

McAfee (formerly MX Logic) Quick Start User's Guide



About McAfee formerly MX Logic

McAfee has acquired MX Logic, a leading global provider of cloud-based email and web security, email archiving, and email continuity services. The MX Logic organization, based in Colorado, will now be known as McAfee SaaS Email & Web Security. This acquisition enables customers to leverage the cloud and enjoy access to a broader set of delivery options, including appliances, software, or in-the-cloud deployments. With an expanded software-as-a-service footprint, McAfee empowers organizations of all sizes to simplify their security architecture. And now, MX Logic customers can rely on McAfee for complete, network-wide security solutions.



Contents

- I. Sign into the Control Console 3
- II. Reset Your Password in the Control Console (Optional) 4
- III. Review a List of Messages in Quarantine (Control Console) 5
- V. Release Email from Quarantine 6
- VI. Delete Email from Quarantine 6
- VII. Add Senders to the Allow List from Quarantine Screen 7
- VIII. Add Senders to the Deny List from Quarantine Screen 7
- IX. Allow or Deny Email from a Sender (Control Console) 8
- X. Add Senders to the Allow or Deny List 8
- XI. Remove Senders from the Allow or Deny List 9
- XII. Save the Allow or Deny List to a File 9
- XIII. Email Continuity 9
- Allow Lists 13
- Yahoo Message Delay Notification 13
- Submitting Spam Messages (that enter your inbox) for Analysis 13
- Outbound Email Limits 13

This comprehensive quick user's guide will provide you with all the steps necessary for getting started with **McAfee formerly MX Logic Ultimate Access Service**.

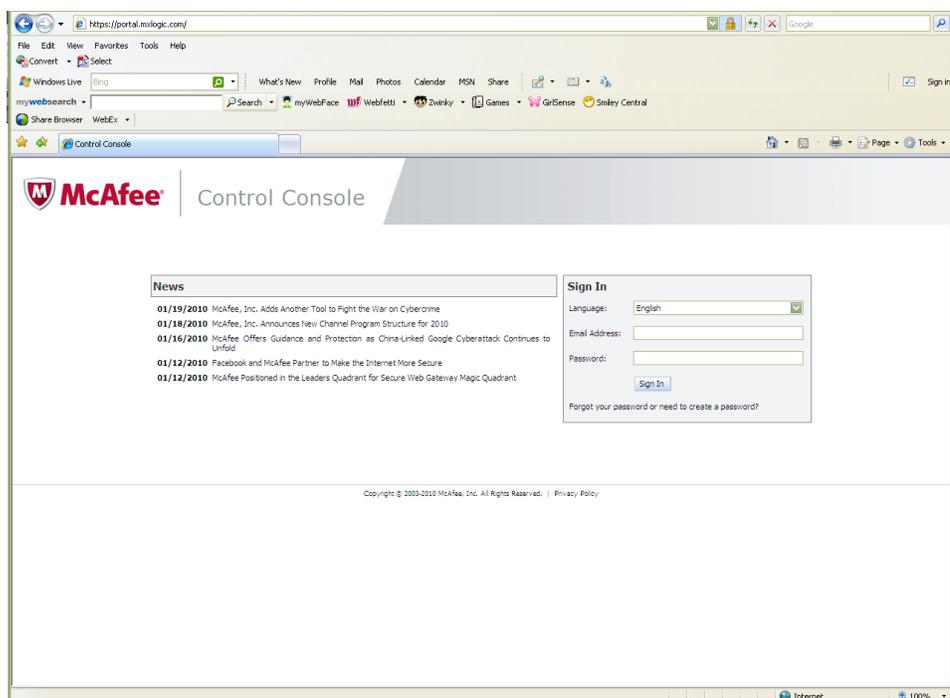
I. Sign into the Control Console

1. Open an Internet browser on your computer and enter the URL or copy and paste URL:
2. <https://portal.mxlogic.com/>
3. Select Language.
4. Enter username: Your email address.
5. Enter password: use the password given to you by your administrator. Initially, your password will be set as password1. *Please note that this password will not be valid until your company's account has been activated.*

(If you do not have a password, see your administrator. If you forgot your password, click the "Forgot your password or need to create a new password?" link and an email will be sent to you with further instructions).

