Email Protection for your account

The Email Protection service works in the cloud to protect your email account from spam, viruses, worms, phishing scams, and fraudulent emails before they ever reach your inbox. When spam is identified, the policies configured for your account determine whether the email is delivered, blocked, or quarantined for further review.

Using the Control Console to manage your account

As an Email Protection user, you can use the Control Console web application to view and manage your quarantined spam, configure your preferences, create allowed and blocked senders lists, and access other optional tools.

- **Preferences** — Configure your Control Console and Email Protection service settings.
- **Aliases** — Add alias email addresses that are associated with your user account.
- **Quarantine** — Review suspicious email messages and decide whether or not they are spam.
- **Email Continuity** — When configured for your account, Email Continuity provides a web-based email client that you can use to send and receive email in the event of an outage.
- **Allowed Senders** — Create a list of email address that are always accepted by the spam filter.
- **Blocked Senders** — Create a list of email addressed that are always denied by the spam filter.
- **Archived Messages** — When configured for your account, copies of your email are stored in an email archive. This tool allows you to search for and view your archived messages. For more information, see the SaaS Email Archiving User Guide.
Accessing the Control Console

Sign into the Control Console
The Control Console is the primary user interface with which you manage your quarantined email, email encryption, Web Protection display settings, and Email Archiving. You can manage quarantined messages by clicking the links in quarantine messages you receive, but to manage any other aspects of your account, you must sign in.

The first time you try to access the Control Console, you must define a password that you will use thereafter to sign in or use one of the following:

- Your corporate network password
- A password given to you by your administrator because some other form of remote authentication is being used

After you have signed into the Control Console, you can change your password at any time.

Task
1. Open a browser on your computer and enter the URL for the Control Console.
   If you don’t have the URL, contact your administrator.

2. On the Control Console Sign in page, from the Language drop-down list, select a language in which you wish to view the Sign in page and receive your Spam Report emails.

3. Enter your email address and password.
   - If you don’t have the email address you should enter, contact your administrator.
   - If you don’t have a password, click the Forgot your password or need to create a password? link.

   If you make five consecutive unsuccessful attempts to log in within a 30-minute period, your account is locked. In this case, you can wait 30 minutes and try to log in again. You can also reset your password or contact your administrator to reset your password immediately.

4. Click Sign in.
   If you have not previously entered an answer to a security question, the Security Question page is displayed.

   The answer to the security question is used to validate you, the user, if you forget your password and request a reminder or reset. If you don’t answer a security question, this page appears the next time you log in. You can later change your security question and/or security answer on the Preferences page of your user account.

5. Select a security question and type the answer. Your answer is not case sensitive.

6. Click OK.
   The Message Quarantine page of the Control Console is displayed.

Reset your password from the Sign in page
If you forget your password or want to reset it as a precaution, you can do so from the Sign In page.

This capability might not be available if your company’s login authentication process uses a central password repository with LDAP, IMAP, or POP3 programs.
**Task**

1. On the Sign in page, click the **Forgot your password or need to create a password?** link.

   The **Change Password** page is displayed.

2. In the **Username** field, type your email address.

3. Select **Email password information to me**.
   - If you don’t have the email address you should enter, contact your administrator.
   - If you don’t have a password, click the **Forgot your password or need to create a password?** link.

   If you make five consecutive unsuccessful attempts to log in within a 30-minute period, your
   account is locked. In this case, you can wait 30 minutes and try to log in again. You can also reset
   your password or contact your administrator to reset your password immediately.

4. Click **Next**.

   You will receive an email momentarily with the subject line **Control Console Login Information**. Continue
   with step 5.

5. Open the email message.

6. Click the link in the email. The link is active for only a limited time after the email is sent (typically
   60 minutes). If the link expires, you must repeat this procedure starting at step 1.

7. If you previously selected a security question, the security question is displayed. If you had not
   previously selected a security question, select a question from the **Security Question** drop-down list.

8. In the **Security Answer** field, type the answer to the question.

9. If you need to change the security question or answer, click **Change** by the **Security Question** field. 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 list.

