Keep access data secure with Cryptonify

Master Key

Keep track of your login information for web services with Cryptonify.

By Erik Bärwaldt

Mail providers, social networks, online retailers, auction sites, banks, forums, cloud services and many other services on the Internet want to make life easier for registered users – and usually require authentication with a username and password. The more of these services you use, however, the greater the danger of forgetting or mixing up usernames and passwords. The worst-case scenario is not being able to access your Inbox or data stored on the cloud; unlocking these services costs time and effort. Here the Cryptonify program [1] steps into the breach to keep your access data secure.

As a Java application, Cryptonify requires a corresponding run-time environment, either the one from the GNU project or the Oracle original. You can check whether one of the two versions is already installed on your system using the `java-version` command in a terminal. If entering the command does not bring a version number to light, you should install the OpenJDK version from the repository of your distribution: This way updates are done automatically when needed. Alternatively, you can use the current Oracle run-time environment [2]. This is no longer included in the distributions' repositories because of the license. Thus, you will need to take care of the necessary updates yourself later.

Getting Started

Cryptonify is available for download for Linux [3] as a 12MB ZIP file. After extracting it, you will find a small shell script in the newly created subdirectory. You can use this shell script to start the software. Manually create a corresponding entry to enable the program by mouse click from a menu.

After launching Cryptonify for the first time, you need to make a few basic settings. The software guides you through several pages of dialog, starting with a greeting and ending with enabling the plugins (Figure 1). The most important steps are specifying the path to the file containing the passwords and creating a master password, which the software requests every time from now on.

The dialog for the master password indicates the strength of the selected password in a color-coded bar. This helps avoid weak character strings. If you want to change the master password later, select the *Change master password* item from the *Settings* menu in the program window and then enter the new access data.

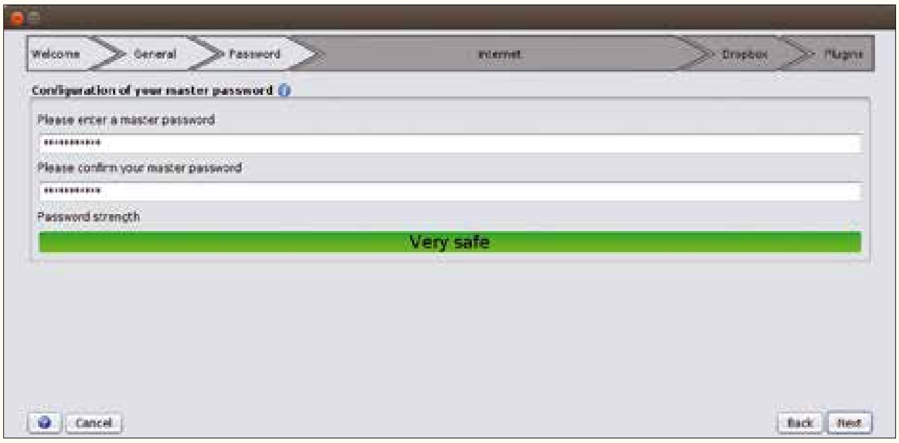
After you have defined the basic settings, the software opens the program window, where you can define categories in a separate area on the left; you can enter the websites belonging to the individual categories with the appropriate data in the larger area on the right.

Configuration

Before creating categories and entries, you should first take a look at the extensive configuration menus where you can

AUTHOR

Erik Bärwaldt is a self-employed IT admin and works for several small and medium-sized companies in Germany.



Configuration of your master password

Please enter a master password: ••••••••••••

Please confirm your master password: ••••••••••••

Password strength: Very safe

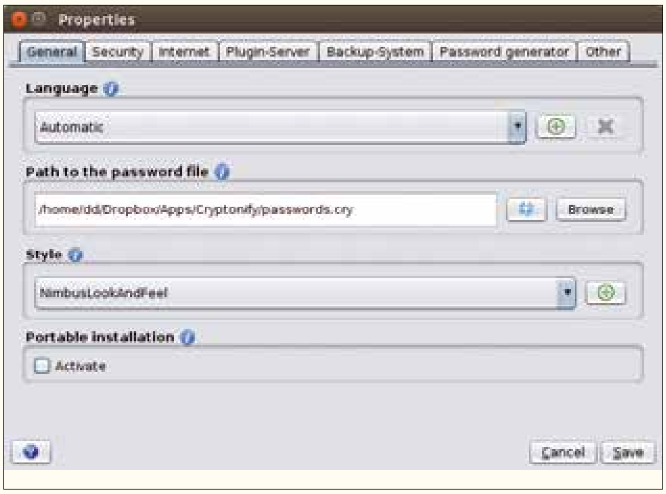
Figure 1: The master password allows you to start Cryptonify and protects the stored data.

