APPTIX®
Connecting Your Business. Anywhere.

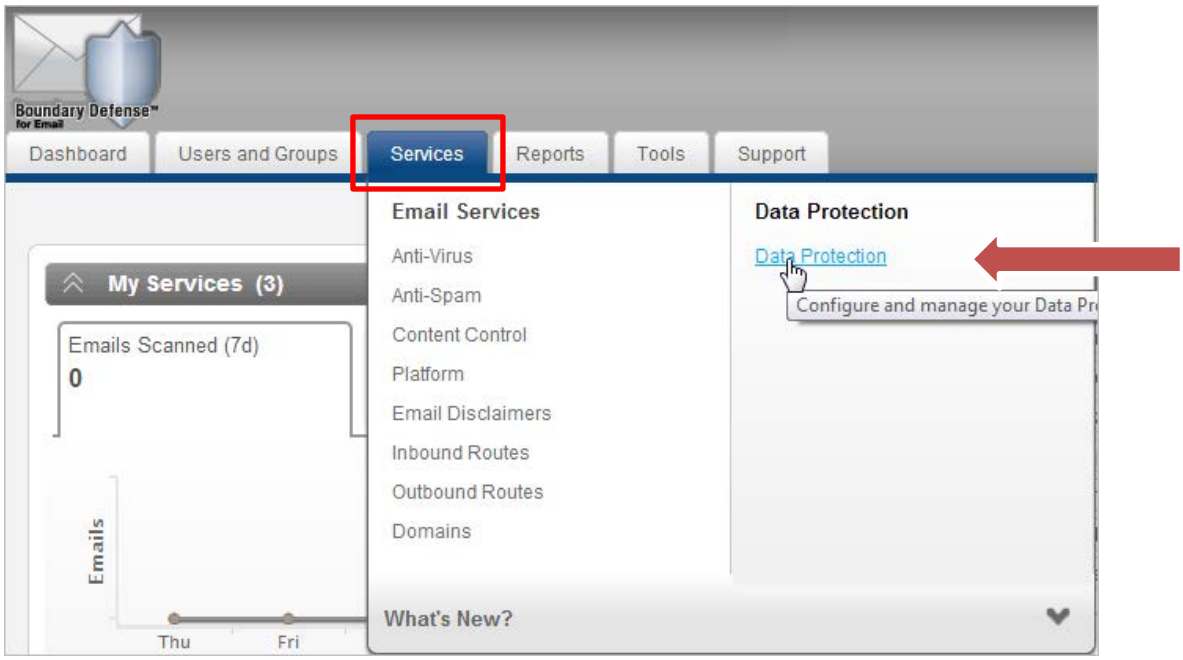
Create a New Data Protection Policy in the Symantec.cloud Management Portal

Document Revision Date: August 14, 2014

Contents

Configure Data Protection Settings in the Symantec.cloud Management Portal

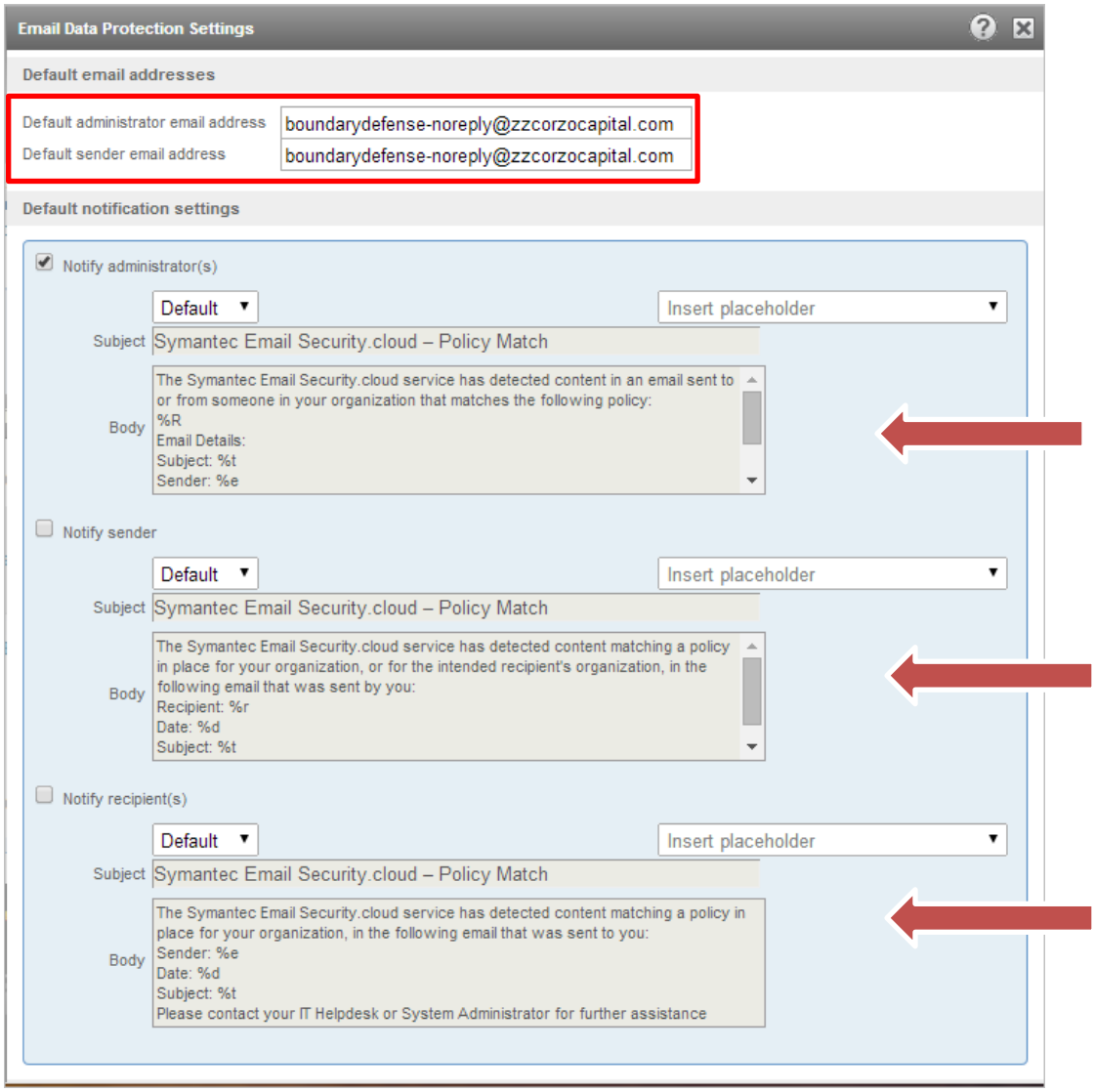
1. Access the *Symantec.cloud* management portal.
2. Select the **Services** tab:



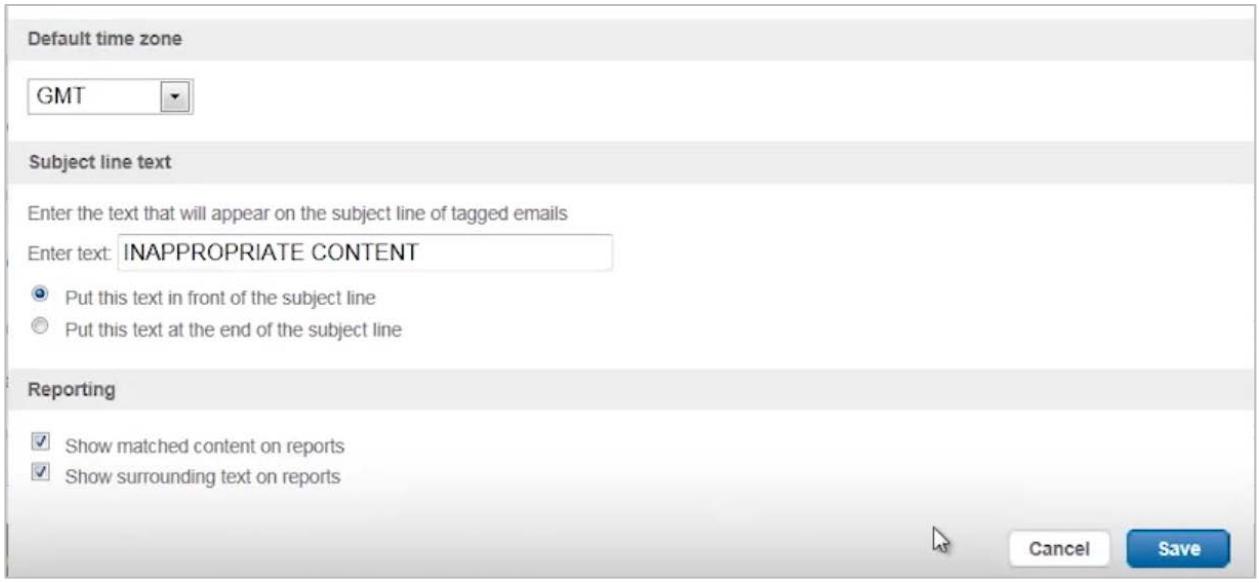
3. Select **Data Protection**.
   The **Email Policies** tab displays
4. Click the **[Settings]** button:

In **Settings**, you can manage the default email addresses, notification settings, default time zone, subject line text (used for tagged emails), and reporting options.

The **Email Data Protection Settings** dialog displays:

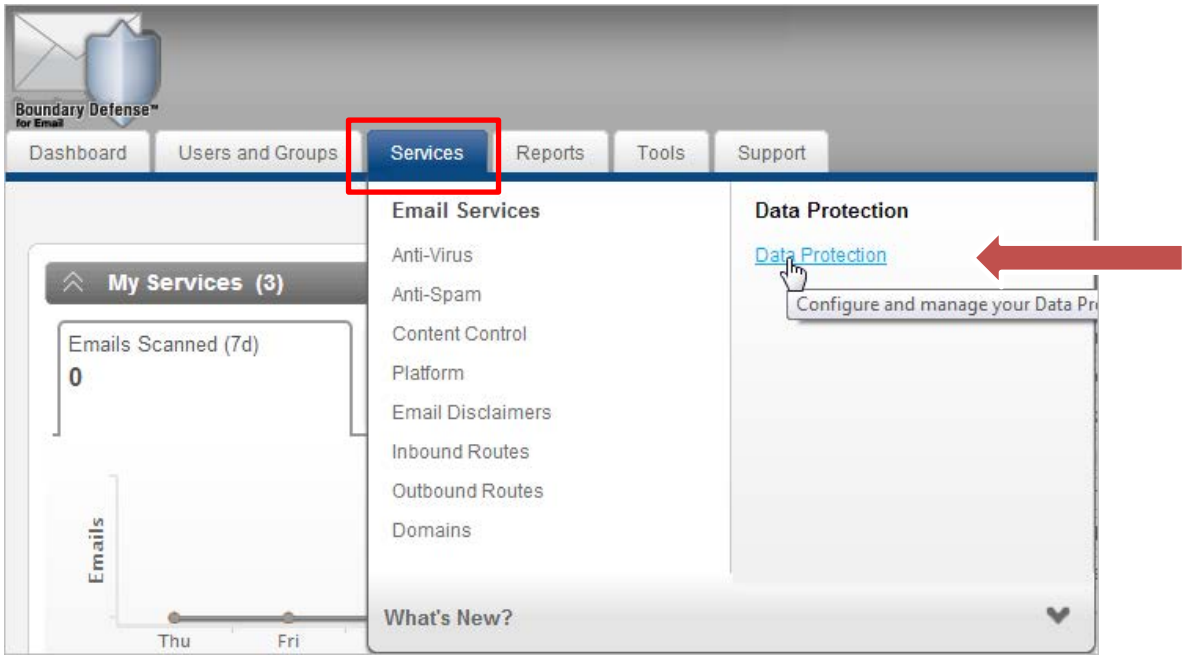


5. Begin by selecting the **Default email addresses** at the top.
6. Notice that you can also manage **Default notification settings** – messages to administrators, sender, and recipients.
7. Scroll down to manage the **Default time zone**, **Subject line text**, and **Reporting** options:


Default time zone
GMT
Subject line text
Enter the text that will appear on the subject line of tagged emails
Enter text: INAPPROPRIATE CONTENT
Put this text in front of the subject line
Put this text at the end of the subject line
Reporting
Show matched content on reports
Show surrounding text on reports
Cancel
Save

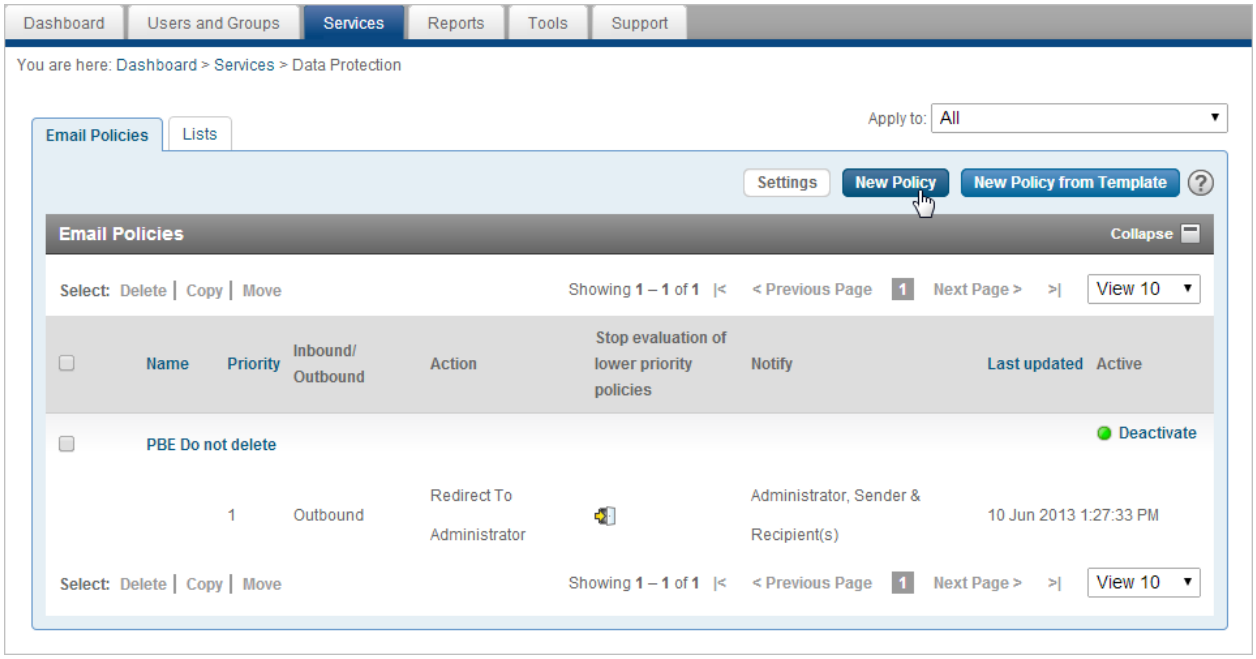
Create a New Policy in the Symantec.cloud Management Portal

1. Select the **Services** tab.
2. Select **Data Protection**.



The **Email Policies** tab displays. Here we will create the new policy.

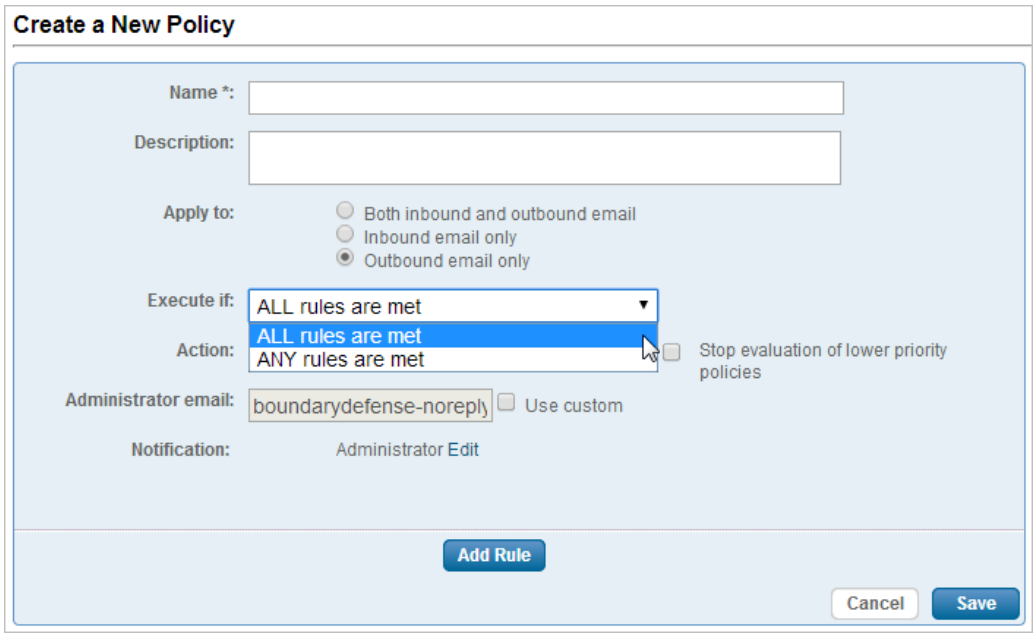
3. Select the **[New Policy]** button:



NOTE: Notice that some policies have already been created in the screen capture above. The green light at

the right indicates that the policy is activated, or on.
When you have more than one policy in your list, you can modify the order by using the up and down arrows _ ▲ ▼ .

4. On the first screen of the **Create a New Policy** wizard, enter a name for the new policy in the **Name** field:

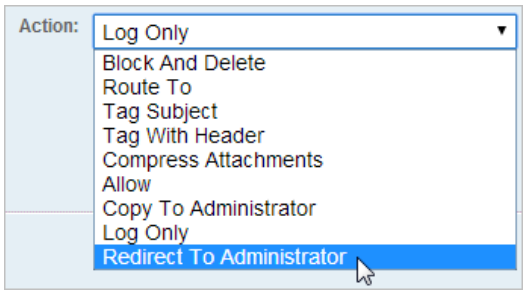


NOTE: **Description** is optional.

5. Select the email direction to which the policy should apply.
NOTE: In this example, we are selecting **Outbound email only**.

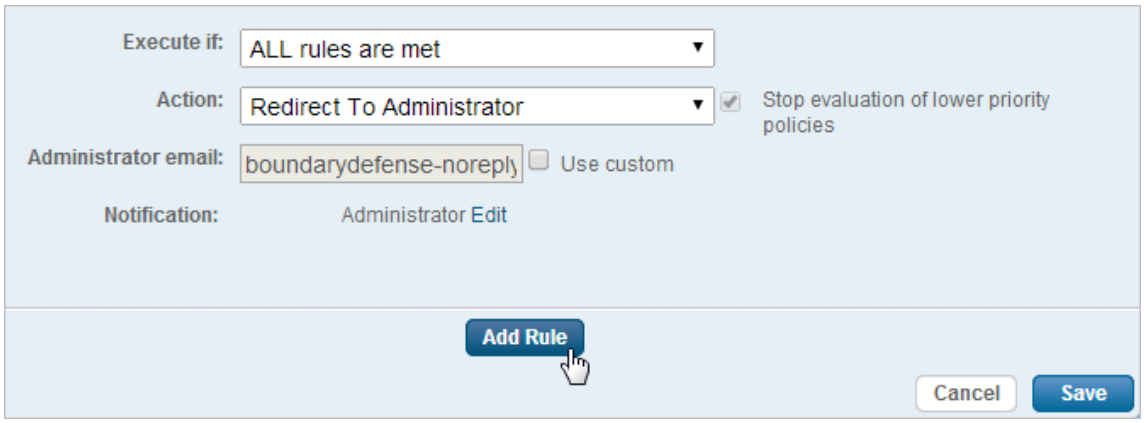
6. Select the **Execute if** field.
NOTE: This field controls the choice of an **AND** or an **ALL** relationship between the rules. In this example, we are using the default setting **ALL rules are met**.

7. From the **Action** drop-down list, select the action for this policy.
NOTE: In this example, we are selecting **Redirect to Administrator**.



Create a Rule for the New Policy

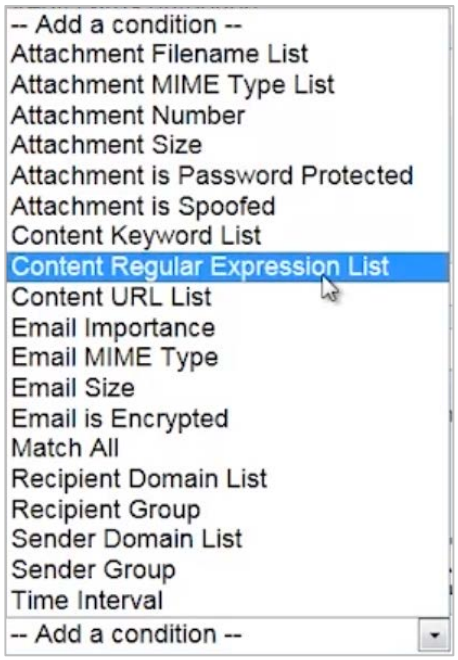
8. Click the **[Add Rule]** button.



The screen expands to include the **Executive if** and **Add a condition** functions.

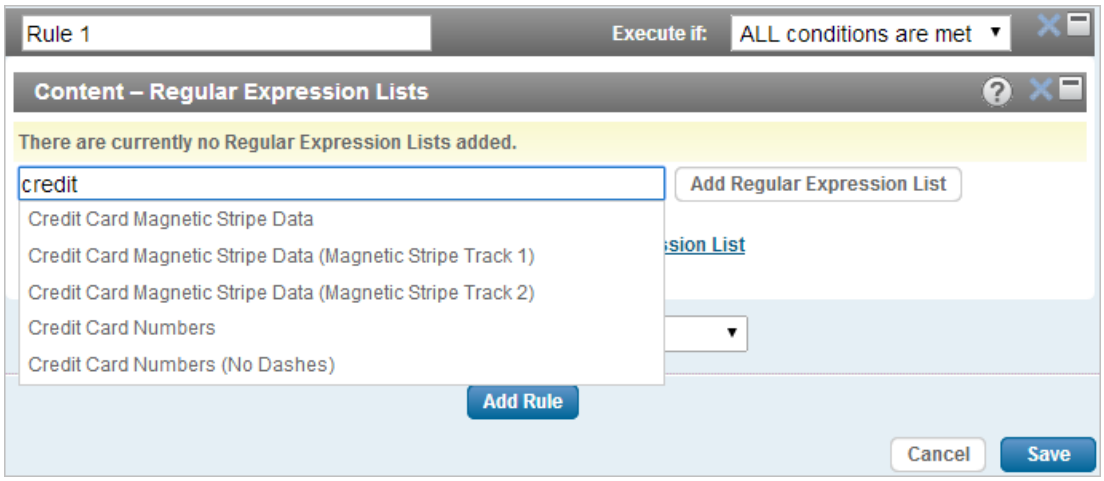
9. Select the appropriate **Execute if** option from the drop-down list:

10. To add a condition to the rule, select the **Add a condition** drop-down menu:



NOTE: In this example we are using the **Content Regular Expression List** (highlighted above).

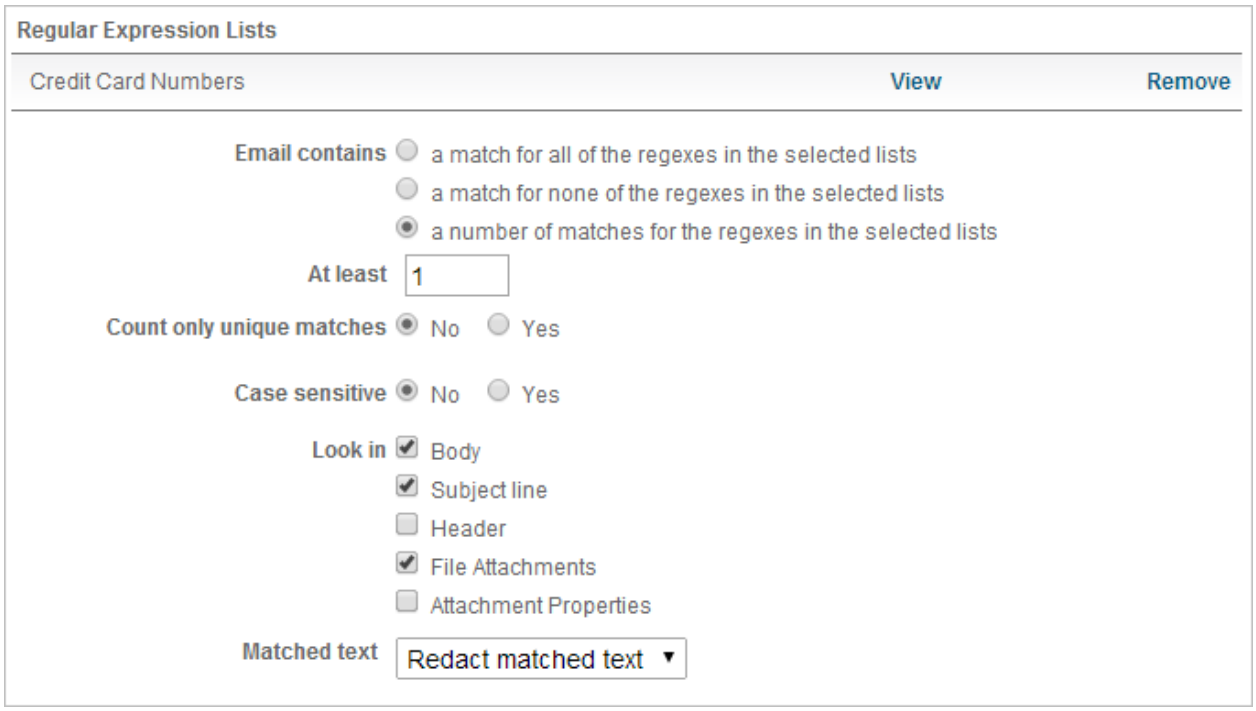
The **Content – Regular Expression Lists** search displays:



11. We are looking for Regular Expression Lists that pertain to credit cards, so we enter "credit" in the **Search** field. As you begin to type, the search performs automatically and results display in a drop-down list beneath your typing. For this example, we select "Credit Card Numbers" from the list.

NOTE: The Regular Expression Lists are built and maintained by Symantec, so the search pattern matches on credit card entries.

The Expression Lists portion of the screen expands to include options:

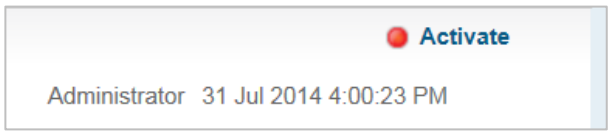


12. Choose which part of the email to match. In this example, we selected **Email contains: a number of matches**

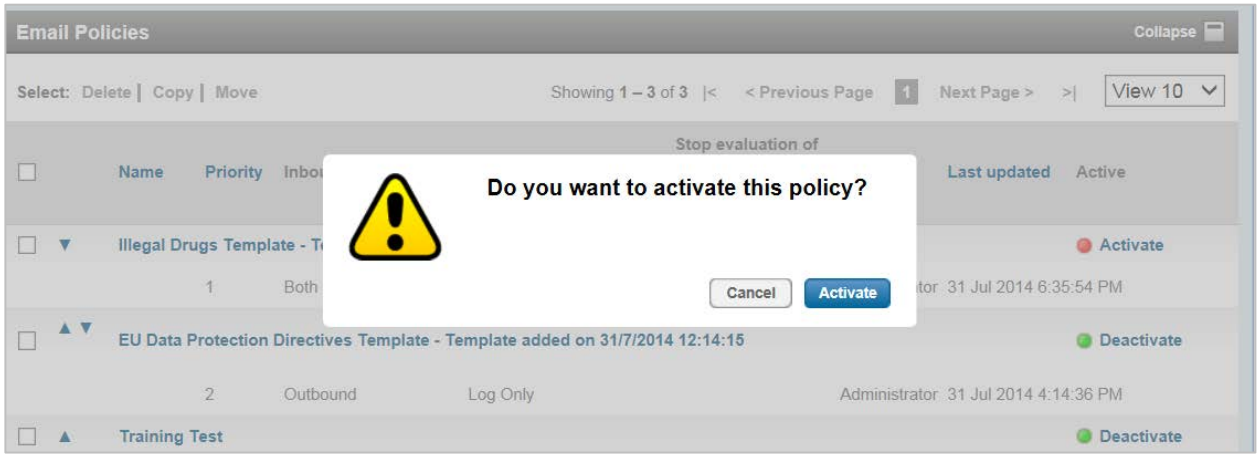
in the regexes in the selected lists, and we are choosing **At least: 1** match.
In this example, we selected to **Look in** the email **Body** and **Subject line**, and the **File Attachments**.
You can add more rules and conditions, but for this example the policy is complete.

13. Click **[Save]** to save the policy:

    The new policy displays at the bottom of the list and a red light displays (the new policy is not activated, or turned on):



14. Click **Activate** to turn the policy on.
    A pop-up window displays, which asks if you want activate the policy:



15. Click **[Activate]** to turn on the policy.
    The red light changes to a green light, and **Deactivate** displays: