Spam Quarantine

This chapter contains the following sections:

Overview of the Spam Quarantine

The Spam Quarantine (also known as ISQ) and End-User Quarantine (also known as EUQ) provides a safeguard mechanism for organizations that are concerned about "false positives" — that is, legitimate email messages that the appliance has deemed to be spam. When the appliance determines that a message is spam or suspected spam, you may want to let the recipient or an administrator review the message before delivering or deleting it. The spam quarantine stores messages for this purpose.

Administrative users of the appliance can view all messages in a spam quarantine. End users, usually the message recipients, can view their own quarantined messages in a slightly different web interface.

The spam quarantine is separate from policy, virus, and outbreak quarantines.

Related Topics

- Centralized Policy, Virus, and Outbreak Quarantines

Local Versus External Spam Quarantine

A local spam quarantine stores spam and suspect spam on the appliance . An external spam quarantine can store these messages on a separate Cisco Content Security Management appliance .

Consider using an external spam quarantine if:

- You want a centralized location to store and manage spam from multiple appliances .
- You want to store more spam than the appliance can hold.
- You want to regularly back up the spam quarantine and its messages.

Setting Up the Centralized Spam Quarantine

Procedure

	Command or Action	Purpose
Step 1	On the Security Management appliance, enable the centralized spam quarantine service.	Enabling and Configuring Spam Quarantine, on page 2
Step 2	On the Security Management appliance, specify the Email Security appliances to include in the centralized spam quarantine.	Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance , on page 6
Step 3	Set up the Security Management appliance for sending notifications and released spam.	Configuring an Outbound IP Interface on the Security Management Appliance , on page 6
Step 4	On the Security Management appliance, configure the spam quarantine browser interface.	Configuring the IP Interface for Browser Access to the Spam Quarantine , on page 7
Step 5	Ensure that the Email Security appliance is configured to send mail to the spam quarantine.	For more information about configuring anti-spam and mail policies, see the "Anti-Spam" section of the *User Guide for AysncOS for Email Security Appliances*.
Step 6	On the Email Security appliances, enable and configure the external spam quarantine.	For more information, see *User Guide for AysncOS for Email Security Appliances*.
Step 7	On the Email Security appliances, disable the local quarantine.	For information about disabling the local spam quarantine to activate the external spam quarantine, see *User Guide for AysncOS for Email Security Appliances.*

Enabling and Configuring Spam Quarantine

- Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 2

- Enabling and Configuring Spam Quarantine on the New Web Interface

Enabling and Configuring the Spam Quarantine on the Legacy Web Interface

Step 1 Select **Management Appliance > Centralized Services > Spam Quarantine**.

Step 2 If you are enabling the spam quarantine for the first time after running the System Setup Wizard:

a) Click **Enable**.

b) Review the end user license agreement, then click **Accept**.

Step 3 If you are editing spam quarantine settings, click **Edit Settings**.

Step 4   Specify options:

Option	Description
Quarantine IP Interface Quarantine Port	By default, the spam quarantine uses the Management interface and port 6025. The IP interface is the interface on the Security Management appliance that is configured to listen for incoming mail. The quarantine port is the port number that the sending appliances use in their external quarantine settings. If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.
Deliver Messages Via	All outgoing quarantine-related email (such as spam notifications and messages released from the spam quarantine) must be delivered via another appliance or server that is configured to send messages. You can route these messages through an SMTP or groupware server, or you can specify the outbound listener interface of an appliance (typically the Data 2 interface). The alternate address is used for load balancing and failover. If you have multiple appliances , you can use the outbound listener interface of any managed appliances for the primary and alternate addresses. Both must use the same interface (either Data 1 or Data 2) as the outbound listener. Read instructions on the screen for additional caveats about these addresses.
Schedule Delete After	Specify the number of days to hold messages before deleting them. Cisco recommends that you configure the quarantine to delete older messages to prevent the quarantine from filling to capacity, but you can elect not to schedule automatic deletion.
Notify Cisco Upon Message Release	Check the **Send a copy of released messages to Cisco for analysis(recommended)** checkbox if you wish to notify Cisco upon message release.

Option	Description
Spam Quarantine Appearance	**Logo**
	By default, the Cisco logo is displayed at the top of the spam quarantine page when the user logs in to view quarantined messages.
	You can view the logo on both new and legacy web interface.
	To use a custom logo instead, upload the logo. The logo should be a .jpg, .gif, or .png file that is at most 50 pixels high by 500 pixels wide.
	Login page message
	(Optional) Specify a login page message. This message is shown to end users and administrators when they log in to view the quarantine.
	If you do not specify a message, the following message appears:
	Enter your login information below. If you are unsure what to enter, please contact your administrator.
Administrative Users	See Configuring Administrative User Access to the Spam Quarantine , on page 8.

Step 5   Submit and commit your changes.

What to do next

- Return to Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance , on page 6

Enabling and Configuring Spam Quarantine on the New Web Interface

Step 1   On the Security Management Appliance, click **Service Status** and hover over the ⚙ corresponding to **Spam Quarantine**, click **Edit Spam Quarantine Settings**.

Step 2   If you are using configuring spam quarantine for the first time after running the System Setup Wizard, review and accept the license agreement and click **Proceed**.

Step 3   Click the toggle switch to enable Spam Quarantine.

Step 4   Specify options:

Option	Description
Quarantine IP Interface Quarantine Port	By default, the spam quarantine uses the Management interface and port 6025. The IP interface is the interface on the Security Management appliance that is configured to listen for incoming mail. The quarantine port is the port number that the sending appliances use in their external quarantine settings.
	If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.

Option	Description
Deliver Messages Via	All outgoing quarantine-related email (such as spam notifications and messages released from the spam quarantine) must be delivered via another appliance or server that is configured to send messages. You can route these messages through an SMTP or groupware server, or you can specify the outbound listener interface of an Email Security appliance (typically the Data 2 interface). The alternate address is used for load balancing and failover. If you have multiple Email Security appliances, you can use the outbound listener interface of any managed Email Security appliances for the primary and alternate addresses. Both must use the same interface (either Data 1 or Data 2) as the outbound listener. Read instructions on the screen for additional caveats about these addresses.
Schedule Delete After	Specify the number of days to hold messages before deleting them. Cisco recommends that you configure the quarantine to delete older messages to prevent the quarantine from filling to capacity, but you can elect not to schedule automatic deletion.
Notify Cisco Upon Message Release	You can choose to send a copy of released messages to Cisco for analysis by checking the respective box.
Spam Quarantine Appearance	**Logo** By default, the Cisco logo is displayed at the top of the spam quarantine page when the user logs in to view quarantined messages. You can view the logo on both new and legacy web interface. To use a custom logo instead, upload the logo. The logo should be a .jpg, .gif, or .png file that is at most 50 pixels high by 500 pixels wide.
	Login page message (Optional) Specify a login page message. This message is shown to end users and administrators when they log in to view the quarantine. If you do not specify a message, the following message appears: Enter your login information below. If you are unsure what to enter, please contact your administrator.
Administrative Users	See Configuring Administrative User Access to the Spam Quarantine , on page 8.

Step 5   Click **Save**.

What to do next

- Return to

Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance

The steps that you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 If you have already added the Email Security appliance to the list on this page:

a) Click the name of the Email Security appliance.

b) Select the **Spam Quarantine** service.

Step 4 If you have not yet added Email Security appliances:

a) Click Add Email Appliance.

b) In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the appliance.

> **Note** A DNS name may be entered in the IP Address text field; however, it will be immediately resolved to an IP address when you click **Submit**.

c) The Spam Quarantine service is pre-selected.

d) Click **Establish Connection.**

e) Enter the username and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.

> **Note** You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

f) Wait for the success message to appear above the table on the page.

g) Click **Test Connection**.

h) Read the test results above the table.

Step 5 Submit and commit your changes.

Step 6 Repeat this procedure for each Email Security appliance for which you want to enable the spam quarantine.

Configuring an Outbound IP Interface on the Security Management Appliance

Configure an interface on the Security Management appliance to send quarantine-related messages (including notifications and released email) to the Email Security appliance for delivery.

Before you begin

Obtain or identify an IP address to use for the outbound interface. This will typically be the Data 2 interface on the Security Management appliance. For more information about network requirements, see Assigning Network and IP Addresses

Note   Use this procedure in conjunction with the information in Configuring IP Interfaces.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > Network IP Interfaces**.

Step 3   Click **Add IP Interface**.

Step 4   Enter the following settings:

- Name

- Ethernet Port

    Typically, this will be Data 2. Specifically, this must match the data interface on the Email Security appliance that you specified for the **Primary Server** in the **Deliver Messages Via** section of the Spam Quarantine Settings page under **Management Appliance > Centralized Services > Spam Quarantine**.

- IP Address

    IP address of the interface that you just specified.

- Netmask

- Hostname

    For example, if this is the Data 2 interface, use data2.sma.example.com .

Do not enter information in the Spam Quarantine section for this interface.

Step 5   Submit and commit your changes.

Configuring the IP Interface for Browser Access to the Spam Quarantine

When administrators and end users access the spam quarantine, a separate browser window opens.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance** > **Network** > **IP Interfaces**.

Step 3   Click the name of the **Management** interface.

Step 4   In the Spam Quarantine section, configure settings for access to the spam quarantine:

- By default, HTTP uses port 82 and HTTPS uses port 83.

- Specify the URL that appears in notifications and in the spam quarantine browser window.

If you do not want to expose the hostname of your Security Management appliance to end users, you can specify an alternate hostname.

Step 5   Submit and commit your changes.

What to do next

Ensure that your DNS server can resolve the hostname that you specified for spam quarantine access.

Configuring Administrative User Access to the Spam Quarantine

All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.

If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:

- Email administrator
- Operator
- Read-only operator
- Help desk user
- Guest
- Custom user roles that have spam quarantine privileges

These users cannot access spam quarantine settings.

Before you begin

Create users or custom user roles that have access to the spam quarantine. For more information, see information about Access to Quarantines for Custom User Role in Distributing Administrative Tasks

Step 1   On the Security Management appliance , click **Service Status** and hover over the ⚙ corresponding to **Spam Quarantine** and click **Edit Spam Quarantine Settings**.

Step 2   Click the toggle switch to enable Spam Quarantine.

Step 3   Click the link for the type of user to add: local, externally authenticated, or custom role.

If you have already added users or roles, click a username or role to view all eligible users or roles.

Step 4   Select the users or roles that you want to add.

Users with Administrator privileges , including Email Administrators, are not listed because they automatically have full access to the spam quarantine.

Step 5   Click **OK**.

Step 6   Click **Submit**.

What to do next

Related Topics

Spam Quarantine Threshold Alert

You can configure to receive alert notification(s) after you set the maximum number of spam messages that can be triggered in a duration. In addition to configuring your own alerts, you can configure Cisco Secure Email and Web Manager to generate alerts either on an hourly or on a daily basis. However, you may also set the maximum number of alerts that can be received within the time duration once the threshold is crossed.

When administrators are mapped to this custom role, they can view the quarantine mails but cannot perform a release, delete, or any other operation.

Cisco Secure Email and Web Manager ensures that you receive the alerts you set as both an email and a syslog addition.

Configuring Spam Quarantine Threshold Alert Settings Using CLI

To configure spam quarantine threshold alerts, use the **spamquarantinethresholdalert** command.

Once you execute the command, you must enable the services you avail.

You must provide values for the:

- Threshold- Numeric Only. Configures threshold of new quarantined spam mails for which alerts will be sent in selected time. Values range between 1-1,00,000.

- Time Duration- Configures the duration in hours in which the spam messages are monitored. Values range between 1800 to 86400 seconds.

- Alert Limit-Numeric Only.Configures the alert limit. Value ranges from 1-20.

Procedure

	Command or Action	Purpose
Step 1	spamquarantinethresholdalert **Example:** `spamquarantinethresholdalert`	Configures the spam quarantine threshold alert.

Example

Configuring Spam Quarantine Threshold Alert Settings Using GUI

Step 1 Click **Centralized Services** > **SPAM Quarantine**

The SPAM Quarantine page is displayed.

Step 2 Enable **Threshold Alert** checkbox.

Spam Quarantine Threshold Alerts are also governed by the System Alerts settings. To configure recipients, you must navigate to **System Administration > Alerts**.

To receive these alerts, you must subscribe to system critical alerts.

Step 3   Enter the threshold value.

Step 4   Choose the **Time Duration** from the drop-down.

Value ranges between half-an-hour to 24 hours.

Step 5   Enter the **Alert Limit**.

Value ranges between 1 to 20.

Step 6   Click **Submit**.

Limiting Which Recipients Have Mail Quarantined

You can use multiple mail policies (Mail Policies > Incoming Mail Policy) to specify a list of recipient addresses for which mail will not be quarantined. Select 'Deliver' or 'Drop' instead of quarantine when configuring the anti-spam settings for the mail policy.

Spam Quarantine Language

Each user selects a language in the spam quarantine from the Options menu at the top right of the window.

Edit Spam Quarantine Page

Using Safelists and Blocklists to Control Email Delivery Based on Sender

Administrators and end users can use safelists and blocklists to help determine which messages are spam. Safelists specify senders and domains that are never treated as spam. Blocklists specify senders and domains that are always treated as spam.

You can allow end users (email users) to manage the safelist and blocklist for their own email accounts. For example, an end user may receive email from a mailing list that no longer interests him. He may decide to add this sender to his blocklist to prevent emails from the mailing list from being sent to his inbox. On the other hand, end users may find that emails from specific senders are sent to their spam quarantine when they do not want them to be treated as spam. To ensure that messages from these senders are not quarantined, they may want to add the senders to their safelists.

Changes that end users and administrators make are visible to and can be changed by either.

