Switch⇄Crypt – A Lightweight File Encryption Tool | V1.1 Manual

Features:

- A lightweight but high secure file encryption tool.
- Keeps your sensitive files always encrypted by default.
- Temporary decryption of files requires to enter your Switch⇄Crypt password which is nowhere stored except in your mind.
- Automatically encrypts all files when you step away from your PC.
- When converting unencrypted files to encrypted files: Overwrites unencrypted files with random data before deleting them [1].
- Easy to install and easy use.
- Runs on your local machine only, doesn't require any internet service.
- Freeware sponsored by DKF, no user activity data are collected, no backdoor and no advertisement.

[1] = Overwriting a file with a random pattern does not protect against forensic investigations on SSD disks.

Dual Purpose: You can use Switch⇄Crypt either as mentioned above to keep your own data encrypted, or - alternatively - you can use Switch⇄Crypt to exchange encrypted data with another person via untrusted email or via an untrusted storage. Consider that you can use Switch⇄Crypt only for one of these two purposes - but not for both of them.

Switch⇄Crypt is based and latest security standards and uses a large cryptographic "Salt". You are fully protected against rainbow table attacks.

Background and Technical Concept

Switch⇄Crypt is a lightweight but high secure file encryption tool that works at directory / file level. It was originally developed to encrypt sensitive files on laptop computers when travelling in "untrusted countries".

Switch⇄Crypt is mostly used to:

- Encrypt OpenVPN client configuration files.
- Encrypt text files which contain usernames and passwords.
- Encrypt Selenium IDE *.side files which contain username and passwords (browser automation files).

You can use Switch⇄Crypt also for any other purpose, like for example encrypting your private photos or encrypting any documents containing sensitive data.

Switch⇄Crypt is easy to use, works out of the box, and does not install any driver. It works as a standard application without needing any special privileges or OS settings.

The encryption is based on a RSA keypair where the public key is used to encrypt the files and the private key is used to decrypt the files. Furthermore, the private key itself is encrypted by an symmetric AES algorithm which uses as key your arbitrary password plus a salt.

Choosing such an approach has the effect that encrypting any file does not require the password.
This means also that encryption can be automated; for example you can automatically encrypt all files when the lid of your laptop is closed or when you lock your screen.

On the other hand, because your password is nowhere stored and remains only in your mind, decrypting a file cannot automated. To decrypt a file, or a couple of files, you have always to enter your password.

There are two programs delivered by the installation kit:

1. **SwitchCryptUI** which is the graphical user interface where you can configure the tool and manually encrypt and decrypt file or folders. From here you can also launch the default application for a (temporary) decrypted file.
2. **SwitchCryptAll** which is a command line utility that encrypts all of your files. You can call this utility from various OS tools like for example from Windows Task Scheduler or from a Linux Cron job.
   SwitchCryptAll will synchronize its actions with SwitchCryptUI in order that you see always the latest state of the files in the graphical user interface.

Initial Setup and Configuration

After installing Switch⇄Crypt you have first to start **SwitchCryptUI** and to choose an arbitrary password. → *This effects that the RSA key pair will generated and a random salt will generated. The private key will be encrypted with your password and the salt.*

The following files are created in your home directory ~/.SwitchCrypt

- public.key
- salt.dat
- encryptedPrivate.key

It's strongly recommended that you backup these 3 files to an USB stick. There is no extra protection required for the USB stick because none of these files contains your password. However, if these files are accidently deleted on your machine there is no way do decrypt any file if you don't have a backup.

Next you have to choose respectively to configure the directories (folders) wherein all files should be encrypted by default. For Example ~/Documents/private. Please start first with some small folders and perform some tests until you are confident to operate the tool (→ see next chapter: Testing the Installation). That's basically all what is needed.

Don't encrypt any directory that is part of the operating system. → *Reboot will fail!*

Don't encrypt the ~/.SwitchCrypt configuration directory. → *Then you are locked out by yourself*

Optimally, but recommended: You may additionally configure various OS tools like for example Windows Task Scheduler to call **SwitchCryptAll** on specific events or times.
This will effect that all files are encrypted by default even when you step away from your PC.

Recommended calls of **SwitchCryptAll** on **Windows** systems:

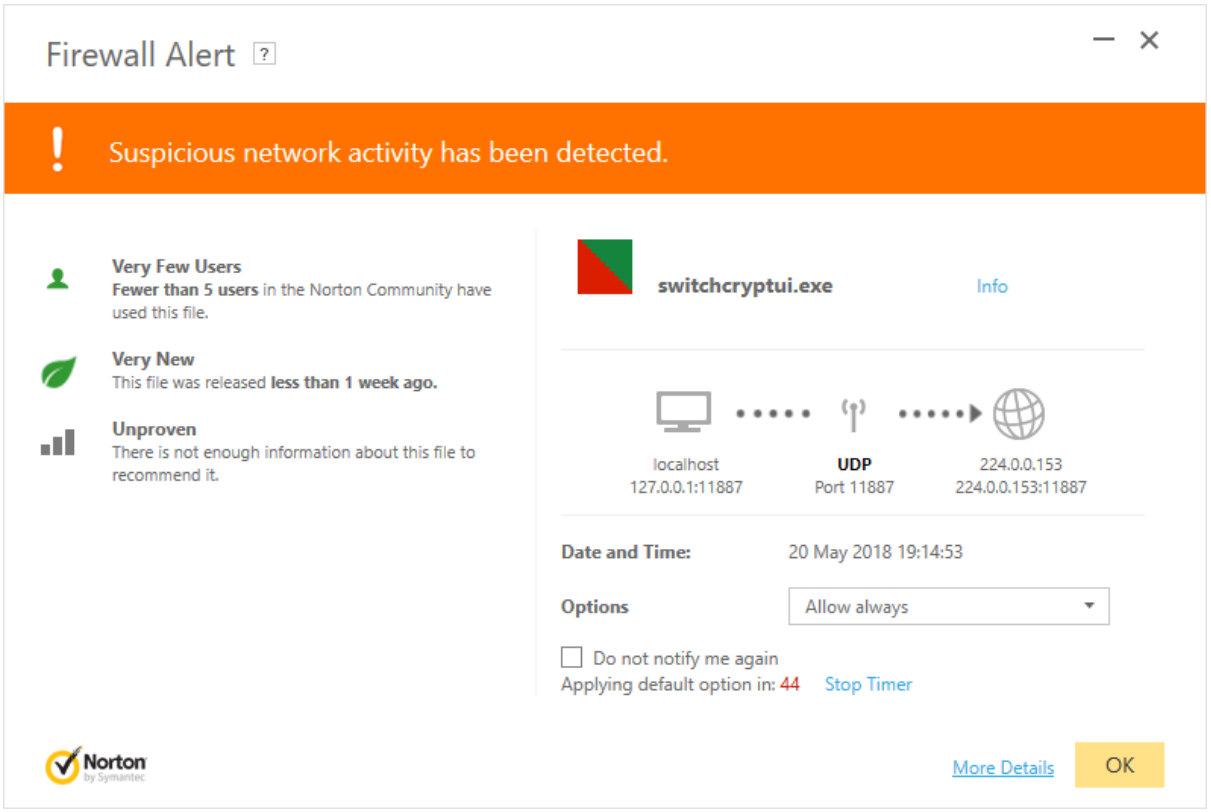
- On Workstation Lock of Any User
- On Workstation Unlock of Any User
- On Remote Connection to Any User Session
- On Remote Disconnect from Any User Session
- At Log On of Any User
- At System Startup

Note that **SwitchCryptAll** must run under the same user account as **SwitchCryptUI**.

→ **See Appendix A: Windows Example of calling SwitchCryptAll from Task Scheduler**

Special Notes for Windows Systems:

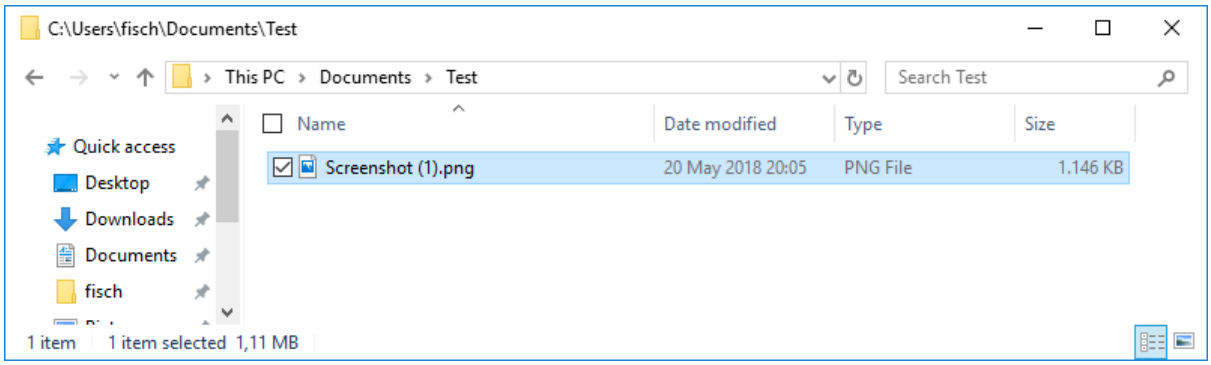
The synchronization between **SwitchCryptAll** and **SwitchCryptUI** is made by **UTP multicast messages** which are send on the local loopback interface only. No data are transmitted over the internet. Depending on your firewall software you may get a security alert on your Windows machine. You have to allow this localhost – localhost UDP communication in order that the synchronization works.



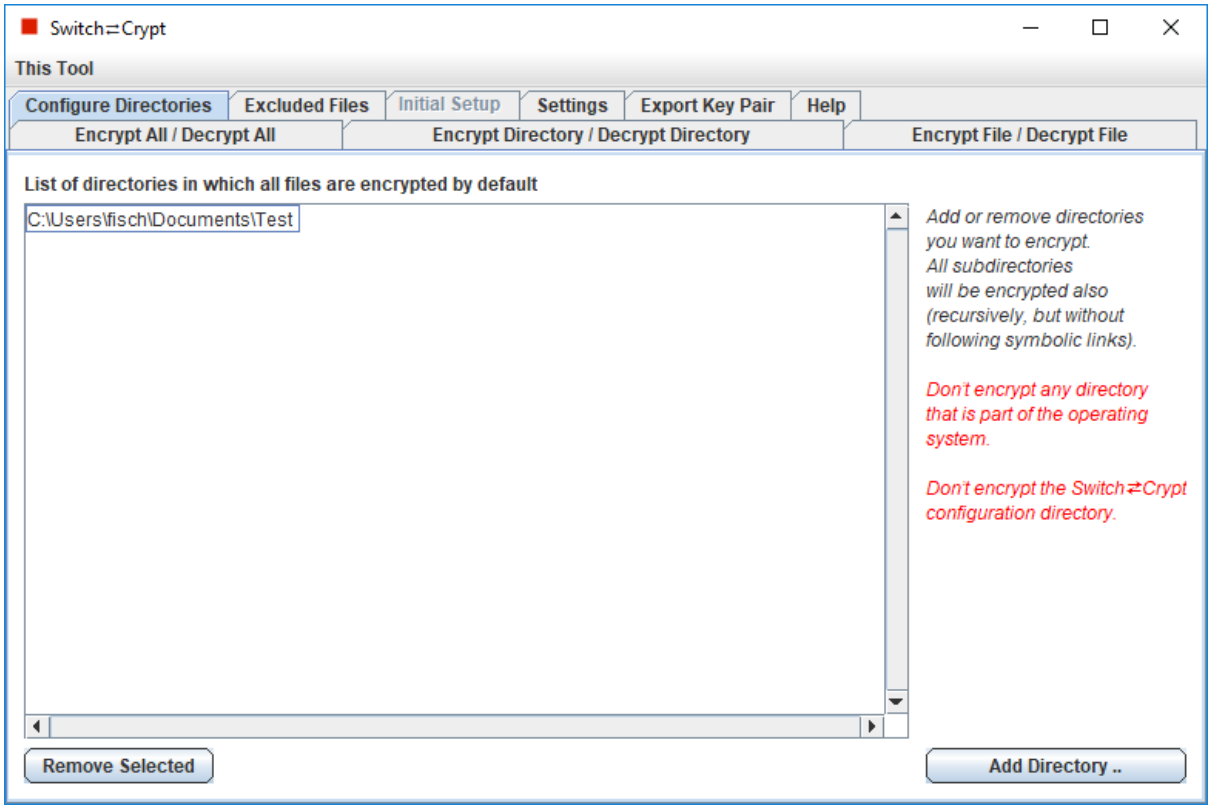
Testing the Installation

Once you have generated your key pair you should test the installation:

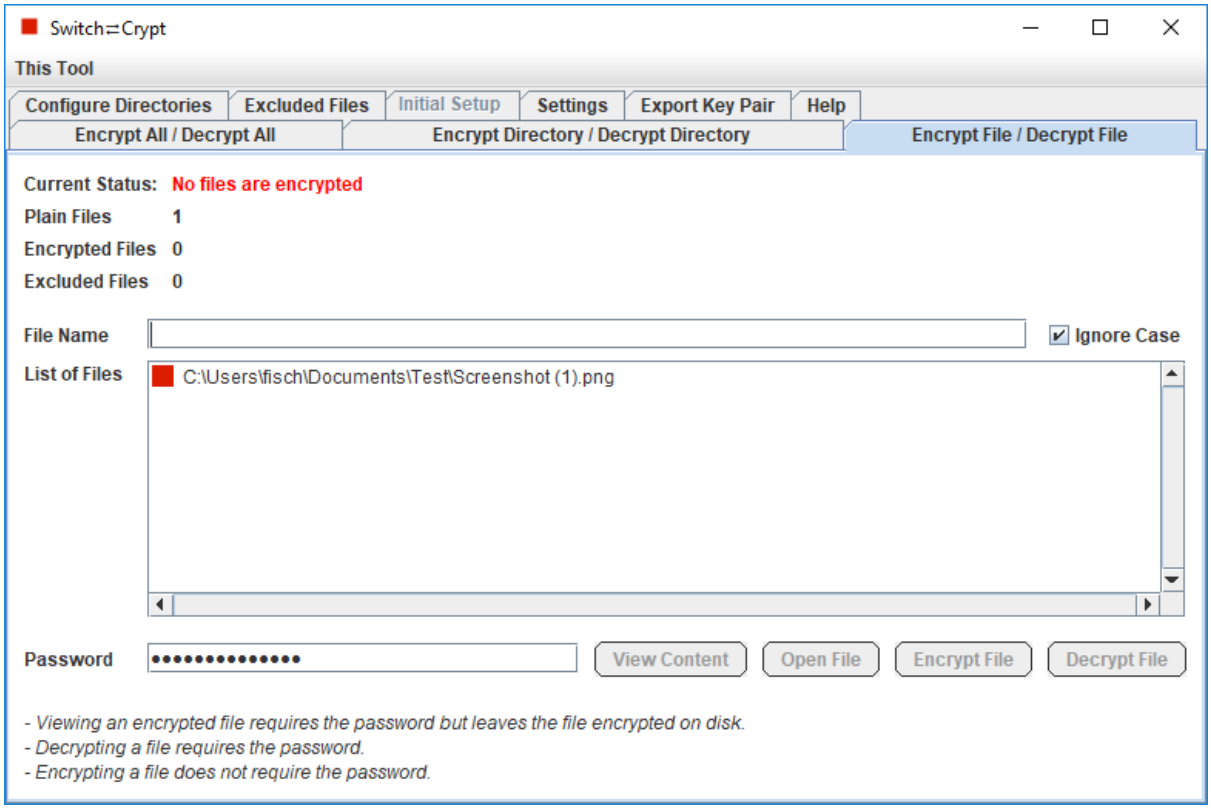
1. Create a directory named Test in your Documents folder and copy any file to this test directory (for example an image):



