



AVG Anti-Virus 2011

使用者手冊

文件修訂版 2011.21 (16.5.2011)

版權所有 AVG Technologies CZ, s.r.o. 保留所有權利。
所有其他商標均歸各自所有者擁有。

此產品採用了 RSA Data Security, Inc. 的 MD5 報文摘要演算法，版權所有 (C) 1991-2, RSA Data Security, Inc. 1991 年建立。
此產品使用來自 C-SaCzech 程式庫的程式碼，版權所有 (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz)。
此產品使用了 zlib 壓縮程式庫，版權所有 (c) 1995-2002 Jean-loup Gailly and Mark Adler。
此產品使用 libbzip2 壓縮程式庫，版權所有 (c) 1996-2002 Julian R. Seward



內容

1. 簡介	7
2. AVG 安裝需求	8
2.1 支援的作業系統	8
2.2 最低和建議的硬體需求	8
3. AVG 安裝選項	9
4. AVG 安裝程序	10
4.1 歡迎	10
4.2 啟動您的 AVG 授權	10
4.3 選取安裝類型	11
4.4 自訂選項	12
4.5 安裝 AVG Security Toolbar	13
4.6 安裝進度	14
4.7 安裝成功	14
5. 安裝之後	16
5.1 產品註冊	16
5.2 存取使用者介面	16
5.3 掃描整台電腦	16
5.4 Eicar 測試	16
5.5 AVG 預設組態	17
6. AVG 使用者介面	18
6.1 系統功能表	19
6.1.1 檔案	19
6.1.2 元件	19
6.1.3 歷程記錄	19
6.1.4 工具	19
6.1.5 說明	19
6.2 安全性狀態資訊	21
6.3 快速連結	22
6.4 元件概觀	22
6.5 統計資料	23
6.6 系統匣圖示	24
6.7 AVG 小工具	25



7. AVG 元件	27
7.1 Anti-Virus	27
7.1.1 Anti-Virus 原理	27
7.1.2 Anti-Virus 介面	27
7.2 Anti-Spyware	28
7.2.1 Anti-Spyware 原理	28
7.2.2 Anti-Spyware 介面	28
7.3 Link Scanner	30
7.3.1 Link Scanner 原理	30
7.3.2 Link Scanner 介面	30
7.3.3 Search-Shield	30
7.3.4 Surf-Shield	30
7.4 Resident Shield	33
7.4.1 Resident Shield 原理	33
7.4.2 Resident Shield 介面	33
7.4.3 Resident Shield 偵測	33
7.5 Family Safety	38
7.6 AVG LiveKive	38
7.7 E-mail Scanner	38
7.7.1 E-mail Scanner 原理	38
7.7.2 E-mail Scanner 介面	38
7.7.3 E-mail Scanner 偵測	38
7.8 更新管理員	41
7.8.1 「更新管理員」原理	41
7.8.2 「更新管理員」介面	41
7.9 授權	43
7.10 Remote Administration	44
7.11 Online Shield	45
7.11.1 Online Shield 原理	45
7.11.2 Online Shield 介面	45
7.11.3 Online Shield 偵測	45
7.12 Anti-Rootkit	48
7.12.1 Anti-Rootkit 原理	48
7.12.2 Anti-Rootkit 介面	48
7.13 PC 分析程式	50
7.14 ID Protection	52
7.14.1 ID Protection 原理	52



7.14.2 ID Protection 介面	52
7.15 Security Toolbar	54
8. AVG Security Toolbar	56
8.1 AVG Security Toolbar 介面	56
8.1.1 AVG 標誌 按鈕	56
8.1.2 AVG Secure Search (powered by Google) 支援的搜尋方塊	56
8.1.3 頁面狀態	56
8.1.4 AVG 新聞	56
8.1.5 新聞	56
8.1.6 刪除歷程記錄	56
8.1.7 電子郵件通知程式	56
8.1.8 氣候資訊	56
8.1.9 Facebook	56
8.2 AVG Security Toolbar 選項	63
8.2.1 「一般設定」標籤	63
8.2.2 「實用按鈕」標籤	63
8.2.3 「安全性」標籤	63
8.2.4 「進階選項」標籤	63
9. AVG 進階設定	67
9.1 外觀	67
9.2 聲音	69
9.3 忽略故障狀況	70
9.4 病毒隔離區	71
9.5 PUP 例外	71
9.6 Online Shield	74
9.6.1 網頁保護	74
9.6.2 即時訊息	74
9.7 Link Scanner	77
9.8 掃描	78
9.8.1 掃描整台電腦	78
9.8.2 殼層延伸掃描	78
9.8.3 掃描特定檔案或資料夾	78
9.8.4 卸除式裝置掃描	78
9.9 排程	83
9.9.1 排程掃描	83
9.9.2 病毒庫更新排程	83
9.9.3 程式更新排程	83



9.10 E-mail Scanner	93
9.10.1 認證	93
9.10.2 郵件篩選	93
9.10.3 伺服器	93
9.11 Resident Shield	101
9.11.1 進階設定	101
9.11.2 排除的項目	101
9.12 快取伺服器	105
9.13 Anti-Rootkit	106
9.14 更新	107
9.14.1 代理	107
9.14.2 撥號連線	107
9.14.3 URL	107
9.14.4 管理	107
9.15 暫時停用 AVG 保護	114
9.16 產品改進計劃	114
10. AVG 掃描	117
10.1 掃描介面	117
10.2 預定義的掃描	118
10.2.1 完整電腦掃描	118
10.2.2 掃描特定檔案或資料夾	118
10.2.3 Anti-Rootkit 掃描	118
10.3 在 Windows 檔案總管中掃描	127
10.4 命令列掃描	128
10.4.1 CMD 掃描參數	128
10.5 掃描排程	130
10.5.1 排程設定	130
10.5.2 如何掃描	130
10.5.3 掃描內容	130
10.6 掃描結果概觀	138
10.7 掃描結果詳細資訊	139
10.7.1 「結果概觀」標籤	139
10.7.2 「感染」標籤	139
10.7.3 「間諜軟體」標籤	139
10.7.4 「警告」標籤	139
10.7.5 Rootkit 標籤	139
10.7.6 「資訊」標籤	139



10.8 病毒隔離區	146
11. AVG 更新	148
11.1 更新層級	148
11.2 更新類型	148
11.3 更新程序	148
12. 事件歷程記錄	149
13. 常見問題集和技術支援	151



1. 簡介

本使用者手冊提供有關 **AVG Anti-Virus 2011** 的詳細介紹。

感謝您購買 AVG Anti-Virus 2011 ！

AVG Anti-Virus 2011 是獲獎的 AVG 產品系列之一，它能夠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 Anti-Virus 2011** 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 Anti-Virus 2011** 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。

所有 **AVG** 產品提供

- 依照您使用電腦和網際網路：網路銀行和購物、上網和搜尋、聊天和傳送電子郵件，或是社交的方式提供保護 - AVG 有適合您的安全保護產品。
- 受到世界各地 1 億 1 千萬人信賴以及經過全球經驗豐富的研究人員所加強的安全保護，一點也不麻煩
- 由全天候的專家支援所支持的保護



2. AVG 安裝需求

2.1. 支援的作業系統

AVG Anti-Virus 2011 可保護執行下列作業系統的工作站：

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

(以及特定作業系統可能更高版本的服務套件)

注意：Windows XP x64 上不支援 [ID Protection](#) 元件。您還是可以在此作業系統中安裝 AVG Anti-Virus 2011，但僅限於不含 IDP 元件的版本。

2.2. 最低和建議的硬體需求

AVG Anti-Virus 2011 的最低硬體需求：

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

AVG Anti-Virus 2011 的建議硬體需求：

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM 記憶體
- 1400 MB 可用硬碟空間 (用於安裝)



3. AVG 安裝選項

您可以使用安裝 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，強烈建議您瀏覽 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 Anti-Virus 2011**。

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 安裝程序

要將 **AVG Anti-Virus 2011** 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](#) 區段下載安裝檔。

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描述。下面提供了每個對話方塊視窗的說明：

4.1. 歡迎

安裝程序啟動時會顯示 **歡迎** 對話方塊視窗。您在這裡選取用於安裝程序的語言，以及 AVG 使用者介面的預設語言。在對話方塊視窗的上半部可以找到下拉式功能表，當中有您可以選擇的語言清單：



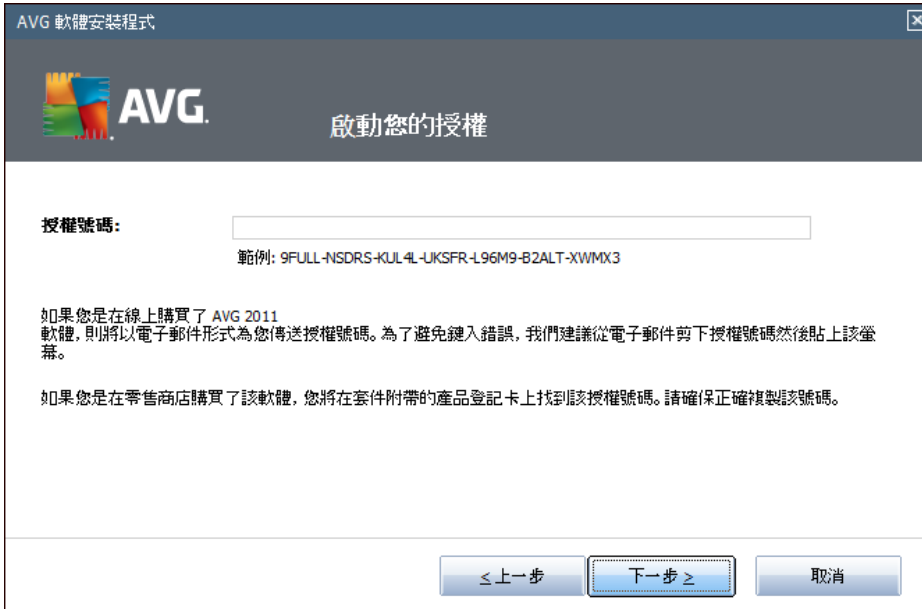
請注意：您在此處選取的是用於安裝程序的語言。您所選的語言將安裝為 AVG 使用者介面的預設語言，並且會自動同時安裝英文。如果您希望為使用者介面安裝其他語言，請在以下名為 [自訂選項](#) 的安裝對話方塊之一中進行定義。

該對話方塊還會提供 AVG 授權合約的完整內文。請仔細閱讀。若要確認您已閱讀、了解並接受合約，請按一下 **接受** 按鈕。如果您不同意授權合約，請按一下 **拒絕** 按鈕，安裝程序隨後將立即終止。

4.2. 啟動您的 AVG 授權

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

銷售號碼位於您的 **AVG Anti-Virus 2011** 盒子 CD 包裝上。授權號碼位於您在線上購買 **AVG Anti-Virus 2011** 後收到的確認電子郵件內。您必須完全按照顯示的號碼準確鍵入。若有提供電子形式的授權號碼（在電子郵件內），建議使用複製和貼上方法插入此號碼。



按下下一步按鈕繼續執行安裝程序。

4.3. 選取安裝類型



選取安裝類型對話方塊提供兩種安裝選項：**快速安裝**和**自訂安裝**。

對於大多數使用者，強烈建議使用**快速安裝**，它會以完全自動的模式，使用程式廠商預先定義的設定來安裝 AVG。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。如果您已選取**快速安裝**選項，按一下**下一步**按鈕可前進至接下來的**安裝 AVG Security Toolbar**對話方塊。



自訂安裝應該只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）。選取此選項後，按一下下一步按鈕可前進至 [自訂選項](#) 對話方塊。

您可以在對話方塊的右側區段找到與 [AVG 小工具](#)（在 Windows Vista/Windows 7 中有支援）相關的核取方塊。如果您希望安裝這個小工具，請標記相應的核取方塊。[AVG 小工具](#) 隨後就可以從 Windows 資訊看板存取，讓您立即存取 **AVG Anti-Virus 2011** 最重要的功能，亦即 [掃描](#) 和 [更新](#)。

4.4. 自訂選項

自訂選項對話方塊可讓您設定兩種安裝參數：



目標資料夾

在對話方塊中的 **目標資料夾** 區段，您應指定 **AVG Anti-Virus 2011** 應該安裝的位置。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。

元件選取

元件選取 區段提供所有可安裝的 **AVG Anti-Virus 2011** 元件的概觀。如果預設設定不符合您的需求，您可以移除 / 新增特定元件。

不過，您只能從您購買的 AVG 版本所含的元件中選取！

亮顯 **元件選取** 清單中的任何項目，個別元件的簡短描述即會顯示在此區段的右側。如需各個元件功能的詳細資訊，請查閱本文件的 [元件概觀](#) 一章。若要還原軟體廠商預先設定



的預設組態，請使用預設值按鈕。

按下下一步按鈕繼續。

4.5. 安裝 AVG Security Toolbar



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

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



4.6. 安裝進度

安裝進度對話方塊會顯示安裝程序的進度，完全無需任何操作：



安裝程序完成後，會將您重新導向至下一個對話方塊。

4.7. 安裝成功



安裝成功對話方塊確認您的 **AVG Anti-Virus 2011** 已安裝及設定完成。



請在此對話方塊中提供您的聯絡資訊，以便接收所有產品相關資訊和新聞。在註冊表下方，您會看到以下兩個選項：

- **是，透過電子郵件通知我安全性新聞和 AVG 2011 優惠** - 標記此核取方塊以表示您想要收到有關 Internet Security 方面的最新消息的通知，並且希望收到有關 AVG 產品優惠、改進和升級等資訊。
- **我同意參與 AVG 2011 網路安全和產品改進計劃...** - 標記此核取方塊以同意您想要參與產品改進計劃 (詳細資訊請參閱 [AVG 進階設定/產品改進計劃](#) 一章)，本計劃會收集有關偵測到的威脅的匿名資訊，以便提高整體網際網路安全性層級。

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

注意：如果使用任何 AVG 企業授權，而且您之前選擇安裝 Remote Administration 項目 (請參閱 [自訂選項](#))，則會出現「安裝成功」對話方塊並顯示下列介面：

您需要指定 AVG DataCenter 參數 - 請以 server:port 的形式提供連線字串給 AVG DataCenter。如果目前沒有此資訊，請將該欄位留空，之後再在進階設定/**Remote Administration** 對話方塊內設定該組態。有關 AVG Remote Administration 的詳細資訊，請參閱 AVG Business Edition 使用者手冊，此手冊可從 AVG 網站 (<http://www.avg.com/>) 下載。



5. 安裝之後

5.1. 產品註冊

完成 **AVG Anti-Virus 2011** 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。

5.2. 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 [AVG 系統匣圖示](#)
- 連按兩下桌面上的 AVG 圖示
- 連按兩下位於 [AVG 小工具](#)（若有安裝的話；在 Windows Vista/ Windows 7 上有支援）
- 存取 **開始 / 所有程式 / AVG 2011 / AVG 使用者介面的功能表**
- 從 [AVG Security Toolbar](#) 透過 **啟動 AVG**

5.3. 掃描整台電腦

電腦病毒很有可能在安裝 **AVG Anti-Virus 2011** 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。

5.4. Eicar 測試

如果要確認 **AVG Anti-Virus 2011** 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](http://www.eicar.com) 檔案，並將其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其儲存在本機磁碟中。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！

5.5. AVG 預設組態

AVG Anti-Virus 2011 的預設組態（即應用程式在剛安裝好時的設定狀態）是由軟體廠商設定，所有元件和功能都經過調整以發揮最佳效能。

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

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



6. AVG 使用者介面

AVG Anti-Virus 2011 開啟時會顯示主視窗：



主視窗由若干區段構成：

- **系統功能表**（視窗頂端的系統行）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**（視窗的上方區段）提供有關 AVG 程式目前狀態的資訊 - [詳細資訊 >>](#)
- **快速連結**（視窗左邊區段）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**（視窗中間區段）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 >>](#)
- **AVG 小工具**（Windows 資訊看板，在 Windows Vista/7 中有支援）可允許快速存取 AVG 掃描和更新 - [詳細資訊 >>](#)



6.1. 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 Anti-Virus 2011** 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：

6.1.1. 檔案

- **結束** - 關閉 **AVG Anti-Virus 2011** 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！

6.1.2. 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** 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** 可保證您的電腦受到保護，免遭間諜軟體和廣告軟體的侵擾 - [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 >>](#)
- **E-mail Scanner** 檢查所有傳入和傳出的郵件是否有病毒 - [詳細資訊 >>](#)
- **家庭安全** 幫助監視您小孩的線上活動，並防止他們瀏覽不當的網站內容 - [詳細資訊 >>](#)
- **LiveKive** 為您的線上資料提供自動備份 - [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 >>](#)
- **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 >>](#)
- **Anti-Rootkit** 偵測想要隱藏惡意軟體的程式和技術 - [詳細資訊 >>](#)
- **PC 分析程式** 提供有關您電腦狀態的資訊 - [詳細資訊 >>](#)
- **Identity Protection** - 此反惡意軟體元件主要關注的是防止身分盜用者竊取您珍貴的個人數位資產 - [詳細資訊 >>](#)
- **Security Toolbar** 讓您直接從您的網際網路瀏覽器使用所選的 AVG 功能 - [詳細資訊 >>](#)



[訊 >>](#)

- **Remote Administration** 只有在您於[安裝程序](#)期間指定安裝此元件，才會顯示在 AVG Network Edition 中

6.1.3. 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。將受感染的檔案隔離到此隔離區域後，您電腦的安全即可獲得保障，同時受感染的檔案也會儲存下來，以供日後修復之用
- [事件歷程記錄](#) - 開啟包含所有記錄的 **AVG Anti-Virus 2011** 動作概觀的歷程記錄介面

6.1.4. 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目錄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目錄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 Anti-Virus 2011**。
- [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 Anti-Virus 2011** 組態。通常建議保留由軟體廠商定義的應用程式之預設設定。

6.1.5. 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 Anti-Virus 2011 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 Anti-Virus 2011** 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 **授權區段**。

- **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。

6.2. 安全性狀態資訊

安全性狀態資訊 區段位於 AVG 主視窗的頂端。您始終可以在這個區段找到有關 **AVG Anti-Virus 2011** 目前安全性狀態的資訊。請參閱此區段中可能描述的圖示概觀及其含義：



— 綠色圖示表示 AVG 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，您必須檢查其屬性 / 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** 區段提供。

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！一個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。

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



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

請注意：AVG 狀態資訊也可隨時從[系統匣圖示](#)中取得。

6.3. 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已開啟的 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 >>](#)
- **立即掃描** - 預設情況下，該按鈕會提供上一次啟動的掃描的資訊 (*掃描類型、上次啟動的日期*)。您可以執行 **立即掃描** 命令來重新啟動同一個掃描，或是遵循 **掃描選項** 連結來開啟 AVG 掃描介面，您可以在此處執行掃描、排程掃描，或編輯其參數 - 請參閱 [AVG 掃描一章 >>](#)
- **立即更新** - 該連結提供上次啟動更新程序的日期。按一下該按鈕可開啟更新介面，並立即執行 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。

6.4. 元件概觀

元件概觀 區段位於 [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使用中還是非使用中的資訊
- 所選元件的說明

在 **AVG Anti-Virus 2011** 中，**元件概觀** 區段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** 可保證您的電腦受到保護，免遭間諜軟體和廣告軟體的侵擾 - [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 >>](#)
- **E-mail Scanner** 檢查所有傳入和傳出的郵件是否有病毒 - [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 >>](#)
- **家庭安全** 幫助監視您小孩的線上活動，並防止他們瀏覽不當的網站內容 - [詳細資訊 >>](#)
- **LiveKive** 為您的線上資料提供自動備份 - [詳細資訊 >>](#)
- **更新管理員** 控制所有 AVG 更新 - [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 >>](#)
- **Anti-Rootkit** 偵測想要隱藏惡意軟體的程式和技術 - [詳細資訊 >>](#)
- **PC 分析程式** 提供有關您電腦狀態的資訊 - [詳細資訊 >>](#)
- **Identity Protection** - 此反惡意軟體元件主要關注的是防止身分盜用者竊取您珍貴的個人數位資產 - [詳細資訊 >>](#)
- **Security Toolbar** 可讓您直接從您的網際網路瀏覽器存取所選的 AVG 功能 - [詳細資訊 >>](#)
- **Remote Administration** 只有在您於 [安裝程序](#) 期間指定安裝此元件時，才會顯示在 AVG Network Edition 中

按一下任何元件的圖示即可在元件概觀中亮顯該元件。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。

6.5. 統計資料

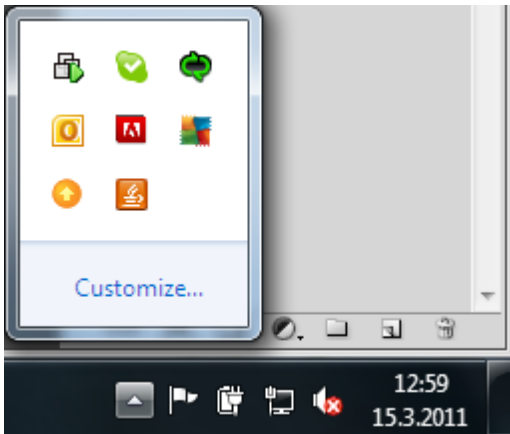
統計資料區段位於 [AVG 使用者介面](#) 的左下方。它提供有關程式作業的資訊清單：



- **病毒庫** - 告知目前安裝的病毒庫的版本
- **AVG 版本** - 通知您有關所安裝的 AVG 版本（編號是以 10.0.xxxx 的形式顯示，當中 10.0 是產品系列版本，而 xxxx 則代表組建的號碼）
- **授權到期** - 提供 AVG 授權到期的日期



6.6. 系統匣圖示

系統匣圖示 (位於 Windows 工具列中) 顯示 AVG Anti-Virus 2011 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 元件都在使用中，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、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](#)
- 掃描 - 按一下此選項可開啟
- 執行 PC 分析程式 - 按一下該選項可啟動 [PC 分析程式](#) 元件
- 執行中的掃描 - 此項目只有在您電腦上目前有正在執行的掃描時才會顯示。您之後可以設定此掃描的優先順序，或是選擇停止或暫停執行中的掃描。接下來，可存取以下動作：設定所有掃描的優先順序、暫停所有掃描或停止所有掃描。
- 立即更新 - 可啟動即時 [更新](#)
- 說明 - 在開始頁開啟說明檔案





6.7. AVG 小工具

AVG 小工具會顯示在 Windows 桌面 (Windows 資訊看板) 上。此應用程式只在 Windows Vista 和 Windows 7 作業系統中有支援。AVG 小工具提供對最重要的 AVG Anti-Virus 2011 功能的立即存取，亦即[掃描](#)和[更新](#)功能：




AVG 小工具提供下列快速存取選項：

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






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



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



- **Facebook 連結**  - 在 Facebook 網站上開啟您的網際網路瀏覽器，特別是開啟在 **AVG 社群** 頁面
- **LinkedIn**  - 此選項僅在網路安裝中可用 (亦即使用 *AVG Business Editions* 其中一種授權安裝 AVG)，而且它會從 LinkedIn 社交網路中將 Internet 瀏覽器開啟到 **AVG SMB Community** 網站
- **PC 分析程式**  - 開啟 **PC 分析程式** 元件中的使用者介面
- **搜尋方塊** - 輸入關鍵字並且使用您的預設網頁瀏覽器在新開啟的視窗立即取得搜尋結果



7. AVG 元件

7.1. Anti-Virus

7.1.1. 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！

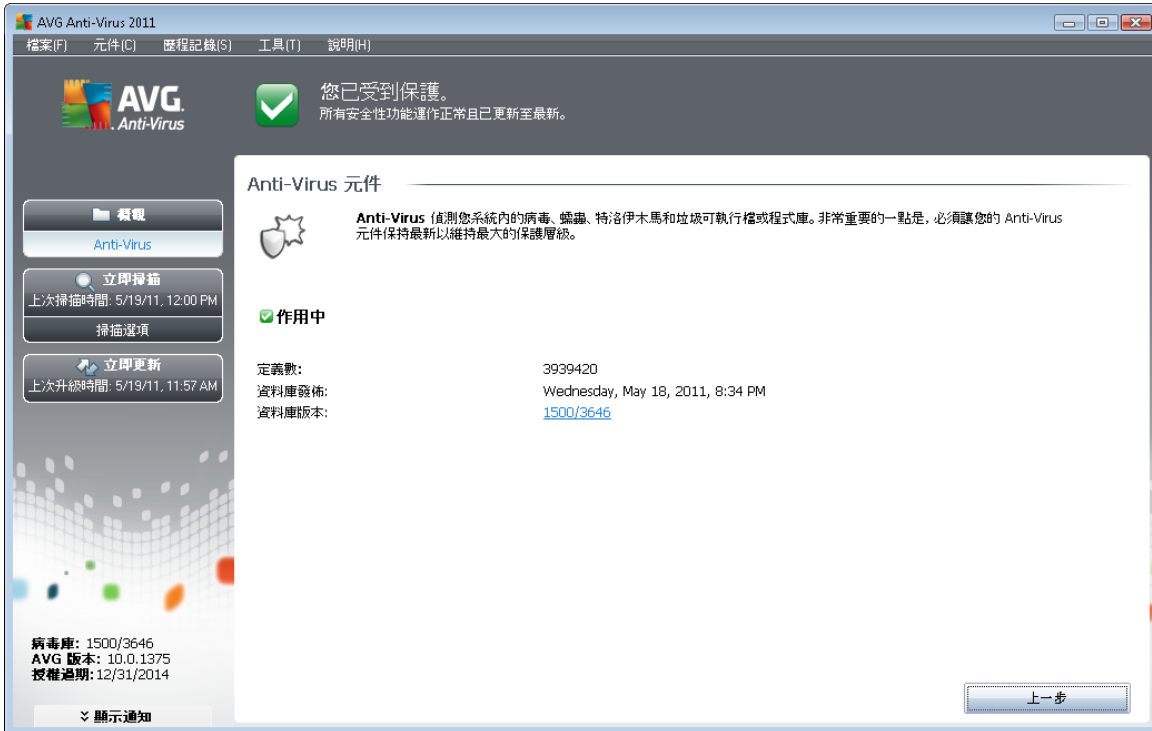
單靠一種技術可能無法充分偵測或識別病毒，因此 **Anti-Virus** 結合了多種技術來確保您的電腦不受病毒侵擾：

- 掃描 - 搜尋具備特定病毒特性的字元字串
- 啟發法分析 - 在虛擬電腦環境中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「潛在不受歡迎程式」(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、暫存網際網路檔案和追蹤 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。



7.1.2. 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** 元件處於使用中狀態時），以及 **Anti-Virus** 統計資料的簡短概觀：

- **定義數** - 此數字提供最新的病毒庫版本中已定義的病毒計數
- **資料庫發行** - 指出病毒庫上一次更新的時間
- **資料庫版本** - 定義最近安裝的病毒庫版本的編號；此編號將隨著病毒庫的更新而遞增

此元件的介面內只有一個可操作的按鈕（[上一步](#)） - 按一下此按鈕可返回至預設的 [AVG 使用者介面](#)（[元件概觀](#)）。

7.2. Anti-Spyware

7.2.1. Anti-Spyware 原理

間諜軟體通常被定義為惡意軟體的一種，即在使用者不知情或未經其同意的情況下從使用者電腦收集資訊的軟體。某些間諜軟體應用程式也可能是有意安裝，且往往包含廣告、快顯視窗或各式各樣令人不悅的軟體。

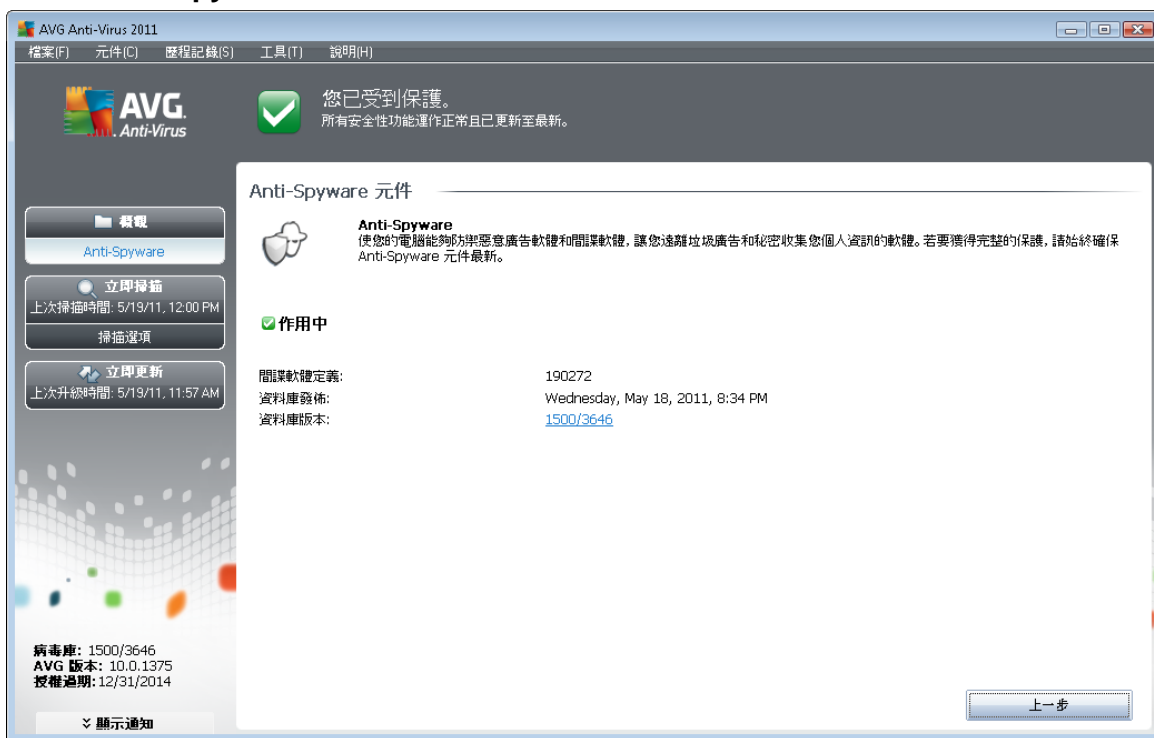
目前，最常見的感染來源是含有潛在危險內容的網站。其他傳輸方式也很普遍，例如透過蠕蟲或病毒傳播的電子郵件或傳輸。最重要的防護措施就是使用永遠開啟的幕後掃描



程式 **Anti-Spyware**，這是一種常駐防護，當您執行應用程式時，它會在幕後掃描應用程式。

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 Anti-Virus 2011** 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使用中的惡意軟體，即已下載但尚未啟動的惡意軟體。

7.2.2. Anti-Spyware 介面



Anti-Spyware 元件的介面提供元件功能的簡短概觀、有關該元件目前狀態的資訊，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
- **資料庫發行** - 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遞增

此元件的介面內只有一個可操作的按鈕（[上一步](#)） - 按一下此按鈕可返回至預設的 [AVG 使用者介面](#)（[元件概觀](#)）。



7.3. Link Scanner

7.3.1. Link Scanner 原理

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

LinkScanner 技術包括兩項功能，即 [Search-Shield](#) 和 [Surf-Shield](#)：

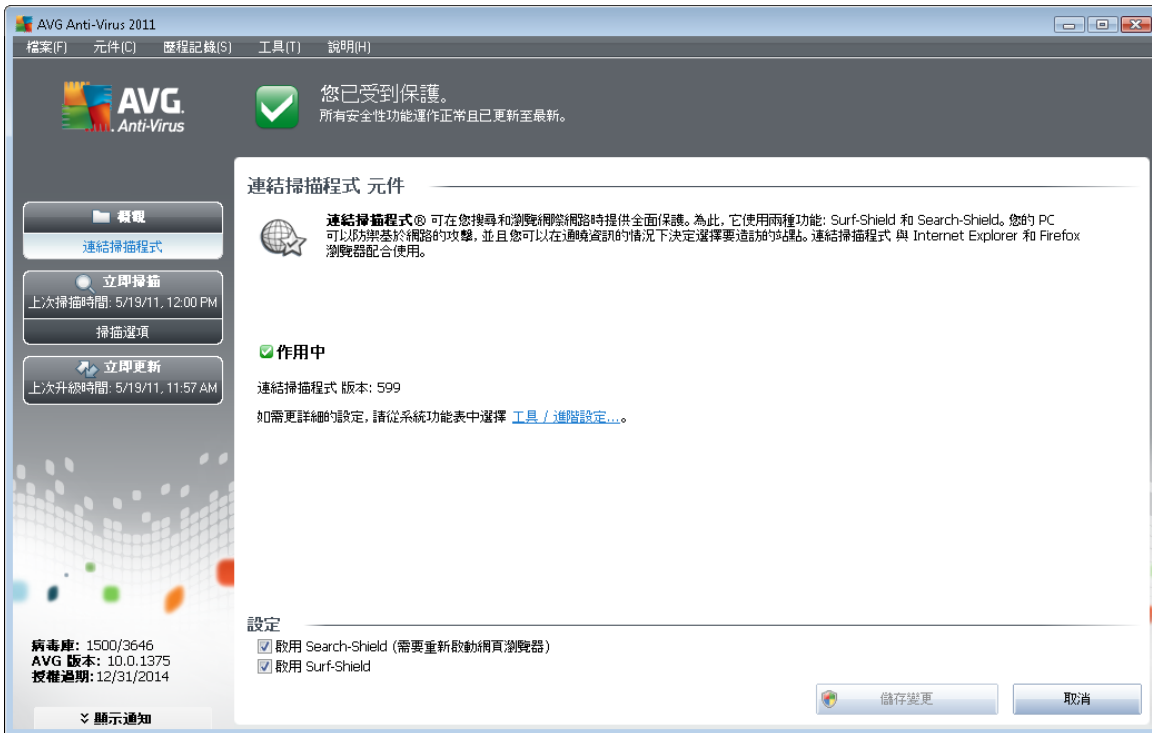
- [Search-Shield](#) 包含已知危險的網站清單 (URL 位址)。使用 Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 進行搜尋時，搜尋的所有結果都會根據此清單進行檢查，並顯示一個裁決圖示 (對於 Yahoo! 搜尋結果，僅顯示「惡意探索網站」裁決圖示)。
- [Surf-Shield](#) 會掃描您正在瀏覽之網站的內容，無論網站位址為何。即使 [Search-Shield](#) 未偵測出某個網站 (例如，當一個新的惡意網站建立，或當之前安全的網站現在包含了某個惡意軟體時) 當您嘗試訪問該網站時，[Surf-Shield](#) 也會偵測到並阻止它。

注意： *LinkScanner* 不適用於伺服器平台！



7.3.2. Link Scanner 介面

[LinkScanner](#) 元件介面提供了元件功能的簡短描述，以及有關其目前狀態的資訊。您還會看到有關最新的 [LinkScanner](#) 資料庫版本號碼 (*LinkScanner 版本*) 的資訊。



LinkScanner 設定

在對話方塊底端，您可以編輯數個選項：






- 啟用 [Search-Shield](#) - (預設情況下為開啟)：在透過 Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 執行的搜尋上提供忠告圖示：事先檢查搜尋引擎傳回的網站內容。
- 啟用 [Surf-Shield](#) - (預設情況下為開啟)：在存取惡意探索站點時，提供主動 (即時) 保護。當使用者透過網頁瀏覽器 (或任何其他使用 HTTP 的應用程式) 存取已知惡意站點時，其連線及其惡意探索內容都將被阻止。

7.3.3. Search-Shield

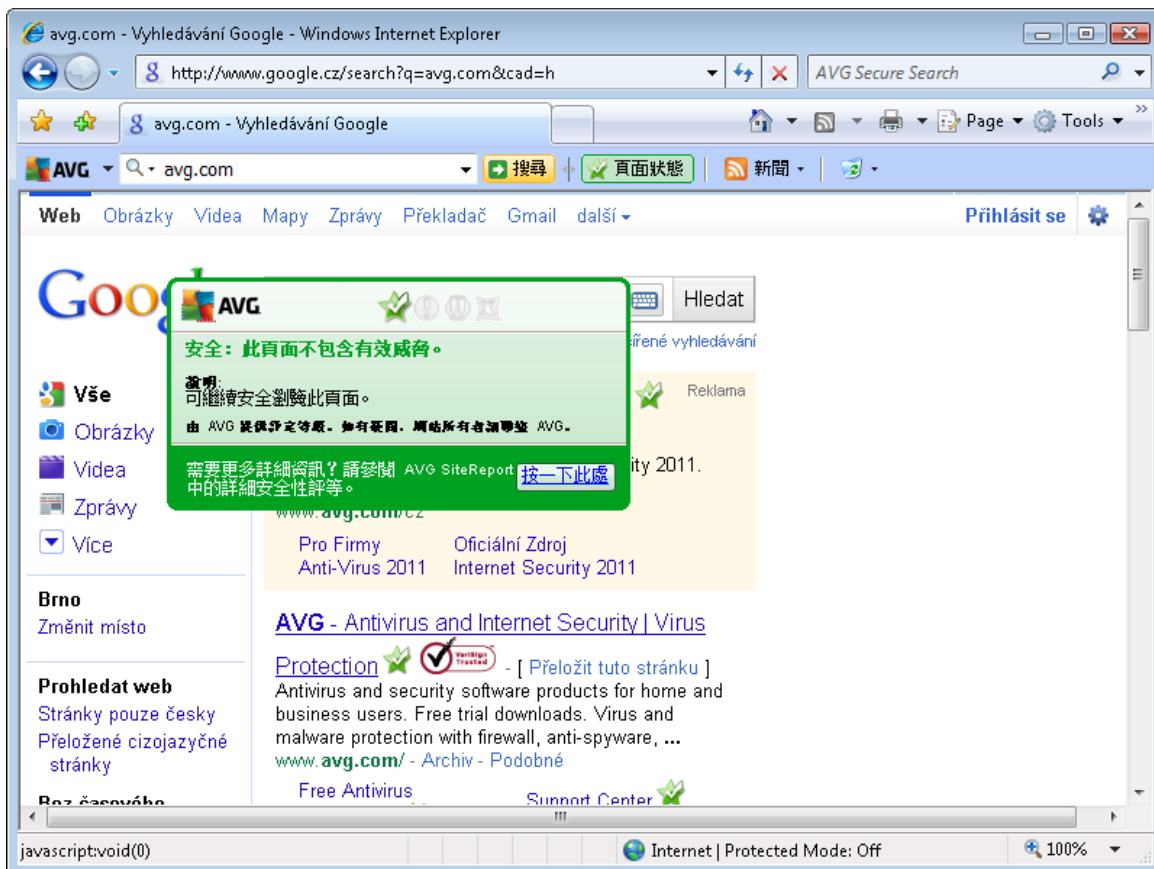
在 [Search-Shield](#) 開啟狀態下搜尋網際網路時，從最常用的搜尋引擎 (Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 和 SlashDot) 傳回的全部結果都會評估是否有危險或可疑的連結。透過檢查這些連結並標示惡意連結，[AVG Link Scanner](#) 會在您按下危險或可疑連結之前先提出警告，藉此確保您只會進入安全的網站。



