



HKBN SAFE+

Quick Start Guide

For PC (Windows/macOS)



Table of contents

About	3
<i>System requirements for Microsoft Windows computer</i>	<i>4</i>
<i>System requirements for Apple macOS computer</i>	<i>4</i>
<i>Welcome E-mail.....</i>	<i>5</i>
HKBN PROTECT	5
<i>HKBN PROTECT account</i>	<i>5</i>
<i>First time login.....</i>	<i>6</i>
<i>Forget password.....</i>	<i>7</i>
Getting started with HKBN SAFE+	9
<i>Add new device from HKBN PROTECT</i>	<i>9</i>
<i>Sharing protection with a family or friend.....</i>	<i>12</i>
Making browsing Internet safe for children with Family Rules	14
<i>Adding a new device for children</i>	<i>15</i>
<i>Setting up Family Rules for children.....</i>	<i>17</i>
<i>Web Content types in Content Filtering</i>	<i>20</i>
Protecting online banking and shopping	22
<i>Browsing safely with Safety ratings</i>	<i>23</i>
<i>Enabling browser extension for Safari/Chrome/Firefox (For Mac only).....</i>	<i>24</i>
<i>Checking that browser extensions are in use (Windows).....</i>	<i>25</i>
<i>Returning from or entering a blocked website.....</i>	<i>26</i>
Protecting your device against Virus & Threats	27
<i>Using real-time scanning</i>	<i>27</i>
<i>Running a virus scan manually.....</i>	<i>28</i>
Protection status icons	31
Gaming Mode (Windows only)	32
Password Vault	33
<i>About Master Password</i>	<i>34</i>
<i>Create HKBN Safe+ master password.....</i>	<i>34</i>
<i>Create and Save Master Password Recovery Code.....</i>	<i>36</i>
<i>Vault.....</i>	<i>39</i>

<i>Create and Save your Password or Create Card Information</i>	39
<i>Using Autofill</i>	40
<i>Connect Devices</i>	41
ID Monitoring	42
HKBN SAFE+ features per platform	43
HKBN Safe+ Password Vault and ID Monitoring Features Per Platform	44
Technical Support	45
<i>Using the support tool</i>	45
<i>Contact us</i>	45

About

HKBN SAFE+ is a comprehensive security service that offers award-winning protection on multiple devices with a single subscription. With HKBN SAFE+, you can protect yourself and your loved ones against all threats on a computer, smartphone, or tablet.

Install the HKBN SAFE+ applications on all your devices to protect your security and privacy. HKBN SAFE+ supports devices running on Windows, Mac, Android, and iOS operating systems. HKBN SAFE+ also protects you and your loved ones while browsing the Internet, with technology like:

- Browsing Protection (referred to as Safe browsing on mobile platforms), which uses advanced cloud-based web reputation checking to verify the web pages and make sure only safe web sites can be accessed.
- Banking Protection, which protects your online banking activities by securing the connection when you access an online banking portal.

HKBN SAFE+ integrates a new service - ID Protection.

When applying for services on third-party platforms such as shopping websites, membership websites and etc, it is inevitable to fill in different personal information. When those institutions are hacked and lead to data leakage, "ID Protection" can be used to monitor closely on the dark web and other channels whether your personal information has been exploited by hackers and immediately notify the situation by email and provide an encrypted password manager to help you generate a strong password to prevent continuous intrusion by hackers.

Gaming Mode GAMING MODE

In the race against time in the e-sports world, HKBN SAFE+ e-sports mode allows you to optimize your computer before playing to make the game smoother, stop unnecessary pop-up notifications, and run programs in the background without sacrificing anti-virus capabilities.

System requirements for Microsoft Windows computer

Operating Systems supported:

- Windows 8.1. or above

Minimum system requirements:

- Processor: 1 gigahertz (GHz) or faster*
- Memory: 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- Hard disk space: 600 MB available hard disk space
- An internet connection is required to validate your subscription and receive updates. Internet access (ISP) fees might apply.

*ARM CPU is not supported.

Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Microsoft Edge (Chromium-based).

System requirements for Apple macOS computer

Operating systems supported:

- macOS version 11.0 or above

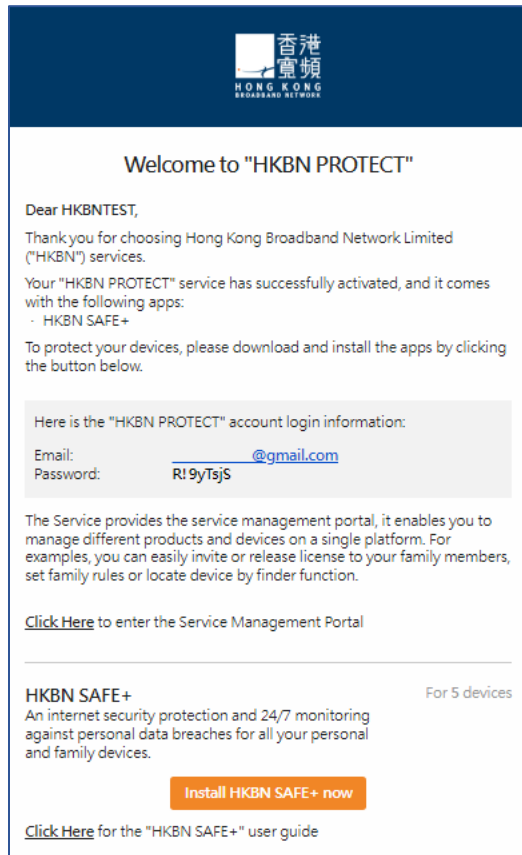
Recommended system requirements:

- Intel processor
- 250 MB of free disk space
- 1 GB or more of memory is recommended
- Internet Connection: An Internet connection is required to validate your subscription and receive updates

Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Safari.

Welcome E-mail



Important info in Welcome E-mail

- Username
- Temporary password
- Subscription information
- HKBN PROTECT portal
- Download Installer website
- Download user guide link

HKBN PROTECT

HKBN PROTECT is an easy-to-use online service you can use to install HKBN SAFE+ onto your selected device remotely and manage your subscription.

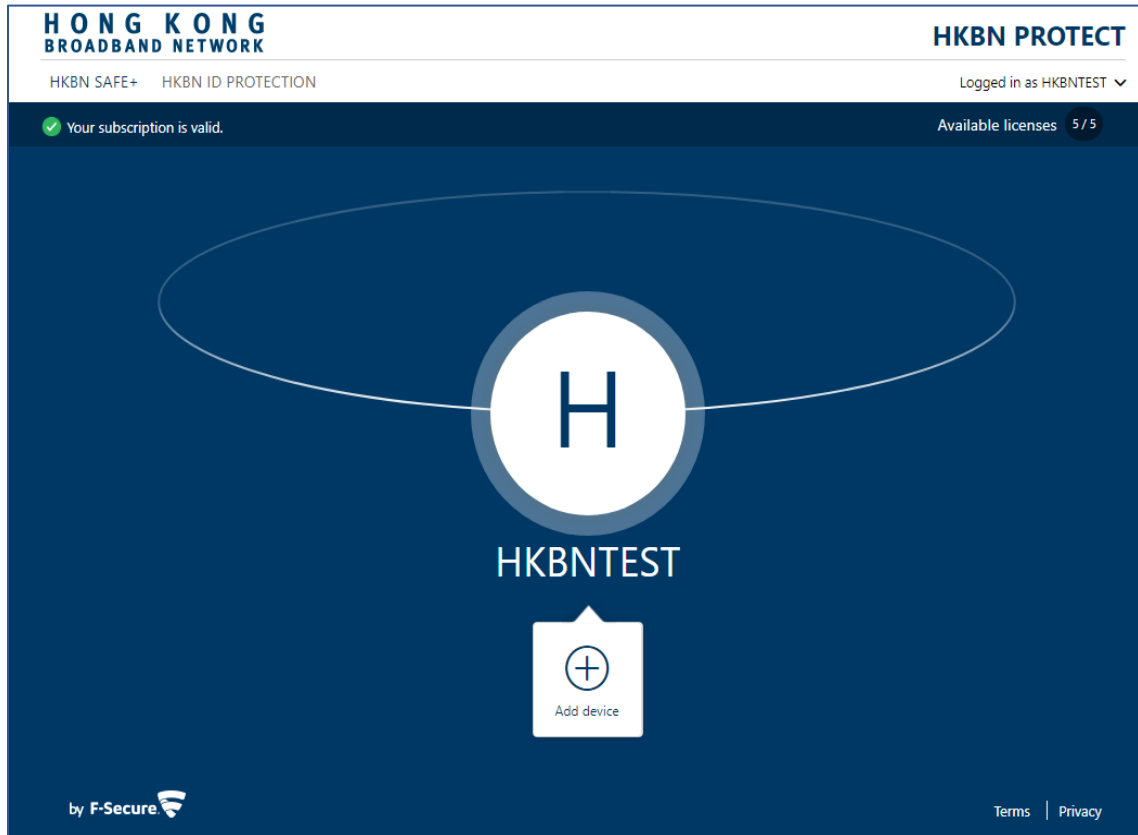
With HKBN PROTECT management portal or the in-app Peoples & Devices view, gives you an overview of the people and their devices that you, as the subscription owner, have protected with your subscription. To see detailed information about a user, just select the user and a user-specific view opens, giving you an overview of the protection of the user.

You can use HKBN PROTECT to easily transfer a HKBN SAFE+ product from one device to another, whenever you choose to do so.

HKBN PROTECT account

To use HKBN SAFE+, you need a HKBN PROTECT account (username and password) to access HKBN PROTECT Portal and to activate the installed HKBN SAFE+ applications. Once you have created your HKBN PROTECT account, you can manage

your device, view your subscription status, and add your family members to share your HKBN PROTECT.



Click on the link below to access to HKBN PROTECT management platform:
<https://ihome2.hkbn.net/fsecureuser>

First time login

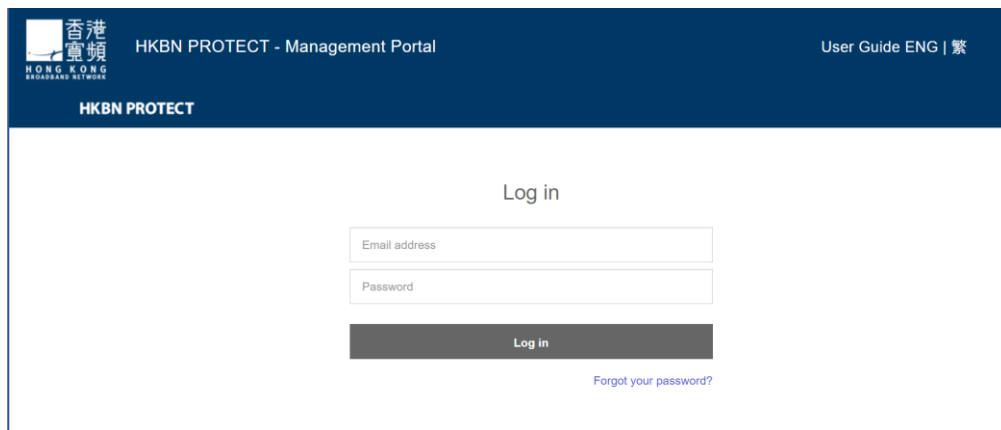
1. Login to HKBN PROTECT portal with your username (email address) and Temp password provided in Welcome Email.
2. On first time login to the portal, you will be requested to set your own password.