customize the software to suit your personal needs. You can access these dialogs via *Settings | Properties* in the main window. Call up the options via seven horizontal tabs in the window that opens (Figure 2). You can set the localization for the interface in the *General* tab, and you can also modify the path to the file with the passwords. Furthermore, you can activate the portable installation, which allows use of the application on removable disks.

In the second tab, *Security*, you can specify the period after which passwords expire and which rules apply for locking the application. Passwords that expire regularly increase security, particularly for online services because, in this way, unauthorized persons cannot permanently acquire data. However, you then also need to change the credentials on the respective websites, which can be rather time-consuming. The mechanism for locking the application makes it possible to lock the interface after a certain period of inactivity and thus deny access to the data by prying eyes. In the *Internet* tab, you can configure automatic updates and activate the downloading of icons used to identify password data.

In the *Plugin-Server* tab, you will find entries to various browser plugins; Cryptonify supports Firefox and Chrome in Linux. The software passes on the data for authentication on set websites to Firefox and Chrome – this enables automatic login. You can enable the corresponding extension by clicking the applicable browser icon in this window. The web browser then opens the traditional integration dialog for add-ons and restarts after the Cryptonify plugin has been successfully installed. There should now be a key icon in a green circle in the browser; this interacts with the Cryptonify plugin server.

A few particularly important settings are found under *Backup-System* (Figure 3): Here you can, for example, define backup intervals for the password file. This file,



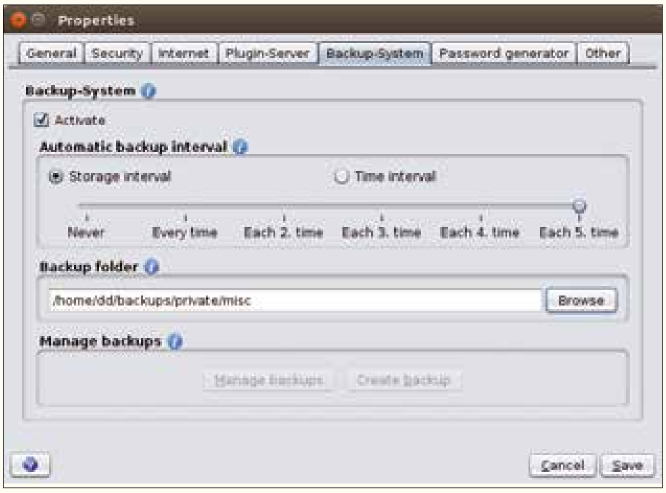
Language: Automatic

Path to the password file: /home/dd/Dropbox/Apps/Cryptonify/passwords.cry

Style: NimbusLookAndFeel

Portable installation: □ Activate

Figure 2: Tailor Cryptonify to your needs before you begin collecting access data.



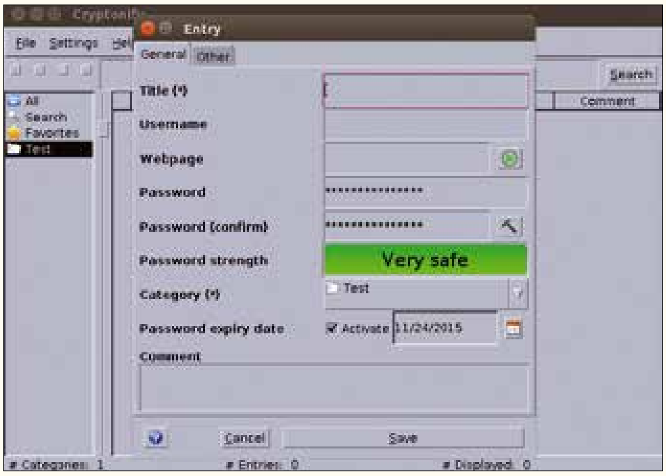
Backup-System: ☑ Activate

Automatic backup interval: ● Storage interval ○ Time interval

Backup folder: /home/dd/backups/private/misc

Manage backups

Figure 3: You should instruct Cryptonify to back up its password file automatically and regularly.



