Email AntiSpam

Administrator Guide and Email Quarantine Deployment Guide

Symantec.cloud

AntiSpam Administration and Email Quarantine Deployment Guide

Documentation version: 1.10

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Clients are advised to seek specialist advice to ensure that they use the Symantec services in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include (but is not limited to) data protection law, privacy law, telecommunications regulations, and employment law. In many jurisdictions, it is a requirement that users of the service are informed of or required to give consent to their email being monitored or intercepted for the purpose of receiving the security services that are offered by Symantec. Due to local legislation, some features that are described in this documentation are not available in some countries.

Configuration of the Services remains your responsibility and entirely in your control. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec advises you to always check local legislation prior to deploying a Symantec service. You should understand your company’s requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. Symantec can accept no liability for any civil or criminal liability that may be incurred by you as a result of the operation of the Service or the implementation of any advice that is provided hereto.

The documentation is provided "as is" and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Symantec Corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information that is contained in this documentation is subject to change without notice.

Symantec may at its sole option vary these conditions of use by posting such revised terms to the website.

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

Section 1

AntiSpam configuration

Chapter 1

Introduction to AntiSpam

This chapter includes the following topics:

About AntiSpam

The following AntiSpam detection methods can be used to scan your incoming emails.

Table 1-1 Email AntiSpam detection methods

Detection method	More information
Skeptic™ heuristic engine	An artificial intelligence engine that creates an ever-expanding knowledgebase for spam identification. AntiSpam distinguishes newsletters from spam. You can choose to detect newsletters as well as spam. See "Enabling predictive (heuristic) spam detection" on page 30.
Signaturing system	Various signature-building engines that create a vast knowledgebase of signatures of spam messages currently in email circulation. See "Using the spam matching (signature) system" on page 29.
Dynamic IP block list	A recognized public block list of IP addresses of globally known sources of spam. See "Using the dynamic IP block list" on page 29.
Exclusions	A list of email addresses to be excluded from the protection of AntiSpam. See "About defining exclusions" on page 60.
Blocked senders list	A list of blocked senders that you can specify at either global, group, and user level (depending on your organization's configuration). The list can contain email addresses, domains, or IP addresses that you recognize as sources of spam or other unwanted email.
Approved senders list	A list of approved senders that you can specify at either global, group, and user level (depending on your organization's configuration). The list can contain email addresses, domains, or IP addresses. The list enables email from a sender on list to pass through the spam service without interruption.
Sender Policy Framework	Sender Policy Framework (SPF) reduces email spam by detecting sender spoofing, which leads to reduced phishing attempts where domain spoofing is commonplace. SPF cannot be configured for specific groups. See "Enabling spoofed sender detection with SPF" on page 24.

Table 1-1 Email AntiSpam detection methods *(continued)*

Detection method	More information
Domain-based Message Authentication, Reporting and Conformance	Domain-based Message Authentication, Reporting, and Conformance (DMARC) detects sender spoofing by standardizing how email recipients perform authentication using SPF and DKIM. DMARC participants publish policies that tell recipients what to do if neither of these authentication methods passes. DMARC cannot be configured for specific groups. See "Enabling spoofed sender detection with DMARC" on page 25.
DomainKeys Identified Mail	DomainKeys Identified Mail (DKIM) is a method for associating a domain name with an email message. This association allows a person, role, or organization to claim responsibility for the message. Domain names and messages are associated by means of a digital signature that recipients can validate. The verifier recovers the signer's public key using the DNS, and then verifies that the signature matches the actual message's content. **Note:** DKIM verification cannot be initiated directly. Rather, DKIM verification takes place as part of the DMARC authentication process. See "Enabling spoofed sender detection with DMARC" on page 25.

You can select the detection methods that you require for your incoming email. For each method apart from SPF and DMARC, you can associate different actions against the suspected email. You can also define any email addresses that are not subject to the scanning process (exclusions).

As an Administrator, you can configure the detection settings in the portal according to your organization's requirements.

Detection settings can be defined at:

- Global level for all of the domains.
- Domain level for individual domains.
- Group level for specific groups.

Specific users can have their own settings and manage their personal approved and blocked lists of senders in their Email Quarantine accounts.

User settings override group and global settings; in turn, group settings override global settings. Administrators may want to use global or group detection settings and enable users to manage their own user approved and blocked senders lists.

Note: Group Settings and User Settings are not available by default. Contact the Support team to be provisioned with this facility.

Settings that administrators need to define when they configure the AntiSpam service are:

- Detection settings.
  - Define the spam detection methods to use.
  - Define the actions to be taken on detection of spam.
  - If spam email redirection is selected as an action, set the email address to which spam email is routed.
  - If tagging the subject line is selected as an action, define the tag text for emails that are tagged as spam.
- Spam Quarantine settings.
  - Depending on your organization's configuration, you may not see Spam Quarantine settings.
- Groups to which you want to apply specific settings.
- Exclusions (addresses to be excluded from scanning).
- Approved senders and blocked senders lists.

Warning: AntiSpam is not automatically enabled when the service is provisioned. You must activate the different spam detection methods to enable the service.

See "AntiSpam best practice settings" on page 14.

See "About Anti-Spam detection settings and actions" on page 20.

See "Overview of quarantine settings" on page 36.

See "Defining groups for AntiSpam" on page 52.

About outbound spam scanning

To provide continuity of service, Email Security scans all outbound emails and rejects the emails we identify as spam. To help you recognize these messages we

send an SMTP permanent error response (5xx) to your message transfer agent (MTA). We suggest that you set your MTA to generate a non-delivery receipt (NDR) to inform the sender that we have blocked the email as spam.

Note that:

- The portal has no configurable actions.
- Track and Trace shows the outbound emails that we reject as spam.
- We do not include suspected outbound spam in Email Security Service reporting in the portal.
- Spam capture rate and spam false positive service levels do not apply to outbound emails.

Note: We are not liable for any damage or loss resulting directly or indirectly from any failure of the service to identify spam. We are also not liable for wrongly identifying an email as spam. Please contact Support for further help.

Locating the AntiSpam pages in the portal

Depending on your organization's configuration, you may not see all of the portal pages that are described.

To locate the AntiSpam pages in the portal

- Click **Services** > **Email Services** > **Anti-Spam**.

  If **Global Settings** is selected in the drop-down list, up to four tabs are displayed: **Detection Settings**, **Quarantine Settings**, **Approved Senders**, and **Blocked Senders**.

  If a specific domain is selected from the domains drop-down list, up to five tabs are displayed, depending on your organization's configuration: **Groups**, **Detection Settings**, **Quarantine Settings**, **Exclusions**, and **List Management**.

  If a group is selected from the groups drop-down list, up to four tabs are displayed: **Group Members**, **Detection Settings**, **Approved Senders**, and **Blocked Senders**.

  All of the AntiSpam settings are defined in these tabs.

See "AntiSpam best practice settings" on page 14.

AntiSpam best practice settings

When you are provisioned with the AntiSpam service, the service is enabled with default settings.

We recommend that you evaluate the tagged spam that you receive using these settings, and how these settings work for your organization's mail flow. When you are confident that the service is only detecting spam email, change to the best practice settings.

To change to the best-practice settings

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select **Global Settings** or a specific domain from the domains drop-down list.
3. In the **Detection Settings** tab, we recommend modifying the relevant settings as follows:

Blocked senders list (IP addresses only)	Set to **Block and delete the mail**.
Blocked senders list (domains and email addresses only)	Set to **Block and delete the mail**.
Dynamic IP block list	Set to **Block and delete the mail**.
Signaturing system	Set to **Block and delete the mail**.
Skeptic™ heuristics	Set to **Tag the subject line but allow mail through**. Once you are happy that only spam is being detected with this setting, change it to **Block and delete**.

See "Enabling predictive (heuristic) spam detection" on page 30.

Defining whether AntiSpam settings apply globally, for a domain, or for a group

You can configure and apply default AntiSpam settings to all domains, or you can apply custom settings to an individual domain by using the domains drop-down list. Most often you will configure the Anti–Spam service using your global settings and making fewer changes on a domain-level basis. If you have defined any groups, you can also apply specific settings for each group.

To define whether settings apply globally, for a domain, or for a group

1. Click **Services** > **Email Services** > **Anti-Spam**
2. Select the domain or group to work with from the drop-down list at top left.
3. Specify the required settings; they are applied at the level that you selected in the previous step.

   When you select a domain or group to work with, the settings from the next highest level are inherited. You can then make your required amendments to apply for the domain or group. Different tabs are available at the various levels, reflecting the settings that are available at each level.

See "Applying AntiSpam global settings " on page 15.

See "Applying AntiSpam settings for a specific domain" on page 16.

See "Applying AntiSpam settings for a group" on page 16.

See "AntiSpam best practice settings" on page 14.

Applying AntiSpam global settings

You can configure and apply default AntiSpam settings to all domains. Use the domains drop-down list. Most often you will configure AntiSpam using your global settings and making fewer changes on a domain-level basis.

To apply global settings

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Ensure that **Global Settings** is selected in the domains drop-down list:

   Up to four tabs are displayed (**Detection Settings**, **Quarantine Settings**, **Approved Senders**, and **Blocked Senders**) depending on your organization's configuration. Any settings at this level apply globally across all of your domains.

See "Defining whether AntiSpam settings apply globally, for a domain, or for a group" on page 14.

See "Applying AntiSpam settings for a specific domain" on page 16.

See "Applying AntiSpam settings for a group" on page 16.

See "AntiSpam best practice settings" on page 14.

Applying AntiSpam settings for a specific domain

For each domain name that is registered for AntiSpam you can override Global Settings and apply different rules and settings to it. You can configure Groups, Detection Settings, Quarantine Settings, Exclusions, and List Management settings.

To apply settings for a specific domain

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select the domain from the domains drop-down list.

   To reduce the number of domains in the list, you can enter the first three or more characters of the domain name. Only those that contain those starting characters are listed.

   Up to five tabs are displayed (**Groups**, **Detection Settings**, **Quarantine Settings**, **Exclusions**, and **List Management**) depending on your organization's configuration.
3. In the **Detection Settings** and **Quarantine Settings** pages, ensure that the **Use custom settings** option is selected. If it is not selected, all fields in these pages remain inactive and unable to be edited.