Forget password

If you forget the account password of the HKBN PROTECT, you can create a new password through the process of forget password:

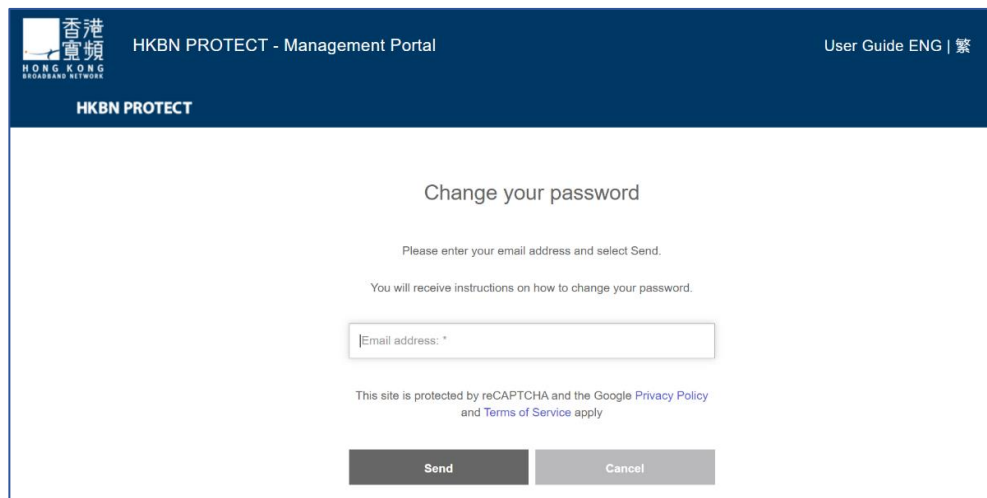
1. Click **Forget Password** on Login page.
2. Enter your e-mail address and click **Send**. A link to change the password will be sent to the registered e-mail address. (Image 1&2)
3. Tab to open the password reset link in e-mail received. (Image 3)
4. Set new password. (Image 4)

(Image 1)



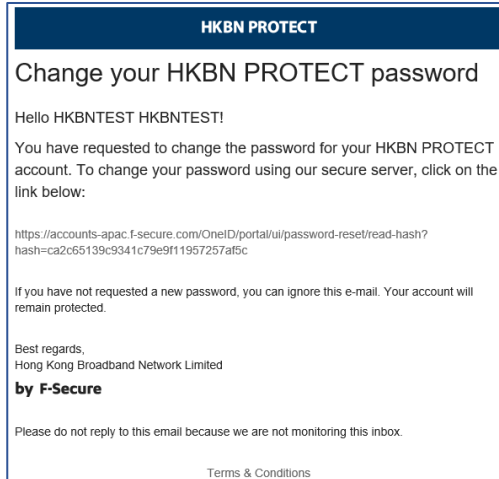
The screenshot shows the login page of the HKBN PROTECT Management Portal. The header includes the HKBN logo (香港寬頻 HONG KONG BROADBAND NETWORK) and the text 'HKBN PROTECT - Management Portal' and 'User Guide ENG | 繁'. Below the header, the text 'HKBN PROTECT' is displayed. The main content area is titled 'Log in' and contains two input fields: 'Email address' and 'Password'. Below these fields is a dark 'Log in' button and a link that says 'Forgot your password?'.

(Image 2)

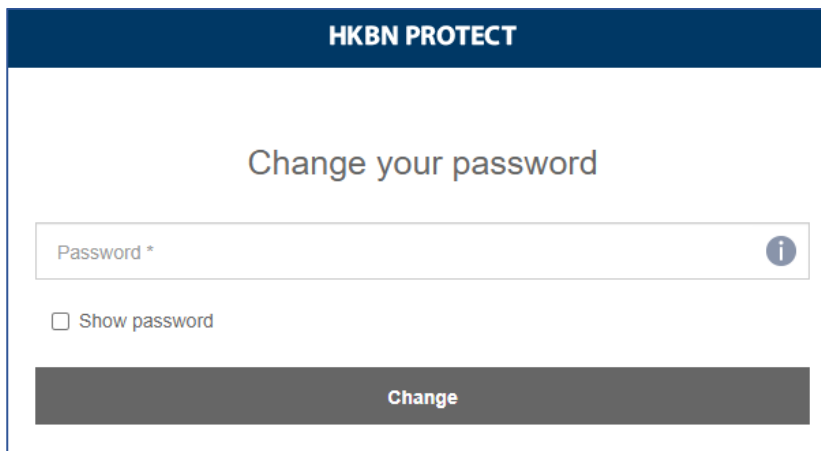


The screenshot shows the 'Change your password' page of the HKBN PROTECT Management Portal. The header is identical to the previous image. The main content area is titled 'Change your password' and contains the following text: 'Please enter your email address and select Send.' and 'You will receive instructions on how to change your password.' Below this text is an input field labeled 'Email address: *'. At the bottom of the page, there are two buttons: 'Send' and 'Cancel'. A footer note states: 'This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply'.

(Image 3)



(Image 4)

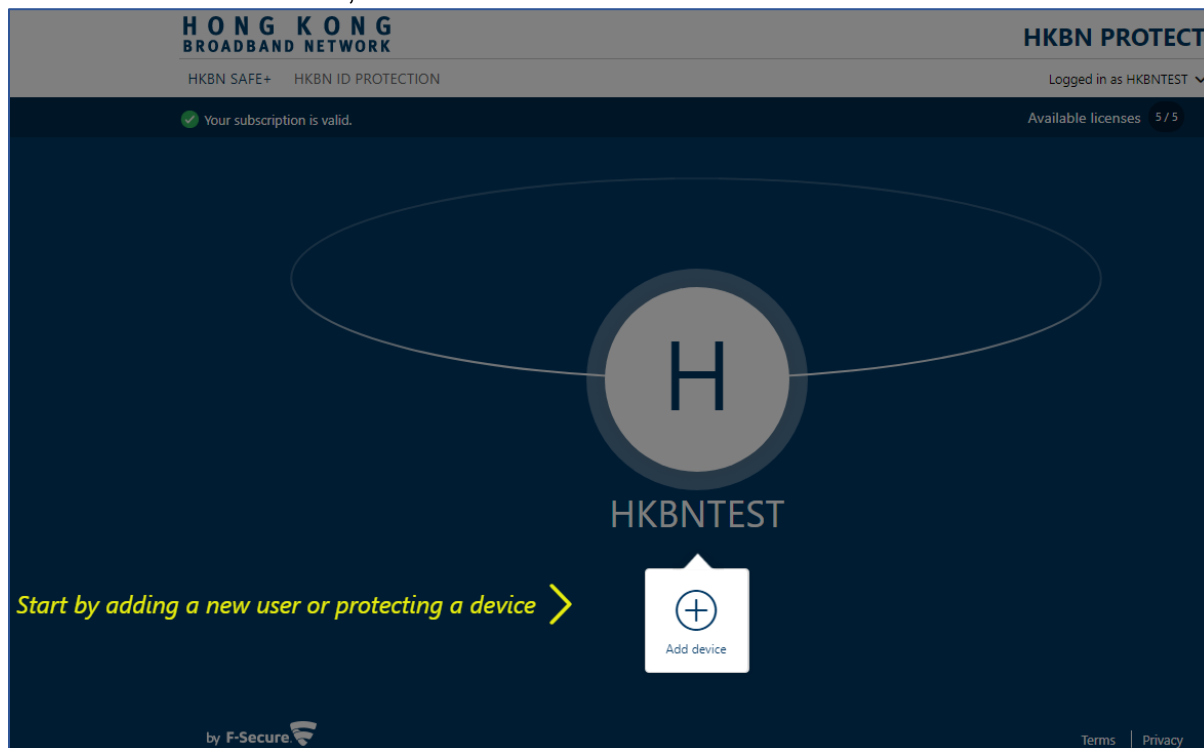


Getting started with HKBN SAFE+

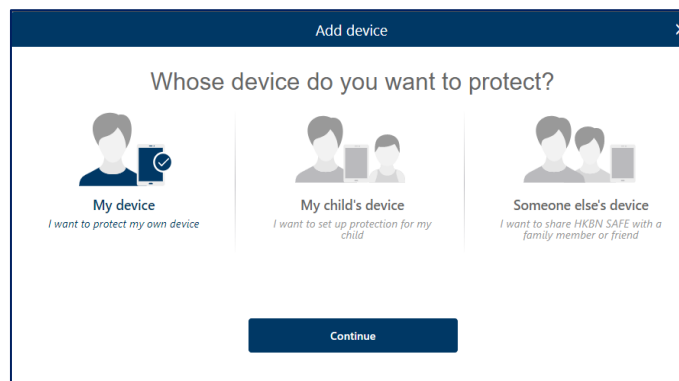
You can download and install HKBN SAFE+ through the HKBN PROTECT. You can also use HKBN PROTECT to send the product to a computer by email or mobile by SMS, making it easy for you to deliver HKBN SAFE+ to a device that you want to protect.

Add new device from HKBN PROTECT

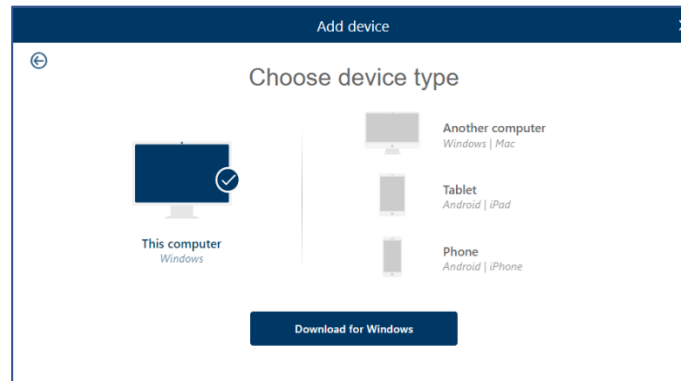
1. Login to HKBN PROTECT with your username and password.
2. Select **HKBN SAFE+**, click **Add device**.



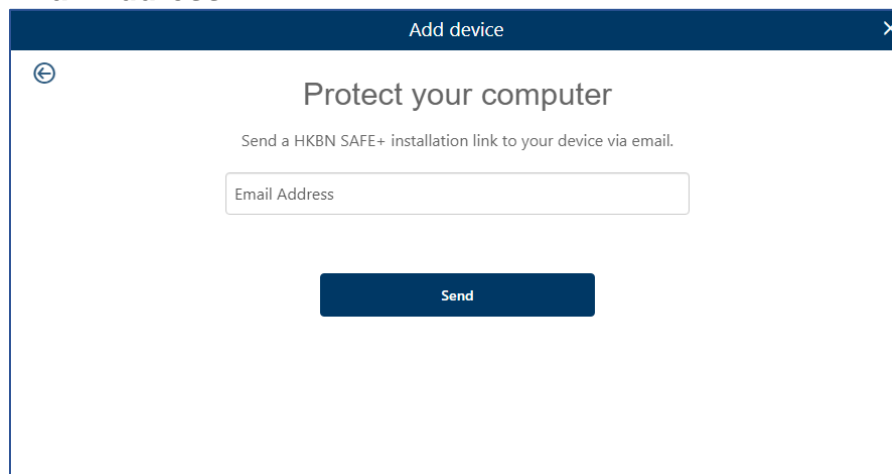
3. Choose whose device do you want to add, select **My Device** (If install to your own devices) and then click **Continue**.



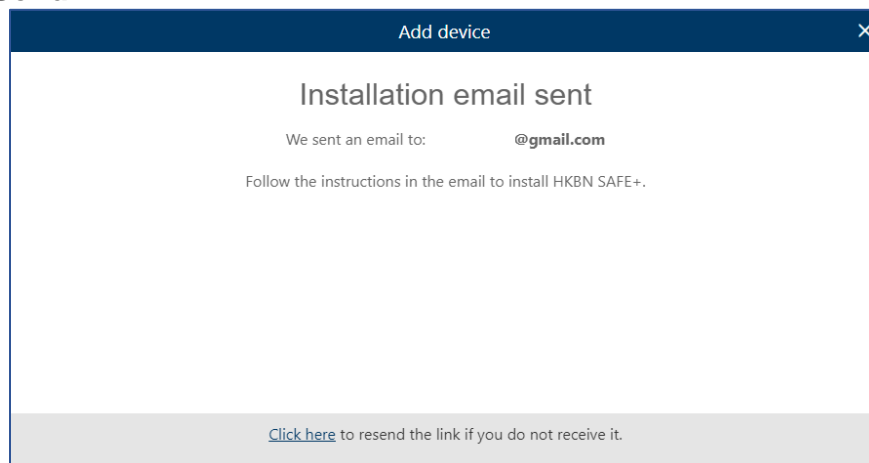
4. Select **This device** to install HKBN SAFE+ on your current device, then select **Download** then start the installation.



