



AVG 9.0 Email Server Edition

使用者手冊

文件修訂版 **90.4 (31. 3. 2010)**

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。



內容

1. 簡介	4
2. AVG 安裝需求	5
2.1 支援的作業系統	5
2.2 支援的電子郵件伺服器	5
2.3 硬體需求	5
2.4 解除安裝之前版本	6
2.5 MS Exchange Service Pack	6
3. AVG 安裝程序	8
3.1 安裝啓動	8
3.2 授權協議	9
3.3 檢查系統狀態	9
3.4 選取安裝類型	10
3.5 啓動 AVG	10
3.6 自訂安裝 - 目標資料夾	11
3.7 自訂安裝 - 元件選取	12
3.8 自訂安裝 - DataCenter	14
3.9 安裝	14
3.10 安裝完成	15
4. E-mail Scanner for MS Exchange Server 2007/2010	18
4.1 概觀	18
4.2 E-mail Scanner for MS Exchange (路由 TA)	22
4.3 E-mail Scanner for MS Exchange (SMTP TA)	24
4.4 E-mail Scanner for MS Exchange (VSAPI)	24
4.5 偵測動作	27
4.6 郵件篩選	28
5. E-mail Scanner for MS Exchange Server 2000/2003	30
5.1 概觀	30
5.2 VSAPI 2.0	33
5.3 E-mail Scanner for MS Exchange (VSAPI)	34
5.4 偵測動作	37
5.5 郵件篩選	38

6. AVG for Kerio MailServer	40
6.1 組態	40
6.1.1 Antivirus	40
6.1.2 附件篩選器	40
7. Anti-Spam 組態	45
7.1 Anti-Spam 介面	45
7.2 Anti-Spam 原理	47
7.3 Anti-Spam 設定	47
7.3.1 Anti-Spam 訓練精靈	47
7.3.2 選取含郵件的資料夾	47
7.3.3 郵件篩選選項	47
7.4 效能	53
7.5 RBL	54
7.6 白名單	55
7.7 黑名單	57
7.8 進階設定	58
8. AVG 設定管理員	59
9. 常見問題集和技術支援	62



1. 簡介

本使用者手冊提供有關 **AVG 9.0 Email Server Edition** 的詳細介紹。

感謝您購買 **AVG 9.0 Email Server Edition** !

AVG 9.0 Email Server Edition 是獲獎的 AVG 產品系列之一，它能為您的電腦提供全面保護，讓您安心無虞。如 AVG 所有的產品一樣，**AVG 9.0 Email Server Edition** 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。

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。

注意：本文件包含特定 E-mail Server Edition 功能的說明。如果您需要有關其他 AVG 功能的資訊，請參閱針對 Internet Security 版本的使用者指南，其中包含所有必要的詳細資訊。您可以從 <http://www.avg.com> 下載該指南。

2. AVG 安裝需求

2.1. 支援的作業系統

AVG 9.0 Email Server Edition 可保護執行下列作業系統的電子郵件伺服器：

- Windows 2008 Server Edition (x86 和 x64)
- Windows 2003 Server (x86 和 x64) SP1
- Windows 2000 Server SP4 + 更新彙總套件 1

2.2. 支援的電子郵件伺服器

以下是支援的電子郵件伺服器：

- **MS Exchange 2000 Server** 版本 (帶有 **Service Pack 1** 或更高版本)

注意：對於 Exchange 2000 Server - 需要套用 Service Pack 1 (或更高版本) 才能使用 AVG 引擎；**AVG for MS Exchange 2000/2003 Server** 使用此 Service Pack 中包含的 VSAPI 2.0 (或 2.5，針對 Exchange 2003 Server) 應用程式介面。

- **MS Exchange 2003 Server** 版本
- **MS Exchange 2007 Server** 版本
- **MS Exchange 2010 Server** 版本
- **AVG for Kerio MailServer** - 版本 6.7.2 及更高版本

2.3. 硬體需求

AVG 9.0 Email Server Edition 的最低硬體需求：

- Intel Pentium CPU 1.5 GHz
- 500 MB 可用硬碟空間 (用於安裝)
- 512 MB RAM 記憶體

AVG 9.0 Email Server Edition 的建議硬體需求：



- Intel Pentium CPU 1.8 GHz
- 600 MB 可用硬碟空間 (用於安裝)
- 512 MB RAM 記憶體

2.4. 解除安裝之前版本

如果您之前安裝了舊版本的 AVG Email Server，在安裝 **AVG 9.0 Email Server Edition** 之前需要先解除安裝舊版本。您必須使用標準 Windows 功能，手動解除安裝先前版本。

- 從「開始」功能表 **開始/設定/控制台/新增或移除程式**，然後從已安裝軟體清單中選取正確的程式。務必選取正確的要解除安裝的 AVG 程式。解除安裝 AVG File Server Edition 前，需要先解除安裝 Email Server Edition。
- 解除安裝 Email Server Edition 後，才能繼續解除安裝 AVG File Server Edition 的先前版本。這可以從「開始」功能表輕鬆完成：**開始/所有程式/AVG/解除安裝 AVG**
- 如果您之前使用過 AVG 8.x 或更舊的版本，不要忘記解除安裝各個伺服器外掛程式。

注意：解除安裝過程中，將需要重新啟動儲存區服務。

Exchange 外掛程式 - 從外掛程式的安裝資料夾使用 /uninstall 參數執行 setupes.exe。

例如 C:\AVG4ES2K\setupes.exe /uninstall

Lotus Domino/Notes 外掛程式 - 從外掛程式的安裝資料夾使用 /uninstall 參數執行 setupln.exe：

例如 C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Pack

由於 **AVG for MS Exchange 2000/2003 Server** 使用 VSAPI 2.0/2.5 病毒掃描介面，因此您必須為您系統中的 MS Exchange 2000 Server 套用 Service Pack 1 (或更高版本)。請造訪下面的連結，以取得 MS Exchange 2000 Server 的最新 Service Pack：

MS Exchange 2000 Server Service Pack：



<http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.aspx>

對於 MS Exchange 2003 Server，不需要額外的 Service Pack；但是建議盡可能讓您的系統擁有最新版本的 Service Pack 和 Hotfix，以確保取得最大安全性。

MS Exchange 2003 Server Service Pack (選用)：

<http://www.microsoft.com/exchange/evaluation/sp2/overview.aspx>

安裝開始時，會檢查所有系統程式庫版本。如果需要安裝更新版本的程式庫，安裝程式會使用副檔名 .delete 重新命名舊的程式庫。系統重新啟動後，會將它們刪除。

MS Exchange 2007 Server Service Pack (選用)：

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>

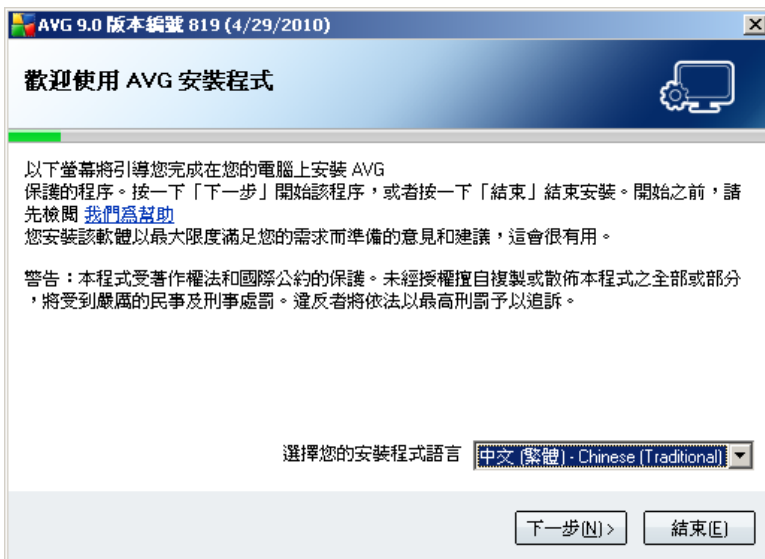
3. AVG 安裝程序

要在電腦上安裝 AVG，您需要取得最新的安裝檔案。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。您可以從 [AVG 網站](http://www.avg.com/download?prd=msw) 下載檔案（網址為 <http://www.avg.com/download?prd=msw>）。

在安裝過程中，系統會要求您提供授權號碼。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。

將安裝檔案下載並儲存到您的硬碟後，就可以啟動安裝程序。安裝作業包含一系列對話方塊視窗，其中會提供每個步驟的簡短說明。下面提供了每個對話方塊視窗的說明：

3.1. 安裝啟動



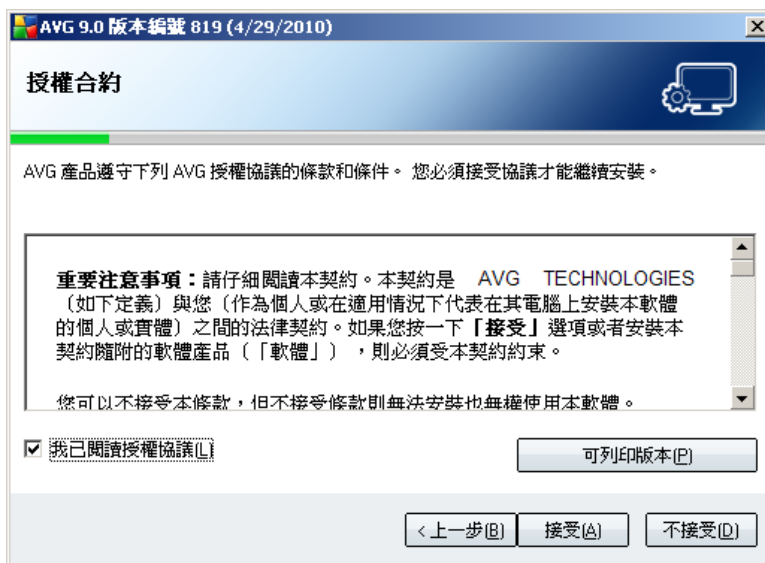
安裝程序啟動時會顯示 **歡迎** 視窗。您可在此處選取用於安裝程序的語言。在對話方塊視窗的下半部，找到 **選擇您的安裝程式語言** 項目，並從下拉式功能表中選取需要的語言。然後按下 **下一步** 按鈕確認並繼續至下一個對話方塊。

注意： 在安裝過程中，您也可以為日後的應用程式介面選擇其他語言。

3.2. 授權協議

授權協議對話方塊提供 AVG 授權協議的完整內容。請仔細閱讀，並核取 **我已閱讀授權協議** 核取方塊，然後按下 **接受** 按鈕，確認您已閱讀、瞭解並接受該協議。如果您不同意所述的使用條款，請按 **不接受** 按鈕，安裝程序隨後將立即終止。

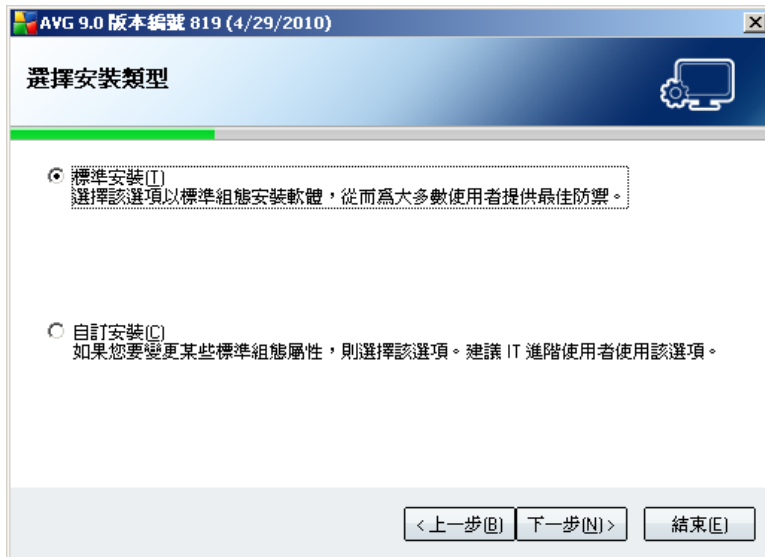
使用 **可列印版本** 按鈕，在一個新視窗中開啓該授權協議以進行列印。



3.3. 檢查系統狀態

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

3.4. 選取安裝類型



*選取安裝類型*對話方塊提供了兩種安裝選項，即：*標準安裝*和*自訂安裝*。

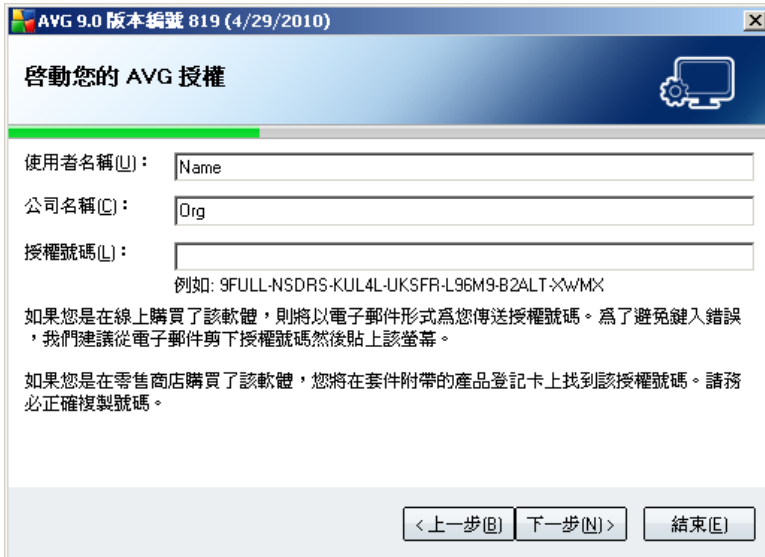
對於大多數使用者，強烈建議保持使用*標準安裝*，它會以完全自動的模式，使用程式供應商預定義的設定來安裝 AVG。這種組態不僅提供最大安全性，並且充分利用資源。在未來如果需要變更此組態，您隨時可以在 AVG 應用程式中直接操作。

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

3.5. 啟動 AVG

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

然後在*授權號碼*文字欄位輸入您的授權號碼。授權號碼位於您在線上購買 AVG 後收到的確認電子郵件內。您必須完全按照顯示的號碼準確輸入。如果授權號碼的數位格式可用（在電子郵件中），則建議使用複製和貼上方法將其插入。



啓動您的 AVG 授權

使用者名稱(N):

公司名稱(O):

授權號碼(L):

