McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

使用手冊

目錄

簡介 **3**

McAfee SecurityCenter....5
SecurityCenter 功能....6
使用 SecurityCenter....7
更新 SecurityCenter....13
修復或略過保護問題....15
使用警示....19
檢視事件....25
McAfee VirusScan....27
VirusScan 功能....28
啓動即時病毒防護....29
啓動其他保護....31
設定病毒防護....35
掃描您的電腦....49
使用掃描結果....51
McAfee Personal Firewall....55
Personal Firewall 功能....56
啓動防火牆....59
使用警示....61
管理資訊警示....63
設定防火牆保護....65
管理程式及權限....75
管理系統服務....83
管理電腦連線....89
記錄、監視及分析....97
瞭解網際網路安全性....107
McAfee QuickClean....109
QuickClean 功能....110
清理您的電腦....111
將電腦進行磁碟重組....114
排程工作....115
McAfee Shredder....121
Shredder 功能....122
銷毀檔案、資料夾及磁碟....123
McAfee Network Manager....125
Network Manager 的功能....126
瞭解 Network Manager 圖示....127
設定一個受管理網路....129
遠端管理網路....135
McAfee EasyNetwork....139
EasyNetwork 的功能....140
設定 EasyNetwork....141

共用和傳送檔案 147
共用印表機 153
參考.....155

字彙 **156**

關於 McAfee **169**

所有權 169
授權 170
客戶及技術支援.....171
使用 McAfee Virtual Technician 172
支援與下載 173

索引 **181**

第 1 章

簡介

McAfee VirusScan Plus 提供可避免惡意攻擊的主動式電腦安全性，可讓您保護重要的資產，並放心進行線上漫遊、搜尋與下載檔案。McAfee SiteAdvisor 的網頁安全評等可協助避免造訪不安全的網站。此服務結合防毒、防間諜軟體與防火牆技術，提供針對多樣攻擊的安全性防護。McAfee 的安全性服務會持續提供最新的軟體，讓您的防護永遠不會過期。您現在可輕鬆新增與管理家庭網路中多部電腦的安全性。再者，提升的效能還可讓電腦安全防護不致干擾您的工作。

在本章中

McAfee SecurityCenter....5
McAfee VirusScan....27
McAfee Personal Firewall....55
McAfee QuickClean....109
McAfee Shredder....121
McAfee Network Manager....125
McAfee EasyNetwork....139
參考....155
關於 McAfee....169
客戶及技術支援....171

第 2 章

McAfee SecurityCenter

McAfee SecurityCenter 可讓您監視電腦的安全狀態，立即了解您電腦的病毒、間諜軟體、電子郵件與防火牆保護服務是否處於最新狀態，並對潛在的安全性弱點進行處理。其提供您需要的瀏覽工具與控制項，協調與管理您電腦保護的所有區域。

在您開始設定與管理電腦的保護之前，請查看 SecurityCenter 介面，並確定您了解保護狀態、保護類別與保護服務之間的差異。然後，更新 SecurityCenter 以確保您擁有 McAfee 的最新保護。

在您的初始設定工作完成後，您可以使用 SecurityCenter 來監視電腦的保護狀態。若 SecurityCenter 偵測到保護問題，便會提出警示，您就可以依嚴重性，對該問題進行修復或略過。您也可以在事件記錄檔中查看 SecurityCenter 事件，例如病毒掃描設定變更。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

SecurityCenter 功能.....6
使用 SecurityCenter.....7
更新 SecurityCenter.....13
修復或略過保護問題.....15
使用警示.....19
檢視事件.....25

SecurityCenter 功能

SecurityCenter 提供下列功能：

簡化的保護狀態

可讓您輕鬆檢視電腦的保護狀態、檢查是否有更新並修正潛在的保護問題。

自動更新與升級

自動下載並安裝您已註冊程式的更新。在訂閱有效期間，當有可用的新版已註冊 McAfee 程式時，您都可以免費取得，確保您永遠擁有最新的保護。

即時警示

安全性警示會通知您緊急的病毒爆發和安全性威脅，並提供移除、消除或深入瞭解該威脅的選項。

第 3 章

使用 SecurityCenter

在您開始使用 SecurityCenter 之前，請查看您將會用來管理電腦保護狀態的元件與設定區域。如需此影像中使用之術語的詳細資訊，請參閱＜瞭解保護狀態＞(第 8 頁)與＜瞭解保護類別＞(第 9 頁)。接著，您可以查看 McAfee 帳戶資訊，並確認您的訂閱有效期間。

在本章中

瞭解保護狀態.....8
瞭解保護類別.....9
瞭解保護服務.....10
管理您的 McAfee 帳戶.....11

瞭解保護狀態

電腦的保護狀態會顯示於 [SecurityCenter 首頁] 窗格上的保護狀態區域中。這裡會表示您電腦是否受到完全的保護以對抗最新的安全性威脅，以及是否受到其他事件的影響，例如外部安全性攻擊、其他安全性程式，與可存取網際網路的程式。

您電腦的保護狀態可能是紅色、黃色或綠色。

保護狀態	說明
紅色	您的電腦未受保護。[SecurityCenter 首頁] 窗格上的保護狀態區域爲紅色，表示您並未受到保護。SecurityCenter 至少回報一個重大安全性問題。 爲達到完整的保護，您必須修復每個保護類別中的所有重大安全性問題 (問題的類別狀態設爲 [必要動作] 時亦爲紅色)。如需如何修復保護問題的相關資訊，請參閱＜修復保護問題＞(第 16 頁)。
黃色	您的電腦受到部份保護。[SecurityCenter 首頁] 窗格上的保護狀態區域爲黃色，表示您並未受到保護。SecurityCenter 至少回報一個非重大安全性問題。 爲達到完整的保護，您必須修復或略過與每個保護類別相關之非重大安全性問題。如需如何修復或略過保護問題的相關資訊，請參閱＜修復或略過保護問題＞(第 15 頁)。
綠色	您的電腦受到完整保護。[SecurityCenter 首頁] 窗格上的保護狀態區域爲綠色，表示您已受到保護。SecurityCenter 並未回報任何重大或非重大安全性問題。 每個保護類別都會列出保護電腦的服務。

瞭解保護類別

SecurityCenter 的保護服務分爲四個類別：電腦與檔案、網際網路與網路、電子郵件與即時訊息，以及未成年保護。這些類別可協助您瀏覽並設定保護電腦的安全性服務。

您可以按一下類別名稱以設定其保護服務，並檢視這些服務所偵測到的安全性問題。若您電腦的保護狀態爲紅色或黃色、一或多個類別顯示 [必要動作] 或 [注意] 訊息，就表示 SecurityCenter 在該類別中偵測到問題。如需保護狀態的更多資訊，請參閱<瞭解保護狀態>(第 8 頁)。

保護類別	說明
電腦與檔案	「電腦與檔案」類別可讓您設定下列保護服務： ▪ 病毒防護 ▪ 潛在無用程式防護 ▪ 系統監視 ▪ Windows 保護
網際網路與網路	「網際網路與網路」類別可讓您設定下列保護服務： ▪ 防火牆保護 ▪ 身分保護
電子郵件與即時訊息	「電子郵件與即時訊息」類別可讓您設定下列保護服務： ▪ 電子郵件保護 ▪ 垃圾郵件保護
未成年保護	「未成年保護」類別可讓您設定下列保護服務： ▪ 內容封鎖

瞭解保護服務

保護服務是 SecurityCenter 的核心元件，可讓您設定以保護電腦。保護服務直接對應至 McAfee 程式。例如，當您安裝 VirusScan 時，將可使用下列保護服務：病毒防護、PUP 保護、系統監視與 Windows 保護。如需有關這些特定保護服務的詳細資訊，請參閱＜VirusScan 說明＞。

依預設，安裝程式時會啓用與程式相關的所有保護服務，但是，您可以隨時停用保護服務。例如，若您安裝 Privacy Service，會同時啓用「內容封鎖」與「身分保護」。若您不打算使用「內容封鎖」保護服務，您可以完全停用它。您也可以在執行安裝或維護工作時，暫時停用保護服務。

管理您的 McAfee 帳戶

透過輕鬆存取及查看您的帳戶資訊並驗證目前的訂閱狀態，從 SecurityCenter 中管理您的 McAfee 帳戶。

附註：若您是從 CD 安裝 McAfee 程式，則必須在 McAfee 網站進行註冊以設定或更新您的 McAfee 帳戶。之後，您才能享有定期且自動的程式更新。

管理您的 McAfee 帳戶

您可輕鬆地從 SecurityCenter 存取 McAfee 帳戶資訊 ([我的帳戶])。

1. 按一下 [常見工作] 下的 [我的帳戶]。
2. 登入您的 McAfee 帳戶。

確認您的訂閱

確認您的訂閱，以確保其尚未到期。

- 在工作列最右邊之通知區域中的 SecurityCenter 圖示 上按一下滑鼠右鍵，然後按一下 [確認訂閱]。

第 4 章

更新 SecurityCenter

SecurityCenter 每四小時會進行檢查並安裝線上更新，以確保您註冊的 McAfee 程式是最新的。視您已安裝並註冊的程式而定，線上更新可能包括最新的病毒定義與駭客、垃圾郵件、間諜軟體或隱私權保護升級。若您要在預設的四小時期間檢查更新，您可以隨時這麼做。您可以在 SecurityCenter 檢查是否有更新時，繼續執行其他工作。

雖然並不建議這麼做，但您可變更 SecurityCenter 檢查與安裝更新的方式。例如，您可設定 SecurityCenter 下載但不安裝更新，或在下載或安裝更新之前通知您。您也可以停用自動更新。

附註：若您是從 CD 安裝 McAfee 程式，除非在 McAfee 網站上進行註冊，否則您將無法定期、自動接收這些程式的更新。

在本章中

檢查更新.....13
設定自動更新.....14
停用自動更新.....14

檢查更新

依預設，當您的電腦連線到網際網路時，SecurityCenter 會每四小時自動檢查更新。但是，若您想在四小時期間內檢查更新，您可以這麼做。若您停用自動更新，則您有責任定期檢查更新。

- 在 [SecurityCenter 首頁] 窗格上，按一下 [更新]。

秘訣：您可在工作列最右邊之通知區域中的 SecurityCenter 圖示 上按一下滑鼠右鍵，然後按一下 [更新] 以檢查更新，無需啓動 SecurityCenter。

設定自動更新

依預設，SecurityCenter 會在您的電腦連線到網際網路時，每隔四小時自動檢查並安裝更新。若要變更此預設行爲，您可設定 SecurityCenter 來自動下載更新，然後，在準備安裝更新時通知您，或下載更新前先通知您。

附註：SecurityCenter 會使用警示在準備下載或安裝更新時通知您。您可以從警示下載或安裝更新，或將更新延期。當您從警示更新程式時，可能會出現提示要求您在下載並進行安裝前先確認訂閱。如需詳細資訊，請參閱＜使用警示＞(第 19 頁)。

1 開啓 [SecurityCenter 設定] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。

2 在 [SecurityCenter 設定] 窗格中，於 [自動更新已停用] 之下，按一下 [開啓]，然後按一下 [進階]。

3 按一下底下其中一個按鈕：

- **自動安裝更新並在服務更新後通知我 (建議使用)**
- **自動下載更新並在即將安裝時時通知我**
- **在下載任何更新之前通知我**

4 按一下 [確定]。

停用自動更新

若您停用自動更新，則您有責任定期檢查更新；否則，您的電腦將無法擁有最新的安全性保護。如需手動檢查更新的相關資訊，請參閱＜檢查更新＞(第 13 頁)。

1 開啓 [SecurityCenter 設定] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。

2 在 [SecurityCenter 設定] 窗格中，於 [自動更新已啓用] 之下，按一下 [關閉]。

秘訣：您可以按一下 [開啓] 按鈕或清除 [更新選項] 窗格上的 [停用自動更新並讓我手動檢查更新]，以啓用自動更新。

第 5 章

修復或略過保護問題

SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。重大保護問題需要立即採取動作，並會變更您的保護狀態 (變更顏色爲紅色)。非重大保護問題不需要立即採取動作，可能會也可能不會變更您的保護狀態 (依問題的類型而定)。爲達到綠色的保護狀態，您必須修復所有的重大問題，並修復或略過所有非重大問題。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。如需 McAfee Virtual Technician 的詳細資訊，請參閱＜McAfee Virtual Technician 說明＞。

在本章中

修復保護問題.....16
略過保護問題.....17

修復保護問題

大部分的安全性問題可進行自動修復，但是，某些問題可能需要您採取動作。例如，若停用防火牆保護，SecurityCenter 可自動將其啓用；但是，若未安裝防火牆保護，則您必須進行安裝。下列表格說明當以手動方式修復保護問題時，您可能需要採取的其他動作：

問題	動作
在過去 30 天內並未執行電腦的完整掃描。	手動掃描您的電腦。如需詳細資訊，請參閱＜VirusScan 說明＞。
您的偵測簽章檔 (DAT) 已過期。	手動更新您的保護。如需詳細資訊，請參閱＜VirusScan 說明＞。
未安裝程式。	從 McAfee 網站或 CD 安裝程式。
程式遺失元件。	從 McAfee 網站或 CD 重新安裝程式。
程式尚未註冊且無法接收完整的保護。	在 McAfee 網站註冊程式。
程式已過期。	在 McAfee 網站上檢查帳戶狀態。

附註：通常，一個保護問題會影響一個以上的保護類別。在這種情況下，在一個類別中修復此問題會清除所有其他保護類別中的這個問題。

自動修復保護問題

SecurityCenter 可自動修復大部分的保護問題。自動修復保護問題時，SecurityCenter 所進行的設定變更並未記錄於事件記錄檔中。如需事件的詳細資訊，請參閱＜檢視事件＞(第 25 頁)。

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格的保護狀態區域中，按一下 [修復]。

手動修復保護問題

在您嘗試自動修復保護問題後，如果仍有一或多個問題存在，則您可以手動修復這些問題。

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 SecurityCenter 回報問題的保護類別。
3. 按一下問題說明之後的連結。

略過保護問題

若 SecurityCenter 偵測到一個非重大問題，您可以修復或略過它。其他非重大問題 (例如，若未安裝 Anti-Spam 或 Privacy Service) 會自動略過。除非您電腦的保護狀態爲綠色，否則略過的問題不會顯示於 [SecurityCenter 首頁] 窗格的保護類別資訊區域中。若您略過問題，但稍後決定要其出現於保護類別資訊區域 (即使您電腦的保護狀態不是綠色)，您仍可顯示略過的問題。

略過保護問題

若 SecurityCenter 偵測到一個您不想修復的非重大問題，您可以略過它。略過它會將問題從 SecurityCenter 中的保護類別資訊區域移除。

1 按一下 [常見工作] 下的 [首頁]。

2 在 [SecurityCenter 首頁] 窗格上，按一下回報問題的保護類別。

3 按一下保護問題旁的 [略過] 連結。

顯示或隱藏略過的問題

視其嚴重性而定，您可顯示或隱藏略過的保護問題。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [SecurityCenter 設定] 窗格上，按一下 [略過的問題]。

3 在 [略過的問題] 窗格上，執行下列動作：

- 若要略過問題，請選取其核取方塊。
- 若要回報保護類別資訊區域中的問題，請清除其核取方塊。

4 按一下 [確定]。

秘訣：您也可按一下保護類別資訊區域中、已回報問題旁的 [略過] 連結，以略過問題。

第 6 章

使用警示

當某些 SecurityCenter 事件發生時，您螢幕右下方所顯示的小型快顯對話方塊爲警示。警示會提供事件的詳細資訊以及建議與選項，以解決可能與該事件相關聯的問題。某些警示也包含與事件相關的其他資訊連結。這些連結可讓您啓動 McAfee 的全球網站，或將資訊傳送至 McAfee 以進行疑難排解。

有三種警示類型：紅色、黃色和綠色。

警示類型	說明
紅色	紅色警示是需要您回應的重大通知。當 SecurityCenter 無法判定如何自動修復保護問題時，便會產生紅色警示。
黃色	黃色警示是不嚴重的通知，通常會需要您的回應。
綠色	綠色警示是不需要您回應的非重大通知。綠色警示會提供與事件相關的基本資訊。

因爲警示在監視與管理您的保護狀態上扮演一個重要的角色，所以您無法停用它們。但是，您可控制某些資訊警示類型是否顯示，以及設定一些其他警示選項 (例如，SecurityCenter 是否在出現警示時播放聲音，或在啓動時顯示 McAfee 片頭畫面)。

在本章中

顯示與隱藏資訊警示.....20
設定警示選項.....22

顯示與隱藏資訊警示

當您的電腦發生不具安全性威脅的事件時，資訊警示會通知您。例如，若您已設定防火牆保護，則依預設，只要授與您電腦上的程式存取網際網路權限時，便會顯示資訊警示。如果您不想顯示特定的資訊警示類型，可將其隱藏。如果您不想顯示任何的資訊警示，可以隱藏所有資訊警示。當您在電腦上以全螢幕模式進行遊戲時，也可以隱藏所有的資訊警示。當您結束遊戲並退出全螢幕模式時，SecurityCenter 會開始再次顯示資訊警示。

若錯誤地隱藏某個資訊警示，您可以隨時再顯示它。依預設，SecurityCenter 會顯示所有的資訊警示。

顯示或隱藏資訊警示

您可以設定 SecurityCenter 以顯示某些資訊警示並隱藏其他資訊警示，或隱藏所有資訊警示。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [SecurityCenter 設定] 窗格上，按一下 [資訊警示]。

3 在 [資訊警示] 窗格上，執行下列動作：

- 若要顯示某個資訊警示，請清除其核取方塊。
- 若要隱藏某個資訊警示，請選取其核取方塊。
- 若要隱藏所有資訊警示，請選取 [請勿顯示資訊警示] 核取方塊。

4 按一下 [確定]。

秘訣：您也可選取警示本身中的 [不要再顯示此警示] 核取方塊，來隱藏某個資訊警示。若這麼做，則您可清除 [資訊警示] 窗格上適當的核取方塊以再次顯示該資訊警示。

遊戲時顯示或隱藏資訊警示

當您在電腦上使用全螢幕模式進行遊戲時，可以隱藏資訊警示。當您結束遊戲並退出全螢幕模式時，SecurityCenter 會開始再次顯示資訊警示。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [警示選項] 窗格上，選取或清除 [偵測到遊戲模式時，顯示資訊警示] 核取方塊。

3 按一下 [確定]。

設定警示選項

警示的外觀與頻率是由 SecurityCenter 所設定；但是您可以調整一些基本的警示選項。例如，您可在出現警示時播放聲音，或在 Windows 啓動時隱藏片頭畫面警示。您也可以隱藏有關線上社群中病毒肆虐及其他安全性威脅之通知的警示。

出現警示時播放聲音

若您要在警示發生時收到聲音的指示，您可以設定 SecurityCenter 在每個警示出現時播放聲音。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [警示選項] 窗格上的 [聲音] 之下，選取 [出現警示時播放聲音] 核取方塊。

在啓動時隱藏片頭畫面

依預設，啓動 Windows 時，McAfee 片頭畫面會有短暫地顯示，通知您 SecurityCenter 正在保護電腦。但是，若您不想顯示片頭畫面，則可將其隱藏。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [警示選項] 窗格上的 [片頭畫面] 之下，清除 [Windows 啓動時顯示 McAfee 片頭畫面] 核取方塊。

秘訣：您可選取 [Windows 啓動時顯示 McAfee 片頭畫面] 核取方塊，於任何時間再次顯示片頭畫面。

隱藏病毒爆發警示

您可以隱藏有關線上社群中病毒肆虐及其他安全性威脅之通知的警示。

1 開啓 [警示選項] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下的右窗格中，按一下 [設定]。
3. 在 [警示] 下，按一下 [進階]。

2 在 [警示選項] 窗格上，清除 [當出現病毒或安全性威脅時，請發出警示給我] 核取方塊。

秘訣：您可以選取 [當出現病毒或安全性威脅時，請發出警示給我] 核取方塊，於任何時間顯示病毒爆發警示。

第 7 章

檢視事件

事件是一個發生於保護類別及其相關保護服務內的動作或設定變更。不同的保護服務記錄不同的事件類型。例如，SecurityCenter 記錄啓用或停用保護服務的事件；Virus Protection 記錄每次偵測到病毒及將其移除的事件；以及 Firewall Protection 記錄每次嘗試網際網路連線而遭到封鎖的事件。如需保護類別的詳細資訊，請參閱＜瞭解保護類別＞(第 9 頁)。

疑難排解設定問題及查看其他使用者執行作業時，您可以檢視事件。許多家長會使用事件記錄檔來監視其子女在網際網路上的行爲。若只要檢查最近發生的 30 個事件，您可以檢視最近的事件。若要檢查所有已發生事件的完整清單，您可以檢視所有事件。檢視所有事件時，SecurityCenter 會啓動事件記錄檔，根據事件發生所在的保護類別來排序事件。

在本章中

檢視最近的事件.....25
檢視所有事件.....25

檢視最近的事件

若只要檢查最近發生的 30 個事件，您可以檢視最近的事件。

- 按一下 [常見工作] 下的 [檢視最近的事件]。

檢視所有事件

若要檢查所有已發生事件的完整清單，您可以檢視所有事件。

1. 按一下 [常見工作] 下的 [檢視最近的事件]。
2. 在 [最近的事件] 窗格上，按一下 [檢視記錄檔]。
3. 在事件記錄檔的左窗格，按一下您要檢視的事件類型。

第 8 章

McAfee VirusScan

VirusScan 的進階偵測與保護服務可保護您與您的電腦免於最新的安全威脅，包括病毒、特洛伊病毒、追蹤 Cookie、間諜軟體、廣告軟體及其他潛在的無用程式。保護將延伸到您的桌上型電腦中的檔案和資料夾，專門針對來自不同進入點的威脅 (包括電子郵件、即時訊息、網路) 提供保護。

使用 VirusScan，您電腦的保護是立即且持續的 (不需要冗長的管理)。當您在工作、遊戲、瀏覽網頁或查閱電子郵件時，它會在背景中執行，同步進行監視、掃描並偵測可能的危害。定期排定執行全方位的掃描，使用更爲複雜的選項組定期檢查您的電腦。VirusScan 提供您自訂此行爲的彈性 (若您要的話)，若不要，您的電腦仍會受到保護。

一般的電腦使用，病毒、蠕蟲及其他潛在威脅可能會潛入您的電腦。若發生這樣的狀況，VirusScan 會通知您威脅的相關資訊，但通常會幫您處理，在任何傷害發生之前清除或隔離受感染的項目。儘管不太可能發生，但有時仍可能需要進一步的動作。在這些狀況下，VirusScan 可讓您決定如何進行 (下次開啓電腦時重新掃描、保留偵測到的項目或移除偵測到的項目)。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

VirusScan 功能 28
啓動即時病毒防護 29
啓動其他保護 31
設定病毒防護 35
掃描您的電腦 49
使用掃描結果 51

VirusScan 功能

VirusScan 提供下列功能。

全面的病毒保護

VirusScan 的進階偵測與保護服務可保護您與您的電腦免於最新的安全威脅，包括病毒、特洛伊病毒、追蹤 Cookie、間諜軟體、廣告軟體及其他潛在的無用程式。保護將延伸到您的桌上型電腦中的檔案和資料夾，專門針對來自不同進入點的威脅 (包括電子郵件、即時訊息、網路) 提供保護。不需要冗長的管理。

資源感知掃描選項

若您覺得掃描速度緩慢，可以停用選項以使用最少的電腦資源，但請記住病毒防護的優先順序將高於其他工作。VirusScan 提供您彈性來自訂即時與手動掃描選項 (若您要的話)，若不要，您的電腦仍會受到保護。

自動修復

在執行即時或手動掃描時，若 VirusScan 偵測到一個安全性威脅，會依據威脅類型來嘗試自動處理威脅。依此方法，大部分的威脅皆可在沒有您的介入下進行偵測與消除。雖然很少發生，VirusScan 可能無法自行消除威脅。在這些狀況下，VirusScan 可讓您決定如何進行 (下次開啓電腦時重新掃描、保留偵測到的項目或移除偵測到的項目)。

在全螢幕模式下暫停工作

在您的電腦上享受觀看電影、玩遊戲或其他會佔用您整個電腦螢幕的活動時，VirusScan 會暫停一些工作，包括自動更新與手動掃描。

啓動即時病毒防護

VirusScan 提供兩種病毒防護類型：即時與手動。即時病毒防護會持續監視您電腦的病毒活動，在您或電腦每次存取檔案時進行掃描。手動病毒防護可讓您依指定掃描檔案。爲確保您的電腦持續受到保護以對抗最新的安全性威脅，請開啓即時病毒防護並設定排程，以進行定期且更完整的手動掃描。依預設，VirusScan 一週會執行一次排定的掃描。如需即時與手動掃描的詳細資訊，請參閱＜掃描您的電腦＞(第 49 頁)。

