How to Change Your Gibberfish Encryption Passphrase

The following instructions will allow you to disable your old encryption passphrase and create a new one. We have made these instructions as simple as possible, but they do require some basic technical ability. We hope to make this a fully automated process in the future.

Please follow the steps carefully, and if at any point you encounter trouble, please don't hesitate to stop and contact info@gibberfish.org for assistance. Including a screenshot of where you got stuck in your email will help us to diagnose the issue quickly.

Make sure you back up all of your important files before you begin, in case of data loss.

This guide will make use of a command-line interface called "SSH" into which you will type commands.

If you are using Windows, you can install a program called Cygwin.

- See here: https://cygwin.com/install.html

If you are using OS X (Mac) then you already have the SSH software installed. You can simply open a Terminal window to begin.

- See here: https://www.wikihow.com/Open-a-Terminal-Window-in-Mac

In the following steps, the commands you need to enter are in **bold text**. You may copy and paste them into your terminal window one at a time, if you wish, except on the steps where you are asked to substitute specific info.

Procedure

1. Select a new encryption passphrase of no more than 64 characters in length. We recommend using the Diceware method, which creates extremely secure passphrases.

- See here: https://www.eff.org/dice

2. Create a new SSH keypair. Open Cygwin or the OS X Terminal program and enter the following command:

```
ssh-keygen
```

You may press Enter when prompted to accept the default values, and optionally set a passphrase for your key. This should be different than the encryption passphrase you created in step 1.

3. Log in to the Management Portal and configure Two-factor authentication (2FA) using the link at the top right. You will need to install an app such as FreeOTP or Google Authenticator on your mobile device. This will give you access to the “SSH Keys” tab in the side menu.

4. Go to the “SSH Keys” tab and add your “public key”. You can display your key by typing the following command in the terminal. Copy the output to the form provided.

```
cat .ssh/id_rsa.pub
```

The key should begin with “ssh-rsa” and end with what looks like an email address.

5. Deploy your server from the Management Portal using your OLD passphrase.

6. Connect to your server via SSH.

```
ssh root@example.gibber.fish
```

If you set a passphrase on your key is step 3, you will be asked to enter it.

7. From the SSH prompt, type:

```
df -h /srv
```

Make sure the “Use%” column is less than 50%. If it is more than 50% please contact Gibberfish for further instructions.

8. Enter the following commands one at a time to copy your data to a new encrypted filesystem:

```
cd /opt/pancrypticon/pancrypticon
```

```
docker-compose stop
```

```
mount /dev/mapper/pancrypticon-srv /mnt
```

```
mount -t ecryptfs -o key=passphrase,ecryptfs_cipher=aes,ecryptfs_key_bytes=32,ecryptfs_passthrough=n,ecryptfs_enable_filename_crypto=y,no_sig_cache=y /mnt /mnt
```

Enter your NEW passphrase. When prompted about the *File Name Encryption Key (FNEK) Signature* press Enter.

Continue entering the following commands:

```
mkdir /mnt/new
```

```
rsync -av /srv/pancrypticon/* /mnt/new/
```

```
umount /srv
```

```
mv /mnt/new /mnt/pancrypticon
```

```
ls /mnt/pancrypticon
```

You should see a list of filenames such as *letsencrypt*, *nextcloud*, etc. If you do not, please contact Gibberfish.

```
umount /mnt
```

9. List the encrypted devices on your system:

```
blkid -s TYPE | grep LUKS
```

You should see something like the following:

```
/dev/sda2: TYPE=”crypto_LUKS”
```

The part before the colon that starts with “/dev/” is the name of your disk device. Note this for later. If you see more than one line of output from this command, repeat the following instructions for each device.

10. Add your new passphrase to the encrypted devices, substituting your actual device name. Repeat this step if necessary for multiple devices.

```
cryptsetup luksAddKey /dev/sda2
```

Enter your OLD passphrase, then your NEW passphrase, when prompted.

11. Reboot the system:

```
reboot
```

12. In a new Tor Browser window, return to the Management Portal and deploy your server using your NEW passphrase. Once it completes, log in to Nextcloud and make sure all of your files are present. If the deploy fails for some reason, do not continue further. Contact Gibberfish.

13. From a terminal prompt, SSH to your server again:

```
ssh root@example.gibber.fish
```

14. Remove the obsolete encrypted data

```
cd /opt/pancrypticon/pancrypticon

docker-compose stop

umount /srv

find /srv -maxdepth 1 -type d -mtime +1 -exec rm -rf {} \;
```

15. Finally, remove your old encryption passphrase, substituting the name of your device. Repeat this step if necessary for multiple devices.

```
cryptsetup luksRemoveKey /dev/sda2
```

At this point, your OLD passphrase should no longer work. You should use your NEW passphrase from now on. Reboot one more time and deploy your server from the Management Portal. If everything comes back up properly, you’re done!

```
reboot
```

If you don’t plan on using your SSH key again, you may wish to delete it from the “SSH Keys” tab in the Management Portal.