AVG 9 Anti-Virus plus Firewall

使用者手冊

文件修訂版 90.21 (3.2.2010)

內容

1. 簡介

本使用者手冊提供有關 AVG 9 Anti-Virus plus Firewall 的詳細介紹。

感謝您購賣 AVG 9 Anti-Virus plus Firewall **!**

AVG 9 Anti-Virus plus Firewall 是獲獎的 AVG 產品系列之一，它能為您的電腦提供全面保護，讓您安心無虞。如 AVG 所有的產品一樣，AVG 9 Anti-Virus plus Firewall 也經過徹底的重新設計，以一種嶄新、更方便使用且更有效率的方式，提供知名且備受信賴的 AVG 安全性保護。

您新購的 AVG 9 Anti-Virus plus Firewall 產品有一個簡化介面，為您提供更主動和快速的掃描效能。為了方便您使用，我們提供了更多自動執行的安全性功能，並涵蓋了新的「智慧型」使用者選項，可讓您調整我們的安全性功能以配合您的使用方式。不用再為了安全性而犧牲可用性！

AVG 是專為保護您的電腦和網路活動而設計和開發。享受由 AVG 帶來的全面保護體驗吧。

2. AVG 安裝需求

2.1. 支援的作業系統

AVG 9 Anti-Virus plus Firewall 可保護執行下列作業系統的工作站:

- Windows 2000 Professional SP4 + 更新彙總套件 1
- 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 Service Pack)

2.2. 最低和建議的硬體需求

AVG 9 Anti-Virus plus Firewall 的最低硬體需求:

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

AVG 9 Anti-Virus plus Firewall 的建議硬體需求:

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

3. AVG 安裝選項

您可從安裝 CD 上提供的安裝檔案，或從 AVG 網站 (http://www.avg.com/) 下載最新的安裝檔案來安裝 AVG。

開始安裝 AVG 前，強烈建議您造訪 AVG 網站 (http://www.avg.com/)，查看是否有新的安裝檔案。如此一來，您就可以確保自己安裝的是最新版本的 AVG 9 Anti-Virus plus Firewall。

建議您試試新的 AVG 下載管理員工具，它能引導您以自己的語言設定安裝檔！

在安裝過程中，系統會要求您提供授權/銷售號碼。請務必在開始安裝之前預先準備好。銷售號碼記錄在 CD 包裝上。如果您是線上購買 AVG 產品，您的授權號碼會透過電子郵件傳送給您。

4. AVG 下載管理員

AVG **下載管理員** 是一個簡單實用的工具，它能幫您的 AVG 產品試用版選擇適合的安裝檔。根據您的輸入資料，管理員將選取特定產品、授權類型、所需元件及語言。最後，AVG **下載管理員** 將開始下載並啟動適當的安裝程序。

警告：請注意，AVG 下載管理員並不適合用來下載 Network Edition 和 SBS Eidtion，而且只支援下列作業系統：Windows 2000 (SP4 + SRP 彙總套件)、Windows XP、Windows Vista 及 Windows 7。

AVG **下載管理員** 可至 AVG 網站 (http://www.avg.com/) 下載。以下是您必須在 AVG **下載管理員** 中採取的各個步驟的簡短說明：

4.1. 語言選擇

在 AVG **下載管理員**的第一個步驟中，從下拉式功能表中選取安裝語言。請注意，您的語言選擇只會套用到安裝程序；完成安裝後，您可直接從程式設定變更語言。然後按下 ***下一步***按鈕繼續。

4.2. 連線檢查

在下一步驟中，AVG **下載管理員** 會試圖建立網際網路連線，以便尋找更新。您必須等到 AVG **下載管理員** 完成連線測試，才能進入下載程序。

- 如果測試顯示沒有連線，請確認您已經連線到網際網路。接著按一下***重試***按鈕

- 如果您使用代理連線到網際網路，請按一下***代理設定***按鈕來指定您的代理資訊：
- 如果檢查成功，請按下 ***下一步***按鈕繼續。

4.3. 代理設定

如果 AVG **下載管理員** 無法辨識您的代理設定，則必須手動指定。請填寫以下資料：

- *伺服器* - 輸入有效的代理伺服器名稱或 IP 位址
- *連接埠* - 提供相應的連接埠號
- *使用代理驗證* - 如果您的代理伺服器需要驗證，請勾選此核取方塊。
- *選取驗證* - 從下拉式功能表選取驗證類型。我們強烈建議您保留預設值 (*代理伺服器隨後將自動向您傳達其需求*)。但是，如果您是有經驗的使用者，您也可以選擇「基本」(*某些伺服器所需*) 或「NTLM」(*所有 ISA 伺服器所需*) 選項。然後輸入有效的*使用者名稱*和*密碼* (選用)。

透過按下*套用*按鈕確認您的設定，並繼續 AVG **下載管理員** 的下一步驟。

4.4. 下載要安裝的檔案

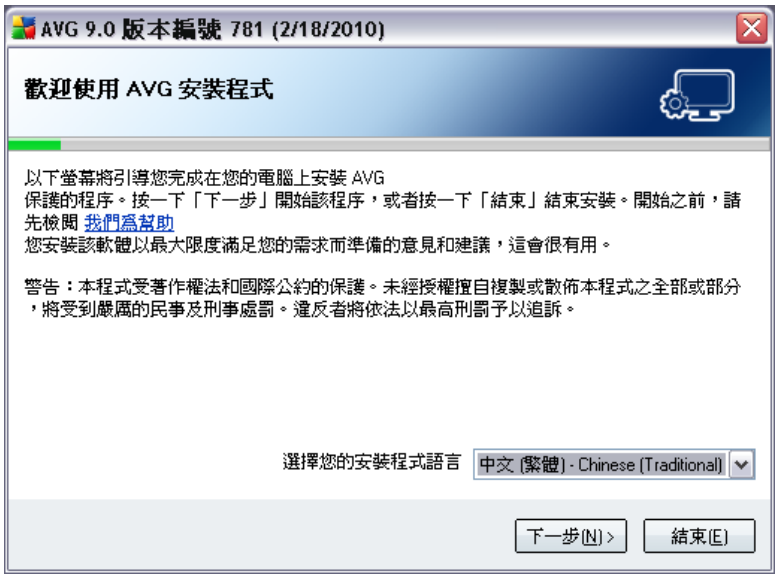
現在，您已經提供 AVG 下載管理員 開始下載安裝套件及啟動安裝程序所需的全部資訊。接著，進入 AVG 安裝程序。

5. AVG 安裝程序

要將AVG 9 Anti-Virus plus Firewall 安裝在您的電腦中，您需要最新的安裝檔。您可以使用產品包裝盒內附的 CD 上的安裝檔案，但此檔案可能已過時。因此我們建議從網上取得最新安裝檔案。您可以到 AVG 網站 (http://www.avg.com/) 的*支援中心 / 下載*部分下載安裝檔。或者，可以利用我們全新的 *AVG 下載管理員*工具，幫助您建立和下載所需的安裝套件，以及啟動安裝程序。

安裝作業包含一系列對話方塊視窗，其中會提供每個步驟的簡短說明。下面提供了每個對話方塊視窗的說明：

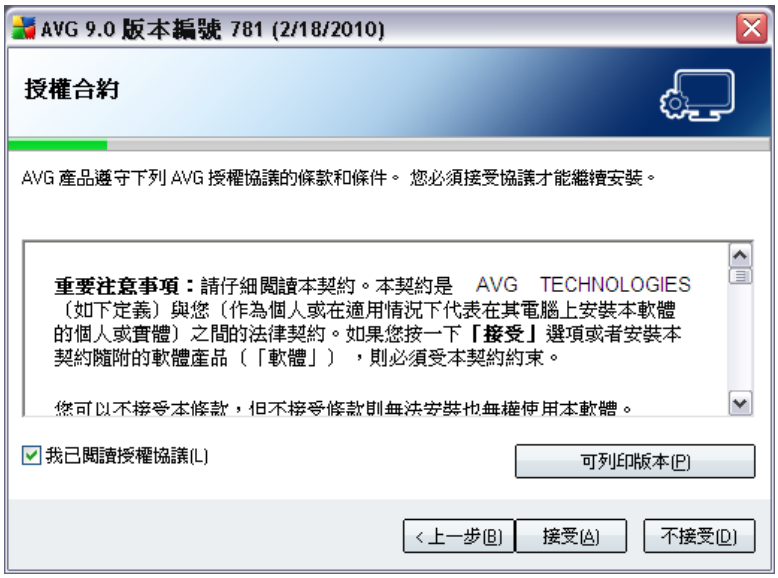
5.1. 安裝啟動



安裝程序啟動時會顯示*歡迎使用 AVG 安裝程式*視窗。您可在此處選取用於安裝程序的語言。在對話方塊視窗的下半部，找到*選擇您的安裝程式語言*項目，並從下拉式功能表中選取需要的語言。然後按下*下一步*按鈕確認並繼續至下一個對話方塊。

請注意：您在此處選取的語言僅用於安裝程序。您選取的語言不會用於 AVG 應用程式 - 該應用程式的語言可稍後在安裝過程中指定！

5.2. 授權協議



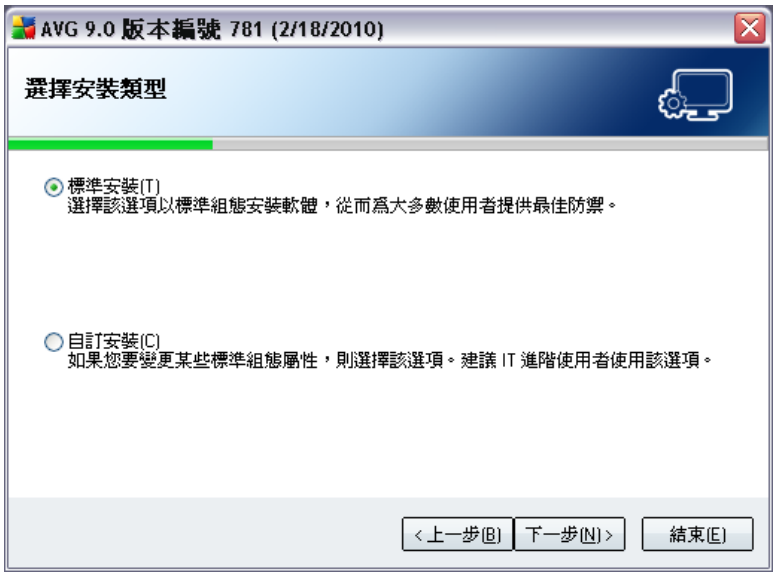
*授權協議*對話方塊提供 AVG 授權協議的完整內容。請仔細閱讀，並核取*我已閱讀授權協議*核取方塊，然後按下*接受*按鈕，確認您已閱讀、瞭解並接受該協議。

如果您不同意所述的使用條款，請按*不接受*按鈕，安裝程序隨後將立即終止。

5.3. 檢查系統狀態

確認授權協議之後，會將您重新導向到*檢查系統狀態*對話方塊。此對話方塊無需您進行任何操作；開始安裝 AVG 之前會先檢查您的系統。請等候程序完成，隨後便會自動進入後續的對話方塊。

5.4. 選取安裝類型



*選取安裝類型*對話方塊提供了兩種安裝選項，即：*標準*和*自訂*安裝。

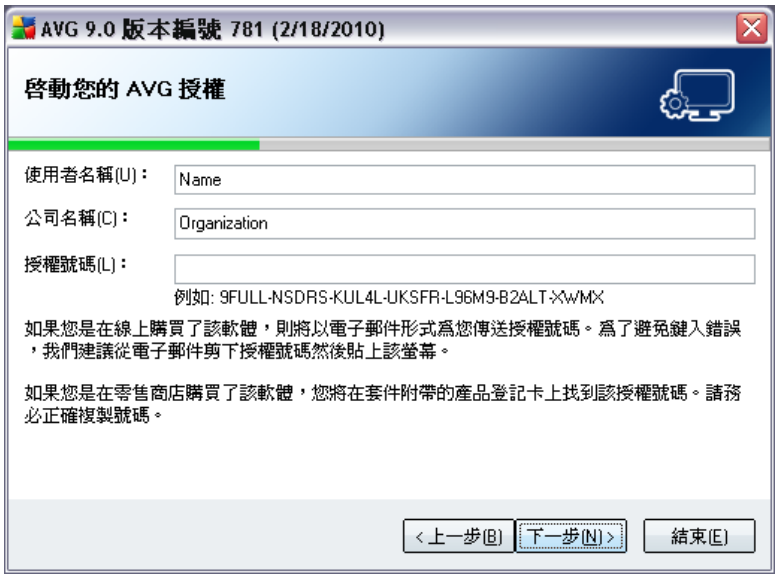
對於大多數使用者，強烈建議保持使用*標準安裝*，它會以完全自動的模式，使用程式供應商預定義的設定來安裝 AVG。這種組態不僅提供最大安全性，並且充分利用資源。在未來如果需要變更此組態，您隨時可以在 AVG 應用程式中直接操作。

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

5.5. 啟動您的 AVG 授權

您必須在*啟動您的 AVG 授權*對話方塊中填寫註冊資料。輸入您的名稱 (*使用者名稱*欄位) 以及您公司的名稱 (*公司名稱*欄位)。

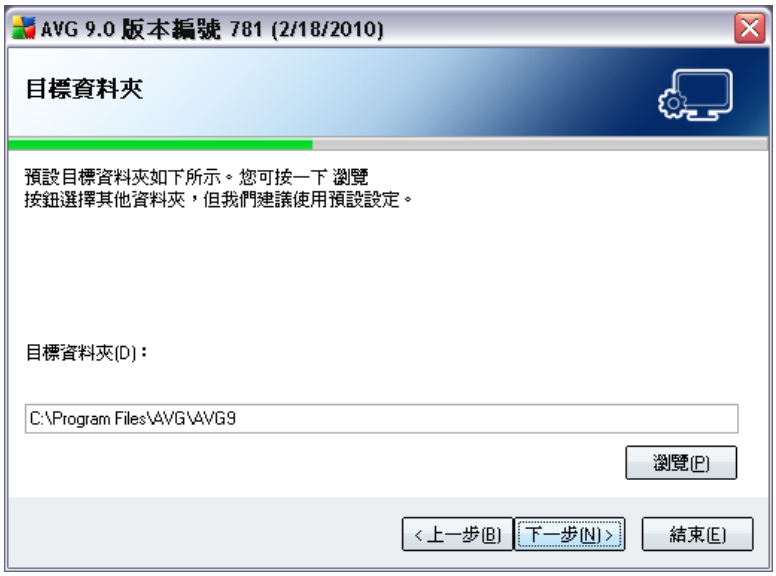
接著在*授權號碼*文字欄位中，輸入您的授權/銷售號碼。銷售號碼位於您的 AVG 9 Anti-Virus plus Firewall 盒裝 CD 包裝上。授權號碼位於您在線上購買 AVG 9 Anti-Virus plus Firewall 後收到的確認電子郵件內。您必須完全按照顯示的號碼準確輸入。若有提供電子形式的授權號碼 (*在電子郵件內*)，建議使用複製和貼上方法插入此號碼。



按下 *下一步* 按鈕繼續執行安裝程序。

如果您已在之前步驟中選取了標準安裝，則會直接將您重新導向至 *AVG Security Toolbar 對話方塊*。如果選取了自訂安裝，您將繼續前進至 *目標資料夾* 對話方塊。

5.6. 自訂安裝 - 目標資料夾

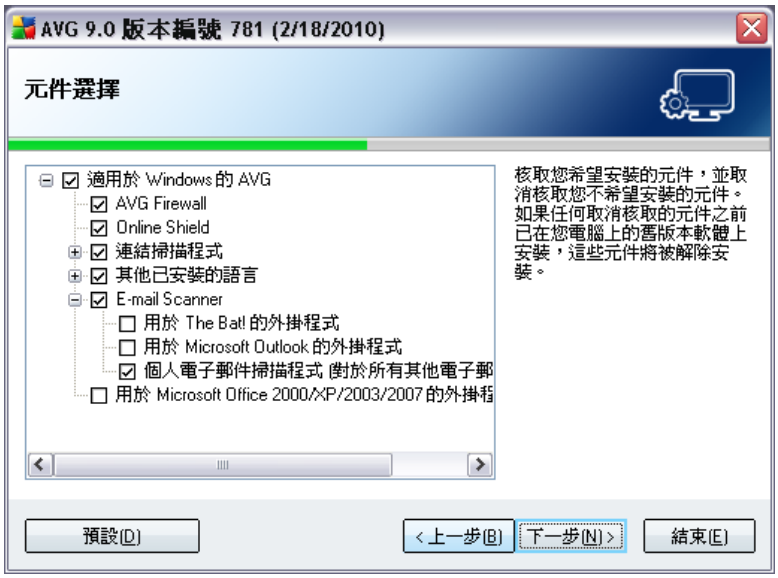


*目標資料夾*對話方塊讓您可指定 AVG 9 Anti-Virus plus Firewall 的安裝位置。預設情況下，AVG 會安裝到磁碟機 C: 的 Program Files 資料夾中。如果該資料夾不存在，會出現一個新的對話方塊要求您確認您同意 AVG 現在建立此資料夾。

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。

按 *下一步*按鈕確認。

5.7. 自訂安裝 - 元件選取



*元件選取*對話方塊顯示可安裝的 AVG 9 Anti-Virus plus Firewall 元件。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，您只能選取包含在您購買的 AVG 版本中的元件。「元件選取」對話方塊中僅提供這些元件讓您安裝！

- ***語言選擇***

  在要安裝的元件清單中，您可以定義以何種語言安裝 AVG。核取*其他已安裝的語言*項目，然後從相應的功能表選取所需語言。

- *E-mail Scanner* ***外掛程式***

  按一下 *E-mail Scanner* 項目來開啟和決定要安裝何種外掛程式來確保電子郵件的安全性。預設情況下會安裝*用於 Microsoft Outlook 的外掛程式*。另一個特定選項是*用於 The Bat! 的外掛程式* 如果您使用任何其他電子郵件用戶端 (*MS*

Exchange、*Qualcomm Eudora 等*)，核取*個人電子郵件掃描程式*選項可自動保障電子郵件通訊的安全性 (無論您執行何種電子郵件程式)。

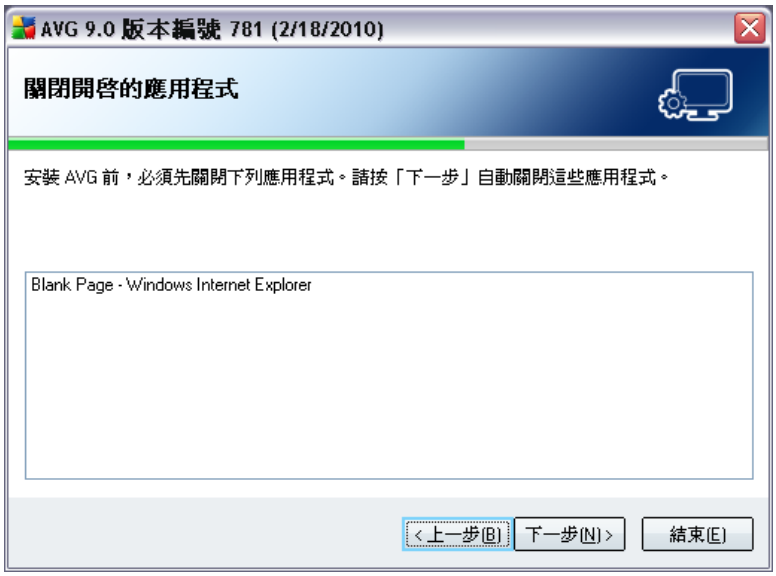
按*下一步*按鈕繼續。

5.8. AVG Security Toolbar

在 *AVG Security Toolbar* 對話方塊中，您可以決定是否要安裝 *AVG Security Toolbar* (*驗證支援網際網路搜尋引擎的搜尋結果*)。如果您不變更預設設定，該元件將自動安裝到您的網路瀏覽器中 (*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. 2.0 或更高版本*)，為您在瀏覽網路時提供全面性的保障。

此外，您還可決定是否選擇 Yahoo!為您預設的搜尋服務提供者。如果同意，請勾選對應的核取方塊。

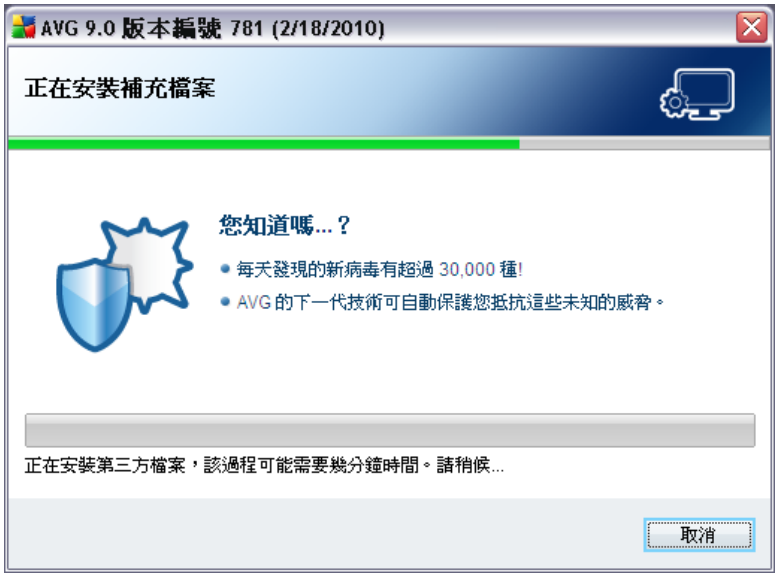
5.9. 關閉開啟的應用程式



在安裝時，只有在您的電腦有其他衝突的應用程式正在執行時，***關閉開啟的應用程式***對話方塊才會開啟。對話方塊中會列出為了完成安裝而需要關閉的應用程式。按***下一步***按鈕確認您同意關閉這些應用程式，繼續進行下一步。

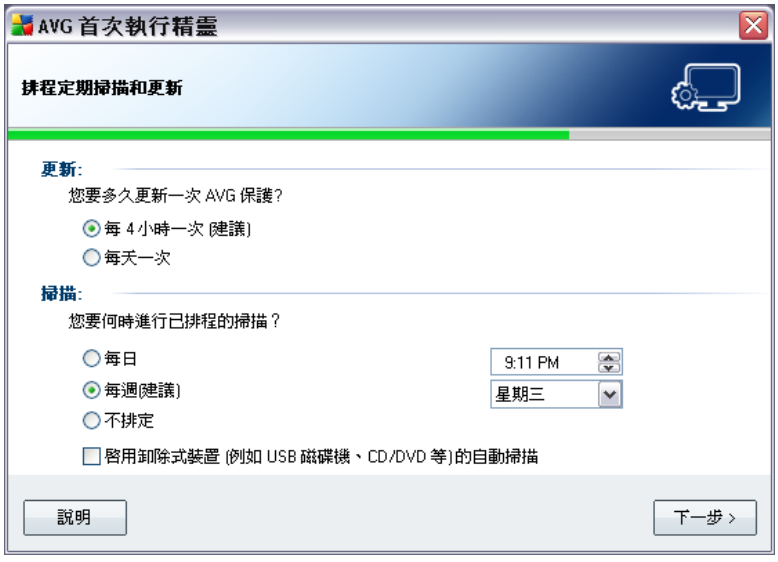
5.10. 安裝 AVG

安裝 AVG 對話方塊會顯示安裝程序的進度，完全無需任何介入操作：



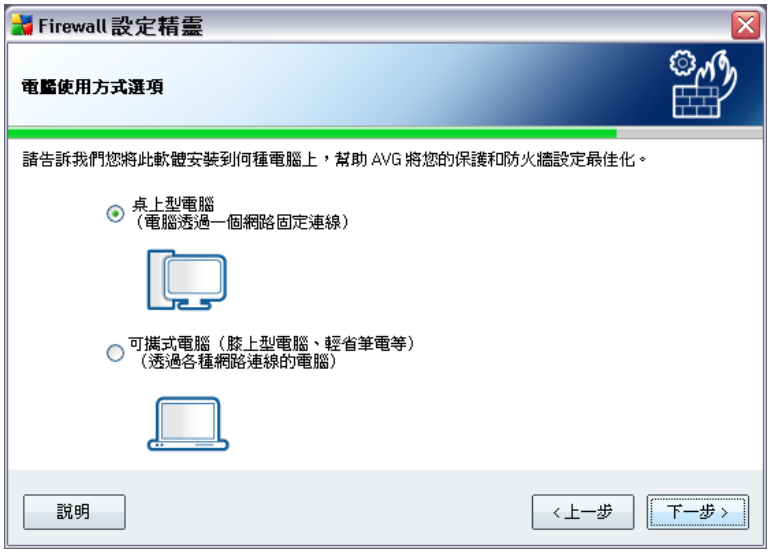
安裝程序完成後，會自動將您重新導向至下一個對話方塊。

5.11. 排程定期掃描和更新



在*排程定期掃描和更新*對話方塊中設定新更新檔案可存取性檢查的時間間隔，以及定義要啟動排程掃描的時間。建議保留預設值。按下*下一步*按鈕繼續。

5.12. 電腦使用方式選擇



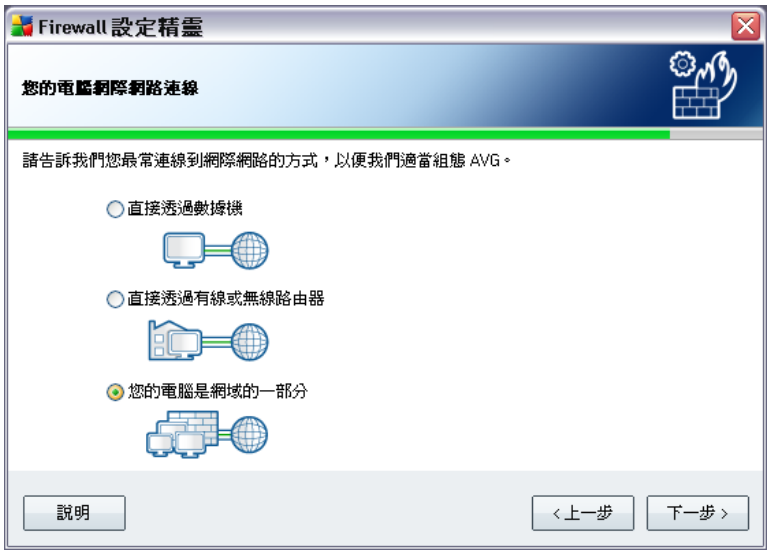
在此對話方塊中，*Firewall 組態精靈*會詢問您所使用的電腦類型。例如，您的筆記型電腦會從許多不同地點（*機場、酒店房間等連線到網際網路*）連線至網際網路，它所需的安全性規則比網域中的電腦（*公司網路等*）。*Firewall* 預設規則會根據所選的電腦使用類型，按不同的安全性層級定義。

您有兩個替代選項可以選擇：

- *桌上型電腦*
- *可攜式電腦*

按一下*下一步*按鈕確認您的選擇，並繼續至下一個對話方塊。

5.13. 您的電腦網際網路連線



在此對話方塊中，*Firewall **組態精靈***會詢問您的電腦連線到網際網路的方式。根據所選的連線類型，*Firewall* 預設規則會根據不同的安全性層級進行定義。

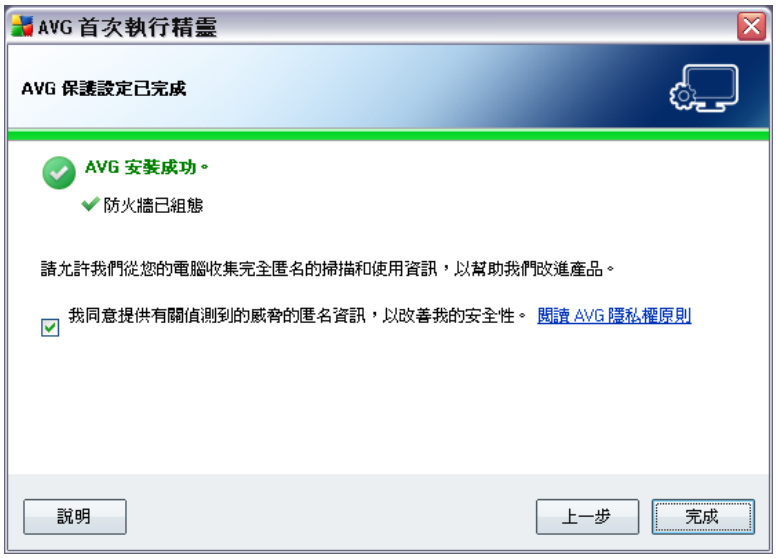
您有三個替代選項可以選擇：

- ***直接透過數據機***
- ***直接透過有線或無線路由器***
- ***您的電腦是網域的一部分***

選取最能描述您的電腦與網際網路之間連線的類型。

按一下 ***下一步***按鈕確認您的選擇，並前進到下一個對話方塊。

5.14. AVG 保護組態已完成



現在，您的 AVG 9 Anti-Virus plus Firewall 組態已配置完成。

在此對話方塊中，您可以決定是否要啓動以匿名方式向 AVG 病毒實驗室報告木馬攻擊程式和惡意網站的選項。如果決定啟動，請勾選*我同意提供有關偵測到的威脅的匿名資訊，以改善我的安全性*選項。

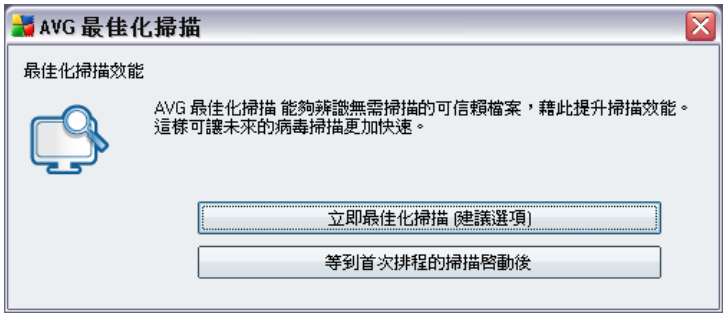
最後，按下*完成*按鈕。您可能需要重新啟動電腦，才能開始使用 AVG。

6. 安裝之後

6.1. 掃描最佳化

該掃描最佳化功能會搜尋 *Windows* 及 *Program Files* 資料夾，偵測相應的檔案 (*目前來說為 *.exe、*.dll 和 *.sys 檔案*)，然後儲存有關這些檔案的資訊。等到下次存取時，這些檔案就不會被掃描，因此可大幅縮短掃描時間。