10. In the **Password** field, type a password.

    The password must comply with the following rules:
    - Length must be a minimum of eight characters.
    - Alpha, numeric, and special character types are allowed.
    - There must be at least one character that differs in character type (alpha, numeric, or special)
      from the majority of characters. Thus, if the password contains mostly alpha characters, then at
      least one character must be either a special character or numeric. For example, **majordude** is
      invalid, but **majordude9** is valid.
    - Spaces are not allowed.
    - Passwords are case sensitive (for example, **Password**, **password**, and **PASSword** would be
        different passwords).
Reset your password in the Control Console

After you access the Control Console, you can change your password without receiving an email.

This capability might not be available if your company’s authentication process uses a central password repository with LDAP, IMAP, or POP3 programs. In addition, your service might be administered so that users cannot change their password.

Task

1. Click Preferences.

2. From the Time Zone drop-down list, select your time zone.

3. Next to the Password field, click Change.

   The Password and Confirm Password fields are displayed. Type the new password in the fields.

4. If you need to change the security question or answer, click Change by the Security Question field. You must answer this question if you forget your password and need to reset it.

   The Security Question and Security Answer fields are displayed.
   - From the Security Question drop-down list, select a question.
   - In the Security Answer field, type an answer.

   Select a question from the Security Question drop-down list. Type the answer to the question in the Security Answer field.

5. Click Apply.

   Your password is set. You must use this password the next time you sign in to the Control Console.

Setting preferences

Set your time zone, language, and entries per page

In the Preferences tab, you can use the options under general settings to configure your default time zone and language. You can also configure the number of items you see per page in list views throughout the Control Console.

Task

For option definitions, click Help in the interface.

1. Select Preferences.

2. From the Time Zone drop-down list, select a location or city near you.

   Each time zone in the list shows the time offset from Greenwich Mean Time (GMT). For example GMT -07:00 indicates that the time zone is seven hours behind GMT.

Spam Reports and processed emails use the time zone of the data center where Email Protection is running instead of your local time zone. As a result, your Spam Reports can contain timestamp information that doesn't match the time zone you select here. For example, an email sent on Tuesday from Japan to New York is processed and quarantined in Denver where it is still late on Monday. This email is included in Monday’s spam report even though the original activity took place on Tuesday.
3. From the Language drop-down list, select a language.

4. From the Entries Per Page drop-down list, select a value.

5. Click Apply to save your settings.

**Manage email filters and spam reporting**

You can use the Preferences page to change some aspects of your email spam filtering and spam reporting.

- Some Email Protection features are optional and may be unavailable if your Email Protection Administrator disabled them.

- These settings affect all your associated email addresses, including your primary address and all alias email addresses.

**Task**

For option definitions, click Help in the interface.

1. Click Preferences.

2. Complete the fields in the Email Protection section.

3. Click Apply.

**Schedule spam reports**

Use the schedule and frequency options in the Preferences tab to schedule the delivery of spam reports.

**Task**

For option definitions, click Help in the interface.

1. Select the Preferences tab.

   - Administrators can select My Account | Preferences.

2. Under Email Protection Settings, complete the scheduling options for spam reports.
   - Schedule and Frequency — Deselect Use policy defaults.
   - Frequency — Select one or more days of the week.
   - Deliver reports by — Select the time of day for Report 1 and Report 2.

   - Select Skip if you do not want to receive a report.

3. Click Apply.

**Preferences tab**

The Preferences tab allows you to configure settings for your account including the default time zone, display language, and the number of entries per page. You can also configure settings for specific application features including spam filtering and spam reporting.

- Some features may be unavailable if your administrator disabled them.

