

F-Secure Anti-Virus 2013

目錄

第 1 章： 安裝.....	5
首次安裝前說明.....	6
首次安裝本產品.....	7
安裝和升級應用程式.....	8
說明和支援.....	9
 第 2 章： 入門.....	 11
如何使用自動更新.....	12
檢查更新狀態.....	12
變更互聯網連線設定.....	12
檢查即時保護網絡的狀態.....	13
如何查看產品已執行的動作.....	14
檢視通知歷程記錄.....	14
變更通知設定.....	14
即時防護網絡.....	15
什麼是「即時防護網絡」.....	15
「即時防護網絡」優點.....	15
您將提供的數據.....	15
我們對您隱私的保護方式.....	16
成為「即時防護網絡」的參與者.....	17
有關「即時防護網絡」的問題.....	17
我如何知道我的訂閱有效.....	18
行動作業中心.....	18
啟動訂閱.....	18
 第 3 章： 簡介.....	 21
檢視整體防護狀態.....	22
檢視產品統計資料.....	23
處理產品更新.....	24
檢視資料庫版本.....	24
變更行動式寬頻設定.....	24
什麼是病毒與其他惡意軟件.....	26
病毒.....	26
間諜軟件.....	26
Rootkit.....	26

危險軟件.....	27
-----------	----

第 4 章： 防護電腦不受惡意軟件侵害.....29

如何掃描我的電腦.....	30
自動掃描檔案.....	30
手動掃描.....	31
掃描電郵.....	35
檢視掃描結果.....	35
如何從掃描排除檔案.....	36
排除檔案類型.....	36
依位置排除檔案.....	36
檢視排除的應用程式.....	37
如何使用隔離區.....	38
檢視隔離的項目.....	38
還原隔離的項目.....	38
什麼是 DeepGuard.....	39
開啟或關閉 DeepGuard.....	39
允許 DeepGuard 已封鎖的應用程式.....	39
在相容模式下使用 DeepGuard.....	40
如何處理可疑行為警示.....	40

安裝

主題：

首次安裝前說明
首次安裝本產品
安裝和升級應用程式
說明和支援

首次安裝前說明

感謝您選擇 F-Secure。


若要安裝此產品，您需要以下項目：

安裝 CD 或安裝套件。若您使用不帶光碟機的迷你筆記型電腦，可從 www.f-secure.com/netbook 下載安裝套件。

您的訂閱密鑰。

互聯網連線。

若您安裝了其他供應商的安全產品，安裝程式會自動嘗試將其移除。若未自動移除，請手動將其移除。

 註：若您的電腦擁有多個帳戶，安裝時請以有管理員權限的帳戶登入。

首次安裝本產品

產品安裝說明。

按這些說明安裝本產品：

1. 插入 CD，或按兩下您下載的安裝程式。

若 CD 未自動啟動，請在「Windows 檔案總管」中按兩下 CD-ROM 圖示，然後按兩下安裝檔案以開始安裝。

2. 請依螢幕上的說明操作。

若您從商店購買產品光碟，則可在《快速安裝指南》的封面上找到訂閱密鑰。


若您從 F-Secure 線上商店下載本產品，則可在購買訂單之確認電郵中找到訂閱密鑰。

您可能需要重新啟動電腦，才能驗證訂閱密鑰並從互聯網下載最新更新。若從 CD 安裝，請記得在重新啟動電腦前取出安裝 CD。

安裝和升級應用程式

新訂閱啟動說明。

請依照以下說明啟動您的新訂閱，或使用啟動列安裝新應用程式：

 註：您可在 Windows 系統匣上找到啟動列圖示。

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
快顯視窗功能表將開啟。
2. 選擇[檢視我的訂閱](#)
3. 在[我的訂閱](#)下，前往[訂閱狀態](#)頁面，然後按一下[啟動訂閱](#)。
[啟動訂閱](#)視窗將開啟。
4. 輸入您的應用程式訂閱密鑰，然後按一下[確定](#)。
5. 驗證並啟動您的訂閱後，按一下[關閉](#)。
6. 在[我的訂閱](#)下，前往[安裝狀態](#)頁面。若安裝未自動開始，請依照以下說明執行：
 - a) 按一下[安裝](#)。
安裝視窗將開啟。
 - b) 按一下[下一步](#)。
應用程式已下載，安裝開始。
 - c) 安裝完成後，按一下[關閉](#)。

新訂閱已啟動。

說明和支援

您可按一下「說明」圖示或在產品的任何畫面下按 F1，以存取線上產品說明。

註冊授權後，您將可使用附加服務，如免費的產品更新和產品支援。您可在 www.f-secure.com/register 註冊。

入門

主題：

[如何使用自動更新](#)

[如何查看產品已執行的動作](#)

[即時防護網絡](#)

[我如何知道我的訂閱有效](#)

有關本產品快速入門方法的資訊。

本節說明透過啟動列變更通用設定和管理訂閱的方式。

啟動列的通用設定是套用至安裝在啟動列上所有程式的設定。您無需分別變更每個程式中的設定，而只需編輯通用設定，所有已安裝的程式都會使用該設定。

啟動列的通用設定包括：

下載，您可在此檢視已下載更新的資訊，並手動檢查是否有新的更新可用。

連線設定，您可在此變更電腦連線至互聯網的方式。

通知，您可在此檢視以往的通知，並設定您想要查看的通知類型。

隱私權設定，您可在此選擇是否允許您的電腦連線至「即時保護網絡」。

您也可透過啟動列管理已安裝程式的訂閱。

如何使用自動更新

自動更新會持續更新您電腦上的防護。

本產品在電腦連線至互聯網時擷取最新更新。它可偵測網絡流量，而且即使網絡連線很慢時，亦不會干擾其他互聯網使用。

檢查更新狀態


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。

確保已擁有最新更新：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[開啟一般設定](#)。
3. 選擇[自動更新](#) > [下載](#)。
4. 按一下 [立即檢查](#)。

產品連線至互聯網並且檢查是否有最新的更新。若電腦未受到最新保護，則該程式會擷取最新更新。

 註：若您正使用數據機或已開啟與互聯網的 ISDN 連線，則在檢查更新前須啟動連線。


變更互聯網連線設定

通常無需變更預設設定，但您可設定伺服器連線至互聯網的方式，以便您可自動接收更新。

變更互聯網連線設定：


1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[開啟一般設定](#)。
3. 選擇[自動更新](#) > [連線](#)。
4. 在[互聯網連線](#)清單上，選擇電腦連線至互聯網的方式。

若電腦一直連線網絡，請選擇[假定一直處於連線狀態](#)。

 註：若電腦實際上沒有一直連線網絡而是設定為指定撥號，則選擇[假定一直處於連線狀態](#)會導致多次撥號。

選擇[偵測連線](#)以便僅在產品偵測到使用中的網絡連線時才會擷取更新。

選擇[偵測網絡流量](#)，以便僅在產品偵測到其它網絡流量時才會擷取更新。

 提示：若採用非通用硬件設定，導致[偵測連線](#)設定無論有無網絡連線時都偵測到使用中的網絡連線，則請選擇[偵測網絡流量](#)。

5. 在 [HTTP Proxy](#) 清單上，選擇電腦是否使用 *Proxy 伺服器* 以連線至互聯網。

若電腦直接連線至互聯網，請選擇[無 HTTP Proxy](#)。

選擇[手動設定 HTTP Proxy 伺服器](#)以設定 *HTTP Proxy* 設定。

選擇[使用我的瀏覽器的 HTTP Proxy](#)，以使用在網頁瀏覽器上已設的相同的 *HTTP Proxy* 設定。

檢查即時保護網絡的狀態

若要正常運作，許多產品功能均取決於即時保護網絡的連線。

如果存在網絡問題，或防火牆封鎖即時保護網絡流量，則狀態為「已中斷連線」。如果未安裝需要存取即時保護網絡的產品功能，則狀態為「未使用」。

若要查看狀態：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[開啟一般設定](#)。
3. 選擇[自動更新](#) > [連線](#)。

在[即時保護網絡](#)下，您可查看「即時保護網絡」的目前狀態。

如何查看產品已執行的動作

您可在[通知](#)頁面上，查看產品為保護您的電腦所執行的動作。

產品執行動作時 (如發現封鎖的病毒時) 將顯示通知。有些通知可能由您的服務供應商傳送，例如，讓您瞭解可用新服務的通知。

檢視通知歷程記錄

您可以在通知歷程記錄中查看顯示過的通知

若要檢視通知歷程記錄：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[開啟一般設定](#)。
3. 選擇[其他](#) > [通知](#)。
4. 按一下[顯示通知歷程記錄](#)。
通知歷程記錄清單會開啟。

變更通知設定

您可以選擇想要產品顯示的通知類型。

若要變更通知設定：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[開啟一般設定](#)。
3. 選擇[其他](#) > [通知](#)。
4. 選擇或清除[允許所有程式訊息](#)，以開啟或關閉程式訊息。
此設定開啟後，產品將顯示來自己安裝程式的通知。
5. 選擇或清除[允許促銷訊息](#)，以開啟或關閉促銷訊息。
6. 按一下[確定](#)。

即時防護網絡

本文件說明 F-Secure Corporation 的一項線上服務「即時防護網絡」，該服務可識別安全的應用程式和網站，同時提供可防禦惡意軟件和網站入侵程式的保護。

什麼是「即時防護網絡」

「即時防護網絡」是一項可對來自互聯網的威脅作出快速應對的線上服務。

作為「即時防護網絡」的參與者，您可以協助我們提高防禦新威脅的能力。「即時防護網絡」收集某些未知、惡意或可疑應用程式的統計資料，以及這些應用程式在您裝置上執行的作業。此資訊是匿名的，且會傳送至 F-Secure Corporation 以供合併數據分析之用。我們將使用分析的資訊提高您裝置的安全性，以防禦最新威脅和惡意檔案。

「即時防護網絡」的運作方式

作為「即時防護網絡」的參與者，您可以提供未知應用程式和網站、網站上惡意應用程式和入侵程式的相關資訊。「即時防護網絡」不會追蹤您的網頁活動或收集有關已分析網站的資訊，也不會收集電腦上已安裝的安全應用程式的相關資訊。

如果不想提供此數據，則「即時防護網絡」不會收集已安裝應用程式或已瀏覽網站的資訊。但產品需要向 F-Secure 伺服器查詢應用程式、網站、郵件和其他物件的信譽。執行查詢時將使用加密總和檢查碼，且被查詢物件本身不會傳送至 F-Secure。我們不會依用戶追蹤數據□僅會增加檔案或網站計數器的計數。

「即時防護網絡」是產品所提供保護中不可或缺的一部份，因此無法完全停止到該網絡的所有網絡流量。

「即時防護網絡」優點

透過「即時防護網絡」，您電腦將取得可防禦最新威脅的更快更準確保護，且不會收到針對非惡意的可疑應用程式發出的不必要警報。

作為「即時防護網絡」的參與者，您可以幫助我們發現新惡意軟件和未偵測到的惡意軟件，並消除病毒碼數據庫中可能出現的誤判情況。

「即時防護網絡」的所有參與者可相互幫助。「即時防護網絡」在您裝置上發現可疑應用程式時，若其他裝置上已發現同一應用程式，則您可利用其分析結果。「即時防護網絡」可提高裝置的整體效能，因為所安裝的安全產品無需重新掃描「即時防護網絡」已分析並認為其安全的應用程式。同樣的，惡意網站以及來歷不明的大量郵件的相關資訊可透過「即時防護網絡」共用，從而讓我們能為您電腦提供防禦網站入侵程式和垃圾郵件的更準確保護。

參與「即時防護網絡」的人越多，則個人參與者受到的保護越全面。

您將提供的數據

作為「即時防護網絡」的參與者，您可以提供裝置上所儲存應用程式和您所瀏覽網站的相關資訊，以便「即時防護網絡」可提供防禦最新惡意應用程式和可疑網站的保護。

分析檔案信譽

「即時防護網絡」僅會收集信譽不明的應用程式相關資訊，以及懷疑或已知為惡意軟件的檔案相關資訊。

「即時防護網絡」會收集裝置上的安全和可疑應用程式的匿名資訊。「即時防護網絡」僅收集可執行檔的資訊（例如，在 Windows 平台上，副檔名為 .cpl、.exe、.dll、.ocx、.sys、.scr 和 .drv 的可攜式執行檔）。

所收集的資訊包括：

裝置中應用程式的檔案路徑、
檔案大小及其建立或修改時間、
檔案屬性和權限、
檔案簽章資訊、
目前的檔案版本及建立檔案的公司、
檔案來源或其下載 URL，以及
已掃描檔案的 F-Secure DeepGuard 和防毒分析結果，以及
其他類似資訊。

除非發現您的個人文件受到感染，否則「即時防護網絡」絕不會收集此類文件中的任何資訊。對於任何類型的惡意檔案，「即時防護網絡」會收集感染名稱以及檔案的殺毒狀態。

透過「即時防護網絡」，您還可提交可疑應用程式以供分析。您所提交的應用程式應僅包含可攜式執行檔。「即時防護網絡」絕不會收集您個人文件的任何資訊，且絕不會上載此類資訊以供分析。

提交檔案以供分析

使用「即時保護網絡」，您還可提交可疑的應用程式，以供分析。


產品提示時，您可以手動提交單個的可疑應用程式。您僅可提交可攜式執行檔。「即時保護網絡」不會上傳您的個人文件。

分析網站信譽

「即時防護網絡」不會追蹤您的網絡活動，或收集已分析網站的相關資訊。它可在您瀏覽網站時確保所存取網站為安全網站。瀏覽網站時，「即時防護網絡」會檢查網站的安全性，並在網站被評定為可疑或惡意網站時向您發出通知。

如果您瀏覽的網站包含惡意或可疑內容，或已知的入侵程式，則「即時防護網絡」會收集網站的完整 URL，以便能分析網頁內容。

如果瀏覽未經評定的網站，則「即時防護網絡」會收集網域和子網域的名稱，在某些情況下還會收集已瀏覽網頁的路徑，以便分析和評定網站。若任何 URL 參數可能包含透過個人身份識別方式可識別出您身份的資訊，則我們會將此類參數移除，以保護您的隱私。

 註：「即時防護網絡」不會評定或分析私人網絡中的網頁，因此絕不會收集私人 IP 地址的任何相關資訊（例如企業內部網絡）。

分析系統資訊

「即時防護網絡」會收集作業系統名稱和版本、互聯網連線相關資訊，以及「即時防護網絡」使用情況的統計資料（例如網站信譽的查詢次數，以及查詢返回結果的平均時間），以便我們可監控和改善該服務。

我們對您隱私的保護方式

我們將以安全方式傳輸資訊，並自動移除數據中可能包含的任何個人資訊。

「即時防護網絡」會在將數據傳送至 F-Secure 前，移除身份識別數據，並在傳輸時將所有已收集資訊加密，以防其遭到未經授權的存取。已收集資訊不會單獨予以處理，而會與來自其他「即時防護網絡」參與者的資訊一起集中處理。所有數據將以統計和匿名方式予以分析，這意味著不會有任何數據以任何形式洩漏您的身份。

所收集數據中不會包含可能識別出您個人身份的任何資訊。「即時防護網絡」不會收集私人 IP 地址或您的個人資訊，如電郵地址、用戶名稱和密碼。雖然我們會盡力移除所有可識別個人身份的數據，但已收集資訊中可能仍會存留某些身份識別數據。在此情況下，我們不會設法利用此類無意中所收集的資料來識別您的身份。

在傳輸、儲存和處理已收集資訊時，我們將採用嚴格的安全措施，以及實體、管理和技術方面的保障措施以保護已收集的資訊。資訊將儲存於妥善位置，並存入位於我們或分包商辦事處由我們控制的伺服器上。僅授權人員方可存取收集的資訊。

F-Secure 可能會與其子公司、分包商、經銷商和合作夥伴共用所收集的資訊，但我們將始終以無法識別個人身份的匿名形式來共用資訊。

成為「即時防護網絡」的參與者

您可提供惡意程式和網站的資訊，以此來幫助我們改善「即時防護網絡」的保護功能。

安裝時，您可以選擇加入「即時防護網絡」。使用預設安裝設定，您可以為「即時防護網絡」提供數據。您可以稍後在產品中變更此設定。

依照以下說明變更「即時防護網絡」的設定：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇**開啟一般設定**。
3. 選擇**其他 > 隱私權**。
4. 勾選「參與」核取方塊，以成為「即時防護網絡」的參與者。

有關「即時防護網絡」的問題

取得「即時防護網絡」任何相關問題的聯絡資訊。

如果您對「即時防護網絡」有任何其他問題，請聯絡：

F-Secure Corporation

Tammasaarekatu 7

PL 24

00181 Helsinki

芬蘭

http://www.f-secure.com/en/web/home_global/support/contact

我們網站上將始終提供此原則的最新版本。

我如何知道我的訂閱有效


您的訂閱類型和狀態會顯示於[訂閱狀態](#)頁面上。

若訂閱即將過期或已過期，對應啟動列圖示上的程式整體保護狀態將隨之變更。

檢查訂閱有效性：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[檢視我的訂閱](#)。
3. 選擇[訂閱狀態](#)，以檢視已安裝程式的訂閱資訊。
4. 選擇[安裝狀態](#)，以查看可安裝的程式。

您的訂閱狀態和過期日期也會顯示於程式的[統計資料](#)頁面。若您的訂閱已過期，您必須在增訂之後方可繼續接收更新和使用本產品。

 註：訂閱過期後，系統匣上的產品狀態圖示會呈現閃爍狀態。

行動作業中心

行動作業中心顯示您需注意的任何重要通知。

如果您的訂閱已過期或即將過期，則行動作業中心將通知您。行動作業中心訊息的背景色彩和內容取決於您的訂閱類型和狀態：


如果您的訂閱即將過期，且有可用的免費訂閱，則訊息將使用白色背景，且包含[啟動](#)按鈕。

如果您的訂閱即將過期，且沒有可用的免費訂閱，則訊息將使用黃色背景，且包含[購買](#)和[輸入密鑰](#)按鈕。

如果您已購買新訂閱，則可按一下[輸入密鑰](#)以提供訂閱密鑰，並啟動新訂閱。

如果您的訂閱已過期，且有可用的免費訂閱，則訊息將使用紅色背景，且包含[啟動](#)按鈕。

如果您的訂閱已過期，且沒有可用的免費訂閱，則訊息將使用紅色背景，且包含[購買](#)和[輸入密鑰](#)按鈕。如果您已購買新訂閱，則可按一下[輸入密鑰](#)以提供訂閱密鑰，並啟動新訂閱。

 註：行動作業中心的[顯示通知記錄](#)連結中顯示產品通知訊息清單，而非之前的行動作業中心訊息。

啟動訂閱

若擁有新的產品訂閱密鑰或活動代碼，您需要將其啟動。


若要啟動訂閱：

1. 在啟動列最右邊的圖示上按一下滑鼠右鍵。
將顯示一個快顯功能表。
2. 選擇[檢視我的訂閱](#)。
3. 選擇以下任一動作：

按一下[啟動訂閱](#)。

按一下[啟動行銷活動代碼](#)。

4. 在開啟的對話方塊中，輸入新的訂閱密鑰或活動代碼，然後按一下[確定](#)。

 提示：若已透過電郵收到訂閱密鑰，則可從電郵中複製此訂閱密鑰，並在該欄位中貼上。

輸入新的訂閱密鑰後，新訂閱的有效日期將顯示在訂閱狀態頁面上。

簡介

主題：

[檢視整體防護狀態](#)

[檢視產品統計資料](#)

[處理產品更新](#)

[什麼是病毒與其他惡意軟件](#)

此產品保護您的電腦免受病毒和其他惡意應用程式的威脅。

產品自動掃描檔案、分析應用程式並更新，不需要您執行任何動作。

檢視整體防護狀態

狀態頁面可讓您快速檢視已安裝的產品功能及其目前狀態。

若要開啟狀態頁面：

在主頁面上按一下狀態。

狀態頁面開啟。

圖示會顯示程式及其安全功能的狀態。

狀態圖示	狀態名稱	說明
	確定	電腦已受保護。功能已開啟，且正在正常執行。
	資訊	產品通知您功能的特殊狀態。 例如，功能正在更新。
	警告	電腦未受到完全保護。 例如，產品長時間未收到更新，或某項功能的狀態需要注意。
	錯誤	您的電腦未受保護 例如，訂閱已過期，或重要功能已關閉。
	關閉	已關閉一個不重要的功能。

檢視產品統計資料

您可以在統計資料頁面中檢視產品自安裝後所執行的工作。

若要開啟統計資料頁面：

在主頁面上按一下統計資料。

統計資料頁面將開啟。

上次成功的更新檢查顯示最新更新的時間。

病毒與間諜軟件掃描會顯示自產品安裝後已掃描及清除多少個受感染的檔案。

應用程式顯示 DeepGuard 自安裝後所允許或封鎖的程式數量。

防火牆連線顯示自安裝以來允許和封鎖的連線次數。

垃圾郵件與網路釣魚篩選顯示產品偵測為有效電郵和垃圾郵件的電郵數目。

處理產品更新


產品保持保護自動更新。

檢視資料庫版本

您可在[資料庫更新](#)頁面中查看最新更新的時間和版本號。

若要開啟[資料庫更新](#)頁面：

1. 在主頁面上按一下[設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇[其他設定](#) > [資料庫版本](#)。

[資料庫版本](#)頁面顯示病毒和間諜軟件定義、DeepGuard、垃圾郵件與網路釣魚篩選更新的最新日期及其版本號。

變更行動式寬頻設定

選擇您是否要在使用行動式寬頻時下載安全更新。


 註：僅在 Microsoft Windows 7 中可使用此功能。

預設情況下，始終在您使用主營運商的網路時下載安全更新。但是，在您瀏覽其他營運商的網路時，將暫停更新。這是因為營運商間的連線價格可能不同，例如，在不同國家的連線價格不同。如果要在瀏覽時節省頻寬，可能還要節約成本，您可考慮將此設定保持不變。

 註：此設定僅可套用於行動式寬頻連線。電腦連線至固定或無線網路時，產品將自動更新。

若要變更設定：

1. 在主頁面上按一下[設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇[其他設定](#) > [行動式寬頻](#) > [下載安全更新](#)。

3. 選擇行動連線的慣用更新選項：

[僅限我的主運營商的網路中](#)

始終在主營運商的網路中下載更新。在您瀏覽其他營運商的網路時，將暫停更新。建議您選擇此選項，以用預期成本將您的安全產品保持為最新狀態。

[從不](#)

使用行動式寬頻時不下載更新。

[始終](#)

無論使用何種網路，將始終下載更新。如果您要不計成本地確保電腦安全性始終保持為最新狀態，請選擇此選項。

4. 如果您要在每次離開主運營商的網路時分別確定，請選擇[每次離開主運營商的網路時詢問](#)。

安全更新已暫停

在主營運商的網絡以外使用行動式寬頻時，安全更新可能暫停。

在此情況下，螢幕右下角會顯示已暫停通知傳單。更新暫停是由於營運商間的連線價格可能不同，例如，在不同國家的連線價格不同。如果要在瀏覽時節省頻寬，可能還要節約成本，您可考慮將此設定保持不變。但是，如果您仍想變更此設定，請按一下變更連結。

 註：

僅在 Microsoft Windows 7 中可使用此功能。

什麼是病毒與其他惡意軟件

惡意軟件為專門損壞電腦，或在您不知情的情況下將電腦用於非法目的，或從電腦上竊取資訊的程式。

惡意軟件會：

- 控制網頁瀏覽器，
- 重新導向搜尋嘗試，
- 顯示不必要的廣告，
- 記錄瀏覽的網站，
- 竊取個人資料如 銀行資訊，
- 使用電腦發送垃圾郵件，及
- 使用您的電腦攻擊其他電腦。

惡意軟件還會降低電腦的速度與穩定性。若您發現電腦速度突然變慢或經常當機，則您的電腦可能已感染 惡意軟件。

病毒

病毒指通常可將自身附在檔案上 並快速複製自身的程式□它們會更改並 取代其他檔案的內容，這樣可能會損毀 您的電腦。

病毒 是一種程式，通常會在您不知情的情況下 安裝到電腦上。安裝後，病毒試圖複製自身。病毒會：

- 使用電腦上某些系統資源，
- 可能會更改或損毀電腦上的檔案，
- 可能試圖使用您的電腦來感染 其他電腦，
- 可能允許使用電腦進行非法 活動。

間諜軟件

間諜軟件為收集您個人資訊的程式。

間諜軟件會收集以下個人資料：

- 您曾瀏覽的互聯網網站、
- 電腦上的電郵地址、
- 密碼或
- 信用卡號碼。

間諜軟件幾乎總是未經您明確授權，就自行安裝。間諜軟件可能隨有用程式安裝，也可能藉由誘使您按下誤導性快顯視窗中的選項進行安裝。

Rootkit

Rootkit 是一種使其他 惡意軟件 難以發現的程式。

Rootkit 會隱藏檔案與處理序。通常而言，其目的是隱藏電腦上的惡意活動。當 Rootkit 隱藏 惡意軟件 之後，很難發現電腦上已安裝了 惡意軟件。

此產品配備有專門針對 Rootkit 而設計的掃描程式，讓 惡意軟件 無法輕易藏身。

危險軟件

危險軟件並非為了損害電腦而特別設計的軟件，但若遭到誤用，仍可能對您的電腦造成損害。

嚴格地說，危險軟件並非惡意軟件。危險軟件程式會執行有用但也具有潛在危險的功能。

危險軟件程式的一些範例為：

- 「即時訊息」程式 (例如 IRC、多人線上交談系統)、
- 透過互聯網上在電腦間 傳送檔案所用的程式、
- 互聯網電話程式 (例如，VoIP - 互聯網語音通訊協定)、
- 遠端存取軟件 (例如 VNC)、
- 可能嘗試恫嚇或欺騙個人購買假安全軟件的恫嚇軟件，或
- 設計來略過 CD 檢查或是複製保護的軟件。

若此程式在您知曉的情形下安裝並 進行妥善設定，則其損壞電腦的可能性就要小得多。

若危險軟件是在您不知情的情形下安裝，則其 很可能含有惡意目的，應將其移除。

防護電腦不受惡意軟件侵害

主題：

[如何掃描我的電腦](#)
[如何從掃描排除檔案](#)
[如何使用隔離區](#)
[什麼是 DeepGuard](#)

病毒與間諜軟件掃描可防護您的電腦，使惡意程式無法入侵電腦進而竊取個人資訊、破壞電腦，或用於非法用途。

根據預設，所有惡意軟件類型一旦發現立即處理，以使其不會造成損害。

預設情況下，病毒與間諜軟件掃描會自動掃描您的本機硬碟、卸除式媒體 (如可攜式磁碟機或光碟) 與下載內容。您也可將其設定為自動掃描您的電郵。

病毒與間諜軟件掃描也會監看您的電腦中是否有任何變更透露出惡意軟件的跡象。若發現任何危險的系統變更 (如系統設定或變更重要系統處理程序的嘗試)，DeepGuard 即會阻止此程式執行，因為這很可能是惡意軟件。

如何掃描我的電腦

病毒和間諜軟件掃描開啟後，會自動掃描電腦中的有害檔案。您可手動掃描檔案，也可設定排程掃描。

建議您始終開啟病毒與間諜軟件掃描。想要確保電腦上沒有有害檔案，或想要掃描已從即時掃描中排除的檔案時，可手動掃描檔案。

透過設定排程掃描，病毒與間諜軟件掃描可在特定時間將有害檔案從電腦移除。

自動掃描檔案

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。

電腦嘗試存取某個檔案時，即時掃描會在允許電腦存取該檔案前，先掃描該檔案中是否含有惡意軟件。若即時掃描發現任何有害內容，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。

掃描耗時較長的檔案：

CD、DVD 光碟機與可攜式 USB 磁碟機等卸除式磁碟機上的檔案。

壓縮檔案，如 .zip 檔案。

 註：依預設不會掃描壓縮檔案。

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。

開啟或關閉即時掃描

保持即時掃描開啟，以在惡意軟件損害電腦前將其阻擋。

若要開啟或關閉即時掃描：

1. 在主頁面上按一下 [狀態](#)。
2. 按一下 [變更此頁面上的設定](#)。

 註：您需要管理權限才能關閉安全功能。


3. 開啟或關閉 [病毒和間諜軟件掃描](#)。
4. 按一下 [關閉](#)。

自動處理有害檔案

即時掃描可自動處理有害檔案，無需詢問您任何問題。

若要讓即時掃描自動處理有害檔案：

1. 在主頁面上按一下 [設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇 **電腦安全** > **病毒和間諜軟件掃描**。
3. 選擇 **自動處理有害檔案**。

若您不選擇自動處理有害檔案，則即時掃描會在發現有害檔案時，詢問您想要怎樣處理。

處理間諜軟件

病毒和間諜軟件掃描在間諜軟件嘗試啟動時立即將其封鎖。

間諜軟件應用程式啟動前，產品會將其封鎖，讓您決定要對其執行的動作。

發現間諜軟件時，選擇以下任一動作：

採取的動作	針對間諜軟件所採取的動作
自動處理	讓產品依據發現的間諜軟件決定採取的最佳動作。
隔離間諜軟件	將間諜軟件移至其無法損害電腦的隔離區。
刪除間諜軟件	從電腦移除所有與間諜軟件相關的檔案。
僅封鎖間諜軟件	封鎖存取間諜軟件，但將其保留在電腦中。
將間諜軟件從掃描中排除	允許間諜軟件執行，並將其從今後的掃描中排除。

處理危險軟件

病毒和間諜軟件掃描在危險軟件嘗試啟動時立即對其進行封鎖。

危險軟件應用程式啟動前，產品會將其封鎖，讓您決定要對其執行的動作。


發現危險軟件時，選擇以下任一動作：

採取的動作	針對危險軟件所採取的動作
僅封鎖危險軟件	封鎖存取危險軟件，但將其保留在電腦中。
隔離危險軟件	將危險軟件移至其無法損害電腦的隔離區。
刪除危險軟件	從電腦移除所有與危險軟件相關的檔案。
將危險軟件從掃描中排除	允許危險軟件執行，並將其從今後的掃描中排除。

自動移除追蹤 Cookie

移除追蹤 Cookie，可阻止其對您在互聯網上訪問的網站進行追蹤。

追蹤 Cookie 指允許網站記錄您訪問的網站的小檔案。依照以下說明讓電腦遠離追蹤 Cookie：

1. 在主頁面上按一下 **設定**。
 註：您需要管理權限才能變更設定。
2. 選擇 **電腦安全** > **病毒和間諜軟件掃描**。
3. 選擇 **移除追蹤 Cookie**。
4. 按一下 **確定**。

手動掃描

您可手動掃描檔案，例如，將外部裝置連線至電腦時，以確保其不包含任何惡意軟件。

啟動手動掃描

您可掃描整個電腦，或掃描指定類型的惡意軟件或指定位置。

若懷疑有某類型的惡意軟件則可僅掃描這種類型。若您懷疑電腦的某位置上有問題，則可僅掃描那個部分。完成這些掃描會比掃描整個電腦更快。

啟動手動掃描電腦：

1. 在主頁面上按一下**掃描**下的箭頭。
將顯示掃描選項。
2. 選擇掃描類型。
選擇**變更掃描設定**，以最佳化手動掃描對電腦中病毒與其他惡意應用程式的掃描。
3. 若選擇**選擇要掃描的項目**，會開啟供您選擇掃描位置的視窗。
掃描精靈隨即開啟。

掃描類型

您可掃描整個電腦，或掃描指定類型的惡意軟件或指定位置。

以下列出不同的掃描類型：

掃描類型	什麼是已掃描	何時使用此類型
病毒和間諜軟件掃描	電腦上某些部分中的病毒、間諜軟件與危險軟件	此類型的掃描比完整掃描快速得多。它只會搜尋系統中包含已安裝之程式檔的部分。若您想要快速檢查電腦是否乾淨無病毒，建議您使用此掃描類型，因為它可有效率地找出並移除電腦上的任何作用中惡意軟件。
全面電腦掃描	您整部電腦 (內部與外部硬碟) 上的病毒、間諜軟件與危險軟件	想要完全確保電腦上無惡意軟件或危險軟件時。此類型的掃描需要較長的時間才能完成。其中包含快速惡意軟件掃描與硬碟掃描。此類型的掃描也會檢查 Rootkit 可能藏匿的項目。
選擇要掃描的項目	特定的檔案、資料夾或磁碟機中的病毒、間諜軟件與危險軟件	懷疑電腦上的某個位置可能含有惡意軟件時，如含有從危險來源 (點對點檔案共用網絡) 下載的內容的位置。掃描所需時間視掃描目標的大小而定。在某些情況下可以快速完成掃描，例如，若掃描僅包含幾個小檔案的資料夾。
Rootkit 掃描	可疑項目可能造成安全問題的重要系統位置。掃描隱藏檔案、資料夾、磁碟機或處理序	當您懷疑電腦上可能安裝了 Rootkit 時。例如，若您最近在電腦上偵測到惡意軟件，而且想要確定它並未安裝 Rootkit。

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病毒、間諜軟件和危險軟件。

掃描磁碟、資料夾或檔案：


1. 請將滑鼠指針置於要掃描的磁碟、資料夾或檔案上，並按一下滑鼠右鍵。
2. 在「按滑鼠右鍵」功能表中，選擇**掃描資料夾中的病毒**。(選項名稱取決於是否正在掃描磁碟、資料夾或檔案。)
掃描精靈視窗會隨即開啟，並啟動掃描。

若發現病毒或間諜軟件，掃描精靈會指導您執行清除步驟。

選擇要掃描的檔案

您可以選擇要對其進行手動或排程掃描以尋找病毒及間諜軟件之檔案類型。

1. 在主頁面上按一下設定。

 註：您需要管理權限才能變更設定。

2. 選擇其他設定 > 手動掃描。

3. 在掃描選項下，從以下設定中選擇：


僅掃描最有可能受到感染的此類檔案類型，例如可執行檔。選擇此選項也可加快掃描速度。已掃描帶有以下副檔名的檔案：
 .ani、.asp、.ax、.bat、.bin、.boo、.chm、.cmd、.com、.cpl、.dll、.doc、.dot、.drv、.eml
 和 .hqx。

已
知
檔
案
類
型

掃描保存檔與資料夾。


掃
描
壓
縮
檔
案
內
部

在掃描期間使用所有可用的啟發式掃描，以尋找新的或未知的惡意軟件。

 註：如果您選擇這個選項，掃描會花費較久的時間，同時可能造成較多的誤判 (把無害的檔案報告為可疑)。

使
用
進
階
啟
發
式
掃
描

4. 按一下確定。


 註：即使您在此選擇掃描排除項目清單上的排除檔案，也不會對其進行掃描。

發現有害檔案時如何處理

選擇發現有害檔案時的處理方法



若要選擇手動掃描過程中發現有害內容時採取的動作：


1. 在主頁面上按一下設定。

 註：您需要管理權限才能變更設定。

2. 選擇其他設定 > 手動掃描。

3. 在發現病毒或間諜軟件時，選擇下列其中一個選項：

選項	說明
詢問我 (預設)	您可以選擇對手動掃描過程中發現的每個項目執行的動作。
清理檔案	產品試圖自動對手動掃描過程中發現的受感染檔案進行殺毒。  註：若產品無法清理受感染的檔案，會對其進行隔離 (除非發現位於網路或卸除式磁碟機上)，以便其無法損害電腦。
隔離檔案	產品會將手動掃描時發現的任何有害檔案移至其無法損害電腦的隔離區。
刪除檔案	產品會刪除手動掃描時發現的任何有害檔案。
僅報告	產品會將手動掃描時發現的任何有害檔案保持原狀，並在掃描報告中記錄此偵測結果。  註：若即時掃描並未開啟，而您選擇此選項，則惡意軟件仍可損害您的電腦。


 註：在排程掃描中發現有害檔案時，會自動將其清理。

排程掃描

將電腦設定為不使用時自動掃描並移除病毒與其他惡意應用程式，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. 在主頁面上按一下設定。

 註：您需要管理權限才能變更設定。

2. 選擇其他設定 > 排程掃描。

3. 開啟排程掃描。

4. 選擇想要掃描啟動的時間。

選項	說明
每日	每天掃描電腦。
每周	在每週的選定日期掃描電腦。從清單中選擇日期。
每月	在每月的選定日期掃描電腦。若要選擇日期： 1. 請選擇天選項。 2. 從清單上 選定日期旁 選擇該月的某日。

5. 選擇您要在選定的日期啟動掃描的時間。

選項	說明
開始時間	在特定時間啟動掃描。
閒置時間達到	未使用電腦達一段指定時間後啟動掃描。

除每次掃描封存檔案並自動清理有害檔案外，排程掃描在掃描電腦時使用手動掃描設定。


掃描電郵

電郵掃描可保護您免遭傳送給您的電郵中有害檔案的威脅。

必須開啟病毒和間諜軟件掃描，以掃描電郵中的病毒。

若要開啟電郵掃描：

1. 在主頁面上按一下**設定**。

 註：您需要管理權限才能變更設定。

2. 選擇**電腦安全** > **病毒和間諜軟件掃描**。

3. 選擇**移除有害電郵附件**。


4. 按一下**確定**。

何時掃描電郵與附件

病毒和間諜軟件掃描可移除所收到電郵中的有害內容。

病毒和間諜軟件掃描移除透過電郵程式 (如 Microsoft Outlook 和 Outlook Express、Microsoft Mail 或 Mozilla Thunderbird) 收到的有害電郵。每次電郵程式使用 POP3 通訊協定從郵件伺服器接收未加密的電郵和附件時，均會對其進行掃描。

病毒與間諜軟件掃描無法掃描 Webmail (包括網路瀏覽器中執行的應用程式，例如 Hotmail、Yahoo! mail 或 Gmail) 中的電郵。若您不移除有害附件或正在使用 Webmail，仍可免遭病毒威脅。打開電郵附件時，即時掃描會在有害附件可能造成損害前將其移除。

 註：即時掃描僅保護您的電腦，而不保護您朋友的電腦。除非您打開附件，否則即時掃描不會掃描附加的檔案。這意味著，若您使用 Webmail，且在打開其附件前轉寄郵件，則可能將受感染的電郵轉寄給朋友。


檢視掃描結果

病毒和間諜軟件歷程記錄顯示產品發現的所有有害檔案。

有時，產品無法執行您已選擇的發現有害內容時執行的動作。例如，若您選擇清除檔案，但有一個檔案無法清除，則產品會將其移至隔離區。您可在病毒和間諜軟件歷程記錄中檢視此資訊。

若要檢視歷程記錄：

1. 在主頁面上按一下**設定**。

 註：您需要管理權限才能變更設定。

2. 選擇**電腦安全** > **病毒和間諜軟件掃描**。


3. 按一下**檢視移除歷程記錄**。

病毒和間諜軟件歷程記錄顯示以下資訊：

有害檔案發現的日期和時間，
惡意軟件的名稱及其在電腦上的位置，以及
已執行的動作。

如何從掃描排除檔案

有時，您可能想要將某些檔案或應用程式從掃描中排除。除非您將其從排除項目清單中移除，否則不會掃描排除的項目。


-  註：即時掃描與手動掃描的排除清單是各自獨立的。例如，若您將一個檔案從即時掃描中排除，除非也將其從手動掃描中排除，否則手動掃描過程中仍會對其進行掃描。

排除檔案類型

依類型排除檔案時，不會掃描具有特定副檔名的檔案中是否含有有害內容。

若要新增或移除要排除的檔案類型：

1. 在主頁面上按一下 [設定](#)。

-  註：您需要管理權限才能變更設定。

2. 選擇是否要將該檔案類型從即時或手動掃描中排除：

選擇 [電腦安全](#) > [病毒和間諜軟件掃描](#)，以從即時掃描排除檔案類型。

選擇 [其他設定](#) > [手動掃描](#)，以從手動掃描排除檔案類型。

3. 按一下 [從掃描排除檔案](#)。

4. 若要排除檔案類型：

a) 選擇 [檔案類型](#) 索引標籤。

b) 選擇 [排除具有以下副檔名的檔案](#)。

c) 在 [新增](#) 按鈕旁的欄位中，鍵入可識別要排除的檔案類型的副檔名。

若要指定無副檔名的檔案，請輸入 '.'。您可以使用萬用字元 '?' 來表示任一單一字元，或使用 '*' 表示多個任意字元。

例如，若要排除可執行檔，請在欄位中輸入 exe。

d) 按一下 [新增](#)。

5. 對要從病毒掃描中排出的其他副檔名重複上一個步驟。

6. 按一下 [確定](#) 以關閉 [從掃描中排除](#) 對話方塊。

7. 按一下 [確定](#) 以套用新設定。


所選的檔案類型會從將來的掃描中排除。

依位置排除檔案

依位置排除檔案時，不會掃描指定磁碟機或資料夾的檔案中是否含有有害內容。

若要新增或移除想要排除的檔案位置：

1. 在主頁面上按一下 [設定](#)。

-  註：您需要管理權限才能變更設定。

2. 選擇是否要將該位置從即時或手動掃描中排除：


選擇 [電腦](#) > [病毒和間諜軟件掃描](#)，以將該位置從即時掃描中排除。

選擇 [電腦](#) > [手動掃描](#)，以將該位置從手動掃描中排除。

3. 按一下**從掃描排除檔案**。

4. 若要排除檔案、磁碟機或資料夾：

- a) 選擇**物件索引標籤**。
- b) 選擇**排除物件(檔案、資料夾...)**。
- c) 按一下**新增**。
- d) 選擇要從病毒掃描中排除的檔案、磁碟或資料夾。

 註：一些磁碟可能為可卸除式磁碟，例如，CD、DVD 或網絡磁碟。不可排除網絡磁碟和空的卸除式磁碟。

e) 按一下**確定**。

5. 重複上一步驟以排除其他不要掃描病毒的檔案、磁碟或資料夾。

6. 按一下**確定**旁的**從掃描中排除**對話方塊。


7. 按一下**確定**以套用新設定。

所選的檔案、磁碟機或資料夾會從將來的掃描中排除。

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。


若即時掃描或手動掃描偵測到行為類似間諜軟件或危險軟件的應用程式，但您知道它是安全的，則可將其從掃描中排除，以便產品不會再因此警示您。

 註：若該應用程式行為類似病毒或其他惡意軟件，則無法排除。

您無法直接排除應用程式。只要您在掃描過程中排除新應用程式，則其會出現在排除清單中。

若要檢視已排除在掃描之外的應用程式：

1. 在主頁面上按一下**設定**。

 註：您需要管理權限才能變更設定。

2. 選擇是否要檢視已從即時或手動掃描中排除的應用程式：

選擇**電腦** > **病毒和間諜軟件掃描**，以檢視已從即時掃描中排除的應用程式。

選擇**電腦** > **手動掃描**，以檢視已從手動掃描中排除的應用程式。

3. 按一下**從掃描排除檔案**。

4. 選擇**應用程式索引標籤**。

 註：只能排除間諜軟件與危險軟件應用程式，而不能排除病毒。

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**。

6. 按一下**確定** 關閉 **從掃描中排除**對話方塊。

7. 按一下**確定**結束。

如何使用隔離區

「隔離區」是用來存放可能具有惡意檔案的安全區域。

被隔離的檔案不會傳播，也不會對電腦造成任何損壞。

您可隔離惡意軟件、間諜軟件和危險軟件，使其不會損害電腦。必要時，也可稍後還原隔離區中的某些應用程式或檔案。

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。

通常，可刪除所隔離的惡意軟件。

在大多數情形下，可刪除隔離的間諜軟件。不過，隔離的間諜軟件可能是合法軟體程式的一部分，移除後目前的部分程式可能無法正常執行。若要將此程式保留在電腦上，可還原隔離的間諜軟件。


