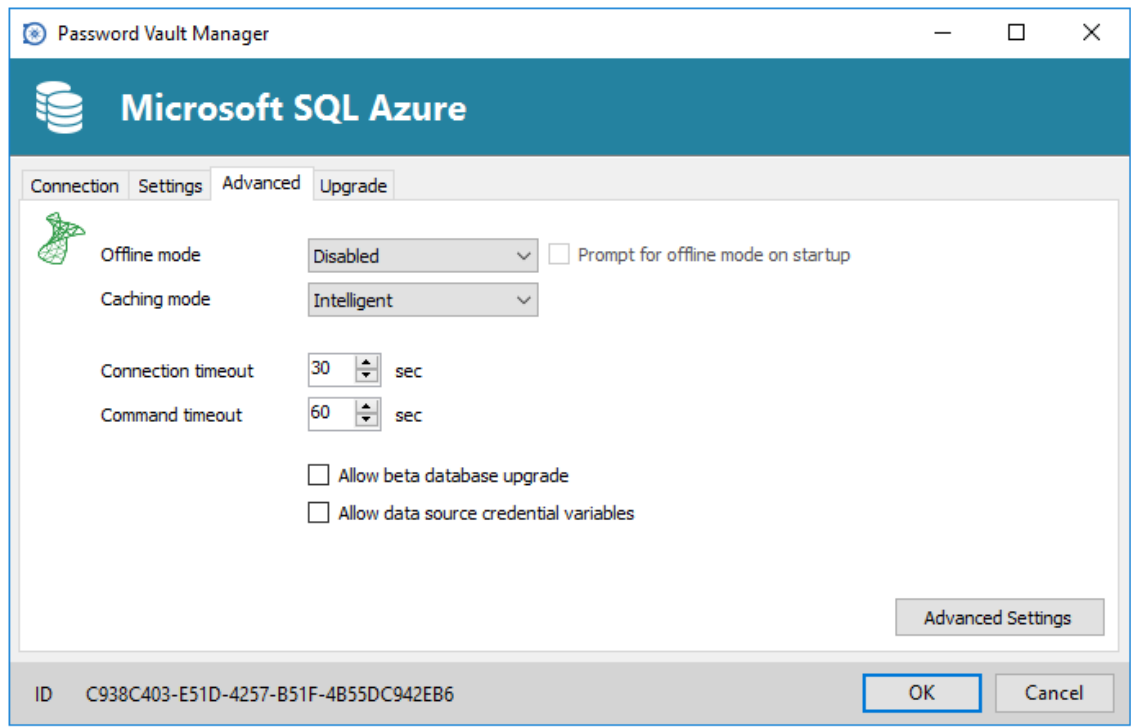
Settings



SQL Azure - Settings tab

Option	Description
Root filter	Enter your SQL Azure root filter.
Auto refresh	Set the interval for the automatic refresh.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> • None • Port Scan
Auto go offline	If the ping online method doesn't respond it will automatically go offline.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.

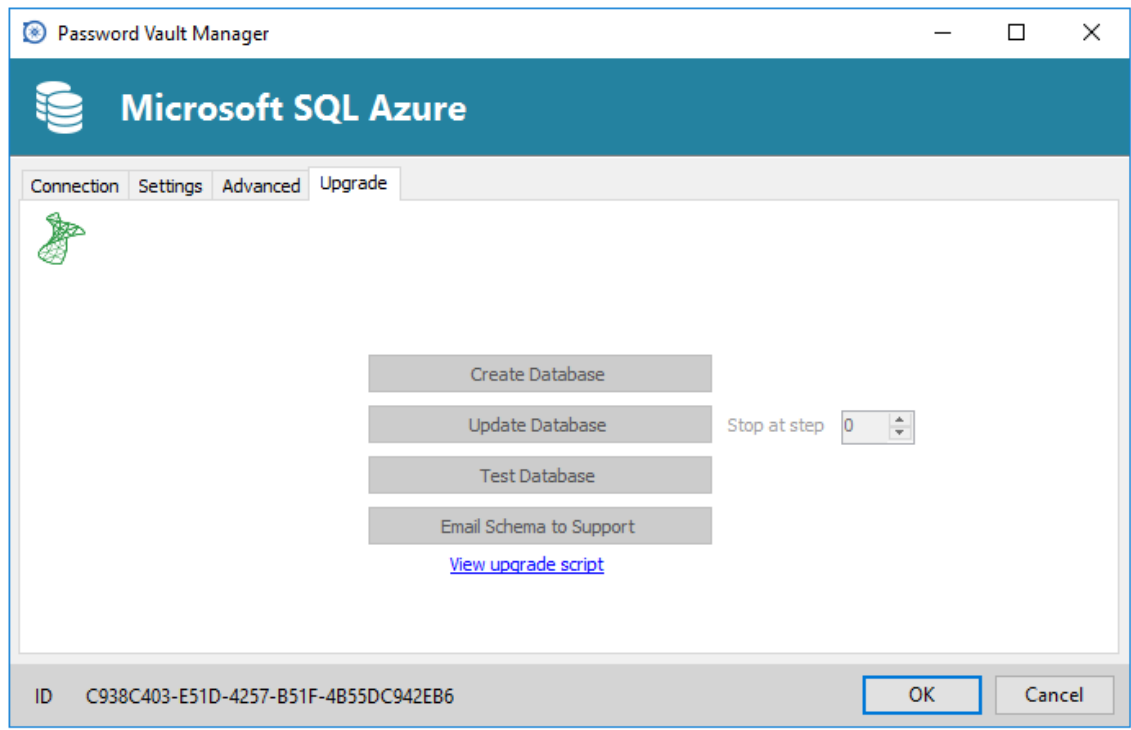
Advanced



SQL Azure - Advanced tab

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode . With this mode, the data source can be available in Read Only or in Read/Write mode
Prompt for offline mode on startup	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Allow beta database upgrade	If an upgrade is required and you are using a beta version and database, it will authorize you to upgrade it.
Allow data source credential variables	Allow to use the data source credential to be use in variables.
Advanced Settings	Edit of the connection string values directly.

Upgrade



SQL Azure - Upgrade tab

Option	Description
Create Database	Create the database on the SQL server to use Password Vault Manager.
Update Database	Update the database on the SQL server, if required to use Password Vault Manager.
Test Database	Test the connection with the database to validate if the proper information has been provided.
Email Schema to Support	Send your schema to the Devolutions Support team.

4.1.11.6 SQL Server

Description



Password Vault Manager uses the power of Microsoft SQL Server to save and manage all sessions.

SQL Server 2012, Express 2012, 2014 and Express 2014 are supported.

We also support the following features:

- **Always on availability group**
- **Clustering**
- **Log Shipping**
- **Database mirroring**

Highlights

- This data source allows user management with a superior security model
- The [Offline Mode](#) can be used when the server is unavailable, or when the user is on the road
- Full connection log and attachment support
- The data source supports an auto refresh at your preferred interval



A proper database backup strategy should be implemented to minimize possible data loss, please refer to [Backups](#) topic.

Settings

Connection

The screenshot shows the 'Microsoft SQL Server' connection configuration window. It includes the following fields and options:

- Name:** A text input field.
- Server:** A dropdown menu currently set to 'SQL Server', followed by a text input field and a browse button (...). A note '(Local) or IP or Server name' is present.
- Integrated security (Active Directory):** An unchecked checkbox.
- User:** A text input field with an 'Editable' checkbox.
- Save password:** A checked checkbox.
- Password:** A text input field.
- Database:** A text input field with a browse button (...).
- Two factor:** A dropdown menu set to 'None'.

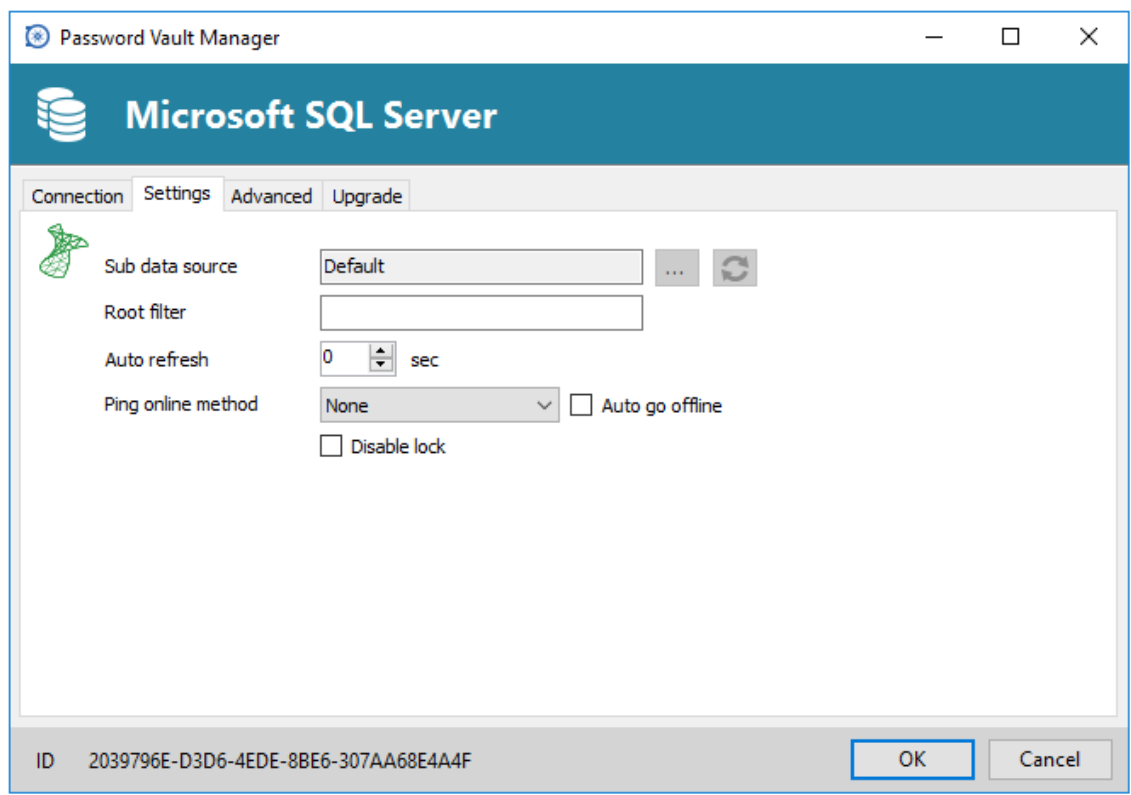
Buttons at the bottom include 'Test Server', 'Test Database', 'OK', and 'Cancel'. An ID field at the bottom left contains the value '2039796E-D3D6-4EDE-8BE6-307AA68E4A4F'.

SQL Server - Connection tab

Option	Description
Name	Name of the data source.
Server	Name of the server where the data source will be store.
Integrated security (Active Directory)	Specify to use Windows Integrated Authentication for authenticating to the data source. When checked, an ellipsis button appears to allow you to browse for the user account in the directory. Consult Integrated Security topic for more information.

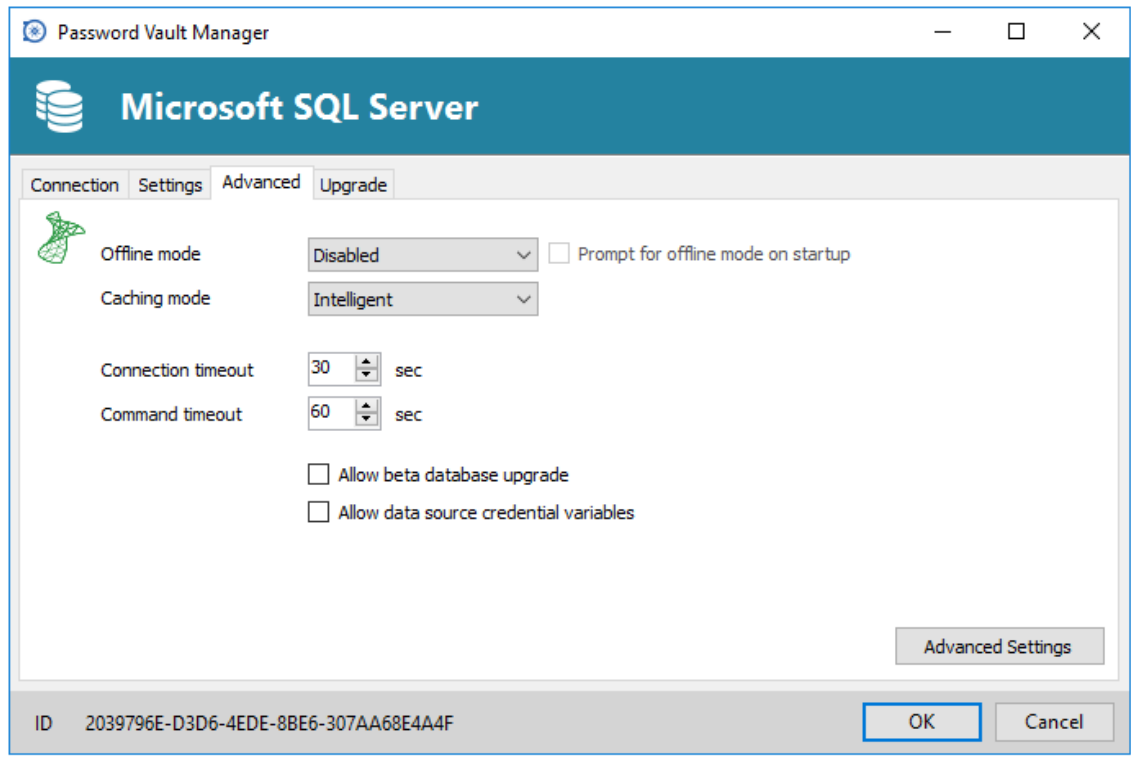
User	Username to access the SQL server.
Password	Password used to access the SQL server.
Database	Name of the database on the SQL server for the utilization of Password Vault Manager.
Test Server	Test the connection with the server to validate if the proper information has been provided.
Two factor	Enable the 2-Factor Authentication to access your data source.
Test Database	Test the connection with the database to validate if the proper information has been provided.

Settings



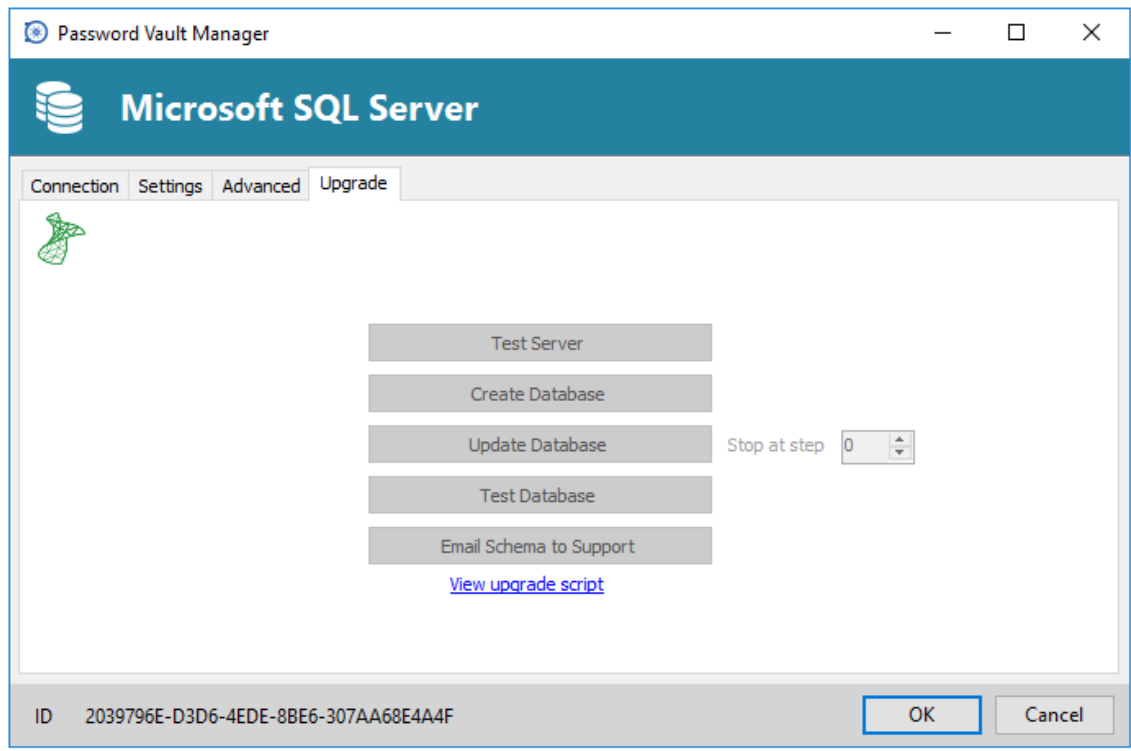
SQL Server - Settings tab

Option	Description
Root filter	
Auto refresh	Set the interval for the automatic refresh.
Ping online method	Indicate the prefer ping online. Select between: <ul style="list-style-type: none"> • None • Port Scan
Auto go offline	If the ping online method doesn't respond it will automatically go offline.
Disable lock	Disable the option to lock the data source directly. You can still lock the application but you won't be prompted for the database password if this option is disabled.

Advanced**SQL Server - Advanced tab**

Option	Description
Offline mode	Determine if you want to use this data source in Offline Mode . With this mode, the data source can be available in Read Only or in Read/Write mode
Prompt for offline mode on startup	Every time you will connect to your data source, you will be prompted to use the data source in offline mode.
Caching mode	Determine how the entries will be reloaded in the data source. See Caching Mode topic for more information.
Connection timeout	Waiting time before a connection timeout.
Command timeout	Waiting time before a command timeout.
Allow beta database upgrade	If an upgrade is required and you are using a beta version and database, it will authorize you to upgrade it.
Allow data source credential variables	Allow to use the data source credential to be use in variables.
Advanced Settings	Edit of the connection string values directly.

Upgrade



SQL Server - Upgrade tab

Option	Description
Test Server	Test the connection with the server to validate if the proper information has been provided.
Create Database	Create the database on the SQL server to use Password Vault Manager.
Update Database	Update the database on the SQL server, if required to use Password Vault Manager.
Test Database	Test the connection with the database to validate if the proper information has been provided.
Email Schema to Support	Send your schema to the Devolutions Support team.
View upgrade script	Generate your updated script.

4.2 2-Factor Authentication

Description



This feature requires an [Advanced Data Sources](#).

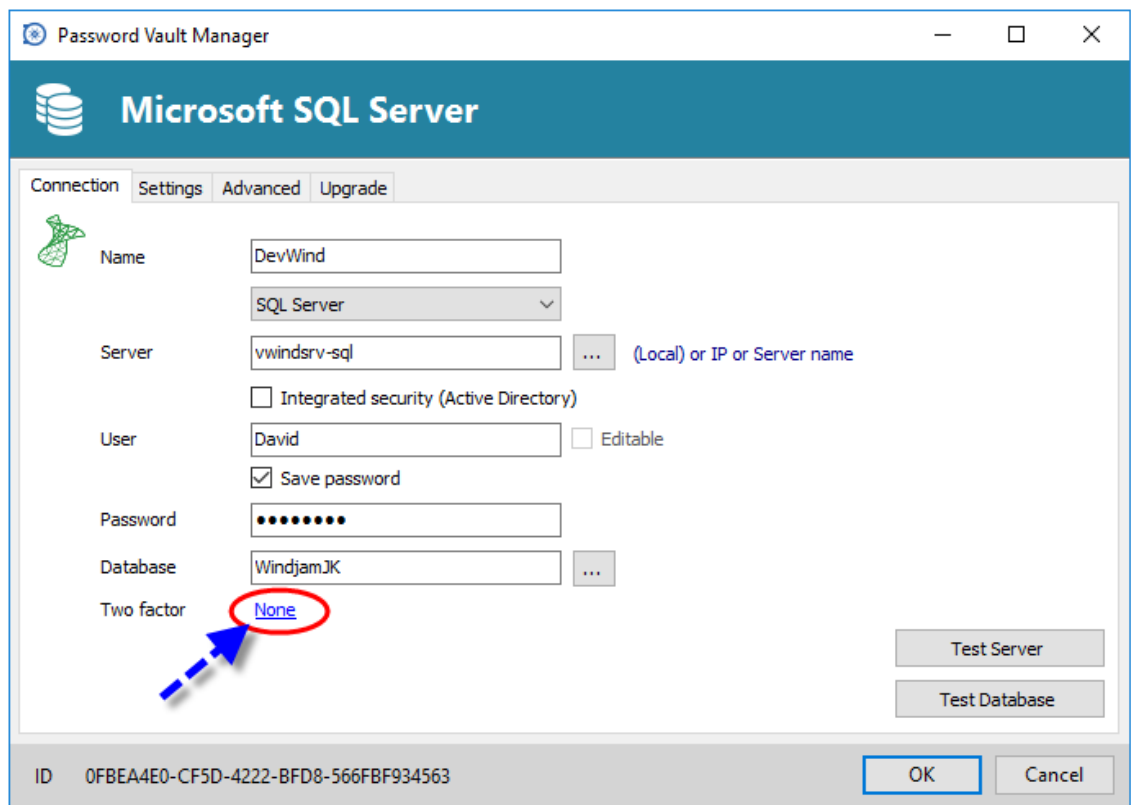
The two-factor authentication provides unambiguous identification of users by means of combination of two different components. These components may be something the user knows or something the user possess.

The use of two-factor authentication is used to prove one's identity is based on the premises that an unauthorized actor is unlikely to be able to supply both factors required for access. If in an authentication attempt at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset being protected by the two-factor authentication will remain blocked.

Password Vault Manager has implemented 2FA to our data sources using [Google Authenticator](#), [Yubikey](#), [Duo](#) and [AuthAnvil](#).

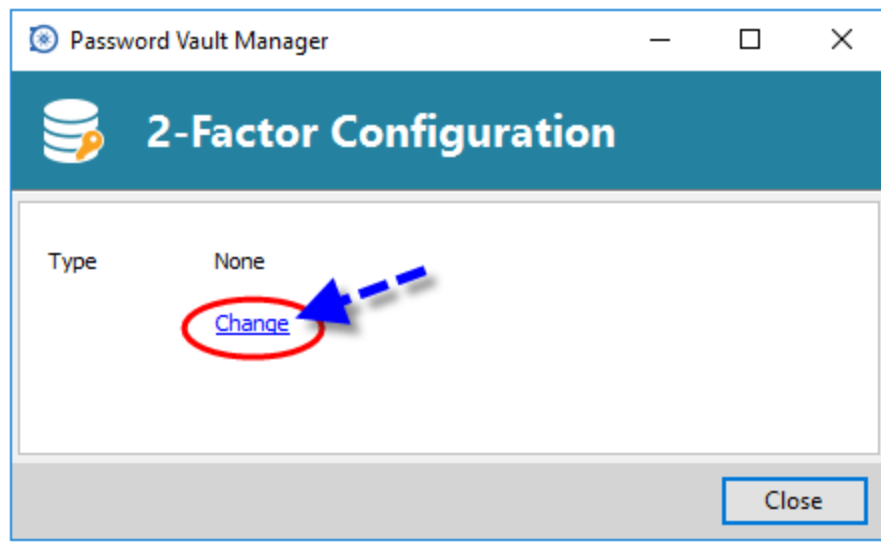
Settings

1. When creating your data source you can choose the **Two factor** option. To modify the option, click on the **None** hyperlink.



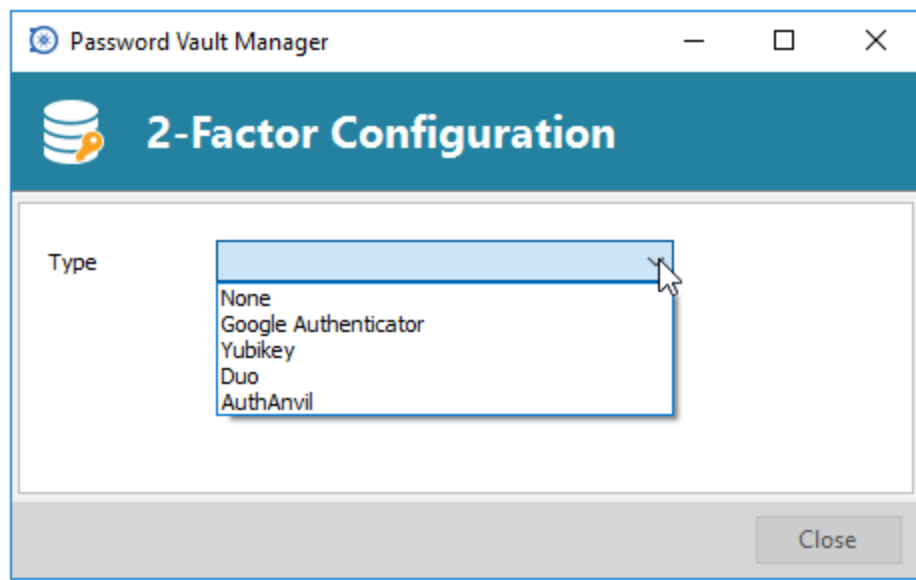
SQL Server - Two factor option

2. In the next window click on **Change**.



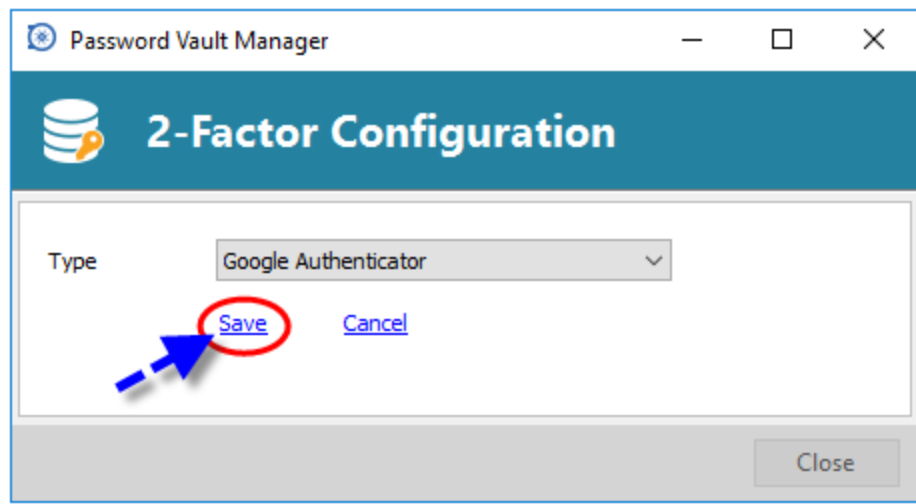
2-Factor Configuration - Change

3. Choose the type of 2-Factor Configuration you wish to use from our supported providers.



2-Factor Configuration type

4. Once you have selected your 2FA click on **Save** to start the configuration.



2-Factor Configuration - Save

4.2.1 Google Authenticator

Description

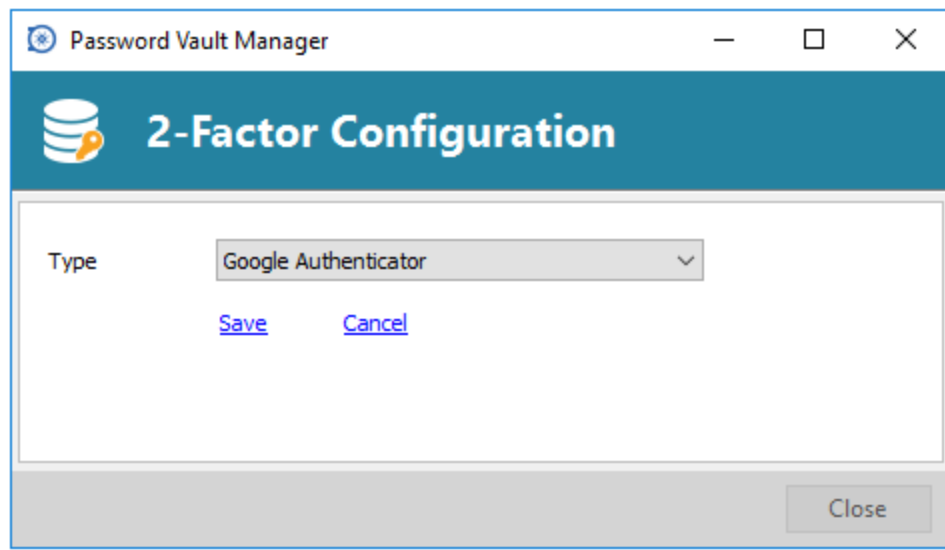
Password Vault Manager allows you to use **Google Authenticator** to provide an additional layer of security when opening a selected data source.

Settings



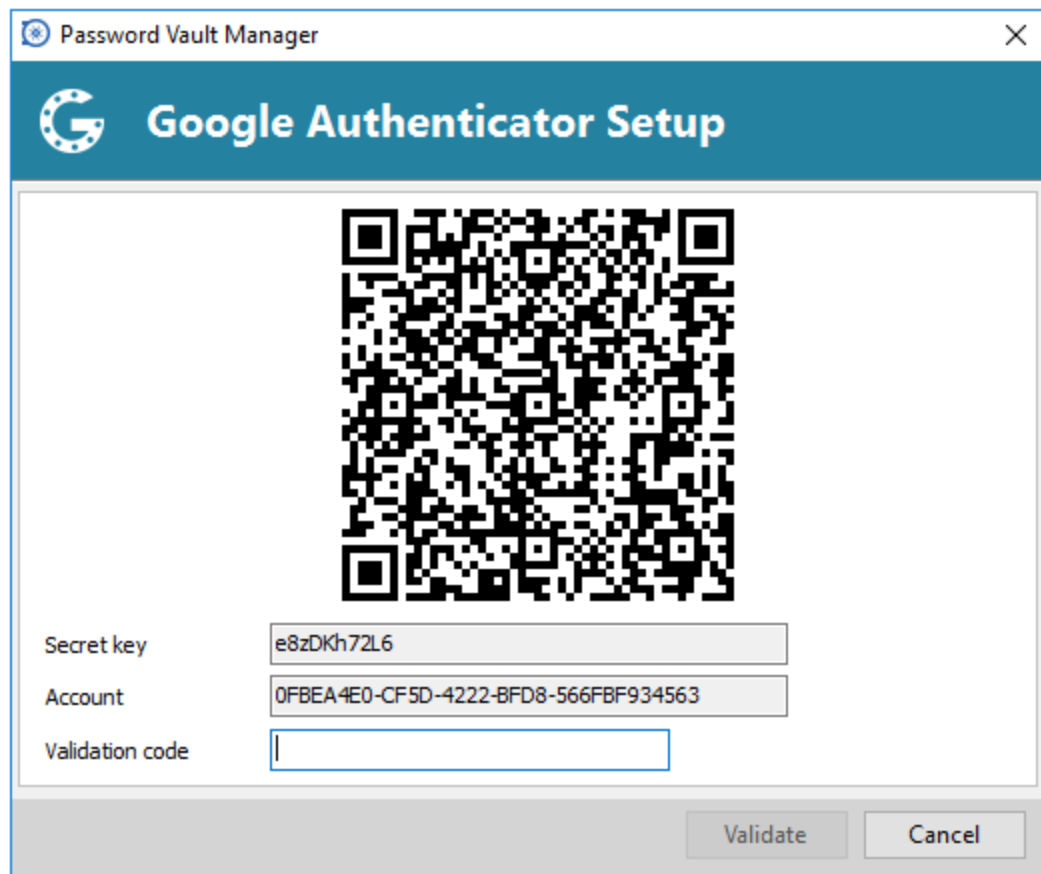
Before you start the configuration, make sure you have installed the [Google Authenticator](#) application on a supported device.

1. Select Google Authenticator as your 2-Factor Authentication and click on **Save**.



2-Factor Configuration - Google Authenticator

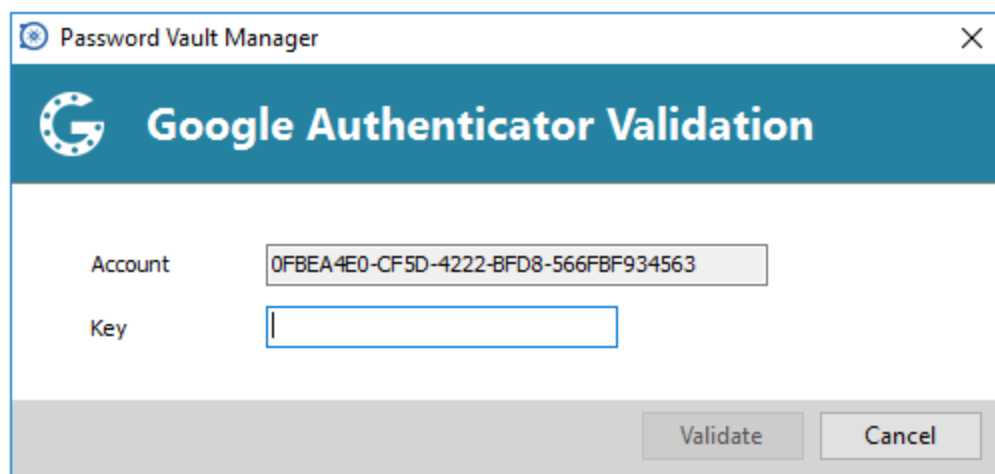
2. Once you have installed the application, scan the QR code on your screen with the Google Authenticator application to setup Password Vault Manager in Google Authenticator. When Password Vault Manager is configured in Google Authenticator, enter the Validation code provided by Google Authenticator in Password Vault Manager. Enter the Validation code and then click on **Validate**.



The screenshot shows a dialog box titled "Password Vault Manager" with a close button (X) in the top right corner. The main header is "Google Authenticator Setup" with a Google logo. In the center is a large QR code. Below the QR code are three input fields: "Secret key" with the value "e8zDKh72L6", "Account" with the value "0FBEA4E0-CF5D-4222-BFD8-566FBF934563", and "Validation code" which is empty. At the bottom right are "Validate" and "Cancel" buttons.

Google Authenticator Setup

3. Relaunch Password Vault Manager and select the protected data source to be prompted for the Google Authenticator code.



The screenshot shows a dialog box titled "Password Vault Manager" with a close button (X) in the top right corner. The main header is "Google Authenticator Validation" with a Google logo. Below the header are two input fields: "Account" with the value "0FBEA4E0-CF5D-4222-BFD8-566FBF934563" and "Key" which is empty. At the bottom right are "Validate" and "Cancel" buttons.

Google Authenticator Validation



Google Authenticator generates a new validation code every 30 seconds. Please consult your device application documentation for more details.

4.2.2 Yubikey

Description

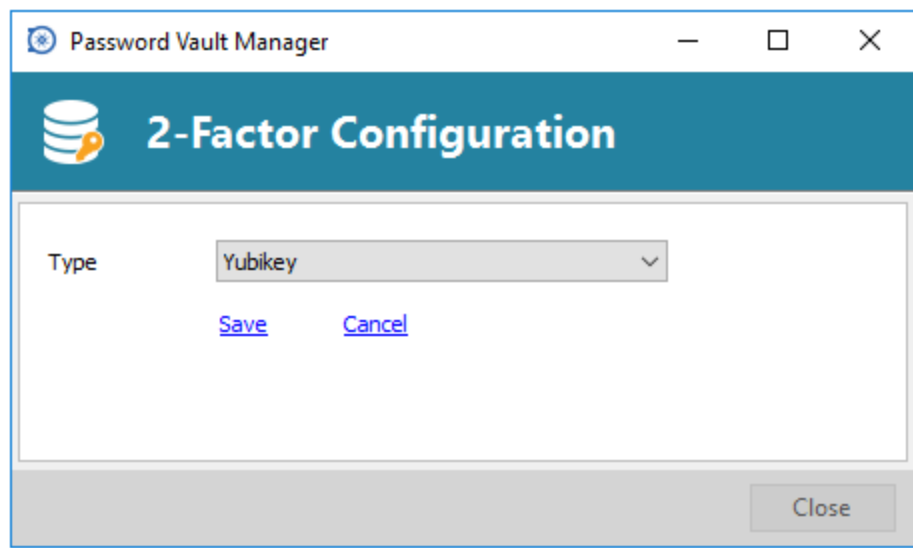
Password Vault Manager allows you to use a **Yubikey** to provide an additional security layer when opening a data source.

Settings



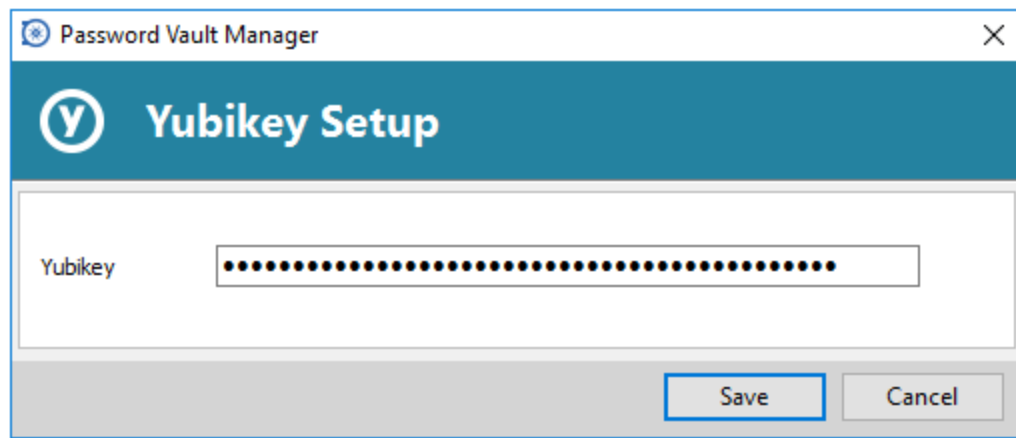
Before you start the configuration, make sure you have a [Yubikey](#) in your possession.

1. Select Yubikey as your 2-Factor Authentication, click on **Save**.



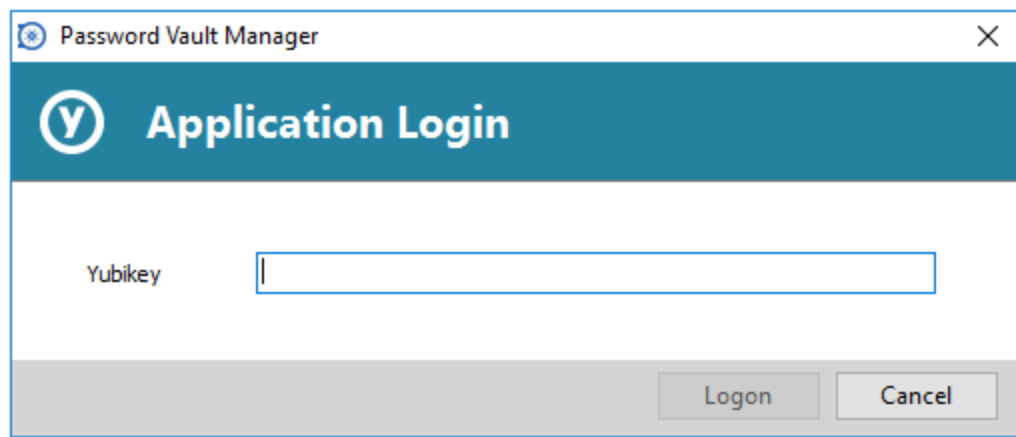
2-Factor Configuration - Yubikey

2. Insert the Yubikey into a USB port of your computer and hold the gold button of the Yubikey to have the code filled in the field, then click on **Save**.



Yubikey Setup

3. Relaunch Password Vault Manager and select your protected data source to be prompted for a Yubikey code.



Yubikey Application Login

4.2.3 Duo

Description

Password Vault Manager allows you to configure a **Duo Authentication** to provide an additional security layer when opening a selected data source.

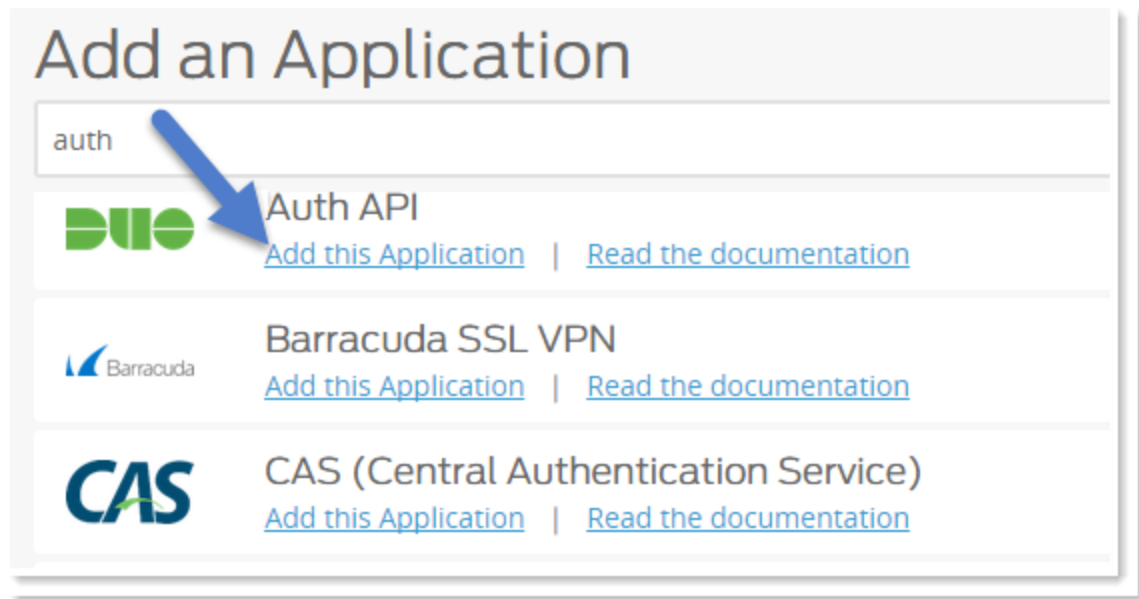
Settings



Before you start the configuration, make sure you have created yourself a Duo account and also have installed the Duo application on your compatible device.

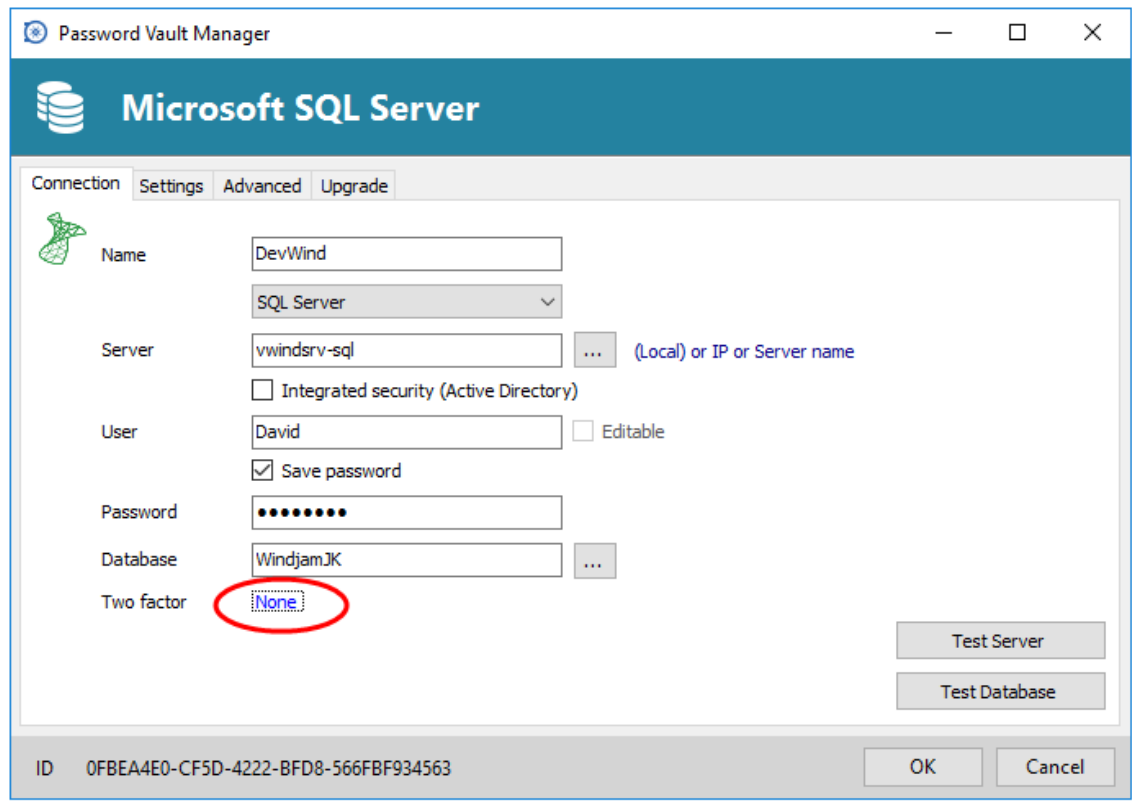
There are three ways of using the authentication with Duo: by land line, by text message or by using their application.

1. In your Duo account you will need to add the application **Auth API**.



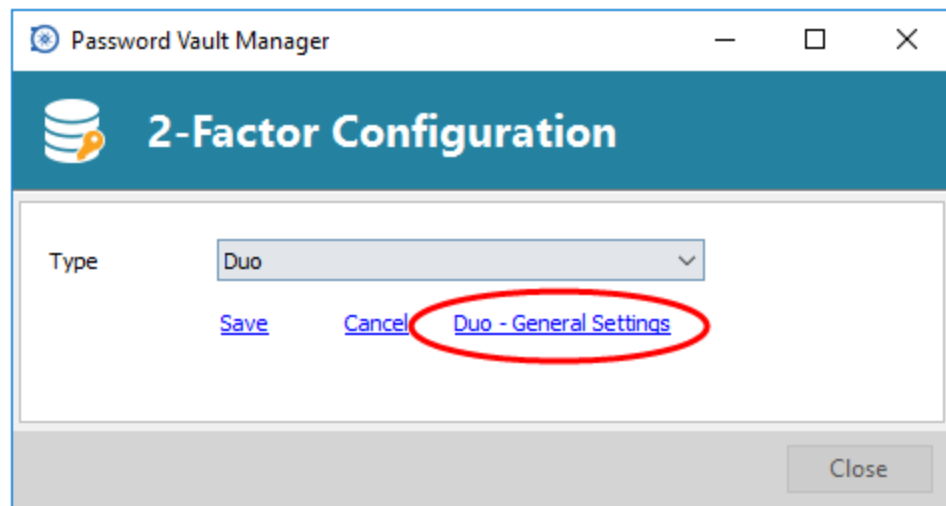
Auth API application

2. In Password Vault Manager select your Data source, in the Two Factor option click on **None** to change your Two factor Authentication mode. In the next window click on **Change**.



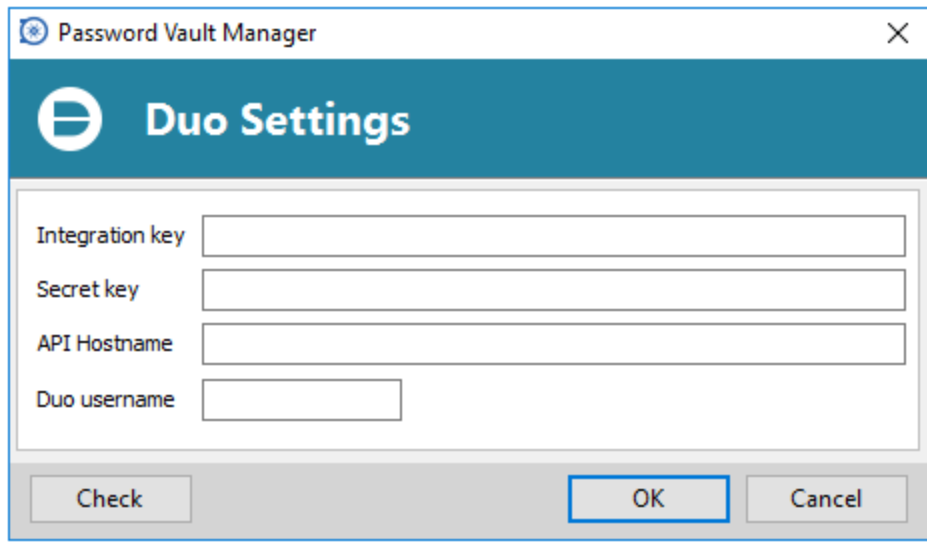
SQL Server - Two Factor - None

3. Select Duo as your Two factor authentication. And then click on **Duo - General Settings**



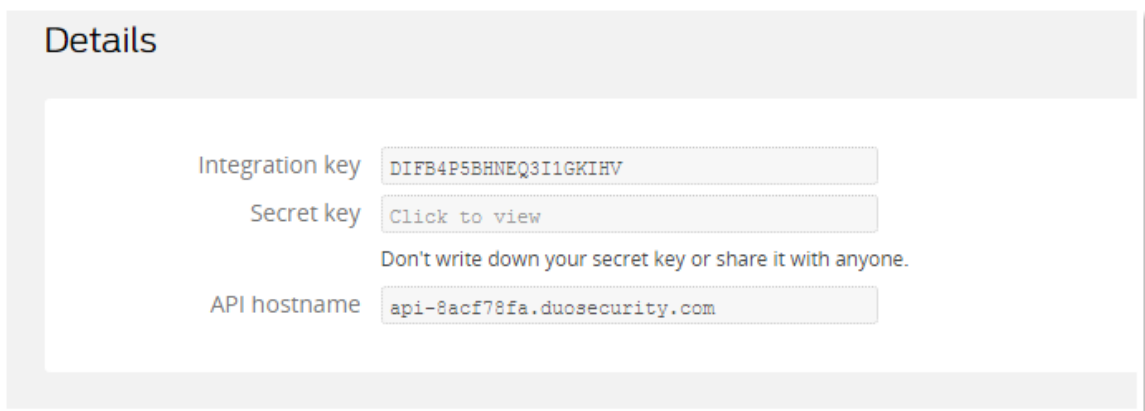
2-Factor Configuration - Duo General Settings

4. All the information needed for the General Settings will be generated for your Duo account. Copy and paste all the information and click on check to be sure the information is valid.



The screenshot shows a dialog box titled "Password Vault Manager" with a sub-header "Duo Settings". It contains four input fields: "Integration key", "Secret key", "API Hostname", and "Duo username". At the bottom, there are three buttons: "Check", "OK", and "Cancel".