雖然很少發生，但仍可能要您暫時停止即時掃描 (例如，要變更某些掃描選項，或疑難排解效能問題)。停用即時病毒防護時，將無法保護您的電腦，且您的 SecurityCenter 保護狀態會是紅色的。如需有關保護狀態的詳細資訊，請參閱 SecurityCenter 說明中的＜瞭解保護狀態＞。

啓動即時病毒防護

預設會開啓即時病毒防護並保護您的電腦，以免於病毒、特洛伊病毒及其他安全性威脅的攻擊。若關閉即時病毒防護，您必須將其再度開啓以進行防護。

1 開啓 [電腦與檔案設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 在 [設定] 窗格上，按一下 [電腦與檔案]。

2 在 [病毒保護] 之下，按一下 [開啓]。

停止即時病毒防護

您可暫時關閉即時病毒防護，然後指定其恢復的時間。您可以選擇在 15、30、45 或 60 分鐘後自動恢復保護、在電腦重新啓動時或永遠停止保護。

1 開啓 [電腦與檔案設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 在 [設定] 窗格上，按一下 [電腦與檔案]。

2 在 [病毒保護] 之下，按一下 [關閉]。

3 在此對話方塊中，選取恢復即時掃描的時間。

4 按一下 [確定]。

第 9 章

啓動其他保護

除了即時病毒防護外，VirusScan 提供進階的保護以對抗指令碼、間諜軟體及可能有害的電子郵件與即時訊息附件的攻擊。依預設會啓用指令碼掃描、間諜軟體、電子郵件及即時訊息保護並保護您的電腦。

指令碼掃描防護

指令碼掃描保護會偵測可能有害的指令碼，並防止它們在您的電腦上執行。它會監視您電腦的可疑指令碼活動，例如建立、複製或刪除檔案的指令碼，或開啓您的 Windows 登錄，並在發生任何傷害之前警示您。

間諜軟體保護

間諜軟體保護會偵測間諜軟體、廣告軟體及其他潛在的無用程式。間諜軟體可偷偷地安裝在您的電腦上以監視您的運作方式、收集個人資訊，甚至安裝其他軟體以干擾您對電腦的控制權或重新導向瀏覽器活動。

電子郵件保護

電子郵件保護會偵測您傳送與接收之電子郵件及附件中的可疑活動。

即時訊息保護

即時訊息保護會偵測您所接收之即時訊息的潛在安全性威脅。它還可以防止即時訊息程式共用個人資訊。

在本章中

啓動指令碼掃描防護.....32
啓動間諜軟體保護.....32
啓動電子郵件保護.....32
啓動即時訊息保護.....33

啓動指令碼掃描防護

開啓指令碼掃描保護以偵測可能有害的指令碼，並防止它們在您的電腦上執行。當指令碼試著建立、複製或刪除您電腦上的檔案，或者變更您的 Windows 登錄時，指令碼掃描保護就會警示您。

1 開啓 [電腦與檔案設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 在 [設定] 窗格上，按一下 [電腦與檔案]。

2 在 [指令碼掃描保護] 之下，按一下 [開啓]。

附註：雖然您隨時都可以關閉指令碼掃描保護，但這麼做將使您的電腦遭到有害的指令碼攻擊。

啓動間諜軟體保護

開啓間諜軟體保護以偵測及移除間諜軟體、廣告軟體，以及其他未經您允許即逕自收集和傳輸資訊的潛在無用程式。

1 開啓 [電腦與檔案設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 在 [設定] 窗格上，按一下 [電腦與檔案]。

2 在 [指令碼掃描保護] 之下，按一下 [開啓]。

附註：雖然您隨時都可以關閉間諜軟體防護，但這麼做將使您的電腦遭到潛在無用程式的攻擊。

啓動電子郵件保護

開啓電子郵件保護以偵測蠕蟲，以及出埠 (SMTP) 與入埠 (POP3) 電子郵件訊息與附件中的潛在威脅。

1 開啓 [電子郵件與即時訊息設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 按一下 [設定] 窗格中的 [電子郵件與即時訊息]。

2 在 [電子郵件保護] 之下，按一下 [開啓]。

附註：雖然您隨時都可以關閉電子郵件保護，但這麼做將使您的電腦遭到電子郵件威脅的攻擊。

啓動即時訊息保護

開啓即時訊息保護以偵測可包含於入埠即時訊息附件中的安全性威脅。

1 開啓 [電子郵件與即時訊息設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 按一下 [設定] 窗格中的 [電子郵件與即時訊息]。

2 在 [即時訊息保護] 之下，按一下 [開啓]。

附註：雖然您隨時都可以關閉即時訊息保護，但這麼做將使您的電腦遭到有害的即時訊息附件攻擊。

第 10 章

設定病毒防護

VirusScan 提供兩種病毒防護類型：即時與手動。即時病毒防護掃描會在您或您的電腦存取檔案時掃描檔案。手動病毒防護可讓您依指定掃描檔案。您可對每種防護類型設定不同的選項。例如，由於即時防護會持續地監視您的電腦，您可能選取某個基本掃描選項組，保留更完整的掃描選項組以供手動指定的保護使用。

在本章中

設定即時掃描選項.....36
設定手動掃描選項.....37
使用 SystemGuard 選項.....41
使用信任的清單.....46

設定即時掃描選項

當您啓動即時病毒防護時，VirusScan 會使用預設的選項組來掃描檔案；但您可依需要變更預設選項。

若要變更即時掃描選項，您必須決定掃描期間 VirusScan 檢查的事項爲何，以及其掃描的位置與檔案類型。例如，您可以決定 VirusScan 是否要檢查網站可用來追蹤您運作方式的未知病毒或 Cookie，及其是否掃描對應至您電腦的網路磁碟機，或只是本機磁碟機。您也可以決定要掃描的檔案類型 (所有檔案，或僅只是程式檔案與文件，因爲這是最容易偵測到病毒之處)。

變更即時掃描選項時，您也必須決定您的電腦具有緩衝區溢位保護是否重要。緩衝區是部分的記憶體，可用來暫時保留電腦資訊。當可疑的程式或程序儲存於緩衝區的資料量超過緩衝區容量時，就會發生緩衝區溢位。發生此情況時，您的電腦會更容易受到安全性攻擊。

設定即時掃描選項

您可設定即時掃描選項，以自訂即時掃描期間 VirusScan 檢查的事項爲何，以及其掃描的位置與檔案類型。選項包含對未知的病毒與追蹤 Cookie 進行掃描，以及提供緩衝區溢位保護。您還可以設定即時掃描，以檢查對應至您電腦的網路磁碟機。

1 開啓 [即時掃描] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定病毒防護已啓用，然後按一下 [進階]。

2 指定您的即時掃描選項，然後按一下 [確定]。

若要...	執行此動作...
偵測未知的病毒與已知病毒的新變種	選取 [使用啓發式技術來掃描不明病毒] 核取方塊。
偵測 Cookie	選取 [掃描並移除追蹤 Cookie] 核取方塊。
偵測連接至您網路之磁碟機上的病毒與其他潛在威脅	選取 [掃描網路磁碟機] 核取方塊。
保護您的電腦以免於緩衝區溢位	選取 [啓用緩衝區溢位保護] 核取方塊。
指定要掃描的檔案類型	按一下 [所有檔案 (建議使用)] 或 [僅程式檔案及文件]。

設定手動掃描選項

手動病毒防護可讓您依指定掃描檔案。開始手動掃描時，VirusScan 會使用更完整的掃描選項組來檢查您電腦的病毒與其他可能有害的項目。若要變更手動掃描選項，您必須決定掃描期間 VirusScan 檢查的事項爲何。例如，您可以決定 VirusScan 是否檢查未知的病毒、潛在的無用程式 (例如間諜軟體或廣告軟體)、隱形程式 (例如可對您的電腦授與未授權之存取權的 Rootkit) 以及網站可用來追蹤您運作方式的 Cookie。您也必須決定要檢查的檔案類型。例如，您可以決定 VirusScan 是否要檢查所有的檔案，或只是程式檔案與文件 (因爲這是最容易偵測到病毒之處)。您也可以決定是否將封存檔 (例如，.zip 檔) 包含在掃描之中。

依預設，VirusScan 會在每次執行手動掃描時檢查您電腦上的所有磁碟機與資料夾，但是您可以依需要變更預設位置。例如，您可以只掃描重要的系統檔案、桌面上的項目或您 Program Files 資料夾中的項目。除非您自己要負責啓動每次的手動掃描，否則您可以設定定期的掃描排程。排定的掃描會永遠使用預設的掃描選項來檢查您整個電腦。依預設，VirusScan 一週會執行一次排定的掃描。

若您覺得掃描速度緩慢，請考慮停用選項以使用最少的電腦資源，但請記住病毒防護的優先順序將高於其他工作。

附註：在您的電腦上享受觀看電影、玩遊戲或其他會佔用您整個電腦螢幕的活動時，VirusScan 會暫停一些工作，包括自動更新與手動掃描。

設定手動掃描選項

您可以設定手動掃描選項，以自訂手動掃描期間 VirusScan 檢查的事項爲何，以及其掃描的位置與檔案類型。選項包含對未知的病毒、檔案封存、間諜軟體與潛在的無用程式、追蹤 Cookie、rootkit 與隱形程式進行掃描。

1 開啓 [手動掃描] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定病毒防護已啓用，並按一下 [進階]。
5. 按一下 [病毒防護] 窗格中的 [手動掃描]。

2 指定您的手動掃描選項，然後按一下 [確定]。

若要...	執行此動作...
偵測未知的病毒與已知病毒的新變種	選取 [使用啓發式技術來掃描不明病毒] 核取方塊。
偵測及移除 .zip 和其他封存檔中的病毒	選取 [掃描 .zip 及其他封存檔] 核取方塊。
偵測間諜軟體、廣告軟體及其他潛在的無用程式	選取 [掃描間諜軟體及潛在無用程式] 核取方塊。
偵測 Cookie	選取 [掃描並移除追蹤 Cookie] 核取方塊。
偵測到可能會改變及入侵現有 Windows 系統檔案的 rootkit 與隱型程式	選取 [掃描 Rootkit 及其他隱形程式] 核取方塊。
使用較少的處理器能力進行掃描，同時讓其他工作 (例如 Web 瀏覽或開啓文件) 擁有較高的優先權	選取 [使用最少的電腦資源進行掃描] 核取方塊。
指定要掃描的檔案類型	按一下 [所有檔案 (建議使用)] 或 [僅程式檔案及文件]。

設定手動掃描位置

您可以設定手動掃描位置，決定 VirusScan 於手動掃描期間檢查病毒與其它有害項目的位置。您可以掃描電腦上的所有檔案、資料夾與磁碟機，或者限制只對特定的資料夾與磁碟機進行掃描。

1 開啓 [手動掃描] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定病毒防護已啓用，並按一下 [進階]。
5. 按一下 [病毒防護] 窗格中的 [手動掃描]。

2 按一下 [要掃描的預設位置]。

3 指定您的手動掃描位置，然後按一下 [確定]。

若要...	執行此動作...
對您電腦上的所有檔案與資料夾進行掃描	選取 [(我的) 電腦] 核取方塊。
對您電腦上特定的檔案、資料夾與磁碟機進行掃描	清除 [(我的) 電腦] 核取方塊，並選取一或多個資料夾或磁碟機。
掃描重要的系統檔案	清除 [(我的) 電腦] 核取方塊，然後選取 [重要的系統檔案] 核取方塊。

排定掃描

排定掃描的時程，在一週內的任一天與任何時間，徹底檢查電腦中的病毒及其他威脅。排定的掃描會永遠使用預設的掃描選項來檢查您整個電腦。依預設，VirusScan 一週會執行一次排定的掃描。若您覺得掃描速度緩慢，請考慮停用選項以使用最少的電腦資源，但請記住病毒防護的優先順序將高於其他工作。

1 開啓 [排程掃描] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定病毒防護已啓用，並按一下 [進階]。
5. 按一下 [病毒防護] 窗格中的 [排程掃描]。

2 選取 [啓用排程掃描]。

3 若要降低一般用於掃描的處理器能力，請選取 [使用最少的電腦資源進行掃描]。

4 選取一天或多天。

5 指定開始時間。

6 按一下 [確定]。

秘訣：您可以按一下 [重設] 來還原預設的排程。

使用 SystemGuard 選項

SystemGuard 會對您電腦上之 Windows 登錄或重要的系統檔案所做之可能未經授權的變更進行監視、記錄、報告與管理。未經授權的登錄與檔案變更可能會損壞您的電腦、危害其安全性並毀損極爲重要的系統檔案。

您電腦上的登錄與檔案變更很常見且會定期發生。由於多數都是無害的，因此 SystemGuard 所設定的預設值是以提供值得信賴、智慧型及實境的保護，以防未經授權的變更所可能造成的嚴重傷害。例如，當 SystemGuard 偵測到不尋常的變更且顯示潛在的嚴重威脅，就會立即回報並記錄該活動。針對較常見、但仍可能造成某種程度毀害的變更，則只會記錄。但是，依預設將會停用對標準與低風險變更的監視。您可以設定 SystemGuard 技術，以延伸其保護至任何您想要的地方。

有三種 SystemGuard 類型：程式 SystemGuard、Windows SystemGuard 與瀏覽器 SystemGuard。

程式 SystemGuard

程式 SystemGuard 會偵測對電腦登錄及其他對 Windows 極爲重要之必要檔案所進行的可能未經授權變更。這些重要的登錄項目與檔案包括 ActiveX 安裝、啓動項目、Windows Shell 執行攔截及 Shell 服務物件延遲載入。藉由監視這些項目，當 Windows 啓動時，程式 SystemGuard 技術除了會停止可自動啓動的間諜軟體與潛在的無用程式之外，還能停止可疑的 ActiveX 程式 (下載自網際網路)。

Windows SystemGuard

Windows SystemGuard 也會偵測對電腦登錄及其他對 Windows 極爲重要之必要檔案所進行的可能未經授權變更。這些重要的登錄項目與檔案包括內容功能表處理程式、appInit DLL 及 Windows 主機檔案。藉由監視這些項目，Windows SystemGuard 技術可協助保護您的電腦，避免透過網際網路傳送與接收未經授權的資訊或個人資訊。它還可以協助停止可疑的程式，這些程式可能會對您及您家庭之重要程式的外觀與運作方式進行不必要的變更。

瀏覽器 SystemGuard

就像程式與 Windows SystemGuard，瀏覽器 SystemGuard 也會偵測對電腦登錄及其他對 Windows 極爲重要之必要檔案進行的可能未經授權變更。但是，瀏覽器 SystemGuard 會對像是 Internet Explorer 附加元件、Internet Explorer URL 與 Internet Explorer 安全區域等重要的登錄項目與檔案變更進行監視。藉由監視這些項目，瀏覽器 SystemGuard 技術可協助防止未經授權的瀏覽器活動，例如重新導向至可疑的網站、在您不知情的情況下變更瀏覽器設定值與選項，以及信任可疑網站。

啓用 SystemGuard 保護

啓用 SystemGuard 保護以偵測並警示您電腦上可能未經授權的 Windows 登錄與檔案變更。未經授權的登錄與檔案變更可能會損壞您的電腦、危害其安全性並毀損極爲重要的系統檔案。

1 開啓 [電腦與檔案設定] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [設定]。
3. 在 [設定] 窗格上，按一下 [電腦與檔案]。

2 在 [SystemGuard 保護] 之下，按一下 [開啓]。

附註：您可按一下 [關閉] 來停用 SystemGuard 保護。

設定 SystemGuard 選項

使用 [SystemGuard] 窗格來設定保護、記錄與警示選項，以對抗與 Windows 檔案、程式及 Internet Explorer 相關的未經授權登錄與檔案變更。未經授權的登錄與檔案變更可能會損壞您的電腦、危害其安全性並毀損極爲重要的系統檔案。

1 開啓 [SystemGuard] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定 SystemGuard 防護已啓用，並按一下 [進階]。

2 從清單中選取 SystemGuard 類型。

- **程式 SystemGuard**
- **Windows SystemGuard**

- **瀏覽器 SystemGuard**

3 在 [我要] 之下，執行下列其中一項動作：

- 若要對與程式、Windows 及瀏覽器 SystemGuard 相關的未經授權登錄與檔案變更進行偵測、記錄與報告，請按一下 [顯示警示]。
- 若要對與程式、Windows 及瀏覽器 SystemGuard 相關的未經授權登錄與檔案變更進行偵測與記錄，請按一下 [僅記錄變更]。
- 若要停用與程式、Windows 及瀏覽器 SystemGuard 相關之未經授權登錄與檔案變更的偵測，請按一下 [停用 SystemGuard]。

附註：如需 SystemGuard 類型的詳細資訊，請參閱＜關於 SystemGuard 類型＞(第 43 頁)。

關於 SystemGuard 類型

SystemGuard 會偵測對電腦登錄及其他對 Windows 極爲重要之必要檔案所進行的可能未經授權變更。有三種 SystemGuard 類型：程式 SystemGuard、Windows SystemGuard 與瀏覽器 SystemGuard。

程式 SystemGuard

當 Windows 啓動時，程式 SystemGuard 技術除了會停止可自動啓動的間諜軟體與潛在的無用程式之外，還能停止可疑的 ActiveX 程式 (下載自網際網路)。

SystemGuard	偵測...
ActiveX 安裝	對「ActiveX 安裝」的登錄進行未經授權的變更，可能會損壞您的電腦、危害其安全性並毀損極爲重要的系統檔案。
啓動項目	間諜軟體、廣告軟體和其他潛在的無用程式會針對「啓動」項目安裝檔案變更，以便在啓動電腦時執行可疑的程式。
Windows Shell 執行攔截	間諜軟體、廣告軟體和其他潛在的無用程式會安裝「Windows Shell 執行攔截」，以阻礙安全性程式正常執行。
Shell 服務物件延遲載入	間諜軟體、廣告軟體和其他潛在的無用程式會對「Shell 服務物件延遲載入」的登錄進行變更，以便在啓動電腦時執行有害的檔案。

Windows SystemGuard

Windows SystemGuard 技術可協助保護您的電腦，避免透過網際網路傳送與接收未經授權的資訊或個人資訊。它還可以協助停止可疑的程式，這些程式可能會對您及您家庭之重要程式的外觀與運作方式進行不必要的變更。

SystemGuard	偵測...
內容功能表處理程式	對「Windows 內容功能表處理程式」的登錄進行未經授權的變更，可能會影響 Windows 功能表的外觀與運作方式。內容功能表可讓您在電腦上執行某些動作，例如用滑鼠右鍵按一下檔案。
AppInit DLLs	對 Windows AppInit_DLLs 的登錄進行未經授權的變更，可能會在啓動電腦時執行可能有害的檔案。
Windows 主機檔案	間諜軟體、廣告軟體和潛在的無用程式會在您的 Windows 主機檔案中進行未經授權的變更，以便將您的瀏覽器重新導向至可疑的網站，並封鎖軟體更新。
Winlogon Shell	間諜軟體、廣告軟體和其他潛在的無用程式會對 Winlogon Shell 的登錄進行變更，以便讓其他程式取代 Windows 檔案總管。
Winlogon User Init	間諜軟體、廣告軟體和其他潛在的無用程式會對 Winlogon User Init 的登錄進行變更，以便在您登入 Windows 時執行可疑的程式。
Windows 通訊協定	間諜軟體、廣告軟體和其他潛在的無用程式會對「Windows 通訊協定」的登錄進行變更，以影響您的電腦在網際網路上傳送與接收資訊的方式。
Winsock 階層服務提供者	間諜軟體、廣告軟體和其他潛在的無用程式會對「Winsock 階層服務提供者 (LSP)」安裝登錄變更，以攔截並變更您在網際網路上傳送與接收的資訊。
Windows Shell Open Command	對 Windows Shell Open Command 進行未經授權的變更，可能會讓蠕蟲及其他有害程式在您的電腦上執行。
共用工作排程器	間諜軟體、廣告軟體和其他潛在的無用程式會對「共用工作排程器」的登錄與檔案進行變更，以便在啓動電腦時執行可能有害的檔案。
Windows Messenger Service	間諜軟體、廣告軟體和其他潛在的無用程式會對 Windows Messenger Service 的登錄進行變更，以便讓未經許可的廣告與遠端執行的程式進入您的電腦。
Windows Win.ini 檔案	間諜軟體、廣告軟體和其他潛在的無用程式會對 Win.ini 檔案進行變更，以便在啓動電腦時執行可疑的程式。

瀏覽器 SystemGuard

瀏覽器 SystemGuard 技術可協助防止未經授權的瀏覽器活動，例如重新導向至可疑的網站、在您不知情的情況下變更瀏覽器設定值與選項，以及信任可疑網站。

SystemGuard	偵測...
瀏覽器協助程式物件	間諜軟體、廣告軟體和其他潛在的無用程式會使用瀏覽器協助程式物件，以追蹤 Web 瀏覽並顯示未經許可的廣告。
Internet Explorer 列	對 Internet Explorer 工具列程式 (例如 [搜尋] 和 [我的最愛]) 的登錄進行未經授權的變更，可能會影響 Internet Explorer 的外觀與運作方式。
Internet Explorer 附加元件	間諜軟體、廣告軟體和其他潛在的無用程式會安裝 Internet Explorer 附加元件，以追蹤 Web 瀏覽並顯示未經許可的廣告。
Internet Explorer ShellBrowser	對 Internet Explorer Shell Browser 的登錄進行未經授權的變更，可能會影響 Web 瀏覽器的外觀與運作方式。
Internet Explorer WebBrowser	對 Internet Explorer Web 瀏覽器的登錄進行未經授權的變更，可能會影響您瀏覽器的外觀與運作方式。
Internet Explorer URL 搜尋攔截	間諜軟體、廣告軟體和其他潛在的無用程式會對「Internet Explorer URL 搜尋攔截」的登錄進行變更，以便在您搜尋 Web 時將您的瀏覽器重新導向至可疑的網站。
Internet Explorer URL	間諜軟體、廣告軟體和其他潛在的無用程式會對 Internet Explorer URL 的登錄進行變更，以影響瀏覽器設定。
Internet Explorer 限制	間諜軟體、廣告軟體和其他潛在的無用程式會對「Internet Explorer 限制」的登錄進行變更，以影響瀏覽器設定與選項。
Internet Explorer 安全區域	間諜軟體、廣告軟體和其他潛在的無用程式會對「Internet Explorer 安全區域」的登錄進行變更，以便在啓動電腦時執行可能有害的檔案。
Internet Explorer 信任的網站	間諜軟體、廣告軟體和其他潛在的無用程式會對「Internet Explorer 信任的網站」的登錄進行變更，以便讓瀏覽器信任可疑的網站。
Internet Explorer 政策	間諜軟體、廣告軟體和其他潛在的無用程式會對「Internet Explorer 政策」的登錄進行變更，以便影響瀏覽器的外觀與運作方式。

使用信任的清單

若 VirusScan 偵測到一個檔案或登錄變更 (SystemGuard)、程式或緩衝區溢位，會提示您信任或移除該變更。若您信任該項目並表示不要收到有關其活動未來的通知，該項目將會新增至信任的清單，且 VirusScan 不會再對該項目進行偵測或通知您其活動的相關資訊。若某項目已新增至信任清單，但您決定要封鎖其活動，您可以這麼做。封鎖可防止該項目在未告知您的情況下企圖執行或對您的電腦進行任何變更。您也可將某個項目從信任的清單移除。移除可讓 VirusScan 再次偵測該項目的活動。

管理信任的清單

使用 [信任清單] 窗格以信任先前受到偵測的項目，或封鎖先前受到信任的項目。您也可將某個項目從信任的清單移除，如此 VirusScan 便可以再次進行偵測。

1 開啓 [信任清單] 窗格。

如何辦到？

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [電腦與檔案]。
3. 於 [電腦與檔案] 資訊區域中，按一下 [設定]。
4. 在 [電腦與檔案設定] 窗格上，確定病毒防護已啓用，並按一下 [進階]。
5. 按一下 [病毒防護] 窗格中的 [信任清單]。

2 選取下列其中一個信任清單類型：

- **程式 SystemGuard**
- **Windows SystemGuard**
- **瀏覽器 SystemGuard**
- **信任的程式**
- **信任的緩衝區溢位**

3 在 [我要] 之下，執行下列其中一項動作：

- 若要讓偵測到的項目可以對您電腦上的 Windows 登錄或重要系統檔案進行變更而不需通知您，請按一下 [信任]。
- 若要封鎖偵測到的項目以防止其對您電腦上的 Windows 登錄或重要系統檔案進行變更而不通知您，請按一下 [封鎖]。
- 若要從信任的清單中移除偵測到的項目，請按一下 [移除]。

4 按一下 [確定]。

附註：如需信任清單類型的詳細資訊，請參閱<關於信任清單類型>(第 47 頁)。

關於信任清單類型

[信任清單] 窗格上的 SystemGuard 表示，VirusScan 先前已偵測到未經授權登錄與檔案變更，但您已從警示或 [掃描結果] 窗格選擇允許。有五種您可在 [信任清單] 窗格上進行管理的信任清單類型：程式 SystemGuard、Windows SystemGuard、瀏覽器 SystemGuard、信任的程式與信任的緩衝區溢位。