Password: ***************

Password (confirm): ***************

Password strength: Very safe

Category (*): Test

Password expiry date: ☑ Activate 11/24/2015

Figure 4: Cryptonify can also change its appearance.

with the extension `.cry`, includes all the access data you have defined in encrypted form. The 256-bit strong AES encryption is used here, whereby Cryptonify generates the key using the master password with a PBE algorithm. If the password file is lost and there is no backup, you will have to enter all the authentication data into the program again manually. You should definitely enable the automatic backing up option in the *Backup-System* settings dialog, where you can select convenient setting options, to avoid this tedious and time-consuming procedure.

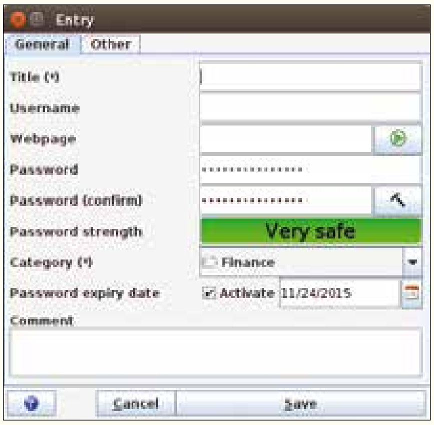
The program allows settings for automatically creating passwords in the *Password generator* tab. The last tab, *Other*, allows you to customize various options for the appearance. This way you can, for example, color the individual lines in the list view separately, which significantly increases clarity, particularly with vast numbers of categories. To this end, click the *Colors* tab on the left side of the window and select the desired color for the odd or even rows. Finally, click *Save* to save your modifications.

Styling

In Linux, Java applications do not exactly stand out with an impressive appearance. However, with Cryptonify, you do not need to come to terms with a rustic look: You are allowed to change the program's theme in the Style field in the *General* tab. A selection window lists four interfaces integrated into the software. Additional themes can be downloaded from the Internet and integrated into Cryptonify. To this end, search for the term "java look and feel" in an Internet search engine.

The *Look And Feel* term denotes ready-made graphical components that define the appearance of an application. These themes are usually available as a Java archive (JAR file). Download the eligible JAR files into a directory of your choice and then click the green plus icon in the Cryptonify settings window on the right in the selection box for the styles.

Then, navigate to the subdirectory containing the JAR file in the file manager that opens and select the file. The new theme is now integrated in Cryptonify, and you can enable it in the selection box. Next, click *Save* and restart the software when prompted. Cryptonify now sports the new appearance (Figure 4).



Password: ***************

Password (confirm): ***************

Password strength: Very safe

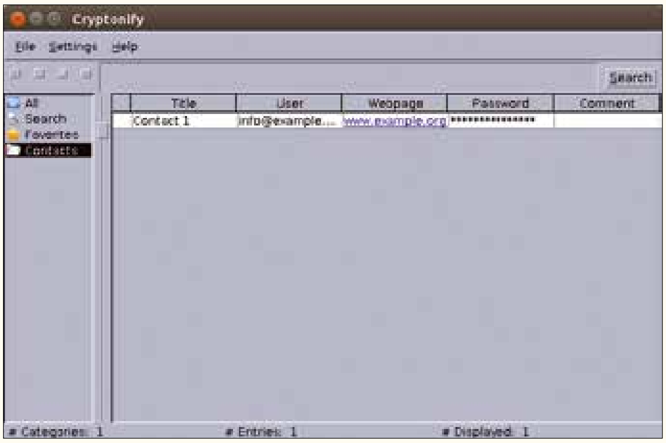
Category (*): Finance

Password expiry date: ☑ Activate 11/24/2015

Figure 5: Enter your access data for individual website in a clearly arranged dialog.

