Email Security
Personal Dashboard User Guide

GoSecure

11.6

Contents

CHAPTER 1 Introduction

To help you manage messages filtered by the GoSecure Email Security product, you can use two tools: the Personal Dashboard and the Spam Digest.

The Personal Dashboard

The Personal Dashboard is a Web portal for managing your email filtering account. It has four tabs:

- **Messages Tab**: View, delete, and release filtered messages.
- **Policies Tab**: Manage your filter settings, including Friends and Enemies lists.
- **Settings Tab**: Manage Spam Digest settings, such as frequency, format, content, and sort order.
- **Status Tab**: Displays your mailbox name, aliases, and digest status.

Note: What actions you can take on yourPersonal Dashboard depends on how the Administrator has configured the Email Security product. You may not be able to perform all actions listed in this guide.

The Spam Digest

The Spam Digest is a list of quarantined messages identified as spam, junk, or containing a virus or other malicious content. You only receive a Spam Digest if you have messages that were blocked or quarantined during the latest digest period. If enabled by your administrator, you can view both inbound and outbound quarantined messages.

Each digest you receive lists newly filtered mail, while older filtered mail is not shown. You can review the list of quarantined messages for any valid messages that were mistakenly filtered out and then use the Personal Dashboard to manage those messages. You can view the list of quarantined messages and release them from the Spam Digest, but for most other actions (viewing, searching, deleting, etc.) you will need to use the Personal Dashboard.

Releasing a Message

To release a message directly from the Spam Digest:

- Click the **Release** link to the left of the message. The message is immediately be released from quarantine.

Stopping Delivery of the Spam Digest

To stop receiving the Spam Digest:

- Click the **Unsubscribe** link in the bottom left corner of the Spam Digest. It will no longer be delivered to your email inbox.

Tip! Click the **my account** link near the top right of the Spam Digest to open the login screen of the Personal Dashboard in your browser. Then bookmark this page in your browser for easy access.

Changing the Frequency of the Spam Digest

The digest delivery frequency can be set to daily, weekly, or never. By default, the Spam Digest is sent out daily.

To change the frequency of the Spam Digest:

- From the Spam Digest, click the **Change Report Frequency** link. This will redirect you to the Personal Dashboard, where you can use the Setting tab to modify the frequency.

Other Spam Digest Settings

To change the frequency of the spam digest or change other settings such as timezone, see Modifying Spam Digest Settings.

CHAPTER 2 Using the Personal Dashboard

This chapter explains how to access your Personal Dashboard and create and change your password.

You can log into your Personal Dashboard through a link or through a Spam Digest.

Note: Depending on your email settings, you may not need a password to log into the Personal Dashboard. If you don't need one, you can create one for added security. You can also use your Microsoft or Google username/password to log in.

Accessing through a Link

When you started your email account, or when the mail system began using the filtering system, your email administrator sent you a link to your Personal Dashboard.

To access your Personal Dashboard through a link:

1. Click the link you were sent or copy and paste it into the address field of your web browser. This opens the Personal Dashboard screen.
2. If you need to create a password, the Personal Dashboard Login screen opens.
3. Click **Signup**. This displays the Signup screen.
4. Enter your email address, then enter and re-enter your password in the text fields, then click **Signup**.. Your password must contain at least six characters.

Note: Contact your email administrator if you receive an error message after trying to sign in.

Accessing through the Spam Digest

When you receive a Spam Digest, you can access the Personal Dashboard directly from a link in the digest.

To access your Personal Dashboard through the Spam Digest:

- Click the **My Account** link in the Spam Digest. The Personal Dashboard screen opens in your browser.

Creating a Password

If your personal dashboard does not require a password, you have the option to one to provide additional security.

To create a password in the Personal Dashboard:

1. Open your Personal Dashboard.

2. From the top of any screen, click **Change Password**.
3. Leave the Old Password text box blank, and enter then reenter your password. Your password must contain at least six characters.
4. Click **Save**.

Changing Your Password

To modify your password:

1. Open your Personal Dashboard.
2. From the top of any screen, click **Change Password**.
3. Enter your old password.
4. Enter and reenter your new password. Your password must contain at least six characters.
5. Click **Save**.

Note: Contact your email administrator if you receive an error message after trying to change your password.

Status Tab

The Status tab is a read-only page that shows:

- Your primary email address and aliases
- The last time your digest was sent
- The number of messages quarantined since the start of email filtering, in text and graphical format

To view the status of your email account and statistics about the latest Spam Digest:

- Click the **Status** tab.

The screenshot below shows an example Status tab. It shows the mailbox name and the aliases. The most recent digest was sent on November 4 and it contained 5 quarantined messages.