   The fields in these pages inherit the global settings until you make any changes.

   When you select **Save & Exit** on this screen, the changes you make are applied only to the selected domain.

   The **Groups**, **Exclusions**, and **List Management** pages are active and editable.

   Changes to approved senders and blocked senders lists can only be made at global or group level.

   When you select a specific domain to work with, the name of the domain is displayed as a heading:

See "Defining whether AntiSpam settings apply globally, for a domain, or for a group" on page 14.

See "Applying AntiSpam global settings " on page 15.

See "Applying AntiSpam settings for a group" on page 16.

See "AntiSpam best practice settings" on page 14.

Applying AntiSpam settings for a group

If you have defined a group, you may want to configure the **Detection Settings**, **Approved Senders**, and **Blocked Senders** for the group. In this manner you can

create different groups that use different levels of detection and that respond to detection in different ways.

To apply settings for a group

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select the domain that the group is in, from the domains drop-down list.
3. Select the group from the groups drop-down list.

   Four tabs are displayed: **Group Members**, **Detection Settings**, **Approved Senders**, and **Blocked Senders**. The name of the domain and group is displayed in the page heading.

   The **Detection Settings** page presents a further option to **Use custom settings**. Unless this is selected, all fields in this page are inactive and cannot be edited. If this option is selected, all fields become active and inherit the domain settings until you make any changes. The available settings are the same as those at global and domain level. The changes you make here are applied only to the selected group (provided the changes are saved).

See "Defining whether AntiSpam settings apply globally, for a domain, or for a group" on page 14.

See "Applying AntiSpam global settings " on page 15.

See "Applying AntiSpam settings for a specific domain" on page 16.

See "Defining groups for AntiSpam" on page 52.

See "AntiSpam best practice settings" on page 14.

About the Email Submission Client

The Email Submission Client enables a Microsoft Exchange user to mark an email as spam by moving the email to a spam submission folder. Spam submission is the process of marking an email as spam by the email user. With spam submission, the threat research team improves the effectiveness of spam filtering by creating appropriate rule sets.

The Email Submission Client simplifies the way you submit spam emails to the threat research team. The Email Submission Client accesses Exchange servers through a Client Access server. After you deploy the Email Submission Client, it obtains a list of all the Exchange servers and mailboxes on your network. The Email Submission Client lets you create a spam submission folder in a user's mailbox or a user group mailbox. The user copies any email that is identified as spam or unwanted email to the spam submission folder.

When an email is placed in the spam submission folder, the Client Access server notifies the Email Submission Client about the email. Based on the notification, the Email Submission Client retrieves this email from the spam submission folder. This email is later sent over HTTPS to the threat research team for analysis. The threat research team uses the emails that are submitted for antispam research. As a result of the research, the team can improve the effectiveness of spam filtering by creating appropriate rule sets. Any rules that are created are integrated into messaging security services.

The Email Submission Client is accessed in the portal at **Tools** > **Downloads**. Under the Email Submission Client section, click the **Download** option to download the Email Submission Client tool.

Note: For further information, refer to these Implementation Guides:

Email Submission Client 1.0 Implementation Guide

Email Submission Client 2.0 Implementation Guide

Chapter 2

Detection settings and actions

This chapter includes the following topics:

About Anti-Spam detection settings and actions

Detection settings define which methods you want the Email Anti-Spam service to use to detect spam messages. You can choose to prevent all detected spam messages from being delivered to recipients. Alternatively, the Anti-Spam service can append a header or tag the message subject lines to notify the recipients that the messages are suspected spam. You can also use Anti-Spam to detect and manage any marketing messages or newsletter messages your organization receives.

Table 2-1 describes the detection methods that you can enable, and Table 2-2 describes the possible actions that you can choose when spam is detected.

When you first enable detection settings, we recommend that you choose “Tag the subject line” or “Quarantine” (if enabled) as an action for each method. You can use these actions to evaluate the messages that are detected as spam and determine how your chosen settings work for your organization’s mail flow. When you are confident that the Anti-Spam service successfully detects spam messages, you can change the actions to the best practice settings.

You can choose detection settings at the global level or the domain level. Also, you can customize the detection methods and actions for specific domains or Email Anti-Spam groups.

Table 2-1 Email Anti-Spam detection settings

Detection methods	Description
Approved Senders	Enable the appropriate **Use approved senders list** options to ensure that any emails that are received from these senders are not identified as spam. You can define lists of approved senders by IP addresses, domains, or email addresses.
Spoofed Sender Detection	Enable **Use SPF** (Sender policy framework) to verify email senders against the list of authorized hosts for a domain. Enable **DMARC** (Domain-based message authentication, reporting, and conformance) to check whether the sender conforms to a published policy that demonstrates whether the sending domain's messages use either SPF or DKIM or both. You can enable spoofed sender detection options for all of your domains or for individual domains. You cannot enable them for individual groups or users.

Table 2-1 Email Anti-Spam detection settings *(continued)*

Detection methods	Description
Responsive Spam Detection	Enable **Use blocked senders list (IP addresses only)** to check senders against a predefined list of IP addresses, domains, or email addresses that you recognize as sources of spam or other unwanted email. Enable **Use blocked senders list (domains and email addresses only)** to check senders against a predefined list of domains or email addresses that you recognize as sources of spam or other unwanted email. Enable **Use dynamic IP block list** to check senders against a public block list of IP addresses that are globally known sources of spam. Companies and individuals in the dynamic public block list have demonstrated patterns of junk emailing. Enable **Use signaturing system** to check emails against a knowledge base of unique strings that identify any spam message samples that are currently in email circulation. The signaturing system requires exact spam signature matches, which reduces the chances that the scanner stops genuine business emails. In addition, the signaturing system speeds up the spam identification process and the message handling process. For each **Responsive Spam Detection** setting that you enable, choose an action from the drop-down list. See Table 2-2 for descriptions.
Predictive Spam Detection	Enable **Use Skeptic heuristics** to evaluate potential spam using Skeptic™, and then specify an action for the Anti-Spam service to take when spam is detected. See Table 2-2 Skeptic uses artificial intelligence to score any email that is not previously known spam against a set of rules. If an email achieves more than a specified score, it is identified as spam.

Table 2-1 Email Anti-Spam detection settings *(continued)*

Detection methods	Description
Newsletter Detection	You can also choose to activate **Newsletter / Marketing detection** to specify the preferred action to handle your organization's newsletters and marketing email. Choose whether to apply the Newsletter Detection actions to your Global Settings or a specific domain. Check the box to enable the **Use Newsletter / Marketing detection** service and select an action from the drop-down menu. Remember that you can also define an **Approved senders list** to ensure that the email newsletters that recipients have chosen to receive are not identified as newsletters.

For each spam detection method, you need to define an action that tells the Anti-Spam service what to do with the detected spam messages.

Table 2-2 Actions for detected email

Action	Description
Append a header but allow the email through	The **Append header…** actions add a string to the email header. The format for the string is: `X-Spam-Flag:YES` This string identifies the email as spam and enables further action when the message enters your email system or your users' email clients. For example, you can divert the email into a folder that you or the recipient have set up to receive spam. The detected email is delivered to the recipient's email inbox.
Append a header and redirect the email to a bulk mail address	The string is added to the header as previously described. When you select this option for a detection method, under **Bulk Mail Address**, the **Enter an email address** field becomes active. The email is redirected to the email address that you enter in this field. The detected email is not delivered to the intended recipient.
Block and delete the email	The detected email is not delivered to the intended recipient. The email is deleted.

Table 2-2 Actions for detected email *(continued)*

Action	Description
Tag the subject line but allow the email through	The **Tag the subject line…** action adds some text that you define to the email's subject line. When you select this option for a detection method, under **Subject Line Text**, the **Enter text** field becomes active. The text that you enter in this field is added to the subject line. You can choose to put the text in front of or after the original subject line text. The detected email is then delivered to the recipient's email inbox.
Quarantine the email	The detected email is not delivered to the recipient's email inbox. The email is quarantined. Depending on your Spam Manager settings, the recipient may be notified that they have received spam. They may have the option to view it and release it to their inbox. If your organization's Anti-Spam service configuration does not include Spam Quarantine, the quarantine option is not available.

Enabling approved senders lists

If you use global, group, or user lists, or a combination of these, you must enable approved senders lists as a detection method.

Note: Group Settings and User Settings are not available by default. Contact the Support team to be provisioned with this facility.

To enable approved senders lists

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Approved Senders** area, select the appropriate checkbox to enable the approved senders list. The selection depends on which type of listed senders are allowed to bypass the scan: only IP addresses, only domain names and email addresses, or all types of sender (select both boxes).
4. Click **Save and Exit**.

   A confirmation of the setting is displayed.

See “Uploading a group member list for AntiSpam” on page 57.

See “About Anti-Spam detection settings and actions” on page 20.

Enabling blocked senders lists

Whether you use global, group, or user lists, or a combination of these, you must enable blocked senders lists. When you enable blocked senders lists, you must define an action for any email that is identified as originating from a blocked sender.

Note: Group Settings and User Settings are not available by default. Contact the Support team to be provisioned with this facility.

To enable blocked senders lists

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Click the **Detection Settings** tab.
3. Under **Responsive Spam Detection**, select the appropriate checkbox to enable the blocked senders list depending on which type of senders in your lists are allowed to bypass the scan: only IP addresses, only domain names and email addresses, or all types of sender (select both boxes).
4. For each **Use blocked senders list** checkbox that you have selected, select an action for the detected spam from the **Action** drop-down list.
5. Click **Save and Exit**.

   A confirmation message is displayed.

See “Uploading a group member list for AntiSpam” on page 57.

See “About Anti-Spam detection settings and actions” on page 20.

Enabling spoofed sender detection with SPF

Sender Policy Framework (SPF) reduces email spam by detecting sender spoofing, which reduces phishing attempts in which domain spoofing is commonplace. Some organization's publish an SPF record in their DNS. The SPF record authorizes sending hosts for their domains. The recipient verifies the email sender against the authorized hosts. If verification fails, the email sender is spoofing and the email should not be trusted.

