The Windows Vaults | Malwarebytes Labs

By Pieter Arntz

Published: 2016-01-10 · Archived: 2026-04-02 11:37:09 UTC

The Credential Manager in Windows is a relatively unknown feature, even though a lot of people are using it without being aware of its existence. Windows stores credentials in special folders that they call “vaults” to help users login to websites and other computers. The Credential Manager as such is introduced with Windows 7.

Operation

Reviewing and manually adding credentials can be done by clicking the “Credential Manager” entry on the “User Accounts and Family Safety” tab of the Control Panel.

There are a few categories. Which ones you have at your disposal depends on your Windows version, but the most common options are:

- Certificate(-Based) Credentials, for SSL authentication
- Domain Credentials, can be shared between applications
- Windows Credentials, only used by Windows and its services
- Web Credentials, used by Internet Explorer
- Generic Credentials, when Credential Manager does not recognize the type as one of the above
- Plaintext Password Credentials, these are very unsafe to use and should be avoided

Location

By default Windows stores the credentials in this location:

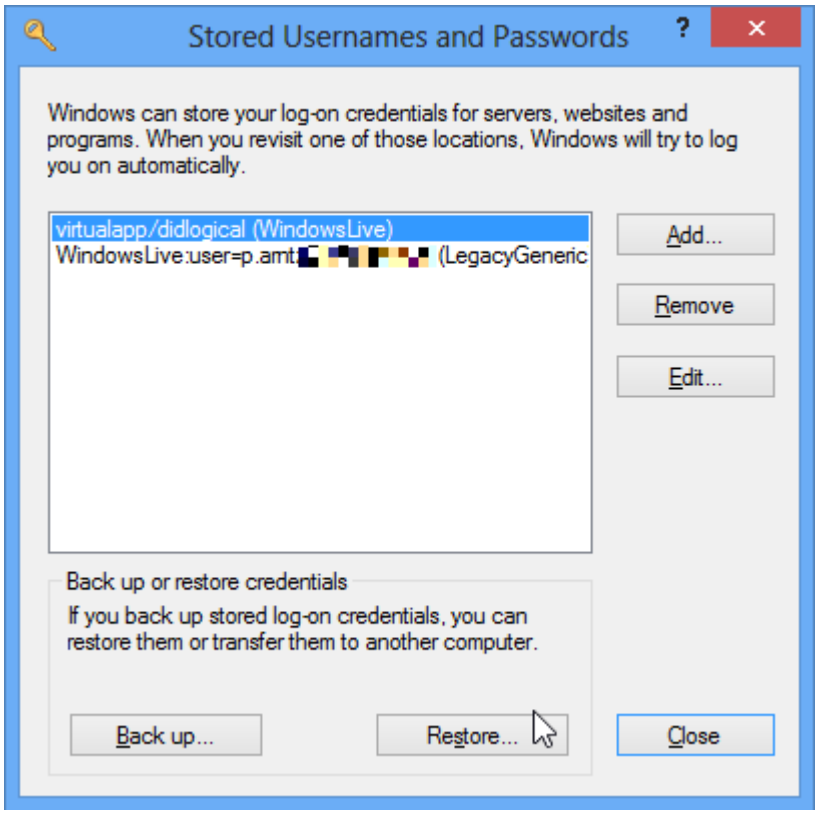
```
%Systemdrive%Users{Username}AppDataLocalMicrosoftCredentials
```

If you are having trouble finding it, you have to set “Show hidden files, folders, and drives” and uncheck “Hide protected operating system files (Recommended)” under the “Folder and Search options” to find the folder and see the content.

