# Setup DNS records for your iRedMail server (A, PTR, MX, SPF, DKIM)

- Setup DNS records for your iRedMail server (A, PTR, MX, SPF, DKIM)
    - A record for server hostname
        - What is an A record
        - How to setup an A Record
    - Reverse PTR record for server IP address
        - What is a reverse PTR record
        - Why do you need a reverse PTR record
        - How to setup a Reverse PTR record
    - MX record for mail domain name
        - What is a MX record
        - How to setup the MX record
    - SPF record for your mail domain name
        - What is a SPF record
        - How to setup the SPF record
    - DKIM record for your mail domain name
        - What is a DKIM record
        - How to setup the DKIM record
    - Register your mail domain in Google Postmaster Tools
    - References

**IMPORTANT NOTE**: `A`, `MX` records are required, `Reverse PTR`, `SPF` and `DKIM` are optional but strongly recommended. All in all, set them all up please.

## A record for server hostname

# What is an A record

`A` records map a FQDN (fully qualified domain name) to an IP address. This is usually the most often used record type in any DNS system. This is the DNS record you should add if you want to point a domain name to a web server.

# How to setup an A Record

- `Name`: This will be the host for your domain which is actually a computer within your domain. Your domain name is automatically appended to your name. If you are trying to make a record for the system `www.mydomain.com`. Then all you enter in the textbox for the name value is `www`.

  **Note**: If you leave the name field blank it will default to be the record for your base domain `mydomain.com`. The record for your base domain is called the root record or apex record.

- `IP`: The IP address of your FQDN. An IP address can be thought of as the telephone number to your computer. It is how one computer knows how to reach another computer. Similar to the country codes, area codes, and phone number it is used to call someone.

- `TTL`: The TTL (Time to Live) is the amount of time your record will stay in cache on systems requesting your record (resolving nameservers, browsers, etc.). The TTL is set in seconds, so 60 is one minute, 1800 is 30 minutes, etc..

Systems that have a static IP should usually have a TTL of 1800 or higher. Systems that have a dynamic IP should usually have a TTL of 1800 of less.

The lower the TTL the more often a client will need to query the name servers for your host's (record's) IP address this will result in higher query traffic for your domain name. Where as a very high TTL can cause downtime when you need to switch your IPs quickly.

Sample record:

```
NAME                TTL     TYPE    DATA


www.mydomain.com.   1800    A       192.168.1.2
mail.mydomain.com.  1800    A       192.168.1.5
```

The end result of this record is that `www.mydomain.com` points to `192.168.1.2`, and `mail.mydomain.com` points to `192.168.1.5`.

# Reverse PTR record for server IP address

## What is a reverse PTR record

PTR record or more appropriately a reverse PTR record is a process of resolving an IP address to its associated hostname. This is the exact opposite of the process of resolving a hostname to an IP address (`A` record). Example, when you ping a name `mail.mydomain.com` it will get resolved to the ip address using the DNS to something like `192.168.1.5`. Reverse PTR record does the opposite; it looks up the hostname for the given IP address. In the example above the PTR record for IP address `192.168.1.5` will get resolved to `mail.mydomain.com`.

## Why do you need a reverse PTR record

The most common use for looking up a PTR record is done by spam filters. Concept behind this idea is that fly by night spammers who send e-mails out using fake domains generally will not have the appropriate reverse PTR setup at the ISP DNS zone. This criterion is used by spam filters to detect spam. If your domain does not have an appropriate reverse PTR record setup then chances are email spam filtering softwares **MIGHT** block e-mails from your mail server.

## How to setup a Reverse PTR record

You would most likely need to contact your ISP and make a request to create a reverse PTR record for your mail server IP address. For example, if your mail server hostname is `mail.mydomain.com` then ask your ISP to setup a reverse PTR record `192.168.1.5` (your internet public IP address) in their revesre DNS zone. Reverse DNS zones are handled by your ISP even though you may have your own forward lookup DNS zone that you manage.

# MX record for mail domain name

## What is a MX record

Mail Exchanger Record or more commonly known as MX record is an entry in the DNS server of your domain that tells other mail servers where your mail server is located. When someone sends an e-mail to a user that exists on your mail server from the internet, MX provides the location or IP address where to send that e-mail. MX record is the location of your mail server that you have provided to the outside world via the DNS.

Most mail servers generally have more than one MX record, meaning you could have more than one mail server setup to receive e-mails. Each MX record has a priority number assigned to it in the DNS. The MX record with **lowest number has the highest priority** and that is considered your primary MX record or your main mail server. The next lowest mx number has the next highest primary and so on. You generally have more than one mail server, one being the primary and the others as backups, only one MX for mail server is OK too.

## How to setup the MX record

If your ISP or domain name registrar is providing the DNS service, you can request them to set one up for you. If you manage your own DNS servers then you need to create the MX records in your DNS zone yourself.

Sample MX record:

```
NAME               PRIORITY     TYPE     DATA
```

```
mydomain.com.   10          mx      mail.mydomain.com
```

The end result of this record is, emails sent to `[user]@mydomain.com` will be delivered to server `mail.mydomain.com`.

# SPF record for your mail domain name

## What is a SPF record

SPF is a spam and phishing scam fighting method which uses DNS SPF-records to define which hosts are permitted to send e-mails for a domain. For details on SPF, please see http://www.openspf.org/

This works by defining a DNS SPF-record for the e-mail domain name specifying which hosts (e-mail servers) are permitted to send e-mail from the domain name.