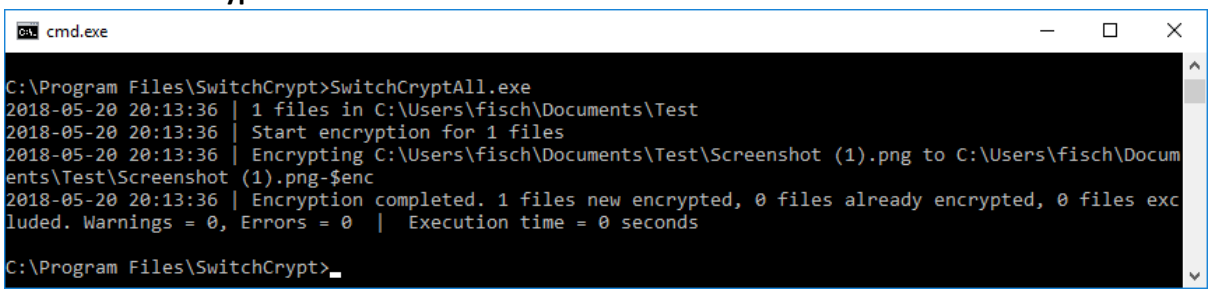
2. Add the Test directory in the **SwitchCryptUI**:



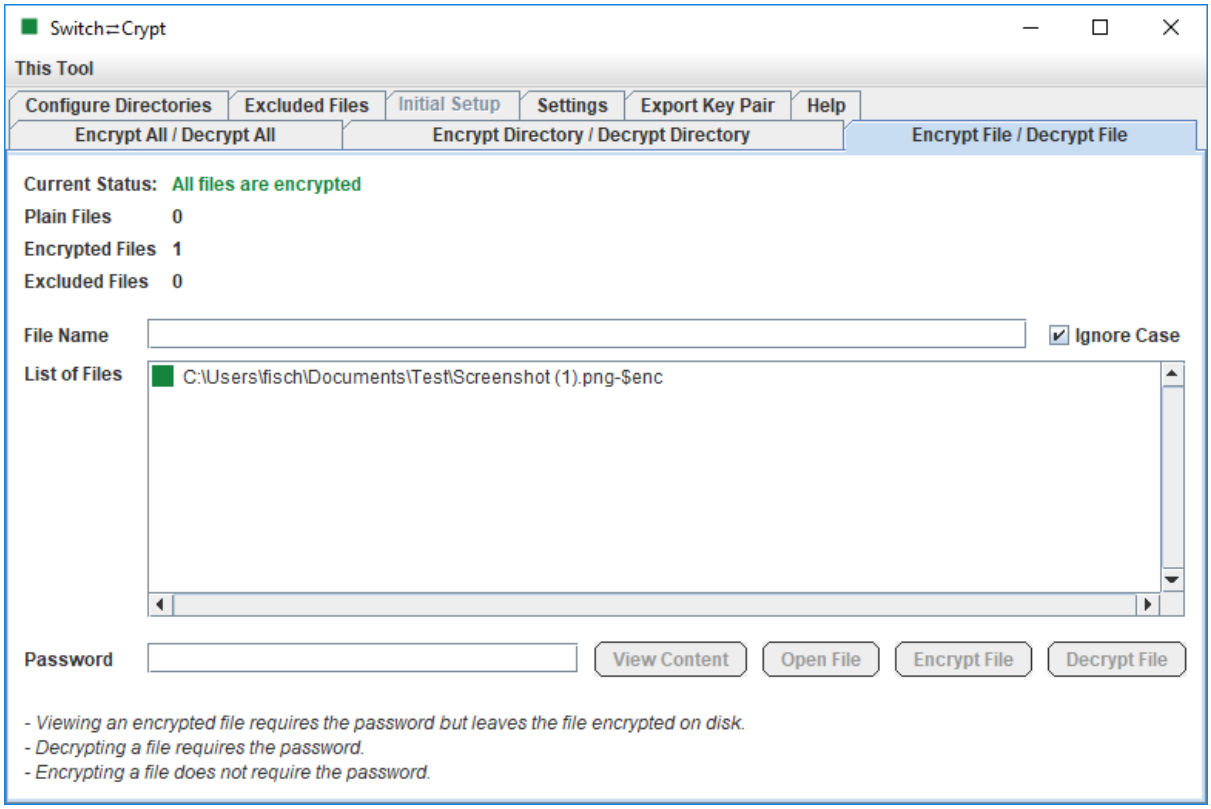
3. Switch to the “Encrypt File / Decrypt File” Tab:



4. Start a terminal and locate to the SwitchCrypt installation directory (C:\Program Files\SwitchCrypt). Then call **SwitchCryptAll**:



5. The file(s) in your test directory should now be encrypted (= test passed):

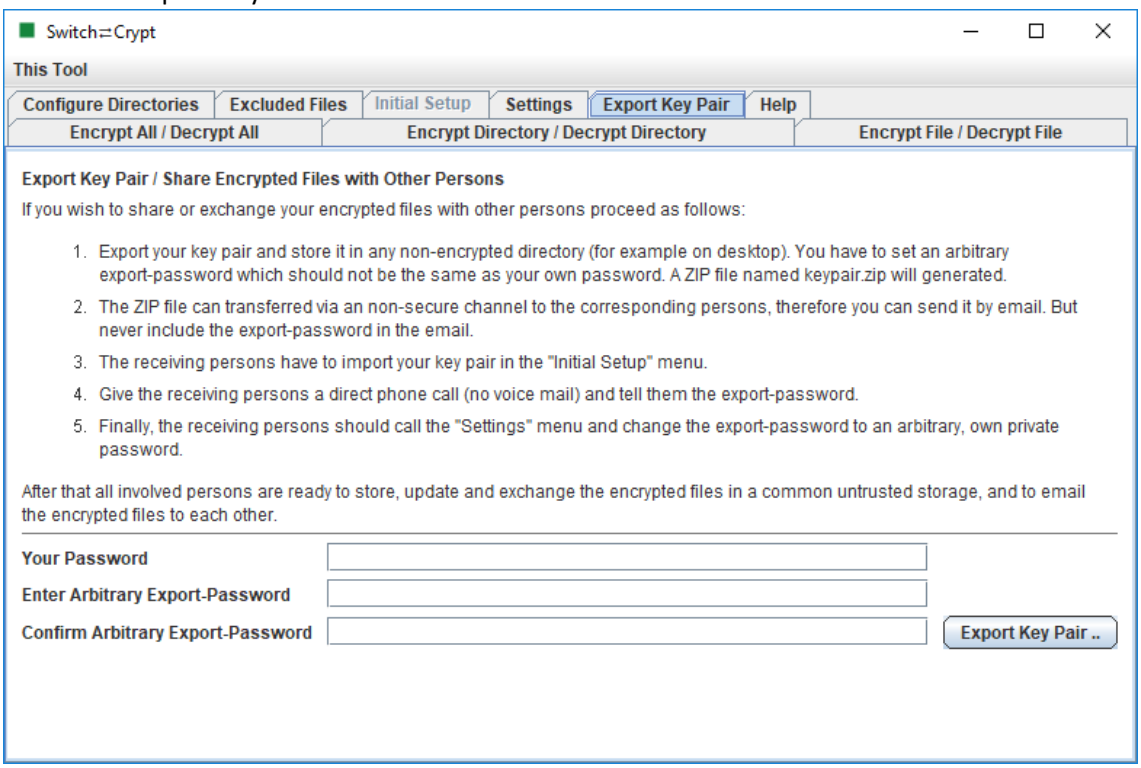


6. Finally remove the Test directory from the **SwitchCryptUI** configuration and delete the Test directory at OS level.

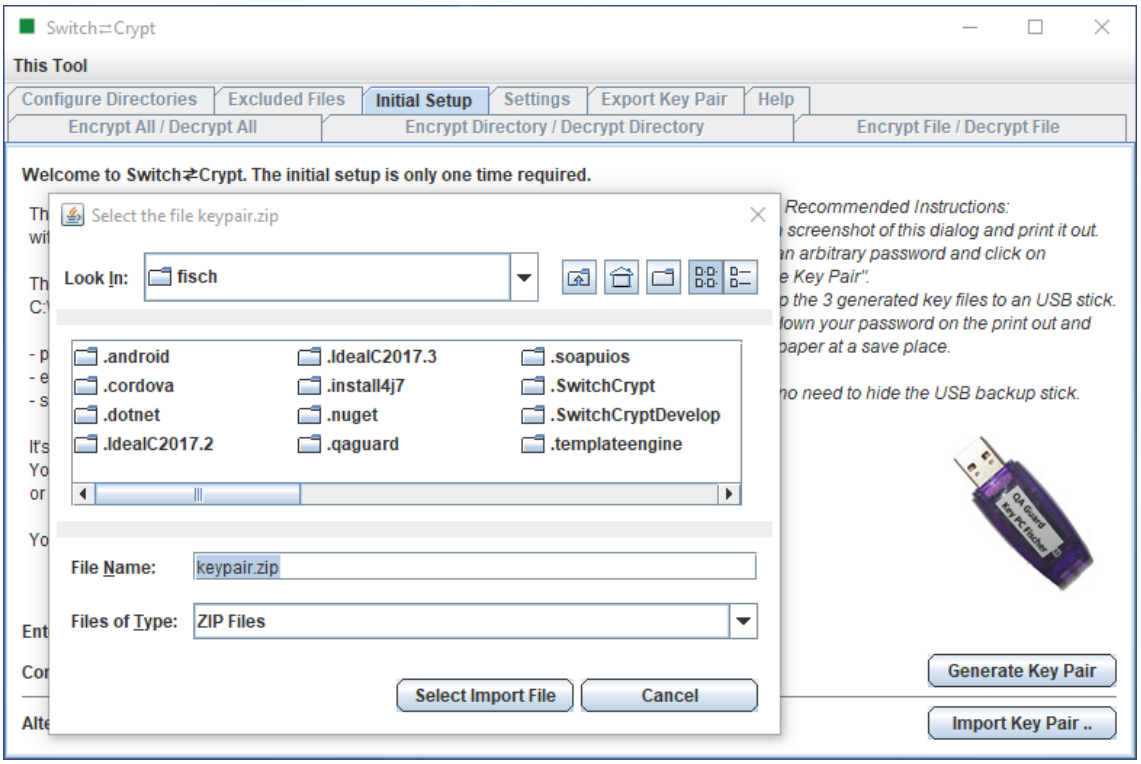
Addition notes for using Switch⇄Crypt to exchange sensitive encrypted data with another person (dual use of the tool, second case)

If you plan to use Switch⇄Crypt to exchange sensitive encrypted data with another person then Switch⇄Crypt should installed and tested first only on one PC as described before. After the first PC is tested, the keypair can be exported and send to the second person. Then the second person should install Switch⇄Crypt and import the key pair during the "Initial Setup" dialog.

First PC → Export Key Pair:



Second PC → Import Key Pair:



In case if you are planning to use an untrusted storage to exchange your encrypted files then the untrusted storage should ***not*** be configured as an encryption/decryption directory in **SwitchCryptUI**. Each person should have its own local encryption/decryption directory.

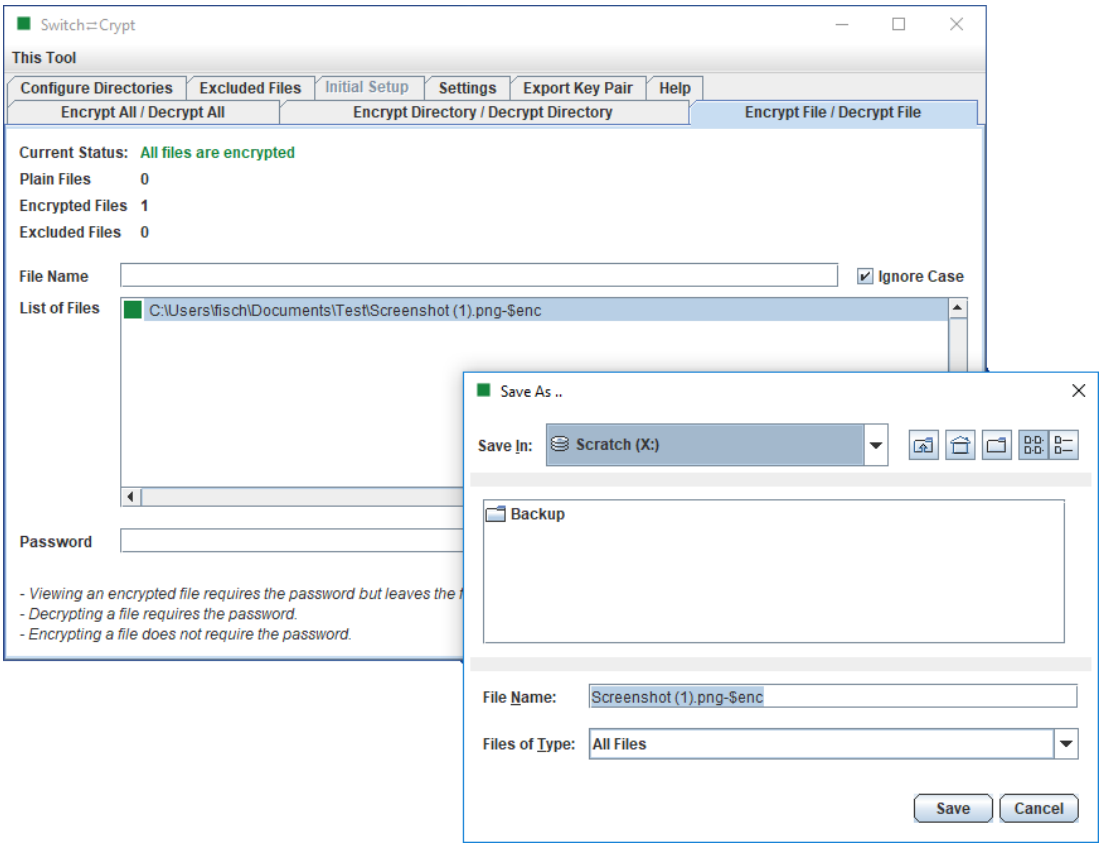
Encrypted files can be exported from the local directory to the untrusted storage by performing a right mouse click to the file name at the “Encrypt File / Decrypt File” tab.

And the encrypted files can imported from the untrusted storage by performing a right mouse click to the local directory at the “Encrypt Directory / Decrypt Directory” tab.

