APPTIX®
Connecting Your Business. Anywhere.

Policy Based Encryption

Admin Guide

Document Revision Date: Dec. 18, 2014

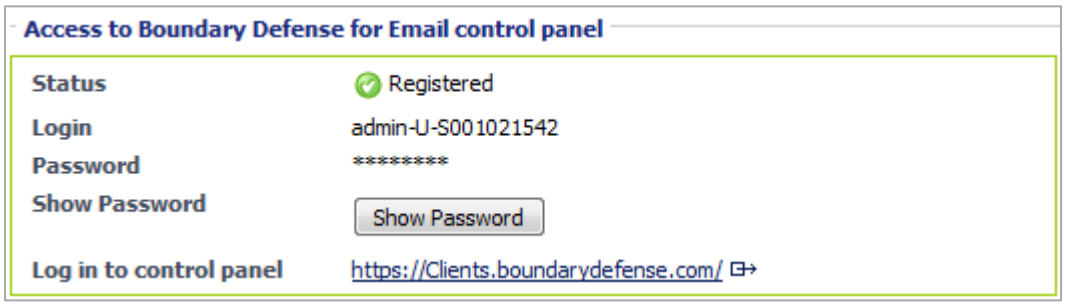
Contents

Description of Policy Based Encryption

The Policy Based Encryption (PBE) service encrypts specific emails based on a data protection policy – that is, a set of rules designed to analyze all email, and encrypt any email that matches the pre-defined conditions. Policy Based Encryption uses the Data Protection rules to identify which email needs to be encrypted.

The Policy Based Encryption Service is managed through the same control panel that you use to manage your Anti-Virus and Anti-Spam settings. This control panel can be accessed through the main Control Panel. Once logged in, click the **Boundary Defense for Email** icon:

Next, log into the Boundary Defense for Email Control Panel:



NOTE: If the password has been changed in the Boundary Defense for Email Control Panel, password will not be synched back to the Control Panel. In this case, that password that is displaying in the Control Panel will not work.

Policy Based Encryption and Email Data Protection

The Policy Based Encryption service is closely integrated with the Email Data Protection service – the policy that filters email is set up in the Email Data Protection Policy configuration screens in the Boundary Defense for Email Control Panel. The Data Protection policy has an action to redirect any emails that meet the rules and conditions to a specified encryption email address.

This email address will be sent to the administrator when the service is purchased. This email address is used solely to process and encrypt the email.

