Email Data Protection

Administrator Guide

Symantec.cloud

Email Data Protection Administrator Guide

Documentation version: 1.0

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 Email Data Protection

This chapter includes the following topics:

About Email Data Protection

The Email Data Protection service is a managed email service that allows you to identify and to control any confidential, malicious, or inappropriate content that your employees send or receive.

The service enables you to monitor and enforce your email security policy. Enforcing your email security policy helps to protect your employees and your brand, and safeguards against the increasing risk of litigation. You define a set of policies that help to enforce your organization's email security policy.

Use the service to enforce policies that:

- Protect corporate reputation
- Preserve confidentiality and security
- Reduce legal liability
- Defend against careless and malicious actions
- Ensure regulatory compliance
- Reduce lost productivity
- Retain network bandwidth.

You build a list of policies that matches your business requirements. When you activate the policies in your list, the system checks your emails against each policy in turn. Each policy in your list can contain multiple conditions.

We provide policy templates that address specific regulatory requirements. We also provide pre-defined lists of keywords that you can use in your policies. The policy templates and the pre-defined lists enable you to build robust and reliable policies easily and quickly.

The Email Data Protection service scans the various parts of an email, including the subject line, and the body, as well as file attachments, such as Microsoft Office documents, documents in PDF format, and text files. The scanning engine unpacks and looks inside compressed files to detect the file extensions or content that is defined in your policies.

If an email triggers a policy in your policy list, an incident is generated that appears in the Email Data Protection reports. You can view the details of the incident and take appropriate action. The action that you take is likely to depend on the agreements that you have reached with your Human Resources and Legal departments.

Configuring the Email Data Protection service - step by step

You configure the Email Data Protection service in the portal. You define a set of policies that help to enforce your organization's email security policy.

Each policy identifies the emails that contain content or the attachments that contravene the policy. An action is associated with each policy. For example, if an email contains a profanity, the action might be to redirect the message to an administrator. You can establish a policy that applies to all domains, or to specific domains.

We suggest the following approach to configuring the service:

Table 1-1 Configuration steps for Email Data Protection

Step	Action	Further details
Step 1	Plan your overall policy in cooperation with your Human Resources, Compliance, and Legal departments.	Do you have an acceptable use policy that determines the way you want your users to use email? For example, there may be privacy issues in your country that you need to speak to your Legal department about.

Table 1-1 Configuration steps for Email Data Protection *(continued)*

Step	Action	Further details
Step 2	Plan the steps that you want to take when an incident occurs.	The policies that you create lead to incidents when a policy is triggered. Email Data Protection reports include the details of the incidents that have been logged. You need to review these reports on a regular basis and follow up on the incidents that are logged. You should implement a process for handling the incidents that appear on the reports. Email Data Protection does not provide an automatic process for dealing with the incidents that arise from the policies that you have created.
Step 2	Decide whether your policies are to apply to all domains or whether you require different polices for specific domains.	It might be useful to create your policies for a single domain and test that they work to your requirements. Then you can copy them to all of your domains.
Step 3	If your policies are to be based on user groups, ensure that you have the correct structure in place.	Create custom user groups and view LDAP groups to specify as senders or recipients to use in the policies. See "About user groups" on page 27.
Step 4	Determine the lists that you require for use in your polices.	Consider the managed lists that we provide. Do these meet your requirements? Create lists of file names, keywords, MIME types, domain names, URLs and so on, to use in your policies. See "About custom and managed lists" on page 36. See "Applying global or custom settings to a domain" on page 25.
Step 4	Provide values for various general settings	The settings include default administrator and sender email address, which are used in email notifications. See "About general settings in Email Data Protection" on page 12.

Table 1-1 Configuration steps for Email Data Protection *(continued)*

Step	Action	Further details
Step 6	Create your policy list.	Review the predefined templates and check whether they meet your requirements. You can amend a template, adding conditions, notifications and actions. You can also create your own policies from scratch. See "About policies and Email Data Protection" on page 59. See "Creating an Email Data Protection policy - process overview" on page 66.
Step 7	Test your policy list.	When you set up a new policy initially, we recommend that you set a less severe action, such as **Log only**, **Tag with Header**, **Tag Subject**, or **Copy to Administrator**. You can then check that the policy works, before instigating a more severe action such as **Redirect to Administrator** or **Block and Delete**.

Email Data Protection best-practice settings

The polices that you define for Email Data Protection assist in monitoring and controlling your company's acceptable use policy. You can use our predefined policy templates as a starting point, to address specific regulatory requirements.

We recommend that initially you set up five policies to log various aspects of content within emails, as follows:

- Log inbound emails over 2MB
- Log outbound profanities
- Block inbound emails over 10MB
- Log audio and video files inbound and outbound.

Once you are familiar with the kinds of emails that are detected, you can feel more confident in blocking some, and redirecting others. The following are some common policies. But every organization is different. We recommend that you do not set up these example rules without understanding the requirements of your business. You can then align your email security policy with these requirements.

Table 1-2 Common Email Data Protection Policies

Policy	Description
Block emails over 25MB	Reduces the size of emails coming into the organization to save bandwidth. All emails over 25MB can be blocked and deleted. You can send notifications to all parties.
Redirect emails to/from suspicious domains	Monitors emails coming from or going out to competitors' domains, restricting the passing on of intellectual property and poaching of employees.
Monitor profanity outbound	Protects the organization's brand and reputation. For example, you can prevent an employee from sending out an email containing slander to a friend.
Redirect encrypted or password-protected mail	Enables you to monitor and control who sends and receives encrypted or password-protected messages.
Compress emails of between 10MB and 25MB	Reduces the bandwidth that is taken up by large messages coming into the organization.

See “About Email Data Protection” on page 7.

See “Configuring the Email Data Protection service - step by step” on page 8.

See “About general settings in Email Data Protection” on page 12.

See “About policies and Email Data Protection” on page 59.

See “Creating an Email Data Protection policy - process overview” on page 66.

Chapter 2

Defining general settings

This chapter includes the following topics:

About general settings in Email Data Protection

You can enter your own default values for some general settings that are used when you create policies. For example, you can define the subject line text for the Tag Subject action.

When you configure the Email Data Protection service, you decide whether you want to use the same values for all of your domains, or create alternative settings for one or more domains.

You create global settings to use with all or some of your domains. For any remaining domains, you create custom settings that are specific to each domain. By default, all domains inherit the global settings, and all your policies inherit these settings. If

you apply custom settings to a domain, all policies that you create for the domain inherit the custom settings. For most of the general settings, you can choose different values for specific policies.

See "Applying global or custom settings to a domain" on page 25.

The following table describes the general settings that you can define for Email Data Protection.

Table 2-1 General settings in Email Data Protection

Setting	Description
Default email addresses	The **Default administrator email address** is the email address to which redirected or copied emails and notifications are sent. The **Default sender email address** is the email address that notifications appear to be sent from. A recipient can use this email address to reply to a notification. See "Defining an administrator email address" on page 14. See "Defining a sender email address" on page 15.
Default notification settings	When a policy is triggered, you can choose to notify the system administrator, the sender of the email, and the recipients of the email. We provide a standard message for each notification. You can replace the standard messages with your own versions. See "Defining the email notification settings" on page 16.
Default time zone	The default time zone is used in the **Time zone** condition. When you add a Time Interval condition to a policy, you can accept the default time zone or change it to a different zone. See "Defining the default time zone" on page 21. See "Adding a Time Interval condition to a policy" on page 88.
Subject line text	Type the text that you want to appear in the Subject line of an email. When you select the **Tag Subject** action for a policy, this text is added to the Subject line of the email before it is delivered to the recipient. See "Defining the default subject line tag text" on page 22.

Table 2-1 General settings in Email Data Protection *(continued)*

Setting	Description
Reporting	The Reporting settings enable you to include certain information in the Email Data Protection detailed report. The report helps you understand the incidents that occur as a result of Email Data Protection processing. When you select **Show matched content on reports**, the content that caused the policy to trigger appears on the report. When you select **Show surrounding text on reports**, the report includes 40 characters on each side of the matched text. See "Defining the reporting settings" on page 23.

Defining an administrator email address

You can define the default email address to which notifications, and copied and redirected emails, are sent. You can define an administrator email address at global, domain, or policy level.

Note that the address you provide for the administrator can be the overall administrator of the service, or a Human Resources representative, or Compliance officer.

An administrator email address bypasses the Email Data Protection scans. Emails that are sent from or to the administrator email address do not trigger your policies.

To define an administrator email address at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select **All** from the **Apply to:** drop-down list, and click **Settings**.

   These are global settings. By default, they apply to all domains.
3. In the **Default email addresses** section, enter an address for the **Default administrator email address**.
4. Click **Save**.

To define an administrator email address at domain level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

   These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.
3. In the **Default email addresses** section, enter an address for the **Default administrator email address**.
4. Click **Save**.

To define an administrator email address at policy level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click the name of an existing policy or click **New policy**.
3. Select the **use custom** check box.
4. Replace the default administrator email address with a custom address that is specific to the policy.
5. Click **Save**.

See "About general settings in Email Data Protection" on page 12.

See "Defining a sender email address" on page 15.

See "Defining a sender email address" on page 15.

Defining a sender email address

You can define the **Default sender email address** that notifications appear to come from. Thus, users can reply to an appropriate person rather than to a generic email address, which may not accept a reply. Note that this address must be from a domain that you have registered in the portal.

You can define a value for the **Default sender email address** setting at global and domain levels. You cannot apply a different setting at policy level.

Note: A notification is sent to the sender of a triggered email if **Notifiy sender** is defined as a general setting.

See "Defining the email notification settings" on page 16.

To define a sender email address at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select **All** from the **Apply to:** drop-down list, and click **Settings**.

   These are global settings. By default, they apply to all domains.
3. In the **Default email addreseses** section, enter an address for the **Default sender email address**.
4. Click **Save**.

To define a sender email address at domain level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

   These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.
3. In the **Default email addreseses** section, enter an address for the **Default sender email address**.
4. Click **Save**.

See "Defining an administrator email address" on page 14.

See "Defining a sender email address" on page 15.

Defining the email notification settings

When a suspect email is detected, you can send a notification email to your system administrator, the email sender, and the email recipients. The text for each notification can be different. You define the information that you want to include in the email. You can provide your users with explicit information about a suspect email and the policy that detected it. For example, you can notify the sender of an email that it contains a video attachment that they can only send after a certain time.

An email may trigger more than one policy. If an email triggers multiple policies, multiple notifications may be sent to the administrator; one for each policy that the email has triggered. In this case, each instance of the email is combined into a single email. If a rule triggers a multi-recipient email to be blocked for a particular recipient, scanning continues for all other intended recipients. The Email Data Protection detailed report records that a policy has been triggered. The service adds the following information into the header of detected emails:

X-ContentInfo	Displays the name of the policy matched.
X-Content-Flag	Set to 'yes' if content is detected.
X-Content	Displays the reason that the email has been detected, that is, the suspect content and its location within the email.

You can define system administrator, sender, and recipient notifications at the following levels.

- Global level
  The notification settings apply to all policies in all domains, unless you choose different settings for one or more domains or policies.
- Domain level.
  The notification settings apply to all policies in a specific domain, unless you choose different settings for one or more policies within the domain. If you do not create notification settings for a domain the policies for the domain use the global notification settings.
- Policy level
  The notification settings apply to a specific policy. If you do not create notification settings for a policy the settings are inherited from the domain, if you have domain level settings, or from the global level.

To define the default email notification settings at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select **All** from the **Apply to:** drop-down list, and click **Settings**.

   These are global settings. By default, they apply to all domains.
3. In the **Default email addresses** section, type an email address for the following:
   - Default administrator email address
     See "Defining an administrator email address" on page 14.
   - Default sender email address.
     See "Defining a sender email address" on page 15.
4. In the **Default notification settings** section, select the check box for **Notify Administrator**, **Notify Sender**, or **Notify Recipient(s)**.
5. Choose whether to accept the default notification text or select **Custom** from the drop-down list to provide your own text.

6 Make your changes to the **Subject** and **Body** fields.

You can add placeholders to provide additional information to the message. For example, you can add the date, the name of a suspect file or the name of the policy that triggered the notification email. Select the placeholders from the **Insert placeholder** drop-down list.

7 Click **Save**.

To define the default email notification settings at domain level

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.

3 In the **Default email addresses** section, type an email address for the following:

- Default administrator email address
  See "Defining an administrator email address" on page 14.
- Default sender email address.
  See "Defining a sender email address" on page 15.

4 In the **Default notification settings** section, select the check box for **Notify Administrator**, **Notify Sender**, or **Notify Recipient(s)**.

5 Choose whether to accept the default notification text or select **Custom** from the drop-down list to provide your own text.

6 Make your changes to the **Subject** and **Body** fields.

You can add placeholders to provide additional information to the message. For example, you can add the date, the name of a suspect file or the name of the policy that triggered the notification email. Select the placeholders from the **Insert placeholder** drop-down list.

7 Click **Save**.

To define the email notification settings at policy level

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Click the name of the policy you want to amend or click **New policy**. A new policy uses a default notification, provided by either the global or the domain level settings. An existing policy uses either a default or a custom notification.

3 To view and edit the current settings click **Edit**.

The **Notifications** dialog is displayed.

4 To apply custom notification settings to the policy, check the **Use custom notification** check box.

5 Select the notifications that you want to send. You can notify any combination of administrator, sender, or recipient.

6 For each notification, accept or update the content in the **Subject** and **Body** fields.

You can add placeholders to provide additional information to the message. For example, you can add the date, the name of a suspect file or the name of the policy that triggered the notification email. Select the placeholders from the **Insert placeholder** drop-down list.

7 To re-apply the default notification settings, uncheck the **Use custom notification** check box.

8 Click **Edit**.

See "Applying global or custom settings to a domain" on page 25.

See "Defining an administrator email address" on page 14.

See "Defining a sender email address" on page 15.

About placeholders in email notifications

You use placeholders to add variables to a notification email. The placeholders enable you to provide useful information to the system administrator, the email sender, and the email recipients. For example, you can include the name of the policy that was triggered, or the name of a suspect attachment.

Use these placeholders when you create the notification text for your global, domain or policy level notifications.

See "Defining the email notification settings" on page 16.

The following table describes the placeholders that are available:

Table 2-2 Placeholders for notifications

Placeholder	Description
%d	Adds the date that the email was sent. For example, "The email was sent on %d"
%t	Adds the subject line of the email. For example, "An email that is sent to you with the following subject line was blocked: %t"

Table 2-2 Placeholders for notifications *(continued)*

Placeholder	Description
%p	Adds the plain text section of the email body. This placeholder is not allowed in messages to administrators. For example, "An email containing the following text has been blocked: %p"
%y	Adds the file name of a suspect attachment. For example, "An email containing the following attachments has been blocked: %y"
%e	Adds the envelope sender of the email, that is the actual sender of the email. For example, "The sender address of the email was: %e"
%s	Adds the message body senders, that is, the reply to address in the email. For example, "The reply to address of the mail was: %s"
%S	Adds the IP address of the sending server. For example, "The sender's IP address was: %S"
%r	Adds the envelope recipients, that is, all recipients, including bcc recipients. This placeholder is not allowed in messages to the recipient or to the administrator, as bcc (blind carbon copy) recipients should only be visible to the sender. For example, "The recipient address of the email was: %r"
%g	Adds the message body recipients. This placeholder does not include bcc recipients.
%E	Adds the reason text. For example, "The email was blocked for the following reason: %E"

Table 2-2 Placeholders for notifications *(continued)*

Placeholder	Description
%F	Adds the matched content, that is, the word, phrase, or string of numbers that has caused the policy to trigger. For example, "The email content %F contravened the policy %R" **Note:** A string of asterisks replaces the matched content if you have chosen to hide matched content. You can hide matched content when you use Content Regular Expression List condition. You might hide matched content to comply with the data privacy regulations in a country in which you operate. See "Adding a Content Regular Expression List condition to a policy" on page 77.
%R	Adds the Email Data Protection policy name, that is, the name that you gave to the policy, when you created it. We recommend that you give your policies meaningful names so that it is easy to understand the function of the policy. When a policy is triggered, the policy name appears in the Email Data Protection Detailed report. You can choose to include the policy name in an email notification to the system administrator, email sender, or email recipient. For example, "The email contravenes the following policy: %R"

Defining the default time zone

You can define the default time zone to apply to the **Time Interval** condition. You might use the Time Interval condition in a policy to restrict the sending of large emails to outside office hours.

You can specify a value for the time zone at global or domain levels. You can choose a different time zone when you add the **Time Interval** condition to a policy.

See "Adding a Time Interval condition to a policy" on page 88.

To define a default time zone at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click **Settings**.
3. Select **All** from the **Apply to:** drop-down list, and click **Settings**.

   These are global settings. By default, they apply to all domains.
4. In the **Default time zone** section, select a zone from the drop-down list.
5. Click **Save**.

To define a default time zone at domain level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click **Settings**.
3. Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

   These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.
4. In the **Default time zone** section, select a zone from the drop-down list.
5. Click **Save**.

See "Defining an administrator email address" on page 14.

See "Defining a sender email address" on page 15.

Defining the default subject line tag text

The subject line tag text applies to the **Tag Subject** action. When you specify an action of Tag Subject for a policy, the tag text appears in the subject line of the email, when it is delivered to the recipient. For example, you can warn the recipient that the email may contain inappropriate content.

You can specify default subject line tag text at global or domain levels. You can also apply custom tag text for a specific policy.

To define default subject line tag text at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select **All** from the **Apply to:** drop-down list, and click **Settings**.

   These are global settings. By default, they apply to all domains.
3. In the **Subject line text** section, enter new text for the tag or accept the default text of *Unacceptable Content*. The maximum number of characters that the tag can have depends on the language that you use. The tag text can contain non-Western characters.
4. Choose to put the text before or after the subject line text in the tagged email.
5. Click **Save**.

To define default subject line tag text at domain level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

   These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.
3. In the **Subject line text** section, enter new text for the tag or accept the default text of *Unacceptable Content*. The maximum number of characters that the tag can have depends on the language that you use. The tag text can contain non-Western characters.
4. Choose to put the text before or after the subject line text in the tagged email.
5. Click **Save**.

To define the subject line tag text at policy level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click the name of an existing policy or click **New policy**.
3. Select **Tag Subject** from the **Action** drop-down list.

   The **Subject line text** field appears, with the default text displayed.
4. Select the **use custom** check box.

   The default subject line text is cleared, and you can enter new text for this policy.

   The maximum number of characters depends on the language. The tag text can contain non-Western characters.
5. Choose to put the text before or after the original subject line text of the email.
6. Click **Save**.

See “Defining an administrator email address” on page 14.

See “Defining a sender email address” on page 15.

Defining the reporting settings

The Email Data Protection reports enable you to investigate the incidents that arise from the scanning processes. The incidents are logged when an active policy is triggered.

The reporting settings are relevant when you include a *content* condition in a policy. In content conditions, you match the items in a keyword list, a regular expression list or a URL list, with the content in an email.

The reporting settings are as follows:

- **Show matched content on reports**
  The Email Data Protection detailed report includes the content in the email that caused the policy to trigger. For example, if a policy includes a condition to find credit card numbers, the numbers that triggered the policy appear in the report. An exception to this behavior occurs when you use the regular expression list condition in a policy and select **Redact matched text**. The **Redact matched text** setting ensures that a string of asterisks replaces matched text in the reports. You might want to use this setting to comply with the data privacy regulations in a country in which you operate.
  See "Adding a Content Regular Expression List condition to a policy" on page 77.
- **Show surrounding text on reports**
  The Email Data Protection detailed report includes 40 characters on each side of the matched content.

You can only define the **Show matched content on reports** and **Show surrounding text on reports** settings at global and domain levels. You cannot apply different reporting settings at policy level.

Note: A user needs the **View Sensitive Data** custom role to view the matched content in the Email Data Protection detailed report.

To define the reporting settings at global level

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Select **All** from the **Apply to:** drop-down list, and click **Settings**

   These are global settings. By default, they apply to all domains.
3. In the **Reporting** section, select the **Show matched content on reports** and **Show surrounding text on reports** radio buttons, as required.
4. Click **Save**.

To define the reporting settings at domain level

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Select a domain from the **Apply to:** drop-down list, click the **Custom** radio button and click **Settings**.

These are custom settings. They apply only to the selected domain. You can switch between custom and global settings using the **Custom** and **Global** radio buttons. These buttons appear when you select a specific domain.

3 In the **Reporting** section, select the **Show matched content on reports** and **Show surrounding text on reports** radio buttons, as required.

4 Click **Save**.

See "About general settings in Email Data Protection" on page 12.

See "Adding a Content Keyword List condition to a policy" on page 75.

See "Adding a Content Regular Expression List condition to a policy" on page 77.

See "Adding a Content URL List condition to a policy" on page 80.

See "Defining an administrator email address" on page 14.

See "Defining a sender email address" on page 15.

Applying global or custom settings to a domain

You can enter your own default values for some general settings that are used when you create policies. For example, you can define the subject line text for the **Tag Subject** action.

When you configure the Email Data Protection service, you decide whether you want to use the same values for all of your domains, or create alternative settings for one or more domains.

You create global settings to use with all or some of your domains. For any remaining domains, you create custom settings that are specific to each domain. By default, all domains inherit the global settings, and all your policies inherit these settings. If you apply custom settings to a domain, all policies that you create for the domain inherit the custom settings. For most of the general settings, you can choose different values for specific policies.

To apply global or custom settings to a domain

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Select a domain from the **Apply to:** drop-down list.

The **Global** and **Custom** radio buttons appear.

3 Do one of the following:

- Click **Global** to apply global settings to the domain.
- Click **Custom** to apply custom settings to the domain.
  When the **Custom** radio button is selected for a domain, click **Settings** to view or amend the settings for the domain.

4 Click **Save**.

Note: You can create and apply custom settings to a domain, then switch back to global settings. Your custom settings are remembered. Click **Custom** to re-apply the original custom settings to the domain.

See "About general settings in Email Data Protection" on page 12.

See "Defining an administrator email address" on page 14.

See "Defining a sender email address" on page 15.

Setting the maximum size of emails received into the organization

You can set a maximum size above which inbound emails to your organization are rejected. You cannot specify the maximum size to be more than 1,000,000 KB.

To set an email size limit

1 Select **Services** > **Email Services** > **Platform**.

2 In the **Message Size** tab, in the **Set maximum email size to** box, enter the maximum size for emails (in KB) .

3 Click **Save**.

When an email is rejected because it exceeds the maximum email size, an alert is sent to the administrator addresses that are configured on the **Services > Anti-Malware > Alert Settings** tab.

Chapter 3

Working with user groups

This chapter includes the following topics:

About user groups

A user group is a set of users to apply to in sender and recipient conditions in your Email Data Protection policies and for your Email Disclaimers.

Users and groups can derive from three sources:

- LDAP users and groups
- Custom users and groups
- Domains

Table 3-1 Types of user group

Type of user group	Description
LDAP users and groups	Synchronize user and group data with your LDAP directory using the Synchronization Tool. The tool extracts user and group information from your LDAP directory data sources and exports this data to the infrastructure. LDAP user groups can be viewed in the portal alongside your custom user groups. You cannot edit LDAP users and groups in the portal. Amendments to these must be performed within your directory data. To use the Synchronization Tool, the portal administrator must have **Edit Configuration** permission for the **LDAP User Groups** service. You cannot add LDAP users to a custom user group, nor custom users to an LDAP user group.
Custom users and groups	Create and edit custom users and user groups in the portal. Custom user groups can be viewed in the portal, alongside your LDAP user groups. You can also upload a CSV file listing custom users in a group. Custom groups are useful if you want to include users in the groups that are not stored in your directory data. For example, you can add external email addresses to your custom groups.

The following characteristics apply to user groups:

- A group can consist of a single user
- A user may belong in more than one group
- If a group is defined at global level, it can contain users from different domains
- A group must have at least one user assigned to it
- A group can contain up to 1,000,000 users

You can view LDAP users and groups, and manage custom groups and users, at global and domain level:

- Global level - enables groups to be managed across all domains
- Domain level - enables you to manage user groups specific to that domain.
  You can use a group that is defined at the global level in an Email Data Protection policy that is specific to an individual domain. An Email Data Protection policy set for a domain applies only to those members of the user group who belong to that domain.
  Only groups defined at global level can be assigned to Email Disclaimers.

Note: For Email Data Protection policies, you can also detect email according to the domains that it is sent to or from. For this, use domain lists in your sender and recipient conditions.

See "About custom and managed lists" on page 36.

Viewing user groups

You can view your LDAP and custom user groups in the portal.

To view your user groups

1. Select **Services** > **Email Services** > **Platform**
2. Click the **User Groups** tab.

   The LDAP and custom user groups available at the level you have selected (global or domain) are listed with the following details:

Group Name	For custom groups, click on the group name to view full details of the group and its members in the **Edit User Group** page.
Group Type	Displays whether the group is an LDAP or custom group.
Members	Displays the number of users in the group
Used By?	Displays whether the group is used in any Email Data Protection policies.
Disclaimers	Displays whether the group has a custom email disclaimer applied to it. You can only assign a group to a single custom disclaimer.
Last Updated	Displays the date and time the group was last edited.

   Only 500 groups are displayed at a time. To avoid too long a list, search using the **Group name** box and the **Group type** filter. The **Group name** search box accepts wildcards for partial matching. The wildcard * is interpreted as zero or more unknown characters, for example, `W*d` finds words including `Wild` and `Withheld`.

To view the members of a custom user group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, click on the name of the group to view in the **Group name** column.

   The **Edit User Group** page is displayed.

   The users in the group are listed in the **Group members** box.

   To locate a specific group member, use the **Email address** search box. Enter a full email address or a partial email address to search for.

Creating a custom user group

You can create a user group manually in the portal and add existing or new email addresses (users) to it.

You can also create and edit the users in a group in a CSV file and upload the file to the portal.

See "Editing a custom user group using a CSV file" on page 32.

To create a custom user group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, click **Create new group** .

   The **Create Group** page is displayed.
3. Enter a name for the user group.

   The user group name must be unique, contain alphanumeric characters and spaces (but no other character types), and begin with an alphabetic character. Double-byte characters are not supported.
4. Search for an existing user by using the **Email address** search box. Select the required user in the **Available users** box.

   The search affects both the **Available users** and **Group members** boxes. Up to 500 users are displayed. To display fewer users, refine your search criteria.

   The available users are those harvested from the emails that are sent from your organization, and those previously added manually or uploaded to a group.
5. Click **Add** .

   The email address is added to the **Group members** box.
6. Click **Save**.

Editing a custom user group manually

You can maintain a custom user group manually in the portal. You can edit the group name, and add and remove users from the group.

You cannot delete a user group if it is in use in an Email Data Protection policy or has a custom email disclaimer applied to it.

Deleting a user from a group does not permanently delete the user, but merely removes it from the user group or groups that it is associated with.

You cannot edit LDAP user groups in the portal. Instead, edit LDAP user groups and their members in your LDAP data source.

To edit a custom user group manually

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, click on the name of the required group.

   The **Edit User Group** page is displayed.
3. Edit the group name if required.
4. Edit the group details as required.

   Locate a user using the **Email address** search box. Add or remove the users as required.

   Only 500 users are displayed at a time. To avoid too long a list, narrow your search criteria.
5. Click **Save**.

To delete a custom user group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, select the checkbox next to the name of the group to delete.
3. Click the **Delete selected group(s)** button.
4. Click **OK** to confirm.

To delete a user from a custom user group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, select the checkbox next to the group name that contains the user to delete.
3. Click **Delete users** .

   The **Delete Users** window is displayed.

4 Locate an existing user, using the **Search existing users** box.

If you leave the box blank, an alphabetical list of all available users is displayed in the **Existing users** box. To avoid the list becoming too long, only the first 500 users are shown. If more than 500 users are available, use the search facility to reduce the list size.

5 Highlight the required user and click **Delete Users**.

The address of the user to delete is displayed in the **Deleted users** box.

6 When you have selected the users to delete, click **Delete Users** at the bottom of the page.

Editing a custom user group using a CSV file

You can maintain a custom user group using a CSV file. Use a CSV (comma-separated values) file to create or edit a list of the users that belong to a user group. You can add new email addresses or edit existing ones offline. Then upload the list to the portal. The file to upload must be a CSV file.

You can download the list again at any time, to make further changes.

Note: You cannot edit LDAP user groups in the portal. Instead, edit LDAP user groups and their members in your LDAP data source.

To download a list of users in a custom user group

1 Select **Services** > **Email Services** > **Platform**

2 In the **User Groups** tab, locate the name of the group to download and click the **Download** button.

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.

To edit a CSV list of users in a group

1. Open a new or a previously downloaded CSV file.
2. Edit the file to your requirements.

   The file contains a list of your users' email addresses in the first column. You can use the second column for associated descriptions (optional).

   To simplify the list, use wildcards to detect email addresses with slight differences in spelling, for example, fre*@domain.com represents fred@domain.com or *freda@domain.com*.
3. Save the file as a CSV file.

To upload a list of users for a custom user group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, select the **Upload** button next to the name of the group to upload the email addresses to.

   The **Upload users** window is displayed.
3. In the **Select file to upload** field, enter the file path and file name to upload or click **Browse** to locate the file.
4. Select either:

Delete existing addresses and replace with uploaded addresses	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	The uploaded list merges into the existing list. This is a useful way to add new entries to an existing list.

5. Click **Upload**.

   If the file contains invalid entries, an error message displays the first 100 invalid addresses but continues to upload all the valid addresses. If this is displayed, click **OK**.

   A confirmation message is displayed.
6. Click **OK**.

Creating a user for a custom group

You can create a new user to add to a custom group.

To create a new user for a custom group

1. Select **Services** > **Email Services** > **Platform**
2. In the **User Groups** tab, locate and select the group to create the new user for.

   The **Edit User Group** page is displayed.
3. Add the new email address in the **New users** box.
4. Click **Save**.

Chapter 4

Working with custom and managed lists

This chapter includes the following topics:

- Migrating lists from Email Content Control to Email Data Protection

About custom and managed lists

In the Data Protection services, a list is a container for one or more items of a particular content type, for example, keywords, domains, URLs, regular expressions, and so on.

A custom list is a list that you create to meet the requirements of your organization. A managed list is a predefined list of items that we provide. You cannot update or delete a managed list. Periodically, we update the managed lists to include new items, such as additional keywords.

We provide managed lists for the following content types:

- Keywords
  These lists contain words and phrases to detect content, such as unacceptable language or personal banking keywords.
  See "About managed keyword lists" on page 37.
- Regular expressions
  Regular expressions are used for pattern matching. The regular expressions often search for personally identifiable information, such as passport numbers, social security numbers, and so on.
  See "About managed regular expression lists" on page 39.

Our policy templates typically include combinations of managed keyword lists and managed regular expression lists. The policy templates address common regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA). When you create your policies, you can base them on one of our templates, then update them to meet your exact requirements.

A list can contain up to 2000 items and you can create a maximum of 500 lists. You can combine multiple lists into list groups. This means that a list group can contain many thousands of items.

Viewing your custom and managed lists

You view your custom lists and the managed lists that we provide in the **Lists** page.

To view your custom and managed lists

1 Select **Services** > **Data Protection** > **Lists**.

  The page displays the custom and the managed lists that are available to you.

2 To view only the custom lists, click the **Custom Lists** title bar.

To view only the managed lists, click the **Managed Lists** title bar.

The following details are displayed for each list.

Content type The list can be one of the following content types:

- File types
- MIME types
- Keywords
- Regular expressions
- URLs

See "About content types and lists" on page 55.

List type The list can be one of the following list types:

- Single
  The list contains one list and the entries in the list are of the same content type.
- Group
  The list contains multiple lists and all the lists in the group are of the same content type.

Category Displays the industry-recognized category of the list or **None**, if a category does not apply.

Active If the list is used in a policy, this column shows the number of policies that use the list.

To view the names of the policies, click the drop-down icon. Then, to see the rules, conditions, notifications, and actions that make up the policy, click the policy name.

Last updated Displays the date on which the list was last amended and the name of the user who made the update.

About managed keyword lists

We provide the following managed keyword lists for you to use with the Data Protection services. We may update a managed list to add new keywords. You cannot update or delete a managed list.

To see the keywords in each list, click the list name in **Services** > **Data Protection** > **Lists**.

Table 4-1 Managed keyword lists in Data Protection

List name or type	Description
ABA Keywords	The ABA routing number is a nine-digit number that is assigned to financial institutions by The American Bankers Association. The ABA number identifies the financial institution upon which a payment was drawn. The list includes words and phrases, such as bank routing number, american bank association routing number, and so on.
Credit Card Keywords	A list of credit card keywords, covering credit card issuers, such as Visa, and related keywords, such as bank card, check card, and so on.
Profanities, and racial and sexual slang	Various lists of keywords are available, covering mild and serious profanities, and sexual and racial slang. The lists are available in English, French, and German.
Health Insurance Portability and Accountability Act (HIPAA)	HIPAA requires the protection of personally identifiable information and the creation of standard procedures to be followed for the execution of electronic transactions. Various lists of keywords are available that cover prescription drugs, disease names, and medical treatments.
Personal Financial	A list of financial words and phrases, such as credit limit, bankrupt, monthly income, and so on.
Personal Financial Banking	A list of banking-related words and phrases, such as signature loan, break-even lease payment, call loan, and so on.
Personally Identifiable Info	A list of words and phrases relating to personally identifiable information, such as Birth Date, Employee ID, National Insurance Number, and so on.
US SSN Keywords	A list of words and phrases that relate to United States social security numbers, including tax ID, SSN, social security, and so on.

About regular expressions

In Data Protection, you use a regular expression to search content for a pattern that may indicate that your users are distributing a particular type of information. For example, you might use a regular expression to detect credit card numbers. If three or more suspected credit card numbers are found in the content, you can follow up on this incident.

You add regular expressions to a list, in a similar way as you add keywords. You can use a managed regular expression that we have created or you can create your own regular expressions.

When you type or paste a regular expression into a list, the system validates that it conforms to the correct syntax for Java 7. It is possible that a regular expression that you create may not perform exactly as you expect. This could mean that the processing of the policy "times out" to protect the performance of our infrastructure for all clients.

About managed regular expression lists

We provide the following managed regular expression lists for you to use with the Data Protection services. Each managed regular expression list contains a single regular expression. When you create your policies, you can combine multiple custom or managed regular expression lists to provide the solution that you require.