例如: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

如果您是在線上購買了該軟體，則將以電子郵件形式為您傳送授權號碼。為了避免鍵入錯誤，我們建議從電子郵件剪下授權號碼然後貼上該螢幕。

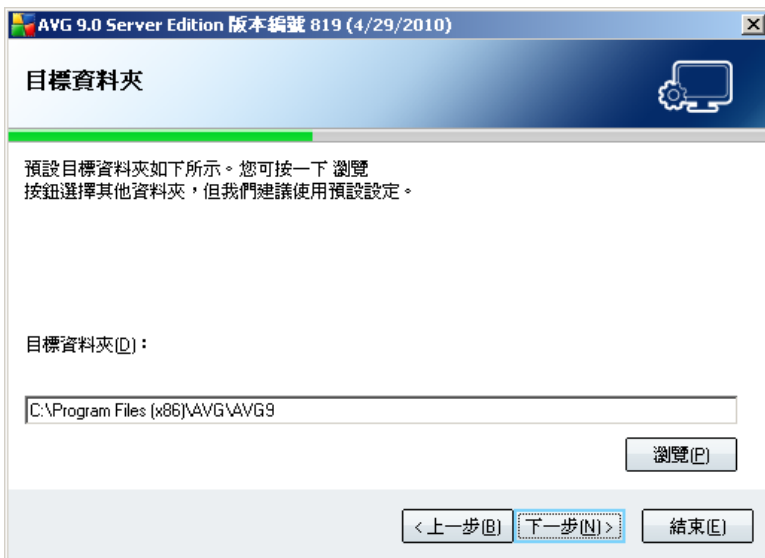
如果您是在零售商店購買了該軟體，您將在套件附帶的產品登記卡上找到該授權號碼。請務必正確複製號碼。

< 上一步(B) 下一步(N) > 結束(E)

按下下一步按鈕繼續執行安裝程序。

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

3.6. 自訂安裝 - 目標資料夾



目標資料夾

預設目標資料夾如下所示。您可按一下 瀏覽 按鈕選擇其他資料夾，但我們建議使用預設設定。

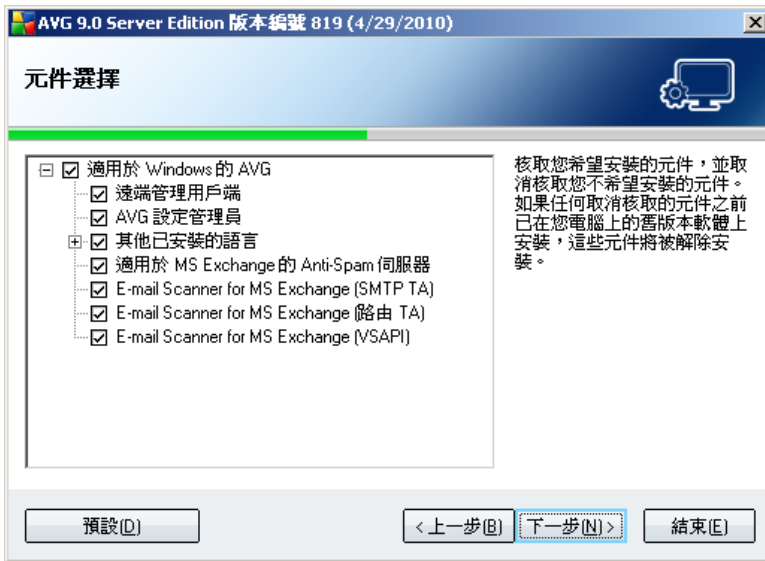
目標資料夾(D):

瀏覽(B)

< 上一步(B) 下一步(N) > 結束(E)

目標資料夾對話方塊可讓您指定安裝 AVG 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。按下一步按鈕確認。

3.7. 自訂安裝 - 元件選取



元件選取對話方塊顯示所有可以安裝的 AVG 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，您只能選取包含在您購買的 **AVG** 版本中的元件。「元件選取」對話方塊中僅提供這些元件讓您安裝！

- **遠端管理元件** - 如果您打算將 AVG 連線至 AVG DataCenter (AVG Network Edition)，需要選取此選項。

注意：只有清單中所列出的伺服器元件可以進行遠端管理！

- **AVG 設定管理員** - 一款主要面向網路管理員的工具，可讓您複製、編輯和分配 AVG 組態。該組態可以儲存到可攜式裝置（如 USB 快閃磁碟機等），然後手動或透過其他方式套用至所選站點。
- **其他已安裝的語言** - 您可以定義 AVG 要以哪種語言安裝。核取**其他已安裝的語言**項目，然後從相應的功能表選取所需語言。

各個伺服器元件的基本概觀：

- **Anti-Spam Server for MS Exchange**

檢查所有傳入電子郵件訊息，並將來路不明的電子郵件標示為垃圾郵件。它會使用多種分析方法來處理每一封電子郵件訊息，從而提供最大的保護來封鎖垃圾電子郵件訊息。

- **E-mail Scanner for MS Exchange (路由傳輸代理程式)**

檢查 MS Exchange HUB 角色路由的所有傳入、傳出和內部電子郵件訊息。

適用於 MS Exchange 2007，且只能為 HUB 角色安裝。

- **E-mail Scanner for MS Exchange (SMTP 傳輸代理程式)**

檢查透過 MS Exchange SMTP 介面的所有電子郵件訊息。

僅適用於 MS Exchange 2007，且可為 EDGE 和 HUB 兩種角色安裝。

- **E-mail Scanner for MS Exchange (VSAPI)**

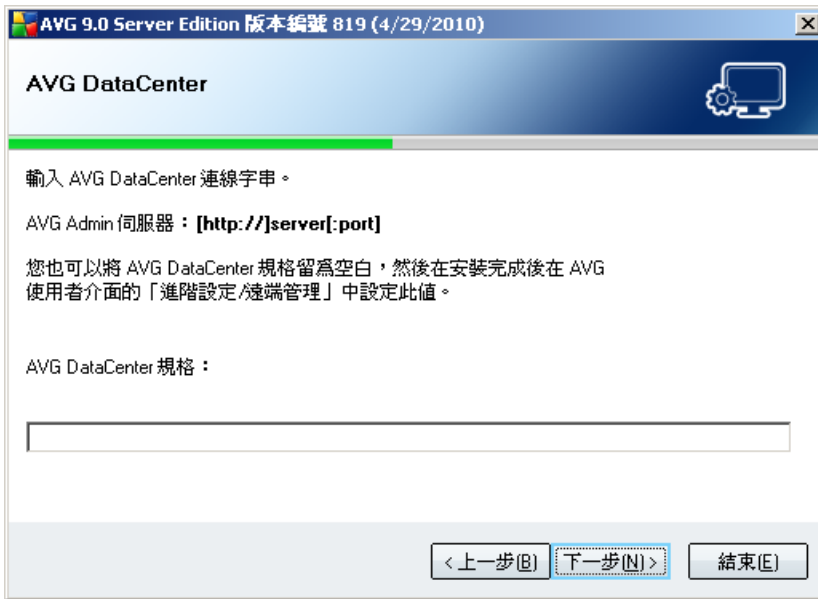
檢查儲存在使用者信箱中的所有電子郵件訊息。如果偵測到任何病毒，便會將其移至病毒隔離區，或者將其完全移除。

注意：適用於 MS Exchange 2007 和 MS Exchange 2003 的選項各不相同。

按下一步按鈕繼續。

3.8. 自訂安裝 - DataCenter

如果在模組選取時已選擇 *遠端管理元件* 模組，那麼您可以在此螢幕中定義連線到您的 AVG DataCenter 所用的連線字符串。

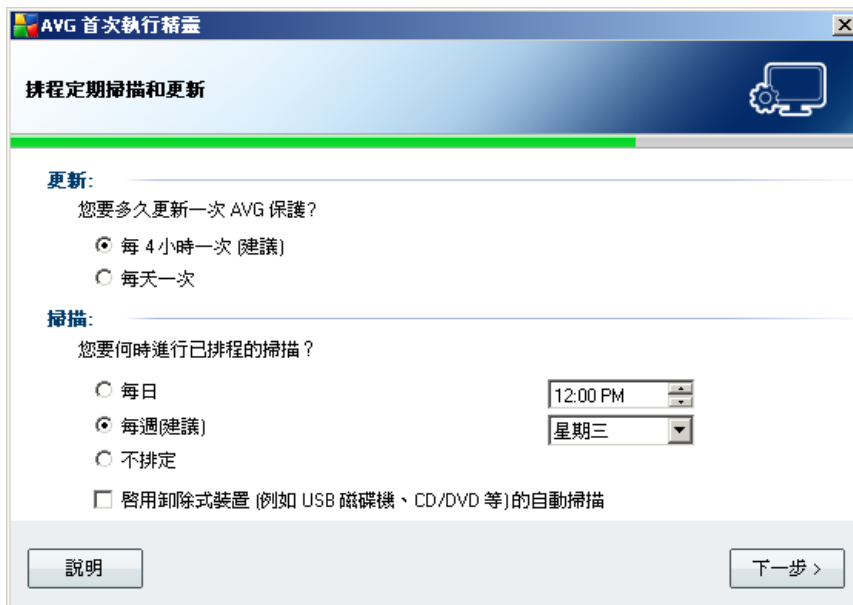


3.9. 安裝

安裝 對話方塊會顯示安裝程序的進度，完全無需任何操作。請等候安裝完成，然後會將您重新導向到 [安裝完成](#) 對話方塊。

3.10. 安裝完成

安裝期間，首次執行精靈會自動啓動，並需要您在完成安裝之前，填寫一些簡單的步驟：

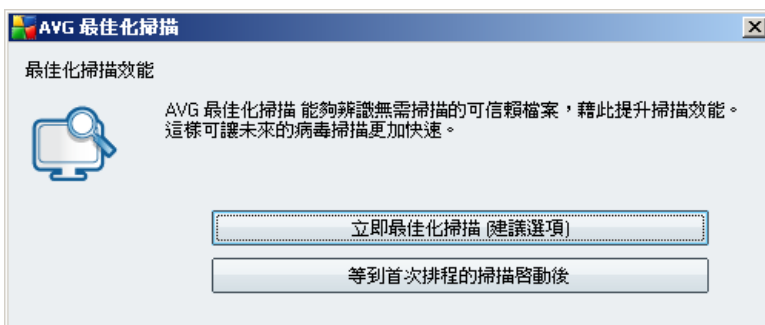


在 *排程定期掃描和更新* 對話方塊中設定新更新檔案可存取性檢查的時間間隔，以及定義要啓動排程掃描的時間。建議保留預設值。按下 *下一步* 按鈕繼續。



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

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



建議您採用此選項，並按一下 *立即進行最佳化掃描* 來執行掃描最佳化程序。

AVG 現已安裝在您的電腦上，且可完整運作。程式在幕後執行，完全處於自動模式。



要為您的個別電子郵件伺服器設定保護，請遵循相關章節的指示：

- [**E-mail Scanner for MS Exchange Server 2007/2010**](#)
- [**E-mail Scanner for MS Exchange Server 2000/2003**](#)
- [**AVG for Kerio MailServer**](#)

4. E-mail Scanner for MS Exchange Server 2007/2010

4.1. 概觀

AVG for MS Exchange Server 2007 組態選項已完全整合到 AVG 9.0 Email Server Edition 中作為伺服器元件。