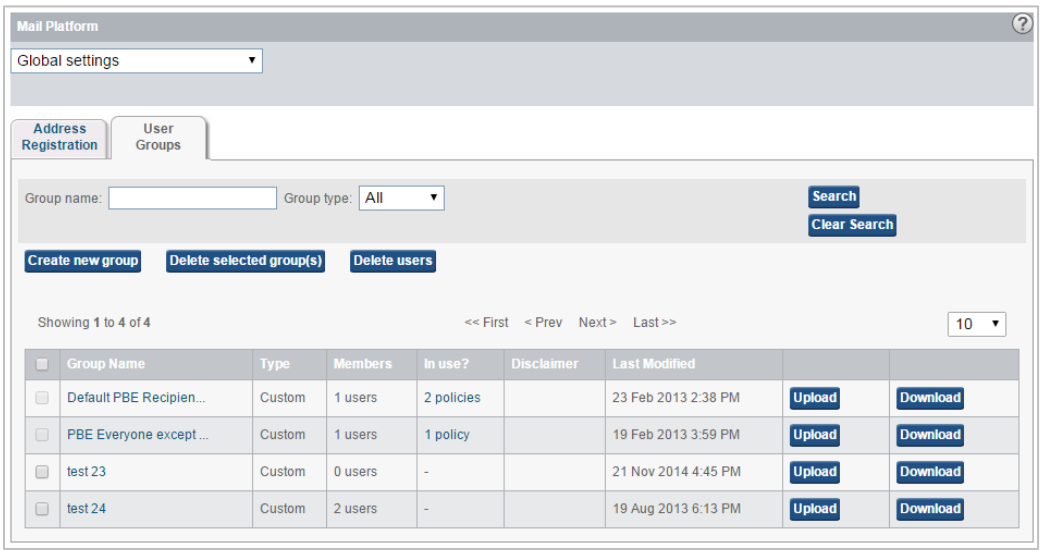
Features Summary

	PBE
Number of recipient languages supported	12
'Best Method Of Delivery' (BMOD)	✓
Encryption strength (-bit)	128
Maximum size of an encrypted email (MB)	50
Maximum number of encrypted emails per user per month	240
Offline reading of emails (possible under certain circumstances)	✓
Support for mobile devices (Blackberry and Windows Mobile 5)	✓
Branding	✓
Configurable password policy	✓
Recipients able to reply securely	✓
Secure portal email expiry time (days)	30
Portal session timeout if inactive (minutes)	10
US Infrastructure	✓
European Infrastructure	✓

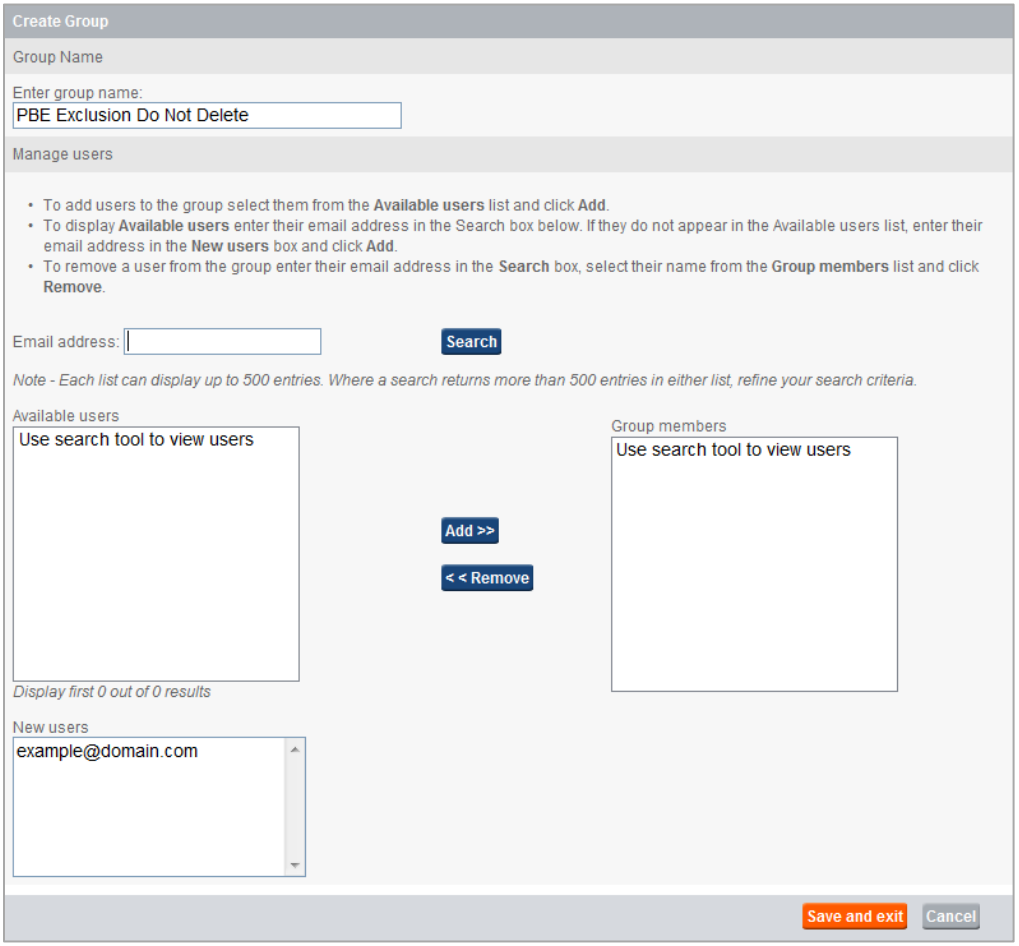
Create an Encryption Group

Prior to creating any data protection policies, an encryption group must be created. This group needs to be added to each rule, as an exception in order for the mail to be forwarded to the Policy Based Encryption Gateway. See below for instructions for adding this group to the encryption rule.

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



2. Then select the **User Groups** tab, and click the **[Create new group]** button.
   The **Create Group** screen displays:



3. Enter the **Group Name**, for example "PBE Exclusion Do Not Delete."
4. Select users from the **Available users** list and click **[Add]** to add them to, and build, the **Group members** list.
5. For new users: in the **New users** field, enter valid email addresses.
6. When your list is complete, click **[Save and exit]**.

