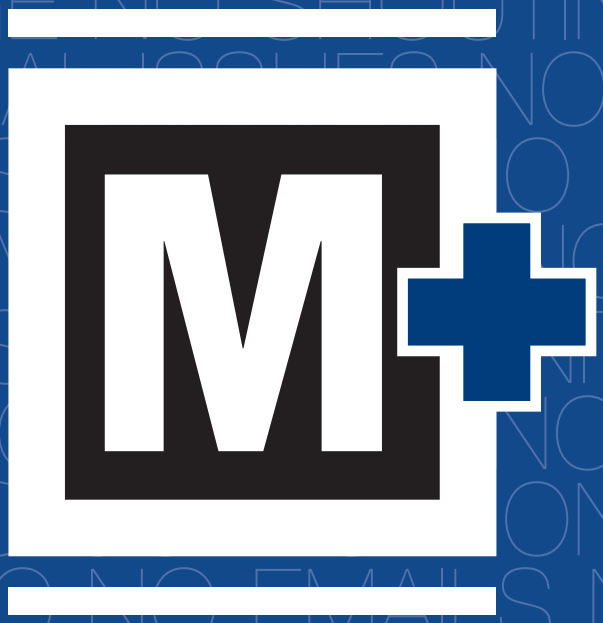
M+Quarantine User Guide



Guardian™

Extreme Email Firewall

RISK FREE EMAIL

Messaging Architects™

BUSINESS DRIVEN EMAIL

Trademarks

Apple Inc ..... Safari™
Messaging Architects ..... M+Guardian™, M+Quarantine™
Microsoft Corporation ..... Microsoft®, Internet Explorer™, Outlook Express™
Mozilla ..... Firefox®,Thunderbird™
Netscape ..... Netscape®
Novell, Inc ..... GroupWise®

Messaging Architects
180 Peel, Suite 333
Montreal, QC Canada H3C 2G7
Tel: 514-392-9220 Fax: 514-392-9120
World Wide Web: www.messagingarchitects.com

Contents

Your Notes

1 About M+Quarantine

M+Quarantine is a web-based application that allows end users to access and manage their quarantined email from anywhere in the world through the Internet. A component of the M+Guardian Extreme Email Firewall, M+Quarantine allows end users to see how many email messages containing viruses, spam, blocked attachments or other filtered mail is being trapped by M+Guardian, and how effective M+Guardian is at protecting the organization's email and messaging collaboration system.

1.1 About this User Guide

This user guide is intended for the M+Quarantine end user and assumes that you have a working knowledge of your computer and its operating system. The guide is structured in a series of tasks to help you learn the M+Quarantine application as quickly as possible. The guide will walk you through each of the tasks you can perform in M+Quarantine.

1.1.1 Style Conventions

The following style conventions are used in this guide:

- The names of files, directory paths, and guides appear in italics. For example,
  - The data is stored in the *sample.xml* file.
  - The file is located in your *C:\Program Files\Messaging Architects* folder.
  - Please refer to your *M+Guardian Administration Guide*.
- Menus and commands that you need to choose are displayed in the form **Menu > Command**. For example, **File > Save** means click the **File** in the menu bar, then click **Save** in the menu that appears.
- The names of keys are displayed in small capital letters, such as **CTRL** key.
- A plus (+) sign is used to indicate combinations of keys and/or mouse operations. For example:
  - **CTRL+C** means to hold down the **CTRL** key while pressing the **C** key.
  - **SHIFT+click** means to hold down the **SHIFT** key while you click an item with the mouse.

1.1.2 Symbols

Throughout the guide, you will sometimes see special symbols in the margins. The symbols are intended to supplement the information in the section where they are found. These symbols serve different functions based on the icon used to represent them. The types of symbols are:

Note: This symbol provides supplemental information and/or configuration tips. Look for this symbol if you want to find additional information for the subject that is being discussed.

Important: This symbol indicates that the information described in the corresponding section is important. Pay attention to this symbol when you encounter it.

Warning: This symbol lets you know when something requires caution. The goal of this symbol is to let you know about the potential errors into which you might run when using the function in question.

Tip: This symbol provides additional configuration tips. Look for this symbol if you want a tip on how to accomplish something.

Your Notes

2 Introducing M+Quarantine

The Quarantine Reports feature of M+Guardian allows system administrators to create policies that automatically send customized Quarantine Reports containing event information to end users in the form of an administrator-sent email message. When new mail is quarantined, M+Guardian automatically sends email messages in the form of Quarantine Reports to your mail client. To access your quarantined email, simply click the URL link contained in the body of the Quarantine Report to automatically launch the M+Quarantine application, or use the available actions in the Quarantine Report. For more information on Quarantine Reports, see "Reviewing Quarantine Reports" on page 15.

2.1 Launching M+Quarantine

To start a M+Quarantine session:

1. Click the URL link contained in the body of the Quarantine Report or follow the URL link provided by your system administrator.

You can also start a M+Quarantine session yourself at any time by opening a standard web browser and entering the URL provided by your system administrator directly in the address bar.

2. On the M+Quarantine login screen, enter your email address and corresponding password in the available text boxes.
3. Under **Language**, choose the language, or leave the default setting at **Auto detect** to automatically detect your browser's language setting.
4. Click **Log In**.

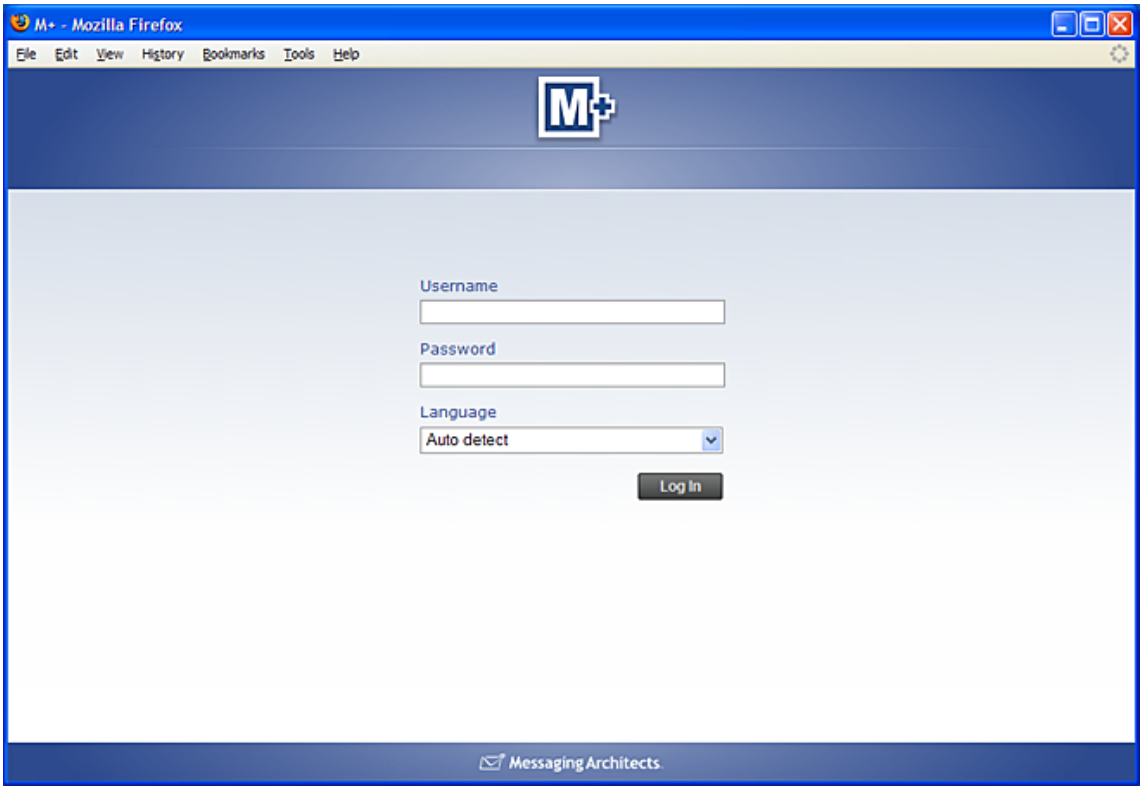


Figure 2-1: M+Quarantine login screen

M+Quarantine supports Internet Explorer 6.0 and higher, Mozilla Firefox 1.5 and higher, Netscape 7.1 and higher and Safari 3.0 and higher. Messaging Architects recommends Mozilla Firefox for enhanced performance.

3 M+Quarantine User Interface

M+Quarantine filters incoming email messages to determine whether the messages contain viruses, spam, blocked file attachments or other forbidden content. The main M+Quarantine interface displays the name and email address of the sender and the subject of the message. You can also open an email message in quarantine and view header details such as the sender of the message and the date and time the message was received in quarantine.

