claranet soho
small office | home office

Image Control and Data Protection

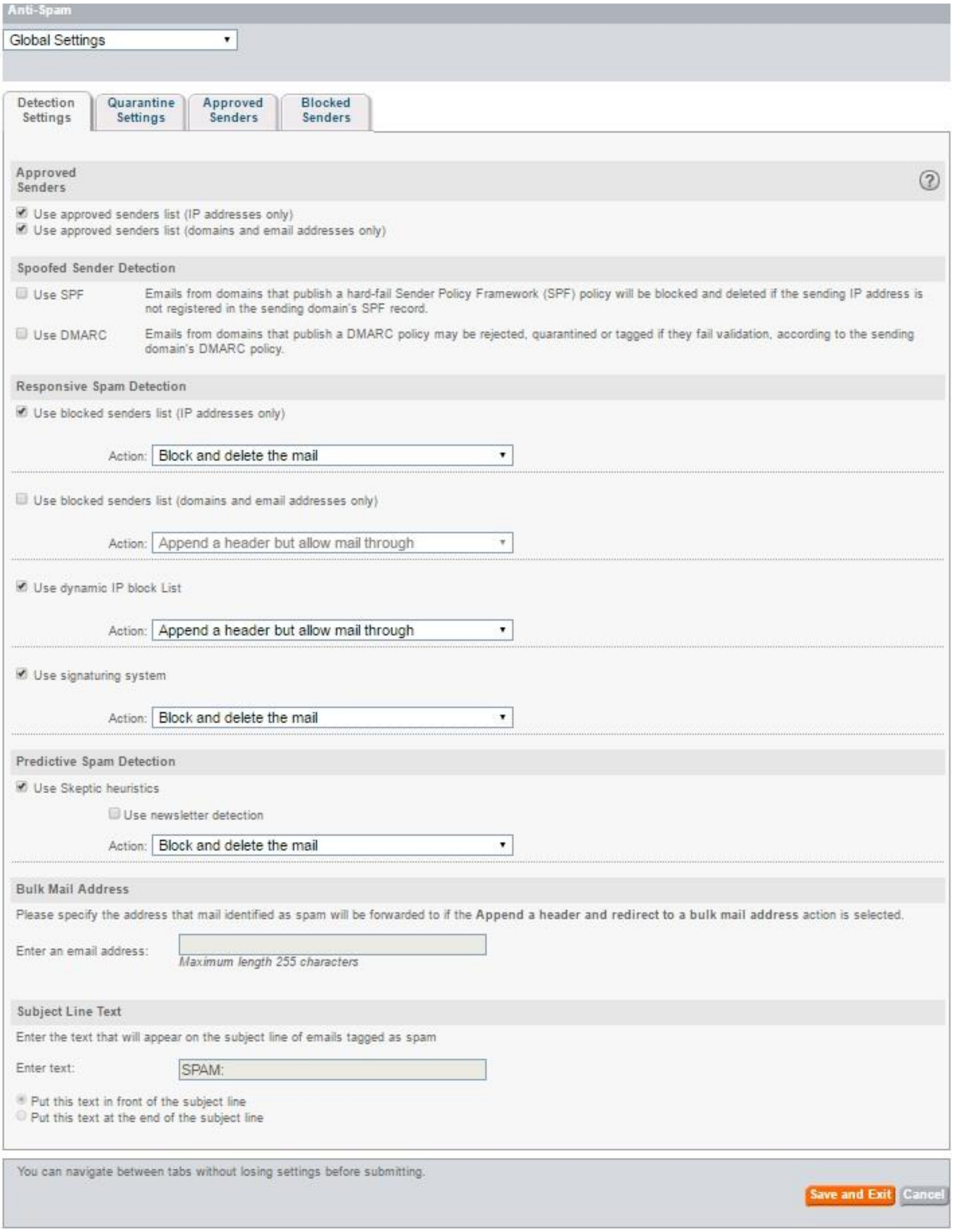
Image Control and Data Protection Support Guide.

Version 1.0

claranet soho
small office | home office

Contents

1 Configuring rules within Image Control



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?

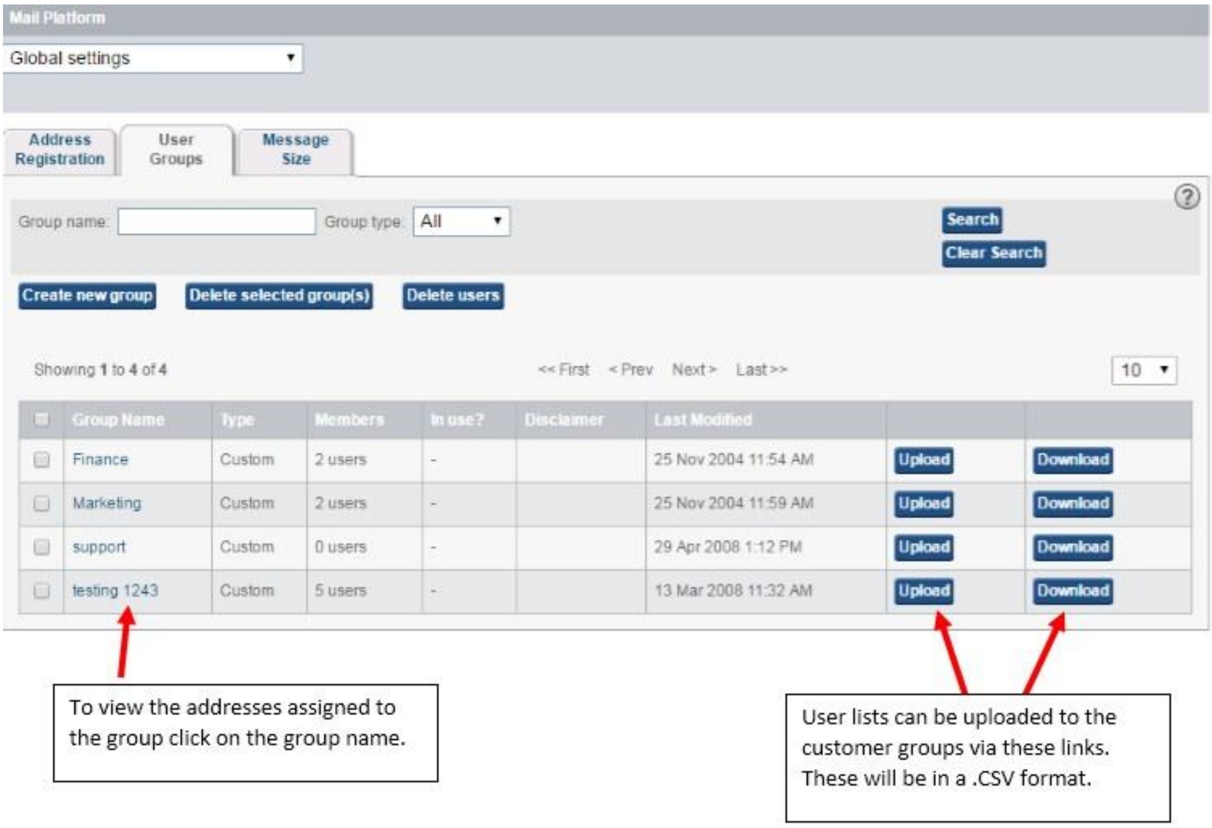
Custom groups are used within the Symantec.cloud system for applying custom disclaimers, filtering, data protection etc. They are useful as they provide a way of administering the portal on a more granular level.