一旦安裝完成，畫面上會出現一個新的對話方塊，詢問您是否執行最佳化掃描：



建議您採用此選項，並按一下***立即進行最佳化掃描***來執行掃描最佳化程序。

6.2. 產品註冊

完成 AVG 9 Anti-Virus plus Firewall 的安裝之後，請在 AVG 網站 (http://www.avg.com/) 的***註冊***頁面 (*依照頁面上直接提供的指示線上註冊您的產品*)。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。

6.3. 存取使用者介面

您可以使用下列幾種方式存取 *AVG 使用者介面*：

- 連按兩下系統匣上的 AVG 圖示
- 連按兩下桌面上的 AVG 圖示
- 存取功能表***開始 / 所有程式*** / *AVG 9.0* / ***AVG 使用者介面***

6.4. 掃描整台電腦

電腦病毒很有可能在安裝 AVG 9 Anti-Virus plus Firewall 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。

有關執行*掃描整台電腦*的說明，請參閱 *AVG 掃描*一章。

6.5. Eicar 測試

如果要確認 AVG 9 Anti-Virus plus Firewall 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，並儲存到您的本機磁碟。確認下載測試檔案之後，*Online Shield* 馬上會有所反應並提出警告。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。但是當您要解壓縮時，*Resident Shield* 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！**

6.6. AVG 預設組態

AVG 9 Anti-Virus plus Firewall 的預設組態 (*即應用程式在剛安裝好時的設定情形*) 是由軟體供應商設定，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！設定變更只能由有經驗的使用者來進行。

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***，然後在剛開啟的 *AVG 進階設定*對話方塊中編輯 AVG 組態。

7. AVG 使用者介面

AVG 9 Anti-Virus plus Firewall 開啟時會顯示主視窗:

主視窗由數個部分構成:

- *系統功能表 (視窗頂端的系統列)* 是標準巡覽, 可讓您存取所有 AVG 元件、服務及功能 - 詳細資訊 >>
- *安全性狀態資訊 (視窗的上方部分)* 提供有關 AVG 程式目前狀態的資訊 - 詳細資訊 >>
- *快速連結 (視窗左邊部分)* 可讓您快速存取最重要及最常用的 AVG 工作 - 詳細資訊 >>

- *元件概觀 (視窗中間部分)* 提供所有已安裝 AVG 元件的概觀 - 詳細資訊 >>
- *統計資料 (視窗左下方)* 提供有關程式作業的所有統計資料 - 詳細資訊 >>
- *系統匣圖示 (監視器右下角，位於系統匣中)* 指出 AVG 目前狀態 - 詳細資訊 >>

7.1. 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 9 Anti-Virus plus Firewall 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：

7.1.1. 檔案

- *結束* - 關閉 AVG 9 Anti-Virus plus Firewall 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！

7.1.2. 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* - 開啟 *Anti-Virus* 元件的預設頁面
- *Anti-Rootkit* - 開啟 *Anti-Rootkit* 元件的預設頁面
- *Anti-Spyware* - 開啟 *Anti-Spyware* 元件的預設頁面
- *Firewall* - 開啟 *Firewall* 元件的預設頁面
- *Link Scanner* - 開啟 *Link Scanner* 元件的預設頁面
- *E-mail Scanner* - 開啟 *E-mail Scanner* 元件的預設頁面
- *授權* - 開啟*授權*元件的預設頁面
- *Online Shield* - 開啟 *Online Shield* 元件的預設頁面
- *Resident Shield* - 開啟 *Resident Shield* 元件的預設頁面

- ***更新管理員*** - 開啟***更新管理員***元件的預設頁面

7.1.3. 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*** - 開啟包含了 *Resident Shield*
- *E-mail Scanner **偵測*** - 開啟包含了 *E-mail Scanner* 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*** - 開啟包含了 *Online Shield*
- ***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。將受感染檔案隔離到此隔離區域後，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*** - 開啟包含所有記錄的 AVG 9 Anti-Virus plus Firewall 動作概觀的歷程記錄介面。
- *Firewall* - 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

7.1.4. 工具

- ***掃描電腦*** - 切換至 AVG 掃描介面並開始掃描整台電腦
- ***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結構中定義要掃描哪些檔案和資料夾
- ***掃描檔案*** - 允許您對從磁碟樹狀結構中選取的單一檔案執行按需測試
- ***更新*** - 自動啟動更新程序 AVG 9 Anti-Virus plus Firewall
- ***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*** - 會開啟 *AVG **進階設定***對話方塊，您可以在這裡編輯 AVG 9 Anti-Virus plus Firewall 組態。通常建議保留由軟體供應商定義的應用程式之預設設定。
- *Firewall **設定*** - 會開啟一個獨立的對話方塊，用於 *Firewall* 元件的進階組態

7.1.5. 說明

- *內容* - 開啟 AVG 說明檔案
- *獲取線上說明* - 開啟 AVG 網站 (http://www.avg.com/) 的客戶支援中心頁面
- *您的 AVG 網站* - 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*個性化 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：如果您使用的是 AVG 9 Anti-Virus plus Firewall *試用版，後兩項會顯示為現在購買及啟動，讓您可立刻購買完整版的授權。如果您在安裝* AVG 9 Anti-Virus plus Firewall *時輸入了銷售號碼，這些選項會顯示為註冊及啟動。欲瞭解更多資訊，請參閱本文件的授權部分。*

- *關於 AVG* - 開啟*資訊*對話方塊，該對話方塊包含五個標籤，提供有關程式名稱、程式和病毒庫版本、系統資訊、授權協議和 *AVG Technologies CZ* 聯絡資訊的資料。

7.2. 安全性狀態資訊

*安全性狀態資訊*部分位於 AVG 主視窗的頂端。您始終可以在這部分找到有關 AVG 9 Anti-Virus plus Firewall 當前安全性狀態的資訊。請參閱此部分中可能描述的圖示概觀及其含義：


綠色圖示表示 AVG 可完全正常運作。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。


橙色圖示警告您有一個或多個元件設定錯誤，您必須檢查其內容/設定。AVG 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 AVG 的保護。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*部分提供。

如果您基於某種原因決定忽略元件的錯誤狀態 (*在 AVG 主視窗的元件概觀中，以滑鼠右鍵按一下對應的元件圖示，從開啟的內容功能表中即可存取「忽略元件狀態」選項*)，也會出現此圖示。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。

 紅色圖示表示 AVG 處於嚴重錯誤狀態！一或多個元件不能正常運作，且 AVG 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。

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！

請注意：AVG 狀態資訊也可隨時從系統匣圖示中取得。

7.3. 快速連結

快速連結 (位於 AVG 使用者介面左側) 允許您立即存取最重要且最常用的 AVG 功能：

- *概觀* - 使用此連結可從任何目前開啟的 AVG 介面切換到具有所有已安裝元件概觀的預設介面 - 請參閱*元件概觀一章 >>*
- *電腦掃描程式* - 使用此連結可開啟 AVG 掃描介面，您可在其中直接執行測試、排程掃描或編輯它們的參數 - 請參閱 *AVG 掃描一章 >>*
- *立即更新* - 此連結會開啟更新介面，並立即啟動 AVG 更新程序 - 請參閱 *AVG 更新一章 >>*

您可隨時從使用者介面存取這些連結。一旦您使用快速連結執行特定程序，GUI 將切換至新對話方塊，但快速連結仍然可用。此外，它還以圖形形式描述執行中的程序。

7.4. 元件概觀

*元件概觀*部分位於 AVG 使用者介面的中間。此區域分成兩個部分：

- 所有已安裝元件的概觀，這些元件組成的面板包含元件的圖示以及有關對應元件是在作用中還是非作用中的資訊
- 所選元件的說明

在AVG 9 Anti-Virus plus Firewall 中，*元件概觀*部分包含以下元件的資訊：

- *Anti-Virus* 確保您的電腦受到保護，阻擋嘗試進入您電腦的病毒 - 詳細資訊 >>
- *Anti-Spyware* 在執行時會於幕後掃描您的應用程式 - 詳細資訊 >>
- *Firewall* 控制您的電腦與網際網路或區域網路上其他電腦交換資料的方式 - 詳細資訊 >>
- *Link Scanner* 檢查網際網路瀏覽器中顯示的搜尋結果 - 詳細資訊 >>
- *Anti-Rootkit* 偵測想要隱藏惡意軟體的程式和技術 - 詳細資訊 >>
- *E-mail Scanner* 檢查所有傳入和傳出的郵件是否有病毒 - 詳細資訊 >>
- *授權*顯示授權號碼、授權類型以及到期時間 - 詳細資訊 >>
- *Online Shield* 掃描網頁瀏覽器正在下載的所有資料 - 詳細資訊 >>
- *Resident Shield* 在幕後執行，並在複製、開啟或儲存檔案時，對其進行掃描 - 詳細資訊 >>
- *更新管理員*控制所有 AVG 更新 - 詳細資訊 >>

按一下任何元件的圖示即可在元件概觀中反白該元件。與此同時，元件的基本功能說明會出現在使用者介面的下方。連按兩下圖示可開啟元件本身的介面，其中包含基本統計資料的清單。

在元件圖示上按一下滑鼠右鍵可展開內容功能表：除了開啟元件的圖形介面，您也可以選擇*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 AVG 保持這種狀態，且不願意再收到系統匣圖示的警告。

7.5. 統計資料

*統計資料*部分位於 AVG 使用者介面的左下方。它提供有關程式作業的資訊清單：

- *上次掃描* - 提供執行上次掃描的日期
- *上次更新* - 提供啟動上次更新的日期
- *病毒庫* - 告知目前安裝的病毒庫的版本
- *AVG 版本* - 告知已安裝的 AVG 版本 *(此號碼的格式為 9.0.xx，其中 9.0 是產品系列版本，xx 代表版本編號)*
- *授權到期* - 提供 AVG 授權到期的日期

7.6. 系統匣圖示

系統匣圖示 (*位於 Windows 工具列中*) 顯示 AVG 9 Anti-Virus plus Firewall 目前的狀態。無論 AVG 主視窗是開啟還是關閉，該圖示都會一直顯示在系統匣中。

如果以完全色彩顯示，則該*系統匣圖示*表示所有 AVG 元件都在作用中，且運作完全正常。另外，如果 AVG 處於錯誤狀態，但您完全瞭解這個情形，且特意決定*忽略元件狀態*，則 AVG 系統匣圖示仍會以全彩顯示。

驚嘆號圖示顯示遇到問題 (*元件未啟動、錯誤狀態等等*)。連按兩下*系統匣圖示*可開啟主視窗並編輯元件。

系統匣圖示還能顯示 AVG 目前的活動和可能的應用程式狀態變更 (*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、發生錯誤狀態等等*)，其方法是從 AVG 系統匣圖示彈出一個快顯視窗：

*系統匣圖示*還可用作為快速連結，隨時存取 AVG 主視窗 - 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，其中包含下列選項：

- *開啟 AVG 使用者介面* - 按一下此選項可開啟 AVG 使用者介面
- *更新* - 可啟動即時更新

8. AVG 元件

8.1. Anti-Virus

8.1.1. Anti-Virus 原理

反病毒軟體的掃描引擎會針對已知病毒掃描所有檔案和檔案活動(開啟/關閉檔案等等)。任何偵測到的病毒都會被封鎖以阻止它採取任何動作，接著會被清除或隔離。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。

反病毒保護的重要特點在於不讓已知的病毒在電腦上執行！

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：

- 掃描 - 掃描具備特定病毒特性的字元字串
- 啟發法分析 - 在虛擬電腦環境中動態模擬掃描的物件的指令
- 一般偵測 - 偵測特定病毒/病毒群組的指令特性

AVG 也能夠分析和偵測可能潛伏在系統中的不明可執行應用程式或 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 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。

8.1.2. Anti-Virus 介面

Anti-Virus 元件的介面提供元件功能的一些基本資訊、元件的目前狀態資訊 (*當 Anti-Spyware 元件處於作用中狀態時*)，以及 *Anti-Virus* 統計資料的簡短概觀：

- ***感染定義*** - 此數字提供最新病毒庫版本中已定義的病毒計數
- ***最新資料庫更新*** - 指出病毒庫上一次更新的時間
- ***資料庫版本*** - 定義最新病毒庫版本的編號；此編號將隨著病毒庫的更新而增加

在此元件的介面中，只有一個可操作的按鈕 (***上一步***) - 按下此按鈕可返回預設的 AVG 使用者介面 (元件概觀)。

請注意：*軟體供應商已對所有 AVG 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有經驗的使用者來進行。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。*

8.2. Anti-Spyware

8.2.1. Anti-Spyware 原理

間諜軟體通常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。

還有一種潛在的風險，就是惡意軟體在您安裝 AVG 之前已經傳輸到電腦上，或是因為疏忽而未使 AVG 9 Anti-Virus plus Firewall 保持最新的資料庫及程式更新。有鑑於此，AVG 可讓您使用掃描功能來完整掃描電腦上的惡意軟體/間諜軟體。它還會偵測睡眠中和非作用中的惡意軟體，即已下載但尚未啟動的惡意軟體。

8.2.2. Anti-Spyware 介面

Anti-Spyware 元件的介面提供元件功能的簡短概觀、元件的目前狀態資訊 (*當 Anti-Spyware 元件處於作用中狀態時*)，以及一些 *Anti-Spyware* 統計資料：

- ***間諜軟體定義*** - 此數字提供在最新間諜軟體資料庫版本中已定義的間諜軟體樣本計數
- ***最新資料庫更新*** - 指出間諜軟體資料庫更新的時間
- ***資料庫版本*** - 定義最新間諜軟體資料庫版本的編號；此編號將隨著病毒庫的更新而增加

在此元件的介面中，只有一個可操作的按鈕 (***上一步***) - 按下此按鈕可返回預設的 AVG 使用者介面 (元件概觀)。

請注意：軟體供應商已對所有 AVG 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有經驗的使用者來進行。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。

8.3. Anti-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。

8.4. Firewall

Firewall 是透過封鎖/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。它可控制您的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。

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。

8.4.1. Firewall 原理

在 AVG 中，*Firewall* 元件控制著您電腦每個網路連接埠上的所有通訊。根據所定義的規則，*Firewall* 會對您電腦上執行 (並且想連線到網際網路或本機網路) 的應用程式，或者從外部接觸您的電腦以嘗試連線到您的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，如果該應用程式為不明類型 (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。

***注意：**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，自動切換設定檔

8.4.2. 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，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，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***:
    - ***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，

或是在安全公司網路以外連線到網際網路的筆記型電腦。如果您是從家裡連線，或是位於沒有中央控制的小型公司網路，請選取此選項。另外，當外出以及使用筆記型電腦從各種不明和可能危險的地方 (*網咖、飯店房間等連線時選取此選項。*) 連線時，也請選取此選項。此選項假設這些電腦沒有額外的保護，而需要最大保護，因此會建立限制較多的規則。

- ***網域中的電腦*** – 適用於位於本機網路 (例如學校或公司網路) 中的電腦。它假定網路已受到某些額外措施的保護，這樣便可將安全性層級設為低於獨立電腦的層級。

- ***小型家庭或辦公網路*** – 適用於小型網路 (例如家庭或小公司) 中的電腦，通常只有幾台電腦連線在一起，沒有中心管理員。

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。

8.4.3. Firewall 介面

Firewall 的介面提供了一些關於元件功能的基本資訊，以及 *Firewall* 統計資料的簡要概觀：

- *Firewall 已啟用時間* - 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封鎖封包的數量
- *整體封包* - Firewall 執行期間檢查的所有封包數量

基本元件組態

- *選取 Firewall 設定檔* - 從下拉式功能表選取其中一個定義的設定檔 - 在任何時候都有兩個可用的設定檔 (*分別名為全部允許和全部封鎖*的預設設定檔)，您可以在 *Firewall 設定*中的*設定檔*對話方塊內編輯設定檔，藉此手動新增其他設定檔。
- *啟用遊戲模式* - 核取此選項可確保在執行全螢幕應用程式 (遊戲、PowerPoint 簡報等) 時，*Firewall* 不會顯示對話方塊來詢問您是想要允許還是封鎖不明應用程

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。

- *Firewall **狀態***：
  - *Firewall **已啟用*** - 選取此選項將允許与在所選 *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）*** - 選取此選項可封鎖每個單獨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 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有經驗的使用者來進行。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

- ***組態精靈*** - 按下此按鈕可切換至稱為***電腦使用方式選擇***的對話方塊（*用於安裝程序內*），您可以在相應的對話方塊指定 *Firewall* 元件組態
- ***儲存變更*** - 按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*** - 按下此按鈕可返回預設的 AVG 使用者介面（*元件概觀*）

8.5. E-mail Scanner

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。

8.5.1. E-mail Scanner 原理

E-mail Scanner 元件會自動掃描傳入/傳出電子郵件。您可以將它與在 AVG 中沒有自己的外掛程式的電子郵件用戶端（*例如，Outlook Express、Mozilla、Incredimail 等等）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，就會立即將其隔離到*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*)。

注意：*AVG E-mail Scanner 不適用於伺服器平台！*

8.5.2. E-mail Scanner 介面

在 *E-mail Scanner* 元件的對話方塊中，您可以看到描述元件功能的簡短文字、有關元件目前狀態的資訊 (*當 E-mail Scanner 處於作用中狀態時*)，以及下列統計資料：

- ***已掃描的電子郵件總數*** - 自 *E-mail Scanner* 上次啟動以來所掃描的電子郵件訊息的數量 (*必要時可以重設這個值；例如，為了統計目的 - 重設值*)

- ***已發現和封鎖的威脅數*** - 提供自從上次啟動 *E-mail Scanner* 以來，在電子郵件訊息中偵測到的感染數目

- ***已安裝的電子郵件保護*** - 有關涉及預設安裝電子郵件用戶端的特定電子郵件保護外掛程式的資訊

基本元件組態

在對話方塊底端可以找到名為 *E-mail Scanner* ***設定***的部分，您可以在此編輯元件功能的一些基本功能：

- ***掃描傳入郵件*** - 核取此項目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。在預設狀態下，此項目處於開啟狀態。建議您不要變更此設定！

- ***掃描傳出郵件*** - 核取此項目可確認所有從您的帳戶寄出的電子郵件都應該接受掃描，檢查是否有病毒。此項目預設是處於關閉狀態。

- ***掃描電子郵件時顯示通知圖示*** - 核取此項目表示您希望 *E-mail Scanner* 元件在掃描電子郵件時，在系統匣中的 AVG 圖示上方顯示一個通知對話方塊。在預設情況下，此項目處於開啟狀態。建議您不要變更此設定！

E-mail Scanner 元件的進階組態可透過系統功能表的***工具 / 進階設定***項目來存取；不過只建議由經驗豐富的使用者使用進階組態！

請注意：軟體供應商已對所有 AVG 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有經驗的使用者來進行。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

E-mail Scanner 介面中可用的控制按鈕如下：

- ***儲存變更*** - 按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*** - 按下此按鈕返回到預設 AVG 使用者介面 (元件概觀)

8.5.3. E-mail Scanner 偵測

在 *E-mail Scanner 偵測*對話方塊中 (*可透過系統功能表選項「歷程記錄/E-mail Scanner 偵測」來存取*), 您會看見 *E-mail Scanner* 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 (***匯出清單到檔案***) 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* - 將您切換回預設 *AVG 使用者介面* (元件概觀)

8.6. 授權

在*授權*元件介面中，您會找到描述該元件功能的簡要文字、關於其目前狀態的資訊 (*當元件處於作用中狀態時*)，以及以下資訊:

- *授權號碼* - 提供您授權號碼的準確形式。輸入授權號碼時，您需要完全根據顯示的號碼準確輸入。因此我們強烈建議始終使用「複製和貼上」方法來處理授權號碼。
- *授權類型* - 指出安裝的產品類型。

- *授權到期日期* - 此日期決定您的授權的有效期限。如果您希望在此日期後繼續使用 AVG 9 Anti-Virus plus Firewall，則必須更新您的授權。您可以在 AVG 網站 (http://www.avg.com/) 上進行線上授權更新。

- *席位數* - 您有權在上面安裝 AVG 9 Anti-Virus plus Firewall 的工作站數目。

控制按鈕

- *註冊* - 會連線到 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。

- *重新啟動* - 開啟*啟動 AVG* 對話方塊，其中包含您在安裝程序 的*個性化 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*)。

注意：*如果您使用的是* AVG 9 Anti-Virus plus Firewall *試用版，這兩個按鈕會顯示為現在購買及啟動，讓您可以立刻購買完整版的授權。如果您在安裝* AVG 9 Anti-Virus plus Firewall *時輸入了銷售號碼，這些按鈕會顯示為註冊及啟動。*

- *上一步* - 按下此按鈕可返回至預設 AVG 使用者介面 (元件概觀)。

8.7. Link Scanner

8.7.1. Link Scanner 原理

LinkScanner 元件提供的保護可防禦那些企圖透過網頁瀏覽器或其外掛程式在您電腦上安裝惡意軟體的網站。*LinkScanner* 技術包括兩項功能，即 *AVG Search-Shield* 和 *AVG Active Surf-Shield*：

- *AVG Search-Shield*包含已知危險的網站清單 (*URL 位址*)。當在 Google、Yahoo!、Bing、百度、Altavista 或 Yandex 進行搜尋時，將依據此清單檢查所有搜尋結果，並顯示裁決圖示 (*對於 Yahoo!搜尋結果，僅會顯示「惡意探索網站」裁決圖示*)。同時，如果您直接在瀏覽器中鍵入某個位址，或按一下任意網站上 (或電子郵件中) 的連結，這些都會自動經過檢查，並在必要時加以封鎖。

- *AVG Active Surf-Shield*會掃描您正在造訪的網站的內容，無論網站位址為何。即使 *AVG Search Shield* 未偵測出某個網站 (*例如，當建立了新的惡意網站，或當之前安全的網站現在包含了某個惡意軟體時*)，但是當您嘗試造訪該網站時，還是會被 *AVG Active Surf-Shield* 偵測出來並加以封鎖。

注意：AVG Link Scanner 不適用於伺服器平台！

8.7.2. Link Scanner 介面

LinkScanner 元件由兩部分組成，您可以在 *LinkScanner 元件*介面中開啟/關閉它們：

LinkScanner 元件介面提供了元件功能的簡短說明，以及有關其目前狀態的資訊（*LinkScanner 處於作用中狀態*）。您接下來會發現最新的 *LinkScanner* 資料庫版本號碼（*LinkScanner 版本*）的相關資訊。

在對話方塊底端，您可以編輯數個選項：

- *啟用 AVG Search-Shield* - (*預設情況下為開啟*)：在 Google、Yahoo!、Bing、百度、Yandex 或 Altavista 中執行搜尋時，會在搜尋引擎傳回站點內容前進行檢查，並顯示告示性通知圖示。
- *啟用 AVG Active Surf-Shield* - (*預設情況下為開啟*)：在存取木馬攻擊探測站點時，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，其連線及其木馬攻擊探測內容將被封鎖。
- *啟用將偵測到的威脅報告給 AVG* - 勾選此項目可允許舉報使用者透過 *Safe*

Surf 或 *Safe Search* 發現的木馬攻擊程式和惡意站點，從而為收集網頁惡意活動資訊的資料庫提供資訊。

8.7.3. AVG Search-Shield

在 *AVG Search-Shield* 開啟狀態下搜尋網際網路時，從最常用的搜尋引擎 (例如 Yahoo!、Google、Bing、Altavista、Yandex 等等) 傳回的所有搜尋結果都會經過評估，確認是否含有危險或可疑的連結。透過檢查這些連結並標示惡意連結，*AVG Link Scanner* 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 (*在 AVG Security Toolbar 內使用 Yahoo! 搜尋引擎不會顯示此圖示！*)。
- 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，您不能造訪該頁面。
- 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。這些資訊包括威脅的額外詳細資訊 (若有的話)、連結的 IP 位址，以及 AVG 掃描頁面的時間：

8.7.4. AVG Active Surf-Shield

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被木馬攻擊程式入侵的網頁感染您的電腦，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，*AVG Link Scanner* 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，*AVG Link Scanner* 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！

8.8. Online Shield

8.8.1. Online Shield 原理

Online Shield 是一種即時常駐保護；它甚至可在將要造訪的網頁的內容 (以及這些網頁中可能包含的檔案) 顯示於網頁瀏覽器中或下載到您的電腦之前即進行掃描。

Online Shield 會偵測到您即將造訪的網頁包含一些危險的 javascript，並會阻止該網頁的顯示。此外，它還可以識別網頁中包含的惡意軟體，並立即阻止這些惡意軟體的下載，使其永遠不會侵入您的電腦。

注意：*AVG Online Shield 不適用於伺服器平台！*

8.8.2. Online Shield 介面

Online Shield 元件的介面描述了此類保護的行為。此外，您還可以找到該元件目前狀態的資訊 (*Online Shield 處於作用中狀態，且運作完全正常。*)。接著，您可以在此對話方塊的底部找到該元件功能的基本編輯選項。

基本元件組態

首先，您可以核取*啟用 Online Shield* 項目，選擇立即開啟/關閉 *Online Shield*。該選項預設情況下為啟用，且 *Online Shield* 元件處於作用中狀態。但是，如果您沒有變更此設定的必要，我們建議您使該元件保持作用中狀態。如果核取了該項目，且 *Online Shield* 處於執行中，則在以下兩個標籤中會出現其他可編輯的組態選項：

- ***網頁*** - 您可以編輯該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：

o ***網頁保護*** - 此選項確認 *Online Shield* 應掃描 www 網頁的內容。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*** - 掃描要顯示的 www 網頁中可能包含的封存的內容
  - ***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。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，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。
  - ***報告延伸性的潛在垃圾程式*** – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正

常而且無害，但稍後可能會被不肖份子用來作惡。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*** - 使用啟發法分析方法（例如：在虛擬電腦環境中模擬和評估掃描物件的指令）來掃描要顯示的網頁內容。因此，它甚至能偵測到尚未在病毒庫中說明的惡意代碼（*請見* *Anti-Virus 原理*）。

- ***待掃描檔案的最大大小*** - 如果包含的檔案列示在顯示的頁面中，則您甚至還可以在將其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。您可以使用滑杆來指定仍使用 *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。

- ***即時訊息*** - 允許您編輯該元件中有關即時訊息（*例如 ICQ、MSN Messenger、Yahoo...*）掃描的設定。

o 即時訊息保護 - 如果您希望 Online Shield 驗證線上通訊是否未遭受病毒侵入，則核取此項目。如果啟用此選項，可以進一步指定您想要控制哪些即時訊息應用程式 - 目前，AVG 9 Anti-Virus plus Firewall 支援 ICQ、MSN 和 Yahoo 應用程式。

*請注意：軟體供應商已對所有 AVG 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有經驗的使用者來進行。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

以下是 *Online Shield* 介面中提供的控制按鈕：

- ***儲存變更*** - 按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*** - 按下此按鈕可返回預設的 AVG 使用者介面 (*元件概觀*)

8.8.3. Online Shield 偵測

Online Shield 甚至會在造訪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：

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* - 偵測到的物件的說明 (*甚至可能包含名稱*)
- *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 (*匯出清單到檔案*) 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 *Online Shield* 偵測到的結果清單。使用*上一步*按鈕可切換回預設的 *AVG 使用者介面* (元件概觀)。

8.9. Resident Shield

8.9.1. Resident Shield 原理

Resident Shield 元件可為您的電腦提供持續保護。它會掃描正在開啟、儲存或複製的每一個檔案，並保護電腦的系統區域。當 *Resident Shield* 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。此程式一般在「幕後」執行，因此您甚至不會注意到它，它只會在發現威脅時通知您；同時，*Resident Shield* 會封鎖該威脅的啟動並將其移除。*Resident Shield* 會在系統啟動期間載入電腦的記憶體中。

警告：*Resident Shield* ***會在電腦啟動時載入電腦的記憶體，因此始終讓*** *Resident Shield* ***保持開啟狀態十分必要。***

8.9.2. Resident Shield 介面

除了包含最重要的統計資料和元件目前狀態資訊的概觀 (*Resident Shield 處於作用中並正常運作*), *Resident Shield* 介面還提供一些基本元件設定選項。統計資料如下:

- *Resident Shield **作用中時間*** - 提供自最近一次啟動元件以來所耗的時間
- ***已偵測到和封鎖的威脅數*** - 已被阻止執行/開啟的偵測到的感染數量 (*如有必要, 可重設該值; 例如, 用於統計資料用途 - 重設值*)

基本元件組態

在對話方塊視窗的底部, 您將找到名為 *Resident Shield **設定***的部分, 您可在其中編輯元件功能的一些基本設定 (*與所有其他元件一樣, 詳細組態可從系統功能表的「工具/進階設定」項目存取*)。

*Resident Shield **作用中***選項可讓您輕鬆開啟/關閉常駐保護。預設情況下, 此功能為開啟。常駐保護開啟時, 您可進一步決定對可能偵測到的感染的處理 (移除) 方式:

- 自動移除 (***自動移除所有威脅***)
- 或僅在使用者批准後移除 (***移除威脅前詢問我***)

此選擇不會對安全性層級產生影響, 僅反映您的偏好。

在以上兩種情況中, 您仍可選取是否要***掃描追蹤 cookie***。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。(*cookie = 伺服器傳送給網頁瀏覽器的文字封包, 隨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, 如站點偏好設定或電子購物車內容*).

