Avira Internet Security
使用手冊

AVIRA

商標與著作權

商標

Windows 是 Microsoft Corporation 在美國與其他國家的註冊商標。
其餘所有品牌與產品名稱皆為各自擁有者的商標或註冊商標。
本手冊中未標示受保護的商標。 不過，這並不表示您可以自由使用這些商標。

著作權資訊

Avira Internet Security 使用之代碼由第三方供應商提供。 感謝著作權擁有者提供可用的代碼供我們運用。
如需著作權詳細資訊，請參閱 Avira Internet Security 程式說明中的「第三方授權」。

目錄表

1. 簡介

Avira
產品可保護您的電腦免於各種病毒、蠕蟲、特洛伊木馬程式、廣告軟體與間諜軟體的入侵。
在本手冊中，這些通常稱為病毒或惡意程式碼 (有害軟體) 及有害程式。

本手冊說明程式安裝與操作方式。

如需詳細選項及資訊，請造訪我們的網站：
http://www.avira.tw

Avira 網站可讓您：

- 存取其他 Avira 桌面程式的資訊
- 下載最新的 Avira 桌面程式
- 下載最新的 PDF 格式產品手冊
- 下載免費支援與修復工具
- 使用我們的全方位知識庫及常見問題集進行疑難排解
- 獲得特定國家的支援。

Avira 團隊敬上

1.1 圖示與強調樣式

下列為使用的圖示：

圖示/指定	說明
✓	如果必須先滿足某項條件才能執行動作時，會放置此圖示。
▸	在您執行某項動作步驟前，會放置此圖示。

↪	在上一個動作之後發生的事件之前，會放置此圖示。
警告	在出現重要資料遺失警告前，會放置此圖示。
注意	放置在有利於使用 Avira 產品的特別重要資訊或提示的連結之前。

下列為使用的強調樣式：

強調樣式	說明
斜體	檔名或路徑資料。
	顯示的軟體介面元素 (例如視窗區段或錯誤訊息)。
粗體	可按下的軟體介面元素 (例如功能表項目、瀏覽區域、選項方塊或按鈕)。

2. 產品資訊

本章包含購買與使用 Avira 產品的所有相關資訊：

- 請參閱下列章節： 提供的功能
- 請參閱下列章節： 系統需求
- 請參閱下列章節： 授權與升級
- 請參閱下列章節：授權管理員

Avira
產品內含完整、彈性的工具，可供您放心地用來保護電腦免於各種病毒、惡意程式碼、有害程式與其他危險的入侵。

▸ 請注意下列資訊：

警告
遺失寶貴的資料通常會帶來無法想像的後果。
即使是最佳的病毒防護程式也無法提供百分之百的資料遺失防護。 定期複製 (Backup) 資料以策安全。

注意
要可靠且有效地防範病毒、惡意程式碼、有害程式與其他危險，必須使用最新的程式方能奏效。 請務必使用自動更新將 Avira 產品維持在最新狀態。
請依據需求設定程式。

2.1 提供的功能

您的 Avira 產品擁有下列功能：

- 用於監視、管理與控制整個程式的控制中心
- 透過使用者友善標準與進階選項和即時線上說明來集中設定

- Scanner (指定掃描)
  搭配由設定檔控制且可設定的掃描，可掃描所有已知的病毒和惡意程式碼類型
- 與 Windows Vista 使用者帳戶控制的整合可讓您執行需要系統管理員權限的工作
- Real-Time Protection (即時掃描) 可持續監視所有檔案存取活動
- ProActiv 元件可永久監視程式動作 (只適用於 32 位元系統)
- Mail Protection (POP3 掃描程式、IMAP 掃描程式 及 SMTP 掃描程式)
  用於永久檢查電子郵件是否有病毒與惡意程式碼，其中包括檢查電子郵件附件
- Avira SearchFree Toolbar
  是一套整合至網頁瀏覽器的搜尋工具列，提供快速且便利的搜尋選項。
  其中也包括最常見的網際網路功能小程式。
- Web Protection 用於監控使用 HTTP 通訊協定從網際網路傳輸的資料與檔案
  (監控連接埠 80、8080、3128)
- 家長監護元件可依據不同的角色，篩選不適當的網站及限制網際網路的使用。
- Avira Free Android Security 應用程式不僅著重在防盜措施，
  還能協助您在遺失後或在更糟的情況下取回行動裝置：遭竊。
  此外，您還可以利用應用程式封鎖撥入通話與簡訊。 Avira Free Android Security
  可以保護執行 Android 作業系統的手機和智慧型手機。
- Backup 元件可為您的資料建立備份 (鏡像備份)
- 可隔離與處理可疑檔案的整合式隔離區管理
- Rootkits Protection 用於偵測安裝在您電腦系統中的隱藏惡意程式碼 (rootkit)
  (不適用於 Windows XP 64 位元)
- 可透過網際網路，針對偵測到的病毒與惡意程式碼直接存取其詳細資訊
- 經由網際網路上的網路伺服器，以單一檔案更新或增量 VDF
  更新方式，簡單、快速地更新程式、病毒定義與搜尋引擎
- 授權管理員中使用者友善的授權方式
- 整合式排程管理員可規劃單次或重複性工作，例如更新或掃描

- 透過創新的掃描技術
  (掃描引擎，包括啟發式掃毒)，達到極高的病毒與惡意程式碼偵測水準
- 可偵測所有典型的封存類型，包括偵測巢狀式封存與智慧副檔名偵測
- 高效能的多執行緒功能 (同時高速掃描多個檔案)
- FireWall
  可保護您的電腦免於透過網際網路或另一個網路的未授權存取，並防範未授權使用者對網際網路或內部網路進行未授權存取

2.2 系統需求

系統需求如下所示：

- 一台具備至少 Pentium 或以上處理器的電腦，速度為 1 GHz
- 作業系統
  - Windows XP，最新 SP (32 或 64 位元) 或
  - Windows 7，最新 SP (32 或 64 位元)

> 注意
> Avira Internet Security 目前正在 Windows 8 中進行認證。

- 至少 150 MB 的可用硬碟記憶體空間 (如果使用 [隔離區]
  做為暫存區域的話，就需要更多記憶體)
- Windows XP 環境下至少需要 512 MB 記憶體
- Windows 7
- 安裝程式：系統管理員權限
- 所有安裝：Windows Internet Explorer 6.0 或更新的版本
- 必要時，提供網際網路連線 (請參閱安裝)

Avira SearchFree Toolbar

- 作業系統

- Windows XP，最新 SP (32 或 64 位元) 或
- Windows 7，最新 SP (32 或 64 位元)

- 網頁瀏覽器
  - Windows Internet Explorer 6.0 或更新的版本
  - Mozilla Firefox 3.0 或更新版本
  - Google Chrome 18.0 或更新版本

> 注意
> 必要時，在安裝 Avira SearchFree Toolbar 之前請先解除安裝以前安裝的搜尋工具列。 否則您將無法安裝 Avira SearchFree Toolbar。

Windows Vista 使用者資訊

在 Windows XP 環境中，許多使用者皆以系統管理員權限來操作。
不過，從安全觀點來看這點並不可取，因為這樣一來病毒與有害程式更容易入侵電腦。

為此，Microsoft 特地在 Windows Vista 中推出「使用者帳戶控制」功能。
此功能可為以系統管理員身份登入的使用者提供更多防護：因此在 Windows Vista 中，系統管理員只有一開始一般使用者的權限。 在 Windows Vista 中，必須有系統管理員權限才能執行的動作會以資訊圖示來清楚標示。
此外，使用者必須明確地確認所需的動作。
使用者必須在取得這項權限之後才能提升權限等級，如此一來，作業系統才能執行系統管理工作。

Avira 產品需要管理權限才能在 Windows Vista 中執行某些動作。
這些動作都標記以下的符號：  。
如果此符號未顯示在按鈕上，則需要管理權限來執行此動作。
如果您目前的使用者帳戶沒有管理員權限，Windows Vista 的 [使用者帳戶控制] 對話方塊會要求您輸入管理員密碼。 如果您沒有管理員密碼，則無法執行此動作。

2.3 授權與升級

2.3.1 授權

若要使用 Avira 產品，您需要一份授權。 請即刻接受授權條款。

授權會以啟用代碼形式來提供。 啟用代碼是由字母和數字組成的一組代碼，在購買 Avira 產品後就會收到。
啟用代碼內含您的授權詳細資料，亦即獲得了哪些程式授權與其授權期間。

如果您透過網路商店購買 Avira
產品，將會經由電子郵件收到啟用代碼，否則會直接附在產品包裝上。

若要授權程式，請輸入啟用代碼以啟用程式。 您可以在安裝期間執行產品啟用程序。
不過，您也可以在安裝 Avira 產品之後，於 **[說明] > [授權]**
底下的授權管理員中執行產品啟用程序。

2.3.2 展延授權

您的授權即將到期時，Avira 將傳送上滑訊息，提醒您展延授權。
若要這麼做，您只需要按一下連結，便將自動移至 Avira 線上商店。
不過，也可以透過授權管理員的 **[說明] > [授權管理]** 展延 Avira 產品的授權。

如果您在 Avira
的授權入口網站完成註冊，您可以透過**授權概覽**直接線上展延您的授權，也可以選取自動更新您的授權。

2.3.3 升級

您可以在授權管理員選擇從 Avira 桌面產品系列啟動產品升級。
不需要手動解除安裝舊產品及手動安裝新產品。 從授權管理員升級時，只要在
[授權管理員] 輸入方塊中輸入要升級之產品的啟用代碼。 新產品隨即自動安裝。

若要達到電腦的高可靠性與高安全性，Avira
會傳送快顯項目提醒您將系統升級至最新版本。
只要按一下快顯項目上的**升級**連結，就能引導您進入產品的指定升級網站。

您可以升級目前的產品，或購買更為全面的產品。
產品概觀頁面會顯示您正在使用的產品類型，並提供與其他 Avira 產品比較的機會。
如果您需要更多資訊，請按一下產品名稱旁的 **[資訊]** 圖示。
如果您想要使用原本的產品，請按一下 **[升級]**，隨即開始下載新版本。
如果您想要購買更為全面的產品，請按一下產品欄位底部的 **[購買]** 按鈕。 您將會自動移至 Avira 線上商店，在此可以購買產品。

> 注意
> 您可能需要系統管理員的權限才能執行升級，視您的產品與作業系統而定。
> 在執行升級之前，請以系統管理員的身分登入。

2.3.4 授權管理員

Avira Internet Security 授權管理員讓您以非常簡單的方式安裝 Avira Internet Security 授權。

Avira Internet Security 授權管理員

您可以按兩下選取 [檔案管理員]
或啟用電子郵件中的授權檔，然後遵循畫面上的相關指示，開始安裝授權。

> 注意
>
> Avira Internet Security
> 授權管理員會自動將對應的授權複製到相關的產品資料夾中。
> 如果已經存在授權，會顯示一則訊息，告知是否要取代現有的授權檔。
> 此時新的授權檔會覆寫現有的授權檔。

3. 安裝與解除安裝

本章包含安裝與解除安裝 Avira 產品的相關資訊。

- 請參閱下列章節：預先安裝：準備安裝電腦的需求
- 請參閱下列章節：快速安裝：根據預設設定進行標準安裝
- 請參閱下列章節：自訂安裝：可設定的安裝
- 請參閱下列章節：測試產品安裝
- 請參閱下列章節：組態精靈
- 請參閱下列章節：變更安裝
- 請參閱下列章節：安裝模組
- 請參閱下列章節：解除安裝：解除安裝

3.1 安裝類型

您可以在安裝期間，在安裝精靈中選取一種安裝類型：

快速安裝

- 將安裝標準元件。
- 程式檔案會安裝至 *C:¥Program Files* 底下的預設資料夾中。
- Avira 產品將以預設設定值安裝。 您可以選擇使用組態精靈定義自訂設定。

自訂

- 您可以選擇安裝個別的程式元件 (請參閱安裝與解除安裝 > 安裝模組)。
- 您可以針對要安裝的程式檔案，選取目標資料夾。
- 您可以在 **[開始]** 功能表中停用 **[建立桌面圖示]** 和 **[程式群組]**。
- 您可以使用組態精靈，定義 Avira 產品的自訂設定，並啟始安裝後自動執行的快速系統掃描。

3.2 預先安裝

> **注意**
> 在安裝前，請檢查您的電腦是否滿足所有最低系統需求。
> 如果您的電腦滿足所有需求，就可以安裝 Avira 產品。

預先安裝

- ✓ 關閉您的電子郵件程式。 同時建議您結束所有執行中的應用程式。
- ✓ 確定沒有安裝其他防毒解決方案。
  不同的資訊安全解決方案的自動保護功能可能會互相影響。
  - ↳ Avira 產品將在電腦中搜尋任何可能的不相容軟體。
  - ↳ 如果偵測到可能不相容的軟體，Avira 會產生這些程式的清單。
  - ↳ 建議移除這些軟體程式，以避免破壞電腦的穩定性。
- ▸ 從清單中選取後，所有選取程式的核取方塊應自動從您的電腦中移除，然後按一下 [下一步]。
- ▸ 您必須手動確認部分程式的解除安裝。 請選取程式並按一下 [下一步]。
  - ↳ 若要解除安裝一或多個選取的程式，必須重新啟動電腦。
    重新開機後，將繼續安裝。

> **警告**
> 在完成 Avira 產品安裝之前，您的電腦將不受保護。

安裝

安裝程式會執行自我說明的對話模式。
每個視窗都包含可控制安裝處理序的特定按鈕選項。

下列功能會指派給最重要的按鈕：

- **確定**：確認動作。
- **中止**：中止動作。
- **下一步**：移至下一個步驟。
- **上一步**：移至上一個步驟。

▸ 建立網際網路連線：您需要網際網路連線以執行下列安裝步驟：

- 針對網際網路型態的安裝並經由安裝程式下載最新的程式檔案與掃描引擎，以及最新的病毒定義檔
- 啟用程式
- 完成安裝後，請適當地執行更新。

▸ 當您想要啟用程式時，請利用 Avira 產品的啟動代碼或授權檔案。

注意

網際網路形態的安裝：
針對程式網際網路形態的安裝，提供一項安裝程式，供您進行網際網路型態的程式安裝；此安裝方式會在 Avira
網路伺服器執行安裝作業之前載入最新的程式檔案。 此程序可確保安裝的 Avira 產品內含最新的病毒定義檔。

利用安裝套件安裝：
安裝套件同時包含安裝程式與所有必要的程式檔案。
安裝套件不包含任何可用的 Avira 產品安裝語言選項。
建議您在安裝之後，執行病毒定義檔更新。

注意

啟用 Avira 產品時，請使用 HTTP 通訊協定與連接埠 80 (網路通訊)，並搭配加密通訊協定 SSL 與連接埠 443，以便和 Avira 伺服器通訊。

如果您是使用防火牆，請確保必要的連線與/或傳入或傳出的資料沒有遭到防火牆封鎖。

3.3 快速安裝

安裝您的 Avira 產品：

按兩下剛從網際網路下載的安裝檔案，或是插入程式光碟，以啟動安裝程式。

網際網路型態的安裝

↳ **歡迎**畫面出現。

- 按 **[下一步]** 繼續安裝。

  ↳ **[語言選擇]** 對話方塊隨即顯示。

- 選取您要用來安裝 Avira 產品的語言，並按 **[下一步]** 確認語言選擇。

  ↳ **[下載]** 對話方塊隨即顯示。 Avira 網路伺服器會開始下載所有必要的安裝檔案。
  [下載] 視窗會在下載結束時關閉。

使用安裝套件來安裝

↳ **[準備安裝]** 視窗隨即顯示。

↳ 這時會開始解壓縮安裝檔案。 安裝常式正式開始。

↳ **[選取安裝類型]** 對話方塊隨即顯示。

注意
快速安裝為預設值。 所有標準元件都將安裝，您無需自行設定。
若您想要執行自訂安裝，請參閱下列章節：安裝與解除安裝 > 自訂安裝。

- **[我要使用 Avira ProActiv 與 Protection Cloud 提升我的防護]**
  核取方塊已預先勾選 (組態 > 一般 > 進階防護)。 如果您不想加入 Avira 社群，請取消勾選此核取方塊。

↳ 如果您確認要加入 Avira 社群，Avira 會將偵測到的可疑程式資料傳送至 Avira 惡意程式碼研究中心。 此資料只會用於進階線上掃描和延伸及精簡偵測技術。
您可以按一下 **ProActiv 與 Protection Cloud**
連結了解更多有關延伸線上與雲端掃描的詳細資訊。

- 確認您已接受**使用者授權合約**。 如需了解**使用者授權合約**的詳細文字說明，請按一下 **EULA** 連結。

  ↳ **授權精靈**隨即開啟，而且會協助您啟用您的產品。

  ↳ 您可以在此設定 Proxy 伺服器。

- 必要時，按一下組態中的 **[Proxy 設定]**，並按 **[確定]** 確認設定。
- 如果您已經收到啟用代碼，請選取 **[啟用產品]** 並輸入啟用代碼。

  -或-

- 如果您沒有啟用代碼，請按一下**購買啟用代碼**連結。

  ↳ 您會移至 Avira 網站。

  或者，按一下**我已經有有效的授權**檔案連結。

  ↳ **[開啟檔案]** 對話方塊隨即顯示。

- 選取 *.KEY* 授權檔案，然後按一下 **[開啟]**。

  ↳ 啟用代碼會複製到授權精靈。

- 如果您想要測試產品，請繼續閱讀章節：測試產品安裝。
- 按 **[下一步]**。

  ↳ 安裝進度會顯示為綠色列。

- 按 **[下一步]**。

  ↳ **[成為百萬名 Avira SearchFree 使用者之一]** 對話方塊隨即出現。

- 如果您不想要安裝 Avira SearchFree Toolbar，請取消勾選 Avira SearchFree Toolbar 和 Avira SearchFree Updater **使用者授權合約**，而定義 **Avira SearchFree (search.avira.com)** 的項目就會成為您的瀏覽器首頁。

> 注意
> 必要時，在安裝 Avira SearchFree Toolbar 之前請先解除安裝以前安裝的搜尋工具列。 否則您將無法安裝 Avira SearchFree Toolbar。

- 按 [下一步]。
  - ↳ Avira SearchFree Toolbar 的安裝進度會顯示為綠色列。
  - ↳ Avira 系統匣圖示位於工作列中。
  - ↳ 如要確定有效的電腦防護，**更新程式**模組將搜尋可能的更新。
  - ↳ **[Luke Filewalker]** 視窗隨即開啟並執行快速系統掃描。會顯示掃描的狀態與結果。
- 如果在掃描後要求您重新啟動電腦，請按一下 **[是]** 確定您的系統已受到完整保護。

安裝成功之後，建議您檢查程式是否為最新狀態 (位於**控制中心**的*狀態*欄位中)。

- 如果您的 Avira 產品顯示您的電腦未受保護，請按一下 **[修正問題]**。
  - ↳ **[還原防護]** 對話方塊開啟。
- 啟動預設選項以最大化您系統的安全性。
- 必要時，請在之後執行完整的系統掃描。

3.4 自訂安裝

安裝您的 Avira 產品：

按兩下剛從網際網路下載的安裝檔案，或是插入程式光碟，以啟動安裝程式。

網際網路型態的安裝

- ↳ **歡迎**畫面出現。
- 按 **[下一步]** 繼續安裝。
  - ↳ **[語言選擇]** 對話方塊隨即顯示。

- 選取您要用來安裝 Avira 產品的語言，並按 **[下一步]** 確認語言選擇。
  - ↳ **[下載]** 對話方塊隨即顯示。 Avira 網路伺服器會開始下載所有必要的安裝檔案。 **[下載]** 視窗會在下載結束時關閉。

使用安裝套件來安裝

- ↳ **[準備安裝]** 視窗隨即顯示。
- ↳ 這時會開始解壓縮安裝檔案。 安裝常式正式開始。
- ↳ **[選取安裝類型]** 對話方塊隨即顯示。

> 注意
> 快速安裝為預設值。 所有標準元件都將安裝，您無需自行設定。
> 若您想要執行快速安裝，請參閱下列章節：安裝和解除安裝 > 快速安裝。

- 選取 **[自訂]** 安裝個別程式元件。
- **[我要使用 Avira ProActiv 與 Protection Cloud 提升我的防護]**
  核取方塊已預先勾選。 如果您不想加入 Avira 社群，請取消勾選此核取方塊。
  - ↳ 如果您確認要加入 Avira 社群，Avira 會將偵測到的可疑程式資料傳送至 Avira 惡意程式碼研究中心。 此資料只會用於進階線上掃描和延伸及精簡偵測技術。
    您可以按一下 **ProActiv 與 Protection Cloud**
    連結了解更多有關延伸線上與雲端掃描的詳細資訊。
- 確認您已接受**使用者授權合約**。 如需了解**使用者授權合約**的詳細文字說明，請按一下 **EULA** 連結。
- 按 **[下一步]**。
  - ↳ **[選擇目的地資料夾]** 視窗隨即開啟。
  - ↳ 預設資料夾位置為 *C:¥Program Files¥Avira¥AntiVir Desktop¥*
- 按一下 **[下一步]** 繼續。

-或-

使用 **[瀏覽]** 按鈕選取其他目的地目錄，並按 **[下一步]** 確認動作。

↳ **[安裝元件]** 對話方塊隨即顯示。

- 選取或取消選取清單中的元件，然後選取 **[下一步]** 繼續。
- 如果您選擇安裝 **Protection Cloud** 元件，但又要手動確認應傳送至雲端進行分析的檔案，您可以啟用 **[傳送可疑檔案至 Avira 時手動確認]** 選項。
- 按 **[下一步]**。
- 您可以在下列對話方塊中，決定是否建立桌面捷徑與/或在 **[開始]** 功能表中建立程式群組。
- 按 **[下一步]**。

↳ **授權精靈** 隨即開啟

您可以透過下列選項來啟用程式。

- 輸入啟用代碼。

↳ 輸入啟用代碼後，Avira 產品可使用您的授權來啟用。

- 如果您沒有啟用代碼，請按一下**購買啟用代碼**連結。

↳ 您會移至 Avira 網站。

- 選取 **[測試產品]** 選項

↳ 一旦您選取 **[測試產品]**，啟用程序就會產生一份評估授權，供您用來啟用。
您可以在特定期限內測試 Avira 產品的完整功能 (請參閱測試產品安裝)。

注意

使用 **[我已經擁有有效的授權檔案]** 選項後，您即可載入有效的授權檔案。
使用有效的啟用代碼來啟用產品時，系統會產生授權金鑰並儲存在 Avira 產品的程式目錄中。 如果您已經啟用產品，而想要重新安裝 Avira 產品，請使用這個選項。

注意

在某些 Avira 產品的銷售版本中，產品會內附啟用代碼。
此時您無須輸入啟用金鑰。 有需要的話，啟用代碼會顯示在授權精靈中。

注意

要啟動程式，必須先建立 Avira 伺服器的連線。 在 **[Proxy 設定]** 底下，您可以設定 Proxy 伺服器的網際網路連結。

- 選擇啟動處理序並按一下 **[下一步]** 確認。
- 如果您已擁有有效的授權檔案，請直接前往章節「選取*我已經有有效的授權檔案*選項」。

產品啟用

↳ 這時會開啟一個對話方塊，供您輸入個人資料。

- 輸入個人資料並按 **[下一步]**。

↳ 您的資料會傳送至 Avira 伺服器並掃描。 您的 Avira 產品會透過授權的方式啟用。

↳ 您的授權資料會顯示在下一個視窗中。

- 按 **[下一步]**。
- 跳過下列章節「選取*我已經有有效的授權檔案*選項」。

選取「我已經有有效的授權檔案」選項

↳ 隨即開啟一個方塊，供您載入授權檔案。

- 選取內含程式授權資料的 *.KEY* 授權檔，然後按一下 **[開啟]**。

↳ 您的授權資料會顯示在下一個視窗中。

- 按 **[下一步]**。

在完成啟用或載入授權檔之後繼續進行

↳ **[成為百萬名 Avira SearchFree 使用者之一]** 對話方塊隨即出現。

- 如果您不想要安裝 Avira SearchFree Toolbar，請取消勾選 Avira SearchFree Toolbar 和 Avira SearchFree Updater **使用者授權合約**，而定義 **Avira SearchFree (search.avira.com)** 的項目就會成為您的瀏覽器首頁。

> 注意 必要時，在安裝 Avira SearchFree Toolbar 之前請先解除安裝以前安裝的搜尋工具列。 否則您將無法安裝 Avira SearchFree Toolbar。

- 按 **[下一步]**。

↳ Avira SearchFree Toolbar 的安裝進度會顯示為綠色列。

↳ 關閉 **[安裝精靈]**後，**[組態精靈]** 隨即開啟。

3.5 測試產品安裝

安裝您的 Avira 產品：

按兩下剛從網際網路下載的安裝檔案，或是插入程式光碟，以啟動安裝程式。

網際網路型態的安裝

↳ **歡迎**畫面出現。

- 按 **[下一步]** 繼續安裝。

↳ **[語言選擇]** 對話方塊隨即顯示。

- 選取您要用來安裝 Avira 產品的語言，並按 **[下一步]** 確認語言選擇。

↳ **[下載]** 對話方塊隨即顯示。 Avira 網路伺服器會開始下載所有必要的安裝檔案。**[下載]** 視窗會在下載結束時關閉。

使用安裝套件來安裝

↳ **[準備安裝]** 視窗隨即顯示。

↳ 這時會開始解壓縮安裝檔案。 安裝常式正式開始。

↳ **[選取安裝類型]** 對話方塊隨即顯示。

注意

快速安裝為預設值。 所有標準元件都將安裝，您無需自行設定。

若您想要執行自訂安裝，請參閱下列章節：安裝與解除安裝 > 自訂安裝。

- **[我要使用 Avira ProActiv 與 Protection Cloud 提升我的防護]**
  核取方塊已預先勾選 (組態 > 一般 > 進階防護)。 如果您不想加入 Avira 社群，請取消勾選此核取方塊。

  ↳ 如果您確認要加入 Avira 社群，Avira 會將偵測到的可疑程式資料傳送至 Avira 惡意程式碼研究中心。 此資料只會用於進階線上掃描和延伸及精簡偵測技術。
  您可以按一下 **ProActiv 與 Protection Cloud**
  連結了解更多有關延伸線上與雲端掃描的詳細資訊。

- 確認您已接受**使用者授權合約**。 如需了解**使用者授權合約**的詳細文字說明，請按一下 **EULA** 連結。

- 按 **[下一步]**。

  ↳ **授權精靈**隨即開啟，而且會協助您啟用您的產品。

  ↳ 您可以在此設定 **Proxy 伺服器**。

- 按一下組態中的 **[Proxy 設定]**，並按 **[確定]** 確認設定。

- 在授權精靈中選取 **[測試產品]** 選項，然後按一下 **[下一步]**。

- 在 **[註冊]** *必填欄位中輸入您的資料*。 請決定是否要訂閱 **Avira 電子報**，然後按一下 **[下一步]**。

  ↳ 安裝進度會顯示為綠色列。

  ↳ **[成為百萬名 Avira SearchFree Toolbar 使用者之一]** 對話方塊隨即出現。

- 如果您不想要安裝 Avira SearchFree Toolbar，請取消勾選 Avira SearchFree Toolbar 和 Avira SearchFree Updater **使用者授權合約**，而定義 **Avira SearchFree (search.avira.com)** 的項目就會成為您的瀏覽器首頁。

> 注意
> 必要時，在安裝 Avira SearchFree Toolbar 之前請先解除安裝以前安裝的搜尋工具列。 否則您將無法安裝 Avira SearchFree Toolbar。

- 按 **[下一步]**。
  - ↳ Avira SearchFree Toolbar 的安裝進度會顯示為綠色列。
- 如果您想要啟用 Avira 產品，必須先重新啟動系統。 按一下 **[是]** 即可立即重新啟動電腦。
  - ↳ Avira 系統匣圖示位於工作列中。
  - ↳ 您的評估授權有效期限為 31 天。

3.6 組態精靈

當使用者定義結束時，組態精靈隨即開啟。 組態精靈可讓您定義 Avira 產品的自訂設定。

- 在組態精靈的歡迎使用視窗中，按 **[下一步]**，開始進行程式的組態設定。
  - ↳ **[設定 AHeAD]** 對話方塊可讓您針對 AHeAD 技術選取一項偵測等級。選取的偵測等級將用於 Scanner (指定掃描) 與 Real-Time Protection (即時掃描) AHeAD 技術設定。
- 選取一項偵測等級，並按 **[下一步]** 繼續安裝。
  - ↳ 在接下來的 **[選取延伸的威脅類別]** 對話方塊中，您可以依據指定的威脅類別調整 Avira 產品保護功能。
- 必要時啟用進一步威脅類別並按 **[下一步]** 繼續安裝。
  - ↳ 如果您已選取 Avira FireWall 安裝模組，**[存取網路及使用網路資源的預設規則]** 對話方塊就會出現。 您可以定義 Avira

FireWall
是否應該允許外部存取啟用的資源，並允許信任的公司應用程式進行網路存取活動。

- 啟用所需選項，並按 **[下一步]**，繼續進行組態設定。
  - ↳ 如果您已選取 Avira Real-Time Protection 安裝模組，**[Real-Time Protection 啟動模式]** 對話方塊就會出現。 您可規定 Real-Time Protection 的啟動時間。 每次電腦重新開機時，Real-Time Protection 會以指定的啟動模式來啟動。

注意
指定的 Real-Time Protection 啟動模式會儲存在登錄中，而且無法經由 [組態] 變更。

注意
如果已選取 Real-Time Protection 的預設啟動模式 (正常啟動) 而且在快速執行啟動後立即處理登入處理序，可能不會掃描啟動後設為自動啟動的程式，因為這些程式皆已在完成啟動 Real-Time Protection 之前啟動並執行。

- 啟用所需選項，並按 **[下一步]**，繼續進行組態設定。
  - ↳ 如果您已選取 Avira Web Protection 安裝模組，**[啟用 Safe Browsing]** 對話方塊就會出現。 您可以選擇對電腦使用者指派不同角色 (兒童、青少年、成人)，以限制網際網路使用。 也可以停用 **Safe Browsing**。
- 定義所需的 Safe Browsing 設定，並按 **[下一步]**，繼續進行組態設定。
  - ↳ 在接下來的 **[指派密碼]** 對話方塊中，您可以用密碼保護組態，避免未經授權的存取。 如果您啟用了家長監護功能，特別建議使用此選項。

↳ 在接下來的 **[系統掃描]** 對話方塊中，您可以啟用或停用快速系統掃描。
快速系統掃描可在組態完成後及電腦重新開機前進行，可掃描執行中的程式與最重要的系統檔案是否藏有病毒與惡意程式碼。

- 啟用或停用 **[快速系統掃描]** 選項，並按 **[下一步]** 繼續進行組態設定。
  - ↳ 在接下來的對話方塊中，您可以按一下 **[完成]**，完成組態。
  - ↳ 隨即接受指定與選取的所有設定。
  - ↳ 如果您已啟用 **[快速系統掃描]** 選項， **[Luke Filewalker]** 視窗隨即開啟。
    掃描程式會執行快速系統掃描。
- 如果在掃描後要求您重新啟動電腦，請按一下 **[是]** 確定您的系統已受到完整保護。

安裝成功之後，建議您檢查程式是否為最新狀態 (位於**控制中心**的**狀態**欄位)。

- 如果您的 Avira 產品顯示您的電腦未受保護，請按一下 **[修正問題]**。
  - ↳ **[還原防護]** 對話方塊開啟。
- 啟動預設選項以最大化您系統的安全性。
- 必要時，請在之後執行完整的系統掃描。

3.7 變更安裝

您可以針對目前的 Avira 產品安裝 (請參閱下列章節：安裝與解除安裝 > 安裝模組)，選擇新增或移除個別程式元件。

如果您想要新增或移除目前的安裝模組，可以使用 **Windows [控制台]** 中的 **[新增或移除程式]** 選項來 **[變更/移除]** 相關程式。

選取 Avira 產品，然後按一下 **[變更]**。 在程式的 **[歡迎]** 對話方塊中，選取 **[修改]** 選項。系統會引導您完成各項安裝變更。

3.8 安裝模組

在使用者定義的安裝或變更安裝中，您可以選取、新增或移除下列安裝模組。

- **Avira Internet Security**
  此模組包含成功安裝 Avira 產品所需的所有元件。
- **Real-Time Protection**
  Avira Real-Time Protection 在背景執行。
  在即時模式下，它會在開啟、寫入與複製等作業期間監視並修復檔案
  (如果有需要的話)。 每當使用者執行檔案操作 (例如，載入文件、執行、複製)，Avira 產品就會自動掃描檔案。 重新命名檔案不會觸發 Avira Real-Time Protection 掃描。
- **Mail Protection**
  Mail Protection
  是您的電腦與電子郵件伺服器之間的介面，後者可供您的電子郵件程式
  (電子郵件用戶端) 下載電子郵件。 連線的 Mail Protection
  可做為電子郵件程式和電子郵件伺服器之間的 Proxy 。
  所有內送的電子郵件都會透過這台 Proxy
  來路由、掃描其中的病毒與有害程式，並轉寄給您的電子郵件程式。
  依據組態不同，程式會自動處理受影響的電子郵件或是要求使用者執行特定動作。
  此外，Mail Protection 能可靠地保護您免於垃圾電子郵件的騷擾。
- **Avira FireWall**
  Avira FireWall 可控制進出電腦的通訊。
  它會依據安全性原則允許或拒絕相關通訊活動。
- **Rootkits Protection**
  Avira Rootkits Protection
  會檢查您的電腦是否已安裝了某種特殊軟體，這類軟體一旦入侵電腦系統後，便無法再以傳統的惡意程式碼保護機制來偵測。
- **ProActiv**
  ProActiv
  元件會監視應用程式動作，並在偵測到典型的惡意程式碼應用程式行為時，向使用者提出警示。 此行為式辨識模式可讓您防範不明的惡意程式碼。 ProActiv 元件已整合為 Avira Real-Time Protection。
- **Protection Cloud**
  Protection Cloud 元件是一種動態線上偵測未知惡意程式碼的模組。

- **Backup**

  Backup 元件可讓您手動與自動建立資料的鏡像備份。

- **Web Protection**

  上網瀏覽時，可以使用網頁瀏覽器要求網路伺服器中的資料。 從網路伺服器傳輸的資料 (HTML 檔案、指令碼與圖片檔、Flash 檔案、影片與音樂串流等)
  通常會直接存入瀏覽器快取以供網頁瀏覽器顯示，意味著 Avira Real-Time Protection 無法執行即時掃描。 如此一來，病毒與有害程式便可能存取您的電腦系統。 Web Protection (即所謂的 HTTP Proxy) 可監視資料傳輸所使用的連接埠 (80、8080、3128) 並掃描傳輸的資料中是否有病毒與有害程式。
  依據組態不同，程式可能會自動處理受影響的檔案，或是提示使用者執行特定動作。

- **殼層延伸**

  殼層延伸會在 [Windows 檔案總管] (滑鼠右鍵按鈕) 的內容功能表中產生一個項目：**利用 Avira 掃描選取的檔案**。
  透過這個項目，您可以直接掃描檔案或目錄。

3.9 解除安裝

如果您希望從電腦移除 Avira 產品，可以使用 **[新增或移除程式]** 以 **[變更/移除]** Windows [控制台] 中的程式。

若要解除安裝 Avira 產品 (例如使用 Windows 7)：

- 經由 Windows **[開始]** 功能表，開啟 **[控制台]**。
- 按兩下 **[程式和功能]**。
- 在清單中選取 Avira 產品，然後按一下 **[解除安裝]**。
  - ↳ 系統會詢問您是否確定要移除程式。
- 按一下 **[是]** 確認。
  - ↳ 系統會詢問您是否要重新啟用 Windows 防火牆 (將停用 Avira FireWall)。
- 按一下 **[是]** 確認。
  - ↳ 這時所有程式元件都會移除。

- 按一下 **[完成]** 完成解除安裝。
  - ↳ 必要時，會顯示對話方塊，建議您重新啟動電腦。
- 按一下 **[是]** 確認。
  - ↳ 這時 Avira 產品已解除安裝，而且當您的電腦重新啟動時，程式的所有目錄、檔案與登錄項目都會一併刪除。

注意

Avira SearchFree Toolbar 不包含在解除安裝的程式中，必須另外依照以上詳述的步驟解除安裝。 若要在 Firefox 中解除安裝必須透過增益集管理員啟用 Avira SearchFree Toolbar。在解除安裝後，搜尋工具列將不再整合至您的網頁瀏覽器中。

4. Avira Internet Security 概觀

本章包含 Avira 產品的功能與操作方式概觀。

- 請參閱下列章節：使用者介面與操作方式
- 請參閱下列章節：Avira SearchFree Toolbar
- 請參閱下列章節：如何...?