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.

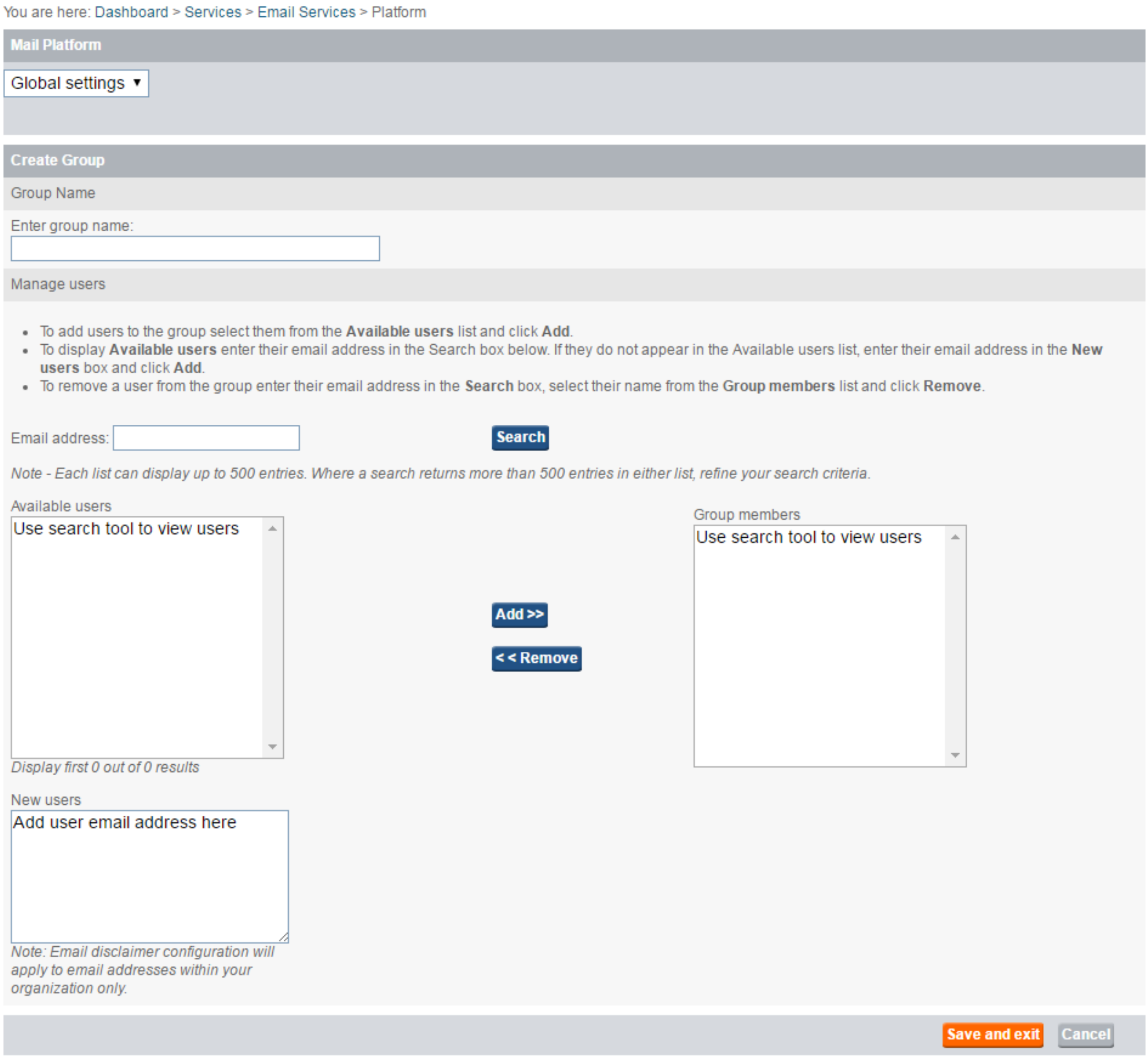
Current user groups will now be displayed. This main page also displays the number of users assigned to each group, the type of group, the date the group was last modified and also allows for user lists to be uploaded and downloaded. Clicking on the group name will allow you to view the list of users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



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.



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.

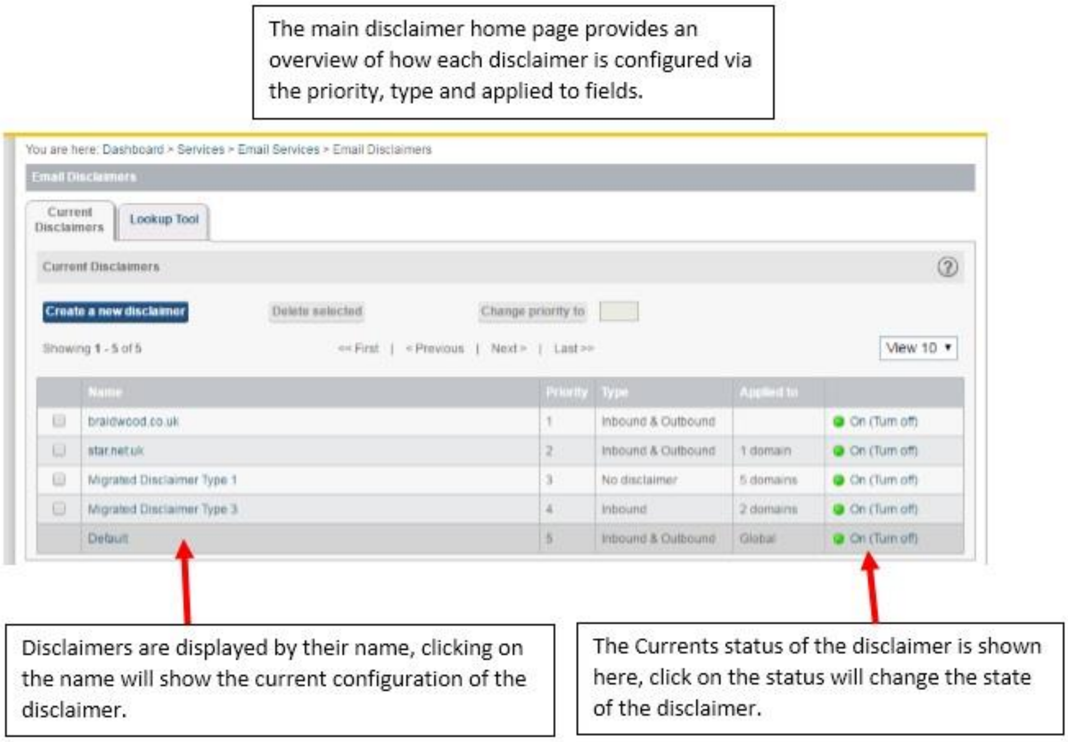
Some industries may require organizations to make certain disclosure statements when communicating by email.

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.

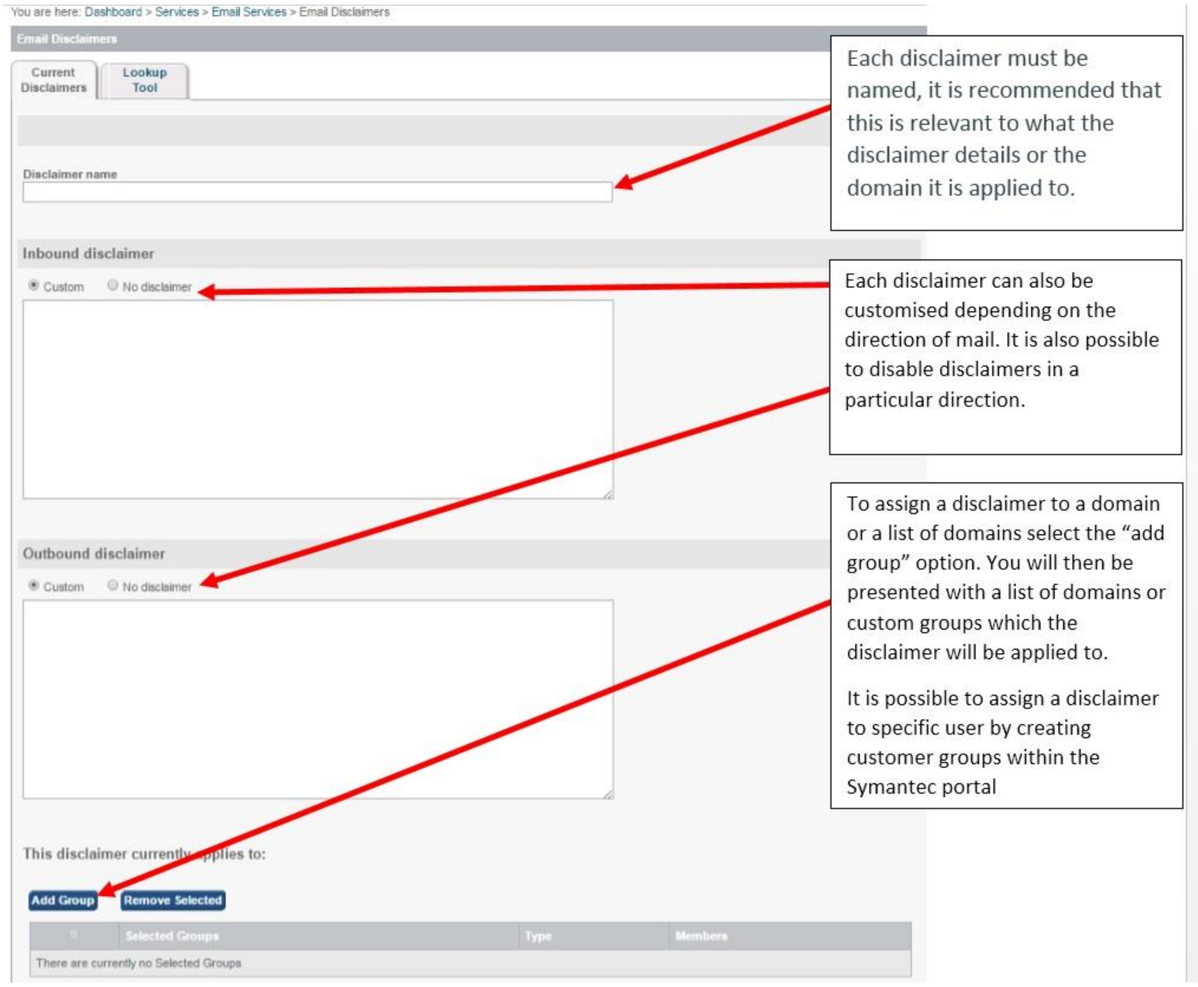
Configuring email disclaimers

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.



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.