選項	說明
程式 SystemGuard	[信任清單] 窗格上的程式 SystemGuard 表示，VirusScan 先前已偵測到未經授權登錄與檔案變更，但您已從警示或 [掃描結果] 窗格選擇允許。 程式 SystemGuard 偵測到與 ActiveX 安裝、啓動項目、Windows shell 執行攔截及 Shell 服務物件延遲載入活動相關的未經授權登錄與檔案變更。這些未經授權的登錄與檔案變更類型可能會損壞您的電腦、危害其安全性並毀損極爲重要的系統檔案。
Windows SystemGuard	[信任清單] 窗格上的 Windows SystemGuard 表示，VirusScan 先前已偵測到未經授權登錄與檔案變更，但您已從警示或 [掃描結果] 窗格選擇允許。 Windows SystemGuard 偵測到與內容功能表處理程式、appInit DLL、Windows 主機檔案、Winlogon Shell、Winsock 階層服務提供者 (LSP) 等相關的未經授權登錄與檔案變更。這類未經授權登錄與檔案變更可能會影響您的電腦在網際網路上傳送與接收資訊的方法、變更程式的外觀與運作方式，並讓可疑的程式在您的電腦上執行。
瀏覽器 SystemGuard	[信任清單] 窗格上的瀏覽器 SystemGuard 表示，VirusScan 先前已偵測到未經授權登錄與檔案變更，但您已從警示或 [掃描結果] 窗格選擇允許。 瀏覽器 SystemGuard 偵測到與瀏覽器協助程式物件、Internet Explorer 附加元件、Internet Explorer URL 與 Internet Explorer 安全區域等相關的未經授權登錄變更與其他不需要的運作方式。這類未經授權登錄變更可能造成不想要的瀏覽器活動，例如重新導向至可疑的網站、變更瀏覽器設定值與選項，以及信任可疑的網站。
信任的程式	信任的程式爲 VirusScan 先前所偵測到的潛在的無用程式，但您已從警示或從 [掃描結果] 窗格選擇信任。

選項	說明
信任的緩衝區溢位	信任緩衝區溢位表示 VirusScan 先前偵測到的可能不需要的活動，但您已從警示或 [掃描結果] 窗格選擇信任。 緩衝區溢位可能會損害您的電腦並毀損檔案。當可疑的程式或程序儲存於緩衝區的資料量超過緩衝區容量時，就會發生緩衝區溢位。

第 11 章

掃描您的電腦

當您首次啓動 SecurityCenter 時，VirusScan 的即時病毒防護便會開始保護您的電腦，避免可能有害的病毒、特洛伊病毒及其他安全性威脅的攻擊。除非您停用即時病毒防護，VirusScan 會持續監視您電腦的病毒活動、在您或您的電腦每次存取檔案時掃描檔案、使用您設定的即時掃描選項。爲確保您的電腦持續受到保護以對抗最新的安全性威脅，請開啓即時病毒防護並設定排程，以進行定期且更完整的手動掃描。如需設定即時與手動掃描選項的詳細資訊，請參閱＜設定病毒防護＞(第 35 頁)。

VirusScan 提供一組更詳細的掃描選項供手動病毒防護使用，可讓您定期執行更廣泛的掃描。您可以從 SecurityCenter 執行手動掃描，依據設定排程鎖定特定位置。然而，您也可以在工作時，直接在 Windows 檔案總管中執行手動掃描。SecurityCenter 中的掃描提供在運作中即時變更掃描選項的優勢。但是，Windows 檔案總管的掃描對電腦安全性提供一個便利的方法。

無論您是從 SecurityCenter 或 Windows 檔案總管執行手動掃描，您都可以在掃描結束時檢視掃描結果。您可以檢視掃描結果，以決定 VirusScan 是否要對病毒、特洛依病毒、間諜軟體、廣告軟體、Cookie 及其他潛在的無用程式進行偵測、修復或隔離。掃描結果可以不同方式顯示。例如，您可檢視掃描結果的基本摘要或詳細資訊，例如感染狀態與類型。您也可以檢視一般掃描與偵測統計資料。

在本章中

掃描電腦.....49
檢視掃描結果.....50

掃描電腦

您可從 SecurityCenter 中的 [進階] 或 [基本] 功能表執行手動掃描。若從 [進階] 功能表執行掃描，您可於掃描之前確認手動掃描選項。若從 [基本] 功能表執行掃描，VirusScan 會使用現有的掃描選項，立即開始掃描。您還可以使用現有的掃描選項，於 Windows 檔案總管中執行掃描。

- 執行下列其中一項：

  在 SecurityCenter 中掃描

若要...	執行此動作...
使用現有的設定進行掃描	按一下 [基本功能表] 上的 [掃描]。
使用變更的設定進行掃描	按一下 [進階功能表] 上的 [掃描]，依序選取要掃描的位置與掃描選項，然後按一下 [立即掃描]。

在 Windows 檔案總管中掃描

1. 開啓 Windows 檔案總管。
2. 在檔案、資料夾或磁碟機上按一下滑鼠右鍵，然後按一下 [掃描]。

附註：掃描結果會顯示於「掃描已完成」的警示中。結果中包含已進行掃描、偵測、修復、隔離及移除的項目數量。按一下 [檢視掃描的詳細資料]，可以瞭解掃描結果或處理感染項目的相關資訊。

檢視掃描結果

當手動掃描結束時，您可以檢視結果以判斷掃描所找到的項目，並分析電腦目前的保護狀態。掃描結果會告訴您 VirusScan 是否已偵測、修復或隔離病毒、特洛依病毒、間諜軟體、廣告軟體、Cookie 及其他潛在的無用程式。

- 在 [基本功能表] 或 [進階功能表] 上，按一下 [掃描]，然後執行下列其中一項工作：

若要...	執行此動作...
檢視警示中的掃描結果	在「掃描已完成」的警示中檢視掃描結果。
檢視有關掃描結果的更多資訊	按一下「掃描已完成」警示中的 [檢視掃描的詳細資料]。
檢視掃描結果的快速摘要	指向您工作列通知區域中的 [掃描已完成] 圖示。
檢視掃描與偵測統計資料	按兩下您工作列通知區域中的 [掃描已完成] 圖示。
檢視已偵測項目、感染狀態與類型的相關詳細資料。	按兩下您工作列通知區域中的 [掃描已完成] 圖示，然後按一下 [掃描進度] 上的 [檢視結果]：[手動掃描] 窗格。

第 12 章

使用掃描結果

在執行即時或手動掃描時，若 VirusScan 偵測到一個安全性威脅，會依據威脅類型來嘗試自動處理威脅。例如，若 VirusScan 在您的電腦上偵測到病毒、特洛伊病毒或追蹤 Cookie，其會嘗試清除受感染的檔案。若無法清除檔案，則 VirusScan 會進行隔離。

由於某些安全性威脅，VirusScan 可能無法順利地清除或隔離檔案。在這種情況中，VirusScan 會提示您處理威脅。您可依威脅類型，採取不同的行動。例如，若於檔案中偵測到病毒，但 VirusScan 無法順利地清除或隔離該檔案，則將拒絕對其進一步的存取。若偵測到追蹤 Cookie，但 VirusScan 無法順利地清除或隔離該 Cookie，則您可決定是否移除或信任該 Cookie。若偵測到潛在的無用程式，VirusScan 不會自動採取任何行動，而是讓您決定是否隔離或信任該程式。

當 VirusScan 隔離項目時，它會進行加密並將其隔離於資料夾中，以防止檔案、程式或 Cookie 損害您的電腦。您可以還原或移除隔離的項目。在大多數情況下，您可刪除隔離的 Cookie 而不會影響您的系統，但是，若 VirusScan 已對您認得且使用的程式進行隔離，則請考慮將其還原。

在本章中

處理病毒及特洛伊病毒.....51
處理潛在的無用程式.....52
處理隔離的檔案.....52
處理隔離的程式與 Cookie.....53

處理病毒及特洛伊病毒

若 VirusScan 於即時掃描或手動掃描期間，在您的電腦上偵測到病毒或特洛伊病毒，它會嘗試清除該檔案。若無法清除檔案，則 VirusScan 會試著進行隔離。若此動作也失敗，則會拒絕存取該檔案 (僅適用於即時掃描)。

1 開啓 [掃描結果] 窗格。

如何辦到？

1. 按兩下您工作列最右方之通知區域中的 [掃描已完成] 圖示。
2. 在 [掃描進度] 上：在 [手動掃描] 窗格中，按一下 [檢視結果]。

2 於掃描結果清單中，按一下 [病毒及特洛伊病毒]。

附註：若要處理 VirusScan 已隔離的檔案，請參閱＜處理隔離的檔案＞(第 52 頁)。

處理潛在的無用程式

若 VirusScan 於即時掃描或手動掃描期間，在您的電腦上偵測到潛在的無用程式，您可以移除或信任該程式。移除潛在的無用程式並不會真的將其從您的系統中刪除。而是隔離該程式以防止其對您的電腦或檔案造成損害。

1 開啓 [掃描結果] 窗格。

如何辦到？

1. 按兩下您工作列最右方之通知區域中的 [掃描已完成] 圖示。
2. 在 [掃描進度] 上：在 [手動掃描] 窗格中，按一下 [檢視結果]。

2 於掃描結果清單中，按一下 [潛在的無用程式]。

3 選取一個潛在的無用程式。

4 在 [我要] 之下，按一下 [移除] 或 [信任]。

5 請確認您選取的選項。

處理隔離的檔案

當 VirusScan 隔離感染檔案時，其會進行加密並將檔案移至資料夾中，以防止檔案損害您的電腦。之後，您可以還原或移除隔離檔案。

1 開啓 [隔離檔案] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [還原]。
3. 按一下 [檔案]。

2 選取隔離的檔案。

3 執行下列其中一項：

- 若要修復感染的檔案，並將其送回原來在您電腦的位置，請按一下 [還原]。

- 若要將感染的檔案從您的電腦移除，請按一下 [移除]。

4 按一下 [是] 以確認您選取的選項。

秘訣：您可以同時還原或移除多個檔案。

處理隔離的程式與 Cookie

當 VirusScan 隔離潛在的無用程式或追蹤 Cookie 時，它會進行加密並將其移至受保護的資料夾中，以防止程式或 Cookie 損害您的電腦。之後，您可以還原或移除隔離的項目。在大多數情況下，您可刪除隔離的項目而不會影響您的系統。

1 開啓 [隔離的程式及追蹤 Cookie] 窗格。

如何辦到？

1. 按一下左窗格中的 [進階功能表]。
2. 按一下 [還原]。
3. 按一下 [程式及 Cookie]。

2 選取隔離的程式或 Cookie。

3 執行下列其中一項：

- 若要修復感染的檔案，並將其送回原來在您電腦的位置，請按一下 [還原]。
- 若要將感染的檔案從您的電腦移除，請按一下 [移除]。

4 按一下 [是] 以確認操作。

秘訣：您可以同時還原或移除多個程式與 Cookie。

第 13 章

McAfee Personal Firewall

Personal Firewall 爲您的電腦和個人資料提供進階保護。Personal Firewall 在您的電腦與網際網路之間建立了障礙，秘密監視網際網路流量中是否有可疑的活動。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

Personal Firewall 功能 56
啓動防火牆 59
使用警示 61
管理資訊警示 63
設定防火牆保護 65
管理程式及權限 75
管理系統服務 83
管理電腦連線 89
記錄、監視及分析 97
瞭解網際網路安全性 107

Personal Firewall 功能

Personal Firewall 提供下列功能。

標準及自訂保護等級

使用 Firewall 的預設值或可自訂的保護設定，來抵抗入侵及可疑的活動。

即時建議

積極的接收建議可幫助您判斷是否要將網際網路存取權授與程式或是否要信任網路流量。

程式的智慧型存取管理

透過警示及事件記錄檔來管理程式的網際網路存取，並設定特定程式的存取權限。

遊戲保護

在全螢幕的模式下進行遊戲時，防止入侵嘗試及可疑活動的警示干擾您。

電腦啓動保護

當 Windows® 一啓動時，Firewall 會立即保護您的電腦避免入侵嘗試及無用程式和網路流量的攻擊。

系統服務通訊埠控制

管理某些程式需要之開啓及關閉的系統服務連接埠。

管理電腦連線

允許和封鎖其他電腦與您電腦之間的遠端連線。

HackerWatch 資訊整合

透過 HackerWatch 的網站追蹤全球的駭客活動及入侵嘗試，也會提供關於電腦上程式的最新安全性資訊，以及全球安全性事件和網際網路連接埠統計資料。

鎖定 Firewall

會立即封鎖電腦和網際網路之間的所有入埠和出埠流量。

還原 Firewall

立即還原 Firewall 的原始保護設定。

進階特洛伊病毒偵測

偵測及封鎖可能的惡意應用程式 (如特洛伊病毒)，阻止它們將您的個人資料轉送到網際網路。

事件記錄

追蹤最近的入埠、出埠及入侵事件。

監視網際網路流量

檢閱顯示惡意攻擊與流量之來源的全球地圖。此外，可尋找起始 IP 位址的擁有者詳細資訊及地理位置資料。同時分析入埠及出埠流量、監視程式頻寬及程式活動。

入侵保護

保護您的隱私，以抵禦可能的網際網路威脅。McAfee 使用啓發式功能，透過封鎖顯示攻擊徵兆或入侵企圖特徵的項目，提供第三層保護。

精密的流量分析

同時檢閱入埠及出埠網際網路流量與程式連線，包含正積極接聽開放連線的連線。這可讓您看到容易遭到入侵的程式並對其採取行動。

第 14 章

啓動防火牆

一旦安裝防火牆，就會保護您的電腦避免入侵以及無用的網路流量。此外，您還可以處理警示，並管理已知或不明程式的入埠及出埠網際網路存取。[自動建議] 及 [信任] 安全性等級 (已選取只允許程式進行出埠網際網路存取的選項) 會自動啓用。

雖然您可以從 [網際網路與網路設定] 窗格停用防火牆，但是停用後將不再繼續保護電腦避免入侵及無用的網路流量，而且也將無法有效管理入埠及出埠的網際網路連線。如果必須停用防火牆保護，請只在需要時暫時停用。您也可以從 [網際網路與網路設定] 窗格啓用防火牆。

Firewall 會自動停用 Windows® 防火牆，並將自己設爲預設防火牆。

附註：若要設定 Firewall，請開啓 [網際網路與網路設定] 窗格。

在本章中

啓動防火牆保護.....59
停止防火牆保護.....59

啓動防火牆保護

您可以啓用 Firewall 來保護您的電腦避免受到入侵以及無用的網路流量，以及管理入埠及出埠的網際網路連線。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已停用防火牆保護] 底下，按一下 [開啓]。

停止防火牆保護

如果您不想保護電腦避免受到入侵及無用的網路流量，可停用 Firewall。停用防火牆時，您將無法管理入埠或出埠的網際網路連線。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [關閉]。

第 15 章

使用警示

防火牆使用一系列警示，協助您管理安全性。這些警示可分成三種基本類型：

- 紅色警示
- 黃色警示
- 綠色警示

警示也可能包含下列用途的資訊：協助您決定如何處理警示，或取得在您電腦上執行之程式的相關資訊。

在本章中

關於警示.....62

關於警示

防火牆具有三個基本警示類型。有些警示包含的資訊也可協助您瞭解或取得在您電腦上執行之程式的相關資訊。

紅色警示

當 Firewall 在您電腦上偵測到特洛伊病毒時，會出現紅色警示並封鎖特洛伊病毒，然後建議您掃描其他威脅。特洛伊病毒看似合法的程式，卻會干擾、損壞您的電腦，以及提供未經授權的存取電腦管道。這個警示會發生在每一種安全性等級，但 [開放] 除外。

黃色警示

最常見的警示類型是黃色警示，它會通知您 Firewall 偵測到的程式活動或網路事件。發生黃色警示時，該警示會說明程式活動或網路事件，然後提供您一或多個需要回應的選項。例如，當已安裝 Firewall 的電腦連線至新網路時，[偵測到新網路] 警示便會出現。您可以選擇信任或不信任網路。如果信任網路，防火牆將允許來自網路上任何電腦的流量，並會新增至 [信任的 IP 位址]。如果已啓用 [自動建議]，則程式會新增至 [程式權限] 窗格。

綠色警示

在大多數的情況下，綠色警示會提供事件的基本相關資訊，且不需要回應。綠色警示預設是停用的，且在設定 [標準]、[信任]、[嚴密] 及 [秘密] 安全性等級時，通常會出現綠色警示。

使用者幫助

許多防火牆警示包含其他可協助您管理電腦安全性的資訊，包括：

- **深入瞭解有關此程式的資訊**：啓動 McAfee 的全球安全性網站，取得防火牆在您電腦上偵測到的程式的相關資訊。
- **通知 McAfee 關於此程式的資訊**：將防火牆在您電腦上偵測到的不明檔案的相關資訊傳送至 McAfee。
- **McAfee 建議**：有關處理警示的建議。例如，警示可能會建議您允許程式存取。

第 16 章

管理資訊警示

Firewall 能讓您在它於特定事件期間 (例如，以全螢幕方式進行遊戲時) 偵測到入侵嘗試或可疑活動時，顯示或隱藏資訊警示。

在本章中

玩遊戲時顯示警示.....63
隱藏資訊警示.....63

玩遊戲時顯示警示

您可以允許 Firewall 在您以全螢幕方式進行遊戲期間，在偵測到入侵嘗試或可疑活動時顯示資訊警示。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [設定]。
3. 在 [SecurityCenter 設定] 窗格上，按一下 [警示] 下的 [進階]。
4. 在 [警示選項] 窗格上，選擇 [偵測到遊戲模式時，顯示資訊警示]。
5. 按一下 [確定]。

隱藏資訊警示

您可以防止 Firewall 在偵測到入侵嘗試或可疑的活動時，顯示資訊警示。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [設定]。
3. 在 [SecurityCenter 設定] 窗格上，按一下 [警示] 下的 [進階]。
4. 在 [SecurityCenter 設定] 窗格上，按一下 [資訊警示]。
5. 在 [資訊警示] 窗格上，執行下列其中一項動作：
   - 選取 [請勿顯示資訊警示]，隱藏所有資訊警示。
   - 清除要隱藏的警示。
6. 按一下 [確定]。

第 17 章

設定防火牆保護

防火牆提供一些方法，讓您管理安全性，以及設計您想要回應安全性事件及警示的方式。

在第一次安裝防火牆之後，電腦的保護安全性等級會設爲 [信任]，而且您的程式只可進行出埠的網際網路存取。但是，防火牆還提供其他等級，其範圍從完全限制到完全允許。

防火牆也讓您有機會接收有關警示及程式之網際網路存取權的建議。

在本章中

管理防火牆安全性等級 66
設定警示的 [自動建議] 70
最佳化防火牆安全性 72
鎖定及還原防火牆 74

管理防火牆安全性等級

Firewall 的安全性等級會控制您要管理及回應警示的程度。當 Firewall 偵測到無用的網路流量以及入埠與出埠的網際網路連線時，這些警示就會出現。Firewall 的安全性等級預設會設爲 [信任]，並只具有出埠存取權。

設爲 [信任] 安全性等級且啓用 [自動建議] 時，黃色警示會提供選項，讓您允許或封鎖需要入埠存取的不明程式存取權。當偵測到已知的程式時，綠色資訊警示即會出現，並自動允許存取權。允許存取權可讓程式建立出埠連線，並監聽來路不明的連入連線。

通常，安全性等級越嚴格 (如 [秘密] 及 [嚴密])，所顯示且必須由您處理的選項數及警示數就越多。

下表說明 Firewall 的六個安全性等級，從最嚴格到最寬鬆：

等級	說明
鎖定	封鎖所有的入埠與出埠網路連線，包含對網站、電子郵件及安全性更新的存取。這個安全性等級的效果相當於移除您的網際網路連線。您可以使用這個設定，來封鎖您在 [系統服務] 窗格上設定爲開放的連接埠。
秘密	封鎖所有入埠網際網路連線 (開放的連接埠除外)，並隱藏您電腦在網際網路上的位置。防火牆會在新程式嘗試進行出埠網際網路連線，或收到入埠連線要求時警示您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。
嚴密	在新程式嘗試進行出埠網際網路連線，或收到入埠連線要求時警示您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。當安全性等級設爲 [嚴密] 時，程式只會要求當時所需的存取權類型，例如限出埠存取權，您可以允許或封鎖此存取權。稍後，如果程式同時需要入埠及出埠連線，您可以從 [程式權限] 窗格允許程式的完整存取。
標準	監視入埠與出埠連線，並在新程式嘗試存取網際網路時警示您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。
信任	允許程式具有入埠及出埠 (完整) 存取權，或限出埠網際網路存取權。預設安全性等級是 [信任]，且已選取允許程式具有限出埠存取權的選項。 如果允許程式具有完整存取權，則 Firewall 會自動信任它，並將它新增到 [程式權限] 窗格上允許的程式清單中。 如果允許程式具有限出埠存取權，則 Firewall 只有在程式進行出埠網際網路連線時才自動信任它。不會自動信任入埠連線。
開放	允許所有入埠及出埠網際網路連線的存取權。

Firewall 也可讓您從 [還原防火牆保護預設值] 窗格，立即將安全性等級重設爲 [信任] (並允許限出埠存取權)。

將安全性等級設爲［鎖定］

您可以將 Firewall 的安全性等級設爲 [鎖定]，以封鎖所有入埠與出埠網路連線。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格上移動滑桿，讓 [鎖定] 顯示爲目前的等級。
4. 按一下 [確定]。

將安全性等級設爲［秘密］

您可以將 Firewall 將安全性等級設爲 [秘密]，以封鎖所有入埠網際網路連線 (開放的通訊埠除外)，並隱藏您電腦在網際網路上的位置。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格上移動滑桿，讓 [秘密] 顯示爲目前的等級。
4. 按一下 [確定]。

附註：在 [秘密] 模式中，Firewall 會在新程式要求進行出埠網際網路連線或接收入埠連線要求時警示您。

將安全性等級設爲［嚴密］

您可以將 Firewall 的安全性等級設爲 [嚴密]，以在新程式嘗試進行出埠網際網路連線或接收入埠連線要求時收到警示。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [安全性等級] 窗格上移動滑桿，讓 [嚴密] 顯示爲目前的等級。

4 按一下 [確定]。

附註：在 [嚴密] 模式中，程式只會要求當時所需的存取權類型，例如限出埠存取權，您可以允許或封鎖此存取權。稍後，如果程式同時需要入埠及出埠連線，您可以從 [程式權限] 窗格將完整存取權賦予程式。

將安全性等級設爲［標準］

您可以將安全性等級設爲 [標準]，以監視入埠及出埠連線，並在新程式嘗試存取網際網路時警示您。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [安全性等級] 窗格上移動滑桿，讓 [標準] 顯示爲目前的等級。

4 按一下 [確定]。

將安全性等級設爲［信任］

您可以將 Firewall 的安全性等級設爲 [信任]，以允許完整存取權或限出埠網路存取權。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [安全性等級] 窗格上移動滑桿，讓 [信任] 顯示爲目前的等級。

4 執行下列其中一項：

- 若要允許完整入埠及出埠網路存取權，請選取 [允許完整存取]。
- 若要允許限出埠網路存取權，請選取 [允許限出埠存取]。

5　按一下 [確定]。

附註：[允許限出埠存取] 是預設選項。

將安全性等級設爲 [開放]

您可以將 Firewall 的安全性等級設爲 [開放]，以允許所有入埠與出埠網路連線。

1　在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2　在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3　在 [安全性等級] 窗格上移動滑桿，讓 [開放] 顯示爲目前的等級。

4　按一下 [確定]。

設定警示的 [自動建議]

您可以將 Firewall 設爲，當任何程式嘗試存取網際網路時，在警示中包含、排除或顯示建議。啓用 [自動建議] 可協助您決定如何處理警示。

當啓用 [自動建議] (且安全性等級設爲 [信任]，並已啓用限出埠存取權) 時，Firewall 會自動允許或封鎖已知的程式，並在偵測到可能有危險的程式時，在警示中顯示建議。

停用 [自動建議] 時，Firewall 既不會允許或封鎖網際網路存取權，也不會在警示中建議動作計劃。

當 [自動建議] 設爲 [僅供顯示] 時，會有一個警示提示您允許或封鎖存取權，不過是在警示中建議動作計劃。

啓用自動建議

您可以啓用 Firewall 的 [自動建議]，自動允許或封鎖程式，並在發現無法辨識和可能有危險的程式時，向您發出警示。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格的 [自動建議] 下，選取 [啓用自動建議]。
4. 按一下 [確定]。

停用自動建議

您可以停用 Firewall 的 [自動建議]，不要允許或封鎖程式，也不要在發現無法辨識和可能有危險的程式時，向您發出警示。但是，警示會排除有關處理程式存取權的任何建議。如果 Firewall 偵測到可疑或是已知可能是威脅的新程式，它會自動封鎖程式存取網際網路。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格的 [自動建議] 下，選取 [停用自動建議]。
4. 按一下 [確定]。