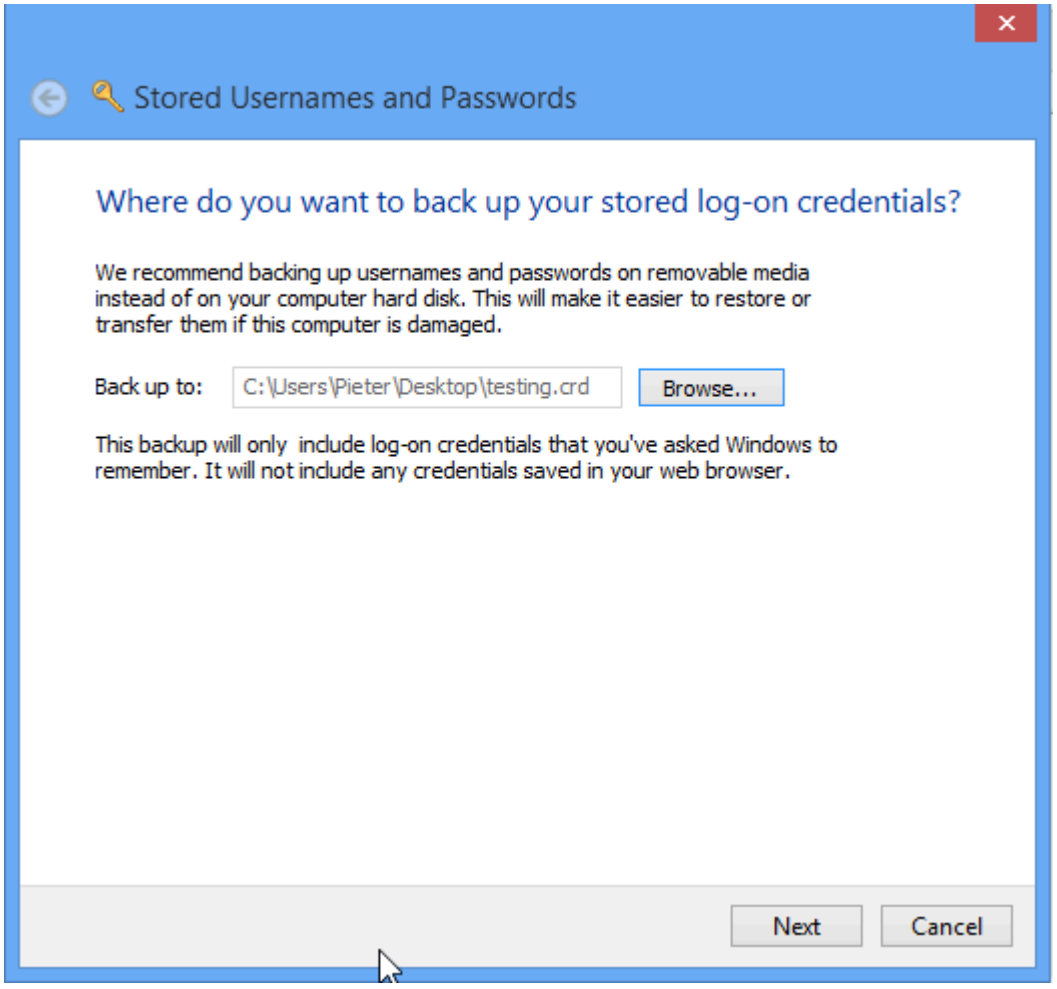
Backup and Restore

For those of us that had no idea how this feature works, it will be a pleasant surprise to learn that you can take your credentials with you when you get a new computer or have to start from scratch with the current one. Here’s how it works:

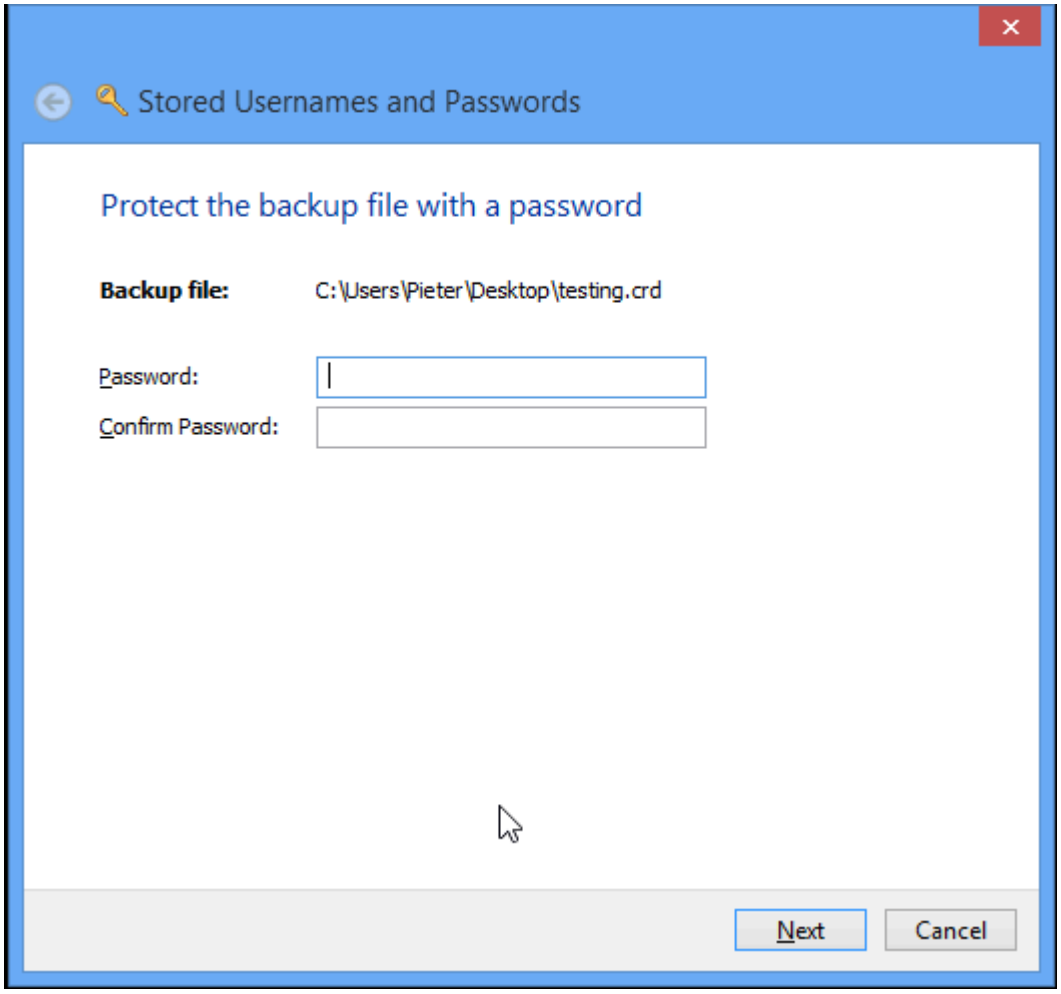
- Click the Credential Manager entry.
- Click the “Back up vault” (for Windows 7) or “Back up Credentials” (for Windows 8 and Windows 10) to open the wizard that will help you with backing up or restoring of your credentials:



- Click the “Back up…” button and use the “Browse” button to choose a name and location for the backup of your credentials:



- Click “Next”, and then you are prompted to switch to the secure desktop by using Ctrl-Alt-Del.
- Once you have done that, you can protect the backup file with a password:



- Click “Next”, remove the “Removable Media” you stored the backup on and click “Finish” to close the wizard.

Restoring the credentials works pretty much the same: Start the wizard, point to the location of the .crd file, switch to secure desktop, enter your password and click “Finish”.

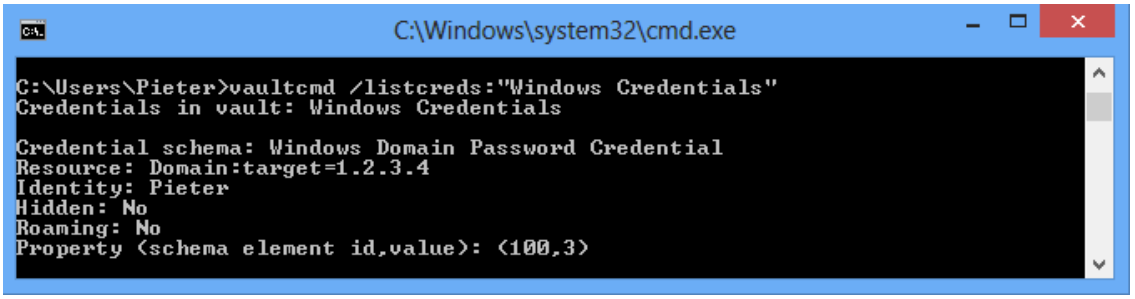
Note that restoring from a .crd file removes any other credentials you may have had in your vault.

Pros and Cons

The ability to store credentials on a computer is a time-saver for the owner or authorized computer users; however, the same can be said for unauthorized users. Based on the simple procedure we have outlined above, stealing your credentials is equally simple. Backing them up to a USB stick or uploading them to the cloud is a piece of cake. Once thieves get hold of the backup, it is not as difficult as you might expect to abuse the credentials. Once they have restored the credentials on another computer or Virtual Machine, they can use “vaultcmd” commands to figure out what they have gained access to.

As an example, I created this hypothetical credential for server 1.2.3.4—

—and used the command **vaultcmd /listcreds:"Windows Credentials"** in a command prompt. This provides an overview of all the credentials stored under "Windows Credentials" as shown below:



And if these thieves feel it is interesting enough, they can use password recovery software to get hold of the password as well, although that is not really necessary, since they will be able to login with your credentials anyway.

If you think the worst thing that could happen if you leave your computer unattended were embarrassing Facebook posts, think again. It would take a professional only seconds to steal your credentials, and after that, they have all the time to figure out what they can do with them.

Online sources:

- What is credential manager?
- Saving Credentials on Windows Computers
- Credential Manager – Where Windows Stores Passwords & Login Details

Pieter Arntz

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
