Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com

+372 600 29 89
info@digiflak.com

User Guide

DigiFlak
2017

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Table of Contents

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Terms and Definitions

Flak – the device, used for data protection from online threats.
USB – serial data interface for low-speed and medium-speed peripheral devices.
NFC (Near Field Communication) — Wireless high-technology short-range communication, which enables the exchange of data between devices at a distance of about 4 centimeters or less.
Firewall – a software or hardware-based network security system that controls the incoming and outgoing network traffic, based on applied rule set.
VPN (virtual private network) – a technology that allows to create a secure connection over the Internet connection, thereby protect the confidentiality of information received and sent by the user over the network.
PIN code – personal identification code for device administration.
PUK code – the code to unblock PIN code.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Flak description

Flak is designed to protect user's computer from network threats and includes these options:

- Computer protection (Firewall)
- Internet connection protection (VPN)

Connection to the computer is done via USB connection.
To find out more about how to install the device on the computer, please refer to “Flak installation guide”.

Flak's functions

When connected to a computer, the device:

- Intercepts input and output Internet traffic and analyzes it,
- Checks the network traffic for network threats, unauthorized access attempts and blocks the connection in the case of a threat (Firewall option),
- Provides VPN connection (Internet Security option),
- Provides password less authentication (Easy Login),
- Allows to encrypt files,
- Allows to encrypt e-mails (E-mail Client),

Provides secure internet surfing by blocking malicious web sites (WebFilter)

System Requirements for Flak Device

Supported Operating Systems:

- Microsoft Windows 7 32bit
- Microsoft Windows 7 64bit
- Microsoft Windows 8.1 32bit
- Microsoft Windows 8.1 64bit

There are no limitations to the Web browsers, except for Internet Explorer, only versions starting from 9.0 are supported.

Memory, CPU and HDD requirements:
There are no special requirements regarding Memory, CPU and HDD.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

General information

After the installation of the Flak on the computer the following modules will be available:

- DigiFlak Administrator
- DigiFlak Web Interface

To find out more about how to install the device on the computer, please refer to the «Flak Installation Guide».

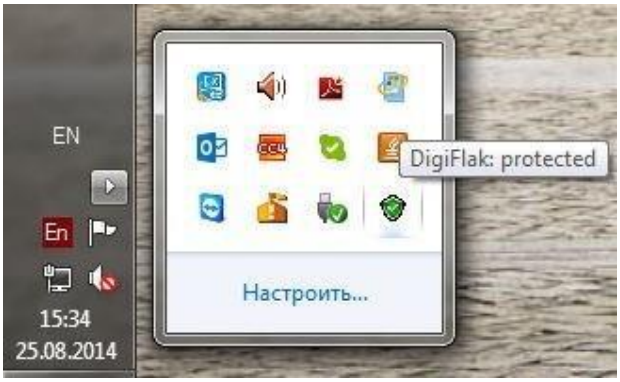
DigiFlak Administrator

To open DigiFlak Administrator click on Start -> All Programs -> DigiFlak folder -> DigiFlak Administrator.

DigiFlak Administrator Status application would start (Picture 1).

Picture 1. DigiFlak Administrator

An application icon would be also placed in the system tray (Picture 2).



Picture 2.System tray.

Vilmsi 5 Tallinn +372 600 29 89
10126 Estonia info@digiflak.com
www.digiflak.com

Right clicking the DigiFlak icon would open the Context menu with the next options:

- DigiFlak Status (starts DigiFlak Administrator Status application).
- DigiFlak Admin (starts Flak Web Interface).

Double clicking DigiFlak icon in the system tray would start DigiFlak Administrator Status window.

The DigiFlak Administrator Status application shows Flak status:

- Flak Connected/disconnected,
- Secured/ Non-secured internet connection
- IP-address, Speed,
- Protected/unprotected traffic.

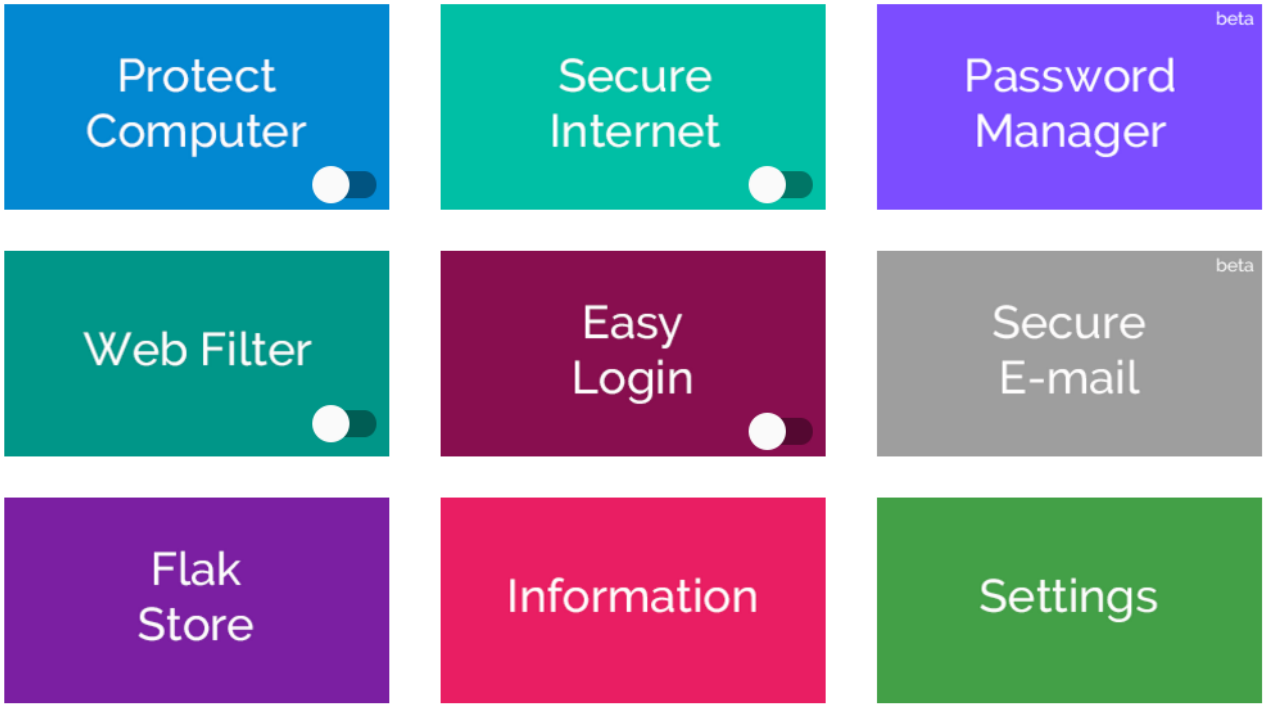
1. When device is connected, then it is displayed in the DigiFlak Administrator Status window, tray icon becomes green and all context menu options become available.
When device is disconnected, it is not displayed in DigiFlak Administrator Status window, the tray icon becomes red and context menu option “DigiFlak Admin” is not available.
2. Internet connection ip-address and speed is displayed in the DigiFlak Administrator Status window.
3. If the device is connected to the PC, internet traffic becomes protected and green traffic-bar is displayed on top of DigiFlak Administrator Status window.
If the device is disconnected from the PC, internet traffic becomes unprotected and red traffic-bar is displayed on top of DigiFlak Administrator Status window.
4. To disable unprotected traffic uncheck the option “Enable unprotected traffic” (Administrator rights are required) – in this case internet connection is available only if device is connected. To enable unprotected traffic check the option – internet connection is available even if device is disconnected.
The option can be checked/unchecked only by administrator.
5. To close DigiFlak Administrator Status select Quit in Tray Context menu.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

DigiFlak Web Interface

DigiFlak Web Interface (Picture 3) allows the customer to manage Flak options:

- Firewall
- VPN
- Software Update
- Manage personal settings (Change PIN)
- View information about Flak device



Picture 3. Web Interface Home screen.

Web Interface can be opened by:

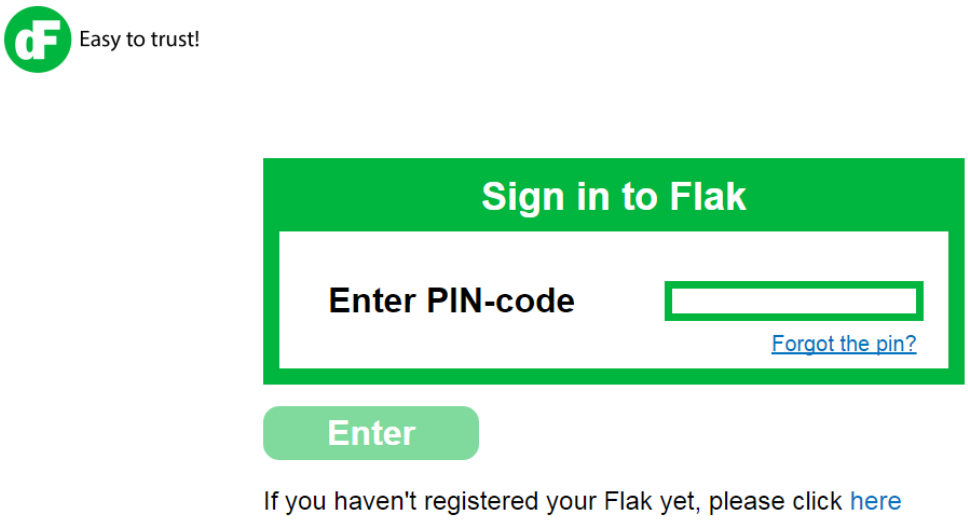
- Selecting context menu DigiFlak Admin in the DigiFlak Administrator in the system tray.
- Typing myflak.com in a browser address bar.

Signing In

1. Open the Web Interface (myflak.com).
2. Type your PIN-code* in the Sign in to FLAK form (Picture 4). Press Enter**.

* PIN-code for first login in beta program is 4242. PIN-code must be changed after the first log in.

** **If the current PIN-code is entered incorrectly 3 times, then it gets blocked. Please refer to PIN Restoration for further explanation on this topic.**



Picture 4.Sign in to FLAK

Web Interface Home screen will be displayed in case the successful log in is (Picture 3).

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

PIN restoration

PIN-code is blocked if it is entered incorrectly 3 times.

1. If your PIN code is blocked or you forget it, you must send an e-mail with your FlakID to support@digiflak.com to get your personal PUK code to restore the PIN-code.
2. To restore the PIN code open the link ("Restore PIN" or "Link") in sign in form (Picture 5).

Picture 5.PIN code is blocked.

3. Restore PIN code form is displayed (Picture 6). Enter received by e-mail (the same e-mail address, which was used during the registration of the FLAK) PUK code into the field and press OK button.

Picture 6.Restore PIN code form.

4. If the PUK code is entered correctly, Sign In form is displayed again.*
5. PIN code 4242 should be used after the restoration of PIN code to sign in Flak via Web interface. You must change the PIN code immediately code after the successful log in.

***If PUK code is entered incorrectly 3 times, FLAK gets blocked forever and can't be unlocked.**

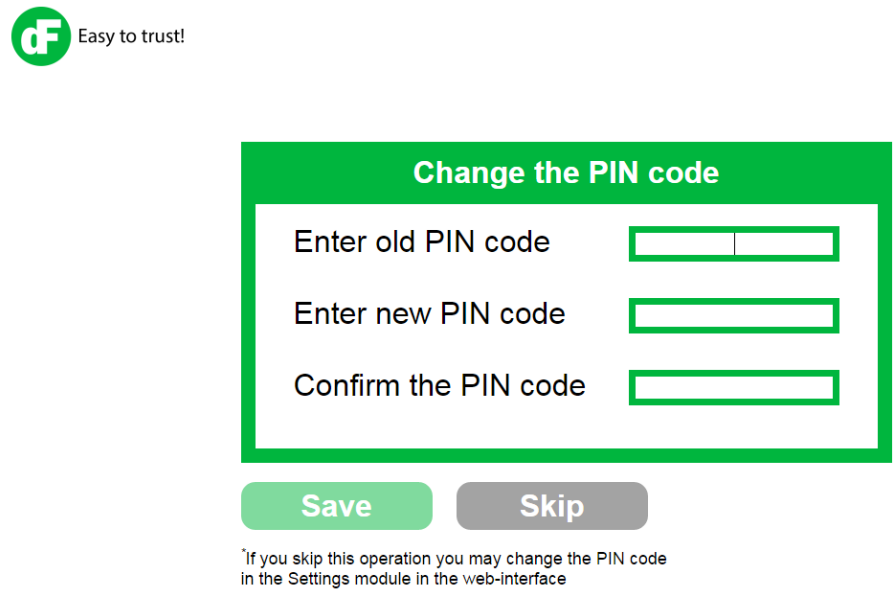
Registration

In order to enjoy premium services (Premium VPN, Flak store, file encryption), you would need to register your Flak first.

You can access the Flak Registration page with non-registered Flak by:

- Clicking on If you haven't registered your Flak yet, please click here on the Web Interface Home page
- Clicking on Flak Store

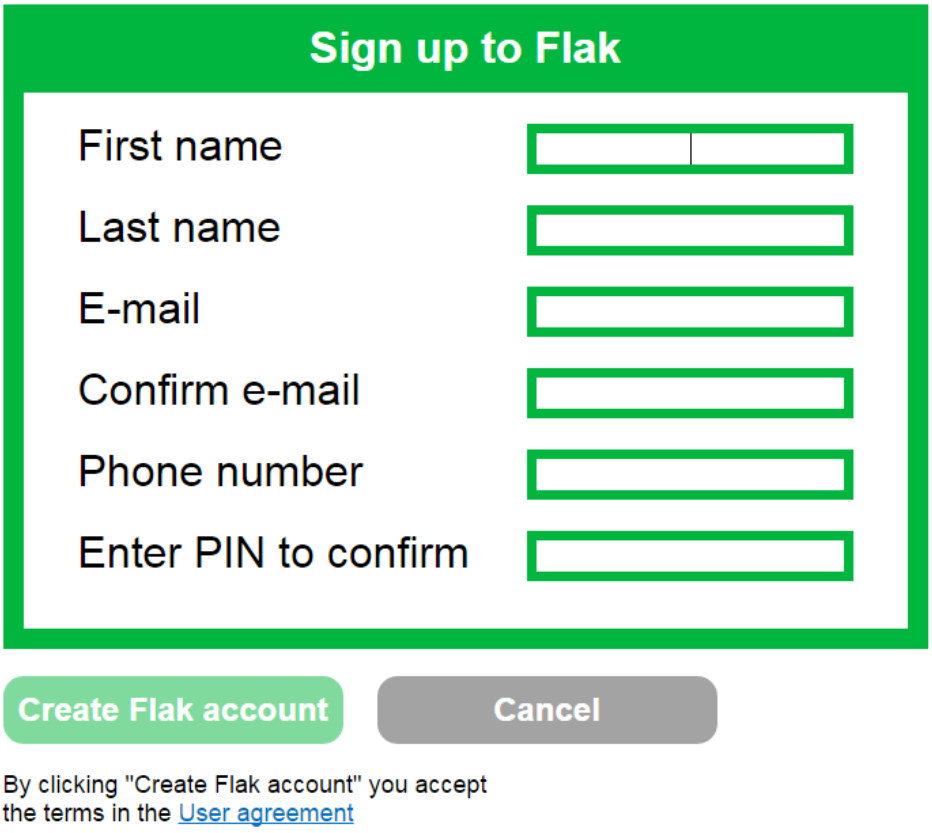
You would first be asked to change your PIN code.



