



HKBN SAFE+

應用程式快速使用指南

(iOS/Android)



目錄

HKBN SAFE+ 簡介	3
流動裝置的系統需求	3
歡迎電郵	4
HKBN PROTECT (管理平台)	5
HKBN PROTECT 帳戶	5
首次登入帳戶	6
忘記密碼	7
下載及安裝 HKBN SAFE+ 應用程式	8
於 HKBN PROTECT 新增裝置	8
邀請家人或好友	11
確保孩子安全地使用互聯網	13
新增子女的裝置	14
為子女的裝置設定家長控制	16
封鎖網頁內容類別	19
在孩子的裝置上停用 Safari (只適用於 iOS)	20
在裝置上刪除其他瀏覽器 (只適用於 iOS)	20
安全瀏覽	21
HKBN SAFE+ 安全瀏覽器	21
網上銀行保護	22
從封鎖網站返回或進入封鎖網站	23
病毒和威脅保護	24
病毒掃描及移除 (只適用於 Android)	24
應用程式通知 (僅適用於 Android 系統)	26
密碼庫	27

有關主密碼.....	28
建立密碼庫主密碼.....	28
建立及儲存主密碼恢復代碼.....	28
密碼管理員 (保管庫).....	30
建立和儲存您的密碼或信用卡.....	30
自動填寫功能.....	31
裝置連線 (同步保管庫).....	32
監控線上身份.....	33
HKBN SAFE+ 不同平台的功能比較	34
HKBN Safe+ 密碼庫及 監控線上身份不同平台的功能比較.....	35
聯絡技術支援.....	36
發送記錄檔給支援部門.....	36
聯絡我們.....	36

HKBN SAFE+ 簡介

HKBN SAFE+ 是一款全面的網絡安全服務，一個訂閱即可為多部裝置提供由 F-Secure 支援並屢獲殊榮的保護服務。HKBN SAFE+ 透過防禦電腦、智慧手機或平板電腦上的網絡安全威脅，從而保護你自己及家人。

在您的所有裝置上安裝 HKBN SAFE+ 應用程式，以保護您的安全和私隱。HKBN SAFE+ 支援 Windows、Mac、Android 和 iOS 各作業系統。並能在瀏覽互聯網時保護您和您的親人，其技術如下：

- 「瀏覽保護」（在移動平台上被稱為「安全瀏覽」），它使用先進的雲端網路信譽檢查來驗證網頁，並確保只有安全的網站才能被瀏覽。
- 「銀行保護」，當你進入網上銀行網站時，透過存取線上銀行入口網站時的連線安全，來保護您的網上銀行活動。

HKBN SAFE+ 整合了嶄新服務 - IDP 個人身份保護。

在第三方平台例如購物網站、會員網站等申請服務時無可避免地需要填上不同的個人資料，當那些機構被黑客入侵而導致資料外洩，“IDP 個人身份保護”都能於暗網及其他渠道密切監察你的個人資料有否被黑客利用，並馬上以電郵通知情況，另提供加密密碼管理器，幫你產生一個強大的密碼免受黑客持續入侵。

流動裝置的系統需求

HKBN SAFE+ 支援以下運行的智能手機和平板電腦：

- 支援的 Android 系統版本: Android 8.0 或更高版本的智能手機和平板電腦。該應用程式的安裝需要約 75MB 的可用存儲空間，並只能安裝在裝置的內部記憶體中。啟動和更新需要連接互聯網。
- 支援的 iOS 系統版本: iOS 15.0 或更高版本的智能手機和平板電腦。用戶端應用程式的安裝需要大約 20-30 MB 的可用磁碟空間。

歡迎電郵



開始啟用「HKBN PROTECT」

親愛的 HKBNTTEST：

多謝您選用香港寬頻網絡有限公司（「香港寬頻」）服務。

您的「HKBN PROTECT」服務已成功啟用，服務計劃包括以下應用程式：

- HKBN SAFE+

開始保護您的裝置，您可按下面的按鈕去下載並安裝所需的應用程式。

您可使用以下的電郵地址去安裝「HKBN PROTECT」的應用程式：

電郵地址：[@f-secure.com](mailto:>@f-secure.com)

服務設有管理平台，讓您可集中輕鬆管理不同產品及裝置，例如邀請和轉換使用授權給家人、進行家長管理設定及尋找裝置等。

[按此](#)進入服務管理平台

HKBN SAFE+

為您及您家人的裝置提供網絡安全防護及24小時主動偵測個人資料有否外洩。

可供 20 部裝置使用

[立即安裝 HKBN SAFE+](#)

[按此](#)參閱「HKBN SAFE+」用戶指南

歡迎電郵內的重要資訊

- 用戶名稱 (電郵地址)
- 臨時密碼
- 授權資訊
- 登入 HKBN PROTECT 管理平台
- 應用程式下載連結
- 用戶指南下載連結

HKBN PROTECT (管理平台)

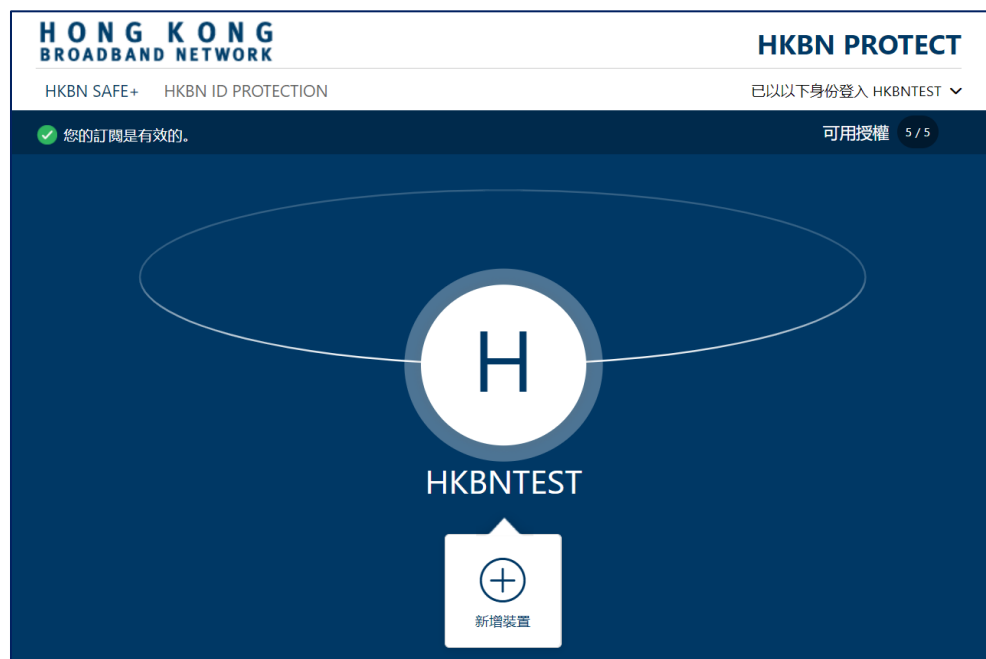
HKBN PROTECT 提供線上管理服務平台，你可以用來將 HKBN SAFE+ 遠端安裝到你選定的裝置上並管理你的訂閱。

透過 HKBN PROTECT 管理平台或手機應用程式中的「人員和裝置」概覽，您可以看到所有通過訂閱保護的人及其裝置的概況。要查看某位使用者的詳細資訊，只需選擇該使用者，就會打開一個針對該用戶的概覽，讓你瞭解該使用者的保護情況。

您可以通過 HKBN PROTECT 隨時方便地將 HKBN SAFE+ 從一台裝置安裝到另一台裝置上。

HKBN PROTECT 帳戶

登入帳戶後，您即可管理服務、檢視訂閱狀態以及將家庭成員添加至您的 SAFE 圈子(用戶群組)。



點擊以下連結進入 My HKBN PROTECT 管理平台：

<https://ihome2.hkbn.net/fsecureuser>

首次登入帳戶

1. 使用您的用戶名稱 (電郵地址) 和臨時密碼登入 HKBN PROTECT ；
2. 首次登入系統會要求使用者更改密碼，輸入新的密碼；
3. 隨後便開始使用 HKBN PROTECT 。

香港寬頻 HONG KONG BROADBAND NETWORK

HKBN PROTECT - 管理平台

用戶指南 ENG | 繁

HKBN PROTECT

登入

電子郵件位址

密碼

登入

[忘記密碼?](#)

忘記密碼

如果您忘記了 HKBN PROTECT 的帳戶密碼，可以通過找回密碼的流程建立新密碼：

1. 點擊「忘記密碼」(圖 1)；
2. 輸入您註冊使用的電郵地址，點擊「傳送」。系統會向所註冊的電郵發出變更密碼的連結(圖 2)；
3. 點擊電郵中的連結(圖 3)；
4. 輸入新密碼(圖 4)。

(圖 1)



(圖 2)



(圖 3)



(圖 4)



下載及安裝 HKBN SAFE+ 應用程式

登入 HKBN PROTECT 下載和安裝 HKBN SAFE+，亦可以使用 HKBN PROTECT 發送電子郵件或SMS 短訊至您的裝置，在要保護的裝置上安裝 HKBN SAFE+。

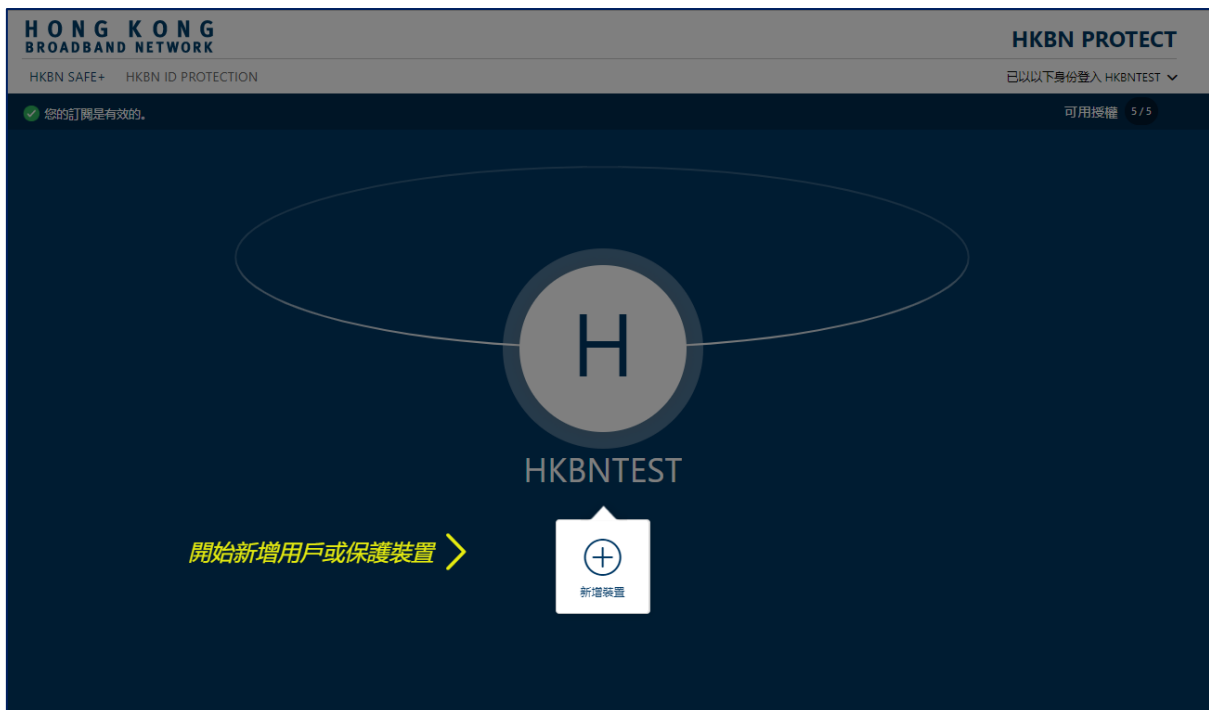
下載應用程式

- 到 Apple 的 App Store 或 Google 的 Play Store 上搜尋「HKBN SAFE+」下載並安裝應用程式



於 HKBN PROTECT 新增裝置

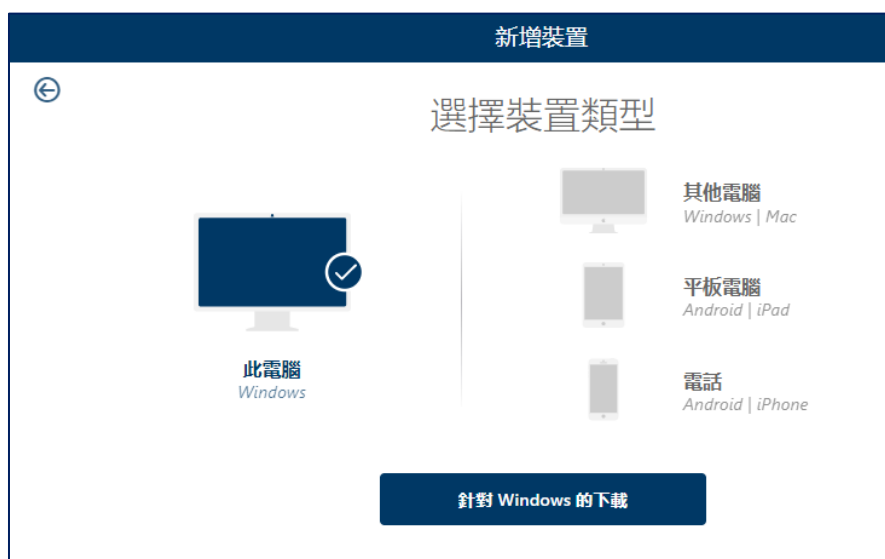
1. 使用您的用戶名稱和密碼登入 HKBN PROTECT；
2. 在 HKBN PROTECT 版面，選擇「新增裝置」；



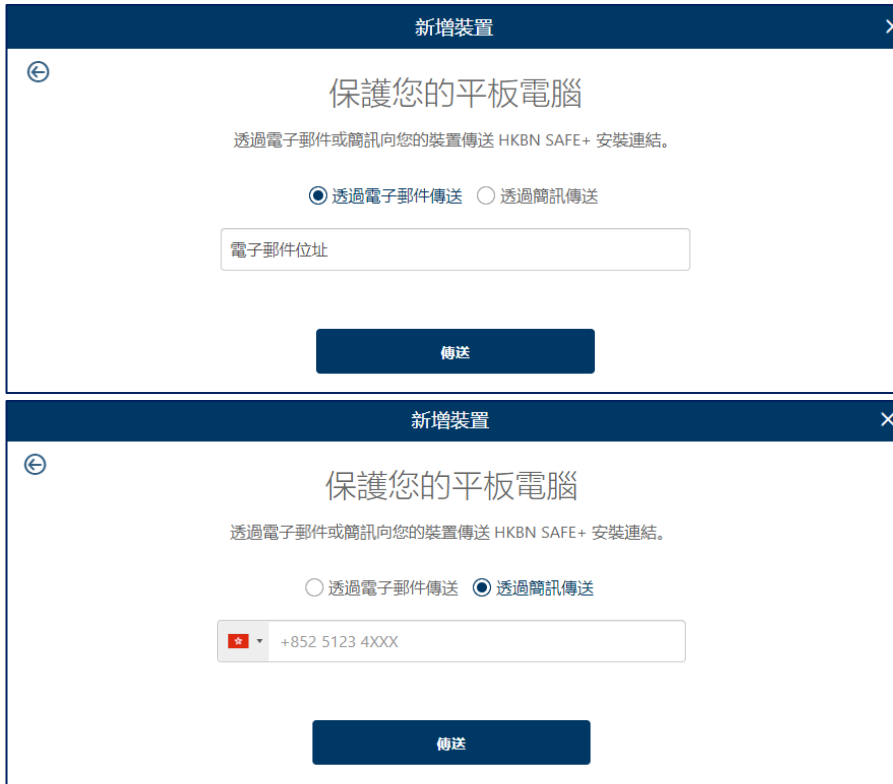
3. 選擇要保護誰的裝置，「我的裝置」，然後點擊「繼續」；



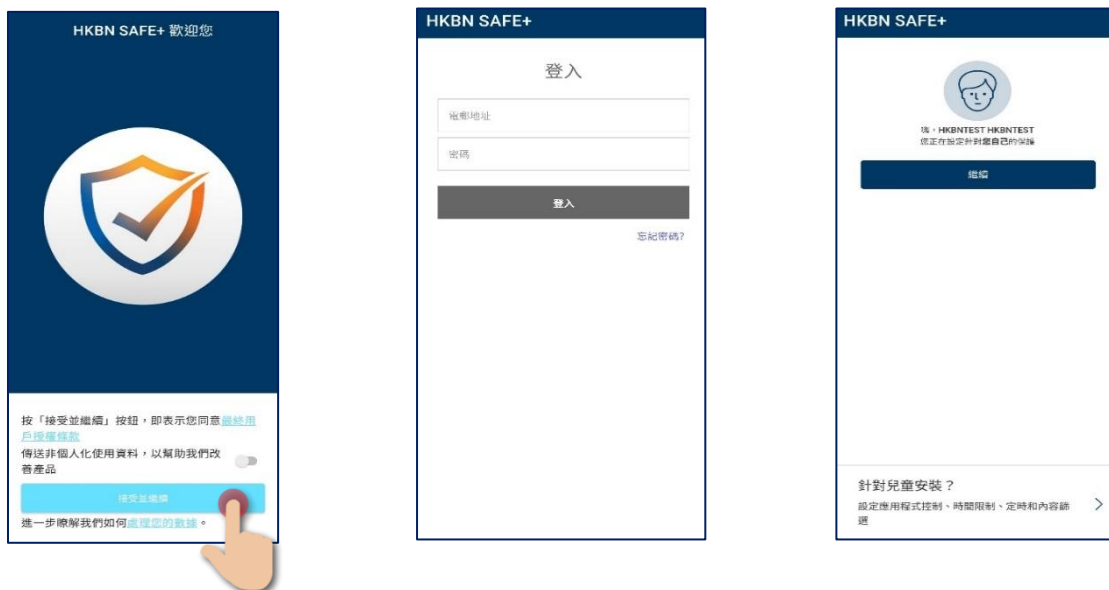
4. 選擇此裝置並將 HKBN SAFE+ 安裝到目前的裝置，然後選擇從應用程式商店安裝，前往 Google Play 或 Apple AppStore，開始安裝



5. 在不同的裝置上安裝該產品
- 選擇裝置類型，然後選擇繼續；
 - 選擇透過短訊傳送，並輸入該裝置的電話號碼。如果裝置沒有電話號碼，選擇通過電子郵件發送，然後輸入一個可以在該裝置上瀏覽的電郵地址。
 - 選擇發送。
 - 按照發送到裝置上的安裝說明進行操作。



6. 安裝完成後，選擇「打開」來啟動應用程式並啟動產品，啟動後方可保護您的裝置。

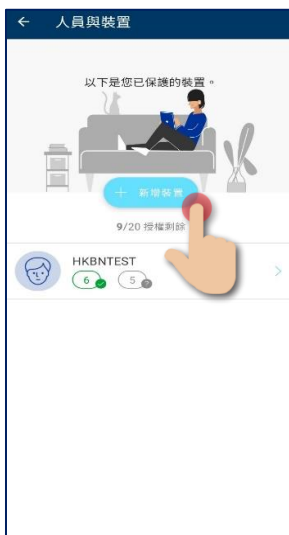


邀請家人或好友

當您邀請家人或好友加入您的 HKBN PROTECT 群組時，受邀者將獲得自己的帳戶，允許他們使用您的產品授權從而令他們的裝置得到保護。

要與其他人分享保護服務：

1. 使用您的用戶名稱和密碼登入 HKBN PROTECT。在 HKBN SAFE+ 版面，選擇「新增裝置」；
或者
開啟手機中的 HKBN SAFE+，點選「人員」。在「人員與裝置」介面，點選「新增裝置」；
2. 選擇「其他人的裝置」，點選「繼續」；



3. 邀請用戶加入您的群組，請輸入以下資料：
 - 用戶的名字
 - 用戶的姓氏
 - 用戶的電郵地址



4. 「傳送邀請」。受邀者將收到邀請短訊並加入您的 HKBN PROTECT 群組。
5. 受邀者收到邀請郵件後會擁有一個帳戶，他們能使用你的許可證來保護他們的裝置。而你用戶間不會看到其他使用者或裝置上的設定或其他細節。

請注意！如果您要邀請的人已經添加到您的群組或屬於另一個 HKBN PROTECT 群組，您將在邀請對話框中看到一條提示說明此人已經屬於您的群組或其他群組。這意味著受邀者的電郵地址已經為 HKBN PROTECT 帳戶使用，您可以通過使用另一個電郵地址（如有）邀請用戶加入您的群組來解決此問題，或者您可以要求該用戶刪除現有的 HKBN PROTECT 帳戶，然後邀請該用戶加入您的群組。

確保孩子安全地使用互聯網

互聯網上充滿各種有趣的網站，但您的孩子在瀏覽時亦會面臨各種風險，當中包括無從監管的不當內容。由於孩子多在無人監督的情況下瀏覽網頁，故隨時會面臨風險。

許多網站含有不適合孩子瀏覽的內容，他們除有可能接觸到不良內容外，並有機會下載惡意軟件而流動裝置損壞，並可能在瀏覽不安全的網站後收到騷擾訊息。

「家長控制」可幫助您讓孩子遠離互聯網上的不良內容。透過「家長控制」家長可以封鎖不當內容，讓您的孩子安全地瀏覽網頁。同時亦可封鎖有害的應用程式，保護孩子的裝置。

透過「家長控制」，你可以：

1. 為裝置的日常使用設置時間限制；
2. 設置一個睡覺時間；
3. 限制可以訪問的應用程式（僅適用於 Android），以及；
4. 阻止某些類型的內容。

為了方便使用，你可以在自己的裝置上管理你孩子的線上活動，遙距控制進行更改、添加或刪除限制，而不需要將孩子的裝置放在身邊。

註：「內容封鎖」僅可與安全瀏覽器搭配使用。停用 Safari 和其他瀏覽器，以防止您的孩子使用它們，並使用密碼保護產品設定。

新增子女的裝置

要開始使用家長控制，請在孩子的裝置上安裝 HKBN SAFE+，同時設置一個孩子設定檔。你可以在安裝 HKBN SAFE+ 應用程式時或之後的任何時候設置家長控制。一旦完成，你就可以開始保護你孩子的線上活動。

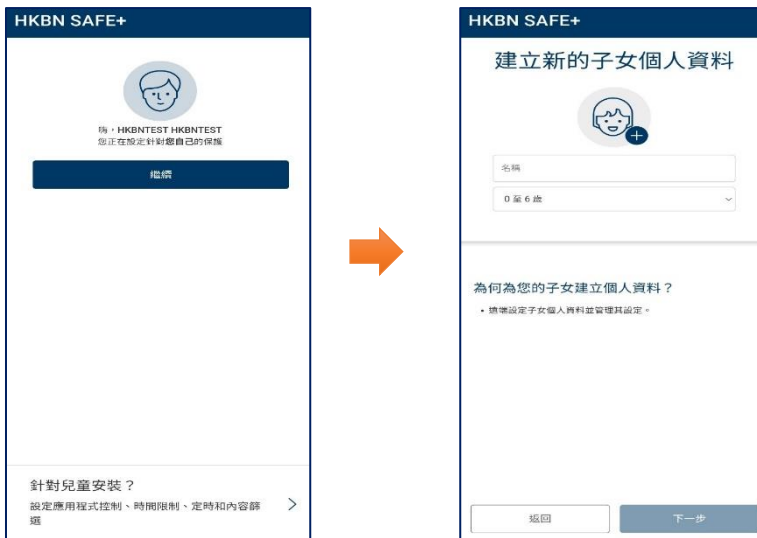
1. 使用您的用戶名稱和密碼登入 HKBN PROTECT。在 HKBN SAFE+ 版面，選擇「新增裝置」；
或者
開啟手機中的 HKBN SAFE+，點選「人員」。在「人員與裝置」介面，點選「新增裝置」；
2. 在「人員與裝置」介面，點選「新增裝置」；
3. 選擇「我的子女的裝置」，點選「繼續」；



4. 選擇透過短訊傳送並輸入裝置的電話號碼。如果裝置沒有電話號碼，則選擇透過電郵傳送並輸入裝置的電子郵件位址。選擇「傳送連結」。遵照傳送至裝置的說明進行安裝。
5. 按照發送到裝置上的安裝說明進行操作。

6. 從列出的現有設定檔中選擇或創建新的孩子設定檔，然後按照螢幕上的指示設置家長控制。
 - 輸入你孩子的名字
 - 選擇你的孩子所屬的年齡組
 - 選擇「下一步」

7. 在你開始設置之前，請與你的孩子一起討論相關設定。



為子女的裝置設定家長控制

家長控制下你能檢查不同的設置，亦可根據需要進行編輯。

a. 應用程式控制（僅適用於 Android 系統）

通過應用程式控制，您可以選擇在設置每日時間限制和就寢時間時允許哪些應用

- 在默認設定下，您可以定義應用控制如何處理一個新安裝的應用：
 - ✓ 限時 – 代表應用程式的使用受到每日時間限制或睡眠時間限制
 - ✓ 已封鎖 – 代表該應用程式根本無法使用
- 在所有程式設置下，您可以閱覽已安裝在裝置上的應用程式，並能針對某任何一個應用程式進行設置。
 - ✓ 限時 – 代表應用程式的使用受到每日時間限制或睡眠時間限制
 - ✓ 始終允許 – 應用程式的使用不受每日時間限制或就寢時間限制
 - ✓ 已封鎖 – 代表該應用程式根本無法使用



b. 每日時間限制

你可以控制孩子使用互聯網的時間。例如設定每天只有一個小時的時間，亦可為平日和週末設置不同的限制。

要設置時間限制，打開「每日時間限制」，設置每天使用設備的最長時數。

如果你不想限制孩子使用裝置的時間，將允許的小時數設置為無限。



c. 睡眠時間

你可以為孩子使用互聯網設置時間限制。(例如，只可使用到晚上 8 點)

在 "就寢時間" 窗格中選擇 "編輯"，以防止在夜間使用設備。你可以為上課日和週末設置不同的就寢時間。

- 要設置上課日的就寢時間，請打開「次日有課的晚上」，並設置就寢時間開始和結束的時間。
- 要設置週末的就寢時間，請打開「週末晚上」，並設置就寢時間開始和結束的時間。

注意：如果你取消了時間限制，你的孩子可以在任何時間使用裝置。



d. 內容篩選

通過限制孩子瀏覽含有不適宜內容的網站和網頁，使他們免受互聯網的威脅。



封鎖網頁內容類別

您可以同時選擇封鎖多種內容類別。

1. **成人內容**：成人市場導向的網站，帶有明顯性內容或包含性暗示。例如性用品商店網站或以性為目的的裸露。
2. **令人困擾**：包含可能令人困擾的影像、說明或遊戲的網站。包括令人厭惡、可怕或恐怖的資訊、影像和視訊，令小孩受到困擾。
3. **毒品**：宣傳吸毒的網站。例如提供任何形式的購買、種植或銷售相關資訊的網站。
4. **賭博**：可供人們使用現金或某種形式的信貸在線上投注的網站。例如，線上賭博和彩票網站，以及包含線上或現實生活中賭博相關資訊的網誌和論壇。
5. **煙酒**：展示或宣傳酒精飲料或煙草產品的網站，例如釀酒廠、葡萄園和啤酒廠等製造商的網站，或宣傳啤酒節、酒吧和夜店的網站。
6. **非法**：包含法律禁止的影像或資訊的網站。
7. **非法下載**：未經授權的檔案共用或軟件盜版網站。例如，提供非法軟件或可疑存取權限的網站，以及開發和散佈可能危害網絡和系統程式的網站。
8. **暴力**：可能鼓吹暴力或包含可怕和暴力影像或視訊之網站。例如包含強姦、騷擾、謀殺、炸彈、襲擊、兇殺和自殺相關資訊的網站。
9. **仇恨**：對特定宗教、人種、國籍、性別、年齡、傷殘或性取向表現出偏見的網站。例如，宣傳傷害人類、動物或機構的網站，或包含對其中任何對象實質攻擊之描述或影像的網站。
10. **武器**：包含武器或可用作武器傷害人類或動物的任何物件之資訊、影像或視訊的網站，包括宣傳此類武器的組織，例如狩獵和射擊俱樂部的網站。此類別包括玩具武器，諸如彩彈槍、氣槍和玩具槍。
11. **約會**：為尋找情侶或性伴侶提供通路之網站。例如配對網站或郵購新娘網站。
12. **購物和拍賣**：可購買任何產品或服務的網站，包括包含有助於線上下單和購買的商品目錄的網站，以及提供關於線上下單和購物的資訊的網站。
13. **社交網絡**：將大眾或特定人群聯繫起來以供社交、業務交流等之用的網絡入口網站。例如，可供您建立會員資料以分享您的個人和職業興趣的網站。這包括各種社交媒體網站，例如 Twitter。
14. **未知**：未分類的網站。您可使用此類別來封鎖未知內容。

在孩子的裝置上停用 Safari (只適用於 iOS)

HKBN SAFE+ 無法防止 Safari 或其他瀏覽器存取不安全的網站，特別是在孩子的裝置上使用安全瀏覽器時，故我們建議您在使用產品時，停用 Safari 和其他瀏覽器。

以下指引是為了在 iOS 13 或更新版本上停用 Safari。通過停用 Safari，你可以確保你的孩子無法使用 Safari 訪問不安全的網站。步驟如下：

1. 開啟手機中的「設定」；
2. 點選「螢幕使用時間」；
3. 點選「內容與私隱限制」；
4. 前往「允許的 App」；
5. 點擊 Safari 的選項，滑動按鈕至關閉便完成。

現在，Safari 已被停用，並從你最喜歡的應用程式列表中消失。

在裝置上刪除其他瀏覽器 (只適用於 iOS)

通過刪除除安全瀏覽器之外的所有其他瀏覽器，您可以防止從其他瀏覽器訪問不安全的網站，大大地提高您網上的安全性。尤其是在孩子裝置上使用安全瀏覽器時，我們建議您從孩子的 iOS 設備中刪除所有其他瀏覽器。HKBN SAFE+ 無法阻止其他瀏覽器訪問不安全的站點。

移除的瀏覽器的步驟如下：

1. 按下 Home 按鈕，找到要移除的瀏覽器圖示。
2. 長按瀏覽器圖示。
3. X 標誌顯示在圖示的左上角。
4. 按下 X 並確認要移除該瀏覽器。

安全瀏覽

安全瀏覽可以幫助你安全地使用互聯網，防止無意中訪問有害的網站，並在網上銀行期間為你的網路瀏覽器增加額外的安全性。

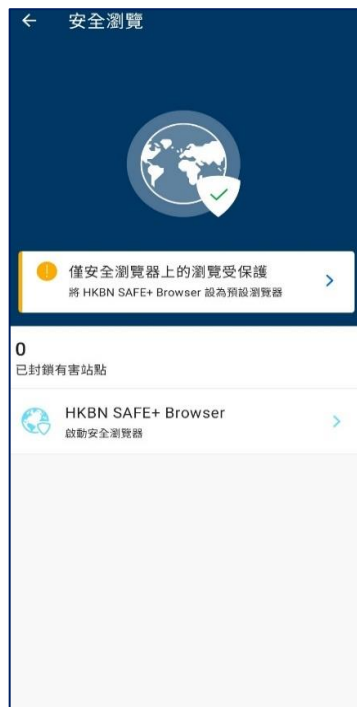
在你訪問網站之前，它會自動檢查該網站的安全性。如果該網站被評為可疑或有害，該產品將阻止對該網站的訪問。一個網站的安全評級是基於幾個來源的資訊，如 F-Secure 惡意軟體分析師和 F-Secure 合作夥伴。

註：安全瀏覽只適用於 HKBN SAFE+ 安全瀏覽器，故需要停用 Safari 和其他瀏覽器，以防止您的孩子使用它們，並用密碼來保護設置。

HKBN SAFE+ 安全瀏覽器

要將 HKBN SAFE+ 安全瀏覽器投入使用，並充分利用該產品，請將安全瀏覽器設置為設備上的預設或主要瀏覽器。當你打開一個支援的網頁時，安全瀏覽器自動啟動。

如果裝置屬於孩子，而你想他們的線上活動得到保護時，作為一項重要的安全措施，你可以考慮從孩子的裝置上刪除其他瀏覽器，以確保孩子不能使用其他瀏覽器訪問其他網站。



網上銀行保護

HKBN SAFE+ 安全瀏覽器保護你免受有害軟體或網站的影響，這些軟體或網站可能會收集和轉發你在網上銀行中輸入的詳細個人資料，包括信用卡號碼、使用者帳戶資訊和密碼等。

在您進入網上銀行網站時，產品將自動保留您需要（以及已由 F-Secure 驗證為安全網站）的網站連線同時阻止任何沒有進入預定網站的連接。您在銀行網站上的操作結束時，所有其他連線將會還原。這一額外的安全性階層可防止有害軟件傳出您的私人詳細資料。

開啟安全瀏覽後，它將自動保護 HKBN SAFE+ 瀏覽器中你所進行的網上銀行操作。

註：如果您使用任何其他瀏覽器，則安全瀏覽不會保護您的網上銀行工作階段。



從封鎖網站返回或進入封鎖網站

如果您在使用安全瀏覽器時意外訪問了有害網站，安全瀏覽會自動阻止繼續進行訪問，並顯示您剛嘗試存取的網站有害並已封鎖。你可以選擇以下兩個動作：

1. 如果您想返回到之前的網頁，請選擇「返回」。
2. 如果您仍想要進入該網站，即使是安全瀏覽已封鎖的網站，請選擇「我仍想進入此網站」。



病毒和威脅保護

HKBN SAFE+ 將掃描您裝置中的病毒、有害內容，以及您裝置或數據的其他威脅。產品將每天自動掃描已安裝的程式和插入的記憶卡，以尋找病毒、間諜軟件和危險軟件。

病毒掃描及移除（只適用於 Android）

您可視乎需要隨時掃描裝置中的病毒和其他惡意軟件。

若要手動掃描裝置和插入的記憶卡中的檔案，請依照以下說明執行：

1. 選擇「病毒和威脅保護」；
2. 選擇「掃描」，防毒掃描將啟動；
3. 掃描完成後，產品會顯示以下資訊：
 - 已檢查的檔案數目
 - 已檢查的應用程式數目
4. 掃描完成後可以查閱結果



5. 如果應用程式在掃描過程中檢測到一個含有病毒或其他惡意程式碼的檔，病毒和威脅保護視圖中會出現一個通知。例如，你可能會看到以下通知。

- 1 檢測 - 潛在的不需要的應用程式
- 1 感染 - 檢測到有害的應用程式

6. 要評估檢測到的檔，請打開掃描詳情頁面。

a) 在病毒和威脅保護中，選擇主視圖上 SCAN 下的通知。

b) 要刪除檔，請選擇刪除所有檢測到的檔，以同時從您的設備中刪除它們。

c) 要查看更多的細節，選擇通知以查看更多關於檢測的細節。你可以看到以下細節。

- 應用程式名稱
- 包裹名稱
- 檢測到的問題
- 大小

d) 選擇「刪除」來完全刪除該檔案。

你可以在 F-Secure 網站 - [F-Secure 實驗室：威脅描述](#) 上找到關於病毒、木馬、蠕蟲和其他形式的無用軟體的描述和資訊。

應用程式通知（僅適用於 Android 系統）

HKBN SAFE+ 會在以下情況下向您發送有關某應用程式活動的通知，例如。

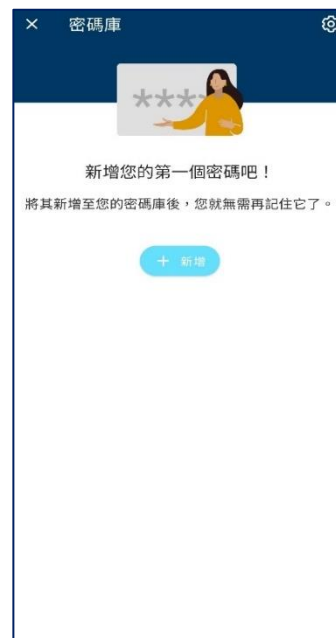
- 當應用程式正在運行時
- 當應用程式正在進行掃描時
- 當孩子的時間限制即將結束的時候

這些通知中部份會一直顯示，其餘則在一段時間後消失。在預設情況下，來自應用程式的通知會自動打開。我們建議保持這些默認設置，以確保裝置得到最好的保護。某些重要的通知，如已安裝的應用程式是有害的，即使你關閉通知也會顯示。

密碼庫(只適用於有訂購 ID PROTECTION 服務)

通過 HKBN Safe+ 密碼保管庫，您可以建立和儲存密碼或信用卡輸入，該應用程式也可以為您的線上服務生成強而獨特的密碼，並檢視密碼的歷史記錄。

1. 進入密碼庫
2. 如果你是新用戶，選擇「我是新用戶」，然後創建一個主密碼（解鎖/恢復你所有保存的資料），你可以開始保存你的密碼/信用卡用於自動填充。
3. 如果您是現有用戶，請選擇我是現有用戶，您可以同步您所有保存的憑證



有關主密碼

您的主密碼非常重要，建議您建立高強度的主密碼並確保記住。主密碼用於開啟裝置鎖，保護存儲的密碼，您也需要使用主密碼在連線裝置上同步密碼。請記得為主密碼創建恢復代碼。

出於提高您的安全性和保護您的數據，應用程式無法重置您的主密碼，因此請建立一個高強度而您能記住的密碼。

建立密碼庫主密碼

1. 選擇設置 > 選擇「建立主密碼」
2. 建議使用高強度的主密碼，點擊「接受並繼續」
3. 重複輸入主密碼並選擇「確認」
4. 請選擇「另存為圖片」來保存您的恢復代碼。

建立及儲存主密碼恢復代碼

當您忘記主密碼時，恢復代碼用作恢復 HKBN SAFE+ 的存取權限。為您的安全起見，忘記的主密碼僅可使用密碼恢復代碼還原。基於安全考慮，我們不能恢復任何主密碼，有關恢復代碼請留意以下事項：

- 當每次更改主密碼時，您需要重新建立恢復代碼。
- 如忘記了主密碼，您必需要最新的恢復代碼以重新登入應用程式。
- 如果您連接到新的設備，應用程序可能會要求您創建新的恢復代碼。在這種情況下，請確保建立新的恢復代碼，因為舊代碼將不再起作用。
- 建議以圖像形式儲存恢復代碼並打印存放在安全的地方。

重要提示：我們強烈建議您在開始使用 HKBN SAFE+ 時，儘快建立主密碼恢復代碼，因為這是當您忘記主密碼時，唯一的解決方法。

1. 打開「設定」，點擊「創建恢復代碼」；



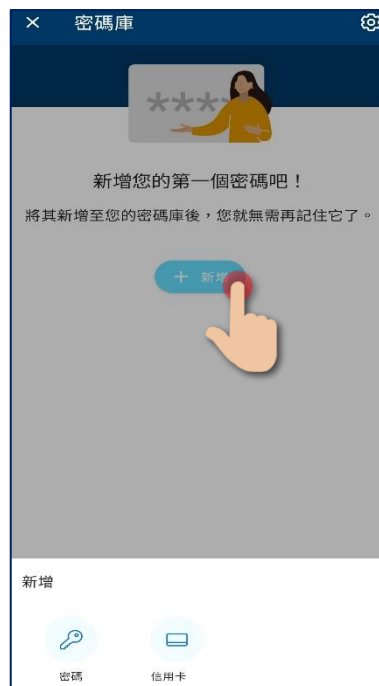
2. 點擊「儲存」，儲存此恢復代碼影像並列印和儲存於安全位置。

密碼管理員 (保管庫)

通過 HKBN Safe+，您可以建立和儲存密碼或信用卡，該應用程式也可以為您的線上服務生成強而獨特的密碼，並檢視密碼的歷史記錄。

建立和儲存您的密碼或信用卡

1. 點擊「密碼庫」；
2. 點擊「新增」；
3. 選擇「密碼」或「信用卡」



自動填寫功能

使用自動填充功能，您無需手動輸入用戶名和密碼即可登錄應用程序和網站。您需要將服務的用戶名，密碼和網址保存在 HKBN Safe+ 中，自動填充功能才能正常工作。使用保存在 HKBN Safe+ 中的憑據登錄到應用程序或網站時，可以讓該應用程序自動輸入用戶名稱和密碼。

要在你的 Android 設備上打開自動填充功能:

1. 進入密碼庫 > 設定 > 其他設定 > 啟用自動填寫功能
2. 選擇 HKBN Safe+ 作為你的服務，然後選擇 OK;

現在可以在你的設備上使用自動填寫功能。

備註: 應用程式的自動填寫功能只適用於 Android 8.0 或 8.1，瀏覽器則需要 Android 9.0。

要在你的 iPhone 或 iPad 上打開自動填充功能:

1. 進入密碼庫 > 設定 > 其他設定 > 啟用自動填寫功能 > 設置
2. 在密碼下，選擇自動填寫密碼 > 選擇 HKBN Safe+

現在可以在你的設備上使用自動填寫功能。

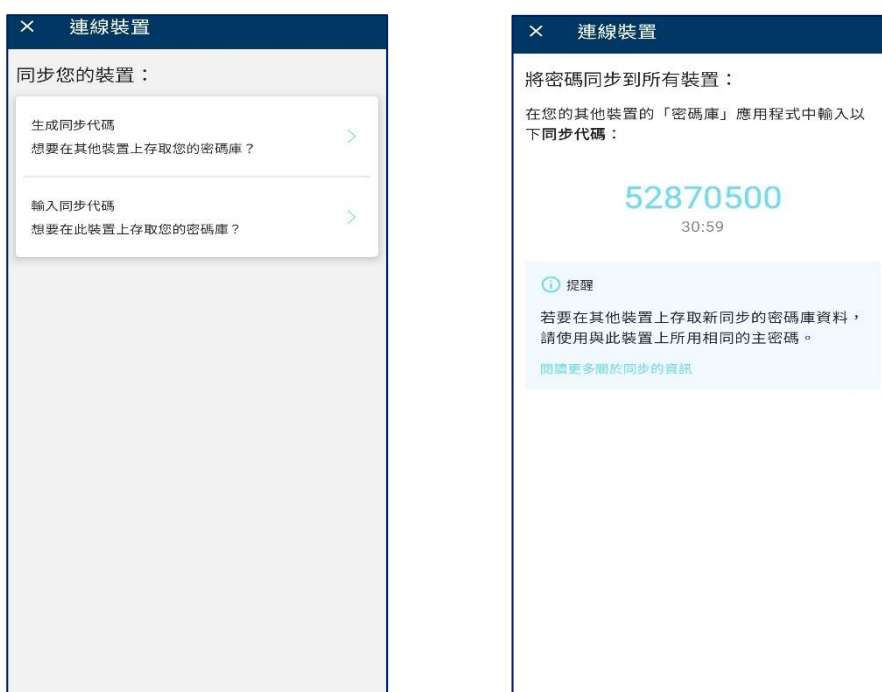
裝置連線 (同步保管庫)

如果您有其他裝置需要同步監控的項目或保管庫的密碼，可透過同步連線裝置來同步到所有裝置。

警告：如果您僅在一設備上安裝了 HKBN SAFE+ 應用程式並執行了原廠重置，重置操作會刪除該設備上的所有保險庫數據。此後將無法取回已刪除的所有數據。

1. 在 A 裝置上，打開「連線裝置」，自動產生同步代碼；

註：同步代碼每 60 秒將會更新一次。



2. 在 B 裝置上，打開「連線裝置」，輸入 A 裝置的同步代碼，點擊「連線」；

3. 連線後，輸入 A 裝置上所設定的主密碼，即可成功同步。

監控線上身份(只適用於有訂購 ID PROTECTION 服務)

透過 HKBN Safe+ 監控線上身份功能你可以添加監控項目，並接受建議，瞭解如果你的個人資訊在資料洩露中被洩露時該如何處理。





通知郵件中包括以下資訊：哪些個人身份資訊 (PII) 與違規事件有關；違規事件的性質；什麼公司或實體企業被違規；違規事件發生的時間；以及哪些其他 PII 與被監控的電子郵寄地址有關，如密碼、信用卡號碼、街道位址等。



HKBN SAFE+ 不同平台的功能比較

	 PC	 Mac	 Android	 iOS
支援系統版本				
惡意軟件防護	●	●	●	—
病毒掃描	●	●	●	—
防勒索軟件保護	●	—	—	—
瀏覽保護	●	●	●	●
網上銀行保護	●	●	●	●
家長控制遙距管理設定	●	●	●	●
家長控制 – 篩選內容	●	●	●	●
家長控制 – 時間限制	●	●	●	—
家長控制 – 睡眠時間	●	●	●	●
家長控制 – 應用程式控制	—	—	●	—
線上管理平台 (HKBN PROTECT)	●	●	●	●
App 線上管理服務「人員與裝置」	●	●	●	●

HKBN Safe+ 密碼庫及監控線上身份不同 平台的功能比較

	 Windows	 macOS	 Android	 iOS
支援系統版本	Windows 7 (SP1) and later	Mac OS X 10.1 and later	Android 6 or later	iOS 13 or later
監控線上身份	•	•	•	•
數據洩漏警報	•	•	•	•
數據洩漏建議	•	•	•	•
安全的密碼存儲	•	•	•	•
導入/輸出密碼	•	•	-	-
密碼生成器	•	•	•	•
密碼分析	•	•	•	•
登入: 主密碼	•	•	•	•
登入: 指紋/人面識別	-	-	•	•
登入: QR 恢復碼	•	•	•	•
同步密碼保管庫	•	•	•	•
系統/應用程式自動輸入	•	•	•	•
瀏覽器自動輸入	•	•	•	•
支援自動輸入的瀏覽器	Firefox, Chrome	Firefox, Chrome	SAFE Browser, Firefox, Chrome, Opera, Edge	At least Safari, Chrome

聯絡技術支援

發送記錄檔給支援部門

為了解決問題，我們的技術支援可能需要關於你的裝置的更多詳細資訊，故此需要創建和發送記錄檔給支援部門。程序如下：

1. 打開該應用程式；
 - Android, 選擇  > 關於.
 - iOS, 選擇  > [說明] > 關於 HKBN SAFE+.
2. 點擊版本號碼七次，直到顯示 Android> [傳送記錄檔] / iOS> [傳送日誌]
3. 以電子郵件方式把檔案傳送給我們的支援部門

聯絡我們

如有任何查詢，請發送電郵至HKBNBroadband@hkbn.net 與我們聯絡。