- These settings affect all your associated email addresses, including your primary and all alias addresses.
### Table 1 Preferences tab field descriptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Password** | While a user can change his or her own password, only a Customer Administrator can set the password of another user. In addition, the ability to change passwords might not be available if:  
  - Your company authentication process uses a central password repository.  
  - Your service is administered so that the ability to change passwords is unavailable.  
  If you use remote LDAP, IMAP, or POP3 authentication for users, the password you reset will normally be replaced with the password on the authentication server the next time the Control Console synchronizes with that server. However, if the user is a Customer Administrator or Domain Administrator, and that user is not also defined in the authentication server, the authentication synchronization will not affect the password you reset for that user.  
  At the Password field, click Change.  
  Type a new password in the Password field.  
  Type a new password in the Confirm Password field.  
  Password rules are the following:  
  - There must be a minimum of eight characters.  
  - Alpha, numeric, and special character types are allowed.  
  - There must be at least one character that differs in character type (alpha, numeric, or special) from the majority of characters. Thus, if the password contains mostly alpha characters, then at least one character must be either a special character or numeric. For example, majordude is invalid, but majordude9 is valid.  
  - The password cannot contain any spaces.  
  - Both uppercase and lowercase letters are allowed.  
  - Passwords are case sensitive (for example, Password, password, and PASSword would be different passwords)  
  - Any of the following symbols are allowed: ( ) ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / |
| **Security Question** | You must answer the security question if you forget your password and need to reset it.  
  The Security Question field is displayed only when you are setting the preferences of your own account. To change the security question or answer, click Change.  
  The Security Question and Security Answer fields are displayed.  
  Select a question from the Security Question drop-down list. Type the answer to the question in the Security Answer field.                                                                                                                                                                                                                                                                                                                                                                           |
| **Time Zone** | You can designate the time zone that is used to time stamp the page display when you sign on to the Control Console.  
  **Note:** The time and date of your Spam Reports and the processed emails will be controlled by the time zone designated by the data center where Email Protection is running. If the time zone that you designate in this field differs from the data center, you may have to select a date different from your current local date in the Control Console to view the data. For example, if your local time zone is 7 hours behind of the time zone of the data center, you may have to select the next day ("tomorrow") in the calendar to view additional emails that may be on your Message Quarantine page. This would be necessary because the data center will roll to the next day 7 hours before your local time. During that 7 hours, the emails processed by the data center will be posted to "tomorrow" relative to your local time and date.  
  Alternatively, you can select to view all the emails and thus see all quarantined emails on the Message Quarantine page.                                                                                                                                                                                                 |
### Table 1  Preferences tab field descriptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Language | This option allows you to select the language in which you want your Spam Report to display. There are eighteen language options:  
- English  
- French  
- German  
- Italian  
- Japanese  
- Spanish  
- Chinese Simplified  
- Chinese Traditional  
- Korean  
- Brazilian Portuguese  
- Dutch  
- Danish  
- Finnish  
- Norwegian  
- Portuguese  
- Swedish  
- Russian  
- Turkish |

| Entries Per Page | From the Entries per page drop-down list, select the number of items to be displayed in lists on the Control Console, for example, quarantined email lists for users and Email Protection log reports for administrators.  
The default list length is 25. |

### Table 2  Email Protection Settings field definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Filtering</td>
<td>Select Enable to filter your messages for spam.</td>
</tr>
</tbody>
</table>
| Spam Actions | • Select Use policy defaults to use the default spam actions.  
• Deselect to customize Medium Spam, High Spam, and Graymail Spam actions. |
| Medium Spam Action | Specifies the default action for spam messages that have a medium likelihood.  
- Prepend "[SPAM]" to message subject — The subject line of the email has the phrase "[SPAM]" added to the beginning of the subject text and the email is sent to you.  
- Quarantine the message — The email is added to your spam quarantine and is not sent to you. The email is reported in your Spam Report.  
- Deny delivery — The email is blocked automatically.  
- Do nothing — The email is forwarded to you with no processing applied. |
| High Spam Action | Specifies the default action for spam messages that have a high likelihood.  
- Prepend "[SPAM]" to message subject — The subject line of the email has the phrase "[SPAM]" added to the beginning of the subject text and the email is sent to you.  
- Quarantine the message — The email is added to your spam quarantine and is not sent to you. The email is reported in your Spam Report.  
- Deny delivery — The email is blocked automatically.  
- Do nothing — The email is forwarded to you with no processing applied. |
### Table 2  Email Protection Settings field definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graymail Spam Action</td>
<td>Specifies the default action for graymail spam messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tag subject with [GRAYMAIL]</strong> — The subject line of the email has the phrase &quot;[GRAYMAIL]&quot; added to the beginning of the subject text and the email is sent to you.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quarantine the message</strong> — The email is added to your spam quarantine and is not sent to you. The email is reported in your Spam Report.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deny delivery</strong> — The email is blocked automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do nothing</strong> — The email is forwarded to you with no processing applied.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow</strong> — Always allow graymail messages.</td>
</tr>
<tr>
<td>Spam Report</td>
<td>Select <strong>Enable</strong> to receive spam reports.</td>
</tr>
<tr>
<td>Schedule and Frequency</td>
<td>• Select <strong>Use policy defaults</strong> to use the default spam report settings.</td>
</tr>
<tr>
<td></td>
<td>• Deselect to customize <strong>Frequency</strong> and <strong>Deliver reports by</strong> settings for spam reports.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Specifies how often you receive spam reports. Select on or more days of the week.</td>
</tr>
<tr>
<td>Deliver Reports by</td>
<td>Specifies the time of day you would like to receive your reports. You have the option of receiving one or two reports per day.</td>
</tr>
<tr>
<td>Format</td>
<td>Specifies the format of the email, <strong>Plain text</strong> or <strong>HTML</strong>.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the content of the report:</td>
</tr>
<tr>
<td></td>
<td>• <strong>New items since last report</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>All quarantined items</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Summary</strong></td>
</tr>
<tr>
<td>Spam Report Alternate Delivery Address</td>
<td>Specifies an alternate email address that allows you to forward your Spam Report to a different address. The address must be provisioned in the system within one of your domains.</td>
</tr>
</tbody>
</table>

