Integrated Marketing Solutions Ltd

Email Deliverability Overview

11th July 2019

Contents

Warming up IP addresses and domains *3*
Domain and IP Reputation *4*
Reputation monitoring *5*
Gmail *5*
How Gmail classifies incoming mail 5
Use Postmaster Tools 5
Microsoft (outlook.com, Hotmail.com) *7*
Sender Solutions 7
Email and Customer Strategy *9*
Clean Customer / Prospect Email Addresses 9
Reliable cadence and volume 9
Subscription 10
Include options to subscribe 10
Include option to unsubscribe 10
Email Formatting *10*
Technical Configuration *11*
IP address strategy *11*
Authenticated Messages *11*
Check whether messages are authenticated 12
Adobe Specific Quarantine *13*
Delivery failure types and reasons 13
Useful links *14*

Warming up IP addresses and domains

Warm up new IPs and domains over time to build your sending reputation. Mismanaging or rushing the warming process can cause email to go to the spam folder and adversely affect your business. Gmail has an additional filter they called Foldering. They look at your mail and reputation and start moving mail from being delivered to the Inbox rather into Update or Promotional email tabs. Worst case scenario they move the email straight to the junk folder.

Yahoo recommends a warmup process as below. Depending on the size of the organisation and the number of customers to engage, the process while being feasible may require a more aggressive delivery strategy.

- To start, send only five messages per connection (open a connection, send five messages, close the connection, then repeat). Increase the number of messages per connection over time.
- Monitor the SMTP codes for signs of throttling. If you receive an error indicating throttling, adjust your connection and throughput settings and slow down the volume until the throttling messages subside.

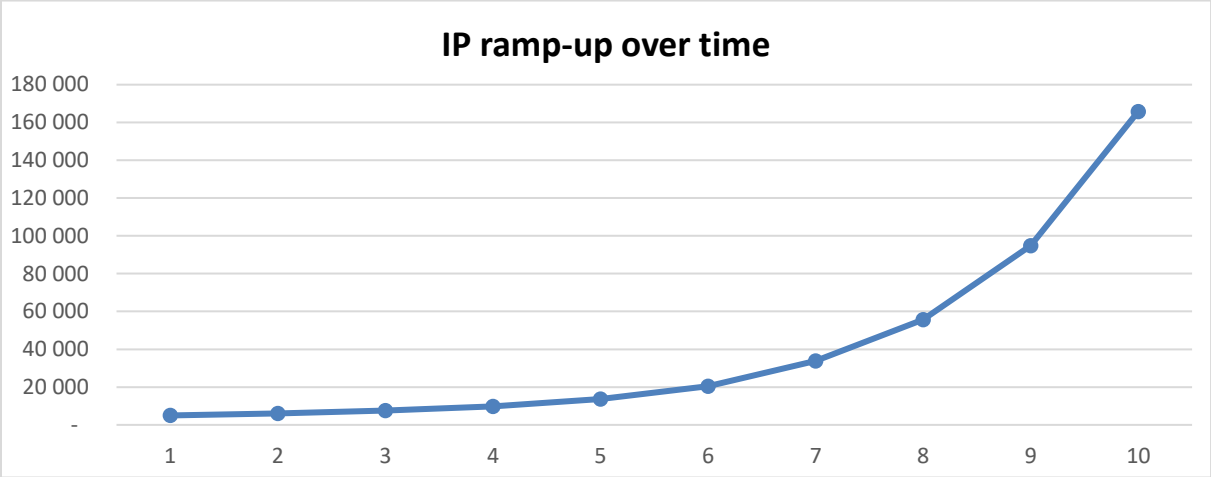
It is absolutely essential that the Postmaster and SNDS accounts are configured for you to monitor your reputation while warming up, and for future monitoring of the IPs.

A classic example of an error that will degrade reputation is if there are spikes in the volume of mails being sent. Gmail (as would be seen in postmaster) will start sending a proportion of the mails to spam as the velocity threshold is met.

