# Hideez Key 2

ST102

# USER MANUAL

Version 1.3.4

Firmware 1.2
Hideez Safe for Windows 1.10
Hideez Safe for Android 2.5
Hideez Safe for iOS 1.0
Hideez Safe for Mac 1.2

© Hideez Group Inc, 2018

# Table of Contents


Table of Contents 2

1. General Information 4

1.1. Compliance Statement 4

1.2. Environmental Protection 4

1.3. Responsibility 4

1.4. Changes 4

1.5. Trademarks 4

1.6. Updates and Patches 4

1.7. Safety Precautions 4

2. Technical Specifications 5

3. System Requirements 5

4. Manufacturer Warranty 6

5. Compliance to Standards 6

5.1. Declaration of conformity to requirements of the Federal commission on communication (FCC) 6

5.2. Statement of observance of FCC with respect to the influence of radiation 6

6. Purpose of Hideez Key 2 ST102 6

7. Principles of operation 7

8. Getting Started 7

8.1. Device Layout 7

8.2. Battery changing 8

8.3. Are my devices compatible with Hideez Key? 9

8.4. Hideez Key 2 ST102 states and control menu 9

**8.5.** Installation of Hideez Safe Software 10

8.6. Registering of My Hideez account 10

8.7. Hideez Key 2 ST102 pairing and Initialization 11

8.8. Pairing With a New Device 12

8.9. Support of Constant Connection 12

8.10. Switching Between Paired Devices 13

8.11. Shutdown and Deleting of Personal Data in Hideez Key 13

8.12. Hideez Safe Application Update 13

8.13. Updating Hideez Key 2 ST102 firmware 13

8.14. Updating the firmware from bootloader mode 14

9. Hideez Key 2 ST102 Operation 15

9.1. Control of access to a PC 15

9.2. Setting up 'My Places' for Android 15
9.3. Protection of Windows PC 15
9.4. Password Manager 17
9.4.1. Working with Passwords in Android and iOS 17
Adding passwords 18
Assigning an existing password to the Android application. 18
Using passwords in iOS 19
Using passwords in Android 19
Changing or removing items in password manager 20
9.4.2. Password Manager in Windows system 20
Add and enter passwords in web browsers 20
Automatic Password Generation 21
Changing Password 21
Adding and Entering Passwords in Desktop Applications 21
Adding Passwords manually 22
Choosing from Several Suitable Accounts 22
Import passwords from CSV-file 22
Using the Default Password 23
Setting Hotkeys 23
Removing Records from the Password Manager 23
9.5. One-time Passwords (OTP) and Two-Factor Authentication 24
9.6. Backup and Recovery of the User Data 25
9.7. Protection and Search of Hideez Key2 ST102 25
9.7.1. How to find key fob with your smartphone 26
9.7.2. Track with Google Maps 27
9.8. Biometric Authentication of Android user 27
9.9. Using of RFID-sensor 27
9.10. Touch guard (Android only) 27
9.11. Remote Control of Android phone, Windows, Mac 27
10. Web-service my.hideez.com 28
Annex 1. Troubleshooting 29
Annex 2. Safety Precautions 30
Annex 3. Hideez Key 2 ST102 Signals and States 31
Annex 4. Frequently Asked Questions 32

# 1. General Information

## 1.1. Compliance Statement

Hideez Group Inc. Company declares that this product meets the main requirements and other provisions of 199/5/WE.

## 1.2. Environmental Protection

This device conforms to the requirements of directive WEEE 2002/96/EC. The symbol on the bottom of the device means that the product should be used as directed and then disposed of properly. This allows for less environmental pollution and health impact.

## 1.3. Responsibility

Hideez Group Inc Company and its licensors don't bear any responsibility for the loss of data, information, profit or other indirect losses due to the use of our equipment as far as the law permits.

Hideez Group Inc Company doesn't bear any responsibility for any problems resulting from improper operation with any operating system and the programs under its control.

## 1.4. Changes

Hideez Group Inc Company reserves the right to change this document or aspects without prior notice. Functionality and images may vary depending on the services and version of the installed software. The screenshots in the document may not coincide with the real device. The appearance of devices may differ from samples.

## 1.5. Trademarks

© Hideez is a registered trademark of Hideez Group Inc. Bluetooth is a registered trademark of Bluetooth SIG. Microsoft® Windows ™ is a registered trademark of Microsoft Corporation. Google, Android and YouTube are registered trademarks of Google Inc. All other products, trademarks and brands that are mentioned are the property of their respective owners.

## 1.6. Updates and Patches

The latest version of the software and User Guide can be found online: www.hideez.com/download.

Online versions of the User License Agreement can be found at: www.hideez.com/legal

## 1.7. Safety Precautions

Please read this section before using the device. The following tips are given to ensure long term operation of the product and to prevent malfunction.

Do not expose the device to extremely high or low temperatures. Protect it from direct sunlight. The internal battery of the device should not be exposed to extremely high or low temperatures. Note: the operating temperature of the device is from -10 ° C to 40 ° C.

Do not expose the device to open fire or smoke (cigarettes, lighters, fire, etc.).

Do not expose the device to strong electromagnetic fields.

Do not drop or bend the device. If the device is damaged, please contact the service center.

Do not use the device underwater. If the device is exposed to water, open the case, remove the battery and contact the service center.

The device receives and emits radio frequency according to Bluetooth 4.0 compatible specifications. It does not need to be turned off in an aircraft, according to an FAA press-release from 10.31.2013. If you use personal medical devices (e.g. pacemakers and hearing aids), consult your doctor or the manufacturer about compatibility.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Keep the device away from children.

## 2. Technical Specifications

| | |
|---|---|
| CPU | Nordic nRF52 |
| Radio | Bluetooth 4.2 Low Energy |
| Battery | One battery CR2032 |
| Battery life-cycle | up 6 months |
| Dimensions | 32,5 x 32,5 x 9,5 mm |
| Weight | 8 grams |
| Operating temperature | -10 °C — +40°C |
| Button | 1 multifunctional |
| LED | 1 (RGB) |
| RFID | 125 kHz, HID and Em-Marine standard |
| Volume of user's memory | 76 Kb |
| Sound | 70 db buzzer |
| One-time passwords (OTP) | RFC 6238 |
| Encryption | AES-128, RSA-1024, ECC |

## 3. System Requirements

Hideez Key 2 ST102 is designed for devices that meet the following requirements:

- Android 4.4 and higher
- iOS 9.3 and higher
- Windows 7, 8* (with an external Bluetooth adapter), 8.1 and higher
- MacOS 10.11 and higher

The device must be equipped with a **Bluetooth 4.0** or higher compatible adapter supporting Low Energy (Bluetooth Smart) mode. See Are my devices compatible with Hideez Key?

* Windows operating systems before version 8.1 may not work correctly with Bluetooth 4.0 compatible devices. To work on such systems, you have to use an external USB Bluetooth adapter based on the CSR 8510 chip. Hideez recommends Hideez Dongle. Hideez cannot guarantee the correct operating using unapproved Bluetooth adapters.

Function of biometric authentication (fingerprint recognition) - TouchID works only on the Android operating system. This function can be used both to access the program Hideez Safe, and to enter the Android device itself.Hideez Safe for **Windows** works with the latest versions of the most popular Internet browsers - **Chrome, Firefox, Opera, Internet Explorer** and **Edge**. In these browsers, Hideez Safe determines the site domain name from the current browser tab and uses it to select the appropriate passwords.

The system will work like a typical desktop application with other browsers, displaying the window caption instead of the domain address.

In Android, Hideez Safe can enter passwords into applications and Web-pages. It works for most of apps as well as for **Chrome, Opera** and **Javelin** browsers. Other browsers are not supported because they do not provide access to the input elements on webpages. For other applications, automatic access depends on the implementation of the application itself. If the password does not work with some apps, contact our support service with detailed information, including the app name and version. Developers will be able to add support for these apps in future versions of Hideez Safe.

Hideez Safe for iOS works with Safari and can't enter passwords into Apps.

Hideez Safe for Mac works with Safari and Chrome browsers and native Mac applications

The RFID Module works with HID and Em-Marine standards. The RFID Module is not compatible with NFC modules that are installed in smartphones and tablets.

**Note**: Hideez Key 2 ST102 and Hideez Safe software is being constantly improved. The list of supported operating systems will be expanded. Please check back for future updates.

# 4. Manufacturer Warranty

The warranty period is 12 months from the purchase date under normal use conditions.

# 5. Compliance to Standards

## 5.1. Declaration of conformity to requirements of the Federal commission on communication (FCC)

This device complies with part 15 of the FCC rules. The following conditions should be taken into account while using the device: (1) this device cannot be the source of adverse effects; (2) this device may receive interference signals, including those that can cause it to malfunction.

## 5.2. Statement of observance of FCC with respect to the influence of radiation

This equipment complies with FCC standards for RF energy in an uncontrolled environment. The transmitter must not be located near any other antenna or transmitter and will not receive their signals.

# 6. Purpose of Hideez Key 2 ST102

Electronic key Hideez Key 2 ST102 (tag) is designed to authenticate users on electronic devices, such as PCs, tablets and smartphones; storing encryption keys, passwords, logins and other personal data; performing encryption, hashing and electronic signature operations; generating one-time passwords (OTP); and identifying users using the RFID protocol (125 kHz HID and Em-Marine standards).