僅顯示自動建議

您可以顯示警示的 [自動建議]，使其只提供動作計劃的建議，如此您可決定要允許或封鎖無法辨識和可能有危險的程式。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格的 [自動建議] 下，選取 [僅供顯示]。
4. 按一下 [確定]。

最佳化防火牆安全性

有許多可能會危及電腦安全性的方式。例如，有些程式會嘗試在 Windows® 啓動之前連線至網際網路。此外，經驗老道的電腦使用者可以追蹤 (或 Ping) 您的電腦，以判斷它是否已連線至網路。Firewall 可讓您藉由啓用啓動保護及封鎖 Ping 要求，應付這兩種類型的入侵。第一個設定會在 Windows 啓動時封鎖程式，使其無法存取網際網路，而第二個設定則會封鎖 Ping 要求，因爲這種要求可協助其他使用者偵測您的電腦是否在網路上。

標準安裝設定包含自動偵測最常見的入侵嘗試，如拒絕服務攻擊或漏洞攻擊。使用標準安裝設定可確保免於這些攻擊及掃描的威脅；不過您可在 [入侵偵測] 窗格中停用一或多個攻擊或掃描的自動偵測。

啓動期間保護您的電腦

您可以在 Windows 啓動時封鎖新程式 (它們在啓動時不需要網際網路存取權，但現在需要)，藉以保護您的電腦。Firewall 會針對要求存取網際網路的程式顯示相關警示，您可以允許或封鎖其存取權。若要使用這個選項，您的安全性等級不得設爲 [開放] 或 [鎖定]。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格的 [安全性設定] 下，選取 [啓用啓動保護]。
4. 按一下 [確定]。

附註：啓用啓動保護時，不會記錄已封鎖的連線及入侵。

設定 Ping 要求設定

您可以允許或防止其他電腦使用者偵測您的電腦是否在網路上。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [安全性等級] 窗格的 [安全性設定] 下，執行下列其中一項動作：
   - 選取 [允許 ICMP Ping 要求]，允許使用 Ping 要求以偵測您的電腦是否在網路上。
   - 清除 [允許 ICMP Ping 要求]，防止使用 Ping 要求來偵測您的電腦是否在網路上。
4. 按一下 [確定]。

設定入侵偵測

您可以偵測入侵嘗試，避免您的電腦受到攻擊及未經授權的掃描。標準的 Firewall 設定包括自動偵測最常見的入侵嘗試，像是「拒絕服務」攻擊或入侵；不過，您可以停用一或多個攻擊或掃描的自動偵測。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [入侵偵測]。
4. 在 [偵測入侵嘗試] 下，執行下列其中一項動作：
   - 選取名稱以自動偵測攻擊或掃描。
   - 清除名稱以停用自動偵測攻擊或掃描。
5. 按一下 [確定]。

設定防火牆保護狀態設定

您可以設定 Firewall，略過您電腦上尚未向 SecurityCenter 報告的特定問題。

1. 在 [McAfee SecurityCenter] 窗格中，於 [SecurityCenter 資訊] 之下，按一下 [設定]。
2. 在 [SecurityCenter 設定] 窗格上，按一下 [保護狀態] 下的 [進階]。
3. 在 [略過的問題] 窗格中，選取下列一個或多個選項：
   - **已停用防火牆保護。**
   - **防火牆的安全性等級已設爲 [開放]。**
   - **防火牆服務未執行。**
   - **防火牆保護未安裝在您的電腦上。**
   - **您的 Windows 防火牆已停用。**
   - **出埠防火牆未安裝在您的電腦上。**
4. 按一下 [確定]。

鎖定及還原防火牆

「鎖定」會立即封鎖所有入埠和出埠的網路流量，以協助您隔離及疑難排解電腦上的問題。

立即鎖定防火牆

您可以鎖定 Firewall，立即封鎖電腦和網際網路間的所有網路流量。

1 在 [McAfee SecurityCenter] 窗格中，於 [常見工作] 之下，按一下 [鎖定防火牆]。

2 在 [鎖定防火牆] 窗格上，按一下 [鎖定]。

3 按一下 [是] 確認。

秘訣：您也可以鎖定 Firewall，方法是以滑鼠右鍵按一下工作列最右邊通知區域中的 SecurityCenter 圖示，然後按一下 [快速連結]，再按一下 [鎖定防火牆]。

立即解除鎖定防火牆

您可以取消鎖定 Firewall，立即允許電腦和網際網路間的所有網路流量。

1 在 [McAfee SecurityCenter] 窗格中，於 [常見工作] 之下，按一下 [鎖定防火牆]。

2 在 [啓用鎖定] 窗格上，按一下 [解除鎖定]。

3 按一下 [是] 確認。

還原防火牆設定

您可以迅速地將防火牆還原爲原始保護設定。此還原會將您的安全性等級重設爲 [信任]，並允許限出埠網路存取權、啓用 [自動建議]、還原 [程式權限] 窗格中的預設程式清單及其權限、移除信任的及禁止的 IP 位址，並還原系統服務、事件記錄檔設定，以及入侵偵測。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [還原防火牆預設值]。

2 在 [還原防火牆保護預設值] 窗格上，按一下 [還原預設值]。

3 按一下 [是] 確認。

秘訣：您也可以還原 Firewall 的預設值，方法是以滑鼠右鍵按一下工作列最右邊通知區域中的 SecurityCenter 圖示，然後按一下 [快速連結]，再按一下 [還原防火牆預設值]。

第 18 章

管理程式及權限

防火牆可讓您爲需要入埠及出埠網際網路存取權的現有程式與新程式管理及建立存取權。防火牆可讓您控制程式的完整存取權或限出埠存取權。您也可以封鎖程式的存取權。

在本章中

允許程式具有網際網路存取權 76
允許程式具有限出埠存取權 78
封鎖程式的網際網路存取權 79
移除程式的存取權 81
瞭解程式 82

允許程式具有網際網路存取權

有些程式 (如網際網路瀏覽器) 需要存取網際網路，才能正常運作。

防火牆可讓您使用 [程式權限] 頁面：

- 允許程式具有存取權
- 允許程式具有限出埠存取權
- 封鎖程式的存取權

您也可以從出埠事件及最近的事件記錄檔允許程式具有完整及限出埠網際網路存取權。

允許程式具有完整存取權

您可以允許您電腦上目前封鎖的程式具有完整的入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，選取具有 [已封鎖] 或 [限出埠存取] 的程式。
5. 在 [動作] 下，按一下 [允許存取權]。
6. 按一下 [確定]。

允許新程式具有完整存取權

您可以允許您電腦上的新程式具有完整的入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，按一下 [新增允許的程式]。
5. 在 [新增程式] 對話方塊上，瀏覽並選取您要新增的程式，然後按一下 [開啓]。

附註：如同現有的程式一樣，您可以選取剛新增的程式，然後在 [動作] 下，按一下 [允許限出埠存取] 或 [封鎖存取權]，以變更該程式的權限。

從最近的事件記錄檔允許完整存取權

您可以允許出現在 [最近的事件] 記錄檔中目前封鎖的程式具有完整的入埠及出埠網際網路存取權。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2 按一下 [報告與記錄檔]。
3 在 [最近的事件] 下，選取事件說明，然後按一下 [允取存取]。
4 在 [程式權限] 對話方塊中，按一下 [是] 以確認。

相關主題

- 檢視出埠事件 (第 99 頁)

從出埠事件記錄檔允許完整存取權

您可以允許出現在 [出埠事件] 記錄檔中目前封鎖的程式具有完整的入埠及出埠網際網路存取權。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2 按一下 [報告與記錄檔]。
3 在 [最近的事件] 下，按一下 [檢視記錄檔]。
4 按一下 [網際網路與網路]，然後按一下 [出埠事件]。
5 選取程式，並按一下 [我要] 下的 [允許存取權]。
6 在 [程式權限] 對話方塊中，按一下 [是] 以確認。

允許程式具有限出埠存取權

您電腦上有些程式需要出埠的網際網路存取權。防火牆可讓您將程式權限設爲允許限出埠的網際網路存取權。

允許程式具有限出埠存取權

您可以允許程式具有限出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，選取具有 [已封鎖] 或 [完整存取] 的程式。
5. 在 [動作] 下，按一下 [允許限出埠存取]。
6. 按一下 [確定]。

從最近的事件記錄檔允許限出埠存取權

您可以允許出現在 [最近的事件] 記錄檔中目前封鎖的程式具有限出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，選取事件說明，然後按一下 [允取限出埠存取]。
4. 在 [程式權限] 對話方塊中，按一下 [是] 以確認。

從出埠事件記錄檔允許限出埠存取權

您可以允許出現在 [出埠事件] 記錄檔中目前封鎖的程式具有限出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
4. 按一下 [網際網路與網路]，然後按一下 [出埠事件]。
5. 選取程式，並按一下 [我要] 下的 [允許限出埠存取]。
6. 在 [程式權限] 對話方塊中，按一下 [是] 以確認。

封鎖程式的網際網路存取權

防火牆可讓您封鎖程式，使其無法存取網際網路。請確保封鎖程式不會中斷您的網路連線或另一個需要存取網際網路才能正常運作的程式。

封鎖程式的存取權

您可以防止程式具有入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，選取具有 [完整存取] 或 [限出埠存取] 的程式。
5. 在 [動作] 下，按一下 [封鎖存取權]。
6. 按一下 [確定]。

封鎖新程式的存取權

您可以防止新程式具有入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，按一下 [新增封鎖的程式]。
5. 在 [新增程式] 對話方塊上，瀏覽並選取您要新增的程式，然後按一下 [開啓]。

附註：您可以選取剛新增的程式，然後在 [動作] 下，按一下 [允許限出埠存取] 或 [允取存取]，以變更該程式的權限。

從最近的事件記錄檔封鎖存取權

您可以防止出現在 [最近的事件] 記錄檔中的程式具有入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，選取事件說明，然後按一下 [封鎖存取權]。
4. 在 [程式權限] 對話方塊中，按一下 [是] 以確認。

移除程式的存取權

移除程式權限之前，請確定沒有該權限並不會影響您的電腦功能或網路連線。

移除程式權限

您可以移除程式，不讓它具有任何入埠及出埠網際網路存取權。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，選取一個程式。
5. 在 [動作] 下，按一下 [移除程式權限]。
6. 按一下 [確定]。

附註：防火牆會藉由將某些動作變灰及停用特定動作，來防止您修改某些程式。

瞭解程式

如果不確定要套用哪一個程式權限，您可以在 McAfee 的 HackerWatch 網站上取得程式的相關資訊。

取得程式資訊

您可以從 McAfee 的 HackerWatch 網站取得程式資訊，來決定要允許或封鎖入埠及出埠網際網路存取權。

附註：請確定您已連線至網際網路，讓瀏覽器能夠啓動 McAfee 的 HackerWatch 網站，這個網站會提供有關程式、網際網路存取需求及安全性威脅的最新資訊。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [程式權限]。
4. 在 [程式權限] 下，選取一個程式。
5. 在 [動作] 下，按一下 [深入瞭解]。

從出埠事件記錄檔取得程式資訊

從 [出埠事件] 記錄檔，您可以從 McAfee 的 HackerWatch 網站取得程式資訊，來決定要允許或封鎖哪些程式具有入埠及出埠網際網路存取權。

附註：請確定您已連線至網際網路，讓瀏覽器能夠啓動 McAfee 的 HackerWatch 網站，這個網站會提供有關程式、網際網路存取需求及安全性威脅的最新資訊。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下選取事件，然後按一下 [檢視記錄]。
4. 按一下 [網際網路與網路]，然後按一下 [出埠事件]。
5. 選取 IP 位址，然後按一下 [深入瞭解]。

第 19 章

管理系統服務

若要正常運作，某些程式 (包括 Web 伺服器和檔案共用伺服器程式) 必須透過指定的系統服務通訊埠接受來自其他電腦之來路不明的連線。通常，防火牆會關閉這些系統服務通訊埠，因爲它們最有可能造成您系統的不安全。但是，若要接受來自遠端電腦的連線，就必須開放系統服務通訊埠。

在本章中

設定系統服務通訊埠.....84

設定系統服務通訊埠

可以設定系統服務通訊埠，以允許或封鎖從遠端網路存取您電腦上的服務。

以下清單會顯示常見的系統服務及其相關通訊埠：

- 檔案傳輸協定 (FTP) 通訊埠 20-21
- 郵件伺服器 (IMAP) 通訊埠 143
- 郵件伺服器 (POP3) 通訊埠 110
- 郵件伺服器 (SMTP) 通訊埠 25
- Microsoft 目錄伺服器 (MSFT DS) 通訊埠 445
- Microsoft SQL 伺服器 (MSFT SQL) 通訊埠 1433
- 網路時間協定通訊埠 123
- 遠端桌面 / 遠端協助 / 終端機伺服器 (RDP) 通訊埠 3389
- 遠端程序呼叫 (RPC) 通訊埠 135
- 安全的 Web 伺服器 (HTTPS) 通訊埠 443
- 通用隨插即用 (UPNP) 通訊埠 5000
- Web 伺服器 (HTTP) 通訊埠 80
- Windows 檔案共用 (NETBIOS) 通訊埠 137-139

也可以設定系統服務通訊埠，以允許電腦與透過相同網路連接的其他電腦共用它的網際網路連線。此連線也稱爲「網際網路連線共用」(ICS)，可讓共用連線的電腦充當通往網際網路的閘道，供其他網路電腦使用。

附註：如果您的電腦上有應用程式會接受網路或 FTP 伺服器連線，則共用該連線的電腦可能需要開放相關的系統服務通訊埠，並允許轉送這些通訊埠的連入連線。

允許存取現有的系統服務通訊埠

您可以開放現有的通訊埠，以允許從遠端存取您電腦上的網路服務。

附註：開放的系統服務通訊埠會讓您的電腦容易遭受網際網路的安全性威脅，因此只應在需要時才開放通訊埠。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [系統服務]。
4. 在 [開放系統服務通訊埠] 下，選取要開放其通訊埠的系統服務。
5. 按一下 [確定]。

封鎖對現有系統服務通訊埠的存取

您可以關閉現有的通訊埠，以封鎖從遠端網路存取您電腦上的服務。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [系統服務]。
4. 在 [開放系統服務通訊埠] 下，清除系統服務以關閉其通訊埠。
5. 按一下 [確定]。

設定新的系統服務通訊埠

您可以在電腦上設定新的網路服務通訊埠，開放或關閉以允許或封鎖從遠端存取您的電腦。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [系統服務]。
4. 按一下 [新增]。
5. 在 [系統服務] 窗格中的 [通訊埠與系統服務] 下，鍵入下列各項：
   - 程式名稱
   - 入埠 TCP/IP 通訊埠
   - 出埠 TCP/IP 通訊埠

- 入埠 UDP 通訊埠
- 出埠 UDP 通訊埠

6 如果您想將這個通訊埠的活動資訊傳送到其他共用網際網路連線的網路 Windows 電腦，請選取 [將此通訊埠上的網路活動轉送給使用「網際網路連線共用」的網路使用者]。

7 (可選) 說明新設定。

8 按一下 [確定]。

附註：如果您的電腦上有應用程式會接受網路或 FTP 伺服器連線，則共用該連線的電腦可能需要開放相關的系統服務通訊埠，並允許轉送這些通訊埠的連入連線。如果您使用「網際網路連線共用」(ICS)，您也需要在「信任的 IP 位址」清單上新增信任的電腦連線。如需相關資訊，請參閱＜新增信任的電腦連線＞。

修改系統服務通訊埠

您可以修改關於現有系統服務通訊埠的入埠及出埠網路存取資訊。

附註：如果輸入不正確的通訊埠資訊，系統服務會失敗。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [防火牆] 窗格上，按一下 [系統服務]。

4 選取系統服務，然後按一下 [編輯]。

5 在 [系統服務] 窗格中的 [通訊埠與系統服務] 下，鍵入下列各項：

- 程式名稱
- 入埠 TCP/IP 通訊埠
- 出埠 TCP/IP 通訊埠
- 入埠 UDP 通訊埠
- 出埠 UDP 通訊埠

6 如果您想將這個通訊埠的活動資訊傳送到其他共用網際網路連線的網路 Windows 電腦，請選取 [將此通訊埠上的網路活動轉送給使用「網際網路連線共用」的網路使用者]。

7 (可選) 說明已修改的設定。

8 按一下 [確定]。

移除系統服務通訊埠

您可以將現有的系統服務通訊埠從電腦中移除。移除之後，遠端電腦就不能再存取您電腦上的網路服務。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [系統服務]。
4. 選取系統服務，然後按一下 [移除]。
5. 提示時，按一下 [是] 以確認。

第 20 章

管理電腦連線

您可以根據網際網路通訊協定位址 (IP) 建立與遠端電腦相關的規則，以設定防火牆來管理電腦的特定遠端連線。您可以信任與信任的 IP 位址相關的電腦連線至您的電腦，並禁止不明、可疑或不信任的 IP 連線至您的電腦。

允許連線時，請確定您信任的電腦是安全的。如果您信任的電腦透過病毒或其他機制受到感染，則您的電腦就可能會受到感染。此外，McAfee 建議您使用防火牆及最新的防毒程式來保護您信任的電腦。防火牆不會針對 [信任的 IP 位址] 清單中的 IP 位址記錄其傳來的流量或產生事件警示。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

在本章中

信任電腦連線.....90
禁止電腦連線.....93

信任電腦連線

您可以在 [信任的和禁止的 IP] 窗格的 [信任的 IP 位址] 下，新增、編輯及移除信任的 IP 位址。

[信任的和禁止的 IP] 窗格中的 [信任的 IP 位址] 清單，允許所有來自特定電腦的流量到達您的電腦。防火牆不會針對 [信任的 IP 位址] 清單中的 IP 位址記錄其傳來的流量或產生事件警示。

防火牆會信任清單上的任何檢查過的 IP 位址，且一定會允許來自信任的 IP 的流量通過任何通訊埠上的防火牆。防火牆不會篩選或分析與信任的 IP 位址相關的電腦和您的電腦之間的活動。[信任的 IP 位址] 預設會列出 Firewall 找到的第一個私人網路。

允許連線時，請確定您信任的電腦是安全的。如果您信任的電腦透過病毒或其他機制受到感染，則您的電腦就可能會受到感染。此外，McAfee 建議您使用防火牆及最新的防毒程式來保護您信任的電腦。

新增信任的電腦連線

您可以新增信任的電腦連線及其相關的 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
4. 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]，然後按一下 [新增]。
5. 在 [新增信任的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [開始 IP 位址] 及 [結束 IP 位址] 方塊中，輸入開始及結束 IP 位址。
6. 如果某個系統服務會使用「網際網路連線共用」(ICS)，則您可以新增下列 IP 位址範圍：192.168.0.1 到 192.168.0.255。
7. (可選) 選擇 [規則到期日期]，然後輸入實施規則的天數。
8. (可選) 輸入規則的說明。
9. 按一下 [確定]。
10. 在 [信任的和禁止的 IP] 對話方塊上，按一下 [是] 以確認。

附註：如需「網際網路連線共用」(ICS) 的相關資訊，請參閱＜設定新系統服務＞。

從入埠事件記錄檔新增信任的電腦

您可以從入埠事件記錄檔新增信任的電腦連線及其相關的 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格中，按一下 [常見工作] 窗格上的 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
4. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。
5. 選取來源 IP 位址，並按一下 [我要] 下的 [信任此位址]。
6. 按一下 [是] 確認。

編輯信任的電腦連線

您可以編輯信任的電腦連線及其相關的 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
4. 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]。
5. 選取 IP 位址，然後按一下 [編輯]。
6. 在 [編輯信任的 IP 位址] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [開始 IP 位址] 及 [結束 IP 位址] 方塊中，輸入開始及結束 IP 位址。
7. (可選) 勾選 [規則到期日期]，然後輸入實施規則的天數。
8. (可選) 輸入規則的說明。
9. 按一下 [確定]。

附註：您無法編輯 Firewall 從信任私人網路自動新增的預設電腦連線。

移除信任的電腦連線

您可以移除信任的電腦連線及其相關的 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
4. 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]。
5. 選取 IP 位址，然後按一下 [移除]。
6. 在 [信任的和禁止的 IP] 對話方塊上，按一下 [是] 以確認。

禁止電腦連線

您可以在 [信任的和禁止的 IP] 窗格的 [禁止的 IP 位址] 下，新增、編輯及移除禁止的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

新增禁止的電腦連線

您可以新增禁止的電腦連線及其相關的 IP 位址。

附註：請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。

1. 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。
2. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
3. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
4. 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]，然後按一下 [新增]。
5. 在 [新增禁止的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [開始 IP 位址] 及 [結束 IP 位址] 方塊中，輸入開始及結束 IP 位址。
6. (可選) 選擇 [規則到期日期]，然後輸入實施規則的天數。
7. (可選) 輸入規則的說明。
8. 按一下 [確定]。
9. 在 [信任的和禁止的 IP] 對話方塊上，按一下 [是] 以確認。

編輯禁止的電腦連線

您可以編輯禁止的電腦連線及其相關的 IP 位址。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。

4 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]，然後按一下 [編輯]。

5 在 [編輯禁止的 IP 位址] 下，執行下列其中一項動作：

- 選取 [單一 IP 位址]，然後輸入 IP 位址。
- 選取 [IP 位址範圍]，然後在 [開始 IP 位址] 及 [結束 IP 位址] 方塊中，輸入開始及結束 IP 位址。

6 (可選) 選擇 [規則到期日期]，然後輸入實施規則的天數。

7 (可選) 輸入規則的說明。

8 按一下 [確定]。

移除禁止的電腦連線

您可以移除禁止的電腦連線及其相關的 IP 位址。

1 在 [McAfee SecurityCenter] 窗格上，按一下 [網際網路與網路]，然後按一下 [設定]。

2 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。

3 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。

4 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]。

5 選取 IP 位址，然後按一下 [移除]。

6 在 [信任的和禁止的 IP] 對話方塊上，按一下 [是] 以確認。

從入埠事件記錄檔禁止電腦

您可以從入埠事件記錄檔禁止電腦連線及其相關的 IP 位址。

入埠事件記錄檔中出現的 IP 位址會遭到封鎖。因此，除非您的電腦使用故意開放的連接埠，或包含已允許存取網際網路的程式，否則禁止某個位址不會新增任何額外的保護。

只有在您有一個或多個故意開啓的通訊埠，並且您有理由相信必須封鎖某個 IP 位址使其無法存取開放的通訊埠時，才應將 IP 位址新增至 [禁止的 IP 位址]。

您可以使用列出了所有入埠網際網路流量之 IP 位址的 [入埠事件] 頁，針對您懷疑爲可疑或不當之網際網路活動的來源，禁止其 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格中，按一下 [常見工作] 下的 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
4. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。
5. 選取來源 IP 位址，並按一下 [我要] 下的 [禁止此位址]。
6. 在 [新增禁止的 IP 位址規則] 對話方塊上，按一下 [是] 以確認。

從入侵偵測事件記錄檔禁止電腦

您可以從出埠事件記錄檔禁止電腦連線及其相關的 IP 位址。

1. 在 [McAfee SecurityCenter] 窗格中，按一下 [常見工作] 下的 [進階功能表]。
2. 按一下 [報告與記錄檔]。
3. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
4. 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。
5. 選取來源 IP 位址，並按一下 [我要] 下的 [禁止此位址]。
6. 在 [新增禁止的 IP 位址規則] 對話方塊上，按一下 [是] 以確認。

第 21 章

記錄、監視及分析

防火牆爲網際網路事件及流量提供詳盡且簡單易讀的記錄、監視及分析。瞭解網際網路流量及事件可協助您管理網際網路連線。

在本章中

事件記錄.....98
使用統計資料.....100
追蹤網際網路流量.....101
監視網際網路流量.....104

事件記錄

防火牆可讓您啓用或停用事件記錄，以及指定啓用後所要記錄的事件類型。事件記錄可讓您檢視最近的入埠、出埠事件及入侵事件。

設定事件記錄檔設定

您可以指定及設定要記錄的 Firewall 事件類型。預設會針對所有事件及活動啓用事件記錄。

1. 在 [網際網路與網路設定] 窗格中的 [已啓用防火牆保護] 底下，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [事件記錄檔設定]。
3. 如果尚未選取它，請選取 [啓用事件記錄]。
4. 在 [啓用事件記錄] 下，選取或清除您要或不要記錄的事件類型。事件類型包括：
   - 封鎖的程式
   - ICMP Ping
   - 來自禁止的 IP 位址的流量
   - 系統服務通訊埠上的事件
   - 不明通訊埠上的事件
   - 入侵偵測 (IDS) 事件
5. 若要防止記錄特定通訊埠的相關資訊，請選取 [請勿記錄下列通訊埠上的事件]，然後輸入以逗號隔開的通訊埠號碼，或以破折號表示的通訊埠範圍。例如，137-139, 445, 400-5000。
6. 按一下 [確定]。