3.1 Navigational Tabs

To start navigating through M+Quarantine, use the navigational tabs on the left of the interface to open the corresponding category.

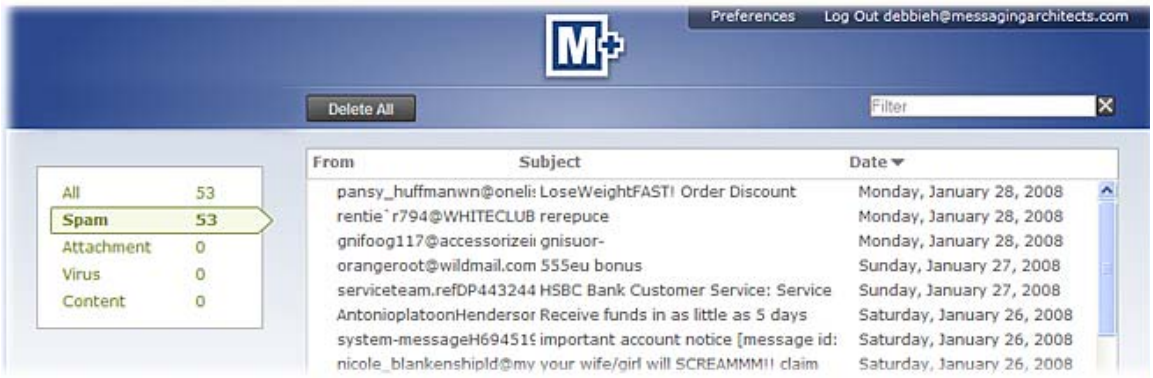


Figure 3-1: M+Quarantine, Navigational tabs

By default, every time you start a new quarantine session, the **Spam** tab is displayed.

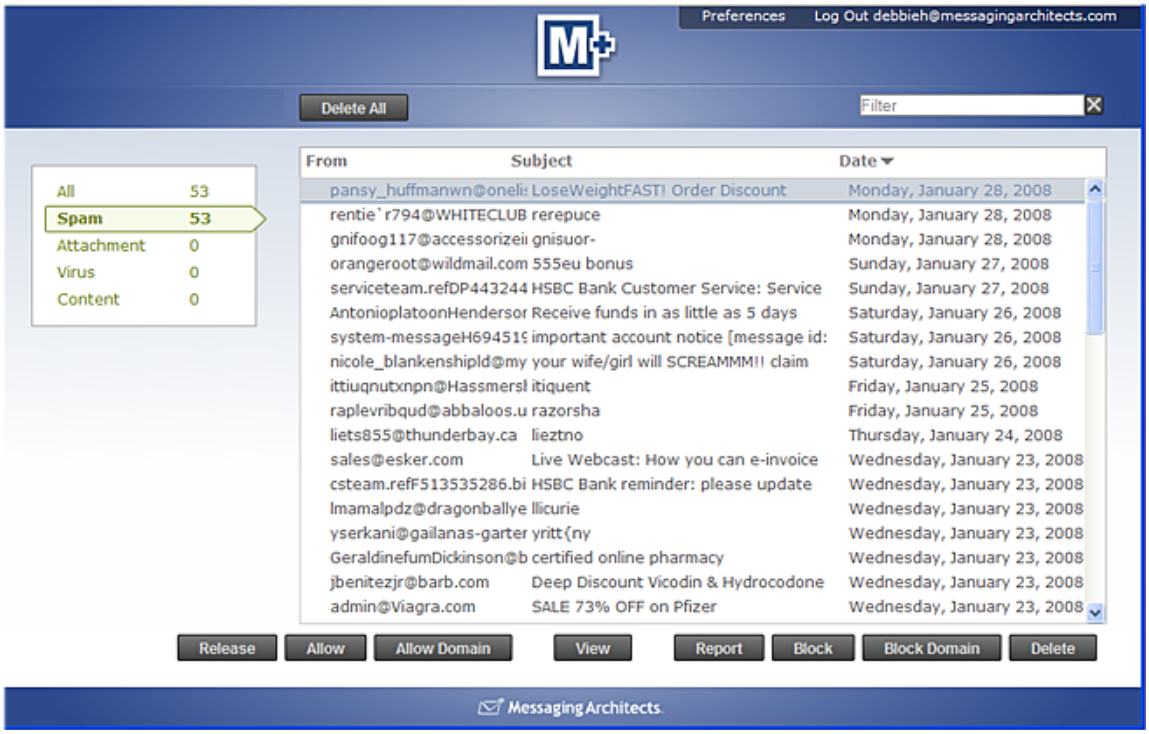


Figure 3-2: M+Quarantine, Spam tab

The **Spam** tab displays a list of email messages tagged as spam in your quarantine. To view a complete list of email messages from all categories, click the **All** tab.

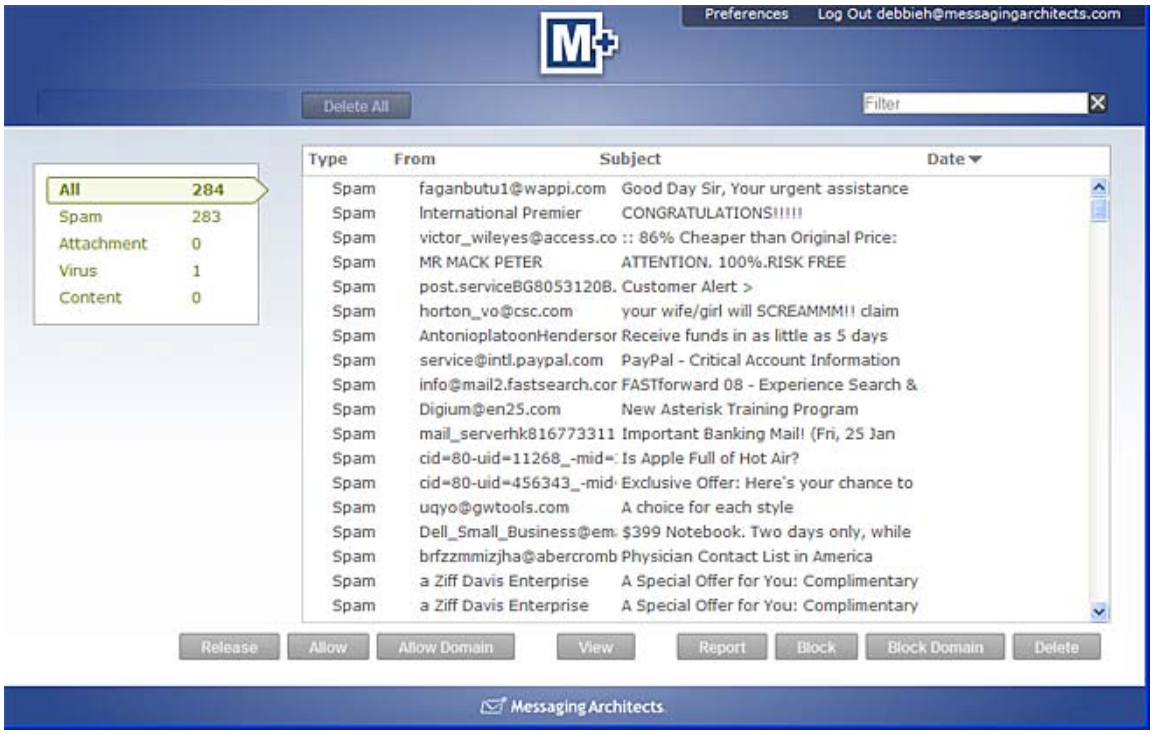


Figure 3-3: M+Quarantine, All tab

The **All** tab displays a complete list of email messages in your quarantine by category. Email messages are quarantined into the following categories under the corresponding category tab:

- **Spam** There are 7 categories of spam that can be filtered into quarantine. These categories and the level of spam filtering applied to each category is determined by the system administrator.
- **Attachment** A blocked file attachment is any file type that is identified as a threat by the system administrator.
- **Virus** A virus is any suspect email that is trapped by the dedicated anti-virus engines.
- **Content** Forbidden content is any type of prohibited content containing words or expressions that the system administrator has banned.

3.2 Reviewing Your Quarantine

You can review your quarantined email messages directly from the quarantine by selecting or highlighting the message in the list and clicking the appropriate message action icon that appears at the bottom of the interface.

A Filter option is also available to allow you to filter items in quarantine by subject or date.

The available message actions include:

3.2.1 Release

This option allows you to release the message from quarantine to your Inbox. Click **Release** to transfer the email message out of quarantine to your Inbox. This option is only available from the **Spam** tab.

Email messages containing blocked file attachments, viruses, and forbidden content cannot be released to your Inbox. Only email messages considered spam can be released from quarantine.

3.2.2 Allow

This option allows you to add an email address to your Allow List directly from the Spam tab. To add an address to your Allow List, highlight the message in the message list, and click **Allow**. You can add individual email addresses to your Allow List, or you can add the entire domain. If you want to add both the email address and the domain to your Allow List, choose **Allow Domain**. Email from addresses and domains on your Allow List will always be sent to your Inbox.

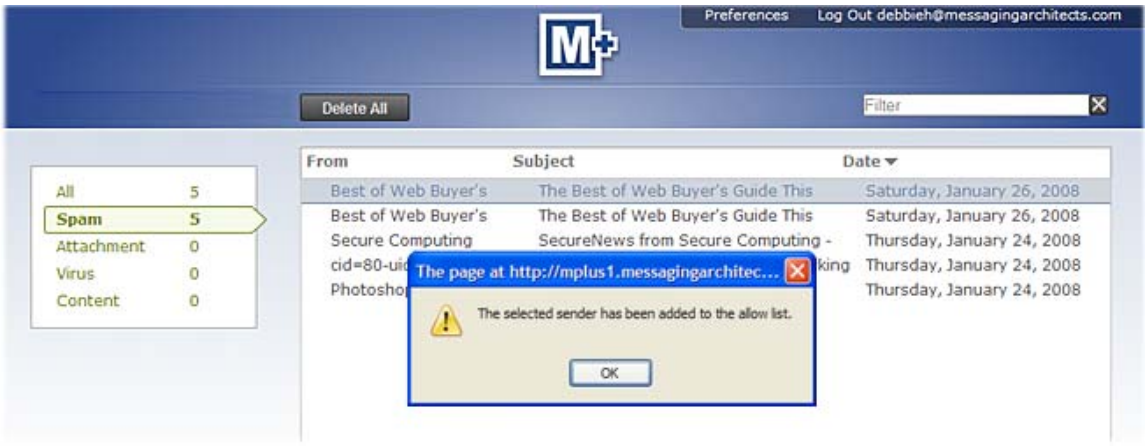


Figure 3-4: M+Quarantine, Allow

3.2.3 Allow Domain

This option allows you to add an entire domain to your Allow List directly from the Spam tab. To add a domain to your Allow List, highlight the message in the list, and click **Allow Domain**. Email from any domain on your Allow List will always be sent to your Inbox.

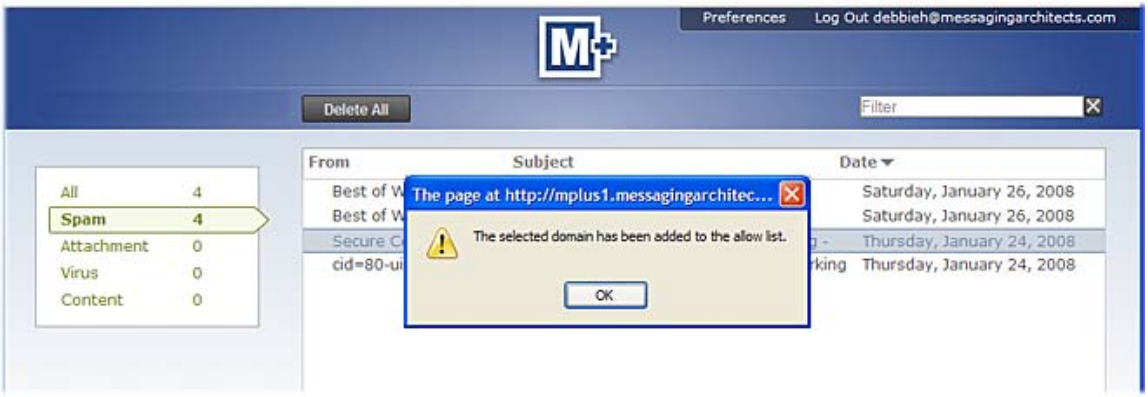


Figure 3-5: M+Quarantine, Allow Domain

3.2.4 View

This option allows you to safely view email directly from any of the navigational tabs. To safely view a message in your quarantine, highlight the message in the list, and click **View**. The message is displayed onscreen. You can then decide what message action you want to take. Use the message actions at the bottom of the message to navigate through messages by clicking **Prev** to view the previous message in the list or **Next** to view the next

message in the list. Other message actions including **Release**, **Allow**, **Block** and **Delete** may also be available, depending on which message category you are viewing.

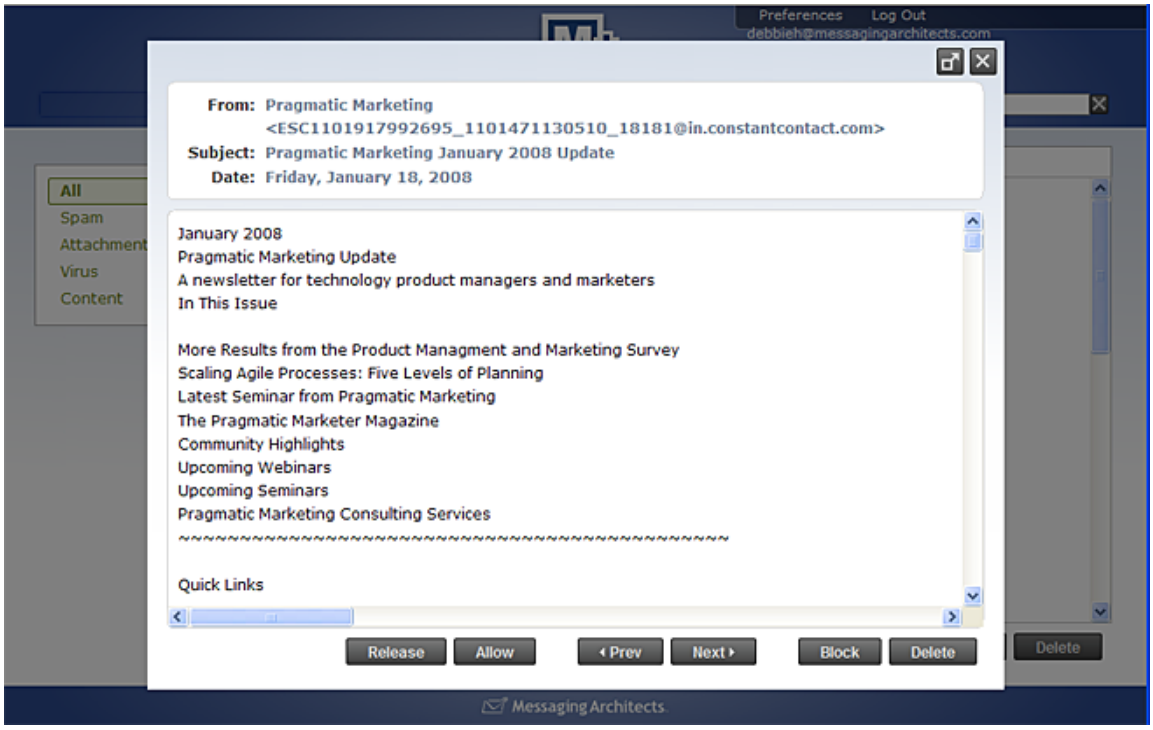


Figure 3-6: M+Quarantine, View Message

To view the message full-screen, click the icon  at the top to message window.

3.2.5 Report

This option allows you to forward a copy of an email message to the system administrator directly from the Spam, Attachment and Content tabs. Occasionally, messages may inadvertently be identified as spam. These messages are known as false positive messages. False positive messages can be released to your Inbox and reported to the system administrator. To report a message to your system administrator, highlight the message in the message list, and click **Report**. The system administrator may then review and report this message as a false positive and update the M+Guardian spam definitions. To reduce the amount of false positive messages you receive, you may also add the email address or domain name to your Allow List so that messages from this source will not be quarantined in future.

You can also use the **Report** option to notify the system administrator that a message containing blocked content or an attachment that you require has been quarantined, so that the system administrator can review and release the message to your Inbox.

