

Customer Submission Tool

version 2.0

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSKAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). • Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. • Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc. • FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, ©1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, ©2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijgaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). • Software copyrighted by Kevlin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, ©2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002. • Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992. • Software copyrighted by Cambridge Broadband Ltd., © 2001-2003. • Software copyrighted by Sparta, Inc., © 2003-2004. • Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. • Software copyrighted by Simon Josefsson, © 2003. • Software copyrighted by Thomas Jacob, © 2003-2004. • Software copyrighted by Advanced Software Engineering Limited, © 2004. • Software copyrighted by Todd C. Miller, © 1998. • Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

Contents

1	Introduction	4
	Product features	4
	What's new in this release	5
	Improved access to the tool	5
	More destinations for submitting email	5
	Automatic use of blacklists and whitelists	6
	No limit on number of submissions	6
	Automatic deletion on submission	6
	Using this guide	7
	Audience	7
	Conventions	8
	Getting product information	9
	Contact information	10
2	About spam and phish	11
	Some useful terms	11
	What is spam?	12
	Avoiding spam	12
	What is phish?	13
	Avoiding phish	13
	What is the Customer Submission Tool?	14
	Bayesian learning	15
	Understanding spam scores	15
3	Installing the tool	16
	Installation checklist	17
	Downloading the installation files	18
	Installing the tool manually	18
	Installing the tool using a script	19
	Examples	21
	Announcing the tool to email users	21
	Changing the configuration	22
4	Using the tool	23
	Submitting your first spam or phish sample	23
	Submitting further spam or phish samples	24
	Submitting your first wrongly categorized sample	25
	Submitting further wrongly categorized samples	26
	Adding your Microsoft Outlook contacts to the whitelist	26
	Configuring the tool	27

1

Introduction

The McAfee Customer Submission Tool works with Microsoft® Outlook® email software to help you reduce the amount of unwanted email (or *spam*) that you receive. The tool forwards email messages directly to McAfee Labs or to other McAfee products where the sample can be analyzed and used to reduce further spam.

These topics are included in this section:

- Product features
- What's new in this release
- Using this guide

Product features

The McAfee Customer Submission Tool works with:

- Secure Content Management appliances
- McAfee Quarantine Manager software

The tool adds toolbar buttons and menu entries to the Microsoft Outlook client, and enables you to:

- Submit samples to McAfee Labs for further analysis.
- Submit samples to a McAfee Quarantine Manager or to a Secure Content Management appliance to help prevent further spam.
- Submit unwanted email that was not categorized as spam (or phish).
- Submit email that was wrongly categorized as spam (or phish).
- Optionally, delete the message after the submission.
- Add a spam sender's email address to a blacklist to prevent more spam.
- Add a sender's email address to a whitelist to prevent further email from that sender being wrongly categorized as spam or phish.
- Add all the email addresses in your Microsoft Outlook Contacts folder to a whitelist, to prevent email from known contacts being wrongly categorized as spam or phish.

You can install the tool using a wizard. If you are installing the product for a number of email users, you can install using a script.

What's new in this release

This release of the Customer Submission Tool includes the following new features or enhancements:

- *Improved access to the tool*
- *More destinations for submitting email*
- *Automatic use of blacklists and whitelists*
- *No limit on number of submissions*
- *Automatic deletion on submission*

Improved access to the tool

Previous release	When subject lines are displayed, buttons are available in the standard toolbar, and entries are available from the Actions menu.
Current release	Additionally, when an email message is being viewed, the buttons are available in the standard toolbar and the entries are available from the Actions menu.
Benefits	The tool is more widely available within Microsoft Outlook.
For more information	See Using the tool on page 23 .

More destinations for submitting email

Previous release	You can submit email to McAfee Labs for analysis. McAfee can analyze wrongly categorized email to improve detection rates in its anti-spam products.
Current release	You can submit email to extra locations: <ul style="list-style-type: none">■ A McAfee Secure Content Management appliance■ McAfee Quarantine Manager software
Benefits	The samples can improve the performance of the Bayesian databases, which can be trained to recognize spam and phish and acceptable messages.
Where to find	This feature is available when the tool is installed or can be configured later.
For more information	See Using the tool on page 23 .