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：

-  連結的網頁是安全的 (不會顯示該圖示以表示 Yahoo! JP 搜尋結果)。
-  連結的頁面不包含威脅，但有可疑之處 (來源或動機有問題，因此不建議進行線上購物等等)。
-  連結的頁面可能本身是安全的，但是包含其他確定危險的頁面的連結；或是程式碼方面很可疑，但目前不會造成直接的威脅。
-  連結的頁面包含有效威脅！為確保您自身的安全，您不能訪問該頁面。
-  連結的頁面無法存取，因此無法掃描。

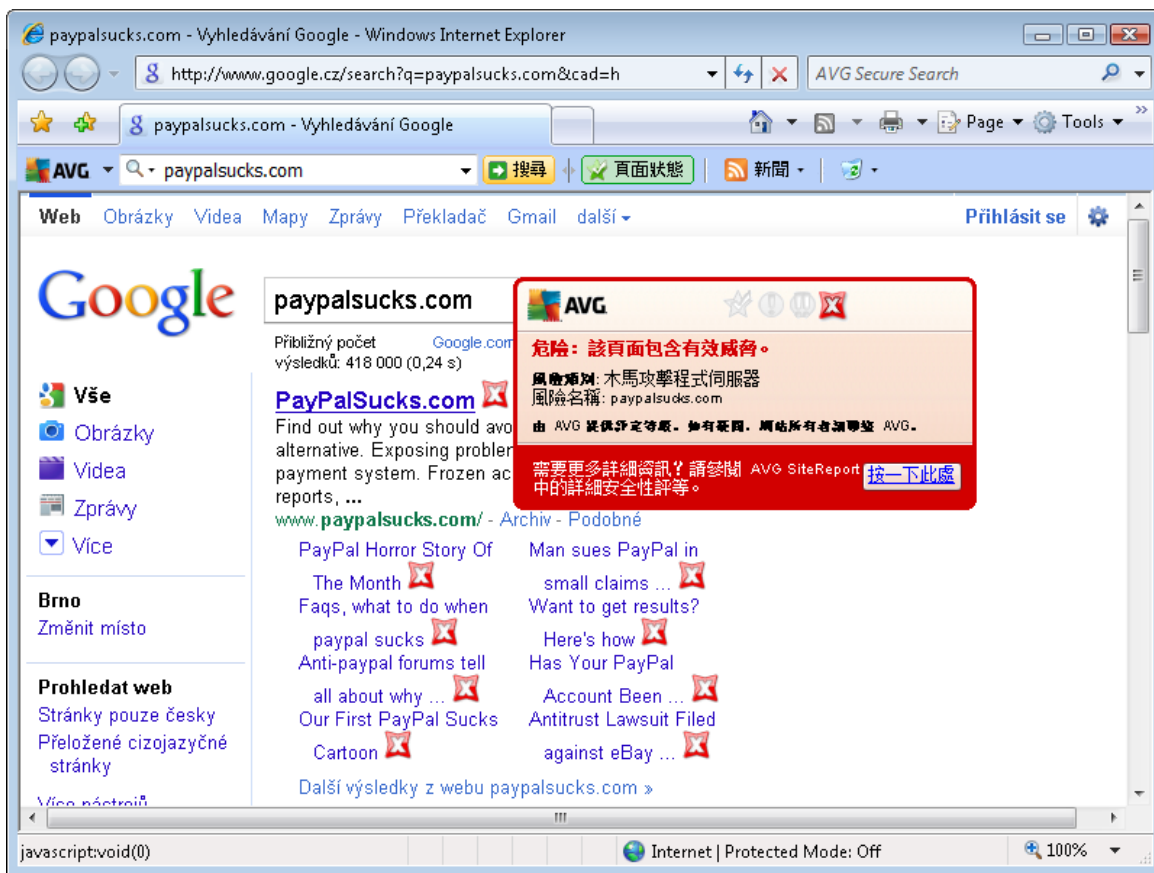
把滑鼠指標停留在單個的等級圖示上即可顯示有關特定連結的詳細資訊。資訊包括該威脅 (如果有的話) 的其他詳細資料：



7.3.4. 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！

7.4. Resident Shield

7.4.1. Resident Shield 原理

Resident Shield 元件可為您的電腦提供持續保護。它會掃描已開啟、儲存或複製的每個檔案，並保護電腦上的各個系統區域。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。

Resident Shield 可以做些什麼：

- 掃描特定類型的可能威脅
- 掃描卸除式媒體（快閃磁碟等）
- 掃描具有特定副檔名或沒有副檔名的檔案
- 允許掃描例外 - 從來不應掃描的特定檔案或資料夾

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。

7.4.2. Resident Shield 介面



除了 **Resident Shield** 功能的概觀、有關該元件目前狀態的資訊之外，**Resident Shield** 介面還會提供一些統計資料：

- **Resident Shield 已執行的時間** - 提供自最近一次啟動元件以來所耗的時間
- **已偵測到和阻止的威脅數** - 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)

Resident Shield 設定



在對話方塊視窗的底端，您將找到名為 **Resident Shield 設定** 的區段，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 使用中 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)
- 或僅在使用者核准後移除 (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，您仍可選擇是否要掃描追蹤 **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：軟體廠商已對所有 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經驗豐富的使用者來執行。如需變更 AVG 組態，請選取系統功能表項目工具/進階設定，然後在新開啟的 [AVG 進階設定](#) 對話方塊中編輯 AVG 組態。

控制按鈕

以下是 **Resident Shield** 介面中提供的控制按鈕：

- **管理例外** - 開啟 [Resident Shield - 排除項目](#) 對話方塊，您可在此處中定義應從 [Resident Shield](#) 掃描排除的資料夾和檔案
- **儲存變更** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- **取消** - 按一下此按鈕可返回預設的 [AVG 使用者介面](#) (元件概觀)



7.4.3. 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：



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

接下來，您必須決定現在應該採取什麼動作 - 有以下選項可用：

注意，根據特定條件 (受感染檔案的類型及其位置)，並非所有選項都可以使用！

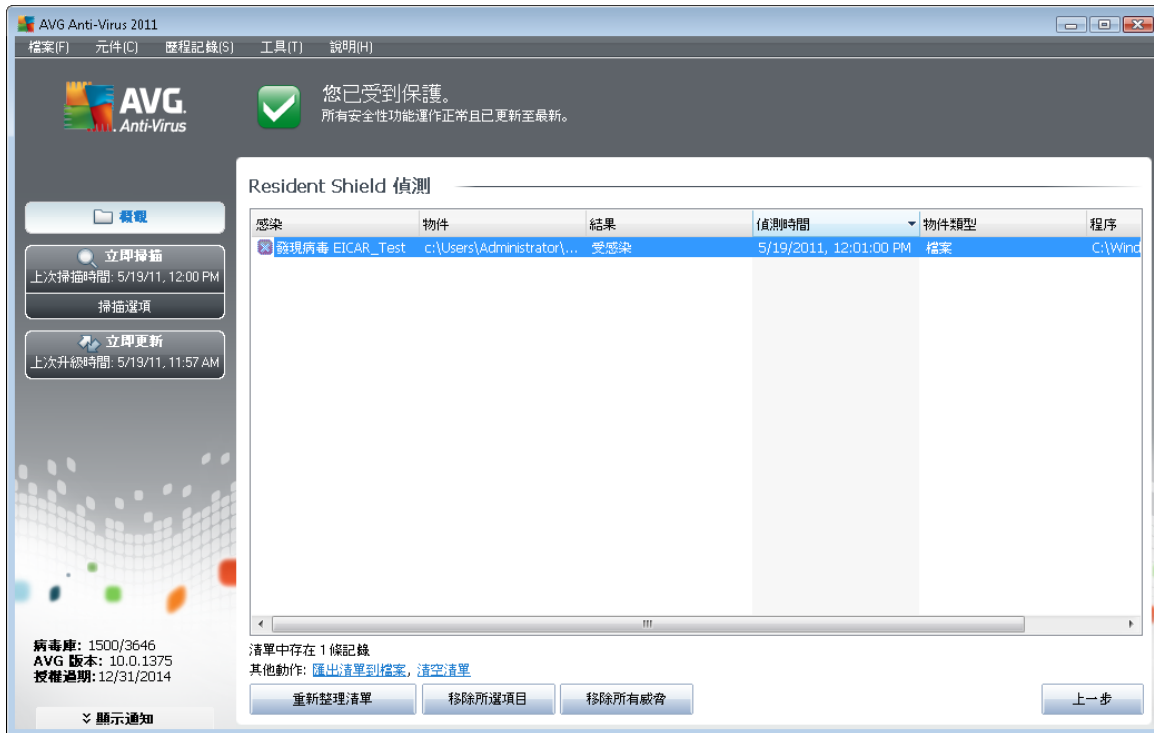
- **以進階使用者身分移除威脅** - 如果您認為作為普通使用者，您移除該威脅的權限不足，請核取該方塊。進階使用者具有更多存取權限，並且如果威脅位於特定的系統資料夾中，您可能就需要使用該核取方塊以將其成功移除。
- **修復** - 此按鈕只有在偵測到的感染可以修復時才會出現。它隨後會將它從檔案中移除，並將檔案還原為原始狀態。如果檔案本身是病毒，請使用此功能來刪除它 (亦即移至 [病毒隔離區](#))
- **移至隔離區** - 病毒將移至 AVG [病毒隔離區](#)
- **移至檔案** - 此選項會將您重新導向至可疑物件的確切位置 (開啟新的 Windows 檔案總管視窗)
- **忽略** - 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！

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



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

您可以在 [Resident Shield 偵測](#) 對話方塊中找到 [Resident Shield 偵測](#) 的所有威脅的整體概觀，此對話方塊可從系統功能表選項 [歷程記錄/Resident Shield 偵測](#) 存取：



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

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

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



7.5. Family Safety

AVG Family Safety 幫助您保護孩子不受不當的網站、媒體內容和線上搜索結果所侵害，並為您提供有關孩子網路活動的報告。您可以為每個孩子設定相應的保護級別，透過唯一的登入資訊對每個孩子進行單獨監視。

該元件僅在您的機器上安裝了 **AVG Family Safety** 產品時才可用。如果您沒有安裝 **AVG Family Safety** 產品，則按一下 **AVG Anti-Virus 2011** 使用者介面中的相應圖示，這會將您重新導向到您在其中可疑找到所有必要詳細資料的產品網站。

7.6. AVG LiveKive

AVG LiveKive 會自動將您的所有檔案、相片和音樂備份到一個安全地方，讓您與家人和朋友分享，並能從任何可使用網路的裝置 (如 iPhone 和 Android 裝置) 存取它們。

該元件僅在您的機器上安裝了 **AVG LiveKive** 產品時才可啟動。如果您沒有安裝 **AVG LiveKive** 產品，則按一下 **AVG Anti-Virus 2011** 使用者介面中的相應圖示，會將您重新導向到可讓您尋找所有必要詳細資料的產品網站。

7.7. 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。

7.7.1. E-mail Scanner 原理

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

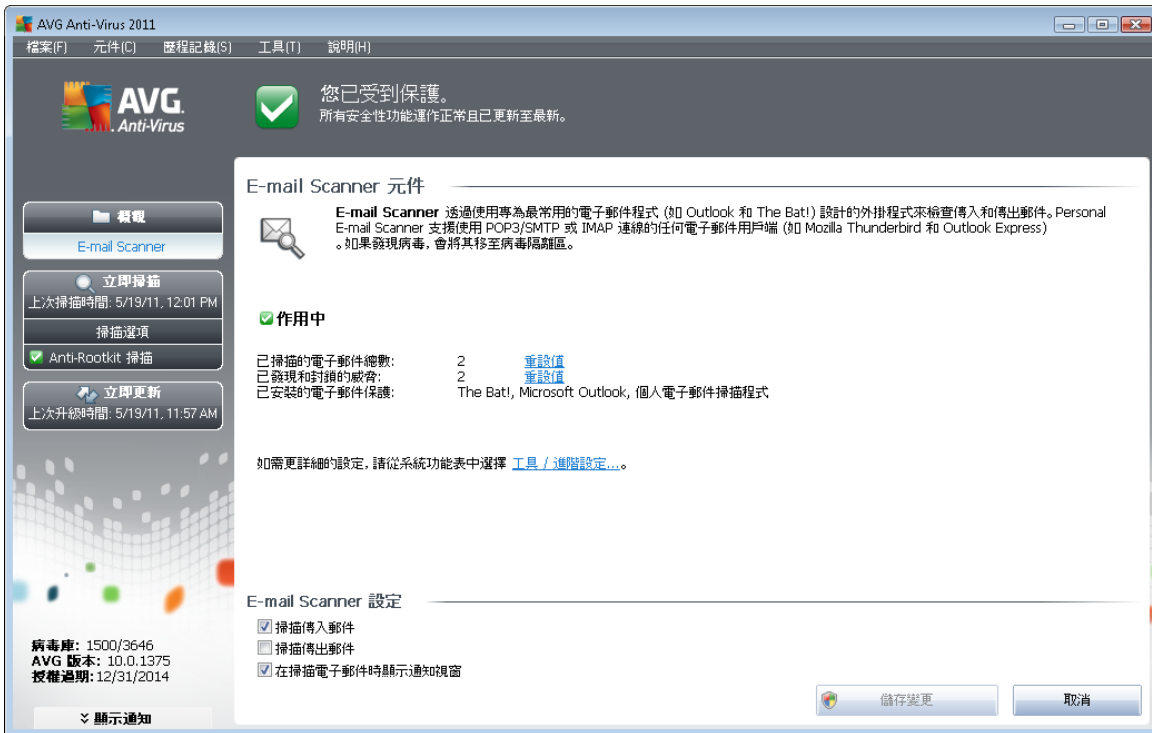
在 AVG [安裝期間](#)，AVG 會針對電子郵件控制項建立自動伺服器：一部用於檢查傳入電子郵件，另一部用於檢查傳出電子郵件。系統會使用這兩部伺服器自動在連接埠 110 和 25 (收發電子郵件的標準連接埠) 上檢查電子郵件。

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

- **傳入郵件**：從伺服器接收郵件時，**E-mail Scanner** 元件會對郵件進行測試以檢查是否有病毒，移除受感染的附件，然後加入認證。一旦偵測到病毒，就會立即將其隔離到 [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！

7.7.2. E-mail Scanner 介面



您可以在 **E-mail Scanner** 元件的對話方塊中找到描述元件功能的簡要文字、有關該元件目前狀態的資訊，以及以下統計資料：

- **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，以便統計 - 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

E-mail Scanner 設定

在對話方塊底端可以找到名為 **E-mail Scanner 設定** 的區段，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視窗** - 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：軟體廠商已對所有 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經驗豐富的使用者來執行。如需變更 AVG 組態，請選取系統功能表項目 **工具 / 進階設定**，然後在新開啟的 [AVG 進階設定](#) 對話方塊中編輯 AVG 組態。

控制按鈕

E-mail Scanner 介面中可用的控制按鈕如下：

- **儲存變更** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- **取消** - 按一下此按鈕可返回預設的 [AVG 使用者介面](#) (元件概觀)

7.7.3. E-mail Scanner 偵測

感染	物件	結果	偵測時間	物件類型
發現病毒 EICAR_Test	eicar_com.zip	已移至病毒隔離區	5/19/2011, 11:59:45 AM	檔案
發現病毒 EICAR_Test	eicar_com.zip	已移至病毒隔離區	5/19/2011, 11:59:43 AM	檔案

您可以在 **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) 看到 [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** (Object) - 偵測到的物件的說明 (甚至可能包含名稱)



- **物件** - 物件位置
- **結果** - 對偵測到的物件執行的動作
- **偵測時間** - 偵測到可疑物件的日期和時間
- **物件類型** - 偵測到的物件的類型

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

控制按鈕

E-mail Scanner 偵測 介面內可用的控制按鈕如下：

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

7.8. 更新管理員

7.8.1. 「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，軟體廠商們不斷發行更新和安全性補充程式，以修復發現的所有安全性漏洞。

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！

7.8.2. 「更新管理員」介面



更新管理員的介面顯示有關該元件功能及其狀態的資訊，並提供相關的統計資料：

- **最新更新** - 指定最後一次資料庫更新的日期和時間
- **病毒庫版本** - 定義最新安裝的病毒庫版本的編號；此編號將隨著病毒庫的每次更新而增加
- **排程的下次更新** - 指定資料庫下次更新的日期和時間

「更新管理員」設定

在此對話方塊的底端，您可以找到「更新管理員」設定區段，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
- **在特定時間間隔** - 定義應該啟動更新的確切時間

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！



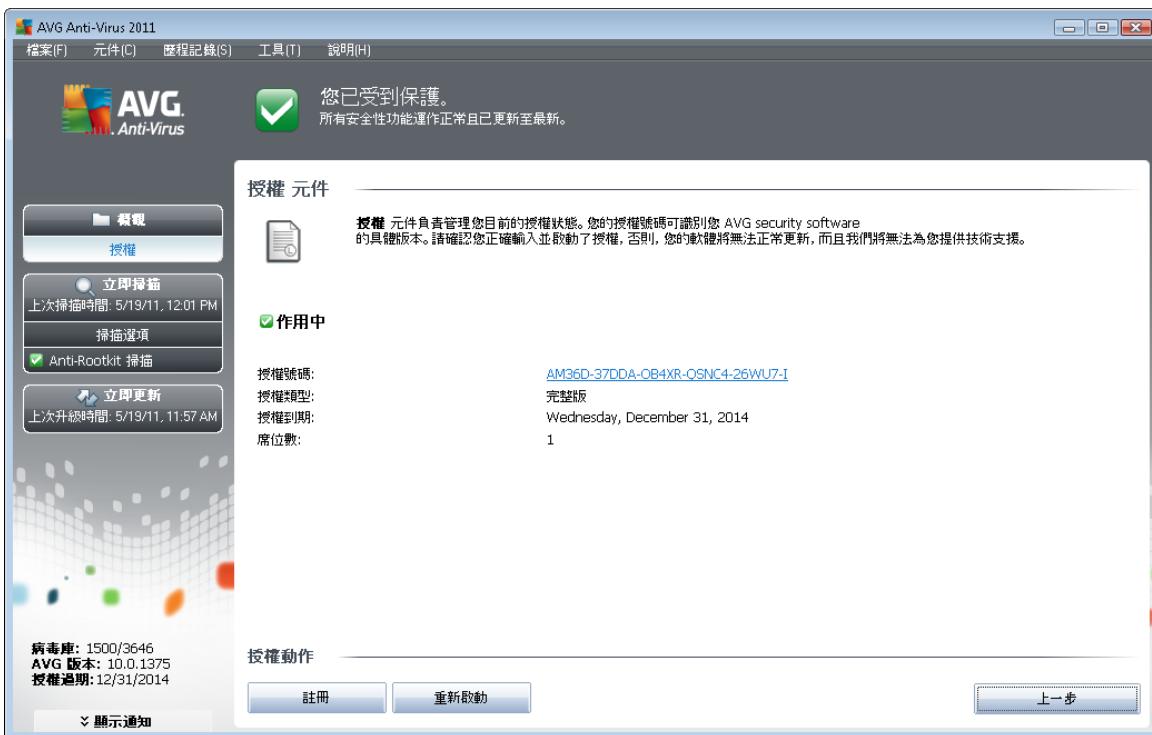
請注意：軟體廠商已對所有 AVG 元件進行設定，以提供最佳效能。除非您確實需要這麼做，否則不要變更 AVG 組態。任何設定變更都只能由經驗豐富的使用者來執行。如需變更 AVG 組態，請選取系統功能表項目工具/進階設定，然後在新開啟的 [AVG 進階設定對話方塊](#) 中編輯 AVG 組態。

控制按鈕

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** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- **取消** - 按一下此按鈕可返回預設的 [AVG 使用者介面](#) (元件概觀)

7.9. 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、有關其目前狀態的資訊，以及以下資訊：

- **授權號碼** - 提供簡短形式的授權號碼 (為了安全起見，將不顯示最後四個符號)。輸入授權號碼時，您需要根據顯示的號碼完全準確鍵入。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 Anti-Virus 2011**，則必須更新您的授權。您可以在 [AVG 網站](#) 上進行線上授權更新。

- **席位數** - 您有權在上面安裝 **AVG Anti-Virus 2011** 的工作站數目。

控制按鈕

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

注意：如果您使用的是 **AVG Anti-Virus 2011 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 Anti-Virus 2011** 時輸入了銷售號碼，這些按鈕會顯示為 **註冊及啟動**。

- **上一步** - 按一下此按鈕可返回到預設 [AVG 使用者介面](#) (元件概觀)。

7.10. Remote Administration



Remote Administration 元件只會在您已安裝產品的 Business Edition 時才會顯示在 `<% main_product_ame_in_text%>` 的使用者介面中 (請參閱元件 [License](#))。您可以在 **Remote Administration** 對話方塊中找到有關元件是否為使用中狀態以及是否連線至伺服器的資訊



。**Remote Administration** 元件的所有設定都是在 **進階設定/Remote Administration** 中完成。

如需在 AVG Remote Administration 系統內取得該元件的選項和功能的詳細描述，請參閱專門針對此主題提供的特定文件。此文件可在 [AVG 網站 \(www.avg.com\)](http://www.avg.com) 的 **支援中心/下載/文件** 頁面下載取得。

控制按鈕

- **上一步** - 按一下此按鈕可返回到預設 [AVG 使用者介面](#) (元件概觀)。

7.11. Online Shield

7.11.1. Online Shield 原理

Online Shield 是一種即時常駐保護；它甚至可在要訪問的網頁的內容（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掃描這些內容。

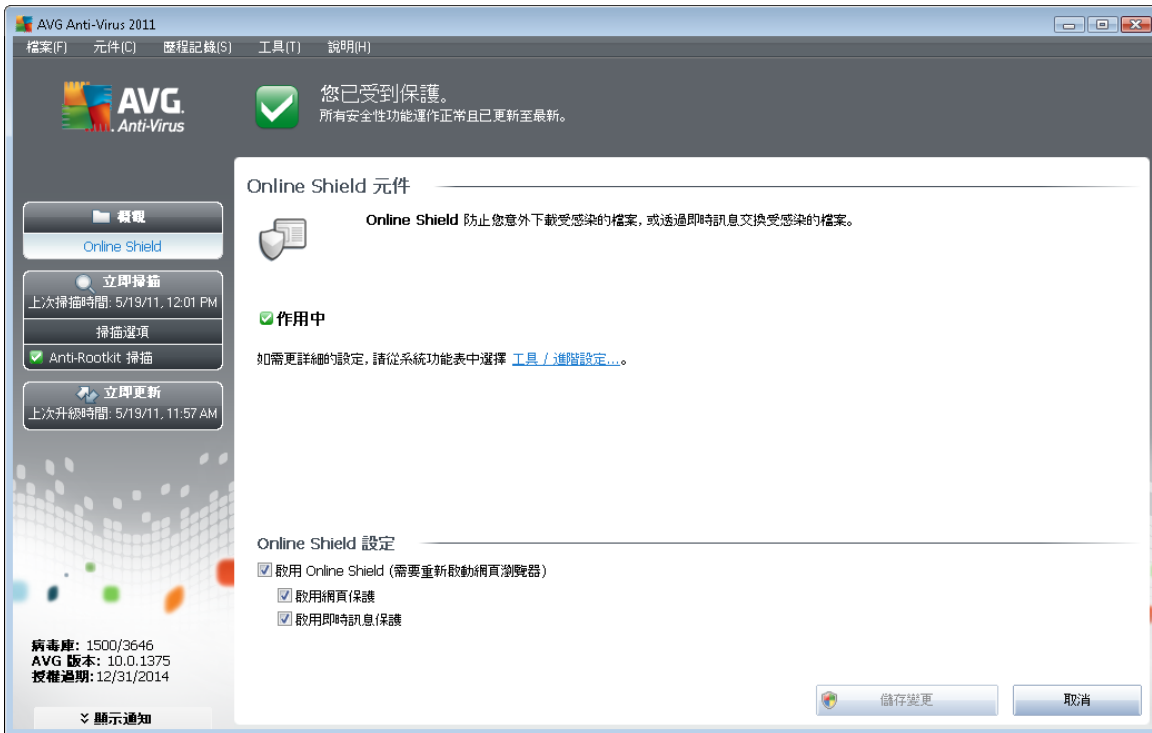
Online Shield 會偵測到您即將訪問的網頁包含一些危險的 javascript，並會阻止該網頁的顯示。此外，它還可以識別網頁中包含的惡意軟體，並立即阻止這些惡意軟體的下載，使其永遠不會侵入您的電腦。

注意： AVG Online Shield 不適用於伺服器平台！



7.11.2. Online Shield 介面

Online Shield 元件的介面描述了此類保護的行為。您還可以找到有關該元件目前狀態的資訊。您之後可以在此對話方塊的底端找到該元件功能的基本編輯選項：



Online Shield 設定

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，我們建議您將該元件狀態保持為使用中。如果核取該項目，並且 **Online Shield** 正在執行中，則會另外啟動兩個組態選項：

- **啟用網頁保護** - 此選項確認 **Online Shield** 應該執行網站內容掃描。
- **啟用即時訊息保護** - 如果您希望 **Online Shield** 確認即時訊息通訊 (亦即 ICQ、MSN Messenger...) 沒有病毒感染，請核取此項目。

請注意：軟體廠商已對所有 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經驗豐富的使用者來執行。如需變更 AVG 組態，請選取系統功能表項目 **工具/進階設定**，然後在新開啟的 **AVG 進階設定** 對話方塊中編輯 AVG 組態。

控制按鈕

以下是 **Online Shield** 介面中提供的控制按鈕：



- **儲存變更** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- **取消** - 按一下此按鈕可返回預設的 [AVG 使用者介面](#) (元件概觀)

7.11.3. Online Shield 偵測

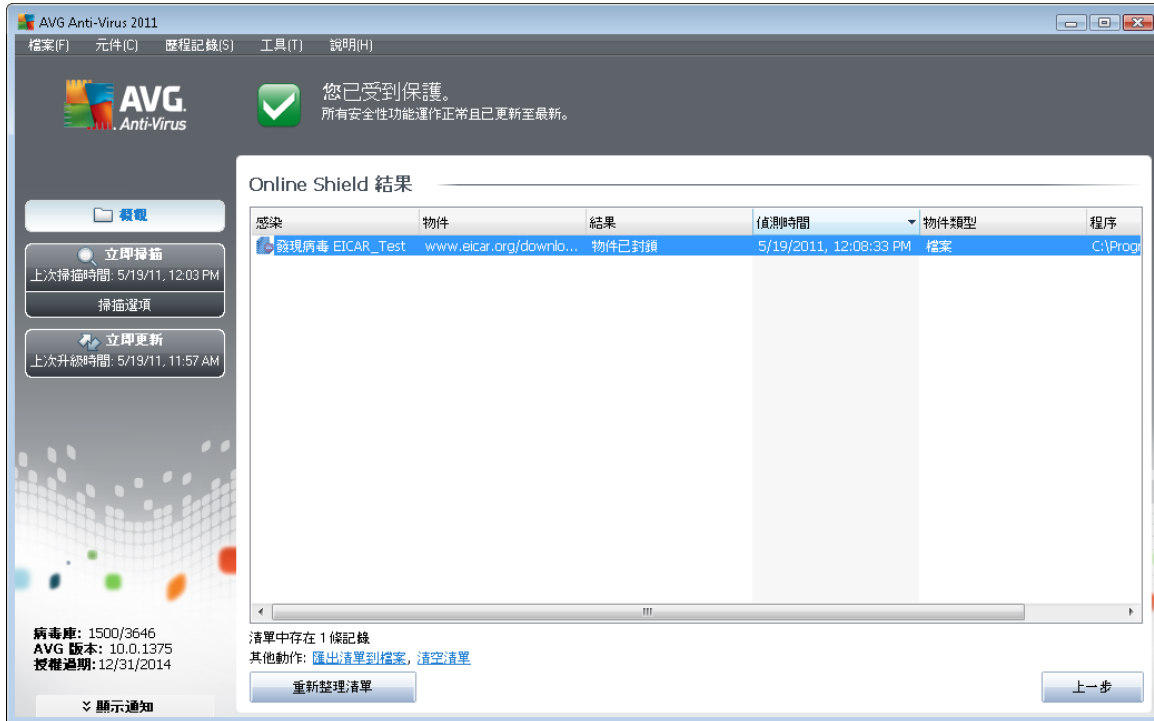
Online Shield 甚至會在瀏覽網頁的內容及這些網頁中可能包含的檔案顯示於您的網頁瀏覽器中或下載到您的電腦之前即進行掃描。如果偵測到威脅，系統將立即顯示下列對話方塊向您發出警告：



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

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

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



針對每個偵測到的物件，提供以下資訊：

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

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

7.12. 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。

7.12.1. Anti-Rootkit 原理

AVG Anti-Rootkit 是一種專門偵測並有效移除危險 rootkit 的工具，rootkit 是指可以在您的電腦上掩飾惡意軟體存在的程式和技術。**AVG Anti-Rootkit** 能夠根據預定義的一組規則偵測 rootkit。請注意，它會偵測所有 rootkit (而不只是受感染的 rootkit)。如果 **AVG Anti-Rootkit** 發現 rootkit，不一定表示該 rootkit 已受感染。rootkit 有時候會被用作驅動程式，或屬於正確應用程式的一部分。

7.12.2. Anti-Rootkit 介面



Anti-Rootkit 使用者介面會提供元件功能的簡短描述，告知該元件的目前狀態，還會顯示上次啟動 **Anti-Rootkit** 測試的資訊 (最後一次 rootkit 搜尋)。 **Anti-Rootkit** 對話方塊會進一步提供 [工具 / 進階設定](#) 連結。使用該連結可重新導向至 **Anti-Rootkit** 元件的進階組態環境。

請注意：軟體廠商已對所有 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經驗豐富的使用者來執行。

Anti-Rootkit 設定

在對話方塊底端可以找到 **Anti-Rootkit 設定** 區段，您可以在此設定一些 rootkit 現行掃描的基本功能。首先，勾選相應的核取方塊來指定要掃描的物件：

- 掃描應用程式
- 掃描 DLL 程式庫



- **掃描驅動程式**

此外，您還可以挑選 rootkit 掃描模式：

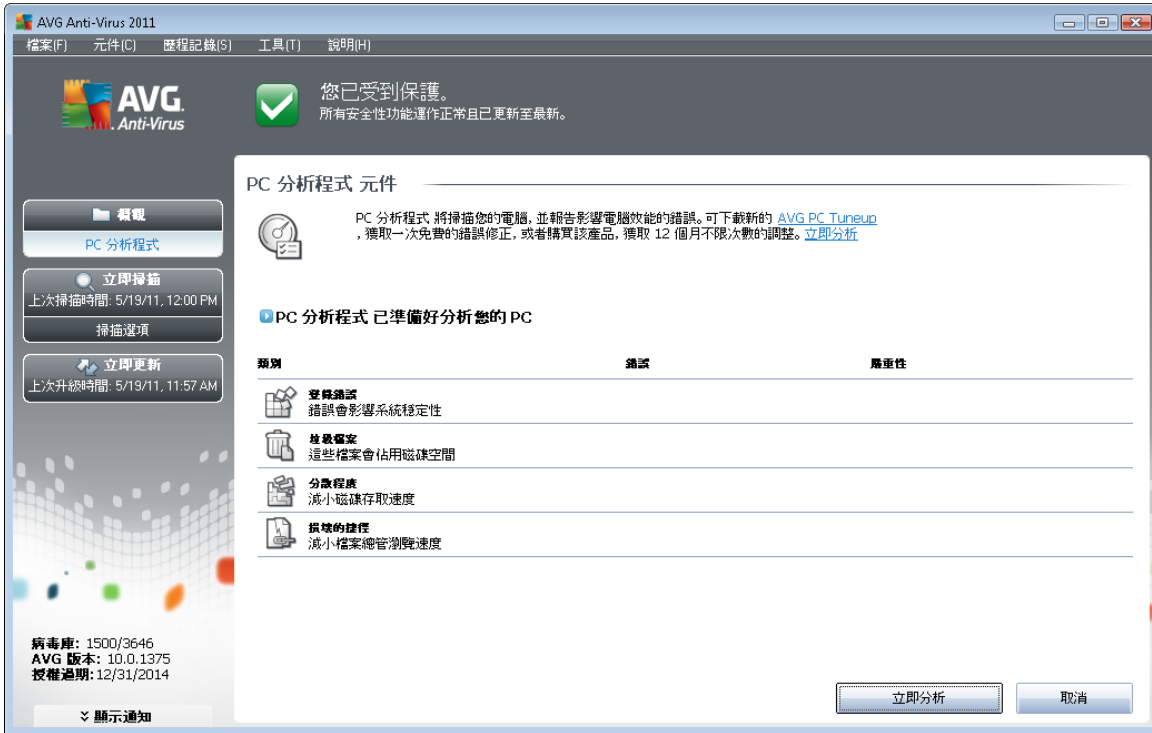
- **快速 rootkit 掃描** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾（通常是 c:\Windows）
- **完整 rootkit 掃描** - 掃描所有執行中的程序、已載入的驅動程式，以及系統資料夾（通常是 c:\Windows），加上所有本機磁碟（包括快閃磁碟機，但不包括磁碟片 / CD 光碟機）

控制按鈕

- **搜尋 rootkit** - 由於 rootkit 掃描不是 [掃描整台電腦](#) 的固有功能，您可以使用此按鈕從 **Anti-Rootkit** 介面直接執行 rootkit 掃描
- **儲存變更** - 按一下此按鈕可儲存在此介面中做出的所有變更，並返回到預設的 [AVG 使用者介面](#)（元件概觀）
- **取消** - 按一下此按鈕可返回到預設的 [AVG 使用者介面](#)（元件概觀），而且不儲存您所做的任何變更

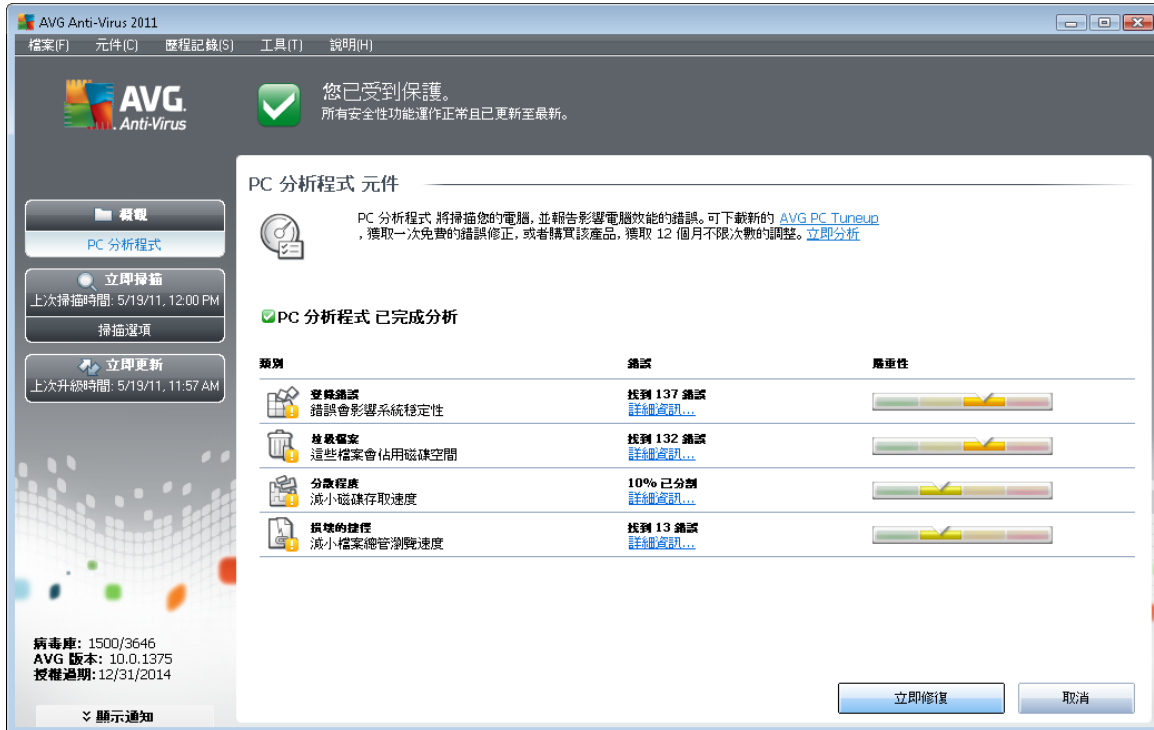
7.13. PC 分析程式

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



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

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



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

控制按鈕

- **立即分析** (在分析開始之前顯示) - 按一下此按鈕可立即開始分析您的電腦
- **立即修復** (完成分析時會立即顯示) - 按一下此按鈕可前往 AVG 網站 (<http://www.avg.com/>) 中提供與 **PC 分析程式** 元件相關的最新詳細資訊的頁面
- **取消** 按一下此按鈕可停止執行中的分析，或在完成分析後立即返回到預設的 [AVG 使用者介面](#) (元件概觀)

7.14. ID Protection

AVG Identity Protection 是一款反惡意軟體產品，著重預防身份盜用者以您的電腦作為目標，透過各種惡意軟體竊取您的密碼、銀行帳戶詳細資訊、信用卡號碼以及您其他重要的個人數位財產。它可以確保您電腦上的所有程式都正常運作。**AVG Identity Protection** 會持續性地找出並封鎖可疑行為，保護您的電腦免遭所有新興惡意軟體的攻擊。

7.14.1. ID Protection 原理

AVG Identity Protection 是一個反惡意軟體元件，它使用行為技術來保護您的電腦免遭各種惡意軟體 (間諜軟體、傀儡程式、身份盜賊等) 的攻擊，並提供針對新病毒的零時差防護 (Zero Day Protection)。隨著惡意軟體變得日益複雜，並且以正常程式的形式出現，使得遠端攻擊者能夠在我們的電腦伺機盜取身份，而 **AVG Identity Protection** 可以保護您的電



腦免遭這些新型惡意軟體的攻擊。它在 [AVG Anti-Virus](#) 的基礎上多補充了一層保障，利用簽名機制和掃描來協助您防禦基於檔案的病毒和已知病毒的攻擊。

我們強烈建議您安裝 [AVG Anti-Virus](#) 和 [AVG Identity Protection](#) 兩種元件，以讓您的電腦獲得完整的保護。

7.14.2. ID Protection 介面



Identity Protection 元件介面提供元件基本功能、其狀態，以及一些統計資料的簡短描述：

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

Identity Protection 設定

在對話方塊底端的 **Identity Protection 設定** 區段，您可以編輯該元件功能的一些基本功能：

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

在某些情況下，**Identity Protection** 可能會報告某個合法檔案很可疑或有危險。由於



Identity Protection 是根據威脅本身的行為來偵測威脅，這通常是發生在當有程式試圖監視按鍵動作、安裝其他程式或在電腦上安裝新驅動程式時。因此請選取下列其中一個選項，指定 **Identity Protection** 元件在偵測到可疑活動時的行為：

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

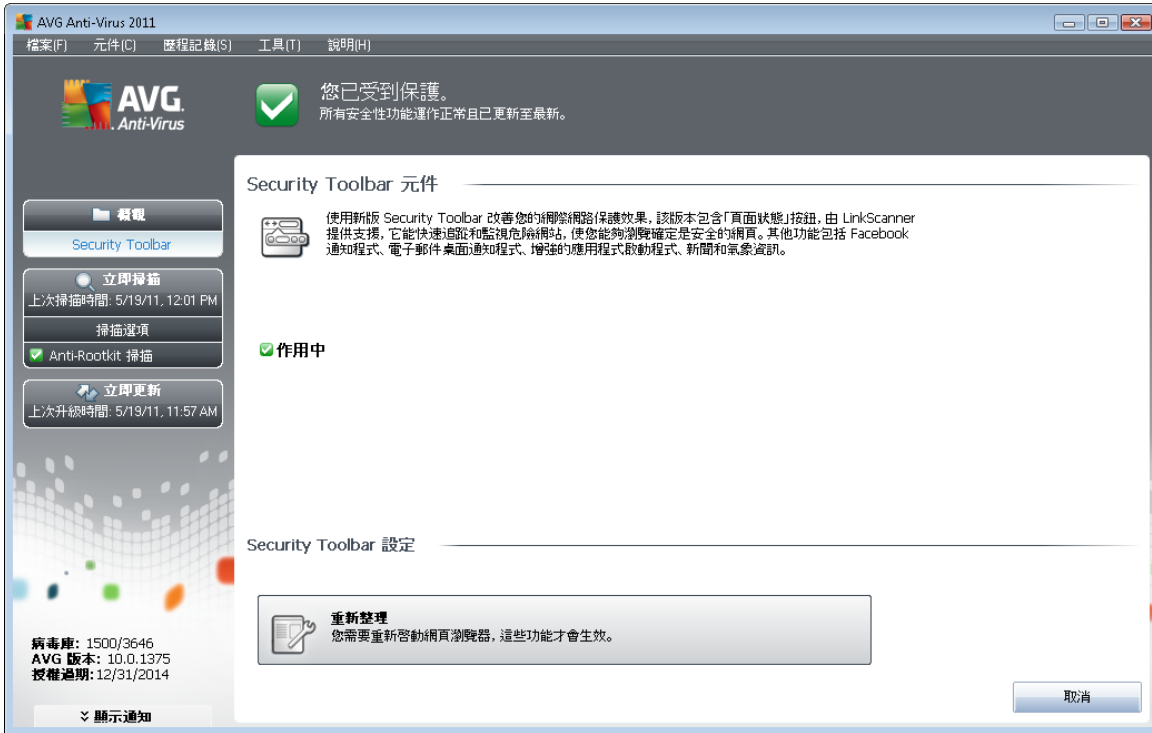
控制按鈕

Identity Protection 介面內可用的控制按鈕如下：

- **儲存變更** - 按一下此按鈕可儲存並套用在此對話方塊中所做的任何變更
- **取消** - 按一下此按鈕可返回預設的 [AVG 使用者介面](#) (元件概觀)

7.15. Security Toolbar

Security Toolbar 是可選的網頁瀏覽器工具列，可在瀏覽網頁時隨時提供增強的 AVG 保護，以及各種功能和工具。目前，**Security Toolbar** 受 Internet Explorer (6.0 或更高版本) 和 Mozilla Firefox (3.0 或更高版本) 網頁瀏覽器所支援：



Security Toolbar 元件的所有設定皆可直接在您網頁瀏覽器內的 [Security Toolbar](#) 中存取。



8. AVG Security Toolbar

AVG Security Toolbar 是一款可與 [LinkScanner](#) 元件搭配運作的新工具。**AVG Security Toolbar** 可用來控制 [LinkScanner](#) 的功能並調整其行為。

如果您選擇在安裝 **AVG Anti-Virus 2011** 期間安裝該工具列，它會自動新增至您的網頁瀏覽器（*Internet Explorer 6.0* 或更高版本、*Mozilla Firefox 3.0* 或更高版本）。目前不支援其他網際網路瀏覽器。

注意：如果您使用的是某種替代網際網路瀏覽器（例如 *Avant Browser*），可能會遇到無法預期的行為。

8.1. AVG Security Toolbar 介面

AVG Security Toolbar 是專門為了與 *MS Internet Explorer*（6.0 版或更高版本）和 *Mozilla Firefox*（3.0 版或更高版本）搭配使用而設計。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：



AVG Security Toolbar 由以下部分構成：

8.1.1. AVG 標誌按鈕

此按鈕提供對一般工具列項目的存取。按一下標誌按鈕即可重新導向至 [AVG 網站](#)。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** - 開啟 **AVG Anti-Virus 2011** [使用者介面](#)
- **AVG 資訊** - 開啟內容功能表，內含以下連結，可連至與以下項目 **AVG Anti-Virus 2011** 相關的重要安全性資訊：
 - **關於威脅** - 開啟 [AVG 網站](#)，顯示有關主要威脅、病毒移除建議、AVG 更新資訊、存取 [病毒庫](#) 和其他相關資訊
 - **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。
 - **AVG 威脅實驗室** - 開啟 [AVG 網站報告](#) 網站，您可以在此處依名稱搜尋特定威脅，並取得個別的詳細資訊

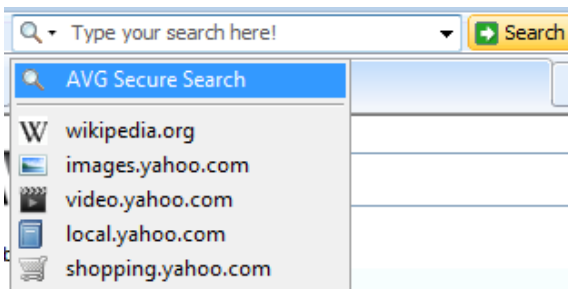


- **選項** - 將開啟一個組態對話方塊，您可以在此處調整 **AVG Security Toolbar** 設定以配合您的需要 - 請參閱以下 [AVG Security Toolbar 選項](#)
- **刪除歷程記錄** - 可讓您在 **AVG Security Toolbar** 內刪除全部歷程記錄，或刪除個別的歷程記錄、刪除下載歷程記錄，以及刪除 cookie。
- **更新** - 檢查 **AVG Security Toolbar** 的新更新
- **說明** - 提供選項以開啟說明檔案、聯絡 [AVG 技術支援](#)、傳送產品相關意見，或檢視工具列目前版本的詳細資訊

8.1.2. AVG Secure Search (powered by Google) 支援的搜尋方塊

AVG Secure Search (powered by Google) 方塊可供您使用 AVG Secure Search (powered by Google) 來搜尋網頁，方便而安全。將一個字或短語輸入搜尋方塊，然後按 **搜尋** 按鈕，或者按 **Enter** 鍵，直接啟動 AVG Secure Search (powered by Google) 伺服器上的搜索功能，不管目前顯示哪個頁面。搜尋方塊還會列出您的搜尋歷程記錄。透過搜尋方塊完成的搜尋會使用 [Search-Shield](#) 保護功能進行分析。

或者，您可以選擇在搜尋欄位中切換到 Wikipedia，或其他一些特定的搜尋服務 - 見圖：



8.1.3. 頁面狀態

此按鈕會顯示目前根據 [Surf-Shield](#) 元件的條件顯示的網頁評估：

- - 連結的頁面是安全的
- - 頁面有些可疑。
- - 頁面包含已確定是危險的頁面之連結。
- - 連結的頁面包含有效威脅！為確保您自身的安全，您不能訪問該頁面。
- - 連結的頁面無法存取，因此無法掃描。

按一下此按鈕可開啟資訊欄，顯示有關該網頁的詳細資訊。




8.1.4. AVG 新聞

此按鈕會直接從 **AVG Security Toolbar** 內開啟媒體和公司新聞稿發佈與 AVG 相關的最新 **頭條新聞的概觀**：




您可以在右上角看到兩個紅色的控制按鈕：

-  - 該按鈕會開啟編輯對話方塊，您可以在此處指定 **AVG 新聞** 按鈕要在 **AVG Security Toolbar** 內顯示的參數：



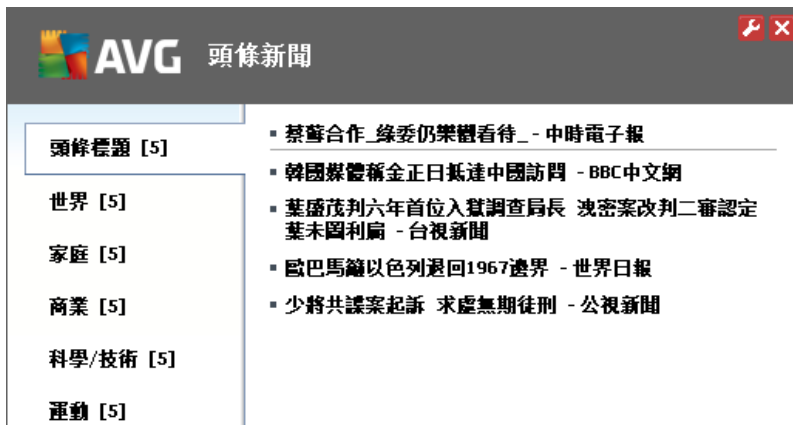
- **顯示訊息** - 變更一次要顯示的訊息數量




- **RSS 設計** - 在目前顯示的新聞概觀的進階 / 基本模式間選擇 (預設是選取進階模式 - 見上圖)
- **隱藏已讀取訊息** - 標示此項目以確認不要再顯示每封已讀取的訊息，以便提供新訊息
-  - 按一下此按鈕以關閉目前開啟的新聞概觀

8.1.5. 新聞


同樣地，此選項會直接從 **AVG Security Toolbar** 內開啟所選媒體的最新新聞，該部分分為若干區段：



您可以在右上角看到兩個紅色的控制按鈕：

-  - 該按鈕會開啟編輯對話方塊，您可在此處指定 **新聞** 按鈕要在 **AVG Security Toolbar** 內顯示的參數：



- **按鈕名稱** - 您可以選擇是否要變更顯示在 **AVG Security Toolbar**
- **新聞版本** - 從清單中選擇國家以顯示所選地區的新聞
- **顯示訊息** - 指定一次要顯示的訊息數
- **RSS 設計** - 在基本 / 進階選項之間切換，以選取新聞概觀的設計（**預設情況下設定為進階設計，請見下圖**）
- **隱藏已閱讀訊息** - 標記此項目以確認不再在新聞概觀中顯示每個已讀取的訊息，並且應以新標題取代
- **顯示按鈕** - 您可以在此欄位中指派在 **AVG Security Toolbar** 新聞概觀應該顯示哪一類的新聞
 -  - 按一下此按鈕以關閉目前開啟的新聞概觀

8.1.6. 刪除歷程記錄

您可以使用此按鈕刪除瀏覽器的歷程記錄，就跟透過 **AVG 標誌 -> 刪除歷程記錄** 選項一樣。

8.1.7. 電子郵件通知程式

電子郵件通知程式 按鈕可讓您啟動在有新抵達的電子郵件時，直接在 **AVG Security Toolbar** 介面中收到通知的選項。該按鈕會開啟下列編輯對話方塊，您可以在此處定義電子郵件帳戶和電子郵件顯示規則的參數。請遵循對話方塊中的指示：



- **帳戶類型** - 指定您的電子郵件帳戶所使用的通訊協定類型。您可以從以下替代選項中選擇：*Gmail*、*POP3*，或從*其他*項目內的下拉式功能表上選擇伺服器名稱（如果您的帳戶是在 *Yahoo! JP Mail* 或 *Hotmail* 上，您可以使用此選項）。如果您不確定您的帳戶所使用的電子郵件伺服器類型，請試著從電子郵件提供者或網際網路服務提供者尋找相關資訊。
- **登入** - 在該以下區段提供了確切形式的 *電子郵件地址*，以及相應的 *密碼*。將 *自動登入* 選項保持勾選狀態，如此就不用重複填寫資料。
- **測試帳戶** - 使用此按鈕測試輸入的詳細資料。
- **重設設定** - 快速移除上面輸入的電子郵件地址詳細資料。
- **每隔 ... 分鐘檢查新電子郵件** - 定義要用來檢查新電子郵件訊息的時間間隔（介於 5-120 分鐘之間），以及指定您是否還要在新郵件抵達時收到通知，以及希望以何種方式收到通知。
- **允許新電子郵件警示** - 取消核取該選項可停用新電子郵件訊息抵達時的直觀通知。
 - **當新電子郵件抵達時播放聲音** - 取消核取該選項可停用新電子郵件抵達時的聲音通知。
 - **5 秒後關閉通知視窗** - 核取該選項可在新電子郵件訊息抵達 5 秒後自動關

閉直觀的通知視窗。

8.1.8. 氣候資訊

氣候按鈕會直接在 *AVG Security Toolbar* 介面內顯示您所選目的地目前溫度的資訊 (每 3-6 個小時更新一次)。按一下該按鈕可開啟新的資訊面板，內含詳細的氣候概觀：



Brno, CZ
[變更位置]

☀️ 25° C

風速: 16,09 公里/小時
日出: 05:04
日落: 20:34

週五
☁️ 高: 24 °C
低: 14 °C

週六
☁️☔ 高: 25 °C
低: 14 °C

更新日期 05/20/2011 13:42:34

YAHOO! NEWS

完整天氣預測 >

以下列出編輯選項：

- **變更位置** - 按一下 **變更位置** 文字可顯示一個名為 **搜尋您的位置** 對話方塊。在文字欄位中填入您所要的位置名稱，並按一下 **搜尋** 按鈕進行確認。接下來，在所有具有相同名稱的位置清單中，選取您正在尋找的目的地。最後，將再次顯示資訊面板，以提供所選位置的氣候資訊。
- **華氏/攝氏溫度轉換** - 在資訊面板的右上角選擇華氏或攝氏溫度刻度。根據您的選擇，將進一步以所選刻度提供溫度資訊。
- **完整預測** - 如果想要完整且詳細的預測，請使用 **完整預測** 連結以前往專門的氣候網站。

8.1.9. Facebook

Facebook 按鈕可讓您直接從 [AVG Security Toolbar](#) 連線到 **Facebook** 社交網路。按一下該按鈕，即會出現登入邀請，再按一下即可開啟 **Facebook** 登入對話方塊。提供您的存取資料，再按一下 **連線** 按鈕。如果您還沒有 [Facebook](#) 帳戶，可以直接使用 **註冊 Facebook** 連結建立帳戶。

一旦完成 [Facebook](#) 註冊程序後，您便會受邀允許 **AVG Social Extension** 應用程式。此應用程式的功能是工具列不可少的 - [Facebook](#) 連線，因此建議允許它的功能，確定您允許之後，即會啟動 [Facebook](#) 連線，而 *AVG Security Toolbar* 內的 **Facebook** 按鈕隨即會提供標準的 [Facebook](#) 功能表選項。



8.2. 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：

8.2.1. 「一般設定」標籤



您可以在此標籤上指定應該在 **AVG Security Toolbar** 面板內顯示或隱藏的工具列控制按鈕。請標記各個按鈕上您想顯示的任何選項。此外，您也可以找到工具列每個按鈕的功能描述：

- **頁面狀態按鈕** - 該按鈕提供在 **AVG Security Toolbar** 內顯示有關目前開啟頁面之安全性狀態資訊的可能性
- **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
- **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
- **電子郵件通知程式按鈕** - 該按鈕可讓您新抵達的電子郵件訊息顯示在 **AVG Security Toolbar** 介面中。
- **氣候按鈕** - 該按鈕提供所選位置中有關天氣狀況的即時資訊
- **Facebook 按鈕** - 該按鈕提供至 [Facebook](#) 社交網路的直接連線

8.2.2. 「實用按鈕」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。

8.2.3. 「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。



- **瀏覽器安全性** - 核取此項目可啟動或關閉 [AVG Search-Shield](#) 和/或 [Surf-Shield](#) 服務
- **等級** - 根據您想要使用的 [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！**

8.2.4. 「進階選項」標籤



在**進階選項**標籤中，首先選擇您要設為預設的搜尋引擎。您可以選擇 *AVG Secure Search (powered by Google)*、*Baidu*、*WebHledani*、*Yandex* 和 *Yahoo!JP*。變更預設搜尋引擎之後，您必須重新開啟 Internet 瀏覽器，變更才會生效。

接下來，您可以啟動或關閉更特定的 **AVG Security Toolbar** 設定 (列出的標題指的是預設



AVG Secure Search (powered by Google) 設定：

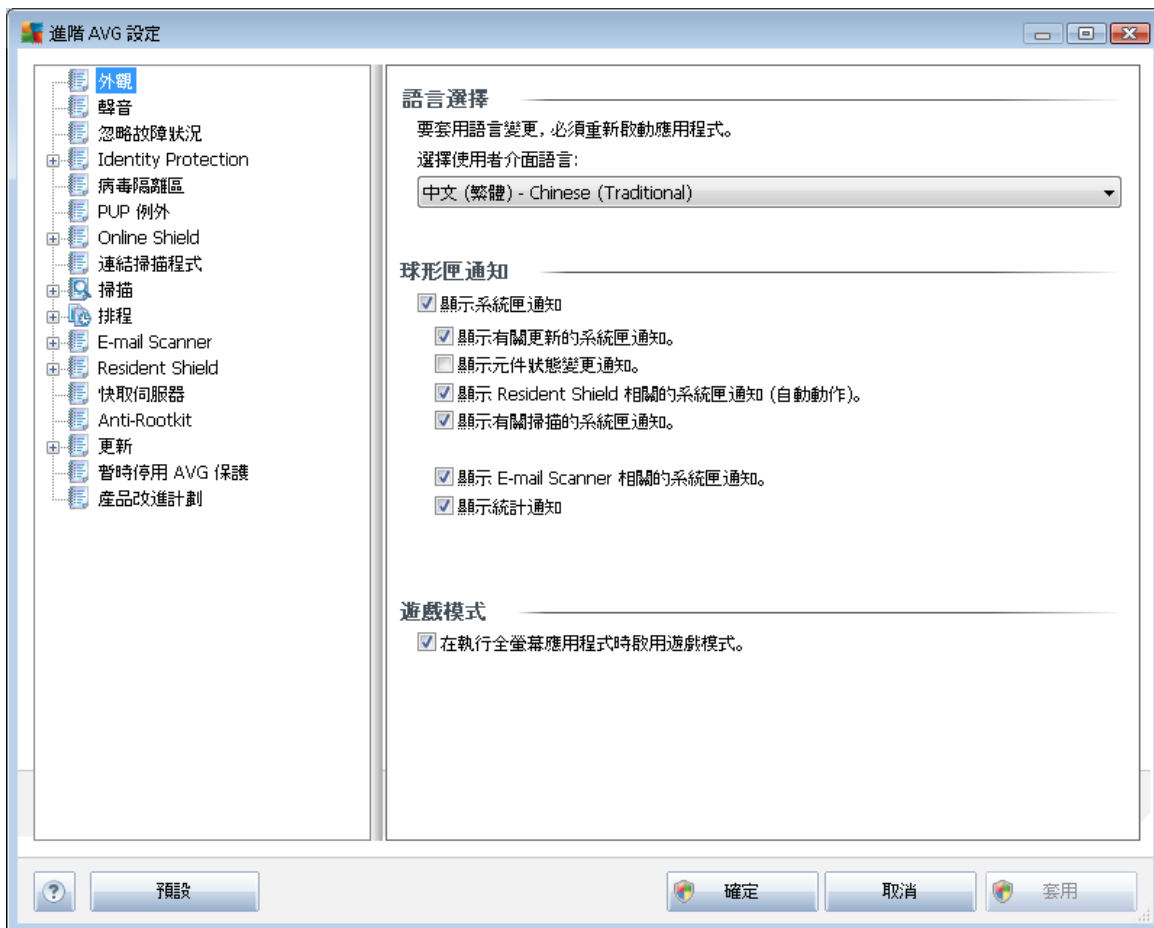
- **設定並將 AVG Secure Search (powered by Google) 保持為地址列上的搜尋提供者** - 如果勾選此選項，它可允許您直接將搜尋關鍵字鍵入 Internet 瀏覽器的地址列中，並會自動使用 Google 服務來搜尋相關網站。
- **讓 AVG 對瀏覽器巡覽錯誤提供建議 (404/DNS)** - 如果您在搜尋網路時遇到不存在的頁面，或者頁面無法顯示 (404 錯誤)，您將被自動重新導向至一個讓您選取其他相關主題的總覽頁面。
- **設定並將 AVG Secure Search (powered by Google) 保持為預設的搜尋提供者** - Google 是 AVG Security Toolbar 中網頁搜尋的預設搜尋引擎，如果啟動該選項，它也會成為您網頁瀏覽器的預設搜尋引擎。

9. AVG 進階設定

AVG Anti-Virus 2011 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。

9.1. 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：



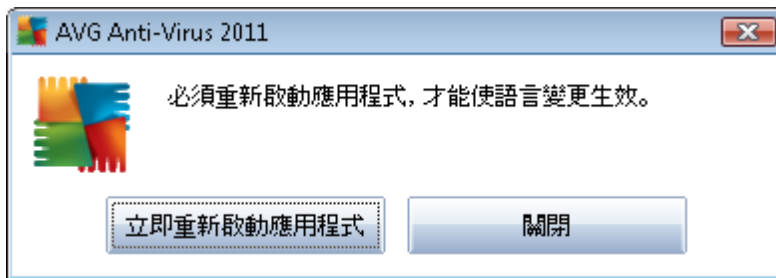
語言選擇

在 **語言選擇** 區段，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。下拉式功能表只會提供您之前在 [安裝程序](#) 期間選擇要安裝的語言 (請參閱 [自訂選項](#) 一章)，外加英文 (預設情況下會安裝的語言)。不過，若要完成將應用程式的語言切換到另一種語言，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，並按一下 **套用** 按鈕 (右下角) 來確認您的選擇



- 按一下 **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

在此區段，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*)，並顯示通知。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 (自動動作)** - 決定要顯示還是隱藏有關檔案儲存、複製或開啟中的程序的資訊 (只有當 Resident Shield [自動修復](#) 功能啟動時，才會顯示該組態)；
 - **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 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。
 - **顯示統計通知** - 將該選項保持核取狀態，可在系統匣中顯示常規統計審核通知。

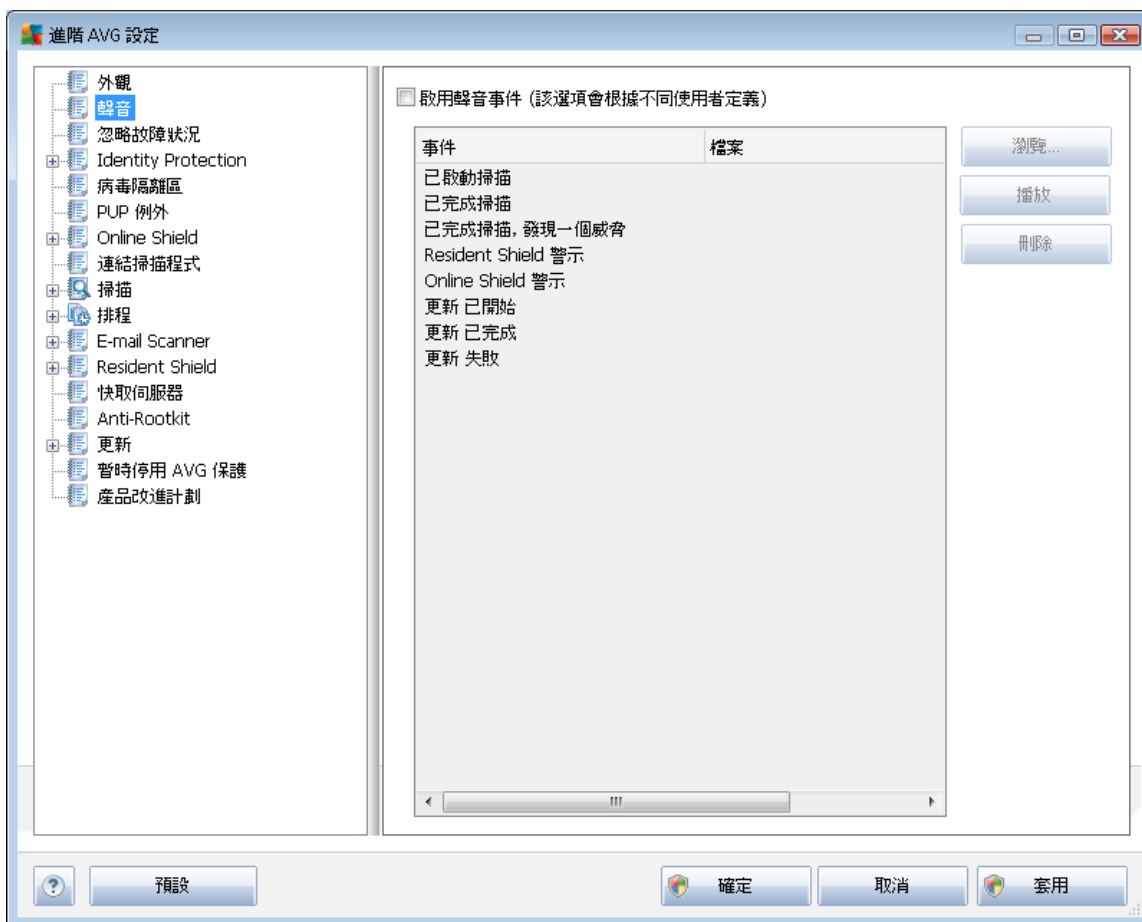
遊戲模式



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

9.2. 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：

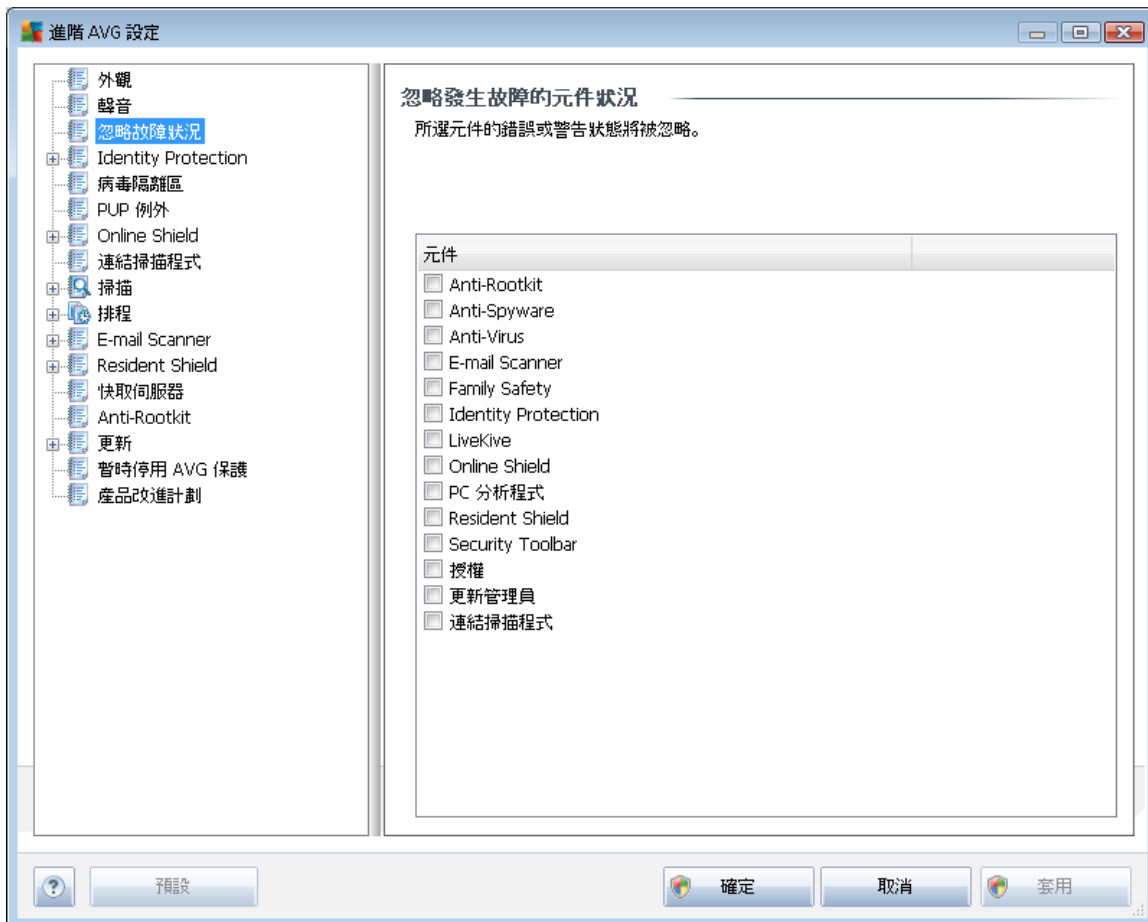


接著，從清單中選取相應事件，並瀏覽 (瀏覽) 您的磁碟以尋找要指派給此事件的適當聲音。若要聆聽所選的聲音，請在清單中反白該事件，再按播放按鈕。使用刪除按鈕即可移除指派給特定事件的聲音。

注意：只支援 *.wav 聲音！

9.3. 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：



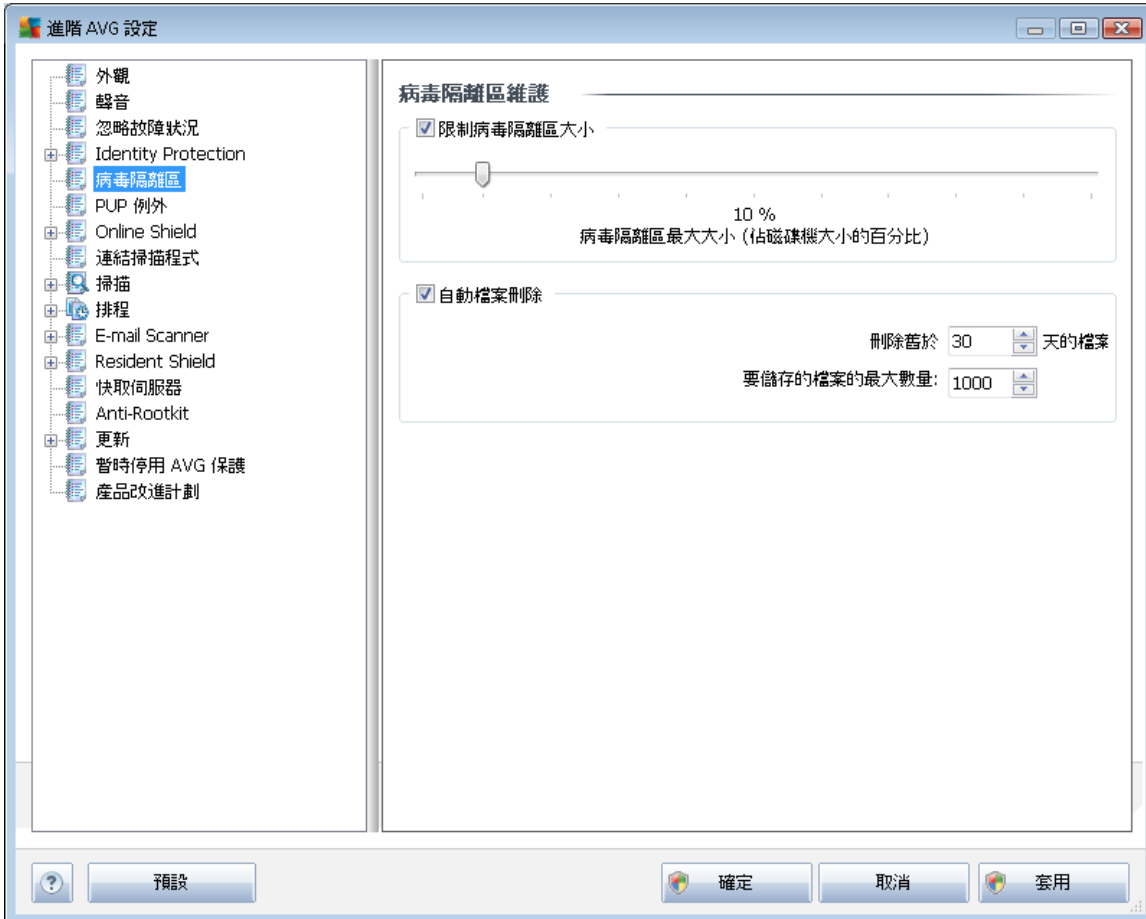
預設情況下，此清單中沒有選取任何元件。這意味著一旦有元件變為錯誤狀態，將立即透過以下方式通知您：

- [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，
- 現有問題的文字描述位於 AVG 主視窗的 [安全性狀態資訊](#) 區段

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

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

9.4. 病毒隔離區

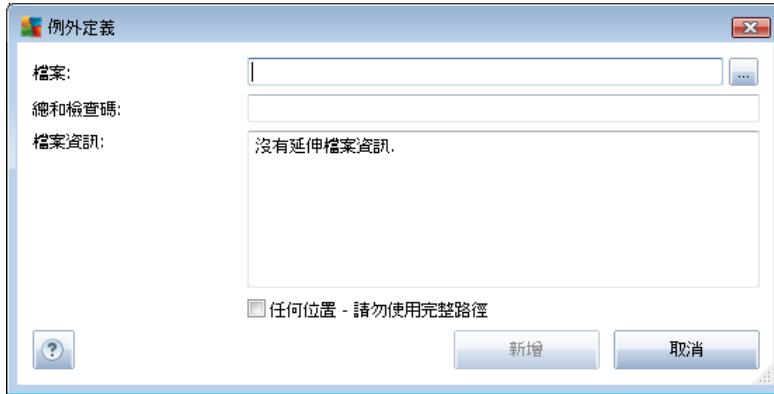


病毒隔離區維護對話方塊可讓您定義多個參數，這些參數與管理儲存在 **病毒隔離區** 中的物件有關：

- **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**)

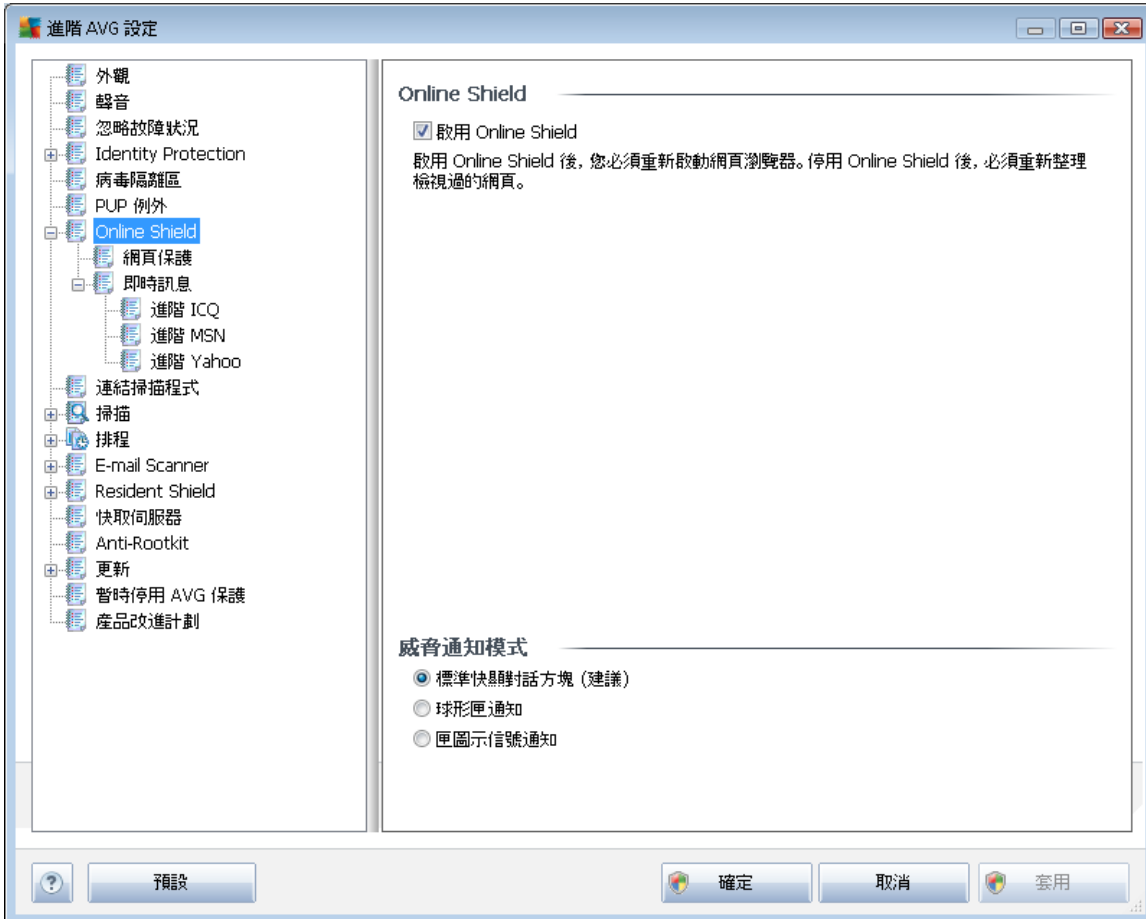
9.5. PUP 例外

AVG Anti-Virus 2011 能夠分析和偵測系統中潛在的不受歡迎的可執行應用程式或 DLL 程式庫。在某些情況下，使用者可能希望將特定的不明程式保留在電腦上 (**故意安裝的程式**)。一些程式 (尤其是免費的) 會包含廣告軟體。AVG 可能會將此類廣告程式偵測和報告為 **潛在的不受歡迎程式**。如果您想在電腦上保留此類程式，可將其定義為潛在的不受歡迎程式例外：



