How to Use DLP and Outbound Mail Encryption

https://campus.barracuda.com/doc/3211265/

> 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, the Barracuda Email Security Service 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

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 the Barracuda Email Security Service.
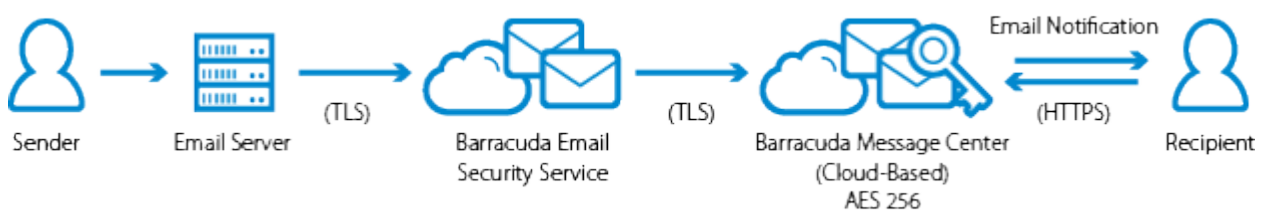
> **Encryption Privacy**
>
> When the Barracuda Email Encryption Service encrypts the contents of a message, the *message body does not display* in the **Message Log**. Only the sender of the encrypted message(s) and the recipient can view the body of an encrypted message. For more information about privacy, see the Barracuda Networks Privacy Policy.

Secure Sensitive Message Transmission

TLS provides secure transmission of email content, both inbound and outbound, over an encrypted channel using the Secure Sockets Layer (SSL) - also known as TLS. For DLP, you should require mail to be sent *outbound* from the Barracuda Email Security Service over a TLS connection. To do so, enable **Force TLS** for each domain on the **Outbound Settings > DLP/Encryption** page. Mail sent to these domains must be transmitted across a TLS connection. If a TLS connection can not be established, then the mail will not be delivered. See also [Secured 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 or body. You can specify simple words or phrases, or use [Regular Expressions](#). Content filtering is 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, 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 the Barracuda Email Security Service 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`
    - **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.

Click **Help** on the **Outbound Settings > Content Policies** page in the Barracuda Email Security Service web interface for more details.
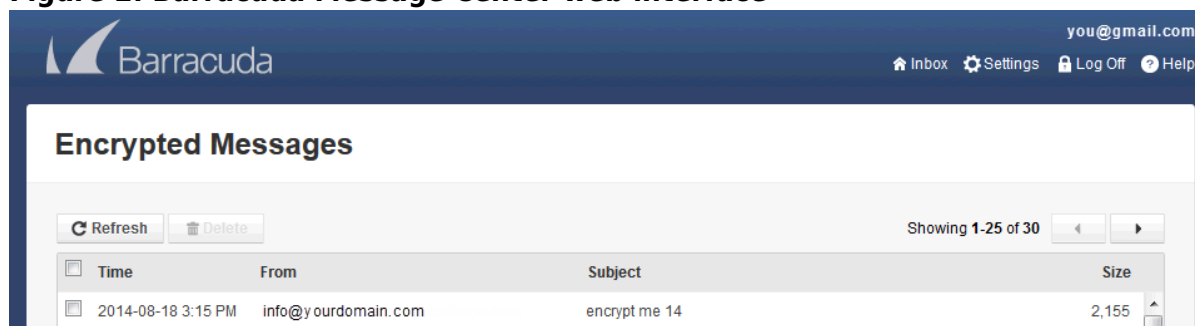
Send and Receive Encrypted Messages

The **Barracuda Message Center** is a web-based email client for receiving and managing encrypted email sent by the Barracuda Email Security Service. 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

Senders have the option to allow replies from recipients to be sent from the Barracuda Message Center. When the recipient replies to the encrypted email message, the response is also encrypted and the sender receives a notification that includes a link to view and retrieve the message from the Barracuda Message Center.

Senders can also enable read receipt to be sent from the Barracuda Message Center so senders know when a message has been read.

An example read receipt email sent to the sender that the recipient has read the message.

From: "noreply@barracuda.com" <noreply@barracuda.com>
Date: Thursday, September 24, 2020 at 5:12 PM
To:
Subject: Your encrypted message has been read by

Your encrypted message has been read.

has read your email message that has been encrypted for privacy and security by the Barracuda Email Encryption Service.

Disclaimer: This email is confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender.

Figures

1. EncryptionDiagram.png
2. EncryptedMessagesBMC.png
3. readreceipts.png
4. readreceipt_email.png