# Email AntiSpam Administrator Guide

Symantec.cloud

# AntiSpam Administration Guide

Documentation version: 2_23_17

## 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

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.<br>AntiSpam distinguishes newsletters from spam. You can choose to detect newsletters as well as spam.<br>See "Enable predictive (heuristic) spam detection" on page 27. |
| Signaturing system | Various signature-building engines that create a vast knowledgebase of signatures of spam messages currently in email circulation.<br>See "Using the spam matching (signature) system" on page 26. |
| Dynamic IP block list | A recognized public block list of IP addresses of globally known sources of spam.<br>See "Using the dynamic IP block list" on page 26. |
| Exclusions | A list of email addresses to be excluded from the protection of AntiSpam.<br>See "About Anti-Spam defining exclusions" on page 40. |
| 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.<br>SPF cannot be configured for specific groups.<br>See "Enabling spoofed sender detection with SPF" on page 22. |

**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.<br>DMARC cannot be configured for specific groups.<br>See "Enabling spoofed sender detection with DMARC" on page 22. |
| 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.<br>**Note:** DKIM verification cannot be initiated directly. Rather, DKIM verification takes place as part of the DMARC authentication process.<br>See "Enabling spoofed sender detection with DMARC" on page 22. |

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 10.

See "About Anti-Spam detection settings and actions" on page 17.

See "Defining groups for AntiSpam" on page 32.

# 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 10.

# 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 "Enable predictive (heuristic) spam detection" on page 27.

# 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 12.

See "Applying AntiSpam settings for a specific domain" on page 13.

See "Applying AntiSpam settings for a group" on page 13.

See "AntiSpam best practice settings" on page 10.

# 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 11.

See "Applying AntiSpam settings for a specific domain" on page 13.

See "Applying AntiSpam settings for a group" on page 13.

See "AntiSpam best practice settings" on page 10.

# 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 11.

See "Applying AntiSpam global settings " on page 12.

See "Applying AntiSpam settings for a group" on page 13.

See "AntiSpam best practice settings" on page 10.

# 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 11.

See "Applying AntiSpam global settings " on page 12.

See "Applying AntiSpam settings for a specific domain" on page 13.

See "Defining groups for AntiSpam" on page 32.

See "AntiSpam best practice settings" on page 10.

# 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.

See “AntiSpam best practice settings” on page 10.

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.<br>You can define lists of approved senders by IP addresses, domains, or email addresses. |

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

| Detection methods | Description |
|---|---|
| **Spoofed Sender Detection** | Enable **Use SPF** (Sender policy framework) to verify email senders against the list of authorized hosts for a domain.<br><br>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.<br><br>See "How SPF and DMARC interact during Anti-Spam scanning" on page 24.<br><br>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. |
| **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.<br><br>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.<br><br>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.<br><br>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.<br><br>For each **Responsive Spam Detection** setting that you enable, choose an action from the drop-down list. See Table 2-2 for descriptions. |

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

| Detection methods | Description |
|---|---|
| **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.<br>See Table 2-2<br>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. |
| **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.<br>Check the box to enable the **Use Newsletter / Marketing detection** service and select an action from the drop-down menu.<br>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.<br>See "FAQs about newsletters and marketing emails" on page 30. |

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:<br>`X-Spam-Flag:YES`<br>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.<br>The detected email is delivered to the recipient's email inbox. |

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

| Action | Description |
|---|---|
| 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.<br>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. |
| 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.<br>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.<br>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.<br>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 37.

See "About Anti-Spam detection settings and actions" on page 17.

# 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 "About Anti-Spam detection settings and actions" on page 17.

# 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 22.

See "How SPF and DMARC interact during Anti-Spam scanning" on page 24.

# 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 22.

See "How SPF and DMARC interact during Anti-Spam scanning" on page 24.

# How SPF and DMARC interact during Anti-Spam scanning

Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC) are two protocols that email senders can use to assure email recipients that senders are who they claim to be. SPF publishes a record that authorizes domains of sending hosts. Recipients then verify the email senders against the authorized hosts. DMARC publishes 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.

In the **Services > Email Services > Anti-Spam > Detection Settings** tab, you can enable SPF and DMARC options separately, though SPF verification is part of

DMARC. The following table summarizes the interactions between the DMARC and the SPF options.