Duo Settings

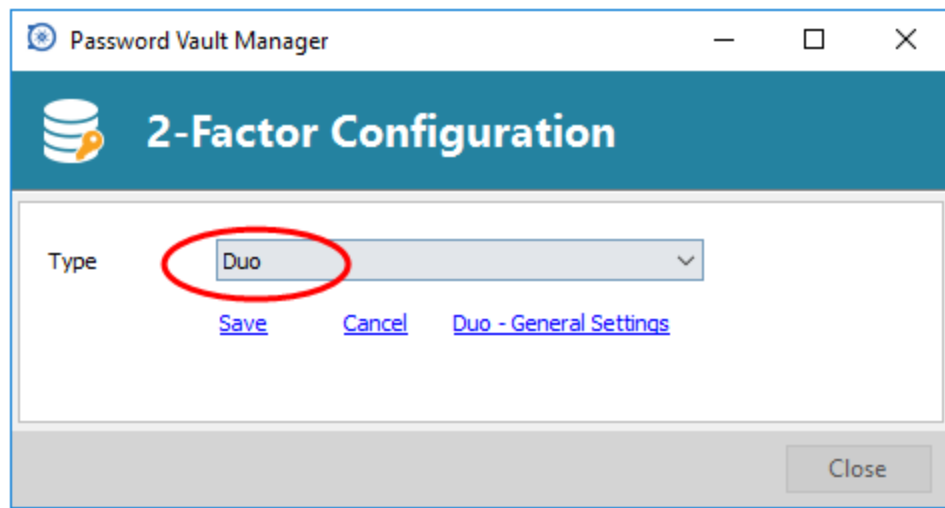


The screenshot shows a "Details" section with the following information:

Integration key	DIFB4P5BHNEQ3I1GKIHV
Secret key	Click to view
Don't write down your secret key or share it with anyone.	
API hostname	api-8acf78fa.duosecurity.com

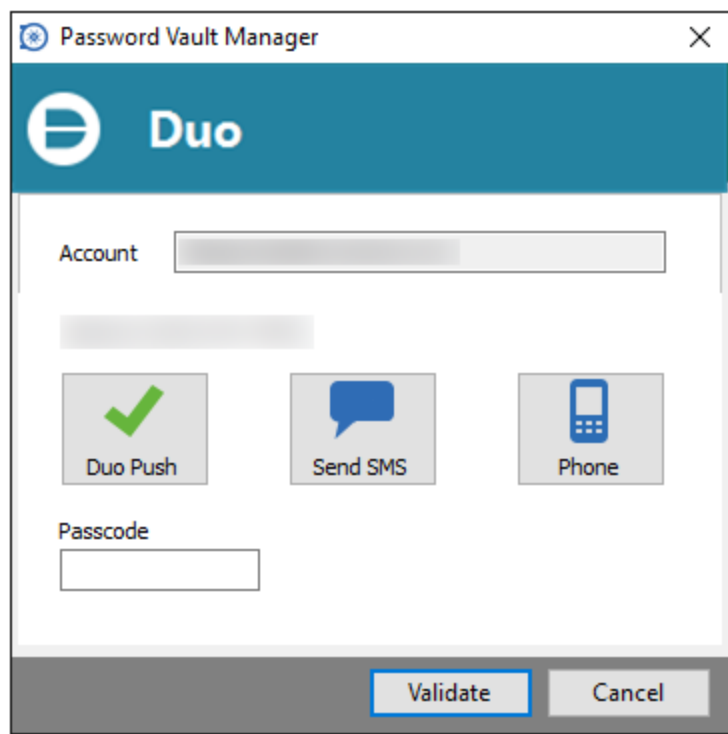
Auth API information from Duo website

5. Click on save to authenticate yourself with your Duo account that has just been activated.



2-Factor Configuration - Duo

6. If you have more than one device connected to your Duo account, select the device you wish to use for your 2-Factor authentication.
7. Select the method by which you would like to receive your Passcode.
 - **Duo Push:** The code is "pushed" to your Duo application.
 - **Send SMS:** You will receive the code by SMS on your registered phone number.
 - **Phone:** You will receive a phone call and a computer generated voice will dictate you the code.



Duo Setup

You will now be prompted with the Duo Authentication every time you try to connect to your secured data source.

4.2.4 AuthAnvil

Description

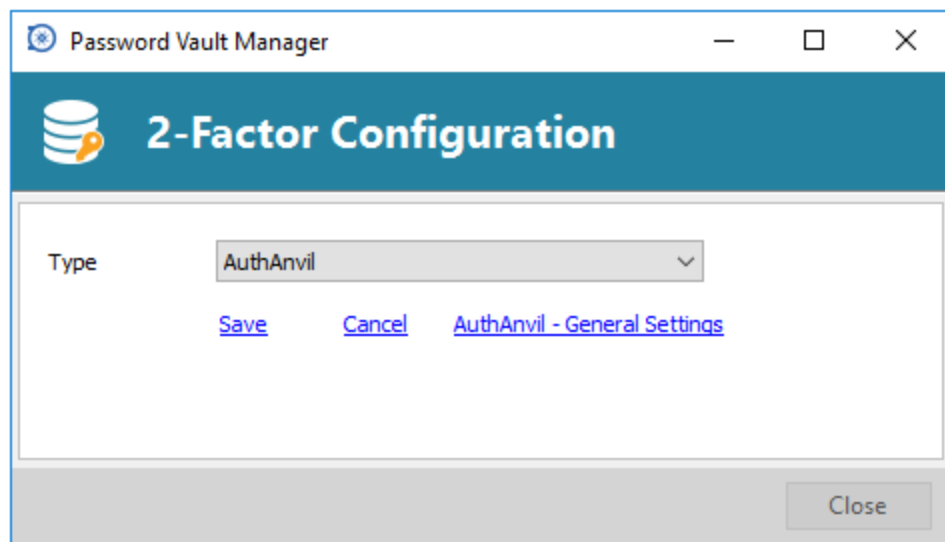
Password Vault Manager allows you to use **AuthAnvil** Authenticator to provide an additional security layer when opening a selected data source.

Settings



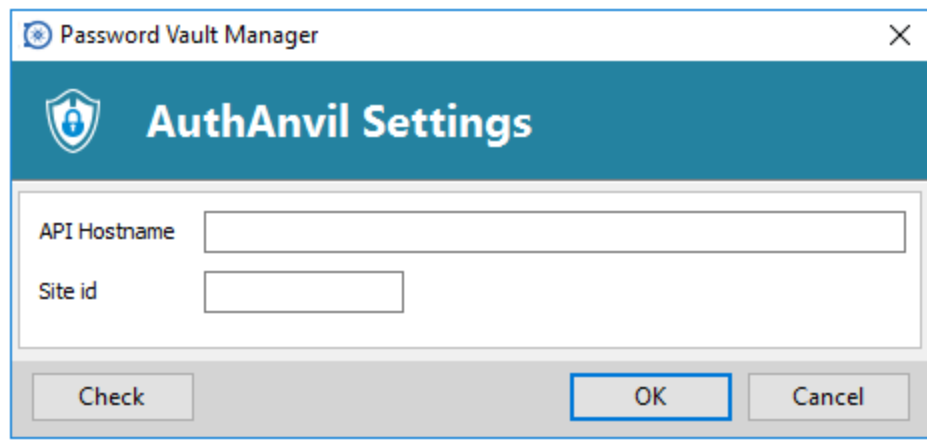
Before you start the configuration in Password Vault Manager, make sure you have created and configured your AuthAnvil account. For more information on AuthAnvil installation please consult <http://www.scorpionsoft.com/tour/intro>.

1. Select AuthAnvil in Password Vault Manager as your 2-Factor Authentication and click on **Save**.



2-Factor Configuration = AuthAnvil

2. Enter the information of your AuthAnvil account and click on **Check** to validate the entered information.



AuthAnvil Settings

4.3 Offline Mode

Description

The **Offline mode** allows you to connect to a local copy of the data source when the live database is unavailable. It can be used when a user is working from a disconnected network or when there is any kind of connectivity issue to the data source.

The read/write offline mode add the possibility for users to manipulate their sessions while disconnected from the data source. This is extremely useful for off site personnel or when working in environments that have sporadic network availability.

- When connected via VPN to clients network
- Working from home
- Working off-site



This feature is not available for all data sources, refer to the help topic of your chosen data source.

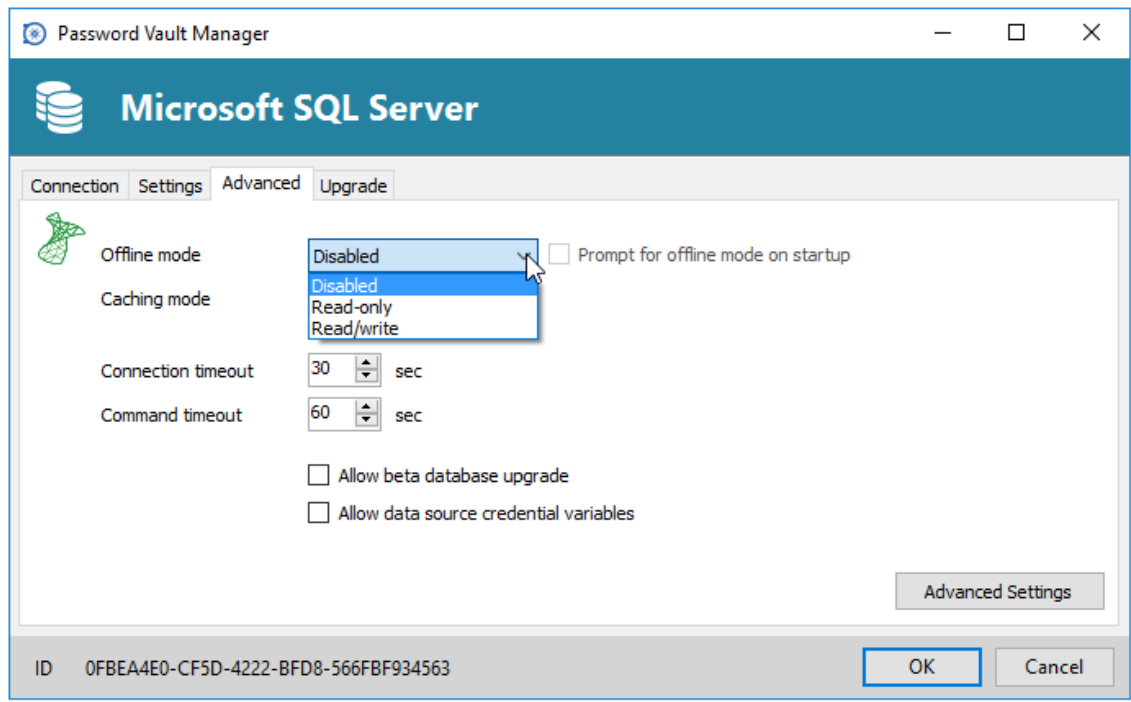


The offline cache is first encrypted using our own private key mixed with some information taken from the local computer. This makes it impossible for a copy on another machine to be readable. By default it is also encrypted with Windows NTFS encryption. In this case, there is no key saved anywhere.

For added security, offline files are set to expire after a delay, the default expiry is set to 7 days but can be modified via the [Data Source Settings](#).

Settings

Offline Mode



Data Source configuration - Advanced tab - Offline mode

Option	Description
Disabled	The offline mode will be disabled for the data source.
Read-only	Session data can be browsed and launched while not communicating back to the data source.
Read/Write	Session data can be browsed/launched/modified.



[Read/Write](#) offline mode is not available with the Basic subscription of [Online Database](#).



Not all functionality of Password Vault Manager is enabled while offline. Even when in read/write access mode you may not be able to perform all actions, for example documents uploaded to your data source are not cached locally. On the other hand, note that the [Private Vault](#) is available in offline mode.

Grant/Remove Offline



The offline mode is controlled at three levels:

- User permissions
- Data source settings (server configuration)
- Data source configuration (local configuration)

A user must be granted Read/Write at all three levels to allow read/write privileges.

User permissions	Data Source Settings	Data Source Configuration	Effective Access
Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Disabled	Disabled
Disabled or Read-only or Read/write	Disabled	Disabled or Read-only or Read/write	Disabled
Disabled	Disabled or Read-only or Read/write	Disabled or Read-only or Read/write	Disabled
Read-only or Read/write	Read-only or Read/write	Read-only	Read-only
Read-only or Read/write	Read-only	Read-only or Read/write	Read-only
Read-only	Read-only or Read/write	Read-only or Read/write	Read-only
Read/write	Read/write	Read/write	Read/write



You want to know the current effective [Offline Mode](#) while connected? See [My Data Source Information](#).

4.3.1 Offline Read/Write

Description

Offline read/write enables the user to perform add, updates and deletion while the data source is offline. Those changes are saved locally and synced back to the data source once the data source becomes available.



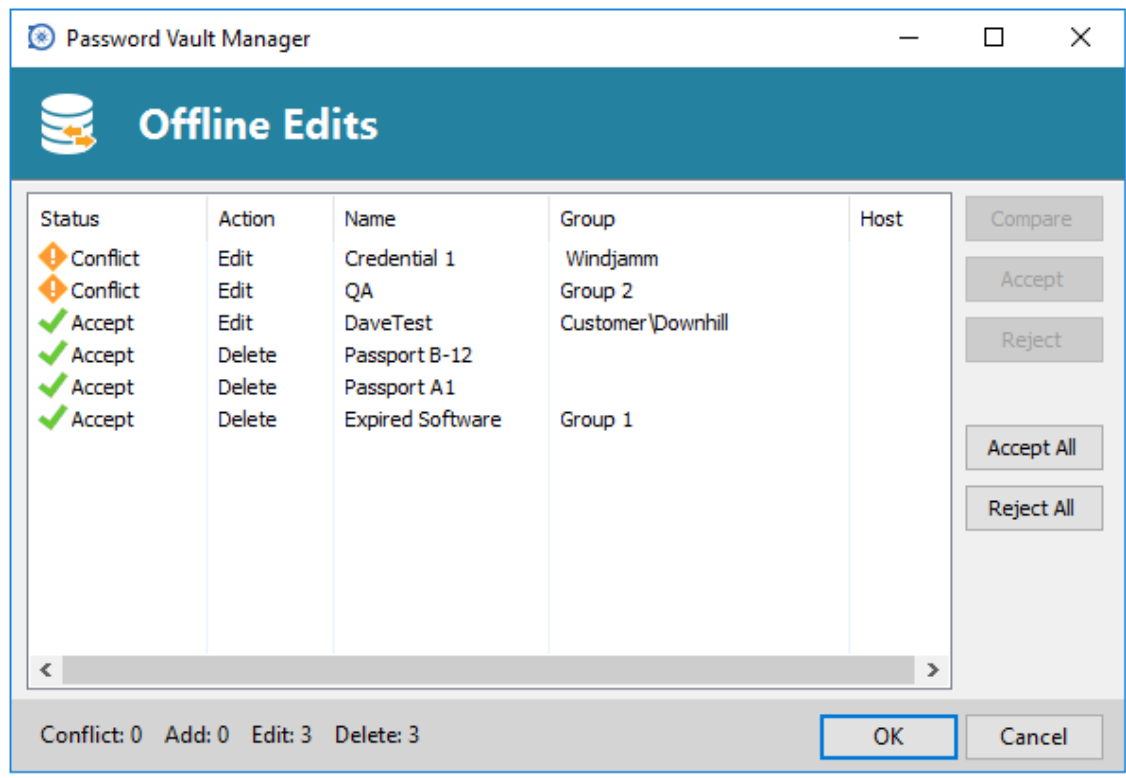
Not all functionality of Password Vault Manager is enabled while offline. Even when in read/write access mode, you may not be able to perform all actions. Note that the [Private Vault](#) feature is available in offline mode.

Once offline, the users security still applies. Add/Edit/Delete privileges granted by the administrator are respected. See [User Management](#).

Offline Edits Workflow

- Connect to the data source.
- Go offline. The fastest method is to use **File - Go Offline**, other methods will need to wait for a timeout.
- Edit any connection
- Use **File - Go Online**.

You will be prompted with:



Offline Edits - Synch change

Use this dialog to accept/reject your offline changes.

You can use the Compare action to have a side by side comparison of your changes with the current live entry.

Entries will be marked:

- **Accept** - when no changes have been detected.
- **Conflict** - when changes have been detected since you were last connected.

4.4 Caching

Description

The caching mode will determine on how the client will re-load entries when changes are detected. On large data sources caching is a must and will increase performance significantly.



This feature requires an [Advanced Data Sources](#).



If you feel the cache is outdated, press CTRL while clicking on refresh, this will force reading from the data source to recreate the cache.

Settings

Modes

Data source configuration - Caching mode

Option	Description
Disabled	No client caching.
Simple	Simple caching is the legacy caching mode. Performance may suffer when connected to data sources containing many sessions. On a modification of data within a data source the server cache token is changed. When Password Vault Manager performs a refresh it will compare it's local cache token with the data source token. In the case where has changed the entire data source is reloaded.
Intelligent	Intelligent cache has the ability to handle many more sessions without experiencing performance degradation. In the case of intelligent cache each modification performs a token update on the server. When Password Vault Manager performs a refresh action it will query the data source for any changes (delta) of changes to be applied client side since it last checked the data source. The delta of the changes is then sent to the application and applied locally. When first opening the data source Password Vault Manager will loaded the session from the offline file then refresh to get the up-to date information.

Storage

The client cache is persisted to disk in %LocalAppData%\Devolutions\RemoteDesktopManager\[GUID:DataSourceID]\Offline.db

There are two engines for the cache, if using a version of Password Vault Manager prior to 11.2, the default engine will be the SQLite, in that case the database is encrypted using a non-portable computed key hash.

If using version 11.2 or newer of Password Vault Manager the default cache engine will be the Microsoft Compound Document Format (MCDF) files.



You can enhance the security of the offline file by setting the Enhanced security in the options. See topic [Offline Security](#)

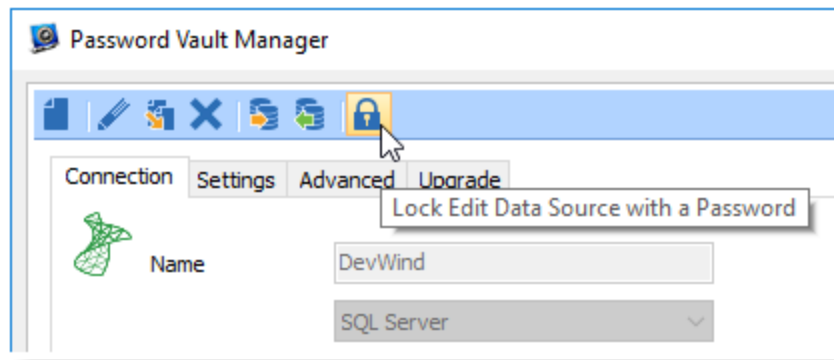


Depending on the configuration of the [Caching Mode](#) and the [Offline Mode](#), the Offline.db file may still exist since the file servers as a dual purpose caching & offline line support.

4.5 Lock Data Source

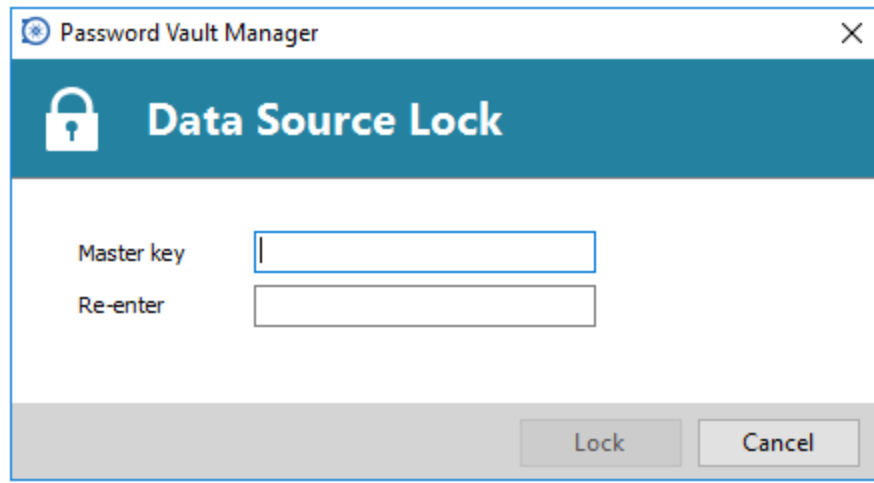
Lock Data Source

To protect sensitive data in your data source configuration (e.g. server URL or credentials), you may wish to lock the data source before installing it to your users. You can do this by using the Lock/Unlock button from the toolbar.



Lock data source toolbar

The locked data source will require a password. The password must be set when the lock is applied. Use the same password to unlock it or to modify the data source configuration



Lock data source dialog

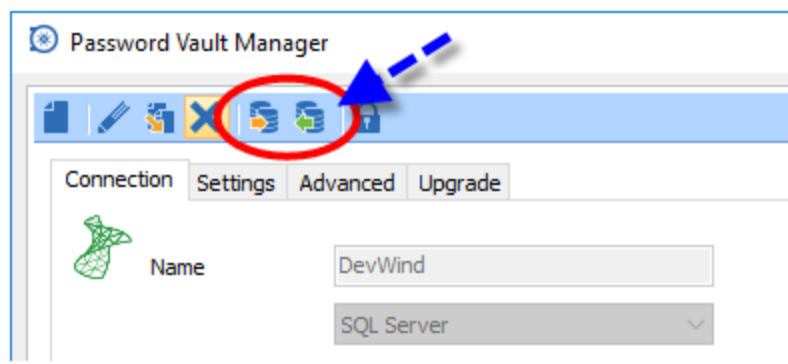


There is ***NO WAY*** of unlocking the data source if the password is lost or forgotten. In such an event, you will need to configure a new data source.

4.6 Import/Export Data Source

Import/Export Data Source

You can simplify deployment for multiple users by importing or exporting the data source. The generated file will have an .rdd extension. Password Vault Manager allows you to export the online data source settings directly to an .rdd file. To do so, simply open the data source dialog (**File - Data Sources**) to import or export the file.

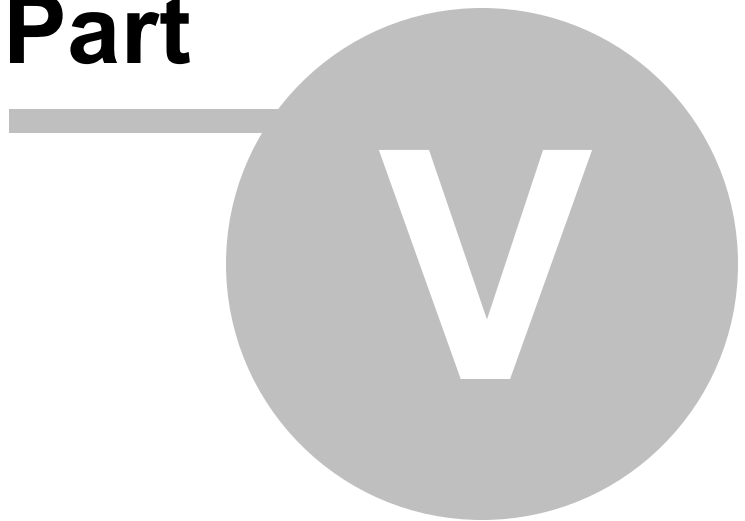


Import / Export data source

Also, a locked data source can be exported and imported, but its content will not be accessible unless a password is entered. See [Lock Data Source](#) for more information.

Entry Types

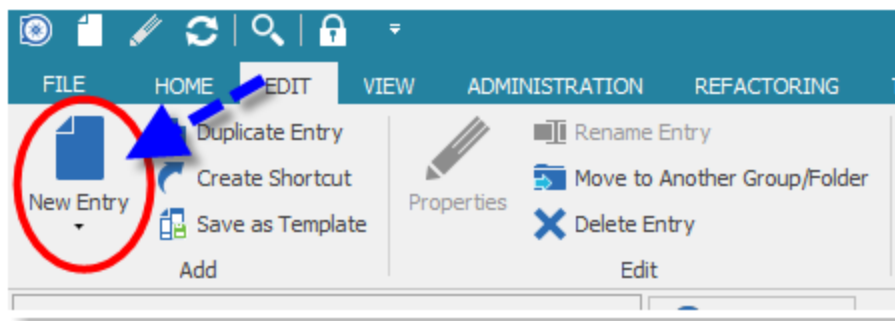
Part



5 Entry Types

Description

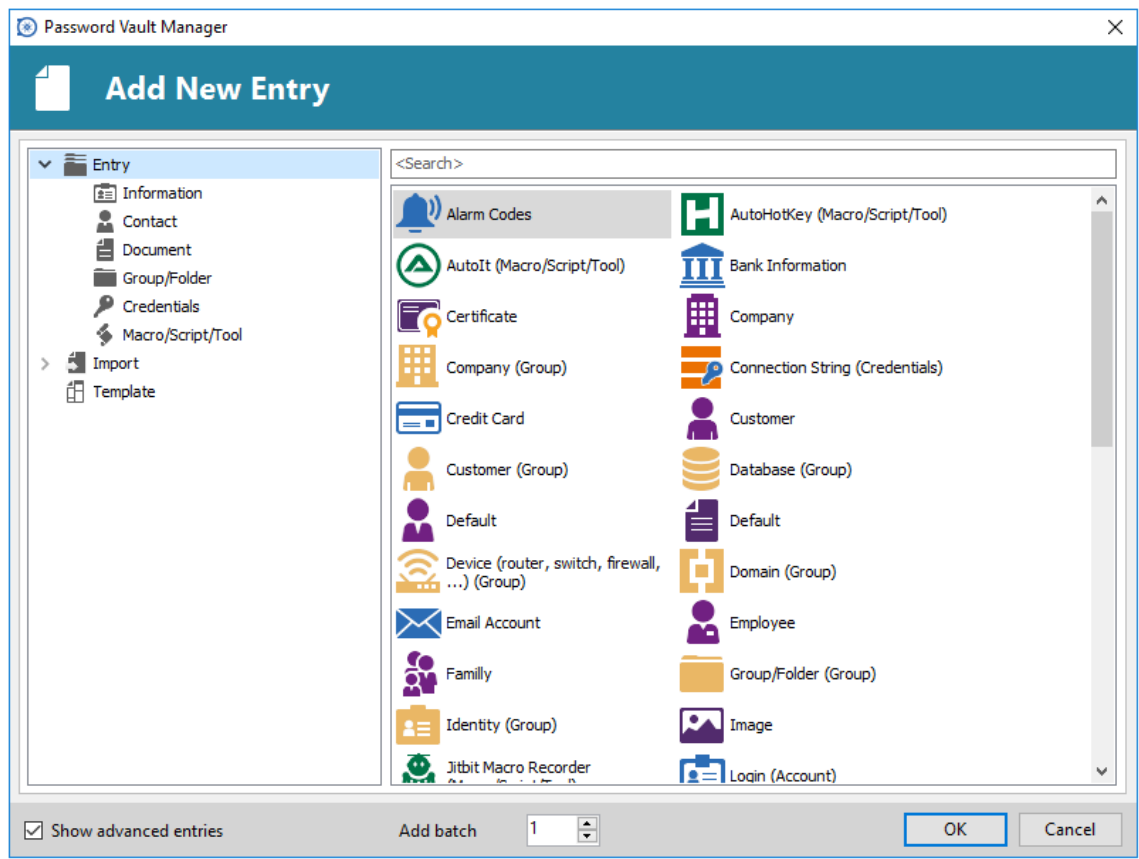
Every item you see in the navigation pane is an **Entry**. You can create a new Entry from the menu **Edit - New Entry** or by right clicking in the navigation pane and clicking on **New Entry**.



Edit - New Entry

Entries come in various types and are described in the following sections:

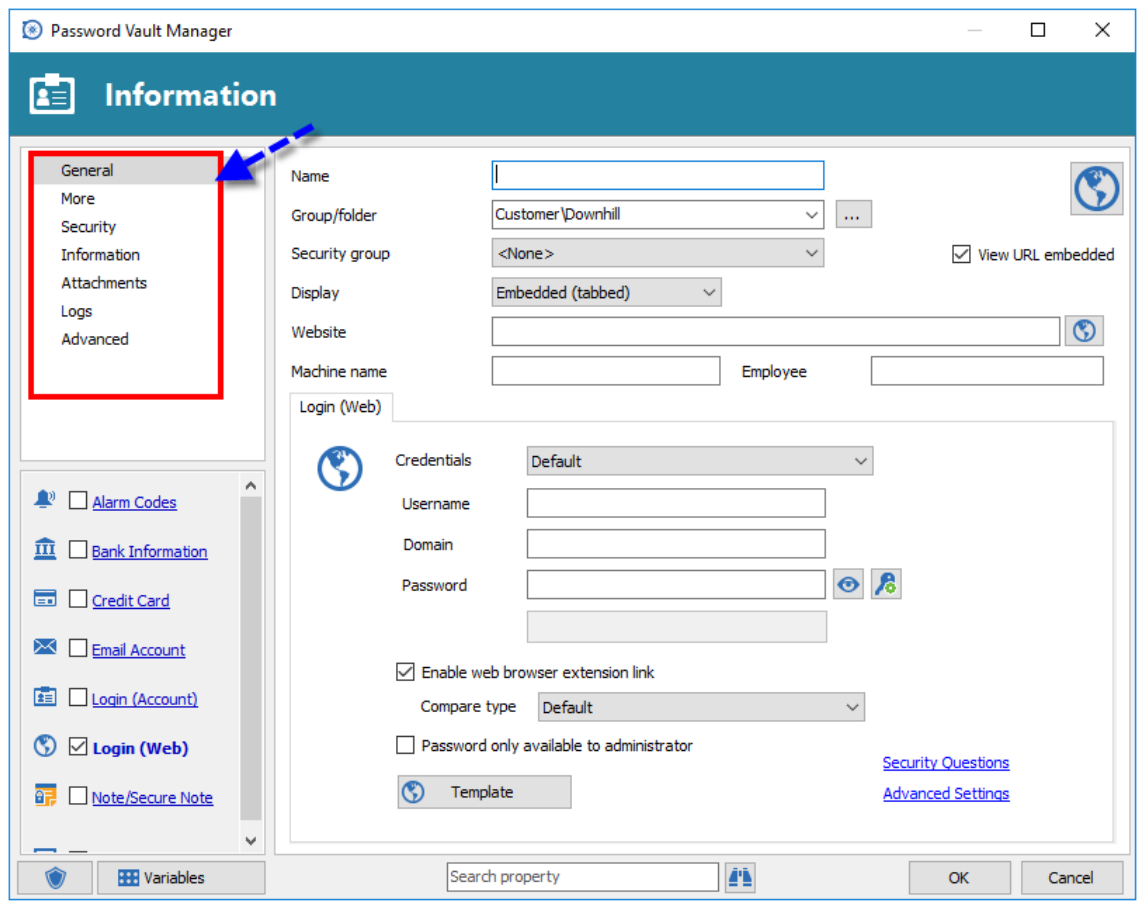
- Information
- Contact
- Document
- Group/Folder
- Credentials
- Macro/Script/tools



5.1 Settings

Description

Some settings are shared settings meaning that they are almost the same for every entry. These options are on the side menu of your entry.



Entry shared settings

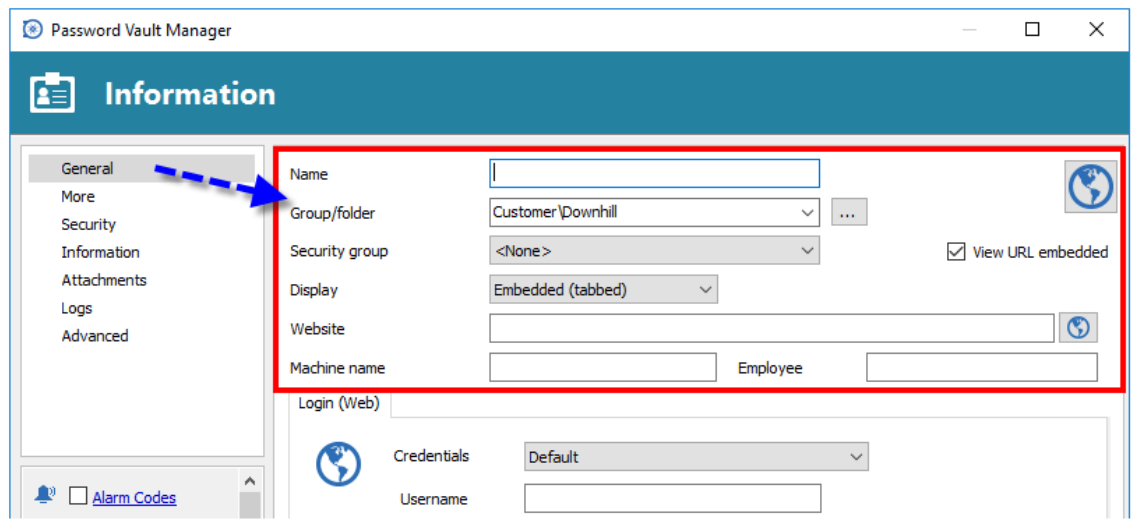
For more information please see:

- [General](#)
- [More](#)
- [Security](#)
- [Information](#)
- [Attachments](#)
- [Logs](#)
- [Advanced](#)

5.1.1 General

Description

The **General** side menu contains general information about your entry.



General side menu

Option	Description
Name	Enter the name of the entry that will be displayed in your treeview.
Group/folder	Useful to organize your entries in different folders, either in the tray icon context menu or in the tree view. Learn more here .
Security Group	In the Enterprise edition the Security field allows the Administrator to assign a security group to a session, and therefore limit a subset users to view the session. For more information please see Security .
Display	Allows the entries to be opened and embedded in Password Vault Manager, or externally. In the case of the latter, and if the application allows it, you may select the monitor on "allows it" to display it. For more information please see Display Mode .

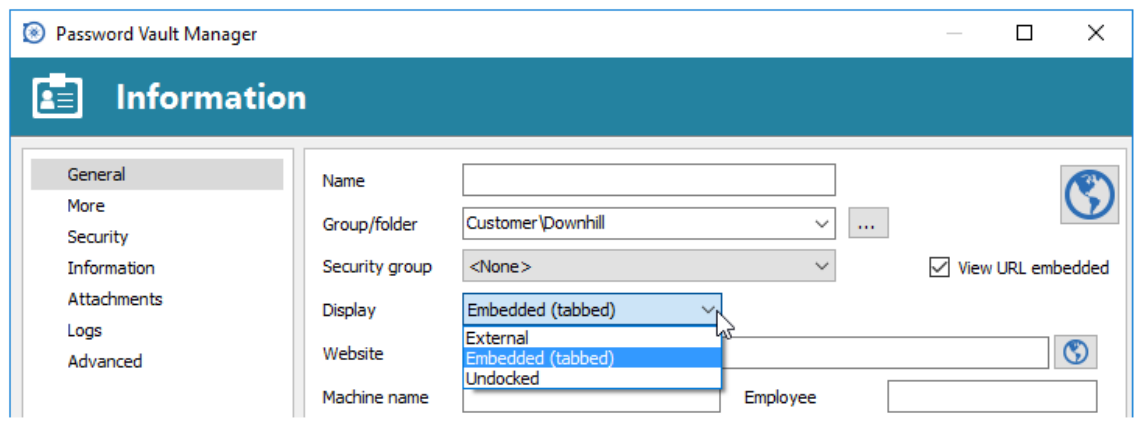
5.1.1.1 Display Mode

Description

Password Vault Manager allows control on how the entry itself is displayed and on how the URL defined in the entry is viewed. There is three types of display mode:

- External
- Embedded
- Undocked

Please note that **not** all entry supports the three modes. It all depends on the integration and the availability of the third party application.



Display mode

Settings

External Mode

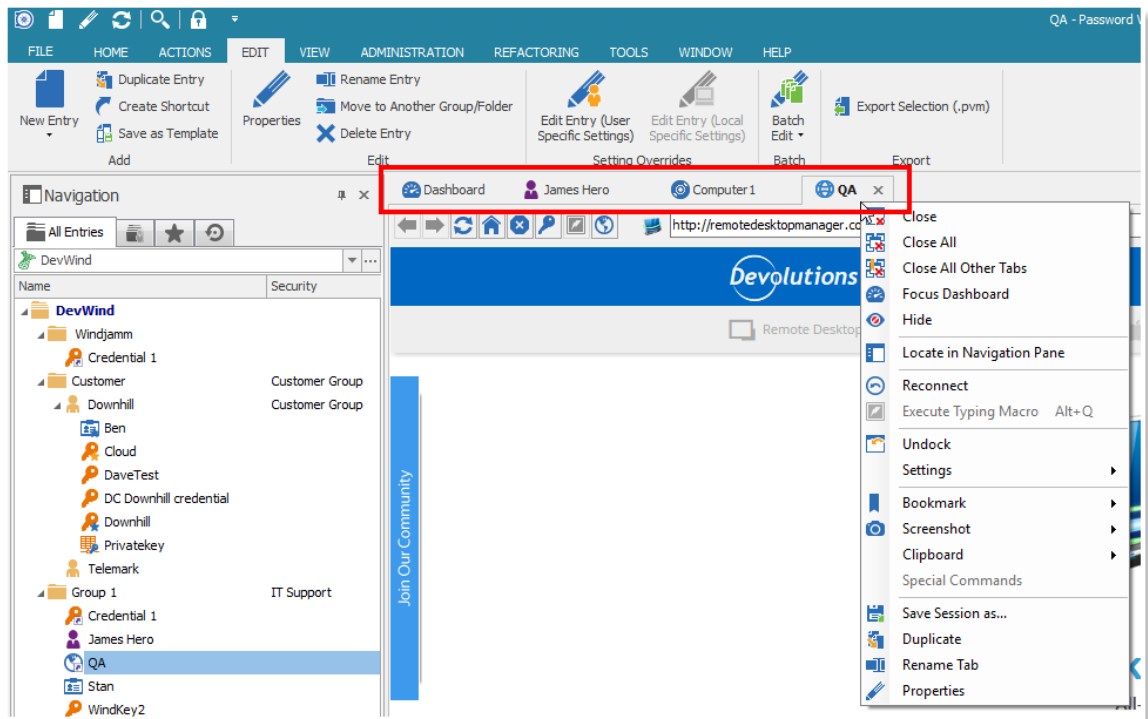
The **External mode** session is opened as an external process with no direct link to Password Vault Manager.

This display mode usually launches the native application. The external mode will automatically run on the Primary monitor. Depending on the type of session, an external mode session view will be updated if Password Vault Manager can detect that its running.

Embedded Mode

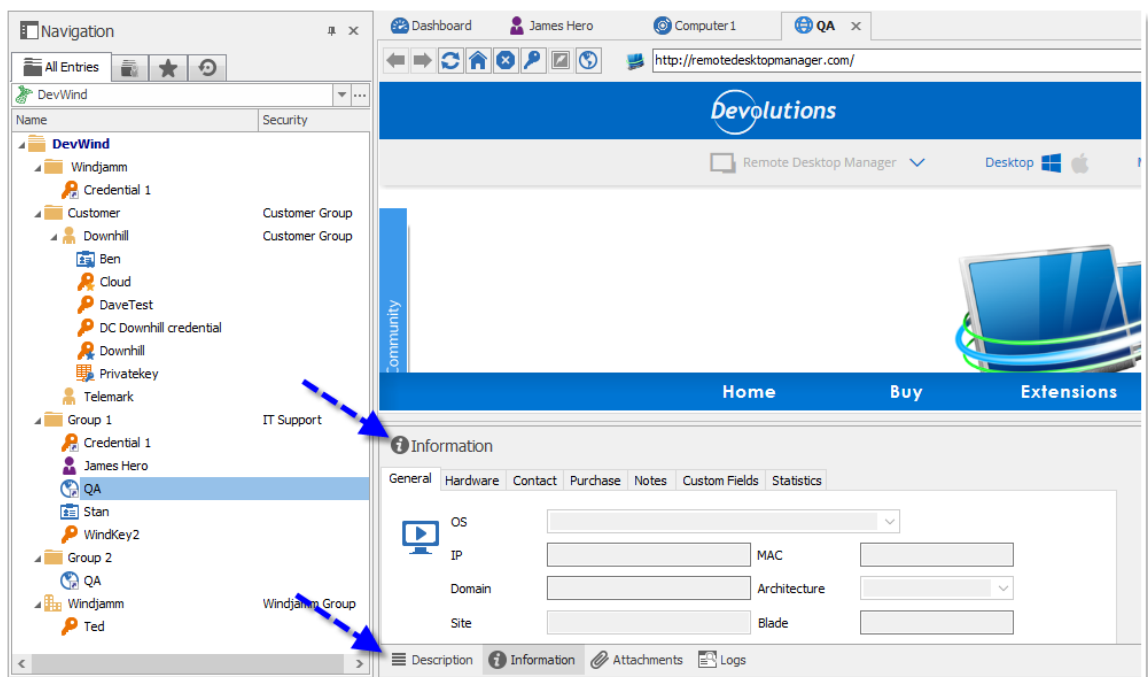
An embedded entry runs within the confines of the Password Vault Manager windows and display tabs at the top of the window. This mode centralizes the opened session in the application which makes it easy to switch from one to another.

There are several entry-specific actions available by right clicking (Context Menu) on the tab title.



Web entry opened in Embedded mode

You can also show the session footer (Description, Information, Attachments, Sub Connections, Logs, etc.) at the bottom of the screen and capture a screenshot of the content.

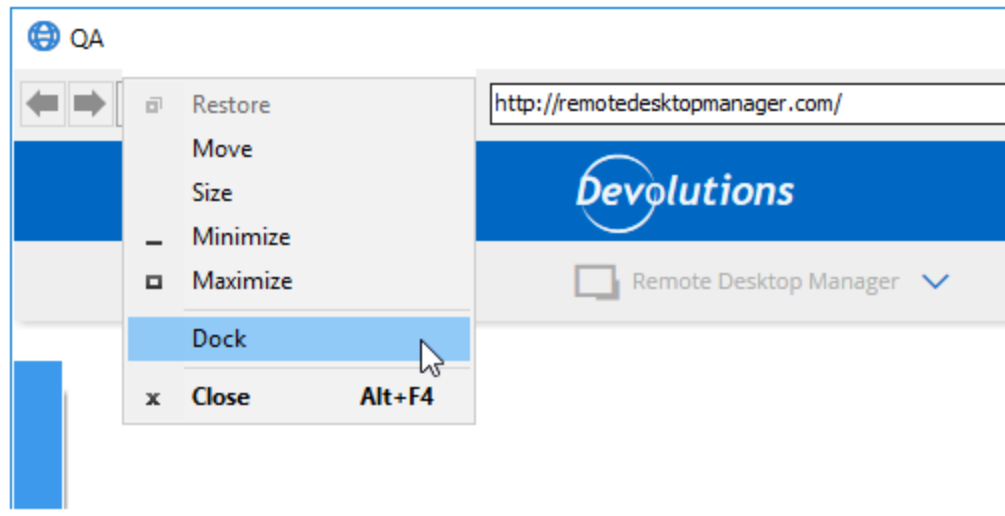


Embedded entry with visible folder

Undocked

While the embedded mode is useful in some cases, you may prefer to move the content in an external window. If so, this can be easily done using the context menu. Password Vault Manager will create a new window to contain the tabbed entry allowing you to move it anywhere else (i.e. on another screen).

To dock the content back to its original place, use the context menu by right clicking on the window icon.



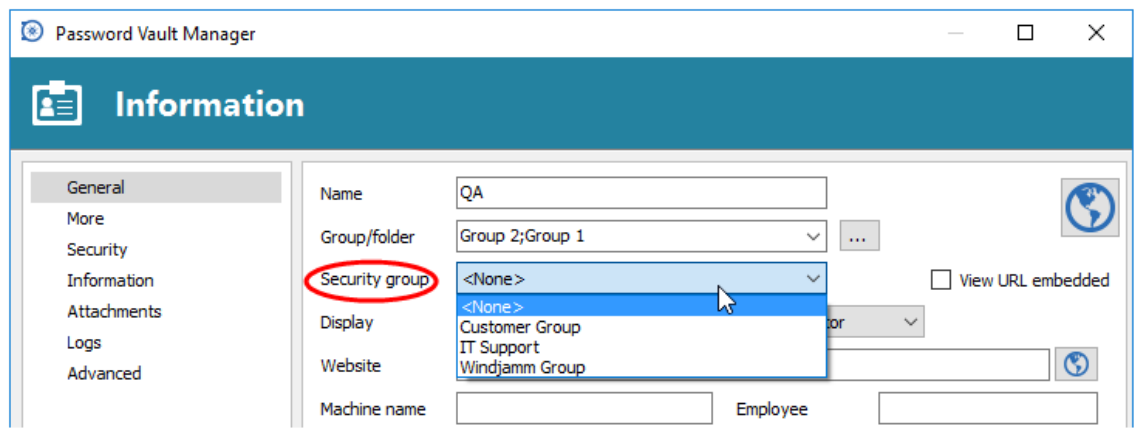
Undocked entry window context menu

5.1.1.2 Security

Description

Security groups are used to protect entries from a subset of system users. Assign your entry to a security group to then control who has access to it and how much control they have on the entry.

For more information see [Security Group Management](#).



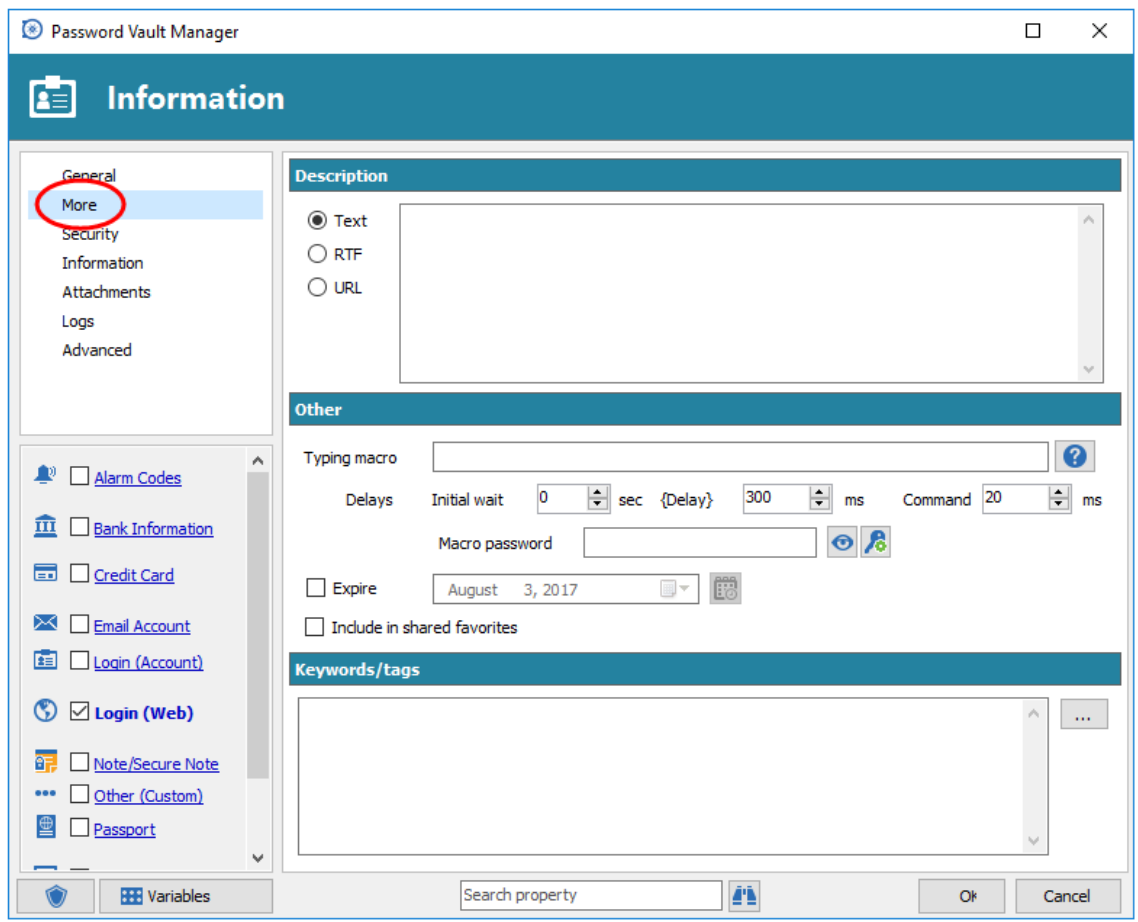
Security Group

5.1.2 More

Description

Please consult the following topics for more information on the sections of the More tab:

- [Description](#)
- [Other](#)
- [Keywords/Tags](#)



More side menu

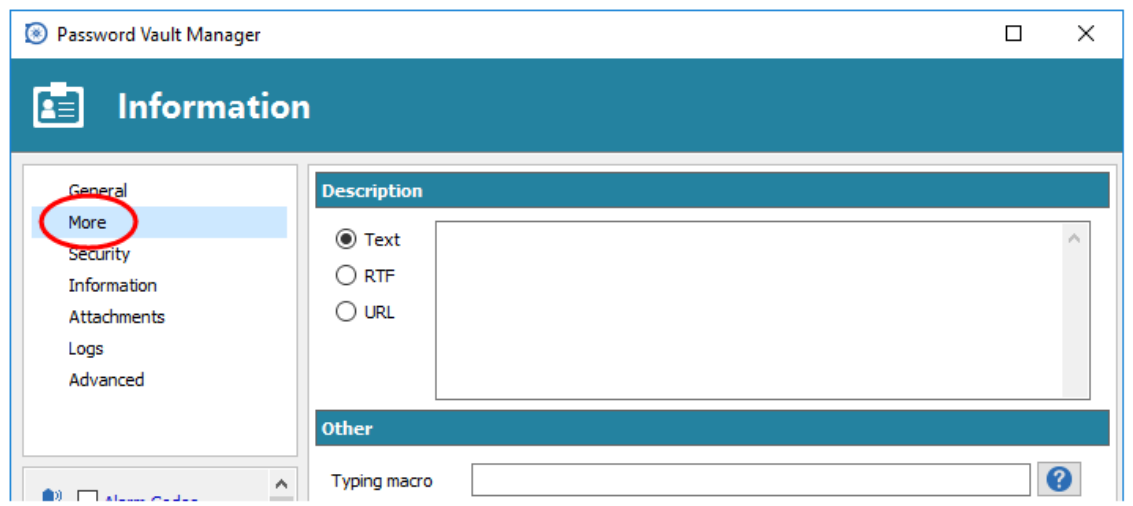
5.1.2.1 Description

Description

Password Vault Manager supports three description types:

- Text
- RTF
- URL

The description is displayed on the dashboard.

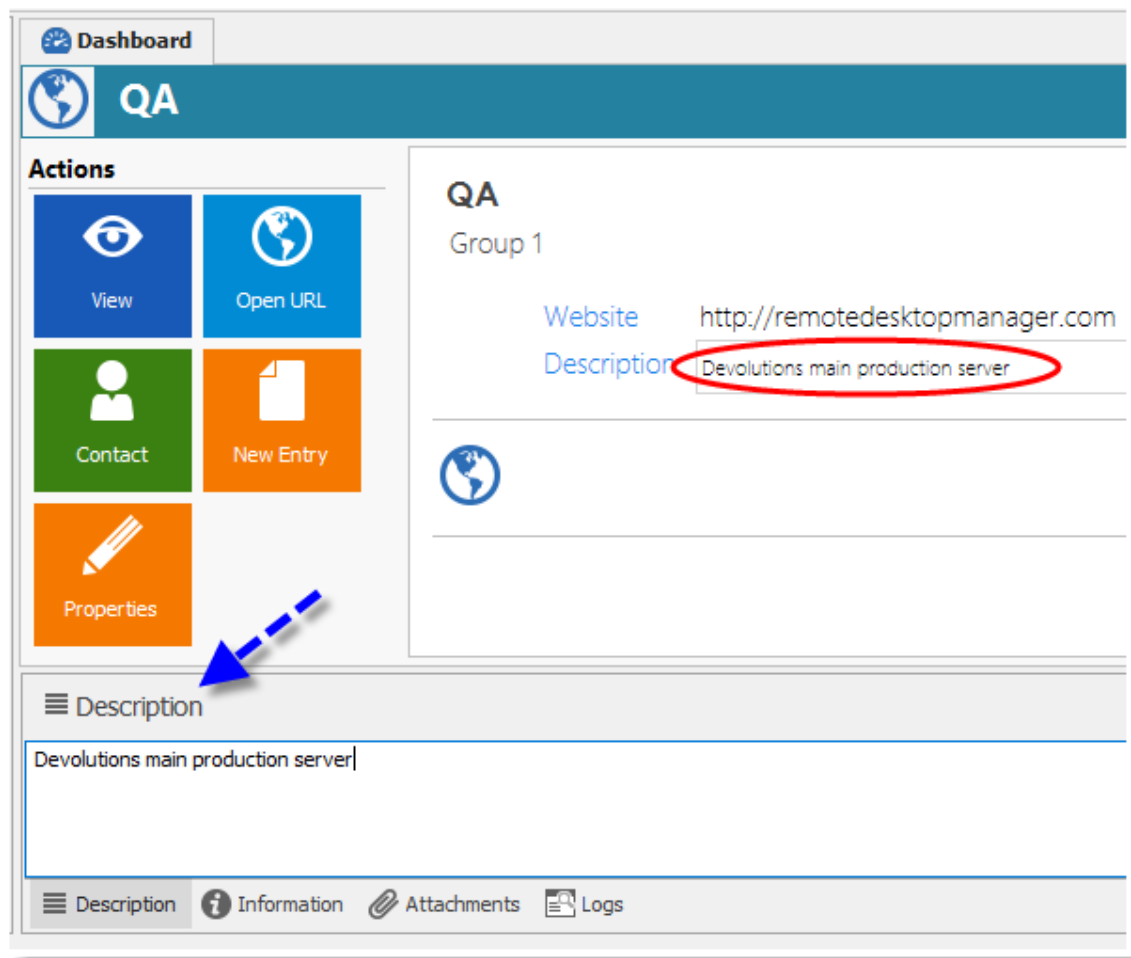


More - Description

Settings

Text

This is the most basic description, and it is simply a text without formatting.



