

F-SECURE ID PROTECTION (CTM)

合作夥伴用家常見問題

January 2022

目錄

目錄	2
1 CTM ID PROTECTION 概要	3
2 常見問題	4
一般情況	4
系統安裝	4
監察	5
VAULT(密碼管理器)	5
訂閱期完結	6

1 CTM ID PROTECTION 概要

CTM ID PROTECTION (以下簡稱 CTM IDP) 監視和偵測網上個人資訊有否外洩，並對身份盜竊的威脅作出快速的反應。此特別針對手機應用程式的解決方案目的在於防禦現今多種形式的身份盜竊，當檢測到個人資訊外洩時，會立即向您發出警報通知。每個警報都會為您提供度身定制的建議，說明如何最有效處理被洩露的資訊，並明確提出下一步建議。CTM IDP 同時還可以作為一個易於使用的密碼管理器，為您提供一個快捷有效的措施以防止身份被盜竊。

通過 CTM IDP，你可以做到以下幾點：

- 保護你自己和你家人的個人資訊，避免成為網路犯罪的受害人。
- 當您的個人資料(或其中一部份)發現被洩露時，您會收到警報通知以及如何應對事件的相關指引。
- 通過設定高強度的密碼，以及在所有設備上同步密碼，提高你的安全性。

本文件的目的是在於收集部份使用者（消費者）的問題及其答案。

2 常見問題

一般情況

問：犯罪分子是如何獲取我的個人資訊？

答：網路犯罪分子可以通過多種方式獲取你的個人資訊，例如通過一般線上服務的填寫資料、惡意軟體入侵、釣魚網站、跟蹤你的網路流量或其他不同方式等。

問：什麼是資料洩露？

答：資料洩露是指有意或無意地將敏感和機密的個人或財務資料在一個不安全的環境中洩露。當網路犯罪分子闖入一家公司或線上服務點並竊取客戶或使用者的私人資訊時，資料就會洩露。這些資訊可能包括個人身份資訊，如姓名、身份證號碼、地址以及重要的財務資訊，如信用卡號碼和銀行帳戶等。

系統安裝

問：CTM IDP 支援哪些作業系統？

答：CTM IDP 支持 Android、iOS、Windows 和 Mac。手機應用程式附有密碼管理器和 ID 監察功能。Windows 和 Mac 應用程式則提供密碼管理功能。

問：CTM IDP 是否只在手機上監察個人資訊？

答：不是。監察實際上在伺服器端進行。手機應用程式作用在於設置監察，並在個人資訊被竊取時顯示警報。手機應用程式令你得到更貼身保護，因為手機通常總是開著，而且在附近。這是能立即通知你的最簡單有效方法。

問：為什麼我需要為 CTM IDP 設定主密碼？

答：主密碼非常重要，因為它可以讓您打開應用程式，並保證您的密碼資料安全。一旦您安裝了 CTM IDP，並首次啟動該應用程式，該應用程式會要求您設定一個主密碼。選擇一個你能記住但難以猜測的主密碼（或口令），而該應用程式或 F-Secure 亦不能重置你的主密碼。而應用程式不能重設主密碼是 F-Secure 有意的決定，此舉能提高個人安全和隱私度，保護您的個人資料。

問：應用程式不斷提醒我輸入主密碼的恢復代碼。為什麼我需要設定此恢復代碼？

答：主密碼的恢復代碼是一個獨特的個人代碼，如果您忘記了主密碼，這是能重新獲得應用程式訪問權的唯一方法。F-Secure 設定上不能恢復任何主密碼，因為這代表著要存取您的主密碼，當中存在安全風險。

問：我可以指紋或面部識別來存取密碼嗎？

答：可以。如果你想使用指紋解鎖應用程式，請選擇「下次使用時使用指紋解鎖」。但請注意，在您使用指紋解鎖 CTM IDP 之前，您首先需要註冊您的指紋。請查閱設備使用者手冊，瞭解如何在您的設備上使用指紋識別。

監察

問：CTM IDP 如何知道要監察哪些個人資訊？

答：在您啟動產品並設定主密碼後，您會被要求將您的一個電子郵件地址添加到監察專案中。一封驗證郵件會發送到您的電子郵件信箱。在您點擊驗證郵件中的連結後，監測就會開始。已經發現的漏洞資料會顯示在應用程式螢幕上。而此電子郵件地址會被自動添加為連絡通知用途。

