TruPax: Easy file encryption

Nate Drake introduces the versatile Java utility that can encrypt your files in just three simple steps in a large container file.

Our expert

Nate Drake is a freelance technology journalist who specialises in cybersecurity and retro tech.

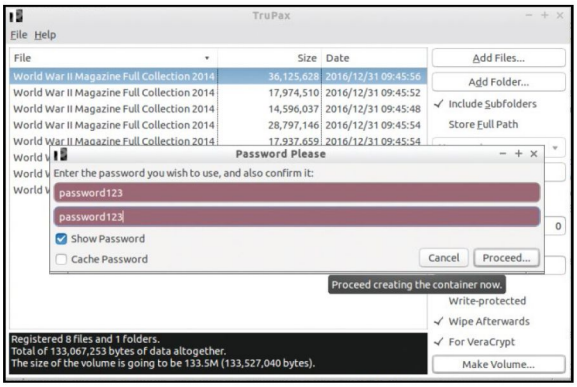
For non-crypto nerds, *VeraCrypt* is a program that enables you to create encrypted containers of any size, inside which you can place your personal photos, bank details or any other data for which the world isn't ready. *VeraCrypt* mounts these containers with a password, which means only you can access your files. For the uber-paranoid there are even options to combine multiple encryption ciphers and use key files in addition to a password.

VeraCrypt does require you to have some idea in advance of the size of all the files you need. Once an encrypted container has been created, it's not possible to resize it. What's more, if you create a container in the full belief that there's enough room for all your files and then find you don't have enough space, there's nothing to do but start the volume creation process all over again.

This is a nuisance at the best of times but is particularly frustrating if you choose to store your encrypted container with a cloud service such as Dropbox, as the upload process has to be restarted.

Trupax posits a solution to creating redundant, huge blocks of data on your machine. This Java app can be used to select files or folders before creating a volume and will create one of exactly the right size. There is even an option to add some more free space if you think you'll need it.

In this tutorial, we will explore how to use *TruPax* to create an encrypted container of exactly the right size, then open it in *VeraCrypt*. In order to proceed, you'll need Java installed on your machine (either the vanilla variety from Oracle of OpenJDK – see below). Once the volume is created, you'll also need *VeraCrypt* pre-installed on your system to mount it.



If the world isn't ready to know you're a military history buff, create a secure container for your magazine collection. Check 'show password' to display as you type.

Quick tip

Before clicking 'Add Folder', be sure to check the box marked 'Include Subfolders' to copy any directories inside it into a new container too.

VeraCrypt can be downloaded from **http://veracrypt.codeplex.com**. The website itself has some excellent documentation on getting started or you can see our previous tutorial in **LXF218**.

This tutorial was written for Ubuntu Linux but both Java and *VeraCrypt* are compatible with all Linux versions, so you should have no trouble running *TruPax* regardless.

Another great advantage of *TruPax* is that admin privileges are not required simply to create a volume or extract its contents elsewhere on the system. *VeraCrypt* will, however, require your admin password to mount the container so that you can edit your files.

TruPax Plus

As convenient as *TruPax* is for creating volumes of just the right size, this comes at the price of extra security.

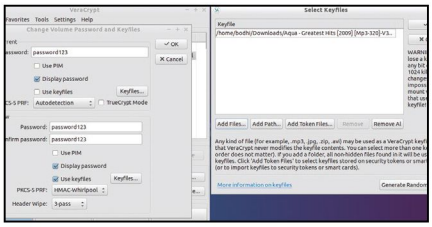
If you wish you can also add a key file. This means in order to mount your *TruPax* volume, *VeraCrypt* would use both your password and a file. This is a form of Two Factor Authentication (something you have and something you know) and hugely reduces the chance that an attacker can access your volume.

VeraCrypt also has a random keyfile generator. Go to Tools > Keyfiles to launch this.

You can use one or a number of files. Remember that the first 64 kilobytes of the file must not change, or the container can't be opened. This is why images and music files work better. *VeraCrypt* doesn't alter the file, so if for instance you choose an MP3 of Aqua's Doctor Jones as your key file, there's no way from examining the file itself to know that it's been used this way.

In *VeraCrypt* choose Volumes > Change Volume password to get started. Enter your password in the field in the Current section, then again in the New section. Check 'Use Keyfiles' then click the 'Keyfiles' button to select the actual files. The order in which you select them doesn't matter at all.

Before clicking 'OK' at the top right, move to the dropdown menu marked 'PKCS-5 PRF' in the New section, and choose 'HMAC-Whirlpool' to use a hash that has been developed entirely independently of our friends in the NSA.



One of the advantages *TruPax* has over *VeraCrypt* is that it's extremely simple to use. Once the program has launched, simply click 'Add Files' or 'Add Folder' to load your data into the main window.

Once the files are added, you'll see a notification at the bottom of the window telling you how large your container will be. If you want space for more files, use the 'Free Space' box on the right-hand side of the window. This is quite intuitive and will recognise values such as '500m' or '2g'.

Optionally you can give your volume a label. Before clicking the 'Make Volume' button at the bottom right, make sure to check 'Wipe Afterwards' if you want to securely delete the original files (see below).

You'll be asked to set a password for the volume, then *TruPax* will begin to generate your container.

