Managing eScout Spam and Virus Filtering
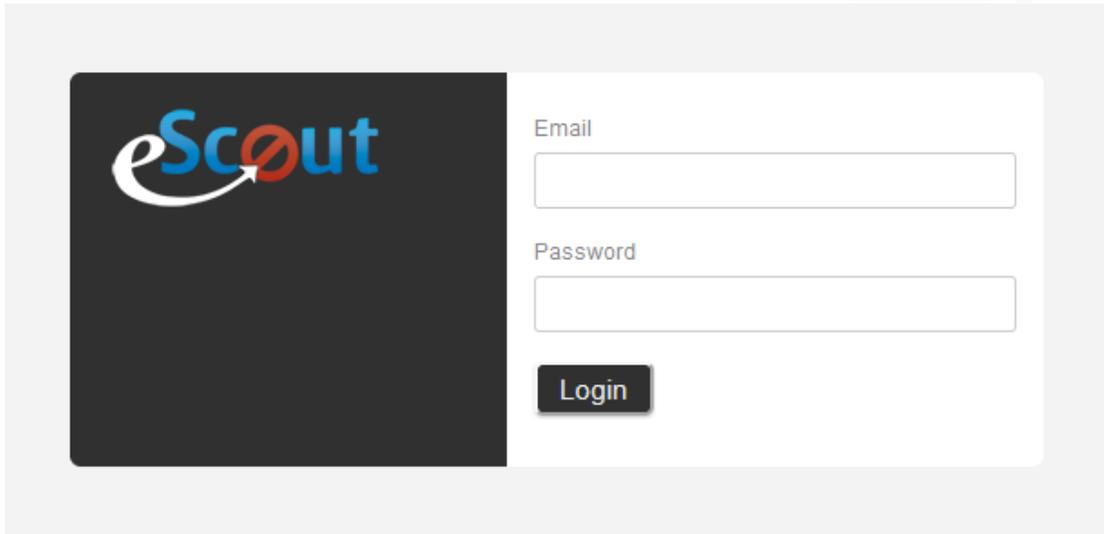
How do I access eScout?

To open your dedicated eScout mail quarantine:

1. Open **https://e-scout.cvctx.com** in your preferred web browser.

2. Log in with the email address and password associated with your mail account. Once logged in, the Suspected Spam section displays, showing emails that have been quarantined as possible spam.

What categories does eScout use to filter spam?

Email messages delivered to your mailbox are cached in the Delivered Messages section of eScout, while quarantined messages will be sorted into one of the following categories: **Suspected Spam, Invalid Headers, Suspicious Attachments,** or **Virus/Malware.** At any time, you can log in and manage the quarantined messages.

Delivered Messages

This section lists all email messages that have been allowed through the filter and delivered to your Hosted Email mailbox. A higher Score represents a higher likelihood that an email message is spam.

Suspected Spam

The Suspected Spam section displays email messages that have been quarantined as possible spam. You can access the email messages in this view for a period of 7 days after their initial quarantine. A higher Score number represents a higher likelihood that an email message is spam.

Invalid Headers

Email messages here have been quarantined for containing invalid, corrupted or malformed headers – a common trait of Spam/Junk mail and other types of suspicious email messages.

Suspicious Attachments

Email messages listed here have suspicious or potentially harmful file attachments. Attachments that are generally quarantined contain executable files, system files, or other file types known to generate unwanted behavior.

Virus/Malware

Any email messages here match known virus or malware signatures. Attempts to Rescue any email messages here will fail as they cannot be released from the quarantine.

How do I manage my spam messages?

eScout is a learning filter that improves its accuracy over time, and one way to help train it is by confirming known good email messages, known spam or virus messages, and rescuing email messages that have been quarantined incorrectly.

The Suspected Spam section displays emails that have been quarantined as possible spam. You can access the emails in this view for a period of 7 days after their initial quarantine. A higher Score number represents a higher likelihood that a message is spam.

To manage emails in the **Suspected Spam** section:

1. Log in to eScout and ensure **Suspected Spam** is displayed. If not, on the left pane, select **Suspected Spam.**
2. Use one of the following options to select the emails you want to manage.
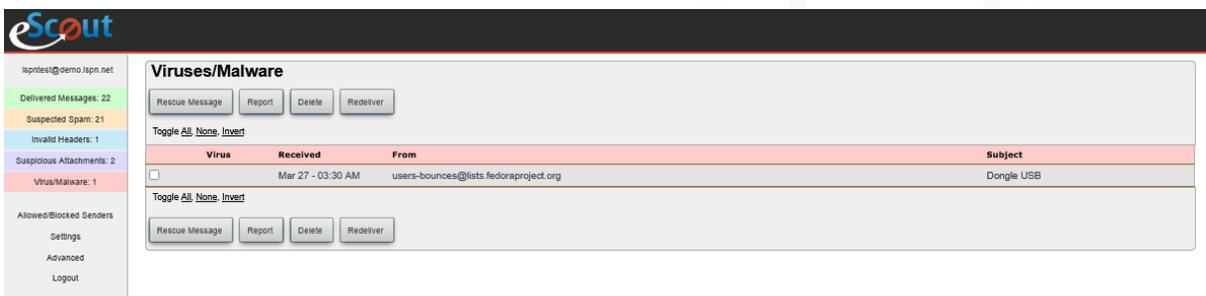   - Select one or more individual checkboxes.
   - To select all checkboxes, select the **All** option.
   - To deselect all checkboxes, select the **None** option.
   - To change any selected checkboxes to unselected and any unselected checkboxes to selected, select the **Invert** option.
3. Complete one of the following actions to manage the selected emails.
   - **Rescue Message:** Immediately delivers the message to your inbox and removes it from the spam quarantine, and informs eScout that the message is legitimate.
   - **Confirm Spam:** Immediately and permanently deletes the message and confirms to eScout that the message is spam/junk mail.
   - **Not sure - Delete:** Deletes the message permanently.
   - **Redeliver:** Immediately delivers a copy of the message to your inbox but does not remove it from the spam quarantine or provide any confirmation to train the filter.

COLORADO VALLEY Communications

Reliable Connections, Rooted in Texas

Note: These same four options are available for the Invalid Headers and Suspicious Attachments sections, which you can also select on the left pane. Messages with Virus/Malware content cannot be moved out of quarantine.

How do I manage Unconfirmed Delivered Messages?
The Unconfirmed Delivered Messages section displays all messages you received in your inbox in the last 7 days. Here, you can report spam that eScout may have missed or recover any mistakenly deleted or lost messages from the past week.

To manage emails in the **Delivered Messages** section:

1. Log in to eScout and, on the left pane, select **Delivered Messages.**
2. Use one of the following options to select the emails you want to manage
   - Select one or more individual checkboxes
   - To select all checkboxes, select the **All** option.
   - To deselect all checkboxes, select the **None** option
   - To change any selected checkboxes to unselected and any unselected checkboxes to selected, select the **Invert** option.
3. Complete one of the following actions to manage the selected emails.
   - **Confirm Non-spam:** Confirms the message as legitimate to eScout and removes it from this list.
   - **Report Spam:** Immediately and permanently deletes the message and confirms to eScout that the message is spam/junk mail.
   - **Not sure - Delete:** Deletes the message permanently from eScout without learning that the message is spam or non-spam.
   - **Redeliver:** Immediately redelivers a copy of the message to your inbox but does not remove it from the list or provide any confirmation to train the filter.

COLORADO VALLEY Communications
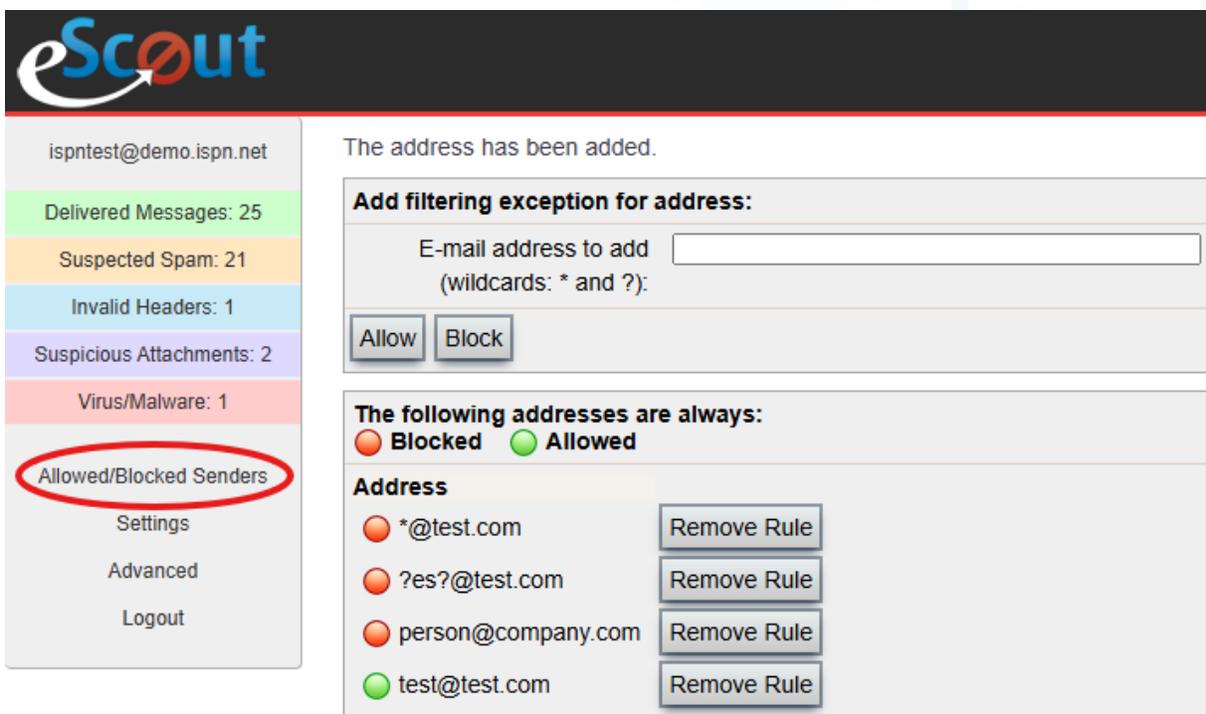Reliable Connections, Rooted in Texas