**Forwarding your Spam Report allows the recipient to have full access to your Control Console account. Be sure to use a trusted address.**

### Table 3  Email Encryption Settings field definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Delivery Method</td>
<td>From the drop-down list, select an option for delivering encrypted mail:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Encryption Console</strong>: Store encrypted message content on encryption server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>My Inbox</strong>: Store encrypted message content in email client.</td>
</tr>
</tbody>
</table>

### Table 4  Preferences tab toolbar options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
<td>Click <strong>Apply</strong> to save your changes.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click <strong>Reset</strong> to undo changes and restore your previously saved settings.</td>
</tr>
</tbody>
</table>
The **Aliases** tab allows you to configure alias email addresses that are associated with your user account.

The purpose of alias email addresses is the following:

- Consolidate emails received for multiple addresses into a single set of quarantine areas (Virus, Spam, Content, and Attachments)
- Have a single Spam Report sent to the user for all quarantined spam emails. The Spam Report and any emails released from any quarantine are sent to the primary email address
- Have the emails received for the alias email addresses be filtered using the same configurations defined for the primary email address

If the domain has alias domain names associated with it, additional alias email addresses using the prefix from the new alias email address will be created automatically for all the alias domain names. These additional alias email addresses cannot be edited individually and can be deleted only by deleting the relevant alias domain name from the domain.

If an existing user account is defined as an alias email address, the user-level configurations for the existing user account will be deleted after the changes are saved in this window (for example, user-level policy configurations, **Allowed Sender** list and **Blocked Sender** list, etc.). Quarantine data for the existing user account will be merged into the quarantine data for the primary email address to which it is being associated as an alias email address. Thereafter, the new alias email address will use the configurations defined for the primary email address.

If your role is as a User, Enterprise Domain Administrator, Quarantine Manager or Reports Manager, you cannot configure alias email addresses for other users.

**Add alias addresses**

To allow the Control Console to apply protection or archiving services to an alias email address, you must add the alias address to the Control Console and associate it with your primary email address. Up to five aliases can be created per user, depending on your company’s configuration.

> If your company is using Intelligent Routing, you can also enter public domain addresses.

**Task**

1. Click **Aliases**.

2. In the **User Alias Address** section, in the blank field that is followed by the @ sign and domain name, type the user’s handle, or name, portion of the alias address.

3. From the drop-down list that follows the **User Alias Address** field, select the domain of the user address.

4. Click **New**.
   - The address is listed in the **User Alias Address** section.

5. Click **Apply**.
The address is listed in the Domain Alias section for the primary domain and for any domain aliases that might be defined.