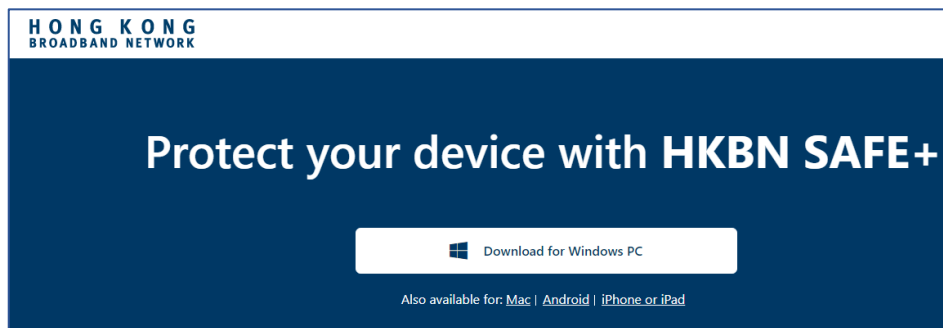
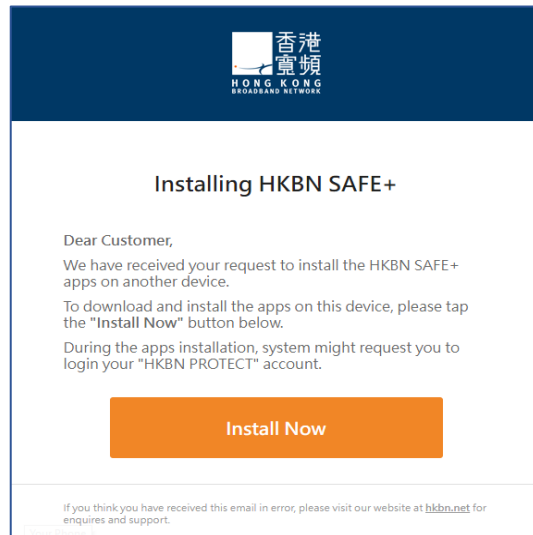
5. To install the product on a different device:
 - a. Select the device type and then select **Continue**.
 - b. Key in **Email Address**



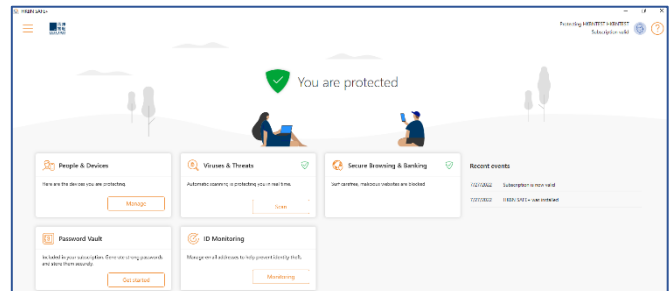
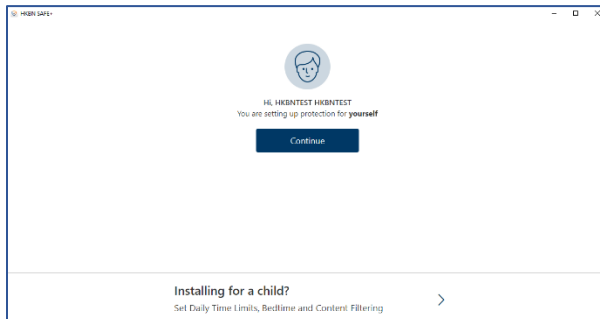
- c. Select **Send**.



- d. Follow the installation instructions that are sent to the email.



6. After the installation is complete, choose **Open** to start the application and to activate the product. The product does not protect your device before you activate it.



Sharing protection with a family or friend

When you invite family members or friends to your group, the invited persons get their own user account that allows them to protect their devices using your licenses. To share protection with someone else:

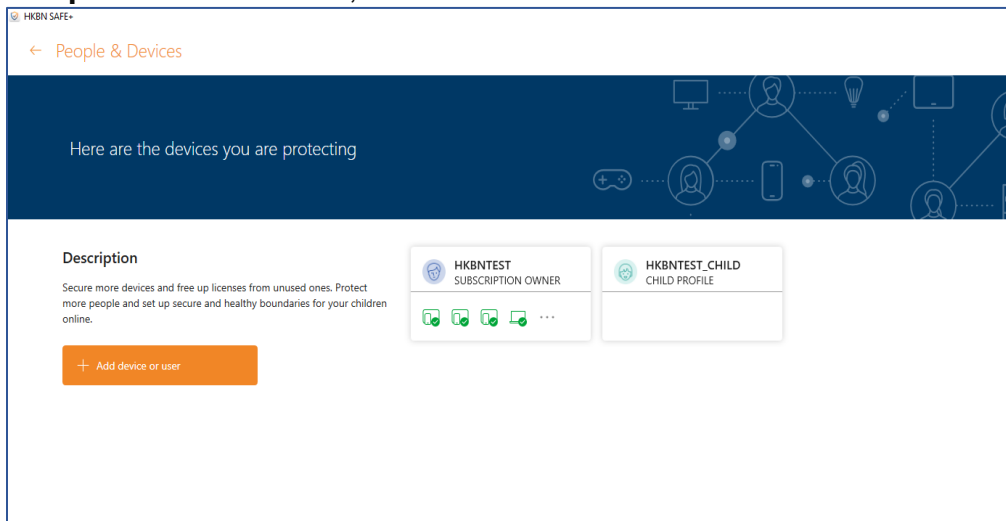
1. Login to HKBN PROTECT with your username and password. Select **HKBN SAFE+**, click **Add device**.

Or,

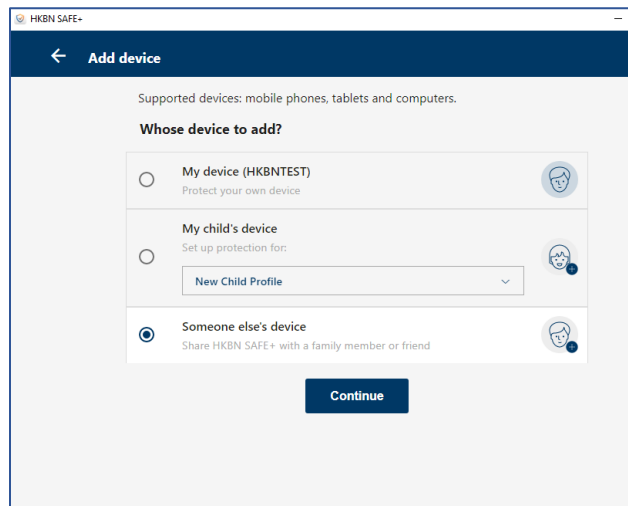
Open the HKBN SAFE+ from Windows Start menu

On the main view, select Manage in **People & Devices**.

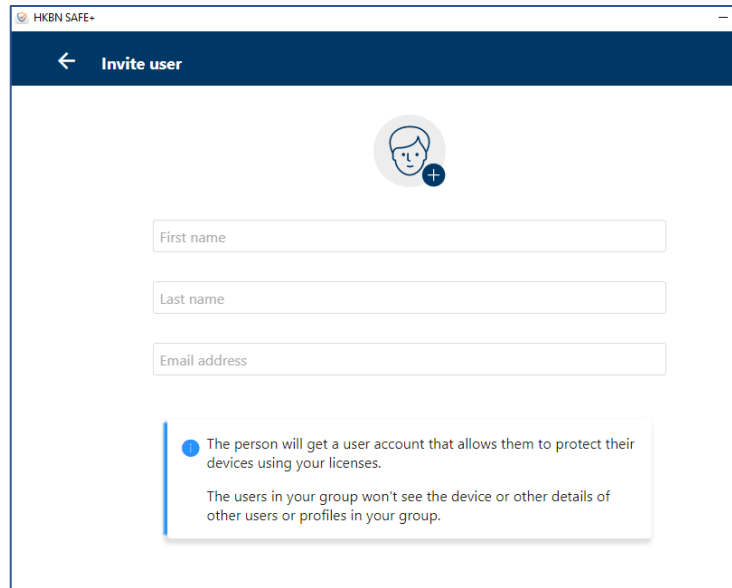
On **People & Devices** view, select **+ Add device or user**.



Select **Someone else's device** > CONTINUE



2. To invite a user to your group:
 - Enter the first name of the user.
 - Enter the last name of the user.
 - Enter the email address of the user.
3. Select **SEND INVITATION**.



HKBN SAFE

← Invite user

First name

Last name

Email address

• The person will get a user account that allows them to protect their devices using your licenses.
The users in your group won't see the device or other details of other users or profiles in your group.

4. This person receives the invitation email and now has an account that allows them to protect their devices using your licenses. The users in your group won't see the devices or other details of other users or profiles in the group.

Note that if the person you want to invite to your group has already been added to your group or belongs to another group, you will see a message in the invitation dialog, saying that the person already belongs to your group or to another group. This means that the email address used in the invitation has already been activated for an account. You can solve this either by using another email address, if any, to invite the user to your group or you can ask this user to delete the existing account after which you can then use the email address in the invitation.

Making browsing Internet safe for children with Family Rules

The Internet is full of interesting web sites, but there are also many risks for children who use the Internet. Children are at risk as they browse the web with their mobile devices, usually unsupervised.

Many web sites contain material that you might consider inappropriate for your children. They can get exposed to inappropriate material, they may accidentally download malware that could damage the mobile device, or they may receive harassing messages after browsing in unsafe web sites.

Family Rules helps you keep your children safe from unsuitable content when on the internet. With Family Rules, there are different ways that you can restrict your child's internet usage as follows:

- You can set time limits for daily use,
- You can set a bedtime,
- You can restrict the apps that your child has access to, and (For Android only)
- You can block certain types of content.

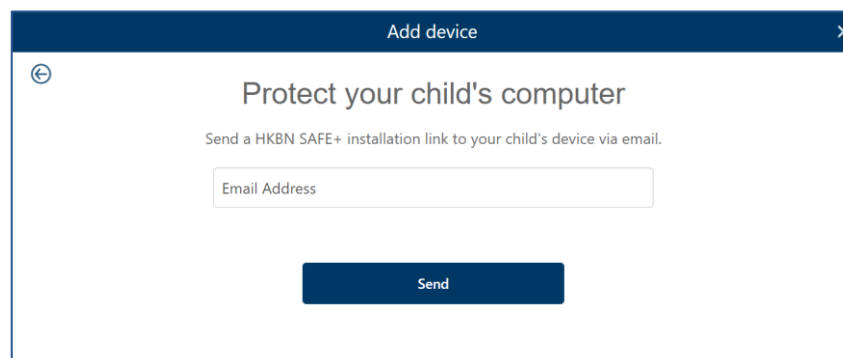
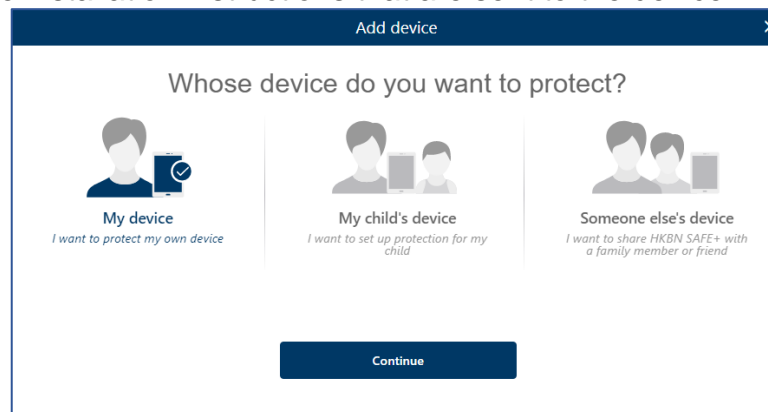
For ease of use, you can manage your child's online activity on your own device. This is a versatile way to make changes, add or remove restrictions on the fly without having your child's device physically with you.

Note: *The Family Rules settings can be edited only on the parent's People & Devices view or by logging in to the HKBN PROTECT.*

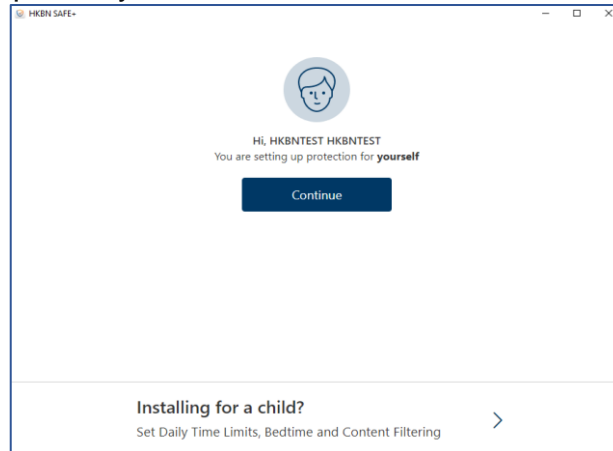
Adding a new device for children

To start using Family Rules, install HKBN SAFE+ on your child's device and set up a child profile. You can set up Family Rules when installing the HKBN SAFE+ app or any time afterwards. Once that's done, you can start protecting your child's online activity.

1. Login to HKBN PROTECT with your username and password. Select **HKBN SAFE+**, click **Add device**.
Or,
Open the HKBN SAFE+ from Windows Start menu
On the main view, select Manage in **People & Devices**.
On **People & Devices** view, select **+ Add device or user**.
2. Select **My Child's Device > Continue**.
3. Select **Send by SMS** and enter the phone number for the device. If the device does not have a phone number, select **Send by email** and enter an email address that you can access on the device. Select **Send**.
4. Follow the installation instructions that are sent to the device.

