

Customer Submission Tool

2.0 版

McAfee®
系统保护

业界领先的入侵防护解决方案

McAfee®

版权

Copyright © 2005 McAfee, Inc.。保留所有权利。

未经 McAfee, Inc. 或其供应商或子公司的书面许可，不得以任何形式或手段将本出版物的任何部分复制、传播、转录、存储于检索系统或翻译成任何语言。

商标归属

ACTIVE FIREWALL、ACTIVE SECURITY、ACTIVESECURITY（及片假名）、ACTIVESHIELD、CLEAN-UP、DESIGN（特殊样式的 E）、DESIGN（特殊样式的 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 和 WEBSHIELD（及片假名）是 McAfee, Inc. 和 / 或其子公司在美国和 / 或其他国家或地区的注册商标或商标。与安全有关的红色是 McAfee 品牌产品的特色。本文档中提及的所有其他注册和未注册商标均为其各自所有者专有。

许可信息

许可协议

所有用户请注意：请仔细阅读与您所购买的许可相关的适当法律协议，其中规定了使用许可软件的一般条款和条件。如果不清楚您购买的许可属于哪一类，请查看软件包装盒附带的销售文档以及许可授权或订单相关的其他文档，或者查看您购买时另行得到的销售文档以及许可授权或订单相关的其他文档，这些文档既可以是手册、产品 CD 上的文件，也可以是从软件包下载网站上获得的文件。如果您不同意此协议规定的所有条款和条件，请勿安装本软件。如果适用，您可以将产品退回 McAfee 或原购买处以获得全额退款。

归属声明

本产品包括或可能包括：

- 由 OpenSSL Project (<http://www.openssl.org/>) 开发以在 OpenSSL Toolkit 中使用的软件。
- 由 Eric A. Young 编写的加密软件 and 由 Tim J. Hudson 编写的软件。
- 一些根据 GNU 通用公共许可（General Public License，即 GPL）或其他类似免费软件许可（除其他权利外，这些许可还允许用户复制、修改和重新分发某些程序或程序的某些部分以及访问源代码）授权（或再授权）用户使用的软件程序。GPL 要求，对于 GPL 涵盖的任何软件，在分发时除可执行的二进制文件外，还必须向用户提供源代码。对于 GPL 下包含的任何这类软件，此 CD 将提供相应源代码。如果任何免费软件许可要求 McAfee 提供比本协议所授予的使用、复制或修改软件程序更广泛的权利，则这些权利优先于此处提及的权利和限制。
- 由 Henry Spencer 原创的软件，Copyright 1992, 1993, 1994, 1997 Henry Spencer。
- 由 Robert Nordier 原创的软件，Copyright © 1996-7 Robert Nordier。
- 由 Douglas W. Sauder 编写的软件。
- 由 Apache Software Foundation (<http://www.apache.org/>) 开发的软件。您可以从 www.apache.org/licenses/LICENSE-2.0.txt 中找到此软件的许可协议。
- International Components for Unicode (ICU) Copyright ©1995-2002 International Business Machines Corporation 及其他公司。
- 由 CrystalClear Software, Inc. 开发的软件，Copyright © 2000 CrystalClear Software, Inc.。
- FEAD® Optimizer® 技术，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 版权所有的软件，© 1998, 1999, 2000。
- Expat maintainers 版权所有的软件。
- The Regents of the University of California 版权所有的软件，© 1996, 1989, 1998-2000。
- Gunnar Ritter 版权所有的软件。
- Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版权所有的软件，© 2003。
- Gisle Aas 版权所有的软件，© 1995-2003。
- Michael A. Chase 版权所有的软件，© 1999-2000。
- Neil Winton 版权所有的软件，© 1995-1996。
- RSA Data Security, Inc. 版权所有的软件，© 1990-1992。
- Sean M. Burke 版权所有的软件，© 1999, 2000。
- Martijn Koster 版权所有的软件，© 1995。
- Brad Appleton 版权所有的软件，© 1996-1999。
- Michael G. Schwern 版权所有的软件，© 2001。
- Graham Barr 版权所有的软件，© 1998。
- Larry Wall 和 Clark Cooper 版权所有的软件，© 1998-2000。
- Frodo Loosjgaard 版权所有的软件，© 1997。
- Python Software Foundation 版权所有的软件，Copyright © 2001, 2002, 2003。您可以从 www.python.org 中找到此软件的许可协议。
- Beman Dawes 版权所有的软件，© 1994-1999, 2002。
- Andrew Lumsdaine, Lie-Quan Lee 和 Jeremy G. Siek 编写的软件，© 1997-2000 University of Notre Dame。
- Simone Bordet 和 Marco Craverio 版权所有的软件，© 2002。
- Stephen Purcell 版权所有的软件，© 2001。
- 由 Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>) 开发的软件。
- International Business Machines Corporation 及其他公司版权所有的软件，© 1995-2003。
- 由 University of California, Berkeley 及其合作伙伴开发的软件。
- 由 Ralf S. Engelschall <rse@engelschall.com> 开发以在 mod_ssl project (<http://www.modssl.org/>) 中使用的软件。
- Kevlin Henney 版权所有的软件，© 2000-2002。
- Peter Dimov and Multi Media Ltd. 版权所有的软件，© 2001, 2002。
- David Abrahams 版权所有的软件，© 2001, 2002。请参阅 <http://www.boost.org/libs/bind/bind.html> 上的文档。
- Steve Cleary, Beman Dawes, Howard Hinnant 和 John Maddock 版权所有的软件，© 2000。
- Boost.org 版权所有的软件，© 1999-2002。
- Nicolai M. Josuttis 版权所有的软件，© 1999。
- Jeremy Siek 版权所有的软件，© 1999-2001。
- Daryle Walker 版权所有的软件，© 2001。
- Chuck Allison 和 Jeremy Siek 版权所有的软件，© 2001, 2002。
- Samuel Krempp 版权所有的软件，© 2001。请参阅 <http://www.boost.org> 上的更新、文档和修订历史记录。
- Doug Gregor (gregod@cs.rpi.edu) 版权所有的软件，© 2001, 2002。
- Cadenza New Zealand Ltd. 版权所有的软件，© 2000。
- Jens Maurer 版权所有的软件，© 2000, 2001。
- Jaakko Järvi (jaakko.jarvi@cs.utu.fi) 版权所有的软件，© 1999, 2000。
- Ronald Garcia 版权所有的软件，© 2002。
- David Abrahams, Jeremy Siek 和 Daryle Walker 版权所有的软件，© 1999-2001。
- Stephen Cleary (shammah@voyager.net) 版权所有的软件，© 2000。
- Housemarque Oy <<http://www.housemarque.com>> 版权所有的软件，© 2001。
- Paul Moore 版权所有的软件，© 1999。
- Dr. John Maddock 版权所有的软件，© 1998-2002。
- Greg Colvin 和 Beman Dawes 版权所有的软件，© 1998, 1999。
- Peter Dimov 版权所有的软件，© 2001, 2002。
- Jeremy Siek 和 John R. Bandela 版权所有的软件，© 2001。
- Joerg Walter 和 Mathias Koch 版权所有的软件，© 2000-2002。
- Carnegie Mellon University 版权所有的软件，© 1989, 1991, 1992。
- Cambridge Broadband Ltd. 版权所有的软件，© 2001-2003。
- Sparta, Inc. 版权所有的软件，© 2003-2004。
- Cisco, Inc. 和 Information Network Center of Beijing University of Posts and Telecommunications 版权所有的软件，© 2004。
- Simon Josefsson 版权所有的软件，© 2003。
- Thomas Jacob 版权所有的软件，© 2003-2004。
- Advanced Software Engineering Limited 版权所有的软件，© 2004。
- Todd C. Miller 版权所有的软件，© 1998。
- The Regents of the University of California 版权所有的软件，© 1990, 1993，其代码源自 Chris Torek 为 Berkeley 开发的软件。