Picture 7. PIN code Change form.

You can either change your default PIN code or Skip this step (and change the PIN code later in the Settings page).

You will be taken to the Flak Registration page. Please fill in all the fields.



Picture 8. Flak Registration page

Please note that you would need to provide a unique e-mail and phone number for your device.

Click on Create Flak account. Do not disconnect the device! After the registration is finished, reinsert Flak into the computer.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Protect Computer

Flak is designed to protect a computer from various internet threats.
Protect computer contains two sections:

- Firewall
- Malware Protection

Switching on/off Protect Computer option would switch on/off both Firewall and Malware Protection sections.

To switch on/off the option click on green/white button on Protect Computer option (Picture 9). Toggling between red/white buttons of Protect Computer option would cause both functions (Malware Protection and Firewall) to be switched on and off. The button would stay green if both functions are switched on. The button would stay white even if only one of functions (Malware Protection and Firewall) is switched off.

Picture 9. Protect Computer option

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Firewall

Firewall option can be switched on/off separately. To change Firewall protection mode click on Protect Computer. There are two options:

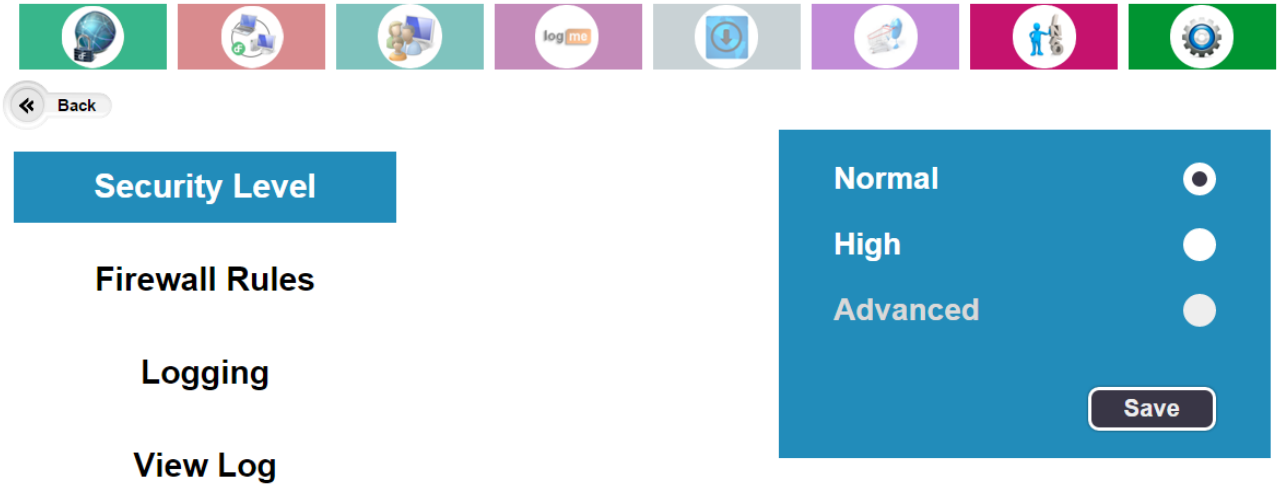
- Malware Protection
- Firewall

Picture 10. Firewall and Malware Protection options.

To switch on/off the firewall click on button on the Firewall option.
By default this option is switched on in Normal protection mode (the on/off button is green).

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Click to Select Firewall option. Firewall settings would open.



Picture 11. Firewall settings.

In this section you can:

- Select either Normal or High protection modes.
- View Firewall Rules for the selected mode.*
- Set Logging option to on/off. *
- View Firewall logs, if Logging option is switched on. *

* These options are available in expert mode only. Please refer to Settings to find out how switch to the expert mode.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Malware Protection

One of Flak's functions is antivirus protection of http traffic.

The Device scans incoming http traffic for harmful content. In case of the possible threat the web site in question gets blocked and the warning message would appear. This option can be found in Protect Computer section. By default this option is switched off.

To toggle between switching the option on and off, click on the white/green button on Malware Protection section

Picture 12. Switch ON/OFF Malware Protection option

Secure Internet

Flak device is allows to protect an internet connection with the VPN connection.

To enable VPN connection select the option Secure Internet. The option is switched off by default. To switch on/off VPN connection press white/green button on the Secure Internet section.

Picture 13.Secure Internet section.

When Secure Internet feature is switched on, then your internet connection becomes secured – all the internet traffic would go via one of the VPN servers.

To choose a VPN gateway click on Secure internet section. On the VPN settings page you would be able to choose one of the 3 VPN connections:

1. One of the three predefined VPN servers (New York, USA; Frankfurt, Germany; Amsterdam, Netherlands)

To choose one of the options from the dropdown list, select Flak Gate radio button and click on Connect. Secure Internet option would be switched on with the selected VPN server. Note: the last selected VPN server settings will be chosen automatically when switching on the Secure Internet option on the main page. If the option Flak Gate does not work, update the x509 certificate (see Settings. VPN certificate update).

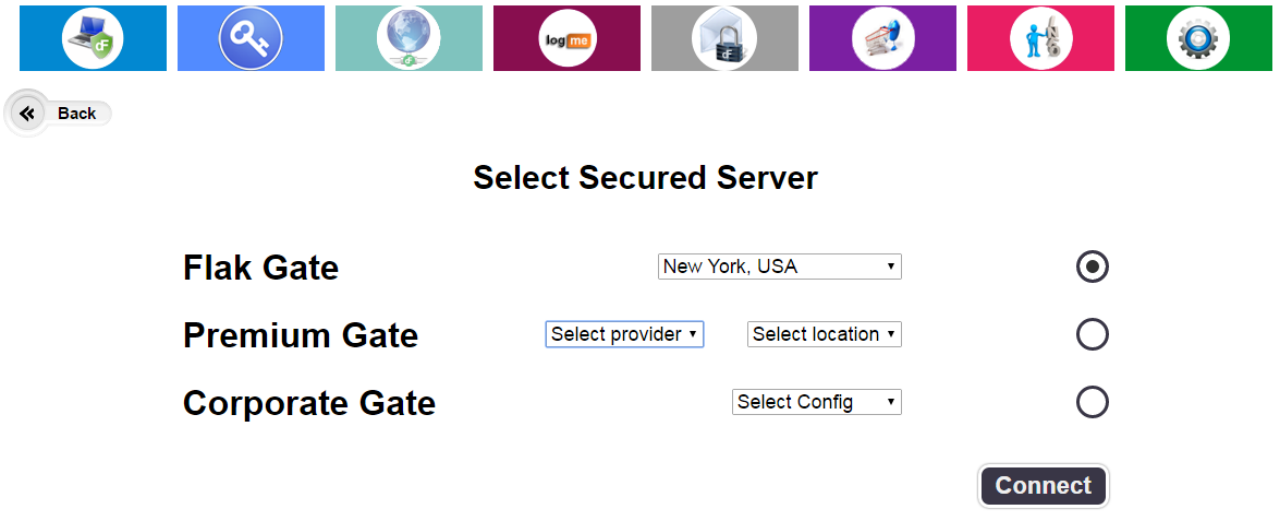
2. Premium VPN server (purchased via Flak store) with access to large amount of VPN servers. This option requires Flak registration.

To choose this option of VPN connection, you would first need to register Flak (check Registration section), and pay for the Premium VPN (check Flak Store). Only then Premium VPN option would become available. To establish a VPN connection select a name of the VPN provider from the list of providers and the server from the list of servers, select Premium Gate radio button and click on

Connect. Note: the last selected VPN server settings will be chosen automatically when switching on the Secure Internet option on the main page.

3. User/defined VPN Server. You would need to upload configuration first. Template can be found here.

Select Load new config from the dropdown list and upload a configuration file in the OpenVPN format. After the file will be uploaded to Flak, it will become available for selection in the Corporate Gate dropdown list. Choose the file in the list, select the Corporate Gate radio button and click on Connect. Note: the last selected VPN server settings will be chosen automatically when switching on the Secure Internet option on the main page.



Picture 14. Secure Internet settings.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Web Filter

Web Filter is one of Flak's main features. If Web Filter option is switched on, then the device is going to block access to dubious internet resources (for example sites containing malware or adult only sites).

To switch the option on/off, press on white/green button on the Web Filter section.

Picture 15.Web Filter section

Note: for this option to work properly you need to clear the DNS cache in Windows. After you have switched the option **On,** run the cmd.exe (Start -> All programs -> Standard -> command prompt) and write in the command prompt window *ipconfig /flushdns* and then press Enter.

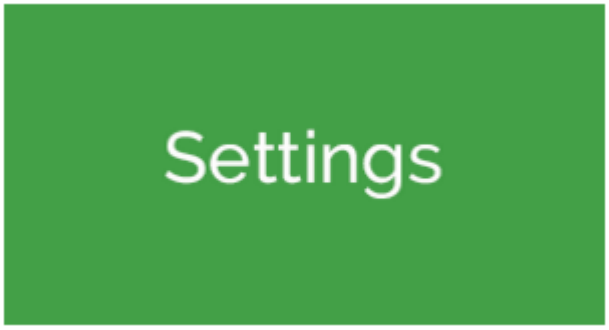
Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Settings

Section Settings allows the customers to perform next actions:

- Change the PIN code
- Update the device
- Update the VPN certificates
- Create a backup copy of the device's content

To open the Settings click on the Settings section on Home screen.



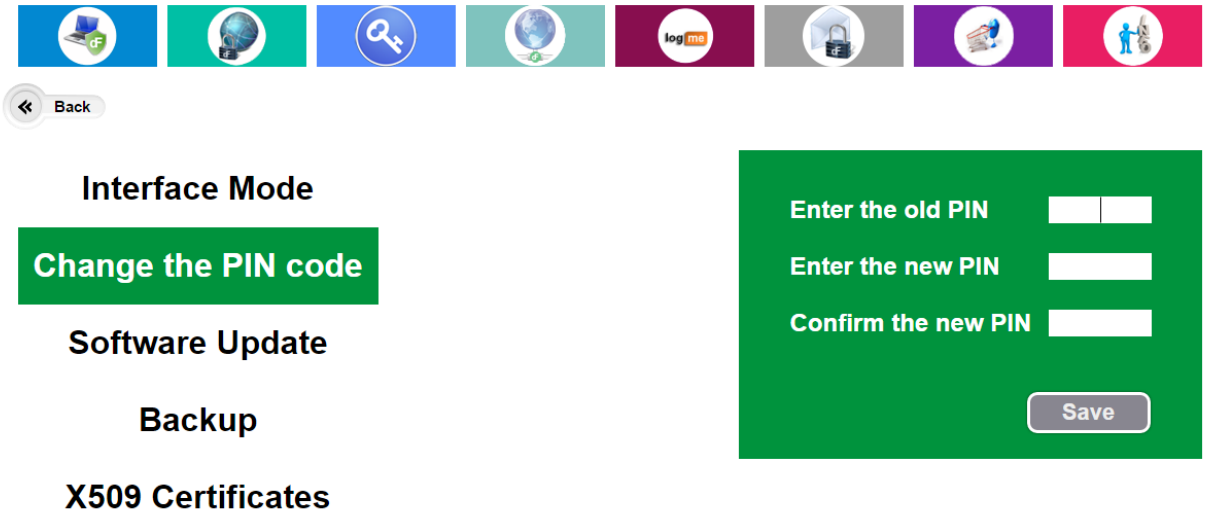
Picture 16.Settings section

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Changing the PIN code

To change PIN code:

1. Click on Settings section and then select option Change PIN code.



Picture 17. Change PIN code

2. Enter your current PIN code* into the field “Old PIN”. ***If current PIN-code is entered incorrectly 3 times it will be blocked**.
3. Enter the new 4-digit PIN code into the field “New PIN”.
4. Enter the new PIN code again into the field “Confirm new PIN” to confirm the new PIN code.
5. Press Save.

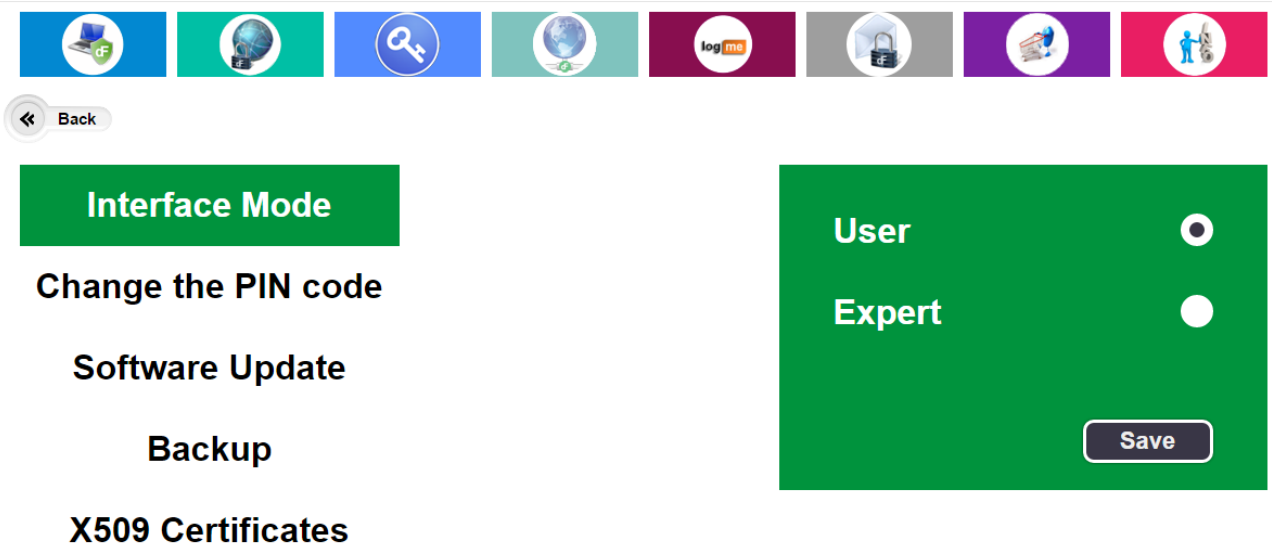
Your PIN code has been changed and now it can be used to sign in to Flak Web Interface.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Interface Mode

In the section Interface Mode you can select one of the existing interface modes:

- User (set by default)
- Expert



Picture 18.Interface mode

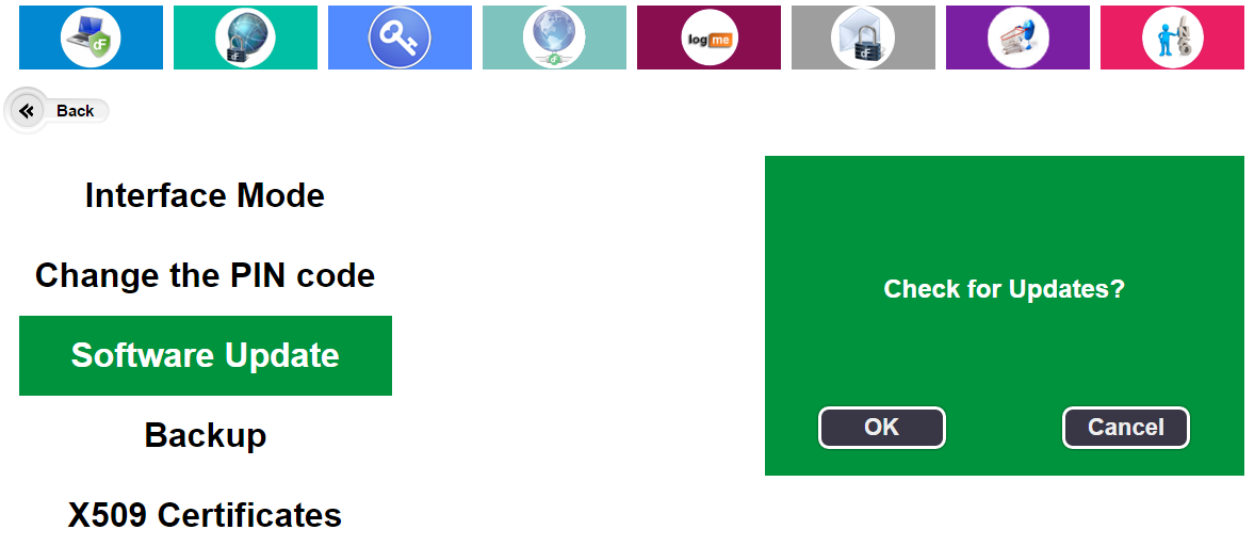
In expert mode following Firewall options are available:

- Firewall Rules.
- Switching logging on/off.
- View logs.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

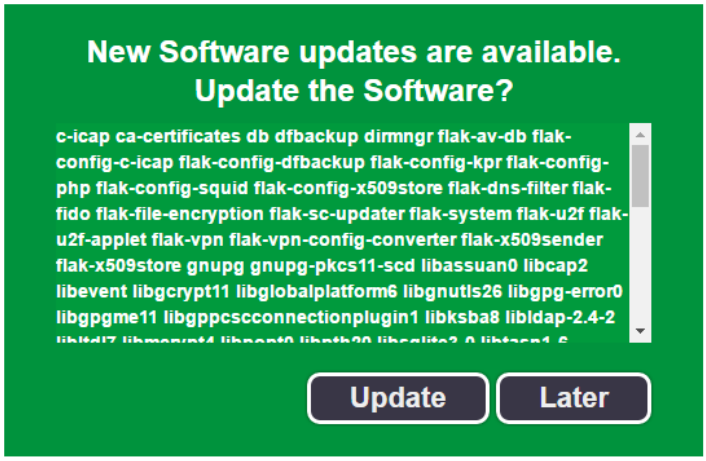
Software update

Please switch off the Firewall and Secure Internet options before starting the update procedure. To update the software, open Settings section and select option Software update.



Picture 19.Software update

1. Click OK to check if there are any updates available.
2. If updates are available, the system prompts you to update software.



Picture 20.Updates are available

3. Click on Update button to update the software.

4. Wait until the updates are downloaded and installed on the device*.

*Do not disconnect the device from PC during the update process; the device might become completely unusable (broken).

5. Reconnect the device to finish update procedure.

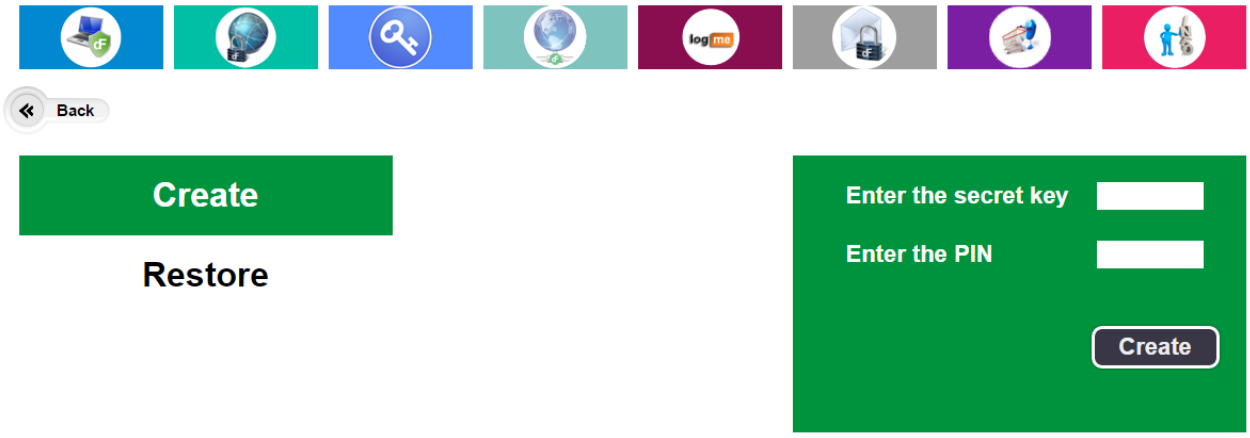
Device data backup

Creating a device data backup

So that your data on the device wouldn't get lost in case the device gets stolen or broken, you can backup data on the device. To run a backup:

1. Go to Settings and select Backup
2. In section Create enter your personal secret key (which can be a phrase or a combination of numbers). Note: only you would know this secret key.
3. Enter the PIN code.

IMPORTANT: Please remember your secret key and a PIN code used when creating a backup. You would need during data restoration.



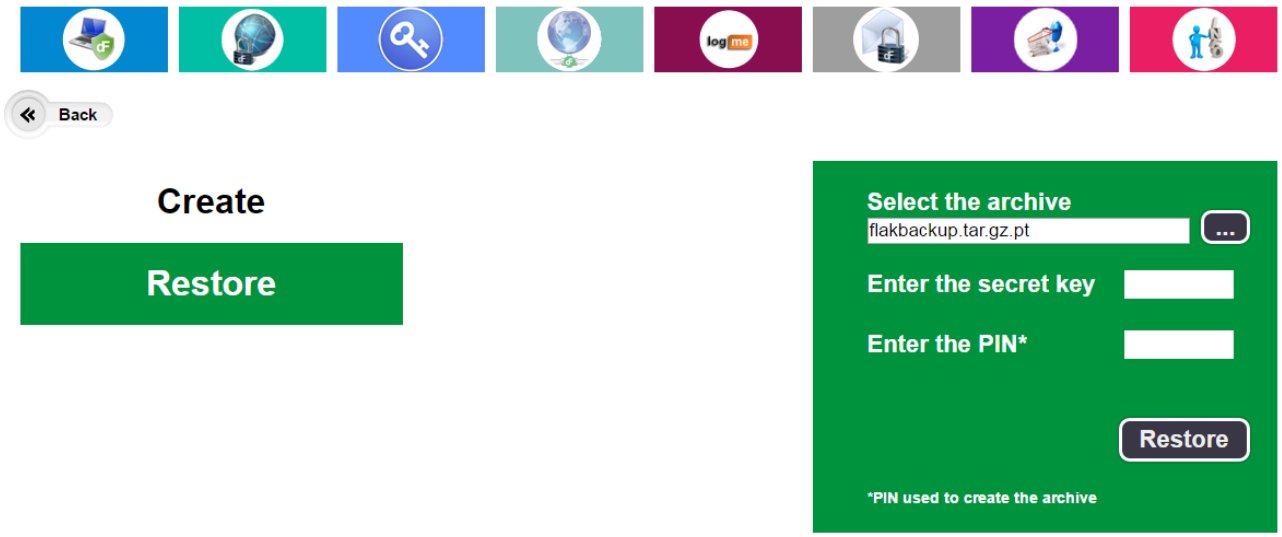
Picture 21. Creating a device data backup

4. Press Create. And archive of Device data backup would be created and downloaded to your computer. Please store the archive on your computer.

Restoring device data from the backup

To restore the data on your device:

1. Go to Settings, select Backup and then Restore.
2. In section Restore enter the path to your archived device data backup by clicking on a button with three dots. Archived file should look like *flakbackup.tar.gz.pt*



Picture 22.Restoring device data from backup

3. Enter the Secret key and the PIN code used when creating a backup.
4. Click on Restore.

   The device would restart with the restored from the archive data.

Attention! There is defect with backup option. Files encryption option becomes broken after the restore device data. The defect will be fixed in future versions.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

VPN certificate update

If the VPN-connection Flak Gate does not work, update the x509 certificate.

1. To update the certificate, open Settings section and select option X509 Certificate.
2. Click OK to check if there is new certificate available.
3. If new certificate is available, the system prompts you to update it.
4. Click on Update button to update the certificate.
5. Wait until the updates are downloaded and installed on the device*.

*Do not disconnect the device from PC during the update process; the device might become completely unusable (broken).

6. After the update of the certificate is finished the device would restart

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

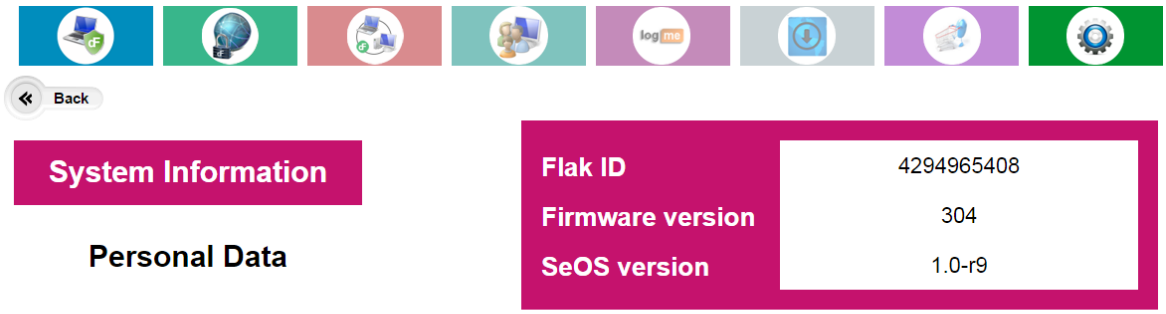
Information

To check Flak ID, firmware version, etc. click to open Information section.

Picture 23.Information section.