Hideez Key 2 ST102 requires the installation of the Hideez Safe software. Using Hideez Key 2 ST102 along with Hideez Safe allows users to perform the following operations:

- Lock/unlock access to a PC, smartphone or tablet based on an estimation of distance using the radio-signal indicator for the Bluetooth signal (RSSI).
- Store user credentials for various programs and web-services.
- Generate one-time passwords for services that use two-factor authentication specification RFC 6238, such as Google, Microsoft, Dropbox and Facebook.
- Perform encryption operations and electronic signatures according to the AES-128, RSA-1024 and ECC standards inside Hideez Key.
- Update Hideez Key 2 ST102 firmware using a Bluetooth channel.
- Using Hideez Key 2 ST102 on an Android smartphone/tablet can also perform the following operations:
- Avoid the loss of the Hideez Key 2 ST102 and valuables where it has been attached, by the control of the Bluetooth connection.
- Take pictures of violators if someone attempts to access the smartphone without the Hideez Key 2 ST102 presence.
- Pressing the button can perform various pre-programmed actions and their sequence (scripts), such as turning on audio and video recording, sending an SMS, initializing phone calls, turning on audio signals, the flashlight and taking photos.
- Send the current geographic position to a preset phone number ("panic button" mode).
- Remember and display geolocation data about where the connection with the tag was lost on a smartphone.

**Note**: The Hideez Key 2 ST102 and Hideez Safe software are constantly being improved. Please, keep your software and firmware updated.

## 7. Principles of operation

Hideez Key 2 ST102 interacts with other electronic devices via radio frequency signals specified by Bluetooth 4.0 compatible Low Energy standard on the 2.4 GHz frequency bandwidth.

This standard requires minimum power consumption and uses data encryption during transmission.

The stable connection distance can reach up to 100 meters outdoors without obstacles, or up to 25 meters indoors. The actual signal strength and range of the connection depends on the surrounding obstacles, including human bodies, that can influence the operating range and performance of certain functions.

Hideez Key 2 ST102 can approximately measure the distance to its paired devices using the received signal strength indication (RSSI). This feature is the basis of most security and signaling functions.

Hideez Key 2 ST102 is also equipped with RFID module that works on the 125 kHz frequency bandwidth. You can learn more about RFID in the section “Using of RFID”.

Operating Hideez Key 2 ST102 with Bluetooth requires the Hideez Safe software installation on a paired device. A detailed manual of the installation process can be found below. Using the RFID features does not require any additional software.

**Notice**: Some devices require turning off their energy saving features to provide correct Bluetooth operation. It is because energy saving mode may turn off Bluetooth and block the execution of background services.

# 8. Getting Started

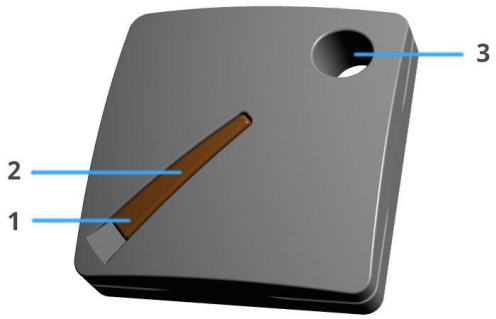
## 8.1. Device Layout

Hideez Key 2 ST102 is a key fob with a single multifunctional button. Two LED indicators (green and red) are located under the button.

A sound element (buzzer) for audible signals and alarms, is located inside the case.

The Bluetooth antenna is located on the main circuit board.

The RFID antenna with the control unit can be found under the top cover. This module is not connected to the main board.

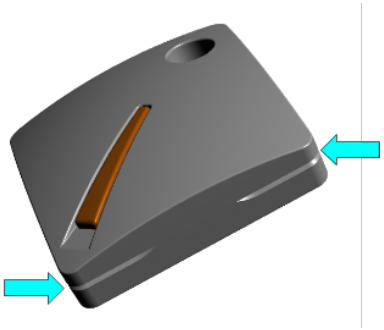



Exterior

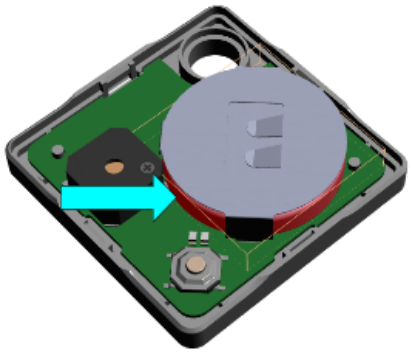
1. Multifunctional button
2. Green and red LED indicators
3. Keychain hole

## 8.2. Battery changing

Hideez Key 2 ST102 comes with a pre-installed battery. The case is made of two halves latched together. To replace the battery, open the case and lift the gap between the halves with a fingernail or a plastic card. Do not use metal objects. Remove the old battery by pushing it from the inside using a narrow plastic object. Install the new CR2032 battery on the narrow side (minus contact) of the board. Hideez Key 2 ST102 will beep and start to work.



Opening the case



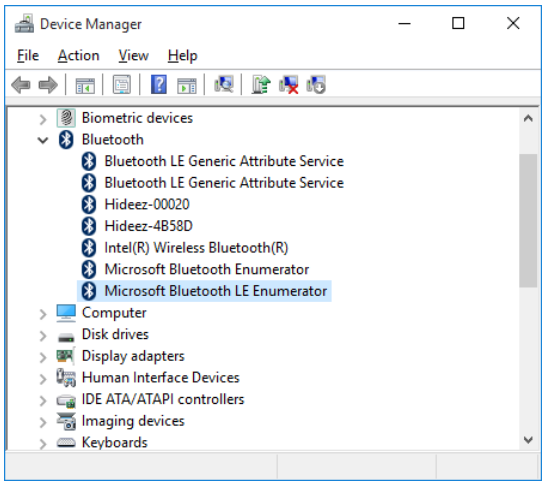
Change the battery

**Notice**: if you don't want to change the battery by yourself, you can contact any electronic service center which replaces watch batteries.

## 8.3. Are my devices compatible with Hideez Key?

Before purchasing Hideez Key, you need to check whether your smartphone, PC or tablet can work with it.

On **Windows** PC**,** go to the Device Manager, find Bluetooth section and make sure that there is an element called Microsoft Bluetooth LE Enumerator




If there is no Microsoft Bluetooth LE Enumerator in your system, it means it does not support Low Energy mode. If there is no Bluetooth section, it means the Bluetooth adapter has not been installed yet. You can purchase an external USB Bluetooth adapter in either case. (Hideez Smart Bluetooth dongle is recommended). Note, that some Bluetooth adapters declare Low Energy mode supporting, but in fact, they only work with their own software. Windows does not recognize these devices as Bluetooth Low Energy adapters (Bluetooth LE Enumerator is not appearing in the device list). Hideez Safe doesn't work in these cases.

For **Android**-based systems, you can download Bluetooth testing software e.g. BLE Checker from Google Play. Your system is supported if you see the "BLE Supported".

## 8.4. Hideez Key 2 ST102 states and control menu

There are three modes of the Hideez Key 2 ST102

**Mode 1 (connected)**

Hideez Key 2 ST102 is connected to a host device (Windows, Android) via Bluetooth.

A green LED is flashing every 4 seconds.
Red LED flashing every 4 seconds means the battery should be changed.

**Mode 2 (not connected)**

There are two options:

a) The device is advertising for previously paired devices, inviting to connect.

b) The device is advertising for any Bluetooth devices. This option shows that Hideez Key 2 ST102 can be visible and paired by each of them.

**Mode 3 (power off)**

Pressing Hideez Key 2 ST102 button can perform the following operations:

**Mode 1 (connected)**

- one to eight short presses sends an appropriate event to the connected host device (PC or smartphone). Hideez Safe app handles this event and executes a preset action.
- Long press (2-4 sec) disconnects Hideez Key 2 ST102 from the current host device and connects to the next one from the paired devices list. If there are no paired devices near here, Hideez Key 2 ST102 will restore connection with the previous device after 30 seconds.
- 9+ short pressings open Hideez Key 2 ST102 system menu. Green LED is constantly on. In this mode, short button pressing means:
  - 3 times- removing of current connection parameters set (bond) and disconnect from host device.
  - 4 times– the device beeps as many times, as the number of paring devices in the list. It is used for debugging purposes.
  - 5 times calls bootloader mode.
- Long press (10 seconds) turns power off.

**Mode 2 (not connected)**

- Short pressing turns power on and makes the device available to connection.
- 9+ short pressings open Hideez Key 2 ST102 system menu, as described above. The only difference is that:
- 3 short pressings remove not only current connection parameter set, but all the connection sets and pairing devices from list.
- Long press (10 seconds) turns power off.

**Mode 3 (power off)**

- Short pressing turns power on and makes the device to advertise.
- Long pressing (10 seconds) calls bootloader mode.

## 8.5. Installation of Hideez Safe Software

**For Android and iOS:** Install Hideez Safe from Google Play. or AppStore. An icon will appear on the screen, along with a notification about launching Hideez Safe.

For **Windows** or **Mac:** download the installation package of Hideez Safe from the web-site http://hideez.com/download, then launch it and follow the installation wizard instructions. You need administrator rights to do the installation.

Hideez Safe automatically downloads and installs updates from Hideez.com. Some antivirus and firewall software might flag or block this functionality. If your antivirus doesn't allow you to install Hideez Safe, turning it off before installation and then turn on again.

An icon will appear on your system tray after the installation. Click the icon to open the Hideez Safe main window.

Hideez Safe will be automatically launched after reboot.

## 8.6. Registering of My Hideez account

Hideez system is a crucial component of user's information infrastructure. It provides wireless user authentication, is a wireless hardware password manager tool, a one-time password generator, as well as an encryption and electronic signature tool. An important component of the protection system is the My Hideez cloud service. Please note that My Hideez does not store any user credentials. It is only used for Hideez Key 2 ST102 hardware devices verification, firmware, application software, providing encrypted data channels, etc.

