AVG Internet Security 2012
使用者手冊

文件修訂版 2012.20 (3/29/2012)

內容

1. 簡介

本使用者手冊提供有關 **AVG Internet Security 2012** 的詳細介紹。

AVG Internet Security 2012 為您的線上作業提供多重保護，這意味著您不必擔心身分盜竊、病毒或瀏覽有害網站。它包括 AVG 保護雲端技術和 AVG 社群保護網絡，這意味著我們會收集最新的威脅資訊並與我們的社群分享，以確保您獲得最佳保護：

- 透過 AVG Firewall、Anti-Spam 和 Identity Protection 便能安全地在線上購物和使用網上銀行
- AVG 社交網路保護保證社交網路中的安全
- 透過 LinkScanner 即時保護安心上網和搜尋

2. AVG 安裝需求

2.1. 支援的作業系統

AVG Internet Security 2012 可保護執行下列作業系統的工作站：

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista（x86 和 x64，所有版本）
- Windows 7（x86 和 x64，所有版本）

（以及特定作業系統可能更高版本的服務套件）

注意：*Windows XP x64 上不支援 ID Protection 元件。您還是可以在此作業系統中安裝 AVG Internet Security 2012，但僅限於不含 IDP 元件的版本。*

2.2. 最低和建議的硬體需求

AVG Internet Security 2012 的最低硬體需求：

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM 記憶體
- 1000 MB 可用硬碟空間 (用於安裝)

AVG Internet Security 2012 的建議硬體需求：

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM 記憶體
- 1550 MB 可用硬碟空間 (用於安裝)

3. AVG 安裝程序

在哪裡可以取得安裝檔案？

要將**AVG Internet Security 2012** 安裝在您的電腦中，您需要最新的安裝檔案。為了確定您安裝的是最新版本的 **AVG Internet Security 2012**，建議您從 AVG 網站 (http://www.avg.com/) 下載安裝檔案。***支援中心/下載***區段提供每個 AVG 版本的安裝檔案的結構化概觀。

如果您不確定需要下載和安裝哪些檔案，建議您使用網頁底端的***選取產品***服務。在您回答三個簡單的問題後，此服務便會定義您真正需要的檔案。按一下***繼續***按鈕即會將您重新導向至針對您的個人需要自訂的下載檔案的完整清單。

安裝程序是什麼樣子？

當您下載了安裝檔案並將其儲存到硬碟後，便可以啟動安裝程序。安裝是一連串簡單又容易瞭解的對話方塊。每個對話方塊都會簡短說明安裝程序的每個步驟要進行什麼動作。我們在下面提供了每個對話方塊視窗的詳細說明：

3.1. 歡迎：語言選擇

安裝程序開始會顯示***歡迎使用 AVG 安裝程式***對話方塊：

您在此對話方塊中可以選取用於安裝程序的語言。在對話方塊的右側角落按一下下拉式清單展開語言功能表。選取所需語言，安裝程序將以您所選的語言繼續進行。

請注意：您目前只能選擇安裝程序的語言。AVG Internet Security 2012 應用程式將以所選語言以及英文 (永遠會自動安裝) 安裝。不過，也可以安裝其他語言，並以其中的任一語言來使用 AVG Internet Security 2012。下列其中一個名為自訂選項對話方塊會請您確認替代語言的完整選擇。

3.2. 歡迎：授權協議

然後，***歡迎使用 AVG 安裝程式***對話方塊還會提供 AVG 授權合約全文：

請認真讀取全文。若要確認您已閱讀、了解並接受合約，請按一下***接受***按鈕。如果您不同意授權合約，請按一下***拒絕***按鈕，安裝程序隨後將立即終止。

AVG 隱私權原則

除了授權合約外，此安裝對話方塊還會為您提供進一步瞭解 AVG 隱私權原則的選項。您可以在對話方塊的左下角看到 ***AVG 隱私權原則***連結。按一下會將您重新導向至 AVG 網站 (http://www.avg.com/)，您可以在這裡找到 AVG Technologies 隱私權原則規範的全文。

控制按鈕

在第一個安裝對話方塊中，只有兩個控制按鈕可用：

- ***可列印版本*** - 按一下可列印 AVG 授權協議的完整版本。
- ***拒絕*** - 按一下此按鈕拒絕授權合約。安裝程序將立即結束。將不會安裝 **AVG Internet Security 2012**！
- ***上一步*** - 按一下此按鈕可返回一個步驟，回到前一個安裝對話方塊。
- ***接受*** - 按一下此按鈕確認您已閱讀、瞭解並接受授權合約。安裝將繼續進行，而您會前進一個步驟到下一個安裝對話方塊。

3.3. 啟動您的授權

在 ***啟動您的授權*** 對話方塊中，會請您將授權號碼填入提供的文字欄位中：

在哪裡可以找到授權號碼

銷售號碼位於您的 **AVG Internet Security 2012** CD 包裝盒上。授權號碼位於您在線上購買 **AVG Internet Security 2012** 後收到的確認電子郵件內。您必須完全按照顯示的號碼準確鍵入。若有提供電子形式的授權號碼 (*在電子郵件內*)，建議使用複製和貼上方法插入此號碼。

如何使用複製和貼上方法

使用 ***複製和貼上*** 方法將您的 **AVG Internet Security 2012** 授權號碼輸入程式可確保該號碼正確輸入。請遵循以下步驟：

- 開啟包含授權號碼的電子郵件。
- 在授權號碼的開頭按一下滑鼠左鍵，按住並拖曳滑鼠直到號碼的結尾，然後釋放滑鼠按鍵。號碼現在應該會反白。
- 按住 ***Ctrl*** 鍵，再按 ***C*** 鍵。如此會複製該號碼。
- 指向您要貼上已複製號碼的位置並按一下。
- 按住 ***Ctrl*** 鍵，再按 ***V*** 鍵。如此會將該號碼貼上您所選的位置。

控制按鈕

就跟大多數安裝對話方塊一樣，內有三個可用的控制按鈕：

- ***取消*** - 按一下此按鈕可立即結束安裝程序；將不會安裝 **AVG Internet Security 2012** ！
- ***上一步*** - 按一下此按鈕可返回一個步驟，回到前一個安裝對話方塊。
- ***下一步*** - 按一下此按鈕可繼續安裝並前進到下一個步驟。

3.4. 選取安裝類型

選取安裝類型對話方塊提供兩種安裝選項：***快速安裝***和***自訂安裝***。

快速安裝

對於大多數使用者，強烈建議固定使用標準快速安裝，它會以完全自動的模式，使用程式廠商預先定義的設定來安裝 **AVG Internet Security 2012** (包括 AVG 小工具)。這種組態不僅提供最大安全性，並且充分利用資源。在未來如果需要變更此組態，您隨時可以在 **AVG Internet Security 2012** 應用程式中直接操作。

在此選項中您可以看到兩個預確認的核取方塊，強烈建議核取兩個選項：

- ***我希望將 AVG Secure Search 設定為我的預設搜尋提供者*** - 保持核取該選項以確認您要使用 AVG Secure Search 引擎，其可緊密與 Link Scanner 合作，最大限度地保持線上安全性。
- ***我要安裝 AVG Security Toolbar*** - 保持核取該選項以安裝 AVG Security Toolbar，這可在您瀏覽網際網路時讓您處於最大安全性狀態。

按下 ***下一步***按鈕，前往下面的安裝 AVG Security Toolbar 對話方塊。

自訂安裝

自訂安裝應該只能在確實需要使用非標準設定來安裝 **AVG Internet Security 2012** 的情況下 (例如為了符合特定系統需求) 由經驗豐富的使用者使用。

如果您決定使用此選項，會在對話方塊中顯示一個稱為***目標資料夾***的新區段。在此，您應該指定安裝 **AVG Internet Security 2012** 的位置。依預設，**AVG Internet Security 2012** 將安裝在磁碟機 C: 上的程式檔案資料夾中 (如對話方塊中的文字欄位所示)。如果想變更此位置，請使用***瀏覽***按鈕顯示磁碟機結構，然後選取對應的資料夾。若要還原軟體廠商預先設定的預設目的地，請使用***預設值***按鈕。

然後按一下 ***下一步***按鈕可前進至自訂選項對話方塊。

控制按鈕

就跟大多數安裝對話方塊一樣，內有三個可用的控制按鈕：

- ***取消*** - 按一下此按鈕可立即結束安裝程序；將不會安裝 **AVG Internet Security 2012**！
- ***上一步*** - 按一下此按鈕可返回一個步驟，回到前一個安裝對話方塊。
- ***下一步*** - 按一下此按鈕可繼續安裝並前進到下一個步驟。

3.5. 自訂選項

自訂選項對話方塊可讓您設定詳細的安裝參數：

元件選取區段提供所有可安裝的 **AVG Internet Security 2012** 元件的概觀。如果預設設定不符合您的需求，您可以移除/新增特定元件。

不過，您只能從您購買的 AVG 版本所含的元件中選取！

亮顯***元件選取***清單中的任何項目，個別元件的簡短描述即會顯示在此區段的右側。如需各個元件功能的詳細資訊，請查閱本文件的元件概觀一章。若要還原軟體廠商預先設定的預設組態，請使用***預設值***按鈕。

控制按鈕

就跟大多數安裝對話方塊一樣，內有三個可用的控制按鈕：

- ***取消*** - 按一下此按鈕可立即結束安裝程序；將不會安裝 **AVG Internet Security 2012**！
- ***上一步*** - 按一下此按鈕可返回一個步驟，回到前一個安裝對話方塊。
- ***下一步*** - 按一下此按鈕可繼續安裝並前進到下一個步驟。

3.6. 安裝 AVG Security Toolbar

在***安裝 AVG Security Toolbar*** 對話方塊中，決定您是否要安裝 AVG Security Toolbar。如果您不變更預設設定，該元件將自動安裝到您的網際網路瀏覽器中 (*目前支援的瀏覽器包括 Microsoft Internet Explorer v. 6.0 或更高版本，以及 Mozilla Firefox v. 3.0 及更高版本*)，為您在上網時提供全面性的保護。

另外，您有權決定是否要選擇 *AVG Secure Search (powered by Google)* 作為您預設的搜尋提供者。如果是，請確保相應核取方塊均為勾選狀態。

控制按鈕

就跟大多數安裝對話方塊一樣，內有三個可用的控制按鈕：

- ***取消*** - 按一下此按鈕可立即結束安裝程序；將不會安裝 **AVG Internet Security 2012** ！
- ***上一步*** - 按一下此按鈕可返回一個步驟，回到前一個安裝對話方塊。
- ***下一步*** - 按一下此按鈕可繼續安裝並前進到下一個步驟。

3.7. 安裝進度

安裝進度對話方塊會顯示安裝程序的進度，完全無需任何操作：

安裝程序完成後，會自動將您重新導向至下一個對話方塊。

控制按鈕

此對話方塊中只有一個可用的控制按鈕 - ***取消***。您應該只在要停止執行中的安裝程序時，才使用此按鈕。請記住，在這種情況下將不會安裝 **AVG Internet Security 2012** ！

3.8. 安裝成功

安裝成功對話方塊確認您 **AVG Internet Security 2012** 已安裝並設定完成：

產品改進計劃

您可以在此對話方塊中決定是否要參與產品改進計劃 (*詳情請參閱 AVG 進階設定/產品改進計劃*一章)，該計劃會收集有關偵測到的威脅的匿名資訊，以提高整體網際網路安全性等級。如果您同意此陳述，請讓***我同意參與 AVG 2012 網路安全和產品改進計劃 ...***選項保持核取狀態 *(預設會確認選項)*。

電腦重新啟動

要完成安裝程序，您必須重新啟動您的電腦：選擇您是要***立即重新啟動***，還是要延緩此動作 - ***稍後重新啟動***。

4. 安裝之後

4.1. 產品註冊

完成 **AVG Internet Security 2012** 安裝之後，請在 AVG 網站 (http://www.avg.com/) 上註冊您的產品。註冊以後，您將能夠獲取 AVG 使用者帳戶的完整存取權限、AVG 更新電子報以及其他僅提供給註冊使用者的服務。

最簡單的註冊方法是直接從 **AVG Internet Security 2012** 使用者介面註冊。在主功能表中請選取說明/立即註冊項目。您將被重新導向至 AVG 網站 (http://www.avg.com/) 上的***註冊頁面。請遵循該頁面中提供的指示。***

4.2. 存取使用者介面

您可以使用下列幾種方式存取 AVG 主對話方塊：

- 連按兩下 AVG 系統匣圖示
- 連按兩下桌面上的 AVG 圖示
- 從功能表***開始/所有程式/ AVG 2012***

4.3. 掃描整台電腦

電腦病毒很有可能在安裝 **AVG Internet Security 2012** 之前便已傳輸到您的電腦中。因此，您必須執行掃描整台電腦以確定您的電腦沒有受到感染。第一次掃描可能花費的時間較長 *(約 1 小時)*，但建議您啟動該掃描以確保您的電腦不受威脅的損害。有關執行掃描整台電腦的說明，請參閱 AVG 掃描一章。

4.4. Eicar 測試

如果要確認 **AVG Internet Security 2012** 是否已正確安裝，您可以執行 EICAR 測試。

EICAR 測試是一種絕對安全的用來測試反病毒系統功能的標準方法。它可以安全地傳遞，因為它不是真的病毒，而且不包含任何病毒程式碼片段。大部分的產品都會將它當作病毒來回應 (*不過報告中通常會提到明確的名稱，像是 "EICAR-AV-Test"*)。您可以從 EICAR 網站下載 EICAR 病毒 (網址是 www.eicar.com)，您還會在網站中看到所有必要的 EICAR 測試資訊。

請試著下載 ***eicar.com*** 檔案，並將其儲存到您的本機磁碟。當您確認下載測試檔案後，Online Shield（*LinkScanner 元件的一部分*）就會立即以警告來回應。此通知表示 AVG 已經正確安裝在您的電腦上。

此外，您還可以到 http://www.eicar.com 網站下載壓縮版的 EICAR 病毒」(*例如 eicar_com.zip*)。Online Shield 允許您下載此檔案並將它儲存在本機磁碟中。但是當您嘗試解壓縮時，Resident Shield (*在 Anti-Virus 元件內*) 會偵測到該 病毒」。

如果 AVG 無法將 EICAR 測試檔案識別為病毒，您應該再次檢查程式組態！

4.5. AVG 預設組態

AVG Internet Security 2012 的預設組態 (*即應用程式在剛安裝好時的設定狀態*) 是由軟體廠商設定，所有元件和功能都經過調整以發揮最佳效能。

除非您確實需要這麼做，否則不要變更 AVG 組態！設定變更只能由經驗豐富的使用者來執行。

從特定的元件使用者介面可直接存取 AVG 元件設定以進行某些細微的編輯。如果您覺得需要變更 AVG 組態才能更符合您的需要，請移至 AVG 進階設定 :選取系統功能表項目***工具/進階設定***，然後在新開啟的 AVG 進階設定對話方塊中編輯 AVG 組態。

5. AVG 使用者介面

AVG Internet Security 2012 開啟時會顯示主視窗：

主視窗由若干區段構成：

- ***系統功能表*** *(視窗頂端的系統列)* 是標準巡覽方式，可讓您存取所有 **AVG Internet Security 2012** 元件、服務及功能 - 詳細資訊 >>
- ***安全性狀態資訊*** *(視窗上半部)* 提供有關 **AVG Internet Security 2012** 程式目前狀態的資訊 - 詳細資訊 >>
- ***在 Facebook 上加入我們*** *(視窗右上部分)* 按鈕可讓您加入 Facebook 上的 AVG 社群。但是，只有所有元件均完全發揮作用並且正常運作時才顯示此按鈕 *(有關如何辨識 AVG 元件的狀態，請參閱章節安全性狀態資訊)*
- ***快速連結*** *(視窗左側部分)*可讓您快速存取最重要及最常用的 **AVG Internet Security 2012** 工作 - 詳細資訊 >>
- ***我的應用程式*** *(視窗的左下部分)* 會開啟 **AVG Internet Security 2012**: LiveKive、Family Safety 和 PC Tuneup
- ***元件概觀*** *(視窗中間部分)* 提供 **AVG Internet Security 2012** 內所有已安裝元件的概觀 - 詳細資訊 >>
- ***系統匣圖示*** *(監視器右下角，位於系統匣中)* 指出 **AVG Internet Security 2012** 目前狀態 - 詳細資訊 >>
- ***AVG 小工具*** *(Windows 資訊看板，在 Windows Vista/7 中有支援)* 允許快速存取**AVG**

Internet Security 2012 內的掃描和更新 - 詳細資訊 >>

5.1. 系統功能表

系統功能表是用於所有 Windows 應用程式的標準巡覽區塊。它橫跨於 **AVG Internet Security 2012** 主視窗的最上方。請使用系統功能表存取特定的 AVG 元件、功能和服務。

系統功能表分為五個主要部分：

5.1.1. 檔案

- ***結束*** - 關閉 **AVG Internet Security 2012** 的使用者介面。但 AVG 應用程式會繼續在幕後執行，您的電腦將繼續受到保護！

5.1.2. 元件

系統功能表的元件項目包含可連至所有已安裝 AVG 元件的連結，可在使用者介面中開啟預設的對話方塊頁面：

- ***系統概觀*** - 切換到預設的使用者介面對話方塊，其中包含所有已安裝元件及其狀態的概觀
- ***Anti-Virus*** 會偵測系統內的病毒、間諜軟體、蠕蟲、特洛伊木馬程式、不要的執行檔或程式庫，並保護您免於惡意廣告軟體的侵擾 - 詳細資訊 >>
- ***LinkScanner*** 可保護您在搜尋和上網時免遭網路攻擊 - 詳細資訊 >>
- ***電子郵件保護***會檢查傳入電子郵件訊息是否為垃圾郵件，並封鎖網路釣魚攻擊或其他威脅 - 詳細資訊 >>
- ***Firewall*** 控制著每個網路連接埠上的所有通訊，保護您防禦惡意攻擊，並且會封鎖所有入侵嘗試 - 詳細資訊 >>
- ***Anti-Rootkit*** 會掃描是否有惡意 rootkit 隱藏在應用程式、驅動程式或程式庫內 - 詳細資訊 >>
- ***系統工具***提供 AVG 環境及作業系統的詳細摘要資訊 - 詳細資訊 >>
- ***PC 分析程式***提供有關您電腦狀態的資訊 - 詳細資訊 >>
- ***Identity Protection*** 不斷地保護您的數位資產免遭新興和不明威脅的侵害 - 詳細資訊 >>
- ***遠端管理***只有在您於安裝程序期間指定安裝此元件時，才會顯示在 AVG Network Edition 中

5.1.3. 歷程記錄

- 掃描結果 - 切換到 AVG 測試介面，也就是切換至掃描結果概觀對話方塊
- Resident Shield 偵測 - 開啟包含 Resident Shield

- E-mail Scanner 偵測 - 開啟包含電子郵件保護元件偵測為危險內容的郵件訊息附件概觀的對話方塊

- Online Shield 結果 - 開啟包含 LinkScanner 元件內的 Online Shield 服務偵測到的威脅概觀的對話方塊

- 病毒隔離區 - 開啟隔離區域的介面 (病毒隔離區), AVG 會將所有偵測到的因故無法自動修復的受感染檔案移到隔離區中。將受感染的檔案隔離到此隔離區後，您電腦的安全將得到保障，同時會儲存受感染檔案以供日後修復之用

- 事件歷程記錄 - 開啟包含有所有記錄的 **AVG Internet Security 2012** 動作概觀的歷程記錄介面

- Firewall 記錄 - 在包含所有 Firewall 動作詳細資訊概觀的記錄標籤上開啟 Firewall 設定介面

5.1.4. 工具

- 掃描電腦 - 啟動完整的電腦掃描。

- 掃描所選資料夾... - 切換至 AVG 掃描介面並允許您在電腦的樹狀目錄結構中定義要掃描哪些檔案和資料夾。

- ***掃描檔案...*** - 可讓您按測試需求在一個特定檔案上執行掃描。按一下此選項開啟包含磁碟樹狀結構的新視窗。選擇所需的檔案，然後確認啟動掃描。

- 更新 - 自動啟動 **AVG Internet Security 2012** 的更新程序。

- ***從目錄更新...*** - 從位於本機磁碟上指定資料夾的更新檔案執行更新程序。但是，只建議在發生網際網路連線中斷等緊急情況下才使用此選項 (*例如，您的電腦受到感染，並與網際網路中斷連線；您的電腦連線至無法存取網際網路的網路等*)。在新開啟的視窗中，選取您先前放置更新檔案的資料夾，然後啟動更新程序。

- 進階設定... - 開啟 AVG 進階設定對話方塊，您可以在這裡編輯 AVG Internet Security 2012 組態。通常建議保留由軟體廠商定義的應用程式之預設設定。

- Firewall 設定... - 開啟一個獨立的對話方塊，用於 Firewall 元件的進階組態。

5.1.5. 說明

- ***內容*** - 開啟 AVG 說明檔案

- ***獲取支援*** - 在客戶支援中心頁面開啟 AVG 網站 (http://www.avg.com/)

- ***您的 AVG 網頁*** - 開啟 AVG 網站 (http://www.avg.com/)

- ***關於病毒和威脅*** - 開啟線上病毒大全，您可在其中查找有關已知病毒的詳細資訊

- ***重新啟動*** - 開啟***啟動 AVG*** 對話方塊，其中包含您在安裝程序的個人化 AVG 對話方塊中輸入的資料。在此對話方塊中，您可以輸入授權號碼以取代銷售號碼 (*您安裝 AVG 所使用的號碼*)，或取代舊的授權號碼 (*例如，當升級至新的 AVG 產品時*)。

- ***立即註冊*** - 連線到 AVG 網站 (http://www.avg.com/) 的註冊頁面。請填入您的註冊資料，只有已註冊 AVG 產品的客戶才能獲得免費的技術支援。

注意：*如果使用的是* **AVG Internet Security 2012** *試用版，後兩項會顯示為****立即購買****及****啟動****，讓您可立刻購買完整版的授權。對於使用銷售號碼安裝的* **AVG Internet Security 2012**，*這些選項會顯示為****註冊****及****啟動****。*

- ***關於 AVG*** - 開啟***資訊***對話方塊，該對話方塊包含六個標籤，提供有關程式名稱、程式和病毒庫版本、系統資訊、授權合約和 ***AVG Technologies CZ***.聯絡資訊的資料。

5.1.6. 支援

支援連結會開啟一個新的***資訊***對話方塊，當中包含您在嘗試尋找協助時可能需要的各種資訊。該對話方塊包括有關已安裝 AVG 程式 (*程式/資料庫版本*) 的基本資料、授權詳細資料，以及快速支援連結清單。

資訊對話方塊分成六個標籤：

版本標籤分成三個區段：

- ***支援資訊*** - 提供有關 **AVG Internet Security 2012** 版本、病毒庫版本、Anti-Spam 資料庫版本，以及 LinkScanner 版本等資訊。

- ***使用者資訊*** - 提供有關授權使用者和公司的資訊。

- ***授權詳細資料*** - 提供有關授權的資訊 (*產品名稱*、*授權類型*、*授權數量*、*到期日和席位數*)。您也可以使用此區段中的***註冊***連結在線上註冊 **AVG Internet Security**

2012，如此可讓您獲取完整的 AVG 技術支援。另外，使用***重新啟動***連結可開啟 ***啟動 AVG*** 對話方塊：將授權號碼填入個別的欄位來取代銷售號碼 *(在 AVG Internet Security 2012 安裝期間所用的號碼)*，或是變更您目前的授權號碼 *(例如當升級到更高版本的 AVG 產品時)*。

您可以在***程式***標籤上找到 **AVG Internet Security 2012** 程式檔案版本，以及用於該產品的第三方代碼等相關資訊：

系統標籤提供作業系統的參數清單 *(處理器類型、作業系統及其版本、組建號碼、使用的 Service Pack、總記憶體大小以及可用的記憶體大小)*:

您可以在***授權合約***標籤上閱讀您與 AVG Technologies 之間的授權合約全文：

支援標籤會顯示聯絡客戶支援所有可能管道的清單。其中也會提供 AVG 網站 (http://www.avg.com/)、AVG 論壇、常見問題集...等的連結。此外，您還可以找到聯絡客戶支援小組時可能會用到的資訊：

聯絡人索引標籤提供 AVG Technologies 所有聯絡人，以及 AVG 當地代表和經銷商聯絡人的清單：

5.2. 安全性狀態資訊

安全性狀態資訊區段位於 **AVG Internet Security 2012** 主視窗的上半部。您始終可以在這個區段找到有關 **AVG Internet Security 2012** 目前安全性狀態的資訊。請參閱此區段中可能描述的圖示概觀及其含義：

 - 綠色圖示表示 ***AVG Internet Security 2012 運作完全正常***。您的電腦受到完全保護，已更新至最新狀態，且所有安裝的元件都運作正常。

 - 黃色圖示警告您有一個或多個元件設定錯誤，您必須檢查其屬性/設定。**AVG Internet Security 2012** 中沒有嚴重問題，而且您可能基於某個原因已決定關閉某個元件。您仍然受到保護！但是，請檢查問題元件的設定！該元件的名稱會在***安全性狀態資訊***區段提供。

如果您因故決定忽略某元件的錯誤狀態，也會顯示黃色圖示。***忽略元件狀態***選項可從 **AVG Internet Security 2012** 主視窗的元件概觀中個別元件圖示上的內容功能表存取 (*以滑鼠右鍵按一下開啟*)。選取此選項表示您知道該元件的錯誤狀態，但基於某種原因，您希望 **AVG Internet Security 2012** 保持這種狀態，且不願意再收到系統匣圖示的警告。在特定情形下您可以使用此選項，但是強烈建議您儘量關閉***忽略元件狀態***選項。

或者，如果您的 **AVG Internet Security 2012** 需要重新啟動電腦 (***需要重新啟動***)，也會顯示黃色圖示。請注意此敬告並使用***立即重新啟動***按鈕重新啟動您的 PC。

 - 橙色圖示表示 ***AVG Internet Security 2012 處於緊急狀態***！一或多個元件不能正常運作，且 **AVG Internet Security 2012** 無法保護您的電腦。請立即檢查並修復報告的問題。如果您自己無法修復錯誤，請與 AVG 技術支援團隊聯絡。

如果 AVG Internet Security 2012 未設為最佳效能，則安全性狀態資訊旁邊會出現一個名為「修復」的新按鈕 (如果問題包含多個元件，則會顯示「全部修復」)。按一下該按鈕可啟動程式簽出和組態的自動程序。這是將 AVG Internet Security 2012 設定為最佳效能並達成最高安全性等級的簡單方法！

強烈建議您檢查安全性狀態資訊，如果報告指出有任何問題，請立即前往並試著解決。否則，您的電腦會處於危險中！

注意：*AVG Internet Security 2012 狀態資訊也可隨時從系統匣圖示中取得。*

5.3. 快速連結

快速連結位於 **AVG Internet Security 2012** 使用者介面的左側。這些連結可讓您立即存取最重要且最常用的應用程式功能，亦即掃描和更新。快速連結可從使用者介面的所有對話方塊存取：

快速連結以圖形的方式分成三個區段：

- ***立即掃描*** - 預設情況下，該按鈕會提供上次啟動的掃描的資訊 *(亦即掃描類型和上次啟動日期)*。按一下***立即掃描***命令可再次啟動相同的掃描。如果您希望啟動不同的掃描，按一下***掃描選項***連結。如此會開啟 AVG 掃描介面，您可以在這裡執行掃描、排程掃描，或編輯其參數。*(詳細資訊請參閱AVG 掃描一章)*
- ***掃描選項*** - 使用此連結可從任何目前開啟的 AVG 對話方塊切換到具有所有已安裝元件概觀的預設視窗。*(詳細資訊請參閱元件概觀一章)*
- ***立即更新*** - 該連結提供上次啟動的更新的日期和時間。按一下此按鈕可立即執行更新程序，並追蹤其進度。*(詳細資訊請參閱 AVG 更新)一章*

快速連結隨時都可從 AVG 使用者介面存取。一旦您使用快速連結執行特定程序，無論掃描或更新，應用程式都將切換至新對話方塊，但快速連結仍然可用。此外，執行中的程序也會在巡覽介面中進一步以圖形方式描述，讓您全權控制當時 **AVG Internet Security 2012** 內正在執行的所有已啟動的程序。

5.4. 元件概觀

元件概觀區段

元件概觀區段位於 **AVG Internet Security 2012** 使用者介面的中央。此區域分成兩個部分：

- ***所有已安裝元件的概觀***包含所有已安裝元件的圖形面板。每個面板都會以該元件的圖示標記，並且提供個別元件當時處於作用中或非作用中狀態的相關資訊。
- ***元件的說明***位於此對話方塊的底端。說明會簡短解釋該元件的基本功能。另外也會提供所選元件目前狀態的相關資訊。

已安裝元件的清單

在 **AVG Internet Security 2012** 中，***元件概觀***區段包含以下元件的資訊：

- ***Anti-Virus*** 會偵測系統內的病毒、間諜軟體、蠕蟲、特洛伊木馬程式、不要的執行檔或程式庫，並保護您免於惡意廣告軟體的侵擾 - 詳細資訊 >>
- ***LinkScanner*** 會保護您在搜尋和上網時免遭網路攻擊 - 詳細資訊 >>

- ***電子郵件保護***會檢查傳入電子郵件訊息是否為垃圾郵件，並封鎖網路釣魚攻擊或其他威脅 - 詳細資訊 >>
- ***Firewall*** 控制著每個網路連接埠上的所有通訊，保護您防禦惡意攻擊，並且會封鎖所有入侵嘗試 - 詳細資訊 >>
- ***Anti-Rootkit*** 會掃描是否有惡意 rootkit 隱藏在應用程式、驅動程式或程式庫內 - 詳細資訊 >>
- ***系統工具***提供 AVG 環境及作業系統的詳細摘要資訊 - 詳細資訊 >>
- ***PC 分析程式***提供有關您電腦狀態的資訊 - 詳細資訊 >>
- ***Identity Protection*** 不斷地保護您的數位資產免遭新興和不明威脅的侵害 - 詳細資訊 >>
- ***遠端管理***只有在您於安裝程序期間指定安裝此元件時，才會顯示在 AVG Network Edition 中

可存取的動作

- ***將滑鼠移至任何元件的圖示上方***即可在元件概觀中反白該元件。與此同時，該元件的基本功能說明會出現在使用者介面的底端。
- ***按一下任何元件的圖示***可開啟該元件自己的介面，其中包含基本統計資料的清單。
- ***在元件的圖示上方按右鍵***可展開內含數個選項的內容功能表：
  - ***開啟*** - 按一下此選項可開啟該元件自己的對話方塊 *(就跟按一下該元件的圖示一樣)*。
  - ***忽略元件狀態*** - 選取此選項表示您知道元件的錯誤狀態，但基於某種原因，您希望保留此狀態，並且不願意再收到系統匣圖示的警告。
  - ***在進階設定中開啟 ...*** - 此選項僅適用於一些元件，亦即提供可進行進階設定的元件。

5.5. 系統匣圖示

AVG 系統匣圖示 *(在監視器右下角的 Windows 工作列上)* 會指出 **AVG Internet Security 2012** 的目前狀態。無論 **AVG Internet Security 2012** 的使用者介面是開啟還是關閉，該圖示都會一直顯示在系統匣中：

AVG 系統匣圖示顯示

- 以全彩顯示、未加元素的圖示表示所有 **AVG Internet Security 2012** 元件皆處於作用中狀態，且運作完全正常。不過，圖示也可能在其中一個元件未完全正常運作但使用者決定忽略元件狀態時以這種方式顯示.*(確認忽略元件狀態選項表示您知道該元件的錯誤狀態但基於某種原因而希望保持此狀態，而且您不想要收到有關此狀況的警告)*。

- 含驚嘆號的圖示表示有一個元件 *(甚或更多元件)* 處於錯誤狀態。請務必注意這類警告，並試著移除設定不當的元件的組態問題。若要在元件的組態中執行變更，請連按兩下系統匣圖示以開啟應用程式使用者介面。有關哪些元件處於錯誤狀態的詳細資訊，請參閱安全性狀態資訊一節。

- 系統匣圖示此外也可能以全彩、加上閃爍和旋轉的光線顯示。此圖形版本象徵著正啟動的更新程序。

- 以全彩圖示、加上箭號的替代顯示表示正在執行 **AVG Internet Security 2012** 掃描。

AVG 系統匣圖示資訊

AVG 系統匣圖示會進一步通知 **AVG Internet Security 2012** 內目前的活動，以及程式中可能的狀態變更 *(例如自動啟動排程掃描或更新、Firewall 設定檔切換元件狀態變更、發生錯誤狀態等)*，其方法是從系統匣圖示彈出一個快顯視窗：

可從 AVG 系統匣圖示存取的動作

AVG 系統匣圖示也可以用作為存取 **AVG Internet Security 2012** 使用者介面的快速連結，只要連按兩下該圖示即可。用滑鼠右鍵按一下系統匣圖示可開啟一個簡要的內容功能表，內含以下選項：

- ***開啟 AVG 使用者介面*** - 按一下此選項可開啟 **AVG Internet Security 2012** 的使用

者介面。

- ***暫時停用 AVG 保護*** - 此選項可讓您一次關閉 **AVG Internet Security 2012** 提供的所有安全保護。請記住，除非迫不得已，請勿使用此選項！在大多數情況下，不必在安裝新軟體或驅動程式之前停用 **AVG Internet Security 2012**，即使安裝程式或軟體精靈建議首先關閉正在執行的程式和應用程式以確保安裝程序期間不會出現意外中斷，也沒有此必要。如果您確實不得不暫時停用 **AVG Internet Security 2012**，則必須在完成其他工作後立即重新啓用它。如果您在反病毒軟體停用時連線至網際網路或網路，您的電腦可能很容易受到攻擊。

- ***Firewall*** - 按一下此選項可開啟 Firewall 設定選項的內容功能表，您可以在這裡編輯主要的參數：Firewall 狀態 (*Firewall 已啟用/Firewall 已停用/緊急模式*)、遊戲模式切換和 Firewall 設定檔。

- ***掃描*** - 按一下此選項可開啟 預先定義的掃描 的內容功能表 (*掃描整台電腦*和*掃描特定檔案或資料夾*)，然後選取所需的掃描，掃描會立即啟動。

- ***執行中的掃描 ...***- 此項目只有在您電腦上目前有掃描正在執行時才會顯示。您之後可以設定此掃描的優先順序，或是選擇停止或暫停執行中的掃描。接下來，可存取以下動作：*設定所有掃描的優先順序*、*暫停所有掃描*或*停止所有掃描*。

- ***執行 PC 分析程式*** - 按一下此選項可啟動 PC 分析程式 元件。

- ***立即更新*** - 可啟動即時更新。

- ***說明*** - 在開始頁開啟說明檔案。

5.6. AVG Advisor

AVG Advisor 是一種效能功能，可監視電腦上所有執行的程序是否有問題，並提供如何避免問題的提示。***AVG Advisor*** 可在系統匣中以滑動快顯的形式顯示。

AVG Advisor 可在以下情況下出現：

- 您使用的 Internet 瀏覽器記憶體用盡，這可減慢您的工作速度 (*AVG Advisor 僅支援 Internet Explorer、Chrome、Firefox、Opera 和 Safari 瀏覽器*)；

- 您電腦中正執行的程序消耗了太多記憶體，減弱了電腦效能；

- 您的電腦將自動連接至未知的 WiFi。

在這些情況下，***AVG Advisor*** 會通知您可能發生的問題，並提供衝突程序或應用程式的名稱或圖示。此外，***AVG Advisor*** 將建議要採取的步驟以避免可能發生的問題。

5.7. AVG 小工具

AVG 小工具 顯示在 Windows 桌面上 (*Windows 資訊看板*)。此應用程式只在 Windows Vista 和 Windows 7 作業系統中有支援。***AVG 小工具***提供對最重要的 **AVG Internet Security 2012** 功能的立即存取，亦即掃描和更新功能：

快速存取掃描和更新

必要時，***AVG 小工具***允許您立即啟動掃描或更新：

- ***立即掃描*** - 按一下***立即掃描***連結即可直接開始掃描整台電腦。您可以在小工具的替代使用者介面觀察掃描程序的進度。會有簡短的統計資料概觀提供有關掃描的物件數、偵測到的威脅，以及修復的威脅等資訊。您始終可以在掃描期間暫停 或停止 掃描程序。有關該掃描結果的詳細資料，請參閱標準掃描結果概觀對話方塊，您可透過***顯示詳細資料***選項直接從小工具開啟 *(資訊看板小工具掃描下將列出個別的掃描結果)*。

- ***立即更新*** - 按一下***立即更新***連結**AVG Internet Security 2012**即可直接從小工具內啟動更新：

社交網路存取

AVG 小工具也提供將您連線到主要社交網路的快速連結。使用個別的按鈕即可連接到 Twitter、Facebook 或 LinkedIn 中的 AVG 社群：

- ***Twitter 連結*** - 開啟新的 ***AVG 小工具***介面，提供 AVG 在 Twitter 張貼的最新摘要概觀。遵循***檢視所有 AVG Twitter 摘要*** 連結即可在新視窗開啟您的網際網路瀏覽器；並且會將您直接重新導向至 Twitter 網站，特別是導向專門提供 AVG 相關新聞的頁面：

- ***Facebook 連結*** - 在 Facebook 網站上開啟您的網際網路瀏覽器，特別是開啟在 ***AVG 社群***頁面。

- ***LinkedIn*** - 此選項僅在網路安裝中可用 (*亦即使用 AVG Business Editions 其中一種授權安裝 AVG*)，而且它會從 LinkedIn 社交網路中將 Internet 瀏覽器開啟到 ***AVG SMB Community*** 網站.

可透過小工具存取的其他功能

- ***PC 分析程式*** - 開啟 PC 分析程式 元件中的使用者介面，並立即開始分析。

- ***搜尋方塊*** - 輸入關鍵字並且使用您的預設網頁瀏覽器在新開啟的視窗立即取得搜尋結果。

6. AVG 元件

6.1. Anti-Virus

Anti-Virus 元件是 **AVG Internet Security 2012** 的基石，它結合了安全性程式的數項基本功能：

- 掃描引擎
- 常駐保護
- Anti-Spyware 保護

6.1.1. 掃描引擎

掃描引擎是 ***Anti-Virus*** 元件的基礎，會掃描所有檔案和檔案活動 *(開啟/關閉檔案等)* 是否有已知病毒。任何偵測到的病毒都會被封鎖以阻止它採取任何動作，接著會清除或隔離在病毒隔離區中。

AVG Internet Security 2012 保護的重要功能是禁止任何已知病毒在電腦上執行！

偵測方法

大部分的反病毒軟體也會使用啟發法掃描，這種掃描方法會掃描檔案中的典型病毒特性，即所謂的病毒簽名。這表示反病毒掃描程式可以偵測新的不明病毒，只要新病毒包含現有病毒的一些典型特性。***Anti-Virus*** 採用以下偵測方法：

- *掃描* - 搜尋具備特定病毒特性的字元字串
- *啟發法分析* - 在虛擬電腦環境中，對掃描物件的指令進行動態模擬
- *一般偵測* - 偵測特定病毒/病毒群組的指令特性

單靠一種技術可能無法充分偵測或識別病毒，因此 ***Anti-Virus*** 結合了多種技術來確保您的電腦不受病毒侵擾。**AVG Internet Security 2012** 也能夠分析和偵測系統中可能存在的垃圾可執行應用程式或 DLL 程式庫。我們將這類威脅稱為 「潛在垃圾程式」*(各種間諜軟體、廣告軟體等等)*。此外，**AVG Internet Security 2012** 會掃描您的系統登錄中是否有可疑項目、Temporary Internet Files 和追蹤 Cookie，並允許您以處理其他任何感染的方式來處理所有潛在的有害項目。

AVG Internet Security 2012 為您的電腦提供不間斷的保護！

6.1.2. 常駐保護

AVG Internet Security 2012 以所謂的常駐保護的形式提供持續的保護。***Anti-Virus*** 元件會掃描開啟、儲存或複製的每個檔案 *(包括特定副檔名或完全無副檔名的檔案)*。它會防衛電腦、卸除式媒體 (*快閃磁碟等*) *的系統區域*。). 在存取的檔案中發現病毒時，它會停止目前正在執行的作業，並會禁止病毒自行啟動。一般來說，您甚至不會注意到這個程序，因為常

駐保護是在 背景執行」。只有在發現威脅時，您才會收到通知，***Anti-Virus*** 與此同時會封鎖威脅的啟動並加以移除。

常駐保護會在電腦啟動時載入電腦的記憶體，因此務必隨時保持其開啟狀態！

6.1.3. Anti-Spyware 保護

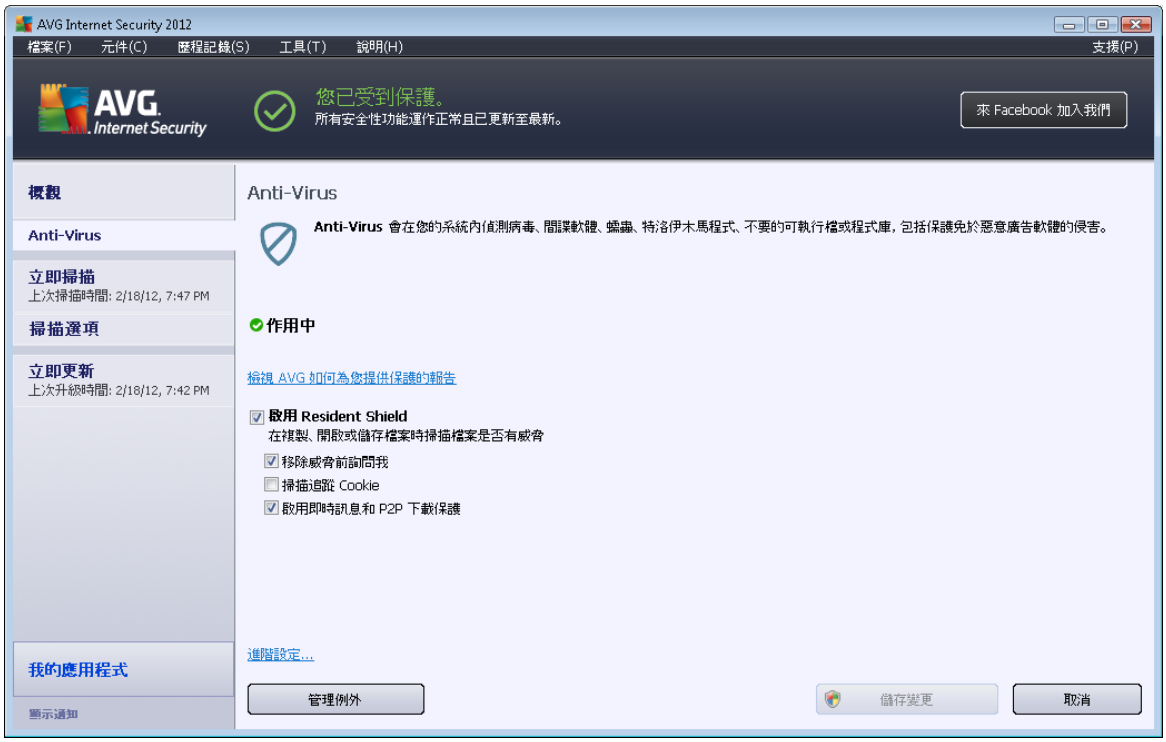
Anti-Spyware 包含一個用於識別已知類型的間諜軟體定義的間諜軟體資料庫。AVG 間諜軟體專家致力於在新的間諜軟體模式成形時，隨即加以識別和描述，並將定義新增到資料庫。透過更新程序，這些新的定義會下載到您的電腦，這樣您就會始終受到可靠的保護，即使是最新的間諜軟體類型也不必擔心。***Anti-Spyware*** 可讓您徹底掃描電腦是否有惡意軟體/間諜軟體。它還會偵測睡眠中和非使用中的惡意軟體，即已下載但尚未啟動的惡意軟體。

什麼是間諜軟體？

間諜軟體通常被定義為惡意軟體的一種，即在使用者不知情或未經其同意的情況下從使用者電腦收集資訊的軟體。某些間諜軟體應用程式也可能是有意安裝，且往往包含廣告、快顯視窗或各式各樣令人不悅的軟體。目前，最常見的感染來源是含有潛在危險內容的網站。其他傳輸方式也很普遍，例如透過蠕蟲或病毒傳播的電子郵件或傳輸。最重要的防護措施就是使用永遠開啟的幕後掃描程式 ***Anti-Spyware***，這是一種常駐防護，當您執行應用程式時，它會在幕後掃描應用程式。

6.1.4. Anti-Virus 介面

Anti-Virus 元件的介面提供該元件功能的簡短說明，該電腦狀態的相關資訊 *(作用中)*，以及該元件的基本組態選項：



組態選項

該對話方塊提供 ***Anti-Virus*** 元件內可用功能的一些基本組態選項。接下來您可以找到以下項目的簡短說明：

- ***檢視 AVG 如何為您提供保護的線上報告*** - 該連結會將您導向 AVG 網站上的特定網頁 (http://www.avg.com/)。您在該頁面上可以找到在指定的一段時間內，電腦上執行的所有 **AVG Internet Security 2012** 活動的詳細統計資料概觀。
- ***啟用 Resident Shield*** - 此選項可讓您輕鬆開啟/關閉常駐保護。Resident Shield 會在複製、開啟或儲存檔案的同時對其進行掃描。當偵測到病毒或任何類型的威脅時，將立即向您發出警告。預設會開啟該功能，也建議您將它保持開啟狀態！常駐保護開啟時，您可進一步決定對可能偵測到的感染應該做何處理：
  - ***移除威脅前詢問我*** - 保持核取此選項，以確認每次將偵測到的威脅移至病毒隔離區之前詢問您。此選擇不會對安全性層級產生影響，僅反映您的偏好。
  - ***掃描追蹤 Cookie*** - 與前個選項無關，您可以決定是否要掃描追蹤 Cookie。*(Cookie 是伺服器傳送給網頁瀏覽器的文字封包，之後每當該瀏覽器存取伺服器時，都會將這些文字封包原封不動地傳回給伺服器。HTTP cookie 用於驗*

證、追蹤和維護使用者的特定資訊，如站點偏好或電子購物車內容。)在特定情況下，您可開啟此選項以獲得最高安全性層級，但在預設情況下，此選項為關閉狀態。

- ***啟用即時訊息保護*** - 如果您希望確認即時訊息通訊(*即 ICQ、MSN Messenger、...*) 沒有病毒感染，請核取此項目。

- ***進階設定***... - 按一下該連結會將您重新導向至**AVG Internet Security 2012 的**進階設定內個別的對話方塊。您可以在該處詳細編輯該元件的組態。但是，請注意，所有元件的預設組態是為了使 **AVG Internet Security 2012** 提供最佳效能和最高安全性而設定。除非您有充分的理由進行變更，否則建議您保持預設組態！

控制按鈕

您可以在對話方塊中使用以下控制按鈕：

- ***管理例外*** - 開啟名為 ***Resident Shield - 例外***的新對話方塊。Resident Shield 掃描的例外組態也可以遵循以下順序從主功能表存取：進階設定/Anti-Virus/Resident Shield/例外 *(請參閱個別章節取得詳細說明)*。您可以在對話方塊中指定應該排除在 Resident Shield 掃描之外的檔案和資料夾。除非必要，否則我們強烈建議不要排除任何項目！該對話方塊提供下列控制按鈕：

  - *新增路徑* –指定要從掃描排除的目錄*(或多個目錄)*，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄。
  - *新增檔案* –指定要從掃描排除的檔案，方法是從本機磁碟巡覽樹狀目錄逐個選取檔案。
  - *編輯項目* –允許您編輯所選檔案或資料夾的指定路徑。
  - *移除項目* –允許您從清單中刪除所選檔案的路徑。
  - *編輯清單* - 允許您在新對話方塊中編輯整個已定義的例外清單，作用就跟標準文字編輯器一樣。

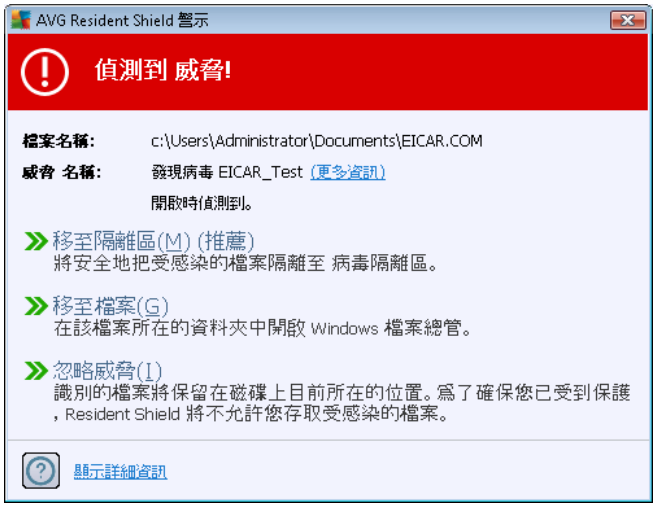
- ***套用*** - 儲存在此對話方塊中對該元件的設定所做的全部變更，並返回的**AVG Internet Security 2012**使用者介面(*元件概觀*)。

- ***取消*** - 取消在此對話方塊中對該元件的設定所做的全部變更。不會儲存任何變更。您將返回 **AVG Internet Security 2012 的主要**使用者介面(*元件概觀*)。

6.1.5. Resident Shield 偵測

偵測到的威脅！

Resident Shield 會在複製、開啟或儲存檔案的同時對其進行掃描。當偵測到病毒或任何類型的威脅時，將立即透過以下對話方塊向您發出警告：



您可以在此警告對話方塊中找到有關被偵測並指派為受感染檔案的資料 (*檔案名稱*)、發現的感染名稱 (*威脅名稱*)，以及病毒大全的連結，您可以在此處找到有關偵測到的感染的詳細資訊，如果已知的話 (*更多資訊*)。

此外，您還必須決定現在應該採取的動作。有幾個替代選項可用。***注意，根據特定條件 (受感染檔案的類型及其位置)，並非所有選項都可以使用！***

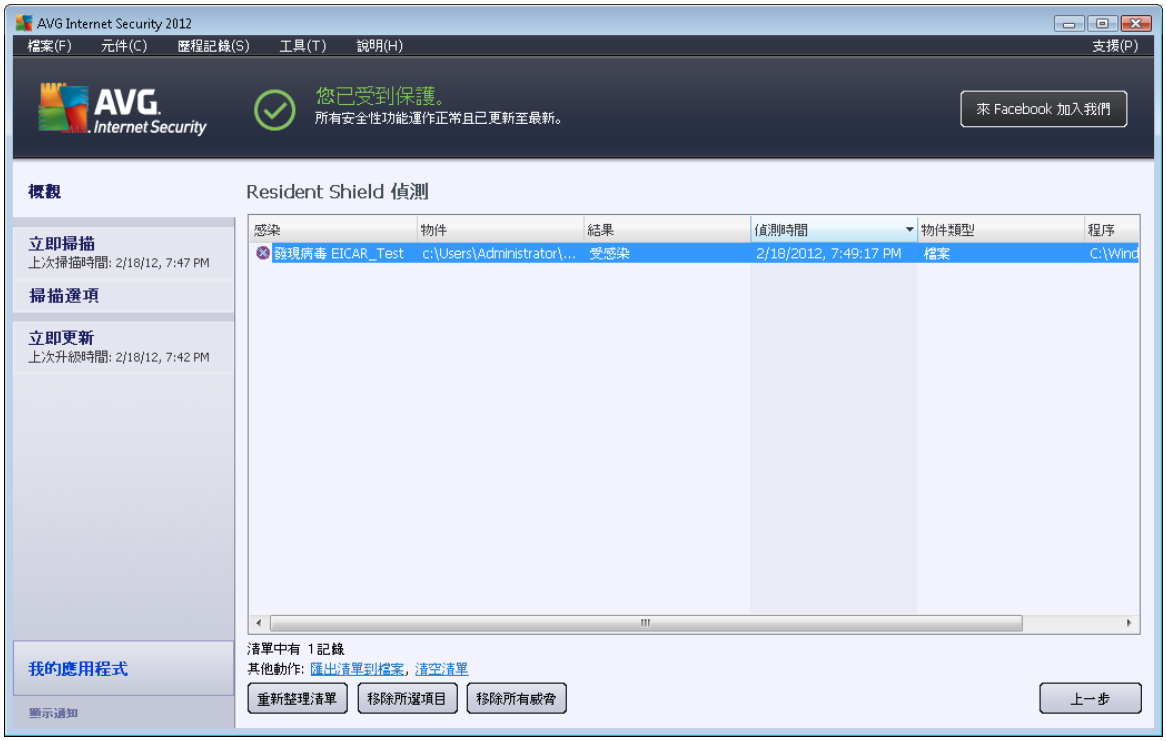
- ***修復*** - 此按鈕只有在偵測到的感染可以修復時才會出現。它隨後會將它從檔案中移除，並將檔案還原為原始狀態。如果檔案本身是病毒，請使用此功能來刪除它 (*亦即移至病毒隔離區*)
- ***移至隔離區 (建議)*** - 病毒將移至病毒隔離區
- ***移至檔案*** - 此選項會將您重新導向至可疑物件的確切位置 (*開啟新的 Windows 檔案總管視窗*)
- ***忽略威脅*** – 除非您確實需要這麼做，否則我們強烈建議不要使用此選項！

注意：*偵測到的物件大小可能會超過病毒庫中的可用空間限制。如果是這種情況，在您嘗試將偵測到的物件移到病毒庫時，會快顯一個警告訊息，告知您該問題。但是，病毒庫大小是可以編輯的。病毒庫大小定義為硬碟實際大小的一個可調比例。若要增加病毒庫的大小，請移至 AVG 進階設定的病毒庫對話方塊中，透過「限制病毒庫大小」選項進行調整。*

您可以在對話方塊的底端找到***顯示詳細資訊連結*** - 按一下該連結可開啟快顯視窗，當中會顯示當偵測到感染時正在執行的程序的資訊，以及程序的識別。

Resident Shield 偵測概觀

您可以在 Resident Shield 偵測對話方塊中找到 ***Resident Shield 偵測***到的所有威脅的整體概觀，此對話方塊可從系統功能表選項歷程記錄/Resident Shield 偵測存取：



Resident Shield 偵測提供經過 Resident Shield 偵測並評估為危險內容，並已修復或移至病毒隔離區之物件的概觀。針對每個偵測到的物件，提供以下資訊：

- ***感染*** - 偵測到的物件的說明 (甚至可能包含名稱)
- ***物件*** - 物件位置
- ***結果*** - 對偵測到的物件執行的動作
- ***偵測時間*** - 偵測到物件的日期和時間
- ***物件類型*** - 偵測到的物件的類型
- ***程序*** - 是執行什麼動作引致該潛在危險物件，並使其被偵測出來

在對話方塊底端的清單下方，您可以找到有關上述偵測到的物件總數的資訊。然後您可將偵測到的物件的整個清單匯出至檔案中 (***將清單匯出到檔案***並刪除有關偵測到的物件的所有項目 (***清空清單***)。***重新整理清單***按鈕將更新 ***Resident Shield*** 偵測結果的清單。***上一步***按鈕會將您切換回預設的 AVG 主對話方塊 (*元件概觀*)。

6.2. LinkScanner

LinkScanner 會保護您抵禦網路上不斷增加且 短暫出沒」的威脅。這些威脅可能藏匿在任一類型網站內，包括政府機構到大型著名的品牌公司，到小型企業都有可能，而且它們極少在這些網站逗留超過 24 個小時。***LinkScanner*** 會透過分析您正在檢視的任何網頁上所有連結背後的網頁，確定它們在最重要的時刻 - 也就是您即將按一下該連結時 - 是安全的，藉此來保護您的電腦。

LinkScanner 不適用於伺服器平台！

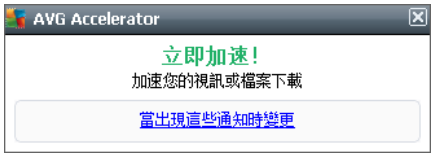
LinkScanner 技術包含以下主要功能：

- Search-Shield 包含已知危險的網站清單 (*URL 位址*)。當使用 Google、Yahoo! JP、eBay、Twitter、Digg、SlashDot、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask 和 Seznam 搜尋時，搜尋的所有結果都會根據此清單進行檢查，並顯示一個裁決圖示 *(對於 Yahoo! 搜尋結果，僅會顯示 「惡意探索網站」裁決圖示)*)。

- Surf-Shield 會掃描您正在瀏覽之網站的內容，無論網站位址為何。即使 Search-Shield *未偵測出某個網站 (例如，當一個新的惡意網站成形，或當之前安全的網站現在包含了某個惡意軟體時)*，當您嘗試造訪該網站時，Surf-Shield 也會偵測到它並加以封鎖。

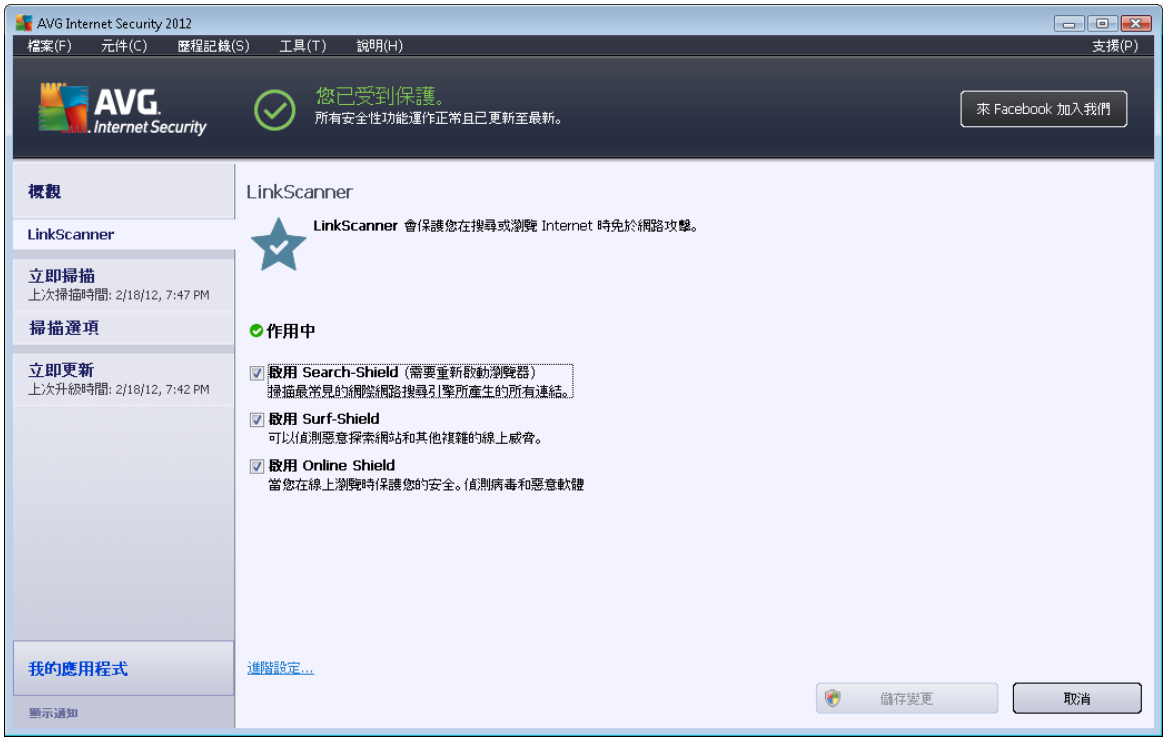
- Online Shield 會在您上網時提供即時保護。它甚至會在瀏覽的網頁顯示在您的網頁瀏覽器或下載到電腦前，掃描其內容，以及其中可能內含的檔案。Online Shield 會偵測您即將瀏覽的頁面內含的病毒和間諜軟體，並且會立即停止下載，防止任何威脅危及您的電腦。

- ***AVG 加速器***使線上視訊的播放更順暢，也更方便進行其他下載。當進行視訊加速程序時，會透過系統匣快顯視窗通知您。



6.2.1. LinkScanner 介面

LinkScanner 元件介面提供該元件功能的簡短說明，以及有關其目前狀態 *(作用中)* 的資訊：



對話方塊底端有一些可用的元件基本組態：

- ***啟用 Search-Shield*** - (*預設為開啟*) :如果您有充分的理由關閉 Search Shield 功能，請取消核取該方塊。
- ***啟用 Surf-Shield*** - (*預設為開啟*) :在存取惡意探索站點時，提供主動 (*即時*) 保護。當使用者透過網頁瀏覽器 (*或任何其他使用 HTTP 的應用程式*) 存取已知惡意站點時，其連線及其惡意探索內容都將被封鎖。
- ***啟用 Online Shield*** - (*預設為開啟*) :即時掃描您即將瀏覽的網頁是否有可能的病毒或間諜軟體。如果偵測到病毒或間諜軟體，會立即停止下載，防止任何威脅危及您的電腦。