檢視最近的事件

如果已啓用記錄，您可以檢視最近的事件。[最近的事件] 窗格會顯示事件的日期及說明。它會顯示已明確封鎖，無法存取網際網路之程式的活動。

- 在 [進階功能表] 的 [常見工作] 窗格下，按一下 [報告與記錄檔] 或 [檢視最近的事件]。或者，從 [基本功能表] 按一下 [常見工作] 窗格下的 [檢視最近的事件]。

檢視入埠事件

如果已啓用記錄，您可以檢視入埠事件。入埠事件包括日期與時間、來源 IP 位址、主機名稱與資訊，以及事件類型。

1 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄檔]。

2 在 [最近的事件] 下，按一下 [檢視記錄檔]。

3 按一下 [網際網路與網路]，然後按一下 [入埠事件]。

附註：您可以從入埠事件記錄檔信任、禁止及追蹤 IP 位址。

檢視出埠事件

如果已啓用記錄，您可以檢視出埠事件。出埠事件包括嘗試進行出埠存取的程式名稱、事件的日期及時間，以及程式在您電腦上的位置。

1 在 [常見工作] 窗格上，按一下 [報告與記錄檔]。

2 在 [最近的事件] 下，按一下 [檢視記錄檔]。

3 按一下 [網際網路與網路]，然後按一下 [出埠事件]。

附註：您可以從出埠事件記錄檔，允許程式具有完整存取權及限出埠存取權。您也可以尋找程式的其他相關資訊。

檢視入侵偵測事件

如果已啓用記錄，您可以檢視入埠入侵事件。入侵偵測事件會顯示事件的日期與時間、來源 IP、主機名稱，以及事件的類型。

1 在 [常見工作] 窗格上，按一下 [報告與記錄檔]。

2 在 [最近的事件] 下，按一下 [檢視記錄檔]。

3 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。

附註：您可以從入侵偵測事件記錄檔禁止及追蹤 IP 位址。

使用統計資料

防火牆會利用 McAfee 的 HackerWatch 安全性網站，提供您有關全球網際網路安全性事件及通訊埠活動的統計資料。

檢視全球安全性事件統計資料

HackerWatch 會追蹤全球的網際網路安全性事件，您可以從 SecurityCenter 檢視這些事件。追蹤的資訊會列出在過去 24 小時、7 天及 30 天內向 HackerWatch 報告的事故。

1. 確定已啓用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [HackerWatch]。
3. 檢視 [事件追蹤] 下的安全性事件統計資料。

檢視全球網際網路通訊埠活動

HackerWatch 會追蹤全球的網際網路安全性事件，您可以從 SecurityCenter 檢視這些事件。顯示的資訊包括過去七天內向 HackerWatch 報告的最重要事件通訊埠。通常，會顯示 HTTP、TCP 及 UDP 通訊埠資訊。

1. 確定已啓用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [HackerWatch]。
3. 檢視 [最近的通訊埠活動] 下的最重要事件通訊埠事件。

追蹤網際網路流量

防火牆會提供一些追蹤網際網路流量的選項。這些選項可讓您追蹤網路電腦的地理位置、取得網域及網路資訊，以及從入埠事件及入侵偵測事件記錄檔追蹤電腦。

追蹤網路電腦的地理位置

您可以使用視覺追蹤器，利用正在連線或嘗試連線至您電腦之電腦的名稱或 IP 位址，找出該電腦的位置。您也可以使用視覺追蹤器存取網路及註冊資訊。執行視覺追蹤器會顯示世界地圖，顯示從來源電腦到您的電腦最有可能的資料傳送路徑。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [視覺追蹤器]。

3 輸入電腦的 IP 位址，然後按一下[追蹤]。

4 在 [視覺追蹤器] 下，選取 [分布圖檢視]。

附註：您無法追蹤迴圈、私人或無效的 IP 位址事件。

取得電腦註冊資訊

您可以使用視覺追蹤，從 SecurityCenter 取得電腦的註冊資訊。這些資訊包括網域名稱、註冊者的名稱及位址，以及管理聯絡人。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [視覺追蹤器]。

3 輸入電腦的 IP 位址，然後按一下[追蹤]。

4 在 [視覺追蹤器] 下，選取 [註冊者檢視]。

取得電腦網路資訊

您可以使用視覺追蹤，從 SecurityCenter 取得電腦的網路資訊。網路資訊包括網域所在網路的詳細資料。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [視覺追蹤器]。

3 輸入電腦的 IP 位址，然後按一下[追蹤]。

4 在 [視覺追蹤器] 下，選取 [網路檢視]。

從入埠事件記錄檔追蹤電腦

從 [傳入事件] 窗格中，您可以追蹤在入埠事件記錄檔中出現的 IP 位址。

1. 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄檔]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。
4. 在 [傳入事件] 窗格上，選取來源 IP 位址，然後按一下 [追蹤此位址]。
5. 在 [視覺追蹤器] 窗格上，按一下下列其中一項：
   - **分布圖檢視**：使用選取的 IP 位址，找出電腦的位址。
   - **註冊者檢視**：使用選取的 IP 位址，尋找網域資訊。
   - **網路檢視**：使用選取的 IP 位址，尋找網路資訊。
6. 按一下 [完成]。

從入侵偵測事件記錄檔追蹤電腦

從 [入侵偵測事件] 窗格中，您可以追蹤在入侵偵測事件記錄檔中出現的 IP 位址。

1. 在 [常見工作] 窗格上，按一下 [報告與記錄檔]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。在 [入侵偵測事件] 窗格上，選取來源 IP 位址，然後按一下 [追蹤此位址]。
4. 在 [視覺追蹤器] 窗格上，按一下下列其中一項：
   - **分布圖檢視**：使用選取的 IP 位址，找出電腦的位址。
   - **註冊者檢視**：使用選取的 IP 位址，尋找網域資訊。
   - **網路檢視**：使用選取的 IP 位址，尋找網路資訊。
5. 按一下 [完成]。

追蹤監視的 IP 位址

您可以追蹤監視的 IP 位址以取得地理檢視，它會顯示從來源電腦到您的電腦最有可能的資料傳送路徑。此外，您也可以取得有關 IP 位址的註冊及網路資訊。

1. 確定已啓用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [流量監視]。
3. 在 [流量監視] 下，按一下 [作用中的程式]。
4. 選取一個程式，然後選取在該程式名稱下出現的 IP 位址。
5. 在 [程式活動] 下，按一下 [追蹤此 IP]。
6. 在 [視覺追蹤器] 下，您可以檢視一個地圖，它會顯示從來源電腦到您的電腦最有可能的資料傳送路徑。此外，您也可以取得有關 IP 位址的註冊及網路資訊。

附註：若要檢視最新的統計資料，請按一下 [視覺追蹤器] 下的 [重新整理]。

監視網際網路流量

防火牆提供一些監視網際網路流量的方法，包括：

- **流量分析圖**：顯示最近的入埠及出埠網際網路流量。
- **流量使用率圖**：顯示過去 24 小時期間使用最頻繁的程式所使用的頻寬百分比。
- **作用中的程式**：顯示目前在您電腦上使用最多網路連線的程式，以及這些程式存取的 IP 位址。

關於流量分析圖

流量分析圖以數字和圖形來表示網際網路流量，包括入埠和出埠流量。此外，流量監視會顯示電腦上使用大量網路連線的程式及這些程式所存取的 IP 位址。

從 [流量分析] 窗格中，您可以檢視最近的入埠及出埠網際網路流量，目前、平均及最大傳輸率。您也可以檢視流量，包括自從啓動防火牆後的流量，以及本月及上個月的總流量。

[流量分析] 窗格會顯示您電腦上的即時網際網路活動，包括您電腦上最近入埠及出埠的網際網路流量及其速率，以及跨網際網路傳輸的位元組總數。

綠色實線表示連入流量的目前傳輸速率。綠色虛線表示連入流量的平均傳輸速率。如果目前傳輸速率與平均傳輸速率相等，則圖中將不顯示虛線。實線同時表示平均傳輸速率和目前傳輸速率。

紅色實線表示連出流量的目前傳輸速率。紅色虛線表示連出流量的平均傳輸速率。如果目前傳輸速率與平均傳輸速率相等，則圖中將不顯示虛線。實線同時表示平均傳輸速率和目前傳輸速率。

分析入埠及出埠流量

流量分析圖以數字和圖形來表示網際網路流量，包括入埠和出埠流量。此外，流量監視會顯示電腦上使用大量網路連線的程式及這些程式所存取的 IP 位址。

1. 確定已啓用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [流量監視]。
3. 在 [流量監視] 下，按一下 [流量分析]。

秘訣：若要檢視最新的統計資料，請按一下 [流量分析] 下的 [重新整理]。

監視程式頻寬

您可以檢視圓餅圖，它會顯示過去 24 小時期間使用最頻繁的程式所使用的大約頻寬百分比。圓餅圖提供程式使用頻寬的相對數量之視覺展示。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [流量監視]。

3 在 [流量監視] 下，按一下 [流量使用率]。

秘訣：若要檢視最新的統計資料，請按一下 [流量使用率] 下的 [重新整理]。

監視程式活動

您可以檢視入埠及出埠程式活動，它會顯示遠端電腦連線及通訊埠。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [流量監視]。

3 在 [流量監視] 下，按一下 [作用中的程式]。

4 您可以檢視下列資訊：

- 程式活動圖：選取要顯示其活動圖的程式。
- 監聽連線：選取程式名稱下的監聽項目。
- 電腦連線：選取程式名稱、系統處理程序或服務下的 IP 位址。

附註：若要檢視最新的統計資料，請按一下 [作用中的程式] 下的 [重新整理]。

第 22 章

瞭解網際網路安全性

防火牆會利用 McAfee 的安全性網站 (HackerWatch)，提供有關程式及全球網際網路活動的最新資訊。HackerWatch 也會提供有關防火牆的 HTML 教學課程。

在本章中

啓動 HackerWatch 教學課程.....108

啓動 HackerWatch 教學課程

若要瞭解防火牆，您可以從 SecurityCenter 存取 HackerWatch 教學課程。

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [HackerWatch]。

3 在 [HackerWatch 資源] 下，按一下 [檢視教學課程]。

第 23 章

McAfee QuickClean

QuickClean 藉由刪除會在您電腦上建立雜亂資訊的檔案，來改進您的電腦效能。它會清空您的資源回收筒，並刪除暫存檔案、捷徑、遺失的檔案片段、登錄檔、快取檔、Cookie、瀏覽器歷史記錄檔、已傳送與刪除的電子郵件、最近使用的檔案、Active-X 檔案，以及系統還原點檔案。QuickClean 也會使用 McAfee Shredder 元件，安全且永久地刪除包含機密個人資訊 (例如您的姓名和地址) 的項目，來保護您的隱私。如需有關銷毀檔案的詳細資料，請參閱＜McAfee Shredder＞。

磁碟重組工具會整理您電腦上的檔案和資料夾，確保它們在儲存至電腦硬碟上時不會變成殘餘片段 (亦即，分散的檔案)。定期爲您的硬碟進行磁碟重組，可確保這些分散的檔案和資料夾會被合併，以便日後可快速擷取。

如果不想手動維護電腦，您可以設定 QuickClean 和磁碟重組工具的排程頻率，並將其當成獨立工作自動執行。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

QuickClean 功能.....110
清理您的電腦.....111
將電腦進行磁碟重組.....114
排程工作.....115

QuickClean 功能

QuickClean 提供各種不同的清理工具，安全且有效率地刪除不需要的檔案。藉由刪除這些檔案，您可以增加電腦硬碟上的空間，並改善其效能。

清理您的電腦

QuickClean 會刪除在您電腦上建立雜亂資訊的檔案。它會清空您的資源回收筒，並刪除暫存檔案、捷徑、遺失的檔案片段、登錄檔、快取檔、Cookie、瀏覽器歷史記錄檔、已傳送與刪除的電子郵件、最近使用的檔案、Active-X 檔案，以及系統還原點檔案。QuickClean 會刪除這些項目，但不會影響其他的必要資訊。

您可以使用任一個 QuickClean 清理工具，從電腦中刪除不需要的檔案。下表說明 QuickClean 清理工具：

名稱	功能
資源回收筒清理工具	刪除資源回收筒中的檔案。
暫存檔清理工具	刪除暫存資料夾中儲存的檔案。
捷徑清理工具	刪除中斷的捷徑及沒有關聯程式的捷徑。
遺失的檔案片段清理工具	刪除電腦中遺失的檔案片段。
登錄清理工具	刪除電腦中已不存在之程式的 Windows® 登錄資訊。 「登錄」是 Windows 將設定資訊儲存於其上的資料庫。登錄包含每個電腦使用者及系統硬體、已安裝程式和內容設定之相關資訊的設定檔。Windows 在其作業期間，會持續參照這項資訊。
快取清理工具	刪除您在瀏覽網頁時累積的快取檔案。這些檔案通常會以暫存檔的形式儲存於快取資料夾中。 快取資料夾是電腦上的暫時儲存區。爲了增加 Web 瀏覽速度及效率，瀏覽器會在您下次要檢視某網頁時，從其快取中擷取該網頁 (而不是從遠端伺服器擷取)。
Cookie 清理工具	刪除 Cookie。這些檔案通常會儲存爲暫存檔。 Cookie 是儲存於電腦上且包含個人瀏覽 Web 之資訊的小型檔案，通常包含使用者名稱和目前的日期與時間。Cookie 主要是網站用來識別先前已向其註冊或曾造訪該網站的使用者，不過，他們也會成爲駭客所用之資訊的來源。
瀏覽器歷史記錄清理工具	刪除您的 Web 瀏覽器歷史記錄。

名稱	功能
Outlook Express 及 Outlook 電子郵件清理工具 (已傳送及已刪除的項目)	從 Outlook® 和 Outlook Express 刪除已傳送及已刪除的電子郵件。
最近使用過的清理工具	刪除利用下列任一程式所建立之最近使用過的檔案： ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX 清理工具	刪除 ActiveX 控制項。 ActiveX 是程式或網頁所使用的軟體元件，用以新增可組合到程式或網頁中、如同程式或網頁中正常組件的功能。大部分的 ActiveX 控制項都是無害的；但是，有些可能會從您的電腦擷取資訊。
系統還原點清理工具	從電腦中刪除舊的系統還原點 (但最新的那一個除外)。 系統還原點是由 Windows 所建立，可標記對您電腦所作的任何變更，如此，若發生任何問題，您還可恢復至先前狀態。

清理您的電腦

您可以使用任一個 QuickClean 清理工具，從電腦中刪除不需要的檔案。完成時，您可以在 [QuickClean 摘要] 之下，檢視清理之後所回收的磁碟空間量、已刪除的檔案數目，以及最後一個 QuickClean 作業在您電腦上執行的日期與時間。

1 在 [McAfee SecurityCenter] 窗格中，於 [常見工作] 之下，按一下 [維護電腦]。

2 在 [McAfee QuickClean] 之下，按一下 [開始]。

3 執行下列其中一項：

- 按 [下一步] 以接受清單中的預設清理工具。

- 選擇或清除適合的清理工具，然後按 [下一步]。如果選擇 [最近使用過的清理工具]，您可以按一下 [內容] 來選擇或清除清單中最近使用程式所建立的檔案，然後按一下 [確定]。
- 按一下 [還原預設值]，還原預設清理工具，再按 [下一步]。

4 執行分析之後，按 [下一步]。

5 按 [下一步] 確認檔案刪除。

6 執行下列其中一項：

- 按 [下一步] 以接受預設的 [否，我要使用標準 Windows 刪除作業來刪除檔案]。
- 按一下 [是，我要使用 Shredder 安全地清除檔案]，並指定操作次數 (最多 10 次)，然後按 [下一步]。如果有大量的資訊需要清除，則銷毀檔案會是一個冗長的過程。

7 如果在清理期間有任何檔案或項目被鎖定，系統可能會提示您重新啓動電腦。按一下 [確定] 關閉提示。

8 按一下 [完成]。

附註：利用 Shredder 刪除的檔案將無法回復。如需銷毀檔案的相關資料，請參閱＜McAfee Shredder＞。

將電腦進行磁碟重組

磁碟重組工具會整理您電腦上的檔案和資料夾，如此，它們在儲存至電腦硬碟上時不會變成殘餘片段 (亦即，分散的檔案)。定期爲您的硬碟進行磁碟重組，可確保這些分散的檔案和資料夾會被合併，以便日後可快速擷取。

將電腦進行磁碟重組

您可以將電腦進行磁碟重組，以改進檔案與資料夾的存取和擷取。

1. 在 [McAfee SecurityCenter] 窗格中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [磁碟重組工具] 底下按一下 [分析]。
3. 遵循螢幕上的指示進行。

附註：如需磁碟重組工具的詳細資訊，請參閱「Windows 說明」。

排程工作

工作排程器會設定 QuickClean 或磁碟重組工具在您電腦上自動執行的頻率。例如，您可以將 QuickClean 工作的排程設定爲在每個星期天早上 9:00 清空您的資源回收筒，或者將磁碟重組工具工作的排程設定爲在每個月最後一天將您的電腦硬碟進行磁碟重組。您可以隨時建立、修改或刪除工作。您必須登入電腦，排定的工作才能執行。如果工作因任何理由而沒有執行，它會在您再次登入之後的五分鐘重新排程。

排程 QuickClean 工作

您可以將 QuickClean 工作的排程設定爲使用一或多個清理工具自動清理您的電腦。完成時，您可以在 [QuickClean 摘要] 之下，檢視您的工作被排定要再次執行的日期與時間。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [McAfee QuickClean]。

3 在 [工作名稱] 方塊中鍵入工作的名稱，然後按一下 [建立]。

4 執行下列其中一項：

- 按 [下一步] 以接受清單中的清理工具。
- 選擇或清除適合的清理工具，然後按 [下一步]。如果您選擇 [最近使用過的清理工具]，您可以按一下 [內容] 來選擇或清除清單中最近使用程式所建立的檔案，然後按一下 [確定]。
- 按一下 [還原預設值]，還原預設清理工具，再按 [下一步]。

5 執行下列其中一項：

- 按一下 [排程] 以接受預設的 [否，我要使用標準 Windows 刪除作業來刪除檔案]。
- 按一下 [是，我要使用 Shredder 安全地清除檔案]，並指定操作次數 (最多 10 次)，然後按一下 [排程]。

6 在 [排程] 對話方塊中，選擇您要執行工作的頻率，然後按一下 [確定]。

7 如果您變更了 [最近使用過的清理工具] 的內容，系統可能會提示您重新啓動電腦。按一下 [確定] 關閉提示。

8 按一下 [完成]。

附註：利用 Shredder 刪除的檔案將無法回復。如需銷毀檔案的相關資料，請參閱＜McAfee Shredder＞。

修改 QuickClean 工作

您可以修改已排程的 QuickClean 工作，以變更其使用的清理工具，或是它在您電腦上自動執行的頻率。完成時，您可以在 [QuickClean 摘要] 之下，檢視您的工作被排定要再次執行的日期與時間。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [McAfee QuickClean]。

3 在 [選擇現有的工作] 清單中選擇工作，然後按一下 [修改]。

4 執行下列其中一項：

- 按 [下一步] 以接受爲此工作所選擇的清理工具。
- 選擇或清除適合的清理工具，然後按 [下一步]。如果您選擇 [最近使用過的清理工具]，您可以按一下 [內容] 來選擇或清除清單中最近使用程式所建立的檔案，然後按一下 [確定]。
- 按一下 [還原預設值]，還原預設清理工具，再按 [下一步]。

5 執行下列其中一項：

- 按一下 [排程] 以接受預設的 [否，我要使用標準 Windows 刪除作業來刪除檔案]。
- 按一下 [是，我要使用 Shredder 安全地清除檔案]，並指定操作次數 (最多 10 次)，然後按一下 [排程]。

6 在 [排程] 對話方塊中，選擇您要執行工作的頻率，然後按一下 [確定]。

7 如果您變更了 [最近使用過的清理工具] 的內容，系統可能會提示您重新啓動電腦。按一下 [確定] 關閉提示。

8 按一下 [完成]。

附註：利用 Shredder 刪除的檔案將無法回復。如需銷毀檔案的相關資料，請參閱＜McAfee Shredder＞。

刪除 QuickClean 工作

如果不想再讓已排程的 QuickClean 工作自動執行，您可以將之刪除。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [McAfee QuickClean]。

3 在 [選擇現有的工作] 清單中選擇工作。

4 按一下 [刪除]，然後按一下 [是] 以確認刪除。

5 按一下 [完成]。

排程磁碟重組工具工作

您可以排程磁碟重組工具工作，以排定您電腦硬碟自動進行磁碟重組的頻率。完成時，您可以在 [磁碟重組工具] 之下，檢視您的工作被排定要再次執行的日期與時間。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [磁碟重組工具]。

3 在 [工作名稱] 方塊中鍵入工作的名稱，然後按一下 [建立]。

4 執行下列其中一項：

- 按一下 [排程] 以接受預設的 [即使可用空間很低，仍執行磁碟重組] 選項。

- 清除 [即使可用空間很低，仍執行磁碟重組] 選項，然後按一下 [排程]。

5 在 [排程] 對話方塊中，選擇您要執行工作的頻率，然後按一下 [確定]。

6 按一下 [完成]。

修改磁碟重組工具工作

您可以修改已排程的磁碟重組工具工作，以變更它在您電腦上自動執行的頻率。完成時，您可以在 [磁碟重組工具] 之下，檢視您的工作被排定要再次執行的日期與時間。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [磁碟重組工具]。

3 在 [選擇現有的工作] 清單中選擇工作，然後按一下 [修改]。

4 執行下列其中一項：

- 按一下 [排程] 以接受預設的 [即使可用空間很低，仍執行磁碟重組] 選項。
- 清除 [即使可用空間很低，仍執行磁碟重組] 選項，然後按一下 [排程]。

5 在 [排程] 對話方塊中，選擇您要執行工作的頻率，然後按一下 [確定]。

6 按一下 [完成]。

刪除磁碟重組工具工作

如果不想再讓已排程的磁碟重組工具工作自動執行，您可以將之刪除。

1 開啓 [工作排程器] 窗格。

如何辦到？

1. 在 [McAfee SecurityCenter] 中，於 [常見工作] 之下，按一下 [維護電腦]。
2. 在 [工作排程器] 之下，按一下 [開始]。

2 在 [選擇要排程的作業] 清單中，按一下 [磁碟重組工具]。

3 在 [選擇現有的工作] 清單中選擇工作。

4 按一下 [刪除]，然後按一下 [是] 以確認刪除。

5 按一下 [完成]。

第 24 章

McAfee Shredder

McAfee Shredder 會永久刪除 (或「銷毀」) 電腦硬碟上的項目。即使手動刪除檔案和資料夾、清空您的資源回收筒，或刪除 [Temporary Internet Files] 資料夾時，您仍然可以使用電腦分析工具來復原這些資訊。同樣地，因爲有些程式會儲存所開啓檔案的暫存隱藏副本，所以可復原已刪除的檔案。Shredder 會安全且永久地刪除這些無用的檔案，以保護您的隱私。請記住，已銷毀的檔案無法再復原，這點很重要。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

Shredder 功能 122
銷毀檔案、資料夾及磁碟 123

Shredder 功能

Shredder 會刪除電腦硬碟上的項目，如此一來，其相關資訊便無法復原。它可以安全並永久地刪除檔案和資料夾、資源回收筒和 [Temporary Internet Files] 資料夾中的項目，以及整個電腦磁碟 (例如可重複寫入的 CD、外接硬碟及磁碟片) 中的內容，來保護您的隱私。

銷毀檔案、資料夾及磁碟

Shredder 能確保資源回收筒和 [Temporary Internet Files] 資料夾內已刪除之檔案和資料夾中所含的資訊將無法復原，即使利用特殊的工具也一樣。利用 Shredder，您可以指定想要銷毀項目的次數 (最多 10 次)。銷毀操作的次數越高，安全刪除檔案的層級就越高。

銷毀檔案與資料夾

您可以銷毀電腦硬碟上的檔案和資料夾，包括資源回收筒和 [Temporary Internet Files] 資料夾中的項目。

1 開啓 [Shredder]。

如何辦到？

1. 在 [McAfee SecurityCenter] 窗格中，按一下 [常見工作] 下的 [進階功能表]。
2. 按一下左窗格中的 [工具]。
3. 按一下 [Shredder]。

2 在 [銷毀檔案與資料夾] 窗格中，於 [我要] 之下，按一下 [清除檔案與資料夾]。

3 在 [銷毀層級] 之下，按一下下列其中一個銷毀層級：

- 快速：銷毀所選取的項目一次。
- 全面：銷毀所選取的項目七次。
- 自訂：銷毀所選取的項目最多十次。

4 按一下 [下一步]。

5 執行下列其中一項：

- 在 [選擇要銷毀的檔案] 清單中，按一下 [資源回收筒內容] 或 [Temporary Internet files]。
- 按一下 [瀏覽]、瀏覽至您想要銷毀的檔案，然後按一下 [開啓]。