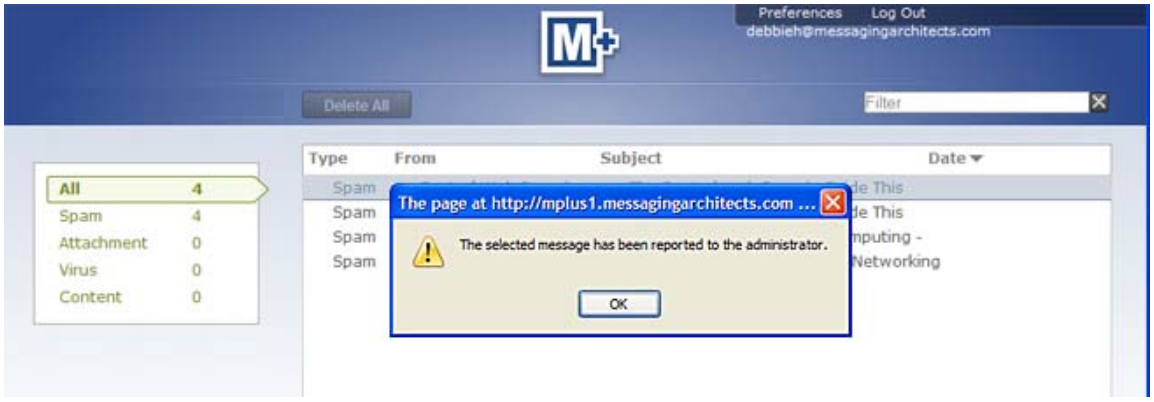


Figure 3-7: M+Quarantine, Report to Administrator

3.2.6 Block

This option allows you to add an email address to your Block List directly from any of the navigational tabs. To add an address to your Block List, highlight the message in the list, and click **Block**. You can add individual email addresses to your Block List, or you can add the entire domain. If you want to add both the email address and the domain to your Block List, choose **Block Domain.** Email from addresses or domains that appear on your Block List will never be sent to your Inbox or to your quarantine.

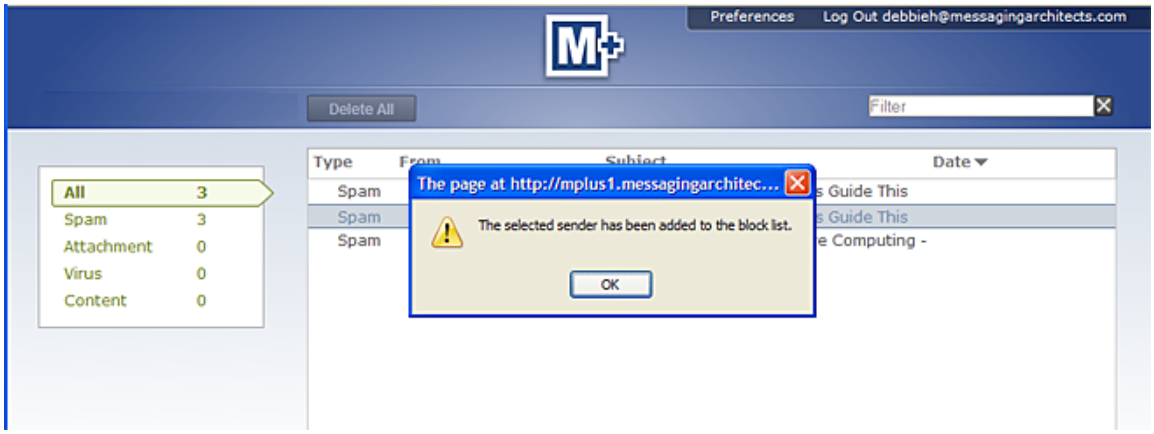


Figure 3-8: M+Quarantine, Add to Block List

3.2.7 Block Domain

This option allows you to add an entire domain to your Block List directly from any of the navigational tabs. To add a domain to your Block List, highlight the message in the list, and click **Block Domain**. Email from any domain on your Block List will never be sent to your Inbox.

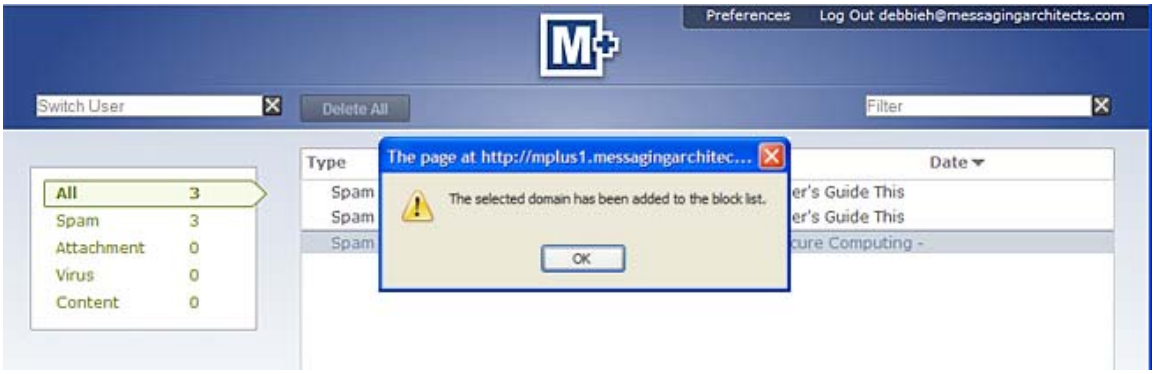


Figure 3-9: M+Quarantine, Block Domain

3.2.8 Delete

This option allows you to delete the message. To delete a message in the message list, highlight the message in the list, and click **Delete**. To delete multiple messages in your message list, use **CTRL+click** or **SHIFT+click** to select the messages you want to delete from your quarantine, and click **Delete**.

3.2.9 Delete All

This option allows you to delete all the email messages in your quarantine with one click of your mouse. The **Delete All** option is available from the **Spam**, **Attachment**, **Virus** and **Content** tabs.

3.3 Reviewing Quarantine Reports

The Quarantine Reports feature of M+Guardian allows system administrators to create policies that automatically send customized Quarantine Reports containing event information to end users in the form of an administrator-sent email message. When new mail is quarantined, M+Guardian automatically sends Quarantine Reports to your mail client. Typically, these reports are sent daily, however you will only receive a Quarantine Report if you have email messages in quarantine at the time M+Guardian generates the reports.

Figure 3-10: Quarantine Report

A Quarantine Report displays information about the email that has been sent to your quarantine since your last report, as well as details about the email that is currently in quarantine.

There are several message actions which you can perform directly from the Quarantine Report.

To perform an action on a quarantined message:

1. Open the email containing your Quarantine Report.
2. Click the hyperlink directly in the Quarantine Report for the message action you want to perform on the quarantined message.
   - **Release** Releases the email message to your Inbox.
   - **Report** Sends a copy of the message to your system administrator for review.
   - **Allow** Add the email address to your Allow List.
   - **Delete** Delete the email from your quarantine.
   - **Allow Domain** Add the domain to your Allow List.
   - **Block** Add the email address to your Block List.
   - **Block Domain** Add the domain to your Block List.

4 Specifying Preferences

With M+Quarantine, you can choose the **Preferences** link located at the top of the M+Quarantine to specify advanced preferences for your quarantine. Use the navigational tabs on the left of the interface to open the corresponding category.

4.1 Policies

The **Policies** tab allows you to choose custom actions for managing and reviewing your quarantined email. Depending on the permissions or user rights you have been granted by the system administrator, some of the following options may not be available to you. To begin choosing custom actions, click the **Policies** tab.

Figure 4-1: M+Quarantine, Options tab

A **Default Action** option may also be available to end users from any of the drop down lists. Messaging Architects provides suggested system defaults that may not have been disabled by the system administrator.

4.1.1 Incoming Spam Action

The Incoming Spam Action option allows you to specify what you want to do when M+Quarantine encounters messages containing spam. If the system administrator has enabled this feature for you, you can use the drop down list to select from the following incoming spam actions:

Allow This option delivers messages containing spam to your mailbox.

Quarantine This option sends messages to your quarantine for review and deletion.

Delete This option deletes messages containing spam.

Add X-SPAM Header Line & Deliver to Mailbox This option adds a spam X-Header to messages and delivers messages containing spam to your mailbox.

Tag Subject & Deliver to Mailbox This option adds custom text to the subject line and delivers messages containing spam to your mailbox.

The names of policies and the text of the actions available to you in the drop down list may vary slightly. The text available here is customized by the system administrator in the M+ Administration Console to implement corporate-wide email security policies.

4.1.2 Outgoing Spam Action

The Outgoing Spam Action option allows you to specify what you want to do if M+Quarantine discovers outgoing messages containing spam in your mailbox. If the system administrator has enabled this feature for you, you can use the drop down list to select from the following outgoing spam actions:

Allow This option delivers messages containing spam to the recipient's mailbox.

Quarantine This option sends messages containing spam to your quarantine for review.

Delete the Message This option deletes messages containing spam.

Add X-SPAM Header Line & Deliver to Mailbox This option adds a spam X-Header to messages and delivers messages containing spam to the recipient's mailbox.

Tag Subject & Deliver to Mailbox This option adds custom text to the subject line and delivers messages containing spam to the recipient's mailbox.

The names of policies and the text of the actions available to you in the drop down list may vary slightly. The text available here is customized by the system administrator in the M+ Administration Console to implement corporate-wide email security policies.

4.1.3 Incoming Virus Action

The Incoming Virus Action option allows you to specify what you want to do when M+Quarantine encounters messages containing viruses. If the system administrator has enabled this feature for you, you can use the drop down list to select from the following incoming virus actions:

Clean This option attempts to clean messages containing viruses before delivery to your mailbox. If a message cannot be cleaned, then the message is automatically deleted.