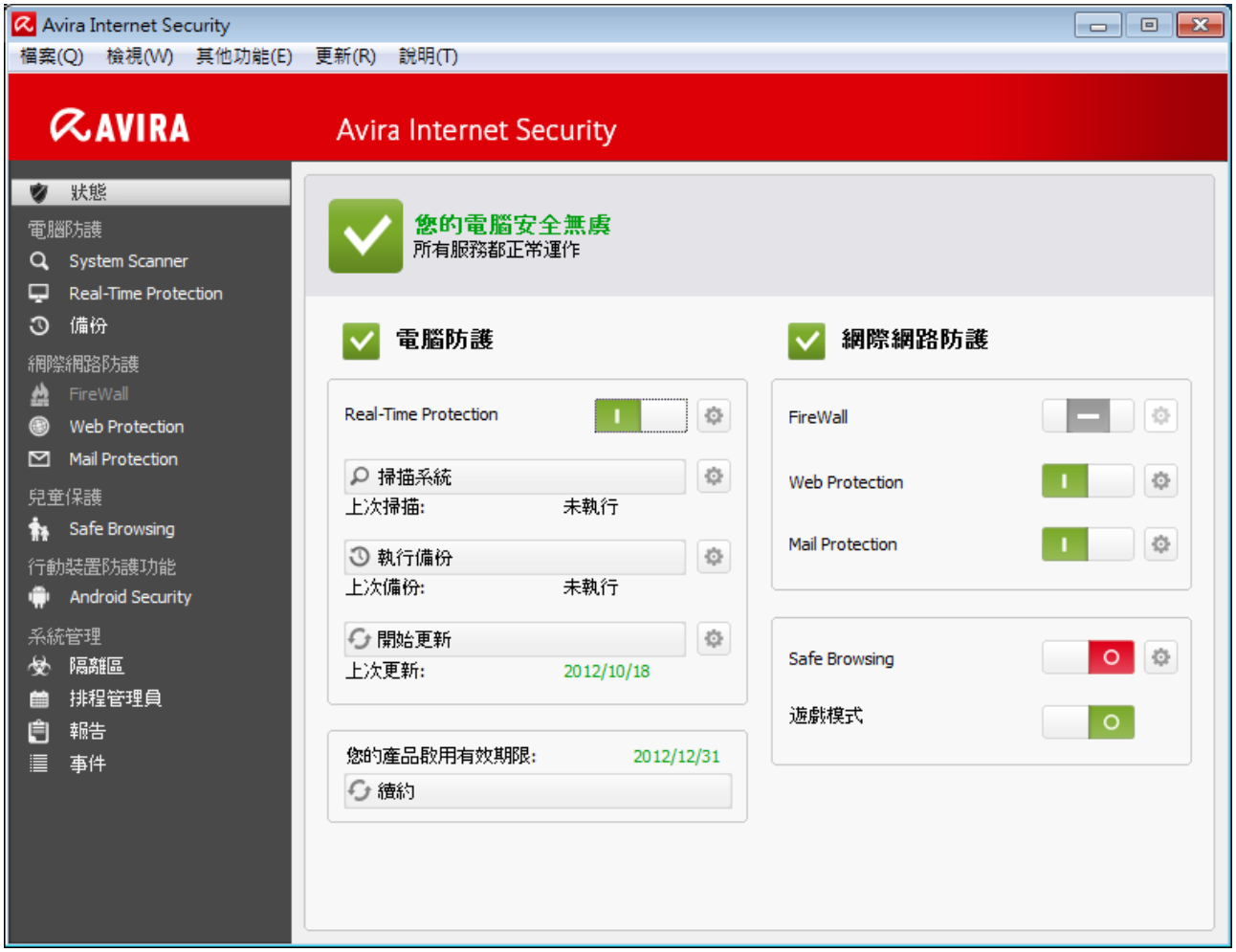
4.1 使用者介面與操作方式

您可以經由三種程式介面元素來操作 Avira 產品：

- 控制中心：監控與控制 Avira 產品
- 組態：設定 Avira 產品
- 系統匣圖示位於工作列的系統匣中：開啟控制中心及其他功能

4.1.1 控制中心

控制中心是專門設計來監視電腦系統的保護狀態，以及控制與操作 Avira 產品的保護元件與各項功能。



[控制中心] 視窗分成三個區域：**功能表列**、**瀏覽區**及詳細資料視窗**狀態**：

- **功能表列**：在控制中心功能表列中，您可以存取一般程式功能與程式相關資訊。
- **瀏覽區域**：在瀏覽區域中，您可以輕鬆切換個別的控制中心區段。
  這些個別的區段包含了程式元件的相關資訊與功能，並依據活動特性來排列瀏覽列。
  例如：活動*電腦防護* - 區段 **Real-Time Protection**。
- **狀態**：控制中心開啟的**狀態**檢視可讓您概要了解您的電腦是否安全，以及可概觀目前作用中的模組、上次備份的日期與上次系統掃描的日期。
  狀態檢視也包含啟動功能或動作的按鈕，如啟動或停止 **Real-Time Protection**。

啟動及關閉控制中心

若要啟動控制中心，可使用下列選項：

- 按兩下桌面上的程式圖示

- 經由 **[開始] > [程式集]** 中的程式項目。
- 經由 Avira 產品的系統匣圖示。

經由 **[檔案]** 功能表中的 **[關閉]**
功能表命令，或是按一下控制中心中的關閉索引標籤，關閉控制中心。

操作控制中心

若要瀏覽控制中心

- 在瀏覽列中選取一項活動。
  - ↳ 此活動會開啟，並顯示其他區段。 會選取活動的第一個區段，並顯示在檢視中。
- 必要時，按一下另一個區段將其顯示在詳細資料視窗中。

> 注意
> 您可藉由 **[Alt]** 鍵，在功能表列中啟用鍵盤瀏覽功能。
> 瀏覽功能一經啟用，您就可以使用**方向鍵**在功能表中移動。 您可以使用 **Return** 鍵來啟用作用中的功能表項目。
> 若要開啟或關閉控制中心中的功能表，或是在各個功能表之間瀏覽，您還可以使用下列按鍵組合：**[Alt]** + 功能表或功能表命令中的底線字母。
> 如果您想要存取功能表、功能表命令或是子功能表，請按住 **[Alt]** 鍵。

若要處理詳細資料視窗中顯示的資料或物件：

- 反白您希望編輯的資料或物件。

  若要反白多項元素 (欄中的元素)，按住 **Ctrl** 按鍵或 **Shift** 按鍵不放並同時選取元素。
- 按一下詳細資料視窗上方列中的適當按鈕來編輯物件。

控制中心概觀

- **狀態**：按一下**狀態**列即可概觀產品功能及效能 (請參閱狀態)。
  - **[狀態]** 區段可讓您概要了解哪一個模組目前為作用中，並提供最近執行的更新資訊。

- *電腦防護*：在此區段中，您可以找到用來檢查電腦系統上的檔案是否藏有病毒與惡意程式碼的元件。
  - Scanner 區段可讓您輕易地設定並啟動指定掃描。
    預先定義的設定檔可搭配已經調整的預設選項來進行掃描。
    同理，您也可以依據個人需求並藉由手動選取 (將儲存)
    或是藉由建立使用者定義的設定檔來調整病毒與有害程式的掃描方式。
  - Real-Time Protection 區段會顯示已掃描檔案的相關資訊與其他統計資料 (可隨時重設)，並讓您存取報告檔案。
    您只需實際「按一下按鈕」，就可獲得有關偵測到的最新病毒或有害程式詳細資訊。
  - 在 Backup 區段，您可以輕鬆、快速地建立資料備份，並啟始備份工作。
- *網際網路防護*：在此區段中，您可以找到用來保護電腦系統免於網際網路上的病毒與惡意程式碼威脅，同時防範未授權之網路存取的元件。
  - FireWall 區段可讓您進行 FireWall 的基本設定。
    此外，還會顯示目前的資料傳輸率以及正在使用網路連線的所有作用中應用程式。
  - Web Protection 區段會顯示已掃描之 URL 與偵測到的病毒相關資訊以及其他統計資料 (可隨時重設)，並讓您存取報告檔案。
    您只需實際「按一下按鈕」，就可獲得有關偵測到的最新病毒或有害程式詳細資訊。
  - Mail Protection 區段可顯示 Mail Protection 所掃描的所有電子郵件及其屬性和其他統計資料。
    您也可以訓練反垃圾郵件篩選器，以排除電子郵件地址免於日後的惡意程式碼或垃圾郵件掃描作業。 您也可以從 Mail Protection 緩衝區刪除電子郵件。
- *兒童保護*：在此區段中，您可以找到確保兒童接受安全網際網路體驗的元件。
  - 在 Safe Browsing 區段中，您可以將使用者角色指派給電腦使用者。
    使用者角色可以設定，並包括一連串允許及封鎖的 URL、禁止的 URL 類別、網際網路使用時間長度，如有必要可加入允許平日使用的時間長度。
- *行動裝置防護功能*：在此區段中，您將會重新導向至 Android 裝置的線上存取。
  - Avira Free Android Security 負責管理所有 android 的裝置。
- *系統管理*：在此區段中，您可以找到用以隔離與管理可疑或受感染檔案，以及用以規劃重複性工作的相關工具。

- 隔離區區段內含所謂的隔離區管理員。
  此區段可集中放置已經遭到隔離的所有檔案或是您想要隔離的可疑檔案。
  也可以將選取的檔案透過電子郵件方式傳送至 Avira 惡意程式碼研究中心。
- 排程管理員區段可讓您設定排定的掃描與更新工作以及備份工作，並讓您調整或刪除現有工作。
- 報告區段可讓您檢視執行的動作結果。
- 事件區段可讓您檢視由特定程式模組所產生的事件。

4.1.2 遊戲模式

如果在您的電腦系統上以全螢幕模式執行應用程式，您可刻意透過啟用遊戲模式來暫停快顯視窗與產品訊息的桌面通知。 您在 Avira FireWall
中設定的所有定義介面卡和應用程式規則皆可套用，但不會隨網路事件通知出現快顯視窗。

您可以按一下 **[開/關]** 按鈕啟用遊戲模式或停留在自動模式。
根據預設值，遊戲模式是設為**自動**，且顯示為綠色。
預設設定將功能設為自動，因此每當您執行需要全螢幕模式的應用程式時，Avira
產品都會自動切換為遊戲模式。

- 按一下 **[關]** 按鈕左邊的按鈕，以啟用遊戲模式。
  - 遊戲模式隨即啟用並顯示為黃色。

> 注意
> 我們建議僅在自動全螢幕識別模式時暫時變更預設設定
> **[關]**，因為您將收不到桌面通知與相關網路事件與可能威脅的警告。

4.1.3 組態

您可以在 [組態] 中定義 Avira 產品的設定。 在安裝完畢後會使用標準設定來設定 Avira 產品，確保為您的電腦系統提供最佳保護。 不過，您可能需要依據電腦系統或是 Avira 產品的特定需求，調整程式的保護元件。

組態會開啟對話方塊：您可以經由 **[確定]** 或 **[套用]** 按鈕來儲存組態設定、按一下 [取消] 按鈕來刪除設定，或是透過 **[預設值]** 按鈕來還原預設的組態設定。
您可以在左側的瀏覽列中，選取個別的組態區段。

存取組態

您可以使用下列幾個選項來存取組態：

- 經由 Windows 控制台。
- 經由 Windows 資訊安全中心 - (從 Windows XP Service Pack 2 開始提供)。
- 經由您 Avira 產品的系統匣圖示。
- 經由控制中心中的其他功能 > 組態功能表項目。
- 經由控制中心中的組態按鈕。

注意

如果您是經由控制中心中的 **[組態]** 按鈕來存取組態，請移至控制中心裡目前作用中的區段之組態登錄。您必須選取**專家模式**以選取個別的組態登錄。在此情況中，會出現一個要求您啟用專家模式的對話方塊。

組態作業

[組態] 視窗與 [Windows 檔案總管] 的瀏覽方式是相同的：

- 按一下樹狀結構中的項目，將此組態區段顯示在詳細資料視窗中。
- 按一下項目前方的加號以展開組態區段，並在樹狀結構中顯示組態子區段。
- 若要隱藏組態子區段，在展開的組態區段前方按一下減號。

注意

若要啟用或停用組態選項並使用按鈕，您還可以使用下列按鍵組合：**[Alt]** + 選項名稱或按鈕說明中的底線字母。

注意

所有的組態區段只會顯示在**專家模式**中。請啟用**專家模式**以檢視所有組態區段。在啟用期間必須定義的密碼，可用來保護專家模式。

如果您想要確認組態設定：

- 按一下 **[確定]**。
  - ↳ 組態視窗隨即關閉，並接受相關設定。

  - 或 -
- 按一下 **[套用]**。

↳ 套用設定。 組態視窗會維持開啟狀態。

如果您想要直接結束組態而不確認設定：

▸ 按一下 **[取消]**。

↳ 組態視窗隨即關閉，並捨棄相關設定。

如果您想要將所有組態設定還原為預設值：

▸ 按一下 **[預設值]**

↳ 組態的所有設定會還原為預設值。
當您還原預設值時，會遺失所有修正與自訂項目。

組態選項概觀

以下為可用的組態選項：

- **Scanner**：指定掃描組態
  - 偵測動作
  - 封存掃描選項
  - 系統掃描例外
  - 系統掃描啟發式掃毒
  - 報告功能設定
- **Real-Time Protection**：即時掃描組態
  - 掃描選項
  - 偵測動作
  - 進一步動作
  - 即時掃描例外
  - 即時掃描啟發式掃毒
  - 報告功能設定
- **Backup**：

- Backup 元件設定 (增量備份、於備份期間掃描病毒)
- 例外：定義要儲存的檔案
- 報告功能設定

- **更新**：更新設定的組態
  - Proxy 設定
- **FireWall**：FireWall 組態
  - 介面卡規則設定
  - 使用者定義的應用程式規則設定
  - 受信任供應商清單 (供應用程式進行網路存取的例外項目)
  - 擴充設定：自動規則逾時、停止 Windows 防火牆、通知
  - 快顯設定 (應用程式進行網路存取的警示)
- **Web Protection**：Web Protection 組態
  - 掃描選項、啟用與停用 Web Protection
  - 偵測動作
  - 封鎖存取：有害的檔案類型與 MIME 類型、已知有害 URL (惡意程式碼、網路釣魚等) 的網路篩選器
  - Web Protection 掃描例外：URL、檔案類型、MIME 類型
  - Web Protection 啟發式掃毒
  - 報告功能設定
- **Mail Protection**：Mail Protection 組態
  - 掃描選項：對 POP3 帳戶、IMAP 帳戶、外寄電子郵件 (SMTP) 啟用監視
  - 偵測動作
  - 進一步動作
  - Mail Protection 掃描啟發式掃毒
  - AntiBot 功能：允許 SMTP 伺服器與電子郵件寄件者
  - Mail Protection 掃描例外
  - 快取組態、清空快取

- 反垃圾郵件訓練資料庫組態、清空訓練資料庫
- 傳送的電子郵件頁尾組態
- 報告功能設定

- **兒童保護**：
  - Safe Browsing：家長監護功能可依據不同的角色，篩選不適當的網站及限制網際網路的使用
- **一般**：
  - Scanner 與 Real-Time Protection 的威脅類別
  - 進階防護：選擇啟用 ProActiv 與 Protection Cloud 功能
  - 應用程式篩選器：封鎖或允許應用程式
  - 控制中心與組態的密碼保護存取
  - 安全性：封鎖自動啟動功能、產品防護、保護 Windows 主機檔案
  - WMI：啟用 WMI 支援
  - 事件記錄組態
  - 報告功能組態
  - 使用的目錄設定
  - 偵測到惡意程式碼時的警示音組態

4.1.4 系統匣圖示

安裝完畢後，您會在工作列的系統匣中看到 Avira 產品系統匣圖示：

圖示	說明
	Avira Real-Time Protection 啟用且 FireWall 啟用
	Avira Real-Time Protection 停用 或 FireWall 停用

系統匣圖示會顯示 Real-Time Protection 與 FireWall 服務的狀態。

您可以經由**系統匣圖示**的內容功能表，快速存取 Avira 產品的核心功能。
若要開啟內容功能表，請以滑鼠右鍵按一下**系統匣圖示**。

內容功能表中的項目

- **啟用 Real-Time Protection**：啟用或停用 Avira Real-Time Protection。
- **啟用 Mail Protection**：啟用或停用 Avira Mail Protection。
- **啟用 Web Protection**：啟用或停用 Avira Web Protection。
- **FireWall**：
  - **啟用 FireWall**：啟用或停用 Avira FireWall
  - **封鎖所有流量**：啟用。 除了傳輸給主機電腦系統 (本機主機/IP 127.0.0.1) 的流量之外，會封鎖所有資料傳輸流量。
- **啟動 Avira Internet Security**：開啟控制中心。
- **設定 Avira Internet Security**：開啟組態.
- **我的訊息**：開啟有關 Avira 產品的目前資訊。
- **我的通訊設定**：開啟產品訊息訂閱中心
- **開始更新**：開始更新。
- **說明**：會開啟線上說明。
- **關於 Avira Internet Security**：會針對 Avira 產品：產品資訊、版本資訊、授權資訊開啟內含詳細資訊的對話方塊。
- **網際網路上的 Avira**：在網際網路上開啟 Avira 入口網站。
  前提是您必須具備有效的網際網路連線。

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar 包括兩個主要元件：Avira SearchFree 與 Toolbar。

Avira SearchFree Toolbar 可作為附加元件安裝。 瀏覽器優先存取時 (Firefox 和 Internet Explorer)，訊息會跳出，詢問您是否允許安裝工具列。 您必須同意才能完成 Avira SearchFree Toolbar 的安裝。

Avira SearchFree 為一搜尋引擎，包含可點選的 Avira 標誌並連結至 Avira 網站與網頁、影像和視訊頻道。 這也能確保 Avira 使用者安全的上網瀏覽。

整合至您網頁瀏覽器的工具列是由搜尋方塊、連結至 Avira 網站的 Avira 標誌、兩個狀態顯示、三個小程式與 **[Options]** 功能表組成。

- 搜尋工具列
  使用搜尋工具列可免費利用 Avira 搜尋引擎快速的搜尋網際網路。
- 狀態顯示
  狀態顯示提供有關 Web Protection 的狀態資訊，以及 Avira 產品的目前更新狀態，並能協助您識別保護電腦需採取的動作。
- 小程式
  Avira 提供三種最重要的網際網路相關功能小程式。 只要按一下就能直接存取 Facebook 與電子郵件，您也可以確保安全的瀏覽網頁 (僅限 Firefox 和 Internet Explorer)。
- 選項
  您可以使用 **[Options]** 功能表來存取工具列選項、清除歷程記錄、尋求工具列協助和資訊，也可以透過網頁瀏覽器直接解除安裝 Avira SearchFree Toolbar (僅限 Firefox 和 Internet Explorer)。

4.2.1 使用

Avira SearchFree

您可以使用 Avira SearchFree 來定義瀏覽網際網路的任意數量字詞。

在搜尋方塊中輸入字詞並按 **Enter** 鍵，或按一下 **[Search]**。 Avira SearchFree 引擎將搜尋網際網路，然後在瀏覽器視窗中顯示所有搜尋結果。

若要了解在 Internet Explorer, Firefox 及 Chrome 上自訂 Avira SearchFree 的方式，請移至 選項。

狀態顯示

Web Protection

您可以使用以下圖示與訊息來識別保護電腦的所需的動作：

圖示	狀態顯示	說明
	*Web Protection*	如果您在圖示上移動游標，下列訊息就會出現：*Avira Web Protection is active. Your browsing is protected.* 不必採取進一步動作。
	*Web Protection is inactive*	如果您在圖示上移動游標，下列訊息就會出現：*Avira Web Protection is off. Click to find out how to turn it on.* ↪ 將會重新導向至其中一個知識庫文章。

	No Web Protection	如果您在圖示上移動游標，將會出現下列其中一種訊息： • *You do not have Avira Web Protection installed. Click to find out how to protect your browsing.* 如果您解除安裝 Avira Antivirus 或安裝的方式不正確，此訊息將會出現。 • *Web Protection is included for free with Avira Antivirus. Click to find out how to install it.* 如果您不安裝 Web Protection 或將其解除安裝，此訊息將會出現。 ↳ 在這兩種情況中，您將重新導向至 Avira 首頁，並可在此下載 Avira 產品。
	Error	如果您在圖示上移動游標，將會出現下列訊息：*Avira reported an error. Click to contact Support for help.* ▸ 按一下灰色圖示或文字以移至 Avira 支援頁面。

小程式

Avira SearchFree
包含時下網際網路網頁瀏覽最重要功能的三個小程式：Facebook、電子郵件與 Browser Security。

Facebook

您可以利用此功能接收所有來自 Facebook 的訊息並隨時更新。

電子郵件

如果您按一下工具列中的電子郵件符號，將顯示下拉式清單。
您可以選擇最常用的電子郵件供應者。

Browser Security

這種小程式的用途為按一下就能獲得日常所需的所有網際網路安全性選項。
此選項僅適用於 Firefox 與 Internet Explorer。
此外，功能名稱有時會隨瀏覽器的變更而異：

- *快顯封鎖程式*

如果啟用此選項，所有快顯視窗都會被封鎖。

- *封鎖 Cookies*

如果您啟用此選項，將不會在您的電腦上儲存任何 cookies。

- *私人瀏覽 (Firefox) / InPrivate 瀏覽 (Internet Explorer)*

如果您不想在瀏覽網站時留下任何私人資訊，請啟用此選項。 此選項不適用於 Internet Explorer 7 與 8。

- *清除最近的記錄 (Firefox) / 刪除瀏覽歷程記錄 (Internet Explorer)*

選取此選項後即可清除網際網路活動的所有痕跡。

Website Safety Advisor

Website Safety Advisor 提供瀏覽時的網站安全評比。
您可以存取正在造訪的網站評價，並檢查影響您安全性的風險高低。
這個小程式也提供有關網站的進一步資訊，如網域擁有者的身份或網站被分類為安全或有風險的原因。

Website Safety Advisor 的狀態會顯示在 Toolbar
和搜尋結果中，如同與其他圖示結合的 Avira 系統匣圖示：

圖示	狀態顯示	說明
	*Safe*	綠色勾選記號代表安全網站。
	*Low risk*	黃色驚嘆號代表網站含有低風險。
	*High risk*	紅色禁止進入符號代表網站存有高安全性風險。
	*Unknown*	當狀態不明時會出現灰色問號。
	*Verifying*	此符號會在確認網站狀態時出現。

Browser Tracking Blocker

啟用 Browser Tracking Blocker
後，您可以在上網瀏覽時停止追蹤程式收集有關您的資訊。
您可以利用小程式來選擇要封鎖與允許的追蹤程式。

追蹤集團分成三個類別：

- 社交網路
- 廣告網路
- 其他集團

4.2.2 選項

Avira SearchFree Toolbar 相容於 Internet Explorer、Firefox 及 Google Chrome，並可以在這三個網頁瀏覽器中設定：

- Internet Explorer 組態選項
- Firefox 組態選項
- Google Chrome 組態選項

Internet Explorer

在 Internet Explorer 中，下列 Avira SearchFree Toolbar 的組態選項皆可在 **[Options]** 功能表中使用：

Toolbar options

Search

Avira search engine

在 **[Avira search engine]** 功能表中，您可以選取要用於搜尋的引擎。
搜尋引擎適用於美國、巴西、德國、西班牙、歐洲、法國、義大利、荷蘭、俄羅斯及英國。

Open searches in

在 **[Open searches in]** 選項功能表中，您可以選取顯示的搜尋結果；[Current] 視窗、[New] 視窗或 [New] 標籤。

Display recent searches

如果啟用 **[Display recent searches]** 選項，您可以在搜尋工具列文字輸入方塊下顯示上一筆搜尋字詞。

Auto clear recent search history when I close the browser

如果您不想要儲存上一筆搜尋項目而想要在關閉網頁瀏覽器時清除記錄，請啟用 **[Auto clear recent search history when I close the browser]** 選項。

More options

Select toolbar language

在 **[Select toolbar language]** 底下，您可以選取 Avira SearchFree Toolbar 的顯示語言。
工具列可用語言有英文、德文、西班牙文、法文、義大利文、葡萄牙文及荷蘭文。

注意

如可行時，預設 Avira SearchFree Toolbar 語言會對應您的程式顯示語言。如果工具列沒有您使用的語言，預設語言將變為英文。

Show button text labels

如果您想要隱藏 Avira SearchFree Toolbar 圖示旁的文字，請停用 **[Show button text labels]** 選項。

Clear history

如果您不要儲存先前的搜尋項目而想要立即清除記錄，請啟用 **[Clear history]** 選項。

Help

按一下 **[Help]** 存取內含相關工具列常見問題集 (FAQs) 的網站。

Uninstall

您也可以在 Internet Explorer 中直接解除安裝 Avira SearchFree Toolbar：透過網頁瀏覽器解除安裝

About

按一下 **[About]** 顯示安裝 Avira SearchFree Toolbar 的版本。

Firefox

在 Firefox 網頁瀏覽器中，可在 **[選項]** 功能表中使用 Avira SearchFree Toolbar 的下列組態選項：

Toolbar options

Search

Select Avira search engine

在 **[Avira search engine]** 功能表中，您可以選取要用於搜尋的引擎。
搜尋引擎適用於美國、巴西、德國、西班牙、歐洲、法國、義大利、荷蘭、俄羅斯及英國。

Display recent searches

如果啟用 **[Display recent searches]** 選項，您可以按一下搜尋工具列中的箭頭顯示上一筆搜尋字詞。
如果您想要重新顯示搜尋結果，請選取字詞。

Auto clear recent search history when I close the browser

如果您不想要儲存上一筆搜尋項目而想要在關閉網頁瀏覽器時清除記錄，請啟用 **[Auto clear recent search history when I close the browser]** 選項。

Display Avira search results when I type keywords or invalid URLs into the browser address bar

如果啟用此選項，每次您在網頁瀏覽器位址列中輸入關鍵字或無效的 URL 時都會啟動搜尋並顯示搜尋結果 URL。

More options

Select toolbar language

在 **[Select toolbar language]** 底下，您可以選取 Avira SearchFree Toolbar 的顯示語言。
工具列可用語言有英文、德文、西班牙文、法文、義大利文、葡萄牙文及荷蘭文。

> 注意
> 如可行時，預設 Avira SearchFree Toolbar 語言會對應您的程式顯示語言。
> 如果工具列沒有您使用的語言，預設語言將變為英文。

Show button text labels

如果您想要隱藏 Avira SearchFree Toolbar 圖示旁的文字，請停用 **[Show button text labels]** 選項。

Clear history

如果您不要儲存先前的搜尋項目而想要立即清除記錄，請啟用 **[Clear history]** 選項。

Help

按一下 **[Help]** 存取內含相關工具列常見問題集 (FAQs) 的網站。

Uninstall

您也可以在 Firefox 中直接解除安裝 Avira SearchFree Toolbar：透過網頁瀏覽器解除安裝。

About

按一下 **[About]** 顯示安裝 Avira SearchFree Toolbar 的版本。

Google Chrome

在 Chrome 網頁瀏覽器中，下列 Avira SearchFree Toolbar 的組態選項皆可在紅色 Avira 雨傘功能表底下使用：

Help

按一下 **[Help]** 存取內含相關工具列常見問題集 (FAQs) 的網站。

解除安裝說明

您可以在此連結至含有解除安裝工具列所需資訊的文章。

About

按一下 **[About]** 顯示安裝 Avira SearchFree Toolbar 的版本。

顯示/隱藏 Avira SearchFree Toolbar

按一下這裡可在您的網頁瀏覽器上隱藏或顯示 Avira SearchFree Toolbar。

4.2.3 解除安裝

若要解除安裝 Avira SearchFree Toolbar (例如使用 Windows 7)：

- 經由 Windows **[開始]** 功能表，開啟 **[控制台]**。
- 按兩下 **[程式和功能]**。
- 在清單中選取 **Avira SearchFree Toolbar plus Web Protection**，然後按一下 **[解除安裝]**。
  - ↪ 系統會詢問您是否確定要解除安裝此產品。
- 按一下 **[是]** 確認。
  - ↪ Avira SearchFree Toolbar plus Web Protection 已解除安裝，而且當您的電腦重新啟動時，Avira SearchFree Toolbar plus Web Protection 的所有目錄、檔案與登錄項目都會一併刪除。

透過網頁瀏覽器解除安裝

您也可以選擇在瀏覽器中直接解除安裝 Avira SearchFree Toolbar。 此選項僅適用於 **Firefox 與 Internet Explorer**：

- 在搜尋工具列中開啟 **[Options]** 功能表。
- 按一下 **[Uninstall]**。
  - ↪ 如果您已經開啟網頁瀏覽器，將詢問您是否要關閉。
- 關閉網頁瀏覽器，然後按一下 **[確定]**。

↪ Avira SearchFree Toolbar plus Web Protection
已解除安裝，而且當您的電腦重新啟動時，Avira SearchFree Toolbar plus Web Protection 的所有目錄、檔案與登錄項目都會一併刪除。

> 注意
> 請注意，若要解除安裝 Avira SearchFree Toolbar，必須在增益集管理員中啟用工具列。

解除安裝增益集

因為安裝的工具列被視為增益集，所以也必須解除安裝：

Firefox

按一下 **[工具] > [增益集] > [擴充]**。 您可以在此管理 Avira 增益集：啟用或停用工具列和解除安裝。

Internet Explorer

移至 **[管理增益集] > [工具列和擴充]**。 您可以在此啟用與停用 Avira SearchFree Toolbar 或解除安裝。

Google Chrome

按一下 **[選項] > [擴充]** 即可輕鬆管理工具列：啟用、停用或解除安裝。

4.3 如何...?

「如何...?」章節提供有關授權與產品啟用的簡短說明，以及相關 Avira 產品的重要資訊。選取的簡短文章可作為有關 Avira 產品功能的概觀。不過這些簡短說明仍無法替代說明中心各區段的詳細資訊。

4.3.1 啟用授權

啟用您 Avira 產品的授權：

使用 *.KEY* 授權檔啟用您 Avira 產品的授權。 您可以透過 Avira 的電子郵件取得授權檔。授權檔包含您在單一訂購程序中訂購的所有產品授權。

如果您尚未安裝 Avira 產品：

- 將授權檔儲存在您電腦的本機目錄中。
- 安裝 Avira 產品。
- 安裝期間，請輸入授權檔的儲存位置。

如果您已經安裝 Avira 產品：

- 按兩下 [檔案管理員] 或是啟用電子郵件中的授權檔，然後在 [授權管理員] 開啟時，遵循畫面上的指示進行。

  - 或 -

  在 Avira 產品的控制中心，選取功能表項目 **[說明] > [授權管理]**

> **注意**
> 在 Windows Vista 中，會出現 [使用者帳戶控制] 對話方塊。
> 必要時，請以系統管理員身分登入。 按一下 **[繼續]**。

- 反白授權檔，然後按一下 **[開啟]**。

  ↳ 訊息隨即顯示。

- 按一下 **[確定]** 加以確認。

  ↳ 此時已啟用授權。

- 必要時，請重新啟動系統。

4.3.2 啟用產品

您可以透過下列選項來啟用 Avira 產品：

使用有效的完整授權來啟用

若要使用完整授權來啟用程式，您需要有效的啟用 (內含所購買的授權資料)。您會透過電子郵件收到我們寄發的啟用代碼，或在產品包裝上找到印刷的金鑰。

使用評估授權來啟用

您可以使用自動產生的評估授權來啟用 Avira 產品，以便在一定的時間內測試 Avira 產品的完整功能。

> 注意
> 如需啟用產品或取得測試授權，您需要作用中的網際網路連結。
> 如果無法建立與 Avira 伺服器的連線，請檢查使用的防火牆設定：透過 HTTP 通訊協定與連接埠 80 (網路通訊) 及加密通訊協定 SSL 和連接埠 443 建立連線以啟用產品。 確定您的防火牆沒有封鎖傳入與傳出的資料。
> 首先檢查是否可以使用網頁瀏覽器來存取網頁。

下列說明啟用 Avira 產品的方式：

如果您尚未安裝 Avira 產品：

- 安裝 Avira 產品。
  - ↳ 系統會在安裝期間，要求您選取啟用選項。
- **啟用產品**：使用有效的完整授權來啟用
- **測試產品**：使用評估授權來啟用
- 輸入啟用代碼，使用完整授權來啟用。
- 按 **[下一步]**，確認選取的啟用程序。
- 必要時，輸入個人註冊資料並按 **[下一步]** 加以確認。
  - ↳ 您的授權資料會顯示在下一個視窗中。 您的 Avira 產品已經啟用。

- 請繼續安裝。

如果您已經安裝 Avira 產品：

- 在控制中心，選取功能表項目 **[說明] > [授權管理]**。
  - ↪ *授權精靈*隨即開啟，供您選取啟用選項。
    接下來的產品啟用步驟與上述程序完全相同。

4.3.3 執行自動更新

若要在 Avira 排程管理員建立工作，以自動更新 Avira 產品：

- 在 [控制中心]，選取*系統管理* **> 排程管理員**區段。
- 按一下 + **[插入新工作]** 圖示。
  - ↪ **[工作的名稱和描述]** 對話方塊隨即顯示。
- 給予工作一個名稱，並適當地提供描述。
- 按 **[下一步]**。
  - ↪ **[工作類型]** 對話方塊隨即顯示。
- 從清單選取 **[更新工作]**。
- 按 **[下一步]**。
  - ↪ **[工作時間]** 對話方塊隨即顯示。
- 選取更新時間：

- **立即**
- **每天**
- **每週**
- **間隔**
- **一次**
- **登入**

注意

我們建議進行定期自動更新。 建議的更新間隔：2 小時.

- 必要時，請依據選取項目指定日期。
- 必要時，請選取額外的選項 (可用性需視工作類型而定)：

- **如果時間已過，重新執行工作**
  會執行過去在指定時間無法執行的工作，例如，因為電腦關機而無法執行的工作。
- **連線至網際網路時開始工作 (撥號連線)**
  除了定義的頻率之外，當連線至網際網路時，也會執行工作。

- 按 **[下一步]**。
  - ↳ **[選取顯示模式]** 對話方塊隨即顯示。
- 選取工作視窗的顯示模式：

- **隱藏**：無工作視窗
- **最小化**：僅限進度列
- **最大化**：整個工作視窗

- 按一下 **[完成]**。
  - ↳ 新建立的工作會出現在*系統管理* > **排程管理員**區段的開始頁面，且狀態為啟用 (核取標記)。
- 必要時，停用不要執行的工作。

使用下列圖示，進一步定義工作：

 檢視工作屬性

 編輯工作

 刪除工作

 開始工作

停止工作

4.3.4 啟動手動更新

您以手動開始更新時有多個選項可選擇：開始手動更新時，病毒定義檔與掃描引擎將隨時更新。

若要手動更新 Avira 產品：

- 以滑鼠右鍵按一下工作列中的 Avira 系統匣圖示。
  - ↳ 內容功能表隨即顯示。
- 選取 **[開始更新]**。
  - ↳ **[更新程式]** 對話方塊隨即顯示。

- 或 -

- 在 [控制中心]，選取 **[狀態]**。
- 在 **[上次更新]** 欄位中，按一下 **[開始更新]** 連結。
  - ↳ [更新程式] 對話方塊隨即顯示。

- 或 -

- 在 [控制中心]，選取 **[更新]** 功能表中的 **[開始更新]** 功能表命令。
  - ↳ [更新程式] 對話方塊隨即顯示。

> 注意
> 我們建議進行定期自動更新。建議的更新間隔：2 小時.

