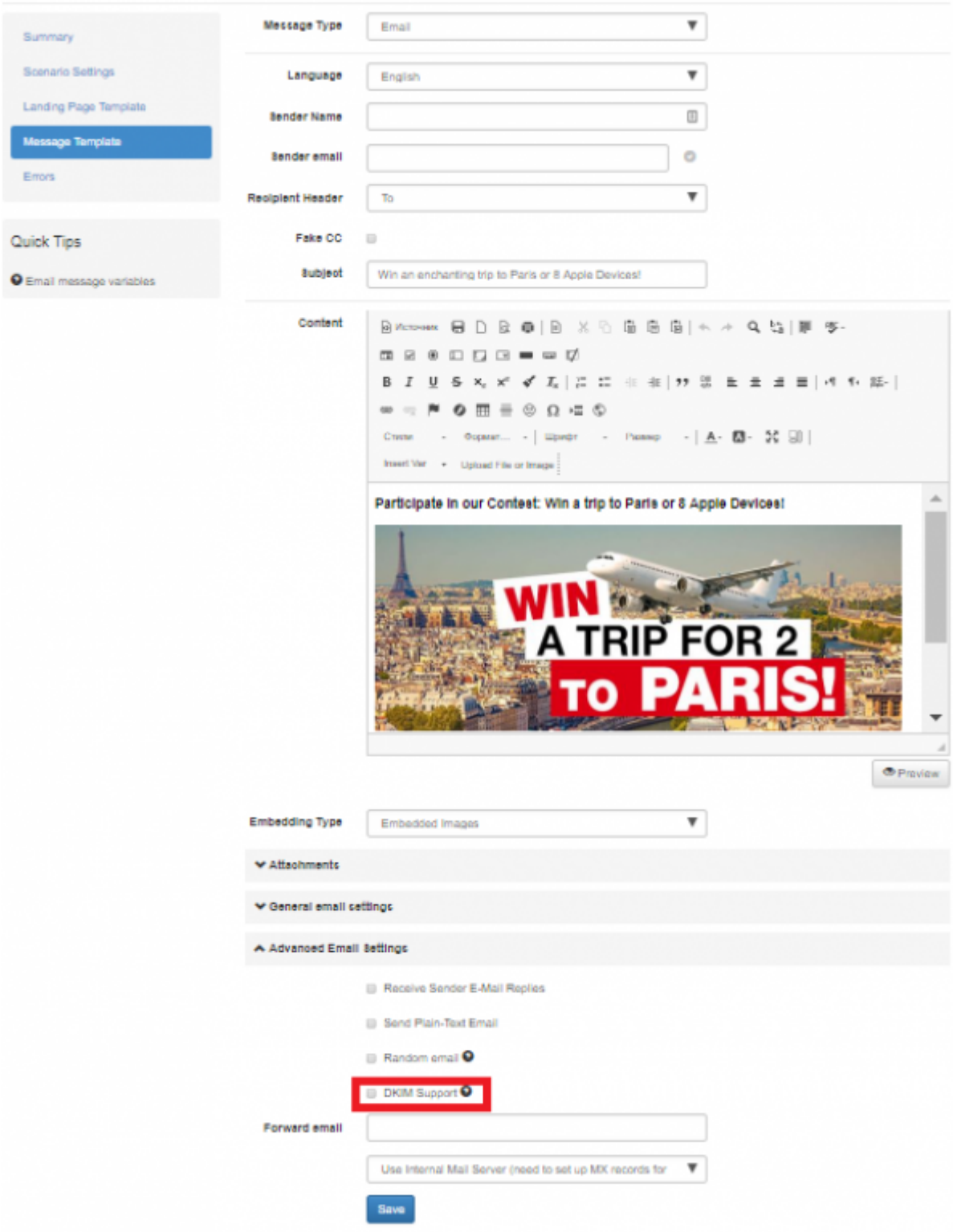
DKIM Background Info:

DKIM attaches a new domain name identifier to a message and uses cryptographic techniques to validate authorization for its presence. The identifier is independent of any other identifier in the message, such in the author's From: field. DKIM is a way of 'signing' emails to prove they came from you. It is a form of email authentication that works via a digital signature and makes it easier to identify spoofed emails. The sending mail server signs the email with the private key, and the receiving mail server uses the public key in the domain's DNS information to verify the signature. One domain can have several DKIM keys publicly listed in DNS, but each matching private key is only on one mail server. When you send emails through the LUCY mail server and have this option enabled, they will be automatically signed.

Setup DKIM in LUCY

Step 1: Within the message template click on DKIM support and save the changes. A DKIM info box will appear:



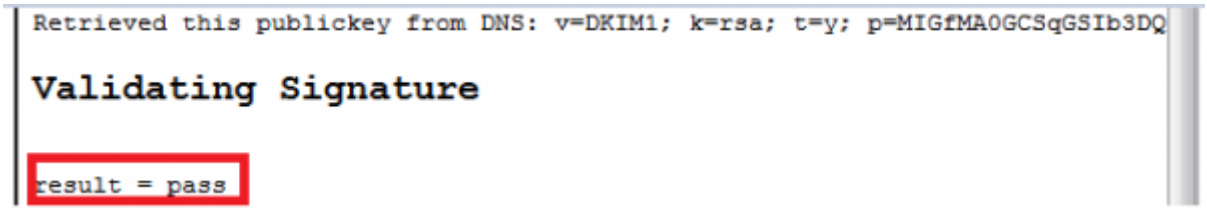
Step 2: Then copy the key and create an according DNS entry. Here is how the correct DNS entry looks like with namecheap.com:

Other configuration links for different providers:

- 1&1: http://help.1and1.com/domains-c36931/manage-domains-c79822/dns-c37586add-or-remove-txt

-records-a792509.html
- Bluehost: https://my.bluehost.com/cgi/help/559
- Cloudflare: https://support.cloudflare.com/hc/en-us/articles/200168696-How-do-I-add-DKIM-records-
- Dreamhost: http://wiki.dreamhost.com/DKIM
- Hostgator: http://support.hostgator.com/articles/hosting-guide/lets-get-started/dns-name-servers/manage-dns-records-with-hostgatorenom
- HostMonster: https://my.hostmonster.com/cgi/help/559
- Hover: https://help.hover.com/entries/21204757-how-to-edit-dns-records-a-cname-mx-txt-and-srv
- Namecheap: https://www.namecheap.com/support/knowledgebase/article.aspx/9214/31/email-authentication-tool-in-cpanel-spf-records
- Network Solutions: http://www.networksolutions.com/support/how-to-manage-advanced-dns-records/

Step 3: Validate your settings. Add a mail from a site like http://dkimvalidator.com/ into your DKIM test recipient group, then start the campaign with that group and analyze the results on http://dkimvalidator.com/. If you configured LUCY and the DNS entry correctly, you should see a status like in the following screenshot:



Note: Lucy sends out DKIM-signed emails with "mail.domainkey_" part built-in and before LUCY 3.2 there is no configuration option to change that. Same for the DKIM header, which is fixed.

DKIM Header Explanation

Here is an example DKIM signature (recorded as an RFC2822 header field) for the signed message:

DKIM-Signature a=rsa-sha1; q=dns; d=example.com; i=user@eng.example.com; s=jun2005.eng; c=relaxed/simple; t=1117574938; x=1118006938; h=from:to:subject:date; b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb av+yuU4zGeeruD00lszZVoG4ZHRNiYzR

Let's take this piece by piece to see what it means. Each "tag" is associated with a value.

- b = the actual digital signature of the contents (headers and body) of the mail message
- bh = the body hash
- d = the signing domain
- s = the selector
- v = the version
- a = the signing algorithm
- c = the canonicalization algorithm(s) for header and body
- q = the default query method

- l = the length of the canonicalized part of the body that has been signed
- t = the signature timestamp
- x = the expire time
- h = the list of signed header fields, repeated for fields that occur multiple times

We can see from this email that:

- The digital signature is dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR. This signature is matched with the one stored at the sender's domain.
- The body hash is not listed.
- The signing domain is example.com.This is the domain that sent (and signed) the message.
- The selector is jun2005.eng.
- The version is not listed.
- The signing algorithm is rsa-sha1. This is the algorith used to generate the signature.
- The canonicalization algorithm(s) for header and body are relaxed/simple.
- The default query method is DNS. This is the method used to look up the key on the signing domain.
- The length of the canonicalized part of the body that has been signed is not listed. The signing domain can generate a key based on the entire body or only some portion of it. That portion would be listed here.
- The signature timestamp is 1117574938. This is when it was signed.
- The expire time is 1118006938. Because an already signed email can be reused to "fake" the signature, signatures are set to expire.
- The list of signed header fields includes from:to:subject:date. This is the list of fields that have been "signed" to verify that they have not been modified.