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

9.6. Online Shield



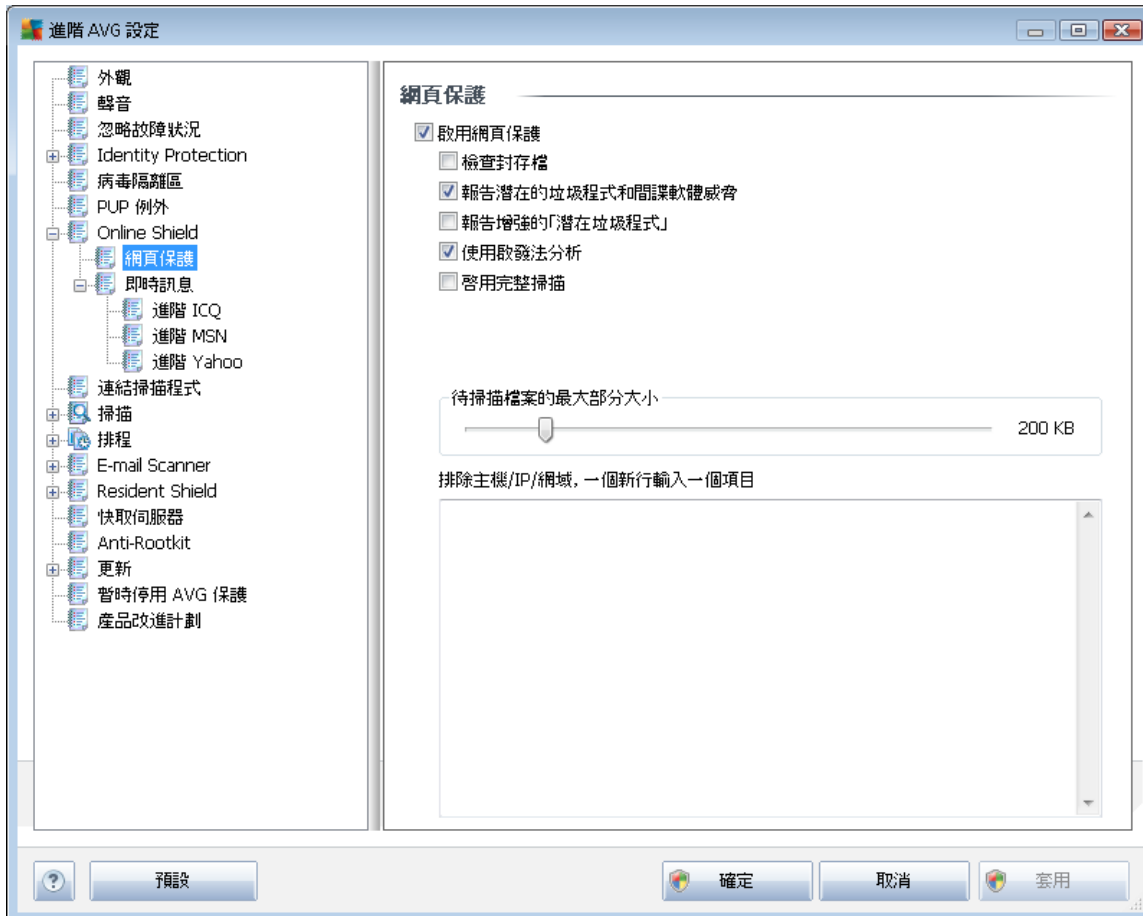
Online Shield 對話方塊可讓您透過 [啟用 Online Shield](#) 選項 (預設已啟動) 啟用 / 停用整個 **Online Shield** 元件。有關此元件的其他進階設定, 請繼續至樹狀巡覽目錄中列出的後幾個對話方塊:

- [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。

9.6.1. 網頁保護

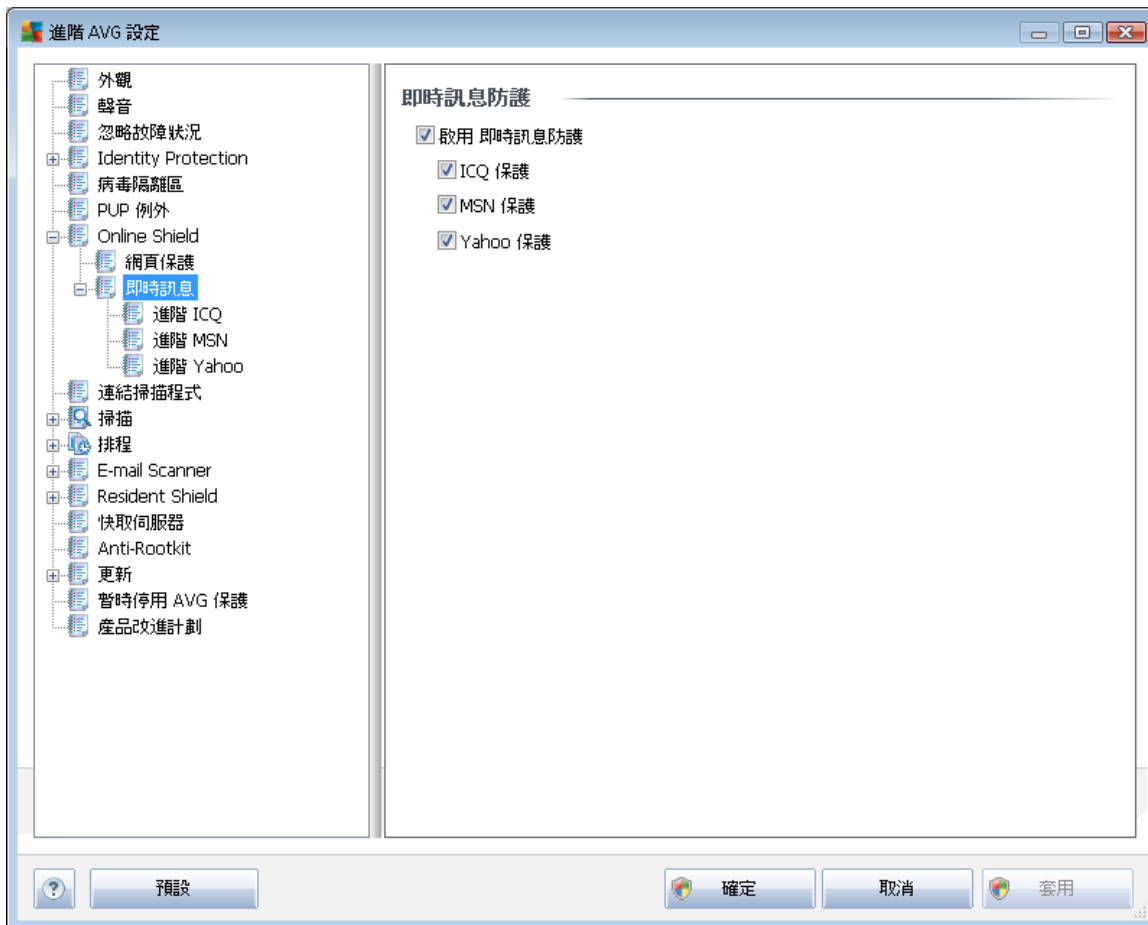


在 **網頁保護** 對話方塊中，您可以編輯元件中有關網站內容掃描的組態。編輯介面可讓您設定以下基本選項：

- **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** - （預設為開啟）：掃描要顯示的 www 網頁中可能包含的封存的內容。
 - **報告潛在的不受歡迎程式和間諜軟體威脅** - （預設為開啟）：核取此方塊可啟動 **Anti-Spyware** 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別；雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
 - **報告增強的潛在不受歡迎程式** - （預設為關閉）：標記此選項以偵測延伸的 **間諜軟體**：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- **使用啟發法分析** - (預設為開啟) : 使用 [啟發法分析](#) 方法 (在虛擬電腦環境中動態模擬掃描物件的指令) 掃描要顯示的網頁內容。
- **啟用完整掃描** (預設為關閉) - 在特殊情況下 (懷疑您的電腦受到感染), 您可以核取此選項來啟動最完整的掃描演算法, 這甚至會掃描幾乎不會被感染的電腦區域, 以防萬一。不過請記住, 這種方法相當耗時。
- **待掃描的檔案的最大部分大小** - 如果包含的檔案列示在顯示的頁面中, 您甚至還可以在下載到電腦上之前掃描其內容。但掃描較大的檔案需花費一定時間, 網頁下載可能會明顯變慢。您可以使用滑桿來指定仍使用 [Online Shield](#) 掃描之檔案的最大大小。即使下載的檔案超過指定大小, 致使無法使用 Online Shield 進行掃描, 您仍然會受到保護: 如果該檔案受感染, [Resident Shield](#) 會立即偵測到。
- **排除主機 / IP / 網域** - 您可以將無需 Online Shield 掃描的伺服器 ([主機](#)、[IP 位址](#)、[含有遮罩的 IP 位址或 URL](#)) 或網域的完整名稱輸入到該文字欄位。因此, 請只排除您能完全確定絕對不會提供危險網站內容的主機。

9.6.2. 即時訊息

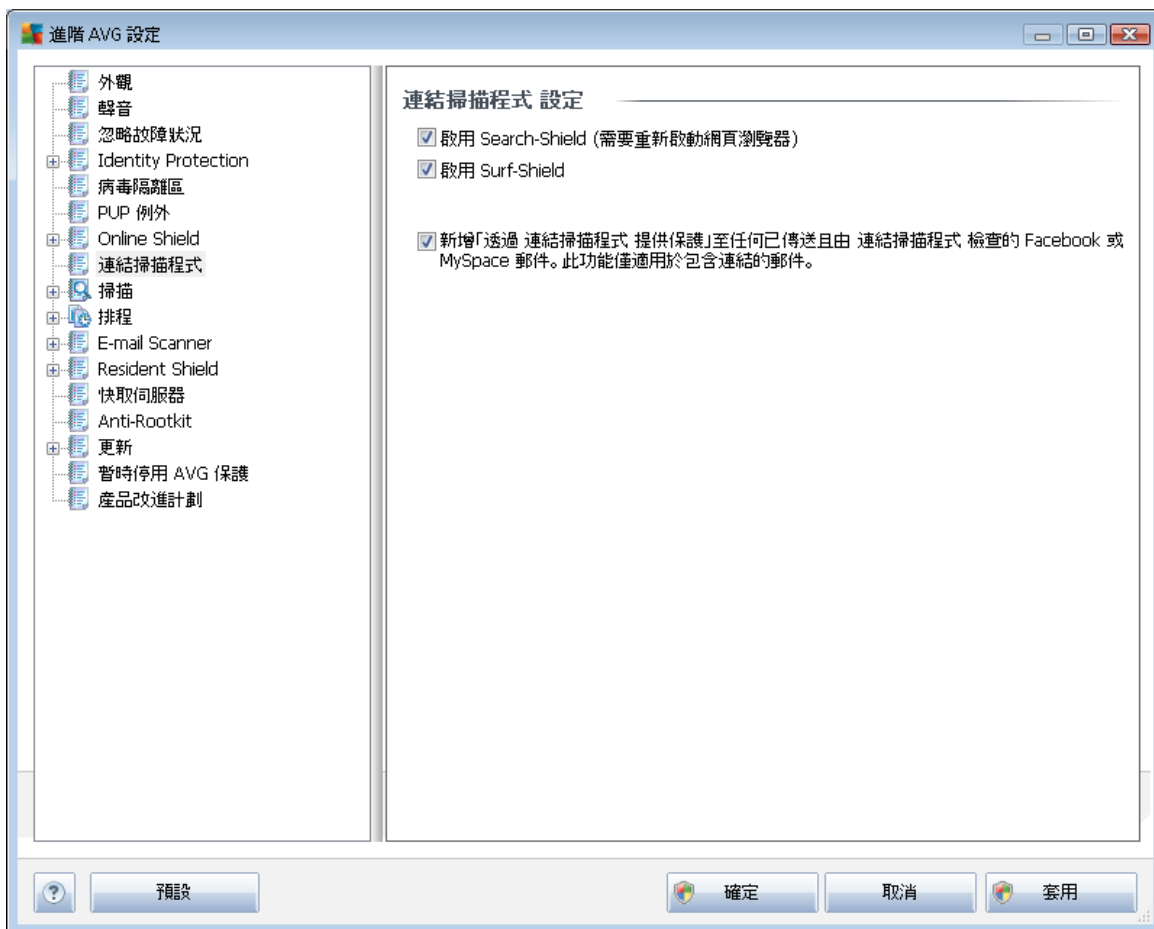


在**即時訊息防護**對話方塊中, 您可以編輯關於即時訊息掃描的 [Online Shield](#) 元件設定。目前支援以下三種即時訊息程式: **ICQ**、**MSN** 和 **Yahoo** - 如果您希望 [Online Shield](#) 驗證線上通訊確實沒有病毒, 請勾選您要的項目。

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)。

9.7. 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 Search-Shield** - (預設情況下開啟)：在透過 Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 執行的搜尋上提供忠告圖示：事先檢查搜尋引擎傳回的網站內容。
- **啟用 Surf-Shield** - (預設情況下為開啟)：在存取惡意探索站點時，提供主動 (即時) 保護。當使用者透過網頁瀏覽器 (或任何其他使用 HTTP 的應用程式) 存取已知惡意站點時，其連線及其惡意探索內容都將被封鎖。
- **新增『受到 LinkScanner 保護』...** - 標記此項目以確認您希望將 **Link Scanner** 檢查上的認證通知輸入所有包含使用中的超連結，以及由 Facebook 和 MySpace 社交網路寄出的郵件。

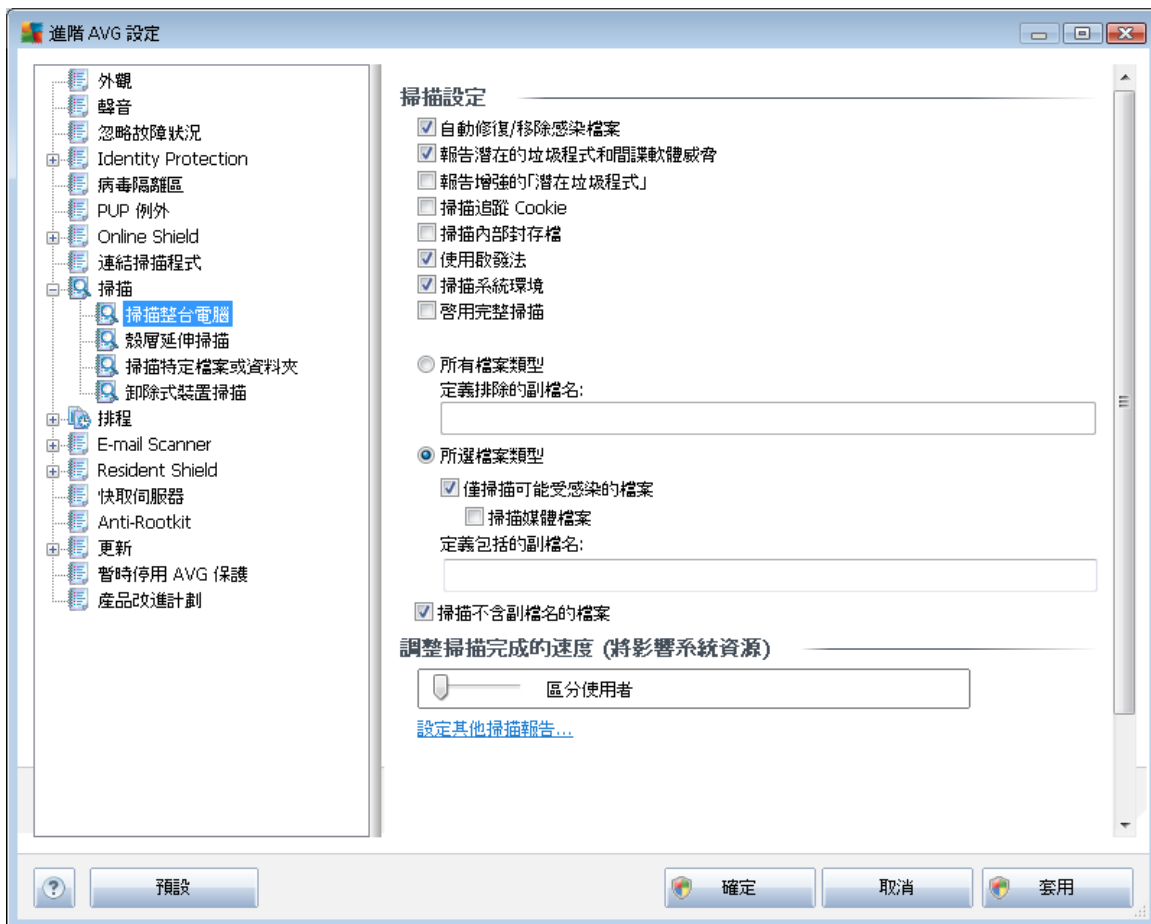
9.8. 掃描

進階掃描設定為四個類別，這些類別指的是軟體廠商定義的特定掃描類型：

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

9.8.1. 掃描整台電腦

[完整電腦掃描](#)選項可供您編輯軟體廠商預先定義的掃描類型之一，即[掃描整台電腦](#)的參數：



掃描設定

[掃描設定](#)區段提供可以選擇性開啟/關閉的掃描參數清單：



- **自動修復/移除感染檔案 (預設為開啟)** - 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至 **病毒隔離區**。
- **報告潛在的不受歡迎程式和間諜軟體威脅 (預設為開啟)** - 核取此方塊可啟動 **Anti-Spyware** 引擎，並掃描間諜軟體和病毒。**間諜軟體** 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式集 (預設為關閉)** - 標記此選項以偵測延伸的 **間諜軟體** 套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
- **掃描追蹤 Cookie (預設為關閉)** - **Anti-Spyware** 元件的此一參數定義在掃描期間應偵測 cookie：(HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容)
- **掃描封存內部 (預設為關閉)** - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在封存內，如 ZIP、RAR...
- **使用啟發法 (預設為開啟)** - 啟發法分析 (在虛擬電腦環境中動態模擬掃描物件的指令) 將成為掃描過程中用於偵測病毒的方法之一；
- **掃描系統環境 (預設為開啟)** - 掃描時還會檢查您電腦的系統區域。
- **啟用完整掃描 (預設為關閉)** - 在特定情況下 (懷疑您的電腦受到感染)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

接下來，您應該決定是否要掃描

- **所有檔案類型** - 您可以透過一份逗號分隔 (儲存之後，逗號會變成分號) 檔案格式的清單來定義掃描例外，使這些檔案不會被掃描；
- **所選檔案類型** - 您可以指定您只想要掃描可能受感染的檔案 (將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔)，包括媒體檔案 (視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。
- 或者，您也可以決定 **掃描不含副檔名的檔案** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

調整完成掃描的速度

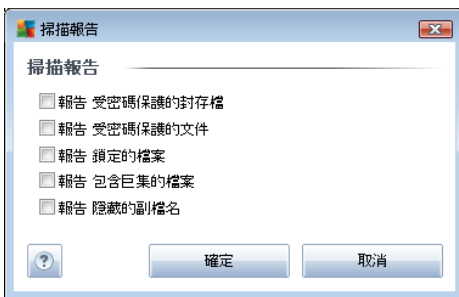
您可以在 **調整完成掃描的速度** 區段內，依據系統的資源使用量來進一步指定需要的掃描速度。預設情況下，該選項值會設為 **區分使用者層級的自動資源使用量**。如果您要加快



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

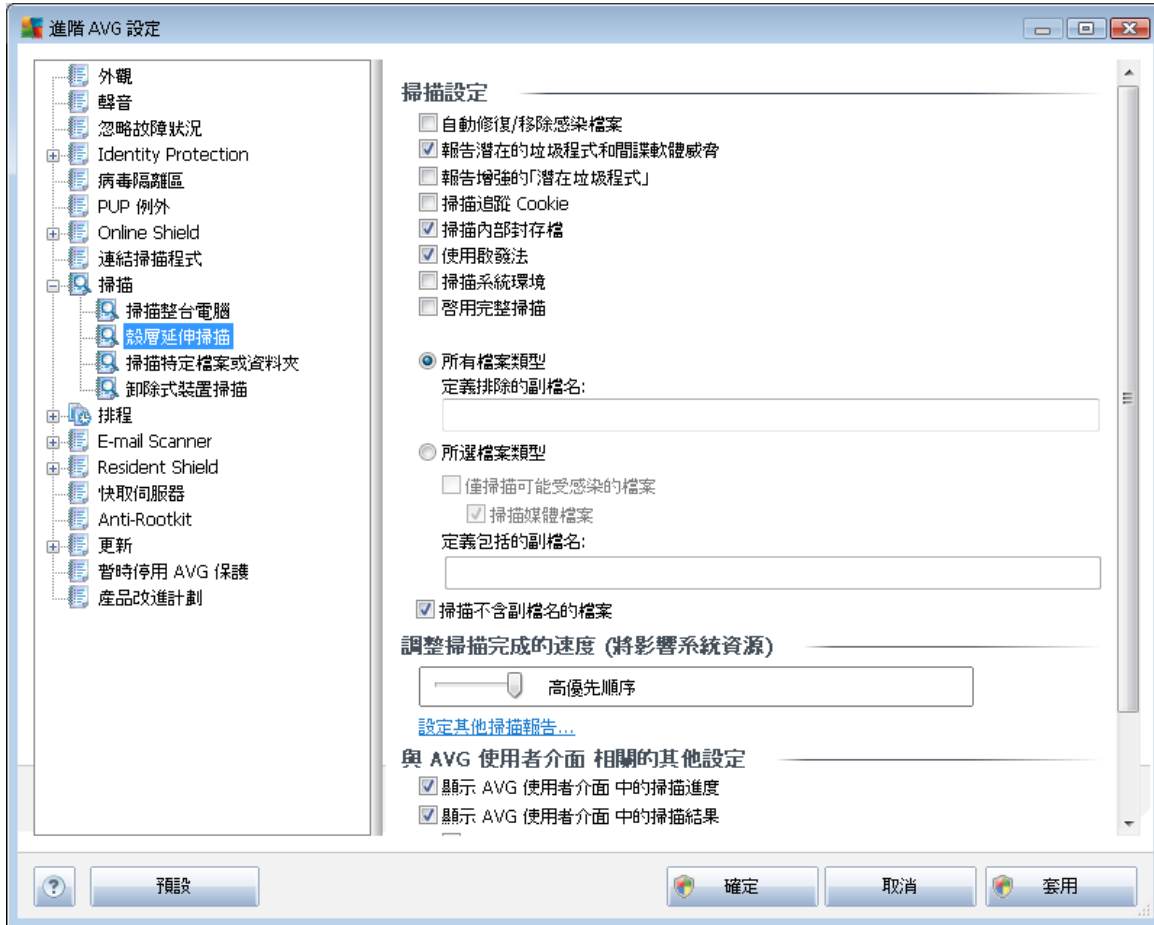
設定其他掃描報告...

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



9.8.2. 殼層延伸掃描

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



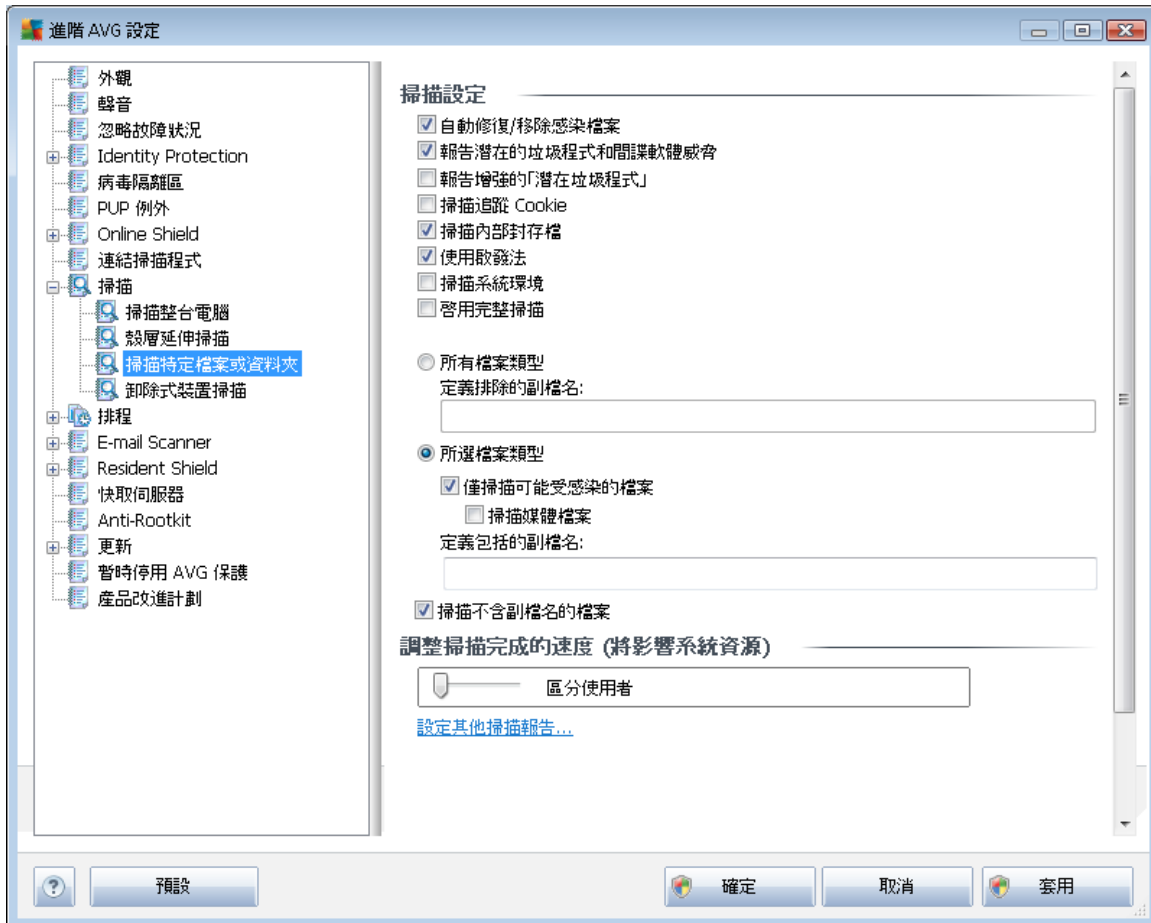
參數清單與 [掃描整台電腦](#) 所用的那些參數完全相同。但是預設設定並不相同（例如，完整電腦掃描在預設情況下並不會檢查封存，但是會掃描系統環境，而殼層延伸掃描則剛好相反）。

注意：有關特定參數的敘述，請查閱 [AVG 進階設定 / 掃描 / 完整電腦掃描](#) 一章。

與 [完整電腦掃描](#) 對話方塊相比，[殼層延伸掃描](#) 對話方塊也包含名為 **與 AVG 使用者介面相關的其他設定** 區段，您可以在此處指定是否可以從 AVG 使用者介面存取掃描進度和掃描結果。另外，您可以定義只在掃描期間偵測到感染檔案時才顯示掃描結果。

9.8.3. 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 **完整電腦掃描** 編輯對話方塊相同。所有組態選項都相同，但是 **掃描整台電腦** 的預設設定較為嚴格：

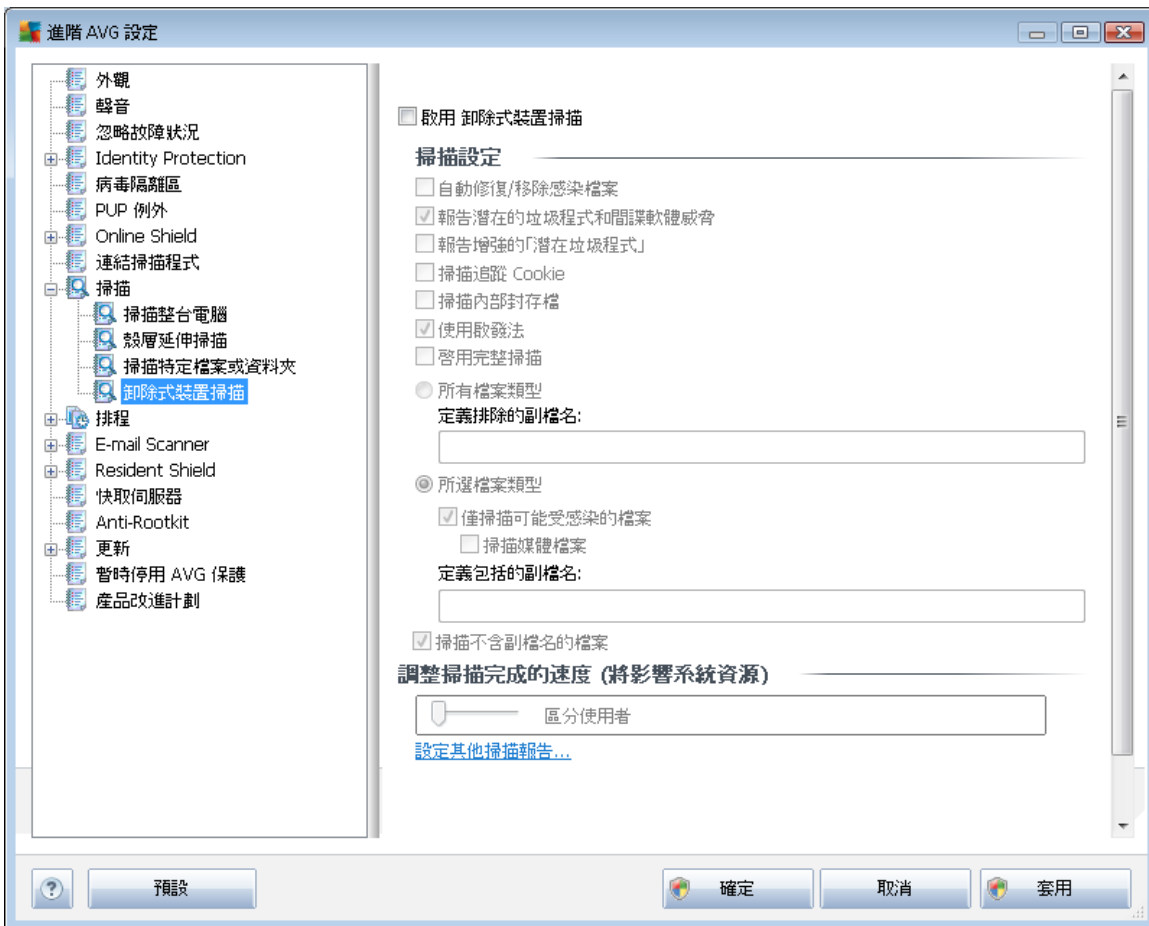


在此組態對話方塊中設定的所有參數，都只會套用到為 **掃描特定檔案或資料夾** 選取的區域！

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

9.8.4. 卸除式裝置掃描

卸除式裝置掃描的編輯介面與[完整電腦掃描](#)編輯對話方塊也十分相似：



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

注意：有關特定參數的說明，請查閱[AVG 進階設定 / 掃描 / 完整電腦掃描](#)一章。

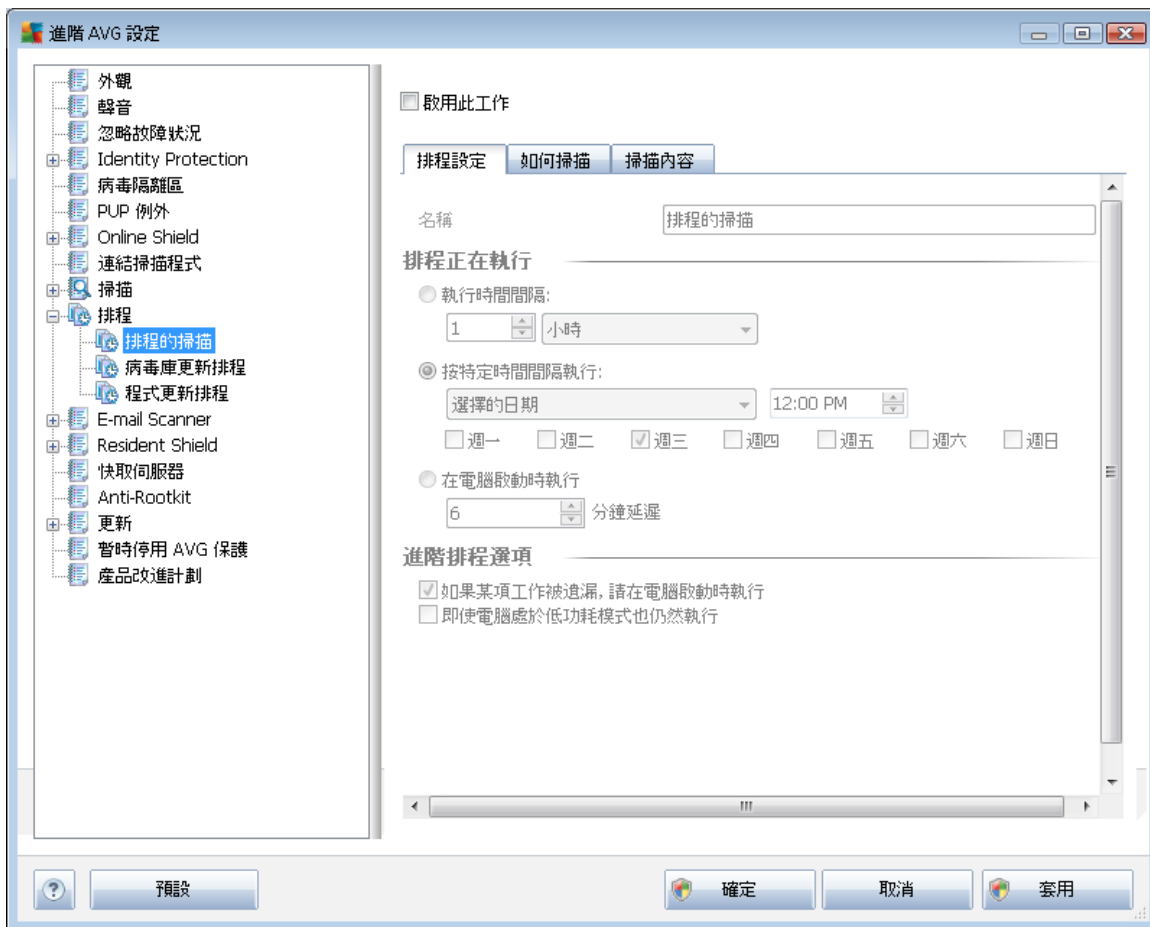
9.9. 排程

在排程部分，您可以編輯以下項目的預設設定：

- [排程掃描](#)
- [病毒庫更新排程](#)
- [程式更新排程](#)

9.9.1. 排程掃描

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



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

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

在此對話方塊中，您可以進一步定義掃描的以下參數：

排程執行



在這裡，您可以為新排程的掃描啟動指定時間間隔。時間安排有以下幾種定義方式：定義一段時間後再次啟動掃描（**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

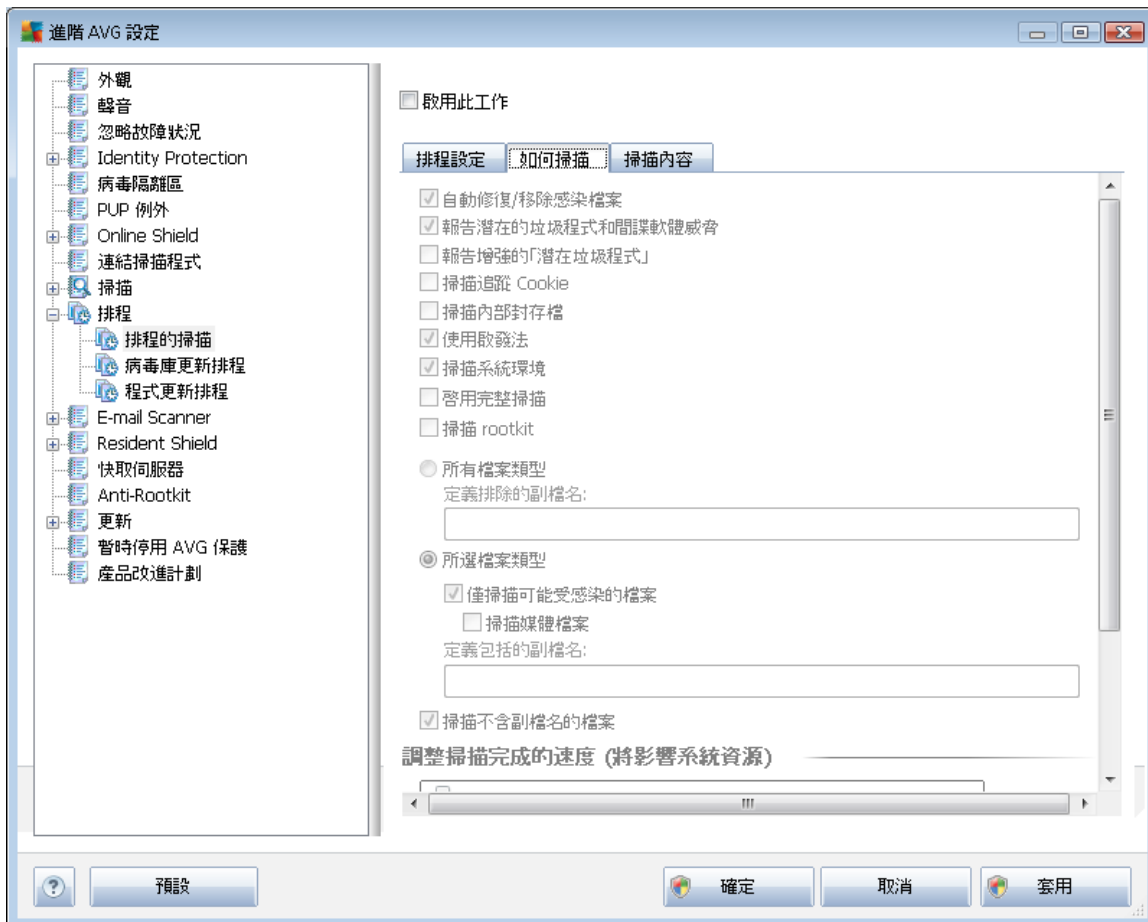
此區段允許您定義若電腦處於低功耗模式或完全關閉模式時，應該在何種條件下啟動 / 不啟動掃描。

