

Avira Free Antivirus

使用手冊

商標與著作權

商標

Windows 是 Microsoft Corporation 在美國與其他國家/地區的註冊商標。
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 Free Antivirus 使用了第三方供應商所提供的代碼。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 Free Antivirus 程式說明中的「第三方授權」。

目錄

1. 簡介.....	7
1.1 圖示與強調樣式.....	7
2. 產品資訊.....	9
2.1 提供的功能	9
2.2 系統需求.....	10
2.3 授權與升級	11
3. 安裝與解除安裝.....	13
3.1 概觀	13
3.1.1 安裝類型	13
3.2 安裝前.....	13
3.3 快速安裝.....	15
3.4 自訂安裝.....	17
3.5 組態精靈.....	18
3.6 變更安裝.....	19
3.7 安裝模組.....	20
3.8 解除安裝.....	20
4. Avira Free Antivirus 概觀	22
4.1 使用者介面與操作方式.....	22
4.1.1 控制中心	22
4.1.2 啟動及關閉控制中心	23
4.1.3 操作控制中心.....	24
4.1.4 控制中心概觀.....	24
4.1.5 組態	25
4.1.6 存取組態	25
4.1.7 組態作業	26
4.1.8 系統匣圖示.....	28
4.1.9 內容功能表中的項目	28

4.2	工具列.....	28
4.2.1	概觀.....	28
4.2.2	使用.....	29
4.2.3	選項.....	30
4.2.4	解除安裝.....	33
4.3	如何...?.....	34
4.3.1	執行自動更新.....	34
4.3.2	啟動手動更新.....	35
4.3.3	使用掃描設定檔來掃描病毒與惡意程式碼.....	36
4.3.4	使用拖放方式掃描病毒與惡意程式碼.....	37
4.3.5	透過內容功能表來掃描病毒與惡意程式碼.....	37
4.3.6	自動掃描病毒與惡意程式碼.....	38
4.3.7	Rootkit 和作用中的惡意程式碼指定掃描.....	39
4.3.8	回應偵測到的病毒與惡意程式碼.....	40
4.3.9	處理隔離區檔案 (*.qua).....	42
4.3.10	還原隔離區的檔案.....	44
4.3.11	將可疑的檔案移至隔離區.....	45
4.3.12	掃描設定檔：修訂或刪除掃描設定檔中的檔案類型.....	46
4.3.13	為掃描設定檔建立桌面捷徑.....	46
4.3.14	篩選事件.....	47
5.	System Scanner.....	48
6.	更新.....	49
7.	常見問題集、秘訣.....	50
7.1	發生問題時的說明.....	50
7.2	快捷鍵.....	52
7.2.1	在對話方塊中.....	52
7.2.2	在說明中.....	53
7.2.3	在控制中心中.....	54
7.3	Windows 資訊安全中心.....	56
7.3.1	一般.....	56
7.3.2	Windows 資訊安全中心和您的 Avira 產品.....	56

8. 病毒與其他資訊	62
8.1 威脅類別	62
8.2 病毒與其他惡意程式碼	65
9. 資訊與服務	69
9.1 連絡地址	69
9.2 技術支援	69
9.3 可疑的檔案	69
9.4 回報誤判	70
10. 參照：組態選項	71
10.1 System Scanner	71
10.1.1 掃描	71
10.1.2 報告	79
10.2 Realtime Protection	80
10.2.1 掃描	80
10.2.2 報告	86
10.3 更新	87
10.3.1 產品更新	87
10.3.2 重新啟動設定	88
10.3.3 網路伺服器	89
10.4 Web Protection	91
10.4.1 掃描	91
10.4.2 報告	97
10.5 一般	98
10.5.1 威脅類別	98
10.5.2 安全性	99
10.5.3 WMI	100
10.5.4 活動	101
10.5.5 報告	101
10.5.6 目錄	102
10.5.7 警示音	102
10.5.8 警示	103

1. 簡介

您的 Avira 產品可保護您的電腦免於各種病毒、蠕蟲、木馬程式、廣告軟體和間諜軟體與其他各種危險的入侵。在本手冊中，這些統稱病毒或惡意程式碼 (有害軟體) 和有害程式。

本手冊說明程式安裝與操作方式。

如需了解更多選項和資訊，請造訪我們的網站：

<http://www.avira.tw/free-av>

您可以在 Avira 網站進行下列作業：

- 存取其他 Avira 桌面程式的相關資訊
- 下載最新版的 Avira 桌面程式
- 下載 PDF 格式的最新產品手冊
- 下載免費的支援和修復工具
- 存取我們的全方位知識庫和常見問題集 (FAQ) 進行疑難排解
- 存取特定國家/地區支援服務地址。

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某項動作，就會放置此圖示。
▶	放置在您執行某項動作步驟的前面。
→	在上一個動作之後發生的事件之前，會放置此圖示。
警告	在針對重要資料可能遺失所提出的警告之前，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之連結前面。
----	--

下列為使用的強調樣式：

強調樣式	說明
<i>斜體</i>	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	可按一下的軟體介面元素 (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](#)

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：

注意

遺失寶貴的資料通常會帶來無法想像的後果。即使是最好的防毒程式也無法 100% 保證免於資料遺失的風險。定期複製 (備份) 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 產品包含下列功能：

- 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
- **System 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。
- **Realtime Protection** (即時掃描) 可持續監視所有檔案存取活動
- **Avira SearchFree Toolbar (powered by Ask.com)** 整合於網頁瀏覽器中的搜尋工具列，可提供快速方便的搜尋選項。
- **Web Protection** (對於 Avira Free Antivirus 使用者，只有在搭配 Avira SearchFree Toolbar 時才能使用此功能) 可監視透過 HTTP 通訊協定從網際網路傳輸的資料與檔案 (監視連接埠 80、8080、3128)

- 可隔離與處理可疑檔案的整合式隔離區管理
- **Rootkits Protection** 可偵測安裝在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
- 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)

2.2 系統需求

下面列出系統需求：

- Pentium 等級或更新的電腦，至少 1 GHz
- 作業系統
 - Windows XP SP2 (32 或 64 位元) 或
 - Windows Vista (32 或 64 位元，SP1) 或
 - Windows 7 (32 或 64 位元)
- 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 Vista、Windows 7 環境下，至少需要 1024 MB 記憶體
- 程式安裝：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 SP3 (32 或 64 位元) 或
 - Windows Vista (32 或 64 位元，建議加裝 SP 1)
 - Windows 7 (32 或 64 位元)
- 網頁瀏覽器

- Windows Internet Explorer 6.0 或更新的版本，或者
- Mozilla Firefox 3.0 或更新版本


注意

若有需要，請先解除安裝任何先前已安裝的搜尋工具列，接著再安裝 Avira SearchFree Toolbar。否則，您將無法安裝 Avira SearchFree Toolbar。

Windows Vista 用戶資訊

在 Windows XP 環境中，許多用戶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。這項功能針對登入為系統管理員的使用者提供多一層的保障：因此在 Windows Vista 中，個別的系統管理員在一開始只具有正常使用者權限。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，用戶必須明確地確認所需的動作。用戶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。

在 Windows Vista 中，某些 Avira 產品動作需要以系統管理員權限來執行。這些動作會以下列符號標示：。如果這項符號同時出現在按鈕上，表示需要以系統管理員權限來執行這項動作。如果您目前的用戶帳戶沒有系統管理員權限，用戶帳戶控制的 Windows Vista 對話方塊會要求您輸入系統管理員密碼。如果您沒有系統管理員密碼，就無法執行這項動作。

2.3 授權與升級

若要使用 Avira 產品，您需要一份授權。請藉此接受授權條款。

授權會以啟用金鑰形式來提供。啟用金鑰是當您購買 Avira 產品之後將收到的一個由字母和數字組成的代碼。啟用金鑰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金鑰，否則會直接附在產品包裝上。

若要授權程式，請輸入啟用金鑰以啟用程式。您可以在安裝期間執行產品啟用程序。不過，您也可以安裝之後，透過授權管理員的說明 > 授權管理來啟用 Avira 產品。

Avira Free Antivirus 中已經包含有效的啟用金鑰。因此，您不需要啟用產品。

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。

為了讓您的系統能擁有高可靠性與安全性，Avira 會傳送快顯項目以提醒您將系統升級至最新版本。只要按一下該快顯項目內的 **[升級]** 連結，就會前往產品的專屬升級網站，從而可移轉至 AV12。

您將可以升級現您慣用的產品，或者取得更全方位的產品。產品概觀頁面會顯示您目前使用的產品種類，並讓您有機會將該產品與其他 Avira 產品進行比較。如需詳細資訊，請按一下產品名稱旁邊的**資訊**圖示。如果您想要使用原來的產品，請按一下 **[升級]**，就會立即開始下載新版本。如果您想要取得更全方位的產品，請按一下產品欄底部的 **[購買]** 按鈕。隨後您將被自動轉往 Avira 線上商店，方便您下單訂購。

注意

依您的產品與作業系統而定，您可能必須具備系統管理員權限才能執行升級。請以系統管理員的身分登入後，再安裝最新版本。

可執行下列產品升級：

- Avira AntiVir Personal 升級為 Avira Free Antivirus。
- Avira AntiVir Personal 升級為 Avira Antivirus Premium 2012。
- Avira AntiVir Premium 升級為 Avira Internet Security 2012。
- Avira AntiVir Premium Security Suite 升級為 Avira Professional Security。

3. 安裝與解除安裝

3.1 概觀

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：[安裝前](#)：需求、備妥電腦以進行安裝
- 請參閱下列章節：[快速安裝](#)：依據預設選項進行標準安裝
- 請參閱下列章節：[自訂安裝](#)：可供設定的安裝方式
- 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

3.1.1 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

- 程式檔案會安裝至 *C:\Program Files* 底下的指定預設資料夾中。
- 您的 Avira 產品會以預設選項進行安裝。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。
- 您可以選擇不要**建立桌面圖示和程式群組** (位於 **[開始]** 功能表中)。
- 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 安裝前

