bitdefender

GAMESAFE

使用者手冊

BitDefender GameSafe
使用者手冊

出版 2008.10.02

法律聲明


bitdefender

內容目錄

授權與保證

如果您不同意這些條款和條件，請勿安裝此軟體。若在安裝前選擇了「我同意」、「確定」、「繼續」、「是」等選項，代表您完全了解及接受這份合約上的條款。

對您來說，這個條款涵概了 BitDefender 家用使用者的解決方案及服務，包含了相關的檔案及任何應用程式的更新及升級，在您所購買的授權或任何相關的服務協定都定義在這份檔案及任何這些條款的複本。

對於您與 BITDEFENDER 公司來說，這份授權合約是份法律協議，在您使用 BitDefender 的軟體產品，它將涵概了電腦軟體、服務，可能也包含了相關的媒體、列印的手冊及線上或電子式的檔案，而這些都將被國際著作權法及國際商標法所保護。在安裝、複製及使用 BitDefender 時，您將同意這個協定上的條款。

如果您不同意這個合約的條款，請不要安裝或使用 BitDefender。

BitDefender 授權。. 像智慧財產權法律及條款一樣，BitDefender 被著作權法律及國際著作權條款所保護。BitDefender 是使用授權而非賣斷。

授權取得。BITDEFENDER 提供您非獨一的、有限的、不可轉移的使用 BitDefender 授權。

軟體的使用。您可以按合約所訂的授權數量上安裝 BitDefender 軟體於許多電腦上。您也可以製作一份額外的複製光碟以備份為用途。

桌上型電腦使用者授權。這個 BitDefender 軟體授權可以安裝在個人電腦上，它並沒有提供網路服務。每個使用者可以安裝這個軟體在一台個人電腦，而且可以製作一份額外的複製當備份用途。主要使用者的數量依授權書上的使用者授權數量。

授權期限。BitDefender 軟體的使用授權於購買日起至軟體到期日止。

使用期滿。當使用期滿時，產品會立即停止執行它的功能。

升級。如果BitDefender標示為升級版，您必須按照合約上規定正確地使用。如果是標示為升級替換或產品補助亦是您升級版的合格依據。您可以按使用合約上規定使用此升級版。 如果BitDefender升級只是整個產品的部分，您仍舊被授權使用單一產品，BitDefender或許可以被部分使用或傳遞但仍不可超過合約規定的使用數量。升級版的條款可能會取代或修改原先您與BitDenfender的原始條款。

版權。BitDefender之所有權利、標題、以及著作權 (包含任何影像、相片、企業標識、動畫、影片、聲音、音樂、文字及BitDefender內之applets)，與列印的材料、及 BitDefender 的任何複製版都屬 BITDEFENDER 公司所擁有。BitDefender 受到著作權法律及國際條款所保護。您必須對待 BitDefender 像其他有版權的媒體一樣。您不可以複製任何 BitDefender 附屬的檔案。您必須在所有包含 BitDefender 的複製

媒體，附上所有的版權聲明。您不可再授權、租、售或分享 BitDefender 的授權。您不可利用反向工程、反編譯、拆解及建立衍生品、修改或解譯 BitDefender 原始程式碼。

有限保證。BITDEFENDER 保證從您收到 BitDefender 產品的 30 日內，可享有免費軟體媒體瑕疵更換的權利。BITDEFENDER 提供保證在收到瑕疵品後，可以選擇更換媒體或退還您購買 BitDefender 的金額。BITDEFENDER 不保證 BitDefender都沒有錯誤或錯誤都會被修正。BITDEFENDER 亦不保證 BitDefender 將符合您所有的需求。

除了合約書上明確的規定外，BitDefender不負責產品其他的明確或暗示性的保證包含改進、維護、支援或有形與無形的材料與服務。 BitDefender 明確地不對任何無限責任，適用於任何特定用途的保證、標題、資料與訊息內容準確性，以及過濾、中斷、清除其他公司軟體間諜程式、廣告、郵件、 cookies 與檔案擔負責任。無論是法令規章、交易條款、慣例與商業用途所導致的。

損害聲明。 任何人使用、測試、評估BitDefenderd可能存在影響BitDefender品質、性能上之風險，BitDefender 將不負任何責任。 BitDefender不對任何損害負責，包含無限的直接或間接使用上的損害，性能或傳送Bitdefender甚至是BitDefender已告知可能存在的損害。BitDefender所負責任將不超過您購買BitDefender的代價。以上聲明與有限責任，您自行決定是否接受使用，評估或測試BitDefender。

用戶重要通知. 本軟體不是容錯的也不是設計用在損壞時會自動啟動的作業環境。本軟體不適用於飛航作業，核能管控或通信系統、武器系統，直接或間接的生命支援監控系統或任何會導致死亡或身體，財產嚴重傷害之系統 。

一般條款。本合約受羅馬尼亞及國際版權之管轄。如有任何違反條款其裁決管轄為羅馬尼亞法院。

BitDefender的價格、費用與酬金如有變動是不會預先通知您的。

本合約的任一條款如有失效，此 一失效的條款將不影響本合約的其他條款的有效性。

BitDefender與其logos是屬BitDefender之商標，在本產品用到所有其他商標與相關的材料屬其他個別公司所有。

如您違反任何條款，本合約將立即終止且不予事先通知。而您也得不到BitDefender或其經銷商任何賠償，且合約條款有關使用上之保密與限制依然有效。

BitDefender可在任何時間修政條款，而修正後的條款將自動地在推出的相關版本的軟體使用且不影響其他條款的有效性。

在各種翻譯語文如有爭議或不一致性時，以BitDefender的英文版條款為基準。

聯絡 SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: office@bitdefender.com.

序言

這份手冊提供選擇給BitDefender GameSafe做為他們個人電腦上的安全解決方案。在這本書上的資訊不只是適合提供給電腦操作者使用，也適合任何一個使用者在Windows下使用。

這本書將為您描述BitDefender GameSafe 是由公司及團隊所建立，並且引導您整個安裝的程序，教導您如何設定它。您將會知道如何使用BitDefender GameSafe，如何去更新、測試及自訂它。您將會學習到如何從 BitDefender 得到最好的服務。

我們希望您有一個愉快且有用的演講。

1. 本書的用法說明

1.1. 印刷上的常規

為了易於閱讀，此書使用了幾種文字的樣式。它們的外觀及意思描述在以下的表格裡面。

外觀	描述
sample syntax	語法樣本一起列印monospaced特性.
http://www.bitdefender.com	這個 URL 連結正指到其他外部的位置，http 或 ftp 伺服器。
support@bitdefender.com	在文字中插入聯絡的電子郵件位址資訊。
"序言" (p. xi)	這是一個內部的連結，連結到這份手冊的其他位置。
filename	檔案及目錄使用monospaced 字型列印。
option	所有產品選項使用strong字元來列印。
`sample code listing`	程式的列表使用monospaced字元列印。

1.2. 警告

警告是以文字、圖表來標示，針對目前的段落，提醒您額外的資訊。

注
註解只是很短的意見。儘管您可以略過它，註解可以提供有價值的資訊，像是特定的功能或連結到一些相關的主題。

重要
這個要求您的注意並且建議不要跳過它。通常它提供非絕對重要但卻是有意義的資訊。

警告
這是極重要的資訊，您必須重視它。如果您依指示去做，將不會有壞的事發生。您應該仔細閱讀並了解它，因為它描述了極危險的事。

2. 本書的架構

本書包含幾個部份包含了幾個主題。 此外，有一個詞彙表讓您清楚一些技術的詞彙。

安裝. 逐步介紹安裝 BitDefender 的工作站。這是一個安裝多元化的個別指引 BitDefender GameSafe詳細的安裝指導。透過這份指導，您可以成功地完成安裝程序。最後，當您需要解除安裝 BitDefender 時，移除步驟也說明在其中。

基本管理. 基本管理及維護BitDefender。

進階安全防護管理. 一個關於BitDefender提供的防護能力的詳細介紹。 這章節詳細介紹所有進階管理主控台。 您會被指導如何設定及使用所有BitDefender模組，使您能更有效地保護您的電腦對抗所有惡意程式的威脅 (病毒、間諜程式、後門程式及其他威脅)。

BitDefender 救援光碟. BitDefender 救援光碟描述。它協助了解及使用這個可開機光碟所提供的功能。

取得協助. 如果有一些未預期的情況發生，從何找尋及詢問，以取得協助。

詞彙表. 詞彙表能夠解釋您在本書上發現的一些技術專有名詞及罕見的項目說明。

3. 意見回饋

我們邀請您協助我們改進這份手冊。我們將盡全力測試及確認所有的資訊。當您發現在這份手冊中任何瑕疵，或者您認為該如何改進以提供給您最好的檔案，請寫下來告訴我們。

透過電子郵件寄到documentation@bitdefender.com讓我們知道。

重要
請用英文寫下您的所有檔案相關的電子郵件，我們可以更有效率地處理它們。

安装

1. BitDefender GameSafe 安裝

BitDefender GameSafe 安裝手冊包含了以下的主題：

- 系統要求
- 安裝步驟
- 初始設定精靈
- 升級
- 修復或移除 BitDefender

1.1. 系統要求

為有效地使用本產品，在安裝之前，請先確定您的電腦正在使用以下其中一個操作系統以及符合系統要求:

- 操作平台: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (或更高要求)

Windows 2000

- 800 MHz處理器或以上
- 最少 256MB記憶體或以上 (建議使用512MB)
- 最小 60MB 可用的硬碟空間

Windows XP

- 800 MHz處理器或以上
- 最少 256MB記憶體或以上 (建議使用1GB)
- 最小 60MB 可用的硬碟空間

Windows Vista

- 800 MHz處理器或以上
- 最少 512MB 記憶體或以上 (建議使用1GB)
- 最小 60MB 可用的硬碟空間

BitDefender GameSafe 評估版可以從以下網址下載 http://www.bitdefender.com

1.2. 安裝步驟

找到安裝檔案並且連按滑鼠兩下。它將開啟精靈，並引導您完成設定程序。

安裝精靈出現之前，BitDefender會檢查更新的安裝檔案。當有新的版本時，您將會給予提示下載。您可以選擇按下Yes(是)以下載新的版本，或者按No(否)繼續進行安裝步驟

安裝步驟

請依照以下步驟來安裝BitDefender GameSafe

1. 按下 Next(下一步) 繼續或按 Cancel(取消) 如果您想要離開安裝程序。
2. 按下 Next(下一步)。

   BitDefender GameSafe 提醒您，假如您的電腦已安裝其他的防毒產品 按下Remove(移除) — 移除所有已安裝的元件。 或者選擇按下 Next(下一步)繼續進行安裝。

警告
在安裝BitDefender病毒防護軟體之前，強烈建議先移除其他的病毒防護軟體，因為於同一部電腦上同時使用兩個或以上的病毒防護軟體，會影響電腦系統的運作。

3. 請閱讀這份授權合約書，選擇 我接受在這份合約書裡的條款 並且按下 下一步。如果您不同意這些條款，則按下 取消。這個安裝程序將被中止，您將離開這個設定。
4. 您可以選擇要安裝 BitDefender 的安裝路徑。 預設的目錄是 C:\\Program Files\\BitDefender\\BitDefender 2008。 如果您要變更安裝路徑，點擊瀏覽並選取您要安裝 BitDefender GameSafe 的目錄。。

   按下 Next(下一步)。
5. 根據安裝程序以選擇適合的項目。 其中有些項目將會被選擇為預設:
   ■開啟讀我檔案 — 在軟體安裝結束後，開啟讀我檔案。
   ■在桌面創造一個捷徑 — 在軟體安裝結束後，在您的桌面上創造一個 BitDefender GameSafe 的捷徑。
   ■安裝完成後退出CD - 在安裝完成後把CD退出；當您選擇用CD安裝時會出現此選項。
   ■關閉Windows防火牆 - 關閉Windows防火牆。

   重要
   由於BitDefender GameSafe 已經包含一個先進的防火牆模組，我們建議您停用Windows防火牆。 在一台電腦上同時運行的兩個防火牆可能會發生問題。

   ■關閉Windows系統維護 - 把Windows系統維護關閉；此選項只適用於Windows Vista。

   按下 Install(安裝) 開始進行軟體的安裝。

   重要
   在安裝的程序中， 初始化精靈 將會出現。安裝精靈協助您註冊您的 BitDefender GameSafe，建立一個 BitDefender 帳號，並且設定重要安全防護任務。
   完成安裝精靈引導的程序以進行下一個步驟。
6. 按下 完成。 您的系統可能被要求重新啟動，令安裝精靈完成您的安裝程序。 我們建議您保留此選項的選擇。

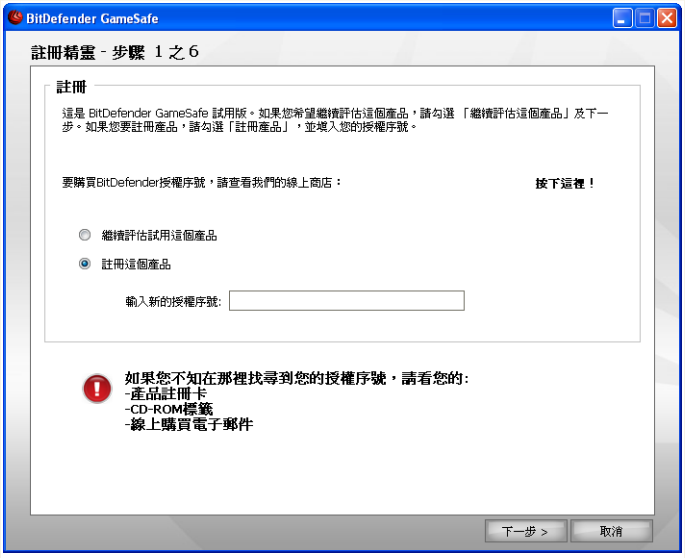
   按下 完成 去完成軟體的安裝。如果您接受預設的安裝路徑，一個新的目錄命名為 BitDefender 被建立在 Program Files 並且包含子目錄 BitDefender 2008。

1.3. 初始化設定精靈

在安裝的程序中，一個初始化精靈會出現。這個初始化精靈協助您註冊您的 BitDefender GameSafe，建立一個 BitDefender 帳號，並且設定重要的防護任務。

完成初始化精靈並非強制的；然而，我們建議您如此做是為了節省時間，並且確保您的系統在 BitDefender GameSafe安裝前是安全的。

1.3.1. 步驟 1/6 — 註冊 BitDefender GameSafe



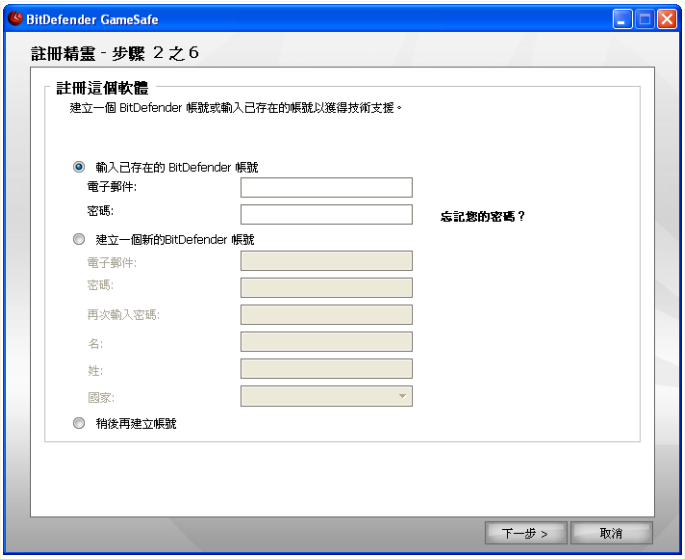
註冊

選擇 註冊軟體 以註冊 BitDefender GameSafe。輸入授權序號在 輸入新的序號 欄位。

希望繼續評估這個軟體，請選擇繼續評估這個軟體。

按下 Next(下一步)。

1.3.2. 步驟 2/6 — 建立一個 BitDefender 帳號



帳號建立

我尚未擁有一個 BitDefender 帳號

為了取得免費的 BitDefender 技術支援及其他免費的服務，您需要建立一個帳號。

注
如果您想稍後才建立新的帳戶，請選擇合適的項目。

選擇 建立新的 BitDefender 帳號 及提供所需的資料。 您在這裡所提供的資料將會被保密。

■E-mail — 輸入您的電子郵件信箱。

■密碼 — 為您的BitDefender帳號輸入一組密碼。

注
密碼長度至少要四個字元。

■重複鍵入密碼 — 重新輸入先前的密碼。

■名 — 輸入您的名字。

■性 — 輸入您的姓氏。

■"國家 —選擇您所在的國家。

注
在http://myaccount.bitdefender.com使用您提供的電子郵件地址和密碼來登錄您的帳戶。

要成功建立一個帳號，您必須啟動您的電子郵件。確認您的電子郵件位址並依循 BitDefender 註冊服務所寄給您的電子郵件中的指示完成。

按下 下一步 繼續。

我已經有一個 BitDefender 帳號。

如果您先前已經在您的電腦上登記一個 BitDefender 帳戶， BitDefender 將會自動地發現。 在這個情況，您需要按下下一步繼續進行安裝。

如果您已經有一個帳戶,但是 BitDefender 不能找到它，請選擇登入到已有的 BitDefender 帳戶 及提供您帳戶的電郵地址及密碼。

注
或者選擇按下 Next(下一步)繼續進行安裝。 按下 下一步 繼續，或按 取消 離開安裝精靈。

如果您忘記您的密碼，按下 忘記您的密碼？ 並依循指示操作。

按下 下一步 繼續。

1.3.3. 步驟 3/6 — 學習 RTVR（即時病毒報告）

RTVR（即時病毒報告）資訊

按下 下一步 繼續，或按 取消 離開安裝精靈。

1.3.4. 步驟 4/6 — 選擇要被執行的任務

任務選擇

為您的系統安全，設定 BitDefender GameSafe 以執行重要的防護任務。

以下的選項是可用的：

■更新 BitDefender 引擎 (可能要求重新啟動) — 在下一個步驟，將更新 BitDefender 引擎，為了保護您的電腦對抗最新的威脅。

■執行一個快速的系統掃描 (可能要求重新啟動) — 在下一個步驟，一個快速的系統掃描將被執行，允許 BitDefender 確認您的檔案在 Windows 及 Program Files 目錄的資料夾不受到感染。

■在每天上午2:00 時執行一個全系統掃瞄 — 在每天上午2:00 時，執行一個全系統掃瞄。

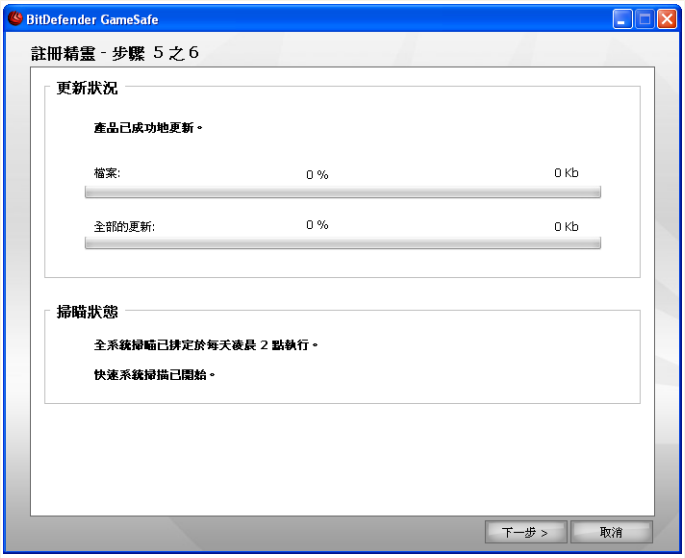
重要

為了確保您系統的安全，我們建議在您進入到下一個步驟前，啟動這些選項。

如果您只選擇最後一個選項，或者沒有選任何選項，您將跳過下一個步驟。

按下 下一步 繼續，或按 取消 離開安裝精靈。

1.3.5. 步驟 5/6 — 等待任務完成



任務狀態

等待任務完成。您可以看到在之前的步驟所選的任務狀態。

按下 下一步 繼續，或按 取消 離開安裝精靈。

1.3.6. 步驟 6/6 — 檢視總結

完成

這是設定精靈的最後一個步驟。

按下 完成 以完成安裝精靈，並繼續進行安裝程序。

1.4. 升級

升級的程序可以在以下其中一種方式完成:

移除您先前的版本，並安裝新的版本 - 適用於所有版本的BitDefender。

首先，您必須先移除您先前的版本，然後重新啟動電腦並安裝新的軟體依照在 "安裝步驟" (p. 3) 的描述。

1.5. 修復或移除BitDefender

如果您想要修復或移除BitDefender GameSafe，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2008 → 修復或移除。

您將被要求按下 下一步去確認您的選擇。一個可讓您選擇的新視窗將會出現：

■修復 — 重新安裝先前設定時的所有程式元件；

如果您選擇修復BitDefender，一個新的視窗將會出現。 按下修復以開始進行修復程序。

重新啟動電腦，然後按下安裝以重新安裝 BitDefender GameSafe。

當安裝程序完成，一個新的視窗會出現。 按下 完成。

■移除 — 移除所有已安裝的元件。

注

我們建議選擇移除當需要完全重新安裝元件。

如果您選擇了移除BitDefender，一個新視窗將會出現：

重要

當移除BitDefender時，您的系統不會被保護受到惡意程式的威脅，例如: 病毒、間諜程式。 假如您希望Windows的系統防護在移除BitDefender後開啟，請選擇適合的核取方塊。

按下移除以開始從您的系統中移除BitDefender GameSafe。

在移除過程中您會被邀請給予我們一些意見 按下 確定以進行我們一份不多於5條問題的問卷。 假如您並不希望填寫我們的問卷，按下 取消。

當移除過程完成後，一個新視窗會出現。 按下 完成。

注

移除程序完成後，我們建議您刪除位於 Program Files裡的BitDefender資料夾。

當移除BitDefender時發生錯誤

當移除BitDefender時發生錯誤時，移除程序會被終止，一個新視窗將會出現。 按下 執行移除工具 以確保BitDefender從您的系統中完全移除。 移除工具會把所有在自動移除程序中不能移除的檔案及登錄機碼移除。

基本管理

2. 開始使用

安裝BitDefender完成後，您的電腦已受到保護。您可以隨時在BitDefender安全防護中心查看您的系統狀態、採取預防的方案或完全設定您的產品。

要進入安全防護中心，依循下面路徑使用 Windows 開始功能表 開始 → 程式集 → BitDefender 2008 → BitDefender GameSafe 或更快的方法，在系統工具列上按兩下 BitDefender 圖示。

BitDefender 安全防護中心

BitDefender 安全防護中心包含兩個部份 ：

■狀態區域：本區域包含安全資訊以及協助您修復您的電腦的安全弱點。您可以容易地看見有多少可能危害您的電腦的事件。點擊紅色的修復所有事件按鈕，您電腦的安全弱點馬上就會被解決或是指引您修復它們。有四個狀態鈕可以對應到四種的安全防護目錄。綠色狀態紐表示目前狀況正常，沒有危險。黃色/紅色狀態鈕則表示有中度/高度的安全風險。點擊黃色/紅色狀態鈕進入選項畫面，您可以直接選擇立刻修復全部，或是選擇修復逐項的進行修復>。灰色則表示不需調整的元件。

■快速任務區域：本區域可以協助防護您的電腦系統安全並且保全您的資料。

此外，BitDefender安全防護中心還包含了數個有用的捷徑。

連結	描述
購買。	開啟一個您可以購買本產品的網頁。
我的帳號	開啟您的 BitDefender 帳號網頁。
註冊。	開啟註冊精靈
說明	開啟說明檔案
支援	開啟 BitDefender 支援網頁。
設定	開啟進階管理主控台。
歷史	開啟BitDefender歷史事件視窗。

2.1. 系統工具列的BitDefender圖示

為了更快速的管理整個程式，您也可以使用系統工具列的BitDefender圖示。

如果您按二下這個圖示，BitDefender安全防護中心將被開啟。您也可以按下滑鼠右鍵，將出現一個右鍵選單。它可以提供BitDefender 的快速管理：

顯示 — 開啟BitDefender 安全防護中心。

BitDefender 圖示。

■

■說明 — 開啟說明檔案。
■關於 — 開啟 BitDefender 網頁。
■修復所有問題 — 幫助您移除所有系統弱點。
■開 / 關遊戲模式 -遊戲模式 開 / 關。
■開啟進階設定 — 允許您去管理主控台。
■立刻更新 — 立刻執行更新。 您可以在新開啟的視窗檢視更新狀況
■離開 — 關閉程式。

當遊戲模式啟動時，您可以看見英文字母 G 顯示在 BitDefender 圖示上。

若發生危害您的系統的事件時，一個驚嘆號將會出現在BitDefender 圖示。 您可以將滑鼠游標移至圖示以檢視危安事件的數量。

2.2. 掃描活動列

這個 掃描活動列 是您的系統上掃描活動的圖形。

在（the 檔案區）的線色線條顯示每秒掃描的檔案，從 0 到 50 的大小。

在（the 網路區）的紅色線條顯示已從網路每秒掃描的檔案，從 0 到 100 的大小。

活動列

注
這個 掃描活動列 將利用紅色交叉線在相對應的（檔案區 或 網路區）空間裡通知您，當防毒機制已關閉時。這種方式使您不用開啟管理主控台即可得知是否被保護。

您可以使用 掃描活動列 來掃瞄目標。選擇 您希望掃描的目標拖至掃描活動列即可。請參閱"拖放掃描" (p. 61)，以獲得更多資訊。

當您不想再看到這個即時的圖形顯示，請按下滑鼠右鍵，並選擇隱藏。 您可以透過點擊進階設定選擇取消允許掃描活動列顯示，已完全關閉掃描活動列。

2.3. BitDefender 手動選擇掃瞄

如果您想快速掃瞄某個資料夾，可以使用 BitDefender 手動選擇掃瞄。

如果您執行手動選擇掃瞄，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2008 → 手動選擇掃瞄。 以下視窗將會顯示:

BitDefender 手動選擇掃瞄

請選擇要掃瞄的資料夾並按下 確定。 BitDefender 掃瞄器會引導您完成整個掃瞄過程。

2.4. 遊戲模式

創新的遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。 當您啟動遊戲模式，下列設定將會被套用：

- 停用全部的BitDefender警告以及彈出提示。
- 即時防護層級將會被設在允許。
- BitDefender 防火牆是設定為 玩家模式.

