

MAIL SERVER DNS RECORDS EXPLAINED

21. September 2020 by Christian Lempa

If you want to run a mail server on the public internet, you need to set up your DNS records correctly. While some DNS records are necessary to send and receive emails, others are recommended to build a good reputation. Why is that so important? Because Spam-Mails are a big problem, most public mail servers just reject mails from servers with a bad reputation. In this article, I explain to you which DNS records you should configure to run a fully functioning mail server with a good reputation.

<https://youtu.be/o66UFsodUYo>

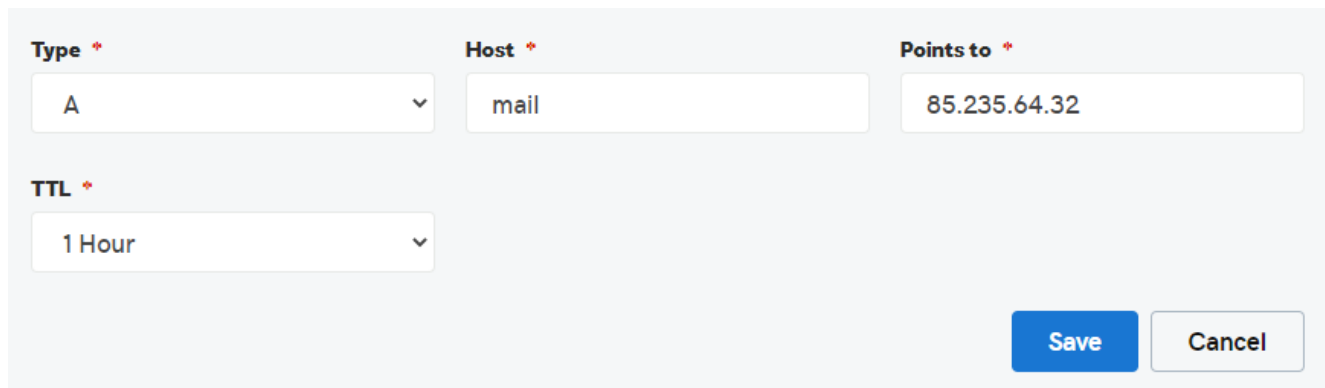
Watch the Video

SET UP AN A RECORD FOR YOUR MAIL SERVER

I strongly recommend adding a separate A record that will resolve to the public ..

address of your mail server. You could use an FQDN, mail.your-domain.com for example. This is also needed when your web server has a different IP address than your mail server.

In the following example, you can see how the mail server's address is configured for the domain the-digital-life.com.



The screenshot shows a DNS configuration interface with the following fields and values:

Type *	Host *	Points to *
A	mail	85.235.64.32

Below these fields is a TTL (Time To Live) field set to 1 Hour. At the bottom right are 'Save' and 'Cancel' buttons.

SET UP AN MX RECORD FOR YOUR MAIL SERVER

The MX record is important when you want to receive emails. This tells everyone which IP address to contact. Let me do a short example. Let's assume you're running a mail server for the domain the-digital-life.com. If someone wants to send you a mail to [christian\(at\)the-digital-life.com](mailto:christian(at)the-digital-life.com), the foreign mail server needs to contact the correct mail server via its IP address. Therefore, the sender's mail server will first look up the MX record (Mail Exchanger) on your DNS server. That tells the sender which mail server is responsible for the domain the-digital-life.com.

The MX record resolves to your mail servers, A record. Enter the mail server's **FQDN (Fully-qualified-domain-name)** that will resolve to the mail server's public IP. In the following example, you can see how the mail server's address is configured for the domain the-digital-life.com.

MX

Host * Points to * Priority *

@ mail.the-digital-life.com 0

TTL *

1 Hour

Save Cancel

SET UP AN RDNS RECORD FOR YOUR MAIL SERVER

The reverse DNS record or also called **PTR (Pointer Resource Record)** is important when you want to send mails. Almost all mail servers check the RDNS record to perform simple anti-spam checks. How does that work? RDNS is just like a DNS query, just backward. The receiving mail server will perform a reverse DNS lookup on your IP address and check if it's matching your mail server's FQDN. If you don't have a matching RDNS record on your public IP address, that looks suspicious. In this case, most mail servers will just reject your mails with an error code PTR 554 or drop them silently.

