



## Image Control and Data Protection

# Image Control and Data Protection Support Guide.

Version 1.0



## Contents

<b>1 Configuring rules within Image Control .....</b>	<b>2</b>
<b>2 What are custom groups? .....</b>	<b>3</b>
Creating custom groups .....	3
<b>3 What are email disclaimers? .....</b>	<b>5</b>
Configuring email disclaimers.....	6
Creating new disclaimers .....	7
Editing existing disclaimers.....	8
Removing disclaimers .....	9
<b>4 What is Track and trace? .....</b>	<b>10</b>
Using track and trace.....	10
<b>5 Configuring rules within Data Protection .....</b>	<b>13</b>
Actions & Notifications.....	14
Block and delete .....	14
Route to .....	14
Tag subject line.....	15
Tag with header .....	15
Compress attachments .....	15
Allow .....	15
Copy to administrator.....	15
Log only .....	15
Redirect to administrator.....	15
<b>6 Lists .....</b>	<b>18</b>

# 1 Configuring rules within Image Control

**Anti-Spam**

Global Settings ▾

Detection Settings
Quarantine Settings
Approved Senders
Blocked Senders

**Approved Senders** ?

Use approved senders list (IP addresses only)

Use approved senders list (domains and email addresses only)

**Spoofed Sender Detection**

Use SPF Emails from domains that publish a hard-fail Sender Policy Framework (SPF) policy will be blocked and deleted if the sending IP address is not registered in the sending domain's SPF record.

Use DMARC Emails from domains that publish a DMARC policy may be rejected, quarantined or tagged if they fail validation, according to the sending domain's DMARC policy.

**Responsive Spam Detection**

Use blocked senders list (IP addresses only)

Action: Block and delete the mail ▾

---

Use blocked senders list (domains and email addresses only)

Action: Append a header but allow mail through ▾

---

Use dynamic IP block List

Action: Append a header but allow mail through ▾

---

Use signaturing system

Action: Block and delete the mail ▾

---

**Predictive Spam Detection**

Use Skeptic heuristics

Use newsletter detection

Action: Block and delete the mail ▾

---

**Bulk Mail Address**

Please specify the address that mail identified as spam will be forwarded to if the **Append a header and redirect to a bulk mail address** action is selected.

Enter an email address:

Maximum length 255 characters

**Subject Line Text**

Enter the text that will appear on the subject line of emails tagged as spam

Enter text:

Put this text in front of the subject line

Put this text at the end of the subject line

You can navigate between tabs without losing settings before submitting.

Save and Exit
Cancel

For inbound routes, it can scan Microsoft documents and PDF's, can use approved and clocked images both global settings or individual ones. The mail will be allowed through but you can confirm what text will go with the mail to person receiving.

The only difference between the inbound and outbound is the text added to the mail is not allowed.

Notifications give the ability of letting an e-mail address know when inappropriate e-mails have been sent or received. Approved and blocked images and senders can be configured to whatever the customer wants.

## 2 What are custom groups?

Custom groups are used within the Symantec.cloud system for applying custom disclaimers, filtering, data protection etc. They are useful as they provide a way of administering the portal on a more granular level.

Custom groups can be created to assign a custom disclaimer to only these users for example whilst the rest of the users on the domain use a standard disclaimer. This is particularly useful for example if a marketing department requires a different disclaimer to a sales department but both reside on the same domain.

### Creating custom groups

When using the various scanning tools within the Symantec.cloud portal there may be a need to create custom user groups in order to assign disclaimers, filters, content rules etc. To do this you will need to navigate to the **Users and Groups** tab and select the **user groups** option.

Current user groups will now be displayed. This main page also displays the number of users assigned to each group, the type of group, the date the group was last modified and also allows for user lists to be uploaded and downloaded. Clicking on the group name will allow you to view the list of users currently assigned.

