Policy Based Encryption E

Administrator Guide

Symantec.cloud™

Policy Based Encryption E Administrator Guide

Documentation version: 1.2

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.

Email or call us	For Support team contact details, log into the portal and navigate to **Support** > **Contact us**.
Open a support ticket	Log into the portal and navigate to **Support** > **Ticketing**. To reduce the time it takes to resolve an issue, before you contact the team refer to the Help on raising support tickets. The Help explains the information that is required for the various types of support issue.
Visit the Online Help	Online Help

We welcome comments and questions about the services and this documentation. Let us know how your service performs. You can also provide suggestions as to how we can support your business needs. Please email us at: helpfeedback.cloud@symantec.com.

We recommend that you check the portal frequently for maintenance information and to learn what's new.

Depending on your organization's setup, you may be able to receive critical service-related issues by text message. Add your mobile number in the **Administration** > **SMS Alerts** section of the portal.

Contents

Chapter 1

About Policy Based Encryption E

This chapter includes the following topics:

Introduction to Policy Based Encryption

Policy Based Encryption encrypts specific emails based on a policy. That is, a set of rules that are designed to analyze all email, and encrypt any email that matches the predefined conditions. Policy Based Encryption uses Content Control rules to identify which email needs to be encrypted. Because most encrypted emails are sent to recipients who are not PBE clients, several delivery methods that enable recipients to read encrypted emails are available.

See "Push or Pull" on page 9.

See "PBE features summary" on page 8.

PBE features summary

The following summary shows some of the features available in the Policy Based Encryption E service:

Table 1-1 Summary of features

Features	PBE E
'Push' delivery	✓
'Pull' delivery	✓
Number of recipient languages supported	12
Third-party Outlook plug-in to create an "Encrypt" button on the toolbar	✓
Third-party OWA extension to create an "Encrypt" button on the toolbar (supports Exchange 2003 and Exchange 2007	✓
Encryption strength (support for standard algorithms, including AES-256 and the use of RSA-1024 bit keys)	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, Windows Mobile 5, and other smartphones)	✓
Branding	✓
Recipients able to reply securely	✓

Table 1-1 Summary of features *(continued)*

Features	PBE E
Secure portal email expiry time (days)	30
Portal session timeout if inactive (minutes)	10
US Infrastructure	✓
European Infrastructure	✓

Push or Pull

The PBE E service has Push and Pull variants of the service.

A push/pull relationship is typically that between a product or piece of information and who is moving it.

In the ‘pull’ delivery method, an email recipient visits the secure email portal website to get access to their encrypted emails. The user has to do something to receive the email.

In contrast, the ‘push’ delivery method pushes messages into the recipient’s email inbox on their computer. The user receives the email without having to do anything.

PBE and Content Control

Policy Based Encryption is closely integrated with Content Control. When an outbound email meets the criteria you define in a Content Control rule, encryption is triggered. The emails that trigger the rule are redirected to a specific email address. This routes the email through the encryption infrastructure and on to the recipient.

To ensure that the email is encrypted, it must match the conditions that trigger the Content Control rule. The email is sent through the encrypted route to the recipient.

You can set up a rule that encrypts all outbound email, or define specific criteria to encrypt only certain emails. The trigger can be a keyword or phrase that the sender types into the body of an email. For example, you can set up a rule that encrypts any emails that include the word ‘Encrypted’. Other triggers for a rule might be that the email contains numbers that appear to be credit card numbers, or particular product or project names.

You may need to communicate the trigger to your PBE users.

The encryption rule must have an action to redirect any emails that meet the rule's conditions to a specified email address. This email address is configured on a subdomain of your organization's domain. The subdomain is used solely for us to process and encrypt the email on the cloud infrastructure.

See "Defining an encryption rule" on page 10.

Defining an encryption rule

To trigger an email to be encrypted, a Content Control rule must be defined. The rule 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 rule (or rules), define the conditions 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.

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

The email address to use to redirect emails to the encryption route are:

Table 1-2 EU and US locations

Location	Administrator email address
EU	secure-pull@encrypte-eu.yourdomain.com
US	secure-pull@encrypte-us.yourdomain.com

To define an encryption rule

1 Select **Services** > **Email Services** > **Content Control**.

2 Click the **Add New Rule** option.

3 Give the rule a name and specify the rule to apply to **Outbound mail**.

4 Specify the conditions that you want to cause email to be encrypted. For example, you may want to encrypt all emails that contain characters that match the credit card number template, or all emails that contain specific words.