> 注意
> 您也可以直接透過 Windows 資訊安全中心，執行手動更新。

4.3.5 使用掃描設定檔來掃描病毒與惡意程式碼

掃描設定檔內含一組要掃描的磁碟機與目錄。

以下為透過掃描設定檔來掃描時的可用選項：

當預先定義的掃描設定檔符合您的需求時，

使用預先定義的掃描設定檔。

當您想要使用自訂掃描設定檔來掃描時，

自訂並套用掃描設定檔 (手動選取)。

當您想要建立自己的掃描設定檔時，

建立並套用新的掃描設定檔。

依據作業系統不同，啟動掃描設定檔時可以使用的圖示也不同：

- Windows XP 與 Windows 2000：

   此圖示會透過掃描設定檔啟動掃描。

- Windows Vista：

  在 Microsoft Windows Vista 中，控制中心目前的權限有限，例如目錄與檔案的存取權限。在控制中心，您只能以延伸的系統管理員權限來執行特定動作與檔案存取。您必須在每次掃描開始時透過掃描設定檔來授予這些延伸的系統管理員權限。

  -  此圖示會透過掃描設定檔啟動有限的掃描。只會掃描 Windows Vista 已授予存取權限的目錄與檔案。
  -  此圖示會以延伸的系統管理員權限來啟動掃描。確認選取後，會針對選取的掃描設定檔掃描其中的所有目錄與檔案。

若要使用掃描設定檔來掃描病毒與惡意程式碼：

- 移至 [控制中心] 並選取 **[PC 防護] > [System Scanner]** 區段。

↳ 預先定義的掃描設定檔隨即顯示。

- 選取其中一項預先定義的掃描設定檔。

  -或-

  調整掃描設定檔 **[手動選取]**。

  -或-

  建立新的掃描設定檔

- 按一下圖示 (Windows XP：  或 Windows Vista： ).
- **[Luke Filewalker]** 視窗隨即顯示，並開始進行系統掃描。

  ↳ 掃描完成時，會顯示結果。

如果您想要調整掃描設定檔：

- 在掃描設定檔中，展開 **[手動選取]**
  檔案樹狀結構，以開啟所有要掃描的磁碟機與目錄。
  - 按一下 **+** 圖示：下一個目錄層級隨即顯示。
  - 按一下 **-** 圖示：下一個目錄層級隨即隱藏。
- 按一下適當目錄層級的相關方塊，反白您要掃描的節點和目錄：

  以下為可用來選取目錄的選項：
  - 目錄，包括子目錄 (黑色勾選標記)
  - 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
  - 無目錄 (無勾選標記)

如果您想要建立新的掃描設定檔：

- 按一下此圖示  **建立新的設定檔**。

  ↳ **[新的設定檔]** 設定檔會顯示在先前建立的設定檔下方。

- 必要時，按一下此圖示，重新命名掃描設定檔  .
- 按一下個別的目錄層級核取方塊，反白要儲存的節點與目錄。

以下為可用來選取目錄的選項：

- 目錄，包括子目錄 (黑色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

4.3.6 使用拖放方式掃描病毒與惡意程式碼

若要使用拖放方式，有系統地掃描病毒與惡意程式碼：

✓ Avira 產品的控制中心已經開啟。

▸ 反白您要掃描的檔案或目錄。

▸ 使用滑鼠左鍵將反白的檔案或目錄拖曳至 **[控制中心]**。

↳ **[Luke Filewalker]** 視窗隨即顯示，並開始進行指定掃描。

↳ 掃描完成時，會顯示結果。

4.3.7 透過內容功能表來掃描病毒與惡意程式碼

若要透過內容功能表，有系統地掃描病毒與惡意程式碼：

▸ 在您要掃描的檔案或目錄上，按一下滑鼠右鍵 (例如，在 [Windows 檔案總管] 中、在桌面上，或是在開啟的 Windows 目錄)。

↳ [Windows 檔案總管] 內容功能表隨即顯示。

▸ 選取內容功能表中的 **[以 Avira 掃描選取的檔案]**。

↳ **[Luke Filewalker]** 視窗隨即顯示，並開始進行指定掃描。

↳ 掃描完成時，會顯示結果。

4.3.8 自動掃描病毒與惡意程式碼

> **Note**
> 安裝後，會在排程管理員中建立**完整系統掃描**掃描工作：以建議的間隔自動執行完整的系統掃描。

若要建立工作以自動掃描病毒與惡意程式碼：

- 在 [控制中心]，選取*系統管理* > **排程管理員**區段。
- 按一下 [+] 圖示。
  - ↳ **[工作的名稱和描述]** 對話方塊隨即顯示。
- 給予工作一個名稱，並適當地提供描述。
- 按 **[下一步]**。
  - ↳ **[工作類型]** 對話方塊隨即顯示。
- 選取 **[掃描工作]**。
- 按 **[下一步]**。
  - ↳ **[選取設定檔]** 對話方塊隨即顯示。
- 選取要掃描的設定檔。
- 按 **[下一步]**。
  - ↳ **[工作時間]** 對話方塊隨即顯示。
- 選取掃描時間：

- **立即**
- **每天**
- **每週**
- **間隔**
- **一次**
- **登入**

- 必要時，請依據選取項目指定日期。
- 必要時，請選取下列額外的選項 (可用性需視工作類型而定)：

  如果時間已過，重新執行工作

  會執行過去在指定時間無法執行的工作，例如，因為電腦關機而無法執行的工作。

- 按 **[下一步]**。

  ↳ **[選取顯示模式]** 對話方塊隨即顯示。

- 選取工作視窗的顯示模式：

- **隱藏**：無工作視窗
- **最小化**：僅限進度列
- **最大化**：整個工作視窗

- 如果您要在完成掃描時自動關閉電腦，請選取 **[完成工作後關閉電腦]** 選項。
  只有當顯示模式設為最小化或最大化時，才能使用此選項。
- 按一下 **[完成]**。

  ↳ 新建立的工作會出現在*系統管理* **> 排程管理員**區段的開始頁面，且狀態為啟用 (核取標記)。

- 必要時，停用不要執行的工作。

使用下列圖示，進一步定義工作：

檢視工作屬性

編輯工作

刪除工作

開始工作

停止工作

4.3.9 指定掃描 Rootkit 和作用中的惡意程式碼

若要掃描作用中的 Rootkit，請使用預先定義的掃描設定檔 **[掃描 Rootkit 和作用中的惡意程式碼]**。

若要有系統地掃描作用中的 Rootkit：

- 移至 [控制中心] 並選取*電腦防護* > **Scanner** 區段。
  - ↳ 預先定義的掃描設定檔隨即顯示。
- 選取預先定義的掃描設定檔 **[掃描 Rootkit 和作用中的惡意程式碼]**。
- 必要時，按一下目錄層級核取方塊，反白要掃描的其他節點與目錄。
- 按一下圖示 (Windows XP：  或 Windows Vista： )。
  - ↳ **[Luke Filewalker]** 視窗隨即顯示，並開始進行指定掃描。
  - ↳ 掃描完成時，會顯示結果。

4.3.10 回應偵測到的病毒與惡意程式碼

針對個別的 Avira 產品保護元件，您可以在 **[組態]** 的 [偵測動作] 區段底下，定義**對偵測到的病毒或有害程式的 Avira 產品回應方式**。

Real-Time Protection 的 ProActiv 元件沒有可設定的動作選項：永遠在 **[Real-Time Protection：可疑應用程式行為]** 視窗中發布偵測通知。

Scanner 的動作選項：

互動式

在互動式動作模式中，Scanner 的掃描結果會顯示在對話方塊中。此選項會啟用為預設值。

如果使用 **Scanner 掃描**，在掃描結束時，您會收到一則警示，內含受影響的檔案清單。

您可以使用即時線上功能表，針對各種受感染的檔案選取要執行的動作。
您可以針對所有受感染的檔案執行標準動作，或是取消 Scanner。

自動

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

Real-Time Protection 的動作選項：

互動式

在互動式動作模式中，會拒絕資料存取並顯示桌面通知。
在桌面通知中，您可以移除偵測到的惡意程式碼，或使用 **[詳細資料]** 按鈕將惡意程式碼傳送至 Scanner 元件，執行進一步病毒管理。 Scanner 會開啟含有偵測通知的視窗，提供您透過內容功能表管理受影響檔案的各種選項 (請參閱偵測 > Scanner)：

自動

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

適用 Mail Protection、Web Protection 的動作選項：

互動式

在互動式動作模式中，一旦偵測到病毒或有害程式，會出現對話方塊供您針對感染的物件選取處理方式。 此選項會啟用為預設值。

自動

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

在互動式動作模式中，您可以針對受感染的物件選取警示中的動作，並按一下 **[確認]** 來執行選取的動作，藉此回應偵測到的病毒與有害程式。

您可以選取下列動作來處理感染的物件：

注意

可用的動作選項視作業系統、防護元件 (Avira Real-Time Protection、Avira Scanner、Avira Mail Protection、Avira Web Protection) 偵測報告及惡意程式碼類型而定。

Scanner 和 Real-Time Protection 的動作 (而不是 ProActiv 偵測)：

修復

檔案已修復。

只有當受感染的檔案可以修復時，才能使用此選項。

重新命名

檔案會以 **.vir* 副檔名重新命名。 如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

隔離區

檔案會封裝為特殊格式 (**.qua*) 並移至硬碟上的隔離區目錄 *INFECTED*，這樣就無法再直接存取。

稍後可以在隔離區中修復此目錄中的檔案，必要時也可傳送至 Avira。

刪除

中找到更多可用的選項。 此處理序在速度上會比 **[覆寫並刪除]** 要來得快速。

如果偵測到開機磁區病毒，可以刪除開機磁區來加以刪除。 會寫入新的開機磁區。

略過

不要採取進一步動作。 受感染的檔案仍會在電腦上繼續運作。

覆寫並刪除

此檔案會以預設範本模式來覆寫，然後刪除。 此檔案無法還原。

警告

這樣可能會導致資料遺失，並對作業系統造成傷害！ 請僅在例外情況下才選取 **[略過]** 選項。

一律忽略

Real-Time Protection 偵測的動作選項：Real-Time Protection 不採取進一步動作。 允許存取檔案。
允許此檔案的所有進一步存取動作，並在電腦重新啟動或更新病毒定義檔之前，不提供任何進一步通知。

複製至隔離區

Rootkit 偵測動作選項：複製偵測的發現到隔離區。

修復開機磁區 | 下載修復工具

動作選項可用於修復偵測到的受感染開機磁區：用於修復感染的磁碟機選項相當多。
如果 Avira 產品無法執行修復，您可以下載用於偵測及移除開機磁區病毒的特殊工具。

注意

如果您對執行中的處理序執行動作，有問題的處理序會先終止，然後執行動作。

ProActiv 元件偵測到狀況時 Real-Time Protection 的動作 (可疑應用程式動作的通知)：

信任的程式

應用程式會繼續執行。 程式已加入許可的應用程式清單中，ProActiv 元件不會監視此程式。 加入至許可的應用程式清單時，監視類型會設為 *[內容]*。
這表示檔案內容保持不變時，ProActiv 元件才不會監視應用程式 (請參閱 應用程式篩選器：要略過的應用程式)。

封鎖程式一次

會封鎖應用程式 (即終止應用程式)。 應用程式的動作持續受到 ProActiv 元件監視。

永遠封鎖此程式

會封鎖應用程式 (即終止應用程式)。 程式已加入封鎖的應用程式清單中，無法再執行 (請參閱 應用程式篩選器：要封鎖的應用程式)。

略過

應用程式會繼續執行。 應用程式的動作持續受到 ProActiv 元件監視。

Mail Protection 動作：內送的電子郵件

移至隔離區

電子郵件 (包括所有附件) 會移至隔離區。 受影響的電子郵件會刪除。
電子郵件本文和所有附件都會以預設內容來取代。

刪除郵件

受影響的電子郵件會刪除。 電子郵件本文和所有附件都會以預設內容來取代。

刪除附件

受感染的附件會以預設內容來取代。
如果電子郵件本文受到影響，會加以刪除並同時以預設內容來取代。
電子郵件本身會遞送出去。

將附件移至隔離區

受感染的附件會放置到隔離區並加以刪除 (以預設內容來取代)。
電子郵件本文會遞送出去。 受影響的附件稍後可由隔離區管理員來遞送。

略過

受影響的電子郵件會遞送出去。

警告

如此一來，病毒與有害程式便可能存取您的電腦系統。 請僅在例外情況下才選取 **[略過]** 選項。

請停用郵件用戶端中的預覽功能，而且絕對不要按兩下附件加以開啟！

Mail Protection 動作：外寄電子郵件

將郵件移至隔離區 (不要傳送)

會將電子郵件 (包括所有附件) 複製到隔離區，而且不會傳送出去。

電子郵件會留在您的電子郵件用戶端寄件匣中。 您的電子郵件程式會出現錯誤訊息。

來自您電子郵件帳戶的其他所有電子郵件，都會接受惡意程式碼掃描。

封鎖郵件的傳送 (不要傳送)

電子郵件不會傳送出去，並會留在您的電子郵件用戶端寄件匣中。

您的電子郵件程式會出現錯誤訊息。

來自您電子郵件帳戶的其他所有電子郵件，都會接受惡意程式碼掃描。

略過

受影響的電子郵件會傳送出去。

警告

病毒與有害程式可以藉由這種方式，入侵電子郵件收件者的電腦系統。

Web Protection 動作：

拒絕存取

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都不會傳送到您的網頁瀏覽器。

網頁瀏覽器上會顯示一則錯誤訊息，通知您已經拒絕存取。

移至隔離區

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都會移至隔離區。
如果受影響的檔案具有參考價值，可以從隔離區管理員復原，或在必要時將其傳送至 Avira 惡意程式碼研究中心。

略過

Web Protection
會將網路伺服器要求的網站與/或傳輸的資料與檔案，傳送到您的網頁瀏覽器。

警告
如此一來，病毒與有害程式便可能存取您的電腦系統。 請僅在例外情況下才選取 **[略過]** 選項。

注意
建議您將任何無法修復的可疑檔案移至隔離區。

注意
您也可以將啟發式掃毒所報告的檔案傳送給我們進行分析。
例如，您可以上傳這些檔案到我們的網站：http://www.avira.tw/sample-upload
您可以透過指定檔案名稱前置詞的 *HEUR/* 或 *HEURISTIC/* 啟發式掃毒報告來識別檔案，例如：*HEUR/testfile.**。

4.3.11 處理隔離區檔案 (*.qua)

若要處理隔離區檔案：

- 在 [控制中心] 選取*系統管理* > **隔離區**區段。
- 檢查哪些檔案受到影響，必要時，可以從其他位置將原始檔案重新載入至電腦。

如果您想要了解檔案詳細資訊：

- 反白檔案，然後按一下  。
  - ↳ **[屬性]** 對話方塊隨即顯示，內含檔案的詳細資訊。

如果您想要重新掃描檔案：

如果 Avira 產品的病毒定義檔已經更新，並懷疑報告為誤判情況時，建議您掃描檔案。您可以藉由重新掃描來確認遭到誤判的檔案，然後還原該檔案。

- 反白檔案，然後按一下  。
  - ↳ 您可以使用系統掃描設定，掃描檔案中是否有病毒與惡意程式碼。
  - ↳ 掃描完畢後會顯示 **[掃描統計資料]** 對話方塊，內含重新掃描前後的檔案狀態統計資料。

若要刪除檔案：

- 反白檔案，然後按一下  。
- 您必須選擇 **[是]** 確認選擇。

如果您要將檔案上傳至 Avira 惡意程式碼研究中心網路伺服器，進行分析：

- 反白您要上傳的檔案。
- 按一下  圖示。
  - ↳ 這時會開啟內含表單的對話方塊，供您輸入連絡資料。
- 請輸入所有必要的資料。
- 選擇類型：**可疑的檔案或疑似 誤判的檔案**。
- 選擇回應格式：**HTML、文字、HTML 與文字**。
- 按一下 **[確定]**。
  - ↳ 檔案隨即以壓縮形式上傳至 Avira 惡意程式碼研究中心網路伺服器。

注意

在下列情況中，建議由 Avira 惡意程式碼研究中心進行分析：

啟發式掃毒 (可疑的檔案)：掃描期間由 Avira 產品分類為可疑的檔案並移至隔離區：建議由 Avira 惡意程式碼研究中心分析病毒偵測對話方塊或透過掃描產生的報告檔案中的檔案。

可疑的檔案：您將視為可疑的檔案移至隔離區，但是針對檔案進行的病毒與惡意程式碼掃描結果卻沒問題。

疑似誤判的檔案：您假設病毒偵測為誤判：您的 Avira 產品回報檔案中的偵測發現，但不太像是被惡意程式碼感染的狀況。

注意

上傳的檔案大小上限為 20 MB (未壓縮) 或 8 MB (壓縮)。

注意

您一次只能上傳一個檔案。

如果您要從隔離區將隔離區物件複製到另一個目錄：

- 反白隔離區物件，然後按一下  。
  - ↳ *[瀏覽資料夾]* 對話方塊隨即開啟，供您選取目錄。
- 選取您要儲存隔離區物件複本的目錄，並確認選擇。
  - ↳ 選取的隔離區物件會儲存到選取的目錄。

注意

隔離區物件不同於還原的檔案。

隔離區物件已加密，無法以其原始格式執行或讀取。

如果您要將隔離區物件的屬性匯出至文字檔中：

- 反白隔離區物件，然後按一下  。
  - ↪ 文字檔*隔離區 - 記事本*會開啟，其中包含選取的隔離區物件資料。
- 儲存文字檔。

您也可以還原隔離區的檔案 (請參閱下列章節：隔離區：還原隔離區的檔案)。

4.3.12 還原隔離區的檔案

不同的作業系統，會以不同的圖示來控制還原程序：

- Windows XP：
  -  此圖示可將檔案還原至原始目錄。
  -  此圖示可將檔案還原至自選的目錄。
- Windows Vista：

  在 Microsoft Windows Vista
  中，控制中心目前僅具有有限的權限，例如存取目錄與檔案。
  在控制中心，您只能以延伸的系統管理員權限來執行特定動作與檔案存取。
  您必須在每次掃描開始時透過掃描設定檔來授予這些延伸的系統管理員權限。
  -  此圖示可將檔案還原至自選的目錄。
  -  此圖示可將檔案還原至原始目錄。
    如果需要透過延伸的系統管理員權限來存取此目錄，系統會顯示對應的要求。

若要還原隔離區的檔案：

> **警告**
> 這樣可能會導致資料遺失，並對電腦作業系統造成傷害！
> 請僅在例外情況下，才使用 **[還原選取的物件]** 功能。
> 請在全新的掃描能夠修復檔案時，才加以還原。

✓ 重新掃描與修復的檔案。

- 在 [控制中心] 選取*系統管理* > **隔離區**區段。

> 注意
>
> 如果副檔名是 **.eml*，電子郵件與其附件只能透過  選項來還原。

若要將檔案還原至原始位置：

- 反白檔案，然後按一下圖示 (Windows XP：  、Windows Vista )。

電子郵件不適用此選項。

> 注意
>
> 如果副檔名是 **.eml*，電子郵件與其附件只能透過  選項來還原。

↳ 會顯示一則訊息，詢問您是否要還原檔案。

- 按一下 **[是]**。

↳ 檔案會還原至當初尚未移至隔離區之前的所在目錄。

若要將檔案還原至指定目錄：

- 反白檔案，然後按一下  。

↳ 會顯示一則訊息，詢問您是否要還原檔案。

- 按一下 **[是]**。

↳ 會顯示 Windows 預設視窗 *[另存新檔]* 供您選取目錄。

- 請選取要還原檔案的目錄，並確認選取。

↳ 檔案會還原至選取的目錄。

4.3.13 將可疑的檔案移至隔離區

若要將可疑的檔案手動移至隔離區：

- 在 [控制中心] 選取*系統管理* > **隔離區**區段。
- 按一下 [+] 圖示。
  - ↳ 會顯示 Windows 預設視窗供您選取檔案。
- 請選取檔案並按下 **[開啟]** 加以確認。
  - ↳ 這時檔案已移至隔離區。

您可以利用 Avira Scanner 掃描隔離區中的檔案
(請參閱下列章節：隔離區：處理隔離區檔案 (*.qua))。

4.3.14 修訂或刪除掃描設定檔中的檔案類型

若要指定要掃描的額外檔案類型，或是從掃描設定檔中排除特定檔案類型
(只能透過手動選取與自訂的掃描設定檔)：

✓ 在 [控制中心] 中，移至*電腦防護* > **Scanner** 區段。

- 請以滑鼠右鍵按一下您要編輯的掃描設定檔。
  - ↳ 內容功能表隨即顯示。
- 選取 **[檔案篩選器]**。
- 按一下內容功能表右側的小三角形，進一步展開內容功能表。
  - ↳ **[預設值]**、**[掃描所有檔案]** 與 **[使用者定義]** 項目隨即顯示。
- 選取 **[使用者定義]**。
  - ↳ **[副檔名]** 對話方塊隨即顯示，內含此掃描設定檔要掃描的所有檔案類型清單。

如果您想要從掃描中排除某個檔案類型：

- 反白檔案類型，然後按一下 **[刪除]**。

如果您想要將某個檔案類型新增至掃描：

- 反白檔案類型。
- 按一下 **[插入]** 並在輸入方塊中輸入檔案類型的副檔名。

  最多可接受 10 個字元，而且不可在字元之前輸入句點。 可以使用萬用字元 (* 與 ?) 來取代相關字元。

4.3.15 為掃描設定檔建立桌面捷徑

您可以直接透過桌面的掃描設定檔捷徑來啟動系統掃描，無須存取 Avira 產品的控制中心。

若要為掃描設定檔建立桌面捷徑：

✓ 在 [控制中心] 中，移至*電腦防護* > **Scanner** 區段。

- 選取您要建立捷徑的掃描設定檔。
- 按一下  圖示。

  ↳ 立即建立桌面捷徑。

4.3.16 篩選事件

Avira 產品程式元件所產生的事件會顯示在控制中心的 *系統管理* > **事件** (Windows 作業系統類比事件顯示) 底下。 程式元件會依字母順序排列如下：

- Backup
- FireWall
- 協助程式服務
- Mail Protection
- Real-Time Protection
- Safe Browsing
- 排程管理員
- Scanner

- 更新程式
- Web Protection

會顯示下列事件類型：

- *資訊*
- *警告*
- *錯誤*
- *偵測的發現*

若要篩選顯示的事件：

- 在 [控制中心]，選取*系統管理* > **事件**區段。
- 勾選程式元件方塊，顯示啟用的元件事件。

  - 或 -

  取消勾選程式元件方塊，隱藏停用的元件事件。
- 勾選事件類型方塊以顯示這些事件。

  - 或 -

  取消勾選事件類型方塊以隱藏這些事件。

4.3.17 排除不要掃描的電子郵件地址

定義哪些電子郵件地址 (寄件者) 要從 Mail Protection 掃描 (白名單) 中排除：

- 移至 [控制中心] 並選取*網際網路防護* > **Mail Protection** 區段。

  ↪ 此名單會顯示內送的電子郵件。
- 反白您要從 Mail Protection 掃描中排除的電子郵件。
- 按一下適當的圖示，從 Mail Protection 掃描中排除電子郵件：

-  不再針對選取的電子郵件地址，掃描其中是否有病毒與有害的程式。
-  不再掃描選取的電子郵件地址來尋找垃圾郵件。

↳ 會將電子郵件寄件者地址包含在排除清單中，未來將不再掃描其中是否含有病毒、惡意程式碼或垃圾郵件。

警告

僅從 Mail Protection 掃描中排除可以完全信任的寄件者電子郵件地址。

注意

在 [組態] 中的 Mail Protection > 一般 > 例外底下，您可以將其他電子郵件地址新增至排除清單，或是從排除清單移除電子郵件地址。

4.3.18 訓練 AntiSpam 模組

AntiSpam 模組內含訓練資料庫。您的個別分類準則會記錄在此訓練資料庫中。經過一段時間後，調整過的內部篩選器、演算法與垃圾郵件評估準則將合乎您的個人準則要求。

若要針對訓練資料庫分類電子郵件：

- 移至 [控制中心] 並選取*網際網路防護* > **Mail Protection** 區段。
  - ↳ 此名單會顯示內送的電子郵件。
- 反白您要分類的電子郵件。
- 按一下適當的圖示，識別標示為垃圾郵件 或想要的郵件，亦即「良好」的電子郵件 。
  - ↳ 電子郵件會輸入至訓練資料庫，並套用至下一個垃圾郵件識別處理序。

注意

您可以在 **Mail Protection > 一般 > AntiSpam** 底下的組態中刪除訓練資料庫。

> 注意
>
> AntiSpam 模組無法用於透過 IMAP 接收的電子郵件。 因為透過 IMAP 接收的電子郵件，無法套用訓練功能 (**[良好的電子郵件 - 用於訓練]**、**[垃圾電子郵件 - 用於訓練]**)。 如果您選取 IMAP 類型的電子郵件，會自動停用訓練功能。

4.3.19 選取 FireWall 的安全性等級

有各種安全性等級可供選擇。 依據選擇的等級，您可以搭配不同的介面卡規則組態選項。

以下為可用的安全性等級：

低

會偵測到洪水攻擊和連接埠掃描。

中

會捨棄可疑的 TCP 和 UDP 封包。

可預防洪水攻擊和連接埠掃描。

(設為預設等級。)

高

電腦不會在網路上顯示出來。

不允許所有外部連線。

可預防洪水攻擊和連接埠掃描。

自訂

使用者定義的規則：一旦選取此安全性等級，程式會自動識別已經修改的介面卡規則。

全部封鎖

所有現有的網路連線都將關閉。

注意

所有預先定義之 Avira FireWall 規則的預設安全性等級設定都是 **[中]**。

若要定義 FireWall 的安全性等級：

- 移至 [控制中心] 並選取*網際網路防護* > **FireWall**。
- 將滑桿移至所需的安全性等級。
  - ↳ 選取的安全性等級會立即套用。

4.3.20 手動建立備份

控制中心中的 Backup 工具可讓您輕鬆、快速地備份個人資料。 在 [Avira Backup] 中，您可以建立所謂的鏡像備份，以便使用最少的資源來儲存最近的資料。 [Avira Backup] 可讓您在備份程序期間掃描資料中的病毒與惡意程式碼。
檔案只要受到感染，就不會儲存起來。

注意

不同於版本備份的是，鏡像備份並不會儲存個別的備份版本。
鏡像備份內含上次備份時的資料庫存。
不過，如果儲存在資料庫存中的檔案已經刪除，後來的備份作業就不會進行任何比對動作，亦即備份中仍舊會存在刪除的檔案。

注意

使用 [Avira Backup]
預設值時，只會儲存修改的檔案，並會掃描檔案中的病毒與惡意程式碼。
您可以在組態的 [Backup] > [設定] 底下變更這些設定。

若要使用 Backup 工具來儲存資料：

- 在控制中心，選取*電腦防護* > **Backup**區段。

↳ 預設的備份設定檔隨即顯示。

- 選取其中一項預設的備份設定檔。

  -或-

  調整備份設定檔 **[手動選取]**。

  -或-

  建立新的備份設定檔

- 請在 **[目的地目錄]** 方塊中，針對選取的設定檔輸入儲存位置。

  備份的儲存位置可以是電腦、連線的網路磁碟機或是卸除式磁碟 (例如 USB 隨身碟或磁碟片) 上的目錄。

- 按一下  圖示。

  ↳ **[Avira Backup]** 視窗隨即顯示，並開始備份。
  備份的狀態與結果會顯示在備份視窗中。

如果您想要修改備份設定檔：

- 在掃描設定檔中，展開 **[手動選取]**
  檔案樹狀結構，以開啟所有要儲存的磁碟機與目錄：

- 按一下 **+** 圖示：下一個目錄層級隨即顯示。
- 按一下 **-** 圖示：下一個目錄層級隨即隱藏。

- 按一下個別的目錄層級方塊，反白要儲存的節點與目錄：

  以下為可用的組態選項，請選取目錄：

- 目錄，包括子目錄 (黑色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

如果您想要建立新的備份設定檔：

- 按一下  **[建立新的設定檔]** 圖示。

↳ **[新的設定檔]** 設定檔會顯示在先前建立的設定檔下方。

- 必要時，按一下  圖示，賦予備份設定檔一個名稱。
- 按一下個別目錄層級的核取方塊，反白要儲存的節點與目錄。

以下為可用的組態選項，請選取目錄：

- 目錄，包括子目錄 (黑色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

4.3.21 建立自動資料備份

本節將說明如何啟始工作來建立自動資料備份：

- 在 [控制中心]，選取*系統管理* **> 排程管理員**區段。
- 按一下  圖示。

↳ **[工作的名稱和描述]** 對話方塊隨即顯示。

- 給予工作一個名稱，並適當地提供描述。
- 按 **[下一步]**。

↳ **[工作類型]** 對話方塊隨即顯示。

- 選取 **[Backup 工作]**。
- 按 **[下一步]**。

↳ **[選取設定檔]** 對話方塊隨即顯示。

- 選取要掃描的設定檔。

> 注意
> 只會顯示已經指定儲存位置的備份設定檔。

- 按 **[下一步]**。

↳ **[工作時間]** 對話方塊隨即顯示。

- 選取掃描時間：

- **立即**
- **每天**
- **每週**
- **間隔**
- **一次**
- **登入**
- **隨插即用**
  如果選取做為備份設定檔儲存位置的卸除式磁碟已連線至電腦，則系統一律會建立「隨插即用」事件備份。 若要啟用「隨插即用」備份事件，需要輸入 USB 隨身碟做為儲存位置。

- 必要時，請依據選取項目指定日期。

- 必要時，請選取下列額外的選項 (可用性需視工作類型而定)：

如果時間已過，重新執行工作

會執行過去在指定時間無法執行的工作，例如，因為電腦關機而無法執行的工作。

- 按 **[下一步]**。

↳ **[選取顯示模式]** 對話方塊隨即顯示。

- 選取工作視窗的顯示模式：

- **最小化**：僅限進度列
- **最大化**：整個備份視窗
- **隱藏**：無備份視窗

- 按一下 **[完成]**。

↳ 新建立的工作會出現在*系統管理* **> 排程管理員**區段的開始頁面，且狀態為啟用 (核取標記)。

- 必要時，停用不要執行的工作。

使用下列圖示，進一步定義工作：

 檢視工作屬性

 編輯工作

 刪除工作

 開始工作

 停止工作

5. Scanner

有了 Scanner 元件，您可以針對病毒與有害程式執行鎖定掃描 (指定掃描)。
以下為掃描受感染檔案時的可用選項：

- **透過內容功能表執行系統掃描**
  例如，當您希望掃描個別檔案與目錄時，建議您透過內容功能表執行系統掃描 (滑鼠右鍵的 **[以 Avira 掃描選取的檔案]** 項目)。
  透過內容功能表來執行系統掃描的另一項優勢，則是不需要先啟動控制中心。
- **透過拖放方式進行系統掃描**
  當您將檔案或目錄拖放到控制中心的程式視窗中時，Scanner 會掃描檔案或目錄與其下的所有子目錄。
  例如，當您希望掃描儲存在桌面上的個別檔案與目錄時，建議您使用此程序進行。
- **透過設定檔進行系統掃描**
  當您希望定期掃描特定目錄與磁碟機時 (例如，您經常在其中儲存新檔案的工作目錄或磁碟機)，建議您使用此程序進行。
  如此一來，您不需要針對每個全新的掃描作業重複選取相關目錄與磁碟機，只要選取使用的相關設定檔即可。
- **透過排程管理員進行系統掃描**
  排程管理員可讓您執行有時效的掃描作業。

若要掃描 Rootkit、開機磁區病毒與作用中的處理序時，就需要特殊的程序。
以下為可用的選項：

- 透過掃描設定檔掃描 Rootkit **掃描 Rootkit 與作用中的惡意程式碼**
- 經由掃描設定檔 **[作用中處理序]** 來掃描作用中的處理序
- 經由 **[其他功能]** 功能表中的 **[開機記錄掃描...]** 功能表命令來掃描開機磁區病毒

6. 更新

防毒軟體的有效性取決於程式是否為最新狀態，特別是病毒定義檔與掃描引擎。
為了執行定時更新，我們已將更新程式元件整合在 Avira 產品。 更新程式可確保 Avira 產品保持在最新狀態，而且有能力處理隨時出現的全新病毒。 更新程式會更新下列元件：

- 病毒定義檔：

  病毒定義檔內含 Avira
  產品掃描病毒與惡意程式碼並修復受感染物件時所用的有害程式病毒模式。

- 掃描引擎：

  搜尋引擎內含 Avira 產品用來掃描病毒與惡意程式碼的方法。

- 程式檔案 (產品更新)：

  產品更新的更新套件可為個別程式元件提供額外的功能。

更新檢查會核對病毒定義檔、掃描引擎和產品是否為最新狀態，必要時會執行更新。
在產品更新後，您可能必須重新啟動電腦系統。
如果只更新病毒定義檔與掃描引擎，電腦不必重新啟動。

當產品更新需重新開機時，您可判斷是否要繼續更新或在稍後重複提醒更新。
若您繼續產品更新，仍可在重新開機後選擇。

若您要讓提醒在稍後出現，病毒定義檔及掃描引擎將會更新，但不會完成產品更新。

> 注意
> 在完成重新開機之前，將不會完成產品更新。
>
> 注意
> 為了安全起見，更新程式會檢查電腦中的 Windows
> 主機檔案是否遭到竄改。舉例來說，惡意程式碼可以藉由這種方式操控更新
> URL，使得更新程式被導向至有害的下載網站。 一旦發生 Windows
> 主機檔案遭到竄改的情形，便會顯示在更新程式報告檔中。

更新會依下列間隔自動執行：2 小時。

您可以在控制中心的**排程管理員**底下建立其他更新工作，讓更新程式在指定的時間間隔內執行這些工作。 您也可以選擇手動啟動更新：

- 在控制中心：**[更新]** 功能表與 **[狀態]** 區段中
- 經由系統匣圖示的內容功能表

您可以經由網際網路從製造商的網路伺服器取得更新。 現有的網路連線是 Avira 下載伺服器的預設連線。 您可以在 [組態] > [更新] 底下的組態中變更此預設設定。

7. FireWall

Avira Internet Security 可讓您根據電腦設定來管理傳入與傳出的資料流量：

- Avira FireWall

如果您的作業系統版本升級至 Windows 7，您的 Avira Internet Security 將包含 Avira FireWall。

8. Backup

建立資料備份時，您可以使用以下各種選項：

透過 Backup 工具備份

您可以使用 Backup 工具來選取或建立 Backup 設定檔，並針對選取的設定檔手動啟動 Backup 作業。

透過排程管理員中的 Backup 工作來備份

[排程管理員] 可讓您選擇建立排程或事件控制的備份工作。 [排程管理員] 會自動執行備份工作。 如果您想要針對特定資料定期進行備份，這個處理序會特別有用。

9. 常見問題集、秘訣

本章包含使用 Avira 產品的所有疑難排解與進一步秘訣的重要資訊。

- 請參閱下列章節：發生問題時的說明
- 請參閱下列章節：快捷鍵
- 請參閱下列章節：Windows 資訊安全中心 (Windows XP 及 Vista) 或 Windows 行動作業中心 (Windows 7 和 8)

9.1 發生問題時的說明

您可在此找到原因相關資訊與各種疑難雜症的解決方案。

- 出現*授權檔案無法開啟*的錯誤訊息。
- 嘗試啟動更新時，出現*下載檔案時連線中斷* ... 的錯誤訊息。
- 無法移動或刪除病毒與惡意程式碼。
- 系統匣狀態圖示已停用。
- 執行資料備份時，電腦變得非常慢。
- 在啟用後我的防火牆立即回報 Avira Real-Time Protection 與 Avira Mail Protection。
- Avira Mail Protection 沒有作用。
- 當主機電腦安裝有 Avira FireWall，並將 Avira FireWall 的安全性等級設為*中*或*高*時，虛擬機器 (例如，VMWare、Virtual PC) 沒有可用的網路連線。
- 當 Avira FireWall 的安全性等級設為*中*或*高*時，會封鎖虛擬私人網路 (VPN) 連線。
- 經由 TLS 連線傳送的電子郵件已被 Mail Protection 封鎖。
- 網路聊天無法使用：聊天訊息將不會顯示

出現*授權檔案無法開啟*的錯誤訊息。

原因：檔案已加密。

- 若要啟用授權，您不需要開啟授權檔案，只要將其儲存在程式中的目錄開啟即可。

嘗試啟動更新時，出現 *下載檔案時連線中斷* ... 的錯誤訊息。

原因：您的網際網路連線沒有作用。 因此無法在網際網路上與網路伺服器建立連線。

- 測試 WWW 或電子郵件之類的其他網際網路服務是否能夠正常運作。
  如果無法運作，請重新建立網際網路連線。

原因：無法連線 Proxy 伺服器。

- 檢查 Proxy 伺服器的登入資料是否已經變更，必要時依據自己的組態加以調整。

原因：您的個人防火牆並未完全核准 *update.exe* 檔案。

- 請確保您的個人防火牆已完全核准 *update.exe* 檔案。

或是：

- 檢查 [組態] (專家模式) 中電腦防護 > 更新底下的設定。

無法移動或刪除病毒與惡意程式碼。

原因：檔案已由 Windows 載入，且為作用中。

- 請更新 Avira 產品。
- 如果您使用 Windows XP 作業系統，請停用 [系統還原]。
- 將電腦啟動在 [安全模式]。
- 啟動 Avira 產品的 [組態] (專家模式)。
- 選取**Scanner > 掃描 > 檔案 > 所有檔案**和利用 **[確定]** 視窗確認。
- 針對所有本機磁碟機啟動掃描。
- 將電腦啟動在 [一般模式]。
- 在一般模式下執行掃描。
- 如果沒有找到任何病毒或惡意程式碼，則啟用 [系統還原] (如果可供使用的話)。

系統匣狀態圖示已停用。

原因：Avira Real-Time Protection 已停用。

- 在控制中心中，按一下 **[狀態]** 並啟用 **[電腦防護]** 區域中的 *[Real-Time Protection]*。

-或-

- 用滑鼠右鍵按一下 [系統匣] 圖示以開啟內容功能表。 按一下 **[啟用 Real-Time Protection]**。

原因：Avira Real-Time Protection 被防火牆封鎖。

- 在防火牆的組態中，定義 Avira Real-Time Protection 的一般核准設定。 Avira Real-Time Protection 僅能用於位址 127.0.0.1 (localhost)。
  不會建立網際網路連線。 相同設定可套用至 Avira Mail Protection。

或是：

- 檢查 Avira Real-Time Protection 服務的啟動類型。
  必要時可啟用服務：在工作列中選取 **[開始] > [設定] > [控制台]**。
  按兩下滑鼠來啟動**服務**組態面板 (在 Windows XP 環境下，服務 Applet 位於 *[系統管理工具]* 子目錄中)。 尋找 *[Avira Real-Time Protection]* 項目。
  啟動類型必須是自動，且狀態必須是已啟動。 必要時，請選取相關字行並按下 **[啟動]** 按鈕，手動啟動該服務。 出現錯誤訊息時，請檢查事件顯示。

