

Customer Submission Tool

2.0 版本

McAfee®
系統保護

業界領先的入侵防禦解決方案

McAfee®

版權

Copyright © 2005 McAfee, Inc.。保留所有權利。

未經 McAfee, Inc. 或其供應商或附屬公司的書面許可，不得將本出版物的任何部份以任何形式，或以任何方式複製、傳送、轉錄、儲存於資訊擷取系統或者翻譯為任何語言。

商標歸屬聲明

ACTIVE FIREWALL、ACTIVE SECURITY、ACTIVESECURITY (及片假名)、ACTIVESHIELD、CLEAN-UP、DESIGN (特殊樣式的 E)、DESIGN (特殊樣式的 N)、ENTERCEPT、EPOLICY ORCHESTRATOR、FIRST AID、FOUNDSTONE、GROUPSHIELD、GROUPSHIELD (及片假名)、INTRUSHIELD、INTRUSION PREVENTION THROUGH INNOVATION、MCAfee、MCAfee (及片假名)、MCAfee AND DESIGN、MCAfee.COM、MCAfee VIRUSSCAN、NET TOOLS、NET TOOLS (及片假名)、NETSCAN、NETSHIELD、NUTS & BOLTS、OIL CHANGE、PRIMESUPPORT、SPAMKILLER、THREATSCAN、TOTAL VIRUS DEFENSE、VIREX、VIRUS FORUM、VIRUSCAN、VIRUSSCAN、VIRUSSCAN (及片假名)、WEBSCAN、WEBSHIELD、WEBSHIELD (及片假名) 均為 McAfee, Inc. 和/或其附屬公司在美國和/或其他國家/地區的註冊商標或商標。代表「安全」的紅色是 McAfee 品牌產品的特色。本文中所有其他已註冊和未註冊商標均為其各自所有者的專有財產。

授權資訊

授權合約

所有使用者請注意：請仔細閱讀與您所購買授權對應的適當法律合約，合約中規定了使用授權軟體所需遵守之一般條款和條件。若您不知道所取得的授權類型，請洽詢銷售人員，並查閱軟體包裝中隨附的、或做為購買的一部分另外收到的其他相關授權或購買訂單文件 (小冊子、產品光碟上的檔案或可從下載軟體套件的網站取得之檔案)。若您不同意該合約中規定的所有條款，請勿安裝本軟體。如果適用，您可以將產品退回 MCAfee 或原購買處以獲得全額退款。

歸屬聲明

本產品包括或可能包括：

- 由 OpenSSL Project (<http://www.openssl.org/>) 開發以在 OpenSSL Toolkit 中使用的軟體。
- 由 Eric A. Young 編寫的密碼編譯軟體和由 Tim J. Hudson 編寫的軟體。
- 一些按照 GNU 通用公共授權 (GPL) 或其他類似免費軟體授權 (除其他權利以外，還允許使用者複製、修改並重新散發某些程式或其部分，並擁有來源碼的存取權) 而授權 (或再授權) 使用者的軟體程式。GPL 要求依據 GPL 散發給他人的可執行二進制格式之任何軟體，其來源碼也應可以由使用者使用。對於 GPL 涵蓋的任何軟體，其來源碼均可從本 CD 中獲得。如果任何免費軟體授權合約要求 McAfee 提供超出本合約中授與的權利範圍的使用、複製或修改軟體程式的權利，則這些權利應優先於此處的權利和限制。
- 由 Henry Spencer 原創編寫的軟體，Copyright 1992，1993，1994。
- 由 Robert Nordier 原創編寫的軟體，Copyright © 1996-7 Robert Nordier。
- 由 Douglas W. Sauder 編寫的軟體。
- 由 Apache Software Foundation (<http://www.apache.org/>) 開發的軟體。此軟體的授權合約位於 www.apache.org/licenses/LICENSE-2.0.txt。
- International Components for Unicode (「ICU」) Copyright © 1995-2002 International Business Machines Corporation 及其他公司。
- 由 CrystalClear Software, Inc. 開發的軟體，Copyright © 2000 CrystalClear Software, Inc.。
- FEAD® Optimizer 技術，Copyright Netopsystems AG, Berlin, Germany。
- Outside In® Viewer Technology © 1992-2001 Stellant Chicago, Inc. 和/或 Outside In® HTML Export，© 2001 Stellant Chicago, Inc.。
- Thai Open Source Software Center Ltd. 和 Clark Cooper 擁有版權的軟體，© 1998，1999，2000。
- Expat maintainers 擁有版權的軟體。
- The Regents of the University of California 擁有版權的軟體，© 1996，1989，1998-2000。
- Gunnar Ritter 擁有版權的軟體。
- Sun Microsystems, Inc. (4150 Network Circle, Santa Clara, California 95054, U.S.A.) 擁有版權的軟體，© 2003。
- Gisle Aas 擁有版權的軟體。
- © 1995-2003。
- Michael A. Chase 擁有版權的軟體，© 1999-2000。
- Neil Winton 擁有版權的軟體，© 1995-1996。
- RSA Data Security, Inc. 擁有版權的軟體，© 1990-1992。
- Sean M. Burke 擁有版權的軟體，© 1999，2000。
- Martijn Koster 擁有版權的軟體，© 1995。
- Brad Appleton 擁有版權的軟體，© 1996-1999。
- Michael G. Schwern 擁有版權的軟體，© 2001。
- Graham Barr 擁有版權的軟體，© 1998。
- Larry Wall 和 Clark Cooper 擁有版權的軟體，© 1998-2000。
- Frodo Looijaard 擁有版權的軟體，© 1997。
- Python Software Foundation 擁有版權的軟體，Copyright © 2001，2002，2003。本軟體的授權合約位於 www.python.org。
- Beman Dawes 擁有版權的軟體，© 1994-1999，2002。
- Andrew Lumsdaine、Lie-Quan Lee 和 Jeremy G. Siek 編寫的軟體，© 1997-2000 University of Notre Dame。
- Simone Bordet 和 Marco Cravero 擁有版權的軟體，© 2002。
- Stephen Purcell 擁有版權的軟體，© 2001。
- Indiana University Extreme!Labs (<http://www.extreme.indiana.edu/>) 開發的軟體。
- International Business Machines Corporation 及其他公司擁有版權的軟體，© 1995-2003。
- University of California, Berkeley 及其投資者開發的軟體。
- Ralf S. Engelschall <rs@engelschall.com> 開發用於 mod_ssl 專案 (<http://www.modssl.org/>) 的軟體。
- Kevlin Henney 擁有版權的軟體，© 2000-2002。
- Peter Dimov 和 Multi Media Ltd. 擁有版權的軟體，© 2001，2002。
- David Abrahams 擁有版權的軟體，© 2001，2002。請參閱 <http://www.boost.org/libs/bind/bind.html> 以獲取說明文件。
- Steve Cleary, Beman Dawes、Howard Hinnant 和 John Maddock 擁有版權的軟體，© 2000。
- Boost.org 擁有版權的軟體，© 1999-2002。
- Nicolai M. Josuttis 擁有版權的軟體，© 1999。
- Jeremy Siek 擁有版權的軟體，© 1999-2001。
- Daryle Walker 擁有版權的軟體，© 2001。
- Chuck Allison 和 Jeremy Siek 擁有版權的軟體，© 2001，2002。
- Samuel Krempf 擁有版權的軟體，© 2001。請參閱 <http://www.boost.org> 以獲取更新、說明文件和修訂歷史記錄。
- Doug Gregor (gregod@cs.rpi.edu) 擁有版權的軟體，© 2000，2002。
- Cadenza New Zealand Ltd. 擁有版權的軟體，© 2000。
- Jens Maurer 擁有版權的軟體，© 2000，2001。
- Jaakko Järvi (jaakko.jarvi@cs.utu.fi) 擁有版權的軟體，© 1999，2000。
- Ronald Garcia 擁有版權的軟體，© 2002。
- David Abrahams、Jeremy Siek 和 Daryle Walker 擁有版權的軟體，© 1999-2001。
- Stephen Cleary (shammah@voyager.net) 擁有版權的軟體，© 2000。
- Housemarque Oy <<http://www.housemarque.com>> 擁有版權的軟體，© 2001。
- Paul Moore 擁有版權的軟體，© 1999。
- Dr. John Maddock 擁有版權的軟體，© 1998-2002。
- Greg Colvin 和 Beman Dawes 擁有版權的軟體，© 1998，1999。
- Peter Dimov 擁有版權的軟體，© 2001，2002。
- Jeremy Siek 和 John R. Bandela 擁有版權的軟體，© 2001。
- Joerg Walter 和 Mathias Koch 擁有版權的軟體，© 2000-2002。
- Carnegie Mellon University 擁有版權的軟體，© 1989，1991，1992。
- Cambridge Broadband Ltd. 擁有版權的軟體，© 2001-2003。
- Sparta, Inc. 擁有版權的軟體，© 2003-2004。
- Cisco, Inc. 和北京郵電大學資訊網路中心擁有版權的軟體，© 2004。
- Simon Josefsson 擁有版權的軟體，© 2003。
- Thomas Jacob 擁有版權的軟體，© 2003-2004。
- Advanced Software Engineering Limited 擁有版權的軟體，© 2004。
- Todd C. Miller 擁有版權的軟體，© 1998。
- The Regents of the University of California 擁有版權的軟體，© 1990，1993，代碼從 Chris Torek 發行至 Berkeley 的軟體擷取。

