Contactlab Send SmartRelay
User Guide

Version <202102.1>

Sommario

1. Introduction

Contactlab SmartRelay provides you with the benefits of a professionally managed email service provider platform while keeping the advantages of a simple and standard SMTP interface to create and deliver **transactional messages or bulk campaigns**.

SmartRelay allows relaying email messages through a SMTP connection but it automatically re-envelopes messages injected in the SMTP connection, so that Contactlab manages all the deliverability-related aspects of a SMTP.

SmartRelay works as a gateway between customer's applications – that generate email messages - and the final recipient, accepting messages on a customer-dedicated SMTP listener.

2. Features

2.1 Top-tier outbound MTAs

SmartRelay uses a high-performance email server cluster based on the Momentum MTA, a top-tier platform by Message Systems.

The same infrastructure hosts the inbound SMTP listener (sr-listener.smtp.contactlab.it) where send your messages to SmartRelay.

2.2 SMTP authentication

The Smart Relay SMTP Listener endpoint is sr-listener.smtp.contactlab.it:587.
To guarantee the best security level, the client must use an explicit TLS connection (STARTTLS) and authenticate using the AUTH LOGIN protocol extension.

2.3 Automatic bounce management

Email bounces - delivery errors - must be managed properly in order to meet sender best practices.

MSPs require large senders to follow closely and strictly their own rules, which are frequently updated, including but not limited to:

- Identify bounces for any given recipient address.
- Keep track of bounces across multiple deliveries and over time.
- Properly parse the obscure bounce error message, update the dictionaries when MSP change their infrastructure and act accordingly.

SmartRelay re-enveloping ensures bounces are sent back to Contactlab to be automatically classified and monitored.

2.4 View and click tracking

SmartRelay tracks the open and view action on sent messages, i.e. it can keep track of when and how many times someone opened a message. It is necessary to add an `<img src>` html tag near the end of the original message and immediately before the ending `</body>` tag. The `src` URL points back to a Contactlab service that can track the request.

SmartRelay tracks also links inside a html email. It recognizes valid HTML href tags (e.g. `<a href=”www.example.com”>some text</a>`) and it rewrites it as a unique URL. Clicking on the unique generated link causes the tracking of the action followed by an immediate reply with a standard HTTP 302 redirect to the original destination URL.

View and click tracking are optional and it is not necessary to activate them.

2.5 Unsubscribe option

A quick unsubscribe option is a best practice and required by the law. If your receiver chooses to unsubscribe instead of sending the message to the spam folder, the complaint rate does not increase and reputation is safe. We strongly suggest the use of unsubscribe links in the emails you will send via Smart Relay.

SmartRelay automatically adds the List-Unsubscribe header to the message. This is coded in a way that email clients supporting this header (e.g. Gmail) trigger a special message to a specific subsystem in Contactlab platform. This subsystem identifies the recipient and automatically add it to the blacklist/suppression list.

There is no need to activate this feature – it is automatically performed by the SmartRelay when re-enveloping a message.

2.6 Feedback loop events management

The complaint rate (the ratio total messages over spam/abuse complaints) measured by each MSP is the most important factor in building a reputation.

Some of the major MSPs offer a “FeedBack Loop feed” to qualified professional senders: when a customer clicks the spam button, the sender receives a message through the Feedback loop feed.

This kind of agreement is not usually available to non-specialized senders, as its setup requires extensive qualification checks by the MSP to avoid providing spammers info about their own users.

Contactlab has FBL feeds agreements with all MSPs offering this kind of facility.

FBL feeds for all MSPs are already automatically available for the SmartRelay setup. FBL feeds is automatically managed by Contactlab’s FBL handling subsystem. And, whenever a new FBL feed becomes available, you benefits automatically from it.

2.7 Email authentication

Major MSPs require volume senders (senders wishing to deliver more than a handful of messages every day to the MSP’s users) to adopt one or more email authentication system to help identify the sending entity and apply reputation settings.

Ignoring this requirement means progressively deprioritizing messages from the sender. Unfortunately, email authentication technology is not always easy to understand and implement, and each MSP is free to select the technology they prefer.

Contactlab’s SmartRelay implements all the necessary authentication technologies, including SPF and DKIM signing, to ensure that emails are not deprioritized.

2.7.1 Sender Domain authentication: SPF

Email as a tool is often the victim of scam and spam activities.
To help mailbox providers like Outlook.com, Gmail, and Yahoo! identifying your emails as legitimate, it is advisable to correctly set the DNS of the sender domain.

SPF is a TXT DNS record which lists all IPs that should be considered legitimate senders for a specific domain.

SmartRelay resolves SPF checks on its own Envelope-from header domain (RFC 5321): t.email-guru.it

This means, all messages you end from SmartRelay are SPF compliant without additional effort.

Nevertheless, some mailbox provider may check also your From header domain (RFC 5322) (visible From domain): the domain that the recipient sees in the mailbox.

Therefore, we recommend adjusting the SPF record of your visible from domain by adding email-guru's reference.

Links:

https://www.easy365manager.com/rfc-5321-and-rfc-5322/#:~:text=The%20RFC%205322%20sender%2Frecipient,normally%20shown%20to%20end%20users

How do I know if my sender domain has an SPF Record?
Please use one of many online tools, such as :
https://mxtoolbox.com/
Enter “spf:mydomain.com” and start the DNS query.

How do I add SmartRelay-’s IPs to an existing SPF record?
Normally, it is enough to add “include:t.email-guru.it” to your existing domain (don’t forget to check the syntax!).
Some SPF record can be very complex: we suggest checking the new record on Vamsoft’s online tool:
https://vamsoft.com/support/tools/spf-policy-tester
Please use “93.94.38.32" as a Sender IP Adress and put your sending address in the Sender Address field.
Vamsoft will provide precise and extensive results.

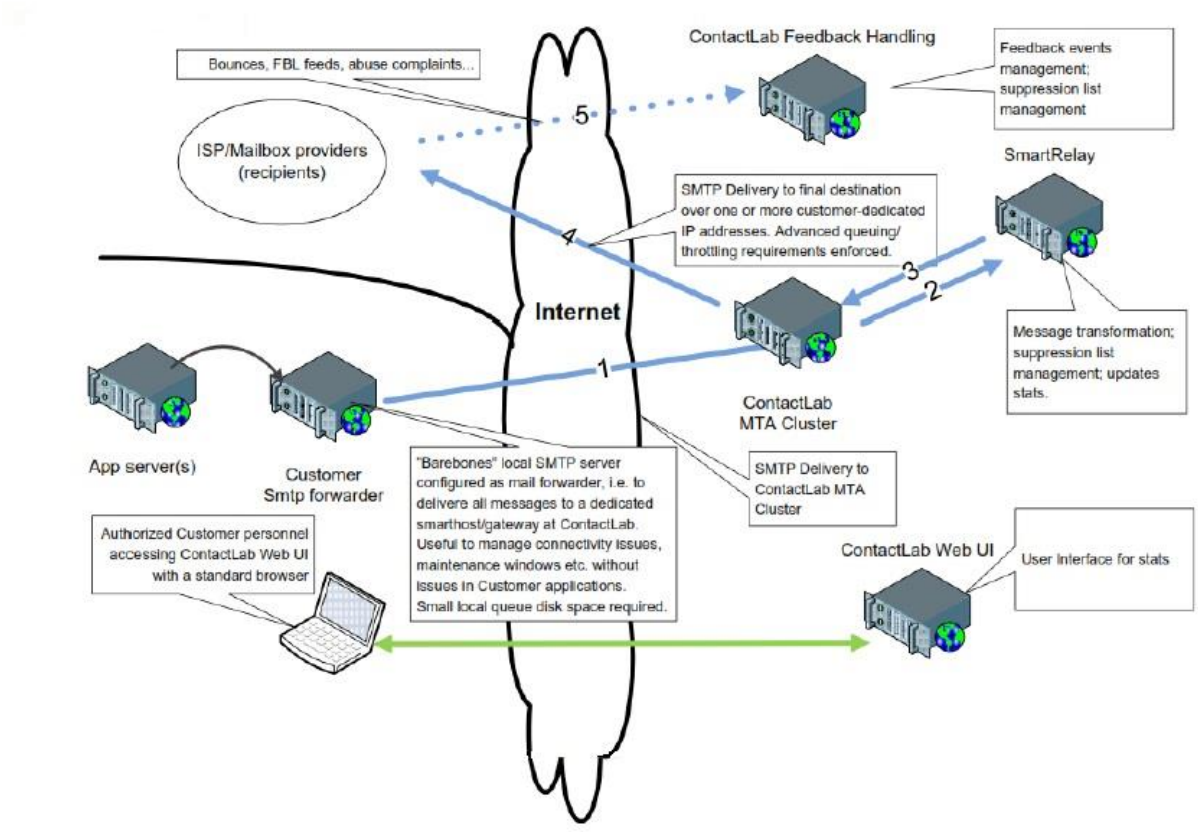
What should I do if I don’t have an SPF record?
If you have no SPF record, you have two options:

- Don’t add any SPF record – just leave it like it is.
- If the sending domain is exclusively used to send emails from SmartRelay, then add the following TXT record for SPF: `v=spf1 include:t.email-guru.it -all`

2.8 Statistics and event data

You will have access to a dedicated web-based and secure User Interface (http://srr.contactlab.it/) with an easy-to-read reporting section where the user can access information like: number of sent messages, bounces, complaints, etc.

3. The complete picture



3.1 SMTP Injection point

The Contactlab MTA Cluster is the entry point into SmartRelay.

SmartRelay has configured SMTP listener that accepts incoming SMTP connections. It is recommended to install a small, forward-only SMTP subsystem in its your infrastructure and let this subsystem accept email messages from the application servers and then just forward all messages to the SMTP injection point.

The following settings are recommended for the SMTP forwarder:

- Configure the SmartRelay listener as a “smarthost” (meaning – every message will be forwarded to it).
- Timeout on SMTP connection should be at least 60 seconds.
- Limit the number of simultaneous outbound SMTP connection to 4
- Set the number of messages for a single connection to a reasonable limit (e.g. 100).[1]

NOTE

- There’s no need to setup the DKIM signature configuration on the SMTP forwarder. The signature will be added to messages by SmartRelay.

Pros and cons of the local SMTP forwarder.

- Pro: easy access to outbound flow for diagnostics and emergency actions (e.g. if the outbound flow is compromised, you can easily “switch it off” while investigating; identifying malfunctioning applications does not require involving our staff).
- Pro: your applications do not need to deal with temporary connectivity issues, since the forwarder takes care of this – SMTP is designed to manage these situations gracefully.
- Pro: Traffic peaks are easily smoothed by the forwarder. If you hits resource limits on the SmartRelay side, Contactlab will “throttle” the entry point down via SMTP 4xx temporary errors. A SMTP forwarder simply backs off and resends the pending messages later.
- Pro: from the security point of view, the setup is much simplified as only one subsystem is allowed to open outbound SMTP connections instead of a potentially large number of application servers
- Con: you need at least one additional server or virtual machine in its farm to perform this duty.
- Con: from the security point of view, you have one additional subsystem to configure and monitor. However, its role and configuration are very simple, if you dedicate the resources to the SMTP forwarder-only role.

3.2 SmartRelay engine

The MTA cluster accepts messages from the SMTP forwarder (or application) and immediately dispatches them to the SmartRelay engine located in the Contactlab’s infrastructure. The SmartRelay engine performs its function, re-envelopes the message and resends it to the MTA cluster.

3.3 Outbound SMTP

The MTA cluster then takes care of delivering the message to its destination, applying all necessary and optional queuing logic according to destination domain requirements, overall throttling agreements etc.

---

[11] Limiting the number of messages delivered in a single connection will usually help your SMTP forwarder manage its own outbound queue more smoothly.

3.4 Feedback handling

Bounces, feedback loop reports, List-unsubscribe processing, abuse complaints, open and click tracking are managed by Contactlab platform with no configuration needed.

4. Limitations

SmartRelay imposes some limitations

- 1 recipient per message e.g. only one “to” address and no “cc” or “bcc” addresses.
- the number of simultaneous SMTP sessions (client connections) to the listener is limited in order to prevent misbehaving or runaway clients consume all available resources. The default configuration for this value is 4 , which should be more than enough for most needs.
- Link tracking, once enabled, is enabled for all the links in the emails.
- Max message size is 200 Kb
- The max number of incorrect login attempts is 3 in 30 minutes (30 minutes of temporary IP blacklisting)

5. Keep high the sender reputation

SmartRelay supports requirements and best practices a good reputable sender should have.

However, you have to cover some important requirements:

- Collect e-mail addresses in a proper way using confirmed opt-in
- Ensure content is perceived as relevant to recipients.
- Ensure not to exercise excessive “communication pressure” – eg. emails frequency.
- Ensure recipients do not feel abused by messages.
- Disclose privacy policies and mailing practices when asking for a subscription.
- Make it easy for recipients to identify and contact the sender.
- Make it easy for recipients to understand why sender is mailing to them.
- Keep track of inactive recipients and gradually stop sending to them to avoid hitting spam-traps when their mailbox becomes inactive for a long time.

6. Dealing with network problems

Network problems occur and it’s important to be able to deal with them. In particular, connections through the Internet are not reliable by definition as no QoS (quality of service) is guaranteed on the public internet.

Contactlab recommends to setup a queue based system locally to your application to be able to deal with network problems. The easiest way by far to setup such a system is to use a local *store-and-forward* SMTP server since SMTP servers are - by definition - queue based systems.

A *store-and-forward* SMTP server can store incoming messages in a local directory (small local queue disk space is usually required) and then forward them all to the SmartRelay. This way you can manage connectivity issues, maintenance window, etc., without issues in its applications, since the SMTP protocol already has all the capabilities to manage temporary issues nicely.

For instance, if you exceeds the agreed rate SmartRelay will “throttle” the SMTP client using the 4xx SMTP error codes – whose meaning is “please retry later”. A standard off-the-shelf SMTP server will automatically store the message in its local storage and retry later – exactly as expected, no need to code it in your application.

7. SMTP-level errors

Generally speaking, SmartRelay is a RFC5321 compliant MTA. Your client (a locally SMTP forwarder, as suggested) must be able to manage RFC5321 standard behavior, most notably, recognizing SMTP reply codes and behave accordingly:

- A *2yz* (200-299) reply is a success code. Operation was successfully completed.
- A *4yz* (400-499) reply is a transient negative completion indicator. The operation should be retried, ideally after some delay. This is gracefully managed by a local SMTP forwarder using the local queue. A SMTP client will have to deal with the logic programmatically.
- A *5yz* (500-599) reply is a permanent negative completion indicator. The operation did not complete successfully and should *not* be retried as it will very likely generate the same error again and again.

Some reply codes which represent interesting cases are listed here below. The list should not be construed as a full list of reply codes.

7.1 452 4.5.3 Service unavailable, recipient per message limit reached

SmartRelay imposes the “1 recipient per message” limitation for injected messages. This is needed to properly manage re-enveloping of the message. If the client is “optimizing” resources by sending identical messages with multiple RCPT TO commands for a single DATA command, you will encounter this reply code. Please send each message with a full MAIL FROM – RCPT TO – DATA protocol sequence.

Note: this has nothing to do with RFC5322. To and/or Bcc headers: those are completely ignored by the MTA. The recipient of a message is always specified in the RCPT TO command exclusively, and it is responsibility of the client to copy recipients to RCPT TO commands.

This is a transient error and as such, sender should simply wait and resend the message.

However, for the retry to succeed, your client should stop sending multiple RCPT TO for a single message, which might require reconfiguration (in the case of a SMTP forwarder) or application code revision (for an application client).

7.2 421 4.4.5 Service unavailable, concurrency limit reached.

SmartRelay imposes limits on the number of simultaneous SMTP sessions (client connections) to the dedicated listener, to prevent misbehaving/runaway clients consume all available resources. The default configuration for this value is 4, which should be more than enough for most needs.

In case the client opens more than the configured maximum number of simultaneous SMTP sessions, you might receive this temporary reply code.

This is a transient error condition - just resend after a while, when a session is again available (a SMTP forwarder will do this automatically).

If there are frequent errors of this kind, it might be some of the clients that are using sessions sub optimally (e.g. they might open a new connection for each message.

7.3 421 4.3.2 Reconfiguration in progress

Contactlab’s MTA infrastructure is fully HA with a cluster of MTA nodes. However, some reconfiguration tasks do require re-initialization of the cluster node. During re-initialization the node will apply the new configuration to new connections, while keeping existing connections active with the old configuration values, waiting for them to complete. In some cases, it might decide it has waited too long and perform a reconfiguration by replying with this transient error.

As with others transient errors, all is needed to recover is to wait some time and resend.

In this specific case, the optimal approach is to terminate the connection and open a new one, but in case this is not possible just follow the usual approach and it will work all the same.

7.4 501 5.5.2 RCPT TO syntax error

The destination email address is invalid according to the RFC2822 Internet Standard.

Please be aware that some systems might allow addresses which are invalid according to the standard.

A typical example is an email address whose *localpart* begins or ends with the character . (dot). This is not allowed by the standard, but some receivers may elect to accept these addresses all the same, sometimes ignoring the additional character, sometimes using it as a part of the unique local part.

The SmartRelay enforces the standard and will refuse to accept an email sent to an invalid address.

This is a permanent error – resending the message will not succeed unless the recipient address is corrected.

7.5 Other Errors

- Generic Error:
  451 - General failure, please retry again or contact the support.
- Sender domain not allowed:
  451 - General failure, this is a private mailfrom domain, usage is not permitted
- Exceeding the purchased package threshold:
  452 - Too many recipients received based on tier configuration.
- Wrong username or password:
  535 - 5.7.8 Sorry. No authentication type succeeded.
- Message size limit exceeded:
  552 - 5.3.4 message size limit exceeded.