各個伺服器元件的基本概觀：

- **[Anti-Spam - Anti-Spam Server for MS Exchange](#)**

檢查所有傳入電子郵件訊息，並將來路不明的電子郵件標示為垃圾郵件。它會使用多種分析方法來處理每一封電子郵件訊息，從而提供最大的保護來封鎖垃圾電子郵件訊息。

- **[EMS \(路由\) - E-mail Scanner for MS Exchange \(路由傳輸代理程式\)](#)**

檢查 MS Exchange HUB 角色路由的所有傳入、傳出和內部電子郵件訊息。

適用於 MS Exchange 2007，且只能為 HUB 角色安裝。

- **[EMS \(SMTP\) - E-mail Scanner for MS Exchange \(SMTP 傳輸代理程式\)](#)**

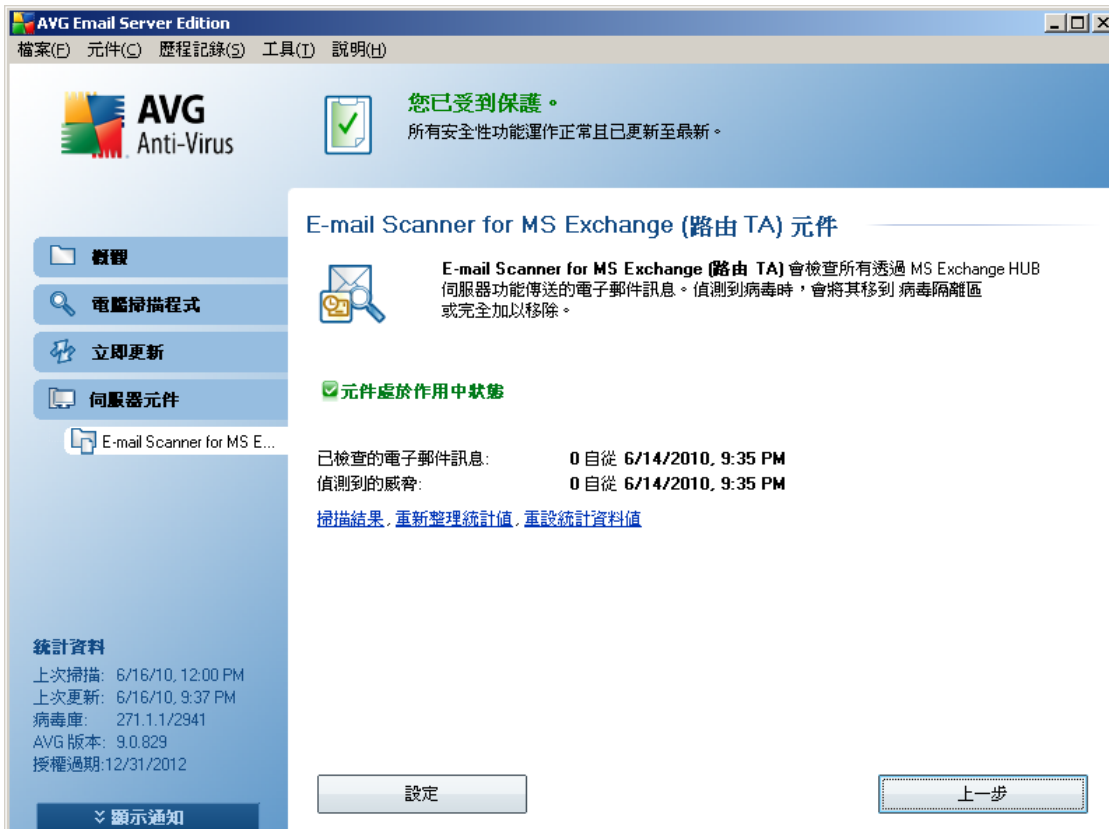
檢查透過 MS Exchange SMTP 介面的所有電子郵件訊息。

僅適用於 MS Exchange 2007，且可為 EDGE 和 HUB 兩種角色安裝。

- **[EMS \(VSAPI\) - E-mail Scanner for MS Exchange \(VSAPI\)](#)**

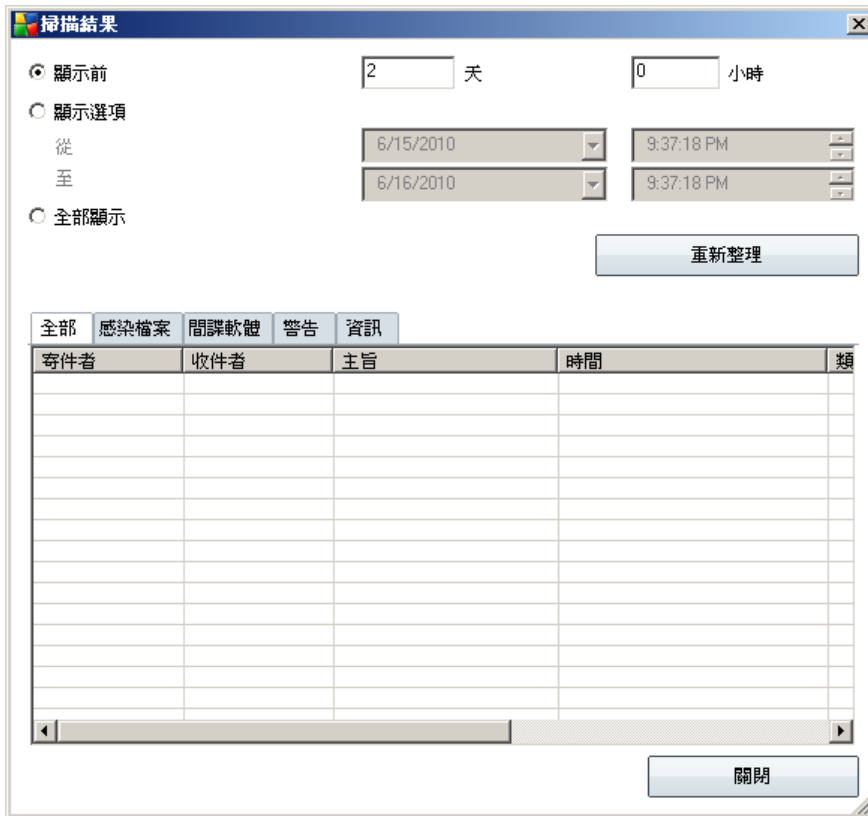
檢查儲存在使用者信箱中的所有電子郵件訊息。如果偵測到任何病毒，便會將其移至病毒隔離區，或者將其完全移除。

連接兩下需要的元件可開啓該元件的介面。除 **Anti-Spam** 外，所有其他元件都包含以下常用控制按鈕和連結：



- **掃描結果**

開啓新對話方塊，您可在此檢視掃描結果：



您可在此檢查訊息，這些訊息按嚴重性細分到數個標籤。要修改嚴重性並進行報告，請參閱個別元件的組態。

預設情況下，只顯示最近兩天的結果。您可以修改以下選項來變更顯示時間：

- **顯示最近** - 插入偏好的天數和小時數。
- **顯示選取範圍** - 選擇自訂的時間和日期間隔。
- **全部顯示** - 顯示整個時間期限內的結果。

使用 **重新整理** 按鈕可重新載入結果。

- **重新整理統計值** - 更新上面顯示的統計資料。
- **重設統計值** - 將所有統計資料重設為零。

工作按鈕如下所示：

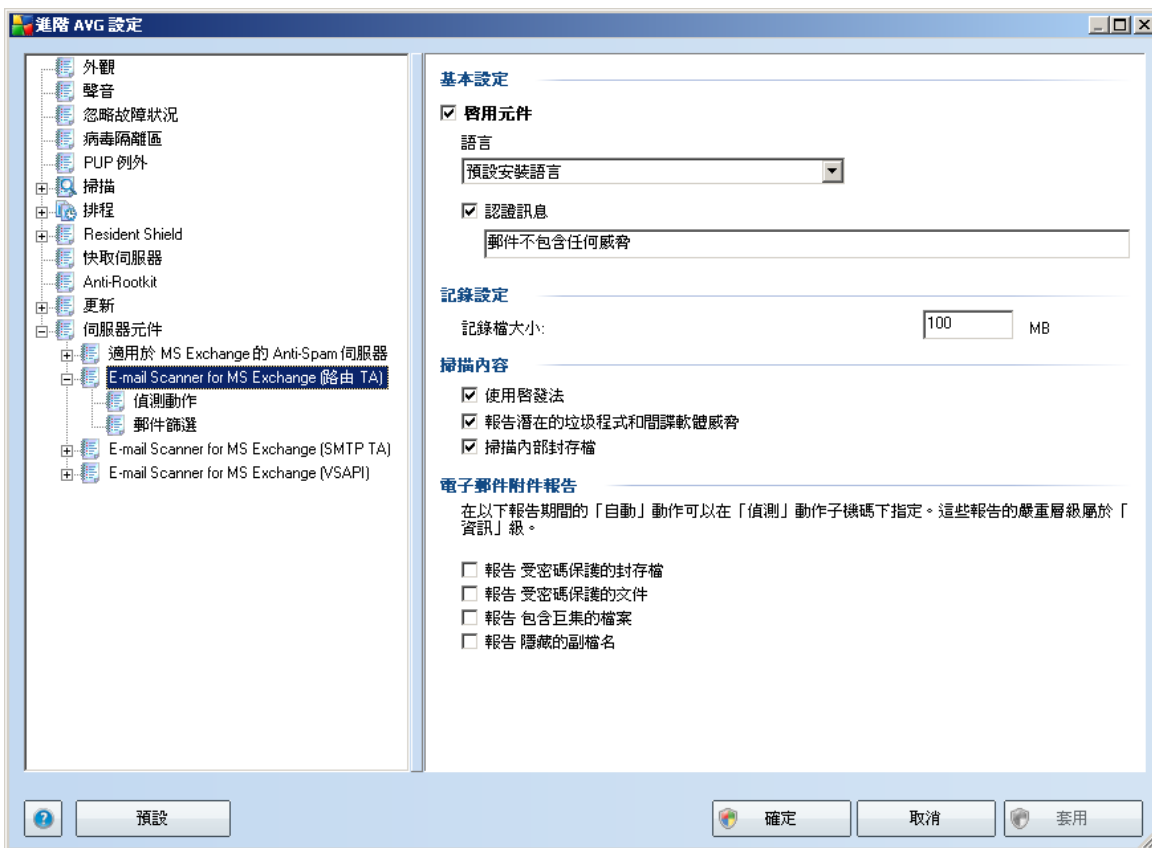
- **設定** - 使用此按鈕可開啓元件的設定。
- **上一步** - 按此按鈕可以返回至「伺服器元件概觀」。

您可以在下面的章節中找到有關所有元件個別設定的更多資訊。

4.2. E-mail Scanner for MS Exchange（路由 TA）

要開啓 **E-mail Scanner for MS Exchange（路由代理傳輸程式）** 的設定，請從元件介面中選取 **設定** 按鈕。

從 **伺服器元件** 清單中選取 **E-mail Scanner for MS Exchange（路由 TA）** 項目：



基本設定部分包含以下選項：

- **啓用元件** - 取消選取該選項會停用整個元件。
- **語言** - 選取偏好的元件語言。
- **認證訊息** - 如果您想爲所有掃描過的訊息加上認證說明，可核取此選項。您可以在后面的欄位中自訂該訊息。

記錄設定部分：

- **記錄檔大小** - 選擇偏好的記錄檔大小。預設值：**100 MB**。

掃描內容部分：

- **使用啓發法** - 核取此方塊可在掃描期間啓用啓發法分析。
- **報告潛在的垃圾程式和間諜軟體威脅** - 核取此選項可報告出現的潛在垃圾程式和間諜軟體。
- **掃描封存內部** - 核取此選項可讓掃描程式也檢查封存（**zip**、**rar**等）內的檔案。

電子郵件附件報告部分允許您選取掃描期間應報告的項目。如果核取該方塊，則包含此項目的每封電子郵件的訊息主旨中都將包含 **[INFORMATION]** 標記。這是預設組態，可以在**偵測動作**部分下的**資訊**部分輕鬆修改（請參閱下文）。

有以下選項可用：

- **報告受密碼保護的封存**
- **報告受密碼保護的文件**
- **報告包含巨集的檔案**
- **報告隱藏的副檔名**

以下樹狀結構中還提供了下列子項目：

- [偵測動作](#)
- [郵件篩選](#)

4.3. E-mail Scanner for MS Exchange (SMTP TA)

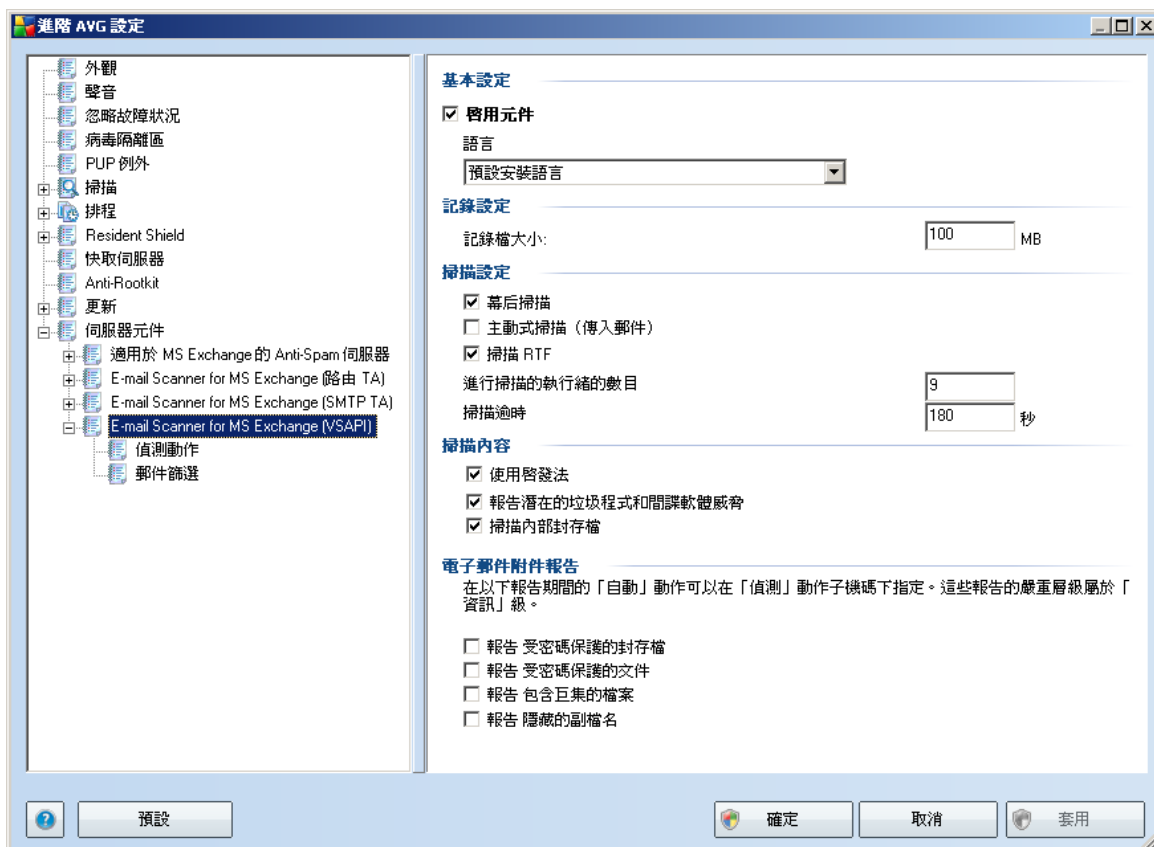
E-mail Scanner for MS Exchange (SMTP TA) 的組態與路由傳輸代理程式的情況完全相同。欲瞭解更多資訊，請參閱上文的 [E-mail Scanner for MS Exchange \(路由 TA\)](#) 一章。

以下樹狀結構中還提供了下列子項目：

- [偵測動作](#)
- [郵件篩選](#)

4.4. E-mail Scanner for MS Exchange (VSAPI)

此項目包含 **E-mail Scanner for MS Exchange (VSAPI)** 的設定。



基本設定部分包含以下選項：



- **啓用元件** - 取消選取該選項會停用整個元件。
- **語言** - 選取偏好的元件語言。

記錄設定部分：

- **記錄檔大小** - 選擇偏好的記錄檔大小。預設值：100 MB。

掃描設定部分：

- **背景掃描** - 您可以在此啓用或停用背景掃描程序。背景掃描是 VSAPI 2.0/2.5 應用程式介面的功能之一。它提供 **Exchange Messaging** 資料庫的執行緒式掃描。每當在使用者信箱資料夾中發現未使用最新的 AVG 病毒庫更新掃描的項目時，會將該項目提交至待掃描的 **AVG for Exchange 2007 Server**。然後會對未檢查過的物件並行執行掃描與搜尋兩種作業。

每個資料庫都會使用一個特定的低優先順序的執行緒，從而確保其他工作（例如，在 **Microsoft Exchange** 資料庫中儲存電子郵件訊息）永遠會優先執行。

- **主動式掃描（傳入郵件）**

您可以在此啓用或停用 VSAPI 2.0/2.5 的主動式掃描功能。當有項目傳遞到資料夾，但用戶端尚未發出要求時會執行此掃描。

一旦訊息提交到 **Exchange** 儲存區，即以低優先順序進入全域掃描佇列（最多 30 個項目）。它們基於先進先出 (FIFO) 原則掃描。如果項目仍在佇列中時被存取，則會變為高優先級。

注意：溢位訊息會繼續留在未掃描的儲存區。

注意：即使您將**背景掃描**和**主動式掃描**兩個選項都停用，當有使用者嘗試使用 **MS Outlook** 用戶端下載訊息時，存取時掃描程式仍處於作用中。

- **掃描 RTF** - 您可以在此指定是否要掃描 RTF 格式的檔案。
- **正在掃描的執行緒數目** - 掃描程序預設會按執行緒執行，以藉由某種程度的並行化處理來提高整體掃描效能。您可以在此處變更執行緒計數。

預設執行緒數目 = 處理器數目 × 2 + 1。

最小執行緒數目 = (處理器數目 + 1) / 2。

最大執行緒數目 = 處理器數目 × 5 + 1。

如果該值小於等於最小值或大於等於最大值，則使用預設值。

- **掃描逾時** - 一個執行緒在存取被掃描的訊息時的最大連續時間間隔（以秒計）（預設值為 180 秒）。

掃描內容部分：

- **使用啓發法** - 核取此方塊可在掃描期間啓用啓發法分析。
- **報告潛在的垃圾程式和間諜軟體威脅** - 核取此選項可報告出現的潛在垃圾程式和間諜軟體。
- **掃描封存內部** - 核取此選項可讓掃描程式也檢查封存（zip、rar 等）內的檔案。