An example of ramping up volume

Overall Volume per day

	Overall send volume	% increase
Day 1	5 000	N/A
Day 2	6 000	20.00%
Day 3	7 500	25.00%
Day 4	9 750	30.00%
Day 5	13 650	40.00%
Day 6	20 475	50.00%
Day 7	33 784	65.00%
Day 8	55 743	65.00%
Day 9	94 763	70.00%
Day 10	165 836	75.00%



Yahoo does announce a process to have IPs whitelisted at
https://help.yahoo.com/contact/postmaster/newsenderapp

Additionally it is advised to use your most engaged customers for the warmup period (we are wanting a higher open rate). Recommendations are to focus on customers that have engaged within the last 30 days.

Domain and IP Reputation

Domain and IP reputation gives a sense of whether the spam filter might mark emails from that Domain or IP as spam or not. Keep in mind that spam filtering is based on thousands of signals, and that Domain & IP reputation are just two of them.

The definition of spam in the section below includes mail detected as spam by Spam Filters, and mail reported by users as Spam.

- Bad — A history of sending an enormously high volume of spam. Mail coming from this entity will almost always be rejected at SMTP or marked as spam.
- Low - Known to send a considerable volume of spam regularly, and mail from this sender will likely be marked as spam.
- Medium/Fair — Known to send good mail, but is prone to sending a low volume of spam intermittently. Most of the email from this entity will have a fair deliverability rate, except when there is a notable increase in spam levels.
- High — Has a good track record of a very low spam rate, and complies with the ISP's sender guidelines. Mail will rarely be marked by the spam filter.

Reputation monitoring

Different ISPs use different tools for customers to monitor their IP addresses

Gmail

How Gmail classifies incoming mail

- Spam: Spam goes to the Spam folder; everything else goes to the inbox.
- Inbox categories: In Gmail's default inbox layout, messages are divided into the following categories:
- Primary
- Social
- Promotions
- Updates
- Forums

Mail classifications automatically adjust to match users' preferences and actions. For example, users can unmark spam, move messages to a different category, or switch categories on or off. Over time, Gmail automatically adjusts classifications according to these corrections

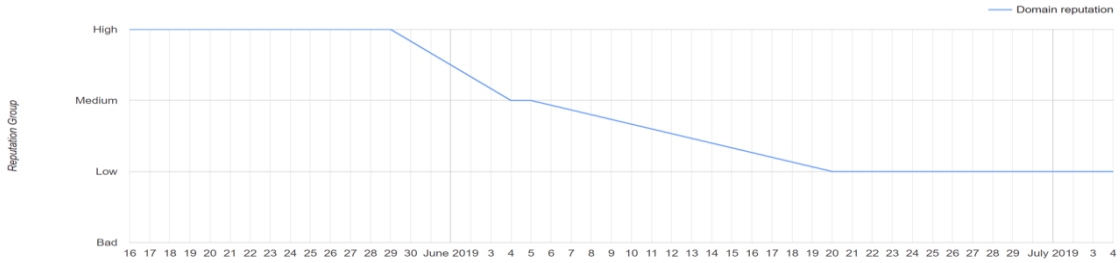
Use Postmaster Tools

Postmaster Tools provides metrics on reputation, spam rate, feedback loop, and other parameters that can help you identify and fix delivery or spam filter issues.

To register for the Google Postmaster tools you will need a verified domain. This is a TXT or CNAME record provided by google, and in turn this needs to be inserted into your DNS record.

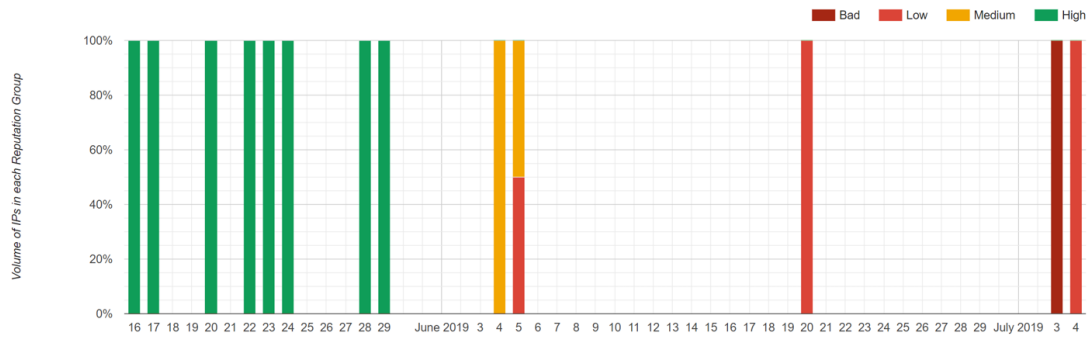
This proves to Gmail you own the domain.