Delete This option deletes messages containing viruses.

The names of policies and the text of the actions available to you in the drop down list may vary slightly. The text available here is customized by the system administrator in the M+ Administration Console to implement corporate-wide email security policies.

4.1.4 Outgoing Anti-Virus Action

The Outgoing Anti Virus Action option allows you to specify what you want to do if M+Quarantine discovers outgoing messages containing viruses in your mailbox. If the system administrator has enabled this feature for you, you can use the drop down list to select from the following outgoing virus actions:

Clean This option attempts to clean messages containing viruses before delivery to a recipient's mailbox. If a message cannot be cleaned, then the message is automatically deleted.

Delete This option deletes messages containing viruses from your mailbox.

The names of policies and the text of the actions available to you in the drop down list may vary slightly. The text available here is customized by the system administrator in the M+ Administration Console to implement corporate-wide email security policies.

4.1.5 Quarantine Report Action

The Quarantine Report Action option allows you to specify when you want quarantine reports delivered to your mailbox. If the system administrator has enabled this feature for you, you can use the drop down list to select how often you want to receive quarantine reports or if you do not want to receive quarantine reports at all.

Even though you may select to receive a quarantine report every day, or the administrator has elected to send quarantine reports daily, you will only receive a report if you have email messages trapped by the M+Guardian Extreme Email Firewall and quarantined.

4.2 Allow List

The **Allow List** tab allows you to create custom Allow Lists, or manage existing lists. Allow Lists contain domain names and email addresses of senders from whom you always want to receive messages. To create custom Allow Lists, or manage existing lists, click the **Allow List** tab.

Figure 4-2: M+Quarantine, Allow List tab

4.2.1 Allowed Domains and Allowed Addresses

This feature allows you to create custom Allow Lists of domain names and email addresses that should be allowed to bypass the anti-spam scanning engines. Enter either domain names or specific email addresses, and click **Add**. Wildcard entries, such as *@domain.com, are supported.

Allow Lists may only bypass the anti-spam scanning engines if the system administrator has enabled this option for end users in the M+ Administration Console.

4.3 Block List

The **Block List** tab allows you to create custom Block Lists, or manage existing lists. Block Lists contain domain names and email addresses of senders from whom you do **not** want to receive messages. To create custom Block Lists, or manage existing lists, click the **Block List** tab.

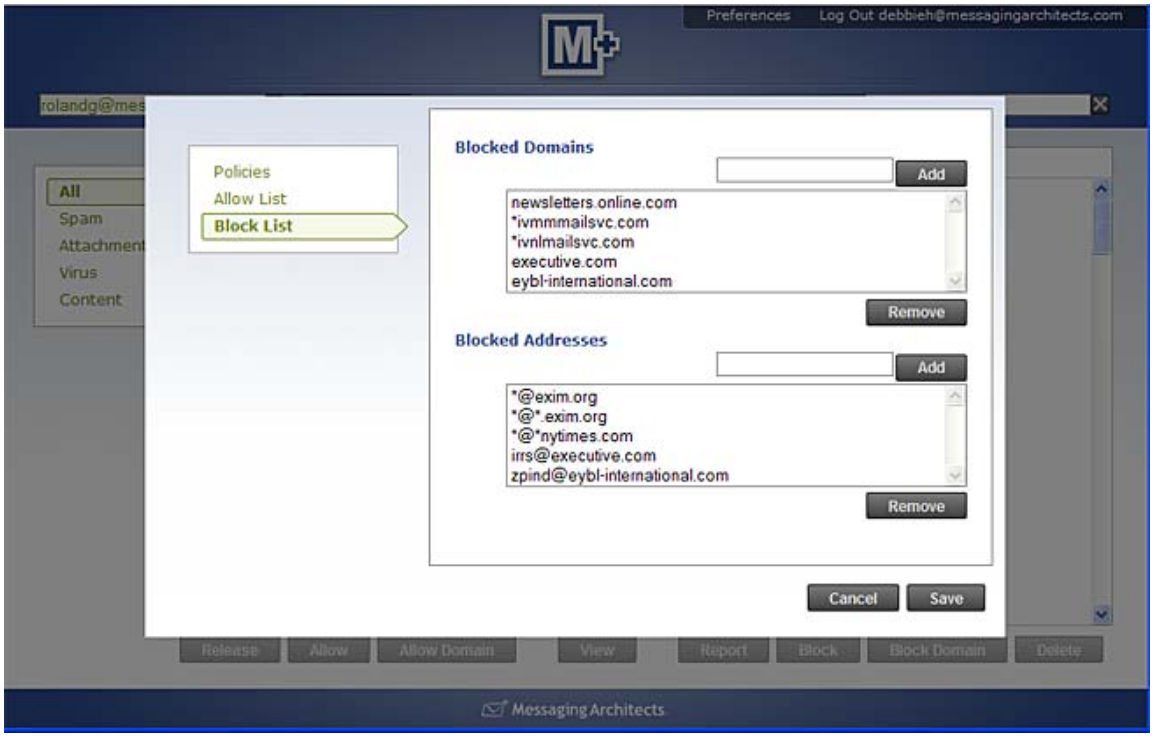


Figure 4-3: M+Quarantine, Block List tab

4.3.1 Blocked Domains and Blocked Addresses

This feature allows you to create custom Block Lists of domain names and email addresses that will be permanently blocked by the M+Guardian Extreme Email Firewall. Email messages from addresses on your Block List will always be blocked, no matter what the content. Enter either domain names or specific email addresses, and click **Add**. Wildcard entries, such as *@domain.com, are supported.

4.3.2 Managing Lists

You can manage existing Allow and Block Lists by selecting or highlighting the domain name or email address in the list and clicking **Remove**.

If you remove entries from your Allow List, email from that domain or email address may be trapped by the anti-spam filter in future. If you remove entries from your Block List, email from that domain or email address may appear in your quarantine in the future.

4.4 Log Out

The **Log Out** link allows you to close the quarantine and log out of the M+Quarantine application.

Appendix A: Accessing Live Quarantine via IMAP

End users can access their live quarantine mailboxes via IMAP by creating a new IMAP account in their mail client and pointing the mail client to the M+Guardian server.

The following procedures describe how to create a new IMAP4 account in Outlook Express, GroupWise and Thunderbird, but these procedures can be modified to create a new IMAP4 or POP3 account in any mail client. Before adding a new IMAP account, you need to know your account name and password, and the name of the incoming and outgoing mail servers. If you do not know this information, contact your system administrator.

To configure Microsoft Outlook Express to access your live quarantine mailbox:

1 Start Outlook Express.

2 If you already have an existing Outlook Express account, click **Tools > Accounts > Add,** then select **Mail** to start the Internet Connection Wizard.