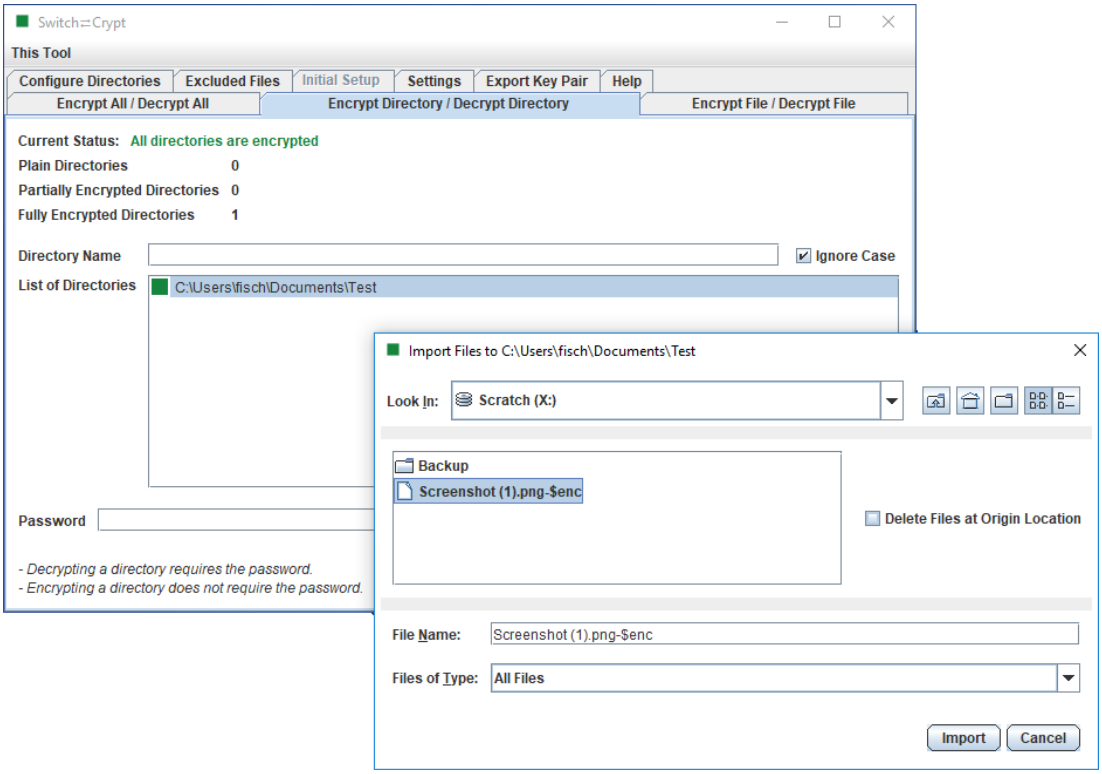
Alternatively, the files can also be moved to or from the untrusted storage by any other tool like by using the file manager of the OS.

Rule of Thumb: Never add a directory of an untrusted storage in the SwitchCryptUI “Configure Directories” tab. Use instead of this the export and import functions to copy the encrypted files. Store only encrypted files on the untrusted storage.

Exporting an encrypted file (Save As ..) from the local directory to the untrusted storage:



Importing an encrypted file from the untrusted storage to the local directory:



FAQs

Q: Can the Switch⇄Crypt password be cracked by a brute force attack?
A: This depends on how long your password is. If your password contains less than 8 characters it can be cracked in seconds. If you choose a password length which is equal or lager than 14 characters then you are at the secure side, as long as such a password is not a common, single word, or a combination of common words. For example “IloveMySweetheart” is not a good password because it contains common words only. Be creative, use several languages, use exotic words, add some spelling errors, and use special chars. For example ”bruchita$$irversiede+-“ is much better.
Rule of thumb: Any common word counts always as two characters only, independently of how long the word is. So, to reach a secure password with common words only you need 14/2 = 7 common words.

Q: Can the Switch⇄Crypt password be cracked by an attack which uses precalculated rainbow tables?
A: No. That’s technically impossible. For each installation Switch⇄Crypt generates a random salt on your machine of 24 bytes (= 192 bits).

Q: I forgot my Switch⇄Crypt password. Is there a way to decrypt the files anyway?
A: No, no way. Suggestion: Step away from your PC, relax and try to remember the password.

Q: Can I accidently (double) encrypt an already encrypted file?
A: No, that’s technically impossible. The tool will take care to prevent this.

Q: If I have renamed an encrypted file and/or did change the file extension of an encrypted file, can I decrypt the file anyway?
A: Yes.

Q: Can I change my Switch⇄Crypt password?
A: Yes, at any time: Settings → Change Password. Note that in such a case a new random salt will generated also, even if you if the new password is the same as the old password.

Q: If I have chosen first a weak Switch⇄Crypt password and changed it later to a strong password, does this make sense, respectively does this increase the security?
A: Yes.

Q: If I install the tool twice on different PCs and choose each time the same password, can I then encrypt a file on one PC, send it to the other PC, and decrypt it on the other PC?
A: The standard answer is "no", because you have normally generated two different key pairs. However, you can export the key pair from the first installed PC and import it on the second installed PC. Then this works.

Q: Does Switch⇄Crypt act in a similar way like a disk encryption tool?
A: No. A disk encryption tools protects your data only at the time when you are not logged in. For example in cases when your laptop is lost or stolen, or when you replace an old disk by a new disk. In opposite to this, Switch⇄Crypt protects your data also at the time when you are logged in. That's because Switch⇄Crypt works on file level, rather than on disk level. However, the technical approach of Switch⇄Crypt has the disadvantage that you cannot encrypt any files needed by the operating system. For example you cannot encrypt /etc/passwd or any files in C:\Windows.

Q: Can Switch⇄Crypt combined with a disk encryption tool?
A: Yes, and we recommend to do that. Rule of thumb: If you combine Switch⇄Crypt with a disk encryption tool, your sensitive data are substantially much more secure than when using a disk encryption tool only.

Q: Does Switch⇄Crypt protect me against trojan horses?
A: This depends on the time when you detect the trojan horse. If you detect the trojan horse before you have manually entered the Switch⇄Crypt password then your files are still protected. Of course, in such a case you have first to make a backup of your sensitive data and then to reinstall the OS. After that restore your key pair, reinstall Switch⇄Crypt and copy the sensitive, encrypted data to the new installed OS.

Q: Does Switch⇄Crypt protect me against ransomware?
A: No. You have to backup your (encrypted) files and keep the backup offline. We recommend that the backup includes also the Switch⇄Crypt configuration directory.

Q: What can happen if the backup device is stolen?
A: Nothing, the files cannot be decrypted because the thief don't know your Switch⇄Crypt password.

Q: What can I do if I get caught at the workplace?
A: Just close the lid of your laptop, or press the two keys <Windows><L> to lock your screen (on PC or laptop). If you have followed the "optional but recommended" installation suggestions all of your sensitive data will be automatically encrypted at this moment.

Q: If somebody knows the password of my login account, does Switch⇄Crypt protect my sensitive files anyway?
A: Yes, because Switch⇄Crypt use a separate password to encrypt your data.

Q: If I use Switch⇄Crypt to exchange sensitive encrypted data with another person (dual use of the tool, second case), how secure is this?
A: High secure. Nobody on this earth can decrypt the encrypted data during transmission via Email, or on your (insecure) shared storage, as long as you have used a strong export password as mentioned before in the FAQs. Follow the instructions at "Export Key Pair". If you have paranoia and don't trust any messenger, you can use Switch⇄Crypt as an alternative to exchange you encrypted files with one or two persons (but not with many persons) in a high secure way. Please keep in mind that all persons use the same key pair, even if they use different passwords. Therefore, if one computer of any person is hacked, all files can be decrypted on all computers. That's the reason why you should share the key pair with only with one or with maximum two other persons. If you are worried that your phone is wiretapped when telling the export password to the other person(s), then use another way to tell them the export password.