已隔離的危險軟件可能為合法軟體程式。若此程式由您自行安裝及設定，則可在隔離區將其還原。若您對危險軟件的安裝不知情，則其很可能有惡意目的，應將其刪除。

檢視隔離的項目

您可檢視隔離區內項目的更多資訊。

若要檢視隔離區內各項目的詳細資訊：

1. 在主頁面上按一下[設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇[電腦安全](#) > [病毒和間諜軟件掃描](#)。


3. 按一下[檢視隔離區](#)。

[隔離區](#)頁面將顯示隔離區中儲存的項目總數。

4. 若要檢視隔離區內各項目的詳細資訊，請按一下[詳細資料](#)。

您可依惡意軟件名稱或檔案路徑將內容排序。

將顯示前 100 個項目的清單，其中包含已隔離項目的類型、其名稱以及檔案安裝路徑。

5. 若要檢視已隔離項目的更多相關資訊，請按一下「[狀態](#)」欄旁的  圖示。


還原隔離的項目

您可還原所需的已隔離項目。

若需要，可從隔離區還原某些應用程式或檔案。請勿從隔離區還原任何項目，除非您確定其不會造成任何威脅。已還原的項目返回至其在電腦上的原始位置。

還原隔離的項目

1. 在主頁面上按一下[設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇[電腦安全](#) > [病毒和間諜軟件掃描](#)。

3. 按一下[檢視隔離區](#)。

4. 選擇要還原的已隔離項目。

5. 按一下[還原](#)。

什麼是 DeepGuard

DeepGuard 分析檔案內容和應用程式行為，並監視不受信任的應用程式。

DeepGuard 封鎖新的和未發現的病毒、蠕蟲以及其他嘗試變更電腦的有害應用程式，並防止可疑應用程式存取互聯網。

DeepGuard 偵測到試圖對系統作出可能有害變更的新應用程式時，會允許該應用程式在安全區域內執行。在安全區域內，該應用程式無法損害您的電腦。DeepGuard 會分析該應用程式嘗試作出的變更，並據以判斷其有多大的可能性是惡意軟件。若該應用程式可能是惡意軟件，DeepGuard 會將其封鎖。

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。

開啟或關閉 DeepGuard

保持 DeepGuard 開啟，以防止可疑應用程式對電腦作出可能有害的系統變更。

若使用 Windows XP，請確保開啟 DeepGuard 前先安裝 Service Pack 2。

若要開啟或關閉 DeepGuard：


1. 在主頁面上按一下 **狀態**。
2. 按一下 **變更此頁面上的設定**。
 註：您需要管理權限才能關閉安全功能。
3. 開啟或關閉 **DeepGuard**。
4. 按一下 **關閉**。

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。

若要允許 DeepGuard 已封鎖的應用程式：

1. 在主頁面上按一下 **工具**。
2. 按一下 **應用程式**。
將顯示 **受監視的應用程式** 清單。
3. 尋找您想要允許的應用程式。
 註：您可以按一下欄位標題，以對清單進行排序。例如，按一下 **權限** 欄位，以將清單分成允許的程式和拒絕的程式兩個群組。
4. 在 **權限** 欄中選擇 **允許**。
5. 按一下 **關閉**。


DeepGuard 將重新允許應用程式作出系統變更。

在相容模式下使用 DeepGuard

為達到最好的保護效能，DeepGuard 會暫時修改執行中的程式。部分程式會檢查其是否受到損壞或修改，因此可能與這一功能不相容。例如，含防作弊工具的線上遊戲執行時，會檢查是否以任何方式遭到修改。在這些情況下，您可開啟相容模式。

若要開啟相容模式：

1. 在主頁面上按一下 [設定](#)。

 註：您需要管理權限才能變更設定。

2. 選擇 [電腦安全](#) > [DeepGuard](#)。
3. 選擇 [使用相容模式](#)。
4. 按一下 [確定](#)。

如何處理可疑行為警示

DeepGuard 監視不受信任的應用程式。若被監視的應用程式嘗試存取互聯網或變更系統，或行為可疑，DeepGuard 會將其封鎖。

在 DeepGuard 設定中選擇 [警示我可疑行為](#)，則在偵測到可能有害的應用程式時，或在啟動信譽未知的應用程式時，DeepGuard 會通知您。

若要決定如何處理 DeepGuard 已封鎖的應用程式：

1. 按一下 [詳細資料](#)，以檢視程式的詳細資訊。

詳細資料部分顯示：

應用程式的位置，
該應用程式在「即時保護網路」中的信譽，以及
該應用程式的普遍程度。

2. 決定是否信任 DeepGuard 已封鎖的應用程式：

若您不想封鎖該應用程式，請選擇 [我信任該應用程式](#)。讓其繼續。

若符合以下情況，則應用程式很可能是安全的：

DeepGuard 由於您的行為而封鎖該應用程式，
您認得此應用程式，或
您從信任的來源取得該應用程式。

若您想保持封鎖該應用程式，請選擇 [我不信任該應用程式](#)。保持封鎖。

若符合以下情況，則應用程式很可能是不安全的：

該應用程式不常見，
該應用程式信譽未知，或
您不知道該應用程式。

3. 若要提交可疑的應用程式進行分析：

a) 按一下 [向 F-Secure 報告該應用程式](#)。

產品將顯示提交條件。

b) 若您同意這些條件並想提交範例，請按一下[接受](#)。

建議您在以下情況下傳送範例：

DeepGuard 封鎖您知道其為安全的應用程式，或
您懷疑該應用程式可能是惡意軟件。