Mail Platform

Global settings

Address Registration | User Groups | Message Size

Group name:  Group type: All Search Clear Search

[Create new group](#) [Delete selected group\(s\)](#) [Delete users](#)

Showing 1 to 4 of 4 << First < Prev Next > Last >> 10

<input type="checkbox"/>	Group Name	Type	Members	In use?	Disclaimer	Last Modified		
<input type="checkbox"/>	Finance	Custom	2 users	-		25 Nov 2004 11:54 AM	<a href="#">Upload</a>	<a href="#">Download</a>
<input type="checkbox"/>	Marketing	Custom	2 users	-		25 Nov 2004 11:59 AM	<a href="#">Upload</a>	<a href="#">Download</a>
<input type="checkbox"/>	support	Custom	0 users	-		29 Apr 2008 1:12 PM	<a href="#">Upload</a>	<a href="#">Download</a>
<input type="checkbox"/>	testing 1243	Custom	5 users	-		13 Mar 2008 11:32 AM	<a href="#">Upload</a>	<a href="#">Download</a>

To view the addresses assigned to the group click on the group name.

User lists can be uploaded to the customer groups via these links. These will be in a .CSV format.

To create a new group select the **create new group** button, you will now see an empty group ready to be created.

Next you will need to select the users who will be assigned to this group. Initially the user's field will be blank. Clicking **search** however will populate a list of already registered users (these are normally taken from the address registration list). You can now select the users you wish to be assigned to this group.

Groups must be named and initially the available users list will not be populated. Clicking **search** will populate this list which is constructed from the address registration list.

You are here: Dashboard > Services > Email Services > Platform

Mail Platform

Global settings ▾

Create Group

Group Name

Enter group name:

Manage users

- To add users to the group select them from the **Available users** list and click **Add**.
- To display **Available users** enter their email address in the Search box below. If they do not appear in the Available users list, enter their email address in the **New users** box and click **Add**.
- To remove a user from the group enter their email address in the **Search** box, select their name from the **Group members** list and click **Remove**.

Email address:  Search

*Note - Each list can display up to 500 entries. Where a search returns more than 500 entries in either list, refine your search criteria.*

Available users

Use search tool to view users

Display first 0 out of 0 results

Add >>

<< Remove

Group members

Use search tool to view users

New users

Add user email address here

*Note: Email disclaimer configuration will apply to email addresses within your organization only.*

Save and exit
Cancel

To add users that are not listed within address registration, enter the address into the new user's field and select **add**. The address will now be populated in the group members' field.

Some users may not be on the registered list, especially if address registration is not in use. It is possible to add these users manually however.

At the bottom of the group's page you will see the **new users** option. Here you can manually type users addresses (multiple addresses can be added in one entry) and add them to the group members list.

### 3 What are email disclaimers?

An email disclaimer is the text in the footer of an email that passes through the Email Services infrastructure.

Using a combination of default and custom email disclaimers, for inbound and outbound emails, at global, domain, and group level, you can configure your disclaimers to your requirements. Plan your disclaimers so that your users have the appropriate disclaimer applied to their emails.

Email disclaimers are also known as Banners and Footers.

Email disclaimers can be used for several reasons. An email disclaimer informs the recipient that the email has been scanned for security purposes. A typical message reassures the email recipients that their emails are legitimate and free of viruses.

In many countries, there is a legal requirement for business email to include the company name, registered office address, and company registration details. You can use email disclaimers to ensure that this information is appended to all email that leaves your organization. Email disclaimers are more reliable than using email signatures that are set up in each user's email client.

Use email disclaimers to limit employer's liability. For example, you can state that any views or opinions that are presented in an email are solely those of the author and do not necessarily represent those of the company.

Some industries may require organizations to make certain disclosure statements when communicating by email.

