The KWallet Handbook

George Staikos
Lauri Watts
Developer: George Staikos

Contents

Abstract

The wallet subsystem provides a convenient and secure way to manage all your passwords.

Chapter 1

Introduction

Computer users have a very large amount of data to manage, some of which is sensitive. In particular, you will typically have many passwords to manage. Remembering them is difficult and writing them down on paper or in a text file is insecure.

KWallet provides a secure way to store passwords and other secret information, allowing the user to remember only a single password instead of numerous different passwords and credentials.

1.1 Create a Wallet

Wallet is a password storage. It is usually sufficient to have just one wallet secured by one master password but you can organize your large collection of passwords by wallets using KWallet Manager.

By default a wallet named **kdewallet** will be used to store your passwords. This wallet is secured by your login password and will automatically be opened at login, if kwallet_pam is installed and properly configured. On certain distros (e.g. Archlinux) kwallet_pam is not installed by default

Other wallets have to be opened manually.

There are two ways to create a new wallet:

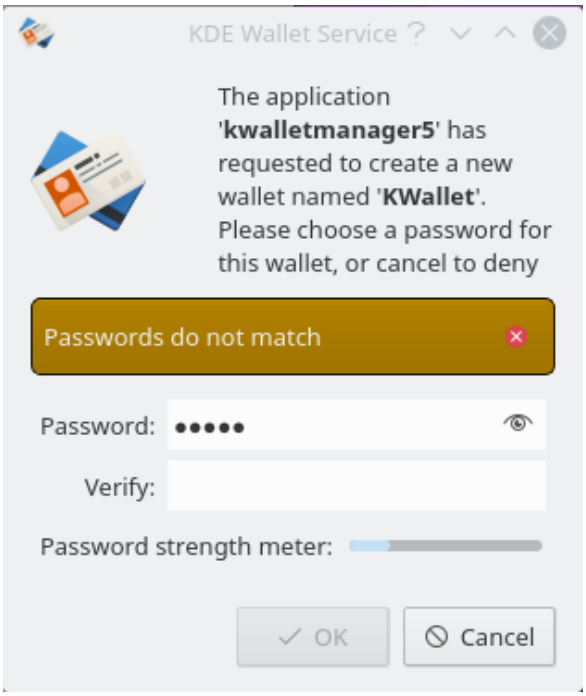
- Use the menu item **File** → **New Wallet** in the KWallet Manager
- Use the **New** button in the System Settings module **KDE Wallet**

If you have not created a wallet yet, see section Using KWallet.

KWallet offers two different ways to store your data:

Blowfish encryption

KWallet saves this sensitive data for you in a strongly encrypted file, accessible by all applications, and protected with a master password that you define.



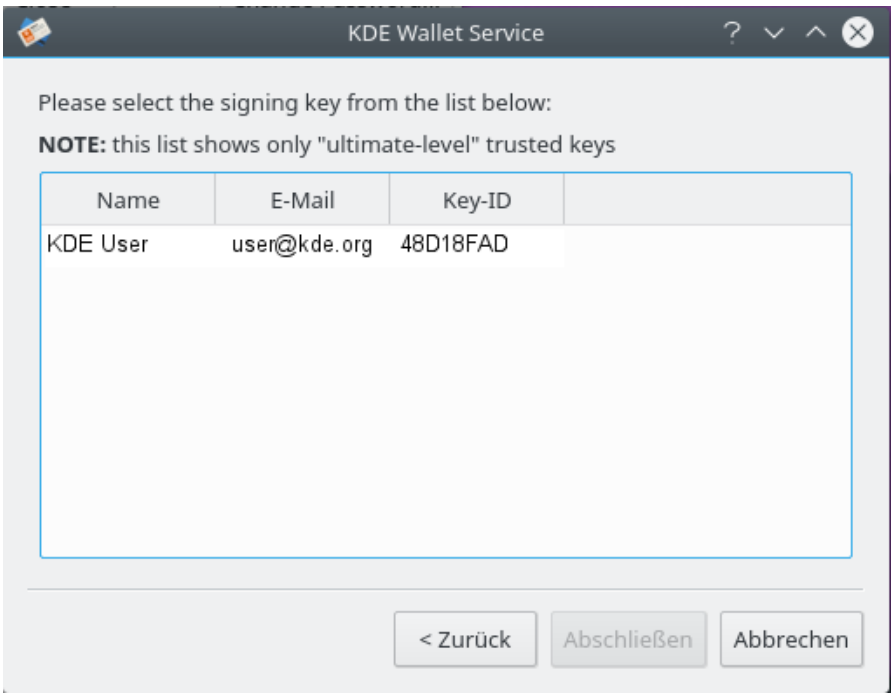
The data is encrypted with the Blowfish symmetric block cipher algorithm, the algorithm key is derived from the SHA-1 hash of the password, with a key length of 156 bits (20 bytes). The data into the wallet file is also hashed with SHA-1 and checked before the data is deciphered and accessible by the applications.

GPG encryption

GnuPG offers some very strong encryption algorithms and uses passphrase protected long keys.

The screenshots above show the case where an encryption capable GPG key was not found on the system. Please use applications like KGpg or Kleopatra to create a key and try again.

If a GPG key was found you will get the next dialog where you can select a key to use for your new wallet.



KWallet will now use GPG when storing wallets and when opening them. The passphrase dialog only shows once. Even if the wallet is closed after initial open, subsequent opening will occur silently during the same session.

The same session can handle simultaneously both file formats. KWallet will transparently detect the file format and load the correct backend to handle it.

To use your sensitive data from your classic wallet with the new backend follow these steps:

- Create a new GPG based wallet
- Launch KWallet Manager using KRunner (**Alt-F2**) or other application launcher (menu) and select your old wallet. Then choose **File** → **Export as encrypted** to create an archive file with your sensitive data.
- Select the new GPG based wallet then choose **File** → **Import encrypted** and select the file you just saved.

- Go to System Settings **Account Details** → **KDE Wallet** and select the newly created GPG based wallet from the **Select wallet to use as default** combobox.

Alternatively use **Import a wallet** but in that case you have to select the `.kwl` file corresponding to your old wallet, located in the folder `kwalletd` in **`qtpaths --paths GenericDataLocation`**.

> **TIP**
> KWallet supports multiple wallets, so for the most secure operation, you should use one wallet for local passwords, and another for network passwords and form data. You can configure this behavior in the KWallet System Settings module, however the default setting is to store everything in one wallet named **kdewallet**.

A wallet is by default closed, which means that you must supply a password to open it. Once the wallet is opened, the contents can be read by any user process, so this may be a security issue.

1.2 Using KWallet

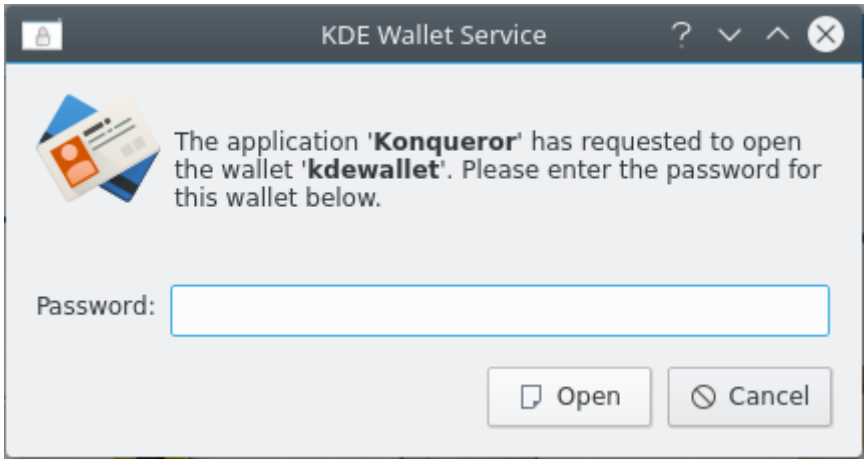
If you visit e.g. the KDE bugtracker and enter the login data for the first time, a dialog pops up offering to store the password in an encrypted wallet:

If you want to store this information, select **Store** to proceed. In case you did not create a wallet so far, the next dialog asks for the encryption backend and creates a wallet named kdewallet.

Next time you visit the same website again, the application retrieves the login data from an open wallet and prefills the forms with these secrets.