6.2.2. Search-Shield 偵測

在 ***Search-Shield*** 開啟狀態下搜尋網際網路時，從最常用的搜尋引擎 (*Google*、*Yahoo!*、*JP*、*WebHledani*、*Yandex*、*Baidu*、*Bing*、*AOL*、*AltaVista*、*EarthLink*、*Ask*、*Seznam*、*eBay*、*Twitter*、*Digg 和 SlashDot*) 傳回的全部結果都會評估是否有危險或可疑的連結。透過檢查這些連結並標示惡意連結，LinkScanner 會在您按下危險或可疑連結之前先提出警告，藉此確保您只會進入安全的網站。

評估搜尋結果網頁上的連結時，您會看到連結旁邊有一個圖形標示，表示正在進行連結驗證。評估完成時，會顯示相應的資訊圖示：

連結的頁面是安全的。

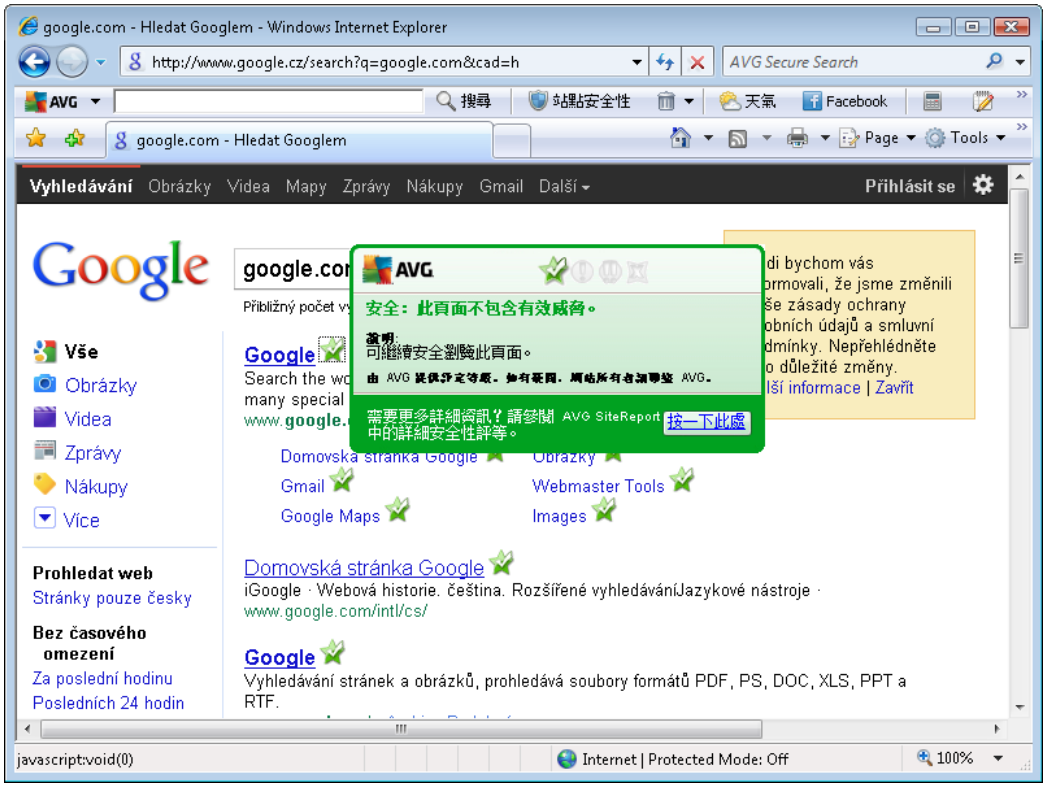
連結的頁面不包含威脅，但有可疑之處 (*來源或動機有問題，因此不建議進行線上購物等等*)。

連結的頁面可能本身是安全的，但是包含其他確定危險的頁面的連結 ;或是程式碼方面很可疑，但目前不會造成直接的威脅。

連結的頁面包含有效威脅！為確保您自身的安全，您不能訪問該頁面。

連結的頁面無法存取，因此無法掃描。

把滑鼠指標停留在單個的等級圖示上即可顯示有關特定連結的詳細資訊。資訊包括該威脅 (*如果有的話*) 的其他詳細資料：

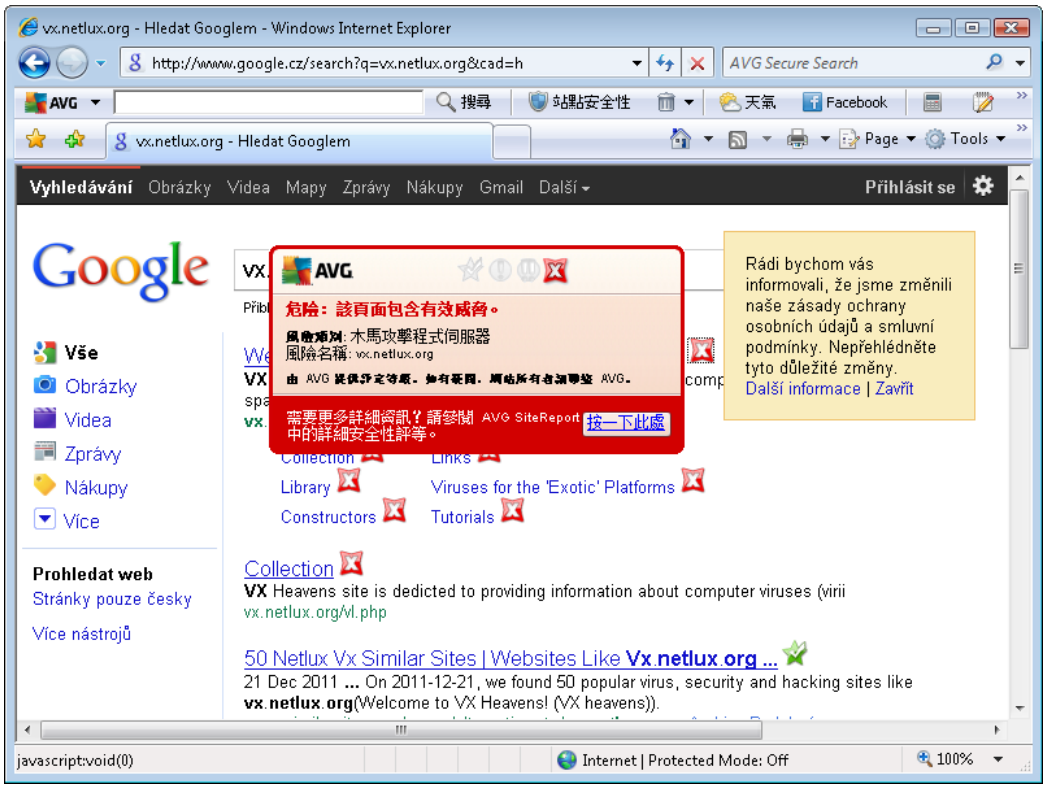


6.2.3. Surf-Shield 偵測

這項強大的保護機制將封鎖您要開啟的任何網頁的惡意內容，並防止它下載到您的電腦中。啟用此功能後，按下危險網站的連結或輸入其 URL 時，會自動將其封鎖，使您無法開啟網頁，藉此防止您無意中受到感染。請記住，光是瀏覽受到影響的網站都有可能讓木馬攻擊探測網頁感染您的電腦，因此當您要求開啟包含木馬攻擊程式或其他嚴重威脅的危險網頁時，LinkScanner 將不允許您的瀏覽器顯示該網頁。

如果您真的遇到惡意網站，LinkScanner 會在您的網頁瀏覽器中顯示如下類似螢幕來提出

警告：



進入這類網站非常危險，不建議進入！

6.2.4. Online Shield 偵測

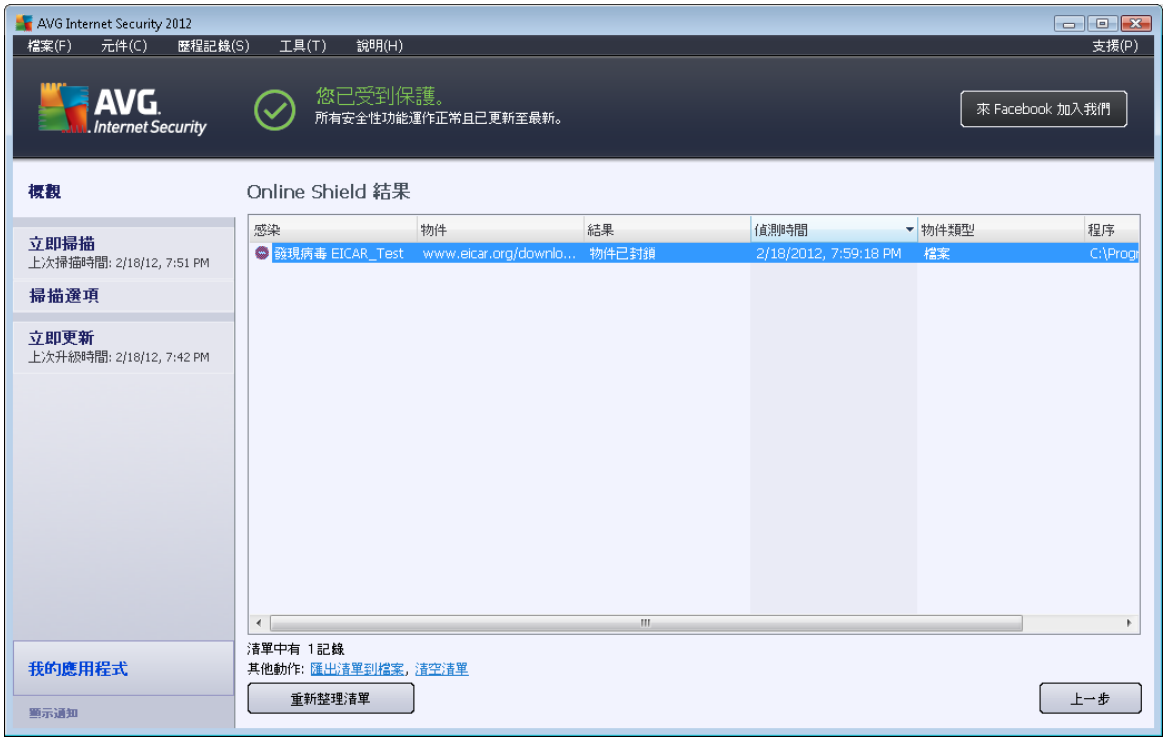
Online Shield 甚至會在瀏覽網頁的內容及這些網頁中可能包含的檔案顯示於您的網頁瀏覽器中或下載到您的電腦之前即進行掃描。如果偵測到威脅，系統將立即顯示下列對話方塊向您發出警告：

您可以在此警告對話方塊中找到被偵測並指派為受感染的檔案資料 (*檔案名稱*)、被視為感染檔案的名稱 (*威脅名稱*)，以及病毒大全的連結，您可以在此處找到有關偵測到的感染的詳細資訊 (*若已知的話*)。該對話方塊提供下列控制按鈕：

- ***顯示詳細資訊*** - 按一下***顯示詳細資訊***按鈕可開啟一個新的快顯視窗，您可以在此處找到當偵測到感染檔案時正在執行的程序的資訊，以及程序的識別。

- ***關閉*** - 按一下該按鈕以關閉警告對話方塊。

將不會開啟可疑的網頁，而且會將威脅偵測結果記錄在 ***Online Shield 結果***的清單中 - 偵測到的威脅的概觀可透過系統功能表歷程記錄/Online Shield 結果存取。



針對每個偵測到的物件，提供以下資訊：

- ***感染*** - 偵測到的物件的描述 (*可能還包含名稱*)
- ***物件*** - 物件來源 (*網頁*)
- ***結果*** - 對偵測到的物件執行的動作
- ***偵測時間*** - 偵測到並封鎖威脅的日期和時間
- ***物件類型*** - 偵測到的物件的類型
- ***程序*** - 是執行什麼動作引致該潛在危險物件，並使其被偵測出來

在對話方塊底端的清單下方，您可以找到有關上述偵測到的物件總數的資訊。然後您可將偵測到的物件的整個清單匯出至檔案中 (***將清單匯出到檔案***並刪除有關偵測到的物件的所有項目 (***清空清單***)。

控制按鈕

- ***重新整理清單*** - 更新 ***Online Shield***

- ***上一步*** - 切換回預設的 AVG 主對話方塊 *(元件概觀)*

6.3. 電子郵件保護

病毒和特洛伊木馬最常見的來源之一就是透過電子郵件。網路釣魚和垃圾郵件使電子郵件成為更嚴重的風險來源。免費的電子郵件帳戶更有可能收到這類惡意電子郵件 (*因為這些帳戶極少採用反垃圾郵件技術*)，而家用電腦使用者又特別依賴這類電子郵件。此外，家用電腦使用者還常瀏覽不明網站，並填寫含個人資料 (*例如他們的電子郵件地址*) 的線上表單，因而提高了受到電子郵件攻擊的可能性。公司通常會使用公司電子郵件帳戶並採用反垃圾郵件篩選器等措施來降低風險。

電子郵件保護元件負責掃描傳送或接收的每一電子郵件訊息；當在電子郵件中偵測到病毒時，會立即將其移除至病毒隔離區。該元件還可以篩選出某些類型的電子郵件附件，並會將一段認證文字加到無感染的訊息中。***電子郵件保護***包括兩項主要功能：

- E-mail Scanner
- Anti-Spam

6.3.1. E-mail Scanner

Personal E-mail Scanner 會自動掃描傳入/傳出電子郵件。您可以將它與那些在 AVG 中沒有自己的外掛程式的電子郵件用戶端搭配使用 *(但也可以用來掃描 AVG 透過特定外掛程式所支援的電子郵件用戶端的電子郵件訊息，例如 Microsoft Outlook、The Bat 和 Mozilla Thunderbird)*。它主要的用途是與 Outlook Express、Incredimail 等此類應用程式搭配使用。

在 AVG 安裝期間，AVG 會針對電子郵件控制項建立自動伺服器：一部用於檢查傳入電子郵件，另一部用於檢查傳出電子郵件。系統會使用這兩部伺服器自動在連接埠 110 和 25 (*收發電子郵件的標準連接埠*) 上檢查電子郵件。

E-mail Scanner 是電子郵件用戶端與網際網路上的電子郵件伺服器之間的介面。

- ***傳入郵件：***從伺服器接收郵件時，***E-mail Scanner*** 元件會對郵件進行測試以檢查是否有病毒，移除受感染的附件，然後加入認證。一旦偵測到病毒，就會立即隔離到病毒隔離區。然後郵件會被傳送到電子郵件用戶端。
- ***傳出郵件：***郵件是從電子郵件用戶端傳送到 E-mail Scanner；它會檢查郵件及其中的附件是否有病毒，然後將郵件傳送至 SMTP 伺服器 (*預設情況下會停用掃描傳出電子郵件，但可以手動設定*)。

E-mail Scanner 不適用於伺服器平台！

6.3.2. Anti-Spam

Anti-Spam 如何運作？

Anti-Spam 會檢查所有傳入電子郵件訊息，並將來路不明的電子郵件標示為垃圾郵件。***Anti-Spam*** 可以藉由新增特殊的文字字串，修改電子郵件 (*被視為垃圾郵件的電子郵件*) 的主旨。您可以輕鬆篩選您電子郵件用戶端內的電子郵件。***Anti-Spam*** 元件會使用多種分析方法來處理每一封電子郵件訊息，從而提供最大的保護來封鎖垃圾電子郵件訊息。***Anti-***

Spam 會使用定期更新的資料庫來偵測垃圾郵件。它也可以使用 RBL 伺服器 (*已知垃圾郵件發件人」電子郵件地址的公用資料庫*), 以及將電子郵件地址手動新增到您的白名單 (*永不標示為垃圾郵件*) 和黑名單 (*永遠標示為垃圾郵件*)。

什麼是垃圾郵件？

垃圾郵件是指來路不明的電子郵件，大部分是產品或服務廣告，它採用批量的方式同時傳送到大量電子郵件地址，一下灌滿收件者的郵箱。垃圾電子郵件並不包括合法的商業電子郵件，因為這種電子郵件的傳送事先已獲得客戶的同意。垃圾電子郵件不僅讓人煩惱，而且經常會是電子郵件詐騙、病毒或攻擊性內容的來源。

6.3.3. 電子郵件保護介面

您可以在 ***電子郵件保護*** 對話方塊找到描述該元件功能的簡短文字，以及其目前狀態的相關資訊*(作用中)*。使用 ***檢視 AVG 如何為您提供保護的線上報告*** 連結在 AVG 網站 (http://www.avg.com/) 的專屬網頁上檢閱 **AVG Internet Security 2012** 活動和偵測的詳細統計資料。

基本電子郵件保護設定

您可以在 ***電子郵件保護*** 對話方塊中進一步編輯該元件的一些基本功能。

- ***掃描傳入郵件*** *(預設為開啟)* - 勾選此方塊可指定所有傳送到您的帳戶的電子郵件都應該接受掃描，檢查是否有病毒。
- ***掃描傳出郵件*** *(預設為關閉)* - 勾選此方塊可確認所有自您帳戶寄出電子郵件都應

該掃描是否有病毒。

- ***在掃描電子郵件時顯示通知視窗*** *(預設為開啟)* - 標示此項目表示您希望在掃描電子郵件時透過系統匣上的 AVG 圖示顯示的通知獲得告知。
- ***啟用 Anti-Spam*** *(預設為開啟)* - 標示此項目可指定您是否要篩選傳入郵件，檢查是否有來路不明的電子郵件。

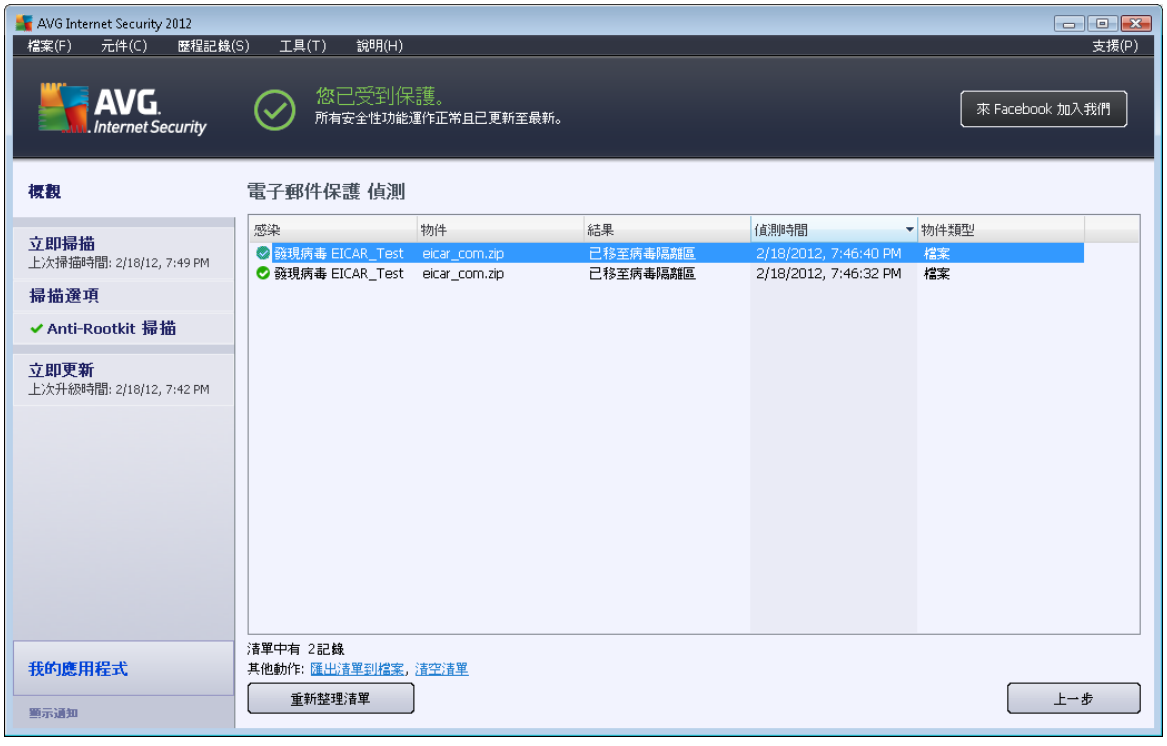
軟體供應商已對所有 AVG 元件進行設定，能提供最佳效能。除非您確實需要這麼做，否則不要變更 AVG 組態。任何設定變更都只能由經驗豐富的使用者來執行。如需變更 AVG 組態，請選取系統功能表項目工具/進階設定，然後在新開啟的 AVG 進階設定對話方塊中編輯 AVG 組態。

控制按鈕

電子郵件保護對話方塊內可用的控制按鈕如下：

- ***儲存變更*** - 按此按鈕可儲存並套用在此對話方塊中所做的任何變更
- ***取消*** - 按此按鈕可返回到預設的 AVG 主對話方塊 *(元件概觀)*

6.3.4. E-mail Scanner 偵測



您可以在 ***E-mail Scanner 偵測***對話方塊中 *(透過系統功能表選項 歷程記錄/E-mail Scanner 偵測」來存取)* 看到電子郵件保護元件偵測到的所有結果清單。針對每個偵測到的物件，提供以下資訊：

- ***感染*** - 偵測到的物件的說明 (甚至可能包含名稱)
- ***物件*** - 物件位置
- ***結果*** - 對偵測到的物件執行的動作
- ***偵測時間*** - 偵測到可疑物件的日期和時間
- ***物件類型*** - 偵測到的物件的類型

在對話方塊底端的清單下方，您可以找到有關上述偵測到的物件總數的資訊。然後您可將偵測到的物件的整個清單匯出至檔案中 (***從清單匯出到檔案***) 並刪除有關偵測到的物件的所有項目 (***清空清單***)。

控制按鈕

E-mail Scanner 偵測介面內可用的控制按鈕如下：

- ***重新整理清單*** - 更新偵測到的威脅清單。
- ***上一步*** - 將您切換回之前顯示的對話方塊。

6.4. Firewall

Firewall 是透過阻止/允許流量，強制在兩個或多個網路之間實施存取控制政策的一種系統。Firewall 包含一個規則集，用於保護內部網路免遭外部攻擊 *(通常來自網際網路)*，並控制每個單一網路連接埠上的所有通訊。根據定義的規則對通訊進行評估，然後允許或禁止該通訊。如果 ***Firewall*** 發現任何入侵企圖，它會將其 「封鎖」並禁止入侵者存取電腦。

Firewall 可組態成允許或拒絕透過定義的連接埠和定義的軟體應用程式進行內部/外部通訊 (雙向，向內或向外)。例如，可將 Firewall 組態成僅允許使用 Microsoft Explorer 實現網頁資料流入和流出。任何企圖透過任何其他瀏覽器進行的網頁資料傳輸都會被封鎖。

Firewall 可保護您的個人可識別資訊，防止在未經您允許的情況下將該資訊傳送給他人。它可控制您電腦在網際網路或本機網路上與其他電腦交換資料的方式。在公司內部，***Firewall*** 還可保護單部電腦免遭來自網路中其他電腦上的內部使用者的攻擊。

未受 Firewall 保護的電腦很容易就變成電腦駭客和資料盜竊的標靶。

建議：*一般不建議在單獨的電腦上使用超過一種防火牆。安裝多種防火牆並不能加強電腦的安全性。更可能的情況是，這兩種應用程式之間會發生一些衝突。因此，我們建議您在電腦上只使用一種防火牆，並停用所有其他防火牆，藉此消除產生潛在衝突的危險，以及與此相關的問題。*

6.4.1. Firewall 原理

在 **AVG Internet Security 2012** 中，***Firewall*** 會控制您電腦每個網路連接埠上的所有流量。根據定義的規則，***Firewall*** 會對您電腦上執行 *(並且想連線到網際網路或區域網路)* 的應用程式，或者從外部嘗試連線到您電腦之應用程式進行評估。然後對於上述每個應用程式，***Firewall*** 會允許或禁止網路連接埠上的通訊。預設情況下，如果該應用程式不明 *(即沒有已*

定義的 Firewall 規則)，則 ***Firewall*** 會詢問您是要允許還是封鎖該通訊嘗試。

AVG Firewall 不適用於伺服器平台！

AVG Firewall 可以做些什麼：

- 自動允許或封鎖已知應用程式的通訊嘗試，或者要求您確認
- 根據需要使用具有預先定義規則的設定檔
- 連線到不同網路或使用不同網路介面卡時，自動

6.4.2. Firewall 設定檔

Firewall 允許您依據以下情況來定義特定的安全性規則，即您的電腦是位於網域中，還是該電腦是一台獨立電腦，甚至是一台筆記型電腦。所有這些選項都需要有一個不同層級的保護，其層級由各自相應的設定檔所涵蓋。簡言之，Firewall 設定檔是 Firewall 元件的一種特定組態，並且您可使用許多這種預先定義的組態。

可用設定檔

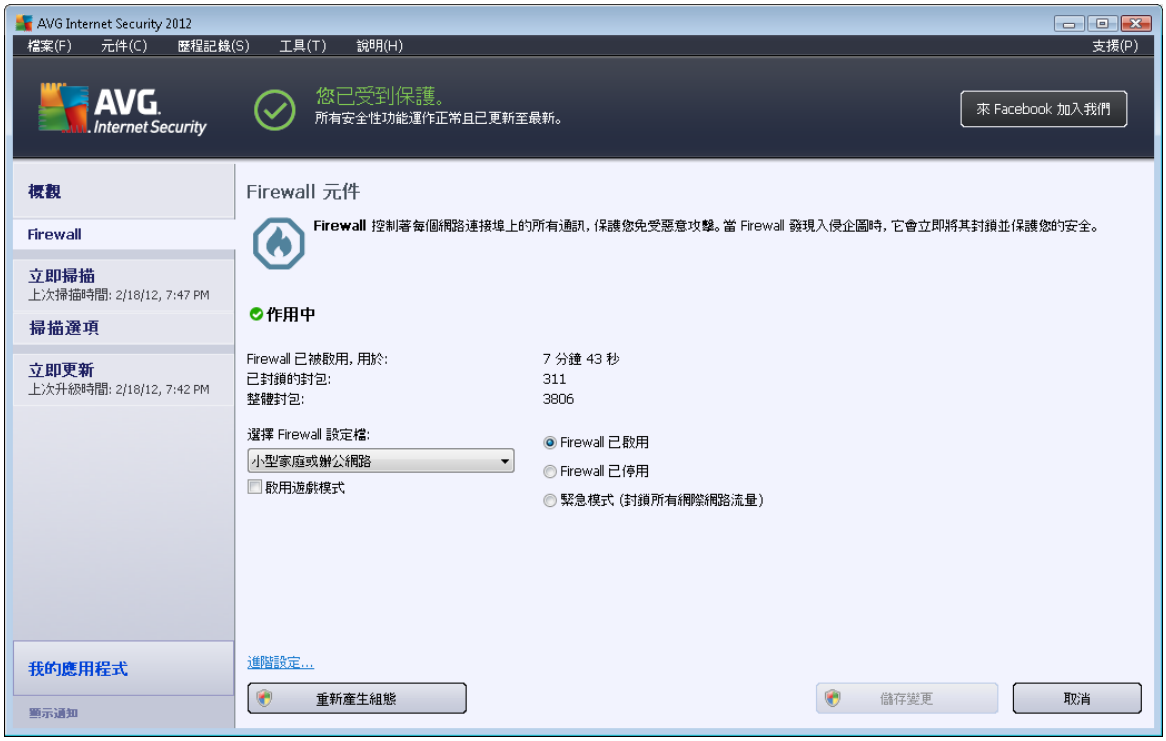
- ***全部允許*** - 製造商已預設好的一個 Firewall 系統設定檔，此檔始終存在。啟動此設定檔後，將允許所有網路通訊，不會套用任何安全性原則規則，就像 Firewall 保護已關閉一樣 (也就是允許所有應用程式，但仍然檢查封包 - 要完全停用所有篩選，需要停用 Firewall)。無法複製、刪除此系統設定檔，也無法修改其設定。
- ***全部封鎖*** - 製造商已預設好的一個 Firewall 系統設定檔，此檔始終存在。啓動此設定檔後，所有網路通訊都會被封鎖，電腦無法從外部網路存取，也無法與外部通訊。無法複製、刪除此系統設定檔，也無法修改其設定。
- ***自訂設定檔*** - 自訂設定檔可讓您利用自動設定檔切換功能。如果您經常連線到不同的網路 *(如使用筆記型電腦)，此功能特別有用。*安裝 **AVG Internet Security 2012** 後，將自動產生自訂設定檔，可滿足 Firewall 政策規則的各種需求。可用的自定設定檔如下：
  - ***直接連線到網際網路*** –適合直接連線到網際網路的一般家用桌上型電腦或筆記型電腦，無需額外保護。當您將網路連線到各種不明而且可能不安全的網路時 (*例如網咖、飯店房間等*) 時，也建議使用此選項。此設定檔最嚴格的 Firewall 政策規則可確保這類電腦受到足夠的保護。
  - ***網域內電腦*** –適合區域網路內的電腦，通常是學校或辦公室。假定網路是得到專業的管理，並透過某些額外措施加以保護，則其安全性層級可能低於以上所述情形，允許存取共用資料夾和磁碟裝置等。
  - ***小型家庭或辦公網路*** –適合小型網路內的電腦，通常是住家或小型企業。通常，這種網路沒有 「中心」管理員，並且僅由幾台共用印表機、掃描儀或類似裝置的電腦相連而成，Firewall 規則必須反映這種情況。

設定檔切換

設定檔切換功能允許在使用某種網路介面卡或者在連線到特定類型的網路時，Firewall 能自動切換到定義的設定檔。如果尚未指派任何設定檔至網路區域，在下次連線至該區域時，Firewall 將顯示對話方塊要求您指派設定檔。您可以為所有本機網路介面或區域指派設定檔，並在區域和介面卡設定檔對話方塊中進一步指定設定，如果您不希望使用該功能，也可以在此處停用它 (*這樣，所有類型的連線都將使用預設設定檔*)。

通常，擁有筆記型電腦和使用各種不同類型連線的使用者將會發現此功能十分有用。如果您擁有桌上型電腦且僅使用一種類型的連線 (*例如，使用纜線連線至網際網路*)，則不必切換設定檔，因為您很可能不會用到它。

6.4.3. Firewall 介面



名為 ***Firewall 元件***的主對話方塊提供關於該元件功能的一些基本資訊，其狀態 *(作用中)*，以及該元件統計資料的簡短概觀。

- ***Firewall 已被啟用，用於*** - 自 Firewall 上次啟動至今經過的時間
- ***已封鎖的封包*** - 經過檢查的封包總數中已阻止封包的數量
- ***整體封包*** - Firewall 執行期間檢查的所有封包數量

基本 Firewall 設定

- ***選取 Firewall 設定檔*** - 從下拉式功能表選取其中一個已定義的設定檔 (*有關每個設定檔的詳細說明及其建議用途，請參閱 Firewall 設定檔一章*)

- ***啟用遊戲模式*** - 核取該選項可確保在執行全螢幕應用程式 (*遊戲、簡報、電影等*) 時，Firewall 不會顯示對話方塊，詢問您是要允許還是阻止不明應用程式的通訊。如果此時不明應用程式嘗試進行網路通訊，Firewall 將根據目前設定檔中的設定，自動允許或封鎖該嘗試。***備註 :***如果開啟游戲模式，則所有排定的工作 (掃描、更新) 都將延遲到該應用程式關閉為止。

- 此外，您可以在這個基本設定區段中從三種定義 Firewall 元件的目前狀態的選項進行選擇：

  - ***Firewall 已啟用*** *(預設設定)* - 選取此選項將允許與在所選 Firewall 設定檔中定義的規則集中指派為「已允許」的應用程式進行通訊。

  - ***Firewall 已停用*** - 此選項可完全關閉 Firewall，不檢查即允許所有網路通訊！

  - ***緊急模式 (封鎖所有網際網路流量)*** - 選取此選項可封鎖各個網路連接埠上的所有流量；Firewall 仍會繼續執行，但會停止所有網路流量。

請注意 :*軟體供應商已對所有 AVG Internet Security 2012 元件進行設定，以提供最佳效能。除非您確實需要這麼做，否則不要變更 AVG 組態。任何設定變更都只能由經驗豐富的使用者來執行。如需變更 Firewall 組態，請選取系統功能表項目* ***工具/Firewall 設定****，然後在新開啟的 Firewall 設定對話方塊中編輯 Firewall 組態。*

控制按鈕

- ***重新生成組態*** - 按一下此按鈕可覆寫目前的 Firewall 組態，並根據自動偵測還原為預設組態。

- ***儲存變更*** - 按此按鈕可儲存並套用在此對話方塊中所做的任何變更。

- ***取消*** - 按此按鈕可返回到預設的 AVG 主對話方塊 (*元件概觀*)。

6.5. Anti-Rootkit

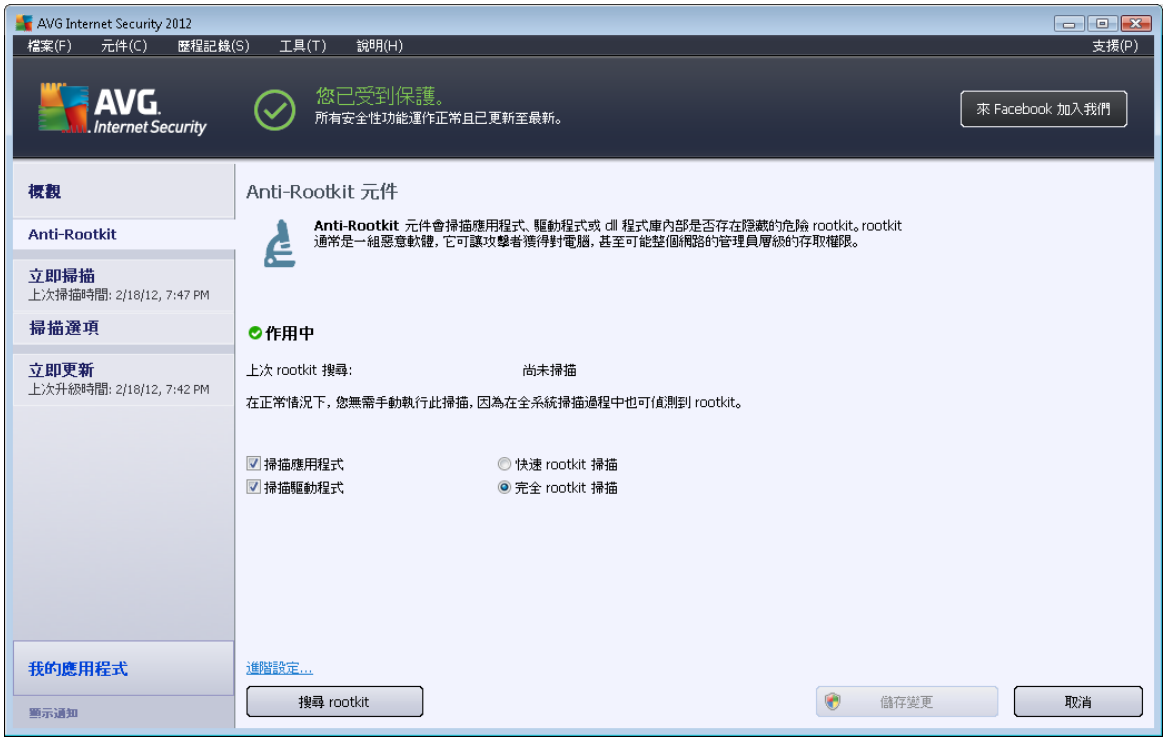
Anti-Rootkit 這項專用工具能偵測並有效移除危險的 rootkit (即能夠在您的電腦上隱藏惡意軟體身份的程式及技術)。***Anti-Rootkit*** 能夠根據預先定義的一組規則偵測 rootkit。請注意，它會偵測所有 rootkit *(而不只是受感染的 rootkit)*。如果 ***Anti-Rootkit*** 發現 rootkit，不一定表示該 rootkit 已受感染。rootkit 有時候會被用作驅動程式，或屬於正確應用程式的一部分。

什麼是 rootkit？

rootkit 是一種試圖在沒有獲得系統所有者或合法管理員授權的情況下，取得電腦系統基本控制權的程式。rootkit 幾乎不需要存取硬體，因為它主要的目的是取得在硬體上執行的作業系統的控制權。一般而言，rootkit 會透過破壞或迴避標準作業系統的安全性機制來隱身於系統中。這些 rootkit 往往也是特洛伊木馬，讓使用者誤以為在系統上執行它們很安全。用來達到此目的的技巧包括對監視程式隱藏執行中的程序，或是隱藏作業系統中的檔案或

系統資料。

6.5.1. Anti-Rootkit 介面



Anti-Rootkit 對話方塊提供元件功能的簡短說明，告知元件的目前狀態 *(作用中)*，並提供最後一次啟動 ***Anti-Rootkit*** 測試的相關資訊 (*最後一次 rootkit 搜尋*，*rootkit 測試是執行*[*完整電腦掃描*]中的預設程序)。***Anti-Rootkit*** 對話方塊會進一步提供[工具/進階設定]連結。使用該連結可重新導向至 ***Anti-Rootkit*** 元件的進階組態環境。

軟體供應商已對所有 AVG 元件進行設定，能提供最佳效能。除非您確實需要這麼做，否則不要變更 AVG 組態。任何設定變更都只能由經驗豐富的使用者來執行。

基本 Anti-Rootkit 設定

您可以在對話方塊底端設定掃描 rootkit 是否存在的基本功能。首先，勾選相應的核取方塊來指定要掃描的物件：

- ***掃描應用程式***
- ***掃描驅動程式***

此外，您還可以挑選 rootkit 掃描模式：

- ***快速 rootkit 掃描*** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾 (*通常是 c:\Windows*)。

- ***完全 rootkit 掃描*** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾 (*通常是 c:\Windows*)，加上所有本機磁碟 (*包括快閃磁碟機，但不包括磁碟片/CD 光碟機*)。

控制按鈕

- ***搜尋 rootkit*** - 由於 rootkit 掃描不是掃描整台電腦的固有功能，您可以使用此按鈕從 ***Anti-Rootkit*** 介面直接執行 rootkit 掃描。
- ***儲存變更*** - 按此按鈕可儲存在此介面中做出的所有變更，並返回到預設的 AVG 主對話方塊 (*元件概觀*)。
- ***取消*** - 按此按鈕可返回到預設的 AVG 主對話方塊 (*元件概觀*)，並且不儲存您所做的任何變更。

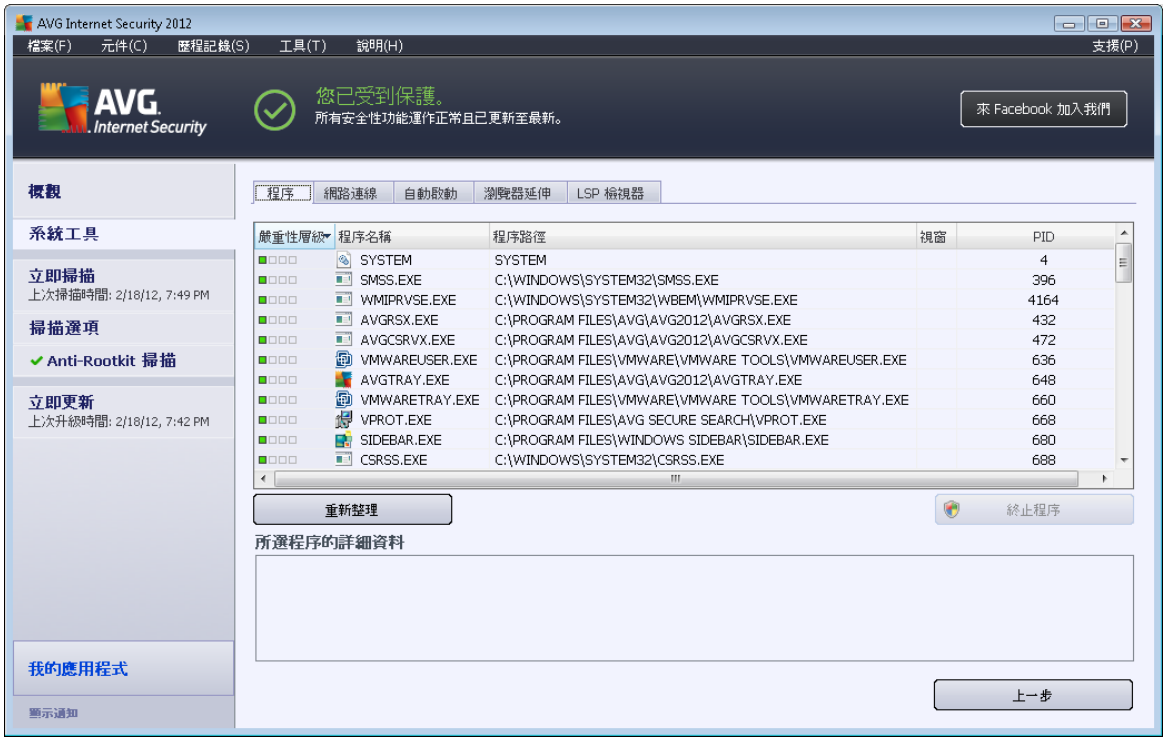
6.6. 系統工具

System Tools 是指一組能提供 **AVG Internet Security 2012** 環境及作業系統詳細摘要的工具。該元件會顯示如下內容的概觀：

- 程序 – 電腦上目前處於使用中的程序清單 (*例如，執行中的應用程式*)。
- 網路連線 – 目前處於使用中的連線的清單
- 自動啟動 – Windows 系統啟動期間執行的所有應用程式的清單
- 瀏覽器延伸 – 在網際網路瀏覽器內安裝的外掛程式 (*亦即應用程式*) 的清單
- LSP 檢視器 – 分層服務提供者 (*LSP*) 的清單

特定概觀也可以進行編輯，但是只建議經驗極其豐富的使用者來執行！

6.6.1. 程序



程序對話方塊包含電腦上目前處於使用中的程序 (*即執行中的應用程式*) 的清單。此清單由數欄構成：

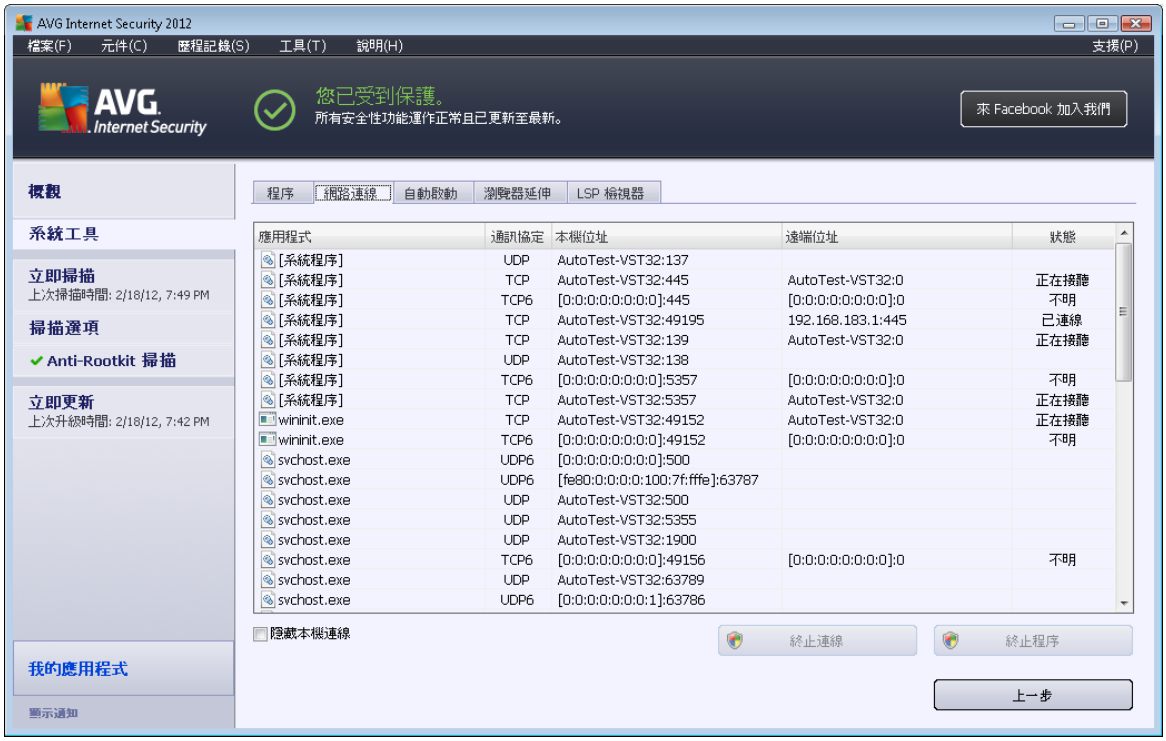
- ***嚴重性層級*** - 按四層級標準，以圖形形式指示相應程序的嚴重性，從不太重要 (■□□□) 到嚴重 (■■■■)
- ***程序名稱*** - 執行中程序的名稱
- ***程序路徑*** - 執行中程序的實體路徑
- ***視窗*** - 表示應用程式視窗的名稱 (如適用)。
- ***PID*** - 即程序識別碼，是 Windows 內部程序的唯一識別元

控制按鈕

程序標籤內可用的控制按鈕如下：

- ***重新整理*** - 根據目前狀態更新程序清單
- ***終止程序*** - 您可以選取一個或多個應用程式，並按此按鈕來終止它們。***我們強烈建議不要終止任何應用程式，除非您完全確定它們確實是威脅！***
- ***上一步*** - 將您切換回預設 AVG 主對話方塊 (*元件概觀*)

6.6.2. 網路連線



網路連線對話方塊包含目前處於使用中連線的清單。該清單由以下兩欄組成：

- ***應用程式*** - 與連線相關的應用程式名稱 (*Windows 2000 除外，此版本不提供該資訊*)
- ***通訊協定*** - 用於連線的傳輸通訊協定類型：
    - TCP - 與網際網路通訊協定 (IP) 搭配使用，透過網際網路傳輸資訊的一種通訊協定
    - UDP - 對 TCP 通訊協定的另一種替代協定
- ***本機位址*** - 本機電腦的 IP 位址和所使用的連接埠號
- ***遠端位址*** - 遠端電腦的 IP 位址和連線的連接埠號如有可能，它還會查詢遠端電腦的主機名稱。
- ***狀態*** - 表示最為可能的目前狀態 (*已連線、伺服器應關閉、待命、主動關閉已完成、被動關閉、主動關閉*)

若只想列出外部連線，請在對話方塊底端的清單下勾選***隱藏本機連線***核取方塊。

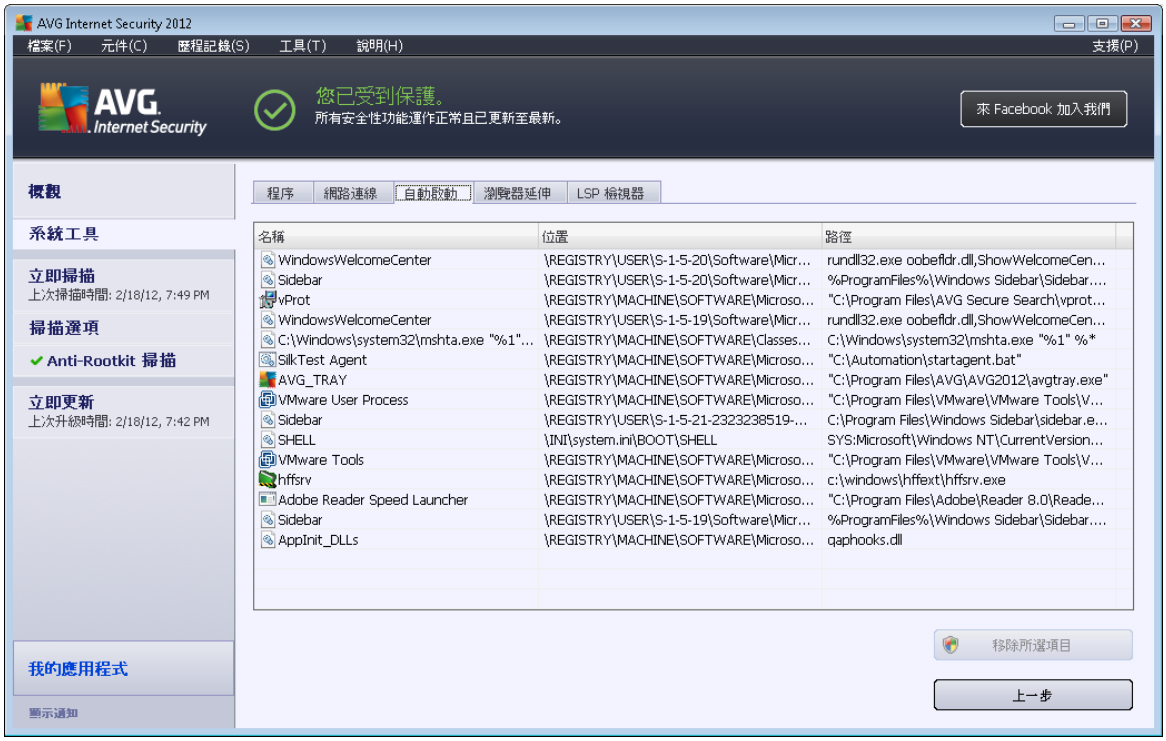
控制按鈕

網路連線標籤內可用的控制按鈕如下：

- ***終止連線*** - 關閉在清單中選取的一個或多個連線
- ***終止程序*** - 關閉一個或多個與清單中所選連線有關的應用程式
- ***上一步*** - 切換回預設 AVG 主對話方塊 (元件概觀)。

有時可能只能終止正處於連線狀態的應用程式。我們強烈建議不要終止任何連線，除非您完全確定它們確實是威脅！

6.6.3. 自動啟動



自動啟動對話方塊會顯示 Windows 系統啟動期間執行的所有應用程式的清單。很常見的一種情況是，數個惡意應用程式會自動將自身加到啓動登錄項目中。

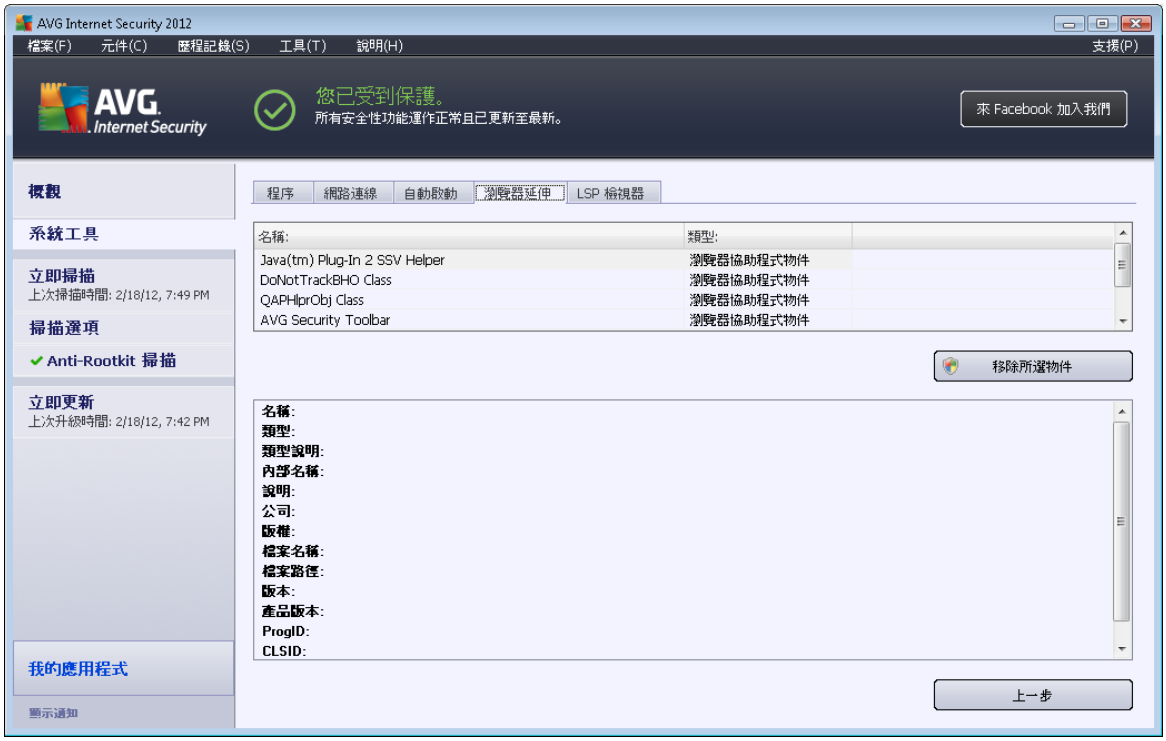
控制按鈕

自動啟動標籤內的可用控制按鈕如下：

- ***移除所選項目*** - 按此按鈕可刪除一個或多個所選項目。
- ***上一步*** - 將您切換回預設 AVG 主對話方塊 *(元件概觀)*。

我們強烈建議不要刪除清單中的任何應用程式，除非您完全確定它們確實是威脅！

6.6.4. 瀏覽器延伸



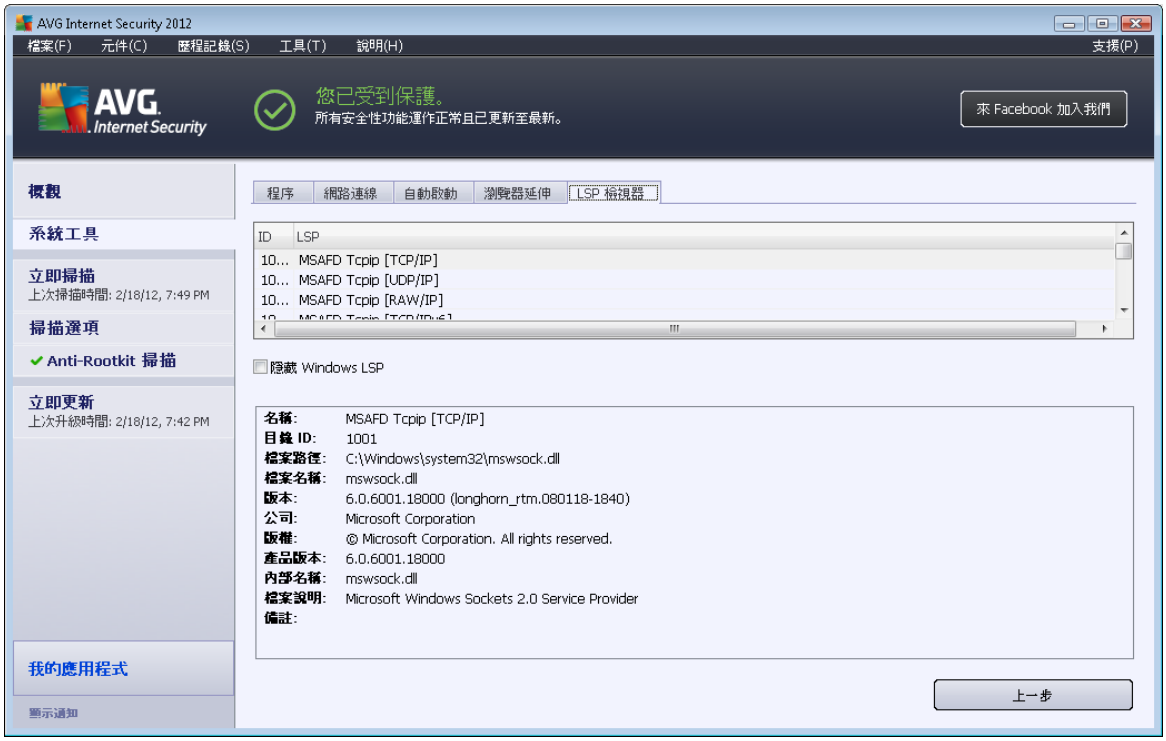
瀏覽器延伸對話方塊包含一份在網際網路瀏覽器中安裝的外掛程式 (*即應用程式*) 清單。該清單可能包含一般應用程式外掛程式，也可能包含潛在的惡意程式。按一下清單內的物件，即可取得所選外掛程式的詳細資訊，此項資訊將顯示在對話方塊的底端。

控制按鈕

瀏覽器延伸標籤內的可用控制按鈕如下：

- ***移除所選物件*** - 移除清單中目前亮顯的外掛程式。***我們強烈建議不要刪除清單中的任何外掛程式，除非您完全確定它們確實是威脅！***
- ***上一步*** - 將您切換回預設 AVG 主對話方塊 *(元件概觀)*。

6.6.5. LSP 檢視器



LSP 檢視器對話方塊顯示分層服務提供者 (LSP) 清單。

分層服務提供者 (LSP) 是連結到 Windows 作業系統網路服務的系統驅動程式。它有權存取所有進出電腦的資料，還有權修改這些資料。為了讓 Windows 能夠連線到其他電腦，包括網際網路，必須使用一些 LSP。但是某些惡意應用程式也可能作為 LSP 進行安裝，從而存取您電腦傳輸的所有資料。因此該檢閱可幫助您檢查所有潛在的 LSP 威脅。

在某些情況下，它還可以修復損壞的 LSP (*例如，當檔案已移除但登錄項目仍保留時*)。一旦發現可修復的 LSP，便會顯示用於修復問題的新按鈕。

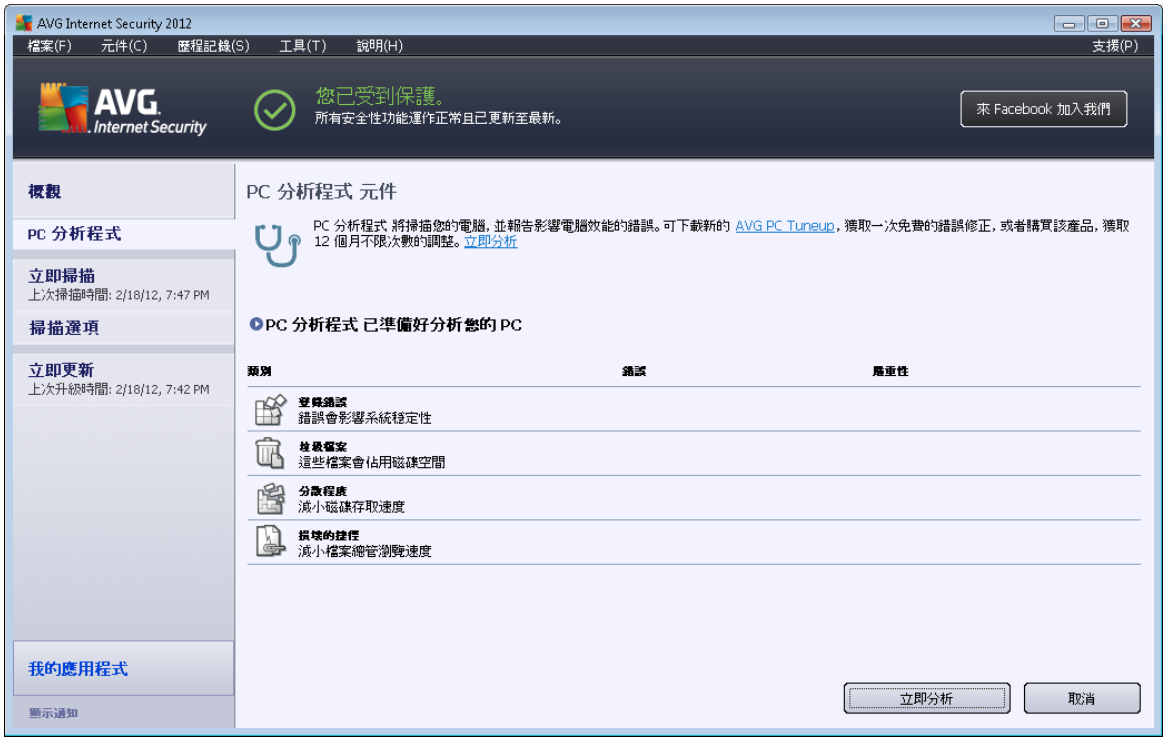
控制按鈕

LSP 檢視器標籤內可用的控制按鈕如下：

- ***隱藏 Windows LSP*** - 若要將 Windows LSP 包含在清單中，請取消核取此項目。
- ***上一步*** - 將您切換回預設的 AVG 主對話方塊 (*元件概觀*)。

6.7. PC 分析程式

PC 分析程式元件能夠掃描您的電腦找出系統問題，並為您提供清楚的概觀，指出可能使您的電腦整體效能惡化的原因。在該元件的使用者介面中，您可以看到一個分成四條線的圖表，分別代表不同的類別 :登錄錯誤、垃圾檔案、分散程度，以及損壞的捷徑：



- ***登錄錯誤***提供 Windows 登錄中的錯誤數量。由於修復登錄要求具備相當進階的知識，因此我們不建議您自行嘗試進行修復。
- ***垃圾檔案***將提供很可能無法處理的檔案數量。通常，這些檔案會是許多暫存檔案以及資源回收筒中的檔案。
- ***分散程度***將計算您硬碟上分散程度的百分比，即使用很長一段時間後，造成大部分檔案現在分散在實體磁碟的不同部分。您可以使用一些磁碟重組工具來修復此問題。
- ***損壞的捷徑***將通知您無法再使用的捷徑，如使用這些捷徑，會將您引向不存在的位置等等。

若要開始分析您的系統，請按一下***立即分析***按鈕。您接著可以直接在圖表中察看分析進度及其結果：

結果概觀提供偵測到的系統問題數目 (***錯誤***)，並依據個別的測試類別加以區分。分析結果也會依***嚴重性***欄的座標以圖形方式顯示。

控制按鈕

- ***立即分析*** (*在分析開始之前顯示*) - 按此按鈕可立即開始分析您的電腦
- ***立即修復*** (*完成分析時會立即顯示*) - 按此按鈕可前往 AVG 網站 (http://www.avg.com/) 中提供與 ***PC 分析程式***元件相關的最新詳細資訊的頁面
- ***取消*** - 按此按鈕可停止執行中的分析，或在完成分析後立即返回到預設的 AVG 主對話方塊 (*元件概觀*)

6.8. Identity Protection

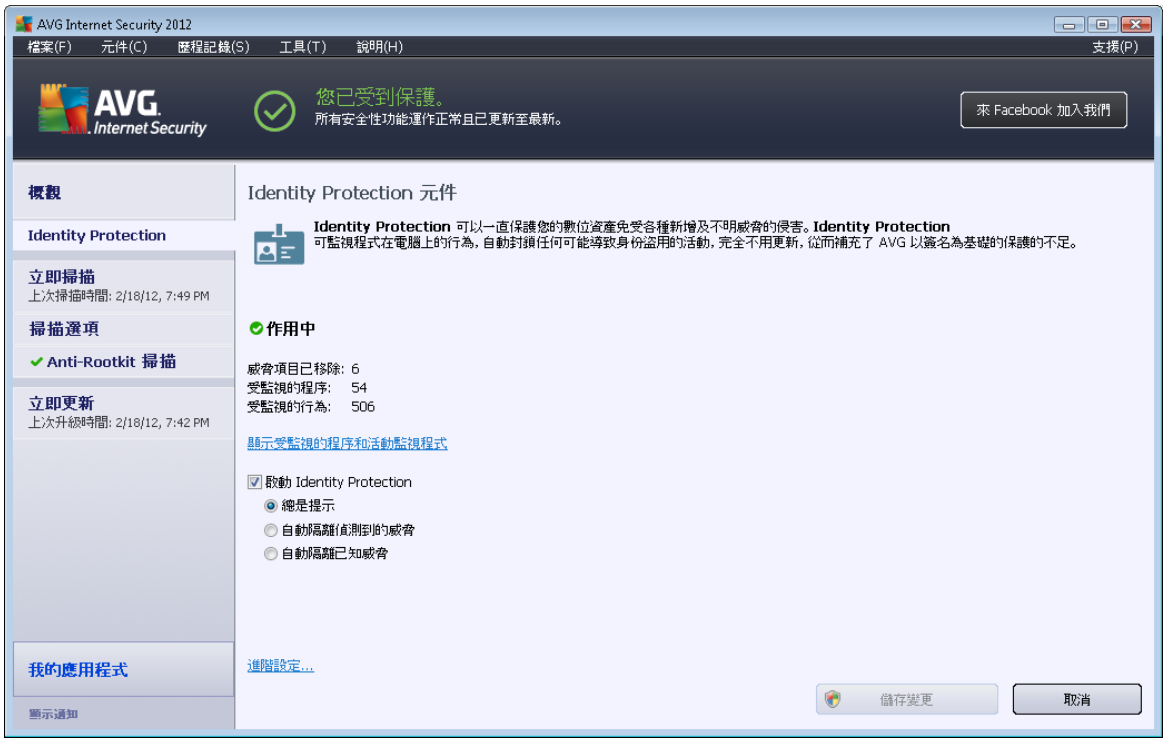
Identity Protection 是一個反惡意軟體元件，它使用行為技術來保護您的電腦免遭各種惡意軟體 (*間諜軟體、傀儡程式、身份盜賊等*) 的攻擊，並提供針對新病毒的零時差防護 (Zero Day Protection)。***Identity Protection*** 主要關注的是防止身份盜用者以您的電腦作為目標，透過各種*惡意軟體*竊取您的密碼、銀行帳戶詳細資訊、信用卡號碼以及您其他有價值的個人數位財產。這可確保您電腦上或共用網路中執行的所有程式均正確運作。***Identity Protection*** 會持續性地找出並封鎖可疑行為，保護您的電腦免遭所有新興惡意軟體的攻擊。

Identity Protection 元件為您的電腦提供即時保護，可防禦新興甚至不明的威脅。它會監視所有 *(包括隱藏的)* 程序和超過 285 種不同行為模式，並能夠判定您系統中是否存在惡意行為。因此，它能夠揭示病毒庫中尚未描述的威脅。當有不明的程式碼進入電腦時，系統會立

即檢查它是否是惡意行為並進行追蹤。如果發現惡意檔案，***Identity Protection*** 會將程式碼移至病毒隔離區並復原任何已對系統所做的變更 *(程式碼插入、登錄變更、連接埠開啟等)*。您無需啟動掃描即可獲得保護。此技術為主動式，因此不太需要更新，並且會一直提供防護。

Identity Protection 是 Anti-Virus 所提供的免費保護。我們強烈建議您安裝兩者，讓您的電腦獲得完整的保護！

6.8.1. Identity Protection 介面



Identity Protection 對話方塊提供元件基本功能的簡短說明、其狀態 *(作用中)*，以及一些統計資料：

- ***惡意軟體項目已移除*** - 提供被偵測為惡意軟體且已移除的應用程式數目
- ***受監視的程序*** - 目前正在執行且受到 IDP 監視的應用程式數目
- ***受監視的行為*** - 在受監視的應用程式內執行的特定動作數目

您可以在下面找到顯示監視的程序和活動監視器連結，此連結會將您帶往 系統工具元件的使用者介面，您可以在此處找到所有監視的程序的詳細概觀。

基本 Identity Protection 設定

您可以在對話方塊底端編輯該元件的一些基本功能：

- ***啟動 Identity Protection*** - (*預設為開啟*) :核取此項目可啟動 IDP 元件，並開啟進一步的編輯選項。

在某些情況下，***Identity Protection*** 可能會報告某個合法檔案很可疑或有危險。由於 ***Identity Protection*** 是根據威脅本身的行為來偵測威脅，這通常是發生在當有程式試圖監視按鍵動作、安裝其他程式或在電腦上安裝新驅動程式時。因此請選取下列其中一個選項，指定 ***Identity Protection*** 元件在偵測到可疑活動時的行為：

  - ***總是提示*** - 如果偵測到一個應用程式有惡意軟體，會詢問您是否該將它封鎖 (*此選項預設為開啟 ;除非您真的有需要，否則建議您不要改變此設定*)
  - ***自動隔離偵測到的威脅*** - 將自動封鎖所有被偵測為惡意軟體的所有應用程式
  - ***自動隔離已知威脅*** - 只有那些百分之百確定帶有惡意軟體的應用程式才會被封鎖

- ***進階設定***... - 按一下該連結會將您重新導向至的**AVG Internet Security 2012**進階設定內個別的對話方塊。您可以在該處詳細編輯該元件的組態。但是，請注意，所有元件的預設組態是為了使 **AVG Internet Security 2012** 提供最佳效能和最高安全性而設定。除非您有充分的理由進行變更，否則建議您保持預設組態！

控制按鈕

Identity Protection 介面內可用的控制按鈕如下：

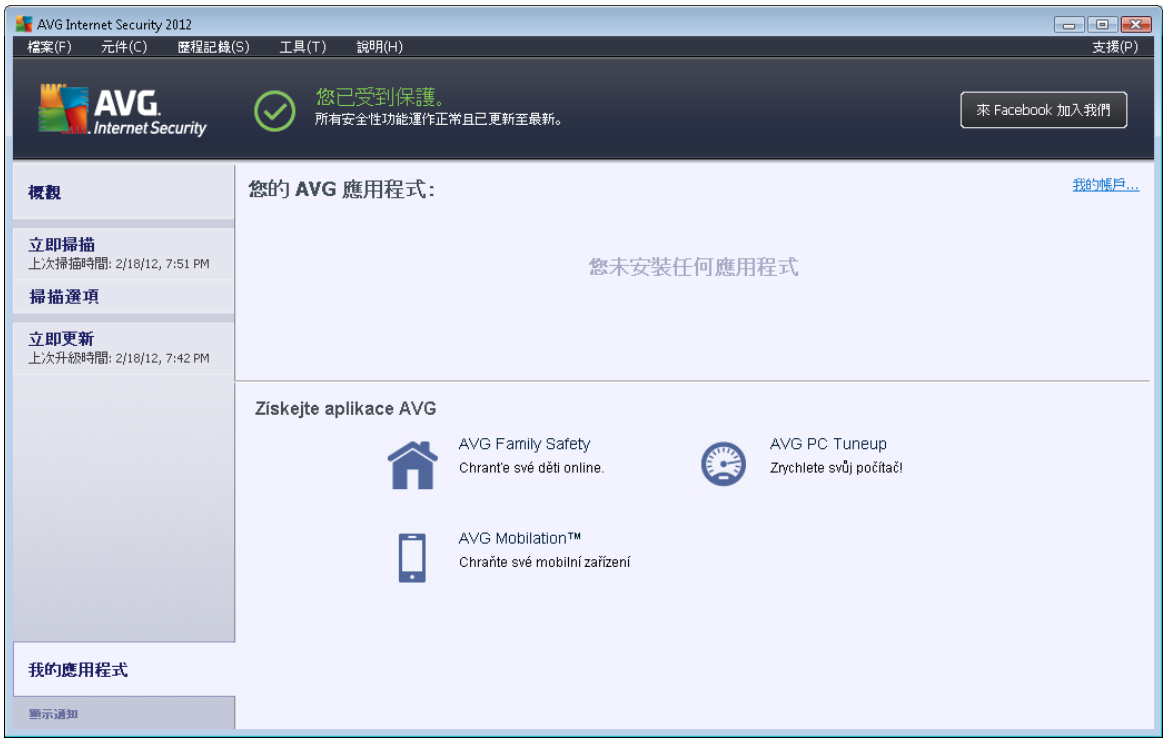
- ***儲存變更*** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- ***取消*** - 按此按鈕可返回到預設的 AVG 主對話方塊 (*元件概觀*)

6.9. 遠端管理

遠端管理元件只會在您已安裝產品的 Business Edition 時才會顯示在 **AVG Internet Security 2012** 的使用者介面中 *(有關用於安裝的授權資訊，請參閱資訊對話方塊的版本標籤，可透過支援系統功能表項目開啟)*。如需在 AVG 遠端管理系統內取得該元件的選項和功能的詳細描述，請參閱專門針對此主題提供的特定文件。此文件可在 AVG 網站 (http://www.avg.com/) 的 ***支援中心/下載/文件***區段中下載。

7. 我的應用程式

我的應用程式對話方塊 *(可直接從 AVG 主對話方塊透過「我的應用程式」存取)* 提供 AVG 獨立應用程式 (包括已安裝在電腦上以及準備好選擇安裝) 的概覽：



此對話方塊分為兩部分：

- ***您的 AVG 應用程式*** - 提供已安裝在電腦上的供 AVG 獨立應用程式的概覽；
- ***獲取 AVG 應用程式*** - 提供您可能感興趣的 AVG 獨立應用程式的概覽。這些應用程式已準備好進行安裝。根據您的授權、地點和其他條件動態變更服務。有關這些應用程式的詳細資訊，請參閱 AVG 網站 (http://www.avg.com/)。

然後請找到的所有應用程式的簡要概覽以及其功能的簡短說明：

7.1. AVG Family Safety

AVG Family Safety 幫助您保護孩子不受不當的網站、媒體內容和線上搜索結果所侵害，並為您提供有關孩子網路活動的報告。***AVG Family Safety*** 使用擊鍵監控來監視您的孩子在聊天室以及社交網站中的活動。如果識別到已知用來線上危害兒童的詞、詞組或語言，將立即透過訊息或電子郵件來通知您。此應用程式可讓您為每個孩子設定相應的保護級別，透過唯一的登入資訊對每個孩子進行單獨監視。

如需詳細資訊，請造訪專屬的 AVG 網頁，也可以在其中立即下載該元件。若要下載該元件，可以使用我的應用程式對話方塊中的 AVG Family Safety 連結。

7.2. AVG LiveKive

AVG LiveKive 專用於安全伺服器的線上資料備份。***AVG LiveKive*** 會自動將您的所有檔案、相片和音樂備份到一個安全地方，使您可以與家人和朋友分享，並能從任何可使用網路的裝置 (如 iPhone 和 Android 裝置) 存取它們。***AVG LiveKive*** 功能包括：

- 萬一電腦和/或硬碟發生損毀時的安全措施
- 從任何連線到網際網路的裝置存取資料
- 方便整理
- 與您授權的任何人分享

如需詳細資訊，請造訪專屬的 AVG 網頁，也可以在其中立即下載該元件。若要這麼做，您可以使用我的應用程式對話方塊內的 AVG LiveKive 連結。

7.3. AVG Mobilation

AVG Mobilation 保護您的行動電話免遭病毒和惡意軟體的攻擊，並且可在您與行動電話分開時，能讓您遠端追蹤您的智能手機。***AVG Mobilation*** 功能包括：

- *File Scanner* 可讓您在不同的儲存位置安全掃描檔案；
- *Task Killer* 可讓您在裝置減慢或卡住時停止應用程式；
- *App Locker* 可讓您透過密碼來鎖定或保護一個或多個應用程式，以避免濫用；
- *Tuneup* 收集各種系統參數*(電池計量器、儲存用量、應用程式安裝大小和位置等)*至一個集中視圖，以幫您控制系統效能；
- *App Backup* 可讓您將應用程式備份至 SD 卡並稍後將其還原；
- *Spam and Scam* 功能可讓您將 SMS 訊息標記為垃圾郵件，以及將網站標記為欺詐網站；
- 如果手機被盜可遠端*清除個人資料*

- *安全網頁瀏覽*可讓您即時監視您造訪的網頁。

如需詳細資訊，請造訪專屬的 AVG 網頁，也可以在其中立即下載該元件。若要下載該元件，可以使用我的應用程式對話方塊中的 AVG Mobilation 連結。

7.4. AVG PC Tuneup

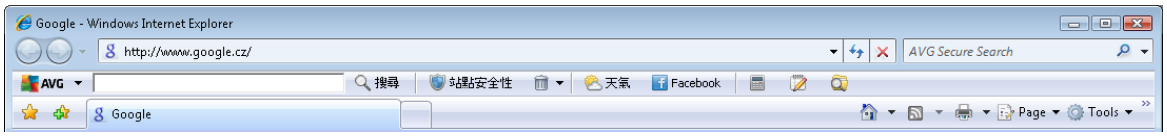
AVG PC Tuneup 應用程式是用於進行詳細系統分析和修正的進階工具，例如分析可以如何提高您電腦的速度以及整體效能。***AVG PC Tuneup*** 功能包括：

- 磁碟清理工具 - 移除減緩電腦速度的垃圾檔案。
- 磁碟重組 - 重組磁碟機並將系統檔案的安置最佳化。
- 登錄清理工具 - 修復登錄錯誤以增加電腦穩定性。
- 登錄重組 - 壓縮登錄，消除使用記憶體的懸殊。
- 磁碟醫生 - 尋找不良的磁區、遺失的叢集和目錄錯誤，並修復它們。
- 網際網路最佳化工具 - 針對特定網際網路連線量身訂做一體適用的設定。
- 追蹤清除工具 - 移除電腦和網際網路使用的歷程記錄。
- 磁碟清除工具 - 清除磁碟上的可用空間，以防機密資料的復原。
- 檔案攪碎工具 - 清除磁碟或 USB 隨身碟上所選檔案，使之無法復原。
- 檔案復原 - 復原從磁碟、USB 隨身碟或相機意外刪除的檔案。
- 重複檔案尋找工具 - 有助於尋找和移除浪費磁碟空間的重複檔案。
- 服務管理員 - 停用延緩電腦速度的多餘服務。
- 啟動管理員 - 允許使用者管理在 Windows 開機時自動啟動的程式。
- 解除安裝管理員 - 徹底解除安裝您不再需要的軟體程式。
- 調整管理員 - 允許使用者微調上百種隱藏的 Windows 設定。
- 工作管理員 - 列出所有執行中的程序、服務和鎖定檔案。
- 磁碟總管 - 顯示哪些檔案占用電腦上最多的空間。
- 系統資訊 - 提供有關已安裝軟硬體的詳細資訊。

如需詳細資訊，請造訪專屬的 AVG 網頁，也可以在其中立即下載該元件。若要這麼做，您可以使用我的應用程式對話方塊內的 AVG PC Tuneup。

8. AVG Security 工具列

AVG Security Toolbar 是與 LinkScanner 元件緊密搭配運作的工具，可在您上網時充分保護您的安全。您可以選擇是否要在 **AVG Internet Security 2012** 內安裝 ***AVG Security Toolbar***，安裝程序期間會邀請您決定是否應該安裝該元件。***AVG Security Toolbar*** 可直接在您的網際網路瀏覽器中使用。目前支援的網際網路瀏覽器有 Internet Explorer (*6.0 版及更高版本*)，以及/或 Mozilla Firefox (*3.0 版及更高版本*)。不支援其他任何瀏覽器 *(如果您使用的是非傳統的網際網路瀏覽器，例如 Avant Browser，可能會遇到無法預期的行為)*。

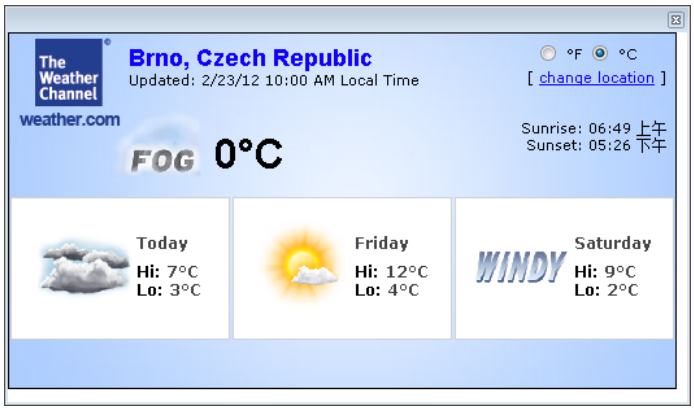


AVG Security Toolbar 包含下列各項：

- ***AVG 標誌*** 含下拉式功能表：
  - ***使用 AVG Secure Search*** - 允許您直接從 ***AVG Security Toolbar*** 使用 ***AVG Secure Search*** 引擎進行搜尋。Search-Shield 服務會持續檢查所有搜尋結果，您絕對可以安心上網。
  - ***目前威脅層級*** - 開啟病毒實驗室網頁，以圖形方式顯示網路上目前的威脅層級。
  - ***AVG Threat Labs*** - 開啟特定的 ***AVG Threat Lab*** 網站 *(位於 http://www.avgthreatlabs.com)*，您可線上找到各種網站安全性以及目前威脅層級的相關資訊。
  - ***Toolbar 說明*** - 開啟涵蓋所有 ***AVG Security Toolbar*** 功能的線上說明。
  - ***提交產品意見*** - 開啟一個網頁，您可以填寫內含的表單，告訴我們您對 ***AVG Security Toolbar*** 的想法。
  - ***關於...*** - 開啟一個新視窗，內含目前安裝的 ***AVG Security Toolbar*** 版本的資訊。
- ***搜尋欄位*** - 使用 ***AVG Security Toolbar*** 搜尋網際網路，因為顯示的所有搜尋結果絕對百分百安全，因此絕對安全無虞。在搜尋欄位中填寫關鍵字或字詞，然後按一下 ***搜尋*** 按鈕 *(或 Enter 鍵)*。Search-Shield 服務會持續檢查所有搜尋結果 *(在 LinkScanner 元件內)*。
- ***站點安全性*** - 此按鈕可開啟提供您所造訪頁面之當前威脅層級 (*目前為安全*) 的相關資訊的新對話方塊。可以展開此簡要概覽，並在瀏覽視窗 (*檢視完整報告*) 中與有關頁面權限的所有安全活動的完整詳細資訊一起顯示：

- ***刪除*** - 「垃圾回收筒」按鈕提供下拉菜單，您可以選擇您是要刪除有關瀏覽、下載、線上論壇還是一次刪除所有的搜尋歷史記錄。

- ***天氣*** - 該按鈕會開啟一個新對話方塊，提供當地目前天氣的相關資訊，以及未來兩天的天氣預測。此項資訊定期每隔 3-6 小時就會更新一次。您可以在該對話方塊中手動變更所要的位置，以及決定以攝氏或是華氏來查看溫度資訊。



- ***Facebook*** - 此按鈕允許您直接從AVG Security Toolbar連線到 Facebook ***社交網路***。

- 供快速存取這些應用程式的捷徑按鈕：***小算盤***、***記事本***、***Windows 檔案總管***.

9. AVG Do Not Track

AVG Do Not Track 幫您識別收集您線上活動資料的網站。您瀏覽器列中的圖示顯示收集有關您的活動資料的網站和廣告商，並讓您選擇允許或禁止。

- ***AVG Do Not Track*** 為您提供有關各個服務隱私權原則的其他資訊以及從服務退出的直接連結 (如果適用)。
- 此外，***AVG Do Not Track*** 支援 W3C DNT 協議以自動通知您不想要被追蹤的那些站點。此通知預設已啟用，但是可以隨時變更。
- ***AVG Do Not Track*** 服務根據以下條款和條件提供：
- ***AVG Do Not Track*** 預設已啟用，但是可以方便停用。相關指示可在常見問題集文章停用 AVG Do Not Track 功能中找到。
- 有關 ***AVG Do Not Track*** 的更多資訊，請造訪我們的網站。

當前，***AVG Do Not Track*** 功能在 Mozilla Firefox、Chrome 和 Internet Explorer 瀏覽器中受支援。*(在 Internet Explorer 中，AVG Do Not Track 圖示位於命令列的右側。使用瀏覽器的預設值查看 AVG Do Not Track 圖示時，您可能會遇到問題，請確保您已啟用命令列。如果您仍然無法看到圖示，請將命令列拖至左側，以顯示此工具列中可用的所有圖示和按鈕。)*

9.1. AVG Do Not Track 介面

在線上時，***AVG Do Not Track*** 偵測到任何類型的資料收集活動會儘快提出警告。您將看到以下對話框：

所有偵測到的資料收集服務按照名稱列示在***此頁面上的追蹤器***概觀中。以下是 ***AVG Do Not Track*** 識別的三種資料收集活動類型：

- ***網站分析*** *(依預設為允許)*：這些服務用於提高個別網站的效能和體驗。在此類別中，您可以找到 Google Analytics、Omniture 或 Yahoo Analytics 等服務。我們建議您不要封鎖網站分析服務，因為網站可能不會按預期運行。

- ***社交按鈕*** *(依預設為允許)*：專為提高社交網路體驗而設計的元件。社交按鈕用於社交網路到您要造訪的站點。如果您登入，這些按鈕會收集有關您線上活動的資料。社交按鈕包括：Facebook Social Plugins、Twitter Button、Google +1。

- ***廣告網路*** *(部分依預設為封鎖)*：這些服務直接或間接地收集或共用有關您在多個網站的線上活動資料，為您提供不同於基於內容廣告的個性化廣告。這基於其網站上提供的每個網路廣告的隱私權原則而確定。依預設，某些廣告網路為已封鎖。

注意：*根據在網站後台執行的服務，以上所述部份可能有三個不顯示在「AVG Do Not Track」對話方塊中。*

該對話方塊中還包含兩個超連結：

- ***什麼是追蹤?***- 按一下對話方塊上半部分中的此連結，您將被重新導向至專屬網頁，其中提供有關追蹤原則的詳細說明和特定追蹤類型的說明。

- ***設定*** - 按一下對話方塊下半部分中的此連結，您將被重新導向至專屬網頁，從中您可以設定各個 ***AVG Do Not Track*** *參數的特定組態 (請參閱 AVG Do Not Track 設定一章瞭解詳細資訊)。*

9.2. 有關追蹤程序的資訊

偵測到的資料收集服務的清單僅提供特定服務的名稱。為了就封鎖還是允許個別服務做出正確的決定，您可能需要瞭解更多。將滑鼠移至各別清單項目。將顯示資訊泡泡圖，提供有關服務的詳細資料。您將瞭解服務收集個人資料還是其他可用的資料；是否與第三方共用資料，以及是否編輯收集的資料進一步用於其他目的。

在下方的資訊泡泡圖中，您可以看到***隱私政策***超連結，可將您重新導向包含所偵測服務之隱私政策的網站。

9.3. 封鎖追蹤程序

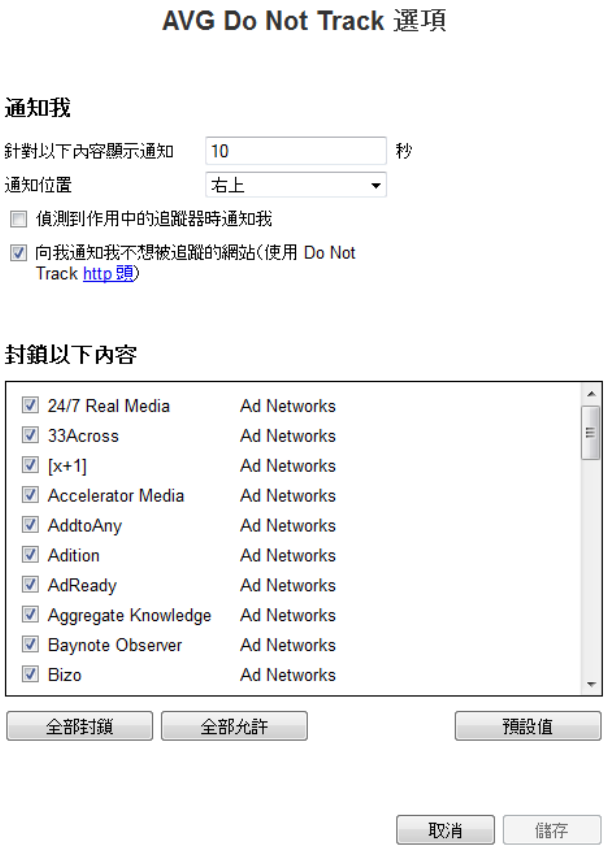
透過所有廣告網路/社交按鈕/網站分析的完整清單，有選項可以控制應封鎖哪些服務。您有兩種選擇：

- ***全部封鎖*** - 按一下位於對話方塊底部的此按鈕，說明您不想存在任何資料收集活動。*(但是，請注意，此動作可能會破壞服務正在執行的個別網頁上的功能！)*
-  - 如果您不想一次封鎖所有偵測到的服務，您可以單獨指定允許或封鎖某服務。您可以允許執行部分偵測到的系統 *(例如，網站分析)* 。這些系統將收集到的資料用於自己的網站優化，並且透過此方式改進所有使用者的常用網際網路環境。但是，您可以同時封鎖被分類為廣告網路之所有程序的資料收集活動。只需按一下每個服務旁邊的  圖示以封鎖資料收集 *(程序名稱將顯示為刪除)* 或再次允許資料收集。

9.4. AVG Do Not Track 設定

直接在 ***AVG Do Not Track***對話方塊中，只有一個組態選項：在底部您可以看到***偵測到作用中的追蹤器時通知我***核取方塊。依預設，此項目為退出狀態。標記該核取方塊，以確認您每次進入包含未封鎖之新資料收集服務的網頁時，都通知您。標記後，如果 ***AVG Do Not Track***在您目前瀏覽的網頁中偵測到新的資料收集服務，您的螢幕上將顯示通知對話方塊。否則，僅 ***AVG Do Not Track***圖示 *(位於您瀏覽器的命令列)* 會從綠色變為黃色，以通知您偵測到新的服務。

但是，在 ***AVG Do Not Track***對話方塊的底部，您可以找到***設定***連結。按一下連結，重新導向到您可以指定詳細的 ***AVG Do Not Track 選項***的頁面：



- ***通知位置*** *(依預設為右上角)* - 開啟下拉式功能表，指定您想要 ***AVG Do Not Track*** 對話方塊在您螢幕中的顯示位置。
- ***顯示通知的時間*** *(依預設為 10)* - 在此欄位中，您可以指定您希望 ***AVG Do Not Track***通知在您螢幕上的顯示時間 (以秒為單位)。您可以指定的範圍為 0 到 60 秒 *(如果選擇 0，通知將不會顯示在您的螢幕上)*。
- ***偵測到作用中的追蹤器時通知我*** *(依預設為關閉)* - 標記該核取方塊，以確認您每次進入包含未封鎖之新資料收集服務的網頁時，都通知您。核取後，如果 ***AVG Do Not Track在您目前瀏覽的網頁中偵測到新的資料收集服務，您的螢幕上將顯示通知對話方塊。***否則，僅 ***AVG Do Not Track***圖示 *(位於您瀏覽器的命令列)會從綠色變為黃色，以通知您偵測到新的服務。*
- ***通知網站我不想被追蹤*** *(依預設為開啟)* - 保持此選項為開啟，確認您想要 ***AVG Do Not Track***通知所偵測資料收集服務的提供商您不想被追蹤。
- ***封鎖以下內容*** *(依預設為允許所列出的所有資料收集服務)* - 在此區段，您可以看到包含已知資料收集服務 (可被分類為廣告網路) 清單的方塊。依預設，***AVG Do Not Track***會自動封鎖部分廣告網路，其他廣告網路是封鎖還是允許，還取決於您的決定。若要這樣做，只需按一下清單下的***全部封鎖***按鈕。

在 ***AVG Do Not Track 選項***頁面中可用的控制按鈕如下所述：

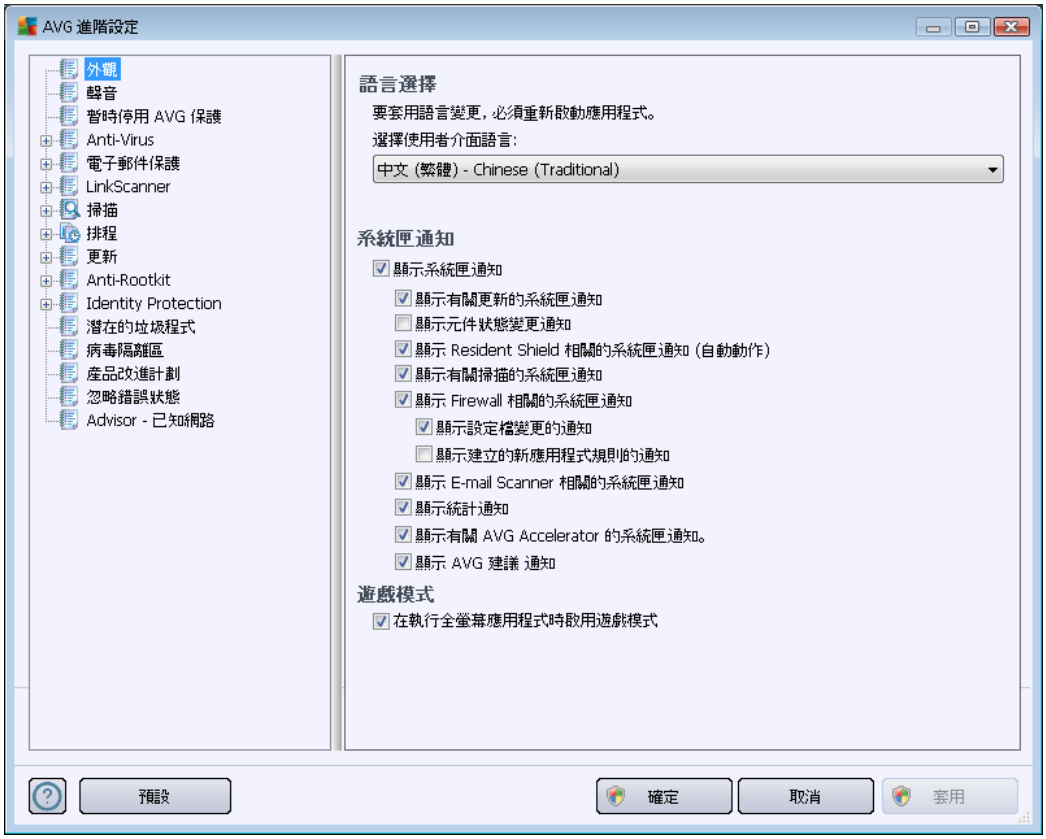
- ***全部封鎖*** - 按一下可立即封鎖上面方塊中列出並分類為廣告網路的所有服務；
- ***全部允許*** - 按一下可立即解除封鎖上面方塊中列出並分類為廣告網路的所有之前封鎖的服務；
- ***預設*** - 按一下可放棄您所有的自訂設定，並恢復預設組態；
- ***儲存*** - 按一下可套用並儲存所有指定的組態；
- ***取消*** - 按一下可取消所有之前指定的設定。

10. AVG 進階設定

AVG Internet Security 2012 會開啟一個叫作***進階 AVG 設定***的新視窗，顯示進階組態選項。這個視窗分成兩個部分 :左邊提供程式組態選項的樹狀目錄式巡覽。選取您要變更其組態 (*或其特定部分*) 的元件，即可在視窗右邊部分開啟編輯對話方塊。

10.1. 外觀

巡覽樹狀目錄的第一個項目，***外觀***是指 **AVG Internet Security 2012** 使用者介面的一般設定，還提供一些應用程式行為的基本選項：

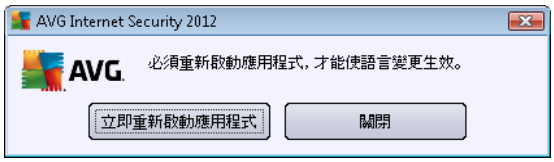


語言選擇

您可以在***語言選擇***區段中從下拉式功能表選擇所要的語言。所選的語言接著將用於整個 **AVG Internet Security 2012** 使用者介面。下拉式功能表只會提供您之前在安裝程序期間選擇要安裝的語言 (*請參閱自訂選項*一章)，外加英文 (*預設情況下，永遠會自動安裝英文*)。您必須重新啟動應用程式，才能完成將 **AVG Internet Security 2012** 切換到其他語言。請遵循以下步驟：

- 在下拉式功能表中選取所要的應用程式語言
- 按一下***套用***按鈕*(對話方塊的右下角) 確認您的選擇*

- 按一下***確定***按鈕進行確認
- 隨即會出現一個新對話方塊，告知您必須重新啟動 **AVG Internet Security 2012**
- 按一下***立即重新啟動應用程式***按鈕同意重新啟動程式，並稍待片刻讓語言變更生效：



系統匣通知

您可以在此區段中隱藏在系統匣通知顯示 **AVG Internet Security 2012** 應用程式的狀態。預設情況下會允許顯示系統通知。強烈建議您保持此組態！系統通知會告知如掃描或更新程序啟動，或 **AVG Internet Security 2012** 元件狀態變更等狀況。您肯定應該注意這些通告！

但是如果出於某種原因，您決定不希望透過這種方式收到通知，或者只希望看到特定通知 *(關於特定的 AVG Internet Security 2012 元件)*，您可以透過核取/取消核取下列選項來定義和指定您的喜好設定：

- ***顯示系統匣通知*** *(預設為開啟)* - 預設情況下會顯示所有通知。取消核取此項目可完全關閉所有系統通知的顯示。開啟時，您可以進一步選取要顯示哪些特定通知：
  - ***顯示有關更新*** *的系統匣通知 (預設為開啟)* - 決定是否要顯示有關 **AVG Internet Security 2012** 更新程序啟動、進度及完成的資訊。
  - ***顯示元件狀態變更通知*** *(預設為關閉)* - 決定是否要顯示有關元件的活動/無活動，或其可能問題的資訊。報告元件的錯誤狀態時，此選項等同於報告任何 **AVG Internet Security 2012** 元件問題的系統匣圖示的通知功能。
  - ***顯示 Resident Shield 相關的系統匣通知 (自動動作)*** *(預設為開啟)* - 決定要顯示還是隱藏有關檔案儲存、複製或開啟中的程序的資訊 (*只有當 Resident Shield 自動修復選項開啟時，才會顯示此組態*)。
  - ***顯示有關掃描*** *的系統匣通知 (預設為開啟)* - 決定是否應該顯示有關已排程掃描的自動啟動、進度及結果的資訊。
  - ***顯示 Firewall相關的系統匣通知*** *(預設為開啟)* - 決定是否應該顯示有關 Firewall 狀態和程序的資訊，例如元件的啟動/停用警告，可能的流量封鎖等。此項目提供其他兩項特定的選項 *(如需各自的詳細說明，請參閱本文的 Firewall 一章)*：
    - ***顯示設定檔變更的通知****(預設為開啟)* - 通知您有關 Firewall 設定檔的自動變更。
    - ***顯示建立的新應用程式規則的通知*** *(預設為關閉)* - 通知您有關根據安全清單為新應用程式自動建立 Firewall 規則的資訊。

- ***顯示 E-mail Scanner 相關的系統匣通知*** *(預設為開啟)* - 決定是否要顯示有關所有傳入和傳出電子郵件訊息掃描的資訊。

- ***顯示統計通知*** *(預設為開啟)* - 將該選項保持核取狀態，可在系統匣中顯示常規統計審核通知。

- ***顯示有關 AVG 加速器的系統匣通知*** *(預設為開啟)* - 決定是否應該顯示 ***AVG 加速器***活動的資訊。***AVG 加速器***服務可使線上視訊播放更順暢，並且更方便進行其他下載。

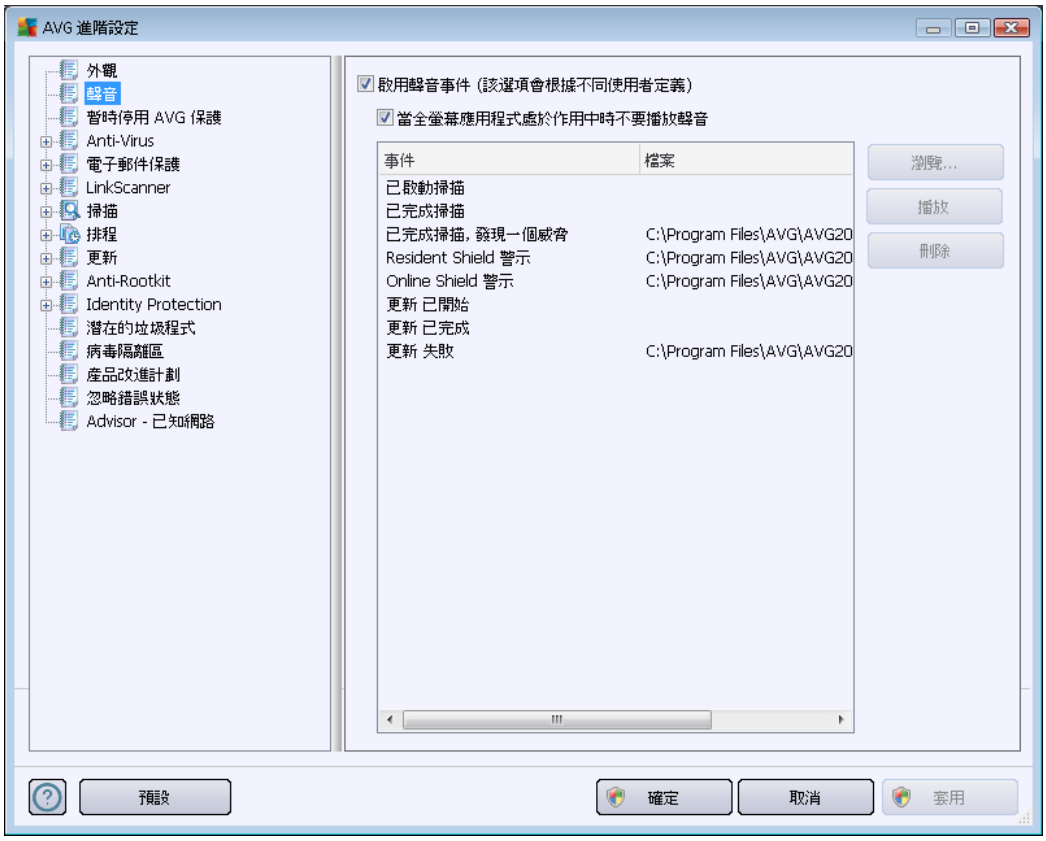
- ***顯示 AVG Advice 效能通知*** *(預設為開啟)* - ***AVG Advice*** 會觀察支援的網際網路瀏覽器 *(Internet Explorer、Chrome、Firefox、Opera 和 Safari)* 效能，並且會在瀏覽器過度使用建議的記憶體時通知您。您的電腦速度在這種情況下可能會大幅減緩，因此建議您重新啟動網際網路瀏覽器來加快處理器速度。將***顯示 AVG Advice 效能通知***項目保持開啟狀態，以便獲得通知。

遊戲模式

此 AVG 功能是用於當可能的 AVG 球形通知 (*例如在排程的掃描開始時顯示*) 可能干擾 (*它們可能使應用程式最小化或破壞其圖像*) 全螢幕應用程式的執行時。若要避免這種情況，請將***在執行全螢幕應用程式時啟用遊戲模式***選項的核取方塊保留為核取狀態 (*預設設定*)。

10.2. 聲音

您可以在***聲音***對話方塊中指定是否想要透過聲音通知功能收到特定 **AVG Internet Security 2012** 動作的通知：



該設定僅對目前的使用者帳戶有效。也就是說，電腦上的每個使用者均可擁有他們自己的聲音設定。如果您想要允許聲音通知，請將***啟用聲音事件***選項保持核取狀態 (*該選項預設為開啟*) 已啟動所有相關動作的清單。另外，建議您核取***當全螢幕應用程式作用中時不要播放聲音***選項在可能會發生干擾的情況下隱藏聲音通知 (*另請參閱本文件中進階設定/外觀一章的遊戲模式*)。

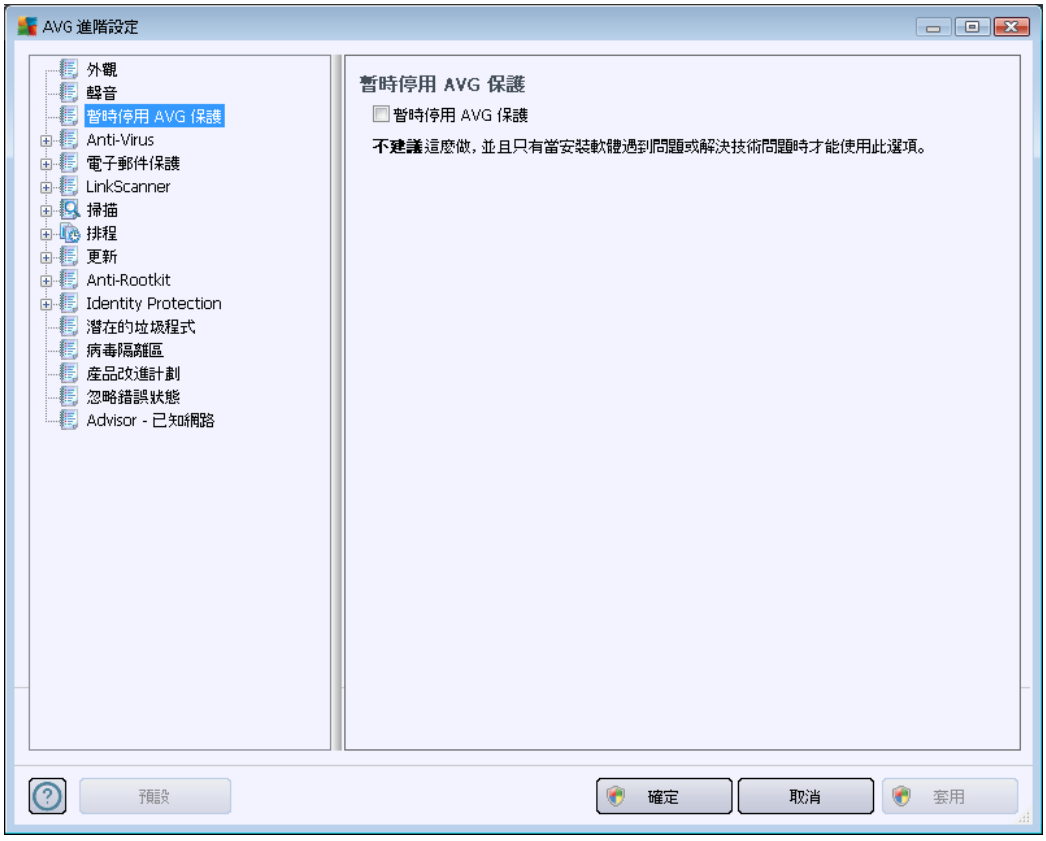
控制按鈕

- ***瀏覽*** - 從清單選取個別事件後，使用***瀏覽***按鈕可搜尋您的磁碟尋找想要指派給該事件的聲音檔。*(請注意，目前僅支援 *.wav 聲音！)*
- ***播放*** - 若要聆聽所選的聲音，請在清單中反白該事件，再按***播放***按鈕。
- ***刪除*** - 使用***刪除***按鈕即可移除指派給特定事件的聲音。

10.3. 暫時停用 AVG 保護

在 ***暫時停用 AVG 保護***對話方塊中，您可以選擇一次關閉由 **AVG Internet Security 2012** 提供的全面性保護。

請記住，除非迫不得已，請勿使用此選項！



在大多數情況下，***不必***在安裝新軟體或驅動程式之前停用 **AVG Internet Security 2012**，即使安裝程式或軟體精靈建議首先關閉正在執行的程式和應用程式以確保安裝程序期間不會出現意外中斷，也沒有此必要。如果您在安裝期間真的遇到問題，可試著先停用常駐保護 (*啟用 Resident Shield*)。如果您確實不得不暫時停用 **AVG Internet Security 2012**，則必須在完成其他工作後立即重新啓用它。如果您在反病毒軟體停用時連線至網際網路或網路，您的電腦可能很容易受到攻擊。

如何停用 AVG 保護

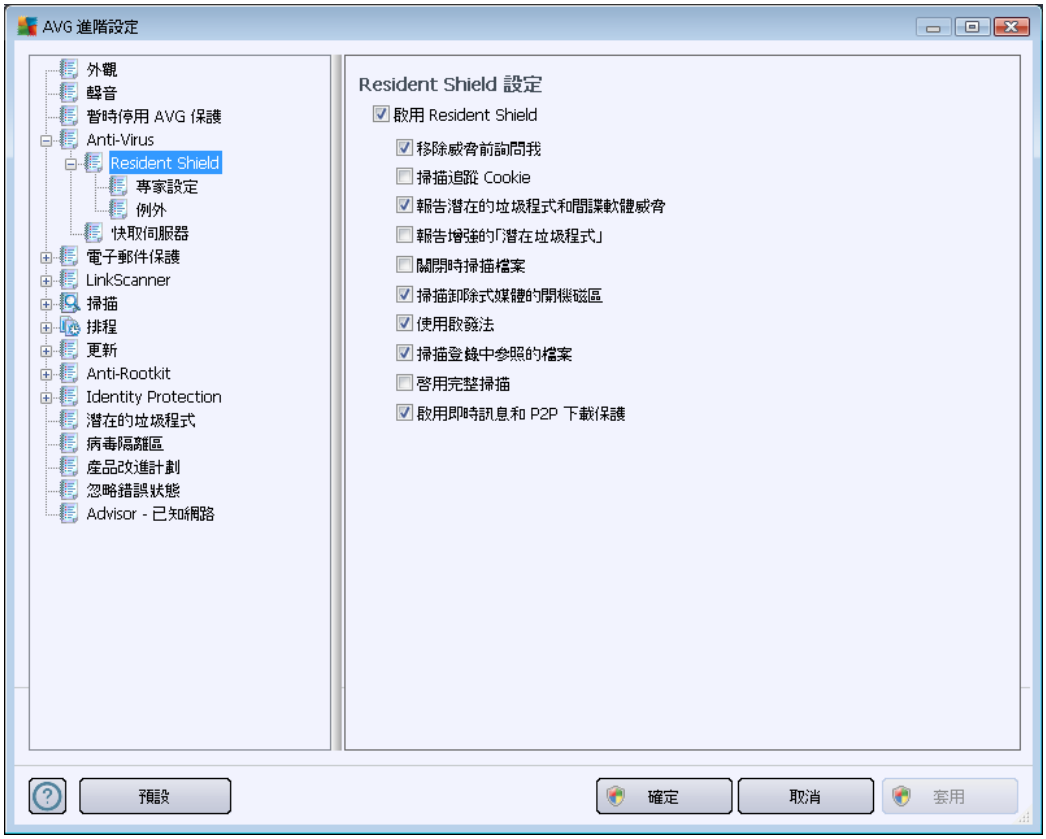
- 標示***暫時停用 AVG 保護***核取方塊，並且按一下***套用***按鈕來確認您的選擇
- 在新開啟的***暫時停用 AVG 保護***對話方塊中指定要停用 **AVG Internet Security 2012** 多久時間。預設情況下，保護將關閉 10 分鐘，這應該足以完成所有常見的工作，例如安裝軟體等。請注意，初始時間限制可能設定為 15 分鐘，但基於安全性理由，您無法用自己的值覆寫該初始值。經過指定的時段之後，將自動重新啟動所有停用的元件。

10.4. Anti-Virus

Anti-Virus *元件會持續保護您的電腦免於所有已知類型的病毒和間諜軟體的侵害 (包括所謂的隱匿和非作用中的惡意軟體，亦即已下載但尚未啟動的惡意軟體)。*

10.4.1. Resident Shield

Resident Shield 為檔案和資料夾提供即時保護，使它們免遭病毒、間諜軟體和其他惡意軟體的攻擊。



您可以在 ***Resident Shield 設定***對話方塊中，透過核取/取消核取***啟用 Resident Shield*** 項目完全啟動或停用常駐保護 (*此選項預設為開啟*)。此外，您還可以選擇應該啟用常駐保護的哪些功能：

- ***移除威脅前詢問我*** *(預設為開啟)* –核取以確保常駐防護不會自動執行任何動作；否則，它將會顯示描述所偵測到的威脅的對話方塊，可讓您決定該如何操作。如果您未核取對話方塊，則**AVG Internet Security 2012**將會自動修復感染，如果無法修復，則該物件將移動至病毒隔離區。

- ***掃描追蹤 Cookie*** (*預設為關閉*) - 此參數定義掃描期間應偵測 cookie。(*HTTP cookie 用於驗證、追蹤和維護使用者的特定資訊，如站點偏好設定或電子購物車內容。*)

- ***報告潛在的垃圾程式和間諜軟體威脅*** (*預設為開啟*) - 核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。

- ***報告增強的潛在垃圾程式*** (*預設為關閉*) - 標示此選項可偵測延伸的間諜軟體套件 :這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- ***關閉時掃描檔案*** (*預設為關閉*) - 關閉時掃描可確保 AVG 掃描處於開啟和關閉狀態的作用中物件 (例如應用程式、文件等…) ;此功能可幫助保護您的電腦免遭一些複雜病毒的攻擊。

- ***掃描卸除式媒體的開機磁區*** (*預設為開啟*)

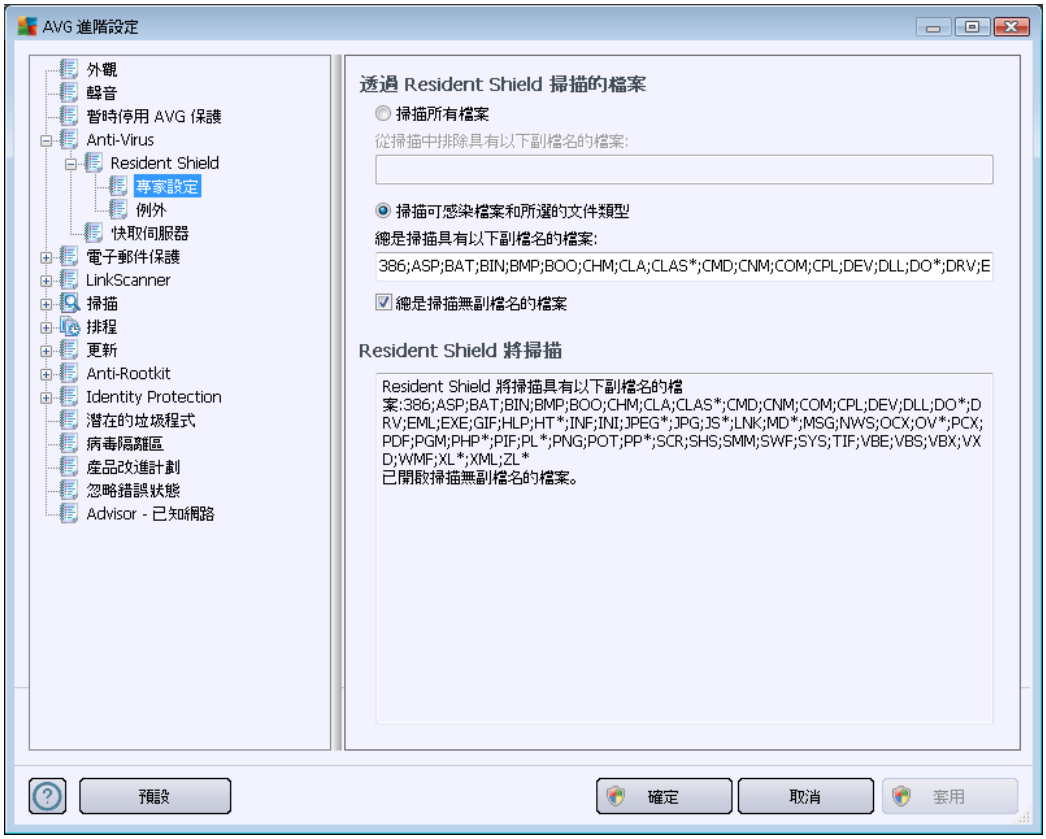
- ***使用啟發法*** (*預設為開啟*) - 啟發法分析將用於偵測 (*在虛擬電腦環境中，對掃描物件的指令進行動態模擬*)。

- ***掃描登錄中參照的檔案*** (*預設為開啟*) - 此參數定義 AVG 將掃描所有新增到登錄的可執行檔案，以防在下次電腦啟動時執行已知的感染檔案。

- ***啟用完整掃描*** (*預設為關閉*) - 在特殊情況下 (*極為緊急的狀況*)，您可以核取此選項來啟動最完整的掃描演算法，這將仔細檢查所有可能的威脅物件。不過請記住，這種方法相當耗時。

- ***啟用即時訊息保護和 P2P 下載保護*** (*預設為開啟*) - 如果您想要驗證即時訊息通訊 (*例如 ICQ、MSN Messenger...*) 和 P2P 下載沒有病毒，請核取此項目。

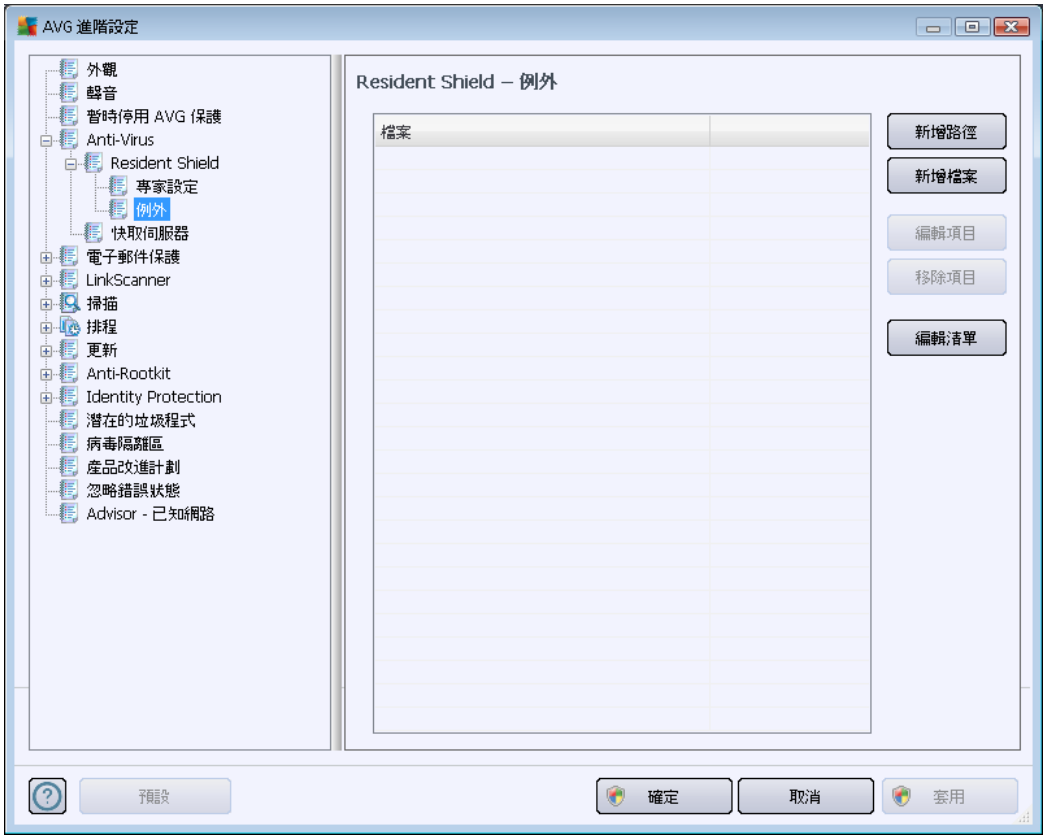
在 ***透過 Resident Shield 掃描的檔案***對話方塊中，可以組態要掃描的檔案 (*根據特定副檔名*)：



標示個別的核取方塊來決定您是要***掃描所有檔案***還是只要***掃描可感染檔案和所選的文件類型***：如果您決定採用後者，可進一步指定定義應該排除在掃描之外的檔案副檔名清單，也可以指定定義無論如何都必須掃描的檔案副檔名清單。

核取***總是掃描無副檔名的檔案*** (*依預設*)，確保常駐防護會掃描任何沒有副檔名且格式不明的檔案。建議您開啓此功能，因為沒有副檔名的檔案都是可疑檔案。

以下區段稱為 ***Resident Shield 將掃描***，當中會概述目前設定，並顯示 ***Resident Shield*** 將實際掃描之內容的詳細概觀。



Resident Shield - 例外對話方塊可讓您定義應該從 ***Resident Shield*** 掃描中排除的檔案和/或資料夾。

除非必要，否則我們強烈建議不要排除任何項目！

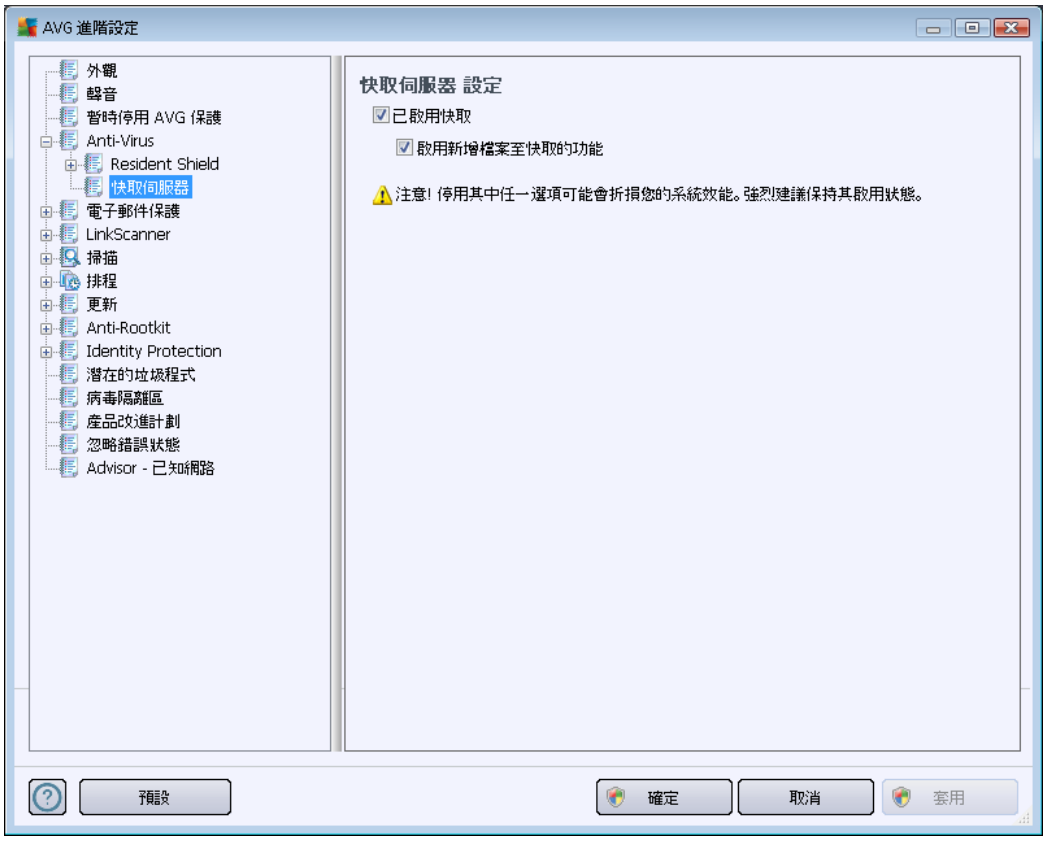
控制按鈕

該對話方塊提供下列控制按鈕：

- ***新增路徑*** - 指定要從掃描排除的目錄，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄
- ***新增檔案*** - 指定要從掃描中排除的檔案，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄
- ***編輯項目*** - 允許您編輯所選資料夾的指定路徑
- ***移除項目*** - 允許您從清單中刪除所選檔案的路徑
- ***編輯清單*** - 允許您在新對話方塊中編輯整個已定義的例外清單，作用就跟標準文字編輯器一樣

10.4.2. 快取伺服器

快取伺服器設定對話方塊是指為了加快所有類型的 **AVG Internet Security 2012** 掃描而設計的快取伺服器程序：



快取伺服器會收集和保留可信任檔案的資訊 (*經過可靠來源數位簽署的檔案即視為可信任檔案*)。之後會將這些檔案自動視為安全檔案，而不需要再掃描，因此掃描期間會跳過這些檔案。

快取伺服器設定對話方塊提供以下組態選項：

- ***啟用快取*** (*預設為開啟*) - 取消核取可關閉***快取伺服器***功能，並清空快取記憶體。請注意，掃描可能變慢，電腦的整體效能可能下降，因為它首先要掃描每一個使用中的檔案以確定是否有病毒或間諜軟體。
- ***啟用新增檔案至快取*** (*預設為開啟*) - 取消核取可停止新增更多檔案至快取記憶體中。所有已加入快取記憶體中的檔案將被保留並使用，直到快取功能完全關閉或是下一次更新病毒庫為止。

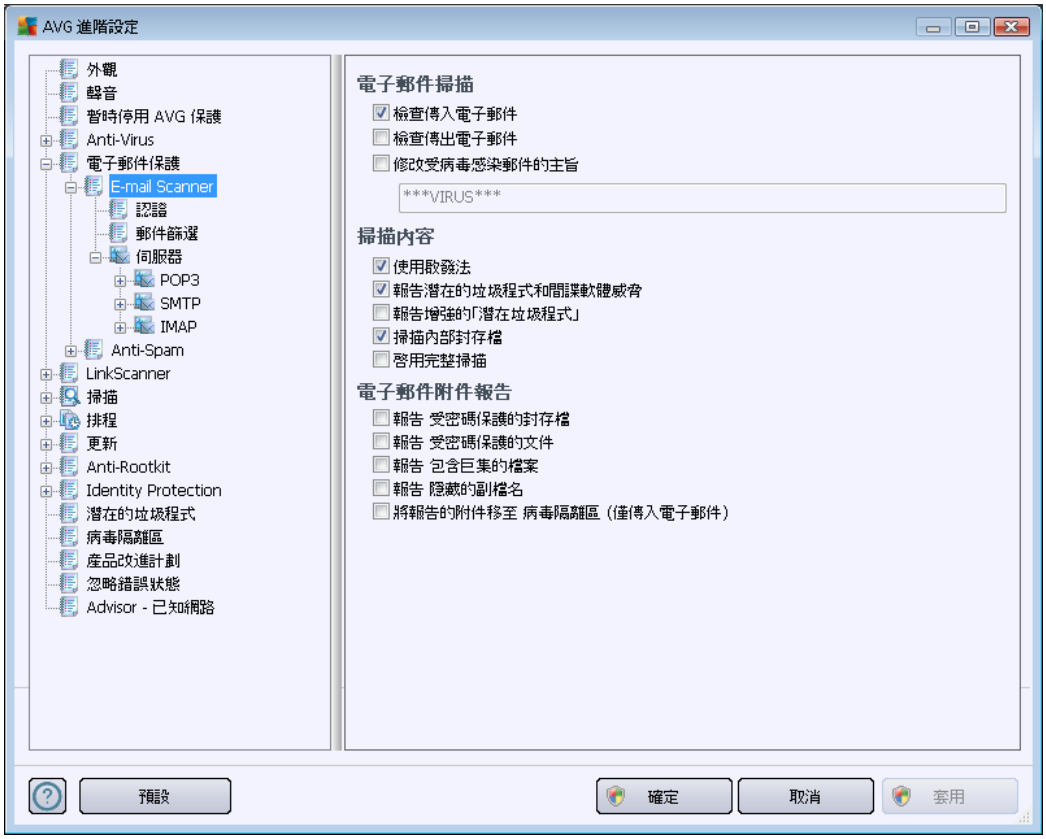
除非有充分的理由關閉快取伺服器，否則強烈建議您保留預設設定，並將兩個選項都保持開啟狀態！不然的話，可能會大幅降低系統速度和效能。

10.5. 電子郵件保護

您可以在***電子郵件保護***區段中編輯 E-mail Scanner 和 Anti-Spam 的詳細組態：

10.5.1. E-mail Scanner

E-mail Scanner 對話方塊由三個區段構成：



電子郵件掃描

您可以在此區段中為傳入和／或傳出的電子郵件訊息設定以下基本資訊：

- ***檢查傳入電子郵件***(*預設為開啟*) – 標記以開啟／關閉掃描傳送到您的電子郵件用戶端的所有電子郵件訊息的選項
- ***檢查傳出電子郵件***(*預設為關閉*) – 標記以開啟／關閉掃描自您的帳戶寄出的所有電子郵件的選項
- ***修改受病毒感染郵件的主旨***(*預設為關閉*) – 如果您想要在掃描的電子郵件訊息被偵測為有病毒感染時收到警告，請標記此項目，並將所要的文字填入文字欄位中。然後，該文字即會新增到每一封受感染電子郵件訊息的「主旨」欄位中，進而便於識別和篩選。預設值為 ***VIRUS***，我們建議保留此值。

掃描屬性

您可以在這個區段中指定電子郵件訊息的掃描方式：

- ***使用啟發法***(*預設為開啟*) – 核取此選項可在掃描電子郵件訊息時使用啟發式偵測方法。開啓此選項後，您不僅可以透過副檔名篩選電子郵件附件，也可以透過考量附件的實際內容來進行篩選。篩選可以在郵件篩選對話方塊中進行設定。

- ***報告潛在的不受歡迎程式和間諜軟體威脅***(*預設為開啟*) – 核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別 :雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。

- ***報告增強的潛在不受歡迎程式***(*預設為關閉*) – 標記此選項來偵測延伸的間諜軟體 :這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- ***掃描封存內部***(*預設為開啟*) – 核取此方塊可掃描附加到電子郵件訊息的封存內容。

- ***啟用完整掃描***(*預設為關閉*) – 在特殊的情況下 *例如懷疑您的電腦受到病毒或入侵程式感染*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

電子郵件附件報告

您可以在這個區段中設定有關潛在危險檔案或可疑檔案的其他報告。請注意，不會顯示警告對話方塊，只會將一段認證文字加到電子郵件訊息的結尾，並且所有這種報告都會列在 E-mail Scanner 偵測 對話方塊中：

- ***報告受密碼保護的封存*** – 受密碼保護的封存 *ZIP、RAR 等*) 無法進行病毒掃描；核取此方塊可將這些封存報告為存在潛在的危險。

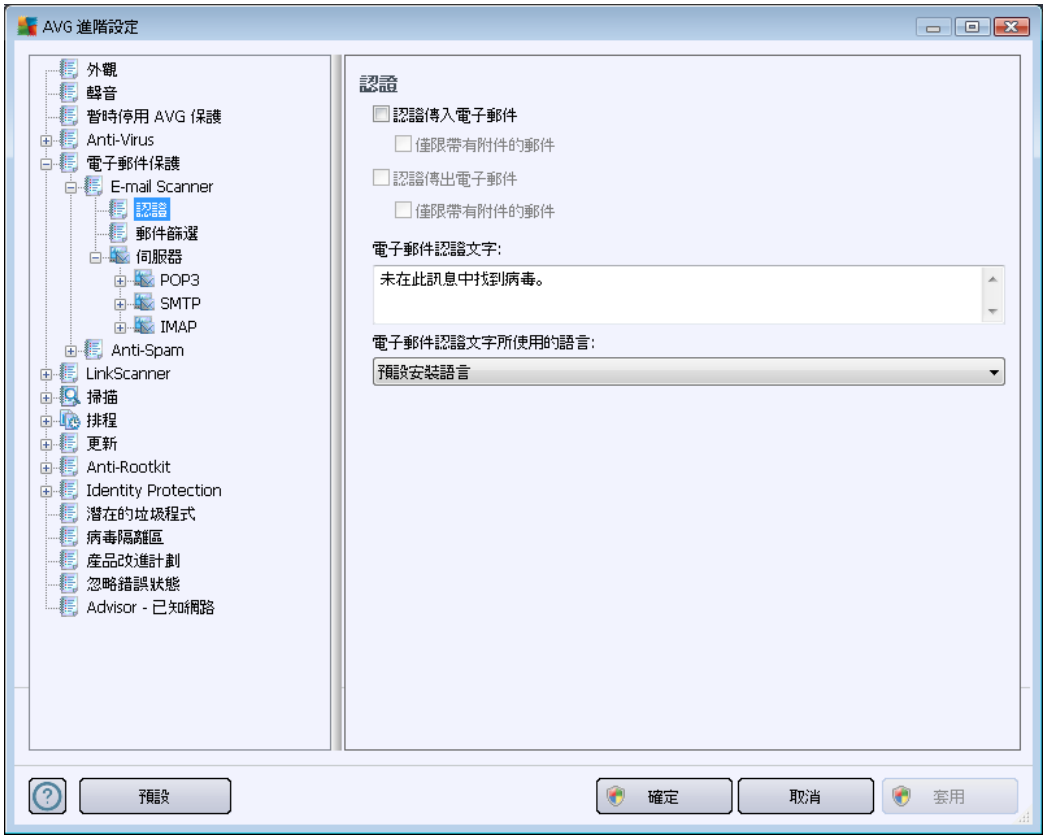
- ***報告受密碼保護的文件*** – 受密碼保護的文件無法進行病毒掃描 ;核取此方塊可將這些文件報告為潛在危險內容。

- ***報告包含巨集的檔案*** –巨集是一種預定義的步驟序列，用於協助使用者更輕鬆地完成某項工作 *例如我們都熟知的 MS Word 巨集*)。因此，巨集可能會包含潛在危險的指示，您可以核取此方塊以確保將包含巨集的檔案報告為可疑內容。

- ***報告隱藏的副檔名*** – 隱藏副檔名可以使諸如可疑的可執行檔 ("something.txt.exe") 等檔案看起來像是無害的純文字檔案 ("something.txt") ;核取此方塊可將這些檔案報告為潛在危險內容。

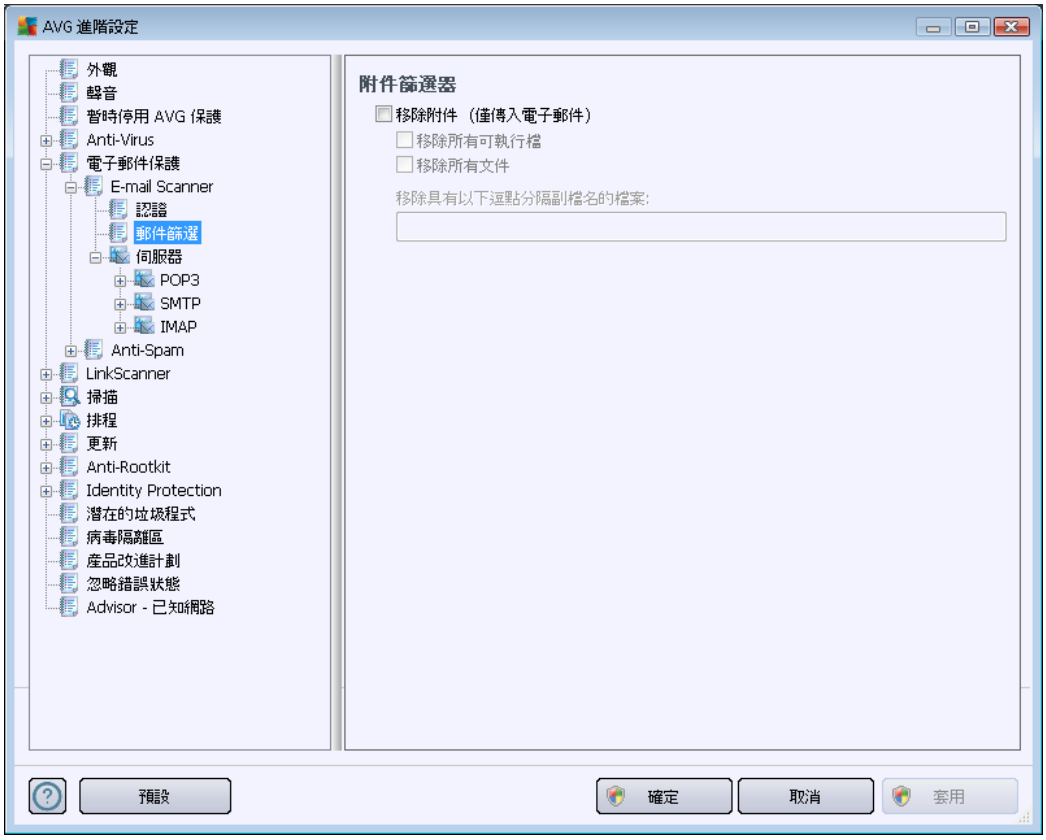
- ***將報告的附件移至病毒隔離區*** – 指定是否要透過電子郵件收到有關以下情況的通知 :偵測到掃描郵件的附件為受密碼保護的封存、受密碼保護的文件、包含巨集的檔案和／或具有隱藏副檔名的檔案。如果在掃描過程中發現這類郵件，定義是否將偵測到的受感染物件移至病毒隔離區。

您可以在***認證***對話方塊中標示特定的核取方塊來決定是否要認證傳入郵件 (***認證傳入電子郵件***) 和/或傳出郵件 (***認證傳出電子郵件***)。您可以針對其中各個選項進一步指定***僅限帶有附件的郵件***參數，只將認證新增到含附件的電子郵件訊息中：



預設情況下，認證文字只包含基本資訊，指出*未在此訊息中找到病毒*。但是，您可以根據需要來擴充或變更這項資訊：將所要的認證文字寫入***電子郵件認證文字***欄位中。您可以在***電子郵件認證文字所使用的語言***區段中進一步定義認證自動產生的部分 (*未在此訊息中找到病毒*) 應該以什麼語言顯示。

注意：*請注意，只有預設文字會以要求的語言顯示，您的自訂文字將不會自動翻譯！*



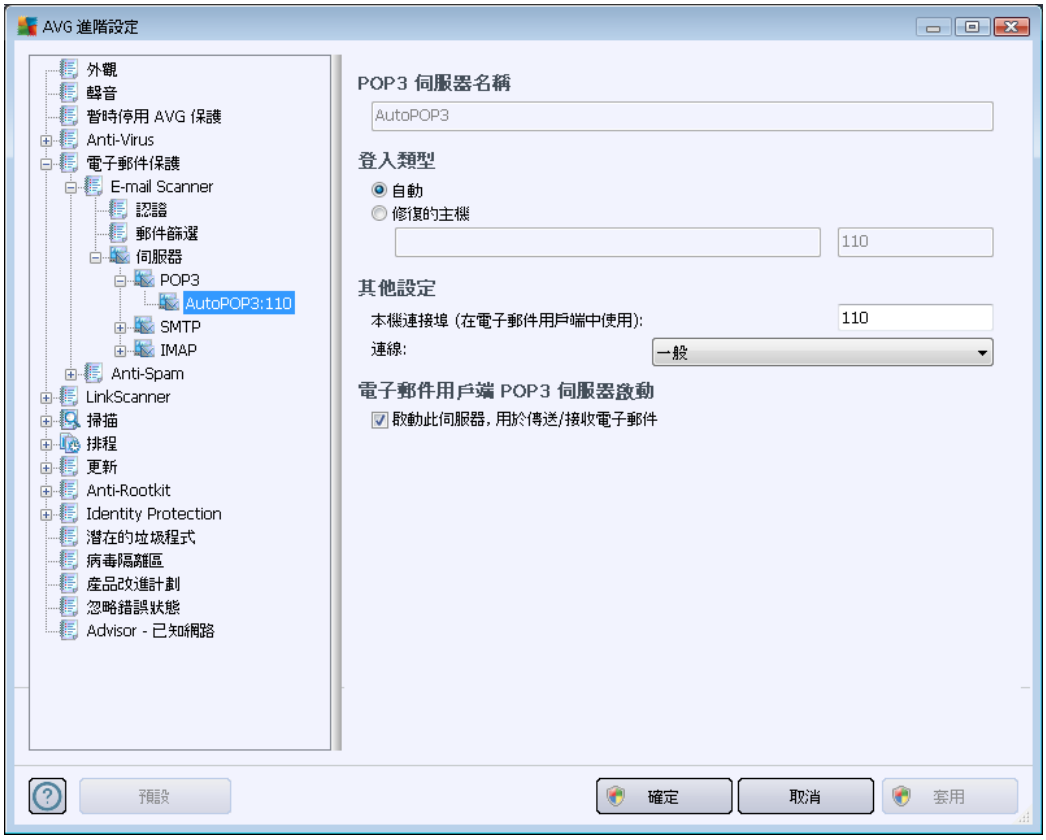
在***附件篩選器***對話方塊中，您可以設定用於電子郵件訊息附件掃描的參數。預設情況下，***移除附件***選項關閉。如果您啟動它，所有偵測為受感染或潛在危險內容的電子郵件訊息附件都將被自動移除。如果要定義應移除的特定附件類型，請選取以下相應選項：

- ***移除所有可執行檔*** - 將刪除所有 *.exe 檔案
- ***移除所有文件*** - 將刪除所有 *.doc、*.docx、*.xls、*.xlsx 檔案
- ***移除具有以下逗點分隔副檔名的檔案*** - 將移除所有具有已定義副檔名的檔案

您可以在***伺服器***區段編輯 E-mail Scanner 伺服器的參數：

- POP3 伺服器
- SMTP 伺服器
- IMAP 伺服器

另外，您也可以使用***新增新伺服器***按鈕來定義用於傳入或傳出郵件的新伺服器。

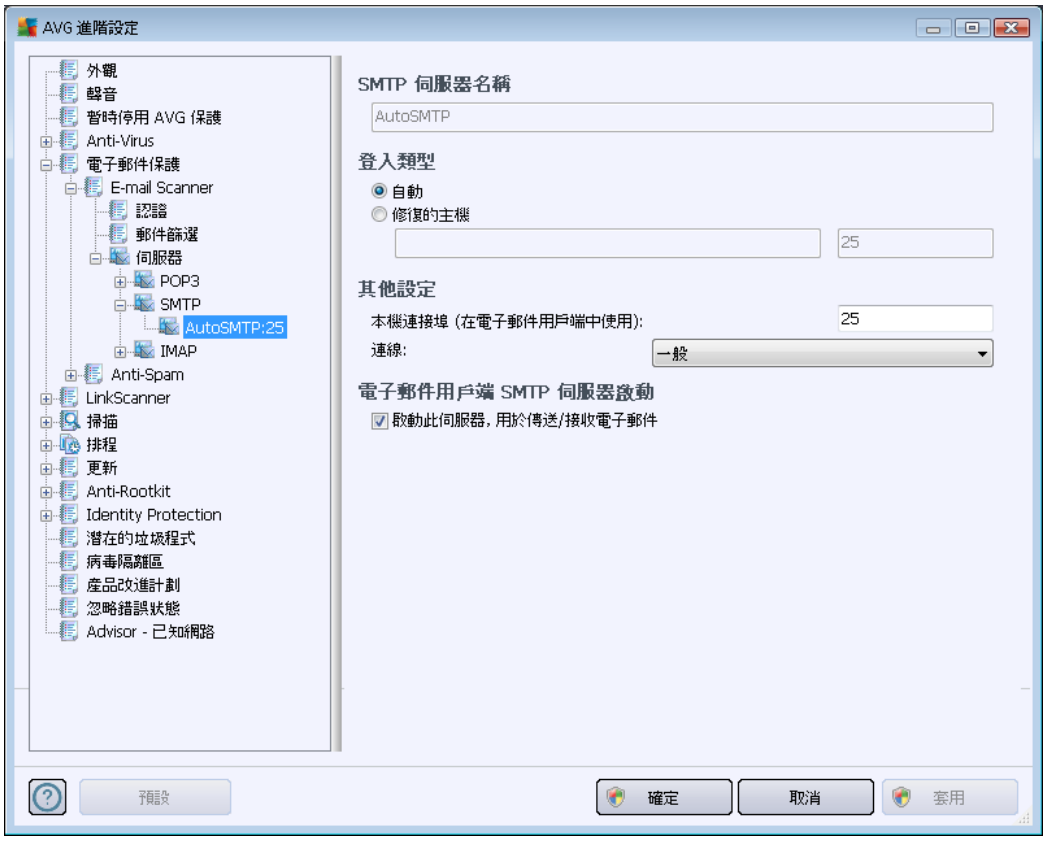


您可以在此對話方塊中 (*透過* ***伺服器/POP3*** 開啟) 設定新的 E-mail Scanner 伺服器，針對傳入郵件使用 POP3 通訊協定：

- ***POP3 伺服器名稱*** - 您可以在此欄位中指定新增的伺服器名稱 (*若要新增 POP3 伺服器，在左側巡覽功能表的 POP3 項目上按一下滑鼠右鍵*)。對於自動建立的 "AutoPOP3" 伺服器，會停用此欄位。
- ***登入類型*** - 定義確定傳入郵件所使用的郵件伺服器的方法：
  - ***自動*** - 根據您的電子郵件用戶端的設定自動執行登入。
  - ***固定主機*** - 在這種情況下，程式總是使用此處指定的伺服器。請指定您的郵件伺服器的位址或名稱。登入名稱保持不變。您可以使用網域名稱 (*如 pop.acme.com*) 和 IP 位址 (*如 123.45.67.89*) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以使用冒號作為分隔符號在伺服器名稱後面指定連接埠 (*如 pop.acme.com:8200*)。用於 POP3 通訊的標準連接埠為 110。
- ***其他設定*** - 指定更多詳細參數：
  - ***本機連接埠*** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 POP3 通訊的連接埠。
  - ***連線*** - 您可以在下拉式功能表中指定要使用的連線方式 (*一般/SSL/預設為*

SSL)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能也僅在目標郵件伺服器支援時才可用。

- ***電子郵件用戶端 POP3 伺服器啟動*** - 核取/取消核取此項目可啟動或停用指定的 POP3 伺服器



您可以在此對話方塊中 (*透過* ***伺服器/SMTP*** 開啟) 設定新的 E-mail Scanner 伺服器，針對傳出郵件使用 SMTP 通訊協定：

- ***SMTP 伺服器名稱*** - 您可以在此欄位中指定新增伺服器的名稱 (*若要新增 SMTP 伺服器，在左側巡覽功能表的 SMTP 項目上按一下滑鼠右鍵*)。對於自動建立的 "AutoSMTP" 伺服器，會停用此欄位。

- ***登入類型*** - 定義確定傳入郵件所使用的郵件伺服器的方法：

  - ***自動*** - 根據您的電子郵件用戶端的設定自動執行登入。

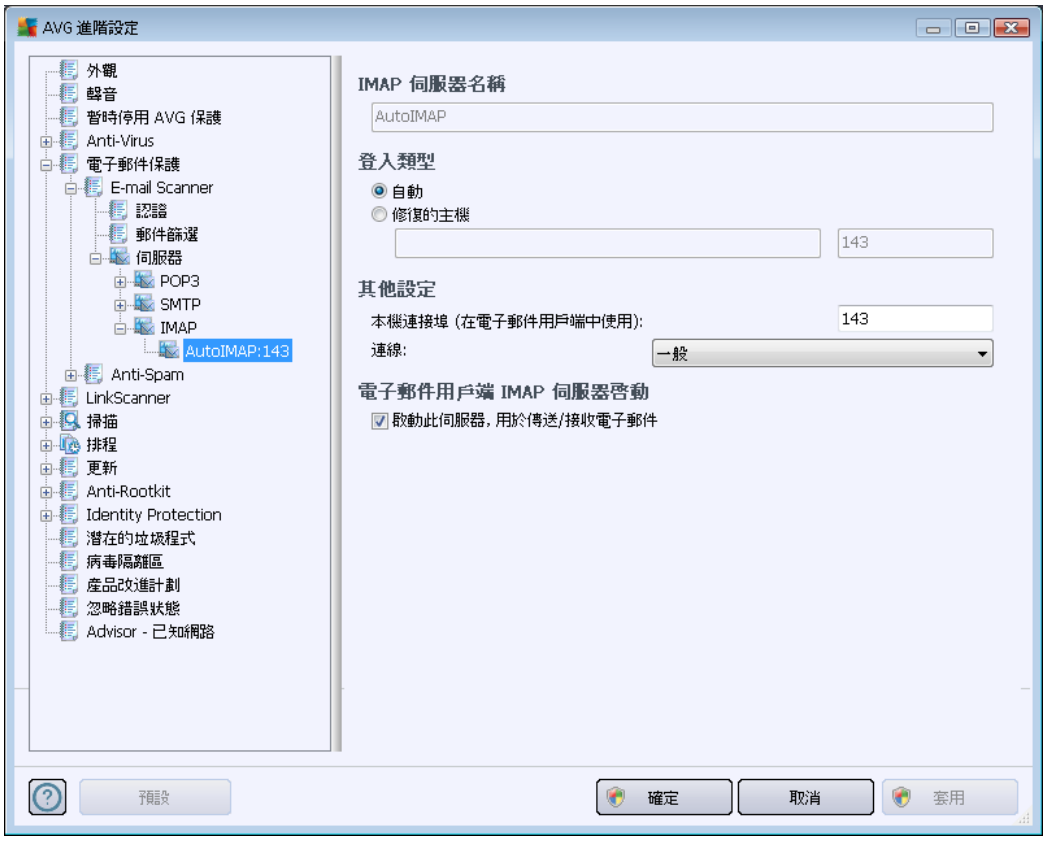
  - ***固定主機*** - 在這種情況下，程式總是會使用此處指定的伺服器。請指定您的郵件伺服器的位址或名稱。您可以使用網域名稱 (*如 smtp.acme.com*) 和 IP 位址 (*如 123.45.67.89*) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以使用冒號作為分隔符號在伺服器名稱後面鍵入連接埠 (*如 smtp.acme.com:8200*)。用於 SMTP 通訊的標準連接埠為 25。

- ***其他設定*** - 指定更多詳細參數：

    - ***本機連接埠*** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 SMTP 通訊的連接埠。

    - ***連線*** - 您可以在此下拉式功能表中指定要使用的連線方式 (*一般/SSL/預設為 SSL*)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能僅在目標郵件伺服器支援時才可用。

- ***電子郵件用戶端 SMTP 伺服器啟動*** - 核取/取消核取此方塊可啟動/停用上面指定的 SMTP 伺服器。



您可以在此對話方塊中 (透過 ***伺服器/IMAP*** 開啟) 設定新的 E-mail Scanner 伺服器，針對傳出郵件使用 IMAP 通訊協定：

- ***IMAP 伺服器名稱*** - 您可以在此欄位中指定新增的伺服器名稱 (*若要新增 IMAP 伺服器，在左側巡覽功能表的 IMAP 項目上按一下滑鼠右鍵*)。對於自動建立的 "AutoIMAP" 伺服器，會停用此欄位。

- ***登入類型*** - 定義確定傳入郵件所使用的郵件伺服器的方法：

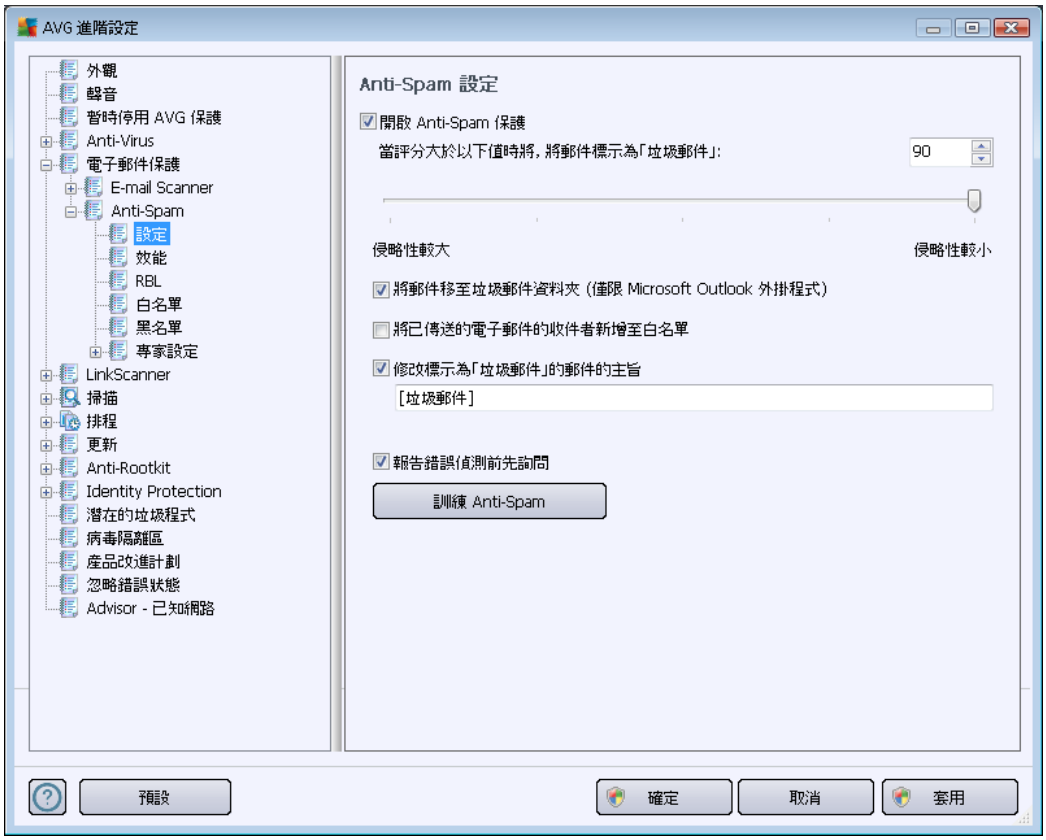
    - ***自動*** - 根據您的電子郵件用戶端的設定自動執行登入。

    - ***固定主機*** - 在這種情況下，程式總是會使用此處指定的伺服器。請指定您的

郵件伺服器的位址或名稱。您可以使用網域名稱 (*如 smtp.acme.com*) 和 IP 位址 (*如 123.45.67.89*) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以使用冒號作為分隔符號在伺服器名稱後面鍵入連接埠 (*例如，imap.acme.com:8200*)。用於 IMAP 通訊的標準連接埠為 143。

- ***其他設定*** - 指定更多詳細參數：
  - ***本機連接埠*** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 IMAP 通訊的連接埠。
  - ***連線*** - 您可以在此下拉式功能表中指定要使用的連線方式 (*一般/SSL/預設為 SSL*)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能僅在目標郵件伺服器支援時才可用。
- ***電子郵件用戶端 IMAP 伺服器啟動*** - 核取/取消核取此方塊可啟用/停用上面指定的 IMAP 伺服器

10.5.2. Anti-Spam



您可以在 ***Anti-Spam 設定***對話方塊中核取/取消核取***開啟 Anti-Spam 保護***核取方塊，以允許/禁止對電子郵件通訊進行反垃圾郵件掃描。此選項預設是處於開啟狀態，除非您確實有必要變更，否則建議保留此組態！

接下來，您還可以選取更高或更低的加強分數標準。***Anti-Spam*** 篩選器會根據數個動態掃描技術，為每封郵件指定一個分數 (*即郵件內容與垃圾郵件的相似程度*)。您可以調整***當評分大於以下值時，將郵件標記為垃圾郵件***設定，方法是輸入值，或左右移動滑桿 (*值的範圍限制為 50 到 90*)。

我們通常建議將閾值設定在 50 到 90 之間，如果您確實不確定，可設為 90。以下是分數閾值的一般說明：

- ***值 80-90*** - 將篩選出很可能是垃圾郵件的電子郵件訊息。某些非垃圾郵件的訊息也可能被誤選。
- ***值 60-79*** - 這是較為加強的組態。可能是垃圾郵件的電子郵件訊息都將被篩選出來。非垃圾郵件的訊息也很可能被誤判。
- ***值 50-59*** - 特別加強的組態。非垃圾郵件的電子郵件訊息很可能被當作真正的垃圾郵件訊息處理。一般情況不建議使用此閾值範圍。

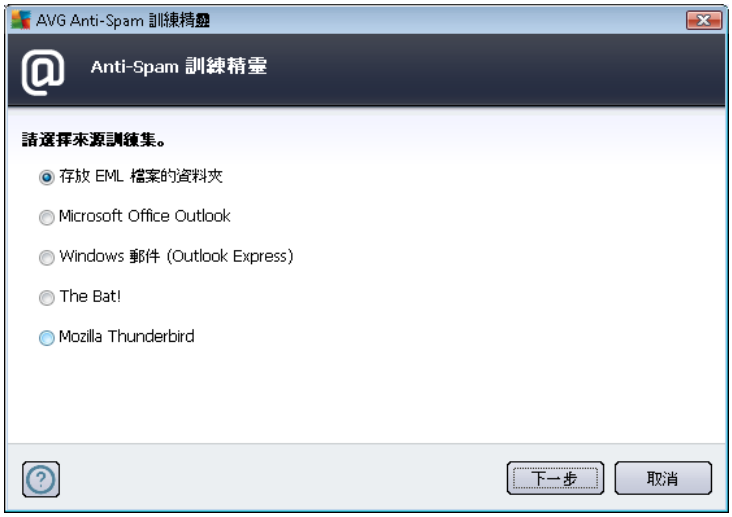
您可以在 ***Anti-Spam 設定***對話方塊中進一步定義應該對偵測到的垃圾電子郵件做何處理：

- ***將郵件移至垃圾郵件資料夾*** *(僅 Microsoft Outlook 外掛程式)* - 勾選此核取方塊可指定每封偵測到的垃圾郵件都應該自動移至您 MS Outlook. 電子郵件用戶端內特定的垃圾郵件資料夾。此時，其他電子郵件用戶端中不支援此功能。
- ***將已傳送電子郵件的收件者新增至白名單*** - 勾選此核取方塊可確認所有已傳送電子郵件的收件者均獲得信任，且可以傳送來自這些電子郵件帳戶的所有電子郵件訊息。
- ***修改標示為「垃圾郵件」的郵件的主旨*** - 如果您希望在電子郵件主旨欄位中以特定的文字或字元標示所有被偵測為垃圾郵件的訊息，請勾選此核取方塊 ;您可以在啟用的文字欄位內輸入所要的文字。
- ***報告錯誤偵測前先詢問*** - 前提是您在安裝程序期間同意參與產品改進計劃。如果您同意，表示您允許向 AVG 報告偵測到的威脅。報告作業會自動進行。然而，您可以標記此核取方塊以確認您想要在向 AVG 報告任何偵測到的垃圾郵件之前先被詢問，以確定訊息確實是被歸類為垃圾郵件。

控制按鈕

訓練 Anti-Spam 按鈕會開啟 Anti-Spam 訓練精靈，下一章節會對此詳加說明。

Anti-Spam 訓練精靈的第一個對話方塊會要求您選取要用於訓練目的之電子郵件訊息的來源。通常，您會要使用誤標為垃圾郵件的電子郵件，或是無法識別的垃圾郵件訊息。



有以下選項可供選擇：

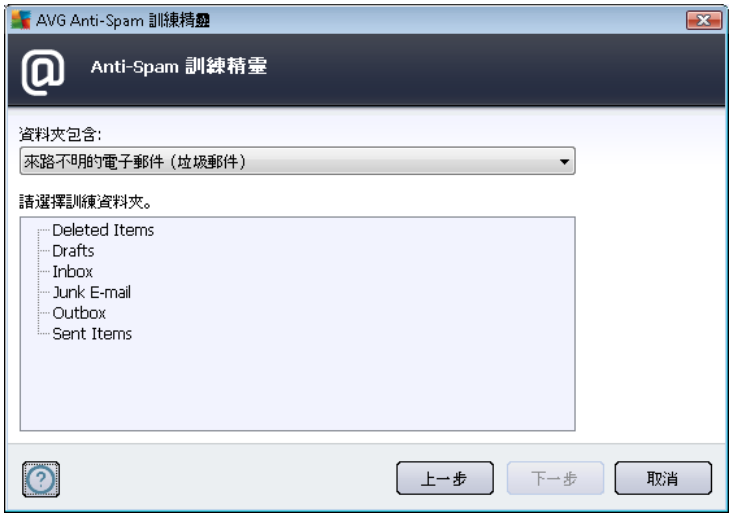
- ***特定的電子郵件用戶端*** - 如果您使用列出的電子郵件用戶端之一 (*MS Outlook*、*Outlook Express*、*The Bat!*)，只需選取相應的選項即可
- ***存放 EML 檔案的資料夾*** - 如果您使用任何其他電子郵件程式，應先將郵件儲存到特定資料夾 (*.eml 格式*)，或確定您知道電子郵件用戶端郵件資料夾的位置。然後選取***存放 EML 檔案的資料夾***，這可讓您在下一步中找到所需的資料夾。

若想讓訓練程序更加快速和方便，提前將資料夾中的電子郵件排序是個不錯的主意，這樣您要用於訓練的資料夾就只包含訓練郵件 (要麼是需要的郵件，要麼是垃圾郵件)。但是，這不是一個必要步驟，因為您稍後可以篩選電子郵件。

選取適當的選項，然後按***下一步***繼續執行精靈。

在此步驟中顯示的對話方塊取決於您之前的選擇。

存放 EML 檔案的資料夾



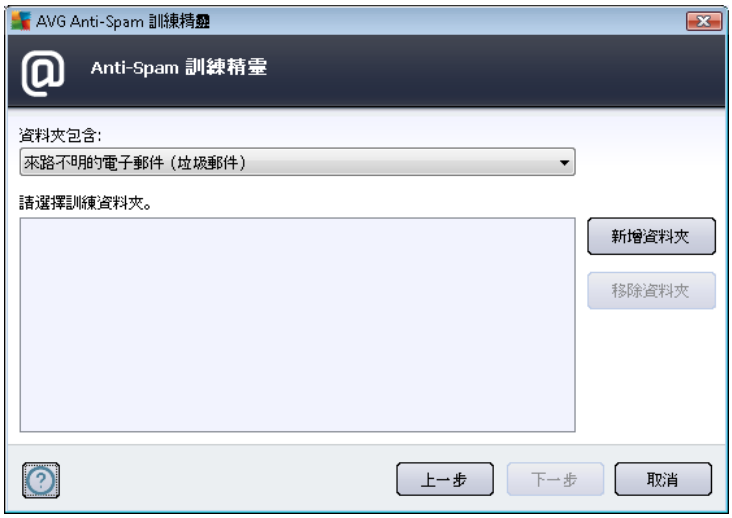
在此對話方塊中，請選取包含您要用於訓練的郵件的資料夾。按一下***新增資料夾***按鈕即可找到存放 .eml 檔案 *(儲存的電子郵件訊息)*的資料夾。然後對話方塊中會顯示該所選資料夾。

在***資料夾包含***下拉式功能表中，設定兩個選項中的一個－即所選資料夾是包含需要的郵件 *(非垃圾郵件)*，還是來路不明的郵件 *(垃圾郵件)*。請注意，您可以在下一步中篩選郵件，因此該資料夾不一定只能包含訓練用的電子郵件。您還可以從清單中移除選取的不需要的資料夾，只要按一下***移除資料夾***按鈕即可。

完成後，按一下***下一步***，前進到郵件篩選選項。

特定電子郵件用戶端

一旦您確認其中一個選項，便會出現一個新的對話方塊。

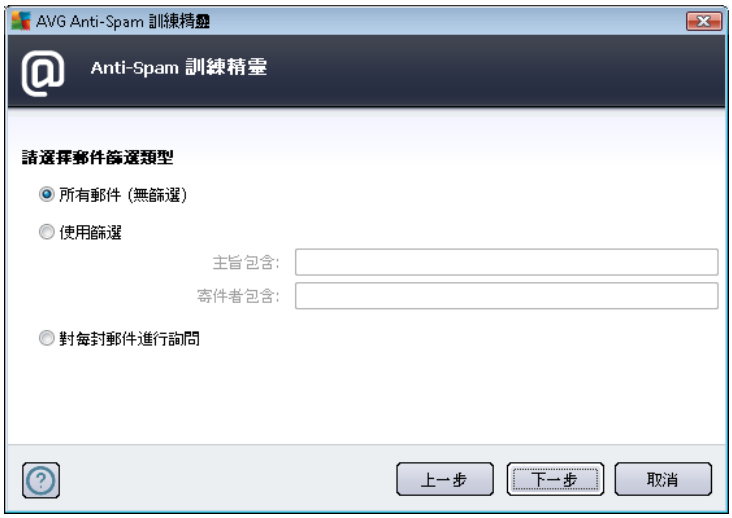


請注意：*如果使用的是 Microsoft Office Outlook，則會提示您先選取 MS Office Outlook 設定*

檔。

在***資料夾包含***下拉式功能表中，設定兩個選項中的一個－即所選資料夾是包含需要的郵件 *(非垃圾郵件)*，還是來路不明的郵件 *(垃圾郵件)*。請注意，您可以在下一步中篩選郵件，因此該資料夾不一定只能包含訓練用的電子郵件。對話方塊的主要區段會顯示所選電子郵件用戶端的巡覽樹狀目錄。請在樹狀目錄中找到所要的資料夾，然後用滑鼠將其亮顯。

完成後，按一下***下一步***，前進到郵件篩選選項。

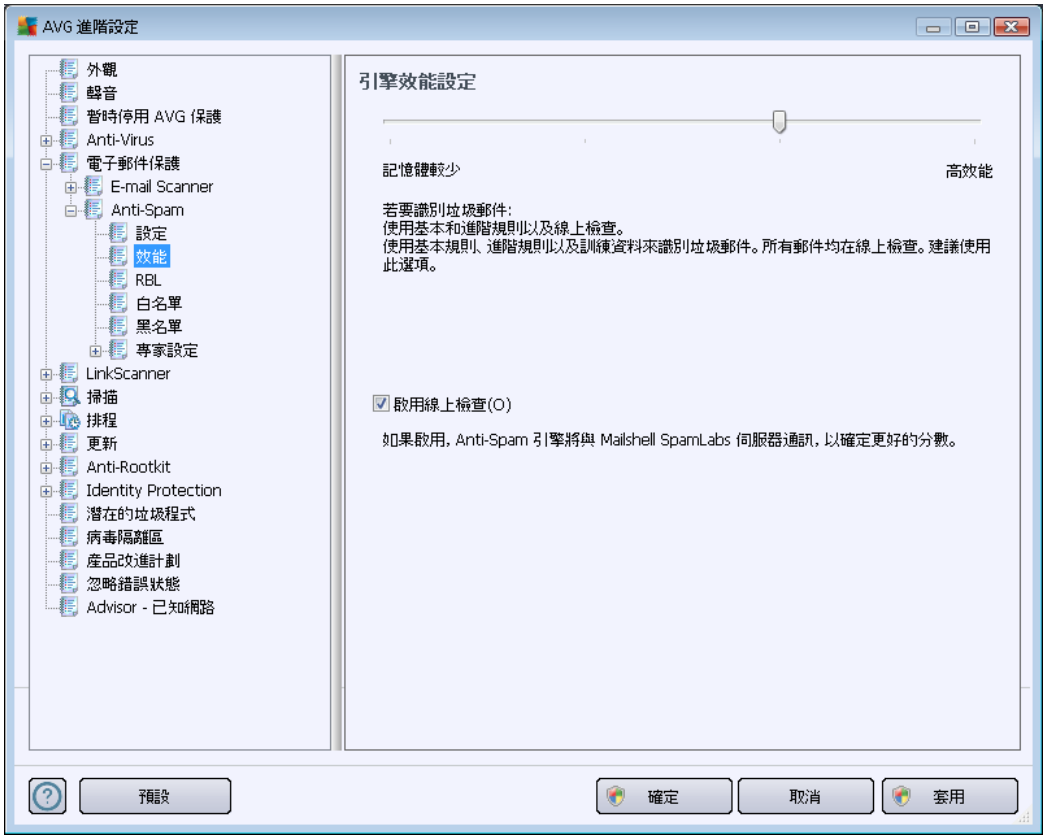


在此對話方塊中，您可以設定篩選電子郵件訊息。

- ***所有郵件 (無篩選)*** - 如果您確定所選資料夾只包含要用於訓練的郵件，請選取***所有郵件 (無篩選)***選項。
- ***使用篩選*** - 如需更為進階的篩選功能，請選取***使用篩選***選項。您可以在電子郵件主旨和/或寄件者欄位填入要搜尋的詞語 *(名稱)*、詞語的一部分或片語。所有與輸入標準完全相符的郵件都將用於訓練，而且不會提供進一步的提示。如果您填寫兩個文字欄位，則也會使用只符合兩個條件之一的地址！
- ***對每封郵件進行詢問*** - 如果您不確定資料夾中包含的郵件，並且想要讓精靈針對每封郵件向您提出詢問 *(這樣您就可以確定是否要將此郵件用於訓練)*，請選取***對每封郵件進行詢問***選項。

選取適當選項後，按一下***下一步***。接著出現的對話方塊僅作提供資訊之用，告知您精靈已就緒，可開始處理郵件。要開始訓練，請再按一下***下一步***按鈕。然後訓練將根據之前所選的選項開始。

引擎效能設定 對話方塊 (*透過左側巡覽的**效能**項目連結*) 提供***Anti-Spam*** 元件效能設定：



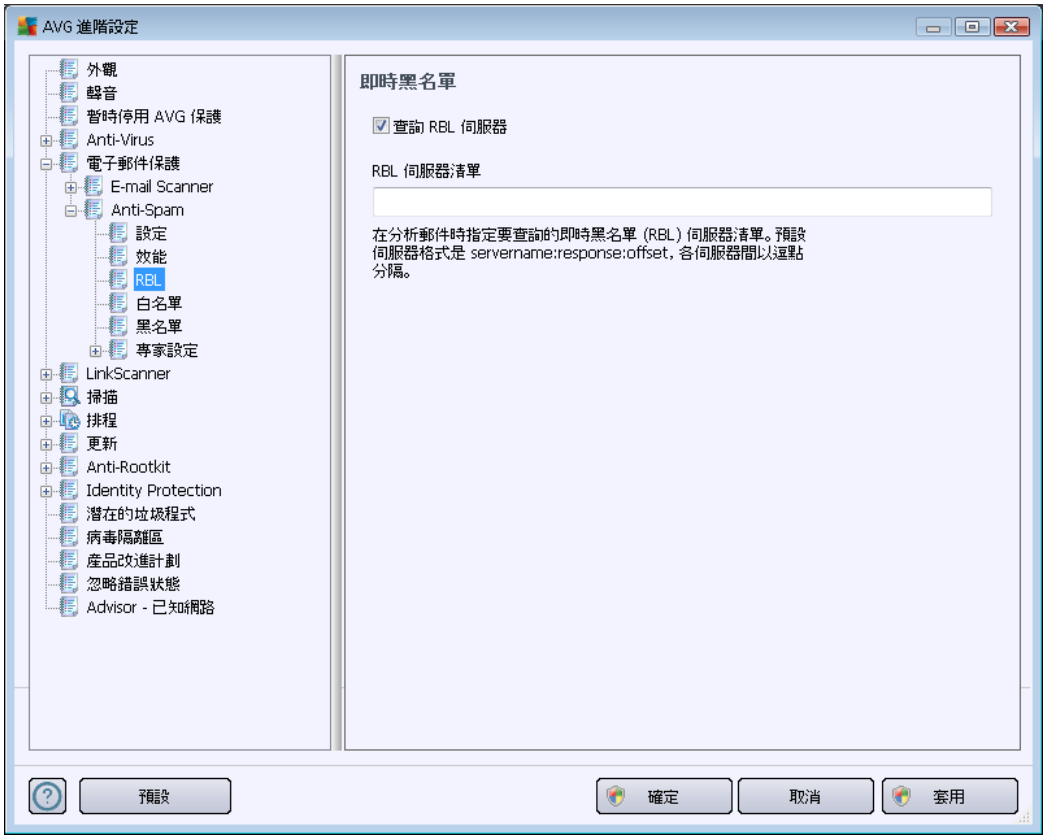
向左或向右移動滑桿，可在***低記憶體/高效能***模式範圍之間變更掃描效能層級。

- ***低記憶體*** - 在識別垃圾郵件的掃描過程中，將不使用任何規則。將只使用訓練資料進行識別。此模式不推薦作為一般用途，除非電腦硬體狀況確實較差。
- ***高效能*** - 此模式將使用大量記憶體。在識別垃圾郵件的掃描過程中，將使用以下功能：規則和垃圾郵件資料庫快取、基本和進階規則、垃圾郵件發信者 IP 位址以及垃圾郵件發信者資料庫。

預設情況下，會開啟***啟用線上檢查***項目。透過與 Mailshell 伺服器通訊，它可產生更為準確的垃圾郵件偵測，例如將掃描的資料與 Mailshell 線上資料庫進行比較。

通常建議保留預設設定，僅在確實有必要時才進行變更。對此組態的任何變更只能由經驗豐富的使用者來執行！

RBL 項目會開啟一個稱為***即時黑名單***的編輯對話方塊，您可以在這裡開啟/關閉***查詢 RBL 伺服器***功能。

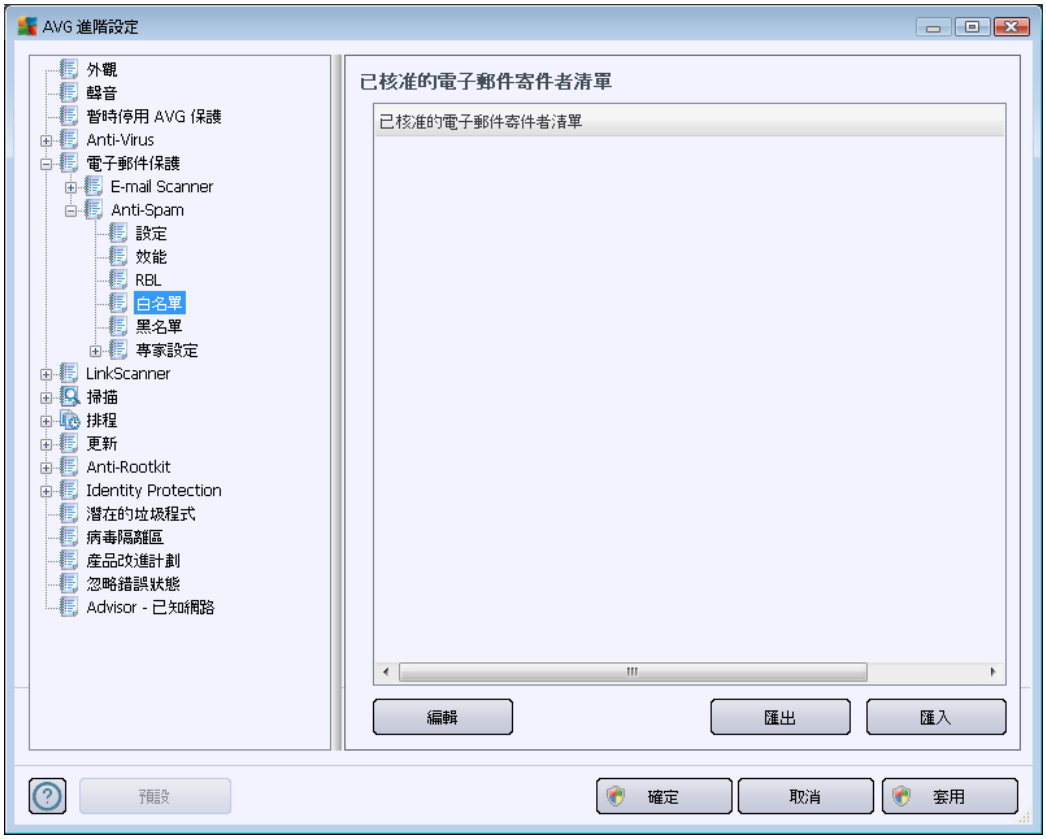


RBL (*即時黑名單*) 伺服器是帶有強大的已知垃圾郵件寄件者資料庫的 DNS 伺服器。開啟該功能時，將根據 RBL 伺服器資料庫驗證所有電子郵件訊息，若發現與資料庫中的任何項目相同，則會將其標示為垃圾郵件。RBL 伺服器資料庫包含最新垃圾郵件指紋，因此可提供最佳和最為準確的垃圾郵件偵測。對於收到大量 Anti-Spam 引擎一般無法偵測出的垃圾郵件的使用者而言，此功能非常有用。

RBL 伺服器清單可讓您定義特定 RBL 伺服器位置 (*請注意，啟用此功能在某些系統和組態上，可能會減緩電子郵件接收程序的速度，因為每封郵件都必須經過 RBL 伺服器資料庫驗證*)。

不會將個人資料傳送至伺服器！

白名單項目會開啟一個稱為***已核准的電子郵件寄件者清單***的對話方塊，其中包含已核准的寄件者電子郵件地址和網域名稱的全域清單，來自此類地址或網域的郵件永遠不會標示為垃圾郵件。



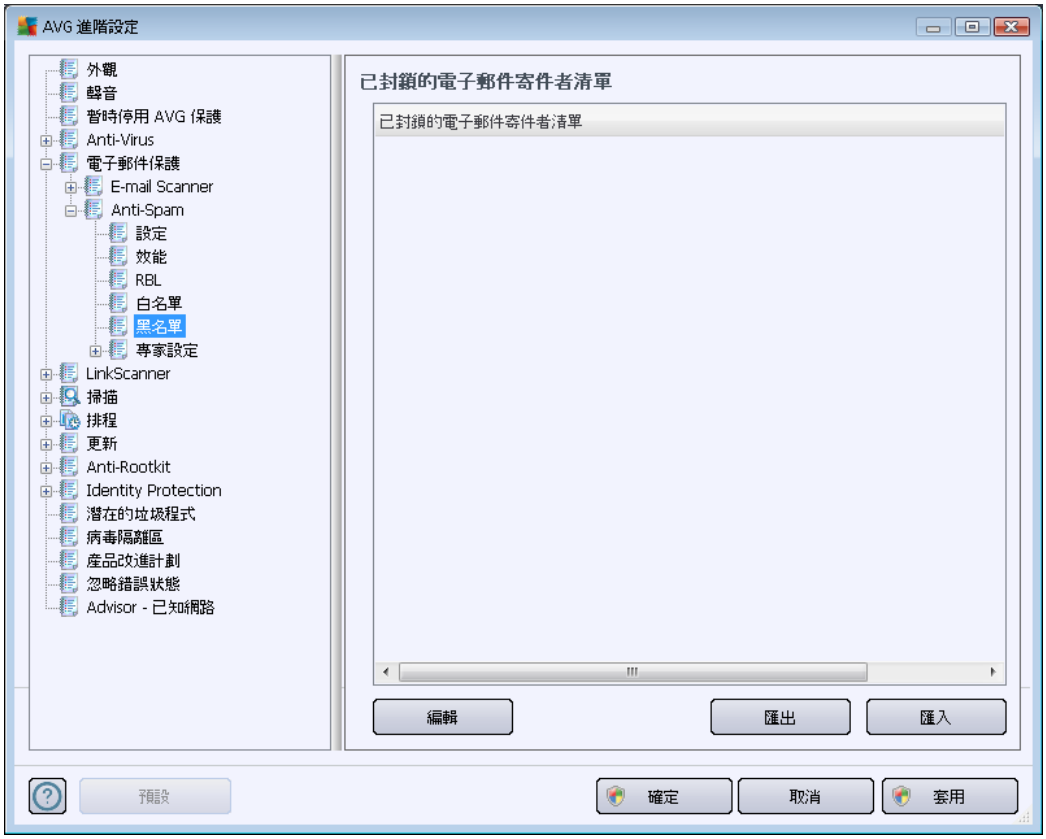
在編輯介面中，您可以制作一份確定永遠不會傳送來路不明的郵件 (垃圾郵件) 的寄件者清單。您也可以制作一份完整網路名稱的清單 (*例如 avg.com*)，以包含您知道不會產生垃圾郵件的網域名稱。準備好這類寄件者和/或網域名稱清單之後，您可以使用下列任一方法將其輸入清單 :直接輸入各個電子郵件地址或一次性匯入整份地址清單。

控制按鈕

可用的控制按鈕如下：

- ***編輯*** - 按下此按鈕會開啟一個對話方塊讓您手動輸入地址清單 (*您也可以使用複製和貼上*)。每一行插入一個項目 (*寄件者*、*網域名稱*)。
- ***匯出*** - 如果您基於某種原因決定匯出記錄，您可以按此按鈕執行。所有記錄都將儲存成純文字檔。
- ***匯入*** - 如果您已經準備好電子郵件地址/網域名稱的文字檔案，只需按下此按鈕即可直接匯入檔案。檔案內容必須在每行僅包含一個項目 (*位址*、*網域名稱*)。

黑名單項目會開啟一個對話方塊，內含封鎖的寄件者電子郵件地址與網域名稱的全域清單，來自此清單中寄件者的訊息將始終會標示為垃圾郵件。



您可以在編輯介面中製作一份預期會寄送來路不明郵件 *(垃圾郵件)*的寄件者清單。您也可以制作一份完整網域名稱的清單 (*例如 spammingcompany.com*)，以包含預期會從其收到或者已經從其收到垃圾郵件的網域名稱。來自其中列出的地址/網域的所有電子郵件都會被識別成垃圾郵件。準備好這類寄件者和/或網域名稱清單之後，您可以使用下列任一方法將其輸入清單 :直接輸入各個電子郵件地址或一次性匯入整份地址清單。

控制按鈕

可用的控制按鈕如下：

- ***編輯*** - 按下此按鈕會開啟一個對話方塊讓您手動輸入地址清單 (*您也可以使用複製和貼上*)。每一行插入一個項目 (*寄件者*、*網域名稱*)。
- ***匯出*** - 如果您基於某種原因決定匯出記錄，您可以按此按鈕執行。所有記錄都將儲存成純文字檔。
- ***匯入*** - 如果您已經準備好電子郵件地址/網域名稱的文字檔案，只需按下此按鈕即可直接匯入該檔案。

進階設定分支包含許多適用於 Anti-Spam 元件的設定選項。這些設定專門適用於經驗豐富的使用者，這通常是指那些需要詳細設定反垃圾郵件保護功能，以便為電子郵件伺服器提供最佳保護的網路管理員。基於這個原因，不針對個別對話方塊額外提供說明；不過，使用者介面中提供有各個選項的簡短說明。

除非您對 Spamcatcher (MailShell Inc.) 的進階設定非常熟悉，否則強烈建議您不要變更任何設定。任何不適當的變更都可能導致電腦效能降低或元件功能錯誤。

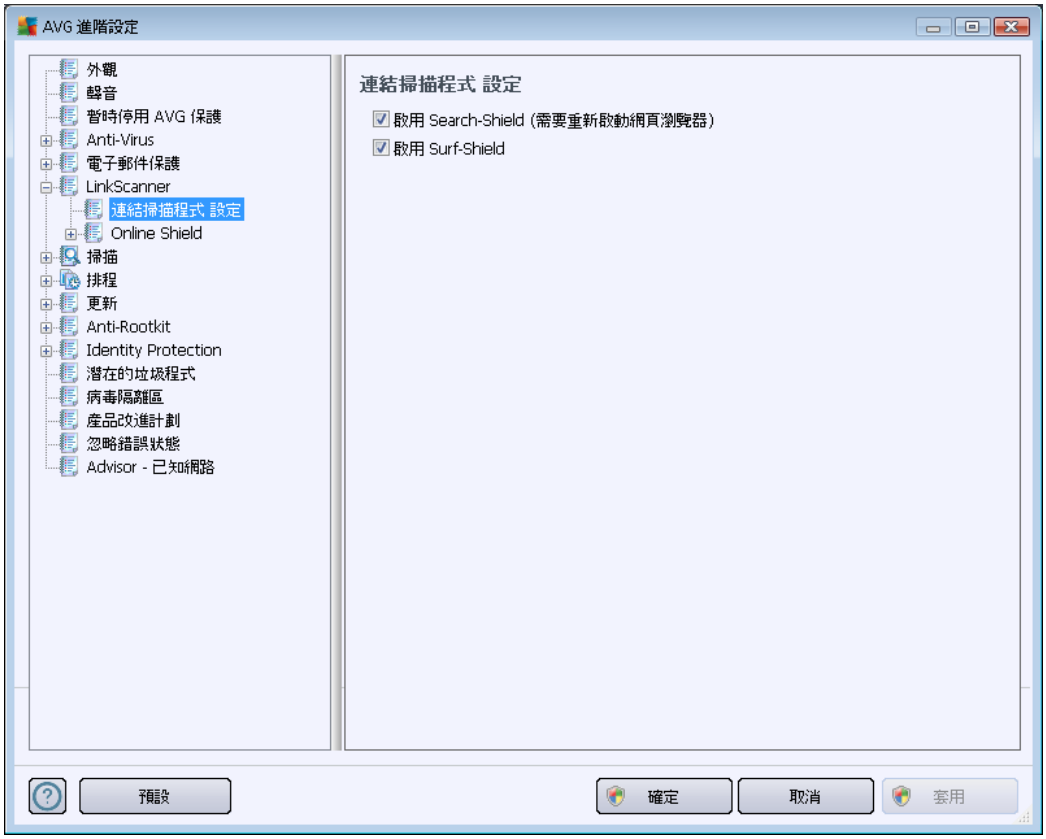
如果您還是認為有必要變更進階層級的 Anti-Spam 組態，請遵循使用者介面中提供的指示。在各個對話方塊中，您通常會看到一個可以編輯的單一特定功能 - 對話方塊本身通常會包含該功能的說明：

- ***擷取*** - 指紋、網域名聲、LegitRepute
- ***訓練*** - 最大輸入字數、自動訓練閾值、權數
- ***篩選*** - 語言清單、國家 (或地區) 清單、已核准的 IP、已阻止的 IP、已阻止的國家 (或地區)、已阻止的字元集、冒名的寄件者
- ***RBL*** - RBL 伺服器、多個結果、閾值、逾時、最大 IP 數
- ***網際網路連線*** - 逾時、代理伺服器、代理伺服器驗證

10.6. LinkScanner

10.6.1. 連結掃描程式設定

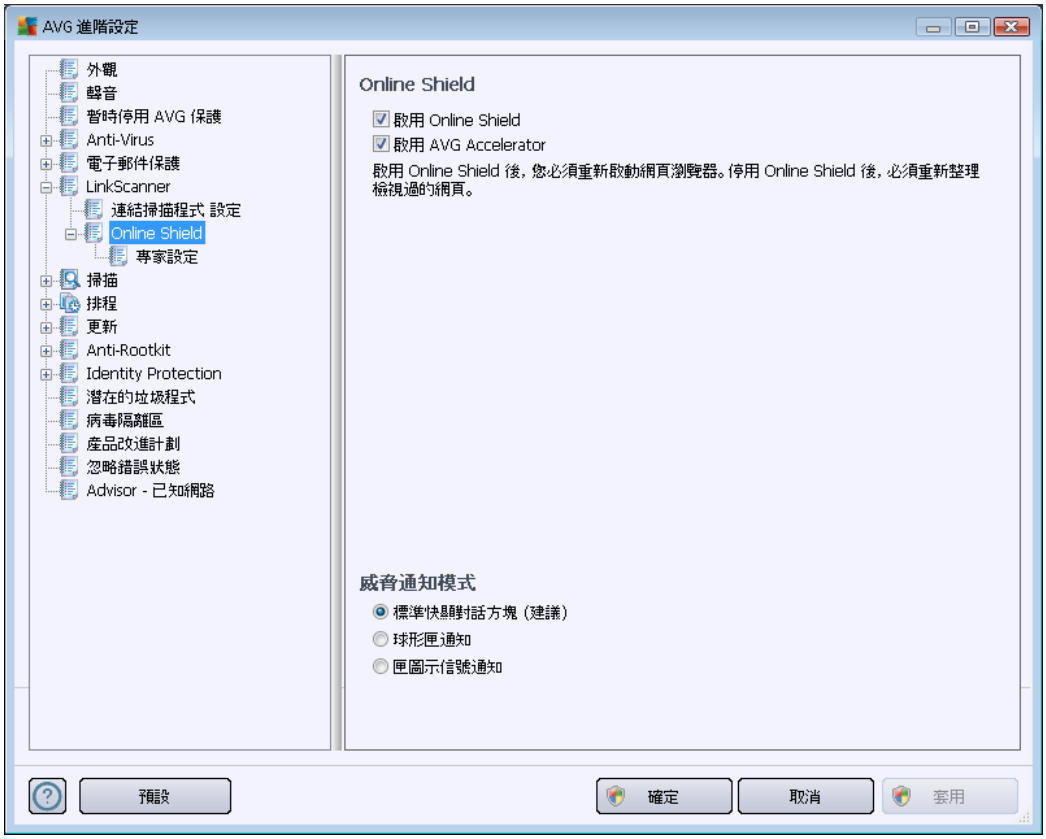
***LinkScanner* 設定**對話方塊可讓您開啟/關閉 LinkScanner 元件的基本功能：



- ***啟用 Search-Shield*** - (*預設情況下開啟*)：在透過 Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 執行的搜尋上提供忠告圖示：事先檢查搜尋引擎傳回的網站內容。

- ***啟用 Surf-Shield*** - (*預設情況下為開啟*)：在存取惡意探索站點時，提供主動 (*即時*) 保護。當使用者透過網頁瀏覽器 (*或任何其他使用 HTTP 的應用程式*) 存取已知惡意站點時，其連線及其惡意探索內容都將被封鎖。

10.6.2. Online Shield

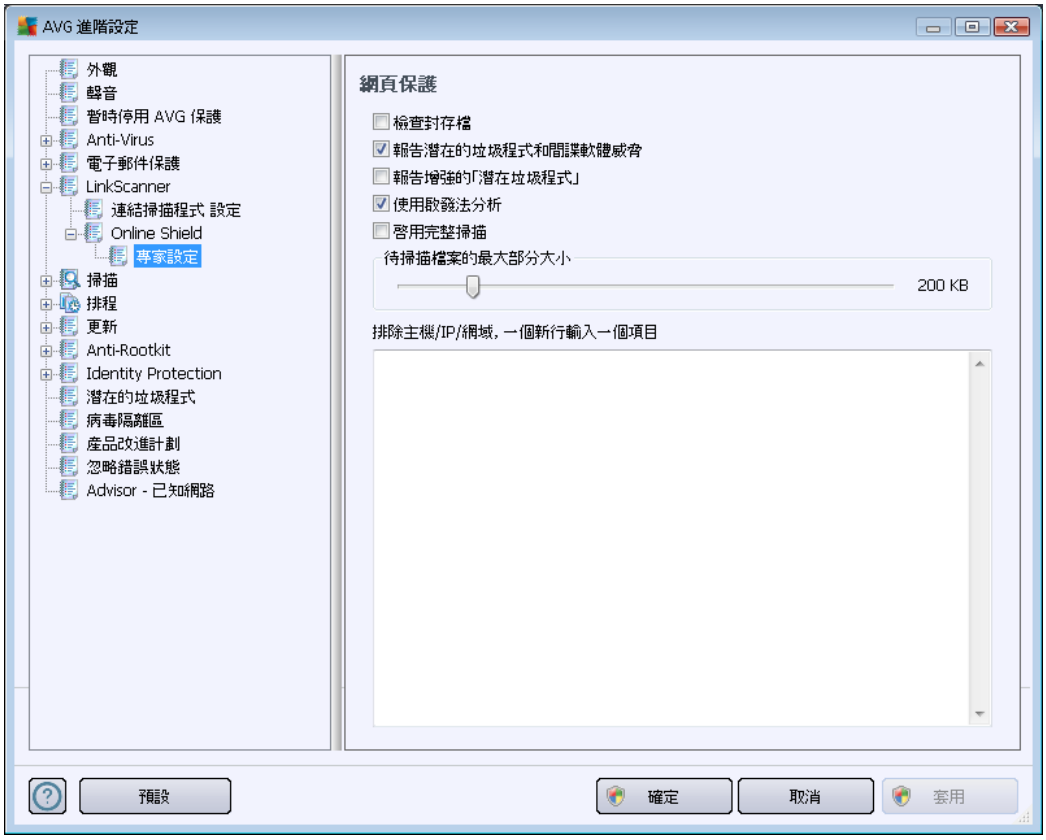


Online Shield 對話方快提供以下選項：

- ***啟用 Online Shield*** *(預設為開啟)* - 啟動/停用整個 ***Online Shield*** 服務。如需 ***Online Shield*** 進一步的進階設定，請繼續到下一個稱為網頁保護的對話方塊。
- ***啟用 AVG 加速器*** *(預設為開啟)* - 啟動/停用 ***AVG 加速器***服務，使線上視訊播放更加順暢，並且更方便進行其他下載。

威脅通知模式

在對話方塊的底端，選取您希望在可能偵測到威脅時獲得通知的方式 :透過標準快顯對話方塊、透過球形匣通知，還是透過系統匣圖示資訊。



在***網頁保護***對話方塊中，您可以編輯元件中有關網站內容掃描的組態。編輯介面可讓您設定以下基本選項：

- ***啟用網頁保護*** - 此選項確認 ***Online Shield*** 應該執行 www 網頁內容的掃描作業。如果啟用此選項 (*預設*)，則還可以開啟/關閉以下項目：
    - ***檢查封存檔*** - (*預設為開啟*)：掃描要顯示的 www 網頁中可能包含的封存檔的內容。
    - ***報告潛在的垃圾程式和間諜軟體威脅*** - (*預設為開啟*)：核取此選項可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
    - ***報告增強的潛在垃圾程式*** - (*預設為關閉*)：標示此選項以偵測延伸的間諜軟體：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
    - ***使用啟發法分析*** - (*預設為開啟*)：使用啟發法分析 方法 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 掃描要顯示的網頁內容。
    - ***啟用完整掃描*** (*預設為關閉*) - 在特殊情況下 (*懷疑您的電腦受到感染*)，您可

以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***待掃描的檔案的最大部分大小*** - 如果包含的檔案列示在顯示的頁面中，您甚至還可以在下載到電腦上之前掃描其內容。但掃描較大的檔案需花費一定時間，網頁下載可能會明顯變慢。您可以使用滑桿來指定仍使用 ***Online Shield*** 掃描之檔案的最大大小。即使下載的檔案超過指定大小，致使無法使用 Online Shield 進行掃描，您仍然會受到保護 :如果該檔案受感染，***Resident Shield*** 會立即偵測到。
- ***排除主機/IP/網域*** - 您可以將無需 *Online Shield* 掃描的伺服器 (***主機、IP 位址、含有遮罩的 IP 位址或 URL***) *或網域的完整名稱輸入到該文字欄位*。因此，請只排除您能完全確定絕對不會提供危險網站內容的主機。

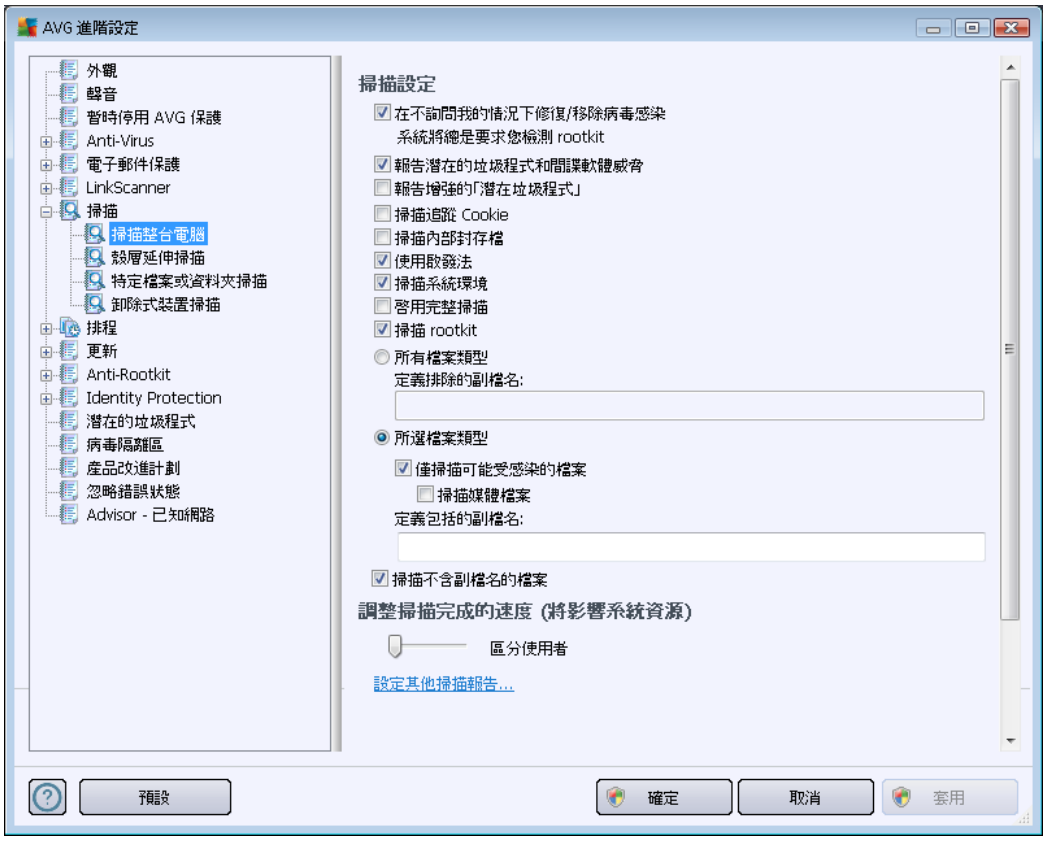
10.7. 掃描

進階掃描設定為四個類別，這些類別指的是軟體廠商定義的特定掃描類型：

- ***掃描整台電腦*** - 標準預先定義的整台電腦掃描
- ***殼層延伸掃描*** - 直接從 Windows 檔案總管環境中執行之選定物件的特定掃描
- ***掃描特定檔案或資料夾*** - 所選電腦區域的標準預先定義掃描
- ***卸除式裝置掃描*** - 與電腦連接的卸除式裝置的特定掃描

10.7.1. 掃描整台電腦

掃描整台電腦選項可供您編輯軟體廠商預先定義的掃描類型之一，即掃描整台電腦的參數：



掃描設定

掃描設定區段提供可以選擇性開啟/關閉的掃描參數清單：

- ***在不詢問我的情況下修復/移除病毒感染*** (預設為開啟) :如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至病毒隔離區。
- ***報告潛在的垃圾程式和間諜軟體威脅*** (*預設為開啟*) - 核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。
- ***報告增強的潛在垃圾程式*** (*預設為關閉*) - 標示此選項可偵測延伸的間諜軟體套件 :這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- ***掃描追蹤 Cookie*** (*預設為關閉*) - Anti-Spyware 元件的此一參數定義在掃描期間應偵測 cookie；(*HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容*)

- ***掃描內部封存檔*** (*預設為關閉*) - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在封存檔內，如 ZIP、RAR...

- ***使用啟發法*** (*預設為開啟*) - 啟發法分析 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 將成為掃描過程中用於偵測病毒的方法之一；

- ***掃描系統環境*** (*預設為開啟*) - 掃描時還會檢查您電腦的系統區域。

- ***啟用完整掃描*** (*預設為關閉*) - 在特定情況下 (*懷疑您的電腦受到感染*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***掃描 rootkits*** (預設為開啟) - Anti-Rootkit 掃描可搜尋您電腦中可能的 rootkits，即可覆蓋您電腦中惡意軟體活動的程式和技術。偵測到 rootkit 不一定表示您的電腦已受到感染。在某些情況下，特定驅動程式或正常應用程式的某些部分都可能被誤偵測為 rootkit。

接下來，您應該決定是否要掃描

- ***所有檔案類型*** - 您可以透過一份逗號分隔 (*儲存之後，逗號會變成分號*) 檔案格式的清單來定義掃描例外，使這些檔案不會被掃描；

- ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔*)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

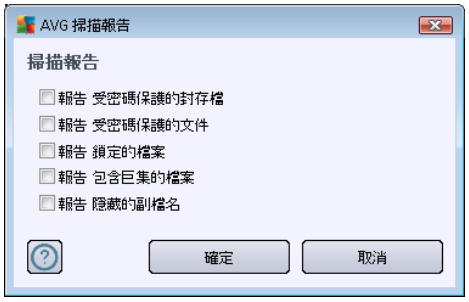
- 或者，您也可以決定***掃描不含副檔名的檔案*** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

調整完成掃描的速度

您可以在***調整完成掃描的速度***區段內，依據系統的資源使用量來進一步指定需要的掃描速度。預設情況下，該選項值會設為*區分使用者*層級的自動資源使用量。如果您要加快掃描速度，此掃描執行所耗用的時間將會減少，同時系統的資源使用量也將顯著增大，並減緩電腦上其他活動的速度 (*可在開啟電腦，但無人作業時，使用此選項*)。另一方面，您可以透過延長掃描時間來降低系統資源使用量。

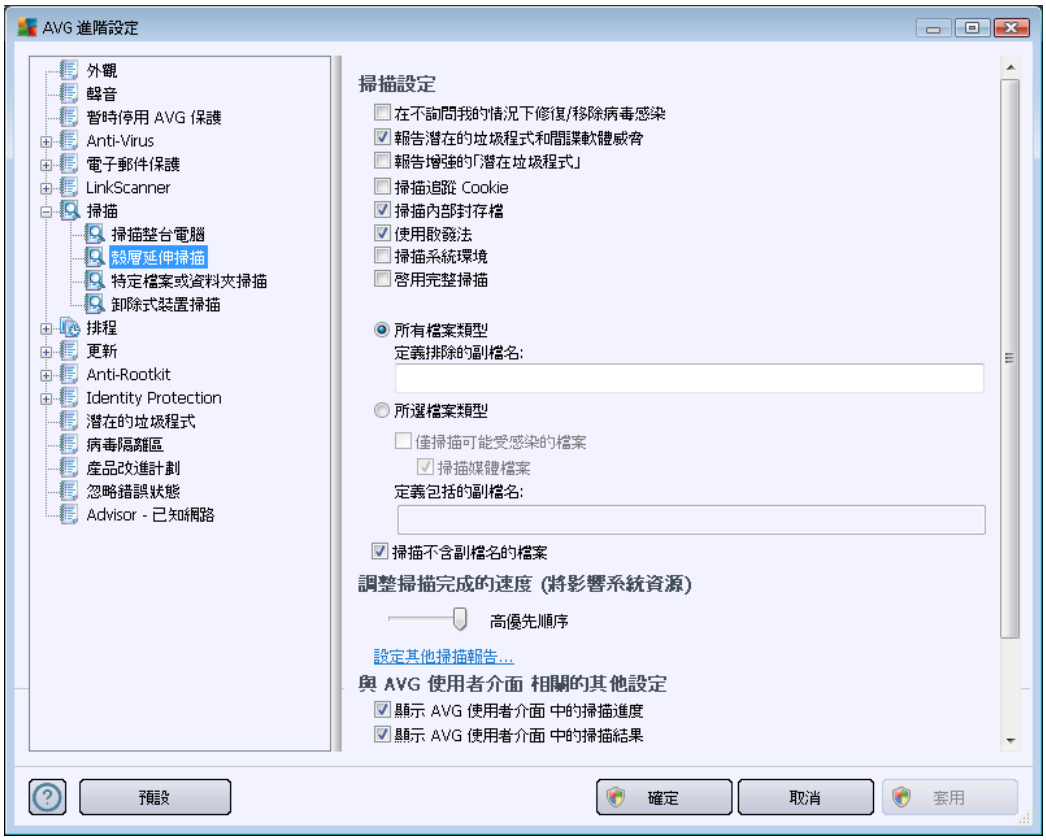
設定其他掃描報告...

按下***設定其他掃描報告...*** 連結，可以開啟名為***掃描報告***的獨立對話方塊視窗，您可在此勾選數個項目，以定義應該報告哪些掃描結果：



10.7.2. 殼層延伸掃描

與之前的掃描整台電腦項目相似，此項目稱為***殼層延伸掃描***，也提供數個編輯軟體廠商預先定義的掃描的選項。這次的組態涉及到掃描從 Windows 檔案總管環境直接啟動的特定物件 (*殼層延伸*)，請參閱掃描 Windows 檔案總管一章：



參數清單與掃描整台電腦所用的那些參數完全相同。但是預設設定並不相同 (*例如，掃描整台電腦在預設情況下並不會檢查封存檔，但是會掃描系統環境，而殼層延伸掃描則剛好相反*)。

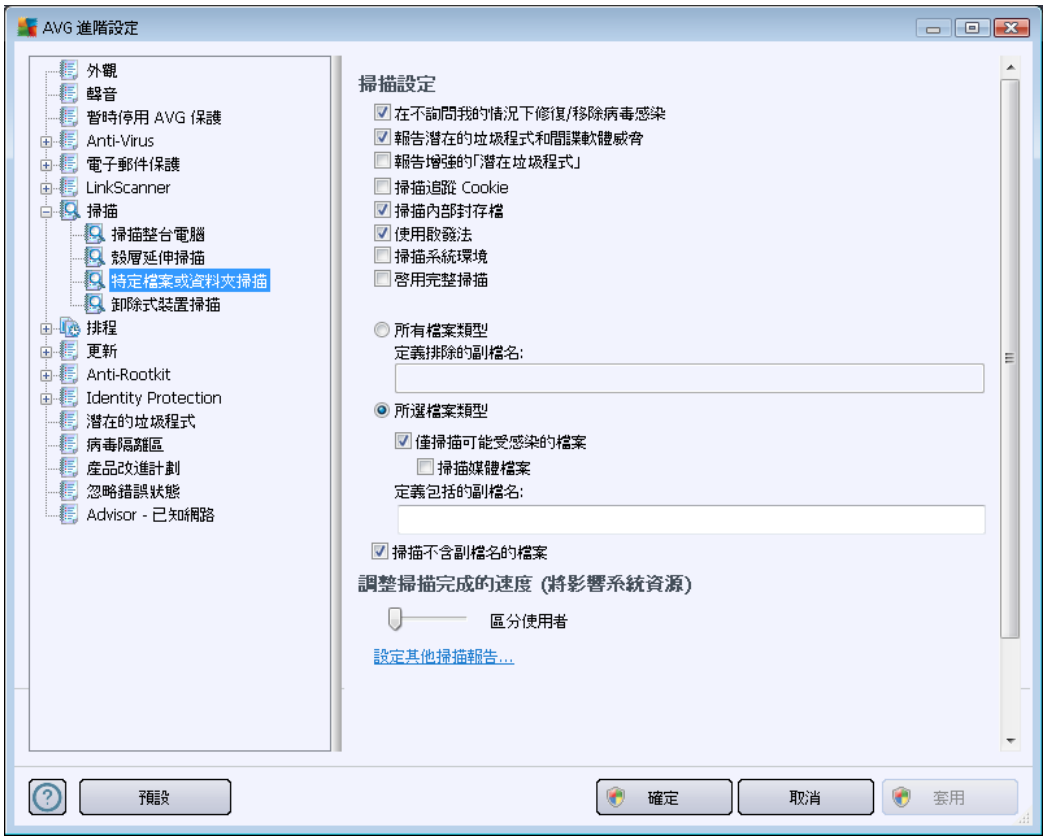
注意：*有關特定參數的敘述，請查閱 AVG 進階設定/掃描/掃描整台電腦一章。*

與掃描整台電腦對話方塊相比，***殼層延伸掃描***對話方塊也包含名為***與 AVG 使用者介面相關的其他設定***區段，您可以在這裡指定是否要從 AVG 使用者介面存取掃描進度和掃描

結果。另外，您可以定義只在掃描期間偵測到感染檔案時才顯示掃描結果。

10.7.3. 特定檔案或資料夾掃描

掃描特定檔案或資料夾 的編輯介面和完整電腦掃描編輯對話方塊相同。所有組態選項都相同，但是掃描整台電腦的預設設定較為嚴格：

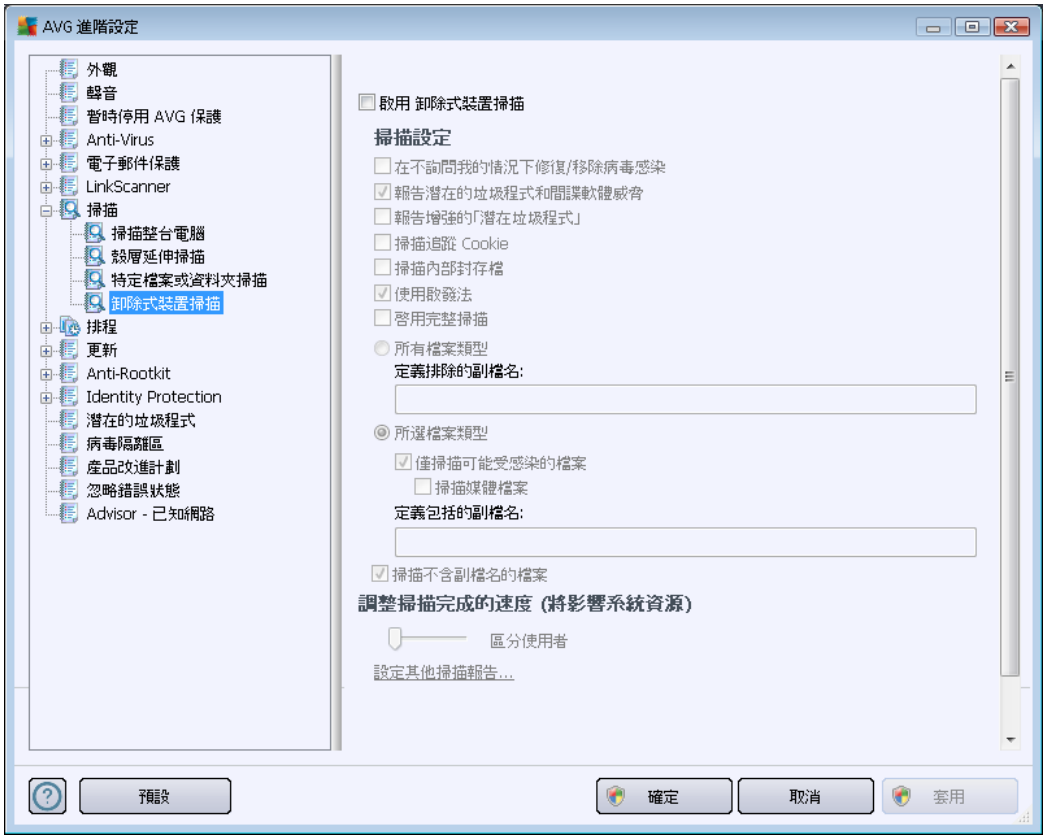


在此組態對話方塊中設定的所有參數，都只會套用到為掃描特定檔案或資料夾選取的區域！

注意：*有關特定參數的描述，請查閱 AVG 進階設定／掃描／完整電腦掃描一章。*

10.7.4. 卸除式裝置掃描

卸除式裝置掃描的編輯介面與完整電腦掃描 編輯對話方塊也十分相似：



卸除式裝置掃描將在您將任何卸除式裝置連接至電腦後自動啟動。預設情況下，此掃描為關閉狀態。但是，掃描卸除式裝置中是否具有潛在威脅非常重要，因為這些裝置是感染的主要來源之一。若要讓該掃描準備就緒並在必要時自動啟動，請勾選***啟用卸除式裝置掃描***選項。

注意：*有關特定參數的說明，請查閱 AVG 進階設定／掃描／完整電腦掃描一章。*

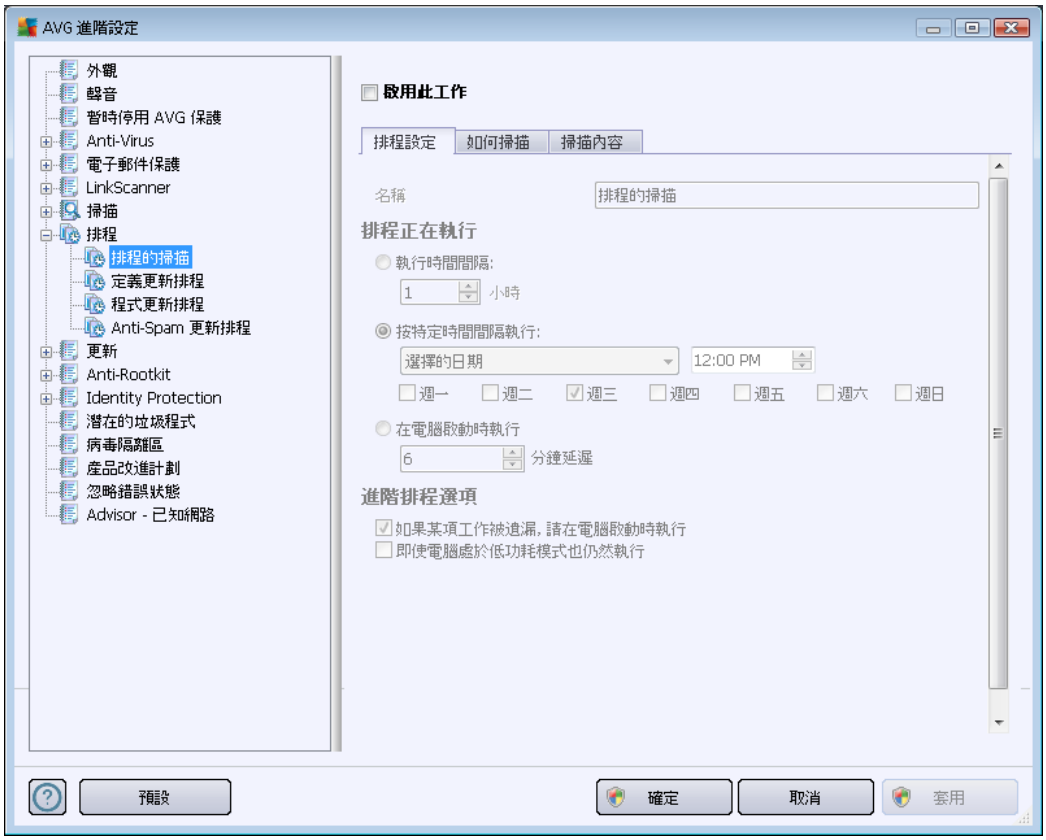
10.8. 排程

在***排程***部分，您可以編輯以下項目的預設設定：

- 排程掃描
- 定義更新排程
- 程式更新排程
- Anti-Spam 更新排程

10.8.1. 排程掃描

排程掃描的參數可在三個標籤上進行編輯 (*或設定新排程*)。您可以在各個標籤中，先核取/取消核取 ***啟用此工作***項目，即可暫時停用排程的測試，然後有需要時再開啟它：



接下來，在稱為***名稱***的文字欄位中 (*已針對所有預設排程停用*) 顯示的是由程式廠商指派給此排程的名稱。對於新增的排程 (*在左方巡覽樹狀目錄中以滑鼠右鍵按一下**排程掃描**項目，即可新增排程*)，您可以指定自己的名稱，若要指定名稱，會開啟文字欄位供您編輯。嘗試始終為掃描使用簡短、恰當的描述性名稱，方便日後與其他掃描區別開來。

例如：*將掃描命名為「新掃描」或「我的掃描」並不合適，因為這些名稱並未指明掃描真正檢查的內容。反過來說，如「系統區域掃描」則是恰當的描述性名稱示例。此外，也沒有必要在掃描的名稱中指明是掃描整台電腦還是只掃描所選檔案或資料夾 - 您的掃描始終是特定版本的掃描所選檔案或資料夾。*

在此對話方塊中，您可以進一步定義掃描的以下參數：

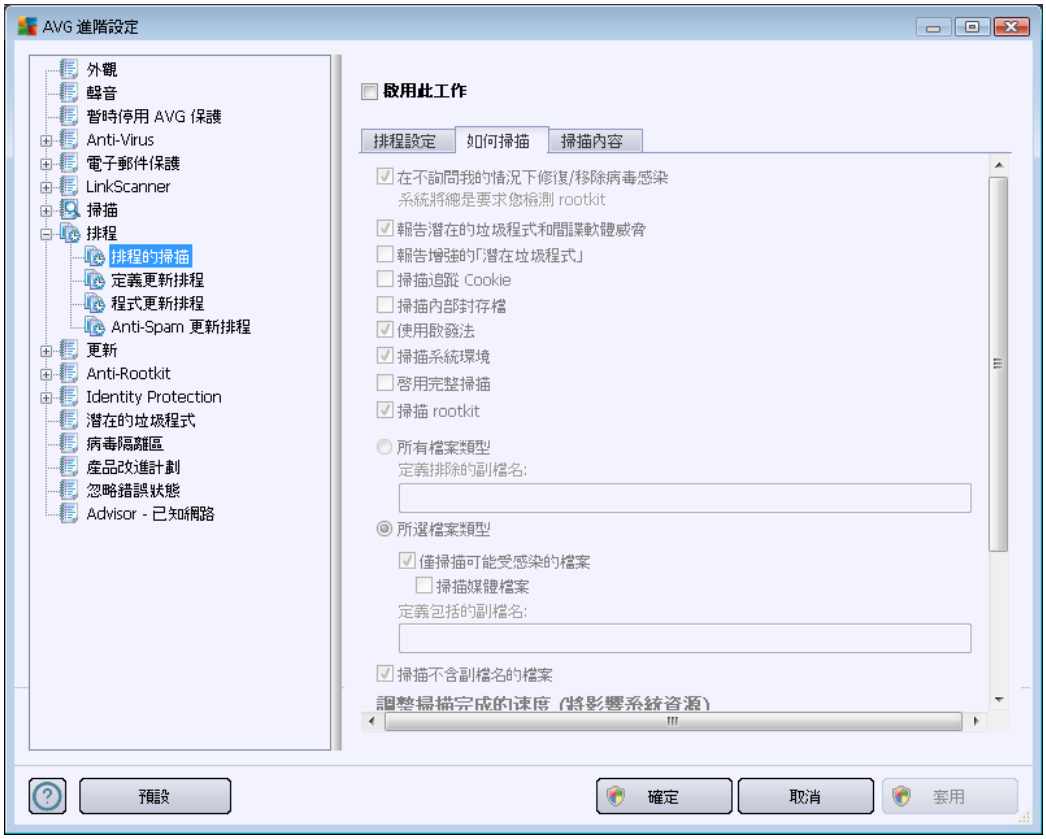
排程執行

在這裡，您可以為新排程的掃描啟動指定時間間隔。時間安排有以下幾種定義方式：定義一段時間後再次啟動掃描 (***執行時間間隔***)，或定義確切的日期和時間 (***按特定時間間隔執行***)，或者可能透過定義一個關聯掃描啟動的事件 (***在電腦啟動時執行***)。

進階排程選項

此區段允許您定義若電腦處於低功耗模式或完全關閉模式時，應該在何種條件下啟動/不啟動掃描。排程的掃描在您指定的時間啟動後，軟體將透過在 AVG 系統匣圖示 中開啟一個快顯視窗來通知您。

接著，會顯示新的 AVG 系統匣圖示 (*全彩並帶有一個閃燈*)，告知您排程的掃描正在執行中。在執行中的掃描 AVG 圖示上按一下滑鼠右鍵，可開啟內容功能表，您可在此處決定暫停甚或停止執行中的掃描，也可以變更目前正在執行的掃描的優先順序。



在***如何掃描***標籤上，您將看到一份可選擇開啟/關閉的掃描參數清單。預設情況下，大多數參數都已開啟，並將在掃描期間套用其功能。***除非您有充分的理由需要變更這些設定，否則建議您保留預先定義的組態***：

- ***在不詢問我的情況下修復/移除病毒感染*** *(預設為開啟)* 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至病毒隔離區。

- ***報告潛在的垃圾程式和間諜軟體威脅*** *(預設為開啟)*：核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。

- ***報告增強的潛在垃圾程式*** (*預設為關閉*)：標示此選項可偵測延伸的間諜軟體套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- ***掃描追蹤 Cookie*** (*預設為關閉*)：Anti-Spyware 元件的此一參數定義在掃描期間應偵測 cookie；(*HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容*)

- ***掃描內部封存檔*** (*預設為關閉*)：此參數定義掃描應檢查所有檔案，即使這些檔案已封裝在封存檔內，如 ZIP、RAR...

- ***使用啟發法*** (*預設為開啟*)：啟發法分析 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 將成為掃描過程中用於偵測病毒的方法之一；

- ***掃描系統環境*** (*預設為開啟*)：掃描時還會檢查您電腦的系統區域；

- ***啟用完整掃描*** (*預設為關閉*)：在特定情況下 (*懷疑您的電腦受到感染*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***掃描 rootkits*** *(預設為開啟)*：Anti-Rootkit 掃描可搜尋您電腦中可能的 rootkits，即可覆蓋您電腦中惡意軟體活動的程式和技術。偵測到 rootkit 不一定表示您的電腦已受到感染。在某些情況下，特定驅動程式或正常應用程式的某些部分都可能被誤偵測為 rootkit。

接下來，您應該決定是否要掃描

- ***所有檔案類型*** - 您可以透過一份不應掃描檔案清單 (以逗號分隔副檔名；*儲存之後，逗號會變成分號*) 來定義掃描例外；

- ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔*)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

- 或者，您也可以決定***掃描不含副檔名的檔案*** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

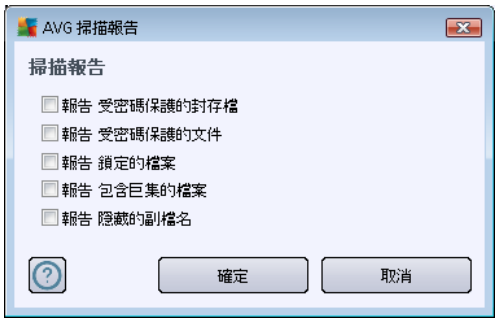
調整完成掃描的速度

您可以在***調整完成描的速度***區段內，依據系統的資源使用量來進一步指定所要的掃描速度。預設情況下，該選項值設為*區分使用者*層級的自動資源使用量。如果您要加快掃描速

度，此掃描的執行所耗用時間將會減少，同時系統的資源使用量也將顯著增大，並減緩電腦上的其他活動的速度 (*可在開啟電腦，但無人作業時，使用此選項*)。另一方面，您可以透過延長掃描時間來降低系統資源使用量。

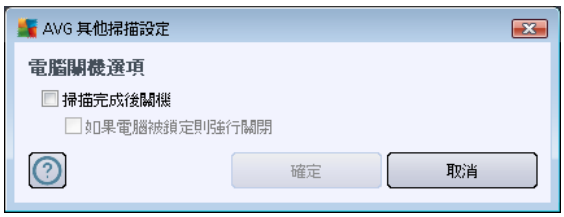
設定其他掃描報告

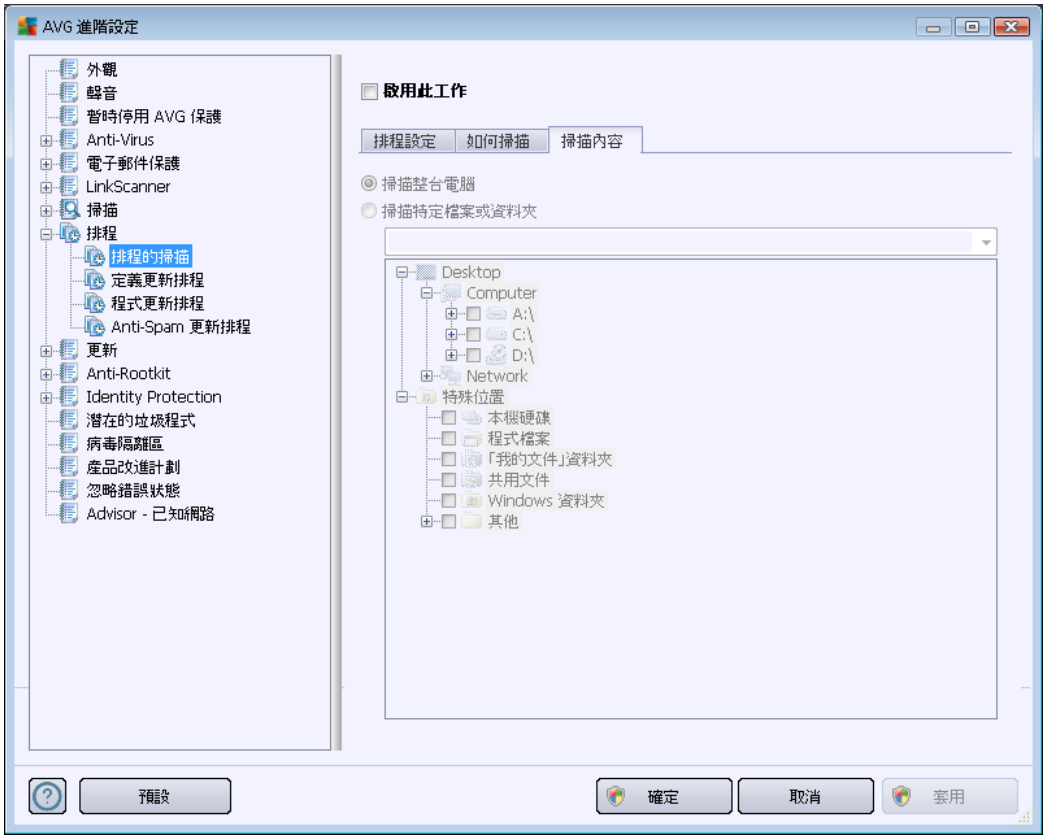
按下***設定其他掃描報告...*** 連結，可以開啟名為***掃描報告***的獨立對話方塊視窗，您可在此勾選數個項目，以定義應該報告哪些掃描結果：



其他掃描設定

按一下***其他掃描設定...*** 即可開啟新的***電腦關機選項***對話方塊，您可在此決定掃描程序執行完成後，電腦是否應自動關機。確認此選項後 (***掃描完成後關機***)，將啟動一個新選項，設定電腦即使在鎖定狀態下也能關機 (***強行關閉鎖定的電腦***)。





在***掃描內容***標籤上，您可以定義是要排程掃描整台電腦，還是掃描特定檔案或資料夾。如果您選取掃描特定檔案或資料夾，則會啟動顯示在此對話方塊底端的樹狀結構，讓您指定要掃描的資料夾。

10.8.2. 定義更新排程

真的有必要時，您可以取消核取***啟用此工作***項目，暫時停用排定的定義更新，稍後再開啟它：

您可以在此對話方塊中設定一些詳細的定義更新排程參數。在稱為***名稱***的文字欄位中 (*已針對所有預設排程停用*)，顯示的是由程式廠商指派給此排程的名稱。

排程執行

在此區段中為新排程的病毒庫更新啟動指定時間間隔。時間安排可定義為每隔一段時間重複啟動更新 (***執行時間間隔***)，或定義確切的日期和時間 (***按特定時間間隔執行 ...***)。

進階排程選項

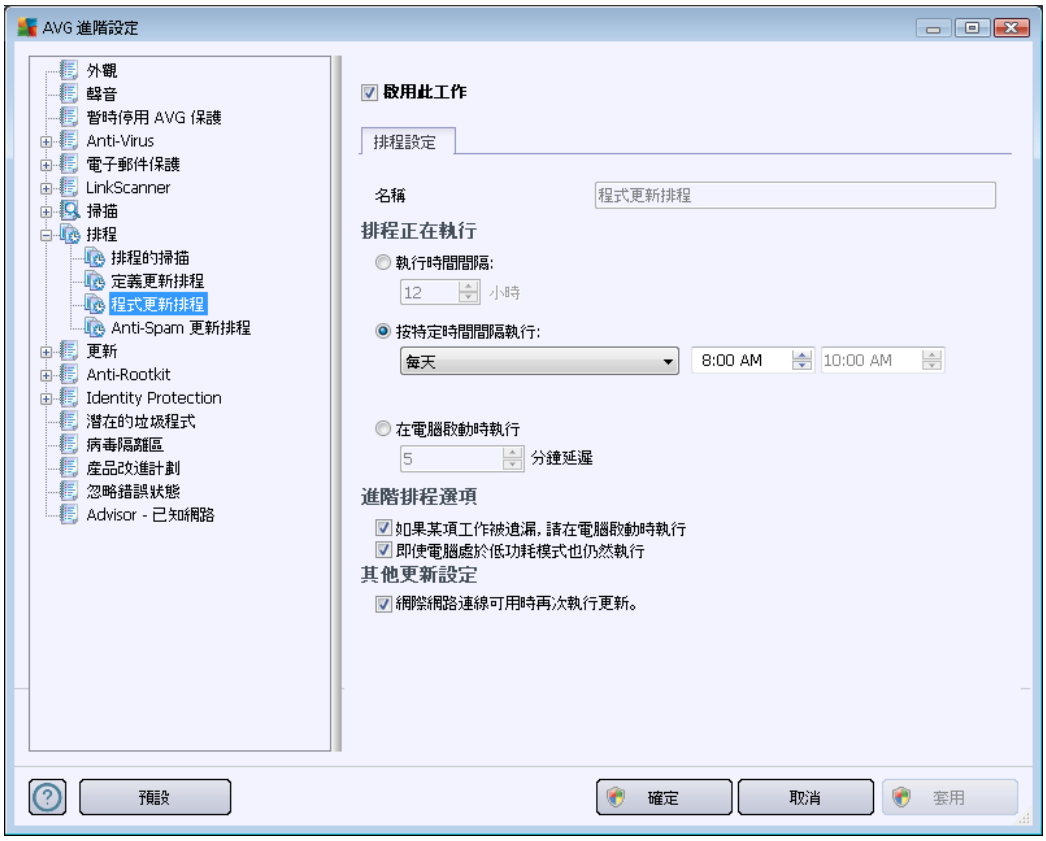
此區段允許您定義電腦處於低功耗模式或完全關閉時，應該在何種條件下啟動/不啟動更新。

其他更新設定

最後，核取***網際網路連線可用時即再次執行更新***選項，確定在發生網際網路連線損毀且更新程序失敗的情況下，它會在網際網路恢復連線後立即重新啟動。在您指定的時間啟動排程的更新後，系統會在 AVG 系統匣圖示上開啟一個快顯視窗來通知您此情況 (*前提是您保留進階設定/外觀對話方塊的預設組態*)。

10.8.3. 程式更新排程

真的有必要時，您可以取消核取***啟用此工作***項目，即可暫時停用排定的程式更新，稍後再開啟它：



在稱為***名稱***的文字欄位中 (*已針對所有預設排程停用*)，顯示的是由程式廠商指派給此排程的名稱。

排程執行

在這裡，為新排程的程式更新啟動指定時間間隔。時間安排有以下幾種定義方式：定義一段時間後再次啟動更新 (***每...執行一次***)，或定義確切的日期和時間 (***在特定時間執行...***)，或者定義更新啟動應關聯的事件 (***在電腦啟動時執行***)。

進階排程選項

此部分允許您定義電腦處於低功耗模式或完全關閉模式時，應該在何種條件下啟動/不啟

動程式更新。

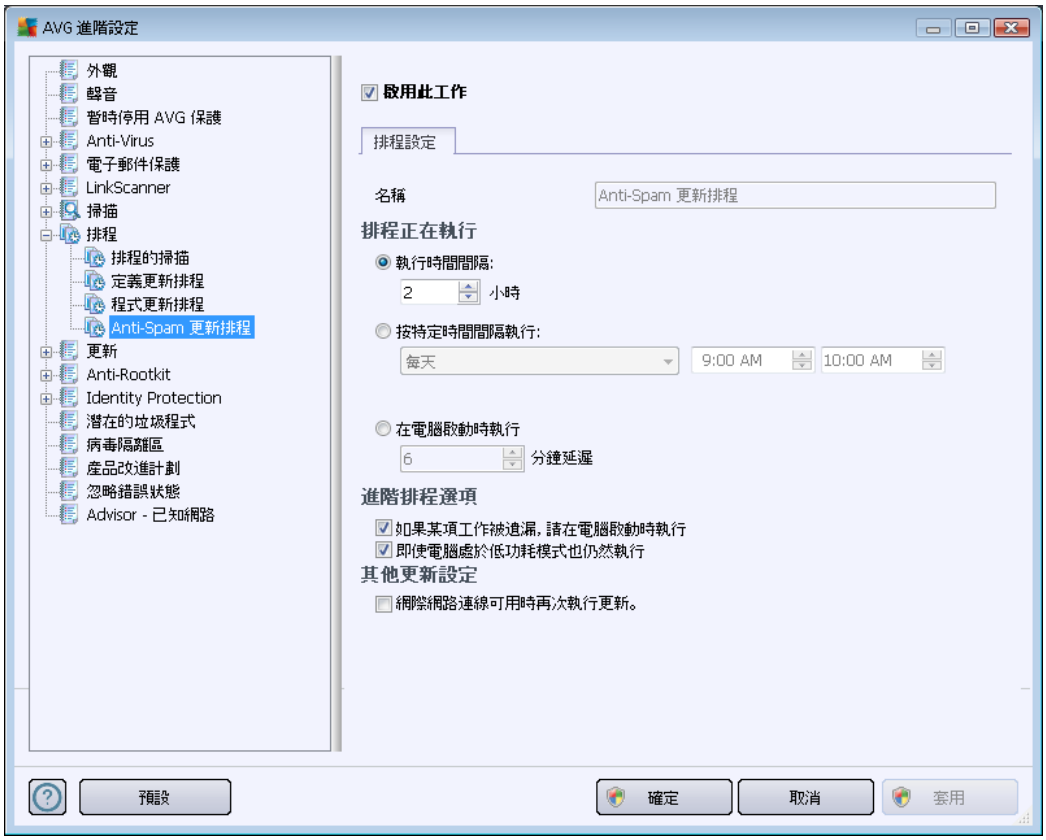
其他更新設定

核取***網際網路連線可用時即再次執行更新***選項，確定在發生網際網路連線損毀且更新程序失敗的情況下，它會在網際網路恢復連線後立即重新啟動。在您指定的時間啟動排程的更新後，系統會在 AVG 系統匣圖示上開啟一個快顯視窗來通知您此情況 (*前提是您保留進階設定/外觀對話方塊的預設組態*)。

注意：*如果一項排程應用程式更新和排程掃描撞期，則程式更新擁有較高的優先順序，而掃描將會暫停。*

10.8.4. Anti-Spam 更新排程

真的有必要時，您可以取消核取***啟用此工作*** 項目，暫時停用 排程的 Anti-Spam 更新，稍後再開啟它。



在此對話方塊中，您可以設定一些詳細的更新排程參數。在稱為***名稱***的文字欄位中 (*已針對所有預設排程停用*)，顯示的是由程式廠商指派給此排程的名稱。

排程執行

在這裡，為新排程的 Anti-Spam更新啟動指定時間間隔。時間安排可定義為一段時間後再次啟動 Anti-Spam 更新啟動 (***執行時間間隔***)，或定義確切的日期和時間 (***按特定時間間隔執行***)，或者可能透過定義一個關聯更新啟動的事件 (***在電腦啟動時執行***)。

進階排程選項

此區段允許您定義電腦處於低功耗模式或完全關閉模式時，應該在何種條件下啟動/不啟動 Anti-Spam 更新。

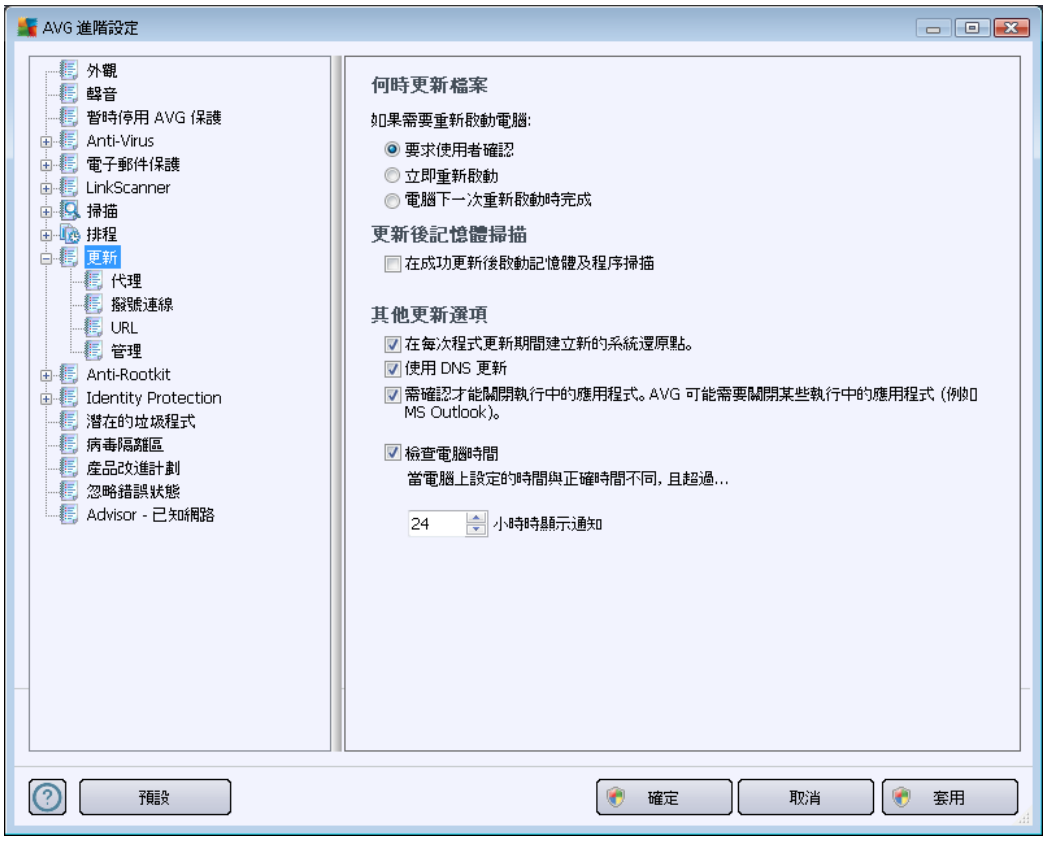
其他更新設定

核取***網際網路連線可用時即再次執行更新***選項，確定在發生網際網路連線損毀且 Anti-Spam 更新程序失敗的情況下，它會在網際網路恢復連線後立即重新啟動。

在您指定的時間啟動排程的掃描後，系統會在 AVG 系統匣圖示上開啟一個快顯視窗來通知您此情況 (*前提是您保留進階設定/外觀對話方塊的預設組態*)。

10.9. 更新

更新巡覽項目會開啟一個新的對話方塊，您可以在這裡指定有關 AVG 更新的一般參數：



何時更新檔案

在本區段中，當更新程序要求電腦重新開機時，您可以選用三種替代選項。您可以將更新排定在下次電腦重新啟動時完成，也可以立即重新啟動：

- ***要求使用者確認*** *(預設)* - 系統會詢問您是否同意重新啟動電腦，以完成更新程序
- ***立即重新啟動*** - 更新程序完成後，無需您的同意，電腦便會立即自動重新啟動。
- ***電腦下次重新啟動時完成*** - 更新程序將延至下次電腦重新啟動時完成。請記住，唯有在您確定電腦會定期啟動 (一天至少一次) 時才建議使用此選項！

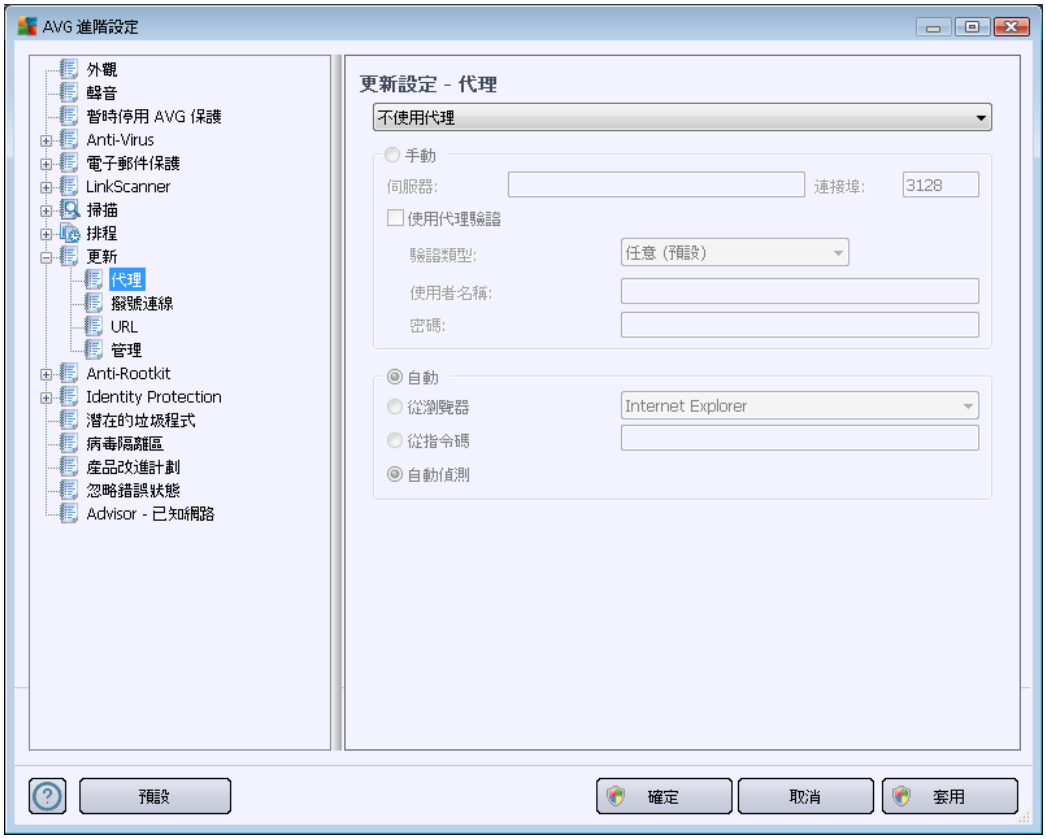
更新後記憶體掃描

標示此核取方塊可定義您想在每次順利完成更新後啟動新的記憶體掃描。最新下載的更新可能已包含新病毒定義，而這些病毒定義可立即套用在掃描中。

其他更新選項

- ***在每次程式更新期間建立新的系統還原點*** - 在每次啟動 AVG 程式更新之前，都會建立一個系統還原點。如果更新程序失敗，且作業系統當機，您始終可以將作業系統還原為在此還原點時的原始組態。該選項可透過 「開始/所有程式/附屬應用程式/系統工具/系統還原」存取，但是，只建議經驗豐富的使用者進行變更！如果您想利用此功能，請將此核取方塊保持為勾選狀態。
- ***使用 DNS 更新*** (*預設為開啟狀態*) - 如果勾選此項目，一旦發佈更新，您的 **AVG Internet Security 2012** 便會查找有關 DNS 伺服器上最新病毒庫版本和最新程式版本的資訊。然後，僅會下載和套用必不可少的最小必要更新檔案。這樣，下載的資料總量會減至最小，更新程序會執行得更快。
- ***需確認才能關閉執行中的應用程式*** (*預設為關閉*) 選項將幫助您確保如果需要關閉目前在執行中的應用程式來完成更新程序，則需經過您的許可才能關閉。
- ***檢查電腦時間*** - 標示此選項，表明您希望在電腦時間與正確時間相差超過指定的小時數時顯示通知。

10.9.1. 代理



代理伺服器是一台獨立伺服器或是在電腦上執行的一項服務，它可以保證更安全的網際網路連線。根據指定的網路規則，您可以直接存取或透過代理伺服器存取網際網路 ;也可以同時使用這兩種方式。然後，在***更新設定 - 代理***對話方塊的第一個項目中，您必須從下拉式方塊功能表中選取要執行的動作：

- ***使用代理***
- ***不使用代理*** - 預設設定
- ***嘗試使用代理連線，如果失敗，則直接連線***

如果您選取了任何使用代理伺服器的選項，還必須指定一些詳細資料。可手動或自動組態伺服器設定。

手動組態

如果您選取手動組態 (核取***手動****選項以啟動相應的對話方塊部分*)，則必須指定以下項目：

- ***伺服器*** –指定伺服器的 IP 位址或伺服器名稱
- ***連接埠*** –指定啟用網際網路存取的連接埠號 (*預設情況下，該號碼設定為 3128，但*

也可設定為其他值 –如果不確定，請聯絡您的網路管理員)

代理伺服器也為每個使用者組態了特定規則。如果您的代理伺服器是依這種方式設定的，請核取***使用代理驗證***選項，以驗證透過代理伺服器連線至網際網路的使用者名稱和密碼是否有效。

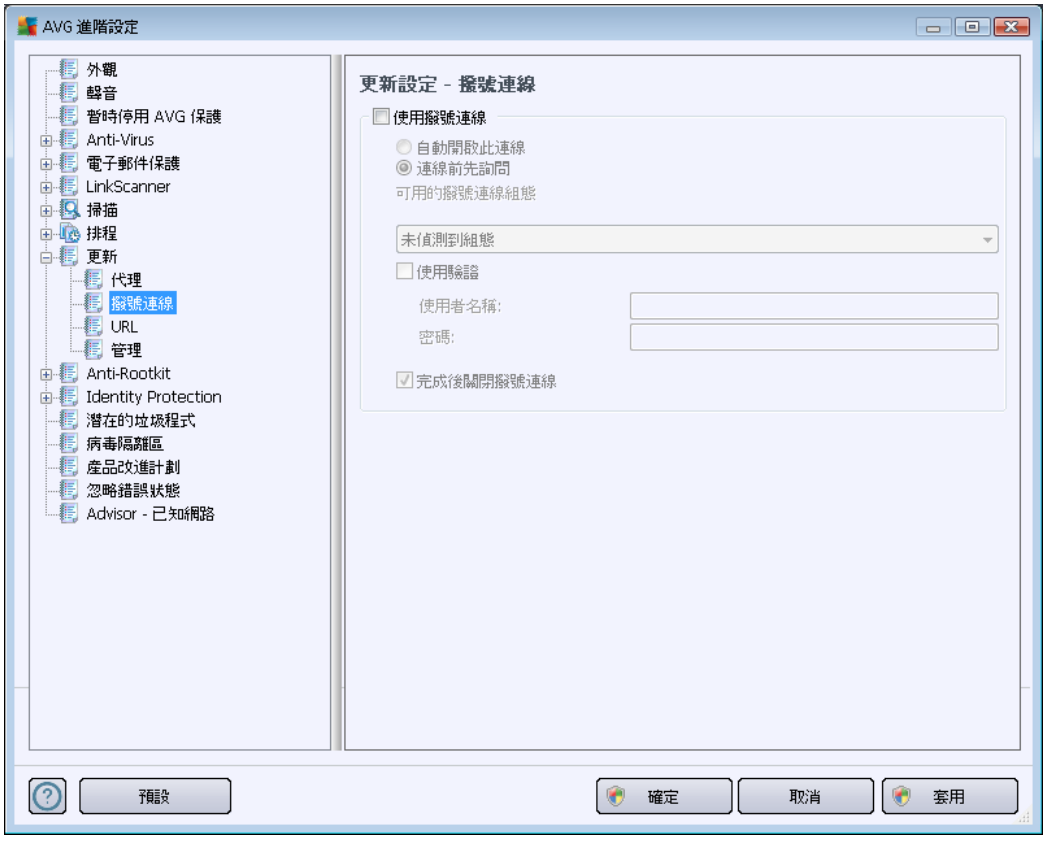
自動組態

如果您選取了自動組態 *(勾選**自動**選項以啟動相應的對話方塊部分)*，則請選取應從何處取得代理組態：

- ***從瀏覽器*** - 將從您預設的網際網路瀏覽器讀取組態。
- ***從指令碼*** - 將從已下載的具有傳回代理位址功能的指令碼讀取組態
- ***自動偵測*** - 將自動直接從代理伺服器偵測組態

10.9.2. 撥號連線

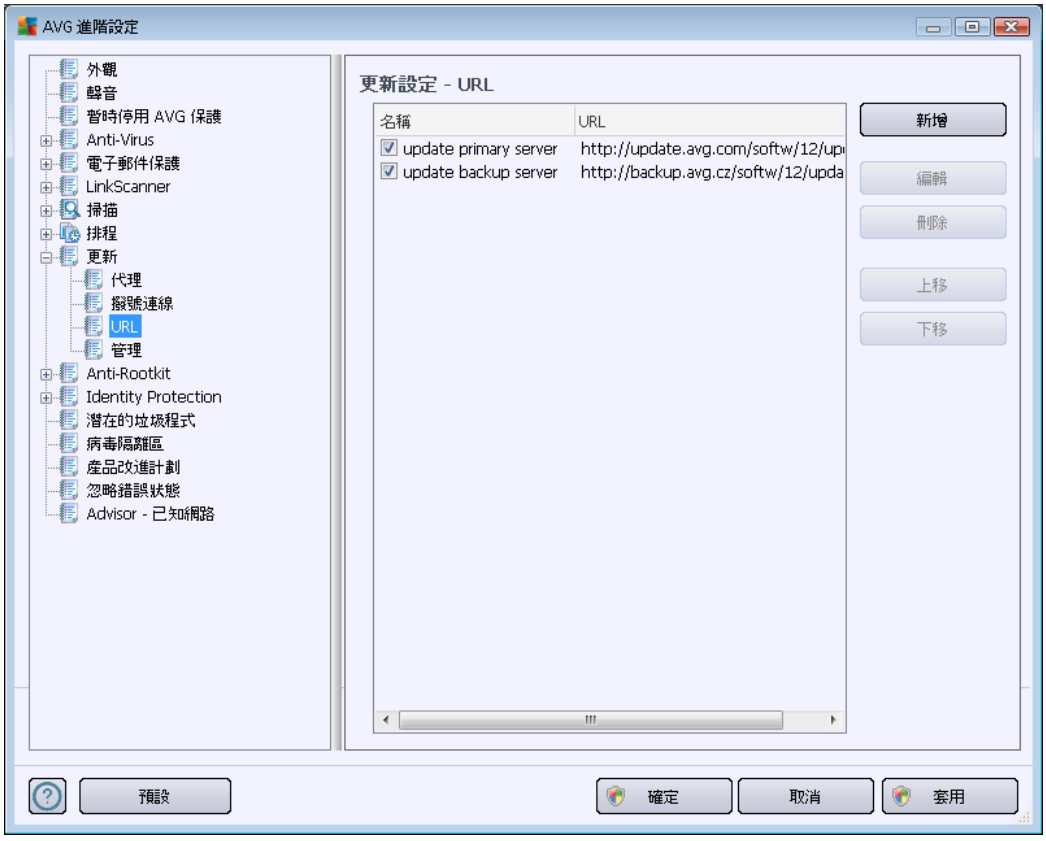
在***更新設定 - 撥號連線***對話方塊中選擇性定義的所有參數均涉及與網際網路的撥號連線。該對話方塊的欄位處於非作用中狀態，除非您核取***使用撥號連線***選項，才會啟動這些欄位。



指定您是否要自動連線到網際網路 (***自動開啟此連線***)，或者您要每次手動確認連線 (***連線前先詢問***)。如果要自動連線，您還需選擇更新完成後是否關閉連線 (***完成後關閉撥號連線***)。

10.9.3. URL

URL 對話方塊提供一份可從中下載更新檔案的網際網路位址清單：



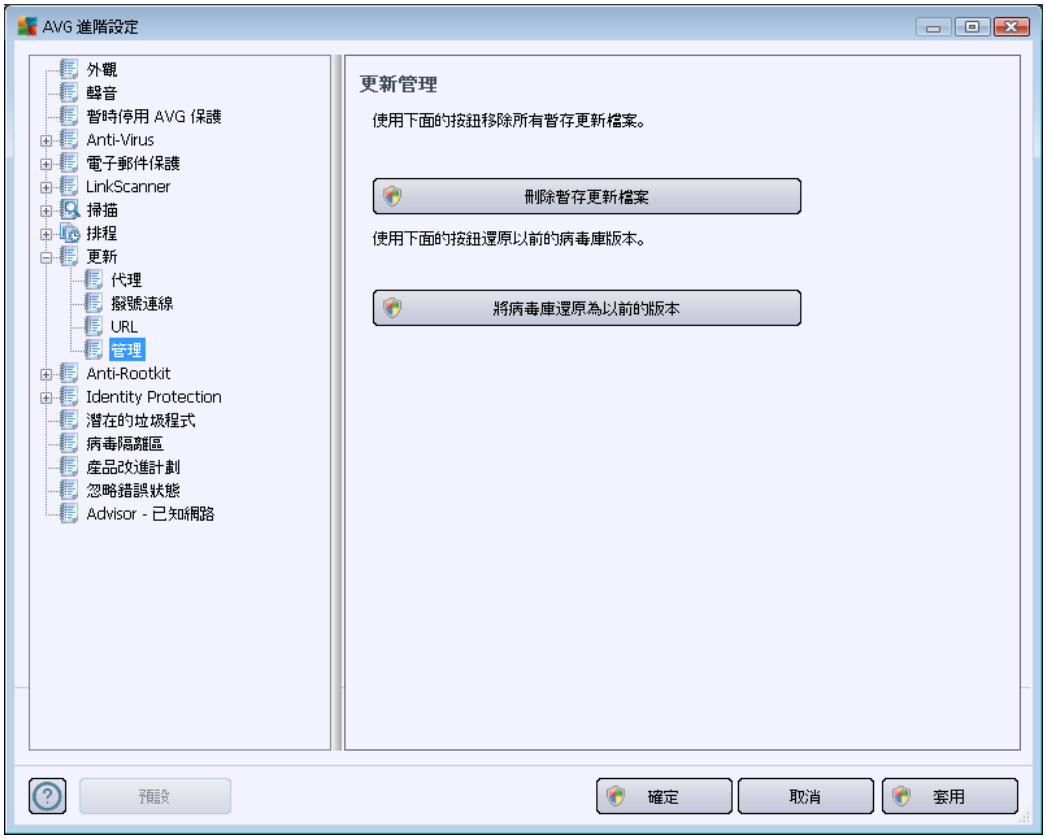
控制按鈕

使用下列控制按鈕可修改該清單及其項目：

- ***新增*** –可開啟一個對話方塊，您可在其中指定要新增到該清單的新 URL
- ***編輯*** - 可開啟一個對話方塊，您可在其中編輯所選 URL 的參數
- ***刪除*** –可從清單中刪除所選 URL
- ***上移*** –可將清單中的選定 URL 向上移動一個位置
- ***下移*** - 可將清單中的選定 URL 向下移動一個位置

10.9.4. 管理

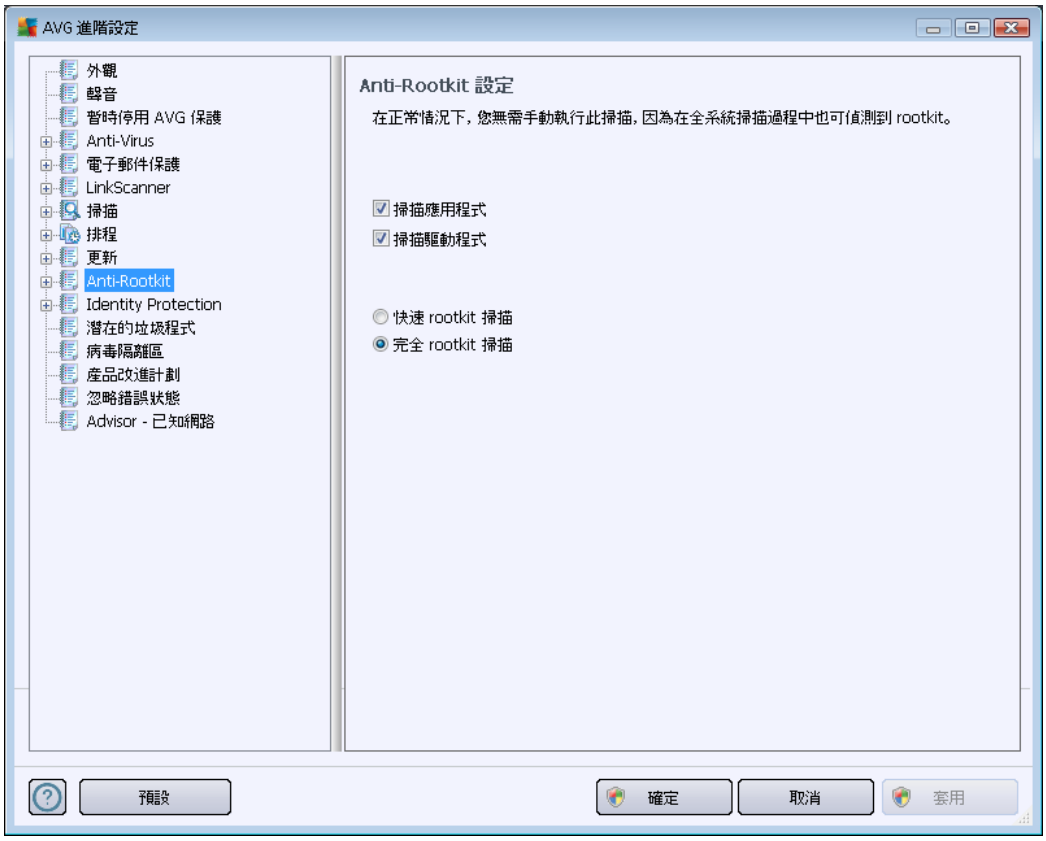
更新管理對話方塊提供兩個可透過兩個按鈕存取的選項：



- ***刪除暫存更新檔案*** - 按下此按鈕可以從硬碟機刪除所有冗餘更新檔案 (*預設情況下，它們將在 30 天後移除*)
- ***將病毒庫還原為以前的版本*** –按下此按鈕可以從硬碟機刪除最新的病毒庫版本，並還原到之前儲存的版本 (*新的病毒庫版本將成為您下次更新的一部分*)

10.10. Anti-Rootkit

在 ***Anti-Rootkit 設定***對話方塊中，您可以編輯 Anti-Rootkit 元件的組態以及 anti-rootkit 掃描的特定參數。Anti-rootkit 掃描是完整電腦掃描的預設程序：



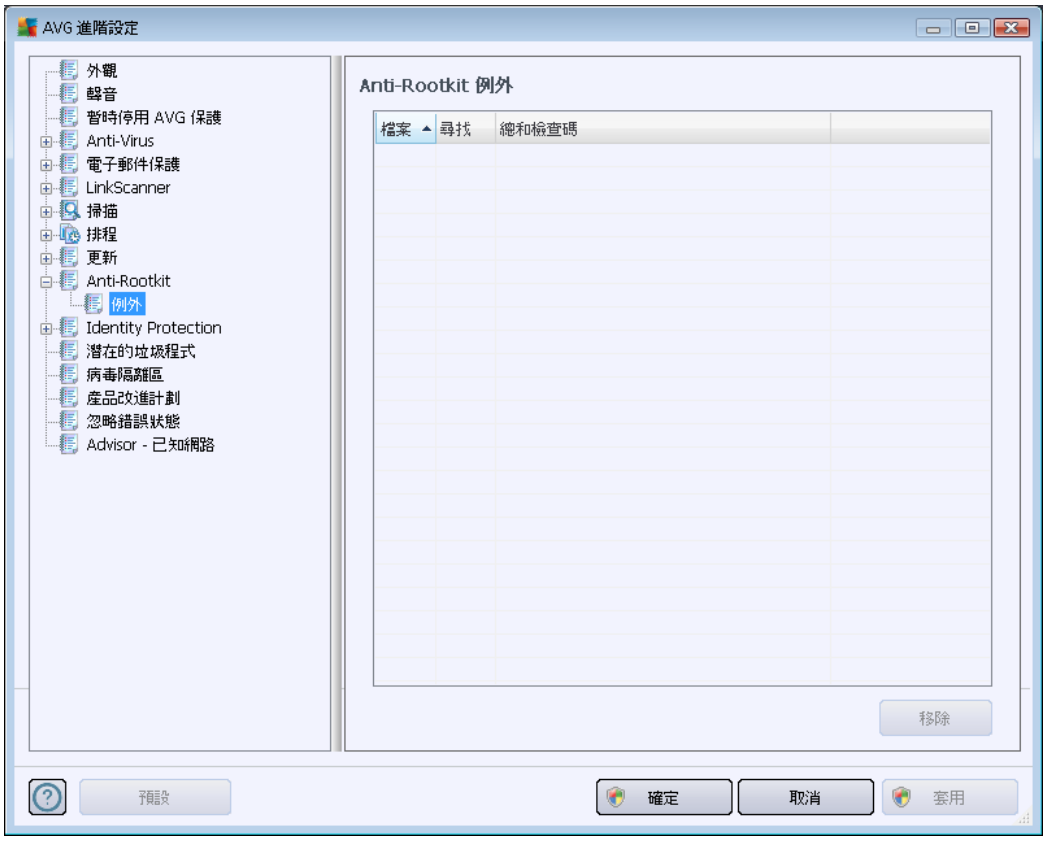
也可以直接從 Anti-Rootkit 元件的介面編輯此對話方塊內提供的所有 Anti-Rootkit 元件功能。

掃描應用程式和***掃描驅動程式***可讓您詳細指定 Anti-Rookit 掃描中應包括的內容。這些設定僅供進階使用者使用；我們建議將所有選項保留為開啟狀態。此外，您還可以挑選 rootkit 掃描模式：

- ***快速 rootkit 掃描*** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾 (*通常是 c:\Windows*)
- ***完全 rootkit 掃描*** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾 (*通常是 c:\Windows*)，加上所有本機磁碟 (*包括快閃磁碟機，但不包括磁碟片/CD 光碟機*)

10.10.1. 例外

您可以在 ***Anti-Rootkit 例外***對話方塊中定義特定檔案 *(例如有些驅動程式可能被誤偵測為 rootkit)* 應該從掃描中排除：

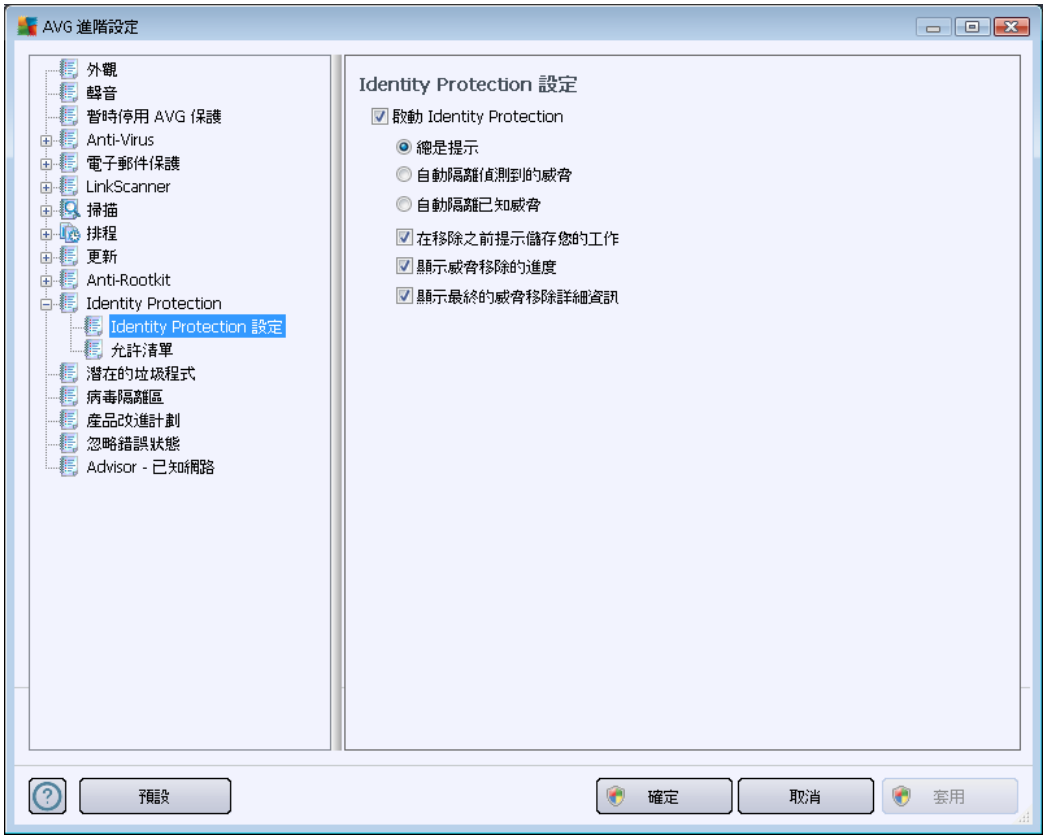


10.11. Identity Protection

Identity Protection 是一款防惡意軟體應用程式，它使用行為技術來保護您的電腦免遭各種惡意軟體 (*間諜軟體、傀儡程式、身份盜賊 ...*) 的攻擊，並提供針對新病毒的零時差防護 *(有關元件功能的詳細說明，請參閱 Identity Protection 章節*)。

10.11.1. Identity Protection 設定

Identity Protection 設定對話方塊可用來開啟／關閉 Identity Protection 元件的基本功能：



啟動 Identity Protection（*預設為開啟*）－取消核取可關閉 Identity Protection 元件。

我們強烈建議您不要這麼做，除非迫不得已！

啓動 Identity Protection 後，您可以指定當偵測到威脅後該怎麼處理：

- ***總是提示***（*預設為開啟*）－當偵測到威脅時，會詢問您是否應移至隔離區，以確保不會移除任何您要執行的應用程式。
- ***自動隔離偵測到的威脅***－勾選此核取方塊以表示您希望將所有可能偵測到的威脅立即移到 病毒隔離區的安全空間。保持預設設定，這樣，當偵測到威脅時，會詢問您是否該將其移至隔離區，以確保不會移除任何您要執行的應用程式。
- ***自動隔離已知威脅***－如果您希望所有被偵測到潛在惡意軟體的應用程式都立即被移至 病毒隔離區，請始終核取此選項。

您可以進一步指派特定項目來啟動 Identity Protection 的其他功能：

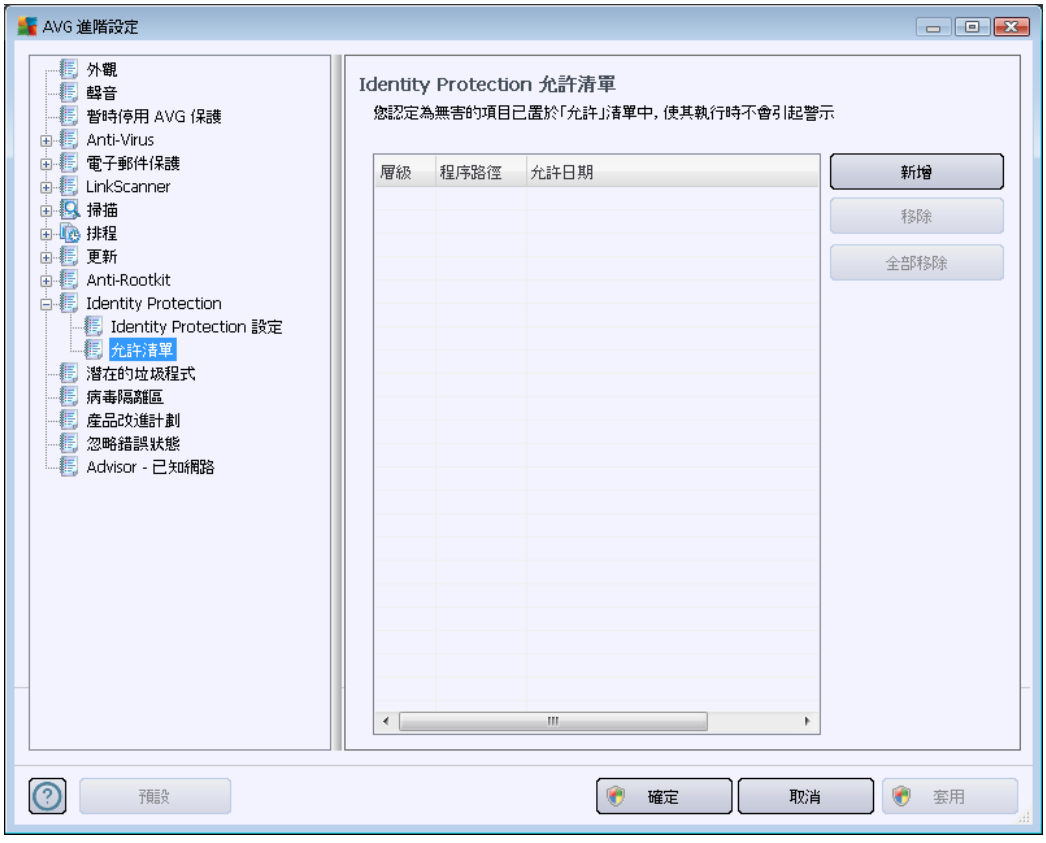
- ***在移除之前提示儲存您的工作***－（*預設情況下為關閉*）－如果您希望在將偵測為可能惡意軟體的應用程式移到隔離區之前收到警告，請始終核取此選項。如果您正在使用該應用程式，您的專案可能會遺失，因此必須先將其儲存。該項目預設為

開啟，強烈建議您不要更動。

- ***顯示威脅移除進度*** – (*預設為開啟*) – 此項開啟時，一旦偵測到潛在惡意軟體，隨即會開啟一個新對話方塊，顯示正被移至隔離區的惡意軟體的移除進度。
- ***顯示最終威脅移除詳細資訊*** – (*預設為開啟*) – 此項目開啟時，***Identity Protection*** 會顯示移至隔離區的每個物件的詳細資訊 *(嚴重性層級、位置等)*。

10.11.2. 允許清單

如果您決定在 ***Identity Protection 設定***對話方塊中取消核取***自動隔離偵測到的威脅***項目，則每次偵測到可能的危險惡意軟體時，都會詢問您是否要移除該軟體。如果您接著將該可疑應用程式 (*依據其行為偵測到*) 指派為安全程式，並確認應將其保留在您的電腦上，則該應用程式會新增至所謂的 ***Identity Protection 允許的清單***中，並且不會再被報告為包含潛在危險內容：



Identity Protection 允許清單中會提供每個應用程式的以下資訊：

- ***層級*** - 按四層級標準，以圖形形式指示相應程序的嚴重性，從不重要 (■□□□) 到嚴重 (■■■■)
- ***程序路徑*** - 應用程式 (*程序*) 可執行檔位置的路徑
- ***允許日期*** - 手動將應用程式指派為安全程式的日期

控制按鈕

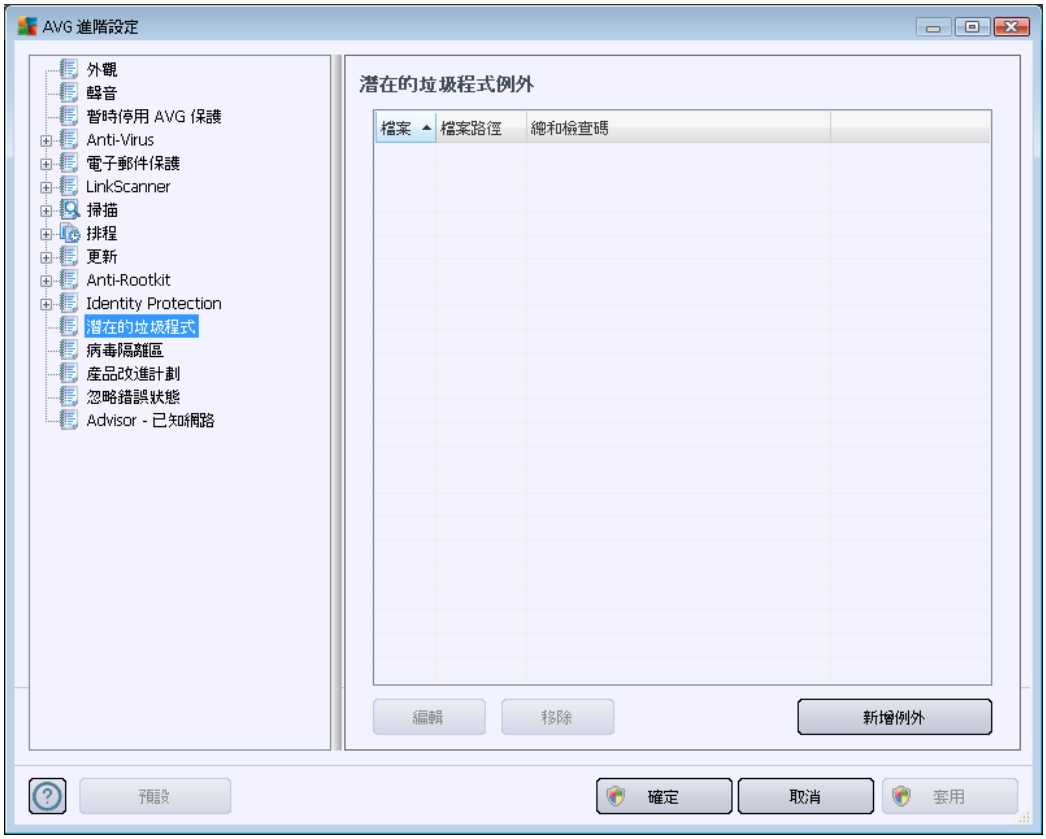
Identity Protection 允許清單對話方塊中可用的控制按鈕如下：

- ***新增*** - 按一下此按鈕可將應用程式新增至允許清單。隨即會快顯下列對話方塊：

  - ***檔案*** - 鍵入您想要標示為例外的檔案 (*應用程式*) 的完整路徑。
  - ***總和檢查碼*** - 顯示所選檔案的唯一「簽名」。此總和檢查碼是自動生成的字元字串，可讓 AVG 清楚地區分所選檔案與其他檔案。總和檢查碼將在成功新增檔案後生成並顯示。
  - ***任何位置 - 不使用完整路徑*** - 如果您要僅針對特定位置將此檔案定義為例外，請不要核取此核取方塊
- ***移除*** - 按一下此按鈕可將選取的應用程式從清單中移除
- ***全部移除*** - 按一下此按鈕可移除列出的所有應用程式

10.12. 潛在垃圾程式

AVG Internet Security 2012 能夠分析和偵測系統中潛在的垃圾可執行應用程式或 DLL 程式庫。在某些情況下，使用者可能希望將特定的不明程式保留在電腦上 (故意安裝的程式)。一些程式 (尤其是免費的) 會包含廣告軟體。**AVG Internet Security 2012** 可能會將這類廣告軟體報告為*潛在的垃圾程式*。如果您想在電腦上保留此類程式，可將其定義為潛在的垃圾程式例外：



潛在的垃圾程式例外對話方塊會顯示已定義且目前有效的潛在垃圾程式例外的清單。您可以編輯清單、刪除現有項目，或新增例外。針對每一項例外，均可在清單中找到下列資訊：

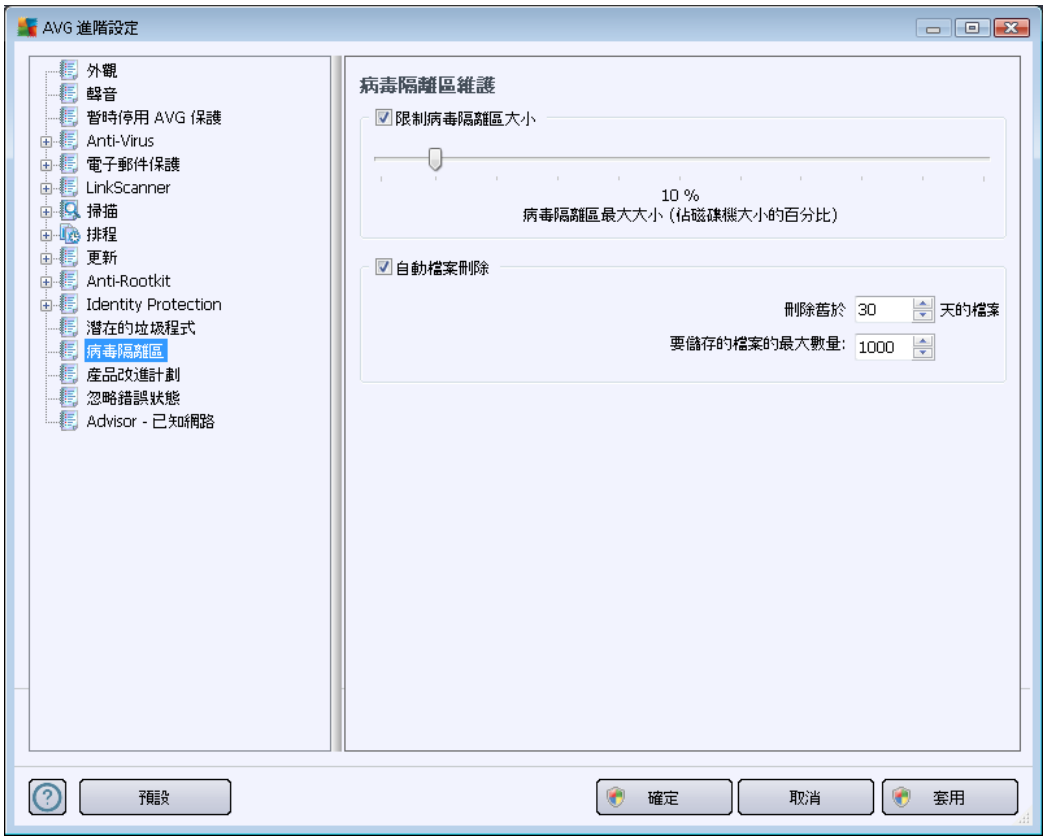
- ***檔案*** - 提供個別應用程式的名稱
- ***檔案路徑*** - 顯示到達應用程式位置的路徑
- ***總和檢查碼*** - 顯示所選檔案的唯一 『簽名』。此總和檢查碼是自動生成的字元字串，可讓 AVG 清楚地區分所選檔案與其他檔案。總和檢查碼將在成功新增檔案後生成並顯示。

控制按鈕

- ***編輯*** - 開啟已定義例外的編輯對話方塊 (*與新例外定義的對話方塊相同，請參閱下文*)，您可以在這裡變更例外的參數
- ***移除*** - 從例外清單刪除所選項目
- ***新增例外*** - 開啟編輯對話方塊，讓您定義要建立的新例外的參數：

- ***檔案*** - 鍵入您想標示為例外的檔案之完整路徑
- ***總和檢查碼*** - 顯示所選檔案的唯一 簽名」。此總和檢查碼是自動生成的字元字串，可讓 AVG 清楚地區分所選檔案與其他檔案。總和檢查碼將在成功新增檔案後生成並顯示。
- ***檔案資訊*** - 顯示與檔案有關的任何其他可用資訊 *(授權/版本資訊等)*
- ***任何位置 - 不使用完整路徑*** - 如果您要僅針對特定位置將此檔案定義為例外，請不要核取此核取方塊。如果已標示該核取方塊，則無論其所在位置為何，都會將指定的檔案定義為例外 *(但是您無論如何都必須填寫指定檔案的完整路徑，該檔案接著會用作為您系統中可能出現兩個相同名稱的檔案的特有範例)*。

10.13. 病毒隔離區



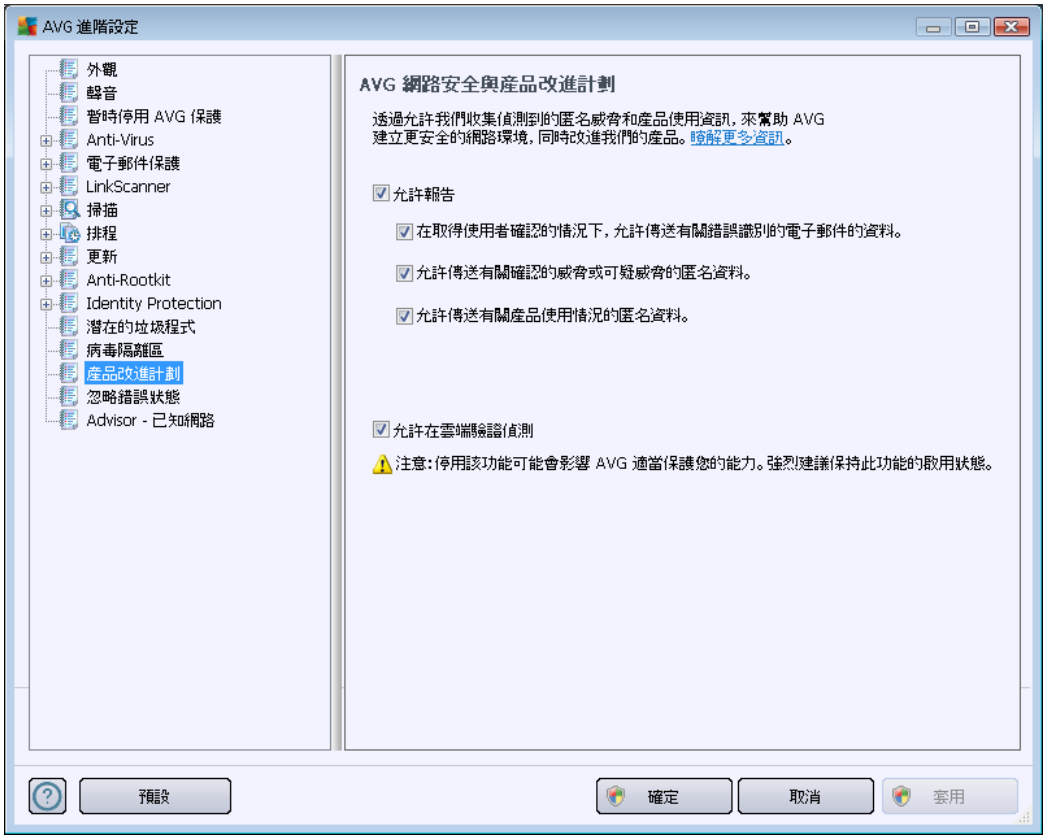
病毒隔離區維護對話方塊可讓您定義多個參數，這些參數與管理儲存在病毒隔離區中的物件有關：

- ***限制病毒隔離區大小*** - 使用滑杆設定病毒隔離區的最大空間。該大小是相較於本機磁碟的大小按比例指定。
- ***自動檔案刪除*** - 在此區段定義物件可以儲存在病毒隔離區的最長時間 (***刪除舊於 ... 天的檔案***)，以及可以儲存在病毒隔離區的最大檔案數 (***要儲存的檔案的最大數量***)。

10.14. 產品改進計劃

AVG 網路安全和產品改進計劃對話方塊會邀請您參與 AVG 產品改進，幫助提高整體網際網路安全性等級。將***允許報告***選項保持標示狀態，即可向 AVG 報告偵測到的威脅。這可以協助我們收集來自全球所有使用者的最新威脅的最新資訊，從而讓我們改進對每個人的保護。

系統會自動處理這些報告，因此不會造成您任何不便，並且報告中不會包含任何個人資料。您可以選擇是否要報告偵測到的威脅，不過我們要求您把這個選項保持開啟狀態。如此可幫助我們改進您與其他 AVG 使用者的保護。



對話方塊中，可用以下設定選項：

- ***允許報告*** *(預設為開啟)* - 如果您希望幫您進一步改進 **AVG Internet Security 2012**，請保持核取此複選方塊。這將向 AVG 報告所有遭遇到的威脅，使我們能夠向世界各地的所有參與者收集有關惡意程式的最新資訊，轉而改進提供給每個人的保護。系統會自動處理這些報告，因此不會給您帶來任何不便，並且報告中不會包含任何個人資料。
    - ***根據使用者確認允許傳送關於識別有誤的電子郵件資料*** *(預設為開啟)* – 傳送有關誤認為垃圾郵件的電子郵件訊息，或是有關 Anti-Spam 元件未偵測到的垃圾郵件的資訊。當傳送這類資訊時，系統會要求您進行確認。
    - ***允許傳送關於已識別或可疑威脅的匿名資料*** (預設為開啟) – *傳送關於在您的電腦上偵測到的任何可疑或確定危險的程式碼或行為模式 (您試圖存取的可能是病毒、間諜軟體或惡意網頁)。*
    - ***允許傳送關於產品使用狀況的匿名資料*** *(預設為開啟)* –傳送關於應用程式使用狀況的基本統計資料，例如偵測數目、已執行的掃描、成功或不成功的更新等。
- ***允許雲端驗證偵測*** (預設為開啟) *–偵測到的威脅都會經過檢查，看看是否已真的受到感染，以排除假警報。*

常見威脅

目前，除了單純的病毒以外，其他種類的威脅不勝枚舉。惡意程式碼和危險網站的作者不斷推陳出新，並且常常有新型的威脅成形，大半都是在網際網路出沒。以下是一些最為普遍的威脅：

- ***病毒***是會自我複製和傳播的一種惡意代碼，通常只在造成損壞後才被發現。有些病毒是嚴重威脅，它會刪除或按其自己的方式故意變更檔案，而有些病毒則執行一些看起來無害的動作，如播放一段音樂。但是，由於其基本的複製能力，所有病毒都是危險的，即使是一個簡單的病毒也可以瞬間佔用所有電腦記憶體並導致電腦崩潰。

- ***蠕蟲***是病毒的一個子類別，它和一般病毒不同，無需附加到「載體」物件；它可以獨立將自身傳送至其他電腦，通常是透過電子郵件，結果導致電子郵件伺服器和網路系統過度負載。

- ***間諜軟體***通常被定義為惡意軟體類別 (*惡意軟體＝任何惡意軟體，包括病毒*) 內含程式 - 通常為特洛伊木馬 - 目的是盜用個人資訊、密碼、信用卡號，或潛入電腦並允許攻擊者進行遠端控制；當然這些動作都是在電腦所有者不知情或未經其同意的情況下執行的。

- ***潛在的垃圾程式***是一種間諜軟體，但並不一定會危害您的電腦。PUP 的具體例子有廣告軟體，它是設計用於散佈廣告的軟體，通常透過廣告快顯視窗的方式顯示；令人煩惱但並非真正有害。

- ***追蹤 cookie*** 也可視為一種間諜軟體，因為這些儲存在網頁瀏覽器中並會在您下次訪問時自動傳送到「上層」網站的小檔案可能包含諸如瀏覽歷程記錄及其他類似資訊等資料。

- ***惡意入侵程式***是一種利用作業系統、網際網路瀏覽器或其他必要程式之漏洞或弱點的惡意代碼。

- ***網路釣魚***是藉由冒充值得信任和知名的組織，進行取得個人機密資料的嘗試。潛在受害者通常會收到一封批量電子郵件，要求其更新銀行帳戶詳細資訊等。為了達到此目的，該電子郵件會邀請收件人進入某個連結，而該連結會將其引導至假的銀行網站。

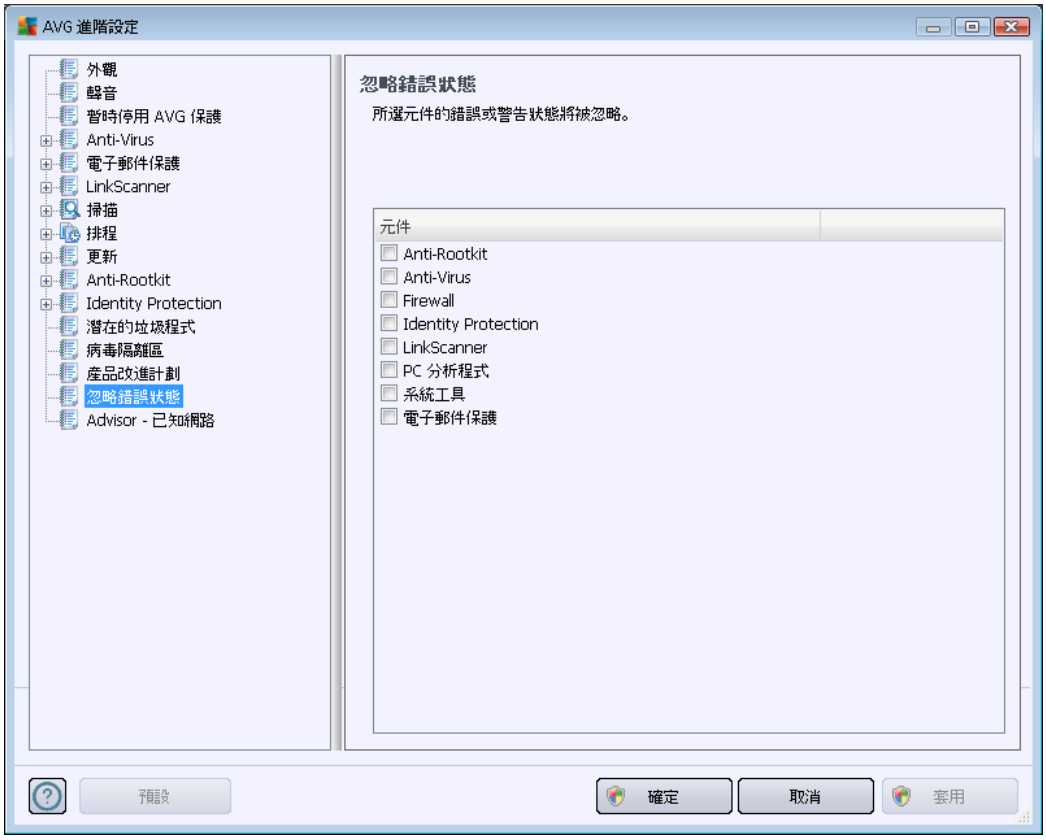
- ***惡作劇***是一種包含危險、警報或騷擾和無用資訊的批量電子郵件。上述威脅中有許多威脅均使用惡作劇電子郵件訊息傳播。

- ***惡意網站***是故意在您的電腦上安裝惡意軟體的一類網站，受駭客入侵的網站也是如此，只是這些網站是被入侵後導致訪問者感染的合法網站。

為了保護您防禦所有這些不同的威脅，AVG Internet Security 2012 包含專門元件。有關這些元件的簡短說明，請參閱元件概觀一章。

10.15. 忽略錯誤狀態

您可以在***忽略錯誤狀態***對話方塊中勾選不希望收到有關其通知的元件：



預設情況下，此清單中沒有選取任何元件。這意味著一旦有元件變為錯誤狀態，將立即透過以下方式通知您：

- 系統匣圖示 - 當所有 AVG 元件運作正常時，此圖示顯示為四種顏色；但若發生錯誤，此圖示會帶有一個黃色驚嘆號，
- 現有問題的文字描述位於 AVG 主視窗的安全性狀態資訊區段

有時出於某種原因，您可能需要將元件暫時關閉 (*通常不建議關閉元件，您應儘量保證所有元件均永久性開啟並處於預設組態，但不排除會發生意外情況*)。此時，系統匣圖示會自動報告元件的錯誤狀態。但是，在此特殊情形下，我們不能將其視為真正的錯誤，因為這是您有意促使它發生的，並且您已對潛在風險有所認識。同時，圖示一旦顯示為灰色，實際上便無法報告其他可能出現的錯誤。

對於這種情況，您可在以上對話方塊中選取可能處於錯誤狀態 (*或已關閉*) 以及您不希望獲取有關其通知的元件。特定元件也有提供相同的選項 *(忽略元件狀態)* 可直接從 AVG 主視窗中的元件概觀存取。

10.16. Advisor - 已知網路

AVG Advisor *包括監視您連線到的網路的功能，如果找到新的網路（具有已經使用過的網路名稱，可能導致混淆）*，它將通知您并建議檢查網路安全性。如果您確定該新的網路可安全連線，您也可將其儲存至該清單；AVG Advisor *將記住該網路的獨特屬性（尤其是 MAC 地址）*，下一次將不再顯示通知。

在此對話方塊視窗中，您可以核取您之前儲存為已知的網路。您可以透過按***移除***按鈕刪除個別項目；則相應網路將重新被視為未知且不安全。

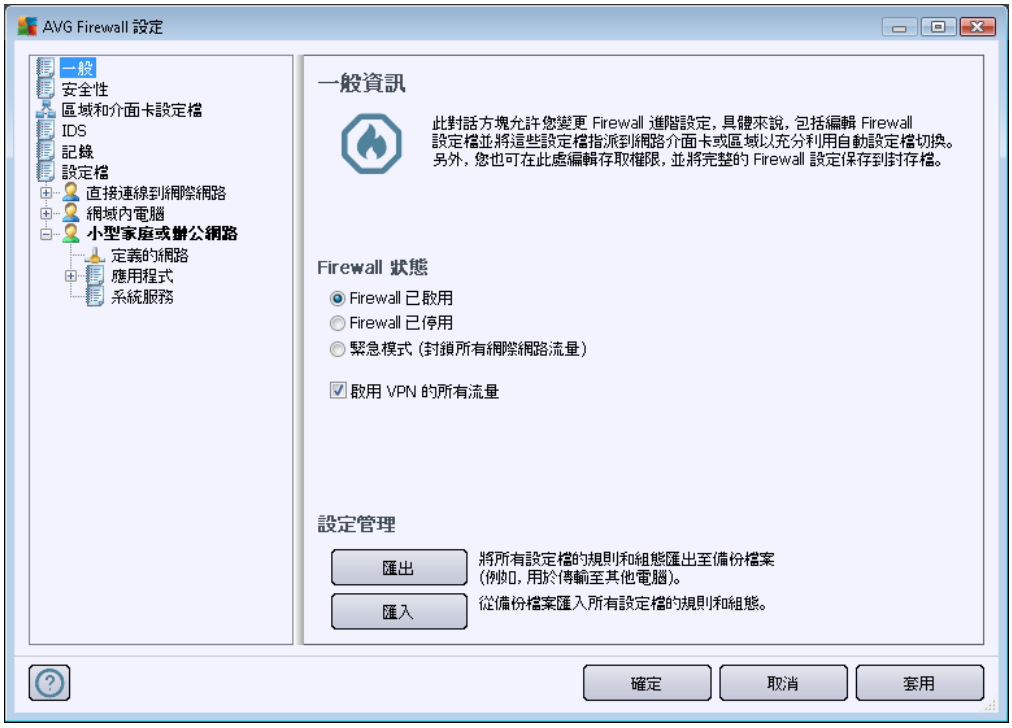
11. Firewall 設定

Firewall 組態會在新視窗中開啟，您可以在其中的幾個對話方塊中設定元件的進階參數。

然而，軟體供應商已對所有 AVG Internet Security 2012 元件進行設定，以提供最佳效能。除非真的有必要，否則請勿變更 AVG 組態。任何設定變更只應由經驗豐富的使用者來執行！

11.1. 一般

一般資訊對話方塊分為兩個區段：



Firewall 狀態

在 ***Firewall 狀態***區段中，您可以在有需要時切換 Firewall 狀態：

- ***Firewall 已啟用*** - 選取此選項將允許與在所選 Firewall 設定檔中定義的規則集中指派為『已允許』的應用程式進行通訊。
- ***Firewall 已停用*** - 此選項可完全關閉 Firewall，不檢查即允許所有網路通訊！
- ***緊急模式 (封鎖所有網際網路流量)*** - 選取此選項可封鎖各個網路連接埠上的所有流量；Firewall 仍會繼續執行，但會停止所有網路流量。
- ***啟用 VPN 所有流量*** *(預設為開啟)* - 如果您使用 VPN *(虛擬私人網路)* 連線，例如從家裡連線到辦公室，建議您核取該方塊。***AVG Firewall*** 將自動搜尋您的網路介面

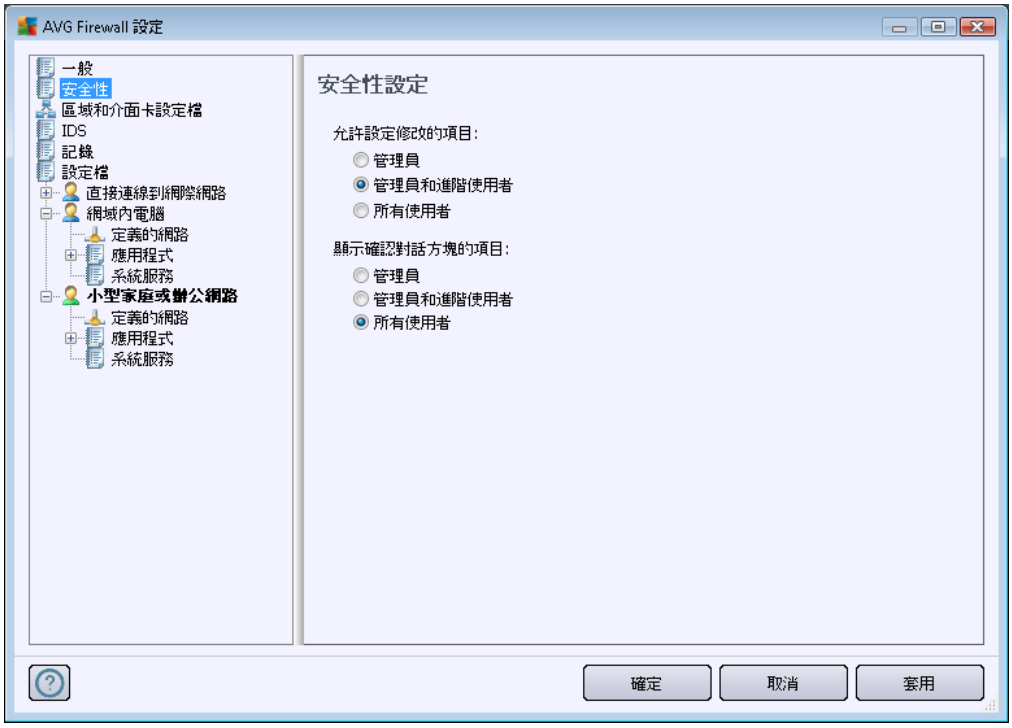
卡，尋找用於 VPN 連線的介面卡，並允許所有應用程式連線到目標網路 *(僅適用於沒有指派特定 Firewall 規則的應用程式)*。在裝有一般網路介面卡的標準系統上，透過這個簡單的步驟，您就不用為每個您需要在 VPN 上使用的應用程式設定詳細規則。

***注意：**若要啟用 VPN 連線，必須允許與下列系統通訊協定通訊：GRE、ESP、L2TP、PPTP。您可以在系統服務對話方塊內完成此動作。*

設定管理

您可以在***設定管理***區段中***匯出***或***匯入*** Firewall 組態，也就是將定義的 Firewall 規則和設定匯出到備份檔案，或是反過來匯入整個備份檔案。

11.2. 安全性



在***安全性設定***對話方塊中，無論所選的設定檔為何，您都可以定義 Firewall 行為的一般規則：

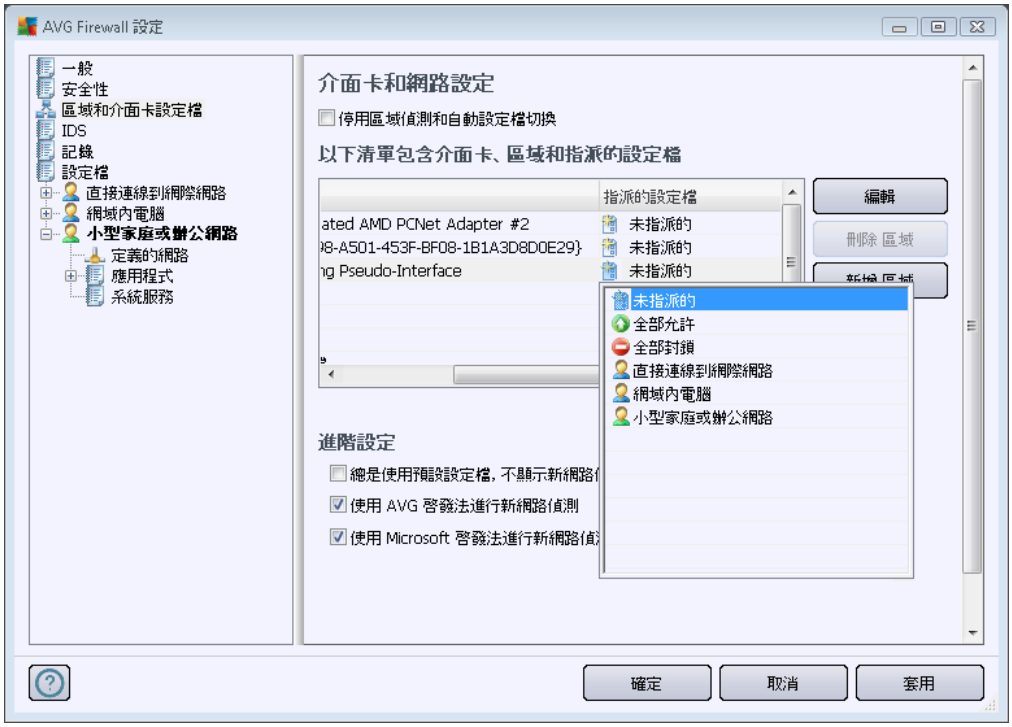
- ***允許設定修改者*** - 指定允許變更 Firewall 組態的使用者。
- ***顯示*** 的確認對話方塊 - 指定應該向其顯示確認對話方塊 *(要求對定義的 Firewall 規則未涵蓋的情形提供決定的對話方塊)* 的使用者。

在這兩種情況下，您都可以將特定權限指派給下列使用者群組之一：

- ***管理員*** –對電腦具備完整控制權，並有權將每個使用者指派到具有特別定義之權限的群組。
- ***管理員和進階使用者*** –管理員可以將任何使用者指派到指定的群組 (*進階使用者*) 並定義群組成員的權限。
- ***所有使用者*** –未指派到任何特定群組的其他使用者。

11.3. 區域和介面卡設定檔

在***介面卡和網路區域設定***對話方塊中，您可以編輯相關設定，將已定義設定檔指派到特定介面卡和對應的網路：



- ***停用區域偵測和自動設定檔切換*** *(預設為關閉)* - 可將其中一個已定義的設定檔指派到各個網路介面類型，並分別指派到各個區域。如果您不想定義特定的設定檔，將使用一個通用設定檔。但是，如果您決定區別各個設定檔，並將它們指派給特定介面卡和區域，但稍後因為某種原因又希望暫時切換此指派，請勾選***停用區域偵測和自動設定檔切換***選項。
- ***介面卡、區域和指派的設定檔清單*** - 在此清單中，您可以找到已偵測到的介面卡和區域的概觀。您可以從定義的設定檔功能表中，為它們各自指派一個特定設定檔。若要開啟此功能表，用滑鼠左鍵按一下介面卡清單中個別的項目 *(在「已指派的設定檔」欄)*，然後從內容功能表選取設定檔。

進階設定

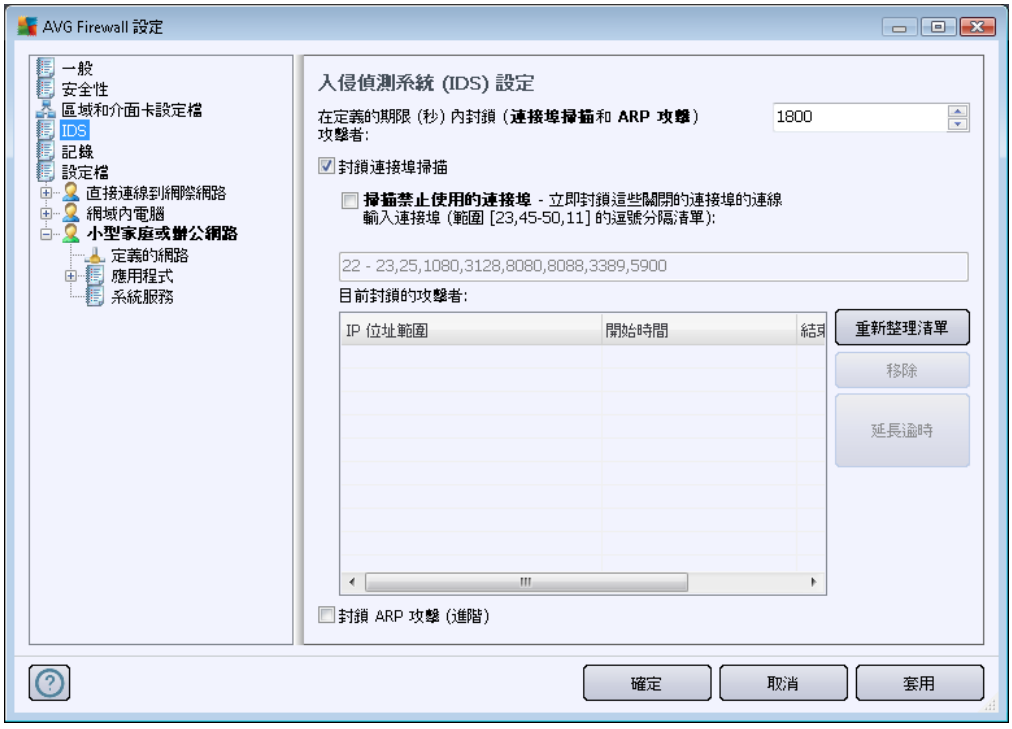
- ***總是使用預設設定檔，不顯示新網路偵測對話方塊*** - 每當您的電腦連線到新網路時，Firewall 都會發出警示並顯示一個對話方塊，提示您選取網路連線類型，以及為它指派 Firewall 設定檔。如果您不希望顯示此對話方塊，請核取此方塊。

- ***使用 AVG 啟發法進行新網路偵測*** - 可透過 AVG 自身的機制收集新偵測到的網路的相關資訊 (*不過，此選項僅適用於 VISTA OS 或更高版本*)。

- ***使用 Microsoft 啟發法進行新網路偵測*** - 可從 Windows 服務取得有關新偵測到的網路的資訊 (*此選項僅適用於 Windows Vista 或更高版本*)。

11.4. IDS

入侵偵測系統是一項特殊的行為分析功能，設計用於識別和封鎖在您電腦特定連接埠上的可疑通訊嘗試。您可以在***入侵偵測系統 (IDS) 設定***對話方塊內設定 IDS 參數：



入侵偵測系統 (IDS) 設定對話方塊提供以下組態選項：

- ***在定義的期限 (秒) 內封鎖 (連接部掃描和 ARP 攻擊)*** - 您可以在此處指定在連接埠上偵測到可疑通訊嘗試時，應將該連接埠封鎖多少秒鐘。預設情況下，時間間隔是設為 1800 秒 (*30 分鐘*)。

- ***封鎖連接埠掃描*** *(預設為開啟)* –核取該方塊可封鎖所有 TCP 和 UDP 連接埠上的外來通訊嘗試。對於任何此類連線，允許五次嘗試，第六次嘗試將被封鎖。該項目預設為開啟，而且建議保留此設定。如果您將***封鎖連接埠掃描***選項保持為開啟狀態，則有一些進一步的詳細組態可用 *(否則，將會停用以下項目)*:

- ***掃描禁止使用的連接埠*** –核取該方塊可立即封鎖以下文字欄位中指定連接埠上的任何通訊嘗試。單個連接埠或連接埠範圍之間應用逗號隔開。如果要使用此功能，有一個建議連接埠的預先定義清單可供您使用。

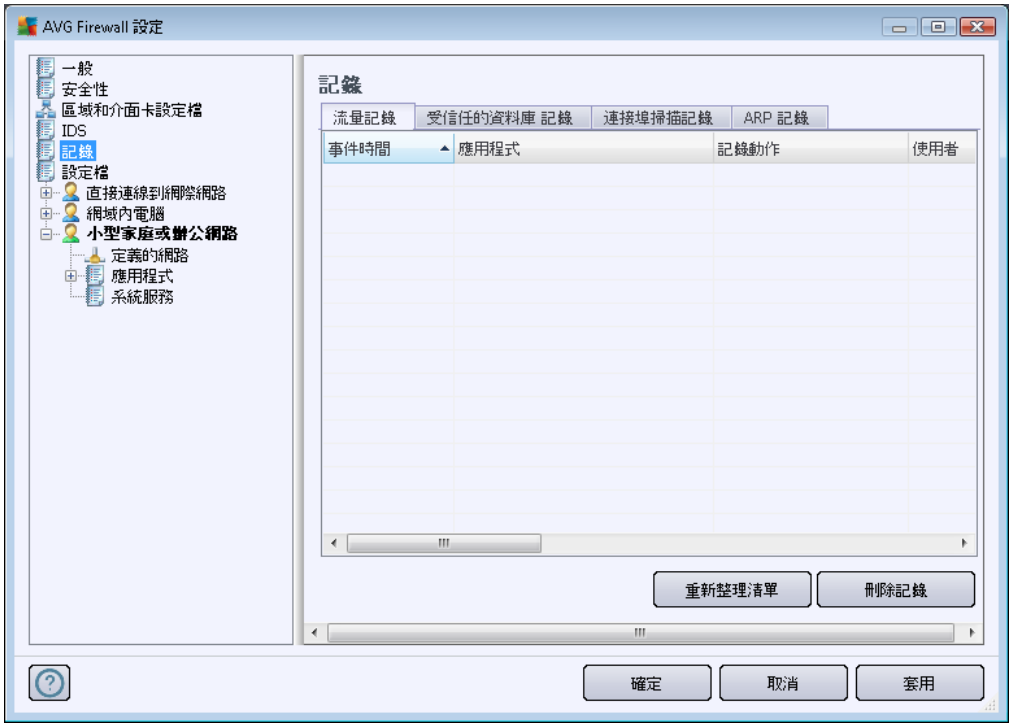
- 目前封鎖的攻擊者 - 此區段中列出了目前遭 Firewall 封鎖的所有通訊嘗試。遭到封鎖的嘗試的完整歷程記錄可在記錄對話方塊 (*連接埠掃描記錄*標籤中) 檢視。

- ***封鎖 ARP 攻擊 (進階)*** *(預設為關閉)* - 標示此選項可啟動封鎖 ***IDS*** 在區域網路中偵測為潛在危險的特殊通訊嘗試類型的功能。套用在***將攻擊者封鎖住一段已定義的時間週期中設定的時間。***我們只建議熟悉其本機網路類型及風險層級的進階使用者使用此功能。

控制按鈕

- ***重新整理清單*** - 按一下該按鈕可更新清單 (*以包含任何最新的阻止嘗試*)
- ***移除*** - 按一下該按鈕可取消所選的阻止
- ***延長逾時*** - 按一下該按鈕可延長阻止所選嘗試的時間。此時出現一個帶有擴充選項的新對話方塊，允許您設定特定時間和日期，或不受限的持續期間。

11.5. 記錄



記錄對話方塊可讓您檢閱四個標籤上所有已記錄的 Firewall 動作和事件清單，以及相關參數的詳細描述 (*事件時間*、*應用程式名稱*、*各自的記錄動作*、*使用者名稱*、*PID*、*流量方向*、

通訊協定類型、遠端和本機連接埠的數量等):

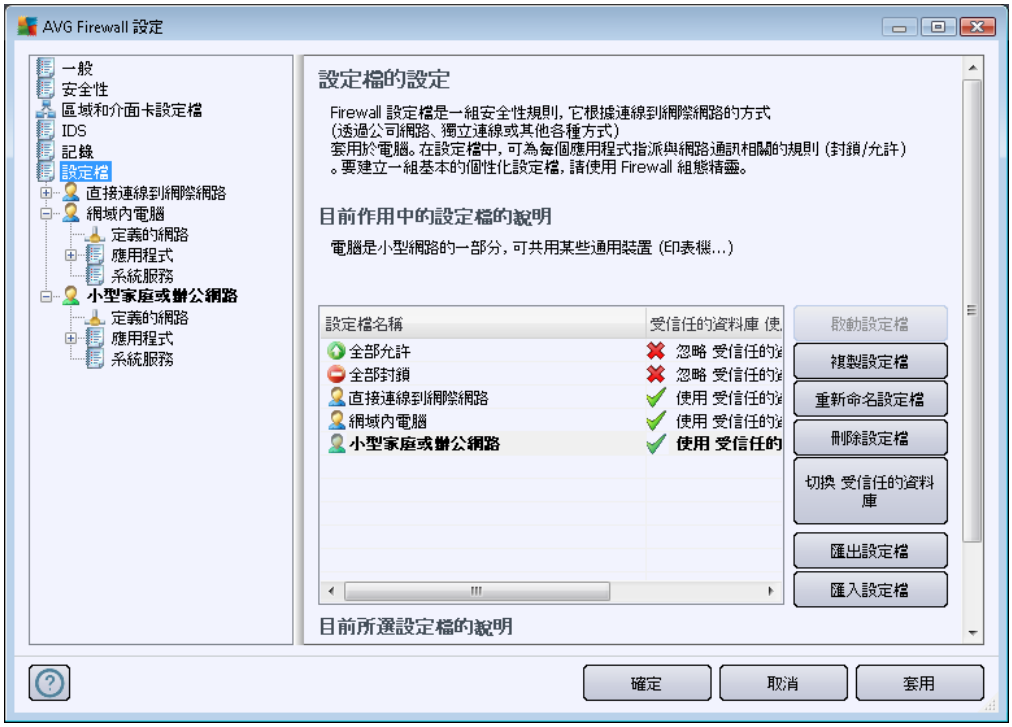
- ***流量記錄*** - 提供所有嘗試連線至網路的應用程式活動的相關資訊。
- ***受信任的資料庫記錄*** - *受信任的資料庫*是 AVG 的內部資料庫，會收集有關已認證和受信任的應用程式資訊，這些應用程式始終都允許進行線上通訊。當新應用程式第一次嘗試連線至網路 (*亦即尚未針對此應用程式指定防火牆規則時*)，有必要瞭解是否應該針對該應用程式允許網路通訊。首先，AVG 會搜尋*受信任的資料庫*，如果上面有列出該應用程式，便會自動授權存取網路。如果在搜尋資料庫之後，發現資料庫內沒有關於該應用程式的資訊，這時才會在獨立的對話方塊中詢問您是否要允許該應用程式存取網路。
- ***連接埠掃描記錄檔*** - 提供所有入侵偵測系統活動的記錄。
- ***ARP 記錄檔*** - 記錄有關阻止本機網路內進行特殊通訊嘗試 (*阻止 ARP 攻擊選項*)，並且被入侵偵測系統偵測為可能有害的資訊。

控制按鈕

- ***重新整理清單*** - 可根據所選屬性排列所有記錄的參數 :按時間先後 (*日期*) 或按字母順序 (*其他欄*) - 只要按一下相應的欄標題就可以了。使用***重新整理清單***按鈕更新目前顯示的資訊。
- ***刪除記錄*** - 按此按鈕可刪除圖表中的所有項目。

11.6. 設定檔

您可以在***設定檔的設定***對話方塊中找到所有可用設定檔的清單：



無法編輯系統設定檔 *(全部允許、全部封鎖)*。不過，可在此對話方塊中使用以下控制按鈕來編輯所有自訂設定檔 *(直接連線到網際網路、網域內電腦、小型家庭或辦公網路)*：

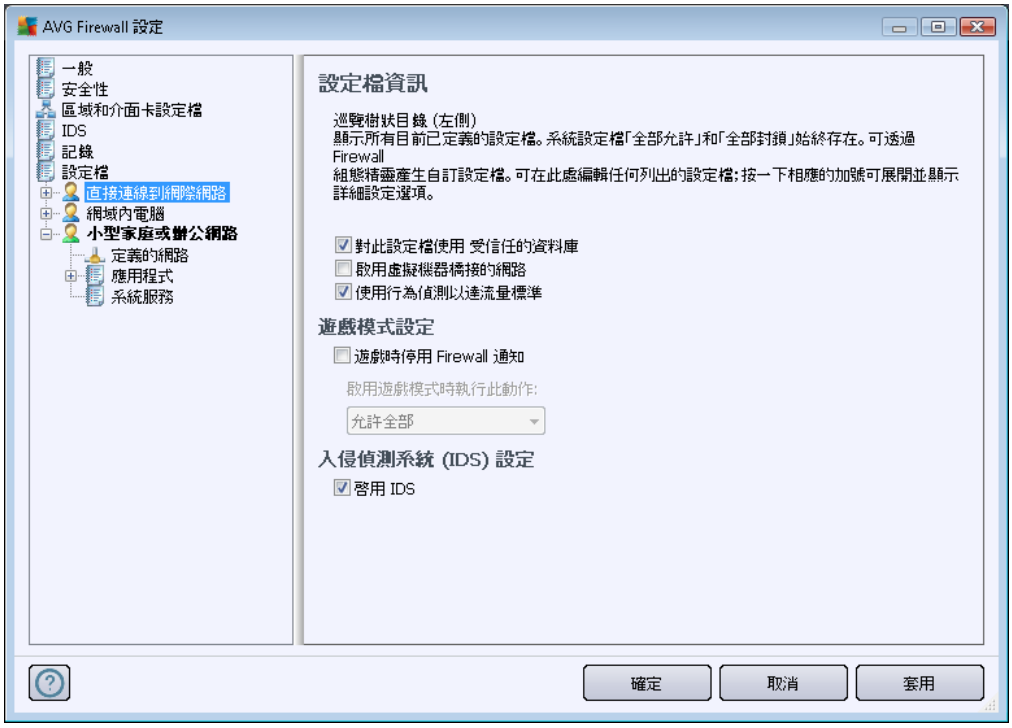
- ***啟動設定檔*** - 此按鈕會將所選設定檔設定為作用中，這表示 Firewall 將使用所選設定檔組態來控制網路流量。
- ***複製設定檔*** - 建立與所選設定檔相同的副本；日後您可編輯和重新命名該副本，以該複製的原始設定檔為基礎建立新設定檔。
- ***重新命名設定檔*** - 允許您為所選設定檔定義新的名稱。
- ***刪除設定檔*** - 從清單中刪除所選設定檔。
- ***切換受信任的資料庫*** - 您可以決定對於所選的設定檔使用*受信任的資料庫*資訊 (*受信任資料庫是 AVG 的內部資料庫，會收集有關已認證和受信任應用程式的資訊，這些應用程式永遠都被允許進行線上通訊。*)。
- ***匯出設定檔*** - 將設定檔的組態記錄到檔案中，並儲存該檔案以供日後使用。
- ***匯入設定檔*** - 根據從備份組態檔案匯出的資料，設定所選設定檔的設定。

您可以在對話方塊的底端找到上述清單中目前所選設定檔的說明。

根據在***設定檔***對話方塊中的清單中所提到的已定義設定檔的數量，左側巡覽功能表的結

構將會相應變更。每個定義的設定檔會在***設定檔***項目下面建立特定分支。然後可在以下對話方塊 (*對所有設定檔均相同*) 中對特定設定檔進行編輯：

11.6.1. 設定檔資訊



設定檔資訊對話方塊是可讓您在與設定檔的特定參數相關的獨立對話方塊中編輯每個設定檔的組態的第一個對話方塊。

- ***對此設定檔使用受信任的資料庫*** (*預設為開啟*) - 標示此選項可啟動*受信任的資料庫* (*即 AVG 內部資料庫，會收集有關進行線上通訊的受信任和已認證的應用程式的資訊。如果沒有為個別的應用程式指定規則，則必須瞭解是否可以授權讓該應用程式存取網路。AVG 會先搜尋受信任的資料庫，如果上面有列出該應用程式，便會將之視為安全，然後允許其在網路上通訊。否則，會請您決定是否應允許應用程式在網路上通訊*)。

- ***啟用虛擬機器橋接的網路*** (*預設為關閉*) - 勾選此項目可允許 WMware 中的虛擬機器直接連線至網路。

- ***使用行為偵測以達流量標準*** (*預設為開啟*) - 標示此選項可允許 Firewall 在評估應用程式時使用 Identity Protection 功能 - Identity Protection 可辨別應用程式是否出現任何可疑行為，或者是否可信任並允許進行線上通訊。

遊戲模式設定

您可以在***遊戲模式設定***區段透過勾選相應項目來決定和確認是否要顯示 Firewall 資訊訊息，即使您的電腦正在執行全螢幕應用程式也一樣 (*這些通常為遊戲，但也適用於全螢幕應用程式，如 PPT 簡報*)，因為資訊訊息可能會產生干擾。

如果您勾選***游戲時停用 Firewall 通知***項目，然後在下拉式功能表選取在有尚未指定任何規則的新應用程式嘗試在網路上通訊時要採取的動作 (*這種應用程式通常會引發詢問對話方塊*)，您可以允許或阻止所有這些應用程式。

開啟遊戲模式後，所有排程的工作 (*掃描*、*更新*) 都會延遲到應用程式關閉後才執行。

入侵偵測系統 (IDS) 設定

標示***啟用 IDS*** 核取方塊可啟動專門用於識別和封鎖在您電腦特定的連接埠上嘗試可疑通訊的特殊行為分析功能 *(有關此功能設定的詳細資訊，請查閱本文件的 IDS 一章)*。

11.6.2. 定義的網路

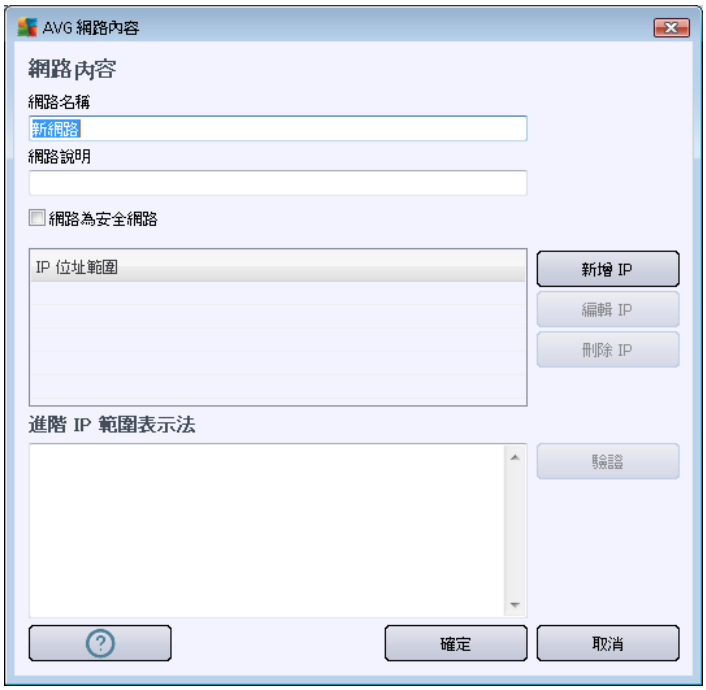
定義的網路對話方塊提供電腦可連線的所有網路清單。

該清單提供每個偵測到的網路的以下資訊：

- ***網路*** - 提供與電腦連線的所有網路的名稱清單。
- ***網路安全*** - 預設情況下，所有網路都視為不安全，只有當您確定某個網路是安全的，才可以將它指派為安全 (*按一下指向對應網路的清單項目，然後從內容功能表中選取 安全*) - 所有安全網路接著會包括到一個群組中，該群組內的應用程式可以透過將應用程式規則設為允許安全網路來進行通訊。
- ***IP 位址範圍*** - 會自動偵測每個網路，並使用 IP 位址範圍的格式指定。

控制按鈕

- ***新增網路*** - 開啟***網路內容***對話方塊視窗，您可在這裡編輯新定義網路的參數：



在此對話方塊中，您可以指定***網路名稱***，提供***網路描述***，還可以將網路指派成安全的。您可以在透過***新增 IP*** 按鈕 (也可以使用***編輯 IP***/***刪除 IP***) 開啟的獨立對話方塊中手動定義新網路，在此對話方塊中，您可以透過提供 IP 範圍或遮罩來指定網路。如果有大量的網路要定義為新建網路的一部分，您可以使用***進階 IP 範圍表示法***選項：在相應文字欄位中輸入所有網路的清單 (*支援所有標準格式*)，然後按一下***驗證***按鈕以確認可以識別格式。接著，按下***確定***確認並儲存資料。

- ***編輯網路*** - 開啟***網路內容***對話方塊視窗 (*請參閱上文*)，您可以在這裡編輯已定義網路的參數 (*這個對話方塊與新增網路的對話方塊完全一樣，請參閱前段說明*)。

- ***刪除網路*** - 從網路清單中移除所選網路的註釋。

- ***標示為安全*** - 預設情況下，所有網路都被視為不安全，而且只有當您確定個別的網路是安全的時候，才可使用此按鈕將它指派為安全 (*反過來也是一樣，網路一旦被指派為安全，按鈕文字就會變更為「標記為不安全」*)。

11.6.3. 應用程式

該***應用程式資訊***對話方塊列出了可能需要進行網路通訊的所有已安裝應用程式，以及已指派的動作對應的圖示：

應用程式清單中的應用程式是您電腦上所偵測到 (*並指派個別動作*) 的應用程式。可使用以下動作類型：

- - 允許所有網路的通訊
- - 只允許定義為 「安全」的網路進行通訊
- - 封鎖通訊
- - 顯示詢問方塊 (*使用者將能夠決定當應用程式嘗試透過網路通訊時，是要允許還是封鎖通訊*)
- - 定義的進階設定

請注意，僅會偵測已安裝的應用程式，因此，如果您日後安裝新應用程式，需要為其定義 Firewall 規則。預設情況下，當新應用程式首次嘗試透過網路連線時，Firewall 將根據受信任的資料庫自動為該應用程式建立規則，或詢問您是希望允許還是希望封鎖該通訊。在第二種情況中，您將可以將您的答案儲存為永久性規則 (隨後會在此對話方塊中列出)。

當然，也可以立即為新應用程式定義規則，方法是在此對話方塊中，按一下***新增***並填入應用程式詳細資訊。

除應用程式外，該清單還包含兩個特殊項目：

- ***優先應用程式規則*** (*位於清單頂端*) 具有最高優先順位，始終在任何單獨應用程式規則之前套用。
- ***其他應用程式規則*** (*位於清單底端*) 具有最低優先順位，只有當其他應用程式規則都不適用時才會套用 (例如一個未知也未定義的應用程式)。選取當這類應用程式試圖在網路上進行通訊時應觸發的動作：
    - o *封鎖*－將一律封鎖通訊。
    - o *允許* –將允許任意網路上的通訊。
    - o *詢問* –將讓您來決定允許還是封鎖通訊。

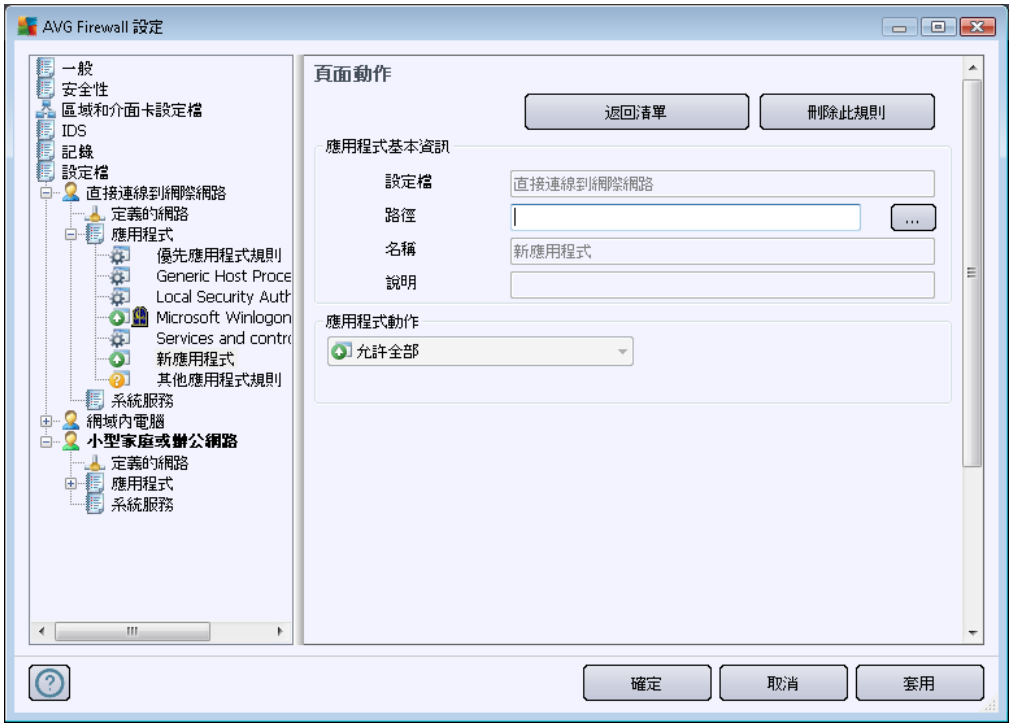
這些項目有不同於一般應用程式的設定選項，僅供經驗豐富的使用者使用。強烈建議您不要修改這些設定！

控制按鈕

您可使用以下控制按鈕來編輯該清單：

- ***新增*** - 開啟一個空白的頁面動作對話方塊以定義新的應用程式規則。
- ***編輯*** - 開啟相同的頁面動作 對話方塊，並提供相關資料，以編輯現有的應用程式規則集。
- ***刪除*** - 從清單中移除所選應用程式。

您可以在***頁面動作***對話方塊中詳細定義各個應用程式的設定：



控制按鈕

該對話方塊的頂端有兩個可用的控制按鈕：

- ***返回至清單*** - 按此按鈕可顯示所有已定義應用程式規則的概觀。
- ***刪除此規則*** - 按此按鈕可清除目前顯示的應用程式規則。***請注意，此動作無法復原！***

應用程式基本資訊

在此區段填入應用程式的***名稱***，如有需要，還可以填入***描述*** *(對您所填資訊的簡短註解)*。在***路徑***欄位中，輸入應用程式 *(可執行檔)* 在磁碟上的完整路徑；或者您也可以在按一下「...」按鈕後，在樹狀結構中輕鬆找到該應用程式。

應用程式動作

在下拉式功能表中，您可以為應用程式選取 Firewall 規則，例如當應用程式嘗試透過網路進行通訊時，Firewall 該怎麼做：

- ***允許所有網路*** - 允許應用程式不受限制地透過所有已定義的網路和介面卡進

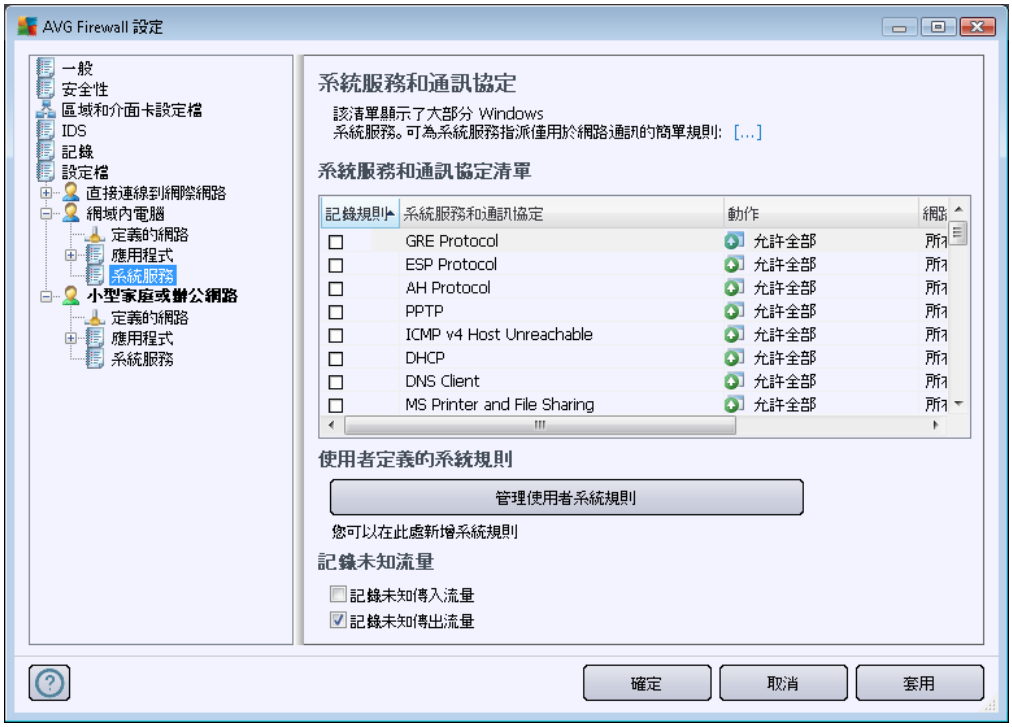
行通訊。

- ***允許安全網路*** - 僅允許應用程式透過定義為安全 *(可信任)*的網路通訊。
- ***封鎖*** - 自動禁止通訊 ;不允許應用程式連線到任何網路。
- ***詢問*** - 顯示一個對話方塊，讓您決定當下是要允許還是封鎖通訊嘗試。
- ***進階設定*** - 在對話方塊底端的***應用程式詳細規則***區段顯示更廣泛且更詳細的設定選項。這些規則將依據清單順序套用，因此您可以根據需要***上移***或***下移***清單中的規則，以設定其優先順序。當您按一下清單中某個規則之後，該規則的詳細資訊概觀就會出現在對話方塊底端。任何有藍色底線的值都可變更，只要在相應的設定方塊中按一下即可。如需刪除亮顯的規則，只要按一下***移除***即可。如需定義一條新的規則，請使用***新增***按鈕來開啟***變更規則詳細資訊***對話方塊，在此指定所有必要的詳細資訊。

11.6.4. 系統服務

「系統服務和通訊協定」對話方塊內的所有編輯作業都只能由經驗豐富的使用者進行！

系統服務和通訊協定對話方塊列出了可能需要透過網路進行通訊的 Windows 標準系統服務和通訊協定：



系統服務和通訊協定清單

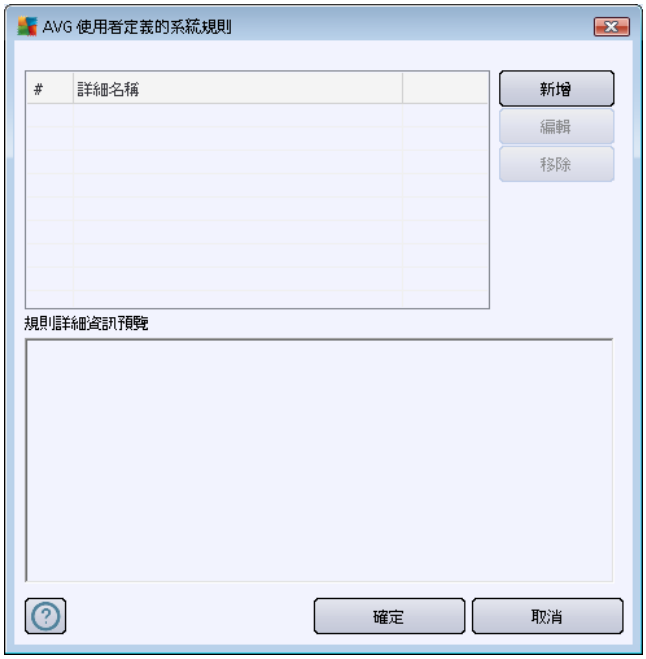
該圖表包含以下欄：

- ***記錄規則動作*** - 此方塊可讓您開啟將每次的規則套用動作記錄到記錄的功能。
- ***系統服務和通訊協定*** - 此欄會顯示各個系統服務的名稱。
- ***動作*** - 此欄會顯示所指派動作的圖示：
  - 允許所有網路的通訊
  - 只允許定義為 安全」的網路進行通訊
  - 封鎖通訊
- ***網路*** - 此欄指出套用系統規則的具體網路。

若要編輯清單中任何項目的設定 (*包括指派的動作*)，請用滑鼠右鍵按一下該項目，然後選取***編輯***。***不過，編輯系統規則應該僅能由進階使用者執行，並且強烈建議不要編輯系統規則！***

使用者定義的系統規則

若要開啓一個新對話方塊來定義您自己的系統服務規則 (*見下圖*)，請按一下***管理使用者系統規則***按鈕。***使用者定義的系統規則***對話方塊的上半部顯示目前正在編輯的系統規則所有詳細資訊的概覽，下半部則顯示所選的詳細資訊。使用者定義的規則詳細資訊可以透過相應的按鈕來編輯、新增或者刪除 ;製造商定義的規則詳細資訊僅可編輯：



請注意，規則詳細資訊設定是進階功能，主要是給需要全權控制 Firewall 組態的網路管理員使用。如果您對通訊協定的類型、網路連接埠號、IP 位址定義等不太熟悉，請不要修改這些設定。如果您真的需要變更組態，請參考各對話方塊中的說明以瞭解

詳細資訊。

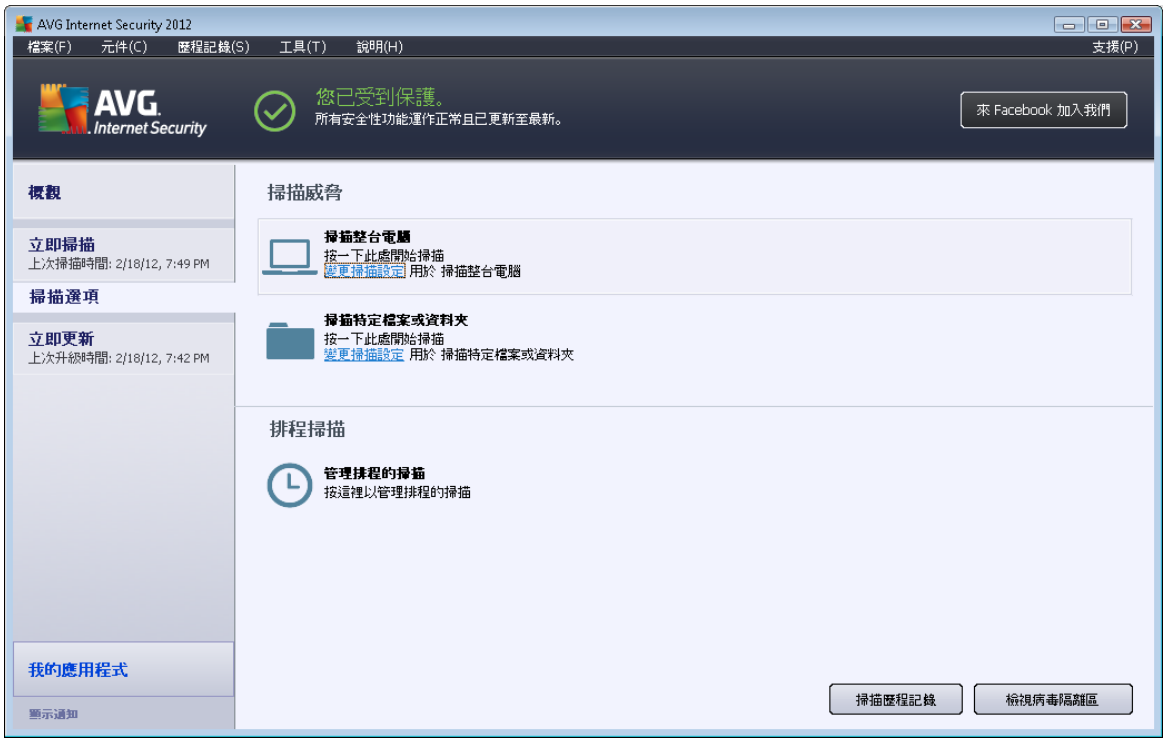
記錄不明流量

- ***記錄不明傳入流量*** *(預設為關閉)* –核取此方塊可在記錄中記錄每個企圖從外部連線到您的電腦的不明嘗試。
- ***記錄不明傳出流量*** *(預設為開啟)* –核取此方塊可在記錄中記錄每個企圖從您的電腦連線到外部位置的不明嘗試。

12. AVG 掃描

預設情況下，**AVG Internet Security 2012** 並不會執行任何掃描，因為在第一次掃描之後您應該會受到 **AVG Internet Security 2012** 常駐元件的全面保護，這是即時防護，完全不會讓任何惡意程式碼進入您的電腦。您當然也可以排程掃描定期執行，或是隨時根據需要手動啟動掃描。

12.1. 掃描介面



AVG 掃描介面可透過***掃描選項***快速連結進行存取。按一下此連結可切換到***掃描威脅***對話方塊。在此對話方塊中，您可以找到下列內容：

- 預定義掃描的概觀 - 軟體廠商定義了三種掃描，可按需或按排程立即使用：
  - 完整電腦掃描
  - 掃描特定檔案或資料夾
- 排程掃描部分 - 您可以在這裡視需要定義新測試和建立新排程。

控制按鈕

測試介面中可用的控制按鈕如下：

- ***掃描歷程記錄*** - 顯示掃描結果概觀對話方塊，其中包含掃描的整個歷程記錄

- ***檢視病毒隔離區*** - 可開啟一個內含病毒隔離區 (用來隔離偵測到之感染檔案的區域) 的新視窗

12.2. 預定義的掃描

AVG Internet Security 2012 的主要特色之一就是按需掃描。按需測試的目的是為了在懷疑發生了病毒感染時，對電腦的各個部分進行掃描。即使您認為電腦沒有感染病毒，我們還是強烈建議定期執行此類測試。

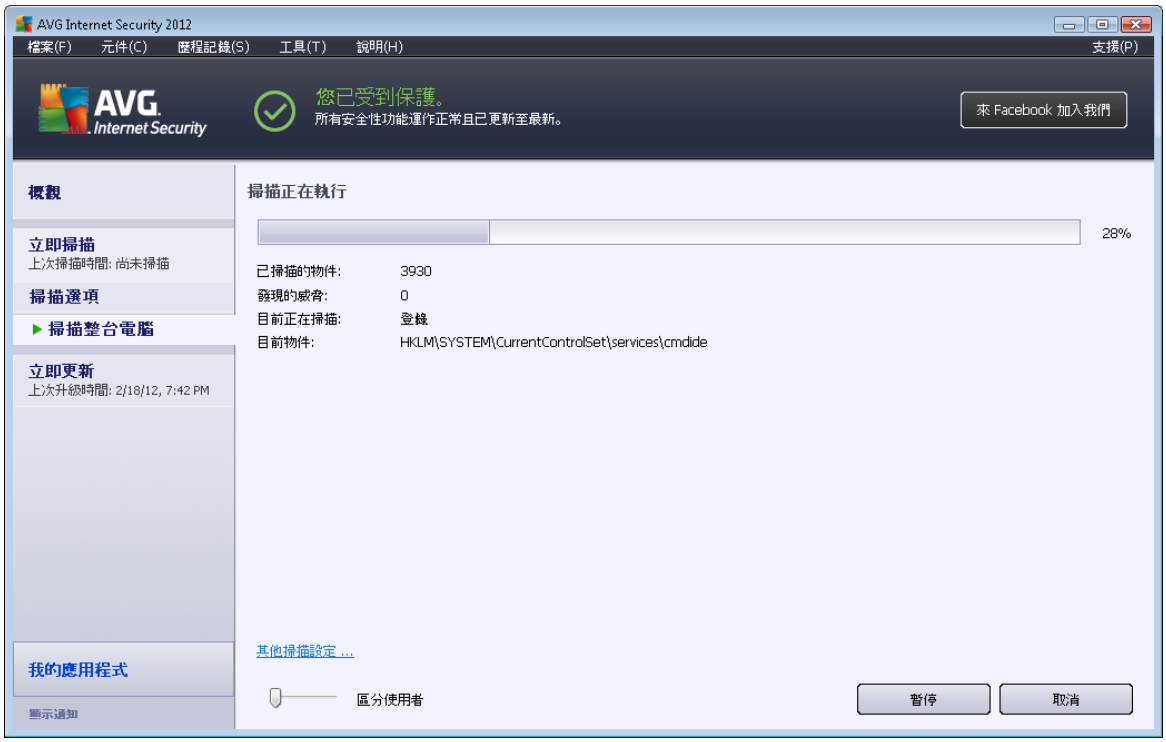
在 **AVG Internet Security 2012** 中，您將看到以下軟體廠商預先定義的掃描類型：

12.2.1. 完整電腦掃描

掃描整台電腦 - 掃描您的整台電腦，檢查是否有可能的感染和/或潛在的垃圾程式。這項測試會掃描電腦的所有硬碟，偵測並修復發現的所有病毒，或將偵測到的病毒感染移至病毒隔離區。掃描整台電腦應排程為每週至少在工作站上執行一次。

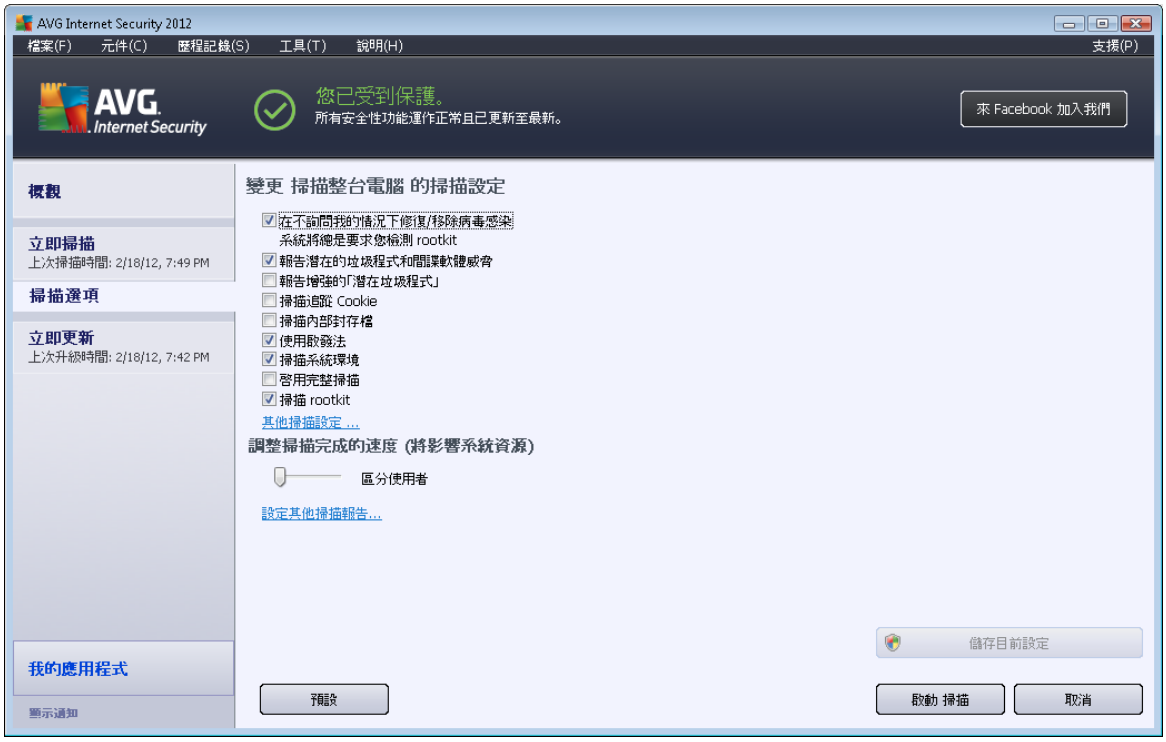
掃描啟動

掃描整台電腦可直接從掃描介面啟動，只要按一下掃描的圖示就可以了。這種掃描無需設定進一步的特定設定，掃描會在***掃描正在執行***對話方塊***中立即啟動*** (*請參閱螢幕擷取畫面*)。必要時，可暫時中斷 (***暫停***) 或取消 (***停止***) 掃描。



掃描組態編輯

您可以選擇編輯***掃描整台電腦***預先定義的預設設定。按一下***變更掃描設定***連結可前往***變更掃描整台電腦的掃描設定***對話方塊 *(可透過掃描整台電腦的 「變更掃描設定」連結從掃描介面存取)*。***建議保留預設設定，除非您確實需要變更！***



- ***掃描參數*** - 您可以在掃描參數清單中視需要開啟/關閉特定參數：

    - ***在不詢問我的情況下修復/移除病毒感染*** (預設為開啟) - 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至病毒隔離區。

    - ***報告潛在的垃圾程式和間諜軟體威脅*** (*預設為開啟*) - 核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別 :雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。

    - ***報告增強的潛在不受歡迎程式集*** (*預設為關閉*) - 標記此選項來偵測延伸的間諜軟體套件 :這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

    - ***掃描追蹤 Cookie***(*預設為關閉*) – Anti-Spyware 元件的此一參數定義在掃描期間應偵測 cookie；(*HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容*)。

    - ***掃描封存內部*** (*預設為關閉*) - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在封存內，如 ZIP、RAR...

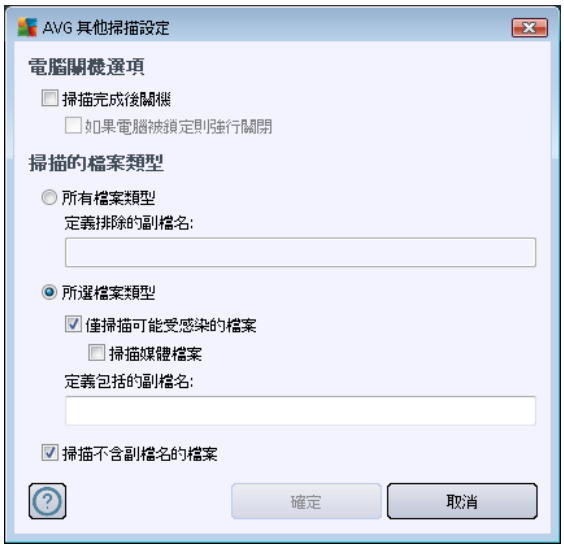
- ***使用啟發法*** (*預設為開啟*) - 啟發法分析 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 將成為掃描過程中用於偵測病毒的方法之一。

- ***掃描系統環境*** (*預設為開啟*) – 掃描時還會檢查您電腦的系統區域。

- ***啟用完整掃描*** (*預設為關閉*) - 在特定情況下 (*懷疑您的電腦受到感染*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***掃描 rootkits*** (預設為開啟) - Anti-Rootkit 掃描可搜尋您電腦中可能的 rootkits，即可覆蓋您電腦中惡意軟體活動的程式和技術。偵測到 rootkit 不一定表示您的電腦已受到感染。在某些情況下，特定驅動程式或正常應用程式的某些部分都可能被誤偵測為 rootkit。

- ***其他掃描設定*** - 此連結會開啟新的***其他掃描設定***對話方塊，讓您指定下列參數：



- ***電腦關機選項*** - 決定在執行完掃描程序後電腦是否應自動關機。確認此選項後 (***掃描完成後關機***)，將啟動一個新選項，可用來設定電腦即使在鎖定狀態下也能關機 (***強行關閉鎖定的電腦***)。

- ***掃描的檔案類型*** - 之後您應該進一步決定是否要掃描：

  - ***所有檔案類型*** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名)，可定義掃描的例外；

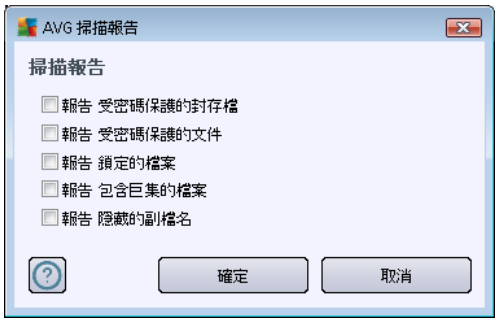
  - ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔*)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

  - 或者，您也可以決定***掃描不含副檔名的檔案*** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可

疑，始終都應該掃描。

- ***調整完成掃描的速度*** - 您可以使用滑桿來變更掃描程序的優先順序。預設情況下，該選項值會設為*區分使用者*層級的自動資源使用量。此外，您也可以用較慢的速度執行掃描程序，也就是讓系統資源的負載降至最低 (*這在您必須使用電腦工作，而不在意掃描進行時間多長的時候十分有用*)，或是提高速度，但會增加系統資源的需求量 (*例如電腦暫時無人使用的時候*)。

- ***設定其他掃描報告*** - 此連結會開啟新的***掃描報告***對話方塊，您可以在這裡選取應該報告哪些類型的結果：



警告：*這些掃描設定與新定義的掃描參數相同 - 如 AVG 掃描/掃描排程/如何掃描一章中所述。您若決定變更**掃描整台電腦**的預設組態，接下來您就可將新的設定儲存為預設組態，以供未來每次掃描整台電腦時使用。*

12.2.2. 掃描特定檔案或資料夾

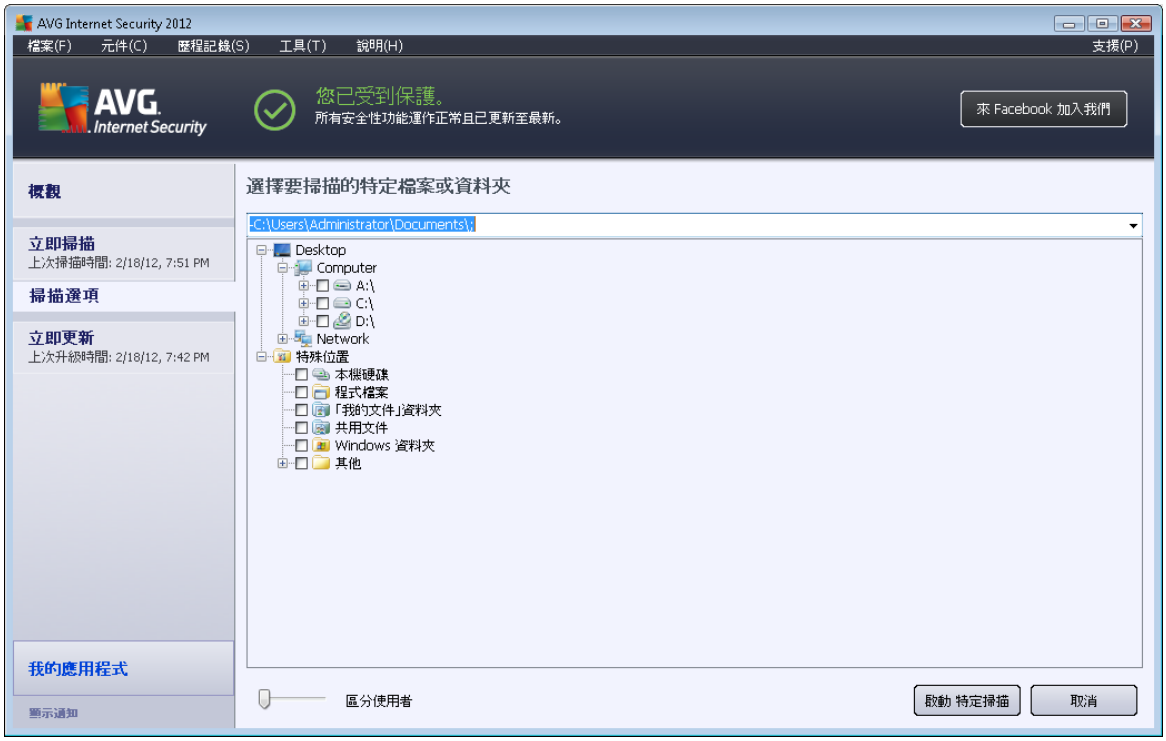
掃描特定檔案或資料夾 - 只掃描您已選取要進行掃描的電腦區域 (*所選資料夾、硬碟、磁碟片、CD* 等)。如果偵測到病毒並進行處置，掃描進度會與整台電腦掃描相同：發現的所有病毒都會被修復，或移至病毒隔離區。特定檔案或資料夾掃描可供您依照自己的需求，設定自己的測試及其排程。

掃描啟動

掃描特定檔案或資料夾可以從掃描介面按一下掃描圖示直接啟動。新的***選取要掃描的特定檔案或資料夾***對話方塊隨即開啟。請在電腦的樹狀目錄結構中選取您想要掃描的資料夾。通往各選取資料夾的路徑會自動生成，並出現在此對話方塊上半部的文字方塊中。

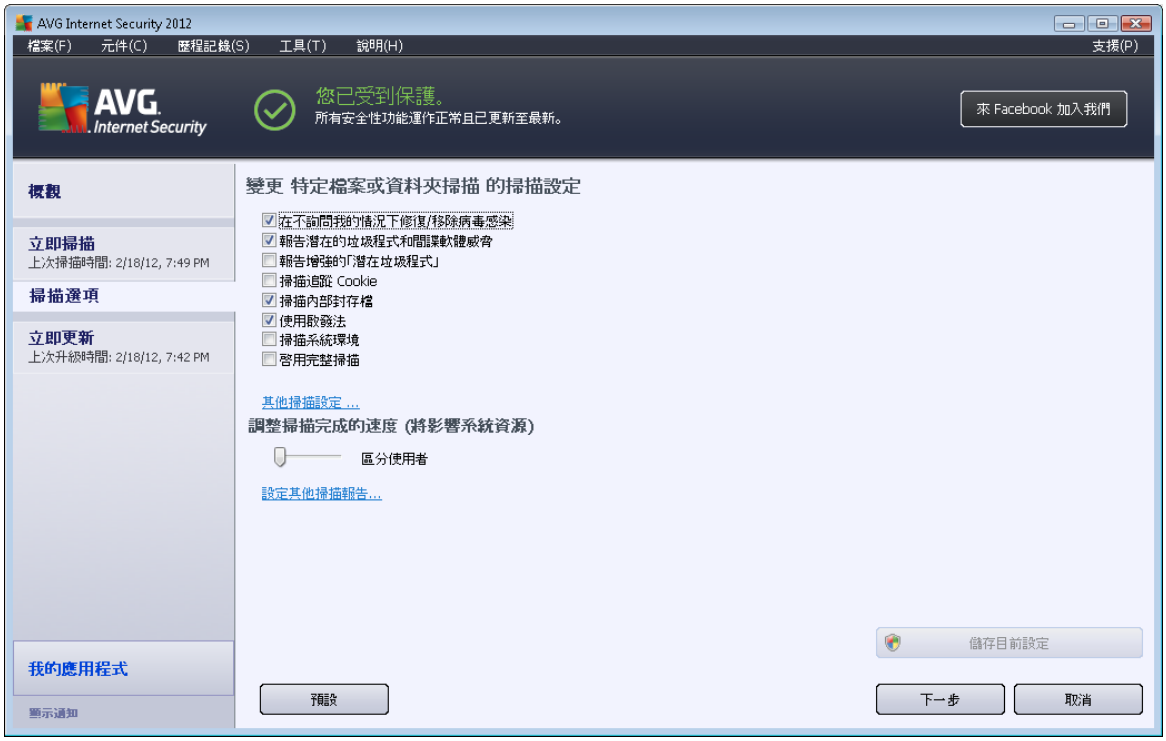
您也可以僅掃描特定資料夾，而不掃描其子資料夾。如果要這麼做，請在自動生成的路徑前方加上一個減號 "-" (***請參閱螢幕擷取畫面***)。若要將整個資料夾排除在掃描範圍外，請使用 "!"參數。

最後，若要啟動掃描，請按一下***開始掃描***按鈕；掃描程序本身基本上與掃描整台電腦相同。



掃描組態編輯

您可以選擇編輯預先定義的預設設定 ***:掃描特定檔案或資料夾***。請按下***變更掃描設定***連結，進入***變更掃描特定檔案或資料夾的掃描設定***對話方塊。***建議保留預設設定，除非您確實需要變更！***



- ***掃描參數*** - 您可以在掃描參數清單中視需要開啟/關閉特定參數：

  - ***在不詢問我的情況下修復/移除病毒感染*** (*預設為開啟*) - 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至病毒隔離區。

  - ***報告潛在的垃圾程式和間諜軟體威脅*** (*預設為開啟*) - 核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別 :雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。

  - ***報告增強的潛在垃圾程式*** (*預設為關閉*) - 標示此選項可偵測延伸的間諜軟體套件 :這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

  - ***掃描追蹤 Cookie*** (*預設為關閉*) - Anti-Spyware 元件的此一參數定義在掃描期間應偵測 cookie ;(*HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容*)。

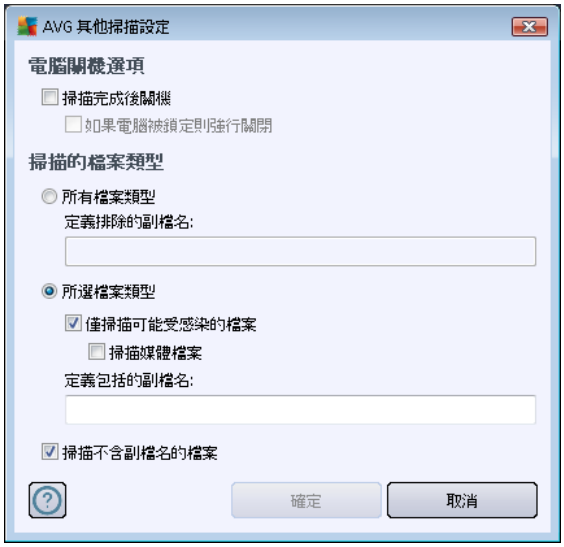
  - ***掃描內部封存檔*** (*預設為開啟*) - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在某種封存檔內，如 ZIP、RAR...

  - ***使用啟發法*** (*預設為開啟*) - 啟發法分析 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 將成為掃描過程中用於偵測病毒的方法之一。

  - ***掃描系統環境*** (*預設為關閉*) - 掃描時還會檢查您電腦的系統區域。

- ***啟用完整掃描*** (*預設為關閉*) - 在特定情況下 (*懷疑您的電腦受到感染*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***其他掃描設定*** - 此連結會開啟新的***其他掃描設定***對話方塊，讓您指定下列參數：



  - ***電腦關機選項*** - 決定在執行完掃描程序後電腦是否應自動關機。確認此選項後 (***掃描完成後關機***)，將啟動一個新選項，可用來設定電腦即使在鎖定狀態下也能關機 (***強行關閉鎖定的電腦***)。

  - ***定義要掃描的檔案類型*** - 然後您應該決定是否要掃描：

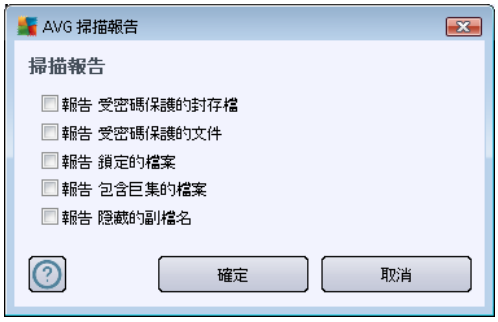
    - ***所有檔案類型*** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名)，可定義掃描例外；

    - ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔*)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

    - 或者，您也可以決定***掃描不含副檔名的檔案*** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

- ***掃描程序優先順序*** - 您可以使用滑桿來變更掃描程序優先順序。預設情況下，該選項值會設為*區分使用者*層級的自動資源使用量。此外，您也可以用較慢的速度執行掃描程序，也就是讓系統資源的負載降至最低 (*這在您必須使用電腦工作，而不在意掃描進行時間多長的時候十分有用*)，或是提高速度，但會增加系統資源的需求量 (*例如電腦暫時無人使用的時候*)。

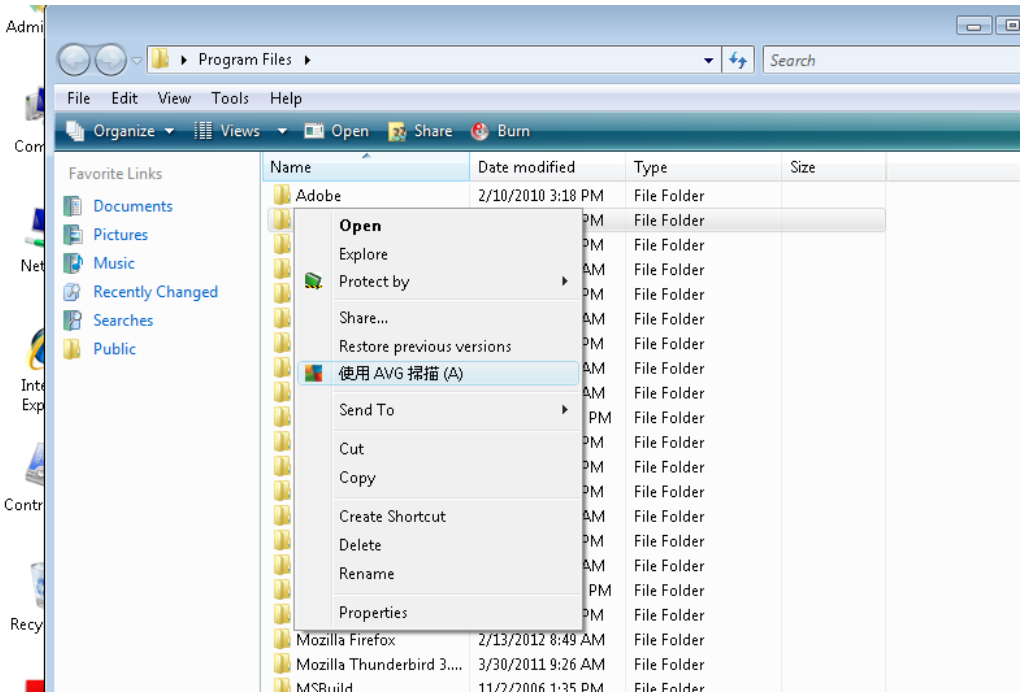
- ***設定其他掃描報告*** - 此連結會開啟新的***掃描報告***對話方塊，您可以在這裡選取應報告哪些類型的結果：



***警告：**這些掃描設定與新定義的掃描參數相同 - 如 AVG 掃描/掃描排程/如何掃描章節中所述。您若決定變更**掃描特定檔案或資料夾**的預設組態，您隨後可將新的設定儲存為預設組態，以供未來每次掃描特定檔案或資料夾時使用。另外，該組態將會成為您所有新排程的掃描的範本 (所有自訂的掃描都以所選檔案或資料夾的目前掃描組態為依據)。*

12.3. 在 Windows 檔案總管中掃描

除了為整台電腦或其中選定區域而啟動的預先定義掃描之外，**AVG Internet Security 2012** 還提供直接在 Windows 檔案總管環境中快速掃描特定物件的選項。如果想要開啟不明檔案，但無法確定其內容，您可以按您的需要進行檢查。請遵循下列步驟：



- 在 Windows 檔案總管中，反白您想要檢查的檔案 *(或資料夾)*
- 在物件上按一下滑鼠右鍵，開啟內容功能表
- 選取***使用 AVG 掃描***選項，讓 AVG 掃描檔案**AVG Internet Security 2012**

12.4. 命令列掃描

在 **AVG Internet Security 2012** 中，您可以選擇從命令列執行掃描。舉例來說，您可以在伺服器上使用此選項，或是在建立批次指令碼以便在電腦開機後自動啟動時使用。從命令列，您可以使用 AVG 圖形使用者介面提供的大部分參數來啟動掃描。

若要從命令列啟動 AVG 掃描，請在安裝 AVG 的資料夾中執行下列命令：

- ***avgscanx*** (適用於 32 位元作業系統)
- ***avgscana*** (適用於 64 位元作業系統)

命令語法

命令語法如下：

- ***avgscanx /參數*** ... 例如，***avgscanx /comp***，可掃描整台電腦
- ***avgscanx /參數 /參數*** .. 若有多個參數，這些參數必須排成一列，以空格和斜線字元分隔
- 如果參數需要提供特定值 (例如，***/scan*** 參數需要有關要掃描的電腦選定區域的資訊，而且您必須提供選定區域的確切路徑)，應以分號分隔這些值，例如 ***:avgscanx /scan=C:\;D:***

掃描參數

若要顯示可用參數的完整概觀，請鍵入相應的命令加上參數 /?或 /HELP (例如，***avgscanx /?***)。唯一的強制參數是 /SCAN，用來指定要掃描的電腦區域。有關選項的詳細說明，請參閱命令列參數概觀。

若要執行掃描，請按一下 ***Enter*** 鍵。在掃描期間，您可以停止掃描程序，方法是按 ***Ctrl+C*** 或 ***Ctrl+Pause*** 組合鍵。

從圖形介面啟動的 CMD 掃描

在 Windows 安全模式下執行電腦時，也可以從圖形使用者介面啟動命令列掃描。掃描本身將從命令列啟動，***命令列編輯器***對話方塊只允許您在適當的圖形介面中指定大部分的掃描參數。

由於此對話方塊只能在 Windows 安全模式下存取，如需此對話方塊的詳細說明，請參閱可直接從對話方塊開啟的說明檔案。

12.4.1. CMD 掃描參數

以下是命令列掃描地所有可用參數的清單：

- ***/SCAN*** 掃描特定檔案或資料夾 */SCAN=路徑;路徑 (例如，/SCAN=C:\;D:\)*
- ***/COMP*** 掃描整台電腦
- ***/HEUR*** 使用啟發法分析
- ***/EXCLUDE*** 從掃描中排除路徑或檔案
- ***/@*** 命令檔案/檔案名稱/
- ***/EXT*** 掃描這些副檔名/例如 EXT=EXE,DLL/
- ***/NOEXT*** 不要掃描這些副檔名/例如 NOEXT=JPG/
- ***/ARC*** 掃描封存檔
- ***/CLEAN*** 自動清除
- ***/TRASH*** 將受感染的檔案移至病毒隔離區
- ***/QT*** 快速測試
- ***/LOG*** 生成掃描結果檔案
- ***/MACROW*** 報告巨集
- ***/PWDW*** 報告受密碼保護的檔案
- ***/ARCBOMBSW*** 報告封存限制 *重複壓縮的封存）*
- ***/IGNLOCKED*** 忽略鎖定的檔案
- ***/REPORT*** 報告給檔案/檔案名稱/
- ***/REPAPPEND*** 附加到報告檔案
- ***/REPOK*** 將未受感染的檔案報告為正常
- ***/NOBREAK*** 不允許透過 CTRL-BREAK 中止
- ***/BOOT*** 啟用 MBR/BOOT 檢查
- ***/PROC*** 掃描作用中的程序
- ***/PUP*** 報告「潛在垃圾程式」
- ***/PUPEXT*** 報告增強的「潛在垃圾程式」

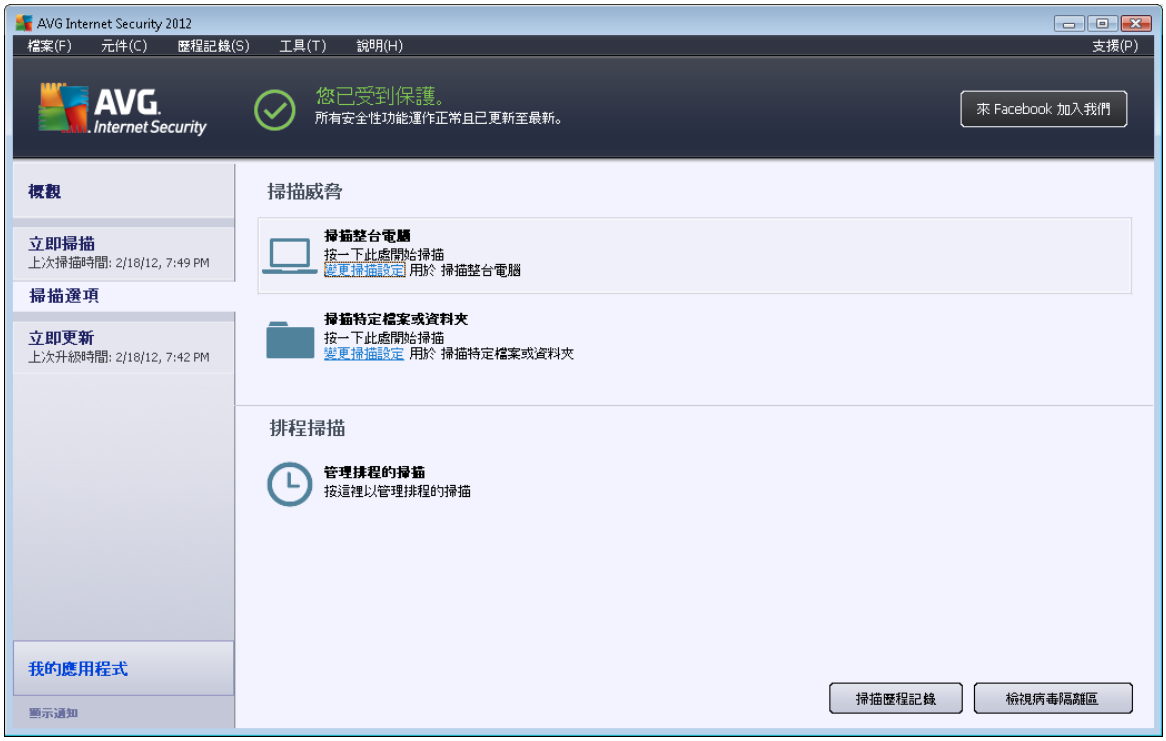
- ***/REG*** 掃描登錄檔
- ***/COO*** 掃描 Cookie
- ***/?*** 顯示此主題的說明
- ***/HELP*** 顯示此主題的說明
- ***/PRIORITY*** 設定掃描優先順序/低、自動、高/ *(請參閱進階設定/掃描)*
- ***/SHUTDOWN*** 掃描完成後關機
- ***/FORCESHUTDOWN*** 掃描完成後強行關閉電腦
- ***/ADS*** *掃描替代資料流 (僅限 NTFS)*
- ***/HIDDEN*** 報告具有隱藏副檔名的檔案
- ***/INFECTABLEONLY*** 僅掃描具有可感染副檔名的檔案
- ***/THOROUGHSCAN*** 掃描期間啟用
- ***/CLOUDCHECK*** 檢查誤報
- ***/ARCBOMBSW*** 報告重新壓縮的封存檔案

12.5. 掃描排程

您可以使用 **AVG Internet Security 2012** 的按需執行掃描功能 (例如在您懷疑電腦受病毒感染時)，或是依據排程的計劃執行。我們強烈建議您按照排程執行掃描：這樣可以確保您的電腦不會有任何受到感染的機會，而且您也無需操心是否要啟動掃描，以及何時啟動掃描。

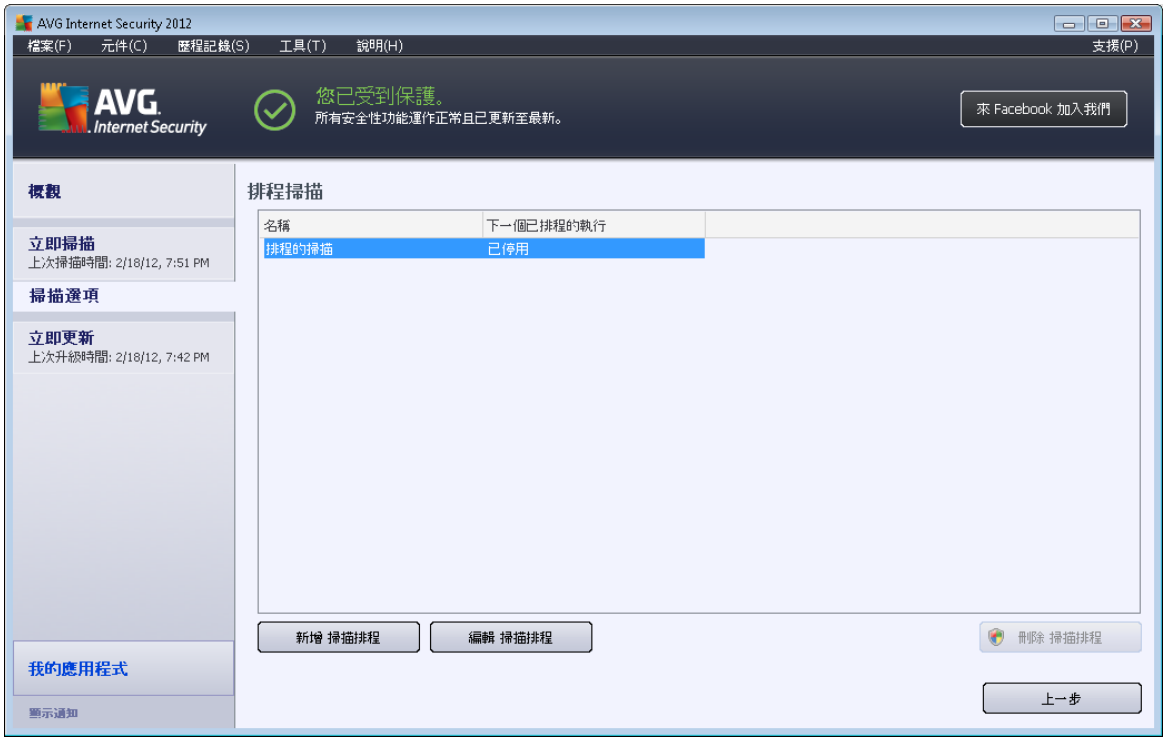
您應該定期啟動掃描整台電腦，至少每週一次。但是如果可能的話，請依照掃描排程預設組態中的設定，每天啟動一次整台電腦的掃描。如果電腦一直開啟，您可以將掃描排定在工作時段以外的時間進行。如果電腦有時會關機，而錯過了掃描工作的時間，則掃描會在電腦啟動的時候執行。

如需建立新的掃描排程，請參閱 AVG 掃描介面，並尋找下方稱為***排程掃描***的區段：



排程掃描

按一下***排程掃描***部分內的圖形圖示會開啟一個新的***排程掃描***對話方塊，您可以在這裡找到所有目前已排程的掃描清單：

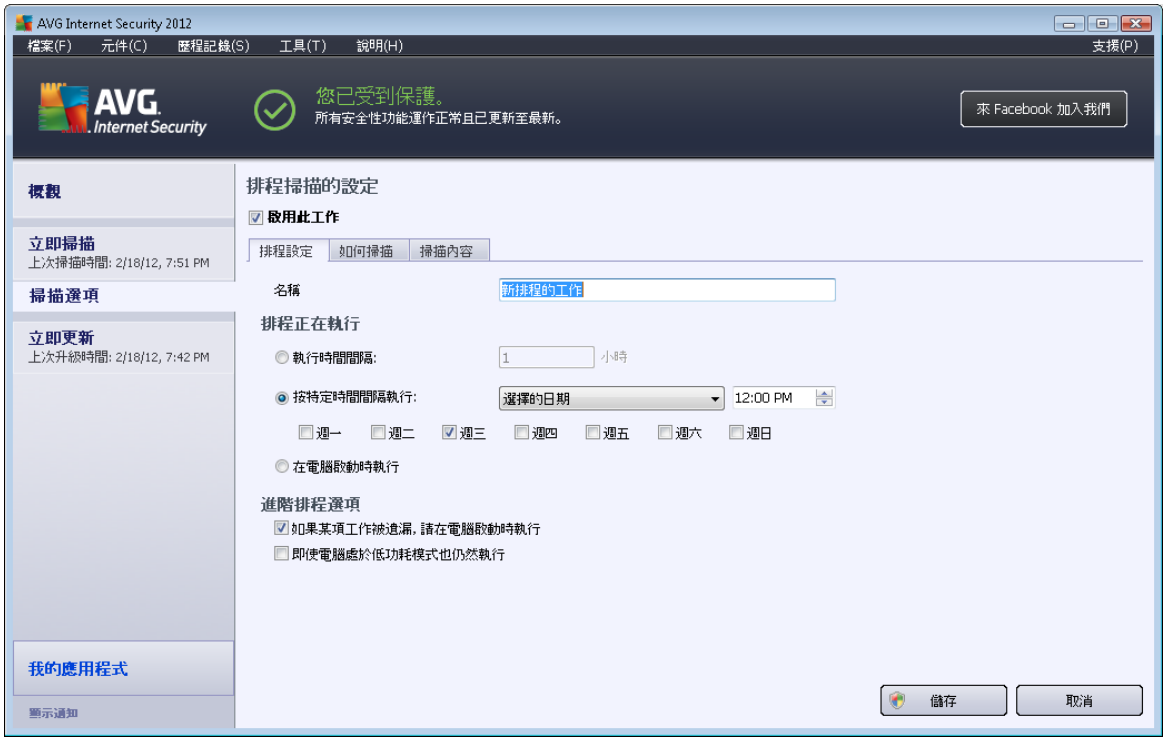


您可以使用以下控制按鈕編輯/新增掃描：

- ***新增掃描排程*** - 此按鈕可以開啟***排程掃描的設定***對話方塊、排程設定標籤。您可以在此對話方塊中指定新定義測試的參數。
- ***編輯掃描排程*** - 此按鈕只有在您之前已從排程的測試清單中選取了現有的測試時才能使用。如果按鈕顯示為處於使用中，您可以按一下按鈕切換至***排程掃描的設定***對話方塊、排程設定標籤。所選測試的參數已經在此指定，而且可供編輯。
- ***刪除掃描排程*** - 此按鈕也在您之前已從排程的測試清單中選取 0了現有的測試時才能使用。接下來您就可以按下控制按鈕，從清單中刪除此測試。但是您只能刪除自己的測試，預設設定中預先定義的***掃描整台電腦排程***永遠無法刪除。
- ***上一步*** - 返回至 AVG 掃描介面

12.5.1. 排程設定

如果您希望排程新測試並定期啟動，請進入***排程測試的設定***對話方塊 (*按一下* ***排程掃描***對話方塊內的***新增掃描排程***按鈕)。此對話方塊分為三個標籤 :***排程設定***(*請參閱下圖 ;會自動將您重新導向到此預設標籤*)、如何掃描以及掃描內容。



在***排程設定***標籤中，您可以首先核取/取消核取***啟用此工作***項目，即可暫時停用排程的測試，然後在有需要時再將其開啟。

接著，為您要建立和排程的掃描指定一個名稱。在***名稱***項目旁的文字欄位中輸入名稱。請儘量為掃描使用簡短、恰當的描述性名稱，方便日後區分此掃描與其他掃描。

例如：*將掃描命名為「新掃描」或「我的掃描」並不合適，因為這些名稱並未指明掃描真正檢查的內容。反過來說，如「系統區域掃描」則是恰當的描述性名稱示例。此外，也沒有必要在掃描的名稱中指明是掃描整台電腦還是只掃描所選檔案或資料夾 - 您的掃描始終是特定版本的[掃描所選檔案或資料夾](#)。*

在此對話方塊中，您可以進一步定義掃描的以下參數：

- ***排程執行時間*** - 指定啟動新排程的掃描的時間間隔。時間安排有以下幾種定義方式：定義一段時間後再次啟動掃描 (***每...執行一次***)，定義確切的日期和時間 (***在特定時間執行...***)，或者定義掃描啟動應關聯的事件 (***依據電腦啟動執行的動作***)。
- ***進階排程選項*** - 此區段允許您定義 (如果電腦是處於低功耗模式或完全關閉模式)，在何種條件下應啟動/不應啟動掃描。

「排程掃描的設定」對話方塊的控制按鈕

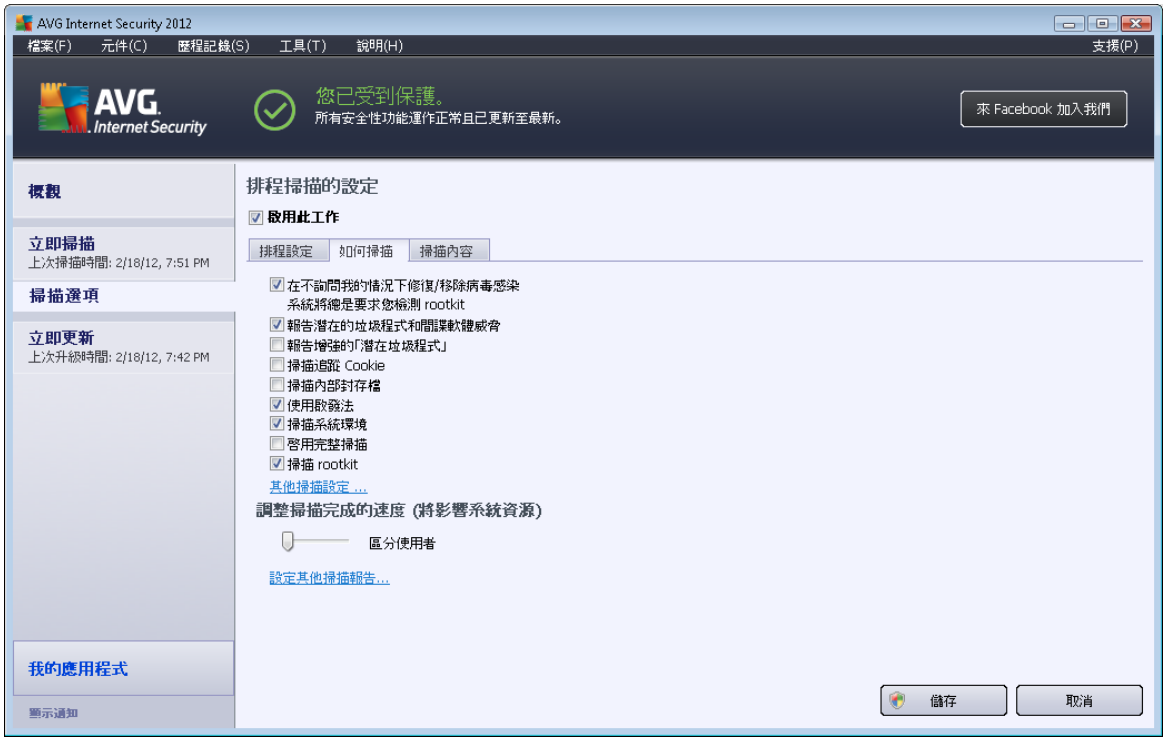
排程掃描的設定對話方塊的所有三個標籤上 (*排程設定*、[*如何掃描*](#)*以及*[*掃描內容*](#)) 都有兩個可用的控制按鈕，並且無論您正位於哪個標籤，它們的作用都是一樣的：

- ***儲存*** - 可儲存您在此標籤或此對話方塊中任何其他標籤上所做的所有變更，然後

切換回 AVG 掃描介面預設對話方塊。因此，如果您想要設定所有標籤上的測試參數，只需在您指定完所有需求後按下該按鈕即可將其儲存。

- ***取消*** - 取消您在此標籤或此對話方塊中任何其他標籤上所做的任何變更，然後切換回 AVG 掃描介面預設對話方塊。

12.5.2. 如何掃描



在***如何掃描***標籤上，您將看到一份可選擇開啟/關閉的掃描參數清單。預設情況下，大多數參數都已開啟，並將在掃描期間套用其功能。除非您確實需要變更這些設定，否則我們建議您保留預先定義的組態：

- ***在不詢問我的情況下修復/移除病毒*** (*預設為開啟*)：如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復)。若無法自動修復受感染的檔案，或是您決定關閉此選項，則會在偵測到病毒時收到相關通知並且必須決定要如何處理偵測到的感染檔案。建議動作是將受感染的檔案移除到病毒隔離區。

- ***報告潛在的垃圾程式和間諜軟體威脅*** (*預設為開啟*)：核取此方塊可啟動 Anti-Spyware 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。

- ***報告增強的潛在垃圾程式*** (*預設為關閉*)：標記此選項以偵測延伸的間諜軟體套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- ***掃描追蹤 Cookie*** (*預設為關閉*)：Anti-Spyware 元件的此一參數定義在掃描期間應偵

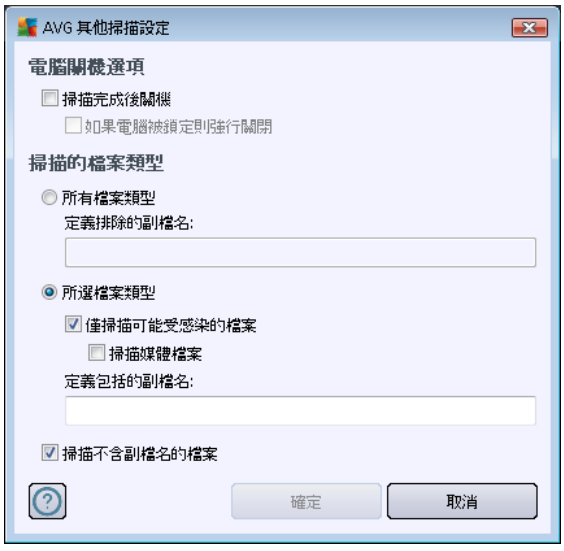
測 cookie (*HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容*)。

- ***掃描內部封存檔*** (*預設為關閉*) :此參數定義掃描應檢查所有檔案，即使這些檔案已被封裝在某種封存內，如 ZIP、RAR...
- ***使用啟發法*** (*預設為開啟*) :啟發法分析 (*在虛擬電腦環境中動態模擬掃描物件的指令*) 將成為掃描過程中用於偵測病毒的方法之一。
- ***掃描系統環境*** (*預設為開啟*) :掃描時還會檢查您電腦的系統區域。
- ***啟用完整掃描*** (*預設為關閉*) - 在特定情況下 (*懷疑您的電腦受到感染時*)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

- ***掃描 rootkits*** (*預設為開啟*): Anti-Rootkit 掃描可搜尋電腦內的 rootkit，即您的電腦中可覆蓋惡意軟體活動的程式和技術。偵測到 rootkit 不一定表示您的電腦已受到感染。在某些情況下，特定驅動程式或正常應用程式的某些部分都可能被誤偵測為 rootkit。

然後，您可以按如下方式變更掃描組態：

- ***其他掃描設定*** - 此連結會開啟新的***其他掃描設定***對話方塊，讓您指定下列參數：



o ***電腦關機選項*** - 決定在執行完掃描程序後電腦是否應自動關機。確認此選項後 (***掃描完成後關機***)，將啟動一個新選項，可用來設定電腦即使在鎖定狀態下也能關機 (***強行關閉鎖定的電腦***)。

o ***掃描的檔案類型*** - 之後您應該進一步決定是否要掃描：

➢ ***所有檔案類型*** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名)，可定義掃描的例外；

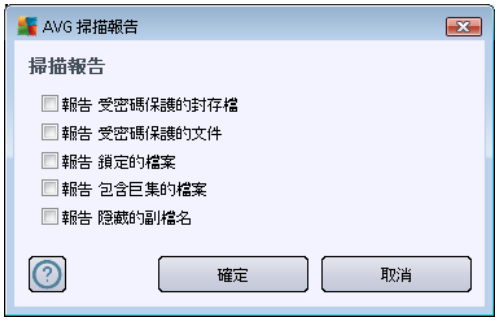
➢ ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描*

不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

- 或者，您也可以決定***掃描不含副檔名的檔案*** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

- ***調整掃描完成的速度*** - 您可以使用滑桿來變更掃描程序的優先順序。預設情況下，該選項值會設為*區分使用者*層級的自動資源使用量。此外，您也可以用較慢的速度執行掃描程序，也就是讓系統資源的負載降至最低 (*這在您必須使用電腦工作，而不在意掃描進行時間多長的時候十分有用*)，或是提高速度，但會增加系統資源的需求量 (*例如電腦暫時無人使用的時候*)。

- ***設定其他掃描報告*** - 此連結會開啟新的***掃描報告***對話方塊，您可以在這裡選取應該報告哪些類型的結果：



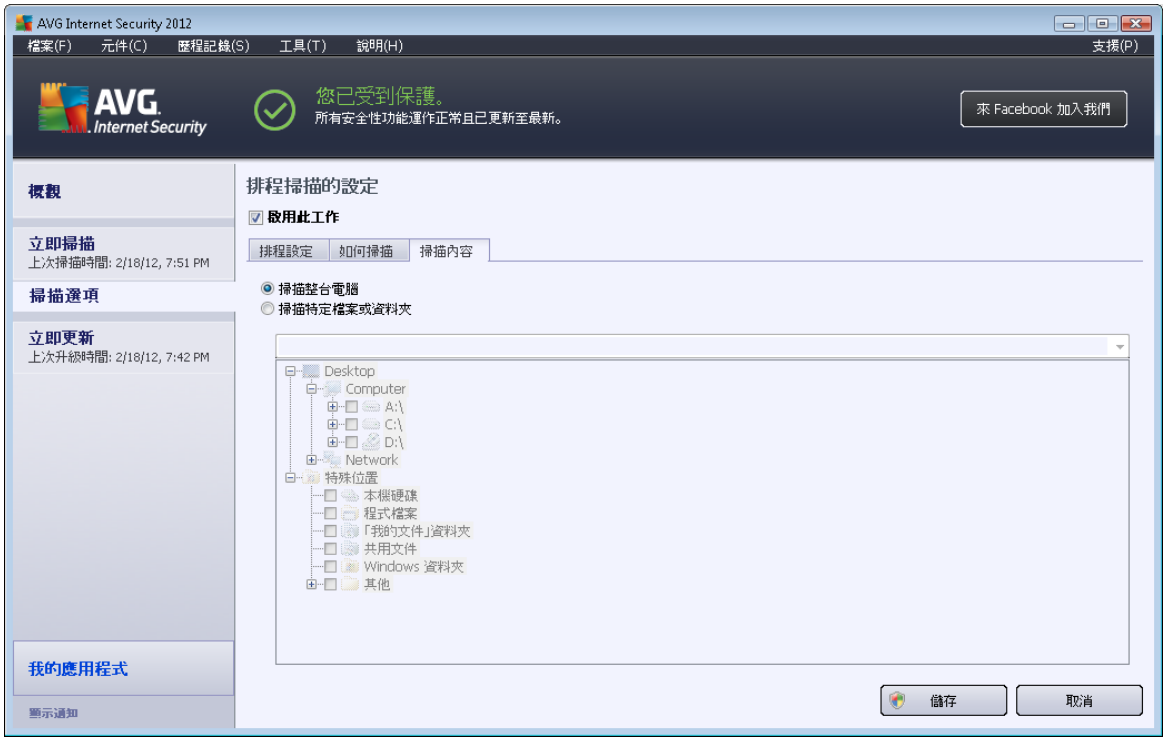
控制按鈕

排程掃描的設定對話方塊的所有三個標籤上 (*排程設定*、*如何掃描*和*掃描內容*) 都有兩個控制按鈕可用，並且無論您正位於哪個標籤，它們的作用都是一樣的：

- ***儲存*** - 可儲存您在此標籤或此對話方塊中任何其他標籤上所做的所有變更，然後切換回 AVG 掃描介面預設對話方塊。因此，如果您想要設定所有標籤上的測試參數，只需在您指定完所有需求後按下該按鈕即可將其儲存。

- ***取消*** - 取消您在此標籤或此對話方塊中任何其他標籤上所做的任何變更，然後切換回 AVG 掃描介面預設對話方塊。

12.5.3. 掃描內容



在***掃描內容***標籤上，您可以定義是要排程掃描整台電腦，還是掃描特定檔案或資料夾。

如果您選擇掃描特定的檔案或資料夾，此對話方塊的底端會顯示已啟動的樹狀目錄結構，您可在此指定想要掃描的資料夾 (*按一下加號節點可以展開項目，直到您找到想掃描的資料夾為止*)。您可以透過核取相應的方塊選取多個資料夾。所選資料夾將顯示在對話方塊頂端的文字欄位中，下拉式功能表將保留您選取的掃描歷程記錄供日後使用。另外，您還可以手動輸入資料夾的完整路徑 (*如果輸入多個路徑，則必須以分號分隔，不要有額外的空格*)。

在此樹狀目錄結構中，您還可以看到一個叫***特殊位置***的分支。以下列出可以透過勾選相應核取方塊來掃描的位置：

- ***本機硬碟*** - 您電腦中的所有硬碟
- ***程式檔案***
    - C:\Program Files\
    - *在 64 位元版本中* C:\Program Files (x86)
- ***我的文件」資料夾***
    - *若是 Win XP* :C:\Documents and Settings\Default User\My Documents\

- *若是 Windows Vista/7*： C:\Users\user\Documents\

- ***共用文件***
  - *若是 Win XP*: C:\Documents and Settings\All Users\Documents\
  - *若是 Windows Vista/7*: C:\Users\Public\Documents\
- ***Windows 資料夾*** - C:\Windows\
- ***其他***
  - 系統磁碟機 - 安裝了作業系統的硬碟機 (通常是 C:)
  - *系統資料夾* - C:\Windows\System32\
  - *暫存檔案資料夾* - C:\Documents and Settings\User\Local\ (*Windows XP*) ;或 C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *暫存網際網路檔案* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) ;或 C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

控制按鈕

排程掃描設定對話方塊的所有三個標籤上 *(排程設定*、*如何掃描和掃描內容)* 同樣都有提供兩個控制按鈕：

- ***儲存*** - 可儲存您在此標籤或此對話方塊中任何其他標籤上所做的所有變更，然後切換回 AVG 掃描介面預設對話方塊。因此，如果您想要設定所有標籤上的測試參數，只需在您指定完所有需求後按下該按鈕即可將其儲存。
- ***取消*** - 取消您在此標籤或此對話方塊中任何其他標籤上所做的任何變更，然後切換回 AVG 掃描介面預設對話方塊。

12.6. 掃描結果概觀

掃描結果概觀對話方塊可以在 AVG 掃描介面中透過***掃描歷程記錄***按鈕存取。此對話方塊提供所有之前啟動的掃描及其掃描結果資訊的清單：

- ***名稱*** - 指定的掃描名稱，可能是預定義的掃描之一的名稱，或是您為自己排程的掃描定下的名稱。每一個名稱都包含代表下列掃描結果的圖示：

  - 綠色圖示表示掃描過程中並未偵測到病毒感染

  - 藍色圖示告訴您掃描過程中偵測到病毒感染，但是受感染的物件已經被自動移除

  - 紅色圖示警告您掃描過程中偵測到受感染的物件，而且無法移除！

  每個圖示都可能是完整的或分成兩半的 - 完整的圖示表示掃描已經正常地完成或結束，分成兩半的圖示則表示掃描遭到取消或中斷。

  請注意：*如需每一項掃描的詳細資訊，請參閱掃描結果對話方塊，此對話方塊可利用檢視詳細資訊按鈕 (在對話方塊的底端) 存取。*

- ***開始時間*** - 掃描啟動的日期和時間
- ***結束時間*** - 掃描結束的日期和時間
- ***已測試的物件*** - 掃描期間檢查過的物件數

- ***感染*** - 偵測到/已移除的病毒感染數量
- ***間諜軟體*** - 偵測到/已移除的間諜軟體數量
- ***警告*** - 偵測到的可疑物件
- ***Rootkit*** - 偵測到的 rootkit
- ***掃描記錄資訊*** - 有關掃描過程和結果的資訊 (通常是關於掃描完成或中斷)

控制按鈕

掃描結果概觀對話方塊的控制按鈕有：

- ***檢視詳細資訊*** - 按一下可切換到掃描結果對話方塊並檢視所選掃描的詳細資料
- ***刪除結果*** - 按一下可將所選項目從掃描結果概觀中移除
- ***返回*** - 切換回到 AVG 掃描介面的預設對話方塊

12.7. 掃描結果詳細資訊

如果您在掃描結果概觀對話方塊中選取了特定的掃描，就可以按一下***檢視詳細資訊***按鈕，切換至***掃描結果***對話方塊，查看所選掃描之過程和結果的詳細資料。此對話方塊又進一步細分為數個標籤：

- 結果概觀 - 本標籤始終處於顯示狀態，提供說明掃描進度的統計資料
- 感染 - 本標籤只有在掃描過程中偵測到病毒感染時才會顯示
- 間諜軟體 - 本標籤只有在掃描過程中偵測到間諜軟體時才會顯示
- 警告 - 只有在掃描過程中偵測到 cookie 時，此標籤才會顯示
- Rootkit - 本標籤只有在掃描過程中偵測到 Rootkit 時才會顯示
- 資訊 - 本標籤只有在偵測到某些潛在的威脅，但無法分類為上述任何一類時，才會顯示；本標籤會提供有關此結果的警告訊息。此外，您也可以在這裡找到無法掃描物件的相關資訊 *(例如：受到密碼保護的封存檔)*。

12.7.1. 「結果概觀」標籤

您可在***掃描結果***標籤上找到包含以下項目的資訊的詳細統計資料：

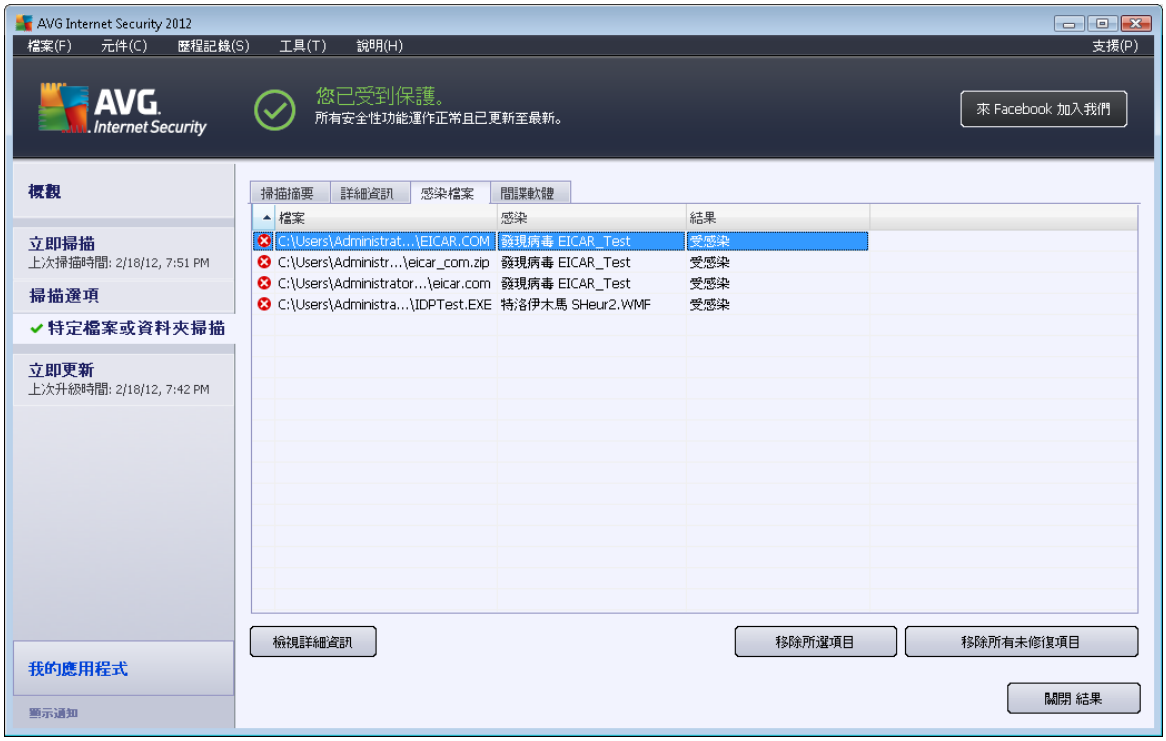
- 偵測到的病毒感染/間諜軟體
- 已移除的病毒感染/間諜軟體
- 無法移除或修復的病毒感染/間諜軟體數量

此外，您將找到有關掃描啟動的日期和確切時間、掃描的物件總數、掃描持續時間，以及掃描時所發生錯誤數量的資訊。

控制按鈕

此對話方塊中僅有一個控制按鈕可用。使用***關閉結果***按鈕返回掃描結果概觀對話方塊。

12.7.2. 「感染」標籤



掃描結果對話方塊只有在掃描期間偵測到***病毒感染***時，才會顯示感染標籤。此標籤分為三個區段，提供了以下資訊：

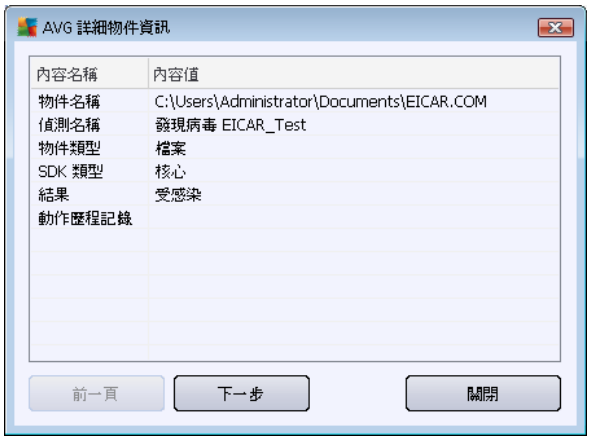
- ***檔案*** - 受感染物件原始位置的完整路徑
- ***感染*** - 偵測到的病毒的名稱 (*關於特定病毒的詳細資訊，請參閱線上病毒大全*)
- ***結果*** - 定義在掃描中偵測到的受感染物件的目前狀態：
    - ***受感染*** - 偵測到受感染物件並將其保留在原始位置 (*例如，當您在特定掃描設定中關閉自動修復選項時*)
    - ***已修復*** - 受感染的物件已被自動修復，並保留在其原始位置
    - ***移至病毒隔離區*** - 受感染物件已移至病毒隔離區隔離
    - ***已刪除*** - 受感染的物件已被刪除
    - ***已新增至 PUP 例外*** - 已將結果評估為例外，並新增至 PUP 例外清單中 (*在進階設定的 PUP 例外對話方塊中設定*)
    - ***鎖定的檔案 - 未經測試*** - 相應的物件已鎖定，AVG 無法對其進行掃描
    - ***潛在危險物件*** - 偵測到物件具有潛在危險，但未受感染 (*例如，可能包含巨集*) ;此資訊僅作為警告之用

- ***完成該動作需重新啟動*** - 無法移除受感染的物件，若要徹底移除，必須重新啟動電腦

控制按鈕

此對話方塊中有三個控制按鈕：

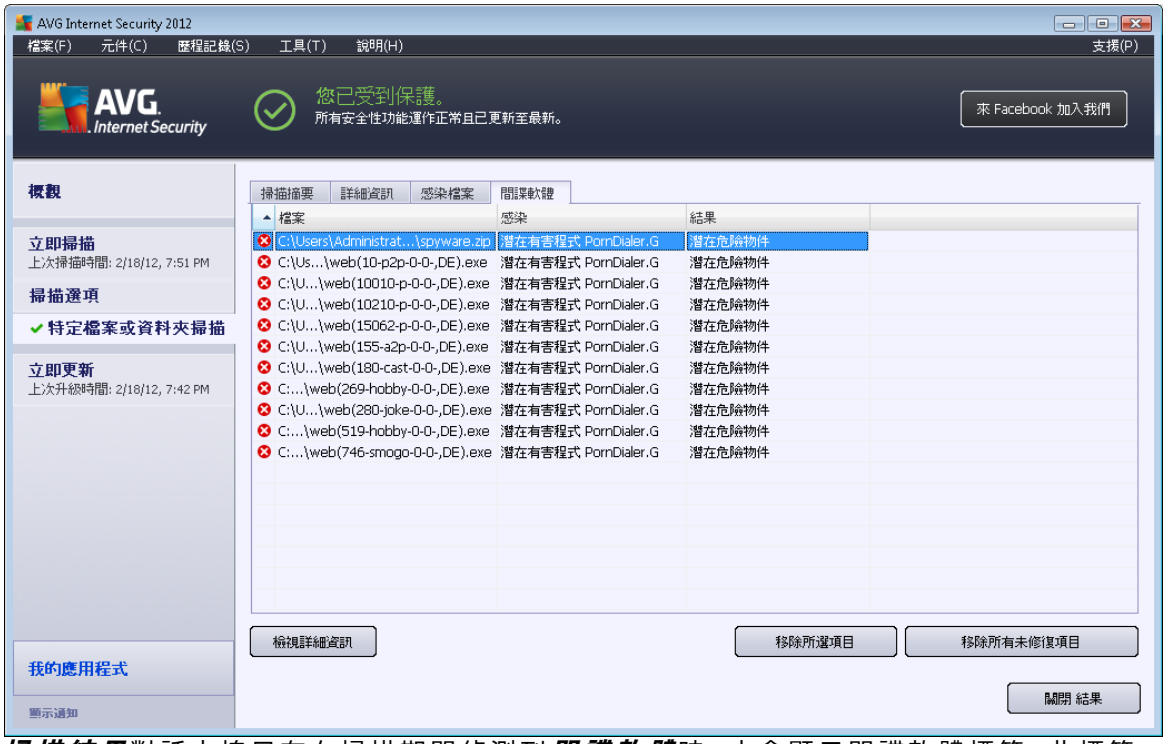
- ***檢視詳細資訊*** - 該按鈕可開啟名為***詳細物件資訊***的對話方塊視窗：



  您可以在此對話方塊中找到有關偵測到的受感染物件的詳細資訊 (*例如受感染的物件名稱和位置、物件類型、SDK 類型、偵測結果，以及與偵測到的物件相關的動作歷程記錄*)。使用***上一個/下一個***按鈕可以檢視特定結果的相關資訊。使用***關閉***按鈕可關閉此對話方塊。

- ***移除選取的感染檔案*** - 使用此按鈕可將選取的結果移至病毒隔離區
- ***移除所有未修復的感染檔案*** - 此按鈕可刪除所有無法修復或無法移至病毒隔離區的結果
- ***關閉結果*** - 終止詳細資訊概觀並返回掃描結果概觀對話方塊

12.7.3. 「間諜軟體」標籤



掃描結果對話方塊只有在掃描期間偵測到***間諜軟體***時，才會顯示間諜軟體標籤。此標籤分為三個區段，提供了以下資訊：

- ***檔案*** - 受感染物件原始位置的完整路徑
- ***感染*** - 偵測到的間諜軟體 *的名稱 (有關特定病毒的詳細資訊，請參閱線上病毒大全)*
- ***結果*** - 定義掃描期間偵測到的物件的目前狀態：
  - ***受感染*** - *偵測到受感染物件並將其保留在原始位置 (例如，當您在特定掃描設定中關閉自動修復選項時)*
  - ***已修復*** - 受感染的物件已被自動修復，並保留在其原始位置
  - ***移至病毒隔離區*** - 受感染物件已移至病毒隔離區隔離
  - ***已刪除*** - 受感染的物件已被刪除
  - ***已新增至 PUP 例外*** - 已將結果評估為例外，並新增至 PUP 例外清單中 *(在進階設定的 PUP 例外對話方塊中設定)*
  - ***鎖定的檔案 - 未經測試*** - 相應的物件已鎖定，AVG 無法對其進行掃描
  - ***潛在危險物件*** - 偵測到物件具有潛在危險，但未受感染 (例如，可能包含巨集) ;此資訊僅作為警告之用

- ***完成該動作需重新啟動*** - 無法移除受感染的物件，若要徹底移除，必須重新啟動電腦

控制按鈕

此對話方塊中有三個控制按鈕：

- ***檢視詳細資訊*** - 該按鈕可開啟名為***詳細物件資訊***的對話方塊視窗：

  您可以在此對話方塊中找到有關偵測到的受感染物件的詳細資訊 (*例如受感染的物件名稱和位置、物件類型、SDK 類型、偵測結果，以及與偵測到的物件相關的動作歷程記錄*)。使用***上一個/下一個***按鈕可以檢視特定結果的相關資訊。使用***關閉***按鈕可離開此對話方塊。

- ***移除選取的感染檔案*** - 使用此按鈕可將選取的結果移至病毒隔離區
- ***移除所有未修復的感染檔案*** - 此按鈕可刪除所有無法修復或無法移至病毒隔離區的結果
- ***關閉結果*** - 終止詳細資訊概觀並返回掃描結果概觀對話方塊

12.7.4. 「警告」標籤

警告標籤會顯示有關掃描期間偵測到之「可疑」物件 (*通常為檔案*) 的資訊。Resident Shield 偵測到的檔案會被封鎖而無法存取。此類結果的典型範例有：隱藏的檔案、cookie、可疑的登錄機碼、受密碼保護的文件或封存檔等。這類檔案對您的電腦或安全性並沒有任何直接的威脅。在您的電腦上偵測到廣告軟體或間諜軟體時，這些檔案的相關資訊一般都非常有用。如果測試結果中只包含 **AVG Internet Security 2012** 偵測到的警告，則不必採取任何動作。

以下是這類物件最常見示例的簡短描述：

- ***隱藏檔案*** - 預設情況下，在 Windows 中看不到隱藏檔案，而有些病毒或其他威脅可能會利用此屬性儲存它們的檔案以躲過偵測。**AVG Internet Security 2012**如果您懷疑報告的隱藏檔案可能是惡意內容，可將它移到您的病毒隔離區。

- ***Cookie*** - Cookie 是網站用來儲存使用者特定資訊的純文字檔，它之後會被用來載入自訂網站版面配置、預先填寫使用者名稱等。

- ***可疑的登錄機碼*** - 某些惡意軟體會將它的資訊儲存到 Windows 登錄中，確保它可以在開機時載入，或擴大它在作業系統上的影響範圍。

12.7.5. Rootkit 標籤

Rootkits 標籤顯示完整電腦掃描中 anti-rootkit 掃描期間偵測到的 rootkits 相關資訊。

rootkit 是一種試圖在沒有獲得系統所有者或合法管理員授權的情況下，取得電腦系統基本控制權的一種程式。rootkit 幾乎不需要存取硬體，因為它主要的目的是取得在硬體上執行的作業系統的控制權。一般而言，rootkit 會透過破壞或迴避標準作業系統的安全性機制來隱身於系統中。這些 rootkit 往往也是特洛伊木馬，讓使用者誤以為在系統上執行它們很安全。用來達到此目的的技巧包括對監視程式隱藏執行中的程序，或是隱藏作業系統中的檔案或系統資料。

此標籤的結構與感染標籤或間諜軟體標籤基本相同。

12.7.6. 「資訊」標籤

資訊標籤包含諸如無法歸類為感染、間諜軟體等 「結果」的相關資料。雖然無法將它們確定地標記為危險內容，但仍值得留意。**AVG Internet Security 2012** 掃描能夠偵測可能未受感染但可疑的檔案。會將這些檔案報告為警告或資訊。

若符合下列原因之一，則會報告嚴重性***資訊***：

- ***執行階段已封裝*** - 檔案的封裝用的是其中一種較不常見的執行階段封裝程式，可能表示有避開掃描此類檔案的意圖。不過，並不是所有這類檔案的報告都表示有病毒。

- ***執行階段循環封裝*** - 與上述類似，但在一般軟體中較為不常見。此類檔案很可疑，應該考慮將其移除或送交分析。

- ***受密碼保護的封存檔或文件*** - **AVG Internet Security 2012** (*或一般任何其他反惡意軟體程式*) 無法掃描受密碼保護的檔案。

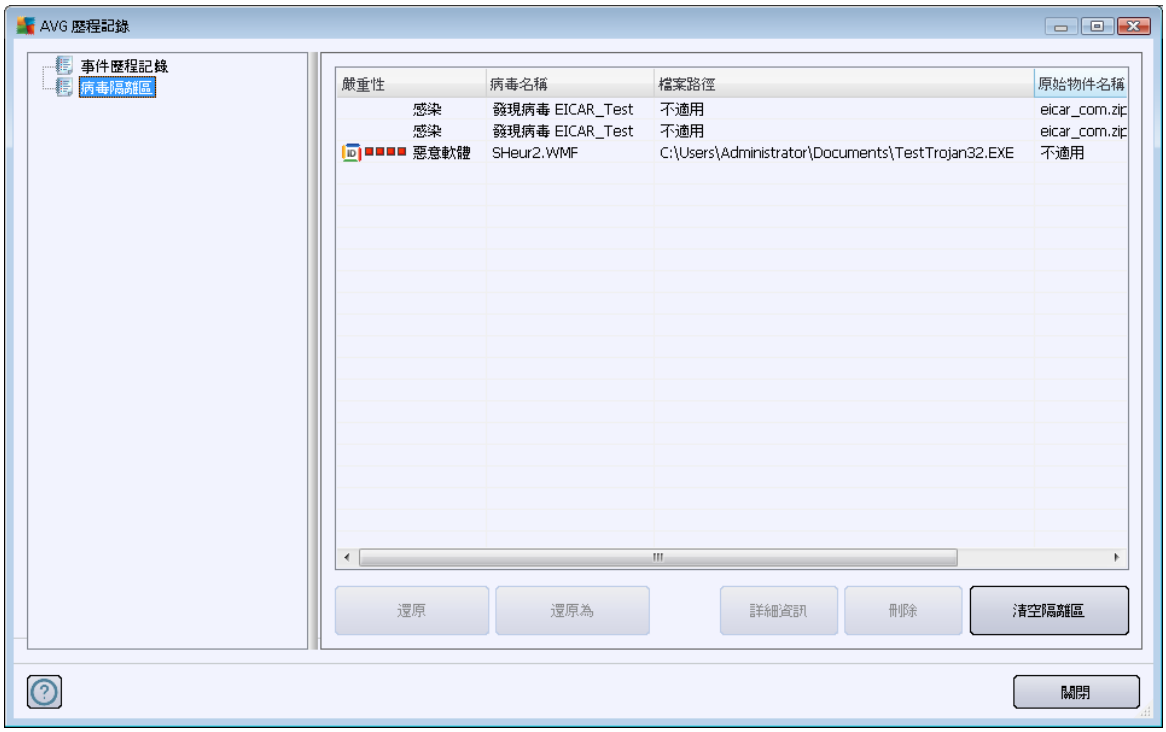
- ***包含巨集的檔案*** - 報告的文件包含巨集，且可能是惡意巨集。

- ***隱藏的副檔名*** - 例如，含隱藏副檔名的檔案可能看似圖片，但實際上是可執行檔 (*例如 picture.jpg.exe*)。預設情況下，在 Windows 中看不到第二個副檔名，而 **AVG Internet Security 2012** 會報告此類檔案以防被意外開啟。

- ***不正確的檔案路徑*** - 若有重要的系統檔案從預設路徑以外的路徑執行 (*例如，winlogon.exe 從 Windows 資料夾以外的位置執行*)，會報告此項差異。**AVG Internet Security 2012** 在某些情況下，病毒會利用標準系統程序的名稱，掩飾它們在系統內的行蹤。

- ***鎖定的檔案*** - 報告的檔案已被鎖定，因此 **AVG Internet Security 2012** 無法掃描。這通常是指有檔案不斷被系統使用 (*例如，交換檔案*)。

12.8. 病毒隔離區



病毒隔離區是一個用於管理 AVG 測試期間偵測到之可疑/受感染物件的安全環境。一旦在掃描期間偵測到受感染的物件，且 AVG 無法自動修復它，則系統會要求您決定要對可疑物件採取什麼措施。建議的解決方案是將物件移到***病毒隔離區***，以待進一步處理。***病毒隔離區***的主要用途是將任何刪除的檔案保留一段特定的時間期限，以便您確定其原始位置不再需要該檔案。如果您發現少了該檔案會造成問題，可以將此可疑檔案送出以進行分析，或者將其還原至原始位置。

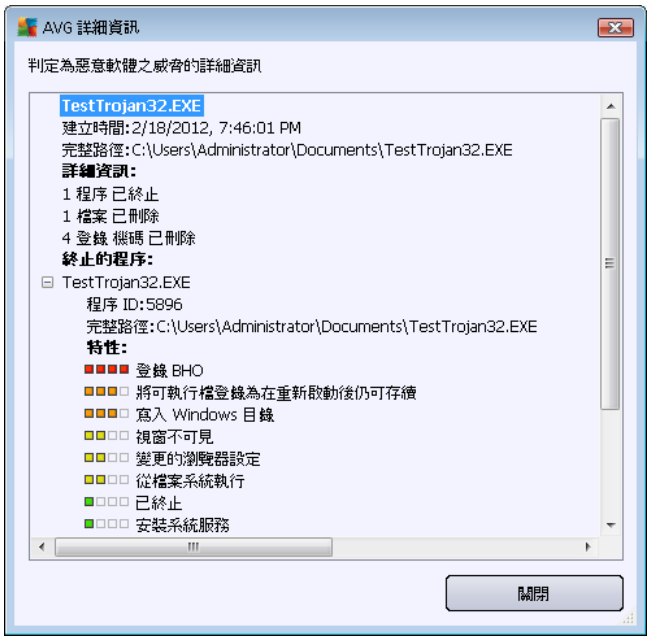
病毒隔離區介面會在單獨的視窗中開啟，提供有關隔離的受感染物件的資訊概觀：

- ***嚴重性*** - 如果您決定在 **AVG Internet Security 2012** 中安裝 Identity Protection 元件，該區段會提供一個識別圖像，並且按嚴重性分為四個層級 - 從無害 (■□□□) 到非常危險 (■■■■)，並提供有關感染類型的資訊 (*依其感染層級 - 所有列出的物件都有實際或潛在的感染*)
- ***病毒名稱*** - 依據病毒大全 *(線上) 指定偵測到的感染的名稱*
- ***檔案路徑*** - 偵測到的感染檔案之原始位置的完整路徑
- ***原始物件名稱*** - 在掃描期間，圖表中列出的所有偵測到的物件均使用 AVG 提供的標準名稱進行標記。如果某個物件具有已知的特定原始名稱 (*例如，與附件實際內容不一致的電子郵件附件的名稱*)，則會在此欄中提供。
- ***儲存日期*** - 偵測到可疑檔案並將其移除到病毒隔離區的日期和時間

控制按鈕

可在***病毒隔離區***介面存取下列控制按鈕：

- ***還原*** - 將受感染的檔案移回磁碟中的原始位置
- ***還原為*** - 將感染檔案移至所選資料夾
- ***詳細資訊*** - 該按鈕通常用於 Identity Protection 偵測到的威脅。若按一下按鈕，它會顯示威脅詳細資訊的概觀 (*哪些檔案/程序被感染、程序特性等等*)。請注意，除了 IDP 偵測到的項目之外，該按鈕一般呈灰色且無法使用！



- ***刪除*** - 將受感染的檔案從***病毒隔離區***完全移除，不可還原。
- ***清空隔離區*** - 徹底移除***病毒隔離區***所有內容。一旦將檔案從***病毒隔離區***中移除，這些檔案就無法還原至磁碟中了 (*並非移至資源回收筒中*)。

13. AVG 更新

任何安全性軟體都必須定期更新才能夠保證真正做到防禦各種威脅！病毒編寫者無時不在尋找軟體和作業系統中能夠利用的新漏洞。新的病毒、新的惡意軟體、新的駭客攻擊每天接踵而至。因此，軟體廠商們不斷發行更新和安全性補充程式，以修復發現的所有安全性漏洞。

有鑑於所有新興電腦威脅，以及它們的傳播速度，定期更新 **AVG Internet Security 2012** 絕對是至關重要的。最佳的解決之道是保留程式的預設設定，也就是設定自動更新。請注意，如果您 **AVG Internet Security 2012** 的病毒庫不是處於最新狀態，該程式將無法偵測最新的威脅！

定期更新您的 AVG 是至關重要的！如有可能，應儘量每天更新基本的病毒定義。不太緊急的程式更新可以每週更新一次。

13.1. 更新啟動

為了提供最高安全性，在預設情況下，會排程 **AVG Internet Security 2012** 每四個小時檢查新的更新。由於 AVG 更新是為了反映新威脅的數量和嚴重性而不定期發行，因此這項檢查對於確保您的 AVG 病毒庫隨時保持最新狀態來說極其重要。

如果您希望減少更新啟動次數，可以設定自己的更新啟動參數。不過，強烈建議您一天至少啟動更新一次！您可以在進階設定/排程區段中編輯該組態，特別是在以下對話方塊內：

- 定義更新排程
- 程式更新排程
- Anti-Spam 更新排程

如果您想要立即檢查新的更新檔案，請使用主要使用者介面中的立即更新快速連結。此連結可隨時從任何使用者介面對話方塊中找到。

13.2. 更新進度

一旦開始更新，AVG 首先確認是否有新的更新檔案發佈。如果有，**AVG Internet Security 2012** 會開始下載這些更新，並自動啟動更新程序。在更新程序期間，系統會將您重新導向到***更新***介面，在這裡您可以檢視以圖形表示的更新程序進度及其相關統計資料參數概觀 (*更新檔案大小*、*接收的資料*、*下載速度*、*耗用的時間*...):

***請注意**：AVG 程式更新在啟動之前，會先建立一個系統還原點。如果更新程序失敗，且作業系統當機，您始終可以將作業系統還原為在此還原點時的原始組態。此選項可透過「開始」/「所有程式」/「附屬應用程式」/「系統工具」/「系統還原」存取。建議僅限經驗豐富的使用者使用！*

13.3. 更新層級

AVG Internet Security 2012 有兩種更新層級可供選擇：

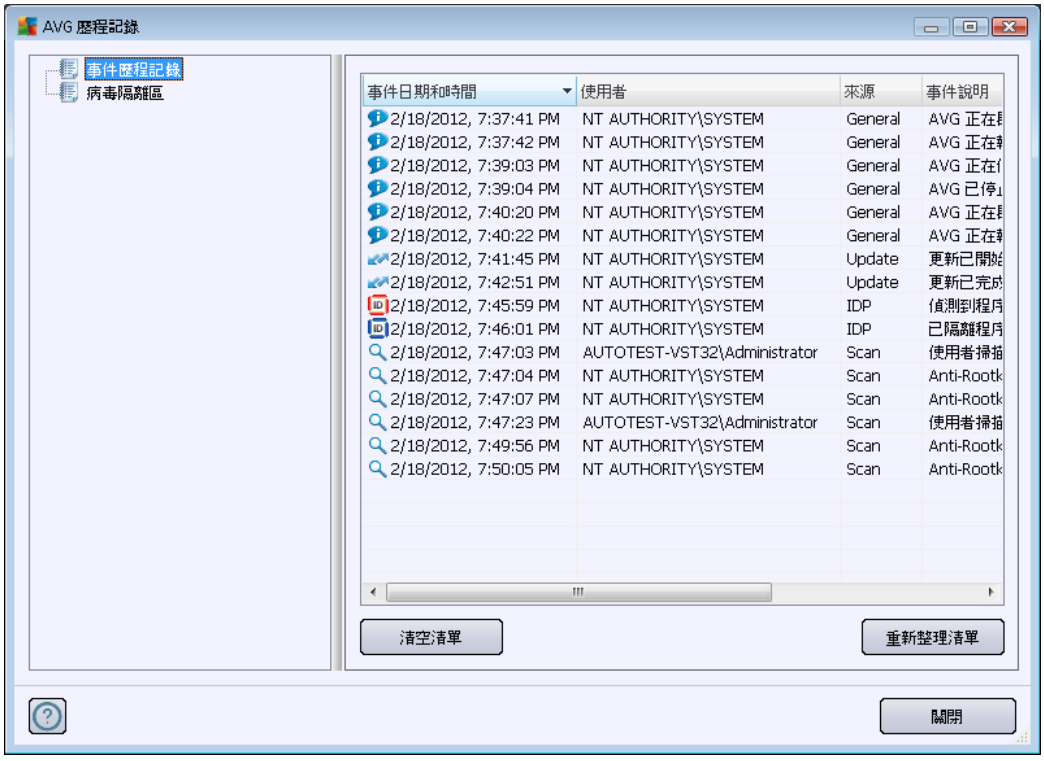
- ***定義更新***包含獲取可靠的反病毒、反垃圾郵件和反惡意軟體保護所需的變更。一般而言，它不包括對程式碼的任何變更，而是只更新定義資料庫。這種更新應在發佈後便立即套用。
- ***程式更新*** - 包含各種程式變更、修復和改進。

當排程更新時，可同時針對兩種更新層級定義特定的參數：

- 定義更新排程
- 程式更新排程

***注意：**如果一項排程應用程式更新和排程掃描撞期，則程式更新擁有較高的優先次序，而掃描將會暫停。*

14. 事件歷程記錄



歷程記錄對話方塊可透過系統功能表的***歷程記錄/事件歷程記錄***項目來存取。在此對話方塊中，您可以找到 **AVG Internet Security 2012** 作業期間發生的重要事件摘要。***歷程記錄***會記錄下列類型的事件：

- 有關 AVG 應用程式更新的資訊
- 掃描開始、結束或停止的相關資訊 (*包括自動執行的測試*)
- 與病毒偵測關聯的事件的相關資訊 (*透過 Resident Shield 或掃描*) 包括發生位置
- 其他重要事件

每個事件都會列出以下資訊：

- ***事件日期和時間***提供事件發生的確切日期和時間
- ***使用者***指出在事件發生當時登入的使用者名稱
- ***來源***提供觸發事件的來源元件或 AVG 系統其他部分的相關資訊
- ***事件描述***提供具體事件的簡短摘要

控制按鈕

- ***清空清單*** - 按此按鈕可刪除事件清單中的所有項目
- ***重新整理清單*** - 按此按鈕可更新事件清單中的所有項目

15. 常見問題集和技術支援

如果您對 **AVG Internet Security 2012** 應用程式在銷售或技術上有任何疑問，有幾種尋求協助的管道。請從以下選項選擇：

- ***獲取支援*** :在 AVG 應用程式中，您可在 AVG 網站 (http://www.avg.com/) 獲得專用的客戶支援。選擇***說明/獲取支援***主功能表，可重新導向具有可用支援途徑的 AVG 網站。若要繼續，請遵循網頁中的指示。

- ***支援 (主功能表連結)*** :AVG 應用程式功能表 (*主要使用者介面頂端*) 包含***支援***連結，會開啟一個新對話方塊，當中包含您在嘗試尋求協助時可能需要的各種資訊。該對話方塊包含您已安裝 AVG 程式 (*程式/資料庫版本*) 的基本資料、授權詳細資料和快速支援連結清單：

- ***在說明檔案中疑難排解*** :新***疑難排解***區段可直接從 **AVG Internet Security 2012** *內含的說明檔中使用 要開啟說明檔，請在應用程式中的任意對話方塊中按一下 F1 鍵)*。此區段提供當使用者有技術問題而想要尋求專業協助時最常發生的狀況清單。請選取最符合您的問題的狀況，然後按一下它可開啟引導問題解決方案的詳細指示。

- ***AVG 網站支援中心*** :或者，您也可以選擇在 AVG 網站 (http://www.avg.com/) 上查詢問題的解決方案。您可以在***支援中心***區段中找到處理銷售和技術問題的主題群組的結構化概觀。

- ***常見問題集*** :您在 AVG 網站 (http://www.avg.com/) 上也可以找到獨立且結構詳細的常見問題集區段。此區段可透過***支援中心/常見問題集***功能表選項存取。同樣地，所有問題都分成經過妥善安排的銷售、技術和病毒類別。

- ***關於病毒與威脅*** :AVG 網站 (http://www.avg.com/) 有一章是專門討論病毒問題 *(可*

透過說明/關於病毒與威脅選項從主功能表存取)。在功能表中選取***支援中心/關於病毒與威脅***可進入提供與線上威脅相關資訊的結構化概觀的頁面。您也可以找到有關移除病毒、間諜軟體的指示，以及如何持續受到保護的建議。

- ***論壇*** :您也可以使用 AVG 使用者論壇，網址是 http://forums.avg.com。