電子郵件附件報告部分允許您選取掃描期間應報告的項目。預設組態可以在**偵測動作**部分下的**資訊**部分輕鬆進行修改（請參閱下文）。

有以下選項可用：

- **報告受密碼保護的封存**
- **報告受密碼保護的文件**
- **報告包含巨集的檔案**
- **報告隱藏的副檔名**

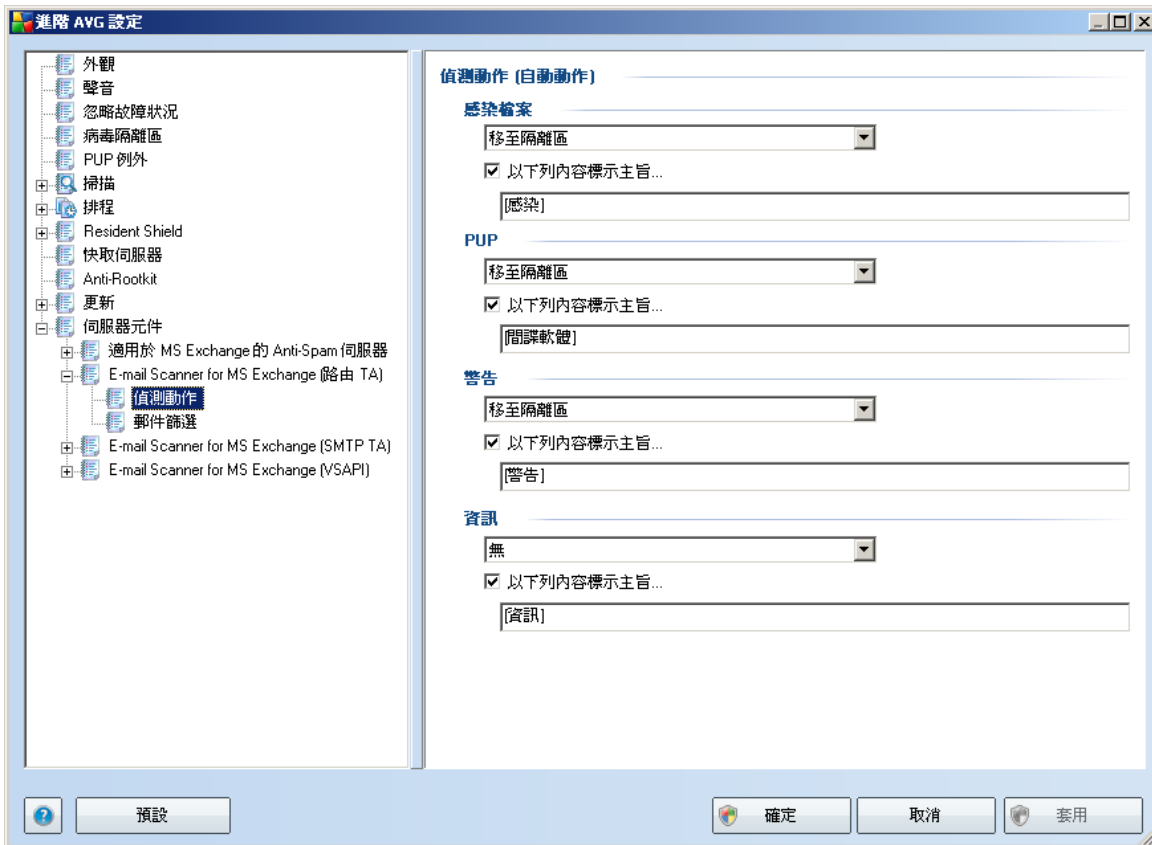
這其中的一些功能通常是 Microsoft VSAPI 2.0/2.5 應用程式介面服務的使用者延伸。欲瞭解有關 VSAPI 2.0/2.5 的詳細資訊，請參閱下面的連結（以及可從參考的項目存取的連結）：

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> - 取得有關 Exchange 和反病毒軟體互動的資訊
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> - 取得有關 Exchange 2003 Server 應用程式中其他 VSAPI 2.5 功能的資訊。

以下樹狀結構中還提供了下列子項目：

- [偵測動作](#)
- [郵件篩選](#)

4.5. 偵測動作



在 **偵測動作** 子項目中，您可以選擇掃描期間應自動執行的動作。

這些動作可以用於以下項目：

- 感染
- **PUP** (潛在垃圾程式)
- 警告
- 資訊

使用下拉式功能表選擇針對每個項目的動作：

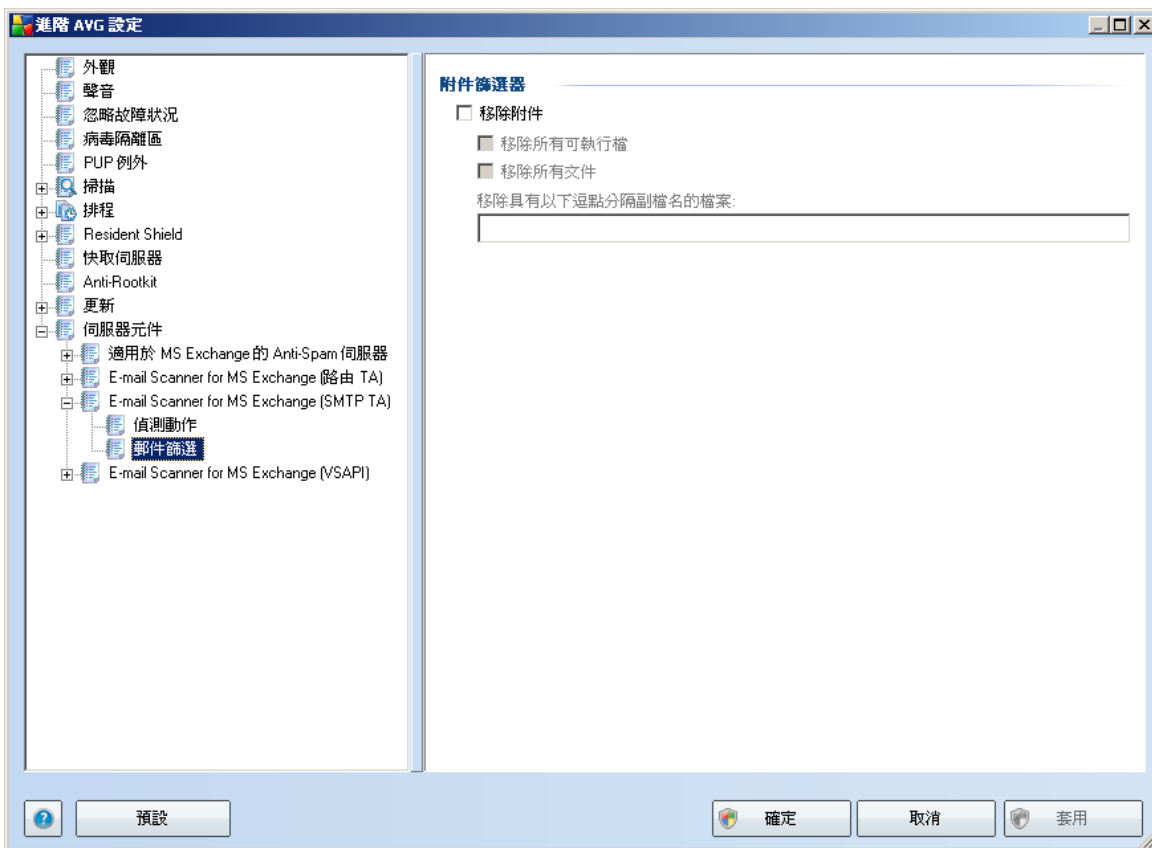
- 無 - 不執行任何動作。

- **移至隔離區** - 特定的威脅將被移至病毒隔離區。
- **移除** - 特定的威脅將被移除。

要為包含特定項目/威脅的訊息選取自訂主題文字，請核取以下列內容標示主旨... 方塊，並填寫偏好的值。

注意：最後提到的功能不適用於 E-mail Scanner for MS Exchange VSAPI。

4.6. 郵件篩選



在 **郵件篩選** 子項目中，您可以選擇應自動移除的附件（若有）。有以下選項可用：

- **移除附件** - 核取此方塊可啟用該該功能。
- **移除所有可執行檔** - 移除所有可執行檔。



- *移除所有文件* - 移除所有文件檔案。
- *移除具有以下逗點分隔副檔名的檔案* - 在此方塊中填入您希望自動移除的檔案的副檔名。使用逗號分隔副檔名。

5. E-mail Scanner for MS Exchange Server 2000/2003

5.1. 概觀

E-mail Scanner for MS Exchange Server 2000/2003 組態選項已完全整合到 AVG 9.0 Email Server Edition 中作為伺服器元件。



伺服器元件包括以下項目：

各個伺服器元件的基本概觀：

- **[Anti-Spam - Anti-Spam Server for MS Exchange](#)**

檢查所有傳入電子郵件訊息，並將來路不明的電子郵件標示為垃圾郵件。它會使用多種分析方法來處理每一封電子郵件訊息，從而提供最大的保護來封

鎖垃圾電子郵件訊息。

- **EMS (VSAPI) - E-mail Scanner for MS Exchange (VSAPI)**

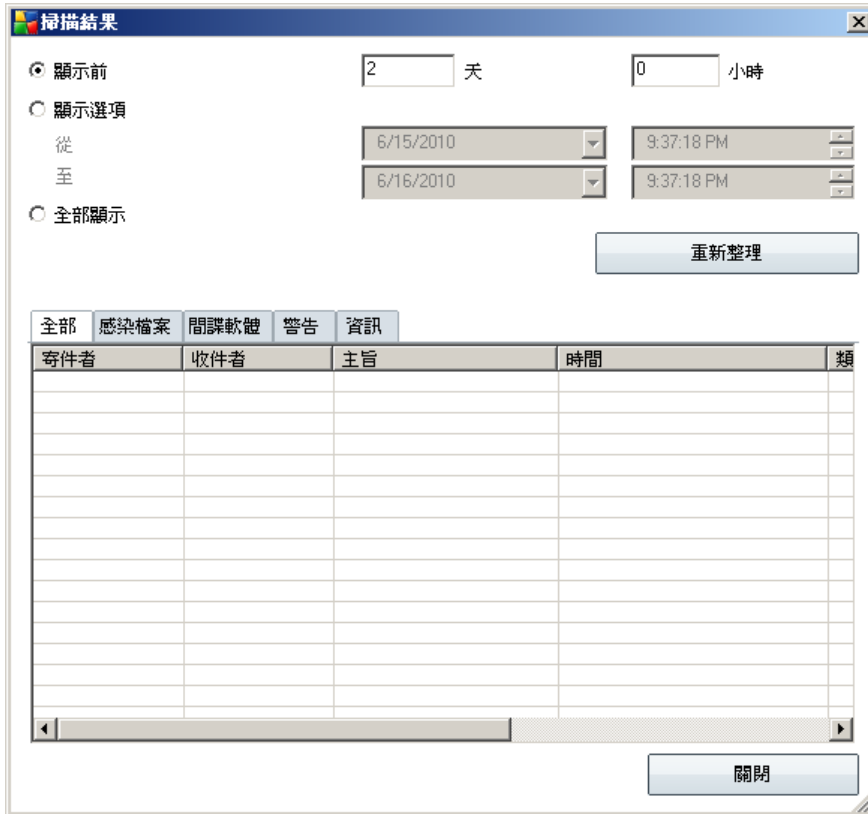
檢查儲存在使用者信箱中的所有電子郵件訊息。如果偵測到任何病毒，便會將其移至病毒隔離區，或者將其完全移除。

連接兩下需要的元件可開啓該元件的介面。除 **Anti-Spam** 外，所有其他元件都包含以下常用控制按鈕和連結：



- **掃描結果**

開啓新對話方塊，您可在此檢視掃描結果：



您可在此檢查訊息，這些訊息按嚴重性細分到數個標籤。要修改嚴重性並進行報告，請參閱個別元件的組態。

預設情況下，只顯示最近兩天的結果。您可以修改以下選項來變更顯示時間：

- **顯示最近** - 插入偏好的天數和小時數。
- **顯示選取範圍** - 選擇自訂的時間和日期間隔。
- **全部顯示** - 顯示整個時間期限內的結果。

使用 **重新整理** 按鈕可重新載入結果。

- **重新整理統計值** - 更新上面顯示的統計資料。
- **重設統計值** - 將所有統計資料重設為零。



工作按鈕如下所示：

- **設定** - 使用此按鈕可開啓元件的設定。
- **上一步** - 按此按鈕可以返回至「伺服器元件概觀」。

您可以在下面的章節中找到有關所有元件個別設定的更多資訊。

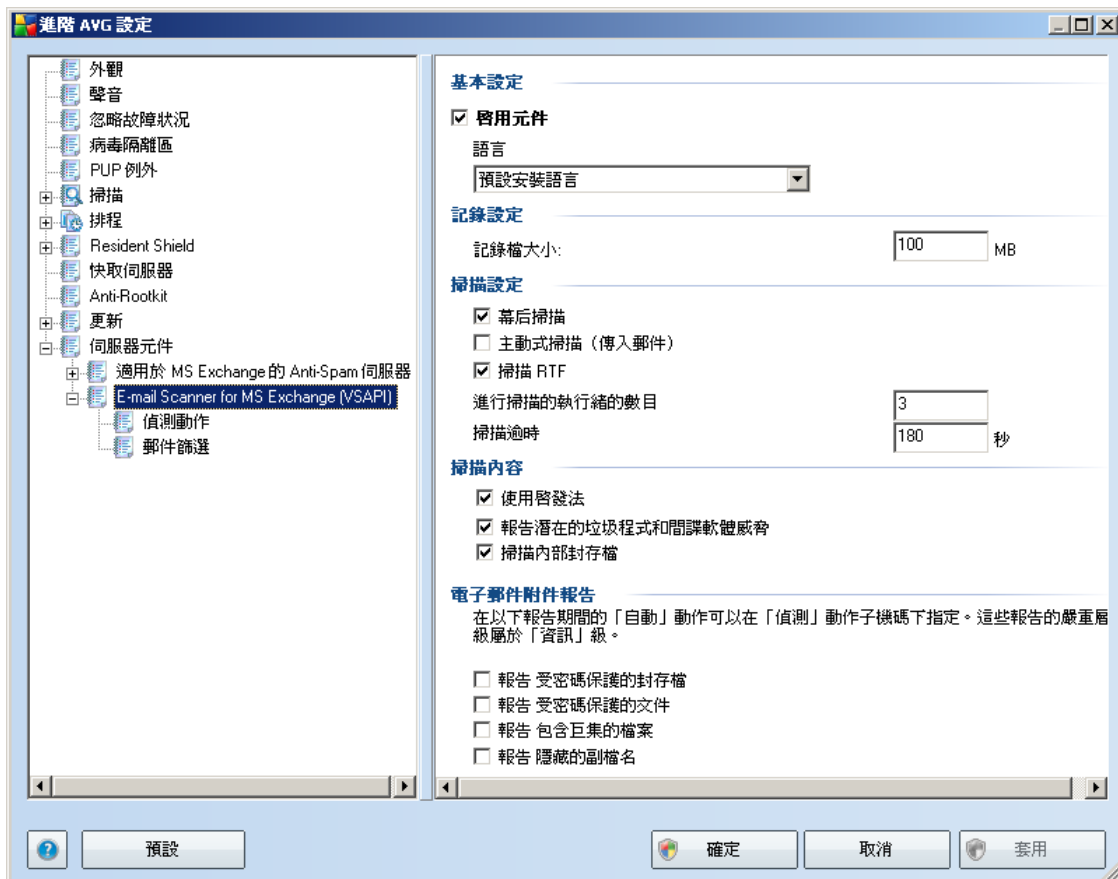
5.2. VSAPI 2.0

病毒掃描 **API 2.0** (MS Exchange 2000 Server 中提供的是 **VSAPI 2.0**) 不允許刪除受感染的電子郵件檔案。雖然受病毒感染的電子郵件附件不可以刪除，但是其檔案名稱會變更：**AVG for Exchange 2000/2003 Server** 會在原始檔案名稱末尾附加 **.virusinfo.txt** 副檔名。檔案內容將被有關已知病毒的訊息覆寫。如果直接在電子郵件訊息中發現病毒，則整個訊息內文會被內容為在此訊息中發現病毒的一條說明覆寫。