6 按一下 [下一步]。

7 按一下 [開始]。

8 當 Shredder 完成時，按一下 [完成]。

附註：在 Shredder 完成工作前，請勿使用任何檔案。

銷毀整個磁碟

您可以一次銷毀整個磁碟的內容。僅可銷毀抽取式磁碟機，例如，外接硬碟、可重複寫入的 CD 及磁碟片。

1 開啓 [Shredder]。

如何辦到？

1. 在 [McAfee SecurityCenter] 窗格中，按一下 [常見工作] 下的 [進階功能表]。
2. 按一下左窗格中的 [工具]。
3. 按一下 [Shredder]。

2 在 [銷毀檔案與資料夾] 窗格中，於 [我要] 之下，按一下 [清除整個磁碟]。

3 在 [銷毀層級] 之下，按一下下列其中一個銷毀層級：

- 快速：銷毀所選取的磁碟一次。
- 全面：銷毀所選取的磁碟七次。
- 自訂：銷毀所選取的磁碟最多十次。

4 按一下 [下一步]。

5 在 [選擇磁碟] 清單中，按一下您想要銷毀的磁碟。

6 按 [下一步]，然後按一下 [是] 加以確認。

7 按一下 [開始]。

8 當 Shredder 完成時，按一下 [完成]。

附註：在 Shredder 完成工作前，請勿使用任何檔案。

第 25 章

McAfee Network Manager

Network Manager 展現了組成家庭網路之電腦與元件的圖形化檢視畫面。您可以使用 Network Manager，從遠端監視您網路上每台受管理電腦的保護狀態，並在遠端修復這些電腦上所報告的安全性弱點。

開始使用 Network Manager 之前，請先熟悉一些常用的功能。Network Manager 說明中會提供有關設定和使用這些功能的詳細資料。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

Network Manager 的功能.....126
瞭解 Network Manager 圖示.....127
設定一個受管理網路.....129
遠端管理網路.....135

Network Manager 的功能

Network Manager 提供了下列功能。

圖形化網路圖

Network Manager 的網路圖提供組成家庭網路之電腦與元件的保護狀態圖形化總覽。當您對網路進行變更時 (例如，增加一部電腦)，網路圖會識別這些變更。您可以重新整理網路圖、重新命名網路、顯示或隱藏網路圖元件以自訂您的檢視畫面。您也可以檢視網路圖上任何元件的相關詳細資料。

遠端管理

使用 Network Manager 網路圖來管理組成您家庭網路之電腦的保護狀態。您可邀請電腦加入受管理網路、監視受管理電腦的保護狀態，並從網路上的遠端電腦修正已知安全性弱點。

瞭解 Network Manager 圖示

下表說明 Network Manager 網路圖上常用的圖示。

圖示	說明
	表示一個線上受管理的電腦
	表示一個離線受管理的電腦
	表示一個安裝了 SecurityCeter 的不受管理電腦
	表示一個離線不受管理的電腦
	表示一個未安裝 SecurityCenter 的線上電腦，或一個未知的網路裝置
	表示一個未安裝 SecurityCenter 的離線電腦，或一個未知的離線網路裝置
	意味著對應的項目受到保護並已連線
	意味著對應的項目可能需要您的注意
	意味著對應的項目立即需要您的注意
	表示無線家用路由器
	表示一個標準的家用路由器
	表示連線時的網際網路
	表示中斷連線時的網際網路

第 26 章

設定一個受管理網路

若要設定一個受管理網路，可使用您網路圖上的項目及將成員 (電腦) 新增至網路來達成。一部電腦必須先成爲網路的信任成員，才能對該電腦進行遠端管理，或授予其遠端管理網路上其他電腦的權限。新電腦的網路成員資格是由具管理權限的現有網路成員 (電腦) 所授予。

您可檢視網路圖中任何元件的相關詳細資料，即使在您變更網路之後 (例如新增電腦之後) 一樣可以。

在本章中

與網路圖一起運作.....130
加入受管理網路.....132

與網路圖一起運作

當您將電腦連線至網路時，Network Manager 會分析網路以決定是否有任何受管理與不受管理成員的存在、路由器的屬性及網際網路狀態。若未發現任何成員，Network Manager 會假設目前連線的電腦是網路上第一台電腦，並使該台電腦成爲具管理權限的受管理成員。依預設，網路名稱包含首部連線至網路且安裝 SecurityCenter 之電腦所在工作群組或網域的名稱；然而，您可隨時重新命名網路。

當您對網路進行變更時 (例如，增加一部電腦)，您可自訂網路圖。例如，您可以重新整理網路圖、重新命名網路，顯示或隱藏網路圖元件以自訂您的檢視畫面。您也可以檢視出現在網路圖上任何元件的相關詳細資料。

存取網路圖

網路圖提供了組成家庭網路之電腦與元件的圖形化呈現。

- 按一下 [基本功能表] 或 [進階功能表] 中的 [管理網路]。

附註：您第一次存取網路圖時，系統會提示您信任網路上的其他電腦。

重新整理網路圖

您可隨時重新整理網路圖；例如，於另一個電腦加入受管理網路後。

1. 按一下 [基本功能表] 或 [進階功能表] 中的 [管理網路]。
2. 按一下 [我要] 下的 [重新整理網路圖]。

附註：[重新整理網路圖] 連結僅適用於未在網路圖上選取任何項目時。若要清除一個項目，請按一下所選取的項目，或按一下網路圖上的空白區域。

重新命名網路

依預設，網路名稱包含首部連線至網路且安裝 SecurityCenter 之電腦所在工作群組或網域的名稱。若您想用其他的名稱，您可以變更。

1. 按一下 [基本功能表] 或 [進階功能表] 中的 [管理網路]。
2. 按一下 [我要] 下的 [重新命名網路]。
3. 於 [網路名稱] 方塊中鍵入網路名稱。
4. 按一下 [確定]。

附註：[重新命名網路] 連結僅適用於未在網路圖上選取任何項目時。若要清除一個項目，請按一下所選取的項目，或按一下網路圖上的空白區域。

顯示或隱藏網路圖上的項目

依預設，您家庭網路中的所有電腦與元件都會出現在網路圖上。然而，若您有隱藏的項目，您可隨時再次顯示他們。只有不受管理的項目可以隱藏；受管理的電腦不能隱藏。

若要...	在 [基本功能表] 或 [進階功能表] 上，按一下 [管理網路]，然後執行...
隱藏網路圖上的項目	按一下網路圖上的項目，然後按一下 [我要] 下的 [隱藏此項目]。於確認對話方塊中，按一下 [是]。
顯示網路圖上隱藏的項目	在 [我要] 下，按一下 [顯示隱藏的項目]。

檢視項目的詳細資料

選取網路圖上的元件，您就可以檢視網路上任何元件的詳細資訊。此資訊包括元件名稱、元件保護狀態，及管理元件所需要的其他資訊。

1 按一下網路圖上的項目圖示。

2 在 [詳細資料] 下，檢視有關項目的資訊。

加入受管理網路

一部電腦必須先成爲網路的信任成員，才能對該電腦進行遠端管理，或授予其遠端管理網路上其他電腦的權限。新電腦的網路成員資格是由具管理權限的現有網路成員 (電腦) 所授予。爲確保只有信任的電腦才可加入網路，授權電腦及加入電腦雙方的使用者必須驗證彼此。

當一部電腦加入網路時，會出現提示要求它對網路上其他電腦顯示其 McAfee 保護狀態。若某部電腦同意顯示其保護狀態，它即會成爲網路的受管理成員。若某部電腦拒絕顯示其保護狀態，它即會成爲網路的不受管理成員。網路的不受管理成員通常是要存取其他網路功能 (例如，傳送檔案或共用印表機) 的來賓電腦。

附註：在您加入後，若您已安裝了其他 McAfee 網路程式 (例如 EasyNetwork)，這些程式仍會將您的電腦視爲一個受管理的電腦。指定給 Network Manager 中之電腦的權限等級會套用至所有 McAfee 網路程式。針對來賓權限、完整權限或系統管理權限在其他 McAfee 網路程式中的意義，請參閱該程式所提供的說明文件，以取得詳細資訊。

加入受管理網路

當您收到加入受管理網路的邀請時，您可以接受或拒絕邀請。您亦可決定是否要讓此電腦與網路上其他電腦互相監視彼此的安全性設定 (例如，電腦的病毒保護是否是最新的)。

1. 在 [受管理網路] 對話方塊中，請確定選取 [允許此網路上的每台電腦監視安全性設定] 核取方塊。
2. 按一下 [加入]。
   當您接受邀請時，即會顯示兩種圖片。
3. 請確認該圖片與邀請您加入受管理網路之電腦上所顯示的圖片相同。
4. 按一下 [確定]。

附註：若邀請您加入受管理網路的電腦並未顯示安全性確認對話方塊中出現的相同圖片，則表示受管理網路上發生安全漏洞。加入網路可能會讓您的電腦面臨風險，因此，請按一下 [受管理網路] 對話方塊中的 [取消]。

邀請電腦加入受管理網路

若某部電腦新增至受管理網路或其他存在於網路中的不受管理電腦，則您可邀請該電腦加入受管理網路。只有在網路上具管理權限的電腦可以邀請其他電腦加入。當您傳送邀請時，您也需要對加入的電腦指定您要指派的權限等級。

1 按一下網路圖上的不受管理電腦圖示。

2 按一下 [我要] 下的 [監視此電腦]。

3 於 [邀請電腦加入受管理網路] 對話方塊中，執行下列其中一項：

- 按一下 [允許受管理網路程式擁有來賓存取權]，允許電腦存取網路 (您可以對家中的臨時使用者使用此選項)。
- 按一下 [允許受管理網路程式擁有完整存取權]，允許電腦存取網路。
- 按一下 [允許受管理網路程式擁有系統管理存取權]，允許電腦以系統管理的權限存取網路。此選項亦可讓電腦對要加入受管理網路的其他電腦授予存取權。

4 按一下 [確定]。
加入受管理網路的邀請會傳送至該電腦。當電腦接受邀請時，即會出現兩種圖片。

5 請確認該圖片與您已邀請加入受管理網路之電腦上所顯示的圖片相同。

6 按一下 [授予存取權]。

附註：若您邀請加入受管理網路的電腦並未顯示安全性確認對話方塊中出現的相同圖片，則表示受管理網路上發生安全漏洞。允許電腦加入網路可能導致其他電腦處於風險之中，因此，按一下安全性確認對話方塊中的 [拒絕存取權]。

停止信任網路上的電腦

如果不小心信任網路上所有其他電腦，您可以停止信任它們。

- 按一下 [我要] 下的 [停止信任此網路上的電腦]。

附註：如果您具有管理權限，且網路中有其他受管理電腦，[停止信任此網路上的電腦] 連結就沒有功用。

第 27 章

遠端管理網路

設定您的受管理網路後，您可在遠端管理組成您網路的電腦與元件。您可以監視電腦與元件的狀態及權限等級，並從遠端修復最危險的安全性弱點。

在本章中

監視狀態與權限.....136
修復安全性弱點.....138

監視狀態與權限

受管理網路中有受管理和不受管理的成員。受管理成員可讓網路上其他電腦監視其 McAfee 保護狀態；而不受管理成員則否。不受管理成員通常是要存取其他網路功能 (例如，傳送檔案或共用印表機) 的來賓電腦。不受管理電腦可隨時爲網路上其他受管理電腦所邀請，成爲一部受管理電腦。同樣的，受管理電腦可隨時成爲不受管理電腦。

受管理電腦具有管理權限、完整權限或來賓權限。管理權限可讓受管理電腦管理網路上所有其他受管理電腦的保護狀態，並對其他電腦授予網路的成員資格。完整權限與來賓權限只允許一部電腦存取網路。您可隨時修改電腦的權限等級。

因爲受管理網路亦有裝置 (例如，路由器)，您可以使用 Network Manager 來管理這些裝置。您還可以設定並修改網路圖上之裝置的顯示內容。

監視電腦的保護狀態

如果某台電腦的保護狀態在此網路上未受到監視 (該電腦不是此網路的成員，或電腦是此網路的不受管理成員)，則您可以要求監視它。

1 按一下網路圖上的不受管理電腦圖示。

2 按一下 [我要] 下的 [監視此電腦]。

停止監視電腦的保護狀態

您可以停止監視網路中受管理電腦的保護狀態；然而，電腦之後會變成不受管理，而您將無法從遠端監視其保護狀態。

1 按一下網路圖上的受管理電腦圖示。

2 按一下 [我要] 下的 [停止監視此電腦]。

3 於確認對話方塊中，按一下 [是]。

修改受管理電腦的權限

您可隨時變更受管理電腦的權限。這能讓您修改哪部電腦可監視網路上其他電腦的保護狀態。

1 按一下網路圖上的受管理電腦圖示。

2 按一下 [我要] 下的 [修改此電腦的權限]。

3 在修改權限對話方塊中，請選取或清除核取方塊，以決定此電腦及受管理網路上的其他電腦是否可以監視彼此的保護狀態。

4 按一下 [確定]。

管理裝置

您可由 Network Manager 存取其管理網頁來管理裝置。

1 按一下網路圖上的裝置圖示。

2 按一下 [我要] 下的 [管理此裝置]。
Web 瀏覽器將會開啓並顯示裝置的管理網頁。

3 在您的 Web 瀏覽器中，請提供您的登入資訊並設定裝置的安全性設定。

附註：若該裝置是一個 Wireless Network Security 保護的無線路由器或存取點，您必須使用 Wireless Network Security 來進行該裝置的安全性設定。

修改裝置的顯示內容

修改裝置顯示內容時，您可以變更網路圖上的裝置顯示名稱，並指定裝置是否爲一個無線路由器。

1 按一下網路圖上的裝置圖示。

2 按一下 [我要] 下的 [修改裝置內容]。

3 若要指定裝置的顯示名稱，請於 [名稱] 方塊中鍵入名稱。

4 若要指定裝置的類型，如果不是無線路由器，請按一下 [標準路由器]，如果是無線路由器，則按一下 [無線路由器]。

5 按一下 [確定]。

修復安全性弱點

具管理權限的受管理電腦可以監視網路上其他受管理電腦的 McAfee 保護狀態，並從遠端修復回報的安全性弱點。例如，若一部受管理電腦的 McAfee 保護狀態指出其 VirusScan 已停用，則另一個具管理權限的受管理電腦可從遠端啓用 VirusScan。

當您從遠端修復安全性弱點時，Network Manager 會修復最常報告的問題。然而，某些安全性弱點可能需要在本機電腦上手動介入。在這種情況下，Network Manager 會修復可遠端修復的問題，然後提示您登入易受入侵之電腦的 SecurityCenter 中，並遵循所提供的建議修復剩下的問題。在某些情況下，建議的解決方案是在遠端或您網路中的電腦上安裝最新版本的 SecurityCenter。

修復安全性弱點

您可使用 Network Manager，修復遠端受管理電腦上的大部分安全性弱點。例如，若在一個遠端電腦上已停用了 VirusScan，您可啓用它。

1 按一下網路圖上的項目圖示。
2 檢視 [詳細資料] 下之項目的保護狀態。
3 按一下 [我要] 下的 [修復安全性弱點]。
4 當安全性問題修復之後，請按一下 [確定]。

附註：雖然 Network Manager 會自動修復大部分的安全性弱點，部分修復仍需要您開啓易受入侵電腦上的 SecurityCenter，並遵循所提供的建議。

在遠端電腦上安裝 McAfee 安全性軟體

若您網路上一或多部電腦並未使用最新版本的 SecurityCenter，則無法從遠端監視其保護狀態。若要遠端監視這些電腦，您必須到每部電腦並安裝最新版本的 SecurityCenter。

1 在您要安裝安全性軟體的電腦上，開啓 SecurityCenter。
2 在 [常見工作] 下，按一下 [我的帳戶]。
3 以您安裝安全性軟體時註冊的電子郵件和密碼登入。
4 選取適當的產品後按一下 [下載/安裝] 圖示，然後依照螢幕上的指示操作。

第 28 章

McAfee EasyNetwork

使用 EasyNetwork 可以在家用網路的電腦之間進行安全的檔案共用、簡化檔案傳輸，並共用印表機。但是，您網路中的電腦必須安裝 EasyNetwork 才能使用它的功能。

開始使用 EasyNetwork 之前，請先熟悉一些常用的功能。EasyNetwork 說明中會提供有關設定和使用這些功能的詳細資料。

附註： SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。

在本章中

EasyNetwork 的功能 140
設定 EasyNetwork 141
共用和傳送檔案 147
共用印表機 153

EasyNetwork 的功能

EasyNetwork 提供下列功能。

檔案共用

EasyNetwork 可讓您輕鬆在網路上與其他電腦共用檔案。當您共用檔案時，同時間便會將這些檔案的唯讀存取權授予其他電腦。只有對您的受管理網路 (成員) 具有完整或管理存取權的電腦，才可以共用檔案或存取其他成員共用的檔案。

檔案傳輸

您可以將檔案傳送給其他對您的受管理網路 (成員) 具有完整或管理存取權的電腦。當您收到檔案時，該檔案會顯示於 EasyNetwork 收件匣中。收件匣是網路上其他電腦傳送給您之所有檔案的暫時儲存位置。

自動印表機共用

當您加入受管理網路之後，便可以與其他成員共用任何連接至電腦的本機印表機，並且將印表機的目前名稱作爲共用印表機名稱。EasyNetwork 也會偵測網路上其他電腦共用的印表機，並讓您設定和使用那些印表機。

第 29 章

設定 EasyNetwork

使用 EasyNetwork 之前，您必須先開啓它，並加入受管理網路。加入受管理網路後，您就可以共用、搜尋與傳送檔案給網路上的其他電腦。您也可以共用印表機。如果您決定離開網路，隨時都可以這麼做。

在本章中

開啓 EasyNetwork 141
加入受管理網路 142
離開受管理網路 145

開啓 EasyNetwork

依預設，系統會在您安裝完 EasyNetwork 後提示您開啓它；但是，您也可以稍後再開啓 EasyNetwork。

- 在 [開始] 功能表上，依序指向 [程式集]、[McAfee]，然後按一下 [McAfee EasyNetwork]。

秘訣：如果您在安裝期間建立桌面圖示和快速啓動圖示，則您也可以按兩下桌面上或工作列最右邊的通知區域中的 McAfee EasyNetwork 圖示來啓動 EasyNetwork。

加入受管理網路

如果您所連線的網路上找不到其他有安裝 SecurityCenter 的電腦，則您會成爲網路的成員，系統也會提示您識別這是否爲信任的網路。因爲您的電腦是第一部加入網路的電腦，所以網路名稱中會包含您的電腦名稱；但是您可以隨時將網路重新命名。

當電腦連線至網路時，會傳送加入請求給網路上的其他電腦。網路上任何具有系統管理權限的電腦都可以允許請求。授權者也可以決定加入網路之電腦的權限等級，例如，來賓存取權 (僅具有檔案傳輸的能力) 或完整/系統管理存取權 (具有檔案傳輸和檔案共用的能力)。在 EasyNetwork 中，具有系統管理存取權的電腦可以將存取權授予其他電腦及管理權限 (將電腦升級或降級)，而具有完整存取權的電腦則無法執行這些系統管理工作。

附註：在您加入後，若您已安裝了其他 McAfee 網路程式 (例如 Network Manager)，這些程式仍會將您的電腦視爲一個受管理的電腦。指派給 EasyNetwork 中電腦的權限等級會套用至所有 McAfee 網路程式。針對來賓權限、完整權限或系統管理權限在其他 McAfee 網路程式中的意義，請參閱該程式所提供的說明文件，以取得詳細資訊。

加入網路

安裝 EasyNetwork 之後，第一次將電腦連線至信任的網路時，系統會出現提示訊息，詢問您是否要加入受管理網路。如果電腦同意加入，加入請求會傳送至網路上具有系統管理存取權的所有其他電腦。此請求必須先獲得允許，電腦才能在網路上共用印表機或檔案，或傳送和複製檔案。網路中的第一台電腦會自動具有系統管理權限。

1. 按一下 [共用檔案] 視窗中的 [加入這個網路]。
   當網路上的系統管理電腦允許您的請求時會出現訊息，詢問是否要允許此電腦和網路上的其他電腦管理彼此的安全性設定。
2. 若要允許此電腦和網路上的其他電腦管理彼此的安全性設定，請按一下 [確定]，否則請按一下 [取消]。
3. 確認允許的電腦所顯示的圖片是否與安全性確認對話方塊中出現的圖片相同，然後按一下 [確定]。

附註：若邀請您加入受管理網路的電腦並未顯示安全性確認對話方塊中出現的相同圖片，則表示受管理網路上發生安全漏洞。加入網路可能會讓您的電腦面臨風險，因此，請按一下安全性確認對話方塊中的 [取消]。

授予對網路的存取權

當電腦請求加入受管理網路時，訊息會傳送至網路上具有系統管理存取權的所有其他電腦。第一部回應的電腦會成爲授權者。如果您是授權者，則您必須負責決定要授予此電腦的存取權類型：來賓存取權、完整存取權或系統管理存取權。

1. 按一下警示中適當的存取層級。
2. 於 [邀請電腦加入受管理網路] 對話方塊中，執行下列其中一項：
   - 按一下 [允許受管理網路程式擁有來賓存取權]，允許電腦存取網路 (您可以對家中的臨時使用者使用此選項)。
   - 按一下 [允許受管理網路程式擁有完整存取權]，允許電腦存取網路。
   - 按一下 [允許受管理網路程式擁有系統管理存取權]，允許電腦以系統管理的權限存取網路。此選項亦可讓電腦對要加入受管理網路的其他電腦授予存取權。
3. 按一下 [確定]。
4. 確認電腦所顯示的圖片與安全性確認對話方塊中出現的圖片相同，然後按一下 [授予存取權]。

附註：如果電腦所顯示的圖片與安全性確認對話方塊中出現的圖片不同，則表示受管理網路上發生安全漏洞。將網路存取權授予此電腦可能會讓您的電腦面臨風險，因此，請按一下安全性確認對話方塊中的 [拒絕存取權]。

重新命名網路

依預設，網路名稱包含第一部加入網路之電腦的名稱；但是您可以隨時變更網路名稱。當您重新命名網路時，您可以變更 EasyNetwork 中顯示的網路說明。

1 在 [選項] 功能表上，按一下 [設定]。

2 在 [設定] 對話方塊的 [網路名稱] 方塊中，輸入網路名稱。

3 按一下 [確定]。

離開受管理網路

如果您在加入受管理網路之後，決定不想繼續成爲網路成員，您可以離開網路。離開受管理網路後，您隨時都可以重新加入，但是您必須再度取得權限。如需加入的詳細資訊，請參閱＜加入受管理網路＞(第 142 頁)。

離開受管理網路

您可以離開先前加入的受管理網路。

1 在 [工具] 功能表上，按一下 [離開網路]。

2 在 [離開網路] 對話方塊中，選取您想要離開的網路名稱。

3 按一下 [離開網路]。

第 30 章

共用和傳送檔案

EasyNetwork 讓您的電腦可以輕鬆地與網路上的其他電腦共用和傳送檔案。當您共用檔案時，同時間便會將檔案的唯讀存取權授予其他電腦。只有受管理網路的成員電腦 (具完整或管理存取權) 可共用或存取其他成員電腦共用的檔案。

附註：如果您共用許多檔案，您的電腦資源將受影響。

在本章中

共用檔案.....148
將檔案傳送至其他電腦.....151

共用檔案

只有受管理網路的成員電腦 (具完整或管理存取權) 可共用或存取其他成員電腦共用的檔案。如果您共用資料夾，則該資料夾及子資料夾中的所有檔案都會共用，但是之後新增至資料夾的檔案則不會自動共用。如果刪除共用的檔案或資料夾，則 [共用檔案] 視窗中會移除這些檔案或資料夾。您可以隨時停止共用檔案。

要存取共用檔案，可以直接從 EasyNetwork 開啓檔案，或將檔案複製到您的電腦上再加以開啓。如果您的共用檔案清單很大且很難找到檔案在哪裡，您可以搜尋它。

附註：使用 EasyNetwork 共用的檔案無法從使用 Windows 檔案總管的其他電腦進行存取，因爲 EasyNetwork 檔案共用必須透過安全連線來執行。

共用檔案

當您共用檔案時，對受管理網路具有完整存取權或系統管理存取權的所有成員都可以使用這個檔案。

1. 在 Windows 檔案總管中，尋找您想要共用的檔案。
2. 將檔案從 Windows 檔案總管中拖曳到 EasyNetwork 的 [共用的檔案] 視窗。

秘訣：您也可以按一下 [工具] 功能表上的 [共用檔案] 來共用檔案。在 [共用] 對話方塊中，瀏覽至您想要共用的檔案所存放的資料夾、選取檔案，然後按一下 [共用]。

停止共用檔案

如果您在受管理網路上共用檔案，則可以隨時停止共用檔案。當您停止共用檔案時，受管理網路上的其他成員就無法存取此檔案。

1. 在 [工具] 功能表上，按一下 [停止共用檔案]。
2. 在 [停止共用檔案] 對話方塊中，選取您不想再繼續共用的檔案。
3. 按一下 [確定]。

複製共用的檔案

您可以複製共用檔案，這樣一來即使檔案不再共用，您的電腦上仍然有該檔案。您可以從受管理網路上的任何電腦複製共用的檔案。

- 將檔案從 EasyNetwork 的 [共用檔案] 視窗拖曳到 Windows 檔案總管或 Windows 桌面上。

秘訣：您也可以選取 EasyNetwork 中的檔案，然後按一下 [工具] 功能表上的 [複製到]，來複製共用的檔案。在 [複製到資料夾] 對話方塊中，導覽至您想要複製檔案的資料夾、選取資料夾，然後按一下 [儲存]。