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

| Options selected | Result |
|---|---|
| **Neither SPF nor DMARC checked** | No email sender validation is performed. |
| **SPF checked + DMARC unchecked** | ■ Do SPF validation.<br>■ 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.<br>■ If SPF validation fails and the sender has a soft-fail or other SPF policy, then SPF verification is ignored.<br>■ If SPF validation passes, deliver normally. |
| **SPF checked + DMARC checked** | ■ Do SPF validation.<br>■ 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.<br>■ If SPF validation fails and the sender has a soft-fail or other SPF policy, then SPF verification is ignored.<br>■ Do DKIM validation and save the results for DMARC.<br>■ 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 validation fails.<br>■ Do DKIM validation and save the results for DMARC.<br>■ 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).

# 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 17.

# 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 17.

# Enable predictive (heuristic) spam detection

The Skeptic™ heuristics detection method differs from the signaturing system because 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 Navigate in the portal to the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.

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

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

4 Click **Save and Exit**.

Confirmation of the setting is displayed.

See "About Anti-Spam detection settings and actions" on page 17.

# Blocking newsletters and marketing emails

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

**To block newsletters and marketing emails:**

1. Navigate in the portal to the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.
2. To block newsletters and marketing emails *globally*, select **Global Settings** from the drop-down list.

   To block newsletters and marketing emails at the *domain* level, select the required domain from the drop-down list.

   To block newsletters and marketing emails for a *group*, select the domain the group belongs to from the drop-down list. Then, select the required group from the groups drop-down list.
3. In the **Newsletter / Marketing Detection** section, select the **Use Newsletter / Marketing detection** check box.
4. Select an **Action** from the drop-down list, to be used for any newsletters or marketing emails.
5. Click **Save and Exit**.

   A confirmation of the setting is displayed.

See "About Anti-Spam detection settings and actions" on page 17.

# Allowing newsletters and marketing emails

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

**To allow newsletters and marketing emails:**

1. Navigate in the portal to the **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** tab.
2. To allow newsletters and marketing emails *globally*, select **Global Settings** from the drop-down list.

   To allow newsletters and marketing emails at the *domain* level, select the required domain from the drop-down list.

   To allow newsletters and marketing emails for a *group*, select the domain the group belongs to from the drop-down list. Then, select the required group from the groups drop-down list.

3 In the **Newsletter / Marketing Detection** section, deselect the **Use Newsletter / Marketing detection** check box.

4 Click **Save and Exit**.

A 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 17.

# 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 17.

# FAQs about newsletters and marketing emails

The following information is provided to help you understand how you can use Anti-Spam to manage inbound newsletters and marketing emails.

**Table 2-4** Newsletters FAQ

| Question | Answer |
|---|---|
| What is the difference between email spam and newsletters or marketing emails? | 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.<br><br>Email messages that are normally delivered through subscription are known as newsletters or marketing emails. To receive a newsletter or marketing email you usually need to subscribe to a mailing list. You may also opt in to a mailing list unwittingly as part of a software installation, download registration, or membership registration. |
| Why do I receive these newsletters or marketing emails that I did not request? | You may have opted into a newsletter or marketing email 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 or marketing email . 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 and marketing emails? | Anti-Spam can differentiate between spam and newsletters or marketing emails. You can manage the handling of any newsletters and marketing emails using specific actions at a global, domain, or group 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 or marketing emails? | You can configure separate newsletter and marketing email detection and actions in the portal. Navigate to **Services** > **Email Services** > **Anti-Spam** > **Detection Settings** > **Newsletter / Marketing Detection**. You can choose an action to apply to the global level, domain level, or group level. |
| Can I still receive selected newsletters if I block newsletters or marketing emails? | Yes. You can add the sender of required newsletters or marketing emails to your approved senders list. |

Chapter 3

# 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.
- Groups can contain one or more addresses

There are two limits to consider when managing Anti-Spam groups. The maximum number of groups per domain is limited to 20. The maximum number of users within these groups is limited to 150 across all groups, per domain.

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.<br>**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.

See "About approved and blocked senders lists" on page 45.

# Uploading a global or group approved or blocked senders 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.<br>**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.

See "About approved and blocked senders lists" on page 45.

Chapter 4

# Exclusions

This chapter includes the following topics:



## About Anti-Spam defining exclusions

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

This list can only be defined at domain level. You cannot specify this setting to affect your Anti-Spam 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 Anti-Spam 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.