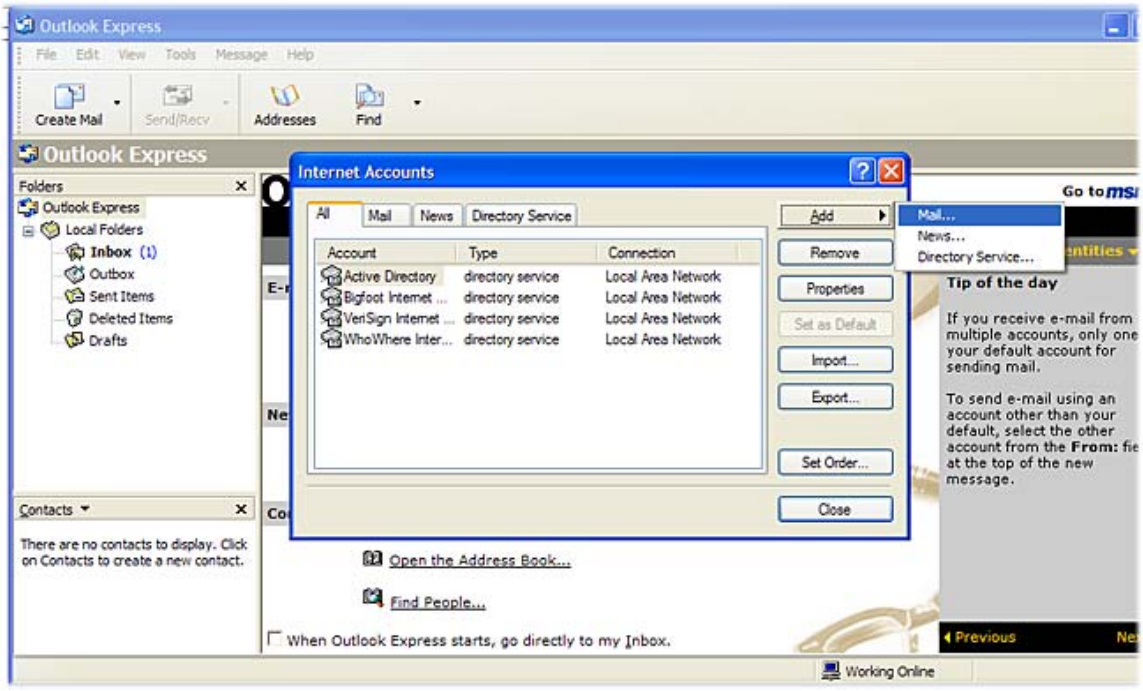


Figure 4-4: Adding an Account

3 The Internet Connection Wizard prompts you for your name.

Figure 4-5: Configuring your Display Name

4 Type your name as you would like it to display on your messages, then click **Next**.

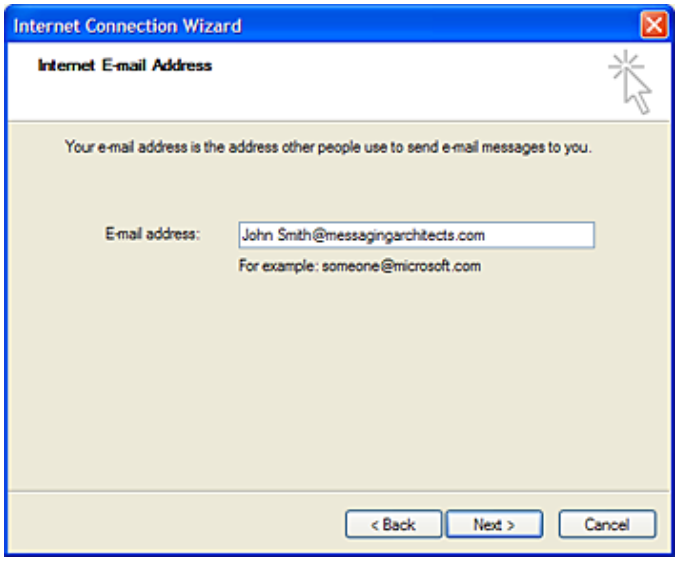


Figure 4-6: Configuring your Email Address

5 Type your email address, then click **Next**.

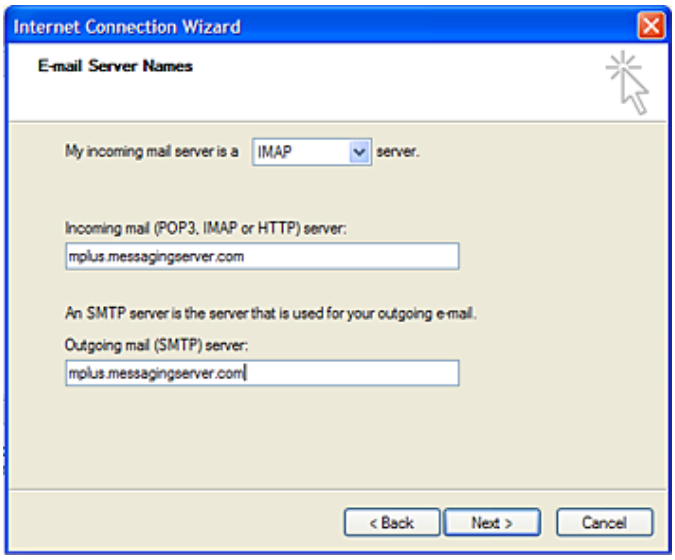


Figure 4-7: Configuring the Incoming and Outgoing Mail Servers

6 From the drop-down list box, select POP3 or IMAP, depending on the agents that are available on your messaging server.

7 In the **Incoming mail server** field, specify the host name of the server where the POP or IMAP Agent is running.

8 In the **Outgoing mail server** field, specify the host name of the server where the SMTP Agent is running, then click **Next**.

Depending on the configuration of your system, the incoming mail server and outgoing mail server can be the same or different messaging servers.

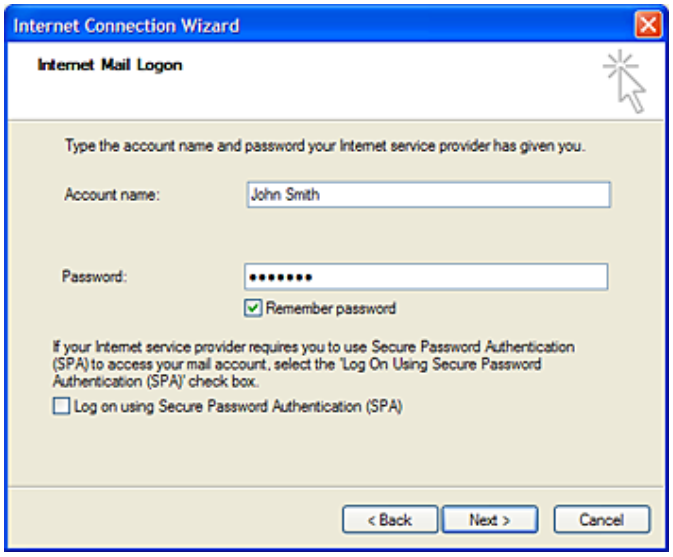


Figure 4-8: Creating an Account

9 Type your POP or IMAP account name and password, then click **Next**.

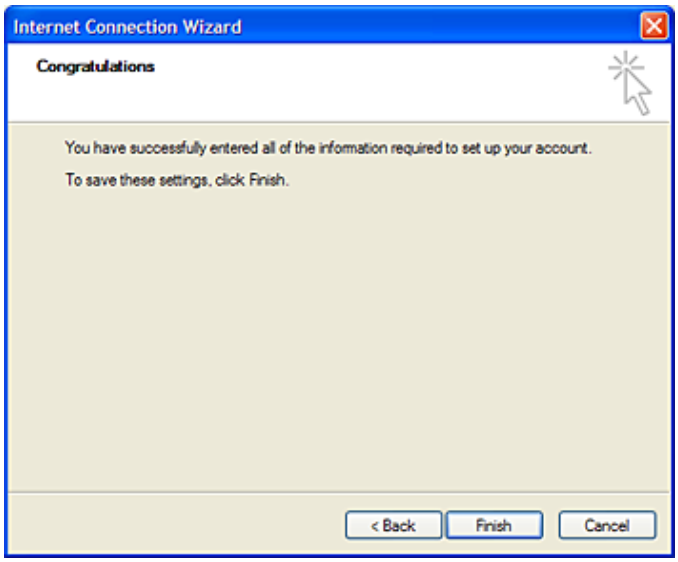


Figure 4-9: Account Setup Complete

10 Click **Finish**.

The folder you created should now be visible in Outlook. The first time you access your live quarantine, you may be prompted to enter the password you regularly use to login to your mail client.

To configure GroupWise to access your live quarantine mailbox:

1 Launch GroupWise mail client.

2 Choose **Accounts > Account Options**.

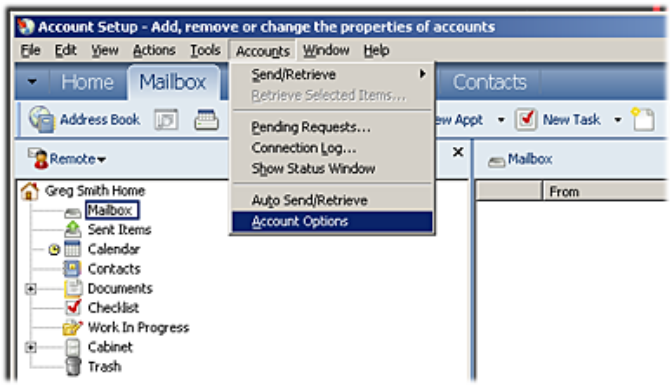


Figure 4-10: Account Options

3 In the **Accounts** dialog box, choose **Add**.

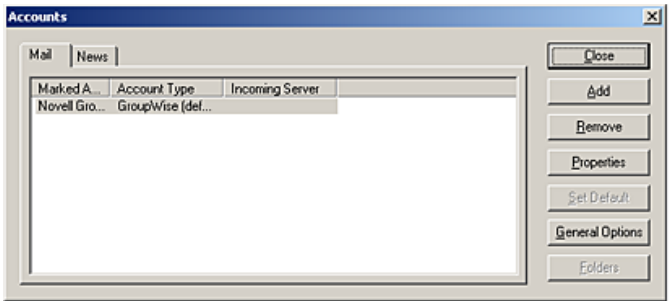


Figure 4-11: Adding an Account

4 In the **Create Account** dialog box, enter a name for your new account, such as M+Quarantine. Under **Account Type,** choose IMAP, and then click **Next**