注意

在安裝之前，請檢查您的電腦是否滿足所有的**基本系統需求**。如果您的電腦符合所有需求，就可以安裝 Avira 產品。

注意

在伺服器作業系統上進行安裝時，無法使用 **Realtime Protection** 與檔案保護功能。

安裝前

- ✓ 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** 產品將會搜尋您的電腦上任何可能不相容的軟體。
 - ↳ 若有偵測到可能不相容的軟體，**Avira** 會產生一份這些程式的清單。
 - ↳ 建議您移除這些軟體程式，以免損及電腦的穩定性。
- ▶ 選取應自動從電腦上移除之程式的核取方塊，然後按 **[下一步]**。
- ▶ 您必須手動確認解除安裝部分程式。請選取所需程式，然後按 **[下一步]**。
 - ↳ 選取的一個或多個程式解除安裝後，您的電腦需要重新啟動。一旦重新開機，安裝程序將繼續進行。

警告

在 **Avira** 產品安裝完成之前，您的電腦都將處於未受保護的狀態。

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
 - 註冊成為使用者
 - 完成安裝後，請適當地執行更新
 - ▶ 當您要啟用程式時，請備妥 **Avira** 產品的授權金鑰。

注意

網際網路型態的安裝：

針對程式的網際網路型態安裝提供一項安裝程式，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。

使用安裝套件來安裝：

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

進行註冊時，Avira 產品會使用 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

- **【歡迎使用】** 畫面隨即顯示。
- ▶ 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

預設的安裝方式為快速安裝。這個安裝方式會安裝所有標準元件，有些可能是您未設定的元件。如果您想要執行自訂安裝，請參閱此章節：[安裝 > 自訂安裝](#)。

- ▶ 確認接受**使用者授權合約**與**私人使用合約**。若要閱讀**使用者授權合約**的詳細內容，請按一下 **[EULA]** 連結。
- ▶ 按 **[下一步]**。
 - ↳ **[Web Protection with Avira SearchFree Toolbar (powered by Ask.com)]** 對話方塊隨即顯示。
- ▶ 如果您要安裝 Avira SearchFree Toolbar，請確認接受 **Ask.com** 使用者授權合約，表示您要安裝 Web Protection with the Avira SearchFree Toolbar。

注意

若有需要，請先解除安裝任何先前已安裝的搜尋工具列，接著再安裝 Avira SearchFree Toolbar。否則，您將無法安裝 Avira SearchFree Toolbar。

- ▶ 若有需要，請啟用 **[將 Ask.com 設為瀏覽器的預設搜尋提供者]** 選項。
 - ↳ 安裝進度會以綠色橫條顯示。
- ▶ 按一下 **[完成]** 結束安裝程序並關閉 **[授權精靈]**。
 - ↳ Avira 系統匣圖示隨即出現在工作列中。
 - ↳ 為了確保您的電腦獲得有效防護，**[更新程式]** 模組將會搜尋可用的更新。
 - ↳ **[Luke Filewalker]** 視窗隨即開啟，並執行快速系統掃描。會顯示檢查的狀態與結果。
- ▶ 如果程式在掃描完畢後要求您重新啟動電腦，請按一下 **[是]** 以確保您的系統獲得完整的保護。

安裝成功之後，建議您檢查控制中心的 **[狀態]** 欄位，確認程式已是最新版本。

- ▶ 如果 Avira 產品指出您的電腦不安全，請按一下 **[修正問題]**。
 - ↳ **[還原防護]** 對話方塊隨即開啟。
- ▶ 啟用預設選項以讓您的系統獲得最佳的安全保障。
- ▶ 必要時，請接著執行完整系統掃描。

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

- **[歡迎使用]** 畫面隨即顯示。
- ▶ 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

預設的安裝方式為快速安裝。這個安裝方式會安裝所有標準元件，有些可能是您未設定的元件。如果您想要執行快速安裝，請參閱此章節：[安裝 > 快速安裝](#)。

- ▶ 選擇 **[自訂]** 以安裝個別程式元件。
- ▶ 確認接受**使用者授權合約**與**私人使用合約**。若要閱讀**使用者授權合約**的詳細內容，請按一下 **[EULA]** 連結。
- ▶ 按 **[下一步]**。
 - **[Web Protection with Avira SearchFree Toolbar (powered by Ask.com)]** 對話方塊隨即顯示。
- ▶ 如果您要安裝 **Avira SearchFree Toolbar**，請確認接受**Ask.com** 使用者授權合約，表示您要安裝 **Web Protection with the Avira SearchFree Toolbar**。

注意

若有需要，請先解除安裝任何先前已安裝的搜尋工具列，接著再安裝 **Avira SearchFree Toolbar**。否則，您將無法安裝 **Avira SearchFree Toolbar**。

- ▶ 若有需要，請啟用 **[將 Ask.com 設為瀏覽器的預設搜尋提供者]** 選項，接著按 **[下一步]**。
 - ↳ **[選擇目的地資料夾]** 視窗隨即開啟。
 - ↳ 預設的資料夾將會是 *C:\Program Files\Avira\AntiVir Desktop*
- ▶ 按 **[下一步]** 繼續。
 - 或-
 - 使用 **[瀏覽]** 按鈕選取其他目的地資料夾，並按 **[下一步]** 確認動作。
 - ↳ **[安裝元件]** 對話方塊隨即顯示：
- ▶ 從清單中選取或取消選取元件，然後按 **[下一步]** 確認並繼續。
 - ↳ 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。
- ▶ 按一下 **[完成]** 結束安裝程序。
 - ↳ **[安裝精靈]** 隨即關閉，並開啟**組態精靈**。

3.5 組態精靈

結束使用者定義的安裝後，會開啟組態精靈。組態精靈可讓您定義您的 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 **System Scanner (指定掃描)** 與 **Realtime 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 Realtime Protection 安裝模組，**[Realtime Protection 啟動模式]** 對話方塊會出現。您可以規範 Realtime Protection 啟動時間。每次電腦重新開機時，Realtime Protection 會以指定的啟動模式來啟動。

注意

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

注意

如果選擇了 **Realtime Protection** 的預設啟動模式 (標準啟動)，且登入處理序於開機時會快速執行，則可能不會針對設定為開機時自動啟動的程式進行掃描，因為這些程式在 **Realtime Protection** 完全啟動之前，可能早已運作且執行中。

- ▶ 啟用所需選項，並按 **[下一步]**，繼續進行組態設定。
 - ↳ 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。
- ▶ 如果程式在掃描完畢後要求您重新啟動電腦，請按一下 **[是]** 以確保您的系統獲得完整的保護。

安裝成功之後，建議您檢查**控制中心**中的 **[狀態]** 欄位，確認程式是否為最新版本。

- ▶ 如果 Avira 產品指出您的電腦不安全，請按一下 **[修正問題]**。
 - ↳ **[還原防護]** 對話方塊隨即開啟。
- ▶ 啟用預設選項以讓您的系統獲得最佳的安全保障。
- ▶ 必要時，請接著執行完整系統掃描。

3.6 變更安裝

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

如果您想要新增或移除目前安裝模組，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，並且按一下 **[變更]**。在程式的 **[歡迎使用]** 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。

注意

解除安裝 Avira SearchFree Toolbar 時會同時解除安裝 Web Protection。

3.7 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 Free Antivirus**
此模組包含成功安裝 Avira 產品所需的所有元件。
- **Avira Realtime Protection**
Avira Realtime Protection 會在背景執行。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，不會造成 Avira Realtime Protection 觸發掃描作業。
- **Avira Web Protection**(對於 Avira Free Antivirus 使用者，只有在搭配 Avira SearchFree Toolbar 時才能使用此功能)
上網瀏覽時，您會使用網頁瀏覽器從網路伺服器要求資料。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 Realtime 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。
- **Avira 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。
- **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 [以 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。

3.8 解除安裝

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

若要解除安裝您的 Avira 產品 (例如，在 Windows XP 和 Windows Vista)：

- ▶ 經由 Windows [開始] 功能表，開啟 [控制台]。
- ▶ 按兩下 [程式集] (Windows XP：[軟體])。
- ▶ 選取清單中的 Avira 產品，並按一下 [移除]。

- 系統會詢問您是否確定要移除程式。
- ▶ 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 並不在這份解除安裝清單中，因此必須另外依照上述步驟來解除安裝。若要在 Firefox 中執行這個動作，您必須透過附加元件管理員來啟用 Avira SearchFree Toolbar (這個步驟不適用於 Internet Explorer)。解除安裝之後，此搜尋工具列就不再內嵌於您的網頁瀏覽器中。