Prefilled login information

If the wallet is closed the application requests to open the wallet. Enter the wallet password and click the **Open** button.



This connects the application to the wallet, enables it to read the login data from the wallet and to restore the login information for this website. Once an application is connected to the wallet, it can automatically restore any login information stored in the wallet.

Chapter 2

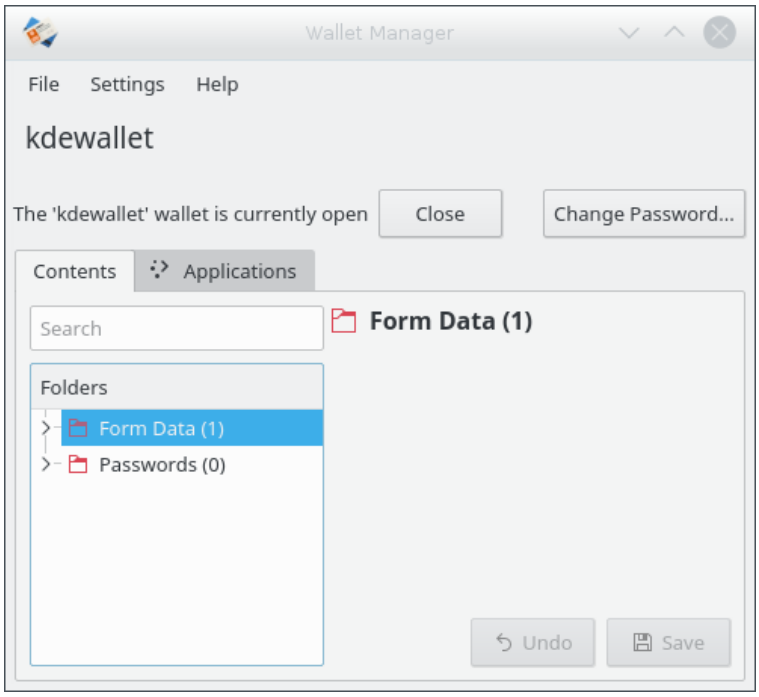
KWallet Manager

KWallet Manager serves a number of functions. Firstly it allows you to see if any wallets are open, which wallets those are, and which applications are using each wallet. You can disconnect an application's access to a wallet from within the KWallet Manager.

You may also manage the wallets installed on the system, creating and deleting wallets and manipulating their contents (changing keys, ...).

The KWallet Manager application is launched with **Applications** → **System** → **Wallet Management Tool** from the application launcher. Alternatively start KRunner with shortcut **Alt**+**F2** and enter **kwalletmanager5**.

Click once on the system tray wallet icon to display the KWallet Manager window.

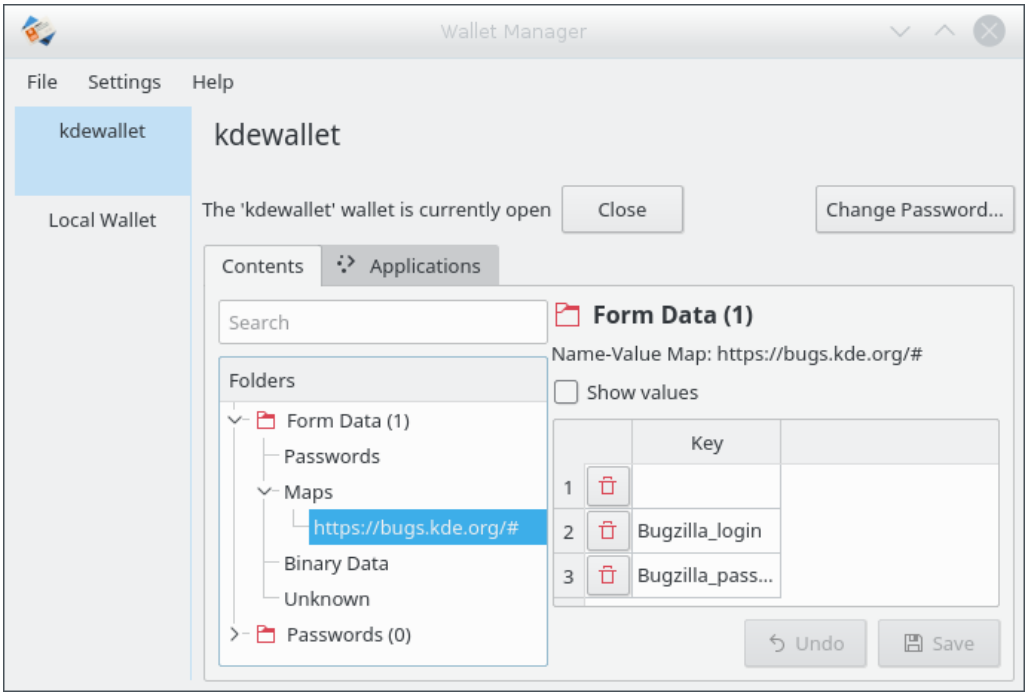


Main window with one wallet

2.1 The Wallet Window

If you have more than one wallet all available wallets are shown on the left.

Clicking on a wallet in the KWallet Manager window will display that wallet's status and the contents of an opened wallet. A wallet may contain any number of folders, which allow storing of password information. By default a wallet will contain folders named Form Data and Passwords.



Main window with two wallets

Use **Open** to display the content of a closed wallet. You will be requested to enter the master password.

2.1.1 Contents tab

The **Contents** tab has three sections:

- A search line to filter the items of the current wallet
- The tree view of the folders contained in the wallet. Click the **>** / **v** icons to expand or collapse the tree view.
- The contents of the selected folder entry at the right side. By default the password and value are hidden. To display and edit them enable **Show values** or click the **Show Contents** button.

Folders may be added or deleted via the context menu, and selecting a folder will update the folder entry list and the summary display. Selecting a folder entry will update the entry contents pane, and allow you to edit that entry.

Entries may also be created, renamed or deleted via the context menu for the folder contents.

All folders and entries may be dragged and dropped into other wallets or folders respectively. This allows a user to easily package up a new wallet for transfer to another environment. For instance, a new wallet could be created and copied onto a removable flash memory device. Important passwords could be transferred there, so you have them available in other locations.

2.1.1.1 Import and Export

If you want to transfer your secrets to another device or computer use the actions in the **File** menu. With **Export as encrypted** wallets can be exported into an encrypted archive file. Importing this archive file with **Import encrypted** you have to provide the master password of the wallet.

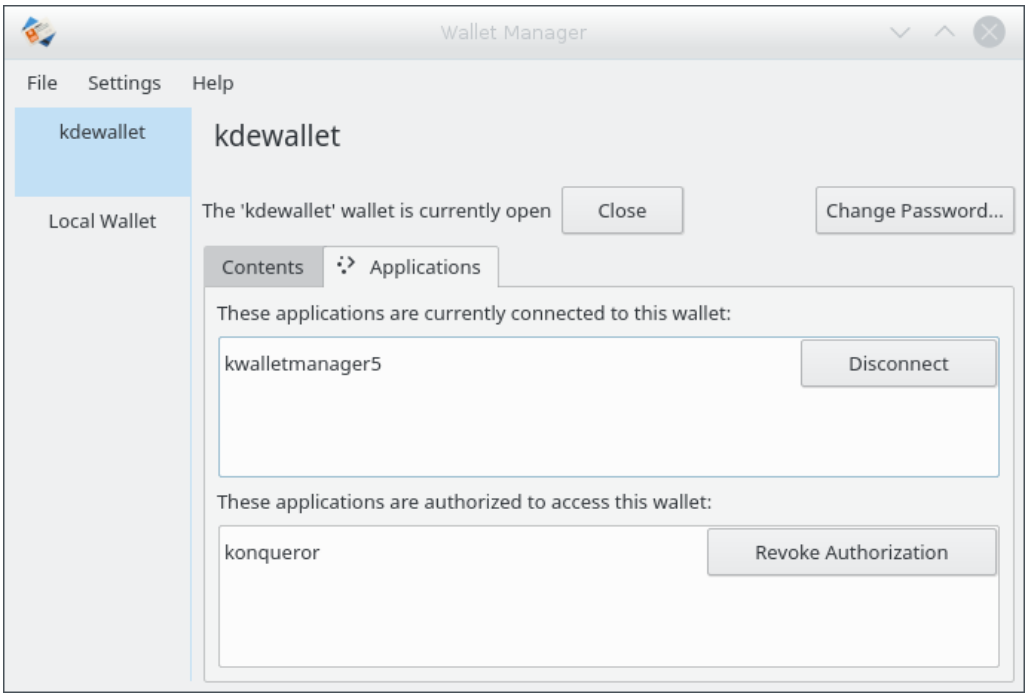
Alternatively a `.xml` file can be used for transferring a wallet. Keep in mind that all secrets are stored as plain text in this file.

2.1.1.2 Adding Entries Manually

Open the context menu with the right mouse button click on **Maps** or **Passwords** in the **Folder** tree view. Select **New** or **New Folder** and choose a name for the new entry.

In the folder contents pane select **New Folder** from the context menu of 'Form Data' or 'Passwords'. For passwords click the **Show Contents** button, enter the new password. For Maps you have to add a **Key** and a **Value**. Click the **Save** button to store the new entries in the encrypted wallet file.

2.1.2 Applications tab



Applications tab

The first list shows all applications currently connected to the selected wallet. Use the button at the right side of each entry to disconnect the application.

In the second list all applications are displayed which are authorized to access the wallet. Use the button right of each entry in the list to revoke the access.

Chapter 3

Configuring KWallet

3.1 Wallet Preferences

KWallet contains a small configuration panel with several options that allow you to tune KWallet to your personal preferences. The default settings for KWallet are sufficient for most users.

Check the box to enable or disable the KDE wallet subsystem entirely. If this box is unchecked, then KWallet is entirely disabled and none of the other options here have any effect, nor will KWallet record any information, or offer to fill in forms for you.

CLOSE WALLET

Close when unused for:
Close the current wallet after a period of inactivity. If you check this option, set the period in the box, default is 10 minutes. When a wallet is closed, the password is needed to access it again.

Close when screensaver starts
Close the wallet as soon as the screen saver starts. When a wallet is closed, the password is needed to access it again.

Close when last application stops using it
Close the wallet as soon as applications that use it have stopped. Note that your wallets will only be closed when all the applications that use it have stopped. When a wallet is closed, the password is needed to access it again.

AUTOMATIC WALLET SELECTION

Select wallet to use as default:
Select which wallet you want to use as default wallet. Please keep in mind that only the wallet named **kdewallet** will be opened automatically at login, if this wallet and your login password are identical.

Different wallet for local passwords:
If checked, choose a different wallet for local passwords.

WALLET MANAGER

Show manager in system tray
Enable the wallet manager to have its icon in the system tray.

Hide System tray icon when last wallet closes

When there is no wallet in use anymore, remove the wallet icon from the system tray.

Finally, there is a button labeled **Launch Wallet Manager**, which does precisely that.

This button is only visible if KWallet Manager is not running

3.2 Access Control

There is only one option on this page:

Prompt when an application accesses a wallet

Signal you when an application gains access to a wallet.

Next there is a tree style view of the access controls for your wallets.

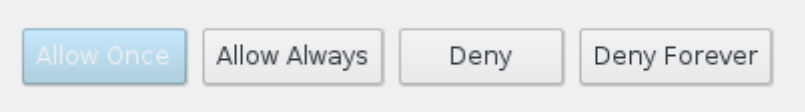
Access Control

Click with the left mouse button on the **>** symbol beside a wallet name to expand the tree. You will see the name of each application that has asked for access to the wallet, and the policy you set for it. You cannot edit policies here, or add them, but it is possible to delete an entry by right mouse button clicking on it and choosing **Delete** from the context menu that appears, or by simply selecting it and pressing the **Del** key.

An application that has been allowed access to a wallet is granted access to all passwords stored inside.

If you erroneously configured an application not to use the KWallet delete the policy for this application here.

On the next start of this application you can define a new policy for access to the wallet.



An application requesting access to a wallet

Chapter 4

Advanced Features

Wallets can be dragged from the KWallet Manager window. This allows you to drag the wallet to a file browser window, where you can choose to copy, move, or link the wallet, as desired.

You might use this to save a wallet to portable media, such as a USB keychain, so that you can take your passwords with you to work or on a vacation, and still have easy access to important sites.

Chapter 5

Credits and License