Define a Data Protection Policy

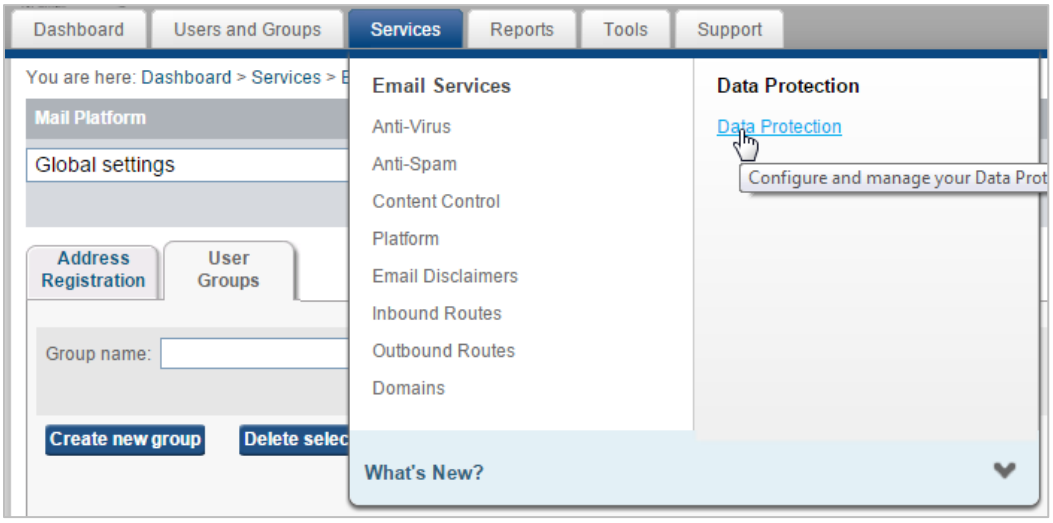
To trigger an email to be encrypted, a Data Protection policy must be defined. The policy specifies an action to redirect the email to a specific email address. The email address depends on the PBE service you use. When you create the policy, define the rules that you want to cause the email to be encrypted. For example, specify a word or phrase that must be contained in the header or body of the email. Then ensure that you inform your users of the word or phrase that must be present to encrypt the email.

Data Protection scans email against the policies in the order they are listed in the portal. If an email triggers a policy with an exit action, it is subject to that action and does not pass on to be scanned for further policies. The redirection action for special PBE policies is an exit action. So it is important to put encryption policies towards the bottom of the policy list, so that other policies defined to comply with the organization's acceptable usage policy are acted on first. If an email triggers a policy with an exit action such as a block action, and that rule is higher in the policy list, the email is not encrypted. The first policy that is encountered blocks the email.

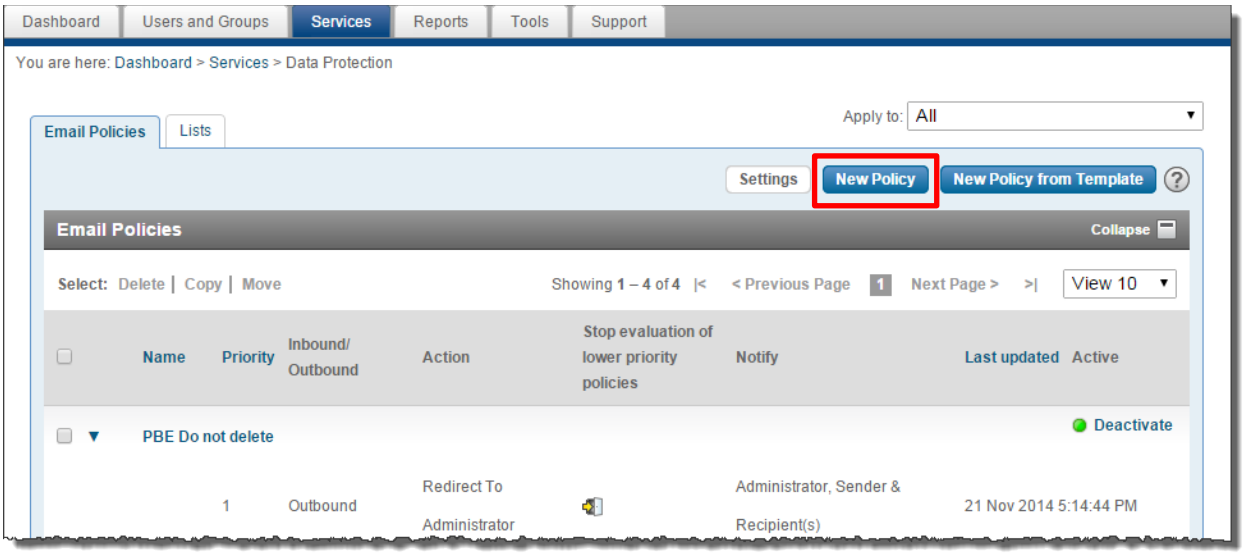
The email address to use to redirect emails to the PBE Email encryption service has been sent to your administrator in the form of a *Welcome* letter.