目录

1	简介	4
	产品功能	4
	此版本中所包含的新功能	5
	改善了对工具的访问	5
	可将电子邮件提交到更多目标	5
	自动使用黑名单和白名单	6
	提交的数量没有限制	6
	提交时自动删除	6
	使用本指南	7
	读者	7
	约定	8
	获取产品信息	9
	联系信息	10
2	关于垃圾邮件和网页仿冒	11
	一些有用术语	11
	什么是垃圾邮件？	12
	避免垃圾邮件	12
	什么是网页仿冒？	13
	避免网页仿冒	13
	什么是 Customer Submission Tool？	14
	Bayesian 学习	15
	了解垃圾邮件记分	15
3	安装此工具	16
	安装检查表	17
	下载安装文件	18
	手动安装此工具	18
	使用脚本安装此工具	19
	示例	21
	向电子邮件用户公布此工具	21
	更改配置	22
4	使用工具	23
	提交第一个垃圾邮件或网页仿冒样本	23
	提交更多垃圾邮件或网页仿冒样本	24
	提交第一个被错误分类的样本	25
	提交更多被错误分类的样本	26
	将 Microsoft Outlook 联系人添加到白名单	26
	配置工具	27

1

简介

McAfee Customer Submission Tool 与 Microsoft® Outlook® 电子邮件软件一起使用可以帮助您减少收到有害电子邮件（或垃圾邮件）的数量。此工具会将电子邮件直接转发到 McAfee 实验室或其他 McAfee 产品，从而可以分析样本，并用于进一步减少垃圾邮件。

本部分包括以下主题：

- 产品功能
- 此版本中所包含的新功能
- 使用本指南

产品功能

McAfee Customer Submission Tool 可以与以下产品一起使用：

- Secure Content Management appliance
- McAfee Quarantine Manager 软件

本工具将在 Microsoft Outlook 客户端中添加工具栏按钮和菜单条目，并使您可以执行以下操作：

- 将样本提交到 McAfee 实验室以进行进一步分析。
- 将样本提交到 McAfee Quarantine Manager 或 Secure Content Management appliance，以帮助阻止更多的垃圾邮件。
- 提交未被分类为垃圾邮件（或网页仿冒）的有害电子邮件。
- 提交被错误分类为垃圾邮件（或网页仿冒）的电子邮件。
- 也可以根据需要在提交后删除邮件。
- 将垃圾邮件发件人的电子邮件地址添加到黑名单，以阻止更多的垃圾邮件。
- 将发件人的电子邮件地址添加到白名单，以防止将来自该发件人的其他电子邮件错误分类为垃圾邮件或网页仿冒。
- 将 Microsoft Outlook “联系人”文件夹中的所有电子邮件地址添加到白名单，以防止将来自已知联系人的电子邮件错误分类为垃圾邮件或网页仿冒。

您可以使用向导安装此工具。如果要为多个电子邮件用户安装此产品，则可以使用脚本进行安装。

此版本中所包含的新功能

本版本的 Customer Submission Tool 包括以下新功能或增强功能：

- [改善了对工具的访问](#)
- [可将电子邮件提交到更多目标](#)
- [自动使用黑名单和白名单](#)
- [提交的数量没有限制](#)
- [提交时自动删除](#)

改善了对工具的访问

先前版本	显示主题行时，标准工具栏上的按钮和“操作”菜单中的条目可用。
当前版本	除此之外，在查看电子邮件时，标准工具栏上的按钮和“操作”菜单中的条目可用。
优势	此工具可更广泛地在 Microsoft Outlook 中使用。
有关详细信息	请参阅 第 23 页的使用工具 。

