

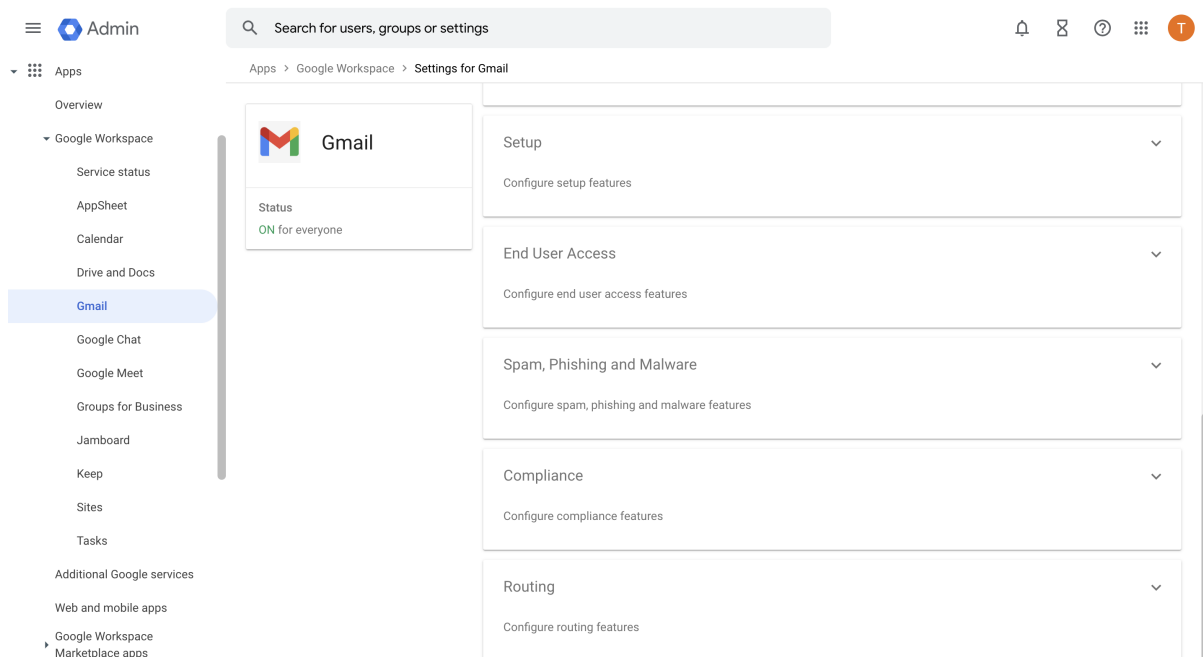
How to Configure Google Workspace for Inbound and Outbound Mail

<https://campus.barracuda.com/doc/3866650/>

This article addresses configuring Google Workspace Business and Education editions with the Barracuda Email Security Gateway as your inbound and/or outbound mail gateway.

Inbound Configuration

1. Log into the Google Workspace admin console at <https://admin.google.com>.
2. From the **Home** page, go to **Apps > Google Workspace > Gmail**. From the **Home** page, go to **Apps > Google Workspace > Gmail > Spam, Phishing, and Malware**.



3. Scroll to the **Inbound gateway** section and, on the right, click **Enable**, and then click **Edit**.
4. In the **Gateway IPs** section, under **IP Addresses / Ranges**, enter the public IP addresses of the Barracuda Spam Email Security Gateway(s), specifying either a block of addresses or individual IP addresses.
5. Select the following options:
 1. **Automatically detect external IP (recommended)**
 2. **Reject all mail not from gateway IPs.** MAKE SURE TO CHECK THIS BOX. All other mail

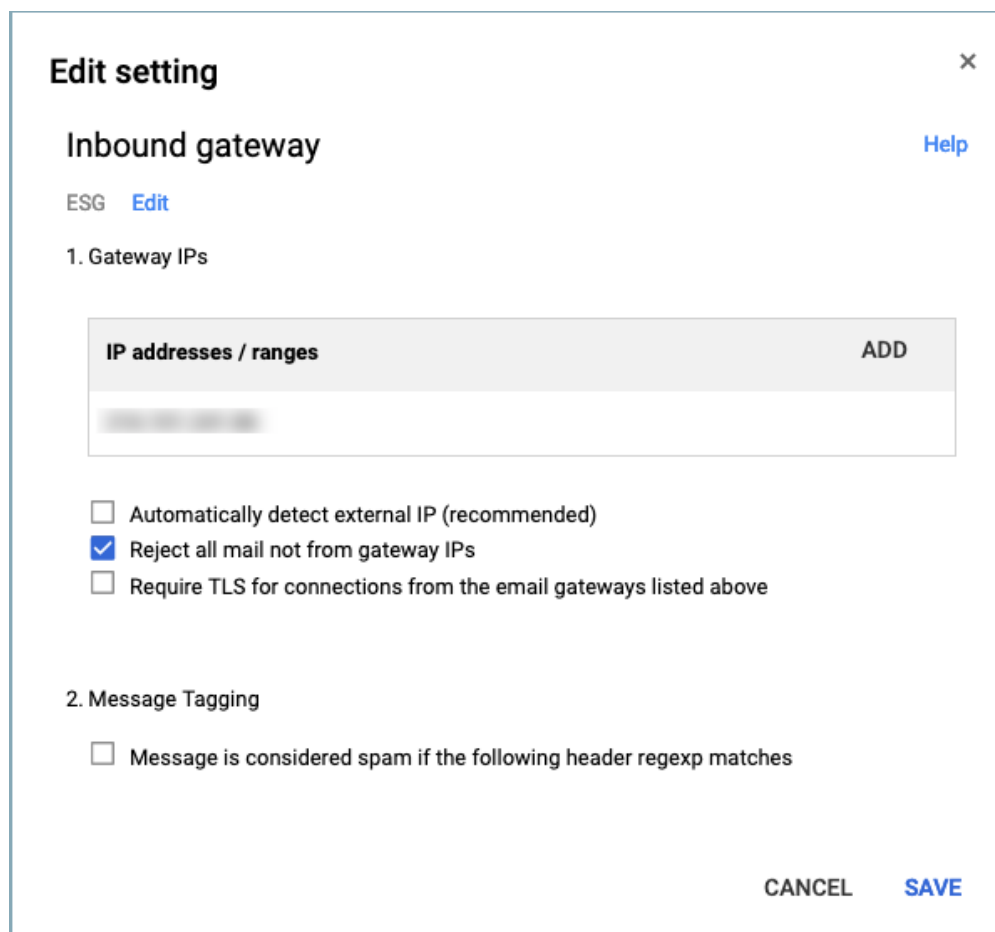
will be rejected.

3. **Require TLS for connections from the email gateways listed above**

6. Click **Save**.

More information on inbound gateways can be found [here](#).

Figure 1: Google Workspace - Inbound Gateway Settings



The screenshot shows a modal window titled "Edit setting" with a close button (X) in the top right corner. Below the title is the section "Inbound gateway" with a "Help" link. Underneath, it says "ESG" followed by an "Edit" link. The first section is "1. Gateway IPs", which contains a table with the header "IP addresses / ranges" and an "ADD" button. Below the table is a blurred input field. The second section is "2. Message Tagging", which contains a checkbox labeled "Message is considered spam if the following header regexp matches". At the bottom of the modal are "CANCEL" and "SAVE" buttons.

Edit setting ×

Inbound gateway [Help](#)

ESG [Edit](#)

1. Gateway IPs

IP addresses / ranges	ADD

☐ Automatically detect external IP (recommended)

☒ Reject all mail not from gateway IPs

☐ Require TLS for connections from the email gateways listed above

2. Message Tagging

☐ Message is considered spam if the following header regexp matches

CANCEL **SAVE**

Outbound Configuration

1. Scroll to the Routing section, and locate **Outbound gateway**.
2. Enter the IP address of the Barracuda Email Security Gateway that is the outbound mail gateway.

Figure 2: Google Workspace - Outbound Gateway Settings

Routing

Outbound gateway
Locally applied

Route outgoing emails to the following SMTP server: ?

! If you authenticate outgoing email using an SPF record or DKIM, you may need to update your configuration. ?

More information about outbound gateways can be found [here](#).

Google Workspace IP Addresses can change, so please refer to this [Google documentation](#).