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**

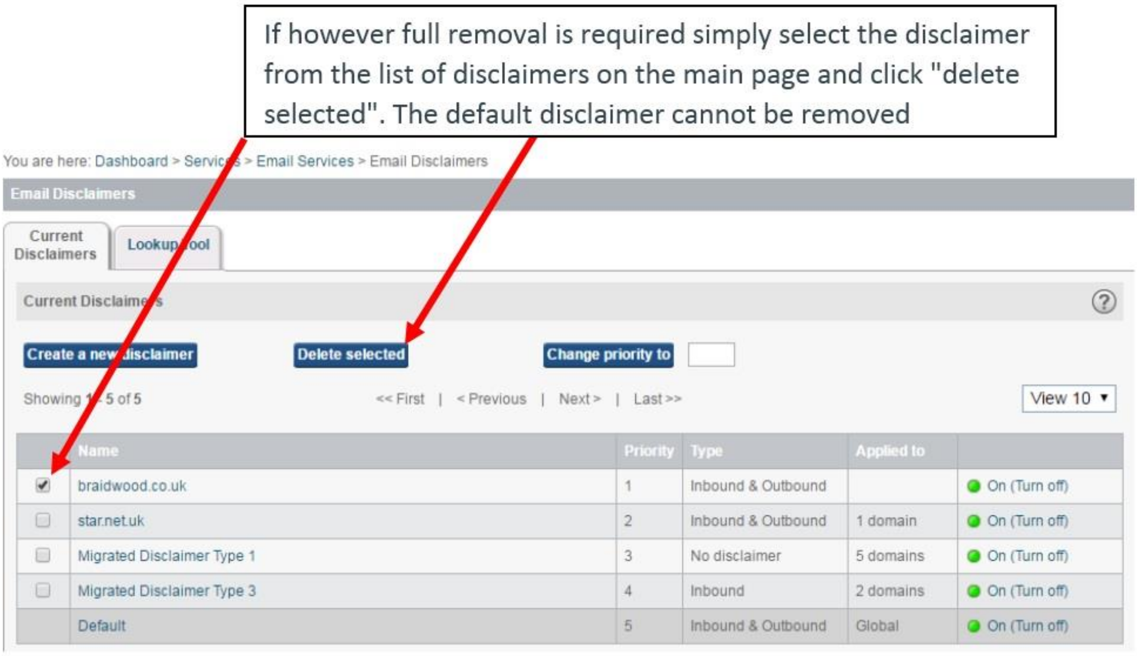
Editing existing disclaimers

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

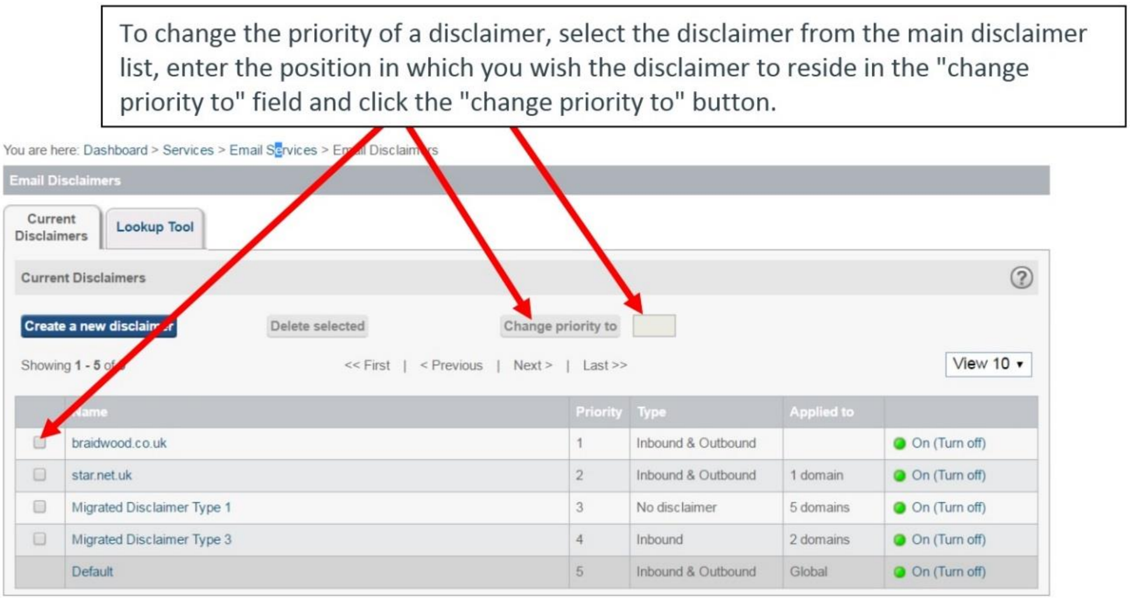
If you wish to remove a disclaimer from the portal full removal may not actually be required. It is possible to simply disable the disclaimer rather than remove it. This is useful if the disclaimer configuration is particularly complex or has a number of custom groups tied to it, as if the disclaimer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



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.



4 What is Track and trace?

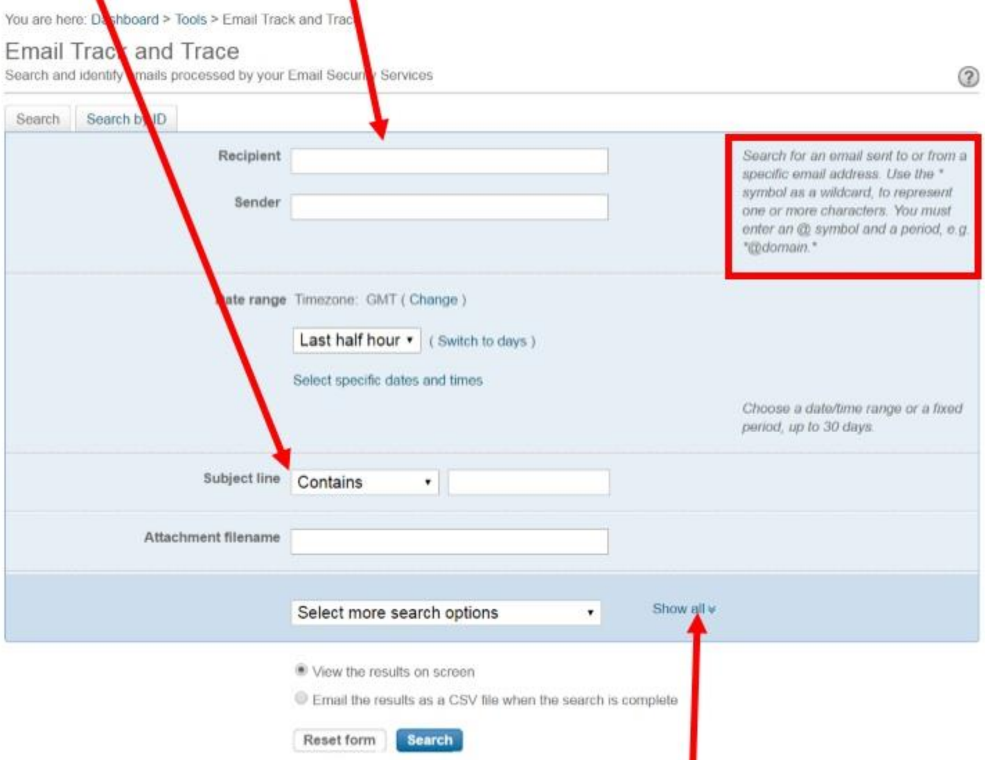
The Email Track and Trace tool lets you trace a specific email and determine if and when it was processed and the action taken. You can search for an email that was processed within the last 30 days.

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

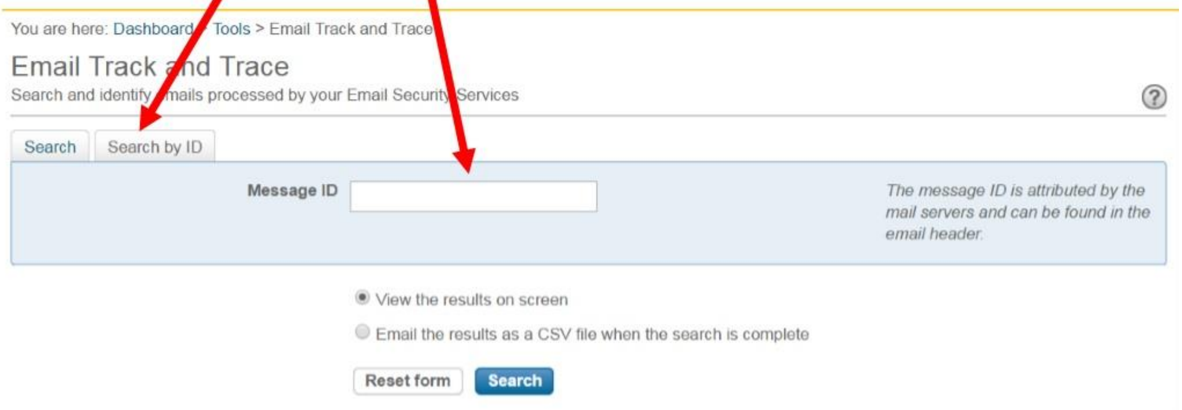
To perform a trace on emails first you will navigate to the tool (Tools-> Email Track and Trace). You will now be able to enter your search criteria. The more information that can be entered into these fields the more accurate the trace will be.

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.



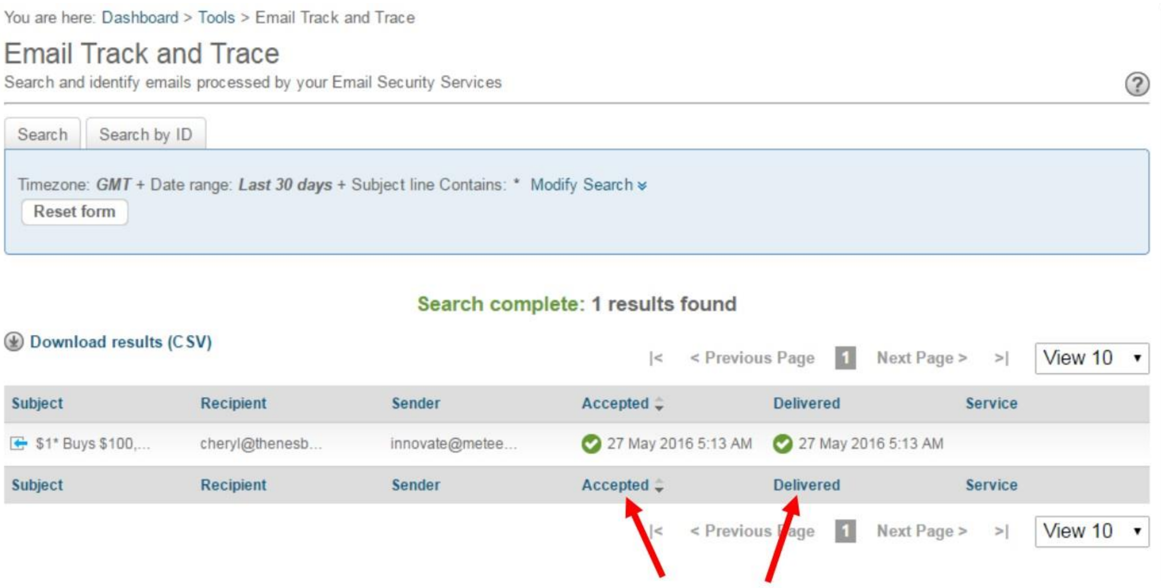
There are further search options available using the show all link at the bottom of the page. These include searching via sending server IP, receiving server IP, email size, the help message sent by the receiving server and any mails that have been triggered by a particular service.

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.



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.

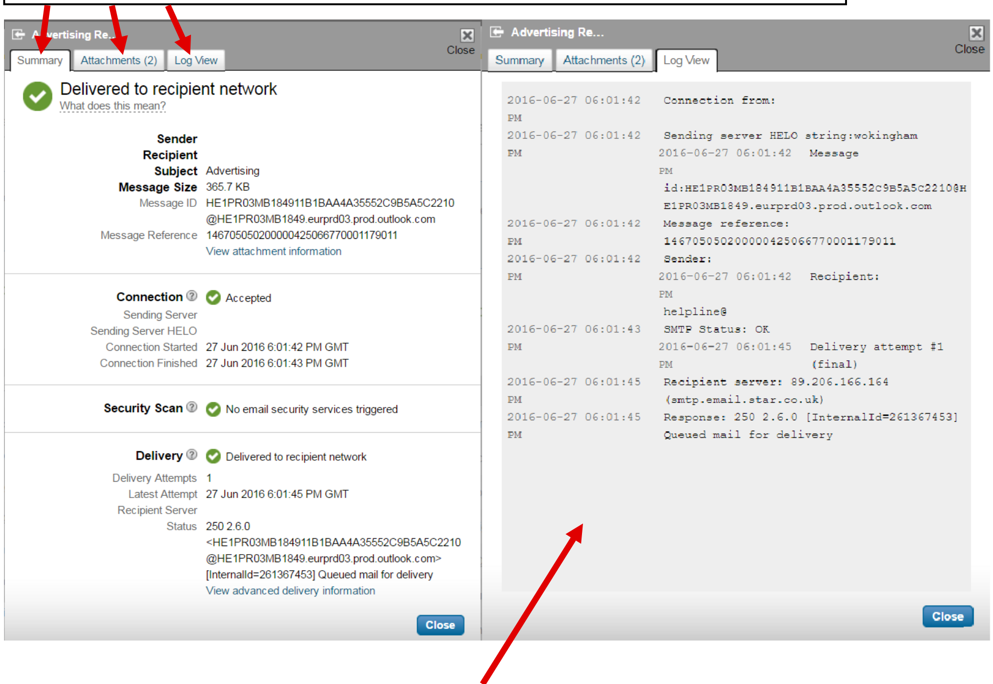


If mail has been delivered successfully both these field will be populated. If the delivery field is not populated or is mark with a red X this suggests either the mail is retrying delivery or it has failed. The SMTP log view will provide more details.

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.



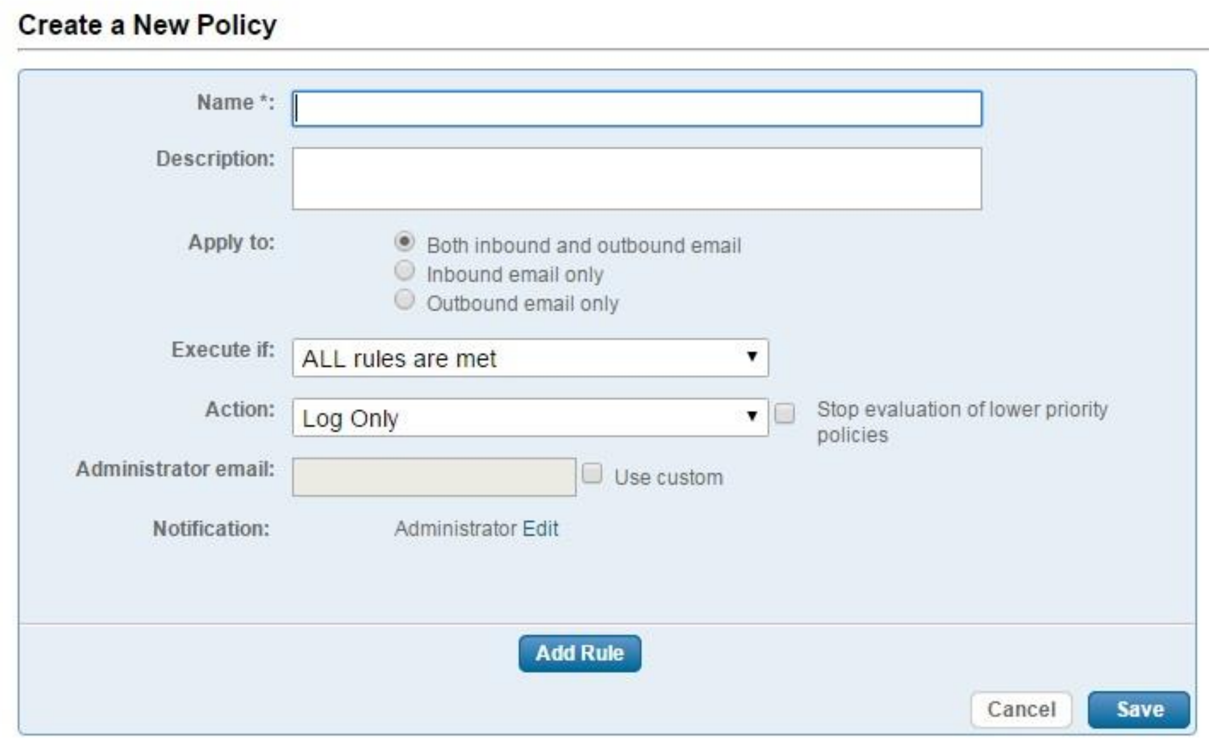
The log view provides a copy of the delivery log for a message. From this extract of the SMTP logs, it is possible to see where delivery was attempted and any errors that occurred during the attempt.

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.



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.