CHAPTER 3 Messages Tab

Quarantined messages are emails that the system has filtered out based on the filtering options set in your **Policies Tab**tab or by Administrator-controlled policies. Quarantined messages are archived for 35 days online, and then they are automatically deleted.

From the Messages tab of the Personal Dashboard, you can review, release, or delete quarantined messages. If enabled by your administrator, you can toggle between viewing inbound or outbound quarantined messages.

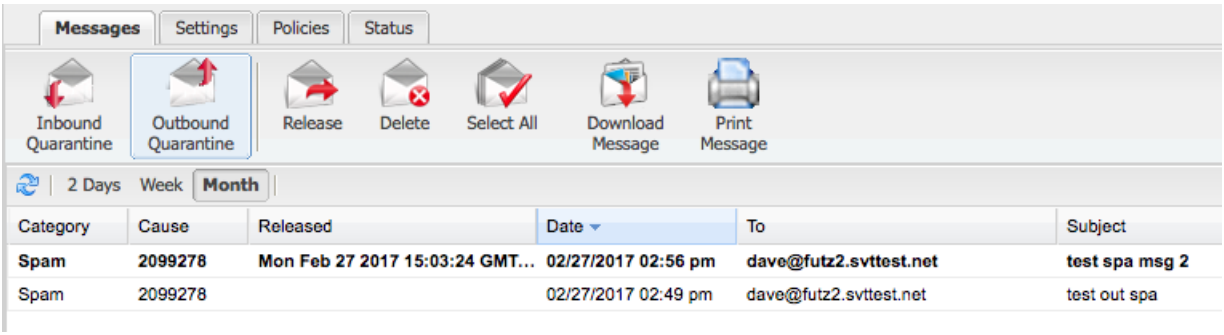


Figure 1. Messages tab

If email continuity is licensed by your organization and enabled, you can also manage your email inbox from the Messages tab. See Email Continuity for details.

Note: On the rare occasion when a significant network issue occurs, a link to a system status alert displays in the status bar.

Viewing a Message

To view a quarantined message:

1. Click the **Messages** tab.
2. Select the message to view. The message contents display on the bottom of the screen.

Searching for Messages

You can search quarantined email to locate individual messages by addresses, names, or any other text string. You can use search to look for mail you think may have been mistakenly filtered. The search does not include attribute fields that are not shown in the quarantine list. For instance, you can check to see if a message from your Aunt Agnes is in the quarantine. Or you can search for a specific phrase that may commonly trigger messages to be filtered.

To search the quarantine for messages:

1. Click the **Messages** tab.
2. In the search box (at the top right of the screen), enter the term to be searched.

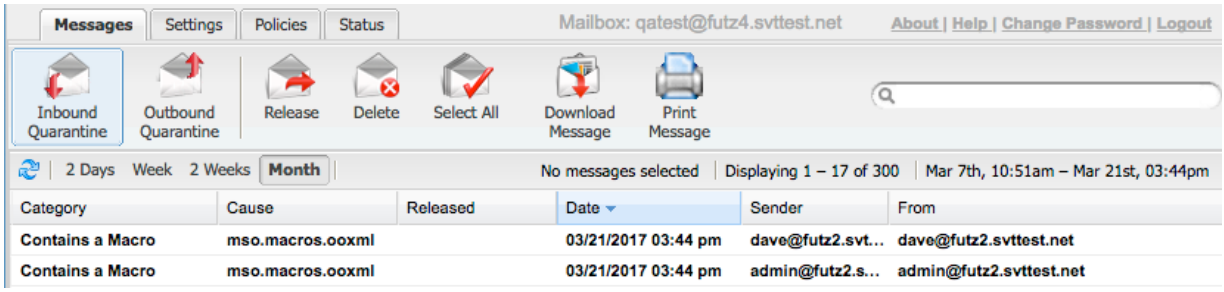


Figure 2. Search box

3. Press Enter. All messages that contain the search term display in the quarantine. All messages that do NOT contain that term are temporarily hidden from view.

Releasing Messages

You can release one or more messages from quarantine. If enabled by your administrator, you can toggle between viewing inbound or outbound quarantined messages.

To release a quarantined message:

1. Click the **Messages** tab.
2. Click either **Inbound Quarantine** or **Outbound Quarantine** to view that list of held messages.
3. Select one or more messages to release. To release more than one message:
   - Use Shift+Click to select adjacent messages.
   - Use Ctrl+Shift to select non-adjacent messages.
4. Click the Release icon. This displays a Confirmation dialog.