When you use SPF spam detection for a domain, inbound email to your domain is verified against the SPF policy of the reported sender. If the reported sender publishes a *hard-fail* SPF policy and the inbound email fails SPF verification, the

email is blocked and deleted. The block and delete action enforces the sender hard fail policy, which says not to accept emails that are not from my authorized host names. A 5xx error is returned to the sender. Other types of SPF policy, for example *soft-fail* is ignored.

You can enable SPF for all of your domains or for individual domains. You cannot enable it for individual groups or users.

To enable the spoofed sender detection

1. Click **Services** > **Email Services** > **Anti-Spam** > **Detection Settings**.
2. Select **Global Settings** or select a domain from the drop-down list.
3. In the **Spoofed Sender Detection** section, check the **Use SPF** check box.
4. Click **Save and Exit**.

   Confirmation of the setting is displayed.

See "Enabling spoofed sender detection with DMARC" on page 25.

See "How SPF and DMARC affect each other" on page 27.

Enabling spoofed sender detection with DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) reduces email spam by detecting sender spoofing, which helps thwart phishing attempts that rely on such spoofing to penetrate an organization's defenses. DMARC standardizes how email recipients perform SPF and DKIM email authentication, and specifies appropriate actions if authentication fails. Organizations publish a DMARC policy that indicates that their emails are protected by SPF or DKIM authentication or both. The DMARC policy also tells a recipient what to do if neither of these authentication methods passes.

When you enable DMARC for a domain, inbound email to that domain is verified against the DMARC policy of the reported sender. If DMARC authentication passes, then the message is delivered normally. If DMARC authentication fails, then the message is quarantined, rejected, or delivered normally, according to the email sender's policy. If a message is from a sender on the approved senders list, then DMARC validation is bypassed even when DMARC is enabled.

DMARC senders can choose to use the policy percentage tag (`pct`) in their policies, which allows senders to phase in and fine-tune their DMARC validation. The `pct` option allows senders to stipulate that only a certain percentage of messages that meet a particular criterion will have the specified action applied to them. For example, if the sender's policy includes the name-value pair `reject, pct=10`, then only ten percent of the messages that fail validation are rejected.

When it is enabled, quarantine is provisioned for all domains in that account. You cannot provision quarantine for a subset of domains in an account. If quarantine is enabled for one of your domains, and the sender's DMARC policy is quarantine, then messages that fail DMARC validation are quarantined for all of your domains. If the senders use the `pct` tag in their policies, then only the specified percentage of messages that fail DMARC will be quarantined.

Note: If the sender's policy is to quarantine the message but you do not have quarantine provisioned, then you must either enable quarantine or specify **Subject Line Text** to indicate that this message may be spam.

DMARC requires that a message not only pass DKIM or SPF validation, but also that it passes *alignment*. To pass alignment for SPF, the message must pass the SPF check. Also, the domain in the `From:` header must also match the domain used to validate SPF. The domain must exactly match for strict alignment, or must share the org name for relaxed alignment. To pass alignment for DKIM, the message must be signed with a valid signature. Also, the `d=` domain of the valid signature must align with the domain in the `From:` header. The domain must exactly match for strict alignment, or must share the org name for relaxed alignment. DMARC validation ignores DKIM signatures with fewer than 1024 bits because such signatures are too easily forged.

DMARC authentication results and actions (quarantine, reject, or deliver normally) are displayed on the **Email Anti-Spam** tab's **Spam Dashboard Summary**. Results and actions are also included in the **Email Anti-Spam's Summary** and **Detail** reports. For messages that fail validation, the reason for the failure is displayed on the **Summary** tab of the **Track and Trace** results. Messages that DMARC validates are listed in the **Log View** tab of the **Track and Trace** results.

Note: DMARC provides a way for the email recipient to report back to the sender about the messages that pass or fail DMARC evaluation. This reporting functionality is not currently supported. However, the fact that reporting is not supported does not affect the ability of the recipient to do inbound authentication.

To perform its validation, DMARC consults authentication data from the sender, performs SPF and DKIM validation, and then adds the result to the message header as `Authentication-Results`. This information is added to message headers for the messages that are delivered normally as well as for those that are quarantined. Administrators can make use of this header information for ad hoc reporting or analysis.

You can enable DMARC for some or all of your domains. You cannot exclude specific senders from DMARC authentication, except by adding them to your

approved senders list. You cannot enable DMARC for individual groups or users; you can only enable it at the domain level.

To enable spoofed sender detection with DMARC

1. Click **Services** > **Email Services** > **Anti-Spam** > **Detection Settings**.
2. Select **Global Settings** or select a domain from the drop-down list.
3. In the **Spoofed Sender Detection** section, check the **Use DMARC** check box.
4. Click **Save and Exit**.

   Confirmation of the setting is displayed.

See "Enabling spoofed sender detection with SPF" on page 24.

See "How SPF and DMARC affect each other" on page 27.

How SPF and DMARC affect each other

SPF and DMARC enable email senders to publish the information that email recipients use to verify that senders are who they claim to be. SPF enables email senders to publish a record that authorizes sending hosts for their domains. Recipients then verify the email senders against the authorized hosts. DMARC allows email senders to publish a policy that indicates that their messages are protected by SPF or DKIM or both. The DMARC policy also tells recipients what to do if both of these authentication methods fail.

The SPF and DMARC options can be enabled and disabled independent of each other, though SPF verification is part of DMARC. Even when the SPF validation option is not enabled, if the DMARC validation option is enabled, then SPF validation takes place.

The following table summarizes the interactions between the DMARC and the SPF options. The table also describes the results of enabling and disabling SPF and DMARC in each possible combination.

Table 2-3 Interaction between the SPF and DMARC spoofed sender detection options

Options selected	Result
Neither SPF nor DMARC checked	No email sender validation is performed.

Table 2-3 Interaction between the SPF and DMARC spoofed sender detection options *(continued)*

Options selected	Result
SPF checked + DMARC unchecked	■ Do SPF validation. ■ If SPF validation fails and the sender has a hard-fail SPF policy, the message is blocked and deleted, and no further action is taken. ■ If SPF validation fails and the sender has a soft-fail or other SPF policy, then SPF verification is ignored. ■ If SPF validation passes, deliver normally.
SPF checked + DMARC checked	■ Do SPF validation. ■ If SPF validation fails and the sender has a hard-fail SPF policy, the message is blocked and deleted, and no further action is taken. ■ If SPF validation fails and the sender has a soft-fail or other SPF policy, then SPF verification is ignored. ■ Do DKIM validation and save the results for DMARC. ■ Do DMARC validation, and take the action that is specified in the sender's DMARC policy if both the SPF and the DKIM validations fail.
SPF unchecked + DMARC checked	■ Do SPF validation, but don't take any immediate action, even if it fails. ■ Do DKIM validation and save the results for DMARC. ■ Do DMARC validation, and take the action that is specified in the sender's DMARC policy if both the SPF and the DKIM validations fail.

Notes

- An SPF pass means that the sender publishes an SPF policy, and the message passes the SPF check.
- A DKIM pass means that the sender publishes a DKIM policy, the message contains a DKIM signature, and the message passes the DKIM check.
- A DMARC pass means that either:
  - SPF passes **and** the message envelope sender matches the message's sender (strict or relaxed).

    OR
  - DKIM passes **and** the signing domain matches the message's sender (strict or relaxed).

See “Enabling spoofed sender detection with SPF” on page 24.

See “Enabling spoofed sender detection with DMARC” on page 25.

See “About Anti-Spam detection settings and actions” on page 20.

Using the dynamic IP block list

The dynamic IP block list is a public block list that contains information about known spammers. The AntiSpam service uses the dynamic IP block list as part of its protection.

To enable the use of a public block list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Click the **Detection Settings** tab.

   In the **Responsive Spam Detection** area, check the **Dynamic IP public block** list box.
3. Specify an **Action** from the drop-down list, to be used for any emails sent by senders on the public block list.
4. Click **Save and Exit**.

   A confirmation of the settings is displayed.

See “About Anti-Spam detection settings and actions” on page 20.

Using the spam matching (signature) system

The signaturing system uses proprietary and commercially available signature-building engines to create a vast knowledgebase of known spam messages currently in email circulation. A signature is a unique string of bits that define a specific spam email, which can then be used to detect further instances of the email. This enables exact matching of spam, significantly reducing chances of false-positives as well as speeding identification and message-handling.

To enable the use of the signaturing system

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Responsive Spam Detection** area, select the **Use signaturing system** checkbox.

4 Select an **Action** from the drop-down list, to be used for any emails that the signaturing system finds.

5 Click **Save and Exit**.

A confirmation of the setting is displayed.

See "About Anti-Spam detection settings and actions" on page 20.

Enabling predictive (heuristic) spam detection

The Skeptic™ heuristics detection method differs from the signaturing system – it uses predictive technology instead of reactive technology. The predictive nature of Skeptic™ targets unknown spam threats and suspicious emails.

Skeptic™ scores each email against a set of rules. If an email achieves more than a specified score, it is identified as spam.

The Skeptic™ heuristics detection method helps to identify those spam emails that change most frequently, such as unsuitable or fraudulent mailings. Many organizations block and delete the suspicious emails that are detected through Skeptic™. However, due to the predictive nature of this method, you may want to quarantine such emails.

The Skeptic™ heuristics detection method also enables you to block newsletters.

To enable the use of Skeptic™

1 Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.

2 In the **Predictive Spam Detection** area, select the **Use Skeptic heuristics** checkbox.

3 To block newsletters, check the **Use newsletter detection** checkbox.

4 Select an **Action** from the drop-down list, to be used for any emails that Skeptic finds.

5 Click **Save and Exit**.

Confirmation of the setting is displayed.

Blocking newsletters

You can block newsletters globally, for a domain, or for a group.

To block newsletters globally

1. Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.
2. Ensure that **Global Settings** is selected in the drop-down list at the top of the page.
3. In the **Predictive Spam Detection** area, ensure that the **Use Skeptic heuristics** checkbox is checked.
4. To block newsletters, check the **Use newsletter detection** checkbox.
5. Select an **Action** from the drop-down list, to be used for any emails that Skeptic finds.
6. Click **Save and Exit**.

   Confirmation of the setting is displayed.

To block newsletters for a domain

1. Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.
2. Select the required domain from the drop-down list at the top of the page.
3. In the **Predictive Spam Detection** area, ensure that the **Use Skeptic heuristics** checkbox is checked.
4. To block newsletters for the selected domain, check the **Use newsletter detection** checkbox.
5. Select an **Action** from the drop-down list, to be used for any emails that Skeptic finds.
6. Click **Save and Exit**.

   Confirmation of the setting is displayed.

To block newsletters for a group

1. Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.
2. Select the domain that the group belongs to from the drop-down list at the top of the page.
3. Select the required group from the groups drop-down list.
4. In the **Predictive Spam Detection** area, ensure that the **Use Skeptic heuristics** checkbox is checked.
5. To block newsletters for the selected domain, check the **Use newsletter detection** checkbox.

6 Select an **Action** from the drop-down list, to be used for any emails that Skeptic finds.

7 Click **Save and Exit**.

Confirmation of the setting is displayed.

Allowing newsletters

You can allow newsletters globally, for a domain, or for a group.

To allow newsletters globally

1 Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.

2 Ensure that **Global Settings** is selected in the drop-down list at the top of the page.

3 In the **Predictive Spam Detection** area, uncheck the **Use newsletter detection** checkbox.

4 Click **Save and Exit**.

Confirmation of the setting is displayed.

To allow newsletters for a domain

1 Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.

2 Select the required domain from the drop-down list at the top of the page.

3 In the **Predictive Spam Detection** area, uncheck the **Use newsletter detection** checkbox.

4 Click **Save and Exit**.

Confirmation of the setting is displayed.

To allow newsletters for a group

1 Select the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.

2 Select the domain that the group belongs to from the drop-down list at the top of the page.

3 Select the required group from the groups drop-down list.

4 In the **Predictive Spam Detection** area, uncheck the **Use newsletter detection** checkbox.

5 Click **Save and Exit**.

Confirmation of the setting is displayed.

Defining a bulk mail address

If a spam detection method includes the action to **Append a header and redirect to a bulk mail address**, you must define the address to which the spam mail is redirected.

To define a bulk email address

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 Click the **Detection Settings** tab.

3 In the **Bulk Mail Address** area, enter the email address to redirect the spam mail to.

This field is inactive unless one of the spam detection actions is **Append a header and redirect to a bulk mail address**.

4 Click **Save and Exit**.

Confirmation of the setting is displayed.

See "About Anti-Spam detection settings and actions" on page 20.

Defining a subject line tag

You can define the text that is used in the subject line of a suspected spam email when the action **Tag the subject line but allow mail through** is selected. The default tag is 'SPAM:' as a prefix to the subject line. You can define whether to put the tag before or after the subject line text.

To define a subject line tag

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 Click the **Detection Settings** tab.

3 In the **Subject Line Text** area, enter the text to appear on the subject line of emails tagged as spam.

This field is inactive unless the **Predictive Spam Detection** action is **Tag the subject line but allow mail through**.

4 Select where to place the inserted text by selecting one option from:

- Put this text in front of the subject line
- Put this text at the end of the subject line

5 Click **Save and Exit**.

A confirmation of the setting is displayed.

See "About Anti-Spam detection settings and actions" on page 20.

Frequently asked questions about newsletters

The following answers are provided to help you understand how you can use Anti-Spam to manage inbound newsletters.

Table 2-4 Newsletters FAQ

Question	Answer
What is the difference between email spam and email newsletters?	Spam is defined as any unsolicited commercial email from unknown sources. The spam sender usually obtains the recipient's email address without the recipient's approval. Examples include phishing emails, advance-fee fraud scams (Nigerian 419), and emails advertising pharmaceuticals. Email messages that are normally delivered through subscription are known as newsletters. To receive a newsletter you need to subscribe to a mailing list. You may opt in to a mailing list unwittingly as part of a software installation, download registration, or membership registration.
Why do I receive these newsletters that I did not request?	You may have opted into an email newsletter without realizing it. Or, a company may pass your details on to third parties unless you actively select an option to stop it from doing so. If you do not opt out, you indirectly authorize the sender.
How can I stop receiving emails from a third party?	You can click the *unsubscribe* link that is provided in the newsletter. However, un-subscribing can be time consuming, especially if you have signed up to multiple third-party newsletters. Also, be aware that some spam messages may use an "unsubscribe" link to harvest your email address when you click on it.

Table 2-4 Newsletters FAQ *(continued)*

Question	Answer
How can Anti-Spam help me manage newsletters?	Anti-Spam can differentiate between spam and newsletters or marketing email. You can manage the handling of any newsletters using specific actions at a global or domain level. The **Detection Settings** screen in the Anti-Spam area of the portal now includes separate actions to choose from.
How do I block newsletters?	You can configure separate newsletter detection and actions in the portal. Go to **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** > **Newsletter Detection**. You can choose the newsletter action to apply to the global level, domain level, or group level.
Can I still receive selected newsletters if I block newsletters?	Yes. You can add the sender of required newsletters to your approved senders list.

Chapter 3

Managing spam quarantine

This chapter includes the following topics:

Overview of quarantine settings

The spam mail that the AntiSpam service detects 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 global and domain level.

The quarantine settings you can define within the portal are described in the following table.

Table 3-1 Email AntiSpam quarantine settings

Quarantine settings	More information
Specifying notifications	Specify whether, when an account is created, 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 notifications" on page 38. See "User notification controls" on page 40. See "Notification content and frequency" on page 40.
Defining a default language for Email Quarantine notifications	Specify the default language for the content of welcome messages and notifications. See "Configuring notifications" on page 38.
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 44.
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 "Enabling users to request approved senders" on page 42.
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 users when an alias is changed" on page 43.

Table 3-1 Email AntiSpam quarantine settings *(continued)*

Quarantine settings	More information
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 44. See "About Email Quarantine password policies" on page 45.
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 Acceptable Use Policy (AUP) available" on page 49.
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 summary notifications" on page 50.

Note: Depending on your organization's configuration of the AntiSpam service, you may not have access to the quarantine service. If you do not, the **Quarantine Settings** pages are not visible in the portal. For further details, contact the Support team.

See also Email Quarantine Quarantine Administrator Guide

See "About deploying Email Quarantine" on page 84.

Configuring 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 received spam emails. They may provide a link for the user to log on to Email Quarantine to view them. Active summary notifications contain **Release** links, for users to release an email directly from the 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, 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** > **Anti-Spam**.
2. Click the **Quarantine Settings** tab.
3. 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 a Email Quarantine user's account, that user may also be able to switch notifications off themselves.
4. If you have selected to send notifications, specify the time zone, frequency, and time of day at which notifications are sent.

   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.
5. Specify the default language for the welcome messages and notifications that are triggered by Email Quarantine.

   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.
6. Click **Save and Exit**.

   A confirmation message is displayed.

Note: You can permit new users to override these notification settings if required.

See “User notification controls” on page 40.

See “Notification content and frequency” on page 40.

User notification controls

The **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** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. Check the **Users can override notification defaults** checkbox to permit users to amend their notification settings, if required.

See “Configuring notifications” on page 38.

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.

For users to receive active summary notifications, ensure that the **Notifications** setting allows users to receive notifications.

To enable active summary notifications

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select the **Quarantine Settings** tab.
3. In the **Time Zone** area, specify the time zone to use for sending notifications to users.
4. In the **Notifications** area, ensure the box **Users receive welcome messages and summary notifications** is checked.
5. Specify the **Summary notification frequency** by selecting an hourly, multi-hourly or daily interval, and then specifying the time of day.
6. In the **Notification content** section, ensure the box **Users can release and delete (Symantec Email Quarantine only) emails directly from notifications** is checked.
7. Specify whether users can block or allow individual senders and domains.
8. Define whether or not users can access Email Quarantine using the **Disable access to Email Quarantine for users** checkbox.
9. Click **Save and Exit**.

   A confirmation message is displayed.

See “Configuring notifications” on page 38.

See “Troubleshooting active summary notifications” on page 42.

Enabling users to request approved senders

can enable Email Quarantine users to request that the sender of an email that is identified as spam is added to the organization's global approved senders . 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.

To enable users to request approved senders

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. To enable users to request additions to the approved senders list, in the **Approved sender request facility** section.
4. Enter the address to which approved senders list requests are sent.

   This address should be the address of the person who is responsible for managing the approved senders lists in the portal.
5. 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 "Uploading a group member list for AntiSpam" on page 57.

Troubleshooting active summary notifications

Table 3-2 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 spam 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 3-2 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 spam 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 "Notification content and frequency" on page 40.

See "Configuring notifications" on page 38.

Notifying users when an alias is changed

Aliases are used to:

- Direct all spam that is sent to a user with multiple email addresses to a single Email Quarantine account.
- Manage spam 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 spam using Email Quarantine as required. If 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** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. In the **Aliases** section, check the box **Users are always informed when administrators change settings which affect their aliases**.
4. 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** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. Enter the email addresses of the Quarantine Administrators. Multiple addresses must be separated with a semi-colon.

Note: The Email Quarantine Quarantine 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** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. In the **Password Controls** section, under **Password policy**, the current policy in use is displayed. This is **Basic**, **Standard**, **Enhanced**, or **Custom**.

   Custom is displayed if any changes have been made to the default settings inserted by any of the templates.

4 Check **Initial password change**.

Any new users that are created after you check this box must change their password when they first log on to Email Quarantine. This new password must comply with the password policy that you have put in place.

When you enable this option, the password change is not enforced for any accounts already in existence, even if they have not yet logged on to Email Quarantine.

5 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** button 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".

6 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?". You must 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."

7 Once you have completed all of the configuration items on this screen, select **Save & Exit**.

See “Configuring a Email Quarantine password policy” on page 47.

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 3-5 on page 46.

The following tables show the default password settings.

Table 3-3 Character requirements

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

Table 3-4 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 3-5 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 3-6 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 3-7 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 3-8 Email Quarantine lockouts (Standard Accounts)

	Basic	Standard	Enhanced
Number of incorrect password entries before lockout	100	20	9
Lockout period	30 minutes	4 hours	1 day

Table 3-9 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 “Configuring a Email Quarantine password policy” on page 47.

Configuring a Email Quarantine password policy

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

See “About Email Quarantine password policies” on page 45.

The settings for the currently selected policy are shown in Anti-Spam > Quarantine Settings > Password Controls > Password policy. The custom policy is displayed if any changes you make changes to the default settings provided by the three template policies.

To configure a Email Quarantine password policy

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select **Quarantine Settings**.
3. Click **Configure password policy**.
4. 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. If this is the first time of viewing this configuration screen since the service was provisioned, the **Basic** setting is probably already selected. To change this, select **Standard** or **Enhanced**. To enable the policy settings to be editable, check the **Customize selected policy** checkbox.
5. 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.
6. **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.
7. **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.
8. 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.
9. 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.

10 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.

11 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.

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

You are returned to the **Password Controls** configuration screen.

See "About Email Quarantine password policies" on page 45.

Making your Acceptable Use Policy (AUP) 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** > **Anti-Spam**.

2 Select **Quarantine Settings**.

3 In the **Acceptable Use Policy** section, check **Users can view your company Acceptable Use Policy (AUP)**.

4 In the field labeled **Specify URL link to your AUP:**, enter the URL for the location of the AUP document.

5 To specify where to place the link to the AUP, check one or both of the following: **Email Quarantine** and **Email Notifications**.

6 Click **Save & Exit** to apply the settings.

Defining what is visible in 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 **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.
3. In the **Visibility** section, check the items that you want to be visible to your users.
4. Click **Save & Exit** to apply the settings.

Activating Email Quarantine

Once we has provisioned your organization with Email Quarantine and you have completed the preparation, configuration, communication, and account creation stages, 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. This technology has an extremely low false-positive rate and significantly reduces the number of messages directed to Email Quarantine accounts. 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**.
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 spam 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.

Chapter 4

Groups

This chapter includes the following topics:

Defining groups for AntiSpam

Defining groups enables you to apply specific detection settings, actions for suspect mail, and approved and blocked senders lists for the members of a group.

- A group consists of a number of email addresses within a domain.
- You cannot define a group whose members are in different domains.
- An address can only belong to one group.
- You can define an unlimited number of groups.
- Groups can contain one or more addresses
- You can assign an unlimited number of addresses across all of your groups.

When a group is defined, a **Groups** drop-down list becomes available alongside the **Domains** drop-down list.

When you select a group from the list, the settings relevant to groups are presented under the following tabs: **Group Members**, **Detection Settings**, **Approved Senders**, and **Blocked Senders**. The **Groups** tab is available at domain level and provides a summary of the settings for the groups in the selected domain.

Note: Group Settings are not available by default. Contact the Support team to be provisioned with this facility.

To define a group

1. From the **Global Settings** drop down list, select a domain name.
2. Click on the **Groups** tab.
3. Click **Create new group**. The Create Group dialog box is displayed.
4. In the **Create Group** dialog box, in the **Group Name** box, type a name.
5. To find email addresses to add to the group, enter them in the **Search Email Addresses** box and click **Search**. Results are displayed in the **Available Email Addresses** box.
6. Select one or more email addresses from the search results and click the **Add to group**. The addresses are displayed in the **Group Members** list.
7. Click **Save** to create the group and confirm its members.

Viewing your AntiSpam groups

Once you have set up groups, you can inspect them and their members in the following ways. These procedures explain how to view groups, search within them and sort search results.

To view your existing groups

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain the group is in.
3. Click the **Groups** tab

   The **Groups** tab is only available at domain level.
4. The groups that have been defined for the selected domain are listed, along with the number of group members in each.

   The **Domain** and **Exclusion** entries are always present in the list. The group counter includes these entries.

To navigate to a specific group

- Use the **Previous** and **Next** navigation controls and scroll through the list.

To search for a group that contains a specific email address

- Use the **Find Email Address** search box. Enter the first part of the email address and click **Search**. The group is listed that contains the email address.

To show all results again after a specific search

- Leave the search box blank and click **Search**.

To display the group members for a group

- Click the name of the group. The **Group Members** page is displayed.

  Email addresses that are marked with *, are users who have been granted control of their personal user approved and blocked senders lists.

To sort the entries

- Click on the **Group** or **Group Members** column headings, as required.

To change the number of entries that are displayed on the page

- Use the **Entries per page** drop-down list.

Creating an AntiSpam group

For each domain name you maintain, you can create user groups consisting of selected email addresses.

To create a group

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain to create the group for.
3. Click the **Groups** tab.
4. Click **Create new group**.

   The **Create Group** window is displayed.
5. Enter a name for the group in the **Group Name** box.

   The group name must not be longer than 50 characters. Group names can only contain alphanumeric characters and spaces.

6 To display the email addresses in the domain, leave the search box blank and click **Search**.

The users in the domain are listed in the **Available Email Addresses** box. To reduce the number of addresses in the list, be more specific with your search text.

Email addresses that are marked with * indicate users who have been granted control of user approved and blocked senders lists.

7 Locate and select an email address to add to the group and click **Add to group**.

The address is displayed in the **Group Members** box.

8 Click **Save**.

The group name is displayed in the **Groups** tab and is listed in the groups drop-down list.

Note: Users cannot be added to groups if they are already on an exclusion list.

Deleting an AntiSpam group

Occasionally you may want to remove groups from the AntiSpam service. Deleting a group does not delete the users within the group.

You are not asked to confirm the deletion, so be certain that you want to delete the selected group.

To delete a group

1 Select **Configuration > Email Services > Anti-Spam**.

2 From the domains drop-down list, select the domain that the group you want to delete belongs to

3 Click the **Groups** tab.

4 Select the checkbox to the left of the group you want to delete.

5 Click **Delete selected group**.

The group is deleted.

Editing an AntiSpam group manually

You can edit the addresses in a group manually, or by downloading the existing list, editing the list offline, and then uploading the revised list to the portal. Editing can also include the group's name.

To edit an address in a group manually

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain to which the group belongs.
3. Do one of the following:
   - Click the **Groups** tab and click the group name in the **Group** column.
   - Select the group from the groups drop-down list and click the **Group Members** tab.

   The **Group Members** page is displayed.
4. To display the existing addresses in the group, leave the search box blank and click **Search**.

   The existing group members are listed in the **Group Members** box, and all of the users in the domain are listed in the **Available Email Addresses** box. To reduce the number of addresses in the list, be more specific with your search text.
5. Use the **Add to group** and **Remove from group** options to edit the addresses in the group as required.
6. Click **Save and Exit**.

To edit the name of a group

1. From the domains drop-down list, select the domain that the group is in.
2. Do one of the following:
   - Click the **Groups** tab and click the group name in the **Group** column.
   - Select the group from the groups drop-down list and click the **Group Members** tab.

   The **Group Members** page is displayed.
3. Enter the new name in the **Group Name** box.
4. Click **Save and Exit**.

Downloading an AntiSpam group member list

You can download a .csv file of group members to edit existing members, add new members offline, and upload the list back to the portal. When you save the list, ensure that it is saved in .csv format (comma-separated values, also known as comma-delimited).

To download a group member list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain that the relevant group is in.
3. Click the **Groups** tab.
4. To the right of the group name, click **Download**.

   A dialog box asks you whether to open or save the CSV file. The download operation may take some time to complete depending on the size of the list.

Uploading a group member list for AntiSpam

You can create or edit a list of group members offline and upload the list to the portal. Two options are available for uploading lists into the portal:

Merge existing addresses with uploaded addresses	By selecting this option, the uploaded list merges into the existing list. This options provides a useful way to add new addresses to an existing list. When you merge, if duplicate addresses exist within both the uploaded list and existing list, the portal displays the duplicates and gives you the option to cancel the list merge process.
Delete existing addresses and replace with uploaded addresses	By selecting this option the uploaded list replaces the existing list. **Warning:** Any addresses in the existing list that are not in the uploaded list are lost.

Addresses must be entered in the form of a full email address. Enter the email addresses in the first column. Only the addresses that belong to the selected domain and that are registered are valid. Wildcards cannot be used.

To upload a group member list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain that the relevant group is in.
3. Click the **Groups** tab.
4. To the right of the group name, click **Upload**.

   The **Upload Group Member Addresses** window is displayed.

5 Use the **Browse** option to locate the folder in which to save the CSV file, and enter the file name.

6 Select the appropriate option in the **On upload** area, depending on whether the new addresses should replace or be merged with any existing addresses (duplicate entries are ignored).

7 Click **Upload**.

The upload operation may take some time to complete, depending on the size of the list.

Uploading a global or group list to the portal for AntiSpam

You can create or edit a list of approved or blocked senders offline, and upload the list to the portal.

Two options are available for uploading lists into the portal:

Merge existing addresses with uploaded addresses	By selecting this option, the uploaded list merges into the existing list. This option provides a useful way to add new entries to an existing list. When you merge, duplicate IP addresses, email addresses, or domain entries may exist within both the uploaded list and existing list. The portal highlights the number of duplicates and gives you the option to overwrite the entries in the existing list (and to change their description, if required), or to cancel the list merge process.
Delete existing addresses and replace with uploaded addresses	By selecting this option the uploaded list replaces the existing list. **Warning:** Any entries in the existing list that are not in the uploaded list are lost.

The maximum file size for each list is 2 MB.

To upload a list

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.

3 Click **Upload**.

The **Upload Approved Addresses** or **Upload BlockedAddresses** (as appropriate) is displayed.

4 Enter the file path and name to upload or click **Browse** to locate the file.

5 Select the appropriate option in the **On upload** area, depending on whether the new addresses should replace or be merged with any existing addresses (duplicate entries are ignored).

6 Click **Upload**.

7 Click **Finish**.

The new list entries are added to the list that appears in the **Approved Senders** or **Blocked Senders** tab.

Chapter 5

Exclusions

This chapter includes the following topics:

About defining exclusions

You can define a list of email addresses to be excluded from the protection of the AntiSpam service.

This list can only be defined at domain level. You cannot specify this setting to affect your AntiSpam configuration globally or at group level.

The exclusions list can contain up to 500 addresses. Before you can populate the exclusions list, you must ensure that all relevant addresses are registered.

Settings for exclusions override any other AntiSpam settings for that user. For example, assume that companyx.com is in a blocked senders list for a specific group of users and is also in the exclusions list. Mail that is sent from that domain is not blocked, even for the users who are subject to the blocked senders list.

An address cannot be added to the exclusions list if it already belongs to a group.

Note: The functionality for exclusions is part of the Group Settings functionality. Depending on your organization's configuration, you may not have access to Group Settings. For more information, contact the Support team.

Creating an exclusions list

You may want to exclude some email addresses from AntiSpam protection. To do so, you can define an exclusion list containing the address you require.

To create an exclusion list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the appropriate domain for the user you want to exclude from AntiSpam.
3. Click the **Exclusions** tab.
4. To display the email addresses in the domain, leave the search box blank and click **Search**.

   The users in the domain are listed in the **Existing Email Addresses** box. To reduce the number of addresses in the list, be more specific with your search text.

   Addresses that belong to a group are not listed and cannot be added to the exclusions list.
5. Locate and select the email address to add to the exclusions list and click **Add to list**.
6. The address is displayed in the **Exclusion List** box.
7. Click **Save and Exit**.

   A confirmation message is displayed.

Note: You cannot select any email addresses currently set as an alias.

Downloading an exclusion list

You can download a .csv file of the users to exclude from the AntiSpam service to edit existing addresses, add new addresses offline, and upload the list back to the portal. When saving the list ensure that it is saved in .csv format (comma-separated values, also known as comma delimited).

To download an exclusion list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the appropriate domain for the user you want to exclude from AntiSpam.

3 Click the **Exclusions** tab.

4 Click **Download email addresses**.

A dialog box asks you whether to open or save the CSV file. The download operation may take some time to complete depending on the size of the list.

Uploading an exclusion list

You can create or edit a list of users to be excluded from the AntiSpam service offline and upload the list to the portal. Two options are available for uploading lists into the portal:

Delete existing addresses and replace with uploaded addresses	By selecting this option the uploaded list replaces the existing list. Any addresses in the existing list that are not in the uploaded list are lost.
Merge existing addresses with uploaded addresses	By selecting this option, the uploaded list merges into the existing list. This option provides a useful way to add new addresses to an existing list. When you merge, if duplicate addresses exist within both the uploaded list and existing list, the portal displays the duplicates and gives you the option to cancel the list merge process.

Addresses must be entered in the form of a full email address. Enter the email addresses in the first column. Only the addresses that belong to the selected domain and that are registered are valid. Wildcards cannot be used.

To upload an exclusion list

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 From the domains drop-down list, select the domain containing the user you want to exclude from AntiSpam.

3 Click the **Exclusions** tab.

4 To the right of the group name, click **Upload email addresses**.

The **Upload Exclusion List** window is displayed.

5 Use the **Browse** option to locate the folder in which to save the CSV file, and enter the file name.

6 Select the appropriate option in the **On Upload** area, depending on whether the new addresses should replace or be merged with any existing addresses (duplicate entries are ignored).

7 Click **Upload**.

The upload operation may take some time to complete, depending on the size of the list.

See "About defining exclusions" on page 60.

Chapter 6

Approved and blocked senders

This chapter includes the following topics:

About approved and blocked senders lists

You can define a list of approved senders or blocked senders for your organization. An approved sender is identified by their IP address, domain name, or email address that you want to receive email from, even though they may be on the public block list or a custom blocked list. A blocked sender is an IP address, domain name, or email address that you want to block emails from.

You can define approved and blocked senders lists at global, group, and user level. For example, you can enable some users to manage their own lists and manage those of others yourself. You can also define a user's lists initially and the individual user can manage them in Email Quarantine thereafter.

You cannot define approved senders and blocked senders lists at domain level. You define approved and blocked senders lists in the following ways:

- Manually add entries to the list in the portal.
- Download the existing list, edit it locally, and upload the revised list back to the portal.

The portal accepts entries in the following formats:

- IP address with wildcard or CIDR notation (/1 to /32)
- Domain name
- Email address

Global approved and blocked senders lists can contain up to 3000 entries each.

Warning: Do not put your domain name in your own approved senders list. By including your own domain name, you open the organization up to a security exploit. This may occur because spammers sometimes spoof the sending email address to match the target email domain (you) in an attempt to bypass AntiSpam scanning. Instead, include your partners' sending IP addresses.

Note: You cannot add a user who is on the exclusion list as an approved or blocked sender.

See also the Email Quarantine Guides

See "Managing group and user approved and blocked senders lists" on page 75.

About CIDR notation

Classless inter-domain routing (CIDR) notation is a compact representation of an IP address and its associated routing prefix. CIDR notation is constructed from the IP address and the prefix size. The prefix size is equivalent to the number of leading 1 bits in the routing prefix mask.

The IP address is expressed according to the standards of IPv4, followed by the slash ("/") character. The prefix size is expressed as a decimal number. The address may denote a single distinct interface address or the beginning address of an entire network.

The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix. For example:

- 192.168.100.0/24 represents the given IPv4 address and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0, which has 24 leading 1-bits.
- The IPv4 block 192.168.100.0/22 represents the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.254.

The portal accepts CIDR prefix sizes ranging from 1-32 in lists of approved senders and blocked senders. CIDR notation at the User level is not supported. CIDR notation is only supported at the Group level.

About group approved and blocked senders lists

Note: Depending on your organization's configuration, you may not have access to Group Settings. For more information, contact the Support team.

If you have created groups, you can create specific approved senders and blocked senders lists to apply to the members of the group. For example, a particular group can receive emails from an address that is on the organization's global blocked senders list. Group lists are defined in the same way as global lists, in the portal. First select the domain the group is in, and then select the group. You can then define the group list as required. You must define the group list from scratch. Group lists are not inherited from global lists.

Group lists are always managed in the portal by an Administrator.

When using group approved and blocked senders lists, be aware of the following guidelines:

- As soon as you give list control to a group, the global lists no longer apply to those group members. The group list either replaces or merges with the global

list, depending on your list priority settings. If list control is then deactivated, the global list automatically applies again.

- When you define either an approved senders list or a blocked senders list, the other list is also custom. If a custom approved senders list is defined for a group, then the blocked senders list is custom. The group is no longer protected by the global blocked senders list. Likewise, if a custom blocked senders list is selected for a group, then the approved senders list is also custom. The group does not receive mail from approved senders on the global approved senders list.
- The maximum number of entries in a group approved and blocked senders lists is 3000 in each.

See "Giving users control of their lists" on page 76.

See "About user approved and blocked senders lists" on page 67.

See "Managing group and user approved and blocked senders lists" on page 75.

About user approved and blocked senders lists

Note: Depending on your organization's configuration, you may not have access to User Settings. For more information, contact the Support team.

User lists enable individuals to have specific approved and blocked senders lists applied for their particular requirements. Depending on how you set up the quarantine settings, the user can manage their own list in Email Quarantine.

You can set up user lists to work in several ways:

- You define the user lists to apply for individual users. And you manage the lists in the portal on the user's behalf
- You enable users to define and manage their own lists in Email Quarantine
- A Quarantine Administrator defines and manages the lists to apply for individual users in Email Quarantine

In each of these scenarios, you must give user list control to the individual users. Users can still see and manage the lists that apply to them in Email Quarantine, even if Administrators define and manage their lists for them.

When using user approved and blocked senders lists, be aware of the following guidelines:

- As soon as you give list control to a user, the global lists no longer apply to those users. The user list either replaces or merges with the global list, depending on

your list priority settings. If list control is then deactivated, the global list automatically applies again.

- Users cannot include IP addresses in their user lists. They can only add email addresses and domain names.
  If a user list is inherited from a group list, the user may see an IP address in the list. The user cannot add an IP address.
- If a group member is enabled to have a user list, the group list is inherited for their user list. They (or an Administrator) can then customize the list.
- If a user who is enabled with user lists is added to a group, the user becomes subject to the group list. The user list functionality in Email Quarantine is disabled. The user's list and settings are remembered. If the user is then removed from the group, the original user lists and settings are applied.
- Where User Settings are active for users to manage their own lists in Email Quarantine, the Administrator can still see and amend the user lists in the portal.
- When you define either an approved senders list or a blocked senders list, the other list is also custom. If a custom approved senders list is defined for a user, then the blocked senders list is custom. The user is no longer protected by the global blocked senders list. Likewise, if a custom blocked senders list is selected for a user, then the approved senders list is also custom. The user does not receive mail from approved senders on the global approved senders list.
- The maximum number of entries in a user approved and blocked senders lists is 3000 in each.
- In the portal, you define user lists slightly differently than global and group lists.

See “Overview of quarantine settings” on page 36.

See “Giving users control of their lists” on page 76.

See “About group approved and blocked senders lists” on page 66.

See “Managing group and user approved and blocked senders lists” on page 75.

Validation rules for approved and blocked senders lists

The following validation rules apply to all approved senders and blocked senders list entries.

Table 6-1 Validation rules for list entries

Entry type	Validation rules
Email address	■ Full email addresses with valid domain names, such as `broberts@shopping.com` are valid ■ Partial email addresses, such as `broberts@shopping` are not valid ■ The `*` wildcard is not valid within an email address
Domain name	■ Full domain names, such as `example.com` are valid ■ Top-level domains, such as `com` or `uk` are valid ■ Partial domains with the top-level domain present, such as `messagelabs.com` are valid ■ Subdomains, such as `name.domain.com` are valid ■ Partial domains without the top-level domain, for example `messagelabs` or `webcam` are not valid ■ The `*` wildcard is not valid within a domain name
IP address	■ A series of basic IP address validation rules prevent any invalid IP addresses being entered into the spam lists ■ The `*` wildcard is valid to match the number in the last part of a dotted-quad IP address. For example `192.168.0.*` can be used to represent all the host IP addresses on the `192.168.0.0/24` network. Two wildcards cannot be used in an IP address ■ IPv6 IP addresses are not valid ■ CIDR accepts prefix sizes from 1-32. All other values (e.g. -1, 0, 33) are treated as a Domain. For example, values of 12.13.15.2/-1, 56.55.66.33/0, or 45.12.58.3/33 are reflected as a Domain under the “Type” column in the portal, not as an IP. ■ A CIDR range containing ‘\’ is treated as a Domain.

Viewing a global and group approved and blocked senders list

Occasionally you may need to check the content of approved and blocked senders lists at the global and group levels. The following procedures describe how to view lists, how to search for individual items within a list and how to sort results

To view an approved or blocked senders list

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 Click the **Approved Senders** or **Blocked Senders** tab, as required.

The global or group senders list is displayed:

Both approved and blocked senders are listed in the same window. Each sender's domain or email address is listed, along with whether it is an approved or blocked sender.

To search for a specific entry

- In the **Domain/Email/IP** box, use the **Search** box to locate a specific entry. Type at least the first few characters of the sender domain, email address, or IP address.

To show all results again after a specific search

- Leave the search box blank and click **Search**.

To sort the entries

- Click the column heading to sort on.

See "Managing group and user approved and blocked senders lists" on page 75.

Viewing a user approved or blocked senders list

Occasionally you may need to check the content of users' approved and blocked senders lists. The following procedures describe how to view lists, how to search for individual items within a list and how to sort results.

To view a user's approved or blocked senders list

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 From the domains drop-down list, select the domain that contains the user to apply the list to.

3 Select the **List Management** tab.

4 In the **Approved and Blocked Senders Lists** area search box, enter the part of the user's email address before the @ sign.

5 Click **Display**.

The **User Approved and Blocked Senders List** is displayed.

Both approved and blocked senders are listed in the same window. Each sender's domain or email address is listed, along with whether it is an approved or blocked sender.

To search for a specific entry

- In the **Domain/Email/IP** box, use the **Search** box to locate a specific entry. Type at least the first few characters of the sender domain, email address, or IP address.

To show all results again after a specific search

- Leave the search box blank and click **Search**.

To sort the entries

- Click the column heading to sort on.

See "Managing group and user approved and blocked senders lists" on page 75.

Adding a global approved or blocked sender

This procedure describes how to add an entry to the approved or blocked senders list.

You can also download a list as a CSV file, edit it locally, and upload it back to the portal.

To add an approved or blocked sender

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Ensure that **Global Settings** is selected in the domains drop-down list.
3. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
4. Click the **Add Entry** option.

   The **Domain/Email/IP** and **Description** fields become editable.
5. In the **Domain/Email/IP** field enter one of the three identifiers: email address, domain name, or (if working at the global level) IP address.
6. In the **Description** field, enter brief details.
7. To add the entry to the list, click **Update**.

   The entry is added to the list.

Adding a group approved or blocked sender

This procedure describes how to add an entry to a group approved or blocked senders list.

You can also download a list as a CSV file, edit it locally, and upload it back to the portal.

To add an approved or blocked sender

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Select the domain that contains the group from the domains drop-down list.
3. In the **Groups** tab, click on the name of the group.

   The group is displayed in the groups drop-down list, beneath the domains drop-down list.
4. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
5. Click the **Add Entry** option.

   The **Domain/Email/IP** and **Description** fields become editable.
6. In the **Domain/Email/IP** field enter one of the three identifiers: email address, domain name, or (if working at the global level) IP address.
7. In the **Description** field, enter brief details.
8. To add the entry to the list, click **Update**.

   The entry is added to the list.

See "Managing group and user approved and blocked senders lists" on page 75.

Downloading a global or group approved or blocked senders list

You can download a CSV file of approved senders or blocked senders. Then you can edit existing entries and insert new entries before you upload it back to the portal. When you save the list, ensure that it is saved in CSV format.

To download a list from the portal

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
3. Click **Download**.

   A dialog box asks you whether to open or save the file.

See "Viewing a global and group approved and blocked senders list" on page 69.

See "Uploading a global or group list to the portal for AntiSpam" on page 58.

Downloading a user approved or blocked senders list

You can download a .csv file of a user approved and blocked senders list to edit existing entries, insert new entries into the list, and upload it back to the portal. When you save the list, ensure that it is saved in .csv format (comma-separated values, also known as comma delimited).

To download a list from the portal

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain that contains the user to apply the list to.
3. Select the **List Management** tab.
4. In the **Approved and Blocked Senders Lists** area search box, enter the part of the user's email address before the @ sign.
5. Click **Display**.

   The **User Approved and Blocked Senders List** is displayed.
6. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
7. Navigate to the user's approved and blocked senders list.
8. Click **Download**.

   A dialog box asks you whether to open or save the file.

See "Managing group and user approved and blocked senders lists" on page 75.

Uploading a user approved or blocked senders list to the portal

You can create or edit a user approved and blocked senders list offline and upload it to the portal. Two options are available for uploading lists into the portal:

Delete existing addresses and replace with uploaded addresses	By selecting this option the uploaded list replaces the existing list. Any entries in the existing list that are not in the uploaded list are lost.

Merge existing addresses with uploaded addresses	By selecting this option the uploaded list merges into the existing list. This option provides a useful way to add new entries to an existing list. When you merge, if duplicate IP, email addresses, or domain entries exist within both the uploaded list and existing list, the portal highlights the number of duplicates and gives you the option to overwrite the entries in the existing list (and to change their description, if required) or to cancel the list merge process.

Enter the email address or domain in the first column. Enter the description in the second column. Enter *Blocked* or *Approved* in the third column.

To upload a list

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain that contains the user to apply the list to.
3. Select the **List Management** tab.
4. In the **Approved and Blocked Senders Lists** area search box, enter the part of the user's email address before the @ sign.
5. Click **Display**.

   The **User Approved and Blocked Senders List** is displayed.
6. Click **Upload**.

   The **Upload User Addresses** box is displayed.
7. Enter the file path and name to upload, or click **Browse** to locate the file.
8. Select the appropriate option in the **On Upload** area, depending on whether the new addresses should replace or be merged with any existing addresses (duplicate entries are ignored).
9. Click **Upload**.
10. Click **Finish**.

    New list entries are added to the **User Approved and Blocked Senders List**.

See "About approved and blocked senders lists" on page 65.

See "Managing group and user approved and blocked senders lists" on page 75.

Managing group and user approved and blocked senders lists

Note: Depending on your organization's configuration, you may not have access to Group Settings and User Settings. For more information, contact the Support team.

Once you have defined your group and user approved and blocked senders lists, you must apply the control of these to the specified groups and users. Until group and user list control is applied, the defined lists are not used.

If you use group and user lists, you may be able to specify how these are prioritized with the global lists. Typically, the group lists and the user lists merge with the global lists, and the global lists have priority if there are conflicts.

Note: When you give list control to a group or a user, the global list no longer applies to those group members or individual users. The group or the user list replaces or merges with the global list, depending on your list priority settings. If list control is then deactivated, the global list automatically applies again.

See "Applying group list control" on page 75.

See "Giving users control of their lists" on page 76.

See "Managing list priorities" on page 77.

Applying group list control

After you define your groups and the approved and blocked senders lists for those groups, you must set list control for each group. Until group list control is set, the group lists are not applied for the group members.

To apply group list control

1. Select **Services** > **Email Services** > **Anti-Spam**.
2. From the domains drop-down list, select the domain that contains the group to apply the group list for.
3. Select the **List Management** tab.
4. Click **Group List Control**.

   The **Group List Control** area is displayed.

5 List all available groups in the domain in the **Existing groups** box by leaving the search box blank and clicking **Search**. You can be more specific with your search text by reducing the number of groups in the list.

6 Select the group to be given group list control and click **Add to list**.

The group is listed in the **Group List Control** box.

7 Click **Save and Exit**.

See "Adding a group approved or blocked sender" on page 71.

See "Applying AntiSpam settings for a group" on page 16.

See "Managing group and user approved and blocked senders lists" on page 75.

Giving users control of their lists

You can enable individual users with their own user approved and blocked senders lists. The user or a Quarantine Administrator can define and manage the user list in Email Quarantine. An Administrator can also define and manage user lists in the portal. When you give a user control of their user lists, the **Approved Senders** and **Blocked Senders** tabs are visible in the user's Email Quarantine account. The user can then add, delete, and edit entries in their lists in Email Quarantine.

Note: A Email Quarantine User Guide is also available.

To give a user control of their user approved and blocked senders lists

1 Select **Services** > **Email Services** > **Anti-Spam**.

2 From the domains drop-down list, select the domain that the user to give control to is in.

3 Select the **List Management** tab.

4 Click **User List Control**.

The **User List Control** area is displayed.

5 List all available email addresses in the domain in the **Existing Email Addresses** box by leaving the search box blank and clicking **Search**. Or be more specific with your search text to reduce the number of addresses in the list.

6 Select the email address to be given user list control and click **Add to list**.

The email address is listed in the **User Control** box.

7 Click **Save and Exit**.

The user can now manage their approved senders and blocked senders lists in Email Quarantine.

See "Managing group and user approved and blocked senders lists" on page 75.

Managing list priorities

When group and user lists are defined, you can specify whether they replace the global lists or merge with the global lists for those group members or users.

Typically, the group lists and the user lists merge with the global lists and the global lists have priority if there are conflicts. For example, *companyx.com* is on the global blocked senders list, and a user also has it on their approved senders list. Typically, the lists are merged and the global list has priority. So emails from *companyx.com* do not reach the user, even though the user has the domain as an approved sender.

Depending on your organization's configuration, you may be able to specify one of the following scenarios for your group or your user lists:

- Group or user lists merge with the global lists and the global lists have priority if there are conflicts (typical)
- Group or user lists merge with the global lists and the group or user lists have priority if there are conflicts
- Group or user lists replace the global lists

Note: Depending on your organization's configuration, you may not be able to specify priorities for your lists. In this case, your group and user lists merge with the global lists and the global lists have priority if there are conflicts. The settings for managing list priorities are not visible in the portal.

To manage user list priorities

1 From the domains drop-down list, select the domain that the user to give control to is in.

2 Select the **List Management** tab.

3 Click **User List Control**.

The **User List Control** area is displayed.

4 Do one of the following:

- To have the user list replace the global list for the selected users click **Replace…**.
- To merge the global and user lists, click **Merge…**. Then specify which take priority in the case of conflicts, by selecting either **Global list** or **User list** from the drop-down list, as required.

5 Click **Save and Exit**.

To manage group list priorities

1 From the domains drop-down list, select the domain that the user to give control to is in.

2 Select the **List Management** tab.

3 Click **Group List Control** .

The **Group List Control** area is displayed.

4 Do one of the following:

- To have the group list replace the global list for the selected groups, click **Replace…**.
- To merge the global and group lists, click **Merge**. Then specify which take priority in the case of conflicts, by selecting either **Global list** or **Group list** from the drop-down list, as required.