***請注意**: 軟體供應商已對所有 AVG 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有經驗的使用者來進行。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

以下是 *Resident Shield* 介面中提供的控制按鈕:

- ***管理例外*** - 開啟 *Resident Shield - **排除目錄***對話方塊, 您可在其中定義應從 *Resident Shield* 掃描排除的資料夾
- ***儲存變更*** - 按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* - 按下此按鈕返回到預設 *AVG 使用者介面* (元件概觀)

8.9.3. Resident Shield 偵測

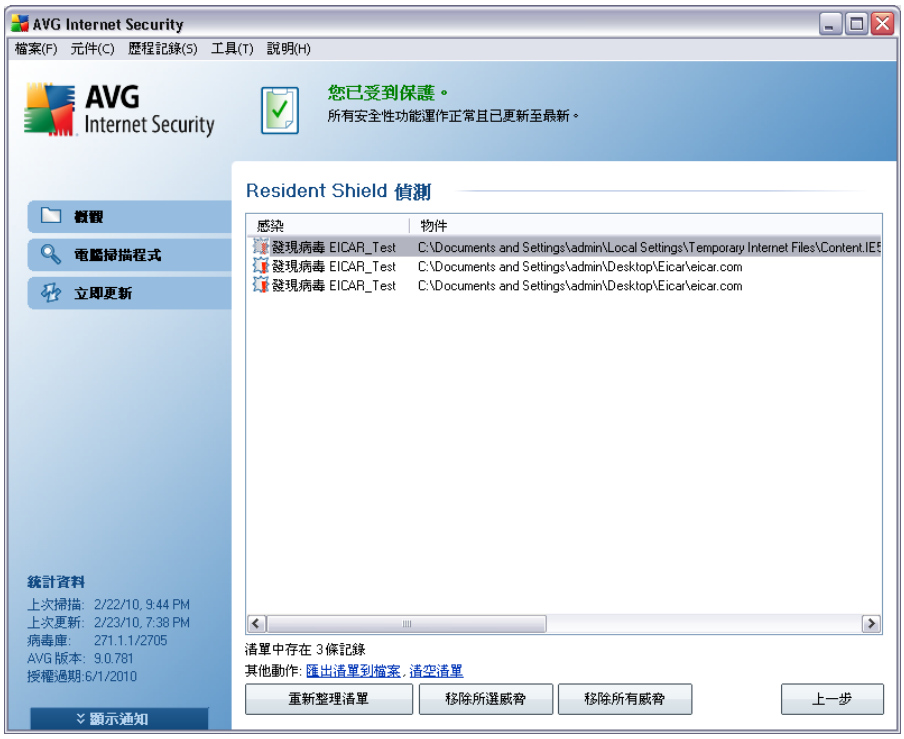
Resident Shield 會在複製、開啟或儲存檔案的同時對其進行掃描。當偵測到病毒或任何類型的威脅時，將立即透過以下對話方塊向您發出警告：

此對話方塊提供有關偵測到的威脅的資訊，並詢問您目前要採取的措施：

- *修復* - 如果有可用的修復方法，AVG 將自動修復受感染的檔案；建議採用此選項
- *移至隔離區* - 病毒將移至 AVG *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* - 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！

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 結果*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 (***匯出清單到檔案***) 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。使用***上一步***按鈕可切換回預設的 *AVG 使用者介面* (元件概觀)。

8.10. 更新管理員

8.10.1. 更新管理員原理

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，軟體供應商們不斷發行更新和安全性補充程式，以修正發現的所有安全性漏洞。

定期更新您的 AVG 是至關重要的！

更新管理員會幫助您控制定期更新。透過此元件，您可以排程從網際網路或本機網路自動下載更新檔案。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。

注意：請留意 AVG 更新一章，以瞭解有關更新類型和層級的資訊！

8.10.2. 更新管理員介面

*更新管理員*的介面顯示有關該元件的功能及其目前狀態 (*更新管理員處於作用中狀態*) 的資訊，並提供相關統計資料：

- ***最新更新*** - 指定資料庫更新的日期和時間
- ***病毒庫版本*** - 定義最新病毒庫版本的編號；此編號將隨著病毒庫的每次更新而增加
- ***下一次排程的更新*** - 指定將資料庫排程在何時再次進行更新。

基本元件組態

在此對話方塊的底部，您可以找到***更新管理員設定***部分，在這裡您可以變更啟動更新程序的一些規則。您可以定義是要自動下載更新檔案 (***開始自動更新***) 還是按需下載。預設情況下，會開啟***開始自動更新***選項，我們建議保持這個設定！定期下載最新的更新檔案，是保證任何安全性軟體正常運作的關鍵！

此外，還可以定義啟動更新的時間：

- ***定期*** - 定義時間間隔
- ***在特定時間*** - 定義確切的日期和時間

預設情況下，會設定每隔 4 個小時更新一次。強烈建議保持該設定，除非您確實需要對其執行變更！

請注意：*軟體供應商已對所有 AVG 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有經驗的使用者來進行。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

*更新管理員*介面中可用的控制按鈕如下：

- ***立即更新*** - 可按需啟動即時更新
- ***儲存變更*** - 按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*** - 按下此按鈕返回到預設 *AVG 使用者介面* (元件概觀)

9. AVG Security Toolbar

AVG Security Toolbar 是一款可與 *AVG Link Scanner* 元件搭配運作的新工具，用於檢查支援的網際網路搜尋引擎 (*Yahoo!*、*Google*、*Bing*、*Altavista*、*百度*) 的搜尋結果。*AVG Security Toolbar* 可用來控制 *AVG Link Scanner* 的功能並調整其行為。

如果您在安裝 AVG 9 Anti-Virus plus Firewall 時選擇安裝 Toolbar，它會自動新增至您的網頁瀏覽器。如果您用的是其他網際網路瀏覽器 (*如 Avant Browser*)，可能會遇到無法預期的行為。

9.1. AVG Security Toolbar 介面

AVG Security Toolbar 設計用於和 *MS Internet Explorer* (*6.0 版或更新版本*) 及 *Mozilla Firefox* (*2.0 版或更新版本*) 搭配運作。一旦您決定要安裝 *AVG Security Toolbar* (*在 AVG 安裝程序期間，會詢問您是否決定要安裝該元件*)，該元件就會出現在網頁瀏覽器的位址列正下方：

請注意：*AVG Security Toolbar 不適用於伺服器平台！*

AVG Security Toolbar 由以下部分構成：

- *AVG **標誌*** - 可存取一般工具列項目。按一下標誌按鈕即可重新導向至 AVG 網站 (http://www.avg.com/)。按一下 AVG 圖示旁的指標將開啟下列項目：
    - *Toolbar **資訊*** - 連結到 *AVG Security Toolbar **首頁，其中包含有關工具列保護的詳細資訊。***
    - *啟動 AVG 9 Anti-Virus plus Firewall* - 開啟 AVG 9 Anti-Virus plus Firewall 使用者介面
    - ***選項*** - 將開啟一個組態對話方塊，您可以在這裡調整 *AVG Security Toolbar* 設定以配合您的需要 - 請參閱下一章 *AVG Security Toolbar **選項***
    - ***刪除歷程記錄*** - 可讓您*刪除 AVG Security Toolbar 的全部歷程記錄*，或*刪除搜尋歷程記錄*、*刪除瀏覽器歷程記錄*、*刪除下載歷程記錄*以及*刪除 cookie*。

- *更新* - 檢查 *AVG Security Toolbar* 的新更新
- *說明* - 提供選項來開啟說明檔案、提出有關產品的回饋意見，或檢視工具列目前版本的詳細資訊

- *搜尋方塊* - 在搜尋方塊中輸入一個字或詞。無論您在哪個頁面中，只要按一下*搜尋*，即可使用指定的搜尋引擎來進行搜尋 (*您可以在 AVG Security Toolbar 進階選項中指定您想使用的搜尋引擎，包括 Yahoo!、Wikipedia、百杜、WebHledani 和 Yandex*)。搜尋方塊也會列出搜尋歷程記錄。軟件會使用 *AVG Search-Shield* 保護功能對透過搜尋方塊完成的搜尋進行分析。
- *完全保護* - 視您的AVG 9 Anti-Virus plus Firewall組態
- *頁面狀態* - 位於工具列中，該按鈕依據 *AVG Search-Shield* 元件的標準來顯示它對目前上傳網頁的評估 (*安全/可疑/肯定危險/包含威脅/無法掃描*)。按一下此按鈕可開啟資訊欄，顯示有關該網頁的詳細資訊。
- *AVG 資訊* - 提供位於 AVG 網站 (http://www.avg.com/) 上重要安全性資訊的連結。
  - *Toolbar 資訊* - 連結到 *AVG Security Toolbar 首頁，其中包含有關工具列保護的詳細資訊。*
  - *關於威脅* - 開啟 AVG 網站，提供目前網際網路上有關病毒及威脅的資訊。
  - *AVG 新聞* - 會開啟提供最新的 AVG 相關新聞稿的網頁。
  - *目前威脅層級* - 會開啟病毒實驗室網頁，以圖形顯示網路上目前的威脅層級。
  - *病毒大全* - 會開啟病毒大全頁面，您可以在此頁面依名稱搜尋特定的病毒，並取得各病毒的詳細資訊。

9.2. AVG Security Toolbar 選項

所有 *AVG Security Toolbar* 參數組態均可直接在 *AVG Security Toolbar* 面板內存取。透過 *AVG/選項*工具列功能表項目，可在稱為 *Toolbar 選項*的新對話方塊中開啟編輯介面，此對話方塊分為四個部分：

9.2.1. 一般設定標籤

您可以在此標籤上指定應該在 *AVG Security Toolbar* 面板內顯示/隱藏的工具列控制按鈕：選擇您想顯示的任何按鈕。此外，您也可以找到工具列每個按鈕的功能說明：

- *AVG **新聞按鈕*** -
- ***新聞按鈕*** - 此按鈕以結構化的總覽提供每日最新新聞內容
- *AVG **資訊按鈕*** - 此按鈕提供有關 AVG 工具列、目前威脅及網路威脅層級的資訊，開啟病毒大全，並提供其他 AVG 產品新訊
- ***刪除歷程記錄按鈕*** - 此按鈕可讓您直接從 AVG Security Toolbar 面板刪除全部歷程記錄或刪除搜尋歷程記錄、刪除瀏覽器歷程記錄、刪除下載歷程記錄或刪除 cookie。

9.2.2. 有用按鈕標籤

*有用按鈕*標籤讓您從一份清單中選擇應用程式，將其圖示加進工具列介面中。這些圖示就是可立即開啟相應的應用程式的快速連結。

9.2.3. 安全性標籤

*安全性*標籤分為兩個部分，即 *AVG 瀏覽器安全性*和*等級*，您可以在此核取特定的核取方塊，以指定您想要使用的 *AVG Security Toolbar* 功能。

- *AVG 瀏覽器安全性* - 核取此項目可啟動或關閉 *AVG Search-Shield* 和/或 *AVG Active Surf-Shield* 服務
- *等級* - 根據您想要使用的 *AVG Search-Shield* 元件，選取要用於搜尋結果等級的圖形符號：
  -  頁面安全
  -  頁面有些可疑
  -  頁面包含確定是危險頁面的連結
  -  頁面包含作用中的威脅
  -  頁面無法存取，因此無法掃描

核取相應選項，確認您想要收到關於此特定威脅層級的通知。但是，您不能關閉紅色

標記的顯示，因為這是指派給內含作用中且危險威脅的頁面。***再次強調，除非您確實需要變更，否則建議保留程式廠商設定的預設組態！***

9.2.4. 進階選項標籤

在標籤*進階選項*中，首先選擇您要設為預設的搜尋引擎。您可以選擇*Yahoo!*、*百度*、*WebHledani* 或 *Yandex*。變更預設搜尋引擎之後，您必須重新開啟網路瀏覽器，變更才會生效。

接下來，您可以啟動或關閉各項 *AVG Security Toolbar* 設定：

- ***將 Yahoo! 設定並保留為位址列的搜尋提供者*** - (*預設情況下為開啟*) - 核取此選項後，您可以直接將搜尋關鍵字輸入網際網路瀏覽器的位址列中，而且會自動使用 Yahoo! 服務來搜尋相關網站。
- ***讓 AVG 對瀏覽器導覽錯誤提供建議 (404/DNS)*** - (*預設為開啟*) - 如果您在搜尋網路時遇到不存在的頁面，或者頁面無法顯示 (404 error)，您將被自動重新導向至一個總覽頁面，您可在此選取其他相關主題的網頁。
- ***將 Yahoo! 設定並保留為您的瀏覽器的搜尋提供者*** - (*預設情況下為關閉*) - Yahoo! 是 AVG Security Toolbar 內進行網路搜尋的預設搜尋引擎，若啟用此選項，它也會成為您網頁瀏覽器的預設搜尋引擎。
- ***重新顯示隱藏的 AVG Security Toolbar (每週)*** - (*預設情況下為開啟*) - 此選項

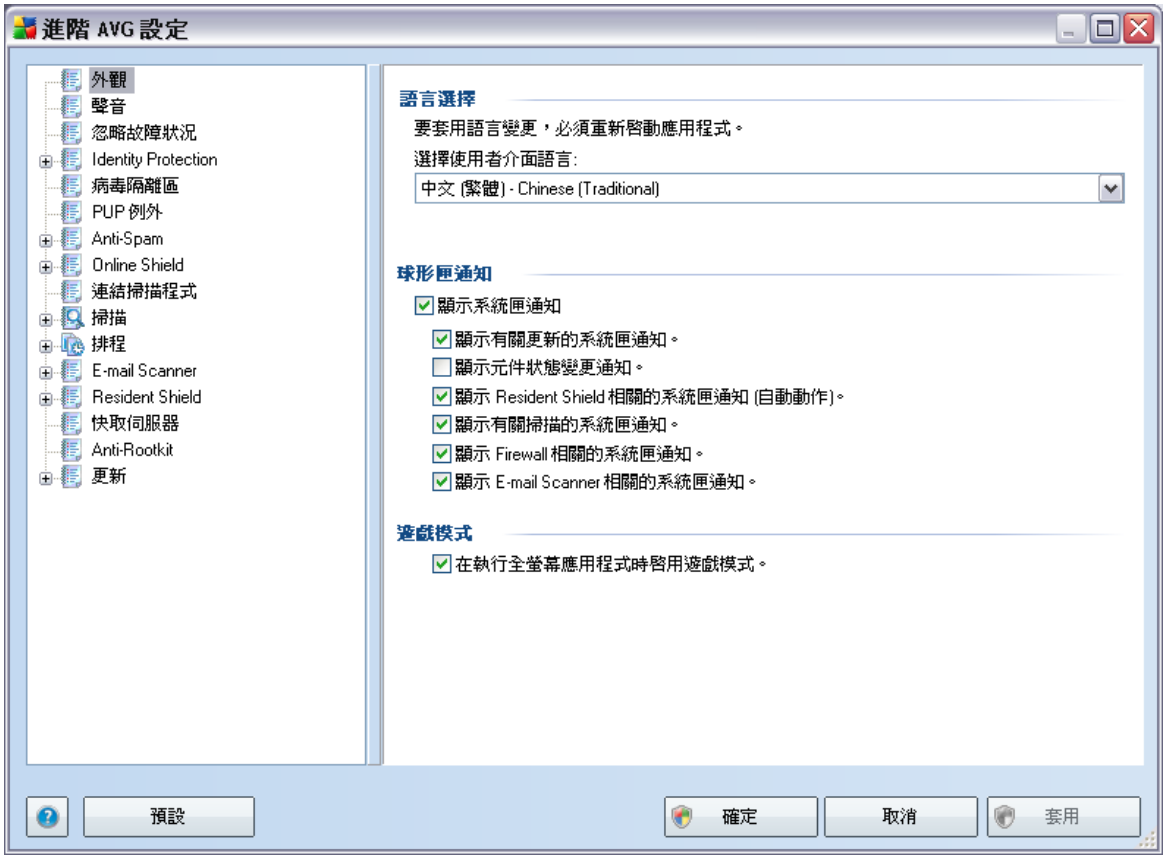
預設處於作用中狀態，當您的 *AVG Security Toolbar* 不小心被隱藏起來時，它會在一個星期內重新顯示。

10. AVG 進階設定

AVG 9 Anti-Virus plus Firewall 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 使用者介面的一般設定，還有一些應用程式行為的基本選項：



語言選擇

在*語言選擇*部分，您可以從下拉式功能表選擇所需語言；整個 AVG 使用者介面接著會套用該語言。下拉式功能表僅提供您之前在安裝程序中選取要安裝的語言 (請參閱自訂安裝 - 元件選取一章)。不過，若要完成將應用程式切換成另一種語言的作業，您必須重新啟動

使用者介面；請遵循以下步驟：

- 選取所需的應用程式語言，並按*套用*按鈕（右下角）來確認您的選擇
- 按*確定*按鈕確認
- 隨即會顯示新的對話方塊視窗，告知您必須重新啟動應用程式才能變更 AVG 使用者介面的語言：

球形匣通知

在此部分，您可以隱藏有關應用程式狀態的系統匣球形通知。預設情況下會允許顯示球形通知，建議您保留此組態！球形通知一般會告知 AVG 元件的狀態變更，您應該注意這類通知！

但是如果出於某種原因，您決定不要顯示這些通知，或者只要顯示特定通知（關於特定的 AVG 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*** - 預設情況下會核取此項目（*已開啟*），而且將顯示通知。取消核取此項目將完全關閉所有球形通知的顯示。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*** - 決定是否要顯示有關 AVG 更新程序啟動、進度及完成的資訊；
  - ***顯示元件狀態變更通知*** - 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。當報告元件的錯誤狀態時，此選項如同系統匣圖示的通知功能（色彩變更），會報告任何 AVG 元件中的問題；
  - ***顯示有關 Resident Shield 的系統匣通知*** - 決定是顯示還是抑制有關檔案儲存、複製或開啟程序的資訊（*只有當 Resident Shield 的自動修復功能啟動時，*）該組態才會顯示；
  - ***顯示有關掃描的系統匣通知*** - 決定是否要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*** - 決定是否要顯示有關 Firewall 狀態和程序的資訊，例如元件的啟動/停用警告、可能的流量封鎖等等；

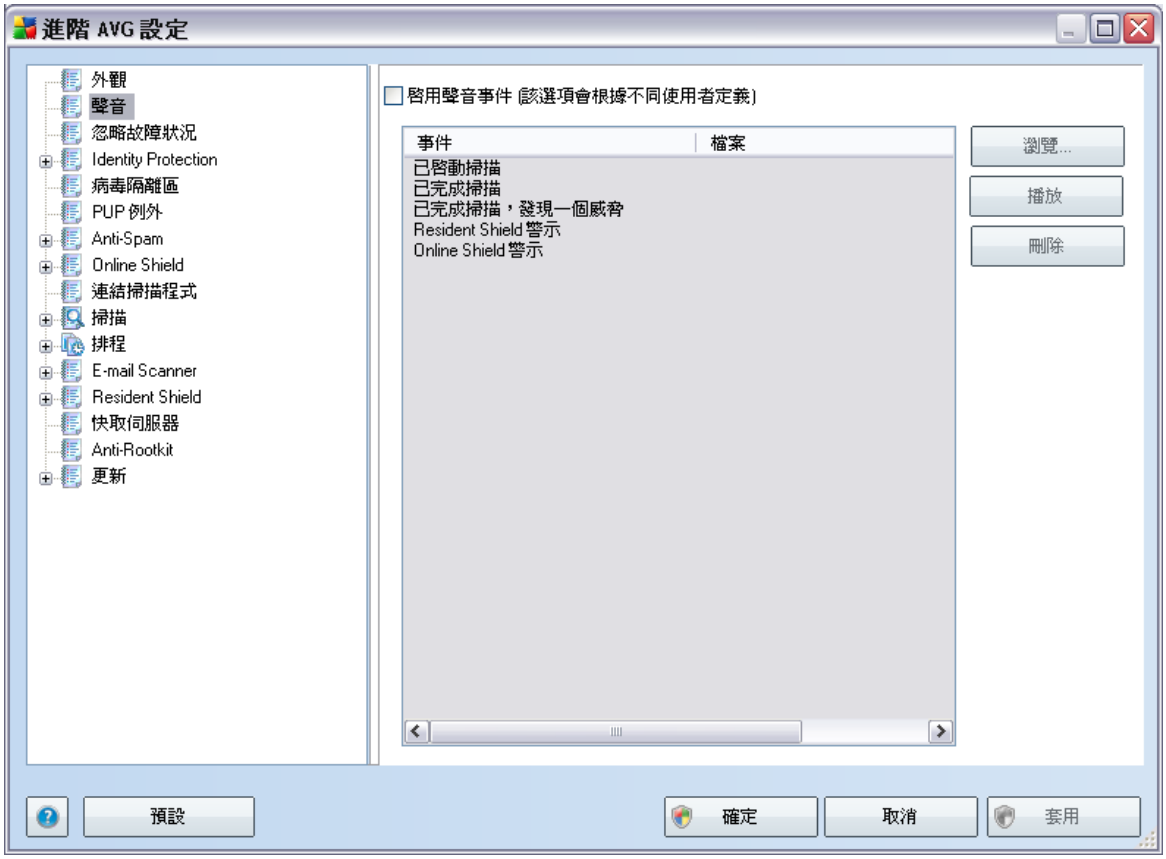
- ***顯示 E-mail Scanner 相關的系統匣通知*** - 決定是否要顯示有關所有傳入和傳出電子郵件訊息掃描的資訊。

遊戲模式

此功能是用於當 AVG 的訊息泡泡 (*例如排程掃描開始*) 可能干擾全螢幕應用程式的執行時 (*它們會使應用程式縮小化或破壞其圖像*)。若要避免發生這種情況，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

在*聲音*對話方塊中，您可以指定是否想要透過聲音通知功能收到特定 AVG 動作的通知。若是如此，請核取*啟用聲音事件*選項（*預設情況下為關閉*）即可啟動 AVG 動作清單：

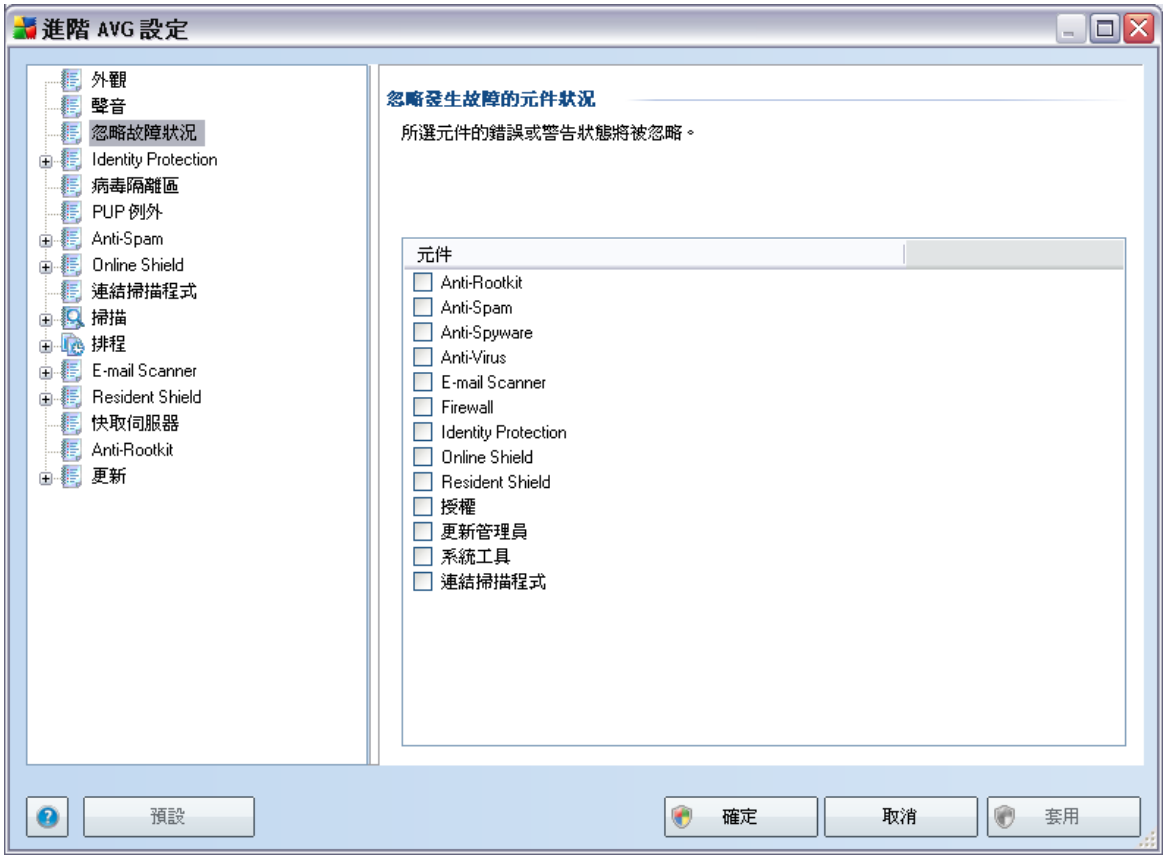


接著，從清單中選取相應事件，並瀏覽（*瀏覽*）您的磁碟以尋找要指派給此事件的適當聲音。若要聆聽所選的聲音，請在清單中反白該事件，再按*播放*按鈕。使用*刪除*按鈕即可移除指派給特定事件的聲音。

*注意：只支援 *.wav 聲音！*

10.3. 忽略故障狀況

在*忽略故障元件狀況*對話方塊中，您可以勾選不希望收到有關其通知的元件：



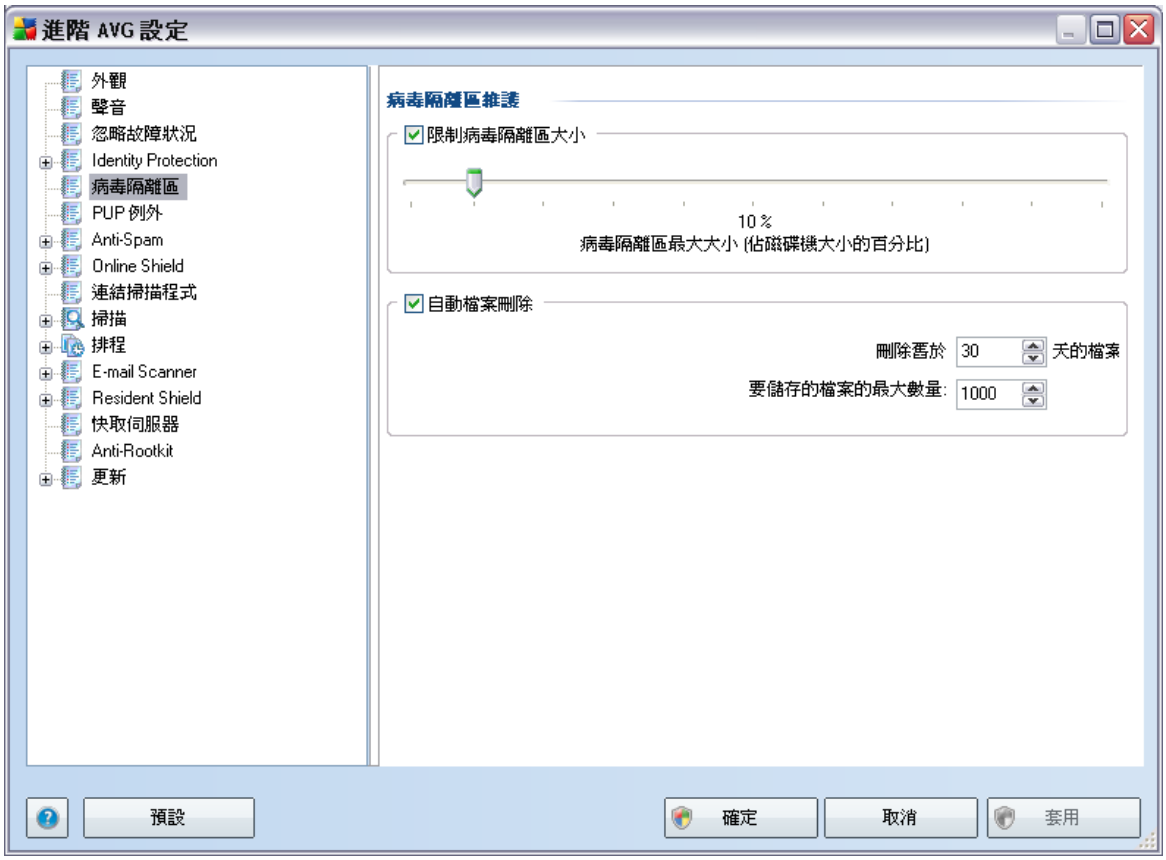
預設情況下，此清單中沒有選取任何元件。這意味著一旦有元件變為錯誤狀態，將立即透過以下方式通知您：

- *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，
- 現有問題的文字說明位於 AVG 主視窗的*安全性狀態資訊*部分

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，但不排除會發生以上情況*)。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*忽略元件狀態*選項，可直接從 AVG 主視窗中的元件概觀存取。