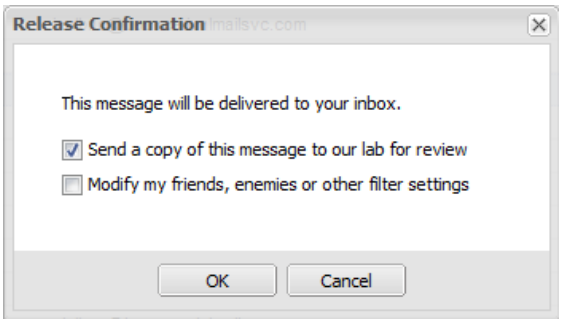


Figure 3. Release Confirmation

5. Check the boxes as applicable and click **OK**.
   - If you want to send a copy of the message to GoSecure to improve filter quality, check the box.
   - If you want to update your friends or enemies or recipient friends list or any policies, check the box. A wizard guides you through additional selections to update the lists. Follow the instructions, clicking **Next/Finish** on each screen.

Note: When the MIME from: header differs from the SMTP envelope sender both are included in the list of senders that can be added to the whitelist.

The messages are sent to your email inbox.

Deleting Messages

You do not need to delete messages from your quarantine. All messages are automatically deleted after 35 days. You can, however, manually delete messages from your quarantine if you like.

To delete a quarantined message:

1. Click the **Messages** tab.
2. Select one or more messages to delete. To delete more than one message:
   - Use Shift+Click to select adjacent messages.
   - Use Ctrl+Shift to select non-adjacent messages.

Note: To delete *all* quarantined messages, click the Select All icon. This selects all messages in the Messages screen plus any other quarantined messages, which may not be visible.

3. Click the Delete icon. The messages are deleted.

Selecting All Messages

You can select all quarantined messages in one step.

To select all quarantined messages:

1. Click the **Messages** tab.
2. Click the Select All icon. This selects all messages in the Messages screen plus any other quarantined messages, which may not be visible.

Downloading a Message

Messages can be downloaded to your computer in .eml format. Many email clients use this format to import files. For more information on the .eml format, see http://www.fileinfo.com/extension/eml.

To download a quarantined message:

1. Click the **Messages** tab.
2. Select the message to download.
3. Click the Download icon. The message is downloaded.

Changing the Messages List Display

On the Messages tab there are several ways to sort and filter the list. You can also change the attributes that are shown.

Sorting and Filtering the Message List

While viewing the list of quarantined messages on the Messages tab, you can limit the messages in the display by received date. You can also sort the list by any of the columns, either in ascending or descending order.

To limit the display:

- Select the timeframe for messages to view. You can show messages received in the last 2 days, week, or month (all messages).

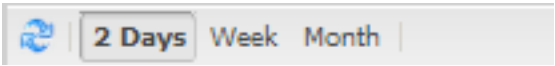


Figure 4. Time selection for messages list

To sort the list of quarantined messages:

- Click a column heading to sort by that column in ascending order.
- Click a second time to sort by that column in descending order.

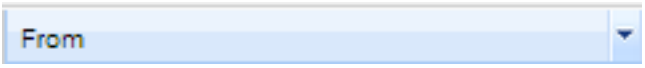


Figure 5. Order of messages in the list

Viewing Inbound and Outbound Messages

Some administrators configure the system to filter outbound email messages. You can perform the same actions on outbound filtered messages as on inbound messages in the Personal Dashboard.

Note: Depending on the settings applied by your email administrator, the outbound filtering option may or may not be available to all users.

To view outbound filtered messages:

1. Click the **Messages** tab.
2. Click the Outbound Quarantine icon. Outbound filtered messages display.

Clearing the Filtered Message Display

When you filter the quarantine display using the Search function, only messages that contain that search term display. To show all filtered messages, clear the search box.

To clear the filtered message display:

1. Click the **Messages** tab.

2. In the search box, delete all text.
3. Press Enter. All quarantined messages now display.

Displaying Message Attributes

All email messages have a number of attributes. By default, quarantined messages in the Personal Dashboard display the message date, removal date, category,type of message (category), the reason it was caught (cause), the sender, the From field of the message, and the message subject. You can remove any of the default attributes from the quarantine message display. You can also add other attributes to the display.

To change display of quarantined message attributes:

1. Click the **Messages** tab.
2. Click the downward shaped triangle on the right of a column heading.
3. Click **Columns**.
4. Select or clear the attribute check boxes as needed. The selected attribute columns display.

Email Continuity

Email Continuity provides access to your email inbox when your regular email server is down. If your organization has licensed this feature AND your system administrator has enabled it, you can use the Messages tab of the Personal Dashboard to manage all of your incoming messages.

When Email Continuity is active, an additional button, Inbox, appears on the Messages tab.

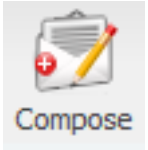
Note: Depending on the settings applied by your email administrator, the Email Continuity inbox may not be available to all users.

To access your inbox:

1. Click the **Messages** tab.
2. Click the Inbox icon. The messages in your inbox display.

Note: The Email Continuity inbox does not include messages that have been released from quarantine.

From the inbox you can create new messages, reply to messages, and forward messages. Use the buttons at the top of the screen to manage your messages:



Compose a new message.

Select a message in the list and click this button to reply to the selected message.

Select a message in the list and click this button to reply to the selected message, including all recipients on the reply.

Select a message in the list and click this button to forward the selected message.

Select a message in the list and click this button to download the selected message.

CHAPTER 4 Settings Tab

You can use the Settings tab on the Personal Dashboard to control options for the Spam Digest:

- The delivery frequency of the Spam Digest
- Whether to receive the Spam Digest in HTML, text, or multipart format
- Which types of messages to include in the Spam Digest
- The sort order of the message list
- Your time zone

To set Spam Digest options:

1. Click the click the **Settings Digest** tab.
2. Click a radio button to select a delivery frequency. Options are Daily, Weekly, or Never.
3. From the drop-down list, select a report format. Options are HTML, Plain Text, or Multipart.
4. From the drop-down list, select the report contents. Options are:
   - Summary: Displays the counts of each type of message.
   - Green Zone: Displays only mail from the green zone (junk).
   - Yellow and Green Zones: Displays mail from the yellow zone (blank, forged, foreign, attachments) plus mail from the Green Zone (junk).
   - Red, Yellow & Green Zones: Displays all mail from the quarantine.
5. From the drop-down list, select the message sort order. Options are Date & Time, Size, Sender, or Subject.
6. Optional: Select the Ascending check box to sort the messages in ascending order.
7. In the Time Zone Setting area, click on the section of the map that contains your location. Then select your time zone from the list. Your settings are immediately updated to the new time zone.

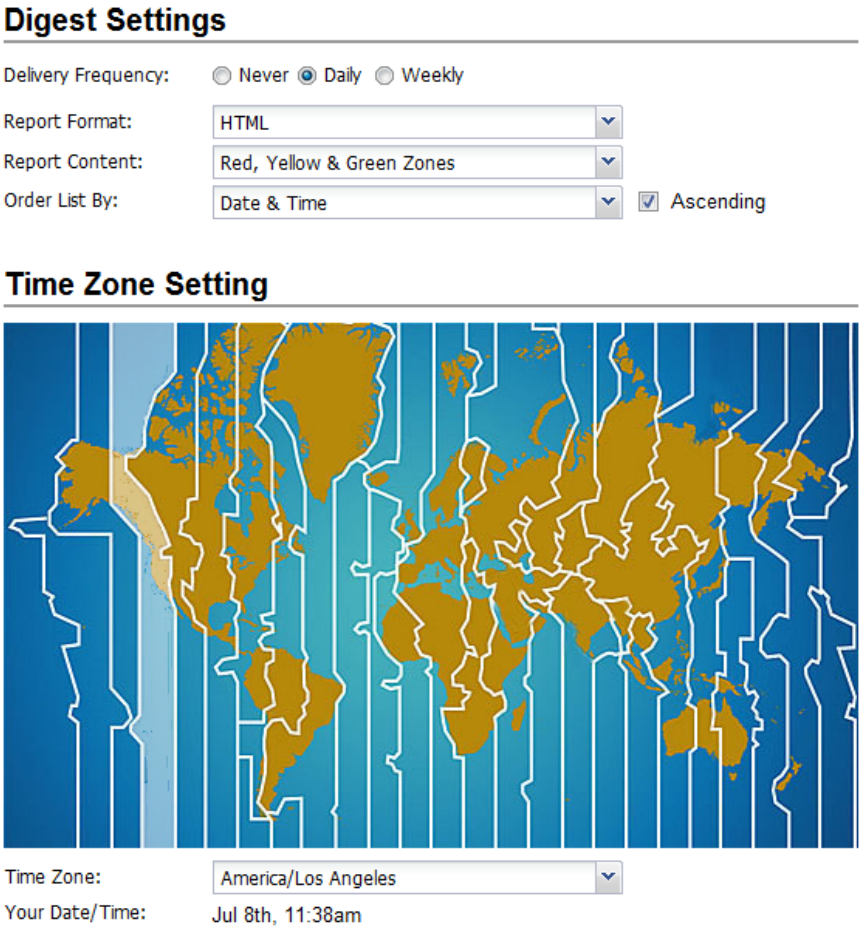


Figure 6. Settings tab

CHAPTER 5 Policies Tab

You can use the Policies tab on the Personal Dashboard to configure how different types of messages are handled.

