Spam Quarantine

This chapter contains the following sections:

- Overview of the Spam Quarantine , on page 1
- Local Versus External Spam Quarantine , on page 1
- Setting Up the Local Spam Quarantine, on page 2
- Using Safelists and Blocklists to Control Email Delivery Based on Sender , on page 7
- Configuring Spam Management Features for End Users , on page 18
- Managing Messages in the Spam Quarantine , on page 26
- Disk Space for the Spam Quarantine , on page 28
- About Disabling the External Spam Quarantine , on page 29
- Troubleshooting Spam Quarantine Features , on page 29

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 email gateway has deemed to be spam. When the email gateway 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 email gateway 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

- Managing Spam and Graymail
- Policy, Virus, and Outbreak Quarantines

Local Versus External Spam Quarantine

A local spam quarantine stores spam and suspect spam on the email gateway. An external spam quarantine can store these messages on a separate Cisco Secure Email and Web Manager.

Consider using an external spam quarantine if:

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

Related Topics

- Disk Space for the Spam Quarantine , on page 28
- Working with an External Spam Quarantine

Setting Up the Local Spam Quarantine

The following table shows how to send messages to a Spam Quarantine

Procedure

	Command or Action	Purpose
Step 1	Enable the Anti-Spam feature if you have not yet done so.	For more information, see Managing Spam and Graymail.
Step 2	Enable and configure quarantine settings.	For more information, see Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 3.
Step 3	Adjust the disk space allocated to the spam quarantine	For more information, see Managing Disk Space
Step 4	Enable browser access to the quarantine.	For more information, see Configuring the IP Interface for Browser Access to the Spam Quarantine , on page 4
Step 5	Configure the email gateway to send spam to the quarantine.	For more information, see • Configuring a Mail Policy to Quarantine Spam , on page 6 • Limiting Which Recipients Have Mail Quarantined , on page 6
Step 6	Specify a default character encoding for messages that do not have this information in the heading.	For more information, see Ensuring That Message Text Displays Correctly , on page 6

What to do next

Related Topics

- Configuring the IP Interface for Browser Access to the Spam Quarantine , on page 4
- Configuring Administrative User Access to the Spam Quarantine , on page 5
- Configuring a Mail Policy to Quarantine Spam , on page 6
- Limiting Which Recipients Have Mail Quarantined , on page 6

• Ensuring That Message Text Displays Correctly , on page 6
• Spam Quarantine Language, on page 7

Enabling and Configuring the Spam Quarantine on the Legacy Web Interface

Procedure

Step 1 [New Web Interface Only] On the email gateway, click to load the legacy web interface.

Step 2 Select **Spam Quarantine**.

Step 3 If you have not previously enabled the spam quarantine, select **Enable Spam Quarantine**.

If you are editing spam quarantine settings, click the **Spam Quarantine** link in the Quarantine Name column of the Spam Quarantine section.

Step 4 Specify options:

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 email gateway 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 gateway (typically the Data 2 interface). The alternate address is used for load balancing and failover. If you have multiple email gateways, you can use the outbound listener interface of any managed email gateways 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. 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 5.

Step 5 Submit and commit your changes.

What to do next

- Return to Setting Up the Local Spam Quarantine, on page 2

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.

Procedure

Step 1 [New Web Interface Only] On the email gateway, click ⚙ to load the legacy web interface.

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

Step 3 Click the interface name (for this example, we will use 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 Cisco Secure Email and Web Manager 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:

- 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 Distributing Administrative Tasks

Procedure

Step 1 On the Cisco Secue Email and Web Manager, 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 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

Configuring End-User Access to the Spam Quarantine , on page 20

Configuring a Mail Policy to Quarantine Spam

Once you have enabled the spam quarantine, you can configure a mail policy to send spam or suspected spam to that quarantine. Anti-spam scanning must be enabled on the mail policy in order to send mail to the spam quarantine.