Data Entry

Once you have made all the adjustments, the next step is to enter the access data. First, you should create categories in Cryptonify in which



Title	User	Webpage	Password	Comment
Contact 1	info@example....	www.example.org	***************	

Figure 6: Categories and access data can be easily gathered in the main window.

you can summarize similar services. To this end, click the leftmost switch *New category* at the top of the program window. In a new window, Cryptonify now prompts you to specify a name for the category.

The new category will appear on the left sidebar of the main window after you click *Save*. Select the new category by simply clicking it, and open the window for data entry by clicking *New entry* at the top left of the main window. Now enter the corresponding data for the website (Figure 5); the password is not displayed in plain text. A bar displayed directly below the fields for entering the password indicates how secure the password is. If passwords are insecure, it is advisable to create a stronger one at the earliest opportunity.

You can also add more information or attach a file containing important additional data (e.g., about the relevant page) in the *Other* tab of the input dialog. Cryptonify encrypts this file when the entry is saved. Once you have done this, save the new entry by clicking *Save*. The software then displays the data in the right list view (Figure 6).

Because the collected passwords are not displayed in plain text, when you need to see one, right-click the corresponding entry on the right side of the main window in the list view. A context menu now opens from which you can select the *Show password* option. Cryptonify then issues the corresponding password in a separate window in very large letters.

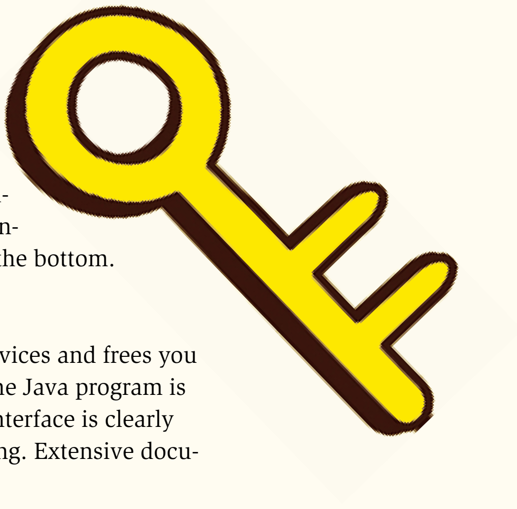
Fully Automatic

The plugin server integrated in Cryptonify enables automatic login on indexed websites in conjunction with a corresponding browser extension. To do this, download and install the extension for the browser used via the Cryptonify settings menu; you also need to enable the plugin server. You can do both of these things in the *Settings* | *Properties* | *Plugin-Server* tab.

When gathering authentication data, you need to enter the exact URL containing the login dialog in the *Website* input field. As soon as you access one of the indexed login pages with Cryptonify launched in the browser, the extension will display that it can automatically transmit the credentials to the website. The Cryptonify icon is only on the login screen in the entry field for the user name. As soon as you click it, the extension automatically fills out the dialog; the browser loads the protected website.

If you have several access-protected accounts with the same provider and have acquired them all with the same login page in Cryptonify, you can obtain the desired access data by clicking the Cryptonify icon in the browser. A list of the individual accounts then appears, from which you can select the desired authentication. Cryptonify automatically fills the corresponding fields in the website and you only need to click the login button on the page to use the service.

When entering authentication data, Cryptonify allows optional comments (e.g., to indicate specific service characteristics for the registration). The browser extension shows a small information icon when you click the icon to the right behind the access data, so you can view the comments later, too. It indicates that a comment has been left for this provider in Cryptonify. To read the comment, click the corresponding entry twice in the main program window. The entry window then opens and displays the comment at the bottom.



Conclusions

Cryptonify puts an end to lost or forgotten access data for web services and frees you of exuberant trails of paperwork for usernames and passwords. The Java program is very well conceived and works quickly and stably. The program interface is clearly arranged and can also be operated without time-consuming training. Extensive documentation for almost every menu item eliminates ambiguities to a great extent. Thus, you no longer have any excuse to use web services with insecure access data or even using the same access data everywhere. ■■■

INFO

[1] Cryptonify: *http://www.marcel-carle.de/software/cryptonify/* (in German)

[2] Oracle Java: *http://java.com/en/*

[3] Cryptonify download: *ftp://ftp.linux-magazine.com/pub/listings/magazine/181*