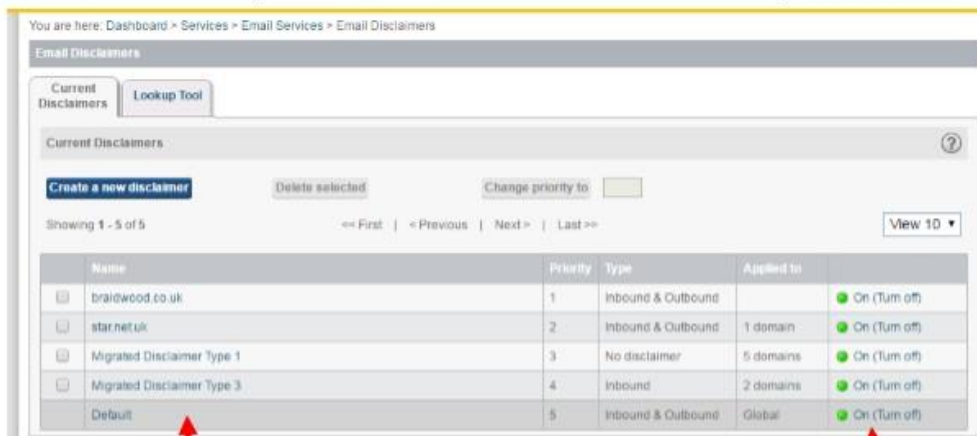
You can create separate groups for each region and apply a specific disclaimer for each group.

Unless you have configured custom disclaimers, the default disclaimer is applied to all of the emails going out and within your organization. The default disclaimer uses the generic text that we have predefined. Or you can define the text to your requirements. You can also choose not to have a disclaimer appended for your inbound email or outbound email, or both.

## Configuring email disclaimers

Once signed in you will need to navigate to the **Email disclaimers** section which can be found under the **Services** tab. The main page will display all currently configured disclaimers and their current status. By default Symantec will apply a disclaimer to all domains detailing that mails have been scanned. This will be applied both inbound and outbound.

The main disclaimer home page provides an overview of how each disclaimer is configured via the priority, type and applied to fields.



Disclaimers are displayed by their name, clicking on the name will show the current configuration of the disclaimer.

The Currents status of the disclaimer is shown here, click on the status will change the state of the disclaimer.

## Creating new disclaimers

To create a new custom disclaimer you will need to click on **Create a new disclaimer**. This will take you to a new page in which you can add the text for the new disclaimer, name the disclaimer for easy management and, using the lookup tool, search for existing disclaimers.



The screenshot shows the 'Email Disclaimers' configuration page. At the top, there is a breadcrumb trail: 'You are here: Dashboard > Services > Email Services > Email Disclaimers'. Below this, there are tabs for 'Current Disclaimers' and 'Lookup Tool'. A text input field for 'Disclaimer name' is shown. Below that, there are sections for 'Inbound disclaimer' and 'Outbound disclaimer', each with radio buttons for 'Custom' and 'No disclaimer'. At the bottom, there are 'Add Group' and 'Remove Selected' buttons, and a table with columns for 'Selected Groups', 'Type', and 'Members'. Three callout boxes with red arrows point to the 'Disclaimer name' field, the 'No disclaimer' options, and the 'Add Group' button.

Each disclaimer must be named, it is recommended that this is relevant to what the disclaimer details or the domain it is applied to.

Each disclaimer can also be customised depending on the direction of mail. It is also possible to disable disclaimers in a particular direction.

To assign a disclaimer to a domain or a list of domains select the “add group” option. You will then be presented with a list of domains or custom groups which the disclaimer will be applied to. It is possible to assign a disclaimer to specific user by creating customer groups within the Symantec portal

Disclaimers can be added for either inbound, outbound or both. If you wish to disable the disclaimer for mails in a particular direction you will need to click on **no disclaimer** on the direction in which you wish to disable.

Email disclaimers can only feature plain text, they do not allow for HTML code to be applied or pictures to be added. They will however allow for the text to be formatted.

When creating disclaimers you may wish to add information that is unique to only certain domains. To do this you will need to create a custom group, using the **group** option, to which you can then add the specified domains. In this way you can manage custom disclaimers for a number of domains without having to create a new disclaimer for each domain.

When a disclaimer has been created please remember that it may take 4-6 hours for the disclaimer to appear on your emails. If you do not see the disclaimer being added after this time please [Contact Us](#)

## Editing existing disclaimers

If you wish to edit existing disclaimers you will need to select the disclaimer via its name from the mail disclaimers page. You will then be presented with the current configuration of the disclaimer. Text can then be added or removed as required and the direction in which the disclaimer is applied can be amended. If a disclaimer is disabled in any direction the text entered will still be saved within the field should there be a need to reactivate it.

Groups can also be added as mentioned in the disclaimer creation section above. Removal of a group is possible by selecting the required group and clicking **remove selected**.

## Removing disclaimers

If you wish to remove a disclaimer from the portal full removal may not actually be required. It is possible to simply disable the disclaimer rather than remove it. This is useful if the disclaimer configuration is particularly complex or has a number of custom groups tied to it, as if the disclaimer is required in future it can be reactivated rather than having to be fully reconfigured.

If however full removal is required simply select the disclaimer from the list of disclaimers on the main page and click "delete selected". The default disclaimer cannot be removed

You are here: Dashboard > Services > Email Services > Email Disclaimers

Email Disclaimers

Current Disclaimers    Lookup Pool

Current Disclaimers ?

Create a new disclaimer    Delete selected    Change priority to

Showing 1 - 5 of 5    << First | < Previous | Next > | Last >>    View 10 ▾

Name	Priority	Type	Applied to	
<input checked="" type="checkbox"/> braidwood.co.uk	1	Inbound & Outbound		● On (Turn off)
<input type="checkbox"/> star.net.uk	2	Inbound & Outbound	1 domain	● On (Turn off)
<input type="checkbox"/> Migrated Disclaimer Type 1	3	No disclaimer	5 domains	● On (Turn off)
<input type="checkbox"/> Migrated Disclaimer Type 3	4	Inbound	2 domains	● On (Turn off)
Default	5	Inbound & Outbound	Global	● On (Turn off)

## Disclaimer priority

Only one disclaimer can be applied per email. As such it is vital to place disclaimers in the correct order within the client net portal. If an address belongs to multiple disclaimers it will be the disclaimer with the highest priority that is applied.

To change the priority of a disclaimer, select the disclaimer from the main disclaimer list, enter the position in which you wish the disclaimer to reside in the "change priority to" field and click the **change priority to** button.

To change the priority of a disclaimer, select the disclaimer from the main disclaimer list, enter the position in which you wish the disclaimer to reside in the "change priority to" field and click the "change priority to" button.

You are here: Dashboard > Services > Email Services > Email Disclaimers

Email Disclaimers

Current Disclaimers Lookup Tool

Current Disclaimers ?

[Create a new disclaimer](#) [Delete selected](#) [Change priority to](#)

Showing 1 - 5 of << First | < Previous | Next > | Last >> View 10 ▾

Name	Priority	Type	Applied to	
<input type="checkbox"/> braidwood.co.uk	1	Inbound & Outbound		<span>●</span> On (Turn off)
<input type="checkbox"/> star.net.uk	2	Inbound & Outbound	1 domain	<span>●</span> On (Turn off)
<input type="checkbox"/> Migrated Disclaimer Type 1	3	No disclaimer	5 domains	<span>●</span> On (Turn off)
<input type="checkbox"/> Migrated Disclaimer Type 3	4	Inbound	2 domains	<span>●</span> On (Turn off)
<input type="checkbox"/> Default	5	Inbound & Outbound	Global	<span>●</span> On (Turn off)

## 4 What is Track and trace?

The Email Track and Trace tool lets you trace a specific email and determine if and when it was processed and the action taken. You can search for an email that was processed within the last 30 days.

Typically, an email is searchable within 15 minutes of entering the Email Services infrastructure. The Email Services infrastructure does not store copies of any emails that pass through it. Rather, it logs key information about each email at the time of processing.

### Using track and trace

To perform a trace on emails first you will navigate to the tool (Tools-> Email Track and Trace). You will now be able to enter your search criteria. The more information that can be entered into these fields the more accurate the trace will be.

However it is possible to search via anyone of the fields on their own. Searching by either the recipient/sender addresses or subject line together will usually return the best results. It is also key to select a date/time range for the search, the smaller the range the quicker the search will complete.

You are here: Dashboard > Tools > Email Track and Trace

### Email Track and Trace

Search and identify emails processed by your Email Security Services

Search Search by ID

Recipient

Sender

Date range Timezone: GMT ( Change )  
Last half hour ( Switch to days )  
Select specific dates and times  
Choose a date/time range or a fixed period, up to 30 days.

Subject line Contains

Attachment filename

Select more search options Show all

View the results on screen  
 Email the results as a CSV file when the search is complete

Reset form Search

Search for an email sent to or from a specific email address. Use the \* symbol as a wildcard, to represent one or more characters. You must enter an @ symbol and a period, e.g. \*@domain.\*

There are further search options available using the show all link at the bottom of the page. These include searching via sending server IP, receiving server IP, email size, the help message sent by the receiving server and any mails that have been triggered by a particular service.

If you have been provided with a bounce message from the sender it is also possible to search via the message ID using the "search by ID" tab.

You are here: Dashboard > Tools > Email Track and Trace

### Email Track and Trace

Search and identify emails processed by your Email Security Services

Search Search by ID

Message ID

*The message ID is attributed by the mail servers and can be found in the email header.*

View the results on screen  
 Email the results as a CSV file when the search is complete

Once the trace has been completed it will be very obvious which mails have triggered any of the scanning rules as the **services** field will be populated with the triggered service name next to the email in question.

After pinpointing the affected mail it is then possible to view the message information as well as a summary of the SMTP logs. This SMTP summary will usually indicate which rule in particular was triggered and for what reason. e.g. "**rule: racial lexical: WOP, wop, WOP**" would be a data protection rule that has been triggered.

You are here: Dashboard > Tools > Email Track and Trace

### Email Track and Trace

Search and identify emails processed by your Email Security Services

Search Search by ID

Timezone: GMT + Date range: Last 30 days + Subject line Contains: \* Modify Search

**Search complete: 1 results found**

|< < Previous Page 1 Next Page > >| View 10

Subject	Recipient	Sender	Accepted	Delivered	Service
\$1* Buys \$100,...	cheryl@thesb...	innovate@metee...	✔ 27 May 2016 5:13 AM	✔ 27 May 2016 5:13 AM	

< < Previous Page 1 Next Page > >| View 10

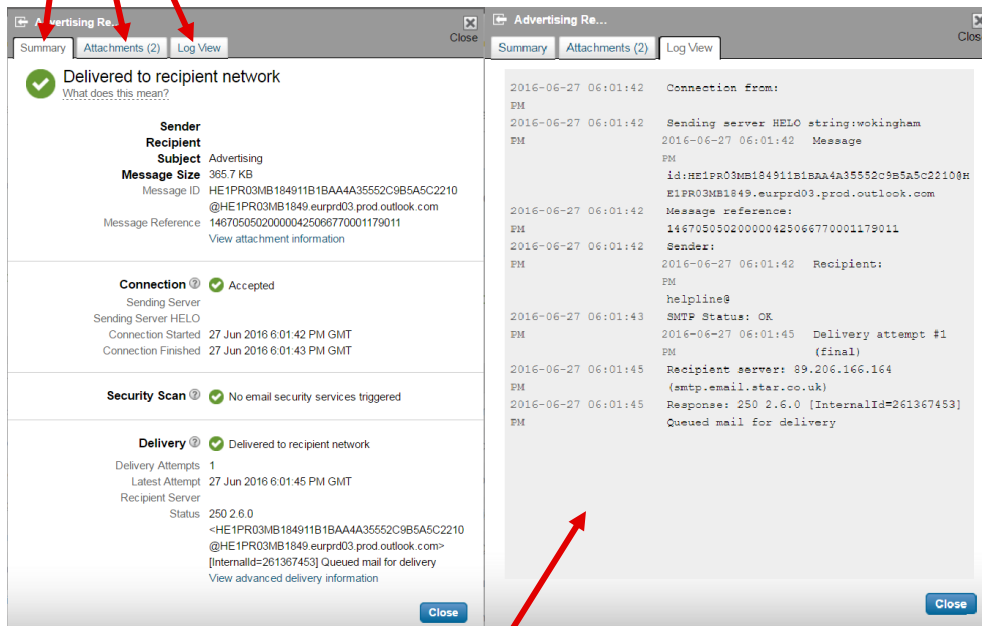
If mail has been delivered successfully both these field will be populated. If the delivery field is not populated or is mark with a red X this suggests either the mail is retrying delivery or it has failed. The SMTP log view will provide more details.

If mail delays have been experienced it will be visible within the trace results as the accepted date/time will be more than 1 minute difference to the delivered date/time. If mails are not shown in the trace this suggests that they have not been routed through the symantec.cloud infrastructure. If this is outbound mail then it is advised to

check the outbound smart host in use to confirm mail is being sent via Symantec. If this is inbound mail then the MX records should be checked to make sure that the domain is pointing to Symantec.

Once the mail has been pinpointed it is then possible to view further information on the mail using the mail summary. This can be opened by clicking on the subject of the mail. You will then be presented with the page below.

Clicking on the message in question will provide the summary of the message and the attachments and log view provide further details on the message content and delivery details. The message reference can be obtained from this view.



The log view provides a copy of the delivery log for a message. From this extract of the SMTP logs, it is possible to see where delivery was attempted and any errors that occurred during the attempt.

If mail issues have been experienced and the reason is not provided in the short log view it is recommended to take note of the message reference and provide this to Star / Symantec, the full STMP logs can be retrieved from this reference and troubleshooting can begin to pinpoint the cause of the issue. Please note however that logs older than 7 day may not be retrievable or may only be partially retrievable. As such please report any issues as soon as possible.

## 5 Configuring rules within Data Protection

To create a new rule navigate to the **Data Protection** main page (Services-> data protection) and select the **New Policy** button.

The first step to creating a rule is to name the rule. This should be relative to what the rule will scan for e.g. "profanity". Rule names can be up to 255 alphanumeric characters long (this includes spacing) but cannot contain other character types.

### Create a New Policy

The screenshot shows a web form titled "Create a New Policy". It contains the following elements:

- Name \*:** A text input field.
- Description:** A larger text input field.
- Apply to:** Three radio button options: "Both inbound and outbound email" (selected), "Inbound email only", and "Outbound email only".
- Execute if:** A dropdown menu currently showing "ALL rules are met".
- Action:** A dropdown menu currently showing "Log Only". To its right is a checkbox labeled "Stop evaluation of lower priority policies".
- Administrator email:** A text input field with a "Use custom" checkbox next to it.
- Notification:** A text input field containing "Administrator Edit".
- Buttons:** "Add Rule" (blue), "Cancel" (white), and "Save" (blue).

After the name has been defined the direction in which the rule applies will need to be selected. Options available are "inbound" which will apply to inbound mail only, "outbound" which will apply to outbound mail only, or "both" which will apply to all mails.

When you have confirmed if inbound and outbound are being scanned then you have choose if the rule is "Execute" if all rules are met or if any rules are met.

## Actions & Notifications

The **Actions** section defines how an email is handled once detection has taken place. The Actions section of this page allows for administrator address to be modified and the way in which the mail is handled. There are a number of actions that can be assigned to a rule, these are listed below:

### Block and delete

The email is prevented from reaching the intended recipients. It is permanently deleted. The scanning process is terminated for this email.

### Route to

Enables you to specify which of your registered inbound email routes each user's emails are delivered to.



## **Tag subject line**

A tag is added to the subject line. You define the text for the tag. Tagging the subject line provides the benefit of warning a user before they open it that the email may contain unacceptable content. The scanning process continues.

## **Tag with header**

A comment is added into the email X-Header to indicate that the email has triggered a Data Protection rule. The scanning process continues.

## **Compress attachments**

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 scanning process continues.

## **Allow**

Will allow the mail through to the location it was looking to go to.

## **Copy to administrator**

The email is flagged to be copied to a nominated Data Protection administrator once scanning is completed. The scanning process continues. The email is sent to the intended recipient.

## **Log only**

The portal Data Protection statistics record that a rule has been triggered. No other action is taken. The scanning process continues.

## **Redirect to administrator**

The email is redirected so that it does not continue on to the intended recipients. Instead, it is sent to a nominated administrator of the Data Protection service. The scanning process is terminated for this email.

Once you have decided on how your rule is going to be “execute” and then what “Action” is going to be taken then you need to add the rules to your policy.



### Create a New Policy

Name \*:

Description:

Apply to:  Both inbound and outbound email  
 Inbound email only  
 Outbound email only

Execute if:

Action:   Stop evaluation of lower priority policies

Administrator email:   Use custom

Notification: Administrator Edit

Rule 1	Execute if: ALL conditions are met
<input type="text" value="-- Add a condition --"/>	

- Add a condition --
- Attachment Filename List
- Attachment MIME Type List
- Attachment Number
- Attachment Size
- Attachment is Password Protected
- Attachment is Spoofed
- Content Keyword List
- Content Regular Expression List
- Content URL List
- Email Importance
- Email MIME Type
- Email Size
- Email is Encrypted
- Match All
- Recipient Domain List
- Recipient Group
- Sender Domain List
- Sender Group
- Time Interval

This box will give you different options when it comes to rules after clicking add new rule.

You can have multiple rules set up on one policy just by clicking **Add Rule** and choose the type of condition you want.

**Create a New Policy** ?

Name\*:

Description:

Apply to:  Both inbound and outbound email  
 Inbound email only  
 Outbound email only

Execute if:

Action:   Stop evaluation of lower priority policies

Administrator email:   Use custom

Notification: Administrator Edit

---

Rule 1 Execute if: ALL conditions are met

**Attachment Properties – Attachment MIME types**

There are currently no MIME Type Lists added

---

Rule 2 Execute if: ALL conditions are met

**Email Properties – Email Size**

(MB including attachments)

**Policy Summary**

CONTAINS (2) Rule(s)

Rule 1  
Attachment MIME Type List

AND

Rule 2  
Email Size

This is where you can see the different rules you have set up on your policy. Also if you look top right you can see a summary about the policy.

If you do not wish to create your own policy you can chose from existing policy that is setup and you can do this from the **New Policy form Template**, each has a description of what these policies will cover.

Create a new policy from a template
?
X

Please select a policy to create from one of the following templates.

**EU Data Protection Directives Template**  
EU Data Protection Directives Template

**HIPAA (Health Insurance Portability and Accountability) Template**  
HIPAA (Health Insurance Portability and Accountability) Template

**PCI (Payment Card Industry) Template**  
PCI (Payment Card Industry) Template

**ITAR (International Traffic in Arms Regulation) Template**  
ITAR (International Traffic in Arms Regulation) Template

**Gramm-Leach-Bliley Template**  
Gramm-Leach-Bliley Template

**PBE E Trigger Template (EU)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or attachments or the header inserted by the PBE E Encrypt Button of an email sent from your organization

**PBE E Trigger Template (US)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or attachments or the header inserted by the PBE E Encrypt Button of an email sent from your organization

**Illegal Drugs Template**  
Illegal Drugs Template

**PBE Z Pull Keyword Trigger Template (EU)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or any attachments or the header inserted by the PBE Z encrypt button of an email sent from your organization. Encrypted emails will be delivered by the Pull method unless the recipient is also a PBE Z customer in which case their preferred delivery method will be used.

**PBE Z Pull Keyword Trigger Template (US)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or any attachments or the header inserted by the PBE Z encrypt button of an email sent from your organization. Encrypted emails will be delivered by the Pull method unless the recipient is also a PBE Z customer in which case their preferred delivery method will be used.

**PBE Z Push Keyword Trigger Template (EU)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or any attachments or the header inserted by the PBE Z encrypt button of an email sent from your organization. Encrypted emails will be delivered by the Push method unless the recipient is also a PBE Z customer in which case their preferred delivery method will be used.

**PBE Z Push Keyword Trigger Template (US)**  
This template requires the administrator address to be modified to that provided to you when you purchased the service. The template is set to look for a specific keyword within the email body or any attachments or the header inserted by the PBE Z encrypt button of an email sent from your organization. Encrypted emails will be delivered by the Push method unless the recipient is also a PBE Z customer in which case their preferred delivery method will be used.

Cancel Create

Pick your policy and then click **Create** and this will actively create a policy and put it live.

## 6 Lists

When you are on the **Data Protection** page there is a **List** tab, this tab is for your to create your own lists of either Key words, URL's or domains.

Apply to: All

Search list name or content  All Search New List New List Group ?

**Custom Lists (3)** Collapse

Select: Delete | Copy | Group Showing 1 – 3 of 3 < Previous Page 1 Next Page > >| View 10

<input type="checkbox"/>	Name	Content type	List type	Category	Active	Last updated
<input type="checkbox"/>	competitors	Filenames	Single	None	No	25 Nov 2004 5:37 PM by STA154 (STA154)
<input type="checkbox"/>	suspicious domains	Domains	Single	None	No	25 Nov 2004 2:43 PM by STA154 (STA154)
<input type="checkbox"/>	video	MIME types	Single	None	No	25 Nov 2004 2:54 PM by STA154 (STA154)

**Managed Lists (110)** Collapse

Managed lists cannot be changed as they are pre-configured and will be updated automatically.

Select: Copy Showing 1 – 10 of 110 < Previous Page 1 2 3 4 5 ... Next Page > >| View 10

<input type="checkbox"/>	Name	Content type	List type	Category	Active	Last updated
<input type="checkbox"/>	ABA Keywords	Keywords	Single	Banking & Finance	No	14 Nov 2011 4:54 PM by Unknown
<input type="checkbox"/>	ABA Routing Numbers	Regular expressions	Single	Banking & Finance	No	23 Feb 2013 9:44 AM by Unknown
<input type="checkbox"/>	application	MIME types	Single	MIME Types	No	31 Oct 2006 7:52 AM by Unknown
<input type="checkbox"/>	audio	MIME types	Single	MIME Types	No	31 Oct 2006 7:52 AM by Unknown
<input type="checkbox"/>	Birthdate	Regular expressions	Single	Personally Identifiable Information	No	14 Nov 2011 4:55 PM by Unknown
<input type="checkbox"/>	Confidential Documents Keywords	Keywords	Single	Confidential	No	23 Feb 2013 9:44 AM by Unknown
<input type="checkbox"/>	Contract Keywords	Keywords	Single	None	No	23 Feb 2013 9:44 AM by Unknown
<input type="checkbox"/>	Controlled Substances	Keywords	Single	None	No	18 May 2013 9:00 AM by Unknown
<input type="checkbox"/>	Credit Card Keywords	Keywords	Single	Banking & Finance	No	14 Nov 2011 4:54 PM by Unknown
<input type="checkbox"/>	Credit Card Magnetic Stripe Data	Regular expressions	Group (2)	Banking & Finance	No	23 Feb 2013 9:44 AM by Unknown

If you click **New List** this is where you would create your list specific to yourself and your company.

Create a New List

Please complete all fields marked with an asterisk (\*)

Name \*:  
Enter a list name...

Description:  
Enter a list description...

Category: None

Content type \*:  
Select a content type

Please select a content type first.

Cancel Save

Name this list what you wish with a description, you can set it to a category if you wish, but the content type is going to be any from the following list:

Create a New List

Please complete all fields marked with an asterisk (\*)

Name \*:  
Enter a list name...

Description:  
Enter a list description...

Category: None

Content type \*:  
Select a content type

- Select a content type
- Domains
- Filenames
- MIME types
- Keywords
- Regular expressions
- URLs

Please select a content type first.

Cancel Save

Once you have created your list of information when you choose the rule on your policy then these list can be used.