Table 4-2 Managed regular expression lists in Data Protection

List name	Notes	Examples of matches	Examples of non-matches
ABA Routing Template	Find matches for an ABA routing number. This is a nine-digit number. There is no match if there is an alphanumeric character or a hyphen in front of or at the end of the digits. There is no match if there is a plus symbol in front of the digits.	012345678 012345678 no 012345678~no	012345678no

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
AJL Credit Card	Find matches for AJL Credit Card numbers.	36159576425302 374615373757171 5269760516591108 4336687003806412 3833 975077 0420 3014-716500-6142 3469-737207-60884 3582-5049-2386-6975 4892 1817 0946 7063	1.36159576425302
Birthdate	Find matches for birth dates.	DOB 01/01/1901 BIRTH 01/01/1901 BIRTHDAY 1-1-1901 BIRTH DAY 1.1.01 BIRTHDATE 01-01-1901 01-01-1901 DOB dob 01/01/1901 birth 1/01/1901 birthday 1-1-1901 birth day 01.01.01 birthdate 01-01-1901 01-01-1901 dob	01/01/1901 01.01.1901 01-01-1901 1.1.01 1/1/01 1-1-01

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
Credit Card Numbers (Restricted Format Matches)	Find matches for all kinds of credit card numbers. A LUHN algorithm check is applied. The separator can be a white space, or nothing, but cannot be a dash (-).	36334984144312 3633 498414 4312 348526158792841 3485 261587 92841 4402064770623264 4402 0647 7062 3264	3633-498414-4312 3485-261587-92841 4402-0647-7062-3264 15796851482832 14376871315261 31900597738008 32047800412648 37778165362375 3843776760017319 3647034435804432 47625697369931 45448191895224 47290380507287 5100-0000-0000-0000 3400-000000-00000

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
Custom Credit Card Numbers	Find matches for custom credit card numbers.	5100 0000 0000 0000 5200 0000 0000 0000 5300 0000 0000 0000 5400 0000 0000 0000 5500 0000 0000 0000 4000 0000 0000 0000 3400 000000 00000 3700 000000 00000 3000 000000 0000 3010 000000 0000 3020 000000 0000 3030 000000 0000 3040 000000 0000 3050 000000 0000 3600 000000 0000 3800 000000 0000 6011 0000 0000 0000 2014 000000 00000 2149 000000 00000 3000 0000 0000 0000 2131 000000 00000 1800 000000 00000 5100-0000-0000-0000 3400-000000-00000 3000-000000-0000 5100000000000000 340000000000000 30000000000000	

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
General DL identifier for records	Find matches for the words *driver license* and similar spellings. The case of the text is ignored.	driver license driver licenses driving license Driver License driver licensing driverlicense dl # dl# lic # lic#	driver's license driver-license driv. license
MA, VA, KY, KS, AZ DL 1 Alpha 8 Numeric	Find matches for driver license expressions for the following US states—MA, VA, KY, KS and AZ. The format of these is a single alphabet character followed by 8 digits.	A12345678 a12345678	123456789 AA1234567 A12345678a
Driver license	Generic Driver license template for the US.	B356 1258 4578 B356-1258-4578	B35612584578 B356 1258-4578
UK DL 1	Find matches for UK driving licenses. There is no match if the expression is at the beginning or the end of a line.	ABCDE 101317 ABCAB ABCD9 101317 AB9AB ABCD0 101317 AB0AB ABCD9 163317 ABCAB ABCDE101317ABCAB	ABCDE A01317 ABCAB ABDDE 101317 ABC12
NJ DL 1 Alpha (1st Letter Last Name) 14 Numeric	Find matches for New Jersey driver licenses. The format of these is a single alphabet character followed by 14 numbers. There is no match if the expression is at the beginning or the end of a line.	A12345678901234	A123456789012345 AA12345678901234 A12345678901234A

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
FL, MD, MI, MN DL Letter plus 12 Digits	Find matches for Florida, Maryland, Michigan and Minnesota driver licenses. The format is a single alphabet character followed by 12 numbers. There is no match if the expression is at the beginning or the end of a line.	A123456789012	AA123456789012 A1234567890123
IL DL First Letter Of Last Name And 11 Digits	Find matches for Illinois driver licenses. The first letter of the last name is followed by 11 numbers. There is no match if the expression is at the beginning or the end of a line.	A12345678901 a12345678901	AB12345678901 A123456789012 A12345678901B
NY SC,CO, CT, HI, MS, NM, ND, OK DL 9 Numeric	Find matches for driver licenses for the following US states—NY, SC, CO, CT, HI, MS, NM, ND, OK. There is no match if the expression is at the beginning or the end of a line.	123456789	A123456789 1234567890 123456789A
CA DL 1 Alpha 7 Numeric	Find matches for California driver licenses. The format is a single alphabet character followed by 7 numbers. There is no match if the expression is at the beginning or the end of a line.	A12345678	AA12345678 A12345678
Custom SSN MED	US Social Security Number.	123-12-1234	123-12-12345
2011 HCPCS in Regex for HIPAA	Find matches for Healthcare Common Procedure Coding System (HCPCS) codes for HIPAA.	12345 123456 123456789 AB12345	H0001
ICD 10 for HIPAA	Find matches for ICD-10 (International Classification of Diseases) codes for HIPAA.	A00.00xA S00.0xxA	A00.1
ICD 9 for HIPAA	Find matches for ICD-9 (International Classification of Diseases) codes for HIPAA.	E12.1 E12.12 12.1 12.12 123.1 123.12	AB12.1 123.12A

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
CPT Category 1 or 2 or 3 Codes for HIPAA	Find matches for HIPAA CPT (Current Procedural Terminology) Category 1, 2 or 3.	CPT 12345 CPT blah 12345	CPT 1000F
2010 FDA NDC Codes for HIPAA	Find matches for FDA (Food and Drug Administration) National Drug Codes.	1234-1234-12 12345-123-12 12345-1234-1	1234-12345-1
Drug Codes US	Find matches for HIPAA, NDC, and variants.	12345-1234-12 12345-123-12 12345-*123-12 12345-1234-1 12345-1234-*1 1234-1234-12 *1234-1234-12 A12345-123-12	1234-1234-123 AB1234-1234-12
US ITIN	Find matches for US Individual Taxpayer Identification Numbers (ITIN).	912-89-1234	812-89-1234
Latvian Personal ID	Find matches for Latvia Identity Card Numbers. The format is DDMMYY-XNNNC. The first six numbers are a birth date. X is the century a person was born in (0 for XIX, 1 for XX and 2 for XXI). NNN is birth serial number in that day. C is checksum digit.	301299-11234 010199-11234 200299-21234	013199-11234 010199-31234
SSN (Complete No Hyphen)	Find matches for social security numbers of the format AAAGGSSSS where AAA is the area number from 000 to 772. This is for valid SSNs prior to June 25th 2011.	123121234	000121234 123001234 123120000 A123121234 123121234 773121234

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
SSN Complete	Find matches for social security numbers of the format AAA-GG-SSSS where AAA is the area code 000 to 772. This is for valid SSNs prior to June 25th 2011. The separator can be a space or a "-". This does not match valid SSNs following by "-". It does not match the number strings inside a math context or pure data list.	123-12-1234 123 12 1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 773-12-1234 123-12-1234-
SSN with space dash slash	Find matches for social security numbers of the format AAA-GG-SSSS where AAA is from 000 to 772. This is for valid SSNs prior to June 25th 2011. The separator "-" can be replaced by " " or "/" in all occurrences.	123-12-1234 123 12 1234 123/12/1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 773-12-1234 123 12/1234
US SSNs (All matches)	Find matches for social security numbers of the format AAA-GG-SSS, which include randomization SSNs and those prior to June 25th 2011. Matches all formats including these delimiters: , ' ! # $ % * + . If an SSN is followed by a separator and then by a digit, it is not a match.	123 45 6789 123/45/6789 123-45-6789 123456789	
US SSNs (Restricted Format Matches)	The same as **US SSNs (All Matches)** except that the delimiter can only be a slash (/) or a white space.		
Custom SSN	Find matches for social security numbers of the format AAA-GG-SSSS where AAA is from 000 to 772. This is for valid SSNs prior to June 25th 2011.	123-12-1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 123 12 1234 773-12-1234

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
UK NINos	Find matches for UK National Insurance Numbers. This only matches if there is a letter at the end. Though only A, B, C or D is valid as the final letter, this template matches with any letter. The letter is not part of the matching sequence; it exists only to cause the JR 56 43 23 to match. Without the final letter, JR 56 43 23 does not match.	JR 56 43 23 A jr 56 43 23 a AA 11 11 11 A JR564323 AA111111 JR 56 43 23 Z AA 11 11 11 F	DA 11 11 11 A JR 56 43 23 AA 11 11 11
SSNVS No Hyphen	Find matches for social security numbers of the format AAAGGSSS, which includes randomization SSNs and those prior to June 25th 2011.	123121234	000121234 123001234 123120000 A123121234 12312/1234 1231212341
SSNVS space, dash, slash	Find matches for social security numbers of the format AAA-GG-SSSS where AAA is from 000 to 772. This is for valid SSNs prior to June 25th 2011. The separator "-" can be replaced by " " or "/" in all occurrences.	123-12-1234 123 12 1234 123/12/1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 773-12-1234 123 12/1234
SSNVS (Restricted Format Matches)	Find matches for social security numbers of the format AAA GG SSS, which includes randomization SSNs and those prior June 25th 2011. The separator " " can be replaced by "/" in all occurrences. It does not match if an SSN is followed by a separator and then by a number.	123 12 1234 123/12/1234	000 12 1234 123 00 1234 123 12 0000 A123 12 1234 123 12/1234 123 12 1234 1
SSNVS (All matches)	Find matches for all social security numbers. It is very similar to **SSNVS space dash slash**, except it allows no separator. A LUHN algorithm check is not applied.		

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
SSNVS Complete	Find matches for social security numbers of the format AAA-GG-SSS, which includes randomization SSNs and those prior June 25th 2011. The separator "-" can be replaced by " " in all occurrences. It does not match if an SSN is followed by a separator and then by a number.	123-12-1234 123 12 1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 123-12/1234 123-12-1234-1
Custom SSN	Find matches for social security numbers of the format AAA-GG-SSS, which includes randomization SSNs and those prior to June 25th 2011. It does not match if an SSN is followed by a separator and then by a number.	123-12-1234	000-12-1234 123-00-1234 123-12-0000 A123-12-1234 123-12/1234 123-12-1234-1
UK National Insurance	Find matches for UK National Insurance Numbers such as JG 121316 A. The last alphabet character can be omitted. No space is allowed between the six numbers.	JG 121316 A JG121316A JG121316 JG 121316	JG 12 13 16 A JG 12 13 16
UK Passport old type	Find matches for old type UK passports.	A1234A A12345 01234A 012345	a1234A 01234a
UK Electoral Role	Find matches for UK electoral role codes.	AB1 AB12 AB123 AB1234 ABC1 ABC1234	ab1 ab12345 ABCD1

Table 4-2 Managed regular expression lists in Data Protection *(continued)*

List name	Notes	Examples of matches	Examples of non-matches
UK Passport new type	Find matches for new type UK passports. The format is xxxxxxxxx, where x is a number.	123456789	1234567890 a123456789 123456789a

Searching your custom lists and managed lists

You can view the custom lists and the managed lists that are available to you. You can search the lists to find a specific list. You can also search for an item within a list. The search returns both single lists and list groups.

To search your custom lists and managed lists

1. Select **Services** > **Data Protection** > **Lists**.
2. Type your search text in the **Search list name or content** field.
3. Choose to search on all lists, or select a specific content type from the drop-down list. For example, you can search only keyword lists.
4. Click **Search**.

   The search returns the lists where the name of the list or the list content contains the search text. For example, if your search text is "profan" then lists with the following names are returned:

   - English profanities
   - Profanity main list
   - Profanities.

   The search does not include support for wildcards. If you type "profan*" in the **Search list name or content** field, the search results include only the lists that contain exactly that string.

Creating a custom list

You can create a custom list in the following ways:

- By creating a new list from scratch, containing all the items that you require
- By copying an existing custom or managed list, and amending it to your requirements.

A list must contain entries of one content type only. For example, you cannot create a list that contains both URLs and regular expressions.

A list can contain up to 2000 items and you can create a maximum of 500 lists. You can combine multiple lists into list groups. This means that a list group can contain many thousands of items.

To create a custom list by copying a custom or managed list

1. Select **Services** > **Data Protection** > **Lists**.
2. Select the check box next to the custom or managed list that you want to copy.
3. Click the **Copy** option.
4. Click **Save**.

   Click on the list to open it and update it to meet your requirements.

To create a custom list from scratch

1. Select **Services** > **Data Protection** > **Lists**.
2. Click **New List**.
3. Type a name and a description for the list and complete the following:

   Category — Do one of the following:

   - Choose a standard industry category for the list, such as Educational or Healthcare
   - Select **None** if you do not want to apply a category to the list.

   Content Type — Choose from the following content types:

   - File types
   - MIME types
   - Keywords
   - Regular expressions
   - URLs

4. Add items to the list, as follows:
   - For a regular expression list, paste a regular expression that you have created and tested into the **Add list items** check box and click **Add**.
   - For all other list types, type the keywords or phrases into the **Add list items** box and click **Add**.
5. Click **Save**.

Editing a custom list

You can edit a custom list to update it to meet your requirements, by adding or removing items.

Look in the **Active** column on the **Lists** page to see if a list is used in a policy. The **Active** column displays the number of policies that use the list. Click the link to view the names of the policies. Click the policy name to view details of how the list is used in the policy. We recommend that you take care when modifying a list that is currently used in an active policy.

To edit a custom list

1. Select **Services** > **Data Protection** > **Lists**.
2. Select a list and amend the following details, as required:
   - Name
   - Description
   - Category
   - List contents.

   You cannot change the content type of a list. Note also that a list can only contain items of one content type. For example, you cannot include keywords and URLs in the same list.
3. Click **Save** to save the changes to the list.

Deleting a custom list

You cannot delete a custom list if it is used in a policy or if it is part of a list group. Look in the **Active** column on the **Lists** page to see if a list is used in a policy. The **Active** column displays the number of policies that use the list. Click the link to view the names of the policies. Click the policy name to view details of how the list is used in the policy.

You cannot delete a managed list.

To delete a custom list

1. Select **Services** > **Data Protection** > **Lists**.
2. Select the check box next to the list that you want to delete.
3. Click the **Delete** link below the **Custom Lists** heading.
4. Click **Delete** to confirm.

About list groups

A list group contains multiple single lists of the same content type. For example, you might want to create a list group that combines the lists of profanities for English, French and German into one master list.

You use list groups in your policies in the same way that you use a single list.

A single list can contain up to 2000 items. There is no restriction on the number of single lists that you can include in a list group. This means that your list group can contain many thousands of items.

A list group can include managed lists and custom lists. A list group is automatically updated when any of the single lists that it includes is changed.

Note: A list group is a convenient way of managing multiple lists of the same content type. However, to use more than one list in a policy, you do not have to create a list group. When you create the policy, you can specify more than one list in your policy condition.

Including and excluding items in a list group

You can specify whether to *Include* or *Exclude* lists from at list group.

Generally, you use *Include* lists, where you combine multiple lists for convenience and ease of management. For example, you might have separate lists of profanities in English, French, German and so on, and you might include all these lists in one list group. You can then use the single list group in your policies.

In some situations, you might want to have both *Include* and *Exclude* lists in a list group. We provide a number of managed lists, and we periodically update them with new items. You can take advantage of this service, but you may want to exclude some items from the list. For example, supposing you want to use our managed lists of profanities in your policies, but there are some items that you do not want to flag as sensitive. To achieve this, do the following:

- Review the managed lists of profanities and note the items that you do not view as sensitive.
- Create a custom list that includes the non-sensitive items.
- Create a list group and select the managed lists as *Include* lists.
- Select your custom list as an *Exclude* list.

When the system evaluates the list, the items that are on the *Exclude* custom list but also on the *Include* managed list are excluded from the list of items that your content is checked for.

Creating a list group

A list group contains multiple single lists of the same content type. For example, you might want to create a list group that combines the single lists of profanities for English, French and German into one master list.

To create a list group

1. Select **Services** > **Data Protection** > **Lists**.
2. Click **New List Group**.
3. Type a name and a description for the list group.
4. Complete the following:

Category	Do one of the following: ■ Choose a standard industry category, such as Educational or Healthcare. ■ Select **None**, if you do not want to match a category with the list group.
Content Type	Choose from the following types: ■ File types ■ MIME types ■ Keywords ■ Regular expressions ■ URLs

   When you choose a content type, the right-hand side of the window displays the lists that are available for that type.

5. Select the lists to include in the new list group. You can also create an *Exclude* list to compare with the *Include* list. Any terms that are in both lists are excluded, when the list is used in a policy.

   See “Including and excluding items in a list group” on page 52.

6. Click **Save**.

Editing a list group

You can edit a list group to add more lists or to remove a list that you no longer want to include.

Note: We recommend that you take care when modifying a list group that is currently used in a policy. Look in the **Active** column on the **Lists** page to see if a list group is used in a policy.

To edit a list group

1. Select **Services** > **Data Protection** > **Lists**.
2. Select the list group that you want to edit.
3. Amend the following details, as required:
   - Name
   - Description
   - Category
   - The lists that are part of the list group, or are excluded from a list group.

   You cannot change the content type of a list group.
4. Click **Save**.

Deleting a list group

You cannot delete a list group that is used in a Data Protection policy. Look in the **Active** column on the **Lists** page to see if a list group is used in a policy.

To delete a list group

1. Select **Services** > **Data Protection** > **Lists**.
2. Select the check box next to the list group that you want to delete. You cannot filter the **Lists** page to show only the available list groups. For a list group, the **List type** column displays *Group*.
3. Click the **Delete** link below the **Custom Lists** heading.
4. Click **Delete** to confirm.

About content types and lists

A list is a list of items of a particular content type that you use in your policies. You cannot mix content types in a list, and you cannot group together lists of different content types.

The following content types are available:

Table 4-3 Content types and Lists

Content type	Description
Regular expressions	Use regular expressions to search content for a pattern that may indicate that your users are distributing a particular type of information. For example, you might create a regular expression to detect credit card numbers. If three or more suspected credit card numbers are found, you can take action, based on your policy for handling Data Protection incidents. All managed regular expression lists contain one regular expression. While it is possible to include multiple expressions in a list, we recommend that you keep to one regular expression per list. The use of regular expressions can be complicated, and it is better to name and describe the purpose of a single regular expression. To use multiple regular expressions in your policies, do one of the following: ■ Create a list group with more than one regular expression lists in the group ■ Select more than one regular expression lists, when you add the **Content Regular Expression List** condition to a policy.

About global and domain level lists

In Email Data Protection you can create custom lists for all domains - a global list - or for a specific domain. If your role is to administer a specific domain, you can create lists for that domain. You can copy a list from the global list of domains to the domain that you are responsible for. When you are responsible for a single domain, you cannot create a list for use with all domains.

The **Apply to:** drop-down list at the top of the page enables you to do the following:

- Filter the **Lists** page to show the custom lists that apply to all domains or only those that apply to a specific domain
- Select the domain that you want a new list to apply to. Choose the required domain, and click **New List** or **New List Group**.

Note: The managed lists that we provide are available for all domains and are unaffected by any selection you make from the **Apply to:** drop-down list.

Migrating lists from Email Content Control to Email Data Protection

The Email Data Protection service is an enhanced version of Email Content Control. It offers greater flexibility in the way that conditions can be combined. It also offers standard policy templates that address specific regulatory requirements.

If you are an existing Email Content Control customer, we will contact you to arrange for you to migrate to Email Data Protection. Your existing rules will be copied over to Email Data Protection. The conversion of Email Content Control rules to Email Data Protection means the following with regard to lists and list management.

- In Email Content Control, there are keyword lists and templates. The templates are regular expressions. The Content Control regular expression templates are converted to lists in Email Data Protection. In Email Data Protection, the Content Control regular expression templates are converted to regular expressions. All the regular expressions that you can use in Email Content Control are also available in Email Data Protection.
- In the Email Content Control service, you can choose a template that includes multiple regular expressions and then select one or more regular expressions to include in the rule.
- In Email Data Protection each list contains one regular expression. To create a combination of regular expression lists, create a list group that contains the regular expression lists that you require. You can then use the list group in your policies.
- If you have Email Content Control rules that are based on multiple regular expressions and you move to Email Data Protection, each regular expression appears as a separate managed list in the **Lists** page.

The following table is a summary of the terminology that relates to lists in Email Content Control, with the equivalent terms in Email Data Protection.

Table 4-4 Comparison of list terminology in Email Content Control and Email Data Protection

Email Content Control	Email Data Protection	Comments
Ordinary List	Custom List	In Email Content Control, you create ordinary lists of various types, such as domains, MIME types and so.on. You can use ordinary lists in your Content Control rules, or you can create a custom list based on an ordinary list. In Email Data Protection, you create custom lists of various types, such as domains, MIME types and so on. You use custom lists in your policies.
Superlist	List Group	In Email Content Control, you create a superlist to combine multiple lists of the same type. In Email Data Protection, you can combine multiple custom lists of the same type into a list group.
Email Template	Managed List	In Email Content Control, an email template contains one or more regular expressions that are used to detect specific patterns in an email's content. In Email Data Protection each regular expression in an email template is converted to a managed list, with a content type of regular expression. You can use managed lists in your policies, or you can copy a managed list and modify it to meet your requirements. The managed list then becomes a custom list.
List Type	Content Type	In Email Content Control the list type of a list can be MIME, file name, domain name, email content, or URL. In Email Data Protection this is known as the Content Type. In Email Data Protection, the type of a list is the content type - MIME type, domain, keyword, and so on.
Email Content	Keyword List	In Email Content Control, when you create a list of words or phrases, you create a list with a list type of Email Content. In Email Data Protection, to create a list of words and phrases to use in a policy, you create a list with a content type of Keywords.

Chapter 5

Creating and managing policies

This chapter includes the following topics:

- Adding a Content URL List condition to a policy
- Adding an Email Importance condition to a policy
- Adding an Email is Encrypted condition to a policy
- Adding an Email MIME Type condition to a policy
- Adding an Email Size condition to a policy
- Adding a Match All condition to a policy
- Adding a Recipient Domain List condition to a policy
- Adding a Recipient Group condition to a policy
- Adding a Sender Domain List condition to a policy
- Adding a Sender Group condition to a policy
- Adding a Time Interval condition to a policy

About policies and Email Data Protection

The Email Data Protection service enables you to control your inbound and your outbound email. You define policies to filter email according to who sent it, who it was sent to, what it contained, and so on. A policy comprises the following components:

Rules	A policy must contain at least one rule. A rule contains one or more conditions and you can specify that all conditions in the rule must be met or any.
Conditions	Conditions are the tests that you want to apply to your content. For example, you may want to check whether more than three unique credit card numbers are in an email. Other conditions check for file attachments that are above a certain size, or for specified MIME types.
Actions	This is the action that you want the system to take when a policy is triggered. For example, you can determine that an email is prevented from being delivered to the recipient if it contains certain content.
Notifications	A notification is the email that is sent to one or more people when a policy has been triggered. You can customize this message so that it reflects the email security policy that is in place at your organization. When an email is blocked, you can choose to send an email to the sender to explain that the email will not be delivered to the recipient.

You can create a policy that matches one or more rules, multiple conditions within a single rule, and exceptions to a rule. Exceptions to a rule allow specific data or individuals to be excluded from detection.

You build a list of policies that match your business requirements. When you activate the policies in your list, the system checks your emails against each policy in turn.

If a policy is triggered, an incident is generated that appears in the Email Data Protection detailed report. You can view the details of the incident and take appropriate action. The action that you take is likely to depend on the agreements that you have reached with your Human Resources and Legal departments.

We include a number of predefined policy templates to help you create effective policies quickly. When you create policies we recommend that you start with a policy template and add or remove rules to suit your requirements.