排程的掃描在您指定的時間啟動後，軟體將透過在 [AVG 系統匣圖示](#) 中開啟一個快顯視窗來通知您：



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





在 **如何掃描** 標籤上，您將看到一份可選擇開啟/關閉的掃描參數清單。預設情況下，大多數參數都已開啟，並將在掃描期間套用其功能。除非您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** (預設為開啟)：如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至 [病毒隔離區](#)。
- **報告潛在的不受歡迎程式和間諜軟體威脅** (預設為開啟)：核取此方塊可啟動 [Anti-Spyware](#) 引擎，並掃描間諜軟體和病毒。[間諜軟體](#) 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式** (預設為關閉)：標記此選項以偵測延伸的 [間諜軟體](#) 套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
- **掃描追蹤 Cookie** (預設為關閉)：[Anti-Spyware](#) 元件的此一參數定義在掃描期間應偵測 cookie；(HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站



喜好或電子購物車內容)

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

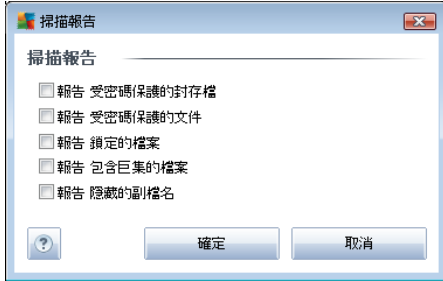
- **所有檔案類型** - 您可以透過一份不應掃描檔案清單 (以逗號分隔副檔名；儲存之後，逗號會變成分號) 來定義掃描例外；
- **所選檔案類型** - 您可以指定您只想要掃描可能受感染的檔案 (將不掃描不會被感染的檔案，例如一些純文字檔或其他一些非可執行檔)，包括媒體檔案 (視訊、音訊檔案 - 若保持取消核取此方塊，將可進一步縮減掃描時間，因為這些檔案通常都很大，而且不太可能被病毒感染)。同樣地，您可以依副檔名指定始終都應該掃描的檔案。
- 或者，您也可以決定**掃描不含副檔名的檔案** - 此選項預設為開啟，而且建議您保留此設定，除非您確實有必要變更。沒有副檔名的檔案非常可疑，始終都應該掃描。

調整完成掃描的速度

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

設定其他掃描報告

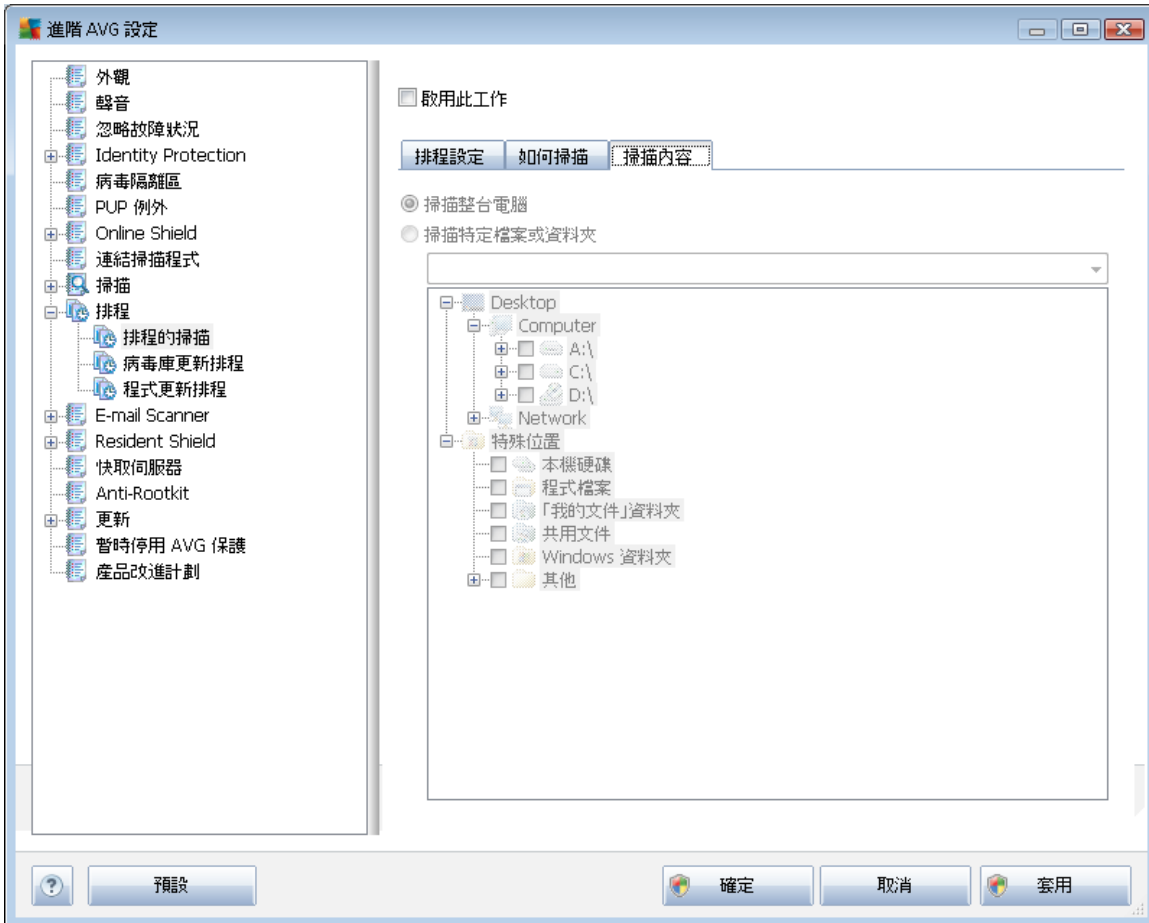
按下**設定其他掃描報告...**連結，可以開啟名為**掃描報告**的獨立對話方塊視窗，您可在其勾選數個項目，以定義應該報告哪些掃描結果：



其他掃描設定

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

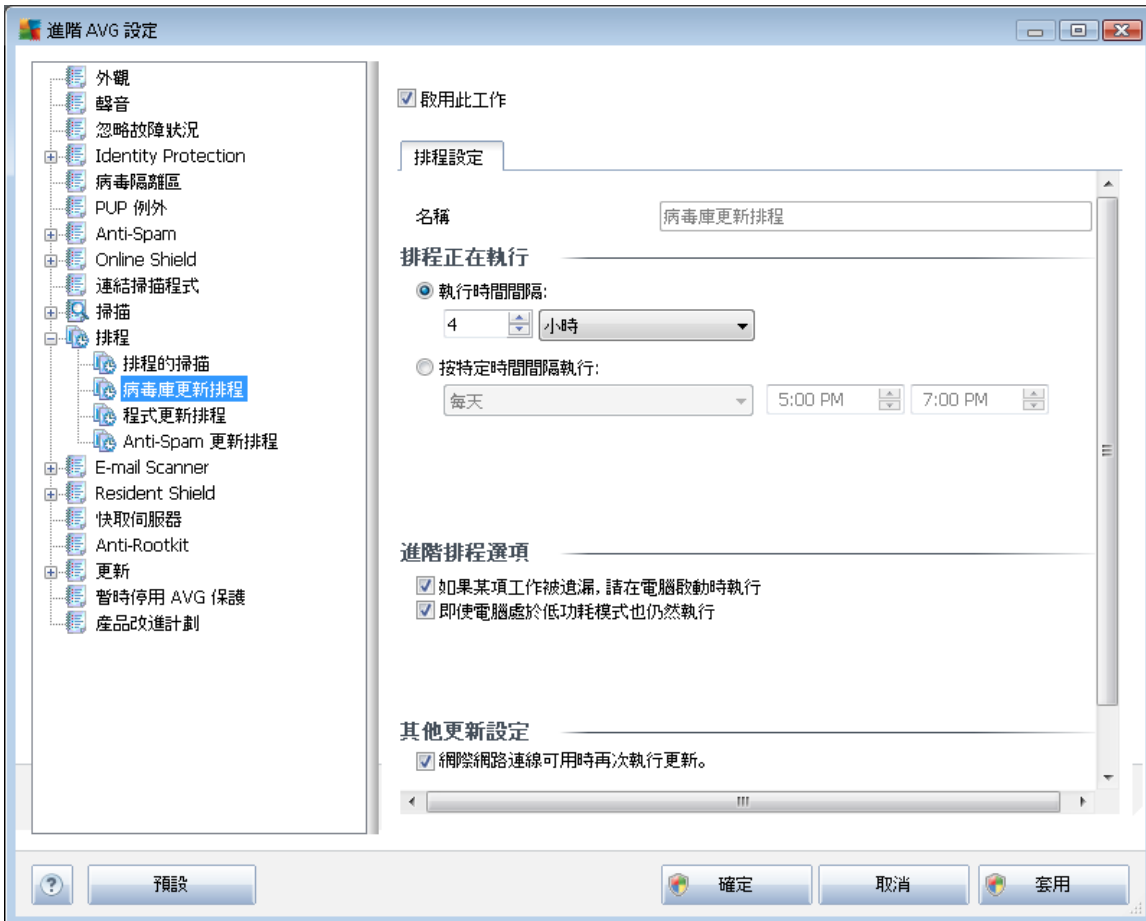




在 **掃描內容** 標籤上，您可以定義是要排程 **掃描整台電腦**，還是 **掃描特定檔案或資料夾**。如果您選取掃描特定檔案或資料夾，則會啟動顯示在此對話方塊底端的樹狀結構，讓您指定要掃描的資料夾。

9.9.2. 病毒庫更新排程

真的有必要時，您可以取消核取啟用此工作項目，即可暫時停用排定的病毒庫更新，稍後再開啟它：



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。

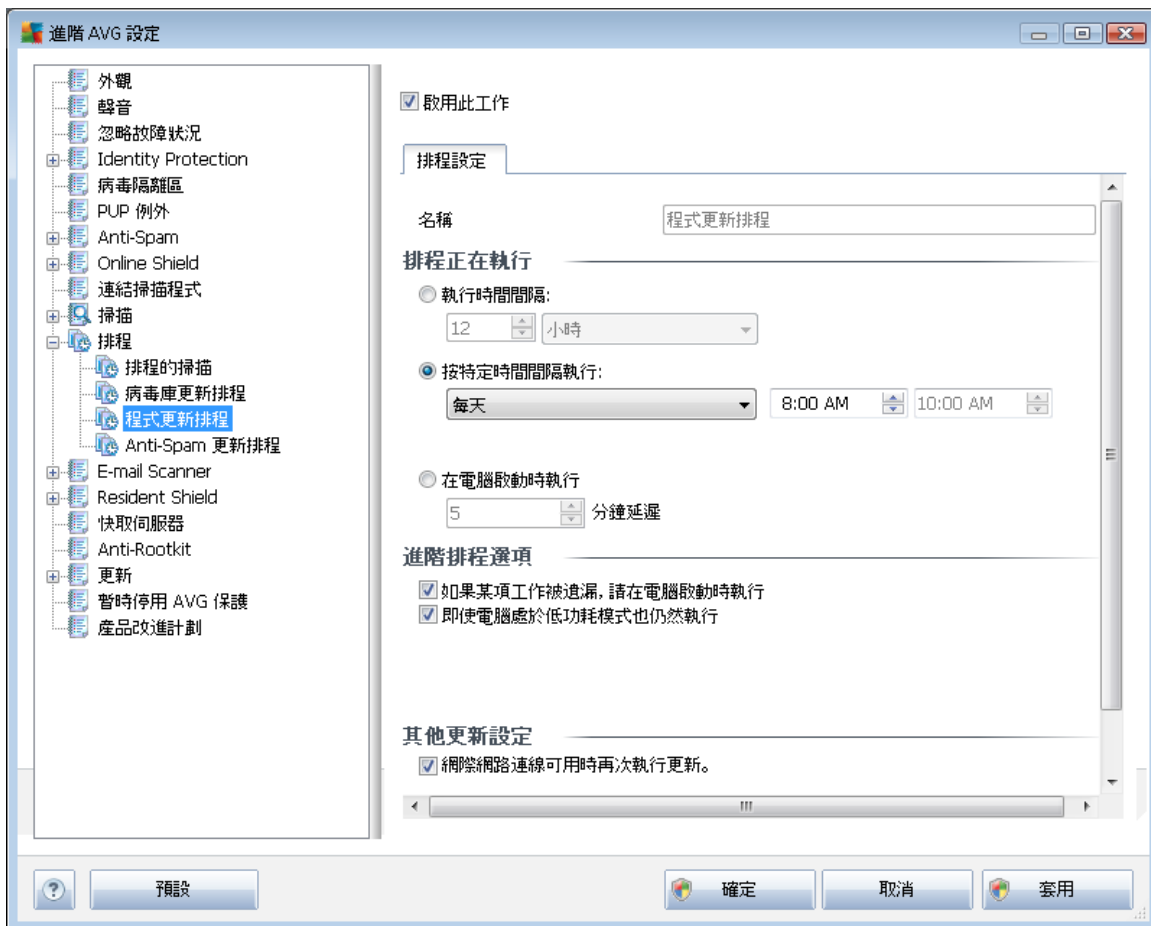
其他更新設定

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)。

9.9.3. 程式更新排程

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



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

排程執行

在這裡，為新排程的程式更新啟動指定時間間隔。時間安排有以下幾種定義方式：定義



一段時間後再次啟動更新 (每...執行一次), 或定義確切的日期和時間 (在特定時間執行...), 或者定義更新啟動應關聯的事件 (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

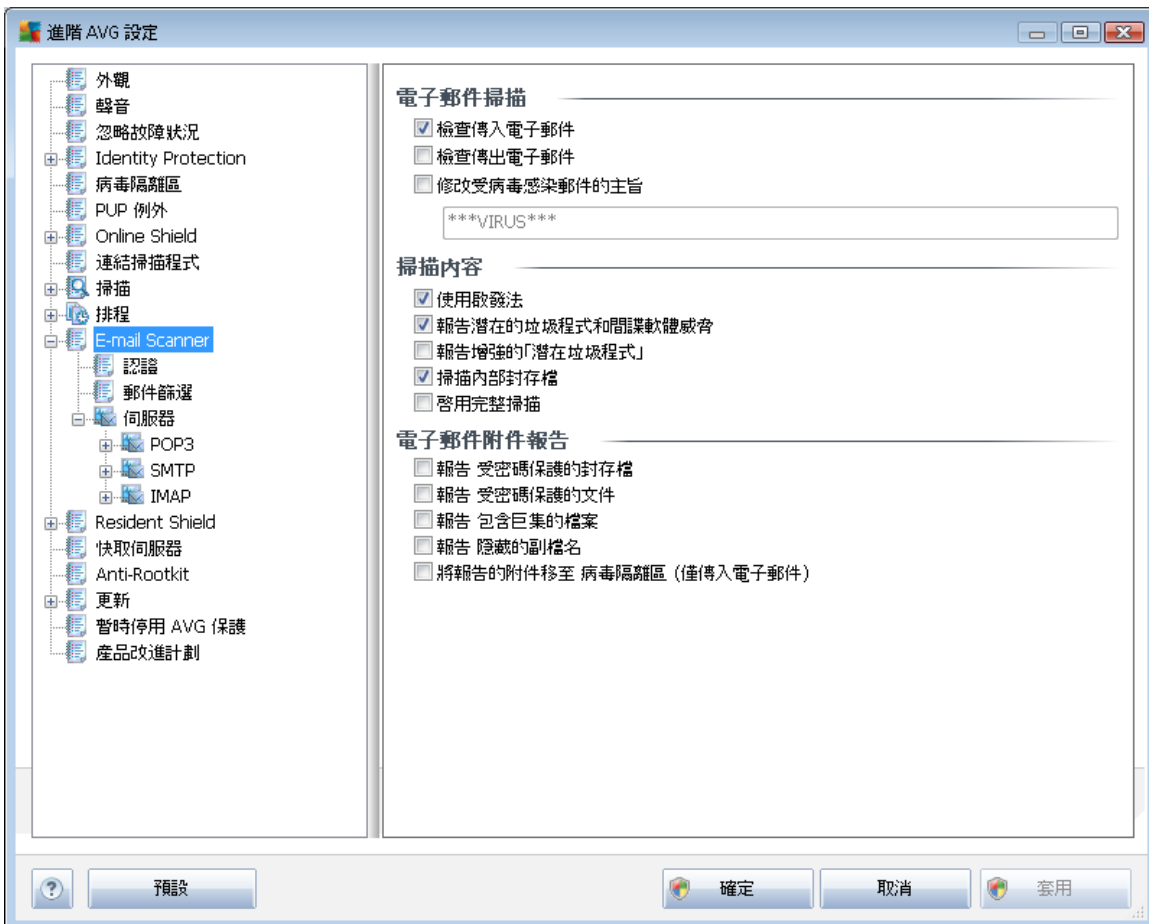
核取 **網際網路連線可用時即再次執行更新** 選項，確定在發生網際網路連線損毀且更新程序失敗的情況下，它會在網際網路恢復連線後立即重新啟動。

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。

9.10. E-mail Scanner

E-mail Scanner 對話方塊由三個區段構成：



電子郵件掃描

您可以在此區段中為傳入和 / 或傳出的電子郵件訊息設定以下基本資訊：

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



掃描屬性

您可以在這個區段中指定電子郵件訊息的掃描方式：

- **使用啟發法 (預設為開啟)** - 核取此選項可在掃描電子郵件訊息時使用 [啟發式偵測方法](#)。開啓此選項後，您不僅可以透過副檔名篩選電子郵件附件，也可以透過考量附件的實際內容來進行篩選。篩選可以在 [郵件篩選](#) 對話方塊中進行設定。
- **報告潛在的不受歡迎程式和間諜軟體威脅 (預設為開啟)** - 核取此方塊可啟動 [Anti-Spyware](#) 引擎，並掃描間諜軟體和病毒。[間諜軟體](#) 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式 (預設為關閉)** - 標記此選項來偵測延伸的 [間諜軟體](#)：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
- **掃描封存內部 (預設為開啟)** - 核取此方塊可掃描附加到電子郵件訊息的封存內容。
- **啟用完整掃描 (預設為關閉)** - 在特殊的情況下 (例如懷疑您的電腦受到病毒或入侵程式感染)，您可以核取此選項來啟動最完整的掃描演算法，這甚至會掃描幾乎不會被感染的電腦區域，以防萬一。不過請記住，這種方法相當耗時。

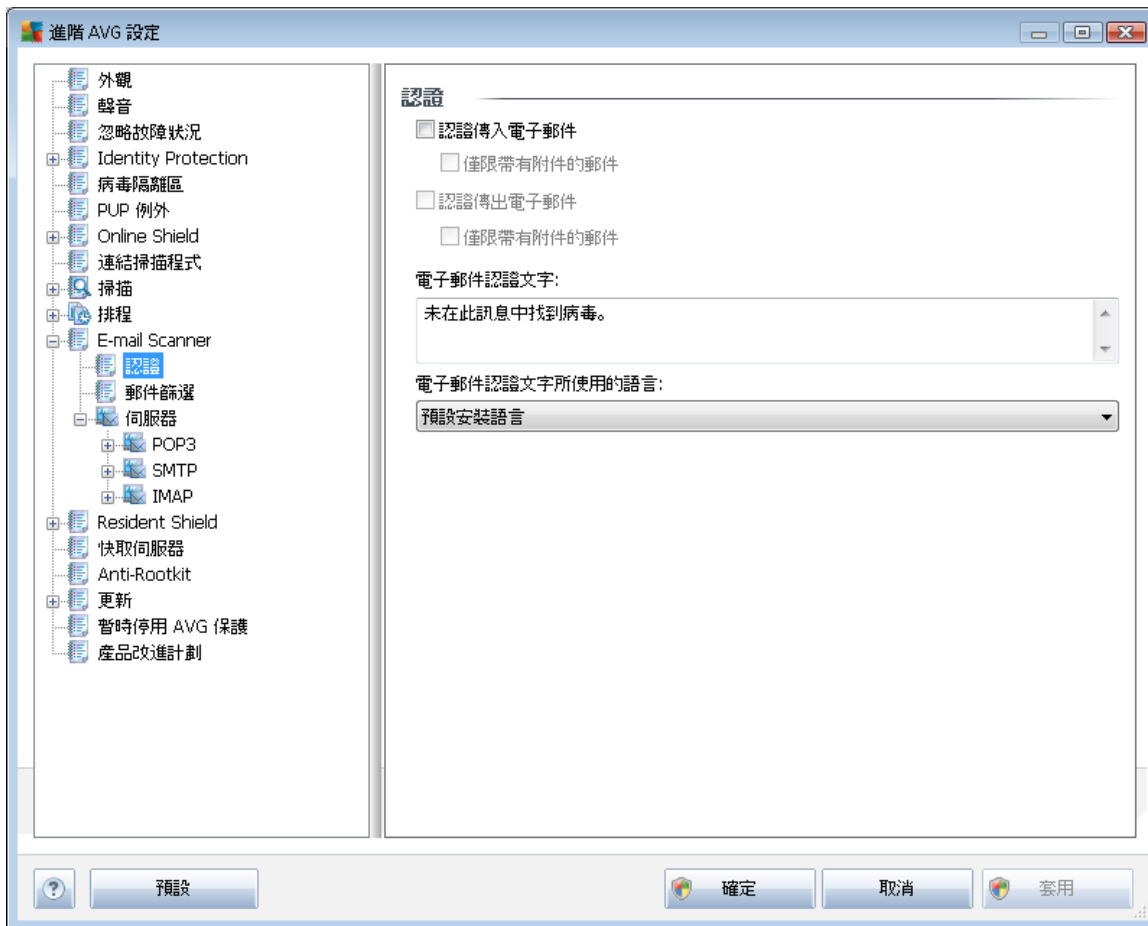
電子郵件附件報告

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

- **報告受密碼保護的封存** - 受密碼保護的封存 (ZIP、RAR 等) 無法進行病毒掃描；核取此方塊可將這些封存報告為存在潛在的危險。
- **報告受密碼保護的文件** - 受密碼保護的文件無法進行病毒掃描；核取此方塊可將這些文件報告為潛在危險內容。
- **報告包含巨集的檔案** - 巨集是一種預定義的步驟序列，用於協助使用者更輕鬆地完成某項工作 (例如我們都熟知的 MS Word 巨集)。因此，巨集可能會包含潛在危險的指示，您可以核取此方塊以確保將包含巨集的檔案報告為可疑內容。
- **報告隱藏的副檔名** - 隱藏副檔名可以使諸如可疑的可執行檔 ("something.txt.exe") 等檔案看起來像是無害的純文字檔案 ("something.txt")；核取此方塊可將這些檔案報告為潛在危險內容。
- **將報告的附件移至病毒隔離區** - 指定是否要透過電子郵件收到有關以下情況的通知：偵測到掃描郵件的附件為受密碼保護的封存、受密碼保護的文件、包含巨集的檔案和 / 或具有隱藏副檔名的檔案。如果在掃描過程中發現這類郵件，定義是否將偵測到的受感染物件移至 [病毒隔離區](#)。

9.10.1. 認證

您可以在**認證**對話方塊中指定傳入和傳出郵件的認證文字和語言：



認證文字包括兩個部分，即使用者部分和系統部分 - 請參閱下面範例：第一行代表使用者部分，其餘則是自動生成：

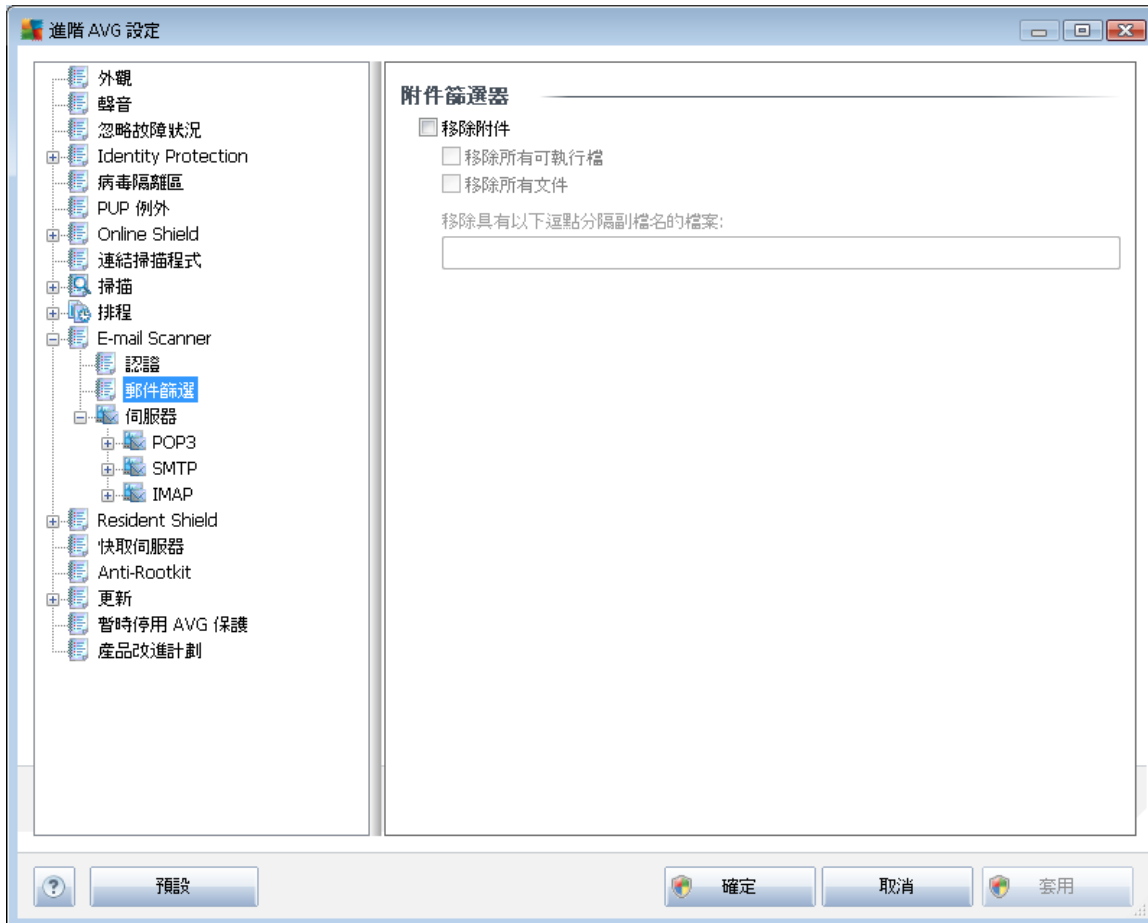
未在此訊息中找到病毒。

已透過 AVG 檢查。

版本：x.y.zz / 病毒庫：xx.y.z - 發行日期：2010年9月12日

如果您決定使用傳入或傳出電子郵件的認證，可以在此對話方塊進一步指定認證文字的使用者部分確切的用詞（**電子郵件認證文字**），並選擇認證自動生成的系統部分應該使用的語言（**用於電子郵件認證文字的語言**）。

9.10.2. 郵件篩選

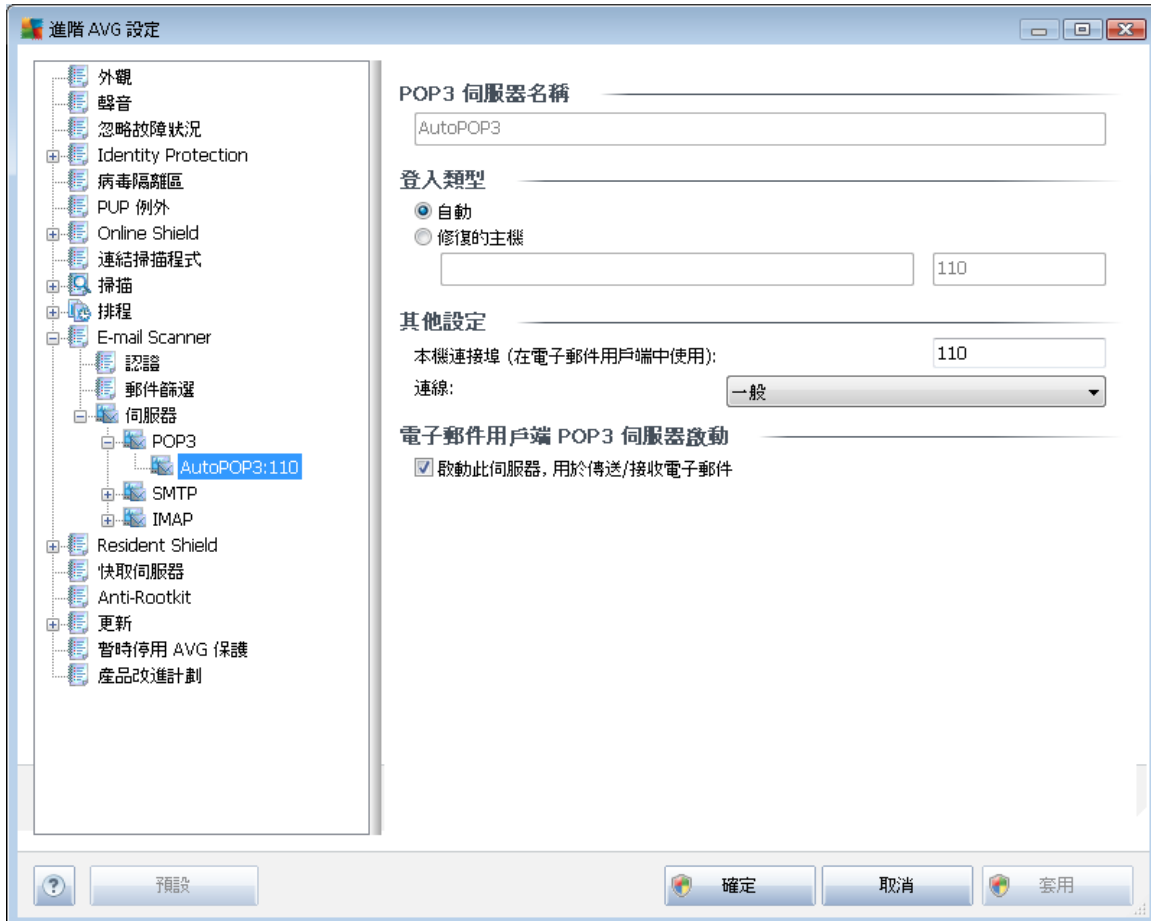


在 **附件篩選器** 對話方塊中，您可以設定用於電子郵件訊息附件掃描的參數。預設情況下，**移除附件** 選項關閉。如果您啟動它，所有偵測為受感染或潛在危險內容的電子郵件訊息附件都將被自動移除。如果要定義應移除的特定附件類型，請選取以下相應選項：

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

9.10.3. 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。

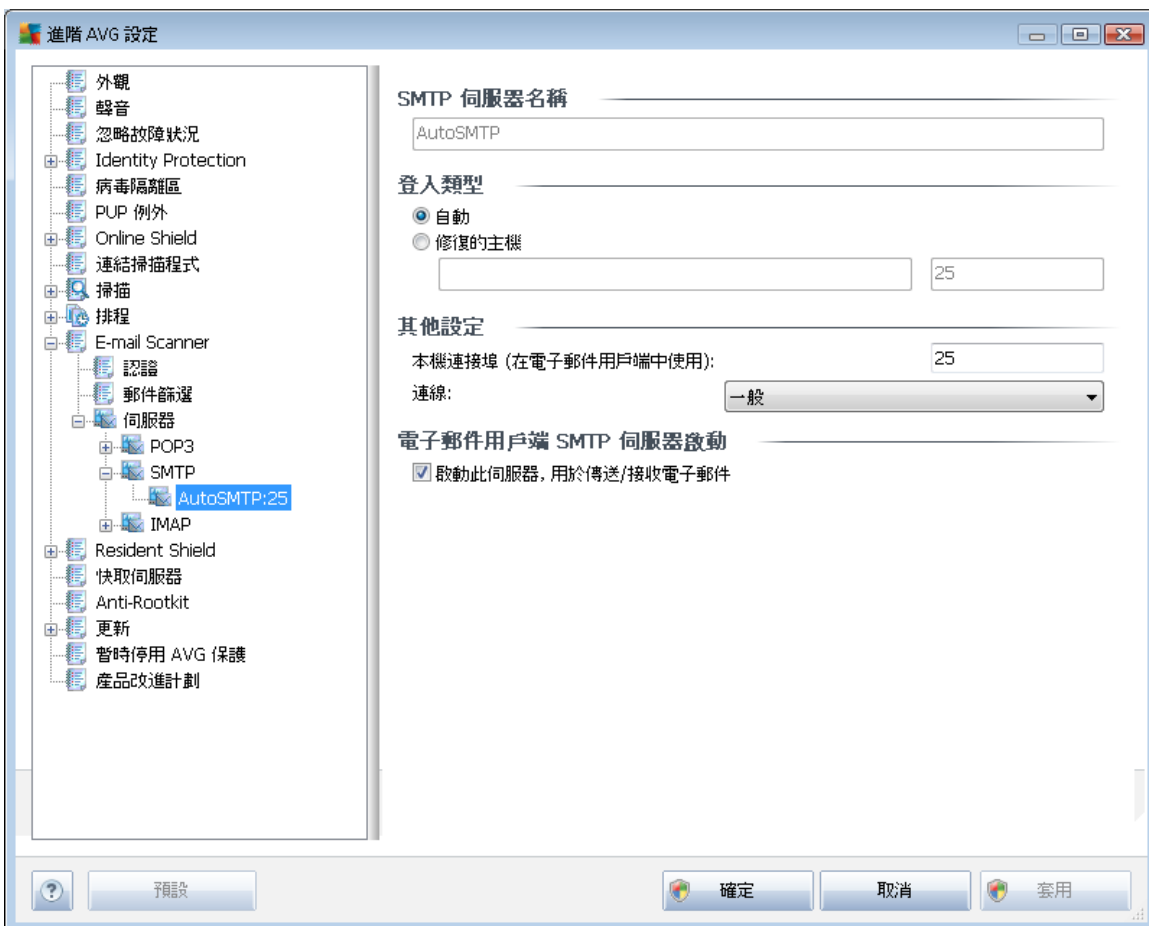


您可以在此對話方塊中 (透過 **伺服器/POP3** 開啟) 設定新的 **E-mail Scanner** 伺服器，針對傳入郵件使用 POP3 通訊協定：

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

您必須在郵件應用程式中將此連接埠指定為用於 POP3 通訊的連接埠。

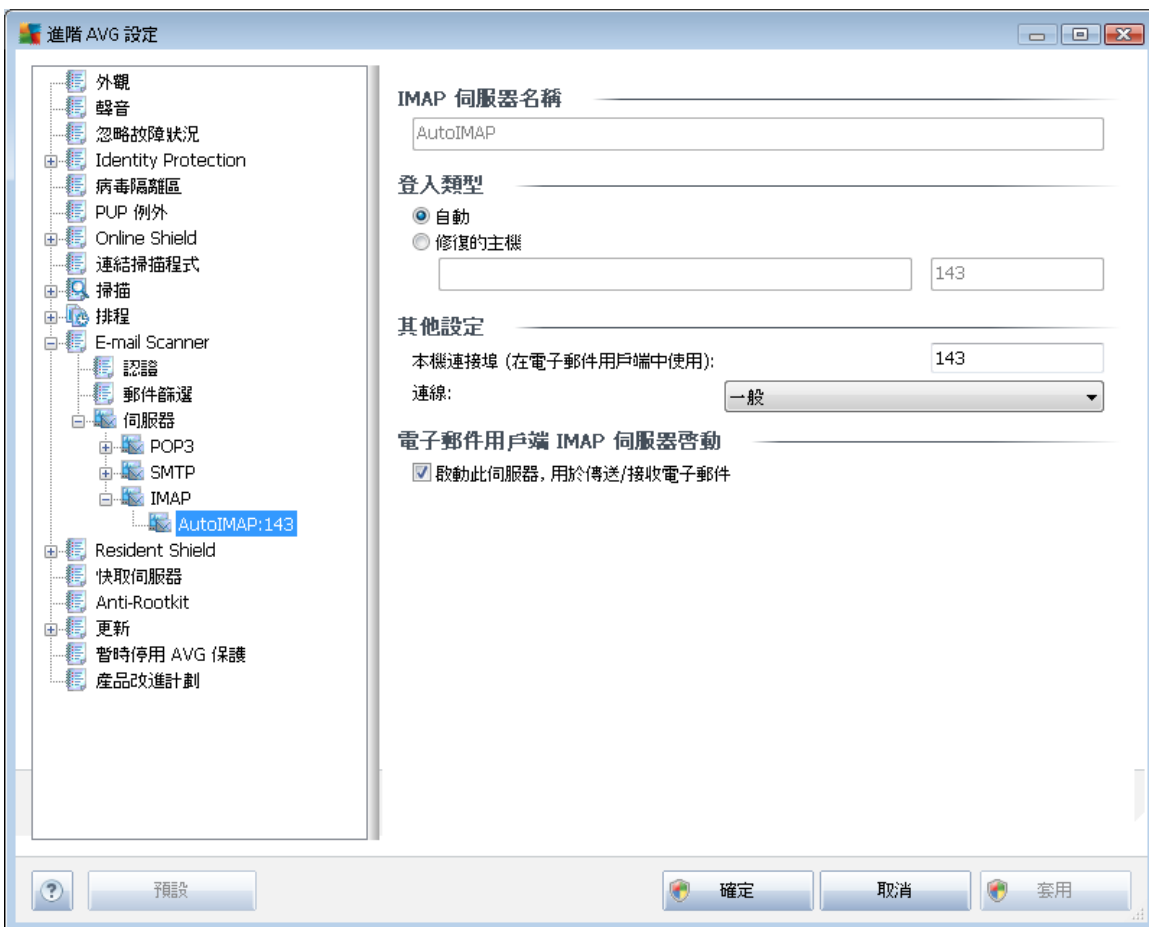
- **連線** - 您可以在下拉式功能表中指定要使用的連線方式 (一般/SSL/預設為 SSL)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能也僅在目標郵件伺服器支援時才可用。
- **電子郵件用戶端 POP3 伺服器啟動** - 核取/取消核取此項目可啟動或停用指定的 POP3 伺服器



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

- **SMTP 伺服器名稱** - 您可以在此欄位中指定新增伺服器的名稱 (若要新增 SMTP 伺服器，在左側巡覽功能表的 SMTP 項目上按一下滑鼠右鍵)。對於自動建立的 "AutoSMTP" 伺服器，會停用此欄位。
- **登入類型** - 定義確定傳入郵件所使用的郵件伺服器的方法：
 - **自動** - 根據您的電子郵件用戶端的設定自動執行登入。

