



# **CTM SAFE**

## **用戶指南**

(Windows / macOS)

March 2022

# 目錄

CTM SAFE 簡介 .....	3
防護管家服務(管理平台).....	5
首次登入帳戶 .....	6
忘記密碼.....	7
下載及安裝 CTM SAFE .....	8
在不同的裝置上安裝 CTM SAFE.....	10
邀請家人或好友使用防護管家服務 .....	11
保護狀態圖示.....	13
確保孩子安全地使用互聯網 .....	14
通過防護管家服務管理平台新增子女的裝置.....	15
為子女的裝置設定家長控制.....	17
a. 應用程式控制 (僅適用於 Android 系統) .....	17
b. 每日時間限制.....	18
c. 睡眠時間 .....	19
d. 內容篩選.....	20
封鎖網頁內容類別 .....	21
保護網上銀行與上網安全.....	22
檢查瀏覽器擴充功能是否在使用中 .....	23
啟用 Safari 的延伸功能 (僅適用於 macOS) .....	24
網站信譽評級圖示 (適用於 Windows 及 macOS).....	25
從封鎖網站返回或進入封鎖網站.....	26
病毒掃描.....	27
使用即時掃描.....	27
手動執行病毒掃描 .....	28
技術支援.....	31
CTM SAFE 不同平台的功能比較.....	32

# CTM SAFE 簡介

CTM 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。CTM SAFE 透過防禦電腦、智慧手機或平板電腦上的網絡安全威脅，從而保護您自己及家人。

透過防護管家服務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，讓您瞭解該使用者的保護情況。

## CTM SAFE 應用程式

在您的所有設備上安裝 CTM SAFE 應用程式，以保護您的安全和私隱。CTM 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訪問。
- 銀行保護，當您進入網上銀行時，它通過保護連接安全來保護您的網上銀行活動。

# Windows 的系統需求

版本: CTM SAFE for PC Release 18.2

支援的作業系統：

- Windows 11.
- Windows 10, (年度更新或最更新版本)
- Windows 8.1.
- Windows 7, SP1 (所有版本)

最低系統要求：

- 處理器：1千GHz或以上\*
- 記憶體：1 GB 記憶體 ( 32位元 ) 或2GB 記憶體 ( 64位元 )
- 硬碟空間：600MB可用硬碟空間
- 需要互聯網連接來驗證您的訂閱和接收更新，或須繳付ISP 費用。  
\*不支援基於ARM的平板電腦。

支援的檢查瀏覽器：

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

# macOS 的系統需求

版本: CTM SAFE for Mac Release 18.1

支援的作業系統版本：

- macOS 版本 12.0 (Monterey)
- macOS 版本 11.0 (Big Sur)
- macOS 版本 10.15 (Catalina, 10.15.5 或更新版本)

建議的系統要求：

- 英特爾處理器
- 250MB的可用磁碟空間
- 建議有1GB或更多的記憶體
- 需要互聯網連接來驗證您的訂閱和接收更新。

支援的檢查瀏覽器:

- Google Chrome
- Mozilla Firefox
- Safari

## 防護管家服務(管理平台)

防護管家服務管理平台是一個易於使用的線上服務平台，您可以用來將 CTM SAFE 遠端安裝到您選定的裝備上並管理您的訂閱。

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)。您可以通過電子郵件或 SMS 短訊將產品安裝連結發送到裝置上進行安裝，遠端管理由 SAFE 保護的智慧型手機或平板電腦，以及管理您的訂閱。隨時方便地從一台裝置上解除使用授權，將 CTM SAFE 安裝至另一台新裝置上。

點擊連結進入防護管家服務管理平台：

<https://safeavenue-jp.f-secure.com/iframe/-sso/ctm/>



# 首次登入帳賬戶

1. 當您的流動電話接收到成功啟動短訊後；
2. 輸入申請服務時登記的電話號碼 (需輸入+853) 及短訊內臨時密碼，然後點選「登入」；
3. 首次登入系統或會要求您更改密碼，輸入新的密碼；
4. 隨後便開始使用防護管家服務。



## 登入

[忘記密碼?](#)



