Summary of steps

For inbound mail with a recipient hosted in G Suite:

1. Preconfigure G Suite to accept mail from the Cisco Cloud Email Security (CES) IPs that are provided in your Cisco welcome letter.
2. In CES, set the destination controls (throttling) to G Suite.
3. Configure CES to accept email for your domain(s) and route it to G Suite.
4. Alter the domain’s DNS to route mail to CES (a Mail Exchange cutover).
5. Test and review the output.

For outbound mail:

1. In CES, create Host Access Table (HAT) entries for G Suite.
2. In G Suite, route mail from G Suite to CES.
3. In CES, implement the outbound message verification filter.
4. Test and review the output.

Note: It is highly recommended that you test these settings well before any planned production mail cutover, because settings may take time to replicate in the G Suite console. At a minimum, allow 1 hour for all changes to take effect.
Configuring incoming email

Your Cisco welcome letter includes your CES IP addresses and other pertinent information. If you have not received or do not have a copy of the letter, please contact ces-activations@cisco.com with your contact information, customer name, and domain name under service.

The IPs are dedicated for each client and are not likely to change without notification. You can use the assigned hostnames or IPs in the G Suite configuration.

1. Log in to the G Suite console and navigate to the administrator menu.
2. Go to Apps > G Suite > Settings for Gmail > Advanced settings > General Settings and scroll down to Spam > Inbound gateway and click Settings.

3. Enter the information as required. Use the information from your Cisco CES welcome letter.

   Enter a name that is easily identified later

   Enter the IPs as found in the welcome letter

   At a minimum, select the first check box

   Choosing the two check boxes under Message Tagging is optional, but highly recommended. We can make use of the Spam folder in Gmail with an x-header.
Check to make sure that CES is not throttled.

4. In CES, navigate to **Mail Policies > Destination Controls**

5. Under **Destination Controls**, complete the configuration to impose a self-throttle. It can be removed later, but these are “new” IPs to G Suite, and we do not want any throttling by Google due to their unknown reputation.

6. Under **Mail Policies > Destination Controls**, click **Add Destination**.

7. Use the following settings:
   - Domain: .aspmx.l.google.com
     *(Note: The dot at the beginning of the host is required.)*
   - 10 concurrent connections
   - 20 messages per connection
   - TLS Preferred (or Mandatory)
• In CES, set the Recipient Access Table (RAT) to accept mail for your domains. Navigate to Mail Policies > Recipient Acceptance Table (RAT) and click Add Recipient. Add your domains and the default action of Accept. The example given is for the domain teamnorthwind.com.

Note: Make sure the Listener is for IncomingMail.

• Finally, in CES go to Network > SMTP Routes and click Add Route. Enter your domain and add the G Suite records provided, adding rows as needed.

• At this point you are ready to cut over the domain through a Mail Exchange (MX) record change. Work with your DNS administrator to resolve your MX records to the IP addresses provided in your Cisco CES welcome letter. Verify the change in the G Suite console. This could take time, depending on your TTL settings.

DNS provider:

In G Suite:
• Test inbound mail by sending a message to your address within G Suite. Check to see that it arrives in your G Suite email inbox. You can use the message tracking tool on your Cisco Content Security Management Appliance (SMA) provided with your CES service. This step could take some time.

In CES message tracking:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Sender</th>
<th>Recipient</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 Nov 2017</td>
<td>09:15:38 (GMT +05:00)</td>
<td><a href="mailto:usman.din@gmail.com">usman.din@gmail.com</a></td>
<td><a href="mailto:usman@teamnorthwind.com">usman@teamnorthwind.com</a></td>
<td>received SMTP response</td>
</tr>
</tbody>
</table>

In G Suite, check the logs under Reports > Email Log Search.

Result of message marked as spam in CES and delivered to the Spam folder:

• (Optional step). If you wish to use CES to send suspected spam to the user’s spam folder in Gmail, the x-header specified in Step 3 can be inserted in the Positive or Suspect Spam settings.

Spam settings page

![Spam settings page](image)
Configuring outgoing email

Note: The below instructions will route all outbound mail to the Cisco Cloud Email Security Service, including user-to-user email. If you wish to keep user-to-user routing internal to G Suite, follow the instructions found here: https://support.google.com/a/answer/6297084

1. Refer to your welcome letter. A secondary interface will be specified for outbound messages. In CES, go to Mail Policies > Host Access Table and make sure the Listener is for OutgoingMail.

2. Click the Sender Group named Relay. Note: You can rename it to be more descriptive if you wish.

3. Click Add Sender and enter .google.com (the starting period is required). Click Submit and Commit your changes.

4. In the G Suite console, go to Apps > G Suite > Settings for Gmail > Advanced settings.

5. Scroll down to the Routing section and enter the hostname or IP of the outbound address into the Outbound gateway setting.
6. To prevent unauthorized messages from Google, an secret x-header can be stamped when messages leave G Suite. This header is then evaluated and removed before delivery to the Internet.

7. In the G Suite console, go to Apps > G Suite > Settings for Gmail > Advanced settings.

8. Scroll down to the Routing section and click Routing and then Add.

9. Add a filter as shown below for outbound flow and adding a customer header.

10. On the CES instance, create a message filter to inspect the presence and value of the x-header, and remove the header if exists. If no header exists, drop the message.

```plaintext
gsuite_outbound: if (sendergroup == "RELAY_GSUITE"){
    if (header("X-OUTBOUND-AUTH") == "^mysecretkey$") {
        strip-header("X-OUTBOUND-AUTH"); } else {drop();}
}
```

11. Test outbound mail.

The x-header does not match:

Successful delivery: