WithSecure Client Security for Windows

目錄

第 章
1

入門

主題：

此部分說明如何存取產品工具和功能，以及如何變更產品設定。

註：您的管理員可執行某些安全設定，也就是說您可能無法在本地變更某些功能。

1.1 免責聲明

F-Secure Business 現在更名為 WithSecure™，以新徽標和名稱的形式體現。

我們正在對我們的產品進行品牌重塑，在此期間，您可能會在產品和門戶中看到F-Secure和WithSecure™的混合，直到完成所有更改。

1.2 系統需求

本節包含有關信息 WithSecure Client Security.

我們強烈建議您閱讀整個文檔。

支持的操作系統

註: WithSecure僅支持其供應商支持的操作系統。如果您有興趣為供應商不再支持的平台提供長期支持，請聯繫您的銷售代表。

WithSecure Client Security支持以下操作系統：

Microsoft Windows 10（所有 32 位和 64 位版本，包括 Windows 10 IoT Enterprise）
Microsoft Windows 11（所有版本）

註: 不支持 ARM。

註: 在安裝產品之前，您必須為您的操作系統安裝 Windows Universal C Runtime 和最新的 Service Pack。

註: 操作系統必須支持 Microsoft Azure 代碼簽名證書。您可以找到更多信息這裡。

系統需求

磁盤空間：2GB 可用磁盤空間用於安裝、自動更新和正常操作。隔離和掃描報告可能需要額外的磁盤空間，具體取決於發現的病毒。
互聯網連接：需要互聯網連接才能接收更新和使用基於雲的技術功能。

支持的語言

支持的語言有：英語、中文（中國、台灣、香港）、捷克語、丹麥語、荷蘭語、愛沙尼亞語、芬蘭語、法語、加拿大法語、德語、希臘語、匈牙利語、意大利語、日語、韓語、挪威語、波蘭語、葡萄牙語、巴西葡萄牙語、羅馬尼亞語、俄語、斯洛文尼亞語、西班牙語、拉丁美洲西班牙語、瑞典語和土耳其語。

1.3 變更產品設定

您可以透過變更設定，控制產品的動作。

請注意，您需要擁有管理員權限方可變更產品設定。部分產品設定可從系統匣圖示上下文菜單存取。

註: 您的管理員可執行某些安全設定，也就是說您可能無法在本地變更某些功能。

相關工作

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

變更 Windows 防火牆設定 位於頁面37
防火牆開啟後，將限制電腦的存取。部分應用程式可能需要您在防火牆中對其進行允許，才能正常運作。

檢視產品的最近事件 位於頁面7

您可在事件歷程記錄頁面查看產品執行的動作以及它如何保護您的電腦。

關閉所有安全功能 位於頁面6
如果您需要釋放更多系統資源，則可關閉所有安全功能。

1.3.1 產品設定快速存取

很多產品設定可從系統匣圖示上下文菜單存取。

要打開托盤圖標上下文菜單，請按照以下說明操作：

註: 如果產品圖示隱藏，則先按一下工作列中的顯示隱藏圖示箭頭。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 內容功能表包含以下選項：

選項	說明
檢視當前狀態	顯示您的電腦的當前保護狀態。
檢查更新	檢查並下載最新更新。
檢視最近的事件	顯示產品為保護您的電腦所執行的動作。
打開設定	打開產品設定。
關於	顯示產品的版本資訊。

1.3.2 關閉所有安全功能

如果您需要釋放更多系統資源，則可關閉所有安全功能。

註: 您的管理員可能設定了阻止您關閉安全功能的原則。

註: 關閉安全功能後，您的電腦將不會受到全面保護。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇關閉所有安全功能。

下次重啟電腦時，功能將自動再次開啟。您還可在產品的主視圖中手動開啟。

1.4 如何檢視產品的功能

防護狀態圖示可表示產品正在運行，而防護統計資料則表示產品對您電腦的防護方式資料。

1.4.1 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。

保護狀態圖示：

狀態圖示	狀態名稱	說明
	確定	您的電腦已受保護。 功能已開啟並正常運行。
	過期	您的電腦未受保護。 該訂閱已過期。
	過期並停用	您的電腦未受保護。 訂閱已過期，產品已被停用。
	已停用：故障	電腦未受到完全保護（或未受保護）。 產品需要即時動作，例如關鍵功能已關閉、故障，或您的更新已極為陳舊。
	已停用	電腦未受到完全保護。 產品需要您的注意，例如，基於信譽的瀏覽等安全功能關閉。
	更新中	正在設立防護。 產品正在更新。

保護狀態托盤圖標

當產品需要您注意或採取操作時，系統托盤上會顯示以下保護狀態圖示。

狀態托盤圖標	狀態名稱	說明
	注意力	電腦未受到完全保護。 該產品需要您的關注，例如，一項或多項安全功能已關閉或更新非常舊。
	警告	您的電腦未受保護。 該產品需要立即採取措施，例如訂閱已過期或關鍵功能故障。

1.4.2 檢視產品的最近事件

您可在事件歷程記錄頁面查看產品執行的動作以及它如何保護您的電腦。

事件歷程記錄為您顯示已安裝產品的各種事件以及產品已採取的保護措施的詳情。例如，您可看到所有檢測到的有害項目，包括已清除或已隔離的。

若要查看產品的整個事件歷程記錄：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇最近事件。
   事件歷程記錄頁面打開。

事件歷程記錄為您顯示各個事件的時間和描述。根據事件類型，您可按一下事件以了解更多相關詳情。例如，就有害檔案而言，您可查看以下資訊：

發現有害檔案的日期和時間
惡意軟件的名稱及其在電腦上的位置
已執行的動作

第 章
2

保護電腦，抵禦有害內容

主題：

產品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，惡意軟件防護會在發現有害檔案時立即予以處理，以免造成損害。

產品會自動掃描您的本機硬碟、任何卸除式媒體(如可攜式磁碟機或光碟) 與下載內容。

產品還將監視計算機是否有任何表明計算機存在有害檔案的變更。產品檢測到任何危險系統變更時(如系統設定變更或重要系統進程變更嘗試)，其 DeepGuard 組件則會阻止應用程式運行，因 為它可能造成損害。

註: 您的管理員可執行某些安全設定，也就是說您可能無法在本地變更某些功能。

2.1 有害內容有什麼影響

有害應用程式和檔案會嘗試損毀您的資料，或未經授權而存取您的電腦系統，以竊取私人資訊。

2.1.1 潛在的垃圾應用程式 (PUA) 和垃圾應用程式 (UA)

「潛在的垃圾應用程式」包含您可能認為不良或有害的運行狀況或特性，「垃圾應用程式」可能對您的裝置或資料產生更嚴重的影響。

如果滿足以下條件，則應用程式被認定為「潛在的垃圾應用程式」(PUA)：

- 影響您的私隱或工作效率 - 例如，暴露個人資訊或執行未經授權的動作
- 對您的裝置的資源施加不必要的壓力 - 例如，使用過多的儲存體或記憶體空間
- 影響您的裝置或儲存在裝置上的資訊的安全 - 例如，讓您接觸到意料之外的內容或應用程式

這些運行狀況或特性對您的裝置或資料的影響可能是輕微或者嚴重的。但卻不足以有害到切實將其歸類為惡意軟件。

如果應用程式有影響更嚴重的運行狀況或特性，則可視為「垃圾應用程式」(UA)。產品將更加謹慎地對待此類應用程式。

產品將根據應用程式為 PUA 或 PA 對應用程式區別處理：

- 潛在垃圾應用程式 - 產品將自動封鎖應用程式的運行。如果您確定應用程式可信，可讓 WithSecure 產品將其從掃描中排除。您必須有管理員權限，方可從掃描中排除已封鎖的檔案。
- 惡意應用程式 - 產品會自動阻止應用程式的運行。

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.1.2 蠕蟲

蠕蟲為透過網路將自身副本從一個裝置傳送至另一個裝置的程式。有些蠕蟲還對受影響的裝置執行有害操作。

很多蠕蟲旨在看起來讓用戶覺得有吸引力。它們偽裝成影像、視訊、應用程式或任何其他類型的有用程式或檔案。欺詐的目的就是為了引誘用戶安裝蠕蟲。其他還有一些蠕蟲力求完全隱蔽，它們利用裝置中 (或裝置中安裝的程式)的瑕疵將自身安裝在裝置中，且永遠不會引起用戶的注意。

一旦安裝，蠕蟲則利用裝置的實體資源建立自身副本，然後將其傳送至任何可以透過網路到達的其他裝置。如果有大量蠕蟲傳送，則裝置的效能可能受損。如果一個網路中的很多裝置受影響並傳送蠕蟲副本，則網路本身可能會中斷。有些蠕蟲還可對受影響的裝置造成更直接的損害，如修改儲存在裝置上的檔案，安裝其他有害應用程式或竊取資料。

大多數蠕蟲僅在一種特定類型的網路中擴散。有些蠕蟲可在兩個或以上的類型中擴散，但這種情況很罕見。一般而言，蠕蟲會嘗試在以下其中一種網路中擴散 (但仍有一些蠕蟲以不太熱門的渠道為目標)：

- 區域網絡
- 電子郵件網路
- 社交媒體網站
- 對等網路 (P2P) 連線
- SMS 或 MMS 訊息

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.1.3 特洛伊木馬程式

特洛伊木馬程式即提供或似乎提供有吸引力的功能或特性，但之後在幕後悄悄執行有害動作的程式。

特洛伊木馬程式以希臘神話中的「特洛伊木馬」命名，力求看起來讓用戶覺得有吸引力。它們偽裝成遊戲、螢幕保護程式、應用程式更新或任何其他類型的有用程式或檔案。有些特洛伊木馬程式模仿或者甚至完全複製熱門或有名的程式，以便看起來更值得信賴。欺詐的目的就是為了引誘用戶安裝特洛伊木馬程式。

一旦安裝，特洛伊木馬程式還可使用「誘餌」，以便讓其看起來合法。例如，偽裝成螢幕保護程式或文件檔案的特洛伊木馬程式將顯示影像或文件。當用戶因為這些誘餌而分心時，特洛伊木馬則可在幕後悄悄地執行其他動作。

特洛伊木馬程式一般會對裝置作出有害變更(如刪除檔案或對其加密，或變更程式設定)或盜取儲存在裝置上的保密資料。特洛伊木馬程序可按照其執行的動作進行分類：

特洛伊木馬程式下載程式：連線至遠端站點以下載並安裝其他程式
特洛伊木馬程式病毒植入程式：包含一個或多個額外程式 (木馬程式安裝)
特洛伊木馬程式密碼盜取程式：竊取儲存在裝置上或輸入至 Web 瀏覽器的密碼

銀行特洛伊木馬程式：明確尋找線上銀行入口網站用戶名和密碼的專門特洛伊密碼盜取程式

特洛伊間諜程式：監控裝置上的活動並將詳情傳送至遠端站點

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.1.4 後門程式

後門為可用於規避程式、裝置、入口網站或服務安全功能的功能或程式。

程式、裝置、入口網站或服務的功能可在以下情況下視為後門：其設計或執行會導致安全風險。例如，線上入口網站的硬式編碼管理員存取可能被用作後門。

後門通常利用程式、裝置、入口網站或服務代碼中的瑕疵。瑕疵可能為 Bug、弱點或未記錄的功能。

攻擊者通常利用後門取得未經授權的存取權限，或執行有害動作以便其規避存取限制、驗證或加密等安全功能。

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.1.5 惡意探索

惡意探索即利用程式中的瑕疵以讓其異常運行的對象或方式。這樣做可創造攻擊者能夠加以利用的條件，以執行其他有害動作。

惡意探索可以是對象或者方式。例如，精心建立的程式、一段代碼或一個字元字串都是對象⊠特定的命令序列則是一種方式。

入侵程式用於利用程式中的瑕疵或漏洞(又稱為弱點)。因為每個程式都是不同的，所以每個入侵程式均需依據特定的程式精心定制。

攻擊者有幾種方式來實施攻擊，從而影響電腦或裝置：

將其嵌入至被駭或精心建立的程式中 - 當您安裝並啟動程式時，惡意探索即啟動
將其嵌入至電子郵件的文件附件 - 當您打開附件時，惡意探索即啟動
將其託管在被駭或有害網站上 - 當您存取網站時，惡意探索即啟動

啟動惡意探索將導致程式異常運行，如強制其崩潰，或篡改系統的儲存體或記憶體。這樣可能為攻擊者創造條件，執行有害動作，如竊取資料或存取作業系統的受限部分。

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.1.6 惡意探索套件

惡意探索套件是攻擊者用於管理惡意探索並將有害程式傳送至易受攻擊的電腦或裝置的工具組。

惡意探索工具組包含惡意探索清單，每個惡意探索均可利用程式、電腦或裝置中的瑕疵(漏洞)。工具組本身一般託管在有害或被駭網站上，這樣任何存取網站的電腦或裝置均會受其影響。

當新的電腦或裝置連線至布有陷阱的網站時，惡意探索工具組將檢測是否存在會受工具組清單惡意探索影響的任何瑕疵，若發現此類瑕疵，則工具組啟動惡意探索並利用該漏洞。

當電腦或裝置受到影響後，惡意探索工具組可向其傳送負載。這通常是在電腦或裝置上安裝和啟動的另一個有害程式，它會反過來執行未經授權的動作。

惡意探索工具組力求模塊化且易於使用，以便其控制器可簡單將惡意探索和負載添加至工具組或將其移除。

相關工作

開啟實時掃描 位於頁面13
保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

執行惡意軟件掃描 位於頁面13
您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

使用 DataGuard 存取控制 位於頁面17
DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

2.2 如何掃描我的電腦

*惡意軟件防護*開啟時會自動掃描電腦的有害檔案。

我們建議您始終保持開啟*惡意軟件防護*。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。如果您要每天或每週定期掃描電腦，請設定排程掃描。

2.2.1 實時掃描如何運作

存取檔案時，「即時掃描」會透過掃描所有檔案，並封鎖存取含有*惡意軟件*的檔案，來防護您的電腦。

當您的電腦嘗試存取檔案時，即時掃描會在允許電腦存取檔案前，先掃描該檔案中有無惡意軟件。

如果即時掃描發現任何有害內容，則會在該檔案造成任何損害前將其放入隔離區。

即時掃描是否會影響電腦效能

通常情形下，您不會注意到掃描過程，因為其耗時較短且佔用較少的系統資源。即時掃描所需時間與系統資源視檔案內容、位置及類型等因素而定。

CD、DVD 光碟機與可攜式 USB 磁碟機等卸除式磁碟機上的檔案需要較長的時間來掃描。

註：實時掃描不掃描壓縮檔，如 ***.zip*** 檔案。

即時掃描會降低電腦運作速度，若：

您的電腦不符合系統需求，或
您同時存取大量檔案。例如，您打開一個目錄，而其中包含許多需要掃描的檔案時。

開啟實時掃描

保持實時掃描開啟，以從電腦中移除有害檔案，避免損害電腦。

若要確保實時掃描已開啟：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇惡意軟件防護 > 編輯設定。

   註：您需要管理權限才能變更某些設定。

4. 開啟即時掃描。

2.2.2 手動掃描

您可以掃描整個電腦以完全確保其不含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、間諜軟件，以及潛在惡意應用程式。它還會檢查可能被 Rootkit 隱藏的項目。全面電腦掃描可能需要較長時間才能完成。您還可僅掃描系統中經常發現有害應用程式的部分，以更有效地移除電腦上的惡意應用程式和有害項目。

掃描檔案和資料夾

如果您懷疑電腦上的特定檔案有問題，您可僅掃描這些檔案或資料夾。完成這些掃描會比掃描整個電腦快得多。例如，當您將外部硬碟或 USB 快閃磁碟機連接至電腦時，您可掃描以確保其不含任何有害檔案。

執行惡意軟件掃描

您可以掃描整個電腦以完全確保其不含任何有害檔案或惡意應用程式。

若要掃描您的電腦，請遵循下述說明：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 如果您要對手動掃描電腦的方式進行最佳化，請在主頁上選擇 ⚙，然後選擇掃描設定。
   a) 如果您不想掃描所有檔案，則選擇僅掃描通常包含有害代碼的檔案類型 (更快)。
      擁有以下副檔名的檔案為您選擇此選項時掃描的檔案類型的示例：`com`、`doc`、`dot`、`exe`、`htm`、`ini`、`jar`、`pdf`、`scr`、`wma`、`xml`、`zip`。
   b) 選擇掃描內部壓縮檔以掃描壓縮存檔內部的檔案，例如 ZIP 檔案。放棄核取該選項以掃描存檔，而是其中的檔案。
3. 在主頁上，選擇 🛡。
4. 選擇惡意軟件掃描或全面電腦掃描。

   掃描電腦的作用中記憶體以及經常發現惡意軟件的位置 (包括檔案資料夾)，惡意軟件掃描即啟動。這樣可以在更短的時間內發現並刪除電腦上的惡意應用程式和有害項目。
   全面電腦掃描會掃描內部和外部硬碟上的病毒、間諜軟件以及潛在有害的應用程式。它還會檢查可能由 Rootkit 隱藏的項目。全面電腦掃描可能需要較長時間才能完成。

   病毒掃描開始。
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，讓檔案保留在您的電腦中。
排除	允許應用程式執行並將其從以後的掃描中排除。

註: 部分選項並非可用於所有有害項目類型。

7. 選擇全部處理以啟動清理程序。
8. 惡意軟件掃描將顯示最終結果以及已清理的有害項目數。

註: 惡意軟件掃描可能需要您重新啟動電腦以完成清理程序。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。

在 Windows 檔案總管中掃描

可在「Windows 檔案總管」中，掃描磁碟、資料夾和檔案以尋找有害檔案和惡意應用程式。

如果您懷疑電腦上的某些文件，您可以僅掃描這些文件或資料夾。這些掃描比掃描整台電腦快得多。例如，當您將外部硬碟或USB隨身碟連接到電腦時，您可以對其進行掃描以確保它們不包含任何有害檔案。

若要掃描磁碟、資料夾或檔案：

1. 在要掃描的磁碟、資料夾或檔案上按一下滑鼠右鍵。
2. 從右鍵單擊菜單中選擇 掃描惡意軟件.