目錄

1	簡介	4
	產品功能	4
	此版本的新增功能	5
	改進的工具存取	5
	將電子郵件提交至更多目標	5
	自動使用黑名單和白名單	6
	不限制提交的樣本數量	6
	提交後自動刪除	6
	使用此指南	7
	適用對象	7
	慣例	8
	取得產品資訊	9
	連絡資訊	10
2	關於垃圾郵件和假冒詐騙	11
	一些有用術語	11
	哪些是垃圾郵件？	12
	避免垃圾郵件	12
	哪些是假冒詐騙？	13
	避免假冒詐騙	13
	何為 Customer Submission Tool？	14
	貝氏學習	15
	瞭解垃圾郵件分數	15
3	安裝此工具	16
	安裝檢核清單	17
	下載安裝檔案	18
	手動安裝此工具	18
	使用指令碼安裝此工具	19
	範例	21
	向電子郵件使用者宣告工具	21
	變更設定	22
4	使用工具	23
	提交第一個垃圾郵件或假冒詐騙樣本	23
	提交更多垃圾郵件或假冒詐騙樣本	24
	提交第一個被錯誤分類的樣本	25
	提交更多被錯誤分類的樣本	26
	新增 Microsoft Outlook 連絡人至白名單	26
	設定此工具	27

1

簡介

McAfee Customer Submission Tool 可與 Microsoft® Outlook® 電子郵件軟體配合使用，以協助您減少所接收無用電子郵件（或垃圾郵件）的數量。此工具會將電子郵件直接轉發至 McAfee Lab 或其他 McAfee 產品，從而能夠分析樣本，並用於進一步減少垃圾郵件。

本章節包含以下主題：

- 產品功能
- 此版本的新增功能
- 使用此指南

產品功能

McAfee Customer Submission Tool 可與以下軟體配合使用：

- Secure Content Management 設備
- McAfee Quarantine Manager 軟體

此工具可為 Microsoft Outlook 用戶端新增工具列按鈕和功能表項目，並可讓您：

- 將樣本提交至 McAfee Lab 以進行進一步分析。
- 將樣本提交至 McAfee Quarantine Manager 或 Secure Content Management 設備，以協助您防止其他垃圾郵件。
- 提交未分類為垃圾郵件（或假冒詐騙）的無用電子郵件。
- 提交被錯誤分類為垃圾郵件（或假冒詐騙）的電子郵件。
- 在提交後可選擇將郵件刪除。
- 將垃圾郵件寄件者的電子郵件地址新增至黑名單，以防止更多的垃圾郵件。
- 將寄件者的電子郵件地址新增至白名單，以阻止將該寄件者的其他電子郵件錯誤分類為垃圾郵件或假冒詐騙。
- 將您 Microsoft Outlook 「聯絡人」資料夾中的所有電子郵件地址新增至白名單，以阻止將來自已知聯絡人的電子郵件錯誤分類為垃圾郵件或假冒詐騙。

您可以使用精靈來安裝此工具。如果您要為多個電子郵件使用者安裝此產品，則可以使用指令碼安裝。

此版本的新增功能

此版本的 Customer Submission Tool 包含以下新增功能或增強功能：

- [改進的工具存取](#)
- [將電子郵件提交至更多目標](#)
- [自動使用黑名單和白名單](#)
- [不限制提交的樣本數量](#)
- [提交後自動刪除](#)

改進的工具存取

舊版	顯示主旨行時，標準工具列上的按鈕和「動作」功能表中的項目均可用。
目前版本	此外，在檢視電子郵件時，標準工具列上的按鈕和「動作」功能表中的項目亦可用。
好處	此工具可更廣泛地在 Microsoft Outlook 中使用。
瞭解更多資訊	請參閱第 23 頁的 「使用工具」 。