- An authorization email is sent to the added alias email address. The email contains a hyperlink, *I authorize this request*, that you must click to authorize the use of the alias email address. This step confirms that you have the right to change the email address to be associated as an alias to your primary email address.

- After the link is clicked in the authorization email, you are returned to the Aliases tab in the Control Console. The alias email address is authorized and associated with the primary email address. If the alias email address had previously been a primary email address, its user configurations are discarded and the new primary email address configurations are applied.

- Thereafter, the alias email address’ quarantine information will be combined with the primary email address and it will be controlled by the user configuration for the primary email address.

- Your configuration settings (for example, allow and deny lists) are transferred to the selected primary email address. The Spam Quarantine Report and any emails released from quarantine will be sent to the primary email address.

Delete an alias address

Delete an alias address that has been deleted from your email server or is no longer in use.

You cannot delete a primary email address or an alias domain email address that was created automatically when an alias domain name was defined.

If the email address that you want to delete is the primary email address, you must convert the primary address to an alias email address first.

Task

1. Click Aliases.

2. Select the Delete checkbox next to the alias email address that you want to delete.

3. Click Apply.

The alias email address is deleted immediately. Email Protection also removes the alias address’s association with the primary email address. However, if you continue to receive email to the deleted address, Email Protection might recreate the email address as a primary email address with default user configurations, depending on system configurations.

Quarantine

The quarantine feature in Email Protection allows you to review suspicious email messages and determine whether or not they are spam.
Message Quarantine window

The Message Quarantine window lists all of the quarantined spam messages for the account of the user currently logged on.

Table 5 Message Quarantine option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;View all quarantined messages&quot;</td>
<td>Specifies the date range for messages displayed in the Message Quarantine tab. Select to view messages for a specific day.</td>
</tr>
<tr>
<td>Sent To:</td>
<td>Specifies the email addresses displayed in the Message Quarantine tab.</td>
</tr>
<tr>
<td>Release</td>
<td>Click to release the selected messages.</td>
</tr>
<tr>
<td>Always Allow</td>
<td>Click to add the selected senders to the Allow list and release the messages (applies to spam messages only).</td>
</tr>
<tr>
<td>Always Deny</td>
<td>Click to block the selected senders.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete the selected messages.</td>
</tr>
<tr>
<td>View</td>
<td>Click to view a message in the Safe Message View tab.</td>
</tr>
</tbody>
</table>

Message Quarantine list

- Date — Displays the date of the message.
- From — Displays the from email address of the message.
- Subject — Displays the subject of the message.
- Score — Displays the quarantine score of the message.
- Size — Displays the size of the message.

Safe Message View

The Safe Message View window provides more information about the quarantined message you have selected. You can also view the message content when policy settings Safe Message View is enabled.

Table 6 Safe Message View

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Click to release a selected message from the quarantine list and have it moved to your email inbox.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete a selected message from the quarantine list.</td>
</tr>
<tr>
<td>Always Allow for User</td>
<td>Click to release messages through to the email recipients. All senders' email addresses are added to the recipient's Allow List. All future messages from the senders will no longer be quarantined.</td>
</tr>
<tr>
<td>Always Deny</td>
<td>Click to block messages to the email recipients.</td>
</tr>
</tbody>
</table>

Email Continuity

Email Continuity provides a comprehensive managed disaster recovery service that protects your email traffic during a network outage. When active, users and administrators can view, send, and manage their email using the online interface while the service stores all inbound and outbound mail activity in the cloud. Afterwards, when connectivity is restored, the service synchronizes your email with your email servers and normal email use can resume.
Email Continuity features and limitations
You can use most of the features of a standard web email client during an outage.

Table 7  Email Continuity features and limitations

<table>
<thead>
<tr>
<th>Email features...</th>
<th>Description</th>
</tr>
</thead>
</table>
| That you can use during an outage | • Standard email options.  
• Attach files  
• Search messages |
| That are unavailable during an outage | • 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 text in the body of a message. |
| That may be different from your standard email client | • You must separate multiple email addresses with commas, no spaces after the comma.  
• 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 Email 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. |

Email Continuity
When Disaster Recovery is active, you can access your email from the console. Use these tools to receive emails, reply to messages, view attachments, and search available folders.