Other e-mail servers can lookup this record when receiving an e-mail from this domain name to verify that sending e-mail server is connecting from a permitted IP address.

## How to setup the SPF record

A new SPF-record type was recently added to the DNS protocol to support this (RFC4408).

However not all DNS and e-mail servers support this new record type yet, so SPF can also be configured in DNS using the TXT-record type.

Examples:

- SPF record refer to MX record. It means emails sent from all servers defined in MX record of `mydomain.com` are permitted by sender organization.

```
mydomain.com.   3600    IN  TXT "v=spf1 mx
```

```
mx:mydomain.com -all"
```

- or SPF record refer to IP address directly. it means emails sent from specified IP address are permitted by sender organization.

  ```
  mydomain.com.   3600    IN  TXT "v=spf1
  ip4:192.168.1.100 -all"
  ```

`-all` means prohibit all others.

There're more valid mechanisms available, please check OpenSPF web site for more details.

# DKIM record for your mail domain name

## What is a DKIM record

DKIM allows an organization to take responsibility for a message in a way that can be verified by a recipient. The organization can be a direct handler of the message, such as the author's, the originating sending site's, or an intermediary's along the transit path. However, it can also be an indirect handler, such as an independent service that is providing assistance to a direct handler. DKIM defines a domain-level digital signature authentication framework for email through the use of public-key cryptography and using the domain name service as its key server technology (RFC4871). It permits verification of the signer of a message, as well as the integrity of its contents. DKIM will also provide a mechanism that permits potential email signers to publish information about their email signing practices; this will permit email receivers to make additional assessments of unsigned messages. DKIM's authentication of email identity can assist in the global control of "spam" and "phishing".

A person or organization has an "identity" -- that is, a constellation of characteristics that distinguish them from any other identity. Associated with this abstraction can be a label used as a reference, or "identifier". This is the distinction between a thing and the name of the thing. DKIM uses a domain name as an identifier, to refer to the identity of a responsible person or organization. In DKIM, this identifier is called the Signing Domain IDentifier (SDID) and is contained in the DKIM-Signature header fields `d=` tag. Note that the same identity can have multiple identifiers.

## How to setup the DKIM record

- Run command in terminal to show your DKIM keys:

```
# amavisd showkeys
dkim._domainkey.mydomain.com.   3600 TXT (
  "v=DKIM1; p="

"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDYArsr2BKbdhv9efugByf7LhaK"


"txFUt0ec5+1dWmcDv0WH0qZLFK711sibNN5LutvnaiuH+w3Kr8Ylbw8gq2j0UBok"


"FcMycUvOBd7nsYn/TUrOua3Nns+qKSJBy88IWSh2zHaGbjRYujyWSTjlPELJ0H+5"

  "EV711qseo/omquskkwIDAQAB")
```

**Note**: On some Linux/BSD distribution, you should use command `amavisd-new` instead of `amavisd`. if it complains `/etc/amavisd.conf not found`, you should tell amavisd the correct path of its config file. For example:

```
# amavisd -c /etc/amavisd/amavisd.conf showkeys
```

- Copy output of command above into one line like below, remove all quotes, but keep `;`. **we just need strings inside the `()` block**, it's the value of DKIM DNS record.

```
v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDYArsr2BKbdhv9efugBy...
```

**Note**: BIND (The most widely used Name Server Software) can handle this kind of multi-line format, so you can paste it in your domain zone file directly.

- Add `TXT` type DNS record for domain name `dkim._domainkey.mydomain.com`, set value to the line you copied above: `v=DKIM1; p=...`.

  > *WARNING: A usual mistake is adding this DKIM record to domain name `mydomain.com`, this is wrong. Please make sure you added to domain name `dkim._domainkey.mydomain.com`.*

- After you added this in DNS, verify it with `dig` or `nslookup`:

  ```
  $ dig -t txt dkim._domainkey.mydomain.com

  $ nslookup -type=txt dkim._domainkey.foodmall.com
  ```

Sample output:

```
dkim._domainkey.mydomain.com. 600 IN TXT
"v=DKIM1\;p=..."
```

And verify it with Amavisd:

```
# amavisd testkeys
TESTING: dkim._domainkey.mydomain.com       => pass
```

If it shows `pass`, it works.

**Note**: If you use DNS service provided by ISP, new DNS record might take some hours to be available.

If you want to re-generate DKIM key, or need to generate one for new mail domain, please check our another tutorial: Sign DKIM signature on outgoing emails for new mail domain.

## Register your mail domain in

# Google Postmaster Tools

This step is **optional**, but **higly recommended**.

Google Postmaster Tools web site: https://postmaster.google.com, and Postmaster Tools FAQs.

It's very simple: just register your mail domain there, and they'll give you a text record for your DNS so that they can validate the ownership of the domain.

Why use Google Postmaster Tools? Quote from Google Postmaster Tools help page:

> *If you send a large volume of emails to Gmail users, you can use Postmaster Tools to see:*
>
> - *If users are marking your emails as spam*
> - *Whether you're following Gmail's best practices*
> - *Why your emails might not be delivered*
> - *If your emails are being sent securely*

It ***MIGHT*** also help to get you out of the `Junk` mailbox.

If you have trouble in sending email to Gmail (or Google Apps), Google offers some information on best practices to ensure that their mail is delivered to Gmail users: Bulk Senders Guidelines.

You may also submit this form to contact Google: Bulk Sender Contact Form

# References

- http://en.wikipedia.org/wiki/MX_record
- http://www.openspf.org/
- http://www.dkim.org/