

Secured Message Transmission

<https://campus.barracuda.com/doc/96022962/>

If you make setting changes, allow a few minutes for the changes to take effect.

To prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies, Email Gateway Defense provides several types of encryption for inbound and outbound message traffic.

Send Messages Over an Encrypted Channel

TLS provides secure transmission of email content, both inbound and outbound, over an encrypted channel using the Secure Sockets Layer (SSL).

Note that the maximum number of entries that can be added for each policy is 2500.

Outbound

To require mail to be sent *outbound* from Email Gateway Defense over a TLS connection, use the **Outbound Settings > DLP/Encryption** page. If a TLS connection cannot be established, mail will not be delivered.

Select one of the following:

- **Use TLS connection for all outbound messages** – Require a TLS connection to all domains. To exempt a recipient domain, enter the exempted recipient domain one at a time and click **Add**, or use the **Bulk Edit** button.
- **Use TLS connection for select recipient domains** – Require a TLS connection to certain recipient domains. Enter the recipient domain one at a time and click **Add**, or use the **Bulk Edit** button.

Inbound

To require mail coming *inbound* to Email Gateway Defense to use a TLS connection, use the **SMTP Encryption** section on the **Domains > Edit Settings** page. If a TLS connection cannot be established, mail will not be delivered.

- Select **Required** for **Use TLS from Barracuda Networks to your mail server(s)** to send inbound mail over a TLS connection if TLS is available on your organization's mail server. If TLS

is not available, mail is sent in cleartext.

- For **Require TLS to Barracuda Networks from these domains**, select one of the following:
 - **All inbound messages** – Require a TLS connection from all domains. To exempt a sender domain, enter the exempted sender domain one at a time and click **Add**, or use the **Bulk Edit** button.
 - **Select sender domains** – Require a TLS connection from certain sender domains. Enter the sender domain one at a time and click **Add**, or use the **Bulk Edit** button.

Outbound Mail Encryption

For guaranteed message encryption and ensured delivery of outbound messages, use the **Barracuda Message Center** to encrypt the contents of certain outbound messages. You can create policies for when to encrypt outbound messages on the **Outbound Settings > Content Policies** page for a domain. For details about using encryption with the Barracuda Message Center, see [How to Use Encryption of Outbound Mail](#). For end-users, see the [Barracuda Message Center User's Guide](#).

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.