將電子郵件提交至更多目標

舊版	您可將電子郵件提交至 McAfee Lab 進行分析。McAfee 可分析被錯誤分類的電子郵件，以改進其防垃圾郵件產品的偵測率。
目前版本	您可以將電子郵件提交至其他位置： <ul style="list-style-type: none"> ■ McAfee Secure Content Management 設備 ■ McAfee Quarantine Manager 軟體
好處	樣本可改進貝氏資料庫的效能，該資料庫經過訓練可識別垃圾郵件、假冒詐騙和可接受郵件。
何處尋找	本功能在安裝此工具後即可使用，或在稍後進行設定。
瞭解更多資訊	請參閱第 23 頁的 「使用工具」 。

自動使用黑名單和白名單

舊版	不具備此功能。
目前版本	<p>本功能在將此工具與 McAfee Quarantine Manager (MQM) 配合使用時可用。</p> <p>可將寄件者自動新增至白名單 (可信任電子郵件地址的清單) 或黑名單 (已知會傳送垃圾郵件至電子郵件地址的清單)。</p> <p>只需按一下，就可將您的 Microsoft Outlook 「聯絡人」新增至白名單。</p>
好處	將來會自動把來自已識別垃圾郵件製造者的電子郵件分類為垃圾郵件，而來自可靠來源的電子郵件則不會被分類為垃圾郵件。
何處尋找	將任何電子郵件提交至 MQM 進行分析時均可使用此功能。
瞭解更多資訊	請參閱第 26 頁的「 新增 Microsoft Outlook 連絡人至白名單 」。

不限制提交的樣本數量

舊版	一次提交至多 10 個樣本。
目前版本	無此限制。
好處	提交郵件更為快捷和輕鬆。

提交後自動刪除

舊版	提交樣本後，必須手動刪除垃圾郵件 (或假冒詐騙)。
目前版本	可以選擇提交後立即刪除所選的每一封郵件。
好處	提交郵件更為快捷和輕鬆。

使用此指南

此指南提供了有關設定和使用產品的資訊。這些主題包括：

- [簡介](#)
產品概觀，包括新增功能或已變更功能的說明、此指南的概觀以及 McAfee 聯絡資訊。
- [關於垃圾郵件和假冒詐騙](#)
有關垃圾郵件和防假冒詐騙以及如何減少垃圾郵件和防假冒詐騙的資訊。
- [安裝此工具](#)
下載這些檔案。使用 Microsoft Windows 安裝程式。使用指令碼安裝。
- [使用工具](#)
如何提交樣本和設定此工具。

適用對象

此資訊主要適用於以下兩類讀者：

- 負責公司電子郵件安全的網路管理員。
- 負責設定軟體偵測選項的使用者。

慣例

本指南使用以下慣例：

粗體縮排	所有的介面文字，包括選項、功能表、按鈕和對話方塊名稱。 例如： 鍵入相應帳戶的「使用者」名稱和「密碼」。
Courier	資料夾或程式的路徑、表示使用者準確鍵入的內容之文字（例如，系統提示符號後的指令）。 範例： 程式的預設位置是： C:\Program Files\McAfee\EPO\3.5.0 在用戶端電腦上執行此指令： scan --help
斜體	出於強調目的或採用新的術語時；用於產品說明文件的名稱及資料內的主題（標題）。 例如： 請參閱《VirusScan Enterprise Product Guide》，以取得更多資訊。
藍色	網站地址 (URL) 和 / 或有效連結。 例如： 造訪 McAfee 網站： http://www.mcafee.com
< 術語 >	使用角括號括住一般術語。 例如： 在主控台樹狀目錄中，於 <「伺服器」> 上按滑鼠右鍵。
	註： 補充資訊，例如執行同一指令的其他方法。
	提示： 進行最佳操作的建議以及來自 McAfee 阻止威脅、效能和效率的建議。
	注意： 保護您的電腦系統、企業、軟體安裝或資料的重要建議。
	警告： 重要建議，用於保護使用者在使用硬體產品時免受身體損傷。

取得產品資訊

除非另有註明，產品說明文件均為 Adobe Acrobat .PDF 檔案，並可從 McAfee 下載站台下載。

產品指南 — 產品及其功能的介紹；安裝和設定軟體的詳細說明；有關部署、重複工作和作業程序的資訊。

「版本注意事項」 — *讀我檔案*。產品資訊、已解決的問題、所有已知問題、產品或其說明文件的最新增加或變更。包含在軟體應用程式中的文字檔案。

授權合約 — McAfee 授權合約手冊，其中包含您可為產品購買的所有授權類型。授權合約中列出了使用授權產品的一般條款和條件。

聯絡人 — McAfee 服務和資源的聯絡資訊：技術支援、客戶服務、安全總部 (AVERT)、Beta 測試計劃和訓練。包含在軟體應用程式中的文字檔案。

連絡資訊

安全總部：AVERT

首頁

<http://www.mcafeesecurity.com/us/security/home.asp>

病毒資訊庫

<http://vil.mcafeesecurity.com>

AVERT WebImmune，提交樣本（需要登入憑證）

<https://www.webimmune.net/default.asp>

AVERT DAT 通知服務

<http://vil.mcafeesecurity.com/vil/join-DAT-list.asp>

下載網站

首頁

<http://www.mcafeesecurity.com/us/downloads/>

防毒 DAT 檔案和引擎更新

<http://www.mcafeesecurity.com/us/downloads/updates/default.asp>

<ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x>

防垃圾郵件規則和引擎更新

<ftp://ftp.mcafee.com/spamdefs/1.x/>

產品升級（需要登入憑證）

<https://secure.nai.com/us/forms/downloads/upgrades/login.asp>

安全性弱點的 HotFix 和修補程式版本（為公眾提供）

<http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp>

產品的 HotFix 和修補程式版本（需要 ServicePortal 帳戶和 McAfee 技術支援授權碼）

<https://mysupport.nai.com/products/products.asp>

產品生命終結支援

http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

軟體和硬體技術支援

首頁

http://www.mcafeesecurity.com/us/support/technical_support

知識庫搜尋

<http://knowledgemap.nai.com/>

McAfee 技術支援 ServicePortal（需要登入憑證）

<https://mysupport.mcafeesecurity.com>

McAfee 安全警示服務 (MSAS)

http://mysupport.nai.com/supportinfo/psvans_info.asp

客戶服務

電子郵件

https://secure.nai.com/us/forms/support/request_form.asp

網站

<http://www.mcafeesecurity.com/us/support/default.asp>

電話 — 美國、加拿大和拉丁美洲免付費電話：

+1-888-VIRUS NO 或 +1-888-847-8766 星期一至星期五，8 a.m. 8 p.m.，中部時間

如需有關連絡 McAfee 世界各地辦事處的資訊，請造訪：

<http://www.mcafeesecurity.com/us/contact/home.htm>

McAfee Beta 測試計劃

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

訓練：McAfee 大學

<http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm>

2

關於垃圾郵件和假冒詐騙

此工具如何協助減少垃圾郵件和假冒詐騙

本章節說明此工具的功能及如何與 McAfee 安全產品配合使用來減少垃圾郵件。

- [一些有用術語](#)
- [第 12 頁的「哪些是垃圾郵件？」](#)
- [第 12 頁的「避免垃圾郵件」](#)
- [第 13 頁的「哪些是假冒詐騙？」](#)
- [第 13 頁的「避免假冒詐騙」](#)
- [第 14 頁的「何為 Customer Submission Tool？」](#)
- [第 15 頁的「貝氏學習」](#)
- [第 15 頁的「瞭解垃圾郵件分數」](#)

一些有用術語

以下定義可能對您有所幫助：

- **漏報** — 尚未分類但包含通常被視為垃圾郵件或假冒詐騙內容的電子郵件。
- **誤報** — 已分類為垃圾郵件或假冒詐騙，但收件者不將其視為垃圾郵件或假冒詐騙的電子郵件。
- **垃圾郵件製造者** — 建立垃圾郵件的人或組織。
- **假冒** — 例如，偽造電子郵件的來源以隱藏寄件者身份，以及建立貌似真實可信的網站。
- **白名單** — 批准的寄件者之清單。
- **黑名單** — 傳送垃圾郵件或假冒詐騙的寄件者之清單。

哪些是垃圾郵件？

所有來路不明和不受歡迎的電子郵件都可以被視為垃圾郵件。垃圾郵件（亦稱為來路不明的大量電子郵件或 UBE）包括商業電子郵件、電子版的**推銷郵件**以及無用的非商業電子郵件（例如，病毒惡作劇、玩笑和連鎖信）。

通常，建立垃圾郵件的人（稱為**垃圾郵件製造者**）會偽造電子郵件標題以隱藏其真實身份，經常將報復轉向無辜者。

哪些不是垃圾郵件？

有些電子郵件被稱為垃圾郵件，但它們並不是。例如，如果您曾經訂閱過新聞快訊或線上論壇、索取過有關某些產品的資訊，或最近離開了工作群組，您的電子郵件地址可能仍在分發清單上。若要減少此類無用電子郵件，請立即從過時的分發清單上移除您的電子郵件地址。

避免垃圾郵件

每次您使用電子郵件地址回應和傳送郵件、張貼至網際網路聊天室或公佈電子郵件地址時，都會將電子郵件帳戶暴露給**垃圾郵件製造者**。垃圾郵件製造者會編譯電子郵件地址清單。隨時間推移，您的地址被新增至垃圾郵件製造者社群內越來越多的清單中，從而極大地增加您接收到的垃圾郵件數目。

請按照您的組織建議的有關電子郵件使用的指示，進行良好的郵件傳送。這可協助您減少接收到的垃圾郵件數目。例如：

- **謹防購買垃圾郵件中公佈的產品。**這會提醒垃圾郵件製造者，該電子郵件地址處於作用中，因此可以出賣給其他垃圾郵件製造者。您也會因此暴露個人資訊。
- **請勿在線上張貼個人電子郵件地址**，而改為在參與新聞群組、參加競賽或協力廠商索要您的電子郵件地址時，使用**可任意丟棄**的電子郵件地址。如果該地址接收到過多的垃圾郵件，您可以停止使用該地址並取得新的地址。
- **請勿回覆垃圾郵件，即使其表示要將您從分發清單中移除。**您的回覆會向垃圾郵件製造者確認電子郵件地址處於作用中，該地址可以被出賣給其他垃圾郵件製造者。

另請參閱第 15 頁的「[瞭解垃圾郵件分數](#)」以瞭解 McAfee 防垃圾郵件產品的設定如何周到地協助您減少垃圾郵件。

哪些是假冒詐騙？

某些垃圾郵件製造者專門假冒電子郵件以哄騙不謹慎的電子郵件使用者暴露有關其身份和財務帳戶的資訊。此種專門的垃圾郵件形式稱為假冒詐騙。

通常，您會接收到看起來是來自權威組織（例如銀行）的電子郵件。電子郵件通常會將您導向至假冒的網站，該網站會要求您提供個人和財務詳細資訊，例如帳號、密碼、信用卡詳細資訊和社會安全號碼。罪犯會使用竊得的身份騙取商品和服務（例如個人貸款），從而直接從您的帳戶竊取、開立銀行帳戶以及洗錢。

避免假冒詐騙

- **謹防要求您提供密碼和其他敏感資訊的電子郵件。**銀行不會直接要求此類資訊，並且通常會透過郵局確認資訊。任何組織都不可能遺失您的帳戶資訊。其一般程序是透過郵局向您發佈新的詳細資訊，而不是要求您自己透過電子郵件或網站提供詳細資訊。
- **謹防網站連結。**您被要求提供敏感資訊時，可能已被假冒的連結欺騙。例如，電子郵件中的連結類似於銀行的網站 (www.example.com)，並將您連接至看起來真實的網站。然而，瀏覽器中的地址會顯示不同的名稱（例如 www.example.net）或 IP 位址（例如 168.192.255.200）。
- **謹防不安全的網站。**合法的組織會運作安全網站，可以在您傳送個人資訊之前加密您的資訊。其網站地址類似於 https://www.example.com，而不是 http://www.example.com。換言之，使用安全的網際網路協定 **https**，而不是 **http**。

何為 Customer Submission Tool ?