Table 8  Criteria

<table>
<thead>
<tr>
<th>Option</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Click to run a search in the selected mail folder using your selected criteria and dates.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click to reset the search criteria values.</td>
</tr>
</tbody>
</table>
| Mail Folders | Select a folder to view your messages and search for mail.  
• Inbox — Click to view your inbox.  
• Deleted Items — Click to view your deleted mail.  
• Sent Items — Click to view your sent items. |
| Search for Mail | Select to run a new search.  
• Criteria — Enter a string to search for values in the To, From, and Subject fields.  
• Start Date — Enter or select a date value.  
• End Date — Enter or select a date value. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbox</strong></td>
<td>• New — Click to compose a new email.</td>
</tr>
<tr>
<td></td>
<td>• Open — Click to open the selected email in a new tab.</td>
</tr>
<tr>
<td></td>
<td>• Preview — Click to view the selected email in the preview panel. Select</td>
</tr>
<tr>
<td></td>
<td>the location of the preview panel, or click the button to cycle through</td>
</tr>
<tr>
<td></td>
<td>the options.</td>
</tr>
<tr>
<td></td>
<td>• Bottom — View the message on the bottom of the tab.</td>
</tr>
<tr>
<td></td>
<td>• Right — View the message on the right of the tab.</td>
</tr>
<tr>
<td></td>
<td>• Hide — Hide the preview.</td>
</tr>
<tr>
<td></td>
<td>• Reply — Click to write a reply to the sender of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Reply All — Click to write a reply to the sender and all recipients of</td>
</tr>
<tr>
<td></td>
<td>the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Forward — Click to forward the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Delete — Click to delete the selected email and move it to the **Deleted</td>
</tr>
<tr>
<td></td>
<td>Items** folder.</td>
</tr>
<tr>
<td></td>
<td>• Actions — Select an action.</td>
</tr>
<tr>
<td></td>
<td>• Mark as read — Click to select messages as read.</td>
</tr>
<tr>
<td></td>
<td>• Mark as unread — Click to select messages as unread.</td>
</tr>
<tr>
<td></td>
<td>• Print — Click to print the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Refresh — Click to refresh the list of the email messages.</td>
</tr>
<tr>
<td><strong>Deleted</strong></td>
<td><strong>Items</strong></td>
</tr>
<tr>
<td></td>
<td>• Open — Click to open the selected email in a new tab.</td>
</tr>
<tr>
<td></td>
<td>• Preview — Click to view the selected email in the preview panel. Select</td>
</tr>
<tr>
<td></td>
<td>the location of the preview panel, or click the button to cycle through</td>
</tr>
<tr>
<td></td>
<td>the options.</td>
</tr>
<tr>
<td></td>
<td>• Bottom — View the message on the bottom of the tab.</td>
</tr>
<tr>
<td></td>
<td>• Right — View the message on the right of the tab.</td>
</tr>
<tr>
<td></td>
<td>• Hide — Hide the preview.</td>
</tr>
<tr>
<td></td>
<td>• Reply — Click to write a reply to the sender of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Reply All — Click to write a reply to the sender and all recipients of</td>
</tr>
<tr>
<td></td>
<td>the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Forward — Click to forward the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Undelete — Click to undelete the selected email and move it to the <strong>Inbox</strong> folder.</td>
</tr>
<tr>
<td></td>
<td>• Actions — Select an action.</td>
</tr>
<tr>
<td></td>
<td>• Mark as read — Click to select messages as read.</td>
</tr>
<tr>
<td></td>
<td>• Mark as unread — Click to select messages as unread.</td>
</tr>
<tr>
<td></td>
<td>• Print — Click to print the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Refresh — Click to refresh the list of the email messages.</td>
</tr>
<tr>
<td>Option</td>
<td>Definitions</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Sent Items</strong></td>
<td>• <strong>Open</strong> — Click to open the selected email in a new tab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Preview</strong> — Click to view the selected email in the preview panel. Select the location of the preview panel, or click the button to cycle through the options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bottom</strong> — View the message on the bottom of the tab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Right</strong> — View the message on the right of the tab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hide</strong> — Hide the preview.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reply</strong> — Click to write a reply to the sender of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reply All</strong> — Click to write a reply to the sender and all recipients of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forward</strong> — Click to forward the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Print</strong> — Click to print the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Refresh</strong> — Click to refresh the list of the email messages.</td>
</tr>
<tr>
<td><strong>Preview panel</strong></td>
<td>• <strong>Open</strong> — Click to open the selected email in a new tab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reply</strong> — Click to write a reply to the sender of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reply All</strong> — Click to write a reply to the sender and all recipients of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forward</strong> — Click to forward the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete</strong> — Click to delete the selected email and move it to the <strong>Deleted Items</strong> folder.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Actions</strong> — Select an action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mark as read</strong> — Click to select messages as read.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mark as unread</strong> — Click to select messages as unread.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Print</strong> — Click to print the selected email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show Headers/Hide Headers</strong> — Click to show or hide email headers.</td>
</tr>
</tbody>
</table>
Table 9  Email Continuity (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opened message tab</td>
<td>• Reply — Click to write a reply to the sender of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Reply All — Click to write a reply to the sender and all recipients of the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Forward — Click to forward the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Print — Click to print the selected email.</td>
</tr>
<tr>
<td></td>
<td>• Show Headers/Hide Headers — Click to show or hide email headers.</td>
</tr>
<tr>
<td>New Message</td>
<td>• Send — Click to send the message.</td>
</tr>
<tr>
<td></td>
<td>• Attach — Click to attach files to the email.</td>
</tr>
<tr>
<td></td>
<td>• Switch to Plain Text/Switch to HTML — Click to select the message format.</td>
</tr>
<tr>
<td></td>
<td>• Plain text — use text-only format.</td>
</tr>
<tr>
<td></td>
<td>• HTML — use HTML WYSIWYG tool to format the message.</td>
</tr>
<tr>
<td></td>
<td>• From: — Select the from address.</td>
</tr>
<tr>
<td></td>
<td>• To: — Enter one or more email addresses.</td>
</tr>
<tr>
<td></td>
<td>• Cc: — Enter one or more Cc email addresses.</td>
</tr>
<tr>
<td></td>
<td>• Bcc: — Enter one or more Bcc email addresses.</td>
</tr>
<tr>
<td></td>
<td>• Subject: — Enter the subject text.</td>
</tr>
<tr>
<td></td>
<td>• Attachment: — Select a file attachment. A new Attachment field displays each time you click Attach and add the file.</td>
</tr>
<tr>
<td></td>
<td>• Delete icon — Click to delete the attachment.</td>
</tr>
<tr>
<td></td>
<td>• Message body — Enter the message body.</td>
</tr>
</tbody>
</table>

