![Barracuda. Your journey, secured.]

How to Use DLP and Outbound Mail Encryption

https://campus.barracuda.com/doc/96022961/

> If you make setting changes, allow a few minutes for the changes to take effect.
>
> This article assumes you have completed the initial service set up and configured outbound mail scanning.

For health care providers, governmental agencies, and other entities who need to protect private, sensitive, and valuable information communicated via email, Email Gateway Defense provides Data Leak Prevention (DLP) features using email encryption. DLP enables your organization to satisfy email compliance filtering for corporate policies and government regulations such as HIPAA and Sarbanes-Oxley (SOX). Advanced content scanning is applied for keywords inside commonly used text attachments, as well as email encryption. You can configure email encryption policies per domain.

Outbound Mail Encryption

> Note that sending encrypted emails from an email address containing a + sign in the user-portion of the email (also known as plus addressing or subaddressing) is not supported. For example, `<name>+<tag>@company.com`.

Encryption is performed by the Barracuda Email Encryption Service, which also provides a web interface, the Barracuda Message Center, for recipients to retrieve encrypted messages.

Figure 1: Mail Flow for Encrypted messages sent through Email Gateway Defense
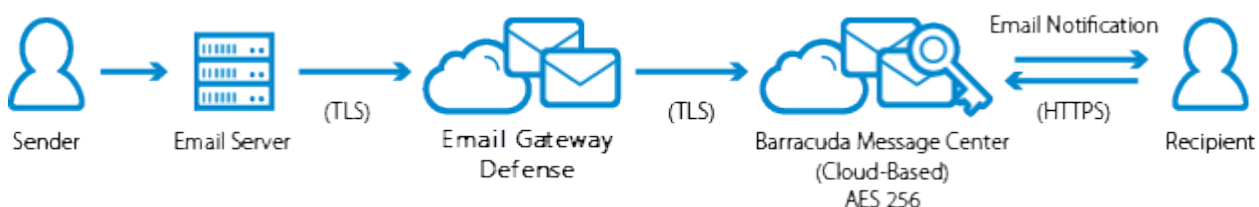
> **Encryption Privacy**
>
> When the Barracuda Email Encryption Service encrypts the contents of a message, the *message body does not display* in the **Message Log**. Only the sender of the encrypted message(s) and the recipient can view the body of an encrypted message. For more information about privacy, see the Barracuda Networks Privacy Policy.

Secure Sensitive Message Transmission

TLS or Transport Layer Security is used to encrypt the communication channels for both inbound and outbound mail. By default, use of TLS is opportunistic - a TLS connection will first be attempted; if unsuccessful, the connection will revert to plain text (unencrypted).

Email Gateway Defense provides capabilities to require TLS connections to and from certain domains, or in certain cases, ALL communication. Connections that require TLS, and fail to do so, will be rejected.

For more information on how to configure these policies, see Configuring Secure Message Transmission.

Define when to Encrypt Messages

Use the **Outbound Settings > Content Policies** page to create policies for encryption of outbound message in one or both sections:

- **Message Content Filters** – Select the **Encrypt** action for outbound email based on characteristics of the message's subject, header, body, attachments, sender, or recipient. You can specify simple words or phrases, or use Regular Expressions. Content filtering is NOT case sensitive. Select **Do not encrypt** to exempt messages, based on the content, from the outbound encryption policy.
- **Predefined Filters** – Select the **Encrypt** action for outbound email messages that contain matches to pre-made patterns in the subject line, headers, message body, or attachment. Use the following pre-defined data leakage patterns (specific to U.S.) to meet HIPAA and other email security regulations:
    - **Credit Cards** – Messages sent through Email Gateway Defense containing recognizable Master Card, Visa, American Express, Diners Club or Discover card numbers will be subject to the action you choose.
    - **Social Security** – Messages sent with valid social security numbers will be subject to the action you choose. U.S. Social Security Numbers (SSN) must be entered in the format nnn-nn-nnnn or nnn nn nnnn .
    - **Privacy** – Messages will be subject to the action you choose if they contain two or more of the following data types, using common U.S. data patterns only: credit cards (including Japanese Credit Bureau), expiration date, date of birth, Social Security number, driver's license number, street address, or phone number.
        - Phone numbers must be entered in one of the following formats:
            - nnn-nnn-nnnn
            - (nnn)nnn-nnnn

- nnn.nnn.nnnn
  - Street address must be an exact match and should not contain any special characters such as periods (.) or commas (,). For example, enter `123 Main St` instead of `123 Main St., Town, State`.
- **HIPAA** – Messages will be subject to the action you choose if they contain TWO of the types of items as described in Privacy above and ONE medical term, or ONE Privacy item, ONE Address and ONE medical term. A street address can take the place of Privacy patterns. So, for example, a U.S. Social Security Number (SSN), an address, and one medical term is enough to trigger the HIPAA filter.

The format of this data varies depending on the country, and these filters are more commonly used in the United States; they do not apply to other locales. Because of the millions of ways that any of the above information can be formatted, a determined person will likely be able to find a way to defeat the patterns used. These filter options are no match for educating employees about what is and is not permissible to transmit via unencrypted email.

Order of Precedence for Attachment Filters, Message Content Filters, and Predefined Filters

The Attachment Filters, Message Content Filters, and Predefined Filters support the following actions, in the following order of precedence:

Order	Filter	Action
1	Message Content Filter	Allow
2	Message Content Filter	Block
3	Predefined Filter	Block
4	Attachment Filter	Block
5	Attachment Filter	Quarantine
6	Message Content Filter	Quarantine
7	Predefined Filter	Quarantine
8	Message Content Filter	Do not encrypt
9	Message Content Filter	Encrypt
10	Predefined Filter	Encrypt

Note that when you select **Do not encrypt** on a **Message Content Filter** and **Encrypt** on a **Predefined Filter**, the Message Content Filter exemption takes precedence over the Predefined Filter and the message will not be encrypted.

Mail sent via the Email Protection Add-In and configured to be encrypted follow the same precedence as documented above. For example, when you select a **Block** and **Encrypt** on a **Message Content Filter**, the Block takes precedence and the message will be blocked.
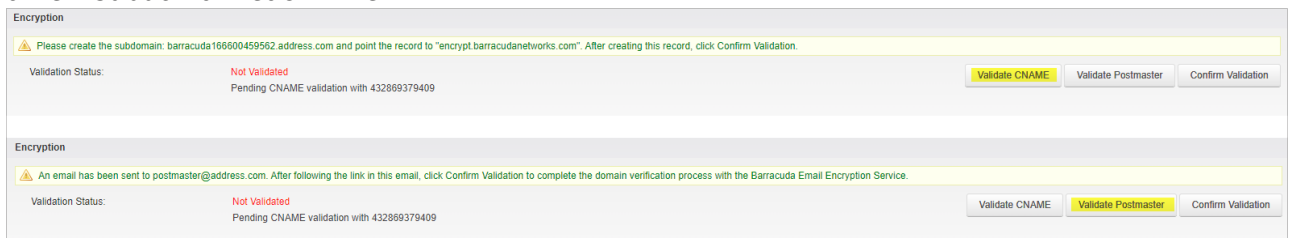
Click **Help** on the **Outbound Settings > Content Policies** page in the Email Gateway Defense web interface for more details.

Validate Your Domain

Note: Validating your domain is not required to use the email encryption capabilities. Additional encryption customization options can be unlocked by validating your domain.

Validate your domain via a CNAME record or send an email to your postmaster address.

1. Under the **Domains** tab, click **Edit** on the domain you use to send email.
2. Scroll down to the **Encryption** section.
3. You will see **Validation Status: Not Validated**.
4. Click **Validate CNAME** or **Validate Postmaster** and follow the instructions in the popup banner to validate your domain. **Note** that clicking **Validate CNAME** multiple times will create a new subdomain each time.

Encryption				
⚠ Please create the subdomain: barracuda166600459562.address.com and point the record to "encrypt.barracudanetworks.com". After creating this record, click Confirm Validation.				
Validation Status:	Not Validated Pending CNAME validation with 432869379409	Validate CNAME	Validate Postmaster	Confirm Validation

Encryption				
⚠ An email has been sent to postmaster@address.com. After following the link in this email, click Confirm Validation to complete the domain verification process with the Barracuda Email Encryption Service.				
Validation Status:	Not Validated Pending CNAME validation with 432869379409	Validate CNAME	Validate Postmaster	Confirm Validation

5. Click **Confirm Validation**.

Once your domain is validated, you can now:

- Add your company logo to the notification message to recipients. Recommended size is 160 x 65 pixels.
- Allow Replies - Allows recipient to reply to messages.
- Enable Read Receipts - Sends a read receipt email to the sender notifying that the recipient has read the message.
  Example read receipt:

- Customize the subject of the notification message.
- Customize the text in the body of the notification message.

Encryption Notification Placeholders

Use the following placeholders in your encryption notification template email:

- **%subject%** – The subject
- **%sender%** – The sender
- **%senderdomain%** – The sender's domain
- **%recipient%** – The encrypted mail recipient
- **%link%** – The Barracuda Message Center link. For example: Click here
- **%logo%** – Your logo image. For example: <img src=%logo%>
- **%displayname%** – The Domain Display Name set for this domain.

Send and Receive Encrypted Messages

The **Barracuda Message Center** is a web-based email client for receiving and managing encrypted email sent by Email Gateway Defense. The email client looks and behaves much like any web-based email program (see Figure 2). For a user's guide, see the Barracuda Message Center User's Guide. The workflow for sending and receiving encrypted messages is as follows:

1. Outbound messages that meet the filtering criteria and policies configured as described above are encrypted and appear in the **Message Log**, but the message body does not appear in the log for security purposes.
2. The Barracuda Message Center sends an email notification to the recipient including a link the recipient can click to view and retrieve the message from the Barracuda Message Center.

3. The first time the recipient clicks this link, the Barracuda Message Center prompts them to create a password.

4. The recipient logs into the Barracuda Message Center and is presented with a list of email messages. All encrypted messages received appear in this list for a finite retention period or until deleted by the recipient.

Figure 2: Barracuda Message Center web interface
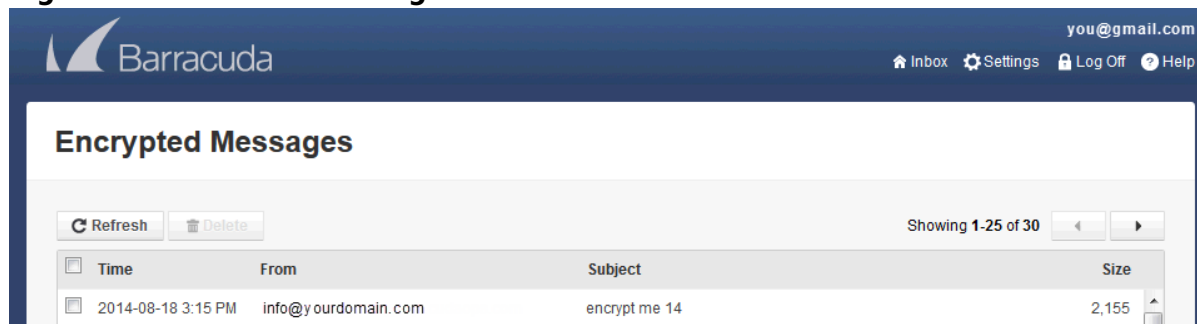
If enabled, recipients of encrypted messages can respond to the sender via the Barracuda Message Center. The new recipient (original sender) will now receive a notification letting senders know about the new encrypted message.

Figures

1. EncryptionDiagram1.png
2. validateCnameOrPostmaster.png
3. readreceipt_email.png
4. EncryptedMessagesBMC.png