防垃圾郵件產品可提供針對垃圾郵件的良好防護。但有時很難偵測到垃圾郵件，垃圾郵件製造者開發新的技術，並且某些較新的垃圾郵件是任何防垃圾郵件產品絕對無法偵測到的。此外，可能會發生錯誤的偵測，並且防垃圾郵件產品可能會將某些真正的郵件錯誤地分類為垃圾郵件。

透過分析新的垃圾郵件（和假冒詐騙）以及任何被錯誤分類的電子郵件，McAfee 可以不斷改進其防垃圾郵件產品。

Customer Submission Tool 與 Microsoft Outlook 電子郵件軟體配合工作，可協助您減少接收到的無用電子郵件（或垃圾郵件）數目。在您閱讀電子郵件時，會有新的按鈕和功能表項目可供使用。

圖 2-1 Microsoft Outlook 中新的按鈕和功能表



此工具可以將電子郵件轉發至 McAfee Lab 或其他 McAfee 防垃圾郵件產品進行分析：

- **將電子郵件傳送至 McAfee Lab**

我們致力於不斷改進防垃圾郵件產品的偵測，檢查我們的軟體或其他供應商的產品錯誤分類的郵件，並瞭解其原因，並相應地改進防垃圾郵件產品。



我們將所有提交的樣本視為機密材料，並且不會為了研究之外的任何目的而轉發或使用它們。為正確分析樣本，我們會查看郵件標題，包括寄件者和主旨以及內文內容（包括文字和附件）。安裝此工具時，會提供完整的隱私權說明。

- **將電子郵件傳送至 Secure Content Management (SCM) 設備**

如果網路受 SCM 設備保護，則您可以將樣本提交至設備進行貝氏學習。請參閱第 15 頁。

- **將電子郵件傳送至 McAfee Quarantine Manager (MQM)**

如果網路包括 MQM 軟體，您可以將樣本提交至 McAfee Quarantine Manager 進行貝氏學習。請參閱第 15 頁。

貝氏學習

Secure Content Management (SCM) 設備和 McAfee Quarantine Manager (MQM) 使用基於貝氏概率理論的資料庫確定電子郵件是否包含垃圾郵件（或假冒詐騙）。

您可以將電子郵件樣本傳送至 SCM 或 MQM 管理員，來協助訓練資料庫識別新的垃圾郵件和假冒詐騙。單一 McAfee Quarantine Manager 可以處理多個 SCM 設備的訓練。

Customer Submission Tool 可讓您僅按一下即傳送樣本。管理員可以決定要提交至資料庫的樣本。軟體會分析每個樣本的內容並學習垃圾郵件樣式的片語，以便將來參考。

同樣，如果您收到已被錯誤分類為垃圾郵件或假冒詐騙的電子郵件，則可以將這些電子郵件傳送至管理員進行非垃圾郵件學習。

正確提交並用於訓練的樣本越多，將來正確分類垃圾郵件和假冒詐騙的機率就越大。

瞭解垃圾郵件分數

我們的防垃圾郵件產品符合大量針對每封電子郵件的規則。每個規則都與一個分數（正數或負數）相關聯。符合垃圾郵件樣式特性的規則為正分數。符合合法郵件屬性的規則為負分數。加在一起的分數是每封郵件的總計垃圾郵件分數。有些規則是相似的，且僅在普通片語上相符。其他規則更為複雜，且在電子郵件的標題資訊和架構上相符。

防垃圾郵件產品可以指定在何種層級將郵件視為垃圾郵件。通常，5 分表示郵件為垃圾郵件。防垃圾郵件產品可以透過將某些文字（例如 **SPAM**）新增至郵件的主旨行來重點標示該郵件。從而您可以輕鬆識別垃圾電子郵件，並決定如何處理該郵件。

正確設定防垃圾郵件產品至關重要，以便在垃圾郵件分數超過特定層級時分類垃圾郵件。如果層級過高（垃圾郵件分數為 10 或更高），防垃圾郵件產品將不會分類某些郵件。如果層級過低，某些真正的電子郵件將被錯誤分類為垃圾郵件。

3

安裝此工具 適用於高級使用者和管理員

本章節說明如何安裝 Customer Submission Tool 軟體 2.0 版本並提供了以下資訊：

- 安裝檢核清單
- 下載安裝檔案
- 手動安裝此工具
- 使用指令碼安裝此工具

如果您要向多個電子郵件使用者提供此工具，我們建議您使用指令碼。請參閱第 19 頁的「[使用指令碼安裝此工具](#)」。

安裝檢核清單

我們將 Customer Submission Tool 作為可從網站下載的檔案分發。安裝 Customer Submission Tool 之前，請閱讀以下檢核清單以確保系統正確設定，可以執行安裝程式，並確保您擁有安裝該程式所需的所有資訊。

- ✓ 電腦具有 Microsoft Windows 2000 (或更高版本) 作業系統。
- ✓ 您已安裝了 Windows 作業系統最新的 Service Pack 和 Windows 更新。
- ✓ 電腦具有 Microsoft Outlook 2000 (或更高版本) 用戶端。Customer Submission Tool 不與 Microsoft Outlook Express 或其他電子郵件用戶端配合使用。
- ✓ 電腦具有從 McAfee 網站下載的安裝檔案之存取權。
- ✓ 您具有安裝 Customer Submission Tool 所需的管理權限和許可。
- ✓ 若要將電子郵件提交至 McAfee Quarantine Manager (MQM)，需提供此資訊：
 - MQM 伺服器的名稱或 IP 位址，例如 server1.domain1 或 192.168.255.200。您可以使用 HTTP 或 HTTPS，或者通訊協定。

依據您的認證程序，可能還需要：

- 使用者名稱以直接存取 MQM，例如 network_user@example.com。
- 密碼以直接存取 MQM。
- ✓ 如果 MQM 軟體不可用，則您可以將電子郵件提交至 Secure Content Management (SCM) 設備。此時需要提供以下資訊：
 - SMTP 伺服器的名稱或 IP 位址，例如，server1.domain1 或 192.168.255.200。

由於 SCM 設備不可從工作站直接存取，因此此位址通常指將電子郵件轉發至 SCM 設備的 SMTP 轉接，可以是 Microsoft Exchange 伺服器。

 - SMTP 伺服器連接埠數目。
 - 用於提交遺失的垃圾郵件或假冒詐騙之電子郵件 位址。
 - 用於提交錯誤分類為垃圾郵件或假冒詐騙的電子郵件地址。

下載安裝檔案

- 1 在硬碟上建立一個暫存資料夾。
- 2 連接至 McAfee 網站上防垃圾郵件產品區段：
<http://www.mcafeesecurity.com/us/products/mcafee/antispam/category.htm>。
- 3 找到「Spam Submission Tool」區段並擷取封存資料夾至暫存資料夾。您可以從很多電子服務中獲取必要的公用程式來擷取 .ZIP 封存檔。

手動安裝此工具



若要向多個電子郵件使用者提供此工具，我們建議您使用指令碼。請參閱第 19 頁。

- 1 關閉所有正在執行的應用程式。
- 2 在下載了工具的暫存資料夾中，連按兩下「McAfee Customer Submission Tool」資料夾。
- 3 找到並執行 MCST.EXE 檔案以開啟安裝精靈。

如果安裝程式未自動選取適當的語言，將開啟一個對話方塊讓您選取語言。

圖 3-1 「安裝精靈」對話方塊



- 4 按一下「下一步」開啟「目標資料夾」頁面。
- 5 按一下「瀏覽」指定其他目標資料夾，或保留預設，然後按一下「下一步」。
- 6 在「準備安裝應用程式」頁面，按一下「下一步」開啟「更新系統」頁面。
該頁面會顯示進度訊息與進度列。複製檔案並安裝軟體。此作業會花費幾分鐘時間。安裝完成後，將顯示「已成功安裝 McAfee Customer Submission Tool」頁面。
- 7 按一下「完成」關閉精靈。
- 8 啟動 Microsoft Outlook。新的按鈕位於 Microsoft Outlook 標準工具列。請參閱第 14 頁的圖 2-1。

使用指令碼安裝此工具

如果您要在多台電腦上安裝 Customer Submission Tool，我們建議您使用指令碼。若要下載您需要的檔案，請參閱第 18 頁的「[下載安裝檔案](#)」。

安裝指令的一般形式為：

```
msiexec /qn /I mcst.msi parameter1 parameter2 parameter3
```

如需有關 Windows 安裝程式的更多資訊，請造訪 [Microsoft 網站](#)。

可以在手動設定工具（如第 27 頁的「[設定此工具](#)」所述）時進行設定的所有功能均可指定為此指令的參數。

以下表格說明這些參數。

表 3-1 一般參數

參數與預設值	說明
CONFIGENABLED 1 (是)	允許使用者透過使「設定提交設定」按鈕可見來設定工具。 0= 否，1= 是。任何其他值均視為 1。
DELETESPAMONSUBMIT 0 (否)	提交後刪除所有垃圾郵件（或假冒詐騙）。 0= 否，1= 是。任何其他值均視為 0。
DONTSHOWSPAMSUBMIT 0 (否)	當使用者按一下用於提交垃圾郵件或假冒詐騙的按鈕時不顯示提交對話方塊。 0= 否，1= 是。任何其他值均視為 0。
DONTSHOWHAMSUBMIT 0 (否)	當使用者按一下用於提交錯誤分類的電子郵件的按鈕時不顯示提交對話方塊。 0= 否，1= 是。任何其他值均視為 0。
INSTALLDIR1 請參閱文字。	在此位置安裝工具。依預設，工具安裝在： 「C:\Program Files\McAfee\Submission Tool」
MAXSUBMISSIONCOUNT 10000	允許使用者一次提交至多 40 億封郵件。任何超出此範圍的值均視為 10000。
REBOOT (無)	安裝完成後重新啟動作業系統。 可能的設定為 F= 強制、S= 抑制或 R= 實際抑制。我們建議使用 S 或 R。

表 3-2 提交至 McAfee Lab 的參數

參數與預設值	說明
ASEENABLED 1 (是)	啟用向 McAfee Lab 提交樣本。
ASERESPONSEFREQ 0 (立即)	McAfee Lab 回應提交的頻率。可能的設定為 0= 「立即」、1= 「每天」或 2= 「每週」或 3= 「從不」。任何其他值均視為 0。
ASERESPONSETYPE 0 (簡短)	McAfee Lab 傳送的確認類型。可能的設定為 0= 「簡短」、1= 「一般」或 2= 「詳細」。任何其他值均視為 0。

表 3-3 向 McAfee Quarantine Manager (MQM) 提交的參數

參數與預設值	說明
MQMENABLED 0 (否)	啟用向 MQM 提交樣本。 0= 否，1= 是。任何其他值均視為 0。
MQMPATH 「http://mqm.example.com/mqmuserui」	至 MQM 上使用者資料夾的 URL。
WHITELISTHAMONSUBMIT 0 (否)	自動將寄件者位址新增至白名單，在其中提交的電子郵件不是垃圾郵件或假冒詐騙。 0= 否，1= 是。任何其他值均視為 0。
BLACKLISTSPAMONSUBMIT 0 (否)	自動將寄件者位址新增至黑名單，在其中提交的電子郵件是垃圾郵件或假冒詐騙。 0= 否，1= 是。任何其他值均視為 0。

表 3-4 向 Secure Content Management (SCM) 提交的參數

參數與預設值	說明
SCMENABLED 0 (否)	啟用向 SCM 設備提交樣本。 0= 否，1= 是。任何其他值均視為 0。
SCMRELAYSERVER 「mail.example.com」	SMTP 伺服器的名稱或 IP 位址，例如，server1.domain1 或 192.168.255.200。
SCMRELAYPORT 25	SMTP 伺服器連接埠數目。 範圍為 1-65535。
SCMSPAMADRESS 「sample_spam@example.com」	用於提交遺失的垃圾郵件或假冒詐騙之電子郵件位址。
SCMHAMADRESS 「sample_nonspam@example.com」	用於提交錯誤分類為垃圾郵件或假冒詐騙的電子郵件地址。

範例



使用雙引號括住字元字串。例如：

```
INSTALLDIR="C:\FOLDER A\FOLDER 1"
```

以下指令使用預設值無訊息安裝 Customer Submission Tool。使用者僅可在 Microsoft Outlook 工具列上看到「提交垃圾郵件或假冒詐騙樣本」和「提交非垃圾郵件樣本」按鈕。安裝完成時不會重新啟動。使用者僅可向 McAfee Lab 提交樣本。使用者無法重設工具。

```
msiexec /qn /i mcst.msi CONFIGENABLED=0 INSTALLDIR="C:\FOLDER A\FOLDER 1" REBOOT=R
```

以下指令可無訊息安裝 Customer Submission Tool 並讓使用者向 McAfee Quarantine Manager 提交樣本。使用者可重設工具。

```
msiexec /qn /I mcst.msi MQMENABLED=1 MQMPATH="http://mqml/userui" REBOOT=R
```

以下指令可安裝 Customer Submission Tool 並讓使用者向 Secure Content Management 設備提交樣本。使用者將在安裝執行時看到安裝過程。使用者可重設工具。

```
msiexec /i mcst.msi SCMENABLED=1 SCMRELAYSERVER="http://server1" SCMRELAYPORT=1234
```

向電子郵件使用者宣告工具

在電子郵件使用者的 Microsoft Outlook 用戶端上安裝了 Customer Submission Tool 後，您可以向其發布宣告。

範例

今天，我們部署了 McAfee 垃圾郵件提交工具。

此工具將協助我們減少組織接收到的垃圾郵件總數。Microsoft Outlook 工具列中將出現兩個新的按鈕。如果您無法看到這兩個按鈕（如下顯示），請重新啟動 Microsoft Outlook。

按一下此按鈕以提交未偵測為垃圾郵件的垃圾郵件樣本：



按一下此按鈕以提交錯誤分類為垃圾郵件的郵件樣本：



變更設定

稍後若要在不重新安裝工具的情況下變更設定的任意部分，您可在以下機碼處變更登錄設定：

HKEY_CURRENT_USER\Software\McAfee\Submission Tool

設定列示於以下表格中：

表 3-5 預設登錄值

名稱	預設值 (十六進位)
AseEnabled	00000001
AseResponseFreq	00000000
AseResponseType	00000000
BlacklistSpamOnSubmit	00000000
ConfigEnabled	00000001
DeleteSpamOnSubmit	00000000
DontShowHamSubmit	00000000
DontShowSpamSubmit	00000000
MaxSubmissionCount	00002710
MqmEnabled	00000000
MqmPath	"http://mqm.example.com/mqmuserui"
ScmDataTimeout	0000ea60
ScmEnabled	00000000
ScmHamAddress	"sample_nonspam@example.com"
ScmRecvTimeout	0000ea60
ScmRelayPort	00000019
ScmRelayServer	"mail.example.com"
ScmSendTimeout	0000ea60
ScmSpamAddress	"sample_spam@example.com"
WhitelistHamOnSubmit	00000000

登錄中的名稱與第 19 頁的「使用指令碼安裝此工具」中的參數名稱相同。

某些名稱 (例如 SCM 逾時) 不可作為參數使用，且僅可從登錄中設定。SCM 逾時預設值為 60000 毫秒 (1 分鐘)。

若要強制使用變更的登錄設定，請重新啟動 Microsoft Outlook。如果您輸入錯誤的值，此工具將使用預設值取代該值。

4

使用工具 按鈕和功能表項目

Customer Submission Tool 會在安裝後新增某些工具列按鈕和功能表項目 (請參閱第 14 頁的圖 2-1) 至 Microsoft Outlook 用戶端。這些按鈕和功能表項目可讓您：

- 提交本應分類為垃圾郵件或假冒詐騙的郵件。
請參閱[提交第一個垃圾郵件或假冒詐騙樣本](#)和[第 24 頁的「提交更多垃圾郵件或假冒詐騙樣本」](#)。
- 提交錯誤分類為垃圾郵件或假冒詐騙的郵件。
請參閱[第 25 頁的「提交第一個被錯誤分類的樣本」](#)和[第 26 頁的「提交更多被錯誤分類的樣本」](#)。
- 新增所有 Microsoft Outlook 連絡人至白名單 (如果使用 McAfee Quarantine Manager)。請參閱[第 26 頁的「新增 Microsoft Outlook 連絡人至白名單」](#)。
- 設定某些工具設定。請參閱[第 27 頁的「設定此工具」](#)。

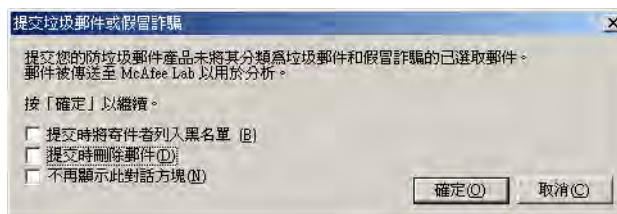
提交第一個垃圾郵件或假冒詐騙樣本

第一次提交電子郵件樣本時，可以按照您自己的喜好設定工具。若要提交垃圾郵件或假冒詐騙樣本，請：



- 1 在 Microsoft Outlook 中，檢視郵件或選取郵件主旨行。
- 2 按工具列上的「提交垃圾郵件或假冒詐騙樣本」按鈕。還可以使用「動作」功能表。將開啟一個對話方塊：

圖 4-1 「提交」對話方塊



3 在此對話方塊中，選取您需要的功能：

功能	說明
提交時將寄件者列入黑名單	此核取方塊僅在使用 McAfee Quarantine Manager 軟體時可用。 將垃圾郵件寄件者新增至黑名單。以後，將封鎖所有來自此寄件者的電子郵件。
提交時刪除郵件	在提交每一封選取的垃圾郵件或假冒詐騙樣本後將其刪除。
不再顯示此對話方塊	阻止此對話方塊再次顯示。以後，您可以在按住 SHIFT 鍵的同時按「提交垃圾郵件或假冒詐騙樣本」按鈕來再次顯示此對話方塊。

按「確定」關閉此對話方塊。樣本已提交。

4 如果要將樣本提交至 McAfee Quarantine Manager，系統會提示您輸入登入名稱和密碼。

5 看到說明樣本已成功提交的訊息方塊後，按「確定」。

此工具不會提交過大的樣本（超過 1 MB），因此 McAfee 建議您刪除此類檔案。

提交更多垃圾郵件或假冒詐騙樣本

若要提交垃圾郵件或假冒詐騙樣本，請：

1 在 Microsoft Outlook 中，檢視郵件或選取郵件主旨行。



檢視電子郵件主旨行時，可以一次提交多個樣本。若要選取一批數封電子郵件來單一提交，請使用 SHIFT 鍵。若要選取數封獨立的郵件，請使用 CTRL 鍵。



2 按工具列上的「提交垃圾郵件或假冒詐騙樣本」按鈕。還可以使用「動作」功能表。

如果顯示了對話方塊，請選取您需要的功能：請參閱第 23 頁的「[提交第一個垃圾郵件或假冒詐騙樣本](#)」。如果未看到此對話方塊，可以在按住 SHIFT 鍵的同時按滑鼠左鍵來顯示它。按「確定」關閉此對話方塊。

樣本已提交。

3 看到說明樣本已成功提交的訊息方塊後，按「確定」。

此工具不會提交過大的樣本（超過 1 MB），因此 McAfee 建議您刪除此類檔案。

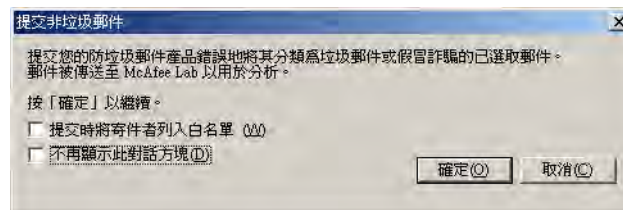
提交第一個被錯誤分類的樣本

第一次提交樣本時，可以按照您自己的喜好設定工具。若要提交被錯誤分類為垃圾郵件或假冒詐騙的樣本，請：



- 1 在 Microsoft Outlook 中，檢視郵件或選取郵件主旨行。
- 2 按工具列上的「提交非垃圾郵件樣本」按鈕。還可以使用「動作」功能表。將開啟一個對話方塊：