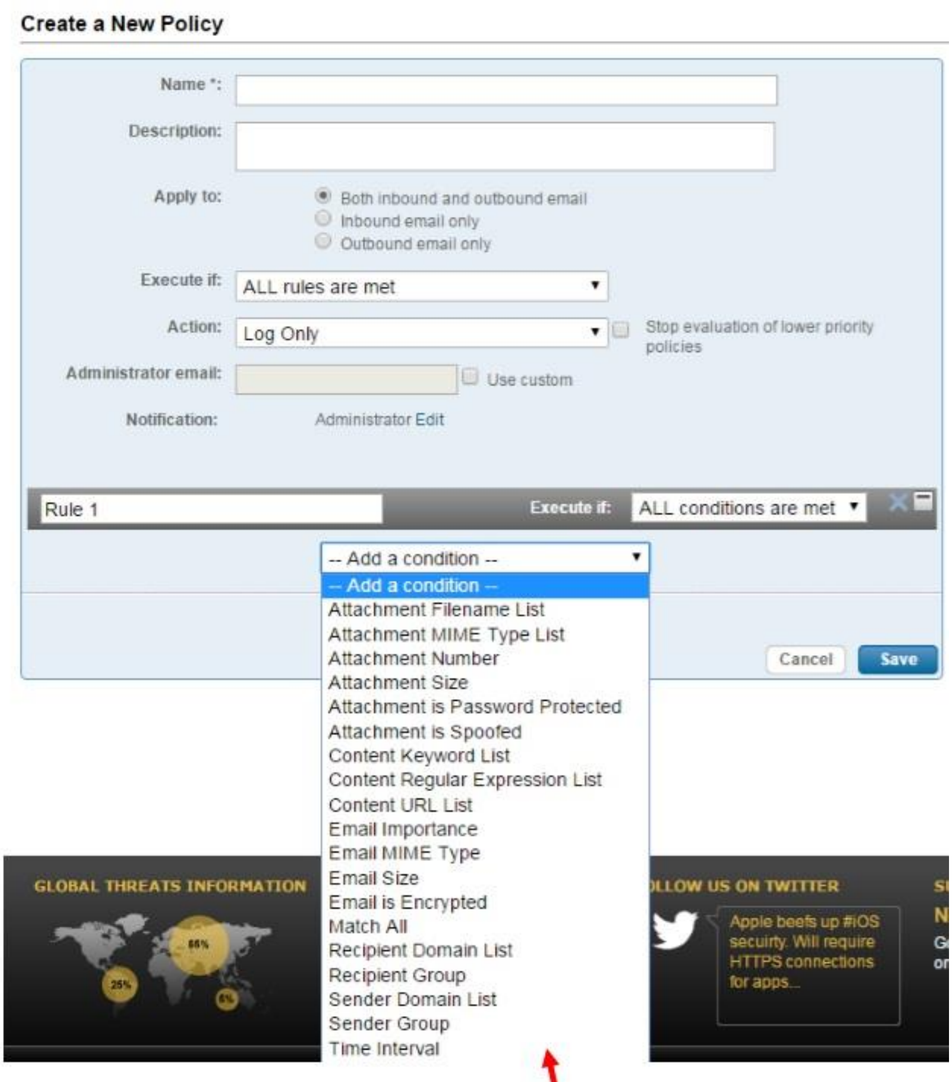
Log only

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

Redirect to administrator

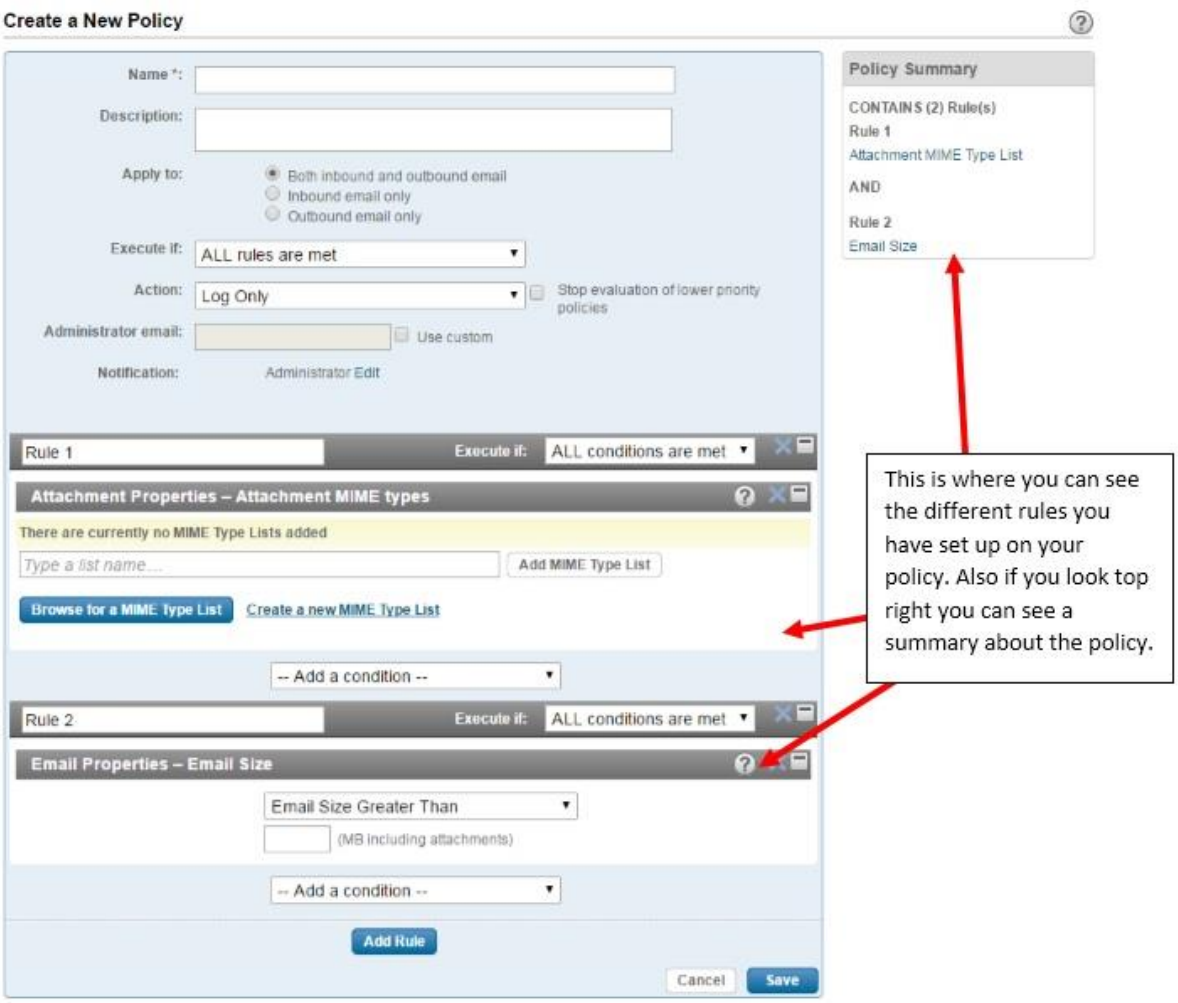
The email is redirected so that it does not continue on to the intended recipients. Instead, it is sent to a nominated administrator of the Data Protection service. The scanning process is terminated for this email.

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.

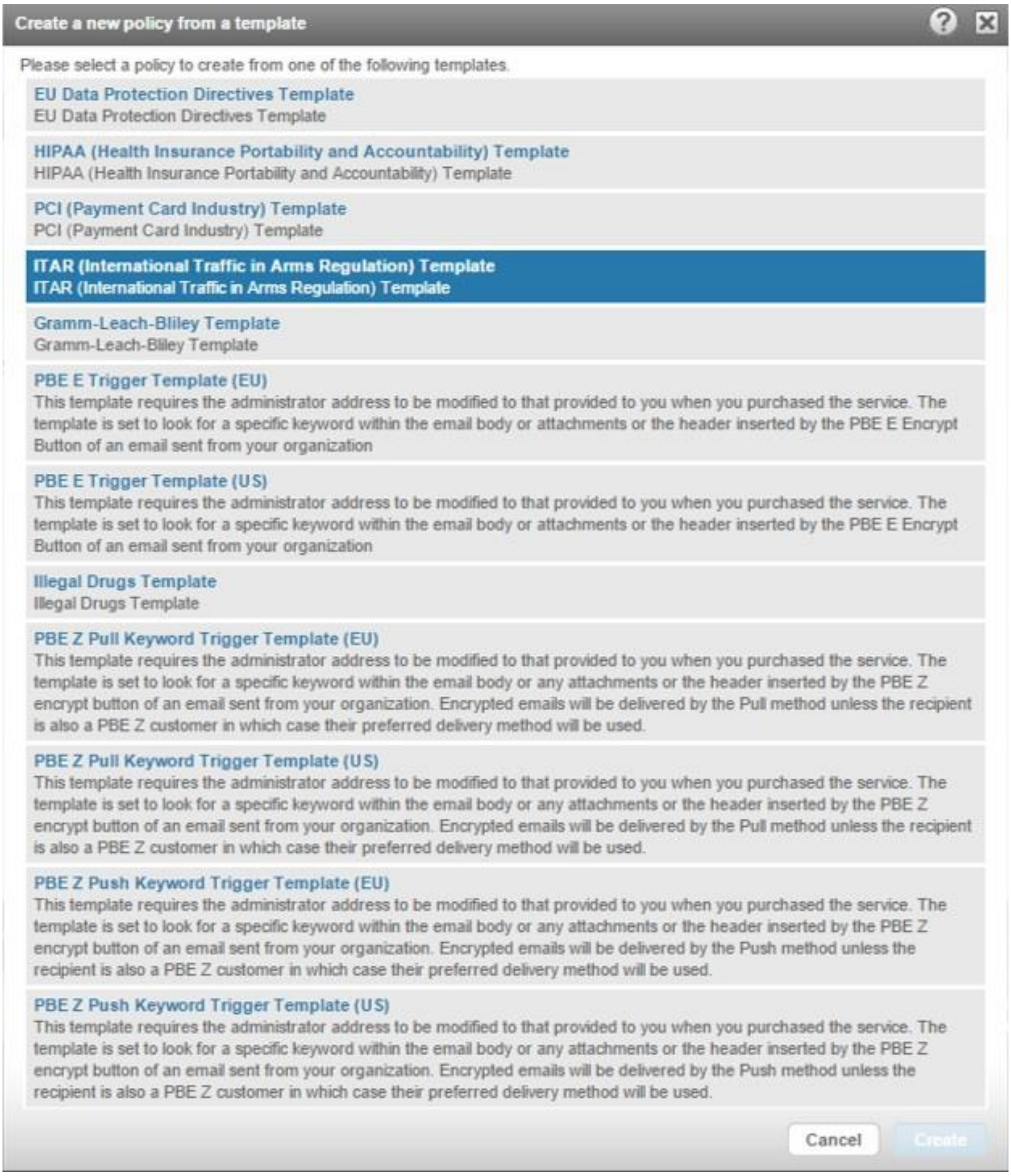


This box will give you different options when it comes to rules after clicking add new rule.

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



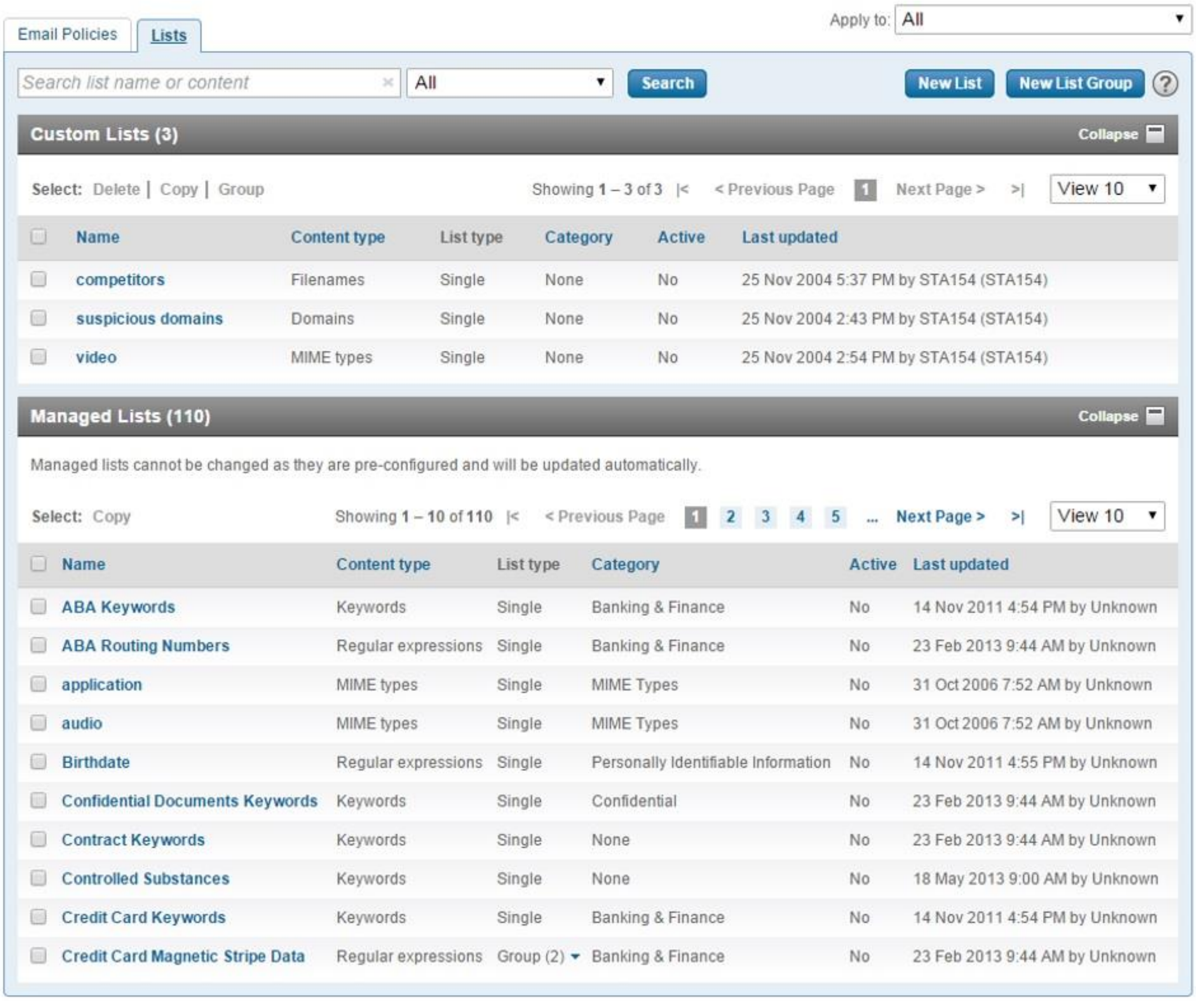
If you do not wish to create your own policy you can chose from existing policy that is setup and you can do this from the **New Policy form Template**, each has a description of what these policies will cover.



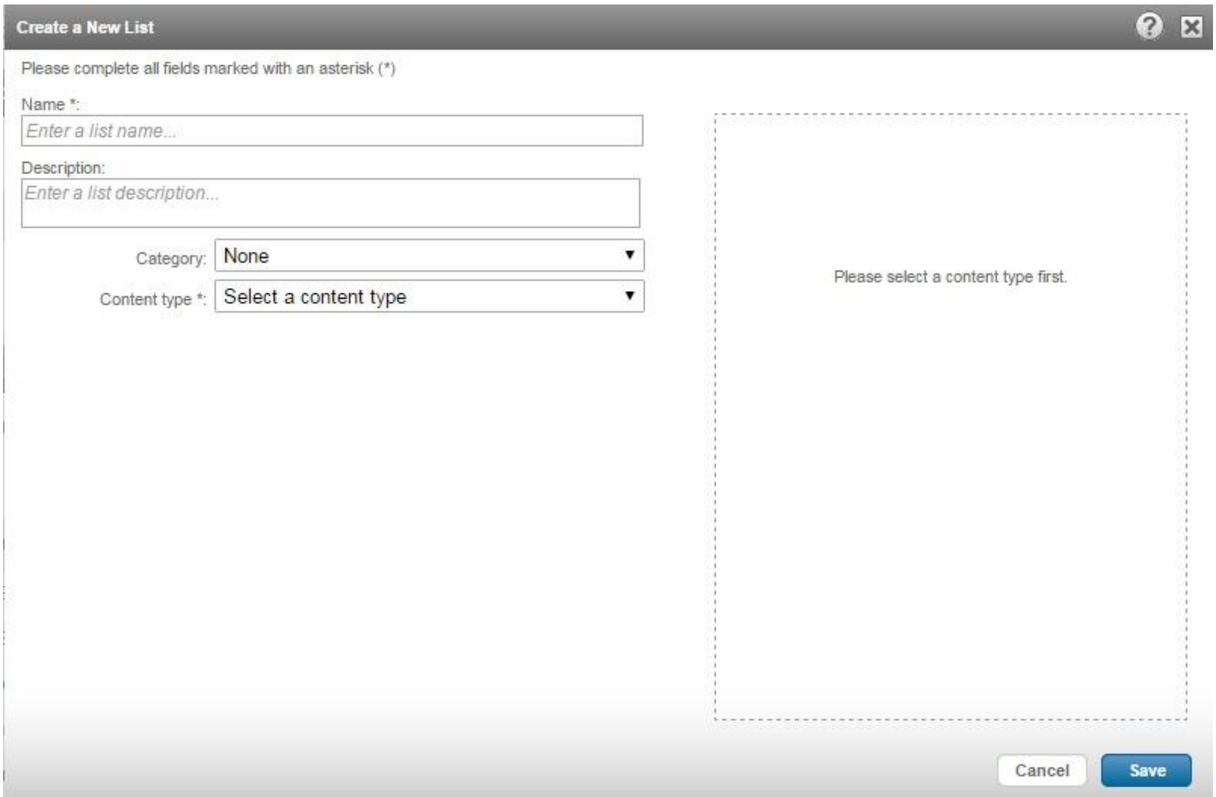
Pick your policy and then click **Create** and this will actively create a policy and put it live.

6 Lists

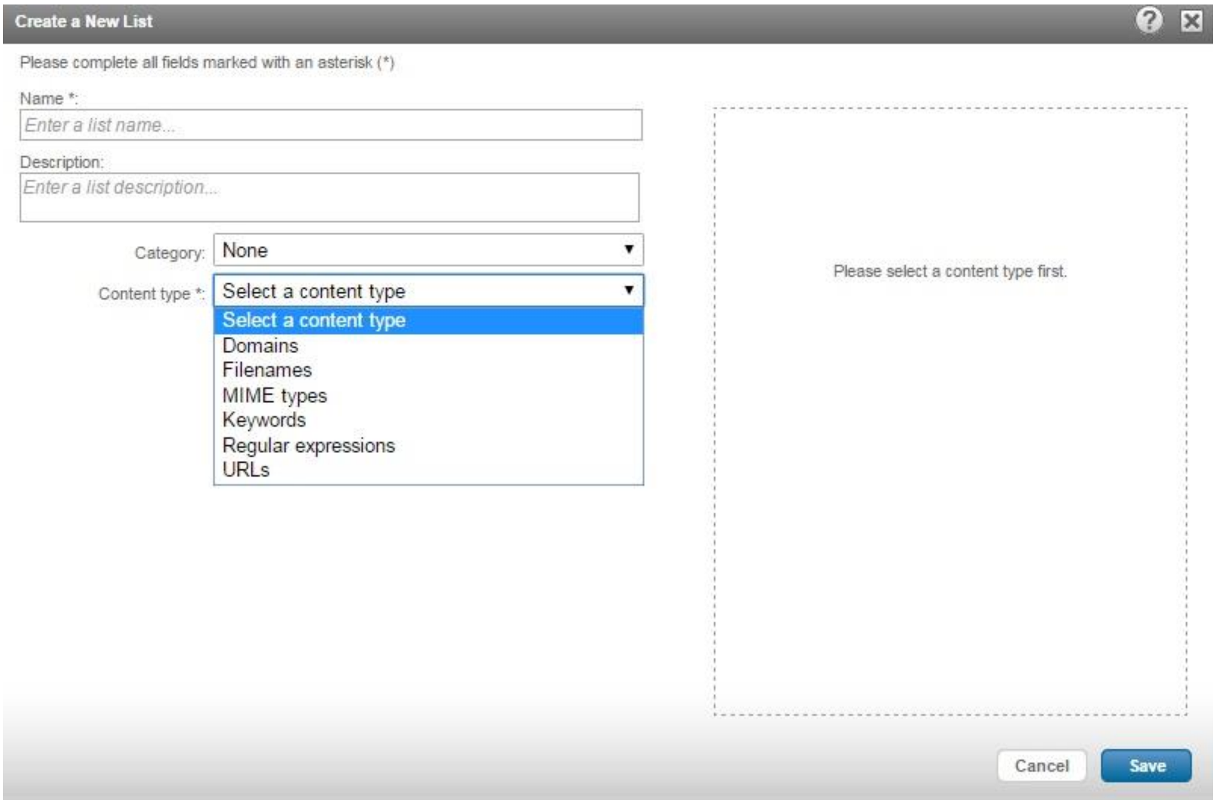
When you are on the **Data Protection** page there is a **List** tab, this tab is for your to create your own lists of either Key words, URL's or domains.



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



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:



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