Related Topics

Message Processing of Safelists and Blocklists

A sender's being on a safelist or blocklist does not prevent the appliance from scanning a message for viruses or determining if the message meets the criteria for a content-related mail policy. Even if the sender of a message is on the recipient's safelist, the message may not be delivered to the end user depending on other scanning settings and results.

When you enable safelists and blocklists, the appliance scans the messages against the safelist/blocklist database immediately before anti-spam scanning. If the appliance detects a sender or domain that matches a safelist or blocklist entry, the message will be splintered if there are multiple recipients (and the recipients have different safelist/blocklist settings). For example, a message is sent to both recipient A and recipient B. Recipient A has safelisted the sender, whereas recipient B does not have an entry for the sender in the safelist or the blocklist. In this case, the message may be split into two messages with two message IDs. The message sent to recipient A is marked as safelisted with an *X-SLBL-Result-Safelist* header and skips anti-spam scanning, whereas the message bound for recipient B is scanned by the anti-spam scanning engine. Both messages then continue along the pipeline (through anti-virus scanning, content policies, and so on) and are subject to any configured settings.

If a message sender or domain is blocklisted, the delivery behavior depends on the blocklist action that you specify when you enable the safelist/blocklist feature. Similar to safelist delivery, the message is splintered if there are different recipients with different safelist/blocklist settings. The blocklisted message splinter is then quarantined or dropped, depending on the blocklist action settings. If the blocklist action is configured to quarantine, the message is scanned and eventually quarantined. If the blocklist action is configured to delete, the message is dropped immediately after safelist/blocklist scanning.

Because safelists and blocklists are maintained in the spam quarantine, delivery behavior is also contingent on other anti-spam settings. For example, if you configure the "Accept" mail flow policy in the Host Access Table (HAT) to skip anti-spam scanning, then users who receive mail on that listener will not have their safelist and blocklist settings applied to mail received on that listener. Similarly, if you create a mail flow policy that skips anti-spam scanning for certain message recipients, these recipients will not have their safelist and blocklist settings applied.

Related Topics

Enabling Safelists and Blocklists

Enabling Safelists and Blocklists on the Legacy Web Interface

Before you begin

- The spam quarantine must be enabled. See Setting Up the Centralized Spam Quarantine , on page 2.

Step 1 Navigate to **Management Appliance > Centralized Services > Spam Quarantine**.

Step 2 Under **End-User Safelist/Blocklist**, click **Edit Settings**.

Step 3 Select **Enable End User Safelist/Blocklist Feature**.

Step 4 Specify **Maximum List Items Per User**.

This is the maximum number of addresses or domains for each list, for each recipient. If you allow a large number of list entries per user, system performance might be adversely affected.

Step 5 Select **Update Frequency**.

This value determines how often AsyncOS updates the safelists/blocklists on the appliances that use the external spam quarantine. The significance of this setting is described in External Spam Quarantine and Safelist/Blocklists , on page 13.

Step 6 Submit and commit your changes.

Enabling Safelists and Blocklists on the New Web Interface

Before you begin

- The spam quarantine must be enabled. See Setting Up the Centralized Spam Quarantine , on page 2.

Step 1 On the Security Management appliance, click **Service Status** and hover over the ⚙ icon corresponding to **Spam Quarantine**.

Step 2 Click **Edit Safelist/Blocklist Settings**.

Step 3 Click the toggle switch to enable Safelist/Blocklist Settings.

Step 4 Specify the **Maximum List Items Per User**.

This is the maximum number of addresses or domains for each list, for each recipient. If you allow a large number of list entries per user, system performance might be adversely affected.

Step 5 Select **Update Frequency**.

This value determines how often AsyncOS updates the safelists/blocklists on the Email Security appliances that use the external spam quarantine. The significance of this setting is described in External Spam Quarantine and Safelist/Blocklists , on page 13.

Step 6 Click **Submit**.

External Spam Quarantine and Safelist/Blocklists

Because the appliance evaluates senders in safelists and blocklists when processing incoming mail, safelists and blocklists that are stored on a Security Management appliance must be sent to the appliance in order to be applied to incoming mail. When you configure the safelist/blocklist feature on a Security Management appliance , you configure the frequency of these updates.

Adding Senders and Domains to Safelists and Blocklists (Administrators)

Manage safelists and blocklists via the spam quarantine interface.

You can also see whether many recipients (end users in your organization) have included a particular sender or domain in allowed list or blocked list.

Administrators see and work with the superset of the same entries that each end user sees and works with.

Before you begin

- Ensure that you can access the spam quarantine. See Accessing the Spam Quarantine (Administrative Users), on page 33.

- Enable access to the safelist/blocklist. See Enabling Safelists and Blocklists on the Legacy Web Interface, on page 12.

- (Optional) To import safelist/blocklists instead of building these lists using the procedure in this section, use the process described in Backing Up and Restoring the Safelist/Blocklist , on page 19.

- Understand the required format of safelist and blocklist entries. See Syntax for Safelists and Blocklist Entries , on page 17.

Step 1   [New Web Interface Only] On the Security Management appliance, click **Quarantine** > **Spam Quarantine** > **Search**.

Or

Choose **Email** > **Message Quarantine** > **Spam Quarantine** and select the **Options** drop-down menu in the upper right corner of the page.

Step 2   Choose **Safelist** or **Blocklist**.

Step 3   (Optional) Search for a sender or recipient.

Step 4   Do one or more of the following:

To	Do This
Add multiple senders for a recipient	To add multiple senders for a recipient on the new web interface:
	a. Select **Recipient** tab.
	b. Click on the + icon to add a recipient address and sender list.
	c. Enter the recipient email address.
	d. Enter the sender email addresses and domains.
	Put each entry on a separate line, or separate each entry with a comma.
	e. Click ✓ to save the entry.
	To modify an existing sender address, select the checkbox next to the required recipient address, click the edit icon, modify the sender address and click ✓ to save the entry.
	To add multiple senders for a recipient on the legacy web interface:
	a. Select **View by: Recipient**
	b. Click **Add**, or click **Edit** for a recipient.
	c. Enter or edit the recipient email address.
	d. Enter sender email addresses and domains.
	Put each entry on a separate line, or separate each entry with a comma.
	e. Click **Submit**.

To	Do This
Add multiple recipients for a sender	To add multiple recipient for a sender on the new web interface: **a.** Select **Sender** tab. **b.** Click + to add a sender address and recipient list. **c.** Enter the sender address or domain. **d.** Enter the recipient email addresses. Put each entry on a separate line, or separate each entry with a comma. **e.** Click ✓ to save the entry. To modify an existing recipient address, select the checkbox next to the required sender address, click the edit icon, modify the sender address and click ✓ to save the entry. To add multiple recipient for a sender on the legacy web interface: **a.** Select **View by: Sender** **b.** Click **Add**, or click **Edit** for a sender. **c.** Enter or edit the sender address or domain. **d.** Enter recipient email addresses. Put each entry on a separate line, or separate each entry with a comma. **e.** Click **Submit**.
Delete all senders associated with a recipient	To delete all senders associated with a recipient on the new web interface: **a.** Select the checkbox next to the recipient or sender address to select the entry. You can select and delete all entries. **b.** Click on the trash can icon to delete an entire table row. To delete all senders associated with a recipient on the legacy web interface: **a.** Select a **View by** option. **b.** Click a trash can icon to delete an entire table row.