Note: Filter settings configured by your email administrator are tagged with the Administrator Settings icon. These settings cannot be removed but they can be modified if permitted.

Options for Filtering Messages

Depending on the settings applied by your email administrator, you may or may not be able to configure your email filtering options. Valid filtering options are:

- **Allow**: Allows the message to pass through the filter and delivers the message to your email inbox.
- **Markup**: Adds a subject tag to the Subject line of the email message. Subject tags can contain up to twenty text characters that are added to the beginning of the email's subject line to alert you that the message has been flagged as suspicious. See Configuring Subject Tags for more information.
- **Quarantine**: Quarantines the message.
- **Block**: Deletes the message. Blocked messages are not recoverable from the quarantine list.

Note: The filter settings configured by your email administrator are tagged with the Administrator Settings icon. These settings cannot be removed but they can be modified if permitted.

To modify your filtering options:

1. Click the **Policies** tab.
2. From the drop-down list below each message type, select the filtering option.

Figure 7. Configuring message filtering

Configuring Subject Tags

Subject tags are up to twenty text characters that can be prepended to an email's subject line to alert you that the message has been flagged as suspicious. For example, you can configure the mail from invalid senders (the Forged: field) to say "Fake:" to alert you that the message is not from the sender it claims to be from. In this example, the tagged message in your mailbox might read "Fake: Your New Store Gift Card!"

Note: GoSecure recommends ending the subject tag with a colon. When most mail programs sort on the subject line they ignore the text before a colon and sort on the content of the subject line.

To configure a subject tag:

1. Click the **Policies** tab.
2. Depending on the message type, do one of the following:
   - For all message types other than Foreign and Attachments, open the **Red Zone** section and then select **Markup** as the filtering option.
   - For Foreign and Attachments, open the **Yellow Zone** section and then right-click the type to mark up and select **Markup**.

   A new text entry box appears on the right of the drop-down list. This text box may have a default subject tag..
3. Optional: Clear the default subject tag and type your text entry into the box.

Selecting Foreign Language Options

Depending on the settings applied by your email administrator, you may have the option to block email that contains foreign characters. A large volume of spam is transmitted using Russian, Cyrillic, Chinese, Korean, and Japanese non-English character sets. If you normally receive email in these languages, configure your settings so that these messages pass through the filters.

By default, the system allows mail with non-English language character sets but adds a subject tag of FOREIGN: before the mail subject line. Foreign language filtering options can be applied individually on a per-language basis.

You can filter messages with foreign language content with the same options described in Options for Filtering Messages. Additionally, you can remove a language from special treatment by deleting the language. Deleting the language means that the Email Security product processes the message as it would with any other message, without any special rules.

Note: You will not be able to delete a language if your email administrator has blocked that option. If so, a pop-up window alerts you that the filtering option has been reset to the administrator default.

To modify foreign language filtering options:

1. Click the **Policies** tab.
2. In the Foreign section (Yellow Zone), click a language to select it.
3. Right-click the language and select a filtering option.

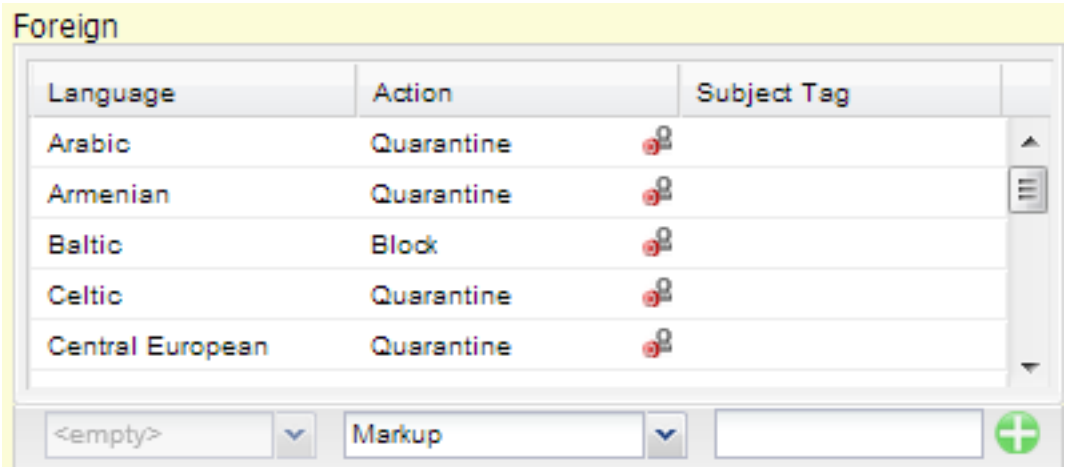


Figure 8. Foreign Language options

To delete a foreign language:

1. Click the **Policies** tab.
2. In the Foreign section (Yellow Zone), right-click a language to delete.
3. Click **Delete**. A confirmation message opens.
4. Click **OK**.

To add a deleted language:

1. Click the **Policies** tab.
2. In bottom left of the Foreign section, select a deleted language.
3. Select the filtering option from the drop-down list. Options are Allow, Markup, Quarantine, and Block.
4. For a marked up attachment, enter a subject tag to prepend to the subject line. See Configuring Subject Tags for information about subject tags.
5. Click + (the plus sign) button to add the language.

Selecting Attachment Options

You can filter messages with attachments with the same options described in Options for Filtering Messages. Additionally, you can add a new attachment type to filter.

To add an attachment type

1. Click on the **Policies** tab.
2. In the Attachments (Yellow Zone) section, enter the file extension of the attachment to filter.

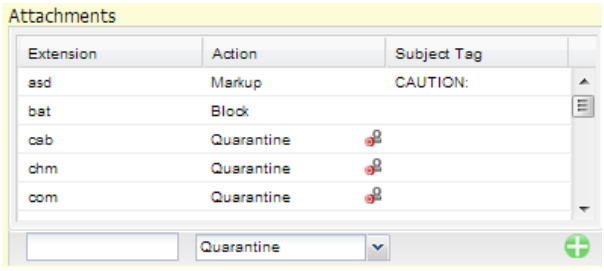


Figure 9. Attachment options

3. Select the filtering option from the drop-down list. Options are Allow, Markup, Quarantine, or Block.
4. For a marked up attachment, enter a subject tag to prepend to the subject line. See Configuring Subject Tags for information about subject tags.
5. Click + (the plus sign) button to add the attachment type.

Using Friends and Enemies Lists

You can use the Friends (whitelist) and Enemies (blacklist) options in the Filter by Sender section to filter by email address or domain name.

- Friends: Mail from these addresses and domains will not be filtered for spam.
- Enemies: Mail from these addresses and domains will be quarantined. If you have a legitimate sender that you do not want to receive further email from, you can add an entry (email address or domain) to the Enemies blacklist.

Figure 10. Friends and Enemies lists

Using these lists are not required to ensure that you do not receive spam.

If there is a conflict between an item on your Friends list and an identical item on the Enemies list for the entire domain (set by your email administrator), your Friends setting takes precedence.

GoSecure does not recommend using these lists to manage email accounts because spammers have adopted techniques to send email from addresses within your own domain (including your own email address). Your Friends list, in this case, would override the spam filter rule and result in the spam and viruses being delivered to you even though the system had identified them as spam. Similar unintended consequences can result from the use of the Enemies list.

Note: GoSecure strongly advises using the email system for a month or more before adding anyone to your Friends or Enemies lists. Testing indicates that these lists are more effective when they are used sparingly.

Viewing the Friends and Enemies Lists

- To view your Friends list or Enemies lists, select the **Policies** tab on the Personal Dashboard then scroll down to the **Filter by Sender** section and click the arrow to the left to display the contents of this section.

Editing the Friends List

To add to your Friends list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open this section.
3. In the Friends text box, enter the email address or domain name to add.
4. Click + (the plus sign) button to add it to this list.

To remove an entry from your Friends list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open this section.
3. In the Friends list, select the item to remove.
4. Click - (the minus sign) button to remove it from the list.

Editing the Enemies Lists

To add to your Enemies list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open this section.
3. In the Enemies text box, enter the email address or domain name to add.
4. Click + (the plus sign) button to add it to the Enemies list.

To remove an entry from your Enemies list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open the section.
3. In the Enemies list, area, select the item you want to remove.

4. Click - (the minus sign) button to remove it from the Enemies list.

Viewing the Administrative Friends and Enemies List

Your email administrator may have set up a Friends (whitelist) or Enemies (blacklist) or Recipient Friends list for all users. You can view this list, but cannot make any changes to it. If you feel that something is whitelisted or blacklisted by mistake, contact your email administrator.

To view an administrative Friends list (whitelist):

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open the section.
3. In the Filter by Sender section, beneath the list, click the Friends link. The list appears in a pop-up window.

To view an administrative Enemies list (blacklist):

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open the section.
3. In the Filter by Sender section, beneath the Enemies list, click the Enemies link. The list appears in a pop-up window.