病毒掃描 **API 2.5** (*MS Exchange 2003 Server 中提供的是 VSAPI 2.5*) 也允許刪除受感染的訊息。此功能可以在 **AVG for MS Exchange 2000/2003 Server** 組態對話方塊中設定。

5.3. E-mail Scanner for MS Exchange (VSAPI)

此項目包含 **E-mail Scanner for MS Exchange (VSAPI)** 的設定。



基本設定部分包含以下選項：

- 啟用元件 - 取消選取該選項會停用整個元件。
- 語言 - 選取偏好的元件語言。

記錄設定部分：

- 記錄檔大小 - 選擇偏好的記錄檔大小。預設值：100 MB。

掃描設定部分：

- **背景掃描** - 您可以在此啓用或停用背景掃描程序。背景掃描是 VSAPI 2.0/2.5 應用程式介面的功能之一。它提供 **Exchange Messaging** 資料庫的執行緒式掃描。每當在使用者信箱資料夾中發現未使用最新的 AVG 病毒庫更新掃描的項目時，會將該項目提交至待掃描的 **AVG for Exchange 2007 Server**。然後會對未檢查過的物件並行執行掃描與搜尋兩種作業。

每個資料庫都會使用一個特定的低優先順序的執行緒，從而確保其他工作（例如，在 **Microsoft Exchange** 資料庫中儲存電子郵件訊息）永遠會優先執行。

- **主動式掃描（傳入郵件）**

您可以在此啓用或停用 VSAPI 2.0/2.5 的主動式掃描功能。當有項目傳遞到資料夾，但用戶端尚未發出要求時會執行此掃描。

一旦訊息提交到 **Exchange** 儲存區，即以低優先順序進入全域掃描佇列（最多 30 個項目）。它們基於先進先出 (FIFO) 原則掃描。如果項目仍在佇列中時被存取，則會變為高優先級。

注意：溢位訊息會繼續留在未掃描的儲存區。

注意：即使您將背景掃描和主動式掃描兩個選項都停用，當有使用者嘗試使用 MS Outlook 用戶端下載訊息時，存取時掃描程式仍處於作用中。

- **掃描 RTF** - 您可以在此指定是否要掃描 RTF 格式的檔案。
- **正在掃描的執行緒數目** - 掃描程序預設會按執行緒執行，以藉由某種程度的並行化處理來提高整體掃描效能。您可以在此處變更執行緒計數。

預設執行緒數目 = 處理器數目 × 2 + 1。

最小執行緒數目 = (處理器數目 + 1) / 2。

最大執行緒數目 = 處理器數目 × 5 + 1。

如果該值小於等於最小值或大於等於最大值，則使用預設值。

- **掃描逾時** - 一個執行緒在存取被掃描的訊息時的最大連續時間間隔（以秒計）（預設值為 180 秒）。

掃描內容部分：

- **使用啓發法** - 核取此方塊可在掃描期間啓用啓發法分析。
- **報告潛在的垃圾程式和間諜軟體威脅** - 核取此選項可報告出現的潛在垃圾程式和間諜軟體。

- **掃描封存內部** - 核取此選項可讓掃描程式也檢查封存（zip、rar 等）內的檔案。

電子郵件附件報告部分允許您選取掃描期間應報告的項目。預設組態可以在**偵測動作**部分下的**資訊**部分輕鬆進行修改（請參閱下文）。

有以下選項可用：

- **報告受密碼保護的封存**
- **報告受密碼保護的文件**
- **報告包含巨集的檔案**
- **報告隱藏的副檔名**

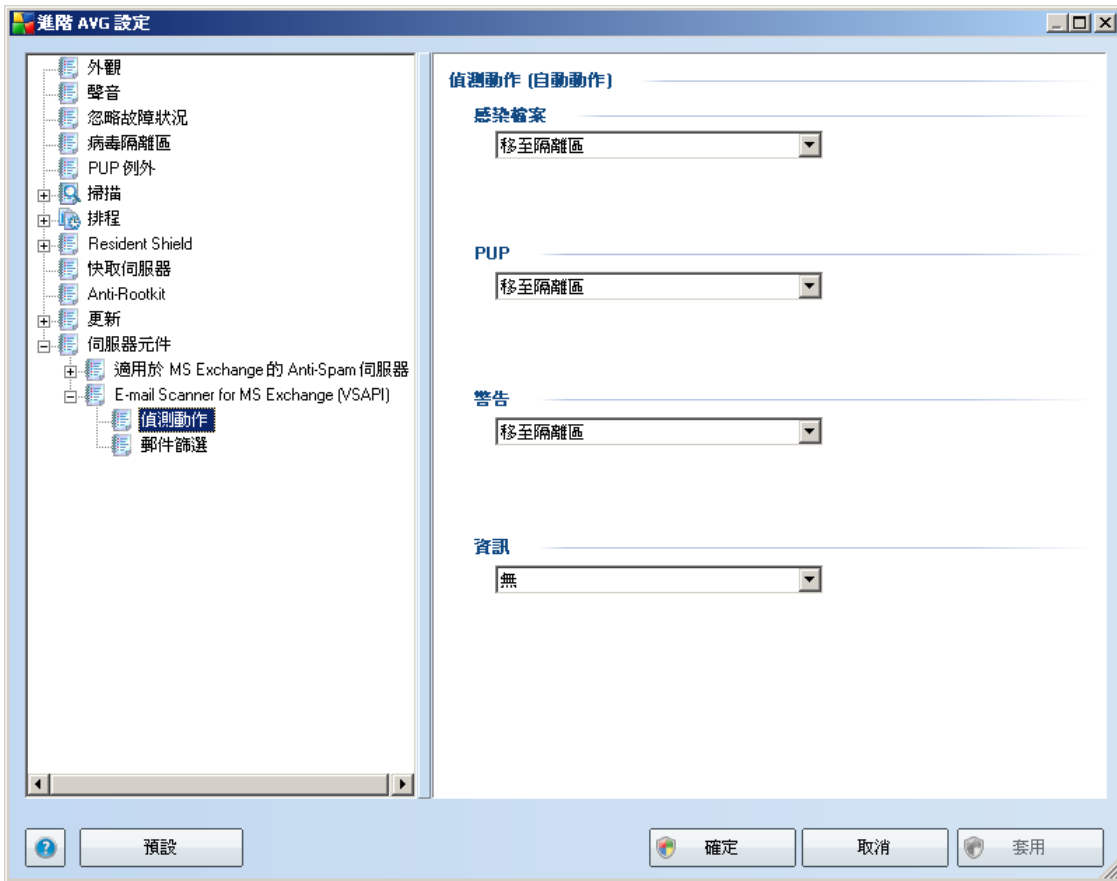
所有這些功能通常都是 Microsoft VSAPI 2.0/2.5 應用程式介面服務的使用者延伸。欲瞭解有關 VSAPI 2.0/2.5 的詳細資訊，請參閱下面的連結（以及可從參考的項目存取的連結）：

- <http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP> - 取得有關 Exchange 2000 Server Service Pack 1 中 VSAPI 2.0 的一般資訊
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> - 取得有關 Exchange 和反病毒軟體互動的資訊
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> - 取得有關 Exchange 2003 Server 應用程式中其他 VSAPI 2.5 功能的資訊。

以下樹狀結構中還提供了下列子項目：

- [偵測動作](#)
- [郵件篩選](#)

5.4. 偵測動作



在 **偵測動作** 子項目中，您可以選擇掃描期間應自動執行的動作。

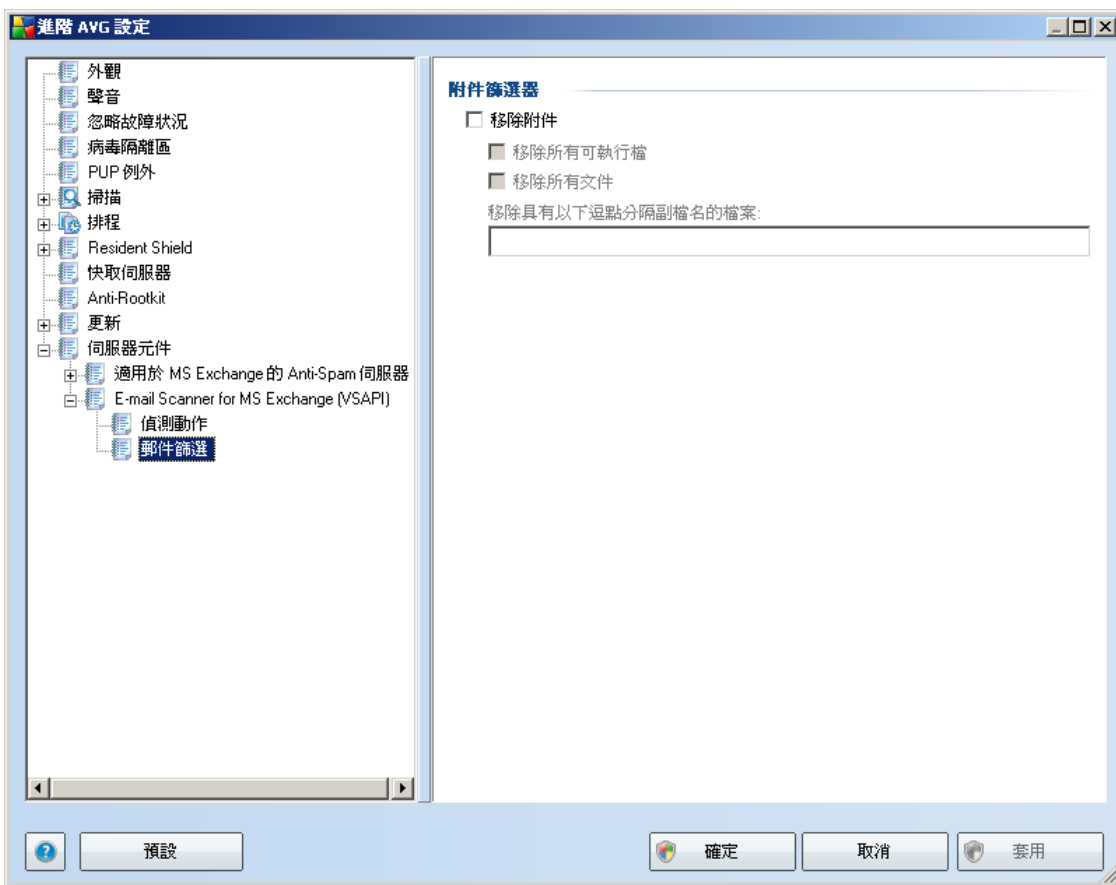
這些動作可以用於以下項目：

- 感染
- **PUP** (潛在垃圾程式)
- 警告
- 資訊

使用下拉式功能表選擇針對每個項目的動作：

- 無 - 不執行任何動作。
- 移至隔離區 - 特定的威脅將被移至病毒隔離區。
- 移除 - 特定的威脅將被移除。

5.5. 郵件篩選



在 **郵件篩選** 子項目中，您可以選擇應自動移除的附件（若有）。有以下選項可用：

- **移除附件** - 核取此方塊可啓用該該功能。
- **移除所有可執行檔** - 移除所有可執行檔。
- **移除所有文件** - 移除所有文件檔案。

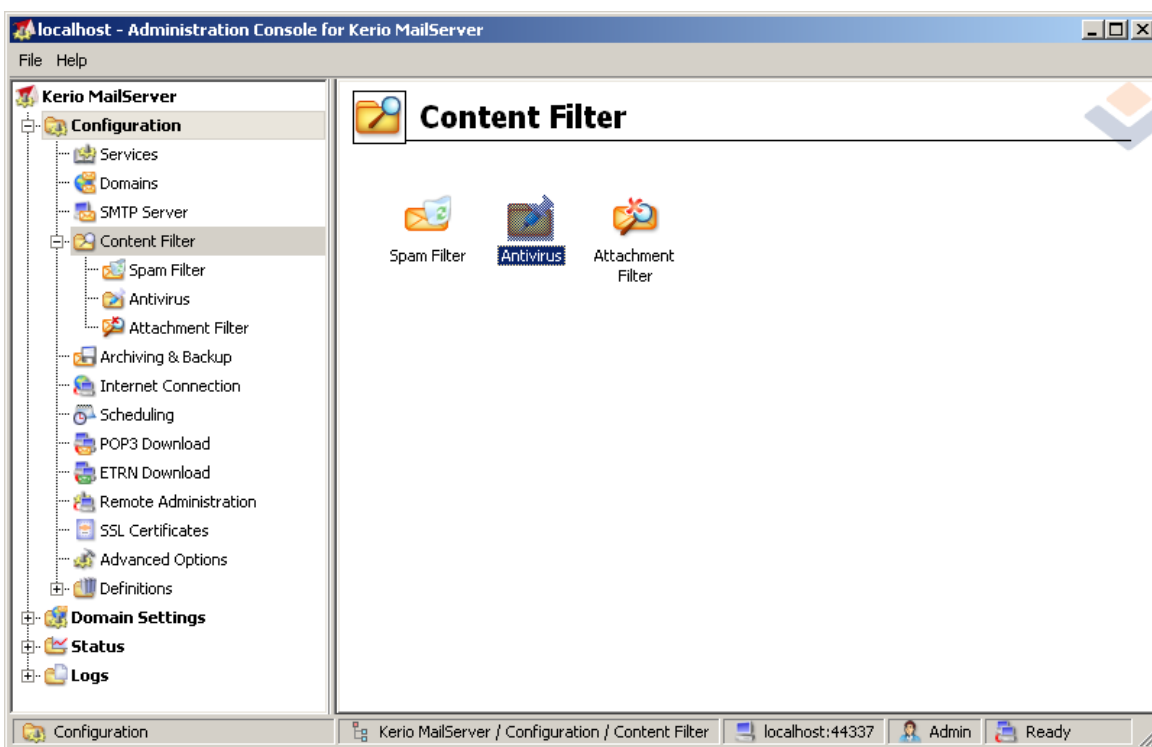


- **移除具有以下逗點分隔副檔名的檔案** - 在此方塊中填入您希望自動移除的檔案的副檔名。使用逗號分隔副檔名。

6. AVG for Kerio MailServer

6.1. 組態

該反病毒保護機制已直接整合到 Kerio MailServer 應用程式中。要啓動 AVG 掃描引擎所提供的 Kerio MailServer 電子郵件保護，請啓動 Kerio Administration Console 應用程式。在應用程式視窗左側控制樹的「組態」分支中，選擇「內容篩選器」子分支：