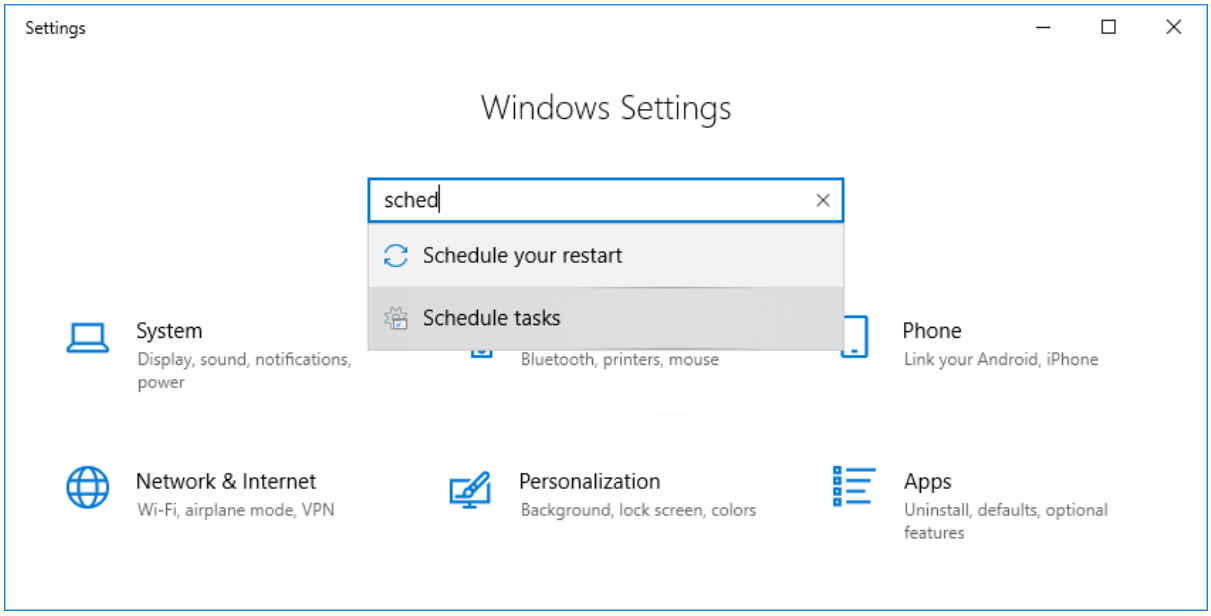
Q: In which programing language is Switch⇄Crypt written?
A: It's written in Java 9.

Q: Which cryptographic algorithm are used by Switch⇄Crypt?
A: RSA key pair length: 2048 bit, hash algorithm for the password and salt: SHA 256, random salt: 24 bytes = 192 bit, random AES key per encrypted file: 256 bit. Random initial vector per encrypted file: 16 bytes.

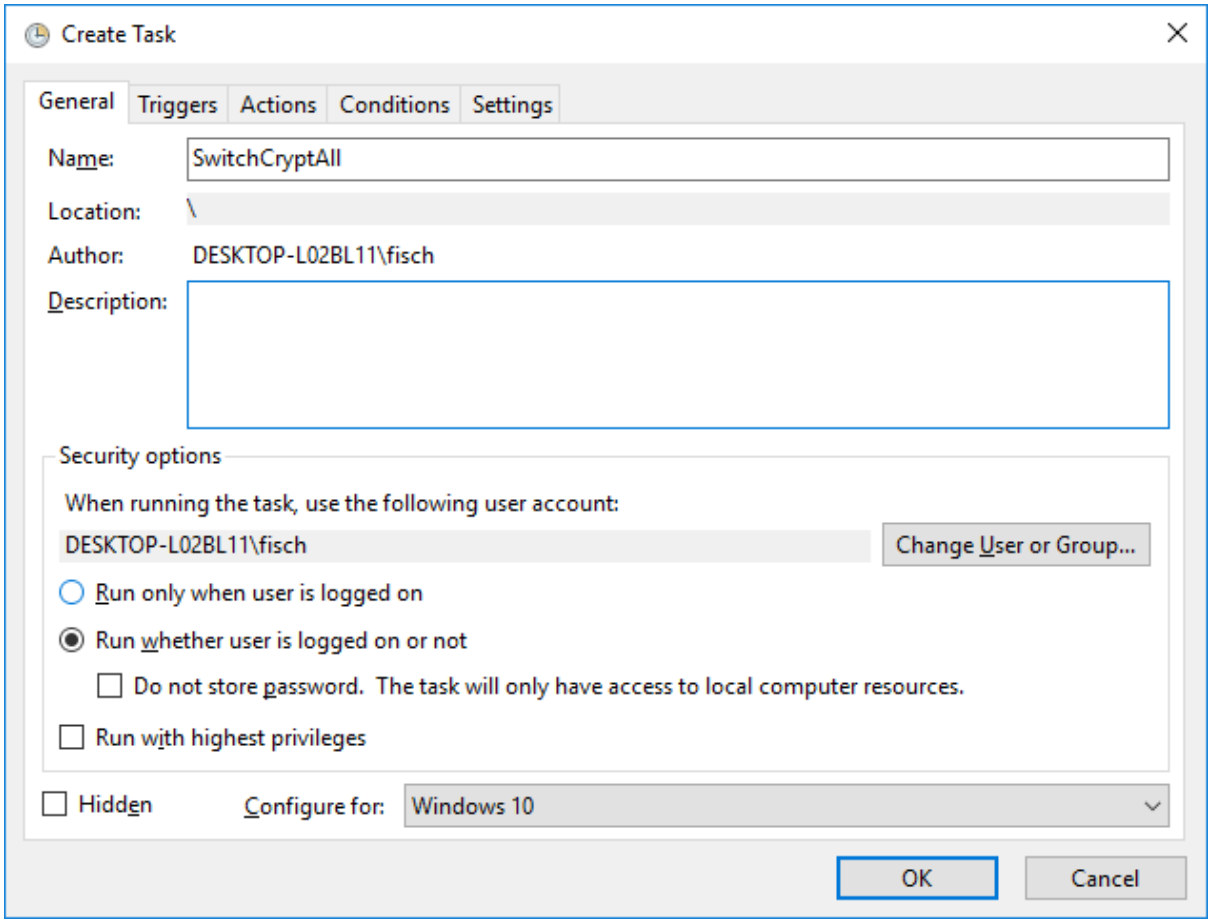
Q: The Switch⇄Crypt tool is freeware, but it's not open source. How can I verify that all encryption algorithms are properly implemented?
A: The core Java class of the Switch⇄Crypt tool that does all encryptions is licensed under the GNU General Public License, V3 (GPL V3). You can check the source code https://www.dkfqa.com/switchcrypt/src/InitialKeyPair-java.html . All other code of the tool is closed source.

Appendix A: Windows Example of calling SwitchCryptAll from Task Scheduler

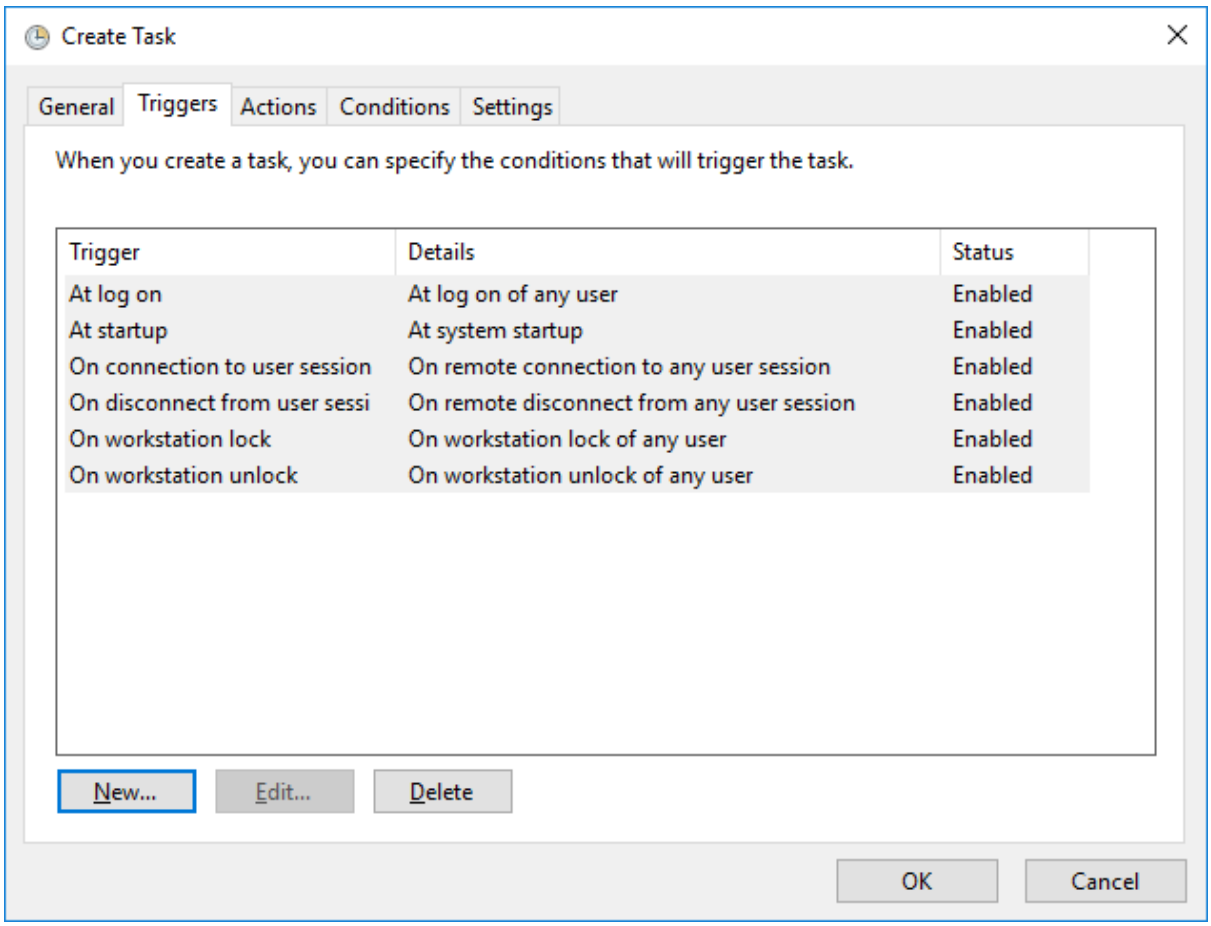
1. Call “Schedule tasks” from Windows Settings:



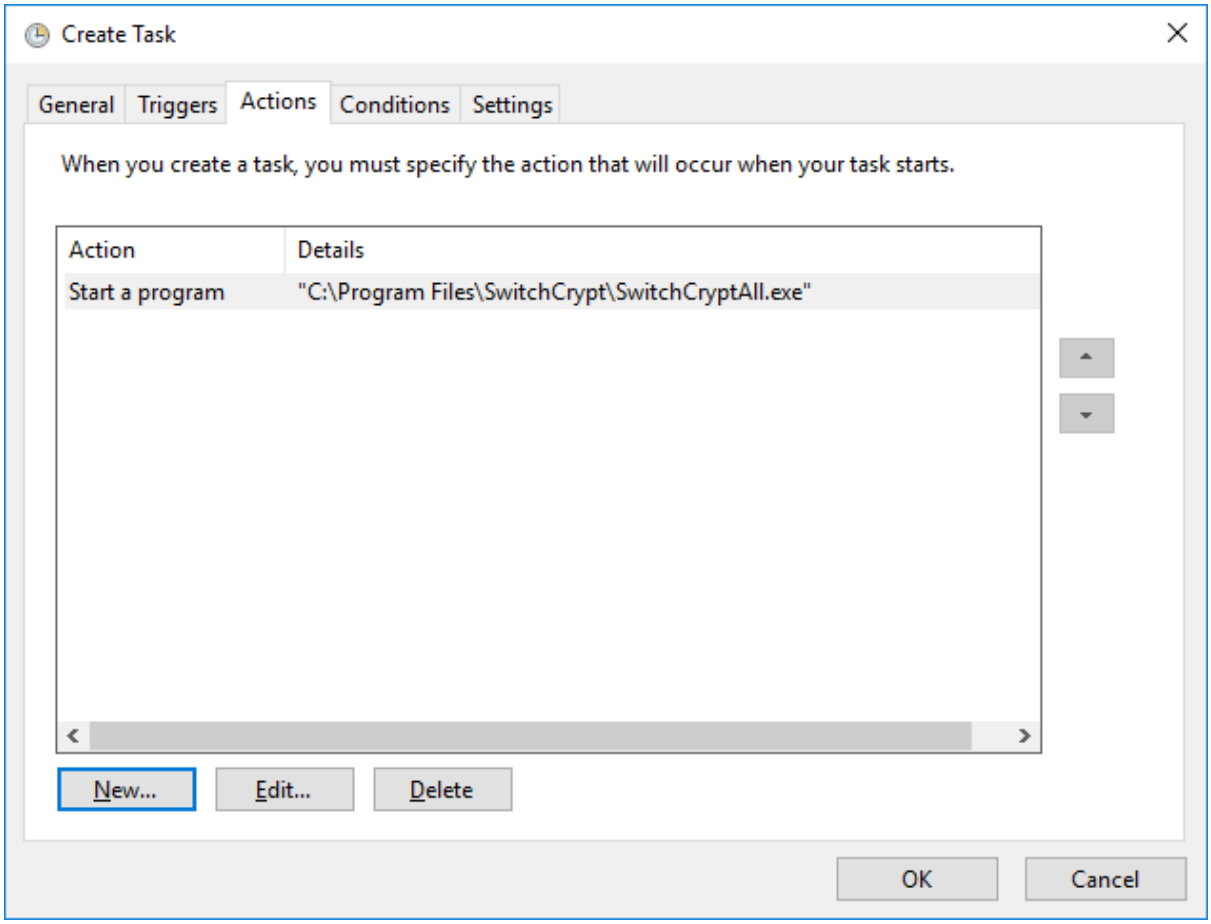
2. Create a new task. Name it SwitchCryptAll, select “Run whether user is logged on or not” and set “Configure for” to “Windows 10”:



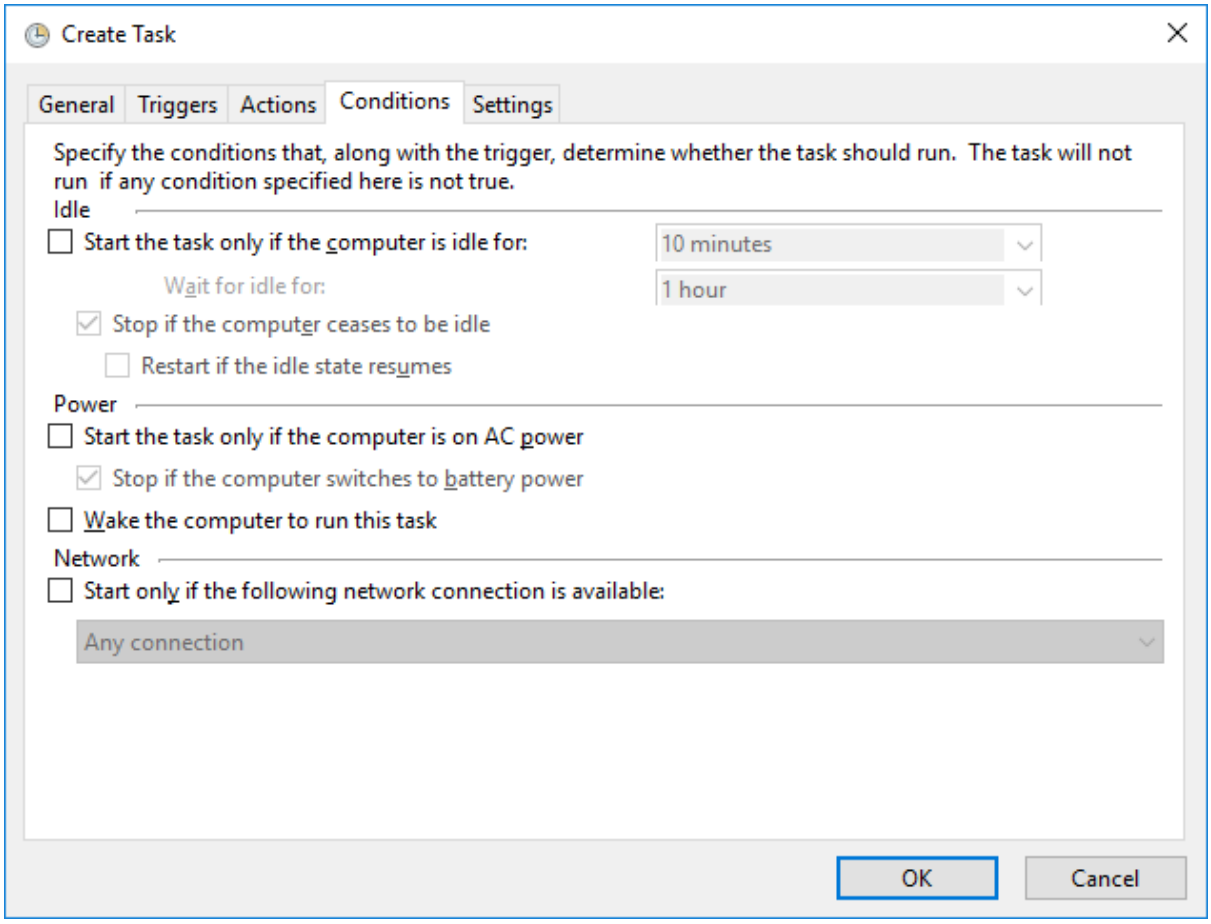
3. Add the following triggers:
   - At log on
   - At startup
   - On connection to user session
   - On disconnect from user session
   - On workstation lock
   - On workstation unlock



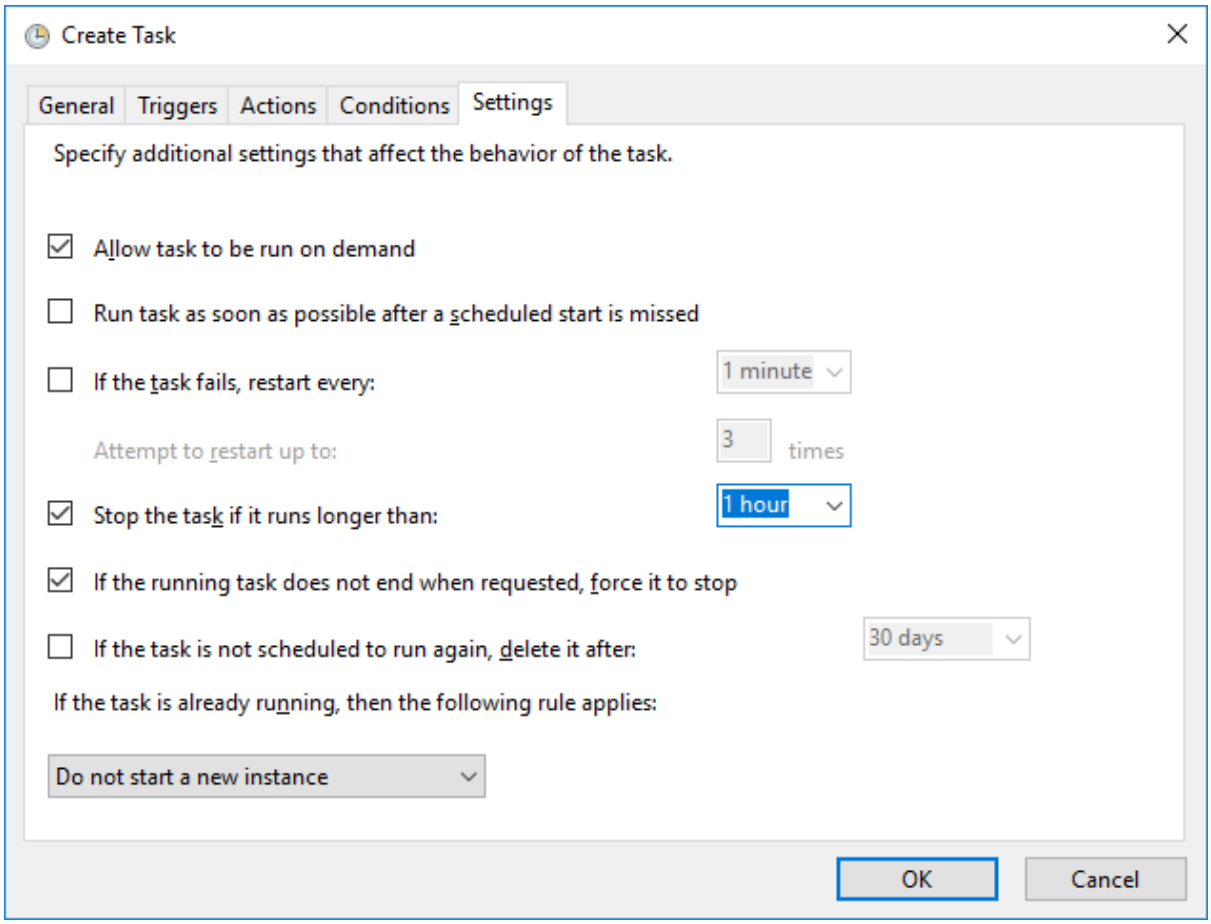
4. Set as action to start SwichCryptAll.exe



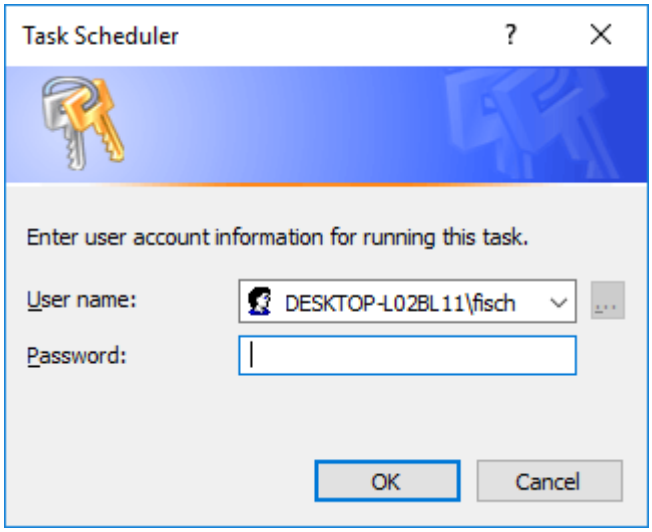
5. Disable all conditions:



6. Set the value of “Stop the task if it runs longer than” to a small value (1 hour), then click on the OK button at the bottom of the window:



7. Finally, enter the password of your Windows account:



8. Perform a small test. Manually decrypt some files with **SwitchCryptUI**. Then lock and unlock your workstation. All files should now be encrypted.