搜尋共用的檔案

您可以搜尋由您或任何其他網路成員所共用的檔案。當您輸入搜尋條件時，EasyNetwork 會在 [共用的檔案] 視窗顯示對應的結果。

1. 在 [共用的檔案] 視窗中，按一下 [搜尋]。
2. 按一下 [包含] 清單中的適當選項 (第 149 頁)。
3. 在 [檔案或路徑名稱] 清單中輸入部分或完整的檔案名稱或路徑。
4. 按一下 [類型] 清單中適當的檔案類型 (第 149 頁)。
5. 在 [開始時間] 與 [結束時間] 清單中，按一下代表檔案建立日期範圍的日期。

搜尋條件

下表說明您在搜尋共用檔案時可以指定的搜尋條件。

檔案或路徑名稱。

包含	說明
包含所有文字	在 [檔案或路徑名稱] 清單中，搜尋包含您所指定之所有文字的檔案名稱或路徑名稱 (不依順序排列)。
包含任何文字	在 [檔案或路徑名稱] 清單中，搜尋包含您所指定之任何文字的檔案名稱或路徑名稱。
包含完全符合的字串	在 [檔案或路徑名稱] 清單中，搜尋包含與您所指定之字串完全符合的檔案名稱或路徑名稱。

檔案類型

類型	說明
任何	搜尋所有共用的檔案類型。

類型	說明
文件	搜尋所有共用的文件。
映像	搜尋所有共用的影像檔。
視訊	搜尋所有共用的視訊檔。
音訊	搜尋所有共用的音訊檔。
已壓縮	搜查所有的壓縮檔 (例如 .zip 檔)。

將檔案傳送至其他電腦

您可以將檔案傳送至屬於受管理網路之成員的電腦。傳送檔案之前，EasyNetwork 會先確認接收檔案的電腦是否有足夠的可用硬碟空間。

當您收到檔案時，該檔案會顯示於 EasyNetwork 收件匣中。收件匣是網路上其他電腦傳送給您之檔案的暫時儲存位置。如果您在接收檔案時開啓 EasyNetwork，則檔案會立即出現在您的收件匣中，否則，在工作列最右邊的通知區域中會出現訊息。如果您不想收到通知訊息 (例如，訊息會打斷您的工作)，可以關閉此功能。如果收件匣中已經有同名的檔案，則新的檔案會加上數值尾碼來重新命名。在您接受檔案 (將檔案複製到您的電腦) 之前，檔案會留在您的收件匣中。

將檔案傳送到另一部電腦

您可以將檔案傳送到受管理網路上的另一部電腦，而不需再共用檔案。接收者電腦上的使用者必須先將檔案儲存至本機位置，才能檢視檔案。如需詳細資訊，請參閱＜從另一部電腦接受檔案＞(第 151 頁)。

1. 在 Windows 檔案總管中，尋找您想要傳送的檔案。
2. 將檔案從 Windows 檔案總管中拖曳到 EasyNetwork 的作用中電腦圖示。

秘訣：在選取檔案時按住 CTRL 鍵，就可以將多個檔案傳送至電腦。您也可以按一下 [工具] 功能表上的 [傳送]，選取檔案，然後按一下 [傳送]，來傳送檔案。

從另一部電腦接受檔案

如果受管理網路上的另一部電腦傳送檔案給您，您必須接受它 (將檔案儲存到您電腦上)。當檔案傳送至您的電腦時，如果您未開啓 EasyNetwork，則您會在工作列最右邊的通知區域中收到通知訊息。按一下通知訊息，即可開啓 EasyNetwork 並存取檔案。

- 按一下 [接受]，然後將檔案從 EasyNetwork 收件匣拖曳至 Windows 檔案總管中的資料夾。

秘訣：您也可以選取 EasyNetwork 收件匣中的檔案，再按一下 [工具] 功能表上的 [接受]，接收另一部電腦的檔案。在 [接受到資料夾] 對話方塊中，導覽至您想要儲存所接收的檔案之資料夾、選取資料夾，然後按一下 [儲存]。

在檔案傳送時收到通知

當受管理網路上的另一部電腦傳送檔案給您時，您可以收到通知訊息。如果沒有執行 EasyNetwork，在工作列最右邊的通知區域中會出現通知訊息。

1. 在 [選項] 功能表上，按一下 [設定]。
2. 選取 [設定] 對話方塊中的 [當其他電腦傳送檔案給我時，請通知我] 核取方塊。
3. 按一下 [確定]。

第 31 章

共用印表機

當您加入受管理網路之後，EasyNetwork 便會共用連接至電腦的本機印表機，並且將印表機的名稱作爲共用印表機名稱。EasyNetwork 也會偵測網路上其他電腦共用的印表機，並讓您設定和使用那些印表機。

如果您將印表機驅動程式設定爲透過網路列印伺服器 (例如，無線 USB 列印伺服器) 進行列印，EasyNetwork 會將印表機當做本機印表機，並在網路上共用此印表機。您也可以隨時停止共用印表機。

在本章中

使用共用的印表機.....154

使用共用的印表機

EasyNetwork 會偵測網路上電腦所共用的印表機。如果 EasyNetwork 偵測到遠端印表機尚未連線至您的電腦，則當您第一次開啓 EasyNetwork 時，[可用的網路印表機] 連結會出現在 [共用檔案] 視窗中。接著您就可以安裝可用的印表機或解除安裝已經連線至您電腦的印表機。您也可以重新整理印表機清單，以確保您看到的是最新資訊。

如果您沒有加入受管理的網路，但卻已經連線至此網路，您可以從 Windows 印表機控制台存取共用的印表機。

停止共用印表機

當您停止共用印表機，網路的成員就不能使用它。

1. 在 [工具] 功能表上，按一下 [印表機]。
2. 在 [管理網路印表機] 對話方塊中，按一下您不想繼續共用的印表機名稱。
3. 按一下 [不共用]。

安裝可用的網路印表機

如果您是受管理網路的成員，就可以存取共用的印表機，但是您必須安裝印表機所用的驅動程式。如果印表機的擁有者停止共用他的印表機，您就不能再使用它。

1. 在 [工具] 功能表上，按一下 [印表機]。
2. 在 [可用的網路印表機] 對話方塊中，按一下印表機名稱。
3. 按一下 [安裝]。

參考

「術語字彙」列出並定義 McAfee 產品中最常用的安全性術語。

字彙

8

802.11

一組跨無線網路傳輸資料的 IEEE 標準。802.11 俗稱 Wi-Fi。

802.11a

802.11 的延伸模組，可在 5 GHz 頻寬中以最高 54 Mbps 的網路傳輸率來傳送資料。雖然傳輸速度比 802.11b 快，但是所覆蓋的距離小很多。

802.11b

802.11 的延伸模組，可在 2.4 GHz 頻寬中以最高 11 Mbps 的網路傳輸率來傳送資料。雖然傳輸速度比 802.11a 慢，但是所覆蓋的距離大很多。

802.1x

在有線及無線網路上用來進行認證的 IEEE 標準。802.1x 通常與 802.11 無線網路一起使用。

A

ActiveX 控制項

程式或網頁所使用的軟體元件，用以新增如同程式或網頁中正常組件的功能。大部分的 ActiveX 控制項都是無害的；但是，有些可能會從您的電腦擷取資訊。

C

Cookie

是儲存於電腦上且包含個人瀏覽網路之資訊的小型檔案，通常包含使用者名稱和目前的日期與時間。Cookie 主要是網站用來識別先前已向其註冊或曾造訪該網站的使用者，不過，他們也會成爲駭客所用之資訊的來源。

D

DAT

(資料簽章檔) 檔案中包含定義，在您的電腦或 USB 磁碟機上偵測到病毒、特洛依病毒、間諜軟體、廣告軟體、及其他潛在無用程式時就會用到它。

DNS

(網域名稱系統) 將主機名稱或網域名稱轉換爲 IP 位址的系統。在網站上，會使用 DNS 將易讀的網站位置 (如 www.myhostname.com) 轉換爲 IP 位址(如 111.2.3.44)，使網站可以被擷取。沒有 DNS，您就必須在 Web 瀏覽器中輸入 IP 位址本身。

DNS 伺服器

(網域名稱系統伺服器) 可將與主機或網域名稱相關之 IP 位址傳回的電腦。另請參閱＜DNS＞。

E

ESS

(延伸服務集) 兩個以上網路的集合，構成單一子網路。

I

Internet

網際網路是由數量龐大、相互連接的網路所組成的，這些網路的定位及資料傳輸都是使用 TCP/IP 通訊協定。網際網路是由美國國防部所創立的大專院校電腦的連結 (1960 年代末期與 1970 年代初期) -- 稱爲 ARPANET -- 演變而來的。現今的網際網路是由近 100,000 個獨立網路組成的全球網路。

IP address (IP 位址)

在 TCP/IP 網路上之電腦或裝置的識別碼。使用 TCP/IP 通訊協定的網路會根據目的地的 IP 位址傳送訊息。IP 位址的格式是 32 位元的數字位址，共有四段數字，以句點分隔。介於 0 與 255 之間的數字 (如 192.168.1.100)。

L

LAN

(區域網路) 跨越較小區域 (例如同一棟建築) 的電腦網路。LAN 裡頭的電腦可以相互通訊並共用資源，如印表機、檔案。

launchpad

U3 介面元件，爲啓動及管理 U3 USB 程式的起始點。

M

MAC 位址

(媒體存取控制位址) 指派給存取網路之實體裝置的獨特序號。

MAPI

(訊息應用程式發展介面) Microsoft 的介面規格，能讓不同的訊息及工作群組應用程式 (包括電子郵件、語音訊息及傳真) 可以透過單一用戶端來工作，例如 Exchange 用戶端。

MSN

(Microsoft 網路) 一套由 Microsoft Corporation 提供的網頁式服務，包括搜尋引擎、電子郵件、即時訊息和入口網站。

N

NIC

(網路介面卡) 插在筆記型電腦或其他裝置上的卡片，可將裝置連接至區域網路。

P

PCI 無線介面卡

(周邊元件連接) 插在電腦 PCI 擴充插槽中的無線介面卡。

plug-in

與較大程式搭配使用的小型軟體程式，可提供額外的功能。例如，外掛程式可以讓 Web 瀏覽器存取及執行內嵌在 HTML 文件中的檔案，而瀏覽器通常無法辨識這些檔案的格式 (如動畫、視訊及音訊檔案)。

POP3

(郵局通訊協定 3) 介於電子郵件用戶端程式和電子郵件伺服器間的介面。大部份家庭使用者都使用 POP3 電子郵件帳號，亦即所謂的標準電子郵件帳戶。

PPPoE

(使用於乙太網路的點對點通訊協定) 使用點對點通訊協定 (PPP) 號通訊協定、以乙太網路作爲傳輸工具的一種方法。

proxy

構成網路與網際網路間的障礙之電腦 (或是這部電腦上執行的軟體)，它對外部網站僅會顯示一個網路位址。Proxy 代表所有內部電腦，可以在保護網路身份的同時，也繼續提供網際網路存取權。另請參閱＜Proxy 伺服器＞。

Proxy 伺服器

一種防火牆元件，負責管理網際網路進出區域網路 (LAN) 的流量。Proxy 伺服器可以提供常用資料 (例如受歡迎的網頁) 以提高效能，還可以篩選、捨棄擁有者認爲是不適當的要求 (例如要求專用檔案的未授權存取權)。

R

RADIUS

(遠端存取撥入使用者服務) 提供使用者驗證的通訊協定，通常會在遠端存取的內容中。RADIUS 通訊協定原本定義要搭配撥入遠端存取伺服器使用，現在則用於各種驗證環境中，包括 WLAN 使用者共用密碼的 802.1x 驗證。

rootkit

工具 (程式) 的集合，授予給使用者電腦或電腦網路的管理員層級存取權。Rookit 可能包含間諜軟體和其他潛在無用程式，這些程式可能會對您的電腦資料和個人資訊造成額外的安全性或隱私權風險。

S

SMTP

(簡易郵件傳輸通訊協定) 將郵件從一部電腦傳送至網路上另一部電腦時，所使用的 TCP/IP 通訊協定。此通訊協定可用在網際網路上遞送電子郵件。

SSID

(服務組識別元) 是識別 Wi-Fi (802.11) 網路的 Token (私密金鑰)。SSID 是由網路管理員設定，且必須由想要加入網路的使用者提供。

SSL

(安全通訊端層) 是由 Netscape 開發的通訊協定，可透過網際網路來傳輸私人文件。SSL 使用公開金鑰來工作，加密透過 SSL 連線傳送的資料。需要 SSL 連線的 URL 都會以 https 開頭，而不是 http。

SystemGuard

McAfee 會偵測電腦上未經授權的變更，並在發生變更時警示您。

T

TKIP

(暫時金鑰完整性協定) 是一種能夠克服 WEP 安全性弱點的協定，尤其是重複使用加密金鑰的弱點問題。每 10,000 個封包，TKIP 會變更一次暫時金鑰，提供動態散發方法，可大幅加強網路的安全性。TKIP (安全性) 程序是從用戶端與存取點 (AP) 之間共用的 128 位元暫時金鑰開始。TKIP 合併暫時金鑰與用戶端的 MAC 位址，然後加入相對較大的 16 個八位元初始化向量，以產生用來加密資料的金鑰。這個程序可確保每個站台用來加密資料的金鑰資料流都不一樣。TKIP 會使用 RC4 來執行加密作業。

U

U3

(您：簡易的、更智慧的行動裝置) 可以讓 Windows 2000 或是 Windows XP 的程式直接從 USB 磁碟上執行的平台。M-Systems 和 SanDisk 在 2004 年率先推出 U3 技術，可讓使用者不需要在 Windows 電腦上安裝或是儲存資料，或是進行設定就可以執行 U3 的程式。

URL

(統一資源定位器) 爲網際網路位址的標準格式。

USB

(通用序列匯流排) 是一種標準化的序列電腦介面，可讓您將周邊裝置 (例如：鍵盤、搖桿以及印表機) 連接到電腦上。

USB 無線介面卡

是一種插入電腦 USB 插槽的無線介面卡。

USB 磁碟

是一種可以插入電腦 USB 埠的小記憶體磁碟。USB 磁碟就像是一個小磁碟機，可讓您更輕易地在電腦之間傳輸檔案。

V

VPN

(虛擬私人網路) 是一種設定在公用網路內的私有網路，因此得以利用公用網路的管理設施。企業使用 VPN 來建立橫跨大範圍的廣域網路 (WAN)，以提供分公司站點對站點的連線，或是讓行動使用者撥接至他們公司的區域網路 (LAN)。

W

Webmail

透過網際網路傳送與接收的電子式郵件。另請參閱＜電子郵件＞。

WEP

(有線等效隱私) 定義爲 Wi-Fi (802.11) 標準一部分的加密及驗證通訊協定。初始版本以 RC4 密碼爲基礎，並具有重大的弱點。WEP 會嘗試透過無線電波來加密資料，以提供安全性，讓資料可以在端點之間傳送時獲得保護。但是，我們發現 WEP 並沒有我們想像中的安全。

Wi-Fi

(無線相容認證) 該術語爲 Wi-Fi 聯盟 (Wi-Fi Alliance) 所使用，指任何類型的 802.11 網路。

Wi-Fi 認證

經由 Wi-Fi 聯盟測試並核准後即爲 Wi-Fi 認證的產品。Wi-Fi 認證 (Wi-Fi Certified) 的產品可彼此互通，即使是來自不同製造商的產品也是一樣。擁有 Wi-Fi 認證產品的使用者，可將任何品牌的存取點 (AP) 用於亦經認證的任何其他品牌用戶端硬體。

Wi-Fi 聯盟 (Wi-Fi Alliance)

由無線硬體及軟體的領導提供者所組成的組織。Wi-Fi 聯盟 (Wi-Fi Alliance) 致力於認證所有 802.11 產品的互通性，將 Wi-Fi 這個術語推廣爲全球性的品牌名稱，用於所有市場上 802.11 無線區域網路的產品。該組織的性質就像協會、測試實驗室，以及想要提升產業成長之廠商的情報交流站。

WLAN

(無線區域網路) 使用無線連線的區域網路 (LAN)。WLAN 使用高頻無線電波 (而非有線) 讓電腦相互通訊。

WPA

(Wi-Fi 保護的存取) 可針對現有及未來無線區域網路系統，強力提升資料保護和存取控制層級的規格標準。WPA 的設計可在現有的硬體上執行，作爲軟體升級，WPA 衍生自 IEEE 802.11i 標準，並與其相容。若安裝得當，可爲無線區域網路使用者高度保證其資料會持續受到保護，而且只有經授權的網路使用者才能存取網路。

WPA-PSK

專爲家庭使用者設計的特殊 WPA 模式，家庭使用者不需要強大的企業級安全性，也沒有驗證伺服器的存取權。在此模式下，家庭使用者要手動輸入啓動密碼，以「預先共用金鑰」模式來啓動「受 Wi-Fi 保護的存取」，並且要經常變更每部無線電腦及存取點的密碼。另請參閱＜WPA2-PSK＞及＜TKIP＞。

WPA2

是 WPA 安全標準的更新，以 802.11i IEEE 標準爲基礎。

WPA2-PSK

一種類似 WPA-PSK 的特殊 WPA 模式，以 WPA2 標準爲基礎。WPA2-PSK 其中一項常見的功能，就是裝置通常會同時支援多種加密模式 (例如：AES、TKIP)，而較舊的裝置通常一次只能支援一種加密模式 (亦即，所有用戶端都必須使用相同的加密模式)。

一劃

一般文字

未加密的文字。另請參閱＜加密＞。

四劃

內容分級群組

在未成年保護中，使用者所屬的年齡組。依據使用者所屬的內容分級群組，顯示或封鎖內容。內容分級群組包括：幼兒、兒童、青少年、少年及成人。

木馬

是一個看似合法的程式，卻可能會毀損極爲重要的檔案、干擾效能，並提供通道以對電腦進行未經授權的存取。

五劃

加密

一種程序，將文字資料轉換成密碼，使資訊變得混亂難懂，讓不知道如何解密的人無法閱讀。加密的資料又稱爲密碼文字。

外接式硬碟

裝在電腦外的硬碟機。

未成年保護

協助限制您的孩童瀏覽 Web 時可以看的內容與可以做的事情之設定值。若要設定未成年保護，您可以啓用或停用影像篩選功能、選擇內容分級群組並設定 Web 瀏覽的時間限制。

用戶端

在個人電腦或工作站上執行，並仰賴伺服器來執行某些作業的應用程式。例如，電子郵件用戶端是可以讓您傳送及接收電子郵件的應用程式。

白名單

容許使用者存取的網站清單，因爲這些網站被認爲不具詐騙性。

六劃

企業內部網路

私人的電腦網路，通常位於組織內部，只有授權的使用者才可以存取。

共用

可以讓電子郵件收件者在一段有限時間內存取所選取的備份檔案。您共用檔案時，會將檔案的備份副本傳送至您指定的電子郵件收件者。收件者會收到 Data Backup 寄送的電子郵件，指出已和收件者共用檔案。電子郵件也會包含到共用檔案的連結。

共用密碼

通訊雙方在開始通訊之前即已分享的字串或金鑰 (通常是密碼)。共用密碼是用來保護 RADIUS 訊息的機密部份。

同步

解決備份檔案與您本機電腦上儲存之檔案不一致的情形。線上備份存放庫中的檔案版本比其他電腦上的檔案版本還要新時，您要將檔案同步。

字典攻擊

一種暴力攻擊法的類型，嘗試用常用字找出密碼。

存取點

一種網路裝置 (一般稱爲無線路由器)，與乙太網路集線器或交換器整合，可延伸無線使用者服務的實際範圍。當無線使用者用行動裝置漫遊時，傳輸會從一個存取點 (AP) 傳遞到另一個存取點以維持連線。

七劃

伺服器

電腦或程式，會接受來自其他電腦或程式的連線，並傳回適當的回應。例如，每次您傳送或接收電子郵件訊息時，您的電子郵件程式就會連線到電子郵件伺服器。

即時掃描

在您或您的電腦存取檔案及資料夾時，掃描它們是否有病毒和其他活動。

完整封存

根據您設定的檔案類型與位置，封存完整的資料集。另請參閱＜快速封存＞。

快取

電腦上的暫時儲存區。例如，爲了增加網路瀏覽速度及效率，瀏覽器會在您下次要檢視某網頁時，從其快取中擷取該網頁 (而不是從遠端伺服器擷取)。

快速封存

只封存自上次完整或快速封存之後，變更過的檔案。另請參閱＜完整封存＞。

快顯視窗

一些小視窗，會在您電腦螢幕上其他視窗之上顯示。快顯視窗通常是在 Web 瀏覽器中，用來顯示廣告。

系統還原點

電腦記憶體或資料庫之內容的快照 (映像)。Windows 會定期並在重要事件發生時 (如安裝程式或驅動程式時) 建立還原點。您也可以隨時建立自己的還原點並爲其命名。

防火牆

一套專門用來防止在未經授權的情況下，與私人網路往來存取的系統 (硬體、軟體、或二者的組合)。人們經常使用防火牆來防止未經授權的網際網路使用者，存取連線至網際網路的私人網路，尤其是內部網路。所有進出內部網路的郵件都要經過防火牆，防火牆會檢查每個郵件，並封鎖不符合特定安全準則的郵件。

八劃

事件

由使用者、裝置或電腦本身初始，會觸發回應的動作。McAfee 會將事件記錄在它的事件記錄檔中。

受管理網路

包含兩種成員的家庭網路：受管理成員與不受管理成員。受管理成員可讓網路上其他電腦監視其保護狀態；而不受管理成員則否。

拒絕服務

一種攻擊的類型，會拖慢或中斷網路的流量。當網路上充斥著許多額外的請求，使正常流量變慢或完全中斷時，就是發生了拒絕服務攻擊 (DoS 攻擊)。這不一定會造成資訊竊取或其他的安全性弱點。

金鑰

由二個裝置用來驗證其通訊作業的一串字母及數字。這二個裝置都必須要有這個金鑰。另請參閱 WEP、WPA、WPA2、WPA-PSK 及 WPA2- PSK。

九劃

信任清單

所包含的項目是您所信任的，而且不會被偵測。如果您錯將某個項目加入信任清單裡 (例如潛在的無用程式或是登錄變更)，或是希望再次偵測該項目，您就必須從清單中移除它。

封存

在 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟機上，建立重要檔案的副本。

指令碼

可以自動執行的命令清單 (亦即不需與使用者互動)。和程式不同的是，指令碼通常是儲存在各自的純文字表單中，在每次要執行時才編譯。巨集和批次檔案也稱爲指令碼。

指定掃描

依要求 (即當您啓動掃描作業) 而啓動的掃描。和即時掃描不一樣的是，指定掃描不會自動啓動。

十劃

家庭網路

家庭中有二部以上的電腦相互連線，彼此可以共用檔案和網際網路存取權。請參閱＜LAN＞。

病毒

是一種會自我複製的程式，可能會更改您的檔案或資料。它們通常看似來自受信任的傳送者，或者看起來內容無害。

訊息認證代碼 (MAC)

一種安全性代碼，用來將電腦間傳輸的郵件加密。如果電腦確認解密的代碼有效，就會接受郵件。

十一劃

僞造 IP

在 IP 封包中僞造 IP 位址。在很多類型的攻擊中，都會使用這種手法，包括工作階段挾持。人們也經常使用此方法，僞造垃圾電子郵件的標題，讓他人難以正確追蹤。

密碼

一組代碼 (通常由字母和數字組成)，您使用這組代碼取得電腦、程式或網站的存取權。

密碼文字

加密文字。密碼文字必須轉換成純文字 (即解密) 之後才能閱讀。

密碼儲存庫

您的個人密碼的安全儲存區域。您可以放心地儲存密碼，沒有任何的其他使用者 (即使是管理員) 能夠存取您的密碼。

捷徑

只包含您電腦上另一個檔案位置的檔案。

掃台者 (wardriver)

配備 Wi-Fi 電腦以及某些特殊硬體或軟體的闖入者，他們開車四處搜尋 Wi-Fi (802.11) 網路。

淺層觀察位置

您電腦上的一個資料夾，Data Backup 會監視這個資料夾的變更。如果您設定淺層觀察位置，Data Backup 會備份該資料夾中的觀察檔類型，但是不會包含其子資料夾。

深層觀察位置

您電腦上的一個資料夾，Data Backup 會監視這個資料夾的變更。如果您設定深層觀察位置，Data Backup 會於該資料夾及其子資料夾內備份觀察檔案類型。