注意

解除安裝 Avira SearchFree Toolbar 時會同時解除安裝 Web Protection。

4. Avira Free Antivirus 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：[工具列](#)
- 請參閱下列章節：[如何...?](#)

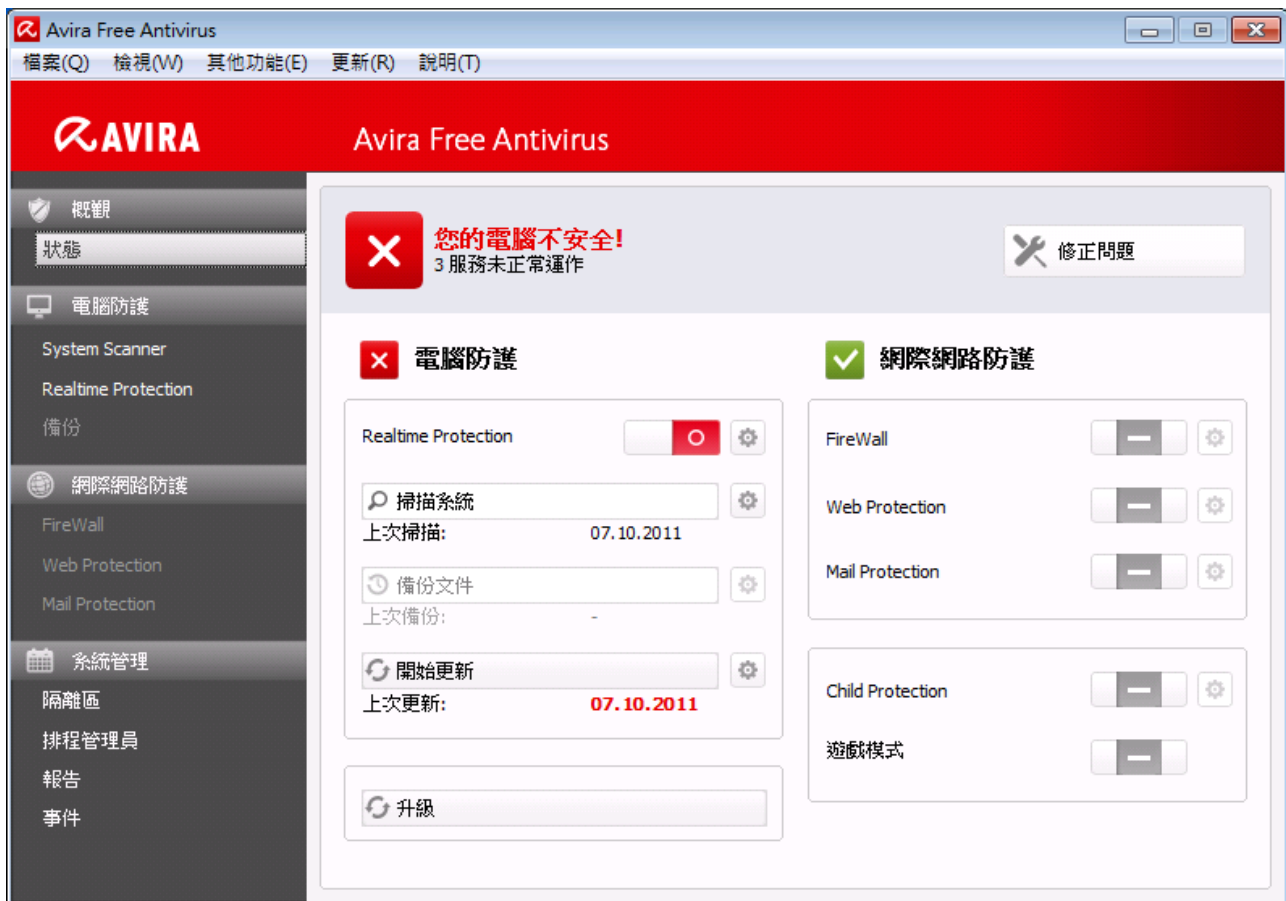
4.1 使用者介面與操作方式

您可以經由三種程式介面元素來操作 Avira 產品：

- [控制中心](#)：監控和控制 Avira 產品
- [組態](#)：設定 Avira 產品
- 工作列的系統匣內的[系統匣圖示](#)：開啟控制中心和其他功能

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。



控制中心視窗分為三個區域：功能表列、瀏覽列與詳細資料視窗狀態：

- **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此程式的相關資訊。
- **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 **[本機保護]-[Realtime Protection]** 區段。
- **狀態**：此視窗會將選取的區段顯示在瀏覽區域中。依據區段而定，您可在詳細資料視窗上方列中，找到可執行各項功能與動作的按鈕。資料或資料物件會顯示在個別區段中的清單裡。您可以按一下方塊來定義清單排序方式，以排序清單。

4.1.2 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]** 功能表中的程式項目。
- 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。

4.1.3 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

您可以藉由 **[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] +** 功能表中含底線的字母或功能表命令。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。

4.1.4 控制中心概觀

- **狀態**：在 **[狀態]** 畫面中，您可以找到所有可用來監視 **Avira** 產品功能的區段。
 - [狀態]** 區段可讓您概要了解哪一個程式模組目前為作用中，並提供最近執行的更新資訊。您還可以藉此了解是否擁有有效的授權。
- **本機保護**：在 **[本機保護]** 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。
 - 掃描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讓您搭配已經調整的標準選項來執行掃描。同理，您也可以依據個人需求並藉由手動選取 (尚未儲存)，來調整病毒與有害程式的掃描方式。
 - Realtime 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。
- **線上保護**：在 **[線上保護]** 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。
 - 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。

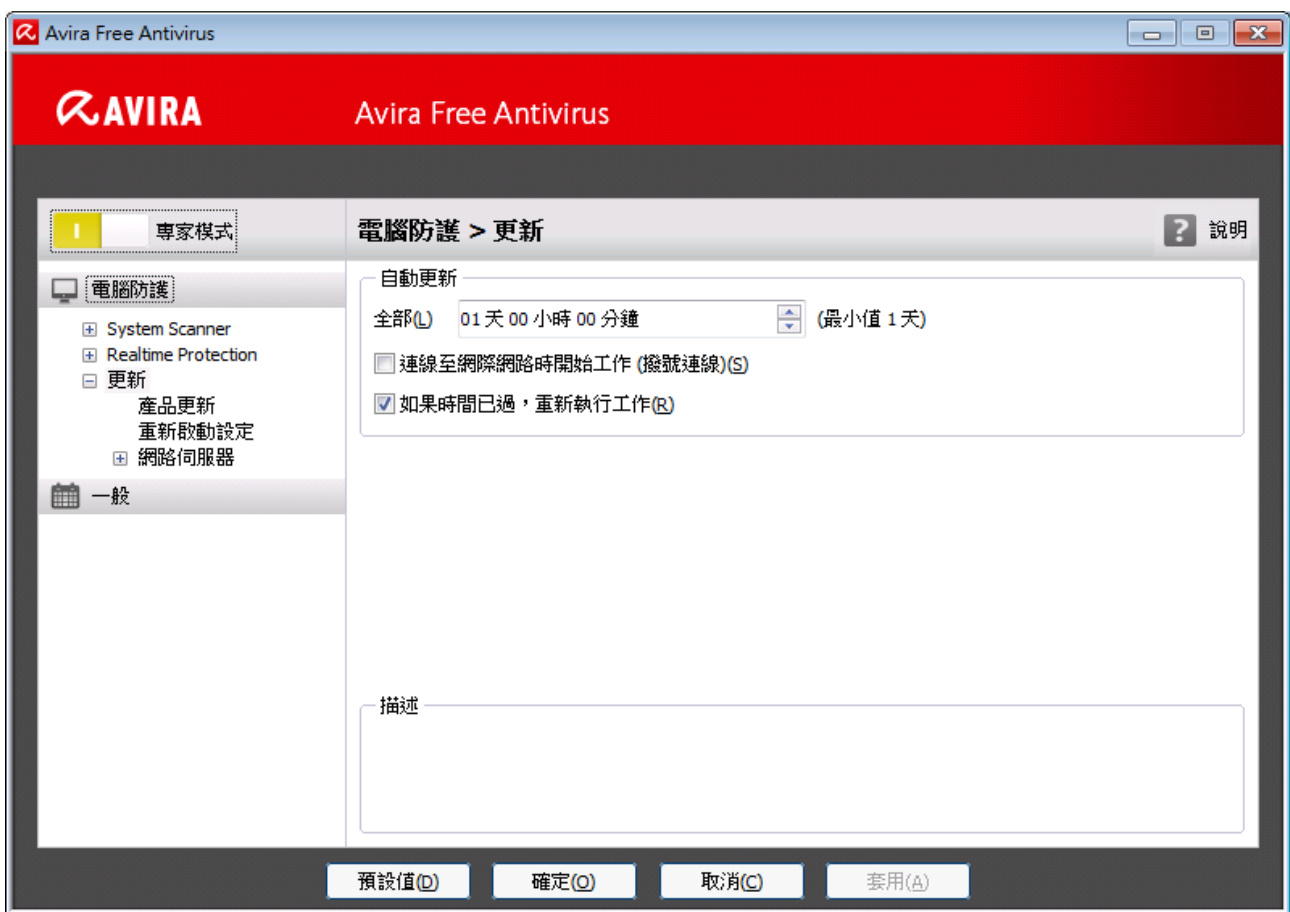
- **管理**：在 **【管理】** 中，您可以找到用以隔離與管理可疑或受感染檔案，以及用以規劃重複性工作的相關工具。

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，並讓您調整或刪除現有工作。

4.1.5 組態

您可以在 **【組態】** 中定義 Avira 產品的設定。安裝完畢後，Avira 產品會採用標準設定進行設定，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。

4.1.6 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 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。您必須啟用 **【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。

4.1.7 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】** + 選項名稱或按鈕描述中含底線的字母。

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 **【接受】**。
 - ↳ 隨即套用所有設定。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 **[還原預設值]**。
- ↳ 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：

- **System Scanner**：指定掃描組態
 - 掃描選項
 - 偵測有所發現時採取的動作
 - 檔案掃描選項
 - 指定掃描例外狀況
 - 指定掃描啟發式掃毒
 - 報告功能設定
- **Realtime Protection**：即時掃描組態
 - 掃描選項
 - 偵測有所發現時採取的動作
 - 即時掃描例外狀況
 - 即時掃描啟發式掃毒
 - 報告功能設定
- **Web Protection**：Web Protection 組態
 - 掃描選項、啟用與停用 Web Protection
 - 偵測有所發現時採取的動作
 - 封鎖存取：已知有害 URL (惡意程式碼、網路釣魚等) 的網路篩選器
 - Web Protection 掃描例外狀況：URL、檔案類型、MIME 類型
 - Web Protection 啟發式掃毒
 - 報告功能設定
- **一般**：
 - 延伸的指定與即時掃描類別
 - 資訊安全：更新狀態顯示、完整的系統掃描狀態顯示、產品保護
 - 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
 - 更新：下載伺服器的連線組態、產品更新的安裝

- 偵測到惡意程式碼時的警示音組態

4.1.8 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 Realtime Protection 已啟用
	Avira Realtime Protection 已停用