可将电子邮件提交到更多目标

先前版本	可以将电子邮件提交到 McAfee 实验室进行分析。McAfee 可以分析被错误分类的电子邮件以提高其防垃圾邮件产品的检测率。
当前版本	您可以将电子邮件提交到其他位置： <ul style="list-style-type: none">■ McAfee Secure Content Management appliance■ McAfee Quarantine Manager 软件
优势	样本可以提高 Bayesian 数据库的性能，该数据库经培训可识别垃圾邮件、网页仿冒和可接受的邮件。
从何处查找	此功能在安装工具后可用，或者可以在以后对其进行配置。
有关详细信息	请参阅 第 23 页的使用工具 。

自动使用黑名单和白名单

先前版本	未提供此功能。
当前版本	<p>此工具与 McAfee Quarantine Manager (MQM) 一起使用时，此功能可用。</p> <p>可以自动将发件人添加到白名单（信任的电子邮件地址列表）或黑名单（已知会发送垃圾邮件的电子邮件地址列表）。</p> <p>只需单击，即可将您的 Microsoft Outlook 联系人添加到白名单。</p>
优势	以后会自动将来自己识别为垃圾邮件发送者的电子邮件分类为垃圾邮件。而不会将来自可靠来源的电子邮件分类为垃圾邮件。
从何处查找	将任何电子邮件提交到 MQM 进行分析时，可以使用此功能。
有关详细信息	请参阅第 26 页的 将 Microsoft Outlook 联系人添加到白名单 。

提交的数量没有限制

先前版本	一次最多可以提交 10 个样本。
当前版本	未使用此限制。
优势	可更快且更轻松执行提交。

提交时自动删除

先前版本	提交样本后，必须手动删除垃圾邮件（或网页仿冒）。
当前版本	可以选择在提交后立即删除每个选择的邮件。
优势	可更快且更轻松执行提交。

使用本指南

本指南提供了有关配置和使用产品的信息。其中包括以下主题：

- [简介](#)
产品的概述，包括新功能或已更改功能的说明、本指南概述和 McAfee 联系信息。
- [关于垃圾邮件和网页仿冒](#)
有关垃圾邮件和网页仿冒以及如何减少它们的信息。
- [安装此工具](#)
下载文件。使用 Microsoft Windows Installer。使用脚本进行安装。
- [使用工具](#)
如何提交样本和配置此工具。

读者

这些信息主要面向以下两类读者：

- 负责公司电子邮件安全的网络管理员。
- 负责配置软件检测选项的用户。

约定

本指南使用以下约定：

Bold	用户界面中的所有文字（包括选项、菜单、按钮和对话框名称）。
Condensed	示例： 输入相应帐户的 用户名 和 密码 。
Courier	文件夹或程序的路径；表示用户实际输入内容的文本（例如系统提示符下的命令）。 示例： 此程序的默认位置为： C:\Program Files\McAfee\EPO\3.5.0 在客户端计算机上运行以下命令： scan --help
<i>斜体</i>	用于强调或引入新术语；用于资料中产品文档和主题（标题）的名称。 示例： 有关详细信息，请参阅《VirusScan Enterprise <i>产品指南</i> 》。
蓝色	web 地址 (URL) 和 / 或实时链接。 示例： 请访问 McAfee 网站： http://www.mcafee.com
< 术语 >	尖括号中包含一般术语。 示例： 在控制台树中，在 < 服务器 > 上单击鼠标右键。
	注： 补充信息，例如执行同一个命令的另一种方法。
	提示： 关于最佳实践的建议和来自 McAfee 的关于威胁预防、性能和效率的建议。
	注意： 保护计算机系统、企业、软件安装或数据的重要建议。
	警告： 用户在使用硬件产品时，用于防止其受到人身伤害的重要建议。

获取产品信息

除非另外注明，否则产品文档均以 Adobe Acrobat .PDF 文件提供，并可以从 McAfee 下载站点获得。

产品指南 — 产品介绍和功能；安装和配置软件的详细说明以及有关部署、重复执行任务和操作过程的信息。

发行说明 — *自述文件*。产品信息、已解决的问题、任何已知问题以及对产品或其文档所做的最新增补或更改。软件应用程序附带了一个文本文件。

许可协议 — 包括可为产品购买的所有许可类型的 McAfee 许可协议手册。许可协议阐明了使用许可产品所必须遵守的一般条款和条件。

联系信息 — McAfee 服务和资源的联系信息：技术支持、客户服务、安全总部 (AVERT)、测试计划和培训。软件应用程序附带了一个文本文件。

联系信息

安全总部：AVERT

主页

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

病毒信息库

<http://vil.mcafeesecurity.com>

AVERT WebImmune，提交样本（需要验证登录身份）

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

AVERT DAT 通知服务

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

下载站点

主页

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

防病毒 DAT 文件和引擎更新

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

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

防垃圾邮件规则文件和引擎更新

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

产品升级（需要验证登录身份）

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

针对安全漏洞的 HotFix 和补丁发布（可免费使用）

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

针对产品的 HotFix 和补丁发布（需要提供 ServicePortal 帐户和 McAfee 技术支持授权号）

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

产品有效期结束支持

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

软件和硬件技术支持

主页

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

知识库搜索

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

McAfee 技术支持 ServicePortal（需要验证登录身份）

<https://mysupport.mcafeesecurity.com>

McAfee 安全警报服务 (MSAS)

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

客户服务

电子邮件

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

Web

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

电话 — 美国、加拿大和拉丁美洲免费电话：

+1-888-VIRUS NO 或 +1-888-847-8766

（美国中部时间星期一到星期五上午 8 点到晚上 8 点）

有关 McAfee 全球各地办事处的联系信息，请访问：

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

McAfee 测试计划

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

培训：McAfee University

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

2

关于垃圾邮件和网页仿冒

此工具如何帮助减少垃圾邮件和网页仿冒

本部分介绍了此工具的功能，以及如何与其他 McAfee 安全产品配合使用来减少垃圾邮件。

- [一些有用术语](#)
- [第 12 页的什么是垃圾邮件？](#)
- [第 12 页的避免垃圾邮件](#)
- [第 13 页的什么是网页仿冒？](#)
- [第 13 页的避免网页仿冒](#)
- [第 14 页的什么是 Customer Submission Tool？](#)
- [第 15 页的 Bayesian 学习](#)
- [第 15 页的了解垃圾邮件记分](#)