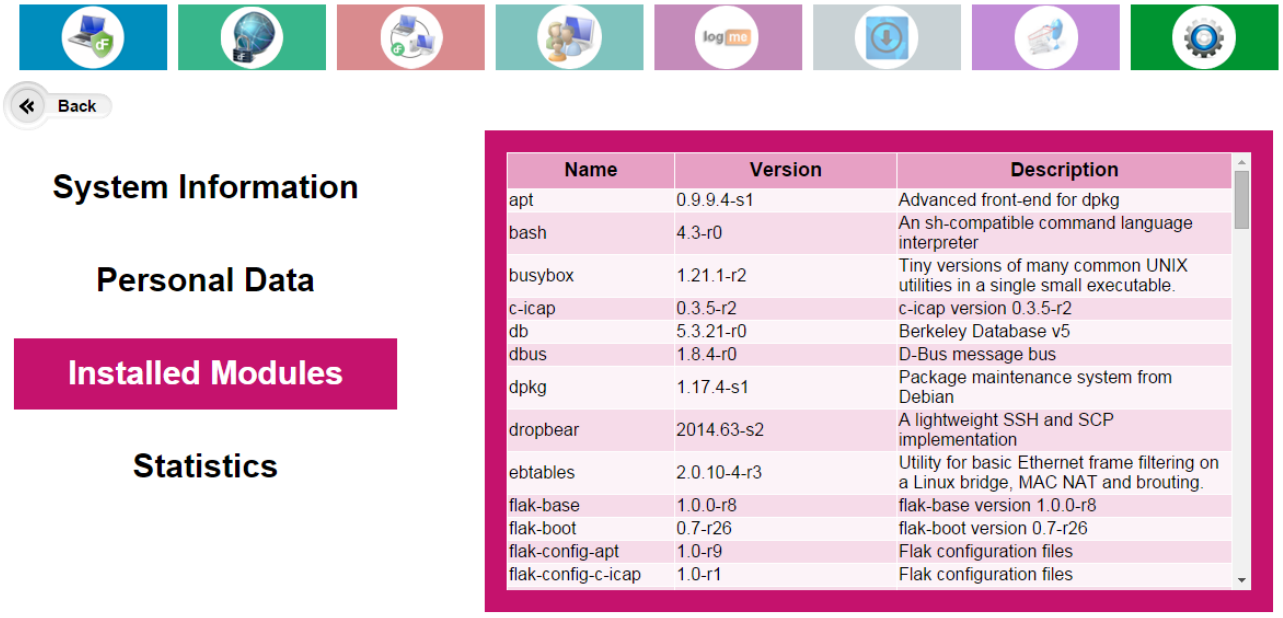
Section Information allows checking of the next information about device:

1. System Information (Flak ID, Firmware version, SeOS version).



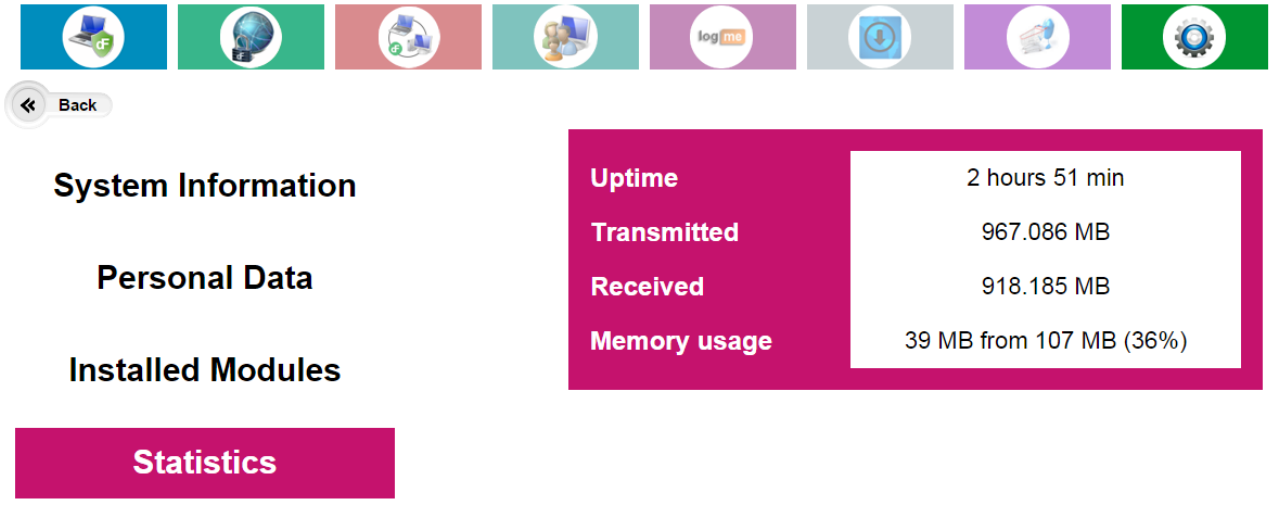
Picture 24.System Information.

2. Installed Modules (all installed modules, versions and description).



Picture 25.Installed Modules.

3. Internet statistics (Uptime, Received/Transmitted traffic, Memory usage).



Picture 26.Statistics.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Easy Login

One of Flak's features is password-less login into internet resources, which support access via SSL certificates.

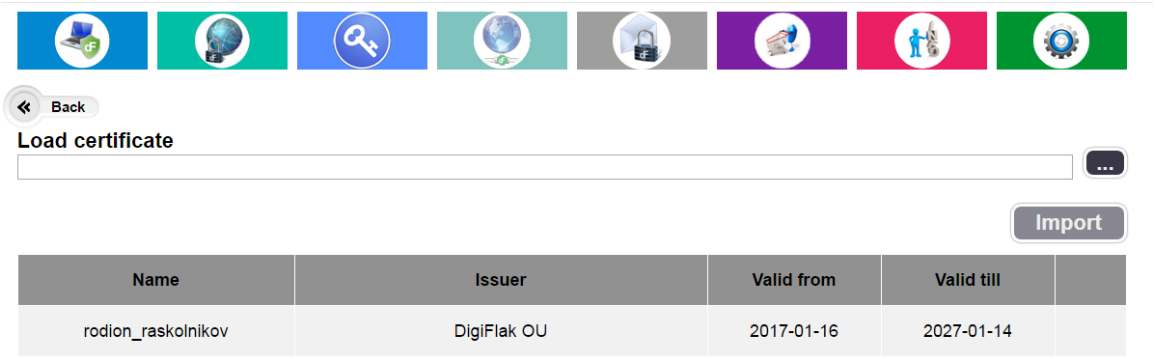
This functionality is provided by Easy Login option.

Picture 27. Easy Login

To be able to login with SSL certificate into supported internet resources, you would need to follow these steps:

1. Prepare the certificate to be imported into the device (you can ask for the certificate on the supported internet resource).
For example, StartSSL.com issues the certificate upon the registration on their site. If the certificate is installed in the browser, then you can export it from the browser. The certificate must be save on the computer first, then you can import it into the device.

2. Click on Easy Login option and then on Certificates. The page with the list of the certificates installed on your device would open. You can add and remove the certificates on this page.



Picture 28. List of certificates

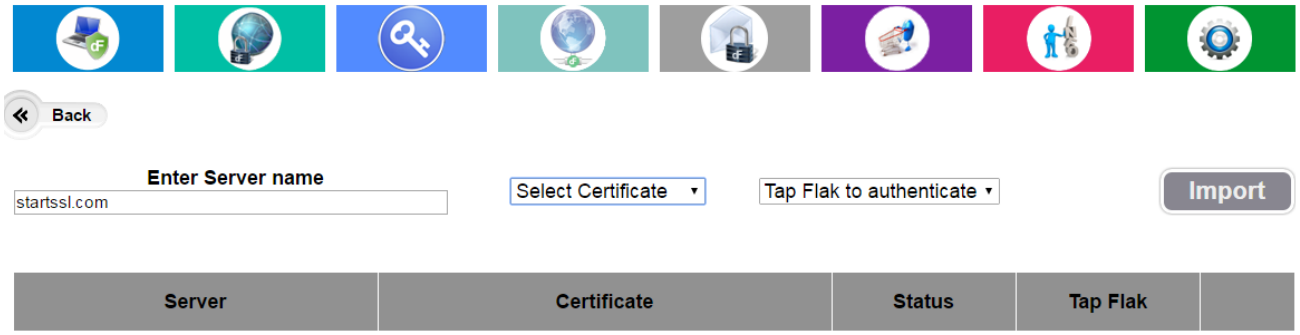
3. To import a certificate into the device, click on the bclack button with three dots. In the opened window select the path to the certificate and click on the button Open. The path to the certificate would appear in the Load Certificate field, click on Import.

You would be asked to provide a password used when the certificate was generated. After the import of the certificate is finished the device would restart. Go back to Certificates page and check for the imported certificate in the list. To remove the certificate from the device click on Delete.

Name	Issuer	Valid from	Valid till	
rodion_raskolnikov	DigiFlak OU	2017-01-16	2027-01-14	
amaysienya@gmail.com	StartCom Class 1 Client CA	2016-02-16	2017-02-16	Delete

Picture 29. Certificate has been added.

4. For the imported certificate to function properly you need to add the server (aka the web address). Go to Easy Login and then to Servers. Type your server name in the Enter Server name field in the form *ServiceProvider.com* (omit www.); click on Select Certificate, and select your imported certificate from the drop down list; click on Tap Flak to Authenticate and select either Yes (if you want to tap the Flak for authentication each time you log in to the Server web site) or No.



Picture 30. List of servers

5. Click on Import. Server will be added to the list of servers.

6. To remove the server from the list click on Delete.

Server	Certificate	Status	Tap Flak	
startssl.com	rodion_raskolnikov	enabled	no	Delete

Picture 31. Server has been added

7. On the main web page click on the button on Easy Login option. The button would turn green.

8. You can now login to the added internet resource (server) and get authenticated with the certificate stored in the device.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

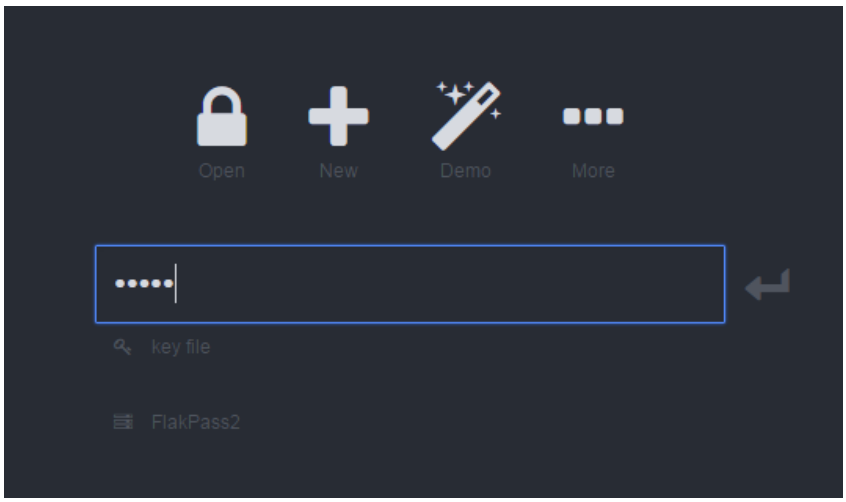
Password Manager

Password Manage is one of devices functions. To start using this function you need to click on Password Manager. Please note, this is option is currently in BETA. We do recommend making backup copies of the Flak at least once a week to keep the database of passwords safe.

Picture 32. Password manager

Logging into Password Manager

Click on Password Manager on the main menu. The master password login screen would appear. This is your main password for the passwords database. The default password is 4242. You would need to change it.



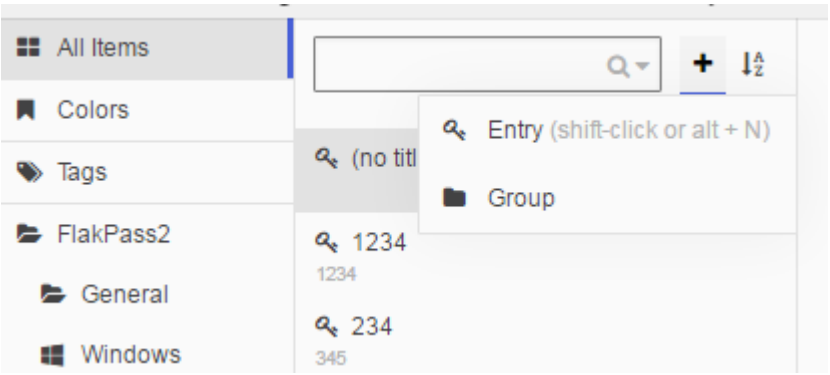
Picture 33. Master password login screen

After you enter the master password, the list of saved passwords would appear.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Adding a new password entry

To add a new password entry to the list, click on plus sign on the top of the list and on the drop down menu select Entry.

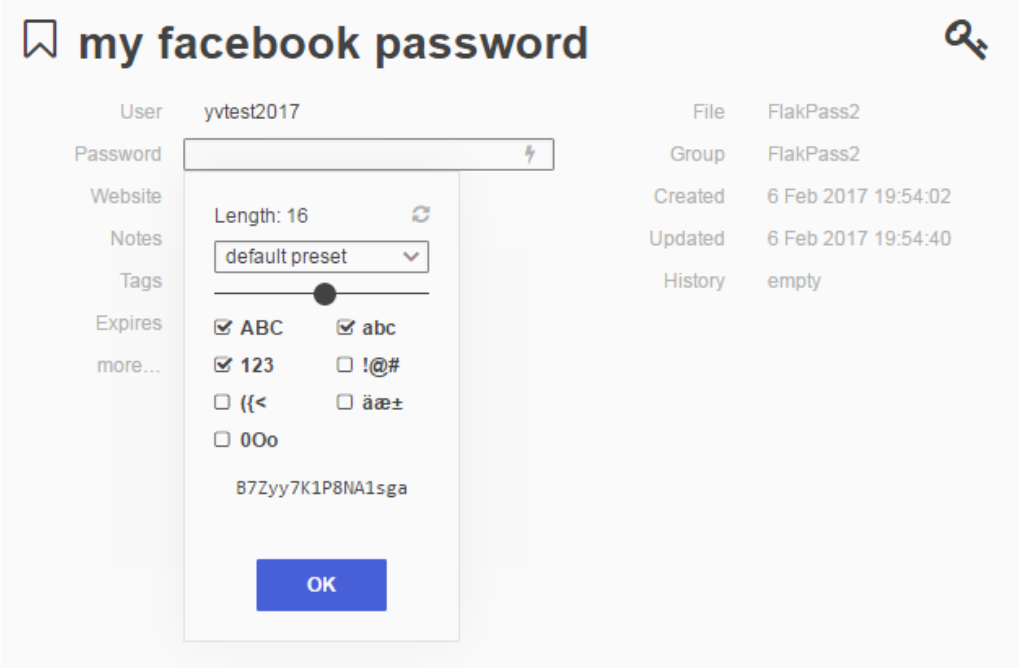


Picture 34. Adding a new password entry

Fill in the next fields:

- Title
- User
- Password
- Website
- Tags
- Notes
- Expires

If you want to password to be generated, click on the lightning sign in the password field. The new window will appear where you can select which options to choose (number of symbols, which combination of symbols, etc). After you are done click on OK. The new password will be generated.



Picture 35. Password generation options

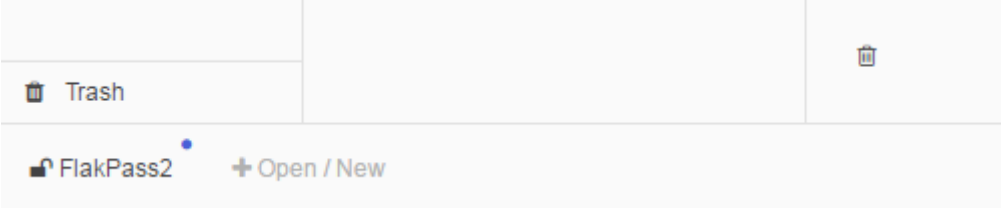
When all the fields will be filled in, the password entry will be automatically saved in the list of passwords.

To copy a password to be used with a web site, right click on the entry you need, and click on Copy password. Password will be saved in the clipboard. You can now paste it into the web site field.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

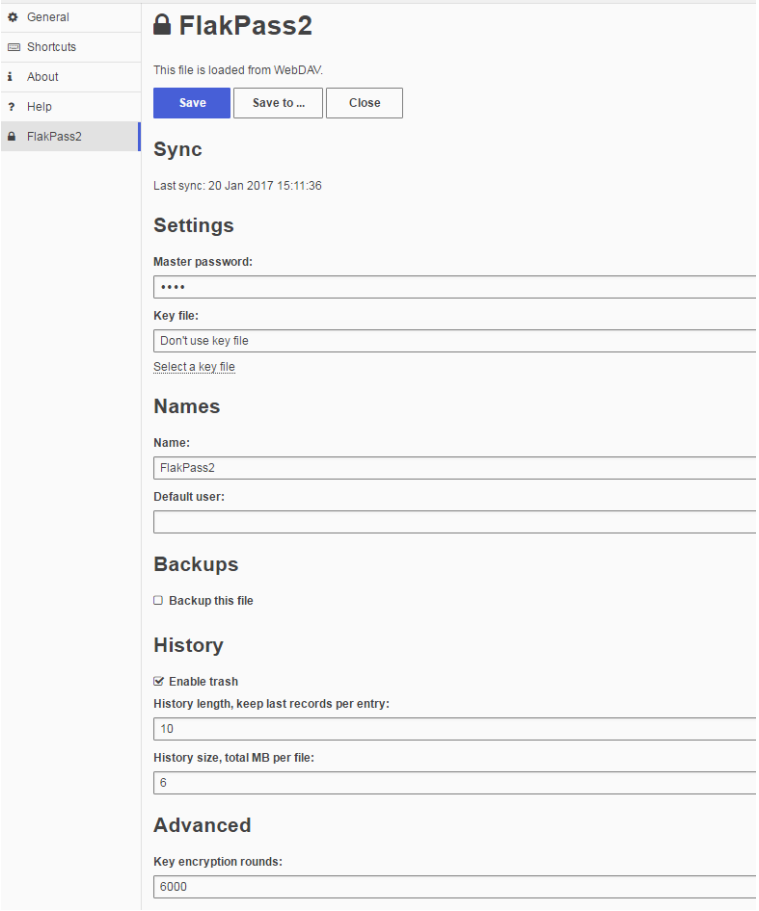
Saving the changes

After you add new passwords, etc in order to save the changes click on FlakPass2 in the bottom left corner.



Picture 36. FlakPass2

Flak Settings page would open. Click on Save on the top of the screen.



Picture 37. File Settings page

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

The changes have been saved. You can also save the changes by clicking on Lock button  in the bottom right corner of the page and then click on Save changes.

Changing the master password

To change the master password:

1. Click on FlakPass2 in the bottom left corner
2. In the Flak Setting page, enter the new master password in the field Master Password.
3. Click on Save.

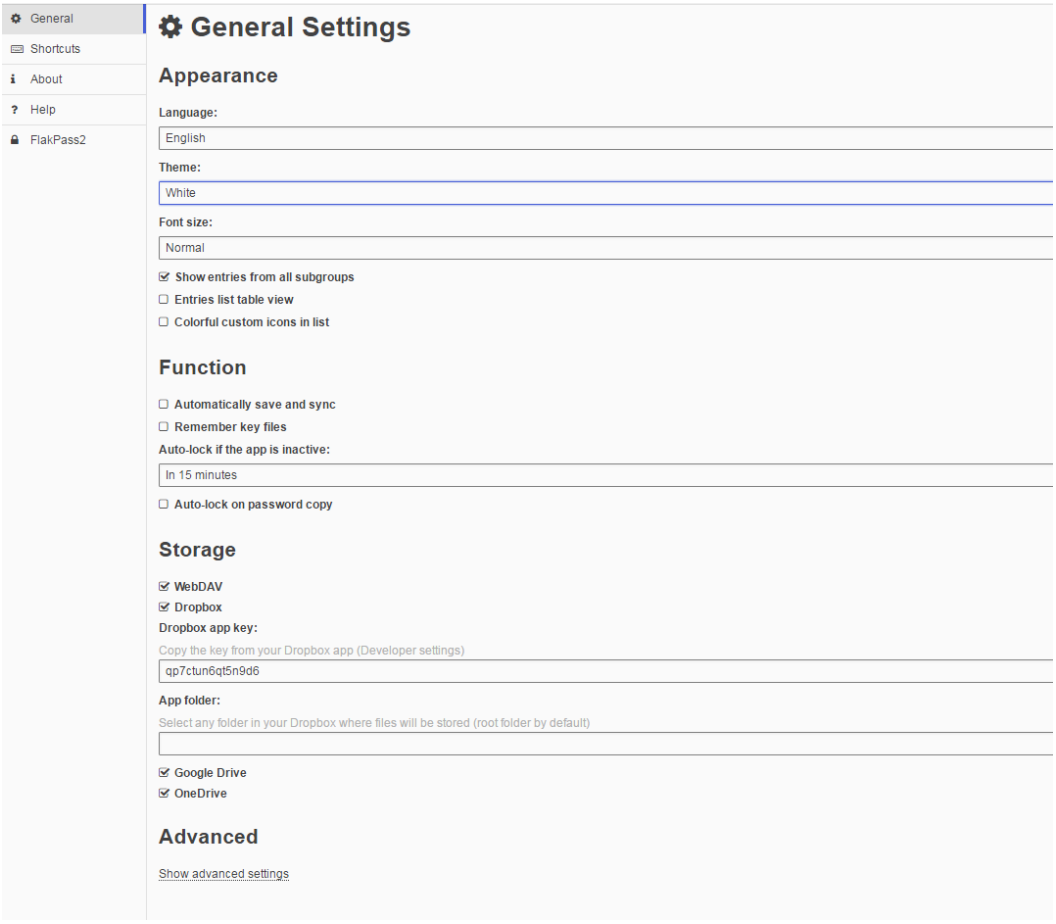
If you will be asked to provide a password again after you clicked on Save, then

- Click on Cancel
- Click on Lock to exit the entry.
- Click on Discard changes.
- Reinsert Flak into the USB port
- Enter the PIN code
- Click on Password Manager on the main screen and repeat the steps described above.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Settings

Click on  to open the Passwords Manager Settings page.



Picture 38. Settings

You can

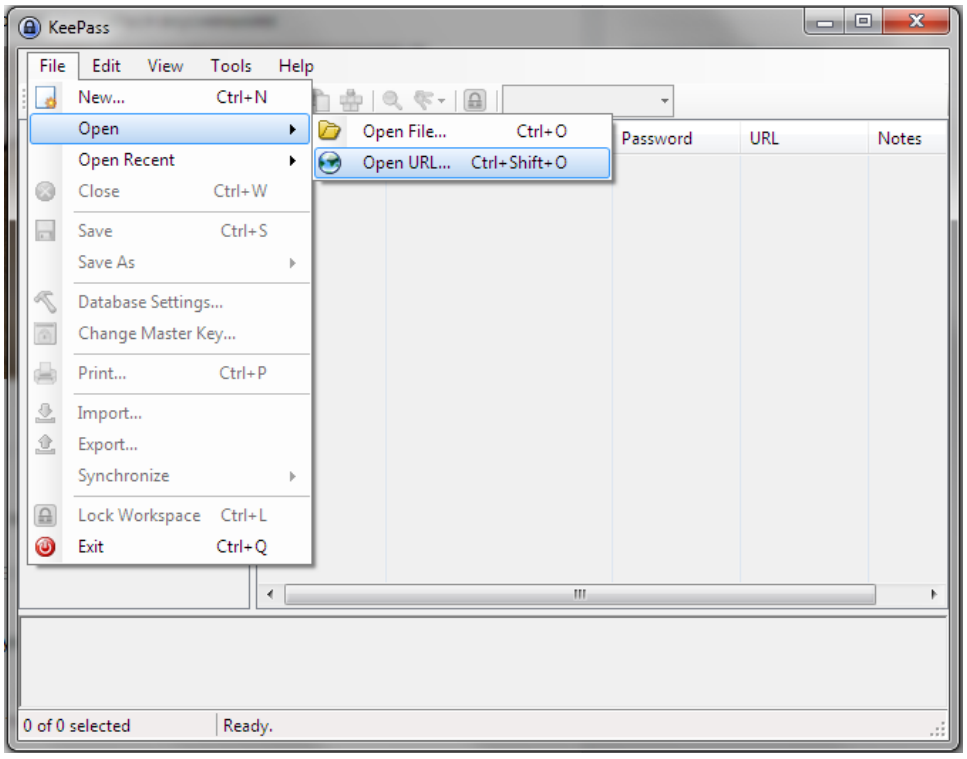
1. Change the langauge
2. Change the background color
3. Change the font size
4. Set the autosave option
5. Set the save options

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Editing the files in the Password Manager for Windows

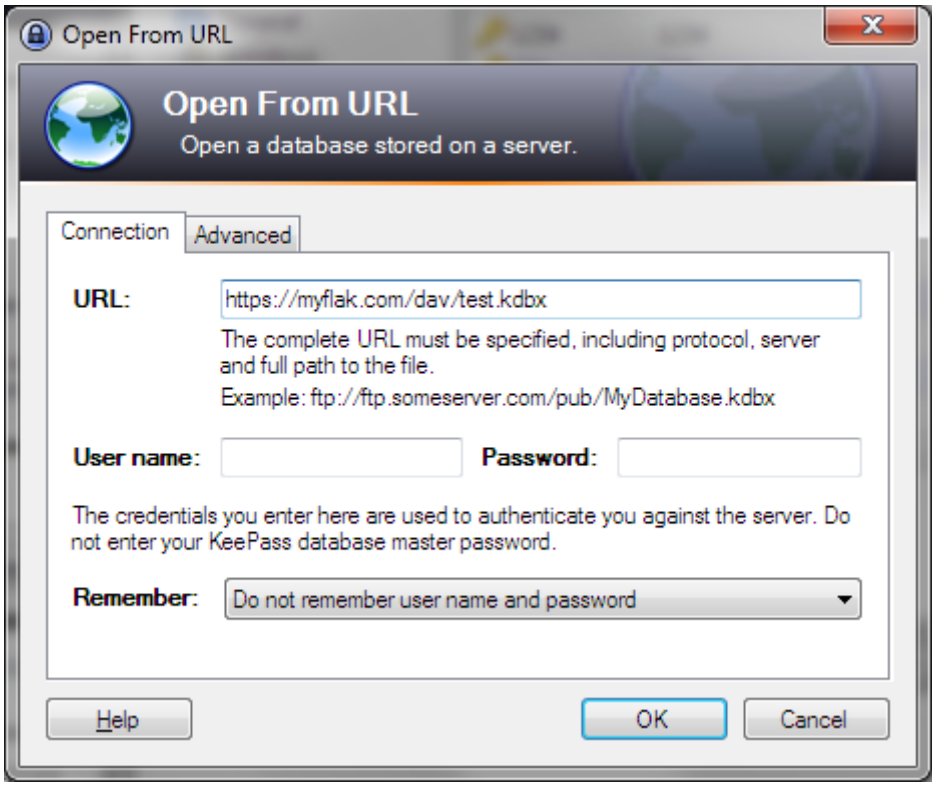
You can also edit the passwords file in KeePass Professional Edition for Windows.
The application can be downloaded here

To open the password file in KeyPass application click in the menu on File -> Open -> Open URL.



Picture 39. Opening the file in KeyPass

Enter the URL https://myflak.com/dav/test.kdbx and click on OK. Enter the Master password.

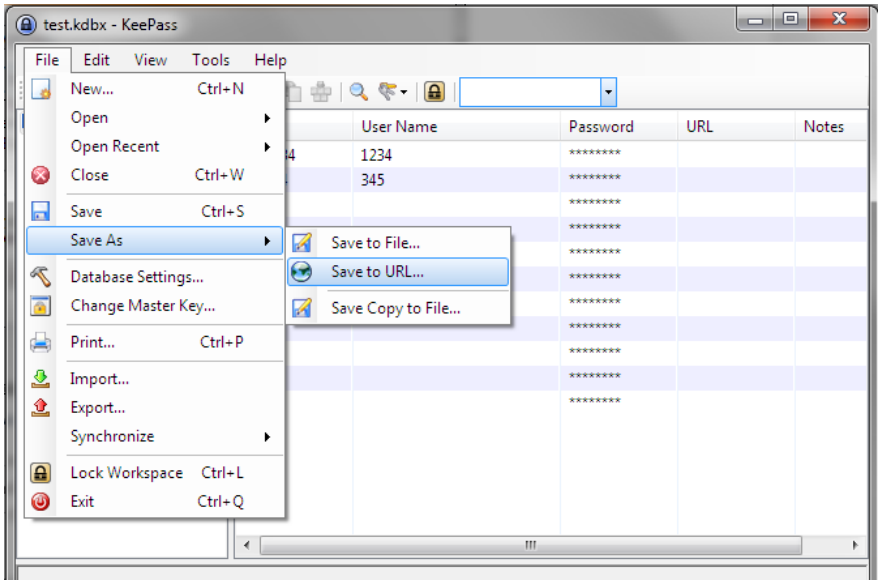


Picture 40. Opening the password file in KeyPass application

NOTE! *So that your password file would open in KeyPass application, you need to enter the PIN code on the device – go to the myflak.com web interface and enter your device PIN code. Otherwise the access to the file via KeyPass will be denied.*

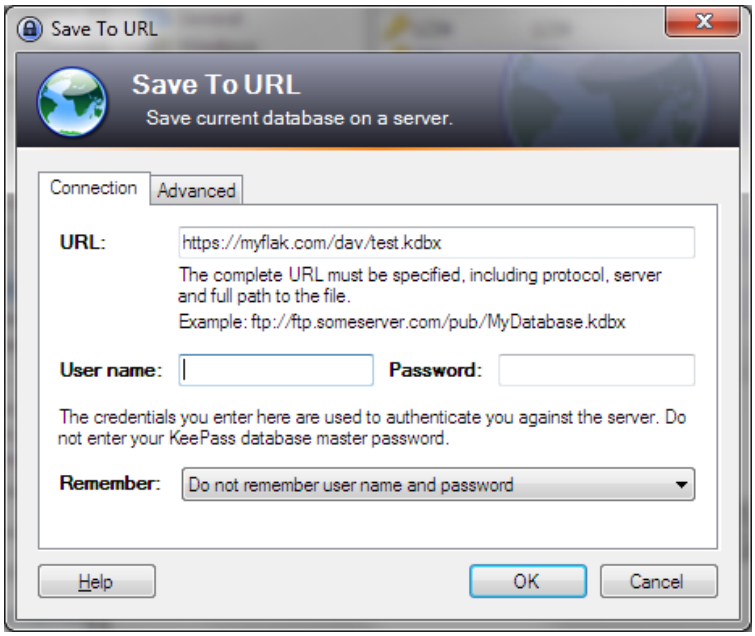
Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

After you finished editing the password file in KeyPass application you need to click on File ->Save As -> Save to URL.



Picture 41. Saving the password file to device

Enter the URL https://myflak.com/dav/test.kdbx and click on Save.



Picture 42. Saving to the device

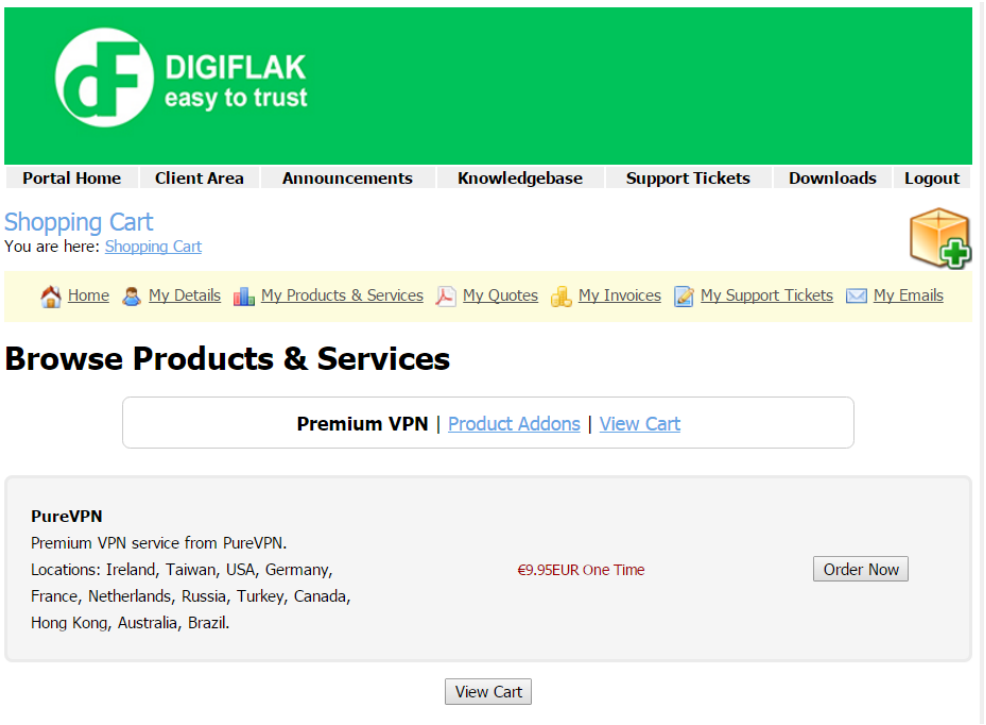
Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Flak Store

Some options are available after payment them in Flak Store (e.g. Premium VPN).
To access the Flak Store click on the Flak Store item in the Main Menu.

Picture 1. Flak Store option..

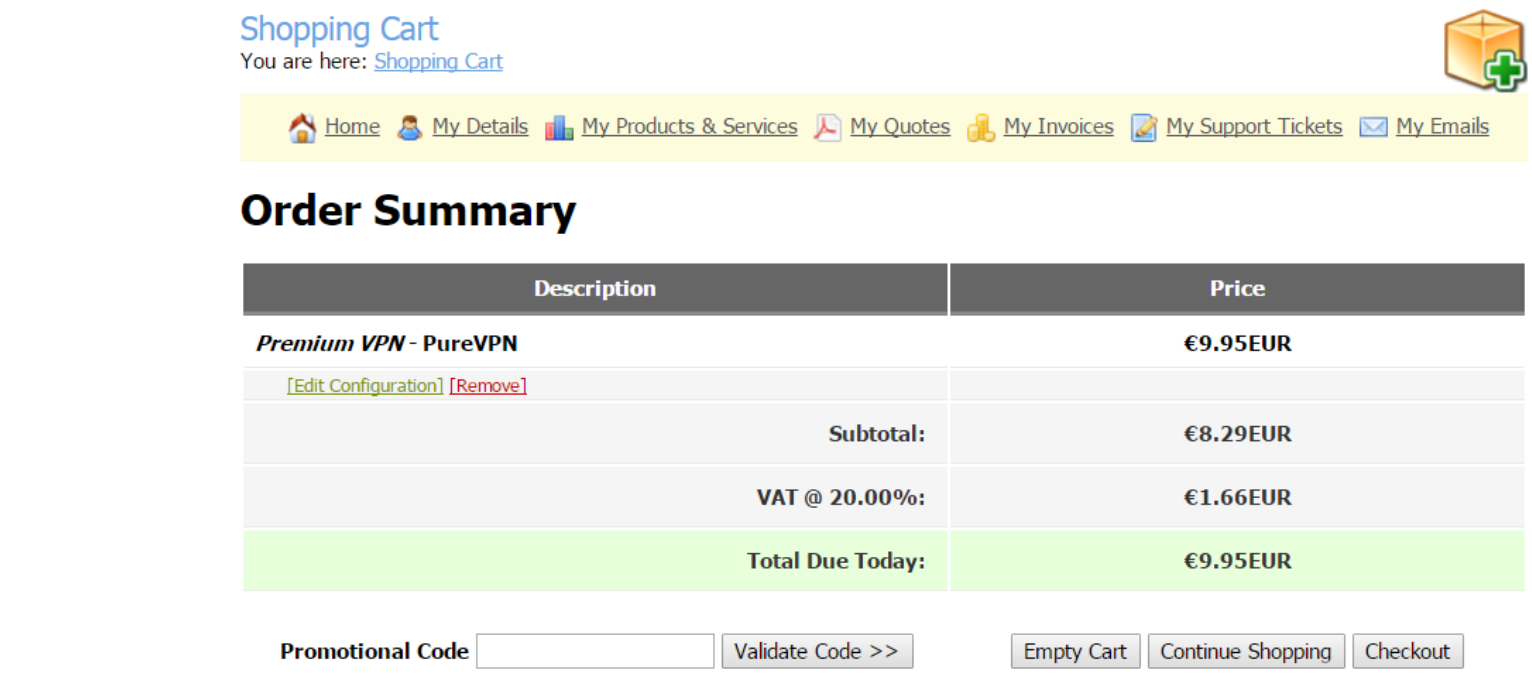
The device should be registered. Otherwise registration form opens.
Flak Store page opens if the device is registered. There are products and services, which are available for a purchase.



Picture 2. Flak Store page.

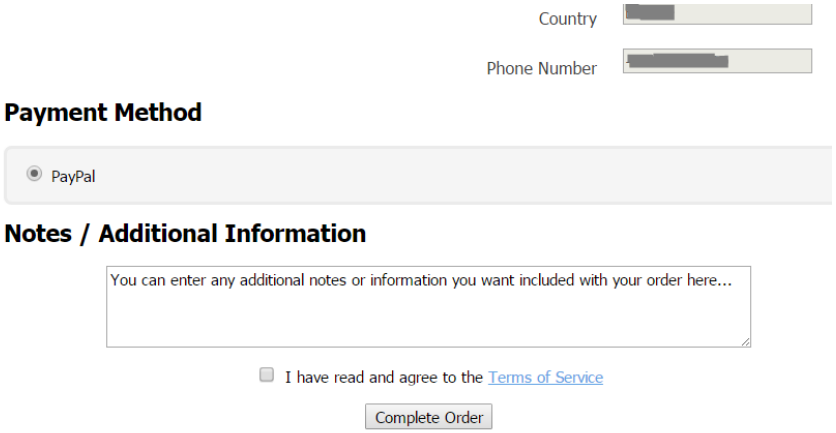
Click Order now button to buy selected product. Order page opens.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com



Picture 3. Order page.

Click Checkout to verify your data and payment way. If your data is presented correctly press Complete order button.



Picture 4. Complete order.

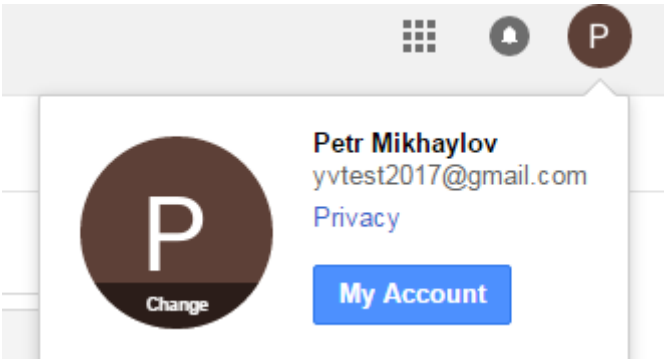
PayPal page opens. You can pay for the selected product. The product will be available in the Web-interface after the payment.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

2-step verification for Google services

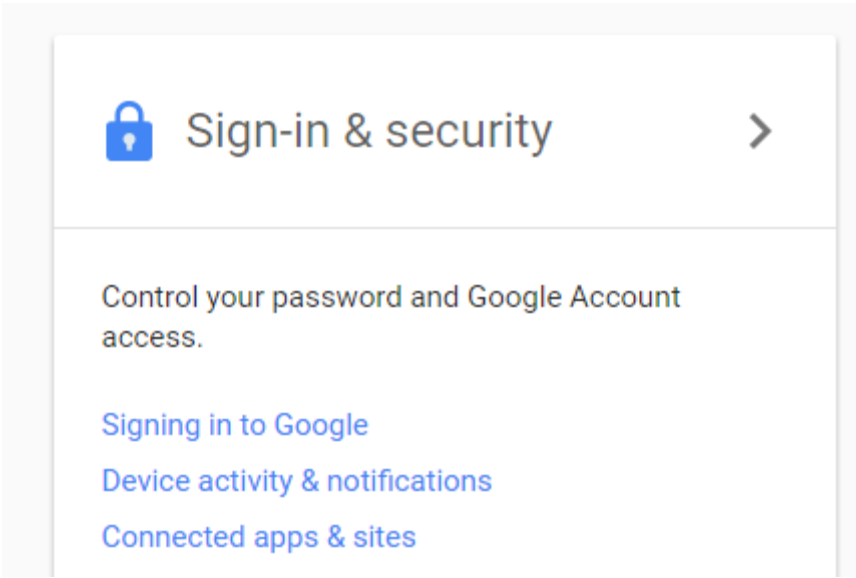
Adding Flak as security key

1. Login to your Google account.
2. Click on your user icon in the upper right corner, and then click on Account link.



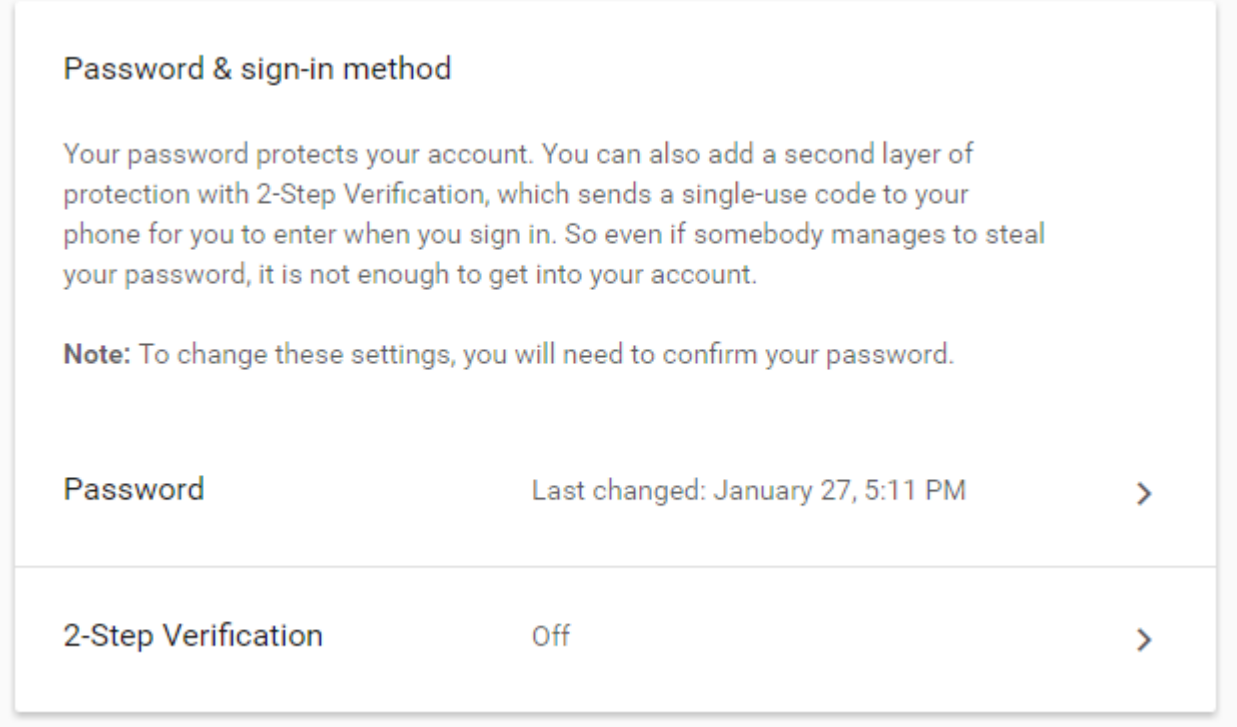
Picture 43. My Account

3. Account settings menu will be opened.
4. Select Sign-in & Security and Signing into Google.



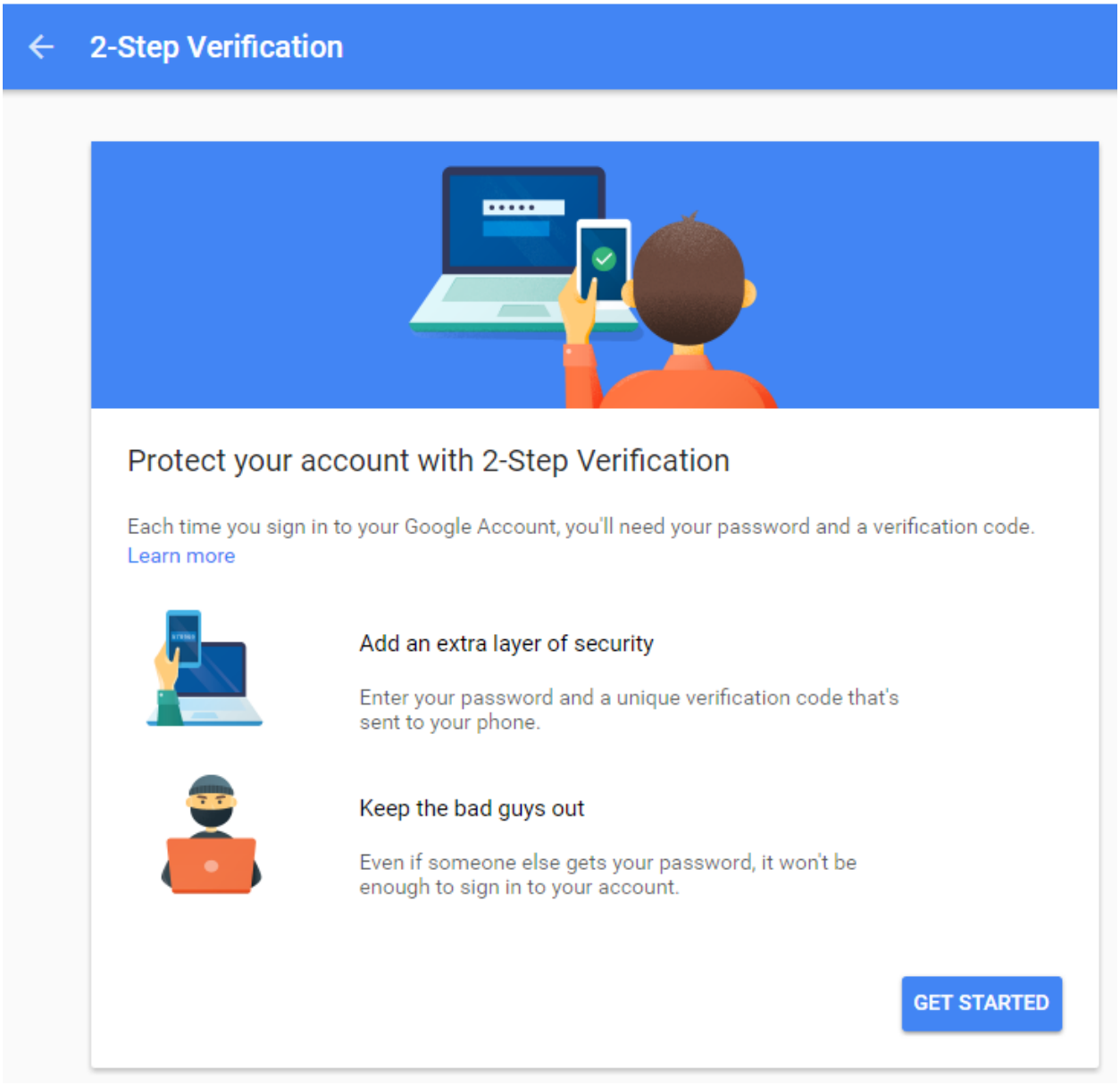
Picture 44. Sign-in & Security

5. Click on 2-step verification item in Signing in section.



Picture 45. Sing-in module in Account settings

6. Click on Start setup.

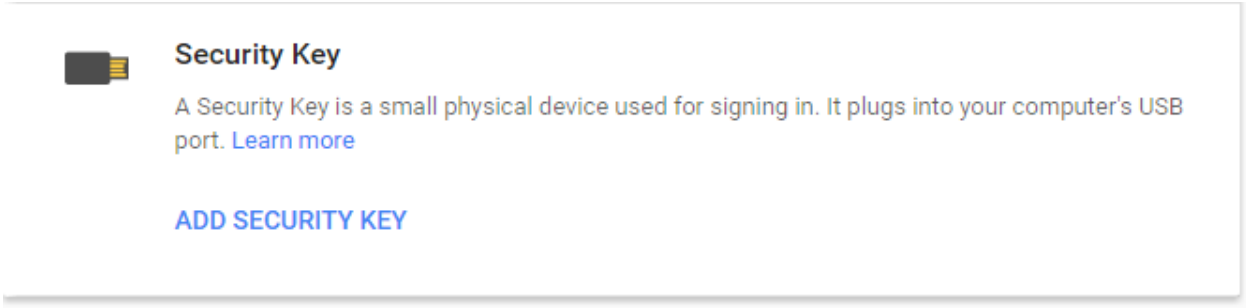


Picture 46. Signing in with 2-step verification

7. Enter your existing Google password.

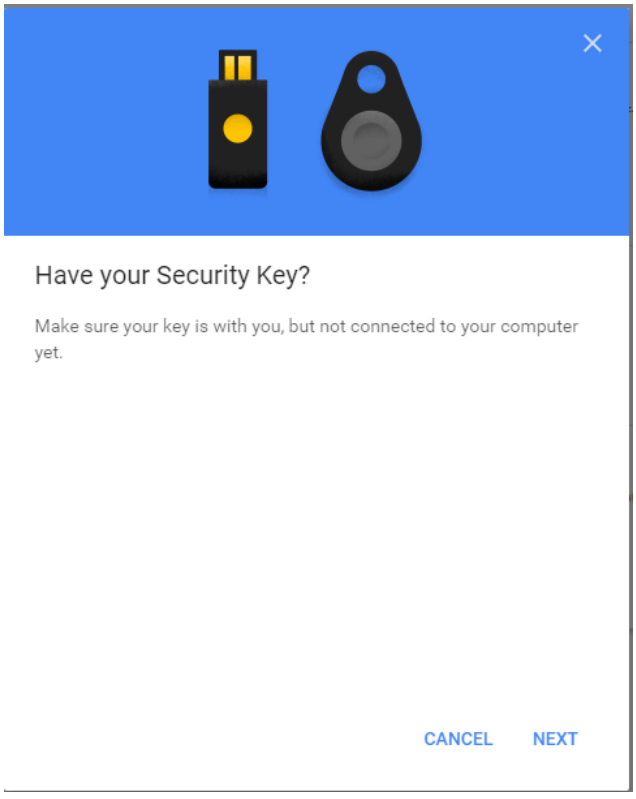
8. You would be asked to provide the mobile phone number where the text message (SMS) with the 4-digit code will be sent.

9. Enter the received 4-digit code in the form and click on Enter.
10. Click on Confirm to activate the 2-step verification.
11. Click on the tab Security Keys and then click on Add security key.



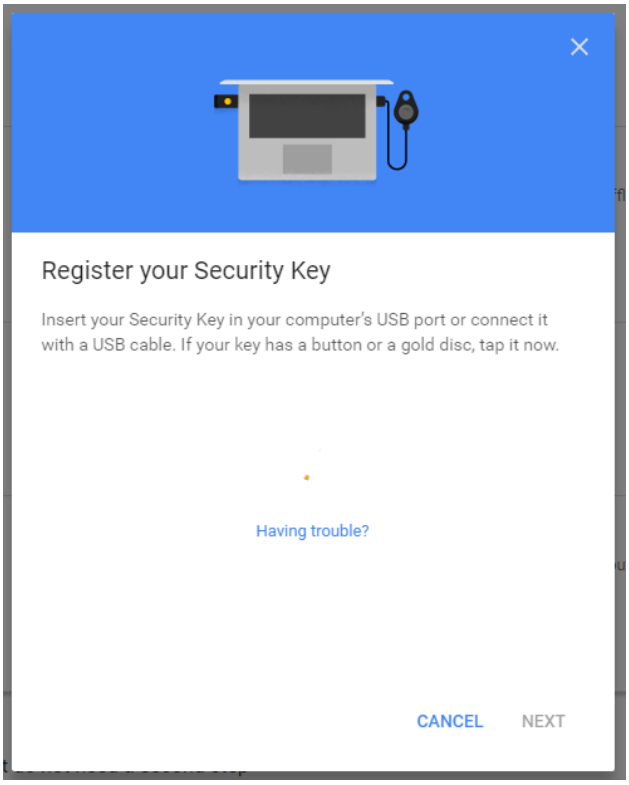
Picture 47. Security Keys

12. Follow the instructions on the screen. Make sure that device is not connected to the computer. Click on Next.



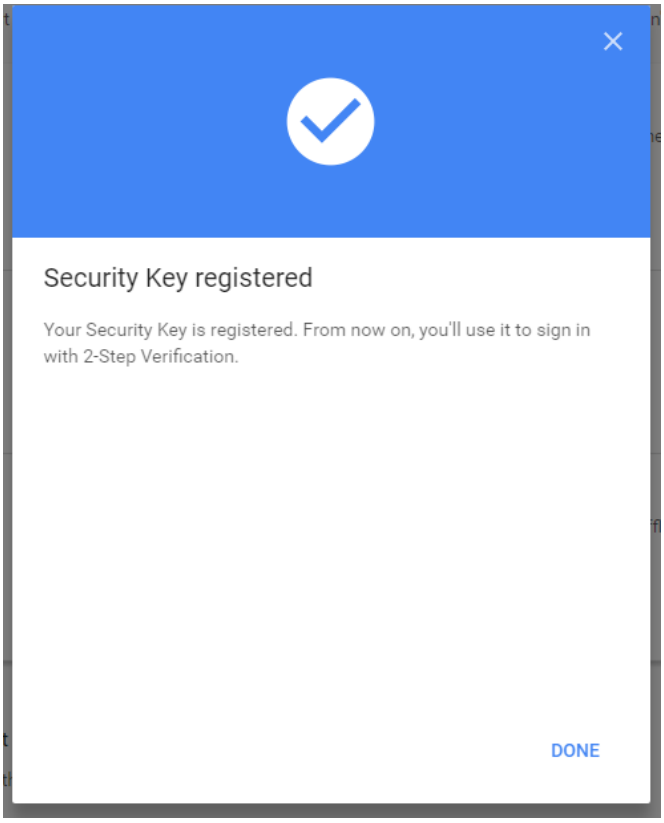
Picture 48. Adding a Security Key

13. Insert device into the USB port and wait for Flak to flash blue, white, and red colors. Slightly click on the area between USB and the logo.



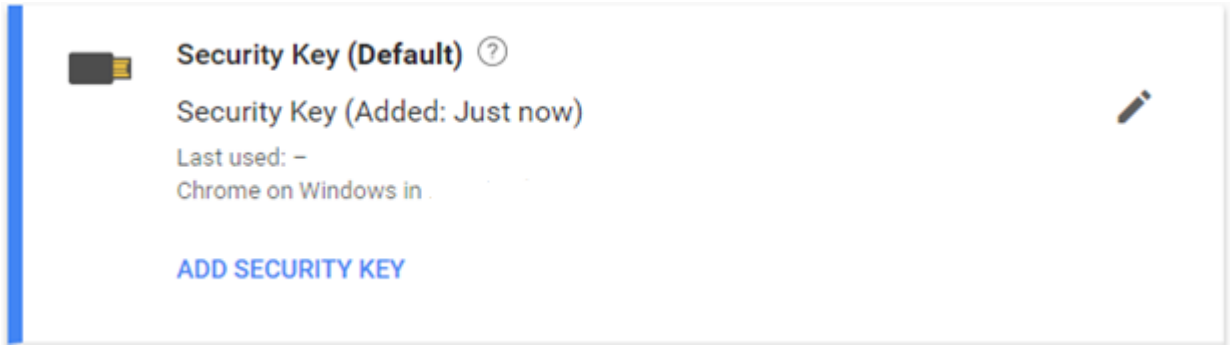
Picture 49. Security Key Registration

14. After you clicked on the device, the device will get registered as Security key in Google account.



Picture 50. Security Key registered

15. Device would appear in the list of security keys. You can add another security key.



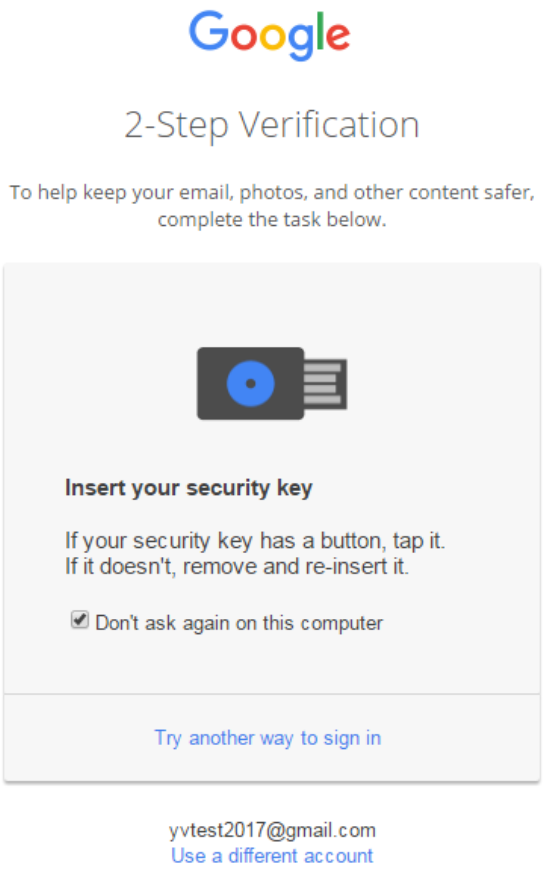
Picture 51. Security Key Added

Signing into Google with your security key

1. Open google.com. In the upper right corner click on Sign in.

2. Enter your username and password.

3. The 2-step verification window would appear. If you see the checkmark by “Don’t ask again in this computer”, then computer is going to be considered trusted and security key would not be needed. Without a checkmark next time you are going to log in to Google you would be asked to insert your security key again.



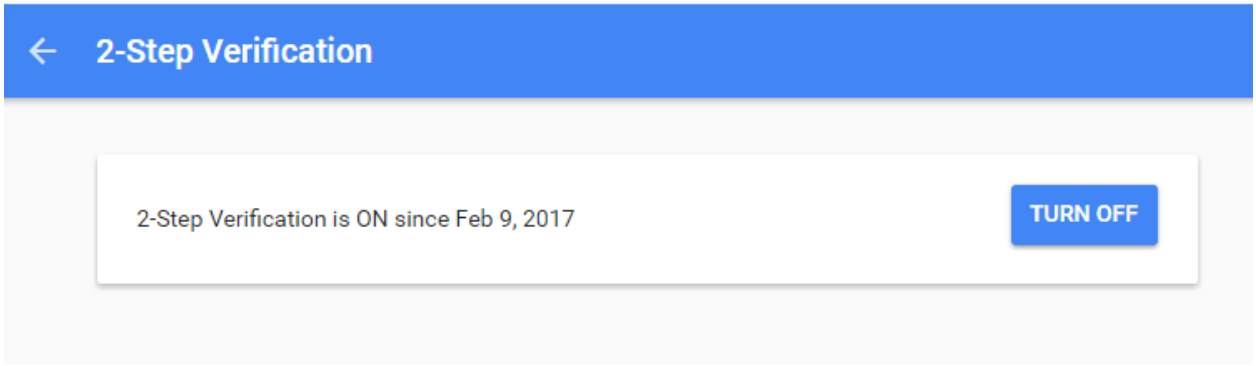
Picture 52. 2-step Verification during login

4. Wait for device to flash blue, white, and red colors, and then slightly click on the area between USB and logo to confirm signing into Google.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

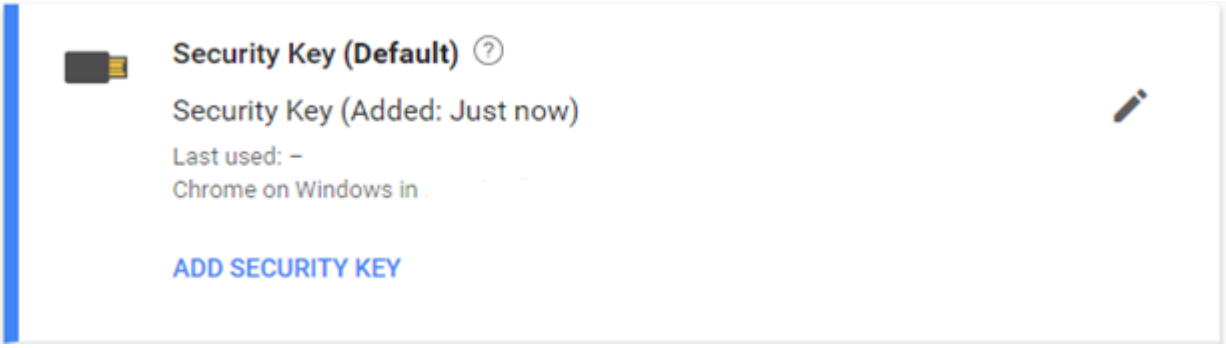
Removing a security key and disabling 2-step verification

1. To remove a security key Login to your Google account (check options 1-4 Signing into Google with your security key).
2. Click on 2-step verification item in Signing in section.
3. To disable 2-step authentication, click on 2-step verification link in the top left corner of the screen. Click on Turn off button on the right side of the screen. 2-step verification will be disabled.



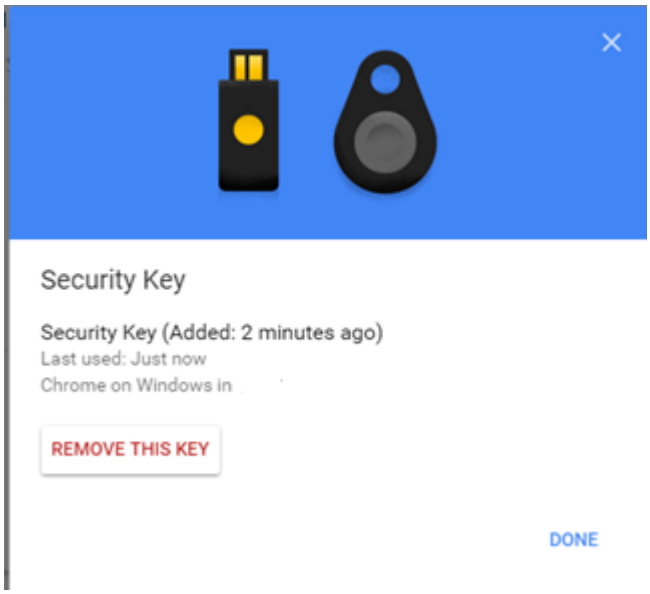
Picture 53. Disabling 2-step verification

4. To remove a security key click tab Security Keys and then on Manage button.



Picture 54. Editing a security key

5. Click on Remove This Key. The security key will be deleted.



Picture 55. Removing a Security key

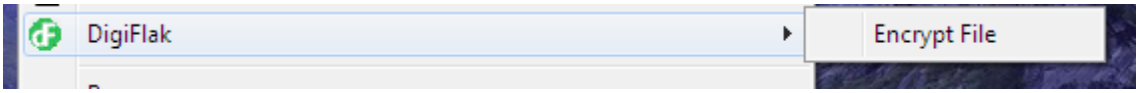
Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Files encryption on your computer

Encryption of files

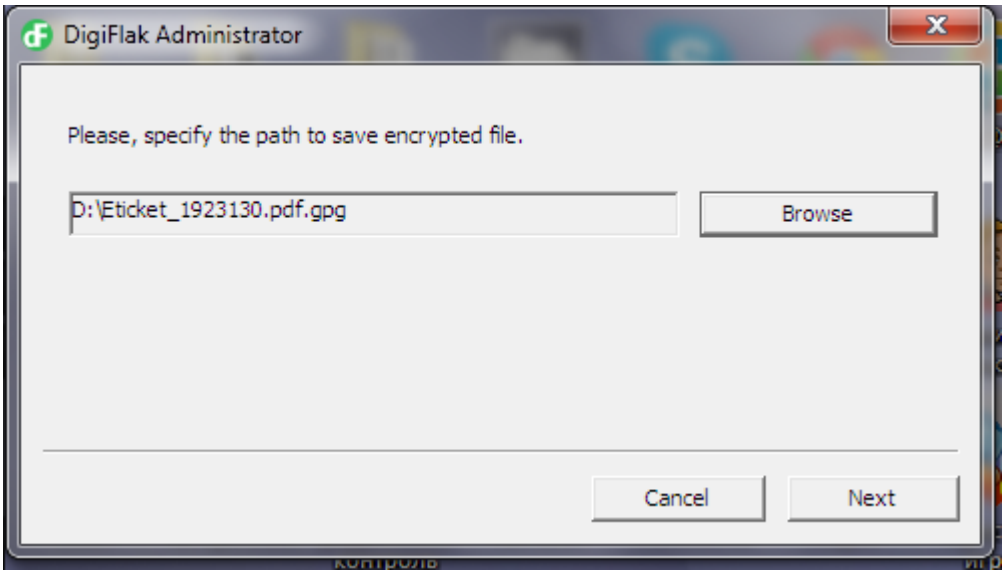
The device allows encrypting your files directly in your Windows file system. To use this function you need to register your device first (look at Registration section)

1. Insert your device into the USB port of the computer
2. Select the file to encrypt and right click on it
3. In the popup menu select DigiFlak → Encrypt file.



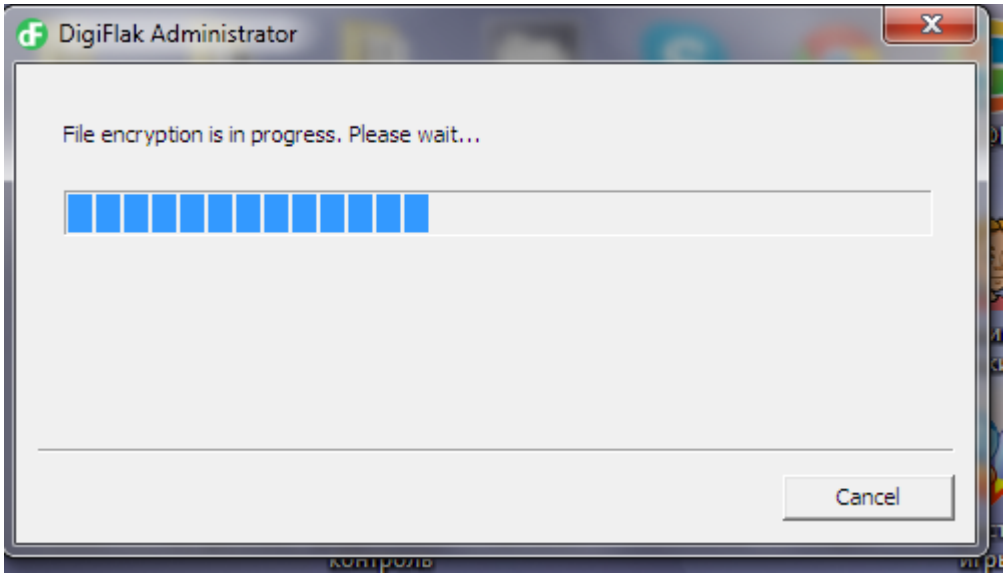
Picture 56. Encrypt file in a menu

4. In the new window type the name of the new encrypted file, click on Save and then specify the path to where to save the encrypted file. After you are done click on Next.



Picture 57. Path to the encrypted file

5. The Encryption Progress window would appear. If you want to stop the encryption prosses by clicking on Cancel.



Picture 58. File encryption process

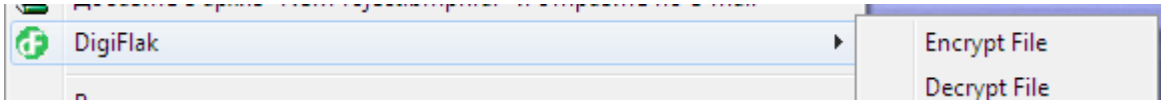
6. After the successful encryption the window with the message “File encrypted correctly” would appear. Click on Close.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Decryption of files encrypted by Flak

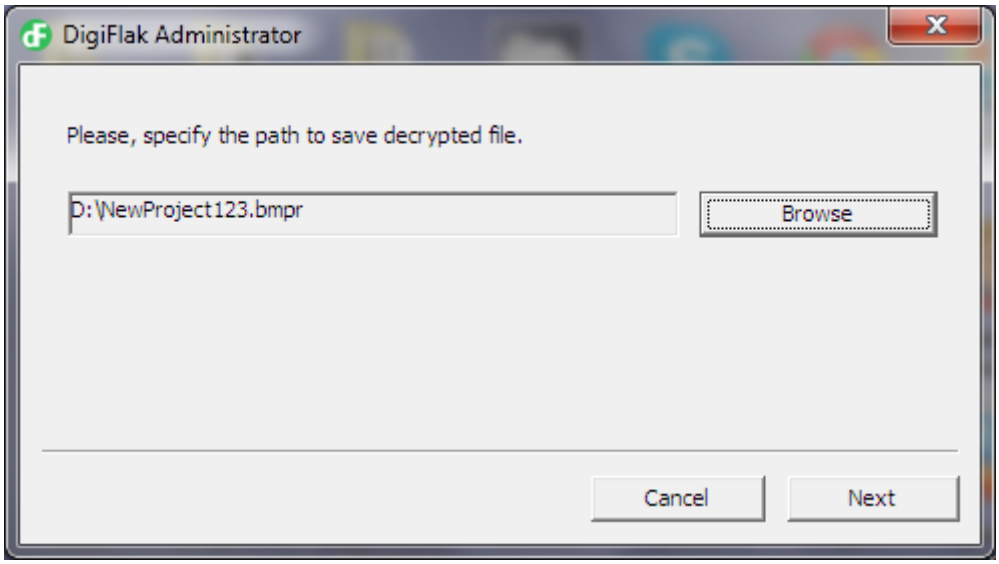
To decrypt a file encrypted by Flak follow these steps:

1. Insert the Flak with which the file was encrypted with into the USB port of the computer
2. Go to web interface myflak.com and enter the PIN code.
3. Right click on the encrypted file and in the popup menu select DigiFlak → Decrypt file



Picture 59. Decrypt File in Menu

4. In the new window type the name of decrypted file and click on Save.
5. Choose the path for the decrypted file and click on Next.



Picture 60. Path to save the decrypted file

6. The decryption process would start. After the successful decryption the decrypted file would appear in the specified path.

Vilmsi 5 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

Declaration of Conformity

J. Vilmsi 5-307 Tallinn
10126 Estonia
www.digiflak.com
+372 600 29 89
info@digiflak.com

DECLARATION OF CONFORMITY (DoC)

We, **DigiFlak OÜ**
Vilmsi 5-307
10126 Tallinn Estonia

As a manufacturer and represenative in EU, Asia, Americas and Africa declare under our sole responsibility that the product listed below

Product:	**FLAK**
Model:	**FLAK Classic**
Trademark:	**DigiFlak**

Complies with the essential requirements, which are specified in the directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility and ROHS directive 2011/65/EU, if used for its intended use and that the following harmonized standard has been applied:

Electromagnetic compatibility (EMC Directive 2004/108/EC)

EN 55022:2010
EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-3-3: 2013
EN 55024:2010
EN 61000-4-2: 2009, EN 61000-4-3: 2006+A1:2008+A2:2010
EN 61000-4-4: 2012, EN 61000-4-5:2006
EN 61000-4-6: 2014, EN 61000-4-8: 2010, EN 61000-4-11: 2004

RoHS directive 2011/65/EU

EPA3050B:1996, EN1122B:2001
EPA3052:1996, EPA3060A:1996
EPA7196A:1992, EPA3540C:1996
EPA8270D:2007, IEC6231-1:2014

Authorized Signature:
Name: Victor Samsonov
Title: CEO

Place, Declaration creation date: Tallinn, Estonia, October 14th, 2014

DigiFlak
2014