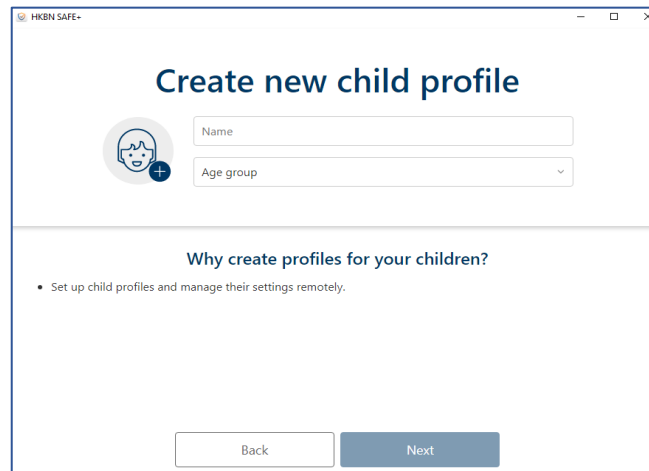


5. After the installation is complete, choose **Installing for a child?** You are prompted to set up Family Rules.



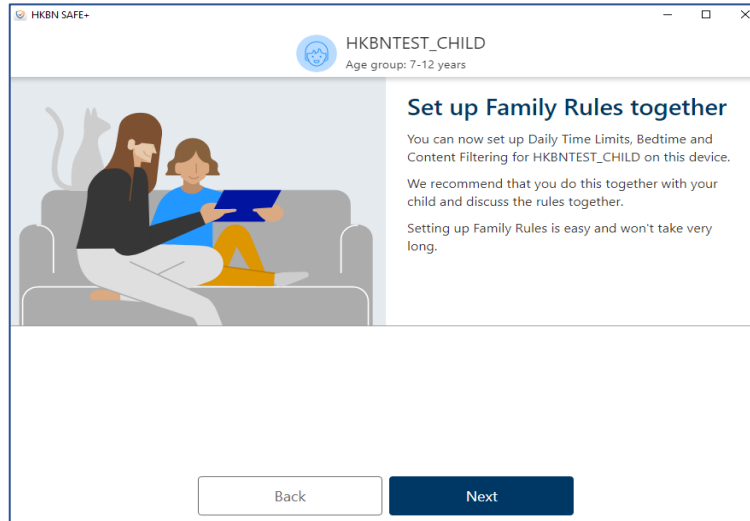
6. Select from existing profile listed or create new child profile, then follow the instructions shown onscreen to set up Family Rules.
- Enter the name of your child.
 - Select the age group your child belongs to.
 - Select Next.

Before you start setting up the Family Rules settings, discuss the family rules together with your child.



Setting up Family Rules for children

Under **FAMILY RULES**, check the different settings and edit them if need be:

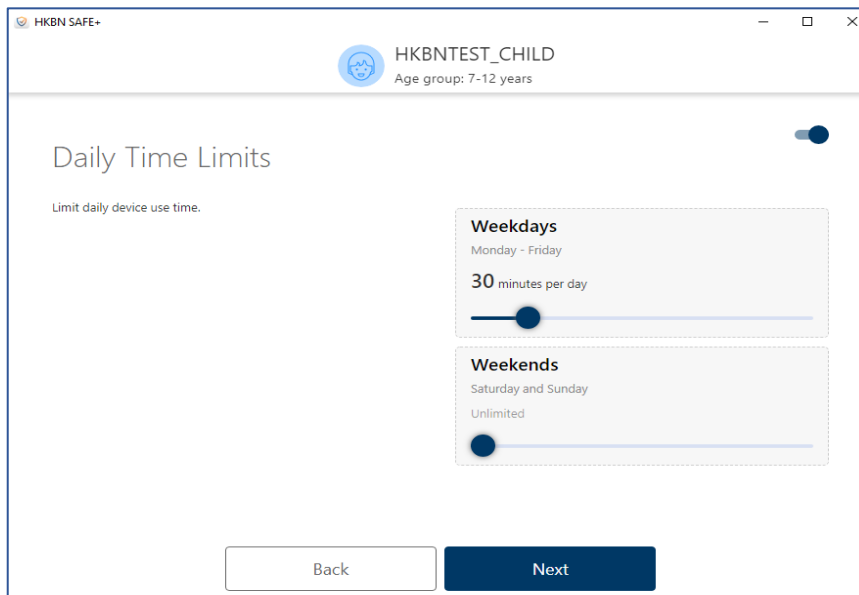


a. **Daily Time Limits**

You can control when and for how long the child can use the Internet. For example, you can allow access for only one hour per day. You can set different limits for weekdays and weekends.

To set the allowed times, open **Daily Time Limits** pane to set the maximum number of hours that the child is allowed to use the device each day.

If you do not want to limit the amount of time that the child spends on the device each day, make sure that the allowed number of hours is set to **Unlimited**.

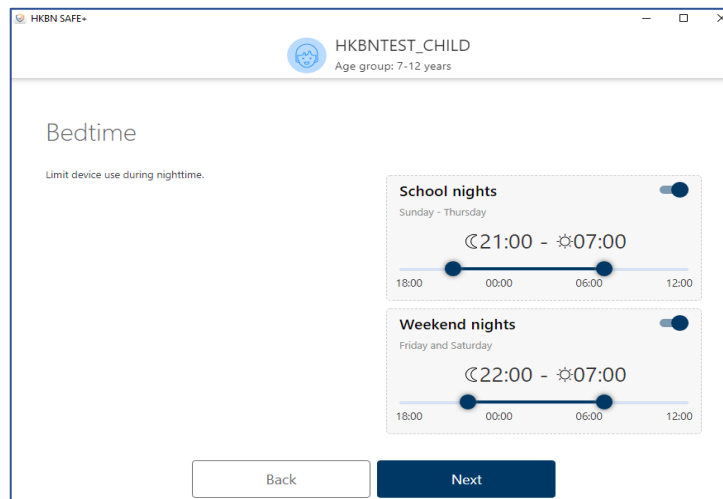


b. Bedtime

By setting a bedtime, you can ensure that your child gets to sleep when they should. For example, you can allow access only until 8 o'clock in the evening. Select **Edit** in the **Bedtime** pane to prevent the use of the device during night-time. You can set a different bedtime for weekdays and weekends.

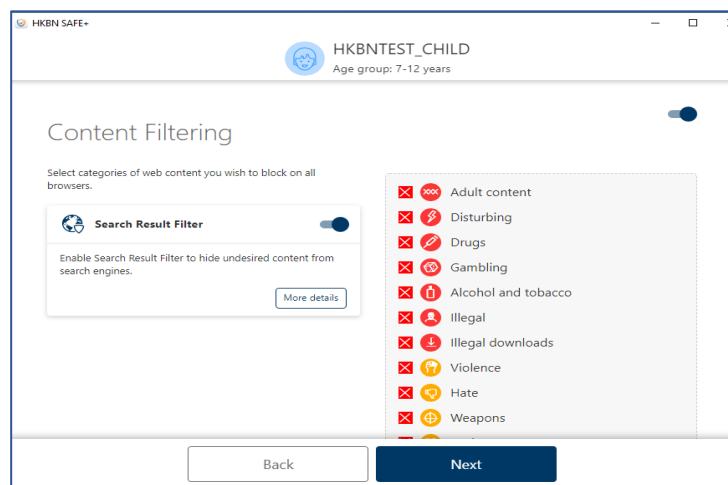
- To set the bedtime on weekdays, turn on **School Nights** and set the time when the bedtime starts and ends.
- To set the bedtime on weekends, turn on **Weekends** and set the time when the bedtime starts and ends.

Note: *If you remove the time limits, your child can use the computer at any time.*



c. Content Filtering

You can block access to web sites and pages that contain unsuitable content, keep your children safe from the many threats of the Internet by limiting the types of content they can view while browsing the web.



Web Content types in Content Filtering

You can choose to block multiple web content types at the same time.

Adult content	Websites that are aimed at an adult audience with content that is clearly sexual or containing sexual innuendo. For example, sex shop sites or sexually-oriented nudity.
Disturbing	Websites that contain images, explanations, or video games that can be disturbing. This category contains information, images and videos that are disgusting, gruesome or scary, which can potentially disturb younger children.
Drugs	Websites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.
Gambling	Websites where people can bet online using real money or some form of credit. For example, online gambling and lottery websites, and blogs and forums that contain information about gambling online or in real life.
Alcohol and tobacco	Websites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and websites of bars and night clubs.
Illegal	Websites that contain imagery or information that is banned by law.
Illegal downloads	Unauthorized file sharing or software piracy web sites. For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.
Violence	Websites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bomb, assault, murder, and suicide.
Hate	Websites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals or institutions, or contain descriptions or images of physical assaults against any of them.
Weapons	Websites that contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and bb guns.
Dating	Websites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.
Shopping and auctions	Websites where people can purchase any products or services, including sites that contain catalogs of items that facilitate online ordering and purchasing and sites that provide information on ordering and buying items online.

Social networks	Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.
Anonymizers	Websites that provide anonymous and untraceable communication via the Internet.
Unknown	Websites that are not categorized. You can use this category to block content that is unknown.

Protecting online banking and shopping

When Banking Protection is turned on, it automatically detects when you access online banking websites or other sites that contain sensitive information.

Banking Protection adds another layer of security to prevent attackers from interfering with your confidential transactions and protects you against harmful activity when you access your online bank or make transactions online. Banking Protection automatically detects secure connections to online banking websites and blocks any connections that do not go to the intended site.

Banking Protection currently supports the following web browsers:

- Safari (macOS)
- Firefox
- Google Chrome
- Microsoft Edge (Chromium)

Once you close the browser or finish the banking session, you do not have to do anything. **Banking Protection** automatically detects that the banking session is over and closes the **Banking Protection** frame.







By default, Banking Protection is enabled. If it is not enabled, turn on Banking Protection in the following way.

1. On macOS computer:
 1. Select the HKBN SAFE+ icon in the menu bar.
 2. Select **Preferences** from the menu.
 3. Select the **Secure Browsing** tab.
 4. Select the lock icon in the bottom-left corner.
Note: You need administrative rights to change these settings.
 5. Select **Turn on Banking Protection**.
2. On Windows computer:
 1. On the main view, select **Secure Browsing & Banking**.
 2. On the **Secure Browsing & Banking** view, select **Settings**.
 3. Select **Edit settings**.
Note: You need administrative rights to change the settings.
 4. Turn on **Banking Protection**.

Note: Banking Protection requires that browser extensions are in use.

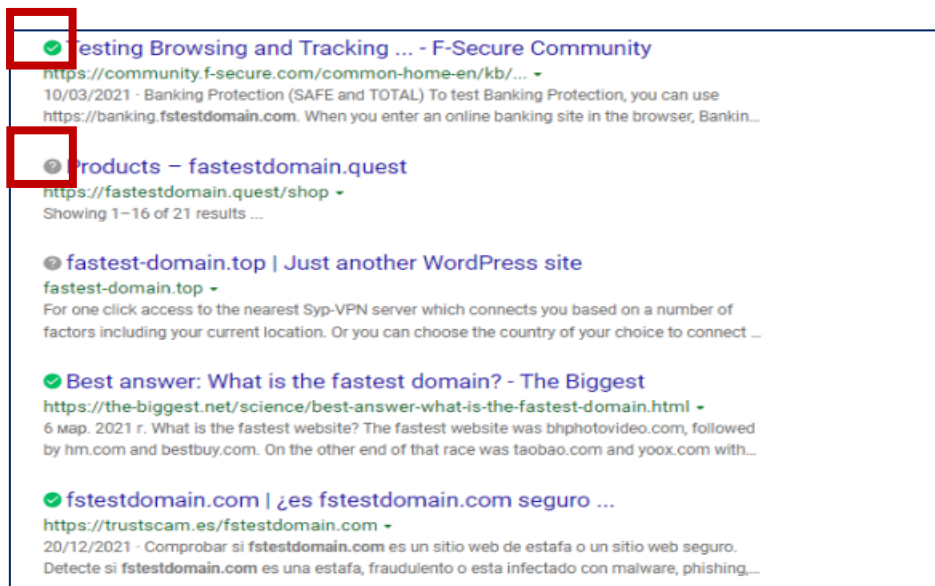
Browsing safely with Safety ratings

Browsing protection shows safety ratings for websites on search engine results. Color-coded icons show the safety rating of the current site. The safety rating of each link on search results is also shown with the same icons:

	The site is safe to the best of our knowledge. We did not find anything suspicious in the web site.
	The site is suspicious, and we recommend that you are careful when you visit this web site. Avoid downloading any files or providing any personal information.
	The site is harmful. We recommend that you avoid visiting this web site.
	We have not analyzed the web site yet or no information is currently available for it.
	The access to this web site is never blocked.
	Administrator has blocked this site and you cannot visit it.

Safety ratings are available on the following search sites:

- Google
- Bing
- Yahoo
- DuckDuckGo



Enabling browser extension for Safari/Chrome/Firefox (For Mac only)

You must enable the browser extension for Safari/Chrome/Firefox to be able to use the browser safely. The product installs the browser extension automatically, and the only thing you need to do is to make sure that the extension is turned on.

To ensure that the browser extension for Safari/Chrome/Firefox is turned on:

1. Select the product icon in the menu bar.
2. Select **Preferences** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.

The **Browsing protection installation** window opens.

5. From the drop-down, select **Safari/Chrome/Firefox** and then **Enable now**.
6. In **the Extensions** dialog, make sure that **Browsing protection** is selected.

You can now use Safari/Chrome/Firefox to browse the internet safely.

Checking that browser extensions are in use (Windows)

Browsing protection **requires** browser extensions to be able to protect your web browsing, online banking, and shopping, and to show you security information while you are browsing the internet. Therefore, make sure that the browser extensions are in use.

When you open your browser, it displays a notification about the newly installed extension, and you may need to enable it. If you miss the notification, the main view of the product shows you if the browser extension has not yet been set up. The easiest way to set up the extension for your browser is to select Set up from the notification shown on the product's main view and follow the on-screen instructions.

- If you use **Firefox**, select first **Install Firefox extension** under **Browser extensions** and then select **Add**. The extension will be added and enabled for Firefox.
- If you use **Chrome**, select first the **Open Chrome Web Store** link under **Browser extensions**. The Browsing Protection by F-Secure page opens in Chrome Web Store. If the extension has already been installed on Chrome but disabled, select the **Enable this item** link from the banner on top of the page. If the extension has not yet been installed, select **Add to Chrome > Add extension**. The extension will be added and enabled for Chrome.
- If you use **Microsoft Edge**, select first the **Open Edge Add-ons** link under **Browser extensions**. The Browsing Protection by F-Secure page opens in Edge Add-ons. If the extension has already been installed on Microsoft Edge but disabled, select **Turn on** to enable it. If the extension has not yet been installed, then select **Get > Add extension**. The extension will be added and enabled for Microsoft Edge.



Browsing protection by F-Secure

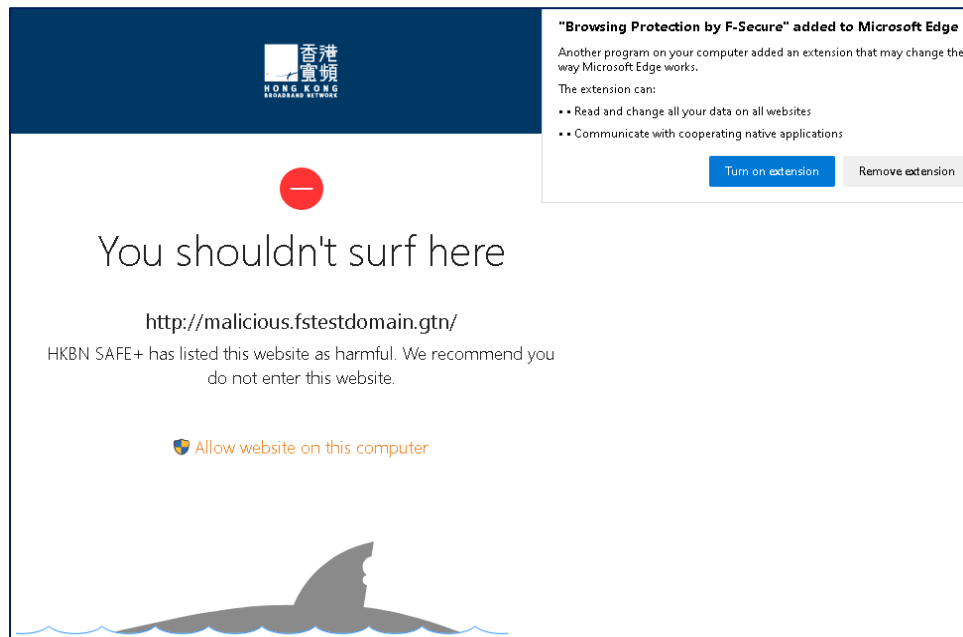
Offered by: F-Secure

Returning from or entering a blocked website

Sometimes you may browse to a website that contains suspicious, infringing, or prohibited content. For example, the website may be a fake, known spam site, contain potentially unwanted programs.

If you want to enter the website, select **Allow website on this computer > Allow**.

- Enter your administrator password and select **OK**.
- The blocked website opens. Also, the product adds the website to the allowed websites list.



Protecting your device against Virus & Threats

HKBN SAFE+ automatically scans your local hard drives, any removable media (such as portable drives or DVDs), and any content that you download. The product also watches your computer for any changes that may suggest that you have harmful files on your computer. When the product detects any dangerous system changes, for example changes in system settings or attempts to change important system processes, its DeepGuard component stops the application from running as it can be harmful.

Using real-time scanning

Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

We recommend that you keep Virus protection turned on all the time. You can also scan files manually and set up scheduled scans if you want to make sure that there are no harmful files on your computer or to scan files that you have excluded from the real-time scan.

To make sure that real-time scanning is on (Windows):

1. Open HKBN SAFE+ from the Start menu or your desktop.
2. On the main view, select “**Viruses & Threats**”.
3. Select “**Settings**”.
4. Select “**Edit settings**”.

Note: You need administrative rights to change the settings.

5. Turn on “**Virus Protection**”.

Running a virus scan manually

You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

The full computer scan scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete. You can also scan only the parts of your system that contain installed applications to find and remove unwanted applications and harmful items on your computer more efficiently.

For Windows, to scan your computer, follow these instructions:

1. Open HKBN SAFE+ from the **Start** menu.
2. On the main view of the product, select “**Viruses and Threats**”.
3. On the Viruses and Threats view, select either **Quick scan** or **Full computer scan**.
4. The scan starts.
5. If the virus scan finds any harmful items, it shows you the list of harmful items that it detected.
6. Click the detected item to choose how you want to handle the harmful content.

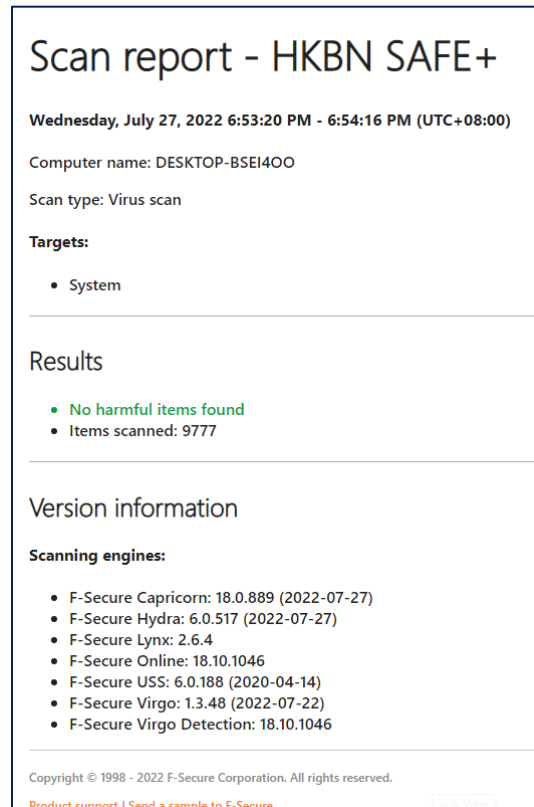
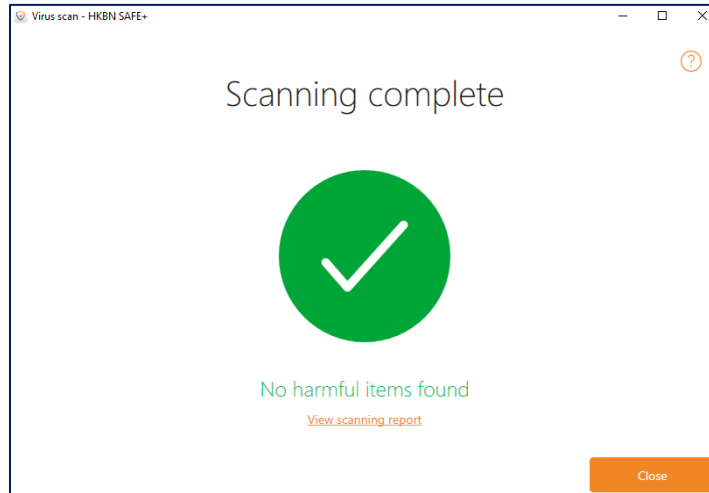
Options	Description
Clean up	Clean the files automatically. Files that cannot be cleaned are quarantined.
Quarantine	Store the files in a safe place where they cannot spread or harm your computer.
Delete	Permanently remove the files from your computer.
Skip	Do nothing for now and leave the files on your computer.
Exclude	Allow the application to run and exclude it from future scans.

Note: Some options are not available for all harmful item types.

7. Select Handle all to start the cleaning process.
8. The virus scan shows the results and the number of harmful items that were cleaned.

Note: The virus scan may require that you restart your computer to complete the cleaning process. If the cleaning requires a computer restart, select **Restart** to finish cleaning harmful items and restart your computer.

You can see the results of the latest virus scan by selecting Open last scanning report.



For macOS, to scan your computer, follow these instructions:

You can scan your Home folder or any location that you specify.

You can manually scan files or folders if suspect that they may contain malware. To start the manual scan:

1. Click on HKBN SAFE+ icon in the menu bar.
2. Select Choose what to scan.

Tip: Select Scan Home folder to scan all files in your Home folder.




A window opens in which you can select which location to scan.

3. Select the files or folders that you want to scan and then select Open. The scan starts. When the scan is completed, you can see the scan result in the scan window.
4. If the product finds any malware during the scan, it shows the name and location of the detected malware and moves the infected file to the Trash automatically.

Tip: Empty the Trash to remove infected files permanently.

Protection status icons

The protection status icon shows you the overall status of the product and its features.

Status icon	Status name	Description
	OK	Your computer is protected. Features are turned on and working properly.
	Warning	Your computer is not fully protected. The product requires your attention, for example it has not received updates in a long time or a security feature is turned off.
	Error	Your computer is not protected. The product requires immediate action, for example a critical feature is turned off or your subscription has expired.

Examples of status messages that you may see:

- **Google Chrome browser extension is not in use**
- **Mozilla Firefox browser extension is not in use**
- **Microsoft Edge browser extension is not in use**
- **Your subscription has expired**

Gaming Mode (Windows only)

Turn on the gaming mode when you want to free up system resources while playing computer games.

Computer games often require a lot of system resources to run smoothly. When you have other applications running in the background while you play a game, they degrade the performance of the game as they consume system resources and use your network.

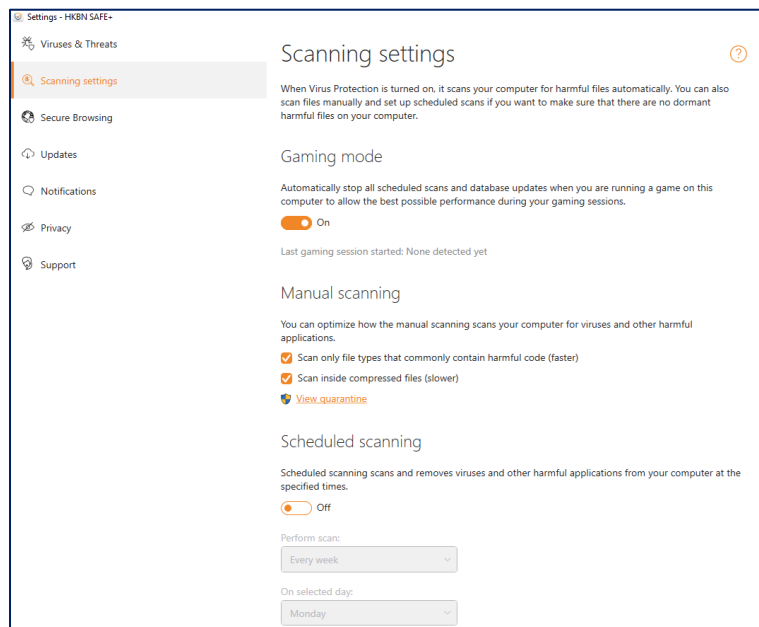
The gaming mode reduces the product's impact on your computer and reduces its network use. This way, it frees up more system resources for computer games while still maintaining the essential functionality of the product. For example, it suspends automatic updates, scheduled scans and other operations that may need a lot of system resources and network traffic.