系統匣圖示會顯示 **Realtime Protection** 服務狀態。

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**。

4.1.9 內容功能表中的項目

- **啟用 Avira Realtime Protection**：啟用或停用 Avira Realtime Protection。
- **啟用 Avira Web Protection**：啟用或停用 Avira Web Protection。
- **啟動 Avira**：開啟控制中心。
- **設定 Avira**：開啟組態
- **開始更新**：開始更新。
- **說明**：會開啟線上說明。
- **關於 Avira Free Antivirus**：開啟包含 Avira 產品相關資訊的對話方塊：產品資訊、版本資訊、授權資訊。
- **瀏覽 Avira 網站**：開啟網際網路上的 Avira 入口網站。前提是您必須具備有效的網際網路連線。

4.2 工具列

4.2.1 概觀

在成功安裝之後，**Avira SearchFree Toolbar** 會整合到網頁瀏覽器中。當第一次存取瀏覽器時，狀態視窗會開啟，其中包含了工具列功能的重要資訊。

工具列包含了搜尋方塊，連結到 Avira 網站的 Avira 商標，二個狀態顯示，以及 **【選項】** 功能表。

- **搜尋工具列**
使用搜尋工具列，免費使用 Ask.com 搜索引擎，快速搜尋網際網路。
- **狀態顯示**
這些狀態顯示會提供關於 Web Protection 狀態和目前 Avira 產品的更新狀態，該更新狀態可協助您辨識您需要用來保護 PC 的執行動作。
- **選項**
您可以使用這些 **【選項】** 功能表來存取工具列選項、清除歷程記錄，尋找工具列說明和資訊，也可以直接透過網頁瀏覽器 (僅限 Firefox) 來解除安裝 Avira SearchFree Toolbar。

4.2.2 使用

搜尋工具列

您可以使用搜尋工具列，定義要用來瀏覽網際網路的詞彙 (不限數目)。

在搜尋方塊中輸入詞彙，並按下 Enter 鍵，或是按一下 **【搜尋】**。Ask.com 搜尋引擎接著會為您搜尋網際網路，並且在瀏覽器視窗中顯示所有符合項目。

若要了解如何自訂，請移至 **【選項】**，設定 Internet Explorer 和 Firefox 中的 Avira SearchFree Toolbar。

狀態顯示

Web Protection

 *Web Protection 已經啟用。*

Avira Web Protection 已經開啟，且您的 PC 已經受到保護。

 *Web Protection 已經停用。*

Avira Web Protection 已經關閉。請檢查您的應用程式，並啟動 Web Protection，以便提供保護。

更新狀態

包含 Avira 更新狀態資訊的狀態訊息會顯示在右側區域。您可以使用圖示和訊息，找出您應該要採取哪個動作來保護您的 PC。

 *每日更新完成。*

當您將游標滑過圖示上方，畫面中出現下列訊息：*Avira 是最新版本，您的 PC 已受到保護。*

- ▶ 不需要採取進一步動作。

! *更新 Avira。*

當您將游標滑過圖示上方，畫面中出現下列訊息：*Avira 不是最新版本。按一下此處下載最新的更新程式，以便繼續保護您的 PC。*

- ▶ 按一下黃色圖示或文字，更新您的 Avira 產品。此時會根據您在 Avira Free Antivirus 所定義的自訂設定執行更新。
 - ↪ 進行更新期間，您將收到訊息「正在更新...」
 - ↪ 成功完成更新之後，綠色圖示會再度出現，並顯示訊息「每日更新完成」。

? *無法使用 Avira。*

當您將游標滑過圖示上方，畫面中出現下列訊息：*無法使用 Avira。為了確定您的保護功能，請檢查並確定應用程式仍為安裝狀態且正在執行中。*

- ▶ 按一下灰色圖示或文字，移至 Avira 說明頁。您將可在該處找到如何進行下一步動作的指示說明。

4.2.3 選項

Avira SearchFree Toolbar 與 Internet Explorer 和 Firefox 相容，因此這兩種網頁瀏覽器都可以用來設定此工具列：

- [Internet Explorer 組態選項](#)
- [Firefox 組態選項](#)

Internet Explorer

在 Internet Explorer 中，可從 **[選項]** 功能表中使用下列 Avira SearchFree Toolbar 的組態選項：

工具列選項

掃描

Ask 搜尋引擎

在 **[Ask 搜尋引擎]** 功能表中，您可以選取要用來搜尋的搜尋引擎。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、俄國和英國等國家/地區。

開啟搜尋於

在 **【開啟搜尋於】** 選項功能表中，您可以選取將要顯示的搜尋結果：在 **【目前視窗】**、在 **【新視窗】** 或是 **【新索引標籤】** 上。

顯示最近使用過的搜尋

如果 **【顯示最近使用過的搜尋】** 選項已經啟用，您可以在搜尋工具列的文字輸入方塊下顯示之前用過的搜尋詞彙。

當我關閉瀏覽器時自動清除最近使用過的搜尋歷程記錄

如果您不要儲存先前使用過的搜尋，並且希望在關閉網頁瀏覽器時清除歷程記錄，請啟用此選項 **【當我關閉瀏覽器時自動清除最近使用過的搜尋歷程記錄】**。

其他選項

選取其他工具列語言

在 **【選取工具列語言】** 中，您可以選取 **Avira SearchFree Toolbar** 顯示時所使用的語言。這個工具列提供英文、德文、西班牙文、法文、義大利文和葡萄牙文等版本。

注意

在可能情況下，預設的 **Avira SearchFree Toolbar** 語言可相應於程式的語言版本。如果工具列不提供您使用的語言，則以英文為預設語言。

顯示按鈕文字標籤

如果您要隱藏 **Avira SearchFree Toolbar** 圖示旁邊的文字，請停用 **【顯示按鈕文字標籤】** 選項。

清除歷程記錄

如果您不希望儲存先前使用過的搜尋，而且希望立刻清除歷程記錄，請啟用 **【清除歷程記錄】** 選項。

說明

按一下 **【說明】**，存取內容為與工具列相關常見問題集 (FAQ) 的網站。

解除安裝

您也可以直接從 Internet Explorer 解除安裝 **Avira SearchFree Toolbar**：[透過網頁瀏覽器解除安裝](#)

資訊

按一下 **【資訊】**，顯示已安裝的 **Avira SearchFree Toolbar** 版本。

Firefox

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

工具列選項

掃描

選取 Ask 搜尋引擎

在 **[Ask 搜尋引擎]** 功能表中，您可以選取要用來搜尋的搜尋引擎。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、俄國和英國等國家/地區。

顯示最近使用過的搜尋

如果 **[顯示最近使用過的搜尋]** 選項已經啟用，您可以按一下搜尋引擎中的箭頭，顯示之前用過的搜尋詞彙。選取您要再次顯示其搜尋結果的詞彙。

當我關閉瀏覽器時自動清除最近使用過的搜尋歷程記錄

如果您不要儲存先前使用過的搜尋，並且希望在關閉網頁瀏覽器時清除歷程記錄，請啟用此選項 **[當我關閉瀏覽器時自動清除最近使用過的搜尋歷程記錄]**。

當我輸入關鍵字或在瀏覽器位址列中輸入無效的 URL 時顯示 Ask 搜尋結果

如果此選項已經啟用，則每當您輸入關鍵字或在網頁瀏覽位址列中輸入無效的 URL 時，便會啟始搜尋，而且顯示搜尋結果。

其他選項

選取其他工具列語言

在 **[選取工具列語言]** 中，您可以選取 Avira SearchFree Toolbar 顯示時所使用的語言。這個工具列提供英文、德文、西班牙文、法文、義大利文和葡萄牙文等版本。

注意

在可能情況下，預設的 Avira SearchFree Toolbar 語言可相應於程式的語言版本。如果工具列不提供您使用的語言，則以英文為預設語言。

顯示按鈕文字標籤

如果您要隱藏 Avira SearchFree Toolbar 圖示旁邊的文字，請停用 **[顯示按鈕文字標籤]** 選項。

清除歷程記錄

按一下 **[清除歷程記錄]** 可刪除所有先前的 Avira SearchFree Toolbar 搜尋詞彙。

說明

按一下 **[說明]**，存取內容為與工具列相關常見問題集 (FAQ) 的網站。

解除安裝

您也可以直接從 Firefox 解除安裝 Avira SearchFree Toolbar：[透過網頁瀏覽器解除安裝](#)

資訊

按一下 **[資訊]**，顯示已安裝的 Avira SearchFree Toolbar 版本。

4.2.4 解除安裝

若要解除安裝您的 Avira SearchFree Toolbar (例如，在 Windows XP 和 Windows Vista 系統中)：

- ▶ 經由 Windows **[開始]** 功能表，開啟 **[控制台]**。
- ▶ 按兩下 **[程式集]** (Windows XP：軟體)。
- ▶ 選取清單中的 **[Avira SearchFree Toolbar plus Web Protection]** 並按一下 **[移除]**。
 - ↳ 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 隨即解除安裝，而 Avira SearchFree Toolbar plus Web Protection 的所有目錄、檔案和登錄項目都將在電腦重新開機時進行刪除。

透過網頁瀏覽器解除安裝

您也可以選擇直接在瀏覽器中解除安裝 Avira SearchFree Toolbar：

- ▶ 在搜尋工具列中開啟 **[選項]** 功能表。
- ▶ 按一下 **[解除安裝]**。
 - ↳ 如果網頁瀏覽器已開啟，則您將收到要求關閉該瀏覽器的指示。
- ▶ 關閉網頁瀏覽器，並按一下 **[確定]**。
 - ↳ Avira SearchFree Toolbar plus Web Protection 隨即解除安裝，而 Avira SearchFree Toolbar plus Web Protection 的所有目錄、檔案和登錄項目都將在電腦重新開機時進行刪除。

注意

解除安裝 Avira SearchFree Toolbar 時會同時解除安裝 Web Protection。


注意

請注意，若要從 Firefox 解除安裝 Avira SearchFree Toolbar，您必須先在附加元件管理員中啟用此工具列。

4.3 如何...？

4.3.1 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。
- ▶ 賦予工作一個名稱，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]**。
 - ↳ **[工作的時間]** 對話方塊隨即顯示。
- ▶ 選取更新時間：
 - 立即
 - 每天
 - 每週
 - 間隔
 - 一次

注意

我們建議您定期且經常進行更新。建議的更新間隔為：**24 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。
- ▶ 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】**。

→ 新建立的工作會在 **【系統管理】 > 【排程管理員】** 區段的起始頁上顯示為啟用狀態 (勾選標記)。


▶ 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

4.3.2 啟動手動更新

您可以透過各種選項來手動啟動更新：手動啟動更新之後，病毒定義檔與掃描引擎會隨時更新。只有當您已在組態中啟用 **【自動下載並安裝產品更新】** 選項 (於 **電腦防護 > 更新 > 產品更新** 底下)，才可進行產品更新。

若要開始手動更新 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 **【概觀】 > 【狀態】** 區段。

- ▶ 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]** 的 **[更新]** 功能表中，選取 **[開始更新]** 功能表命令。
 - ↳ **[更新程式]** 對話方塊隨即顯示。

注意

我們建議您定期自動進行更新。建議的更新間隔為：**24** 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。

4.3.3 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)。

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 **[電腦防護] > [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]**。
- ▶ 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：
- ▶ 按一下的方塊，反白您要掃描的節點：

4.3.4 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。
- ▶ 使用滑鼠左鍵將反白的檔案拖曳至 **[控制中心]**。
 - ↳ **[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。

4.3.5 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，並開始進行系統掃描。


→ 掃描完成時，會顯示結果。

4.3.6 自動掃描病毒與惡意程式碼

注意

安裝後，會在排程管理員中建立 **[完整系統掃描]** 的掃描工作：完整的系統掃描會依據建議間隔自動執行。

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。
- ▶ 按一下此圖示 。
- **[工作的名稱和描述]** 對話方塊隨即顯示。
- ▶ 賦予工作一個名稱，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]**。
- **[工作的時間]** 對話方塊隨即顯示。
- ▶ 選取掃描時間：
 - 立即
 - 每天
 - 每週
 - 間隔
 - 一次
- ▶ 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 **【工作完成後，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】**。

→ 新建立的工作會在 **【系統管理】 > 【排程管理員】** 區段的起始頁上顯示為啟用狀態 (勾選標記)。


▶ 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

4.3.7 Rootkit 和作用中的惡意程式碼指定掃描

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】 > 【System 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，並開始進行系統掃描。
- 掃描完成時，會顯示結果。

4.3.8 回應偵測到的病毒與惡意程式碼

針對 Avira 產品的個別保護元件，您可以在 **[組態]** 的 **[偵測有所發現時採取的動作]** 區段底下，定義 Avira 產品對偵測到的病毒或有害程式的回應方式。

Realtime Protection 元件沒有可設定的動作選項。偵測到病毒或有害的程式時，您會收到桌面通知。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]** 按鈕將惡意程式碼轉送至 **System Scanner** 元件，執行進一步病毒管理。**System 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 > System Scanner)：

System Scanner 的動作選項：

互動式

在互動式動作模式中，**System 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 **System 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 **System 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。

、**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，您可以從警示中選取受感染物件適用的動作，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

可使用的動作取決於作業系統、負責報告偵測的保護元件 (Avira Realtime Protection、Avira Mail Protection、Avira Web Protection)，以及偵測到的惡意程式碼類型。

System Scanner：

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

此檔案會重新命名為 *.vir 副檔名。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

檔案將會刪除。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

不需要採取進一步動作。受感染的檔案仍會在電腦上繼續運作。

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

Realtime Protection 偵測到狀況時的動作選項：Realtime Protection 未執行其他動作。允許存取檔案。直到電腦重新啟動或該病毒定義檔更新為止，允許對此檔案進行其他存取，並且不會提供任何其他通知。

複製至隔離區

偵測到 Rootkit 時的動作選項：偵測項目會複製至隔離區。

修復開機磁區 | 下載修復工具

偵測到受感染開機磁區時的動作選項：可使用一些修復受感染磁碟機的選項。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。

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。

4.3.9 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 **[重新掃描統計資料]** 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 。
- ▶ 您必須按 **[是]** 確認您的選擇。

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 。
- 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。
- ▶ 選取類型：**[可疑的檔案]** 或 **[懷疑可能為誤判]**。
- ▶ 選取回覆格式：**[HTML]**、**[文字]** 或 **[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，建議交由 Avira 惡意程式碼研究中心進行分析：

啟發式掃毒目標 (可疑的檔案)： 在掃描期間，某一檔案經由 Avira 產品歸類為可疑，並移至隔離區；病毒偵測對話方塊或是掃描產生的報告檔案已建議將檔案交由 Avira 惡意程式碼研究中心進行分析。


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。

如果您要將隔離區物件的屬性匯出在文字檔中：



- ▶ 反白隔離區物件，然後按一下 。
- ↳ **[隔離區 - 記事本]** 文字檔隨即開啟，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](#))。

4.3.10 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 與 Windows 2000：

-  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


電子郵件與其附件如果要進行還原，只能透過此選項  (如果檔案副檔名為 *.eml)。

若要將檔案還原至原始位置：

- ▶ 反白檔案，然後按一下圖示 (Windows 2000/XP :  、 Windows Vista )。


電子郵件不適用此選項。

注意

電子郵件與其附件如果要進行還原，只能透過此選項  (如果檔案副檔名為 *.eml)。


- ↳ 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]**。
 - ↳ Windows 預設的 **[另存新檔]** 視窗隨即顯示，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。

4.3.11 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 。
- ↳ 會顯示 Windows 預設視窗供您選取檔案。
- ▶ 選取檔案後按一下 **[開啟]** 以進行確認。

→ 這時檔案已移至隔離區。

您可以使用 **Avira System Scanner** 來掃描隔離區的檔案 (請參閱下列章節：[隔離區：處理隔離區檔案 \(*.qua\)](#))。

4.3.12 掃描設定檔：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)：

- ✓ 在 [控制中心]，移至 **[電腦防護] > [System 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：


- ▶ 反白任一檔案類型。
- ▶ 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 ?)。

4.3.13 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]，移至 **[電腦防護] > [System Scanner]** 區段。
- ▶ 選取您要建立捷徑的掃描設定檔。
- ▶ 按一下此圖示 。
 - 立即建立桌面捷徑。

4.3.14 篩選事件

Avira 產品的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】** 底下 (類似於您的 Windows 作業系統的事件顯示)。這些程式元件如下 (依字母順序列出)：

- 協助程式服務
- Realtime Protection
- 排程管理員
- System 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。

5. System Scanner

有了 System 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：

- **經由內容功能表進行系統掃描**

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。

- **經由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，System Scanner 會掃描該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。

- **經由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。請參閱經由設定檔進行系統掃描。

- **經由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。請參閱經由排程管理員進行系統掃描。

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 和作用中的惡意程式碼]** 掃描 Rootkit
- 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。為了執行定期更新，我們已將更新程式元件整合在 **Avira** 產品中。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：
 - 掃描引擎內含 **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。

更新會檢查病毒定義檔與掃描引擎是否為最新，必要時還會實作更新。依據組態設定，更新程式還會執行產品更新，或是通知您可用的產品更新。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。

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。

更新程式會在下列間隔自動執行：24 小時。您可以透過組態編輯或停用自動更新 ([組態 > 更新](#))。

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：在 **[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]** 的 **一般 > 更新** 底下變更這項預設設定。

7. 常見問題集、秘訣

本章包含有關使用 Avira 產品時的疑難排解與其他秘訣的重要資訊。

- 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](#)

7.1 發生問題時的說明

您可在這裡找到原因相關資訊與各種疑難雜症的解決方案。

- 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。
- 防火牆在啟動之後，立即回報 [Avira Realtime Protection](#)。
- 網路聊天無法運作：聊天訊息無法顯示

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。無法順利建立可連接至網際網路 Web 伺服器的連線。

- ▶ 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。如果不行的話，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：

- ▶ 檢查位在 [一般 > 更新](#) 底下 [組態] (專家模式) 中的您的設定。

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。

- ▶ 更新您的 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 產品與 [組態] (專家模式)。
- ▶ 選取 **System Scanner > 掃描 > 檔案 > 所有檔案**，並於視窗中選取 **[確定]** 以確認。
- ▶ 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 Realtime Protection 已經停用。

- ▶ 在 Avira Realtime Protection 區域底下狀態區段中的控制中心，按一下 **[啟用]** 按鈕。

原因：Avira Realtime Protection 已遭防火牆封鎖。

- ▶ 在防火牆的組態中，定義 Avira Realtime Protection 的一般核准設定。Avira Realtime Protection 僅能在 127.0.0.1 (localhost) 位址上運作。不會建立網際網路連線。

或是：

- ▶ 檢查 Avira Realtime Protection 服務的啟動類型。必要時，請啟用該服務：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 2000 與 Windows XP 環境下，服務 Applet 位於 **[系統管理工具]** 子目錄中)。找到 **[Avira Realtime 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：Avira Realtime Protection 會在備份程序期間掃描備份程序所使用的所有檔案。

- ▶ 選取 [組態] (專家模式) 中的 **Realtime Protection > 掃描 > 例外狀況**，並輸入備份軟體的處理序名稱。

防火牆在啟動之後，立即回報 Avira Realtime Protection

原因：您可以透過 TCP/IP 網際網路通訊協定，與 Avira Realtime Protection 通訊。防火牆可透過此通訊協定監視所有連線。

- ▶ 定義 Avira Realtime Protection 的一般核准設定。Avira Realtime Protection 僅能在 127.0.0.1 (localhost) 位址上運作。不會建立網際網路連線。