問：為什麼在顯示結果之前我需要驗證電子郵件地址？

答：出於安全和隱私的考慮，每個添加的電子郵件地址都需要經過驗證。這樣其他人就不能在他們的應用程式中添加你的電子郵件地址，並看到你被洩露的個人資訊詳情。

問：CTM IDP 是否對我在密碼管理器中添加的所有電子郵件地址進行監察？

答：不。監察範圍只適用於在應用程式的監察選項中加入的電子郵件地址。

問：CTM IDP 在數據洩露的資料中發現了我的個人資訊。這些不同漏洞的嚴重程度代表什麼意思？

答：F-Secure 根據資料洩露的不同嚴重程度進行排名，其依據是：1) 您的資料被洩露的程度，2) 洩露的潛在危害程度，以及 3) 洩露的資料是否以易讀取的格式還是已加密的格式，從而分為三個嚴重級別：

嚴重程度(高) - 包括你的密碼或你的信用卡細節在以可讀的格式下被讀取。

嚴重程度(中) - 可能涉及您的身份證號碼或您的密碼以亂碼的形式出現，或其他較低重要性的個人資訊被洩露。

嚴重程度(低) - 涉及以下個人資訊洩露如用戶名、全名、出生日期、電話號碼或地址等。

問：我在洩露通知中能得到什麼資訊？

答：如果您的個人資訊在洩露事件中被發現，通知內容中會提到：

- 1) 哪些個人身份資訊 (PII) 與該洩露事件有關連，
- 2) 相關的洩露事件內容，
- 3) 什麼公司或團體被牽涉當中，
- 4) 事件在何時發生，以及
- 5) 洩露的其他個人身份資訊(如有)。

VAULT(密碼管理器)

問：我怎樣才能在密碼管理器中添加密碼？

答：你可以在應用程式的密碼管理器選項中按加號圖示，輕鬆存儲新密碼。

問：我以前使用過另一個密碼管理器。我可以在密碼管理器中導入我的密碼嗎？

答：可以。CTM IDP 支援用不同的格式導入資料。

問：我怎樣才能使用存儲在密碼管理器中的密碼？

答：您可以使用手機的剪貼板（複製/粘貼）功能或通過啟用自動填寫功能手動複製這些資料。自動填寫功能可以在大多數瀏覽器 and 應用程式中使用。

問：我怎樣才能在我的所有設備上同步密碼？

答：為了準備密碼的備份，我們建議你啟用密碼同步功能。而為了能夠在所有設備上同步你的資料，你需要連接安裝了此應用程式的設備。然後通過「功能表>連接設備」進行設置。當你進入該功能表時，會自動生成一個同步代碼，它每次的有效期是 60 秒。當前代碼過期後會立即生成一個新的代碼。在您想同步您的應用程式資料的設備上打開應用程式。進入功能表>連接設備，並輸入同步代碼。選擇連接。當出現提示時，輸入您在其他設備上使用的主密碼。當同步成功時，選擇確認。

問：F-Secure 能否看到我存儲在 CTM IDP 中的密碼？

答：不可以。您的主密碼和主加密金鑰絕不會存儲在任何地方。加密金鑰只在您使用該產品時存在。當您關閉 CTM IDP 時，加密金鑰會被銷毀。保存在 CTM IDP 中的資訊並沒有辦法能解密。此外，任何使用 CTM IDP 的人對 F-Secure 來說都是匿名的，因此我們無法識別使用者的資料。我們在任何情況下都看不到你的任何資訊，因此我們無法解密或將其交給其他廠商。然而，這也意味著，如果你忘記了主密碼，F-Secure 也沒有辦法為你恢復密碼或資料。

訂閱期完結

問：如果我取消訂閱 CTM IDP，存儲的密碼會怎樣？

答：ID 監察和在設備之間的同步密碼會在過期的訂閱後停止存取，但仍然可以存取密碼。

問：過期後，我是否需要立即卸載 CTM IDP？

答：不，您可以繼續將其作為非同步密碼管理器使用。但添加新密碼並不如以前方便，因為它們不會在您的所有設備上同步。