執行資料備份時，電腦變得非常慢。

原因：在備份程序期間，Avira Real-Time Protection 會掃描備份程序使用的所有檔案。

- 在 [組態 (專家模式)] 中選取 **[Real-Time Protection] > [掃描] > [例外]**，然後輸入備份軟體處理序的名稱。

在啟用後我的防火牆立即回報 Avira Real-Time Protection與 Avira Mail Protection。

原因：經由 TCP/IP 網際網路通訊協定與 Avira Real-Time Protection 和 Avira Mail Protection 進行通訊。 防火牆可透過此通訊協定監視所有連線。

- 定義 Avira Real-Time Protection 與 Avira Mail Protection的一般核准設定。
  Avira Real-Time Protection 僅能用於位址 127.0.0.1 (localhost)。
  不會建立網際網路連線。 相同設定可套用至 Avira Mail Protection。

Avira Mail Protection 沒有作用。

如果 Avira Mail Protection 發生問題，請利用下列檢查清單確認 Avira Mail Protection 運作是否正確。

檢查清單

- 檢查您的郵件用戶端是否能夠透過 Kerberos、APOP 或 RPA 來登入伺服器。
  目前不支援這些驗證方法。
- 檢查您的郵件用戶端是否能夠透過 SSL (也稱為 TLS – 傳輸層安全性) 回報伺服器。
  Avira Mail Protection 不支援 SSL，因此會終止任何加密 SSL 連線。
  如果您想要使用不受 Mail Protection 保護的加密 SSL 連線，必須對此連線使用不受 Mail Protection 監視的連接埠。 由 Mail Protection 監視的連接埠可在 **[Mail Protection] > [掃描]** 底下的組態中設定。
- Avira Mail Protection 服務是否啟用？ 必要時可啟用服務：在工作列中選取 **[開始] > [設定] > [控制台]**。 按兩下滑鼠來啟動**服務**組態面板 (在 Windows XP 環境下，服務 Applet 位於 *[系統管理工具]* 子目錄中)。 尋找 *[Avira Mail Protection]* 項目。 啟動類型必須是自動，且狀態必須是已啟動。
  必要時，請選取相關字行並按下 **[啟動]** 按鈕，手動啟動該服務。
  出現錯誤訊息時，請檢查事件顯示。 如果沒有成功，您可能需要經由 **[開始] > [設定] > [控制台] > [新增或移除程式]**，來完整解除安裝 Avira 產品並重新啟動電腦，接著重新安裝。

一般

目前無法保護以 SSL (安全通訊端層，通常亦稱為 TLS (傳輸層安全性)) 加密的 POP3 連線，因此會加以略過。

目前僅支援透過「密碼」對郵件伺服器進行驗證， 目前不支援「Kerberos」與「RPA」。

Avira 產品不會檢查外寄電子郵件中的病毒與有害程式。

> 注意
> 建議您定期安裝 Microsoft 更新來修補任何安全漏洞。

當主機電腦安裝有 Avira FireWall，並將 Avira FireWall 的安全性等級設為*中*或*高*時，虛擬機器 (例如，VMWare、Virtual PC) 沒有可用的網路連線。

如果在執行虛擬機器 (例如 VMWare、虛擬電腦等) 的電腦上安裝 Avira FireWall，檔 Avira FireWall 的安全性等級設為*中*或*高*時，Avira FireWall 會封鎖虛擬機器的所有網路連線。 如果將安全性等級設為*低*，FireWall 會允許網路連線。

原因：虛擬機器會透過軟體模擬網路卡運作。
此模擬機制會將虛擬系統的資料封包封裝在特殊封包 (UDP 封包) 並透過外部閘道將這些封包引導至原本的主機系統。 Avira FireWall 會從安全性等級*中*開始，拒絕來自外部的封包。

若要避免此行為發生，請執行下列步驟：

- 移至 [控制中心] 並選取區段 *[網際網路防護]* > **[FireWall]**。
- 按一下 **[組態]** 按鈕。

  [組態] 對話方塊隨即顯示。 您目前位於 *[應用程式規則]* 的組態區段中。
- 啟用 **[專家模式]** 選項。
- 選取 **[介面卡規則]** 組態區段。

- 按一下 **[新增規則]**。
- 選取 **[傳入規則]** 區段中的 *[UDP]*。
- 在規則的 **[區段名稱]** 中輸入規則名稱。
- 按一下 **[確定]**。
- 檢查該規則是否直接優先於 **[拒絕所有 IP 封包]** 規則。

> **警告**
> 此規則有可能造成危險，因為它能讓 UDP 封包直接進入而不經過篩選！
> 使用過虛擬機器後，請變更為原本的安全性等級。

當 Avira FireWall 的安全性等級設為*中*或*高*時，會封鎖虛擬私人網路 (VPN) 連線。

原因：依預設會捨棄不符合預先設定規則的所有封包。 VPN 軟體所發送的封包 (所謂的 GRE 封包) 不符合其他類別，因此會遭到這些規則篩選。

在 Avira FireWall 組態的 **[介面卡規則]** 中，新增規則**允許 VPN 連線**。
此規則將允許所有的 VPN 相關封包。

經由 TLS 連線傳送的電子郵件已被 Mail Protection 封鎖。

原因：Mail Protection 目前不支援傳輸層安全性
(TLS：網際網路上的資料傳輸加密通訊協定)。 以下為傳送電子郵件時可用的選項：

- 使用連接埠 25 (SMTP 使用的連接埠) 以外的其他連接埠。 Mail Protection 將略過監視。
- 關閉 TLS 加密連線並停用電子郵件用戶端中的 TLS 支援。
- 在 **[Mail Protection] > [掃描]** 底下的組態中停用 (暫時) Mail Protection 掃描外寄電子郵件。

網路聊天無法使用：聊天訊息無法顯示；資料正在載入瀏覽器。

此現象可能會在以 HTTP 通訊協定為基礎，且內含 'transfer-encoding: chunked' 的聊天中出現。

原因：Web Protection
首先會完整檢查傳送的資料中是否有病毒與有害程式，然後再將資料載入網路瀏覽器。在使用 ‘transfer-encoding: chunked’ 進行資料傳輸期間，Web Protection 無法判斷訊息長度或資料量。

- 請將網路聊天 URL 組態輸入為例外 (請參閱組態：**Web Protection > 掃描 > 例外**)。

9.2 快捷鍵

鍵盤命令 (亦稱為快捷鍵) 可讓您快速瀏覽與擷取個別模組，並透過程式啟動相關動作。

以下列出可用的鍵盤命令概觀。 請在對應的說明章節中，找到各項功能的相關介紹。

9.2.1 在對話方塊中

快捷鍵	說明
Ctrl + Tab **Ctrl + Page down**	控制中心的瀏覽 移至下一個區段。
Ctrl + Shift + Tab **Ctrl + Page up**	控制中心的瀏覽 移至上一個區段。

←↑→↓	組態區段中的瀏覽 首先，請使用滑鼠設定組態區段中的焦點。 在標示的下拉式清單中，或於選項群組中的各個選項之間切換選項。
Tab	變更至下一個選項或選項群組。
Shift + Tab	變更至上一個選項或選項群組。
空格鍵	啟用或停用核取方塊 (作用中的選項必須是核取方塊)。
Alt + **含底線的字元**	選取選項或啟動命令。
Alt + ↓ **F4**	開啟選取的下拉式清單。
Esc	關閉選取的下拉式清單。 取消命令與關閉對話方塊。
Enter	針對作用中的選項或按鈕啟動命令。

9.2.2 在說明中

快捷鍵	說明
Alt + 空格鍵	顯示系統功能表。
Alt + Tab	切換說明與其他開啟的視窗。
Alt + F4	關閉說明。
Shift + F10	顯示說明的內容功能表。
Ctrl + Tab	移至瀏覽視窗的下一個區段。
Ctrl + Shift + Tab	移至瀏覽視窗的上一個區段。
Page up	變更至顯示在內容、索引或是搜尋結果清單上方的主題。
Page down	變更至顯示在內容、索引或是搜尋結果清單下方的主題。

Page up **Page down**	瀏覽主題。

9.2.3 在控制中心中

一般

快捷鍵	說明
F1	顯示說明
Alt + F4	關閉控制中心
F5	重新整理
F8	開啟組態
F9	開始更新

掃描區段

快捷鍵	說明
F2	重新命名選取的設定檔
F3	以選取的設定檔開始掃描
F4	為選取的設定檔建立桌面連結
Ins	建立新的設定檔

Del	刪除選取的設定檔

FireWall 區段

快捷鍵	說明
Return	屬性

隔離區區段

快捷鍵	說明
F2	重新掃描物件
F3	還原物件
F4	傳送物件
F6	將物件還原至...
Return	屬性
Ins	新增檔案

Del	刪除物件

排程管理員區段

快捷鍵	說明
F2	編輯工作
Return	屬性
Ins	插入新工作
Del	刪除工作

報告區段

快捷鍵	說明
F3	顯示報告檔
F4	列印報告檔
Return	顯示報告
Del	刪除報告

事件區段

快捷鍵	說明
F3	匯出事件
Return	顯示事件
Del	刪除事件

9.3 Windows 資訊安全中心

- Windows XP Service Pack 2 至 Windows Vista -

9.3.1 一般

Windows 資訊安全中心會檢查電腦狀態以了解重要的安全層面。

一旦在這些要點中偵測到問題
(例如，過時的防毒程式)，資訊安全中心就會發出警示並針對如何保護電腦安全提供相關建議。

9.3.2 Windows 資訊安全中心與您的 Avira 產品

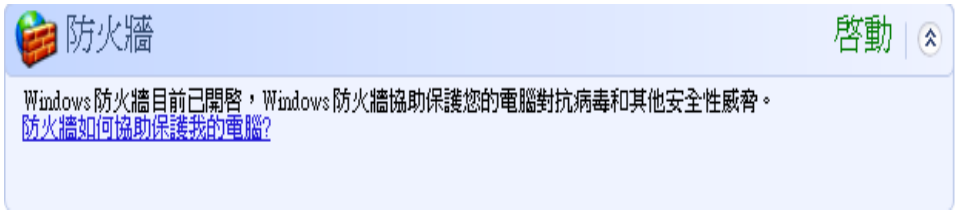
FireWall

您可能會從資訊安全中心收到有關防火牆的下列資訊：

- FireWall 啟用/FireWall 啟動
- FireWall 停用/FireWall 關閉

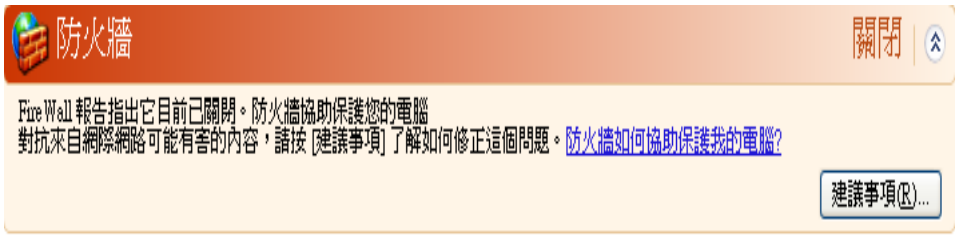
FireWall 啟用/FireWall 啟動

在安裝 Avira 產品並關閉 Windows 防火牆 後，您會收到下列訊息：



FireWall 停用/FireWall 關閉

當您停用 Avira FireWall 時，將會立即收到下列訊息：



> 注意
>
> 您可以經由控制中心的狀態索引標籤，啟用或停用 Avira FireWall。

> 警告
>
> 如果您將 Avira FireWall
> 關閉，未授權的使用者可能會再次透過網路或網際網路擅自存取電腦。

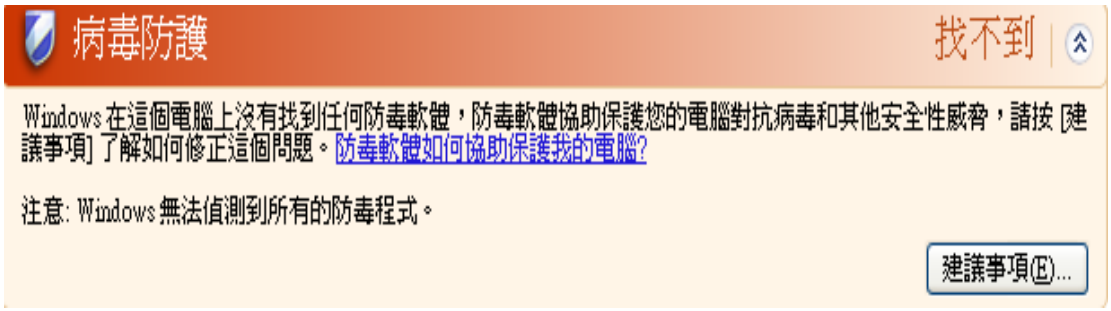
防毒軟體/抵禦惡意軟體

您可能會從 Windows 資訊安全中心收到有關防毒的下列資訊。

- 找不到防毒保護
- 防毒保護已非最新狀態
- 防毒保護已開啟
- 防毒保護已關閉
- 防毒保護未受監視

找不到防毒保護

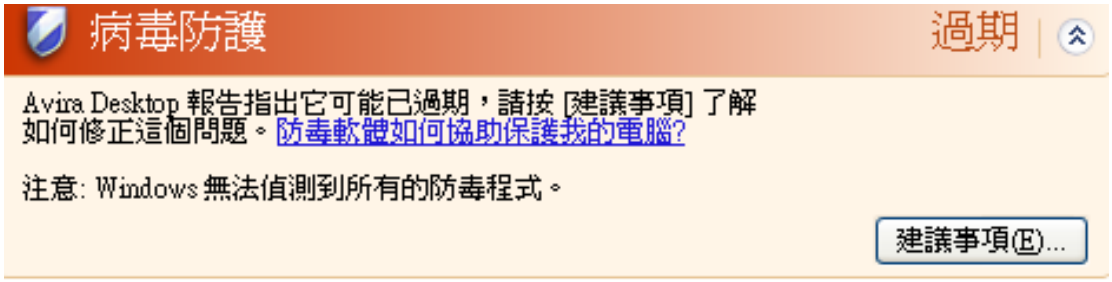
當 Windows 資訊安全中心無法在您的電腦上找到任何防毒軟體時，就會顯示此類資訊。



> 注意
>
> 請在電腦上安裝 Avira 產品，協助電腦防禦病毒與其他有害程式！

防毒保護已非最新狀態

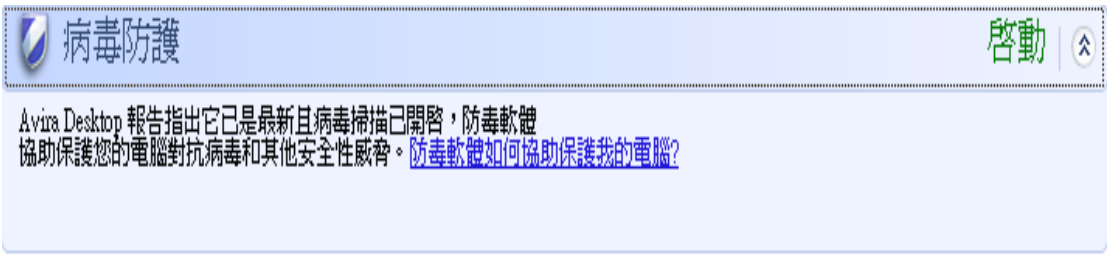
如果您先安裝 Windows XP Service Pack 2 或 Windows Vista 後再安裝 Avira 產品，或是將 Windows XP Service Pack 2 或 Windows Vista 安裝在已經安裝了 Avira 產品的系統上，會收到下列訊息：



> 注意
>
> 為了讓 Windows 資訊安全中心能辨識您的 Avira 產品為最新狀態，必須在安裝後執行更新。 請執行更新來更新系統。

防毒保護已開啟

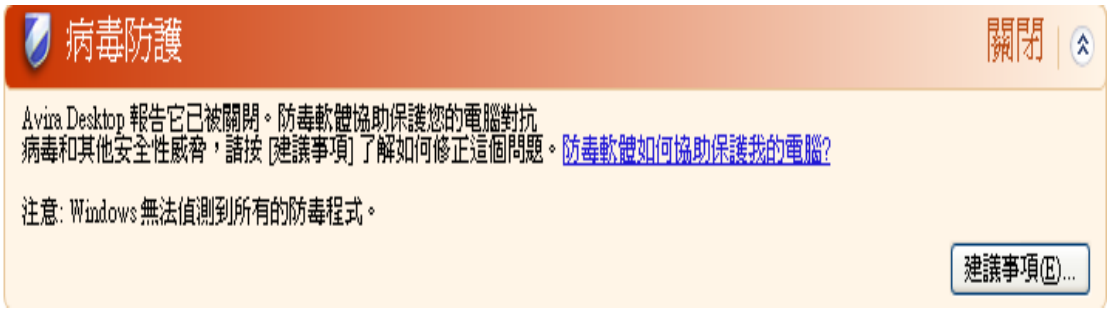
在安裝 Avira 產品及後續更新後，您將會收到下列訊息：



這代表您的 Avira 產品為最新狀態且 Avira Real-Time Protection 已啟用。

防毒保護已關閉

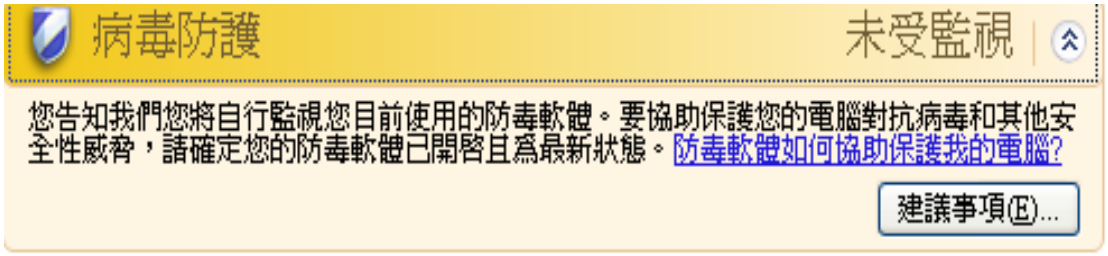
如果您停用 Avira Real-Time Protection 或停止 Real-Time Protection 服務，將會收到下列訊息。



> 注意
>
> 您可以在**控制中心**的狀態區段中啟用或停用 Avira Real-Time Protection。您也可以藉由工作列中的小紅傘圖示是否開啟，來判斷 Avira Real-Time Protection 是否已經啟用。

防毒保護未受監視

如果您從 Windows 資訊安全中心收到下列訊息，表示您已決定自行監視防毒軟體的狀態。



注意

Windows Vista 不支援這項功能。

注意

Avira 產品支援 Windows 資訊安全中心。 您隨時可以透過 **[建議]** 按鈕來啟用這個選項。

注意

即使您已經安裝 Windows XP Service Pack 2 或 Windows Vista，仍舊需要防毒解決方案。 雖然 Windows 會監視您的防毒軟體，本身卻不含任何防毒功能。 因此，如果沒有配備其他防毒解決方案，您將無法防範各種病毒與其他惡意程式碼！

9.4 Windows 行動作業中心

- Windows 7 與 Windows 8 -

9.4.1 一般

注意：

使用 Windows 7 時，**Windows 資訊安全中心已重新命名為Windows 行動作業中心**。 您可以在此區段底下找到所有安全性選項的狀態。

Windows 行動作業中心會檢查電腦狀態以了解重要的安全層面。
您可以按一下工具列中的小旗標直接存取，或移至 **[控制台] > [行動作業中心]** 底下。

一旦在這些要點中偵測到問題
(例如，過時的防毒程式)，行動作業中心就會發出警示並針對如何保護電腦安全提供相關建議。 這表示如果一切正常，您將不會被這些訊息打擾。 您仍可以在 **[安全性]** 項目底下的 **[Windows 行動作業中心]** 中觀看電腦的安全性狀態。
Windows 行動作業中心 也可讓您選擇管理已安裝的程式及選擇項目
(例如*檢視已安裝的防間諜程式*)。

您甚至可以在 **變更行動作業中心設定]** 底下關閉警告訊息
(例如*關閉有關間諜軟體與相關防護的訊息*)。

9.4.2 Windows 行動作業中心與您的 Avira 產品

網路防火牆

您可能會從 **Windows 行動作業中心**中收到有關 FireWall 的下列資訊：

- Avira FireWall 報告目前為開啟。
- Windows 防火牆 與 Avira FireWall 將會一起回報關閉狀態。
- Windows 防火牆 已關閉或設定不正確

Avira FireWall 報告目前為開啟。

在安裝 Avira 產品並關閉 Windows 防火牆 後，您會在 **[行動作業中心] > [安全性] > [網路防火牆]**底下見到下列訊息：*Avira FireWall 報告為開啟狀態*。 這代表您已選擇 Avira FireWall 作為防火牆方案。 (請注意 Windows 防火牆 與 Avira FireWall 之間的差異在於大寫的 W)。

> **警告**
> **在 [控制台] > [Windows 防火牆] 選項底下，只會顯示 Windows 防火牆而不會顯示 Avira FireWall 的產品。**

這就是所有選項都標記為紅色且出現訊息的原因：*更新您的防火牆設定和 **Windows 防火牆未使用建議的設定來保護您的電腦**。*

您什麼事都不需要做，Avira 產品就能發揮效果並保護您的電腦。

Windows 防火牆與 Avira FireWall 將會一起回報關閉狀態

當您停用 Avira FireWall 時，將會立即收到下列訊息：

警告

如果您將 Avira FireWall 關閉，未授權的使用者可能會再次透過網路或網際網路擅自存取電腦。

Windows 防火牆 已關閉或設定不正確

這表示 Windows 的防火牆或 Avira 的防火牆皆未啟動。

- **在 Windows 7 之下**

  Avira FireWall 的設定不正確或安裝錯誤。 Windows 行動作業中心應會立即偵測到 Avira FireWall。 請嘗試將電腦重新開機，如果沒有作用，請再次安裝 Avira。

防毒保護

您可能會從 Windows 行動作業中心收到有關防毒的下列資訊：

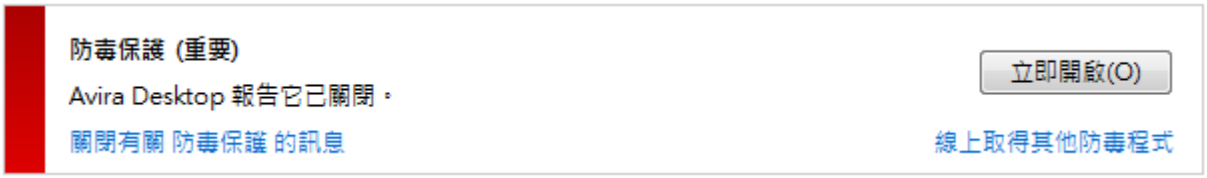
- Avira Desktop 報告目前為最新狀態且病毒掃描為開啟。
- Avira Desktop 報告目前為關閉
- Avira Desktop 報告目前為最新狀態
- Windows 找不到這部電腦上的防毒軟體。
- Avira Desktop 已過期。

Avira Desktop 報告目前為最新狀態且病毒掃描為開啟

在安裝 Avira 產品及後續更新後，您將不會再收到 Windows 行動作業中心的任何訊息。但如果您移至 **[行動作業中心] > [安全性]**，就會看到：*Avira Desktop 報告目前為最新狀態且病毒掃描為開啟。* 這代表您的 Avira 產品為最新狀態且 Avira Real-Time Protection 已啟用。

Avira Desktop 報告目前為關閉

如果您停用 Avira Real-Time Protection 或停止 Real-Time Protection 服務，將會收到下列訊息。



注意

您可以在 **Avira 控制中心**的狀態區段中啟用或停用 Avira Real-Time Protection。 您也會注意到工具列中由打開紅傘啟用的 Avira Real-Time Protection。 也可以按一下 Windows 行動作業中心訊息上的 *[立即開啟]* 按鈕以啟用 Avira 產品。 您將會收到要求提供執行 Avira 的權限通知。 按一下

[是，我信任發行者，並準備執行這個程式]，Real-Time Protection 將再度啟用。

Avira Desktop 報告目前為最新狀態

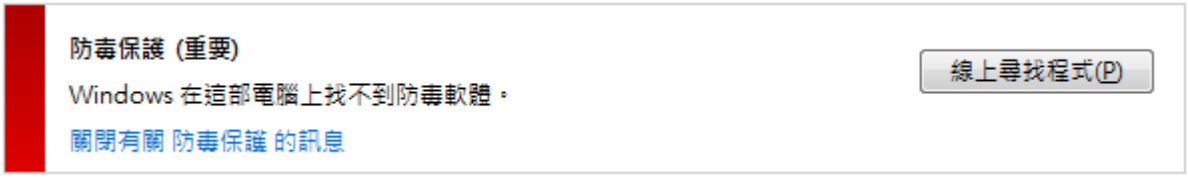
若您只是單純安裝 Avira 或因故只安裝病毒定義檔，則不會自動更新掃描引擎或您 Avira 產品的程式檔（例如，若從舊的 Windows 作業系統升級，且舊系統已安裝 Avira 產品），您會收到下列訊息：

注意

為了讓 Windows 行動作業系統能辨識您的 Avira 產品為最新狀態，必須在安裝後執行更新。 請執行更新來更新 Avira 產品。

Windows 找不到這部電腦上的防毒軟體

當 Windows 行動作業中心無法在您的電腦上找到任何防毒軟體時，就會顯示此類資訊。



注意

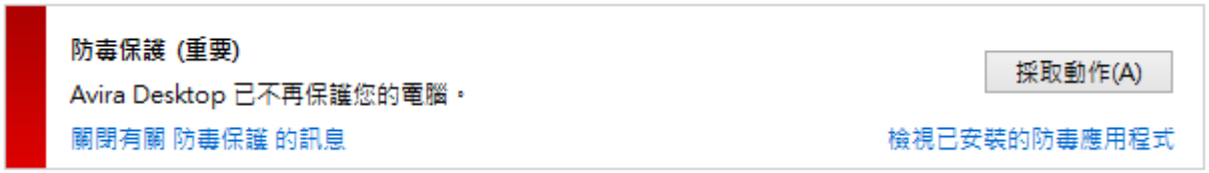
請注意，此選項將不會出現在 Windows 8 中，因為 Windows Defender 現在也有預先設定的病毒防護功能。

注意

請在電腦上安裝 Avira 產品，協助電腦防禦病毒與其他有害程式！

Avira Desktop 已過期。

Avira 產品的授權過期後，就會出現此 Windows 行動作業中心的資訊。
若您按下 **[更新訂閱]** 按鈕，將會重新導向至可購買新授權的 Avira 網站。



> 注意
> 請注意，本選項僅供 Windows 8 使用。

間諜軟體與有害軟體防護

您可能會從 Windows 行動作業中心收到有關間諜軟體防護的下列資訊：

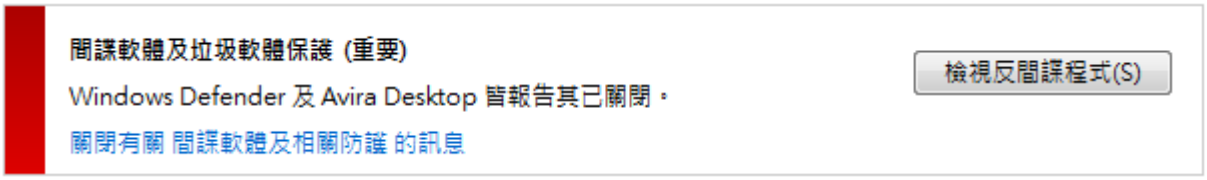
- Avira Desktop 報告目前為開啟。
- Windows Defender 與 Avira Desktop 將會一起回報關閉狀態。
- Avira Desktop 報告目前為最新狀態
- Windows Defender 已過期。
- Windows Defender 關閉。

Avira Desktop 報告目前為開啟

在安裝 Avira 產品及後續更新後，您將不會再收到任何 Windows 行動作業中心的訊息。
但如果您移至**行動作業中心 > 安全性**，就會看到：*Avira Desktop 報告目前為開啟。*
這代表您的 Avira 產品為最新狀態且 Avira Real-Time Protection 已啟用。

Windows Defender 與 Avira Desktop 將會一起回報關閉狀態。

如果您停用 Avira Real-Time Protection 或停止 Real-Time Protection 服務，將會收到下列訊息。



注意

您可以在 **Avira 控制中心**的狀態區段中啟用或停用 Avira Real-Time Protection。 您也會注意到工具列中由打開紅傘啟用的 Avira Real-Time Protection。 也可以按一下 Windows 行動作業中心訊息上的 *[立即開啟]* 按鈕以啟用 Avira 產品。 您將會收到要求提供執行 Avira 的權限通知。 按一下 *[是，我信任發行者，並準備執行這個程式]*，Real-Time Protection 將再度啟用。

Avira Desktop 報告目前為最新狀態

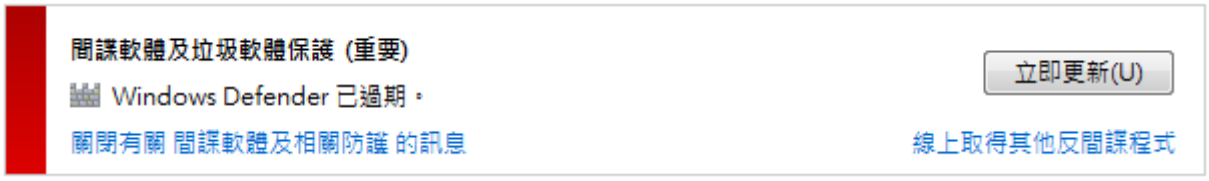
若您只是單純安裝 Avira 或因故只安裝病毒定義檔，則不會自動更新掃描引擎或您 Avira 產品的程式檔（例如，若從舊的 Windows 作業系統升級，且舊系統已安裝 Avira 產品），您會收到下列訊息：

注意

為了讓 Windows 行動作業系統能辨識您的 Avira 產品為最新狀態，必須在安裝後執行更新。 請執行更新來更新 Avira 產品。

Windows Defender 已過期

如果 Windows Defender 已啟用，您也許會收到下列訊息。 如果您已經安裝 Avira 產品，此訊息就不會顯示。 請確認安裝是否正常。

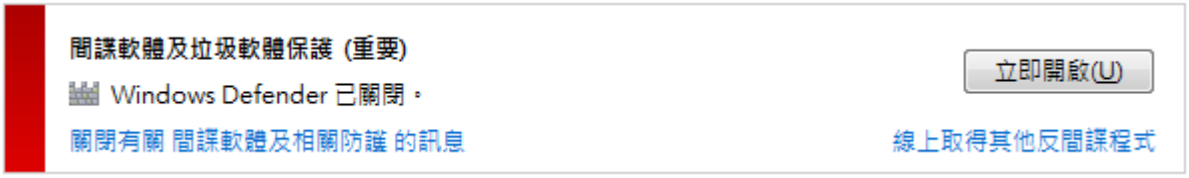


注意

Windows Defender 為 Windows
預先設定的間諜軟體及病毒防護解決方案。

Windows Defender 關閉

Windows 行動作業中心在電腦上找不到作業系統預設：Windows Defender 整合的其他防毒軟體時，就會出現此 Windows 行動作業中心的資訊。
若您先前已在電腦上安裝其他防毒軟體，將會停用本應用程式。 若您已安裝 Avira 產品，不會出現本訊息：Avira 應被自動偵測。 請確認安裝是否正常。



10. 病毒與其他資訊

Avira Internet Security 不僅會偵測病毒和惡意程式碼，還可針對其他威脅提供保護。
在本章中，您可以一覽不同類型的潛伏惡意程式碼與其他威脅的背景、行為和突發的說明。

相關主題：

- 威脅類別
- 病毒與其他惡意程式碼

10.1 威脅類別

廣告軟體

廣告軟體指的是透過電腦畫面上顯示的訊息列來呈現橫幅廣告或快顯視窗的軟體。
這些廣告通常無法移除且會持續顯示。
在資料安全方面，連線資料可以讓人從中得出許多使用行為上的資訊，因此也會造成一些問題。

您的 Avira 產品偵測到廣告軟體。 **[廣告軟體]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品中偵測到廣告軟體時收到對應的警示。

廣告軟體/間諜軟體

這些可能是有害的軟體，因為它們會顯示廣告，或是在使用者不知情或未經使用者同意的情況下，將使用者個人資料傳送給第三方。

您的 Avira 產品識別出「廣告軟體/間諜軟體」。 **[廣告軟體/間諜軟體]** 選項一經啟用 (與組態中 [威脅類別] 底下勾選)，您會在 Avira 產品中偵測到廣告軟體或間諜軟體時收到對應的警示。

應用程式

APPL 一詞表示使用的應用程式可能有風險，或其來源很可疑。

您的 Avira 產品識別出「應用程式 (APPL)」。 **[應用程式]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類行為時收到對應的警示。

後門程式用戶端

後門伺服器程式是基於竊取資料或操縱電腦的目的，在使用者不知情的狀況下私自混進系統中。 這種程式可以由第三方利用後門控制軟體 (用戶端)
透過網際網路或內部網路進行控制。

您的 Avira 產品識別出「後門程式用戶端」。 **[後門程式用戶端]**選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類軟體時收到對應的警示。

撥號木馬程式

網際網路上有某些服務必須付費。 在德國，這類服務都是透過 0190/0900
開頭號碼的撥號木馬程式來開立發票 (在奧地利與瑞士則是透過 09x0
開頭的號碼；在德國，這組號碼會在轉接途中變更為 09x0 開頭)。
一旦安裝在電腦上，這些木馬程式可保證以合適的優惠費率號碼來連線，且各地收費方式都不同。

透過電話帳單來行銷線上內容是合法的，而且對使用者有利。
真正的撥號木馬程式毫無疑問地可由使用者應用在特定用途上。
這些木馬程式只能在使用者同意 (經由完整、不模糊而且可清楚辨識的標籤或要求)
下安裝在使用者的電腦上。 真正的撥號木馬程式會清楚顯示撥接程序。
此外，真正的撥號木馬程式會明確無誤地告知產生的費用。

不過，有些撥號木馬程式會透過模擬兩可的方式，甚至以欺騙的手法偷偷地安裝在電腦上。
例如，它們會取代 ISP (網際網路服務供應商)
的網際網路使用者預設資料通訊連結，並在每次成功連線後，撥出 0190/0900
開頭的號碼 (會產生費用而且經常貴得嚇人)。
受影響的使用者大概在下一次帳單抵達之前，都不會注意到電腦上有害的 0190/0900
撥號木馬程式已經在每次連線時撥出優惠費率號碼，導致電話帳單費用暴增。

建議您直接要求電話業者封鎖這類號碼範圍以便立即防範不需要的撥號木馬程式 (0190/0900 撥號木馬程式)。

Avira 產品預設會偵測到熟悉的撥號木馬程式。

[撥號木馬程式] 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在偵測到撥號木馬程式時收到對應的警示。
現在您可以直接刪除可能有害的 0190/0900 撥號木馬程式。
不過，如果是想要的撥接程式，您可以將其宣告為例外檔案，日後便不會加以掃描。

雙重副檔名檔案

以可疑的方式來隱藏真實副檔名的可執行檔。 這種偽裝的方法是惡意程式碼慣用的伎倆。

您的 Avira 產品識別出「雙重副檔名檔案」。 **[雙重副檔名檔案]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類檔案時收到對應的警示。

詐騙軟體

又稱做「恐嚇軟體」或「流氓軟體」，這種詐騙軟體會佯裝您的電腦已被病毒或惡意程式碼感染。
這種軟體看似與專業的防毒軟體十分相像，但主要目的在於增加不確定性或恐嚇使用者。
用意在於讓受害者對即將發生的不實危險感到害怕，進而付費消除恐懼感。
還有一些情況是，此類軟體會讓受害者相信自己已經遭受攻擊，進而引導他們執行某個動作，而引發真正的攻擊活動。

您的 Avira 產品偵測到恐嚇軟體。 **[詐騙軟體]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類檔案時收到對應的警示。

遊戲

到處都有網咖可供玩遊戲，不過工作場所不見得有 (除非在午休時間)。
不過，隨著網際網路上的可下載遊戲越來越多，公司員工與公僕們也開始迷上踩地雷之類的小遊戲。 您可以經由網際網路下載一系列遊戲。

電子郵件遊戲也逐漸變得流行：在網路上風行的遊戲千變萬化，其中包括簡易的戰棋如「艦隊演習」(包括魚雷作戰)：對應的動作會經由電子郵件程式傳送給對手，並做出回應。

各項研究顯示投入到電腦遊戲的工作時數已經達到相當的經濟規模。
因此，不難想像越來越多公司開始考慮禁止員工利用公司電腦來玩電腦遊戲。

您的 Avira 產品識別出電腦遊戲。 **[遊戲]** 選項一經啟用 (於組態中 [威脅類別]
底下勾選)，您會在 Avira 產品偵測到遊戲時收到對應的警示。
講真的，遊戲現在已經沒有發展空間，因為您可以直接加以刪除。