注意

建議您定期安裝 Microsoft 更新來修補任何安全漏洞。

網路聊天無法運作：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 組態輸入為例外狀況 (請參閱組態中的 [Web Protection > 例外狀況](#))。

7.2 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。

以下簡介您可用的鍵盤命令。請在對應的說明章節中，找到各項功能的相關介紹。

7.2.1 在對話方塊中

快捷鍵	說明
Ctrl + Tab Ctrl + Page down	控制中心的瀏覽 移至下一節。
Ctrl + Shift + Tab Ctrl + Page up	控制中心的瀏覽 移至上一節。
← ↑ → ↓	組態區段的瀏覽 首先，使用滑鼠將焦點放在組態區段。
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。
← ↑ → ↓	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。
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 + 含底線的字母	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。

7.2.2 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。

7.2.3 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
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

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

7.3 Windows 資訊安全中心

- Windows XP Service Pack 2 或更新版本 -

7.3.1 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。

7.3.2 Windows 資訊安全中心和您的 Avira 產品

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

請在電腦上安裝您的 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 後再安裝您的 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 資訊安全中心將 Avira 產品識別為最新狀態，請在安裝後執行更新。請執行更新來更新系統。

防毒保護已開啟

在安裝了 Avira 產品與後續更新之後，您將會收到下列訊息：



您的 Avira 產品現在已是最新的，並已啟用 Avira Realtime Protection。

防毒保護已關閉

當您停用 Avira Realtime Protection 或是停止 Realtime Protection 服務時，會收到下列訊息。



注意

您可以從控制中心的概觀 > 狀態區段中，啟用或停用 **Avira Realtime 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 Realtime 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

您的 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 XP Service Pack 2 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！

8. 病毒與其他資訊

8.1 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 產品可偵測廣告軟體。**[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 產品可辨識「廣告軟體/間諜軟體」。**[廣告軟體/間諜軟體]** 選項一經啟用 (於組態中**威脅類別**底下勾選)，您會在 Avira 產品偵測到廣告軟體或間諜軟體時收到對應的警示。

應用程式

APPL (與應用程式相關) 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 產品可辨識「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 產品偵測到這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 產品可辨識「後門控制軟體」。**[後門控制軟體]** 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)。

您的 Avira 產品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 (於組態中一旦在組態的**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 產品可辨識「雙重副檔名檔案」。**[雙重副檔名檔案]** 選項一經啟用 (於組態中一旦在組態的**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

詐騙軟體亦稱為「恫嚇軟體」或「流氓軟體」，會謊報您的電腦已遭受病毒或惡意程式碼感染。這類軟體看起來就像專業防毒軟體，但其意圖是要令人不安或嚇唬使用者。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 產品可偵測恫嚇軟體。**[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。電子郵件遊戲也開始越來越盛行：為數眾多的變種遊戲開始流通，從簡單的西洋棋到艦隊遊戲等 (包括水雷對戰) 不一而足：夥伴則是經由電子郵件程式來回應合作夥伴對應的行動。

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 產品可辨識電腦遊戲。**[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

惡作劇程式單純地只是想要嚇嚇某人，或是博君一笑，沒有任何惡意。惡作劇程式一經載入，電腦通常會在某個運作時間點播放一段音樂或是在螢幕上顯示一些奇怪的畫面。諸如磁碟機中的洗衣機 (DRAIN.COM) 或是會吃掉畫面的怪物 (BUGSRES.COM) 等，都是惡作劇程式的例子。

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 產品可辨識「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 產品可偵測「安全性隱私風險」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 產品此類軟體時收到對應的警示。

少見的執行階段壓縮程式

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 產品可辨識「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。

8.2 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

後門程式會藉由繞過電腦存取安全機制來取得電腦的存取權。

在背景執行的某個程式會開啟方便之門，賦予攻擊者無限的權限。使用者的個人資料可能會遭後門程式竊取。而且主要是被用來在相關系統上植入更多的電腦病毒和蠕蟲。

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。出現的怪異行為之一為：電腦系統從此無法載入...

殭屍網路

定義為遠端 (網際網路上) 電腦網路的殭屍網路，包含許多可互相通訊的殭屍病毒。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)。殭屍網路有多重目的，包括阻斷服務攻擊等等，通常會在電腦使用者不知情的情況下執行。殭屍網路最可怕的地方在於其規模可達到成千上萬台電腦，流量總和甚至會超過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

詐騙軟體亦稱為「恫嚇軟體」或「流氓軟體」，會謊報您的電腦已遭受病毒或惡意程式碼感染。這類軟體看起來就像專業防毒軟體，但其意圖是要令人不安或嚇唬使用者。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

誘捕機制是安裝在網路上的一種服務 (程式或伺服器)。它的功能在於監控網路和記錄攻擊事件。合法的使用者不會知道這項服務，正因為如此，也就沒人去注意到相關問題。如果攻擊者探查網路上的弱點並利用誘捕機制所提供的服務，就會加以記錄並觸發警示。

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，就是讓自己隱形起來。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很常見。特洛伊木馬程式包括會假裝具有特殊功能，但是在執行之後便顯露出真面目，而且在大多數情況下會執行具有毀滅性的功能。特洛伊木馬程式無法自我分裂繁殖，這點與其他病毒和蠕蟲不同。這類程式大部分都有一個有趣的名稱 (SEX.EXE 或

STARTME.EXE)，用意就是引起使用者注意，進而啟動特洛伊木馬程式。這類程式一經執行，馬上會開始活躍，並可能開始大肆破壞，例如將硬碟格式化。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。

9. 資訊與服務

本章包含我們的連絡資訊。

- 請參閱下列章節：[連絡地址](#)
- 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](#)

9.1 連絡地址

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。請從控制中心的 **[說明]** > **[關於 Avira Free Antivirus]** 底下找到我們的連絡地址。

9.2 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/personal-support>

以便我們快速處理並提供您值得信賴的協助。請您備妥下列資訊：

- **版本資訊**。您可以在 **[說明]** > **[關於 Avira Free Antivirus]** > **[版本資訊]** 功能表項目底下找到程式介面。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**。

9.3 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) 中，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。

- 將所需的檔案壓縮成 WinZIP、PKZip、Arj 之類的格式，並以電子郵件附件方式寄至下列地址：
virus-personal@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)。

9.4 回報誤判

如果您認為 Avira 產品回報的檔案極有可能是「沒問題」，請將所需的檔案壓縮起來 (WinZIP、PKZip、Arj 等格式) 並以電子郵件附件方式寄至下列地址：

virus-personal@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)。

10.參照：組態選項

組態參照會記錄所有的可用組態選項。

10.1 System Scanner

組態的 **[System Scanner]** 區段負責指定掃描的組態。(選項僅適用於專家模式。)

10.1.1 掃描

您可以定義指定掃描常式的行為 (選項僅適用於專家模式)。如果您選取了要掃描的特定目錄，依據組態而定，**System 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

System 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**選項，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，此程式會自動選擇要掃描病毒或有害程式的檔案。這表示您的 **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選項一經啟用，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，會開啟一個對話方塊並顯示所有於 **【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，**System Scanner** 會針對選取的系統掃描磁碟機掃描其中的開機磁區。此選項會啟用為預設值。

掃描主開機磁區

此選項一經啟用，**System 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。此選項會啟用為預設值。

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。使用此選項。

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，**System 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

此選項僅適用於多處理器系統。

追蹤符號連結

此選項一經啟用，**System 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 **System 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**，但是執行效能卻快上許多。

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。

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！此選項會啟用為預設值。

掃描程式優先順序

透過指定掃描，**System 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 **System Scanner**，亦即，當作業系統中只執行 **System Scanner** 時，將保持全速運作。總之，這時使用其他程式將可獲得最佳效率：當 **System 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

System 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

System 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，**System Scanner** 會全速完成掃描。

偵測有所發現時採取的動作

您可以定義當偵測到病毒或有害程式時，**System Scanner** 要執行的動作。(選項僅適用於專家模式。)

互動式

此選項一經啟用，會在對話方塊中顯示 **System Scanner** 掃描的結果。使用 **System 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 **System Scanner**。

注意

在 **System 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，偵測到病毒時將不會出現任何對話方塊。System Scanner 會根據您在這個區段中預先定義為主要和次要動作的設定來反應。

執行動作前先將檔案複製至隔離區

此選項一經啟用，System 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 System Scanner 發現病毒或有害程式時優先執行的動作。如果選取了 **【修復】** 選項，但卻無法修復受影響的檔案，便會執行在 **【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在 **【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，System Scanner 會自動修復受影響的檔案。如果 System 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 System Scanner 將修改工作站上的檔案。

重新命名

此選項一經啟用，System 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，System 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。

略過

此選項一經啟用，可允許存取檔案，並保留檔案原貌不動。

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！

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，**System 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，**System 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。

略過

此選項一經啟用，可允許存取檔案，並保留檔案原貌不動。

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！

注意

若您已選取 **[刪除]** 或做為主要或次要動作，請注意下列事項：當啟發式掃毒模式偵測到病毒時，並不會刪除受影響的檔案，而是將之移至隔離區。

封存

掃描封存時，**System Scanner** 會使用遞迴掃描：封存在內的封存在經過解壓縮之後，會掃描其中是否有病毒與有害程式。按鈕來終止病毒或有害程式的掃描。(選項僅適用於專家模式。)

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，**System Scanner** 還是會偵測檔案是否為壓縮檔案格式 (封存)，並加以掃描。不過，為此每個檔案必須開啟，而這點會使掃描速度變慢。例如：如果 *.zip 封存含有 *.xyz 的副檔名，則 **System 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，**System 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 **System Scanner** 應該掃描的封存。為此，您必須選取相關項目。

例外狀況

*要讓 **System Scanner** 略過的檔案物件 (選項僅適用於專家模式)。*

此視窗中的清單包含當 **System 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狀況項目，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