圖 4-2 「提交」對話方塊



- 3 在此對話方塊中，選取您需要的功能：

功能	說明
提交時將寄件者列入白名單	此核取方塊僅在使用 McAfee Quarantine Manager 時可用。以後，不會將所有來自此寄件者的電子郵件分類為垃圾郵件。
不再顯示此對話方塊	若要以後檢視此對話方塊，您可以在按住 SHIFT 鍵的同時按「提交非垃圾郵件樣本」按鈕。

- 4 按「確定」關閉此對話方塊。樣本已提交。
- 5 如果要將樣本提交至 McAfee Quarantine Manager，系統會提示您輸入登入名稱和密碼。
- 6 看到說明樣本已成功提交的訊息方塊後，按「確定」。

此工具不會提交過大的樣本（超過 1 MB），因此 McAfee 建議您刪除此類檔案。

提交更多被錯誤分類的樣本

若要提交被錯誤分類為垃圾郵件或假冒詐騙的樣本，請：

- 1 在 Microsoft Outlook 中，檢視郵件或選取郵件主旨行。



檢視電子郵件主旨行時，可以一次提交多個樣本。若要選取一批數封電子郵件來單一提交，請使用 SHIFT 鍵。若要選取數封獨立的郵件，請使用 CTRL 鍵。



- 2 按工具列上的「提交非垃圾郵件樣本」按鈕。還可以使用「動作」功能表。

如果顯示了對話方塊，請選取所需功能（如第 25 頁的「提交第一個被錯誤分類的樣本」中所述），然後按「確定」關閉對話方塊。如果未看到此對話方塊，可以在按住 SHIFT 鍵的同時按滑鼠左鍵來顯示它。按「確定」關閉此對話方塊。

樣本已提交。

- 3 看到說明樣本已成功提交的訊息方塊後，按「確定」。

此工具不會提交過大的樣本（超過 1 MB），因此 McAfee 建議您刪除此類檔案。

新增 Microsoft Outlook 連絡人至白名單



此功能僅在安裝了 McAfee Quarantine Manager，且將 Customer Submission Tool 設定為顯示工具列上的「設定提交設定」按鈕時可用。

若要阻止將來自 Microsoft Outlook 連絡人的電子郵件被分類為垃圾郵件（或假冒詐騙），您可以將連絡人新增至白名單：



- 1 在 Microsoft Outlook 中，按工具列上的「設定提交設定」按鈕。
- 2 在「Customer Submission Tool」對話方塊中，按「新增連絡人地址至白名單」。
- 3 按「確定」關閉此對話方塊。

以後，將不會對從白名單中的電子郵件地址傳送給您的郵件進行垃圾郵件或假冒詐騙掃描。（但會對所有電子郵件進行病毒掃描。）

設定此工具

如果工具列上的「設定提交設定」按鈕可用，您可以設定 Customer Submission Tool 的某些功能。此按鈕僅在檢視電子郵件主旨行時可用。



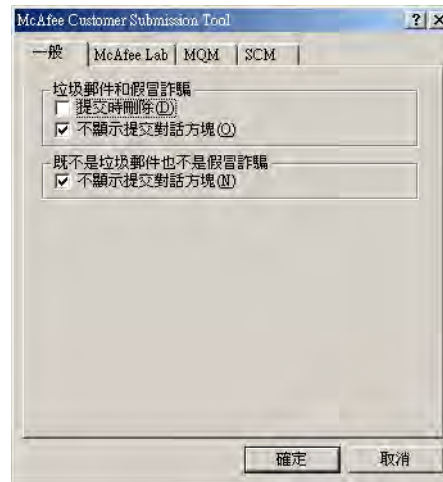
如果透過未啟用此工具的指令檔安裝了此工具，則此按鈕不可用。

若要設定此工具，請：



- 1 按工具列上的「設定提交設定」按鈕來開啟對話方塊：

圖 4-3 「設定」對話方塊



- 2 在此對話方塊中，選取您需要的功能：

標籤	功能說明
提交時刪除	在成功提交每一封垃圾郵件或假冒詐騙郵件後將其刪除。
不顯示提交對話方塊	阻止在提交垃圾郵件或假冒詐騙（或被錯誤分類的電子郵件）後顯示對話方塊。

- 3 如果要將樣本提交至 McAfee Lab 進行分析，請選取「McAfee Lab」標籤，然後選取「啟用」，再選取其他任意值：

標籤	功能說明
回應頻率	指定 McAfee Lab 必須傳送自動電子郵件以確認您的提交的頻率。 如果選取了「立即」並同時傳送了多個樣本，則可能會在稍後的幾分鐘內接收到數個回覆。
回應類型	指定每封自動電子郵件中的詳細資訊。例如，「簡短」僅提供確認。

第一次使用此工具時，McAfee 建議您選取「立即」和「簡短」。

- 4 如果要將樣本提交至 McAfee Quarantine Manager，請選取「MQM」標籤，然後選取「啟用」，再選取一些功能：

標籤	功能說明
URL	MQM 伺服器的地址，例如以下其中一種： <ul style="list-style-type: none"> ■ http://www.example.com ■ 192.168.255.200
使用者名稱	與 MQM 進行直接通訊時使用的使用者名稱（例如 user@example.com）。
密碼	與使用者名稱相關聯的密碼。
提交後將寄件者地址新增至黑名單	以後，將封鎖所有來自此寄件者的電子郵件。
提交後將寄件者地址新增至白名單	以後，不會對所有來自此寄件者的電子郵件進行垃圾郵件或假冒詐騙掃描。但始終會對電子郵件進行病毒掃描。

- 5 如果要將電子郵件提交至 Secure Content Management 設備，請選取「SCM」標籤，然後選取「啟用」，再選取一些功能：

標籤	功能說明
伺服器	伺服器名稱，例如以下其中一種： <ul style="list-style-type: none"> ■ server1 ■ 192.168.255.200 ■ mailto:192.168.255.200 ■ http://example.com/user ■ http://example.com/user:8080/user1/folder1
連接埠	連接埠號碼，例如 25。
垃圾郵件和假冒詐騙	地址（按照設備上的設定），例如 spam@example.com。
既非垃圾郵件亦非假冒詐騙	地址（按照設備上的設定），例如 not-spam@example.com。

- 6 按「確定」關閉此對話方塊。新的設定會立即生效。