當遊戲模式啟動時，您可以看見英文字母 G 顯示在 BitDefender 圖示上。

2.4.1. 執行遊戲模式

可以選擇下列其中一種方式啟動遊戲模式：

- 從系統工具列按下滑鼠右鍵點擊 BitDefender 圖示，並選擇 啟動遊戲模式。
- 同時按下 Alt+G鍵；(預設的熱鍵)。

重要
千萬記得要將遊戲模式關閉，當您結束使用遊戲程式時。只要重複執行開啟的方式，即可關閉。

2.4.2. 變更遊戲模式熱鍵

如您想更改快速鍵，請跟隨以下步驟:

1. 按下BitDefender 安全防護中心點擊設定，開啟管理主控台

注
從 系統工具列 按下滑鼠右鍵的 BitDefender 圖示，並選擇 開啟進階選項。

2. 按下 進階。
3. 在遊戲模式熱鍵選項，設定您要的熱鍵。

■您可以選用下列的功能鍵：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)

■在編輯欄鍵入您常用的字母以對應熱鍵。

舉例而言，如果您想要用Ctrl+Alt+D當作熱鍵，您必須鍵入Ctrl and Alt and type D。

注
取消遊戲模式熱鍵 就可以停用該熱鍵。

3. 安全防護狀態

安全狀態顯示有系統組織您電腦上的弱點清單。 每當有問題可能影響您的電腦安全，BitDefender GameSafe 將會通知您。

安全防護狀態鈕有3種：

■電腦安全
■網路安全。
■身分管控

同時，您可以在右邊看見危安事件的數量以及一個紅色的修復全部事件鈕。

依據目前的防護層級，3個狀態鈕會以綠色、黃色、紅色、灰色呈現。

■按綠色表示低安全風險。
■按黃色表示中安全風險。
■按紅色表示高安全風險。
■灰色 表示尚未被設置的元件

只要滑鼠左鍵在修復全部事件 鈕上一點，即可以輕鬆地解決安全防護問題。 一個新的視窗將會開啟。

安全事件

您可以看見一個安全事件的清單以及關於事件的簡述。

若只想修復單一事件，在您想要修復的事件點擊修復鈕。即可立刻修復或是透過精靈的指示完成。如果您決定要一次完成修復，點擊 立刻修復全部 鈕並且依照精靈的指引的步驟完成。

如果您需要更多幫助，點擊畫面下方的更多幫助鈕。 一個說明頁面將會開啟，此頁面將會提供您關於事件的詳細資訊以及該如何修復事件。

重要

每一個事件旁邊都有一個核取方塊，如果您有特定的事件不希望被列入安全風險考量，取消事件旁的核取方塊即可。請您謹慎使用這項功能，如此可能導致您的電腦安全風險增加。

您也可點擊 關閉，稍後再做處理。

3.1. 電腦安全防護狀態鈕

如果安全狀態按鈕顯示綠色，表示現時沒任何風險。不然，如果按鈕顯示黃色、紅色或灰色，表示您的電腦現時處於中或高保安風險，易受入侵。

當您做了可能影響安全防護的設定變更，或是您很久沒有執行重要的防護任務，如：系統掃描，狀態鈕的顏色都會改變。

下方的表格將會告訴您有哪些因素會被列入安全風險的評估。

事件	顏色
您已經很久沒有執行系統掃描了	黃色
您已經非常久沒有執行系統掃描了	紅色
即時防護已被停用	紅色
病毒防護層級已被設為寬鬆	黃色
自動更新已被停用	紅色
您已經一天沒有進行更新了	紅色

依照這些步驟以修復事件：

1. 點擊網路安全防護狀態鈕
2. 您可以點擊立刻修復全部鈕立刻處理所有事件，或是選擇修復鈕進行逐項的修復。
3. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

3.2. 網路安全防護狀態鈕

如果網路安全狀態按鈕顯示綠色，表示現在沒有任何風險。不然，如果按鈕顯示紅色，即表示您的電腦現處於高風險，並不安全。

下方的表格將會告訴您有哪些因素會被列入安全風險的評估。

事件	顏色
防火牆被關閉	紅色
隱藏模式被關閉	紅色
無線連接並不安全	紅色

依照這些步驟以修復事件：

1. 按下網路安全狀態按鈕
2. 您可以點擊立刻修復全部鈕立刻處理所有事件，或是選擇修復鈕進行逐項的修復。

3. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

3.3. 身分管控狀態鈕

如果身分管控狀態鈕呈現綠色，您不需要擔心任何威脅。如果狀態鈕呈現紅色或是紅色，則表示您的電腦正暴露在中度或是高度的風險之中!

下方的表格將會告訴您有哪些因素會被列入安全風險的評估。

事件	顏色
隱私權防護已被開啟	綠色
[新] 隱私權防護已設定及關閉	紅色
[新] 隱私權防護未設定	灰色

依照這些步驟以修復事件：

1. 點擊家長管控狀態鈕
2. 您可以點擊立刻修復全部鈕立刻處理所有事件，或是選擇修復鈕進行逐項的修復。
3. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

4. 快速任務

3個狀態鈕的下方有一個快速任務區域

4.1. 安全防護

BitDefender 的安全防護模組能夠協助您的電腦免受病毒威脅並且能夠隨時自動更新。

請點擊病毒防護 標籤，進入病毒防護模組。

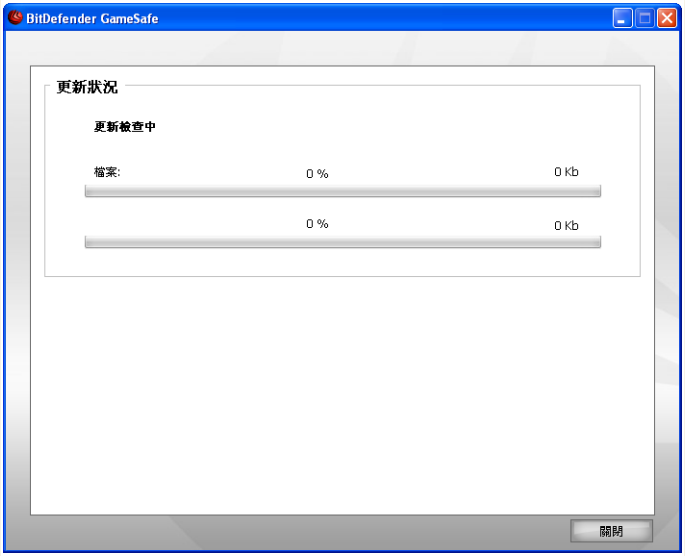
以下的選項是可用的：

■立即更新 — 立刻執行更新。
■掃描我的文件 — 執行一個針對我的檔案資料夾的快速掃描。
■深度系統掃瞄 — 執行一個針對您的電腦系統的完整掃瞄(包含已資料封存)。
■全系統掃描 — 執行一個完整的系統掃描(除了資料封存)。

4.1.1. 更新 BitDefender

每一天都有新的惡意程式被發現。這就是為什麼 BitDefender 需要保持最新的病毒特徵碼是非常重要的。預設上，BitDefender 是每個小時自動檢查更新。

預設上，當您啟動您的電腦系統時，BitDefender就會檢查是否有更新，之後每小時都會持續的檢查更新。 然而，如果您想要自行執行更新，點擊立即更新Update Now鈕。更新程序會立即被啟動並且出現下列視窗:



更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序在上的表現,表示要更新的檔案被漸進地替換。 這樣，更新程序將不影響產品性能，同時所有的弱點將被排除。

假如您想要關閉此視窗，請點擊關閉。 然而，這並不會終止更新程序。

注
如果您是利用撥號方式連線到網際網路，建議您定期地去更新 BitDefender 以獲的最好的防護效果。

重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。 假如您不想一直被提醒重新啟動電腦，請選擇稍後再重新啟動電腦。 如此，下次更新時將不會提醒您重新啟動電腦，BitDefender會先使用更新前的檔案直到您自行重新開機。

點擊重新啟動以重新啟動您的電腦。

假如您想要稍後再重新啟動您的系統，請點擊確定。 我們建議您盡快重新啟動您的系統。

4.1.2. 使用 BitDefender 掃瞄

點擊對應的按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述:

任務	描述
掃描我的文件	利用這個功能掃描重要的使用者資料夾：我的資料夾, 桌面 and 開始功能表。 這麼做可以保障您的檔案安全並且提供安全的環境運作應用程式。
深度系統掃描	掃描整個系統 在預設的配置中，它能構掃描您電腦中所有種類的惡意威脅
全系統掃瞄	掃描整個系統，資料封存(Archive)除外。 在預設的配置中，它能構掃描您電腦中所有種類的惡意威脅

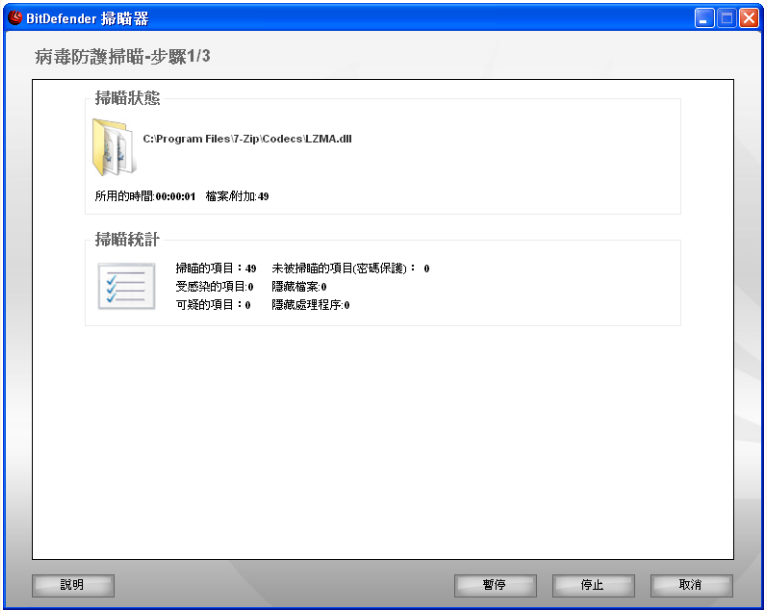
注
深度系統掃瞄 與 全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，甚至在您的系統閒置時更好。

當您執行掃描程序時，BitDefender 掃描器會立刻出現。

依照三步驟指引執行掃描任務。

步驟 1/3 — 進行掃描

BitDefender 將會開始掃描選擇的項目。



掃瞄中

您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

注
掃描程序將依它的複雜程度而需花費一些時間。

您可以點擊暫停，暫時停止掃描程序。點擊 回復以繼續掃描任務。

您可以點擊停止，完全停止掃描程序，而您將會直接被引導到最後的步驟。

等待BitDefender 完成掃描。

步驟 2/3 — 選擇動作。

當掃描程序完成，一個新的視窗會出現，您可以在該視窗檢視掃描結果。

動作

您可以檢視可能影響您的系統的事件數量。

被感染的物件會依照感染它們的惡意程式分組做表示。 點擊對應的威脅，您便可以得到更多關於被感染物件的資訊。

您可以針對不同的威脅類型的分組採取行動，也可以逐項地進行處理。

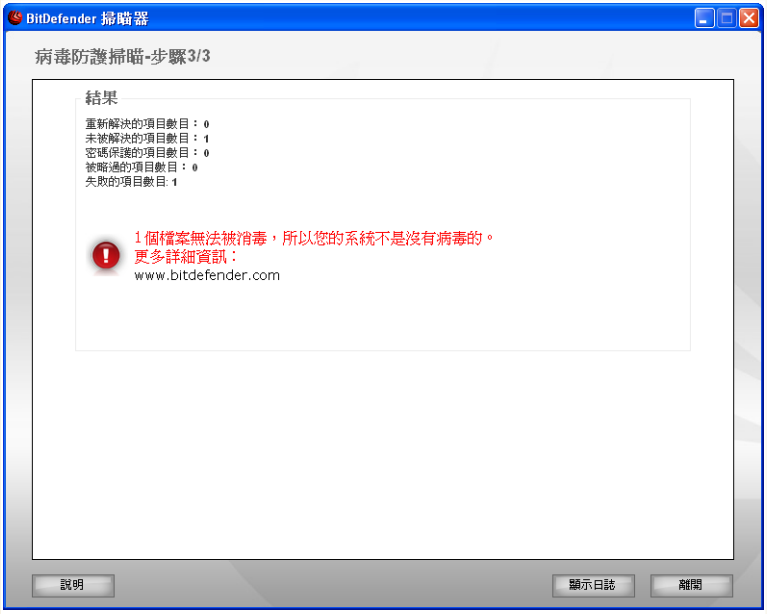
下列選項將會出現在選單中：

動作	描述
沒有動作	不對複製的檔案採取任何行動。
消毒檔案	消毒被感染的檔案。
刪除檔案	刪除所有被偵測的檔案
解除隱藏	顯示隱藏的物件。

請點擊 繼續 以套用指定的動作。

步驟 3/3 — 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗。



總結

您可以檢視結果。 在各別掃描任務的 內容視窗，報告檔案會自動儲存在 掃描日誌頁面。

重要
您的系統可能被要求重新啟動，令安裝精靈完成您的安裝程序。

按下 離開 去關閉視窗。

BitDefender 可能無法解決某些問題

在大部分的情形中，BitDefender 能夠成功地消毒被感染的檔案或是將之隔離。 然而，可能有極少部分的問題無法被解決。

在這種情況下，我們建議您聯絡BitDefender 在網頁www.bitdefender.com的支援小組。 我們的技術支援代表將會協助您解決您遭遇的問題。

BitDefender 偵測到密碼保護的物件

被密碼保護的目錄通常包含兩個種類：資料封存以及安裝程式檔。 通常它們不會是真正的安全威脅，除非內含被感染的物件而且被執行。

確定這些項目是無害的:

- 將被密碼保護的資料封存解壓縮，進行對內容物件的掃描。 在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2008。
- 假如被密碼保護的是安裝程式檔，請確認您的即時防護 是被啟用的，再執行。 如果安裝程式受到感染，BitDefender 將會將它隔離。

假如您不希望這些檔案再次被BitDefender掃描，您可以將這些檔案加入例外清單。想增加例外掃瞄，按下設定來開啟管理主控台然後到病毒防護；及例外。 請參照 被排除掃描的物件，獲得更多資訊。

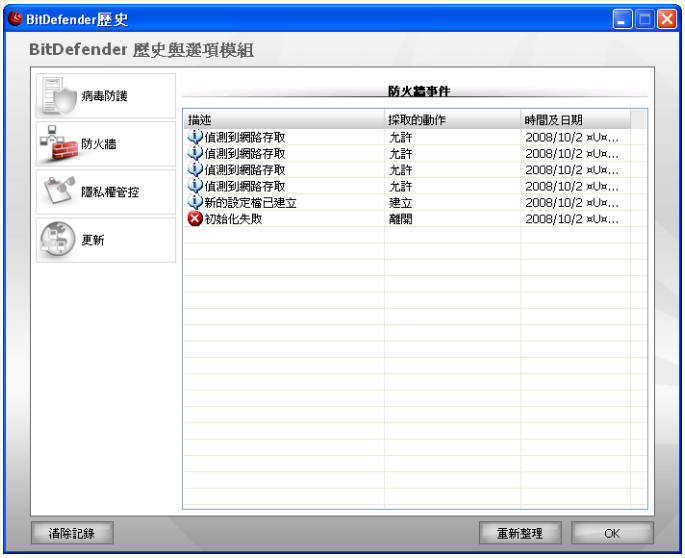
BitDefender 偵測到可疑的檔案

可疑的檔案是被探索式分析歸類被潛在的、沒有正式發布惡意程式碼所感染的檔案。

如果偵測到可疑的檔案，您會被要求將可疑的檔案遞交給BitDefender Lab。 點擊好將這些檔案送交BitDefender Lab做進一步的分析。

5. 歷史紀錄

在BitDefender安全防護中心視窗下方的 歷史紀錄鈕將可以開啟另一個視窗BitDefender歷史紀錄& 事件。這個視窗提供您概括性的檢視與安全性相關的事件。



事件

為了協助您過濾BitDefender歷史紀錄，視窗左側將提供以下目錄:

■病毒防護
■防火牆
■隱私權管控
■更新

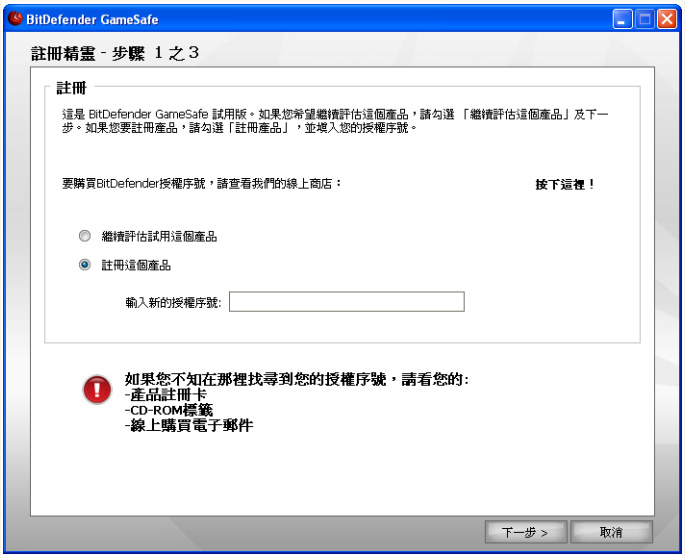
每一個目錄都有一個可用的事件清單，每個清單包含下列資訊：簡短的敘述、BitDefender所執行的動作、發生的時間日期。如果您想了解更多只需要在事件上點擊兩下即可。。

點擊 清除紀錄 如果您想要清除舊的紀錄。點擊 重新整理 以顯示最新的日誌。

6. 註冊

BitDefender GameSafe 有30天試用期。 如果您想要登記 BitDefender GameSafe, 更改授權序號或者建立一個 BitDefender 帳戶, 按下 註冊連接, 在 BitDefender 安全防護中心視窗的頂端設置。 註冊精靈將會出現。

6.1. 步驟 2/5 — 註冊 BitDefender GameSafe



註冊

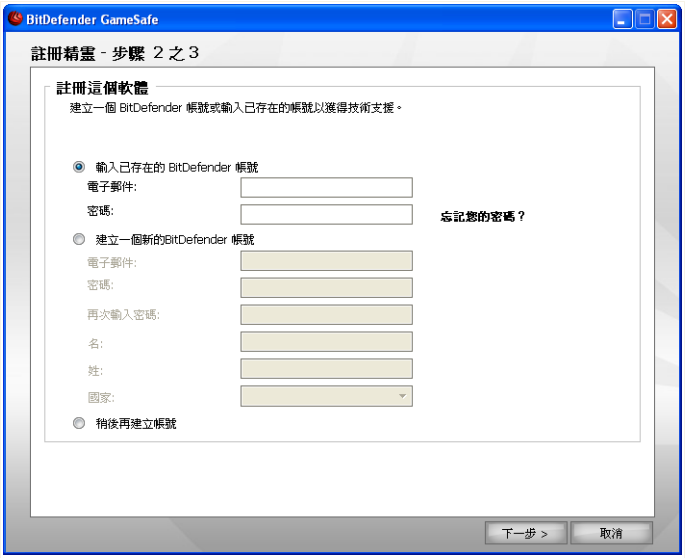
假如您沒有BitDefender的授權，您可以連線至BitDefender 線上商店購買授權序號。

要註冊GameSafe，選擇 註冊軟體，輸入授權序號在 輸入新的序號 欄位。

如未過試用期間您希望繼續評估這個軟體，請選擇繼續評估這個軟體。

按下 下一步 繼續。

6.2. 步驟 2/3 — 建立一個 BitDefender 帳號



帳號建立

我尚未擁有一個 BitDefender 帳號

為了取得免費的 BitDefender 技術支援及其他免費的服務，您需要建立一個帳號。

注
如果您想稍後才建立新的帳戶，請選擇合適的項目。

選擇 建立新的 BitDefender 帳號 及提供所需的資料。 您在這裡所提供的資料將會被保密。

■E-mail — 輸入您的電子郵件信箱。

■密碼 — 為您的BitDefender帳號輸入一組密碼。

注
密碼長度至少要四個字元。

■重複鍵入密碼 — 重新輸入先前的密碼。

■名 — 輸入您的名字。

■性 — 輸入您的姓氏。

■"國家 —選擇您所在的國家。

注
在http://myaccount.bitdefender.com使用您提供的電子郵件地址和密碼來登錄您的帳戶。

要成功建立一個帳號，您必須啟動您的電子郵件。確認您的電子郵件位址並依循 BitDefender 註冊服務所寄給您的電子郵件中的指示完成。

按下 下一步 繼續。

我已經有一個 BitDefender 帳號。

如果您先前已經在您的電腦上登記一個 BitDefender 帳戶， BitDefender 將會自動地發現。 在這個情況，您需要按下下一步繼續進行安裝。

如果您已經有一個帳戶,但是 BitDefender 不能找到它，請選擇登入到已有的 BitDefender 帳戶 及提供您帳戶的電郵地址及密碼。

注
或者選擇按下 Next(下一步)繼續進行安裝。 按下 下一步 繼續，或按 取消 離開安裝精靈。

如果您忘記您的密碼，按下 忘記您的密碼？ 並依循指示操作。

按下 下一步 繼續。

6.3. 步驟 2/5 — 註冊 BitDefender GameSafe

總結

選擇 開啟我的 BitDefender 帳號 輸入您的 BitDefender 帳號。要求網際網路連線。

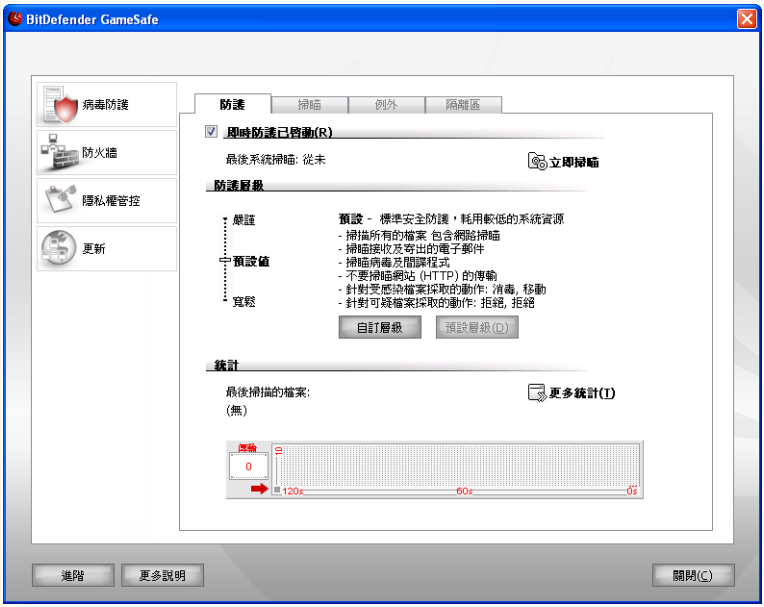
按下 完成 去關閉視窗。

進階安全防護管理

7. 管理主控台

BitDefender GameSafe內部的中央化管理主控台可以讓您進行進階的調整管理 BitDefender。

請點擊設定以進入管理主控台。



管理主控台

管理主控台包含以下模組：病毒防護、隱私權管控 、防火牆以及 更新。 這讓您容易地處理安全問題的類型為基礎的 BitDefender 。

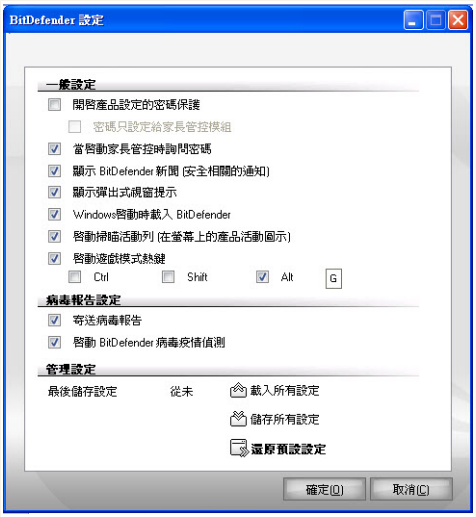
在管理主控台的左方，您可以看到模組的選擇器：

■病毒防護 — 在這個頁面您可以設定 病毒防護 模組。
■防火牆 — 在這個頁面您可以設定 防火牆 模組。
■隱私權管控 — 在這個頁面您可以設定 隱私權管控 模組。
■更新 — 在這個頁面您可以設定 更新 模組。

如果您需要更多幫助，點擊畫面下方的更多幫助鈕。 一個說明頁面將會開啟，此頁面將會提供您關於各個區域的詳細資訊。

7.1. 調整一般設定

若要為 BitDefender GameSafe 配置一般設定，按下進階. 一個新的視窗將會開啟。



一般設定

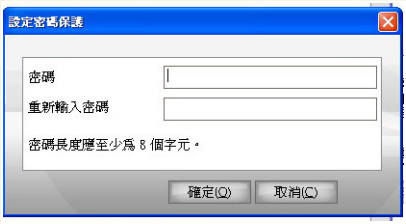
在這裡可以設定所有 BitDefender 喜好。預設上，BitDefender 會在 視窗啟動時被載入，並執行最小化在系統工具列上。

7.1.1. 一般設定

■啟動密碼保護 — 此選項為了保護 BitDefender 管理主控台的設定。

注
如果您不是此電腦唯一擁有管理權限的人，建議您設定密碼保護您的 BitDefender 設定。

如果您選擇了此選項，下一個視窗將會出現：



輸入密碼

在密碼欄位上，輸入密碼，在重新輸入密碼欄位上，重新輸入密碼，並按下確定。

一旦您設了密碼，每次您要變更BitDefender設定時，您都會被要求輸入密碼。 其他的系統管理者(假如有)若要變更設定也是需要此密碼。

重要
如果忘記密碼，您必須修正此軟體才可進行 BitDefender 的設定。

■顯示 BitDefender 消息 (安全通知) — 由 BitDefender 伺服器寄送關於病毒疫情擴散的即時安全通知。
■顯示彈出式視窗 (螢幕上的提示) — 在彈出式視窗顯示軟體狀態。
■在 Windows 啟動後載入 BitDefender — 在系統啟動後，自動地開啟 BitDefender。 我們建議您保留此選項的選擇。
■啟動掃描活動列 (螢幕上顯示掃描活動的狀態 — 啟動/關閉 掃描活動列。 您可以取消這個核取方塊假如您不想看見掃描活動列。

注
此選項只能被目前的Windows使用者調整。

■使用熱鍵開啟遊戲模式 — 允許您使用這件啟動或停用遊戲模式。 預設的熱鍵為 Alt+G。

您可以依據以下指示變更熱鍵設定：

1. 您可以選用下列的功能鍵：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)。
2. 在編輯欄鍵入您常用的字母以對應熱鍵。

7.1.2. 病毒報告設定

■寄送病毒報告 — 當您的電腦發現病毒時，寄發病毒報告到 BitDefender 實驗室。它將協助我們保持病毒疫情擴散的追蹤。

這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。這個資訊只包含病毒名稱，並且僅僅用來建立統計報告。

■啟動 BitDefender 疫情擴散偵測 — 將潛在病毒疫情擴散報告寄送到 BitDefender 實驗室。

這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。這個資訊只包含潛在病毒並且僅僅用來偵測新的病毒。

7.1.3. 管理設定

使用 儲存所有設定 / 載入所有設定 按鈕，進行儲存 / 載入您在 BitDefender 所做的設定。在您重新安裝或修護 BitDefender 時，您可以使用相同的設定。

重要

只有具有管理權限的使用者才可以儲存及載入設定。

要讀取預設設定，按下 還原到預設設定 。

8. 病毒防護

您會被指導如果裝配及使用所有BitDefender模組使更有效地保護您的電腦對抗所有惡意程式的威脅 (病毒、間諜程式、病毒製造工具及其他)。

使用啟發式偵測掃描檔案。啟發式掃描技術針對的目前是辨識新的病毒，在一個病毒定義被發現前，是依靠著確定的樣本及演算法。錯誤警告訊息會出現。當這種檔案被偵測到時，它會被當成可疑的檔案。在這種情況下，我們建議您寄送這個檔案到 BitDefender 實驗室進行分析。

BitDefender 的安全防護可分為二大種：

- 正在使用掃瞄 - 阻止新的惡意軟體帶來的威脅進入您的系統。 這也叫做即時的保護 - 當您正在使用他們的時候，檔案也可被掃描。 舉例來說，當您打開它的時候，BitDefender 將會掃描您正在開啟的 Word 檔案，以及您接收中的電子郵件。
- 要求的掃描 - 允許發現而且除去惡意軟體在您的系統。 手動掃描 — 偵測已存在於您電腦中的病毒、間諜程式或其他的惡意程式。這是使用者典型的掃描方式 — 您可以選擇想要掃描的磁碟機、目錄或檔案，BitDefender 將手動掃描它。 您可以依照您的習慣設計掃描任務。

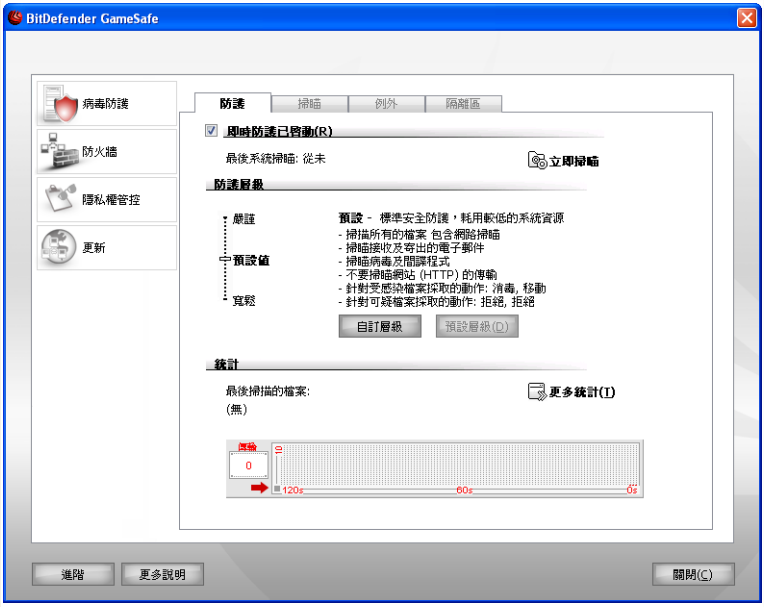
在使用者手冊的 病毒防護 手冊包含了以下的主題:

- 即時掃描
- 手動掃描
- 例外項目掃瞄
- 隔離區

8.1. 即時掃描

掃描存取的檔案及點對點的傳輸選項 — 掃描被存取的檔案及透過即時傳訊軟體溝通的應用程式 (ICQ、NetMeeting、Yahoo Messenger、MSN Messenger)。選擇您所要掃描的檔案型態。

要調整及監控即時防護，請點擊在管理主控台的病毒>防護。 以下視窗將會顯示:



即時防衛

重要

為了防止病毒感染您的系統，請保持即時防護 啟動的狀態。

在這個頁面的底部，您可以看到即時防護統計掃描檔案及電子郵件的狀態。按下 更多統計您可以看到更多詳細的內容。

要開始快速掃瞄，按下立即掃瞄。

8.1.1. 更改防護層級

您可以選擇最適合您安全需求的防護等級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

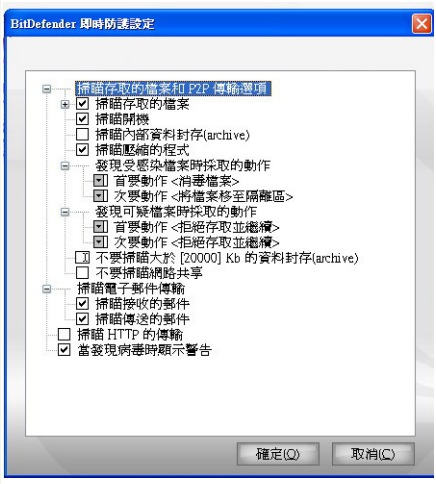
防護層級	描述
許可的	含概基本的安全需求。資源耗用層級非常低。 只有應用程式和接收的電子郵件會被掃描。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。
預設	提供標準的安全。資源耗用層級屬低。 所有檔案、接收及傳送的電子郵件都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。
嚴謹	提供較高的安全。耗用資源層級屬中等。 所有檔案、接收及傳送的電子郵件及網站的傳輸都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。

如果您想要回復到預設層級，按下 預設層級。

8.1.2. 自訂保護層級

進階的使用者可以使用 BitDefender 所提供掃描設定的優勢。掃描器中可以設定排除一些副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

您可以自訂 即時防護，按下 自訂層級。以下的視窗將會出現：



防護機制設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 按下 "+" 的小方框以展開選項或按下 "-" 的小方框關閉選項。

注
您會注意到雖然一些掃描選項前面出現 "+"，但卻無法被展開。這是因為這些選項尚未被選取。您會注意到，如果您選擇了這些選項，則其細項即可被展開。

■掃描存取的檔案及點對點的傳輸選項 — 掃描被存取的檔案及透過即時傳訊軟體溝通的應用程式 (ICQ、NetMeeting、Yahoo Messenger、MSN Messenger)。選擇您所要掃描的檔案型態。

選項		描述
掃描存取的檔案	掃描所有檔案	所有存取的檔案都將被掃描，不管其型態為何。
	只掃描應用程式檔案	只有應用程式檔案將被掃描。代表只有以下副檔名的檔案才會被掃描：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole;

選項		描述
		.exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。
	掃描危險程式	掃描記憶體裡隱藏的惡意程式。 被偵測掃描的危險程式將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。 選擇 掃描中跳過撥號程式及應用程式，如果在掃描過程中，您想要排除這類型的檔案進行掃描。
掃描開機區域"		掃描系統開機磁區。
掃描內部資料封存		被存取的資料封存將被掃描。當這個選項啟動時，電腦將會變慢。
掃描壓縮檔案		所有壓縮檔案將會被掃描。
第一個動作		從下拉式選單選擇當遇到受感染及可疑檔案時，第一個動作所要採取的行動。
	禁止存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。
	清除檔案	消毒被感染的檔案。
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。
	移動檔案到隔離區	移動受感染的檔案到隔離區。
第二個動作		從下拉式選單選擇當遇到受感染的檔案時，所要採取的第二個動作。(當第一個動作失敗時)
	禁止存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。

選項		描述
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。
	移動檔案到隔離區	移動受感染的檔案到隔離區。
不要掃描大於 [x] Kb 檔案		輸入要被掃描的最大檔案大小。如果大小為 0Kb， 代表所有檔案將被掃描，而不管這些檔案的大小。
不要掃描網路共用檔案		如果啟動此選項，BitDefender 將不掃描網路共用檔案，提供您更快的網路連結。 假如您的網路作業環境已經有病毒防護措施，我們才建議您啟動此選項。

■掃描電子郵件傳輸 — 掃描電子郵件的傳輸。

以下的選項是可用的：

選項	描述
掃描接收的電子郵件	掃描所有接收的電子郵件訊息。
掃描傳送的電子郵件	掃描所有傳送的電子郵件訊息。

■掃描 Http 傳輸 — 掃描 Http 傳輸。

■當發現病毒時提出警告 — 在檔案或電子郵件中發現病毒時，開啟一個警告視窗。

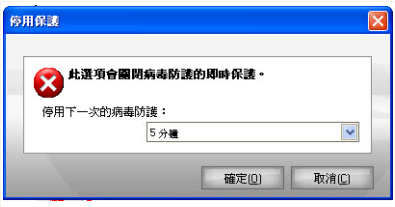
一個受感染的警告視窗將包含病毒名稱、發現的路徑、BitDefender 所採取的行動及一個連結到 BitDefender 的網站，在那裡您可以得到更多關於此病毒的資訊。在一個受感染的電子郵件警示視窗裡也包含了寄件者及收件者的資訊。

當偵測到一個可疑的檔案時，您可以從警告視窗裡開啟一個精靈，它將協助您寄送檔案到 BitDefender 實驗室進行分析。您可以輸入您的電子郵件位址以得到這個報告的相關資訊。

按下 確定 儲存這個設定並關閉視窗。

8.1.3. 停用即時防護

如果您想要停用即時防護，一個警告視窗將會出現：



停用即時防護

您可以從視窗選擇您要停用即時防護的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。

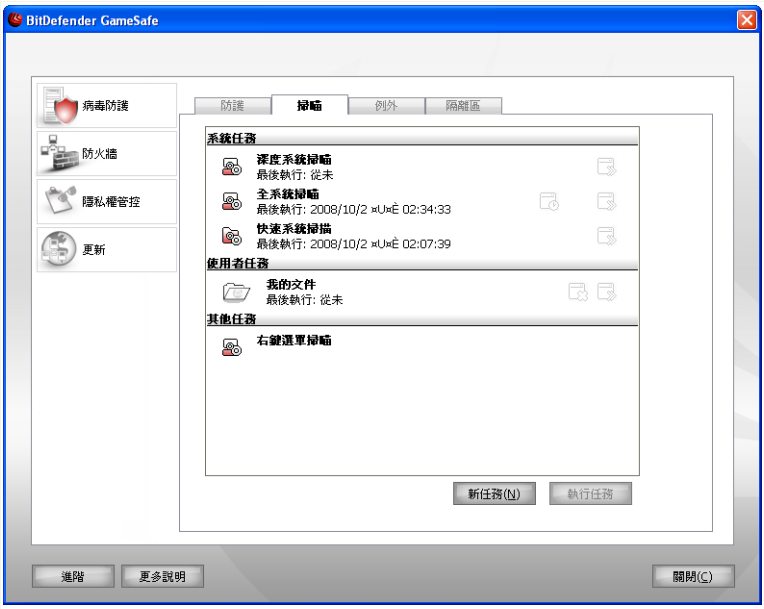
警告
這是個極為重要的安全防護問題。我們建議您盡量縮短停用即時防護的時間。假如您停用即時防護，您的電腦將暴露於各種惡意程式威脅之中。

8.2. 手動掃描

BitDefender 的主要目的是維護您的電腦免受到病毒的威脅。保持新的病毒遠離您的電腦是最首要的目標，透過掃描電子郵件、新下載的檔案或複製到您系統的檔案。

在您安裝 BitDefender 前，可能已經有病毒存在於您的系統中。這是為什麼在您完成安裝 BitDefender 後，要求掃描您的系統，以找出存在的病毒。經常掃描您的電腦是個很好的建議。

在管理主控台點擊病毒防護>掃描，可以調整以及啟動手動掃描。 以下視窗將會顯示:



掃描任務

手動掃描是以掃描任務為基礎。掃描任務決定要被掃描的物件以及掃選項。 您可以用預設的掃描任務或是您(使用者)自訂的掃描任務來掃描電腦。您也可以規劃它們用基本的方式進行或是當您的電腦閒置時，以避免影響您的作業。

8.2.1. 掃描任務

在系統預設情況下BitDefender以幾項任務，建立包含普通安全問題。 您也能建立您自訂的掃瞄任務。

每項任務有屬性允許您配置任務和看掃描結果的視窗。 對於更多信息，查看"設定掃描任務" (p. 50).

掃描任務有三個類別：

■系統任務 — 包含預設的系統掃描。下方是可用的掃描任務：

預設的任務	描述
深度系統掃描	掃描整個系統 在預設的配置中，它能構掃描您電腦中所有種類的惡意威脅
全系統掃瞄	掃描整個系統，資料封存(Archive)除外。 在預設的配置中，它能構掃描您電腦中所有種類的惡意威脅
快速的系統掃描	掃描Windows ， Program Files 以及 All Users 資料夾。 在預設的設定中，可以掃描除後門程式外所有的惡意程式，但是不會掃描記憶體、登錄碼、cookies.

注
深度系統掃瞄 與 全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，甚至在您的系統閒置時更好。

■用戶的任務 — 包含用戶定義的任務。

有一個叫做 我的檔案的掃描任務。 使利用這個掃描任務執行掃描重要的使用者資料夾，如：我的檔案 、桌面 以及 開始功能表。

■其他的任務 — 包含其他掃描任務的清單。這些掃描任務參考到其他替代的掃描型態，而且它無法在這個視窗中執行。您只可以修改它們的設定及檢視掃描報告。

每個掃描任務頁面的右邊有三個可按的標籤頁面：

■ 排程任務 — 選擇將以排程來執行的任務。 從 內容視窗裡，按下 排程器 頁面，您可以修改這個設定。

■ 刪除 — 刪除所選擇的掃描任務。

注
系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

■ 立即掃描 — 執行所選的掃描任務，進行一個 立刻掃描。

在每個任務的左方您可看見內容 — 允許您去設定任務以及檢視掃描日誌。

8.2.2. 使用捷徑選單

每個掃描任務都有一個捷徑選單可使用。在選擇的掃描任務按下滑鼠右鍵去開啟它：

在捷徑選單上有以下可用的命令：

立即掃描 — 立刻掃描所選的掃描任務。

捷徑選單

■

■變更掃描目標 — 開啟 內容 視窗，掃描路徑 標籤頁，您可以更改所選掃描任務的掃描目標；

注
在系統掃描任務頁面，這著選項將會顯示掃描路徑被替代，而只能看見掃描目標。

■任務排程 — 選擇將要排程執行的任務。 從 內容視窗裡，點擊 排程器 標籤，您可以在此進行任務排程。

■檢視掃描日誌 — 開啟內容 視窗，掃描日誌 標籤頁，在掃描任務執行後，您可以檢視產生的報告。

■複製 — 複製所選擇的掃描任務。

注
當建立新的掃描任務時，您可以方便地修改已複製的掃描任務的設定。

■刪除 — 刪除所選擇的掃描任務；

注
系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

■內容 — 開啟內容視窗，檢視 標籤頁，您可以更改所選掃描任務的設定=;

注
由於特性不同，在 其他任務 的類別裡，只有 內容 及 檢視掃描日誌 二種選項可使用。

8.2.3. 建立掃描任務

您可以選擇以下其中之一種方法建立掃描任務：

■複製 一個存在的掃描任務，您可以在 內容 視窗中更改它的名稱或做必要的修改設定；
■按下 新的任務 ，建立一個新的掃描任務並且設定它。

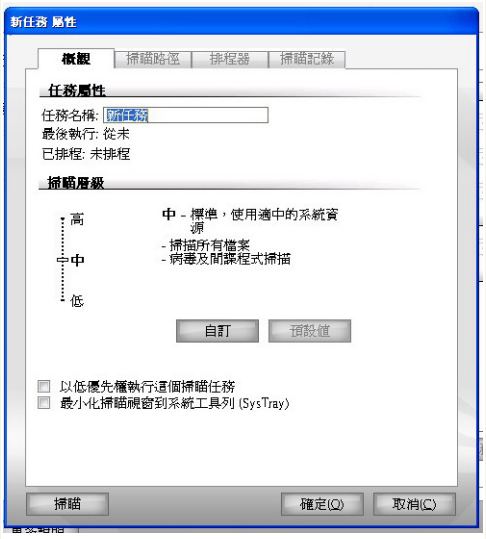
8.2.4. 設定掃描任務

每個掃描任務都有它的 內容 視窗，您可以設定掃描的選項、掃描的目標、指定排程或檢視報告。從這個視窗裡的任務名稱按二下。下面的視窗將會出現： 按下右邊的開啟鈕，開啟視窗(或是在任務上點擊滑鼠右鍵，選擇開啟)。

注
更多關於 日誌 頁面的資訊，請參考 "檢視掃描日誌" (p. 66)。

調整掃描設定

要調整任何特定的掃描任務，請按下滑鼠右鍵，並選擇內容。 以下視窗將會顯示:



概觀檢視

在這裡，您可以檢視掃描任務的資訊（名稱、上次執行的時間及排程狀態）及設定掃描的設定。

選擇掃瞄層級

首先，您必須選擇掃瞄的層級。拖曳滑桿到合適的掃瞄層級。

一共有三個掃瞄層級：

防護層級	描述
低	提供適當的偵測效率。耗用系統資源資源屬低。 只有應用程式被掃描是否有病毒。除了基本的特徵掃描，也使用了啟發式的分析。當有檔案受到感染時。
中	提供良好的偵測效率。耗用系統資源層級屬中等。 所有檔案都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。當有檔案受到感染時。

防護層級	描述
高	提供高水準的偵測效率。耗用系統資源層級較多。 所有檔案及檔案都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。當有檔案受到感染時。

在掃描程式中可用到的一系列設定選項：

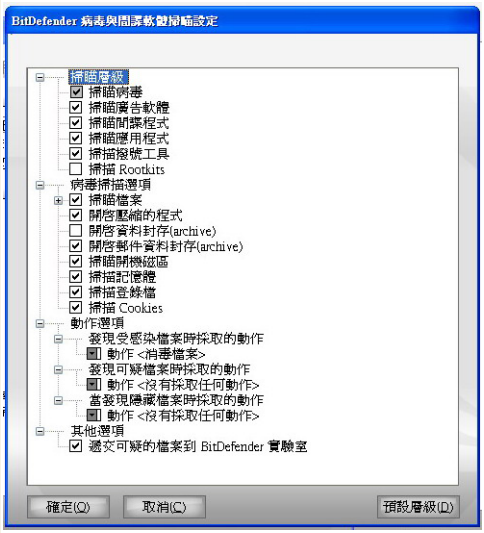
選項	描述
以低優先權執行任務	降低掃描程序的優先權。您可以讓其他程式執行的更快，但這個掃描程序將會花更長的時間去完成。
系統啟動後，將視窗最小化到系統工具列	將掃描視窗最小化到 系統工具列。可以按二下 BitDefender 圖示去開啟它。

按下 確定 要保存變動和關上視窗。 進行任務，正義點擊掃描 。

自訂掃瞄層級

進階的使用者可以使用 BitDefender 所提供掃描設定的優勢。掃描器中可以設定排除一些副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

按下 自訂，將會出現一個新視窗，您可以設定自己的掃描選項：



掃描設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 按下 "+" 的小方框以展開選項或按下 "-" 的小方框關閉選項。

掃描選項被分為四個類型：

■掃瞄層級
■病毒掃描選項
■動作選項
■其他選項

■從掃瞄層級選單選擇適合的選項，儘指定您要BitDefender掃瞄的惡意程式類型。

以下的選項是可用的：

選項	描述
掃描病毒	掃描已知病毒威脅。

選項	描述
	BitDefender也能夠偵測到不完整的病原體，因此能夠移除您系統內的可能威脅。
掃描廣告程式	掃描廣告程式。被偵測到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。
掃描間諜程式	掃描已知的間諜程式。被偵測到的檔案將被當成受感染的檔案。
掃描應用程式	掃描應用程式（檔名為.exe 或 .dll的檔案）。
掃描撥號程式	掃描高收費陷阱的撥號程式。這些被掃描到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含這類型撥號程式的軟體將無法運作。
掃描後門程式	掃描隱藏的物件，一般統稱後門程式。

■選擇要被掃描的元件型態（資料封存、檔案、電子郵件，等）以及其他選項。這個設定可以從 病毒掃描選項 中去進行設定。。

以下的選項是可用的：

選項		描述
掃描檔案	掃描所有檔案	所有被存取的檔案都將被掃描，不管其型態為何。
	只掃描應用程式檔案	只有應用程式將會被掃描。這代表只有以下的副檔名將被掃描：exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml 及 nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。

選項	描述
開啟被壓縮的程式	掃描壓縮的檔案。
資料封存	掃描內部資料封存。
開啟電子郵件資料封存	掃描電子郵件資料封存。
掃描啟動磁區	掃描系統開機磁區。
掃描記憶體	掃描記憶體是否有病毒或其他的惡意程式。
掃描登錄碼	掃描登錄碼內容。
掃描 Cookies	掃描 cookie 檔案。

■請針對受感染或可疑的檔案應執行的指定動作。為了檢視遭遇到這些檔案時所有可能的動作，請開啟 動作選項 類別。

• 選擇當偵測到受感染的檔案時執行的動作： 以下的選項是可用的：

動作	描述
無 (只記錄物件)	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
消毒檔案	消毒被感染的檔案。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	移動受感染的檔案到隔離區。

• 選擇採取行動在檢測有可疑檔案。 以下的選項是可用的：

動作	描述
無 (只記錄物件)	不會採取行動在可疑檔案。 這些檔案將出現於報告檔案。
刪除檔案	立刻刪除受感染的檔案，不需任何警告。
移動檔案到隔離區	移動可疑的檔案到隔離區。

注

假如有檔案被探索式分析偵測為可疑的檔案，我們建議您將這些檔案送交至 BitDefender Lab。

• 選擇當偵測到隱藏的物件(後門程式)行的動作。 以下的選項是可用的：

動作	描述
無 (只記錄物件)	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
移動檔案到隔離區	移動受感染的檔案到隔離區。
顯示隱藏的檔案	顯示所有隱藏的檔案。

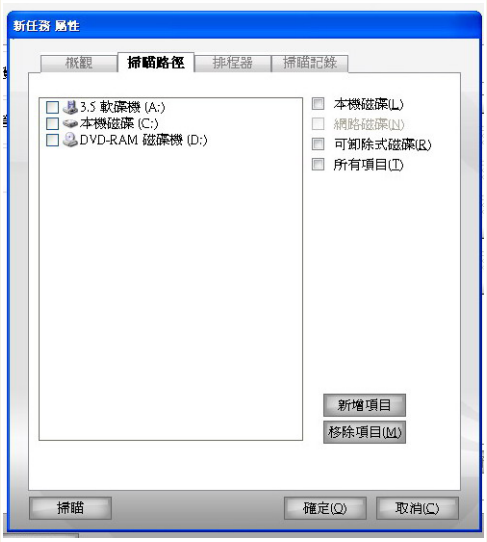
注
如果您選擇不理會被偵測的檔案或是選擇的動作失敗了，您將必須在精靈選擇行動。

■在其他選項頁面，點擊遞交可疑的檔案至 BitDefender Lab。

如果您按下 預設層級 您將載入預設的設定值。 按下 確定 儲存這個設定並關閉視窗。

設定掃描目標

要設定特定使用者掃描任務的掃描目標，請按下滑鼠右鍵，並選擇變更掃描目標。 以下視窗將會顯示:



掃描目標

您可以看見本系統、網路、可拆除式磁碟中的檔案。所有被選擇的物件都會被掃描。這個頁面包含了以下的按鈕：

■新增物件 — 開啟一個瀏覽的視窗，您可以選擇所要掃描的檔案。

注
您可以將檔案拖曳增加至檔案/目錄到清單中。

■">移除物件 — 從掃描清單中移除先前所選擇的檔案或目錄。

注
只有後來被加入檔案 / 資料夾才能被刪除。

除了上面解釋過的按鈕，也有一些選項允許您快速選擇掃描位置。

■本機磁碟 — 掃描本機磁碟。

■網路磁碟 — 掃描所有網路磁碟。
■可拆除式磁碟 — 掃描可拆除式的磁碟（光碟、軟碟）。
■所有項目 — 掃描所有磁碟，不管是本機、網路或者可拆除式的磁碟。

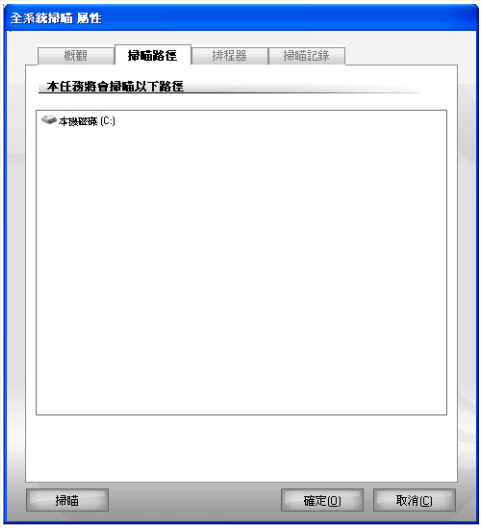
注
如果您想要掃描整個電腦是否有病毒，請選擇核取方塊對應的 所有項目。

按下 確定 要保存變動和關上視窗。 進行任務，正義點擊掃描 。

檢視系統任務的掃描目標

您無法變更在系統任務目錄下的掃描目標 您只可以看見掃描的目標。

若要檢視特定任務的掃描目標，按下滑鼠右鍵，並選擇顯示任務路徑。 以全系統掃描為例，以下的視窗將會出現：



全系統掃描的掃描目標

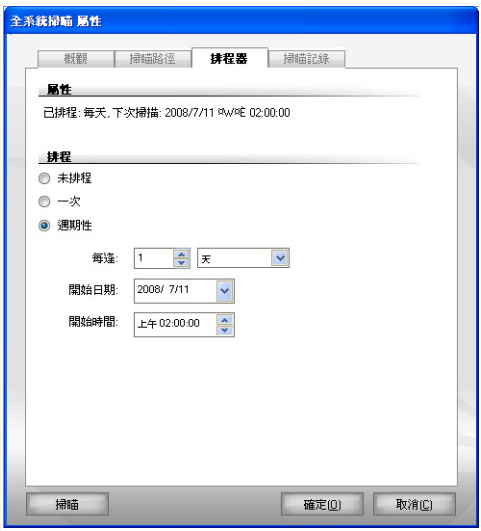
全系統掃描 與 深度系統掃描 將會掃描所有的本機磁碟，而 快速系統掃描只會掃描 Windows 與 Program Files 的檔案與資料夾。

按下 確定 關閉視窗。 要執行本任務，按下 掃描。

排程掃描任務

在複雜的掃描任務中，掃描程序將花費一些時間，如果您可以關閉其他應用程式，那掃描工作將會進行得更順利。這也就是為什麼當您沒有使用電腦或者電腦閒置時，是您進行排程掃描的最佳時機。

要看見特定的任務排程或要調整它，在任務按右鍵並選擇 排程。 以下視窗將會顯示:



排程器

您能見到排程任務,如果有的話。

當排程一個掃描任務時，您必須選擇以下選項的其中之一：

- 未被排程 — 只有當使用者要求時，這些任務才會被啟動。
- "一次 — 在一定的時間，只執行一次的掃描任務。在 開始日期/時間 欄位，指定開始的日期及時間。
- 定期 — 定期地執行掃描任務，在一定的時間間隔裡(小時、天、週、月、年) 依指定的日期及時間開始進行掃描。

在確定的時間間隔裡，如果您想要重覆某個掃描任務，請選擇 定期 並且編輯 每一欄位裡 minutes /hours /days / weeks/ months/ years 的數字，以指出掃描程序的執行頻率。您必須在 開始日期/時間 欄位上指出開始執行的日期及時間開始日期/時間 檔案

按下 確定 要保存變動和關上視窗。 進行任務，正義點擊掃描 。

8.2.5. 掃描物件

在您開始一個掃描程序之前，您應該先確認BitDefender 的惡意程式驗證碼是最新的。在管理主控台點擊更新>更新，可以確認是否已經擁有最新的更新。

注
為了讓 BitDefender 完成一個完整的掃描，您必須關閉所有開啟的程式。特別是電子郵件程式(如：Outlook、Outlook Express 或 Eudora) 更需要在完整掃描時進行關閉。

掃描方式

BitDefender 提供四個型態的手動掃描：

- 立刻掃描 —從系統/用戶任務進行掃瞄任務。
- 右鍵選單掃描 — 在檔案或者目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2008。
- 拖放掃描 — 拖曳一個檔案或目錄放到 掃描活動列上。
- 手動選擇掃描 — 使用BitDefender 手動選擇掃描瀏覽並選擇要掃描的檔案或檔案。

立刻掃描

要掃描您的電腦或部分您能進行缺省掃瞄任務或您自己掃瞄任務 這被稱為立刻掃描。

您可以選擇以下方式的其中之一：

- 在清單要執行的任務連續點擊兩下。
- 按下所對應任務的 立即掃描 鈕。
- 選擇任務，並按下執行任務。

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 62)。

右鍵選單掃描

您可以直接使用右鍵選單直接掃描檔案或是資料夾。 右鍵選單掃描

右鍵選單掃描

在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2008。

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 62)。

在 右鍵選單掃描 任務的 屬性 視窗，您可以修改掃描選項並檢視報告檔案。

拖放掃描

拖放您想要掃描的檔案或資料夾到下方顯示的 掃描活動列。

拖曳檔案

放開檔案

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 62)。

手動選擇掃描

您能夠在開始功能表中的程式集使用手動選擇掃描選項，直接瀏覽並掃描檔案。

注
手動選擇掃描是一個很方便的功能，在Windows的安全模式中也能使用。

如果您想要在開始功能表執行BitDefender掃描功能，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2008 → BitDefender 手動選擇掃描。

以下視窗將會顯示:

手動選擇掃描

選擇要掃描的物件並按下 確定。

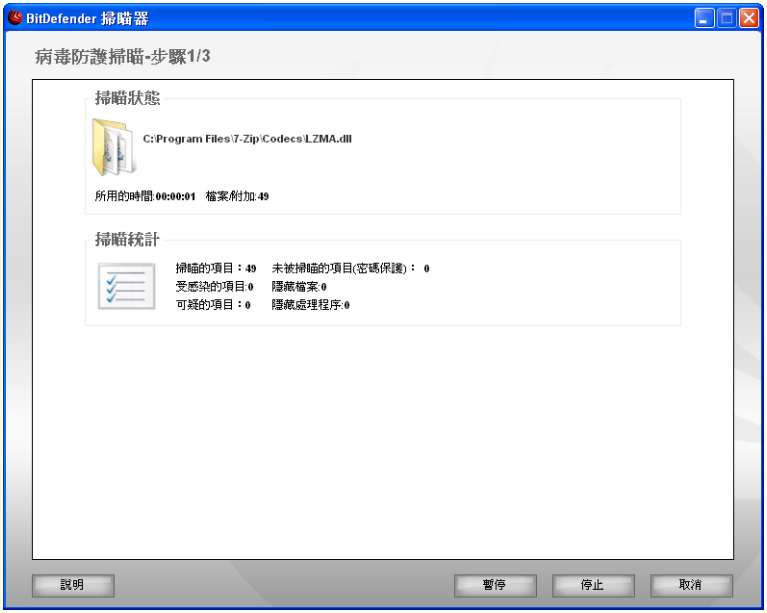
BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 62)。

BitDefender 掃描器

當您開始一個手動掃描程序時，BitDefender 掃描器將會出現。 依照三步驟指引執行掃描任務。

步驟 1/3 — 進行掃描

BitDefender 將會開始掃描選擇的項目。



掃瞄中

您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

注
掃描程序將依它的複雜程度而需花費一些時間。

您可以點擊暫停，暫時停止掃描程序。點擊 回復以繼續掃描任務。

您可以點擊停止，完全停止掃描程序，而您將會直接被引導到最後的步驟。

等待BitDefender 完成掃描。

步驟 2/3 — 選擇動作。

當掃描程序完成，一個新的視窗會出現，您可以在該視窗檢視掃描結果。

動作

您可以檢視可能影響您的系統的事件數量。

被感染的物件會依照感染它們的惡意程式分組做表示。 點擊對應的威脅，您便可以得到更多關於被感染物件的資訊。

您可以針對不同的威脅類型的分組採取行動，也可以逐項地進行處理。

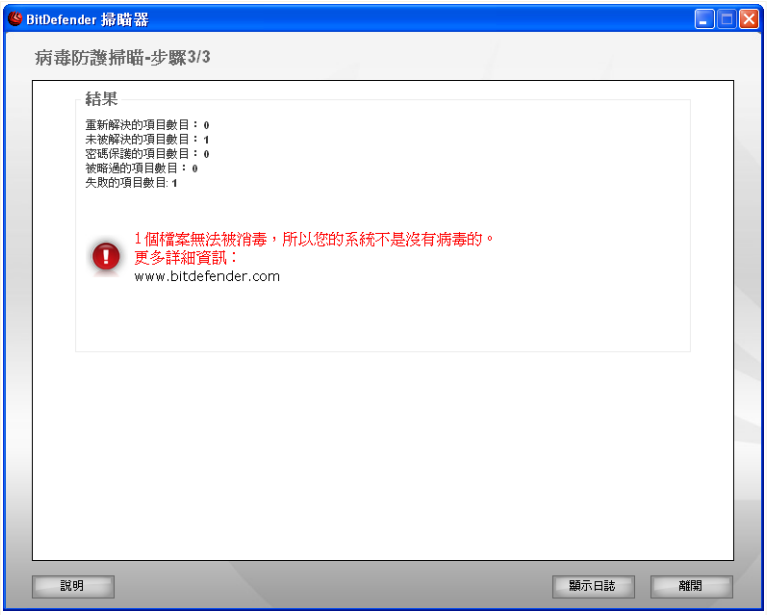
下列選項將會出現在選單中：

動作	描述
沒有動作	不對複製的檔案採取任何行動。
消毒檔案	消毒被感染的檔案。
刪除檔案	刪除所有被偵測的檔案
解除隱藏	顯示隱藏的物件。

請點擊 繼續 以套用指定的動作。

步驟 3/3 — 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗。



總結

您可以檢視結果。 在各別掃描任務的 內容視窗，報告檔案會自動儲存在 掃描日誌頁面。

重要
您的系統可能被要求重新啟動，令安裝精靈完成您的安裝程序。

按下 離開 去關閉視窗。

BitDefender 可能無法解決某些問題

在大部分的情形中，BitDefender 能夠成功地消毒被感染的檔案或是將之隔離。 然而，可能有極少部分的問題無法被解決。

在這種情況下，我們建議您聯絡BitDefender 在網頁www.bitdefender.com的支援小組。 我們的技術支援代表將會協助您解決您遭遇的問題。

BitDefender 偵測到密碼保護的物件

被密碼保護的目錄通常包含兩個種類：資料封存以及安裝程式檔。 通常它們不會是真正的安全威脅，除非內含被感染的物件而且被執行。

確定這些項目是無害的:

- 將被密碼保護的資料封存解壓縮，進行對內容物件的掃描。 在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2008。
- 假如被密碼保護的是安裝程式檔，請確認您的即時防護 是被啟用的，再執行。 如果安裝程式受到感染，BitDefender 將會將它隔離。

假如您不希望這些檔案再次被BitDefender掃描，您可以將這些檔案加入例外清單。想增加例外掃瞄，按下設定來開啟管理主控台然後到病毒防護；及例外。 請參照 被排除掃描的物件，獲得更多資訊。

BitDefender 偵測到可疑的檔案

可疑的檔案是被探索式分析歸類被潛在的、沒有正式發布惡意程式碼所感染的檔案。

如果偵測到可疑的檔案，您會被要求將可疑的檔案遞交給BitDefender Lab。 點擊好將這些檔案送交BitDefender Lab做進一步的分析。

8.2.6. 檢視掃描日誌

當任務結束時，在任務按下滑鼠右鍵並選擇檢視任務日誌，您可以檢視掃描結果。 以下視窗將會顯示:

掃描日誌

在此您可以檢視被執行過的任務報告。

在這裡您可以看到掃描任務被執行時，每一個時間所產生的報告檔案。當掃描被執行及掃描任務完成時，每個檔案會包含它的詳細資訊，清除/受感染、日期及時間等訊息。

有二個按鈕是可用的：

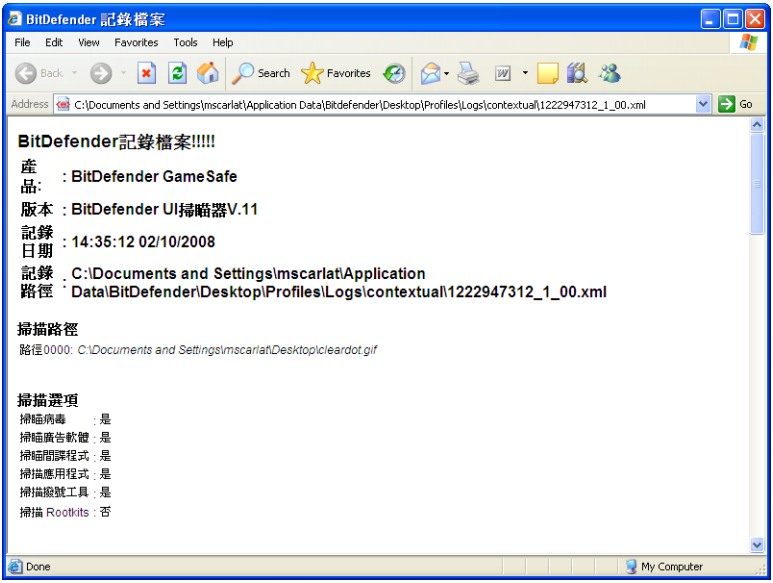
■刪除日誌 — 刪除選擇的掃瞄日誌；
■顯示日誌 — 檢視選擇的報告日誌； 掃描報告將用您的預設瀏覽器開啟。

注
在檔案上按下右鍵也可以執行檢視/刪除的動作。

按下 確定 要保存變動和關上視窗。 進行任務，正義點擊掃描 。

掃描日誌範例

下表呈現一個掃描日誌的範例：



掃描日誌範例

掃描日誌包含了詳細的資訊，例如：掃描項目、掃描目標、發現的威脅與所採取的行動。

8.3. 被排除掃描的物件

當您可能需要掃描時，某些檔案會被排除。 例如，您可以要EICAR存取測試掃描或 .avi 檔案在要求時掃描。

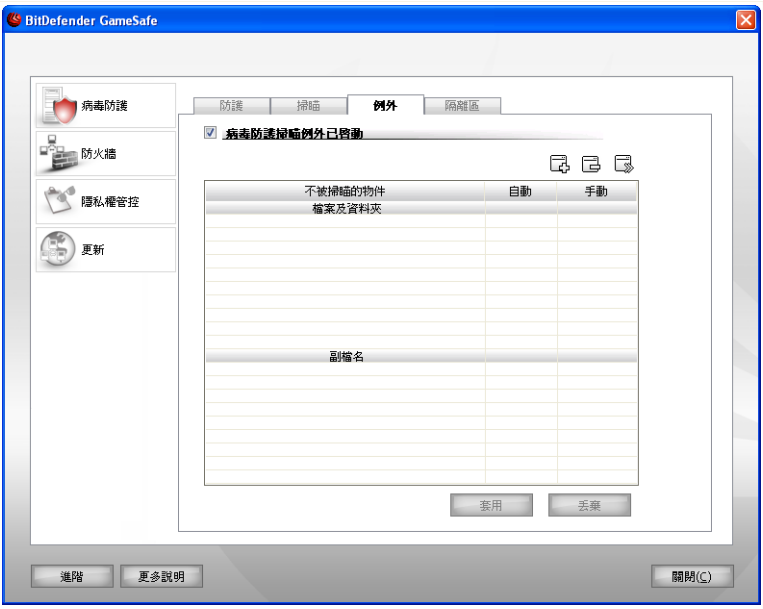
BitDefender 允許您排除物件不被掃描，如此可以減少掃描所花費的時間以及減少對您工作的影響。

兩種能夠被排除掃描的物件：

■路徑 — 排除掃描所有在指定路徑下的檔案與資料夾。
■副檔名 — 排除掃描所有特定副檔名的檔案。

注
所有被自動掃描排除的物件將不會被掃描，無論您是否有執行。

要管理被排除掃描的物件，請在管理主控台按下病毒防護>例外。 以下視窗將會顯示:



指定例外

您可看見被排除掃描的物件。在每個物件上您可以看見它是被哪一種掃描類型排除。

注
在此，被指定的副檔名將無法使用右鍵選單掃描。

要移除項目，選擇並點擊 刪除鈕。

要編輯項目，只需選擇並點擊 編輯 按鈕或者連續按二下。 一個新的視窗將會出現，您可以在此編輯要被掃描排除的副檔名或是路徑，您也可以在此設定需要排除的掃描類型。編輯完成後，請點擊確定。

注
您也可以在物件上按下右鍵，使用右鍵功能表編輯。

在您尚未按下套用之前，可點擊 拋棄 ，回復尚未儲存的設定。

8.3.1. 被排除掃描的路徑

從掃描要排除捷徑，點擊 增加 按鈕. 一個調整精靈將會出現，並且引導您完成設定

步驟 1/3 — 選擇物件類型

物件類型

選擇要被排除的路徑選項

按下 Next(下一步)。

步驟 2/3 — 指定要排除的路徑

排除的路徑

您可依照下列方式設定：

■按下 瀏覽，選擇要排除的檔案或資料夾並按下 加入。
■鍵入您要排除的路徑並點擊加入。

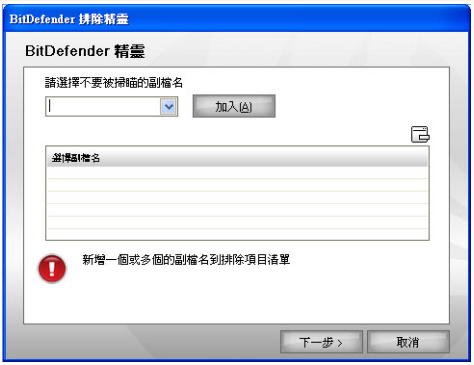
注
假如指定的路徑不存在或是出現錯誤訊息，點擊確定並檢查路徑的正確性。

當您加入路徑時，它會出現在表格中。

要移除項目，選擇並點擊 刪除鈕。

按下 Next(下一步)。

步驟 ./3 — 選擇掃描類型



掃描類型

您會看見一個表格包含有被排除的路徑與被排除的類型。

預設設定中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

按下 完成。

按下 套用 去儲存這個變更。

8.3.2. 被排除掃描的副檔名

要排除指定的副檔名，請按下 加入 按鈕。 一個調整精靈將會出現，並且引導您完成設定。

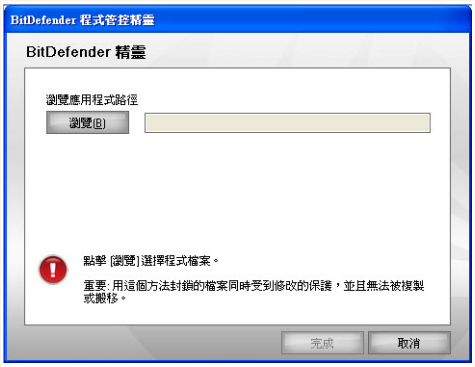
步驟 1/3 — 選擇物件類型

物件類型

選擇要排除的副檔名選項。

按下 Next(下一步)。

步驟 2/3 — 指定的要排除的副檔名



要排除的副檔名

您可依照下列引導執行設定：

■從選單中選擇要排除的副檔名並且按下加入。

注
選單包含您系統所有副檔名的清單。當您選擇任何一個副檔名，您可以看見簡述(若有)。

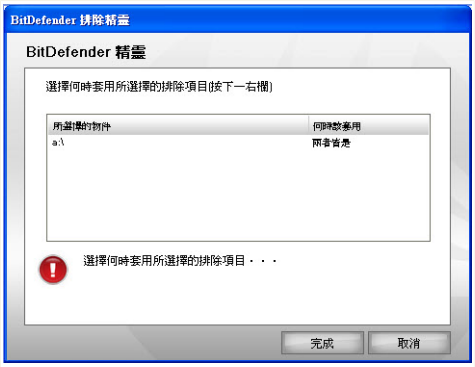
■在編輯欄內鍵入您想排除的副檔名，並點擊加入。

當您加入副檔名時，它會出現在表格內。

要移除項目，選擇並點擊 刪除鈕。

按下 Next(下一步)。

步驟 ./3 — 選擇掃描類型



掃描類型

您會看見一個表格包含有被排除的副檔名與被排除的類型。

預設設定中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

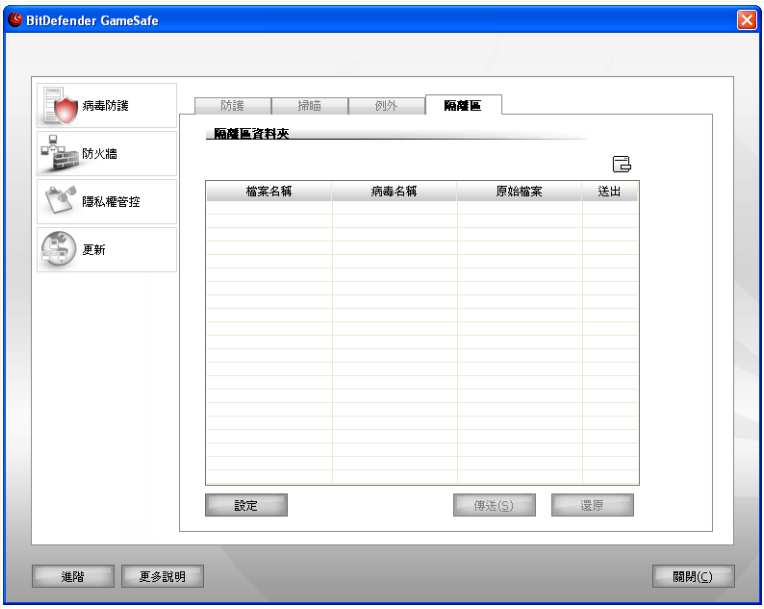
按下 完成。

按下 套用 去儲存這個變更。

8.4. 隔離區

BitDefender 允許隔離受感染或可疑檔案到一個被防護的區域，名為隔離區。將這些檔案隔離在隔離區裡，會減少感染擴散的風險，同時，您也可以寄送這些檔案到 BitDefender 實驗室。

在管理主控台點擊病毒防護>隔離區，便能調整設定並管理被隔離的檔案。



隔離區

8.4.1. 管理被隔離的檔案

您會注意到，在 隔離區 頁面包含所有被隔離檔案的清單。每個檔案包含它的檔名、大小、被隔離的日期及遞交的日期。如果您想要知道更多關於隔離檔案的資訊，請按下 更多說明。

注
當病毒在隔離區中，它不能造成任何的危害，因為它們無法被執行或讀取。

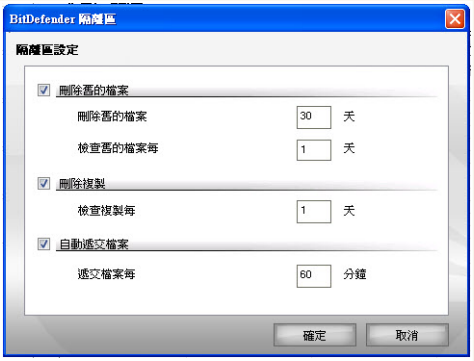
從隔離區選擇要刪除的檔案，按下 移除 按鈕。如果您想要還原所選擇的檔案到它原始的位置，請按下 還原。

從隔離區，您可以寄送任何選擇的檔案到 BitDefender 實驗室，按下 寄送。

右鍵選單. 右鍵選單能夠讓您容易地管理隔離區。您可以選擇重新整理 更新隔離區內的項目。

8.4.2. 隔離區設定

要調整隔離區設定，按下 設定。 一個新的視窗將會開啟。



隔離區設定

您可以直接設定BitDefender執行下列動作：

刪除舊的檔案。. 要自動刪除舊的被隔離檔案BitDefender，請選擇對應的項目。 您必須設定要刪除幾天以前被隔離的檔案，以及BitDefender 檢查舊檔案的頻率。

注
預設上，BitDefender會每天檢查一次並自動刪除十天以前的舊檔案。

刪除複本。. 如果您想稍後才建立新的帳戶，請選擇合適的項目。 一定要指定每隔幾天再檢查複本。

注
BitDefender 預設每天檢查離區中重複的檔案。

自動遞交檔案。. 如果您要自動遞交被隔離的檔案，請選擇合適的項目。 您必須指定遞交檔案的頻率。

注
BitDefender 預設每60分鐘一自動遞交被隔離的檔案。

按下 確定 儲存這個設定並關閉視窗。

9. 防火牆

防火牆 保護您電腦免於內送及外送的未授權連線威脅。它就像是進出口的警衛 — 它會保持注意您的網際網路連線，並追蹤誰可以存取網際網路，誰被阻擋存取。

注
如果您有寬頻或DSL連線，防火牆是必要的。

防火牆模組過濾網路傳輸並控制應用程式連線到網際網路的存取權限。在隱匿模式下，您的電腦將會「匿蹤」 避免暴露於惡意軟體及駭客的威脅之下。防火牆模組有能力可以自動偵測並防範連接埠掃描 (一連串的封包傳送到一部機器，以找出「進入點」，通常是攻擊前的準備工作)。

這個使用者手冊中的 防火牆 手冊包含了以下的主題：

- 防火牆洞察力
- 防火牆狀態
- 傳輸防護
- 進階設定
- 防火牆活動
- 網路區

9.1. 防火牆洞察力

BitDefender防火牆的設計是提供最佳的保護為您的網路/網際網路連接，您不必設定它。 如果您直接地連接到網路，到一個唯一網路或到幾個網路(乙太網路、無線、VPN或者其他網路類型)，或信任或不信任，防火牆不會自己配置適應對應的情況。

系統預設情況下， BitDefender在您的電腦自動查出網路分佈，並且它創造適當的基本的防火牆設定檔。 它也補充網路到設定檔作為被信任的或不信任的網路區域，根據他們的配置。

9.1.1. 什麼是防火牆設定檔？

防火牆設定檔是控制應用的網路/網際網路存取

根據網路分佈在您的電腦， BitDefender自動地建立設定檔。 創造的基本設定檔包含網路存取規則或基本的網路存取規則，必需由系統應用程式和BitDefender元件。

注
單一防火牆設定檔已建立，不管您連接網路的數量。

基本的設定檔有三個類別：

設定檔	描述
直接連線	包含允許基本存取網路的網路進入規則。 這規則不允許網路用戶存取您的電腦或您瀏覽網路。
不信任的	包含與不信任的網路相關的存取規則。 這規則允許您瀏覽網路，但防止其他網路成員進入您的電腦。
信任的	包含信任的網路相關的存取規則。 沒有限制規定強加給網路存取。 意指您得以進入對網路分享、網路印表機和其他網路資源。 同時，網路成員能連接到您的電腦和進入您的分享。

當應用程式嘗試連接到網路，規則將會適本地新增到設定檔。 在系統預設情況下您能選擇允許或拒絕規則尚未配置的應用程式存取網路，或者只允許預設的白名單應用程式。

注
為設定第一次連接到網際網路的應用要指定通入策略，去 狀態 區分並且設置保護層級。 要編輯已存在的設定檔，到 傳輸 頁面，並點擊 編輯設定檔 選項。

9.1.2. 什麼是網路區域？

網路區域代表一台電腦在網路裡或完全被隔開您的電腦的一個整個網路或，相反，可能查出您的電腦和連接到它。 實際上，區域是IP地址或允許或對您的電腦被否認通入IP地址的範圍。

在系統預設情況下， BitDefender自動地增加區域為網路具體分佈。 區域存取創造一個適當的網路存取規則增加，可適用於一個整個網路，在當前的設定檔。

區域類別有兩種：

區域類型	描述
信任的區域	電腦從一個信任的區域可以連接到您的電腦，並且您能連接到它們

區域類型	描述
	所有試圖連接是來自這些區域，以及所有連接企圖從您的電腦到這些允許區域。 如果增加網路作為一個信任的區域，您得以進入網路分享、無限制的網路印表機和其他網路資源。 並且，網路成員能連接到您的電腦和進入您的分享。
非信任的區域	電腦從一個不信任的區域無法連接到您的電腦，並且您不可能連接到它們。 所有試圖連接是來自這些區域，以及所有連接企圖從您的電腦到這些區域被阻攔。 當ICMP交流被否認，並且秘密行動方式起動，您的電腦幾乎看不見在電腦那個區域。

注

要編輯區域，到區域頁面 要編輯所對應區域的規則，到 傳輸 頁面，並點擊 編輯設定檔 選項 。

9.1.3. 防火牆作業

當安裝之後重新起動系統時， BitDefender自動地查出您的網路分佈，創造適當的基本的設定檔並且根據偵測到的網路新增區域。

注

如果您直接地連接到網際網路，網路區域沒有建立對應的網路分佈。 如果您被連線到超過一個網路，各自根據網路增加區域。

每次網路分佈改變，您是否連接到另一個網路或您使網路失去連接能力，已建立新的設定檔防火牆。 同時，相應地修改網路區域。

當新的防火牆設定檔建立時，舊的設定檔會被保存，因此，當您回到它對應的網路分佈時，它可以再次被讀取。

根據網路分佈， BitDefender將相對應地自行配置。 這是系統預設情況下如何配置BitDefender防火牆：

■如果您直接連接到網際網路，不論您是否被連結到其他網路，一個直接連接設定檔會被建立。 否則， BitDefender會建立不信任的防火牆設定檔。

注

由於安全考量，信任的設定檔沒有在系統預設的情況下建立。 要建立被信任的設定檔，首先您必須重設已存在的設定檔。要了解更多，請參閱"修改設定檔" (p. 93)。

■根據網路設置加入區域。

區域類型	網路調整
信任的區域	個人IP沒有沒有閘道 -電腦是一個區域網(LAN)的一部分和不連接到網際網路。 這樣情況的例子是建立一個家庭網路允許家庭成員分享檔案、印表機或者其他資源。
	個人IP有網域控制器偵測 -電腦是LAN的一部分並與一個網域連接。 這樣情況的例子是一個能夠允許用戶分享檔案或其他資源在一個網域裡面的辦公室網路。 網域意指一組電腦成員所使用的規範。
非信任的區域	開放的無線連線 — 電腦是無線區域網路的一部分。 這樣情況的例子是，當您從一個公共場所的自由存取點存取網際網路。

注

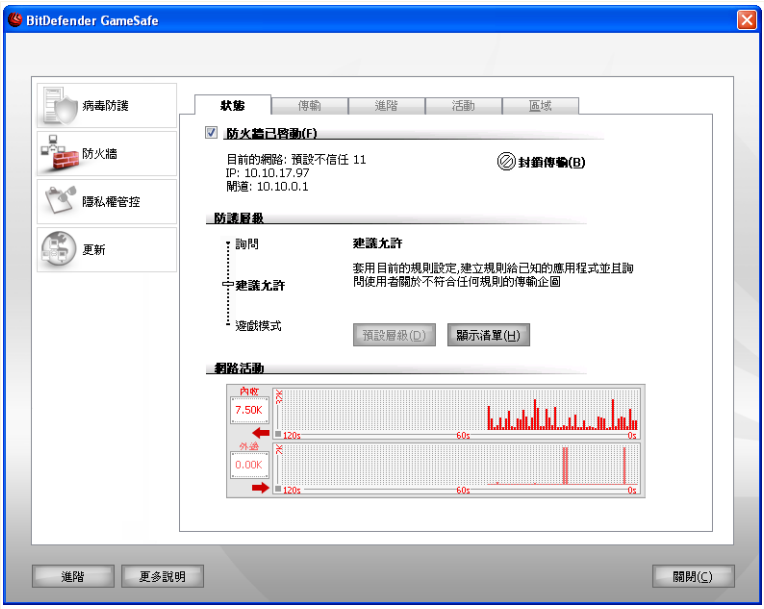
區域不是為了某些建立網路而結構，例如:

- 公開的IP位址電腦是直接連線到網際網路
- 私人IP用戶，但沒有查出區域控制器 - 電腦是LAN的一部分，一部分沒有是區域的，並且它連接到網際網路存取用戶。 例如一個如此的情形，一個讓使用者分享檔案或其他的資源的學校校園網路。

■隱藏模式已啟動。
■VPN和遠端的連接被允許
■網際網路連線分享不被不信任的區域允許。
■應用程式列入白名單會自動地被允許存取,然而其他應用程式您將被要求許可，當他們第一次嘗試連接網路。

9.2. 防火牆狀態

要配置防火牆防護，點擊防火牆>狀態 在管理主控台。 以下視窗將會顯示:



防火牆狀態

在這個頁面您可以啟動/停用 防火牆，阻擋所有網路/網際網路傳輸，並設定預設的對應的行動當新的事件發生時。

重要
防護您的系統以抵抗網際網路的攻擊，請保持 防火牆 啟動。

要阻檔所有網路/網路傳輸按下 封鎖傳輸及確定確定您的選擇。 您的電腦在網路將與其他電腦隔絕。

要解封所有網路/網際網路傳輸，只需按下 解封傳輸 。

在部分的下端您能看BitDefender統計關於進入和退出的傳輸。 圖表顯示傳輸網路容量在前二分鐘期間。

注
這個圖形會出現，甚至在 防火牆 已停用的時候。

9.2.1. 更改防護層級

您可以選擇最適合您安全需求的防護等級。拖曳滑桿設定合適的防護層級。

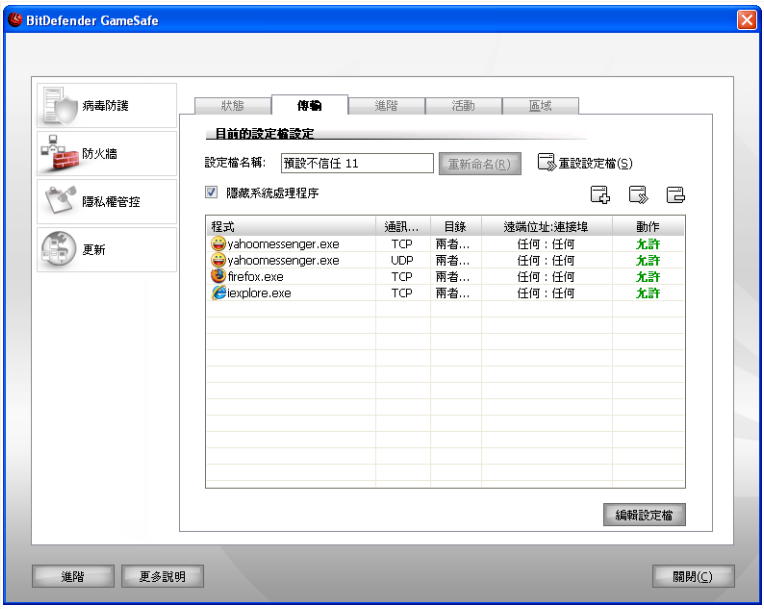
有三種防護層級：

防護層級	描述
遊戲模式	套用目前的規則並且不用提示就允許所有與目前規則不相符的傳輸試圖。 這個做法強烈不建議使用者設定，但它也許對網路系統管理者或是遊戲玩家是有用的。
允許建議的	套用目前規則並且允許所有由BitDefender合法的程式(whitelisted)外傳的連接企圖從，無需提示。 其餘連接企圖， BitDefender將請求您的允許。 當他們在建立您能看傳輸規則傳輸 部分 白名單的程式是世界通用常見的應用程式。 包含已知的網路瀏覽器，多媒體播放器，聊天和檔案共享的程式，以及伺服器客戶端和作業系統的應用程式 如果您想要檢視哪些程式列為白名單，按下 顯示白名單。
詢問	如果傳輸企圖並沒有符合目前規則，則先詢問使用者是否應該被允許。

按下 預設層級 設定預設的層級（允許所有的白名單）。

9.3. 傳輸管控

要處理目前的設定檔防火牆規則，按下防火牆> 傳輸在管理主控台。 以下視窗將會顯示:



傳輸管控

在這個頁面，您可以在建立的規則裡，利用特定的通訊協定、連接埠、應用程式或遠端的位址，針對內送或外送的連線，設定允許或拒絕。

規則可以自動輸入（透過警示視窗）或手動（按下 新增 按鈕，並選擇規則的參數）。

9.3.1. 自動地新增規則

當 防火牆 啟動時，每當要存取網際網路的連線時，BitDefender 將徵求您的同意：

防火牆警告

您可以檢視以下的訊息：哪些應用程式嘗試存取網際網路，透過什麼通訊協定、IP 位址及 連接埠在哪個應用程式正在嘗試連接。。

按允許允許所有通道(進入和退出)引起這種應用地方到任何目的地，在各自IP通訊協定和在所有連接埠。 如果您按下封鎖，應用程式將會被完全否認在分別的 IP 記錄上的通訊協定接觸網際網路。

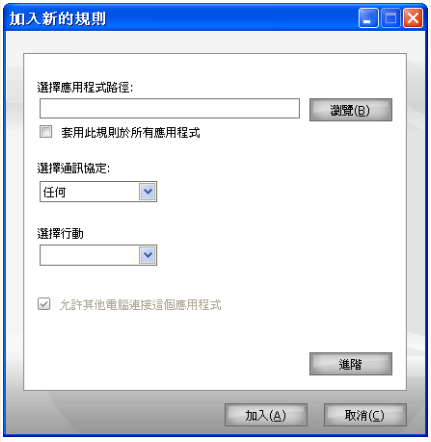
基於您的答案,規則將在桌面建立， 應用以及列出。 之後應用程式試著連接,這一條規則將被預先設定地應用。

重要

只有允許您絕對信任的 IP 位址或網域進行內送的連線企圖。

9.3.2. 手動新增規則

按下 新增規則 按鈕，並選擇規則的參數。則會出現以下的視窗： 以下視窗將會顯示:



新增規則

若要增加新的防火牆規則，遵從這些步驟:

1. 選擇應用程式新的防火牆，便會建立規則

   選擇應用程式，按下瀏覽器，，放置它和按確定.

   如果您要建立一個規則並套用到全部的應用程式，只要選擇　套用此規則到全部的應用程式。
2. 選擇通訊協定將適用於指定的記錄。

   一個常用的通訊協定清單可用，以協助您選擇特定的通訊協定。選擇需要的通訊協定(或規則所要套用的)　從相對應的下拉式選單或選擇　任何　去選擇所有的通訊協定。

   下列的表格列出您能選擇通訊協定與簡述:

通訊協定	描述
ICMP	網際網路控制訊息通訊協定 - 延長對網際網路通訊協定 (IP).ICMP 支援包含錯誤，控制和資訊的訊息。PING　指令，舉例來說，使用 ICMP 測試一個網際網路連接。

通訊協定	描述
TCP	傳輸控制通訊協定 - 傳輸控制協議使二個系統能夠建立連接和資料的交流地方。 傳輸控制協議保証在他們送出的相同次序中被傳送資料以及保證他的傳送。
UDP	使用者 Datagram 通訊協定 - UDP 是為高表現設計以 IP 為基礎的運輸系統。遊戲和其他的以錄影帶為基礎的應用程式使用 UDP 。

3. 從所對應的選單來選擇規則的動作。

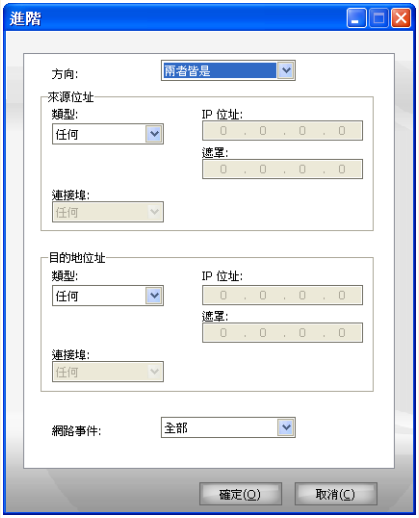
動作	描述
允許	指定的應用程式將被允許在指定的環境下的網路 / 網際網路存取。
拒絕	指定的應用程式將被拒絕在指定的環境下的網路 / 網際網路存取。

4. 如果先前選擇的通訊協定是TCP或者 UDP,當它擔任一個伺服器的時候，您能指定規則是否套用於應用程式。

   按允許其他電腦連接到此應用程式 套用行動到所有的網路活動。 您允許或者拒絕這個應用程式開啟連接阜。

   如果您想要為 UDP 和接通和應用只有到接通; 連接為傳輸控制協議，分別清除對應的核取方塊。

您可以按下 進階，假如您要進行更進一步的調整。一個新的視窗將會出現可讓您選擇:



進階規則設定

您可以進行下列調整：

■方向 — 選擇傳輸的方向。

類型	描述
外送	這個規則只套用到外傳的傳輸內容。
內送	這個規則只套用到內送的傳輸內容。
兩者皆是	這個規則套用到進出二個方向。

■來源位址 — 指定來源的位址。

記載來源位址，選擇來自選擇單的位址類型而且記載必需的資料。 以下的選項是可用的：

類型	描述
任何	這個規則套用到任何的來源位址。

類型	描述
系統	這個規則只套用到特定的來源主機位址。 您一定要在系統的 IP 位址中輸入
網路。	這個規則只套用到特定的網路來源。 您一定要在 IP 位址和網路遮蓋中輸入。
本地主機	這個規則只套用到來源是本地主機。 如果您使用超過一個網路界面，來自選擇單的選擇規則適用於您的網路界面。 如果您想要適用規則於所有的地方系統，選擇任何.
本地網路	這個規則只套用到來源是本地網路。 如果您被連接到超過一個網路，從選單選擇適用規則套用於您的網路。 如果您想要套用規則於所有的本地網路，選擇任何.

如果您已經選擇傳輸控制通訊協定或 UDP通訊協定，您能設定一個特定的連接阜或範圍在 0 和 65535之間. 如果您想要的規則適用於所有的連接阜,選擇任何.

■目的地位址 — 指定目的地位址。

記載網域位址，選擇來自選擇單的位址類型而且記載必需的資料。 以下的選項是可用的：

類型	描述
任何	這個規則套用到任何的目的地位址。
系統	這個規則只套用到是特定主機的目的地。 您一定要在系統的 IP 位址中輸入
網路。	這個規則只套用到特定網路的目的地。 您一定要在 IP 位址和網路遮蓋中輸入。
本地主機	這個規則只套本地主機的目的地。 如果您使用超過一個網路界面，來自選擇單的選擇規則適用於您的網路界面。 如果您想要適用規則於所有的地方系統，選擇任何.
本地網路	這個規則只套用到本地網路的目的地。 如果您被連接到超過一個網路，從選單選擇適用規則套用於您的網路。 如果您想要套用規則於所有的本地網路，選擇任何.

如果您已經選擇傳輸控制通訊協定或 UDP通訊協定，您能設定一個特定的連接阜或範圍在 0 和 65535之間. 如果您想要的規則適用於所有的連接阜,選擇任何.

■網路事件 - 如果您已經選擇傳輸通訊協定或作為通訊協定的 UDP，選擇規則套用於的網路事件。

按下 確定 去關閉視窗。

點擊建立新的設定檔 並依循精靈去建立一個基本的防火牆規則。

9.3.3. 管理規則

您可以在表格中檢視設定檔規則清單。

選擇勾取相對應的核取方塊 隱藏系統程序 去隱藏關於系統的規則或 BitDefender 程序。

規則是以優先順序由上而下排列。按下 編輯設定檔 進入 詳細的檢視 畫面，在那裡您可以移動上下來改變規則的優先順序。

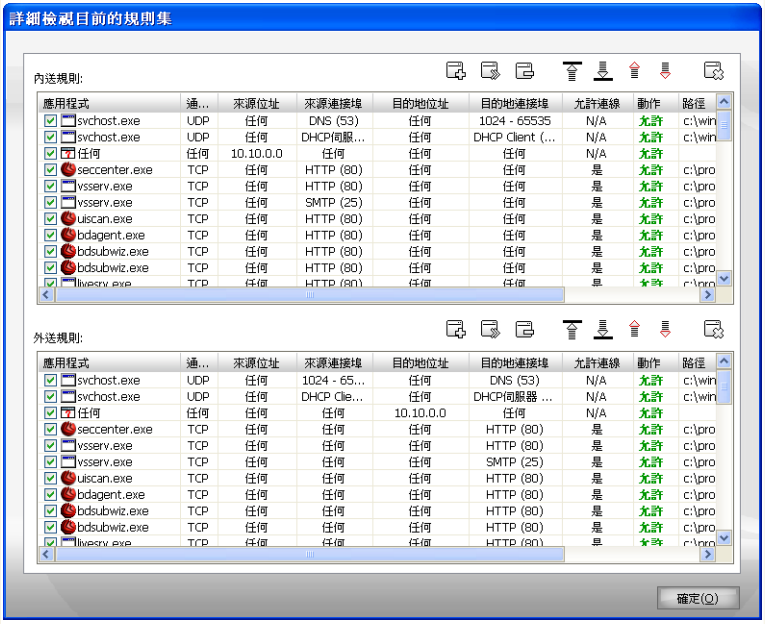
要刪除規則，選擇並按下 刪除規則按鈕。

要編輯一個規則，只需點選規則並按下 編輯規則 按鈕或者連續按二下。以下的視窗即會出現：

注
右鍵選單也可以使用，它包含以下的選項：新增規則、刪除規則 及 編輯規則。

9.3.4. 修改設定檔

您可以按下 編輯設定檔 修改一個設定檔。以下的視窗將會出現：



詳細的檢視

規則被分成二個頁面：內送規則及外送規則。您可以檢視每條規則的應用程式及參數(來源位址、目的位址、來源連接埠、目的連接埠、動作等)。

要刪除一個規則，只要選擇它並按下 刪除規則 按鈕。要刪除所有規則，按下 清除清單 按鈕。要修改一個規則，同樣選擇它並按下 編輯規則 或者在規則上按二下。如果只是暫時取消規則，不需刪除它，只需取消核取方塊。

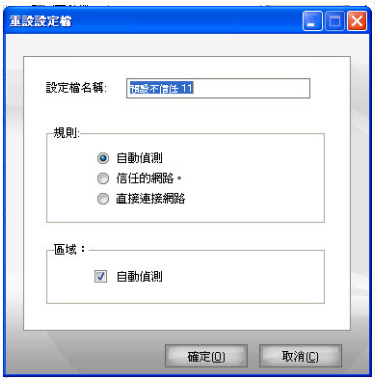
您可以增加或減少規則的優先順序。在選擇的規則上，按下 上移 按鈕增加優先順序或按下 下移 按鈕減低其優先順序。 要將一個規則設為最高優先權，點擊 優先移動 按鈕。 要將規則設為最低優先權，點擊 最後移動按鈕。

注
一個右鍵選單可用，它包含以下選項：新增規則、編輯規則、刪除規則、上移、下移、優先移動、最後移動及 清除清單。

按下 確定 關閉視窗。

9.3.5. 修改設定檔

先進的使用者可能選擇再配置防火牆設定檔，若要將防火牆保護最佳化或者依照他們的需要制定它。 要重設防火牆設定檔，您可以按下 重設設定檔。 以下視窗將會顯示:



重新設定設定檔

您可以進行下列調整：

■設定檔名稱 — 輸入新的名稱。
■規則 —指定要建立給系統應用程式的規則類型。

以下的選項是可用的：

選項	描述
自動偵測	讓 BitDefender 偵測網路設置並且建立適當的基礎規則。
信任的網路	建立一個信任的網路區域網路的規則。
直接網際網路連線	為網際網路建立一組適當的規則。

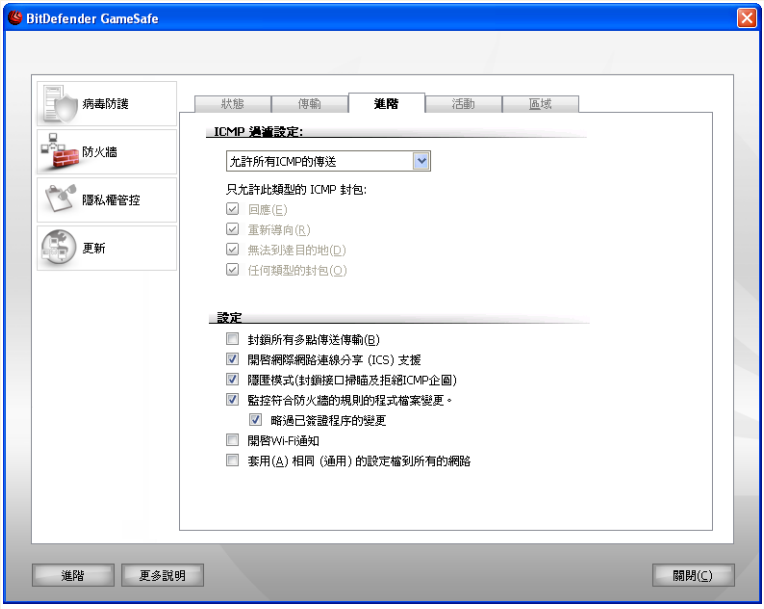
■區域 - 按自動偵測讓 BitDefender 於偵測到的網路建立適當的區域

按下 確定 去重設設定檔並關閉視窗。

重要
如果您選擇重新設定網路設定檔，則您在這頁所增加的規則都將會消失。

9.4. 進階設定

若要配置 BitDefender 防火牆的先進設定,按下 防火牆l>進階在管理主控台。 以下視窗將會顯示:



進階設定

在這個頁面，您可以調整防火牆的進階設定。 在這個頁面，您可以設定 BitDefender 防火牆進階選項。這個進階選項可以允許您針對 ICMP 傳輸指定過濾規則（ICMP 過濾器設定） 以及封鎖廣播的傳輸封包、分享您的網際網路連線、讓您的電腦遠離惡意程式及駭客（設定）。

9.4.1. ICMP 過濾器設定

從這個選單，您可以選擇以下其中之一的對策，去過濾 ICMP 傳輸內容：

■允許所有 ICMP 傳輸 — 允許所有 ICMP 傳輸。
■封鎖所有 ICMP 傳輸。
■自訂 ICMP 過濾 — 自訂過濾 ICMP 傳輸。您可以設定以下的選項： 您能夠選擇哪一類的 ICMP 允許包裝。

以下的選項是可用的：

選項	描述
回應	這個選擇能使回聲回復和回聲請求消息。 回聲請求是寄發資料到主人的ICMP消息並且期待在回送的資料回聲回復。 主人必須反應所有回聲請求以包含確切的資料的回聲回復被接受在請求消息。 回聲回復是ICMP消息引起以回應ICMP回聲請求消息，並且對所有主人和網路器是必須的。
重新導向	這是通知一個主人更改它的網路選擇信息方向的ICMP消息(送小包在一條變更進路)。 如果主人設法存取網路器(R1)送資料另一個網路器(R2)然後到達主人，並且一個直接方式從主人到R2是可使用的，改方向將通知主人路線。 網路器更將先進的資料圖意欲的目的地。 然而，如果資料圖包含路由選擇信息，不要傳送這信息，即使一條更好的路線是可使用的。
無法到達目的地	這是被網路器產生告知客戶的一個 ICMP 訊息目的地主人是無法到達的,除非 datagram 有一個多點廣播住址。 這一個訊息的理由可能包含和主人的組織不存在有關聯 (距離是無限), 被指出的通訊協定或者不積極的連接埠, 或資料一定要被不完整的 '完整'的旗子是開的。
其他封包類型	當這個選項啟動時，則其他封包 回應、無法到達目的地 或 重新導向 都將存取。

9.4.2. 進階的防火牆設定

以下的進階防火牆設定是可用的：

■阻擋所有的導向 - 降低收到的任何的多點廣播包裹

多點傳送傳輸是種位在一個網路之中的特別群組傳輸。 封包被傳送到一個特別地址，在那裡多點傳送客戶能接受他們，如果他們同意的話。

例如，一個擁有TV-tuner的網路成員可能廣播（送到每個網路成員）或者多點廣播(送到一個特別的位址)影像串流。 接收多點廣播位址的電腦能接受或者拒絕封包。如果接受,影像串流能被多點廣播給客戶看。

過量的多點廣播導向消耗頻寬和資源。當這選項啟動，任何接受多點廣播封包的數量將會降低。 然而，我們不建議這選擇。

■啟動網際網路連線分享(ICS) 支援能支持網際網路為連接分享(ICS)。

注
這個選項不會自動地在您的系統允許ICS，但您可以從作業系統設定允許這個連結型態。

網際網路連線分享(ICS) 允許區域網路電腦透過您的電腦存取到網際網路。當您處於一個特別的網際網路連線(如：無線網路)時，您可以透過這種方式，分享網際網路的連線給區域網路內的其他電腦。

與本地區域網路的成員分享您的網際網路連接導致一個比較高度層級的資源消費而且可能包含特定的風險。 它也在一些您的區域（被正在使用您的網際網路連接的那些成員打開)。

■隱形模式 — 讓您的電腦遠離惡意程式及駭客。

透過連線到連接埠，看它是否有任何回應，是一個簡單發現您電腦是否有存在弱點的方法。這就稱為連接埠掃描。BitDefender 會自動地偵測並封鎖連接埠掃描。

不懷好意的駭客及惡意程式會試圖找出存在於網路上的電腦，以進行各種惡意的破壞。隱匿模式的功能可以讓您的電腦停止回應這類試圖找出開啟連接埠的企圖，以避免被有心人士發現。

■監控符合防火牆規則的程式檔案變更 - 檢查每一個試圖連接到網際網路的應用程式看是否有變更，自從控制存取的規則被新增。 如果應用程式被變更，警告將提醒您允許或阻檔應用程式存取網際網路。

通常，更新改變會應用程式。 但是，在網路也許有被風險被惡意程式變更應用程式，目的為感染您的電腦和其他電腦。

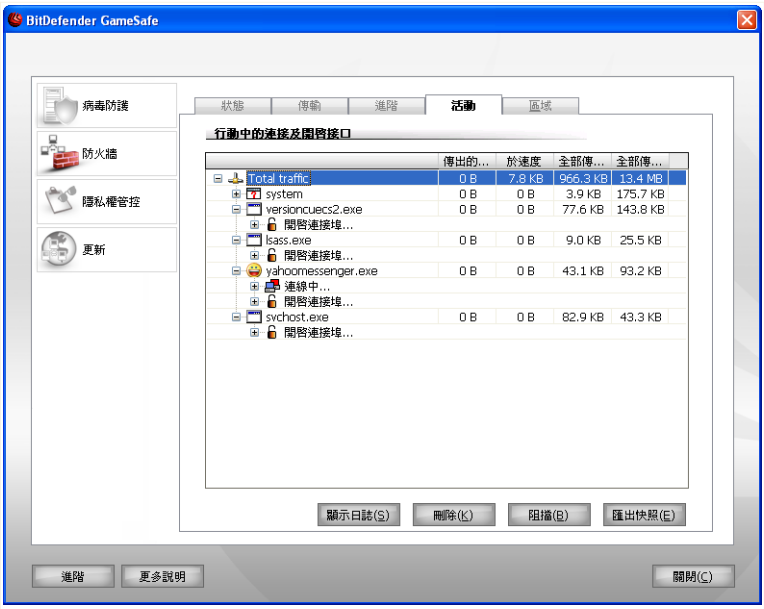
注
我們建議您這選擇此選項並且在控制他們的存取規則被建立之後，只允許存取變更你希望的應用程式

被作記號應用程式應該被信任並且有高度安全 您可以檢查略過已記號程序的變更為了允許當改變過的被記號應用程式連接到網際網路時，您無需因此被警告。

- 啟動Wi-Fi通知 -使用Wi-Fi通知。
- 套用相同的設定檔到全部的新網路- 建立預設值（一般的）防火牆設定檔，命名 一般的網路，當一個新的網路被偵測到時加以套用。 如果您回去一個有防火牆設定的舊網路設定時，防火牆設定檔將會被載入並取代一般設定檔。

9.5. 連線管控

要監控目前以應用程式分類的網路/網際網路活動(TCP和UDP)並且打開BitDefender防火牆日誌，在管理主控台按下防火牆>活動 。 以下視窗將會顯示:



連線管控

您能見到以應用程式分類的所有傳輸。 對每個應用程式，您能看見它的連結與開啟的連接埠口;外傳與內送的傳輸速度與資料送 /收到的全部數量。

視窗即時地呈現目前的網路 / 網際網路活動. 當連接或埠口被關閉, 您能見到對應的統計資料漸漸微暗最後消失。 同一件事發生到全部統計所對應的高傳輸或是開啟埠口的應用程式並且也被您關閉。

點擊 阻擋 建立限制傳輸的規則。您將會被要求確認您的選擇。這個規則在 傳輸 頁面都可以在未來進行調整。

注
當您要阻擋應用程式或是網路連線，請按下滑鼠右鍵，並選擇阻擋。

按下 終止 來結束所選擇的處理程序。 您將需要確認您的選擇。

注
要終止一個程序，請按下滑鼠右鍵，並選擇終止。

按下 匯出快照 去匯出清單到一個 .txt 為副檔名的檔案。

一個完整名單關於防火牆用法(開始或停止防火牆，傳輸阻擋，使用隱匿模式，修改設置，應用程式設定檔)或由它偵測的活動引起(掃描區域，阻擋連接企圖或交通根據規則)檢查可以存取點擊"展示 . BitDefender>防火牆。 檔案位於當前視窗用戶的普通檔案資料夾，在道路之下：...BitDefender \ BitDefender防火牆\ bdfirewall.txt。

9.6. 網路區域

區域是由一個 IP 位址或者多個 IP 位址的一條特別規則被建立入設定檔。 規則或允許網路成員無限制地接觸您的電腦 (信任的區域) 或者, 在相反者上，完全地隔離來自網路電腦 (不信任的區域) 在您的電腦.

預設上，BitDefender 自動偵測您已連接到的網路並新增新的網路區域取決於網路設置。

注
如果您連接到一些網路相信他們的結構,那您可能會增加超過一個區域。

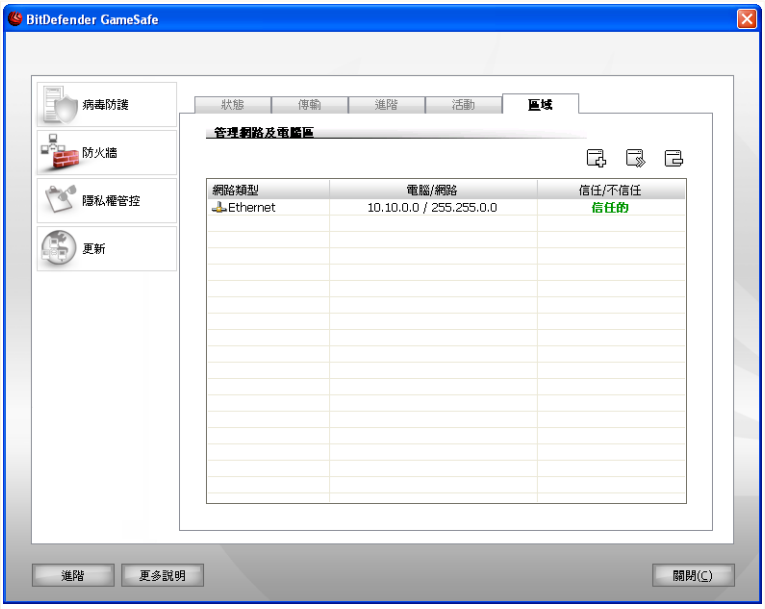
被信任的區域為下列的網路結構被預先設定增加:

■私人的 IP 沒用通道 - 電腦是一個本地的區域網路（區域網路）的一部份，而且它不對網際網路連接。
■個人IP有網域控制器偵測 -電腦是LAN的一部分並與一個網域連接。

不信任的區域預設上會被加入到下列的網路設置:

■開放的無線連線 — 電腦是無線區域網路的一部分。

要處理網路區域，在管理主控台按下防火牆>區域。 以下視窗將會顯示:



網路區域

您能看到網路區域對應於在表格列出的目前設定檔。您可看到每個區域的網路類型(網路，無線， PPP等等)，連到該區域的電腦或者網路，而該區域是否被信任或不被信任。

要編輯區域，只需點選並按下 編輯區域 按鈕或者連續按二下。以下的視窗即會出現。

注

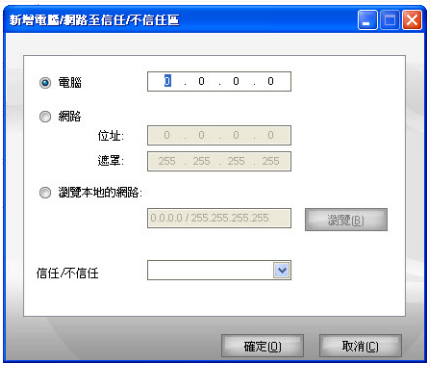
預設上， BitDefender 將開放無線網路加入為不信任的區域。 如果您與信任的電腦(在家或者與好友) 一起連接到一個開放的無線網路,您可能想要編輯相關的區域。 為了要能夠與其他網路成員分享資源，您一定要將該區域設定為信任的網路。

要刪除一個區域，按下 刪除區域 按鈕。

9.6.1. 新增區域

您能手動新增區域 舉例來說,這允許您與您的好友在一個開放的無線網路 (藉由新增他們的電腦到信任的區域) 分享檔案，或阻擋來自一個信任的網路電腦.(新增它到不信任的區域)

若要增加一個新的區域，按下 新增規則 按鈕啟動設定精靈。 以下視窗將會顯示:



增加區域

要增加區域，請依據這些步驟:

1. 指定一個來自本地網路或者一整個本地網路到您想要新增的區域。 您可以選擇以下方法的其中之一：
   - ■若要新增加一個指定的電腦，選擇電腦並提供它的 IP 住址。
   - ■若要新增加一個指定的網路，選擇 網路而且提供它的 IP 位址和遮罩 。
   - ■瀏覽本地的網路來尋找以及新增增加一部電腦或一個網路。

     若要瀏覽本地的網路，選擇 瀏覽本地網路 然後按下 瀏覽 新的視窗將出現。

從清單選擇您想要新增加到一個區域的電腦或者網路並按下確定
2. 從選單選擇您要建立的區域。 (信任或者不信任)
3. 按下 確定 來新增區域。

10. 隱私權管控

BitDefender 監視您的系統中多處可能受間諜程式攻擊的熱點，並檢查您的系統和軟體的異動。這是有效封鎖木馬程式及其他駭客安裝的工具程式，駭客會試圖竊取您的個人資料（如：信用卡號碼等）並寄送出去。

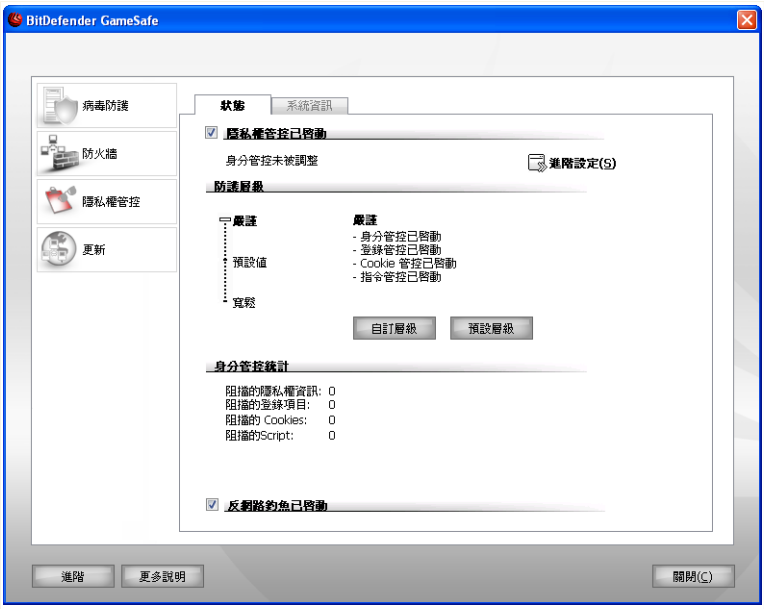
BitDefender 能夠掃描您正在瀏覽的網站，並提醒您是否有網路釣魚的威脅。

這個手冊中的 隱私權管控 頁面，包含以下主題:

- 隱私權管控狀態
- 進階設定 — 身分管控
- 進階設定 — 登錄管控
- 進階設定 — Cookie 管控
- 進階設定 — Script 管控
- 系統資訊
- 反網路釣魚工具列

10.1. 隱私權管控狀態

要調整隱私權管控，在管理主控台點擊隱私權管控>狀態。 以下視窗將會顯示:



隱私權管控狀態

10.1.1. 隱私權管控

重要
為了防止資料遭竊並保護您的隱私，請持續保持啟動 隱私權管控。

隱私權管控模組透過五個重要的防護控制保護您的電腦:

■身分管控 - 依據您在 身分 頁面建立的規則，對外的 HTTP 及 SMTP 傳輸內容都會先被過濾，以保護您的機密資料。

注
在頁底您可以看到 身分管控統計資料。

■登錄管控 — 當一個程式為了要能夠在開始功能表被執行而嘗試修改登錄項目時，先徵求您的同意。

■Cookie 控制 — 當一個新的網站嘗試設定一個 cookie時，先徵求您的同意。

■Script管控 — 當一個網站嘗試啟動一個 script 或其他內容時，先徵求您的同意。

要設定這些管控的內容，請按下 進階設定。

更改防護層級

您可以選擇最適合您安全需求的防護等級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

防護層級	描述
許可的	只有 登錄管控 是啟動的。
預設	登錄管控 及 身分管控 是啟動的。
嚴謹	登錄管控、身分管控 及 Scrpit管控 是啟動的。

您可以按下 自訂層級去自訂防護層級。 在出現的視窗中，選擇您要啟動的防護管控並點擊確定。

點擊預設層級，將滑桿定位在預設層級。

10.1.2. 反網路釣魚防護

網路釣魚是犯罪的行為，利用偽造電子郵件或網站作為誘餌，矇騙使用者洩漏個人機密資料，如：銀行帳戶密碼、信用卡號碼等。

大多數的案例，網路釣魚利用假以亂真的偽造網站或是假藉知名公司之名義發出大量電子郵件訊息設定檔。這些誘騙的郵件被送入目標受害者的信箱中，並期待有不知情的受害者上勾，提供個人的私密資料協助犯案。

網路釣魚信息通常都以您的線上帳戶相關事項為誘餌。它誘使您點擊相關連結進入偽造的網站，並要求您輸入相關的個人資料。您可能會被要求輸入：身分證號碼、銀行帳戶等。 有時，更狡猾的設計會假裝您的帳戶已被入侵，誘使您一定會點擊詐騙的連結。

網路釣魚也會利用間諜程式直接入侵您的電腦竊取資料。

網路釣魚攻擊的主要目標是針對線上付費服務的網站，像是：ebay、paypal，或是有線上帳戶功能的銀行。 最近，線上的社群網站也被列為網路釣魚的攻擊目標。

要防護您的系統抵抗網路釣魚的威脅，請保持 反網路釣魚 啟動。 如此，BitDefender將能掃描每個您要瀏覽的網站並且提醒您任何網路釣魚工具的出現。 您可以設定網站白名單，如此BitDefender將不會掃描這些網站。

使反網路釣魚保護和安全清單更容易管理，把BitDefender 反網路釣魚工具列整合到Internet Explorer 使用。 更多詳細的資料，請參閱 "反網路釣魚工具列" (p. 121)。

10.2. 進階設定 — 身分管控

保持機密資料的安全是個重要的議題。在網際網路的發展下，資料竊盜技術也隨之進步，它利用一些新的方法來騙取人們提供個人私密的資料。

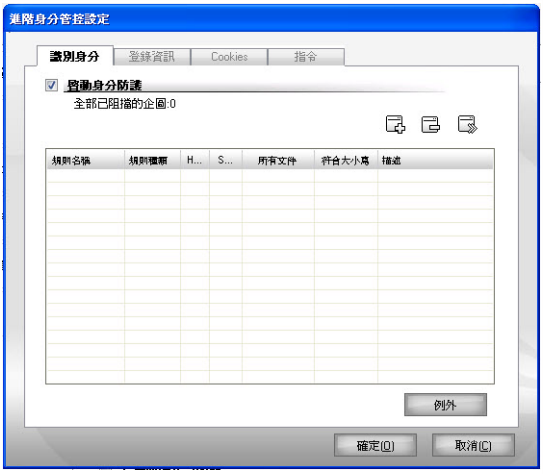
身分管控 協助您保持機密資料的安全。它會掃描 HTTP 或 SMTP 傳輸內容，對於您所定義的身分資料進行過濾。當有發現時，它將會阻擋該網頁及電子郵件。

多使用者支援，其他使用者不會看見您在電腦上做的調整。

每個隱私權規則都可以在 身分 頁面以供未來的調整。 要進入此頁面，開啟進階隱私權管控設定視窗，並點擊 身分標籤。

注

要開啟進階隱私權管控設定視窗，在管理主控台點擊隱私權管控>狀態 的 進階設定。



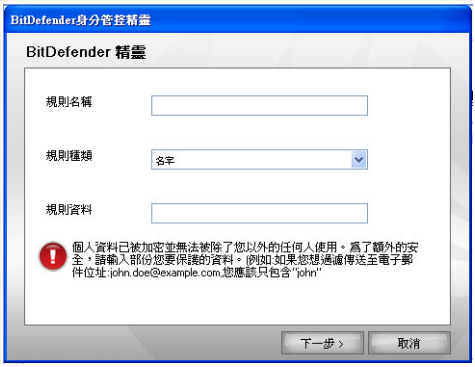
身分管控

10.2.1. 建立身分管控規則

身分管控規則必須手動輸入（按下 加入 按鈕，並選擇規則的參數)。將會出現設定精靈。

設定精靈包含三個步驟。

步驟 1/3 — 設定規則類型及資料



設定規則類型及資料

在編輯欄位裡輸入規則的名稱。

您必須設定以下的參數：

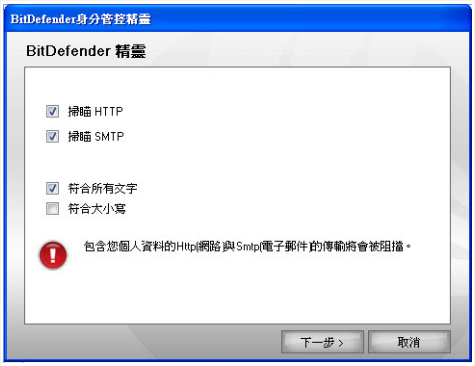
■規則類型 — 選擇規則類型（住址、姓名、信用卡號碼、身份證號碼等）。
■規則資料 — 輸入規則的資料。

注
假如您輸入少於三個字母，您將會被提示驗證資料。我們建議您最少三個字母以避免被阻擋錯誤發生。

在這裡您所輸入的資料都會被加密。為了加強安全性，請不要輸入您所有希望被保護的資料。

按下 Next(下一步)。

步驟 2/3 — 選擇傳輸方式



選擇傳輸方式

選擇您希望 BitDefender 掃描的傳輸方式： 以下的選項是可用的：

■掃描 HTTP — 掃描 HTTP(網站) 傳輸，並封鎖符合規則的出街資料。
■掃描 SMTP — 掃描 SMTP(電郵) 傳輸，並封鎖符合規則的外送電郵。

當規則的資料完全符合您的要求，您可以選擇套用。

按下 Next(下一步)。

步驟 3/3 — 規則描述

規則描述

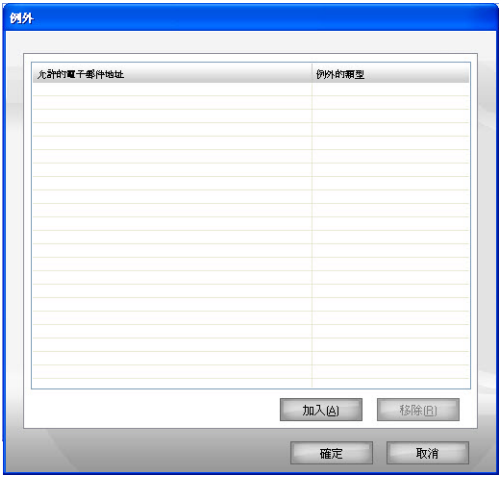
在編輯的欄位上輸入一個規則的簡短描述。

按下 完成。

10.2.2. 例外規則定義

您可能須要定義對特定的身份規則用特定的例外情況。 當您真的需要將您的信用卡資料藉由網路傳送遞交時，您可以設定控管規則的例外。

要管理例外規則，按下 例外 。



指定例外

要加入例外規則，請依照下列步驟：

1. 點擊加入在表格裡加入新的項目。
2. 在指定允許的位址 關閉裝置 點擊兩下，輸入您要加入例外的網址或是電子郵件位址。
3. 點擊兩下選擇類型的選單選擇對應的您輸入的資料選項。
   ■假如您指定了一個網址，請選擇HTTP。
   ■假如您指定了一個電子郵件位址，請選擇SMTP。

從例外清單裡選擇並按下 移除即可移除不用的例外項目。

點擊套用 去儲存變更。

10.2.3. 管理規則

您可以在表格中檢視規則清單。

要刪除一個規則，只需點選規則並按下 刪除 按鈕。如果只是要暫時不啟動規則，不需刪除它，只要取消對應勾選的方框即可。

要編輯一個規則，只需點選規則並按下 編輯 按鈕或者雙擊規則。一個新的視窗即會出現：

編輯規則

在這裡，您可以變更規則的名稱、描述及參數(種類、資料及掃描傳輸的方式)。按下 確定 儲存設定。

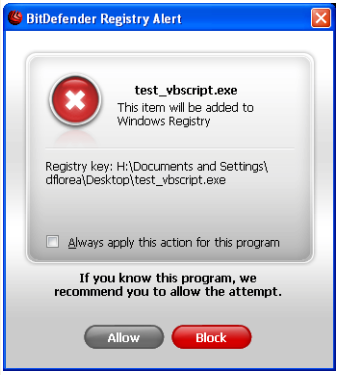
按下 確定 儲存這個設定並關閉視窗。

10.3. 進階設定 — 登錄管控

登錄碼 在 Windows 作業系統是一個非常重要的部份。這是 Windows 放置設定、安裝的程式、使用者資訊等相關重要設定的地方。

這個 登錄碼 也被使用來定義哪個程式在 Windows 啟動時自動執行。當使用者重新啟動電腦時，病毒通常也利用這個方式自動啟動。

登錄控管 監察 Windows 登錄碼的變化 — 這是偵測木馬程式有效的方法。每當一個程式試著修改登錄碼，以便在 Windows 啟動時被執行時，它將會先警告您。



登錄警示

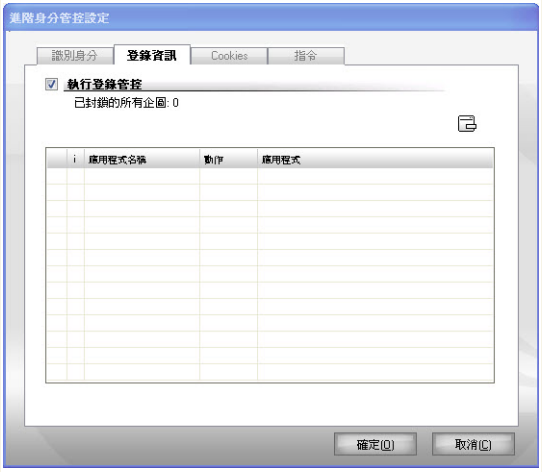
您可以拒絕這個修改，按下 取消 或者允許這個設定，按下 確定 。

如果您想要 BitDefender 記住您的答案，勾選 記住這個答案。 如此，一個新的規則將被建立並且在外部程式變動系統登錄項目是持行相同動作。

注
當您安裝新的程式且必須在下次系統啟動時執行，BitDefender 將會提示您。多數情形下，這些程式是合法且可被信任的。

每個已建立的規則可在 登錄 頁面做進一步的調整。 要進入這個頁面，打開進階隱私權管控設定視窗，選擇登錄)標籤。

注
要開啟進階隱私權管控設定視窗，在管理主控台點擊隱私權管控>狀態 的 進階設定。



登錄管控

您可以在表格中檢視目前已建立規則清單。

要刪除一個規則，只需點選規則並按下 刪除 按鈕。 要暫時地停用規則，請清除對應的核取方塊。

去變更規則採取的動作，連點擊兩下動作欄可從選單中選取適合的選項。

按下 確定 關閉視窗。

10.4. 進階設定 — Cookie 管控

Cookies 是網際網路上一個常見的記錄。它是存在您電腦裡非常小的一些檔案。網站透過建立這些 cookies 以保持您的追蹤資訊。

Cookie 讓您的生活變得更方便。舉例來說，它們可以讓網站記住您的名字及相關的資訊，所以，您不需要每次造訪網站時都重新輸入這些資訊。

但透過追蹤您的記錄樣本，cookie 也可能被利用洩露您的隱私資料。

這是 Cookie管控 協助。當您啟動 Cookie 管控，無論何時一個新的網站試圖設定一個 cookie 時，將先徵求您的同意：

Cookie 警戒

您可以看見正試圖寄送 cookie 檔案的應用程式名稱。

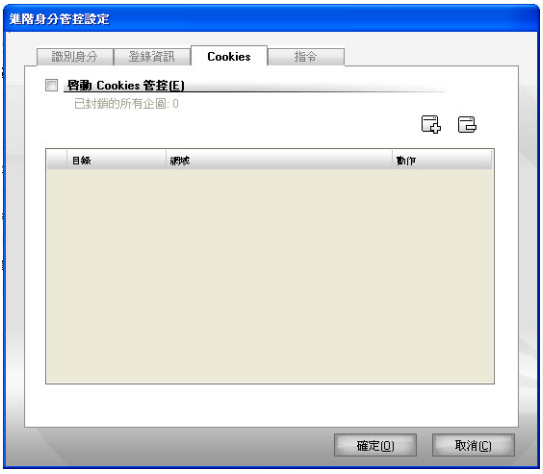
按下 記住這個答案 選項，並按下 是 或 否，建立並套用規則，並列於表格裡。當您下次再連線到相同的網站時，您將不再被通知。

這將會協助您選擇哪個網站您要信任或不信任。

注
現今大量的 cookie 被使用在網際網路上，Cookie 管控 一開始使用可能有點麻煩。首先，當網站試圖儲存 cookie 在您的電腦時，它將詢問一些問題。很快地，您新增常閱覽的網站到規則清單裡，它將變得比以前更容易。

在 Cookie 頁面，每個規則都可以儲存以供未來的調整用途。 要進入這個頁面，打開進階隱私權管控設定視窗，選擇Cookie)標籤。

注
要開啟進階隱私權管控設定視窗，在管理主控台點擊隱私權管控>狀態 的 進階設定。



Cookie 管控

您可以在表格中檢視目前已建立規則清單。

重要
規則將依序它們的優先權由上而下排列，越高就越優先。拖曳這些規則以更改他們的優先權。

要刪除一個規則，選擇它並按下 刪除 按鈕。要去修改一個規則的參數只要雙擊它的欄位，並修改您需要的設定。若只是暫時不啟動規則不需要刪除它，只需取消勾選即可。

規則可以自動輸入（透過警示視窗）或手動（按下 新增 按鈕，並選擇規則的參數）。設定精靈將會出現。

10.4.1. 設定精靈

設定精靈是一個只有一步的程序。

步驟 1/1 — 選擇位址、動作及方向。

選擇位址、動作及方向

您可以設置參數：

■網域位址 — 在規則裡，輸入所應套用的網域。
■動作 — 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 cookie 將會被執行。
拒絕	在這個網域的 cookie 將不會被執行。

■方向 — 選擇傳輸的方向。

類型	描述
外傳	這個規則只套用在被傳送到連線網站的 cookies。
接收	這個規則只套用在從連線網站所接收的 cookies。
兩者皆是	這個規則套用到進出二個方向。

按下 完成。

注
您可以接受 cookies 但不回傳它們： 拒絕 外送 方向。

按下 確定 儲存這個設定並關閉視窗。

10.5. 進階設定 — Script 控制

Scripts 及其他類似 ActiveX 控制 及 Java applets，是被用來建立互動式網頁，可以被設計成有害的程式。舉例來說，ActiveX 元素可以獲取您的資料，它們可以從您的電腦讀取資料、刪除資訊、擷取密碼並在您上線時攔截訊息。您應該只接受您所信任網站的主動式內容。

BitDefender 讓您選擇去執行這些元件或者封鎖它們的執行。

透過 Script 管控 您可以指定哪個網站是您信任或者不信任。BitDefender 將會先徵求您的同意無論何時一個網站試著啟動一個 script 或其他主動式的內容：

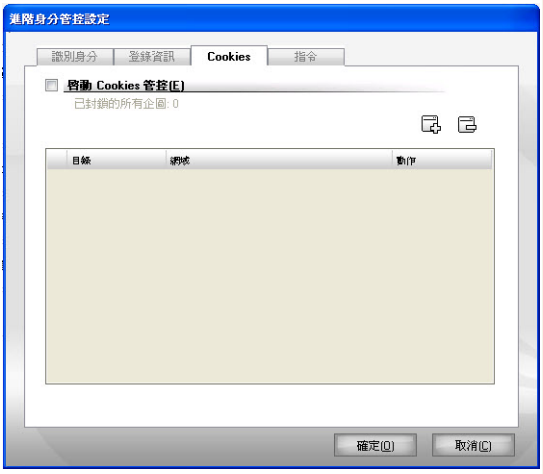
Script 警告

您可以檢視資源的名稱。

按下 記住這個答案 選項並按下 確定 或 取消 ，一個規則將被建立、套用並列於規則表格中。當相同網站試圖寄送您一個主動式的內容時，您將不再受到通知。

每個規則都可以被存取在 Script 頁面以供未來的調整。 要進入這頁面，開啟進階隱私權管控設定 視窗，並點擊Script標籤。

注
要開啟進階隱私權管控設定視窗，在管理主控台點擊隱私權管控>狀態 的 進階設定。



Script 管控

您可以在表格中檢視目前已建立規則清單。

重要
規則將依序它們的優先權由上而下排列，越高就越優先。拖曳這些規則以更改他們的優先權。

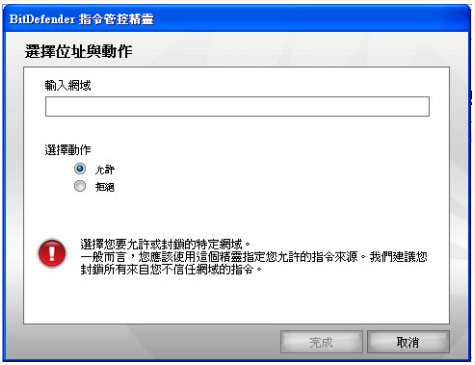
要刪除一個規則，選擇它並按下 刪除 按鈕。要去修改一個規則的參數只要雙擊它的欄位，並修改您需要的設定。若只是暫時不啟動規則不需要刪除它，只需取消勾選即可。

規則可以自動輸入（透過警示視窗）或手動（按下 新增 按鈕，並選擇規則的參數）。設定精靈將會出現。

10.5.1. 設定精靈

設定精靈是一個只有一步的程序。

步驟 1/1 — 選擇位址與動作



選擇位址與動作

您可以設置參數：

■網域位址 — 在規則裡，輸入所應套用的網域。
■動作 — 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 scripts 將會被執行。
拒絕	在這個網域的 scripts 將不會被執行。

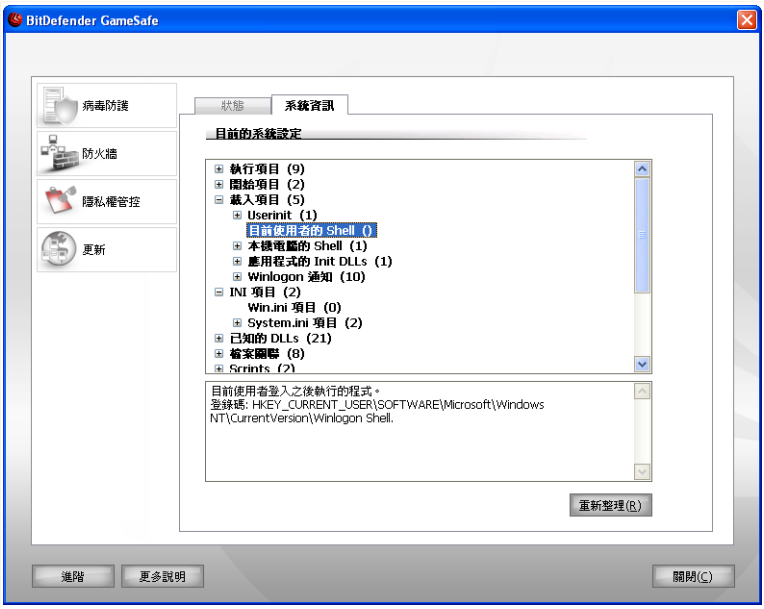
按下 完成。

按下 確定 儲存這個設定並關閉視窗。

10.6. 系統資訊

BitDefender 使您從單一個地方便能夠檢視開機時所有的系統設定以及登錄執行的應用程式。如此，您可以監控所有系統的活動並能夠辨識感染的發生。

要獲得系統資訊，請在管理主控台點擊隱私權管控>系統資訊。 以下視窗將會顯示:



系統資訊

這個清單包含所有被載入的項目，當系統啟動時，這些項目會被不同應用程式所載入。有三個按鈕可用：

■移除 — 刪除所選的項目。 點擊 是 確認您的選擇。

注
若您不想在這個頁面，重覆地要您確認，點不要再問。

■到 — 開啟您所選擇項目的視窗（如：登錄）

■重新整理 — 重新整理 系統資訊 頁面。

注
隨著所選的物件不同，移除 或者 到按鈕，不一定會出現。

10.7. 反網路釣魚工具列

BitDefender能夠防護您的電腦免於網路釣魚的威脅。 它能夠掃描您正在瀏覽的網站，並提醒您是否有網路釣魚的威脅。 您可以設定網站白名單，如此BitDefender將不會掃描這些網站。

您可以利用BitDefender設立在Internet Explorer 的反網路釣魚工具列可以容易地管理防護工具，以及建立白名單。

反網路釣魚工具列位於Internet Explorer 的上方，以 BitDefender 圖示表示。要開啟工具列選單，請點擊圖示。

注
假如您無法看見工具列，開啟 檢視 選單， 選擇工具列 並點擊BitDefender 工具列。

反網路釣魚工具列

在工具列選單會有以下可用的命令：

■啟動 / 停用 — 啟動 / 停用 BitDefender 工作列。

注
假如停用反網路釣魚工作列，您將不在受到抵抗網路釣魚的保護。

■設定 — 開啟一個視窗，您可以設定反網路釣魚工作列。

以下的選項是可用的：

- 啟動掃描 — 啟動反網路釣魚掃描。
- 加入白名單前先詢問 —在您將網站加入白名單前，先詢問您。

■加入白名單 — 將目前的網站加入白名單。

注
將網站加入白名單意謂著BitDefender將不會在針對該網站使用反網路釣魚功能。我們建議您只將您絕對信任的網站加入。

■檢視白名單 — 開啟白名單清單。

您可以看見所有不會被BitDefender反網路釣魚引擎掃描的網站。

假如您要從白名單中移除任何網站使您可以得知此網站是否有網路釣魚威脅，點擊他旁邊的移除按鈕。

您可以將您絕對信任的網站加入白名單，如此這些網站將不會在被Remove反網路釣魚引擎掃描。 要將網站加入白名單，在所對應的欄位輸入網站的網址並點擊加入。

■說明 — 開啟說明檔案。

■關於 — 開啟一個視窗，在此您可以得到更多關於BitDefender的資訊並且可以尋求相關協助。

11. 更新

每一天都有新的惡意程式被發現。這就是為什麼 BitDefender 需要保持最新的病毒特徵碼是非常重要的。預設上，BitDefender 是每個小時自動檢查更新。

如果您是透過寬頻或 ADSL 連線到網際網路，BitDefender 會特別注意這個。當您啟動您的電腦後，它將每 小時 確認更新。

如果偵測到更新時，依據 自動更新選項 頁面的設定，您將被詢問是否要執行更新或者自動地安裝更新。

更新程序傳送中，表示正在取代日益增加的檔案。在更新的同時，產品也不會有漏洞。

更新會利用以下幾種方式：

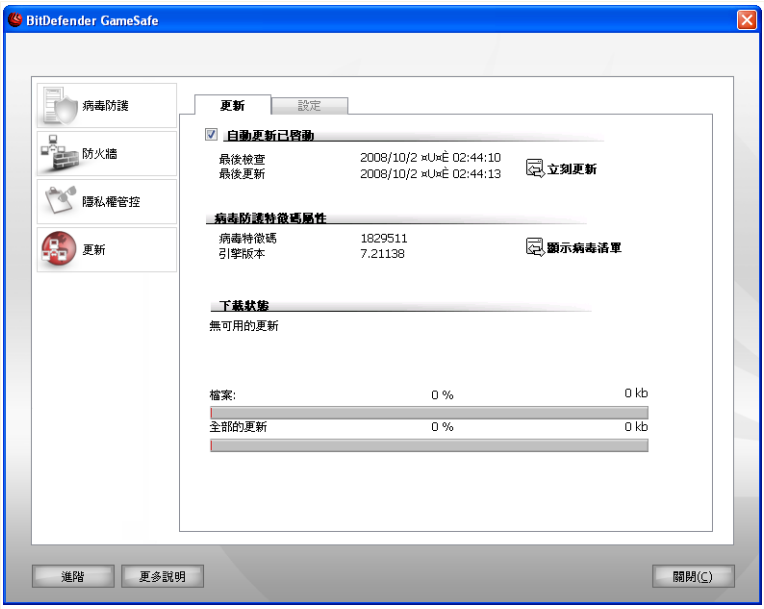
- 反垃圾郵件引擎更新 — 新的規則將會被加入到啟發式與URL過濾器；新的圖片也會被加到圖片過濾器。這個更新的型態是我們熟識的 反垃圾郵件更新。
- 反間諜程式引擎更新 — 新的間諜程式特徵碼將會被加入到資料庫。這個更新的型態是我們熟識的 反間諜程式更新。
- 軟體更新 — 當一個新的軟體版本被發行時，新的功能的掃描技術都為了提升軟體的效能，這個更新的型態是我們熟識的 軟體更新。

在使用者手冊的 更新 手冊包含了以下的主題：

- 自動更新
- 更新設定

11.1. 自動更新

要看見更新相關的資訊並執行自動更新，在管理主控台點擊更新>更新。 以下視窗將會顯示:



自動更新

您可以在此檢視最近一次的更新是何時進行的、更新時是否成功。防毒引擎的版本資訊以及所有的特徵碼數量也會在此被檢視。

按下 顯示病毒清單 您可以取得 BitDefender 惡意程式的特徵碼。一個 HTML 檔案包含所有可用的特徵碼都會被建立。按下 BitDefender病毒清單 ，您可以到線上 BitDefender 特徵碼資料庫搜尋特定的惡意程式特徵碼。

假如您在更新的過程開啟此頁面，您將能夠檢視狀況。

重要
防護您的系統以抵抗最新的病毒威脅，請保持 自動更新 啟動。

11.1.1. 要求更新

您可以按下 立即更新 在任何時候您想進行自動更新。這種更新方式是 使用者要求的更新。

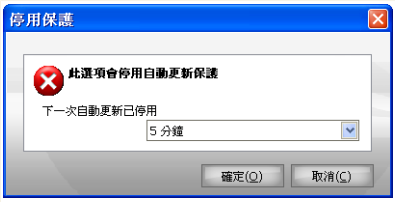
這個 更新 模組將連線到 BitDefender 更新伺服器並且確認是否有更新可用。如果偵測到一個更新，將依據 手動更新設定 頁面的設定，您將被詢問是否要執行更新或者自動地安裝更新。

重要
當您完成更新時，可能需要將電腦重新啟動。我們建議盡可能重新開機。

注
如果您是利用撥號方式連線到網際網路，建議您定期地去更新 BitDefender 以獲的最好的防護效果。

11.1.2. 停用自動更新

如果您關閉自動更新，您就會收到一個警告視窗。



關閉自動更新

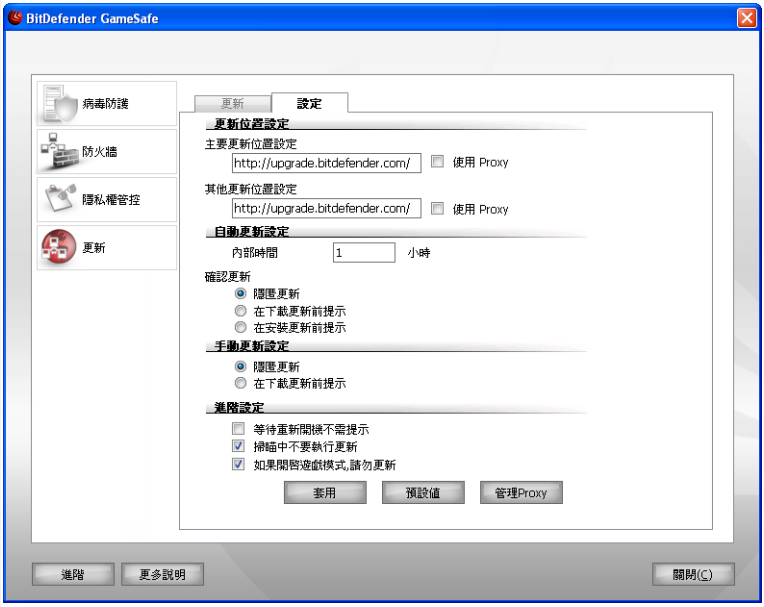
您可以從視窗選擇您要停用自動更新的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。

警告
這將會是個嚴重的安全防護事件，我們建議您盡可能減少停用自動防護的時間。假如BitDefender無法正常地實行更新，它將無法防護您的電腦抵抗最新的威脅。

11.2. 更新設定

可以從本地網路、或直接連線到網際網路或透過 Proxy 伺服器進行更新。 預設上，BitDefender能夠每小時檢查是否有新的可用更新並且能夠自動下載安裝到您的電腦。

要調整更新設定與管理proxy，在管理主控台點擊更新>設定。 以下視窗將會顯示:



更新設定

在更新設定的視窗包含四個類型的選項 (更新位置設定、自動更新設定、手動更新設定 及 進階設定) 以可展開的選單方式呈現。

11.2.1. 更新位置設定

設定更新位置設定的位置。這個設定透過更新位置設定目錄來進行。

注
配置這些設定，只有當如果您連接到只地方性地儲存 BitDefender 惡意軟體驗證的一個本地區域網路，或者如果您經過一個代理伺服器(Proxy)對網際網路連接。

為了更穩定及更快速地更新，您可以設定二個更新位置：一個是 主要的更新位置，另一個是 其他的更新位置。這兩個預設都是 http://upgrade.bitdefender.com。

要調整更新位置，在對應的URL欄位提供鏡像位置的URL。

注
我們推薦您設置主要更新位置為您身處的地區的鏡像，讓其他更新位置保持不變，以防萬一連不到本地的鏡像。

通常，公司會使用代理伺服器連接網際網路，把使用Proxy打勾，並點擊管理代理伺服器清單設置代理伺服器。

注
更多資訊，請參閱"管理Proxies" (p. 128)

11.2.2. 設置自動更新

要調整BitDefender的自動更新程序，使用自動更新設定裡的選項。

您可以在時間間隔的欄位設定一段時間。預設上，更新時間間隔為一小時。

要指定自動更新如何執行，請選擇下列項目：

■隱匿更新 — BitDefender 自動地下載及執行更新。
■下載前先詢問 — 每次當有更新可用時，在下載前先詢問您。

注
即使您已經離開了安全防護中心，下載更新前還是會先詢問您。

■安裝前先詢問 — 每一次有下載更新時，在安裝前先詢問您。

注
即使您已經離開了安全防護中心，下載安裝前還是會先詢問您。

11.2.3. 調整手動更新

要調整BitDefender的手動更新程序，使用手動更新設定裡的選項：

■隱匿更新 — 手動更新將自動地執行不會顯示使用介面。
■下載前先詢問 — 每次當有更新可用時，在下載前先詢問您。

注
即使您已經離開了安全防護中心，下載更新前還是會先詢問您。

11.2.4. 調整進階設定

要避免BitDefender更新程序影響您的作業，請調整在進階設定目錄裡的選項：

■等待重新開機以取代提示 — 如果一個更新要求重新開機時，軟體將仍以舊的檔案繼續運作，直到系統被重新開機。使用者將不會被提示重新開機，因此 BitDefender 更新程序將不會妨礙使用者的工作。

■如果正在執行掃描程序，則不要更新 — 如果正在執行掃描程序，BitDefender 將不會進行更新。這樣 BitDefender 更新程序將不會影響掃描工作。

注
當掃描正在進行時，如果 BitDefender 執行更新，則掃描程序將會被終止。

■如果遊戲模式開啟時，則不要更新 — 如果BitDefender遊戲模式設為開啟，則不會執行更新。 如此，您便能夠將遊戲影響最小化。

11.2.5. 管理Proxies

若您的公司使用代理伺服器上網，您一定要設置代理設定使BitDefender可以自己更新。否則，它會使用裝了產品的管理者代理設定 或者 目前使用者預設瀏覽器的代理設定，若有的話。