To	Do This
Delete all recipients associated with a sender	To delete all recipients associated with a sender on the new web interface: a. Select the checkbox next to the recepient or sender address to select the entry. You can select and delete all entries. b. Click on the trash can icon to delete an entire table row. To delete all recipients associated with a sender on the legacy web interface: a. Select a **View by** option. b. Click a trash can icon to delete an entire table row.
Delete individual senders for a recipient	To delete individual senders for a recipient on the new web interface: a. Select the checkbox next to the recepient or sender address to select the entry. You can select and delete multiple entries. b. Click on the edit icon to modify an individual recipient or sender. c. Add or remove entries from the text box. You must leave at least one entry. d. Click ✓ to save the entry. To delete individual senders for a recipient on the legacy web interface: a. Select a **View by** option. b. Click **Edit** for an individual recipient or sender. c. Add or remove entries from the text box. You must leave at least one entry. d. Click **Submit**.

To	Do This
Delete individual recipients for a sender	To delete individual recipient for a sender on the new web interface: **a.** Select the checkbox next to the recepient or sender address to select the entry. You can select and delete multiple entries. **b.** Click on the edit icon to modify an individual recipient or sender. **c.** Add or remove entries from the text box. You must leave at least one entry. **d.** Click ✓ to save the entry. To delete individual senders for a recipient on the legacy web interface: **a.** Select a **View by** option. **b.** Click **Edit** for an individual recipient or sender. **c.** Add or remove entries from the text box. You must leave at least one entry. **d.** Click **Submit**.

What to do next

Related Topics

Syntax for Safelists and Blocklist Entries

Senders can be added to safelists and blocklists using the following formats:

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

An identical entry, such as a sender address or a domain, cannot be included on both the safelist and the blocklist at the same time. However, a domain can be on a safelist while an email address for a sender belonging to that domain is on the blocklist (or vice versa), and both rules apply. For example, if *example.com* is on the safelist, *george@example.com* can be on the blocklist. In this case, the appliance delivers all mail from *example.com* without scanning for spam, except mail from *george@example.com,* which is treated as spam.

It is not possible allow or block a range of subdomains using the following syntax: *.domain.com* . However, it is possible to block a specific domain using the following syntax: *server.domain.com* .

Clearing All Safelists and Blocklists

If you need to delete all safelist and blocklist entries, including all senders and all recipients, import a file with no entries using the procedure in Backing Up and Restoring the Safelist/Blocklist , on page 19.

About End-User Access to Safelists and Blocklists

End users access their safelist and blocklist via the spam quarantine. To configure end-user access to the spam quarantine, see Setting Up End-User Access to the Spam Quarantine via Web Browser .

You may want to give your end users the URL of the spam quarantine and the instructions below, as applicable.

Related Topics

- Adding Entries to Safelists (End Users)
- Adding Senders to Blocklists (End Users)

Adding Entries to Safelists (End Users)

Note Delivery of messages from safelisted senders depends on other settings that are configured in the system. See Message Processing of Safelists and Blocklists , on page 11.

End users can add senders to safelists in two ways:

- Adding the Sender of a Quarantined Message to the Safelist , on page 18
- Adding Senders to the Safelist Without a Quarantined Message , on page 18

Adding the Sender of a Quarantined Message to the Safelist

End users can add senders to the safelist if the message has been sent to the spam quarantine.

[New Web Interface Only] Click **Release and Add to Safelist** icon to release the message and add it to the safelist.

Or

Select **Release and Add to Safelist** from the drop-down menu.

The envelope sender and the from header for the specified mail are both added to the safelist, and the released messages proceed directly to the destination queue, skipping any further work queue processing in the email pipeline.

Adding Senders to the Safelist Without a Quarantined Message

Step 1 [New Web Interface Only] Choose **Safelist**.

Step 2 [New Web Interface Only] Enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.

Step 3 [New Web Interface Only] Click ✓ to save the entry.

Step 4 Access Spam Quarantine page.

    a) Choose **Monitor > Spam Quarantine**.

    b) Select the **Options** drop-down menu in the upper right corner of the page

    c) Choose **Safelist**.

    d) From the Safelist dialog box, enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.

    e) Click **Add to List**.

Adding Senders to Blocklists (End Users)

Messages from blocklisted senders may be rejected or quarantined, depending on the safelist/blockist action settings defined by your administrator.

✎

Note You can add blocklist entries only using this procedure.

Step 1 [New Web Interface Only] Choose **Blocklist**, click the + icon and enter the domain or email address that you want to blocklist. You can enter multiple domains and email addresses, separated by commas.

Step 2 [New Web Interface Only] Click ✓ to save the entry.

Step 3 Access Spam Quarantine page.

    a) Choose **Monitor > Spam Quarantine**.

    b) Choose **Blocklist** from the **Options** drop-down menu in the upper right corner of the page.

    c) Enter the domain or email address that you want to blocklist. You can enter multiple domains and email addresses, separated by commas.

    d) Click **Add to List**.

Backing Up and Restoring the Safelist/Blocklist

Before you upgrade your appliance or run the installation wizard, you should back up the safelist/blocklist database. Safelist/blocklist information is not included in the main XML configuration file that contains your appliance configuration settings.

Safelist/blocklist entries can also be backed up along with other data on the Security Management appliance. See Backing Up Security Management Appliance Data.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Select **Management Appliance > System Administration** > **Configuration File**.

Step 3 Scroll to the **End-User Safelist/Blocklist Database (Spam Quarantine)** section.

To	Do This
Export the safelist/blocklist	Note the path and filename of the .csv file, and modify as needed. Click **Backup Now**. The appliance saves a .csv file to the /configuration directory of the appliance using the following naming convention: *slbl<serial number><timestamp>.csv*
Import the safelist/blocklist	**Caution** This process will overwrite all existing entries in safelists and blocklists for all users. Click **Select File to Restore**. Select the desired file from the list of files in your configuration directory. Select the safelist/blocklist backup file that you want to restore. Click **Restore**.

Troubleshooting Safelists and Blocklists

To troubleshoot issues with safelists and blocklists, you can view the log files or system alerts.

When an email is blocked due to safelist/blocklist settings, the action is logged in the ISQ_log files or the antispam log files. Emails that are safelisted are marked as safelisted with an *X-SLBL-Result-Safelist* header. Emails that are blocklisted are marked as blocklisted with an *X-SLBL-Result-Blocklist* header.

Alerts are sent out when the database is created or updated, or if there are errors in modifying the database or running the safelist/blocklist processes.

For more information about alerts, see Managing Alerts .

For more information about log files, see Logging .

Related Topics

Message from Safelisted Sender Was Not Delivered

Problem

Message from a safelisted sender was not delivered.

Solution

Possible causes:

- If you have multiple appliances and the sender was recently added to the safelist, then safelist/blocklists might not have been synchronized at the time the message was processed. See External Spam Quarantine and Safelist/Blocklists , on page 13 .

Configuring Spam Management Features for End Users

To	See
Understand the benefits and limitations of the different authentication methods for end-user access to spam management features.	Configuring End-User Access to the Spam Quarantine , on page 24 and subsections
Allow end users to access the spam quarantine directly via browser.	Authentication Options for End Users Accessing Spam Management Features , on page 21
Send users a notification when messages addressed to them are routed to the spam quarantine. Notifications can include links for access to the spam quarantine.	Notifying End Users About Quarantined Messages , on page 26
Allow users to specify email addresses and domains of senders whom they know to be safe, and of senders whom they know to be sending spam or other unwanted mail.	Using Safelists and Blocklists to Control Email Delivery Based on Sender , on page 10

Related Topics

- Authentication Options for End Users Accessing Spam Management Features , on page 21
- Setting Up End-User Access to the Spam Quarantine via Web Browser , on page 23
- Notifying End Users About Quarantined Messages , on page 26
- Configuring End-User Quarantine for Shared Mailbox , on page 30

Authentication Options for End Users Accessing Spam Management Features

Note Mailbox authentication does not allow users to view messages addressed to an email alias.

For End-User Spam Quarantine Access	Do This
Directly via web browser, authentication required and Via a link in a notification, authentication required	1. In the End User Quarantine Access settings, choose **LDAP,** SAML 2.0, or **Mailbox (IMAP/POP)**. 2. In the Spam Notifications settings, deselect **Enable login without credentials for quarantine access**.

For End-User Spam Quarantine Access	Do This
Directly via web browser, authentication required and Via a link in a notification, authentication not required	1. In the End User Quarantine Access settings, choose **LDAP,** SAML 2.0, or **Mailbox (IMAP/POP)**. 2. In the Spam Notifications settings, select **Enable login without credentials for quarantine access**.
Only via a link in a notification, authentication not required	In the End User Quarantine Access settings, choose **None** as the authentication method.
No access	In the End User Quarantine Access settings, deselect **Enable End-User Quarantine Access**.

Related Topics

LDAP Authentication Process

1. A user enters his or her username and passphrase into the web UI login page.
2. The spam quarantine connects to the specified LDAP server either to perform an anonymous search or as an authenticated user with the specified "Server Login" DN and passphrase. For Active Directory, you will usually need to have the server connect on the "Global Catalog port" (it is in the 6000s) and you need to create a low privilege LDAP user that the spam quarantine can bind as in order to execute the search.
3. The spam quarantine then searches for the user using the specified BaseDN and Query String. When a user's LDAP record is found, the spam quarantine then extracts the DN for that record and attempts bind to the directory using the user records' DN and the passphrase they entered originally. If this passphrase check succeeds then the user is properly authenticated, but the spam quarantine still needs to determine which mailboxes' contents to show for that user.
4. Messages are stored in the spam quarantine using the recipient's envelope address. After a user's passphrase is validated against LDAP, the spam quarantine then retrieves the "Primary Email Attribute" from the LDAP record to determine which envelope address they should show quarantined messages for. The "Primary Email Attribute" can contain multiple email addresses which are then used to determine what envelope addresses should be displayed from the quarantine for the authenticated user.

Related Topics

IMAP/POP Authentication Process

1. Depending on your mail server configuration, a user enters their username (joe) or email address (joe@example.com) and passphrase into the web UI login page. You can modify the Login Page Message to tell your users whether they should enter a full email address or just their username (see Configuring End-User Access to the Spam Quarantine , on page 24).

2. The spam quarantine connects to the IMAP or POP server and uses the entered login (either username or email address) and passphrase to try to log into the IMAP/POP server. If the passphrase is accepted then the user is considered authenticated and the spam quarantine immediately logs out of the IMAP/POP server.

3. Once the user is authenticated, the spam quarantine lists email for the user, based on the email address:

   • If you have configured the spam quarantine to specify a domain to append to bare usernames (like joe), then this domain is appended and that fully qualified email address is used to search for matching envelopes in the quarantine.

   • Otherwise, the spam quarantine uses the entered email address to search for matching envelopes.

For more information about IMAP, see the University of Washington web site:

http://www.washington.edu/imap/

SAML 2.0 Authentication Process

See section *SSO Using SAML 2.0* in the *Cisco Content Security Management Appliance Guide*

Setting Up End-User Access to the Spam Quarantine via Web Browser

Step 1 Understand the benefits and limitations of the different authentication methods for end-user access to spam management features.

Step 2 If you will authenticate end users using LDAP, configure an LDAP server profile, including the **Spam Quarantine End-User Authentication Query** settings on the **System Administration > LDAP > LDAP Server Profile** page.

Example:

```
If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the
 System Administration > SAML page.
```

Integrating With LDAP and subsections

SSO Using SAML 2.0

Step 3 Configure end-user access to the spam quarantine.

Configuring End-User Access to the Spam Quarantine , on page 24

Step 4 Determine the URL for end-user access to the spam quarantine.

Determining the URL for End-User Access to the Spam Quarantine, on page 25

What to do next

Related Topics

Configuring End-User Access to the Spam Quarantine

Administrative users can access the spam quarantine whether or not end-user access is enabled.

Before you begin

See requirements in Authentication Options for End Users Accessing Spam Management Features , on page 21.

Step 1   If you are on the legacy interface, navigate to **Management Appliance** > **Centralized Services** > **Monitor** > **Spam Quarantine** > **Edit Settings**, and then scroll down to **End-User Quarantine Access**.If you are on the new web interface, then navigate to Security Management appliance , click **Service Status** and hover on ⚙ icon and click **Edit End-User Quarantine Settings**. You will be redirected to the legacy interface.

Step 2   Select **Enable End-User Quarantine Access**.

Step 3   Specify the method to use to authenticate end users when they attempt to view their quarantined messages.

Select This Option	More Information
None	Choose this option to make the quarantined messages accessible to the end-users via links in the spam notification without additional authentication.
Mailbox (IMAP/POP)	For sites without an LDAP directory to use for authentication, the quarantine can validate user email addresses and passphrases against a standards-based IMAP or POP server that holds their mailbox.
	When logging in to the spam quarantine, end users enter their full email address and mailbox passphrase.
	If the POP server advertises APOP support in the banner, then for security reasons (i.e., to avoid sending the passphrase in the clear) the Cisco appliance will only use APOP. If APOP is not supported for some or all users then the POP server should be reconfigured to not advertise APOP.
	Select SSL if you have configured your server to use it. If users enter username only, you can specify a domain to add to automatically complete the email address. Enter the domain of the envelope for users logging in to "Append Domain to Unqualified Usernames."
LDAP	Configure LDAP settings as described in the sections referenced in the Before You Begin section of this topic.
SAML 2.0	Enable single sign-on for Spam Quarantine.
	Before using this option, make sure that you have configured all the settings on Management Appliance > System Administration > SAML page. See section *SSO Using SAML 2.0* in the *Cisco Content Security Management Appliance Guide* .

Step 4 Specify whether or not to display message bodies before messages are released.

If this box is selected, users may not view the message body via the spam quarantine page. Instead, to view the body of a quarantined message, users must release the message and view it in their mail application (such as Microsoft Outlook). You can use this feature for policy and regulation compliance — for example, if a regulation requires that all viewed email be archived.

Step 5 Submit and commit your changes.

What to do next

(Optional) Customize the page that users see when they access the spam quarantine, if you have not yet done so. See setting descriptions in Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 2.

Determining the URL for End-User Access to the Spam Quarantine

The URL that end users can use to directly access the spam quarantine is formed from the hostname of the machine and the settings (HTTP/S and port numbers) configured on the IP interface on which the quarantine has been enabled. For example, `HTTP://mail3.example.com:82`.

The end-users can now access the Spam Quarantine on the new web interface in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/euq-login`.

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/euq-login`.

  where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

Note Local and externally-authenticated users cannot log into the end-user Spam Qurantine portal.

Which Messages an End User Sees

Generally, end users see only their own messages in the spam quarantine.

Depending on the method of access (via notification or directly via web browser) and authentication method (LDAP or IMAP/POP), users may see mail for multiple email addresses in the spam quarantine.

When LDAP authentication is used, if the Primary Email attribute has multiple values in the LDAP directory, all of those values (addresses) will be associated with the user. Therefore, quarantined messages addressed to all email addresses associated with the end user in the LDAP directory are present in the quarantine.

If the authentication method is IMAP/POP, or the user accesses the quarantine directly via a notification, then the quarantine will display only messages for that user's email address (or the address to which the notification was sent).

For information about messages that are sent to aliases of which the user is a member, see Recipient Email Mailing List Aliases and Spam Notifications , on page 28.

Related Topics

- Configuring End-User Access to the Spam Quarantine , on page 24
- Recipient Email Mailing List Aliases and Spam Notifications , on page 28

Notifying End Users About Quarantined Messages

You can configure the system to send a notification email to some or all users when they have spam and suspected spam messages in the spam quarantine.

By default, spam notifications lists the end user's quarantined messages. Notifications include a link that you can use to view the quarantined messages in the spam quarantine. You can then decide whether to have the quarantined messages delivered to the inbox or to delete them.

> **Note** In cluster configurations, you can choose which users receive notifications only at the machine level.

Before you begin

- For end users to manage messages listed in notifications, they must be able to access the spam quarantine. See Configuring End-User Access to the Spam Quarantine , on page 24.

- Understand and implement the authentication options for managing spam using notifications. See Authentication Options for End Users Accessing Spam Management Features , on page 21.

- If end users receive email at multiple aliases, see Recipient Email Mailing List Aliases and Spam Notifications , on page 28.

Step 1 If you are on the legacy interface, navigate to **Management Appliance** > **Centralized Services** > **Spam Quarantine** > **Edit Settings**, and then scroll down to **Spam Notifications**. However if you are on the new web interface, navigate to

Security Management appliance , click **Service Status**, hover over the ⚙ icon, and click **Edit Spam Notification Settings**. You will be redirected to the legacy interface.

Step 2 Select **Enable Spam Notification**.

Step 3 Enter a From: address for the notifications.

Step 4 Specify the end-users whom you want to notify.

Step 5 (Optional) Customize the subject for the notification.

Step 6 (Optional) Customize the title for the notification.

Step 7 Select the default language for notifications.

Step 8 Configure the quarantine access for the end-users.

    a) Check the **Login without credentials** check box to automatically log users into the spam quarantine when they access it by clicking a link in a notification. The end-users can release messages by clicking the **Release** links in the notification. If you uncheck this option, the end-users cannot release messages by clicking the **Release** links in the notification.

This option is visible only if you choose one of the following end-user authentication methods: Mailbox (IMAP/POP), LDAP, or SAML 2.0. If you have chosen None as the authentication method, when the end-users click on the links in the spam notification, they are automatically logged into the spam quarantine.

b) Set an expiration period (in days) for the links in the notification. Enter a number between 0 and 365. These links will expire automatically after the specified period. Enter 0 if you do not want the links to expire.

(For Mailbox (IMAP/POP), LDAP, and SAML 2.0) This option is configurable only if you check the **Login without credentials** check box.

You can also set the expiration period using the **spamdigestconfig** command in the CLI.

Step 9 Customize the message body:

a) (Optional) Customize the default text and variables.

To insert a variable, place the cursor where you would like the variable inserted and then click the name of the variable in the Message Variables listing on the right. Or type in the variable.

The following message variables are expanded to the actual value for the specific end user:

- **New Message Count** (%new_message_count%)— The number of new messages since the user last logged in.

- **Total Message Count** (%total_message_count%)— The number of messages for the user in the spam quarantine.

- **Days Until Message Expires** (%days_until_expire%)

- **Quarantine URL** (%quarantine_url%)— URL to log in to the quarantine and view messages.

- **Username** (%username%)

- **New Message Table** (%new_quarantine_messages%)— A list of the user's new quarantined messages, showing sender, message subject, date, and a link to release the message. The user clicks a message subject to view the message in the spam quarantine.

- **New Message Tablewithout Subject** (%new_quarantine_messages_no_subject%) — Similar to New Message Table, but only a "View Message" link is shown in place of the subject for each message.

b) Choose whether to show or hide the links to view all the quarantined messages in a spam notification. Under **Show link to see all quarantined messages in Notification Mails**, choose **Yes** or **No** depending on your requirement.

(For Mailbox (IMAP/POP), LDAP, and SAML 2.0). This option is visible only if you check the **Login without credentials** check box (under Quarantine Access).

If you choose **Yes**, you can force the end-user to authenticate before accessing the spam quarantine. Check **Challenge Access**. This option is not available if you have chosen None as the end-user authentication method.

You can also show or hide the links using the **spamdigestconfig** command in the CLI.

c) Click **Preview Message** to verify that the message is as you want it to be.

Step 10 Select a message format (HTML, Text, or HTML/Text).

Step 11 Specify the address to which bounced notifications will be sent.

Step 12 (Optional) Select **Consolidate messages sent to the same LDAP user at different addresses**.

Step 13 Set the notification schedule.

Step 14   Submit and commit your changes.

What to do next

To ensure that end users receive these notifications, consider recommending that they add the From: address for the spam quarantine notification emails to the "allowed list" in the junk mail settings of their mail application (such as Microsoft Outlook or Mozilla Thunderbird.)

Related Topics

Recipient Email Mailing List Aliases and Spam Notifications

Notifications can be sent to each Envelope Recipient that has quarantined email, including mailing lists and other aliases. Each mailing list receives a single digest. If you send notifications to a mailing list, all subscribers to the list will receive the notification. Users who belong to multiple email aliases, or who belong to LDAP groups that receive notifications, or who use several email addresses, may receive multiple spam notifications. The following table shows example situations in which users may receive multiple notifications.

Table 1: Notifications per Address/Alias

User	Email Addresses	Aliases	Notifications
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com, admin@example.com	hr@example.com	3

If you use LDAP authentication, you can choose not to send notifications to mailing list aliases. Or, if you choose to send spam notifications to mailing list aliases, you can prevent some occurrences of multiple notifications. .

Users who access the spam quarantine by clicking a link in a notification will not see quarantined messages for any other aliases that the end-user may have, unless the appliance is using a spam quarantine alias consolidation query for email notifications. If the notification was sent to a distribution list that is expanded after processing by the appliance, then multiple recipients may have access to the same quarantine for that list.

This means that all subscribers to a mailing list will receive the notification and can log in to the quarantine to release or delete messages. In this case, end users visiting the quarantine to view messages mentioned in a notification may find that those messages have already been deleted by other users.

Note   If you do not use LDAP and you do not want your end users to receive multiple email notifications, consider disabling notifications and instead allow end users to access the quarantine directly and authenticate via LDAP or POP/IMAP.

Testing Notifications

You can test notifications by configuring a testing mail policy, and having spam quarantined for just a single user. Then, configure the spam quarantine notification settings: Select the **Enable Spam Notification** checkbox and do not select **Enable End-User Quarantine Access**. Then only the administrator configured in the **Deliver Bounced Messages To** field is notified of new spam in the quarantine.

Troubleshooting Spam Notifications

Related Topics

User Receives Multiple Notifications

Problem

A user receives multiple spam notifications for a single message.

Solution

Possible causes:

- The user has multiple email addresses and the spam message was sent to more than one of those addresses.
- The user is a member of one or more email aliases that received the spam message. To minimize duplications, and for more information, see Recipient Email Mailing List Aliases and Spam Notifications , on page 28.

Recipient Does Not Receive Notifications

Problem

Recipient is not receiving spam notifications.

Solution

- If notifications are being sent to the "Deliver Bounce Messages To:" address instead of to spam recipients, this means that spam notifications are enabled, but spam quarantine access is not enabled. See Authentication Options for End Users Accessing Spam Management Features , on page 21.
- Have the user check the junk mail settings of their email client.
- Check for issues with the appliance or server that you specified for **Deliver Messages Via** in Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 2.

Configuring End-User Quarantine for Shared Mailbox

You can now access the End-User Quarantine (EUQ) of the Shared Mailbox and perform any actions on the spam quarantined messages when an administrator enables single sign-on to access EUQ and you have delegated access to that Shared Mailbox. It reduces the workload on administrators and assists in the timely delivery of quarantined messages.

You can access EUQ to search the spam quarantine messages of the Shared Mailbox if you can log into EUQ through SAML 2.0 authentication. You can view the spam quarantined messages of your Primary Mailbox, and you can now add the Shared Mailbox to which you have access and view the spam quarantined messages of that Shared Mailbox.

EUQ allows you to add multiple Shared Mailboxes and provides an option to view, search, release, release and add to safelist, and delete the spam quarantined messages.

Related Topics

Accessing EUQ for Shared Mailbox

Before you begin:

- The administrator must register an Microsoft Azure Active Directory application to access the identity information.

  For more details on registering the Microsoft Azure Active Directory application, see Registering Azure Active Directory Application.

  - The administrator must provide the redirect Uniform Resource Identifier (URI) as the URI of their EUQ.

  - The administrator must grant user.read permission rights in Microsoft Azure Active Directory for the application to access the identity information.

- The administrator must enable single sign-on.

- The administrator must enable the account settings for SAML server.

You can access EUQ in the following ways:

- Click **your email quarantine** or **View All Quarantined Messages** link provided in the Spam Quarantine Notification mail.

- Log in to Secure Email and Web Manager EUQ using Spam Quarantine portal.

Note If multiple users access EUQ using the same browser on the same device, you might see the Shared Mailbox of the other user. Therefore, it is advised to use a private browser though it is less likely that multiple users are using the same browser on the same device.

Configuring Account Settings

Administrators must configure account settings in Secure Email and Web Manager to enable users to view quarantined messages of Shared Mailboxes. To configure Account Settings:

Step 1 [New Web Interface Only] Click ⚙ on Secure Email and Web Manager to load the legacy web interface.

Step 2 Go to **Centralised Services > System Administration > Account Settings** page.

The **Account Settings** page is displayed. By default, the Account Settings are disabled.

Step 3 Click **Enable** to configure the account settings.

The **Account Profile Settings** window is displayed.

Step 4 Select **Enable Shared Mailbox Settings** and enter the details in the following fields:

- **Profile Name:** The default name of the account profile is displayed.

- **Description:** The default description of the account profile is displayed.

- **Client ID:** Enter the client ID.

- **Tenant ID:** Enter the tenant ID.

- **Client Secret:** Enter the client secret.

- **Redirect URL:** Enter the URL to which you must be redirected.

Step 5 Submit and commit your changes.

The **Account Profile Settings** window now displays the entered account profile details.

Step 6 Click **Edit** to modify the details.

Accessing EUQ using Spam Quarantine Notification Mail

You can access EUQ using the link provided in the Spam Notification mail (with or without authentication).

To access EUQ and view the quarantined messages of the Shared Mailbox using the Spam Notification mail, perform the following steps:

Step 1 Click **your email quarantine** or **View All Quarantined Messages** link provided in the Spam Quarantine Notification mail.

[When authentication is not required] The **Spam Quarantine** page displays the quarantined messages of the Primary Mailbox, and the Shared Mailbox is not added. You can also search for any required quarantined messages.

Step 2 [When authentication is not required] Go to step 6 of the procedure.

Step 3 [Applicable for authentication only] Enter your login credentials and authenticate.

The **Permission Requested** page is displayed. Note that you are prompted to grant access permission rights only for the first time you access EUQ.

Step 4 [Applicable for authentication only] Click **Accept** to grant the access permission rights to Secure Email and Web Manager to access and view your messages.

The **Spam Quarantine** page displays the quarantined messages of the Shared Mailbox and Primary mailbox. If you do not have access to the entered Shared Mailbox, an error message is displayed, and the quarantined messages of your Primary Mailbox are displayed.

Step 5   [Applicable for authentication only] Add a Shared Mailbox. See Adding Shared Mailbox, on page 32 to add a Shared Mailbox.

Step 6   Enter the quarantined message in the **Search Messages and another random message** text box and click **Search** to search for a particular quarantined message.

The quarantined message that you searched is displayed in the **Search Results** window.

Step 7   Select the quarantined message of the Shared Mailbox from the **Search Results** window and select the actions from the **Select Actions** drop-down list.

Step 8   Click **Submit** to release or delete the quarantined messages of the Shared Mailbox.