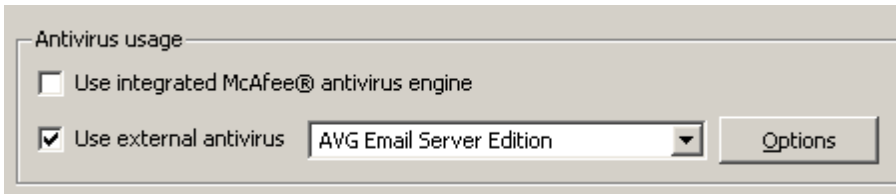


按一下「內容篩選器」項目，將顯示一個帶有三個項目的對話方塊：

- [垃圾郵件篩選器](#)
- [反病毒](#)（請參閱反病毒部分）
- [附件篩選器](#)（請參閱附件篩選器部分）

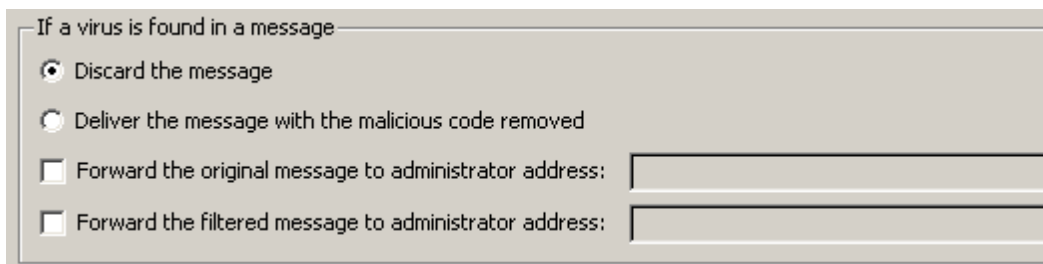
6.1.1. Antivirus

要啓動 AVG for Kerio MailServer，請選取「使用外部反病毒軟體」核取方塊，然後從組態視窗之「反病毒軟體使用」畫面的「外部軟體」功能表選擇「AVG Email Server Edition」項目：



在以下部分，您可以指定應該如何處理受感染或篩選出來的訊息：

- 如果在訊息中發現病毒



此畫面指定在訊息中偵測到病毒後或當訊息被附件篩選器篩選出以後應執行的動作：

- **捨棄訊息** - 選取此選項後，受感染或篩選出來的訊息將被刪除。
 - **移除訊息中的惡意代碼後再傳遞訊息** - 選取此選項後，訊息將傳遞至收件者，但不帶潛在有害的附件。
 - **將原始訊息轉送至管理員地址** - 選取此選項後，受病毒感染的訊息會轉送至地址文字欄位中指定的地址
 - **將篩選出來的訊息轉送至管理員地址** - 選取此選項後，篩選出來的訊息會轉送至地址文字欄位中指定的地址
- 如果訊息的一部分無法掃描（例如檔案被加密或損毀）

If a part of message cannot be scanned (e.g. encrypted or corrupted file)

Deliver the original message with a prepended warning

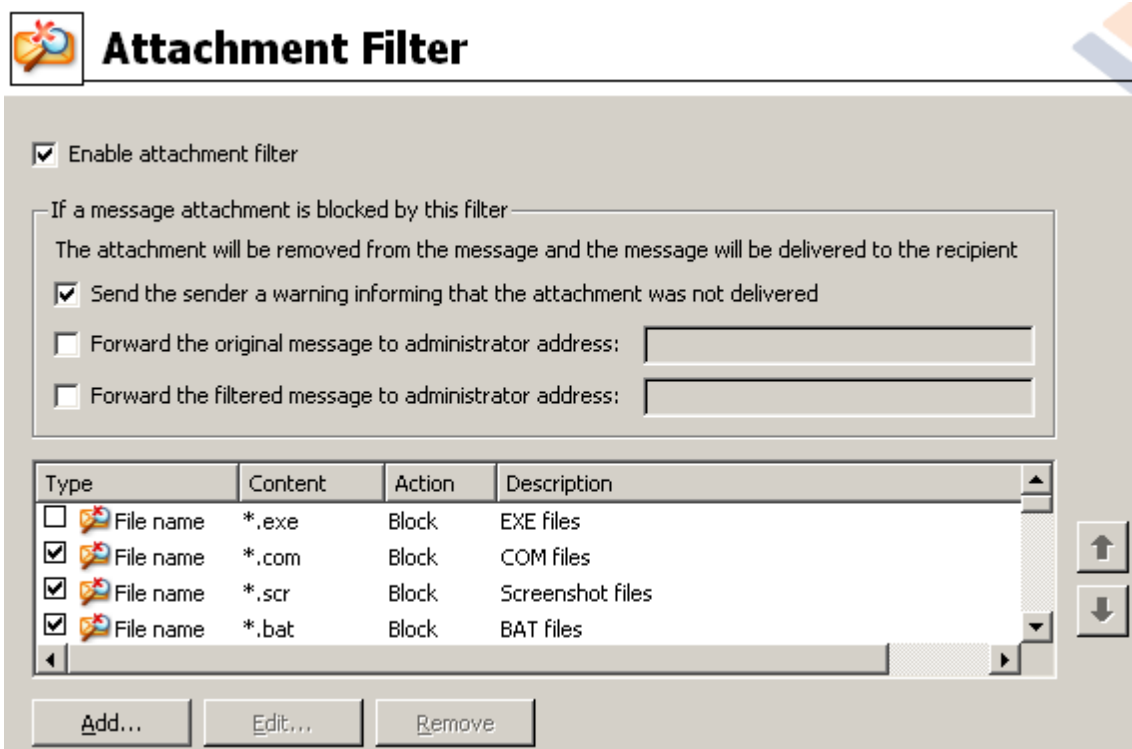
Reject the message as if it was a virus (use the settings above)

此畫面指定當訊息或附件的一部分無法掃描時應執行的動作：

- **傳遞原始訊息並附上事先警告** - 不對訊息或附件進行檢查，直接傳送。會提醒使用者，該訊息可能仍然包含病毒。
- **將訊息視為病毒並拒絕接收** - 系統會作出與偵測到病毒時相同的反應（即在不帶附件的情況下傳遞訊息，或者拒絕接收該訊息）。此選項很安全，但是傳送受密碼保護的封存幾乎是不可能的。

6.1.2. 附件篩選器

「附件篩選器」功能表提供了各種附件定義的清單：



Attachment Filter

Enable attachment filter

If a message attachment is blocked by this filter

The attachment will be removed from the message and the message will be delivered to the recipient

Send the sender a warning informing that the attachment was not delivered

Forward the original message to administrator address:

Forward the filtered message to administrator address:

Type	Content	Action	Description
<input type="checkbox"/>	File name *.exe	Block	EXE files
<input checked="" type="checkbox"/>	File name *.com	Block	COM files
<input checked="" type="checkbox"/>	File name *.scr	Block	Screenshot files
<input checked="" type="checkbox"/>	File name *.bat	Block	BAT files

您可以透過選取「啓用附件篩選器」核取方塊，啓用或停用郵件附件篩選。如有需

要，您可以變更以下設定：

- **向寄件者傳送附件未傳遞警告**

寄件者將收到來自 Kerio MailServer 的以下警告：他/她所傳送的訊息包含病毒或被封鎖的附件。

- **將原始訊息轉寄至管理員地址**

訊息將（按原樣 - 帶有受感染或禁止的附件）轉寄至之前定義的電子郵件地址，無論是本機地址還是外部地址。

- **將篩選出來的訊息轉寄至管理員地址**

訊息將（除下面選取的動作之外）轉寄至指定的電子郵件地址，不帶受感染或禁止的附件。這可用來驗證反病毒功能和/或附件篩選器是否正常運作。

在副檔名清單中，每個項目有四個欄位：

- **類型** - 透過「內容」欄位中提供的副檔名確定的附件種類。可能的類型包括檔案名稱或 MIME 類型。您可以選取此欄位下相應的方塊，以將項目包括到附件篩選中或從中排除。
- **內容** - 可以在此處指定要篩選的副檔名。您可以在此處使用作業系統萬用字元（例如字符串 `*.doc.*` 代表任何帶有 `.doc` 副檔名的檔案，後接任何其他副檔名）。
- **動作** - 定義要對某個特定附件執行的動作。可能的動作包括「接受」（接受附件）和「封鎖」（將執行在停用附件清單上方定義的動作）。
- **說明** - 附件的說明在此欄位中定義。

按「移除」按鈕可以將項目從清單中移除。按**新增...** 按鈕可以將另一個項目新增到清單。或者，您也可以按**編輯...** 按鈕編輯現有記錄。然後會出現以下視窗：



- 在「說明」欄位中，您可以為要篩選的附件填寫簡短說明。
- 在「如果郵件訊息包含附件」欄位中，您可以選取附件類型（檔案名稱或 **MIME** 類型）。您還可以從提供的副檔名清單中選擇某個特定的副檔名，您也可以直接輸入副檔名萬用字元。

在「則」欄位中，您可以決定是封鎖定義的附件還是接受該附件。

7. Anti-Spam 組態

7.1. Anti-Spam 介面



您將在 *伺服器元件* 部分 (左側功能表) 看到 **Anti-Spam** 伺服器元件對話方塊。該對話方塊包含有關伺服器元件功能的簡要資訊及其目前狀態的資訊 (*Anti-Spam Server for MS Exchange 元件處於作用中*)，以及一些統計資料。

可用連結：

- [掃描結果](#)

開啓一個新的對話方塊，您可在其中查看反垃圾郵件掃描結果：



您可在此處查看被偵測為垃圾郵件（來路不明的訊息）或有網路釣魚意圖（企圖竊取您的個人資料、銀行帳戶詳細資訊或身份等）的郵件。預設情況下，僅會顯示最近兩天內的掃描結果。您可以透過修改以下選項來變更顯示的期限：

- **顯示前** - 輸入希望的天數和小時數。
- **顯示選取範圍** - 選擇自訂的時間和日期間隔。
- **顯示全部** - 顯示整個時間期間的掃描結果。

使用**重新整理**按鈕可重新載入掃描結果。

- **重新整理統計值** - 更新以上顯示的統計值。
- **重設統計值** - 將所有統計值重設為零。

工作按鈕如下所示：

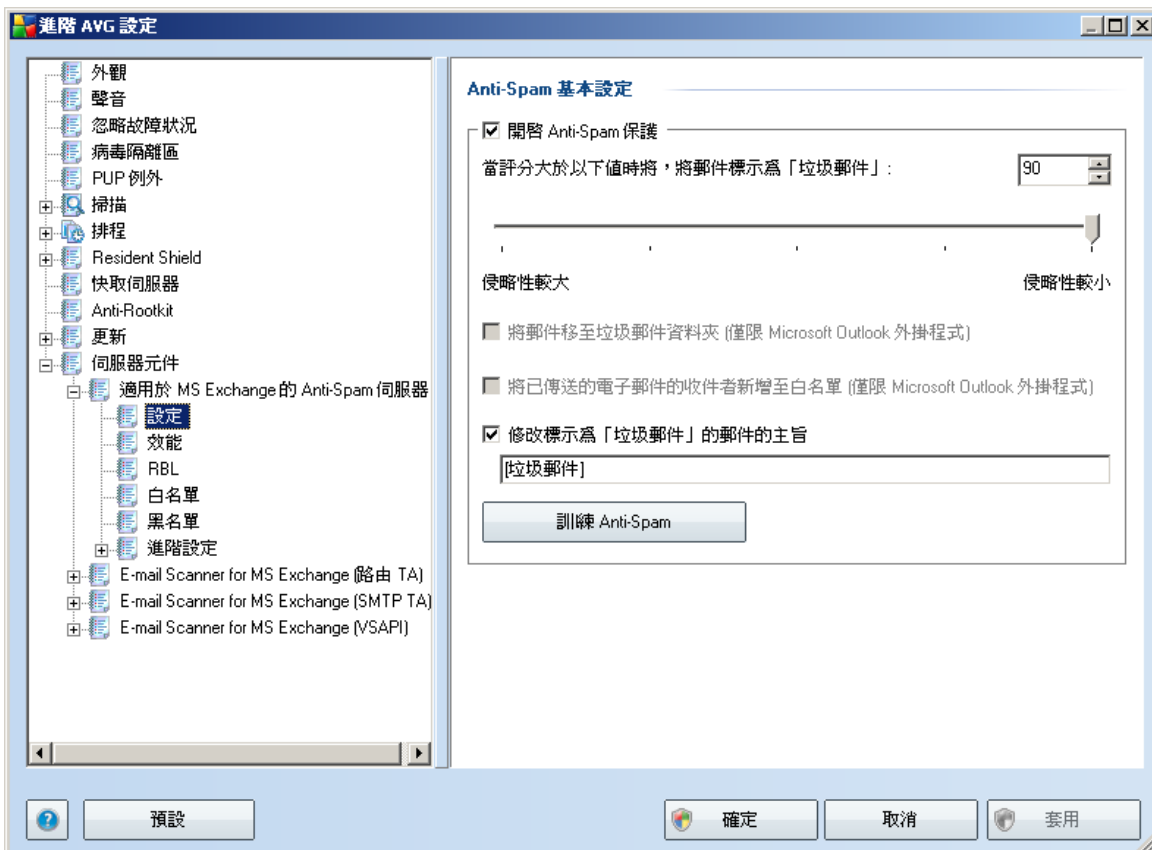
- **設定** - 使用此按鈕可開啓 [Anti-Spam 設定](#)。
- **上一步** - 按下此按鈕可返回至「伺服器元件概觀」。