- **固定主機** - 在這種情況下，程式總是會使用此處指定的伺服器。請指定您的郵件伺服器的位址或名稱。您可以使用網域名稱 (如 *smtp.acme.com*) 和 IP 位址 (如 *123.45.67.89*) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以使用冒號作為分隔符號在伺服器名稱後面鍵入連接埠 (如 *smtp.acme.com:8200*)。用於 SMTP 通訊的標準連接埠為 25。
- **其他設定** - 指定更多詳細參數：
 - **本機連接埠** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 SMTP 通訊的連接埠。
 - **連線** - 您可以在此下拉式功能表中指定要使用的連線方式 (一般/SSL/預設為 SSL)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能僅在目標郵件伺服器支援時才可用。
- **電子郵件用戶端 SMTP 伺服器啟動** - 核取/取消核取此方塊可啟動/停用上面指定的 SMTP 伺服器。

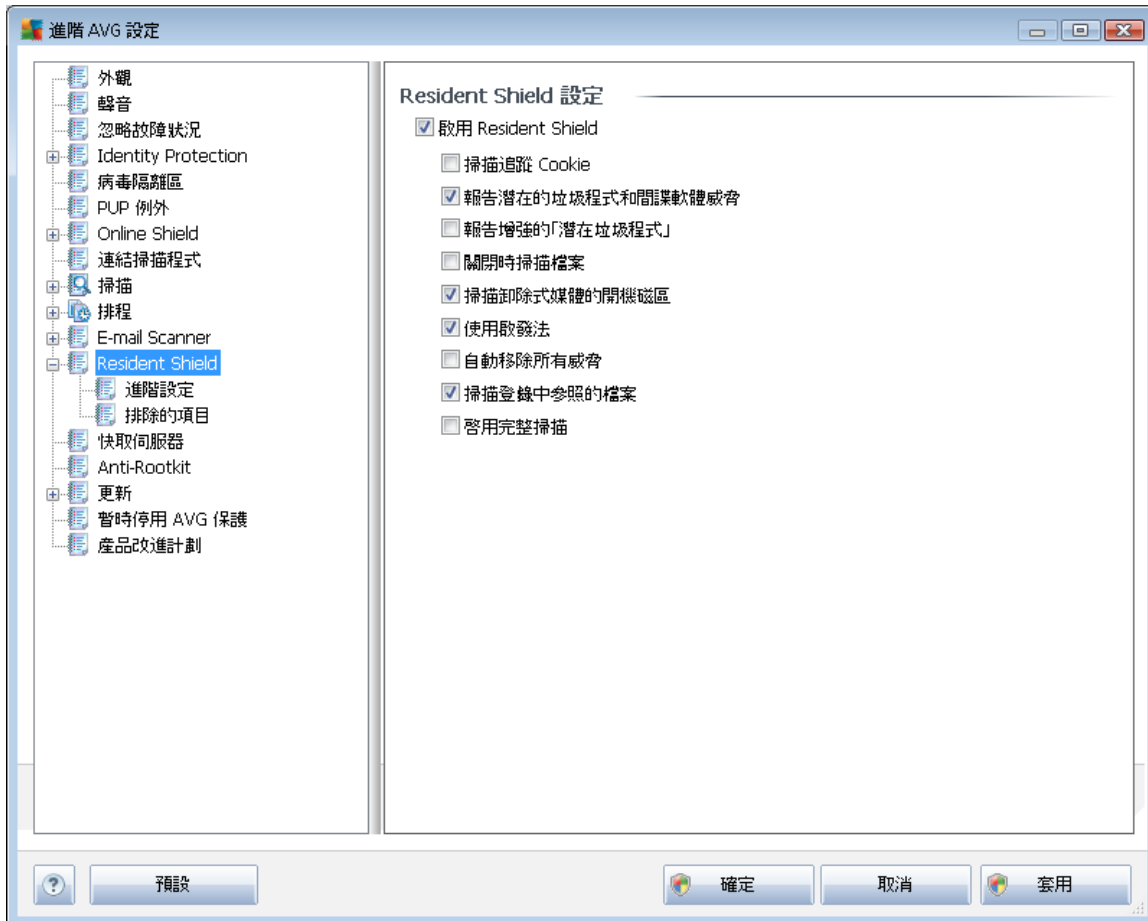


您可以在此對話方塊中 (透過 **伺服器/IMAP** 開啟) 設定新的 **E-mail Scanner** 伺服器，針對傳出郵件使用 IMAP 通訊協定：

- **IMAP 伺服器名稱** - 您可以在此欄位中指定新增的伺服器名稱 (若要新增 IMAP 伺服器，在左側巡覽功能表的 IMAP 項目上按一下滑鼠右鍵)。對於自動建立的 "AutoIMAP" 伺服器，會停用此欄位。
- **登入類型** - 定義確定傳入郵件所使用的郵件伺服器的方法：
 - **自動** - 根據您的電子郵件用戶端的設定自動執行登入。
 - **固定主機** - 在這種情況下，程式總是會使用此處指定的伺服器。請指定您的郵件伺服器的位址或名稱。您可以使用網域名稱 (如 *smtp.acme.com*) 和 IP 位址 (如 *123.45.67.89*) 作為名稱。如果郵件伺服器使用非標準連接埠，您可以使用冒號作為分隔符號在伺服器名稱後面鍵入連接埠 (例如，*imap.acme.com:8200*)。用於 IMAP 通訊的標準連接埠為 143。
- **其他設定** - 指定更多詳細參數：
 - **本機連接埠** - 指定您的郵件應用程式進行通訊預期使用的連接埠。接著，您必須在郵件應用程式中將此連接埠指定為用於 IMAP 通訊的連接埠。
 - **連線** - 您可以在此下拉式功能表中指定要使用的連線方式 (一般/SSL/預設為 SSL)。如果您選擇 SSL 連線，則傳送的資料會經過加密，而不會有被第三方追蹤或監視的風險。此功能僅在目標郵件伺服器支援時才可用。
- **電子郵件用戶端 IMAP 伺服器啟動** - 核取/取消核取此方塊可啟用/停用上面指定的 IMAP 伺服器

9.11. 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**（預設為關閉） - 此參數定義掃描期間應偵測 cookie。（HTTP cookie 用於驗證、追蹤和維護使用者的特定資訊，如站點偏好設定或電子購物車內容）
- **報告潛在的不受歡迎程式和間諜軟體威脅** - （預設為開啟）：核取此方塊可啟動 **Anti-Spyware** 引擎，並掃描間諜軟體和病毒。間諜軟體代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式是刻意安裝在電腦中的。建議您始終將此功能保持開啟狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式**（預設為關閉） - 標記此選項以偵測延伸的 **間諜軟體**：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程

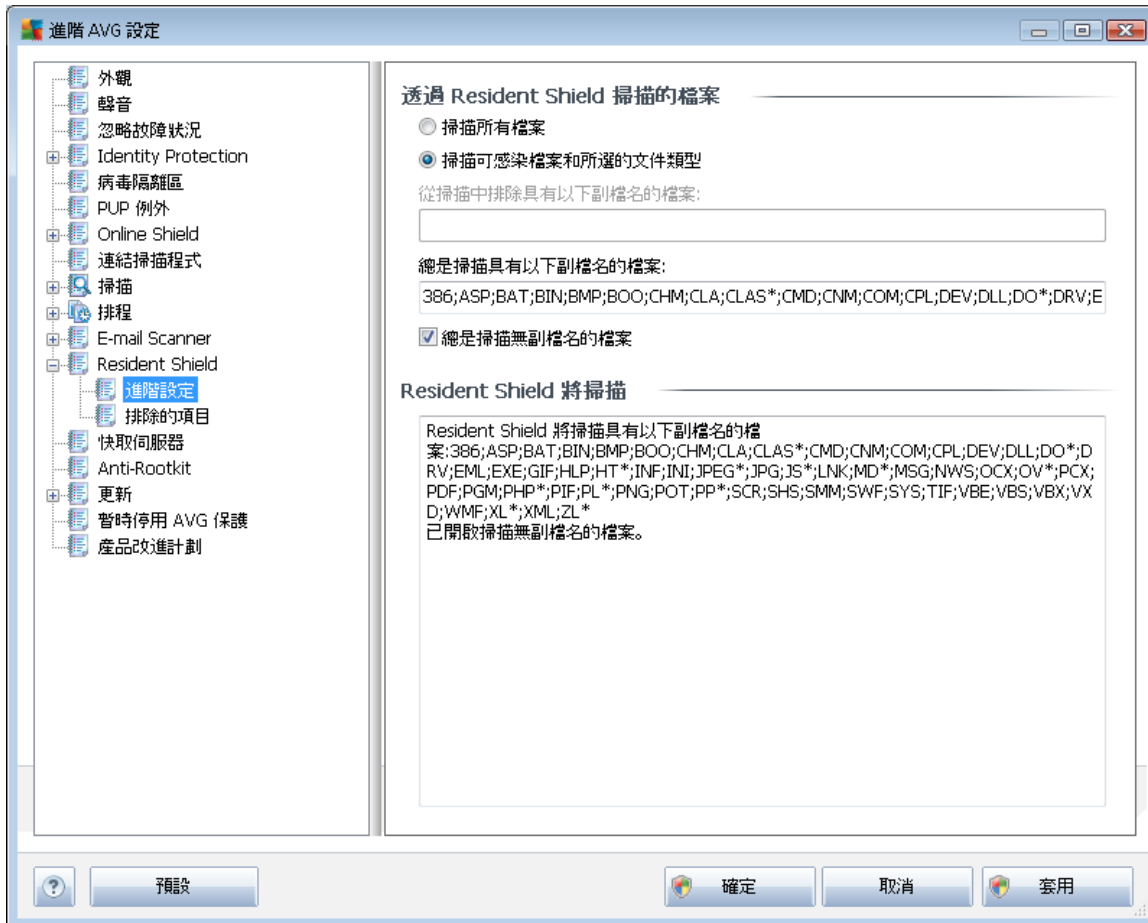


式，因此預設為關閉。

- **關閉時掃描檔案**（預設為關閉） - 關閉時掃描可確保 AVG 掃描處於開啟和關閉狀態的作用中物件（如應用程式、文件等）；此功能可幫助保護您的電腦免遭一些複雜病毒的攻擊
- **掃描卸除式媒體的開機磁區**（預設為開啟）
- **使用啟發法** - （預設為開啟） [啟發法分析](#) 將用於偵測（在虛擬電腦環境中，對掃描物件的指令進行動態模擬）
- **自動移除所有威脅**（預設為關閉） - 如果有可用的修復方法，則會自動修復任何偵測到的感染，並且會移除所有無法修復的感染檔案。
- **掃描在登錄內參照的檔案**（預設為開啟） - 此參數定義 AVG 將掃描所有新增到登錄的可執行檔案，以防在下次電腦啟動時執行已知的感染檔案。
- **啟用完整掃描**（預設為關閉） - 在特殊情況下（極為緊急的狀況），您可以核取此選項來啟動最完整的掃描演算法，這將仔細檢查所有可能的威脅物件。不過請記住，這種方法相當耗時。

9.11.1. 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）：



決定您是要掃描所有檔案，還是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。

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

9.11.2. 排除的項目



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

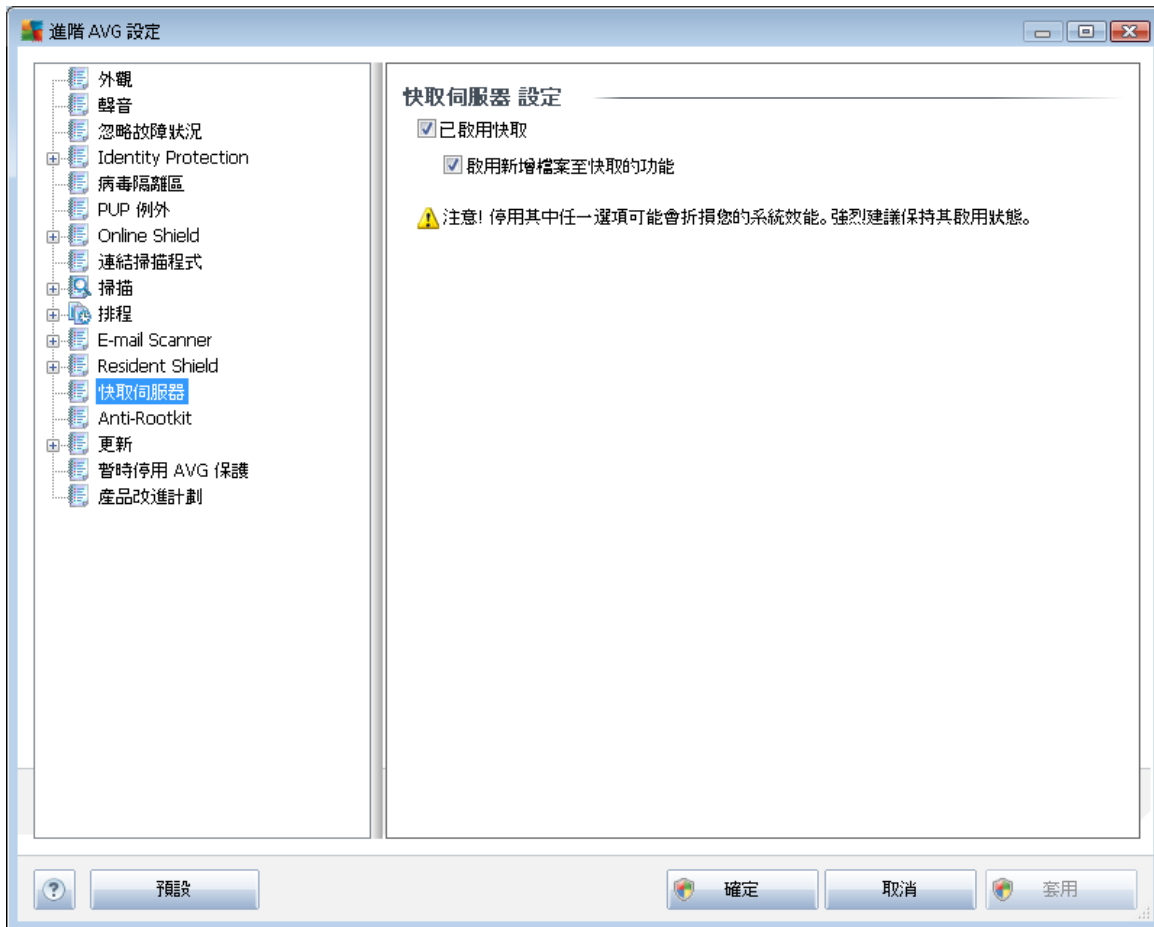
除非必要，否則我們強烈建議不要排除任何項目！

該對話方塊提供下列控制按鈕：

- **新增路徑** - 指定要從掃描排除的目錄，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄
- **新增檔案** - 指定要從掃描中排除的檔案，方法是從本機磁碟巡覽樹狀目錄逐個選取目錄
- **編輯項目** - 允許您編輯所選資料夾的指定路徑
- **移除項目** - 允許您從清單中刪除所選檔案的路徑

9.12. 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。



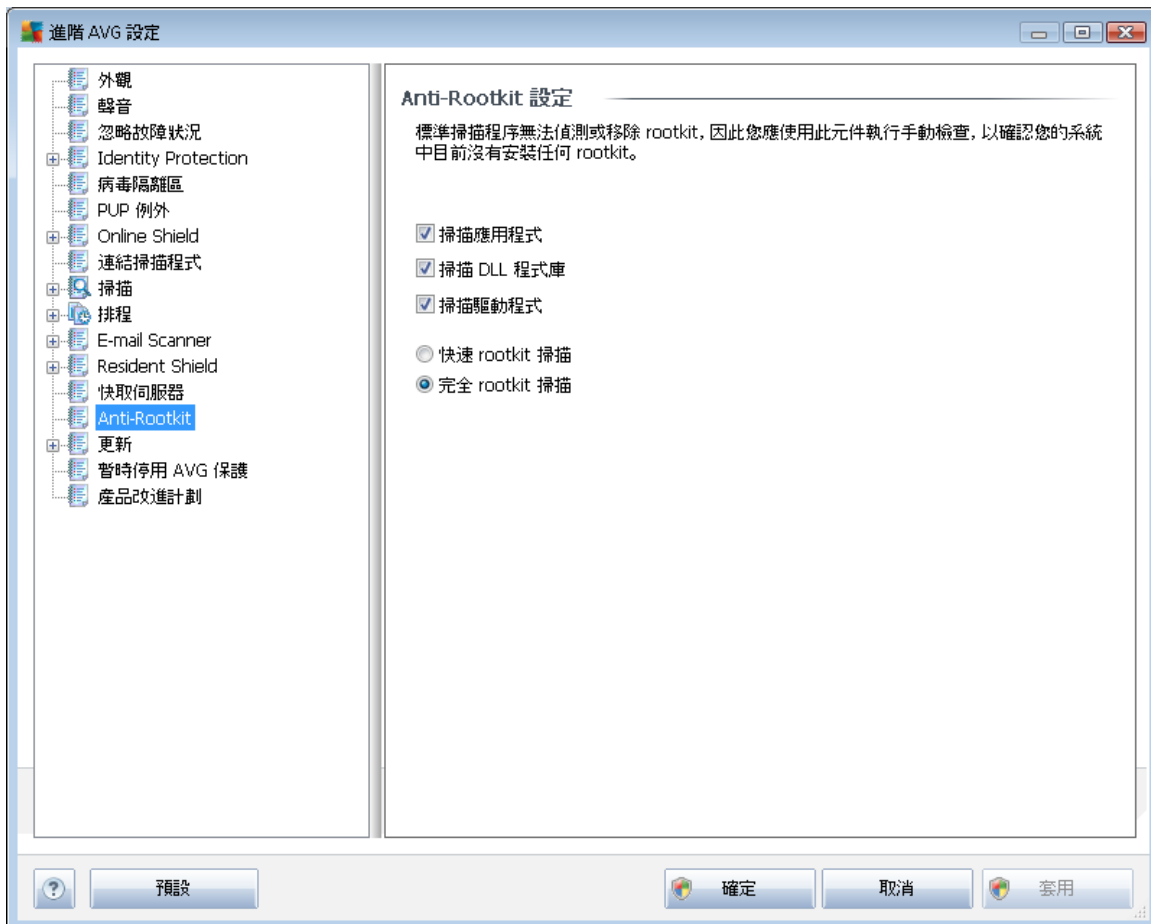
設定對話方塊提供兩個選項：

- **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。



9.13. 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：

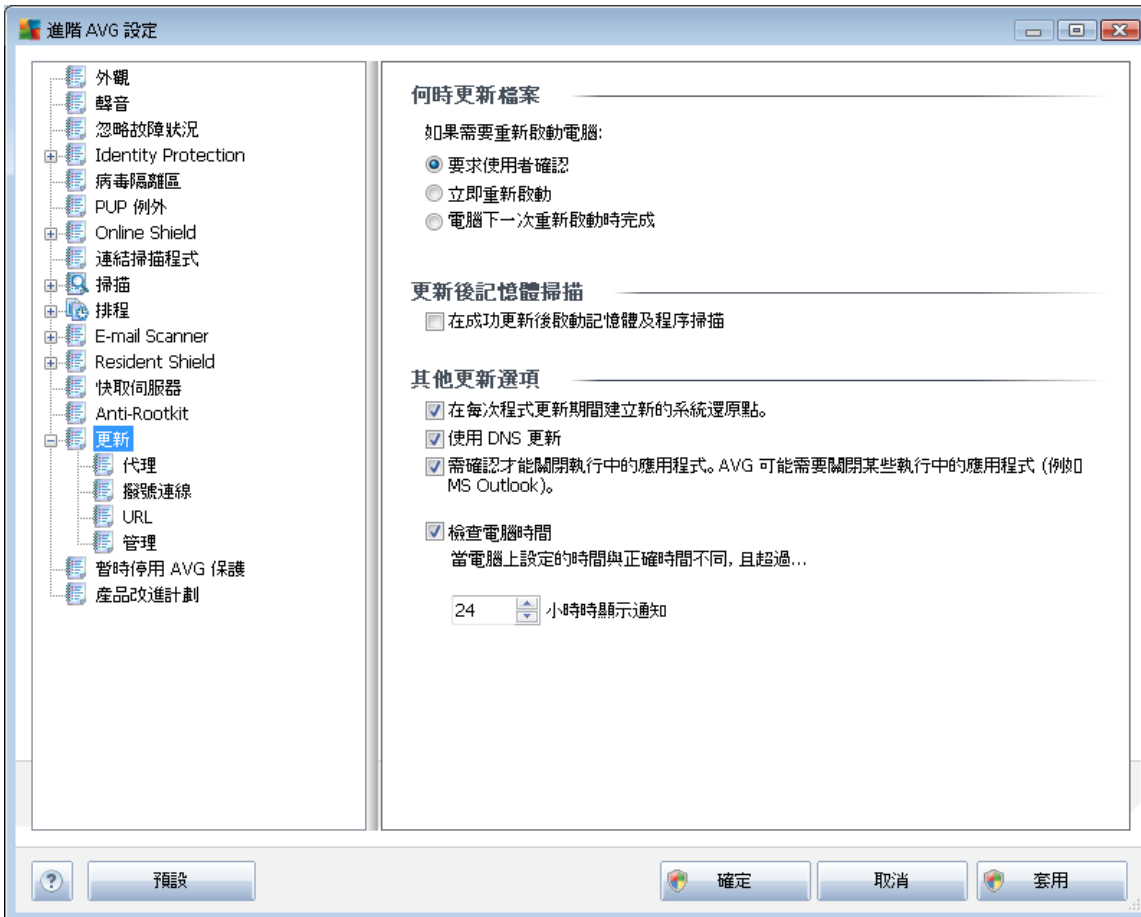
- **掃描應用程式**
- **掃描 DLL 程式庫**
- **掃描驅動程式**

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)

9.14. 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

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

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



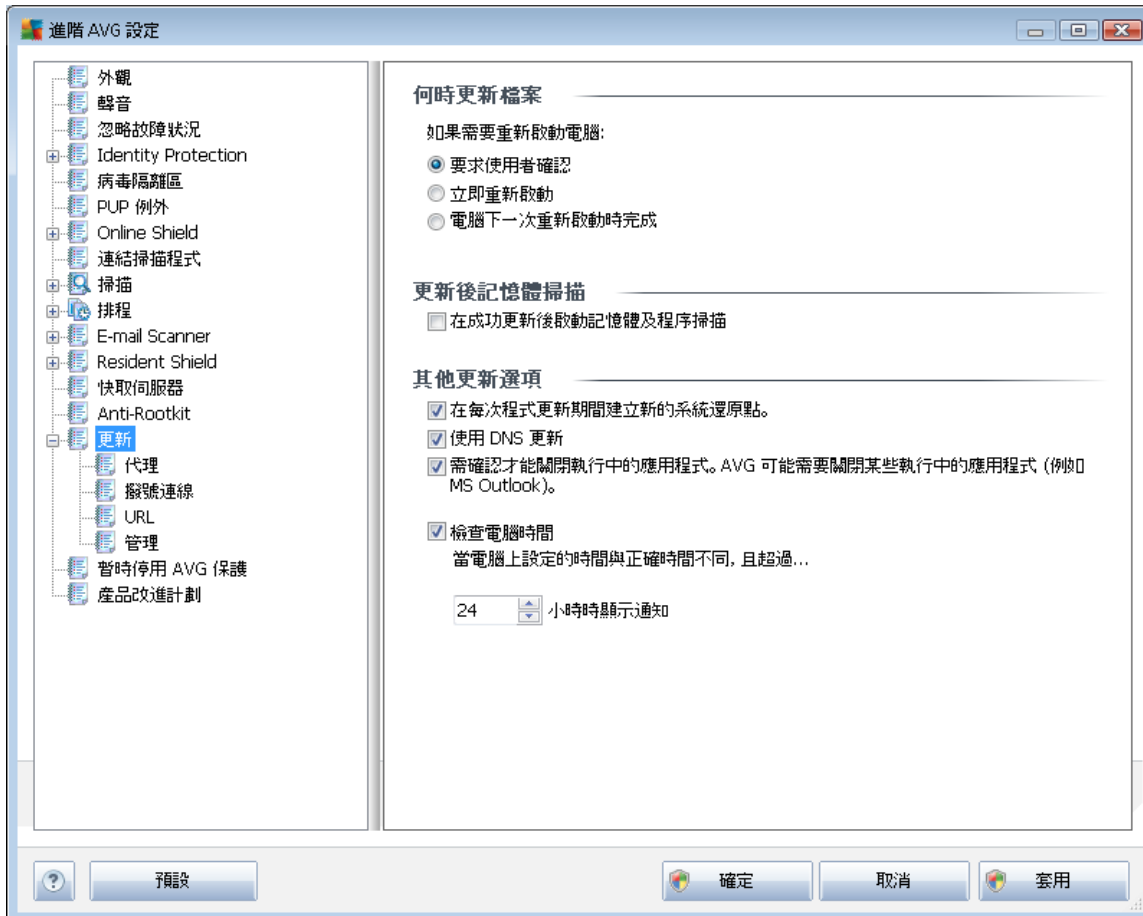
更新後記憶體掃描

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

- **在每次程式更新期間建立新的系統還原點** - 在每次啟動 AVG 程式更新之前，都會建立一個系統還原點。如果更新程序失敗，且作業系統當機，您始終可以將作業系統還原為在此還原點時的原始組態。該選項可透過「開始/所有程式/附屬應用程式/系統工具/系統還原」存取，但是，只建議經驗豐富的使用者進行變更！如果您想利用此功能，請將此核取方塊保持為勾選狀態。
- **使用 DNS 更新 (預設為開啟狀態)** - 如果勾選此項目，一旦發佈更新，您的 **AVG Anti-Virus 2011** 便會查找有關 DNS 伺服器上最新病毒庫版本和最新程式版本的資訊。然後，僅會下載和套用必不可少s的最小必要更新檔案。這樣，下載的資料總量會減至最小，更新程序會執行得更快。
- **需確認才能關閉執行中的應用程式 (預設情況下為開啟)** 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。

9.14.1. 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)

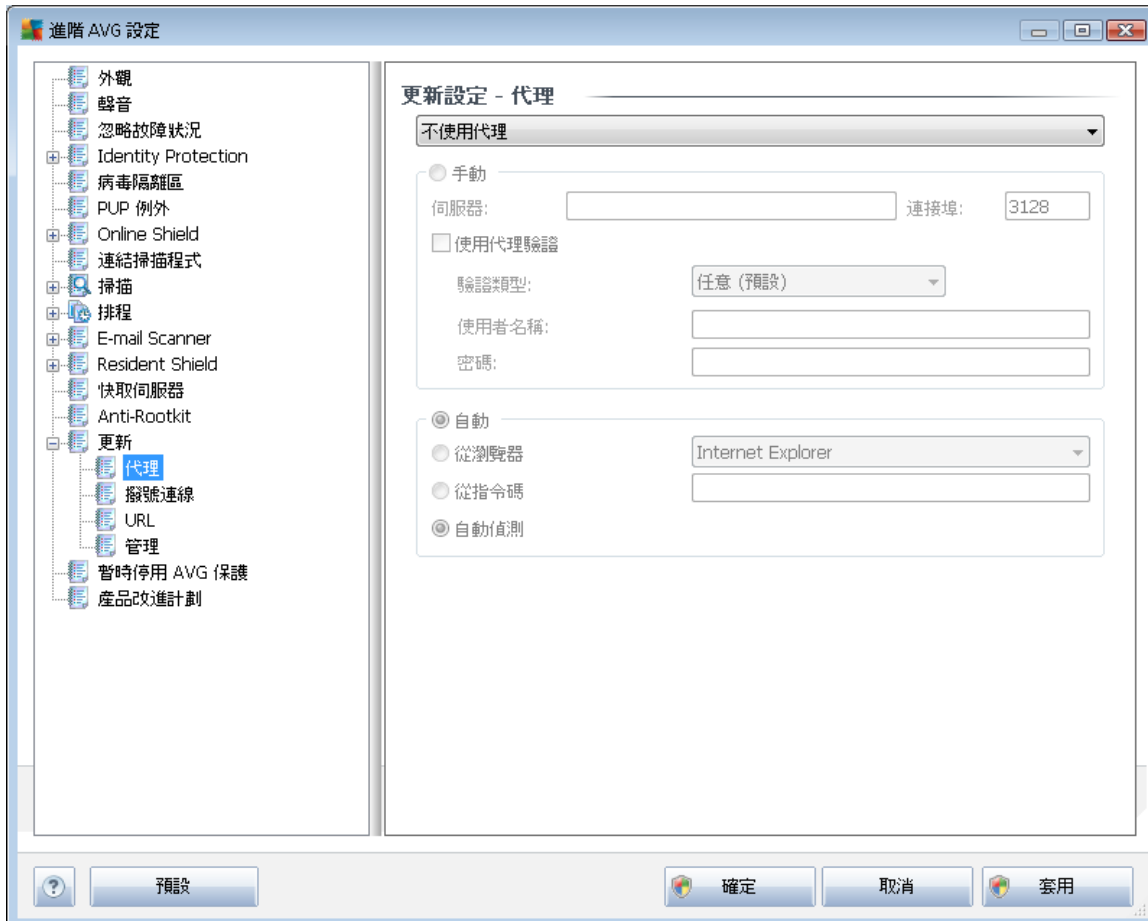
代理伺服器也為每個使用者組態了特定規則。如果您的代理伺服器是依這種方式設定的, 請核取**使用代理驗證**選項, 以驗證透過代理伺服器連線至網際網路的使用者名稱和密碼是否有效。

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

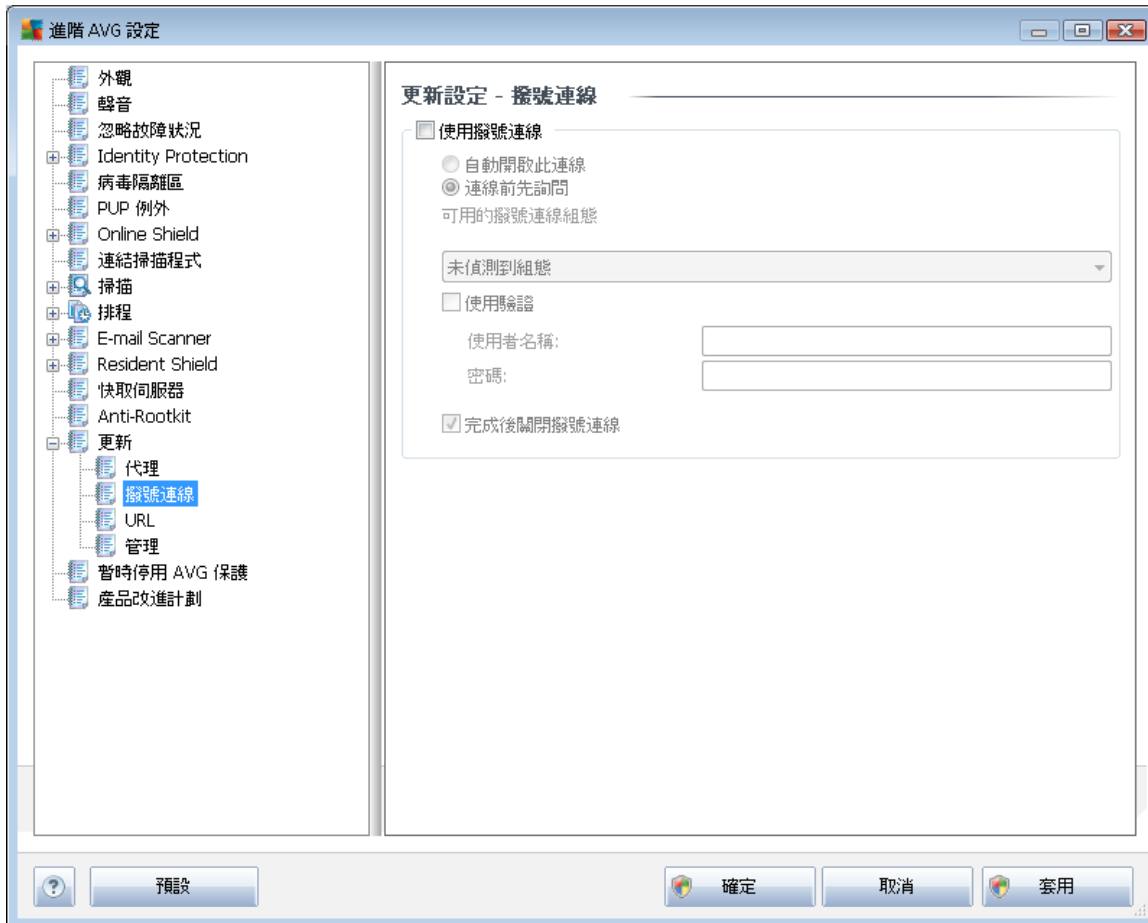
9.14.2. 撥號連線



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**)。

9.14.3. URL

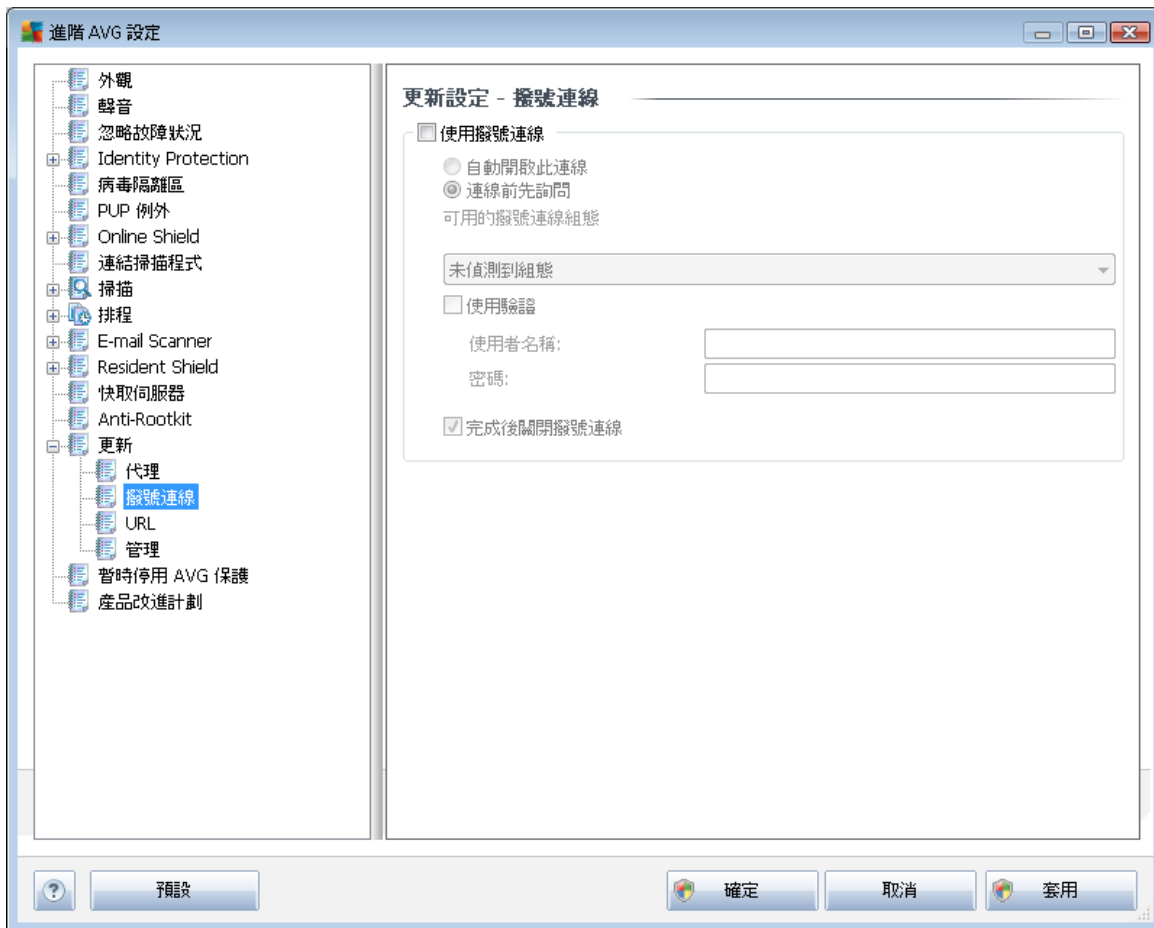


URL 對話方塊提供一份可從中下載更新檔案的網際網路位址清單。使用下列控制按鈕可修改該清單及其項目：

- **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

9.14.4. 管理

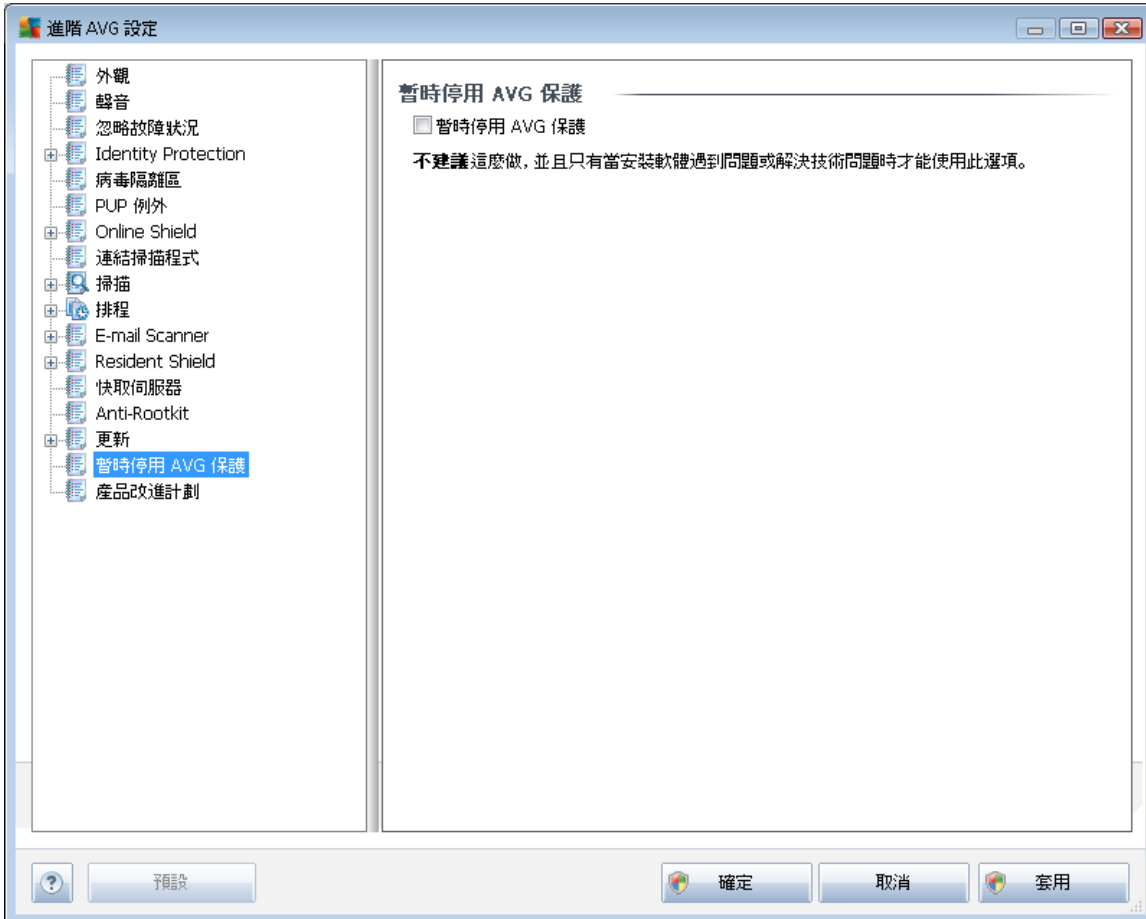
管理對話方塊提供有兩個選項，可分別透過兩個按鈕存取：



- **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)