Create a New Data Protection Policy

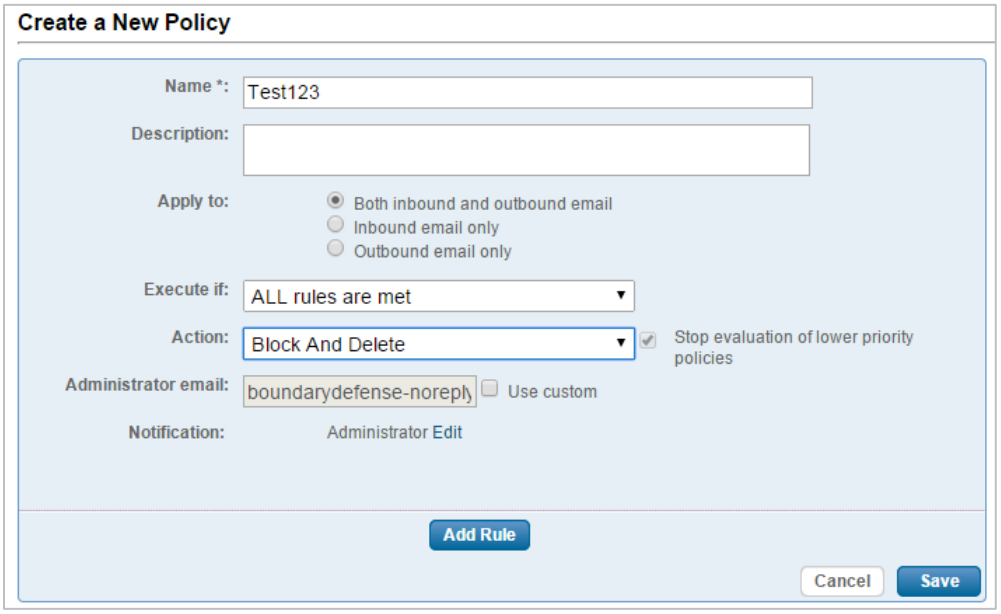
1. Select **Services > Data Protection**.



2. On the **Email Policies** tab, click the **[New Policy]** button:



The **Create a New Policy** screen displays:



3. Give the new policy a **Name** (required) and **Description** (optional).
4. Select **Outbound email only** for encryption (**you can only encrypt outbound email**).
5. Select **All rules are met** or **Any rules are met** from the **Execute if** drop-down.
6. Select **Copy To Administrator** from the **Action** drop-down.
7. Select the **Use custom** check box and enter an appropriate email address for the admin (sent in the *Welcome* letter after purchase).

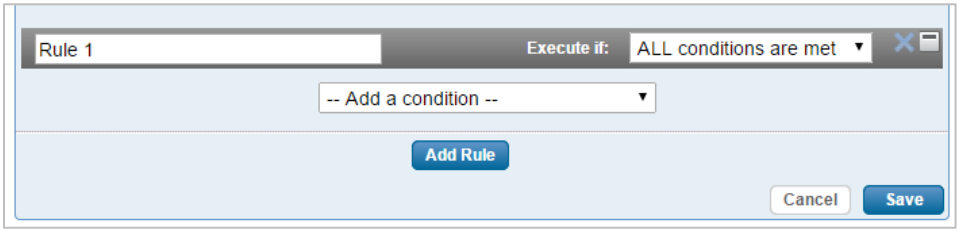
   NOTE: When forwarding a message to the administrator email, it is vital the forwarding email address is correct in the **Administrator email** field. If this address is not correct, mail will not

flow correctly, and will not reach the encryption gateway or the proper recipient.