10.4. 病毒隔離區

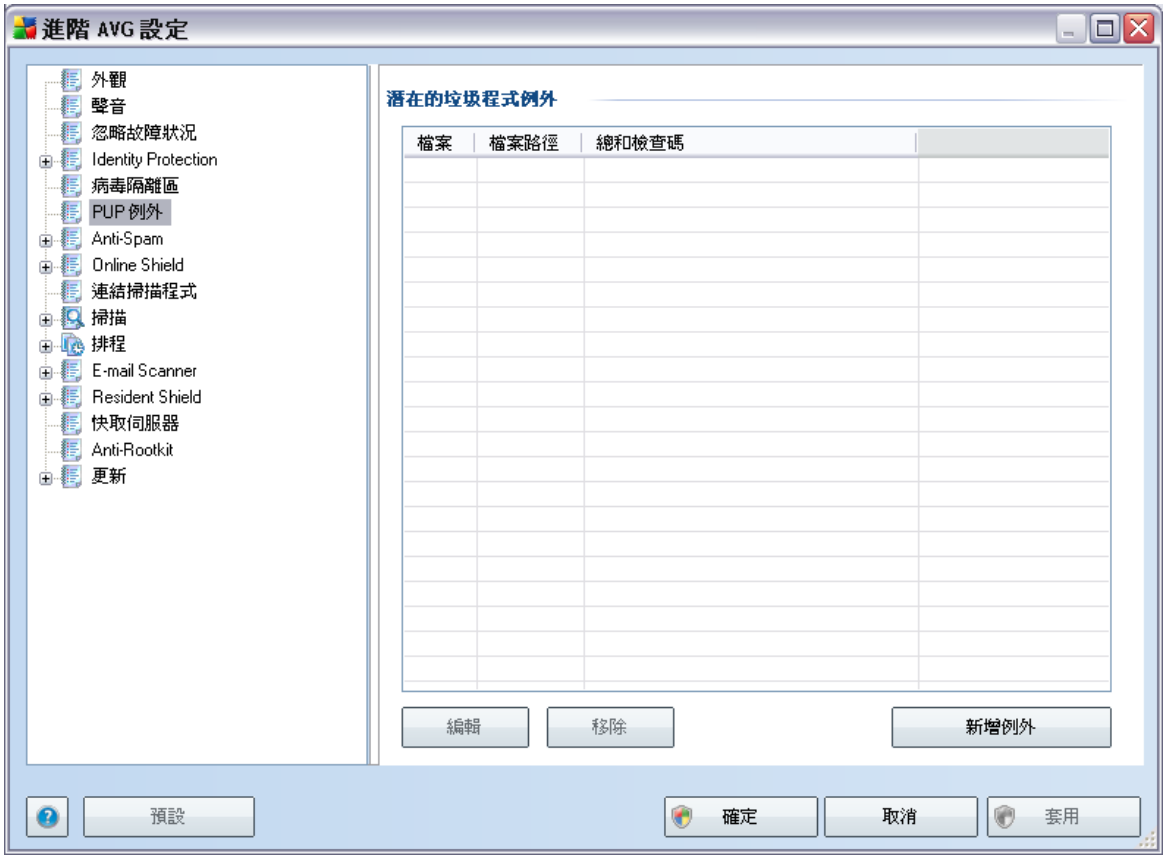


*病毒隔離區維護*對話方塊可讓您定義多個參數，這些參數與管理儲存在*病毒隔離區*中的物件有關：

- *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* - 在此部分定義物件可以儲存在*病毒隔離區*的最長時間 (*刪除 ... 天以上的檔案*) 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*)

10.5. PUP 例外

AVG 9 Anti-Virus plus Firewall 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。在某些情況下，使用者可能希望將特定的垃圾程式保留在電腦上 (*故意安裝的程式*)。一些程式 (尤其是免費的) 包含廣告軟體。AVG 可能會將此類廣告程式偵測和報告為*潛在垃圾程式*。如果您想在電腦上保留此類程式，可將其定義為潛在垃圾程式例外：



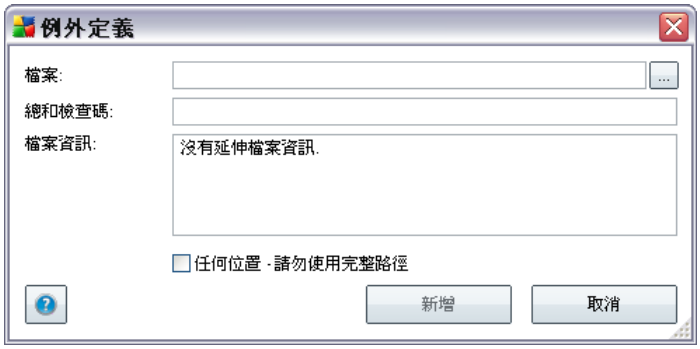
*潛在垃圾程式例外*對話方塊會顯示已定義且目前有效的潛在垃圾程式例外的清單。您可以編輯清單、刪除現有項目，或新增例外。針對每一項例外，均可在清單中找到下列資訊：

- *檔案* - 提供相應應用程式的名稱
- *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產生的字元字串，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

產生和顯示。

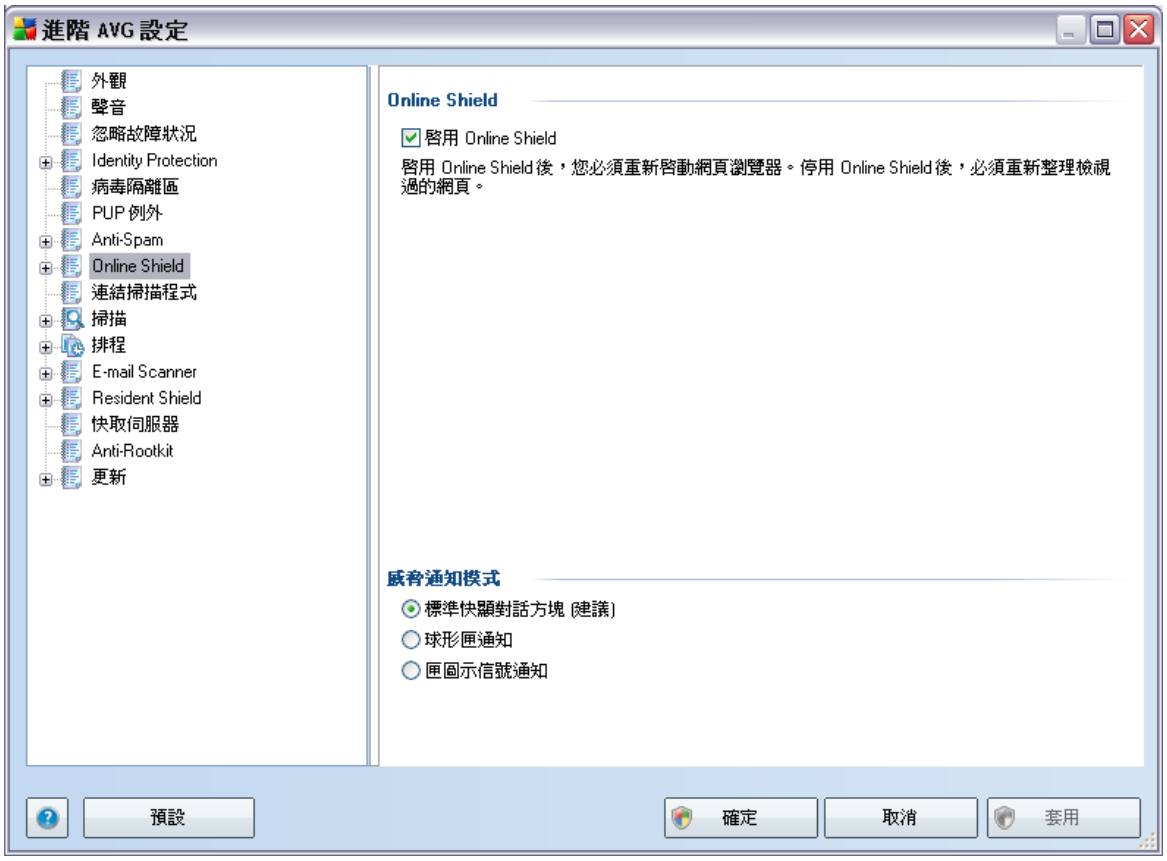
控制按鈕

- ***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*** - 輸入您想標示為例外的檔案的完整路徑
  - ***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產生的字元字串，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產生和顯示。
  - ***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

10.6. Online Shield



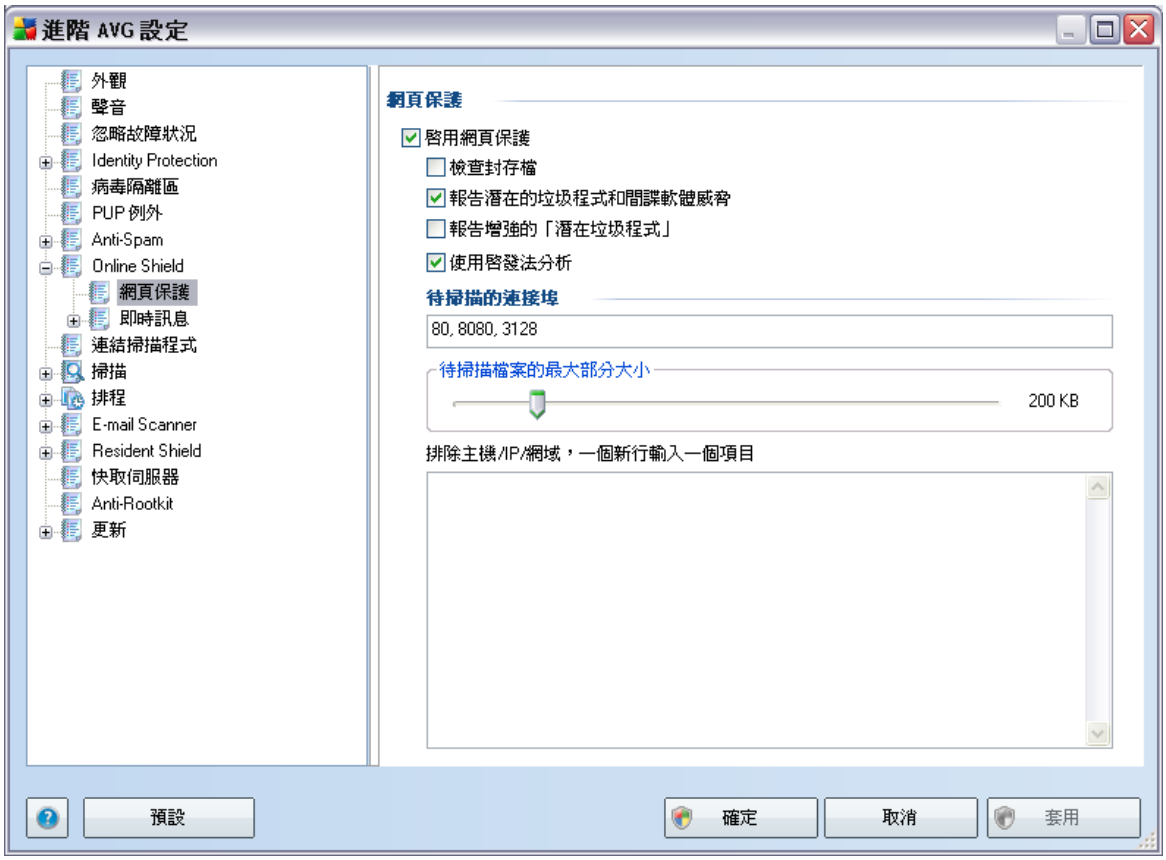
*網頁保護*對話方塊可讓您透過*啟用 Online Shield* 選項 (*預設已啟動*) 啟動/停用整個 *Online Shield* 元件。有關此元件的其他進階設定，請繼續至樹狀巡覽目錄中列出的後幾個對話方塊：

- *網頁保護*
- *即時訊息*

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。

10.6.1. 網頁保護



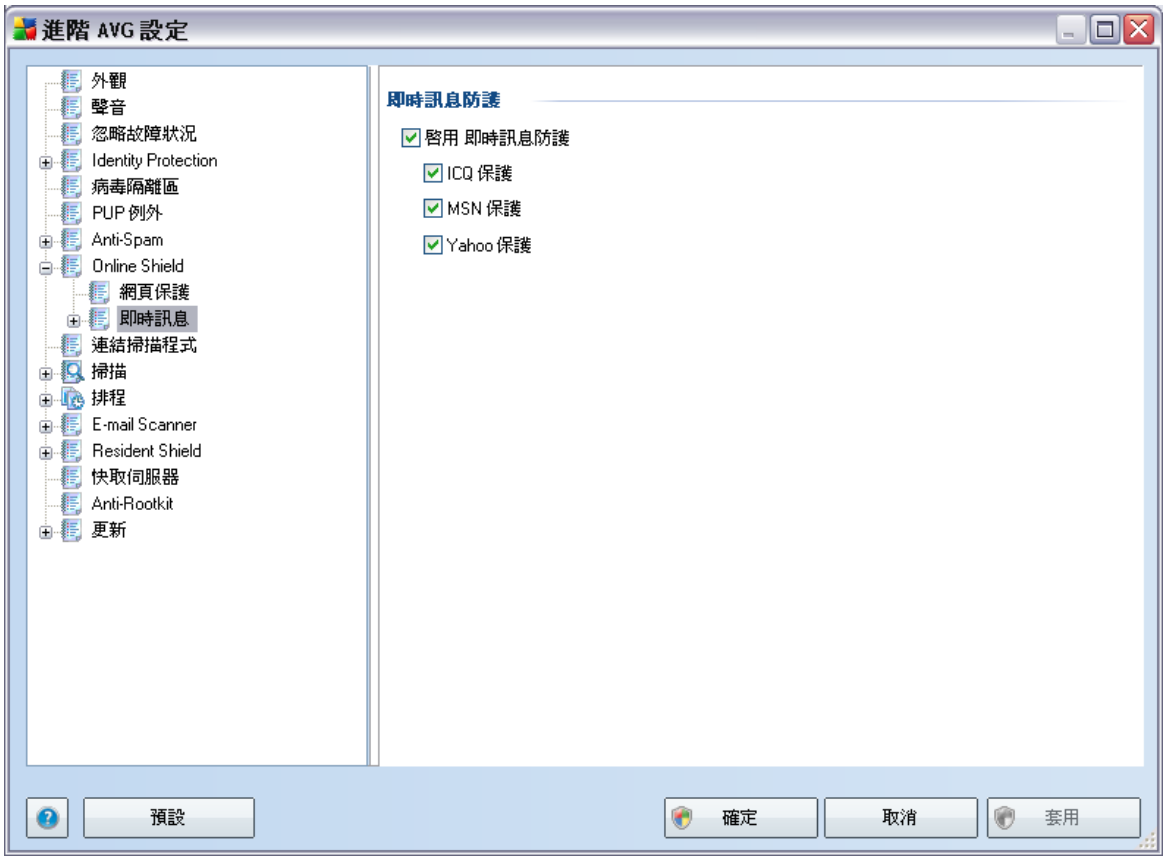
在*網頁保護*對話方塊中，您可以編輯元件中有關網站內容掃描的組態。編輯介面可讓您設定以下基本選項：

- *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* - 掃描要顯示的 www 網頁中可能包含的封存的內容。
    - *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。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，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。
    - *報告延伸性的潛在垃圾程式* – 當前一個選項啟動之後，您也可以核取此方

塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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*** - 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。
- ***待掃描的連接埠*** - 此欄位會列出標準 http 通訊接埠號。如果您的電腦組態不同，可以視需要變更連接埠號。
- ***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。您可以使用滑杆來指定仍使用 *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。

10.6.2. 即時訊息

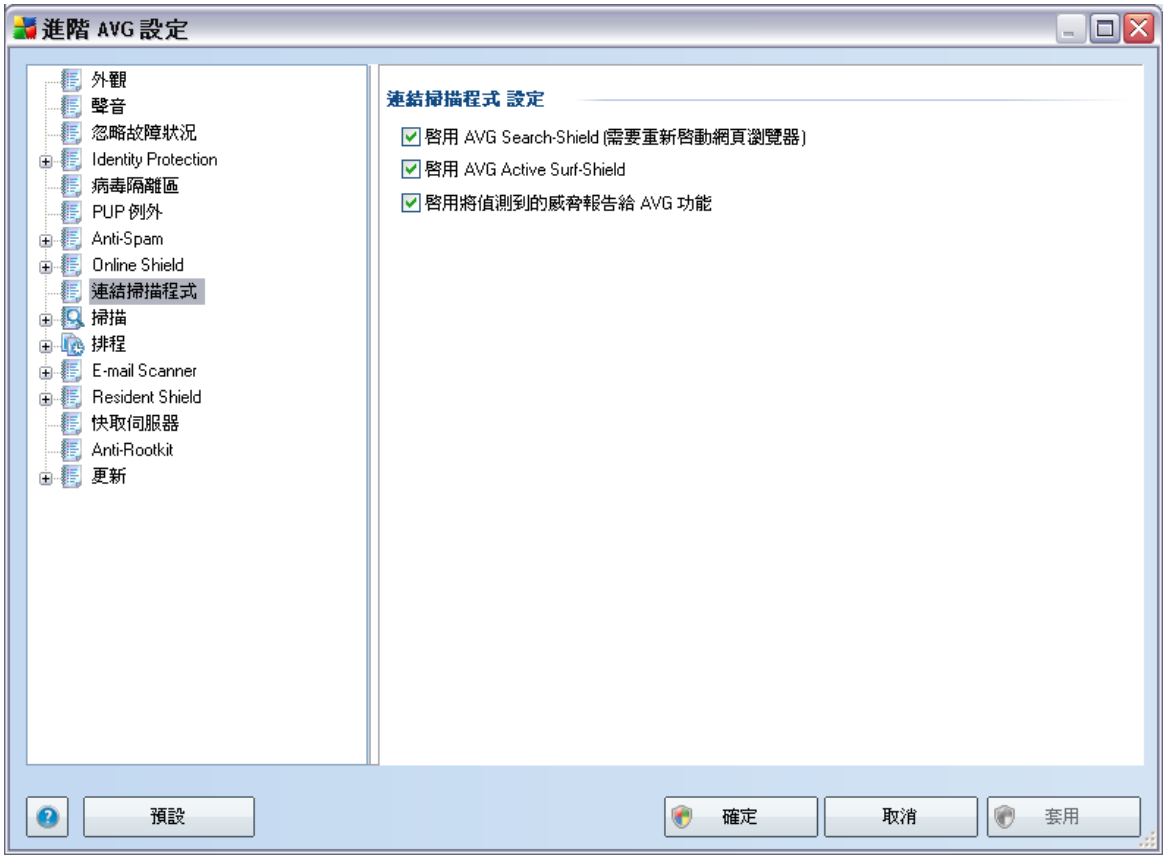


在*即時訊息防護*對話方塊中，您可以編輯關於即時訊息掃描的 *Online Shield* 元件設定。目前支援以下三種即時訊息程式：*ICQ*、*MSN* 和 *Yahoo* - 如果您希望 *Online Shield* 驗證線上通訊確實沒有病毒，請勾選您要的項目。

若要進一步指定允許/封鎖的使用者，您可以查看和編輯各自的對話方塊（*ICQ **進階設定***、*MSN **進階設定***、*Yahoo **進階設定***），並指定*白名單*（*允許與您通訊的使用者清單*）和*黑名單*（*應該封鎖的使用者*）。

10.7. Link Scanner

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



- *啟用 AVG Search-Shield-* (*預設為開啟*)：在 Google、Yahoo!、Bing、Yandex、Altavista 或百度中執行搜尋時，會在搜尋引擎傳回站點內容前進行檢查，並顯示告示性通知圖示。
- *啟用 AVG Active 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，其連線及其木馬攻擊探測內容將被封鎖。
- *啟用將偵測到的威脅報告給 AVG* - (*預設情況下為開啟*)：勾選此項目可允許回報使用者經由 *AVG Active Surf-Shield* 或 *AVG Search-Shield* 發現的木馬攻擊程式和惡意站點，從而為收集網頁惡意活動資訊的資料庫提供資訊。

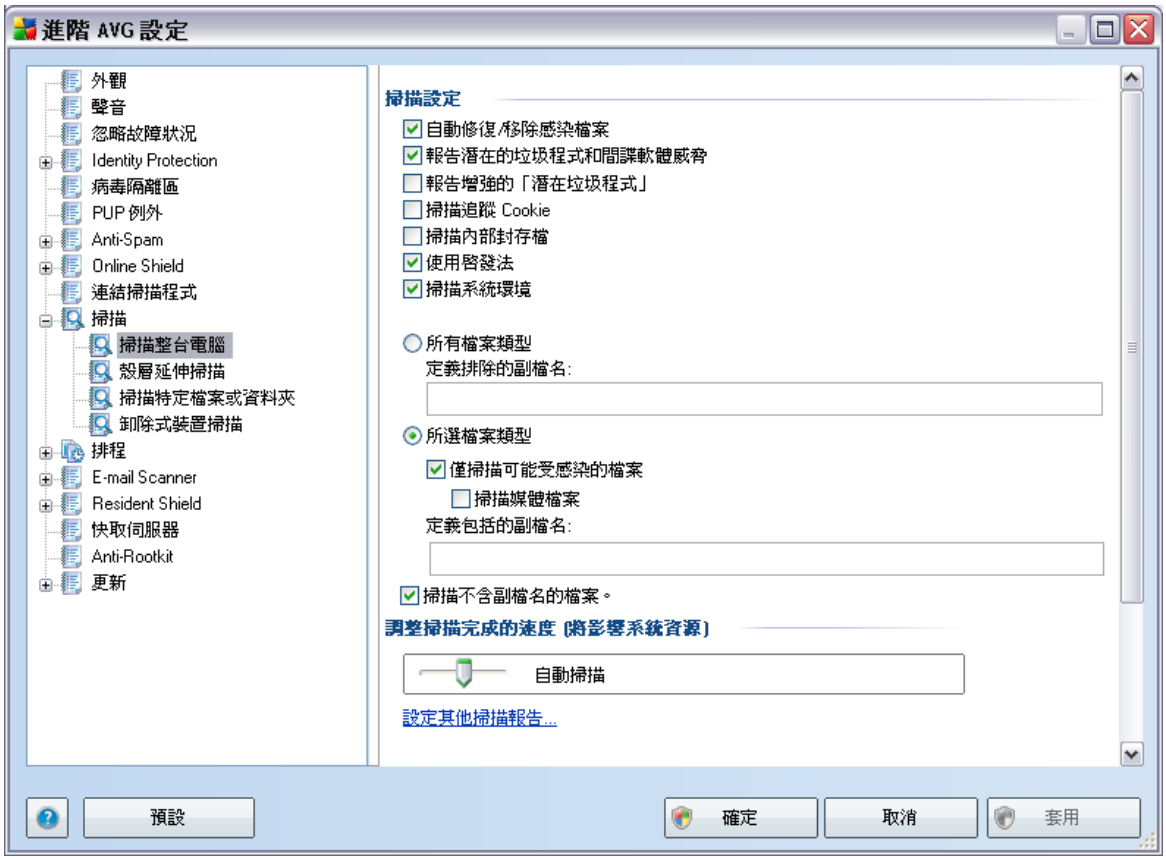
10.8. 掃描

進階掃描設定分為三個類別，這些類別指的是軟體供應商定義的特定掃描類型：

- *掃描整台電腦* - 整台電腦的標準預定義掃描
- *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

10.8.1. 掃描整台電腦

*掃描整台電腦*選項可供您編輯軟體供應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*部分提供可以選擇性開啟/關閉的掃描參數清單:

- *自動修復/移除感染檔案* - 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，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。間諜軟體代表一個可疑的惡意軟體類別: 雖然它通常代表安全性上的風險，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。
- *報告延伸性的潛在垃圾程式* – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體: 當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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* - 這個 Anti-Spyware 元件參數規定在掃描期間應偵測 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*)
- *掃描內部封存* - 這項參數定義掃描時應檢查所有檔案，即使儲存在封存 (例如 ZIP、RAR 等) 中亦然。
- *使用啟發法* - 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* - 掃描也會檢查電腦的系統區域。

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

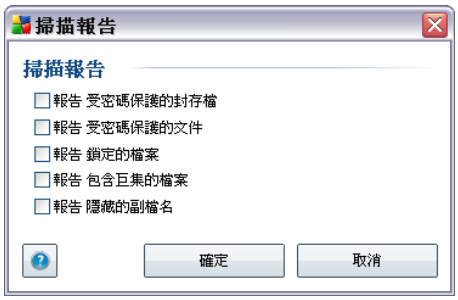
描。

掃描程序優先順序

在*掃描程序優先順序*部分，您可以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，此選項的值會設為中等層級的自動資源使用量。如果您要加快掃描速度，在減少掃描中所耗用時間的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。

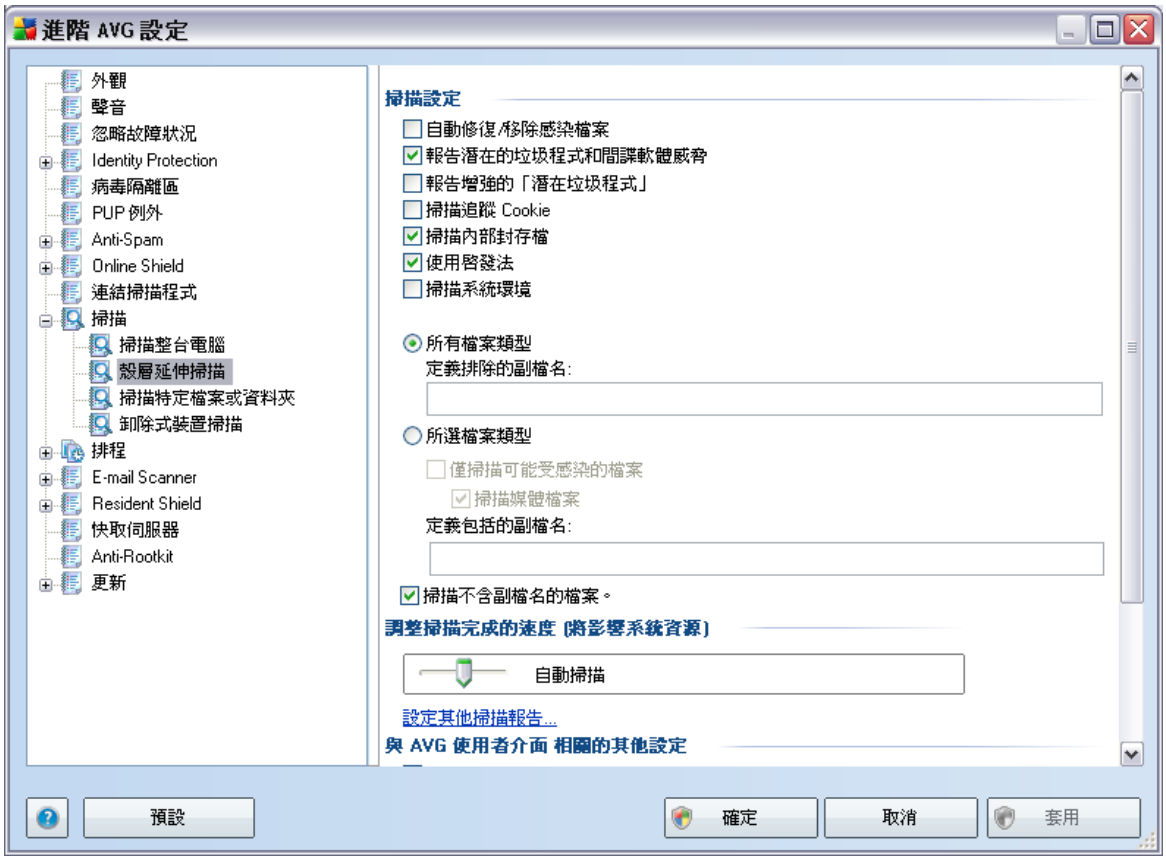
設定其他掃描報告...

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：



10.8.2. 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*，也提供多個對由軟體供應商預定義的掃描進行編輯的選項。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：

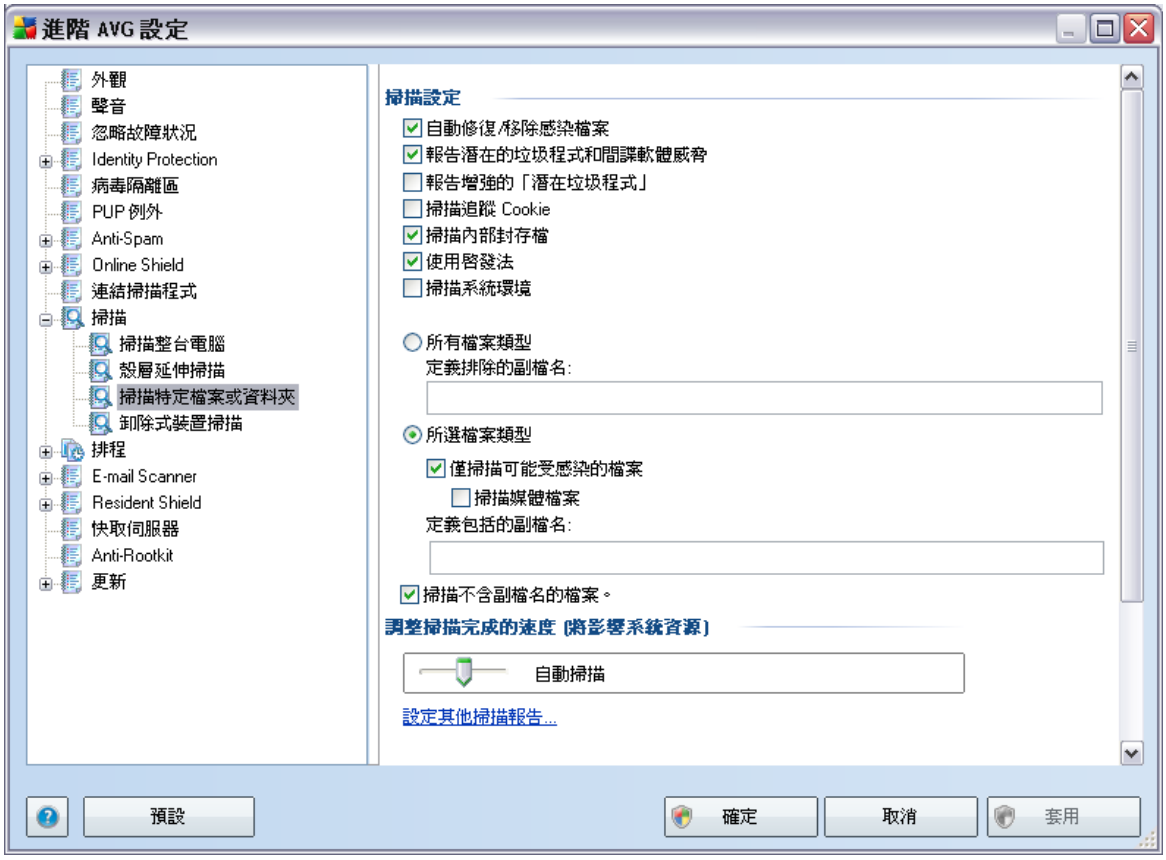


參數清單與*掃描整台電腦*所用的那些參數完全相同。但是，它們的預設設定不同：***掃描整台電腦***會選取大多數參數，而***殼層延伸掃描***（*掃描 Windows 檔案總管*）則只會開啟相關的參數。

注意：*有關特定參數的說明，請參閱 AVG 進階設定 / 掃描 / 掃描整台電腦一章。*

10.8.3. 掃描特定檔案或資料夾

*掃描特定檔案或資料夾*的編輯介面和*掃描整台電腦*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：有關特定參數的說明，請參閱 AVG 進階設定 / 掃描 / 掃描整台電腦一章。

10.8.4. 卸除式裝置掃描

*卸除式裝置掃描*的編輯介面與*掃描整台電腦*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，請參閱 AVG 進階設定 / 掃描 / 掃描整台電腦一章。

10.9. 排程

在*排程*部分，您可以編輯以下項目的預設設定：

- 完整電腦掃描排程

- 病毒庫更新排程
- 程式更新排程

10.9.1. 排程掃描

排程掃描的參數可在三個標籤上進行編輯 (*或設定新的排程*):

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。嘗試始終給掃描取簡短、恰當的說明性名稱，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」則是恰當的說明性名稱示例。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

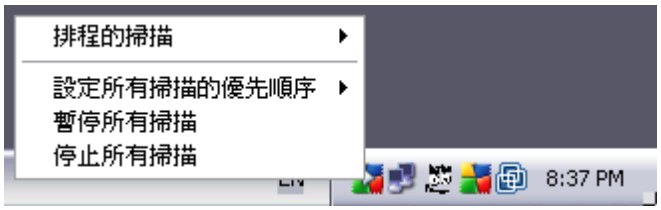
在這裡，您可以為新排程的掃描啟動指定時間間隔。時間安排有以下幾種定義方式：定義一段時間後再次啟動掃描（*每...執行一次*），或定義確切的日期和時間（*在特定時間執行...*），或者可能透過定義一個關聯掃描啟動的事件（*依據電腦啟動執行的動作*）。

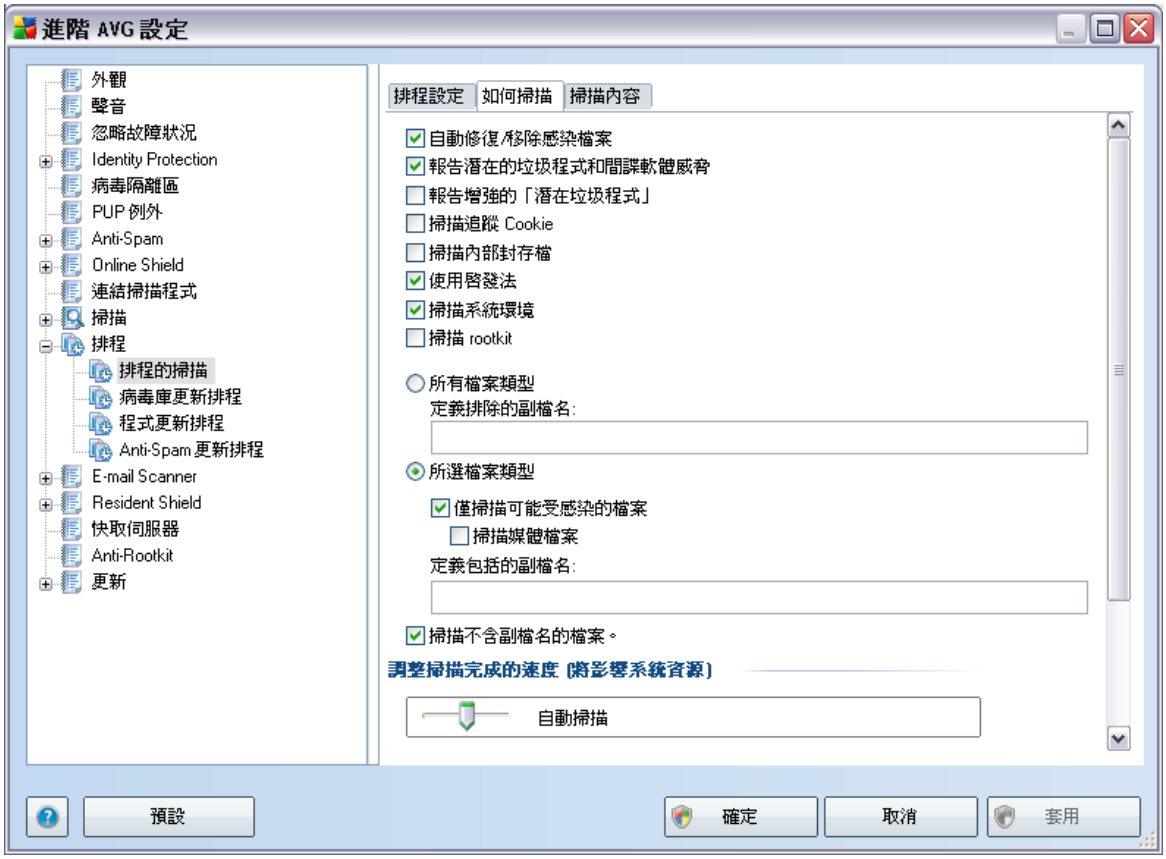
進階排程選項

此部分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（*全彩並帶有一個白色箭頭 - 請參閱上圖*），告知您排程的掃描正在執行中。用滑鼠右鍵按一下執行中的掃描 AVG 圖示，以開啟一個內容功能表，您可以在這裡決定暫停（甚至停止）執行中的掃描：





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：

- *自動修復/移除感染檔案* - 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。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，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。
- *報告延伸性的潛在垃圾程式* – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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*** - (*預設情況下為開啟*)：*Anti-Spyware* 元件的這個參數定義在掃描期間應偵測的 cookie (*HTTP cookie 用於驗證、追蹤和維護使用者的特定資訊，如站點偏好或電子購物車內容*)

- ***掃描內部封存*** - (*預設情況下為開啟*)：這項參數定義掃描時應該檢查所有檔案，即使它們儲存在封存 (例如 ZIP、RAR 等) 中亦然。

- ***使用啟發法*** - (*預設情況下為開啟*)：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*** - (*預設情況下為開啟*)：掃描還會檢查電腦的系統區域；

- ***掃描 rootkit*** - 如果您要將 rootkit 偵測包含到整個電腦掃描中，則請勾選此項目。rootkit 偵測也在 *Anti-Rootkit* 元件中單獨有提供；

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；

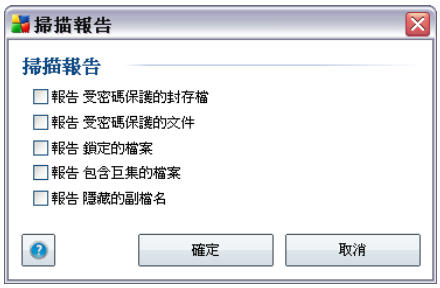
- ***所選檔案類型*** - 您可以指定您只想要掃描可能受感染的檔案 (*將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔*)，包括媒體檔案 (*視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染*)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。

- 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。

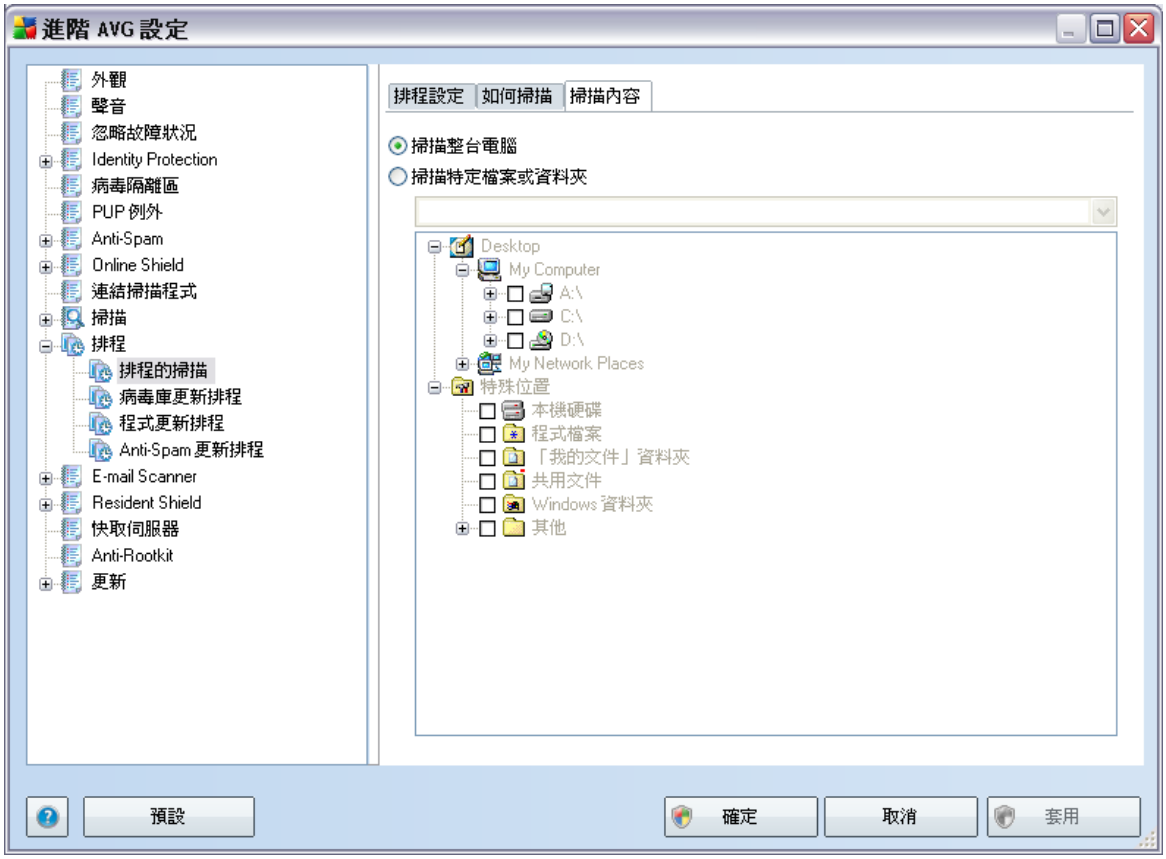
掃描程序優先順序

在***掃描程序優先順序***部分，您可以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，此選項會設為中等層級的自動資源使用量。如果您要加快掃描速度，在減少執行中所耗用時間的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。

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：



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*)，一個新選項將啟動，可使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。

10.9.2. 病毒庫更新排程

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病毒庫更新，然後在有需要時再將其開啟。在*更新管理員*元件中已經包含基本病毒庫更新的排程。在此對話方塊中，您可以設定病毒庫更新排程的部分詳細參數。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

在此部分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（*每 ... 執行一次*），或定義確切的日期和時間（*在某個時間執行 ...*）。

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

動病毒庫更新。

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*）。

在*排程設定*標籤上，您可以首先核取/取消核取*啟用此工作*項目，直接暫時停用排程的程式更新，並在需要時再將其開啟。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啓動指定時間間隔。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（*依據電腦啟動的動作*）。

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。

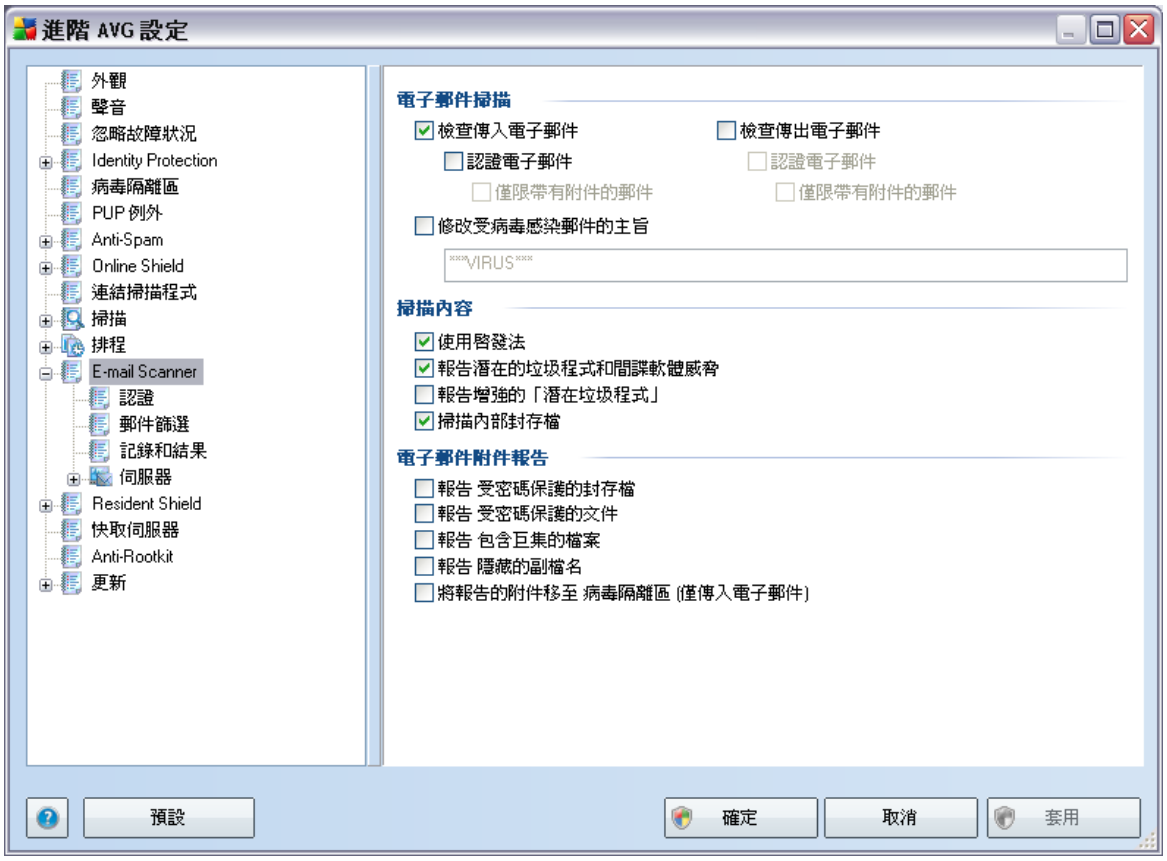
其他更新設定

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次序，而掃描將會暫停。

10.10. E-mail Scanner



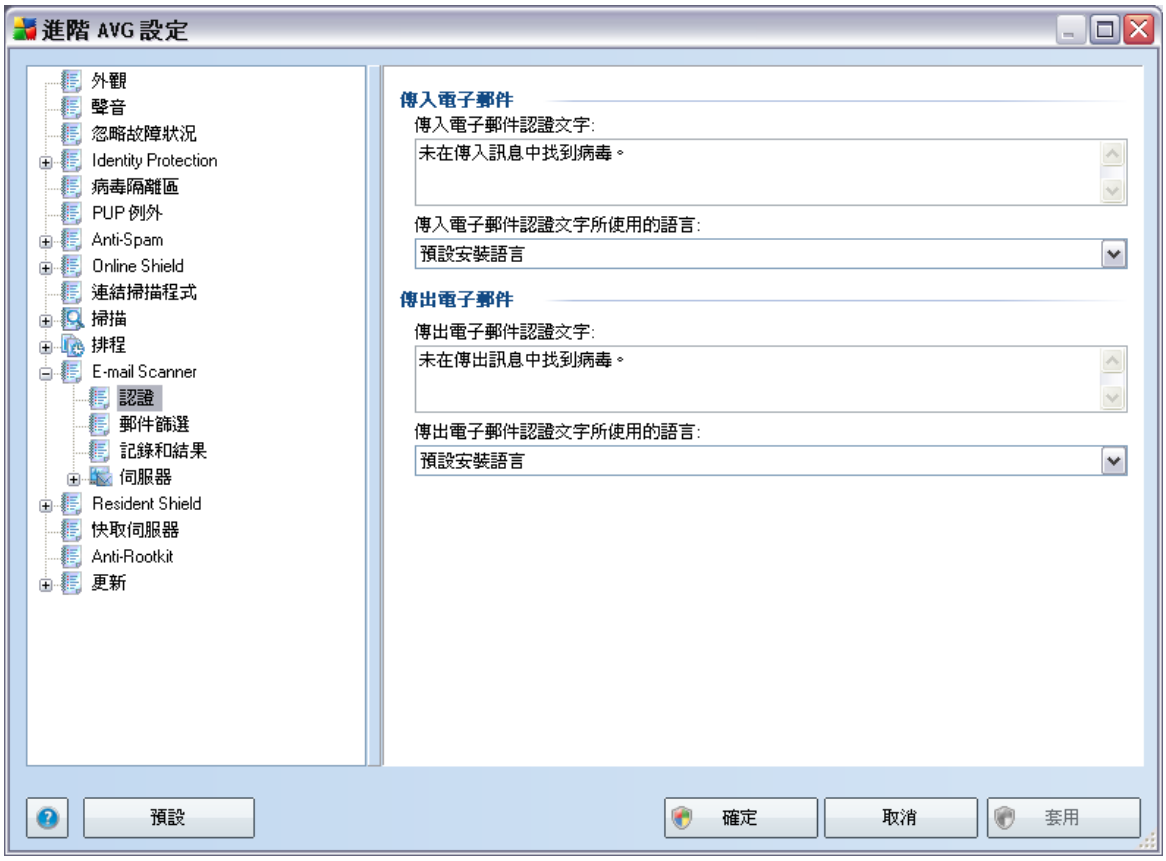
E-mail Scanner 對話方塊由三個部分構成:

- ***電子郵件掃描*** - 您可以為傳入和/或傳出的電子郵件訊息設定以下基本資訊:
    - 是否必須對電子郵件訊息進行病毒掃描。
    - 是否必須在每一訊息的結尾加上認證文字，以指明其不含病毒。該文字內容可以在認證對話方塊中修改。
    - 是否只能在帶有附件的郵件中加上認證文字。

若要***修改受病毒感染郵件的主旨***，請核取該方塊並在文字欄位中鍵入所需的值。然後，該值即會新增到每一受感染電子郵件訊息的主旨欄位中，從而便於識別和篩選。預設值為 ***VIRUS***，我們建議保留此值。

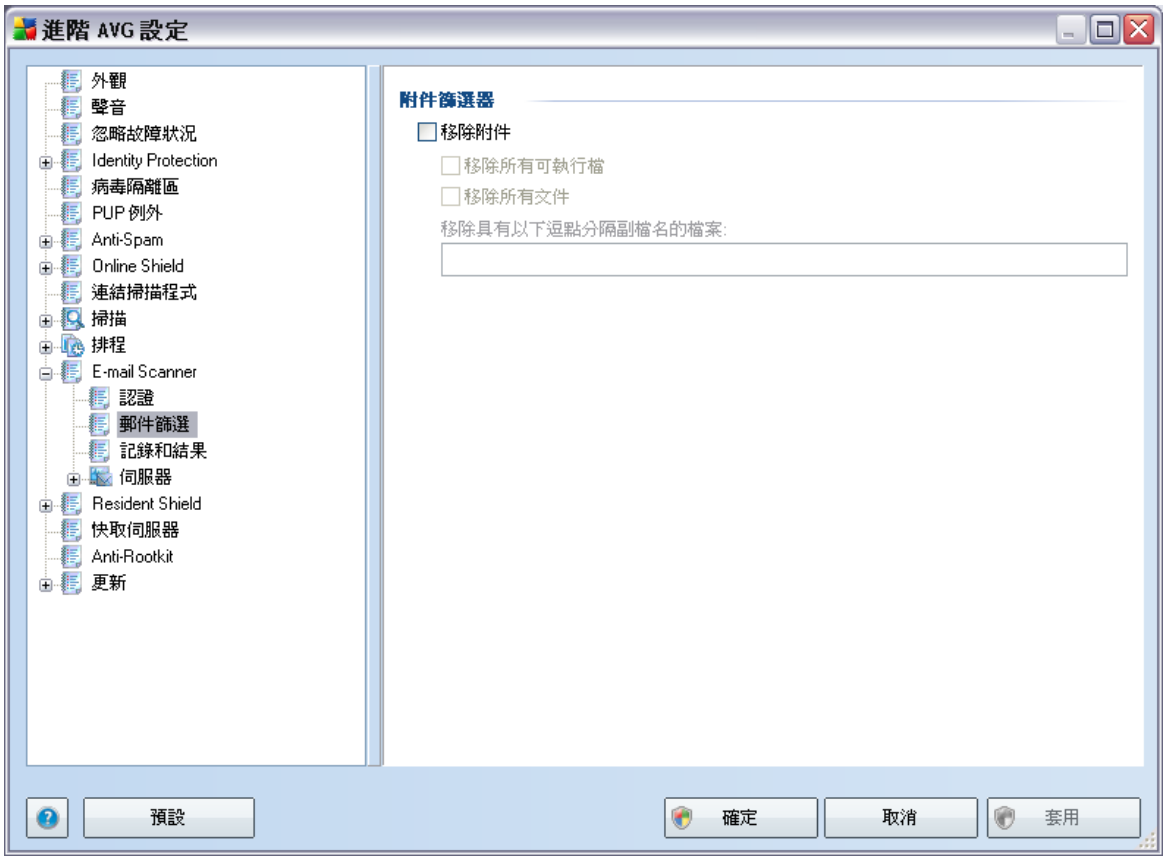
- ***掃描內容*** - 在這個部分，您可以指定電子郵件訊息的掃描方式。
    - ***使用啟發法*** – 核取此選項可在掃描電子郵件訊息時使用啟發式偵測法。開啓此選項後，您不僅可以透過副檔名篩選電子郵件附件，也可以透過考量附件的實際內容來進行篩選。篩選可以在郵件篩選對話方塊中設定。
    - ***報告潛在的垃圾程式和間諜軟體威脅*** – (*預設為開啟*)：核取此方塊可啟動 *Anti-Spyware* 引擎，並掃描間諜軟體和病毒。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。
    - ***報告延伸性的潛在垃圾程式*** – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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。
    - ***掃描內部封存*** – 核取此方塊可掃描附加到電子郵件訊息之封存的內容。
- ***電子郵件附件報告*** - 在這個部分，您可以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潛在危險內容。
    - ***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***。

10.10.1. 認證



在*認證*對話方塊中，您可以明確指定認證說明中應包含的文字以及所使用的語言。您必須分別為*傳入郵件*與*傳出郵件*進行指定。

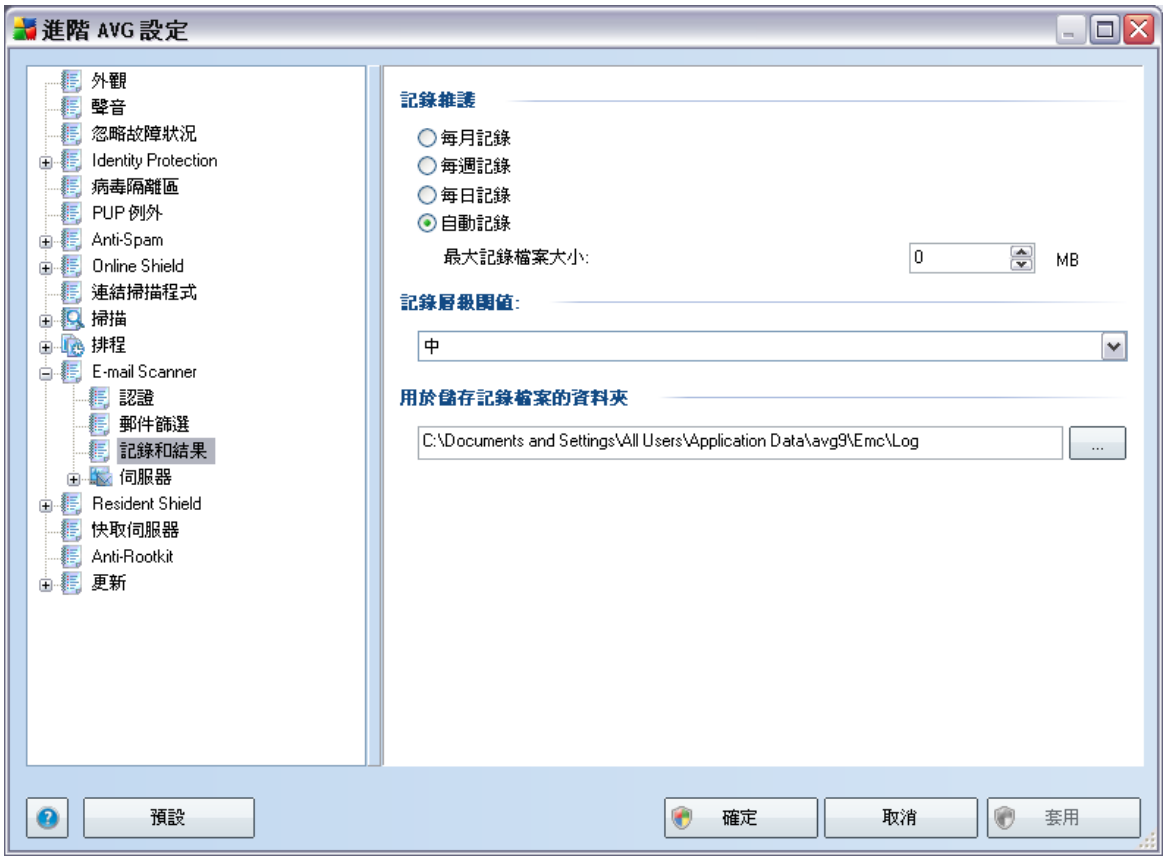
10.10.2. 郵件篩選



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

10.10.3. 記錄和結果

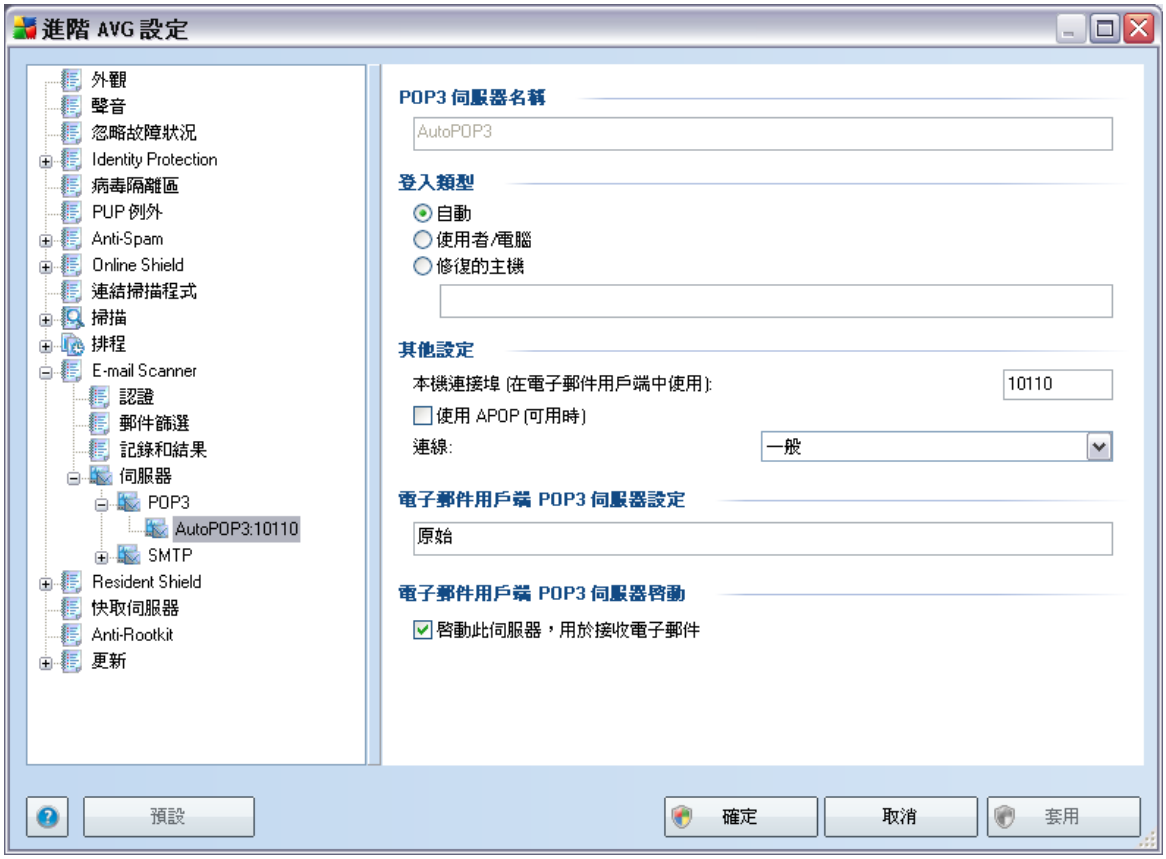


在透過*記錄和結果*巡覽項目開啟的對話方塊中，您可以指定用於維護電子郵件掃描結果的參數。此對話方塊由數個部分構成：

- *記錄維護* - 定義您是否要每天、每週、每月...記錄電子郵件掃描資訊；同時指定記錄檔案的最大大小 (*以 MB 為單位*)
- *記錄層級閾值* - 預設為中等層級 - 您可以選取一個較低的層級 (*記錄基本連線資訊*) 或較高層級 (*記錄所有流量*)
- *用於儲存記錄檔案的資料夾* - 定義記錄檔案的位置

10.10.4. 伺服器

在*伺服器*部分，您可以編輯 *E-mail Scanner* 元件伺服器的參數，或使用*新增新伺服器*按鈕設定新的伺服器。



在此對話方塊中 (透過*伺服器 / POP3* 開啟)，您可透過使用 POP3 通訊協定，為傳入郵件設定新的 *E-mail Scanner* 伺服器：

- *POP3 伺服器名稱* - 輸入伺服器的名稱或保留 AutoPOP3 預設名稱
- *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。
    - *使用者 / 電腦* - 確定目標郵件伺服器最簡單且最常用的方法為代理方法。如需使用此方法，請將名稱或位址 (或者還有連接埠) 指定為指定郵件伺服器之登入使用者名稱的一部分，使用 / 字元分隔。例如，對於伺服器 pop.acme.com 和連接埠 8200 上的帳戶 user1，您可使用 user1/pop.acme.com:8200 作為登入名稱。
    - *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，您可以指定此連接埠，方法是將連接埠號置於伺服器名稱後面，使用冒號作為分隔符號 (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：

