

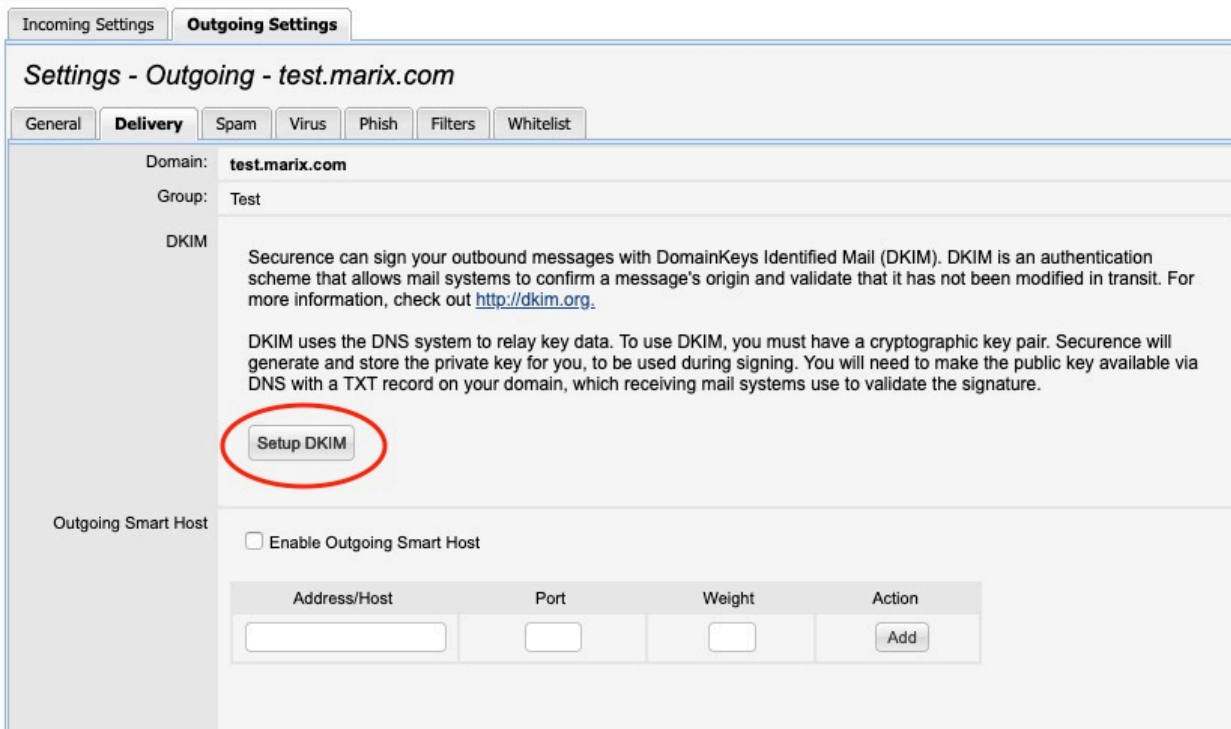
Using DKIM to sign your outbound mail

Securence can sign your outbound messages with DomainKeys Identified Mail (DKIM). DKIM is an authentication scheme that allows mail systems to confirm a message's origin and validate that it has not been modified in transit. DKIM signing is a strongly recommended email practice. Along with SPF, DKIM is an essential part of protecting your domain from phishing and impersonation attacks.

DKIM uses the DNS system to relay key data. To use DKIM, you must have a cryptographic key pair. Securence will generate and store the private key for you, to be used during signing. You will need to make the public key available via DNS with a TXT record on your domain, which receiving mail systems use to validate the signature.

Locating your domain's DKIM configuration

1. Login to the Securence admin portal (<https://admin.securence.com>).
2. On the Home screen, click the domain you wish to configure.
3. Select the *Outgoing Settings* tab, then *Delivery*.
4. Under the *DKIM* section, click **Setup DKIM**.



The screenshot shows the 'Settings - Outgoing - test.marix.com' page in the Securence admin portal. The 'Outgoing Settings' tab is selected, and the 'Delivery' sub-tab is active. The 'DKIM' section is expanded, displaying explanatory text about DKIM and a 'Setup DKIM' button, which is highlighted with a red circle. Below the DKIM section, there is an 'Outgoing Smart Host' section with an unchecked checkbox and a table for adding hosts.

Address/Host	Port	Weight	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Setting up DKIM for your domain

After clicking the **Setup DKIM** button, you will be ushered through a couple short steps to setup the cryptographic key pair for your domain, and enable DKIM signing in Securence.

1. *Choosing a key length.*

The recommended length is 1024 bits, which provides necessary security and maximum compatibility with existing DNS providers. For advanced setups, a 2048 bit option is available. However, this requires a TXT record that may not be supported by your DNS provider. Before choosing 2048 bits, make sure your DNS supports it and that you understand how to configure TXT records exceeding the 255 character limit.

2. *Choosing a Selector.*

A DKIM Selector is simply a name for the key which becomes part of the DKIM domain record. For example, you may choose to enter "securence" or "mail" or "201907".

3. *Add a TXT record to your DNS*

You will need to add a TXT record containing the public key. Copy the DKIM data provided by the setup wizard in Securence, and paste it into your DNS settings under the appropriate subdomain. For example, if you chose "securence" as your selector, you would add a TXT record under **securence._domainkey.yourdomain.com**.

4. *Validate the TXT record.*

From within Securence, click the **Validate** button. Securence will perform a DNS lookup to confirm that the record exists and is formatted properly.

DKIM Setup - Generate

1. Choose a key length.

The recommended length is 1024 bits, which provides necessary security and maximum compatibility with existing DNS providers. For advanced setups, a 2048 bit option is available. However, this requires a TXT record that may not be supported by your DNS provider. Before choosing 2048 bits, make sure your DNS supports it and that you understand how to configure TXT records exceeding the 255 character limit.

2. Choose a Selector.

A DKIM Selector is simply a name for the key which becomes part of the DKIM domain record. For example, you may choose to enter "securence" or "mail" or "201907".

Key Length (bits):

Selector:

Next

Close

1 / 3

DKIM Setup - Validate

Update DNS TXT Record

Fully qualified TXT domain:

securence._domainkey.test.marix.com

TXT record value:

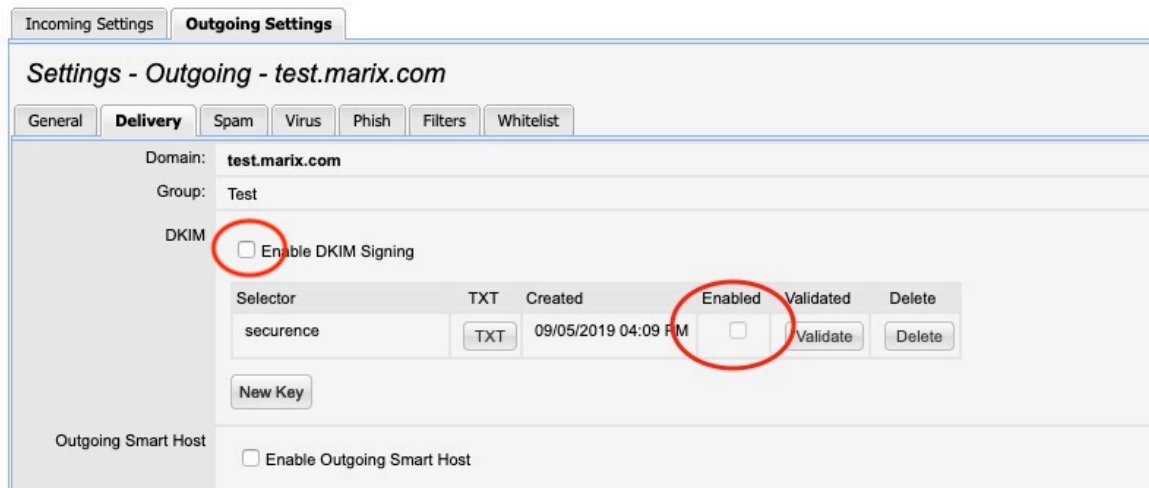
```
v=DKIM1; k=rsa;
p=MIGfMA0GCQsGSlb3DQEBAQUAA4GNADCBiQKBgQCq9h/Foh8Z3ahNm3ITjhtAKK7z89dQ9afizr/eU
FfSa4RdurM1KKAoOu/53FnPDB1480w5uHAwwSnNpZa/BgQicIBOUtpm8t8kHr0mmHcVdmmPRsln+M7X
61w7usJkIBRvCIVAsp37Hoq84ybFN1Y1ZwZjmpiMs5z5BCpTFJwIDAQAB
```

* Please enter the above information into the TXT record for your domain's DNS settings. Click the 'Validate' button to confirm the settings have been entered correctly.

Validate

Close

2 / 3



5. Enable DKIM signing.

Check “Enable DKIM Signing” under the Outgoing Settings for your domain to start signing. You must also have at least one of your keys enabled for signing. Make sure your desired signing key has the “Enabled” box checked in the list.

If you leave the setup wizard without validating your DNS, the key will still be securely stored. You may return later and click the **Validate** button for the key you wish to finish setting up. You will not be able to enable a key for signing until it has been successfully validated.

FAQs

Q: How do I test to make sure it's working properly?

A: You can test your DKIM setup at <http://www.appmaildev.com/en/dkim/>

If you have a Gmail account to test with, send a message to it and follow the instructions under “Use Gmail to test DKIM”. Otherwise, you can click the “Next Step” button and send a message to the temporary email address provided. Wait for it to be received and the DKIM results will be displayed.

Q: Can I sign with multiple DKIM keys?

A: Yes. DKIM allows messages to be signed with multiple keys from multiple domains. A message may be signed by multiple domains or by multiple keys owned by the same domain. This is useful when testing different key lengths or when cycling out of an old key in the process of issuing new keys. Simply check the “Enabled” box in Securrence for each key that you want to use. A separate signature will be generated for each enabled key.