How do I allow and block senders?

If eScout is repeatedly and mistakenly quarantining messages from known domains or senders, you can add them to your Allowed Senders list to ensure that all messages are promptly delivered to your Inbox, regardless of its spam score. You can add complete email addresses, or partial matches, such as "@domain.com."

Alternately, if you receive spam in your inbox from known domains or senders, you can add them to your Blocked Senders list to ensure that no messages from these sources are delivered to your inbox.

To add an allowed or blocked sender or domain to eScout's filtering:

1. Log in to eScout and, on the left pane, select **Allowed/Blocked Senders.**

2. For **Add filtering exception for address**, enter all or part of the domain or sender you want eScout to filter.

   You can add complete email addresses or partial matches, such as "@yourdomain.com". Refer to the example image above.

   You can also include one of the following wildcard characters to broaden your filtering:
      ? = single character wildcard
      * = multiple character wildcard

3. Complete one of the following actions:
   - To ensure that eScout always delivers messages from this sender, select **Allow.**
   - To ensure that eScout never delivers messages from this sender, select **Block.**

How do I change my protection level?

By default, eScout's filtering strength is set to a moderate level. However, you can adjust the spam protection level slider bar to your suit your preferences.

For the safety of your data and identifying information, we do not recommend setting this slider bar to **Off.**

To edit your current protection level:

1. Log in to eScout, on the left pane, select **Settings.**
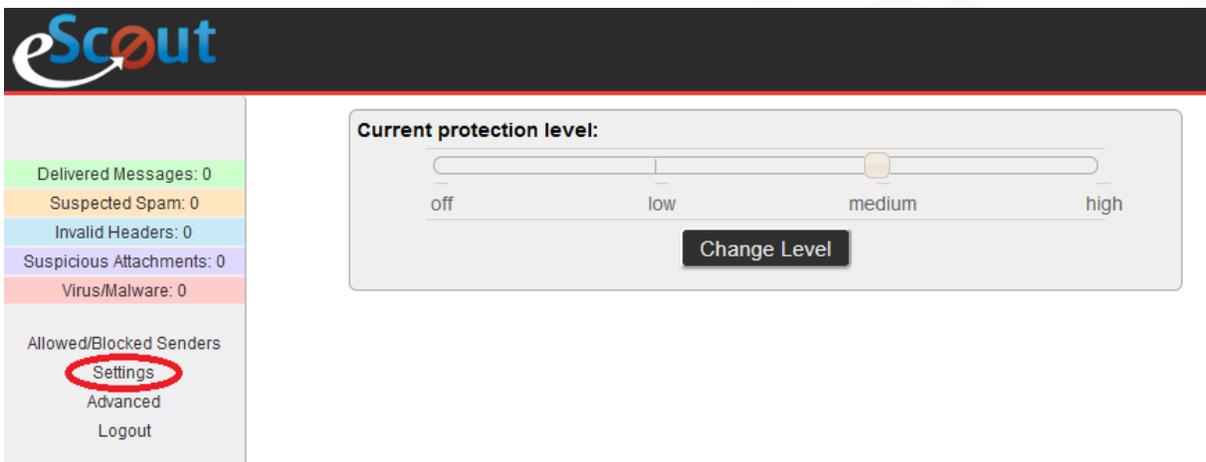
2. For **Current protection level**, click and drag the bar to the desired setting and then click the **Change Level** button when done.