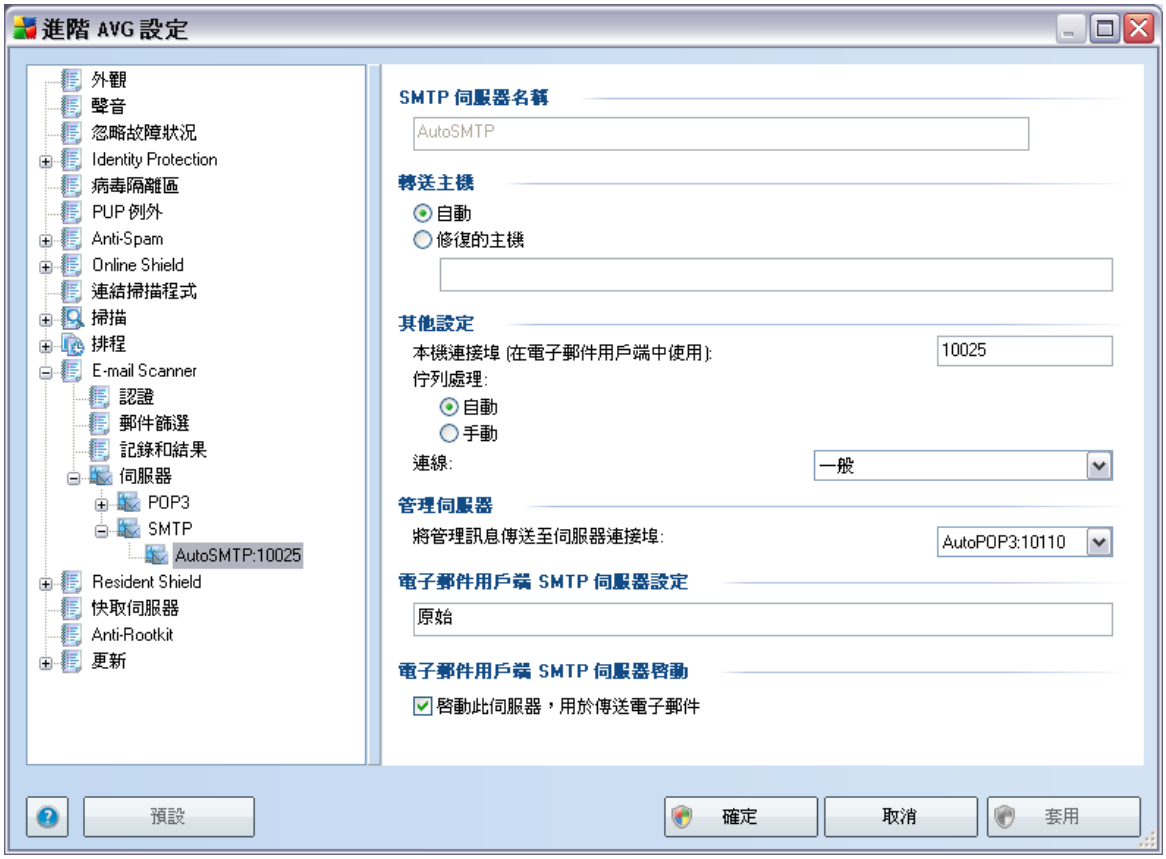
  - ***本機連接埠*** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 POP3 通訊的連接埠。

  - ***使用 APOP (可用時)*** - 此選項提供更安全的郵件伺服器登入。這可以確保 E-mail Scanner 使用替代方法轉送用於登入的使用者帳戶密碼，並使用來自伺服器的變數鏈以加密 (而非公開) 格式向伺服器傳送密碼。當然，此功能僅在目標郵件伺服器支援時可用。

  - ***連線*** - 您可以在下拉式功能表中指定要使用的連線類型 (一般/SSL/SSL 為預設)。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 伺服器設定*** - 提供了正確設定您的電子郵件用戶端所需的組態設定相關的簡短資訊 (以便 E-mail Scanner 檢查所有傳入郵件)。這是基於在此對話方塊以及其他相關對話方塊中指定的相應參數的摘要。

- ***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



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

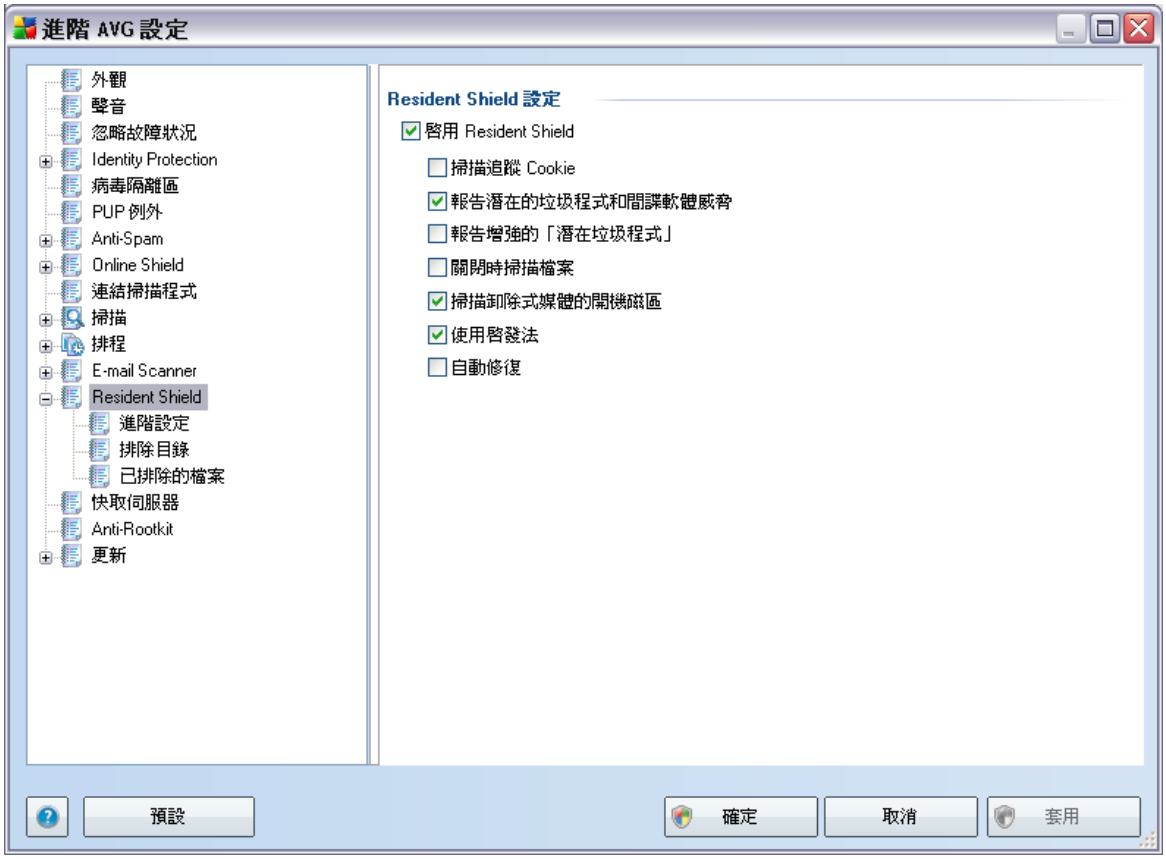
- *SMTP 伺服器名稱* - 鍵入伺服器的名稱或保留 AutoSMTP 的預設名稱
- *轉送主機* - 定義用於決定傳出郵件所用的郵件伺服器的方法：
    - *自動* - 根據您的電子郵件用戶端的設定自動執行登入。
    - *固定主機* - 在這種情況下，程式永遠會使用此處指定的伺服器。請指定您的郵件伺服器的位址或名稱。您可以使用網域名稱 (例如 smtp.acme.com) 和 IP 位址 (例如 123.45.67.89) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以在伺服器名稱後面鍵入連接埠，並用冒號作為分隔符號 (例如 smtp.acme.com:8200)。用於 SMTP 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。
- *佇列處理* - 決定 *E-mail Scanner* 在處理傳送郵件訊息的要求時的行為。
  - 自動 - 傳出郵件將立即傳遞 (傳送) 至目標郵件伺服器
  - 手動 - 郵件插入傳出郵件的佇列中，並稍後再傳送
- *連線* - 您可以在此下拉式功能表中指定要使用的連線類型 (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。

- *管理伺服器* - 顯示將用於反向傳遞管理報告的伺服器連接埠號。當目標郵件伺服器拒絕傳出郵件或者此郵件伺服器不可用時，便會產生這種郵件。
- *電子郵件用戶端 SMTP 伺服器設定* - 提供有關如何設定用戶端郵件應用程式，以使傳出郵件訊息接受檢查 (使用目前修改的伺服器來檢查傳出郵件) 的資訊。這是基於在此對話方塊以及其他相關對話方塊中指定的相應參數的摘要。
- *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。

10.11. Resident Shield

Resident Shield 元件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。



您可在 *Resident Shield 設定*對話方塊中，透過核取/取消核取*啟用 Resident Shield* 項目來完全啟動或停用 *Resident Shield* 保護 (*此選項預設情況下為開啟狀態*)。此外，您可選取應啟動哪些 *Resident Shield* 功能：

- ***掃描追蹤 cookie*** - 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。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，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。

- ***報告延伸性的潛在垃圾程式*** – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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*** - 關閉時掃描可確保 AVG 開啟和關閉在作用中的物件（如應用程式、文件等）時進行掃描；此功能可幫助保護您的電腦免遭一些複雜病毒的攻擊

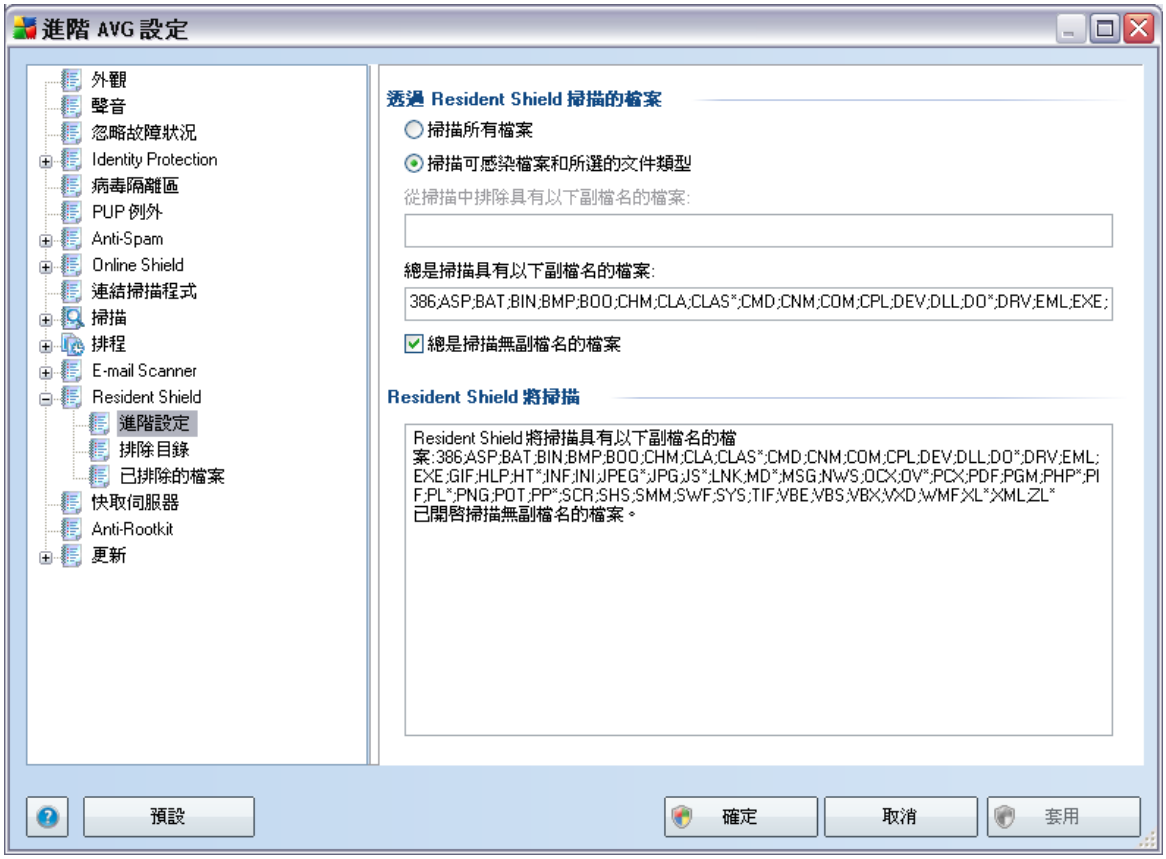
- ***掃描卸除式媒體的開機磁區*** - (*預設情況下為開啟*)

- ***使用啟發法*** - (*預設情況下為開啟*) 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*)

- ***自動修復*** - 如有可用的修復方法，將自動修復任何偵測到的感染

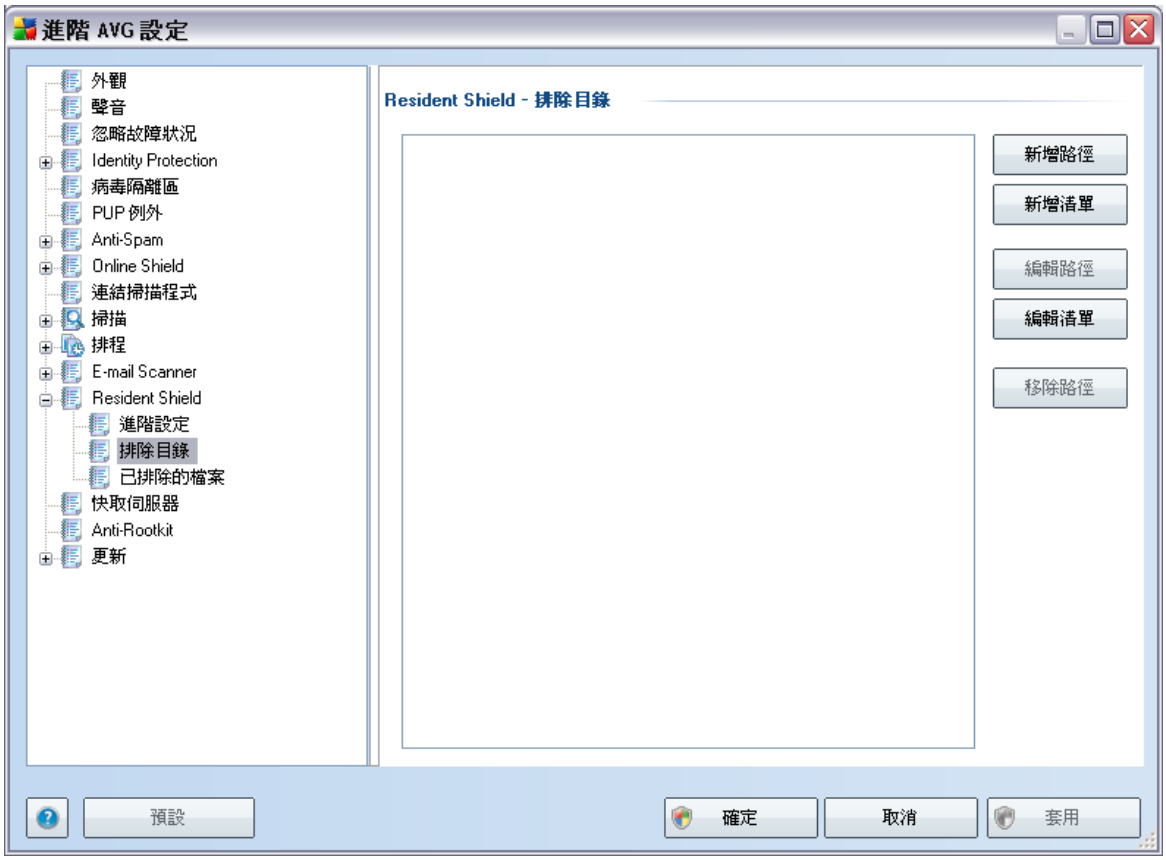
10.11.1. 進階設定

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*)：



決定您要掃描所有檔案，或只掃描可感染的檔案 - 若要這麼做，您還可以進一步指定副檔名清單來定義要從掃描排除的檔案，或是指定檔案副檔名清單來定義無論如何都必須掃描的檔案。

10.11.2. 排除目錄



*Resident Shield - **排除目錄***對話方塊可讓您定義要從 *Resident Shield* 掃描中排除的資料夾。

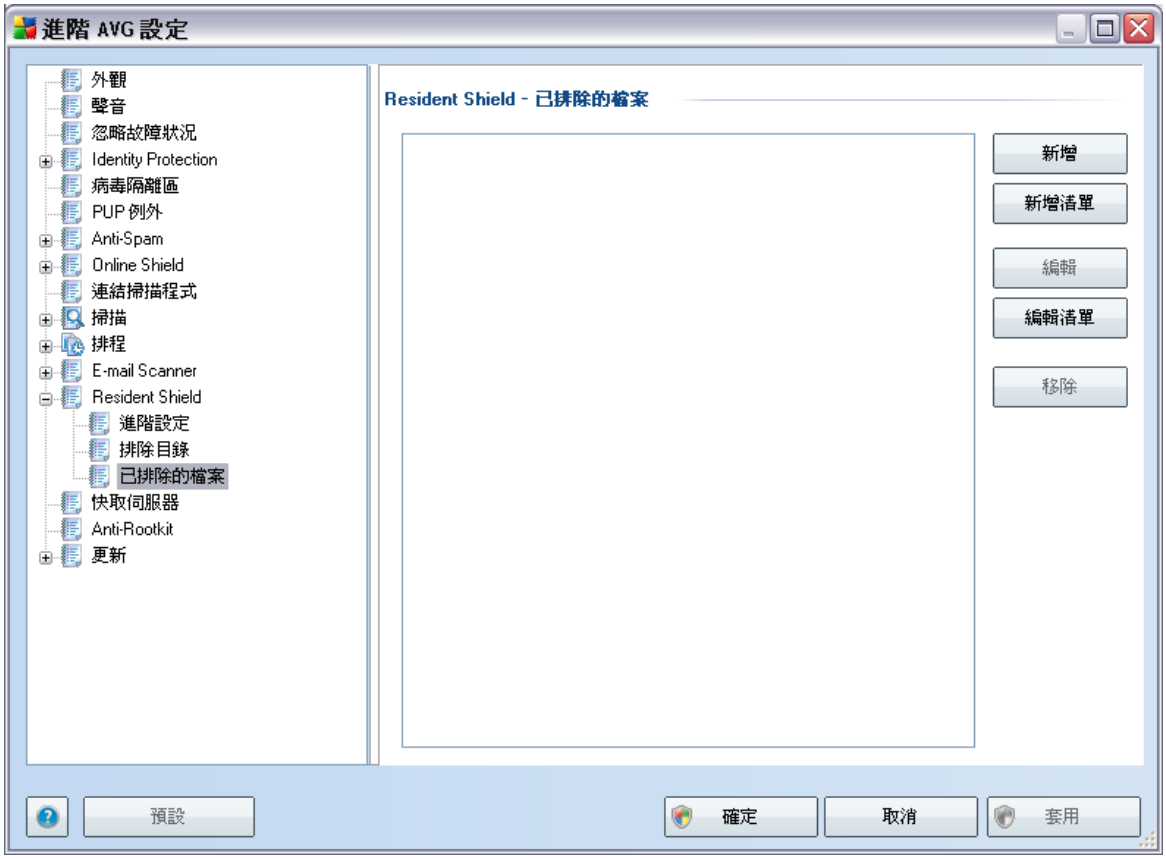
除非必要，否則我們強烈建議不要排除任何目錄！

該對話方塊提供下列控制按鈕：

- ***新增路徑***– 指定從掃描排除的目錄，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄
- ***新增清單***– 可讓您輸入要從 *Resident Shield* 掃描排除的整份目錄清單
- ***編輯路徑***– 可讓您編輯所選資料夾的指定路徑
- ***編輯清單***– 可讓您編輯資料夾清單

- *移除路徑*– 可讓您從清單刪除所選資料夾的路徑

10.11.3. 已排除的檔案



*Resident Shield - 已排除的檔案*對話方塊的運作方式就跟前述 *Resident Shield - 排除目錄一樣*，但您現在不是指定資料夾，而是定義應該從 *Resident Shield* 掃描中排除的特定檔案。

若非必要，我們強烈建議不要排除任何檔案！

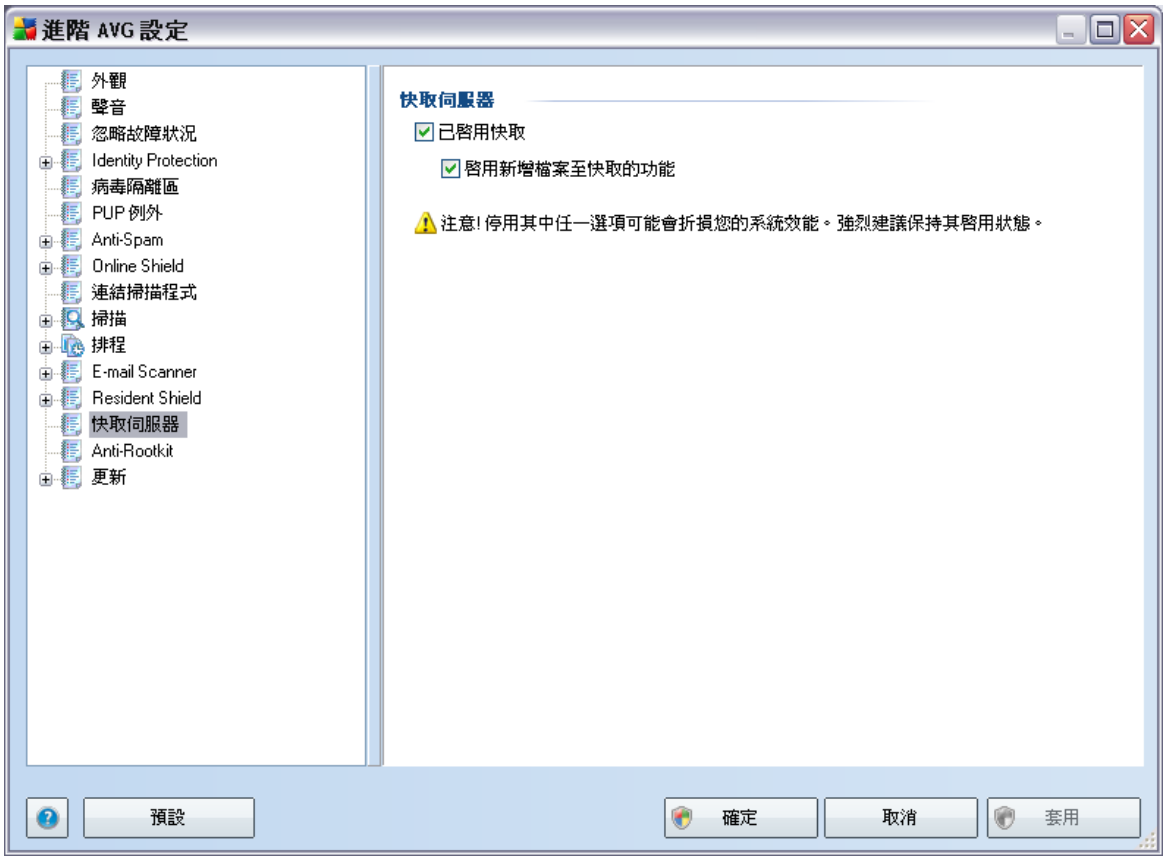
該對話方塊提供下列控制按鈕：

- *新增*– 透過從本機磁碟巡覽樹狀目錄逐一選取目錄來指定要從掃描中排除的檔案
- *新增清單*– 可讓您輸入要從 *Resident Shield* 掃描排除的整份檔案清單
- *編輯* – 可讓您編輯所選檔案的指定路徑

- *編輯清單* – 可讓您編輯檔案清單
- *移除* – 可讓您從清單中刪除所選檔案的路徑

10.12. 快取伺服器

*快取伺服器*是用來加速所有掃描 (*按需掃描*、*排程完整電腦掃描*、*Resident Shield 掃描*) 的一種程序。它能收集並保留可信任檔案的資訊 (*例如有電子簽章的系統檔*)：這些檔案被視為安全，在掃描時會跳過。



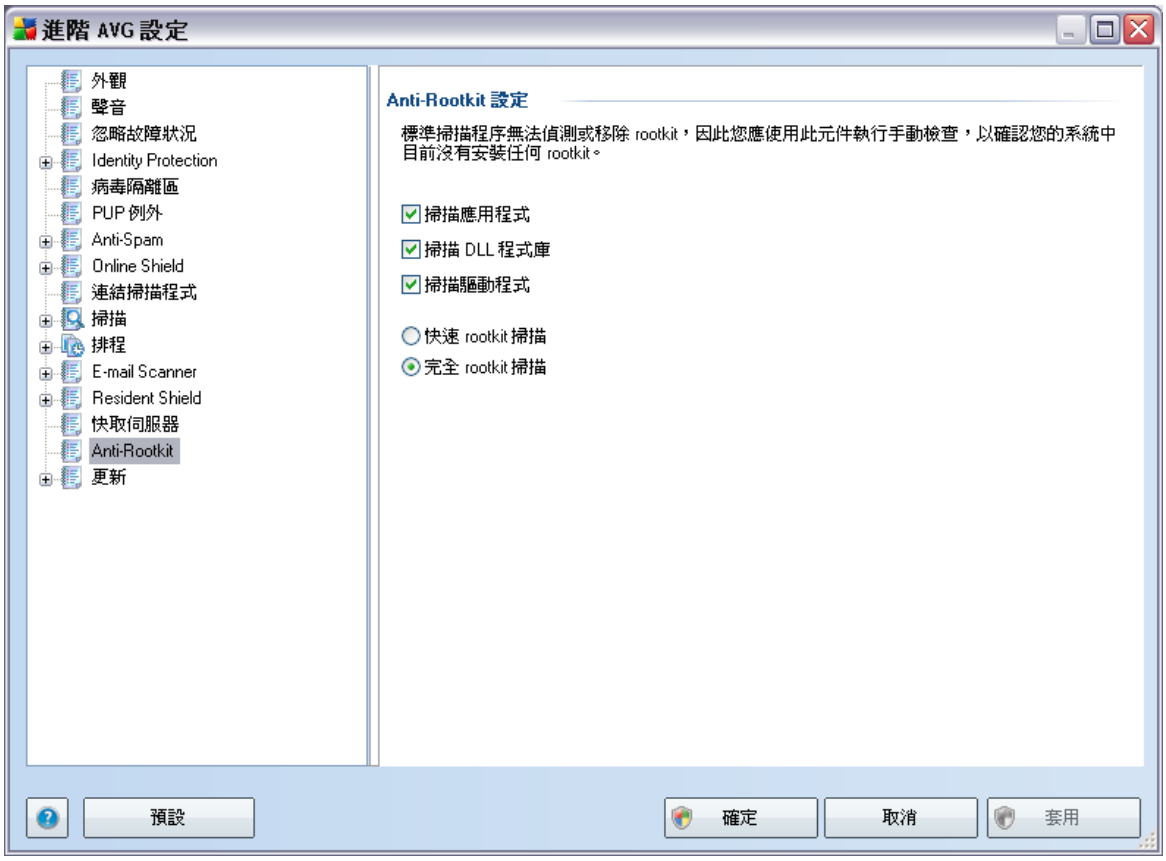
設定對話方塊提供兩個選項：

- *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。

10.13. Anti-Rootkit

在此對話方塊中，您可以編輯 *Anti-Rootkit* 元件的組態：



您也可以直接從 *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。

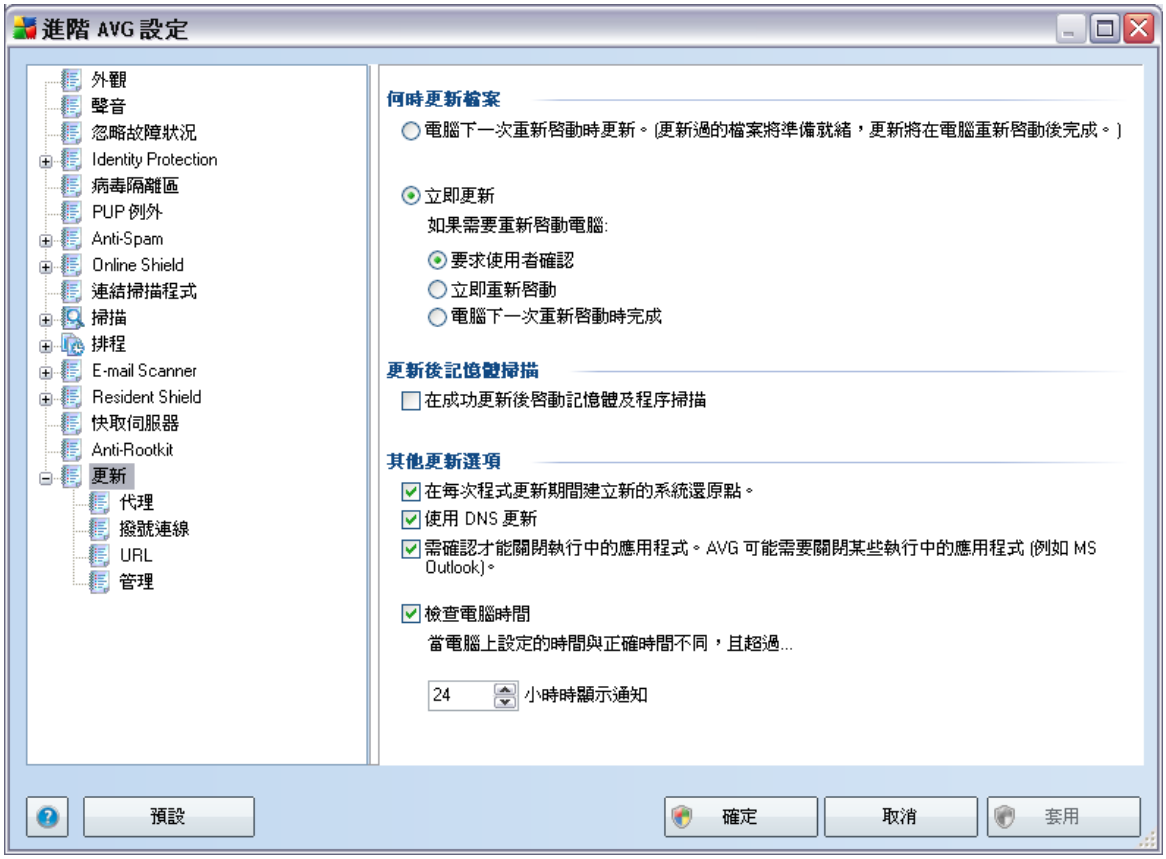
勾選相應的核取方塊來指定要掃描的物件：

- *掃描應用程式*
- *掃描 DLL 程式庫*
- *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*)
- *完整 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*)