Wipe and extract

Unless you specifically ask it not to, by unchecking the box 'Wipe Afterwards', *TruPax* will securely erase the original files after copying them into a secure container. Make sure before you begin that they are backed up to a safe place.

You can use File > Extract in the menu at the top left to make an unencrypted copy of your files, provided you know the password. As such, if you only want to encrypt files for long term storage, such as for backups, you may find that you don't need to use *VeraCrypt* at all.

If, which is more likely, you want to be able to edit these files from time to time and add more to your container, you can still use *TruPax* to create the container initially and then actually mount it using *VeraCrypt*.

TruPax is written in Java and therefore needs a JRE (Java Runtime Environment) installed on your machine. The tutorial lists how to add the repository for this on your machine as well as how to install Java 8, which is the minimum required for *TruPax* to run.

Security conscious people and/or those committed to truly free and open source software may prefer to install OpenJDK which is also developed by the good people of Oracle but contains no closed-source code. If you prefer to do this, ignore Step One of the tutorial and run the commands:

```
sudo add-apt-repository ppa:openjdk-r/ppa
sudo apt-get update
sudo apt-get install openjdk-8-jre
```

If you are one of those people who goes straight to the tutorial before reading the main article (you know who you are), rest assured both Oracle's Java RunTime Environment and OpenJDK can live on the same machine happily together. Run the command `sudo update-alternatives --config java` if you want to change the default Java program to OpenJDK. Select the correct number, press 'Enter', then restart your machine to apply your changes.

Tru lies

TruPax in itself can only create encrypted containers for files and folders, then extract them all at once elsewhere. This isn't very handy for day to day use, which is why we recommend using it in tandem with *VeraCrypt*.

Unlike *VeraCrypt*, *TruPax* cannot create hidden volumes, whereby you can have two passwords for the container – one which you can give to an adversary and leads to harmless data and another which leads to your real files. You can of course use *VeraCrypt* to create a hidden volume and copy your *TruPax* container there if you wish.

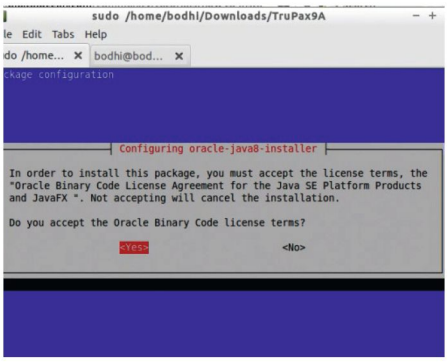
If you follow the steps in 'TruPlax Plus' to increase the security of your container through adding key files, you won't be able to extract the contents using *TruPax*.

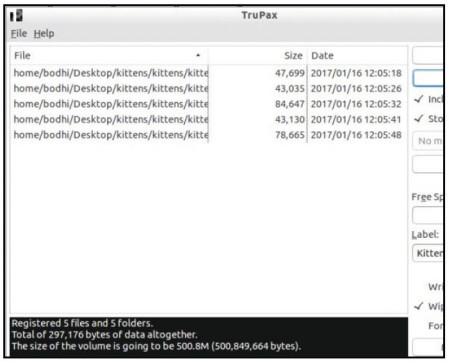
For more details about configuring *TruPax*, make sure to read the **trupax_EN.html** that you downloaded along with the program, or take yourself along to the developer's website at **www.coderslagoon.com**. LXF

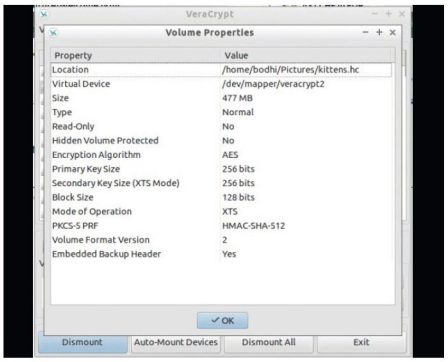
Quick tip

By default, *TruPax* creates containers that are compatible with *VeraCrypt*'s predecessor *TrueCrypt*, which comes with a number of security flaws. So for safety, make sure to check 'For Veracrypt' when creating a volume.

Encrypting with TruPax







1 Download JRE & TruPax

Open Terminal and add the PPA for Java with `sudo add-apt-repository ppa:webupd8team/java`. Next run `sudo apt-get update` then `sudo apt-get install default-jre oracle-java8-installer`. Head to **http://coders lagoon.com** to download *TruPax* for your machine. Right click the file, choose 'Extract', then use `cd` to navigate to its folder, eg, `cd /home/bodhi/Downloads/TruPax9A`.

2 Launch TruPax

Run `java -jar trupax.jar` to launch *TruPax*. Choose your language (German or English are the choices). Click 'Add Files' or 'Add Folder' to select data for encryption. Click 'Make Volume' when you are ready to set a password. *TruPax* will ask you where to save the file and to set a name, such as **kittens.hc**. You can use any name that takes your fancy as an extension.

3 Mount in VeraCrypt

Launch *VeraCrypt*, then click 'Select File'. Navigate to your *TruPax* volume, then click 'Mount'. Enter the password you chose earlier. Find more information about your new volume by choosing Volumes > Volume Properties. This will show where the container is mounted, eg, **/dev/mapper/veracrypt2**. At this stage, you may wish to increase the security (see 'TruPax Plus').