Allowing or blocking email from senders

You can define lists of senders whose email addresses either will always be accepted without spam filtering (Allowed Sender List) or will never be accepted for delivery (Blocked Sender List).

Types of spam to block

Two basic definitions of spam can help you determine whether a sender address should be added to the Blocked Senders list.

• Unwanted emails received from recognized senders — For example, a salesperson for a company may be sending you unwanted emails. In this scenario, it is unlikely that the sender address will be changed often by the spammer, so this type of address is a good candidate to be added to Blocked Senders list.

• Unwanted emails containing questionable or offensive content sent by senders deliberately attempting to bypass blacklisting and content filtering rules — For example, emails from a sender might contain a fraudulent money-making offer or offensive sexual content. In this scenario, these spammers often change their email addresses, email content, etc., in an attempt to bypass any blacklist filtering. This type of address is not a good candidate to be added to the Blocked Senders list because the denial is effective for only a brief time.
Your Allowed Senders and Blocked Senders lists versus allow or deny Lists in your groups policy

Your Email Protection administrator can define Allow and Deny lists as part of the policy for your group. In this case, the settings made by the administrator might take precedence and be applied before your Allowed Senders or Blocked Senders settings.

Email that contains viruses, attachment violations, or content violations might also be denied or quarantined based on those violations, regardless of your allow list. Also, emails that have been quarantined by Email Protection might not need to be added to Blocked lists because they are already being blocked from entering your email network.

Add senders to the allowed list

You can define lists of senders whose email addresses are always accepted without spam filtering (Allowed Senders list).

Before you begin

The maximum number of email addresses and domain names a user can include in a senders list is 300. Any duplicate or invalid email addresses or domain names are discarded automatically. However, an administrator can add up to 1000 addresses on behalf of a user by selecting Account Management | Users, selecting a user, and selecting Email Protection. The administrator can then select a senders list to add addresses to allow or block.

You can add senders using the Message Quarantine tab or the Allowed Senders tab.

Task

1. If necessary, click Allowed Senders.

2. For each domain or sender you want to add, perform these steps:
   a. In the New field, enter a sender address.

      The following values are allowed in list entries:
      - Domain Name — Qualified domain name (for example, xyz.com) or subdomains (for example, *@*.xyz.com) allows emails from any subdomain of the XYZ domain, such as user@abc.xyz.com). If you want to allow all emails from this domain, then use this option instead of typing in each email address associated with the domain
      - Sender Address — Complete email address (for example, user@xyz.com) or partial address (for example, user*@xyz.com or *@xyz.com)

   b. Click New.

      The entry is moved to the sender list.

3. Click Apply.

Upload a list of allowed senders

You can create a file containing a list of senders and upload that list to the Allowed Senders page.

For option definitions, click Help in the interface.
Task
1  Create the file with the list of senders.
2  Select Allowed Senders.
3  Click Browse for the Allowed Senders List field.
4  Find the file on your computer and click Upload.
5  Click Apply.

Remove senders from the allowed senders list
You can remove one or more senders from the list using the delete feature. Emails from these senders are again subject to ordinary filtering policies. For option definitions, click Help in the interface.

Task
1  Select Allowed Senders.
2  Select the Delete checkbox for each sender you want to remove from the list.

To select all users on the page at one time:
1  Select the first user on the page.
2  Press and hold Shift+Ctrl.
3  Select the last user on the page.

3  Click Apply.

Add senders to the blocked list
You can define lists of senders whose email addresses will never be accepted for delivery (Blocked Senders list).

Before you begin
The maximum number of email addresses and domain names a user can include in a senders list is 300. Any duplicate or invalid email addresses or domain names are discarded automatically. However, an administrator can add up to 1000 addresses on behalf of a user by selecting Account Management | Users, selecting a user, and selecting Email Protection. The administrator can then select a senders list to add addresses to allow or block.

You can add senders using the Message Quarantine tab or using the Blocked Senders tab.

A common spamming technique is to change the sender email address often or even hijack a user's email address to send spam. The Blocked Senders list might not prevent future spam emails from these spammers. The Blocked Senders 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).

Task
1  If necessary, click Blocked Senders.
2  For each domain or sender you want to add, perform these steps:
   a  In the New field, enter a sender address.
The following values are allowed in list entries:

- **Domain Name** — Qualified domain name (for example, xyz.com) or subdomains (for example, *@*.xyz.com) allows emails from any subdomain of the XYZ domain, such as user@abc.xyz.com. If you want to allow all emails from this domain, then use this option instead of typing in each email address associated with the domain.

- **Sender Address** — Complete email address (for example, user@xyz.com) or partial address (for example, user*@xyz.com or *@xyz.com)

1. Click **New**.
   - The entry is moved to the sender list.

2. Click **Apply**.

**Upload a list of blocked senders**

You can create a file containing a list of senders and upload that list to the Blocked Senders page. For option definitions, click **Help** in the interface.

**Task**

1. Create the file with the list of senders.

2. Select **Blocked Senders**.

3. Click **Browse** for the **Blocked Senders List** field.

4. Find the file on your computer and click **Upload**.

5. Click **Apply**.

**Remove senders from the blocked senders list**

You can remove one or more senders from the list using the delete feature. Emails from these senders are again subject to ordinary filtering policies. For option definitions, click **Help** in the interface.

**Task**

1. Click **Blocked Senders**.

2. Select the **Delete** checkbox for each sender you want to remove from the list.

   - To select all users on the page at one time:
     1. Select the first user on the page.
     2. Press and hold **Shift+Ctrl**.
     3. Select the last user on the page.

3. Click **Apply**.