5 Click **Save and Exit**.

See “Managing group and user approved and blocked senders lists” on page 75.

Chapter 7

Spam Analysis Tool

This chapter includes the following topics:

About the Spam Analysis Tool

Note: Depending on your organization's configuration, you may not have access to all of the functionality that is described here.

The Spam Analysis Tool is a self-service tool that is accessed in the portal in the Tools section. To determine if a particular email message is spam, check the email sample with the Spam Analysis Tool.

To submit an email sample for checking by the Spam Analysis Tool

1 Export the message you want analyzed from your email application to your desktop in .eml or .msg format.

Note: If a user within your organization has a message that requires analysis, that user must forward the message to you as an attachment. In particular, the user must export the email message to their desktop in .eml or .msg format. Then, the user must forward the .eml or .msg file to you as an attachment that you can then export to your desktop.

---

2 Navigate to **Tools** > **Spam Analysis Tool** in the portal.

3 Click **Browse**.

A file folder navigation window opens.

4 On your desktop, locate the .eml or .msg message file for analysis and select **Open**.

5 Click **Check** to submit the email sample for analysis.

The Spam Analysis Tool performs an analysis of your sample and returns a message that confirms the results of the check.

See "Exporting an email from Microsoft Outlook" on page 80.

See "Exporting an email from Lotus Notes" on page 81.

For information on how to export email from other applications, refer to the list that is provided at http://www.haltabuse.org/help/headers/index.shtml.

See "About AntiSpam" on page 9.

See "About Anti-Spam detection settings and actions" on page 20.

See "Submitting potential false-positive spam samples for analysis" on page 82.

See "Frequently asked questions about newsletters" on page 34.

See "About phishing emails" on page 82.

See "Blocking newsletters" on page 30.

See "Allowing newsletters" on page 32.

Exporting an email from Microsoft Outlook

Use one of the following procedures to export an email file from Microsoft Outlook.

To export an email from Outlook using drag and drop

1. In your Outlook window, select the email you want to export.
2. Click and drag the email message to your desktop, which creates an .msg file.

To export an email from Outlook using the "Save as" function

1. Open the email message you want to export.
2. From the email window, select the **Save as** menu item.
3. Save the email to your desktop in .msg or .eml format.
4. Make note of the location where you save the file.

See "Exporting an email from Lotus Notes" on page 81.

For information on how to export email from other applications, refer to the list that is provided at http://www.haltabuse.org/help/headers/index.shtml.

Exporting an email from Lotus Notes

Follow these steps to export an email message from Lotus Notes.

To export an email from Lotus Notes 5.x

1. Open your inbox and highlight the message you want to export.
2. Choose **File** > **Export**.
3. Type in a file name, leaving the file type as **Structured Text**, and click **Export**.
4. From the dialog box that pops up, choose **Selected Document** and click **OK**.
5. Open the document in WordPad or Notepad.
6. Save the file to your desktop in .eml or .msg format.
7. Make note of the location where you save the file.

To export an email from Lotus Notes 6.x, 7.x, or 8.x

1. Open the email message you want to export.
2. From the menu, select **View** > **Show** > **Page Source**.

   The email source information is displayed.
3. Cut and paste the source information into a text document in WordPad or Notepad.
4. Save the file to your desktop in .eml or .msg format.
5. Make note of the location where you save the file.

See "Exporting an email from Microsoft Outlook" on page 80.

For information on how to export email from other applications, refer to the list that is provided at http://www.haltabuse.org/help/headers/index.shtml.

About phishing emails

Phishing emails mimic legitimate organizations in branding, graphics, and style. “Phishing” emails are sent in an attempt to trick recipients into divulging personal and private information, such as credit card numbers and social security numbers.

Phishing emails are invariably bogus and the email content is designed to convince users to log on to a fake website. Phishing websites are designed to steal any information that a user inputs, with the intention of obtaining legitimate credentials for the purposes of identity theft.

See “Frequently asked questions about newsletters” on page 34.

See “About AntiSpam” on page 9.

See “About Anti-Spam detection settings and actions” on page 20.

See “About the Spam Analysis Tool” on page 79.

Submitting potential false-positive spam samples for analysis

When you submit a spam sample for analysis using the Spam Analysis Tool, the sample may already be classified as spam. If you feel that the sample should not be classified as spam, contact the Support team to request further investigation. The Support team can determine whether or not the email triggered a false-positive spam detection.

To find your Support team's contact details in the portal, navigate to **Support** > **Contact us**.

See “AntiSpam best practice settings” on page 14.

See “About the Spam Analysis Tool” on page 79.

About the Email Submission Client

Section 2

Email Quarantine deployment

Chapter 8

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. Spam is also compared against public and company blocked and approved senders lists. You can configure AntiSpam 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.

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 spam 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 8-1 Overview of Email Quarantine Deployment

Stages	Description	More information
Preparation	Ensure that the AntiSpam service has 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 87.
Configuration	Implement the decisions made about the deployment of Email Quarantine in the AntiSpam and Spam Quarantine configuration pages in the portal.	See "About Anti-Spam detection settings and actions" on page 20.
Communication	Notify users about the upcoming rollout of Email Quarantine, and its implications.	See "Communications to your organization about Email Quarantine " on page 94.
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 spam in a single owner account.	See "Email Quarantine accounts and aliases - pre-activation announcement" on page 100.
Creation of aliases from LDAP	Import into Email Quarantine any aliased email addresses specified in Active Directory. This will create accounts for primary email addresses, and their associated aliases, so that users can manage spam in a single owner account.	
Activation	Switch on Email Quarantine for the selected domains, in the portal.	See "Activating Email Quarantine" on page 50.

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

See "Email Quarantine deployment checklist" on page 102.

See "About AntiSpam" on page 9.

See "Overview of quarantine settings" on page 36.

About configuring Email Quarantine

Email Quarantine is configured in the portal. TheAntiSpam service 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**)
- 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** > **Anti-Spam** > **Quarantine Settings**)
- 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** > **Anti-Spam** > **Quarantine Settings**)
- 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** > **Anti-Spam** > **Quarantine Settings**)
- 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** > **Anti-Spam** > **Quarantine Settings**)
- 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** > **Anti-Spam** > **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** > **Anti-Spam** > **Quarantine Settings**)

Chapter 9

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 "About AntiSpam" on page 9.
  See "AntiSpam best practice settings" on page 14.
  See "About Anti-Spam detection settings and actions" on page 20.
  See "Overview of quarantine settings" on page 36.

See "About approved and blocked senders lists" on page 65.
See "About defining exclusions" on page 60.

- Listing domains
  See "Listing domains" on page 88.
- Deciding the deployment policy
  See "Deciding the Email Quarantine deployment policy" on page 88.
- Identifying Quarantine Administrators
  See "Identifying Quarantine Administrators" on page 90.
- Identifying account groups
  See "Identifying account groups" on page 91.
- Identifying aliases
  See "Identifying aliases" on page 91.
- Providing Web access
  See "Providing Web access" on page 92.
- Deciding support policy
  See "Deciding Email Quarantine support policy" on page 93.

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 9-1 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 Email Quarantine 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 spam 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 spam messages so that they can manage this spam 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.
- 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, spam 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 spam 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, to 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 spam 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 spam 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 manage spam 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, spam 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.

Note: Quarantine Administrators' tasks are described in the Email Quarantine Quarantine Administrator Guide. The guide includes a table showing how the Quarantine Administrators' tasks relate to the stages of deployment that are described here.

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 9-2 Example list of Quarantine Administrators

Name	Email address	Domain
Alex White	a.white@example.com	example.com
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 spam of several individual's accounts.

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

Table 9-3 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 spam 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, spam 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 9-4 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 spam 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 User Guide* should be updated to include this information.

Note: A Microsoft Word version of the *Email Quarantine User Guide* is available on request.

Chapter 10

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 Email Quarantine Quarantine Administrator functions, based on the content of the *Email Quarantine Quarantine Administrator Guide*.

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.

Note: See the Email Quarantine Guides

See “Identifying Quarantine Administrators” on page 90.

See “About configuring Email Quarantine” on page 86.

See “Email Quarantine accounts and aliases - pre-activation announcement” on page 100.

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 communication may include or reference the Email Quarantine User Guide.

The following is an example of an advance announcement email:

From: IT Administrator

To: All Users

Subject: Email Quarantine - A New Way To Manage Spam

As you may know, <organization> has taken measures to deal with the increasing problem of spam (unsolicited junk email). We have rolled out theAntiSpam service

from <securityservicesupplier>, the most accurate and effective antispam service available.

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

Email Quarantine identifies spam messages on your behalf and directs them to your own personal Email Quarantine account. Our antispam service is extremely accurate already, but Email Quarantine gives you a way to review the messages that the system has identified as spam. 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 anti-spam 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 spam on your behalf.

Email Quarantine will direct spam messages to your personal Email Quarantine account. Our anti-spam service is very accurate already, but Email Quarantine gives you a way to review messages sent to you that the system has identified as spam. 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 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 91.

See “Email Quarantine accounts and aliases - pre-activation announcement” on page 100.

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 Spam

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

Your current Email Quarantine setup identifies spam emails on your behalf and directs them to your own personal Email Quarantine account. Our anti-spam service is extremely accurate already, but Email Quarantine gives you a way to review your messages that the system has identified as spam. You access your Email Quarantine account via a Web browser.

The spam 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 11

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

Accounts are created in **Email Quarantine** > **Administration**. For full details, see the Email Quarantine Quarantine Administrator Guide.

Accounts are created in **Email Quarantine** > **Administration**. For full details, see the *Email Quarantine Quarantine Administrator Guide*.

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 90.

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 91.
  - To consolidate the spam of a user with multiple email addresses into a single owner account (alias).
    See "Identifying aliases" on page 91.

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

See "Activating Email Quarantine" on page 50.

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.

See the *Anti-Spam Service Administrator Guide* for further details.

See the Email Quarantine Quarantine Administrator Guidefor further details.

Email Quarantine deployment checklist

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

Table 11-1 Deployment checklist

Step	Process	Date completed
1. Preparation	■ Set up the AntiSpam 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** > **Anti–Spam** > **Quarantine Settings** 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.	

Table 11-1 Deployment checklist *(continued)*

Step	Process	Date completed
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**.	