註: 在 Windows 11 上，選擇 顯示更多選項然後選擇 惡意軟件掃描.

病毒掃描開始，並掃描磁碟、資料夾或所選檔案。

如果在掃描期間發現有害檔案或應用程式，病毒掃描會引導您完成清理過程。

2.2.3 排程掃描

將電腦設定為不使用時自動掃描並移除惡意軟件與其他有害應用程式，或將掃描設定為定期執行，以確保電腦安全。

若要排程掃描：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇掃描設定。
4. 開啟排程掃描。
5. 在執行掃描中選擇您想要自動掃描電腦的頻率。

選項	說明
每日	每天掃描電腦。
每週	在每週的選定日期掃描電腦。從清單中選擇日期。
每四週	在所選日子掃描您的電腦，每四週一次。在清單中選擇日子。掃描會在下次遇到該日子時開始。

6. 在啟動時間中選擇何時啟動定時掃描。
7. 選擇按低優先順序運行掃描以讓排程掃描較少地干預到電腦上的其他活動。按低優先順序掃描需花費更長的時間完成掃描。

8. 如果您不想掃描所有檔案，則選擇僅掃描通常包含有害代碼的檔案類型 (更快)。
   擁有以下副檔名的檔案為您選擇此選項時掃描的檔案類型的示例：com、doc、dot、exe、htm、ini、jar、pdf、scr、wma、xml、zip。
9. 選擇掃描內部壓縮檔以掃描壓縮存檔內部的檔案，例如 ZIP 檔案。放棄核取該選項以掃描存檔，而是其中的檔案。

註: 簡報模式開啟時，排程掃描會取消。關閉*簡報模式*後，掃描會再次依照排程執行。

2.3 DeepGuard 是什麼

DeepGuard 提供針對未知威脅的主動、即時保護。

DeepGuard 監控應用程序以實時檢測和阻止對系統的潛在有害更改。它確保您只使用安全的應用程序。應用程序的安全性通過受信任的雲服務進行驗證。如果無法驗證應用程序的安全性，DeepGuard 將開始監控應用程序行為。

提示: 如果您希望 WithSecure 將您的應用程序添加到允許的應用程序列表中，請提交您的應用程序以供分析這裡.一旦我們分析了程序，如果您向我們提供了您的聯繫方式，我們將通知您分析結果。

DeepGuard阻止了新的和未被發現的 *木馬*，*蠕蟲*，*漏洞利用*以及試圖更改您的計算機並阻止可疑應用程序訪問Internet的其他有害應用程序。

DeepGuard 偵測的可能有害系統變更包括：

系統設定 (如 Windows 登錄) 變更，
嘗試關閉重要系統程式，例如安全程式：本產品，及
嘗試編輯重要的系統檔案。

若要確保 DeepGuard 已啟用：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇惡意軟件防護 > 編輯設定。

註: 您需要管理權限才能變更某些設定。

4. 選擇編輯設定。

註: 您需要管理權限才能變更某些設定。

5. 開啟 **DeepGuard**。

DeepGuard 開啟時，會自動封鎖嘗試對系統作出潛在有害變更的應用程式。

註: 所有用戶都可以看到所有 DeepGuard 規則。規則可能包括帶有個人信息的文件名和文件夾名稱。因此，請注意同一台計算機的其他用戶可以看到 DeepGuard 規則中包含的路徑和文件名。

相關工作
安全數據 位於頁面44
該服務向 WithSecure 發送有關潛在惡意活動或受保護設備的查詢*安全雲*.

2.3.1 允許 DeepGuard 已封鎖的應用程式

您可控制 DeepGuard 允許和封鎖的應用程式。

有時 DeepGuard 可能會封鎖安全的應用程式讓它無法執行，即使您想要使用該應用程式而且知道它是安全的。這是因為該應用程式嘗試可能損壞電腦的系統變更。也有可能在顯示 DeepGuard 快顯視窗時，您不經意地封鎖了該應用程式。

允許 DeepGuard 已封鎖的應用程式：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。

2. 在主頁上，選擇 ⋯。
3. 選擇隔離和排除。

   註: 您需要管理權限才能變更設定。

   

   應用程式和檔案控制檢視打開。
4. 選擇已封鎖索引標籤。
   您可了解一系列 DeepGuard 已封鎖的應用程式。
5. 找到您要允許的應用程序，然後選擇 允許。
6. 選擇 是確認您要允許該應用程序。

所選的應用程式新增至已排除清單，DeepGuard 允許應用程式再次作出系統變更。

2.3.2 使用 DataGuard

DataGuard 監控一組資料夾是否會遭遇勒索軟件或其他類似有害軟件的潛在有害變更。

勒索軟件是一種有害軟件，會將您電腦上的重要檔案加密，使您無法存取。犯罪分子會索要贖金，並答應恢復檔案，但即便您支付贖金，也無法保證能拿回個人資料。

DataGuard僅允許安全的應用程式存取受保護資料夾。產品將通知您是否有任何不安全的應用程式嘗試存取受保護資料夾。如果您了解並信任應用程式，則可允許其存取資料夾。DataGuard 還讓 DeepGuard 使用其受保護資料夾清單，以獲得額外一層保護。

您可選擇哪些資料夾需要針對勒索軟件等破壞性軟件的額外保護層。

註: 您必須開啟 DeepGuard 以使用 DataGuard。 DataGuard 僅在 Premium 版本中可用。

若要管理您的受保護資料夾：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇惡意軟件防護 > 編輯設定。

   註: 您需要管理權限才能變更某些設定。

   
4. 開啟 **DataGuard**。
5. 選擇檢視受保護資料夾。
6. 選擇受保護索引標籤。
   您將可看到所有當前受保護資料夾的清單。
7. 根據需要新增或刪除資料夾。
   若要新增新的受保護資料夾：
   a) 按一下新增。
   b) 選擇您想要保護的資料夾。
   c) 按一下選擇資料夾。
   若要移除資料夾：
   a) 選擇清單上的資料夾。
   b) 按一下移除。

   提示: 如果您想要撤銷安裝產品以來對受保護資料夾清單所作的變更，則按一下還原預設。

   

相關工作
新增和刪除受保護資料夾 位於頁面16
您可選擇哪些資料夾需要針對勒索軟件等破壞性軟件的額外保護層。

2.3.3 新增和刪除受保護資料夾

您可選擇哪些資料夾需要針對勒索軟件等破壞性軟件的額外保護層。

DataGuard 阻止任何對您的受保護資料夾的不安全存取。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇隔離和排除。

   註: 您需要管理權限才能變更設定。

   應用程式和檔案控制檢視打開。
4. 選擇受保護索引標籤。
   您將可看到所有當前受保護資料夾的清單。
5. 根據需要新增或刪除資料夾。
   若要新增新的受保護資料夾：
   a) 按一下新增。
   b) 選擇您想要保護的資料夾。
   c) 按一下選擇資料夾。

   提示: 因為您必須分開允許需要存取受保護資料夾的所有應用程式，我們建議您不要新增包含已安裝遊戲或應用程式的資料夾 (例如 Steam Library 資料夾)。否則，這些應用程序可能無法正常工作。

   若要移除資料夾：
   a) 選擇清單上的資料夾。
   b) 按一下移除。

   提示: 如果您想要撤銷安裝產品以來對受保護資料夾清單所作的變更，則按一下還原預設。

2.4 使用 DataGuard 存取控制

DataGuard 存取控制透過阻止未知應用程式存取資料夾來保護資料夾免受勒索軟件 (加密勒索) 的侵害。

註: DataGuard 僅在 Premium 版本中可用。

若要開啟 **DataGuard 存取控制**：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇惡意軟件防護 > 編輯設定。

   註: 您需要管理權限才能變更某些設定。
4. 開啟 **DataGuard 存取控制**。

2.4.1 檢視隔離的項目

您可檢視隔離區內項目的更多資訊。

「隔離區」是用來存放可能具有惡意檔案的安全區域。產品可將有害項目和潛在惡意應用程式放置在隔離區，使它們不會損害電腦。如有需要，稍後可以還原隔離區中的應用程式或檔案。若不再需要某個被隔離的項目，可將其刪除。刪除隔離區的項目會將其從電腦中永久移除。

若要檢視關於隔離區內項目的資訊：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇隔離和排除。

   註: 您需要管理權限才能變更設定。

應用程式和檔案控制檢視打開。

4. 選擇已隔離索引標籤。
   該清單向您顯示每個已隔離項目的名稱、檢測日期和感染類型。
5. 按兩下已隔離項目以了解更多資訊。
   就單個項目而言，您可了解已隔離項目的原始位置。

2.4.2 還原隔離的項目

您可還原所需的已隔離項目。

如果需要，您可以從隔離區恢復應用程序或文件。不要從隔離區恢復任何項目，除非您確定這些項目不構成威脅。恢復的項目移回計算機上的原始位置。

若要還原已隔離項目：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇隔離和排除。

   註：您需要管理權限才能變更設定。

   應用程式和檔案控制檢視打開。
4. 選擇已隔離索引標籤。
5. 選擇您想要還原的已隔離項目。
6. 按一下允許。
7. 按一下是以確認您想要還原已隔離項目。

所選的項目自動還原至其原始位置。項目可能從未來掃描中排除，具體視感染類型而定。

註：若要檢視當前已排除的檔案和應用程式，選擇應用程式和檔案控制檢視表中的已排除索引標籤。

2.4.3 將檔案或資料夾從掃描中排除

當您將檔案或資料夾從掃描中排除時，便不會掃描其是否存在有害內容。

若要將檔案或資料夾從掃描中排除：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⋯。
3. 選擇隔離和排除。

   註：您需要管理權限才能變更設定。

   應用程式和檔案控制檢視打開。
4. 選擇已排除索引標籤。
   此檢視表顯示已排除的檔案和資料夾的清單。
5. 選擇新增。
6. 選擇您不想納入掃描的檔案或資料夾。
7. 選擇確定。

所選的檔案或資料夾會從將來的掃描中排除。

2.4.4 檢視排除的應用程式

您可檢視已從掃描中排除的應用程式，若您將來想要對其進行掃描，可將其從排除項目清單中移除。

如果產品檢測到您已知為安全的潛在惡意應用程式，或您需要保留在計算機上以使用某些其他應 用程式的間諜軟體，則可將其從掃描中排除，這樣產品便不會再提醒您。

註: 若該應用程式行為類似病毒或其他惡意應用程式，則無法排除。

此外，DeepGuard不會阻止某些Steam遊戲。因此，您不必從掃描中排除Steam遊戲或關閉DeepGuard即可運行它們。

若要檢視已排除在掃描之外的應用程式：

1. 從Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ···。
3. 選擇隔離和排除。

   註: 您需要管理權限才能變更設定。

   應用程式和檔案控制檢視打開。
4. 選擇已排除索引標籤。
   此檢視表顯示已排除的檔案和資料夾的清單。
5. 若要重新掃描排除的應用程式：
   a) 選擇想要加入掃描中的應用程式。
   b) 按一下移除。

新的應用程式僅在您掃描時將其排除后顯示在排除清單上，不會直接新增至排除清單。

2.4.5 新增和刪除受保護資料夾

您可選擇哪些資料夾需要針對勒索軟件等破壞性軟件的額外保護層。

DataGuard 阻止任何對您的受保護資料夾的不安全存取。

1. 從Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ···。
3. 選擇隔離和排除。

   註: 您需要管理權限才能變更設定。

   應用程式和檔案控制檢視打開。
4. 選擇受保護索引標籤。
   您將可看到所有當前受保護資料夾的清單。
5. 根據需要新增或刪除資料夾。
   若要新增新的受保護資料夾：
   a) 按一下新增。
   b) 選擇您想要保護的資料夾。
   c) 按一下選擇資料夾。

   提示: 因為您必須分開允許需要存取受保護資料夾的所有應用程式，我們建議您不要新增包含已安裝遊戲或應用程式的資料夾(例如Steam Library資料夾)。否則，這些應用程序可能無法正常工作。

   若要移除資料夾：
   a) 選擇清單上的資料夾。
   b) 按一下移除。

   提示: 如果您想要撤銷安裝產品以來對受保護資料夾清單所作的變更，則按一下還原預設。

2.5 防止應用程式下載有害檔案

您可防止電腦上的應用程式從互聯網下載有害檔案。

某些網站包含可能損害電腦的入侵程式和其他有害檔案。透過進階網路保護，您可在有害檔案到達電腦前，阻止應用程式下載這些有害檔案。

若要封鎖任何應用程式下載有害檔案：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 選擇編輯設定。

   註：您需要管理權限才能變更設定。

3. 在主頁上，選擇 ⚙。
4. 選擇惡意軟件防護 > 編輯設定。

   註：您需要管理權限才能變更某些設定。

5. 開啟進階網路保護。

   註：即使您關閉防火牆，此設定也有效。

2.6 利用 AMSI 整合識別基於指令碼的攻擊

反惡意程式碼掃描介面 (AMSI) 是允許對內置指令碼服務進行深入檢查的 Microsoft Windows 組件。

註：AMSI 整合僅適用於 Windows 10。

進階惡意軟件使用偽裝或加密的指令碼，以避免傳統的掃描方法。此類惡意軟件通常直接載入記憶體，因此不會使用裝置上的任何檔案。

AMSI是一種介面，在Windows上運行的應用程式和服務可利用該介面將掃描請求傳送到電腦上安裝的反惡意程式碼產品。這針對使用核心 Windows 組件 (如 PowerShell 和 Office365) 或其他應用程式上的指令碼或巨集以逃避偵測的有害軟件提供了額外防護。

開啟 AMSI 產品整合：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇惡意軟件防護 > 編輯設定。

   註：您需要管理權限才能變更某些設定。

4. 開啟反惡意程式碼掃描介面 (AMSI)。
   產品現在通知您 AMSI 偵測到的任何有害內容，並將這些偵測記錄在事件歷程記錄中。

第 章
3

保護您的 Web 瀏覽

主題：

瀏覽保護可在瀏覽器上提供網站的安全評級，並封鎖評級為有害的網站，幫助您安全瀏覽互聯網。

3.1 封鎖有害網站

開啟時，瀏覽保護會封鎖對有害網站的存取。

確保銀行保護已開啟：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇安全瀏覽。
4. 選擇編輯設定。

   註：您需要管理權限才能變更設定。

5. 開啟瀏覽保護。
6. 如果您的瀏覽器開啟，請重新啟動瀏覽器以套用變更的設定。

   註：瀏覽保護要求您使用的 Web 瀏覽器開啟瀏覽保護延伸。

3.1.1 封鎖可疑或禁止的網站

瀏覽保護可防止您無意中存取不可信或包含禁止內容的網站。

有時，您可能瀏覽至包含可疑、侵權，或禁止內容的網站。例如網站可能為虛假、已知垃圾資訊網站，包含潛在惡意程式，或無論在何位置均是非法的。

您可使用瀏覽保護來避免不小心存取此類網站。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇安全瀏覽。
4. 選擇編輯設定。

   註：您需要管理權限才能變更設定。

5. 確保瀏覽保護已開啟。
6. 除被視為有害的網站外，如果您要封鎖被評定為可疑的網站，請選擇封鎖可疑網站。
7. 如果您想要封鎖包含禁止內容的網站，則請選擇封鎖禁止的網站。
8. 如果您的瀏覽器開啟，請重新啟動瀏覽器以套用變更的設定。

   註：瀏覽保護要求您使用的 Web 瀏覽器開啟瀏覽保護延伸。

3.1.2 使用信譽評級圖示

在您使用 Google、Bing、Yahoo 或 DuckDuckGo 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定。搜尋結果上每個連結的安全評定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。
⛔	該網站有害。我們建議您避免瀏覽該網站。或者，管理員已封鎖此網站，您無法瀏覽它。
❓	該網站尚未經過分析且目前沒有可用的資訊。
✅	此網站的存取權限不會封鎖。

若要查看搜尋結果中的信譽評級圖示：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇安全瀏覽。
4. 選擇編輯設定。

   註: 您需要管理權限才能變更設定。

5. 確保瀏覽保護已開啟。
6. 選擇在搜尋結果中顯示網站的信譽評定。
7. 如果您的瀏覽器開啟，請重新啟動瀏覽器以套用變更的設定。

   註: 瀏覽保護要求您使用的 Web 瀏覽器開啟瀏覽保護延伸。

3.1.3 網站遭到封鎖時要執行的動作

當您嘗試存取評定為有害的網站時，瀏覽保護封鎖頁面即會顯示。

當瀏覽保護封鎖頁面顯示時：

1. 如果要進入網站，請選擇在這台電腦上允許網站。您需要管理員權限才能允許被封鎖的網站。新增允許的網站視窗打開，顯示您將要允許的地址。
2. 選擇確定。

被封鎖的網站打開。此外，產品會將網站新增到允許的網站清單中。

如果您認為被封鎖的網站是安全的，根本不應該被封鎖，則可在此提交網站以進行分析。

註: 如果沒有顯示封鎖頁面，請確保您使用的 Web 瀏覽器已開啟瀏覽保護延伸。

3.1.4 網站例外

網站例外清單會顯示允許或封鎖的特定網站。

註: 如果您的管理員明確封鎖某網站或某網站包含已封鎖的內容，則即使您已將其新增至允許的網站清單，也無法存取該網站。

若要檢視和編輯網站例外：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇安全瀏覽 > 編輯設定。
4. 選擇檢視網站例外。

   若您要編輯的網站已列為已允許或已拒絕的網站，而您要將其從一個清單移到其他清單：

   a) 根據您要編輯的網站清單，選擇已允許或已拒絕索引標籤。
   b) 在清單中的該網站上按一下滑鼠右鍵，然後選擇允許或拒絕。

   如果任一清單中均不包含該網站：

   a) 若您要允許網站，請選擇已允許索引標籤⊠若您要封鎖網站，請選擇已拒絕索引標籤。
   b) 選擇新增，以將新網站新增到清單中。
   c) 輸入要新增的網站位址，然後選擇確定。
   d) 在網站例外對話方塊中，選擇關閉。

5. 選擇確定以返回主頁面。

若要變更已允許或已封鎖的網站地址，請在清單中的該網站上按一下滑鼠右鍵，然後選擇編輯。

若要從清單中移除已允許或已封鎖的網站，請選擇該網站，然後按一下移除。

3.2 透過 GPO 瀏覽保護擴充部署

有關如何在 Google Chrome、Microsoft Edge 和 Mozilla Firefox 中安裝 WithSecure Browsing Protection 擴充功能的說明。

註: 說明是 Elements Endpoint Protection-特定於管理員使用者。

WithSecure瀏覽保護是 Web 瀏覽器的擴展，為已安裝的瀏覽器提供 HTTPS 協定支持 WithSecure安全產品。

註: 在不使用擴充的情況下提供 HTTP 支援。

該擴展使與安全使用 HTTPS 時，阻止頁面支援不需要的 Web 內容、評級圖示和搜尋引擎的安全搜尋模式。作為管理員，您可以將與安全e 瀏覽保護開啟並使用 Windows 群組原則強制開啟。

3.2.1 如何在 Google Chrome 中安裝 WithSecure 瀏覽保護擴充功能

這些說明是 Elements Endpoint Protection 特定的說明，適用於管理員使用者。

要安裝並開啟瀏覽保護擴充功能：

1. 下載最新的Google Chrome 群組原則範本 ADMX 文件。
2. 將以下 Chrome 管理範本檔案和您系統中使用的語言的語言資料夾複製到 `C:\Windows\PolicyDefinitions`目錄：

   `policy_templates/windows/admx/chrome.admx and google.admx`
3. 將檔案和系統中使用的語言的語言資料夾也複製到 SYSVOL 資料夾中：`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.

   例如：`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`。

   註: 如果您沒有 PolicyDefinitions 資料夾，則需要建立它。
4. 開啟 Windows 群組原則管理主控台 (`gpmc.msc`）並建立新的群組原則或編輯現有策略。

   註: 欲了解更多信息，請參閱在 Windows 中建立和管理群組原則管理範本的中央存儲。
5. 去 `Computer Configuration/Policies/Administrative Templates/Google/Google Chrome/Extensions/Configure the list of Force-Installed apps and extensions` 並如下編輯策略：

   a) 選擇 啟用開啟該策略。

   b) 在選項下，選擇 展示...並輸入以下值：

   ```
   jmjjnhpacphpjmnnlnccpfmhkcloaade
   ```

   註: 有關更多信息，請參閱如何設定 Chrome 瀏覽器政策。

當群組原則啟動時，WithSecure Browsing Protection 會開啟並強制開啟。

3.2.2 如何在 Microsoft Edge (Chromium) 中安裝 WithSecure 瀏覽器保護擴充功能

這些說明是 Elements Endpoint Protection 特定的說明，適用於管理員使用者。

註: WithSecure 瀏覽器擴充功能是透過 Microsoft 群組原則物件 (GPO) 從 Google Store 安裝的。該裝置必須是 Microsoft Active Directory 網域的成員，否則無法完成此安裝。

要安裝並開啟瀏覽器保護擴充功能：

1. 使用 Microsoft Edge 策略檔案執行下列操作：
   a) 去Microsoft Edge (Chromium) 群組原則範本 ADMX 文件。
   b) 選擇 下載**Windows**策略在瀏覽器的版本和內部版本以及您的作業系統下，然後選擇 接受並下載。
   c) 提取您下載的 cab 檔案。
   d) 從提取的資料夾中，複製到 `C:\Windows\PolicyDefinitions`資料夾和您的 SYSVOL 資料夾（`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`）以下文件和資料夾：

      Microsoft Edge (Chromium) 管理範本檔案：`msedge.admx`和 `msedgeupdate.admx`
      您系統中使用的語言的語言資料夾

      註: 如果您沒有 PolicyDefinitions 資料夾，則需要建立它。

2. 開啟 Windows 群組原則管理主控台 (gpmc.msc) 並執行下列其中一項操作：

      註: 欲了解更多信息，請參閱在 Windows 上設定 Microsoft Edge 策略設定。

   建立新的群組原則
   去 `Computer Configuration/Policies/Administrative Templates/Microsoft Edge/Extensions/Control which extensions are installed silently`並如下編輯策略：

   a. 選擇 啟用開啟該策略。
   b. 在選項下，選擇 展示...並輸入以下值：

```
cpikpibllpjmpnchjajlibnmmomnnhnm
```

當群組原則啟動時，WithSecure Browsing Protection 會開啟並強制開啟。

3.2.3 如何在 Mozilla Firefox 中安裝 WithSecure 瀏覽保護擴充功能

這些說明是 Elements Endpoint Protection 特定的說明，適用於管理員使用者。

要安裝並開啟瀏覽器保護擴充功能：

1. 下載最新的Mozilla Firefox 群組原則範本 ADMX 文件。
2. 解壓縮 cab 檔案並將以下 Mozilla Firefox 管理範本檔案和系統中使用的語言的語言資料夾複製到 `C:\Windows\PolicyDefinitions`目錄：

   `windows/mozilla.admx and firefox.admx`

3. 將系統中使用的語言的檔案和語言資料夾也複製到 SYSVOL 資料夾中：
   `\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.
   例如：`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`。

      註: 如果您沒有 PolicyDefinitions 資料夾，則需要建立它。

4. 開啟 Windows 群組原則管理主控台 (`gpmc.msc`）並建立新的群組原則或編輯現有策略。
5. 去 `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions to install`並如下編輯策略：
   a) 選擇 啟用開啟該策略。
   b) 在選項下，選擇 展示...並輸入以下值：

```
https://download.sp.f-secure.com/online-safety/fs_firefox_https.xpi
```

6. 去 `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Prevent extensions from being disabled or removed`並如下編輯策略：
   a) 選擇 啟用開啟該策略。
   b) 在選項下，選擇 展示...並輸入以下值：`ols@f-secure.com`。

當群組原則啟動時，WithSecure Browsing Protection 會開啟並強制開啟。

3.3 檢查瀏覽器延伸是否在使用中

基於信譽的瀏覽需要瀏覽器延伸來保護您的網頁瀏覽、線上銀行和購物，並在您瀏覽互聯網時向您顯示安全資訊。

在電腦上安裝產品後，產品會嘗試自動安裝瀏覽器延伸。當您打開瀏覽器時，它會顯示有關新安裝的延伸的通知，您可能需要啟用它。

如果您的瀏覽器中未列出 WithSecure 瀏覽保護延伸，則需手動重新安裝該延伸。

如果您錯過了通知，產品主視圖會顯示瀏覽器延伸是否尚未安裝。針對瀏覽器安裝延伸的最簡單方法是從產品主視圖上顯示的通知中選擇安裝，然後按照螢幕上的說明進行操作。

但是，如果您在產品的主視圖上沒有看到通知或者您錯過了通知，則可透過以下方式檢查瀏覽器延伸是否已安裝和啟用：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇左下角彈出螢幕中的編輯設定。

   註：您需要管理權限才能變更某些設定。

4. 選擇是以允許應用程式對您的裝置作出變更。
5. 選擇安全瀏覽。
6. 根據您使用的 Web 瀏覽器，執行以下動作：

   如果您使用 **Firefox**，請在附加元件和主題 > 延伸下方，選擇 新增至 **Firefox**。延伸即新增完畢並針對 Firefox 啟用。

   如果您使用**Chrome**，請先選擇瀏覽器延伸下方的打開**Chrome**線上應用程式商店連結。WithSecure 瀏覽保護頁面將在 Chrome 線上應用程式商店中打開。如果延伸已安裝在 Chrome 上但關閉，請前往延伸並將其開啟。如果尚未安裝延伸，請選擇新增至 **Chrome** > 新增延伸。延伸即新增完畢並針對 Chrome 啟用。

   如果您使用 **Microsoft Edge**，請先選擇瀏覽器延伸下方的打開 **Edge** 附加元件連結。 WithSecure 的「瀏覽保護」頁面將在 Edge 附加元件中打開。如果延伸已安裝在 Microsoft Edge 上但已停用，請選擇開啟以將其啟用。如果尚未安裝延伸，則選擇獲取 > 新增延伸。延伸即新增完畢並針對 Microsoft Edge 啟用。

   註：升級產品或安裝新瀏覽器後，您可能需要重新安裝延伸。

您可以在瀏覽器中打開以下測試頁面，以檢查瀏覽器延伸是否已開啟：https://unsafe.fstestdomain.com。如果產品區頁面打開，則瀏覽器延伸正在使用中。如果未看到產品區頁面，則需手動開啟瀏覽器延伸。

第 章

4

保護您的敏感資料

主題：

*連線控制*提高安全性以防止攻擊者干擾您的保密交易，並讓您在存取線上銀行或進行線上交易等情況下免遭有害活動的侵害。

*連線控制*自動偵測與線上銀行網站的安全連線，並封鎖任何不指向既定網站的連線。開啟線上銀行網站時，將僅允許線上銀行網站連線，或對線上銀行業務而言安全的網站連線。

如果您需要存取被封鎖的網站以完成進行中的交易，則可暫時允許存取被封鎖的頁面，或結束*連線控制*工作階段。

*連線控制*目前支援以下瀏覽器：

Microsoft Edge (Chromium)
Firefox
Google Chrome

4.1 開啟連線控制

*連線控制*開啟時會額外保護您的安全連線。

*連線控制*開啟時可封鎖不安全的連線。例如，當您存取銀行網站或進行線上支付時，*連線控制*將啟用並封鎖所有對線上銀行業務而言不必要的連線，這樣它們便無法干擾您的保密交易。

若要開啟*連線控制*：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇安全瀏覽 > 編輯設定。

   註：您需要管理權限才能變更設定。

4. 開啟連線控制。
5. 若要調整*連線控制*設定：

   如果您不希望*連線控制*關閉您已經打開的連線，則清除斷開不受信任的應用程式。如果您保持選中該設定，則*連線控制*亦會在啟用時關閉您當前的所有網路連線。
   如果您必須使用被*連線控制*封鎖的外部工具，則清除斷開命令列和指令碼處理工具。

   註：我們建議您保持選擇該設定，除非絕對需要存取您的銀行認證和個人資訊，因為一些惡意軟件攻擊可使用內置的 Windows 組件，如 PowerShell。

   選擇您想要*連接控制*處理已復製到剪貼簿的資料的方式。預設情況下，*連線控制*工作階段結束時，*連接控制*清除剪貼簿中的所有資料，以保護您的隱私。

   如果您不想*連線控制*清除您的剪貼簿，則清除此設定。

   預設情況下，銀行工作階段期間會封鎖對您的裝置的遠端存取。銀行交易始終是私密且保密的，如果有人能遠端存取您的裝置，則切勿登入您的線上銀行。

   重要：切勿在其他人要求的情況下清除在銀行工作階段期間封鎖遠端存取設定，除非您知道請求存取的人和請求的確切目的。

4.2 使用連線控制

*連線控制*開啟時會在您存取線上銀行網站時自動執行偵測。

在瀏覽器中打開線上銀行網站時，*連線控制*指示器會顯示在螢幕的頂端。銀行保護處於使用中狀態時，將封鎖所有其他連線。

提示：如果您不希望在*連線控制*啟用時中斷其他已啟用連線，則選擇連線控制指示器，然後選擇連線控制通知右上角的 ⚙，以變更設定。

若要結束您的*連線控制*工作階段並還原您的其他連線：

1. 按一下螢幕頂部的連線控制 指示器。
2. 按一下通知上的結束。

第 章

5

設定內容控制

主題：

您可以限制對不當內容的存取，以避免在網路上看到不適當的材料。

網路上到處都是有趣的網站，但有些網站會包含您認為不合適或不適當的內容。

使用內容封鎖程式，您可透過限制可以檢視哪些網頁並安排可以上網的時間來確保不會在電腦上看到不當內容。您還可阻止指向成人內容的連結在搜尋引擎結果中顯示。

5.1 封鎖網頁內容

您可限制瀏覽網頁時可以檢視的內容類型。

您可以封鎖對含有不當內容的網頁的存取。

若要選擇要封鎖的網絡內容類型：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇 **Web** 內容控制。
4. 從下拉式功能表中選擇設定適用於誰。
5. 開啟內容篩選以限制您在所有瀏覽器上選擇的內容。

   要按內容類型阻止網頁，請選擇 阻止網頁內容。然後，選中要阻止的內容類型旁邊的複選框。
   要僅允許訪問某些網頁，請選擇 只允許選擇的網站。然後，選擇 查看允許的網站並輸入您要允許的網址。

6. 要從搜索結果中隱藏成人內容，請打開 搜索結果過濾器。

5.1.1 內容類別

您可以阻止存取多種類型的內容。

流產	包含有關墮胎、墮胎診所和中心以及一般墮胎主題的資訊或圖像的網站。例如，可能支持墮胎或支持墮胎的論壇。
廣告服務	指向各種 Flash、文字、影片或圖像檔案或包含廣告的其他類似文件的 Web 連結。
成人	成人受眾且內容明顯涉及性或包含性暗示的網站。例如，性用品商店網站或以性為導向的裸體。
酒精和菸草	展示或宣傳酒精飲料或吸煙和菸草產品的網站，包括釀酒廠、葡萄園和啤酒廠等製造商。例如，宣傳啤酒節的網站以及酒吧和夜總會的網站。
匿名者	允許或指導人們如何繞過網路過濾器的網站，包括允許人們這樣做的基於網路的翻譯網站。例如，提供可用於繞過可能的網路過濾器的公共代理程式清單的網站。
拍賣	人們可以在其中購買和銷售其產品或服務的線上市場網站。這包括提供產品或服務清單的網站，即使實際交易可能發生在其他地方。
銀行業	銀行和其他金融機構的網站，包括儲蓄和投資銀行、證券交易和外匯交易網站。
部落格	人們或機構發布資訊並可以分享新聞、故事、影片和照片的部落格。由於其個體性質，部落格中討論的主題可能有很大差異，並且可以包含任何主題。
聊天	人們可以透過文字、音訊或視訊相互聊天的線上入口網站和通訊工具。例如，基於網路的聊天和即時通訊應用程式以及聊天網站。
約會	提供尋找浪漫或性伴侶入口網站的網站。例如，婚友網站或郵購新娘網站。
藥品	宣傳吸毒的網站。例如，提供有關購買、種植或銷售任何形式的這些物質的資訊的網站。
娛樂	與娛樂產業相關的網站，例如電視節目、書籍、漫畫、電影和劇院以及藝廊。例如，電視和廣播節目指南以及音樂、電視和電影評論網站。
賭博	人們可以使用真錢或某種形式的信用進行線上投注的網站。例如，線上賭博和彩票網站，以及包含有關線上或現實生活賭博資訊的部落格和論壇。
遊戲	線上遊戲網站以及人們可以玩、下載或購買遊戲的網站。
駭客攻擊	提倡尋找和利用電腦系統或電腦網路中的弱點以獲取利潤、挑戰或享受的網站。例如，包含駭客指南和駭客工具的網站。
恨	顯示對特定宗教、種族、國籍、性別、年齡、殘疾或性取向有偏見的網站。例如，宣揚對人類、動物或機構造成傷害的網站，或包含針對其中任何人進行人身攻擊的描述或圖像。

非法下載	未經授權的檔案共用或軟件盜版網站。例如，提供軟件的非法或可疑存取權限的此類網站，以及開發和散佈可能危害網絡和系統的程式的此類網站。
求職	就業機構和承包商的網站，人們可以在其中搜尋和找到新工作。例如，職業搜尋引擎、職業網路團體和就業網站。
支付服務	處理購物網站與銀行或其他金融服務（例如信用卡）之間付款的網站。其中包括一般可用於支付的網站。
騙局	透過承諾在填寫調查、參加測驗或執行類似操作後提供獎品來引誘人們的網站。
購物	人們可以在其中購買任何產品或服務的網站，包括包含有助於線上訂購和購買的商品目錄的網站以及提供有關線上訂購和購買商品資訊的網站。
社群網路	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，諸如 Twitter。
軟體下載	用於下載各種軟體的線上入口網站。
垃圾郵件	從垃圾郵件收集的網站。
串流媒體	免費或透過訂閱模式提供串流影片或音訊內容的網站。
暴力	可能煽動暴力或包含恐怖和暴力圖像或影片的網站。例如，包含強姦、騷擾、鼻煙、炸彈、攻擊、謀殺和自殺資訊的網站。
武器	包含武器或任何可用作武器對人類或動物造成傷害的資訊、圖像或影片的網站，包括推廣這些武器的組織，例如狩獵和射擊俱樂部。此類別包括玩具武器，例如漆彈槍、氣槍和 BB 槍。
網路郵件	允許人們透過網頁瀏覽器建立和存取其電子郵件帳戶的網站。例如，這包括雅虎 Mail 和 Gmail，以及本地、ISP 連結的網頁郵件服務。

第 章
6

使用搜尋結果過濾

主題：

搜索結果過濾器通過確保 Google、Yahoo、Bing 和 YouTube 使用安全搜索“嚴格”級別來隱藏成人內容。

雖然這不能阻止所有不適當和露骨的內容出現在您的搜索結果中，但它可以幫助您避免大多數此類材料。

6.1 打開搜尋結果過濾器

您可以開啟搜尋結果過濾以從搜尋結果中封鎖偏激內容。

開啟搜尋結果過濾：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 。
3. 選擇 **Web** 內容控制。
4. 開啟搜尋結果過濾。

搜尋結果篩選開啟時，會對登入該 Windows 用戶賬戶的任何人覆寫網站上的 SafeSearch 設定。

第 章
7

集中管理

主題：

該產品按照中央管理模式運行，而產品設定由受信任的專家遠端控制。

在集中管理模式下：

可能會在遠端設定部分或全部產品設定。
可能會鎖定上述部分設定，這樣，您自己便無法對其進行變更。

常用設定 > 集中管理頁面向您顯示關於您的電腦的資訊。如果您的產品設定有問題，則可將該資訊提供給您的 IT 管理員。

使用 Windows 事件檢視器來檢查記錄的錯誤。

7.1 開啟 Windows 事件檢視器

若懷疑產品發生問題，您可使用 Windows 事件檢視器檢查是否記錄了錯誤。

Windows 事件檢視器儲存匯入系統事件的詳細資訊。這包括此產品的動作和錯誤的詳細資訊。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇集中管理。
4. 按一下打開事件檢視器。
   Windows 事件檢視器將會開啟。
5. 若要查找來自該產品的訊息，則按一下 **Windows 日誌**並選擇應用程式或系統。

   註: 您可按一下來源以按來源對訊息排序。這可讓您更方便地找到來自此產品的訊息。

第 章
8

什麼是防火牆

主題：

*防火牆*防止入侵者和有害應用程式透過網際網路進入您的電腦。

防火牆只允許來自您的電腦的安全網路連線並封鎖網路入侵。

8.1 變更 Windows 防火牆設定

防火牆開啟後，將限制電腦的存取。部分應用程式可能需要您在防火牆中對其進行允許，才能正常運作。

產品使用 Windows 防火牆保護電腦。

變更 Windows 防火牆設定：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主視圖中，選擇病毒和威脅。
3. 選擇 **Windows** 防火牆設定。

如需 Windows 防火牆的詳細資訊，請參閱 Microsoft Windows 文件。

8.2 使用個人防火牆

產品設計為與 Windows 防火牆搭配使用。其他個人防火牆需要進行額外的設定才能與產品搭配使用。

產品使用 Windows 防火牆作為基本的防火牆功能，如控制傳入網路流量，以及保持您的內部網路獨立於公共網路。此外，DeepGuard 監控已安裝的應用程式，並防止可疑應用程式未經您允許存取網際網路。

如果您將 Windows 防火牆替換為個人防火牆，請確保它允許所有 WithSecure 進程的傳入和傳出網絡流量，並且當個人防火牆提示您這樣做時，您允許所有 WithSecure 進程。

提示：如果您的個人防火牆具有手動過濾模式，請使用它來允許所有 WithSecure 進程。

第 章
9

使軟件保持最新

您可以使用產品來檢查安裝在電腦上的軟件，並安裝缺失的更新。

註: 您的管理員可限制在受管理的電腦上安裝軟件更新。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 。
   軟件更新視圖顯示尚未安裝的更新。
3. 選擇按一下此處以管理更新。

   註: 您需要管理員權限方可安裝缺失的更新。
4. 若要查看是否有新更新可用，請選擇立即檢查。
5. 選擇要安裝的更新。
6. 選擇安裝所選更新。
   安裝索引標籤顯示每個所選更新的狀態和進度。

第 章
10

如何使用更新

主題：

更新可以保護您的電腦免受最新威脅。

當您連線至網路時，產品會自動擷取電腦的最新更新。它會偵測網路流量，即使網路連線速度較慢，也不會干擾您的其他網路使用。

10.1 檢視最新更新

檢視最新更新的日期和時間。

當自動更新開啟時，您連線到互聯網後，產品會自動接收最新的更新。

若要查看安裝產品最新更新的詳細資料，則可：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇更新。
4. 可在連線下檢視最新更新的詳細資訊。
5. 若要手動檢查最新的更新，則選擇立即檢查。
   如有可用更新，產品將自動安裝。

   註：想要檢查最新更新時，互聯網連線必須處於啟用狀態。

10.2 更新隔離的 Client Security 主機上的惡意軟體定義

如果您在沒有網路連線的主機上安裝了 Client Security，則可以使用原則管理員提供的工具更新惡意軟體定義。

下載更新的工具與策略管理器捆綁在一起，可以使用提供的腳本進行提取。當您在任何可以存取互聯網的電腦上運行它時，該工具會下載最新的更新和所需的差異以產生一體化存檔。

預設情況下，該工具使用 `data\updates`資料夾用於儲存下載的更新二進位檔案。它還儲存更新歷史記錄，以用作將相關差異下載到最新版本的參考。

除了更新二進位檔案之外，您還需要 `fsaua-update_32`用於匯入準備好的更新的工具。該工具包含在 Client Security 安裝套件中：`C:\Program Files (x86)\F-Secure\Client Security\fsaua-update_32.exe`。

若要更新惡意軟體定義：

1. 在策略管理器電腦上執行以下命令來準備該工具：

   視窗：`<F-Secure installation folder> \管理伺服器 5\bin\prepare-fspm-definitions-update-tool.bat<destination folder>`
   Linux：`/opt/f-secure/fspms/bin/prepare-fspm-definitions-update-tool<destination folder>`

2. 如有必要，將準備好的二進位檔案傳輸到可以存取互聯網的電腦。
3. 如有必要，修改工具配置：

   `conf\channels.json`：這包含要更新的頻道清單。預設情況下，它包含由策略管理器管理的所有支援客戶端的更新，因此我們建議您僅保留您的環境所需的 Client Security 版本。

4. 運行該工具：

   視窗：`fspm-definitions-update-tool.bat`
   Linux：`fspm 定義更新工具`

   產生的存檔包含全套最新定義以及與此版本的差異。如果所有資料都是最新的，則不會產生存檔。
5. 傳輸準備好的存檔（`data\f-secure-updates.zip`預設）到隔離 Client Security 主機上的隔離主機目錄：`C:\Program Files (x86)\F-Secure\Client Security`
6. 在隔離主機上啟動更新：運行`C:\Program Files (x86)\F-Secure\Client Security\fsaua-update_32.exe`具有管理員權限。

10.3 變更連線設定

關於如何更改電腦連線至互聯網的方式以及您在使用行動網路時想要如何處理更新的說明。

您的互聯網服務提供商 (ISP) 可能提供或要求您使用 Proxy。Proxy 擔當您電腦與互聯網之間的中介。它會攔截發往互聯網的所有請求，檢查是否能夠使用自身快取來滿足請求。利用Proxy可提昇效能、篩選請求，並能在互聯網上隱藏您的電腦，從而提高安全性。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇更新 > 編輯設定。

   註: 您需要管理權限才能變更某些設定。

4. 在手動 **Proxy** 設定下，選擇電腦是否使用 Proxy 伺服器連線至網際網路。

   若電腦直接連線至互聯網，請選擇不使用。
   選擇使用瀏覽器的設定，以使用您在預設網頁瀏覽器中已設定的相同 HTTP Proxy 設定。
   選額自訂位址並隨後加入 Proxy 位址與連接埠以手動配置你的 HTTP Proxy 設定。

第 章
11

私隱權

主題：

該部分講述什麼是 Security Cloud 以及您能夠如何貢獻匿名資料並幫助我們改善產品。

11.1 安全數據

該服務向 WithSecure 發送有關潛在惡意活動或受保護設備的查詢安全雲.