When you use any full-screen application, for example when you are viewing a presentation, slideshow or video, or play a game in full-screen mode, we show only critical notifications if they require your immediate attention. Other notifications are only shown when you exit the full-screen or gaming mode.

In default, gaming mode is already on. You can check the setting via here:

1. Locate Viruses & Threats > Settings > Scanning Settings > Gaming Mode

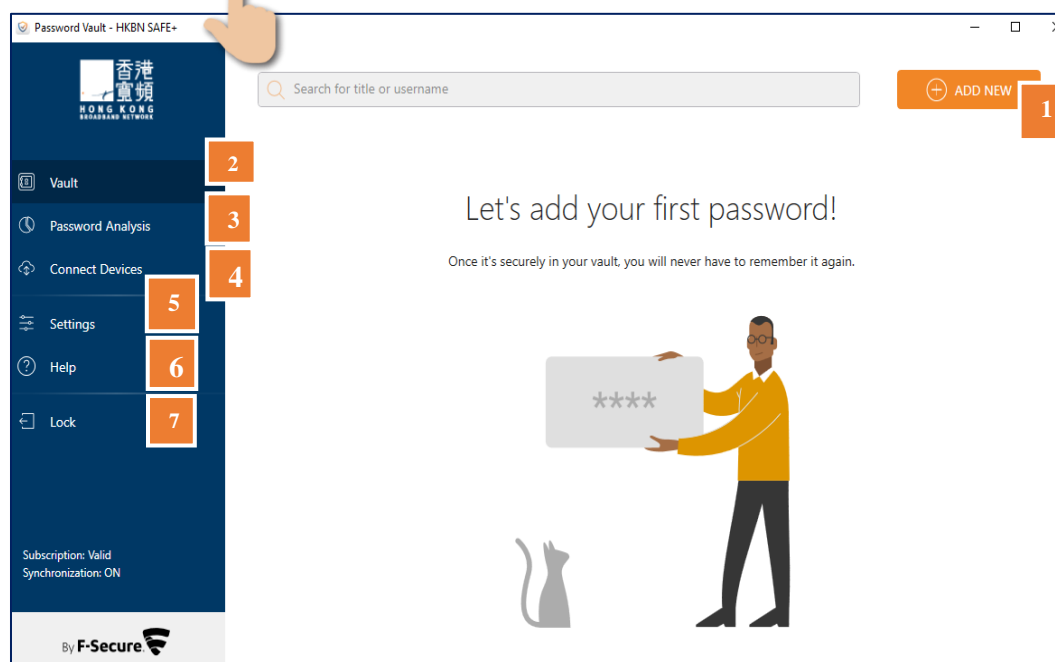
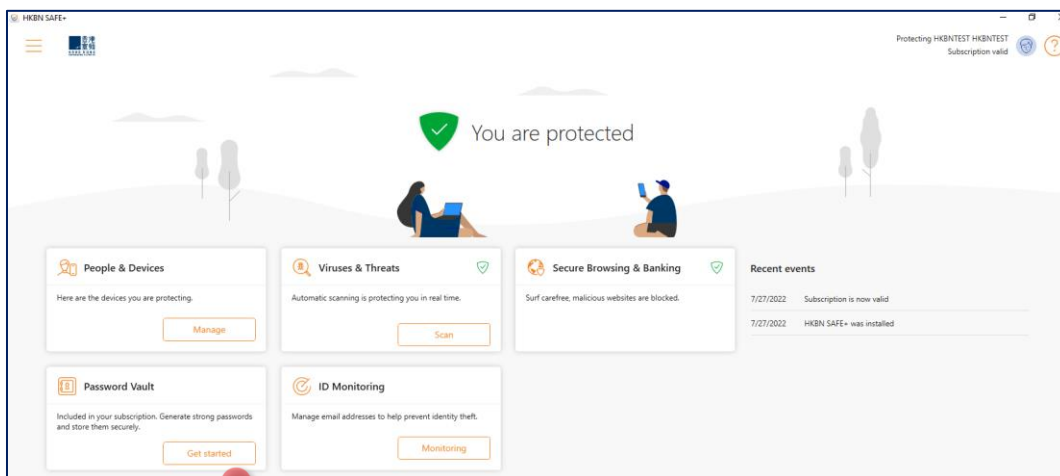
Tip: You need to have Administrator rights to change the settings.



Password Vault (Applicable to the subscription of ID PROTECTION Service)

With HKBN Safe+ Password Vault, you can create and edit password and payment card entries, let the app generate strong passwords for your online services, and access your password history.

1. Go to Password Vault
2. Choose I'm a new user if you are a new user, then create a master password (to unlock / restore all your saved credentials), and you can start to save your password / credit card for autofill purpose.
3. Choose I'm an existing user if you are existing user and you can sync all your saved credentials.



1. Add New to add new password / credit card
2. Vault to store and manage your password
3. Password Analysis to analyse your password strength
4. Connect Devices to sync across all your devices
5. Settings to configure setting for Password Vault
6. Help to look for assistance and system information
7. Lock to exit Password Vault

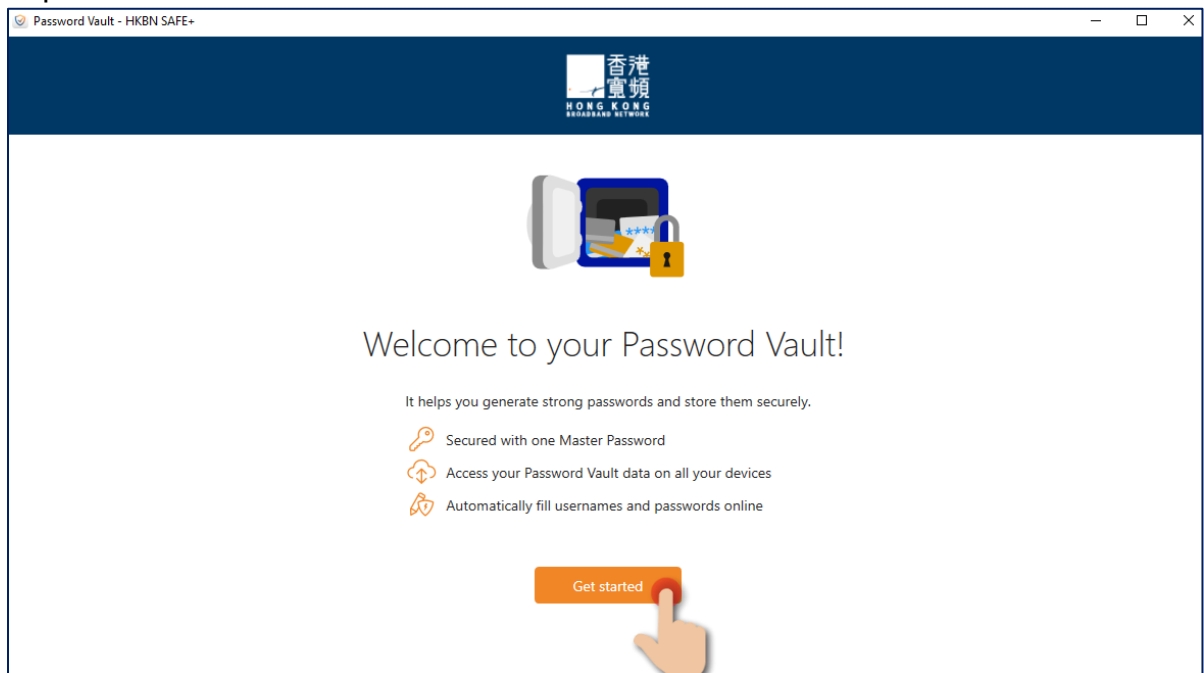
About Master Password

The master password is very important as it gives you access to the app and keeps your password data safe. Once you've installed HKBN Safe+ and you start the application for the first time, the app asks you to create a master password.

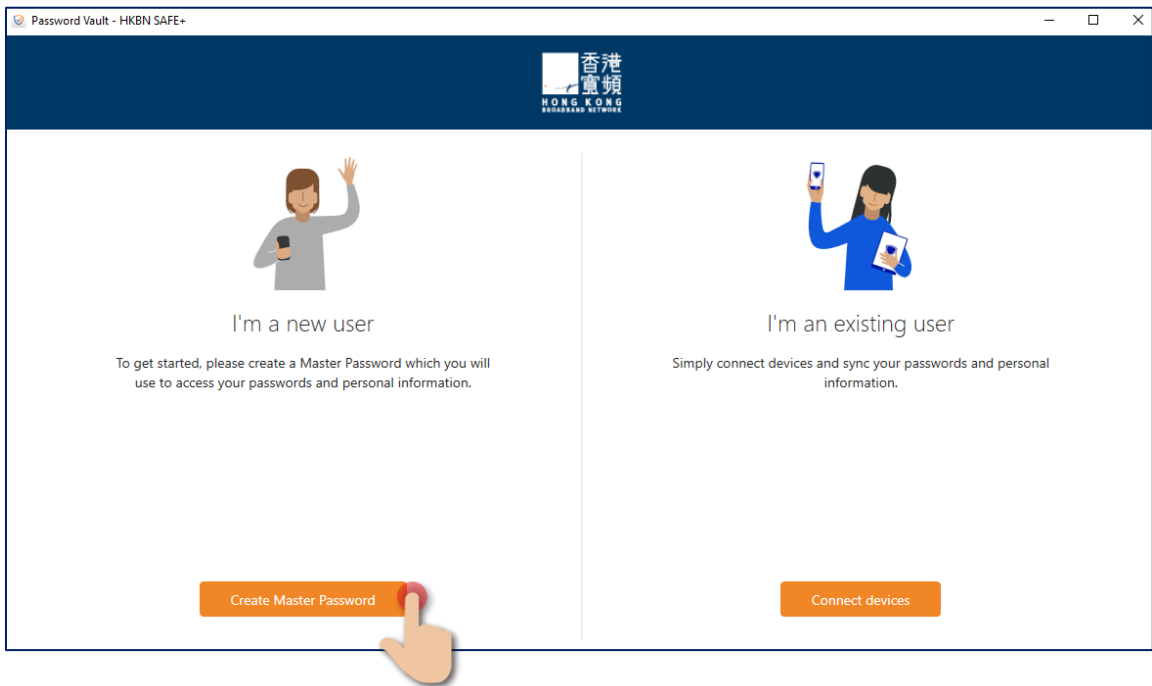
Choose a hard-to-guess master password or passphrase that you can remember, as the app is not able to reset your master password. The fact that the app cannot reset the master password has been a conscious decision by F-Secure to increase your security and privacy and protect your data.

Create HKBN Safe+ master password

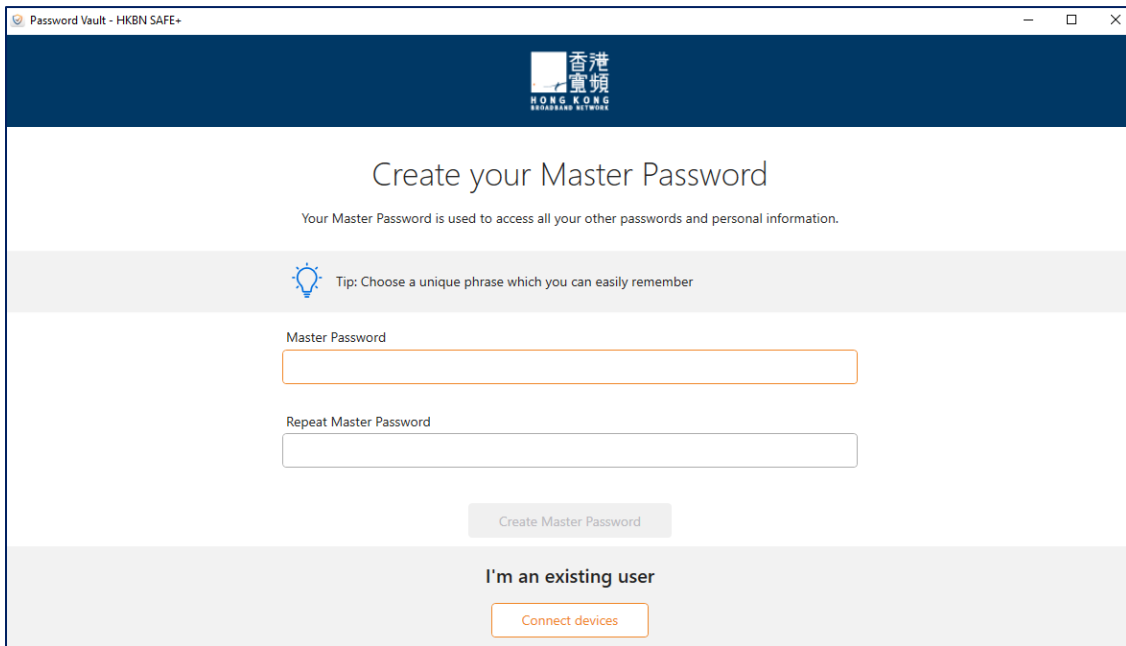
1. Tap “Get Started” to use Password Vault