Procedure

Step 1 On the **Mail Policies > Incoming Mail Policies** page, click the link in the Anti-Spam column for the corresponding mail policy.

Step 2 In the Anti-Spam Settings section, select **Use IronPort Anti-Spam service**.

Step 3 In the Positively-Identified Spam Settings section, select **Spam Quarantine** for the **Apply This Action to Message** option.

Step 4 Configure settings for suspected spam and marketing email.

Step 5 Submit and commit your changes.

Limiting Which Recipients Have Mail Quarantined

You can use multiple mail policies on the email gateway (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.

Ensuring That Message Text Displays Correctly

AsyncOS attempts to determine the character set of a message based on the encoding that is specified in the message headers. However, if the encoding specified in the headers does not match that of the actual text, the message will not be displayed properly when viewed in the spam quarantine. This situation is more likely to occur with spam messages.

To ensure that message text displays correctly for these messages, see .

Related Topic

- Specifying a Default Encoding , on page 6

Specifying a Default Encoding

If an incoming message does not have a character set encoding specified in the headers, you can configure your email gateway to specify a default encoding.

Doing so will help ensure that these types of messages display properly in the spam quarantine. However, specifying a default encoding can cause messages in other character sets to display incorrectly. This setting applies only to messages that do not specify the encoding in the message headers. Generally, you would only set a default encoding if you expect the majority of your mail that falls into this category to be of one specific encoding.

For example, if most quarantined messages that do not specify the character set encoding in the message headers are in Japanese (ISO-2022-JP), you can set the encoding on the Scan Behavior page as **Japanese (ISO-2022-JP)**.

Procedure

Step 1 Click **Security Services** > **Scan Behavior**.

Step 2 Under Global Settings, click **Edit Global Settings**.

Step 3 From the **Encoding to use when none is specified** drop-down list, select the desired encoding type.

Step 4 Click **Submit**.

Step 5 Click **Commit Changes**.

Spam Quarantine Language

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

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 , on page 8
- Enabling Safelists and Blocklists on the Legacy Web Interface, on page 8
- External Spam Quarantine and Safelist/Blocklists , on page 9
- Adding Senders and Domains to Safelists and Blocklists (Administrators) , on page 9
- About End-User Access to Safelists and Blocklists , on page 14
- Synchronizing Safelists or Blocklists on Multiple Email Gateways (Deployments Without a Cisco Secure Email and Web Manager) , on page 16
- Backing Up and Restoring the Safelist/Blocklist , on page 16
- Troubleshooting Safelists and Blocklists, on page 17

Message Processing of Safelists and Blocklists

A sender's being on a safelist or blocklist does not prevent the email gateway 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 email gateway scans the messages against the safelist/blocklist database immediately before anti-spam scanning. If the email gateway 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 on the Legacy Web Interface, on page 8
- External Spam Quarantine and Safelist/Blocklists , on page 9

Enabling Safelists and Blocklists on the Legacy Web Interface

Before you begin

- The spam quarantine must be enabled. See Setting Up the Local Spam Quarantine, on page 2.
- Configure the email gateway to use an external safelist/blocklist. See instructions for setting up an external spam quarantine in the documentation for your email gateway.

Procedure

Step 1 [New Web Interface Only] On the email gateway, click ⚙ to load the legacy web interface.

Step 2 Navigate to **Spam Quarantine**.

Step 3 Under **End-User Safelist/Blocklist**, click **Edit Settings**.

Step 4 Select **Enable End User Safelist/Blocklist Feature**.

Step 5 Select **Quarantine** or **Delete** for the Blocklist Action.

Step 6 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 7 Select **Update Frequency**.

This value determines how often AsyncOS updates the safelists/blocklists on the email gateways that use the external spam quarantine. The significance of this setting is described in External Spam Quarantine and Safelist/Blocklists , on page 9.

Step 8 Select the update frequency. This value determines how often AsyncOS updates the safelists/blocklists on the email gateways that use the external spam quarantine. The significance of this setting is described in External Spam Quarantine and Safelist/Blocklists , on page 9.

Step 9 Submit and commit your changes.

External Spam Quarantine and Safelist/Blocklists

If you use an external spam quarantine on a Cisco Secure Email and Web Manager, the safelist/blocklist is saved on the management appliance. This gives you a single location to manage safe and blocked senders for all appliances.

Because the email gateway evaluates senders in safelists and blocklists when processing incoming mail, safelists and blocklists that are stored on a Cisco Secure Email and Web Manager must be sent to the email gateway in order to be applied to incoming mail. When you configure the safelist/blocklist feature on a Cisco Secure Email and Web Manager, you configure the frequency of these updates.

For more information about working with external safelists and blocklists on a Cisco Secure Email and Web Manager, see the topics under the *Cisco Secure Email and Web Manager User Guide*

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 26.
- Enable access to the safelist/blocklist. See Enabling Safelists and Blocklists on the Legacy Web Interface, on page 8.

- (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 16.
- Understand the required format of safelist and blocklist entries. See Syntax for Safelists and Blocklist Entries , on page 13.

Procedure

Step 1 [New Web Interface Only] On the email gateway, click **Quarantine** > **Spam Quarantine** > **Search**.

Or

Choose **Monitor** > **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 , on page 13
- Clearing All Safelists and Blocklists , on page 14

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 email gateway 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 16.

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 8.

End users can add senders to safelists in two ways:

- Adding the Sender of a Quarantined Message to the Safelist , on page 14
- Adding Senders to the Safelist Without a Quarantined Message , on page 15

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.

Procedure

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

Or

Choose **Monitor > Spam Quarantine > Safelist**.

Step 2 [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

Procedure

Step 1 [New Web Interface Only] Choose **Quarantine > Spam Quarantine > Safelist** and click the plus icon on the top right side page.

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 Optionally you can perform this task from the legacy interface:

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.

Procedure

Step 1 [New Web Interface Only] Choose **Quarantine > Spam Quarantine** .

Step 2 [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 3 [New Web Interface Only] Click ✓ to save the entry.

Step 4 Optionally you can perform this task from the legacy interface:

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**.

Synchronizing Safelists or Blocklists on Multiple Email Gateways (Deployments Without a Cisco Secure Email and Web Manager)

If you use multiple email gateways without a Cisco Secure Email and Web Manager, you may need to manually synchronize the safelist/blocklist and its configuration settings across the different email gateways.

You can export and import a .csv file using the procedure described in Backing Up and Restoring the Safelist/Blocklist , on page 16, then use FTP to upload and download the file.

Backing Up and Restoring the Safelist/Blocklist

Before you upgrade your email gateway 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.

You can also use this procedure to save a copy of the safelist/blocklist to synchronize multiple email gateways.

Procedure

Step 1 [New Web Interface Only] On the email gateway, clcik ⚙ to load the legacy web interface.

Step 2 Select **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 email gateway saves a .csv file to the /configuration directory of the email gateway using the following naming convention: *slbl<serial number><timestamp>.csv*

To	Do This
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 Alerts.

For more information about log files, see Logging.

Related Topics

- Message from Safelisted Sender Was Not Delivered , on page 17

Message from Safelisted Sender Was Not Delivered

Problem

Message from a safelisted sender was not delivered.

Solution

Possible causes:

- The message was dropped for malware or content violations. See Message Processing of Safelists and Blocklists , on page 8.
- If you have multiple email gateways 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 9 and Synchronizing Safelists or Blocklists on Multiple Email Gateways (Deployments Without a Cisco Secure Email and Web Manager) , on page 16.

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 20 and subsections
Allow end users to access the spam quarantine directly via browser.	Authentication Options for End Users Accessing Spam Management Features , on page 18
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 22
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 7

Related Topics

- Authentication Options for End Users Accessing Spam Management Features , on page 18
- Setting Up End-User Access to the Spam Quarantine via Web Browser , on page 20
- Notifying End Users About Quarantined Messages , on page 22

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,** or **Mailbox (IMAP/POP)**. 2. In the Spam Notifications settings, deselect **Enable login without credentials for quarantine access**.
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,** or **Mailbox (IMAP/POP)**. 2. In the Spam Notifications settings, select **Enable login without credentials for quarantine access**.

For End-User Spam Quarantine Access	Do This
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 , on page 19
- Configuring End-User Access to the Spam Quarantine , on page 20
- Notifying End Users About Quarantined Messages , on page 22
- Authentication Options for End Users Accessing Spam Management Features , on page 18
- About End-User Access to Safelists and Blocklists , on page 14

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

- Authentication Options for End Users Accessing Spam Management Features , on page 18

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 20).
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/

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

Procedure

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.
```

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

Configuring End-User Access to the Spam Quarantine , on page 20

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 21

What to do next

Related Topics

- Configuring End-User Access to the Spam Quarantine , on page 20
- Determining the URL for End-User Access to the Spam Quarantine, on page 21
- Which Messages an End User Sees , on page 22

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 18.

Procedure

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 Cisco Secure Email and Web Manager, 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.

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.

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 25.

Related Topics

- Configuring End-User Access to the Spam Quarantine , on page 20
- Recipient Email Mailing List Aliases and Spam Notifications , on page 25

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 20.
- Understand and implement the authentication options for managing spam using notifications. See Authentication Options for End Users Accessing Spam Management Features , on page 18.
- If end users receive email at multiple aliases, see Recipient Email Mailing List Aliases and Spam Notifications , on page 25.

Procedure

Step 1 [New Web Interface Only] On the email gateway, click ⚙ to load the legacy web interface.

Step 2 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 Cisco Secure Email and Web Manager, click **Service Status**, hover over the ⚙ icon, and click **Edit Spam Notification Settings**. You will be redirected to the legacy interface.

Step 3 Select **Enable Spam Notification**.

Step 4 Enter a From: address for the notifications.

Step 5 Specify the end-users whom you want to notify.

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

Step 7 (Optional) Customize the title for the notification.

Step 8 Select the default language for notifications.

Step 9 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 10 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 11 Select a message format (HTML, Text, or HTML/Text).

Step 12 Specify the address to which bounced notifications will be sent.

Step 13 (Optional) Select **Consolidate messages sent to the same LDAP user at different addresses**.

Step 14 Set the notification schedule.

Step 15 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 , on page 25
- Testing Notifications, on page 25
- Troubleshooting Spam Notifications , on page 25

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. See Spam Quarantine Alias Consolidation Queries.

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 , on page 26

- Recipient Does Not Receive Notifications , on page 26
- User Receives Multiple Notifications , on page 26
- Recipient Does Not Receive Notifications , on page 26

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 25.

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 18.
- Have the user check the junk mail settings of their email client.

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 26
- Searching for Messages in the Spam Quarantine, on page 27
- Viewing Messages in the Spam Quarantine, on page 27
- Delivering Messages in the Spam Quarantine, on page 28
- Deleting Messages from the Spam Quarantine, on page 28

Accessing the Spam Quarantine (Administrative Users)

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

Procedure

Step 1 [New Web Interface Only] Choose **Quarantine** > **Spam Quarantine** > **Search**.

Step 2 Select **Monitor** > **Spam Quarantine**, then click the number in the Messages column.

Searching for Messages in the Spam Quarantine

Procedure

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, on page 27

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.

- **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 29) 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

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.

Related Topics

- Managing Disk Space

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 .
- To completely disable an external spam quarantine, disable it on both the email gateway and the Cisco Secure Email and Web Manager.

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

Troubleshooting Spam Quarantine Features

- Troubleshooting Safelists and Blocklists, on page 17
- Troubleshooting Spam Notifications , on page 25
- Ensuring That Message Text Displays Correctly , on page 6