通訊協定

在兩個裝置之間傳輸資料的格式 (硬體或軟體)。如果您想與其他電腦通訊，您的電腦或裝置必須支援正確的通訊協定。

連接埠

資訊進出電腦的地方。例如，傳統的類比數據機是連接到序列埠。

十二劃

備份

在安全的線上伺服器建立重要檔案的副本。

惡意存取點

未經授權的存取點。將惡意存取點安裝在安全公司網路上，可以把網路存取權授予未經授權的一方。也能建立惡意存取點讓攻擊者進行攔截式攻擊。

智慧型磁碟

另請參閱＜USB 磁碟機＞。

無線介面卡

可讓電腦或 PDA 增加無線通訊能力的裝置。它可透過一些方式來連接電腦，例如 USB 埠、PC 卡 (CardBus) 插槽、記憶體卡插槽或內建在 PCI 匯流排中。

登錄

儲存 Windows 組態資訊的資料庫。登錄包含每個電腦使用者及系統硬體、已安裝程式和內容設定之相關資訊的設定檔。Windows 在其作業期間，會持續參照這項資訊。

發佈

將備份的檔案放到網際網路上供人公開存取。您可以透過搜尋 Data Backup 檔案庫來存取已發佈的檔案。

黑名單

防網路釣魚時，被視爲詐欺性的網站清單。

十三劃

節點

與網路連線的單一電腦。

資源回收筒

Windows 系統中模擬的垃圾筒，用來放置刪除的檔案和資料夾。

路由器

將資料封包從一個網路轉送至另一個網路的網路裝置。路由器會根據內部路由表讀取每一個進來的封包，並根據任何來源和目的地位址以及目前的資料傳輸狀況 (如負載量、線路價值、不良線路) 的組合來決定要如何轉送封包。路由器有時候也稱爲存取點 (AP)。

隔離

把不要的隔離。例如，VirusScan 偵測到可疑的檔案會將其隔離，使其不會對您的電腦或檔案造成傷害。

電子郵件

(電子郵件) 可跨電腦網路以電子方式傳送和接收的訊息。另請參閱＜Webmail＞。

電子郵件用戶端

在您的電腦上執行，用來傳送和接收電子郵件的程式(如 Microsoft Outlook)。

十四劃

漫遊

從一個存取點 (AP) 覆蓋區移動至另一個區，而不會中斷服務或連線。

監視位置

Data Backup 在您電腦上監視的資料夾。

網域

區域性的子網路，或是網際網路上網站的描述元。

在區域網路 (LAN) 上，網域是由用戶端和伺服器電腦組成、由一個安全性資料庫控制的子網路。在這種環境中，網域可增進效能。在網際網路上，網域是網址的一部份 (例如 www.abc.com，其中 abc 是網域)。

網路

存取點及其相關使用者的集合，等同於 ESS。

網路臭蟲

一些小圖形檔案，可以將自己內嵌在您的 HTML 頁面中，允許未授權的來源在您的電腦上設定 Cookie。這些 Cookie 之後便可將資訊傳輸至未經授權的來源。網路臭蟲也稱爲網站信標、像素標籤、透明影像圖檔，或看不見的影像圖檔。

網路釣魚

專門爲了從不知情的個人取得寶貴資訊 (如信用卡號碼、社會安全號碼、使用者識別碼、密碼) 的網際網路詐騙手法，以進行詐欺。

網路圖

圖形化展現組成家庭網路的電腦與元件。

網路磁碟機

連接至多位使用者共用的網路上之伺服器的磁碟或磁帶機。網路磁碟機有時亦稱爲遠端磁碟機。

十五劃

影像篩選

未成年保護的選項，會封鎖可能不當的 Web 影像出現。

撥接程式

幫助您建立網際網路連線的軟體。如果惡意使用，撥接程式可以將您的網路連線重新導向您預設的網際網路服務供應商 (ISP) 以外的供應商，不告知您需要額外的花費。

暫存檔

作業系統或其他程式在記憶體中或磁碟上建立的檔案，會在階段作業中使用，之後就會放棄。

暴力攻擊法 (brute-force attack)

將加密的資料 (如密碼) 解碼的一種方法，是利用不斷的嘗試錯誤 (暴力) 而不是運用智慧的策略來破解。暴力法雖然耗時，但不失爲有效的攻擊方法。暴力攻擊法又叫做暴力破解法。

標準電子郵件帳戶

請參閱＜POP3＞。

潛在的無用程式 (PUP)

未經同意便收集及傳輸個人資訊的程式 (如間諜軟體、廣告軟體)。

熱點

Wi-Fi (802.11) 存取點 (AP) 涵蓋的地理界限。使用者利用無線筆記型電腦進入熱點，就可以連線到網際網路，前提是熱點有信標 (亦即廣告它的行蹤) 且不需要認證。熱點通常位於人潮擁擠的地方，如機場。

線上備份存放庫

位於線上伺服器上的位置，您的檔案在備份後會儲存在此位置。

緩衝區溢位

當可疑的程式或程序嘗試將超過緩衝區存放量的資料儲存在電腦的緩衝區 (暫時儲存區) 時，會發生的情況。緩衝區溢位會損毀或覆寫相鄰緩衝區中的資料。

十六劃

整合式閘道

合併存取點 (AP)、路由器及防火牆的裝置。有些裝置亦包含安全加強功能及橋接功能。

頻寬

在固定的時間內能夠傳輸的資料量。

十七劃

壓縮

一種程序，將檔案壓縮成一種格式，使其儲存或傳輸所需的空間減到最小。

檔案片段

散佈在整個磁碟的檔案殘餘片段。檔案片段是因檔案的新增或刪除而產生，會使電腦的處理效能變慢。

檔案庫

已備份和發佈之檔案的線上儲存區。Data Backup 檔案庫是網際網路上的網站，可供擁有網際網路存取權的任何人存取。

還原

從線上備份存放庫或封存，擷取檔案的副本。

十八劃

瀏覽器

用於檢視網際網路上網頁的程式。主流的 Web 瀏覽器包括 Microsoft Internet Explorer 和 Mozilla Firefox。

十九劃

關鍵字

可以指派給已備份檔案的字，以便和指派了相同關鍵字的其他檔案建立關係或連接。爲檔案指派關鍵字，可以更容易搜尋您已發佈至網際網路的檔案。

二十劃

攔截式攻擊

一種攔截的方法，可能會修改通訊二方之間的郵件，而二方皆不知道他們的通訊連線已經被入侵。

蠕蟲

是一種會自我複製的病毒，存在於主動式記憶體中，可透過電子郵件來傳送自身的副本。蠕蟲會複製並消耗系統資源，進而降低效能或中止工作。

二十三劃

驗證

識別個人的程序，通常是用一組獨特的名稱及密碼。

二十五劃以上

觀察的檔案類型

Data Backup 備份或封存在觀察位置中之檔案的類型 (例如，.doc、.xls 等)。

關於 McAfee

總部位於加州 Santa Clara 的 McAfee, Inc. 在防護入侵及安全性危機管理上是全球業界的領導者，提供前瞻且經證實的解決方案與服務，並致力於保護全球的系統及網路安全。McAfee 本著無人可及的安全性專業技術並致力於創新之精神，爲家用使用者、企業、公立機構及服務供應商，提供封鎖攻擊、防止破壞以及持續追蹤並改善其安全性的能力。

所有權

商標特性

AVERT、EPO、EPOLICY ORCHESTRATOR、FLASHBOX、FOUNDSTONE、GROUPSHIELD、HERCULES、INTRUSHIELD、INTRUSION INTELLIGENCE、LINUXSHIELD、MANAGED MAIL PROTECTION、MAX (MCAFEE SECURITYALLIANCE EXCHANGE)、MCAFEE、MCAFEE.COM、NETSHIELD、PORTALSHIELD、PREVENTSYS、PROTECTION-IN-DEPTH STRATEGY、PROTECTIONPILOT、SECURE MESSAGING SERVICE、SECURITYALLIANCE、SITEADVISOR、THREATSCAN、TOTAL PROTECTION、VIREX、VIRUSSCAN。

授權

所有使用者請注意：請仔細閱讀與您所購買之授權相應的適當法律合約，該合約提供了使用授權軟體的一般條款及條件。如果您不知道所取得的授權類型，請洽詢銷售人員，並查閱其他相關授權或您的軟件包裝中隨附、或作爲購買的一部份另外收到的購買訂單文件 (如手冊、產品 CD 上的檔案或從下載軟體套裝的網站上獲得的檔案)。如果您不完全同意合約中提出的條款，請勿安裝軟體。如果適合，您可以將所購買的產品退至 MCAFEE, INC. 或購買地點，以取得全額退款。

第 32 章

客戶及技術支援

SecurityCenter 在偵測到重大與非重大的保護問題時都會回報。重大保護問題需要立即採取動作，並會變更您的保護狀態 (變更顏色爲紅色)。非重大保護問題不需要立即採取動作，可能會也可能不會變更您的保護狀態 (依問題的類型而定)。爲達到綠色的保護狀態，您必須修復所有的重大問題，並修復或略過所有非重大問題。若您需要協助診斷保護問題，可以執行 McAfee Virtual Technician。如需 McAfee Virtual Technician 的詳細資訊，請參閱＜McAfee Virtual Technician 說明＞。

若您是從 McAfee 的合作夥伴或供應商處購買安全性軟體，而不是從 McAfee 購買，請開啓 Web 瀏覽器並前往 www.mcafeehelp.com。然後，在「合作夥伴連結」下，選取您的合作夥伴或供應商以使用 McAfee Virtual Technician。

附註：若要安裝並執行 McAfee Virtual Technician，您必須以 Windows 管理員身份登入電腦。若您不是，則 MVT 可能無法解決您的問題。如需以 Windows 管理員身份登入的相關資訊，請參閱 Windows 說明。使用 Windows Vista™ 當執行 MVT 時系統會提示您。發生這種狀況時，請按一下 [接受]。Virtual Technician 無法與 Mozilla® Firefox 搭配使用。

在本章中

使用 McAfee Virtual Technician.....172
支援與下載.....173

使用 McAfee Virtual Technician

Virtual Technician 就像一般人員、技術支援代表一樣，可以收集您 SecurityCenter 程式的相關資訊，協助解決您電腦的保護問題。執行 Virtual Technician 時，它會進行檢查以確保您的 SecurityCenter 程式可以正常運作。若發現了問題，Virtual Technician 會爲您進行修復，或提供您更多與問題相關的詳細資訊。結束時，Virtual Technician 會顯示其分析結果，且若有需要，還可讓您尋求來自 McAfee 的其他技術支援。

爲維護您電腦與檔案的安全性與完整性，Virtual Technician 不會收集可識別個人身份的相關資訊。

附註：如需 Virtual Technician 的更多資訊，請按一下 Virtual Technician 中的 [說明] 圖示。

啓動 Virtual Technician

Virtual Technician 會收集 SecurityCenter 程式的相關資訊，以協助解決您的保護問題。爲保護您的隱私，此資訊並不包含可識別個人身份的相關資訊。

1. 按一下 [常見工作] 下的 [McAfee Virtual Technician]。
2. 請遵循螢幕上的指示下載並執行 Virtual Technician。

支援與下載

請參閱下列表格以取得您所在國家/地區的「McAfee 支援與下載」網站資訊，包括《使用手冊》。

支援與下載

國家/地區	McAfee 支援	McAfee 下載
澳大利亞	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
巴西	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
加拿大 (英文)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
加拿大 (法文)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
中國 (簡體中文)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
台灣 (繁體中文)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
捷克	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
丹麥	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
芬蘭	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
法國	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
德國	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
英國	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
義大利	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
日本	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
韓國	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
墨西哥	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
挪威	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
波蘭	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

葡萄牙	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
西班牙	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
瑞典	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
土耳其	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
美國	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection 使用手冊

國家/地區	McAfee 使用手冊
澳大利亞	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
中國 (簡體中文)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
台灣 (繁體中文)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
丹麥	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
芬蘭	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
法國	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
德國	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
英國	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
荷蘭	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
義大利	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

韓國	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
波蘭	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
美國	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security 使用手冊

國家/地區	McAfee 使用手冊
澳大利亞	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
中國 (簡體中文)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
台灣 (繁體中文)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
丹麥	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
芬蘭	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
法國	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf

德國	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
英國	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
荷蘭	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
義大利	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
韓國	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
波蘭	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
美國	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus 使用手冊

國家/地區	McAfee 使用手冊
澳大利亞	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
中國 (簡體中文)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
台灣 (繁體中文)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf

捷克	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
丹麥	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
芬蘭	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
法國	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
德國	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
英國	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
荷蘭	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
義大利	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
韓國	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
波蘭	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
美國	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan 使用手冊

國家/地區	McAfee 使用手冊
澳大利亞	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf

加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
中國 (簡體中文)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
台灣 (繁體中文)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
丹麥	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
芬蘭	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
法國	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
德國	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
英國	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
荷蘭	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
義大利	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
韓國	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
波蘭	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
美國	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

請參考下列表格，以取得您所在國家/地區的 McAfee Threat Center 與病毒資訊網站。

國家/地區	保安總部	病毒資訊
澳大利亞	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
巴西	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
加拿大 (英文)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
加拿大 (法文)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
中國 (簡體中文)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
台灣 (繁體中文)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
捷克	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
丹麥	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
芬蘭	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
法國	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
德國	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
英國	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
荷蘭	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
義大利	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
日本	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
韓國	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
墨西哥	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
挪威	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
波蘭	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
葡萄牙	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
西班牙	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
瑞典	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
土耳其	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
美國	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

請參考下列表格，以取得您所在國家/地區的 HackerWatch 網站。

國家/地區	HackerWatch
澳大利亞	www.hackerwatch.org
巴西	www.hackerwatch.org/?lang=pt-br
加拿大 (英文)	www.hackerwatch.org
加拿大 (法文)	www.hackerwatch.org/?lang=fr-ca
中國 (簡體中文)	www.hackerwatch.org/?lang=zh-cn
台灣 (繁體中文)	www.hackerwatch.org/?lang=zh-tw
捷克	www.hackerwatch.org/?lang=cs
丹麥	www.hackerwatch.org/?lang=da
芬蘭	www.hackerwatch.org/?lang=fi
法國	www.hackerwatch.org/?lang=fr
德國	www.hackerwatch.org/?lang=de
英國	www.hackerwatch.org
荷蘭	www.hackerwatch.org/?lang=nl
義大利	www.hackerwatch.org/?lang=it
日本	www.hackerwatch.org/?lang=jp
韓國	www.hackerwatch.org/?lang=ko
墨西哥	www.hackerwatch.org/?lang=es-mx
挪威	www.hackerwatch.org/?lang=no
波蘭	www.hackerwatch.org/?lang=pl
葡萄牙	www.hackerwatch.org/?lang=pt-pt
西班牙	www.hackerwatch.org/?lang=es
瑞典	www.hackerwatch.org/?lang=sv
土耳其	www.hackerwatch.org/?lang=tr
美國	www.hackerwatch.org

索引

8

802.11 156
802.11a 156
802.11b 156
802.1x 156

A

ActiveX 控制項 156

C

Cookie 156

D

DAT 156
DNS 156
DNS 伺服器 157

E

EasyNetwork 的功能 140
ESS 157

I

Internet 157
IP address (IP 位址) 157

L

LAN 157
launchpad 157

M

MAC 位址 157
MAPI 157
McAfee EasyNetwork 139
McAfee Network Manager 125
McAfee Personal Firewall 55
McAfee QuickClean 109
McAfee SecurityCenter 5
McAfee Shredder 121
McAfee VirusScan 27
MSN 157

N

Network Manager 的功能 126
NIC 157

P

PCI 無線介面卡 158
Personal Firewall 功能 56
plug-in 158
POP3 158
PPPoE 158
proxy 158
Proxy 伺服器 158

Q

QuickClean 功能 110

R

RADIUS 158
rootkit 158

S

SecurityCenter 功能 6
Shredder 功能 122
SMTP 158
SSID 159
SSL 159
SystemGuard 159

T

TKIP 159

U

U3 159
URL 159
USB 159
USB 無線介面卡 159
USB 磁碟 159

V

VirusScan 功能 28
VPN 160

W

Webmail 160
WEP 160
Wi-Fi 160

Wi-Fi 認證 160
Wi-Fi 聯盟 (Wi-Fi Alliance)....160
WLAN....160
WPA....160
WPA2....161
WPA2-PSK....161
WPA-PSK....160

一劃

一般文字....161

四劃

允許存取現有的系統服務通訊埠....85
允許程式具有完整存取權....76
允許程式具有限出埠存取權....78
允許程式具有網際網路存取權....76
允許新程式具有完整存取權....76
內容分級群組....161
分析入埠及出埠流量....104
手動修復保護問題....16
支援與下載....173
木馬....161

五劃

出現警示時播放聲音....22
加入受管理網路....132, 142, 145
加入網路....142
加密....161
外接式硬碟....161
未成年保護....161
用戶端....161
白名單....161
立即解除鎖定防火牆....74
立即鎖定防火牆....74

六劃

企業內部網路....162
共用....162
共用印表機....153
共用和傳送檔案....147
共用密碼....162
共用檔案....148
同步....162
在啓動時隱藏片頭畫面....22
在遠端電腦上安裝 McAfee 安全性軟體 138
在檔案傳送時收到通知....152
字典攻擊....162
存取網路圖....130
存取點....162
安裝可用的網路印表機....154
自動修復保護問題....16

七劃

伺服器....162
刪除 QuickClean 工作....117
刪除磁碟重組工具工作....118
即時掃描....162
完整封存....162
快取....162
快速封存....162
快顯視窗....163
更新 SecurityCenter....13
系統還原點....163
防火牆....163

八劃

事件....163
事件記錄....98
使用 McAfee Virtual Technician....172
使用 SecurityCenter....7
使用 SystemGuard 選項....41
使用共用的印表機....154
使用信任的清單....46
使用掃描結果....51
使用統計資料....100
使用警示....14, 19, 61
取得程式資訊....82
取得電腦註冊資訊....101
取得電腦網路資訊....101
受管理網路....163
所有權....169
拒絕服務....163
玩遊戲時顯示警示....63
金鑰....163

九劃

信任清單....163
信任電腦連線....90
客戶及技術支援....171
封存....163
封鎖程式的存取權....79
封鎖程式的網際網路存取權....79
封鎖新程式的存取權....79
封鎖對現有系統服務通訊埠的存取....85
指令碼....163
指定掃描....164

重新命名網路.....130, 144
重新整理網路圖.....130

十劃

修改 QuickClean 工作.....116
修改系統服務通訊埠.....86
修改受管理電腦的權限.....136
修改裝置的顯示內容.....137
修改磁碟重組工具工作.....118
修復安全性弱點.....138
修復或略過保護問題.....8, 15
修復保護問題.....8, 16
家庭網路.....164
病毒.....164
記錄、監視及分析.....97
訊息認證代碼 (MAC).....164
追蹤監視的 IP 位址.....103
追蹤網路電腦的地理位置.....101
追蹤網際網路流量.....101

十一劃

僞造 IP.....164
停止共用印表機.....154
停止共用檔案.....148
停止即時病毒防護.....29
停止防火牆保護.....59
停止信任網路上的電腦.....134
停止監視電腦的保護狀態.....136
停用自動更新.....14
停用自動建議.....70
參考.....155
密碼.....164
密碼文字.....164
密碼儲存庫.....164
將安全性等級設爲 [信任].....68
將安全性等級設爲 [秘密].....67
將安全性等級設爲 [開放].....69
將安全性等級設爲 [標準].....68
將安全性等級設爲 [鎖定].....67
將安全性等級設爲 [嚴密].....68
將電腦進行磁碟重組.....114
將檔案傳送至其他電腦.....151
將檔案傳送到另一部電腦.....151
從入侵偵測事件記錄檔追蹤電腦.....102
從入侵偵測事件記錄檔禁止電腦.....95
從入埠事件記錄檔追蹤電腦.....102
從入埠事件記錄檔新增信任的電腦.....91
從入埠事件記錄檔禁止電腦.....95
從出埠事件記錄檔允許完整存取權.....77
從出埠事件記錄檔允許限出埠存取權.....78
從出埠事件記錄檔取得程式資訊.....82
從另一部電腦接受檔案.....151
從最近的事件記錄檔允許完整存取權.....77
從最近的事件記錄檔允許限出埠存取權.....78
從最近的事件記錄檔封鎖存取權.....80
捷徑.....164
掃台者 (wardriver).....164
掃描您的電腦.....29, 49
掃描電腦.....49
授予對網路的存取權.....143
授權.....170
排定掃描.....39
排程 QuickClean 工作.....115
排程工作.....115
排程磁碟重組工具工作.....117
啓用 SystemGuard 保護.....42
啓用自動建議.....70
啓動 HackerWatch 教學課程.....108
啓動 Virtual Technician.....172
啓動即時病毒防護.....29
啓動即時訊息保護.....33
啓動防火牆.....59
啓動防火牆保護.....59
啓動其他保護.....31
啓動指令碼掃描防護.....32
啓動期間保護您的電腦.....72
啓動間諜軟體保護.....32
啓動電子郵件保護.....32
淺層觀察位置.....164
清理您的電腦.....111, 112
深層觀察位置.....164
略過保護問題.....17
移除系統服務通訊埠.....87
移除信任的電腦連線.....92
移除程式的存取權.....81
移除程式權限.....81
移除禁止的電腦連線.....94
處理病毒及特洛伊病毒.....51
處理隔離的程式與 Cookie.....53
處理隔離的檔案.....52
處理潛在的無用程式.....52
設定 EasyNetwork.....141
設定 Ping 要求設定.....72
設定 SystemGuard 選項.....42
設定一個受管理網路.....129

設定入侵偵測 73
設定手動掃描位置 38
設定手動掃描選項 37
設定自動更新 14
設定即時掃描選項 36
設定系統服務通訊埠 84
設定防火牆保護 65
設定防火牆保護狀態設定 73
設定事件記錄檔設定 98
設定病毒防護 35, 49
設定新的系統服務通訊埠 85
設定警示的 [自動建議] 70
設定警示選項 22
通訊協定 165
連接埠 165

十二劃

備份 165
最佳化防火牆安全性 72
惡意存取點 165
智慧型磁碟 165
無線介面卡 165
登錄 165
發佈 165
開啓 EasyNetwork 141
黑名單 165

十三劃

僅顯示自動建議 71
搜尋共用的檔案 149
搜尋條件 149
新增信任的電腦連線 90
新增禁止的電腦連線 93
禁止電腦連線 93
節點 165
資源回收筒 165
路由器 166
遊戲時顯示或隱藏資訊警示 20
隔離 166
電子郵件 166
電子郵件用戶端 166

十四劃

漫遊 166
監視位置 166
監視狀態與權限 136
監視程式活動 105
監視程式頻寬 105
監視電腦的保護狀態 136
監視網際網路流量 104
管理系統服務 83
管理防火牆安全性等級 66
管理信任的清單 46
管理您的 McAfee 帳戶 11
管理程式及權限 75
管理裝置 137
管理資訊警示 63
管理電腦連線 89
網域 166
網路 166
網路臭蟲 166
網路釣魚 166
網路圖 166
網路磁碟機 167
與網路圖一起運作 130
遠端管理網路 135

十五劃

影像篩選 167
撥接程式 167
暫存檔 167
暴力攻擊法 (brute-force attack) 167
標準電子郵件帳戶 167
潛在的無用程式 (PUP) 167
熱點 167
確認您的訂閱 11
編輯信任的電腦連線 91
編輯禁止的電腦連線 94
線上備份存放庫 167
緩衝區溢位 167
複製共用的檔案 149
銷毀整個磁碟 124
銷毀檔案、資料夾及磁碟 123
銷毀檔案與資料夾 123

十六劃

整合式閘道 167
頻寬 167

十七劃

壓縮 168
檔案片段 168
檔案庫 168
檢查更新 13, 14
檢視入侵偵測事件 99
檢視入埠事件 99

檢視出埠事件.....77, 99
檢視全球安全性事件統計資料.....100
檢視全球網際網路通訊埠活動.....100
檢視事件.....16, 25
檢視所有事件.....25
檢視掃描結果.....50
檢視最近的事件.....25, 98
檢視項目的詳細資料.....131
瞭解 Network Manager 圖示.....127
瞭解保護服務.....10
瞭解保護狀態.....7, 8, 9
瞭解保護類別.....7, 9, 25
瞭解程式.....82
瞭解網際網路安全性.....107
還原.....168
還原防火牆設定.....74
邀請電腦加入受管理網路.....133
隱藏病毒爆發警示.....22
隱藏資訊警示.....63

十八劃

瀏覽器.....168
簡介.....3
鎖定及還原防火牆.....74
離開受管理網路.....145

十九劃

關於 McAfee.....169
關於 SystemGuard 類型.....43
關於信任清單類型.....46, 47
關於流量分析圖.....104
關於警示.....62
關鍵字.....168

二十劃

攔截式攻擊.....168
蠕蟲.....168

二十三劃

顯示或隱藏略過的問題.....17
顯示或隱藏資訊警示.....20
顯示或隱藏網路圖上的項目.....131
顯示與隱藏資訊警示.....20
驗證.....168

二十五劃

觀察的檔案類型.....168