Automatic use of blacklists and whitelists

Previous release	This feature was not available.
Current release	<p>This feature is available when you use the tool with McAfee Quarantine Manager (MQM).</p> <p>Senders can be automatically added to a whitelist (a list of trusted email addresses) or blacklist (a list of email addresses that are known to send spam).</p> <p>Your Microsoft Outlook Contacts can be added to a whitelist with a single click.</p>
Benefits	Email sent from identified spammers is automatically categorized as spam in the future. Email from reliable sources is not categorized as spam.
Where to find	The feature operates when any email is submitted for analysis to MQM.
For more information	See Adding your Microsoft Outlook contacts to the whitelist on page 26 .

No limit on number of submissions

Previous release	You were able to submit up to 10 samples at one time.
Current release	The limit does not apply.
Benefits	Submissions are faster and easier to make.

Automatic deletion on submission

Previous release	You must manually delete spam (or phishing) messages after you submit a sample.
Current release	You can choose to have each selected message deleted immediately after the submission.
Benefits	Submissions are faster and easier to make.

Using this guide

This guide provides information on configuring and using your product. These topics are included:

- [Introduction](#)
An overview of the product, including a description of new or changed features, an overview of this guide, and McAfee contact information.
- [About spam and phish](#)
Information about spam and phish and how to reduce them.
- [Installing the tool](#)
Downloading the files. Using a Microsoft Windows Installer. Installing using a script.
- [Using the tool](#)
How to submit samples and configure the tool.





Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's email security.
- Users who are responsible for configuring their software's detection options.

Conventions

This guide uses the following conventions:

Bold Condensed	All words from the interface, including options, menus, buttons, and dialog box names. Example: Type the User name and Password of the appropriate account.
Courier	The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt). Examples: The default location for the program is: <code>C:\Program Files\McAfee\EPO\3.5.0</code> Run this command on the client computer: <code>scan --help</code>
<i>Italic</i>	For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material. Example: Refer to the <i>VirusScan Enterprise Product Guide</i> for more information.
Blue	A web address (URL) and/or a live link. Example: Visit the McAfee web site at: http://www.mcafee.com
<TERM>	Angle brackets enclose a generic term. Example: In the console tree, right-click <SERVER>.
	Note: Supplemental information; for example, another method of executing the same command.
	Tip: Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	Caution: Important advice to protect your computer system, enterprise, software installation, or data.
	Warning: Important advice to protect a user from bodily harm when using a hardware product.

Getting product information

Unless otherwise noted, product documentation comes as Adobe Acrobat .PDF files, available from the McAfee download site.

Product Guide — Introduction to the product and its features; detailed instructions for installing and configuring the software; information on deployment, recurring tasks, and operating procedures.

Release Notes — *ReadMe*. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. A text file is included with the software application.

License Agreement — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement presents general terms and conditions for use of the licensed product.

Contacts — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT), beta program, and training. A text file is included with the software application.

Contact information

Security Headquarters: AVERT

Home Page

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

Virus Information Library

<http://vil.mcafeesecurity.com>

AVERT WebImmune, Submitting a Sample *(Logon credentials required)*

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

AVERT DAT Notification Service

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

Download Site

Home Page

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

Anti-Virus DAT File and Engine Updates

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

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

Anti-Spam Rules File and Engine Updates

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

Product Upgrades *(Logon credentials required)*

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

HotFix and Patch Releases for Security Vulnerabilities *(Available to the public)*

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

HotFix and Patch Releases for Products *(ServicePortal account and McAfee Technical Support grant number required)*

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

Product End-of-Life Support

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

Software and Hardware Technical Support

Home Page

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

KnowledgeBase Search

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

McAfee Technical Support ServicePortal *(Logon credentials required)*

<https://mysupport.mcafeesecurity.com>

McAfee Security Alerting Service (MSAS)

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

Customer Service

Email

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

Web

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

Phone — US, Canada, and Latin America toll-free:

+1-888-VIRUS NO or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

For information on contacting McAfee worldwide offices:

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

McAfee Beta Program

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

Training: McAfee University

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

2

About spam and phish

How the tool helps to reduce them

This section describes what the tool does, and how it works with other McAfee security products to help reduce spam.

- [Some useful terms](#)
- [What is spam? on page 12](#)
- [Avoiding spam on page 12](#)
- [What is phish? on page 13](#)
- [Avoiding phish on page 13](#)
- [What is the Customer Submission Tool? on page 14](#)
- [Bayesian learning on page 15](#)
- [Understanding spam scores on page 15](#)

Some useful terms

The following definitions may be useful to you:

- **false negative** — An email message that has not been categorized but contains content that is generally considered to be spam or phish.
- **false positive** — An email message that has been categorized as spam or phish but the recipient does not consider to be spam or phish.
- **spammer** — A person or organization that creates spam.
- **spoofing** — Examples include forging the origin of an email message to conceal the identity of the sender, and creating a web site that looks authentic.
- **whitelist** — A list of approved senders.
- **blacklist** — A list of senders who send spam or phish.