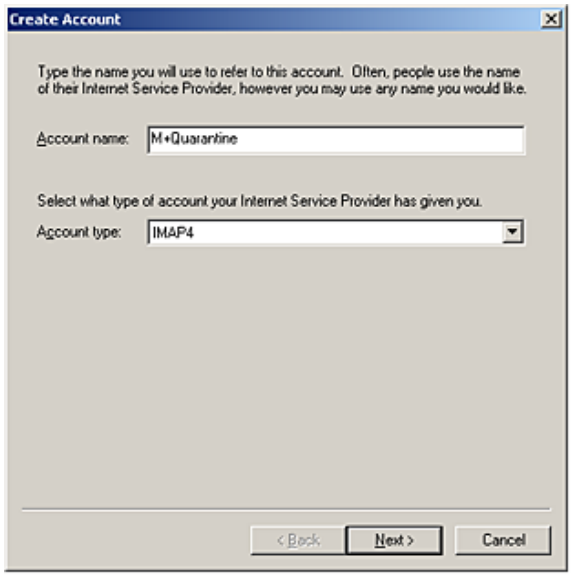


Figure 4-12: Create New Account

5 In the **Create Internet Account** dialog box, enter the following information:

- Under **Incoming mail server**, enter the location of your incoming IMAP mail server, such as mplus.messagingarchitects.com.
- Under **Login name**, enter the login name you use to log in to your mail client and access your GroupWise mailbox, following by your email address, such as maxm@messagingarchitects.com
- Under **Outgoing mail server**, enter the location of your outgoing SMTP mail server, such as mplus.messagingarchitects.com.
- Under **Email address**, enter your email address, such as gsmith@messagingarchitects.com. If this field is already pre-populated for you, make sure that the address that appears in the field is correct.

- Under **From name**, enter a display name, and then click **Next** to continue.

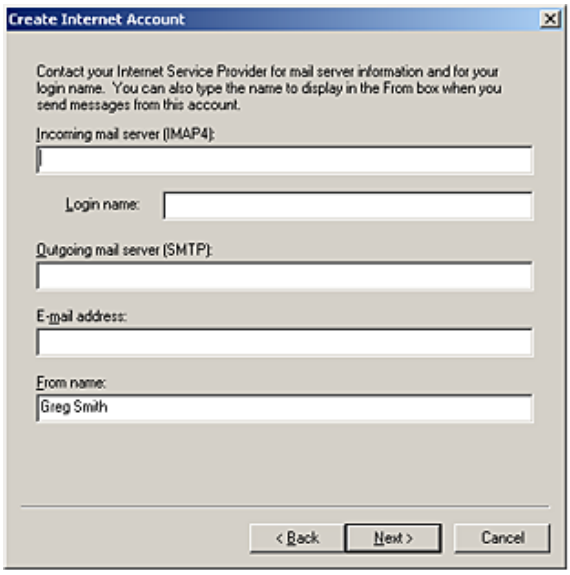


Figure 4-13: Configuring Incoming and Outgoing Mail Server

6 In the **Create Internet Account** dialog box, select the **Connect through my local area network (LAN)** option, and then click **Next**.

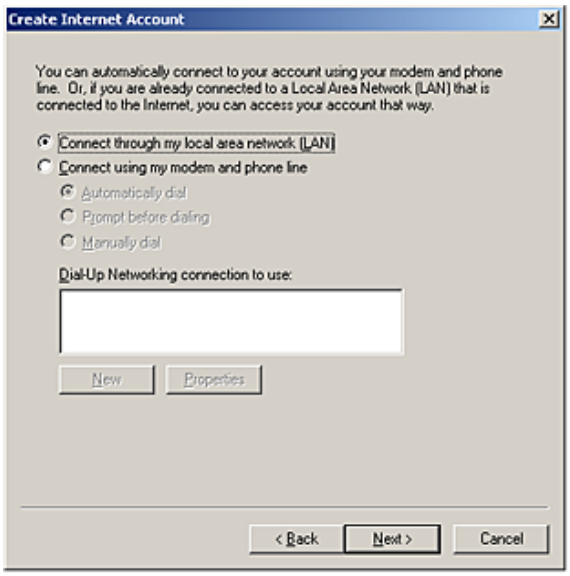


Figure 4-14: Selecting Connection Options

7 In the **Create IMAP folder**, provide a description of your IMAP folder (optional), and then click **Finish**.

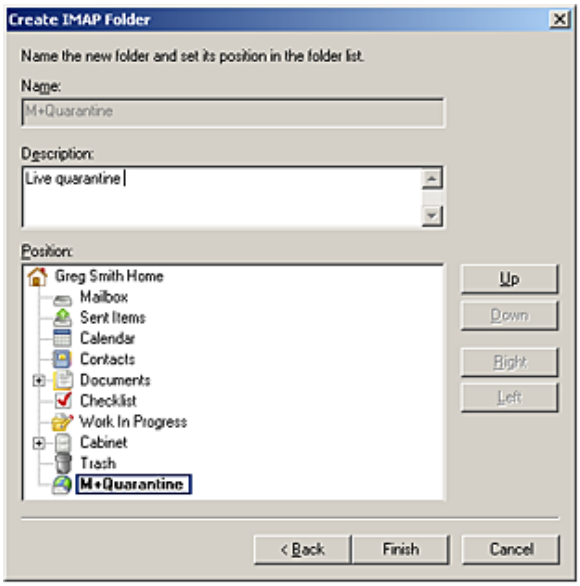


Figure 4-15: Create IMAP Folder

The M+Quarantine folder you created should now be visible in GroupWise. The first time you access your live quarantine, you may be prompted to enter the password you regularly use to login to your mail client.

To configure Mozilla Thunderbird to access your live quarantine:

1. Start your Thunderbird client.
2. Choose **Tools > Account Settings**, and then click **Add Account**.
3. To set up your new accounts, select **Email account**, then click **Next**.

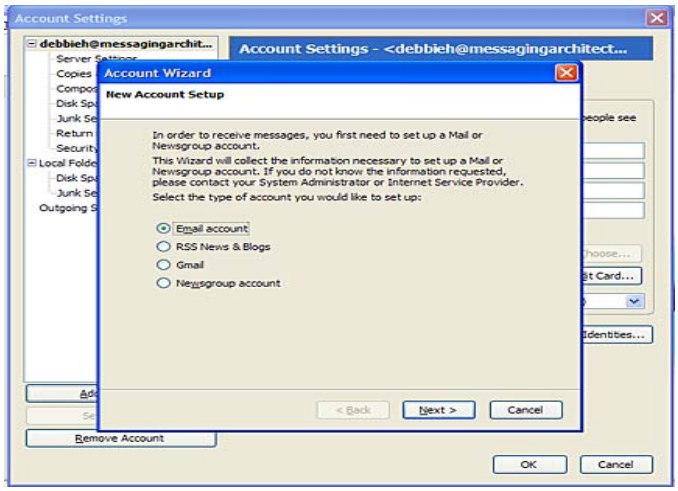


Figure 4-16: Add Account Setup

4. In the **Your Name** field, type your name as you would like it to display on your messages.
5. In the **Email Address** field, enter your email address, and then click **Next**.

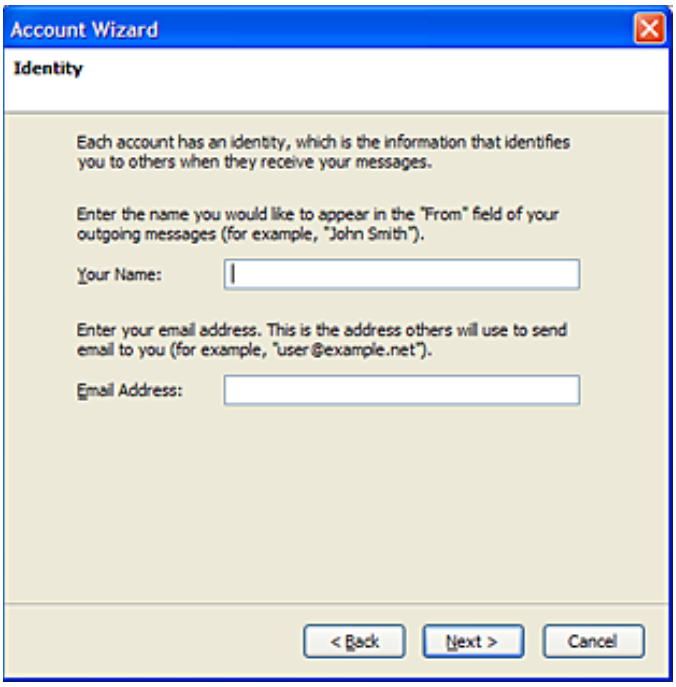


Figure 4-17: Configuring User Settings

6 Select POP3 or IMAP, depending on the agents that are available on your messaging server.

7 In the **Incoming Server** field, specify the host name of the server where the POP or IMAP Agent is running, and then click **Next**.