10.14. 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

在此部分，有兩個選項供您選擇：可以排程電腦下一次重新啟動時進行更新，或者啟動立即更新。預設情況下會選取立即更新選項，如此一來，AVG 便可以確保最高的安全層級。

只有在您確定電腦會定期重新啟動 (至少每天一次) 時，才建議使用排程電腦下一次重新啟動時進行更新。

如果您決定保持預設組態並立即啟動更新程序，可以指定在哪種情況下應該重新啟動電腦：

- ***要求使用者確認*** - 系統會詢問您是否批准重新啟動電腦，以完成更新程序
- ***立即重新啟動*** - 更新程序完成後，無須您的批准，電腦便會立即自動重新啟動
- ***電腦下一次重新啟動時完成*** - 更新程序的完成將延遲到下一次電腦重新啟動 - 再強調一次，請記住，只建議您在確定電腦會定期重新啟動 (至少每天一次) 時才使用此選項。

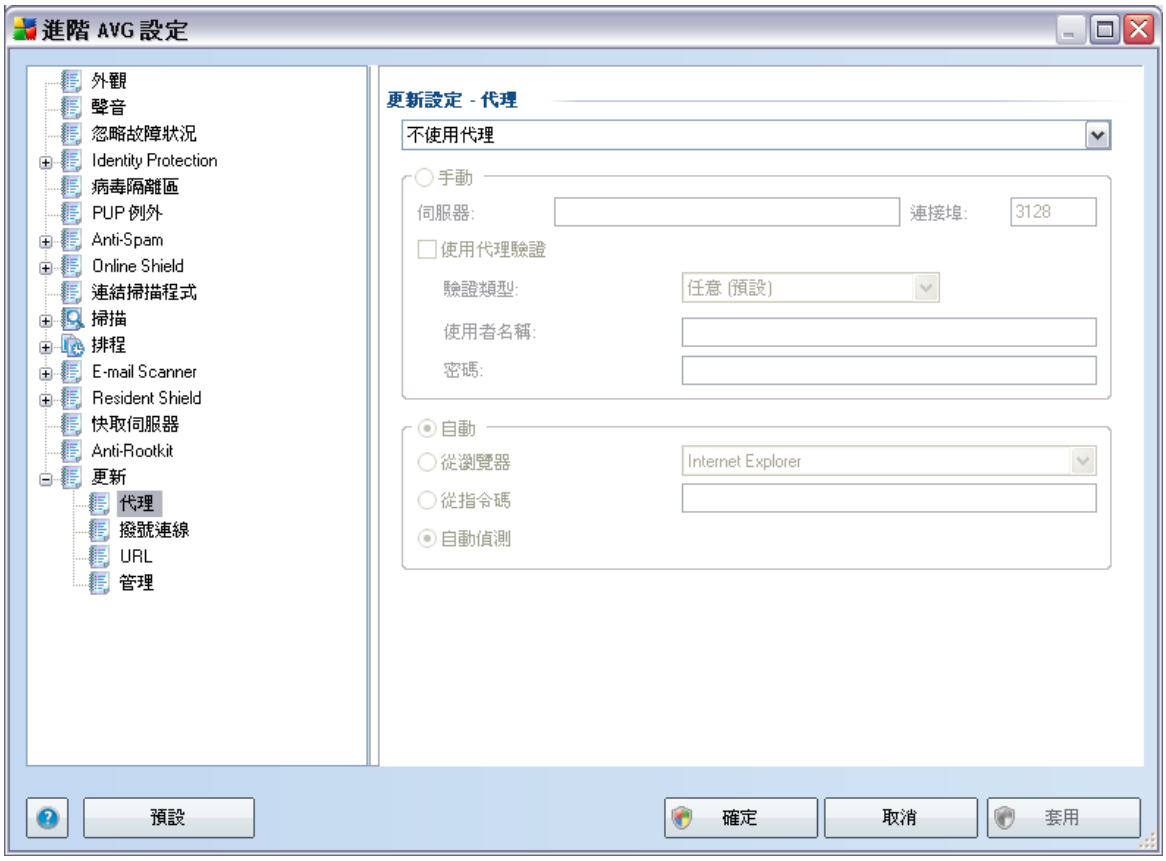
更新後記憶體掃描

核取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

- ***在每次程式更新完畢後生成新的系統還原點*** - 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*** - 勾選此核取方塊，可確認您要使用更新檔案偵測方法來消除更新伺服器和 AVG 用戶端之間傳輸的資料量；
- ***需確認才能關閉執行中的應用程式*** (*預設情況下為開啟*) 這個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，則要經過您的許可才能關閉；
- ***檢查電腦時間*** - 核取此選項，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。

10.14.1. 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*
- *不使用代理伺服器* - 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*)

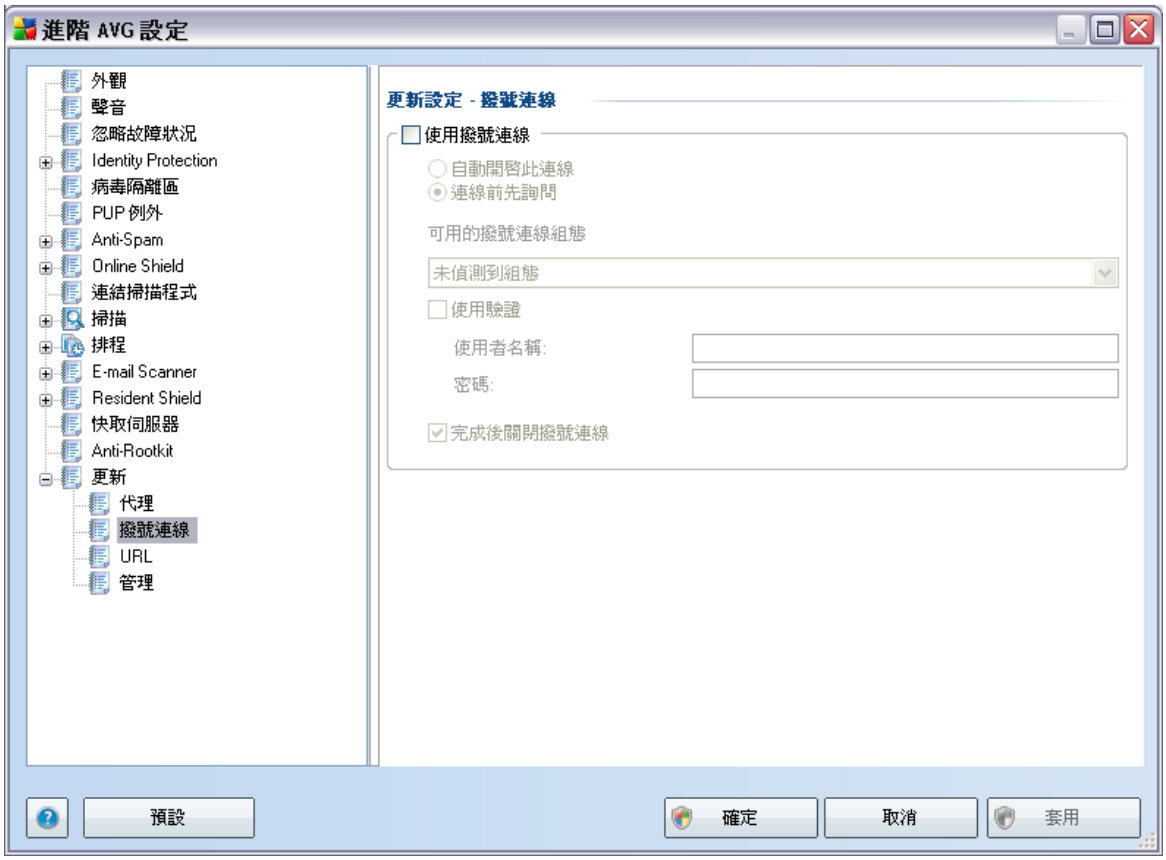
代理伺服器也為每個使用者組態了特定規則。如果您的代理伺服器是依這種方式設定的, 請核取*使用代理驗證*選項, 以驗證透過代理伺服器連線至網際網路的使用者名稱和密碼是否有效。

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

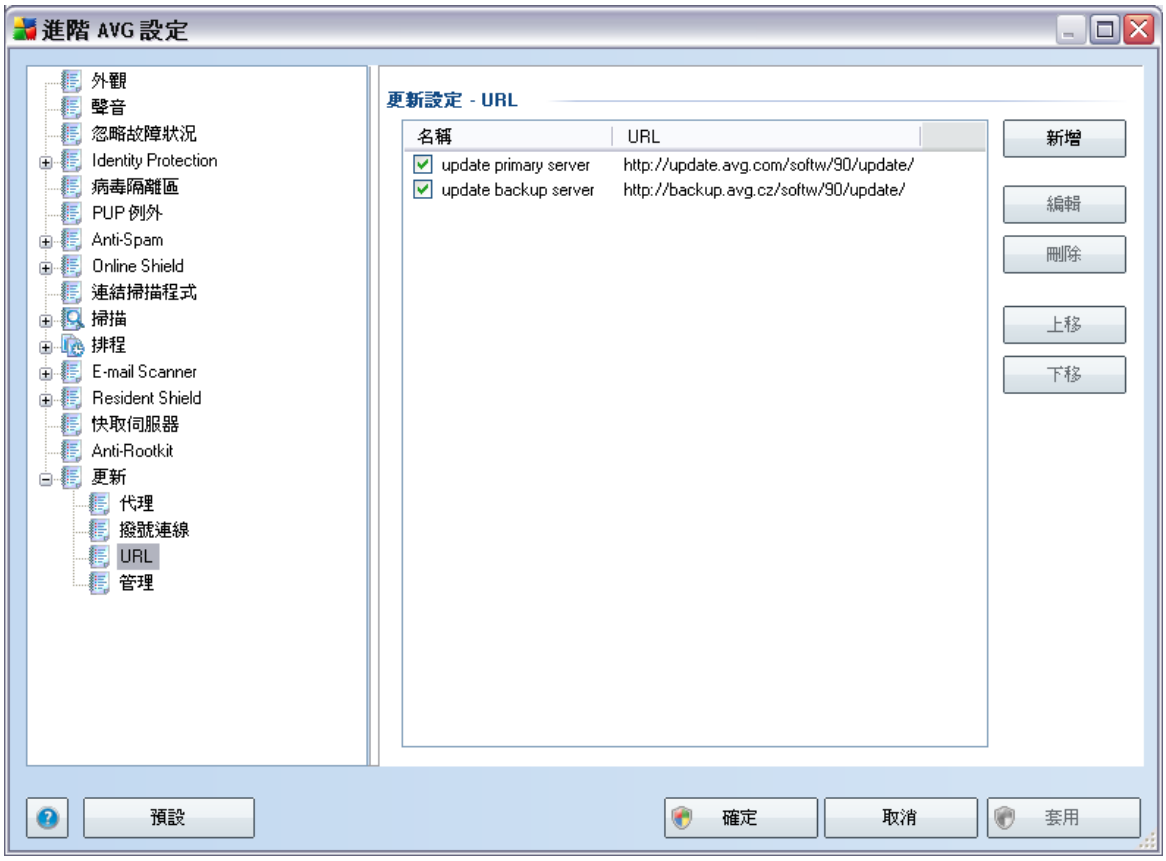
10.14.2. 撥號連線



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。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*)。

10.14.3. URL

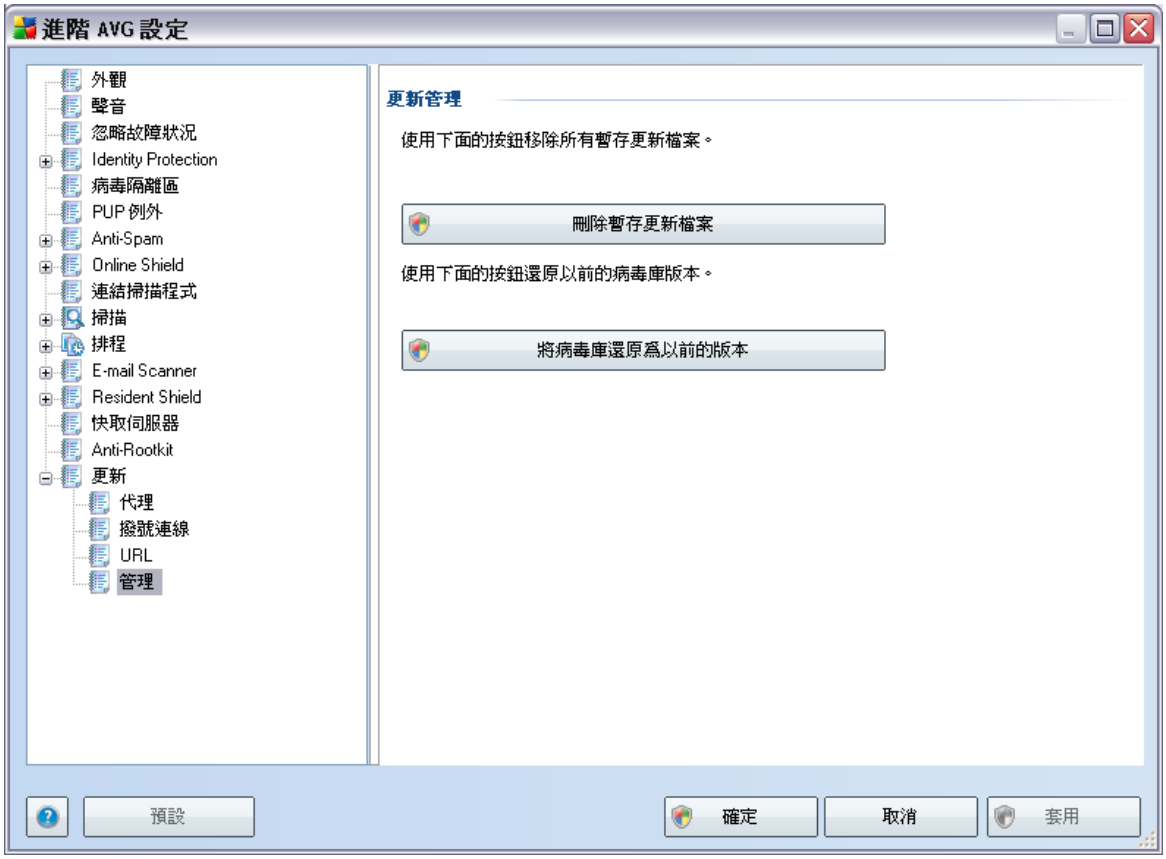


URL 對話方塊提供一份可從中下載更新檔案的網際網路位址清單。使用下列控制按鈕可修改該清單及其項目：

- ***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

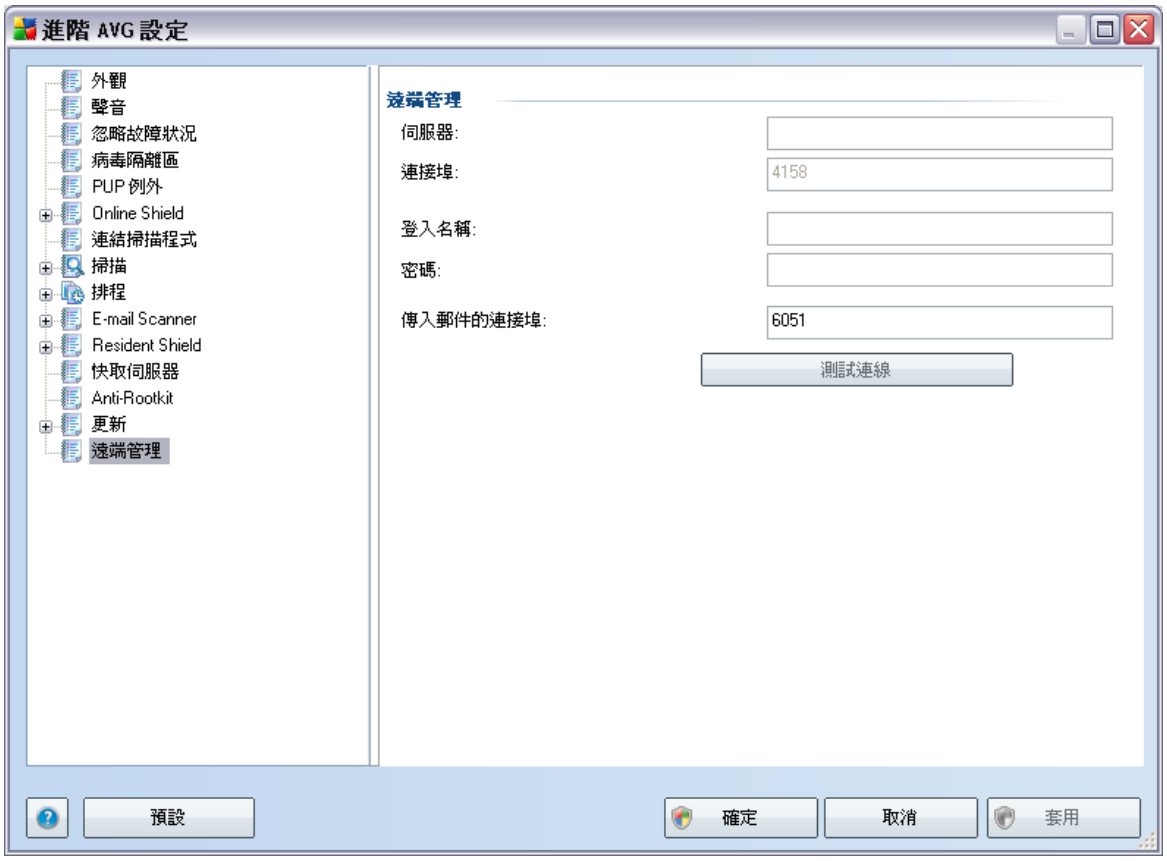
10.14.4. 管理

*管理*對話方塊提供有兩個選項，可分別透過兩個按鈕存取：



- *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*)

10.15. 遠端管理



*遠端管理*設定與從 AVG 用戶端站點到遠端管理系統的連線有關。如果您打算將個別站點連線至遠端管理，請指定以下參數：

- *伺服器* - 伺服器名稱 (或伺服器 IP 位址)，即安裝 AVG Admin 伺服器的位置
- *連接埠* - 提供 AVG 用戶端與 AVG Admin 伺服器進行通訊所使用的連接埠號 (*連接埠號 4158 為預設值 - 若使用此連接埠號，便無需明確指定該號碼*)
- *登入* - 如果將 AVG 用戶端與 AVG Admin 伺服器之間的通訊定義為安全，則請提供您的使用者名稱...
- *密碼* - ...和您的密碼
- *傳入郵件的連接埠* - AVG 用戶端接受來自 AVG Admin 伺服器的傳入郵件時所使用的連接埠號

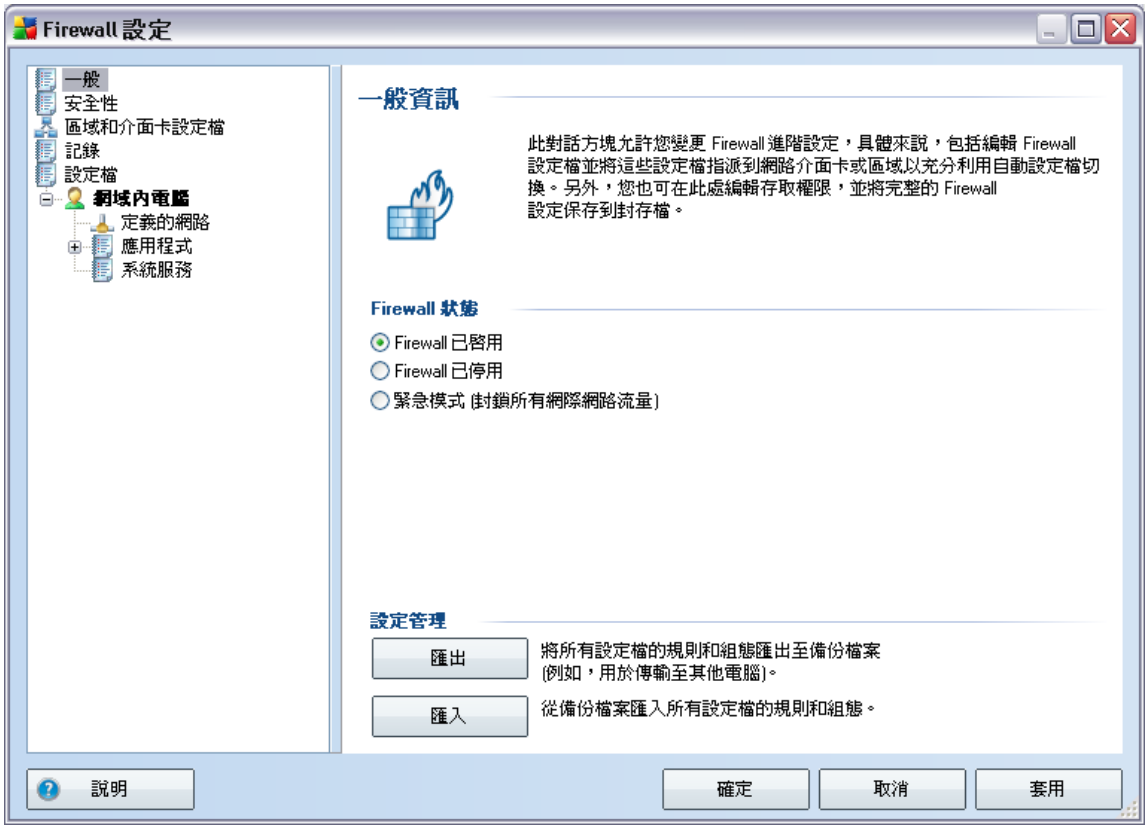
*測試連線*按鈕可幫助您驗證所有以上所述的資料是否有效，且是否可用於成功連線至 DataCenter。

注意：有關遠端管理的詳細說明，請參閱 AVG Network Edition 文件。

11. Firewall 設定

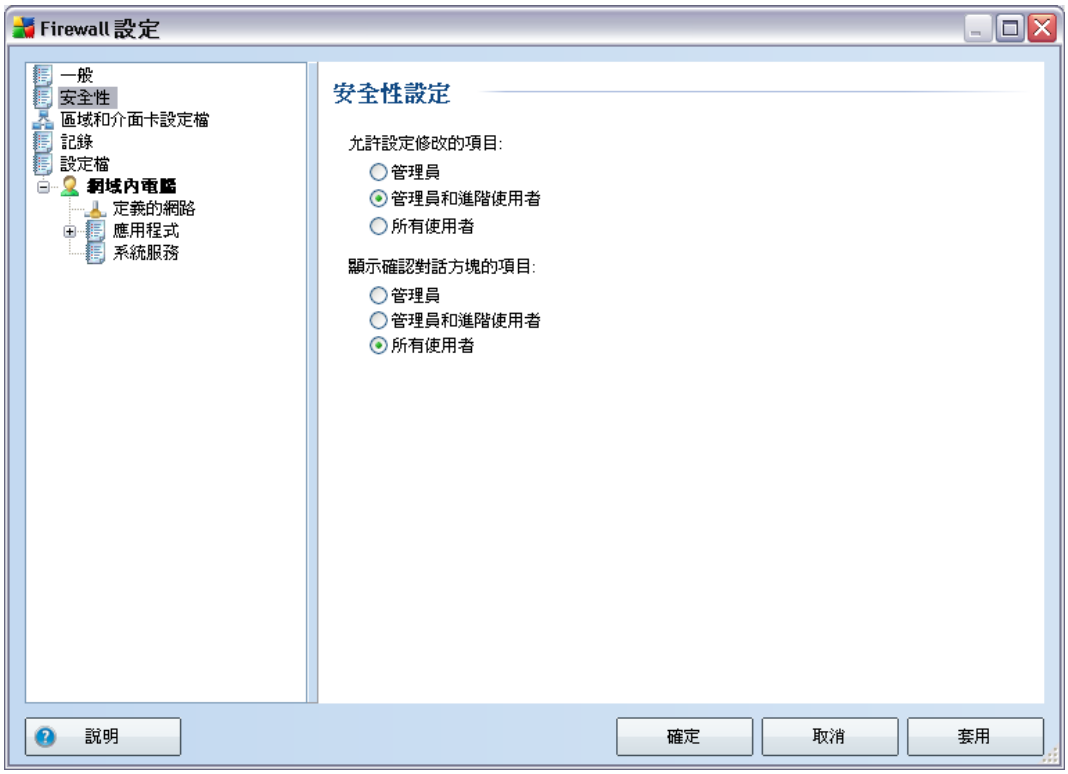
Firewall 組態會在新視窗中開啟，您可以在其中的幾個對話方塊中設定元件的進階參數。*不過，只有專家和經驗豐富的使用者才適合編輯進階組態。*

11.1. 一般



您可以在*一般資訊*中*匯出/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



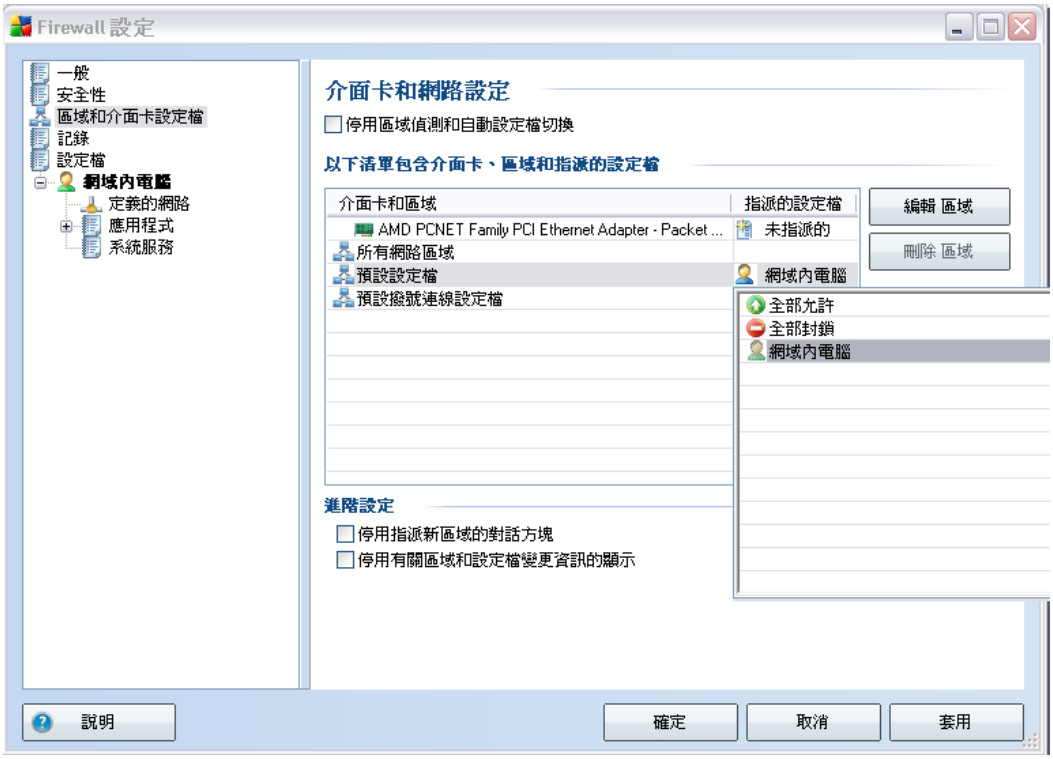
在*安全性設定*對話方塊中，無論所選的設定檔為何，您都可以定義 *Firewall* 行為的一般規則：

- *允許設定修改者* - 指定允許變更 *Firewall* 組態的使用者
- *顯示確認對話方塊的項目* - 指定向其顯示確認對話方塊（*要求對定義的 Firewall 規則*未涵蓋的情形給予確認的對話方塊）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



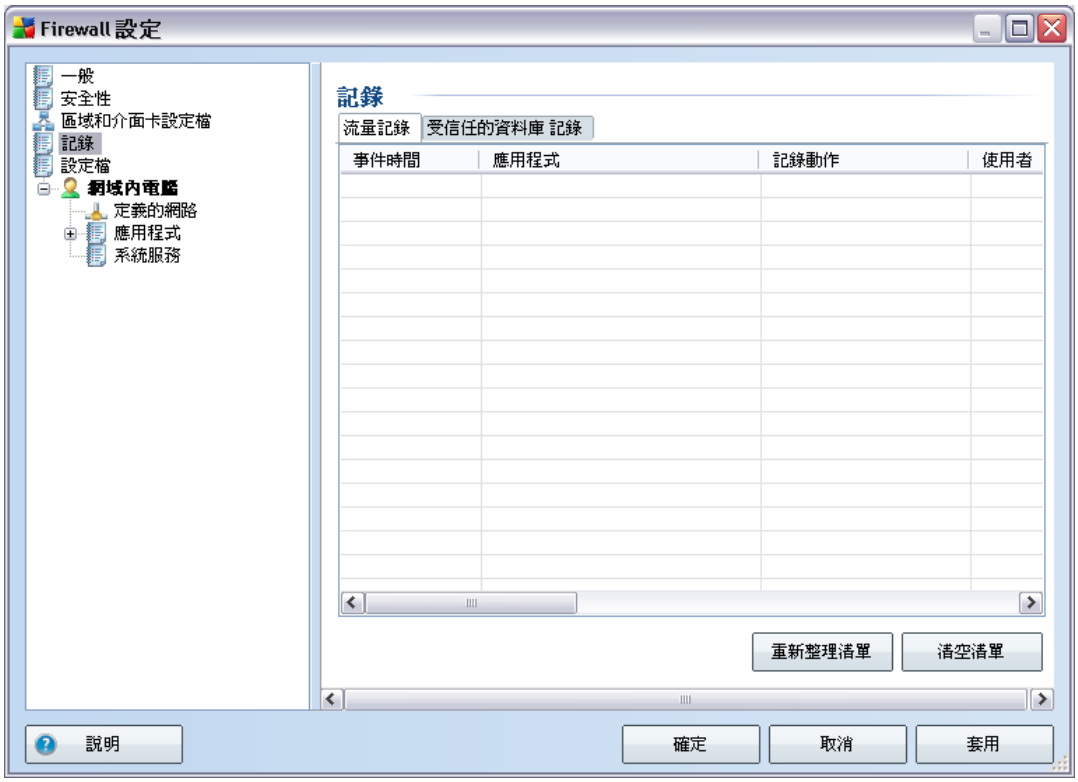
在*介面卡和網路區域設定*對話方塊中，您可以編輯相關設定，將已定義設定檔指派到特定介面卡和對應的網路：

- *停用區域偵測和自動設定檔切換* - 可將已定義的設定檔之一指派到各個網路介面類型，並分別指派到各個區域。如果您不希望定義特定設定檔，則將使用您在*安裝程序*期間選擇的電腦使用方式和電腦網路設計所定義的通用設定檔。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，請在介面卡清單中按一下對應項目，並選取設定檔。

- *進階設定* - 勾選對應選項將停用顯示資訊訊息的功能.