What is spam?

Any unsolicited and unwelcome email messages can be considered spam. Spam (also known as Unsolicited Bulk Email, or UBE) includes commercial email messages, the electronic equivalent of *junk mail*, and unwanted non-commercial email messages, such as virus hoaxes, jokes, and chain letters.

Frequently, people who create spam, known as *spammers*, forge the headers of the email messages to hide their true identity, often deflecting retaliation toward innocent parties.

What is not spam?

Some email is called spam, but it is not. For example, if you had subscribed to a newsletter or online forum, or requested information about some products, or recently left a workgroup, your email address is probably still on a distribution list. To reduce this type of unwanted email, remove your email address promptly from any out-of-date distribution lists.

Avoiding spam

Every time you use an email address to respond to and send messages, post to an Internet chat room, or advertise an email address, you expose that email account to *spammers*. Spammers compile lists of email addresses. Over time, the address is added to more and more lists within spammer networks, greatly increasing the amount of spam that you receive.

Follow any guidelines about email usage that your organization recommends to promote good messaging practices. This can help reduce the number of spam messages that you receive. For example:

- **Beware of purchasing products advertised within spam messages.** This alerts the spammer that the email address is active so the address can then be sold to other spammers. You also provide personal information.
- **Do not post a personal email address online.** Instead, use a *disposable* email address when you participate in newsgroups, join contests, or whenever a third party requests your email address. If the address receives an excessive amount of spam, you can stop using that address and obtain a new one.
- **Do not reply to spam messages, even if they offer to remove you from the distribution list.** Your reply confirms to the spammer that the email address is active, and the address can then be sold to other spammers.

See also [Understanding spam scores on page 15](#) to understand how careful configuration of McAfee anti-spam products can help reduce spam.

What is phish?

Some spammers specialize in *spoofing* email messages to trick unsuspecting email users into disclosing information about their identity and financial accounts. This specialized form of spam is known as *phish*.

Typically, you receive email that appears to come from a respected organization such as a bank. The email message normally directs you to a *spoofed* web site where you are asked for personal and financial details such as account number, password, credit card details, and social security numbers. Criminals can use the stolen identity to fraudulently obtain goods and services (such as personal loans), to steal directly from your account, open bank accounts and launder money.

Avoiding phish

- **Beware of any email that asks for passwords and other sensitive information.** Banks do not ask for such information directly and normally verify information using the post. It is unlikely for any organization to have *lost* your account information. Their normal procedure is to issue new details to you by post, rather than ask you to provide the details yourself through email or via a web site.
- **Beware of links to web sites.** When asked to provide sensitive information, you might be directed via a *spoofed* link. For example, a link in an email looks like your bank's web site (www.example.com) and connects you to a site that appears authentic. However, the address in the browser shows a different name (such as www.example.net) or an IP address (such as 168.192.255.200) instead.
- **Beware of insecure web sites.** Legitimate organizations operate secure web sites that encrypt your personal information before you send it. Their web sites have addresses such as https://www.example.com rather than http://www.example.com. In other words, they use a secure Internet protocol known as **https** rather than **http**.

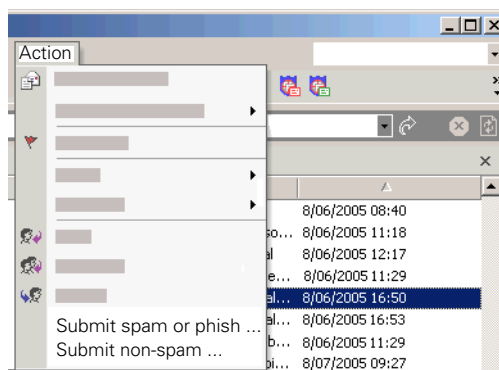
What is the Customer Submission Tool?

Anti-spam products provide good protection against spam. However, spam is sometimes difficult to detect; spammers develop new techniques and some newer spam is inevitably not detected by *any* anti-spam product. In addition, some false detections can occur; an anti-spam product can wrongly categorize some genuine messages as spam.

By analyzing new spam (and phish) and any wrongly categorized email, McAfee can continuously improve its anti-spam products.