## 變更您的密碼

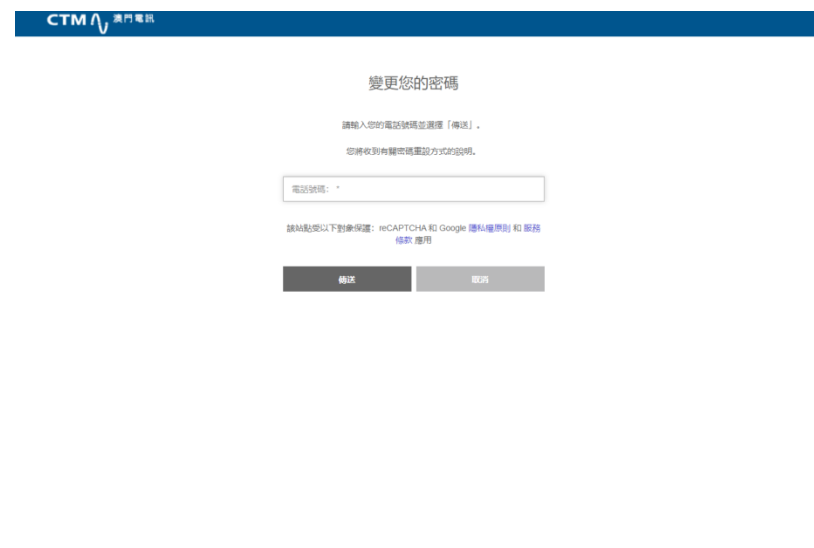
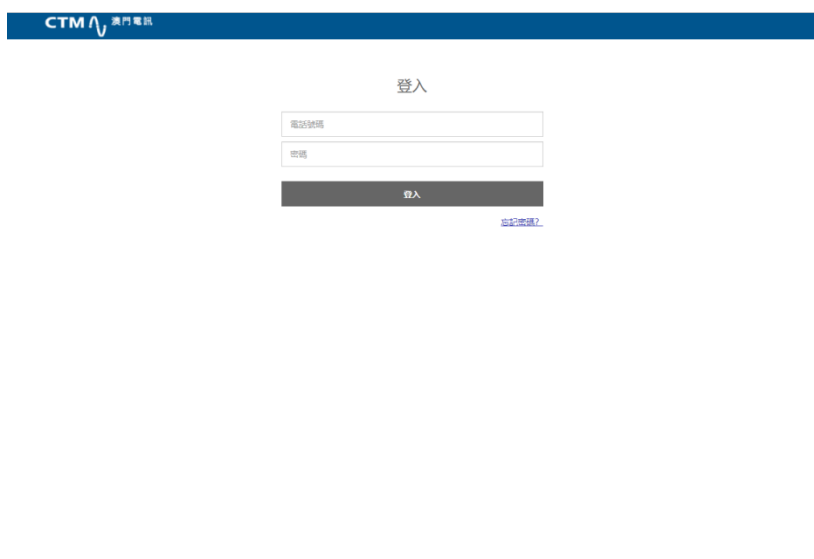
電話號碼  
+85362887050

  
 顯示密碼  
 

# 忘記密碼

如果您忘記了防護管家服務的賬戶密碼，可以通過找回密碼的流程建立新密碼：

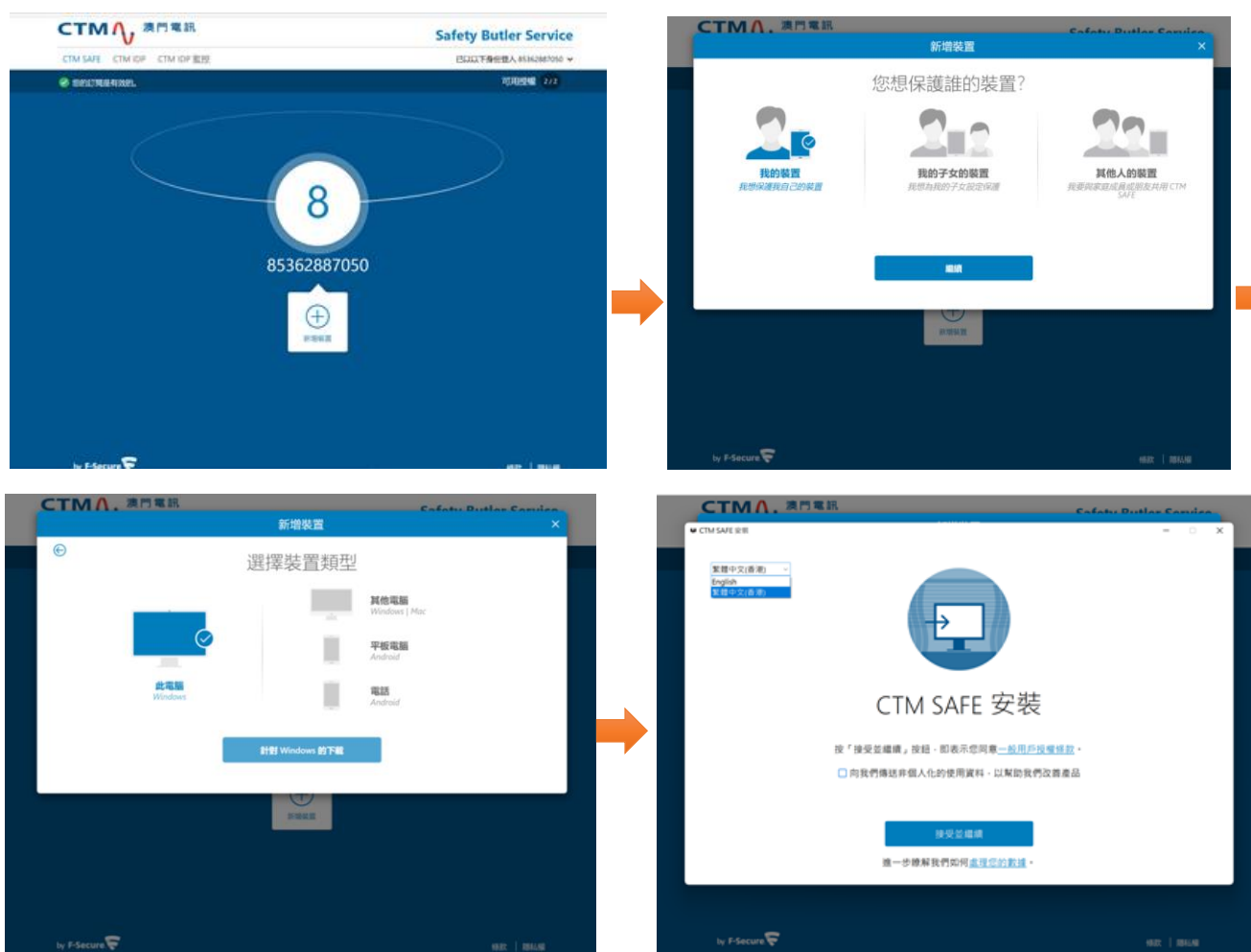
1. 點擊「忘記密碼」；
2. 輸入您註冊用的電話號碼，點擊「傳送」。系統會向流動裝置發送變更密碼的短訊；
3. 點擊短訊中的連結；
4. 輸入新的密碼。



# 下載及安裝 CTM SAFE

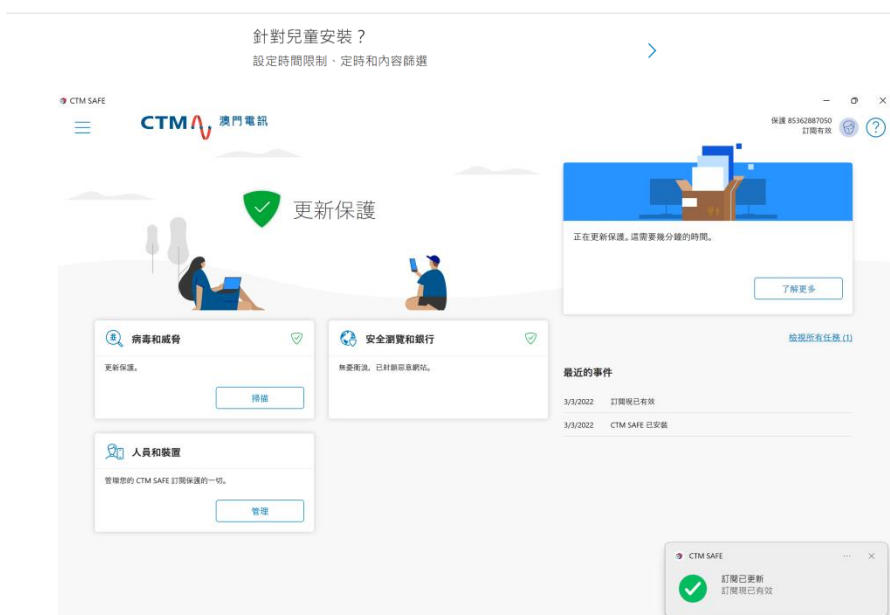
登入防護管家服務管理平台下載和安裝 CTM SAFE，亦可以發送電子郵件或 SMS 短訊至您的裝置，在要保護的裝置上安裝 CTM SAFE。

1. 使用您的電話號碼 (需輸入+853) 和密碼登入防護管家服務管理平台；
2. 在 CTM SAFE 版面，選擇「新增裝置」；
3. 選擇要保護誰的裝置，如「我的裝置」，然後點選「繼續」；選擇此裝置並將 CTM SAFE 安裝到目前的裝置，選擇為 Windows / Mac 下載，獲取安裝套件；
4. 啟動下載的安裝套件，於左上角選擇語言，點選「接受並繼續」下載及安裝 CTM SAFE；您的電腦可能需要重新啟動，從而驗證訂購並下載最新更新；



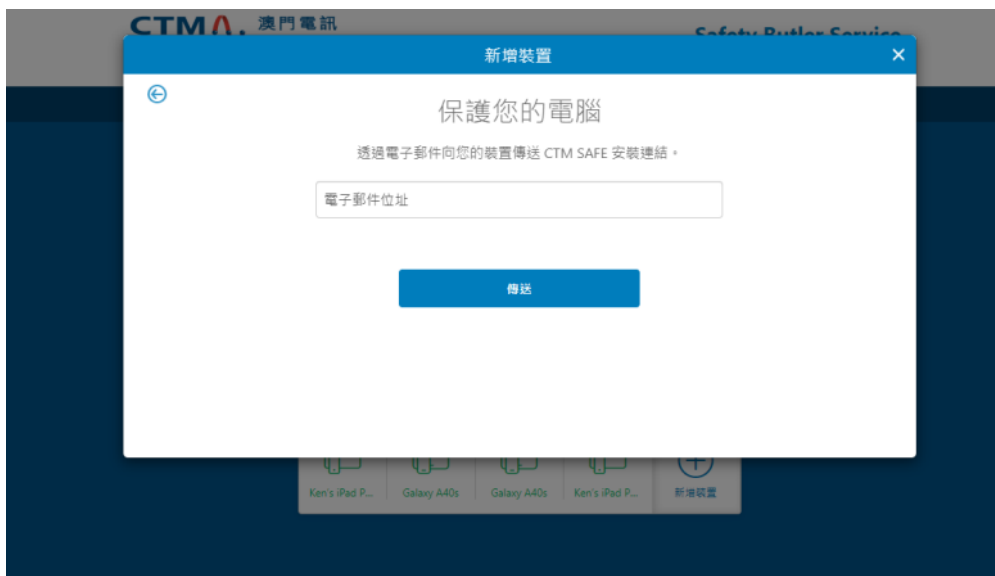


安裝完成後，開啟並登入 CTM SAFE 以啟動產品，啟動後方可保護您的裝置。



## 在不同的裝置上安裝 CTM SAFE

1. 選擇裝置類型，然後點擊「繼續」；
2. 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，選擇透過電郵傳送並輸入裝置的電郵地址；
3. 選擇「傳送」；
4. 按照發送到設備上的安裝說明進行安裝。

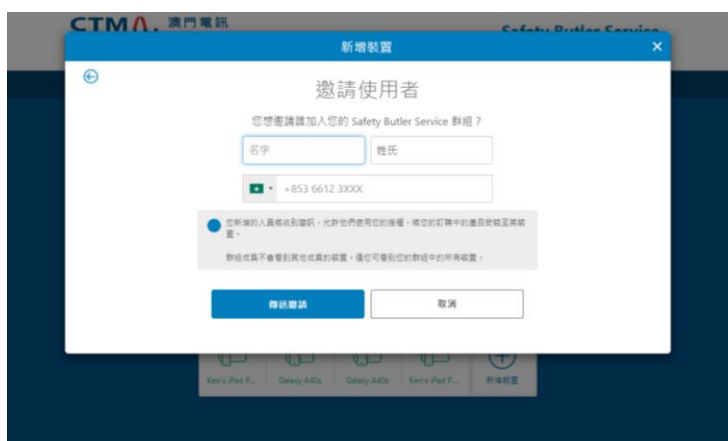


# 邀請家人或好友使用防護管家服務

當您邀請家人或好友加入您的防護管家服務群組時，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。

要與其他人分享防護管家服務：

1. 在 CTM SAFE 版面，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
  - 用戶的手機號碼
4. 「傳送邀請」。受邀者將收到邀請短訊並加入您的防護管家服務群組。
5. 受邀者收到邀請短訊後會擁有一個帳戶，他們能使用您的產品授權來保護他們的裝置。而受邀者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防護管家保護服務群組，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。這意味著受邀者的手機號碼已經為防護管家保護服務賬戶使用，您可以通過使用另一組手機號碼（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防護管家保護服務賬戶，然後邀請該用戶加入您的群組。

# 保護狀態圖示

保護狀態圖示為您顯示產品及其功能的整體狀態。

狀態圖示	狀態	說明
	正常	您的電腦已受保護。 功能已開啟並正常運行。
	已過期	您的電腦未受保護。 訂閱已過期。
	已過期及已關閉	您的電腦未受保護。 例如關鍵功能已關閉或您的訂閱已過期。
	已關閉或錯誤	您的電腦未受到完全保護。 產品需要即時動作，例如關鍵功能已關閉或長時間未收到更新。
	警告	您的電腦未受到完全保護。 產品需要您注意，例如安全功能已關閉。
	更新中	產品更新中

顯示的狀態訊息的示例：

- **Google Chrome** 瀏覽器延伸未在使用
- **Mozilla Firefox** 瀏覽器延伸未在使用
- **Microsoft Edge** 瀏覽器延伸未在使用中
- 您的訂閱已過期

# 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，或有機會下載可能損壞流動裝置的惡意軟件，或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」，您可以：

1. 為裝置的日常使用設置時間限制；
2. 設置就寢時間；
3. 限制可以訪問的應用程式（僅適用於 Android），以及；
4. 封鎖某些類型的網頁內容。

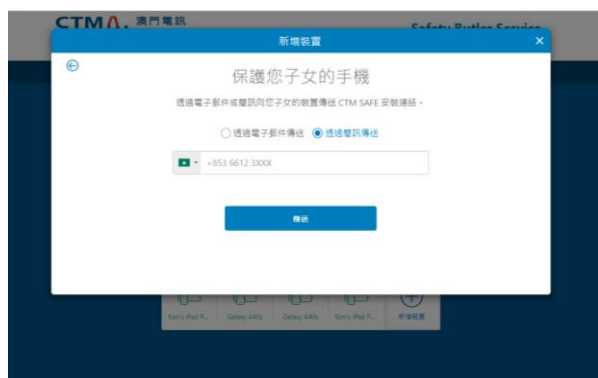
為了方便使用，您可以在自己的裝置上管理您孩子的線上活動，遙距控制進行更改、添加或刪除限制，而不需要將孩子的裝置放在身邊。

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，並使用產品密碼保護產品設定。

## 通過防護管家服務管理平台新增子女的裝置

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


1. 在 CTM SAFE 版面，點選「新增裝置」；
2. 選擇「我的子女的裝置」，點選「繼續」；
3. 選擇裝置類型；
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郵地址。點選「傳送」。
5. 遵照傳送至裝置的說明進行安裝。



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庭規則。
  - 輸入您孩子的名字
  - 選擇您的孩子所屬的年齡組
  - 選擇「下一步」

在您開始設置之前，請與您的孩子一起討論相關設定。

CTM SAFE



嗨，Tester  
您正在設定針對您自己的保護

繼續

CTM SAFE

登入

電話號碼


密碼

登入

[忘記密碼?](#)

CTM SAFE

建立新的子女個人資料



名稱

0 至 6 歲

---

為何為您的子女建立個人資料？

- 這確認了子女個人資料並管理其設定。

返回

下一步

---

針對兒童安裝？

設定應用程式控制、時間限制、定時和內容篩選 >



# 為子女的裝置設定家長控制

家長控制下您能檢查不同的設置，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

您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。

如果您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。

The screenshot shows the 'CTM SAFE' app interface for a child named Mary, aged 0 to 6. The main heading is '每日時間限制' (Daily Time Limit), which is currently turned on. Below this, there is a note: '限制所有應用程式的每日使用時間。開啟應用程式控制以選擇針對哪些應用程式啟用。' (Limit the daily usage time of all apps. Turn on app control to select which apps to enable for.) and a sub-note: '始終允許手叫和收發簡訊。' (Always allow hand calls and sending/receiving messages.).

There are two sections for setting time limits:

- 工作日** (Weekdays): 週一-週五 (Monday-Friday), 每天 1 小時 (1 hour per day). The slider is set to 1 hour.
- 週末** (Weekends): 週六和週日 (Saturday and Sunday), 每天 2 小時 (2 hours per day). The slider is set to 2 hours.

At the bottom, there are two buttons: '返回' (Back) and '下一步' (Next Step).

### C. 睡眠時間

您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。您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：如果您取消了時間限制，您的孩子可以在任何時間使用裝置。

The screenshot shows the 'CTM SAFE' app interface for a child named Mary (age 0-6). The '睡眠時間' (Sleep Time) section is active, indicated by a blue toggle switch. Below this, there are two settings for sleep times:

- 次日有課的晚上** (Next day with school on the evening): Days 週日 - 週四 (Sunday - Thursday). The time range is set to 20:00 - 08:00. A slider below the range shows the start and end times on a 24-hour scale from 18:00 to 12:00.
- 週末晚上** (Weekend evening): Days 週五和週六 (Friday and Saturday). The time range is also set to 20:00 - 08:00, with a corresponding slider.

At the bottom of the screen, there are two buttons: '返回' (Back) and '下一步' (Next Step).

#### 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。

# 保護網上銀行與上網安全

銀行保護可在您進入網上銀行或進行線上交易時，保護您免遭有害行為的侵襲。銀行保護自動偵測與識別出網上銀行網站的連線，並在您瀏覽此類網站時通知您。

銀行保護系統增加了另一層安全保護，以防您的機密交易受到干擾，系統防止您在網上銀行工作階段期間輸入的個人資料（包括信用卡號碼、用戶帳戶資訊，以及密碼）被洩露。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）的網站以外的所有其他網絡連線。您在銀行網站上的操作結束時，將還原所有其他連線。

銀行保護目前支援以下瀏覽器：

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

一旦您關閉瀏覽器或結束網上銀行業務，銀行保護會自動檢測並關閉保護框架。預設情況下，**銀行保護**是長期啟用的。如果沒有啟用，請按以下方法打開**銀行保護**框架。

## 1. 在macOS電腦上

1. 選擇功能表列中的CTM SAFE圖示。
2. 從功能表上選擇「喜好設定」。
3. 選擇**安全瀏覽**選項。
4. 選擇左下角的鎖定圖示。  
注意：你需要管理許可權來改變這些設置。
5. 選擇「**開啟銀行保護**」。

## 2. 在Windows電腦上。

1. 在功能表主頁面中，選擇**安全使用線上銀行**。
2. 在**安全使用線上銀行概覽**中，選擇設置。
3. 選擇**編輯設置**。  
注意：你需要管理許可權來改變設置。
4. **開啟銀行保護**。  
注意：銀行保護需要使用瀏覽器擴充功能。

## 檢查瀏覽器擴充功能是否在使用中

瀏覽保護需要瀏覽器擴充功能方可運作，從而保護你瀏覽網頁、網上銀行和購物。此外亦能為您提供可能有害的網站的安全資訊，並在搜尋結果中顯示安全評級圖示。

當你打開瀏覽器時，它會顯示一個關於新安裝的擴展功能通知，此時需要點擊啟用。如果你錯過了該通知，主頁面會顯示你是否尚未設置瀏覽器擴展功能。最簡單的方法是在主頁面上顯示的通知中選擇設置，並按照螢幕上的指示操作。

- 如果你使用 Firefox 瀏覽器，首先選擇瀏覽器擴展功能下的安裝 Firefox 擴展功能，然後選擇添加。擴展功能將被添加在 Firefox 上啟用。
- 如果您使用 Chrome 瀏覽器，首先選擇瀏覽器擴展下的「打開 Chrome 網路商店」連結。F-Secure 的瀏覽保護頁面會在 Chrome Web Store 中打開。如果該擴展功能程式已經在 Chrome 上安裝但被禁用，請從頁面頂部上選擇啟用該專案連結。如果該擴展程式尚未安裝，請選擇添加到 Chrome > 添加擴展功能程式。該擴展功能將被添加並在 Chrome 上啟用。
- 如果你使用 Microsoft Edge，首先選擇瀏覽器擴展下的 Open Edge Add-ons 連結。F-Secure 的瀏覽保護頁面會在 Edge 附加元件中打開。如果該擴展功能已經安裝在 Microsoft Edge 上但被禁用，請選擇「打開」以啟用它。如果該擴展尚未安裝，則選擇獲取 > 添加擴展。該擴展將被添加並為 Microsoft Edge 啟用。



Browsing protection by F-Secure

Offered by: F-Secure

## 啟用 Safari 的延伸功能 ( 僅適用於 macOS )

您必須啟用 Safari 的瀏覽器延伸功能，以便能夠安全地使用該瀏覽器。本產品會自動安裝該瀏覽器延伸功能中，但需確保該延伸功能已啟用。

要確保 Safari 瀏覽器的延伸功能已啟用：







1. 選擇功能表列中的產品圖示。
2. 從功能表中選擇「喜好設定」。
3. 打開安全瀏覽選項。
4. 選擇安裝瀏覽器延伸功能 (瀏覽保護視窗打開)。
5. 從下拉式功能表中，選擇 Safari，然後選擇立即啟用。
6. 在延伸功能程式中，選擇瀏覽保護。

現在您可以使用 Safari 安全地瀏覽互聯網。



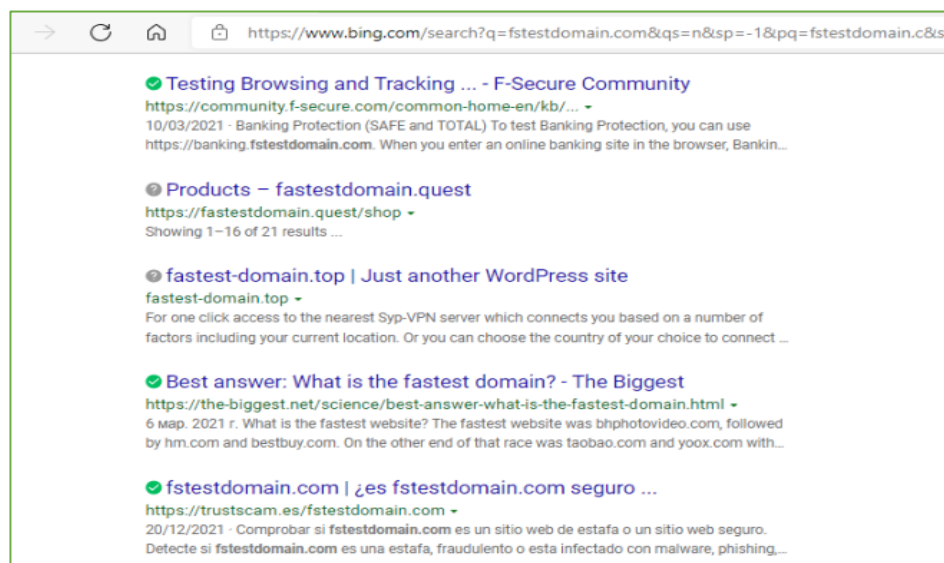
## 網站信譽評級圖示 (適用於 Windows 及 macOS)

在您使用 Google、Bing 或 Yahoo 時，瀏覽保護會在搜尋結果頁面上顯示網站安全性評等。彩色圖示顯示目前網站的安全評等，搜尋結果上每個連結的安全評等也會以相同的圖示顯示：

	據我們所知該網站是安全的。我們沒有在網站中發現任何可疑內容。
	該網站是可疑的，建議您在造訪該網站時保持謹慎，避免下載任何檔案或提供任何個人資訊。
	該網站是有害的。建議您避免造訪該網站。
	該網站尚未經過分析且目前沒有可用的資訊。
	管理員已允許您造訪該網站。
	管理員已阻止該網站，因此您無法訪問。

安全評級可在以下搜索網站上找到：

- Google
- Bing
- Yahoo
- DuckDuckGo

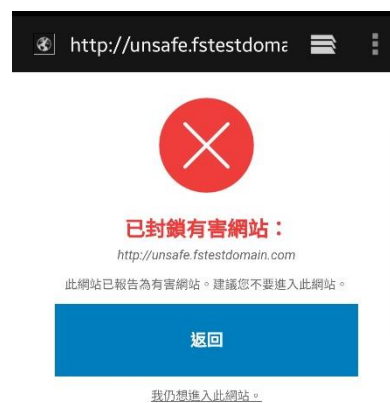


## 從封鎖網站返回或進入封鎖網站

如果您在使用安全瀏覽器時意外瀏覽了有害網站，安全瀏覽會自動阻止繼續進行瀏覽，並顯示您剛嘗試存取的網站有害並已封鎖。

如果您仍想進入網頁，請選擇「在此電腦上允許網站」

1. 輸入你的管理員密碼並選擇確定
2. 被封鎖的網站會打開，產品將該網站添加到允許的網站列表中。



Protection by F-Secure

# 病毒掃描

CTM SAFE 可防止不法程式竊取個人資訊、損壞電腦，或將電腦用於非法用途。預設情況下，病毒防護會在發現有害檔案時立即予以處理，以免造成損害。

CTM SAFE 會自動掃描您的本機硬碟、任何卸載式媒體 (如可攜式磁碟機或光碟) 與所有下載內容。CTM SAFE 還將監視電腦並建議針對電腦存在有害檔案的變更。CTM SAFE 檢測到任何危險系統變更時 (如嘗試系統設定變更或重要系統進程變更時)，其 DeepGuard 組件則會阻止應用程式運行，因為它可能造成損害。

## 使用即時掃描

保持即時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

我們建議您始終保持開啟「病毒防護」。如果您要確保電腦上無有害檔案或要掃描已從即時掃描中排除的檔案，則還可手動掃描檔案和設定排程掃描。

若要確保即時掃描已開啟 (Windows)：

1. 打開 CTM SAFE 功能表，選擇「病毒和威脅」；
2. 選擇「設定」；
3. 選擇「編輯設定」；

**註：您需要管理權限才能變更設定。**

4. 開啟「病毒防護」。

## 手動執行病毒掃描

您可掃描整部電腦以完全確保沒有任何有害檔案或惡意應用程式。全面電腦掃描可掃描所有內部和外部硬碟以尋找病毒、間諜軟體和潛在惡意應用程式。同時亦會檢查可能由 Rootkit 隱藏的項目，因此全面電腦掃描需要較長時間來完成。您亦可僅掃描部份已安裝應用程式，更有效的尋找和移除電腦上的惡意應用程式和有害檔案。

以下是 **Windows** 的手動執行病毒掃描流程：

1. 打開 CTM SAFE 功能表，選擇「病毒和威脅」；
2. 選擇「設定」；
3. 如果您要對手動掃描電腦的方式進行最佳化，請選擇「變更掃描設定」。
4. 選擇「病毒掃描」或「全面電腦掃描」。
5. 如果病毒掃描找到任何有害項目，則會為您顯示其偵測到的有害項目清單；
6. 按一下偵測到的項目以選擇您要處理該有害內容的方式；

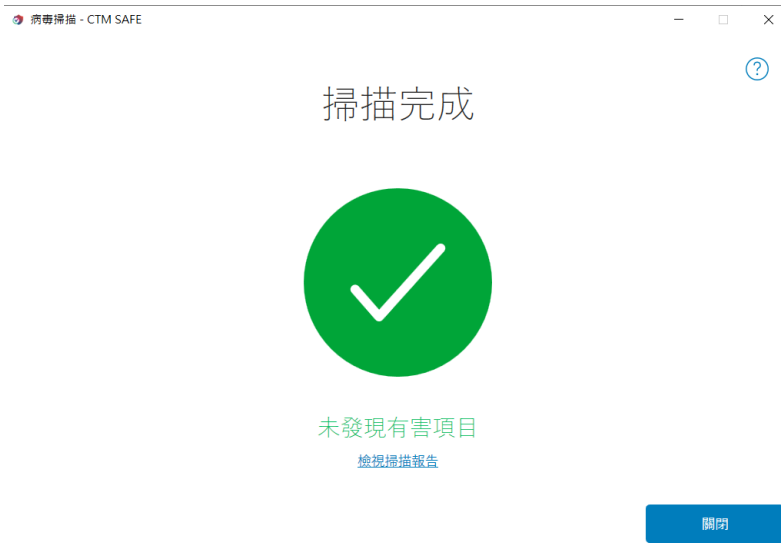
選項	說明
清除	自動清理檔案。無法清理的檔案將被隔離。
隔離區	將檔案存放在無法傳播或損害您的電腦的安全區域。
刪除	將檔案從您的電腦中永久移除。
跳過	暫時不執行任何動作，讓檔案留在您的電腦中。
排除	允許應用程式執行並從日後的掃描中將其排除。