11.4. 記錄



*記錄*對話方塊可讓您檢閱所有已記錄的 *Firewall* 動作和事件清單，以及相關參數的詳細說明（*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*），這些資訊位於兩個標籤上：

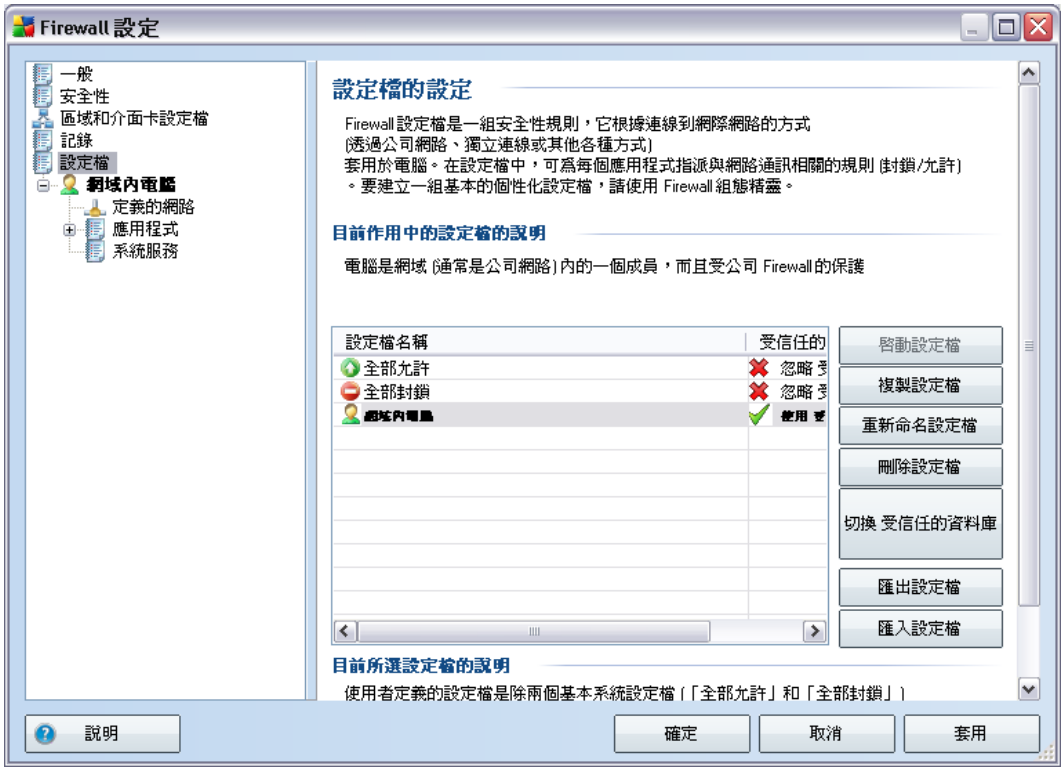
- *流量記錄* - 提供所有嘗試連線至網路的應用程式活動的相關資訊。
- *受信任的資料庫記錄* - *受信任的資料庫*是 AVG 的內部資料庫，會收集有關已認證和受信任的應用程式資訊，這些應用程式始終都允許進行線上通訊。當新應用程式第一次嘗試連線至網路（*亦即尚未針對此應用程式指定防火牆規則時*），有必要瞭解是否應該針對該應用程式允許網路通訊。首先，AVG 會搜尋*受信任的資料庫*，如果上面有列出該應用程式，便會自動授權存取網路。如果在搜尋資料庫之後，發現資料庫內沒有關於該應用程式的資訊，這時才會在獨立的對話方塊中詢問您是否要允許該應用程式存取網路。

控制按鈕

- *說明* - 開啟與此對話方塊相關的說明檔案。
- *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。
- *清空清單* - 刪除圖表中的所有項目。

11.5. 設定檔

在*設定檔的設定*對話方塊中，您可以找到所有可用設定檔的清單。



除系統設定檔以外的所有設定檔均可透過使用以下控制按鈕在此對話方塊中進行編輯：

- *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*** - 可讓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*** - 對於所選的設定檔，您可以決定使用*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
- *說明* - 開啟對話方塊相關的說明檔案

在對話方塊的底端部分，找到上述清單中目前選定的設定檔的說明。

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：

11.5.1. 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。

- ***將受信任的資料庫用於此設定檔*** - (*預設情況下為開啟*) 核取此選項可啟動個別設定檔的*受信任的資料庫* (*此為 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* - (*預設情況下為關閉*) 勾選此選項可允許 WMware 中的虛擬機器直接連線至網路

遊戲模式設定

在*遊戲模式設定*部分，您可透過勾選個別項目以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 (*通常為遊戲，但也適用於全螢幕應用程式，如 PPT 簡報*)。因為資訊訊息可能很容易產生干擾。

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*)，您可以允許或封鎖所有這些應用程式。

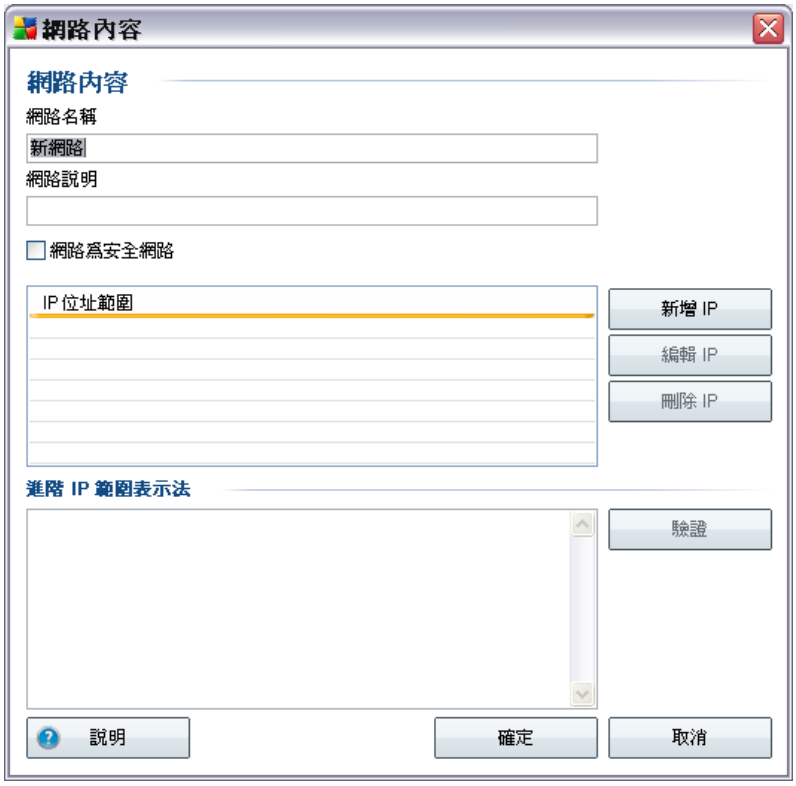
11.5.2. 定義的網路

*定義的網路*對話方塊提供電腦可連線的所有網路清單。針對每個偵測到的網路，提供以下資訊：

- *網路* - 與電腦連線的所有網路的名稱清單
- *網路安全* - 預設情況下，所有網路都被視為是不安全的，只有當您確定某個網路是安全的，才可以將它指派為安全的 (*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」*) - 然後，所有安全的網路才會包括到應用程式可以透過其進行通訊 (應用程式規則設為「允許安全」) 的群組中
- *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，您可在其中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***網路說明***，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*)，您可以在其中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，請參閱上段說明*)

- ***刪除網路*** - 從網路清單中移除所選網路的註釋。

- *標示為安全* - 在預設狀態下，所有網路都被視為不安全。只有當您確定某個網路為安全時，才應該用此按鈕來標示為安全 (*反之，一旦該網路被標示為安全，按鈕中的文字就會變成「標示為不安全」*)。

- *說明* - 開啟對話方塊相關的說明檔案

11.5.3. 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：

- 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
- 顯示詢問對話方塊 (*此時使用者能決定是允許還是封鎖此通訊*)
- 定義的進階設定

清單中的應用程式是在 *Firewall 組態精靈*搜尋期間或者日後 (若存在不明應用程式或新安裝應用程式) 在您電腦上偵測到的應用程式 (*且已為其指定對應動作*)。

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，您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*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)。

這些項目對於一般應用程式都會有不同的設定選項，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*** - 開啟原本的*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
- *說明* - 開啟對話方塊相關的說明檔案

在此對話方塊中，您可以為各個應用程式定義詳細的設定。

頁面動作

- *返回至清單*按鈕將顯示所有已定義應用程式規則的概觀。
- *刪除此規則*按鈕將刪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

在此部分填寫應用程式的*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通訊時，Firewall 該怎麼做：

- ***允許全部***將允許應用程式透過所有定義的網路和介面卡通訊，沒有任何限制。
- ***允許安全***將只允許應用程式透過定義為「安全」(受信任) 的網路通訊。
- ***封鎖***將自動禁止通訊；不允許應用程式連線到任何網路。
- ***詢問***將顯示一個對話方塊，讓您決定此時是要允許還是封鎖通訊。
- ***進階設定***在***應用程式詳細規則***部分的對話方塊底部進一步顯示更全面和詳細的設定選項。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部。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。如需刪除反白顯示的規則，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，在此輸入所有必要的詳細資訊。

11.5.4. 系統服務

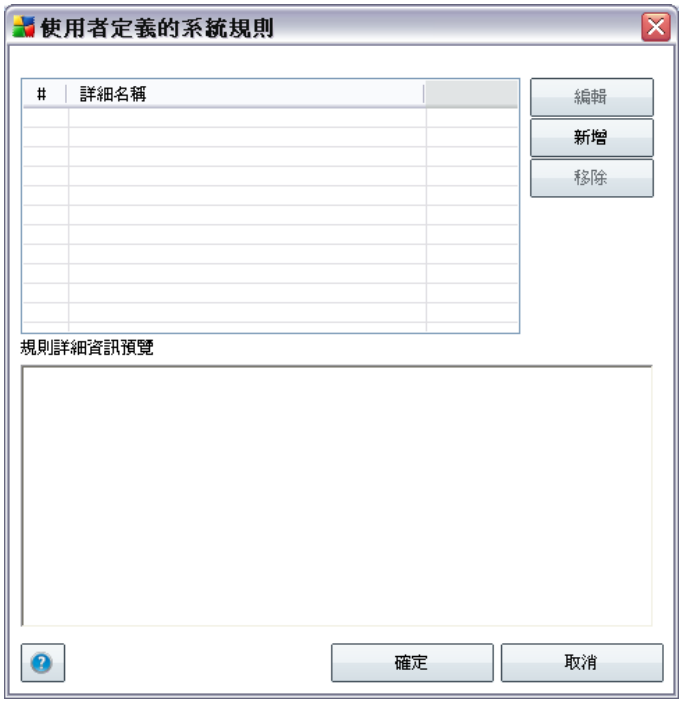
「系統服務和通訊協定」對話方塊內的所有編輯作業都只能由經驗豐富的使用者進行！

此***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。該圖表包含以下欄：

- ***記錄規則動作*** - 此方塊可讓您選擇將每次規則套用都記錄到記錄中。
- ***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*** - 此欄指示套用系統規則的具體網路。

您可以用下列按鈕來編輯清單內容 (*包含分派的動作*):

- 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***。
- 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***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按鈕來編輯、新增或者刪除; 製造商定義的規則詳細資訊只能被編輯:



警告: 這些詳細規則設定是進階設定, 主要供網路管理員使用, 他們需要對 Firewall 組態有完全的控制權。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*** – 核取此方塊可在記錄中記錄每個不明嘗試, 這些嘗試企圖

從外部連線到您的電腦。

- *記錄不明傳出流量* – 核取此方塊可在記錄中記錄每個不明嘗試，這些嘗試企圖從您的電腦連線到外部位置。

12. AVG 掃描

掃描是 AVG 9 Anti-Virus plus Firewall 功能中的關鍵部分。您可以執行按需測試，或是根據適當的時間排程測試以定期執行。

12.1. 掃描介面

AVG 掃描介面可透過*電腦掃描程式*快速連結存取。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：
  - *掃描整台電腦*
  - *掃描特定檔案或資料夾*
  - *Anti-Rootkit 掃描*
- 掃描排程部分 - 您在這裡可以按需要定義新的測試並建立新的排程。

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 9 Anti-Virus plus Firewall 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 9 Anti-Virus plus Firewall 中，您將看到軟體製造商預先定義的兩種掃描類型:

12.2.1. 掃描整台電腦

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*可以從掃描介面按一下掃描圖示直接啟動。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

您可以選擇編輯預先定義的預設設定：***掃描整台電腦***。請按下***變更掃描設定***連結，進入***變更掃描整台電腦的掃描設定***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*** - 在掃描參數清單中，您可以視需要開啟/關閉特定參數。預設情況下，大多數參數都已開啟，而且會在掃描期間自動套用。
- ***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*)，一個新選項將啟動，可使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* - 您應該進一步決定是否要掃描：

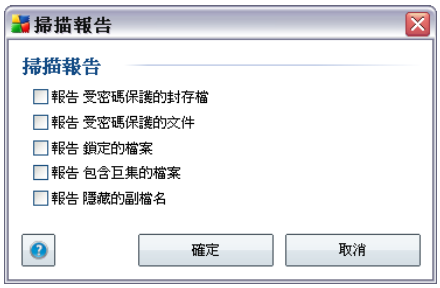
  - *所有檔案類型* - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名)，可定義掃描的例外；

  - *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。

- *掃描程序優先順序* - 您可以使用滑杆來變更掃描程序優先順序。預設情況下，優先順序設定為中等層級 (*自動掃描*)，使掃描程序速度和系統資源使用都能達到最佳化。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產生，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，請在自動產生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* - 在掃描參數清單中，您可以視需要開啟/關閉特定參數（*有關此設定的詳細描述，請參考* *AVG 進階設定/掃描/掃描特定檔案或資料夾*一章）。
- *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***), 一個新選項將啟動, 可使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*** - 您應該進一步決定是否要掃描:

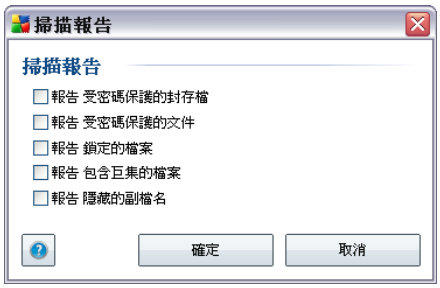
  - ***所有檔案類型*** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名), 可定義掃描例外;

  - ***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*** - 您可以使用滑杆來變更掃描程序優先順序。預設情況下, 優先順序設定為中等層級 (*自動掃描*), 使掃描程序速度和系統資源使用都能達到最佳化。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*)。

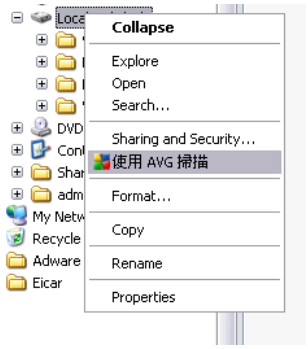
- ***設定其他掃描報告*** - 此連結會開啟新的***掃描報告***對話方塊, 您可以在這裡選取應報告哪些類型的結果:



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 / 如何掃描一章中所述。您若決定變更掃描特定檔案或資料夾的預設組態，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定義掃描之外，AVG 9 Anti-Virus plus Firewall 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，將您想要檢查的檔案 (或資料夾) 反白
- 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

12.4. 命令列掃描

在 AVG 9 Anti-Virus plus Firewall 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
- */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
- */MACROW* 報告巨集
- */PWDW* 報告受密碼保護的檔案
- */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「潛在的垃圾程式」
- */REG* 掃描登錄
- */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)

12.5. 掃描排程

您可以使用 AVG 9 Anti-Virus plus Firewall 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***的部分：

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作用中，您可以按下按鈕切換至***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***完整電腦掃描排程***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* (*自動將您重新導向到的預設標籤*)、***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。請儘量替掃描取簡短、恰當的說明性名稱，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」則是恰當的說明性名稱示例。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*** - 此部分允許您定義（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

在*排程掃描的設定*對話方塊的三個標籤 (*排程設定*、*如何掃描*及*掃描內容*) 上均有兩個控制按鈕可用，不管您目前位於哪個標籤，這些按鈕都具有相同的功能：

- *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定義的組態：

- *自動修復/移除感染檔案* - (*預設情況下為開啟*)：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)。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。間諜軟體代表一個可疑的惡意軟體類別：雖然它通常代表安全性上的風險，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。

- *報告延伸性的潛在垃圾程式* – 當前一個選項啟動之後，您也可以核取此方塊來偵測廣義的間諜軟體：當您直接向製造商購買時，該軟體完全正常而且無害，但稍後可能會被不肖份子用來作惡。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* - (*預設情況下為開啟*)：這個 *Anti-Spyware* 元件參數規定在掃描期間應偵測 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*)；

- *掃描內部封存* - (*預設情況下為開啟*)：此參數定義掃描應檢查所有檔案，即使這些檔案已封裝在某種封存內，如 ZIP、RAR...

- *使用啟發法* - (*預設情況下為開啟*)：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* - (*預設情況下為開啟*)：掃描還會檢查電腦的系統區域；

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：

- *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*)，一個新選項將啟動，可使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* - 您應該進一步決定是否要掃描：

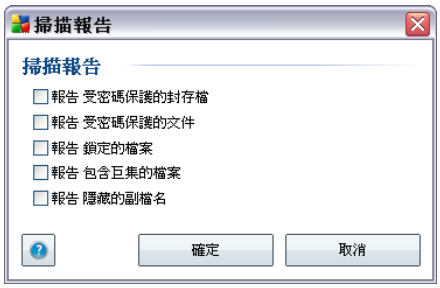
  - *所有檔案類型* - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名)，可定義掃描例外；

  - *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* - 您可以使用滑杆來變更掃描程序優先順序。預設情況下，優先順序設定為中等層級 (*自動掃描*)，使掃描程序速度和系統資源使用都能達到最佳化。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：



注意：預設情況下，掃描組態已為提供最佳效能而進行相應設定。除非您確實需要變更掃描設定，否則強烈建議您保留預定義的組態。任何組態變更只能由有經驗的使用者來進行。如需更多掃描組態選項，請參閱進階設定對話方塊，該對話方塊可透過檔案 / 進階設定系統功能表項目存取。

控制按鈕

*排程掃描的設定*對話方塊的三個標籤上 (*排程設定*、*如何掃描*和*掃描內容*) 均提供兩個控制按鈕，並且無論您正位於哪個標籤，它們的功能都是相同的：

- *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，此對話方塊的底部會顯示已啟動的樹狀結構圖，您可在此指定想要掃描的資料夾 (*按一下加號可以展開項目，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*)。

在此樹狀結構圖中，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\
- *我的文件資料夾* - C:\Documents and Settings\User\My Documents\
- *共用文件* - C:\Documents and Settings\All Users\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 – Windows/System32
  - 暫存檔資料夾 – Documents and Settings/User/Local Settings/Temp
  - Temporary Internet Files – Documents and Settings/User/Local Settings/Temporary Internet Files

「排程掃描的設定」對話方塊的控制按鈕

在*排程掃描的設定*對話方塊的三個標籤 (*排程設定*、*如何掃描*及*掃描內容*) 上均有兩個控制按鈕可用，不管您目前位於哪個標籤，這些按鈕都具有相同的功能:

- *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

- *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，有關無法掃描物件的資訊也會在這裡顯示 (例如：受到密碼保護的封存)。

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。此標籤分為三個部分，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*

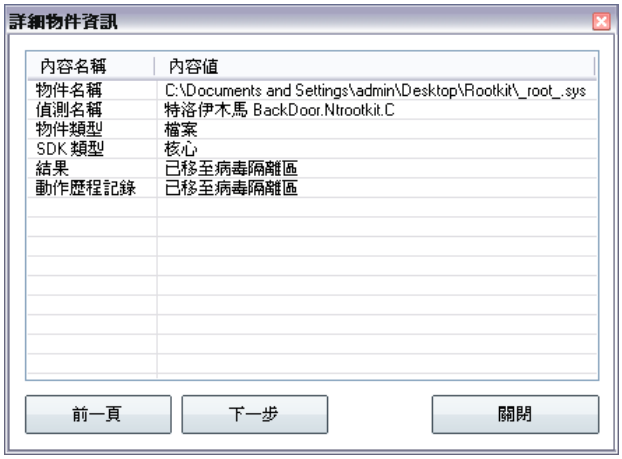
進階設定的PUP 例外對話方塊中組態)

- *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*詳細掃描結果資訊*的新對話方塊視窗：



在此對話方塊中，您可以找到已偵測到的受感染物件的位置資訊 (*內容名稱*)。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。

- *移除所選的感染* - 使用此按鈕可將所選結果移到*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

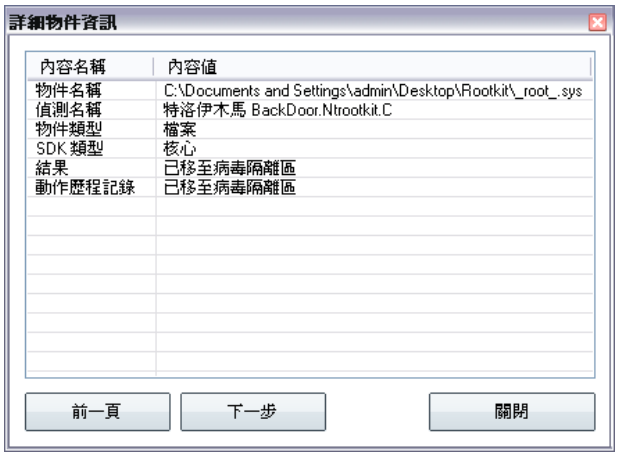
*掃描結果*對話方塊只有在掃描期間偵測到*間諜軟體*時，才會顯示間諜軟體標籤。此標籤分為三個部分，提供了以下資訊：

- *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*詳細掃描結果資訊*的新對話方塊視窗：



在此對話方塊中，您可以找到已偵測到的受感染物件的位置資訊 (*內容名稱*)。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。

- *移除所選的感染* - 使用此按鈕可將所選結果移到*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 AVG 測試只偵測到「警告」，就沒有必要採取任何動作。

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。如果您懷疑 AVG 報告的隱藏檔案可能是惡意內容，可將它移到您的 *AVG 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

如果您已啟動 *Anti-Rootkit 掃描*，或已將 Anti-rootkit 掃描選項手動新增至***掃描整台電腦*** (*此選項預設為關閉*)，那麼*Rootkit* 標籤會顯示掃描期間偵測到的 rootkit 的相關資訊。

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 掃描能夠偵測出可能沒有被感染但可疑的檔案。這些檔案會被報告為*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。
- *受密碼保護的封存或文件* - AVG (*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。
- *帶巨集的文件* - 報告的文件包含巨集，且可能是惡意巨集。
- *隱藏副檔名* - 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*)。在 Windows 中預設情況下看不到第二個副檔名，而 AVG 會報告此類檔案以防意外被開啟。
- *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*)，AVG 會報告此項差異。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 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* - 資訊 (*依其感染層級- - 所有列出的物件都有肯定或潛在的感染*)
- *病毒名稱* - 依據病毒大全 (線上) 為偵測到的感染指定名稱
- *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* - 如果您決定將偵測到的感染物件從*病毒隔離區*移到某個選定的資料夾中，請使用此按鈕，偵測到的可疑物件將使用其原始名稱進行儲存。如果原始名稱未知，則會使用標準名稱。
- *詳細資訊* - 該按鈕通常用於 *Identity Protection*偵測到的威脅。若按下按鈕，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

為了確保可以儘快偵測到所有新發現的病毒，讓您的 AVG 保持在最新狀態極其重要。

在 AVG 安裝程序中，您可選擇多久更新 AVG 一次。提供的選項包括*每 4 小時*或者*每天*(請見*排程定期掃描和更新*對話方塊)。由於 AVG 更新是根據新威脅的數量和嚴重性不定期發佈，因此建議您至少每天檢查一次是否有新的更新。每 4 小時更新一次能保證您的 AVG 9 Anti-Virus plus Firewall 在一天中隨時保持更新狀態。

13.1. 更新層級

AVG 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，可以選取應下載和套用哪個優先順序的更新。

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。

13.2. 更新類型

您可以區分兩種類型的更新：

- *按需更新* - 這是可隨時在需要時執行的一種即時 AVG 更新。
- *排程的更新* - 在 AVG 中，還可以預設更新計劃。此後，計劃的更新會依據設定的組態定期執行。無論何時在指定位置上出現新的更新檔案，均可直接從網際網路或網路目錄中下載這些檔案。如果沒有新的更新出現，則不會執行任何動作。

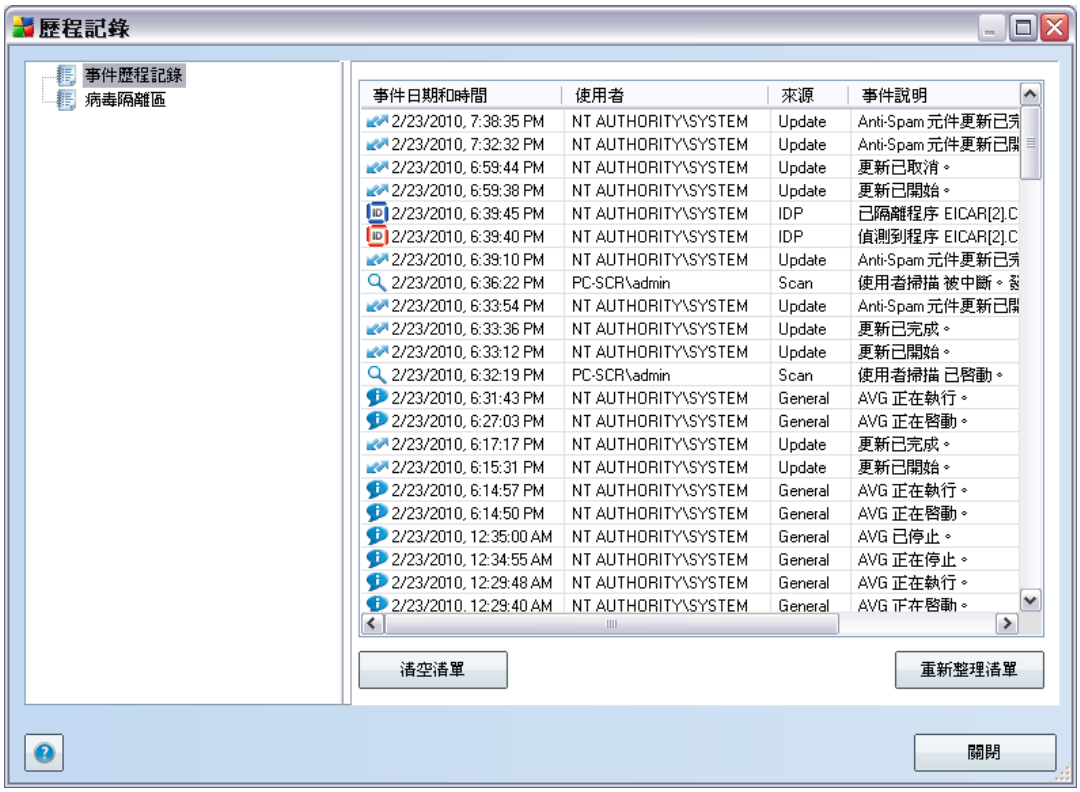
13.3. 更新程序

按一下*立即更新*快速連結即可在需要時立即啟動更新程序。該連結可隨時從任何 AVG 使用者介面對話方塊中找到。但是，還是強烈建議您根據可以在更新管理員元件中編輯的更新排程執行定期更新。

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 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。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！

14. 事件歷程記錄



*事件歷程記錄*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 9 Anti-Virus plus Firewall 作業期間發生的重要事件摘要。*事件歷程記錄*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 (包括自動執行的測試)
- 與病毒偵測關聯的事件 (透過 Resident Shield 或掃描)，包括發生位置
- 其他重要事件

控制按鈕

- *清空清單* - 刪除事件清單中的所有項目

- *重新整理清單* - 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 有任何業務或技術方面的問題，請參閱 AVG 網站的*常見問題集*部分 (http://www.avg.com/)。

如果按此方法沒有找到協助，請透過電子郵件聯絡技術支援部。請透過*說明 / 取得線上說明*，使用可從系統功能表存取的聯絡表。