9.15. 暫時停用 AVG 保護



在暫時停用 AVG 保護對話方塊中，您可以選擇一次關閉由 AVG Anti-Virus 2011 提供的全面性保護。

請記住，除非迫不得已，請勿使用此選項！

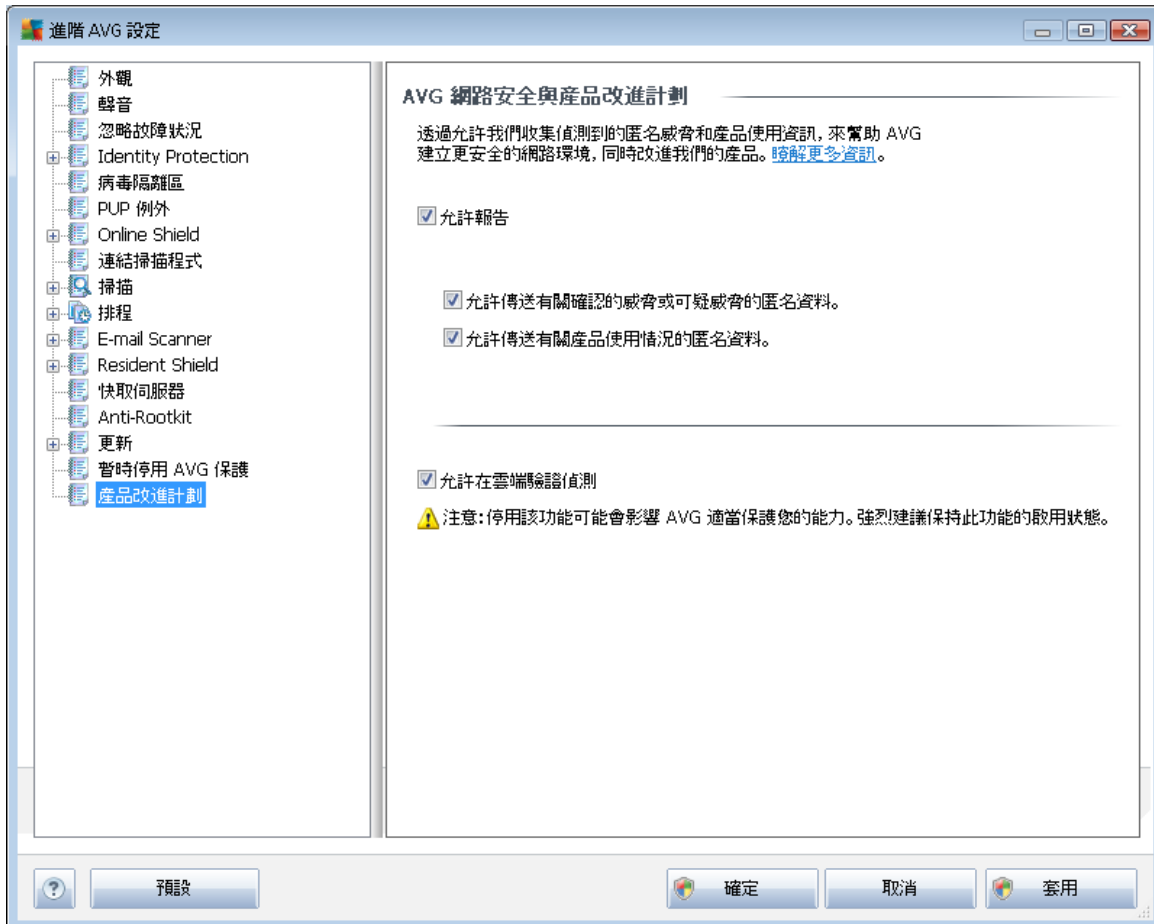
大多數情況下，安裝新的軟體前沒有必要先停用 AVG，即使安裝程式或軟體精靈建議應先關閉正在執行的程式和應用程式以確保安裝程序期間不會出現意外中斷也一樣。如果您真的在安裝期間遇到問題，可試著先停用 **Resident Shield** 元件。如果您必須暫時停用 AVG，應該在安裝完成後盡速重新啟用它。如果您在反病毒軟體停用時連線至網際網路或網路，您的電腦可能很容易受到攻擊。

9.16. 產品改進計劃

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

系統會自動處理這些報告，因此不會給您帶來任何不便，並且報告中不會包含任何個人資料。報告偵測到的威脅為選用選項，但是我們建議您也開啟這個功能，因為它有

助於我們改進對您及其他 AVG 使用者的保護。



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

- **病毒是會自我複製和傳播的惡意代碼，通常只在造成損壞後才被發現。**有些病毒是嚴重威脅，它會刪除或按其自己的方式故意變更檔案，而有些病毒則執行一些看起來無害的動作，如播放一段音樂。但是，由於其基本的複製能力，所有病毒都是危險的，即使是一個簡單的病毒也可以瞬間佔用所有電腦記憶體並導致電腦崩潰。
- **蠕蟲是病毒的一個子類別，它和一般病毒不同，無需附加到「載體」物件；它可以獨立將自身傳送至其他電腦，通常是透過電子郵件，結果導致電子郵件伺服器 and 網路系統過度負載。**
- **間諜軟體通常被定義為惡意軟體類別 (惡意軟體 = 任何惡意軟體，包括病毒) 內含程式 - 通常為特洛伊木馬 - 目的是盜用個人資訊、密碼、信用卡號，或潛入電腦並允許攻擊者進行遠端控制；當然這些動作都是在電腦所有者不知情或未經其同意的情況下執行的。**



- **潛在的不受歡迎程式**是一種間諜軟體，但並不一定會危害您的電腦。PUP 的具體例子有廣告軟體，它是設計用於散佈廣告的軟體，通常透過廣告快顯視窗的方式顯示；令人煩惱但並非真正有害。
- **追蹤 cookie** 也可視為一種間諜軟體，因為這些儲存在網頁瀏覽器中並會在您下次訪問時自動傳送到「上層」網站的小檔案可能包含諸如瀏覽歷程記錄及其他類似資訊等資料。
- **惡意入侵程式**是一種利用作業系統、網際網路瀏覽器或其他必要程式之漏洞或弱點的惡意代碼。
- **網路釣魚**是藉由冒充值得信任和知名的組織，進行取得個人機密資料的嘗試。潛在受害者通常會收到一封批量電子郵件，要求其更新銀行帳戶詳細資訊等。為了達到此目的，該電子郵件會邀請收件人進入某個連結，而該連結會將其引導至假的銀行網站。
- **惡作劇**是一種包含危險、警報或騷擾和無用資訊的批量電子郵件。上述威脅中有許多威脅均使用惡作劇電子郵件訊息傳播。
- **惡意網站**是故意在您的電腦上安裝惡意軟體的一類網站，受駭客入侵的網站也是如此，只是這些網站是被入侵後導致訪問者感染的合法網站。

為了保護您免受這些不同類型威脅的侵害，AVG 包含了以下專用元件：

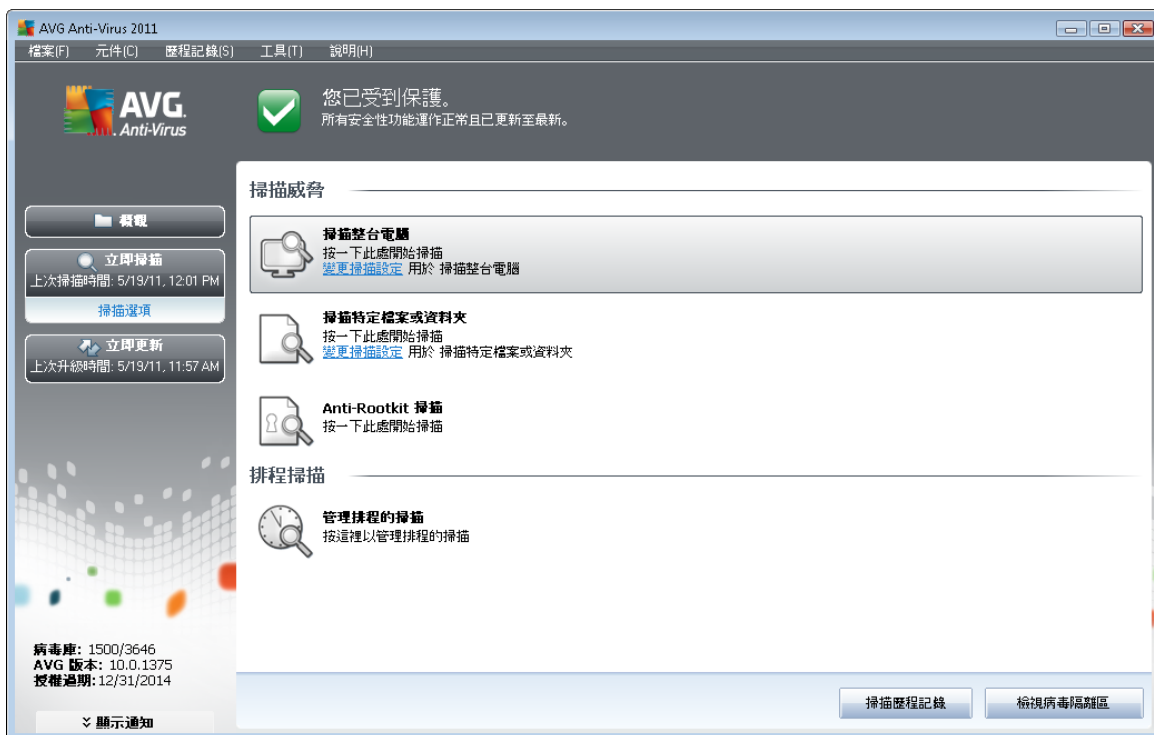
- **[Anti-Virus](#)** 保護電腦免遭病毒攻擊
- **[Anti-Spyware](#)** 保護電腦免遭間諜軟體攻擊
- **[Online Shield](#)** 可保護您的線上作業同時免遭病毒和間諜軟體的侵擾。
- **[LinkScanner](#)** 保護您免遭本章中提到的其他線上威脅的攻擊



10. AVG 掃描

掃描是 AVG Anti-Virus 2011 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](#)。

10.1. 掃描介面



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

- [預定義掃描](#) 的概觀 - 軟體廠商定義了三種掃描，可按需或按排程立即使用：
 - [完整電腦掃描](#)
 - [掃描特定檔案或資料夾](#)
 - [Anti-Rootkit 掃描](#)
- [掃描排程](#) 區段 - 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

10.2. 預定義的掃描

AVG Anti-Virus 2011 的主要特色之一就是按需求掃描。按需求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。

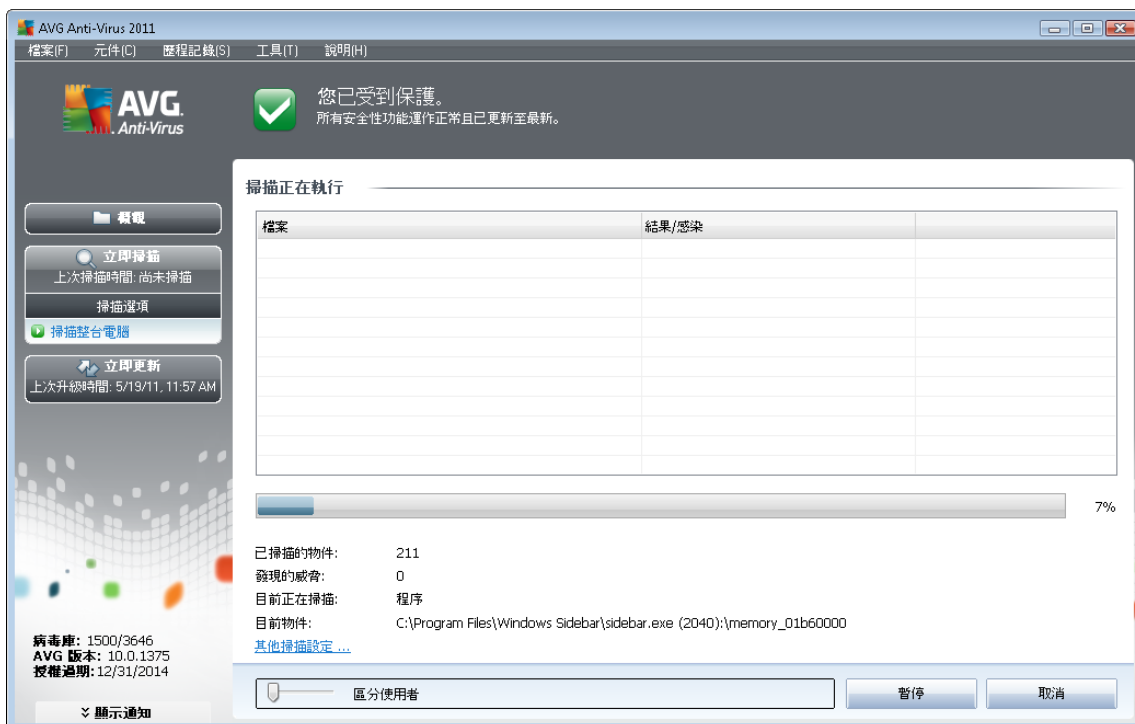
在 AVG Anti-Virus 2011 中，您將看到以下軟體廠商預先定義的掃描類型：

10.2.1. 完整電腦掃描

完整電腦掃描 - 掃描您的整台電腦，檢查是否有可能的感染和/或潛在的不受歡迎程式。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

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

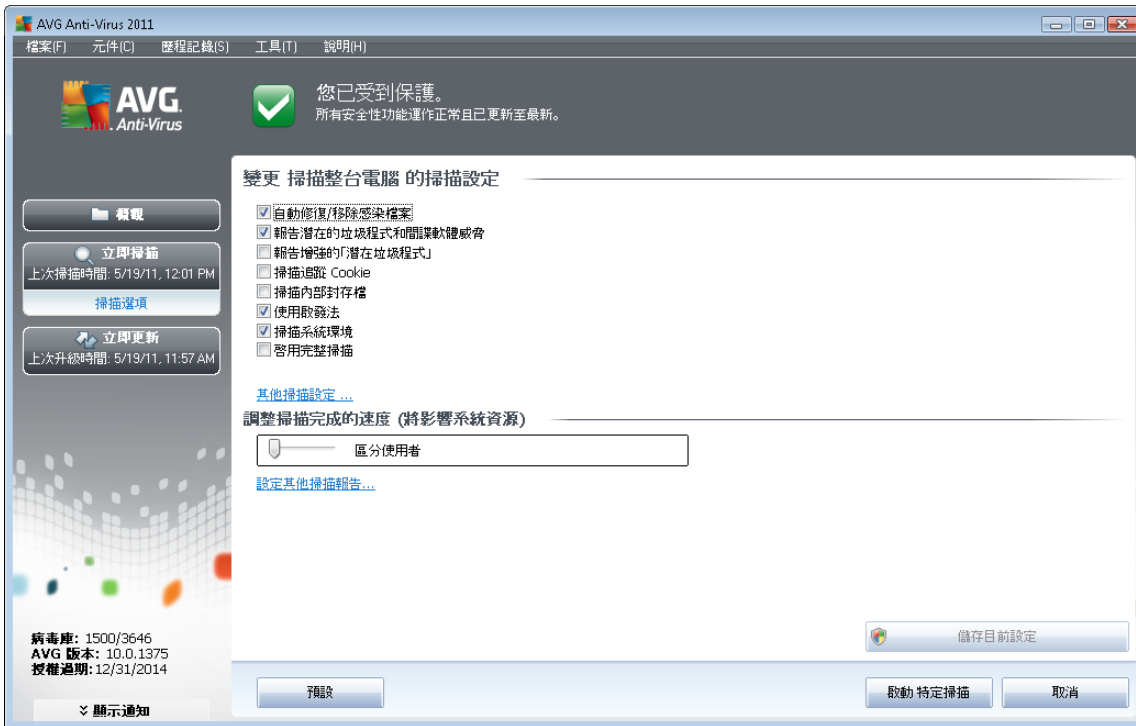


掃描組態編輯

您可以選擇編輯 **完整電腦掃描** 預先定義的預設設定。按一下 **變更掃描設定** 連結可前往

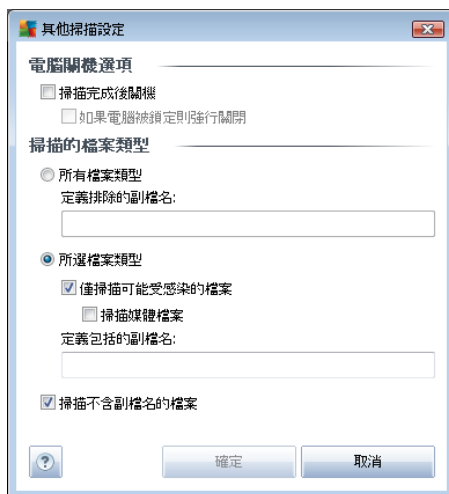


變更完整電腦掃描的掃描設定對話方塊 (可透過完整電腦掃描的「變更掃描設定」連結從掃描介面存取)。建議保留預設設定，除非您確實需要變更！



- **掃描參數** - 您可以在掃描參數清單中視需要開啟/關閉特定參數：
 - **自動修復/移除感染檔案** (預設為開啟) - 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至 **病毒隔離區**。
 - **報告潛在的不受歡迎程式和間諜軟體威脅** (預設為開啟) - 核取此方塊可啟動 **Anti-Spyware** 引擎，並掃描間諜軟體和病毒。**間諜軟體** 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
 - **報告增強的潛在不受歡迎程式集** (預設為關閉) - 標記此選項來偵測延伸的 **間諜軟體** 套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
 - **掃描追蹤 Cookie** (預設為關閉) - **Anti-Spyware** 元件的此一參數定在掃描期間應偵測 cookie；(HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容)。
 - **掃描封存內部** (預設為關閉) - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在封存內，如 ZIP、RAR...

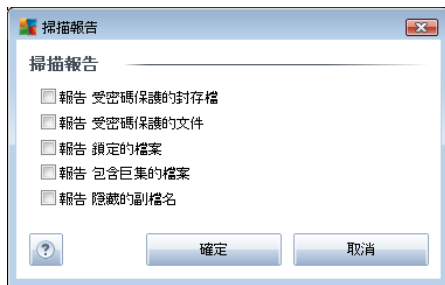
- **使用啟發法 (預設為開啟)** - 啟發法分析 (在虛擬電腦環境中動態模擬掃描物件的指令) 將成為掃描過程中用於偵測病毒的方法之一。
 - **掃描系統環境 (預設為開啟)** - 掃描時還會檢查您電腦的系統區域。
 - **啟用完整掃描 (預設為關閉)** - 在特定情況下 (懷疑您的電腦受到感染), 您可以核取此選項來啟動最完整的掃描演算法, 這甚至會掃描幾乎不會被感染的電腦區域, 以防萬一。不過請記住, 這種方法相當耗時。
- **其他掃描設定** - 此連結會開啟新的**其他掃描設定**對話方塊, 讓您指定下列參數:



- **電腦關機選項** - 決定在執行完掃描程序後電腦是否應自動關機。確認此選項後 (**掃描完成後關機**), 將啟動一個新選項, 可用來設定電腦即使在鎖定狀態下也能關機 (**強行關閉鎖定的電腦**)。
- **定義要掃描的檔案類型** - 您應該進一步決定是否要掃描:
 - **所有檔案類型** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名), 可定義掃描的例外;
 - **所選檔案類型** - 您可以指定您只想要掃描可能受感染的檔案 (將不掃描不會被感染的檔案, 例如一些純文字檔或其他一些非可執行檔), 包括媒體檔案 (視訊、音訊檔案 - 若保持取消核取此方塊, 將可進一步縮減掃描時間, 因為這些檔案通常都很大, 而且不太可能被病毒感染)。同樣地, 您可以依副檔名指定始終都應該掃描的檔案。
 - 或者, 您也可以決定**掃描不含副檔名的檔案** - 此選項預設為開啟, 而且建議您保留此設定, 除非您確實有必要變更。沒有副檔名的檔案非常可疑, 始終都應該掃描。
- **調整完成掃描的速度** - 您可以使用滑桿來變更掃描程序的優先順序。預設情況下, 該選項值會設為區分使用者層級的自動資源使用量。此外, 您也可以使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。

10.2.2. 掃描特定檔案或資料夾

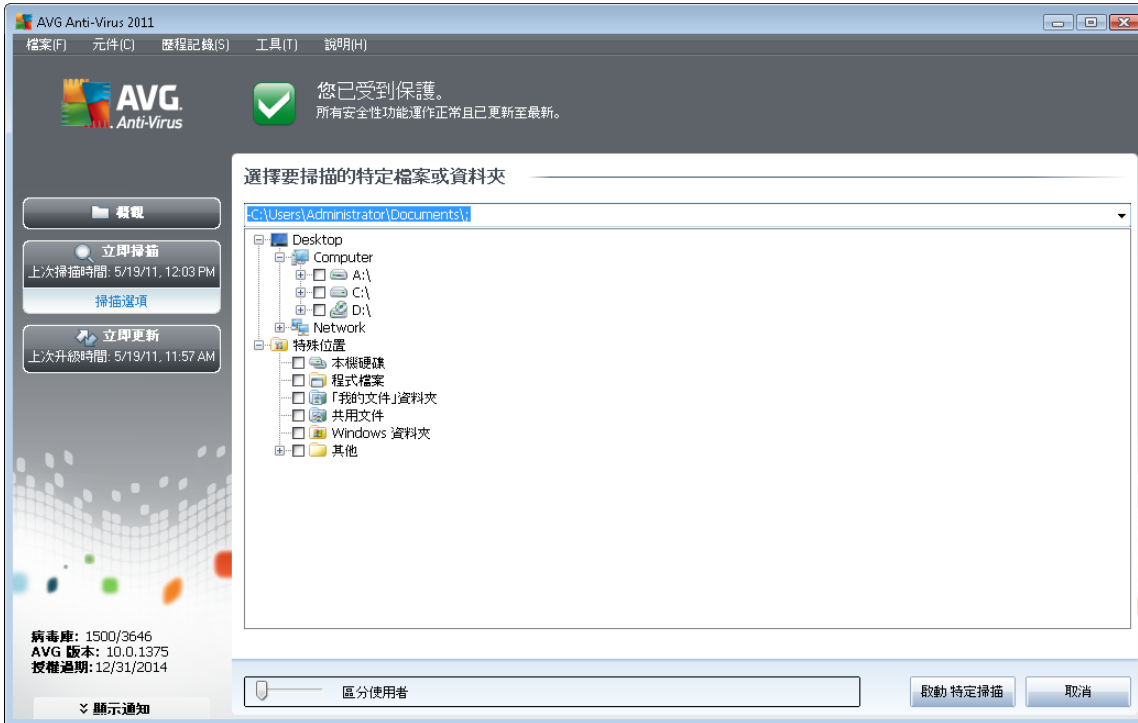
掃描特定檔案或資料夾 - 只掃描您已選取要進行掃描的電腦區域 (所選資料夾、硬碟、磁碟片、CD 等)。如果偵測到病毒並進行處置，掃描進度會與整台電腦掃描相同：發現的所有病毒都會被修復，或移至 [病毒隔離區](#)。特定檔案或資料夾掃描可供您依照自己的需求，設定自己的測試及其排程。

掃描啟動

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

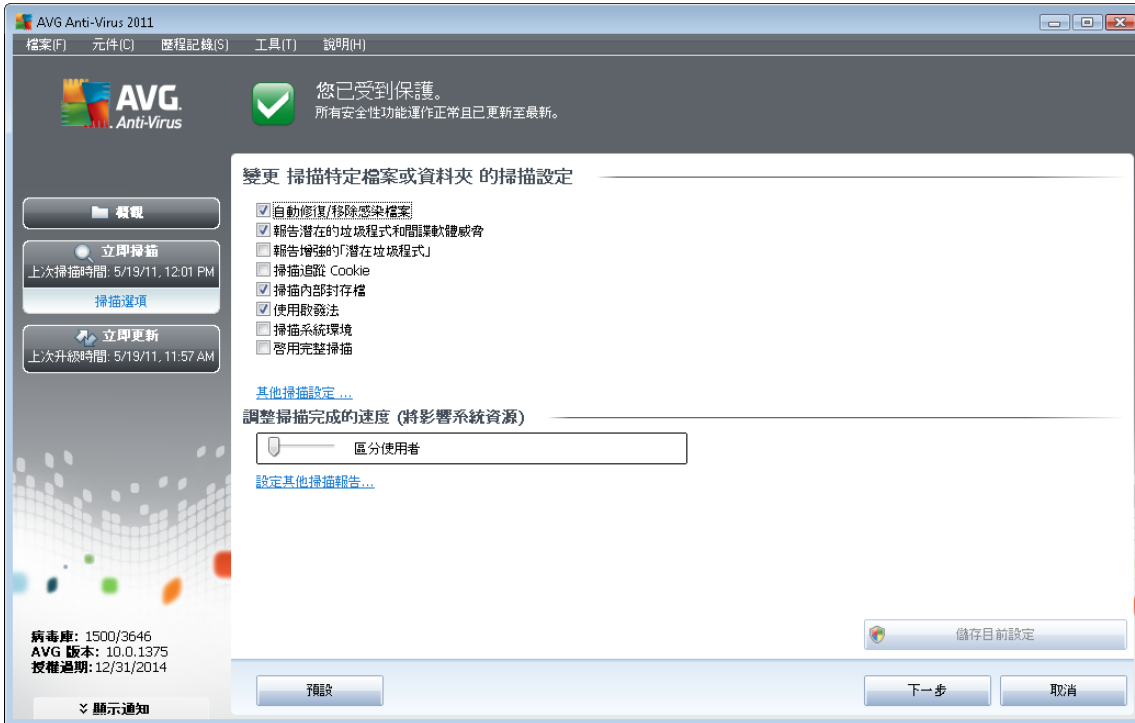
您也可以僅掃描特定資料夾，而不掃描其子資料夾。如果要這麼做，請在自動生成的路徑前方加上一個減號 "-" ([請參閱螢幕擷取畫面](#))。若要將整個資料夾排除在掃描範圍外，請使用 "!" 參數。

最後，若要啟動掃描，請按一下 **開始掃描** 按鈕；掃描程序本身基本上與 [完整電腦掃描](#) 相同。



掃描組態編輯

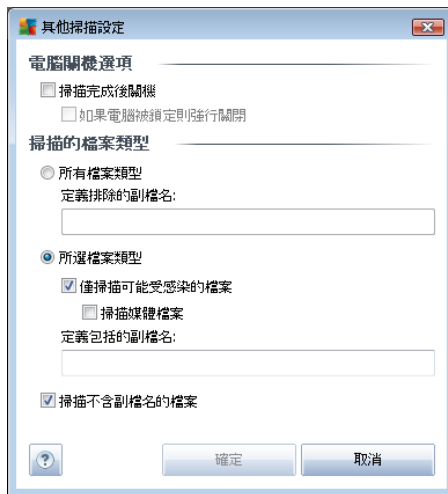
您可以選擇編輯預先定義的預設設定：**掃描特定檔案或資料夾**。請按下**變更掃描設定連結**，進入**變更掃描特定檔案或資料夾的掃描設定對話方塊**。建議保留預設設定，除非您確實需要變更！



- **掃描參數** - 您可以在掃描參數清單中視需要開啟/關閉特定參數：

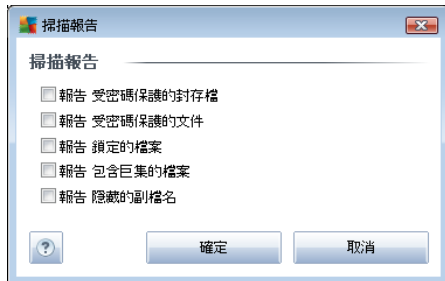
- **自動修復/移除感染檔案 (預設為開啟)** - 如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。如果受感染的檔案無法自動修復，該受感染的物件將會被移至 **病毒隔離區**。
- **報告潛在的不受歡迎程式和間諜軟體威脅 (預設為開啟)** - 核取此方塊可啟動 **Anti-Spyware** 引擎，並掃描間諜軟體和病毒。**間諜軟體** 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式集 (預設為關閉)** - 標記此選項來偵測延伸的 **間諜軟體** 套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。
- **掃描追蹤 Cookie (預設為關閉)** - **Anti-Spyware** 元件的此一參數定義在掃描期間應偵測 cookie；(HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊，如網站喜好或電子購物車內容)。
- **掃描封存內部 (預設為開啟)** - 此參數定義掃描時應檢查所有檔案，即使這些檔案已封裝在某種封存內，如 ZIP、RAR...
- **使用啟發法 (預設為關閉)** - 啟發法分析 (在虛擬電腦環境中動態模擬掃描物件的指令) 將成為掃描過程中用於偵測病毒的方法之一。

- **掃描系統環境** (預設為關閉) - 掃描時還會檢查您電腦的系統區域。
- **啟用完整掃描** (預設為關閉) - 在特定情況下 (懷疑您的電腦受到感染), 您可以核取此選項來啟動最完整的掃描演算法, 這甚至會掃描幾乎不會被感染的電腦區域, 以防萬一。不過請記住, 這種方法相當耗時。
- **其他掃描設定** - 此連結會開啟新的**其他掃描設定**對話方塊, 讓您指定下列參數:



- **電腦關機選項** - 決定在執行完掃描程序後電腦是否應自動關機。確認此選項後 (**掃描完成後關機**), 將啟動一個新選項, 可設定電腦即使在鎖定狀態下也能關機 (**強行關閉鎖定的電腦**)。
- **定義要掃描的檔案類型** - 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** - 您可以使用滑桿來變更掃描程序優先順序。預設情況下, 該選項值會設為區分使用者層級的自動資源使用量。此外, 您也可以用較慢的速度執行掃描程序, 也就是讓系統資源的負載降至最低 (這在您必須使用電腦工作, 而不在意掃描進行時間多長的時候十分有用), 或是提高速度, 但會增加系統資源的需求量 (例如電腦暫時無人使用的時候)。
- **設定其他掃描報告** - 此連結會開啟新的**掃描報告**對話方塊, 您可以在這裡選取

應報告哪些類型的結果：



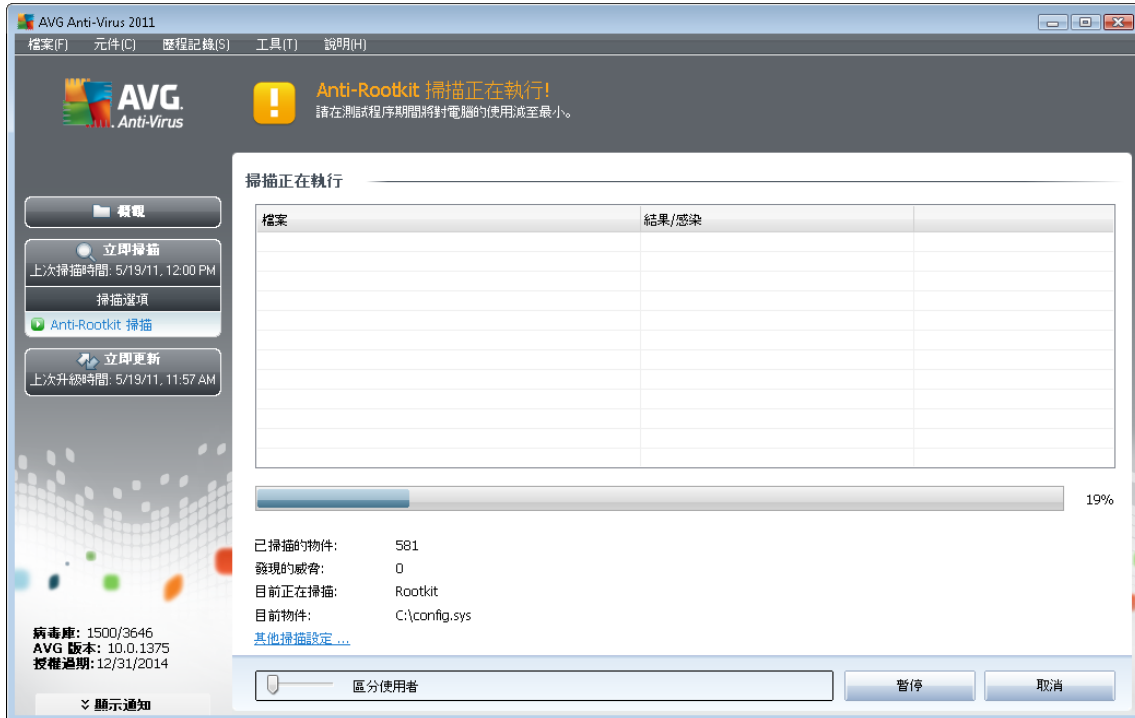
警告：這些掃描設定與新定義的掃描參數相同 - 如 [AVG 掃描/掃描排程/如何掃描](#) 章節中所述。若您決定變更掃描特定檔案或資料夾的預設組態，您隨後可將新的設定儲存為預設組態，以供未來每次掃描特定檔案或資料夾時使用。另外，該組態將會成為您所有新排程的掃描的範本 ([所有自訂的掃描都以所選檔案或資料夾的目前掃描組態為依據](#))。

10.2.3. Anti-Rootkit 掃描

Anti-Rootkit 掃描會搜尋您的電腦，以確認是否存在 rootkit (即一些可掩蓋您電腦內惡意軟體活動的程式和技術)。偵測到 rootkit 不一定表示您的電腦已受到感染。在某些情況下，特定驅動程式或正常應用程式的某些部分都可能被誤偵測為 rootkit。

掃描啟動

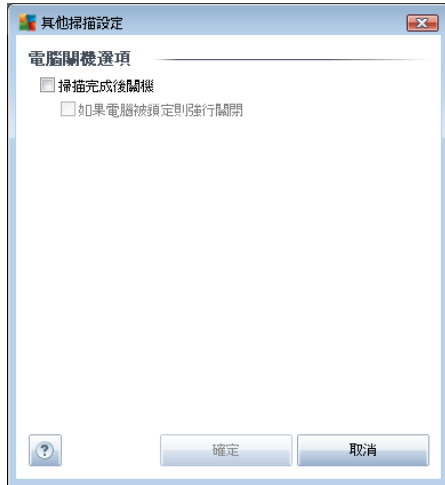
Anti-Rootkit 掃描可直接從 [掃描介面](#) 啟動，只要按一下掃描的圖示就可以了。這類掃描無需組態進一步的特定設定，掃描便會在 **掃描正在執行** 對話方塊內立即執行 (請參閱螢幕擷取畫面)。必要時，可暫時中斷 (**暫停**) 或取消 (**停止**) 掃描。



掃描組態編輯

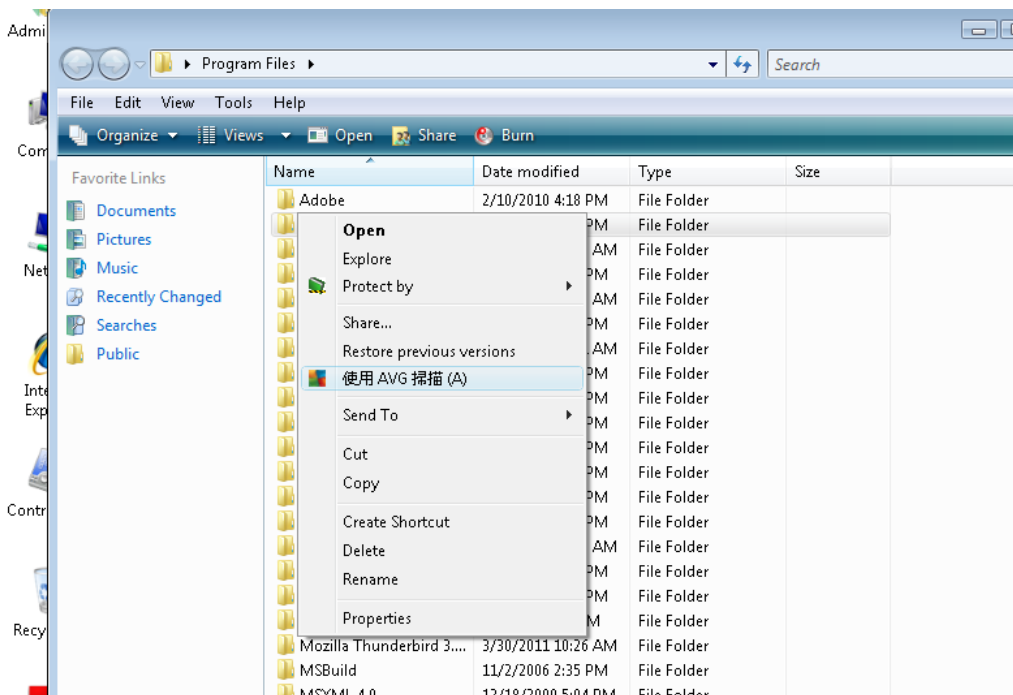
Anti-Rootkit 掃描在預設設定中永遠都處於啟動狀態，而且要編輯掃描參數，只能在 [AVG 進階設定/Anti-Rootkit](#) 對話方塊內進行。掃描介面中會提供下列組態，但只能在掃描執行中時使用：

