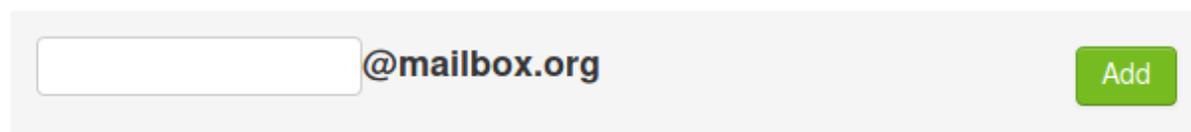# Using e-mail addresses of your domain
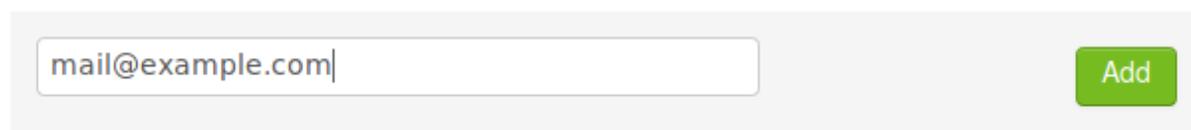
You can use mailbox.org with individual domains. However, there are a few points you need to keep in mind, so please read this article carefully.

Note the following requirements:

- You still need a normal mailbox.org account with your mailbox.org e-mail address.
- If you registered your own domain somewhere in such a way that it belongs to you, you can view the MX records in the DNS data of your domain on mailbox.org.
- In addition, you need to store a mailbox.org security key in the DNS data so that we know that the domain belongs to you. We will explain the details in a moment.
- Once this has been done, you can create other e-mail addresses as aliases for your mailbox.org account. You continue to log in using your usual mailbox.org e-mail address; however, this account now receives e-mails with the created e-mail addresses of your own domain and you can select the created aliases as the sender when sending e-mails.
- All mailbox.org accounts have their own, individual security key. ***This makes it possible to associate external domains to several mailbox.org accounts, if desired, simply by adding their different security keys to the DNS configuration.***
- It is not possible to use our enforced TLS sending ('@secure.mailbox.org') with your own domains.
- It is possible to use an address from an external domain as your mailbox.org main account.

Step 1: The mailbox.org security key

Log in to your mailbox.org Office and go to mailbox.org Settings in the settings area. The 'Add external addresses' option is available under 'E-mail Aliases'. Enter the desired e-mail address.

Our system then checks the DNS data to see whether this domain already contains the mailbox.org security key. If everything is OK, the alias will be created and can be used instantly. You can then proceed to step 2 of these instructions.

If there is no DNS security key, for example, because this is the first time you are registering an e-mail address of a domain with us, the system presents you with a DNS entry. To set the DNS security key you have to create a subdomain and set the TXT record of this sub-domain. Once you have updated this entry, you can try to register your e-mail address again.

The figure below shows an example:

1. First you have to create the sub-domain "fa938c...XXXXX...f2c554.example.net".
2. Than set the TXT record "c9652...xxxx....115a7" for this sub-domain.

Note: Due to the DNS cache times, it may take several hours before a newly created security key is visible on our systems!

E-mail Aliases

Error: Validation of external domain failed

Please refer to the **detailed notes on using your own domains in our Help section**.

Your mailbox.org Securitycode is:

`fa938c01d██████████████████d129f2c554.example.net.  IN TXT c965215████████████44da4fc110115a7`

By setting this security key, you are confirming that you **have read the Help section**, that you know what you are doing, and that you are aware of the consequences. Only when this security key is entered in the DNS can you return here and set up aliases under your own domains with mailbox.org. Please note that we cannot provide any assistance with the DNS configuration of your domain.

Step 2: Set the correct MX records

When our system finds the mailbox.org security key in the DNS, you can register e-mail addresses as aliases under this domain. Once you have done this and no errors have occurred, you can change your domain's MX records so that they appear on the mailbox.org mail relays. Set the following MX records in the DNS:

```
example.net. IN MX 10 mxext1.mailbox.org.
example.net. IN MX 10 mxext2.mailbox.org.
example.net. IN MX 20 mxext3.mailbox.org.
```

Replace 'example.net' with your own domain.

Note: As soon as your MX records appear on our server, we will receive all of your domain's e-mails. If the target mailboxes were not set as aliases on our end, our system will reject the e-mails with a failure notification ('User unknown')! For this reason, always create mailboxes first and then change the corresponding MX records!

Step 3: Howto set the SPF records

SPF records should be configured in the DNS zone of your web domain. All you need to do is create an "include" statement for the SPF entries of mailbox.org. Add a TXT or SPF record for your domain with the following content:

```
v=spf1 include:mailbox.org
```

As a result, your current configuration will inherit the SPF settings of mailbox.org. That means the IP addresses of our outgoing mail systems (which are used for sending your mailbox.org e-mails) will be passed on automatically. If you use more than one server for sending e-mails, you should extend the statement above to include their IP networks as well.

Please note that we cannot offer any further support for individual SPF setups. Also note that we tend to frown upon the use of "-all" in SPF records, when used for ordinary web domains. This is the reason, why our SPF records are set to "~all". For details on this particular issue, please consult this talk about SPF/DKIM by the Heinlein Support GmbH.

Can I use DKIM?

In order to enable DKIM for your embedded domain, you just need to add the following public keys as records to your DNS server.

If your provider offers a web frontend:

```
Subdomain: MBO0001._domainkey
Ressource Record: TXT
Text:
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2K4PavXoNY8eGK2u61LIQlOHS8
f5sWsCK5b+HMOfo0M+aNHwfqlVdzi
/IwmYnuDKuXYuCllrgnxZ4fG4yVaux58v9grVsFHdzdjPlAQfp5rkiETYpCMZwgsmdseJ4Co
ZaosPHLjPumFE/Ua2WAQQljnnunsM9TONM9L6KxrO9t5IISD1XtJb0bq1lVI/e72k3mnPd
/q77qzhTDmwN4TSNJZN8sxzUJx9HNSMRRoEIHSDLTIJUK+Up8IeCx0B7CiOzG5w
/cHyZ3AM5V8lkqBaTDK46AwTkTVGJf59QxUZArG3FEH5vy9HzDmy0tGG+053/x4RqkhqMg5
/ClDm+lpZqWwIDAQAB
```

If this fails to work, please substitute all in the string above beginning with p=MIIBI.... with the strings below, including the ".

If you need to write it as a bind configuration:

```
MBO0001._domainkey IN TXT ( "v=DKIM1; k=rsa; "
   "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2K4PavXoNY8eGK2u61"
   "LIQlOHS8f5sWsCK5b+HMOfo0M+aNHwfqlVdzi/IwmYnuDKuXYuCllrgnxZ4fG4yV"
   "aux58v9grVsFHdzdjPlAQfp5rkiETYpCMZwgsmdseJ4CoZaosPHLjPumFE/Ua2WA"
   "QQljnnunsM9TONM9L6KxrO9t5IISD1XtJb0bq1lVI/e72k3mnPd/q77qzhTDmwN4T"
   "SNJZN8sxzUJx9HNSMRRoEIHSDLTIJUK+Up8IeCx0B7CiOzG5w/cHyZ3AM5V8lkqB"
   "aTDK46AwTkTVGJf59QxUZArG3FEH5vy9HzDmy0tGG+053/x4RqkhqMg5/ClDm+lp"
   "ZqWwIDAQAB" )
```

In addition to that, we offer a backup key. Please also add this to your configuration.

Web frontend:

```
Subdomain: MBO0002._domainkey
Ressource Record: TXT
Text:
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqxEKIg2c48ecfmy
/+rj35sBOhdfIYGNDCMeHy0b36DX6MNtS7zA/VDR2q5ubtHzraL5uUGas8kb
/33wtrWFYxierLRXy12qj8ItdYCRugu9tXTByEED05WdBtRzJmrb8YBMfeK0E0K3wwoWfhIk
/wzKbjMkbqYBOTYLlIcVGQWzOfN7
/n3n+VChfu6sGFK3k2qrJNnw22iFy4C8Ks7j77+tCpm0PoUwA2hOdLrRw3ldx2E9PH0GVwIM
JRgekY6cS7DrbHrj
/AeGlwfwwCSi9T23mYvc79nVrh2+82ZqmkpZSTD2qq+ukOkyjdRuUPck6e2b+x141Nzd81dI
ZVfOEiwIDAQAB
```

Bind:

```
MBO0002._domainkey IN TXT ( "v=DKIM1; k=rsa; "
   "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqxEKIg2c48ecfmy/+r"
   "j35sBOhdfIYGNDCMeHy0b36DX6MNtS7zA/VDR2q5ubtHzraL5uUGas8kb/33wtrW"
   "FYxierLRXy12qj8ItdYCRugu9tXTByEED05WdBtRzJmrb8YBMfeK0E0K3wwoWfhI"
   "k/wzKbjMkbqYBOTYLlIcVGQWzOfN7/n3n+VChfu6sGFK3k2qrJNnw22iFy4C8Ks7"
   "j77+tCpm0PoUwA2hOdLrRw3ldx2E9PH0GVwIMJRgekY6cS7DrbHrj/AeGlwfwwCS"
   "i9T23mYvc79nVrh2+82ZqmkpZSTD2qq+ukOkyjdRuUPck6e2b+x141Nzd81dIZVf"
   "OEiwIDAQAB" )
```

Optional: DMARC

DMARC specifies how receiving servers verify e-mails send from your domain using our servers.

A DMARC-Entry can look like this:

Record-Type: TXT
Host/Domain: _dmarc.example.com
TTL: 400
Text/Data: v=DMARC1;p=none;rua=mailto:postmaster@example.com;ruf=mailto:admin@example.com

Important options are:

v	protocol-version
ruf	forensic report will be send to:
rua	aggregated report will be send to:
p	how to handle e-mails of main domain

Please note that if the options are set too strict your e-mails may be rejected by the receiving server. Sometimes forwardings can also break a DKIM signature.

If you want to give DMARC a try we recommend to use our example above and check the incoming reports before you further adjust your settings.

Optional: How to enable auto-configuration in e-mail clients

If you would like to use the auto-configuration assistants offered by e-mail clients like Thunderbird or KMail, then you can do so by referring to an autoconfig XML file that is available on our web server. The easiest way to get this done is to add a reference in two particular DNS records for your domain name. These are the CNAME and the SRV records.

Set the following CNAME record to enable automatic e-mail configuration:

```
autoconfig IN CNAME mailbox.org.
```

Set the following SRV record to enable automatic e-mail configuration:

```
_autodiscover._tcp IN SRV 0 0 443 mailbox.org.
```

Alternatively, you can upload an XML file that contains the required autoconfig data to your own web server. Please note the required location and naming conventions: https://autoconfig.example.net/mail/config-v1.1.x...

We have a template for this XML file, which you can simply obtain by opening it with a browser or using either this command:

```
curl -o config-v1.1.xml https://mailbox.org/mail/config-v1.1.xml
```

or that one:

```
wget https://mailbox.org/mail/config-v1.1.xml
```

All you need to do is insert the corresponding entries for <domain>, <displayName> and <displayShortName>. Please see the example below:

```
<clientConfig version="1.1">
  <emailProvider id="mailbox.org">
     <domain>exmaple.net</domain>
     <displayName>example.net  Mailserver (Beschreibung)</displayName>
     <displayShortName>EGCOM (Kürzel, z.B. Initialen)</displayShortName>

     <incomingServer type="imap">
[...]
```

Further Questions – Help and FAQ

I do not have a domain. Can I register one on mailbox.org?

No. mailbox.org is intended for anonymous use. Since we would need your address data for a domain registration, this would be in conflict with our "anonymous use" policy. In addition, mailbox.org works as a prepaid system, and if we were to register domains, the risk would be too great that complications would arise and we would have to delete them at some stage.

Can I take advantage of this offer with domains from other providers?

No. Changing the DNS MX records means that all e-mail traffic runs exclusively through mailbox.org. It is not possible to redirect individual e-mail addresses to us. However, you could still use the option to have e-mail addresses from other providers as senders.

I don't know what the DNS is. What should I change and where and how?

This option requires a certain amount of technical expertise regarding how domains work which includes knowing what DNS is. If you have purchased your own domain, you will probably have done that through a specific provider (registrar). Contact your registrar for help with setting up your DNS for mailbox.org

Can mailbox.org help me solve problems with DNS setup for my own domain?

No. Please contact the provider that you purchased your domain at.

What can I do if I no longer want to run my own domain on mailbox.org?

You can switch at any time. Change your domain's MX records to the desired new provider and don't forget to delete the created aliases from your mailbox.org account.

Can I use catch-all addresses with my own domain with mailbox.org?

Yes, that's possible. Have a look at the article using catch-all alias with your own domain.

Is there a limit to the number of e-mail addresses?

Yes. As far as mailbox.org is concerned, the aliases created under your own domain are normal aliases. The possible number varies depending on the package. Please refer to our table of packages. If you create additional aliases, it may be necessary to switch to a better mail package when your permitted aliases are no longer sufficient.

NOTE: Aliases for username postmaster@, abuse@, hostmaster@ and webmaster@ are not counted and is for free.

Can I remain anonymous while using my own domain name?

Yes. While in principle, a domain name will always allow others to retrieve related ownership information using a registrar website or other whois-database, there is a way to remain anonymous by hiding this information behind a „whois-proxy server".

Many ordinary domain providers in Germany are offering this kind of service to customers. For instance, the company „CPS Datensysteme"
has proxies covering more than 200 different top-level domains:
https://www.cps-datensysteme.de/index.php?id=377&L=1

Internationally, there are a number of reliable (!) providers that allow anonymous domain registration:
https://www.inwx.de/de/offer/whoisprivacy
https://uk.godaddy.com/domainaddon/private-registration.aspx

Can I use this for my organisation/business?

Yes and No. mailbox.org has been designed for use by freelancers or small businesses. If there are several people who want to use email
accounts with the same domain name, each of them will need their own mailbox.org account. For each of these accounts a security key
needs to be added to your DNS entries. Unfortunately shared calendars and address books cannot yet be used in such configurations.

Related Articles

- How to integrate external e-mail accounts
- CalDAV and CardDAV for other devices
- Using e-mail addresses of your domain
- Changing the accounts main e-mail address
- Data Synchronization - Overview