WithSecure Security Cloud 是一個基於雲的網絡威脅分析系統，由 WithSecure 運營。我們收集最少的數據，為您提供您已訂閱的安全服務，並為我們的用戶提供高質量的保護。

借助 Security Cloud，WithSecure 可以保持對全球威脅形勢的最新概覽，並在首次發現新威脅時保護我們的客戶免受威脅。

Security Cloud 僅收集可能包含有關因安全原因被 WithSecure 阻止的文件或網站的信息的數據。安全數據不用於個性化營銷目的。

貢獻資料

作為貢獻者，您允許 Security Cloud 保留有助於我們加強您對新出現的威脅的保護的安全數據。以這種方式收集的數據僅保留有限的時間，並在該期限過後刪除。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 轉到 隱私設置頁面。
4. 選擇編輯設定。

   註: 您需要管理權限才能變更設定。

   
5. 在 **Security Cloud** 下，選擇允許深入分析。

11.2 改善產品

您可透過傳送使用資料以幫助我們改善產品。

若要傳送使用資料：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 轉到 隱私設置頁面。
4. 選擇編輯設定。

   註: 您需要管理權限才能變更設定。

   
5. 在產品改進下，選擇傳送非個人使用資料。

   註: 您可以閱讀我們的隱私聲明這裡.

   

第 章
12

技術支援

主題：

在這裡，您能找到可幫助您解決技術問題的資訊。

如果您對產品有任何疑問或問題，請在聯繫我們的客戶支持之前訪問WithSecure社區看看你是否能在那裡找到你的問題的答案。

12.1 產品的版本資訊在何處

需要與我們聯絡時，我們的客戶支援可能會詢問你的產品版本。

要檢視目前的版本資訊：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇支援。
4. 在版本資訊下可找到目前已安裝產品的資訊。

12.2 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、網路配置與已安裝軟體的基本資訊。

如果您的安全產品出現技術問題，我們的客戶支援可能會要求您建立 WSDIAG 檔案並將其發送給我們的技術支援。該文件包含可用於故障排除和解決特定於您的電腦的問題的資訊。

您可以使用支持工具創建文件。該工具收集有關您的系統及其配置的信息。這些信息包括產品詳細信息、操作系統日誌和系統設置。請注意，部分信息可能是機密的。收集的信息存儲在一個文件中，該文件保存在您的計算機桌面上。

要運行支援工具：

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。
3. 選擇支援。
4. 選擇編輯設定。

   註: 您需要管理權限才能變更設定。

5. 選擇 運行支持工具。
6. 在支援工具視窗選擇執行診斷。
   支援工具隨機啟動並顯示資料搜集的進度。

該工具完成運行後，會將收集的數據保存到桌面上的存檔中。您可以在此處提交收集的數據（診斷文件）：https://www.withsecure.com/en/support/contact-support/email-support .

提示: 如果您無法透過產品本身存取支援工具，請轉至支援工具網頁及以下 適用於 **Windows** 的支援工具 **(WSDIAG)**， 選擇 下載並保存 `wsdiag_standalone.exe`文件，例如在您的下載資料夾中。雙擊該檔案以運行該工具。

12.3 調試產品問題

調試日誌記錄可幫助我們的客戶支持分析和解決產品中的問題（如果有）。

您可以暫時授予我們的客戶支持特定權限以分析產品中的問題。請注意，調試日誌收集的信息可能被視為敏感信息。

WebView2 是一種用於在本機應用程序中嵌入 Web 內容的技術。比如我們的賬號登錄頁面就使用了 WebView2技術。

如果您在使用嵌入式 Web 視圖時遇到問題，WebView2 控制台調試器可以幫助我們的客戶支持為您分析 Web 視圖問題。

授予我們的支持人員調試產品問題的臨時權限：

註: 轉動 調試日誌僅當我們的客戶支持代理要求您這樣做時。

1. 從 Windows 開始功能表中打開 WithSecure Client Security。
2. 在主頁上，選擇 ⚙。

3. 選擇編輯設定。

   註: 您需要管理權限才能變更設定。

4. 在下面 工具, 選擇撥動開關開啟 調試日誌.
   啟用調試日誌記錄後，**WebView2** 控制台調試器選項變得可見。
5. 如果你想開啟 **WebView2** 控制台調試器, 選擇撥動開關。
   輸入嵌入式 Web 視圖後，控制台窗口將打開。
6. 一旦我們的客戶支持完成對問題的分析，請關閉 調試日誌通過選擇切換開關。

12.4 電話詐騙以及如果您認為自己是目標該怎麼辦

不幸的是，隨著詐騙者使用社會工程來瞄準受害者，電話詐騙呈上升趨勢。

本主題旨在幫助您識別這些呼叫，並在最壞的情況下（如果您已成為目標）為您提供有關下一步操作的一些信息。

什麼是電話詐騙

電話可以作為冷呼叫開始，也可以通過廣告或鏈接觸發您的計算機上的彈出窗口。這些彈出窗口會敦促您撥打廣告中的技術支持號碼彈出窗口可能會突然出現並且不是那麼容易擺脫。

如何識別電話詐騙

這些類型的電話通常遵循一定的模式：詐騙者通常聲稱您的計算機有問題，比如病毒（實際上並沒有），然後他們誘騙您為也不存在的服務付費。他們讓你措手不及，玩弄你的情緒。這是基本場景：

電話詐騙者聲稱來自知名公司，例如 Microsoft、您的銀行，甚至您的網絡運營商。由於他們使用信譽良好的名稱，這讓您更放心。他們似乎也知識淵博並使用技術術語，這使他們看起來合法且可信。

由於風險似乎真實存在並且您擔心可能的計算機病毒，因此您讓騙子訪問您的計算機。他們說服您讓他們安裝一個應用程序，讓他們可以使用遠程訪問工具訪問您的計算機。

一旦騙子可以訪問您的計算機，他們就會假裝修復病毒，並且還可能會要求您提供個人憑據。當騙子“解決”了問題後，他們會要求您登錄您的網上銀行或要求您填寫一張包含信用卡詳細信息的表格。騙子會向您收取虛假服務的費用，結果比您想像的要多得多。事實上，很難知道他們真正向您收取了多少費用。

如果您認為自己被騙了怎麼辦

如果您認為自己被騙了，並且認識到我們上面描述的場景，請執行以下操作：

立即行動。
立即聯繫您的信用卡公司或銀行，報告騙局並取消任何銀行或信用卡。如果您及時採取行動，他們甚至可以停止交易並撤銷收費。
向有關當局報告騙局。
更改您認為可能受到影響的每個網站或服務上的所有密碼。
卸載任何未知的第三方軟件。
在您的計算機上運行完整掃描：打開您的安全產品，然後選擇 病毒和威脅 > 全電腦掃描.

關於不請自來的電話要記住的事情

如果您接到此類電話，請想一想：我有要求嗎

註: 通常，如果您已經與他們聯繫並創建了支持票，則客戶支持會打電話給您。

遠程會話通常用於技術支持，作為幫助您解決問題的一種方式。

記住: 只允許與您認識和信任的人或公司進行遠程會話。僅當您事先聯繫過您的服務提供商並與他們有有效的支持案例時，才允許遠程會話。此外，請像保護任何其他密碼一樣保護您的遠程訪問數據。

永遠不要讓您不認識的人訪問您的設備。授予詐騙者遠程訪問權限實際上意味著您將管理員權限移交給了您的計算機。即使您安裝了防病毒軟件，這也無法再保護您，因為騙子會控制您的計算機。

Microsoft 已通知其用戶，他們絕不會在其軟件的錯誤消息或警告消息中包含電話號碼。

切勿隨意交出任何個人憑據或信用卡詳細信息。

立即掛斷電話。

這些類型的電話是非法的，如有疑問，請向處理欺詐行為的相關部門求助並舉報。

安全產品如何提供幫助

安裝安全產品後，您的計算機將免受病毒、木馬和勒索軟件的侵害。瀏覽保護、銀行保護和遠程訪問工具保護功能還增加了另一層保護，確保您可以安全地瀏覽和進行網上銀行。

如果您已成為目標並且已經安裝了安全產品，您可以立即運行完整的計算機掃描，以幫助檢測詐騙者可能安裝的任何應用程序這些被稱為潛在不需要的應用程序 (PUA)。但是，該產品無法保護您免受這些類型的電話詐騙。

保持警惕並保持安全。