Additional settings:

- nslookup -q=TXT _netblocks.google.com 8.8.8.8
- server: google-public-dns-a.google.com
- address: 8.8.8.8
- Non-authoritative answer:

_netblocks.google.com text ="v=spf1 ip4:216.239.32.0/19ip4:64.233.160.0/19ip4:66.249.80.0/20

ip4:72.14.192.0/18ip4:209.85.128.0/17ip4:66.102.0.0/20ip4:74.125.0.0/16
ip4:64.18.0.0/20ip4:207.126.144.0/20ip4:173.194.0.0/16 ?all"

Configuring the Barracuda Email Security Gateway

1. Navigate to **DOMAINS > Domain Manager** and specify your domain in **New Domain Name**, then click **Add Domain**.
2. Click the Manage Domain link and then **BASIC > IP Configuration**. Add the Google Workspace destination mail servers as follows:

Priority	Value/Answer/Destination
1	ASPMX.L.GOOGLE.COM
5	ALT1.ASPMX.L.GOOGLE.COM
5	ALT2.ASPMX.L.GOOGLE.COM
10	ALT3.ASPMX.L.GOOGLE.COM
10	ALT4.ASPMX.L.GOOGLE.COM

Also add the **Destination Server** name/IP address or hostname that receives email after spam and virus scans. It is usually best to use a hostname rather than an IP address so that the destination mail server can be moved and DNS updated at any time without having to make changes to the Barracuda Email Security Gateway configuration.

If you set **Use MX Records** (on the same page) to Yes, you must enter a domain name for this field. If multiple servers are specified, then the delimiter used determines the behavior (see below). Note that you can either configure **Use MX Records** for *all* domains from the **BASIC > IP Configuration** page, or you can configure it per-domain from **DOMAINS > Domain Manager > Manage Domains**, then using the **BASIC > IP Configuration** page for the domain you choose to manage. It is *NOT* recommended to set **Use MX Records** to Yes to avoid a potential mail loop.

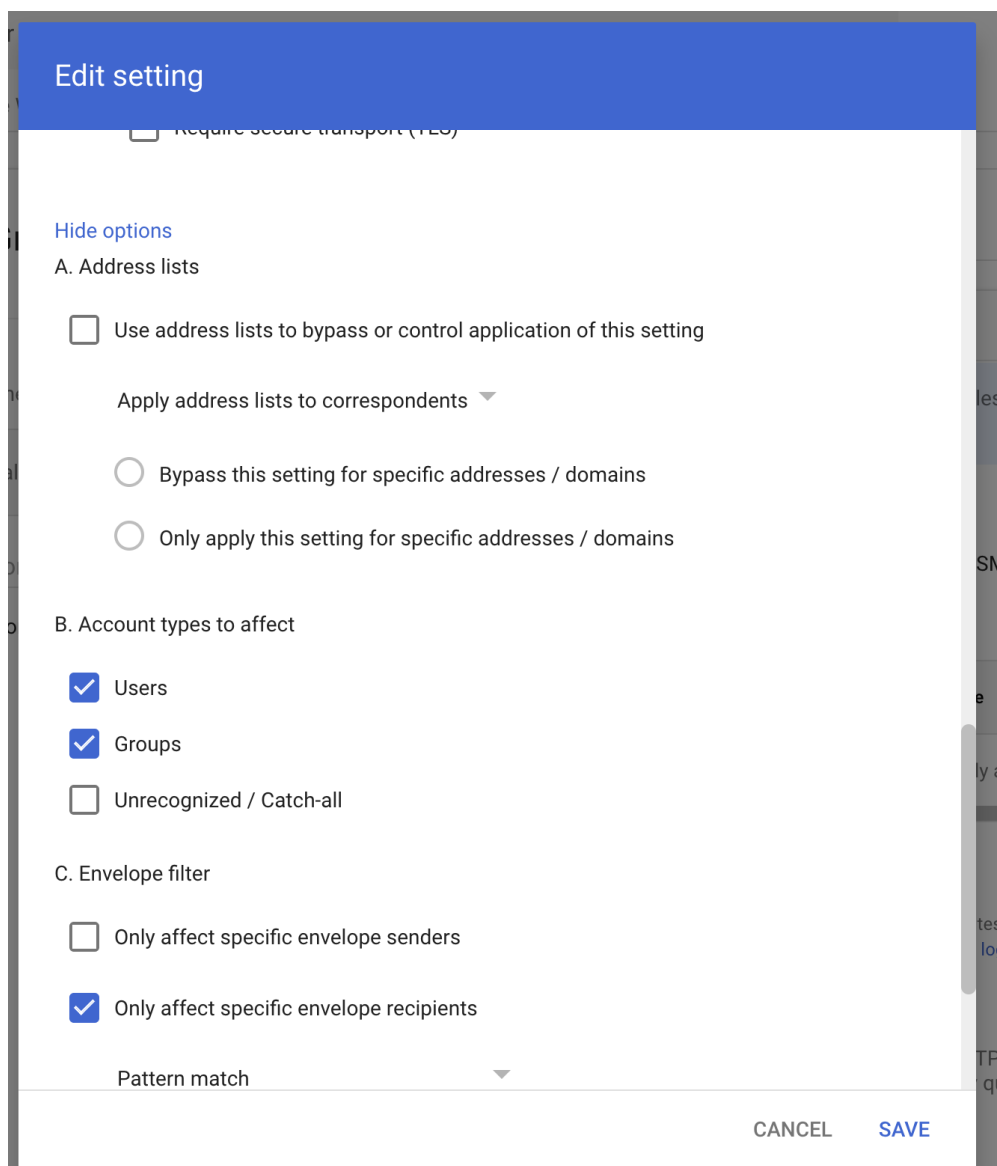
1. **Comma** (",") or semi-colon (";") - Each entry in the list will be used in round-robin fashion, with relative weights determined by the number of times a particular entry is listed.
2. **Space** (" ") - Each entry in the list will be treated as a failover list, with an entry being used only if all entries preceding it in the list are unreachable.