惡作劇程式

惡作劇程式的目的只在於惡作劇或提供一般消遣，而不會造成傷害或進行重製。
當載入惡作劇程式時，電腦通常會在某個時間播放一段音樂或在螢幕上顯示異常的事物。
惡作劇程式的範例包括磁碟的清洗動作 (DRAIN.COM) 或畫面消失 (BUGSRES.COM)。

但是，請注意！ 所有的惡作劇程式徵狀有可能同時源自於病毒或特洛伊木馬程式。
使用者至少會受到極大的驚嚇，或是過度恐慌，以致於造成真正的傷害。

多虧了掃描與識別常式延伸功能，Avira
產品可以偵測到惡作劇程式並在必要時將這些程式當成有害的程式予以消除。
[惡作劇程式] 選項一經啟用 (於組態中 [威脅類別]
底下勾選)，您會在偵測到惡作劇程式時收到對應的警示。

網路釣魚

網路釣魚 (又稱為品牌詐騙)
是一種聰明的資料竊盜手法，主要瞄準網際網路服務供應商、銀行、網路銀行服務、註冊機關之類團體的客戶或潛在客戶下手。
當您在網際網路上提交電子郵件地址、填寫線上表單、存取新聞群組或網站時，資料可能會遭到「網際網路資料抓取程式 (Internet Crawling
Spider)」攔截並在您不知情的情況下用來行使其他詐騙或不法行為。

您的 Avira 產品識別出「網路釣魚」。 **[網路釣魚]** 選項一經啟用 (於組態中 [威脅類別]
底下勾選)，您會在 Avira 產品偵測到此類行為時收到對應的警示。

侵犯私人網域的程式

當軟體會破壞系統安全、初始有害的程式活動、損害您的隱私或是窺視您的使用者行為時，可能已經成為有害的程式。

您的 Avira 產品偵測到「安全隱私風險」軟體。 **[侵犯私人網域的程式]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類軟體時收到對應的警示。

少見的執行階段壓縮程式 (PCK)

使用少見的執行階段壓縮程式來壓縮並因此而歸類為可疑檔案的檔案。

您的 Avira 產品識別出「少見的執行階段壓縮程式」。 **[少見的執行階段壓縮程式]** 選項一經啟用 (於組態中 [威脅類別] 底下勾選)，您會在 Avira 產品偵測到此類壓縮程式時收到對應的警示。

10.2 病毒與其他惡意程式碼

廣告軟體

廣告軟體指的是透過電腦畫面上顯示的訊息列來呈現橫幅廣告或快顯視窗的軟體。
這些廣告通常無法移除且會持續顯示。
在資料安全方面，連線資料可以讓人從中得出許多使用行為上的資訊，因此也會造成一些問題。

後門程式

後門程式會藉由遠端管理機制來取得電腦的存取權。

該程式會在背景執行，且通常會授予攻擊者無限的權限。
使用者的個人資料可能會遭到後門程式竊取。
但大部分是用來在相關系統中安裝電腦病毒或蠕蟲。

開機病毒

硬碟的開機或主要開機磁區主要會受到開機磁區病毒感染。
這些病毒會覆寫系統執行時所需的重要資訊。
其中一個嚴重的後果：無法再載入電腦系統…

殭屍網路

定義為遠端 (網際網路上) 電腦網路的傀儡網路，包含許多可互相通訊的傀儡電腦。
殭屍網路由一系列遭到破解的機器組成，這些機器會在一般命令與控制基礎結構下執行一些程式 (通常稱為蠕蟲與特洛伊木馬程式)。
傀儡網路有多重目的，包括阻斷服務攻擊等等，有時候還會在電腦使用者不知情的情況下執行。
傀儡網路最可怕的地方在於其規模可達到成千上萬台電腦，流量總和甚至可塞爆最常設的網際網路頻寬限制。

惡意探索程式碼

惡意探索程式碼 (安全漏洞)
是一種電腦程式或指令碼，它會利用錯誤、異常或漏洞來提升權限或是讓電腦系統觸發阻斷服務。 例如，有一種惡意探索程式碼會透過受操控的資料套件從網際網路發動攻擊。
這些程式碼會滲透到程式當中以取得更高的存取權。

詐騙軟體

又稱做「恐嚇軟體」或「流氓軟體」，這種詐騙軟體會佯裝您的電腦已被病毒或惡意程式碼感染。
這種軟體看似與專業的防毒軟體十分相像，但主要目的在於增加不確定性或恐嚇使用者。
用意在於讓受害者對即將發生的不實危險感到害怕，進而付費消除恐懼感。
還有一些情況是，此類軟體會讓受害者相信自己已經遭受攻擊，進而引導他們執行某個動作，而引發真正的攻擊活動。

惡作劇病毒

網際網路與其他網路使用者多年來紛紛收到刻意透過電子郵件散播的病毒警示。
這些警示會透過電子郵件散播出去，並要求收件者盡可能將它們傳送給最多的同事與其他使用者以便讓每個人都知道「危險」。

誘捕機制

誘捕機制是一種安裝在網路中的服務 (程式或伺服器)。
其功能為監控網路和進行記錄攻擊。 合法使用者並不知道該服務的存在 -
也因此將不會被定址。
如果攻擊者找到網路的弱點，並使用誘捕機制提供的服務，則系統會進行記錄病發出警告。

巨集病毒

巨集病毒指的是以應用程式巨集語言所撰寫的小型程式 (例如，WinWord 6.0 底下運作的 WordBasic)，通常只能透過這類應用程式文件來散播。
因為這個原因，人們也將之稱為文件病毒。
這類病毒若要發揮作用，對應的應用程式必須啟動，而且任何一項已感染病毒的巨集也必須執行才行。
與「一般」病毒不同的是，巨集病毒不會因此攻擊可執行檔，而是攻擊對應主機應用程式的文件。

網址嫁接

網址嫁接技術會操控網頁瀏覽器的主機檔案，將查詢轉向假冒的網站。
這是傳統網路釣魚的翻新手法。
網址嫁接詐騙份子將假冒的網站儲存在自己管理的大量伺服器陣列中。 各種 DNS 攻擊類型都可歸類到網址嫁接。
在主機檔案遭到操控的情況下，攻擊者可透過特洛伊木馬程式或是病毒對某個系統進行特別操控。 影響所及，系統現在只能存取假冒的網站，就算輸入了正確的網址也沒用。

網路釣魚

網路釣魚指的是瞄準網際網路使用者的個人資料下手的詐騙手法。
網路釣客通常會將看似正式的信函寄送給被害人，並透過這類郵件引誘被害人在不疑有他的情況下揭露機密資訊，尤其是使用者名稱與密碼或是網路銀行帳戶的 PIN 碼或 TAN 碼。
透過竊取的存取資料，網路釣客可以假冒被害人的身分來執行一連串的交易行為。
可確定的一點是：銀行與保險公司絕對不會透過電子郵件、簡訊或是電話要求提供信用卡號碼、PIN 碼、TAN 碼或是其他存取資料。

千面人病毒

千面人病毒真的是千變萬化。 它們會更改自身的程式碼，因此偵測起來非常困難。

程式病毒

所謂的電腦病毒，指的是在執行之後能夠將自身附加到其他程式上，並引發感染。
與邏輯炸彈和特洛伊木馬程式不同的是，這些病毒會自我分裂繁殖。
這種病毒必須搭配宿主程式以便植入有毒的程式碼，這點與蠕蟲不同。
通常宿主程式的執行狀況並不會改變。

Rootkit

Rootkit
是一群軟體工具，會在成功滲透電腦系統之後進行安裝並隱藏滲透者的登入資料、隱藏相關處理序與記錄資料。
一般而言，為了將隱藏自己，它們會嘗試更新已經安裝的間諜軟體，並重新安裝已刪除的間諜軟體。

指令碼病毒與蠕蟲

這類病毒的程式非常容易編寫，而且只要具備所需的技術，在幾小時內就能透過電子郵件散播到全世界。

指令碼病毒與蠕蟲會使用 Javascript、VBScript
之類的指令碼語言滲透到其他新的指令碼中，或呼叫作業系統功能來進行散播。
這種情況通常會藉由電子郵件或是在交換檔案 (或文件) 期間發生。

蠕蟲是一種會自我分裂繁殖的程式，但不會感染宿主。
因此，蠕蟲並不會成為其他程式序列的一部分。
蠕蟲通常只會經由安全措施有限的系統，滲透到任何受損的程式中。

間諜軟體

間諜軟體指的是會在使用者不知情的情況下，攔截或掌控部分電腦作業內容的間諜程式。
間諜軟體是專為攻擊受感染的電腦以獲取商業利益而設計。

特洛伊木馬程式 (簡稱特洛伊木馬)

特洛伊木馬程式目前相當常見。
其所包含的程式通常偽裝成特殊功能，但在執行之後就會現出原形並執行不同的功能，大部分的情況都具有破壞性。
特洛伊木馬程式不會自行繁殖，因此與其他病毒和蠕蟲有所區別。
這些程式大部分的名稱都很吸引人 (SEX.EXE 或
STARTME.EXE)，以意圖吸引使用者啟動該程式。
這些程式在執行之後會立即啟動，例如格式化硬碟。
病毒植入程式是特洛伊木馬程式的特殊型態，可以將病毒嵌入電腦系統當中。

僵屍電腦

僵屍電腦是受到惡意程式攻擊的電腦，可讓駭客透過遠端控制來為所欲為，藉此達到其犯罪目的。 例如，受感染的電腦會發動阻斷服務 (DoS)
攻擊，或是散播垃圾郵件與網路釣魚郵件。

11. 資訊與服務

本章包含我們的聯絡資訊。

- 請參閱下列章節：聯絡地址
- 請參閱下列章節：技術支援
- 請參閱下列章節：可疑的檔案
- 請參閱下列章節：回報誤判
- 請參閱下列章節：歡迎您提供安全性提升意見

11.1 聯絡地址

如果您對於 Avira 產品系列還有任何疑問或要求的話，我們將很樂意提供協助。
如需我們的聯絡地址，請參閱說明 > 關於 Avira Internet Security 底下的控制中心。

11.2 技術支援

Avira 支援可提供您可靠的協助，幫您解答各式各樣的問題或是解決技術問題。

您可以從我們的網站，找到我們全方位支援服務的所有必要資訊。

http://www.avira.tw/premium-suite-support

如此一來，我們即可提供您快速、可靠的協助，而您應事先備妥下列資訊：

- **授權資訊**。 您可以在功能表項目說明 > 關於 Avira Internet Security > **授權資訊**底下的程式介面中找到此項資訊。 請參閱授權資訊。
- **版本資訊**。 您可以在功能表項目說明 > 關於 Avira Internet Security > **版本資訊**底下的程式介面中找到此項資訊。 請參閱版本資訊。
- **作業系統版本**與任何一項安裝的 Service Pack。
- **安裝的軟體套件**，例如，其他廠商的防毒軟體。

- 程式或報告檔案的**準確訊息**。

11.3 可疑的檔案

請將我們的產品無法偵測或是移除的病毒，或是可疑的檔案寄給我們。
您可以透過下列方式進行。

- 在隔離區管理員
  (位於 控制中心)，識別檔案，並使用內容功能表或對應的按鈕來選取**傳送檔案**項目。
- 以電子郵件附件的形式封裝 (壓縮為 WinZIP、PKZip、Arj 等)
  並將所需的檔案傳送至下列地址：
  virus-premium-suite@avira.tw
  由於某些電子郵件閘道會配置防毒軟體，請同時提供加密壓縮的檔案
  (記得告訴我們解壓縮密碼)。
- 您也可以透過我們的網站將可疑的檔案傳送給我們：http://www.avira.tw/sample-upload

11.4 回報誤判

如果您認為 Avira 產品回報的檔案偵測發現很可能是「無毒的」，請將相關的封裝檔案
(壓縮成 WinZIP、PKZip、Arj 等) 以電子郵件附件形式傳送至下列地址：

virus-premium-suite@avira.tw

由於某些電子郵件閘道會配置防毒軟體，請同時提供加密壓縮的檔案
(記得告訴我們解壓縮密碼)。

11.5 您的意見將協助我們提供更完善的資訊安全服務

對 Avira 來說，客戶的安全是最重要的。 因此，在每個 Avira
產品上市之前，我們的專屬專業團隊都會測試產品的品質與安全性。
我們也非常重視與安全性漏洞有關的任何跡象以及其可能造成的問題。

如果您在我們的產品中發現任何安全漏洞，請以電子郵件將相關意見寄至下列地址：

vulnerabilities-premium-suite@avira.tw

12. 參考：組態選項

組態參照會記錄所有可用的組態選項。

12.1 Scanner

組態的 **[Scanner]** 區段負責指定掃描的組態。 (僅在專家模式中才能使用選項。)

12.1.1 掃描

您可以定義指定掃描常式的行為 (僅在專家模式中才能使用選項)。
如果您選取了要掃描的特定目錄，依據組態而定，Scanner 的掃描行為可能會是：

- 帶有特定掃描優先順序、
- 同時掃描開機磁區與主記憶體、
- 掃描目錄中的所有檔案或選取的檔案。

檔案

Scanner 可以透過篩選器來專門掃描帶有特定副檔名 (類型) 的檔案。

所有檔案

此選項一經啟用，所有檔案 (不論其內容或副檔名為何)
都會進行病毒或惡意程式的掃描。 不使用任何篩選器。

> 注意
> 一旦啟用**所有檔案**，便無法選取**副檔名**按鈕。

使用智慧副檔名辨識

此選項一經啟用，程式會自動選擇要掃描病毒或有害程式的檔案。 這表示 Avira 程式會依據檔案內容決定是否要加以掃描。

此程序在速度上會比透過使用副檔名清單方式來得緩慢，不過卻比較安全，因為並不只有針對特定副檔名才進行掃描。 系統不只預設啟用此選項，也建議使用這個選項。

注意

使用智慧副檔名辨識一經啟用，便無法選取副檔名按鈕。

使用副檔名清單

此選項一經啟用，只會掃描帶有指定副檔名的檔案。
所有可能包含病毒與有害程式的檔案類型都會預先設定好。
此清單可經由「**副檔名**」按鈕手動加以編輯。

注意

此選項一經啟用，而且您已從清單中刪除所有特定副檔名項目時，會在 **[副檔名]** 按鈕底下顯示「*無副檔名*」字樣。

副檔名

藉由此按鈕，會開啟一個對話視窗並顯示所有於「**使用副檔名清單**」模式中掃描的所有副檔名。 系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

注意

請注意，預設清單會依版本不同而有所差異。

其他設定

掃描所選取磁碟機的開機磁區

此選項一經啟用，Scanner 只會針對選取的系統掃描磁碟機掃描其中的開機磁區。
此選項預設為啟用狀態。

掃描主開機磁區

此選項一經啟用，Scanner 會針對系統中使用的硬碟掃描其中的主開機磁區。

略過離線檔案

此選項一經啟用，直接掃描會在掃描期間完全略過所謂的離線檔案。
亦即，不會掃描這些檔案當中是否有病毒與有害程式。
舉例來說，離線檔案指的是由所謂的階層儲存管理系統 (HSMS)
從硬碟實際移動到磁帶的所有檔案。 此選項預設為啟用狀態。

系統檔案完整性檢查

此選項一經啟用，每次進行指定掃描時，系統會針對最重要的 Windows
系統檔案進行特別安全檢查，查看是否有任何檔案遭到惡意程式碼變更。
如果偵測到修改的檔案，會將此檔案報告為可疑。 這項功能會使用大量的電腦資源。
因此預設會停用此選項。

> 注意
> 此選項僅能用於 Windows Vista (含) 以上版本。

> 注意
> 如果您是使用可修改系統檔案並依據個人需求調整開機或開始畫面的第三方工具，不應使用此選項。 這類工具的範例為 skinpacks、TuneUp 公用程式或 Vista Customization。

最佳化掃描

此選項一經啟用，Scanner 的掃描期間會以最高效率來運用處理器資源。
為了不影響效能，最佳化掃描只會記錄為標準等級。

> 注意
> 只能在多處理器系統下使用此選項。

追蹤符號連結

此選項一經啟用，Scanner
所執行的掃描會追蹤掃描設定檔或選取目錄中的所有符號連結，並掃描連結檔中是否有病毒與惡意程式碼。

> 注意
> 此選項並未包含任何捷徑，而是專門指檔案系統中清楚易見的符號連結 (由 mklink.exe 產生) 或連接點 (由 junction.exe 產生)。

先搜尋 Rootkit 再掃描

此選項一經啟用，啟動掃描後 Scanner 會掃描 Windows
系統目錄中所謂的捷徑是否有作用中的 Rootkit。 此處理序不像掃描設定檔「**掃描 Rootkit**」能夠完整地掃描電腦中是否有作用中的
Rootkit，但是執行效能卻是快上許多。 此選項只會變更您建立的設定檔設定。

> 注意
> Rootkit 掃描不適用於 Windows XP 64 位元

掃描登錄

此選項一經啟用，會掃描登錄中是否有惡意程式碼的參照。
此選項只會變更您建立的設定檔設定。

略過網路磁碟機上的檔案和路徑

此選項一經啟用，執行指定掃描時會排除與電腦連線的網路磁碟機。
當伺服器或其他工作站都配備專屬的防毒軟體時，建議您啟用此選項。
預設會停用此選項。

掃描程序

允許停止掃描程式

此選項一經啟用，您隨時可以經由 [Luke Filewalker] 視窗中的「**停止**」按鈕來終止病毒或有害程式的掃描。 一旦停用此設定，[Luke Filewalker] 視窗中的 **[停止]** 按鈕會呈現灰色背景。
因此，您無法提前終止掃描處理序！ 此選項預設為啟用狀態。

掃描程式優先順序

透過指定掃描，Scanner 可以區分優先順序等級。
只有當工作站上同時執行多個處理序，此設定才有作用。 此選項會影響掃描速度。

低

只有當其他處理序都不需要運算時，才會將處理器時間分配給 Scanner，亦即，當作業系統中只執行 Scanner 時，將保持全速運作。
總而言之，搭配其他程式可獲得最佳結果：當 Scanner 持續在背景中運作時，如果其他程式需要運算資源，電腦便可以更快速地回應。

一般

Scanner 將以正常優先順序來執行。
作業系統會針對所有處理序配置等量的處理器資源。
系統不只預設啟用此選項，也建議使用這個選項。
在特定情況下，使用其他應用程式的效能可能會受到影響。

高

Scanner 具有最高的優先順序。 同時使用其他應用程式幾乎不可能。 不過，Scanner 會全速完成掃描。

偵測動作

您可以定義當偵測到病毒或有害程式時，Scanner 要執行的動作。
(僅在專家模式中才能使用選項。)

互動式

此選項一經啟用，會在對話方塊中顯示 Scanner 掃描的結果。 使用 Scanner 掃描時，在掃描結束時，您會收到一則警示，內含受影響的檔案清單。
您可以使用即時線上功能表，針對各種受感染的檔案選取要執行的動作。
您可以針對所有受感染的檔案執行標準動作，或是取消 Scanner。

> 注意
> 在 Scanner 通知中，預設會預先選取 **[隔離區]** 動作。
> 可經由內容功能表選取進一步動作。

自動

此選項一經啟用，在偵測到病毒時不會出現任何對話方塊。 Scanner 會依據您在此區段預先定義的主要與次要動作設定來因應。

執行動作前先將檔案複製至隔離區

此選項一經啟用，Scanner 會在執行要求的主要或次要動作之前建立備份複本。
如果檔案具有參考價值，可以將備份複本儲存在隔離區以便稍後還原。
您也可以將備份複本傳送給 Avira 惡意程式碼研究中心做進一步調查。

主要動作

主要動作是 Scanner 發現病毒或有害程式時優先執行的動作。
如果選取「**修復**」選項但無法修復受影響的檔案，會執行在「**次要動作**」底下選取」的動作。

> 注意
> **次要動作**選項必須當您已選取 **[修復]** 設定 (位於**主要動作**底下) 時才能選取。

修復

此選項一經啟用，Scanner 會自動修復受影響的檔案。 如果 Scanner 無法修復受影響的檔案，會執行在次要動作底下選取的動作。

注意

我們建議使用自動修復動作，不過這意味著 Scanner 將修改工作站上的檔案。

重新命名

此選項一經啟用，Scanner 會重新命名檔案。 如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。 檔案可以在之後修復並重新賦予其原始名稱。

隔離區

此選項一經啟用，Scanner 會將檔案移至隔離區。
稍後可以修復這些檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

刪除

此選項一經啟用，會刪除檔案。 此處理序在速度上會比「覆寫並刪除」要來得快速。

略過

此選項一經啟用，可允許存取檔案，並保持檔案原狀。

警告

工作站上受影響的檔案仍會繼續運作！ 此做法可能會對工作站造成嚴重的傷害！

覆寫並刪除

此選項一經啟用，Scanner 會先使用預設模式來覆寫檔案，再加以刪除。
此檔案無法還原。

次要動作

「**次要動作**」選項必須當您已選取 **[修復]** 設定 (位於「**主要動作**」底下) 時才能選取。
透過這個選項，現在您可以決定要對無法修復的檔案採取哪些處置方式。

重新命名

此選項一經啟用，Scanner 會重新命名檔案。 如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。 檔案可以在之後修復並重新賦予其原始名稱。

隔離區

此選項一經啟用，Scanner 會將檔案移至隔離區。
稍後可以修復這些檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

刪除

此選項一經啟用，會刪除檔案。 此處理序在速度上會比「覆寫並刪除」要來得快速。

略過

此選項一經啟用，可允許存取檔案，並保持檔案原狀。

> **警告**
> 工作站上受影響的檔案仍會繼續運作！ 此做法可能會對工作站造成嚴重的傷害！

覆寫並刪除

此選項一經啟用，Scanner 會先使用預設模式來覆寫檔案，再加以刪除 (抹除)。
此檔案無法還原。

> 注意
> 如果您已選取 **[刪除]** 或 **[覆寫並刪除]**
> 作為主要或次要動作，您應該注意下列事項：當啟發式掃毒偵測到發現時，受影響的檔案不會刪除，而會移至隔離區。

封存

掃描封存時，Scanner
會使用遞迴掃描：封存中的封存也會解壓縮並掃描病毒與有害的程式。
檔案經過掃描之後，會解壓縮並重新掃描一遍。 (僅在專家模式中才能使用選項。)

掃描封存

此選項一經啟用，會掃描封存清單中選取的封存。 此選項會啟用為預設值。

所有封存類型

此選項一經啟用，會選取封存清單中的所有封存類型並加以掃描。

智慧副檔名辨識

此選項一經啟用，即使副檔名與一般副檔名有所差異，Scanner 還是會偵測檔案是否為壓縮檔案格式 (封存)，並加以掃描。
由於，每個檔案必須開啟，因此會影響到掃描速度。 如果 *.zip 封存含有 *.xyz 的副檔名，則 Scanner 也會解壓縮此封存並加以掃描。 此選項會啟用為預設值。

> 注意
> 僅支援封存清單中標示的封存類型。

限制遞迴深度

解壓縮與掃描遞迴封存需要大量的電腦運算時間與資源。
此選項一經啟用，您可以將多重壓縮封存中的掃描深度限制在特定的壓縮層級數量 (最大遞迴深度)。 此舉可節省時間與電腦資源。

> 注意
> 為了在封存中找到病毒或有害程式，Scanner 最多必須掃描至病毒或有害程式所在的遞迴層級。

遞迴深度上限

若要輸入最大遞迴深度，必須啟用 [限制遞迴深度] 選項。
您可以直接輸入要求的遞迴深度，或是透過輸入欄位上的向右箭頭按鍵。 允許的值介於 1 到 99。 建議的標準值為 20。

預設值

此按鈕會還原用於掃描封存的預先定義值。

封存

您可以在此顯示區域，設定 Scanner 應該掃描的封存。 為此，您必須選取相關項目。

例外

Scanner 忽略的檔案物件(僅在專家模式中才能使用選項。)

此視窗中的清單包含當 Scanner 掃描病毒或有害程式時，不應包含的檔案與路徑。

在此請盡可能不要輸入例外項目，否則請輸入無論如何一定得排除在正常掃描作業之外的項目。
在您將檔案包含在此清單之前，建議您一律加以掃描，確定其中沒有病毒或有害程式！

> 注意
> 單上的項目結果總數不得超過 6000 個字元。

> **警告**
> 這些檔案不會包含在掃描作業中！

> 注意
> 此清單上的檔案已全部記錄在報告檔案中。
> 請隨時檢查報告檔案中是否有未掃描的檔案，因為您先前排除檔案的原因現在可能已經不存在。 在此情況下，請再次從此清單中移除檔案名稱。

輸入方塊

您可以在此輸入方塊中輸入不要包含在指定掃描中的檔案物件名稱。
預設不會輸入任何檔案物件。

...

此按鈕會開啟新的視窗，供您選取必要的檔案或路徑。
如果您輸入包含完整路徑的檔案名稱，只有此檔案不會接受掃描。

如果您輸入不含路徑的檔案名稱，就不會掃描含有此名稱的所有檔案(無論路徑或所屬磁碟機為何)。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。 如果沒有選取任何項目，此按鈕將無作用。

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。 (僅在專家模式中才能使用選項。)

Avira
產品內含內含威力非常強大的啟發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。
病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。 如果掃描的程式碼表現出相關特徵，就會回報為可疑。
但這並不代表程式碼本身就是惡意程式碼。 有時可能會出現誤判。
使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啟發式掃毒

巨集病毒啟發式掃毒

您的 Avira 產品內含強大的巨集病毒啟發式掃毒功能。
此選項一經啟用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。
系統不只預設啟用此選項，也建議使用這個選項。

先進啟發式掃毒分析與偵測 (AHeAD)

啟用 AHeAD

您的 Avira 程式內含內含威力強大的 Avira AHeAD 啟發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。
此選項一經啟用，您可以定義此啟發式掃毒技術的「積極」程度。
此選項預設為啟用狀態。

低偵測等級

此選項一經啟用，會偵測到稍微不明的惡意程式碼，在此情況下錯誤警示的機率也很低。

中偵測等級

此選項結合強大的偵測等級與低風險錯誤警示。
如果您已選取使用此啟發式掃毒技術，預設會啟用中偵測等級。

高偵測等級

如果啟用此選項，會偵測到明顯更多不明的惡意程式碼，但也有可能是誤判。

12.1.2 報告

Scanner 包含完整的報告功能。 因此，您可以取得指定掃描結果的準確資訊。
報告檔案包含系統的所有項目，以及指定掃描的警示與訊息。
(僅在專家模式中才能使用選項。)

> 注意
> 要能建立 Scanner 已執行的動作，您應在偵測到病毒或有害程式時啟動專家模式組態中的報告檔案。

報告功能

關閉

此選項一經啟用，Scanner 就不會報告指定掃描的動作與結果。

預設值

啟用此選項時，Scanner 會記錄相關檔案名稱的及其路徑。
此外，目前的掃描組態、版本資訊與被授權人的資訊，全都會寫入報告檔中。

延伸

啟用此選項時，除了預設資訊以外，Scanner 還會記錄警示與秘訣。
報告也包含「(cloud)」後置字元來辨識 Protection Cloud 中偵測到的發現。

完整

此選項一經啟用，Scanner 還會記錄所有掃描的檔案。
此外，會將相關的所有檔案與警示和提示包含在報告檔中。

> 注意
> 如果您必須寄送報告檔給我們 (以便排解疑難)，請在此模式中建立此報告檔案。

12.2 Real-Time Protection

組態的 **[Real-Time Protection]** 區段負責即時掃描的組態。
(僅在專家模式中才能使用選項。)

12.2.1 掃描

通常您會需要不間斷地監視您的系統。 您可以使用 Real-Time Protection (= 即時掃描系統掃描程式)。
然後您可以在電腦上以「連續掃描」的方式掃描所有已複製或開啟的檔案，以找出病毒及不需要的程式。 (僅在專家模式中才能使用選項。)

檔案

Real-Time Protection 可以透過篩選器，專門掃描特定副檔名 (類型) 的檔案。

所有檔案

此選項一經啟用，所有檔案 (不論其內容或副檔名為何)
都會進行病毒或惡意程式的掃描。

> 注意
> 一旦啟用**所有檔案**選項，便無法選取**副檔名**按鈕。請注意，如果啟用所有檔案，將無法選取副檔名按鈕。

使用智慧副檔名辨識

此選項一經啟用，程式會自動選擇要掃描病毒或有害程式的檔案。
這表示程式會依據檔案內容決定是否要加以掃描。
此程序在速度上會比透過**使用副檔名清單**方式來得緩慢，不過卻比較安全，因為並不只有針對特定副檔名才進行掃描。

> 注意
> **使用智慧副檔名辨識**一經啟用，便無法選取**副檔名**按鈕。

使用副檔名清單

此選項一經啟用，只會掃描特定副檔名的檔案。
所有可能包含病毒與有害程式的檔案類型都會預先設定好。
此清單可經由「**副檔名**」按鈕手動加以編輯。
此選項預設為啟用狀態，也建議使用這個選項。

> 注意
> 此選項一經啟用，而且您已從清單中刪除所有特定副檔名項目時，會在**副檔名**按鈕底下顯示「無副檔名」字樣。

副檔名

藉由此按鈕，會開啟一個對話視窗並顯示所有在「**使用副檔名清單**」模式中掃描的副檔名。 系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

> **注意**
> 請注意，副檔名清單會依版本不同而有所差異。

掃描模式

此處可定義檔案的掃描時間。

讀取時掃描

此選項一經啟用，Real-Time Protection
會在應用程式或作業系統讀取或執行檔案時，先行加以掃描。

寫入時掃描

此選項一經啟用，Real-Time Protection 會在寫入檔案時先行掃描。
您必須等候此處理序完成，才能再次存取檔案。

讀取與寫入時掃描

此選項一經啟用，Real-Time Protection
會在開啟、讀取與執行檔案之前，並在寫入檔案之後掃描檔案。
此選項預設為啟用狀態，也建議使用這個選項。

磁碟機

監視網路磁碟機

此選項一經啟用，會掃描諸如伺服器磁碟區、對等磁碟機等網路磁碟機 (對應磁碟機) 上的檔案。

注意

為了避免電腦效能降低太多，請僅在例外情況時才啟用 **[監視網路磁碟機]** 選項。

警告

此選項一經停用，就**不會**監視網路磁碟機。
因此，這些磁碟機也就無法防範病毒或有害程式！

注意

在網路磁碟機上執行檔案時，不管 **[監視網路磁碟機]** 選項設定為何，Real-Time Protection 都會掃描這些檔案。
在某些情況下，網路磁碟機上的檔案會在開啟狀態下進行掃描，即使已經停用 **[監視網路磁碟機]** 選項亦然。 原因：這些檔案可由 [執行檔案] 權限加以存取。 如果想要讓這些檔案，甚至是網路磁碟機上的已執行檔案不要接受 Real-Time Protection 掃描，請在要排除的檔案物件清單中輸入這些檔案 (請參閱：Real-Time Protection > 掃描 > 例外)。

啟用快取

此選項一經啟用，Real-Time Protection 快取中會提供網路磁碟機上監視的檔案。 不具快取功能的網路磁碟機監視比較安全，但執行效能不如具快取功能的網路磁碟機監視。

封存

掃描封存

此選項一經啟用，會掃描封存。 壓縮檔案經過掃描之後，會解壓縮並重新掃描一遍。 預設會停用此選項。 封存掃描會受限於遞迴深度、要掃描的檔案數量以及封存大小。 您可以設定最大遞迴深度、要掃描的檔案數量以及封存大小上限。

注意

由於此處理序會對電腦效能產生極大的需求，因此系統預設會停用此選項。
通常我們建議使用指定掃描來檢查封存。

遞迴深度上限

掃描封存時，Real-Time Protection
會使用遞迴掃描：封存中的封存也會解壓縮並掃描病毒與有害的程式。
您可以定義遞迴深度。 建議的遞迴深度預設值為
1，直接位在主封存中的所有檔案都會予以掃描。

檔案數上限

掃描封存時，可以限制封存中要掃描的檔案數量上限。
要掃描的預設與建議檔案數量上限值為 10 個。

大小上限 (KB)

掃描封存時，可以限制要解壓縮的封存大小上限。 建議的標準值為 1000 KB。

偵測動作

您可以定義當偵測到病毒或有害程式時，Real-Time Protection 要執行的動作
(僅在專家模式中才能使用選項。)

互動式

此選項一經啟用，只要 Real-Time Protection
偵測到病毒或有害的程式，就會出現桌面通知。
您可以選擇移除偵測到的惡意程式碼，或經由「**詳細資料**」按鈕存取其他可用的病毒處理動作。 這些動作會顯示在對話方塊中。 此選項預設為啟用狀態。

許可的動作

您可以在此顯示方塊中，指定要用於對話方塊中做為進一步動作的病毒管理動作。
您必須為此啟用對應的選項。

修復

Real-Time Protection 會盡可能修復受感染的檔案。

重新命名

Real-Time Protection 會重新命名檔案。 如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。 檔案可以在之後修復並重新命名。

隔離區

Real-Time Protection 會將檔案移至隔離區。
如果檔案具有參考價值，可以從隔離區管理員復原，或在必要時將其傳送至 Avira 惡意程式碼研究中心。 依檔案特性，您可以在隔離區管理員中找到更多可用的選項。

刪除

將檔案刪除。 此處理序在速度上會比 **[覆寫並刪除]** 要來得快速 (請參閱以下)。

略過

允許存取檔案並忽略檔案。

覆寫並刪除

Real-Time Protection 會先使用預設模式來覆寫檔案，再加以刪除。
此檔案無法還原。

警告

如果 Real-Time Protection 設為 **[寫入時掃描]**，將不會寫入附加的檔案。

預設值

此按鈕可讓您選取偵測到病毒時，對話方塊中預設啟用的動作。
請選取預設啟用的動作，並按一下「**預設值**」按鈕。

注意

您無法選取 **[修復]** 動作作為預設動作。

如需詳細資訊，請按一下這裡。

自動

此選項一經啟用，在偵測到病毒時不會出現任何對話方塊。 Real-Time Protection 會依據您在此區段預先定義的主要與次要動作設定來因應。

執行動作前先將檔案複製至隔離區

此選項一經啟用，Real-Time Protection
會在執行要求的主要或次要動作之前建立備份複本。 備份複本會儲存至隔離區。
如果該項目具有參考價值，可以透過隔離區管理員加以還原。
您也可以將備份複本傳送給 Avira 惡意程式碼研究中心。
依物件特性，您可以在隔離區管理員中找到更多可用的選項。

主要動作

主要動作是 Real-Time Protection 發現病毒或有害程式時優先執行的動作。
如果選取「**修復**」選項但無法修復受影響的檔案，會執行在「**次要動作**」底下選取的動作。

> 注意
> **次要動作**選項只有在您已選取**修復**設定 (位於**主要動作**底下) 時才能選取。

修復

此選項一經啟用，Real-Time Protection 會自動修復受影響的檔案。 如果 Real-Time Protection 無法修復受影響的檔案，會執行在**次要動作**底下選取的動作。

> 注意
> 我們建議使用自動修復動作，不過這意味著 Real-Time Protection
> 將修改工作站上的檔案。

重新命名

此選項一經啟用，Real-Time Protection 會重新命名檔案。
如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。
檔案可以在之後修復並重新賦予其原始名稱。

隔離區

此選項一經啟用，Real-Time Protection 會將檔案移至隔離區。
稍後可以修復此目錄中的檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

刪除

此選項一經啟用，會刪除檔案。 此處理序在速度上會比 **[覆寫並刪除]** 要來得快速。

略過

此選項一經啟用，可允許存取檔案，並保持檔案原狀。

警告
工作站上受影響的檔案仍會繼續運作！ 此做法可能會對工作站造成嚴重的傷害！

覆寫並刪除

此選項一經啟用，Real-Time Protection
會先使用預設模式來覆寫檔案，再加以刪除。 此檔案無法還原。

拒絕存取

此選項一經啟用，報告功能必須已經啟用，Real-Time Protection
才會將偵測項目輸入到報告檔案中。 此外，此選項一經啟用，Real-Time Protection
會將項目寫入事件記錄。

警告
如果 Real-Time Protection 設為 **[寫入時掃描]**，不會寫入受影響的檔案。

次要動作

「**次要動作**」選項只有在您已選取「**修復**」選項 (位於「**主要動作**」底下)
時才能選取。 透過這個選項，現在您可以決定要對無法修復的檔案採取哪些處置方式。

重新命名

此選項一經啟用，Real-Time Protection 會重新命名檔案。
如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。
檔案可以在之後修復並重新賦予其原始名稱。

隔離區

此選項一經啟用，Real-Time Protection 會將檔案移至隔離區。
稍後可以修復檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

刪除

此選項一經啟用，會刪除檔案。 此處理序在速度上會比 **[覆寫並刪除]** 要來得快速。

略過

此選項一經啟用，可允許存取檔案，並保持檔案原狀。

警告
工作站上受影響的檔案仍會繼續運作！ 此做法可能會對工作站造成嚴重的傷害！

覆寫並刪除

此選項一經啟用，Real-Time Protection
會先使用預設模式來覆寫檔案，再加以刪除。 此檔案無法還原。

拒絕存取

此選項一經啟用，將不會寫入受影響的檔案；報告功能必須已經啟用，Real-Time Protection 才會將偵測項目輸入到報告檔案中。 此外，此選項一經啟用，Real-Time Protection 會將項目寫入事件記錄。

注意
如果您已選取 **[刪除]** 或 **[覆寫並刪除]**
作為主要或次要動作，請注意：當啟發式掃毒偵測到發現時，受影響的檔案不會刪除，而會移至隔離區。

進一步動作

使用事件記錄

此選項一經啟用，每次偵測到病毒時，就會將項目新增至 Windows 事件記錄。
您可以在 Windows 事件檢視器中呼叫這些事件。 此選項預設為啟用狀態。
(僅在專家模式中才能使用選項。)

例外

透過這些選項，您可以設定 Real-Time Protection 的例外物件 (即時掃描)。
相關物件不會包含在即時掃描中。 Real-Time Protection
會在透過待忽略處理序清單進行即時掃描時忽略這些物件的檔案存取。
例如，這在資料庫或備份解決方案中會很有用。 (僅在專家模式中才能使用選項。)

指定處理序及忽略檔案物件時請注意下列事項：由上至下處理清單。
清單越長，每次處理存取的清單時，所需的處理器時間也會越久。
因此，請盡可能將清單變短一點。

Real-Time Protection 忽略的處理序

此清單中處理序的所有檔案存取行為，全都不會受到 Real-Time Protection 的監視。

輸入方塊

在此欄位中，輸入要讓即時掃描略過的處理序名稱。 預設不會輸入任何處理序。

指定的處理序路徑和檔案名稱長度上限為 255 個字元。 您最多可以輸入 128 個處理序。 清單上的項目結果總數不得超過 6000 個字元。

輸入處理序時，可接受 Unicode 符號。
因此您可以輸入含有特殊符號的處理序或目錄名稱。

磁碟資訊必須輸入如下： ［磁碟代號］：\

分號 (:) 僅用於指定磁碟。

指定處理序時，您可以使用萬用字元 * (任何數量的字元) 及 ? (單一字元)。

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

若要避免處理序監視遭 Real-Time Protection 全域排除，專門組成下列字元的規格皆無效：* (星號)、? (問號)、 / (正斜線)、 \ (反斜線)、 . (點)、 : (分號)。

您可以選擇在不輸入完整路徑內容的情況下，排除由 Real-Time Protection 監視的處理序。 例如：`application.exe`

不過，這只適用於可執行檔位在硬碟中的處理序。

位在連線磁碟機上的可執行檔處理序則需要完整的路徑詳細資訊，例如網路磁碟機。請注意連線網路磁碟機例外標記上的一般資訊。

請勿指定任何位在動態磁碟上的可執行檔處理序例外。 動態磁碟可用於卸除式磁碟，如 CD、DVD 或 USB 隨身碟。

警告

請注意，所有由清單中記錄之處理序完成存取的檔案，都會從病毒與有害程式的掃描作業中排除！

...

此按鈕會開啟新的視窗，供您選取可執行檔。

處理序

「**處理序**」按鈕會開啟「**處理序選項**」視窗，顯示執行中的處理序。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的處理序新增至顯示視窗。

刪除

藉由這個按鈕，您可以從顯示視窗刪除選取的處理序。

要由 Real-Time Protection 忽略的檔案物件

對此清單所列檔案物件的存取，全都不會受到 Real-Time Protection 的監視。

輸入方塊

您可以在此方塊中輸入不要包含在即時掃描中的檔案物件名稱。
預設不會輸入任何檔案物件。

清單上的項目總計不得超過 6000 個字元。

指定要忽略的處理序時，您可以使用萬用字元 * (任何數量的字元) 及 ？(單一字元)：也會排除個別副檔名 (內含萬用字元)：

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

目錄名稱必須以反斜線 \ 作為結束。

如果排除目錄，會一併自動排除所有子目錄。

針對每個磁碟機，透過輸入完整路徑 (以磁碟機代號開頭)，最多可指定 20 個例外。例如：

```
C:\Program Files\Application\Name.log
```

不含完整路徑的例外上限為 64。 例如：

```
*.log
\computer1\C\directory1
```

萬一已經有動態磁碟機在其他磁碟上裝載為目錄，就必須在例外清單中使用整合的磁碟作業系統別名，例如：

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

假如您使用裝載點 (例如 `C:\DynDrive`)，還是會掃描動態磁碟。 您可以從 Real-Time Protection 的報告檔中判斷要使用的作業系統別名。

...

此按鈕會開啟新的視窗，供您選取要排除的檔案物件。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

刪除

藉由這個按鈕，您可以從顯示視窗刪除選取的檔案物件。

指定例外時請注意進一步資訊：

為了排除使用簡短 DOS 檔名 (8.3 DOS 名稱慣例)
存取的物件，還必須在清單中輸入相關的簡短檔名。

內含萬用字元的檔名不可以反斜線來結束。 例如：
`C:\Program Files\Application\applic*.exe\`
此項目無效且不會視為例外！

請注意下列有關**連接網路磁碟上的例外**：如果您使用連接網路磁碟的磁碟代號，指定的檔案與資料夾皆無法從 Real-Time Protection 掃描中排除。 如果例外清單中的 UNC 路徑與連線至網路磁碟機所使用的 UNC 路徑不同 (IP 位址指定要連線至網路磁碟機的電腦名稱)，就「不會」將指定的資料夾與檔案排除在 Real-Time Protection 掃描範圍之外。 在 Real-Time Protection 報告檔中尋找相關的 UNC 路徑：
`\\<電腦名稱>\<啟用>\` - **或** - `\\<IP 位址>\<啟用>\`

您可以在 Real-Time Protection 報告檔中尋找 Real-Time Protection 用來掃描感染檔案的路徑。 請在例外清單中清楚指出相同的路徑。 繼續如下：在 [Real-Time Protection] > [報告] 底下的組態中將 Real-Time Protection 的通訊協定功能設定為 **[完整]**。 接著在 Real-Time Protection 已啟用的狀態下，存取檔案、資料夾、裝載的磁碟機或是連線的網路磁碟機。 現在您可以從 Real-Time Protection 報告檔中讀取要使用的路徑。 報告檔可在 [本機保護] > [Real-Time Protection] 底下的控制中心中存取。

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。 (僅在專家模式中才能使用選項。)

Avira

產品內含內含威力非常強大的啟發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。

病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。 如果掃描的程式碼表現出相關特徵，就會回報為可疑。

但這並不代表程式碼本身就是惡意程式碼。 有時可能會出現誤判。

使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啟發式掃毒

巨集病毒啟發式掃毒

您的 Avira 產品內含強大的巨集病毒啟發式掃毒功能。

此選項一經啟用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。

系統不只預設啟用此選項，也建議使用這個選項。

先進啟發式掃毒分析與偵測 (AHeAD)

啟用 AHeAD

您的 Avira 程式內含內含威力強大的 Avira AHeAD 啟發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。

此選項一經啟用，您可以定義此啟發式掃毒技術的「積極」程度。

此選項預設為啟用狀態。

低偵測等級

此選項一經啟用，會偵測到稍微不明的惡意程式碼，在此情況下錯誤警示的機率也很低。

中偵測等級

此選項結合強大的偵測等級與低風險錯誤警示。

如果您已選取使用此啟發式掃毒技術，預設會啟用中偵測等級。

高偵測等級

如果啟用此選項，會偵測到明顯更多不明的惡意程式碼，但也有可能是誤判。

12.2.2 報告

Real-Time Protection
包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。
(僅在專家模式中才能使用選項。)

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啟用，Real-Time Protection 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啟用，Real-Time Protection 會將重要的資訊
(有關病毒偵測、警示與錯誤事項)
記錄到報告檔中，並忽略較不重要的資訊，讓報告更為簡明易懂。
此選項預設為啟用狀態。

延伸

此選項一經啟用，Real-Time Protection 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啟用，Real-Time Protection
會將所有可用資訊記錄到報告檔中，包括檔案大小、檔案類型、日期等等。

限制報告檔

將大小限制為 n MB

此選項一經啟用，可將報告檔大小限定為特定大小。 允許介於 1 到 100 MB 之間的值。 當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。 如果記錄檔大小超出指定大小 50 KB 以上，會先刪除舊的項目，直到達到指定大小減去 50 KB。

縮短報告前先備份

此選項一經啟用，縮短報告檔案前會先加以備份。

在報告檔中寫入組態

此選項一經啟用，會將即時掃描的組態記錄在報告檔中。

> 注意
> 如果您未指定任何報告檔案限制，會在報告檔案達到 100MB 時自動建立新報告檔。 並會建立舊報告檔的備份。 最多可儲存三個舊報告檔的備份。 日期最早的備份會最先遭到刪除。

12.3 更新

您可以在 **[更新]** 區段中設定自動接收更新。 您可以指定各種更新間隔。

自動更新

共 n 天/小時/分鐘

在此方塊中，您可以指定執行自動更新的間隔。 若要變更更新間隔，請反白方塊的其中一個時間選項，使用輸入方塊右方的箭號加以變更。

連線至網際網路時開始工作 (撥號連線)

此選項一經啟用，除了指定的更新間隔之外，只要建立網際網路連線，就會執行更新工作。 (僅在專家模式中才能使用選項。)

如果時間已過，重新執行工作

此選項一經啟用，就會執行過去在指定時間無法執行的更新工作，例如，因為電腦關機而無法執行的工作。(僅在專家模式中才能使用選項。)

12.3.1 網路伺服器

網路伺服器

您可以經由網際網路上的網路伺服器，直接執行更新。 (僅在專家模式中才能使用選項。)

網路伺服器連線

使用現有的連線 (網路)

如果您是透過網路進行連線，會顯示此設定。

使用下列連線

如果您個別定義連線，會顯示此設定。

更新程式會自動偵測有哪些可用的連線選項。
不可用的連線選項會反白顯示，而且無法啟用。 例如，您可以透過 Windows 中的電話簿項目，手動建立撥號連線。

使用者

輸入選取的帳戶使用者名稱。

密碼

輸入此帳戶的密碼。 為了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

> 注意
> 如果您忘記了現有的網際網路帳戶名稱或密碼，請連絡您的網際網路服務供應商。

注意

目前尚無法透過所謂的撥接工具 (例如，SmartSurfer、Oleco 等等)進行更新程式的自動撥接服務。

終止為更新設定的撥號連線

此選項一經啟用，只要順利完成下載，就會立即再次自動中斷針對更新所進行的撥號連線。

注意

此選項僅能用於 Windows XP。

在較新的作業系統底下，只要執行下載，開啟撥號連線進行更新將一律終止。

Proxy 設定

Proxy 伺服器

不要使用 Proxy 伺服器

此選項一經啟用，便無法透過 Proxy 伺服器建立網路伺服器的連線。

使用 Proxy 系統設定

此選項一經啟用，便會使用目前的 Windows 系統設定，經由 Proxy 伺服器連線至網路伺服器。 在 **[控制台] > [網際網路選項] > [連線] > [區域網路設定]**底下，您可以進行 Windows 系統設定以使用 Proxy 伺服器。您也可以在 Internet Explorer 的 **[工具]** 功能表中存取網際網路選項。

警告

如果您使用需要驗證的 Proxy 伺服器，請在 **[使用此 Proxy 伺服器]** 底下輸入所有所需的資料。 **[使用 Proxy 系統設定]** 選項只能用於無須驗證的 Proxy 伺服器。

使用此 Proxy 伺服器

如果您是經由 Proxy 伺服器設定網路伺服器連線，可在此輸入相關資訊。

位址

請輸入連線至網路伺服器時應該使用的 Proxy 伺服器之電腦名稱或 IP 位址。

連接埠

請輸入連線至網路伺服器時應該使用的 Proxy 伺服器之連接埠編號。

登入名稱

輸入使用者名稱以登入 Proxy 伺服器。

登入密碼

在此輸入 Proxy 伺服器的相關登入密碼。
為了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

例如：

位址：`proxy.domain.com` 連接埠：`8080`

位址：`192.168.1.100` 連接埠：`3128`

12.4 Backup

您可以在 **[組態] > [本機保護] > [Backup]** 底下設定 Avira 備份功能。
(僅在專家模式中才能使用選項。)

12.4.1 設定

您可以在 **[設定]** 中，設定 Backup 元件的行為。

僅 Backup 經過修改的檔案

此選項一經啟用，會建立增量備份：由於上次備份儲存在備份設定檔中，所以只有已修改的檔案。
如果已停用此選項，系統會針對每個儲存的備份設定檔建立完整備份：所有檔案都會儲存在備份設定檔中。

系統不只預設啟用此選項，也建議使用這個選項，因為與完整資料備份相較之下，增量備份的建立速度較快，也較不耗用資源。

備份前先掃描有無病毒或有害的程式

此選項一經啟用，會在備份期間掃描儲存的檔案中是否有病毒與惡意程式碼。
檔案只要受到感染，就不會儲存起來。
系統不只預設啟用此選項，也建議使用這個選項。

12.4.2 例外

在各種**例外**情況下，您可以指定備份時要儲存與不儲存的檔案物件與檔案類型。

不要納入備份的檔案

本視窗中的清單包含備份中未儲存的檔案與路徑。

> 注意
> 單上的項目結果總數不得超過 6000 個字元。

> 注意
> 此清單上的檔案已全部記錄在報告檔案中。

輸入方塊

在此方塊中輸入不要儲存的檔案物件名稱。
預設會輸入已登入使用者的本機設定暫存目錄路徑。

此按鈕會開啟新的視窗，供您選取必要的檔案或路徑。
如果您擁有檔案的完整名稱與路徑，則可以從備份中隔離特定檔案。
如果您已經輸入檔案名稱或路徑，就不會儲存具有此名稱的每個檔案
(無論檔案路徑或所屬磁碟機為何)。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。 如果沒有選取任何項目，此按鈕將無作用。

重設清單

此按鈕會還原預先定義的預設值。

請注意下列各點：

- 檔名只能包含萬用字元 * (任何數量的字元) 與 ? (單一字元)。
- 此清單將由上而下進行處理。
- 如果排除目錄，會一併自動排除所有子目錄。
- 也會排除個別副檔名 (內含萬用字元)。
- 為了排除使用簡短 DOS 檔名 (8.3 DOS 名稱慣例)
  存取的物件，還必須在清單中輸入相關的簡短檔名。

> 注意
>
> 內含萬用字元的檔名不可以反斜線來結束。 例如：
> `C:\Program Files\Application\applic*.exe\`
> 此項目無效且不會視為例外！

例如：

- `application.exe`
- `\Program Files\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Program Files\Application\application.exe`

- C:\Program Files\Application\applic*.exe
- C:\Program Files\Application\applic*
- C:\Program Files\Application\applic?????.e*
- C:\Program Files\
- C:\Program Files
- C:\Program Files\Application*.mdb

副檔名清單

考慮所有副檔名

此選項一經啟用，將儲存備份設定檔中的所有檔案。

啟用要排除的副檔名清單

此選項一經啟用，會儲存備份設定檔中的所有檔案
(已輸入排除的副檔名清單中的檔案則除外)。

副檔名

此按鈕會開啟對話方塊，顯示當啟用「**啟用要排除的副檔名清單**」選項時，未在備份期間儲存的所有副檔名。
系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

啟用要包含的副檔名清單

此選項一經啟用，只會儲存其副檔名已經輸入至要考慮的副檔名清單中的檔案。

副檔名

此按鈕會開啟對話方塊，顯示當啟用「**啟用要包含的副檔名清單**」選項時，在備份期間儲存的所有副檔名。
系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

12.4.3 報告

Backup 元件包含完整的記錄功能。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啟用，Backup 元件便無法建立記錄。
請只有在例外情況下才關閉記錄功能。

預設值

此選項一經啟用，Backup 元件會將重要的資訊
(有關儲存、病毒偵測、警示與錯誤事項)
記錄到報告檔中，並忽略較不重要的資訊，讓報告更為簡明易懂。
此選項會啟用為預設值。

延伸

此選項一經啟用，Backup 元件會將較不重要的資訊包含在報告檔中。

完整

此選項一經啟用，Backup
元件會將備份處理序及病毒掃描的所有相關資訊都包含在報告檔中。

12.5 FireWall

12.5.1 設定 FireWall

Avira Internet Security 可讓您設定 Avira FireWall：

- Avira FireWall

12.5.2 Avira FireWall

[組態] > [網際網路防護] 底下的 **[FireWall]** 區段負責 Avira FireWall 的組態 。

介面卡規則

在 Avira FireWall 中，介面卡指的是模擬硬體裝置 (例如，miniport、橋接器連線等) 的軟體或是真實硬體裝置 (例如網路卡)。

Avira FireWall 會針對電腦上已安裝驅動程式的所有現有介面卡顯示其介面卡規則。
(僅在專家模式中才能使用選項。)

- ICMP 通訊協定
- TCP 連接埠掃描
- UDP 連接埠掃描
- 傳入規則
- 傳出規則
- 管理規則的按鈕

預先定義的介面卡規則取決於安全性等級。 您可以在控制中心的 **網際網路防護 > FireWall** 底下變更*安全性等級*或定義自己的介面卡規則。
如果您已定義自己的介面卡規則，控制中心 FireWall 區段中的*安全性等級*就會設為 **[自訂]**。

> 注意
> 所有預先定義之 Avira FireWall 規則的預設*安全性等級*設定都是 **[中]**。

ICMP 通訊協定

網際網路控制訊息通訊協定 (ICMP) 可用來交換網路上的錯誤與資訊訊息。
此通訊協定也可搭配 ping 或 tracer 命令使用以顯示狀態訊息。
有了這項規則，您可以定義傳入與傳出的已封鎖訊息類型、洪水攻擊時的行為，以及 ICMP 分段封包的反應。 此規則可用來防止所謂的 ICMP
洪水攻擊，但是由於它會回應每一個封包，因此會導致遭受攻擊的電腦 CPU 負載增加。

預先定義的 ICMP 通訊協定規則

設定	規則
低	封鎖的傳入類型：**無類型**。 封鎖的傳出類型：**無類型**。 如果封包之間的延遲小於 **50** 毫秒，即假設為洪水攻擊。 **拒**絕分段的 ICMP 封包。
中	低等級適用相同規則。
高	封鎖的傳入類型：**多種類型** 封鎖的傳出類型：**多種類型** 如果封包之間的延遲小於 **50** 毫秒，即假設為洪水攻擊。 **拒**絕分段的 ICMP 封包。

封鎖的傳入類型：無類型/多種類型

只要在連結上按一下滑鼠，就會立即顯示 ICMP 封包類型清單。
您可以透過這份清單，指定要封鎖的傳入 ICMP 訊息類型。

封鎖的傳出類型：無類型/多種類型

只要在連結上按一下滑鼠，就會立即顯示 ICMP 封包類型清單。
您可以透過這份清單，選取要封鎖的傳出 ICMP 訊息類型。

假設發生洪水攻擊

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入允許的 ICMP 延遲上限。
範例：50 毫秒。

拒絕分段的 ICMP 封包

只要在連結上按一下滑鼠，就可選擇「**拒絕**」與「**不拒絕**」分段的 ICMP 封包。

TCP 連接埠掃描

有了這項規則，您就可以定義何時 FireWall 會認定為 TCP 連接埠掃描，以及在這種情況下需要採取的行動為何。 此規則可用來預防所謂的 TCP 連接埠掃描攻擊，後者會導致偵測電腦上開放的 TCP 連接埠。
此類攻擊會搜尋電腦上的弱點，並且經常伴隨著更危險的攻擊類型。

預先定義的 TCP 連接埠掃描規則

設定	規則
低	如果在 **5,000** 毫秒內，掃描了 **50** 個 (或) 以上的連接埠，即假設為 TCP 連接埠掃描。偵測到此現象時，即**記錄**攻擊者的 IP，但**不要新增**規則來封鎖攻擊。
中	如果在 **5,000** 毫秒內，掃描了 **50** 個 (或) 以上的連接埠，即假設為 TCP 連接埠掃描。偵測到此現象時，即**記錄**攻擊者的 IP，並**新增**規則以封鎖攻擊。
高	中等級適用相同規則。

連接埠

只要在連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入掃描過多少個連接埠之後，會認定為 TCP 連接埠掃描。

連接埠掃描時間間隔

只要在此連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入在認定為 TCP 連接埠掃描活動之前，特定數量的連接埠掃描活動的時間間隔。

事件資料庫

只要在連結上按一下滑鼠，就可選擇「**記錄**」與「**不記錄**」攻擊者的 IP 位址。

規則

只要在連結上按一下滑鼠，就可選擇「**新增**」與「**不新增**」規則以封鎖 TCP 連接埠掃描攻擊。

UDP 連接埠掃描

有了這項規則，您就可以定義何時 FireWall 會認定為 UDP 連接埠掃描，以及在這種情況下需要採取的行動為何。 此規則可預防所謂的 UDP 連接埠掃描攻擊，後者會導致偵測電腦上開放的 UDP 連接埠。
此類攻擊會搜尋電腦上的弱點，並且經常伴隨著更危險的攻擊類型。

預先定義的 UDP 連接埠掃描規則

設定	規則
低	如果在 **5,000** 毫秒內，掃描了 **50** 個 (或) 以上的連接埠，即假設為 UDP 連接埠掃描。偵測到此現象時，即**記錄**攻擊者的 IP，但**不要新增**規則來封鎖攻擊。
中	如果在 **5,000** 毫秒內，掃描了 **50** 個 (或) 以上的連接埠，即假設為 UDP 連接埠掃描。偵測到此現象時，即**記錄**攻擊者的 IP，並**新增**規則以封鎖攻擊。

高	中等級適用相同規則。

連接埠

只要在連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入掃描過多少個連接埠之後，會認定為 UDP 連接埠掃描。

連接埠掃描時間間隔

只要在此連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入在認定為 UDP 連接埠掃描活動之前，特定數量的連接埠掃描活動的時間間隔。

事件資料庫

只要在連結上按一下滑鼠，就可選擇「**記錄**」與「**不記錄**」攻擊者的 IP 位址。

規則

只要在連結上按一下滑鼠，就可選擇「**新增**」與「**不新增**」規則以封鎖 TCP 連接埠掃描攻擊。

傳入規則

傳入規則可定義為使用 Avira FireWall 來控制傳入的資料流量。

> **警告**
> 封包經過篩選之後，就會連續套用對應的規則，因此規則順序就非常重要。
> 只有當您很清楚自己的行為有何後果時才變更規則順序。

預先定義的 TCP 流量監視器規則

設定	規則
低	無任何遭到 Avira FireWall 封鎖的傳入資料流量。
中	**允許在 135 建立 TCP 連線** 如果本機連接埠位於 **{135}** 且遠端連接埠位於 **{0-65535}**，則**允許**來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 TCP 封包。 適用**現有連線的封包**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。 **拒絕 135 上的 TCP 封包** 如果本機連接埠位於 **{135}** 且遠端連接埠位於 **{0-65535}**，則拒絕來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 TCP 封包。 適用**所有封包**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。 **TCP 正常流量監視** 如果本機連接埠位於 **{0-65535}** 且遠端連接埠位於 **{0-65535}**，則**允許**來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 TCP 封包。 適用**連線初始化和現有連線封包**。 **當封包符合規則時，不要記錄**。 進階：選取具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。 如果本機連接埠位於 **{0-65535}** 且遠端連接埠位於 **{0-65535}**，則**捨棄 TCP 流量** **拒絕**來自位址 **0.0.0.0** 的 TCP 封包(遮罩為 **0.0.0.0**)。 適用**所有封包**。 **當封包符合規則時，不要記錄**。 進階：選取具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。

高	如果本機連接埠位於 **{0-65535}** 且遠端連接埠位於 **{0-65535}**，則**監視已建立的 TCP 流量** **允許**來自位址 **0.0.0.0** 的 TCP 封包(遮罩為 **0.0.0.0**)。 適用**現有連線的封包**。 **當封包符合規則時，不要記錄**。 進階：選取具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。

允許/拒絕 TCP 封包

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 TCP 封包。

IP 位址

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 遮罩。

本機連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義本機連接埠編號或是完整的連接埠範圍。

遠端連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義遠端連接埠編號或是完整的連接埠範圍。

套用方式

只要在此連結上按一下滑鼠，就可選擇套用「**連線初始化與現有連線封包**」的規則，或是僅套用「**現有連線封包**」或「**所有封包**」的規則。

事件資料庫

如果封包符合規則，只要在連結上按一下滑鼠，就可以選擇「**記錄**」與「**不記錄**」至事件資料庫。

進階

進階功能允許進行內容篩選設定。
例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。
如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

已篩選內容：位元組

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

已篩選內容：遮罩

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

已篩選內容：位移

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。
此位移是從 TCP 標頭結尾開始計算。

預先定義的 UDP 資料流量監視器規則

設定	規則
低	-
中	如果本機連接埠位於 **{0-66535}** 且遠端連接埠位於 **{0-66535}**，則 **UDP 接受的資料流量** **允許**來自位址 **0.0.0.0** 的 UDP 封包 (遮罩為 **0.0.0.0**)。 適用**所有串流**的**開放連接埠**。 當封包符合規則時，**不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。 如果本機連接埠位於 **{0-65535}** 且遠端連接埠位於 **{0-65535}**，則**捨棄 UDP 流量** **拒絕**來自位址 **0.0.0.0** 的 UDP 封包(遮罩為 **0.0.0.0**)。 適用**所有串流**的**所有連接埠**。 **當封包符合規則時，不要記錄**。 進階：選取具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。
高	**監視已建立的 UDP 流量** 如果本機連接埠位於 **{0-65535}** 且遠端連接埠位於 **{53, 67, 68, 123}**，則 **允許來自位址 0.0.0.0 (遮罩為 0.0.0.0) 的 UDP 封包。** 適用**所有串流**的**開放連接埠**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。

允許/拒絕 UDP 封包

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 UDP 封包。

IP 位址

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 遮罩。

本機連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義本機連接埠編號或是完整的連接埠範圍。

遠端連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義遠端連接埠編號或是完整的連接埠範圍。

套用方式

連接埠

只要在此連結上按一下滑鼠，就可選擇將此規則套用至所有連接埠，或僅套用至所有開放的連接埠。

串流

只要在此連結上按一下滑鼠，就可選擇將此規則套用至所有串流，或僅套用至輸出串流。

事件資料庫

如果封包符合規則，只要在連結上按一下滑鼠，就可以選擇「**記錄**」與「**不記錄**」至事件資料庫。

進階

進階功能允許進行內容篩選設定。
例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。
如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

已篩選內容：位元組

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

已篩選內容：遮罩

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

已篩選內容：位移

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。
此位移是從 UDP 標頭結尾開始計算。

預先定義的 ICMP 流量監視器規則

設定	規則
低	-
中	**不依據 IP 位址捨棄 ICMP** **允許**位址來自 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 ICMP 封包。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。
高	中等級適用相同規則。

允許/拒絕 ICMP 封包

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 ICMP 封包。

IP 位址

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 遮罩。

事件資料庫

如果封包符合規則，只要在連結上按一下滑鼠，就可以選擇「**記錄**」與「**不記錄**」至事件資料庫。

進階

進階功能允許進行內容篩選設定。
例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。
如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

已篩選內容：位元組

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

已篩選內容：遮罩

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

已篩選內容：位移

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。
此位移是從 ICMP 標頭結尾開始計算。

預先定義的 IP 封包規則

設定	規則
低	-
中	-

高	**拒絕所有 IP 封包** **拒絕來自位址 0.0.0.0 (遮罩為 0.0.0.0) 的 IPv4 封包。** 當封包符合規則時，不要記錄。

允許/拒絕

只要在連結上按一下滑鼠，就可決定是否要接受或拒絕特別定義的 IP 封包。

IPv4/IPv6

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IPv4 或 IPv6 遮罩。

事件資料庫

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入事件資料庫。

傳出規則

傳出規則可定義為使用 Avira FireWall 來控制傳出資料的流量。
您可以為下列其中一項通訊協定定義傳出的規則：IP、ICMP、UDP、TCP。
請參閱新增規則。

> **警告**
> 封包經過篩選之後，就會連續套用對應的規則，因此規則順序就非常重要。
> 只有當您很清楚自己的行為有何後果時才變更規則順序。

管理規則的按鈕

按鈕	說明
新增規則	允許您建立新的規則。 如果您按下此按鈕，就會開啟 **[新增規則]** 對話方塊。 您可以在此對話方塊中選取新規則。
移除規則	移除選取的規則。
規則上移	將選取的規則上移一行，也就是提高規則的優先順序。
規則下移	將選取的規則下移一行，也就是降低規則的優先順序。
重新命名規則	允許您為選取的規則賦予另一個名稱。

注意

您可以為電腦上個別介面卡或所有介面卡新增規則。
若要為所有介面卡新增介面卡規則，從顯示的介面卡階層選取 **[我的電腦]**，然後按一下 **[新增規則]** 按鈕。 請參閱新增規則。

注意

若要變更規則位置，您還可以使用滑鼠將規則拖曳到所需的位置。

新增規則

您可以在此視窗選取新的傳入與傳出規則。 選取的規則與預設資訊會包含在 **[介面卡規則]** 視窗中，您可從此位置定義更詳細的內容。 除了傳入與傳出規則之外，還提供更多規則。

可能的規則

允許對等網路

允許點對點連線：連接埠 4662 上的傳入 TCP 通訊與連接埠 4672 上的傳入 UDP 通訊

TCP 連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入允許的 TCP 連接埠。

UDP 連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入允許的 UDP 連接埠。

允許 VMWARE 連線

允許 VMware 虛擬機器通訊

封鎖 IP

封鎖來自指定 IP 位址的所有流量

網際網路通訊協定版本

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 位址。

封鎖子網路

封鎖來自指定 IP 位址與子網路遮罩的所有流量

網際網路通訊協定版本

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 位址。

子網路遮罩

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的子網路遮罩。

允許 IP

允許來自指定 IP 位址的所有流量

網際網路通訊協定版本

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 位址。

允許子網路

允許來自指定 IP 位址與子網路遮罩的所有流量

網際網路通訊協定版本

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 位址。

子網路遮罩

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的子網路遮罩。

允許網路伺服器

允許從連接埠 80 上的網路伺服器通訊：在連接埠 80 上傳入 TCP 通訊

連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入網路伺服器使用的連接埠。

允許 VPN 連線

允許與指定 IP 進行 VPN (虛擬私人網路) 連線：X 個連接埠上的傳入 UDP 資料流量、X 個連接埠上的傳入 TCP 資料流量、使用通訊協定 ESP(50)、GRE(47) 的傳入 IP 資料流量

網際網路通訊協定版本

只要在此連結上按一下滑鼠，您即可選擇 IPv4 或 IPv6。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 位址。

允許「遠端桌面」連線

允許在連接埠 3389 上進行「遠端桌面」連線 (遠端桌面通訊協定)

連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入應用於允許的遠端桌面連線的連接埠。

允許 VNC 連線

允許在連接埠 5900 上進行 VNC (虛擬網路運算) 連線

連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入應用於允許的遠端桌面連線的連接埠。

允許「檔案及印表機共用」。

允許存取印表機與檔案核准：來自指定 IP 位址的連接埠 137、139 上的傳入 TCP 資料流量，與連接埠 445 上的傳入 UDP 資料流量。

可能的傳入規則

- **傳入 IP 規則**
- **傳入 ICMP 規則**

- 傳入 UDP 規則
- 傳入 TCP 規則
- 傳入 IP 通訊協定規則

可能的傳出規則

- 傳出 IP 規則
- 傳出 ICMP 規則
- 傳出 UDP 規則
- 傳出 TCP 規則
- 傳出 IP 通訊協定規則

> 注意
> 可能的傳入與傳出規則選項，與預先定義的相關通訊協定規則語法完全一樣，請參閱FireWall > 介面卡規則底下的說明。

按鈕

按鈕	說明
確定	反白的規則已納入為新的介面卡規則。
取消	視窗已關閉，且未新增任何新規則。

應用程式規則

使用者的應用程式規則

此清單包含系統中的所有使用者。
如果您是以系統管理員身分登入，可以選取要套用規則的使用者。
如果您不是具有權限的使用者，則只能看到目前登入的使用者。

應用程式

此表顯示已定義規則的應用程式清單。 應用程式清單包含了電腦上安裝 Avira FireWall 之後，曾經執行過而且已儲存規則的每個應用程式。

一般檢視

欄位	說明
應用程式	應用程式名稱。
啟用連線	應用程式開啟的啟用連線數量。
動作	顯示當應用程式正在使用網路時，Avira FireWall 將自動採取的行動 (不管網路使用類型為何)。 使用滑鼠按一下連結時，可以切換為其他動作類型。 動作類型分為**詢問**、**允許**或**拒絕**。 **詢問**是預設動作。

進階組態

如果應用程式的網路存取活動需要使用個別規則，則您可以依據封包篩選器並比照先前建立介面卡規則的方式來建立應用程式規則。

- 若要變更應用程式規則的進階組態，請先啟用 **[組態]** 視窗中的 **[專家模式]** 選項。
- 接著移至 **[組態] > [網際網路防護] > FireWall > [設定]**，再啟用 **[應用程式規則]** 底下的 *[進階設定]* 選項。
- 按一下 **[套用]** 或 **[確定]** 儲存設定。

↳ 在 **[組態] > [網際網路防護] > [FireWall] > [應用程式規則]** 區段底下，應用程式規則清單中會顯示額外的 **[篩選]** 標題欄位，且各應用程式皆有 **[基本]** 項目。

欄位	說明
應用程式	應用程式名稱。
啟用連線	應用程式開啟的啟用連線數量。
動作	顯示當應用程式正在使用網路時，Avira FireWall 將自動採取的行動 (不管網路使用類型為何)。 如果您在 **[篩選]** 欄位中選擇 **[基本]**，即可按一下選擇其他動作類型的連結。這些數值分為**詢問**、**允許**或**拒絕**。 如果您在 **[篩選]** 欄位中選擇 **[進階]**，則會顯示 **[規則]** 動作類型。 **[規則]** 連結會開啟 **[進階應用程式規則]** 視窗，您可在此輸入應用程式的特定規則。
篩選	顯示篩選類型。 您可以按一下連結選取另一個篩選類型。 **基本**：如果是簡易篩選，則會對軟體應用程式執行的所有網路活動進行指定的動作。 **進階**：如果是這種篩選類型，則會套用已加入延伸組態的規則。

- 如果您想要建立應用程式特定的規則，請選取 **[篩選]** 底下的 **[進階]** 項目。
  - ↳ **[規則]** 項目隨即顯示在 **[動作]** 欄中。
- 按一下 **[規則]** 即可開啟用來建立特定應用程式規則的視窗。

進階組態中的指定應用程式規則

利用指定的應用程式規則可讓您針對應用程式允許或拒絕指定的資料流量，或是允許或拒絕被動聆聽個別連接埠。 以下為可用的選項：

允許/拒絕植入程式碼

「植入程式碼」這項技巧可將程式碼引入另一個處理序的位址空間以執行相關動作，進而強制此處理序載入動態連結程式庫 (DLL)。
惡意程式碼特別喜歡利用植入程式碼方式，以其他程式為掩護來執行程式碼。
如此一來，便可隱藏網際網路存取活動，不讓防火牆發現。
預設模式會針對所有簽署的應用程式啟用植入程式碼功能。

允許/拒絕被動聆聽連接埠上的應用程式

允許/拒絕流量

允許或拒絕傳入與/或傳出的 IP 封包

允許或拒絕傳入與/或傳出的 TCP 封包

允許或拒絕傳入與/或傳出的 UDP 封包

您可以針對每一個應用程式，建立想要的應用程式規則，而且數量不限。
應用程式規則執行順序如下所示 (相關資訊請參閱進階應用程式規則)。

> 注意
> 如果您要將應用程式規則的 **[進階]** 切換為 **[基本]** 篩選，已在進階組態中的現有應用程式規則只是停用，並不會永久刪除。當您再次選取 **[進階]** 篩選時，現有應用程式規則會重新啟用，並顯示在 **[應用程式規則]** 組態視窗中。

應用程式詳細資料

在此方塊中，您可以檢視應用程式清單方塊中選取的應用程式詳細資料。

- *名稱* - 應用程式名稱

- *路徑* - 可執行檔的完整路徑。

按鈕

按鈕	說明
新增應用程式	允許您建立新的應用程式規則。 如果您按下此按鈕，就會開啟對話方塊。您可在此選取所需的應用程式，以建立新規則。
移除規則	移除選取的應用程式規則。
顯示詳細資料	「**顯示詳細資料**」視窗會顯示應用程式清單方塊中選取的詳細資料。(選項僅能用於專家模式。)
重新載入	重新載入應用程式清單，並同時捨棄剛才的變更。

進階應用程式規則

[進階應用程式規則]
視窗可讓您針對應用程式資料流量及接聽連接埠所需，建立指定的規則。 您可以使用 **[新增規則]** 按鈕，建立新的規則。 您可以在視窗下方進一步指定規則。
您可以為應用程式建立想要的規則，而且數量不限。 規則會按照顯示的順序依序執行。
您可以使用 **[規則上移]** 與 **[規則下移]** 按鈕，變更規則的順序。