Domain Reputation



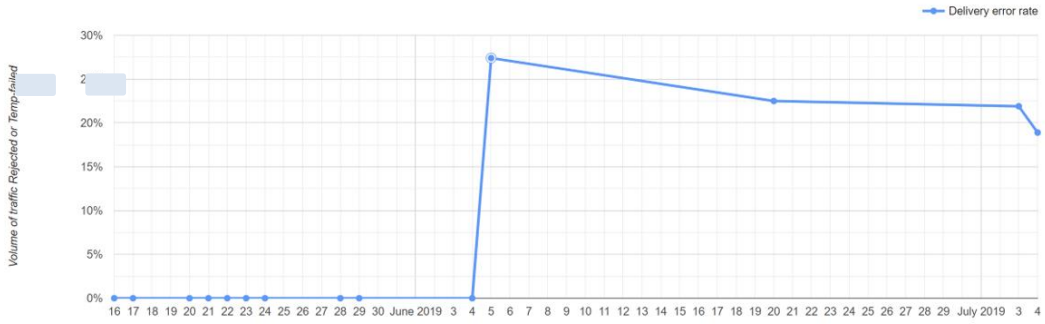
Date	Domain reputation
Jul 4, 2019	Low
Jul 3, 2019	Low
Jun 20, 2019	Low
Jun 5, 2019	Medium

IP Reputation



Low reputation IPs for June 20
130.248.153.167-130.248.153.168

Delivery Errors



Error Type for June 5	Reason	Percentage
TempFail	Rate limit exceeded	27.4%

Microsoft (outlook.com, Hotmail.com)

They use a free service called Smart Network Data Services. Microsoft lists the process to register as '*To access SNDS, please log in with a Microsoft Account and then request access to the IPs for which you are responsible. You'll be taken through a simple authorization process*'

Sender Solutions

Email abuse, junk email, and fraudulent emails (phishing) continue to burden the entire email ecosystem. To help build back consumer trust in the use of email, Microsoft has put in place various policies and technologies to help protect our consumers. However, Microsoft understands that legitimate email senders should not be negatively affected. Therefore, we have established a suite of services to help senders improve their deliverability to Outlook.com consumers by proactively managing their sending reputation.
Below is an overview of services that can benefit your organization including links for more information:

Service	Benefits
Postmaster	A starting point for any questions related to delivering communications to Outlook.com users Includes a simple online guide with our policies and requirements An overview of the junk email filters and authentication technologies employed by Microsoft
Return Path Certification	The industry's most recognized and valued email certification program. A third-party accreditation and reputation service used to "safe list" senders. Learn more at https://returnpath.com/solutions/email-deliverability-optimization/ip-certification/ Learn sender best practices from Return Path and avoid the most common sender reputation pitfalls like complaints and spam traps: http://pages.returnpath.com/email-sending-best-practices.html Learn email security best practices from Return Path and keep your sensitive data safe and your systems secured: http://pages.returnpath.com/email-security-best-practices.html Learn how Return Path Certification helps senders get into more inboxes more quickly: http://pages.returnpath.com/get-certified.html
Junk Email Reporting Program	A free service to provide reports on junk email issues reported by Outlook.com users

	Returns the full message with headers of any email marked as "junk" or "phishing" Provides senders an opportunity to clean their email lists and improve the quality of their content Helps identify potential problems with your marketing practices and content Helps improve sender reputation by removing unwanted subscribers from lists Enroll at https://postmaster.live.com/snds/JMRP.aspx and typically start receiving feedback within as little as 72 hours
Smart Network Data Services	A free service that provides high-level insight on how users are rating the email they receive and the health of your IP space as viewed by the Outlook.com system Provides easy online registration and access to data Improves understanding of how our filters rate your email Reveals how many users complained about your email Learn more at https://postmaster.live.com/snds
Support	Provides escalation support for deliverability issues. Support information can be found on the Troubleshooting page.

IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 3 IPs		**12,241**	**12,241**	**11,854**	**1 Red IPs**	**< 0.1%**		**0**	**0 distinct values**	**0 distinct values**	
172. 31	6/4/2019 4:00 PM - 6/4/2019 8:00 PM	11397	11397	11010		< 0.1%		0			
130. .167	6/4/2019 11:00 AM - 6/4/2019 1:00 PM	426	426	426		< 0.1%		0			
130. .168	6/4/2019 11:00 AM - 6/4/2019 1:00 PM	418	418	418		< 0.1%		0			
Total: 3 IPs		**12,241**	**12,241**	**11,854**	**1 Red IPs**	**< 0.1%**		**0**	**0 distinct values**	**0 distinct values**	

Activity period	RCPT commands	DATA commands	Message recipients	Filter result	Complaint rate	Trap message period	Trap hits	Sample HELO	Sample MAIL FROM	Comments
Total: 13 days	**181,026**	**179,680**	**179,288**	**12 red days**	**< 0.1%**		**0**	**0 distinct values**	**0 distinct values**	
7/7/2019 8:00 AM - 7/7/2019 2:00 PM	12146	12146	12146		< 0.1%		0			
7/5/2019 6:00 PM - 7/5/2019 10:00 PM	24529	24528	24528		< 0.1%		0			
7/1/2019 7:00 AM - 7/1/2019 11:00 AM	21851	21851	21851		< 0.1%		0			
6/28/2019 8:00 AM - 6/29/2019 1:00 AM	22350	22350	22350		< 0.1%		0			
6/15/2019 7:00 AM - 6/15/2019 11:00 AM	16638	16638	16638		< 0.1%		0			
6/14/2019 7:00 AM - 6/14/2019 2:00 PM	18672	17327	17323		< 0.1%		0			
6/13/2019 7:00 AM - 6/13/2019 12:00 PM	12398	12398	12398		< 0.1%		0			
6/12/2019 8:00 AM - 6/12/2019 3:00 PM	4339	4339	4339		< 0.1%		0			
6/11/2019 6:00 PM - 6/11/2019 11:00 PM	8701	8701	8701		< 0.1%		0			
6/4/2019 4:00 PM - 6/4/2019 8:00 PM	11397	11397	11010		< 0.1%		0			
6/1/2019 10:00 AM - 6/2/2019 1:00 AM	12248	12248	12248		< 0.1%		0			
5/27/2019 7:00 AM - 5/27/2019 10:00 PM	13090	13090	13089		< 0.1%		0			
5/19/2019 10:00 AM - 5/19/2019 1:00 PM	2667	2667	2667		< 0.1%		0			
Total: 13 days	**181,026**	**179,680**	**179,288**	**12 red days**	**< 0.1%**		**0**	**0 distinct values**	**0 distinct values**	

Email and Customer Strategy

Clean Customer / Prospect Email Addresses

Sending emails to invalid addresses has a negative impact on the reputation of the sending IP. It's advisable to:

- Run initial and ongoing formatting rules against all email addresses captured for recipients
- For new customers that may be registering with the business, use a form of validation to confirm the email address. Examples would be sending an email with a verification link, or sending a code to the email address the customer is required to capture to prove the email address. Not only does this ensure a clean email address, the opening of the email will also improve the open rate and reputation for the IP.
- Create a feedback loop from Campaign to your customer / CRM system and update hard bounces against the customer record. Adobe Campaign will quarantine hard bounces after a single failed send, and soft bounces after 5 failed sends by default.
- Run technical campaigns for invalid email addresses via another channel, such as SMS, driving the customer to a landing page for update of the email address.

Reliable cadence and volume

Aim to spread the email volume over more days with a consistent volume rather than spikes in email volume over fewer days.

Subscription

- Automatically unsubscribe users whose addresses bounce multiple times
- Occasionally send confirmation messages to users
- Include each mailing list recipients are signed up for, and give them the option to unsubscribe from any they're no longer interested in

Include options to subscribe

- Provide each recipient on your distribution list either "opt-in" option below:
    - An email asking them to subscribe
    - A checkbox on a web form or in software they need to manually check
- Confirm each recipient's email address is correct before subscribing them.
- Avoid:
    - Purchasing an email address from a third-party
    - Including a checkbox on a web form or in software that is automatically checked and subscribes users by default

Include option to unsubscribe

When users receive a lot of email they don't open, Gmail will show a card with the option to unsubscribe. Allowing users to unsubscribe can improve open rates, click through rates, and spend efficiency.

- Make sure recipients can unsubscribe through either:
    - A prominent link in the body of an email leading to a confirmation page, without requiring recipients to provide additional information
    - An option to reply to your email to unsubscribe

- Gmail provides an option to add a 'List-Unsubscribe' header in one of the following ways:
    - Add the following headers for one-click unsubscribe as described in RFC 8058:

      List-Unsubscribe-Post: List-Unsubscribe=One-Click
      List-Unsubscribe: https://example.com/unsubscribe/opaquepart

      If the recipient unsubscribes, you'll get this POST request:
      POST /unsubscribe/opaquepart HTTP/1.1
      Host: example.com
      Content-Type: application/x-www-form-urlencoded
      Content-Length: 26

      List-Unsubscribe=One-Click

    - Point to an email address using 'mailto:'

Email Formatting

Make sure your messages have:

- Formatting according to RFC 5322 and, if using HTML, HTML standards
- A valid 'Message-ID:' header field
- An indication that you're sending bulk emails in the 'Precedence: bulk' header field
- Visible information about the true sender and true landing page for links
- Subject lines that are relevant to the message content and not misleading
- Domain formatting according to the highly-restrictive Unicode Security Profile guidelines for international domain names, including:
- Authenticating domain
- Envelope From domain
- Payload domain
- Reply-to domain
- Sender domain

It is also advised that for html based emails there is also a text equivalent (simple to do in AC). Additionally emails can be negatively scored if the ratio between images and text is too low. A product like Spam Assassin will vet the email copy and provide a score with suggestions to improve.

Technical Configuration

- The sending IP must have a PTR record (i.e. a reverse DNS of the sending IP) and match the IP obtained via the forward DNS resolution of the hostname specified in the PTR record.
- Sign messages with DKIM. Gmail for example don't authenticate messages signed with keys that use fewer than 1024 bits.
- Publish a SPF record.
- Publish a DMARC policy.

IP address strategy

It is highly recommended that separate IP addresses are used for different classifications of email. The common split is to separate financial / transactional type of mails from marketing. The reason being is that if marketing messages are reducing reputation of the IP or Domain, transactional messages from the same IP will be treated in the same way.

The suggestion therefore is to use separate IP addresses and / or domains for different classifications of communications.

Authenticated Messages

Messages must be authenticated to make sure they're classified correctly. Also, unauthenticated messages are very likely to get rejected. Because spammers can also authenticate mail, authentication by itself isn't enough to guarantee your messages can be delivered.

Emails can be authenticated using SPF or DKIM.

SPF specifies which hosts are allowed to send messages from a given domain by creating an SPF record.

DKIM allows the sender to electronically sign legitimate emails in a way that can be verified by recipients using a public-key. Use RSA keys that are at least 1024-bits long. Emails signed with less than 1024-bit keys are considered unsigned and can easily be spoofed.

How the Private/Public keys operate
The domain owner generates a pair of keys (public/private) that will be used to sign the messages sent by the users of this domain. The public key is placed in the DNS of the domain as a TXT type record. The private key is kept on the messaging server that sends emails for this domain. When an email is sent by the user of the domain, the messaging server uses the private key to sign the message. The signature is added to the message header before it is sent.
When a signed message is received, the messaging server reads the signature and message domain then queries the DNS in order to obtain the public key of the domain. With this public key, the messaging server then checks whether the signature of the message is valid.

Check whether messages are authenticated

Send a proof to your mail client and….

Check Gmail messages

1. On your computer, open Gmail.
2. Open an email.
3. Below the sender's name, click the Down arrow ⌄.

The message is authenticated if you see:

- "Mailed by" header with the domain name, like google.com.
- "Signed by" header with the sending domain.

The message isn't authenticated if you see a question mark next to the sender's name. If you see this, be careful about replying or downloading any attachments.

Check messages in another mail client, like Outlook or Apple Mail
If you're checking your email on another email client, you can check the message headers.

1. Open an email message.
2. Find the "Authentication-Results" header.
3. If the message was authenticated by SPF/DKIM, you'll see "spf=pass" or "dkim=pass."

If a message you sent arrived with a question mark "?" next to your email address, the message wasn't authenticated.

Adobe Specific Quarantine

Delivery failure types and reasons

There are three types of errors when a delivery fails:

- **Hard**: A "hard" error indicates an invalid address. This involves an error message that explicitly states that the address is invalid, such as: "Unknown user".
- **Soft**: This might be a temporary error, or one that could not be categorized, such as: "Invalid domain" or "Mailbox full".
- **Ignored**: This is an error that is known to be temporary, such as "Out of office", or a technical error, for example if the sender type is "postmaster".

The possible reasons for a delivery failure are:

- **User unknown** (Hard type): the address does not exist. No further deliveries will be attempted for this profile.
- **Quarantined address** (Hard type): the address was placed in quarantine.
- **Unreachable** (Soft/Hard type): an error has occurred in the message delivery chain (incident on SMTP relay, domain temporarily unreachable, etc.). According to the error returned by the provider, the address will be sent to quarantine directly or the delivery will be tried again until Campaign receives an error which justifies the Quarantine status or until the number of errors reaches 5.
- **Address empty** (Hard type): the address is not defined.
- **Mailbox full** (Soft type): the mailbox of this user is full and cannot accept more messages. This address can be removed from the quarantine list to make another attempt. It is removed automatically after 30 days. In order for the address to be automatically removed from the list of quarantined addresses, the **Database cleanup** technical workflow must be started.
- **Refused** (Soft/Hard type): the address has been placed in quarantine due to a security feedback as a spam report. According to the error returned by the provider, the address will be sent to quarantine directly or the delivery will be tried again until Campaign receives an error which justifies the Quarantine status or until the number of errors reaches 5.
- **Duplicate**: the address has already been detected in the segmentation.
- **Not defined** (Soft type): the address is in qualification because errors have not been incremented yet. This type of error occurs when a new error message is sent by the server: it can be an isolated error, but if it occurs again, the error counter increases, which will alert the technical teams.
- **Error ignored**: the address is in the whitelist and an email will be sent to it in any case.
- **Blacklisted address**: the address was blacklisted at the time of sending.
- **Account disabled** (Soft/Hard type): when the Internet Access Provider (IAP) detects a lengthy period of inactivity, it can close the user's account: deliveries to the user's address will then be impossible. The Soft or Hard type depends upon the type of error received: if the account is temporarily disabled due to six months of inactivity and can still be activated, the status **Erroneous** will be assigned and the delivery will be tried again. If the error received signals that the account is permanently deactivated then it will directly be sent to Quarantine.
- **Not connected**: the profile's mobile phone is switched off or not connected to the network when the message is sent.
- **Invalid domain** (Soft type): the domain of the email address is incorrect or no longer exists. This profile will be targeted again until the error count reaches 5. After this, the record will be set to Quarantine status and no retry will follow.
- **Text too long**: the number of characters in the SMS message exceeds the limit. For more on this, see SMS encoding, length and transliteration.
- **Character not supported by encoding**: the SMS message contains one or more characters that are not supported by the encoding. &For more on this, see Table of characters - GSM Standard.

Useful links

https://docs.campaign.adobe.com/doc/standard/getting_started/en/ACS_Deliverability.html

https://docs.campaign.adobe.com/doc/AC/en/DLV_Deliverability_management_Technical_recommendations.html

Credits and Acknowledgement

All information in this document has been developed and replicated through company experience, association with and in partnership with Adobe, and through best practices published from Adobe, Google and Microsoft.