Improve Sassie Email Deliverability

Last review: May 4, 2023.

Improve Sassie Email Deliverability

This guide instructs how to improve deliverability for email messages sent by Sassieshop's email servers. The goal is to set SPF, DKIM, and DMARC policies in a way to allow or at least be friendly to our email servers' IP addresses, which is necessary when we send messages using the customer's domain name.

SPF

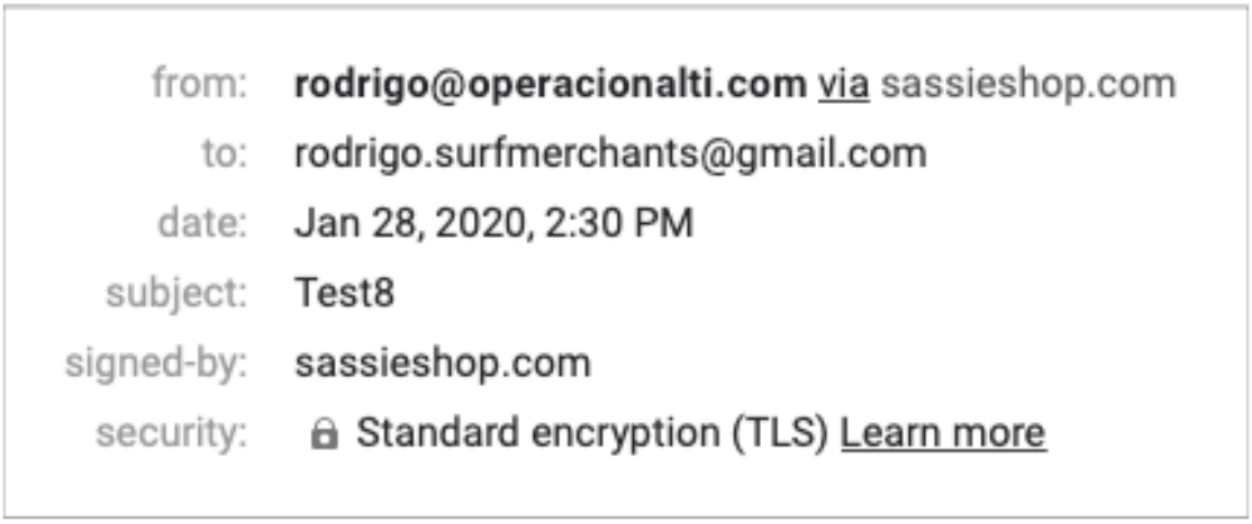
SPF records are used to define a policy of who is allowed to send emails by a domain.
If a client wants to see its own domain in the From address on email messages sent by Sassie, they must allow our email servers' IP addresses in its SPF DNS record, for instance, taking "operacionalti.com" as the customer's domain name:

```
operacionalti.com IN TXT “v=spf1 mx a include:_spf.sassieshop.com
~all”
```

If you already have a SPF record set for your domain, you just have to add the "include:_spf.sassieshop.com" before the "~all" or "-all".

DKIM

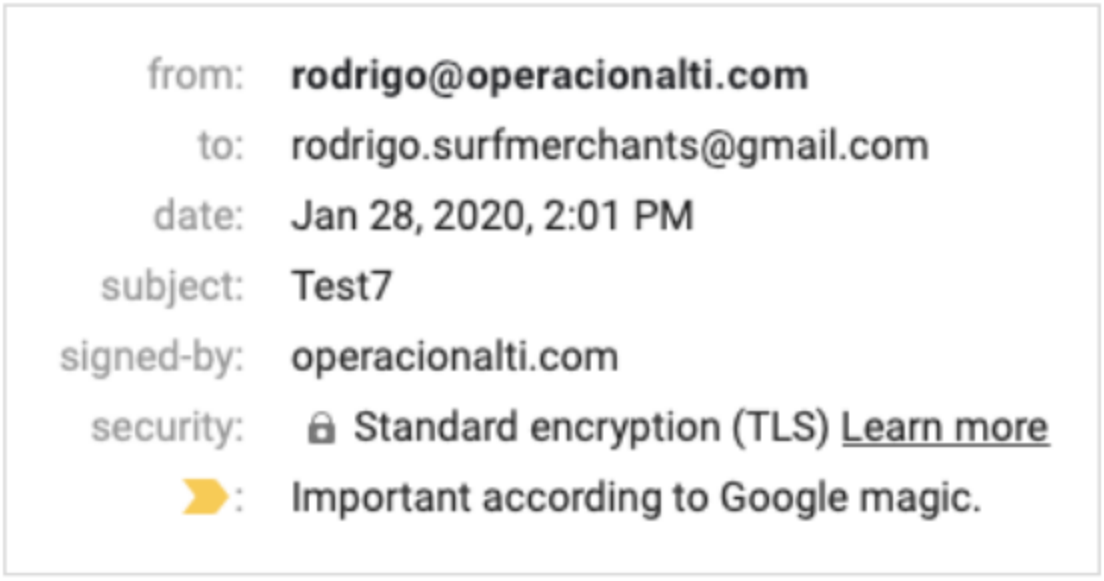
DKIM makes it possible for receivers to verify if a message was sent by the owner of a domain or by someone authorized.
We are already signing email messages sent through our email servers.
Taking `operacionalti.com` again as the customer's domain, the messages will be received like this:



It was sent by an @operacionalti.com address, via sassieshop.com, and signed by sassieshop.com domain, which is compliant to DKIM policy, but might still be rejected depending on your DMARC policy.

Custom signatures

Taking operacionalti.com again as the customer's domain, received messages will look like this:



It was sent and signed by an operacionalti.com address and won't be denied by the recipient even if the DMARC policy is set to reject messages that are not strictly aligned to DKIM.

If you want your messages to be signed like that, follow the instructions below.

Create a CNAME record for DKIM

The following record must be created in the admin panel you use to manage your domain:

```
sassieshop._domainkey.operacionalti.com. IN CNAME
dkim.sassieshop.com
```

The only thing that must be changed is the domain address. The "sassieshop._domainkey" and the "dkim.sassieshop.com", as the CNAME record type, must remain.

DMARC

DMARC policy specifies which action to take when a message is not compliant to DKIM or to SPF policies.
Our recommendation is that our customers set their DMARC policy as following:

```
_dmarc.operacionalti.com. IN TXT "v=DMARC1; p=none; sp=none;
adkim=r; aspf=r;"
```

- `p=quatantine`: means that if a message fails to complain about either DKIM or SPF policies it will be put into the **spam** box.
- `sp=none`: no policy is defined for subdomains.
- `adkim=r`: DKIM alignment is set to relaxed (default). Allows Sassie's email servers to sign messages for your domain.
- `aspf=s`: means that SPF alignment is set to `strict`. Sassie will be able to send mails using your domain name, but it's necessary to set Sassie's IP addresses in your SPF DNS record first, adding the "`include:_spf.sassieshop.com`".

References

RFCs:

- SPF
- DKIM
- DMARC

Tools used for testing

- Test DKIM, SPF, DMARC, DomainKey, RBL - Online Test Tool
- Newsletters spam test by mail-tester.com