註：一些選項並非可用於所有有害項目類型。

- 選擇全部處理以啟動清理程式；
- 病毒掃描將顯示最終結果以及已清理的有害檔案數量。

註: 病毒掃描可能需要您重新啟動電腦以完成清理程式。如果清理需要重新啟動電腦，請選擇重新啟動以完成有害項目清理並重新啟動電腦。

- 您可以透過選擇開啟上一次的掃描報告，來查看上次病毒掃描的最終結果。



## 掃描報告 - CTM SAFE

2022年3月4日 15:54:41 - 15:55:27 (UTC + 08:00)

電腦名稱：DESKTOP-T1FJOBJ

掃描類型：病毒掃描

目標：

- 系統

### 結果

- 未發現有害項目
- 已掃描項目：7067

### 版本資訊

掃描引擎：

- F-Secure Capricorn: 18.0.824 (2022-03-04)
- F-Secure Hydra: 6.0.425 (2022-02-26)
- F-Secure Lynx: 2.6.4
- F-Secure Online: 18.10.897
- F-Secure USS: 6.0.179 (2020-04-14)
- F-Secure Virgo: 1.3.28 (2022-03-02)
- F-Secure Virgo Detection: 18.10.897

版權所有 © 1998 - 2021 F-Secure Corporation。保留所有權利。

[產品支援](#) | [隱私政策](#) | [F-Secure](#)

對於由 F-Secure 全球資訊網網頁或經由第三方建立或發佈的任何材料，F-Secure 不承擔任何責任。除非您在提交材料至我們任何網頁或透過電子郵件或 F-Secure CGI 電子郵件明確表明，否則，表示您同意您所提供的材料可在 F-Secure 全球資訊網頁面上或以印刷版本的形式發佈。按一下加載的鏈結，您即可進入 F-Secure 公共網站。此時，您的存取權與網域名稱將會記錄至我們的私人存取統計資料中。此資訊不會提供給任何第三方，您同意不針對所提交的材料向我們提出任何訴訟，除非另有明確說明，否則，提交材料即表示您授權 F-Secure 可在 F-Secure 產品/出版物中採用材料中的任何概念，而無需承擔任何責任。

以下是 macOS 的手動執行病毒掃描流程：

您可以掃描你的主資料夾或你指定的任何位置。如果懷疑檔或資料夾可能包含一些惡意軟體，您可以手動掃描這些檔或資料夾。

要開始手動掃描：

1. 選擇功能表列中的 CTM SAFE 圖示。
2. 選擇「選擇要掃描的內容」。

提示:將打開一個視窗，您可以在其中選擇要掃描的內容及位置。

3. 如果產品發現任何惡意軟體在掃描過程中，它會顯示檢測到的惡意軟體的名稱和位置，並將受感染的檔移動到垃圾桶。

提示: 清空垃圾桶以永久刪除受感染的文件。

4. 點擊主頁上的「病毒掃描」，掃描電腦上的病毒。


# 技術支援

在這裡，您能找到可幫助您解決技術問題的資訊。

## 使用支援工具

在聯絡支援前，請運行支援工具搜集有關硬體、作業系統、網路配置及已安裝軟體的基本資訊。

在 Windows 運行支援工具：

1. 從 Windows **開始**功能表打開 F-Secure SAFE。
2. 在主視圖上選擇  功能表按鈕。
3. 選擇**說明和支援**。
4. 選擇**編輯設定**。  
**註: 您需要管理權限才能運行該工具。**
5. 選擇 **運行支援工具**。
6. 在**支援工具**視窗選擇**執行診斷**。

macOS 用戶運行支援工具：

1. 前往**應用程式**下的產品資料夾，然後執行**支援工具**應用程式。
2. 在**支援工具**視窗選擇**執行診斷**。
3. 輸入計算機的管理員密碼。  
支援工具隨機啟動並顯示資料搜集的進度。
4. 數據收集完成後，選擇要保存結果的位置 **tar.gz** 存檔然後選擇 **節省**。  
支援工具可開啟 **Finder** 視窗，顯示儲存的檔案。

**註: 您需要管理權限才能運行該工具。**

工具完成執行後，會將收集的資料儲存至桌面的封存檔案中。聯絡客戶支援時，您可提供收集的資料(診斷檔案)。

# CTM SAFE 不同平台的功能比較

	 PC	 Mac	 Android	 iOS
惡意軟件防護	•	•	•	-
病毒掃描	•	•	•	-
防勒索軟件保護	•	-	-	-
瀏覽保護	•	•	•	•
銀行保護	•	•	•	•
家長控制功能 - 遙距管理設定	•	•	•	•
家長控制功能 - 篩選內容	•	•	•	•
家長控制功能 - 時間限制	•	•	•	•
家長控制功能 - 應用程式控制	-	-	•	-

## 聯絡我們

如有任何查詢，請聯絡澳門電訊服務第一熱線：1000。