For more information about what it means to use MX records, please see [Using MX Records](#).

How to Configure Google Workspace to Bypass the Barracuda Email Security Gateway for Internal Mail

In the Google Workspace Admin console:

1. Go to **Apps > Google Workspace > Gmail > Advanced Settings**.
2. On the **General Settings** tab, scroll down to the **Routing** section. This is where you set your Outbound Gateway to route mail to the Barracuda Email Security Gateway. To the right, click **EDIT**, and add a route as shown.
3. Select **Internal - sending**.
4. Under Show Options, **Envelope filter**, select **Only affect specific envelope recipients**.
5. Under **Pattern match**, enter a REGEX expression containing your domain. For example, for myworkdomain.com, you could use `.*@mywork\.com`



Edit setting

☐ Require secure transport (TLS)

[Hide options](#)

A. Address lists

☐ Use address lists to bypass or control application of this setting

Apply address lists to correspondents ▼

☐ Bypass this setting for specific addresses / domains

☐ Only apply this setting for specific addresses / domains

B. Account types to affect

☒ Users

☒ Groups

☐ Unrecognized / Catch-all

C. Envelope filter

☐ Only affect specific envelope senders

☒ Only affect specific envelope recipients

Pattern match ▼

CANCEL SAVE

6. Scroll down in the popup and, under **Route**, select **Change route**.

Edit setting ×

Route
☒ Change route
☐ Also reroute spam
☒ Suppress bounces from this recipient
Internal Email ▼

Envelope recipient
☐ Change envelope recipient

Spam
☐ Bypass spam filter for this message

Attachments
☐ Remove attachments from message

Also deliver to
☐ Add more recipients

Encryption (onward delivery only)
☐ Require secure transport (TLS)

CANCEL SAVE

7. Scroll down and click [Show Options](#).

Edit setting ×

☐ Also reroute spam

☒ Suppress bounces from this recipient

Google Domains Email Forwarding ▼

Envelope recipient

☐ Change envelope recipient

Spam

☐ Bypass spam filter for this message

Attachments

☐ Remove attachments from message

Also deliver to

☐ Add more recipients

Encryption (onward delivery only)

☐ Require secure transport (TLS)

Show options

CANCEL SAVE

8. Under **Account Types to affect**, select **Users** and **Groups**. Click **SAVE**.

Edit setting ×

☐ Remove attachments from message

Also deliver to
☐ Add more recipients

Encryption (onward delivery only)
☐ Require secure transport (TLS)

[Hide options](#)

A. Address lists
☐ Use address lists to bypass or control application of this setting
Apply address lists to correspondents

☐ Bypass this setting for specific addresses / domains
☐ Only apply this setting for specific addresses / domains

B. Account types to affect
☒ Users
☒ Groups
☐ Unrecognized / Catch-all

CANCEL

SAVE

Now all internal mail is routed directly to Google servers, and all other mail routes through Outbound Gateway.

Figures

1. InboundConfig1.png
2. InboundGatewayGSuite.png
3. OutboundGatewayGSuite.png
4. EditSetting.png
5. ChangeRouteGSuite.png
6. ShowOptionsEditRouteGSuite.png
7. AccountTypesGSuite.png

© Barracuda Networks Inc., 2024 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.