清單中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。

注意

如果您將完整的磁碟分割新增到檔案物件清單，只有直接儲存在磁碟分割底下的檔案不用接受掃描，但此規則不適用位於對應磁碟分割上子目錄中的檔案：
例如：要略過的檔案物件：D:\ = D:\file.txt 將排除在 **System Scanner** 的掃描範圍外，而 D:\folder\file.txt 不會排除在掃描範圍外。

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。(選項僅適用於專家模式。)

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，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 產品內含威力非常強大的巨集病毒啟發式掃毒工具。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，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

中偵測等級

如果您已選取使用此啟發式掃毒技術，這將會是預設選項。

高偵測等級

此選項一經啟用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

10.1.2 報告

System 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。(選項僅適用於專家模式。)

注意

為確認在偵測到病毒或有害程式時，System Scanner 已執行的相關動作，應該在專家模式組態下啟用報告檔。

報告功能

關閉

此選項一經啟用，**System Scanner** 就不會報告指定掃描的動作與結果。

預設值

此選項一經啟用，**System Scanner** 會記錄相關檔案名稱與其路徑。此外，目前的掃描組態、版本資訊與被授權人的資訊，全都寫入報告檔中。

延伸

此選項一經啟用，除了預設資訊以外，**System Scanner** 還會記錄警示與秘訣。

完整

此選項一經啟用，**System 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。

10.2 Realtime Protection

組態的 **[Realtime Protection]** 區段負責即時掃描的組態。(選項僅適用於專家模式。)

10.2.1 掃描

通常您會想要持續監視系統。為達到這個目的，請使用 **Realtime Protection (= 即時 System Scanner)**。這樣您就可以針對病毒與有害程式，即時掃描電腦上所有複製或開啟的檔案。(選項僅適用於專家模式。)

檔案

Realtime Protection 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。

注意

一旦啟用**所有檔案**選項，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，此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

一旦啟用[使用智慧副檔名辨識](#)選項，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。系統不只預設啟用此選項，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，會開啟一個對話方塊並顯示所有於 **[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，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，**Realtime 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，**Realtime 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，**Realtime 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。系統不只預設啟用此選項，也建議使用這個選項。

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，**Realtime Protection** 會使用遞迴掃描：封存在內的封存在經過解壓縮之後，會掃描其中是否有病毒與有害程式。您可以定義遞迴深度。預設與建議的遞迴深度為 1 層：直接位於主封存的所有檔案會經過掃描程序。

檔案數上限

掃描封存時，可以限制封存在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。

偵測有所發現時採取的動作

使用事件記錄

此選項一經啟用，每次偵測到病毒時，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。此選項會啟用為預設值。(選項僅適用於專家模式。)

例外狀況

透過這些選項，您可以設定 **Realtime Protection** (即時掃描) 的例外狀況物件。這時進行即時掃描時就不會包含相關物件。**Realtime Protection** 可以透過要略過的處理序清單，在即時掃描期間忽略這些物件的檔案存取行為。例如，使用資料庫或備份解決方案時，這種作法最有用。(選項僅適用於專家模式。)

請在指定要略過的處理序和檔案物件時注意下列事項：此清單將由上而下進行處理。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。

要讓 *Realtime Protection* 略過的處理序

此清單中處理序的所有檔案存取行為，全都不會受到 **Realtime 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。清單中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，您可以輸入名稱中包含特殊符號的處理序或目錄。

磁碟機資訊必須採用下列格式輸入： [磁碟機代號]:\

磁碟機時只能用冒號 (:) 來指定。

當指定處理序時，您可以使用萬用字元 * (任何字元數目) 和 ? (單一個字元)。

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

為了避免處理序遭全域性排除而不受 **Realtime Protection** 監視，包括下列字元的指定將排除為無效：* (星號)、? (問號)、/ (斜線)、\ (反斜線)、. (點)、:(冒號)。

您可以選擇不提供完整路徑詳細資料來設定排除 **Realtime Protection** 監視的處理序。例如：application.exe

不過這種作法僅適用於可執行檔位於硬碟的處理序。

請勿針對可執行檔位在動態磁碟機上的處理序指定任何例外狀況。動態磁碟機可指定為卸除式磁碟，例如 **CD**、**DVD** 或 **USB** 隨身碟等。

警告

請注意，所有由清單中記錄之處理序存取的檔案，全部都會從病毒與有害程式的掃描作業中排除！無法排除 **[Windows 檔案總管]** 與作業系統本身。會忽略清單中對應的項目。



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。

要讓 *Realtime Protection* 略過的檔案物件

對此清單所列檔案物件的存取，全都不會受到 **Realtime 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。

當指定要略過的檔案物件時，您可以使用萬用字元 * (任何字元數目) 和 ?? (單一個字元)：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 (\) 結尾，否則會假定為檔案名稱。

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 個例外狀況。例如：

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

不含完整路徑的例外狀況上限為 64。例如：

```
*.log
```

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

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

如果您使用裝載點 (例如，C:\DynDrive)，還是會掃描動態磁碟。您可以從 **Realtime 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。