The Customer Submission Tool works with Microsoft Outlook email software to help you reduce the amount of unwanted email (or *spam*) that you receive. Extra buttons and menu entries become available when you read your email.

Figure 2-1 Extra buttons and menus in Microsoft Outlook



The tool can forward email messages to McAfee Labs or to other McAfee anti-spam products for analysis:

- **Sending email to McAfee Labs**

We are dedicated to continuously improving detection in our anti-spam products. We examine messages that were incorrectly categorized by our software or other vendors' products, and learn *why*, and thereby improve our anti-spam products.



We treat all submitted samples as confidential material and do not forward or use them for any purpose other than research. To analyze the sample properly, we look at the message headers, including sender and subject, and body contents, including text and attachments. A full privacy statement is available at the time that you install the tool.

- **Sending email to a Secure Content Management (SCM) appliance**

If the network is protected by an SCM appliance, you can submit samples to an appliance for Bayesian learning. See [page 15](#).

- **Sending email to McAfee Quarantine Manager (MQM)**

If the network includes MQM software, you can submit samples to a McAfee Quarantine Manager for Bayesian learning. See [page 15](#).

Bayesian learning

The Secure Content Management (SCM) appliances and McAfee Quarantine Manager (MQM) use a database based on the Bayes theory of probability to determine whether an email message contains spam (or phish).

You can help to train the databases to recognize new types of spam and phish by sending email samples to the SCM or MQM administrator. A single McAfee Quarantine Manager can handle the training of several SCM appliances.

The Customer Submission Tool enables you to send the samples with a single click. The administrator can decide which samples to submit to the database. The software analyzes the content of each sample and *learns* the spam-like phrases for future reference.

Similarly, if you receive email messages that have been incorrectly categorized as spam or phish, you can send the email messages to the administrator for non-spam learning.

The more samples that are correctly submitted and used for training, the greater the chance that spam and phish can be correctly categorized in the future.

Understanding spam scores

Our anti-spam products match an extensive set of rules against every email message. Each rule is associated with a score — positive or negative. Rules that match for spam-like characteristics give a positive score. Rules that match attributes of legitimate messages give a negative score. When added together, the scores give each message an overall *spam score*. Some rules are simple, and match only on popular phrases. Other rules are more complex and match on the header information and structure of email messages.

Anti-spam products can specify a level at which to regard a message as spam. Typically, a score of 5 indicates that a message is spam. Your anti-spam product can highlight messages by adding some text, such as ****SPAM**** to the subject line of the message. You can then easily identify a spam email message, and decide how to handle the message.

It is important that your anti-spam product is correctly set to categorize spam when the spam score exceeds a certain level. If the level is too high (a spam score 10 or more), the anti-spam product will not categorize some spam messages. If the level is too low, some genuine email messages will be wrongly categorized as spam.

3

Installing the tool

For expert users and administrators

This section explains how to install the Customer Submission Tool software version 2.0 and provides the following information:

- Installation checklist
- Downloading the installation files
- Installing the tool manually
- Installing the tool using a script

If you intend to provide the tool to many email users, we recommend that you use a script. See [Installing the tool using a script on page 19](#).

Installation checklist

We distribute the Customer Submission Tool as a file to download from our web site. Before you install the Customer Submission Tool, read the following checklist to ensure that your system is configured correctly to run the installation program, and that you have all the information that you need to install the program.

- ✓ The computer has a Microsoft Windows 2000 (or later) operating system.
- ✓ You have installed the latest service packs for Windows operating systems and Windows updates.
- ✓ The computer has a Microsoft Outlook 2000 (or later) client. The Customer Submission Tool does not work with Microsoft Outlook Express or other email clients.
- ✓ The computer has access to the installation files that are downloaded from the McAfee web site.
- ✓ You have the administrative rights and permissions needed to install the Customer Submission Tool.
- ✓ To submit email to McAfee Quarantine Manager (MQM), have this information ready:

- Name or IP address of the MQM server such as server1.domain1 or 192.168.255.200. You can use HTTP or HTTPS, or the protocol.

Depending on your authentication process, you might also need:

- Your user name to access MQM directly, such as network_user@example.com.
- A password to access MQM directly.
- ✓ If MQM software is not available, you can submit email to a Secure Content Management (SCM) appliance. Have this information ready:
 - Name or IP address of the SMTP server such as server1.domain1 or 192.168.255.200.

The appliance is unlikely to be directly accessible from a workstation, so this address typically refers to the SMTP relay that forwards email to a SCM appliance. This can be the Microsoft Exchange server.
 - Number of the SMTP server port.
 - Email address for submitting missed spam or phish.
 - Email address for submitting email that was wrongly categorized as spam or phish.

Downloading the installation files

- 1 Create a temporary folder on your hard disk.
- 2 Connect to the section for anti-spam products on the McAfee web site:
<http://www.mcafeesecurity.com/us/products/mcafee/antispam/category.htm>.
- 3 Locate the **Spam Submission Tool** section and extract the archived folder to the temporary folder. You can obtain the necessary utilities to extract .ZIP archives from most electronic services.

Installing the tool manually

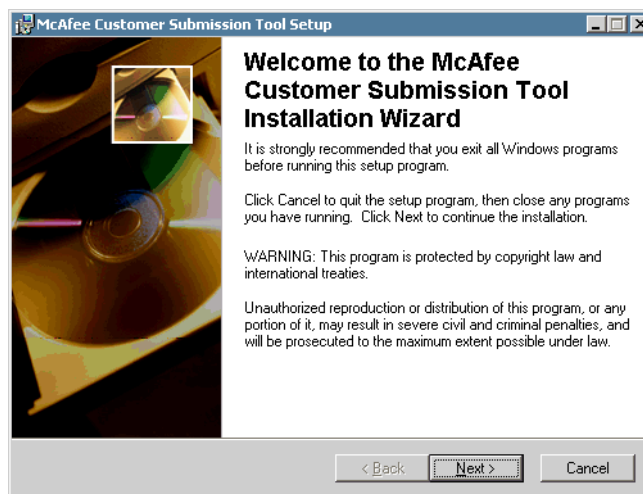


To provide the tool to many email users, we recommend that you use a script. See [page 19](#).

- 1 Close all running applications.
- 2 In the temporary folder where you downloaded the tool, double-click the **McAfee Customer Submission Tool** folder.
- 3 Locate and run MCST.EXE file to open the installation wizard.

If the installer has not automatically selected the appropriate language, a dialog box opens to enable you to select a language.

Figure 3-1 Installation Wizard dialog box



- 4 Click **Next** to open the **Destination Folder** page.
- 5 Click **Browse** to specify a different destination folder, or keep the default, then click **Next**.

- 6 At the **Ready to Install the Application** page, click **Next** to open the **Updating System** page.

The page displays progress messages and a progress bar. The files are copied and the software is installed. This can take a few minutes. When the installation is complete, the **McAfee Customer Submission Tool has been successfully installed** page appears.

- 7 Click **Finish** to close the wizard.
- 8 Start Microsoft Outlook. Extra buttons are available on the Microsoft Outlook standard toolbar. See [Figure 2-1 on page 14](#).

Installing the tool using a script

If you intend to install the Customer Submission Tool on several computers, we recommend that you use a script. To download the files that you need, see [Downloading the installation files on page 18](#).

The install command has the general form:

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

For more information about the [Windows Installer](#), visit the [Microsoft web site](#).

All of the features that can be set when configuring the tool manually (as on [Configuring the tool on page 27](#)) can be specified as parameters in this command.

The following tables describe the parameters.

Table 3-1 General parameters

Parameter and default value		Description
CONFIGENABLED	1 (Yes)	Allow the user to configure the tool by making the Configure submissions settings button visible. 0=No, 1 = Yes. Any other value is treated as 1.
DELETESPAMONSUBMIT	0 (No)	Delete any spam (or phishing) email after submission. 0=No, 1 = Yes. Any other value is treated as 0.
DONTSHOWSPAMSUBMIT	0 (No)	Do not show the submission dialog when the user clicks the button to submit spam or phishing. 0=No, 1 = Yes. Any other value is treated as 0.
DONTSHOWHAMSUBMIT	0 (No)	Do not show the submission dialog box when the user clicks the button to submit an incorrectly categorized email message. 0=No, 1 = Yes. Any other value is treated as 0.
INSTALLDIR1	See text.	Install the tool at this location. By default, the tool is installed at: "C:\Program Files\McAfee\Submission Tool"
MAXSUBMISSIONCOUNT	10000	Allow the user to submit up to 4 billion messages at one time. Any value outside this range is treated as 10000.
REBOOT	(None)	Reboot the operating system when the installation finishes. Possible settings are F=Forced, S=Suppress, or R=Really Suppress. We recommend S or R.