6. Answer Security Question.

(You must answer this question if you forget your password and need to reset it.)

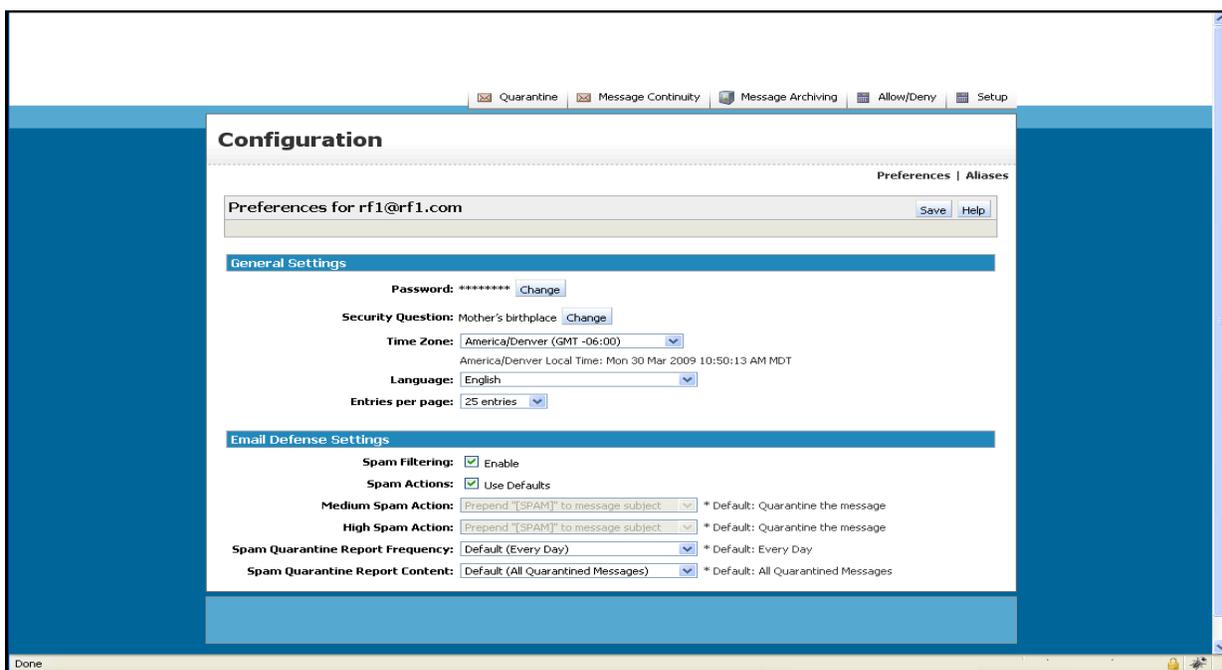


II. Reset Your Password in the Control Console (Optional)

To change your password, perform the following steps:

1. Log into the Control Console or access the Control Console by clicking a link in a Spam Quarantine Report or Spam Quarantine Summary.
2. Click **Setup**.

The Preferences screen is displayed.



