Email Quarantine Administrator and Deployment Guide

Email Security .cloud Portal

Symantec.cloud

Email Quarantine Administration and Deployment Guide

Documentation version: Phase 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support** > **Contact us**.

Contents

Chapter 1

Managing email quarantine

This chapter includes the following topics:

Overview of Email Quarantine settings

The spam mail that the Anti-Spam service detects (along with email blocked by Data Protection or Image Control policies, if your company uses these) is held in

Email Quarantine. From there the mail can be viewed, released to the original recipient's inbox, or deleted. Depending on the deployment policy that you choose, individual users or other nominated individuals can handle the messages in Email Quarantine. The emails in Email Quarantine can be reviewed regularly or checked only occasionally for specific messages.

Quarantine settings can be defined to apply at a global or domain level. The quarantine settings that you can define within the portal are described in the following table.

Table 1-1 Email quarantine settings

Quarantine settings	More information
Specifying notifications	When you create a new account, you can specify whether a welcome message is generated and summary notifications are enabled. Notifications provide information to your users and ask them to register with and log on to Email Quarantine. You can also specify whether the users should receive active summary notifications. Such notifications contain **Release** links to release the email directly from the notification. See "Configuring Email Quarantine notifications" on page 9. See "Email Quarantine user notification controls" on page 10. See "Email Quarantine notification content and frequency" on page 10.
Defining a default language for Email Quarantine notifications	Specify the default language for the content of welcome messages and notifications. See "Configuring Email Quarantine notifications" on page 9.
Defining Quarantine Administrators	Quarantine Administrators are users of Email Quarantine who have extended privileges to perform administrative functions in Email Quarantine. See "Defining Quarantine Administrators" on page 15.
Approved sender request facility	Specify whether your users can request that senders of suspect emails can be added to the organization's global approved senders list. See "Configure Email Quarantine approved sender requests" on page 12.

Table 1-1 Email quarantine settings *(continued)*

Quarantine settings	More information
Aliases	Specify whether your Email Quarantine users are informed when the Quarantine Administrator in Email Quarantine creates aliases. For example, if a user has multiple email addresses, each with their own Email Quarantine account, they can be aliased to a single account. The spam that is sent to any of their email addresses is managed using a single Email Quarantine account. See "Notifying Email Quarantine users when an alias is changed" on page 15.
Password controls	Password controls are used to enable and enforce your password policy for Email Quarantine. You can select from three default templates to form the basis for a password policy. See "Defining Email Quarantine password controls" on page 16. See "About Email Quarantine password policies" on page 17.
Acceptable Use Policy	You can make your Acceptable Use Policy (AUP) available online for your users to read by a link in Email Quarantine and also in summary notifications. See "Making your Email Quarantine Acceptable Use Policy available" on page 21.
Visibility	You can control the access that your users have to the information in their quarantined emails. You can select the following: ■ Users can view the subject lines of the emails in Email Quarantine ■ Users can preview the message content in Email Quarantine ■ Users can delete messages within Email Quarantine ■ Include subject line in summary notifications Users can delete, approve or block messages directly from summary notifications Summary notifications are also known as digest notifications. See "Defining what is visible in Email Quarantine summary notifications" on page 21.

Note: Depending on your organization's configuration of the Anti-Spam, Data Protection, or Image Control service, you may not have access to the quarantine service. If you do not, the **Email Quarantine** pages are not visible in the portal. For further details, contact the Support team.

Configuring Email Quarantine notifications

When you create an account, you can specify whether a welcome message is generated and whether summary notifications are enabled. Welcome messages ask users to register with and log on to Email Quarantine.

Summary notifications contain a list of emails quarantined because they violated spam, data protection or image control policies. They may provide a link for the user to log on to Email Quarantine to view them. Active summary notifications (previously called Active Digest notifications) contain **Release** links. Release links allow users to release an email directly from a summary notification without repeatedly logging on to Email Quarantine. Active summary notifications may also allow users to delete messages and to block or allow individual domains and senders. If User Settings are enabled, the **Envelope Sender** link enables users to add the address to an allowed or blocked senders list.

If welcome messages and notifications are not sent, the Email Quarantine deployment is silent. That is, a designated Quarantine Administrator accesses the user's Email Quarantine account on the user's behalf.

To configure Email Quarantine notifications

1. Select **Services** > **Email Services** > **Email Quarantine** and navigate to the **New Account Defaults** section.
2. In the **Notifications** area, check **Users receive welcome messages and summary notifications** to enable this feature.

   Typically, this setting to send welcome messages and summary notifications is applied to all new accounts that are created in Email Quarantine. This notification setting can be overridden when a Quarantine Administrator creates an account. Also, where notifications are enabled for an Email Quarantine user's account, that user may also be able to switch notifications off themselves. You can permit new users to override these notification settings if required.
3. If you have selected to send notifications, specify the time zone, frequency, and time of day at which notifications are sent.

Note: This setting only affects the default configuration for new accounts. If this setting is changed after the activation of Email Quarantine, it does not affect existing accounts.

---

4 Specify the default language for the welcome messages and notifications that Email Quarantine sends. If a user selects a different language for the Email Quarantine display, the default setting for notifications is overridden. Email Quarantine is not associated with a specific domain or client. Email Quarantine can detect the appropriate language for the logon screen using the web browser's localization settings.

5 Click **Save and Exit**.

See "Email Quarantine user notification controls" on page 10.

See "Email Quarantine notification content and frequency" on page 10.

Email Quarantine user notification controls

The Email Quarantine **Users can override notification defaults** setting determines whether users can override the default notification setting. If the setting is enabled, users are given notification options in their Email Quarantine accounts.

Note: This setting only affects the default configuration for new accounts and does not affect existing accounts.

To permit users to override default notification settings

1 Select **Services** > **Email Services** > **Email Quarantine**.

2 Navigate to the **New Account Defaults** section.

Check the **Users can override notification defaults** checkbox to permit users to modify their notification settings, if required.