注
Proxy設定只能備有管理權限的使用者調整。

要管理員proxy設定，點擊 管理proxies 。 Proxy管理員將會出現。

Proxy管理員

管理代理伺服器設定有三個類別：

■管理者代理伺服器設定(安裝時) — 在安裝時偵測管理者帳戶內的代理設定，只有當您登入到該帳戶時才能設置代理。如果代理伺服器需要一個使用者名稱和一個密碼，您一定要在對應的欄位中填上。

■使用目前使用者預設瀏覽器的代理伺服器設定在目前使用者的預設瀏覽器中導出。如果代理伺服器需要一個使用者名稱和一個密碼，您一定要在對應的欄位中填上。

注
被支持的瀏覽器有Internet Explorer, Mozilla Firefox 和 Opera。若您預設用其他的瀏覽器，BitDefender就不能夠讀取目前使用者設定了。

■您自訂的proxy設定 — 當您以系統管理者登入時，您可以調整的proxy設定。

以下的選項是必須被指定的：
- 網域位址 — 輸入proxy伺服器的IP。
- 連接埠 — 輸入BitDefender 要使用連線到 Proxy 伺服器的連接埠。

- 使用者名稱 — 輸入 Proxy Server 可識別的使用者名稱。
- Proxy 密碼 — 輸入先前指定使用者的有效密碼。

當嘗試連接到網路，每一組的代理伺器設定都會去試，直至BitDefender連上。

首先，包含屬於您的代理設定會先連上網。若連不到，就會嘗試用在安裝時所讀取到的代理設定來試。最後，如果都不行，就會用目前使用者預設瀏覽器的代理來上網。

按下 確定 儲存這個設定並關閉視窗。

按下 套用 去儲存變更或按下 預設 去載入預設值。

BitDefender 救援光碟

12. 概觀檢視

BitDefender GameSafe 含有可開機光碟 (BitDefender 救援光碟) 在您的作業系統啟動前，可進行掃描及清除所有存在的磁碟機。

您可以在您的作業系統因為病毒而無法運作時，使用 BitDefender 救援光碟。當您未使用任何病毒防護產品時，這種情形會常常發生。

病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

BitDefender 救援 CD 是 BitDefender加強後的Knoppix 分支。這片光碟是整合了最新的Linux保安技術的GNU/Linux Knoppix Live CD，提供一個桌面供掃描及清除包含NTFS的硬碟上的病毒之用。同時BitDefender在您不用進入可以Windows時，還原您的資料。

注
BitDefender 救援光碟可於下列位置被下載：http://download.bitdefender.com/rescue_cd/

12.1. 系統要求

在使用 BitDefender 救援 CD 開啟電腦前，您必須先確認您的系統符合以下的需求。

CPU 種類
x86 相容機種、最少需要 166 MHz，但不能期望有很好的效能。i686 系列的處理器、800 MHz，可能運作的更有效率。

記憶體
最少 512MB 記憶體或以上 (建議使用1GB)

光碟機
BitDefender救援光碟是由光碟機執行，因此，光碟機及可以從 BIOS 啟動開機為其要求項目。

網際網路連線
雖然BitDefender救援光碟是不需要在網際網路連線下執行，但更新的程序會要求啟動 HTTP 連線，甚至可以透過 Proxy 伺服器。因此，為了提供完整的防護，網際網路的連線是_必需_的。

圖形介面的解析度
標準 SVGA-相容圖像顯示卡

12.2. 包含的軟體

BitDefender 救援光碟包含以下的軟體程式。

Xedit
這是文字檔案編輯器。

Vim
這是更強的文字檔案編輯器，包含強調的語法格式，圖形用戶界面。要更多資訊，請參閱Vim 網站。

Xcalc
這是一個計算機。

RoxFiler
RoxFiler是一個快速而強大的圖像化檔案管理員

想要更多資料，請瀏覽 RoxFiler 網站。

MidnightCommander
GNU Midnight Commander (mc) 是一個文字介面檔案管理員。

想要更多資料，請瀏覽 MC 網頁。

Pstree
Pstree顯示正在執行的程序。

Top
上方顯示Linux工作區。

Xkill
Xkill用來終結X資源的一位用戶。

Partition Image
Partition Image幫您貯存整個分割區(EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32)至一個映像檔。此軟體能協助您備份。

要更多資料，請瀏覽Partimage 網頁.

GtkRecover
GtkRecover是個GTK版本的檔案復原工具。它能助您挽回檔案。

要更多資料，請參閱GtkRecover 網頁。

ChkRootKit
ChkRootKit能助您掃描電腦內的rootkit。
要更多資料，請參閱ChkRootKit 網頁.

Nessus Network Scanner
Nessus是一個Linux, Solaris, FreeBSD, and Mac OS X遠端掃描器。
要更多資料，請參閱Nessus 網頁。

Iptraf
Iptraf是個IP網路監控軟體。
要更多資料，請參閱Iptraf 網頁。

Iftop
Iftop顯示每個接口的頻寬用量。
要更多資料，請參閱Iftop 網頁。

MTR
MTR是一個網路診斷工具。
要更多資料，請參閱MTR 網頁

PPPStatus
PPPStatus顯示TCP/IP流出流入的統計。
要更多資料，請參閱PPPStatus homepage。

Wavemon
Wavemon是一個無線網路裝置監控軟體。
要更多資料，請參閱Wavemon 網頁。

USBView
USBView顯示已連接到USB bus的裝置資料。
要更多資料，請參閱USBView 網頁。

Pppconfig
Pppconfig助您自動設置ppp撥號連線。

DSL/PPPoe
DSL/PPPoe 設置PPPoE (ADSL寬頻)連線。

I810rotate
I810rotate調節 i810硬件i810switch(1)的影像輸出。

要更多資料，請參閱I810rotate 網頁。

Mutt

Mutt一個強大的文字介面MIME郵件客戶端。

要更多資料，請參閱Mutt 網頁。

Mozilla Firefox

Mozilla Firefox 瀏覽器是一個大家耳熟能詳的網站瀏覽器。

要更多資料，請參閱Mozilla Firefox 網頁。

Elinks

Elinks是一個文字介面的網站瀏覽器。

要更多資料，請參閱Elinks 網頁。

13. BitDefender 救援CD 說明

這一節會教您怎樣使用BitDefender 救援CD ,掃描惡意程式無論電腦上已癱瘓不能開的Windows，以至隨插即用裝置。您更可以藉本CD做更多使用手冊上沒記載的事。

13.1. 啟動BitDefender 救援光碟

要啟動光碟，從BIOS設定您的電腦由光碟機啟動，放入光碟片並啟動電腦。確認您的電腦可以由光碟機啟動。

等待螢幕畫面出現，依循著畫面的指示去進行BitDefender 救援光碟。

啟動的畫面

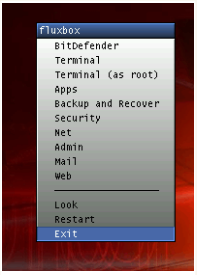
病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

當啟動程序完成時，您將看到下一個桌面。您將開始使用 BitDefender 救援CD 。

桌面

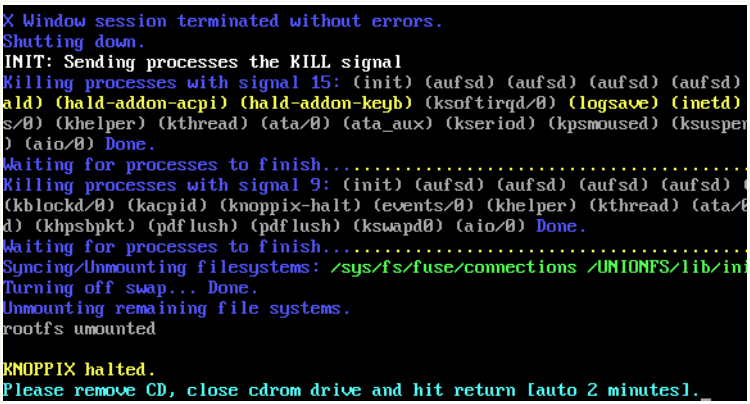
13.2. 停止BitDefender 救援光碟

在選擇離開 或 執行halt指令後，您可以放心關機。



選擇 "離開"

當 BitDefender救援光碟已經成功關閉所有程式，它會顯示如以下的畫面。您可以從光碟機取出光碟片。現在可以關閉您的電腦或重新開機。



等待這個訊息才關機。

13.3. 如何執行一個病毒防護掃描？

開機程序完成後，一個精靈便會出現。它會提示您掃描您的電腦。您只須按下開始按扭。

注
若您的螢幕解像度不足，系統會問您須不須用文字模式掃描。

依照三步驟指引執行掃描任務。

1. 您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

   注
   掃描程序將依它的複雜程度而需花費一些時間。

2. 您可以檢視可能影響您的系統的事件數量。

   結果會以群組顯示。 按下 "+" 的小方框以展開選項或按下 "-" 的小方框關閉選項。

   您可以針對不同的威脅類型的分組採取行動，也可以逐項地進行處理。

3. 您可以檢視結果。

如果您只想掃描某些特定資料夾，這樣做：

瀏覽您的資料夾，在檔案或目錄按下滑鼠右鍵，選擇 傳送到。然後選擇 BitDefender 掃描器。

或者，您可以用root執行下一個命令。BitDefender 病毒防護掃瞄開始掃描預設位置被選取的檔案或資料夾。

```
# bdscan /path/to/scan/
```

13.4. 我如何使用代理伺服器更新 BitDefender？

若您的電腦要使用代理伺服器才能上網，您須要做一些設定，才能更新病毒定義。

要經代理伺服器更新，這樣做：

1. 右擊桌面， BitDefender救援CD 右鍵選單彈出。
2. 選終端機 (as root)
3. 鍵入以下命令cd /ramdisk/BitDefender-scanner/etc。
4. 鍵入mcedit bdscan.conf命令，來以GNU Midnight Commander (mc)編輯這個檔案。
5. 解除這行的註解#HttpProxy =(只是刪去#號)，再打網域，使用者名稱，密碼，伺服器連接埠。例如，這幾行一定像這樣：

   HttpProxy = myuser:mypassword@proxy.company.com:8080
6. 按下 F2 去儲存目前的檔案，按下 F10 關閉它。
7. 打這個命令bdscan update。

13.5. 如何儲存我的資料？

假設您因一些不知明的原導致您不能進入Windows。同一時間，您拼命地想存取一些重要的資料。這就是使用BitDefender救援CD 的時候了。

用攜帶裝置像USB手指，來救回您的資料。這樣做：

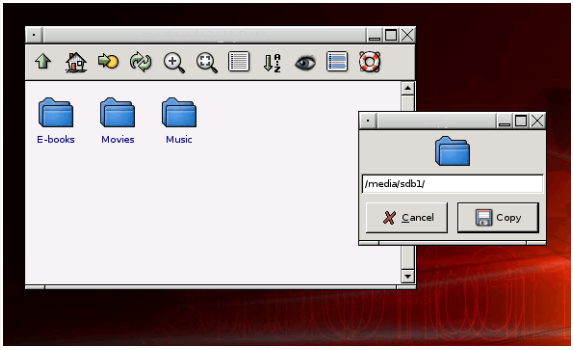
1. 放 BitDefender救援CD 入光碟機，放記憶卡入USB槽，然後重新開機。
2. 等到 BitDefender救援CD 開好機。以下視窗就會彈出。

桌面

3. 點擊兩下您想復原的資料所屬的硬碟分割區(例如：[sda3])。

注
在 BitDefender救援CD 中，硬碟分割區會使用Linux-type名稱。所以[sda1]好大可能對應Windows-type中的(C:)，而[sda3] 對 (F:), 以及 [sdb1] 指向記憶卡。

4. 瀏覽您的資料夾。例如：我的資料 包含 影片, 音樂 和 E-books 子資料夾。
5. 右擊您想要的路徑，選複製。這個視窗就會彈出來。



貯存資料

6. 鍵入/media/sdb1/至對應的欄位，再點複製。

取得協助

14. 支援

一個具有價值的提供者，BitDefender 努力提供客戶一個快速且精確層級的技術支援。支援部門 (您可以透過以下提供的郵件地址與他們聯絡) 不停地保持對抗最新的威脅。在這裡所有您提出的問題都會被及時地回覆。

BitDefender 專心致力減少客戶的時間及金錢，在一個合理的價格上提供最好的產品給客戶。此外，我們相信一個成功的事業是建購在良好的溝通及承諾提供卓越的客戶服務。

您可以在任何時間提出支援需求，利用以下的電子郵件帳號 support@bitdefender.com 為了迅速地回覆，請在您的郵件裡盡可能地詳述您的 BitDefender 版本、您的作業系統及您遇到的問題。

14.1. 捷康科技股份有限公司

地址: 100台北市羅斯福路三段149號10樓
電話: (02) 2365 - 0238
傳真: (02) 2365 - 0196
sales@bitdefender-asia.com.tw
http://www.bitdefender-asia.com.tw/

詞彙表

ActiveX

ActiveX是一個程式模型讓其他程式和作業系統執行它們。ActiveX技術是用來給微軟Internet Explorer令動態網頁比靜態網頁看起來更像電腦程式。藉由 ActiveX，使用者能使用按鈕，和其他網頁中的互動元件詢問問題或回答問題，。 ActiveX 控制時常使用 Visual Basic 編寫。

ActiveX 對完全缺乏保安控制的電腦是值得注意的；電腦安全專家對它在網際網路上的ActiveX也感到沮喪。

廣告軟體

廣告軟體(Adware)通常包含在一些應用程序。這個軟體不會經使用者同意才安裝。因為這些廣告軟體在同意版權合同之後就安裝，這也是這個軟件的目的。而這個過程沒有犯罪。

然而，自動彈出(pop-up)的廣告能變成一種煩惱，同時亦會降低電腦的效率。同時，這些軟體所收集的資料可能會涉及個人私隱而安裝授權沒有完全記載。

資料封存

一個磁片、磁帶或目錄，包含了已經備份的檔案。

檔案裡包含一個或多個以壓縮格式存在的檔案。

後門

一個系統設計者或管理員故意留下的保安漏洞。不是每個漏洞都是不好的。例如：伺服器支術員或代理商的維護電腦程式編寫員都希望要有個有特權的帳戶從密閉空間來。

開機磁區

每個硬碟的開頭都貯存了這隻硬碟的結構，(磁區大小、簇大小，等等)。若是開機硬碟，開機磁區包含着一個程序使開機時載入操作系統。

開機型病毒

一種在硬碟或磁碟上使開機磁區受感染的病毒。由磁碟開機然後曼延至記憶體上。每次您開機，您就會激活該在記憶體的病毒。

瀏覽器

網站瀏覽器的簡稱，這個軟體用來顯示網頁。目前二大最受歡迎的瀏覽器是 Netscape Navigator 及 Microsoft Internet Explorer。二者都是圖形化介面的瀏覽器，代表它們同時可以顯示圖片及文字。除此之外，在加入其他的程式元件，也可以顯示多媒體資訊，包含聲音、影片。

Command line (命令列)
在命令列介面，使用者可以直接在畫面輸入命令

Cookie
在網際網路內，cookies是個別電腦的資訊的小的檔案，它又被喻為包含著能被分析而且能被廣告界使用者追蹤您的關於上網的興趣和品味的。在這範圍，cookies技術仍然繼續發展，而且意圖直接地把您感興趣的廣告瞄準著您。這是一把雙面刃。因為一方面，這種技術會更有效率，因為您只會看到您感興趣的廣告。另一方面，事實上，它會「追蹤」並「跟隨」您去了哪和按了什麼鍵。可理解地，這有私隱上的爭論，他們覺得被網站看作"SKU數字" (就好像在包裝紙上的條形碼)的辯論。當然這樣的觀點是極端的，但是在某些情況下是準確的。

磁碟機
磁碟機可允許讀取資料及寫入資料。

硬碟機可以讀取及寫入資料到硬碟機。

軟碟機可以存取磁碟片。

硬碟機有包含內接式 (放置在電腦主機內) 或外接式 (放置在一個獨立的機殼裡，並與電腦主機連線)。

Download (下載)
要把資料(通常全部檔案)從一個主要的來源複製到週邊裝置。這詞語通常用來形容從線上服務到某人的電腦上。下載通常看成從網路上的檔案伺服器複製到一部電腦上。

E-mail (電子郵件)
電子郵件。經由本地或全球網路在電腦上傳遞郵件的服務。

事件
由軟體偵察到的一個動作或一件事件。事件可以是使用者的動作，例如：用滑鼠點擊或按鍵盤上的鍵或系統事件，例如：記憶體用完。

False positive (誤判)
當掃描器識別出一個檔案受到感染，而事實上並不是。

Filename extension (副檔名)
檔案名稱的一部份，它會跟隨在一個 "." 之後，它指出檔案是何種類型的資料。

許多作業系統使用副檔名，如：Unix、VMS 及 MS-DOS。它們通常含有一到三個字元。例如：c 代表 C 語言的原始檔、ps 則是 PostScripts 格式、txt 則是文字檔。

Heuristic (啟發式技術)

識別新的病毒的基礎方法。這類的掃描不依賴特定的病毒驗証。好處是不會被舊病毒的變種愚弄。然而，它可能有時在正常的軟體中報告有該軟件懷疑是病毒。產生所謂的「假陽性(false positive)」。

IP

網際通訊協定 －在TCP/IP中的一組通訊協定可定路線通訊協定。負責IP位址，決定路徑和IP packet的分拆和合併。

Java applet

一個Java程序，它設計用來只是在網頁上執行。要在網頁上使用applet，您需要先定好applet的名，大小(長和闊，單位用像素)來讓applet應用。當那存取那網頁，瀏覽器會從伺服器下載那applet，並在使用者的電腦上執行。Applet和其他的軟體分別在於Applet有嚴格的通訊協定。

例如：即使Applet在客戶端上執行，它也不能讀寫客戶端上的資料。加上，Applet在網路上有著更嚴格的監管。他們只能讀寫同一網域上的資料。

Macro virus (巨集型病毒)

這類型的病毒是在檔案中含有巨集程式。許多應用程式如：Microsoft Word 及 Excel，都有支援巨集語言。

這些應用程式允許您在一個檔案裡插入一個巨集，在檔案每一次被開啟時，巨集程式即可被執行。

Mail client (電子郵件程式)

一個電子郵件程式是一個應用程式，它讓您可以傳送及收發電子郵件。

記憶體

電腦內部的儲存空間。這詞語指資料被貯存為很多小碎片。而「貯存」這個詞語是指已經在磁帶或者硬碟內。每部電腦都有一定數量的實體記憶體。通常我們通稱它為主記憶體，內存，或RAM。

非Heuristic (非啟發式技術)

這個方法是依賴特定的病毒驗證。非啟發式技術的好處是它不會把相似的當是病毒，以及它不會彈出錯誤的警告。

壓縮程式

一個被壓縮的檔案格式。很多操作系統和應用程式包含這個命令使您把格案壓縮減少使用的記憶體。例如：您有一個文字檔案包含著十個連續的空格。通常，會用十個元組(bytes)來貯存。

然而，程式會把檔案壓縮，用一特定空格組合字元取代空白字完。在這個情況，十個空格字元會被取代成二個位元。這只是其中一隻壓縮技術，還有其他很多種。

路徑

一個電腦裏切確檔案的方向。 根據等級制度檔案系統，這些方向通常描述從上到下來。

兩點之間的路徑，例如：兩電腦之間的通訊頻道。

Phishing (網路釣魚工具)

將一份電子郵件送到一個使用者，虛偽地自稱是合法的企業，並要求受害者主動地提交自己的個人資料，使犯人竊盜受害者的私人資料。電子郵件指示使用者到一個像合法的組織的網站，更新個人的資料，像是密碼和信用卡、社會福利和銀行帳號的網站。 然而，網站是假的，建立起來只是用來偷使用者的資料。

多形病毒

病毒會改變它的形式來傳染每個檔案。 因為他們沒有一致的二進制樣式，這樣的病毒很難辨認。

Port (連接埠)

一個連接埠在您能連接設備的電腦。 個人電腦有的連接埠各種各樣的類型。 內部，有幾個埠口為連接的驅動器、顯示屏和鍵盤。 外部，個人電腦有連接埠為連接的數據機、印表機、滑鼠和其他周邊設備。

在TCP/IP和UDP網路，一個終點對邏輯連接。 通道數辨認什麼樣的埠口。 例如，連接埠80為HTTP交通使用。

Report file (報告檔)

這個檔案列出 BitDefender 發生的行為。BitDefender 在報告檔裡列出掃描的路徑、目錄、掃描的檔案數量及被掃描的檔案，有多少受感染及可疑檔案被發現。

Rootkit(後門程式)

rootkit是一套提供系統的管理員層級存取的軟體工具。 規定為UNIX操作系統首先使用了，並且它提到了入侵者行政權利的重新編譯的工具，給他們隱存看見系統管理員。

rootkits的主要角色是隱藏程序、檔案、註冊和日誌。 如果他們合併適當的軟體，他們也許也攔截資料從終端、網路連接或者外圍設備。

Rootkits不是惡意的本質。 例如，系統和有些應用使用rootkits掩藏重要檔案。然而，他們主要用於掩藏malware或隱瞞入侵者的存在入系統。 當與malware時結合， rootkits造成巨大威脅正直和系統的安全。 他們可以監測工具，建立backdoors系統，修改檔案和日誌和避免偵查

指令

有別於巨集或批次檔案，script 是一連串要被執行的命令，而且不需要使用者介入。

Spam (垃圾郵件)

電子郵寄宣傳品或破爛物新聞組投稿。 通常通認作為任何未經請求的電子郵件

間諜程式

存取用戶的網際網路連接隱蔽地收集用戶信息，不用他們的知識所有軟體，為做廣告通常打算。 Spyware應用典型的免費軟件或共享軟件節目一個暗藏的組分可以從網際網路被下載; 然而，值得注意的是，多數共享軟件和免費軟件應用與spyware。 一旦安裝， spyware在網際網路在背景中監測用戶活動並且傳送那信息給別人。 Spyware可能也收集關於電子郵件和密碼和甚而信用卡數字的信息。

Spyware的相似電腦程式內的病毒是事實用戶無心地安裝產品，當他們安裝其他時。 一個共同的方式適合spyware的受害者將下載交換今天是可利用的產品的某一同輩對同輩檔案。

除概念和保密性的問題之外， spyware從用戶竊取存取使用電腦存儲器資源並且由它送信息回到spyware的本壘存取用戶的網際網路連接。 由於spyware使用記憶和系統資源，跑在背景中的應用可能導致系統事故或一般系統不穩定。

啟動項目

當電腦起動，在這個資料夾安置的所有檔案開始。 例如，一個啟動屏幕、一個聲音的檔案將運作的，當電腦起動時，提示日曆或者應用程序可以是起始的項目。 通常，檔案的別名在這個資料夾而不是檔案位置。

系統工具列

介紹與Windows 95，系統鍵盤位於視窗taskbar (通常在底部在時鐘旁邊)並且包含微型像為對系統作用的容易的通入例如電傳、印表機、調制解調器，容量和更多。 按下兩下或用滑鼠右鍵單擊像檢視和存取細節和控制。

TCP/IP

傳輸控制通訊協定 / 一套網路通訊協定用途廣泛在提供通信橫跨電腦在互聯的網路以不同的硬件結構和各種各樣的操作系統的網際網路。 TCP/IP包含標準為怎樣電腦溝通和大會為連接的網路和尋址交通。

Trojan (木馬程式)

一種良性應用的一個破壞性的程式。 不同於病毒，特洛伊馬不複製自己，但是他們可以是正破壞性。 其中一個電腦程式內的病毒的最陰險的類型是趕走您的電腦要求病毒，反而是病毒的程式。

期限在Homer's Iliad一個故事，希臘人給一匹巨型木馬他們的仇敵，特洛伊人，外表作為和平獻禮。 但在特洛伊人以後扯拽馬在他們的城市牆壁裡面，希臘戰士偷偷地走在馬的空心腹部外面並且打開城市門，允許他們的同胞傾吐和抓住Troy。

更新

一個軟體或硬體產品的新版本，設定用來取代相同產品的舊版本。此外，更新的安裝規則需要先去檢查是否已經存在一個舊版本在您的電腦，如果不是，您無法安裝這個更新。

BitDefender 擁有它自己的更新模組，它允許您手動檢查更新，或者讓它自動地更新軟體。

病毒

一個程式的片段在不讓您知道的情況之下載入您的電腦並且不聽從您的控制。多數病毒能夠自行複製自己。 所有電腦病毒都是人為造成的。 一個簡單的病毒能複製自己病且帶來危險，因為它將迅速耗盡所有記憶體並且導致系統運行延宕。一個更加危險類型的病毒是一個能傳送橫跨網路和繞過安全防護系統的設定。

病毒定義檔

病毒的二進位典型,根據病毒防護計畫使用發現並且除去病毒。

蠕蟲病毒

一個在網路之上繁殖它本身的計畫, 再製造它本身當它進行之時。 它不能夠把它本身附在其他的計畫。