Accessing EUQ using Spam Quarantine Portal

You can access EUQ using the Spam Quarantine portal.

To access EUQ and view the quarantined messages of the Shared Mailbox using Spam Quarantine portal, perform the following steps:

Step 1   Log in to the Spam Quarantine portal using your credentials.

Step 2   Log in to Secure Email and Web Manager EUQ with SAML account.

The **Spam Quarantine** page is displayed.

Step 3   Add a Shared Mailbox. See Adding Shared Mailbox, on page 32 to add a Shared Mailbox.

Step 4   Select the Shared Mailbox from **View Messages for Mailbox** drop-down list to see the list of quarantined messages of that Shared Mailbox.

Step 5   Enter the quarantined message in the **Search Messages and another random message** text box and click **Search** to search for a particular quarantine message.

The quarantined message that you searched is displayed in the **Search Results** window.

Step 6   Select the quarantined message of the Shared Mailbox from the **Search Results** window and select the actions from the **Select Actions** drop-down list and click **Submit** to release or delete the quarantined messages of the Shared Mailbox.

Adding Shared Mailbox

You can add a Shared Mailbox to which you have access to view the quarantined messages of that Shared Mailbox.

Note   The respective mailbox ID is displayed at the top right corner of the **Spam Quarantine** page, when you access the quarantine messages of your Primary Mailbox or Shared Mailbox.

To add a Shared Mailbox, perform the following steps:

Step 1   Click the **View Message for mailbox** drop-down list and select **Add Shared mailbox** on the Spam Quarantine page.

Step 2   Enter the name of the mailbox in **Mailbox name** and click **Add Mailbox** in the **Add Mailbox** pop-up window. Now, the Shared Mailbox is added to the **View Message for Mailbox** drop-down list.

If you do not have access to the entered Shared Mailbox, an error message is displayed.

Note that the list of added Shared Mailbox is retained in the cookie. If you are using the same browser and the cookie is available, the Shared Mailbox is retained. You have to add the Shared Mailbox again, if you log into EUQ using a different system.

Note   If the administrator disables your Shared Mailbox access, but you have already added that Shared Mailbox, then you can access it for 40 minutes until the next refresh token from Microsoft Azure is received.

When the administrator enables your access to the Shared Mailbox, you cannot add the Shared Mailbox immediately, and it takes up to 30 minutes to access it.

Managing Messages in the Spam Quarantine

This section explains how to work with messages in local or external spam quarantines.

Administrative users can see and manage all messages in the spam quarantine.

Related Topics

- Accessing the Spam Quarantine (Administrative Users), on page 33
- Searching for Messages in the Spam Quarantine, on page 33
- Viewing Messages in the Spam Quarantine, on page 34
- Delivering Messages in the Spam Quarantine, on page 35
- Deleting Messages from the Spam Quarantine, on page 35

Accessing the Spam Quarantine (Administrative Users)

Administrative users can see and manage all messages in the spam quarantine.

Accessing the Spam Quarantine (Administrative Users)

Administrative users can see and manage all messages in the spam quarantine.

Step 1   [New Web Interface Only] On the Security Management appliance, choose **Quarantine** > **Spam Quarantine** > **Search**.

Step 2   Select **Email > Message Quarantine > Spam Quarantine**, then click the **Spam Quarantine** link.

The spam quarantine opens in a separate browser window.

Searching for Messages in the Spam Quarantine

Step 1   Specify an envelope recipient.

Note   You can enter a partial address.

Step 2   Select whether the search results should match the exact recipient you entered, or whether the results should contain, start with, or end with your entry.

Step 3   Enter a date range to search through. Click the calendar icons to select a date.

Step 4   Specify a From: address, and select whether the search results should contain, match exactly, start with, or end with the value you entered.

Step 5   Click **Search**. Messages matching your search criteria are displayed below the Search section of the page.

What to do next

Related Topics

Searching Very Large Message Collections

If you have a very large collection of messages in the spam quarantine, and if your search terms are not narrowly defined, your query may take a very long time to return information, or it may time out.

You will be prompted to confirm whether you want to resubmit your search. Please note that having multiple large searches running simultaneously can impact performance.

Viewing Messages in the Spam Quarantine

The message listing shows messages in the spam quarantine. You can select how many messages are shown at one time. You can sort the display by clicking on the column headings. Click the same column again to reverse the sorting.

Click the subject of a message to view the message, including the body and headers. The message is displayed in the Message Details page. The first 20K of the message is displayed. If the message is longer, it is truncated at 20K and you can download the message via the link at the bottom of the message.

From the Message Details page you can delete a message (select **Delete**) or select **Release** to release the message. Releasing a message causes it to be delivered.

To view additional details about the message, click the **Message Tracking** link.

Note the following:

- **Viewing Messages with Attachments**

  When viewing a message that includes an attachment, the body of the message is displayed, followed by a list of attachments.

  In the new web interface, if a message includes an attachment, you can view the details of the attachment in the Attachments section of the message.

- **Viewing HTML Messages**

  The spam quarantine attempts to render an approximation of HTML-based messages. Images are not displayed.

- **Viewing Encoded Messages**

Base64-encoded messages are decoded and then displayed.

Delivering Messages in the Spam Quarantine

To release a message for delivery, click the checkbox next to the message or messages that you want to release and select **Release** from the drop-down menu. Then click **Submit**.

Click the checkbox in the heading row to automatically select all messages currently displayed on the page.

Released messages proceed directly to the destination queue, skipping any further work queue processing in the email pipeline.

Deleting Messages from the Spam Quarantine

The spam quarantine can be configured to automatically delete messages after a certain amount of time. Also, the spam quarantine can be configured to automatically delete the oldest messages once the quarantine has reached its maximum size. You may also delete messages from the spam quarantine manually.

To delete specific messages, click the checkbox next to the messages that you want to delete and then select **Delete** from the drop-down menu. Then click **Submit**. Click the checkbox in the heading row to automatically select all of the messages currently displayed on the page.

To delete all messages in the spam quarantine, disable the quarantine (see About Disabling the External Spam Quarantine , on page 35) and then click the **Delete All Messages** link. The number in parenthesis at the end of the link is the number of messages in the spam quarantine.

Disk Space for the Spam Quarantine

Available disk space for the quarantine varies by appliance model. See Viewing Disk Space, Quotas and Usage.

By default, messages in the spam quarantine are automatically deleted after a set amount of time. If the quarantine gets full, older spam is deleted. To change this setting, see Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 2.

Related Topics

About Disabling the External Spam Quarantine

If you disable the spam quarantine:

- If messages are present in the spam quarantine when it is disabled, you can opt to delete all of the messages.
- Any mail polices set to quarantine spam or suspected spam will instead be set to deliver the message. You may need to adjust mail policies on the Email Security appliance.

- To completely disable an external spam quarantine, disable it on both the appliance and the Security Management appliance .

Disabling an external spam quarantine on the appliance only does not delete the external quarantine or its messages and data.

Troubleshooting Spam Quarantine Features