About policy templates

A policy template is a collection of predefined rules that addresses a specific requirement. For example, you might use a policy template to ensure that you comply with a set of regulations, such as the European Union Data Protection Directives.

We provide a number of templates that help you create and deploy policies quickly and easily. A policy template usually contains a combination of the following:

- Keyword lists
  These lists contain words and phrases to detect content, such as unacceptable language or personal banking information.
- Regular expression lists
  Regular expressions are used for pattern matching. The regular expressions often search for personally identifiable information, such as passport numbers, social security numbers, and so on.

You cannot create your own templates, so that they appear when you click **New policy from template**. You must use the templates that we provide with the service. You can, however, copy a template and update it to suit your requirements.

When you create a policy from a template, you can view the rules, the conditions, the keywords lists, and the regular expressions that make up the policy.

Note: Although our regulation-based policy templates aim to address a set of regulations, we recommend that you consult with your Legal and Compliance departments to ensure that you are compliant in the countries in which you operate.

The default action for the templates is to log each incident. This means that you can view a report that details the emails that have triggered a policy, but the emails are still delivered. Check that these settings meet your requirements.

About actions and Email Data Protection

When you create a policy, you decide the action to take if the rules in the policy are met and the policy is triggered. For example, you might want to allow an email to be sent to the recipient but direct a copy of it to your administrator.

An email may trigger more than one policy. The policies may have different actions. So, the order in which the policies appear in your policy list is important.

If an email triggers a policy that applies an *exit* action, such as **Block and delete**, the email does not continue through any further policies.

The **Action** drop-down list enables you to specify the required action for the policy.

The **Exit** check box, next to the **Action** drop-down list, determines whether the email is checked against further policies in the list, if a policy is triggered.

The available actions and the effect of the **Exit** check box are as follows:

Table 5-1 Actions and Email Data Protection

Action	Exit check box	Description
Block and Delete	Checked	The email is prevented from reaching the intended recipients. It is permanently deleted. The **Exit** check box is automatically selected and cannot be unchecked. If a policy with this action is triggered for an email, the scanning process stops. The email is not checked against any further policies on your policy list.

Table 5-1 Actions and Email Data Protection *(continued)*

Action	Exit check box	Description
Route to	Checked or unchecked	For an inbound policy, this action enables you to specify which of your existing registered email routes each user's emails are delivered to. To define an inbound routing rule, select the **Route To** action. Select the required named route from the **Named route** drop-down list. Your existing registered inbound email routes are defined in **Services** > **Email Services** > **Inbound Routes**. For an outbound policy, this action enables you to specify an IP or host name that your emails are routed to after they have been scanned. For example, you can route them to a third party for branding. To define an outbound routing rule select the **Route to** action, and enter the primary and the secondary IP address or host name, as required. IPv6 IP addresses are not currently supported. The **Exit** check box is unchecked by default. If you leave the box unchecked, the email is checked against the next policy on your policy list.
Tag Subject	Checked or unchecked	A tag is added to the subject line. You define the text for the tag. Tagging the subject line warns the recipient before they open the email that it may contain unacceptable content. The **Tag Subject** action is available for inbound emails only. The **Exit** check box is unchecked by default. If you leave the box unchecked, subsequent polices on your policy list are evaluated.
Tag with Header	Checked or unchecked	A comment is added into the email X-Header to indicate that the email has triggered a policy. **The Tag with Header** action is available for inbound emails only. The **Exit** check box is unchecked by default. If you leave the box unchecked, the email is checked against the next policy on your policy list.
Compress Attachments	Checked or unchecked	All email attachments of an email are individually converted to .zip files. By individually compressing each attachment, the attachment count and file naming is preserved, while the overall email size is reduced. If the email does not have any attachments, the action has no effect. The **Exit** check box is unchecked by default. If you leave the box unchecked, the email is checked against the next policy on your policy list.

Table 5-1 Actions and Email Data Protection *(continued)*

Action	Exit check box	Description
Allow	Checked	The **Exit** check box is automatically selected and cannot be unchecked. If a policy with this action is triggered for an email, the scanning process stops. The email is not checked against any further policies on your policy list. This action is not logged in any report. You might want to use this action in combination with a condition based on a sender group, to avoid checking an email that a member of the sender group has sent.
Copy to Administrator	Checked or unchecked	The email is copied to the nominated administrator once scanning is completed. The email is sent to the intended recipients. The **Exit** check box is unchecked by default. If you leave the box unchecked, the email is checked against the next policy on your policy list.
Log Only	Checked or unchecked	The Email Data Protection detailed report logs an entry when the policy is triggered. The **Exit** check box is unchecked by default. If you leave the box unchecked, the email is checked against the next policy on your policy list.
Redirect to Administrator	Checked	The email is redirected to a nominated administrator of the service. The email is not sent to the intended recipients. The **Exit** check box is automatically selected and cannot be unchecked. If a policy with this action is triggered for an email, the scanning process stops. The email is not checked against any further policies on your policy list.

About conditions and Email Data Protection

A policy is made up of one or more rules. A rule is made up of one or more conditions. When you use conditions in a policy you compare the content of an email with a list of keywords, a regular expression, an email size limit, and so on. The conditions that you can add to a rule are as follows:

Table 5-2 Email Data Protection conditions

Condition	Description
Attachment Filename List	Specify a condition that compares the name of a file that is attached to an email with the filenames in one or more lists. See "Adding an Attachment Filename List condition to a policy" on page 71.
Attachment MIME Type List	Specify a condition that compares the MIME type of a file that is attached to an email with the MIME types in one or more lists. See "Adding an Attachment MIME Type List condition to a policy" on page 73.
Attachment Number	Specify a limit on the number of files that are attached to an email. See "Adding an Attachment Number condition to a policy" on page 74.
Attachment Size	Specify a limit on the total size of the files that are attached to an email. See "Adding an Attachment Size condition to a policy" on page 74.
Attachment is Password Protected	Specify a condition for file attachments that are password protected. For example, you might want to block all emails that contain file attachments with password protection. See "Adding an Attachment is Password Protected condition to a policy" on page 72.
Attachment is Spoofed	Specify a condition for file attachments that are spoofed, that is, where the file extension has been changed. See "Adding an Attachment is Spoofed condition to a policy" on page 72.
Content Keyword List	Specify a condition that compares the content of an email with the keywords in one or more lists. You can choose the parts of an email that you want to compare with the keyword list, for example, the body, the subject line, file attachments and so on. See "Adding a Content Keyword List condition to a policy" on page 75.

Table 5-2 Email Data Protection conditions *(continued)*

Condition	Description
Content Regular Expression List	Specify a condition that uses the regular expressions in one or more lists to detect patterns in the content of an email. For example, you can create regular expressions to detect credit card numbers, passport numbers, and so on. You can choose the parts of an email that you want to compare with the regular expression list, for example, the body, the subject line, file attachments and so on. See "Adding a Content Regular Expression List condition to a policy" on page 77.
Content URL List	Specify a condition that compares the content of an email with the URLs in one or more lists. You can choose the parts of an email that you want to compare with the URL list, for example, the body, the subject line, file attachments and so on. See "Adding a Content URL List condition to a policy" on page 80.
Email Importance	Specify a condition that compares the importance of an email with an importance level of low, normal, or high. See "Adding an Email Importance condition to a policy" on page 82.
Email MIME Type	Specify a condition that compares the MIME type of an email with the MIME types in one more lists. See "Adding an Email MIME Type condition to a policy" on page 83.
Email Size	Specify a condition that compares the size of an email, including its attachments, with a specified size in megabytes (MB). See "Adding an Email Size condition to a policy" on page 83.
Email is Encrypted	Specify a condition that checks for encrypted emails. Note that an encrypted email is not decrypted. The content matching conditions do not therefore apply to encrypted emails. See "Adding an Email is Encrypted condition to a policy" on page 82.
Match All	Specify a condition that matches on all content. For example, you can use the condition to log all inbound or outbound emails. See "Adding a Match All condition to a policy" on page 84.

Table 5-2 Email Data Protection conditions *(continued)*

Condition	Description
Recipient Domain	Specify a condition that compares the domain of the recipient of an email with the domains in one or more lists. See "Adding a Recipient Domain List condition to a policy" on page 85.
Recipient Group	Specify a condition that compares the recipient of an email with the users in one or more user groups. You can choose LDAP or Email custom groups. See "Adding a Recipient Group condition to a policy" on page 85.
Sender Domain	Specify a condition that compares the domain of the sender of an email with the domains in one or more lists. See "Adding a Sender Domain List condition to a policy" on page 86.
Sender Group	Specify a condition that compares the sender of an email with the users in one or more user groups. You can choose from LDAP and Email custom groups. See "Adding a Sender Group condition to a policy" on page 87.
Time Interval	Specify a condition to compare the time an email was sent with a specified time period. See "Adding a Time Interval condition to a policy" on page 88.

Creating an Email Data Protection policy - process overview

A policy comprises rules, actions, and notifications. A rule includes the conditions that must be satisfied before the policy is triggered and an Email Data Protection incident occurs. An action is the action to take when an incident occurs. A notification is an email that can be sent to the administrator, the sender, and the recipient, when an incident occurs.

You can create a policy based on a predefined template. When you base your policy on a template, you can add, remove, and amend rules, as required. A template includes suggested notifications and actions, but you should review these settings to ensure that they meet your requirements.

The service enables you to create highly flexible policies. You can combine multiple conditions in a rule and multiple rules in a policy. You can have multiple polices.

Note that the system does not check that the policies you create are logical. You can enter combinations of conditions and rules that contradict each other and are ineffective. We recommend that you analyze your requirements carefully before creating your policies. You should also test your policies to ensure that they deliver the results you expect.

You can create policies at global and domain level. The policies that are defined at global level can be applied to an individual domain by copying the policy to the domain. Similarly, a policy that is defined for a domain can be copied to global level.

The following table provides an overview of the procedure for creating a policy:

Table 5-3 Steps for creating an Email Data Protection policy

Step	Action	Details
Step 1	Select **Services** > **Data Protection** > **Email Policies**.	Much of the logic that you include in a policy consists of lists of keywords, regular expressions, URLs and so on. You compare the content of an email with the items in a list. Ensure that you have all the lists that you require before you start to create your policies. See "About custom and managed lists" on page 36.
Step 2	Click **New policy** or **New policy from template**.	When you create a new policy from scratch, you add the conditions, notifications, and actions that you require. When you create a new policy from a template, you base the policy on a predefined set of conditions. You can then amend the conditions and add notifications and actions, to suit your requirements. See "About policy templates" on page 60.
Step 3	Provide a **Name** and **Description** for the policy.	We recommend that you provide meaningful names for the policies that you create. The policy names appear in reports and in the key statistics that you can choose to display on the Dashboard for the Email Data Protection service. Also, when a policy is triggered the name can be included in the notification email that is sent to an administrator. Avoid unacceptable language in a policy name.
Step 4	Choose to apply the policy to inbound email, outbound email, or to both inbound and outbound email.	Note that some actions only apply to inbound email, for example the Tag Subject action.

Table 5-3 Steps for creating an Email Data Protection policy *(continued)*

Step	Action	Details
Step 5	Select an option from the **Action** drop-down list and review or change the setting of the **Exit** check box.	Choose the action to take when the content of an email triggers a policy. For example, with the Block and Delete action, a suspicious email is prevented from being delivered to the recipient and is removed. See "About actions and Email Data Protection" on page 61.
Step 6	Decide on your use of notifications for the policy.	A notification is the email that is sent to an administrator, sender, or recipient when the content of an email triggers a policy. You can decide the default notification settings to apply to your policies, at global and domain level. You can also choose specific notifications at policy level. See "Defining the email notification settings" on page 16.
Step 7	Click **Add Rule** and type a name for the rule.	The rule name defaults to Rule 1, Rule 2 and so on. We recommend that you replace these defaults with meaningful names, as a reminder of the function of the rule.
Step 8	Select a condition from the **Add a condition** drop-down list.	Complete any additional information for the condition. For example, for a **Content Keyword List** condition, you can specify the minimum number of keywords that must appear in the content to satisfy the condition. See "About conditions and Email Data Protection" on page 63.
Step 9	Choose the required setting for the **Execute if** drop-down list, if your rule requires further conditions.	This setting applies to the conditions in the rule. Choose from the following options: ■ **All conditions are met** The rule is triggered if all conditions in the rule are satisfied. ■ **Any conditions are met** The rule is triggered if one or more of the conditions in the rule are satisfied.
Step 10	Click **Add Rule**	A rule must contain at least one condition.
Step 11	Add more rules to the policy as required.	A policy can contain multiple rules. **Note:** The system does not check that the policies you create are logical. You can enter combinations of conditions and rules that contradict each other and are ineffective. Ensure that you test your policies before you implement the service for your users.

Table 5-3 Steps for creating an Email Data Protection policy *(continued)*

Step	Action	Details
Step 12	Select an option from the **Execute if** drop-down list.	This setting applies to the rules in the policy. Choose from the following options: ■ **All rules are met** The policy is triggered if all the rules in the policy are satisfied. ■ **Any rules are met** The policy is triggered if one or more of the rules in the policy are satisfied.
Step 13	Click **Save** to save the policy.	When you save a new policy, it is inactive. Until you activate the policy it is not used to check email content.
Step 14	Review the rules and conditions in the policy	Click on the policy to open it and review the rules that you have created. The **Policy Summary** section displays the rules and conditions that you have added to the policy.
Step 15	Check that the policy appears in the right place in your policy list.	An email is checked against the active policies in your policy list, in the order in which they appear in the **Email Policies** tab. See "Managing the policy list" on page 70.
Step 16	Activate the policy	To activate a policy, click on the link in the **Active** column in the **Email Policies** tab.

Editing a policy

You can edit a policy to update the rules, conditions, actions, and notifications.

To edit a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click the name of the policy that you want to edit.

   The details of the policy are displayed.
3. Make the changes you require to the policy.
   - You can add new rules to policy

     To remove a rule from a policy click the cross symbol in the title bar of the rule.
   - You can update the conditions in a rule

To remove a condition from a rule, click the cross symbol in the title bar of the condition.

- You can change the logic that determines when a policy is triggered. For example, you can change the **Execute if** selector so that the policy is triggered when all rules are satisfied or if any of the rules are satisfied.
- You can change the action to take if the policy is triggered.
- You can check the box for "Stop evaluation of lower priority policies". Checking this box ensures that if an email is blocked due to this policy, no other policies with lower priority are processed. In other words, no other policies that are ordered lower in your policy list are processed. Note that you can change the priority of your policies by reordering them on the policy list at **Dashboard** > **Services** > **Data Protection**. You can use either the arrow icons to change policy priority positions, or use the policy row's check box and select **Move** in the table header.
- You can also change the notification details to display a different message to the user if the policy is triggered.

4 Review the **Policy Summary** to check that the rules and conditions in the policy meet your requirements.

5 Click **Save** to save your changes.

Deleting a policy

You can delete a policy that you no longer require. You can also deactivate a policy so that it is no longer used to check your email traffic. If you think that you might want to reuse the logic that is included in a policy, we recommend that you deactivate the policy, instead of deleting it.

To delete a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Select the check box next to the name of the policy that you want to delete.

3 Click the **Delete** link.

4 Click **Delete** to confirm that you want to delete the policy.

Managing the policy list

The **Email Policies** tab displays the policies that you have created. The order in which the policies appear in the list is important. Each policy is checked in turn, in the order they appear in the list, until one of the following occurs:

- All policies in the list have been checked
- A policy with an exit action has been triggered.

When an exit action is triggered, no further policies are checked against the email. Ensure that you position a policy with an exit action at the top of the policy lists, to avoid unnecessary processing.

For example, supposing you apply an action of Block and Log to a policy, and the policy appears at the top of the policy list. If the policy is triggered, the email is not checked against any of the other policies that appear in your list. This is because the Block and Log action is an exit action.

You can change the position of a policy in the list, and change the status of a policy to be active or inactive. When active, the policy is used in the scanning of email traffic. When inactive, the policy is not used in the scanning of email traffic. The **Active** column in the **Email Policies** tab displays the active status of the policy.

To change the position of a policy in your policy list

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Click the up or down arrow next to the policy. When you click the down arrow next to a policy, you move the policy below the next policy in the list.

To change the status of a policy in your policy list

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Locate the policy that you want to change and click the **ON/OFF** switch in the **Active** column to make the policy active or inactive.

Adding an Attachment Filename List condition to a policy

The **Attachment Filename List** condition enables you to compare the name of a file that is attached to an email against a list of file names in one or more lists. For example, you might want to check for attachments with a .exe extension. Compressed archive and Microsoft Office attachments are also scanned. The scanner opens a compressed archive file and scans the file types within it.

To add an Attachment Filename List condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule**.

4 Select the **Attachment Filename List** condition from the **Add a condition** drop-down list.

5 Click **Browse for a Filename List**, select one or more lists and click **Add**.

6 Choose one of the following from the drop-down list.

Any	The condition is satisfied if the name of the file matches any of the file names in the selected lists.
None	The condition is satisfied if the name of the file does not match any of the file names in the selected lists.

7 Add more conditions to the rule or click **Save**.

Adding an Attachment is Password Protected condition to a policy

The **Attachment is Password Protected** condition enables you to check for password-protected files that are attached to an email. This setting can help you identify if users send unauthorized confidential material out of the company.

The attachments that are checked are Microsoft Office 2003, 2007, and 2010 format files, and PDF files. Password-protected file attachments are not scanned for content-based conditions. For this reason, we suggest that you establish a policy whereby password-protected file attachments are redirected to your system administrator. In this way, you can monitor who sends or receives these attachments. You can then take action based upon your agreed email security policy.

To add an Attachment is Password Protected condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Attachment is Password Protected** condition from the **Add a condition** drop-down list.

4 Add more conditions to the rule or click **Save**.

Adding an Attachment is Spoofed condition to a policy

The **Attachment is Spoofed** condition checks whether the file extension of an email attachment matches the implied contents.

The Email AntiVirus service detects malicious files that may be spoofed. The Email Data Protection service takes the detection of malicious files a step further and

investigates all recognized file types. It determines whether they are spoofed or not. A policy rule that includes this condition ensures that users cannot get around an organization's email security policy by spoofing files.

To add an Attachment is Spoofed condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Attachment is Spoofed** condition from the **Add a condition** drop-down list.
4. Add more conditions to the rule or click **Save**.

Adding an Attachment MIME Type List condition to a policy

The **Attachment MIME Type List** condition enables you to monitor for an attachment that is of the same MIME type as the type in one or more lists. Compressed archive and Microsoft Office attachments are also scanned. The scanner opens a compressed archive file and scans the file types within it.

To add an Attachment MIME Type List condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Attachment MIME Type List** condition from the **Add a condition** drop-down list.
4. Click **Browse for a Filename List**, select one or more lists and click **Add**.
5. Choose from the following settings:

Any	The condition is satisfied if the MIME type of the file matches any of the MIME types in the selected lists.
None	The condition is satisfied if the MIME type of the file does not match any of the MIME types in the selected lists.

6. Add more conditions to the rule or click **Save**.

Adding an Attachment Size condition to a policy

The Attachment Size condition enables you to compare the size of an email attachment with a specified size in megabytes. You might want to set an attachment size condition to check for large files that could contain company data.

We suggest that you set an attachment size condition to block attachments coming into your organization that are larger than 25Mb. Ensure that your notification settings inform both the sender and the recipients that this action has been taken.

To add an Attachment Size condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Attachment Size** condition from the **Add a condition** drop-down list.
4. Choose from the following settings:

Equal	The condition is satisfied if the size of the file is equal to the value you enter in megabytes.
Greater Than	The condition is satisfied if the size of the file is greater than the value you enter in megabytes.
Greater Than or Equal	The condition is satisfied if the size of the file is greater than or equal to the value you enter in megabytes.
Less Than	The condition is satisfied if the size of the file is less than the value you enter in megabytes.
Less Than or Equal	The condition is satisfied if the size of the file is less than or equal to the value you enter in megabytes.

5. Specify a value for the size of the attachment in megabytes.
6. Add more conditions to the rule or click **Save**.

Adding an Attachment Number condition to a policy

The **Attachment Number** condition enables you to check for the number of files that are attached to an email.

To add an Attachment Number condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Attachment Number** condition from the **Add a condition** drop-down list.

4 Choose from the following settings:

Equal	The condition is satisfied if the number of files that are attached to the email matches the number that you enter for this condition.
Greater Than	The condition is satisfied if the number of files that are attached to the email is greater than the number that you enter for this condition.
Greater Than or Equal	The condition is satisfied if the number of files that are attached to the email is greater than or equal to the number that you enter for this condition.
Less Than	The condition is satisfied if the number of files that are attached to the email is less than the number that you enter for this condition.
Less Than or Equal	The condition is satisfied if the number of files that are attached to the email matches the number that you enter for this condition.

5 Add more conditions to the rule or click **Save**.

Adding a Content Keyword List condition to a policy

The Content Keyword List condition enables you to compare an email and its attachments with one or more lists of keywords.

To add a Content Keyword List condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Content Keyword List** condition from the **Add a condition** drop-down list.

4 Click **Browse for a Keyword List**, select one or more lists and click **Add**.

5 Choose from the following settings:

Email contains all of the keywords in the selected lists	The condition is satisfied when a match is found in the email for every keyword in the selected lists.

Email contains none of the keywords in the selected lists	The condition is satisfied when no match is found in the email for any of the keywords in the selected lists.
Email contains a number of matches for the keywords in the selected lists	Enter the minimum number of matches (the threshold) that is required for the condition to be satisfied. The **Count only unique matches** option appears when you select this option. You can choose either **Yes** or **No** for unique matching. When **Count only unique matches** is set to **No**, multiple matches of the same keyword count towards the threshold. When **Count only unique matches** is set to **Yes**, only one match of a keyword counts towards the threshold. Example A: Your content keyword list contains 20 keywords. You want a minimum of three keywords to be found in the email for the condition to be satisfied. Do the following: ■ Set the threshold to 3 ■ Set **Count only unique matches** to **Yes**. Example B: Your content keyword list contains one keyword. You want the condition to be satisfied if the keyword is found five or more times in the email. Do the following: ■ Set the threshold to 5 ■ Set **Count only unique matches** to **No**.
Case sensitive	Choose whether to take account of case when matching on the keywords in the selected lists. By default, case sensitivity is turned off.

Look in

Select one or more of the following:

- **Body**
  Scans the content in the body of an email.
- **Subject line**
  Scans the content in the subject line of an email.
- **Header**
  Scans the content in the header of an email.
- **File attachments**
  Scans the content within attached Microsoft Office 2003, 2007 and 2010, PDF, HTML, and text (.txt) files. This option provides protection against specific types of files, which are hidden within other files.
- **Attachment file properties**
  Scans the information that is stored in the document properties of attached Microsoft Office 2003, 2007 and 2010, and PDF files. Document properties include standard properties, such as author, title, subject, and custom properties that the originator of the document has included.

6 Add more conditions to the rule or click **Save**.

Adding a Content Regular Expression List condition to a policy

The **Content Regular Expression List** condition enables you to search for patterns in email content using regular expressions. For example, you can create a regular expression to check for credit card numbers or social security data.

To add a Content Regular Expression List condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Content Regular Expression List** condition from the **Add a condition** drop-down list.

4 Click **Browse for a Regular Expression List**, select one or more lists and click **Add**.

5 Choose from the following settings:

Email contains a match for all of the regexes in the selected lists	The condition is satisfied when a match is found in the email for every regular expression in the selected lists.
Email contains a match for none of the regexes in the selected lists	The condition is satisfied when no match is found in the content for any of the regular expressions in the selected lists.
Email contains a number of matches for the regexes in the selected lists.	Enter the minimum number of matches (the threshold) that is required for the condition to be satisfied. For example, if you enter 5, the condition is satisfied if the content contains 5 or more matches of any of the regular expressions in the selected lists The **Count only unique matches** setting appears when you select this option. You can choose either **Yes** or **No** for unique matching. The default setting is **No**. When set to **No**, the matches that are found do not have to be unique to count towards the threshold. When set to **Yes**, only unique matches count towards the threshold. For example, supposing you create a **Content Regular Expression List** condition to find credit card numbers. If you set **Count only unique matches** to **No**, and specify a threshold of 3, the condition is satisfied if 3 or more credit card numbers are found, even if the same credit card number is found three times If **Count only unique matches** is set to **Yes**, three different credit card numbers must be found in the content for the condition to be satisfied. In this example, you probably want to use unique matching. The presence of multiple, different credit card numbers in content is likely to indicate a data leak.
Case sensitive	Choose whether to take account of case when evaluating the regular expression. By default, case sensitivity is turned off.

Look in

Select one or more of the following:

- **Body**
  Scans the content in the body of an email.
- **Subject line**
  Scans the content that appears in the subject line of an email.
- **Header**
  Scans the content in the header of an email.
- **File attachments**
  Scans the content in attached Microsoft Office 2003, 2007 and 2010, PDF, HTML, and text (.txt) files. This option provides protection against specific types of files, which are hidden within other files.
- **Attachment file properties**
  Scans the information that is stored in the document properties of attached Microsoft Office 2003, 2007 and 2010, and PDF files. Document properties include standard properties, such as author, title, subject, and custom properties that the originator of the document has included.

Matched text

Matched text is the content that a regular expression finds in an email or in an email attachment. The content may cause a policy to trigger and an incident to be logged. The **Matched text** setting controls how the content is stored. when an incident is logged. Select from the following options:

- **Redact matched text**
  This is the default setting. The incident is logged with the matched text redacted. That is, a series of asterisks hides the matched text that the regular expression has found. Choose this setting to ensure that the matched text can never be shown in a report. You may want to hide the matched text to comply with the regulations that cover data privacy in your country.
- **Log matched text**
  The matched text that the regular expression finds is not redacted. Choose this setting if you want to be able to see the text that caused a policy to trigger. Note that regular expressions are often used to search for credit card details or social security information. For data privacy reasons, you may not want anyone to be able to view this information.

Note: The **Matched text** setting controls how the matched text is stored. To view the text on a report, select **Show matched content on reports** in the **Email Data Protection Settings** page.

See "Defining the reporting settings" on page 23.

6 Add more conditions to the rule or click **Save**.

Adding a Content URL List condition to a policy

The **Content URL List** condition enables you to detect content in the form of a URL within the various parts of an email. You can use the **Content URL List** condition to restrict the communication of specified URLs around your organization.

To add a Content URL List condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Content URL List** condition from the **Add a condition** drop-down list.

4 Click **Browse for a URL List**, select one or more lists and click **Add**.

5 Choose from the following settings:

Email contains all of the URLs in the selected lists	The condition is satisfied when a match is found in the email for every URL in the selected lists.
Email contains none of the URLs in the selected lists	The condition is satisfied when no match is found in the email for any of the URLs in the selected lists.
Email contains a match for a number of the URLs in the selected lists	Enter the minimum number of URLs (the threshold) that is required for the condition to be satisfied. The **Count only unique matches** setting appears when you select this option. You can choose either **Yes** or **No** for unique matching. When set to **No**, the URLs that are found do not have to be unique to count towards the threshold. When set to **Yes**, the URLs must be unique to count towards the threshold. For example, if you want every URL in your list to be present in the email for the condition to be satisfied, ensure that the threshold matches the number of URLs in your list, and set **Count only unique matches** to **Yes**.
Case sensitive	Choose whether to take account of case when matching on the URLs in the selected lists. By default, case sensitivity is turned off.

Look in

Select one or more of the following:

- **Body**
  Scans the content in the body of an email.
- **Subject line**
  Scans the any content that appears in the subject line of an email.
- **Header**
  Scans the content in the header of an email.
- **File attachments**
  Scans the content within attached Microsoft Office 2003, 2007 and 2010, PDF, HTML, and text (.txt) files. This option provides protection against specific types of files, which are hidden within other files.
- **Attachment file properties**
  Scans the information that is stored in the document properties of attached Microsoft Office 2003, 2007 and 2010, and PDF files. Document properties include standard properties, such as author, title, subject, and custom properties that the originator of the document has included.

6 Add more conditions to the rule or click **Save**.

Adding an Email Importance condition to a policy

The **Email Importance** condition enables you to detect emails with a specific priority level. The available options are low, normal, and high. The options correspond to the importance levels for an email that are available in Microsoft Outlook.

To add an Email Importance condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Email Importance** condition from the **Add a condition** drop-down list.

4 Choose **Low**, **Normal**, or **High** for the **Importance Level**.

5 Add more conditions to the rule or click **Save**.

Adding an Email is Encrypted condition to a policy

The **Email is Encrypted** condition detects whether an email is encrypted. Only S/MIME encryption is detected.

Encrypted emails are not scanned for content-based conditions, such as the **Content Keyword List** condition. We suggest that you establish a policy whereby encrypted emails are redirected to your system administrator. In this way, you can monitor who sends or receives these emails. You can then take action based on your agreed email security policy.

To add an Email is Encrypted condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Email is Encrypted** condition from the **Add a condition** drop-down list.
4. Add more conditions to the rule or click **Save**.

Adding an Email MIME Type condition to a policy

The **Email MIME Type** condition compares the MIME type of the email against one or more lists of MIME types. This condition relates to the MIME type of the email and not the MIME type of any files that are attached to the email.

To add an Email MIME Type condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Email MIME Type** condition from the **Add a condition** drop-down list.
4. Click **Browse for a URL List**, select one or more lists and click **Add**.
5. Choose from the following settings:

Any	The condition is satisfied if the MIME type of the email matches any of the MIME types in the selected lists.
None	The condition is satisfied if the MIME type of the email does not match any of the MIME types in the selected lists.

6. Add more conditions to the rule or click **Save**.

Adding an Email Size condition to a policy

The **Email Size** condition enables you to compare the size of an email, including attachments, with a specified size in MB.

To add an Email Size condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Email Size** condition from the **Add a condition** drop-down list.
4. Choose one of the following from the **Size** drop-down list.

Equal	The condition is satisfied if the size of the email, including attachments, is equal to the value you enter in megabytes.
Greater Than	The condition is satisfied if the size of the email, including attachments, is greater than the value you enter in megabytes.
G**reater Than or Equal**	The condition is satisfied if the size of the email, including attachments, is greater than or equal to the value you enter in megabytes.
Less Than	The condition is satisfied if the size of the email,, including attachments, is less than or equal to the value you enter in megabytes.
Less Than or Equal	The condition is satisfied if the size of the email,, including attachments, is less than the value you enter in megabytes.

5. Specify a value for the size of the email, including attachments, in megabytes.
6. Add more conditions to the rule or click **Save**.

Adding a Match All condition to a policy

The **Match All** condition enables you to create a condition that matches all content. For example, you might want to monitor inbound or outbound email traffic by logging all emails regardless of their content.

To add a Match All condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Match All** condition from the **Add a condition** drop-down list.

4 Click **Save**.

Adding a Recipient Domain List condition to a policy

The **Recipient Domain** condition enables you to create a condition that compares the domain of the recipient of an email with the domains in one or more lists. For a policy apply to all recipients, do not define any recipient domain conditions. In a **Recipient Domain** condition, you use the domain lists that you have created in the **Lists** tab.

To add a Recipient Domain condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Recipient Domain** condition from the **Add a condition** drop-down list.

4 Click **Browse for a Domain List**, select one or more lists and click **Add**.

5 Choose from the following settings:

All	The condition is satisfied if the domain of the recipient is in all of the selected lists.
Any	The condition is satisfied if the domain of the recipient is in any of the selected lists.
None	The condition is satisfied if the domain of the recipient is in none of the selected lists.

6 Add more conditions or click **Save**.

Adding a Recipient Group condition to a policy

The **Recipient Group** condition enables you to compare the recipient of an email with the users in one or more user groups. You can combine the **Recipient Group** condition with other conditions to create a policy that only applies to certain recipients. You can build a **Recipient Group** condition, based on the following types of group:

- LDAP groups

You manage LDAP groups by synchronizing your directory data with the portal, using the Synchronization Tool.

- Custom groups
  You create and manage custom groups in the portal.
  See "About user groups" on page 27.

To add a Recipient Group condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Recipient Group** condition from the **Add a condition** drop-down list.
4. Click **Browse for a Group**, select one or more groups and click **Add**.
5. Choose from the following settings:

All	The condition is satisfied if the recipient is in all of the selected groups.
Any	The condition is satisfied if the recipient is in any of the selected groups.
None	The condition is satisfied if the recipient is in none of the selected groups.

6. Add more conditions to the rule or click **Save**.

Adding a Sender Domain List condition to a policy

The **Sender Domain** condition enables you to compare the domain of the sender of an email with the domains in one or more lists. For a policy apply to all senders, do not define any **Sender Domai**n conditions. In a **Sender Domain** condition, you use the domain lists that you have created in the **Lists** tab.

To add a Sender Domain condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Sender Domain** condition from the **Add a condition** drop-down list.
4. Click **Browse for a Domain List**, select one or more lists and click **Add**.

5 Choose from the following settings:

All	The condition is satisfied if the domain of the sender is in all of the selected lists.
Any	The condition is satisfied if the domain of the sender is in any of the selected lists.
None	The condition is satisfied if the domain of the sender is in none of the selected lists.

6 Add more conditions to the rule or click **Save**.

Adding a Sender Group condition to a policy

The **Sender Group** condition enables you to compare the sender of an email with the users in one or more user groups. You can combine the **Sender Group** condition with other conditions to create a policy that only applies to certain senders. You can build a **Sender Group** condition, based on the following types of group:

- LDAP groups
  You manage LDAP groups by synchronizing your directory data with the portal, using the Synchronization Tool.
- Custom groups
  You create and manage custom groups in the portal.
  See "About user groups" on page 27.

To add a Sender Group condition to a policy

1 Select **Services** > **Data Protection** > **Email Policies**.

2 Open the policy that you want to amend, or choose to create a new policy.

3 Click **Add Rule** and select the **Sender Group** condition from the **Add a condition** drop-down list.

4 Click **Browse for a Group**, select one or more groups and click **Add**.

5 Choose from the following settings:

All	The condition is satisfied if the sender is in all of the selected groups.
Any	The condition is satisfied if the sender is in any of the selected groups.
None	The condition is satisfied if the sender is in none of the selected groups.

6 Add more conditions to the rule or click **Save**.

Adding a Time Interval condition to a policy

You can define a condition based on the time that an email is sent or received. A policy based on a time condition can be useful to limit email size to retain network bandwidth during the working day, for example. Times are based on when the email arrives on a mail server within the cloud infrastructure. It is then converted to the time zone specified.

To add a Time Interval condition to a policy

1. Select **Services** > **Data Protection** > **Email Policies**.
2. Open the policy that you want to amend, or choose to create a new policy.
3. Click **Add Rule** and select the **Time Interval** condition from the **Add a condition** drop-down list.
4. Select whether to apply the condition to emails that are scanned within or outside of the specified time intervals.
5. To specify a time zone other than the default, select the required zone from the drop-down list. The default time zone is specified in the **Email Data Protection Settings** page.
6. Add more conditions to the rule or click **Save**.