ResponseGenius

New Client Set-Up Guide

Congratulations on becoming a ResponseGenius client!
We look forward to working with you to optimize your email messaging. First step: setting up your account to realize the most benefits we offer.

Sending Domain Name

You cannot use a domain or subdomain that is currently being used in another email client (such as your corporate email account.) Choose a domain or subdomain name that is solely for use with the solution and has no email accounts currently set-up on it. You may create multiple sending domains. All steps below must be followed for each sending domain.

*Response*Genius Account Set-Up

There are two set up options available:

Full Serve

- We will go to GoDaddy.com and purchase the domain name. There is a fee of $150.00 per domain for RG to purchase and set up the domain.
- Provide RG with a list of several preferred domains, and we will purchase the first one available.
- RG will create the DNS, SPF, DKIM, MX and FBL settings and links.
- We will set up the Mailer Sending Domain you provide us.
- Once the account is set up, we will send you a log in link and temporary password.
- We will set up the Yahoo and Gmail required settings.
- We will schedule an initial training session with you.

Self Serve

- **REGISTER YOUR NEW DOMAIN OR SUBDOMAIN AND CREATE THE DNS SETTINGS.**
  You cannot use a domain or subdomain that is already being used for emails or webhosting. If your root domain is in use, you can create a new subdomain for use by the email platform. It's very important that all of the records below are entered correctly and also keep in mind that it can take 24-48 hours for the records to fully propagate around the Internet. Missing or broken records could result in delivery issues, blacklisting, blocking and a higher rate of complaints.

- Custom sending domains can either be setup at the root allowing for Email Campaigns to be sent using something like **<anything here>@somedomain.com** but if that's not possible then a subdomain can be used such as **<anything here>@XXX.somedomain.com**

- Any name can be used for the subdomain and 'XXX' is just a placeholder.

• DKIM (DOMAINKEYS IDENTIFIED MAIL)

DKIM requires a valid public key and can be created in DNS using the record listed below.

- If you're using the root domain: **dkim1024._domainkey CNAME dkim.responsegenius.com**.
- If you're using a subdomain e.g. 'mail': **dkim1024._domainkey.XXX CNAME dkim.responsegenius.com**

• SPF (SENDER POLICY FRAMEWORKS)

A TXT record containing details of the IP addresses used for mail delivery from the solution is required. For those familiar with SPF records, they can be customised easily using multiple 'include' references.

If you're using the root domain:

@ MX response- genius*.smtp.dnsrt.co.uk @ TXT v=spf1 include:spf.responsegenius.com* -all

If you have purchased your own control panel, the name to enter here is the control panel domain

If you're using the sub domain: **XXX CNAME response- genius*.smtp.dnsrt.co.uk**

If you have purchased your own control panel, the name to enter here is the control panel domain

• CUSTOM CLICK TRACKING DOMAINS

Custom click tracking domains require a CNAME record which you enter into the control panel where your domain is registered. Choose any name for the subdomain for tracking clicks in email, e.g. clicks.

clicks CNAME response-genius*.clicks.dnsrt.co.uk

If you have purchased your own control panel, the name to enter here is the control panel domain

• PUBLISH DMARC RECORD

- Create a TXT record in DNS for _dmarc.[your-domain] with your DMARC record.
- Use the following syntax in the DMARC TXT record:

v=DMARC1; p=none; fo=1; rua=mailto:dmarc_agg@auth.returnpath.net; ruf=mailto:dmarc_afrf@auth.returnpath.net.

This is the suggested record for when you first implement DMARC. v=DMARC1 indicates the protocol version. The suggested DMARC record above includes a monitor policy (p=none). This means that you are not instructing mailbox providers to take any action with your email that fails authentication.

rua contains the address where you want to receive aggregate reports.

ruf contains the address where you want to receive forensic reports.

To begin receiving DMARC reports without impacting your current email program, we suggest publishing the record with p=none. Make sure you have at least an A record, Mail Exchange (MX) record, or AAAA record in the DNS for the domain if you plan on using it to send email.

• SET UP THE YAHOO FBL LINK

- Go to http://postmaster.yahoo.com and sign in with your Yahoo! account.
- Click on "Feedback Loop Application" in the right-hand side of the page
- Enter your details.
- Set the "Reporting Email" to **reports@spamloop.co.uk.**
- Set the "Selector" to *.
- Set the "Domain" to everything following the @ symbol e.g. for something@mail.mydomain.com set it to **mail.mydomain.com.**

- Tab out of the “Domain” field but do not press the submit button.
- Immediately send an email to Support@ResponseGenius.com alerting us to an incoming code from Yahoo. Yahoo does not identify the code applicant within their email, so you must inform us to be on the lookout.
- Yahoo! will email a code to Support@ResponseGenius.com, and we will immediately forward it to you.
- Contact support if you have not received your verification code email.
- Once you have the code, enter it into the box and click submit.
- Send an email to Support@ResponseGenius letting us know you’ve set this up. We will receive a notification from
- Yahoo so we can complete the process.

• SET UP GMAIL REQUIREMENTS

- Add & Verify Authentication Domains (this must be done for every sending domain)
- Go to postmaster.google.com
- On the bottom right, click the + button.
- Enter your authentication domain in the box that pops up.
- Add a DNS TXT or a DNS CNAME record. (see above)

Complete Account SetUp

Let us know when you’ve set up all the DNS settings, and we will verify them and let you know if we see any issues. Once the account is set up, we will send you a log in link and temporary password.
Email us at support@responsegenius.com to schedule training once you’ve created a password.

• ADDITIONAL GMAIL SETTINGS

- Set up the Gmail FBL link. This is highly recommended by Gmail for better delivery and inbox placement. Senders will need to embed a new header called the Feedback-ID, consisting of parameters (called Identifiers) that uniquely identify their individual campaigns. Any Identifiers with an unusual spam rate and that might cause deliverability issues will be reported in the Postmaster Tools FBL dashboard.
Header format: **Feedback-ID: a:b:c:SenderId** where **Feedback-ID** is the name of the Header to be embedded. **a, b, c** are optional fields that can be used by the sender to embed up to 3 Identifiers (campaign/customer/other). **SenderId** is a mandatory unique Identifier (5–15 characters) chosen by the sender. It should be consistent across the mail stream.

- The aggregate data will be generated for the first 4 fields (as separated by ‘:’) of the Feedback-ID: , starting from the right side. If the SenderId is empty, no data will be generated. If another field is empty, data will be generated for the rest of the fields.

- In order to prevent spoofing of the Feedback-ID, the traffic being sent to Gmail needs to be DKIM signed by a domain owned (or controlled) by the sender, after the addition of this header. This domain should be added and verified to the Gmail Postmaster Tools, so the sender can access the FBL data.

- Senders should ensure that their traffic has only one such verified header.

- Senders will have to publish the IPs from which they’re sending mail in the SPF records of their signing domains. The sending IPs must have PTR records and resolve to a valid hostname (preferably one of the DKIM domains).

- For a given day's traffic, FBL reports are generated only if a given Identifier is present in a certain volume of mails as well as in distinct user spam reports.

- FBL data will be aggregated on each Identifier independently. This also allows for the use of less than 3 Identifiers, if needed.

- For a given day's traffic, the sender should ensure that the Identifiers across fields not repeated, so that data is not aggregated across unrelated Identifiers. If there is a concern about the uniqueness of the Identifier namespace, or if the sender prefers for the data to be grouped between two Identifiers, the hash of one Identifier can be appended to the other.

- When choosing the Identifiers, the sender should not use a parameter that will be unique across every single mail (for example, a unique Message-ID).

- Here is an example for illustration: **Feedback-ID: CampaignIDX:CustomerID2:MailTypeID3:SenderId** where **CampaignIDX** is a campaign Identifier specific to Customer2 and is unique across the board (that is,. no 2 customers share the same campaign ID). **CustomerID2** is a unique customer Identifier. **MailTypeID3** is an Identifier for the type of mail (a newsletter vs. a product update, for example) and can be either unique or common across customers, based on how the sender wants to view the data. **SenderId** is the sender's unique Identifier and can be used for overall statistics. In the above case, we would send the spam percentages for each of the 4 Identifiers independently, if they had an unusual spam rate.

• INCLUDE GMAIL SPECIFIC UNSUBSCRIBE

- To make sure recipients can unsubscribe without leaving Gmail, Gmail recommends adding a "List Unsubscribe. Header in one of the following ways:

1. Add the following headers for one-click unsubscribe as described in RFC 8058:
2. List-Unsubscribe-Post: List-Unsubscribe=One-Click
3. 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:' Note: If both options are added to the List-Unsubscribe header, Gmail will use the method specified first.

Before Your First Mailing

• Create Email Profiles (Templates > Email Profiles)
• Create Default Opts Outs and From Lines (Solution Settings > Config > General Settings)
• Add Test and Seed Lists (Lists)