Using SPF Exceptions

You can use the SPF Exceptions list in the Filter by Sender section to allow emails by domain name, IP address, or CIDR block.

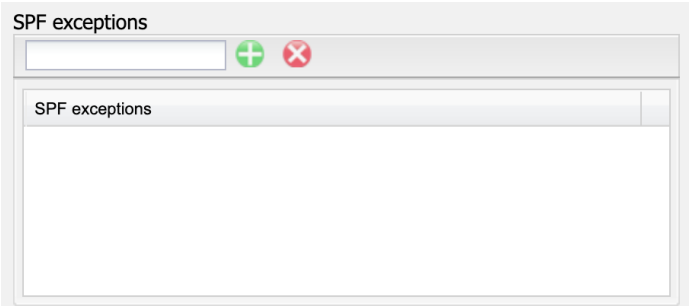


Figure 11. SPF Exceptions lists

Viewing the SPF Exceptions List

- To view the SPF Exceptions list, select the **Policies** tab on the Personal Dashboard then scroll down to the **Filter by Sender** section and click the arrow to the left to display the contents of this section. SPF Exceptions is below the Friends and Enemies lists.

Editing the SPF Exceptions List

To add to the list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open this section.

3. In the SPF Exceptions text box, enter the item to add.
4. Click + (the plus sign) button to add it to this list.

To remove an entry from the list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open this section.
3. In the SPF Exceptions list, select the item to remove.
4. Click - (the minus sign) button to remove it from the list.

Using the Recipient Friends Lists

You can use the Recipient Friends list in the Filter by Recipient section to filter by email address or domain name. Mail to these addresses and domains will always receive mail from your mailbox. Mail sent to these addresses will not be subject to outbound filtering if all recipients are on this list.

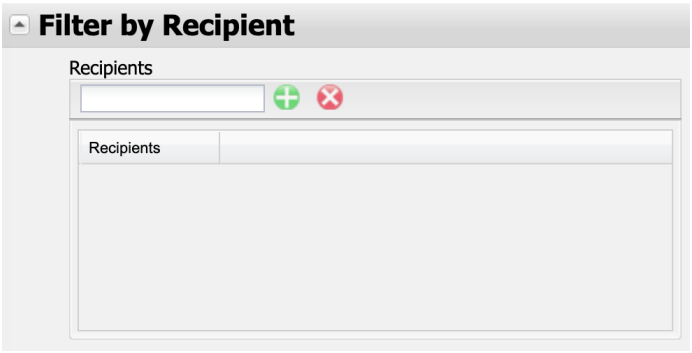


Figure 12. Recipient Friends list

Note: GoSecure strongly advises using the email system for a month or more before adding anyone to your Recipient list. Testing indicates that these lists are more effective when they are used sparingly.

Viewing the Recipient Friends List

- To view your Recipient Friends list, select the **Policies** tab on the Personal Dashboard, then click the arrow next to Filter by Recipient to open that section and display the Recipient Friends list.

Editing the Recipient Friends List

To add to your Recipient Friends list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open that section.
3. In the Recipient Friends list, enter the email address or domain name to add.
4. Click + (the plus sign) button to add it to this list.

To remove an entry from your Recipient Friends list:

1. Click the **Policies** tab.
2. Click the arrow to the left of **Filter by Sender** to open that section.
3. In the list, select the email address or domain name to remove.
4. Click - (the minus sign) button to remove it from the list.

Troubleshooting

What if my password doesn't work?

If you forget your password, or your password does not work, click the Forgot Password link, enter your email address, and a new password will be emailed to you. If you log in to the Personal Dashboard using LDAP, Microsoft, or Google, then you need to work through those channels to update your password.

Note: Contact your system administrator if you receive an error message after trying to sign in or to have your password sent to you.

Some spam still gets through to my mailbox. What do I do?

Our thousands of decoy mailboxes typically identify and block new spam campaigns within minutes. If you continue to receive spam, please forward samples as attachments to spam@edgewave.com so that we can improve the quality of this service.

I mistakenly released a spam message. What happens now?

Released messages are automatically sent to your email inbox. This does not, however, affect future spam filtering. Identical spam will still be quarantined in the future.

Why am I getting returned mail as "Undeliverable" or "NDR"?

Recently many users have received NDR (Non Delivery Receipt) or “bounceback” messages. Bounceback/NDR messages are standard messages that notify a sender of a failed delivery. This mechanism has now been hijacked by spammers.

