Maximizing deliverability for your emails

Overview

Getting your MailUp account properly configured is an important part of maximizing your **deliverability**, that is your ability to deliver your emails in your recipients' inbox. You can think of deliverability as an equation: the result is whether or not your emails end up in the inbox, and many variables affect it. Among them: your reputation as a sender, the content of the message being sent, the level of engagement of the message recipients, the reputation of the sending infrastructure that you are using, etc. etc.

- In the **glossary**, we'll spend a bit of time on email terminology
- We'll review **email authentication methods**, which are an important part of the deliverability equation
- Finally, we'll provide some recommended **configuration steps** to properly set up your MailUp account

Glossary

- **Authentication**
  Email authentication is a collection of techniques aimed at equipping messages of the email transport system with verifiable information. Its purpose is to validate the identities of the parties who participated in transferring a message, as they can modify the message. The results of such validation can then be used in delivery decisions that do not imply any "content filtering" mechanism. There are several authentication methods (FCrDNS, ADSP, SPF, DKIM, DMARC) and each of them go one step further in assessing sender validation and reputation.

- **Commercial email**
  An email message that has as one of its purposes that of participation in a commercial activity. Commercial email typically promotes a product or service.

- **Transactional email**
  A one-to-one email message, usually sent as a result of a specific user's action (e.g. online order). Transactional emails are topically receipts, confirmations, reminders, or any non-commercial email personalized specifically to the recipient. Legally speaking (e.g. CASL), a transactional message that includes commercial content becomes a commercial email (*see above*).

- **Content Filtering / Fingerprinting**
  Techniques aimed at evaluating the content of an email message (specific words, URLs or "chunk") to detect spam messages or spammy patterns. Content filtering is more utilized in the corporate world where system administrators may set content restrictions on what employees can receive. In the consumer world, instead, major ISPs (e.g. Google, Yahoo!, etc.) see authentication, reputation and user interaction (see "Engagement") as more reliable than content filtering in detecting spam, though they may use both.

- **Engagement**
  A "measure" of how subscribers respond to and act on the email messages you are sending to them. Positive engagement - such as views, time spent viewing, clicks, and replies - will likely improve the sender reputation and deliverability. Negative engagement, meant as the absence of any action or, worse, deleting or marking a message as spam, is very likely to cause deliverability issue in the short term.

- **Envelope Sender / Return Path**
  An e-mail address to which asynchronous bounce messages are delivered. As this email address is included in the Header section of the email, its domain takes part in the reputation assessment process.

- **Dedicated IP**
  An IP address used exclusively for one sender or for a portion of its email traffic (e.g.. transactional emails). When a dedicated IP is used, email traffic being sent from that IP address is isolated to that specific sender. Consistent sending frequency - and of course high quality of the messages being sent - are crucial factors in building and maintaining a good reputation for dedicated IP addresses. Lack of sending volume and/or frequency can cause lack of reputation for the dedicated IP, which can lead to deliverability issues. For this reason, a dedicated IP address may or may not be a recommended solution.

- **Shared IP**
  A group of IP addresses used for multiple customers that share common reputation metrics and allow them - as a whole - to maintain a consistent sending frequency.

- **Rate limiting / Throttling**
  Rate limiting is the process that ISPs use to delay the delivery of unwanted (or unknown) email, filter spam, and ensure that wanted (e.g. transactional) emails reach the inbox in a timely manner. Each ISP has its own sending limits on a per-hour and/or per-day basis, and they can throttle the sending volume when it’s too high or too low.

- **Domain / Apex domain**
  The right portion of the domain used by a sender when sending emails (e.g. mycompany.com). It is the root of all reputation and authentication mechanisms, and should be directly linked to the sender's corporate web site or brand identity.

- **Subdomain**
  A lower-level domain. If *mycompany.com* is the top-level (apex) domain, *news.mycompany.com* is a subdomain of it. Since usually the apex domain is already configured to properly serve a sender's corporate web site, and any modifications to it could have unwanted side effects, it is usually recommended that a sender create subdomains to be used for email messaging purposes (3rd level domains such as *news.mycompanyname.com* and 4th level domain such as *bounce.news.mycompanyname.com*). The choice of domain, sub-domain, and naming conventions is important because it can have a significant effect on how ISPs and anti-spam authorities will consider the email stream. Please see *Configuration steps* below for more information.

- **Web interface domain:**
  A subdomain that will be used:

  - in all tracked links in your email messages;
  - in the URL of the Web version of the message;
  - in the URL of all Web pages used by the system (e.g. subscription confirmation landing page);
  - in your MailUp admin console URL.

Email authentication methods

1. **Sender Policy Framework (SPF):**
   SPF (Sender Policy Framework) is one of the ways to authenticate email communication. Some information is added to your Web domain settings indicating that certain systems are authorized to send email on your behalf. Adding SPF authentication can increase your deliverability. That is: the percentage of your messages that are delivered to in the Inbox instead of the Spam folder. In more detail, SPF provides a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorized by that domain's administrators. The list of authorized sending IPs for a domain is published in the Domain Name System (DNS) records for that domain in the form of a specially formatted TXT record (see using SPF authentication with MailUp).

2. **DomainKeys Identified Mail (DKIM)**:
   DKIM is one of the ways to authenticate email communication by adding an encrypted signature to your emails. Some information (our DKIM public Key) is added to your Web domain settings, and a specific signature is added to all the emails that we send for you. This signature is encrypted based on some elements of the email being sent and, for this reason, it is unique for each email. When the receiving mail server analyzes your email, it will decrypt the signature using the public key mentioned above and It will generate a new hash string based on the same elements. If the decrypted signature matches the newly generated hash string then the email is considered DKIM authenticated. An example of DKIM signature is the following:

   ```
   DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=transactional; d=mailup.com;
    h=From:To:Date:Subject:MIME-Version:Content-Type:List-Id:List-Unsubscribe:Message-ID; i=news-
   it@mailup.com;
    bh=eFMbGLxi/7mcdDRUg+V0yHUTmA1F4EXExVBQxIxBr2I=;
    b=ra3pGFHHvCr9OZsm9vnOid........Yj00/+nTKs=
   ```

   If the message has a valid signature (it is not forged), the signing domain, identified by the d= tag will tell the receivers who you are and they will handle your mail accordingly. Reputation assessment systems will look at the reputation of the signing domain and decide whether place the email in the inbox or in the spam folder based on that assessment.

3. **Domain-based Message Authentication, Reporting and Conformance (DMARC)**:
   DMARC is a method of email authentication focused on mitigating email-based phishing. It allows a domain owner and sender of email messages to ask mailbox providers not to deliver unauthorized messages that appear to have been sent from the same domain.This helps in the prevention of phishing schemes and spoofing attacks.

   Technically speaking, DMARC – which stands for Domain-based Message Authentication, Reporting & Conformance – is a system that builds on the DKIM and SPF authentication protocols to help receiving servers (e.g. Gmail, Yahoo!, Hotmail, etc.) know what to do when a message cannot be authenticated. It does so by allowing the sender of an email to publish a "policy" on which mechanism (DKIM, SPF or both) is employed when sending email, which will instruct how email receivers should deal with failures (monitor, send to spam or reject the messages).
   Additionally, it provides a reporting mechanism of actions performed under those policies. It thus coordinates the results of DKIM and SPF and specifies under which circumstances the FROM. which is often visible to end users, should be considered legitimate.

   For more, please see to using DMARC with MailUp.

4. **Forward-confirmed reverse DNS (FCrDNS)**:
   Also known as full-circle reverse DNS, double-reverse DNS, or iprev, FCrDNS is a networking parameter configuration in which a given IP address has both forward (name-to-address) and reverse (address-to-name) Domain Name System (DNS) entries that match each other. This is the standard configuration expected by the Internet standards supporting many DNS-reliant protocols and It is recommend as a best practice. A FCrDNS verification can create a weak form of authentication that there is a valid relationship between the owner of a domain name and the owner of the network that has been given an IP address.
5. **Author Domain Signing Practices (ADSP):**
   ADSP is an optional extension to the DKIM e-mail authentication scheme, whereby a domain can publish the signing practices it adopts when relaying mail on behalf of associated authors. It is a way to tie the DKIM signing domain with the domain in the email address in the *From:* header of a message (also known as the "author domain"). To create that connection, a domain owner publishes an ADSP record in the DNS, containing a policy statement about the mail sent from that domain. A policy of "all" is intended to convey to receiving

systems that all of their mail is signed with DKIM, but does not make any request about what to do with unsigned mail. A policy of "discardable" requests that unsigned messages be discarded. ADSP never achieved widespread adoption and in 2013 it was demoted to "historic". It has been superseded by DMARC.

Authentication on custom domains

Each MailUp account comes with authentication enabled by default (FCrDNS, SPF, DKIM), but on domains owned by us and directly associated with our sending infrastructure. These domains - by definition - are not related with the sender's brand identity. Even though the default settings are enough in terms of email authentication, some senders may need additional configurations (e.g. DMARC) and branding by using a custom domain.

Notes:

- Emails will appear to come directly from their domain, instead of from our servers.
- Use of a custom domain is mandatory for enhanced authentication settings such as DMARC.
- Custom DKIM signatures and DNS settings are needed, which require that the sender has full access to their domain's DNS records.
- The Delivery+ service is included in ENTERPRISE Edition

Configuration steps

1. **Pick the FROM domain**
   Which domain will you be using to send emails with MailUp? Your top-level domain (i.e. the *apex domain* as discussed above) or a subdomain (e.g. *news.mydomain.com*)? In the first scenario, the FROM EMAIL would be something like *updates@mydomain.com*, whereas in the second it would be something like *updates@news.mydomain.com*. The decision should be based on whether you have access and can modify the DNS records of that domain. Check with the person in your organization that has access to your domain management system to find the answer. In the examples below we are assuming that the sending domain corresponds to the apex domain (*mydomain.com*). If you cannot modify the DNS records of your apex domain, then you will need to set up a subdomain (eg *news.mydomain.com*) and refer to that one (in place of *mydomain.com*) in the steps outlined below.

2. **Verify your FROM EMAIL**
   Now that you have picked the FROM domain, create a FROM EMAIL under that domain, and verify it in your MailUp account. To prevent abuse, MailUp requires that the FROM EMAIL is verified before it can be used. Verification is very simple: MailUp will send a verification message to the provided FROM EMAIL address, and you will need to click the link contained in the message. You can verify the FROM EMAIL when you configure a List in your MailUp account, when you set up a new mailing or when you add a new From email in Senders authentication page.

3. **Configure the SPF record for the sending domain**
   Adding SPF authentication is easy. Here is what you need to do:

   - Contact your Web hosting company, domain registrar, or network administrator that manages this domain
   - Tell them that you need to make a change to the DNS (Domain Name System) records
   - If you are not already publishing an SPF record, ask them to add the following TXT record:

     v=spf1 include:musvc.com ~all

   - If you already have an SPF record in place (e.g.: you have a TXT record starting with v=spf1) then you should only add the "include:musvc.com" before the final "all" keyword

     Example: v=spf1 include:mydomain1.com include:mydomain2.com include:musvc.com ~all

   - Wait 24-48 hours: it takes a bit of time to changes to the DNS to propagate around the Internet
   - Run the SPF test in Senders authentication to confirm that the SPF record has been successfully updated.

4. **Enable DKIM authentication**
   Adding DKIM authentication is easy. Here is what you need to do:
   - Contact your Web hosting company, domain registrar, or network administrator that manages this domain
   - Tell them that you need to make a change to the DNS (Domain Name System) records
   - Ask them to create the following two CNAMEs (replace "mydomain.com" with your domain)

     `(1) ml01._domainkey.mydomain.com`

   - ... and point it to

     `ml01.dkim.musvc.com`

     `(2) ml02._domainkey.mydomain.com`

   - ... and point it to

     `ml02.dkim.musvc.com`

- If a CNAME cannot be created, you may also establish DKIM authentication by adding the following TXT records to the DNS settings. Please contact us for additional details

- Wait 24-48 hours: it takes a bit of time to changes to propagate around the Internet
- Run the DKIM test in Senders authentication to confirm that the CNAMEs have been successfully updated.

5. **Configure a Web interface domain (optional)**
   If you wish to use a custom Web interface domain (see the *Glossary* above for a definition), create a C-NAME in your domain management system (e.g. *news.mydomain.com*) and point **c.mailup.com**
   For more information, please see MailUp account settings. Please note that this configuration is available only for PRO and ENTERPRISE clients.

6. **Configure a custom Envelope Sender (optional)**
   Using a custom Envelope Sender (see the *Glossary* above for details) you can to "align" it with the FROM EMAIL address, which allows for more advanced sender configurations, as mentioned above. This address can be any email account of your choice under a subdomain as the one used for the FROM EMAIL (e.g. if the FROM EMAIL is news@mydomain.com the Envelope Sender could be bounce@bounce.mydomain.com). In order for the MailUp system to be able to process bounces, it will need to access sent to that address.
   Create two DNS records as follows:
   1) Type: MX
   Name: bounce.mydomain.com
   Value: mx01.musvc.com
   Priority:10

   2) Type: TXT
   Name: bounce.mydomain.com
   Value:"v=spf1 include:musvc.com ~all"

   For more information regarding the second record(SPF) please see this page.

   > ⚠ By modifying the MX record, MailUp will take control over the email management for that domain that will be handled by the platform. Previously created accounts will no longer be able to send and receive emails.

7. **PTR of SMTP servers (For dedicated IPs):**
   If your email streams will be delivered through dedicated SMTP servers, each one of them should have a PTR aligned with the base host domain. Example:

   ```
   mx67202.mydomain.com A 93.174.67.202
   mx67203.mydomain.com A 93.174.67.203
   ```

   Each PTR should have the same SPF / Sender ID records as the sending domain:

   ```
   mx67202.newsletter.mydomain.com TXT v=spf1 include:musvc.com ~all
   mx67202.newsletter.mydomain.com TXT spf2.0/pra include:musvc.com ~all
   ```

8. **Enable DMARC**
   Since DMARC is built upon SPF and DKIM all the previous steps are required before enabling DMARC.

   The proper TXT record (_dmarc.mydomain.com) should be added to the DNS settings for your sending domain.
   It can change depending on what you want your DMARC policy to be.

   A simple DMARC record is the following: v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc.rua@mycompany.com; ruf=mailto:auth-reports@mycompany.com.
   where:
   * **v** is the version, DMARC1 is the only version available at the moment.
   * **p** is the policy. Allowed values are *none* (take no action, just collect data and send reports) *quarantine* (treat with suspicion unqualified mail) *reject* (block any unqualified mail for the domain)
   * **pct** is the percentage of non-aligned messages that should be rejected (from 1 to 100 where 100 means all the messages)
   * **rua:** Send aggregate reports to this address (should be closely monitored)
   * **ruf:** Send forensic (detailed) reports to this address.

   Note that the email addresses that receive the aggregate and detailed reports (“rua” and “ruf”) can be on any domain, not necessarily the domain used for the authentication, for reporting purposes only.

   We strongly suggest ramping up DMARC use slowly by using the p=none policy at first. Monitor your traffic and look for anomalies in the reports (eg.: messages that are not yet being signed)
   Then, once you have verified that all legitimate messages are correctly being authenticated, move to "quarantine."
   Review the results again (look also in your spam folder) and when you're absolutely sure all of your messages are signed, change the policy setting to "reject" to make full use of DMARC.

   You can also leverage the pct tag to sample your DMARC deployment. If you want to be extremely conservative, after moving to the quarantine policy, you may start with pct=1 and then move to 10, 25, 50, 100...