Table 3-2 Parameters for submissions to McAfee Labs

Parameter and default value		Description
ASEENABLED	1 (Yes)	Enable the submission of samples to McAfee Labs.
ASERESPONSEFREQ	0 (Immediately)	How often McAfee Labs respond to the submissions. Possible settings are 0= Immediate , 1= Daily or 2= Weekly or 3= Never . Any other value is treated as 0.
ASERESPONSETYPE	0 (Brief)	Type of acknowledgement that McAfee Labs sends. Possible settings are 0= Brief , 1= Normal , or 2= Detailed . Any other value is treated as 0.

Table 3-3 Parameters for submissions to McAfee Quarantine Manager (MQM)

Parameter and default value		Description
MQMENABLED	0 (No)	Enable the submission of samples to MQM. 0=No, 1 = Yes. Any other value is treated as 0.
MQMPATH		URL to the user's folder on MQM. "http://mqm.example.com/mqmuserui"
WHITELISTHAMONSUBMIT	0 (No)	Automatically add the sender's address to a whitelist, where the submitted email was not spam or phish. 0=No, 1 = Yes. Any other value is treated as 0.
BLACKLISTSPAMONSUBMIT	0 (No)	Automatically add the sender's address to a blacklist, where the submitted email was spam or phish. 0=No, 1 = Yes. Any other value is treated as 0.

Table 3-4 Parameters for submissions to Secure Content Management (SCM)

Parameter and default value		Description
SCMENABLED	0 (No)	Enable the submission of samples to an SCM appliance. 0=No, 1 = Yes. Any other value is treated as 0.
SCMRELAYSERVER		Name or IP address of the SMTP server such as server1.domain1 or 192.168.255.200. "mail.example.com"
SCMRELAYPORT	25	Number of the SMTP server port. The range is 1-65535.
SCMSPAMADDRESS		Email address for submitting missed spam or phish. "sample_spam@example.com"
SCMHAMADDRESS		Email address for submitting email that was wrongly categorized as spam or phish. "sample_nonspam@example.com"

Examples



Enclose character strings in double quotes. For example:

```
INSTALLDIR1="C:\FOLDER A\FOLDER 1"
```

The following command silently installs the Customer Submission Tool using the default values. The user will see only the **Submit spam or phish sample** and **Submit non-spam sample** buttons on the Microsoft Outlook toolbar. No reboot occurs when the installation finishes. The user can submit samples to McAfee Labs only. The user cannot reconfigure the tool.

```
msiexec /qn /i mcst.msi CONFIGENABLED=0 INSTALLDIR1="C:\FOLDER A\FOLDER 1" REBOOT=R
```

The following command silently installs the Customer Submission Tool and enables the user to submit samples to McAfee Quarantine Manager. The user can reconfigure the tool.

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

The following command installs the Customer Submission Tool and enables the user to submit samples to a Secure Content Management appliance. The user will see the installation as it runs. The user can reconfigure the tool.

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

Announcing the tool to email users

You can issue an announcement to the email users when the Customer Submission Tool has been installed on their Microsoft Outlook clients.

Example

Today, we are deploying the McAfee spam submission tool.

The tool will help us all to reduce the amount of SPAM that our organization receives. Two extra buttons will appear in the toolbar of Microsoft Outlook. If you cannot see the buttons (shown below), restart Microsoft Outlook.

Click this button to submit samples of spam that were not detected as spam:



Click this button to submit samples of messages that were wrongly categorized as spam:



Changing the configuration

To change any part of the configuration later without having to re-install the tool, you can change registry settings at the following key:

HKEY_CURRENT_USER\Software\McAfee\Submission Tool

The settings are listed in the following table:

Table 3-5 Default registry values

Name	Default value (in hexadecimal)
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

The names in the registry are identical to the parameters in [Installing the tool using a script on page 19](#).

Some names, such as the SCM time-outs, are not available as parameters and can only be set from the registry. The SCM time-outs have default values of 60000 milliseconds (1 minute).

To enforce the changed registry settings, restart Microsoft Outlook. If you enter any incorrect values, the tool replaces them with the default values.