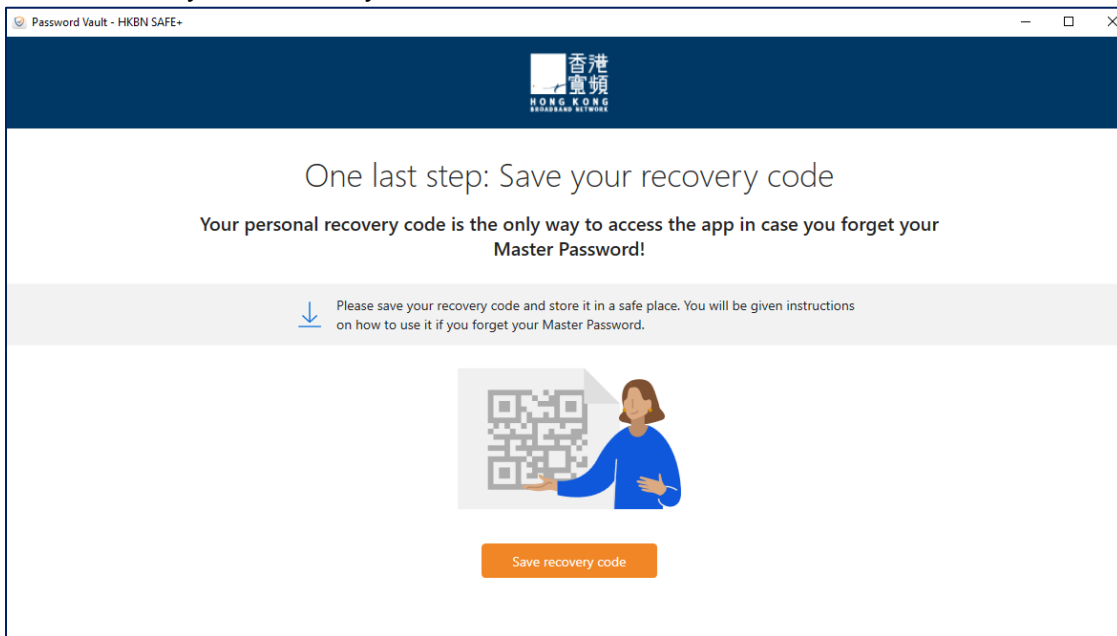
2. Choose “I’m a new user” and “Create Master Password”



3. Suggest to use strong master password and then tap “Create Master Password”.



4. Please save your recovery code.



Create and Save Master Password Recovery Code

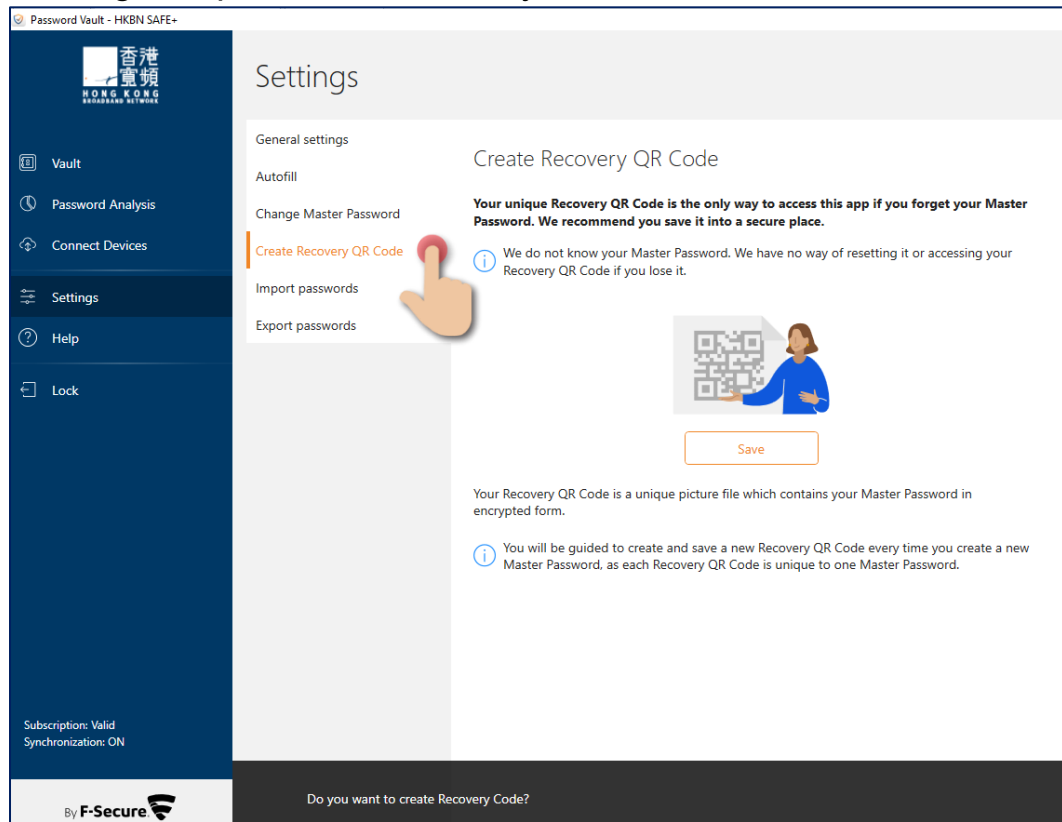
The master password recovery code is a unique and personal code that is the only way of regaining access to the app, should you forget your master password. We cannot restore any master passwords, as this would mean accessing your master password, which could be a security risk. It is strongly encrypted and can only be decrypted on one of your connected devices. This means that it cannot be decrypted on any other user device.

There are a few important things to note about the master password recovery code:

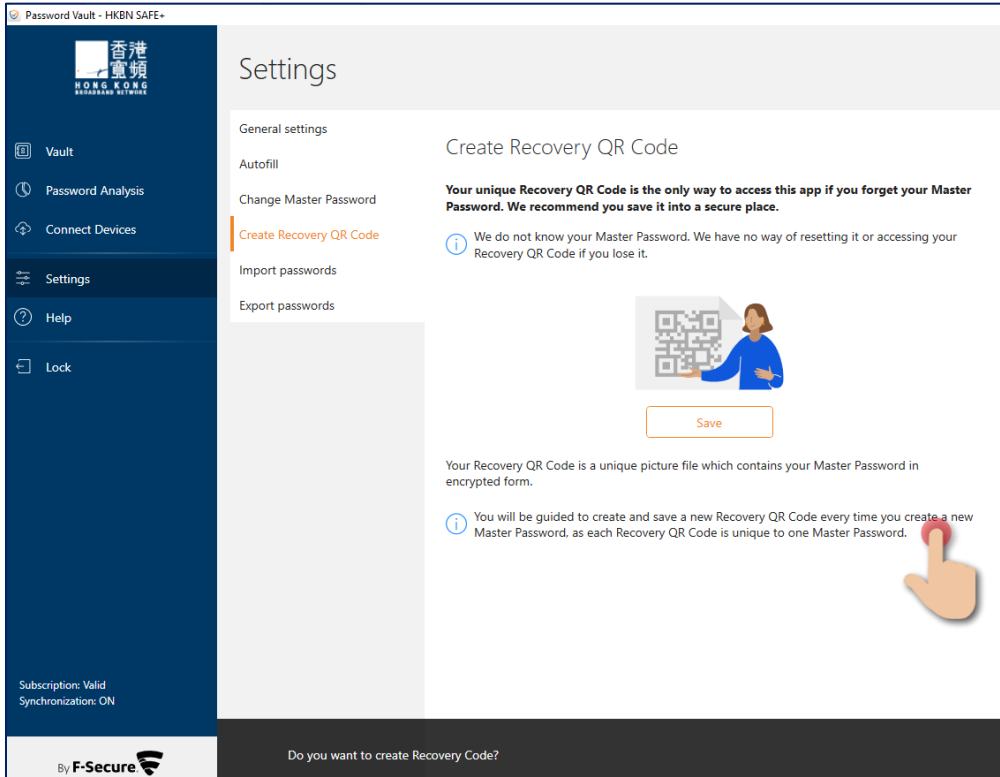
- Every time you change your master password, you need to create a new recovery code.
- You always need the latest recovery code to regain access to the app.
- If you connect new devices, the app may ask you to create a new master password recovery code. If this is the case, make sure you create a new master password recovery code, as the older code will not work anymore.
- We recommend saving the code as an image and print a copy for safekeeping. The master password recovery code printout should not be stored in the same location as your device.

Reminder: We strongly recommend that you also create a recovery code for the master password as soon as you have taken Password Vault into use. It is the only way for you to regain your master password if you forget it.

1. In “Settings”, tap “Create Recovery Code”.



2. Tap “Save as image” and save this Recovery Code image and print and store it in a safe place.

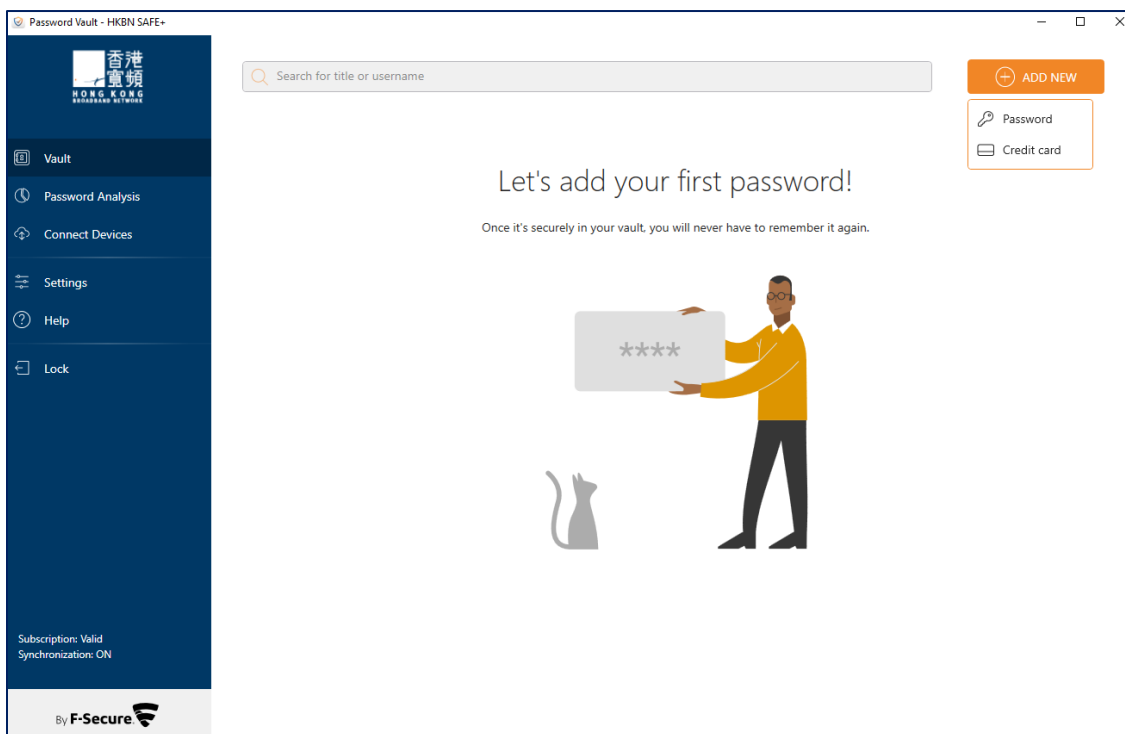


Vault

With HKBN Safe+, you can create and edit password and payment card entries, let the app generate strong passwords for your online services, and access your password history.

Create and Save your Password or Create Card Information

1. Click “Vault”;
2. Click “Create your first password”;
3. Select “Password” or “Credit Card”.

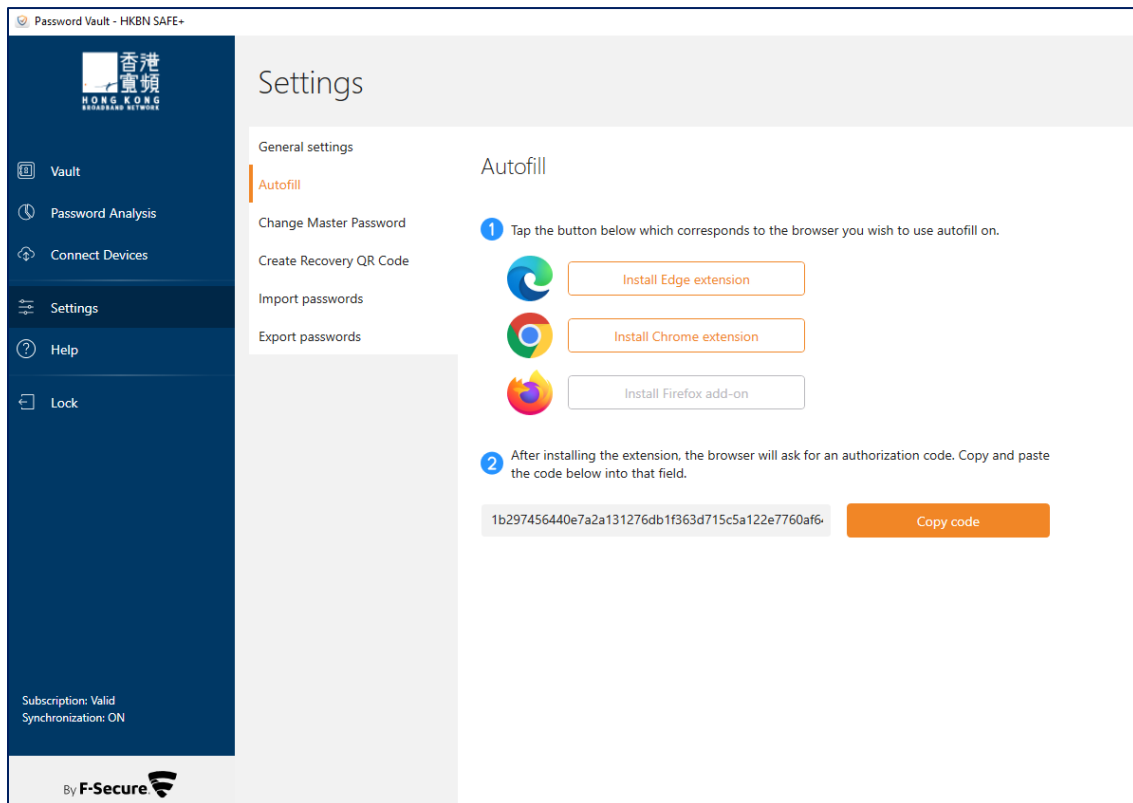


Using Autofill

With the Autofill feature, you can log in to apps and websites without needing to enter usernames and passwords manually.

You need to have the username, password and web address of the service saved in HKBN Safe+ for Autofill to work. When you log in to an app or website with credentials that are saved in Password Vault, you can have the app enter your username and password automatically.

1. Open Password Vault
2. Go to **Settings > Autofill**
3. Under **Autofill**, select and install the extension according to your browser preference, follow on screen instruction and copy authorization code.



Connect Devices

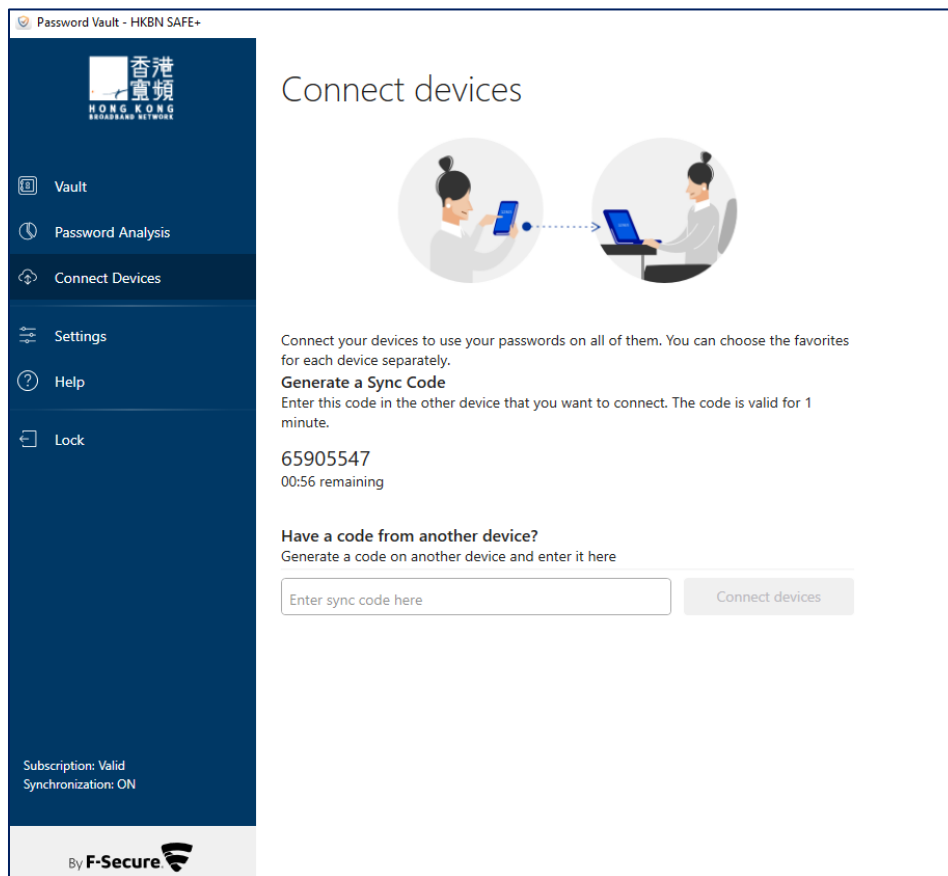
You can connect your devices to synchronize your Vault data across them all.

To be able to sync your Vault data across all your devices, you need to connect the devices that have the HKBN Safe+ app installed.

Warning: *If you only have the app on one mobile device and you carry out a factory reset, the reset wipes also all your Vault data from the device. After this, there is no way to get the data back.*

1. On device A, select “Connect devices” to generate a Sync Code;

Remark : *Synchronize passwords will be renew every 60 seconds.*

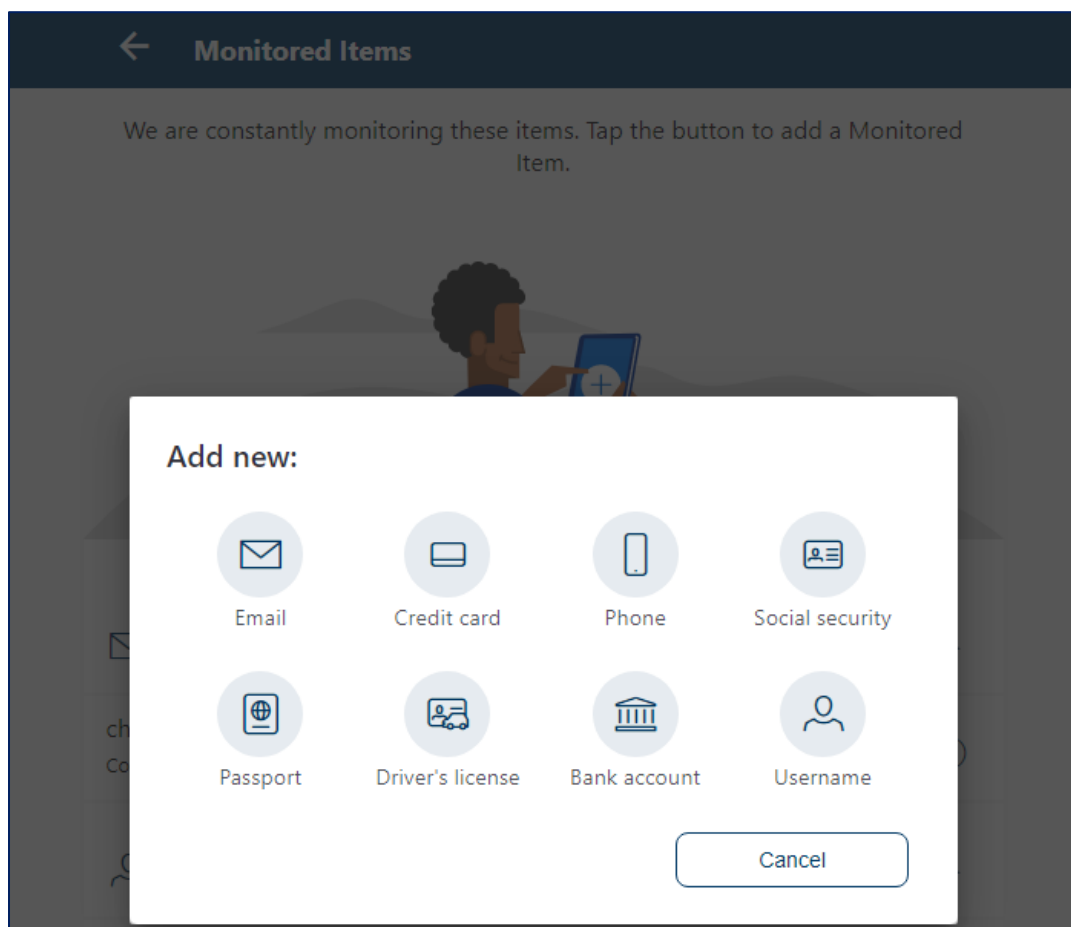


On device B, select “Connect devices” and enter this sync code and then click “Connect”.





ID Monitoring (Applicable to the subscription of ID PROTECTION Service)

With HKBN Safe+ ID Monitoring, you can add items for monitoring and receive guidance on what to do if your personal information has been leaked in a data breach.





The notification email includes information on what personally identifiable information (PII) has been associated with the breach; what the breach was; what company or entity was breached; when the breach took place; and what other pieces of PII has been associated with the monitored email address, such as passwords, credit card numbers, street address, and so on.



HKBN SAFE+ features per platform

	 PC	 Mac	 Android	 iOS
Malware Protection	●	●	●	-
Virus Scanning	●	●	●	-
Advanced Ransomware Protection	●	-	-	-
Browsing Protection	●	●	●	●
Banking Protection	●	●	●	●
Family Rules – Remote Management	●	●	●	●
Family Rules – Content Filtering	●	●	●	●
Family Rules – Daily Time Limits	●	●	●	-
Family Rules – Bed Time	●	●	●	●
Family Rules – App Control	-	-	●	-
Management Portal - (HKBN PROTECT)	●	●	●	●
In-App Management - "Peoples & Devices" view	●	●	●	●

HKBN Safe+ Password Vault and ID Monitoring Features Per Platform

	 Windows	 macOS	 Android	 iOS
Supported OS versions	Windows 7 (SP1) and later	Mac OS X 10.1 and later	Android 6 or later	iOS 13 or later
ID Monitoring	•	•	•	•
Breach alerts	•	•	•	•
Breach guidance	•	•	•	•
Secure password storage	•	•	•	•
Password import/export	•	•	-	-
Password generation	•	•	•	•
Password quality analysis	•	•	•	•
Login: Master password	•	•	•	•
Login: Fingerprint/Face	-	-	•	•
Login: QR Recovery Code	•	•	•	•
Password Synchronization	•	•	•	•
System/ app autofill	•	•	•	•
Auto-fill in Browsers	•	•	•	•
Supported browsers for auto-fill	Firefox, Chrome	Firefox, Chrome	SAFE Browser, Firefox, Chrome, Opera, Edge	At least Safari, Chrome

Technical Support

Here you can find information that can help you solve your technical issues.

Using the support tool

Before contacting support, run the support tool to collect basic information about hardware, operating system, network configuration and installed software.

- To run the support tool on Windows computer:
 1. Open HKBN SAFE+ from the Windows **Start** menu.
 2. On the main view, select the ☰ menu button.
 3. Select **Help & Support**.
 4. Select **Edit settings**.
Note: You need administrative rights to change the settings
 5. Select **Run support tool**.
 6. Select **Run diagnostics** on the **Support Tool** window.
- To run the support tool on Mac computer:
 1. Go to HKBN SAFE+ folder under **Applications** and run the **Support Tool** application.
 2. Select **Run Diagnostics** on the **Support Tool** window.
 3. Enter the administrator password for your computer.
The support tool starts and displays the progress of the data collection.
 4. When the data collection is complete, select where you want to save the resulting **tar.gz** archive and then select **Save**.
The support tool opens a **Finder** window showing the saved file.
 5. Send the file to customer support when you are asked for it.
Note: You need administrative rights to change the settings

The support tool starts and displays the progress of the data collection. When the tool has finished running, it saves the collected data to an archive on your desktop. You can provide the collected data (the diagnostics file) when contacting customer support.

Contact us

Should you have any query, please email to HKBNBroadband@hkbn.net