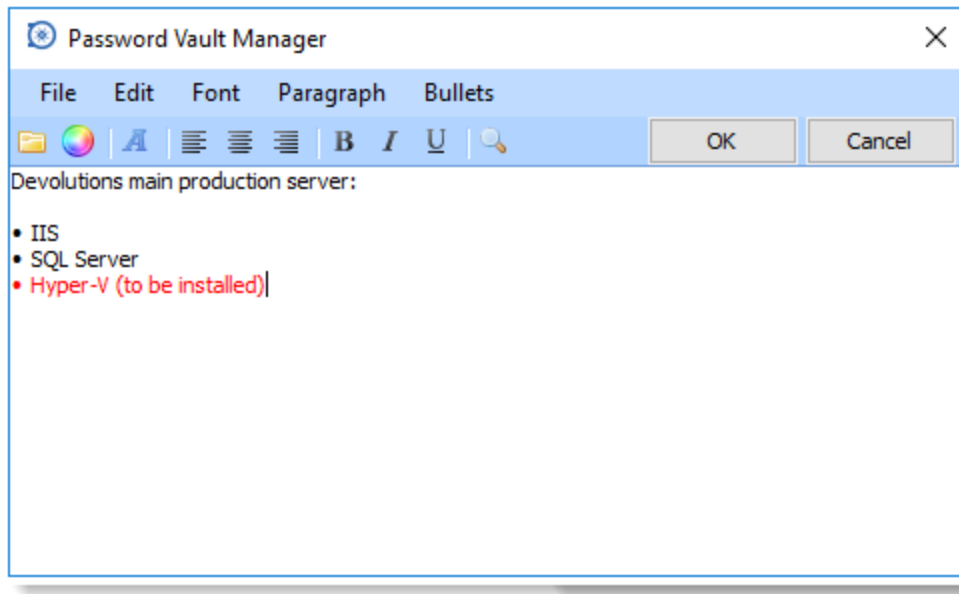
Description - Text

RTF

The RTF (Rich Text Format) description offers more formatting options, and allows you to change:

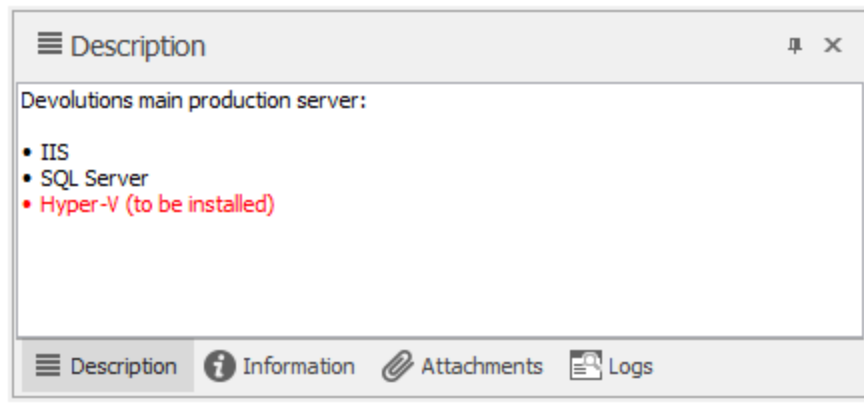
- Text color
- Font size
- Font style
- Text alignment

You can also create lists (numbered and bullets). Password Vault Manager will display the description exactly the way it was formatted in the editor.



Description - RTF Editor

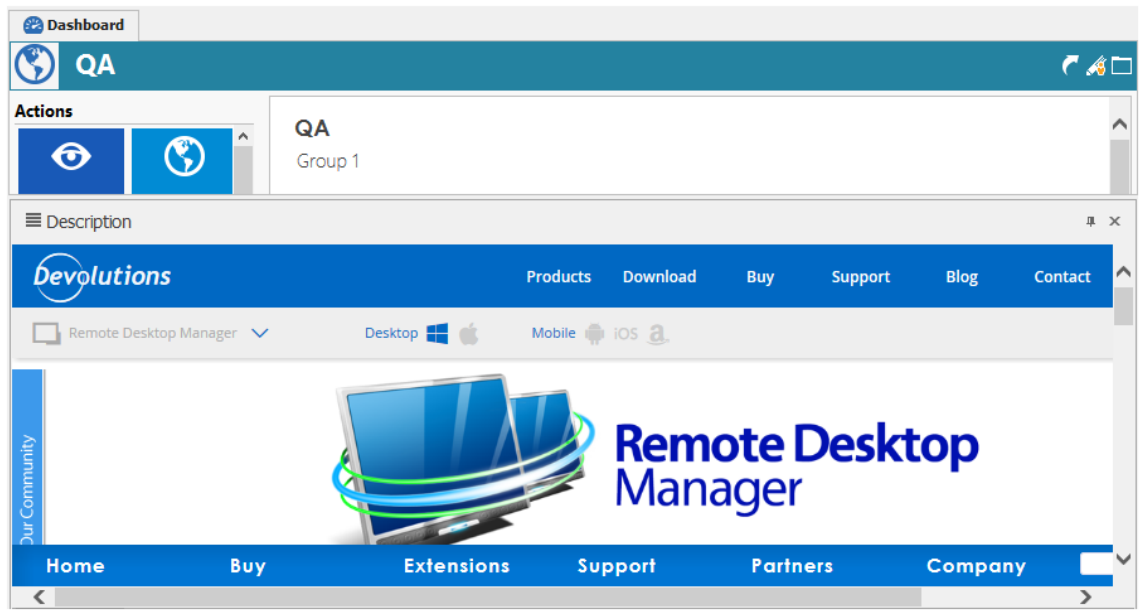
Password Vault Manager will display the description exactly the way it was formatted in the editor.



Description - RTF

URL

The description may also be a link to a website (e.g. on a server in the Intranet). By using session variables (\$SESSION_ID\$, \$SESSION_NAME\$, etc.), the website can generate an HTML page dynamically. This lets you integrate an external system or a custom application.

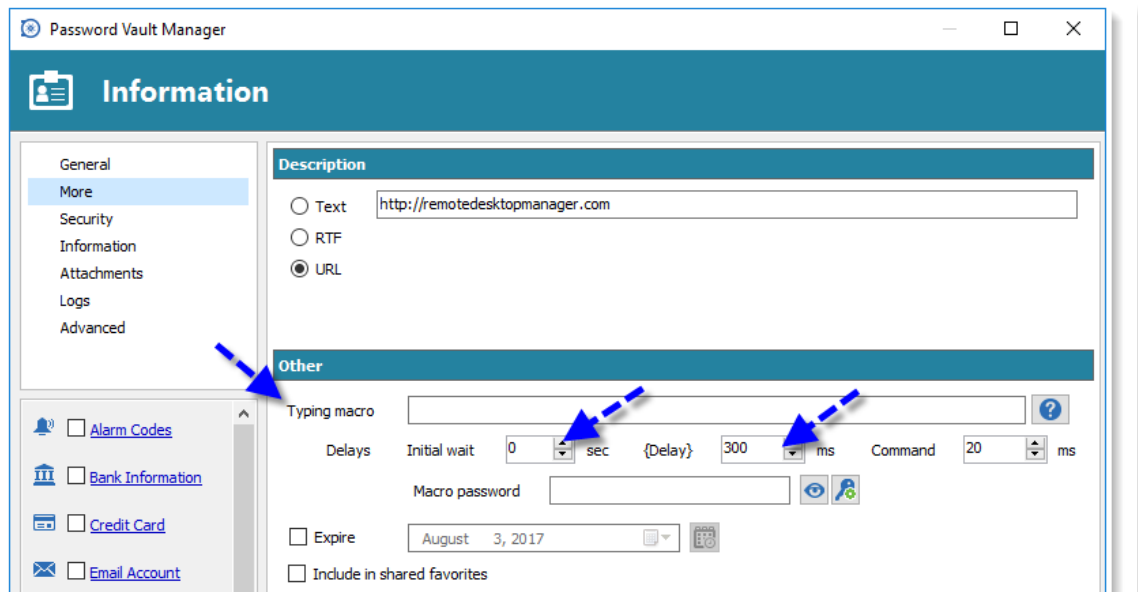


Description - URL

5.1.2.2 Typing macro

Description

The Typing Macro allows you to manually launch a typing macro once an entry has been opened.



More - Other

Typing Macro

Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. For example, to represent the letter A, pass in the string "A" to the method. To represent

more than one character, append each additional character to the one preceding it. To represent the letters A, B, and C, specify the parameter as "ABC".

The *initial wait* setting allows you to launch the macro and then switch the focus to whatever window you'd like to run the macro in.

Special keys

To specify characters that aren't displayed when you press a key, such as ENTER or TAB, and keys that represent actions rather than characters, use the codes in the following table.

Key	Code
BACKSPACE	{BACKSPACE}, {BS}, or {BKSP}
BREAK	{BREAK}
CAPS LOCK	{CAPSLOCK}
DEL or DELETE	{DELETE} or {DEL}
DOWN ARROW	{DOWN}
END	{END}
ENTER	{ENTER}
ESC	{ESC}
HELP	{HELP}
HOME	{HOME}
INS or INSERT	{INSERT} or {INS}
LEFT ARROW	{LEFT}
NUM LOCK	{NUMLOCK}
PAGE DOWN	{PGDN}
PAGE UP	{PGUP}
PRINT SCREEN	{PRTSC}
RIGHT ARROW	{RIGHT}
SCROLL LOCK	{SCROLLLOCK}
TAB	{TAB}
UP ARROW	{UP}
F1	{F1}
F2	{F2}
F3	{F3}
F4	{F4}
F5	{F5}
F6	{F6}
F7	{F7}

F8	{F8}
F9	{F9}
F10	{F10}
F11	{F11}
F12	{F12}
F13	{F13}
F14	{F14}
F15	{F15}
F16	{F16}
Keypad add	{ADD}
Keypad subtract	{SUBTRACT}
Keypad multiply	{MULTIPLY}
Keypad divide	{DIVIDE}

To specify keys combined with any combination of the SHIFT, CTRL, and ALT keys, precede the key code with one or more of the following codes.

Key	Code
SHIFT	+
CTRL	^
ALT	%

To specify that any combination of SHIFT, CTRL, and ALT should be held down while several other keys are pressed, enclose the code for those keys in parentheses. For example, to specify to hold down SHIFT while E and C are pressed, use "+(EC)". To specify to hold down SHIFT while E is pressed, followed by C without SHIFT, use "+EC".

Special commands

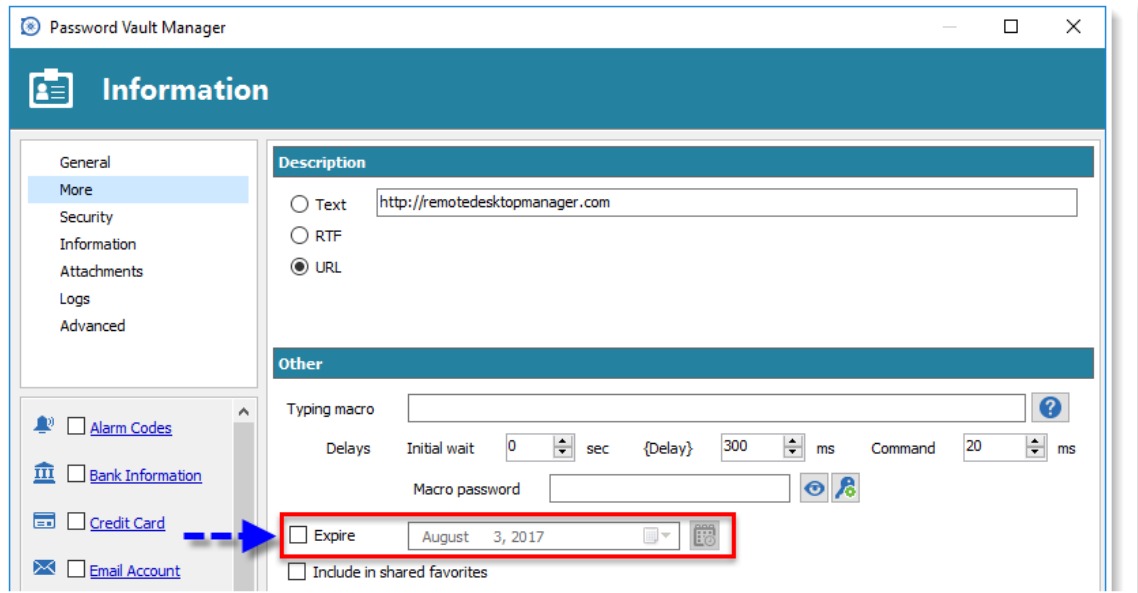
Commands	Description
{DELAY}	This command introduces a small delay of 300 ms (default value) before the next command.
{WINDOW:???	This command focus a window containing the specified name after the semi colon.
{PREV-WINDOW}	Select the previous window before executing the remaining commands.

Macro Password

You can define a password that is to be used within the typing macro exclusively. Use the variable **\$MACRO_PASSWORD\$** to access the password.

Expiration

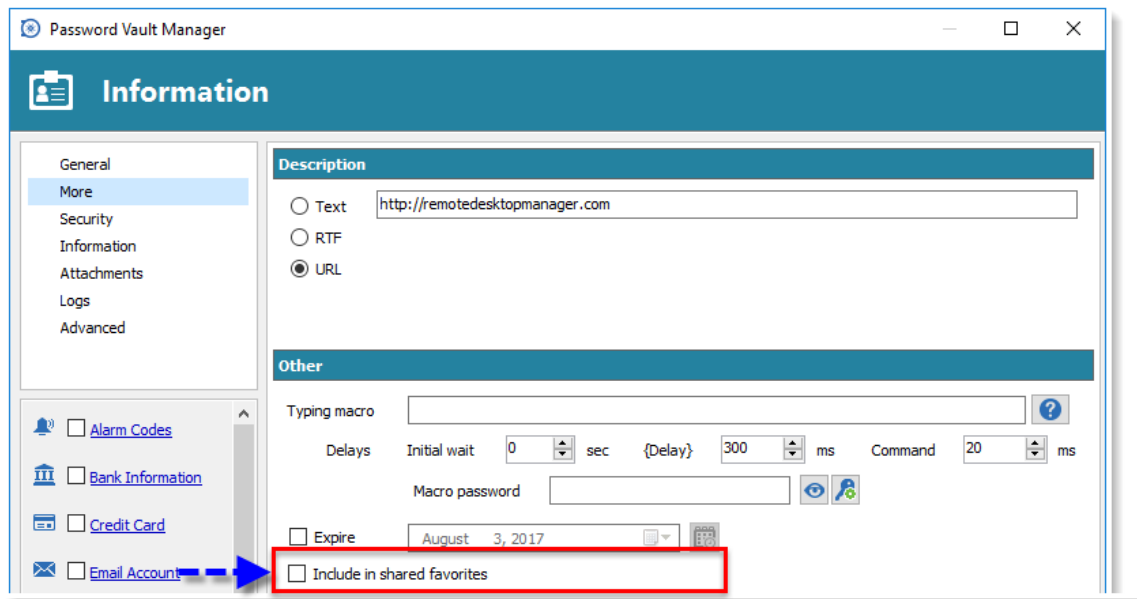
Enter a date to automatically change your entry Status to Expired or to get it listed in the expired session report.



More - Expire

Shared Favorites

Shared favorites are shared by all users who are connected to the data source and are directly configured from the entry. You can include your entry in your shared favorites. For more information please see [Favorite](#).

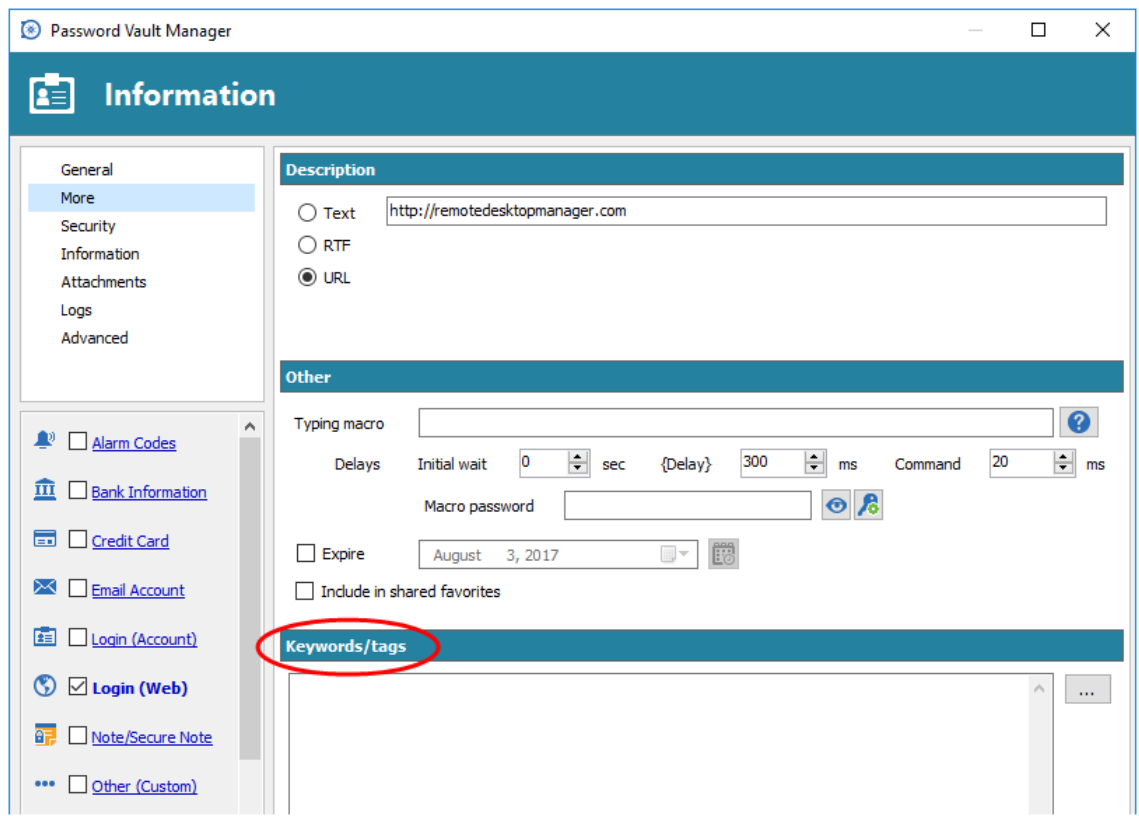


More - Include in shared favorites

5.1.2.3 Keywords/Tags

Description

Add keywords or tags for easier search.

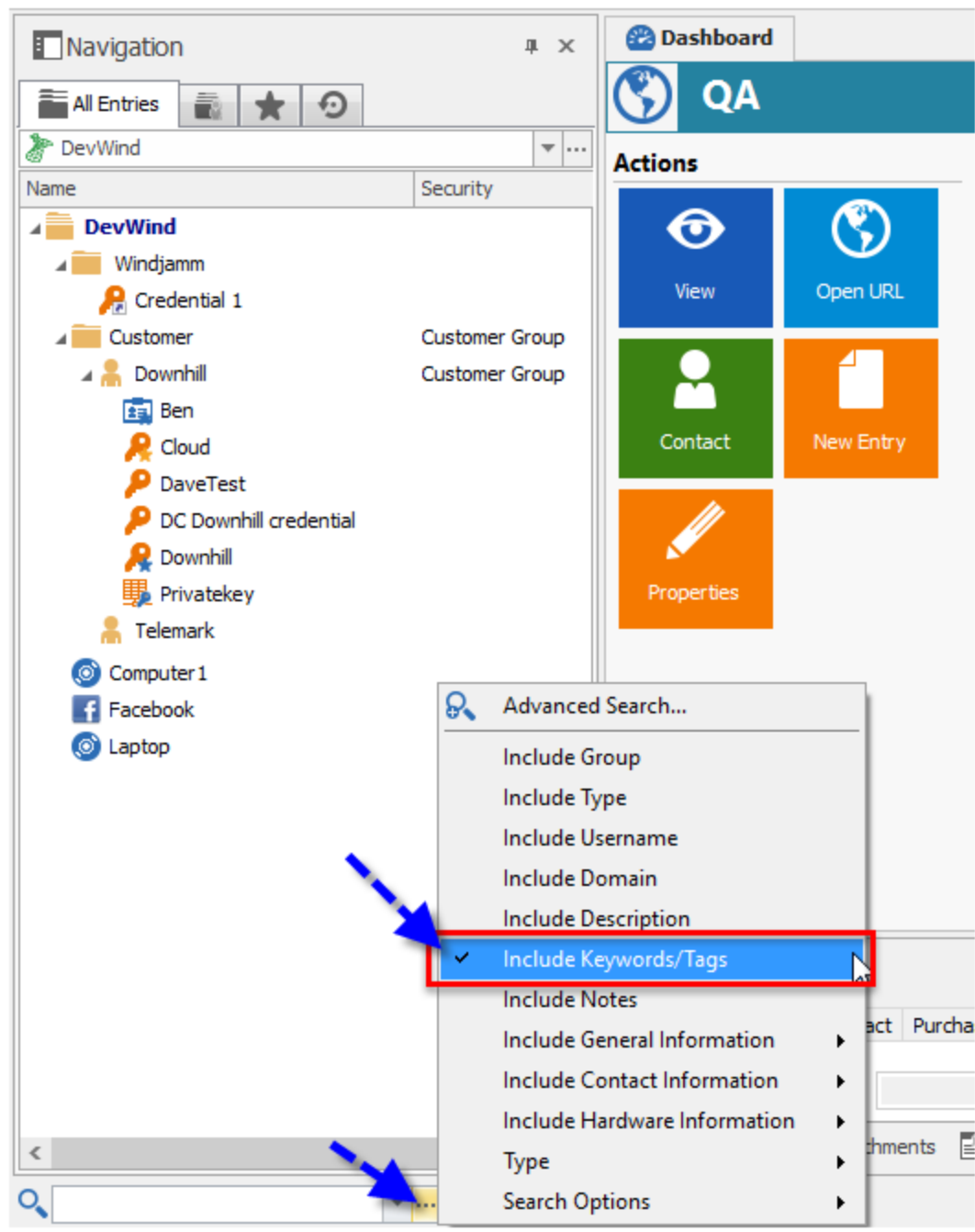


More - Keywords/tags

Settings

Searching

The Keywords/Tags option must be enable in your search filter.

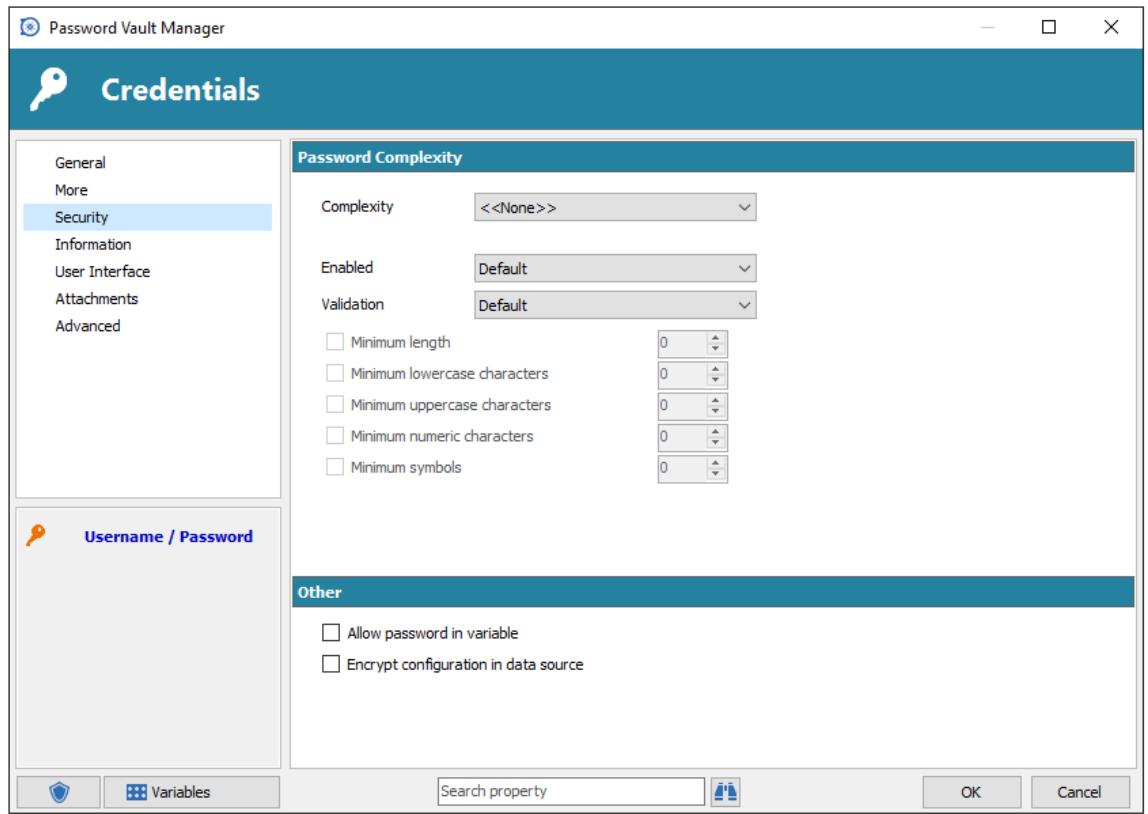


Search Filter - Include Keywords/Tags

5.1.3 Security

Description

The **Security** tab is used to determine whether passwords must meet predetermined complexity requirements that has been configured. [Password Complexity](#) requirements are enforced when passwords are changed or a new entry is created.



Security Section

Settings

Password Complexity

To learn more about Password Complexity please follow this [link](#).

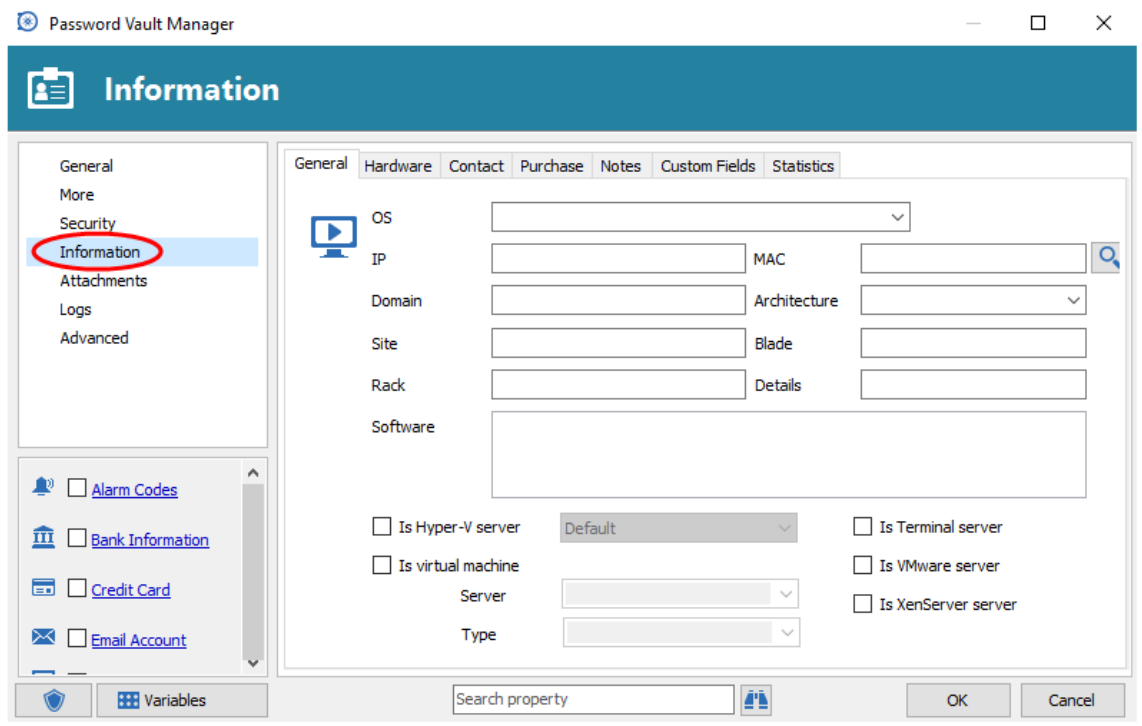
Other

Option	Description
Allow password in variable	You must enable this setting for the \$PASSWORD\$ variable to be available with the command line.
Encrypt configuration in data source	Encrypt your session configuration in your data source.

5.1.4 Information

Description

The **Information** side menu contains general information regarding your computer, software, hardware, expiration warranty, etc...



Please consult the following topics for more information:

- [General](#)
- [Hardware](#)
- [Contact](#)
- [Purchase](#)
- [Notes](#)
- [Custom Fields](#)
- [Statistics](#)

5.1.4.1 General

Description

The **General** tab allows you to enter specific information regarding the computer, such as operating system, MAC address and hardware description. This will also enable certain actions within the dashboard.

The screenshot shows the 'General' tab of the Password Vault Manager interface. It features a navigation bar with tabs: General, Hardware, Contact, Purchase, Notes, Custom Fields, and Statistics. The main form area contains the following fields and options:

- OS:** A dropdown menu showing 'Windows Server 2012'.
- IP:** A text input field containing '192.168.0.0'.
- MAC:** A text input field containing '00:0C:00:00' with a search icon to its right.
- Domain:** A text input field containing 'Windjam'.
- Architecture:** A dropdown menu showing '32-bit'.
- Site:** An empty text input field.
- Blade:** An empty text input field.
- Rack:** An empty text input field.
- Details:** An empty text input field.
- Software:** A list box containing 'Remote Desktop Manager', 'TightVNC', and 'Microsoft Visual C++'.
- Is Hyper-V server:** An unchecked checkbox.
- Is Terminal server:** An unchecked checkbox.
- Is virtual machine:** An unchecked checkbox.
- Is VMware server:** An unchecked checkbox.
- Is XenServer server:** An unchecked checkbox.
- Server:** A dropdown menu with 'Default' selected.
- Type:** An empty dropdown menu.

Information - General tab

Option	Description
OS	Specify the remote computer Operating System. You can type another value if it's not listed.
IP	Specify the IP address of the remote computer.
MAC	Contains the remote computer MAC address.
Domain	Specify the remote computer domain name.
Architecture	Specify the processor architecture between 32-bit or 64-bit.
Site	Indicate the physical site where the remote computer is located.
Blade	Indicate remote computer blade location.
Rack	Indicate in which rack the device is located.
Details	Indicate the details where the device is located.
Software	List all software installed on the remote computer.
Is Hyper-V server	Indicate if the entry is a Hyper-V server and enable Hyper-V console in the footer.
Is Terminal server	Indicate if the entry is a Terminal Server and enable Terminal console in the footer.
Is virtual machine	Indicate if the entry is a virtual machine. You can specify the name as well.
Is VMware server	Indicate if the entry is a VMware server and enable VMware console in the footer.
Is XenServer server	Indicate if the entry is a XenServer and enable XenServer console in the footer.

5.1.4.2 Hardware

Description

The **Hardware** tab allows you to specify the hardware information of the remote computer.

Settings

Information - Hardware

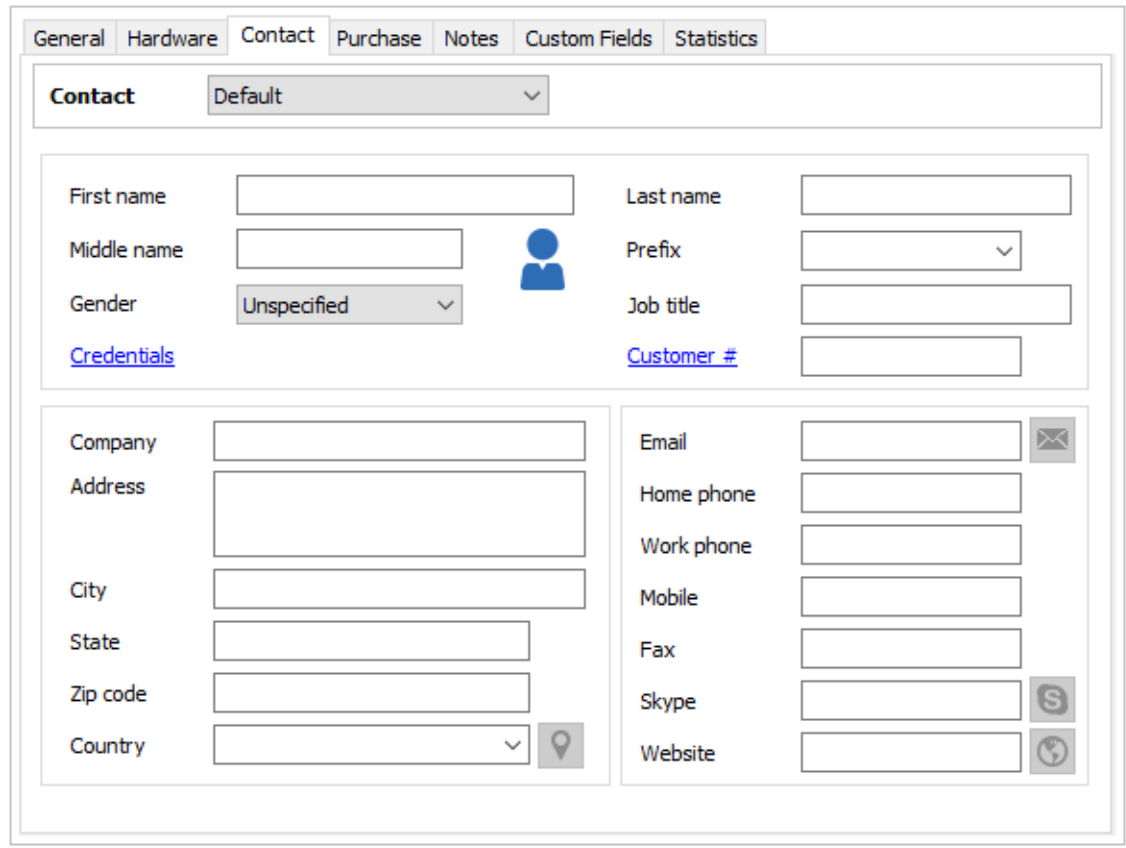
Option	Description
CPU	Indicate the remote computer CPU model.
CPU core count	By default the CPU core count is at one but can be modify here if you have more than one.
Logical CPU count	By default the Logical CPU count is at one but can be modify here if you have more than one.
Memory	Indicate the remote computer memory amount and the memory type as well.
Monitors	Used to enumerate the list of monitors and the models.
Drives	Indicate the remote computer Drives.
Asset Tag	Indicate the remote computer asset tag.
Details	Indicate any other details related to the hardware. For example it could be the video card or the hard disk sizes.

5.1.4.3 Contact

Description

The **Contact** tab allows you to enter some contact information for the given entry. It is very useful when managing a third party server and it is also possible to link the entry to an existing contact.

Settings

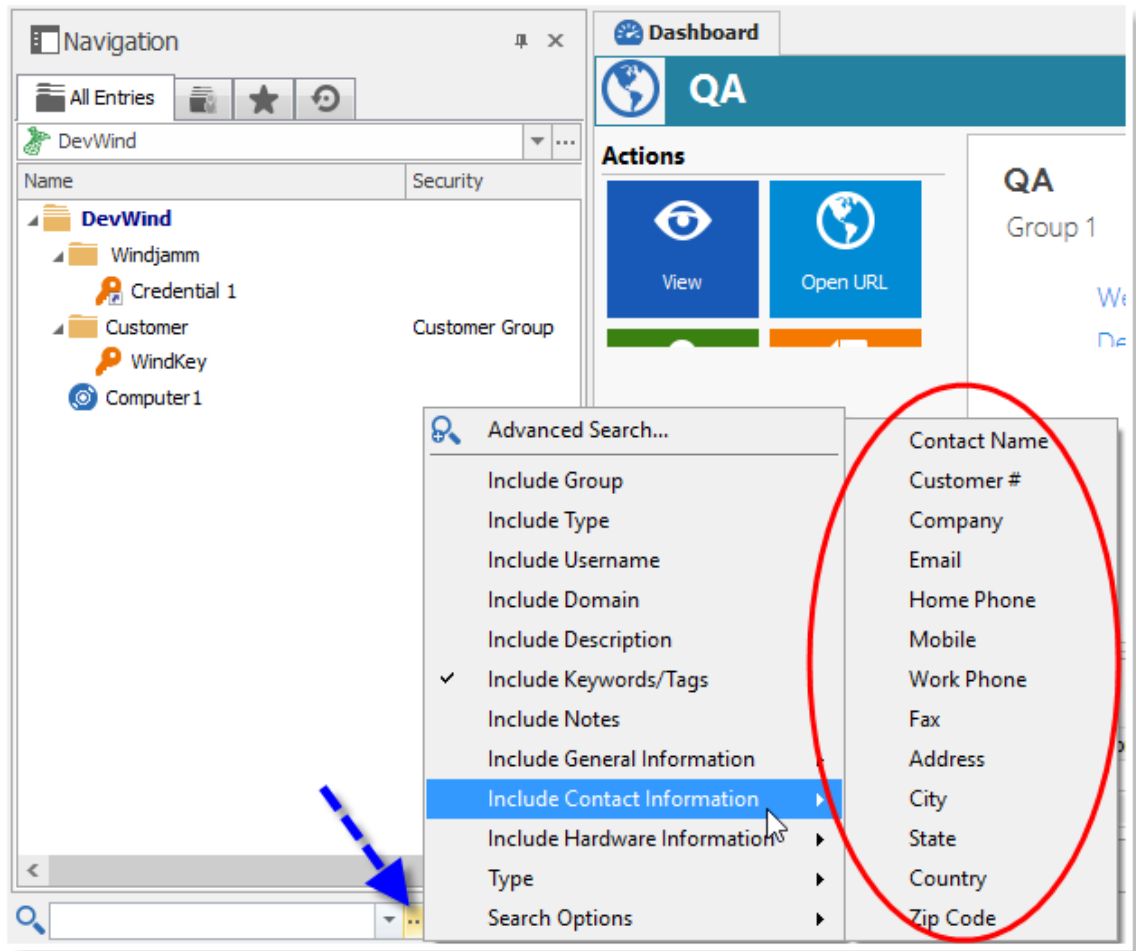


Information - Contact tab

Option	Description
Contact	Select your contact mode between: Default: Enter the contact information directly in the entry. Reference: Associate a contact to a contact entry. The contact information will be displayed in read-only.
Country	Enter the complete contact address in the appropriate fields and the button next to Country will show you the location in Google Maps.
Email	Enter the contact email address and then click on the button next to the field to directly open your default mail application with his email address already in it.
Skype	Enter your Skype contact username and click on the button next to the field to directly contact this person via Skype.
Website	Enter the contact website and click on the button next to the field to go directly on that website.

Searching

When using the **Search/Filter** from the Navigation Pane, most information found in the Contact tab can be used as a search criteria. Please refer to [Search/Filter](#).





Search - Contact Information



5.1.4.4 Purchase

Description

The Purchase tab allows you to enter information related to the invoice or the purchase of the equipment.

Settings

Purchase	
Date	<input type="checkbox"/> 2016-08-04  Age
Vendor	Default  <input type="text"/>
Serial number	<input type="text"/>

Warranty	
Expiration	<input checked="" type="checkbox"/> 2016-06-22   Remaining Overdue
Service tag	<input type="text"/>
Service level	<input type="text"/>

Purchase

Option	Description
Date	Indicate the equipment purchase date.
Vendor	Specify the name of the vendor who sold the equipment.
Serial number	Indicate the serial number associated to the equipment.

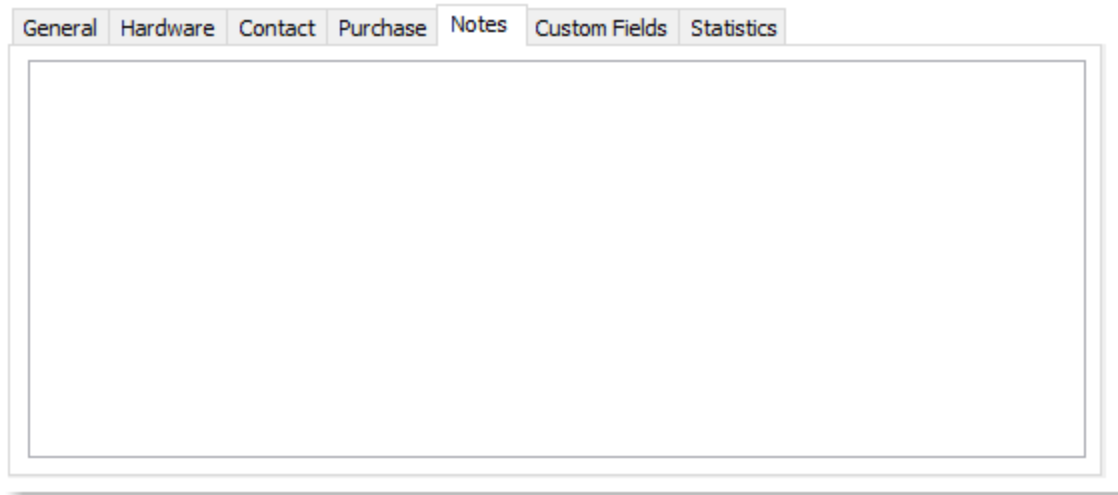
Warranty

Option	Description
Expiration	Specify the expiration date of the warranty. This is used when generating an Expired warranty report .
Service tag	Indicate the equipment service tag.
Service level	Indicate the technical service level purchased for this equipment.

5.1.4.5 Notes

Description

The **Notes** tab allows you to enter any text related to the entry.



Information - Notes tab

5.1.4.6 Custom Fields

Description

The **Custom fields** allows for defining custom properties and values that can then be accessed via variables (\$CUSTOM_FIELD1\$, \$CUSTOM_FIELD2\$, etc.) in child connections or Macros/Scripts/Tools.

Custom field 1, 2 & 3 can be encrypted for enhanced security. When used with an advanced data source users must have reveal password capabilities to be able to decrypt and view the value.



Custom field 1, 2 and 3 can be encrypted for enhanced security. When used with an [Advanced Data Source](#) users must have reveal password capabilities to be able to decrypt and view the value. Click on the small checkbox beside the text field to protect the content.



You must be an administrator or have reveal password privileges to see the protected values.

Settings

The field can be renamed to your liking, just click on the hyperlink to display a dialog to enter a new name.

Encryption of Custom Fields 1,2 and 3 are controlled by these check boxes

Information - Custom Fields tab

5.1.4.7 Statistics

Description

The Statistics tab provides different information about the entry including:

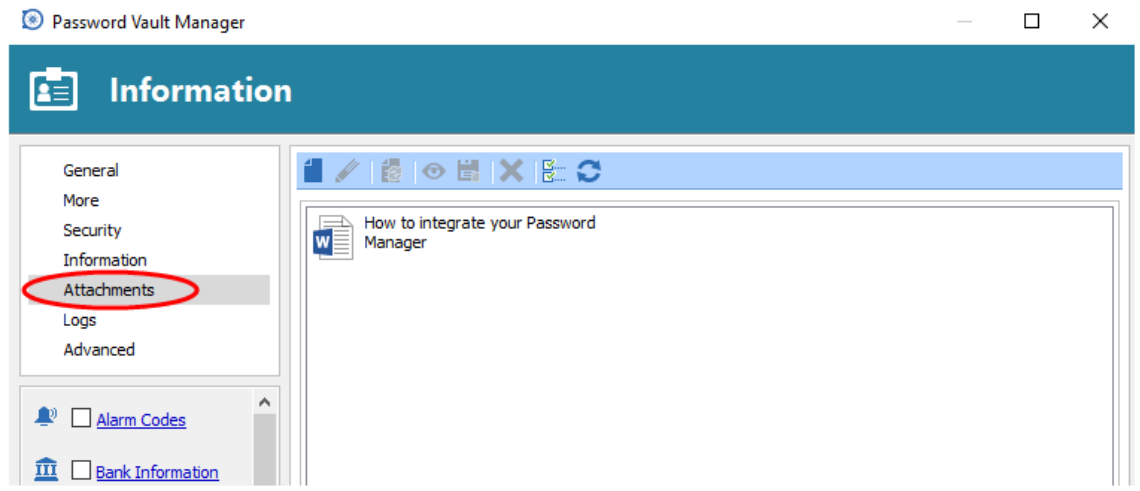
- The user who created the entry
- The entry creation date
- The user who performed the last update on the entry
- The last date the entry was updated

Information	
Created by	VDEVOLUTIONS
Creation date	2016-07-11 11:05 AM
Last update by	VDEVOLUTIONS
Last update date	2016-08-03 4:04 PM

5.1.5 Attachments

Description

With the Enterprise edition and an [Advanced Data Source](#), you can add attachments to entries and the file will be stored directly in the database. Please note that the file will not be available in [Offline Mode](#).



Information - Attachments

Attachments can be of any types and of any sizes, depending on your bandwidth and database. You can also view a saved attachment from: the session context menu, the session properties or directly on the dashboard.

The update button will allow you to update directly your selected document instead of deleting it. Use it to save your local modifications after an edit.

5.1.6 Events

Description

Password Vault Manager offers you the flexibility to run operations before or after establishing a connection.

The operations are defined via the **Events** tab of the session properties window. Define a script or a command line that will be executed at the appropriate time and it will automatically execute the parameters, such as the session ID, the session name, or the configured user name. For example, this can be used to execute a batch file or an external application that prompts the user for more information or to update a log on an external server.

Settings

Before Connect

Before Connect After Connect Before Disconnect After Disconnect

Before connect

Command line

Command

Wait for exit Use default working directory Wait timeout

Run as Administrator Run in 64-bit mode Post execution pause

Miscellaneous

Power On Mode

Wait timeout sec

Retry count

Events - Before connect

Option	Description
None	No script, command line or message prompt is executed before the connection.
Script	Select a script that will be executed before the opening of the session.
Command Line	Enter a command line that will be executed before the opening of the session.
Message Prompt	Enter a message that will be prompted before the connection.
Passcode	Enter a passcode to access the session after the message prompt.
Wait for exit	Activate the waiting time before disconnecting on a timeout.
Run as administrator	Execute the script as an administrator.
Use default working directory	Use the default working directory when connected to the session.
Run in 64 bits mode	Execute the script in 64 bits mode
Wait timeout	Enter the time (in seconds) to disconnect when there is a timeout.
Post execution pause	Pause the process that is currently running. This is sometime necessary in order to allow the process to complete a task.
Power On Mode	Select between None and WakeonLAN. If your trying to send a command to a close computer it will open WakeonLan with a define timeout and the number of time to retry.



With **Before connect** events the only scripting file format is VBScript (.vbs).

After Connect

Before Connect | **After Connect** | Before Disconnect | After Disconnect

After connect



None

After connect - Macro

Execute automatically Initial wait 0 sec

Default

Typing macro ?

Macro password   Delay time {Delay} 300 ms

Command 20 ms

Event - After Connect

Option	Description
Execute automatically	Execute the macro or the link automatically when session is connected.
Initial wait	Enter the waiting time before the macro start to run.
Link	Link a predefined Macros/Scripts/Tools entry type to the session.
Default	Select Default to activate the typing macro.
Typing macro	Please consult topic Auto Typing Macro .
macro password	Enter a password to execute the macro.
Delay time	Enter the delay time for the macro to run.

Before Disconnect



With **Before disconnect** events the only scripting file format is VBScript (.vbs).

Before Connect After Connect **Before Disconnect** After Disconnect

Before disconnect

Command line

Command

Wait for exit Use default working directory Wait timeout

Run as Administrator Run in 64-bit mode Post execution pause

Event - Before Disconnect

Option	Description
None	No script, command line or message prompt is executed before disconnecting.
Script	Select a script that will be executed before disconnecting to the session.
Command Line	Enter a command line that will be executed before disconnecting to the session.
Message Prompt	Enter a message that will be prompt before disconnecting.
Passcode	Enter a passcode to disconnect after the message prompting.
Wait for exit	Will activate the waiting time before disconnecting on a timeout.
Run as administrator	Execute the script as an administrator.
Use default working directory	Use the default working directory when connected to the session.
Run in 64 bits mode	Execute the script in 64 bits mode
Wait timeout	Enter the time (in seconds) to disconnect when there is a timeout.
Post execution pause	Pause the process that is currently running. This is sometimes necessary in order to allow the process to complete a task.