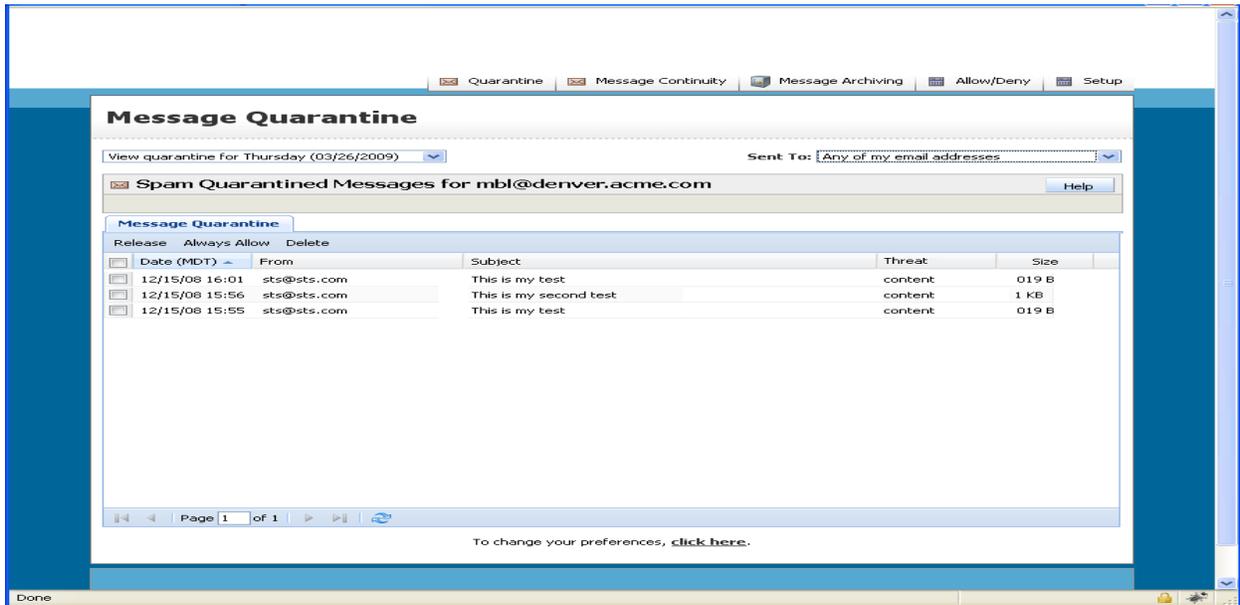
3. Next to the Password field, click **Change**.
The **Password** and **Confirm Password** fields are displayed. Type the new password in the fields.
4. For the **Security Question** field, click **Change** if you need to change the security question or answer. You must answer this question if you forget your password and need to reset it.
The **Security Question** and **Security Answer** fields are displayed. Select a question from the **Security Question** drop-down menu. Type the answer to the question in the **Security Answer** field.
5. Click **Save**.
6. Your password is set. You must use this password the next time you log in to the Control Console.

***Also, on the screen, you can change the frequency of Spam Quarantine Reports sent to your mailbox. In the Email Defense Settings section, select "Spam Quarantine Report Frequency".**



III. Review a List of Messages in Quarantine (Control Console)

When you first log in to the Control Console, the **Message Quarantine** screen is displayed by default. The messages, if any that were quarantined for the current day are displayed.