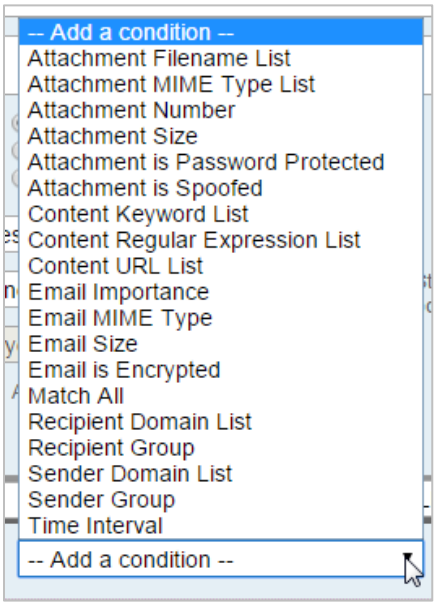
8. Add a rule (or rules) to your new policy (see below).

Add a Rule to the Policy

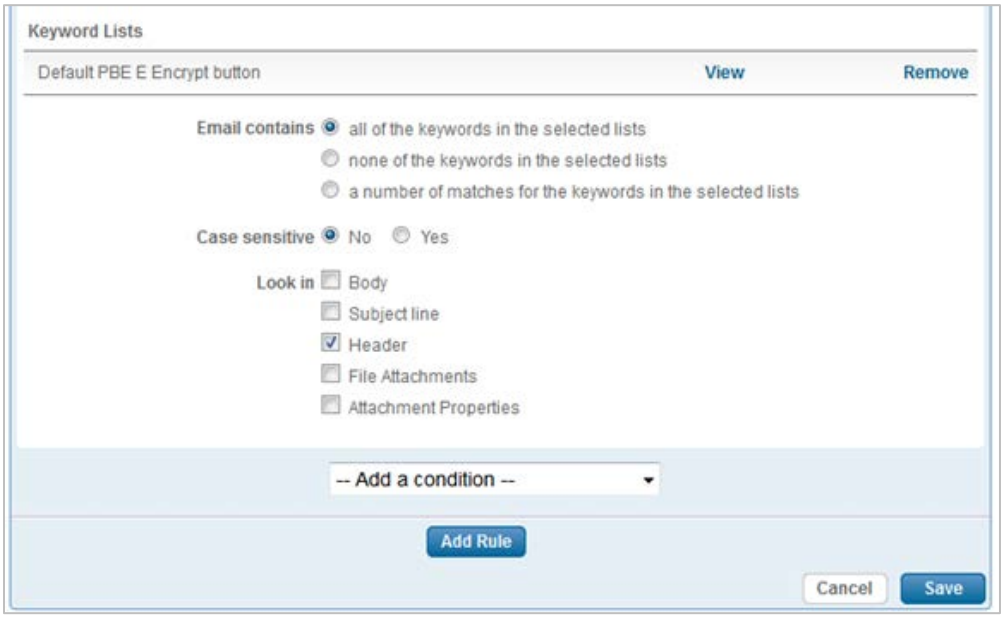
1. Click **[Add Rule]**.
   New fields and options display for creating the rule:



2. Select an **Execute if** option: **ALL conditions are met** or **ANY conditions are met**.
3. Select the **Add a condition** drop-down.



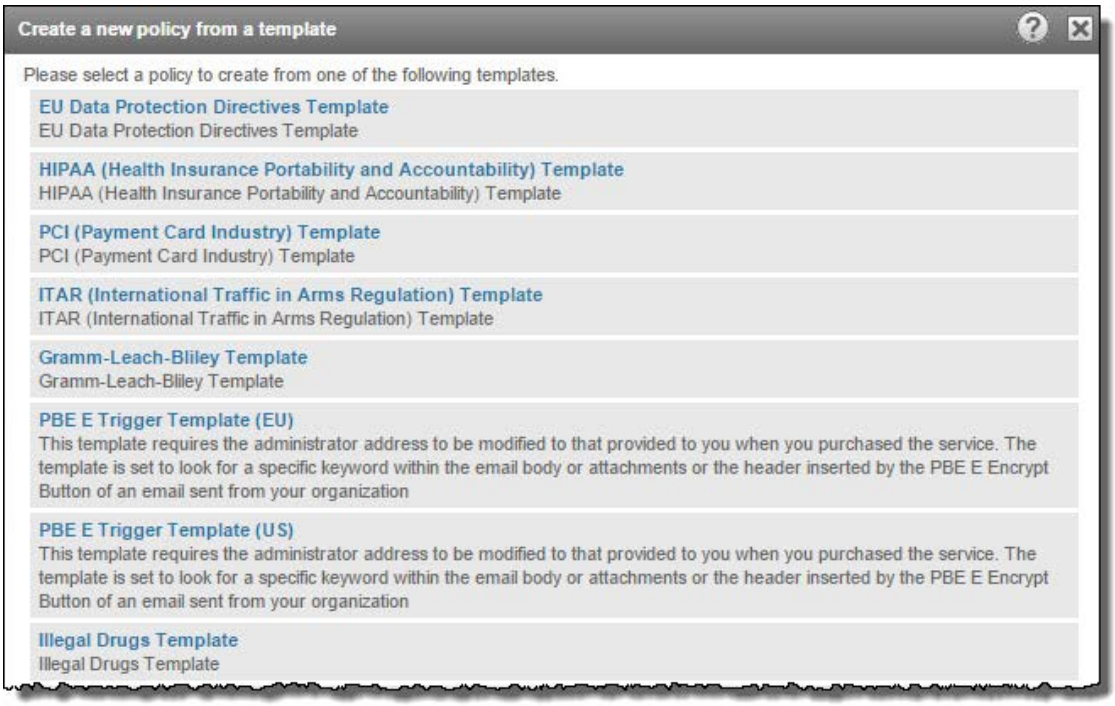
4. Select from the available conditions.
5. If you have additional rules to add to the policy, click **[Add Rule]** and repeat steps 2-4 above. You may add as many new
6. Select **Recipient Group** options and specify a group condition.
   All PBE policies require a recipient group rule to fire. By default, the rule in the template is configured to fire if the message recipient does not match an address in the **Default PBE Recipient Group**, which by default contains "example@domain.com," so as long as "example@domain.com" is not a recipient of the message the rule will always fire. This will work for almost all customers and therefore would rarely need to be modified.



7. Add a keyword list and search parameters in the **Keyword Lists** section.
   NOTE: When setting up filter keywords, it is recommended to review the keywords internally, to ensure they meet the encryption needs of the organization.
8. When complete, click **[Save]**.