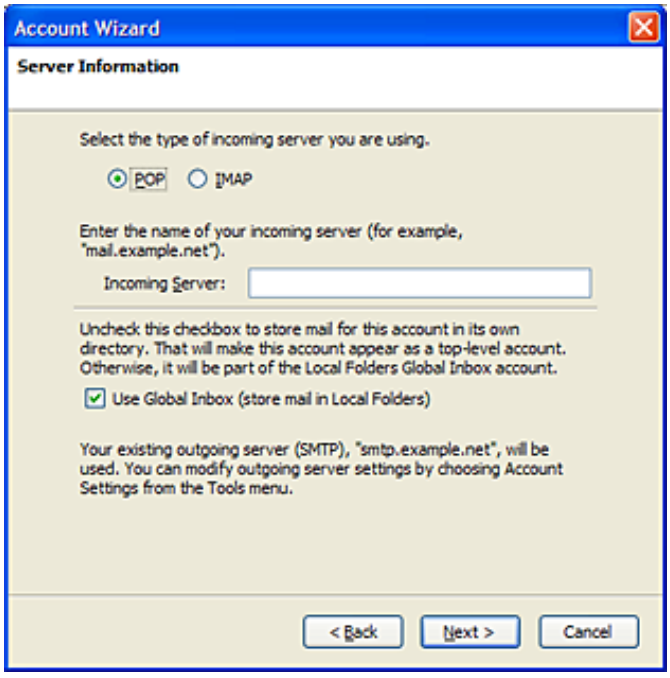


Figure 4-18: Configuring Server Information

8 In the **Incoming User Name** field, enter your incoming user name, and then click **Next**.

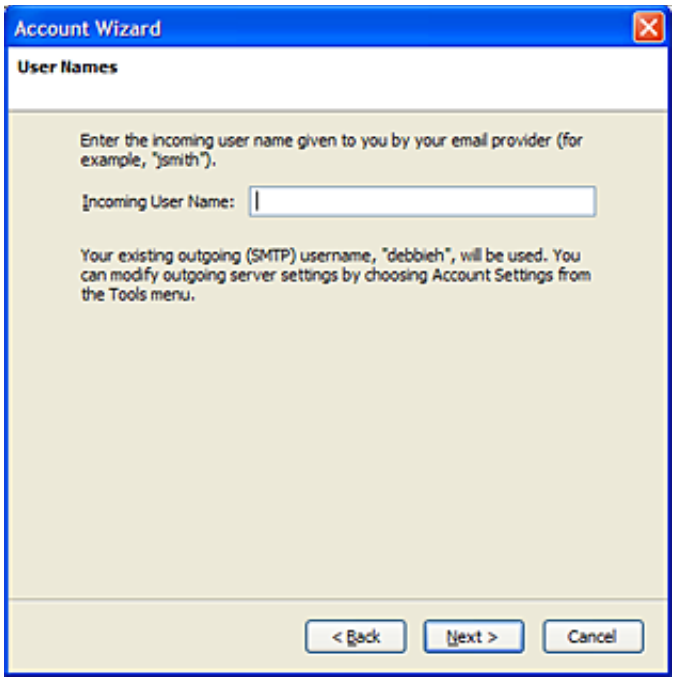


Figure 4-19: Configuring User Names

9 In the **Account Name** field, enter the name of the account, such as M+Quarantine, and then click **Next**.

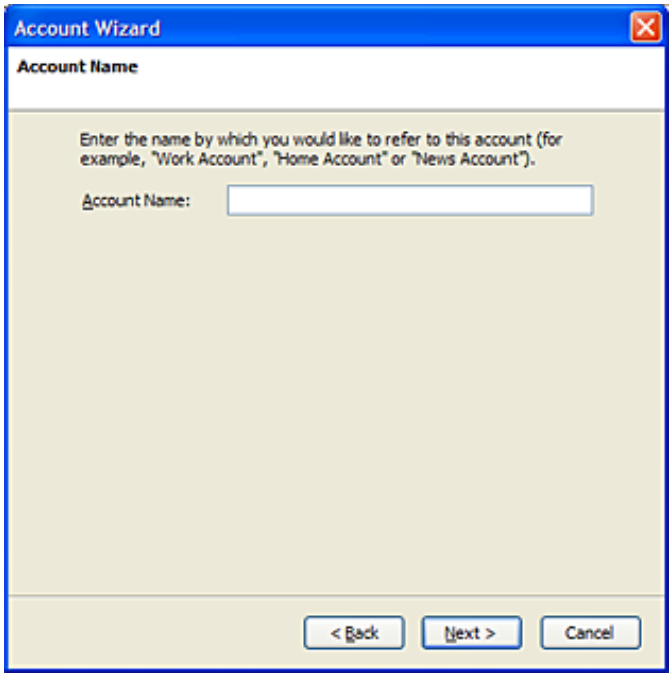


Figure 4-20: Creating Account Name

10 Verify your configuration settings and then click **Finish**.

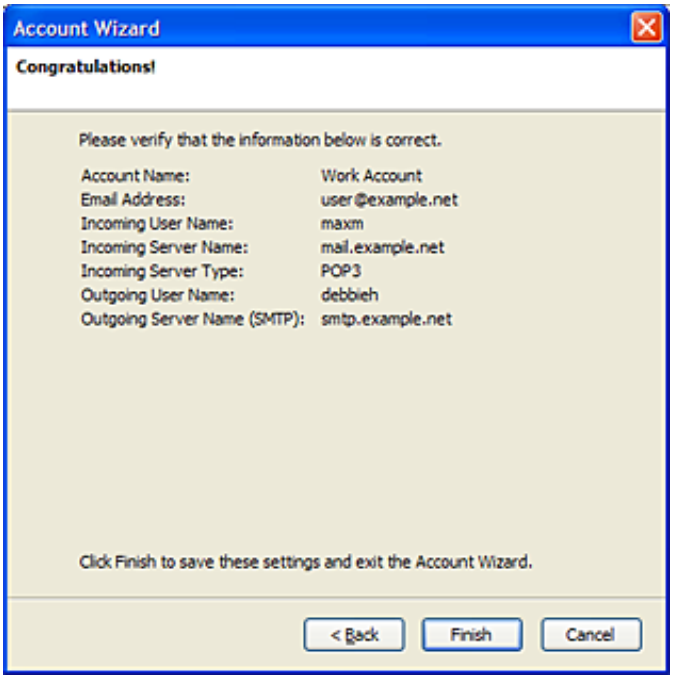


Figure 4-21: Account Wizard Complete

The folder you created should now be visible in Thunderbird. The first time you access your live quarantine, you may be prompted to enter the password you regularly use to login to your mail client.

Glossary

Allow List

Allows end users to designate email addresses and domain names from which all mail will be accepted, even if individual messages earn high spam ratings.

Blocked Attachment

Any file type attached to an email message that is identified as a potential threat.

Block List

Allows end users to designate email addresses and domain names from which no mail will be accepted.

Browser (also Web Browser)

This is a software application that allows you to view (or "browse") and interact with websites on the Internet. Some of the most common web-browsing software applications are Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera and Safari.

Browser Compatibility

The term browser compatibility refers to the fact that web-browsing applications from different companies sometimes display the same web pages with different formatting. This is to say that they interpret the code behind a web page (code which consists of HTML tags) differently. Sometimes these differences are minimal, but unfortunately these interpretational differences can sometimes also mean that you simply cannot view some parts of a website that have used particular HTML code tags because your web browser does not know how to display those parts (which use specific HTML tags).

Content Filtering

Scans plain text for key phrases and/or regular expressions that indicate that the message is spam.

False Negative

A false negative is an email that is spam, but was not identified as spam by the anti-spam scanning engines and was released to your Inbox as legitimate email.

False Positive

A false positive is a legitimate email that was incorrectly identified as spam by the anti-spam scanning engines and withheld from your Inbox.

Quarantine

To quarantine an email message is to isolate an email message suspected of containing a threat such as a virus or a suspicious file attachment so that the message cannot be opened.

Quarantine Report

A quarantine report is an administrator-sent email message that allows end user to see how many email messages containing viruses, spam, blocked attachments or other filtered mail have been withheld from the end user's Inbox. The quarantine report contains a URL link in the body of the email message to allow end users to manage their own quarantined email in the web-based M+Quarantine application.

Server

A computer that runs administrative software (for the purposes of this user guide, a server is a computer on the Internet that runs an email exchange program).

Spam

Unsolicited, unwanted, bulk, commercial e-mail.

URL (Universal or Uniform Resource Locator)

An Internet address used by web browsers for a specific computer or a document (resource).

Index


Messaging
Architects™
BUSINESS DRIVEN EMAIL