7.2. Anti-Spam 原理

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

Anti-Spam 會檢查所有傳入電子郵件訊息，並將來路不明的電子郵件標示為垃圾郵件。它會使用多種分析方法來處理每一封電子郵件訊息，從而提供最大的保護來封鎖垃圾電子郵件訊息。

7.3. Anti-Spam 設定



在 **Anti-Spam 基本設定** 對話方塊中，您可以核取 **開啓 Anti-Spam 保護** 核取方塊，以允許/禁止對電子郵件通訊進行反垃圾郵件掃描。

在此對話方塊中，您也可以選取更高或更低的加強分數標準。**Anti-Spam** 篩選器會根據數個動態掃描技術，為每封郵件指定一個分數（即郵件內容與垃圾郵件的相似程度）。您可以調整當評分大於等於以下值時，將郵件標示為垃圾郵件設定，方法是輸入值（0 到 100），或左右移動滑杆（使用滑杆時，值的範圍限制為 50 到 90）。

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

- **值 90-99** - 大部分的傳入電子郵件訊息都能正常傳遞（不會被標示為垃圾郵件）。這樣會篩選出最容易識別的垃圾郵件，但是可能會允許大量的垃圾郵件傳入。
- **值 80-89** - 將篩選出很可能是垃圾郵件的電子郵件訊息。某些非垃圾郵件的訊息也可能被誤選。
- **值 60-79** - 這是較為加強的組態。可能是垃圾郵件的電子郵件訊息都將被篩選出來。非垃圾郵件的訊息也很可能被誤判。
- **值 1-59** - 特別加強的組態。非垃圾郵件的電子郵件訊息很可能被當作真正的垃圾郵件訊息處理。一般情況不建議使用此閾值範圍。
- **值 0** - 在此模式中，您只能接收到來自您的白名單中之寄件者的電子郵件訊息。任何其他電子郵件訊息都會被視為垃圾郵件。一般情況不建議使用此閾值範圍。

您可以進一步定義應該如何處理偵測到的垃圾電子郵件訊息：

- **修改標示為垃圾郵件的郵件主旨** - 如果您希望所有偵測為垃圾郵件的訊息都在電子郵件主旨欄位標明特定文字或字元，請勾選此核取方塊；可在啟動的文字欄位中輸入所需文字。

訓練 Anti-Spam 按鈕開啓 **Anti-Spam 訓練精靈**，[下一章](#)會詳加解說。

7.3.1. Anti-Spam 訓練精靈

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



有以下選項可供選擇：

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

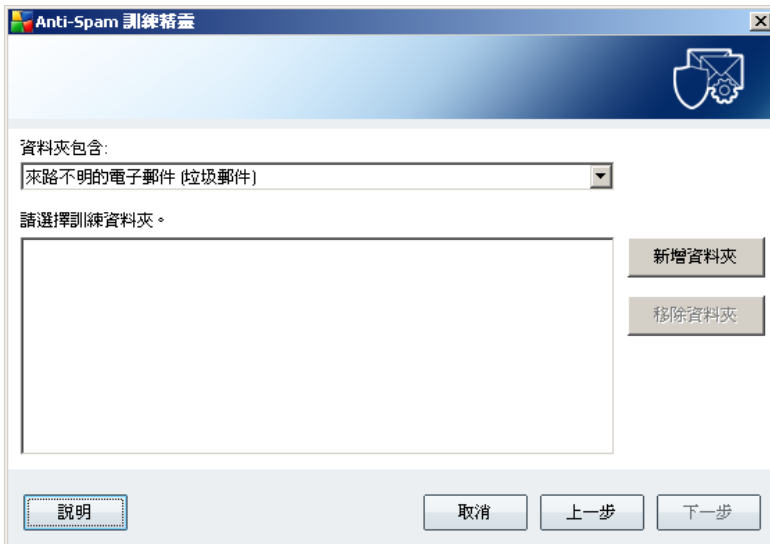
若想讓訓練程序更加快速和方便，提前將資料夾中的電子郵件排序是個不錯的主意，這樣您要用於訓練的資料夾就只包含訓練郵件（要麼是需要的郵件，要麼是垃圾郵件）。但是，這不是一個必要步驟，因為您稍後可以篩選電子郵件。

選取適當的選項，然後按**下一步**繼續執行精靈。

7.3.2. 選取含郵件的資料夾

在此步驟中顯示的對話方塊取決於您之前的選擇。

存放 EML 檔案的資料夾



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

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

完成後，按一下 **下一步**，前進到 [郵件篩選選項](#)。

特定電子郵件用戶端

一旦您確認其中一個選項，便會出現一個新的對話方塊。

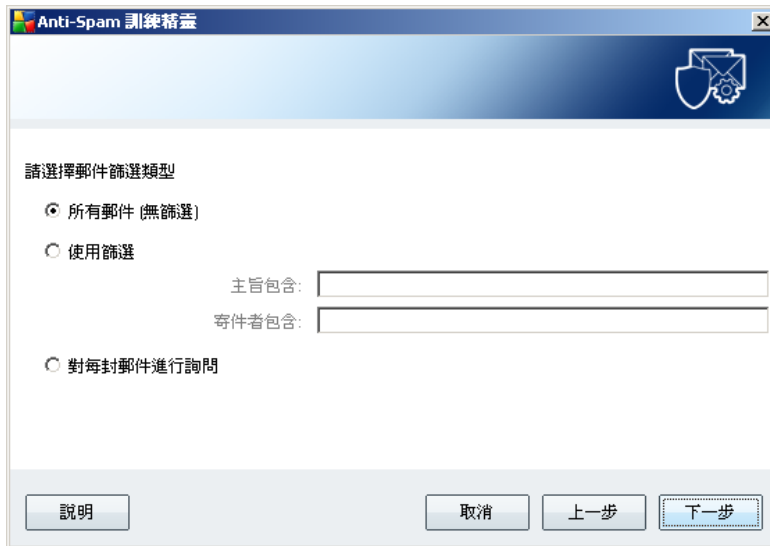


請注意：如果使用的是 *Microsoft Office Outlook*，則會提示您先選取 *MS Office Outlook* 設定檔。

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

完成後，按一下 **下一步**，前進到 [郵件篩選選項](#)。

7.3.3. 郵件篩選選項



在此對話方塊中，您可以設定篩選電子郵件訊息。

如果您確定所選資料夾只包含要用於訓練的郵件，請選取**所有郵件 (無篩選)**選項。

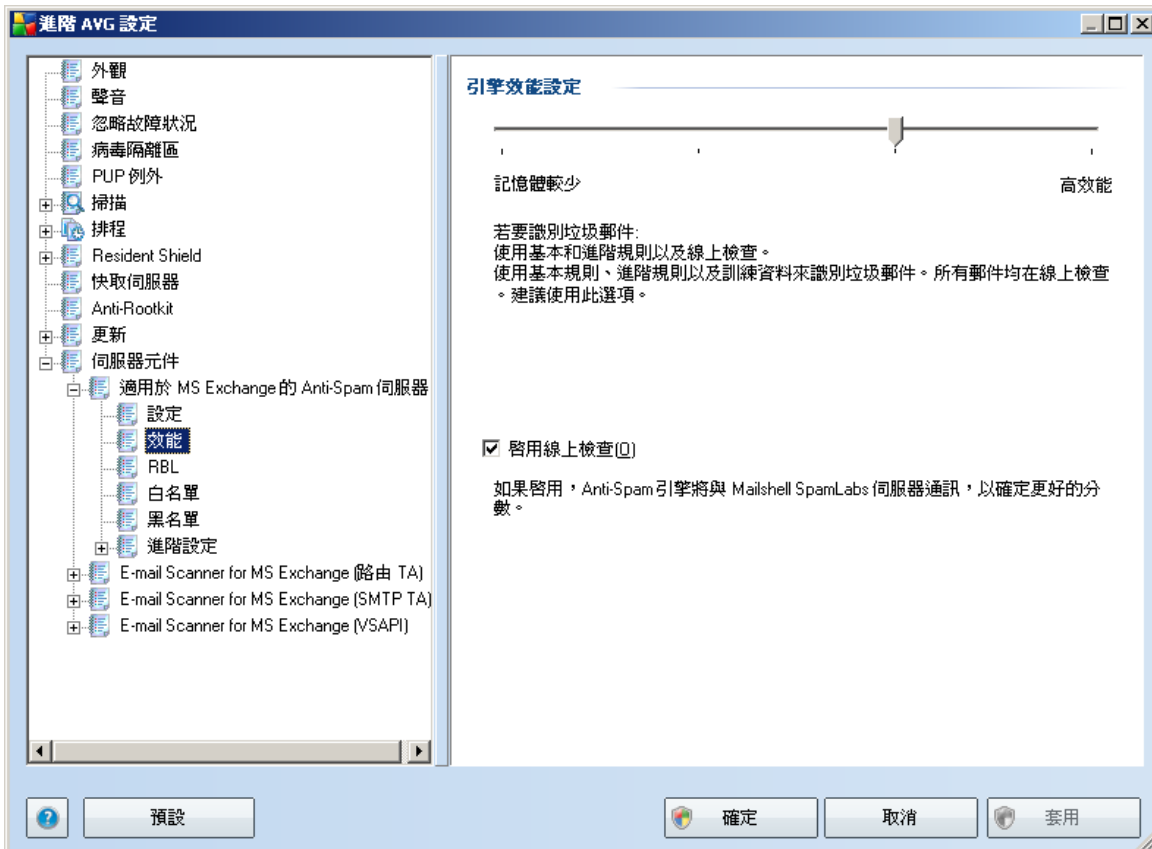
如果您不確定資料夾中包含的郵件，並且想要讓精靈針對每封郵件提出詢問（這樣您就可以確定是否要將此郵件用於訓練），請選取**針對每封郵件提出詢問**選項。

如需更為進階的篩選功能，請選取**使用篩選**選項。您可以在電子郵件主旨和/或寄件者欄位填入要搜尋的詞語（**名稱**）、詞語的一部分或片語。與輸入標準完全相符的所有郵件都將用於訓練，不會給出進一步提示。

注意！：若兩個文字欄位都有填寫，只符合兩個條件之一的地址也會被使用！

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

7.4. 效能



引擎效能設定對話方塊 (可透過左側巡覽的效能項目連結) 提供了 **Anti-Spam** 元件效能設定。向左或向右移動滑杆，可在低記憶體/高性能模式範圍之間變更掃描效能層級。

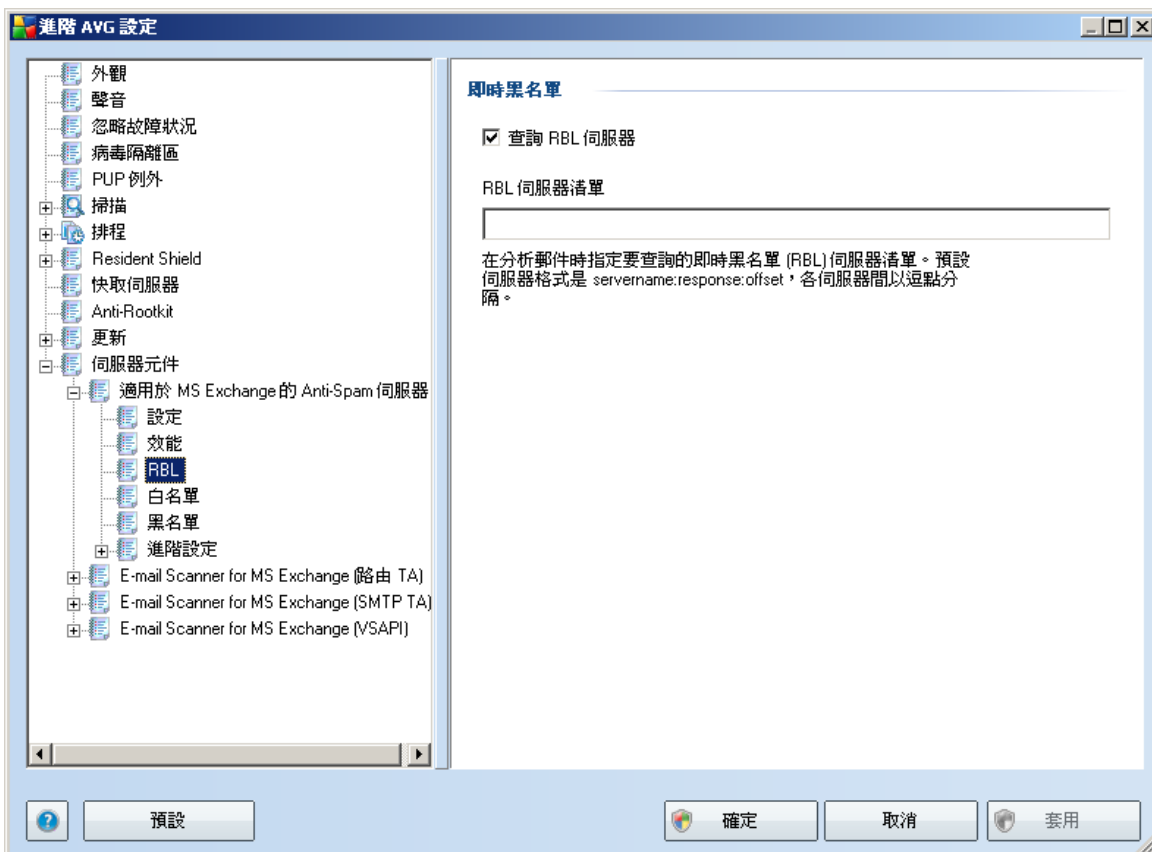
- **低記憶體** - 在識別垃圾郵件的掃描過程中，將不使用任何規則。將只使用訓練資料進行識別。此模式不推薦作為一般用途，除非電腦硬體狀況確實較差。
- **高性能** - 此模式將使用大量記憶體。在識別垃圾郵件的掃描過程中，將使用以下功能：規則和垃圾郵件資料庫快取、基本和進階規則、垃圾郵件發信者 IP 位址以及垃圾郵件發信者資料庫。

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

通常建議保留預設設定，僅在確實有必要時才進行變更。對此組態的任何變更只能由有經驗的使用者來進行！

7.5. RBL

RBL 項目會開啓一個名爲*即時黑名單*的編輯對話方塊：



您可在此對話方塊中開啓/關閉*查詢 RBL 伺服器*功能。

RBL (即時黑名單) 伺服器是帶有強大的已知垃圾郵件寄件者資料庫的 **DNS** 伺服器。開啓該功能時，將根據 **RBL** 伺服器資料庫驗證所有電子郵件訊息，若發現與資料庫中的任何項目相同，則會將其標示爲[垃圾郵件](#)。