4

Using the tool Buttons and menu entries

Once installed, the Customer Submission Tool adds some toolbar buttons and menu entries (see [Figure 2-1 on page 14](#)) to the Microsoft Outlook client, which enable you to:

- Submit messages that should have been categorized as spam or phish.
See [Submitting your first spam or phish sample](#) and [Submitting further spam or phish samples on page 24](#).
- Submit messages that have been wrongly categorized as spam or phish.
See [Submitting your first wrongly categorized sample on page 25](#) and [Submitting further wrongly categorized samples on page 26](#).
- Add all your Microsoft Outlook contacts to a whitelist (if McAfee Quarantine Manager is in use). See [Adding your Microsoft Outlook contacts to the whitelist on page 26](#).
- Configure some of the tool settings. See [Configuring the tool on page 27](#).

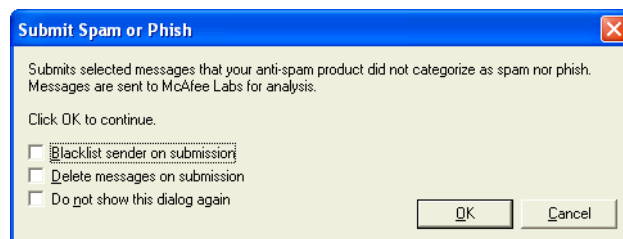
Submitting your first spam or phish sample

When you first submit an email sample, you can configure the tool as you prefer. To submit a spam or phish sample:



- 1 In Microsoft Outlook, view the message or select the subject line of the message.
- 2 Click the **Submit spam or phish sample** button on the toolbar. You can also use the **Action** menu. A dialog box opens:

Figure 4-1 Submission dialog box



- 3 At the dialog box, select the features that you want:

Feature	Description
Blacklist sender on submission	This checkbox is available only if McAfee Quarantine Manager software is in use. Add the sender of the spam email to a blacklist. In future, any email from this sender will be blocked.
Delete messages on submission	Delete each selected spam or phish sample, after it is submitted.
Do not show this dialog again	Prevent this dialog box appearing again. In future, you can SHIFT-click the Submit spam or phish sample button to show this dialog box again.

Click **OK** to close the dialog box. The sample is submitted.

- 4 If you are submitting the sample to McAfee Quarantine Manager, you are prompted for your logon name and password.
- 5 When you see a message box stating that the sample was submitted successfully, click **OK**.

The tool does not submit samples that are too large (over 1MB), so McAfee recommend that you delete such files.

Submitting further spam or phish samples

To submit a spam or phish sample:

- 1 In Microsoft Outlook, view the message or select the subject line of the message.



When viewing the email subject lines, you can submit more than one sample at a time. To select a block of several email messages for a single submission, use the SHIFT key. To select several separate messages, use the CTRL key.



- 2 Click the **Submit spam or phish sample** button on the toolbar. You can also use the **Action** menu.

If a dialog box appears, select the features that you want. See [Submitting your first spam or phish sample on page 23](#). If you do not see the dialog box, you can use SHIFT-click to display it. Click **OK** to close the dialog box.

The sample is submitted.

- 3 When you see a message box stating that the sample was submitted successfully, click **OK**.

The tool does not submit samples that are too large (over 1MB), so McAfee recommend that you delete such files.

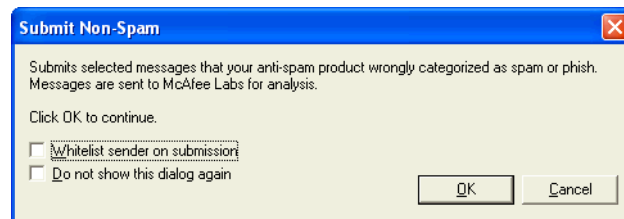
Submitting your first wrongly categorized sample

When you first submit a sample, you can configure the tool as you prefer. To submit a sample that was wrongly categorized as spam or phish:



- 1 In Microsoft Outlook, view the message or select the subject line of the message.
- 2 Click the **Submit non-spam sample** button on the toolbar. You can also use the **Action** menu. A dialog box opens:

Figure 4-2 Submission dialog box



- 3 At the dialog box, select the features that you want:

Feature	Description
Whitelist sender on submission	This checkbox is available only if McAfee Quarantine Manager is in use. In future, any email from this sender will not be categorized as spam.
Do not show this dialog again	To view this dialog box in the future, you can SHIFT-click the Submit non-spam sample button.

- 4 Click **OK** to close the dialog box. The sample is submitted.
- 5 If you are submitting the sample to McAfee Quarantine Manager, you are prompted for your logon name and password.
- 6 When you see a message box stating that the sample was submitted successfully, click **OK**.

The tool does not submit samples that are too large (over 1MB), so McAfee recommend that you delete such files.