一些有用术语

以下定义可能会对您有所帮助：

- **漏报** — 尚未分类但包含通常被视为垃圾邮件或网页仿冒内容的电子邮件。
- **误报** — 已被分类为垃圾邮件或网页仿冒，但收件人并不将其视为垃圾邮件或网页仿冒的电子邮件。
- **垃圾邮件制造者** — 创建垃圾邮件的人或机构。
- **假冒** — 例如伪造电子邮件的来源以隐藏发件人的身份，以及创建貌似真实可信的网站。
- **白名单** — 已认可的发件人列表。
- **黑名单** — 发送垃圾邮件或网页仿冒的发件人列表。

什么是垃圾邮件？

所有未经请求和不受欢迎的电子邮件均被视为垃圾邮件。垃圾邮件（也称为未经请求的大量电子邮件或 UBE）包括商业电子邮件、电子版的垃圾邮件以及有害的非商业电子邮件（例如病毒恶作剧、恶作剧和连锁信）。

通常，创建垃圾邮件的人（称为垃圾邮件制造者）会伪造电子邮件的邮件头来隐藏其真实身份，经常使无辜的一方蒙受不白之冤。

什么是非垃圾邮件？

有些电子邮件被称为垃圾邮件，但其并非垃圾邮件。例如，如果您曾经订阅过新闻快讯或在线论坛，索取过有关某些产品的信息，或最近离开了工作组，您的电子邮件地址可能仍在通讯组列表上。要减少此类型的有害电子邮件，请立即从所有过期的通讯组列表中删除您的电子邮件地址。

避免垃圾邮件

每次您使用某个电子邮件地址回复和发送电子邮件、将其发布到 Internet 聊天室或公布某个电子邮件地址时，均会将此电子邮件帐户泄露给垃圾邮件制造者。垃圾邮件制造者将编译电子邮件地址列表。随着时间的推移，此地址会被添加到垃圾邮件制造者社群内越来越多的列表中，从而极大地增加了您接收到的垃圾邮件数目。

请遵守您所在单位或机构建议的有关电子邮件使用的所有准则，养成良好的邮件传送习惯。这有助于减少您接收到的垃圾邮件的数目。例如：

- **谨慎购买垃圾邮件中宣传的产品。**这会提醒垃圾邮件制造者，此电子邮件地址处于活动状态，因此可以将其出售给其他垃圾邮件制造者。您也会因此泄露个人信息。
- **请勿在网上发布个人电子邮件地址。**而改为在参与新闻组和参加竞赛或第三方索要您的电子邮件地址时，使用可任意处置的电子邮件地址。如果此地址收到过多数量的垃圾邮件，则可以停止使用此地址并获取一个新地址。
- **请勿回复垃圾邮件，即使其提出要将您从通讯组列表中删除。**您的回复将向垃圾邮件制造者证实此电子邮件地址处于活动状态，并且随后此地址将被出售给其他垃圾邮件制造者。

另请参阅第 15 页的[了解垃圾邮件记分](#)以了解 McAfee 防垃圾邮件产品的配置会如何周到地协助您减少垃圾邮件。

什么是网页仿冒？

某些垃圾邮件制造者专门 *假冒* 电子邮件来欺骗毫无戒心的电子邮件用户泄露有关其身份和财务帐户的信息。这种特定形式的垃圾邮件称为 *网页仿冒*。

通常，您会接收到看起来是来自某个权威机构（例如银行）的电子邮件。该电子邮件通常会将您引导到一个 *假冒* 的网站，其中要求您提供个人和财务详细信息（例如帐号、密码、信用卡详细信息及社会安全号码）。罪犯可以使用窃取的身份骗取商品和服务（例如个人贷款）、直接从您的帐户中窃取资金、开立银行帐户和洗钱。

避免网页仿冒

- **谨慎对待任何要求您提供密码和其他敏感信息的电子邮件。** 银行不会直接要求提供此类信息，并且通常会通过邮递方式确认信息。任何机构都不可能丢失您的帐户信息。其通常程序是通过邮递方式向您发布新的详细信息，而不是要求您自己通过电子邮件或通过网站提供详细信息。
- **谨慎对待网站链接。** 当要求提供敏感信息时，您可能已被 *假冒* 的链接欺骗。例如，电子邮件中的一个链接看起来像是您银行的网站 (www.example.com)，并且会将您连接到一个看起来可信的站点。但是，浏览器中的地址却显示不同的名称（例如 www.example.net）或 IP 地址（例如 168.192.255.200）。
- **谨慎对待不安全的网站。** 合法机构会运作安全网站，可以在您发送个人信息之前将其加密。其网站地址类似于 https://www.example.com，而不是 http://www.example.com。换言之，他们使用称为 **https** 的安全 Internet 协议，而不是 **http**。

什么是 Customer Submission Tool?