After Disconnect

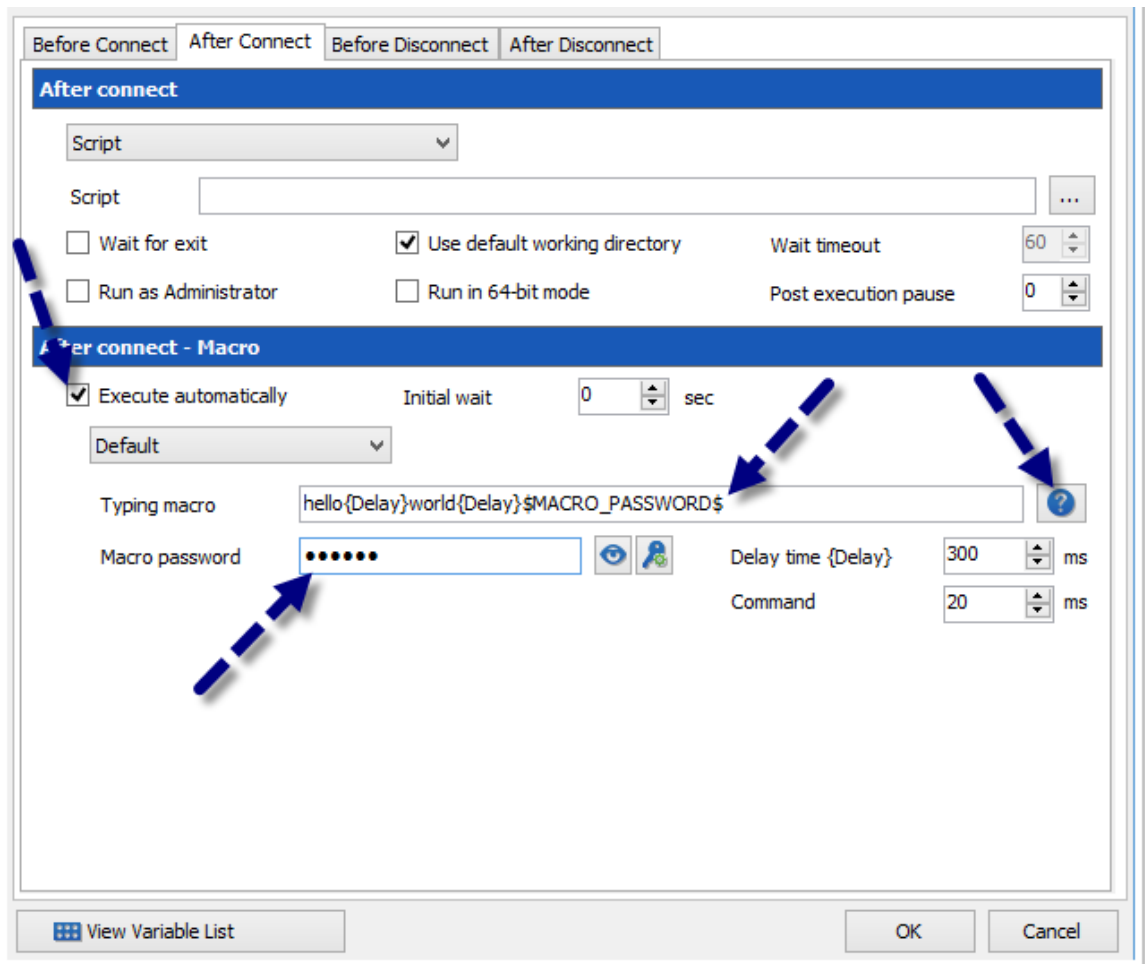
Event - After Disconnect

Option	Description
None	No script, command line or message prompt is execute after disconnect.
Script	Select a script that will be execute when the session will be disconnect.
Command Line	Enter a command line that will be execute when the session will be disconnect.
Message Prompt	Enter a message that will be prompt at disconnect.
Wait for exit	Will active the waiting time before disconnect on a timeout.
Run as administrator	Execute the script as an administrator.
Use default working directory	Use the default working directory when disconnect from the session.
Run in 64 bits mode	Execute the script in 64 bits mode
Wait timeout	Enter the time (in seconds) to disconnect when there a timeout.
Post execution pause	Pause the process that currently running. This is sometimes necessary in order to allow the process to complete a task.

5.1.6.1 Auto Typing Macro

Description

The Auto Typing Macro allows you to automatically execute a typing macro once a session has been established.



Auto typing macro

Settings

Typing Macro

Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. For example, to represent the letter A pass in the string "A" to the method. To represent more than one character, append each additional character to the preceding one. To represent the letters A, B, and C specify the parameter as "ABC".

Special keys

To specify characters that aren't displayed when you press a key, such as ENTER or TAB, as well as the keys that represents actions rather than characters. Refer to the codes in the following table.

Key	Code
BACKSPACE	{BACKSPACE}, {BS}, or {BKSP}
BREAK	{BREAK}
CAPS LOCK	{CAPSLOCK}

DEL or DELETE	{DELETE} or {DEL}
DOWN ARROW	{DOWN}
END	{END}
ENTER	{ENTER}
ESC	{ESC}
HELP	{HELP}
HOME	{HOME}
INS or INSERT	{INSERT} or {INS}
LEFT ARROW	{LEFT}
NUM LOCK	{NUMLOCK}
PAGE DOWN	{PGDN}
PAGE UP	{PGUP}
PRINT SCREEN	{PRTSC}
RIGHT ARROW	{RIGHT}
SCROLL LOCK	{SCROLLLOCK}
TAB	{TAB}
UP ARROW	{UP}
F1	{F1}
F2	{F2}
F3	{F3}
F4	{F4}
F5	{F5}
F6	{F6}
F7	{F7}
F8	{F8}
F9	{F9}
F10	{F10}
F11	{F11}
F12	{F12}
F13	{F13}
F14	{F14}
F15	{F15}
F16	{F16}
Keypad add	{ADD}
Keypad subtract	{SUBTRACT}

Keypad multiply	{MULTIPLY}
Keypad divide	{DIVIDE}

To specify keys combined with any combination of the SHIFT, CTRL, and ALT keys, precede the key code with one or more of the following code.

Key	Code
SHIFT	+
CTRL	^
ALT	%

To specify that any combination of SHIFT, CTRL, and ALT should be held down while several other keys are pressed, enclose the code for those keys in parentheses. For example, to specify to hold down SHIFT while E and C are pressed use "+(EC)". To specify to hold down SHIFT while E is pressed, followed by C, without SHIFT, use "+EC".

Special commands

Commands	Description
{DELAY}	This command introduces a delay of 300 ms (default value) before the next command.
{WINDOW:???	This command focus a window containing the specified name after the semi colon.
{PREV-WINDOW}	Select the previous window before executing the remaining commands.

Macro Password

You can define a password to be use within the typing macro exclusively. Use the variable **\$MACRO_PASSWORD\$** to access the password.

5.1.7 Logs

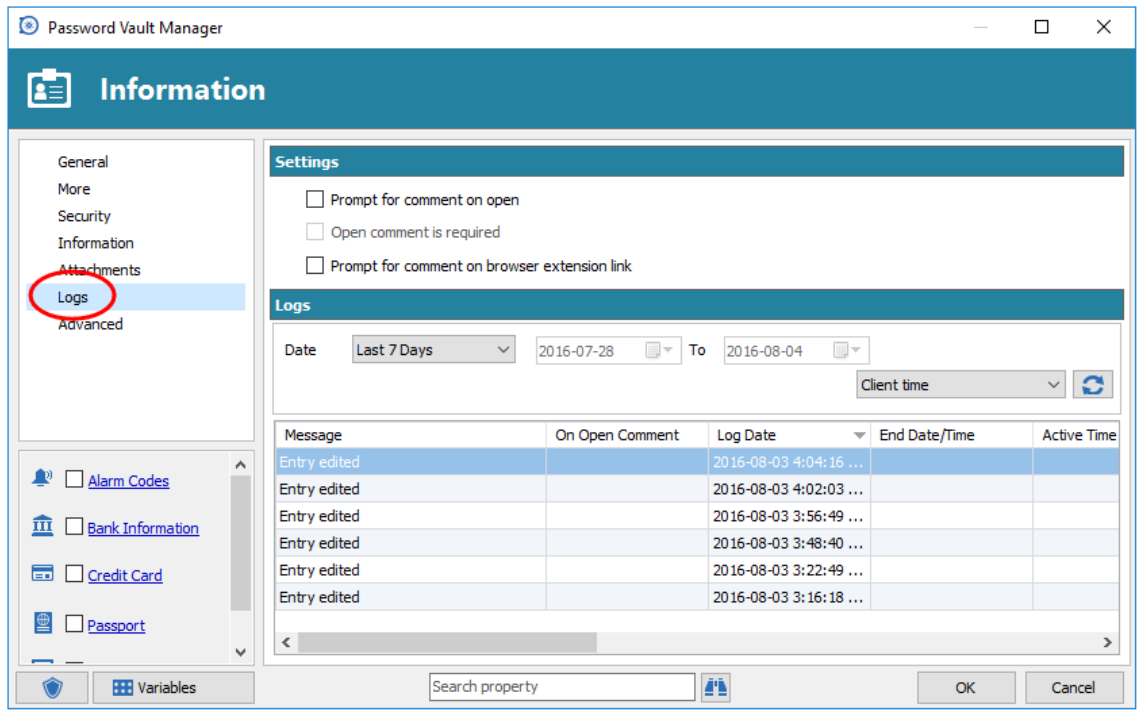
Description



This feature requires an [Advanced Data Sources](#).


The Logs tab displays the usage/edition logs for the entry.

Settings



Information - Logs

There are options to prompt for comments, required or not, when an entry is opened.



The open comments are supported in [embedded and in external mode](#).

Settings

Option	Description
Prompt for comment on open	The program will prompt you for a comment when you open the session. The comment will appear in the log.
Open comment is required	Force the user to enter an Open session comment.
Prompt for comment on close	The program will prompt you for a comment when you close the session. The comment will appear in the log.

Logs

Option	Description
Date drop down menu	Choose the period of interest to you. You can select custom in order to enter specific dates.
Date time edit controls	Enabled when the date drop down is at Custom. Enter the start date and end date in the controls.

Time	Choose between Client Time, Local Time and UTC Time. Useful for distributed systems.
Refresh	Perform a manual refresh using the Refresh button.

Right click on the log entry to display the contextual menu to show the log details form, refer to Log Details for information on that form.

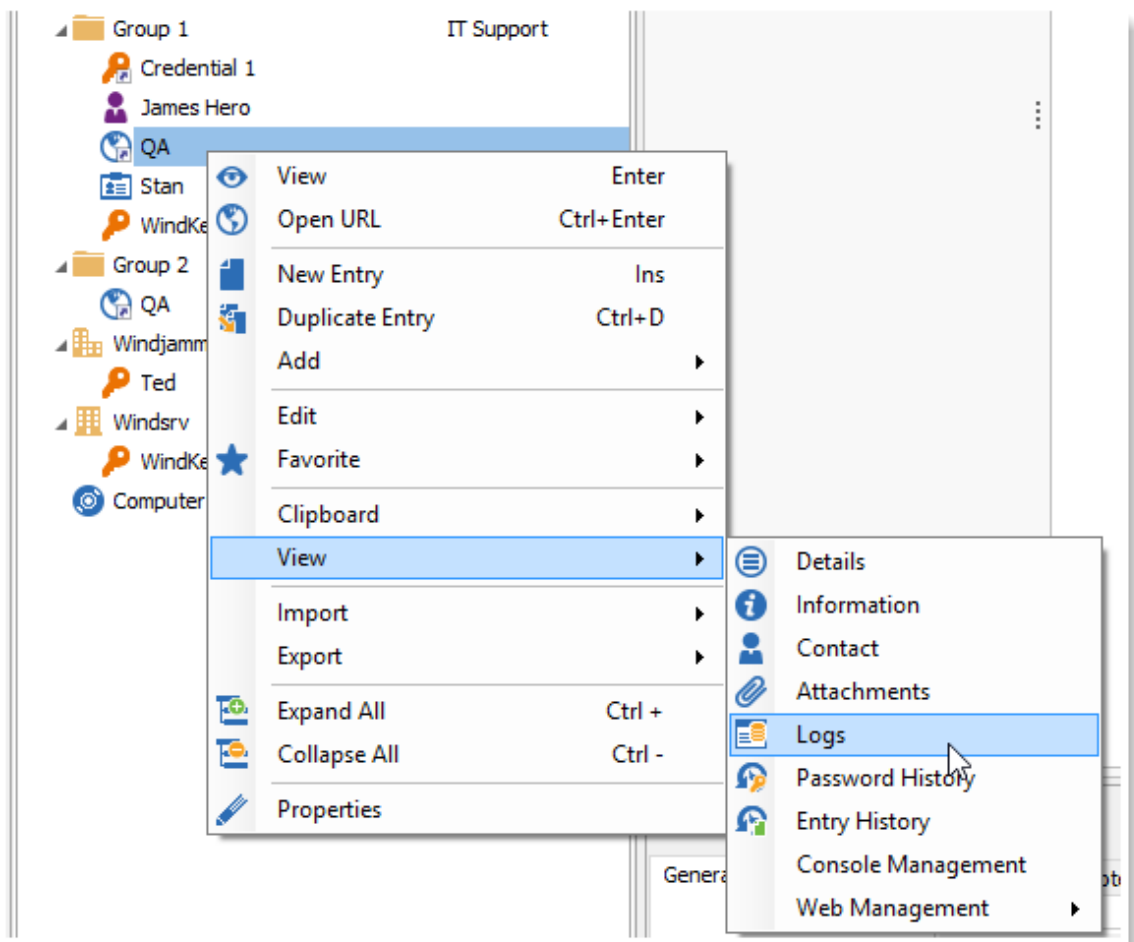
5.1.7.1 View Logs

Description



This feature requires an [Advanced Data Sources](#).

Allows for viewing session activity logs. The log viewer displays information about entry activity. Things like open session durations, open/close comments, user who performed the action and action time.



Entry View - Logs

Message	On Open Comment	Log Date	End Date/Time	Active Time	Duration	On Close Comment
Entry edited		2016-08-03 4:04:16 ...				
Entry edited		2016-08-03 4:02:03 ...				
Entry edited		2016-08-03 3:56:49 ...				
Entry edited		2016-08-03 3:48:40 ...				
Entry edited		2016-08-03 3:22:49 ...				
Entry edited		2016-08-03 3:16:18 ...				

Entry Log

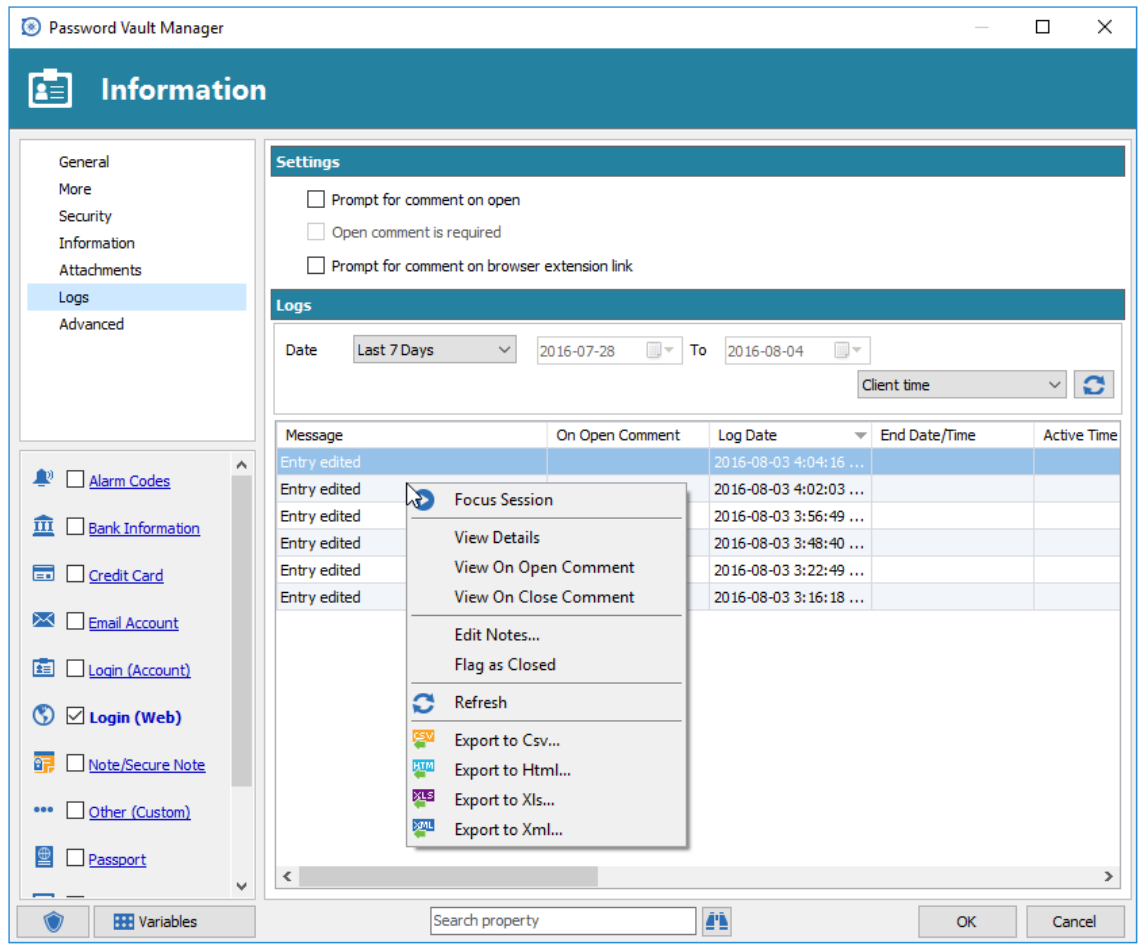
Right click on the log entry to display the contextual menu to show the log details form, refer to Log Details for information on that form.

5.1.7.2 Log Details

Description

When viewing an entry usage log, either in the entry [Logs](#) or in the [View Logs](#) (Accessible via **View - View Usage Log (Database)**) you are presented with a contextual menu.

Settings



Log Entry Contextual menu

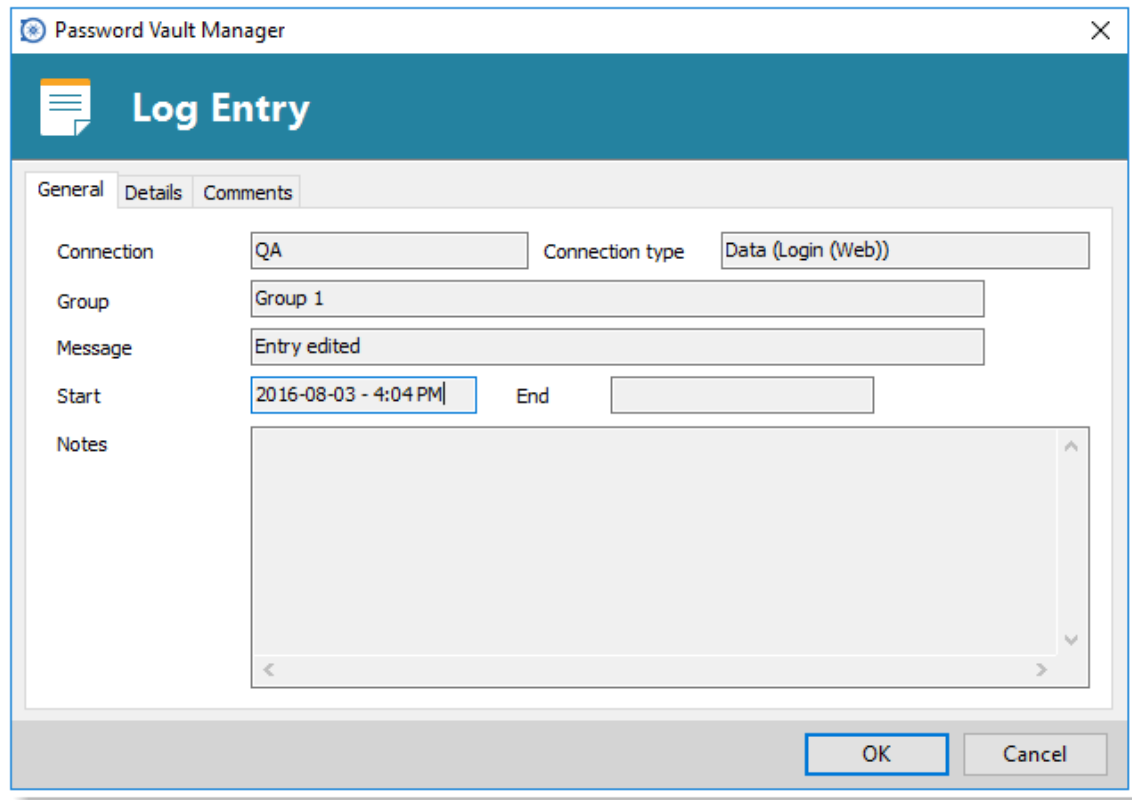
Option	Description
Focus Session	Set the focus on the corresponding entry in the navigation tree view.
View Details	Display the information window for the log entry.
View On Open Comment	Display the Open comment in a simplified window.
View on Close Comment	Display the Close comment in a simplified window.
Edit Notes	Edit the log entry note in a simplified window.
Flag as Closed	Enabled only for open entries, it will force the status to Closed.
Refresh	Performs a refresh of the log entry
Export to Csv	Opens a dialog to export the content of the grid to a Csv file.
Export to Html	Opens a dialog to export the content of the grid to a Html file.
Export to Xls	Opens a dialog to export the content of the grid to a Xls file.
Export to Xml	Opens a dialog to export the content of the grid to a Xml file.

View Details window

The View Details window has three tabs: **General**, **Details** and **Comments**.

General Tab

The **General** tab displays session information to identify the entry and also displays the session running time. Notes can be entered using the contextual menu in the log entry grid.



The screenshot shows the 'Log Entry' window in Password Vault Manager, with the 'General' tab selected. The window title is 'Password Vault Manager' and the main title is 'Log Entry'. The 'General' tab is active, showing the following fields:

Connection	QA	Connection type	Data (Login (Web))
Group	Group 1		
Message	Entry edited		
Start	2016-08-03 - 4:04 PM	End	
Notes	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>		

At the bottom right, there are 'OK' and 'Cancel' buttons.

Log Entry - General

Details tab

The **Details** tab display information on the User and computer from which the session was started, and on the destination host. It also displays information if the session was forcibly closed using the Close menu.

The screenshot shows a window titled "Password Vault Manager" with a "Log Entry" header. Below the header are three tabs: "General", "Details", and "Comments". The "Details" tab is active and contains the following fields:

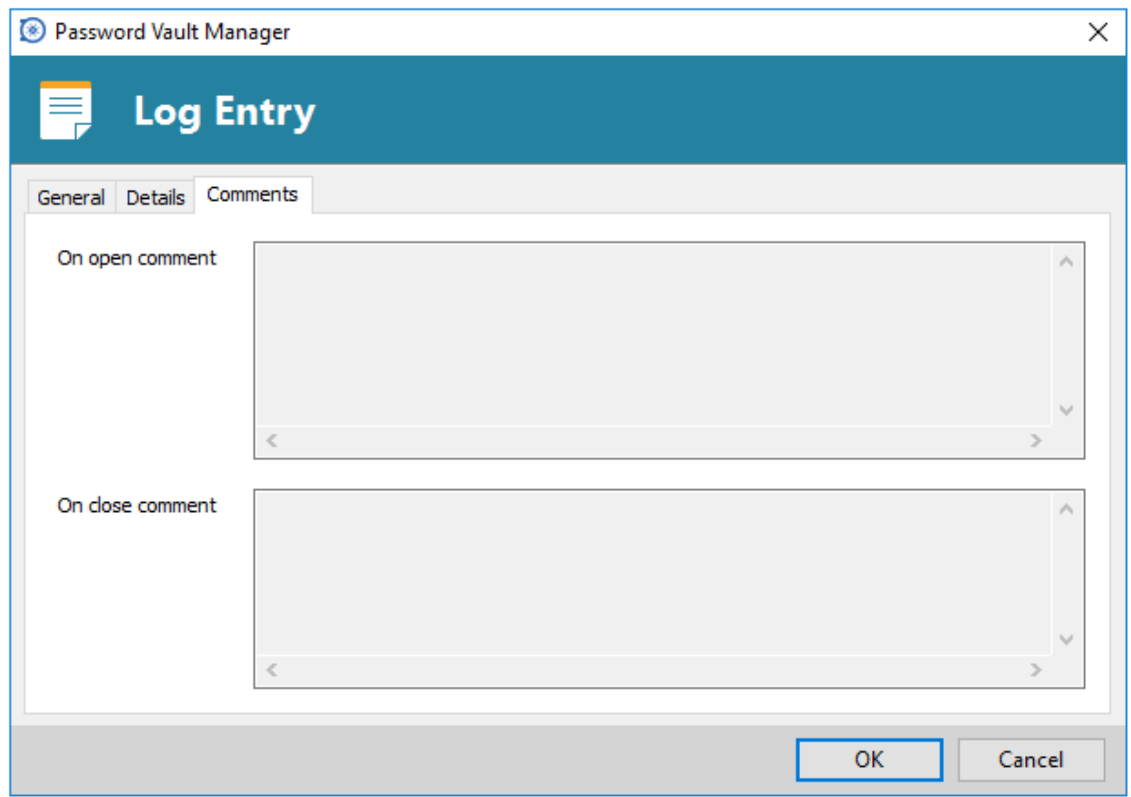
Username	VDEVOLUTIONS56\jkafo		
Database username	David		
Machine name	VDEVOLUTIONS56		
Message type	Edit Session	Application	Password Vault Manager
Host		Version	7.6.2.0
Manual Close Information			
Closed by			
Close time			

At the bottom right of the dialog are "OK" and "Cancel" buttons.

Log Entry - Details

Comments tab

The ***Comments*** tab displays the ***On Open comment*** and ***On Close comment***.



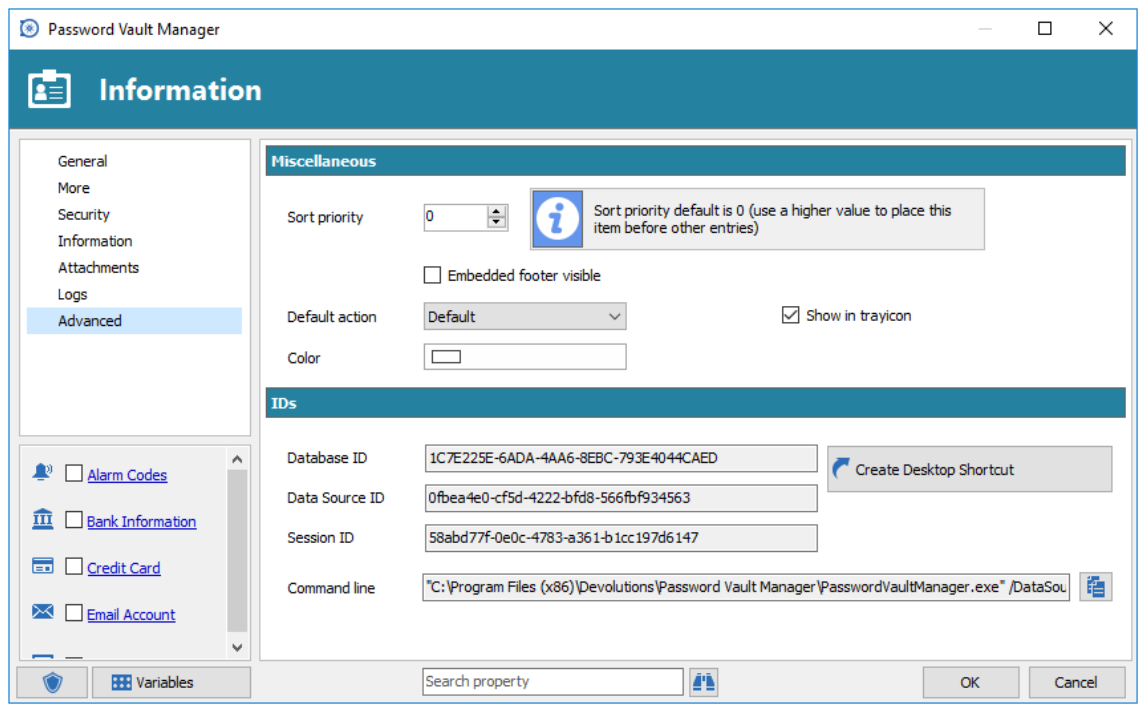
Log Entry - Details

5.1.8 Advanced

Description

The **Advanced** tab contains advanced settings related to the session, such as the internal data source ID and session ID. These values can be used to invoke Password Vault Manager from a command line to open the session or to run a batch modification.

Settings



Information - Advanced

Miscellaneous

Option	Description
Sort priority	Sort priority allows you to place your entry before other entries in your treeview. The higher the value the entry will be.
Embedded footer visible	In embedded mode make the footer visible.
Default action	All entry types have a default action associated with them, this action is executed on "Open", but you can modify it for certain entry types. You may specify different options, such as: <ul style="list-style-type: none"> • Default • View Entry • Open URL (embedded, external or default) • Copy Password • View dashboard • Edit
Color	Select a tab color for your entry when opened using the embedded mode.

IDs (Used in a Command line or in PowerShell scripts)

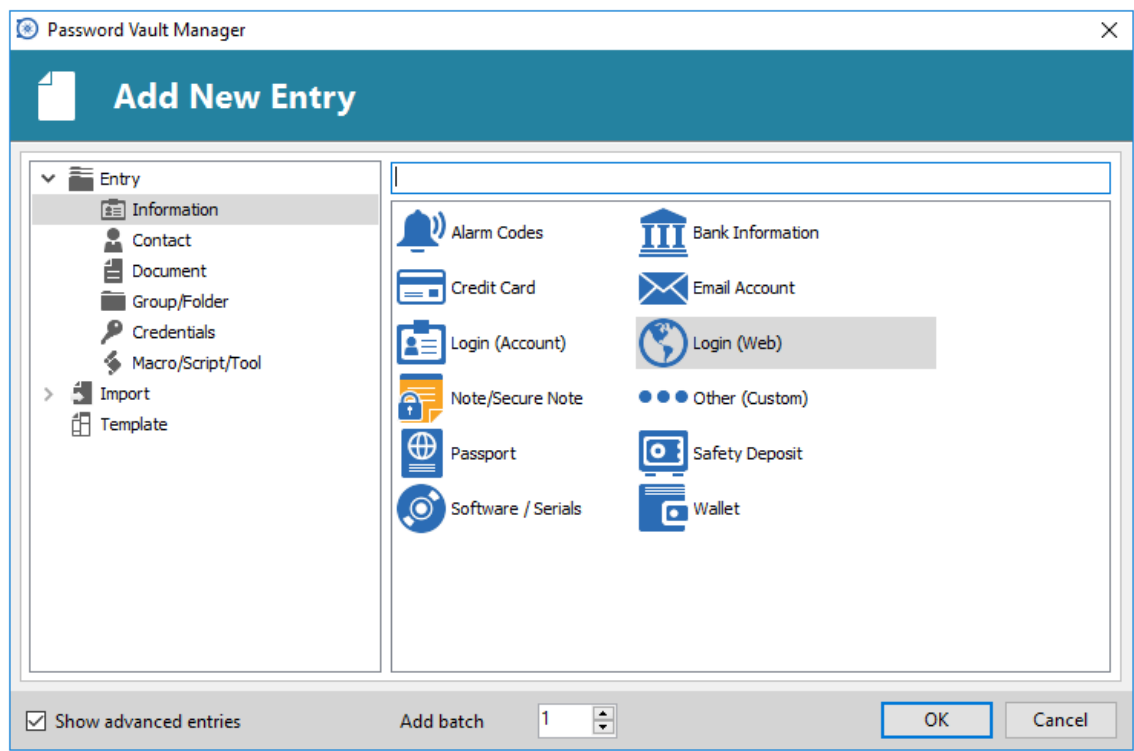
Option	Description
Database ID	Internal PVM database ID. Used as a Command Line Arguments or when using PowerShell extensions.
Data Source ID	Internal PVM data source ID. Used as a Command Line Arguments or when using PowerShell extensions.

Session ID	Internal PVM session ID. Used as Command Line Arguments or when using PowerShell extensions.
Command Line	Fully defined command line to start this entry via a command line. Hit the copy button to copy the entire command line.
Create Desktop Shortcut	Automatically create a Password Vault Manager shortcut on your desktop.

5.2 Information

Description

Information entry types are used to store sensitive information like alarm codes information, serial numbers, credit card information and more into the data source.



Add a new Information entry

Refer to these topics for more information:

- [Alarm Codes](#)
- [Bank Information](#)
- [Credit Card](#)
- [Email Account](#)
- [Login \(Account\)](#)
- [Login \(Web\)](#)
- [Note/Secure Note](#)
- [Other \(Custom\)](#)
- [Passport](#)

- [Safety Deposit](#)
- [Software / Serials](#)
- [Wallet](#)

5.2.1 Alarm Codes

Description



The **Alarm Codes** data entry type is used for securely storing employee/alarm code pairings.

Settings

Alarm Codes

Name	Alarm Code	Employee Code
Bryan	*****	123

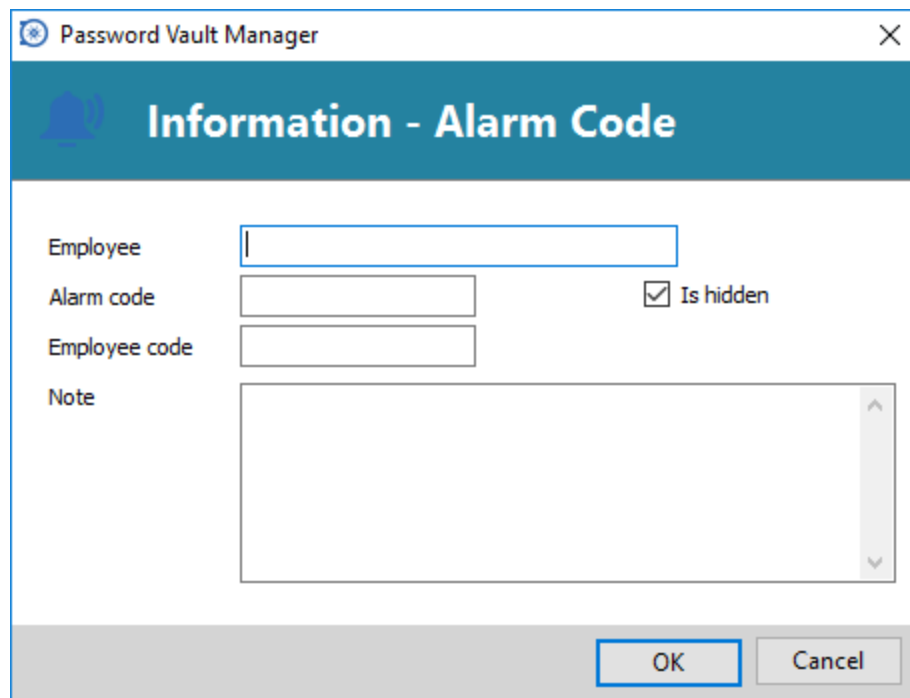
Alarm Codes entry

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Employee		The employee name
Alarm code	✔	The alarm code
Is hidden		Is the alarm code hidden (secure). On export a hidden alarm code will be encrypted
Employee code		The employee code
Note		Alarm code note

Actions

Click on **Add** to create a new Alarm Code entry and fill in the fields.



The screenshot shows a dialog box titled "Password Vault Manager" with a close button (X) in the top right corner. The main heading is "Information - Alarm Code". Below the heading, there are four input fields: "Employee" (a single-line text box), "Alarm code" (a single-line text box with a checked checkbox labeled "Is hidden" to its right), "Employee code" (a single-line text box), and "Note" (a multi-line text area with a vertical scrollbar on the right). At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

5.2.2 Bank Information


Description



The **Bank Information** entry is useful for storing sensitive banking information such as account number and PIN.

Settings

Bank Information



Bank name


Bank branch

Account type

Account owner

Account number

Routing number

PIN 

SWIFT

Phone

Address

Contact

Bank Information

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Bank name		Reference bank name
Bank branch		Reference bank branch
Account type		Type of account
Account owner		The name of the owner of the account
Account number		Bank account number
Routing number		Insert the routing number
PIN	✓	Bank account PIN number
SWIFT		Enter your SWIFT account number
Phone		Bank phone number
Address		Bank address
Contact		Bank contact

5.2.3 Credit Card


Description



The **Credit Card** data entry is useful for storing sensitive credit card information such as card number, PIN or CVC.

Settings

Credit Card



Card owner	<input type="text"/>	
Card type	<input type="text" value="v"/>	
Card number	<input type="text"/>	<input type="checkbox"/> Is hidden
Valid from	<input type="text"/> <input type="text"/>	
Expiration	<input type="text"/> <input type="text"/> Validation (CVC)	<input type="text"/>
PIN	<input type="text"/>	
Password	<input type="text"/>	
Verified by	<input type="text"/>	
Secure code	<input type="text"/>	
Issuing bank	<input type="text"/>	
Customer service phone	<input type="text"/>	
International service phone	<input type="text"/>	

Credit Card

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Card owner		Credit card owner as it appears on the actual card
Card type		Card type, choose from the list or type in the card type if it is not available in the list
Card number	✓	Credit card number as it appears on the actual card
Valid from	✓	Valid from date as it appears on the actual card
Expiration	✓	Expiration date as it appears on the actual card
Validation (CVC)	✓	The 3 or 4 digit security code as it appears on the back of the card
PIN	✓	The PIN number for the card
Is hidden		Controls the security information for this card. If hidden is set all secured fields will be encrypted on export and hidden in view mode.
Password	✓	If you have a password that protects your credit card account
Verified by	✓	Name of who it is verified by.
Secure code	✓	Your secure code to have access to your credit card account.
Issuing bank		What bank is your credit card from.
Customer service phone		The customer service phone number.

International service
phone

The International customer service phone number.

5.2.4 Email Account

Description



Securely store email account settings including POP3/IMAP/SMTP servers, user name and passwords.

Settings


General

General

Name	Encrypted	Description
Your name		Account name
Email		Email
S/MIME		Does this email account require/use Secure/Multipurpose Internet Mail Extensions


POP3

Email Account

 General POP3 IMAP SMTP

Host name Port

Username

Password 

SSL


Authentication

POP3

Name	Encrypted	Description
Host name		POP3 host name
Username		POP3 user name
Port		POP3 port, default 110
Password	✓	POP3 password
SSL		POP3 requires SSL connection
Authentication		POP3 authentication mode


IMAP

Email Account

 General POP3 **IMAP** SMTP

Host name Port

Username

Password 

SSL


Authentication

IMAP

Name	Encrypted	Description
Host name		IMAP host name
Port		IMAP port, default 110
Username		IMAP user name
Password	✓	IMAP password
SSL		IMAP requires SSL connection
Authentication		IMAP authentication mode

SMTP

Email Account


 General POP3 IMAP SMTP

Host name Port

My outgoing server (SMTP) requires authentication

Use same settings as my incoming mail server

Username

Password 

SSL

Authentication

SMTP

Name	Encrypted	Description
Host name		SMTP host name
Port		SMTP port, default 110
My outgoing server (SMTP) requires authentication		Does the SMTP server require authentication
Use same settings as my incoming mail server		Use POP3 or IMAP settings for the outgoing server authentication
User name		SMTP user name
Password	✓	SMTP password
SSL		SMTP requires SSL connection
Authentication		SMTP authentication mode

5.2.5 Login (Account)


Description



The **Account** information entry type is used for storing account information including user name, domain and password.

Settings

Login (Account)



Username



Domain

Password

Password only available to administrator

Enable web browser extension link

Compare type Default

[Advanced Settings](#)

Login (Account)

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Username		The user name associated to the account
Domain		The domain associated to the account
Password	✔	The password associated to the account
Password only available to administrator		Must be administrator to be able to view the password
Enable web browser extension link		Data entry will be available for the auto fill feature
Advanced Settings		Manage web advanced settings such as username and password

5.2.6 Login (Web)

Description



The **Web** data entry type is used for storing web site credential information including user name and password.

Settings

Login (Web)

Credentials

Username

Domain

Password

Session specified credentials

▼

Enable web browser extension link

Compare type Default

Password only available to administrator

Template

[Security Questions](#)

[Advanced Settings](#)

Login (Web)

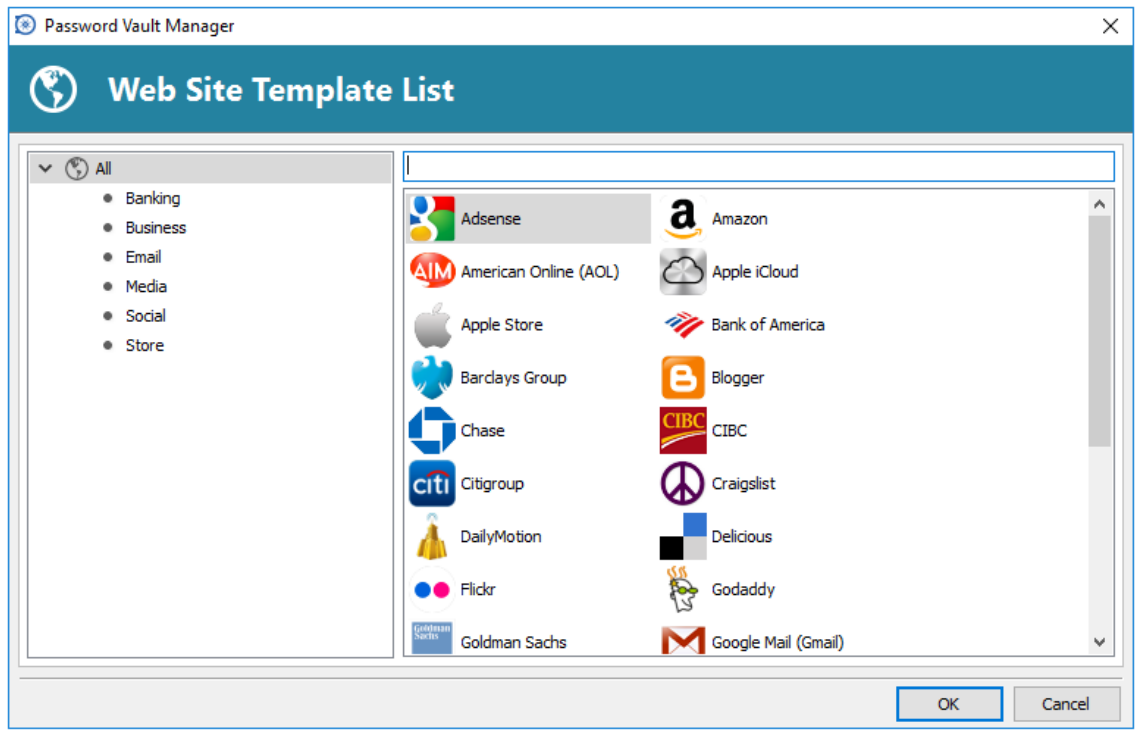
You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Credentials		You can choose to use credentials from: <ul style="list-style-type: none"> • Session specified credentials • Credential repository • Embedded credential entry
User name		The user name associated to the account
Domain		The domain associated to the account
Password	✔	The password associated to the account
Enable web browser extension link		Data entry will be available for the auto fill feature
Password only available to administrator		Must be administrator to be able to view/reveal password the password
Template		See Templates section
Security Questions		You can choose to add a Security Questions to your web entry for added security.
Advanced Settings		Enter HTML elements.

Templates

You can chose from over 55 pre-built templates to help eliminate guess work. For example:

- Facebook
- Hotmail
- LogMeIn
- Paypal
- Twitter



Web Site Template List

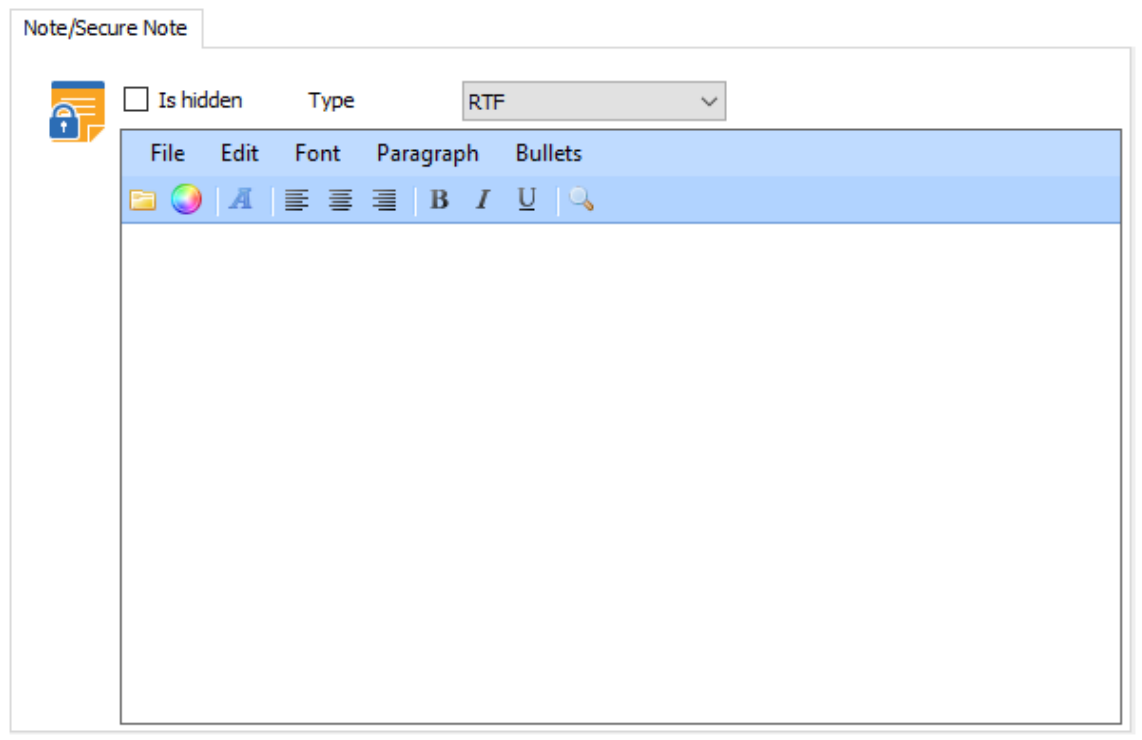
5.2.7 Note/Secure Note

Description



Note entry is a simple free form note allowing you to securely store any type of free form information.

Settings



Secure Note

You will notice that some fields are encrypted by default.

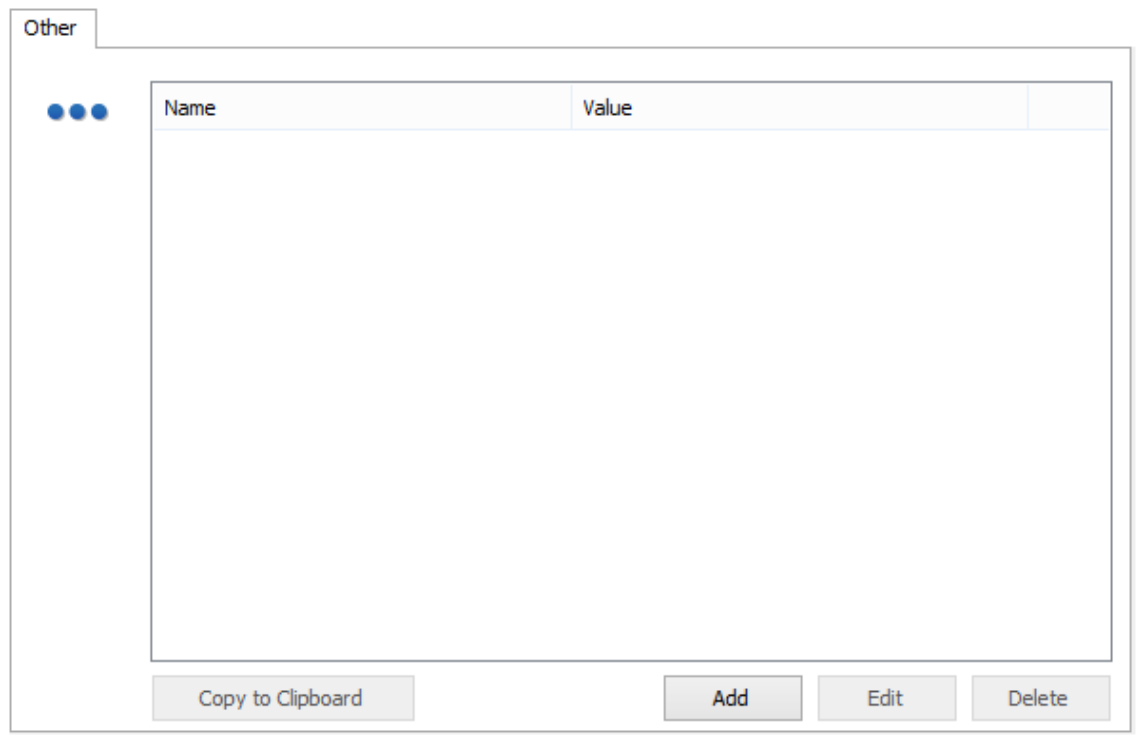
Name	Encrypted	Description
Note	✓	Select between RTF or Text type
Is hidden		Controls the encryption of the note on export and view
Type		Select between RTF and Text format

5.2.8 Other (Custom)

Description

●●● The **Other** entry type is used for securely storing name/value pairings of information.

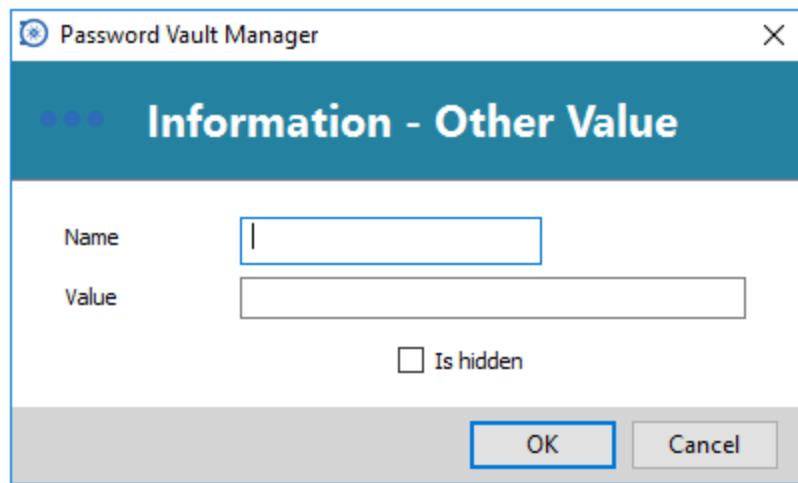
Settings



Other

Actions

Click on Add to create a new Other entry and then fill in the required fields.



Information - Other Value

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Name		Name of the settings

Value	✓	Value of the settings
Is hidden		Is the value hidden (secured). On export a hidden value will be encrypted

5.2.9 Passport

Description



The **Passport** entry is useful for storing your passport information such as your passport number and its expiration date.

Settings

Passport

Last name

First / middle name

Gender Male Female

Passport number

Expiration

Country of issue

Passport

You will notice that some fields are encrypted by default.

Name	Encrypted	Description
Last name		Last name on the passport
First/middle name		First/middle name on the passport
Gender		Male or Female
Passport number	✓	Enter your passport number
Expiration		Enter the expiration date of your passport
Country of issue		Enter the country who issued the passport

5.2.10 Safety Deposit


Description



The **Safety Deposit** entry is used to store your safety deposit information.

Settings


Safety Deposit



Institution

Address

Customer service number

Box number 

Passcode

Safety Deposit

You will notice that some fields are encrypted by default.

Option	Encrypted	Description
Institution		Name of the institution
Address		Address of the institution
Customer Service Number		Customer service number
Box number		Personal Box number
Passcode	✔	Personal Passcode

5.2.11 Software / Serials

Description



Software/Serial is an entry that provides the ability to store software serial number information. Including version, expiry date, name and license key.

Settings


General


Software / Serials


General Details

Software

Version Build

Licensed to 


License count 

Licenses 


Option	Encrypted	Description
Software		Software name
Version		Software version number
Build		Indicate the build number
Licensed to		Name of person who register the license
License count		Indicate the number of license you may have of the software
Licenses		Single key or list of keys


Details

Software / Serials

 General Details

Associated email

Purchase date 2016-05-19 

Renewal date 2016-05-19 

Language

Manufacturer

Supplier

Subscription

Automatic renewal

Option	Encrypted	Description
Associated email		Email associate to the license
Purchase date		Purchase date of the license
Renewal date		Date to renew the license
Language		Enter the software language
Manufacturer		Enter the software manufacturer
Supplier		Enter the software supplier
Subscription		Indicate if you have a subscription for that software
Automatic renewal		Indicate if you have an automatic renewal for this software

5.2.12 Wallet

Description



The **Wallet** entry is used to store your wallet information such as driver license or social security number.

Settings

Driver license



The screenshot shows a window titled 'Wallet' with a blue icon of a wallet. Inside the window, there is a form with two fields. The first field is labeled 'Type' and has a dropdown menu with 'Driver license' selected. The second field is labeled 'Driver license' and is an empty text input box.