RBL 伺服器資料庫包含最新垃圾郵件指紋，因此可提供最佳和最爲準確的[垃圾郵件](#)偵測。對於收到大量 **Anti-Spam** 引擎一般無法偵測出的垃圾郵件的使用者而言，此功能非常有用。

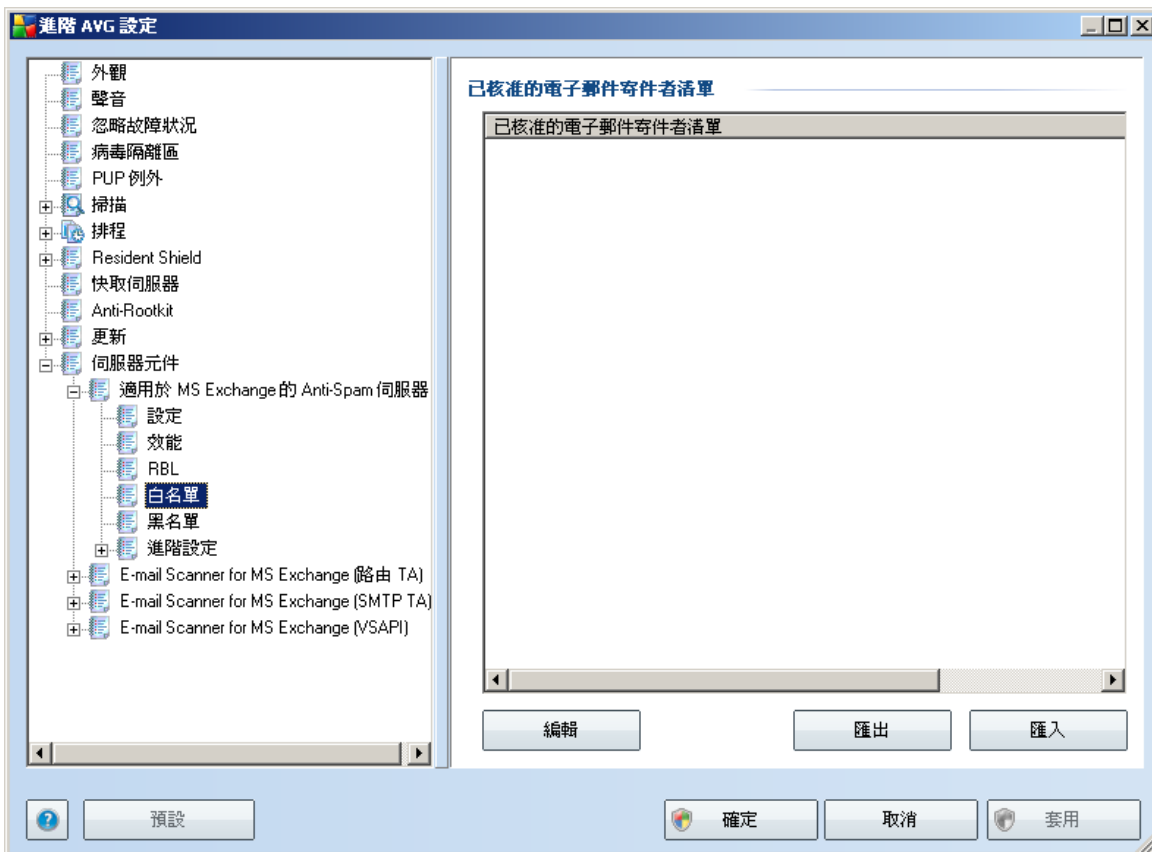
RBL 伺服器清單允許您定義特定 RBL 伺服器位置。預設情況下，會指定兩個 RBL 伺服器位址。我們建議保留預設設定，除非您是有經驗的使用者並且確實需要變更這些設定！

*注意：*對於某些系統和組態，此功能的啓用可能會減緩電子郵件接收程序的速度，因為每封郵件都必須根據 RBL 伺服器資料庫進行驗證。

不會將個人資料傳送至伺服器！

7.6. 白名單

白名單項目會開啓一個對話方塊，其中包含已批准的寄件者電子郵件地址和網域名稱的全域清單，來自這些地址的郵件將始終不會被標示為[垃圾郵件](#)。



在編輯介面中，您可以制作一份確定永遠不會傳送來路不明的郵件 ([垃圾郵件](#)) 的寄件者清單。您也可以製作一份您知道不會產生垃圾郵件的完整網域名稱 (例如 [avg.com](#)) 清單。

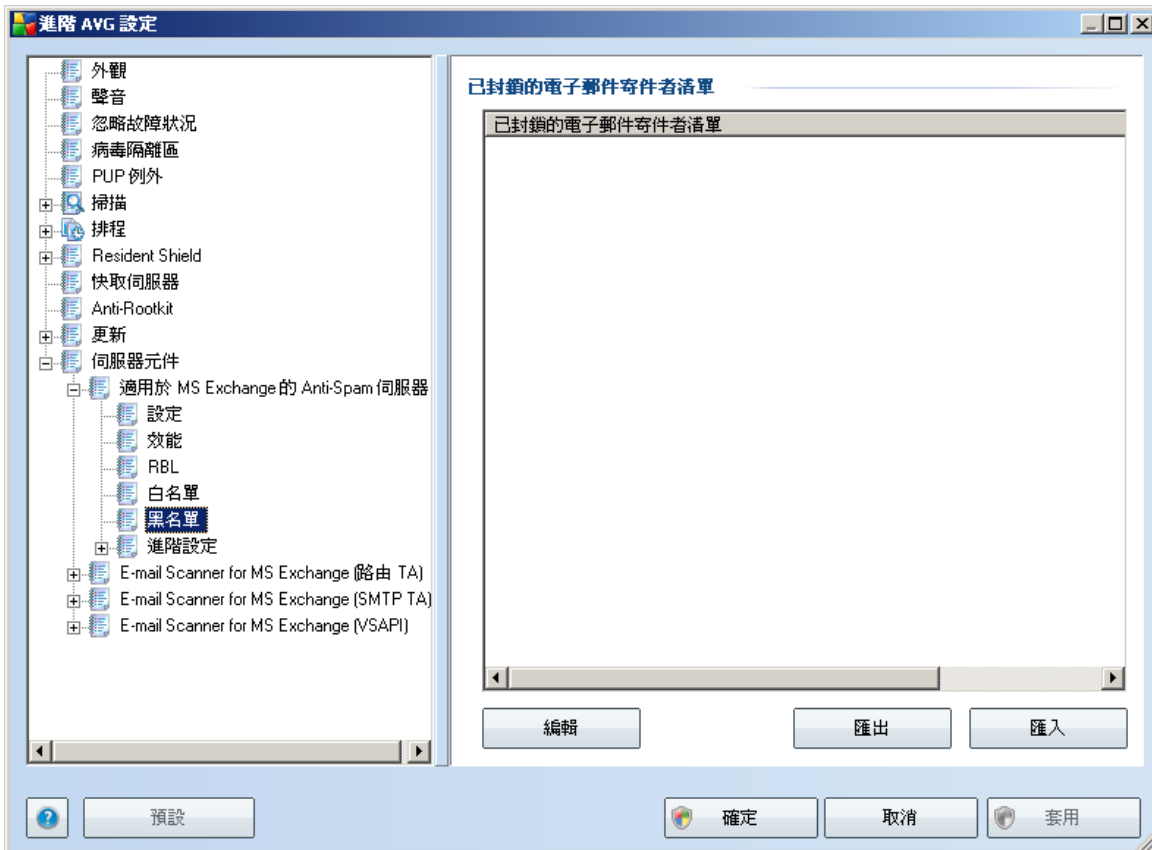


準備好這類寄件者和/或網域名稱清單之後，您可以使用下列任一方法將其輸入清單：直接輸入各個電子郵件地址或一次性匯入整份地址清單。可用的控制按鈕如下：

- **編輯** - 按下此按鈕會開啓一個對話方塊讓您手動輸入地址清單 (您也可以使用複製和貼上)。每一行插入一個項目 (寄件者、網域名稱)。
- **匯入** - 如果您已經準備好電子郵件地址/網域名稱的文字檔案，只需按下此按鈕即可直接匯入檔案。輸入檔案必須是純文字格式，且內容中的每行只能包含一個項目 (地址、網域名稱)。
- **匯出** - 如果您基於某種原因決定匯出記錄，您可以按此按鈕執行。所有記錄都將儲存成純文字檔。

7.7. 黑名單

黑名單項目會開啓一個對話方塊，其中包含封鎖的寄件者電子郵件地址與網域名稱的全域清單，來自此清單中寄件者的訊息將總是被標示為[垃圾郵件](#)。



在編輯介面中，您可以制作一份預期會寄送來路不明郵件 ([垃圾郵件](#)) 的寄件者清單。也可以編譯一份您預期或收到過垃圾郵件的完整網域名稱的清單 (例如，[spammingcompany.com](#))。來自其中列出的地址/網域的所有電子郵件都會被識別成垃圾郵件。

準備好這類寄件者和/或網域名稱清單之後，您可以使用下列任一方法將其輸入清單：直接輸入各個電子郵件地址或一次性匯入整份地址清單。可用的控制按鈕如下：

- **編輯** - 按下此按鈕會開啓一個對話方塊讓您手動輸入地址清單 (您也可以使用複製和貼上)。每一行插入一個項目 (寄件者、網域名稱)。

- **匯入** - 如果您已經準備好電子郵件地址/網域名稱的文字檔案，只需按下此按鈕即可直接匯入檔案。輸入檔案必須是純文字格式，且內容中的每行只能包含一個項目（地址、網域名稱）。
- **匯出** - 如果您基於某種原因決定匯出記錄，您可以按此按鈕執行。所有記錄都將儲存成純文字檔。

7.8. 進階設定

通常，建議保留預設設定，僅在確有必要時才進行變更。任何組態變更都只能由有經驗的使用者來進行！

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

- **快取** - 指紋、網域名聲、LegitRepute
- **訓練** - 最大輸入字數、自動訓練閾值、比重
- **篩選** - 語言清單、國家(地區)清單、已批准的 IP、已封鎖的 IP、已封鎖的國家(地區)、已封鎖的字元集、冒名的寄件者
- **RBL** - RBL 伺服器、多個結果、閾值、逾時、最大 IP 數
- **網際網路連線** - 逾時、代理伺服器、代理伺服器驗證

8. AVG 設定管理員

AVG 設定管理員是一款主要適用於小型網路的工具，可讓您複製、編輯和分配 AVG 組態。該組態可以儲存到可攜式裝置（如 USB 快閃磁碟機等），然後手動套用至所選站點。

此工具包括在 AVG 安裝中，可從 Windows 的「開始」功能表使用：

所有程序/AVG 9.0/AVG 設定管理員



- **編輯此電腦的 AVG 組態**

使用此按鈕可以開啓帶有您本機 AVG 進階設定的對話方塊。在此處進行的所有變更也會反映到本機安裝的 AVG。

- **載入和編輯 AVG 組態檔**

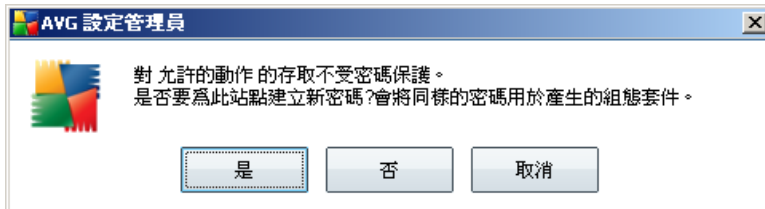
如果您已擁有 AVG 組態檔 (.pck)，使用此按鈕可開啓該檔案進行編輯。按**確定**或**套用**確認所做的變更後，該檔案將被新設定替換！

- **將檔案中的組態套用至此電腦上的 AVG**

使用此按鈕可以開啓 AVG 組態檔 (.pck) 並將其套用至本機安裝的 AVG。

- 將本機 **AVG** 組態儲存到檔案

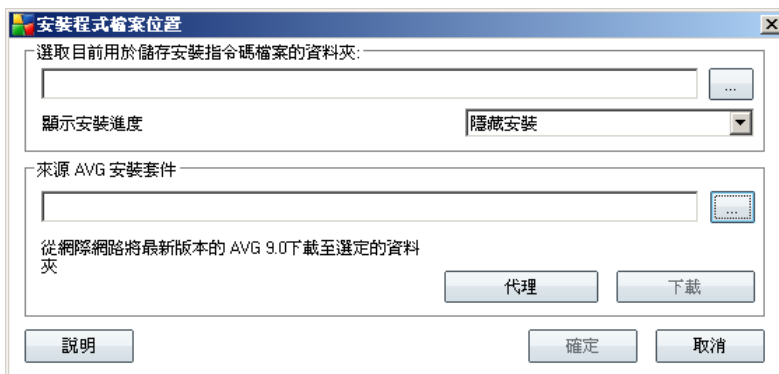
使用此按鈕可以儲存本機安裝的 **AVG** 組態檔 (.pck)。如果您沒有為允許的動作設定密碼，可能會出現以下對話方塊：



回答 *是*，此時您希望為允許的項目設定存取密碼，然後填寫必要的資訊並確認您的選擇。回答 *否* 則跳過密碼設定，並繼續將本機 **AVG** 組態儲存到檔案。

- 複製 **AVG** 安裝

此選項允許您透過使用自訂選項建立安裝套件來製作完全相同的本機 **AVG** 安裝副本。請先選取儲存安裝指令碼的資料夾以繼續。



然後從下拉式功能表中選取以下其中一項：

- **隱藏安裝** - 安裝過程中不顯示任何資訊。
- **僅顯示安裝進度** - 安裝不需要使用者執行任何動作，但會清楚顯示安裝進度。
- **顯示安裝精靈** - 安裝過程可見，並且需要使用者手動確認所有步驟。

使用 **下載** 按鈕直接從 **AVG** 網站將可用的最新 **AVG** 安裝套件下載到選定的資料夾，或者手動將 **AVG** 安裝套件放到該資料夾。



您可以使用 *代理* 按鈕定義代理伺服器設定（如果您的網路需要此設定才能成功連線）。

按一下 *確定* 後，複製程序開始，並且應很快完成。也可能會顯示一個對話方塊，詢問是否要為允許的項目設定密碼（見上文）。完成後，**AvgSetup.bat** 以及其他一些檔案應出現在所選的資料夾中。如果執行 **AvgSetup.bat** 檔案，它會根據上面所選的參數安裝 AVG。



9. 常見問題集和技術支援

如果您對 AVG 有任何業務或技術上的疑問，請參閱 AVG 網站 <http://www.avg.com> 上的 *常見問題集* 部分。

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。