---

See “About Anti-Spam defining exclusions” on page 40.

See “Downloading an exclusion list ” on page 41.

See “Uploading an exclusion list” on page 42.

# 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.

See "About Anti-Spam defining exclusions" on page 40.

See "Creating an exclusions list" on page 41.

See "Uploading an exclusion list" on page 42.

# 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 Anti-Spam defining exclusions” on page 40.

See “Creating an exclusions list” on page 41.

See “Downloading an exclusion list ” on page 41.

Chapter 5

# 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

The maximum number of entries in a group's approved and blocked senders lists is 150 entries per list, for a total of 300 entries.

---

**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 Anti-Spam 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.

---

Email Anti-Spam Administrator Guide and Email Quarantine Deployment Guide

See "Adding a global approved or blocked sender" on page 51.

See "Adding a group approved or blocked sender" on page 52.

See "Downloading a global or group approved or blocked senders list" on page 52.

See “Downloading a user approved or blocked senders list” on page 53.

See “Managing group and user approved and blocked senders lists” on page 55.

# 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's approved and blocked senders lists is 150 entries per list, for a total of 300 entries.

See "Giving users control of their lists" on page 56.

See "About user approved and blocked senders lists" on page 47.

See "Managing group and user approved and blocked senders lists" on page 55.

# 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 “Giving users control of their lists” on page 56.

See “About group approved and blocked senders lists” on page 46.

See “Managing group and user approved and blocked senders lists” on page 55.

# Validation rules for approved and blocked senders lists

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

**Table 5-1** 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<br>■ Partial email addresses, such as `broberts@shopping` are not valid<br>■ The `*` wildcard is not valid within an email address |
| Domain name | ■ Full domain names, such as `example.com` are valid<br>■ Top-level domains, such as `com` or `uk` are valid<br>■ Partial domains with the top-level domain present, such as `messagelabs.com` are valid<br>■ Subdomains, such as `name.domain.com` are valid<br>■ Partial domains without the top-level domain, for example `messagelabs` or `webcam` are not valid<br>■ 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<br>■ 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<br>■ IPv6 IP addresses are not valid<br>■ 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.<br>■ A CIDR range containing ‘\’ is treated as a Domain. |

See “About approved and blocked senders lists” on page 45.

See “Adding a global approved or blocked sender” on page 51.

# 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 55.

# 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 55.

# 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.

See "About approved and blocked senders lists" on page 45.

See "Validation rules for approved and blocked senders lists" on page 48.

See "Downloading a global or group approved or blocked senders list" on page 52.

See "Uploading a user approved or blocked senders list to the portal" on page 54.

# 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.

The maximum number of entries in a group's approved and blocked senders lists is 150 entries per list, for a total of 300 entries.

**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 "About approved and blocked senders lists" on page 45.

See "Validation rules for approved and blocked senders lists" on page 48.

See "Downloading a global or group approved or blocked senders list" on page 52.

See "Managing group and user approved and blocked senders lists" on page 55.

# 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 "Uploading a global or group approved or blocked senders list to the portal for AntiSpam" on page 38.

See "About approved and blocked senders lists" on page 45.

# 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 "About approved and blocked senders lists" on page 45.

See "Uploading a user approved or blocked senders list to the portal" on page 54.

See "Managing group and user approved and blocked senders lists" on page 55.

# 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 45.

See "Managing group and user approved and blocked senders lists" on page 55.

# 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 55.

See "Giving users control of their lists" on page 56.

See "Manage list priorities" on page 57.

See "About approved and blocked senders lists" on page 45.

# 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 "Managing group and user approved and blocked senders lists" on page 55.

# 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.

Email Quarantine User Guide

**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 55.

# Manage 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**.

Chapter 6

# 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 60.

See "Export an email from Lotus Notes" on page 61.

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 Anti-Spam detection settings and actions" on page 17.

See "Submit potential false-positive spam samples for analysis" on page 62.

# 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 “Export an email from Lotus Notes” on page 61.

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.

# Export 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 60.

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 “FAQs about newsletters and marketing emails” on page 30.

See “About Anti-Spam detection settings and actions” on page 17.

See “About the Spam Analysis Tool” on page 59.

# Submit 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 10.

See “About the Spam Analysis Tool” on page 59.