請在指定例外狀況時注意下列更多事項：

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\application*.exe\  
此項目無效，且不會被視為例外狀況！
```

您可以在 **Realtime Protection** 報告檔中找到 **Realtime Protection** 用來掃描受感染檔案的路徑。請在例外狀況清單中清楚指出相同的路徑。請如以下所示進行：將 **Realtime Protection** 的通訊協定功能設為 **[完整]** (於組態的 [Realtime Protection > 報告](#))。接著在 **Realtime Protection** 已啟用的狀態下，存取檔案、資料夾、裝載的磁碟機。現在您可以從 **Realtime Protection** 報告檔中讀取要使用的路徑。報告檔案存取路徑為控制中心的本機保護 > **Realtime Protection**。

啟發式掃毒

此組態區段包含掃描引擎的啟發式掃毒設定。(選項僅適用於專家模式。)

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，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** 產品內含威力非常強大的巨集病毒啟發式掃毒工具。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，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

中偵測等級

如果您已選取使用此啟發式掃毒技術，這將會是預設選項。

高偵測等級

此選項一經啟用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

10.2.2 報告

Realtime 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。(選項僅適用於專家模式。)

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，**Realtime 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，**Realtime 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。此選項會啟用為預設值。

延伸

此選項一經啟用，**Realtime 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，**Realtime 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

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

如果您尚未指定任何報告檔限制，當此報告檔達到 100MB 時，新的報告檔會自動建立。舊報告的備份隨即建立。最多可儲存 3 個舊報告檔案的備份。最舊的備份會最先遭到刪除。

10.3 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

所有 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。

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。(選項僅適用於專家模式。)

10.3.1 產品更新

在 **[產品更新]** 底下，設定產品更新或可用產品更新通知的處理方式。(選項僅適用於專家模式。)

產品更新

自動下載並安裝產品更新

此選項一經啟用，一旦有可用的更新，更新程式元件就會立即下載產品更新並自動安裝。不管此設定為何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。

下載產品更新。如果需要重新啟動，請在系統重新啟動之後再安裝更新，否則請立即安裝更新

此選項一經啟用，一旦有可用的新產品更新時，就會下載產品更新。如果不需要重新啟動，下載更新檔案後就會自動安裝這項更新。如果產品更新要求重新啟動電腦，下次使用者控制的系統重新開機時才會執行重新啟動，而不是在下載更新檔案後立即執行。其優點是，當使用者在電腦工作時不會執行重新啟動。不管此設定為何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。

可取得產品更新時，通知使用者

此選項一經啟用，一旦有可用的新產品更新時，您就會收到電子郵件通知。不管此設定為何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。您可以透過桌面快顯視窗與更新程式的警示 (於控制中心的 **[概觀]** > **[事件]** 底下)，接收通知。

在 n 天數後，再通知一次

如果未在初始通知後安裝產品更新，請在此方塊中輸入在經過幾天後再次通知您可取得產品更新。

[不要下載產品更新]

此選項一經啟用，便無法執行自動產品更新或是由更新程式發出可用產品更新通知。不管此設定為何，您都可以獨立進行病毒定義檔與搜尋引擎的更新。

警告

不管產品更新設定為何，您都可以在每次更新處理序期間執行病毒定義檔與搜尋引擎的更新 (請參閱 [更新](#) 一章裡的說明)。

注意

如果您已經啟用自動產品更新選項，可以在 [重新啟動設定](#) 底下設定其他重新啟動通知和取消選項。(選項僅適用於專家模式。)

10.3.2 重新啟動設定

由 Avira 產品執行產品更新時，您可能必須重新啟動電腦系統。如果您已經選取 [本機保護 > 更新 > 產品更新](#) 底下的自動產品更新，可以在 **[重新啟動設定]** 底下選擇不同的重新啟動通知和重新啟動取消選項。(選項僅適用於專家模式。)

注意

請注意，重新啟動設定可讓您在組態的 [本機保護 > 更新 > 產品更新](#) 底下，有關執

行產品更新需要電腦重新啟動的兩個選項擇其一。

自動下載並安裝產品更新：當使用者在電腦工作，同時會執行更新和重新啟動。如果您已啟用此選項，最好選取有取消選項或提醒功能的重新啟動常式。

下載產品更新。如果需要重新啟動，請在系統重新啟動之後再安裝更新，否則請立即安裝更新：在使用者啟動電腦及登入之後，執行更新和重新啟動。建議對這個選項使用自動重新啟動常式。

在以下秒數後重新啟動電腦 (顯示倒數計時訊息，無法取消)

此選項一經啟用，執行產品更新之後，就會在指定間隔**自動**執行必要的重新啟動。這時會出現倒數計時訊息，其中沒有取消電腦重新啟動的選項。

定期重新啟動提醒

此選項一經啟用，執行產品更新之後，**不會**自動執行必要的重新啟動。在指定間隔，您會收到沒有取消選項的重新啟動通知。這些通知可讓您確認電腦重新啟動或選取 **[再次提醒我]** 選項。

詢問是否要重新啟動電腦

此選項一經啟用，執行產品更新之後，**不會**自動執行必要的重新啟動。您將只會收到一則訊息，提供您選擇直接執行重新啟動或取消重新啟動常式。

不需詢問，直接重新啟動電腦

此選項一經啟用，執行產品更新之後，就會**自動**執行必要的重新啟動。您不會收到任何通知。

10.3.3 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 (選項僅適用於專家模式)。

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

目前不提供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

Vista 及 Windows 7 環境下無法使用此選項。在這些作業系統下，為更新作業開啟的撥號連線一律在順利完成下載之後立即終止。

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 伺服器建立對網路伺服器的連線。

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。設定 Windows 系統設定值，以便根據 **[控制台] > [網際網路選項] > [連線] > [區域網路 (LAN) 設定]** 區段來使用 Proxy 伺服器。您也可以使用 Internet Explorer，在 **[其他功能]** 功能表中存取 **[網際網路]** 選項。

警告

如果您要使用必須進行驗證的 Proxy 伺服器，則請在選項 **[使用此 Proxy 伺服器]** 下方輸入所有必要的資料。選項 **[使用 Proxy 系統設定]** 只能用於不用驗證的 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。

地址

請輸入您在連線至網路伺服器時要使用的 Proxy 伺服器之電腦名稱或 IP 位址。

連接埠

請輸入您在連線至網路伺服器時要使用之 Proxy 伺服器的連接埠編號。

登入名稱

請輸入使用者名稱來登入 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：

地址：proxy.domain.com 連接埠：8080

地址：192.168.1.100 連接埠：3128

10.4 Web Protection

[組態] > [線上保護] 底下的 **[Web Protection]** 區段負責 Web Protection 的組態。

10.4.1 掃描

Web Protection 可針對各種透過網際網路載入網頁瀏覽器的網頁，防範藉此抵達您電腦的病毒或惡意程式碼。**[掃描]** 選項可用來設定 Web Protection 元件的行為。(選項僅適用於專家模式。)

掃描

啟用 IPv6 支援

此選項一經啟用，Web Protection 即支援網際網路通訊協定版本 6。

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-frames]** 選項可讓您檢查與封鎖載入的 I-Frame。

封鎖可疑的 I-frames

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。

偵測有所發現時採取的動作

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。(選項僅適用於專家模式。)

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方塊，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。此桌面通知係針對下載網站內含較大量資料時所特別設計：如果您使用 Web Protection 來瀏覽，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，按一下此處。

自動

此選項一經啟用，偵測到病毒時將不會出現任何對話方塊。Web Protection 會根據您在這個區段中預先定義為主要和次要動作的設定來反應。

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。

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任何參考價值，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

網路篩選器可讓您封鎖網路釣魚和惡意程式碼 URL。Web Protection 可預防資料從網際網路傳輸到您的電腦系統上。(選項僅適用於專家模式。)

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

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 > 例外狀況](#) 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。

例外狀況

這些選項可讓您依據 URL (網際網路位址) 的 MIME 類型 (傳輸資料的內容類型) 與檔案類型，設定 Web Protection 的掃描例外狀況。Web Protection 會略過指定的 MIME 類型與 URL，亦即不會針對傳輸到電腦系統的資料掃描其中是否有病毒與惡意程式碼。(選項僅適用於專家模式。)

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 類型與檔案類型的名稱。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

輸入檔案類型與 MIME 類型時，無法使用任何萬用字元 (* 代表任何數量的字元，而 ? 則代表單一字元)。

警告

排除清單上的所有檔案類型與內容類型都會下載到網際網路瀏覽器，不需要再經過 Web Protection 的掃描：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 類型之範例：

- 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

您可以在此方塊中輸入要排除不進行 **Web Protection** 掃描的 **URL** (網際網路位址)，例如 `www.domainname.com`。您可以使用前導或後續句點來指出網域層級，藉此指定 **URL** 的各部分：`.domainname.com` 代表網域的所有網頁與所有子網域。使用後續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

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` (有效的格式，但不建議採用)

不含句點的指定項目，例如 `*name*`，會解譯為頂層網域的一部分，因此不建議使用。

警告

排除 **URL** 清單上的所有網站都會下載到網際網路瀏覽器中，不會經由網路篩選器或 **Web Protection** 做進一步的掃描：至於排除 **URL** 清單中的所有項目，會略過網路篩選器中的項目 (請參閱 [Web Protection > 掃描 > 封鎖的要求](#))。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。

例如：略過的 **URL**

- `www.avira.com` -或- `www.avira.com/*`
= 所有內含 `www.avira.com` 網域的 **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` 等等。
內含 `www.avira.de` 網域的 **URL** 不會從 **Web Protection** 掃描中排除。
- `avira.com` -或- `*.avira.com`
= 所有內含 `avira.com` 之第二層與頂層網域的 **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` 等等。

- avira.-或-*.avira.*
= 所有內含 avira 之第二層網域的 URL 都會從 Web Protection 掃描中排除：此規定意指以下項目的所有現有頂層網域或子網域：`.avira: www.avira.com`、`www.avira.de`、`forum.avira.com` 等等。
- .*domain*.*
所有內含 domain 字串之第二層網域的 URL 都會從 Web Protection 掃描中排除：`www.domain.com`、`www.new-domain.de`、`www.sample-domain1.de` 等等。
- net.-或-*.net
= 所有內含 net 之頂層網域的 URL 都會從 Web Protection 掃描中排除：`www.name1.net`、`www.name2.net` 等等。

警告

盡可能準確地輸入要從 Web Protection 掃描中排除的 URL。請避免指定整個頂層網域或部分第二層網域，因為這類全域排除設定可能會導致 Web Protection 掃描漏掉會散佈惡意程式碼與有害程式的網頁。建議您至少指定完整的第二層網域與頂層網域：`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。(選項僅適用於專家模式。)

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，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 產品內含威力非常強大的巨集病毒啟發式掃毒工具。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，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

中偵測等級

如果您已選取使用此啟發式掃毒技術，這將會是預設選項。

高偵測等級

此選項一經啟用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

10.4.2 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。此選項會啟用為預設值。

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

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 **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

如果您尚未指定任何報告檔限制，當此報告檔達到 **100MB** 時，舊項目會自動刪除。項目將遭到刪除，直到報告檔大小達到 **80 MB**。

10.5 一般

10.5.1 威脅類別

選取延伸的威脅類別 (選項僅適用於專家模式)

您的 **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/間碟軟體
- 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。

10.5.2 安全性

選項僅適用於專家模式。

自動啟動

封鎖自動啟動功能

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** 自動啟動功能執行都會遭到封鎖。啟用 **Windows** 自動啟動功能時，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。這項功能附帶高度安全風險，不過，惡意程式碼和有害程式可能會隨著自動啟動而安裝。自動啟動功能對於 **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** 光碟機上允許自動啟動功能。

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** 光碟機的自動啟動功能。

系統防護

保護 **Windows** 主機檔案不被變更

如果此選項設為啟用，則 **Windows** 主機檔案會加上寫入保護。以後無法再進行操作。例如，惡意程式碼將無法把您重新導向至有害的網站。系統會預設啟用此選項。

產品保護

注意

如果 **Realtime Protection** 尚未以使用者定義安裝選項完成安裝，您就無法使用產品保護選項。

保護處理序，避免意外終止

此選項一經啟用，會保護此程式的所有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。此選項會啟用為預設值。

進階處理序保護

此選項一經啟用，此程式的所有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。此選項會啟用為預設值。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。請在這些情況下停用處理序保護。

保護檔案和登錄項目，避免操作

此選項一經啟用，會保護此程式的所有登錄項目與所有程式檔 (二進位與組態檔) 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

請記住，一旦此選項停用，可能就無法修復遭受特定類型惡意軟體感染的電腦。

注意

此選項一經啟用，便只能透過使用者介面來進行對組態進行變更，包括對掃描或更新要求的變更。

注意

檔案和登錄項目保護不適用於 Windows XP 64 位元！

10.5.3 WMI

選項僅適用於專家模式。

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。您的 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)、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。

10.5.4 活動

選項僅適用於專家模式。

限制事件資料庫的大小

限制的大小上限為 n 個項目

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 到 10000 個項目。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。

10.5.5 報告

選項僅適用於專家模式。

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。

刪除超過此天數的所有報告

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 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，便不會限制報告份數。

10.5.6 目錄

選項僅適用於專家模式。

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

您可以查看系統儲存暫存檔案的位置為何 – 例如，在 Windows XP 環境中，可以進入：**[開始] > [設定] > [控制台] > [系統] > [進階]** 索引卡 **[環境變數]** 按鈕。該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)，與其相關數值。

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，輸入程式將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。

10.5.7 警示音

選項僅適用於專家模式。

當 **System Scanner** 或 **Realtime Protection** 偵測到病毒或惡意程式碼，會以互動式動作模式發出警示音。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

System Scanner 的動作模式是在組態的 **System Scanner > 掃描 > 偵測有所發現時採取的動作** 底下進行設定。

無警告

此選項一經啟用，當 System Scanner 或 Realtime 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 System Scanner 或 Realtime Protection 偵測到病毒時，會發出預設的警示音訊號。警示音會從 PC 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 System Scanner 或 Realtime 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。可輸入程式預設警示訊號做為標準設定。



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。

10.5.8 警示

您的 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】** 中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。您可以日後在 **【警示】** 組態視窗中重新啟用通知。

更新

如果上次更新超過以下天數，則發出警示

在此方塊中，您可以輸入自上次更新之後，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。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 / 注意以下情況

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 > 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，您就會收到桌面通知：無法建立與下載伺服器的連線，或無法安裝更新檔案。

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。

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。

本手冊係本公司用心製作。然而，在設計和內容上的錯誤在所難免。
未經 Avira Operations GmbH & Co. KG 事先書面同意，不得以任何形式重製本出版品或其某些部分。

本公司保留修改錯誤及技術內容的權利。



live free.™