> 注意
> 若要變更應用程式規則的位置，您還可以使用滑鼠將規則拖曳到所需的位置。

應用程式詳細資料

所選取應用程式的相關資訊會顯示在 *[應用程式詳細資料]* 區域中。

- *名稱* - 應用程式名稱。
- *路徑* - 應用程式可執行檔的路徑。

規則選項

拒絕/允許植入程式碼

只要在連結上按一下滑鼠，就可決定是否要針對選取的應用程式允許或拒絕植入程式碼。

規則類型：流量/接聽

只要在連結上按一下滑鼠，就可決定是否要針對監視流量或是接聽連接埠建立規則。

拒絕/允許動作

只要在此連結上按一下滑鼠，就可以決定要使用規則執行哪一項動作。

連接埠

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入要套用接聽規則的本機連接埠。 您也可以輸入一些連接埠或連接埠範圍。

傳出、傳入、所有套件

只要在連結上按一下滑鼠，就可決定讓流量規則只監視傳出的封包或是只監視傳入的封包。

IP 封包/TCP 封包/UDP 封包

只要在此連結上按一下滑鼠，就可以決定由哪一項通訊協定監視流量規則。

IP 封包選項：

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 位址。

IP 遮罩

只要在連結上按一下滑鼠，就會立即開啟對話視窗供您輸入所需的 IP 遮罩。

TCP 封包 / UDP 封包選項：

本機 IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入本機 IP 位址。

本機 IP 遮罩

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的本機 IP 遮罩。

遠端 IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的遠端 IP 位址。

遠端 IP 遮罩

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的遠端 IP 遮罩。

本機連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義本機連接埠編號，甚至是完整的連接埠範圍。

遠端連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義一個或多個所需的遠端連接埠，甚至是完整的連接埠範圍。

報告檔

只要在連結上按一下滑鼠，就可選擇執行規則時要「**記錄**」或「**不記錄**」到程式的報告檔。

按鈕

按鈕	說明
新增規則	建立新的應用程式規則。
移除規則	刪除選取的應用程式規則。

規則上移	將選取的規則上移一行，也就是提高規則的優先順序。
規則下移	將選取的應用程式規則下移一行，也就是降低規則的優先順序。
重新命名規則	編輯選取的規則，以便輸入新的規則名稱。
套用	Avira FireWall 會接受所做的變更並立即套用。
確定	套用所做的變更。 關閉用來設定應用程式規則的視窗。
取消	關閉用來設定應用程式規則的視窗，而不套用所做的變更。

信任的供應商

[信任的供應商] 底下會顯示一份信任的軟體生產商清單。
(僅在專家模式中才能使用選項。)

您可以透過 **[網路事件]** 快顯視窗裡的 **[一律信任此供應商]** 選項，從清單中新增或移除製造商。 您可以啟用 **[自動允許受信任供應商的應用程式]** 選項，預設允許由清單中的供應商所簽署的應用程式網路存取行為。

使用者的受信任供應商

此清單包含系統中的所有使用者。
如果您是以系統管理員身分登入，可以選取要檢視或更新信任的供應商清單的使用者。
如果您不是具有權限的使用者，則只能看到目前登入的使用者。

自動允許受信任供應商建立的應用程式

此選項一經啟用，會自動允許內含已知及受信任供應商簽章的應用程式存取網路。
此選項會啟用為預設值。

供應商

此清單列出歸類為受信任的所有供應商。

按鈕

按鈕	說明
移除	反白的項目會從受信任的供應商清單中移除。 若要從清單中永久移除選取的供應商，在組態視窗裡按一下 **[套用]** 或 **[確定]**。
重新載入	已回復所做的變更。 已載入上次儲存的清單。

> 注意
>
> 如果您從清單中移除供應商，並選取 **[套用]**，則會從清單中永久移除供應商。使用 **[重新載入]** 無法回復變更。 不過，您可以透過 **[網路事件]** 快顯視窗裡的 **[一律信任此供應商]** 選項，再次將供應商新增至受信任的供應商清單中。

> 注意
>
> FireWall
>
> 會先排列應用程式規則的優先順序，再輸入信任的供應商清單中：如果您已建立應用程式規則且應用程式供應商列在信任的供應商清單中，則會執行應用程式規則。

設定

僅在專家模式中才能使用選項。

進階選項

啟動時停止 Windows 防火牆

此選項一經啟用，一旦電腦重新開機，就會停用 Windows 防火牆。
此選項會啟用為預設值。

自動規則逾時

永遠封鎖

此選項一經啟用，舉例來說，會保留在連接埠掃描期間自動建立的規則。

在 n 秒後移除規則

此選項一經啟用，舉例來說，在連接埠掃描期間自動建立的規則會在經過您定義的時間之後再次遭到移除。 此選項會啟用為預設值。
在方塊中你可以指定在數秒之後將會移除的規則。

通知

通知項目可定義您希望從 FireWall 收到桌面通知的相關事件。

連接埠掃描

此選項一經啟用，只要 FireWall 偵測到連接埠掃描，您就會收到桌面通知。

洪水攻擊

此選項一經啟用，只要 FireWall 偵測到洪水攻擊，您就會收到桌面通知。

封鎖的應用程式

此選項一經啟用，只要 FireWall 拒絕活動
(例如封鎖了某個應用程式的網路活動)，您就會收到桌面通知。

封鎖的 IP

此選項一經啟用，只要 FireWall 拒絕活動 (例如封鎖了來自某個 IP 位址的資料流量)，您就會收到桌面通知。

應用程式規則

您可在 FireWall > 應用程式規則區段中，使用應用程式規則選項來設定其組態選項。

進階設定

此選項一經啟用，就可以個別規定應用程式的網路存取行為。

基本設定

此選項一經啟用，不同的應用程式網路存取行為只能設定一項動作。

快顯設定

僅在專家模式中才能使用選項。

檢查處理序啟動堆疊

此選項一經啟用，處理序堆疊便可更精準地控制處理序堆疊偵測作業。FireWall 會假定堆疊中只要有任何一個處理序實際上透過所屬的子處理序來存取網路的處理序，就不值得信賴。
因此，處理序堆疊會針對每個不值得信賴的處理序開啟個別的快顯視窗。
預設會停用此選項。

允許每個處理序有多個快顯

此選項一經啟用，每次應用程式進行網路連線時，就會觸發快顯視窗。
或者，您只會在第一次連線嘗試時才會收到通知。 預設會停用此選項。

記住此應用程式的動作

一律啟用

一旦啟用此選項，會啟用「**網路事件**」對話方塊中預設的「**記住此應用程式的動作**」選項。

一律停用

一旦啟用此選項，會停用「**網路事件**」對話方塊中預設的「**記住此應用程式的動作**」選項。

僅對已簽署的應用程式啟用

一旦啟用此選項，簽署的應用程式會在網路存取期間自動啟用「**網路事件**」對話方塊中預設的「**記住此應用程式的動作**」選項。
簽署的應用程式將由所謂的「信任的供應商」來分配 (請參閱信任的供應商)。

記住上次使用的狀態

一旦啟用此選項，「**網路事件**」對話方塊中的「**記住此應用程式的動作**」選項啟用狀態，會比照上次的網路事件。
如果「**記住此應用程式的動作**」選項已啟用，則後續的網路事件便會啟用此選項。
如果已針對上次網路事件停用「**記住此應用程式的動作**」，則後續的網路事件也會停用此選項。

顯示詳細資料

在此組態選項群組中，您可以設定 **[網路事件]** 視窗中的詳細資訊顯示方式。

應要求顯示詳細資料

此選項一經啟用，詳細資訊只會應要求顯示在「**網路事件**」視窗，亦即，您可以按一下「**網路事件**」視窗中的「**顯示詳細資料**」按鈕，顯示詳細資訊。

一律顯示詳細資料

此選項一經啟用，一律在「**網路事件**」視窗中顯示詳細的資訊。

記住上次使用的狀態

此選項一經啟用，會使用先前管理網路事件的方式來管理詳細資訊的顯示方式。
如果在上次網路事件期間曾經檢視或存取詳細資訊，則後續的網路事件也會顯示詳細資訊。
如果在上次網路事件期間曾經隱藏而不顯示詳細資訊，則後續網路事件便不會顯示詳細資訊。

12.6 Web Protection

[組態] > [網際網路防護] 底下的 **[Web Protection]** 區段負責 Web Protection 的組態。

12.6.1 掃描

當您從網際網路載入網頁瀏覽器時，Web Protection 可避免病毒或惡意程式從網頁入侵電腦。 **掃描**選項可以用來設置Web Protection 組件的行為。 (僅在專家模式中才能使用選項。)

掃描

啟用 IPv6 支援

此選項一經啟用，Web Protection 隨即支援網際網路通訊協定版本 6。
此選項不適用於 Windows 8 下的新安裝或變更安裝。

偷渡式攻擊保護

偷渡式攻擊保護可讓您設定封鎖 I-Frame (亦稱為內置框架)。 I-Frame 是 HTML 元件，亦即區隔網頁區域的網際網路頁面元素。 I-Frame 可用來載入不同的網頁內容 (通常是其他的 URL) 並在瀏覽器的子視窗中將其顯示為獨立的文件。 I-Frame 大部分用來提供橫幅廣告服務。 在某些情況下，I-Frame 會被用來隱藏惡意程式碼。 在這些情況下，瀏覽器幾乎是看不到 I-Frame 區域的。 **[封鎖可疑的 I-frame]** 選項可讓您檢查與封鎖載入的 I-Frame。

封鎖可疑的 I-frame

此選項一經啟用，會依據特定準則掃描您所要求網頁上的 I-Frame。
如果要求的網頁上有可疑的 I-Frame，會將其封鎖。 I-Frame 視窗中顯示錯誤訊息。

偵測動作

您可以定義當偵測到病毒或有害程式時，Web Protection 要執行的動作 (僅在專家模式中才能使用選項。)

互動式

此選項一經啟用，一旦在指定掃描期間偵測到病毒或有害程式時會顯示對話視窗，供您選擇對受影響檔案的處置方式。 此選項會啟用為預設值。

顯示進度列

此選項一經啟用，當網站內容下載時間超過 20 秒的逾時規定時，桌面上會出現包含下載進度列的通知。
桌面通知是專為下載更大資料容量的網站而設計：如果您使用 Web Protection，網站內容不會以增量方式下載到網際網路瀏覽器中，因為這些內容在透過網際網路瀏覽器顯示之前，會先掃描是否有病毒與惡意程式碼。 預設會停用此選項。

如需詳細資訊，請按一下這裡。

自動

此選項一經啟用，在偵測到病毒時不會出現任何對話方塊。 Web Protection 會依據您在此區段預先定義的主要與次要動作設定來因應。

主要動作

主要動作是 Web Protection 發現病毒或有害程式時優先執行的動作。

拒絕存取

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都不會傳送到您的網頁瀏覽器。網頁瀏覽器上會顯示一則錯誤訊息，通知您已經拒絕存取。 Web Protection 會在報告功能啟用時，將偵測結果記錄到報告檔案。

移至隔離區

偵測到病毒或惡意程式碼時，網路伺服器要求的網站與/或傳輸的任何資料或檔案，都會移至隔離區。
如果受影響的檔案具有參考價值，可以從隔離區管理員復原，或在必要時將其傳送至 Avira 惡意程式碼研究中心。

略過

Web Protection 會將網路伺服器要求的網站與/或傳輸的資料與檔案，傳送到您的網頁瀏覽器。
允許存取檔案並忽略檔案。

警告

工作站上受影響的檔案仍會繼續運作！ 此做法可能會對工作站造成嚴重的傷害！

封鎖的要求

您可以在 **[鎖定的要求]** 中，指定 Web Protection 要封鎖的檔案類型與 MIME 類型 (傳輸資料的內容類型)。 網路篩選器可讓您封鎖已知的網路釣魚和惡意程式碼 URL。 Web Protection 可避免從網際網路傳輸資料到您的電腦系統。
(僅在專家模式中才能使用選項。)

Web Protection 會封鎖下列檔案類型/MIME 類型

清單中的所有檔案類型與 MIME 類型 (傳輸資料的內容類型) 會遭到 Web Protection 封鎖。

輸入方塊

請在此方塊中，輸入您希望 Web Protection 封鎖的 MIME 類型與檔案類型名稱。 請針對檔案類型輸入副檔名，例如**.htm**。 針對 MIME 類型，請指出媒體類型與子類型 (適用的話)。 兩個陳述式之間可以使用單斜線來分隔，例如**video/mpeg** 或 **audio/x-wav**。

注意

不過，已經以網際網路暫存檔形式存放在電腦系統，並遭到 Web Protection 封鎖的檔案，可以由電腦的網際網路瀏覽器從網際網路下載到本機。
網際網路暫存檔指的是由網際網路瀏覽器儲存在電腦上的檔案，可供您更快速地存取網站。

注意

如果您將封鎖的檔案與 MIME 類型清單輸入到排除的檔案與 MIME 類型清單 (於 Web Protection > 掃描 > 例外底下)，則會略過此清單。

> 注意
> 輸入檔案類型及 MIME 類型時，不可以使用萬用字元 (*
> 代表任何數量的字元，或 ?代表單一字元)。

MIME 類型：媒體類型範例：

- `text` = 代表文字檔案
- `image` = 代表圖形檔案
- `video` = 代表視訊檔案
- `audio` = 代表聲音檔案
- `application` = 代表與特定程式連結的檔案

排除的檔案與 MIME 類型範例：

- `application/octet-stream` = 應用程式/octet-stream MIME 類型檔案 (可執行檔 *.bin、*.exe、*.com、*dll、*.class) 都會遭到 Web Protection 封鎖。
- `application/olescript` = 應用程式/olescript MIME 檔案類型 (ActiveX 指令碼檔案 *.axs) 都會遭到 Web Protection 封鎖。
- `.exe` = 所有帶有副檔名 .exe (可執行檔) 的檔案都會遭到 Web Protection 封鎖。
- `.msi` = 所有帶有副檔名 .msi 的檔案 (Windows Installer 檔案) 都會遭到 Web Protection 封鎖。

新增

此按鈕可讓您從輸入欄位中，將 MIME 與檔案類型複製到顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。 如果沒有選取任何項目，此按鈕將無作用。

網路篩選器

網路篩選器以內部資料庫為基礎，會每日更新並依據內容來分類 URL。

啟用網路篩選器

此選項一經啟用，符合網路篩選器清單中選取類別的所有 URL 都會遭到封鎖。

網路篩選器清單

在網路篩選器清單中，您可以選取要讓 Web Protection 封鎖其 URL 的內容類別。

注意

網路篩選器會略過排除的 URL 清單中的項目 (於 Web Protection > 掃描 > 例外底下)。

注意

垃圾**郵件 URL** 指的是透過垃圾電子郵件傳送的 URL。

「**詐騙**」類別涵蓋帶有「訂閱到期」與其他由供應商隱藏成本的服務項目等特徵的相關網頁。

例外

這些選項可讓您根據 MIME 類型 (傳輸資料的內容類型) 設定例外情況以及 Web Protection 掃描的 URL (網際網路位址) 檔案類型。 Web Protection 忽略指定的 MIME 類型和 URL，例如，該資料傳送至電腦系統時未掃描病毒和惡意程式。
(僅在專家模式中才能使用選項。)

Web Protection 略過的 MIME 類型

您可以在此欄位中，選取要讓 Web Protection 在掃描期間略過的 MIME 類型 (傳輸資料的內容類型)。

Web Protection 略過的檔案類型/MIME 類型 (使用者定義)

Web Protection 會在掃描期間略過清單中的所有 MIME 類型 (傳輸資料的內容類型)。

輸入方塊

您可以在此方塊中，輸入要讓 Web Protection 在掃描期間略過的 MIME 類型和檔案類型名稱。 請針對檔案類型輸入副檔名，例如**.htm**。 針對 MIME 類型，請指出媒體類型與子類型 (適用的話)。
兩個陳述式之間可以使用單斜線來分隔，例如**video/mpeg** 或 **audio/x-wav**。

注意
輸入檔案類型及 MIME 類型時，不可以使用萬用字元 (*
代表任何數量的字元，或 ?代表單一字元)。

警告
在沒有進一步掃描封鎖要求的情況下，排除清單上的所有檔案類型及內容類型會下載至網際網路瀏覽器 (在 [Web Protection] > [掃描] > [封鎖請求] 中封鎖的檔案清單及 MIME 類型) 或經由 Web Protection：針對所有排除清單上的項目，檔案清單及 MIME 類型上要封鎖的項目都會忽略。 不會執行病毒與惡意程式碼掃描。

MIME 類型：媒體類型範例：

- `text` = 代表文字檔案
- `image` = 代表圖形檔案
- `video` = 代表視訊檔案
- `audio` = 代表聲音檔案
- `application` = 代表與特定程式連結的檔案

排除的檔案與 MIME 類型範例：

- `audio/` = 代表要從 Web Protection 掃描中排除的所有音訊媒體類型檔案
- `video/quicktime` = 代表要從 Web Protection 掃描中排除的所有 Quicktime 子類型視訊檔案 (*.qt、*.mov)
- `.pdf` = 代表要從 Web Protection 掃描中排除的所有 Adobe PDF 檔案。

新增

此按鈕可讓您從輸入欄位中，將 MIME 與檔案類型複製到顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。 如果沒有選取任何項目，此按鈕將無作用。

Web Protection 略過的 URL

此清單中的所有 URL 會從 Web Protection 掃描中排除。

輸入方塊

在此方塊中，您可以輸入要從 Web Protection 掃描中排除的 URL (網際網路位址)，例如 `www.domainname.com`。
您可以指定部分URL，使用前導或後續句點來指定網域層級：`domainname.com`可代表所有網頁和子網域。 使用結尾句點來指定任何頂層網域 (`.com` 或 `.net`) 的網站：`domainname.`。
如果您不使用前導或結尾句點來指定字串，會將字串解譯為頂層網域，例如 `net` 可代表所有 NET 網域 (`www.domain.net`)。

注意

在指定 URL 時，您也可以使用萬用字元 *來代表任何數量的字元。
您也可以使用前導或後續句點並結合萬用字元來指定網域層級：
`.domainname.*`
`*.domainname.com`
`.*name*.com` (有效但不建議)
不使用句點指定，如 `*name*`，會將字串解譯為頂層網域，不建議採用此方式。

警告

在沒有經由網站篩選器或 Web Protection 進一步掃描的情況下，排除 URL 清單上的所有網站會下載至網際網路瀏覽器：針對網路篩選器中所有排除 URL 清單上的項目 (請參閱 [Web Protection] > [掃描] > [封鎖請求]) 都會忽略。

不會執行病毒與惡意程式碼掃描。 因此，請僅讓信任的 URL 從 Web Protection 掃描中排除。

新增

此按鈕可讓您將輸入到輸入欄位中的 URL (網際網路位址)，複製到檢視器視窗。

刪除

此按鈕會從清單刪除選取的項目。 如果沒有選取任何項目，此按鈕將無作用。

範例：略過的 URL

- `www.avira.com` -OR- `www.avira.com/*`
  = 所有含網域 `www.avira.com` 的 URL 都會從 Web Protection 掃描中排除：*www.avira.com/en/pages/index.php*、*www.avira.com/en/support/index.html*、*www.avira.com/en/download/index.html*等。
  含網域 `www.avira.de` 的 URL 都不會從 Web Protection 掃描中排除。
- `avira.com` -或- `*.avira.com`
  = 所有含第二層與頂層網域 `avira.com` 的 URL 都會從 Web Protection 掃描中排除：此規定意指 `.avira.com` 的所有現有子網域：*www.avira.com*、*forum.avira.com* 等。
- `avira。` -或- `*.avira.`
  * = 含 `avira` 之第二層網域的所有 URL 都從 Web Protection 掃描中排除：此規定意指 `.avira` 的所有現有頂層網域或子網域：*www.avira.com*、*www.avira.de*、*forum.avira.com* 等。
- `.*domain*.*`
  包含有字串 `domain` 的所有第二層網域 URL 都從 Web Protection 掃描中排除：*www.domain.com*、*www.new-domain.de*、*www.sample-domain1.de* ...
- `net` -或- `*.net`
  = 有頂層網域 `net` 的所有 URL 都從 Web Protection 掃描中排除：*www.name1.net*、*www.name2.net* 等。

警告

請盡可能精準地輸入要從 Web Protection 掃描中排除的 URL。
請避免指定整個頂層網域或部分的第二層網域，因為可能會散佈惡意程式和不適當程式的網際網路頁面可能會透過排除下方的全域規格從 Web Protection 掃描中排除。
建議您至少指定完整的第二層網域和頂層網域：domainname.com

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。 (僅在專家模式中才能使用選項。)

Avira
產品內含內含威力非常強大的啟發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。
病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。 如果掃描的程式碼表現出相關特徵，就會回報為可疑。
但這並不代表程式碼本身就是惡意程式碼。 有時可能會出現誤判。
使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啟發式掃毒

您的 Avira 產品內含強大的巨集病毒啟發式掃毒功能。
此選項一經啟用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。
此選項預設為啟用狀態，也建議使用這個選項。

先進啟發式掃毒分析與偵測 (AHeAD)

啟用 AHeAD

您的 Avira 程式內含內含威力強大的 Avira AHeAD 啟發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。
此選項一經啟用，您可以定義此啟發式掃毒技術的「積極」程度。
此選項預設為啟用狀態。

低偵測等級

此選項一經啟用，會偵測到稍微不明的惡意程式碼，在此情況下錯誤警示的機率也很低。

中偵測等級

此選項結合強大的偵測等級與低風險錯誤警示。
如果您已選取使用此啟發式掃毒技術，預設會啟用中偵測等級。

高偵測等級

如果啟用此選項，會偵測到明顯更多不明的惡意程式碼，但也有可能是誤判。

12.6.2 報告

Web Protection
包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啟用，Web Protection 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啟用，Web Protection 會將重要的資訊 (有關病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更為簡明易懂。
此選項預設為啟用狀態。

進階

此選項一經啟用，Web Protection 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啟用，Web Protection
會將所有可用資訊記錄到報告檔中，包括檔案大小、檔案類型、日期等等。

限制報告檔

將大小限制為 n MB

此選項一經啟用，可將報告檔大小限定為特定大小；可能的值如下：允許的值介於 1 到 100 MB。 當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。
如果記錄檔大小超出指定大小 50 KB
以上，會先刪除舊的項目，直到達到指定大小減去 20%。

在報告檔中寫入組態

此選項一經啟用，會將即時掃描的組態記錄在報告檔中。

> 注意
> 如果您未指定任何報告檔案限制，會在報告檔案達到 100MB
> 時自動刪除較舊的項目。 項目會持續刪除直到報告檔案大小達到 80 MB。

12.7 Mail Protection

[組態] 的 **[Mail Protection]** 區段負責 Mail Protection 的組態。

12.7.1 掃描

使用 Mail Protection 來掃描內送電子郵件中的病毒、惡意程式碼與垃圾郵件。
外寄的電子郵件可以使用 Mail Protection 來掃描其中的病毒與惡意程式碼。
電腦上由不明的傀儡程式所寄發的垃圾郵件可由 Mail Protection
加以封鎖以防堵垃圾郵件。

掃描內送電子郵件

此選項一經啟用，會掃描內送電子郵件中是否有病毒與惡意程式碼以及垃圾郵件。
Mail Protection 支援 POP3 與 IMAP 通訊協定。
啟用電子郵件用戶端所使用的收件匣帳戶，接收由 Mail Protection 監視的電子郵件。

監視 POP3 帳戶

此選項一經啟用，會在指定的連接埠上監視 POP3 帳戶。

監視的連接埠

請在此欄位中，輸入 POP3 通訊協定要當做收件匣使用的連接埠。
多個連接埠可用逗號來分隔。 (僅在專家模式中才能使用選項。)

預設值

此按鈕會將指定的連接埠重設為預設的 POP3 連接埠。
(僅在專家模式中才能使用選項。)

監視 IMAP 帳戶

此選項一經啟用，會在指定的連接埠上監視 IMAP 帳戶。

監視的連接埠

請在此欄位中，輸入 IMAP 通訊協定要當做收件匣使用的連接埠。
多個連接埠可用逗號來分隔。 (僅在專家模式中才能使用選項。)

預設值

此按鈕會將指定的連接埠重設為預設的 IMAP 連接埠。
(僅在專家模式中才能使用選項。)

掃描外寄電子郵件 (SMTP)

此選項一經啟用，會掃描外寄的電子郵件中是否有病毒與惡意程式碼。
由不明傀儡程式所寄發的垃圾郵件會遭到封鎖。

監視的連接埠

請在此欄位中，輸入 SMTP 通訊協定要當做寄件匣使用的連接埠。
多個連接埠可用逗號來分隔。 (僅在專家模式中才能使用選項。)

預設值

此按鈕會將指定的連接埠重設為預設的 SMTP 連接埠。
(僅在專家模式中才能使用選項。)

> 注意
> 若要確認使用的通訊協定與連接埠，請開啟電子郵件用戶端程式中的電子郵件帳戶內容。 正常情況下會使用預設連接埠。

啟用 IPv6 支援

此選項一經啟用，Mail Protection 隨即支援網際網路通訊協定第 6 版。
(選項僅可在專家模式中使用，不適用於 Windows 8 下的新安裝或變更安裝。)

偵測動作

此組態區段內含當 Mail Protection
在電子郵件或附件中發現病毒或有害程式時，所要採取的動作設定。
(僅在專家模式中才能使用選項。)

> 注意
> 這些動作會同時在內送與外寄的電子郵件中偵測到病毒時執行。

互動式

此選項一經啟用，一旦在電子郵件或附件中偵測到病毒或有害程式時會顯示對話方塊，供您選擇對相關電子郵件或附件的處置方式。 此選項預設為啟用狀態。

顯示進度列

此選項一經啟用，Mail Protection 會在電子郵件下載期間顯示進度列。
只有當「**互動式**」選項已經選取時，才會啟用此選項。

自動

此選項一經啟用，發現病毒或有害程式時便不會再通知您。 Mail Protection 會依據您在此區段定義的設定來因應。

受影響的電子郵件

選擇 Mail Protection 在電子郵件中發現病毒或有害程式時，為「*受影響的電子郵件*」所執行的動作。
「**略過**」選項一經選取，就可以同時在「*受影響的附件*」底下選取當偵測到附件中的病毒或有害程式時要執行的動作。

刪除

此選項一經啟用，當偵測到病毒或有害程式時，會自動刪除受影響的電子郵件。
電子郵件本文會以如下所示的預設內容取代。
此規則同樣適用所有包含的附件；這些附件會同時以預設內容取代。

略過

此選項一經啟用，即使偵測到病毒或有害程式，都會略過受影響的電子郵件。
不過，您可以決定要如何處置受影響的附件。

移至隔離區

此選項一經啟用，當偵測到病毒或有害程式時，會將完整的電子郵件 (包括所有附件) 放置到隔離區。 日後必要時，可以將它還原。 受影響的電子郵件本身會被刪除。
電子郵件本文會以如下所示的預設內容取代。
此規則同樣適用所有包含的附件；這些附件會同時以預設內容取代。

受影響的附件

「*受影響的附件*」選項只有在您已經選取「**略過**」設定 (位於「*受影響的電子郵件*」底下) 時才能選取。
透過這個選項，現在您可以決定當偵測到附件中的病毒或有害程式時，要執行的動作。

刪除

此選項一經啟用，當偵測到病毒或有害程式時，會將受影響的附件刪除並以預設內容取代。

略過

此選項一經啟用，即使偵測到病毒或有害程式，都會略過並遞送附件。

警告

此選項一經選取，Mail Protection 便無法保護您免於病毒或有害程式的侵擾。
只有當您很清楚自己的行為有何後果時才選取此項目。
請停用電子郵件程式中的預覽功能，而且絕對不要按兩下附件加以開啟！

移至隔離區

此選項一經啟用，會將受影響的附件置放到隔離區並予以刪除 (以預設內容取代)。日後必要時，可以將受影響的附件還原。

進一步動作

此組態區段內含當 Mail Protection
在電子郵件或附件中發現病毒或有害程式時，所要採取的動作設定。
(僅在專家模式中才能使用選項。)

注意

這些動作只有在內送的電子郵件中偵測到病毒時才會執行。

刪除及移動電子郵件時顯示的預設文字

此方塊中的內容會插入到電子郵件中 (而非受影響的電子郵件中) 並當成郵件傳送出去。您可以編輯此訊息。內容長度上限為 500 個字元。

您可以使用下列按鍵組合來格式化郵件：

Ctrl + Enter = 插入換行符號。

預設值

此按鈕會將預先定義的預設內容插入編輯方塊中。

刪除與移動附件時顯示的預設文字

此方塊中的內容會插入到電子郵件中 (而非受影響的附件中) 並當成郵件傳送出去。您可以編輯此訊息。 內容長度上限為 500 個字元。

您可以使用下列按鍵組合來格式化郵件：

Ctrl + Enter = 插入換行符號。

預設值

此按鈕會將預先定義的預設內容插入編輯方塊中。

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。 (僅在專家模式中才能使用選項。)

Avira
產品內含威力非常強大的啟發式掃毒模組，可主動發現不明的惡意程式碼，例如，可在完成用來對抗破壞元素的特殊病毒簽章之前，以及在病毒保護更新傳送之前先行制敵機先。
病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。 如果掃描的程式碼表現出相關特徵，就會回報為可疑。
但這並不代表程式碼本身就是惡意程式碼。 有時可能會出現誤判。
使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啟發式掃毒

您的 Avira 產品內含強大的巨集病毒啟發式掃毒功能。
此選項一經啟用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。
系統不只預設啟用此選項，也建議使用這個選項。

先進啟發式掃毒分析與偵測 (AHeAD)

啟用 AHeAD

您的 Avira 程式內含內含威力強大的 Avira AHeAD 啟發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。

此選項一經啟用，您可以定義此啟發式掃毒技術的「積極」程度。
此選項會啟用為預設值。

低偵測等級

此選項一經啟用，會偵測到稍微不明的惡意程式碼，在此情況下錯誤警示的機率也很低。

中偵測等級

此選項結合強大的偵測等級與低風險錯誤警示。
如果您已選取使用此啟發式掃毒技術，預設會啟用中偵測等級。

高偵測等級

如果啟用此選項，會偵測到明顯更多不明的惡意程式碼，但也有可能是誤判。

AntiBot

Mail Protection 的 AntiBot 功能可防止您的電腦變成所謂的殭屍網路的一部份，並被用於傳送垃圾郵件：要透過殭屍網路傳送垃圾郵件，攻擊者通常會利用傀儡程式感染大量的電腦，然後再連接至 IRC 伺服器、打開特定的頻道並等待命令傳送給垃圾郵件。
為了區分由不明傀儡電腦所寄發的垃圾電子郵件與正常電子郵件，Mail Protection 會檢查外寄電子郵件的 SMTP 伺服器與寄件者是否包含在許可的伺服器與寄件者清單中。如果與預期不符，則會封鎖外寄的電子郵件，亦即不會寄發電子郵件。
封鎖的電子郵件會顯示在對話方塊中。 (僅在專家模式中才能使用選項。)

> 注意
> 只有在啟用 Mail Protection 掃描外寄郵件時才會使用 AntiBot 功能 (請參閱 [Mail Protection] > [掃描] 底下的 **[掃描外寄郵件]** 選項)。

允許的伺服器

此清單中的所有伺服器皆由 Mail Protection 授權傳送電子郵件：傳送至這些伺服器的電子郵件不會被 Mail Protection 封鎖。

如果清單中沒有任何伺服器，就不會掃描用來傳送外寄電子郵件的 SMTP 伺服器。
如果清單中有伺服器，Mail Protection 會封鎖未列在清單中的所有 SMTP 伺服器所寄出的電子郵件。

輸入方塊

請在此方塊中，輸入要用來寄送電子郵件的 SMTP 伺服器主機名稱或 IP 位址。

> 注意
> 您可以在電子郵件程式中當初建立使用者帳戶的日期底下，找到電子郵件程式用來傳送電子郵件的 SMTP 伺服器詳細資料。

新增

您可以使用這個按鈕，將輸入方塊中指定的伺服器納入許可的伺服器清單中。

刪除

此按鈕會從許可的伺服器清單中，刪除反白的項目。
如果沒有選取任何項目，此按鈕將無作用。

全部清除

此按鈕會從許可的伺服器清單中，刪除所有項目。

允許的寄件者

此清單中的所有寄件者皆由 Mail Protection 授權傳送電子郵件：由此電子郵件地址傳送的電子郵件不會被 Mail Protection 封鎖。
如果清單中沒有任何寄件者，就不會掃描用來傳送外寄電子郵件的電子郵件地址。
如果清單中有寄件者，Mail Protection 會封鎖未列在清單中的所有寄件者所寄出的電子郵件。

輸入方塊

請在此方塊輸入您的電子郵件寄件者地址。

新增

您可以使用這個按鈕，將輸入方塊中指定的寄件者納入許可的寄件者清單中。

刪除

此按鈕會從許可的寄件者清單中，刪除反白的項目。
如果沒有選取任何項目，此按鈕將無作用。

全部清除

此按鈕會從許可的寄件者清單中，刪除所有項目。

12.7.2 一般

例外

掃描例外

此表會顯示排除在 Mail Protection 描範圍外的電子郵件地址清單 (白名單)。

> 注意
> Mail Protection 會針對內送電子郵件，獨佔使用例外清單。

掃描例外

輸入方塊

您可以在此方塊中，輸入要新增至不接受掃描的電子郵件地址清單中的電子郵件地址。
依據您的設定，Mail Protection 日後將不再掃描這些電子郵件地址。

> 注意
> 您輸入電子郵件地址時，可以使用萬用字元：* 代表任何數量的字元與 ? 代表單一字元。
> 不過，您可以專門針對不接受垃圾郵件掃描的電子郵件地址使用萬用字元。

如果您藉由勾選 **[惡意程式碼]**
排除清單方塊，嘗試從惡意程式碼掃描中排除包含萬用字元的地址時，會收到錯誤訊息。
請注意，當您輸入包含萬用字元的地址時，指定的字元順序必須與電子郵件地址結構相符 (*@*.*)。

警告
使用萬用字元時，請參考提供的範例。
請選擇性使用萬用字元，並注意要將哪些包含萬用字元的電子郵件地址納入垃圾郵件白名單中。

範例：在電子郵件地址中使用萬用字元 (垃圾郵件白名單)

- `virus@avira.* / =`
  所有含此地址的電子郵件與任何頂層網域：virus@avira.de、virus@avira.com、virus@avira.net 等。
- `*@avira.com` = 所有從 **avira.com** 網域傳送的電子郵件：virus@avira.com、contakt@avira.com、employee@avira.com
- `info@*.com` = 所有含頂層網域的電子郵件地址 **com** 與地址 **info**：第二層網域可以為：info@name1.com, info@name2.com,...