5 In the **Recipients** tab, specify a user group condition. Note the following:

- All encryption rules must specify a recipient user group condition.
- To encrypt emails that are sent by anyone in the organization, create a user group called 'PBE All', for example. Populate the group with a single non-valid email address such as example@domain.com. Then select the option **All recipients EXCEPT those in selected groups**. The rule is applied to all of your users. So all emails trigger the rule and are therefore encrypted.
- If a domain list is also specified as a recipient, in the **Rule conditions** section, you must select **All the conditions below need to be satisfied...**

6 In the **Actions & Notifications** tab, select the action to **Redirect to administrator** from the drop-down list, and check the **Use Custom Email address** box.

In the **Administrator's email address** box, enter the PBE-specific email address for your domains. For the correct email address to use for your datacenter location and the required delivery method, refer to the table above:

- EU and US locations

Deploying Policy Based Encryption

Deployment and implementation of Policy Based Encryption can take several weeks because of the different options available and the branding requirements.

The subdomains you deploy the service to, must be registered with, and point to us.

Caution: If you already use the Boundary Encryption service, the service mode must change to 'Secure Connect'. Email between you and us must be enforced over TLS exclusively. The Secure Connect service mode does not change any existing domain-to-domain Boundary Encryption enforcements. Arrangements to change to the 'Secure Connect' mode, are made at a mutually convenient time. Changing to Secure Connect is an essential step. Failure to make this change may result in a mail outage.

The following procedure provides the steps that are required to deploy the service. Your sales contact or Client Services representative will be pleased to go through this procedure with you.

To deploy Policy Based Encryption

1. Obtain the Policy Based Encryption (PBE) Provisioning Form, available from your sales contact.
2. If you do not already use the Boundary Encryption (BE) service, obtain the BE Provisioning Form, available from your sales contact.
3. Complete the provisioning forms. Then liaise with Client Services to ensure that we have the necessary information to provision the PBE, Content Control, and Boundary Encryption services, as necessary.

   Provide the appropriate graphics files and other details for your branding. Send these to use with your contract and Provisioning Forms. Details about the files and information that are required for branding are included in the Policy Based Encryption provisioning form. If the branding JPGs are not included with the completed provisioning forms, deployment may be delayed.
4. Ensure that the appropriate subdomains for all domains to use the PBE service are registered.

   The subdomains that are required are as follows, depending on whether you are provisioned on the US or Europe infrastructure:

US	`encrypte-us.yourdomain.com`
Europe	`encrypte-eu.yourdomain.com`

5. Ensure that all the subdomains point to the correct cloud infrastructure. Client Services can supply you with these details.
6. Do one of the following:
   - If you already use the Boundary Encryption service, ensure that you have worked with us to ensure that the email between you and us is enforced over TLS.
   - If you do not already use Boundary Encryption, when you are ready to enable TLS, a Client Services representative will run tests to ensure that your mail servers can establish TLS connections.
7. Do one of the following:
   - If no TLS errors are shown, the deployment can continue.

- If the TLS tests are unsuccessful, the problems must be resolved for the deployment to continue. Client Services will advise you on resolving any problems. If they cannot resolve the issues, a call is with the Engineering Support Team on your behalf.

When the steps are completed successfully, Policy Based Encryption can be deployed. Client Services will confirm when the service is successfully deployed. Typically, this is within two weeks. You can then configure and test the service to ensure that it operates as expected.

Managing PBE E credentials

The Credentials Management section of the Encrypted Mail Gateway (EMG) console is used to add third-party credentials for decryption and certificates for encryption. When messages are sent through the Encrypted Mail Gateway for encryption or decryption, it first checks for any credentials that have been uploaded to the Credentials Management page.

Private keys can be uploaded to the **Credentials Management** page and then used to automatically decrypt email messages.

Certificates can be uploaded to the **Credentials Management** page and then mapped to a specific domain or email address:

- *By Domain*: If you upload a certificate and then map it to a domain (e.g., ‘bankabc.com’), all email messages that match that domain (i.e., ‘bankabc.com) are encrypted using the uploaded certificate.
- *By Email Address*: If you upload a certificate and then map it to an email address (e.g., ‘jim@bankabc.com’), all email messages that match that email address (i.e., ‘jim@bankabc.com’) are encrypted using the uploaded certificate.

Viewing credentials management	See “To view credential management” on page 14.
Adding a private key	See “To add a private key” on page 14.
Downloading a private key	See “To download an existing private key” on page 14.
Removing a private key	See “To remove a private key” on page 14.
Adding a certificate	See “To add a certificate” on page 14.
Downloading a certificate	See “To download an existing certificate” on page 15.
Removing a certificate	See “To remove a certificate” on page 15.

To view credential management

1. Log on to the EMG Console.
2. Click **Default Profile Management** or select a profile from the drop-down menu and click **Continue**.
3. From the **Encrypted Mail Gateway Console** home page, click **Manage Credentials**.

   The **Profile Settings** page appears.

To add a private key

1. From the **Credentials Management** page, click **Add Private Key**.
2. For the **Credential File** field, enter the path to the private key or click **Browse** and select the appropriate private key (*.P12 or *.PFX) file.
3. For the **CN** field, enter the email address that is associated with the private key.
4. For the **Password** field, enter the password for the private key.
5. For **Credential Type**, select whether the key is S/MIME or PGP.
6. Click **OK**. The private key appears in the **Private Key** list.

To download an existing private key

1. From the **Credentials Management** page, click **Download** next to the private key you want to download. A **File Download** prompt appears.
2. Click **Save** and then select a location to save the private key.
3. Click **Save**. The private key is downloaded locally.

To remove a private key

1. From the **Credentials Management** page, click **Remove** next to the private key you want to remove. A confirmation prompt appears.
2. Click **OK** to permanently delete the private key.

To add a certificate

1. From the **Credentials Management** page, click **Add Certificate**.
2. For the **Credential File** field, enter the path to the certificate or click **Browse** and select the appropriate certificate (a PEM-formatted certificate; e.g., *.CER or *.PEM) file.
3. For the **Email/Domain** field, enter the appropriate email address or domain.
4. Select **Email** (if you entered an email address in Step 3) or **Domain** (if you entered a domain in Step 3).

5 For **Credential Type**, select whether the key is S/MIME or PGP.

6 Click **OK**. The certificate appears in the **Certificate** list.

To download an existing certificate

1 From the **Credentials Management** page, click **Download** next to the certificate you want to download. A **File Download** prompt appears.

2 Click **Save** and then select a location to save the private key.

3 Click **Save**. The certificate is downloaded locally.

To remove a certificate

1 From the **Credentials Management** page, click **Remove** next to the certificate you want to remove. A confirmation prompt appears.

2 Click **OK** to permanently delete the certificate.

FAQs about Policy Based Encryption

The following frequently asked questions provide further information about Policy Based Encryption.

Table 1-3 FAQs

Question	Answer
Is an email encrypted on its way to the Email Services infrastructure?	Yes. Policy Based Encryption intervenes in the method by which an email gets from the sender to the recipient. Mail cannot be identified as requiring to be encrypted until it is scanned by the Content Control service. When an email triggers a Content Control encryption rule, it is encrypted in its journey from you to us, using the Boundary Encryption service's 'Secure Connect' feature.
Is there a maximum size for an email that can be sent using Policy Based Encryption?	Yes. The maximum size of an encrypted email is 50MB.
Will an encrypted email be available indefinitely?	When using the pull methodology, emails are not retained indefinitely. Messages expire and are no longer available after the configured time. If a user needs to access emails after this time, their content must have been printed or copied into another format before expiry. Expired emails cannot be retrieved. Emails that are sent using the push method are available until deleted. They are stored in the recipient's email system.

Table 1-3 FAQs *(continued)*

Question	Answer
Is there a limit on how many emails a user can send using Policy Based Encryption?	Yes. The maximum number of encrypted emails per user per month is 240.
By following a link in a notification email, are users exposing themselves to a phishing risk?	A third party on the Internet can generate an email that looks like an encrypted message notification. Such a message can contain a URL that leads to a Web site that looks like the secure email portal, but which is hosted by the malicious party. The perpetrator can then acquire the user's logon credentials, and use them to read encrypted emails using the genuine secure email portal. To avoid this, check the portal's URL. The URL for the secure email portal always appears in the format `https://securemail#.messagelabs.com` , where # represents a number, for example `https://securemail5.messagelabs.com` In addition, the Email Services Skeptic ® engine is tuned to detect phishing of PBE, and we recommend that all Policy Based Encryption clients have the cloud AntiVirus service enabled.
Is Policy Based Encryption capable of non-Latin-based language support?	Yes. To ensure that PBE supports non-Latin-based languages, users should set their email client to encode emails using UTF-8. To set Microsoft Outlook to encode emails using UTF-8: 1 Uncheck **Auto select encoding for outgoing messages** 2 Select **Tools** > **Options** > **Mail Format** > **International Options** 3 Set **Preferred encoding for outgoing messages** to **Unicode [UTF-8]**
Does an email that an Administrator sends, bypass encryption?	Yes. The PBE service does not intercept any emails that an administrator sends—to avoid rules blocking Administrator emails. We recommend that administrators use a special email address (e.g. ccadmin@exampledomain.com) for administrative purposes, instead of their own personal email address. Then all emails that are sent from the personal email address can be encrypted when they trigger the encryption rule, as normal.

Table 1-3 FAQs *(continued)*

Question	Answer
Does the order of Content Control rules make any difference to how Policy Based Encryption works?	Yes. Content Control scans emails for each rule in order. When an email triggers a rule with an exit action, such as the redirection to an email address that is used in Policy Based Encryption, the email is not scanned for any further rules. Put encryption rules towards the bottom of the rule set, so that any other rules relevant are acted on first. If there is an applicable rule that runs an exit action higher in the rule set, the email may not be encrypted.
Does the use of Policy Based Encryption affect the use of any other Email Services?	Yes. Policy Based Encryption cannot be used alongside the Message Manager facility. When a message is released from Message Manager's quarantine, it can mean that it is delivered without being encrypted. For this reason, a client using Message Manager cannot be provisioned with Policy Based Encryption.
The sender of a sensitive email wants to ensure that it is encrypted at the touch of a button. Is this possible?	Yes, for Outlook users. An Add-In for Outlook has been developed to complement the PBE E service. The Add-In puts an Encrypt option in the Outlook toolbar when an email is composed. The Add-In can be downloaded from the following site:

Policy Based Encryption user tasks

This chapter includes the following topics:

Composing an outbound email

To compose an outbound email, a user in your organization creates an email in the normal way using your email client software.

To ensure that the email is encrypted, it must contain the content that triggers the Content Control rule that sends the email through the encrypted route to the recipient.

See "PBE and Content Control" on page 9.

External users composing an encrypted email to your organization

When an external user has received an encrypted email from someone in your organization, they then have credentials to access the secure email portal Web site. They can compose an encrypted email to your organization, which is not in reply to an email you have sent.

To compose an encrypted email to a user in your organization

1. The user logs on to the secure email portal, using the email address and password that they set up when they received the email from your organization.
2. They select the **Compose** tab.
3. Next they enter the appropriate email address, enter the text, and select **Send**.

Receiving an outbound email with Pull

For recipients who receive email from your users, the method of delivery depends on the variant of Policy Based Encryption that you use.

‘Pull’ is when a user acts to retrieve their encrypted emails. The recipient logs on to a secure Web-based email portal to read a ‘pulled’ email.

Process for mail delivery:

- Email is passed to the cloud infrastructure from the customer using Boundary Encryption’s Secure Connect feature.
- We pass the email to the encryption server using Boundary Encryption.
- We send a plain text notification email to the recipient.
- The recipient uses a Web browser to read the email securely (over HTTPS).

Receiving an email

1. The user receives a notification email. Click on the link to view the encrypted email.
2. The expiry date for the secure message is typically 14 days to 30 days after the notification is sent. After that date the email is no longer available.
3. At the secure email portal logon prompt, the recipient enters their email address and password.
4. The encrypted email appears on screen

See “Receiving an outbound email with Push” on page 20.

Receiving an outbound email with Push

For recipients who receive email from your users, the method of delivery depends on the variant of Policy Based Encryption that you use.

'Push' is when information is sent direct to a user over the Internet, without them having to request it specifically. In Policy Based Encryption, a 'pushed' email is delivered direct to the recipient's email inbox. The user can then view and reply to a message using Encrypted Mail Reader—a small, downloadable application for viewing secure messages. The user is instructed to download the Encrypted Mail Reader when they receive their first encrypted message.

Before a user can use the Push feature, they must enable it within the Web portal .

To enable Push

1 Log on to the Web portal .

2 In the **Options** tab, click the **Change My Delivery Method** link.

3 Click the link: **click here to complete the Encrypted Mail Reader registration form**.

4 Review your registration information and click **Yes**.

The user's existing encrypted messages and future encrypted messages will be sent to their email address and they will receive an email notification with instructions on how to download and install Encrypted Mail Reader.

Process for mail delivery:

- The recipient of an encrypted email receives a readable email in their inbox, with an attachment. The attachment contains the encrypted email.
- When the user opens the attachment, they are asked for their Secure ID password. The mechanism for decrypting the email relies on there being a connection to the key server. Even if the user has saved the encrypted attachment to their computer, they cannot read the encrypted email when not connected to the Internet (offline).
- After the user enters the correct password or logon details, they can read the email and its attachments. When the user closes the encrypted email, it remains in their email system in its encrypted form. The password or logon details are required to open it again.
- The user can send an encrypted reply to the sender directly from Encrypted Mail Reader. A copy of the reply is saved locally in encrypted form.

See "Receiving an outbound email with Pull" on page 20.

Receiving an inbound email

An email that is received from another user in the organization using PBE, or from another PBE client, is delivered in a readable form to the recipient's email inbox. It is encrypted throughout its journey to your email server. An inbound email may have been sent from the secure Web-based email portal or directly from the email client.

Recovering from a forgotten password

If a user forgets their password, they can request a new one.

To receive a new password

1. Open the Web portal logon page.
2. Click the **Forgot your password?** link.
3. In the **Email Address** field, enter the email address that is associated with the account.
4. Click **Next**.

   A message is sent to their personal email address with a new password.