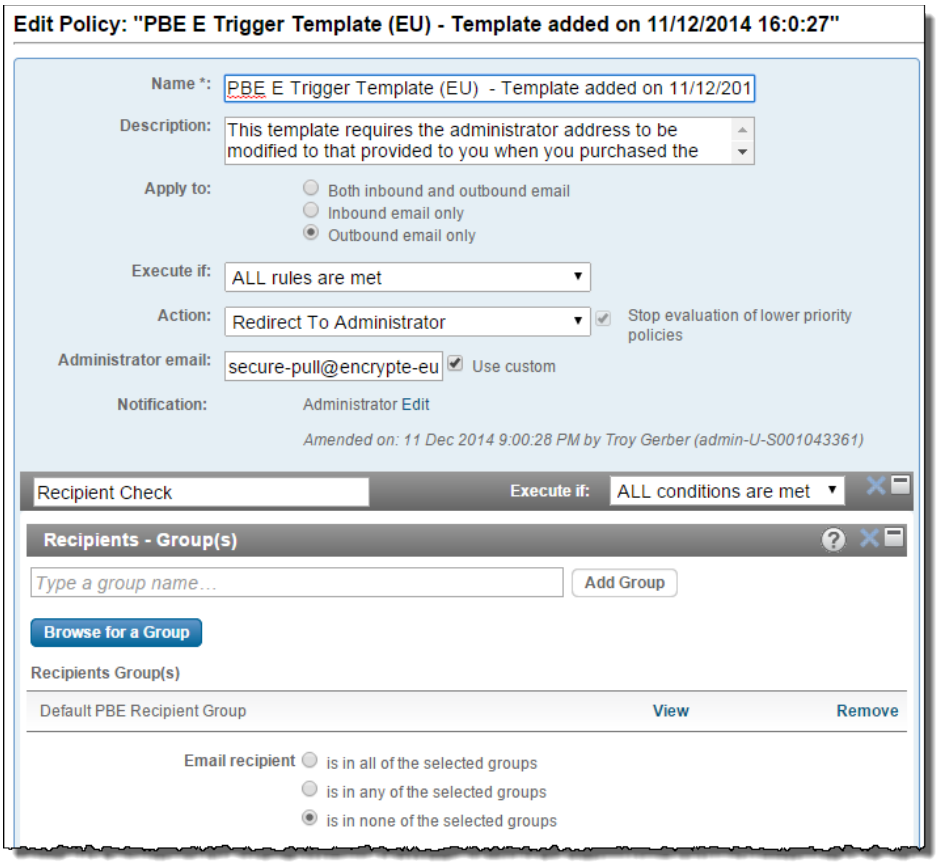
Create a Policy from a Template

1. Select **Services > Data Protection**.
2. On the **Email Policies** tab, click the **[New Policy from Template]** button.
   A list of templates displays:



NOTE: "PBE Z" templates are not available for use.

3. Select the appropriate template from the list and click **[Create]**.
   The new policy from template is created and displays at the bottom of the policies list on the **Email Policies** tab.
4. Select the new policy by clicking the policy name.
   The **Edit Policy** screen displays:



NOTE: The policy will already be applied **Outbound mail** only and the **Action** will be pre-configured to **Redirect to Administrator**.

5. Assuming the correct template was selected, modify the **Administrator email address** so that it is using the appropriate redirect address for your domain (sent in the *Welcome* letter after purchase).
6. The first rule in the template policy is a **Recipient Group** rule; note that all PBE policies require a recipient group rule to fire. By default, the rule in the template is configured to fire if the message recipient does not match an address in the **Default PBE Recipient Group,** which by default contains "example@domain.com," so as long as "example@domain.com" is not a recipient of the message the rule will always fire. This will work for almost all customers and therefore would rarely need to be modified.
7. The PBE templates contain two further rules by default that customers can use to help identify messages containing sensitive data. The first rule looks for common keywords that might be found in messages customers may want to be encrypted.
   Examples of these keywords are **confidential**, **sensitive**, and **encrypt**. The second rule looks for headers that will be found in the message if the sender has flagged the message for encryption using one of the Outlook plug-ins.
   Customers can leave these rules in place or may choose to remove them and create new rules to

help identify messages with sensitive data.

8. Once the policy is finalized, click the **[Save]** button in the bottom right corner of the page.
   Once saved, customers can move the policy to where they would like it positioned in their policy list.
   At this point, the policy can be activated by clicking the **Activate** link in the far right column of the policy. Once activated, a policy will typically be in effect within 30-60 minutes.

Tips & Suggestions

Below are some tips and suggestions for setting up and configuring Policy Based Encryption rules and Data Protection policies:

- It is highly recommended to use a test group before activating rules or policies. This allows you to limit any issues caused by mail flow a rule or policy to only affect a subset of the organization. Once the rule or policy has been tested and proper functionality has been verified, it can be enabled for the entire organization.
- Each customer's encryption requirements are different, so there are no default rules configured initially upon purchase of the service.
- As messages flow through the system, they are filtered according to the order that the rules appear on the screen, from top to bottom. When a message meets the criteria of a rule, the actions of that rule are enforced, and the message will not reach the rules that follow.
- **Policy Based Encryption rules should only be configured for outbound mail.**
- Encrypted messages can be sent to any email user. If the recipient is not a subscriber, he or she will be directed to a secure web portal to access the encrypted message after creating a log-in. If the recipient is a subscriber, the message will be delivered to the recipient's mailbox.
- Policy Based Encryption can be used in conjunction with the Secure Mail encryption client.
- Policy Based Encryption encrypts messages sent via the Outlook client, the OWA web client, or any mobile device.
- If a rule is no longer required, the organization may want to deactivate the rule instead of deleting the rule. The rule will no longer filter messages, but it remains available so that the organization can refer back to the rule or activate it in the future, should the need arise.