More information about security functions can be found in the Hideez Security White Paper.

To start using the Hideez Key, the user should register it with a my.hideez.com account. After that Hideez Key 2 ST102 will not need Internet access. Registration prevents the Hideez Key 2 ST102 from unauthorized connection to any other PC/smartphones without the user account password. Watch the video of the user registration on youtube.com/hideez.

The user should specify a login and password during the first Hideez Safe launch. If the My Hideez account has not been created yet, it can be done now. To sign up for My Hideez, please click on the 'Sign Up Now' link, enter your e-mail address and create a new password. The confirmation letter will be sent to your email. Please click on the link in this message, to complete the registration.

**Notice**: If you forget your password you can restore it through your e-mail using the my.hideez.com service. If you lose access to your e-mail, you will not be able to register and use Hideez Key 2 ST102 on new devices.

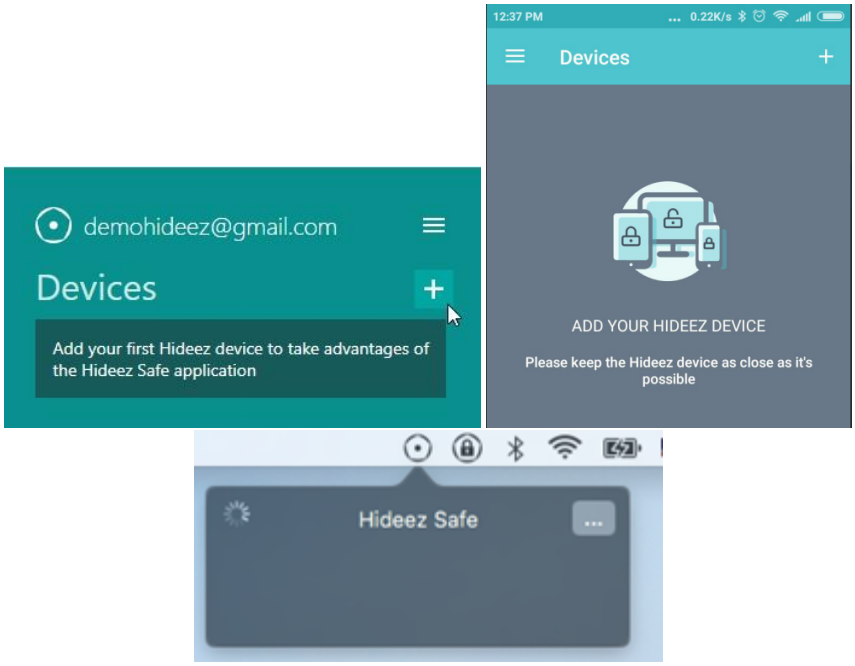
## 8.7. Hideez Key 2 ST102 pairing and Initialization

The Hideez Key 2 ST102 initialization is an exchange procedure of Bluetooth channel encryption keys, as well as a loading the user encryption key. The user's key is downloading encrypted data from My Hideez service and cannot be intercepted.

At the same time, the Bluetooth channel encryption keys can be potentially intercepted and used for further decryption of the data exchange. Therefore, this procedure should be carried out in a safe environment that restricts the chance that someone is using eavesdropping equipment. In order to minimize these risks, the power of the transmitter is reduced during of the connection initialization. That is why Hideez Key 2 ST102 should be placed as close as possible to the PC / phone. The channel will be encrypted and protected from interception after the initialization is finished.

Since the Hideez Key 2 ST102 initialization procedure uses a web service, it requires an Internet connection. After the initialization is finished, the work without an Internet connection is possible.

Click [ + ] (adding new devices) in the main window of Hideez Safe.




Then press the key fob's button. The device turns on for 60 seconds and becomes visible for Bluetooth connection (a LED-indicator flashes green slowly).

Hideez Key 2 ST102 is seen as Hideez-XXXXX in the Bluetooth environment of your cell phone or PC, where XXXXX are the last digits of its serial number.

After detecting the Hideez Key, please click it in the list and follow installation wizard instructions. Your My Hideez credentials will be asked during one of these steps.

If the registration doesn't finish successfully for any reason, the key fob will turn off in 60 seconds. You will need to remove the Hideez Key 2 ST102 from the device list and repeat the procedure over again.

When the registration is finished, the device will stay turned on permanently. The battery should work up to 6 months, depending on the amount of use and the battery quality. The highest energy consumption occurs when the audio signal is used.

## 8.8. Pairing With a New Device

When Bluetooth communication is established between two Bluetooth devices, one of them is a host and another – a client. The Hideez Key 2 ST102 is usually a client, so, according to Bluetooth specification, it can be connected to only one host at the same time. Also, the Hideez Key 2 ST102 is invisible to other devices when it is connected.

To create a new Bluetooth connection, the Hideez Key 2 ST102 has to be disconnected from any hosts. To do that, simply place the currently connected device outside the signal range or switch off its Bluetooth module. The new Bluetooth connection procedure is the same as described above.

Although it is possible to maintain only one active connection, Hideez Key 2 ST102 can store the list of connection parameters set for up to 8 devices and can switch between them. When a 9th device is connected, the oldest one is removed from the device list.

## 8.9. Support of Constant Connection

Hideez Key 2 ST102 is designed for non-stop connection with the host-device. If the connection is broken because the devices are out of range, it will be restored automatically when they are close enough. If the key fob paired device list has more than one device, it will connect to the first one it can find.

The host device (phone or PC) have to scan the Bluetooth channel from time to time to detect the Hideez Key2 ST102. Scanning cannot be performed constantly for several reasons:

- The Bluetooth scanning antenna cannot be used to communicate with other Bluetooth devices during the scanning process.
- Scanning requires a lot of energy that may negatively affect the operating time of the battery.
- Some Bluetooth adapters are combined with Wi-Fi adapters and use the same antenna for both protocols. During scanning, the Bluetooth antenna cannot be used for data transmission by Wi-Fi, which can cause a decrease in data transition rates.

For these reasons the scanning time should be minimized.

The Hideez Safe scanning algorithm constantly adjusts according to usage and the length of time since the last connection was lost. However, there can be a delay of 10-15 seconds to connect the key fob.

**Notice:** Bluetooth adapter drivers do not always work properly. With intensive use, especially when they need to reconnect frequently to different devices, the adapter can go down. In these cases, Bluetooth connection and scanning are impossible. Software reset of the Bluetooth adapter may help. It may also be necessary to restart a PC.

## 8.10. Switching Between Paired Devices

Hideez Key 2 ST102 can switch between Paired Devices. To do this, press and hold the multifunctional button for 2-4 seconds. Hideez Key 2 ST102 will disconnect from the current device and will start advertising for other devices from its list. The first device which finds Hideez Key, will connect it.

If these devices do not respond, or only one device is present in the list, Hideez Key 2 ST102 will connect to the previous device again.

Switching between devices can take up to 10 seconds for the reasons described in the previous section.

## 8.11. Shutdown and Deleting of Personal Data in Hideez Key

If you need to give Hideez Key 2 ST102 out to another person, you need to perform the command "Remove from account" first. This command deletes all the user data (including credentials and encryption keys) from the device. After that, the key fob is clean and can be connected to another account.

This command requires an Internet connection. You will be asked to enter the password from your Hideez account while deleting the data.

If you gave the key fob to another person, but forgot to remove it from your account, a new user will receive the error message "The device is registered to another user." This person will not be able to initialize or read data from Hideez Key. In this case, you can remove the Hideez Key 2 ST102 from your account remotely with my.hideez.com service. When the device is removed from the server list, the Hideez Safe on the new user's phone / PC will make a complete reset of the key fob. After that, the Hideez Key 2 ST102 can be used by the new owner.

**Notice**: If you lost your key fob, do not delete it from your account. No one can use it or have access to your data without your My Hideez account password. If you remove the key fob from your account, someone will be able to start using it as a new device.

## 8.12. Hideez Safe Application Update

The Hideez Safe Client software is regularly updated. New features, localizations to other languages and bug fixes are constantly improving the stability and convenience of the device.

An update of Hideez Safe app for Android or iOS are similar to any other software installed through these app markets.

Hideez Safe for PC checks for updates by itself. The user can also check for available updates on the main screen of the app. By clicking on [Update] you will start the download and installation process.

## 8.13. Updating Hideez Key 2 ST102 firmware

The Hideez Key 2 ST102 firmware is improved constantly. The user can get new features by updating the firmware via the Hideez Safe application. The availability of firmware updates is checked automatically on a regular basis. The user can also check for updates by clicking the "Check for Firmware Updates".

It is highly recommended to update the Hideez Safe application before updating the firmware.

Place the Hideez Key 2 ST102 as close as possible to a paired device for the fastest and most stable connection during the update.

The micro program consists of two components: the loader and the firmware. The loader downloads the firmware via Bluetooth and replaces the old version. The firmware contains all the working logic. The bootloader can also be updated; however, its updates are required much less often than firmware updates. To perform a firmware update, you need to:

- Connect the Hideez Key 2 ST102 to host device (PC or tablet with) Hideez Safe installed.
- Make sure Hideez Key 2 ST102 battery is charged (there is no notification of low battery).
- Connect the host device to the Internet.
- Select the item "Check for Updates" and follow the instructions on the screen in Hideez Safe program.

Upgrading the firmware from Windows is more complicated than from Android. The reason is that there are OS limits on Bluetooth connection operation by software. During the update process, the user will be asked to add / remove devices in the system window of Bluetooth settings for several times.

Please note, that it is always necessary to add or remove a device with a name that starts with "v23", e.g. "v23-Hideez-12345".

If firmware updates haven’t been installed for a long time, it might be needed to install it step by step. For example, to install the latest version of the firmware 1.1x, then latest version of 1.2x etc.

**Note**: The firmware from the Hideez site is always encrypted by Hideez private key. This prevents firmware spoofing and malicious code injection into the Hideez Key.

## 8.14. Updating the firmware from bootloader mode

If the firmware updating process fails for any reason, the Hideez Key 2 ST102 can remain in bootloader mode. A LED is illuminated constantly (the green color means the key fob is not connected, and the red one means it is connected.)

In this mode, a Hideez Key 2 ST102 is seen under the name "v23-Hideez-XXXXX", where XXXXX is the last five digits of the serial number.

Connect the key fob as usual, using the adding the new device function in Hideez Safe. This device is able to be updated or removed only. Once connected, please, check for updates and follow to the updating wizard instructions.

The most common reason for update failure is a discharged battery. In this case, replace the battery. Do not use the Wi-Fi of the paired phone or PC while update process, because Wi-Fi can affect the quality of the Bluetooth connection.

**Note:** The battery discharges much quicker in bootloader mode than in regular mode. Do not leave the key fob in this mode for a long time. If you cannot update the firmware for some reason, remove the battery and contact technical support.

# 9. Hideez Key 2 ST102 Operation

## 9.1. Control of access to a PC

There are a lot of authentication methods, such as passwords, or smart cards with PIN or biometric authentication. However, Hideez Key 2 ST102 provides one more authentication method - using the physical presence of the key fob next to a device that needs to be accessed. This is the most convenient method, but it requires Hideez Key 2 ST102 to be kept secure.

You can use the access control function for both Windows Desktop and Android-based devices.

## 9.2. Setting up 'My Places' for Android

My Places allows you to configure device settings based on the location. It is used for Touch Guard and Theft Alarm.

The program uses three location profiles: Home, Office and Street. It is possible to specify certain criteria to determine the location for home and office. The Street profile means the user is away from both home and office. Hideez Safe determines the location by GPS or by the presence of specific Wi-Fi networks. To add a new criterion, press the button (+) of the desired profile. After that the setup wizard will launch and allow you to choose one of these options:

- **A point on the map.** Open the map and then press and hold the point until a circle appears around it. Then you can change the radius of the circle using the control at the bottom of the window. If you want to change the position of the circle, press and hold another point on the map. The setting will be activated when the phone's coordinates are inside the circle.
- **District location.** Specify the perimeter on the map. Click the point of one of the corners; the first marker will appear on the map. Then click a point for the second angle and place a second marker. After adding the third marker, you will see a line connecting all the points in a circle. Add as many points as required to indicate the selected area. To remove a point, just click on it and then click on the icon "X" over the point. The criterion will be turned on when phone coordinates enter the outlined area.
- **Wi-Fi**. Choose the name of a Wi-Fi network from the drop-down list. The criterion will be turned on if the zone is visible.

On the last step of the wizard you can change the criterion name that was generated automatically.

You may edit or delete a criterion by swiping to the left or right and confirming the operation.

You can also switch the profile manually using the icon at the top of the main window. If the profile is changed manually, it will be active until any other criterion is triggered.

**Note:** to ensure My Places works best, you should turn on the GPS on your phone. This option can be found in the Settings. Please note that this may increase battery consumption.

## 9.3. Protection of Windows PC

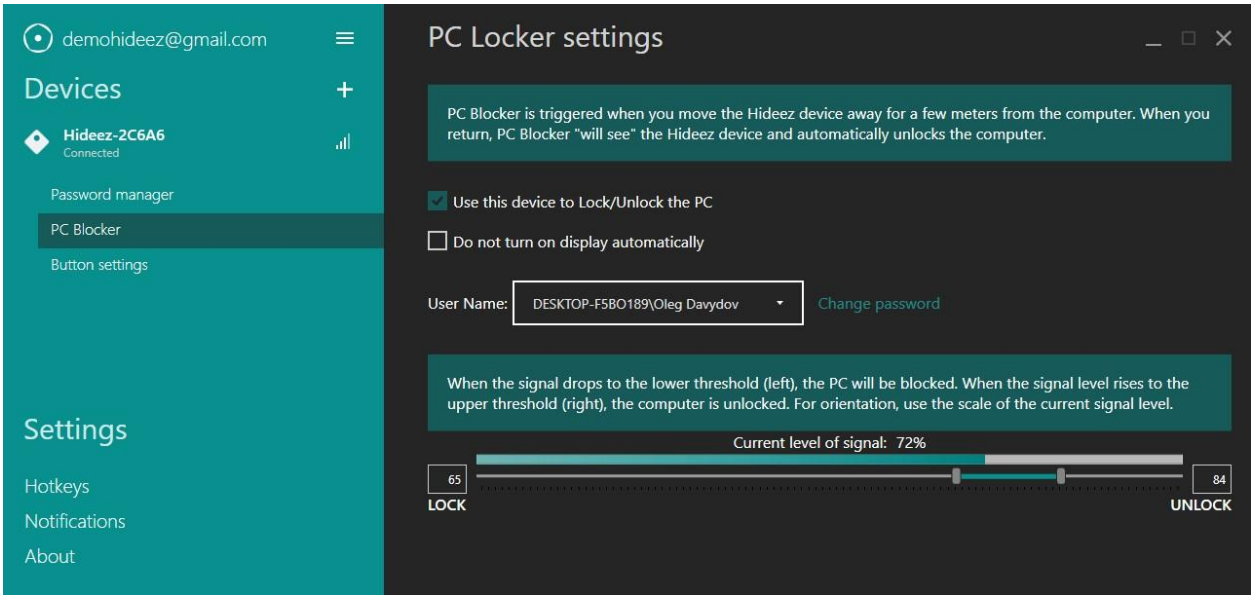
Hideez Safe for Windows PC adds one more way to log into PC – via Hideez Key 2 ST102 presence. The full list of possible authorization methods can be seen in "Sign-in options" on the PC lock screen:

On the picture above there are four ways to enter: Hideez Key, fingerprint reader, PIN code and password.

When choosing Hideez Key, the computer will automatically be unlocked if your key fob is placed close enough.

You will need to adjust the input options of the program Hideez Safe ("PC Llocker" tab):

- Set the checkbox ‘Use this device to Lock/Unlock the PC’.
- Type in your local / domain user name. Use the dropdown to pick one of the local PC users.
- Type in the appropriate password. This password is stored in the Hideez Key, not on the PC
- Save the changes.




With the *Advanced Settings.* you can adjust the Bluetooth signal levels to lock or unlock the PC. The left border is set for the locking level of the signal. When the level drops below this value, the computer will be locked. There is a few-second delay to ensure that the signal level has actually dropped. This reduces the possibility of a false lock from random interference on the radio channel.

The level of the signal unlock is on the right. If the level goes above this value, Your PC can be unlocked either manually or automatically. The current signal level is shown in an indicator above the settings for the signal levels. Use this indicator to find a specific value at which to lock and unlock your PC. Set the lower signal threshold 20% higher to avoid locking it accidentally.

The "Do not switch the screen automatically" option is disabled by default. This means that when you approach the computer and the signal level reaches the upper value, the screen is turned on. Your computer will be unlocked and you will see the desktop without even touching your computer. If this option is enabled, you will need to press Enter or swipe the lock screen (on devices with touch screens).

**Note:** All your previous input methods can be also used.

## 9.4. Password Manager

Hideez Key 2 ST102 can store any credentials. The number of passwords and logins is limited only by the amount of available internal memory (76 KB). These credentials can be entered into any application or web browser. Android 5.0 and above allows you to automatically input credentials or credentials can also be entered by clicking the key fob button or by pressing keyboard hotkeys (for Windows).

The Hideez Password Manager uses the term “account” that is a combination of a username and a password, OTP secret key and the account name. Detailed information about one-time passwords can be found in the "One-time passwords" section. Account names help users to distinguish accounts in the list. Account names must be unique or contain different logins. By default, the account name matches the domain of the web site, the title of the application for Android or the window title for Windows applications.

Along with these fields, accounts also contain additional information about account usage. The root domain name is added for a web site; an Android package name is added for Android applications and the title of the program window is added for Windows applications. Web sites information is common for all operating systems and will be visible on any device. However, specific information about Android or Windows applications is only displayed in the corresponding OS.

All information is stored in the key fob, but not on PCs or phones. Accounts that you store on your device are shared and can be seen on all devices. This option helps to avoid the problem of data synchronization between devices without using cloud storage.

A single Password manager account can be linked to multiple web-sites or applications, including different operating systems. If a password was changed, all the linked applications and sites will automatically use the new password.

### 9.4.1. Working with Passwords in Android and iOS

Hideez Key 2 ST102 works differently on Android and iOS.

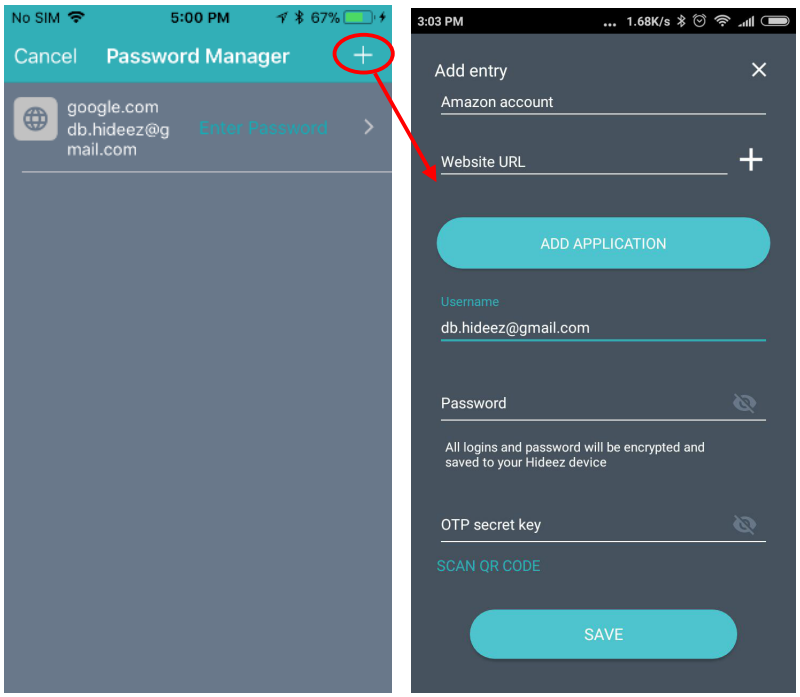
Entering passwords in iOS is only possible in Safari.

For Android, passwords are entered in web pages (only Chrome and Opera browsers), as well as in most applications installed on the smartphone (this depends on the implementation of the application). If you find a program in which the password does not work, contact Hideez technical support. When a solution is found, it will be included in the following updates of the Hideez Safe program.

*Adding passwords*

Launch the password manager from the main application window. When you launch the program for the first time, the program will ask your permission to enter passwords automatically and will open the Android settings window. Please, allow Hideez Safe access, enabling the appropriate radio button.

To add a password, press "+" on the top of the window. The account adding window will be opened.




Select “Application” to open a list of installed Android applications. Choose one and then enter a login and password for it.

If a website “http://” is selected, enter a URL. The password will be applicable to all the pages on this domain and its subdomains.

Please note that the ‘login’ field can be empty for some sites or applications.

If an app needs a PIN-code, please enter it into the password field.

Save the item.

To edit an account item, click it in the account list. To delete it, swipe it out and confirm deleting it in the pop-window.

A stored password cannot be read. The user can only replace the old password with a new one.

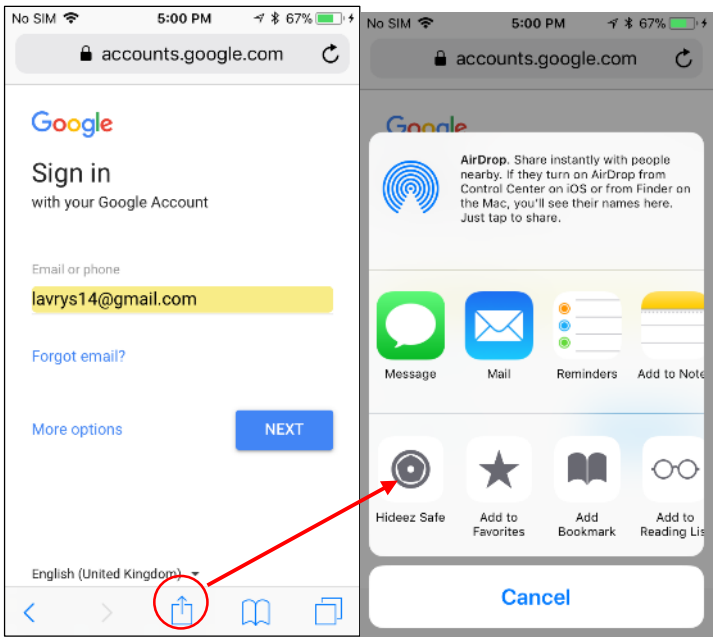
### *Assigning an existing password to the Android application.*

Web applications often have "native" smartphone applications. It is convenient to use a single the same password manager item for both webpage and app. The item can be "attached" to the mobile application on the smartphone.

Make sure the app is installed, then open the Hideez Safe password manager, open the item, tap “Add application" and choose one from the list.

### *Using passwords in iOS*

The password can be entered into the web form opened in Safari using the Hideez Safe button on the extension panel (see the figure below).

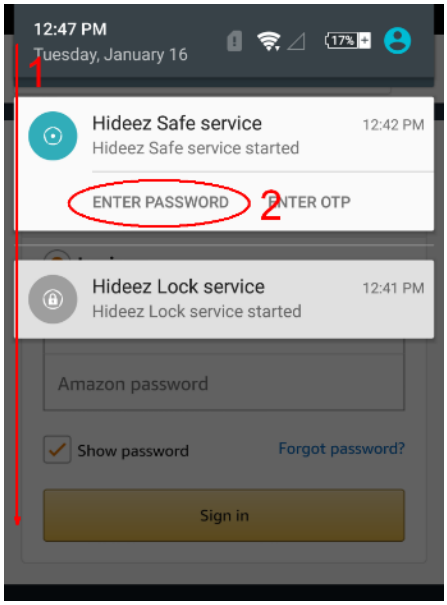



Run the target application. The login and password fields can now be filled in by pressing the Hideez Key 2 ST102 button. For an Android smartphone, the password can be also entered by button on notification bar.

### *Using passwords in Android*

You can apply a password in two ways:

a. Open the target application or web page and press the Hideez Key 2 ST102 button twice. The login and password fields will be automatically filled in.
b. On Android 6.0 and above, you can use notification bar. To access it, do "top-down" gesture.




*Changing or removing items in password manager*

To edit an account, click on the desired line in the list. To delete an account, you can "swipe" it from the list to the side and confirm the operation in the pop-up window.

Saved passwords cannot be viewed but only changed.

See the appropriate video for Android and iOS.

### 9.4.2. Password Manager in Windows system

Passwords cannot be entered automatically for Windows OS. You need to use either combinations of “hot keys” or the key fob button. The combinations of keys below are set by default:

| ***Command*** | ***Windows*** | ***MacOS*** |
|---|---|---|
| *Enter login* | Control + Alt + L | ^⇧A |
| *Enter password* | Control + Alt + P | ^⇧P |
| *Enter password by default* | Control + Alt + D | ^⇧D |
| *Add new password* | Control + Alt + A | ^⇧A |
| *Generate OTP* | Control + Alt + O | ^⇧O |

The key fob button has the following settings:

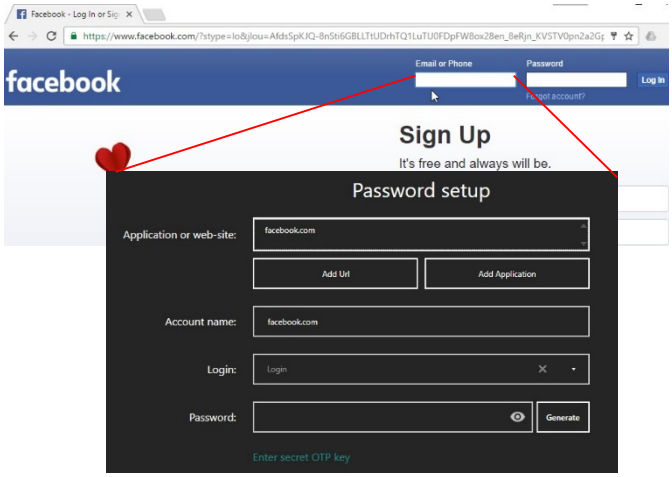
| ***Amount of the clicks*** | **Action** |
|---|---|
| *1 click* | Block the PC |
| *2 clicks* | Enter password |
| *3 clicks* | Enter login |
| *4 clicks* | Generate OTP |

You can easily change these settings.

*Add and enter passwords in web browsers*

The easiest way to add a new password (account) is to do it from the target application directly. For example, open an Internet browser, go to any website that requires a password and click on the password field. Click

the key fob button twice or press the hotkey combination. Since this site is new and there is no password stored yet, Hideez Safe will open a window to add a new account.




The "Application or the site" field will contain the site domain name. This field is used to search in the list later on; thus, it is recommended not to change it. However, you can remove a subdomain any time. For example, you may leave enter hideez.com instead of my.hideez.com. This makes the record applicable to all site subdomains. This field can contain several web-domains, each one on a new row.

The "Account Name" is also automatically filled in with a domain name. You can enter any text here.

The "Login" field should be filled in manually. If the login has been used earlier, you can choose it from the drop-down list. Logins are removed from this list automatically when they are no longer being used.

The "Password" must be filled in manually.

After filling in all the fields, click [Save], and then return to the text field in the browser and press the appropriate hotkey combination. Your password will be entered into the target text field. Logins and OTPs (see details here: One-time passwords) can be entered the same way.

**Note**: The Hideez Safe program can work with the latest versions of the most popular Internet browsers – Chrome, Firefox, Opera, Internet Explorer, Edge (Windows) and Safari, Chrome (Mac). For other browsers, the system will perform like a normal desktop application, using the window title instead of web-domain.

**Tip:** Upgrade your browser to the latest version, if the web-domain is not automatically recognized by Hideez Safe.

**Tip:** If you are registered on the same resource for multiple logins, the program will ask you to add the first account and then will apply this account further. To add another login, please use a special hotkey combination “Control + Alt + A” to create a new account in Hideez Safe Password manager.

### *Automatic Password Generation*

When you create new credentials for web, it is convenient to use an automatic password generation. The generated password will be unique and secure. To create it press the “Generate” button while editing the account. A generated password can be seen by clicking on the icon. Then save your account, go to the registration page in the browser and use the stored password in both fields in order to enter and confirm the password.

**Tip**: Always create unique passwords for different services. If someone does manage to compromise of one of the passwords, the other passwords will not be affected.

### *Changing Password*

It is often necessary to change the password on any of the web resources. You usually need to enter the old password, then enter the new one and confirm it. First, use the key fob to enter the old password. Then open the Hideez Safe box, go to the password manager, search for the necessary account and open it for editing. In the editing window, click “Change Password” and the “Generate” button. Then save your account, open the browser and use the new password.

**Tip**: If an error occurs on the web server before the password change is complete, you can use the backup data copy to load the initial password to the key fob and repeat the procedure again. Please remember, that this procedure restores the whole Hideez Key 2 ST102 memory including other Password Manager items.

### *Adding and Entering Passwords in Desktop Applications*

Hideez Safe can enter credentials into web pages, as well as into applications. Just place the cursor on the input field of the login and password, and press the appropriate hotkey combination, or the key fob button. The program determines the current active window, gets the window title and the name of the program process and tries to find the information for the appropriate account. Just as with websites, if there is no corresponding account, you will be asked to add a new one.

The "*Application or website*" field will be automatically filled in with the window title. This field will be used to search for the account. You can remove irrelevant words from this field. The search will use the following algorithm: the account is considered to be a match if every word of this field can be found in the title of the window where the password is being entered. This field can include several lines; each line is processed independently. So, you can set up an account for several different programs.

The "*Account Name*" field is also automatically filled in with the window title. You can enter any name here.

The "Login" field should be filled in manually. If you entered the login earlier, you can select it from the drop-down list. Logins are removed from the list automatically when they are no longer being used.

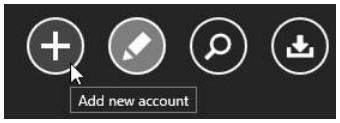
The "*Password*" field must be filled in manually.

After filling in all the fields, click “Save”, and then return to the window, where you need to enter your password and press the key combination again. The password will be entered automatically. Similarly, you can enter your username or OTP.

See video “How to add passwords” to WEB and desktop apps for Windows and Mac on the channel http://youtube.com/hideez.

### *Adding Passwords manually*

You can also add a new account for the selected program using the Hideez Safe interface. First, press the “+” in the Password Manager as it shown on the picture below.




The "Application or website" option has [Add URL] and [Add application] buttons. “Add application” opens a list of window titles for all the opened programs on your PC. “Add Url” displays domain names in opened tabs

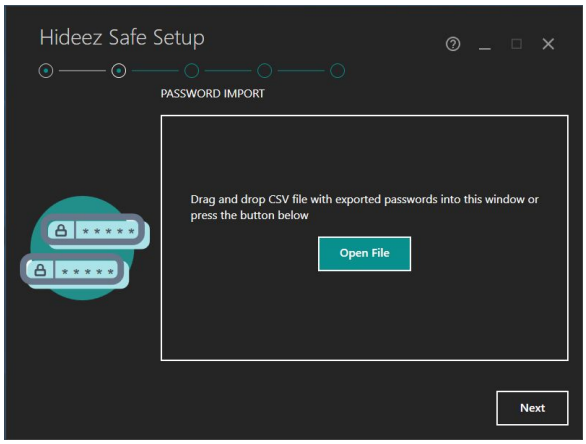
of the opened browser windows. Choose the needed entry from the list. Filling all the other parameters as described in the Add and Enter Passwords in the Web Browsers and Adding and Entering Passwords in Desktop Applications sections.

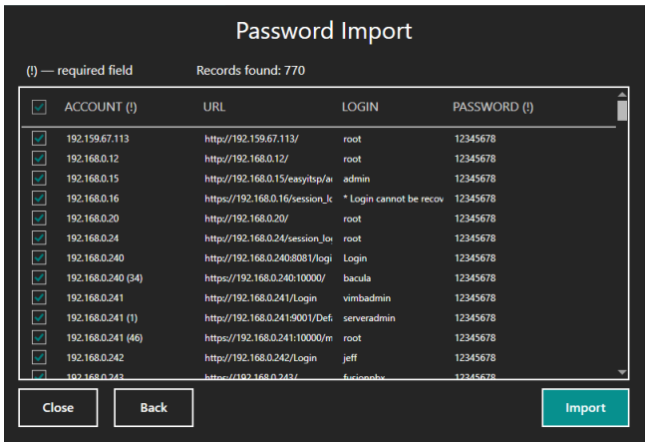
### *Choosing from Several Suitable Accounts*

Sometimes you need to create several accounts for a single resource. For example, you may have a personal and corporate email with Gmail. Hideez Safe cannot know which Gmail account you want to use, so you need to choose from a list of suitable accounts. This list will appear in the corner of the screen near the Hideez Safe icon.

### *Import passwords from CSV-file*

Hideez Safe can import passwords from a CSV file into Hideez Key. To do that click the icon in the Password Manager. You will see the figures like below.




Among the found items, mark the necessary ones and click the [Import] button.

Hideez Safe for Mac works similarly.

### *Using the Default Password*

One of your passwords can be assigned as the default password. This password will be entered every time you press a hotkey combination to enter the “default password” (the default setting is Control + Alt + D). To set this password, open the “Hotkey” tab and select it in the list.

### *Setting Hotkeys*

Hotkey combinations make credentials usage much easier. The default settings are easy to remember, however, you can change them in the Hotkeys section. Place the cursor in the needed input field and press a new hotkey combination that you want to assign. If this does not work, then this combination is already being used by the operating system or other software. In this case, choose a different hotkey combination.

When you start Hideez Safe, it registers all the key combinations with Windows, so that they can be used in any program. If another program has already registered the combination, Hideez Safe will notify you. In this case, you must choose a different shortcut.

### *Removing Records from the Password Manager*

To delete a Password Manager entry, open it for editing and click "Delete Account" at the bottom of the screen. If it is not used for another account, the appropriate login will also be deleted from the key fob.

**Note**: You can completely clean the Hideez Key 2 ST102 memory by clicking "Remove from account" in your device settings.

## 9.5. One-time Passwords (OTP) and Two-Factor Authentication

Hideez Key 2 ST102 supports one-time passwords (time based one-time password, TOTP) according to RFC 6238 standard.

The main idea of using one-time passwords is that there is a shared secret known only by two devices (a private key). Using encryption, one of the devices generates a short (e.g., six-digit) one-time password based on this key. This password is sent to the second device to be checked. The second device uses the same algorithm. It generates the same secret key, creates a one-time password and compares it with the password received from the first device. If the passwords are the same - access will be granted.

One-time passwords are so called because of their generation algorithm. In addition to the private key, the one-time password counter is also used here. Each time the password will differ from the previous one. The counters on both sides must be synchronized: if at least one password is missed, they will not be the same and the algorithm will be broken. Another convenient option for one-time password generation can be synchronization by time. In this case, the generation algorithm does not use the counter, but the current time. With time synchronization between the devices, you always get the same passwords on both sides. According to RFC 6238 standards, the time is rounded up to the nearest 30 seconds: for example, every 30 seconds your one-time password will change.

Hideez Key 2 ST102 uses the second option: synchronization by time. Time synchronization between the key fob and the computer / smartphone occurs when a connection is established between them. In order to work properly, you need to set the correct time on your PC, otherwise it will not coincide with the time on the server that checks the OTP and the passwords will not match.

You can add the OTP secret key to any account in the password manager window.

The following information shows how to use Hideez Key 2 ST102 for Google two-factor authentication (2FA).

- Go to your account security settings https://accounts.google.com/b/0/SmsAuthConfig
- Turn on 2FA for your account (corporate clients may need corporate admin confirmation).
- Google may ask for your mobile number. Input it and put in the special code received from Google via SMS.
- Choose “Get codes via our mobile app instead”, and check “Android”.
- In the “Set up Google Authenticator” dialog click on the link “Can't scan the barcode?” and find the 32-symbol secret key shown in the form of text.
- Copy the secret key into the clipboard.
- Open your Password manager entry, click “Enter secret OTP key”, paste the copied data and save the changes.
- After that, open the browser and click OK to complete the settings. Google will immediately ask you to enter a one-time password to be sure that you have configured everything properly. Press the key combination to enter the OTP (the default is Control + Alt + O). A one-time password will be created in the key fob and will be entered in the input field. Before it checks the OTP, the secret key will not be applied and the two-factor authentication will be turned off.

See video of Google 2FA settings with Hideez Key 2 ST102 for Windows and Mac on the channel http://youtube.com/hideez.

**Note**: Each new secret code generation on the Google web-service makes the previous code invalid, so you need to install the private key on all the devices simultaneously, e.g. Hideez Key 2 ST102 and Google Authenticator on your smartphone.

## 9.6. Backup and Recovery of the User Data

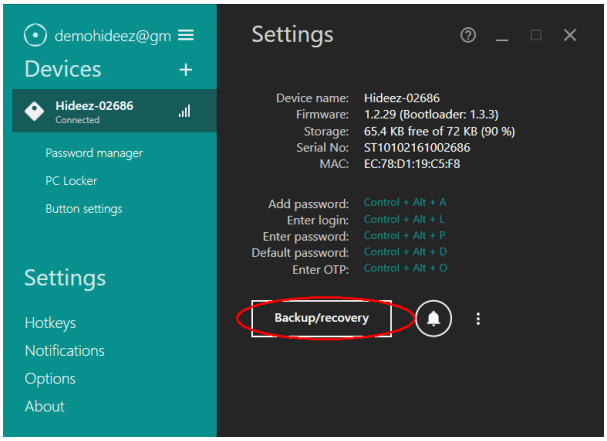
Hideez Key 2 ST102 contains 76 KB of user memory and can store thousands of passwords, logins, keys and other information. To prevent losing this data, Hideez Safe can backup and restore user data.

The backup file should be kept on local PC/tablet storage only. The file is encrypted by your My Hideez password according to AES-256.

The file name contains the *.hb extension. It includes the device name as well as the date and time of last modification of data in the key fob memory.

To recover the file, you need to enter the password manually. Please note, if you change your account password, you will need to enter the password that was used when the backup was created.

In Hideez Key 2 ST102 for Android, the “backup and recovery” menu can be found in the context menu of the key fob. For the Windows version, it is in the Hideez Key 2 ST102 properties section.




Although the backup file is encrypted, it is recommended to store it in a safe place. If lost, any local file can potentially be cracked through brute force decryption. For details, see. Recommendations for safe usage.

**Note:** The Hideez Key 2 ST102 should be registered and initialized to perform backup / recovery operations.

**Tip:** The backup / restore procedure can be used to transfer data between Hideez Key 2 ST102 devices of one user as well as to transfer data between devices of different users. (the password that was used to backup will be required).

## 9.7. Protection and Search of Hideez Key

Due to the constant Bluetooth connection, Hideez Key 2 ST102 helps prevent its own loss, as well as the loss of other devices that are associated with it.

The key fob is considered forgotten if the phone switches from “Home” / “Office” profile to “Street” profile and Hideez Key 2 ST102 device is not connected.

The key fob is considered lost if it had been connected and suddenly the level dropped below the threshold.

When your phone switches to the “Street” profile, it verifies whether all the key fobs are connected. If any of them are absent, both the warning sound and notice log recording are activated. Each key fob has a separate log recording. The audio warning is played once for each forgotten tag.

A device protection mode is available in Hideez Safe for Android only. You can enable and configure it in the "Theft Alarm" section:

- Turn on the "Watch for the loss of connection" switch
- Set a ringtone that will notify you about the loss.
- Select the option to turn the sound on for the key fob. If it is turned off, the sound will only be activated on the phone.
- Specify the profiles that you want to use this feature. By default, it is turned on for “Office” and “Street” modes, while it is turned off for “Home” profile.

The program is set to trigger when the signal level drops to 10%. If you want to change these settings, go to the "Advanced Mode" menu. After that, there will be more options in the "Theft alarm" window:

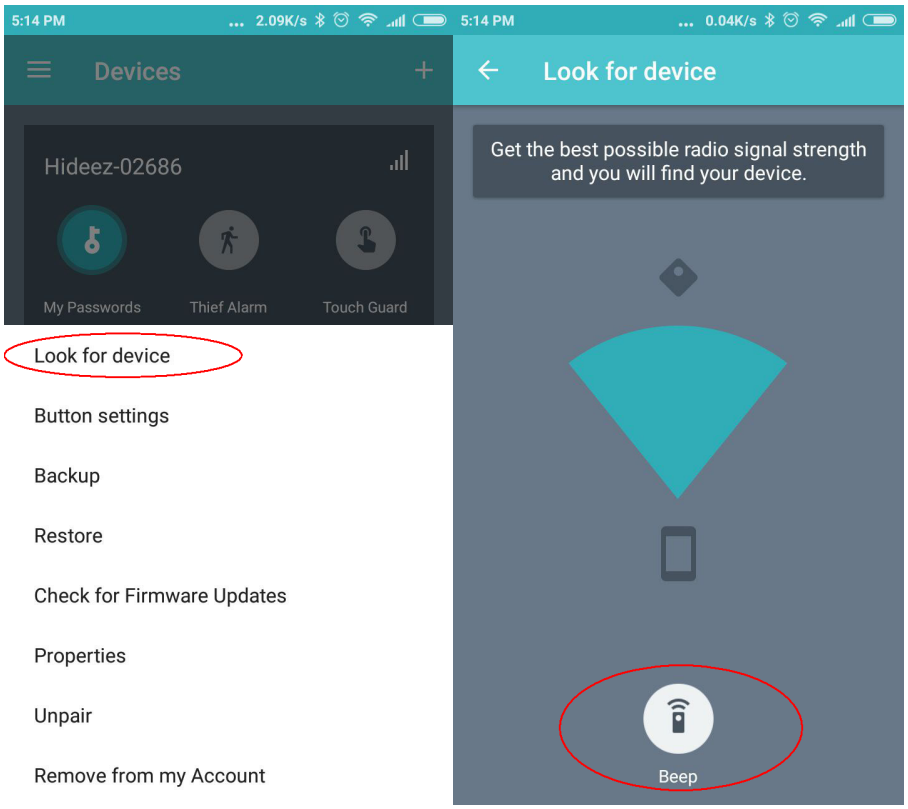
- **Proximity level** is the distance between two Bluetooth devices. It is defined as a percentage ranging from 0 to 100, where 100 is the best signal and 0 is a connection loss.

- **Latency** is the time delay before triggering. It is used along with “Proximity level” and helps to avoid false alarms caused by temporary fluctuations in signal strength. The action to take when the signal drops below the threshold level is not made until the time passes (Latency).

**Note:** Using audio signals on the key fob can significantly drain the battery, so this option is disabled by default.

### 9.7.1. How to find keyfob with your smartphone

If the key fob has an active connection, but you cannot find it, you can turn on its audible signal:




If the sound for some reason is not audible, you can focus on the signal level, which directly depends on the distance between the smartphone and key fob.

**Note**: The phone displays the signal level, not the signal direction. The signal level depends very much on the antenna’s location within the phone, the phone location in the hand, obstacles in the area, signal reflections etc.

### 9.7.2. Track with Google Maps

If Hideez Key 2 ST102 connection is lost, Hideez Safe app remembers the coordinates when it happened. Go to the device drop down menu and choose “Last seen” to see the key fob last location on Google Maps.

## 9.8. Biometric Authentication of Android user

Hideez Safe uses biometric identification of TouchID - fingerprint recognition for easy authentication.

To use Biometric Authentication TouchID - Fingerprint recognition, please do the following:

1. Open "Settings" from the main menu.
2. Ensure that the "Require PIN to sign in to the application" is turned on.
3. Enable the "Activate fingerprint scanner".

4. Setup is complete, now you can use TouchID with Hideez Key.

## 9.9. Using of RFID-sensor

Each Hideez Key 2 ST102 device is equipped with radio frequency identification module (RFID) Atmel T5577, operating at a frequency of 125 kHz. This module operates independently from the Bluetooth module and is not connected to it.

The RFID module is commonly used for identification in access control systems. Hideez Key 2 ST102 can work on two different standards: HID or Em-Marine. However, they cannot be used simultaneously.

The key fob comes with a unique code that has already been put in Em-Marine standard. This code can be replaced by any other code both in the Em-Marine and HID standard. This procedure requires special hardware called a programmer. This equipment is supplied as a part of commercial access control systems (ACS), or it can be purchased separately. Detailed information about these issues can be found in the documentation for access control systems and will not be described in detail in this manual.

See video of программировании RFID модуля on the channel http://youtube.com/hideez.

**Note**: RFID module is **not compatible with NFC modules** that are installed in smartphones and tablets, as it works on another frequency.

## 9.10. Touch guard (Android only)

The Hideez Safe application for Android can take a series of photos at if someone picks phone up when it is left unattended,. Photos will be taken under the following conditions:

- "Touch guard" mode is on and phone is in stand-by mode.
- Hideez Key 2 ST102 is connected to the phone and RSSI level is less than it's set in settings.
- An accelerometer shows an activity (the phone start moving).

## 9.11. Remote Control of Android phone

Hideez Safe for Android enables you to perform an action on your Paired Device when the multifunctional button is clicked on your Hideez Key. To do this, select "Actions" from the main screen. Use one of the following actions:

- Send an SMS. You will need to provide a phone number and SMS text in the settings.
- Turn on the recorder. By pressing the button again, you will stop recording. Listening to the recording is available only through the Hideez Safe gallery; recorded files are not encrypted.
- Initiate an outgoing call. You will need to set a phone number in the settings.
- Take a photo. Photos will be encrypted, so you can only see them through the Hideez Safe gallery.
- Send the current coordinates. You will need to provide a phone number in the settings.
- Turn on the flashlight. Pressing the button again turns off the flashlight.
- Take a video. Watching the video is only available through the Hideez Safe gallery; however, video files are not encrypted. By pressing the button again, you will stop recording.
- Turn on the beep. You can specify the type of signal in the settings.

Setting up these actions done with a step-by-step wizard:

1. Open 'Actions' in the Main Menu and click [+} to start step-by-step wizard.
2. Choose the type of action (the number of button presses). The list will include only those options that are not yet selected.
3. Select an action from the list.

4. Select any additional parameters for the chosen action, for example, the type of the camera or phone number.

Hideez Safe program has set some default actions:

| ***Type of click*** | **Action** |
|---|---|
| *1 click* | Enter OTP |
| *2 clicks* | Enter login and password |
| *Long press (2-4 seconds)* | Swith Hideez Key 2 ST102 to another PC/phone |
| *Long press (10 seconds)* | Turn off keyfob |

## 10. Web-service my.hideez.com

My Hideez personal cabinet allows you to view the list of your Hideez Keys, including information about the device model, serial number and date of first registration.

Using a web-based service, you can remove Hideez Key 2 ST102 from your account. For example, it you gave it to another person, but forgot to “clean” it, the new user will receive the error message "The device is registered to another user," while trying to connect. The new owner will not be able to use this Hideez Key 2 ST102 or read data from it. When the device is removed from your account on My Hideez, Hideez Safe app on new user’s phone / PC will do a complete reset and clear Hideez Key, allowing it to be used again.

**Notice**: If you lost your Hideez Key, do not delete it from your account. No one can use it or have access to your data. If you remove this Hideez Key 2 ST102 from your account, someone can use key fob as if it were a new device.

Changing the password on your My Hideez account is also performed here. You will need to specify the old and new passwords. After this, Hideez Safe applications on your devices will ask you to re-log in, as the old password will no longer work.

If you forgot the password to your account, you can reset it through the web service. A confirmation of the password reset will be sent to your email.

# 11. Annex 1. Troubleshooting

### *Hideez Key 2 ST102 does not work and does not respond to button clicks*

You should replace the battery as described in "Getting Started."

### *Unable to find the Hideez Key 2 ST102 by Bluetooth-channel*

In order to make Hideez Key 2 ST102 available for connection, press the button once. If the key fob is connected to another device, you must first break the connection by turning off the Bluetooth on the device or by bring the Hideez Key 2 ST102 out of radio signal range.

Note. On some devices broadcasting, doesn't work when geolocation in the Android settings is off You will need to turn on these settings during pairing.

### *The device has fallen into the water and stopped working*

Water can significantly damage the device. You should remove the device from water as soon as possible, then open the case, remove the battery and dry the board, for example, with a household hair dryer.

After drying you will need to install a new battery and test the functionality.

### *Hideez Key 2 ST102 stopped making sounds*

The beep function turns off when the battery is low. All the other functions are working properly, so you cannot use the device until the battery is replaced.

### *I cannot remove Hideez Safe from Android: the option to remove is locked*

If you use the Smart Lock function, that means Hideez Safe was added to the list of administrators of your device. To uninstall the software, you need to remove the app from the list first. To do this, go to Settings - Security - Device Administrators.

### *My PC or phone can't see Hideez Key*

The action list below can help you with that:

- Turn off and on Bluetooth on PC/phone
- Turn off and on Geolocation on Android
- If you use Windows 7 and Bluetooth Dongle, please set a special driver from Hideez Safe directory for Bluetooth adapter (see video).
- Delete "bondes" (pairing information) from Hideez Key. To do that press the Hideez button 9 times, then, after light is on, press it 3 times.. Remember, that you will have to do connection procedure on the all your devices again.
- You may have to do preliminary pairing procedure for the Hideez Key 2 ST102 and the phone in Bluetooth settings.

# 12. Annex 2. Safety Precautions

**1. Use a strong password for your Hideez account.**

This password, unlike the others, you will need to enter manually. To create a strong password, please follow these general guidelines:

- The password must contain at least six characters.
- The password can contain numbers, letters, spaces and special characters (".", ",", "?", "!", "<", ">". "" " and others).
- It is strongly recommended that you make a password using a mix of numeric and alphabetic (uppercase and lowercase) characters.

Do not use the following as a password:

- Common words and phrases.
- Sets of symbols that are the combinations of keys arranged in a row on the keyboard, such as: qwerty, 123456789, qazxsw etc...
- Personal data, such as names, addresses, passport numbers, insurance certificates, etc., and the passwords you use to run other programs (e-mail, databases, etc.).

**2. Create a new, unique password for every service you use.**

**3. If possible, use automatic password generation.** Such passwords are very secure.

**4. Securely store the backup files**, because any local file can be hacked through a brute force attack. It is a good idea to store the copy on your second Hideez Key 2 ST102 device. If someone attempts to find the key to access the device, it will be blocked forever after 1000 failed attempts. The web service my.hideez.com has similar protection. The backup can be also stored on secure flash drives, or kept in a safe place, such as a safety deposit box.

5. Use anti-virus software, do not visit suspicious sites, do not install software from untrusted sources and do not open e-mail attachments with the extensions *.exe, or *.apk.

# 13. Annex 3. Hideez Key 2 ST102 Signals and States

### *Sound Signals*

1. Alarm — an alternating sound at 6000 Hz, 2680 Hz, 1080 Hz for about 5 s
2. Single beep — short beep 480 Hz * 80 ms
3. Double beep — two short beeps 2680 Hz * 80 ms
4. Roger beep — two short beeps 480 Hz * 80 ms
5. Error beep — three beeps 200 Hz *200 ms
6. Connected beep — 960 Hz * 80 ms, 1360 Hz * 80 ms
7. Disconnected beep — 960 Hz * 80 ms, 800 Hz * 80 ms, 800 Hz * 80 ms
8. Peripheral beep — 3400 Hz * 160 ms, 3600 Hz * 80 ms, 3800 Hz * 160 ms
9. Roger beep in menu — 1480 Hz * 80 ms, 1880 Hz * 80 ms, 3200 Hz * 160 ms

**Warning!** If the battery is below 30%, the audio signal will be turned off to save battery life.

### *Light Signals*

1. Connected — indicates an active Bluetooth connection was established, 100 ms on, 3900 ms off (cycled)
2. Fast flash — 100 ms on, 100 ms off (cycled)
3. Slow flash— 500 ms on, 500 ms off (cycled)
4. Double flash — 100 ms on, 100 ms off,100 ms on, 800 ms off (single)
5. Single flash — 100 ms on, 100 ms off. (single)
6. Constant – continuous light

### *Signals Description*

| Signal | | Event, state |
|---|---|---|
| Sound | LED | |
| Single beep | Single flash green | Accompanies a single push of the multifunctional button<br>Counts the seconds that the multifunctional button was held down |
| Double beep | Double flash green | Ready to work after power is on |
| Roger beep | Double flash green | Confirms a command from the multifunctional button was accepted;<br>Confirms a command from the menu has run |
| Error beep | Double blink red | Command or scenario execution error |
| Connected beep | flash green | Indicates a Bluetooth connection was established |
| Disconnected beep | Double flash red | Indicates a Bluetooth connection was broken |
| | Connected green | Hideez Key 2 ST102 is connected to a device |
| Peripheral beep | Fast flash red | Entered menu mode |
| Broadcasting beep | Slow flash green | Hideez Key 2 ST102 is broadcasting to connect (advertising mode) to any device (whitelist is ignored) |
| | Constant green | Hideez Key 2 ST102 is on bootloader mode, not connected to the any device |
| | Constant red | Hideez Key 2 ST102 is on bootloader mode and connected to the paired device |

# *14.* Annex 4. Frequently Asked Questions

*How long does the Hideez Key 2 ST102 work before the battery needs to be changed?*

The estimated operation time of Hideez Key 2 ST102 is up to 6 months, depending on usage and the quality of the battery. The highest energy consumption occurs when using audio signals on the key fob.

*How do I change the battery? Will the data be lost?*

All user data is stored in non-volatile memory. When the power is turned off, they are always saved.

*Will Hideez Key 2 ST102 work with an iPhone or Mac?*

Yes, it will work after Hideez Safe for iOS is released. However, the lock / unlock functions on the iPhone are not available because of iOS limitations.

*How I can I clean my Hideez Key 2 ST102 if I want to give it to someone else?*

Each Hideez Key 2 ST102 is registered to the My Hideez account of its owner. To give it to someone else, the owner should run the "Unregister" procedure. This will clean the device registration and wipe out all the user data. If you forgot to unregister before giving the device to another person, you can do it in your my.hideez.com personal cabinet.

*What physical conditions are dangerous for the Hideez Key? What about electromagnetic radiation, direct sunlight and magnetic fields?*

The Hideez Key 2 ST102 is made of plastic and doesn't provide extra resistance. Electronic components retain their characteristics in normal environments (direct sunlight, electromagnetic radiation) that are safe for humans. It is not recommended that you expose the device to prolonged sunlight to avoid damaging the plastic housing.

*Is the Hideez Key 2 ST102 allowed on planes?*

Yes, it is. The device receives and transmits radio frequency according to the Bluetooth 4.0 compatible standard for a short distance, and does not need to be turned off in an aircraft, according to FAA instructions from October 31, 2013. If you use personal medical devices (such as pacemakers and hearing aids), consult with your doctor or the manufacturer to find out whether they are protected against external RF signals.

*What should I do if my Hideez Key 2 ST102 was stolen?*

If only the Hideez Key 2 ST102 was stolen, but your computer and your phone are with you, then remove the key fob from the Hideez Safe programs. Do not use the "Delete my account" command, since you will allow to use your Hideez Key 2 ST102 to be used as a new device. No one can connect to or use your devices, if they do not know the password to your account. The Web server and the label are protected from attempts to guess the password.

If the Hideez Key 2 ST102 was stolen together with an attached device, you will need to change the password on your Hideez account. After Hideez Safe programs are restarted, they will not be able to log in to the server and therefore will not be able to use the key fob.

*Can I use the key fob if my PC does not have Bluetooth 4.0 compatible adapter?*

Yes, you can purchase a separate adapter that will be connected via USB. You can find the details on the section *Are my devices compatible with Hideez Key?*

*Where are my passwords physically stored? Are they copied to a computer / phone, or to the cloud?*

Passwords are stored on the key fob only. When a password is required for a computer or phone, Hideez Safe requests it from the key fob, enters the password and immediately removes it from memory. The passwords are not copied to the cloud, but you can make a copy of the data from the key fob using an encrypted local file.

*Can I make a backup copy of the data from the key fob?*

Yes, the Hideez Safe client provides data backup to a local file. The file is encrypted with the password of your account (the password that you use to launch the program). Then the encrypted file is saved to the disk. AES256 encryption algorithm in CBC mode is always used.

It is worth mentioning that the key fob and the web service are protected from hacking by brute force attacks. However, the backup file cannot be fully protected with this level of protection. That is why we highly recommend keeping the backup file in a safe place (for example, USB flash drive in a safe deposit box). Do not store it on a hard drive or in the cloud.

*Is there any teaching materials regarding Hideez Key 2 ST102 using?*

On the channel http://youtube.com/hideez there are short clips, combined to teaching playlists. See them here: Android, iOS, Mac и Windows.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.