新增

透過這個按鈕，您可以將輸入方塊中所輸入的電子郵件地址，新增至不要掃描的電子郵件地址清單中。

刪除

此按鈕會從清單中刪除反白的電子郵件地址。

電子郵件地址

不會再掃描的電子郵件。

惡意程式碼

此選項一經啟用，就不會再掃描該電子郵件地址來尋找惡意程式碼。

垃圾郵件

此選項一經啟用，就不會再掃描該電子郵件地址來尋找垃圾郵件。

上移

您可以使用此按鈕，將反白的電子郵件地址上移至較高的位置。
如果沒有反白的項目，或者反白的地址已經列在清單首位，此按鈕就不會啟用。

下移

您可以使用此按鈕，將反白的電子郵件地址下移至較低的位置。
如果沒有反白的項目，或者反白的地址已經列在清單末尾，此按鈕就不會啟用。

匯入 Outlook 通訊錄

透過這個按鈕，您可以從 MS Outlook
電子郵件程式的通訊錄中，將電子郵件地址匯入例外清單中。
匯入的電子郵件地址便不會經過垃圾郵件掃描。

Import Outlook Express 通訊錄 (Windows XP) / 匯入 Windows Mail 通訊錄 (Windows Vista、Windows 7)

透過這個按鈕，您可以從 MS Outlook Express 或 Windows Mail
電子郵件程式的通訊錄中，將電子郵件地址匯入例外清單中。
匯入的電子郵件地址便不會經過垃圾郵件掃描。

快取

Mail Protection 快取包含掃描的電子郵件相關資料，並以統計資料形式顯示在控制中心的 **Mail Protection** 下。 (僅在專家模式中才能使用選項。)

內送電子郵件的副本同時也會寄存在快取中。
反垃圾郵件模組的訓練功能也可使用這些電子郵件 (*良好的電子郵件 – 用於訓練*、*垃圾郵件 – 用於訓練*)。

> **注意**
> 您必須啟用反垃圾郵件模組以便將內送電子郵件備份到快取中。

存放在快取區中的電子郵件數目上限

此欄位可用來設定 Mail Protection 要存放在快取中的電子郵件數量上限。
日期最早的電子郵件會最先刪除。

儲存電子郵件的天數上限

您可在此方塊中，輸入電子郵件儲存天數上限。
過了這段時間，就會從快取中移除電子郵件。

清空快取

按一下此按鈕以刪除存放在快取中的電子郵件。

頁尾

您可以在 **[頁尾]** 底下設定所傳送的電子郵件中顯示的電子郵件頁尾。
(僅在專家模式中才能使用選項。)

這項功能需要啟用外寄電子郵件的 Mail Protection 掃描功能 (請參閱 **[組態] > [Mail Protection] > [掃描]** 底下的 **[掃描外寄電子郵件 (SMTP)]** 選項)。 您可以使用定義的 Avira Mail Protection 頁尾，確認病毒防護程式已掃描傳送的電子郵件。
您也可以選擇插入使用者定義的頁尾文字。
如果同時使用兩個頁尾選項，使用者定義文字會置於 Avira Mail Protection 頁尾之後。

要傳送的電子郵件頁尾

附加 Mail Protection 頁尾

此選項一經啟用，就會在外寄電子郵件的訊息文字底下顯示 Avira Mail Protection 頁尾。 Avira Mail Protection 頁尾確認傳送的電子郵件已通過 Avira Mail Protection 病毒和有害程式掃描，而且不是源自不明的傀儡程式。 Avira Mail Protection 頁尾包含下列文字：「*透過 Avira Mail Protection 掃描 [產品版本] [搜尋引擎的初始及版本號碼] [病毒定義檔的初始及版本號碼]*」。

附加下列頁尾

此選項一經啟用，您在輸入方塊中插入的文字就會在傳送的電子郵件中顯示為頁尾。

輸入方塊

您可以在此輸入方塊插入文字，這些文字就會在傳送的電子郵件中顯示為頁尾。

AntiSpam

Avira Mail Protection 服務會檢查電子郵件及附件是否有病毒與有害程式。
此外，它能可靠地保護您免於垃圾電子郵件的騷擾。 (僅在專家模式中才能使用選項。)

啟用 AntiSpam 模組

啟用此選項，會連帶啟用 Mail Protection 的反垃圾郵件功能。

標記電子郵件主旨

此選項一經啟用，一旦偵測到垃圾電子郵件，就會在原始主旨行中加上註解。

簡易

收到垃圾郵件或網路釣魚郵件時，會新增 [垃圾郵件] 或 [網路釣魚] 的附錄。
此選項會啟用為預設值。

詳細

屬於網路釣魚性質的垃圾郵件主旨行會加上一段前置詞，以提醒收件者注意該郵件可能為垃圾郵件。

啟用記錄功能

此選項一經啟用，Mail Protection 會建立特殊的反垃圾郵件報告檔。

使用即時黑名單

此選項一經啟用，會即時查詢所謂的「黑名單」，並透過此名單所提供的額外資訊來判斷來源可疑的電子郵件是否為垃圾郵件。

逾時：n 秒

如果在經過 n 秒之後黑名單仍舊無法提供相關資訊，則會中止查詢黑名單的嘗試動作。

清除訓練資料庫

按一下此按鈕以刪除訓練資料庫。

自動將外寄郵件的收件者新增至白名單

此選項一經啟用，外寄電子郵件的收件者地址會自動新增至垃圾郵件的白名單中
(不會掃描在 **[Mail Protection] > [一般] > [例外]**
中定義的電子郵件清單是否為垃圾郵件)。
來自垃圾郵件白名單上地址的內送電子郵件，不會接受垃圾郵件掃描。
不過，這些郵件會接受病毒與惡意程式碼掃描。 預設會停用此選項。

> 注意
> 只有在啟用 Mail Protection 掃描外寄郵件時才會啟用此選項 (請參閱 [Mail Protection] > [掃描] 底下的 **[掃描外寄郵件]** 選項)

12.7.3 報告

Mail Protection
包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。
(僅在專家模式中才能使用選項。)

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啟用，Mail Protection 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啟用，Mail Protection 會將重要的資訊 (有關病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更為簡明易懂。
此選項預設為啟用狀態。

延伸

此選項一經啟用，Mail Protection 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啟用，Mail Protection 會將較不重要的資訊同時包含在報告檔中。

限制報告檔

將大小限制為 n MB

此選項一經啟用，可將報告檔大小限定為特定大小；可能的值如下：允許的值介於 1 到 100 MB。 當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。
如果記錄檔大小超出指定大小 50 KB
以上，會先刪除舊的項目，直到達到指定大小減去 50 KB。

縮短報告前先備份

此選項一經啟用，縮短報告檔案前會先加以備份。

在報告檔中寫入組態

此選項一經啟用，會將 Mail Protection 組態記錄在報告檔中。

注意

如果您未指定任何報告檔案限制，會在報告檔案達到 100MB 時自動建立新報告檔。 並會建立舊報告檔的備份。
最多可儲存三個舊報告檔的備份。 日期最早的備份會最先遭到刪除。

12.8 兒童保護

使用 Avira 的*兒童保護*功能可確保幼童或其他使用電腦的人獲得安全網際網路體驗的元件。

- 有了**Safe Browsing**功能後，您即可指派角色給電腦上的各個 Windows 使用者。每個角色都能定義允許或拒絕存取的 URL 或網際網路內容類別，以及每日上網時間長度或時間限制。

相關主題：

- 關於Safe Browsing

12.8.1 Safe Browsing

您可以使用 **Safe Browsing** 功能來篩選不適當或違法的網際網路內容及限制網際網路的使用時間長度。 **Safe Browsing** 功能是*兒童保護*元件的一部份。

您可以在電腦上指派使用者角色給 Windows 使用者帳戶。
每個使用者角色都包含有下列準則的規則設定：

- 允許及封鎖的 URL (網際網路位址)
- 禁止的 URL 類別
- 網際網路使用持續時間以及必要時允許的週間日使用期限

若要依據特定類別封鎖網際網路內容，Avira 使用功能強大的 URL 清單來根據網頁的內容篩選 URL。 URL 篩選清單每小時執行一次更新、調整和擴充。
兒童、青少年與成人角色會以相關的禁止類別來加以預先設定。
網際網路使用記錄是以至少長達 5 分鐘的網際網路要求為基準。

如果啟用 **Safe Browsing**，將根據使用者角色篩選使用者要求瀏覽的所有網頁。
如果網頁遭封鎖，在瀏覽器上會顯示訊息。
如果已超過許可的使用期間或嘗試在許可的使用期間外使用，則會封鎖所要求的網站，並在瀏覽器上顯示訊息。

警告
請注意，使用 **Safe Browsing** 功能時，您必須啟用 **Web Protection** 服務。

警告
啟用 **Safe Browsing** 時，請利用密碼保護 Avira 產品的組態。
如果沒有使用密碼來保護組態，所有的電腦使用者都可以更改或停用 **Safe Browsing** 設定。 您可以在 [組態] > [一般] > [密碼] 底下啟用密碼保護。

相關主題：

- 啟用 Safe Browsing
- 指派 Safe Browsing 角色
- Safe Browsing 組態

啟用 Safe Browsing

- 開啟 Avira 控制中心，然後按一下瀏覽列中的 **[狀態]**。

  若要使用 Safe Browsing 功能，您必須啟用 **Web Protection** 服務。

- 必要時，按一下 *[網際網路防護]* 底下的 **[狀態]** 檢視旁紅色開關，即可啟用 **Web Protection** 服務。

  Web Protection 狀態在啟用時應為綠色 (I)。

  按一下 **[狀態]** 檢視旁的紅色開關以啟用 **Safe Browsing** 服務。

  Safe Browsing 的狀態在啟用時應為綠色 (I)。

- 若要為兒童或其他使用者設定 Safe Browsing 設定檔，請按一下 **[狀態]** 檢視中 **Safe Browsing**旁的組態按鈕。

相關主題：

- 關於Safe Browsing
- 指派 Safe Browsing 角色
- Safe Browsing 組態

指派 Safe Browsing 角色

先決條件：

✓ 確定您已設定個別 Windows 帳戶給各個使用已安裝 Avira 電腦的使用者後，即可指派 Safe Browsing 角色給各個 Windows 使用者帳戶。

✓ 在 Avira 產品中啟用 **Safe Browsing** 功能。

✓ 在指派角色給使用者之前，請檢查各角色的設定並進行變更。

- 在 **[狀態]** 檢視中，按一下 **Safe Browsing** 旁的組態按鈕。
- 在 **[使用者選項]** 下拉式清單中，選取要指派角色的使用者名稱。

  該清單包含在您電腦上設定的 Windows 使用者帳戶。
- 按一下 **[新增]** 按鈕。

  ↪ 使用者隨即新增至清單中。

  Avira Internet Security 擁有三種預先設定的使用者角色：

  - **兒童**
  - **青少年**
  - **成人**

  根據預設值，當您新增使用者至清單中時，指派的角色為**兒童**。
- 您可以重複按一下個別使用者的角色以指派其他的角色。

注意

啟用 **Safe Browsing** 時，Safe Browsing 組態期間尚未被指派角色的預設電腦使用者都會被指派為**兒童**的角色。您也可以變更**預設使用者**的角色。

- 按一下 **[套用]** 以儲存組態。

相關主題：

- 變更角色的屬性
- 新增或移除角色

變更角色的屬性

- 在 **[狀態]** 檢視中，按一下 **Safe Browsing** 旁的組態按鈕。
- 必要時，按一下旁邊的綠色開關以啟用**專家模式**。

  啟用後，**專家模式**的狀態會變為黃色 (I)。

  ↳ 在 **Safe Browsing** 組態視窗中，會出現 **[角色]** 選項。
- 按一下要變更的角色名稱 (例如，**青少年**) 然後按一下 **[變更]** 按鈕。

  ↳ 選取角色的 **[屬性]** 視窗隨即顯示。
- 進行所需的變更，然後按一下 **[確定]**。

相關主題：

- 角色的屬性
- Safe Browsing 組態

新增或移除角色

- 在 **[狀態]** 檢視中，按一下 **Safe Browsing** 旁的組態按鈕。
- 必要時，按一下旁邊的綠色開關以啟用**專家模式**。

  啟用後，**專家模式**的狀態會變為黃色 (I)。

↳ 在 Safe Browsing 組態視窗中，會出現 **[角色]** 選項。

- 若要刪除角色，請按一下角色名稱 (例如，**年輕人**) 然後再按一下 **[移除]** 按鈕。

> 注意
> 如果角色已指派給使用者，您無法刪除角色。

- 若要新增角色，請在輸入欄位中鍵入角色名稱 (最多 30 個字元)，然後按一下 **[新增]** 按鈕。
- 從角色清單中選取新角色名稱，然後按一下 **[變更]** 按鈕以編輯其屬性。

相關主題：

- Safe Browsing 組態
- 角色的屬性
- 指派 Safe Browsing 角色

如果您已經配置 **Safe Browsing** 密碼，組態隨即隱藏，而 **[密碼保護]** 按鈕則會顯示。

密碼保護

若要啟用「**Safe Browsing**」組態，請按「**密碼保護**」按鈕，並在「**輸入密碼**」視窗中輸入密碼。

Safe Browsing 啟用

此選項一經啟用，「**Safe Browsing**」功能會依據指派給註冊使用者的角色，檢查使用者在瀏覽網際網路時所要求的所有網頁。 如果指派的角色已將這些要求的網頁歸類為封鎖，便會加以封鎖。

> 注意
> 啟用 **Safe Browsing** 時，**Safe Browsing** 組態期間尚未被指派角色的預設電腦使用者都會被指派為**兒童**的角色。
> 您可以變更預設使用者的角色。

安裝後，會建立兒童、青少年和成人使用者角色。 預先設定的角色 (兒童、青少年、成人) 會停用網際網路使用的時間限制。

使用者選擇

使用者下拉式清單

此清單包含系統中的所有使用者。

新增

您可以使用此按鈕，將選取的使用者新增至保護的使用者清單中。

刪除

此按鈕會從清單刪除選取的項目。

使用者角色清單

此清單會顯示所有已指派角色的新增使用者。
新增使用者時，程式預設會指派兒童角色。
使用滑鼠按一下顯示的角色時，可以切換為其他角色。

注意
*預設*使用者無法刪除。

角色 (僅在專家模式中才能使用選項。)

輸入方塊

您可以在此欄位中，輸入要新增至使用者角色的角色名稱。

變更

「變更」按鈕可用來設定選取的角色。
這時會顯示對話方塊，供您針對角色定義封鎖與允許的 URL，並依據類別定義選取的禁止網頁內容。 (請參閱角色的屬性)。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的角色新增至可用的角色清單中。

移除

此按鈕會從清單刪除反白的角色。

清單

此清單會顯示所有新增的角色。 按兩下顯示的角色，可以開啟定義角色的對話方塊。

> 注意
> 已經指派給使用者的角色無法刪除。

相關主題：

- 關於 Safe Browsing
- 角色的屬性
- 使用時間長度
- 使用時間

角色的屬性

[屬性] 視窗可讓您定義使用網際網路時所需的選取的角色。
(僅在專家模式中才能使用選項。)

您可以明確地允許或禁止存取 URL。 您可以依據選取項目，封鎖特定網頁內容類別。
您也可以選擇限制網際網路使用時間。

控制下列 URL 的存取

此清單會顯示所有帶有 **[封鎖]** 或 **[允許]** 指派規則的新增 URL。 新增 URL 時，程式預設會指派 **[封鎖]** 規則。 您可以按一下規則，切換指派的規則。

新增 URL

此欄位可供您指定家長監護功能要控制的 URL。
您可以指定部分URL，使用前導或後續句點來指定網域層級：domainname.com 可代表所有網頁和子網域。 使用結尾句點來指定任何頂層網域 (.com 或 .net) 的網站：domainname.。
如果您不使用前導或結尾句點來指定字串，會將字串解譯為頂層網域，例如 net 可代表所有 NET 網域 (www.domain.net)。 您也可以使用萬用字元 * 來代表任何數量的字元。
您也可以使用前導或後續句點並結合萬用字元來指定網域層級。

注意

URL 規則會依據指定的網域標籤數目來排列優先順序。
指定的網域標籤數目越多，表示規則的優先順序等級越高。 例如：
URL：www.avira.com - 規則：允許
URL：.avira.com - 規則：封鎖
該規則允許在 *www.avira.com* 網域的所有 URL。 *forum.avira.com* URL則封鎖。

注意

. 或 * 涵蓋所有 URL。
例如只想要釋出少量明確指定網頁供兒童角色瀏覽時，您可以使用這些詳細資料並依下列規則設定：
URL：* 或 . 規則：封鎖
URL：kids.yahoo.com - 規則：允許
URL：kids.nationalgeographic.com - 規則：允許
除了帶有 *kids.yahoo.com* 及 *kids.nationalgeographic.com* 網域的 URL 外，此規則可設定封鎖所有 URL。

新增

藉由這個按鈕，您可以將輸入的 URL 新增到控制的 URL 清單。

刪除

此按鈕會從控制的 URL 清單中刪除反白的 URL。

封鎖下列 URL 類別的存取

此選項一經啟用，會封鎖類別清單中屬於選取的類別的網頁內容。

允許的使用期間

[允許的使用期間]
會開啟對話方塊，供您針對所設定角色指定網際網路使用的時間限制。
您可以選擇依據每週、每月來規範網際網路使用，或在週間日和週末有不同的設定。
進一步對話方塊可讓您規範精確的週間日使用期間。 請參閱使用期間。

要控制的 URL 範例

- `www.avira.com` -或- `www.avira.com/*`
  = 涵蓋帶有網域 `www.avira.com`的所有 URL：*www.avira.com/en/pages/index.php*、 *www.avira.com/en/support/index.html*、 *www.avira.com/en/download/index.html*、 ..
  不包括帶有網域 *www.avira.de* 的 URL。
- `avira.com` -或- `*.avira.com`
  = 涵蓋包含*avira.com*之第二層與頂層網域的所有 URL。 此規定意指 `avira.com` 的所有現有子網域：*www.avira.com*、 *forum.avira.com* 等。
- `avira。` -或- `*.avira*`
  = 涵蓋包含 `avira` 之第二層與頂層網域的所有 URL。 此規定意指 `.avira` 的所有現有頂層網域或子網域：*www.avira.com*、 *www.avira.de*、 *forum.avira.com* 等。
- `.*domain*.*`
  涵蓋包含有字串 `domain` 的所有第二層 URL：*www.domain.com*、 *www.new-domain.de*、 *www.sample-domain1.de* ...
- `net` -或- `*.net`
  = 涵蓋包含 `net`：*www.name1.net*、 *www.name2.net* 等頂層網域的所有 URL。

相關主題：

- 關於 Safe Browsing
- Safe Browsing 組態
- 使用時間長度
- 使用時間

使用時間長度

在 **[使用時間長度]** 視窗中，您可以選擇規範使用者角色的網際網路使用持續時間上限。
In網際網路使用記錄是以至少長達 5 分鐘的網際網路要求為基準。
必要的角色瀏覽時間上限可以依據每週、每月來指定，或在週間日和週末有不同的指定。

使用網際網路的限制時間

此選項可讓您對具有指派角色的所有電腦使用者限制網際網路使用持續時間。
如果已超過許可的使用期間，則會封鎖電腦使用者所要求或存取的網站，
並在網頁瀏覽器上顯示警示。

每週、每月、每日的時間限制 (週一到週五、週六到週日)

必要的使用期間可使用滑桿或輸入方塊右方的方向鍵加以調整。
您也可以直接在時間欄位中輸入使用期間。 請注意時間規格的特定格式。

程式不會將不同的使用期間規格調整成一致的單位。
程式會使用任何時間的最小適用值，以限制使用期間。

精確的使用時間

[精確的使用時間]
按鈕會開啟對話方塊，供您規範已定義使用持續時間上限的當日時間。
請參閱使用時間。

相關主題：

- 關於Safe Browsing
- Safe Browsing 組態
- 角色的屬性

- 使用時間

使用時間

在 **[使用時間]** 視窗中，您可以為選取的角色設定許可的使用時間。
您可以依據每日定義當日網際網路使用的特定時間。

只允許在特定時間使用網際網路

此選項讓您對已指派設定角色的所有電腦使用者設定當日瀏覽時間。
如果使用者試圖在規範的時間外使用網際網路，則會封鎖所要求的網站，
並在網頁瀏覽器上顯示一則訊息。

- 若要指定當日網際網路使用時間，請反白需要的時間欄位。

  您可以利用下列選項來定義允許及禁止的時間間隔：

- **要定義允許的瀏覽時間**：按一下取消反白時間欄位或在取消反白時間欄位上拖曳滑鼠左鍵。
- **要定義禁止的瀏覽時間**：按一下反白的時間欄位或在反白的時間欄位上拖曳滑鼠左鍵。

- 在按日期排列的反白或取消反白的區域上按一下滑鼠右鍵，顯示詳細資料視窗，其中包含週間日的定義間隔。 範例：
  網際網路使用的封鎖從 00:00 到 11:00。

相關主題：

- 關於Safe Browsing
- Safe Browsing 組態
- 角色的屬性
- 使用時間長度

12.9 行動裝置防護功能

12.9.1 行動裝置防護功能

Avira 不僅能保護您的電腦系統免於惡意程式碼與病毒的侵擾，還能保護執行 Android 作業系統的智慧型手機免於遺失及遭竊。 使用 Avira Free Android Security 也可以封鎖有害通話或簡訊。
只需從通話記錄、簡訊記錄和聯絡人清單中新增電話號碼至黑名單，或手動建立要封鎖的聯絡人即可。

如需詳細資訊，請參閱我們的網站：

http://www.avira.com/android

12.10 一般

12.10.1 威脅類別

選取延伸的威脅類別 (僅在專家模式中才能使用選項)

Avira 產品可保護您免受電腦病毒的威脅。
此外，您可以依據下列延伸的威脅類別來進行掃描。

- 廣告軟體
- 廣告軟體/間諜軟體
- 應用程式
- 後門程式用戶端
- 撥號木馬程式
- 雙重副檔名檔案
- 詐騙軟體
- 遊戲
- 惡作劇程式

- 網路釣魚
- 侵犯私人網域的程式
- 少見的執行階段壓縮程式

只要按一下相關方塊，就會啟用 (加上勾選標記) 或停用 (無勾選標記) 選取的類型。

全部選取

此選項一經啟用，就會啟用所有類型。

預設值

此按鈕會還原預先定義的預設值。

> 注意
> 如果停用某個類型，就不會再指出識別為相關程式類型的檔案。
> 報告檔案不會列出任何項目。

12.10.2 進階防護

ProActiv (僅在專家模式中才能使用選項。)

啟用 ProActiv

此選項一經啟用，就會在系統上監視並檢查程式是否有可疑的惡意程式碼動作。
偵測到典型的惡意程式碼行為時，您會收到訊息。
您可以封鎖程式或選擇「**略過**」繼續使用程式。
監視處理序會排除：歸類為信任的程式、許可的應用程式篩選器中預設包含的信任且已簽署的程式，以及您已加入至許可程式的應用程式篩選器中的所有程式。

ProActiv 保護您免於尚無病毒定義或啟發式掃毒的不明新威脅。 ProActiv 技術整合至 Real-Time Protection 元件，會觀察及分析程式所執行的動作。
並根據典型的惡意程式碼動作模式檢查程式的行為：動作類型與動作順序。
如果程式出現典型的惡意程式碼行為，就會被當成偵測到的病毒處理
：您可以選擇封鎖程式或略過通知，然後繼續使用程式。

您可以將程式歸類為信任的程式，並將它加入至許可程式的應用程式篩選器。
您也可以選擇使用 **[永遠封鎖]** 命令，將程式加入至封鎖程式的應用程式篩選器。

ProActiv 元件使用 Avira
惡意程式碼研究中心開發的規則集，來識別惡意程式碼的典型行為。 此規則集由 Avira 資料庫提供。 ProActiv 會將偵測到任何可疑程式的資訊傳送至 Avira 資料庫以供記錄。
在安裝 Avira 期間，您可以選擇停用對 Avira 資料庫的資料傳輸。

> 注意
> ProActiv 技術仍無法用於 64 位元系統！

Protection Cloud (僅在專家模式中才能使用選項。)

啟用 Protection Cloud

所有可疑檔案的指紋都會傳送至 Protection Cloud 進行線上動態檢驗。
可執行檔會立即辨識為無毒、受感染或不明。

Protection Cloud 可作為觀察企圖在我們使用者資料庫中從事網路攻擊的中心位置。
由電腦存取的檔案會比對儲存在雲端中的檔案指紋。
在雲端完成的掃描越多，防毒應用程式所需的處理能力就越少。

當**快速系統掃描**工作執行時，會產生惡意程式碼經常鎖定的檔案位置清單。
此清單包括執行處理序、開機時執行的程式與服務。 產生的各檔案指紋都會傳送至 Protection Cloud，接著會分類為「無毒」或「惡意程式碼」。 不明的程式檔案會上傳至 Protection Cloud 進行分析。

傳送可疑檔案給 Avira 時，以人工方式加以確認

您隨即會看到要傳送至 Protection Cloud
的可疑檔案清單，而您可以選擇要傳送的檔案。

封鎖的應用程式

在 *[要封鎖的應用程式]* 底下，您可以輸入歸類為有害的程式以及 Avira ProActiv 預設會封鎖的應用程式。 加入的應用程式無法在電腦系統上執行。 您也可以經由 Real-Time Protection 可疑程式行為通知，透過選取 **[永遠封鎖此程式]** 選項，將程式加入至封鎖應用程式篩選器。

要封鎖的應用程式

應用程式

此清單包含您經由組態輸入或是經由通知 ProActiv 元件而歸類為有害程式的所有應用程式。 清單上的應用程式遭到 Avira ProActiv 封鎖，無法在電腦系統上執行。 當封鎖的程式啟動時，會出現作業系統訊息。 Avira ProActiv 依據指定的路徑和檔案名稱來識別封鎖的應用程式，封鎖時不考慮內容。

輸入方塊

在此方塊中輸入您要封鎖的應用程式。
必須指定完整路徑、檔案名稱和副檔名來識別應用程式。
路徑必須顯示應用程式所在的磁碟機或以環境變數開頭。

此按鈕會開啟新的視窗，供您選取要封鎖的應用程式。此按鈕會開啟新的視窗，供您選取要封鎖的應用程式。

新增

您可以使用「**新增**」按鈕，將在輸入方塊中指定的應用程式轉移至要封鎖的應用程式清單。

> 注意
> 無法加入作業系統正常運作所需的應用程式。

刪除

「**刪除**」按鈕讓您從要封鎖的應用程式清單中移除反白的應用程式。

允許的應用程式

[要略過的應用程式] 區段列出 ProActiv 元件排除監控的應用程式：根據預設值，已簽署的程式會被分類為信任的應用程式並列入清單中，而所有被分類為信任的應用程式都會新增至應用程式篩選器中：您可以新增許可的應用程式到 [組態] 中的清單。 也可以選擇使用 Real-Time Protection 通知中的 **[信任的程式]** 選項，經由 Real-Time Protection 通知將應用程式加入至可疑程式行為。

要略過的應用程式

應用程式

此清單包含 ProActiv 元件不監視的應用程式。
在預設安裝設定中，此清單包含來自受信任供應商的已簽署應用程式。
您可以選擇在組態或 Real-Time Protection 通知中加入視為受信任的應用程式。
ProActiv 元件使用路徑、檔案名稱和內容來識別應用程式。
建議您檢查程式內容，因為惡意程式碼可透過變更 (例如更新) 加入至程式。
您可以決定是否要從指定的**類型**中執行內容檢查：如果是「*內容*」類型，ProActiv 元件監視作業排除依路徑和檔案名稱指定的應用程式之前，會先檢查檔案內容是否變更。 如果檔案內容已修改，ProActiv 元件會重新監視應用程式。
如果是「*路徑*」類型，Real-Time Protection 監視作業排除應用程式之前，不會執行內容檢查。
若要變更排除類型，請按一下顯示的類型。

警告

請僅在例外情況下才使用 *[路徑]* 類型。
惡意程式碼會透過更新新增至應用程式。
原本無害的應用程式現在已成為惡意程式。

注意

即使不包含在清單中，有些信任的應用程式預設不受 ProActiv 元件監視，例如包括 Avira 產品的所有應用程式元件。

輸入方塊

在此方塊中輸入 ProActiv 元件監視作業要排除的應用程式。
必須指定完整路徑、檔案名稱和副檔名來識別應用程式。
路徑必須顯示應用程式所在的磁碟機或以環境變數開頭。

此按鈕會開啟新的視窗，供您選取要排除的應用程式。

新增

您可以使用「**新增**」按鈕，將在輸入方塊中指定的應用程式轉移至要排除的應用程式清單。

刪除

「**刪除**」按鈕讓您從要排除的應用程式清單中移除反白的應用程式。

12.10.3 密碼

您可以使用密碼，保護 Avira 產品的不同區域。
一旦密碼已經發行，每當您想要開啟保護的區域時，系統就會要求您輸入此密碼。

密碼

輸入密碼

在此輸入要求的密碼。 為了安全起見，您在此輸入的實際字元將以星號 (*) 取代。
密碼長度上限為 20 個字元。 密碼一經發行，程式就會在輸入錯誤的密碼時拒絕存取。
空白方塊代表「無密碼」。

確認

在此再次輸入密碼，以確認以上輸入的密碼。
為了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

> 注意
> 密碼區分大小寫！

由密碼保護的區域 (僅在專家模式中才能使用選項)

您可以使用密碼，保護 Avira 產品的個別區域。
只要按一下相關方塊，就可以視需要針對個別區域停用或重新啟用密碼要求。

受密碼保護的區域	功能
控制中心	此選項一經啟用，便需要預先定義的密碼來啟動控制中心。
啟用/停用 Real-Time Protection	此選項一經啟用，便需要使用預先定義的密碼來啟用或停用 Avira Real-Time Protection。
啟用/停用 Mail Protection	此選項一經啟用，便需要使用預先定義的密碼來啟用或停用 Mail Protection。
啟用/停用 FireWall	此選項一經啟用，便需要使用預先定義的密碼來啟用或停用 FireWall。

啟用/停用 Web Protection	此選項一經啟用，便需要使用預先定義的密碼來啟用或停用 Web Protection。
Safe Browsing啟用/停用	此選項一經啟用，便需要使用預先定義的密碼來啟用或停用家長監護。
隔離區	此選項一經啟用，便會啟用所有可能受到密碼保護的隔離區管理員區域。 只要按一下相關方塊，就可以在要求下再次針對個別區域停用或重新啟用密碼查詢功能。
還原受影響的物件	此選項一經啟用，便需要預先定義的密碼來還原物件。
重新掃描受影響的物件	此選項一經啟用，便需要預先定義的密碼來重新掃描物件。
受影響物件的屬性	此選項一經啟用，便需要預先定義的密碼來顯示物件屬性。
刪除受影響的物件	此選項一經啟用，便需要預先定義的密碼來刪除物件。
傳送電子郵件至 Avira	此選項一經啟用，便需要預先定義的密碼以將物件傳送至 Avira 惡意程式碼研究中心進行檢查。

複製受影響的物件	此選項一經啟用，便需要預先定義的密碼來複製受影響的物件。
新增與修改工作	此選項一經啟用，便需要預先定義的密碼來新增與修改排程管理員中的工作。
組態	此選項一經啟用，就需要先輸入預先定義的密碼才能進行程式的組態
安裝/解除安裝	此選項一經啟用，就需要預先定義的密碼以安裝或解除安裝程式。

12.10.4 資訊安全

僅在專家模式中才能使用選項。

自動執行

封鎖自動執行功能

此選項一經啟用，包括 USB 隨身碟、CD 和 DVD 光碟機以及網路磁碟機在內，所有連線磁碟機的 Windows 自動執行功能執行都會遭到封鎖。 啟用 Windows 自動執行功能時，會在載入或連線時立即讀取資料媒體或網路磁碟機上的檔案，因此會自動啟動及複製檔案。

不過這項功能附帶高度安全風險，因為惡意程式碼和有害程式可能會隨著自動啟動而安裝。 自動執行功能對於 USB 隨身碟尤其重要，因為隨身碟上的資料可能隨時會變更。

排除 CD 和 DVD

此選項一經啟用，CD 和 DVD 光碟機上就允許自動執行功能。

警告

務必只有在確定使用的是信任的資料媒體時，才停用 CD 和 DVD 光碟機的自動執行功能。

系統防護

保護 Windows 主機檔案不被變更

此選項一經啟用，Windows 主機檔案即為防寫狀態。 之後就無法再進行操作。例如，惡意程式碼將無法把您重新導向至有害的網站。 此選項預設為啟用狀態。

產品保護

注意

如果未使用使用者定義的安裝選項安裝 Real-Time Protection，產品保護選項便無法使用。

保護處理序，避免意外終止

此選項一經啟用，會保護所有的程式處理序免於遭到病毒與惡意程式碼的惡意終止，或是避免使用者透過 [工作管理員] 加以「強制」終止。 此選項預設為啟用狀態。

進階處理序保護

此選項一經啟用，所有程式處理序都會受到進階選項保護，避免意外終止。進階處理序保護比簡易處理序保護需要更多電腦資源。 此選項預設為啟用狀態。若要停用此選項，您必須重新啟動電腦。

注意

密碼保護不適用於 Windows XP 64 位元！

警告

如果啟用處理序保護，則其他軟體產品可能會出現互動問題。
在這些情況下，請停用處理序保護。

保護檔案和登錄項目，避免操作

此選項一經啟用，會保護所有程式登錄項目與所有程式檔 (二進位與組態檔)以免於遭到操作。
免於遭到操作代表預防使用者或外部程式寫入、刪除，以及在某些情況下，讀取登錄項目或是程式檔案。 若要啟用此選項，您必須重新啟動電腦。

警告

請注意，此選項一旦停用，修復遭特定類型惡意程式碼感染的電腦就會失敗。

注意

此選項一經啟用，只能對組態進行變更，包括對掃描或更新要求的變更需透過使用者介面進行。

注意

檔案和登錄項目保護不適用於 Windows XP 64 位元！

12.10.5 WMI

僅在專家模式中才能使用選項。

支援 Windows Management Instrumentation

Windows Management Instrumentation 是基本的 Windows 管理技巧，它運用指令碼與程式設計語言同時允許在本機與遠端讀取與寫入 Windows 系統上的設定。 Avira 產品支援 WMI 並透過介面提供相關資料

(狀態資訊、統計資料、報告、預計要求等等)、事件。 WMI
可讓您選擇從程式下載作業資料

啟用 WMI 支援

此選項一經啟用，就可以透過 WMI 從程式下載作業資料。

12.10.6 事件

僅在專家模式中才能使用選項。

限制事件資料庫的大小

限制的大小為上限 n 項

此選項一經啟用，可將事件資料庫中所列的事件數量上限限定為特定大小，可能的值為：100 至 10000 項。 如果輸入的數量超出此限，會從最舊的項目開始刪除。

刪除超過以下天數的所有事件

此選項一經啟用，經過特定期間之後會刪除事件資料庫中所列的事件，可能的值為：1 至 90 天。 系統預設會啟用此選項，並使用 30 天的預設值。

無限制

此選項一經啟用，便不會限制事件資料庫大小。 不過，程式介面的 [事件] 底下最多顯示 20,000 個項目。

12.10.7 報告

僅在專家模式中才能使用選項。

限制報告

限制數目上限為 n 份

此選項一經啟用，可將報告份數上限限定為特定數量。 允許介於 1 到 300 之間的值。如果超出此指定數量，會從最舊的報告開始刪除。

刪除超過 n 天的所有報告

此選項一經啟用，會在經過特定天數後自動刪除報告。 允許的值為：1 到 90 天。系統預設會啟用此選項，並使用 30 天的預設值。

無限制

此選項一經啟用，便不會限制報告份數。

12.10.8 目錄

僅在專家模式中才能使用選項。

暫存檔路徑

使用預設系統設定

此選項一經啟用，會使用系統設定來處理暫存檔案。

> 注意
> 例如使用 Windows XP 時，在：**[開始] > [設定] > [控制台] > [系統] > [索引卡]**「**進階**」按鈕「**環境變數**」底下可以看到系統儲存暫存檔的位置。此處會顯示目前登錄的使用者與系統變數 (TEMP、TMP) 的暫存檔變數 (TEMP、TMP) 及其相關數值。

使用下列目錄

此選項一經啟用，會使用輸入方塊中顯示的路徑。

輸入方塊

在此輸入方塊中，輸入程式儲存其暫存檔的路徑。

...

此按鈕會開啟新的視窗，供您選取必要的暫存檔路徑。

預設值

此按鈕會還原預先定義的暫存檔路徑目錄。

12.10.9 警示音

僅在專家模式中才能使用選項。

當 Scanner 或 Real-Time Protection
偵測到病毒或惡意程式碼，會以互動模式發出警示音。
您現在可以選擇啟用或停用警示音，並選取其他 WAVE 檔做為警示音。

> 注意
> Scanner 的動作模式是在組態的Scanner > 掃描 > 偵測動作 底下進行設定。
> Real-Time Protection 的動作模式是在組態的 Real-Time Protection > 掃描 > 偵測動作 底下進行設定。

無警告

此選項一經啟用，當 Scanner 或 Real-Time Protection
偵測到病毒時，不會發出任何警示音。

使用 PC 喇叭 (僅在互動式模式)

此選項一經啟用，當 Scanner 或 Real-Time Protection
偵測到病毒時，會發出預設的警示音訊號。 警示音會從電腦的內部喇叭發出。

使用下列 WAVE 檔 (僅限互動式模式)

此選項一經啟用，當 Scanner 或 Real-Time Protection
偵測到病毒時，會發出選取的 WAVE 檔警示音。 選取的 WAVE
檔會透過連接的外部喇叭播放。

WAVE 檔

您可以在輸入方塊輸入自選的音訊檔名稱與關聯路徑。
可輸入程式的預設警示訊號作為標準設定。

此按鈕會開啟視窗，讓您透過檔案總管的協助選取所需的檔案。

測試

此按鈕可用來測試選取的 WAVE 檔。

12.10.10 警示

Avira 產品會針對特定事件產生所謂的上滑式訊息桌面通知，提供有關成功或失敗程式序列 (例如更新) 的資訊。 您可以在 **[警示]** 底下啟用或停用特定事件的通知。

利用桌面通知，您可以選擇直接在上滑式訊息停用通知。 您可以在 **[警示]** 組態視窗中重新啟用通知。

更新

如果上次更新是在 n 天之前，則發出警示

在此方塊中，您可以輸入上次更新之後允許經過的天數上限。
經過此天數後，控制中心的 **[狀態]** 底下會顯示更新狀態的紅色圖示。

如果病毒定義檔已非最新狀態，顯示通知

此選項一經啟用，一旦病毒定義檔不是最新的，您就會收到警示訊息。
透過警示選項，您可以設定在上次更新超過 n 天後，要發出的警示時間間隔。

警告 / 注意下列情形

已使用撥號連線

此選項一經啟用，一旦撥號木馬程式在您的電腦上透過電話或 ISDN 網路建立撥號連線時，您就會收到桌面通知警示。
連線可能由不明且有害的撥號木馬程式所建立，而且可能是付費電話。
(請參閱病毒與其他資訊 > 延伸的威脅類別：撥號木馬程式)

檔案已成功更新

此選項一經啟用，只要成功執行更新且更新檔案，您就會收到桌面通知。

更新失敗

此選項一經啟用，只要更新失敗：無法與下載伺服器建立連線或無法安裝更新檔案，您就會收到桌面通知。

沒有必要更新

此選項一經啟用，每當啟動更新之後，卻因為您的程式是最新版本而不需要安裝檔案時，您就會收到桌面通知。