Driver License

Option	Description
Type	Select the type of wallet entry that you wish to create between: <ul style="list-style-type: none">• Driver license• Social security number• Membership
Driver license, Social Security Number or Membership	Enter the driver license, social security number or the membership depending of the type selection.

5.2.13 Auto Fill

Description

The Auto Fill feature enters the user name and password defined in a entry into the web site login controls. For this feature to work you need to have a browser extension installed and configured properly. The most popular Windows based browsers are supported: Google Chrome, Mozilla Firefox and Microsoft Internet Explorer.

Installation

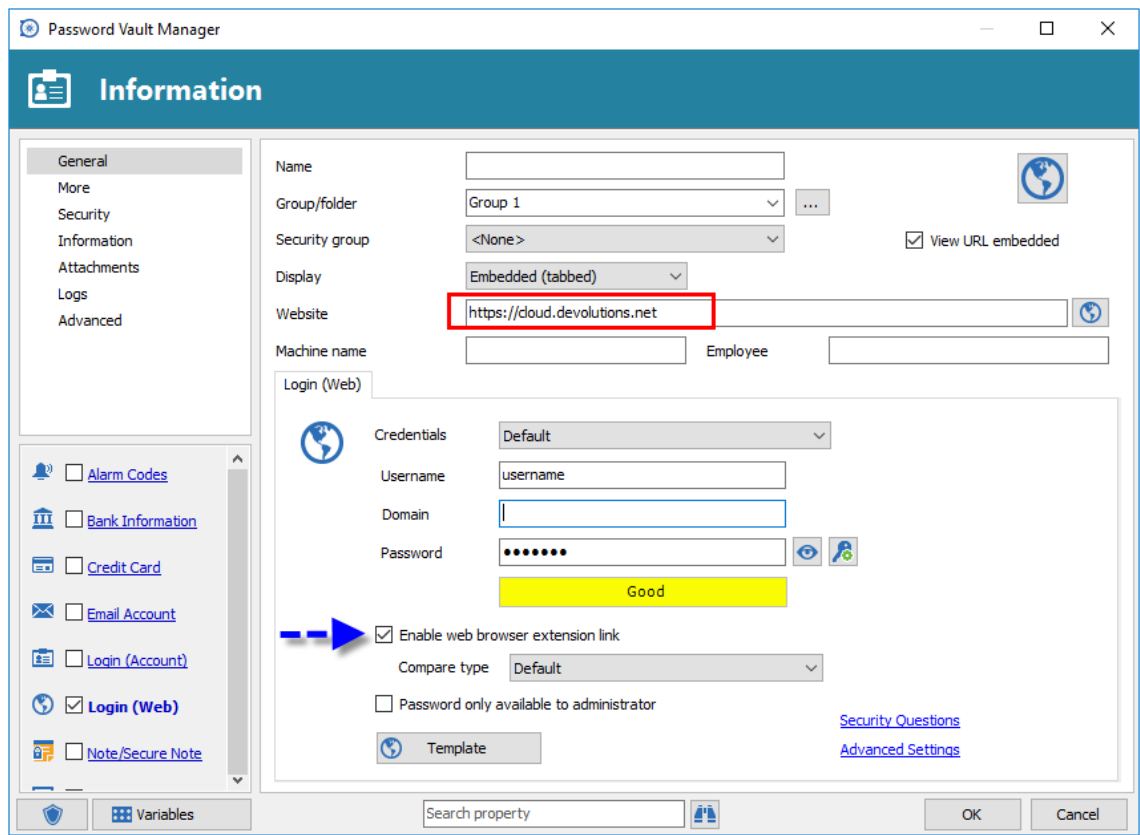
Refer to these topics for the browser of choice. You can use many of them concurrently without causing issues in Password Vault Manager.

- [Chrome Extension](#)
- [Firefox Extension](#)

- [IE Extension](#)

Creating Data Entries

Web and Account entry types both support Auto Fill. They must however be configured to allow web browser extension links. The URL field must be the URL of the login page for the given webpage (Ex. <http://login.live.com>). You must also enable the **Enable web browser extension link** option.



Troubleshoot

Information entries must be marked (checked) as **Enable web browser extension link** for auto fill feature to work.

If Password Vault Manager is configured with multiple data sources only the currently active data source will be queried.

When multiple data entries match the web site Password Vault Manager will prompt for you to select a specific data entry.

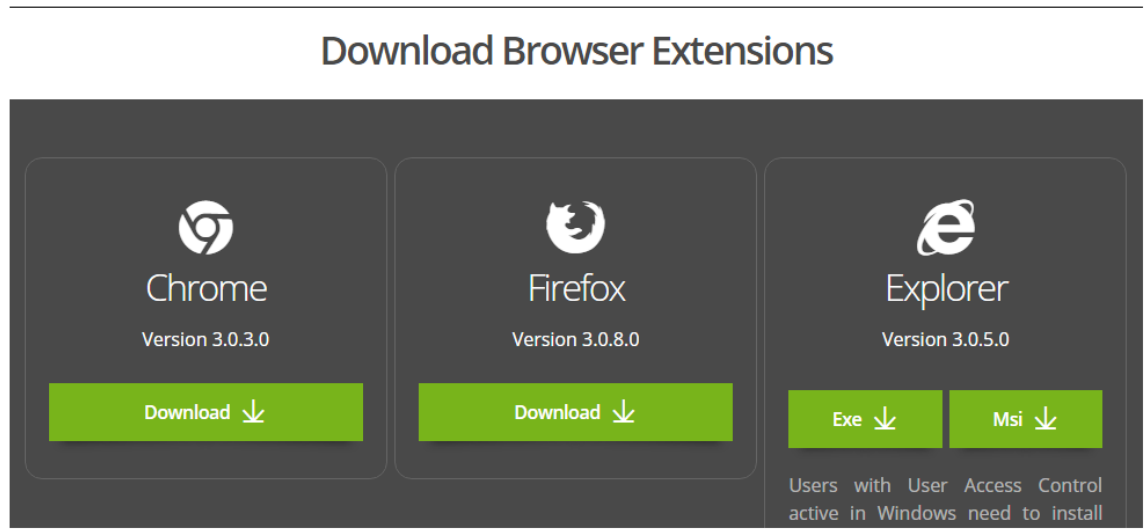
5.2.13.1 Chrome Extension

Description

Password Vault Manager - Chrome Extension

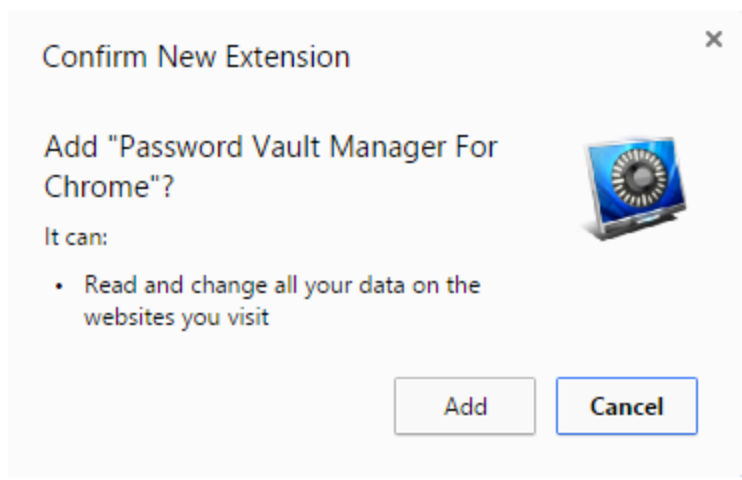
Installation

- Start Chrome
- Go [here](#) & download the .crx file Password Vault Manager for Chrome Extension



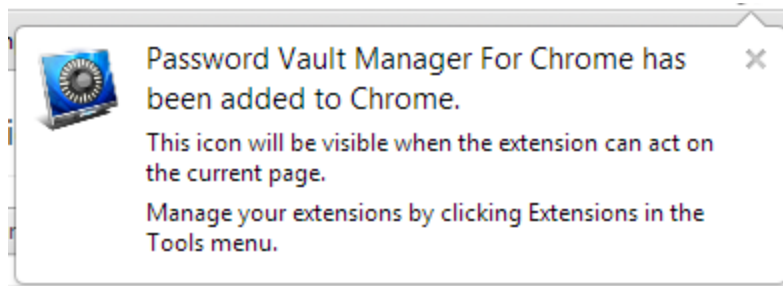
Download Browser Extension

- Click on **Add**



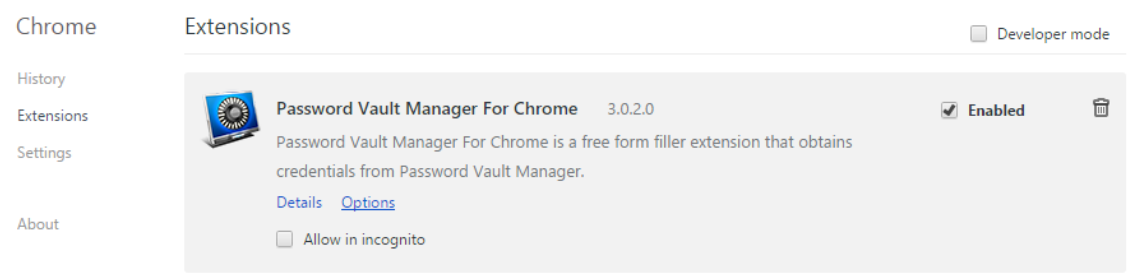
Confirm Chrome Extension Installation

- Installation is now complete, you should see a confirmation window



Password Vault Manager> For Chrome is now installed

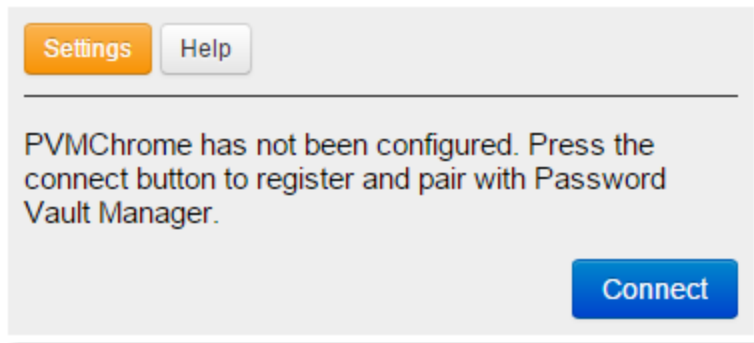
- To view/manager all installed Chrome extensions go to **More Tools - Extensions**



Password Vault Manager For Chrome is now installed

Using

- Open Password Vault Manager if not already started
- You will need to configure the Password Vault Manager for Chrome extension of first use



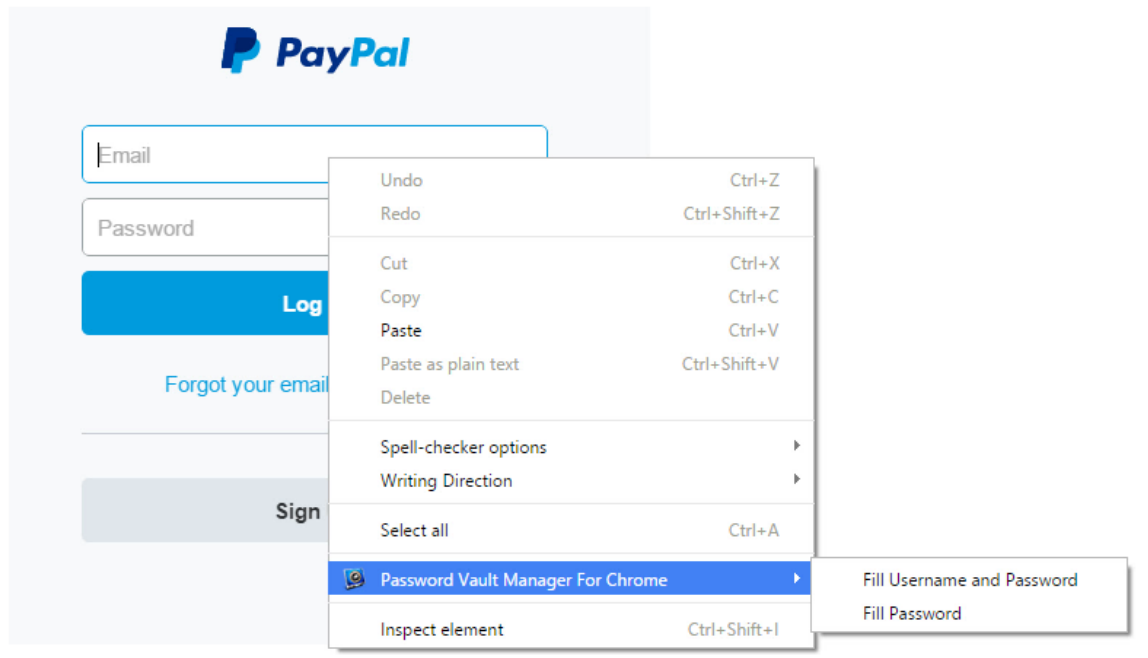
Connect Extension to Password Vault Manager

- Open a web site that has been configured in Password Vault Manager
- Check the status of the extension



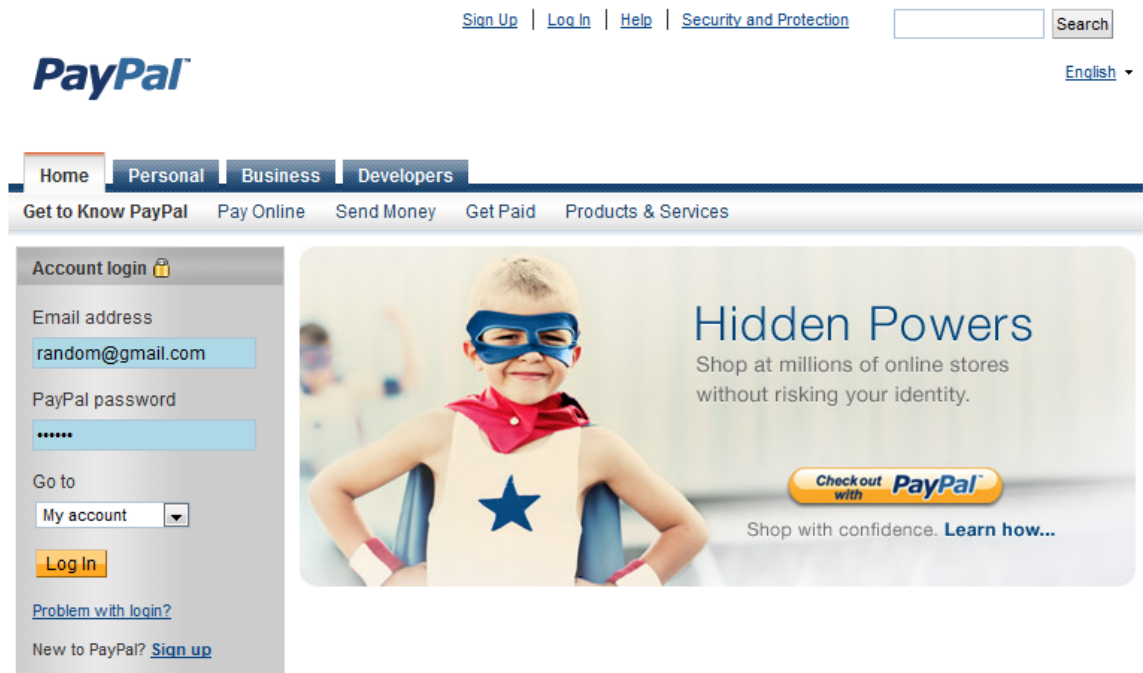
Connect Extension to RDM

- Right click in either the username or password field and select the fill option



Select Fill Option

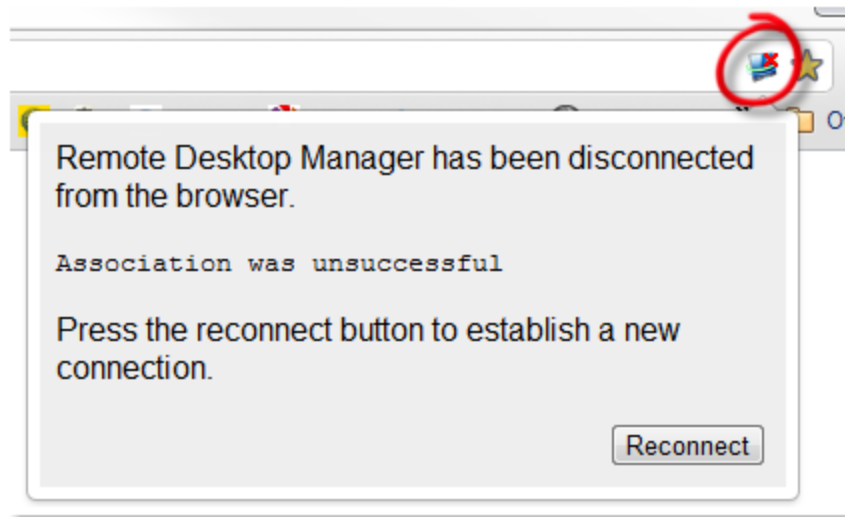
- Result



Sample web site populated with Password Vault Manager auto fill feature

Troubleshoot

If an error occurs the extension icon will show the error icon. Simply click on the icon for further information.



Sample Extension Error

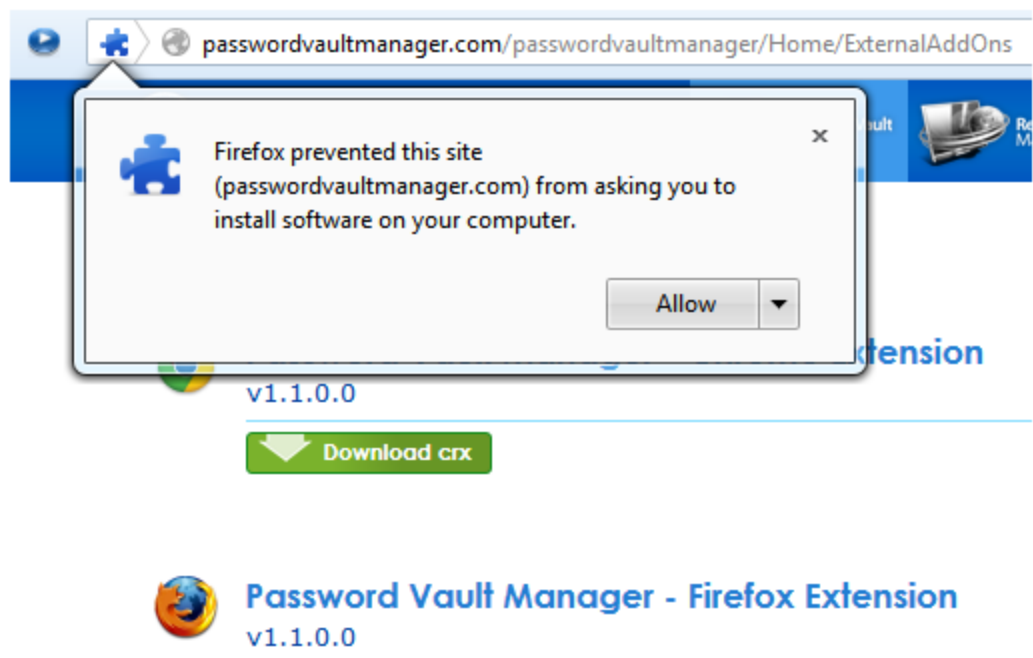
5.2.13.2 Firefox Extension

Description

Password Vault Manager - Firefox Extension

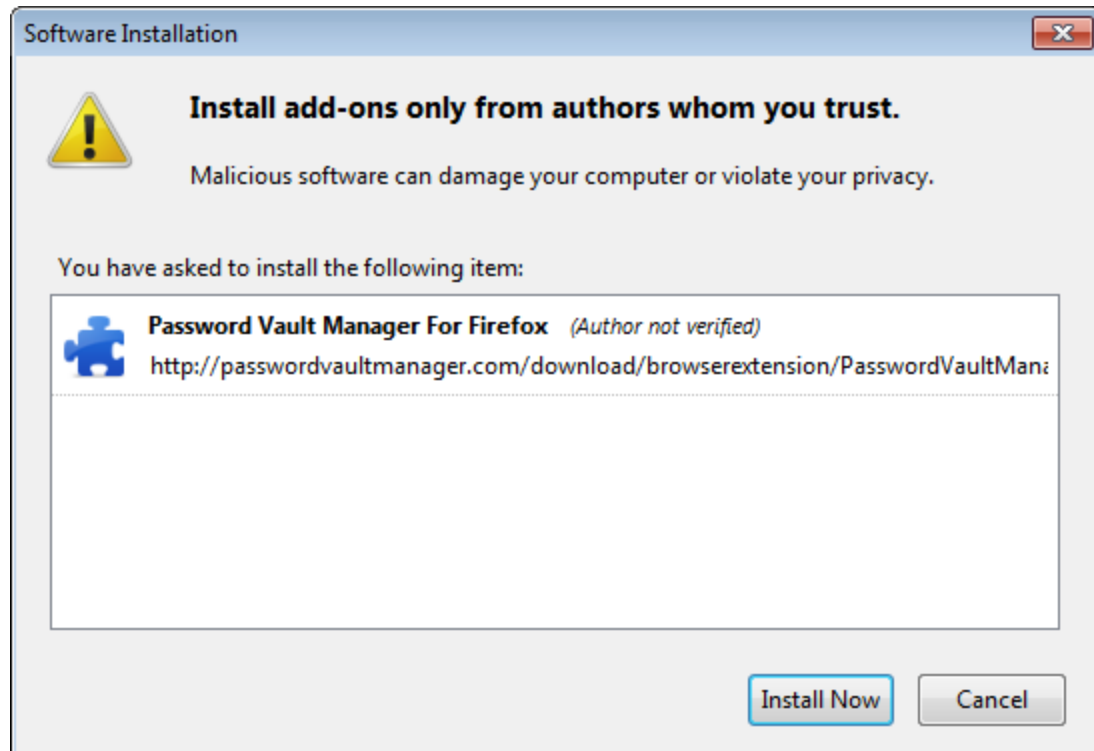
Installation

- Start Firefox
- Go [here](#) & download the .xpi file Password Vault Manager - Firefox Extension



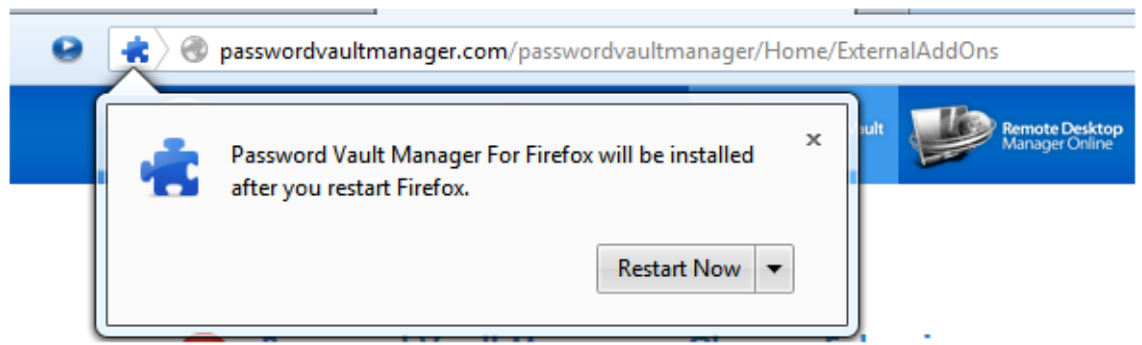
Allow Password Vault Manager Firefox Extension

- Confirm the installation



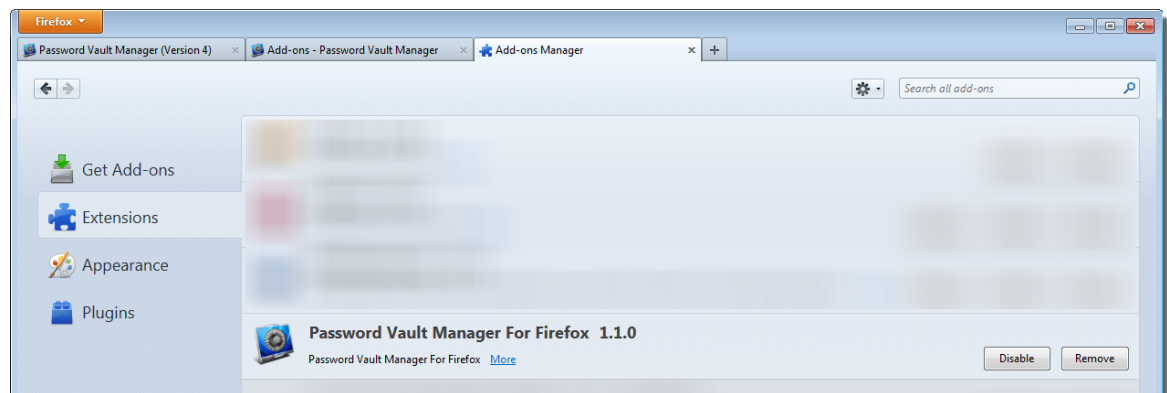
Confirm Password Vault Manager Firefox Extension Installation

- Restart Firefox



Restart Firefox

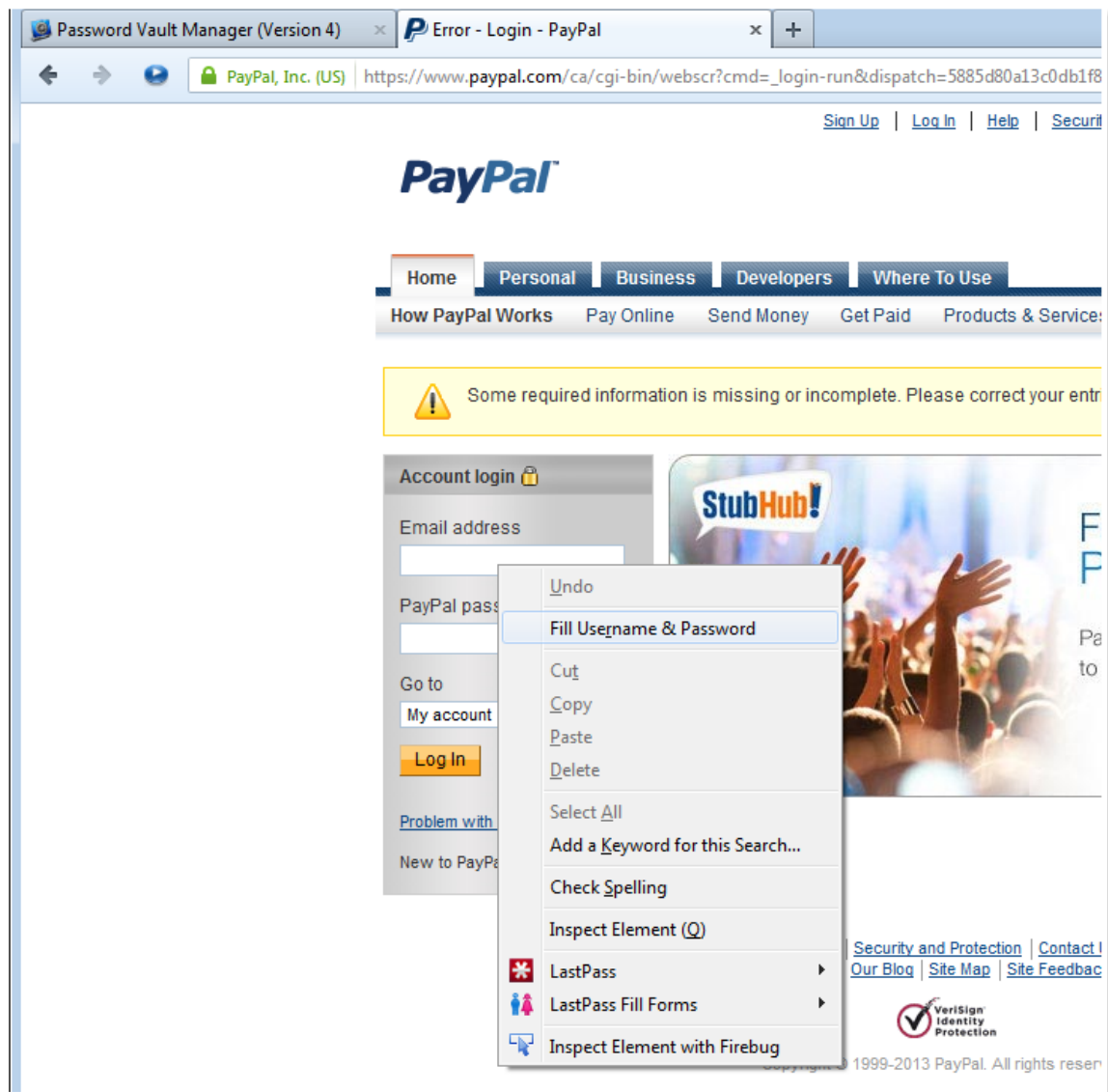
- To view/manager all installed Firefox extensions see Add-ons menu



Password Vault Manager For Firefox is now installed

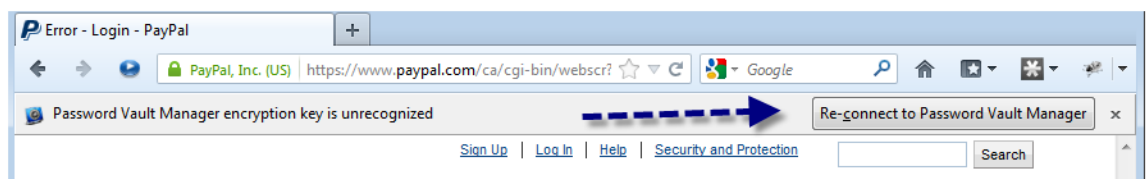
Using

- Open Password Vault Manager if not already started Password Vault Manager
- Right click in either the username or password field and select the fill option



Select Fill Option

- You will need to configure the Password Vault Manager for Firefox extension on first use



Connect Extension to RDM

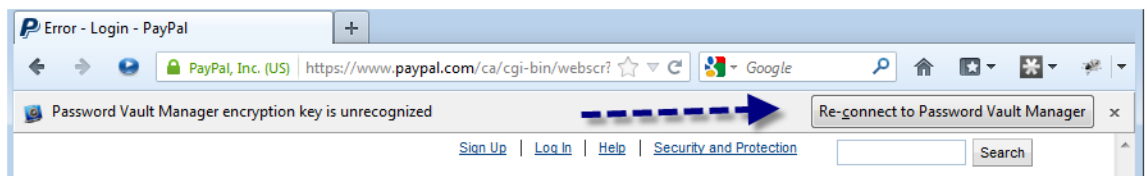
- Right click again
- Result



Sample web site populated with Password Vault Manager auto fill feature

Re-connecting

You will need to re-configure the Password Vault Manager for Firefox extension every time use a different datasource within the browser.



Password Vault Manager for Firefox extension re-connect message.

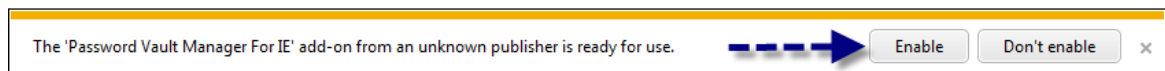
5.2.13.3 IE Extension

Description

Web browser auto fill is only available for Internet Explorer 8 or better.

Installation

- Download ([here](#)) & install the Internet Explorer Extension
- Start Internet Explorer
- If prompted to enable, make sure to enable

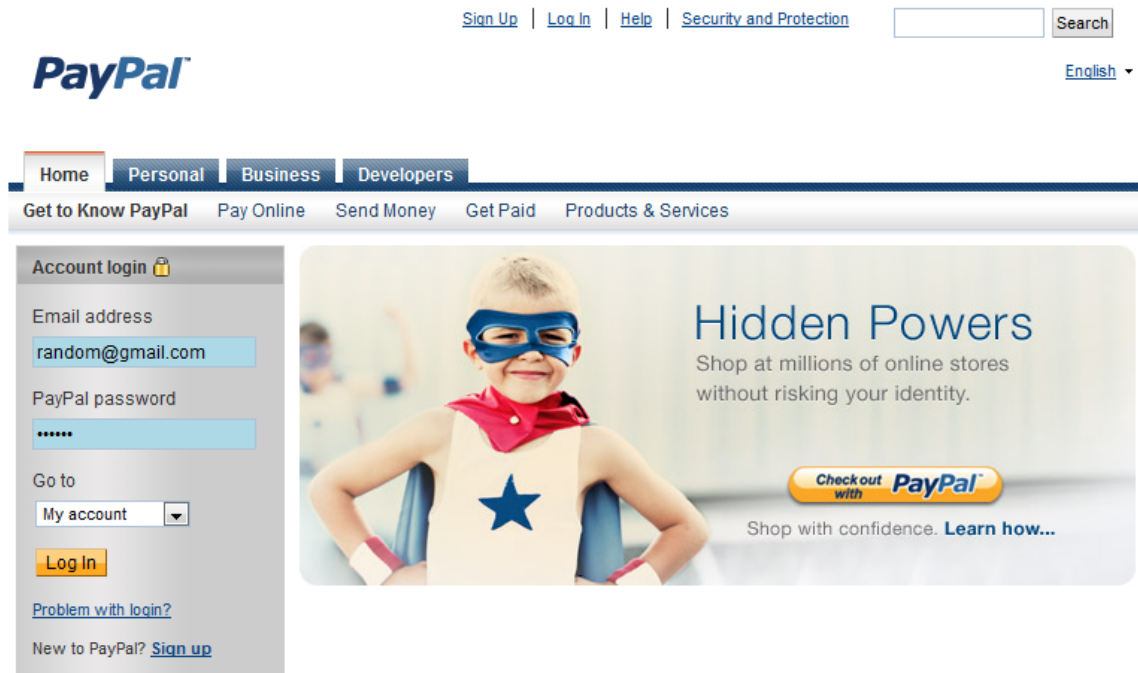


Enable Password Vault Manager For IE add-on

- Restart Internet Explorer

Using

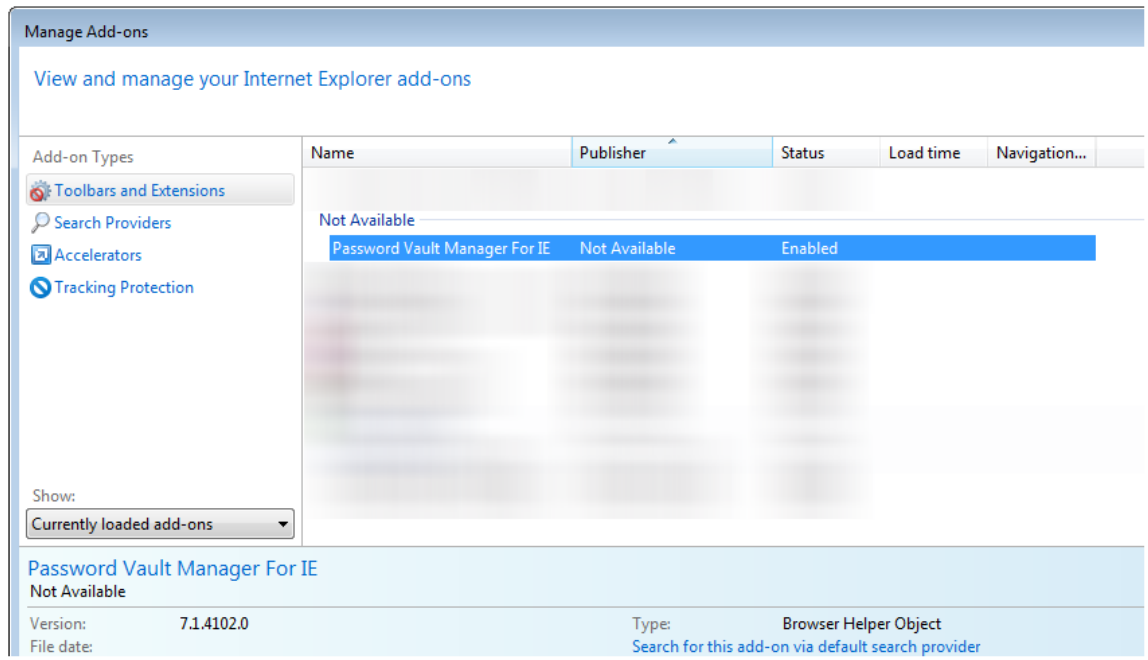
- Open Password Vault Manager if not already started
- Open a web site that has been configured in Password Vault Manager, you should have the username & password automatically populated and both text boxes should now be light-blue



Sample web site populated with Password Vault Manager auto fill feature

Troubleshoot

Double check that the add-on is in fact enabled. In Internet Explorer Manage add-ons window.



Enable/Disable Password Vault Manager for IE








5.3 Contact

Description

Contact entry types are used to manage your contacts in Password Vault Manager.

Settings


You can choose between 7 different types of contacts

	Contact type	Description
	Company	Used to define and configure a "Company" contact.
	Customer	Used to define and configure a "Customer" contact.
	Default	Used to define and configure a contact with no defined type. Use this type of entry if your contact does not fit in any other category.
	Employee	Used to define and configure a "Employee" contact.
	Family	Used to define and configure a "Family" contact.
	Supplier	Used to define and configure a "Supplier" contact.
	Support	Used to define and configure a "Support" contact.


Enter all the information related to a contact to create your entry.

Contact Default Entry

Country

Enter a complete address for a contact and the  button will show you his location in Google Maps.

Email

Enter an email address for a contact and click the  button to send him directly an email.

Skype

Enter a Skype username for a contact and click  button to contact him via Skype directly.

Website

Enter a website for a contact and click  button to open the contact website.

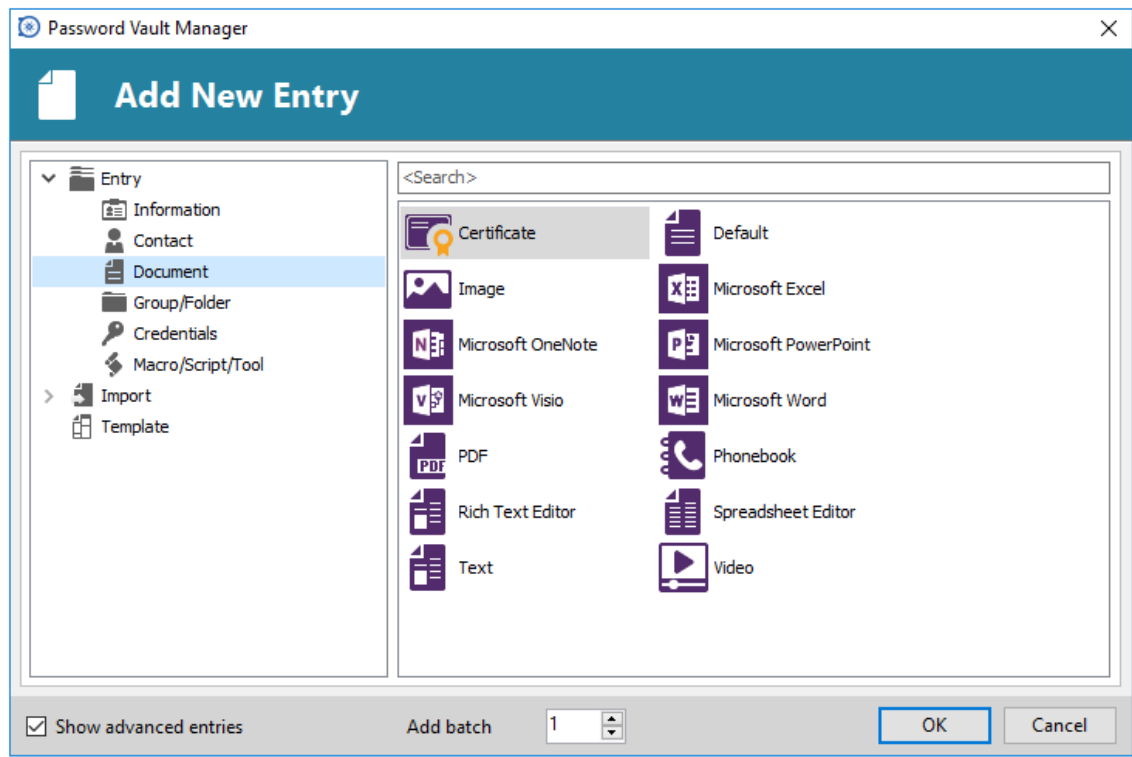
5.4 Documents

Description

Document entry types are used to store any type of document directly in the data source.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update of our products.



New Entry - Documents

Refer to these topics for more information:

- [Certificate](#)
- [Default](#)
- [Image](#)
- [Microsoft Office \(Word, Excel, PowerPoint, Visio and OneNote\)](#)
- [PDF](#)
- [Phonebook](#)
- [Rich Text Editor](#)
- [Spreadsheet Editor](#)
- [Text](#)
- [Video](#)

5.4.1 Certificate

Description



This entry is used to define and configure a **Certificate** document entry.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

Link to file

 ...

Url

Stored in database Use default credentials

 ...

File size

Created by

Creation date

Certificate

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



When updating a document it will also save the new filename.

5.4.2 Default

Description



This entry is used to define and configure a **Default** document entry. Use this type whenever Password Vault Manager does not offer support for your specific file type.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

Link to file

 ...

Url

Stored in database Use default credentials

 ...

File size

Created by

Creation date

Default

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.3 Image

Description



This entry is used to define and configure a **Image** document entry. Image entry support the embedded mode.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

Link to file

...

Url

Stored in database

Use default credentials

...

File size

Created by

Creation date

Image

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.4 Microsoft Office (Word, Excel, PowerPoint, Visio and OneNote)

Description

These entries are used to define and configure a **Microsoft Office** document entry. Word, Excel and PowerPoint support the embedded mode when both Password Vault Manager and MS Office are running using the 32 bit architecture.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Microsoft Office document types

- Word
- Excel
- PowerPoint
- Visio
- OneNote

Settings

MS Office

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.5 PDF

Description



This entry is used to define and configure a **PDF** document entry. PDF entries support the embedded mode.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

The screenshot shows a configuration window for a PDF entry. It has two tabs: 'General' and 'Other'. Under the 'General' tab, there is a PDF icon and three radio button options: 'Link to file' (selected), 'Url', and 'Stored in database'. Each option has a corresponding text input field. The 'Link to file' field has a '...' button to its right. The 'Stored in database' option has a checkbox labeled 'Use default credentials' next to it. Below the input fields, there are three labels: 'File size', 'Created by', and 'Creation date'.

PDF

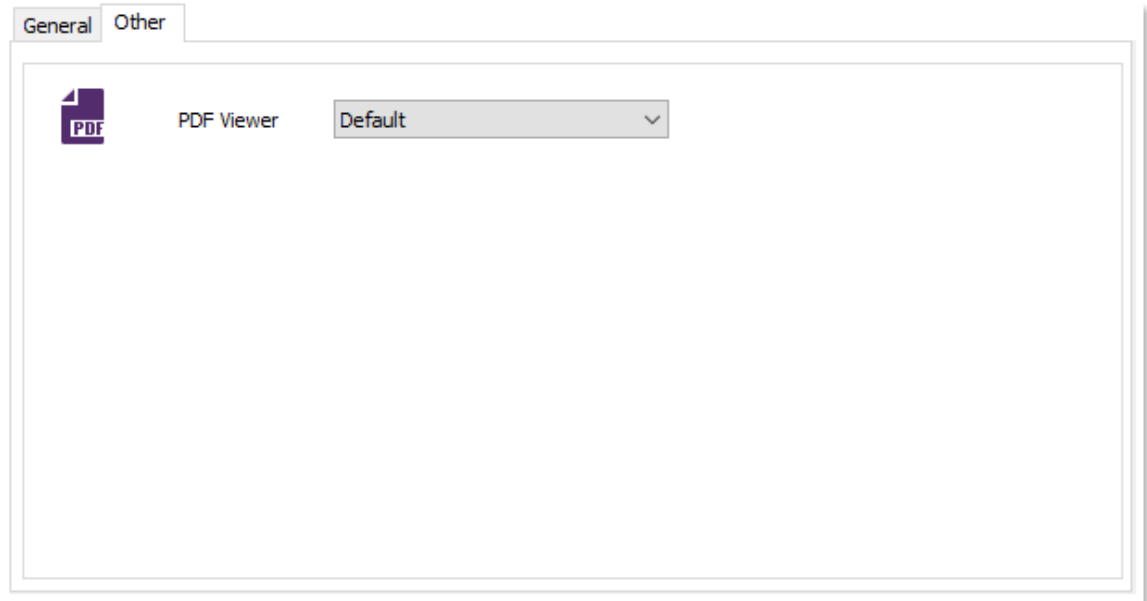
Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

Other

Allows you to select the PDF Viewer that you wish to use.



PDF - Other

Supported PDF Viewer

- Default
- Acrobat Reader
- PDF-XChange Viewer
- PDF-XChange Viewer Pro
- Firefox pdf viewer
- Native

5.4.6 Phonebook

Description




This entry is used to define and configure a **Phonebook** document entry.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General



Link to file

 ...

Url

Stored in database

 ...

Use default credentials

File size

Created by

Creation date

Phonebook

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

5.4.7 Rich Text Editor

Description



This entry is used to define and configure a **Rich Text** document entry. This allow you to modify the entry directly in the application.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

General Other

Link to file

Url

Stored in database Use default credentials

Existing text file

New text file

File size

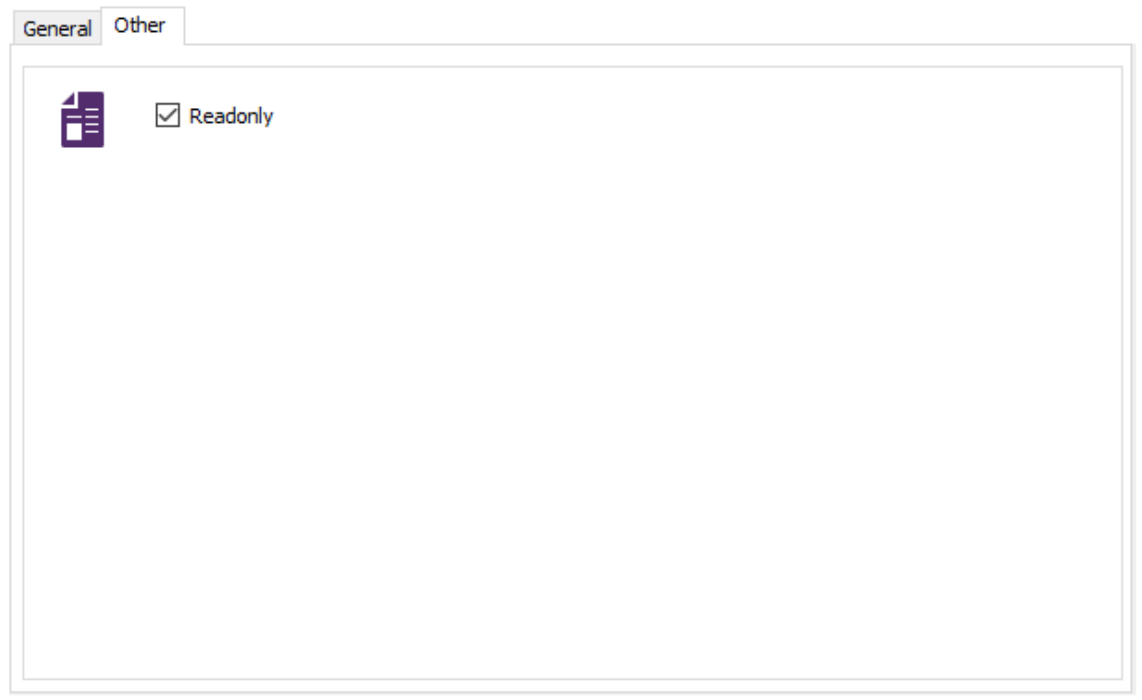
Created by

Creation date

Rich Text Editor

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.

Other



The screenshot shows a settings window with two tabs: 'General' and 'Other'. The 'Other' tab is active. Inside the 'Other' tab, there is a document icon and a checkbox labeled 'Readonly' which is checked.

Rich Text Editor - Other

Option	Description
Readonly	Check this box if you wish to disallow the permission to edit your entry.

5.4.8 Spreadsheet Editor

Description



This entry is used to define and configure a **Spreadsheet** entry. This allow you to modify excel document directly in the application.




For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

General **Other**

 Link to file
 ...

Url

Stored in database Use default credentials

Existing spreadsheet
 ...

New spreadsheet

File size
 Created by
 Creation date

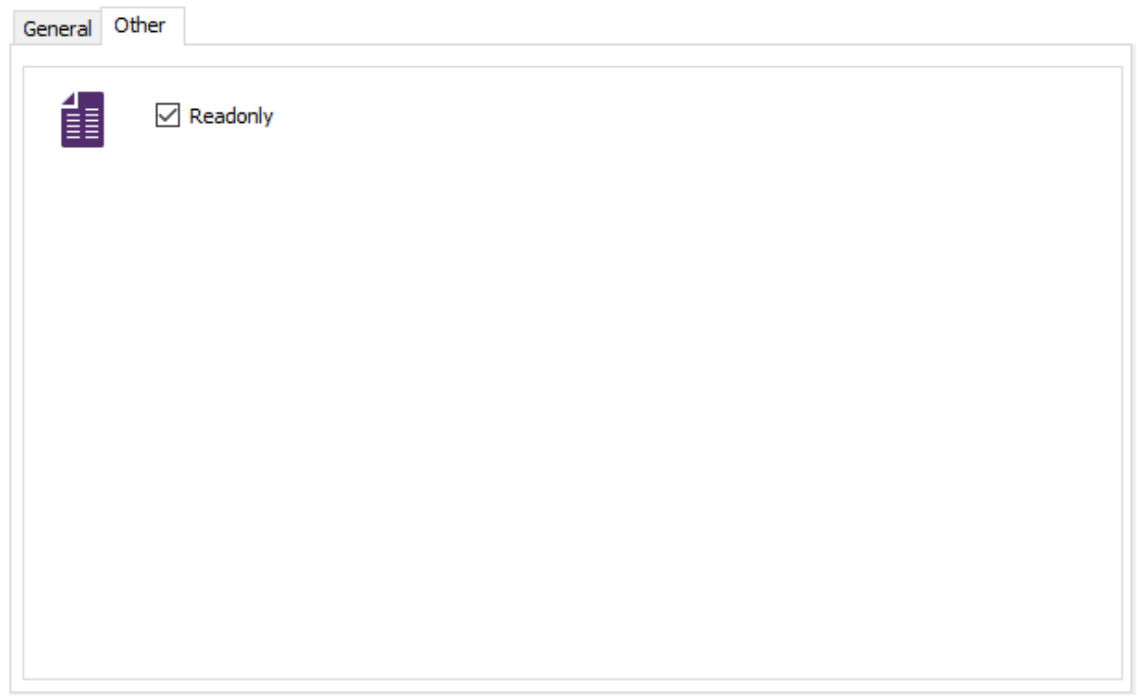
Spreadsheet Editor

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.
Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.



If you update a document this will also save the new filename.

Other



Spreadshhet Editor - Other

Option	Description
Readonly	Check this box if you want to disallow the permission to edit your entry.