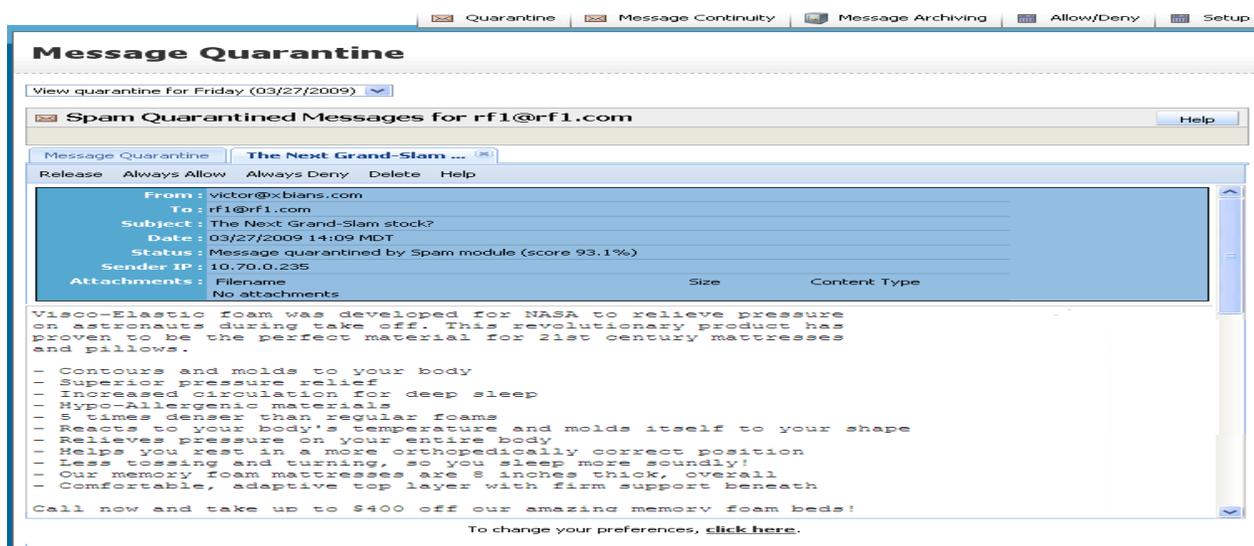


1. From the **View quarantine ...** drop-down menu, select **View all quarantined messages** or select the specific day, from the last week, for which you want to view messages.
2. From the **Sent to** drop-down menu, select **Any of my email addresses** or the specific email address for which you want to view messages.



IV. View Details of a Message

On the Message Quarantine screen, double-click any message you want to view.



V. Release Email from Quarantine

To release one or more emails from quarantine and deliver them to your primary email address, do the following:

1. On the **Message Quarantine** window, select the check box in front of each email that you want to release.
2. Click **Release**.

If the email was originally sent to an alias email address, the email is released to the primary email address. The following message is displayed:

The selected message has been released. It should appear in your Inbox within several minutes.

VI. Delete Email from Quarantine

To delete one or more emails at the same time, do the following:

1. On the **Message Quarantine** window, select the check box in front of each email that you want to delete.
2. Click **Delete**.

VII. Add Senders to the Allow List from Quarantine Screen

You can define lists of senders whose email addresses will always be accepted without spam filtering. However, your EDS Administrator may block emails from addresses in your **Allow** list using other email policy configurations. In this case, you will still not receive emails from these addresses.

To add the senders of one or more emails to your **Allow** list, do the following:

1. On the **Message Quarantine** window, select the check box in front of each email whose sender you want to add to your **Allow** list.
2. Click **Always allow**.

The following message is also displayed:

The sender has been added to your Allowed Senders List and all quarantined messages from the sender have been released.

Note: After completing these steps, all emails received from these senders' email addresses will not be checked for spam content.

VIII. Add Senders to the Deny List from Quarantine Screen

There are two basic definitions of spam that may help you determine whether a sender address should be added to your **Deny** list.

To add the senders of one or more emails to your **Deny** list, do the following:

1. On the **Message Quarantine** window, select the check box in front of each email whose sender you want to add to your **Deny** list.
2. Click **always deny** at the bottom of the window to add these senders' email addresses to your **Deny** list.

The following message is also displayed:

The selected message(s) have been deleted and the sender added to your Denied Senders List.