Note, that your RDNS record is not configured on your DNS server, instead, it's configured on your hosting provider where you got your public IP address from. In the following example, you can see how the mail server's FQDN is configured on my public address.

rDNS

Hier können Sie den rDNS-Eintrag Ihrer eigenen IP-Adressen ändern.

Jede IP löst per rDNS zu einem Host auf. Es ist empfehlenswert Ihre IPs zu einem Hostname z

IPv4-Adresse 85.235.64.32

Hostname mail.the-digital-life.com

SET UP SPF, DKIM, AND DMARC FOR YOUR MAIL SERVER DNS RECORDS

Probably not all mail servers will reject your mails when one of these

records is missing. Nevertheless, you should configure them all to build a good reputation for your mail server. Because some mail servers just reject emails silently without sending you an error code. Do your best efforts to make sure everybody is receiving your emails and set up SPF, DKIM, and DMARC records.

SPF (SENDER POLICY FRAMEWORK)

Why do we need an **SPF (Sender Policy Framework)** record? The problem is that you can send mails with any sender address by modifying the “envelope from”, even if the domain doesn’t belong to you. This is called spoofing and is a common vulnerability. The SPF is a TXT record on your DNS server that specifies which hosts are allowed to send mails for a given domain. When a mail server receives mail that seems to come from your domain, it can check if it’s a valid message. Some mail servers reject mails if they can’t validate that the message comes from an authorized mail server.

To set up your SPF record, create a new TXT record for your domain `v=spf1 ip4:<your-mail-server-public-ip> -all`. In the following example, you can see how the mail server’s SPF record looks for the domain the-digital-life.com



The screenshot shows a form for creating a new DNS record. At the top, it says "TXT". Below this, there are three fields: "Host", "TXT Value", and "TTL". The "Host" field contains an "@" symbol. The "TXT Value" field contains the text "v=spf1 ip4:85.235.64.32 -all". The "TTL" field is a dropdown menu set to "1 Hour". At the bottom right, there are two buttons: "Save" (in blue) and "Cancel" (in light gray).

Host *	TXT Value *	TTL *
@	v=spf1 ip4:85.235.64.32 -all	1 Hour

[Save](#) [Cancel](#)

DKIM (DOMAIN KEY IDENTIFIED MAIL)

SPF is a good way to protect against spoofing, but it has some limitations. **DKIM (Domain Keys Identified Mail)** allows the receiving mail server to check that an email was indeed sent by the owner of that domain. The sending mail server adds a digital signature to every mail that is sent. This DKIM signature is added as a header and secured with encryption. These signatures are not visible to the end-user, it’s all done on the mail servers. The sending mail server generates a random hash value that is encrypted via a private key and adds it to the DKIM signature. The receiving mail server checks if the DKIM signature is valid by obtaining the

corresponding public key on the sender's DNS server.

If you want to add DKIM to your mail server, you first need to create a private and a public key pair. When creating your DKIM key, you also need to configure a DKIM selector on your mail server. Only your mail server should know the private key, don't share this with anyone! Then you need to create a TXT record for the host `<dkim-selector>._domainkey` with the value `v=DKIM1;k=rsa;p=public-key`.

In the following example, you can see how to create a DKIM key on the Mailcow server.

Domain: the-digital-life.com

Key valid
Selector dkim
2048 bit

Private key

v=DKIM1;k=rsa;t=s;s=email;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBGKCAQEA0hAIuskiQf6hDoQY1u0y0E7QaZctw6pYYBksm46875s!htVQsEEx0zshK6TtsLy1DnlwVaSVvt770fBbGL8VpE/CraGxDnfwUCk60Vty8LCv7Cshzr1pX9pXCrc4uHh+ER1hHf+xgc04PKo+AusFwtz/jbk1Vawmvv02GxRIPPYubPN3vmFkX9tIoAUGm8MTX2Yt/kVVGRv1z31rNw19M1uaXVQpxRCbnAkUc7dN6b72z!S0330wLsvFHLcA4EKKSq1Q3d+mpv4+acA/VhqaH86oaq8a5Av30s142jkd7Te6nAtINvz6x905X0Hw1wFXLXR0Pbm+AXo3IwHQIDAQAB

Add ARC/DKIM key

Domain/s
example.org, example.com
Select domains with missing keys

Selector
dkim

DKIM key length (bits)
2048 bit

+ Add

Import private key

Duplicate DKIM record

If you're not using the Mailcow server, you can use a free DKIM generator like DKIMcore.org.

This is an example of how to create the DKIM record on your DNS server.

TXT

Host *
dkim._domainkey

TXT Value *
v=DKIM1;k=rsa;t=s;s=email;p=...

TTL *
1 Hour

Save Cancel

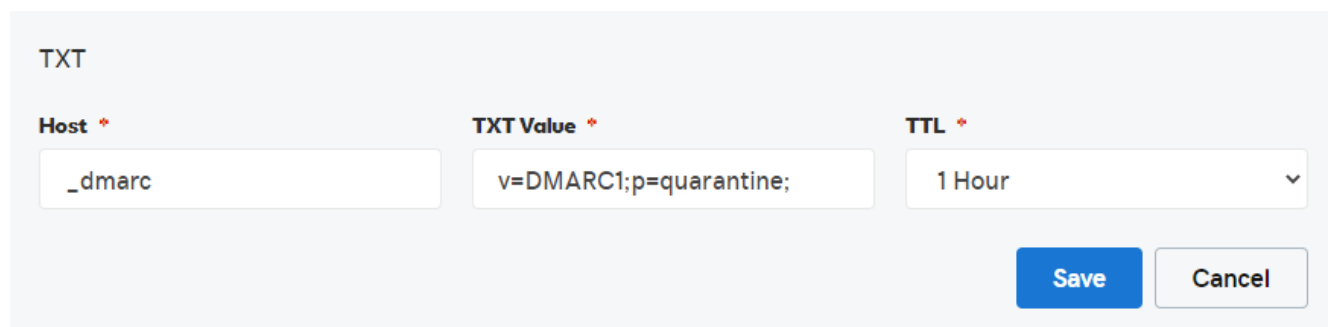
DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE)

DMARC (Domain-based Message Authentication, Reporting, and

Conformance) extends your existing SPF and DKIM records. It makes sure that the sender's emails are protected by SPF and DKIM, and tells the receiving mail server what to do if these checks fail.

To set up your DMARC record, create a new TXT record for the host `_dmarc` with the value `v=DMARC1;p=<policy>`. The policy argument tells the receiving mail server what it should do with a mail if it fails DMARC. You can set this to either **"none"**, **"quarantine"** or **"reject"**. There are some other optional arguments you can use to send daily reports or a specific percentage of suspicious emails the DMARC policy should apply to. You can find more details about all the different options in my DMARC cheat sheet.

In the following example, you can see how the DMARC record looks for the domain the-digital-life.com



The screenshot shows a form for creating a new DNS record. At the top, it says "TXT". Below this, there are three fields: "Host", "TXT Value", and "TTL". The "Host" field contains "_dmarc". The "TXT Value" field contains "v=DMARC1;p=quarantine;". The "TTL" field is a dropdown menu set to "1 Hour". At the bottom right, there are two buttons: "Save" (in blue) and "Cancel" (in light gray).








Host *	TXT Value *	TTL *
_dmarc	v=DMARC1;p=quarantine;	1 Hour

Save **Cancel**

SET UP AUTOCONFIGURATION DNS RECORDS FOR YOUR MAIL SERVER

If you're using mail clients like Outlook, Thunderbird on your Computer, or Mobile devices they offer the ability to do an "autoconfiguration" also called **Auto-discover**. That means you just need to enter your email address and password and the mail client tries to resolve the mail server IP addresses, used ports, and encryption settings for IMAP and SMTP. You can achieve this by adding SRV DNS records that are defined in the RFC 6186 standard and some specific records that are used in Outlook clients.