5.4.9 Text

Description



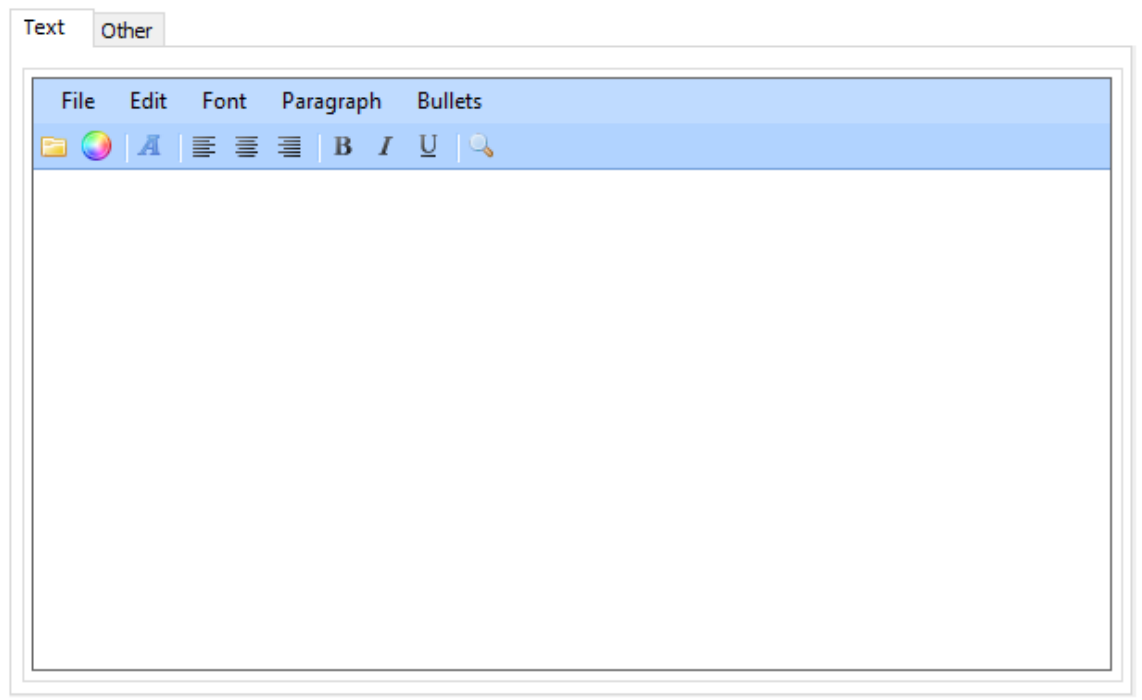
This entry is used to define and configure a **Text** document entry. We support the Rich Text format (RTF).



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

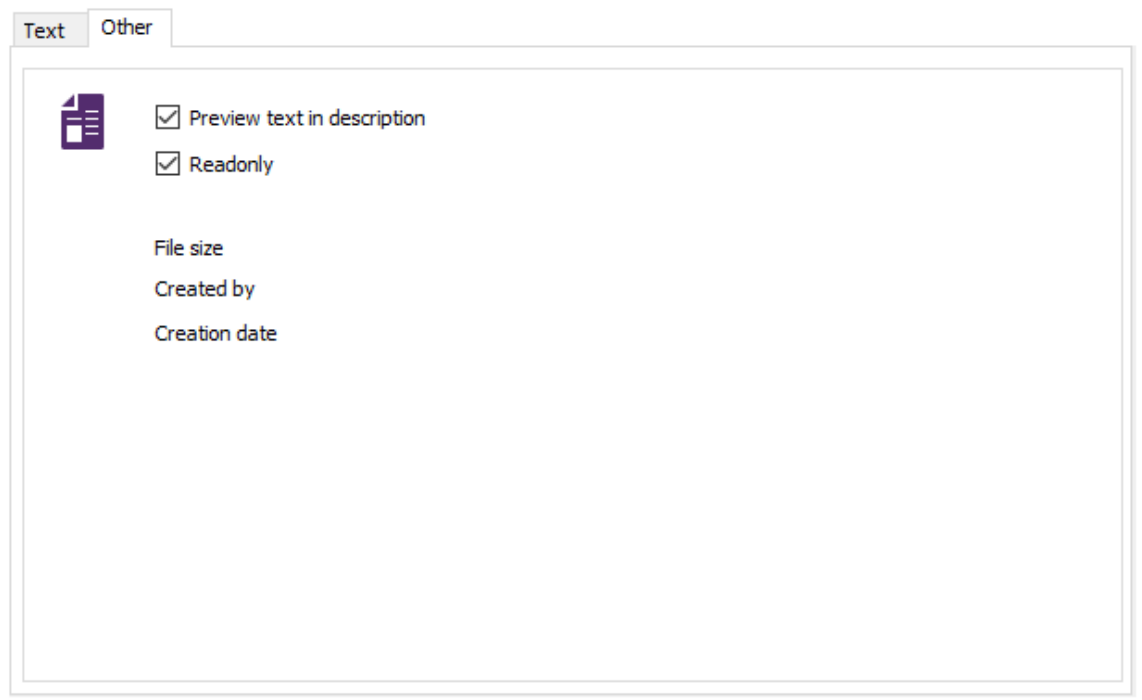
Settings

Text

**Text**

Type the text in the blank section to create your text entry.

Other

**Text - Other**

Option	Description
Preview text in description	Display your text in the description field before opening your text file.
Readonly	Disallow the permission to edit your entry.

5.4.10 Video

Description



This entry is used to define and configure a **Video** document entry.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.

Settings

General

Link to file

...

Url

Stored in database Use default credentials

...

File size

Created by

Creation date

Video

Option	Description
Link to file	Enter the path to a file located on your PC or on your network.
Url	Open a file using a URL. You can also use your default Windows Credentials to open the file.

Stored in database	Select a file that will be stored in the database. Some data sources do not support this mode.
--------------------	--

5.5 Groups

Description

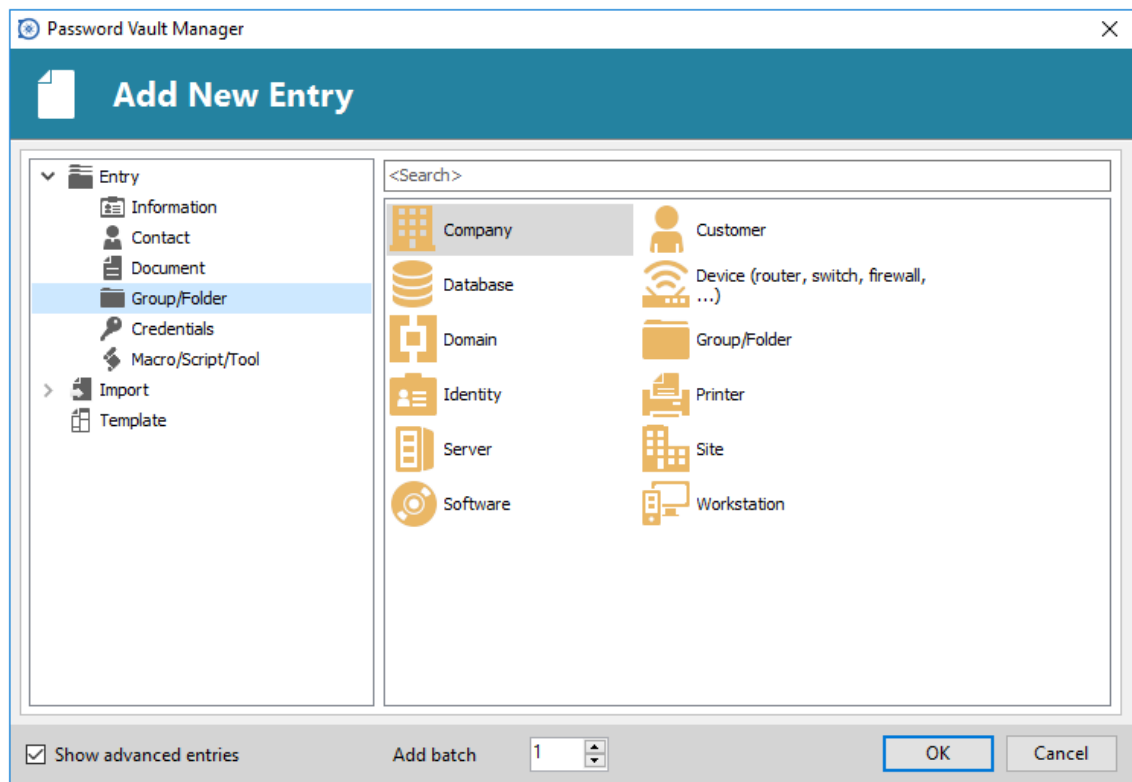
Groups or folders are used to organize your sessions in a logical way. It's possible to create groups and sub groups, which Password Vault Manager will automatically sort alphabetically.

Groups can be created in two different ways:

- Via the session properties
- From the session tree view

You can assign a group type to simplify the organization or use variables:

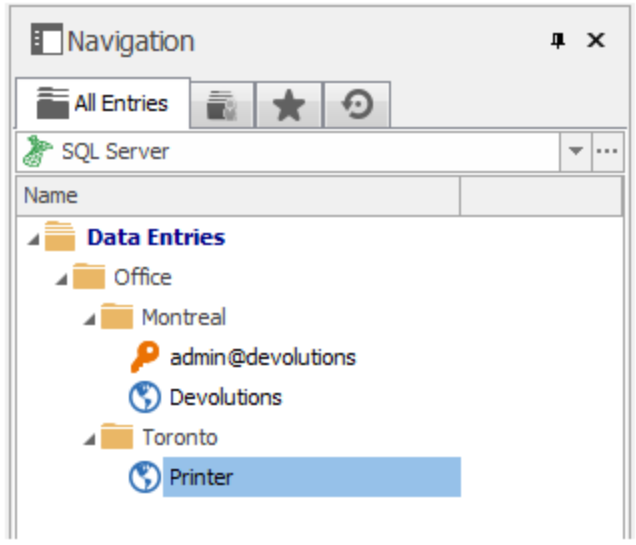
- Company/Site
- Customer/identity
- Database
- Device/Server/Workstation
- Folder



New Entry - Group/Folder

Creating Groups via the Entry Settings

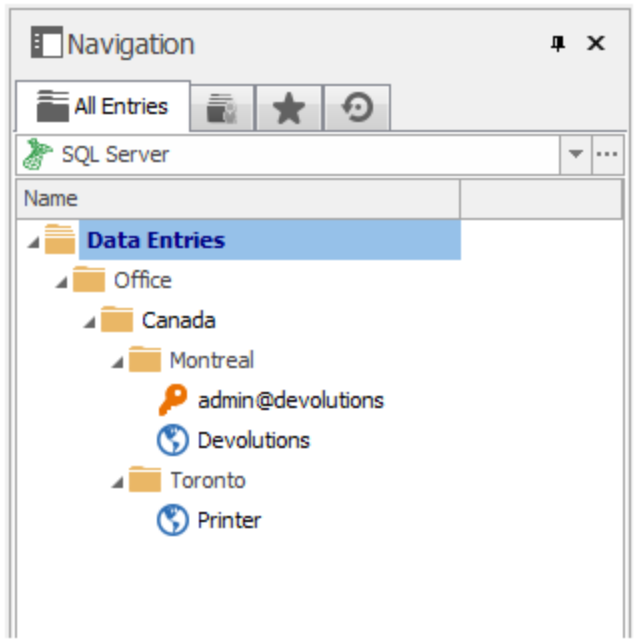
Groups can be specified in the session properties. Simply fill this field with your desired group name, and Password Vault Manager will generate the corresponding tree structure. Use the backslash (\) to create a sub group.



Folder Structure

For example, "Office\Canada\Montreal" will create three nodes in the tree:

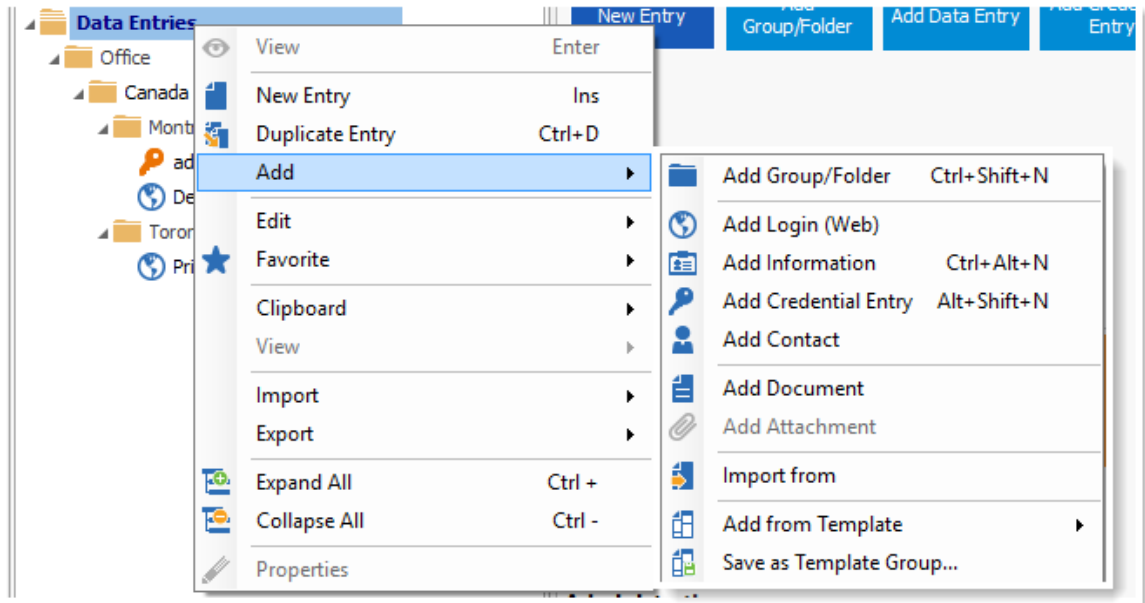
- Office
- Canada
- Montreal



Folder Structure

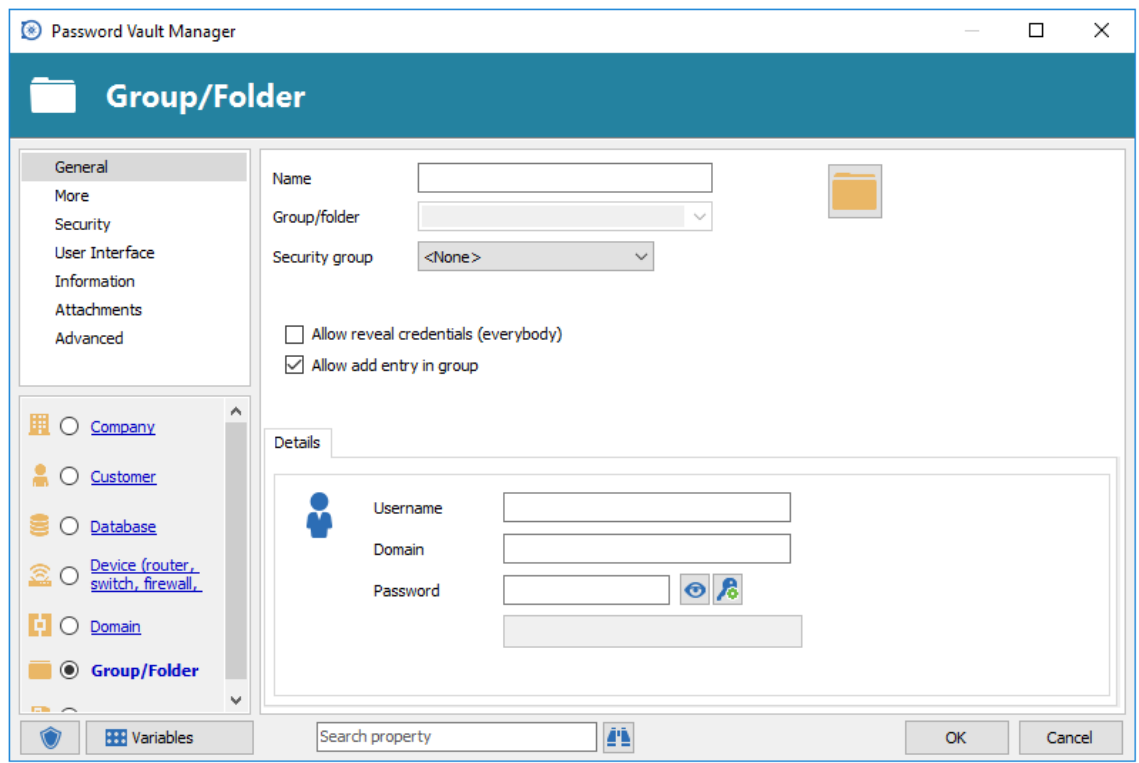
Creating Groups from the Tree View

By right clicking the root node of a group or an existing session, a context menu appears allowing you to create a new group.



Add Group/Folder

The **Add Group** dialog box will then prompt you to enter the name of the group, and choose its parent group.



Group/Folder Entry

Once a group is created, you can add a session by using the menu, or by dragging its node directly to the content of the group.

5.5.1 Company




Description



This entry is used to organize a **Company** group.

Settings

Details

	Username	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
		<input type="text"/>

Group - Company

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use \$COMPANY_variables\$. For more information, please consult the [Variables](#) topic.

5.5.2 Customer




Description



This entry is used to organize a *Customer* group.

Settings

Details

	Username	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
		<input type="text"/>

Group - Customer

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use \$CUSTOMER_variables\$. For more information, please consult the [Variables](#) topic.

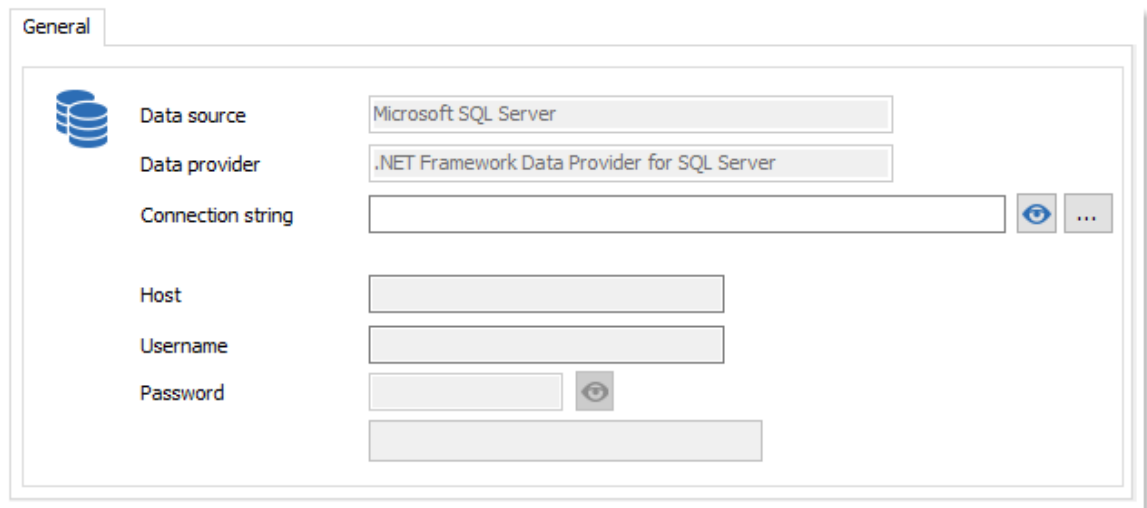
5.5.3 Database

Description



This entry is used to organize a *Database* group.

Settings



The screenshot shows the 'General' tab of a configuration window for a 'Group - Database'. It contains the following fields:

- Data source:** Microsoft SQL Server
- Data provider:** .NET Framework Data Provider for SQL Server
- Connection string:** An empty text box with a visibility icon and an ellipsis button.
- Host:** An empty text box.
- Username:** An empty text box.
- Password:** An empty text box with a visibility icon.

Group - Database

Enter the connection information if you wish for the child entries to inherit them. Press the ellipsis button to be able to select the data source and data provider. This will generate the connection string with the information entered in the dialog.



To access field from this group entry, you should use `$DB_variables$`. For more information, please consult the [Variables](#) topic.

5.5.4 Device (router, switch, firewall)






Description



This entry is used to organize a **Device** group.

Settings

Details

	Computer	<input type="text"/>	
	IP	<input type="text"/>	
	Username	<input type="text"/>	
	Domain	<input type="text"/>	
	Password	<input type="password"/>	 
		<input type="text"/>	

Group - Device

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to *inherit* them, you need to specify the inherited credentials setting in the session.



To access field from this group entry, you should use `$COMPUTER_variables$`. For more information, please consult the [Variables](#) topic.

5.5.5 Domain

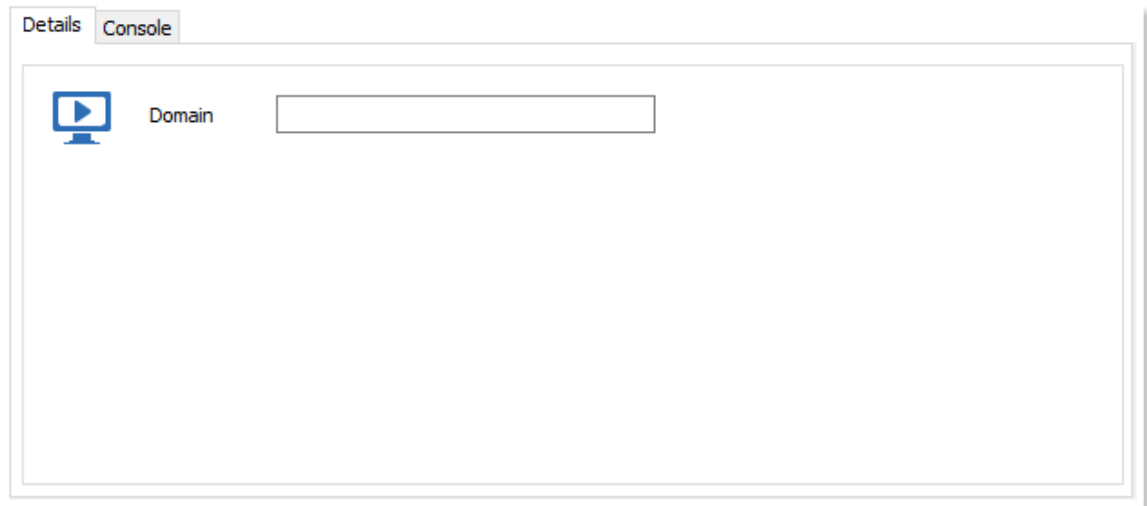
Description



This entry is used to organize a *Domain* group.

Settings

Details



Group - Domain

Enter the domain name.



To access field from this group entry, you should use `$DOMAIN_variables$`. For more information, please consult the [Variables](#) topic.

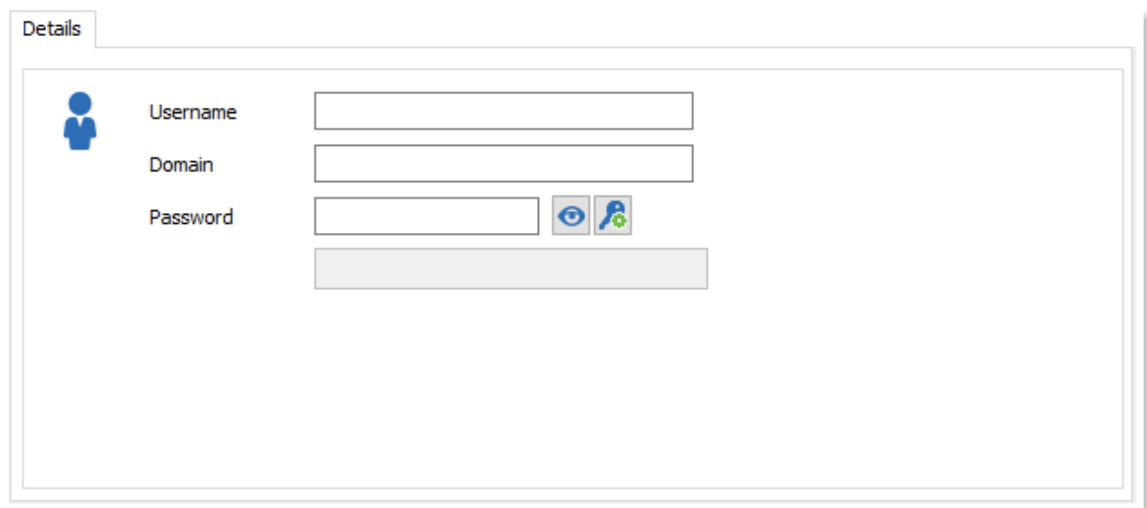
5.5.6 Group/Folder

Description



This entry is used to organize the content in **Group/Folder**.

Settings



Group - Group/Folder

Enter the user name, domain and password for credentials that you wish to associate with that group.

If you wish for children entries to use the specified credentials, you need to set the **Credentials** setting to **inherited** in the session.



The folders in **Credentials** and **Macros/Scripts/Tools** must have children in order to appear.

If you type in a folder structure directly in an entry, "virtual" folders are created. You can edit those folders and transform them in "physical" folders.

5.5.7 Identity


Description



This entry is used to organize a **Identity** group.

Settings

Details



Username

Domain

Password

Group - Identity

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the **inherited** credentials setting in the session.



To access field from this group entry, you should use `$IDENTITY_variables$`. For more information, please consult the [Variables](#) topic.

5.5.8 Printer





Description



This entry is used to organize a **Printer** group.

Settings

Details

	Computer	<input type="text"/>	...
	IP	<input type="text"/>	
	Username	<input type="text"/>	
	Domain	<input type="text"/>	
	Password	<input type="password"/>	 
		<input type="text"/>	

Group - Printer

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the **inherited** credentials setting in the session.



To access field from this group entry, you should use `$COMPUTER_variables$`. For more information, please consult the [Variables](#) topic.

5.5.9 Server



Description



This entry is used to organize a **Server** group.

Settings

Details

	Computer	<input type="text"/>	<input type="button" value="..."/>
	IP	<input type="text"/>	
	Username	<input type="text"/>	
	Domain	<input type="text"/>	
	Password	<input type="password"/>	<input type="button" value="eye"/> <input type="button" value="lock"/>
		<input type="text"/>	

Group - Server

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use `$COMPUTER_variables$`. For more information, please consult the [Variables](#) topic.

5.5.10 Site




Description



This entry is used to organize a *Site* group.

Settings

Details

	Username	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
		<input type="text"/>

Group - Site

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use `$$SITE_variables$`.
For more information, please consult the [Variables](#) topic.

5.5.11 Software




Description



This entry is used to organize a **Software** group.

Settings

Details

	Username	<input type="text"/>
	Domain	<input type="text"/>
	Password	<input type="password"/>  
		<input type="text"/>

Group - Software

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the *inherited* credentials setting in the session.



To access field from this group entry, you should use `$(SOFTWARE_variables$`.
For more information, please consult the [Variables](#) topic.

5.5.12 Workstation

Description



This entry is used to organize a *Workstation* group.

Settings

Details

Computer ...

IP

Username

Domain

Password

Group - Workstation

Use the ellipsis button to select from a list of discoverable computers or enter the name or IP address manually.

Enter the user name, domain and password.

If you wish for children entries to inherit them, you need to specify the inherited credentials setting in the session.



To access field from this group entry, you should use `$COMPUTER_variables$`. For more information, please consult the [Variables](#) topic.

5.6 Credentials

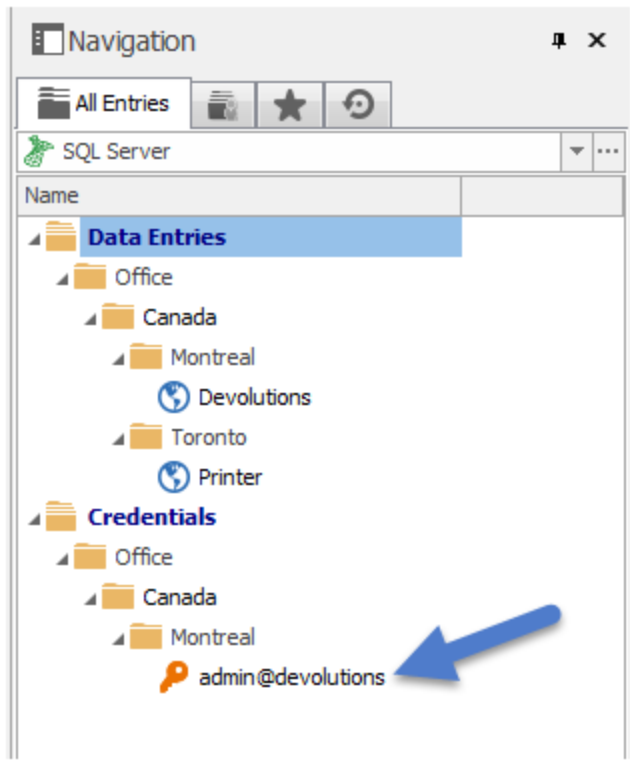
Description

The credential repository is available in the Enterprise edition and allows you to set multiple sessions to a specific set of credential. This simplifies management by forcing users to modify their credentials in one place. The list is visible in the tree view under the session list.

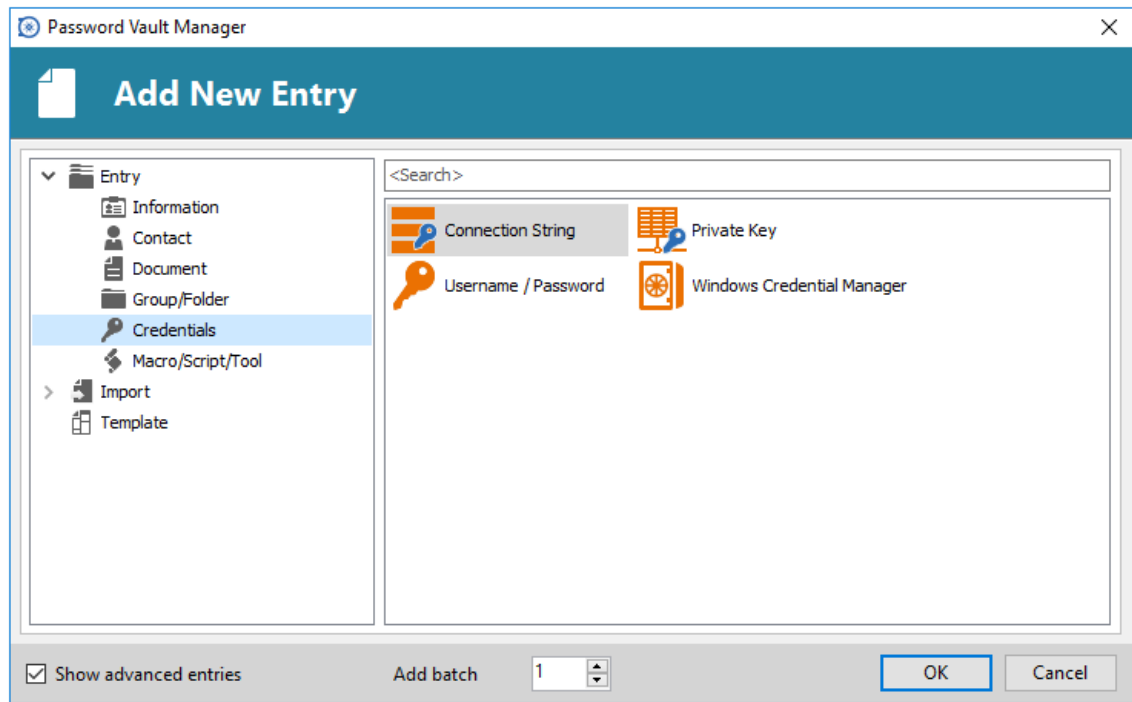
To create an entry, use the session's context menu and select **Add - Credential Repository**.

Settings

The Credentials branch is visible in the tree view under the session list by default (if the **Merge credentials list with sessions** option is not enabled in [File - Options - User Interface - Tree View](#)).

**Credentials**

You can configure the credential repository to prompt you to select a set of credentials which allows you to use multiple credentials for the same host.

**New Entry - Credentials**

5.6.1 Connection String

Description



This entry is used to define and configure a **Connection String** credential entry. Connection string credential entries are exactly the same as a [Database Group](#) with the exception that they are not limited by the inheritance hierarchy of groups.

Settings

The screenshot shows the 'General' settings tab for a 'Connection String' credential. The form contains the following fields:

- Data source:** Microsoft SQL Server
- Data provider:** .NET Framework Data Provider for SQL Server
- Connection string:** (Empty text box with a visibility toggle icon and a menu icon)
- Host:** (Empty text box)
- Username:** (Empty text box)
- Password:** (Empty text box with a visibility toggle icon)

Credentials - Connection String

Option	Description
Data source	Contains data source types like ODBC, OLEDB or native. This value is read only and is extracted from the connection string.
Data provider	Specify the provider used for the database access. This value is read only and is extracted from the connection string.
Connection string	This value contains the database connection string and it can be hidden/encrypted for higher security.
Host	Connection server name.
Username	Username to connect on the server.
Password	Password to connect on the server.

5.6.2 Private Key

Description



This entry is used to define and configure a **Private Key** credential entry.

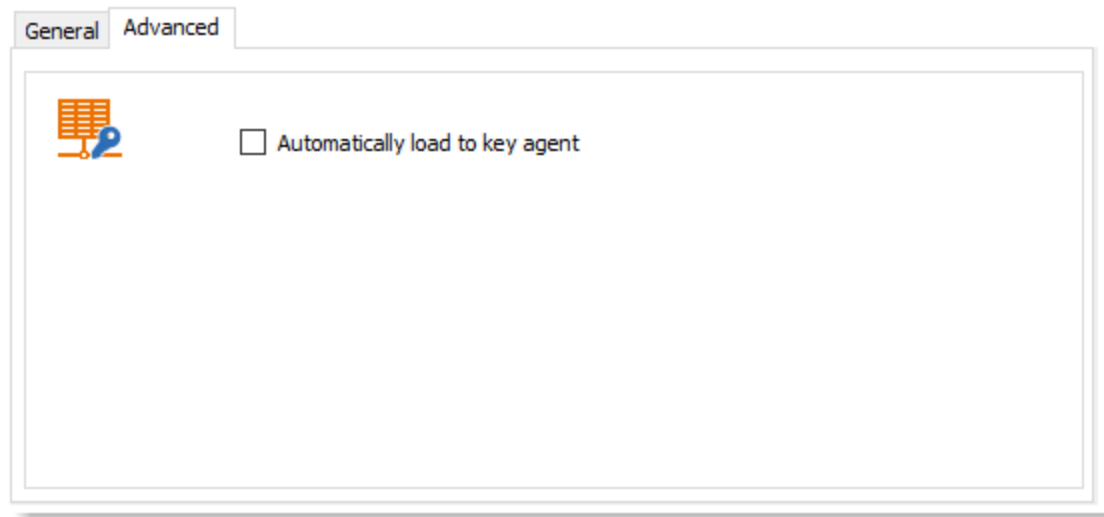
Settings

General

Credentials - Private Key - General tab

Option	Description
Private key type	Select the private key type to use. Select between: <ul style="list-style-type: none"> • No private key: No private key will be sent. • File: Allows you to select a key file to submit as credentials. • Data: Allows you to specify the textual data of the key. This results in the key being stored within the entry itself and eases distribution.
Passphrase	Enter the passphrase to connect.
Username	Always ask for passphrase when connecting.
Password	If using the option File or Data in your Private key type, you have the option to override the username.
File	Select the proper file key.
Private key	Indicate the specific textual data of the key.

Advanced



Credentials - Private Key - Advanced tab

Option	Description
Automatically load to key agent	Automatically load your Private Key in your Key Agent Manager .

5.6.3 Username/Password


Description



This entry is used to define and configure a **Username/Password** credential entry. Provide the username, domain and password to save the credential. This is the default credential type.



Settings

General

 Username

Domain

Always ask password

Password  

Credentials - Username/Password

Option	Description
Username	Enter the username to connect.
Domain	Enter the domain to connect.
Always ask for password	Always ask for password when connecting.
Password	Enter the password to connect.

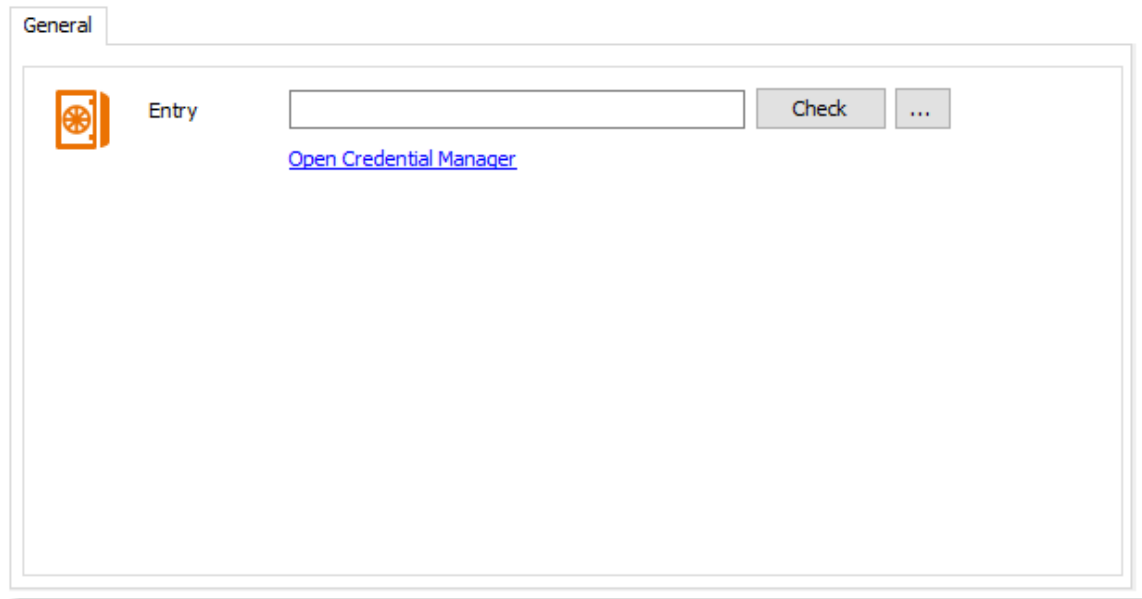
5.6.4 Windows Credential Manager

Description



This entry is used to define and configure a **Windows Credential Manager** credential entry. Use an existing credential entry from the Windows Credential Manager (also called Windows vault).

Settings

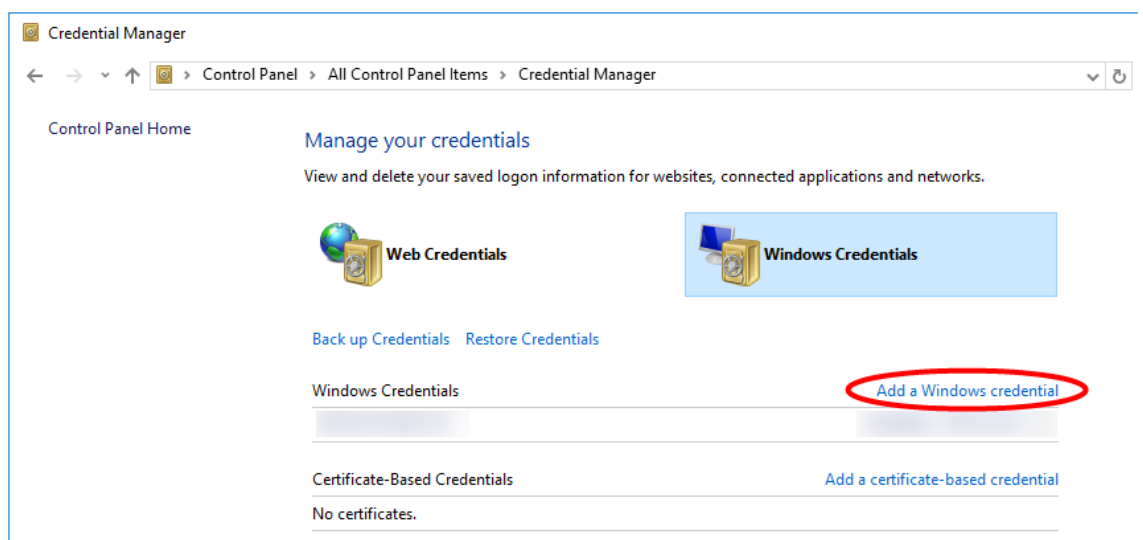


Windows Credential Manager

Option	Description
Entry	Select your entry located in your Credential Manager.

Add a Windows Credential

The Windows Credential Manager allows you to store credentials, such as user names and passwords, which you can use to log on to websites or other computers on a network. By storing your credentials, Windows can automatically log you on to websites or other computers. Credentials are saved in special folders on your computer called vaults. Windows and other programs (such as web browsers) can securely give the credentials in these vaults to other computers and websites.



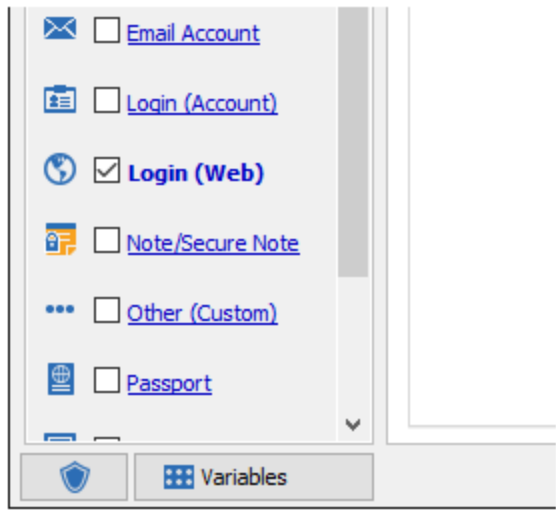
Windows Control Panel - Credential Manager

5.7 Variables

Description

Session variables can be used in any session configuration or with any templates. The variables will be replaced by their corresponding values just prior to establishing a connection.

You can select a variable by double clicking on it directly in the dialog. For ease of use there is a button at the bottom of the edition screen that allows you to select a variable to insert in the currently focused field.

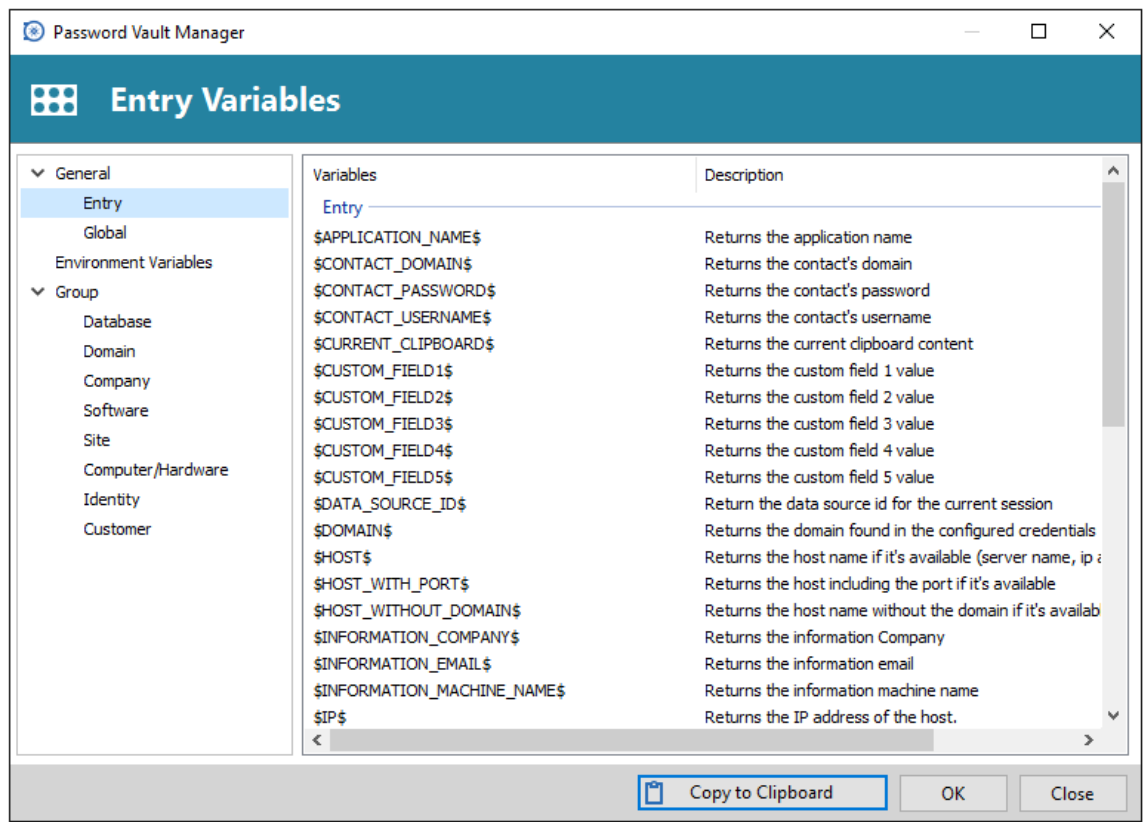


Variables



Variables are case-sensitive and must be typed in UPPERCASE.

Settings



Variables list

The variables are classified under multiple tabs. Not all contexts are available depending on the entry being edited, for example the Parent tab is present only when editing a sub connection.

General



\$PASSWORD\$: For security reasons, this is only available with some specific session types. You must enable it in the [Security](#) section of the entry with "**Allow password in variable**" option.

For an [Advanced Data Source](#), the administrator can [disable](#) usage of this variable for the whole data source.

Entry variables

Option	Description
\$APPLICATION_NAME\$	Return the application name
\$CONTACT_DOMAIN\$	Return the contact's domain
\$CONTACT_PASSWORD\$	Return the contact's password
\$CONTACT_USERNAME\$	Return the contact's username
\$CURRENT_CLIPBOARD\$	Return the current clipboard content
\$CUSTOM_FIELD1\$	Return the custom field field 1 value

\$CUSTOM_FIELD2\$	Return the custom field field 2 value
\$CUSTOM_FIELD3\$	Return the custom field field 3 value
\$CUSTOM_FIELD4\$	Return the custom field field 4 value
\$CUSTOM_FIELD5\$	Return the custom field field 5 value
\$DATASOURCE_ID\$	Return the data source id for the current session
\$DOMAIN\$	Return the domain found in the configured credentials
\$HOST\$	Return the host name if it's available (server name or IP address...)
\$HOST_WITH_PORT\$	Return the host including the port if it is available
\$HOST_WITHOUT_DOMAIN\$	Return the host name without the domain if it is available
\$INFORMATION_COMPANY\$	Return the company specified in information
\$INFORMATION_EMAIL\$	Return the email specified in information
\$INFORMATION_MACHINE_NAME\$	Return the machine name specified in information
\$IP\$	Return the IP specified in information
\$MAC\$	Return the MAC address specified in information
\$MACHINE_DOMAIN\$	Return the machine domain specified in information
\$MACRO_PASSWORD\$	Return the typing macro password
\$NAME\$	Return the entry name
\$PASSWORD\$	This variable is replaced by the password. It's only available when enabled in the advanced options
\$PORT\$	Return the host port if it's available and when it's not the default
\$QUICK_CONNECT\$	This variable is replaced by the quick connect value.
\$REMOTE_MANAGEMENT_SERVER\$	Return the Remote Management Server url (if configured)
\$REMOTE_MANAGEMENT_SERVER_HOST\$	Return the host part of the Remote Management Server url (if configured)
\$SERIAL\$	Return the serial number from invoice tab
\$SERVICE_TAGS\$	Return the service tag field specified in information
\$SESSION_ID\$	Return the current session id (guid)
\$TOOL_DOMAIN\$	Return the tool domain
\$TOOL_PASSWORD\$	Return the tool password
\$TOOLS_USERNAME\$	Return the tool username
\$USERNAME\$	Return the user name found in the configured credentials
\$VIRTUAL_MACHINE_ID\$	Return the virtual machine ID specified in information
\$VPN_DOMAIN\$	Return the VPN's domain
\$VPN_HOST\$	Return the VPN's host
\$VPN_PASSWORD\$	Return the VPN's password

\$VPN_USERNAME\$	Return the VPN's username
------------------	---------------------------

Global variables

Option	Description
\$APPLICATION_PATH\$	Return the application path
\$APPLICATION_USER\$	Return the current data source logged user
\$DATE\$	Return the current date
\$DATE_TEXT\$	Return the current date in a text format to use in a file name. Ex: January 30th 2013 - 20130130
\$DATE_TEXT_ISO\$	Return the current date in a basic ISO 8601 format. EX: January 30th 2013 - 20130130
\$FULLSCREEN_HEIGHT\$	Return the screen full screen height
\$FULLSCREEN_WIDTH\$	Return the screen full screen width
\$LOCAL_IP\$	Return the local IP v4 address
\$MY_MACHINE_NAME\$	Return the current machine name
\$PUBLIC_IP\$	Return the public IP exposed on the internet
\$TIME\$	Return the current time
\$TIME_TEXT\$	Return the current time in a text format to use in a file name. EX: 8h15 30 - 081530
\$TIME_TEXT_ISO\$	Return the text of the current time in the basic ISO 8601 format. EX: 8h15 30 - 081530
\$WORKAREA_HEIGHT\$	Return the screen work area height
\$WORKAREA_WIDTH\$	Return the screen work area width

Global - Data Source variables

Option	Description
\$DATA_SOURCE_DOMAIN\$	Return the current data source domain
\$DATA_SOURCE_NAME\$	Return the current data source name
\$DATA_SOURCE_PASSWORD\$	Return the current data source password
\$DATA_SOURCE_USERNAME\$	Return the current data source user name
\$DATA_SOURCE_USERPROFILE_EMAIL\$	Return the current data source user's email
\$DATA_SOURCE_USERPROFILE_FIRSTNAME\$	Return the current data source user's firstname
\$DATA_SOURCE_USERPROFILE_LASTNAME\$	Return the current data source user's lastname
\$DATA_SOURCE_USERPROFILE_PHONE\$	Return the current data source user's phone number

Environment Variables

This context allows you to access **ANY** environment variable defined in your system. The ones available in the form are the standard ones, but any value enclosed by the percent sign will be expanded using the Windows environment. You could use this to set a custom security token in your user profile and use it from within Password Vault Manager.