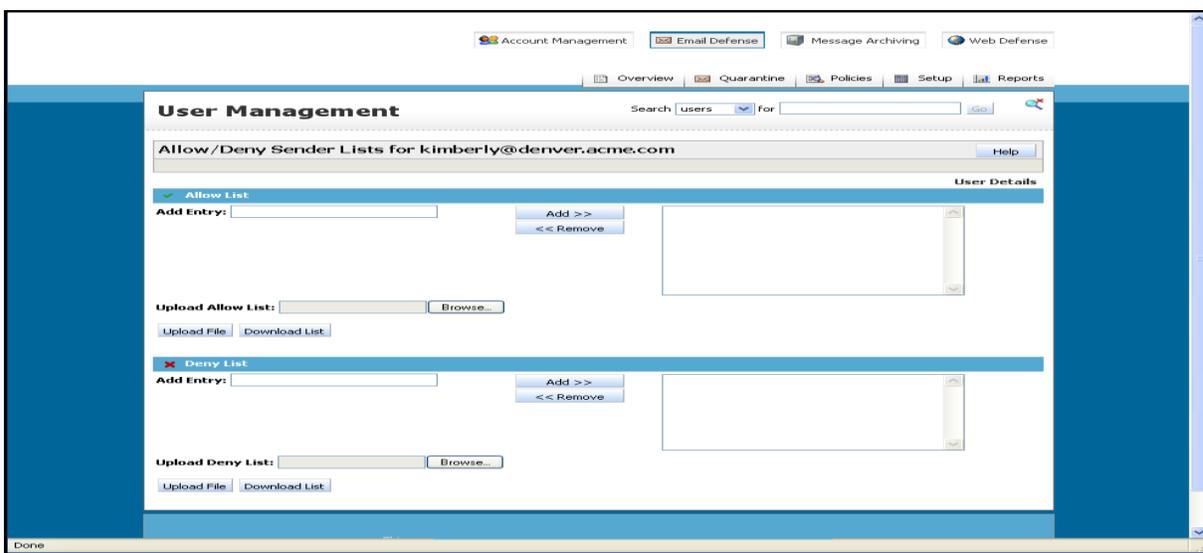
Caution: A common technique of spammers is to change their sender email address often or even hijack an innocent user's email address to send spam. Be aware that your **Deny** list may not prevent future spam emails from these spammers. The **Deny** list primarily is used to block emails from unwanted senders who consistently send from the same address (for example, unwanted sales emails from a known company).

Note: After completing these steps, all emails from these senders' email addresses will never be accepted for delivery. Another term for this process is "blacklisting."



IX. Allow or Deny Email from a Sender (Control Console)

To access your allow/deny sender lists, click the **Allow/Deny** menu option in the Control Console. The **Allow/Deny Sender Lists** screen is displayed.



X. Add Senders to the Allow or Deny List

- In the **Add Entry** field for either the **Allow List** or **Deny List**, type a sender address or domain from which you always want to allow email. You entry can do any of the following:
 - Designate a single email address (for example, "person@abc.com") to force the emails received from just that address to be always or never delivered
 - Designate an entire domain (for example, "abc.com") to force the emails received from all addresses from that domain to be always or never delivered.
 - Use wildcards to enter a range of email address (for example, j*@abc.com to force the emails received from all addresses starting with "j" from that domain to be always or never delivered).
- Click **Add>>** next to that **Add Entry** field.

The email address or domain appears in the list box.



XI. Remove Senders from the Allow or Deny List

This procedure allows you to remove sender addresses from your **Allow** or **Deny** list.

1. On the **Allow/Deny Sender Lists** window, do one of the following:
 - Click to select the sender address in the appropriate list box.
 - Press and hold the <Shift> or <Ctrl> keys while clicking to select multiple email addresses.
2. Click <<**Remove** next to the list box where the sender addresses are selected.

The selected sender addresses disappear from the list box.

XII. Save the Allow or Deny List to a File

This procedure allows to you save the contents your **Allow** or **Deny** list to a spreadsheet file that is in .csv format.

1. On the **Allow/Deny Sender Lists** window, click **Download List** in the appropriate area.

The **File Download** dialog appears.

2. Do one of the following.

Click **Open** to open the spreadsheet application and view the downloaded list. You must have an Excel-compatible spreadsheet application on your computer to use this feature.

Click **Save** to save the downloaded list to a file. The **Save As** dialog appears.

3. On the **Save As** dialog, enter the desired filename and destination and click **Save**.

XIII. Email Continuity

Email Continuity enables Web-based email access, management, and use during planned or unplanned outages. The service retains all inbound and outbound mail sent or received during the outage, and intelligently synchronizes an accurate record of all outage-period message activity with the business email server(s).

The steps outlined below are designed to help you set up and use Message Continuity in the event your email network is down.