See "Configuring Email Quarantine notifications" on page 9.

Email Quarantine notification content and frequency

The notification content setting allows users to receive active summary notifications. Active summary notifications enable users to release blocked emails directly into their inbox from the notifications without continually logging on to Email Quarantine. You can also elect to allow users to delete messages and to block or approve individual senders and domains directly from the notification email.

When active summary notifications are enabled, the notification email that is sent contains the same information as the regular Email Quarantine notification: subject line, date, and envelope sender—the sender's actual email address, rather than the Reply-To address. If User Settings are enabled on your domain, click the link

to add this envelope sender address to your allowed or blocked senders lists if required. A **Release** link appears next to each spam email.

If a user receives active summary notifications, you can disable access to their Email Quarantine accounts. An account is still created for them, which a Quarantine Administrator can manage, but the user need have no visibility of it. If access to Email Quarantine accounts is disabled, those users' notifications do not contain a link to log on to Email Quarantine.

The **Release** link in active summary notifications is only displayed in notifications where email clients allow HTML. This is especially pertinent on mobile devices. If this setting is enabled for users without HTML email, their notifications do not contain the Release link. In this case, it is advisable to let users access their Email Quarantine accounts or designate a Quarantine Administrator to manage their spam email.

For security reasons, a user can only release an email once from an active summary notification. It prevents a malicious user from releasing an email multiple times, thereby performing a denial of service (DoS) attack. The email can be released multiple times from Email Quarantine. Or the Quarantine Administrator can release it on behalf of the user.

Active summary notifications can be set for the whole organization or per domain. By default, active summary notifications are disabled.

To enable active summary notifications

1. Select **Services** > **Email Services** > **Email Quarantine** and navigate to the **New Account Defaults** section.
2. In the **Notifications** area, ensure the box **Users receive welcome messages and summary notifications** is checked.
3. Specify the **Summary notification frequency** by selecting an hourly, multi-hourly or daily interval, and then specifying the time of day.
4. In the **Notification content** section, ensure the box **Users can release and delete emails directly from notifications** is checked.
5. Define whether or not users can access Email Quarantine using the **Disable access to Email Quarantine for users** checkbox.
6. Specify whether users can send an email request to approve a sender.
7. Click **Save and Exit**.

See "Configuring Email Quarantine notifications" on page 9.

See "Troubleshooting Email Quarantine active summary notifications" on page 12.

Configure Email Quarantine approved sender requests

You can configure Email Quarantine to let users request that the sender of an email that is identified as spam is added to the organization's global approved senders list. Then, the user has the option to request an approved sender when they release the email from Email Quarantine.

Note: If your users control their own approved and blocked senders lists at user level in Email Quarantine, the **Approved sender request facility** does not need to be enabled.

Configure approved sender requests

1. Select **Services** > **Email Services** > **Email Quarantine**.
2. Navigate to the **New Account Defaults** section, and check the **Email Quarantine users can send an email request to approve a sender** option.
3. Enter the email address that handles the approved sender requests.

   This address should be the address of the person who is responsible for managing the approved senders lists in the portal.
4. Click **Save & Exit**.

   The address is validated to check that it is a valid email address format and has a domain that belongs to you.

See "Overview of Email Quarantine settings" on page 6.

Troubleshooting Email Quarantine active summary notifications

Table 1-2 Troubleshooting active summary notifications

Issue	Answer
A user has tried to release an email, but is directed to the Email Quarantine logon page	The user's Email Quarantine account may have been deleted. The user can still have an active summary notification in their inbox. If a release link is clicked, Email Quarantine detects that there is no such account and redirects them to the logon page.
A user receives standard notification emails instead of active ones	If a new user has never logged into Email Quarantine and set up a password, they receive the standard notification. Once they log on for the first time, the user will receive active summary notifications in future.

Table 1-2 Troubleshooting active summary notifications *(continued)*

Issue	Answer
Some entries in a user's active summary notification do not have a release link	If you enable active summary notifications in the portal before a scheduled notification is sent out, some emails do not have the release link. This is because the emails were flagged as unwanted before the feature was enabled and the release link was not assigned to them. All subsequent emails within the active summary notifications contain the release link.
A Email Quarantine Quarantine Administrator clicks the release link for another user's account and a message says that the email has been deleted.	If the email has not been deleted from Email Quarantine, it is likely that the Administrator revoked access for that user's account since the active summary notification was sent out.
A user's email cannot be released	■ The email has already been deleted. ■ The quarantine period has expired. ■ The user's access permissions have been revoked. ■ Active summary notifications have been disabled since the notification was sent, or some other change to the Email Quarantine configuration has been made that causes the release not to be possible.

See "Email Quarantine notification content and frequency" on page 10.

See "Configuring Email Quarantine notifications" on page 9.

See "Settings that affect delivery of Email Quarantine messages and notifications" on page 13.

Settings that affect delivery of Email Quarantine messages and notifications

The matrix that follows shows the interactions between the configuration settings that affect delivery of email quarantine welcome messages and summary notifications.

Table 1-3 Settings that affect delivery of messages and notifications

Users receive welcome messages and summary notifications	Users can release or delete emails from active notifications (AD)	Address Registration (AR)[1]	Auto Account Creation (AC)	Does Symantec send the welcome email to quarantine users?	Does Symantec send the summary notification?	Comments
On	Off	On	No	Yes	Phase 1:[2] No Phase 2: Yes	See [3]
On	Off	Off	No	Yes	Yes*	See [4]
On	On	On	Yes	Phase 1: No Phase 2: Yes	Yes	See [5]
On	On	Off	No	Phase 1: No Phase 2: Yes	Phase 1: No Phase 2: Yes*	See [6]
Off	On	On	Yes	No	No	N/A
Off	On	Off	No	No	No	N/A

[1] The Email Quarantine service has been released in two phases. Phase 1 included the transition from Spam Manager to Email Quarantine. Phase 2 includes the transition from Message Manager to Email Quarantine, the relocation of the **Email Quarantine** page, and the addition of quarantine for Data Protection and Image Control.

[2] Configure on the **Services > Email Services > Platform > Address Registration** page.

[3] If AD is OFF then account is not created automatically (AC). If AR is on then Email Security.cloud portal administrators register end users and Symantec sends summary notifications without active notification links.

[4] *Summary notifications are sent if the recipient follows the instructions in the welcome email to register for the quarantine account. If AD and AR are off then the

account is not created automatically and no notification is sent. Welcome email is still sent.

[5] Symantec sends welcome email and Active Digest summary notifications.

[6] *If AD is on and AR is off then there is no automatic account creation (AC) and no notification, but welcome email is sent.

See "Troubleshooting Email Quarantine active summary notifications" on page 12.

Notifying Email Quarantine users when an alias is changed

Aliases are used to:

- Direct all quarantined email that is sent to a user with multiple email addresses to a single Email Quarantine account.
- Manage quarantined email sent to a distribution list email address, using a single Email Quarantine account.

By their nature, aliases operate in the background and users check any quarantined messages using Email Quarantine as required. If Quarantine Administrators make any changes to aliases, it may be useful for the users who are affected to be made aware of those changes.

To notify users when a change is made to an alias

1. Select **Services** > **Email Services** > **Email Quarantine**.
2. In the **Aliases** section, check the box **Users are always informed when administrators change settings which affect their aliases**.
3. Click **Save and Exit**.

Defining Quarantine Administrators

Quarantine Administrators are users of Email Quarantine who have extended privileges. These privileges allow them to perform some administrative functions in Email Quarantine, including:

- Viewing details of Email Quarantine accounts
- Creating accounts
- Deleting accounts
- Creating aliases and account groups to direct the spam of a distribution list or group of users to a single account

- Logging on to another user's Email Quarantine account and managing their spam.

You can enter up to 100 Quarantine Administrator email addresses.

To define Quarantine Administrators

1. Select **Services** > **Email Services** > **Email Quarantine** and navigate to the **Administrators** section.
2. Enter each email addresses of your organization's Quarantine Administrators and click **Add**. Multiple addresses must be separated with a semi-colon.

Note: The Email Quarantine User and Administrator Guide describes the Quarantine Administrator role and tasks.

Defining Email Quarantine password controls

This procedure describes how to ensure that all newly created users must change their passwords when they first use the service. It also explains how to force an individual user to change their password.

To define Email Quarantine password controls

1. Select **Services** > **Email Services** > **Email Quarantine** and navigate to the Password Controls section.
2. To force an individual user to change their password, enter their email address in the box, and select the **Single account password change** option. You must then click the **Change** option to ensure the password change is enforced.

   When the change is successful, a confirmation message is displayed to confirm that the "Single account password has been changed".
3. To force all users to change their passwords when they next log on, select the **All accounts password change** option. You must then click the **Change** button to ensure the password change is enforced.

   A warning pop-up is displayed to confirm your choice: "This will reset the passwords on all accounts. Do you wish to continue?" Select **OK** to continue, or **Cancel**. If you select OK and the changes are successful, a confirmation message is displayed to confirm that "All account passwords have been changed."
4. Use the **Unlock passwords** search tool to unlock any locked accounts.
5. Once you have completed all of the configuration items on this screen, select **Save & Exit**.

See “Configure an Email Quarantine password policy” on page 19.

About Email Quarantine password policies

Password controls are used to enable and enforce your password policy for Email Quarantine. You can select from three default templates to form the basis for a password policy.

These policies are intended as a starting guideline only. We recommend that you customize these settings to your organization’s requirements and to fit in with your Acceptable Use and Security policies.

Basic	These settings are for minimal security and would (for example) permit weak passwords to be used which can be easily guessed or cracked. This setting is the default setting for the system when it is first provisioned. We recommend that you adjust these settings to your requirements, or select the Standard or Enhanced security settings level.
Standard	These settings offer increased security, which you may consider to be sufficient for your requirements. This setting includes mandatory numeric characters in passwords. The security levels of some of the settings have increased values.
Enhanced	These settings are for enhanced security. All of the features are turned on. The security levels of appropriate items are set to an advanced security level. The system still maintains a manageable level of usability.

See Table 1-6 on page 18.

The following tables show the default password settings.

Table 1-4 Character requirements

	Basic	Standard	Enhanced
Minimum characters required in a password	8	8	12
Character requirements – Alphabetic	✓	✓	✓
Character requirements – Numeric	✗	✓	✓

Table 1-4 Character requirements *(continued)*

	Basic	Standard	Enhanced
Character requirements – Non-alphanumeric	✗	✗	✓

Table 1-5 Repeated characters and sequences in passwords

	Basic	Standard	Enhanced
Max length of sequences of repeated characters	4	4	2
Max number of characters in alphabetic, numeric, or keyboard order	Not Set	Not Set	3

Table 1-6 Other content in passwords

	Basic	Standard	Enhanced
Use of words in a dictionary (including common substitutions)	Allowed	Not Allowed	Not Allowed
Use of part of the user email address (including common substitutions)	Not Allowed	Not Allowed	Not Allowed

Table 1-7 Re-use and changes

	Basic	Standard	Enhanced
Number of password resets before a user can re-use the same password	3	5	20
Maximum number of password changes in 24 hours	10	10	5

Table 1-8 Password expiry

	Basic	Standard	Enhanced
Password expiry time	90 days	30 days	30 days
Time before expiry to alert users	7 days	7 days	7 days

Table 1-9 Email Quarantine lockouts (Standard Accounts)

	Basic	Standard	Enhanced
Number of incorrect password entries before lockout	100	20	9

Table 1-9 Email Quarantine lockouts (Standard Accounts) *(continued)*

	Basic	Standard	Enhanced
Lockout period	30 minutes	4 hours	1 day

Table 1-10 Email Quarantine lockouts (Administrator accounts)

	Basic	Standard	Enhanced
Number of incorrect password entries before lockout	20	10	3
Lockout period	1 hour	8 hours	Permanent

See "Configure an Email Quarantine password policy" on page 19.

Configure an Email Quarantine password policy

Three preset password policies are available: Basic, Standard, and Enhanced.

See "About Email Quarantine password policies" on page 17.

The settings for the currently selected policy are shown in the Email Quarantine portal screen in the Password policy section. A custom policy is displayed if changes are made to the default settings provided by any of the three template policies.

To configure an Email Quarantine password policy

1. Select **Services** > **Email Services** > **Email Quarantine** and navigate to the **Password policy** section.
2. Select the radio button for the template to be used as a starting point for your password policy: **Basic**, **Standard**, or **Enhanced**. The page is populated with the default settings for that policy. To modify any of the default template policy settings, check the **Customize selected policy** option.
3. Specify the minimum length for your users' passwords, using the drop-down list in the **Character requirements** section. The character types that are required in passwords can be selected by checking the boxes - **alphabetic**, **numeric** and **non-alphanumeric** characters. If a box is not checked, that type of character can still be used in passwords, but its use is not enforced.
4. **Character repetition** controls the number of times a particular character is repeated (for example, `dddd`). Specify the maximum number of repeated characters that are allowed in passwords by using the drop-down list.

5 **Character sequences** controls the number of alphabetic (for example `defg`), numeric (for example `4567`), and keyboard (for example `qwerty`) characters which are allowed in sequence. Select the maximum number of characters in the sequence that can be used by using the drop-down list.

These character sequences take into account several languages, which includes English, where they affect the alphabet or keyboard layout.

6 From the drop-down list, select whether any words in a standard dictionary can be used in passwords. Also select whether a user can include in their password part of the email address they use when logging on to Email Quarantine.

Both of these conditions include substituting characters with commonly used alternatives. Examples include the use of the number 3 for the letter E, or the use of the number 1 instead of the letters I or L.

7 Set the options for reuse of the same password, and how frequently users can reset their password. You can use these options to prevent users from resetting their password repeatedly until they can use the password that they began with.

8 Password expiry settings are selected using the drop-down lists. The password expiry time is the time that elapses after a password is set up until it expires. When it expires, the user is allowed to log on using the old password, but is immediately prompted to change it. It can be helpful to prompt users in advance of their password expiring, to give them the opportunity to think of a new password. Set this advance warning time as required.

9 When a user or administrator logs on to Email Quarantine, you can limit the number of attempts to key in the correct password.

This is to stop password cracking systems from persisting in trying random passwords until they gain access to the system. When the user or administrator is locked out, they cannot gain access to Email Quarantine until the lockout expires, even if they use the correct logon credentials.

The most extreme setting for the administrator lockout is Permanent. Administrators who are locked out in this way must contact the Support team to have their account unlocked before they can log on to Email Quarantine.

10 Select **Save & Exit** to apply the password control settings.

See “About Email Quarantine password policies” on page 17.

See “Overview of Email Quarantine settings” on page 6.

Making your Email Quarantine Acceptable Use Policy available

You can make your Acceptable Use Policy (AUP) available online for your users to read by a link in Email Quarantine and also in summary notifications.

To make your Acceptable Use Policy available

1. Select **Services** > **Email Services** > **Email Quarantine**.
2. In the **Acceptable Use Policy** section, check **Users can view your company Acceptable Use Policy (AUP)**.
3. In the field labeled **Specify URL link to your AUP:**, enter the URL for the location of the AUP document.
4. To specify where to place the link to the AUP, check one or both of the following: **Web Portal** and **Email Notifications**.
5. Click **Save & Exit**.

See "Overview of Email Quarantine settings" on page 6.

Defining what is visible in Email Quarantine summary notifications

Email Quarantine users can view the subject lines of emails, preview email text content, and delete emails. In summary notifications, the subject line of emails can be displayed.

These options are particularly relevant in countries where legislation does not allow these email components to be displayed if the recipient has not read the whole email. In these countries these items must not be viewed without the email being received in the normal way.

To define what is visible in summary notifications

1. Select **Services > Email Services > Email Quarantine**.
2. In the **Visibility** section, check the items that you want to be visible to your users.
3. Click **Save & Exit** to apply the settings.

Activating Email Quarantine

After you have completed the preparation, configuration, communication, and account creation stages for Email Quarantine, you can activate Email Quarantine for your selected domains.

Note: You are advised not to apply the **Quarantine the mail** action to the Signaturing System detection method. The suggested action for this detection method is **Block and delete the mail**.

To activate Email Quarantine

1. Log on to the portal.
2. Select **Services** > **Email Services** > **Anti-Spam**.

   If your organization plans to quarantine emails that violate Data Protection or Image Control policies, select **Services > Data Protection** or **Services > Email Services > Image Control** respectively, and follow steps 3-6 below.
3. In the **Detection Settings** tab, either:
   - Activate Quarantine settings for all domains, select **Global Settings** from the drop-down list
   - Activate Quarantine settings for an individual domain, select the domain from the drop-down list and ensure that the **Use custom settings** option is selected.

   You can activate any of the domains that you have told us about.
4. For email identified by a particular detection method to be sent to Email Quarantine, select **Quarantine the mail** from the **Action** drop-down list below that detection method.
5. If you use custom settings for individual domains, repeat steps 2 and 3 for all domains that you want to activate.
6. Click **Save**.

Note: If the **Quarantine the mail** option does not appear as an action for the selected domain, check that the domain was included in the list given to us. Refer any queries to your client services representative.

See "Overview of Email Quarantine settings" on page 6.

Chapter 2

About deploying Email Quarantine

This chapter includes the following topics:

About deploying Email Quarantine

The AntiSpam service checks all email entering your organization. Email is scanned for spam by a variety of means, including the Skeptic™ heuristics engine and proprietary signature scanners. Email is also compared against public and company blocked and approved senders lists. You can configure Email Quarantine to deal with email found by the various detection methods using the portal. Detected spam can be blocked and deleted, tagged, forwarded to a bulk email address, or it can be quarantined. You can also choose to quarantine email that violates rules for Image Control or Data Protection if your organization uses those services.

Quarantined emails do not reach the user's inbox, but can be stored in Email Quarantine and deleted or released to the user's normal email inbox. Depending on your organization's security policy, the text content of detected emails may be viewed. The emails in Email Quarantine can be managed by individual users or by other nominated individuals, depending on the deployment policy chosen. Emails in Email Quarantine are stored for 14 days before being deleted automatically. Users can review these emails as frequently as they want.

Users can receive periodic notifications when quarantined email is received. Notifications either provide a link to log on to Email Quarantine or contain **Release** links for users to release individual emails without repeatedly logging on to Email Quarantine.

There are several ways of deploying Email Quarantine within your organization and decisions need to be made about these before you activate the AntiSpam quarantine service.

The stages to ensure that Email Quarantine is deployed in an effective manner for your organization are as follows:

Table 2-1 Overview of Email Quarantine Deployment

Stages	Description	More information
Preparation	Ensure that the AntiSpam, Data Protection and Image Control services have been configured and tested. Plan the deployment of Email Quarantine and gather some essential information. **Note:** Ensure that Address Registration is set up for your organization.	See "Preparing to deploy Email Quarantine" on page 26.
Configuration	Implement the decisions made about the deployment of Email Quarantine in the AntiSpam, Data Protection, Image Control, and Email Quarantine configuration pages in the portal.	See the relevant Email and Web Security.cloud help sections for information about configuring AntiSpam, Data Protection, Image Control and Email Quarantine.
Communication	Notify users about the upcoming rollout of Email Quarantine, and its implications.	See "Communications to your organization about Email Quarantine " on page 33.
Creation of accounts and aliases	Create any new accounts that need to override the default notification setting. Set up account groups, for example, for group email addresses. Set up alias accounts for users with multiple accounts to manage quarantined mail in a single owner account.	See "Email Quarantine accounts and aliases - pre-activation announcement" on page 39.
Activation	Switch on Email Quarantine for the selected domains, in the portal.	See "Activating Email Quarantine" on page 22.

Use the deployment checklist to record when stages have been completed during the deployment of Email Quarantine.

See "Email Quarantine deployment checklist" on page 41.

See "Overview of Email Quarantine settings" on page 6.

About configuring Email Quarantine

Email Quarantine is configured in the portal. TheAntiSpam, Data Protection, and Image Control services (if your organization uses them) should be configured and fine tuned before you deploy Email Quarantine to your users.

The following general quarantine settings are defined within the portal.

- Defining an action that spam should be quarantined
  Define quarantine as an action for spam identified by the various detection methods (in **Services** > **Email Services** > **Anti-Spam** > **Detection Settings**).
  Define quarantine as an action for email identified by the detection methods in **Services > Data Protection > Email Policies** and **Services > Email Services > Image Control > Actions** if your organization uses these services.
- Specifying notifications
  Specify whether a welcome message is generated and summary notifications are enabled when an account is created. Notifications provide information to your users and ask them to register with and log on to Email Quarantine (in **Services** > **Email Services** > **Email Quarantine**).
- Defining a default language for Email Quarantine
  Specify the default language used in both Email Quarantine and the content of welcome messages and notifications (in **Services** > **Email Services** > **Email Quarantine**).
- Defining Quarantine Administrators
  Quarantine Administrators are users of Email Quarantine who have extended privileges to perform administrative functions in Email Quarantine (in **Services** > **Email Services** > **Email Quarantine**).
- Enabling the portal users to request additions to the approved senders list
  Specify whether your users can request that senders of suspect emails can be added to the approved senders list (in **Services** > **Email Services** > **Email Quarantine**).
- Enabling users to manage personal approved and blocked senders lists
  Specify whether users with Email Quarantine accounts can define and manage their own approved and blocked senders lists (in **Services** > **Email Services** > **List Management**)
- Notifying users of aliasing
  Specify whether the Email Quarantine users are informed when aliases are created by the Quarantine Administrator in Email Quarantine (in **Services** > **Email Services** > **Email Quarantine**).

Chapter 3

Preparing to deploy Email Quarantine

This chapter includes the following topics:

Preparing to deploy Email Quarantine

The planning stages and early considerations that enable a smooth deployment and subsequent running of the Email Quarantine service tailored to your organization's needs are important.

The following tasks must be considered:

- Configuring the AntiSpam service
  See Email AntiSpam configuration overview
- Configuring the Data Protection or Image Control services (if desired):
  See About actions and Email Data Protection policies or Define detection methods and actions for Image Control

- Listing domains
  See "Listing domains" on page 27.
- Deciding the deployment policy
  See "Deciding the Email Quarantine deployment policy" on page 27.
- Identifying Quarantine Administrators
  See "Identifying Quarantine Administrators" on page 29.
- Identifying account groups
  See "Identifying account groups" on page 30.
- Identifying aliases
  See "Identifying aliases" on page 30.
- Providing Web access
  See "Providing Web access" on page 31.
- Deciding support policy
  See "Deciding Email Quarantine support policy" on page 32.

Ensure that address registration is set up for your organization.

See Help on Address Registration.

Listing domains

Provide a list of all the domains for which Email Quarantine should be activated to your client services representative. The number of email addresses that are associated with each domain should also be recorded.

Table 3-1 Example list for the number of users per domain

Domain	Number of users per domain
example.com	5,000
examplecorp.com	300
example.de	100

Deciding the Email Quarantine deployment policy

Decide how quarantined emails will be handled before deploying Email Quarantine. The deployment policy decisions to make are whether individual users can manage their own Email Quarantine accounts or whether you will create account groups to

manage the quarantined email for multiple users. The issues to consider with regard to these options are as follows:

- Direct management
  All users can register with and log on to Email Quarantine. They will receive periodic notifications of their quarantined messages so that they can manage these emails themselves. The notifications either request the user to log into Email Quarantine to view or release the emails, or contain a Release link for users to release them without needing to log into Email Quarantine (active summary notifications). Users may also be able to define and manage their own approved and blocked senders lists and delete quarantined emails.
- Silent deployment
  Users are not asked to register with and log on to Email Quarantine, and they do not receive notifications. A Quarantine Administrator can access and manage users' Email Quarantine accounts on their behalf.
- Targeted deployment
  Some targeted users (for example, key personnel) are given access to their Email Quarantine accounts, while silent deployment is used for others.

You must consider your requirements regarding the kinds of Email Quarantine accounts that can be used for grouping multiple email addresses into a single Email Quarantine account:

- Aliases
  Email addresses that are managed by the account of another email address (the owner address). In this way, email that is sent to each of the aliased addresses is managed by and uses the settings of the owner account.
- Account groups
  A single account to manage the quarantined email sent to a number of designated addresses. The settings for the individual accounts still apply and group members can still access their individual accounts, if necessary.

Under the direct management policy, you may set up both kinds of account before activation of the Email Quarantine service. You can also set these up once Email Quarantine has been activated. Under the targeted deployment policy, you can create accounts that override the default notification setting to give access to targeted users when the default is silent deployment.

Note: You can implement a mix of deployment policies; for example, you can have silent deployment for some users, with other users managing their own Email Quarantine accounts, and some account groups. You can also deploy Email Quarantine silently to direct all quarantined email to one or more account groups.

Identifying Quarantine Administrators

Depending on your organization's deployment policy, you may need to establish one or more Quarantine Administrators. Quarantine Administrators are users who have extended privileges within their Email Quarantine accounts. A Quarantine Administrator may be responsible for a single domain or multiple domains.

The tasks that Quarantine Administrators can perform for the domains to which they have permission include:

Displaying details of Email Quarantine accounts	Showing the identity, last access date, and status of accounts.
Creating accounts	Generating new user accounts and specifying whether to enable the sending of welcome messages and notifications.
Creating account groups	Consolidating the unwanted email that is sent to a number of designated addresses into a single account group. The settings for the individual accounts still apply and users can still access their individual accounts, if necessary. Account groups help to direct unwanted mail to distribution lists and other group email addresses.
Creating aliases	Consolidating multiple email addresses under a single email address (the owner address). In this way, unwanted email sent to each of the aliased addresses is managed by and uses the settings of the ‘owner’ account. Aliases are useful where an individual has several email addresses within your organization.
Accessing different accounts	Accessing the account of another user, and being able to work as if logged on as that user.
Deleting accounts	Deleting selected accounts.

You should identify the most appropriate people to become Quarantine Administrators, according to your organization's deployment policy. Remember that Quarantine Administrators occupy a trusted role.

Record the details of the Quarantine Administrators, so that you can use this information later. Quarantine Administrators are created in the portal during the configuration stage. An example list is provided below.

Table 3-2 Example list of Quarantine Administrators

Name	Email address	Domain
Alex White	a.white@example.com	example.com

Table 3-2 Example list of Quarantine Administrators *(continued)*

Name	Email address	Domain
Kay Smith	k.smith@examplecorp.com	examplecorp.com

Identifying account groups

You should identify all group email addresses that are visible externally within the Email Quarantine domains; for example, sales@example.com and info@example.com. You can then nominate a single member of each group to be responsible for managing the Email Quarantine account for that group. This avoids all members of a group receiving notifications from the group email address's Email Quarantine account. The settings for the individual accounts still apply and users can still access their individual accounts, as necessary.

You can also set up account groups to enable a single owner to manage the quarantined mail of several individual's accounts.

The following table provides an example for collating account group information.

Table 3-3 Account group owners

Group email address	Owner	Email address	Domain
sales@example.com	Joe Smith	jsmith@example.com	example.com
all@examplecorp.com	Lisa Jones	ljones@examplecorp.com	examplecorp.com
user1@example.com	Steve Wilkins	swilkins@example.com	example.com
user2@example.com	Steve Wilkins	swilkins@example.com	example.com
user3@example.com	Steve Wilkins	swilkins@example.com	example.com

When the configuration is completed, a Quarantine Administrator can set up the necessary account groups to direct unwanted mail sent to the members of a group to the owner's Email Quarantine account. This should be completed before Email Quarantine is activated.

Identifying aliases

Depending on your deployment policy, you may want to identify any aliases that are required. Aliasing lets you (and Email Quarantine users) consolidate multiple email addresses under a single email address (the owner address). In this way, unwanted email sent to each of the aliased addresses is managed by and uses the

settings of the 'owner' account. This is useful, for example, where an individual has several email addresses within your organization.

An example list of alias owners is provided below.

Table 3-4 Example list of alias owners

Name	Owner email address	Alias email addresses	Domain
Helen Wright	hwright@example.com	hwright@@example.com	example.com
		helenwright@sales.example.com	
		hwright@ethics.example.com	
Mark Harvey	mharvey@example.com	kmuir@example.com	example.com
		dlucas@example.com	
		pshields@example.com	
		mbrown@example.com	

When the configuration stage is complete, a Quarantine Administrator can set up the necessary aliases to direct the quarantined email from all accounts to the owner's Email Quarantine account. This should be completed before Email Quarantine is activated.

Providing Web access

Users access their Email Quarantine accounts through a Web browser. The following browsers are recommended:

- Microsoft Internet Explorer version 5.5 or above
- Netscape version 6.2 or above
- Mozilla version 2 or above (includes Firefox version 3)

Support for other browsers cannot be guaranteed.

You will need to ensure that:

- Each user's Web browser has secure browsing enabled (using SSL)
- Each user's Web browser has cookies enabled for the Email Quarantine Web site
- Any internal security features, such as firewalls or Web access control services, are set to allow access to the Email Quarantine Web site

Depending on your organization's security policy, you may want to configure Web browsers to retain authentication information (email address and password) for each Email Quarantine account.

Deciding Email Quarantine support policy

Decide how to handle inquiries from users. We cannot take support inquiries directly from your users. You need to ensure that your users understand how their questions should be raised internally by publishing support procedures and policies. The *Email Quarantine Portal User and Administrator Guide* should be updated to include this information.

Chapter 4

Communicating to your organization about Email Quarantine

This chapter includes the following topics:

Communications to your organization about Email Quarantine

A series of timed and targeted communications should be sent to those people within your organization who use Email Quarantine. The people who need to be prepared for the introduction of Email Quarantine are:

- Quarantine Administrators
  Quarantine Administrators play a key role in the successful deployment of Email Quarantine. They need to be briefed on their role and responsibilities according to the deployment policy that will be implemented within your organization. Training should be provided on the Quarantine Administrator functions.

Once the Quarantine Administrators are set up in the portal during the configuration stage, they need to be provided with the Email Quarantine URL. Then they can register with Email Quarantine and request a password.

- Users for whom Email Quarantine accounts are created
  Your choice of deployment policy determines the users who you send these communications to. For example, you may decide to inform only a subset of users of the presence of Email Quarantine.

  Examples of the types of communication that need to be sent are given in the following sections. These examples relate to regular users of Email Quarantine and also to those individuals nominated to manage the spam of a group.

  Once Email Quarantine is activated, users for whom accounts are created may receive an automatic welcome message, depending on the options that you select during the configuration and the account creation stages. Advising your users before Email Quarantine is activated and before any welcome message are received facilitates a smooth transition to the deployment of Email Quarantine.

See "Identifying Quarantine Administrators" on page 29.

See "About configuring Email Quarantine" on page 25.

See "Email Quarantine accounts and aliases - pre-activation announcement" on page 39.

Advance announcement

The first communication should be a general announcement about the upcoming introduction of Email Quarantine, outlining Email Quarantine's purpose, functionality, and benefits.

The following is an example of an advance announcement email:

From: IT Administrator

To: All Users

Subject: Email Quarantine - A New Way To Manage Unwanted Email

As you may know, <organization> has taken measures to deal with the increasing problem of spam (unsolicited junk email) and other email-borne threats. We have rolled out the AntiSpam service from <securityservicesupplier>, the most accurate and effective email security service available.`[Add Data Protection and Image Control after AntiSpam in the previous sentence if you deploy those services as well.]`

We are excited to announce a new feature that will benefit all of our email users: Email Quarantine.

Email Quarantine identifies unwanted messages on your behalf and directs them to your own personal Email Quarantine account. Email Quarantine gives you a way to review the messages that the system has identified as unwanted. You can access your Email Quarantine account via a Web browser.

Email Quarantine will normally hold messages for 14 days before they are automatically deleted. You will be able to set up notifications to let you know when you have messages in your Email Quarantine account.`[If you choose not to enable notifications, or not to let users control notifications, remove the preceding sentence.]`

If Email Quarantine captures a message that you want to receive, you can release such a message to your normal email inbox.`[If are deploying active summary notifications, remove this paragraph.]`

If Email Quarantine captures a message that you want to receive to your email inbox, you can release it from the active summary notification without logging into Email Quarantine. You can still log into Email Quarantine to release such a message if you prefer.`[If are NOT deploying active summary notifications, remove this paragraph.]`

We intend to introduce the Email Quarantine service on <date> and will issue a reminder closer to this time.

If you wish to learn more about Email Quarantine, read the additional information in the user guide <attached/on this intranet page>, and in <organization>'s Security and Acceptable Use policies <attached/on this intranet page>.

Pre-activation reminder

The second communication should be a reminder of the activation date to all email users. It should set expectations about Email Quarantine and be sent out just before you activate Email Quarantine.

An example of a pre-activation reminder is:

From: IT Administrator

To: All Users

Subject: Email Quarantine-Going Live <Date>

Recently we announced that we would introduce a new feature to benefit all our email users: Email Quarantine.

This is a reminder to all users that the new Email Quarantine service will be deployed on <date/time>.

Your email will not be affected, and you will need to take no action until you receive messages directly from the Email Quarantine service itself. These messages will inform you of what you need to do to use your Email Quarantine account. Do not be concerned if you do not receive a message from Email Quarantine. This probably indicates that the service has not yet captured any unwanted email on your behalf.

Email Quarantine will direct unwanted messages to your personal Email Quarantine account. Email Quarantine gives you a way to review messages sent to you that the system has identified as unwanted. You can access your Email Quarantine account via a Web browser.

Email Quarantine normally holds captured messages for 14 days before they are automatically deleted. You will be able to set up notifications to let you know when you have messages in your Email Quarantine account. `[If you choose not to enable notifications, or not to let users control notifications, remove the preceding sentence.]`

If Email Quarantine captures a message that you want to receive, you can release such a message to your normal email inbox by logging on to Email Quarantine. `[If you have deployed active summary notifications, delete this paragraph.]`

If Email Quarantine captures a message that you want to receive, you can release such a message to your normal email inbox using the link in your active summary notifications or by logging on to Email Quarantine. `[If you have NOT deployed active summary notifications, delete this paragraph.]`

If you receive messages wrongly detected as spam on a regular basis, you may have the option to notify the administrator. The administrator can decide whether to add the sender to an approved list, ensuring that, in future, similar messages will not be redirected to your Email Quarantine account.

Should you encounter any problems using Email Quarantine, check the Email Quarantine online help, and the Email Quarantine User and Administrator Guide. If these do not address your issue then please contact the <organization> helpdesk.

Pre-activation alias owner - announcement

Shortly after a preactivation general announcement is sent, you should send a follow-up communication to individuals who are responsible for handling the spam for aliased accounts. These communications should be customized for each individual.

See “Identifying aliases” on page 30.

See "Email Quarantine accounts and aliases - pre-activation announcement" on page 39.

An example of a preactivation alias owner announcement email is given below.

From: IT Administrator

To: <Owner Name>

Subject: Email Quarantine Responsibilities for <group name> List <Group Owner>

In addition to managing your own email address, <owner's work email address>, through Email Quarantine, you have been nominated to manage the Email Quarantine account for the <group name/address> group. Due to your involvement with this list, you are the most appropriate person to be responsible for it.

Once Email Quarantine is activated you will see that <group email address> is added as an 'alias' to your Email Quarantine account. This can be reviewed by the following steps:

- *Log on to your Email Quarantine account.*
- *Select the* **Options** *tab at the top of the page.*
- *Click on* **Manage Aliases**.

Having the group list aliased to your Email Quarantine account should not place any additional burden on you. It can be managed in the same way that you manage your own email address.

Should you encounter any problems using Email Quarantine, check the Email Quarantine online help, and the Email Quarantine User Guide. If these do not address your issue, contact the <organization> helpdesk.

Change to active summary notifications - announcement

This email informs users that you are moving from the standard notifications to active summary notifications. Active summary notifications enable users to release wanted emails using a link within the notification. The user does not then need to log into Email Quarantine to release emails. (Initial creation of the account is still needed and the user will need to create a password.)

An example of an announcement about changing to active summary notifications is:

From: IT Administrator

To: All Users

Subject: Email Quarantine-An update to the way you manage unwanted email

We are excited to announce a new feature that will benefit all of our email users: Active summary notifications.

Your current Email Quarantine setup identifies unwanted emails on your behalf and directs them to your own personal Email Quarantine account. Email Quarantine gives you a way to review your messages that the system has identified as unwanted. You access your Email Quarantine account via a Web browser.

The summary notifications you are used to have been improved: If Email Quarantine captures a message that you want to receive in your email inbox, you can release the email directly from the new 'active' summary notification without the need to log on to Email Quarantine. You can still log on to Email Quarantine to release a message if you prefer.

To learn more about Email Quarantine, read the additional information in the user guide <attached/on this intranet page>, and in <organization>'s Security and Acceptable Use policies <attached/on this intranet page>.

Chapter 5

Deploying Email Quarantine

This chapter includes the following topics:

Email Quarantine accounts and aliases - pre-activation announcement

New Email Quarantine accounts for your organization's users can be created either manually or automatically:

- Manually - when a Quarantine Administrator creates a new account, the Quarantine Administrator may override the default settings for welcome messages and notifications
- Automatically in the following circumstances:
  - When a user responds to a welcome message from Email Quarantine by requesting a password.
    If welcome messages are enabled, a welcome message is sent to an email address that has no account, when it receives its first spam.
  - When a Quarantine Administrator sets up a group or aliased account and the email address of the owner does not yet exist
  - When a Quarantine Administrator accesses an account that does not yet exist.
    To access another account search for an email address in **Email Quarantine** > **Administration** > **Access Different Account**.

- When a user receives an active summary notification allowing them to release an email directly from the notification

---

Warning: Where accounts are created automatically, they use the default Email Quarantine settings. You may not be able to override the default settings for welcome messages and notifications for these accounts.

The first accounts to be created are those for the Quarantine Administrators that are identified in the preparation stage. Quarantine Administrators should be able to access Email Quarantine before it is activated for all regular users.

See "Identifying Quarantine Administrators" on page 29.

Once the Quarantine Administrator's accounts are created they can complete this stage of Email Quarantine deployment by creating the rest of the necessary accounts. Depending on your deployment policy, before Email Quarantine is activated, the Quarantine Administrators may need to:

- Manually, create Email Quarantine accounts that override the default notification setting (usually to give access to targeted users when the default is silent deployment)
- Set up account groups and aliases:
  - To direct the spam of any group email address to a nominated owner.
    See "Identifying account groups" on page 30.
  - To consolidate the spam of a user with multiple email addresses into a single owner account (alias).
    See "Identifying aliases" on page 30.

When you have created your accounts, you can activate Email Quarantine for your selected domains.

See "Activating Email Quarantine" on page 22.

New account groups

You might want to create a new externally visible account group after the initial activation of Email Quarantine. You should perform the following tasks before the list is created and the address made public:

- Identify a group owner to handle the spam for the group.
- Ask a Quarantine Administrator to create an account group to be managed by the group owner.

Managing passwords

For security reasons, passwords should be changed periodically. You should configure Email Quarantine with the minimum password security requirements to comply with your security policy, including the frequency of changing passwords.

Email Quarantine deployment checklist

Use this checklist to record completed activities during deployment of Email Quarantine.

Table 5-1 Deployment checklist

Step	Process	Date completed
1. Preparation	■ Set up the AntiSpam (and optionally the Data Protection and Image Control] service in the portal. ■ Compile a list of domains and the number of email addresses and give to your client services representative. ■ Decide deployment policy for Email Quarantine. ■ Decide who will be Quarantine Administrators. ■ Identify account groups and aliases and record these on template. ■ Provide Web access - check browser configuration. ■ Decide support policy for users and publish support procedures and policies	
2. Configuration	■ Implement deployment policy and establish Quarantine Administrators in **Services** > **Email Service** > **Email Quarantine** and **List Management**.	
3. Pre-activation account and alias creation	■ Quarantine Administrators create any accounts that need to override defaults for welcome messages and notifications. ■ Quarantine Administrators set up aliases and account groups.	
4. Communication	■ Decide who you need to communicate with, and what those users need to be told. ■ Decide whether the user guide will be sent by email or posted on an intranet or both. ■ Send advance announcement. ■ Send pre-activation reminder. ■ Send pre-activation alias announcement to each nominated owner of an alias or group email address.	
5. Activation	■ Activate domains in **Services** > **Email Service** > **Anti–Spam** > **Detection Settings**, **Services > Data Protection > Email Policies** and **Services > Email Services > Image Control**.	