防垃圾邮件产品可提供良好的垃圾邮件防护。但是，有时很难检测到垃圾邮件。垃圾邮件制造者会开发新的技术，而且任何防垃圾邮件产品都不可避免地无法检测到某些较新的垃圾邮件。另外，可能会发生某些错误的检测。防垃圾邮件产品可能会错误地将某些真正的邮件分类为垃圾邮件。

通过分析新的垃圾邮件（和网页仿冒）以及任何被错误分类的电子邮件，McAfee 可以不断改进其防垃圾邮件产品。

Customer Submission Tool 与 Microsoft Outlook 电子邮件软件一起使用可以帮助您减少收到有害电子邮件（或垃圾邮件）的数量。在您阅读电子邮件时，会有新的按钮和菜单条目可供使用。

图 2-1 Microsoft Outlook 中的额外按钮和菜单



此工具可以将电子邮件转发到 McAfee 实验室或其他 McAfee 防垃圾邮件产品以进行分析：

■ 将电子邮件发送到 McAfee 实验室

我们致力于不断改进我们防垃圾邮件产品中的检测。我们会检查被我们的软件或其他供应商的产品错误分类的邮件，并了解原因，从而改进我们的防垃圾邮件产品。



我们将所有提交的样本视为机密材料，并且不会为了除研究以外的任何目的而转发或使用它们。为了正确地分析样本，我们会查看邮件头（包括发件人和主题）和正文内容（包括文本和附件）。在安装此工具时，将提供完整的隐私声明。

■ 将电子邮件发送到 Secure Content Management (SCM) appliance

如果网络受 SCM appliance 保护，则可以将样本提交到设备以进行 Bayesian 学习。请参阅第 15 页。

■ 将电子邮件发送到 McAfee Quarantine Manager (MQM)

如果网络包括 MQM 软件，则可以将样本提交到 McAfee Quarantine Manager 以进行 Bayesian 学习。请参阅第 15 页。

Bayesian 学习

Secure Content Management (SCM) appliance 和 McAfee Quarantine Manager (MQM) 使用基于 Bayes 概率理论的数据库来确定电子邮件是否包含垃圾邮件（或网页仿冒）。

您可以将电子邮件样本发送到 SCM 或 MQM 管理员，来协助培训数据库识别新的垃圾邮件和网页仿冒。单个 McAfee Quarantine Manager 可以处理多个 SCM appliance 的培训。

此 Customer Submission Tool 使您可以通过简单的单击发送样本。管理员可以决定向数据库提交哪些样本。软件会分析每个样本的内容并学习垃圾邮件样式的片语，以备将来参考。

同样，如果您收到被错误分类为垃圾邮件或网页仿冒的电子邮件，则可以将电子邮件发送给管理员以进行非垃圾邮件学习。

正确提交并用于培训的样本越多，将来对垃圾邮件和网页仿冒进行正确分类的可能性就越大。

了解垃圾邮件记分

我们的防垃圾邮件产品将覆盖范围广泛的规则集与每封电子邮件进行匹配。每个规则均与一个记分（正分或负分）相关联。与垃圾邮件样式的特征相匹配的规则对应一个正的记分。与合法邮件属性相匹配的规则对应一个负的记分。将这些记分加在一起，为每封邮件打出一个总的 *垃圾邮件记分*。某些规则很简单，仅根据普通片语进行匹配。其他的规则比较复杂，根据电子邮件的邮件头信息和结构进行匹配。

防垃圾邮件产品可以指定将邮件视为垃圾邮件的级别。通常，记分为 5 即表示邮件为垃圾邮件。防垃圾邮件产品可以通过向邮件的主题行添加某些文本（例如 **SPAM**）来突出显示邮件。您即可以轻松地识别垃圾电子邮件，并决定如何处理此邮件。

请务必正确设置防垃圾邮件产品以在垃圾邮件记分超过某个级别时对垃圾邮件进行分类。如果级别太高（垃圾邮件记分为 10 或更高），则此防垃圾邮件产品将不会对某些垃圾邮件进行分类。如果级别太低，某些真正的电子邮件将会被错误地分类为垃圾邮件。

3

安装此工具 适用于高级用户和管理员

本部分介绍了如何安装 Customer Submission Tool 软件 2.0 版，并提供了以下信息：

- 安装检查表
- 下载安装文件
- 手动安装此工具
- 使用脚本安装此工具

如果您要向多个电子邮件用户提供此工具，建议您使用脚本。请参阅[第 19 页的使用脚本安装此工具](#)。

安装检查表

我们将 Customer Submission Tool 分发为文件，以便可以从我们的网站下载。在安装 Customer Submission Tool 之前，请阅读以下检查表，确保系统正确配置，可以运行安装程序，并确保拥有安装此程序所需的所有信息。

- ✓ 计算机具有 Microsoft Windows 2000（或更高版本）操作系统。
- ✓ 已安装了 Windows 操作系统的最新 Service Pack 和 Windows 更新。
- ✓ 计算机具有 Microsoft Outlook 2000（或更高版本）客户端。Customer Submission Tool 不与 Microsoft Outlook Express 或其他电子邮件客户端一起使用。
- ✓ 计算机可以访问从 McAfee 网站下载的安装文件。
- ✓ 您具有安装 Customer Submission Tool 所需的管理权限和许可。
- ✓ 要将电子邮件提交到 McAfee Quarantine Manager (MQM)，需提供以下信息：
 - MQM 服务器的名称或 IP 地址，例如 server1.domain1 或 192.168.255.200。您可以使用 HTTP、HTTPS 或协议。

根据您的验证进程，可能还需要以下信息：

- 可以直接访问 MQM 的用户名，例如 network_user@example.com。
- 可以直接访问 MQM 的密码。
- ✓ 如果 MQM 软件不可用，则可以将电子邮件提交到 Secure Content Management (SCM) appliance。此时需要提供以下信息：
 - SMTP 服务器的名称或 IP 地址，例如 server1.domain1 或 192.168.255.200。

由于 SCM appliance 不可从工作站直接访问，因此该地址通常指将电子邮件转发到 SCM appliance 的 SMTP 中继。其可以为 Microsoft Exchange 服务器。