How it works: Spammers are using email addresses of known valid users to broadcast large volumes of messages pretending to be from those valid email addresses. Then, when hundreds or even thousands of those messages reach invalid recipients, the receiving mail servers “bounce” the message back to the users whose email addresses had been used for the campaign. Some users have received several hundred of these bounced messages in a given day.

This condition affects mail servers throughout the Internet. Your are not responsible for your email address being used in this manner. There is no action you can take to prevent this misuse from happening. If you continue to get this type of spam, please forward samples as attachments to spam@edgewave.com so that we can improve the quality of our service.

FAQ

How does filtering work?

The system flags messages that have suspicious content and sorts them into one of the danger zones based on the potential harm they could cause you or to your computer. In increasing danger, mail is classified into the following zones:

- **Green Zone**: Junk mail, including unsolicited advertising
- **Yellow Zone**: Suspicious mail, including blank, foreign, and with attachments
- **Red Zone**: Potentially dangerous, including spam, virus, and adult

How do you identify spam?

The system investigates bulk email that is captured from numerous decoy mailboxes worldwide. When these mailboxes receive a suspected message, we classify the content.

We use the following filtering techniques:

- Signature filtering for virus detection
- Real time blacklists
- Message rate throttling
- Reputation scores
- Message finger print analysis
- Graphic image analysis
- Verifying recipient account name
- String based text rules
- Pattern rules
- Human review

Is somebody reading my mail?

No. We filter mail through a series of rules-based programs to flag suspicious messages. The only time a person looks at a specific message is if it has been sent to a decoy account or a wrong address, or is flagged by a user and sent to us for analysis.

Will the filtering delay my mail?

The filtering process typically introduces a delay of less than one second.

Do I need to worry about viruses?

The system filters all email through two separate anti-virus programs. If your email has a virus, we will catch it.

What are my filtering options?

Depending on how aggressively you want to filter your email, you can configure each of the filtering categories to block the messages (delete them immediately), quarantine the messages for review, forward the messages to your mailbox with a tag in the subject line, or allow the messages to pass directly to your mailbox without a tag.

Note: You cannot modify a filtering option your administrator has set to block.

What are Administrator settings?

The Administrator settings icon on the Policies tab denotes a filtering option that has been configured by your system administrator. These settings cannot be removed, but they can be modified if permitted.

How do I view or change my filtering options?

Log in to the Personal Dashboard and select the Policies tab. This tab displays your current settings. You can change a setting for most filtering categories by selecting a different option from the drop-down list to the right of the message type.

Change foreign and attachments settings by right-clicking the item and selecting an option from the pop-up window. You can add a file extension to the Attachments list by typing in the extension in the text entry box, selecting the filtering option from the drop-down list, and clicking the plus sign button.

Log in to the Personal Dashboard. Filtering options are on the Policies, Foreign, and Attachments tabs. These tabs display your current settings. You can change a setting by selecting a different option from the drop-down list to the right of the message type or category.

Note: You cannot modify a filtering option your administrator has set to block.

What is "phishing"?

Phishing messages fraudulently attempt to lure the user into giving up personal information such as credit card numbers, passwords, and social security numbers. They appear to originate from banks, department stores, online merchants, and other trusted sources.

What is a bot?

A bot is an autonomous piece of software used by criminal hackers to infect computers, which then come under the command of the hacker. A network of these hijacked PCs is called a botnet, and it is often used to send spam. GoSecure Email Security defends against bot infections on both the inbound and outbound mail streams.

What are subject tags?

Subject tags are short bits of text (up to 50 characters) prepended to the subject line of an email message to alert you that a message has been flagged as suspicious. You can use the tags to set up filtering rules in your mail client.

Note: GoSecure recommend enclosing the subject tag in brackets; for example [JUNK]. When sorting on the subject line, most mail programs ignore these brackets and sort on the content of the rest of the subject line.

Why are attachments risky?

Some attachments can contain potentially harmful programs, such as viruses, spyware, and keyboard loggers that can cause loss of data and/or personal information. We recommend that you never open an attachment from senders you do not know, or those from senders you DO know, but from whom you were not expecting a file.

How do I select which attachments to block, filter, or mark up?

Log in to the Personal Dashboard and select the Policies tab. In the Attachments area, right-click the attachment type and select an option from the pop-up window.

You can add a new attachment type by entering the file extension in the leftmost text box, selecting the action from the drop-down list, and clicking the green plus icon. For marked up attachments, you can enter the subject tag in the rightmost text box.

Select the Attachments tab, then select the attachment from the drop-down list. Select a filter option. Your new selection is automatically saved.

To add a new attachment type, enter the file extension in the Add Extension: text box, then select the desired action from the drop-down list. For marked up attachments, you can enter the subject tag in the rightmost text box.