



Spam Quarantine

This chapter contains the following sections:

- [Overview of the Spam Quarantine](#) , page 1
- [Local Versus External Spam Quarantine](#) , page 1
- [Setting Up the Centralized Spam Quarantine](#) , page 2
- [Edit Spam Quarantine Page](#), page 8
- [Using Safelists and Blocklists to Control Email Delivery Based on Sender](#) , page 8
- [Configuring Spam Management Features for End Users](#) , page 15
- [Managing Messages in the Spam Quarantine](#) , page 22
- [Disk Space for the Spam Quarantine](#) , page 24
- [About Disabling the External Spam Quarantine](#) , page 24
- [Troubleshooting Spam Quarantine Features](#) , page 24

Overview of the Spam Quarantine

The spam quarantine (also known as ISQ, End-User Quarantine, and 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 Email Security 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.

Local Versus External Spam Quarantine

A local spam quarantine stores spam and suspect spam on the Email Security 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 Email Security appliances.
- You want to store more spam than the Email Security appliance can hold.
- You want to regularly back up the spam quarantine and its messages.

Setting Up the Centralized Spam Quarantine


DETAILED STEPS

	Command or Action	Purpose
Step 1	On the Security Management appliance, enable the centralized spam quarantine service.	Enabling and Configuring the Spam Quarantine , on page 3
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 5
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 5
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 6
Step 5	Ensure that the Email Security appliance is configured to send mail to the spam quarantine.	In the documentation for your Email Security appliance, see information about configuring anti-spam and mail policies. Links to relevant sections are in the table in the section on setting up a local spam quarantine.
Step 6	On the Email Security appliances, enable and configure the external spam quarantine.	See the documentation for your Email Security appliance.
Step 7	On the Email Security appliances, disable the local quarantine.	See information about disabling the local spam quarantine to activate the external spam quarantine in the documentation for your Email Security appliance.

Enabling and Configuring the Spam Quarantine



Note If you use an external spam quarantine, you will configure the settings described in this section on the Security Management appliance.

- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 3** If you are enabling the spam quarantine for the first time after running the System Setup Wizard:
- Click **Enable**.
 - Review the end user license agreement, then click **Accept**.
- Step 4** If you are editing spam quarantine settings, click **Edit Settings**.
- Step 5** Specify options:

Option	Description
Quarantine IP Interface Quarantine Port	<p>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.</p> <p>If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.</p>
Deliver Messages Via	<p>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.</p> <p>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).</p> <p>The alternate address is used for load balancing and failover.</p> <p>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.</p> <p>Read instructions on the screen for additional caveats about these addresses.</p>

Option	Description
Quarantine Size	<p>If you deselect When storage space is full, automatically delete oldest messages first, newer messages will not be added to a full quarantine. Cisco recommends that you enable this option so that a full quarantine will not cause messages to queue (back up) on your appliance.</p> <p>To manage disk space for your quarantine, see Managing Disk Space .</p>
Schedule Delete After	<p>Specify the number of days to hold messages before deleting them.</p> <p>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.</p>
Notify Cisco Upon Message Release	—
Spam Quarantine Appearance	<p>Logo</p> <p>By default, the Cisco logo is displayed at the top of the spam quarantine page when the user logs in to view quarantined messages.</p> <p>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.</p> <p>Login page message</p> <p>(Optional) Specify a login page message. This message is shown to end users and administrators when they log in to view the quarantine.</p> <p>If you do not specify a message, the following message appears:</p> <p>Enter your login information below. If you are unsure what to enter, please contact your administrator.</p>
Administrative Users	See Configuring Administrative User Access to the Spam Quarantine , on page 7.


Step 6 Submit and commit your changes.

What to Do Next

- Return to [Setting Up the Centralized Spam Quarantine](#) , on page 2

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 Cloud Email Security Management Console, click on the gear  icon 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:
- Click the name of the Email Security appliance.
 - Select the **Spam Quarantine** service.
- Step 4** If you have not yet added Email Security appliances:
- Click Add Email Appliance.
 - 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**.
 - The Spam Quarantine service is pre-selected.
 - Click **Establish Connection**.
 - Enter the username and password 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.
 - Wait for the success message to appear above the table on the page.
 - Click **Test Connection**.
 - Read the test results above the table.
- Step 5** Click **Submit**.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable the spam quarantine.
- Step 7** Commit your changes.
-

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](#)

-
- Step 1** Use this procedure in conjunction with the information in [Configuring IP Interfaces](#)
- Step 2** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 3** Choose **Management Appliance > Network IP Interfaces**.
- Step 4** Click **Add IP Interface**.
- Step 5** 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 6** 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 Cloud Email Security Management Console, click on the gear  icon 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**
- Step 5** 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 6 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** If you are not already editing the spam quarantine settings page:
- a) [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
 - b) Choose **Management Appliance > Centralized Services > Spam Quarantine**.
 - c) Click **Edit Settings** the **Spam Quarantine** link in the Quarantine Name column of the Spam Quarantine section.
- Step 2** 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 3** 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 4 Click **OK**.

Step 5 Submit and commit your changes.

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.

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.

Enabling Safelists and Blocklists

Before You Begin

- The spam quarantine must be enabled. See [Setting Up the Centralized Spam Quarantine](#), on page 2.
- Configure the Email Security appliance to use an external safelist/blocklist. See instructions for setting up an external spam quarantine in the documentation for your Email Security appliance.

Step 1

[New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.

Step 2

Choose **Management Appliance > Centralized Services > Spam Quarantine**.

Step 3

In the **End-User Safelist/Blocklist (Spam Quarantine)** section, select **Enable**.

Step 4

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

Step 5

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 6

Submit and commit your changes.

External Spam Quarantine and Safelist/Blocklists

Because the Email Security 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 Email Security 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 whitelisted or blacklisted a particular sender or domain.

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 22.
- Enable access to the safelist/blocklist. See [Enabling Safelists and Blocklists](#), on page 9.
- (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 13.
- Understand the required format of safelist and blocklist entries. See [Syntax for Safelists and Blocklist Entries](#), on page 11.

-
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click **Quarantine > Spam Quarantine**. You must login to the legacy web interface again.
- Step 2** Click on the spam quarantine link.
- Step 3** Select the **Options** drop-down menu in the upper right corner of the page.
- Step 4** Choose **Safelist** or **Blocklist**.
- Step 5** (Optional) Search for a sender or recipient.
- Step 6** Do one or more of the following:

To	Do This
Add multiple senders for a recipient	<ol style="list-style-type: none"> 1 Select View by: Recipient 2 Click Add, or click Edit for a recipient. 3 Enter or edit the recipient email address. 4 Enter sender email addresses and domains. Put each entry on a separate line, or separate each entry with a comma. 5 Click Submit.

To	Do This
Add multiple recipients for a sender	<ol style="list-style-type: none"> 1 Select View by: Sender 2 Click Add, or click Edit for a sender. 3 Enter or edit the sender address or domain. 4 Enter recipient email addresses. Put each entry on a separate line, or separate each entry with a comma. 5 Click Submit.
Delete all senders associated with a recipient Delete all recipients associated with a sender	<ol style="list-style-type: none"> 1 Select a View by option. 2 Click a trash can icon to delete an entire table row.
Delete individual senders for a recipient Delete individual recipients for a sender	<ol style="list-style-type: none"> 1 Select a View by option. 2 Click Edit for an individual recipient or sender. 3 Add or remove entries from the text box. You must leave at least one entry. 4 Click Submit.

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 13.

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](#), on page 17.

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

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

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

-
- Step 1** From the spam quarantine, select the checkbox next to the message.
 - Step 2** Choose **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** Access the spam quarantine via browser.
 - Step 2** Select the **Options** drop-down menu in the upper right corner of the page.
 - Step 3** Choose **Safelist**.
 - Step 4** From the Safelist dialog box, enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.
 - Step 5** Click **Add to List**.
-

Adding Senders to Blocklists (End Users)

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


Note


You can add blocklist entries only using this procedure.

-
- Step 1** Log in to the spam quarantine.
 - Step 2** Select the **Options** drop-down menu in the upper right corner of the page.
 - Step 3** Enter the domain or email address that you want to blocklist. You can enter multiple domains and email addresses, separated by commas.
 - Step 4** 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 Cloud Email Security Management Console, click on the gear  icon 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	<p>Note the path and filename of the .csv file, and modify as needed.</p> <p>Click Backup Now.</p> <p>The appliance saves a .csv file to the /configuration directory of the appliance using the following naming convention:</p> <p><i>sbl<serial number><timestamp>.csv</i></p>

To	Do This
Import the safelist/blocklist	<p>Caution This process will overwrite all existing entries in safelists and blocklists for all users.</p> <p>Click Select File to Restore.</p> <p>Select the desired file from the list of files in your configuration directory.</p> <p>Select the safelist/blocklist backup file that you want to restore.</p> <p>Click Restore.</p>

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](#).

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 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 9.

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 17 and subsections
Allow end users to access the spam quarantine directly via browser.	Authentication Options for End Users Accessing Spam Management Features , on page 15
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 19
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 8

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	<ol style="list-style-type: none"> 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.
Directly via web browser, authentication required and Via a link in a notification, authentication not required	<ol style="list-style-type: none"> 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.

For End-User Spam Quarantine Access	Do This
No access	In the End User Quarantine Access settings, deselect Enable End-User Quarantine Access .

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.

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 17).
- 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

DETAILED STEPS


	Command or Action	Purpose
Step 1	Understand the benefits and limitations of the different authentication methods for end-user access to spam management features.	See section <i>SSO Using SAML 2.0</i> in the <i>Cisco Content Security Management Appliance Guide</i>
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 17
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 18

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 15.

-
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Select **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 3** Click **Edit Settings** .
- Step 4** Scroll down to the **End-User Quarantine Access** section.
- Step 5** Select **Enable End-User Quarantine Access**.
- Step 6** Specify the method to use to authenticate end users when they attempt to view their quarantined messages.

Select This Option	More Information
None	—

Select This Option	More Information
Mailbox (IMAP/POP)	<p>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.</p> <p>When logging in to the spam quarantine, end users enter their full email address and mailbox passphrase.</p> <p>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.</p> <p>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.”</p>
LDAP	Configure LDAP settings as described in the sections referenced in the Before You Begin section of this topic.
SAML 2.0	<p>Enable single sign-on for Spam Quarantine.</p> <p>Before using this option, make sure that you have configured all the settings on Management Appliance > System Administration > SAML page. See section <i>SSO Using SAML 2.0</i> in the <i>Cisco Content Security Management Appliance Guide</i> .</p>

- Step 7** 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 8** 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 page 3.

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.

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 20.

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 list the user's quarantined messages. Notifications can also include a link that users can click in order to view their quarantined messages in the spam quarantine. These links do not expire. The user can view the quarantined messages and decide whether to have them delivered to their inbox or 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 17.
- Understand the authentication options for managing spam using notifications. See [Authentication Options for End Users Accessing Spam Management Features](#) , on page 15.
- If end users receive email at multiple aliases, see [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 20.

Step 1

[New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.

Step 2

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

Step 3

Click **Edit Settings** .

Step 4

Scroll down to the **Spam Notifications** section.

Step 5

Select **Enable Spam Notification**.

Step 6

Specify options.

To 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 Table without 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) If you have enabled an authentication method in the End User Quarantine Access section on this page:

- To automatically log users in to the spam quarantine when they access it by clicking a link in a notification, select **Enable login without credentials for quarantine access**. End users can release messages simply by clicking "Release" links in the notification.
- To require users to log in to the spam quarantine when they access it by clicking a link in a notification, deselect this option. End users cannot release messages simply by clicking "Release" links in the notification.

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

Step 7 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 "whitelist" in the junk mail settings of their mail application (such as Microsoft Outlook or Mozilla Thunderbird.)

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

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 20.

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 15.
- 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 page 3.

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.

Accessing the Spam Quarantine (Administrative Users)

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

Accessing the Spam Quarantine (Administrative Users)

-
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, choose **Quarantine > Spam Quarantine**. The spam quarantine opens in a separate browser window.
- 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.
-

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 24) 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 page 3.

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 policies 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 Email Security appliance and the Security Management appliance.

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

Troubleshooting Spam Quarantine Features

- [Troubleshooting Safelists and Blocklists](#), on page 14
- [Troubleshooting Spam Notifications](#), on page 21