 - SMTP 服务器端口号。
 - 用于提交遗漏的垃圾邮件或网页仿冒的电子邮件地址。
 - 用于提交被错误分类为垃圾邮件或网页仿冒的电子邮件的电子邮件地址。

下载安装文件

- 1 在硬盘上创建临时文件夹。
- 2 连接到 McAfee 网站上的防垃圾邮件产品部分，网址为：
<http://www.mcafeesecurity.com/us/products/mcafee/antispam/category.htm>。
- 3 找到“垃圾邮件提交工具”部分，并将存档文件夹解压缩到此临时文件夹。您可以从大多数电子服务中获取必要的实用程序来解压缩 .ZIP 存档文件。

手动安装此工具



要向多个电子邮件用户提供此工具，建议您使用脚本。请参阅第 19 页。

- 1 关闭所有正在运行的应用程序。
- 2 在下载此工具的临时文件夹中，双击“McAfee Customer Submission Tool”文件夹。
- 3 找到并运行 MCST.EXE 文件以打开安装向导。

如果安装程序未自动选择相应的语言，则将打开一个对话框，让您选择一种语言。

图 3-1 “安装向导”对话框



- 4 单击“下一步”以打开“目标文件夹”页面。
- 5 单击“浏览”以指定其他目标文件夹，或保留默认文件夹，然后单击“下一步”。
- 6 在“准备安装应用程序”页面，单击“下一步”以打开“更新系统”页面。

此页面将显示进度消息和进度栏。复制文件并安装软件。此过程可能需要几分钟时间。完成安装时，屏幕将显示“McAfee Customer Submission Tool 已成功安装”页面。

- 7 单击“完成”以关闭此向导。
- 8 启动 Microsoft Outlook。Microsoft Outlook 标准工具栏上将提供其他按钮。请参阅第 14 页的图 2-1。

使用脚本安装此工具

如果您要在多台计算机上安装 Customer Submission Tool，建议使用脚本。要下载所需的文件，请参阅第 18 页的[下载安装文件](#)。

安装命令的一般形式为：

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

有关 Windows Installer 的详细信息，请访问 [Microsoft 网站](#)。

可以在手动配置此工具时进行设置的所有功能（如第 27 页的[配置工具](#)上所述）均可指定为此命令的参数。

以下各表介绍了这些参数。

表 3-1 一般参数

参数和默认值	描述
CONFIGENABLED 1 (是)	允许用户通过使“配置提交设置”按钮可见来配置工具。 0 = 否，1 = 是。任何其他值均视为 1。
DELETESPAMONSUBMIT 0 (否)	提交后删除任何垃圾电子邮件（或网页仿冒）。 0 = 否，1 = 是。任何其他值均视为 0。
DONTSHOWSPAMSUBMIT 0 (否)	当用户单击按钮提交垃圾邮件或网页仿冒时不显示提交对话框。 0 = 否，1 = 是。任何其他值均视为 0。
DONTSHOWHAMSUBMIT 0 (否)	用户单击按钮提交被错误分类的电子邮件时不显示提交对话框。 0 = 否，1 = 是。任何其他值均视为 0。
INSTALLDIR1 请参阅文本。	在此位置安装工具。默认情况下，工具安装在：“C:\Program Files\McAfee\Submission Tool”
MAXSUBMISSIONCOUNT 10000	使用户一次最多可以提交 40 亿封邮件。超出此范围的任何值均视为 10000。
REBOOT (无)	安装完成时重新引导操作系统。 可能的设置为 F = 强制，S = 禁止或 R = 真正禁止。建议使用 S 或 R。

表 3-2 向 McAfee 实验室提交的参数

参数和默认值	描述
ASEENABLED 1 (是)	启用向 McAfee 实验室提交样本。
ASERESPONSEFREQ 0 (立即)	McAfee 实验室响应提交的频率。可能的设置为 0 = 立即、1 = 每日或 2 = 每周或 3 = 从不。任何其他值均视为 0。
ASERESPONSETYPE 0 (简短)	McAfee 实验室发送的确认类型。可能的设置为 0 = 简短、1 = 正常或 2 = 详细。任何其他值均视为 0。

表 3-3 向 McAfee Quarantine Manager (MQM) 提交的参数

参数和默认值	描述
MQMENABLED 0 (否)	启用向 MQM 提交样本。 0 = 否, 1 = 是。任何其他值均视为 0。
MQMPATH “http://mqm.example.com/mqmmuserui”	MQM 上用户文件夹的 URL。
WHITELISTHAMONSUBMIT 0 (否)	自动将发件人的地址添加到白名单, 其中提交的电子邮件不是垃圾邮件或网页仿冒。 0 = 否, 1 = 是。任何其他值均视为 0。
BLACKLISTSPAMONSUBMIT 0 (否)	自动将发件人的地址添加到黑名单, 其中提交的电子邮件是垃圾邮件或网页仿冒。 0 = 否, 1 = 是。任何其他值均视为 0。

表 3-4 向 Secure Content Management (SCM) 提交的参数

参数和默认值	描述
SCMENABLED 0 (否)	启用向 SCM appliance 提交样本。 0 = 否, 1 = 是。任何其他值均视为 0。
SCMRELAYSERVER “mail.example.com”	SMTP 服务器的名称或 IP 地址, 例如 server1.domain1 或 192.168.255.200。
SCMRELAYPORT 25	SMTP 服务器端口号。 范围为 1-65535。
SCMSPAMADRESS “sample_spam@example.com”	用于提交遗漏的垃圾邮件或网页仿冒的电子邮件地址。
SCMHAMADRESS “sample_nonspam@example.com”	用于提交被错误分类为垃圾邮件或网页仿冒的电子邮件的电子邮件地址。

示例



将字符串包含在双引号内。例如：

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

以下命令将使用默认值无提示安装 Customer Submission Tool。用户在 Microsoft Outlook 工具栏上仅可以看到“**提交垃圾邮件或网页仿冒样本**”和“**提交非垃圾邮件样本**”按钮。安装完成时不会发生重新引导。用户仅可以将样本提交到 McAfee 实验室。用户无法重新配置此工具。

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

以下命令将无提示安装 Customer Submission Tool，并使用户可以将样本提交到 McAfee Quarantine Manager。用户可以重新配置此工具。

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

以下命令将安装 Customer Submission Tool，并使用户可以将样本提交到 Secure Content Management appliance。用户将在安装运行时看到安装过程。用户可以重新配置此工具。

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

向电子邮件用户公布此工具

电子邮件用户的 Microsoft Outlook 客户端上安装了 Customer Submission Tool 时，您可以向这些用户发布通知。

示例

今天，我们部署了 McAfee 垃圾邮件提交工具。

此工具将帮助我们所有人减少我们机构收到垃圾邮件的数量。Microsoft Outlook 工具栏中将显示两个额外的按钮。如果您无法看到这两个按钮（如下所示），请重新启动 Microsoft Outlook。

单击此按钮以提交未检测为垃圾邮件的垃圾邮件样本：



单击此按钮以提交被错误分类为垃圾邮件的邮件样本：



更改配置

要在以后更改配置的任何部分而无需重新安装此工具，您可以在以下项处更改注册表设置：

HKEY_CURRENT_USER\Software\McAfee\Submission Tool

以下表中列出了这些设置：

表 3-5 默认注册表值

名称	默认值（十六进制）
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

注册表中的名称与第 19 页的[使用脚本安装此工具](#)中的参数相同。

某些名称（例如 SCM 超时）不可用作参数，且仅能从注册表设置。SCM 超时的默认值为 60000 毫秒（1 分钟）。

要使更改的注册表设置生效，请重新启动 Microsoft Outlook。如果您输入了不正确的值，此工具将使用默认值替换这些值。

4

使用工具 按钮和菜单条目

安装后，Customer Submission Tool 会将某些工具栏按钮和菜单条目（请参阅第 14 页的图 2-1）添加到 Microsoft Outlook 客户端，这些按钮和菜单条目可让您执行以下操作：

- 提交本应分类为垃圾邮件或网页仿冒的邮件。
请参阅“[提交第一个垃圾邮件或网页仿冒样本](#)”和[第 24 页的提交更多垃圾邮件或网页仿冒样本](#)。
- 提交已被错误分类为垃圾邮件或网页仿冒的邮件。
请参阅[第 25 页的提交第一个被错误分类的样本](#)和[第 26 页的提交更多被错误分类的样本](#)。
- 将所有 Microsoft Outlook 联系人添加到白名单（如果使用 McAfee Quarantine Manager）。请参阅[第 26 页的将 Microsoft Outlook 联系人添加到白名单](#)。
- 配置某些工具设置。请参阅[第 27 页的配置工具](#)。

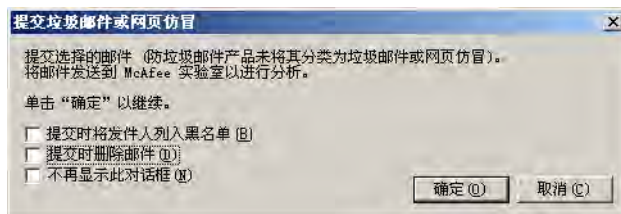
提交第一个垃圾邮件或网页仿冒样本

首次提交电子邮件样本时，您可以按照自己的喜好配置工具。要提交垃圾邮件或网页仿冒样本，请执行以下操作：



- 1 在 Microsoft Outlook 中，查看邮件或选择邮件的主题行。
- 2 单击工具栏上的“**提交垃圾邮件或网页仿冒样本**”按钮。也可以使用“操作”菜单。屏幕将打开以下对话框：

图 4-1 “提交”对话框



- 3 在该对话框中，选择所需功能：

功能	描述
提交时将发件人列入黑名单	此复选框仅在使用 McAfee Quarantine Manager 软件时可用。 将垃圾邮件的发件人添加到黑名单。以后，将禁止任何来自此发件人的电子邮件。
提交时删除邮件	在提交每个选择的垃圾邮件或网页仿冒样本后将其删除。
不再显示此对话框	阻止此对话框再次显示。以后，您可以在按住 SHIFT 键的同时单击“提交垃圾邮件或网页仿冒样本”按钮以再次显示此对话框。

单击“确定”以关闭对话框。样本已提交。

- 4 如果要提交样本到 McAfee Quarantine Manager，系统将提示您输入登录名称和密码。
- 5 当看到报告样本已成功提交的消息框时，请单击“确定”。

此工具无法提交过大的样本（大于 1MB），因此 McAfee 建议您删除此类文件。

提交更多垃圾邮件或网页仿冒样本

要提交垃圾邮件或网页仿冒样本，请执行以下操作：

- 1 在 Microsoft Outlook 中，查看邮件或选择邮件的主题行。



在查看电子邮件的主题行时，您可以一次提交多个样本。要选择一次提交数封连续电子邮件，请使用 SHIFT 键。要选择一次提交数封不连续邮件，请使用 CTRL 键。



- 2 单击工具栏上的“提交垃圾邮件或网页仿冒样本”按钮。也可以使用“操作”菜单。

如果屏幕显示对话框，请选择所需功能。请参阅第 23 页的[提交第一个垃圾邮件或网页仿冒样本](#)。如果未看到此对话框，可以在按住 SHIFT 键的同时单击鼠标左键以显示该对话框。单击“确定”以关闭对话框。