Step One: Configure your computer for Email Continuity

1. Enable JavaScript or Active Scripting on your web browser
 - a. If your preferred web browser is Internet Explorer, enable Active Scripting at:

Tools > Internet Options > Security tab > "Custom Level..." button > scroll down to Scripting > Active Scripting > Enable.
 - b. If your preferred Web browser is Mozilla Firefox, enable Java Script at:

Tools > Options > Content > select Enable JavaScript.



2. Configure your browser security settings to Medium. You will be unable to access or use Message Continuity if your security setting is at High.
 - a. Internet Explorer > Tools > Internet Options > Security tab > click the "Default Level" button.
3. Configure the pop-up blocker in your Web browser.
 - a. Internet Explorer:
 Tools > Internet Options > Privacy tab > click the "Settings" button > Filter Level: (choose "Medium: Block most automatic pop-ups" from the drop-down list).
 - b. Mozilla Firefox:
 Tools > Options > Content tab. If "Block pop-up windows" is selected, click the Exceptions button and enter the appropriate address for the Control Console into the website address field and click "Allow" button. [Contact your administrator if you do not know the address.]

Step Two: Access the Control Console

Message Continuity access and use is performed through the Control Console, our Web-based administrative portal. You can access the Control Console by one of the following methods:

Direct Login

Log into the Control Console at the appropriate address. If you do not have a password, or do not remember it, click the password assistance link on the login page. It is important that you determine your password prior to an actual outage, as new or replacement passwords are issued via email. Note: Either Bookmark the Control Console link or add it to your Favorites, for easy access later

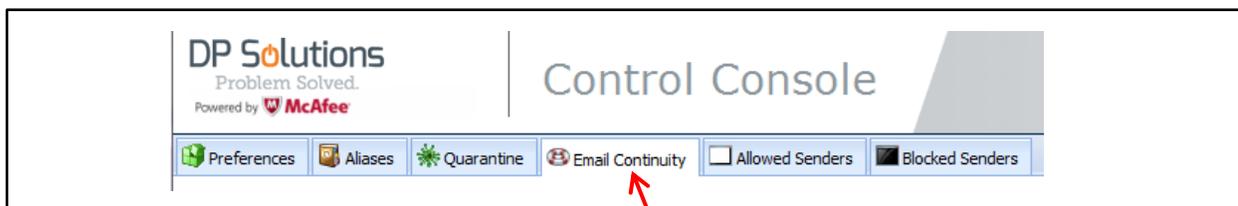
OR

Spam Quarantine Report Link

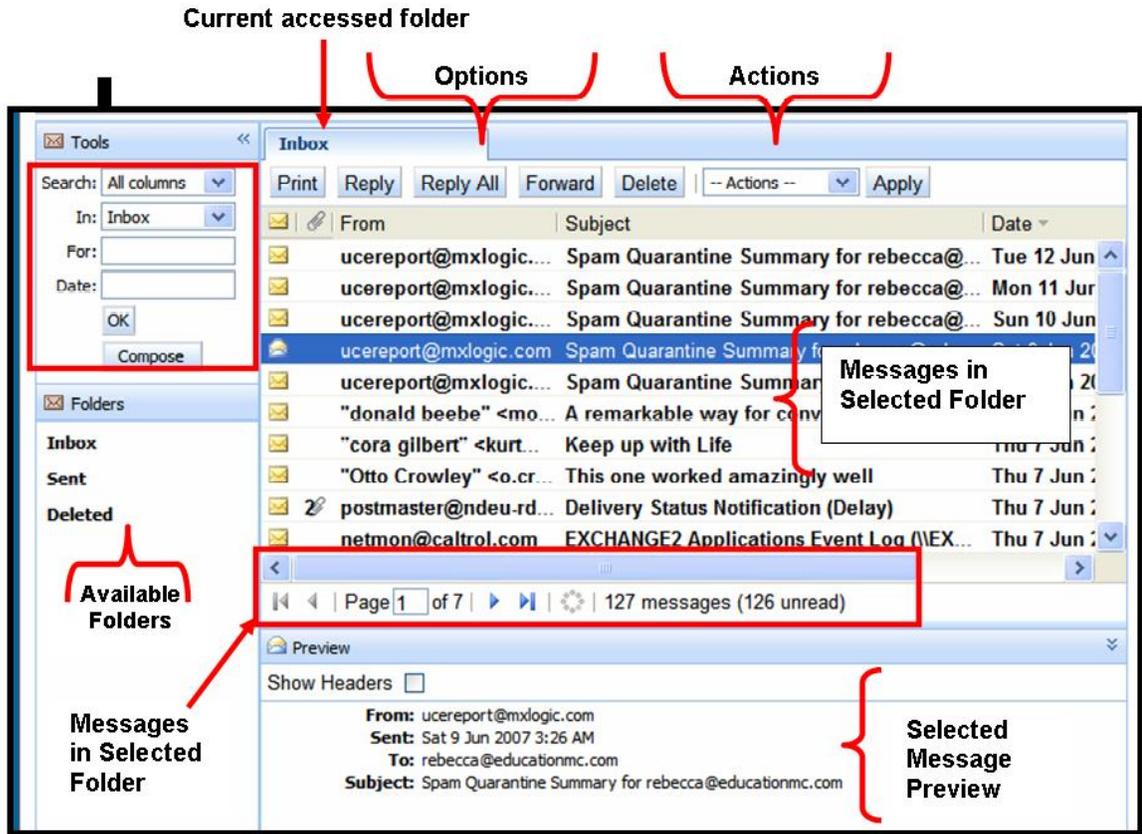
If you receive Spam Quarantine Reports (SQRs) via email from admin@dpsolutions.com, you can enter the portal by clicking on the "View List of All Quarantined Messages" link at the bottom of the Report.

Step Three: Access Email Continuity

Once you have successfully logged into the Control Console, click on the Email Continuity tab:



Email Continuity Screen



Email Continuity Functionality

Available

- Standard email options, including Compose, Print, Reply, Reply All, Forward, Delete.
- Can take Actions on email (select item from drop-down list, then click the "Apply" button). Actions include Mark as Read or Mark as Unread.
- Attach files
- Search messages by From, Subject, or Date columns.

Not Available

- Cannot change your "From:" email address.
- No access to your Global Address List or Personal Contact List. These Distribution Lists are on the corporate server, and during an outage, the corporate server is not available.
- No Spell Check.
- No Drafts Folder.
- No "Check names" functionality to verify email address prior to sending.
- Cannot search for words in the body of a message.

Multiple email addresses

- Must separate multiple email addresses with commas, no spaces after the comma.

Other

- You must enter a fully qualified email address in the "To:" field when composing a new message.
- If you have opened several messages, a tab for each message will appear.
- Messages deleted in Message Continuity are not permanently deleted. Once your email outage is over, all email activity is synchronized with your organization's email server(s), which handles final message disposition.
- Attaching files to messages should be done by using the 'Browse' button to browse to the desired file rather than by typing in the path and filename.



Important Notes

Allow Lists

Do not add your domain to the sender allow list. Doing so will allow spam messages to bypass MX Logic's filters and freely enter your inbox.

Yahoo Message Delay Notification

When sending messages to yahoo.com addresses, you may receive a notification email stating that your message will be temporarily delayed. Please be aware that this occurs due to a Yahoo policy against spammers. Your messages **will** be delivered and do not need to be resent!

Submitting Spam Messages (that enter your inbox) for Analysis

1. Right-Click the Inbox item
2. Click on "Options" (on the menu) , The "Message Options" dialog box opens
3. Towards the bottom of this dialog box you should see "Internet Headers"
4. Click **Ctrl A** and copy the contents of "Internet Headers"
5. Paste each into a new and separate email message and please forward this to noc@dpsolutions.com

Outbound Email Limits

The maximum number of emails allowed from one address is 99 per hour. Any outbound messages sent by any 1 email address exceeding this amount will trigger MX Logic's spammer alert system.