Option	Description
%ALLUSERSPROFILE%	C:\ProgramData
%APPDATA%	C:\Users\{username}\AppData\Roaming
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES(x86)%	C:\Program Files (x86)\Common Files
%COMPUTERNAME%	{computername}
%COMSPEC%	C:\Windows\System32\cmd.exe
%HOMEDRIVE%	C:
%HOMEPATH%	\Users\{username}
%LOCALAPPDATA%	C:\Users\{username}\AppData\Local
%LOGONSERVER%	\\{domain_logon_server}
%PATH%	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;{plus program paths}
%PATHEXT%	.com;.exe;.bat;.cmd;.vbs;.vbe;.js;.jse;.wsf;.wsh;.msc
%PROGRAMDATA%	C:\ProgramData
%PROGRAMDATA%	%SystemDrive%\ProgramData
%PROGRAMFILES%	%SystemDrive%\Program Files
%PROGRAMFILES(X86)%	%SystemDrive%\Program Files (x86) (only in 64-bit version)
%PROMPT%	Code for current command prompt format. Code is usually \$P\$G {Drive};
%PSModulePath%	%SystemRoot%\system32\WindowsPowerShell\v1.0\Modules\
%PUBLIC%	%SystemDrive%\Users\Public
%SystemDrive%	C:
%SystemRoot%	%SystemDrive%\Windows
%TEMP%	%SystemDrive%\Users\{username}\AppData\Local\Temp
%TMP%	%SystemDrive%\Users\{username}\AppData\Local\Temp
%USERDOMAIN%	{userdomain}
%USERNAME%	{username}
%USERPROFILE%	%SystemDrive%\Users\{username}
%WINDIR%	C:\Windows

Group

Database

The following context will find any [Database](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$DB_APPLICATION_NAME\$	Return the application name
\$DB_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$DB_CUSTOM_FIELD1\$	Return the database custom field field 1 value
\$DB_CUSTOM_FIELD2\$	Return the database custom field field 2 value
\$DB_CUSTOM_FIELD3\$	Return the database custom field field 3 value
\$DB_CUSTOM_FIELD4\$	Return the database custom field field 4 value
\$DB_CUSTOM_FIELD5\$	Return the database custom field field 5 value
\$DB_DOMAIN\$	Return the domain found in the configured credentials
\$DB_INFORMATION_COMPANY\$	Return the company specified in the database information
\$DB_INFORMATION_EMAIL\$	Return the information email
\$DB_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$DB_NAME\$	Return the session name
\$DB_SERIAL\$	Return the serial number in the invoice tab
\$DB_SERVICE_TAG\$	Return the service tag field located in the information tab
\$DB_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Domain

The following context will find any [Domain](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$DOMAIN_APPLICATION_NAME\$	Return the application name
\$DOMAIN_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$DOMAIN_CUSTOM_FIELD1\$	Return the domain custom field field 1 value
\$DOMAIN_CUSTOM_FIELD2\$	Return the domain custom field field 2 value
\$DOMAIN_CUSTOM_FIELD3\$	Return the domain custom field field 3 value
\$DOMAIN_CUSTOM_FIELD4\$	Return the domain custom field field 4 value
\$DOMAIN_CUSTOM_FIELD5\$	Return the domain custom field field 5 value
\$DOMAIN_DOMAIN\$	Return the domain found in the configured credentials

\$DOMAIN_INFORMATION_COMPANY\$	Return the company specified in the domain information
\$DOMAIN_INFORMATION_EMAIL\$	Return the information email
\$DOMAIN_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$DOMAIN_NAME\$	Return the session name
\$DOMAIN_SERIAL\$	Return the serial number in the invoice tab
\$DOMAIN_SERVICE_TAG\$	Return the service tag field located in the information tab
\$DOMAIN_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Company

The following context will find any [Company](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$COMPANY_APPLICATION_NAME\$	Return the application name
\$COMPANY_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$COMPANY_CUSTOM_FIELD1\$	Return the company custom field field 1 value
\$COMPANY_CUSTOM_FIELD2\$	Return the company custom field field 2 value
\$COMPANY_CUSTOM_FIELD3\$	Return the company custom field field 3 value
\$COMPANY_CUSTOM_FIELD4\$	Return the company custom field field 4 value
\$COMPANY_CUSTOM_FIELD5\$	Return the company custom field field 5 value
\$COMPANY_DOMAIN\$	Return the domain found in the configured credentials
\$COMPANY_INFORMATION_COMPANY\$	Return the company specified in the company information
\$COMPANY_INFORMATION_EMAIL\$	Return the information email
\$COMPANY_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$COMPANY_NAME\$	Return the session name
\$COMPANY_SERIAL\$	Return the serial number in the invoice tab
\$COMPANY_SERVICE_TAG\$	Return the service tag field located in the information tab
\$COMPANY_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Software

The following context will find any [Software](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$SOFTWARE_APPLICATION_NAME\$	Return the application name

\$SOFTWARE_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$SOFTWARE_CUSTOM_FIELD1\$	Return the custom field field 1 value
\$SOFTWARE_CUSTOM_FIELD2\$	Return the custom field field 2 value
\$SOFTWARE_CUSTOM_FIELD3\$	Return the custom field field 3 value
\$SOFTWARE_CUSTOM_FIELD4\$	Return the custom field field 4 value
\$SOFTWARE_CUSTOM_FIELD5\$	Return the custom field field 5 value
\$SOFTWARE_DOMAIN\$	Return the domain found in the configured credentials
\$SOFTWARE_INFORMATION_COMPANY\$	Return the information Company
\$SOFTWARE_INFORMATION_EMAIL\$	Return the information email
\$SOFTWARE_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$SOFTWARE_NAME\$	Return the session name
\$SOFTWARE_SERIAL\$	Return the serial number in the invoice tab
\$SOFTWARE_SERVICE_TAG\$	Return the service tag field located in the information tab
\$SOFTWARE_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Site

The following context will find any [Site](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$SITE_APPLICATION_NAME\$	Return the application name
\$SITE_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$SITE_CUSTOM_FIELD1\$	Return the site custom field field 1 value
\$SITE_CUSTOM_FIELD2\$	Return the site custom field field 2 value
\$SITE_CUSTOM_FIELD3\$	Return the site custom field field 3 value
\$SITE_CUSTOM_FIELD4\$	Return the site custom field field 4 value
\$SITE_CUSTOM_FIELD5\$	Return the site custom field field 5 value
\$SITE_DOMAIN\$	Return the domain found in the configured credentials
\$SITE_INFORMATION_COMPANY\$	Return the company specified in the site information
\$SITE_INFORMATION_EMAIL\$	Return the information email
\$SITE_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$SITE_NAME\$	Return the session name
\$SITE_SERIAL\$	Return the serial number in the invoice tab
\$SITE_SERVICE_TAG\$	Return the service tag field located in the information tab
\$SITE_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Computer/Hardware

The following context will find any [Device](#), [Printer](#) and [Workstation](#) entry type as long as it is in the hierarchy above your current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$COMPUTER_APPLICATION_NAME\$	Return the application name
\$COMPUTER_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$COMPUTER_CUSTOM_FIELD1\$	Return the computer custom field field 1 value
\$COMPUTER_CUSTOM_FIELD2\$	Return the computer custom field field 2 value
\$COMPUTER_CUSTOM_FIELD3\$	Return the computer custom field field 3 value
\$COMPUTER_CUSTOM_FIELD4\$	Return the computer custom field field 4 value
\$COMPUTER_CUSTOM_FIELD5\$	Return the computer custom field field 5 value
\$COMPUTER_DOMAIN\$	Return the computer domain found in the configured credentials
\$COMPUTER_HOST\$	Return the host name if it's available (server name, IP address...)
\$COMPUTER_HOST_WITHOUT_DOMAIN\$	Return the host name without the domain if it's available
\$COMPUTER_INFORMATION_COMPANY\$	Return the company specified in the computer information
\$COMPUTER_INFORMATION_EMAIL\$	Return the information email
\$COMPUTER_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$COMPUTER_IP\$	Return the IP Address
\$COMPUTER_MAC\$	Return the MAC address defined
\$COMPUTER_NAME\$	Return the session name
\$COMPUTER_SERIAL\$	Return the serial number in the invoice tab
\$COMPUTER_SERVICE_TAG\$	Return the service tag field located in the information tab
\$COMPUTER_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Identity

The following context will find any [Identity](#) entry type as long as it is in the hierarchy above you current entry. If there is multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$IDENTITY_APPLICATION_NAME\$	Return the application name
\$IDENTITY_CURRENT_CLIPBOARD\$	Return the current clipboard content

\$IDENTITY_CUSTOM_FIELD1\$	Return the identity custom field field 1 value
\$IDENTITY_CUSTOM_FIELD2\$	Return the identity custom field field 2 value
\$IDENTITY_CUSTOM_FIELD3\$	Return the identity custom field field 3 value
\$IDENTITY_CUSTOM_FIELD4\$	Return the identity custom field field 4 value
\$IDENTITY_CUSTOM_FIELD5\$	Return the identity custom field field 5 value
\$IDENTITY_DOMAIN\$	Return the domain found in the configured credentials
\$IDENTITY_INFORMATION_COMPANY\$	Return the company specified in the identity information
\$IDENTITY_INFORMATION_EMAIL\$	Return the information email
\$IDENTITY_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$IDENTITY_NAME\$	Return the session name
\$IDENTITY_SERIAL\$	Return the serial number in the invoice tab
\$IDENTITY_SERVICE_TAG\$	Return the service tag field located in the information tab
\$IDENTITY_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Customer

The following context will find any [Customer](#) entry type as long as it is in the hierarchy above you current entry. If there IS multiple matches it will take the entry closest in the hierarchy to the current entry.

Option	Description
\$CUSTOMER_APPLICATION_NAME\$	Return the application name
\$CUSTOMER_CURRENT_CLIPBOARD\$	Return the current clipboard content
\$CUSTOMER_CUSTOM_FIELD1\$	Return the customer custom field field 1 value
\$CUSTOMER_CUSTOM_FIELD2\$	Return the customer custom field field 2 value
\$CUSTOMER_CUSTOM_FIELD3\$	Return the customer custom field field 3 value
\$CUSTOMER_CUSTOM_FIELD4\$	Return the customer custom field field 4 value
\$CUSTOMER_CUSTOM_FIELD5\$	Return the customer custom field field 5 value
\$CUSTOMER_DOMAIN\$	Return the domain found in the configured credentials
\$CUSTOMER_INFORMATION_COMPANY\$	Return the company specified in the customer information
\$CUSTOMER_INFORMATION_EMAIL\$	Return the information email
\$CUSTOMER_INFORMATION_MACHINE_NAME\$	Return the information machine name
\$CUSTOMER_NAME\$	Return the session name
\$CUSTOMER_SERIAL\$	Return the serial number in the invoice tab
\$CUSTOMER_SERVICE_TAG\$	Return the service tag field located in the information tab
\$CUSTOMER_VIRTUAL_MACHINE_ID\$	Return the virtual machine ID

Custom fields

Custom fields can contain any required data and can be accessed using the *_CUSTOM_FIELD* variables. Please refer to [Custom Fields](#) for details.

Quick Connect

The **\$QUICK_CONNECT\$** variable will be replaced by the value in the Quick Connect control. It is only useful when a template connection is selected.

5.8 Macro/Script/Tools

Description

The macro script tools can be either a script, a command line, or a helper applicable to a selected entry. Each can be configured and shared in the data source.

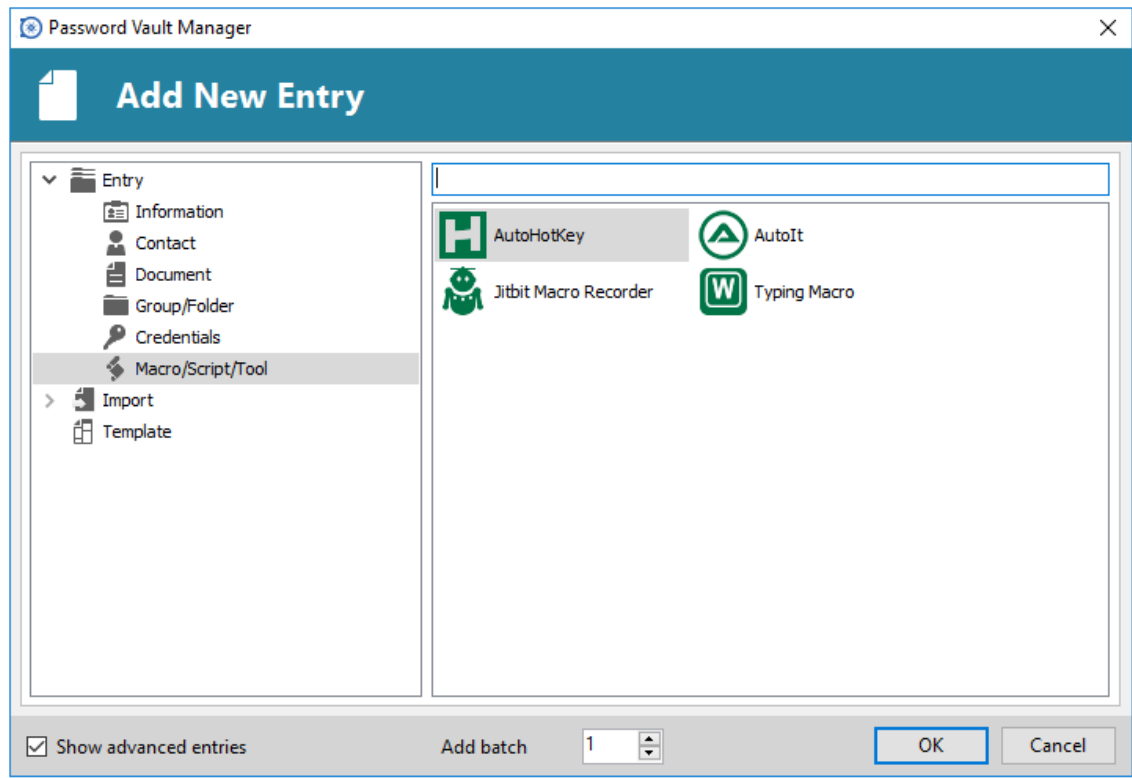
They are listed in the dashboard under the **Macros/Scripts/Tools** section or in the context menu under **Macros/Scripts/Tools**.

Tools are commonly used to retrieve information, perform an action, change an item, or change a configuration.



The [Variables](#) can be used as parameters for the Macro/Script/Tool.

Macro/Script/Tool Manager



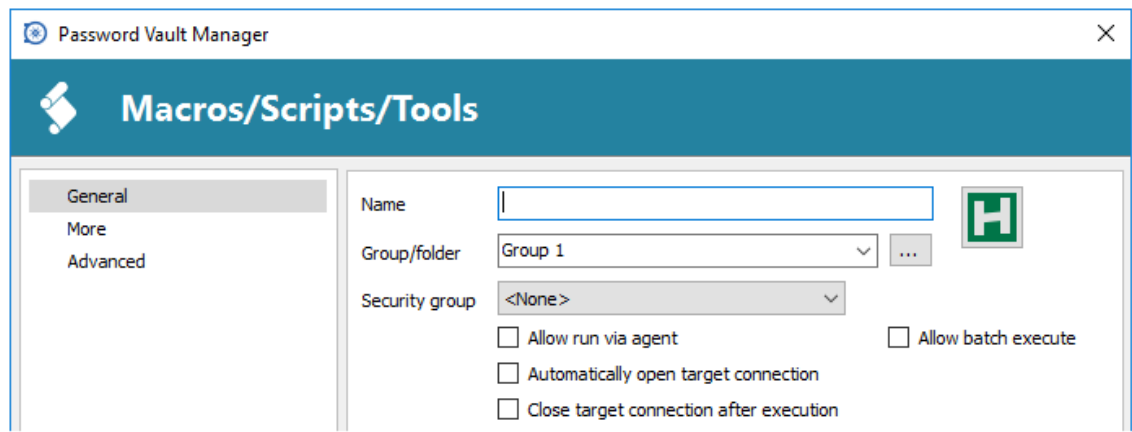
New Entry - Macro/Script/Tool

Please consult these topics below for more details:

- [AutoHotKey](#)
- [AutoIt](#)
- [Jitbit Macro Recorder](#)
- [Typing Macro](#)

General Settings

Those settings are identical for every Macro/Script/Tools entry.



Macro/Scripts/Tools - General settings

Option	Description
Allow run via agent	Allows you to launch a script through an Agent.
Automatically open target connection	Force the opening of a connection before executing the macro/script/tool.
Close target connection after connection	Automatically close the connection after executing the macro/script/tool.
Allow batch execute	Allows you to execute the macro on multiple machines at the same time.

5.8.1 AuthoHotKey

Description



This entry is used to integrate **AutoHotKey** freeware tool. It is used for automation, Hotkeys and scripting.

Settings

Command file mode

The default mode is to run command files. Simply press the button to select your file. This entry is used to integrate **AutoHotKey** freeware tool. It is used for automation, Hotkeys and scripting.

General

H Run Command File Embedded Script

Launch unconditionally Restart Errors to StdOut

Arguments

Use Default Working directory

Wait for application to exit (Remote Desktop Manager will be unavailable)

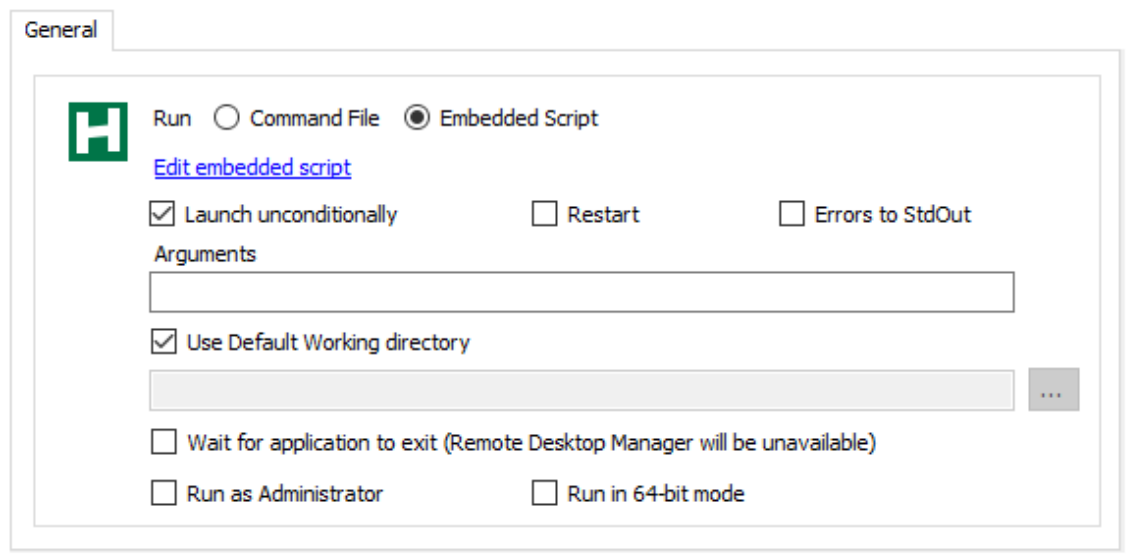
Run as Administrator Run in 64-bit mode

Option	Description
Launch unconditionally	This is sometimes required because some hooks are not installed to preserve memory. Please consult the AutoHotKey manual.
Restart	Restarts the script if it is currently running.

Errors to StdOut	Errors messages are redirected to the standard output instead of displaying dialog.
Arguments	Parameters to send to your AutoHotKey script.
Working directory	Choose to run from the default working directory of AutoHotKey, or specify the working directory.
Wait for application to exit	Runs the script synchronously, this means that the RDM process will wait for the script to return before resuming execution. This will cause RDM to be unresponsive while the script runs.
Run as Administrator	Elevates the process to run as an administrator.
Run in 64-bit mode	Runs by using the 64 bit architecture.

Embedded script mode

Choosing the Embedded Script radio button toggles the interface as follows.



Macros/Scripts/Tools - AutoHotKey

Prerequisites

- Local installation of AutoHotKey

5.8.2 Autolt

Description



This entry is used to integrate **Autolt** macro/script/tool.

Settings

Command file mode

The default mode is to run command files. Simply press the ellipsis button to select your file.

General

Run Command File Embedded Script

Arguments

Use Default Working directory

Wait for application to exit (Remote Desktop Manager will be unavailable)

Run as Administrator Run in 64-bit mode


Autolt - Command File

Option	Description
Arguments	Parameters to send to your Autolt script.
Use default Working directory	Choose to run from the default working directory of Autolt, or specify the working directory.
Wait for application to exit	Runs the script synchronously, this means that the Password Vault Manager process will wait for the script to return before resuming execution. This will cause Password Vault Manager to be unresponsive while the script runs.
Run as Administrator	Elevates the process to run as an administrator .
Run in 64-bit mode	Runs by using the 64-bit architecture.

Embedded script mode

Choosing the Embedded Script radio button toggles the interface as follows.

General

 Run Command File Embedded Script

[Edit embedded script](#)

Arguments

Use Default Working directory

...

Wait for application to exit (Remote Desktop Manager will be unavailable)

Run as Administrator Run in 64-bit mode

Autolt - Embedded Script

Option	Description
Edit embedded script	Type your own script which will then be embedded in the session.
Arguments	Parameters to send to your Autolt script.
Use default Working directory	Choose to run from the default working directory of Autolt, or specify the working directory.
Wait for application to exit	Runs the script synchronously, this means that the Password Vault Manager process will wait for the script to return before resuming execution. This will cause Password Vault Manager to be unresponsive while the script runs.
Run as Administrator	Elevates the process to run as an administrator .
Run in 64-bit mode	Runs by using the 64-bit architecture.

5.8.3 Jitbit Macro Recorder

Description



This entry is used to integrate a **Jitbit Macro Recorder** macro/script/tool.

Settings

Command File

Jitbit Macro Recorder - Command File

Option	Description
Wait for application to exit	Runs the command line synchronously, this means that the Remote Desktop Manager process will wait for the command line to return before resuming execution. This will cause Remote Desktop Manager to be unresponsive during that time.
Shell Execute	Uses the shell execute mode. Please refer to the Windows documentation.

Embedded Script

JitBit Macro Recorder - Embedded Script

Option	Description
Edit embedded script	Type your own script which will then be embedded in the session.
Wait for application to exit	Runs the command line synchronously, this means that the Remote Desktop Manager process will wait for the command line to return before resuming execution. This will cause Remote Desktop Manager to be unresponsive during that time.

Shell Execute	Uses the shell execute mode. Please refer to the Windows documentation.
---------------	---

5.8.4 Typing Macro


Description




This entry is used to integrate a ***built-in macro***. It allows you to automatically execute a typing macro once a session has been established.

Settings

General

 Typing macro



Initial wait sec

Delay time {Delay} ms

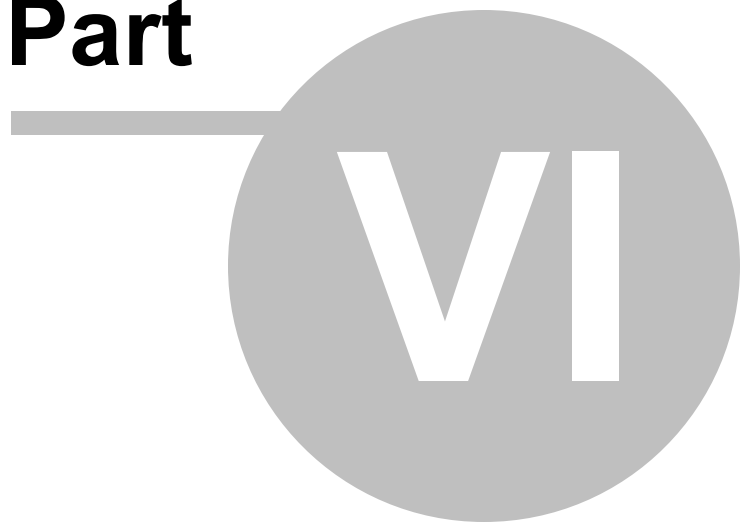
Command ms

Typing Macro

For more information please see [Typing Macro](#).

Support/Resources

Part



6 Support/Resources

6.1 Keyboard Shortcuts

Description

Here are the default keyboard shortcuts for various commands. These can be modified in **File - Options - User Interface - Keyboard**.

General

Action	Shortcut
Filter	Ctrl+F
Force Refresh	Ctrl+F5
Online Help	F1
Quick Connect	Ctrl+Alt+Q
Refresh	F5

Edit

Action	Shortcut
Add Credential Entry	Alt+Shift+N
Add Group/Folder	Ctrl+Shift+N
Add Information	Ctrl+Alt+N
Add Session	Ctrl+N
Delete Entry	Ctrl+Del
Duplicate Entry	Ctrl+D
Edit Entry	Ctrl+E
Edit Entry (Local Specific Settings)	Ctrl+Alt+E
Edit Entry (User Specific Settings)	Ctrl+Shift+E
New Entry	Ins
Rename Entry	F2

Actions

Action	Shortcut
Clipboard - Copy Connection String	Ctrl+Alt+H
Clipboard - Copy Domain	Ctrl+Alt+B
Clipboard - Copy Host Name	Ctrl+H
Clipboard - Copy Password	Ctrl+Shift+B
Clipboard - Copy Url	Ctrl+Shift+H

Clipboard - Copy Username	Ctrl+B
Execute Typing Macro	Ctrl+Shift+A
Run Macro From List	None
View Password	Ctrl+P

View

Action	Shortcut
Dashboard	Alt+F6
Details	F12
Favorite Entries	F10
Filter	None
Footer Pane	Alt+Shift+F7
Grouped Tab Pane	Ctrl+Alt+F9
Header Pane	Alt+Shift+F6
Large Icons	F6
Most Recent Used Entries	F9
Opened Sessions	F8
Status Bar	Alt+F7
Tabbed Entries Pane	Alt+F9
Tiles	F3
Top Pane	Alt+F11
Tree View	F7
View Credential Entries	None
View Macro/Script/Tool Entries	None
View Synchronizers	None
View Usage Log (Local)	F11
View Usage Log	None
View VPN Entries	None

Navigation

Action	Shortcut
Change Current Data Source	Ctrl+Shift+D
Focus Dashboard	Ctrl+Shift+L
Focus Tab	Ctrl+Shift+Up
Focus Tree/List	Ctrl+L
Goto Bookmark 1	Ctrl+1
Goto Bookmark 2	Ctrl+2
Goto Bookmark 3	Ctrl+3
Goto Bookmark 4	Ctrl+4
Goto Bookmark 5	Ctrl+5

Goto Bookmark 6	Ctrl+6
Goto Bookmark 7	Ctrl+7
Goto Bookmark 8	Ctrl+8
Goto Bookmark 9	Ctrl+9
Select Next Tab	Ctrl+Shift+Left
Select Previous Tab	Ctrl+Shift+Right
Set Bookmark 1	Ctrl+Shift+1
Set Bookmark 2	Ctrl+Shift+2
Set Bookmark 3	Ctrl+Shift+3
Set Bookmark 4	Ctrl+Shift+4
Set Bookmark 5	Ctrl+Shift+5
Set Bookmark 6	Ctrl+Shift+6
Set Bookmark 7	Ctrl+Shift+7
Set Bookmark 8	Ctrl+Shift+8
Set Bookmark 9	Ctrl+Shift+9

ImportExport

Action	Shortcut
Export Entry as Remote Desktop File (.rdp)	None
Export Selection (.rdm)	None
Import Entries (.rdm, .pvm, .vnc, .rdp)	Ctrl+Shift+I

6.2 Command Line Arguments

Description

Password Vault Manager can be launched using a command line.



Some features are only available in the Enterprise edition.

Usage: RemoteDesktopManager.exe [parameters]

Parameters	
{filename [*.rdm,*.rdp]}	Open in embedded or external mode the connection from file name.
/Silent	Execute the application minimized in a system tray icon. This option cannot be combined with other parameters.
/Datasource:{datasource id}	Specify the data source id (available in the Advanced Tab of the session).

/Session:{session ID};{session ID}...	Specify one or more session IDs (available in the Advanced Tab of the session)
/UserName:{username}	
/Domain:{domain}	
/Password:{password}	
/ChangePassword:{new password}	Change the session password. Only available for Remote Desktop sessions and embedded passwords. The data source ID and the session ID are required.
/RegisterUser:"{registration user}"	Change the Password Vault Manager username. The value must be in double quotes.
/RegisterSerial:"{serial number}"	Change the Password Vault Manager serial number. The value must be in double quotes.
/Template:{template ID}	Open the template ID with the specified host name and an optional username/password.
/Host:{host name}	
/UserName:{username}	
/Domain:{domain}	The template ID is the Session ID of the template (available in the Advanced Tab of the template).
/Password:{password}	
/Profiler	Starts the profiler at start of application. Good for profiling the start process.
/Title:"{title}"	Specify a tab title when using an embedded session.
/Filter:{filter}	Execute the application with the filter filled with a parameter.
/TabPage: Dashboard	The Dashboard is selected at startup of the application.

Usage

Example #1 - Open a template and connect to a host

```
PasswordVaultManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Template:a
```

Example #2 - Open a session

```
RemoteDesktopManager.exe /DataSource:178c2fda-dab4-4f41-98df-6e3205c0a011 /Session:47
```

Example #3 - Register the application

```
RemoteDesktopManager.exe /RegisterUser:"First name, Last name" /RegisterSerial:"xxxxx
```

6.3 Lexicon

Description

Password Vault Manager is a feature rich program that has an extensive set of functionality. Here are the major concepts that are important to understand in order to use the program to its full potential.

Data source

A container for entries. It can be a local file, a database (either local or shared), or our own Devolutions Online Database service. You can use multiple distinct data sources in the program, although only one is considered active at one point in time. See data source [Overview](#) for more information.

Entry

All items in your data source are entries. There are multiple types and sometimes even sub-types. The [entry](#) is an abstract concept that serves as a container for all specific types.

Credential entry

A [credential entry](#) is used to control access to a resource by identifying the user. It can be a classic username/password pair held by the program, or even by an external source.

Information entry

An [information entry](#) is meant to contain various information like account information, emails, serial numbers. It's principal use in Password Vault Manager is to hold Web site information, from the URL to the credentials. This allows auto login on the specified web site.

6.4 Technical Support

Standard Support plan

Support is solely through our online forums at <http://forum.devolutions.net/>.

Extended and Premium support plans

Subscribers of a paid support plan receive an email address and a plan ID. You should send your support requests to the appropriate email address and provide your plan ID in the subject line.

You are also encouraged to find information and ask questions in our forums at <http://forum.devolutions.net/>. They contain years of relevant information and have the benefit of being enriched for the whole community when we post an answer.



Please consult our [Support Policy](#) for more information.








6.5 Follow Us

Overview

Get the hottest information about our products - tips and tricks, case studies and new release announcements!

This is not a marketing newsletter. We focus on the issues that matter to you, whether you're looking for up-to-the-minute software tutorials, additional outside resources, or a peek at how others are using our products.

Links		
	Facebook	http://facebook.remotedesktopmanager.com
	LinkedIn	http://linkedin.remotedesktopmanager.com

	RSS feeds	http://rss.remotedesktopmanager.com
	Twitter	http://twitter.remotedesktopmanager.com
	YouTube	http://youtube.remotedesktopmanager.com
	Blog	http://blog.remotedesktopmanager.com
	Google+	http://plus.remotedesktopmanager.com/
	Spicework	http://spice.devolutions.net
	Forum	http://forum.devolutions.net

6.6 Troubleshooting

Description

Consult these sections for more information.

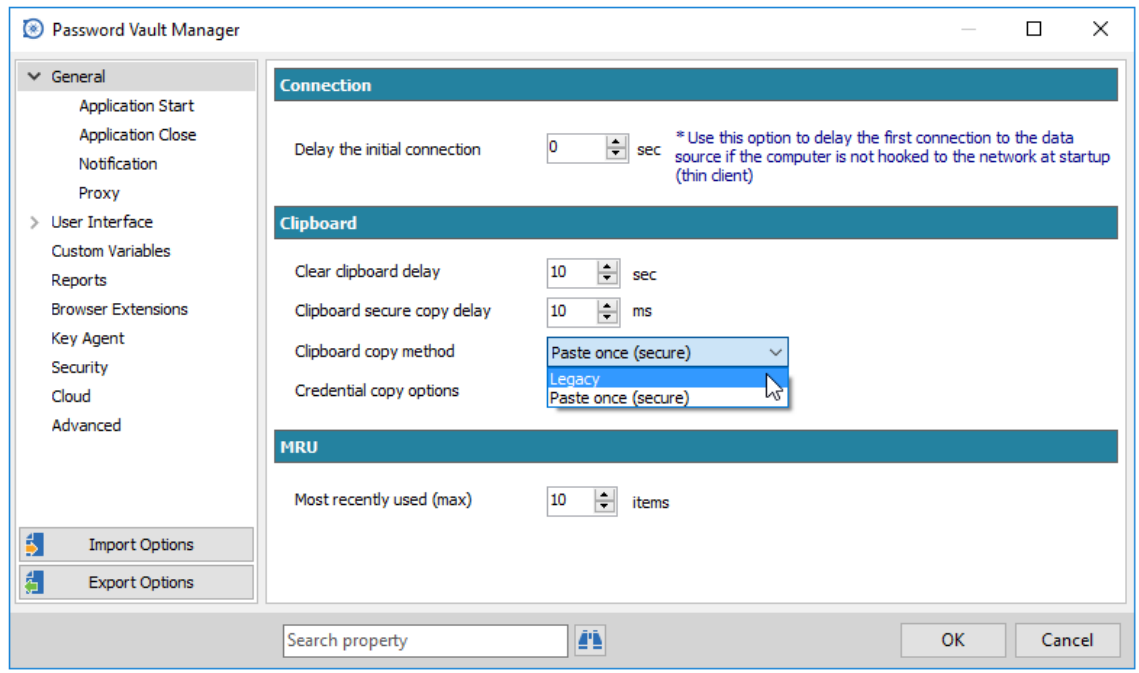
- [Clipboard](#)
- [2-Factor Authentication](#)
- [Data Sources](#)
- [Performance](#)
- [Unable to uninstall](#)
- [General](#)
- [SQL Server](#)
- [Welcome Page](#)

6.6.1 Clipboard

Issues

Citrix GotoAssist interferes with the data in the clipboard, preventing you from copy/pasting information.

We have a system option where you can revert to the legacy copy/paste method. ***File - Options - General (section) - Clipboard (sub-section) - Clipboard copy method*** and set it to ***Legacy***. This should resolve the issue.



File - General

6.6.2 2-Factor Authentication

Issues

With Google Authenticator, you are getting an Invalid Password error even though you are sure of entering the proper one.

The computer clock must be within a small error margin in order to generate the proper authenticator code. We recommend using a NNTP server in order to keep your computer clock synchronized.

You have lost the device

Your Password Vault Manager is set to authenticate with Yubikey or Google Authenticator. You no longer have the Yubikey key or the Google Authenticator and you want to turn off this option to connect on Password Vault Manager.

If you had install it using the default settings, the configuration file is %localappdata%\Devolutions\PasswordVaultManager\PasswordVaultManager.cfg

You can choose to simply delete it, obviously all of your settings will be lost, alternatively you can open it and remove everything between the EncryptedDataSources tags. You will have to re-enter all of your data sources and point to either the file or database that you were using.

6.6.3 Data Sources

Errors

Unable to connect to a Data Source

1. The name of the data source is entered incorrectly.

2. The machine is unable to resolve the name of the data source host using DNS.
3. An Anti-virus or Firewall is blocking the application.

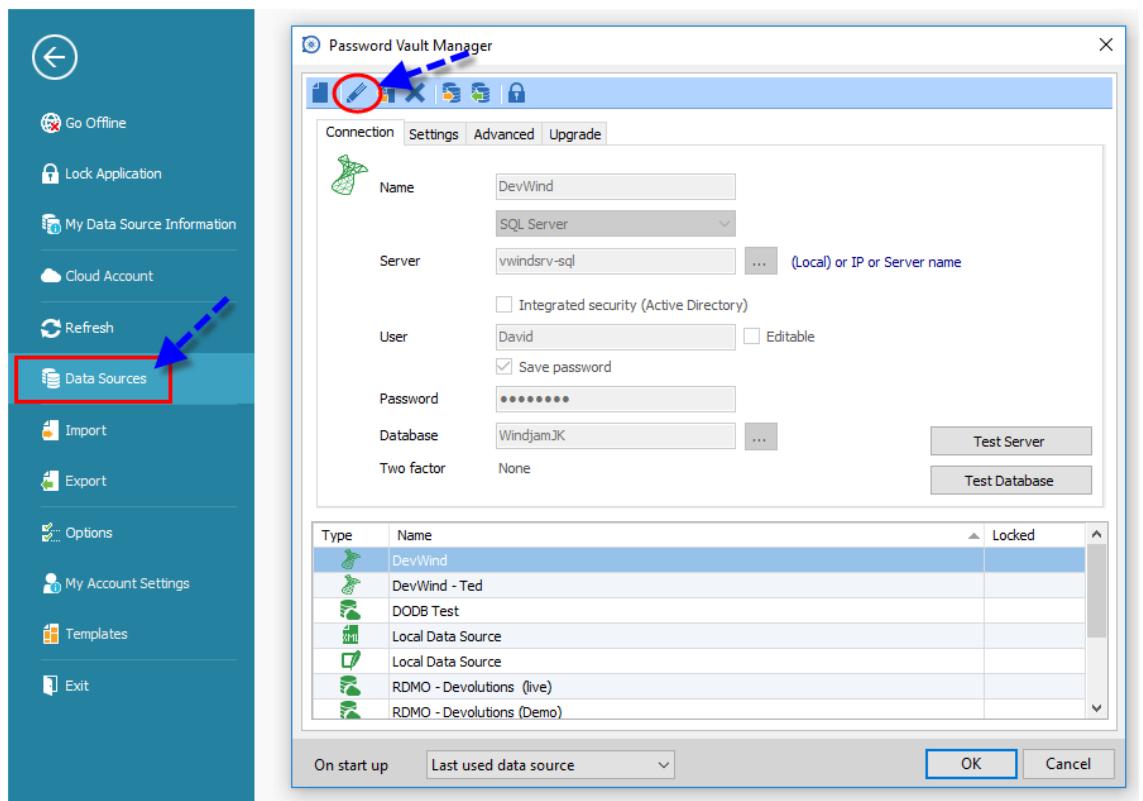
Sending the schema to Devolutions for analysis



This feature is only available for data sources that are backed by a database management system: MariaDB, SQL Azure, SQL Server and MySQL.

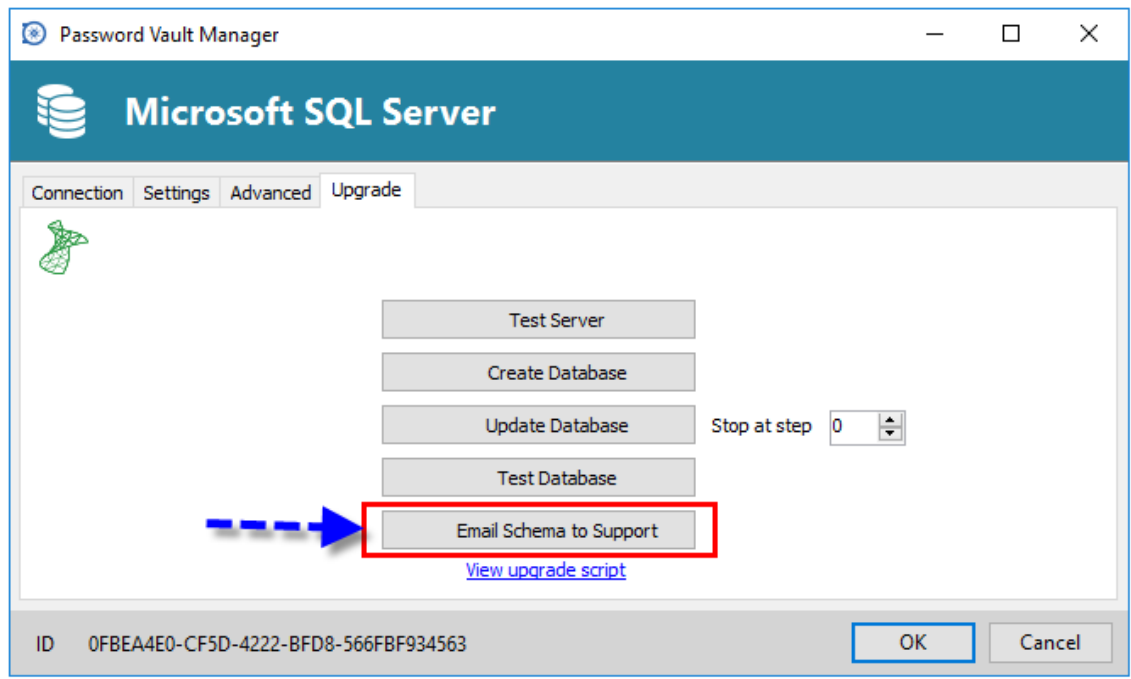
When requested by the Devolutions Support team during a support process, you may be asked to send us your database schema for thorough analysis of your issue.

1. Go in **File - Data Sources - Edit Data Source**



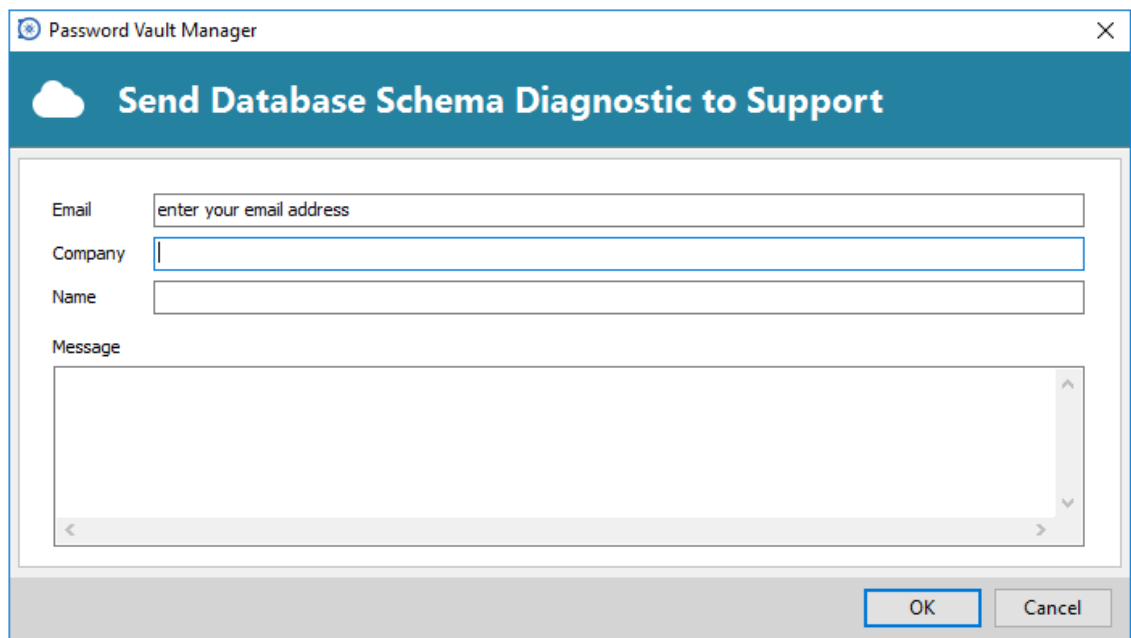
File - Data Sources - Edit

2. In the tab **Upgrade** click on **Email Schema to Support**



Email Schema to Support

3. Fill in all the requested information and click on **Send**. Enter your email address in the **Email** field, it will automatically be sent to our Support team.



Send Diagnostic

Option	Description
Email	Enter your own email address.

Company	Enter your Company name.
Name	Use the same title as the one first used to report the issue
Message	If you haven't described your issue before, enter a short description of it.

6.6.4 Performance

Description

Please consult the topics below for more information on how to troubleshoot performance issues.

- [Diagnostic](#)
- [Refresh](#)
- [Startup](#)

6.6.4.1 Diagnostic

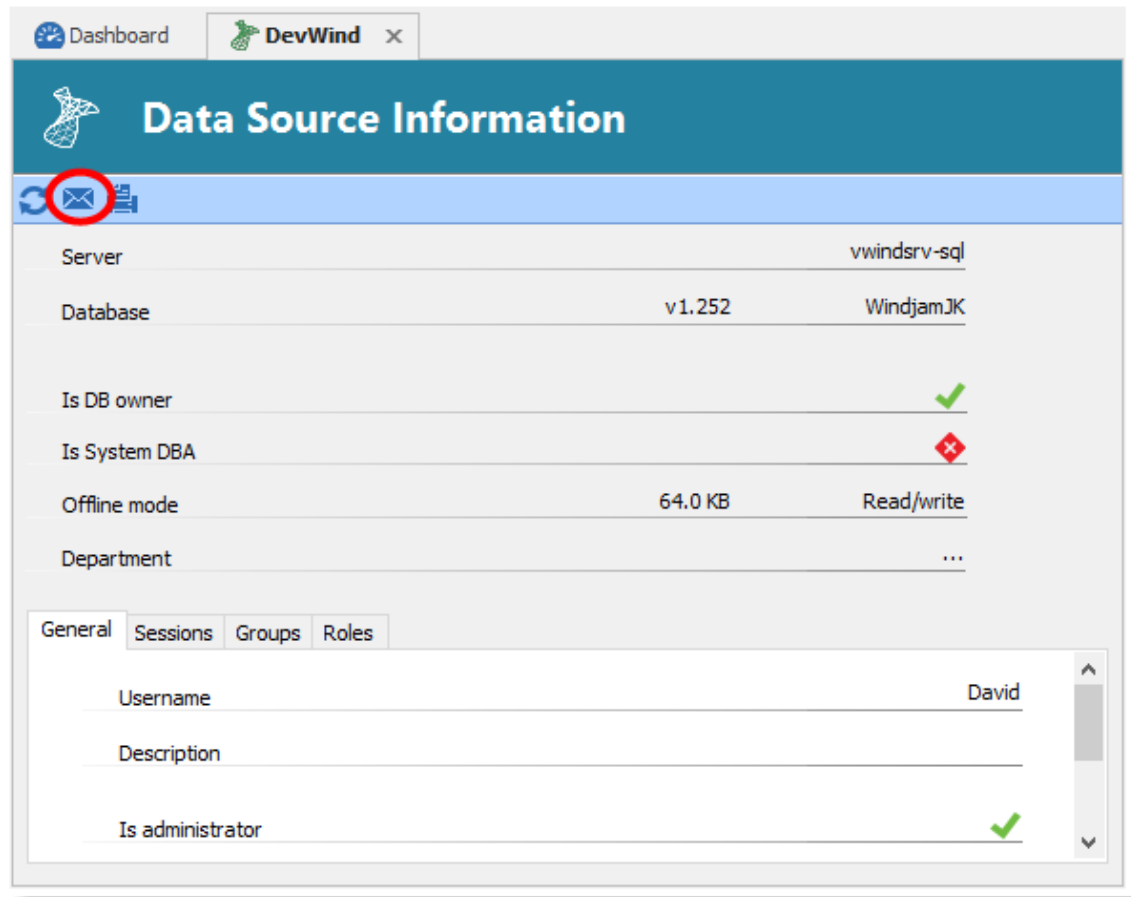
Description

Sometimes when a performance issue occurs while using Password Vault Manager, the support personnel may ask you to send information. Here are three sources of information that the support team requires to help diagnose your issue.

Procedures

My Data Source Information

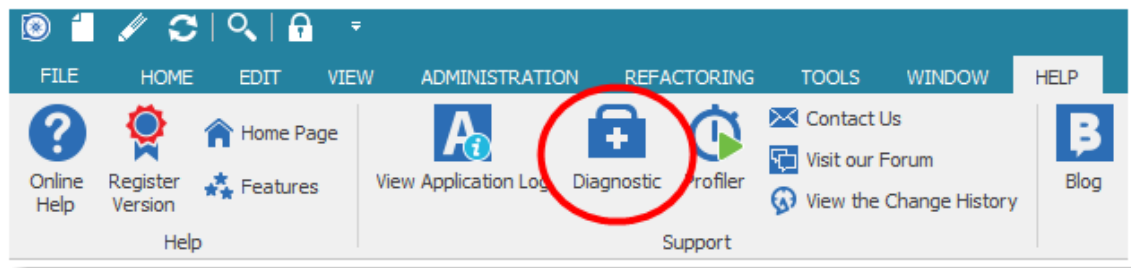
1. Open **File - My Data Source Information**.
2. Click on the **envelope button** to send the information to our support team. In the following dialog, ensure you specify enough information to link the report to the appropriate ticket, if the process was started from the forum include your forum user name.



Data Source Information

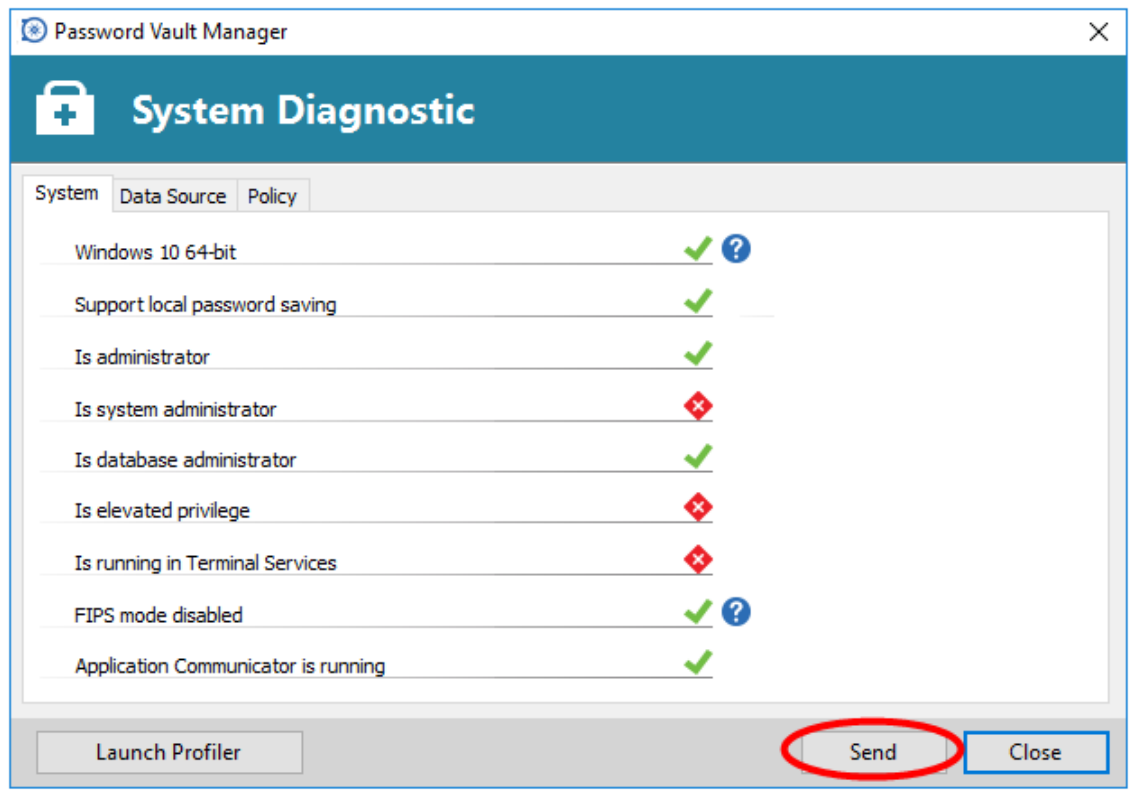
Diagnostic

1. Open **Help - Diagnostic**.



Help - Diagnostic

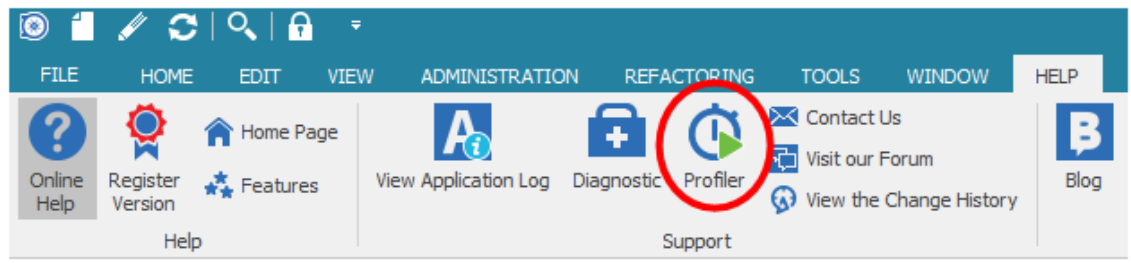
2. Click on the **Send** button. In the following dialog, ensure you specify enough information to link the report to the appropriate ticket, if the process was started from the forum, please include your forum user name.



System Diagnostic

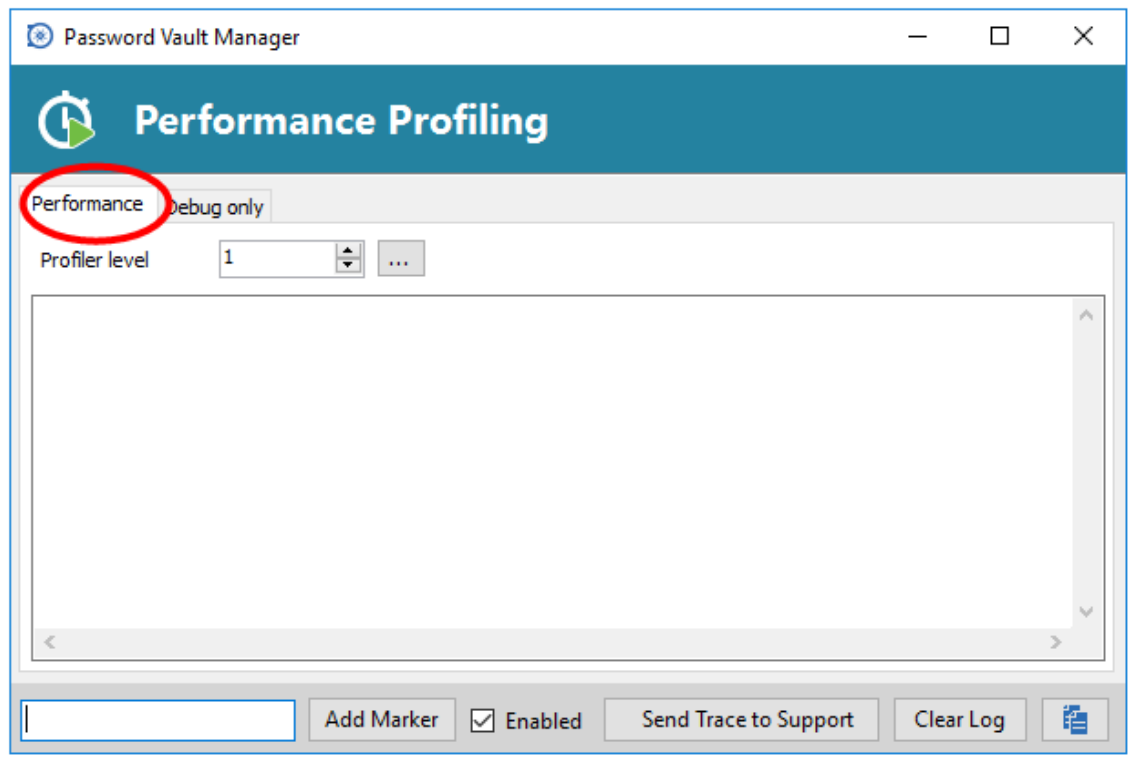
Profiler

1. Open **Help - Profiler**, move the window aside to clear the main window of Password Vault Manager



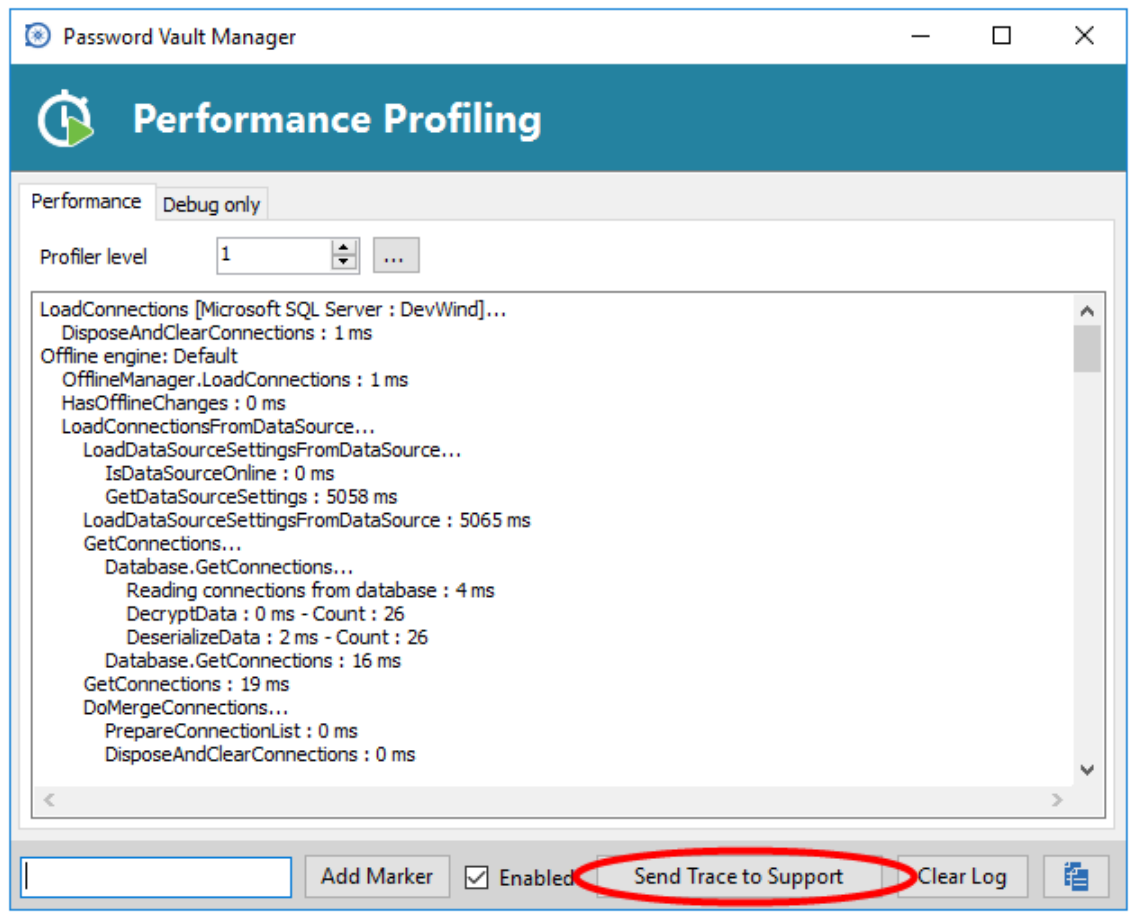
Help - Profiler

2. Select the **Performance** tab.



Performance Profiling - Performance

3. In Password Vault Manager, hold the **CTRL** key and press the refresh button.
4. Information will be added in the **Performance** tab.



Profiler

5. Click on the **Send Trace to Support** button. In the following dialog, ensure you specify enough information to link the report to the appropriate ticket, if the process was started from the forum, please include your forum user name.

6.6.4.2 Refresh

Description

This category affects all data source refreshes, therefore also the initial load at program startup.

Heavy usage of custom images

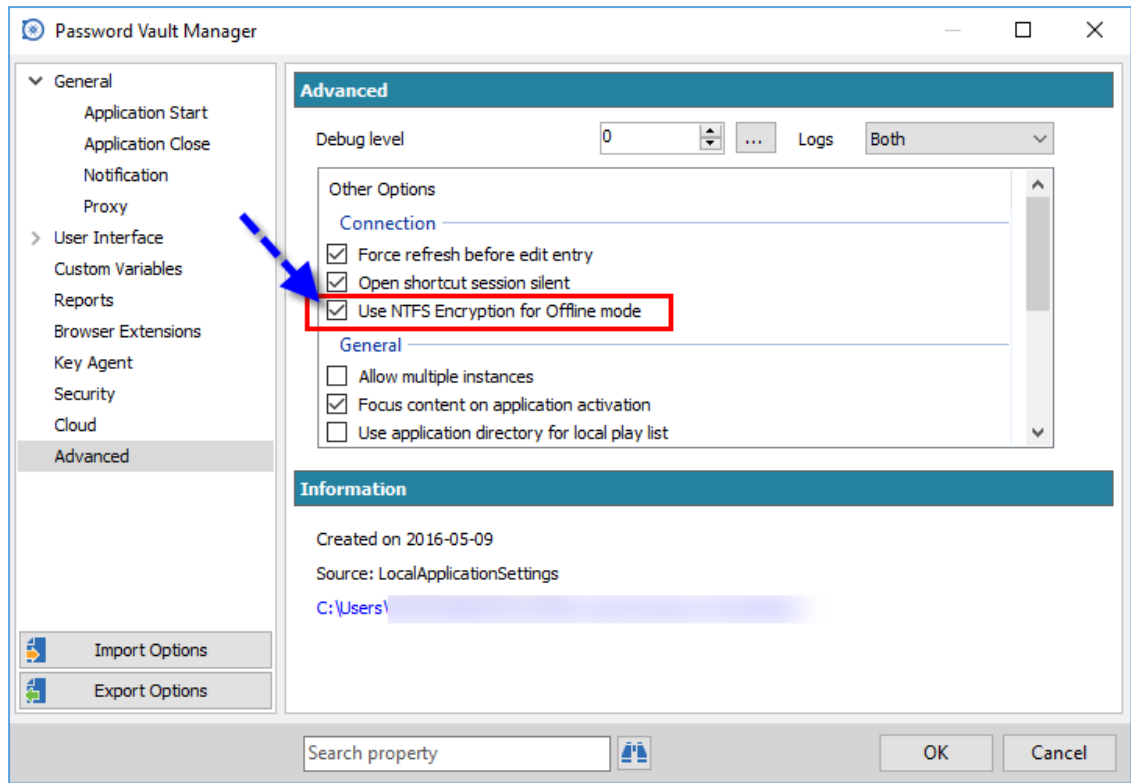
Custom images need to be stored in the data source, this results in the size of the configuration becoming problematic if there are too many entries using them. If that becomes the case it would be better to revert to built-in images.

Heavy usage of RTF description

RTF in itself is not a real issue until you decide to embed images in the description. This results in the same problem as using custom images, namely the size of the configuration becoming too large. If that becomes the case, reduce the size of your descriptions.

Offline mode activated for data source

When you enable the [Offline Mode](#), a local file is created and is kept in sync with the data source. This file is encrypted using the Windows built-in NTFS encryption which can cause delays in refreshing the local data file. This is rarely the case but seems to happen on computers on a domain which has been hardened by the network administrator. You can turn off this option by unchecking **Use NTFS Encryption for offline mode in File - Options - Advanced**.



NTFS Encryption

Classic UI

The new Ribbon UI is modern and allows for infinite variations of panel organization, but it does take more calculations by the UI layer. On most system this is not a cause for noticeable performance slowdown, but on others setting the User Interface to Classic UI (v7.x) in the general options tab will definitely help.

6.6.4.3 Startup

Startup

If you experience slow startup times there are a few things to try in order to reduce the time before the application is available for use. Please note that this is exceptional and occurs when your data source contains a great number of connections.

Slow startup on machines that are not connected to the internet.

For your security, we "sign" our program with a code signature. This results in the validity of the signature being checked at application startup. If the machine is not connected to the internet the application will wait for a response until a timeout occurs. For a detailed explanation and a workaround please read the following:

- [Improving Application Start Up Time](#)
- <http://blogs.technet.com/b/markrussinovich/archive/2009/05/26/3244913.aspx>

The workaround is to create a text file in Password Vault Manager installation folder, named RemoteDesktopManager.exe.config and containing the following:

```
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

6.6.5 Unable to uninstall

Description

Unable to install or uninstall Remote Desktop Manager from your computer

To fix issues that you may encounter with the installation or removal of the application, please run the Microsoft Troubleshooter tool on your computer

https://support.microsoft.com/en-us/mats/program_install_and_uninstall

6.6.6 General

Errors

“Could not load file or assembly "System.EnterpriseServices Wrapper.dll or one of its dependencies. The system cannot find the path specified.”

This error is due to a corrupted Microsoft's .NET Framework 2.0 installation. We recommend that you try and repair the .NET Framework, or follow the instructions in the Microsoft Knowledge base article "[How to repair an existing installation of the .NET Framework](#)".

My mapped network drive(s) are not available when using Run As Administrator to launch Password Vault Manager

This is because of User Access Control (UAC), a built-in security layer of Windows. Effectively you are considered a different user with different preferences, the Mapped network drives being one such preference. In order to have the same mapped drives you have a few options

1. Using an elevated command prompt, recreate the same mapped drive(s) using the *NET USE {DRIVENAME} {SHARENAME} /PERSISTENT:YES* command
2. Modifying the registry to link connections between the accounts , see <http://support.microsoft.com/kb/937624>.

6.6.7 SQL Server

Errors

Unable to connect to SQL Server

On a new SQL Server installation, remote connections must be allowed manually. Follow these [Directions](#) to enable connectivity.

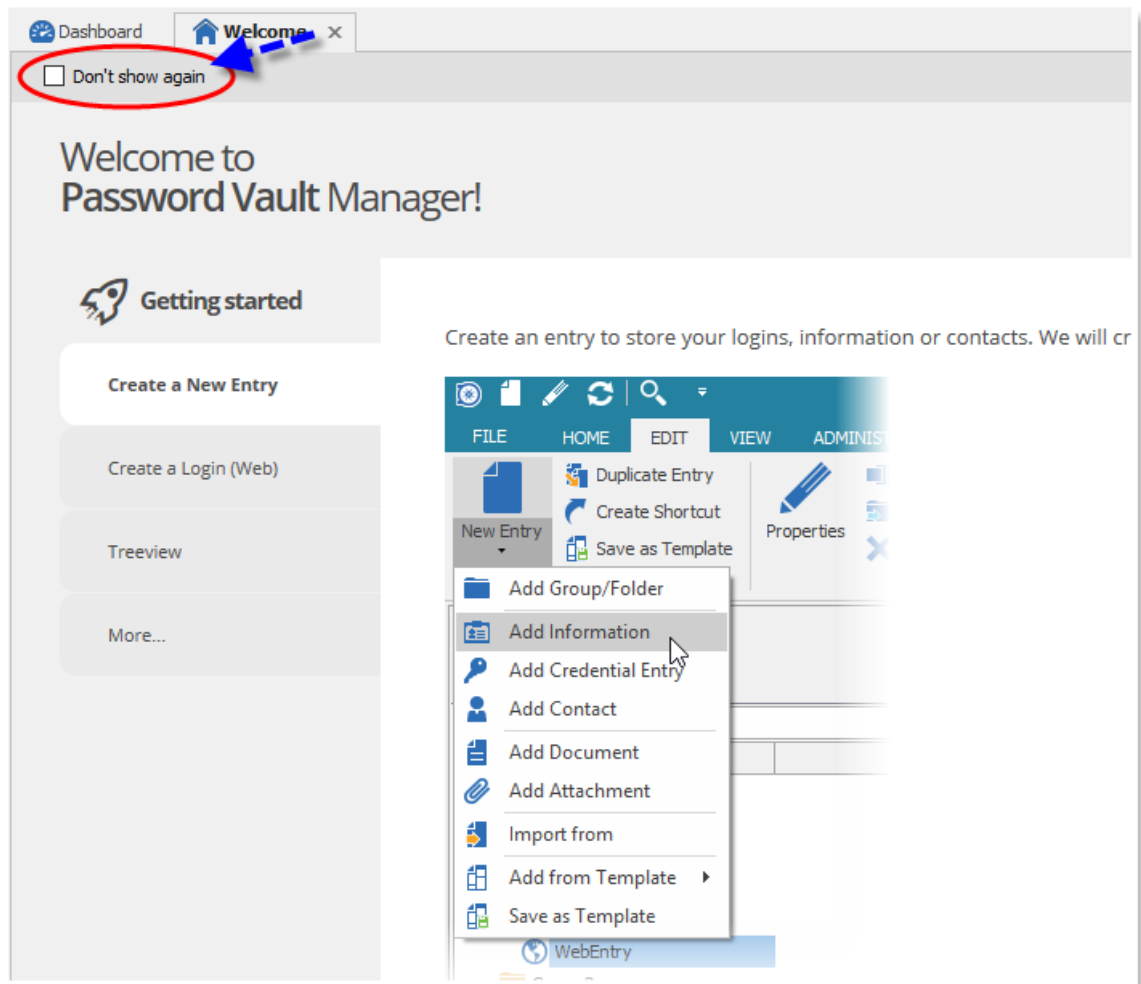
6.6.8 Welcome Page

Description

We added a new **Getting Started** page at the opening of Password Vault Manager but you don't want to see it every time you open our application.

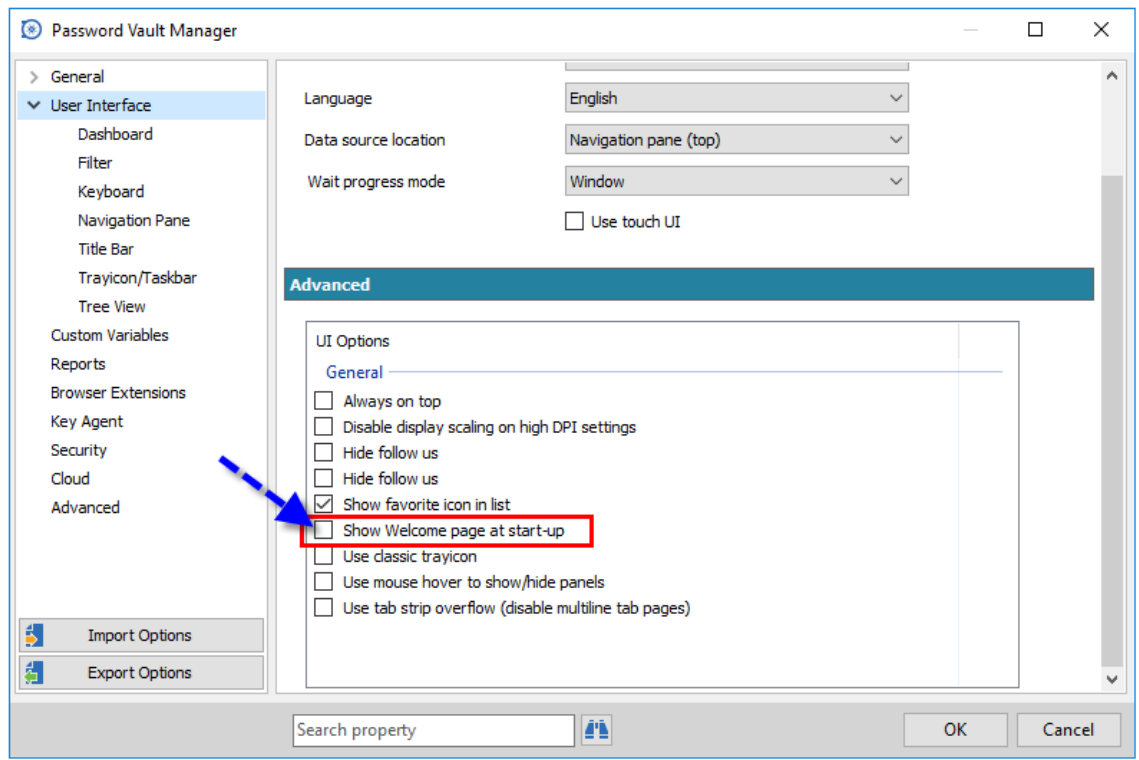
There are 2 ways of removing that page.

1. Simply click on **Don't show again**.



Getting Started

2. Go in **File - Options- User Interface** and uncheck **Show Welcome page at start-up**.



User Interface - Advanced

6.7 Knowledge Base

6.7.1 Internet outbound access

Description

While using Password Vault Manager, some of these URL are visited and should be added to the proxy's configuration if it is present on the infrastructure of the network.

URL	Description
http://passwordvaultmanager.com/	If File - Options - Application Start - Check for update at startup is activated.
https://cloud.devolutions.net	When a Devolutions cloud account is used.
http://help.passwordvaultmanager.com	When the Help button is clicked.
https://crm.devolutions.net	For licensing or registrations check.
URL of the cloud service	Depending on the service used (Azure, AWS, Devolutions Server, Spiceworks, etc.).

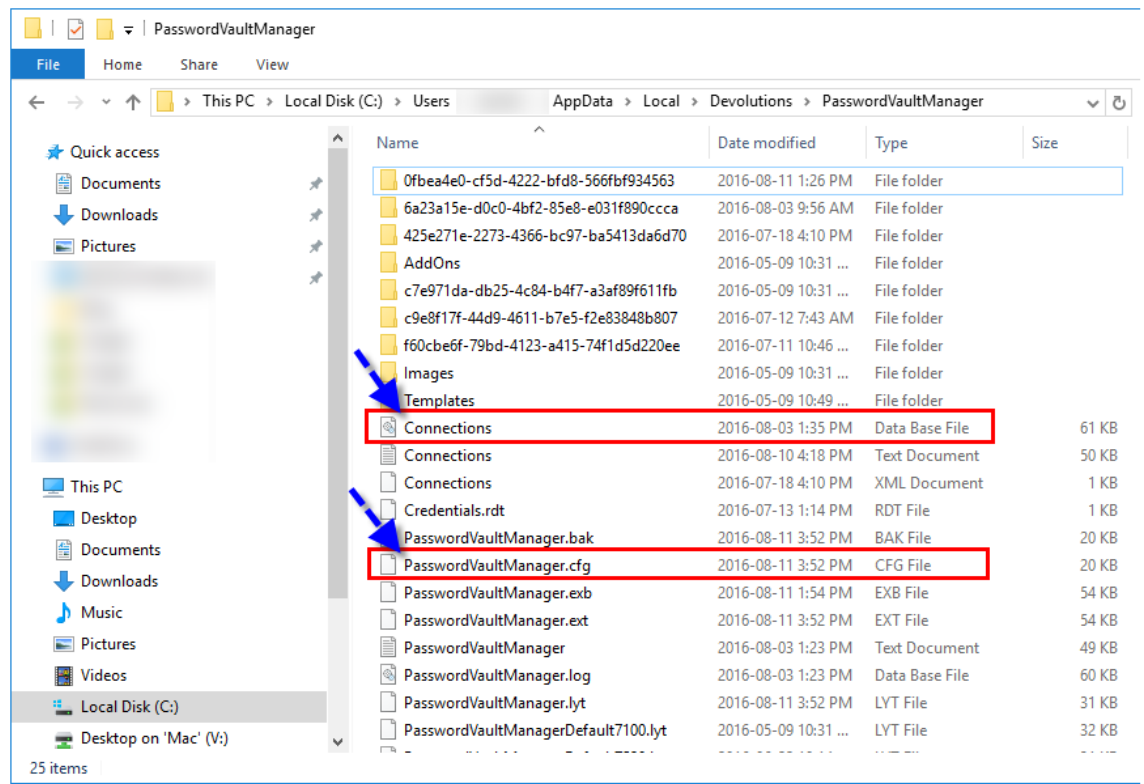
6.7.2 Free Edition to Enterprise

Description

This Knowledge Base article will help you get through the process of passing from the free edition of Password Vault Manager to the enterprise edition.

Steps

1. Start by installing Password Vault Manager [Enterprise Edition](#).
2. Once the installation is completed, transfer your data and configuration from `%localappdata%\Devolutions\PasswordVaultManagerFree` to `%localappdata%\Devolutions\PasswordVaultManager`. The configuration is in the PasswordVaultManagerFree.cfg file and the data, by default, is in Connections.db.



AppData Folder

3. Those are the 2 most important files to keep. Once you have copied those two files from your **Password Vault Manager Free** to your **Password Vault Manager Enterprise Edition** and completed your set up, you can then safely uninstall Password Vault Manager Free edition.

6.8 Best Practices

Description

The following recommendations are provided for new and experienced users alike. Password Vault Manager has a lot of flexibility and sometimes we are faced with so many choices that we aren't sure of

the proper decision to make or its impacts. Read below to find out what our own AND the community's experience has shown is the preferred way of operating Password Vault Manager in various scenarios.

Most of these recommendations apply to the Enterprise Edition because the range of options is so much greater than the Free Edition.

6.8.1 Backups

Description

It is recommended to always have a current backup of your data source. Since we support a wide range of data stores, you should use the best solution for your chosen data source.



Amazon S3

Please consult Amazon website for their backup policy.



Devolutions Server

Devolutions Server use a SQL Server database to store the data. We recommend creating a maintenance plan to perform automatic backups regularly. This video is a good start on the subject: [Setting up a Maintenance Plan to Backup Databases](#)



Dropbox

Please consult Amazon website for their backup policy.



FTP

We recommend creating a maintenance plan to perform automatic backups regularly.



MariaDB

We recommend creating a maintenance plan to perform automatic backups regularly.



Microsoft Access

Our recommended backup solution is to use our free [Online Backup Service](#)



Microsoft SQL azure

We recommend creating a maintenance plan to perform automatic backups regularly.



Microsoft SQL Server

We recommend creating a maintenance plan to perform automatic backups regularly. This video is a good start on the subject: [Setting up a Maintenance Plan to Backup Databases](#)



MySQL

We recommend creating a maintenance plan to perform automatic backups regularly.



Online Database

The protection offered by Online Database is for Disaster recovery only, for instance a hardware failure. Note that we cannot restore a backup of a single database. Using our [Entry History](#) and our [View Deleted](#) features, you can revert any change on specific sessions.



Online Drive

Our recommended backup solution is to use our free [Online Backup Service](#)



SFTP

We recommend creating a maintenance plan to perform automatic backups regularly.



SQLite

Our recommended backup solution is to use our free [Online Backup Service](#)



Web

We recommend creating a maintenance plan to perform automatic backups regularly.



XML

Our recommended backup solution is to use our free [Online Backup Service](#)

6.8.2 Credential Management for Teams

Description

Password Vault Manager allows for multiple ways of handling credentials in a team environment. This brings flexibility, but at the cost of creating difficulty when you need to choose an implementation for a particular requirement.

Below are multiple methods to handle credentials, you may choose one or many depending on your requirements. We often see scenarios where our client manages his own infrastructure, as well as their customers'. Group entries below groups/folders depending on the kind of credential management that you must use. Each of these groups/folders could use a different scheme.

Preamble

Here are a few notions that you must know prior to getting to the scenarios, they are at the core of Password Vault Manager usage.

Inherited Credentials

Credentials can be set using many schemes, be it on entries themselves, or even on groups/folders. This allows you to set a credential for an entry to *inherited*. Whenever this is used, the credential resolver will simply go up a level and use the credential set on the parent entry. If this is a folder, and you also set this to *inherited* credentials, it indicates to the resolver to simply continue up to the parent folder.

Private Vault

The [Private Vault](#) is available for some advanced data sources, please consult its topic to learn more. It allows you to create your own private entries. In the cases where a user must use a credential that is exclusive to him, using the private vault is an obvious choice.

User Specific Settings

[User Specific Settings](#) allows you to override some settings of entries in the data source. One of the most typical use for this is to override the credentials. It can be done on credentials, sessions, groups/folders, etc.

Scenarios

All devices are accessed with a common set of shared credentials

The common set of credentials are set on the entries themselves in the navigation tree view. If the credentials are the same for certain entries, store the entries under a group/folder to which you've assigned the credentials, and set the child sessions to use ***inherited*** credentials.

Every user must use their own credentials for all of the entries

All of the entries and intermediate groups/folders are set to inherited credentials. At the top level folders, use the ***User Specific Settings*** to fill in your credentials. You can type them in directly if you have only one set of credentials, but if you have many we suggest you create them in your [Private Vault](#) and link to them.

Most users use a common set of shared credentials, admins must use different credentials

The common set of credentials are set on the entries themselves in the navigation tree view. Admins must use the User Specific Settings in order to override the credentials. The source for the credentials can be directly on the overridden entry or from the private vault.

Password Vault Manager features that can help you refactor multiple entries at once

You had already created multiple entries and you need to modify a lot of them... Well no worries, we have the following features to help you out.

Batch Edit

[Batch Edit](#) allows you to modify multiple entries at once, please consult its topic to see how to modify credentials for multiple entries at once.

6.9 Tutorials

Our tutorials are published on [Devolutions YouTube channel](#). We have three main categories of tutorials:

- Overview: Brief presentation of a product.
- Getting Started: Procedure to get up and running in a quick fashion.
- Spotlight on: Detailed presentation of a specific aspect of our products.

Obviously some tutorials will not fit in one of these categories, but our focus is to deliver quality information as soon as possible after the release of a new or modified feature.

Please use our forums if documentation is missing or plain wrong, we will do our best to correct the situation.

6.9.1 Overview

Description

Our tutorials are published on [Devolutions YouTube channel](#). We have three main categories of tutorials:

- [Overview](#): Brief presentation of a product.
- [Getting Started](#): Procedure to get up and running in a quick fashion.
- [Spotlight On...](#): Detailed presentation of a specific aspect of our products.

Obviously some tutorials will not fit in one of these categories, but our focus is to deliver quality information as soon as possible after the release of a new or modified feature.


Please use our forums if documentation is missing or plain wrong, we will do our best to correct the situation.

6.9.2 Getting Started

Description

Please consult [our tutorials page](#).

Getting Started videos should present a step-by-step sequence to start using a product. They differ from our "Spotlight On..." series in that they are targeted on significant feature of the product, rather than on a piece of a whole.

Getting Started...	Description	Link
with Password Vault Manager	Learn how to quickly and easily set up Password Vault Manager and get started with your team.	 Watch Vid

Please consult [our tutorials page](#)

6.9.3 Spotlight On...

Description

This video category is destined to contain a great number of short tutorials that provide information on a really specific aspect or feature of Password Vault Manager.

Ultimately, all longer videos will be replaced by a series of **Spotlight on...** tutorials.

Our [Getting Started](#) topic contains a sequence of steps to follow to go through the initial setup under various conditions. Please refer to it for the best sequence for your environment.

Spotlight On...

Title	Description	Link
... User Interface	Learn how to manipulate the user interface elements of Password Vault Manager and adapt it	Coming soon

Title	Description	Link
	according to your preferences.	
... Data Sources		Coming soon
... Offline Mode		Coming soon
... Search/Filter		Coming soon
... Quick Connect		Coming soon
... Entries		Coming soon
... Security Groups		Coming soon
... Templates and Default Settings		Coming soon

6.10 Tips and Tricks

Description

Our favorite tips and tricks are in this section.

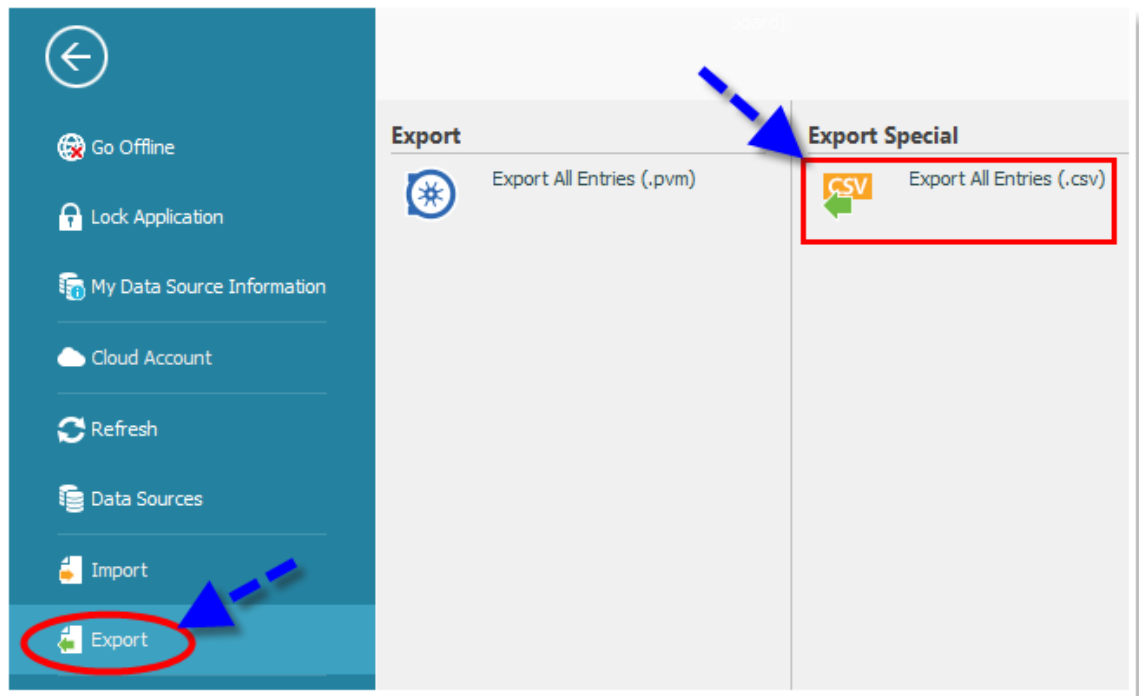
If you have a suggestion for improving an existing tip or even to suggest a new one, please send a note to infos@devolutions.net.

6.10.1 Create a list of Credentials

Description

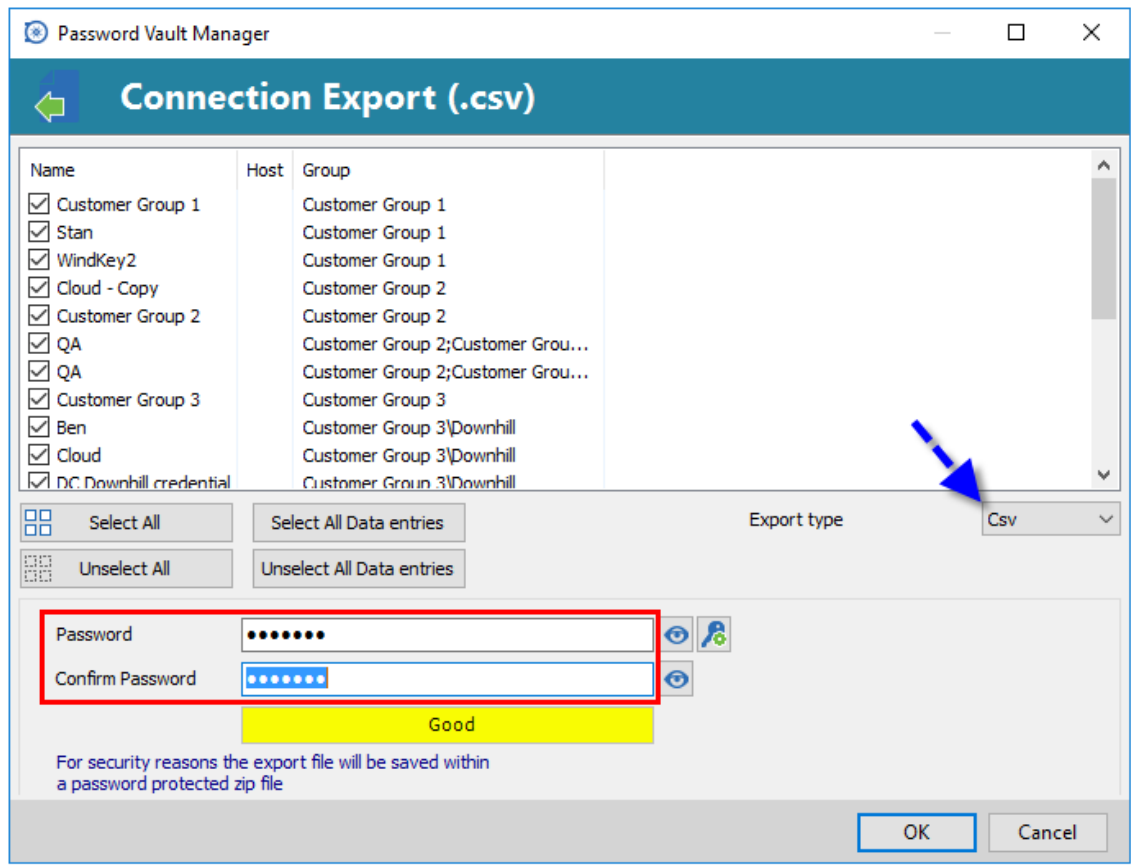
If you wish to create a report containing a full list of all your credentials here are the steps to follow:

1. In the menu **File - Export - Export Special**, select the option **Export All Entries (.csv)**.



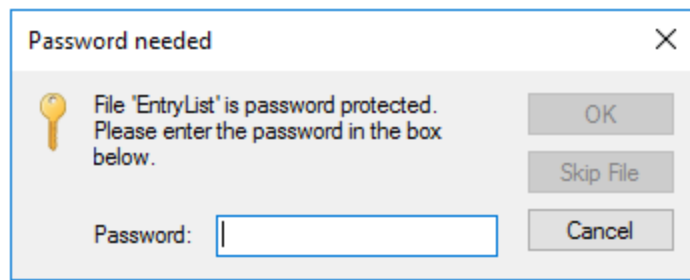
Export All Entries (.csv)

2. Enter a password to create a password protected zip file.



Connection Export

3. When opening your zip file, you will be prompted for your password.



Password

4. Once you have entered your password, your full list of credentials will open in an Excel sheet format (.csv).

	A	B	C	D	E
1	ConnectionType	ConnectionSubType	SubMode	Name	Group
2	Group/Folder		0	Customer Group 1	Customer Group 1
3	Data (Login (Account))		0	Stan	Customer Group 1
4	Username / Password		0	WindKey2	Customer Group 1
5	Username / Password		0	Cloud - Copy	Customer Group 2
6	Group/Folder		0	Customer Group 2	Customer Group 2
7	Data (Login (Web))		0	QA	Customer Group 2;Customer Group 1
8	Data (Login (Web))		0	QA	Customer Group 2;Customer Group 1
9	Group/Folder		0	Customer Group 3	Customer Group 3
10	Data (Login (Account))		0	Ben	Customer Group 3\Downhill

List of Credentials - Excel Sheet

6.10.2 Data Migration

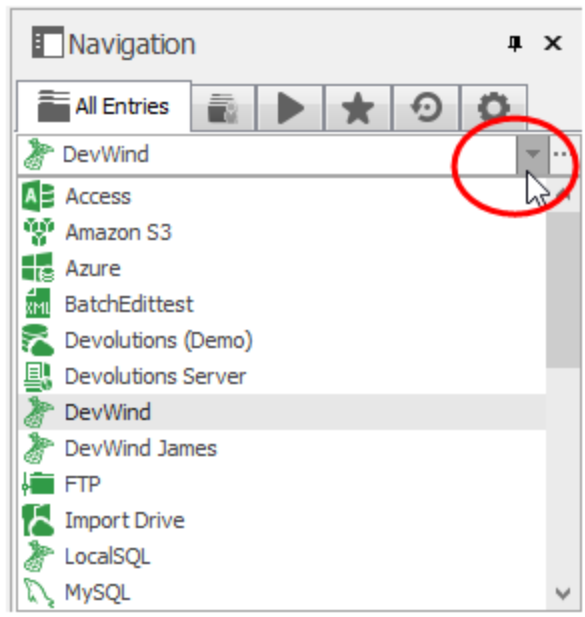
Description

Here are the steps to follow when copying data from one data source to another.

The migration is simply an export of your original data source followed by an import in the new destination data source.

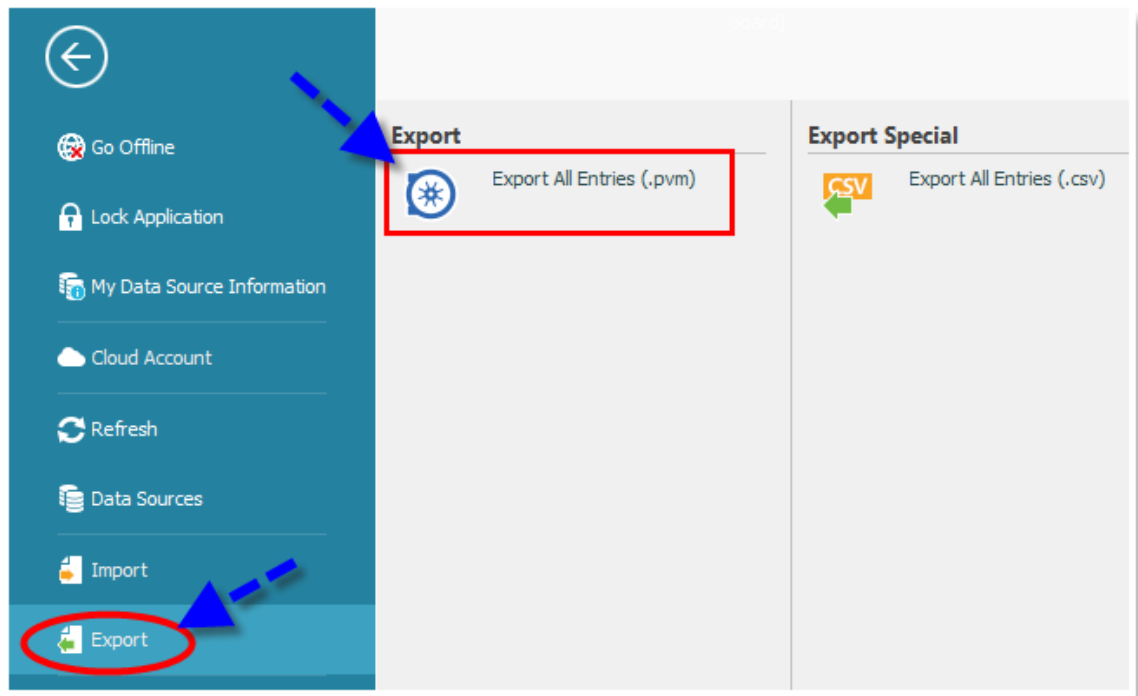
Export

1. Select your data source in the data source selection drop down.



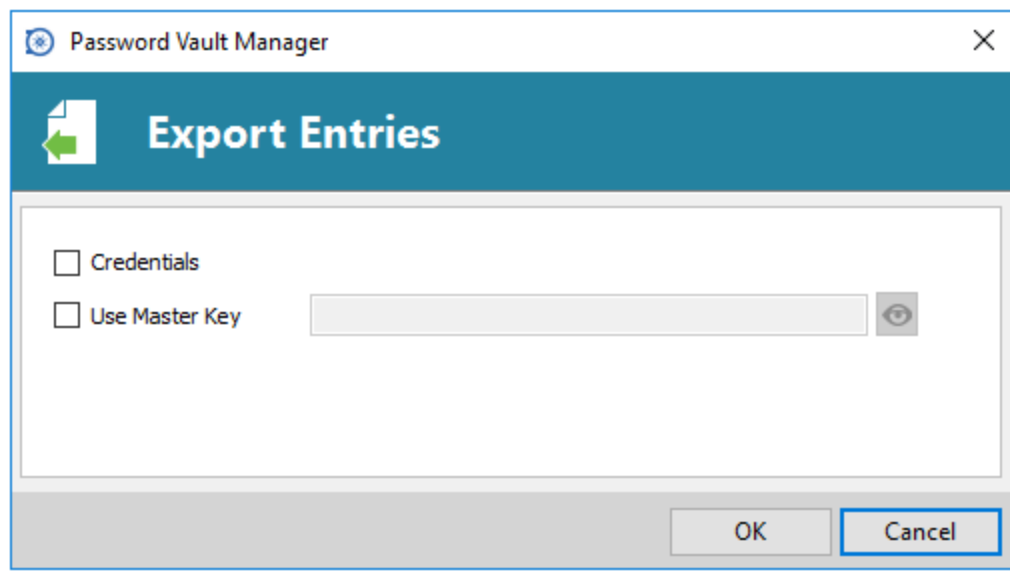
Data source drop down menu

2. Select **File - Export - Export All Entries (.rdm)**.



Export All Entries (.pvm)

3. Select your export entries options. You can choose to include your credentials in your export and may also select to use a Master Key as an added security layer.



Export Entries options

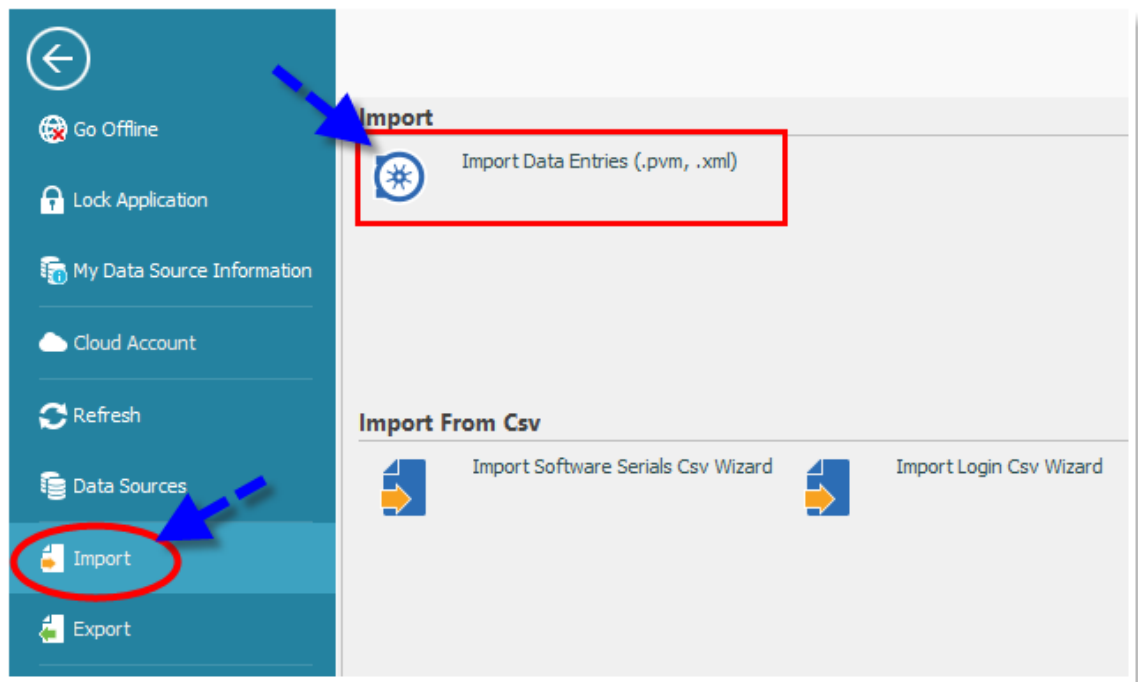


Ensure that you do not forget the Master Key as you will not be able to decrypt the data without it.

4. Save the file with the name and location of your choice.

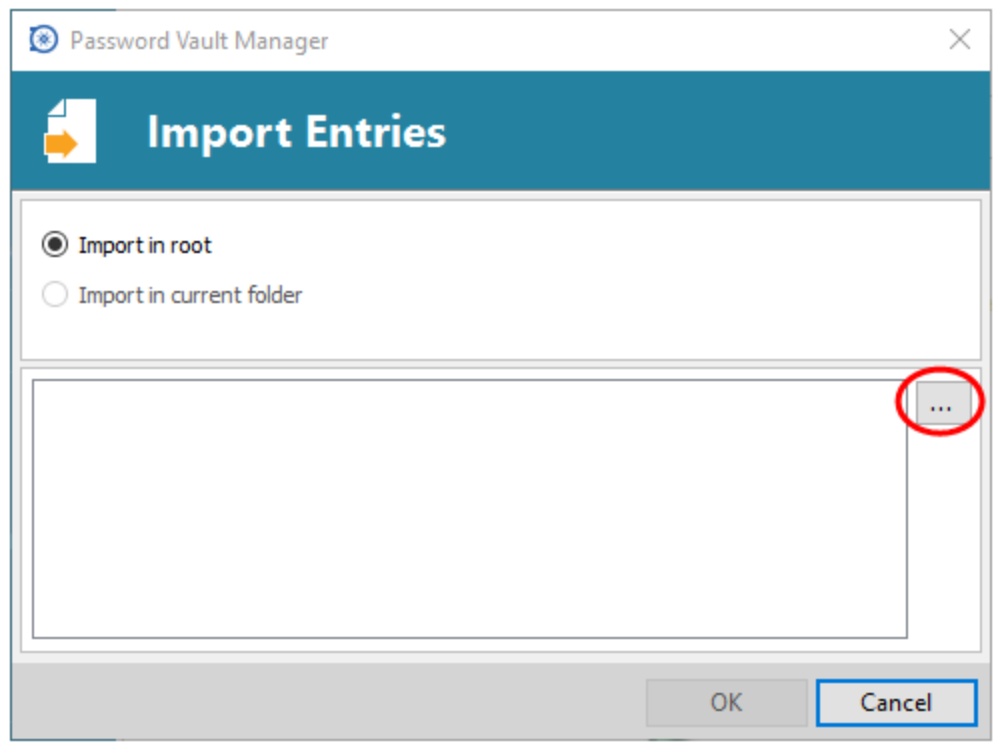
Import

1. Select the destination data source in the data source selection drop down.
2. Select **File - Import - Import Data Entries (.pvm, .xml)**.



Import Data Entries (.pvm, .xml)

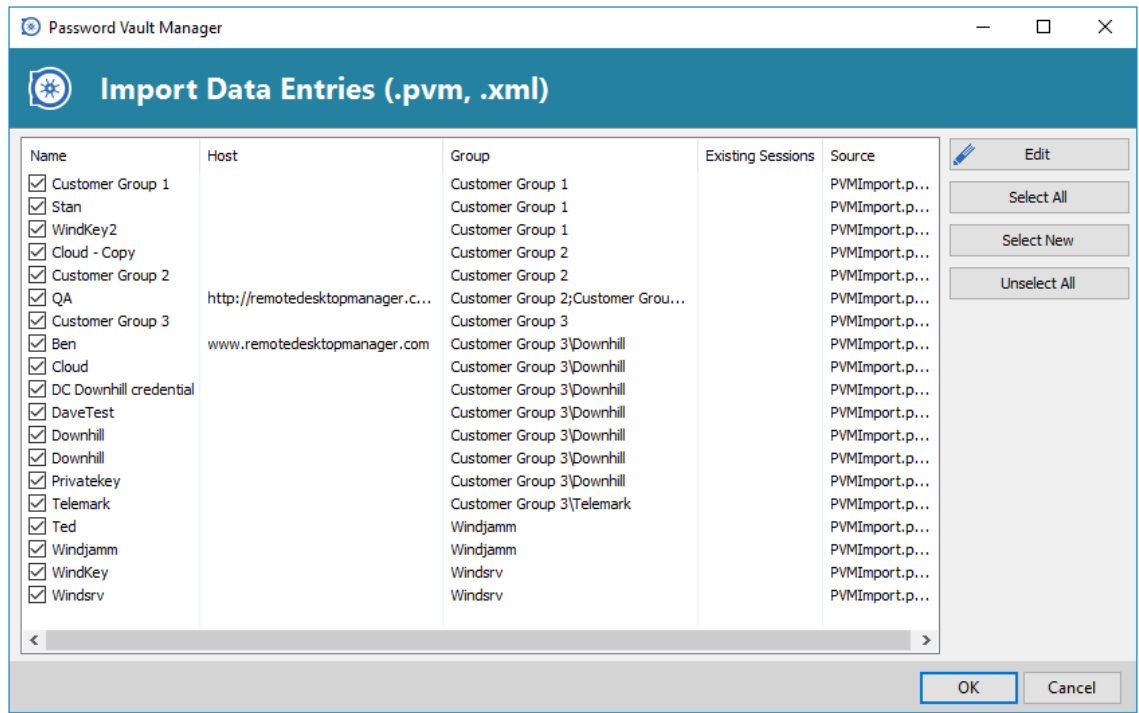
3. In the Import Entries dialog use the ellipsis button to browse for the data file exported in the previous section.



Import Entries

Option	Description
Import in root	Import your entries in the root of your data source, meaning it will keep the exact same structure (group, folder, credentials) as the one you've exported. It is the suggested method of import.
Import in current folder	Import all your entries under the selected folder of the data source.

4. In the next dialog you'll be presented with a list of all entries that are in the data file. You can select which entry you wish to import or you can **Select All** to import all of your entries. Simply press **OK** to complete the process



Import Data Entries