样本已提交。

- 3 当看到报告样本已成功提交的消息框时，请单击“确定”。

此工具无法提交过大的样本（大于 1MB），因此 McAfee 建议您删除此类文件。

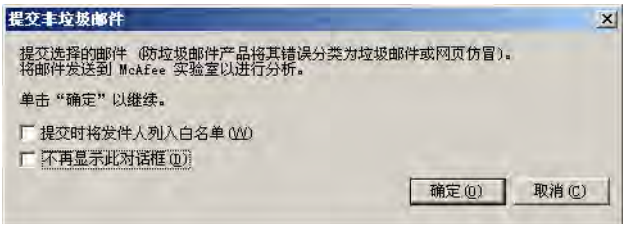
提交第一个被错误分类的样本

首次提交样本时，您可以按照自己的喜好配置工具。要提交被错误分类为垃圾邮件或网页仿冒的样本，请执行以下操作：



- 1 在 Microsoft Outlook 中，查看邮件或选择邮件的主题行。
- 2 单击工具栏上的“提交非垃圾邮件样本”按钮。也可以使用“操作”菜单。屏幕将打开以下对话框：

图 4-2 “提交”对话框



- 3 在该对话框中，选择所需功能：

功能	描述
提交时将发件人列入白名单	此复选框仅在使用 McAfeeQuarantine Manager 时可用。以后，不会将任何来自此发件人的电子邮件分类为垃圾邮件。
不再显示此对话框	以后要查看此对话框，您可以在按住 SHIFT 键的同时单击“提交非垃圾邮件样本”按钮。

- 4 单击“确定”以关闭对话框。样本已提交。
 - 5 如果要样本提交到 McAfee Quarantine Manager，系统将提示您输入登录名称和密码。
 - 6 当看到报告样本已成功提交的消息框时，请单击“确定”。
- 此工具无法提交过大的样本（大于 1MB），因此 McAfee 建议您删除此类文件。

提交更多被错误分类的样本

要提交被错误分类为垃圾邮件或网页仿冒的样本，请执行以下操作：

- 1 在 Microsoft Outlook 中，查看邮件或选择邮件的主题行。



在查看电子邮件的主题行时，您可以一次提交多个样本。要选择一次提交数封连续电子邮件，请使用 SHIFT 键。要选择一次提交数封不连续邮件，请使用 CTRL 键。



- 2 单击工具栏上的“**提交非垃圾邮件样本**”按钮。也可以使用“**操作**”菜单。

如果屏幕显示对话框，选择所需功能（如第 25 页的[提交第一个被错误分类的样本](#)中所述），然后单击“**确定**”以关闭该对话框。如果未看到此对话框，可以在按住 SHIFT 键的同时单击鼠标左键以显示该对话框。单击“**确定**”以关闭对话框。

样本已提交。

- 3 当看到报告样本已成功提交的消息框时，请单击“**确定**”。

此工具无法提交过大的样本（大于 1MB），因此 McAfee 建议您删除此类文件。

将 Microsoft Outlook 联系人添加到白名单



此功能仅在安装了 McAfee Quarantine Manager，并将工具栏上的 Customer Submission Tool 配置为显示“**配置提交设置**”按钮后才可用。



要防止将来自任何 Microsoft Outlook 联系人的电子邮件分类为垃圾邮件（或网页仿冒），您可以将联系人地址添加到白名单：

- 1 在 Microsoft Outlook 中，单击工具栏上的“**配置提交设置**”按钮。
- 2 在 Customer Submission Tool 对话框中，单击“**将联系人地址添加到白名单**”。
- 3 单击“**确定**”以关闭对话框。

以后，将不会对来自白名单中电子邮件地址的邮件进行垃圾邮件或网页仿冒扫描。（但会对所有电子邮件进行病毒扫描。）

配置工具

如果工具栏上的“配置提交设置”按钮可用，您可以配置 Customer Submission Tool 的某些功能。此按钮仅在查看电子邮件主题行时可用。



如果通过未启用此工具脚本安装了此工具，则此按钮不可用。

要配置工具，请执行以下操作：



- 1 单击工具栏上的“配置提交设置”按钮以打开对话框：

图 4-3 “配置”对话框



- 2 在该对话框中，选择所需功能：

标签	功能描述
提交时删除	在成功提交每封垃圾邮件或网页仿冒电子邮件后将其删除。
不显示提交对话框	阻止在提交任何垃圾邮件或网页仿冒（或被错误分类）后显示该对话框。

- 3 如果要样本提交到 McAfee 实验室以进行分析，请选择“McAfee 实验室”选项卡，选择“启用”，然后选择其他任何值：

标签	功能描述
响应频率	指定 McAfee 实验室必须发送自动电子邮件以确认提交的频率。 如果已选择“立即”，并同时发送了多个样本，则在稍后几分钟内可能会收到数个回复。
响应类型	指定每个自动电子邮件中的详细信息。例如，“简短”仅提供确认。

首次使用此工具时，McAfee 建议您选择“立即”和“简短”。

- 4 如果要样本提交到 McAfee Quarantine Manager，请选择“MQM”选项卡，再选择“启用”，然后选择以下功能：

标签	功能描述
URL	MQM 服务器的地址，例如以下之一： <ul style="list-style-type: none"> ■ http://www.example.com ■ 192.168.255.200
用户名	直接与 MQM 进行通讯时使用的用户名（例如 user@example.com）。
密码	密码与用户名相关联。
提交时将发件人的地址添加到黑名单	以后，将禁止任何来自此发件人的电子邮件。
提交时将发件人的地址添加到白名单。	以后，将不会对任何来自此发件人的电子邮件进行垃圾邮件或网页仿冒扫描。始终对电子邮件进行病毒扫描。

- 5 如果要电子邮件提交到 Secure Content Management appliance，请选择“SCM”选项卡，再选择“启用”，然后选择以下功能：

标签	功能描述
服务器	服务器名称，例如以下之一： <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
端口	端口号，例如 25。
垃圾邮件和网页仿冒	地址（按照设备上的配置），例如 spam@example.com。
既不是垃圾邮件也不是网页仿冒	地址（按照设备上的配置），例如 not-spam@example.com。

- 6 单击“确定”以关闭对话框。新设置会立即生效。