- **自動掃描** - 您可以使用滑桿來變更掃描程序的優先順序。預設情況下，該選項值會設為區分使用者層級的自動資源使用量。此外，您也可以用較慢的速度執行掃描程序，也就是讓系統資源的負載降至最低（這在您必須使用電腦工作，而不在意掃描進行時間多長的時候十分有用），或是提高速度，但會增加系統資源的需求量（例如電腦暫時無人使用的時候）。
- **其他掃描設定** - 此連結會開啟新的 **其他掃描設定** 對話方塊，您可以在此定義與 **Anti-Rootkit 掃描** 相關的可能電腦關機條件（掃描完成後關機，可能還有強行關閉鎖定的電腦）：



10.3. 在 Windows 檔案總管中掃描

除了為整台電腦或其中選定區域而啟動的預先定義掃描之外，**AVG Anti-Virus 2011** 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，亮顯您想要檢查的檔案 (或資料夾)
- 在物件上按一下滑鼠右鍵，開啟內容功能表
- 選取 **使用 AVG 掃描** 選項，讓 AVG 掃描檔案



10.4. 命令列掃描

在 **AVG Anti-Virus 2011** 中，您可以選擇從命令列執行掃描。舉例來說，您可以在伺服器上使用此選項，或是在建立批次指令碼以便在電腦開機後自動啟動時使用。從命令列，您可以使用 AVG 圖形使用者介面提供的大部分參數來啟動掃描。

若要從命令列啟動 AVG 掃描，請在安裝 AVG 的資料夾中執行下列命令：

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

命令語法

命令語法如下：

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

掃描參數

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

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

從圖形介面啟動的 CMD 掃描

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

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



10.4.1. 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** [完整電腦掃描](#)
- **/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「[潛在的不受歡迎程式](#)」
- **/REG** 掃描登錄檔
- **/COO** 掃描 Cookie
- **/?** 顯示此主題的說明



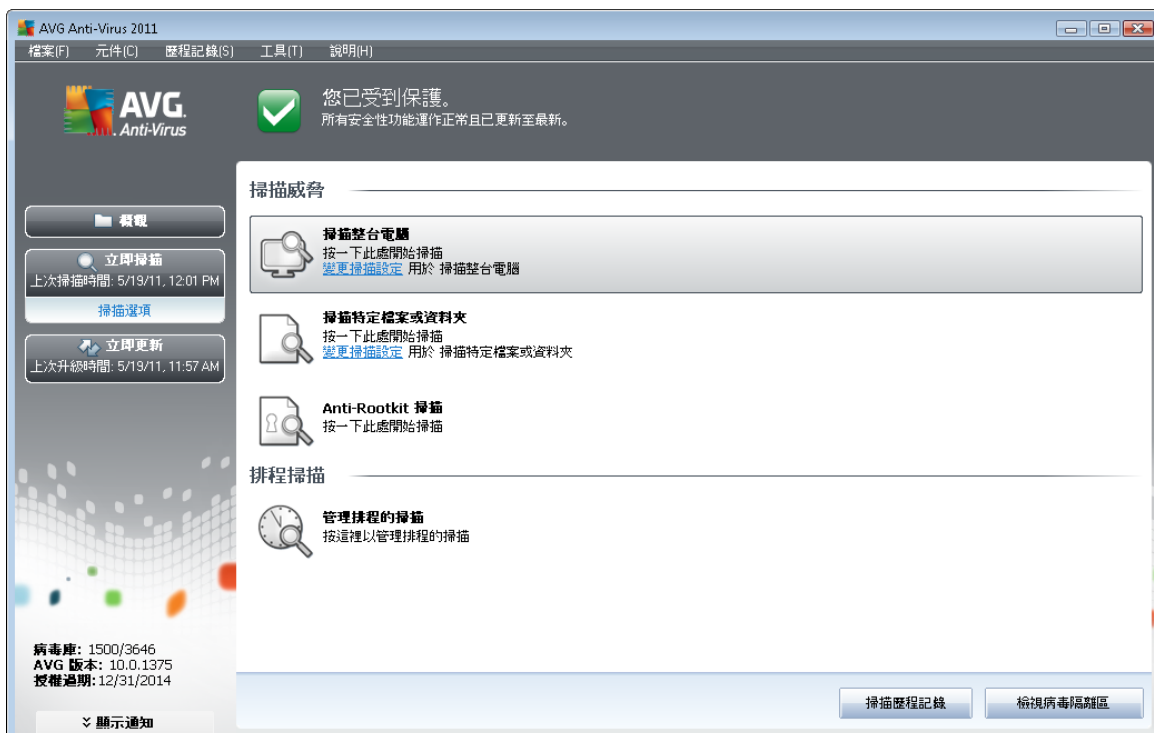
- **/HELP** 顯示此主題的說明
- **/PRIORITY** 設定掃描優先順序 / 低、自動、高 / (請參閱[進階設定 / 掃描](#))
- **/SHUTDOWN** 掃描完成後關機
- **/FORCESHUTDOWN** 掃描完成後強行關閉電腦
- **/ADS** 掃描替代資料流 (僅限 NTFS)
- **/ARCBOMBSW** 報告重新壓縮的封存檔案

10.5. 掃描排程

您可以使用 **AVG Anti-Virus 2011** 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 [完整電腦掃描](#), 至少每週一次。但是如果可能的話, 請依照掃描排程預設組態中的設定, 每天啟動一次整台電腦的掃描。如果電腦一直開啟, 您可以將掃描排定在工作時段以外的時間進行。如果電腦有時會關機, 而錯過了掃描工作的時間, [則掃描會在電腦啟動的時候執行](#)。

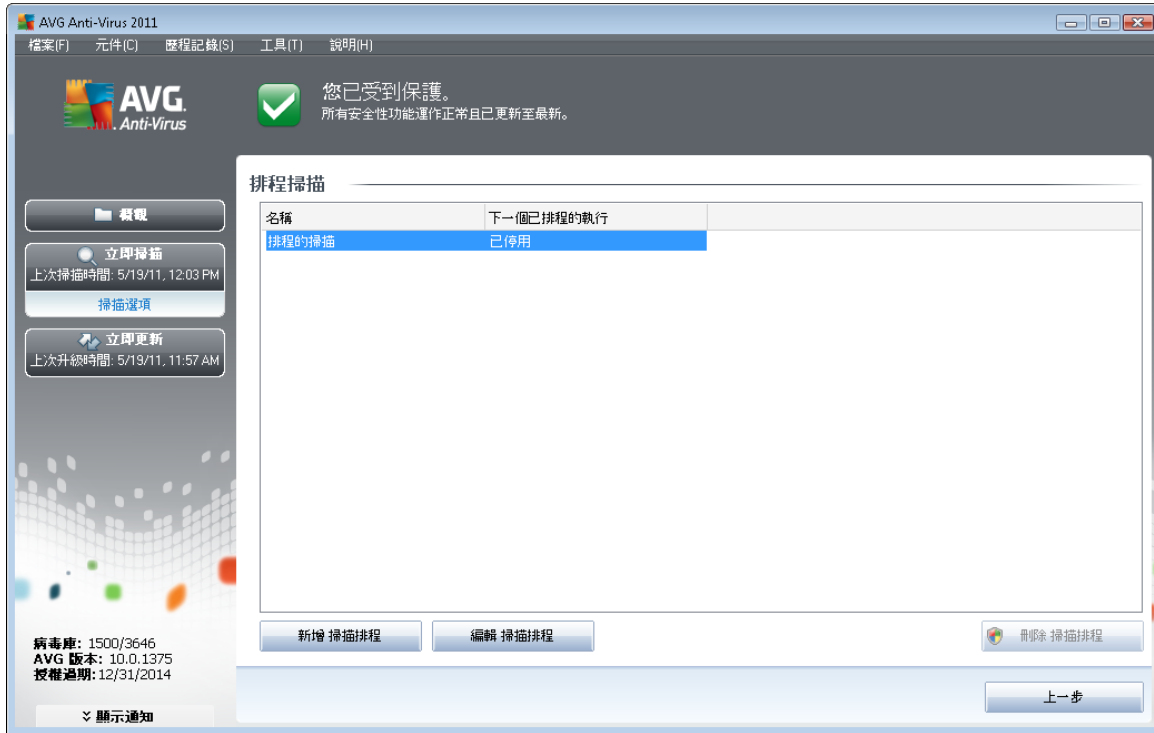
如需建立新的掃描排程, 請參閱 [AVG 掃描介面](#), 並尋找下方稱為 *排程掃描* 的區段:



排程掃描



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

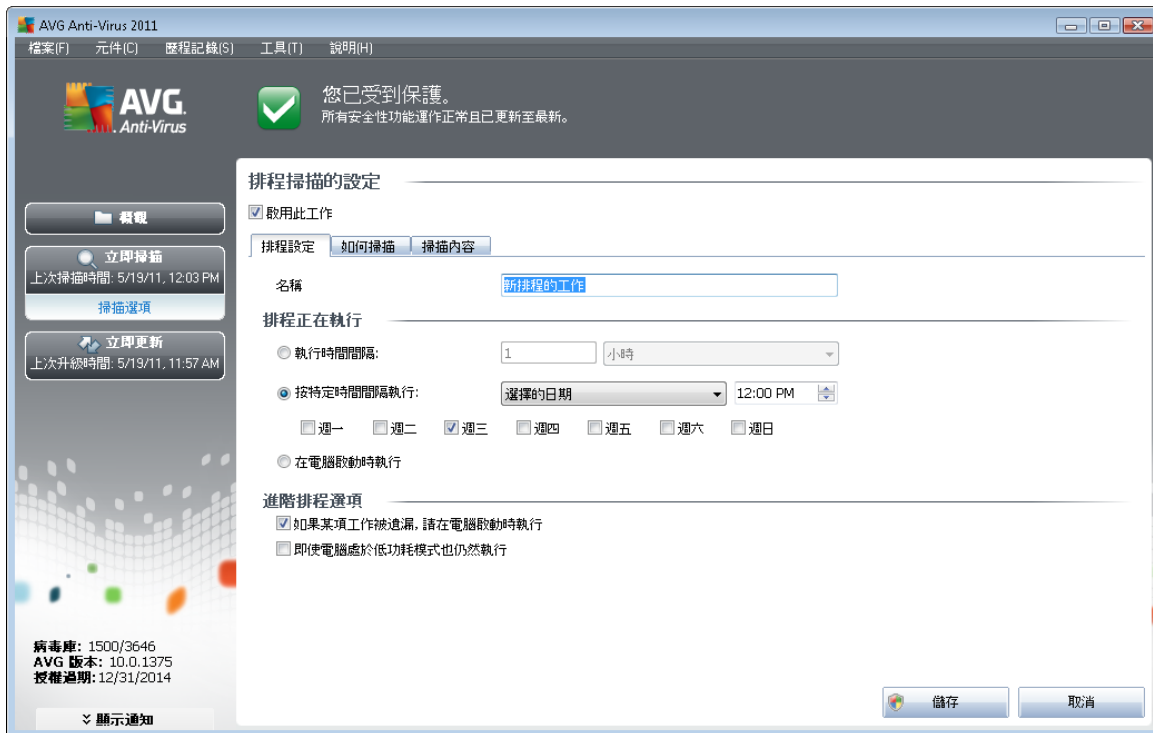


您可以使用以下控制按鈕編輯/新增掃描：

- **新增掃描排程** - 此按鈕可以開啟 **排程掃描的設定** 對話方塊、[排程設定](#) 標籤。您可以在此對話方塊中指定新定義測試的參數。
- **編輯掃描排程** - 此按鈕只有在您之前已從排程的測試清單中選取了現有的測試時才能使用。如果按鈕顯示為處於使用中，您可以按一下按鈕切換至 **排程掃描的設定** 對話方塊、[排程設定](#) 標籤。所選測試的參數已經在此指定，而且可供編輯。
- **刪除掃描排程** - 此按鈕也在您之前已從排程的測試清單中選取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](#)

10.5.1. 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。請盡量為掃描使用簡短、恰當的描述性名稱，方便日後區分此掃描與其他掃描。

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

在此對話方塊中，您可以進一步定義掃描的以下參數：

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

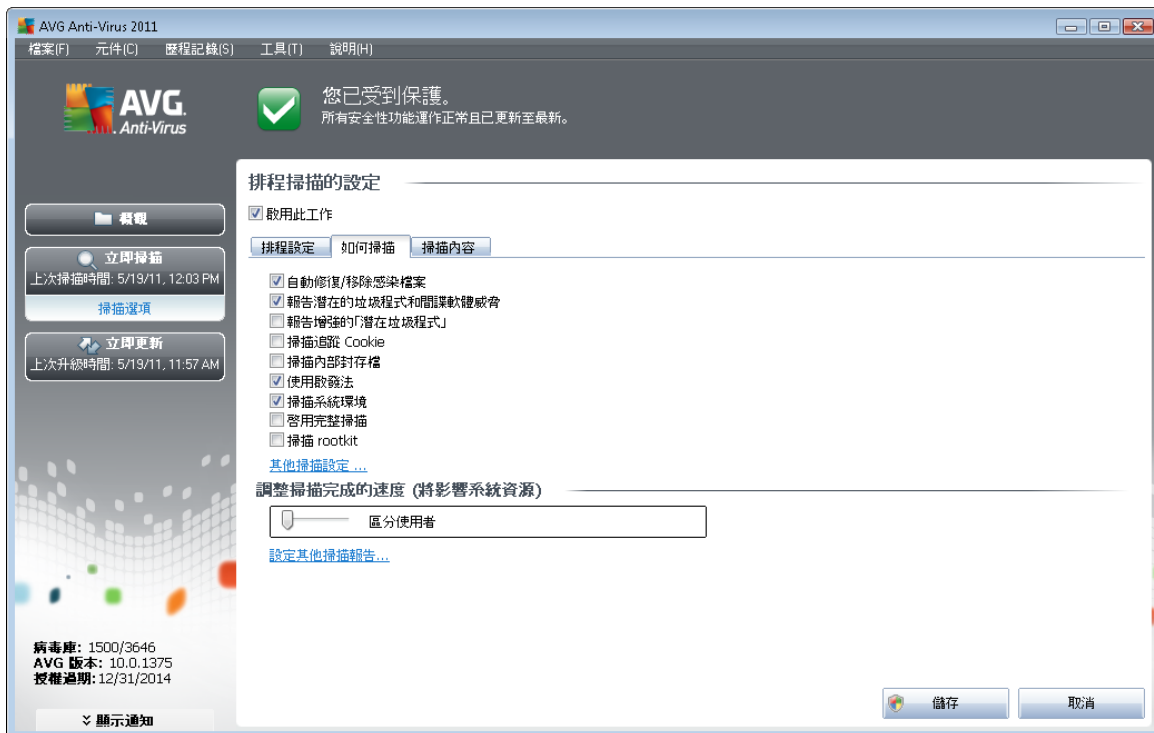
「排程掃描的設定」對話方塊的控制按鈕

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](#)。

10.5.2. 如何掃描



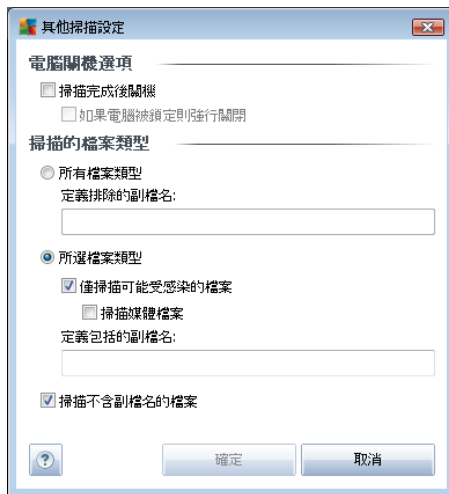
在 **如何掃描** 標籤上，您將看到一份可選擇開啟/關閉的掃描參數清單。預設情況下，大多數參數都已開啟，並將在掃描期間套用其功能。除非您確實需要變更這些設定，否則我們建議您保留預先定義的組態：

- **自動修復/移除感染檔案 (預設為開啟)**：如果在掃描期間發現病毒，可自動對其進行修復 (如果有可用的修復方法)。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](#)。
- **報告潛在的不受歡迎程式和間諜軟體威脅 (預設為開啟)**：核取此方塊可啟動 [Anti-Spyware](#) 引擎，並掃描間諜軟體和病毒。[間諜軟體](#) 代表一種可疑的惡意軟體類別：雖然它通常代表安全性風險，但有些程式可能是刻意安裝在電腦中的。建議您始終將此功能保持啟動狀態，因為它能提高您電腦的安全性。
- **報告增強的潛在不受歡迎程式集 (預設為關閉)**：標記此選項以偵測延伸的 [間諜軟體](#) 套件：這些程式在您直接向製造商購買時皆完全正常而且無害，但稍後可能會被不肖份子濫用。這個附加措施能進一步提高電腦安全性，但有可能會封鎖合法程式，因此預設為關閉。

- **掃描追蹤 Cookie (預設為關閉)** : **Anti-Spyware** 元件的此一參數定義在掃描期間應偵測 cookie (HTTP cookie 是用於驗證、追蹤和維護使用者的特定資訊, 如網站喜好或電子購物車內容)。
- **掃描封存內部 (預設為關閉)** : 此參數定義掃描應檢查所有檔案, 即使這些檔案已被封裝在某種封存內, 如 ZIP、RAR...
- **使用啟發法 (預設為開啟)** : 啟發法分析 (在虛擬電腦環境中動態模擬掃描物件的指令) 將成為掃描過程中用於偵測病毒的方法之一。
- **掃描系統環境 (預設為開啟)** : 掃描時還會檢查您電腦的系統區域。
- **啟用完整掃描 (預設為關閉)** - 在特定情況下 (懷疑您的電腦受到感染時), 您可以核取此選項來啟動最完整的掃描演算法, 這甚至會掃描幾乎不會被感染的電腦區域, 以防萬一。不過請記住, 這種方法相當耗時。

然後, 您可以按如下方式變更掃描組態 :

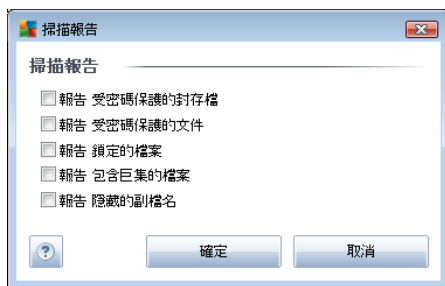
- **其他掃描設定** - 此連結會開啟新的**其他掃描設定**對話方塊, 讓您指定下列參數 :



- **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**), 將啟動一個新選項, 可用來設定電腦即使在鎖定狀態下也能關機 (**強行關閉鎖定的電腦**)。
- **定義要掃描的檔案類型** - 您應該進一步決定是否要掃描 :
 - **所有檔案類型** - 透過提供不應掃描的檔案清單 (以逗號分隔副檔名), 可定義掃描的例外 ;
 - **所選檔案類型** - 您可以指定您只想要掃描可能受感染的檔案 (將不掃描不會被感染的檔案, 例如一些純文字檔或其他一些非可執行檔), 包括媒體檔案 (視訊、音訊檔案 - 若保持取消核取此方塊, 將可進一步縮減掃描時間, 因為這些檔案通常都很大, 而且不太可能被病毒感染)。同樣地, 您可以依副檔名指定始終都應該掃描的檔案。

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

- **調整掃描完成的速度** - 您可以使用滑桿來變更掃描程序的優先順序。預設情況下，該選項值會設為區分使用者層級的自動資源使用量。此外，您也可以使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先定義的組態。任何組態變更只能由經驗豐富的使用者來執行。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](#)。



10.5.3. 掃描內容



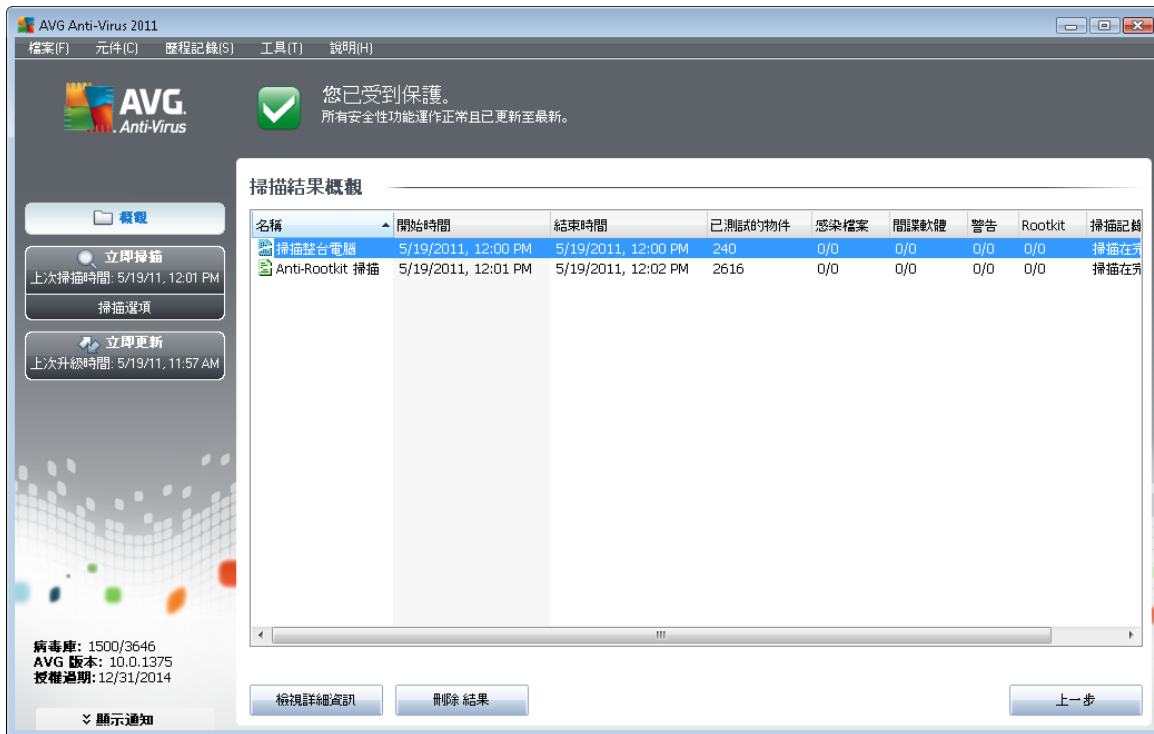
在 **掃描內容** 標籤上，您可以定義是要排程 **掃描整台電腦**，還是 **掃描特定檔案或資料夾**。

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

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


- **本機硬碟** - 您電腦中的所有硬碟
- **程式檔案**
 - C:\Program Files\
 - 在 64 位元版本中 C:\Program Files (x86)
- **「我的文件」資料夾**
 - 若是 Win XP : C:\Documents and Settings\Default User\My Documents\
 - 若是 Windows Vista/7 : C:\Users\user\Documents\


10.6. 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](#)

10.7. 掃描結果詳細資訊

如果您在 [掃描結果概觀](#) 對話方塊中選取了特定的掃描，就可以按一下 **檢視詳細資訊** 按鈕，切換至 [掃描結果](#) 對話方塊，查看所選掃描之過程和結果的詳細資料。

此對話方塊又進一步細分為數個標籤：

- **結果概觀** - 本標籤始終處於顯示狀態，提供說明掃描進度的統計資料
- **感染** - 本標籤只有在掃描過程中偵測到 [病毒感染](#) 時才會顯示
- **間諜軟體** - 本標籤只有在掃描過程中偵測到 [間諜軟體](#) 時才會顯示
- **警告** - 只有在掃描過程中偵測到 cookie 時，此標籤才會顯示
- **Rootkit** - 本標籤只有在掃描過程中偵測到 [Rootkit](#) 時才會顯示
- **資訊** - 本標籤只有在偵測到某些潛在的威脅，但無法分類為上述任何一類時，才會顯示；本標籤會提供有關此結果的警告訊息。此外，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)。



10.7.1. 「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：

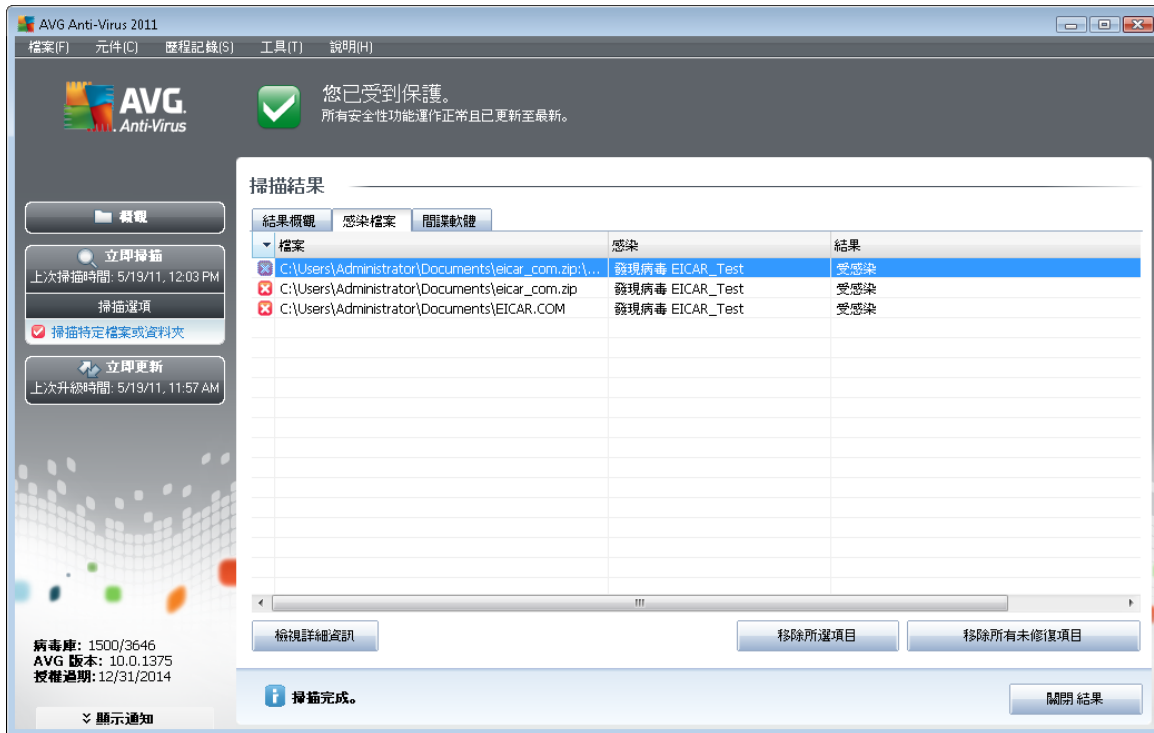
- 偵測到的 [病毒感染/間諜軟體](#)
- 已移除的 [病毒感染/間諜軟體](#)
- 無法移除或修復的 [病毒感染/間諜軟體](#) 數量

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。

10.7.2. 「感染」標籤



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

- **檔案** - 受感染物件原始位置的完整路徑
- **感染** - 偵測到的 **病毒** 的名稱 (關於特定病毒的詳細資訊，請參閱線上 [病毒大全](#))
- **結果** - 定義在掃描中偵測到的受感染物件的目前狀態：
 - **受感染** - 偵測到受感染物件並將其保留在原始位置 (例如，當您在特定掃描設定中 [關閉自動修復選項](#) 時)
 - **已修復** - 受感染的物件已被自動修復，並保留在其原始位置
 - **移至病毒隔離區** - 受感染物件已移至 [病毒隔離區](#) 隔離
 - **已刪除** - 受感染的物件已被刪除
 - **已新增至 PUP 例外** - 已將結果評估為例外，並新增至 PUP 例外清單中 (在進階設定的 [PUP 例外](#) 對話方塊中組態)
 - **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：

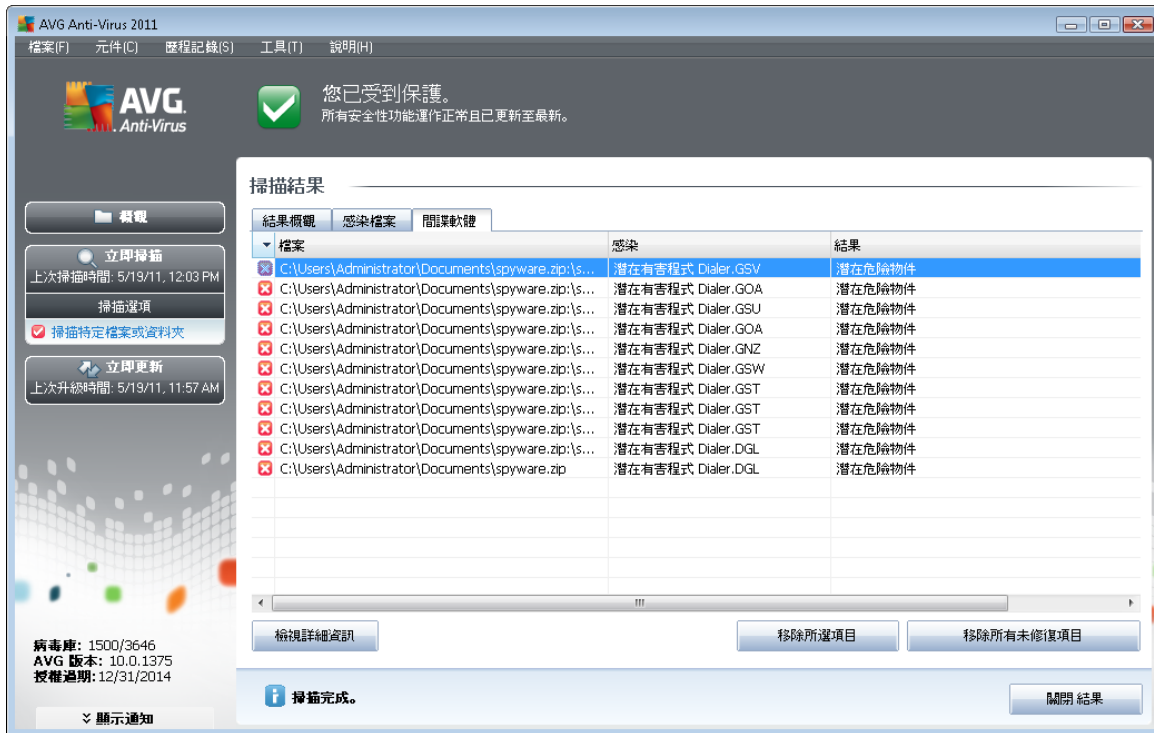
- **檢視詳細資訊** - 該按鈕可開啟名為**詳細物件資訊**的對話方塊視窗：



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

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

10.7.3. 「間諜軟體」標籤



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

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

集)；此資訊僅作為警告之用

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

控制按鈕

此對話方塊中有三個控制按鈕：

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



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

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

10.7.4. 「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。

10.7.5. Rootkit 標籤

如果您已啟動 [Anti-Rootkit 掃描](#)，**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一種程式。rootkit 幾乎不需要存取硬體，因為它主要的目的是取得在硬體上執行的作業系統的控制權。一般而言，rootkit 會透過破壞或迴避標準作業系統的安全性機制來隱身於系統中。這些 rootkit 往往也是特洛伊木馬，讓使用者誤以為在系統上執行它們很安全。用來達到此目的的技巧包括對監視程式隱藏執行中的程序，或是隱藏作業系統中的檔案或系統資料。

此標籤的結構與 [感染標籤](#) 或 [間諜軟體標籤](#) 基本相同。

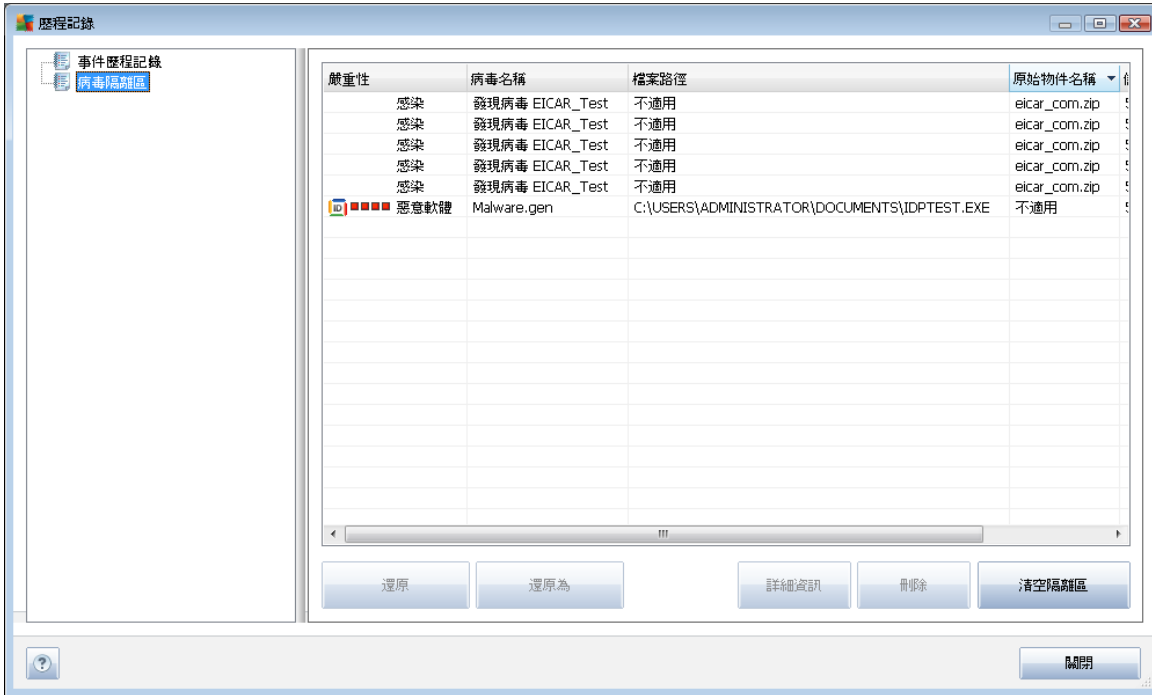
10.7.6. 「資訊」標籤

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)。

10.8. 病毒隔離區



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

病毒隔離區介面會在單獨的視窗中開啟，提供有關隔離的受感染物件的資訊概觀：

- **嚴重性** - 如果您決定在 **AVG Anti-Virus 2011** 中安裝 **Identity Protection** 元件，該區段會提供一個識別圖像，並且按嚴重性分為四個層級 - 從無害 (□□□□) 到非常危險 (■■■■)，並提供有關感染類型的資訊 (依其感染層級 - 所有列出的物件都有實際或潛在的感染)
- **病毒名稱** - 依據 **病毒大全** (線上) 指定偵測到的感染的名稱
- **檔案路徑** - 偵測到的感染檔案之原始位置的完整路徑
- **原始物件名稱** - 在掃描期間，圖表中列出的所有偵測到的物件均使用 AVG 提供的標準名稱進行標記。如果某個物件具有已知的特定原始名稱 (例如，與附件實際內容不一致的電子郵件附件的名稱)，則會在此欄中提供。
- **儲存日期** - 偵測到可疑檔案並將其移除到**病毒隔離區**的日期和時間

控制按鈕

可在 **病毒隔離區** 介面存取下列控制按鈕：

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



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



11. 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。

由於 AVG 更新是根據新威脅的數量和嚴重性不定期發行，因此建議至少一天檢查一次是否有新的更新。唯有透過這種方式，您才能確定 AVG Anti-Virus 2011 當天也處於最新狀態。

11.1. 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。

11.2. 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。

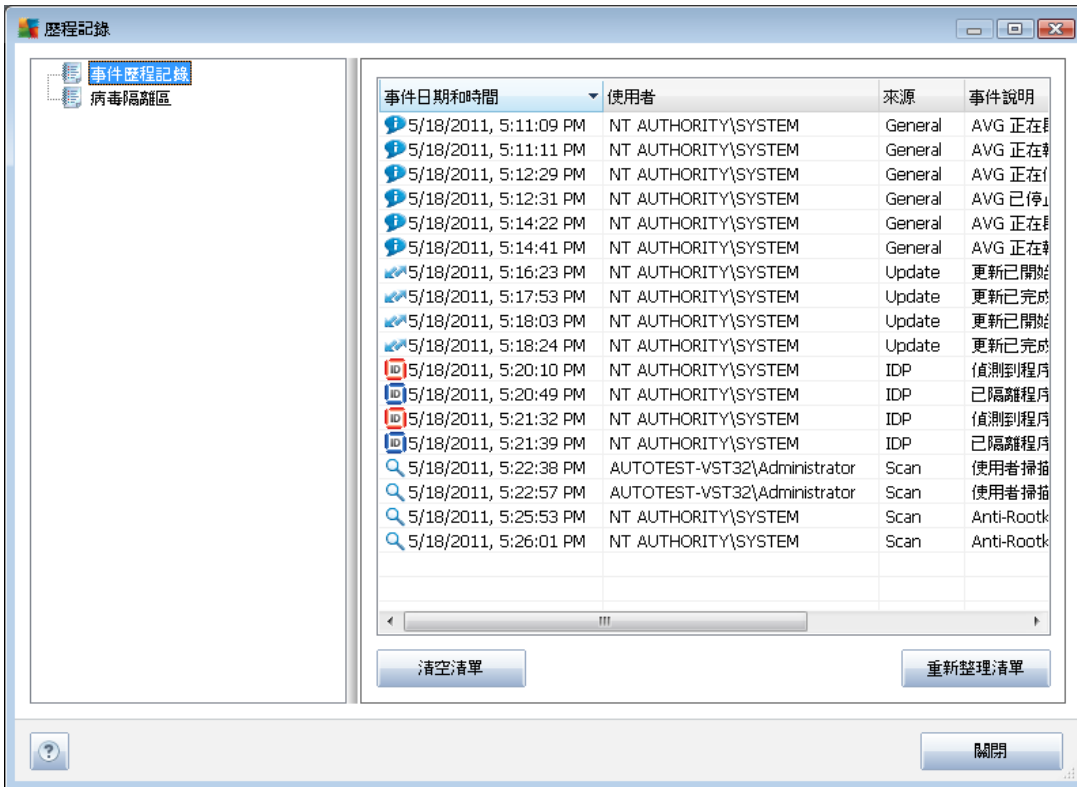
11.3. 更新程序

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！

12. 事件歷程記錄



歷程記錄對話方塊可透過系統功能表的歷程記錄 / 事件歷程記錄項目來存取。在此對話方塊中，您可以找到 AVG Anti-Virus 2011 作業期間發生的重要事件摘要。歷程記錄會記錄下列類型的事件：

- 有關 AVG 應用程式更新的資訊
- 掃描開始、結束或停止（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

每個事件都會列出以下資訊：

- **事件日期和時間**提供事件發生的確切日期和時間
- **使用者**指明誰啟動該事件
- **來源**說明觸發事件的來源元件或 AVG 系統的其他部分
- **事件描述**提供具體事件的簡短摘要



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



13. 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](http://www.avg.com/)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。