Submitting further wrongly categorized samples

To submit a sample that was wrongly categorized as spam or phish:

- 1 In Microsoft Outlook, view the message or select the subject line of the message.



When viewing the email subject lines, you can submit more than one sample at a time. To select a block of several email messages for a single submission, use the SHIFT key. To select several separate messages, use the CTRL key.



- 2 Click the **Submit non-spam sample** button on the toolbar. You can also use the **Action** menu.

If a dialog box appears, select the features that you want (as described in [Submitting your first wrongly categorized sample on page 25](#)), then click **OK** to close the dialog box. If you do not see the dialog box, you can use SHIFT-click to display it. Click **OK** to close the dialog box.

The sample is submitted.

- 3 When you see a message box stating that the sample was submitted successfully, click **OK**.

The tool does not submit samples that are too large (over 1 MB), so McAfee recommend that you delete such files.

Adding your Microsoft Outlook contacts to the whitelist



This feature is available only if McAfee Quarantine Manager is installed, and the Customer Submission Tool is configured to display the **Configure submissions settings** button on the toolbar.

To prevent email from any of your Microsoft Outlook contacts being categorized as spam (or phish), you can add the addresses of your contacts to your whitelist:



- 1 In Microsoft Outlook, click the **Configure submission settings** button on the toolbar.
- 2 In the **Customer Submission Tool** dialog box, click **Add contact addresses to whitelist**.
- 3 Click **OK** to close the dialog box.

In the future, messages sent to you from email addresses in your whitelist will not be scanned for spam or phish. (All email messages are scanned for viruses.)

Configuring the tool

If the **Configure submission settings** button is available on the toolbar, you can configure some features of the Customer Submission Tool. The button is available only when viewing email subject lines.



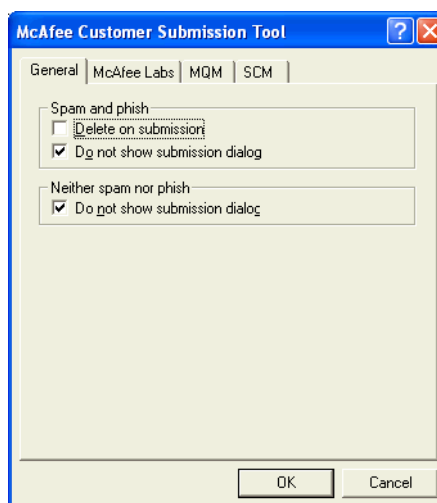
The button is not available if the tool was installed via a script that did not enable it.

To configure the tool:



- 1 Click the **Configure submission settings** button on the toolbar to open a dialog box:

Figure 4-3 Configuration dialog box



- 2 At the dialog box, select the features that you want:

Label	Description of feature
Delete on submission	Delete each spam or phish email after it is successfully submitted.
Do not show submission dialog	Prevent a dialog box appearing when any spam or phish (or wrongly categorized) email is submitted.

- 3 If you intend to submit samples to McAfee Labs for analysis, select the **McAfee Labs** tab, select **Enable**, then select any other values:

Label	Description of feature
Frequency of response	Specify how often McAfee Labs must send an automatic email to acknowledge your submissions. If you have selected Immediately , and then send many samples at the same time, you might receive several replies within the following few minutes.
Type of response	Specify the detail in each automatic email. For example, Brief provides an acknowledgement only.

When you first use the tool, McAfee recommend that you select **Immediately** and **Brief**.

- 4 If you intend to submit samples to McAfee Quarantine Manager, select the **MQM** tab, select **Enable**, then select the features:

Label	Description of feature
URL	The address of the MQM server such as one of the following: <ul style="list-style-type: none"> ■ http://www.example.com ■ 192.168.255.200
User name	The user name (such as user@example.com) that is used when communicating with MQM directly.
Password	The password associated with the user name.
Add senders' addresses to blacklist on submission	In future, any email from this sender will be blocked.
Add senders' addresses to whitelist on submission	In future, any email from this sender will not be scanned for spam or phish. Email is always scanned for viruses.

- 5 If you intend to submit email to a Secure Content Management appliance, select the **SCM** tab, select **Enable**, then select the features:

Label	Description of feature
Server	A server name such as one of the following: <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
Port	A port number such as 25.
Spam and phish	An address (as configured on the appliance) such as spam@example.com.
Neither spam nor phish	An address (as configured on the appliance) such as not-spam@example.com.

- 6 Click **OK** to close the dialog box. The new settings take immediate effect.