In the following example, you can see how the autoconfiguration records look for the domain the-digital-life.com.

SRV	_autodiscover._tcp.@	0 1 443 mail.the-digital-life.com	1 Hour	
SRV	_imap._tcp.@	0 1 143 mail.the-digital-life.com	1 Hour	
SRV	_imaps._tcp.@	0 1 993 mail.the-digital-life.com	1 Hour	
SRV	_pop3._tcp.@	0 1 110 mail.the-digital-life.com	1 Hour	
SRV	_pop3s._tcp.@	0 1 995 mail.the-digital-life.com	1 Hour	
SRV	_submission._tcp.@	0 1 587 mail.the-digital-life.com	1 Hour	
SRV	_smtps._tcp.@	0 1 465 mail.the-digital-life.com	1 Hour	

This is an example of how to create such a record for the _autodiscover record used in Outlook clients.

SRV

Service *

_autodiscover

Protocol *

_tcp

Name *

@

Target *

mail.the-digital-life.com

Priority *

0

Weight *

1

Port *

443

TTL *

1 Hour

Save

Cancel

How to check if your DNS records are configured correctly on your mail server?

Now you should be able to send and receive mails, your domain is protected against spoofing and your mail clients can be configured via auto-discovery. To check your mail server DNS records, you can use a diagnostic tool like <https://www.mxtoolbox.com>.

It can check if you set up all your DNS records correctly and also perform other checks, f.e. the blacklist check. This reveals if your mail server's IP is blacklisted, which could be problematic when you want to send mails.

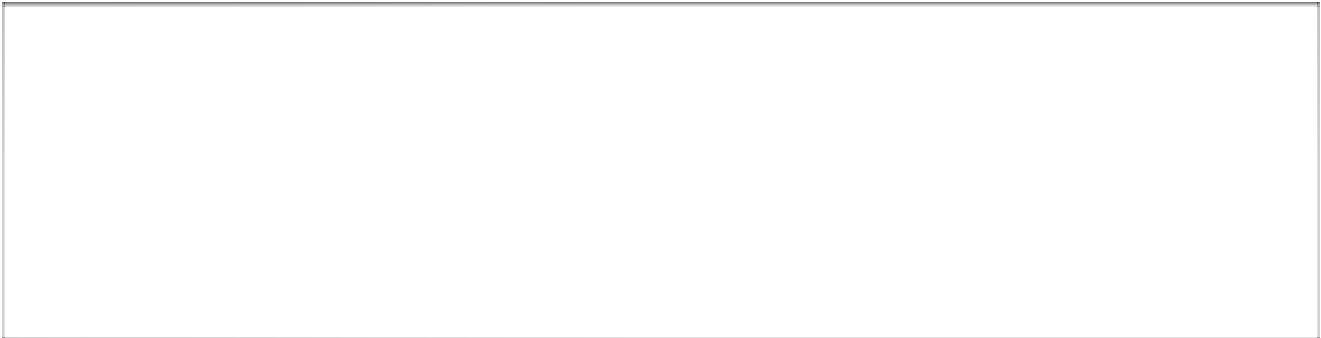
COMMUNITY

Get help, raise issues and connect with other people.

JOIN OUR DISCORD

• • •

MY LAST VIDEO



• • •

GERMAN CONTENT

Watch me live, or on YouTube in German language.

ChristianLempa is
offline.

Learn more about
them on their channel!

► [Visit ChristianLempa](#)

TWITCH

YOUTUBE

FOLLOW ME ON

TOPICS

[docker](#)

[linux](#)

[security](#)

[portainer](#)

[docker-compose](#)

[ansible](#)

[nginx](#)

[automation](#)

RESOURCES

[Dotfiles](#)

[Tools](#)

[Boilerplates](#)

[Cheat-Sheets](#)

MEET OUR COMMUNITY

JOIN OUR DISCORD

[LEGAL NOTICE / IMPRESSUM](#) | [PRIVACY POLICY](#) | [AFFILIATE DISCLOSURE](#)

© 2022 BY THE DIGITAL LIFE - DESIGN BY CL CREATIVE