

# How To Install and Configure DKIM with Postfix on Debian Wheezy

Posted February 28, 2014  258.6k [EMAIL](#) [SECURITY](#) [DNS](#) [DEBIAN](#)

  
58

## Introduction

The frustration of getting falsely flagged as a spammer is not strange to most of the mail server admins. By excluding the possibility of a compromised server, a false flag is usually caused by one of the following:

- the server is an open mail relay
- the sender's or server's IP address is blacklisted
- the server does not have a Fully Qualified Domain Name ([FQDN](#)) and a PTR record
- the Sender Policy Framework ([SPF](#)) DNS record is missing or it is misconfigured
- the DomainKeys Identified Mail ([DKIM](#)) implementation is missing or it's not properly set up

These are some of the basic properties that are being checked by the majority of proprietary and open source spam filters (including SpamAssassin). Passing these tests is extremely important for a well configured mail server.

This tutorial will focus on installing and configuring [OpenDKIM](#): an open source implementation of the DKIM sender authentication system.

It is assumed that the reader knows how to access the server over SSH, Postfix and Dovecot is already installed and configured ([tutorial](#)), the host name and the FQDN are set up ([tutorial](#), [tutorial](#)) and the SPF record is in place ([tutorial](#)).

## About DKIM

DKIM is an Internet Standard that enables a person or organisation to associate a domain name with an email message. This, in effect, serves as a method of claiming responsibility for a message. At its core, DKIM is powered by asymmetric cryptography. The sender's Mail Transfer Agent (MTA) signs every outgoing message with a private key. The recipient retrieves the public key from the sender's DNS records and verifies if the message body and some of the header fields were not altered since the message signing took place.

## Install OpenDKIM

Before starting the installation, a system update is recommended:

```
sudo apt-get update
sudo apt-get dist-upgrade
```

Install OpenDKIM and it's dependencies:

```
sudo apt-get install opendkim opendkim-tools
```

Additional packages will be listed as dependencies, type **yes** and press **Enter** to continue.

## Configure OpenDKIM

A couple of files must be created and edited in order to configure OpenDKIM.

**Nano** will be used as an editor because it's installed by default on DigitalOcean droplets and it's simple to operate:

- navigate with the arrow keys
- exit without saving changes: press **CTRL + X** and then **N**
- exit and save changes: press **CTRL + X** and then **Y**, and finally press **Enter**

**Important:** replace every instance of **example.com** with your own domain in all commands and configuration files. Don't forget to save your files after editing.

Let's start with the main configuration file:

```
sudo nano /etc/openssl.conf
```

Append the following lines to the end of the conf file (each parameter is explained below). Optionally, you can choose a custom port number for the **Socket**. Make sure that it's not used by a different application.

```
AutoRestart      Yes
AutoRestartRate  10/1h
UMask            002
Syslog           yes
SyslogSuccess    Yes
LogWhy           Yes

Canonicalization relaxed/simple

ExternalIgnoreList refile:/etc/openssl/TrustedHosts
InternalHosts      refile:/etc/openssl/TrustedHosts
KeyTable           refile:/etc/openssl/KeyTable
SigningTable       refile:/etc/openssl/SigningTable

Mode             sv
PidFile           /var/run/openssl/openssl.pid
SignatureAlgorithm rsa-sha256

UserID            openssl:openssl

Socket            inet:12301@localhost
```

- **AutoRestart:** auto restart the filter on failures
- **AutoRestartRate:** specifies the filter's maximum restart rate, if restarts begin to happen faster than this rate, the filter will terminate; **10/1h** - 10 restarts/hour are allowed at most
- **UMask:** gives all access permissions to the user group defined by **UserID** and allows other users to read and execute files, in this case it will allow the creation and modification of a **Pid** file.
- **Syslog, SyslogSuccess, \*LogWhy:** these parameters enable detailed logging via calls to syslog
- **Canonicalization:** defines the canonicalization methods used at message signing, the **simple** method allows almost no modification while the **relaxed** one tolerates minor changes such as whitespace replacement; **relaxed/simple** - the message header will be processed with the **relaxed** algorithm and the body with the **simple** one
- **ExternalIgnoreList:** specifies the external hosts that can send mail through the server as one of the signing domains without credentials
- **InternalHosts:** defines a list of internal hosts whose mail should not be verified but signed instead

- **KeyTable:** maps key names to signing keys
- **SigningTable:** lists the signatures to apply to a message based on the address found in the `From:` header field
- **Mode:** declares operating modes; in this case the militer acts as a signer ( `s` ) and a verifier ( `v` )
- **PidFile:** the path to the Pid file which contains the process identification number
- **SignatureAlgorithm:** selects the signing algorithm to use when creating signatures
- **UserID:** the opendkim process runs under this user and group
- **Socket:** the militer will listen on the socket specified here, Posfix will send messages to opendkim for signing and verification through this socket; `12301@localhost` defines a TCP socket that listens on `localhost` , port `12301`

This simple configuration is meant to allow message signing for one or more domains, to learn about other options please go [here](#).

Connect the militer to Postfix:

```
sudo nano /etc/default/opendkim
```

Add the following line, edit the port number only if a custom one is used:

```
SOCKET="inet:12301@localhost"
```

Configure postfix to use this militer:

```
sudo nano /etc/postfix/main.cf
```

Make sure that these two lines are present in the Postfix config file and are not commented out:

```
militer_protocol = 2
militer_default_action = accept
```

It is likely that a filter (SpamAssasin, Clamav etc.) is already used by Postfix; if the following parameters are present, just append the opendkim militer to them (miters are separated by a comma), the port number should be the same as in `opendkim.conf` :

```
smtpd_milters = unix:/spamass/spamass.sock, inet:localhost:12301
non_smtpd_milters = unix:/spamass/spamass.sock, inet:localhost:12301
```

If the parameters are missing, define them as follows:

```
smtpd_milters = inet:localhost:12301
non_smtpd_milters = inet:localhost:12301
```

Create a directory structure that will hold the trusted hosts, key tables, signing tables and crypto keys:

```
sudo mkdir /etc/opendkim
sudo mkdir /etc/opendkim/keys
```

Specify trusted hosts:

```
sudo nano /etc/openssl/TrustedHosts
```

We will use this file to define both `ExternalIgnoreList` and `InternalHosts`, messages originating from these hosts, domains and IP addresses will be trusted and signed.

Because our main configuration file declares `TrustedHosts` as a regular expression file ( `refile` ), we can use wildcard patterns, `*.example.com` means that messages coming from `example.com`'s subdomains will be trusted too, not just the ones sent from the root domain.

Customize and add the following lines to the newly created file. Multiple domains can be specified, do not edit the first three lines:

```
127.0.0.1
localhost
192.168.0.1/24

*.example.com

#*.example.net
#*.example.org
```

Create a key table:

```
sudo nano /etc/openssl/KeyTable
```

A key table contains each selector/domain pair and the path to their private key. Any alphanumeric string can be used as a selector, in this example `mail` is used and it's not necessary to change it.

```
mail._domainkey.example.com example.com:mail:/etc/openssl/keys/example.com/mail.private

#mail._domainkey.example.net example.net:mail:/etc/openssl/keys/example.net/mail.private
#mail._domainkey.example.org example.org:mail:/etc/openssl/keys/example.org/mail.private
```

Create a signing table:

```
sudo nano /etc/openssl/SigningTable
```

This file is used for declaring the domains/email addresses and their selectors.

```
*@example.com mail._domainkey.example.com

#*@example.net mail._domainkey.example.net
#*@example.org mail._domainkey.example.org
```

## Generate the public and private keys

Change to the keys directory:

```
cd /etc/openssl/keys
```

Create a separate folder for the domain to hold the keys:

```
sudo mkdir example.com
cd example.com
```

Generate the keys:

```
sudo opendkim-genkey -s mail -d example.com
```

-s specifies the selector and -d the domain, this command will create two files, `mail.private` is our private key and `mail.txt` contains the public key.

Change the owner of the private key to `opendkim`:

```
sudo chown opendkim:opendkim mail.private
```

## Add the public key to the domain's DNS records

Open `mail.txt`:

```
sudo nano - $ mail.txt
```

The public key is defined under the `p` parameter. Do not use the example key below, it's only an illustration and will not work on your server.

```
mail._domainkey IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQC5N3lrvYgPCRSqn+awTpE+iGYcKBPpo8HHbcFFCIIV10Hwo4PhCo
```

Copy that key and add a TXT record to your domain's DNS entries:

Name: `mail._domainkey.example.com.`

Text: `"v=DKIM1; k=rsa; p=MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQC5N3lrvYgPCRSqn+awTpE+iGYcKBPpo8HHbcFFCIIV10Hwo4PhCoGZSaKVH0jDm4yefKXI`

Select Record Type

A
CNAME
MX
TXT
SRV
NS

mail.\_domainkey.example.com.
"v=DKIM1; k=rsa; p=MIGfMA0GC
CREATE

|       |                              |  |   |
|-------|------------------------------|--|---|
| A     | @                            | 141.197.25.209                           | × |
| CNAME | www                          | @  | × |
| MX    | 0                            | www.example.com.                         | × |
| TXT   | @                            | "v=spf1 mx a -all"                       | × |
| TXT   | mail._domainkey.example.com. | "v=DKIM1; g=*; k=rsa; p=MIGfMA0GCsGSIb3C | × |

SCROLL TO TOP

Please note that the DNS changes may take a couple of hours to propagate.

Restart Postfix and OpenDKIM:

```
sudo service postfix restart
sudo service opendkim restart
```

**Congratulations! You have successfully configured DKIM for your mail server!**

The configuration can be tested by sending an empty email to `check-auth@verifier.port25.com` and a reply will be received. If everything works correctly you should see `DKIM check: pass` under `Summary of Results`.

```
=====
Summary of Results
=====
SPF check:          pass
DomainKeys check:   neutral
DKIM check:         pass
Sender-ID check:    pass
SpamAssassin check: ham
```

Alternatively, you can send a message to a Gmail address that you control, view the received email's headers in your Gmail inbox, `dkim=pass` should be present in the `Authentication-Results` header field.

```
Authentication-Results: mx.google.com;
  spf=pass (google.com: domain of contact@example.com designates --- as permitted sender) smtp.mail=contact@example.com;
  dkim=pass header.i=@example.com;
```

Submitted by: P. Sebastian

♥ Upvote (58)

✚ Subscribe

🔗 Share

[Spin up an SSD cloud server in under a minute.](#)

Simple setup. Full root access. Straightforward pricing.

DEPLOY SERVER

SCROLL TO TOP

#### Related Tutorials

[Why You May Not Want To Run Your Own Mail Server](#)

[How To Use Google's SMTP Server](#)

[How to Set Up a Mail Relay with Postfix and Mailgun on Ubuntu 16.04](#)

[How To Install and Configure Postfix on Ubuntu 16.04](#)

[How to Install and Configure Postfix as a Send-Only SMTP Server on Ubuntu 16.04](#)

## 57 Comments

Leave a comment...

[Log In to Comment](#)

^ [sianios](#) May 15, 2014

0 I went over this again and again and still get:  
DKIM check: neutral  
Can you update the pictures with new links? This might help.  
Thank you.

^ [bachvtuan](#) May 20, 2014

0 Hi. how to pass "DomainKeys check" ?

^ [xxar](#) October 27, 2014

0 Please refer to my recent response to "Jon" (in this same thread), regarding DomainKeys authentication deprecation.  
  
-xxar

^ [orekdm](#) May 26, 2014

0 Hey, I followed your article to a tee, but am still having some problems. Also, I am performing these steps on Ubuntu 14.04.

Everything seems perfect, but I got the two following errors from opendkim that I can't figure out the fix for:

```
opendkim[8078]: AC355401B9: SSL error:0D07207B:asn1 encoding routines:ASN1_get_object:header too long
opendkim[8078]: AC355401B9: dkim_eom(): resource unavailable: d2i_PrivateKey_bio() failed
```

My searches suggest that the problem may be with the cert itself so I re-did that step slowly (including the updated TXT record), but I still get the errors. I also thought maybe it was a simple permissions issue with opendkim reading the cert itself, but after chown -R opendkim:opendkim /etc/opendkim it still didn't work.

Thank you for getting me this far, if you have further insight, please help.

[SCROLL TO TOP](#)

^ [orekdm](#) May 31, 2014

0 I solved the problem that I was having. The formatting of the tutorial was the problem. In the section where you create the KeyTable the formatting makes it appear that this stanza is on two lines instead of one:

```
mail_domainkey.example.com example.com:mail:/etc/opendkim/keys/example.com/mail.private
```

By joining those lines together with a space between them, everything finally worked as expected.

It was quite satisfying to see the dkim=pass!

Thanks for the howto!

^ [ournet.biz](#) June 19, 2014

0 Hi, I receive error:

```
sudo apt-get install opendkim opendkim-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package opendkim
E: Unable to locate package opendkim-tools
```

can you consult? thank you.

^ [maugrande](#) July 4, 2014

0 ournet.biz, I remember that error of "Unable to locate package opendkim" happens because you have not ran the "apt-get update" before starting with the install option.

Try and see....

^ [joseantonioireyna](#) July 31, 2014

0 Hello, im getting this:

=====

Summary of Results

SPF check: pass

DomainKeys check: neutral

DKIM check: pass

DKIM check: pass

Sender-ID check: pass

SpamAssassin check: ham

But my email is still being flagged as spam on gmail, what is wrong?

^ [vincentc](#) April 10, 2015

1 how did you solve this? got the same now

^ [maxmitch](#) May 25, 2015

0 I have the same too!

^ [digitalocean768613](#) August 13, 2014

0 Some webhosters don't allow to add capital letters in the IN TEXT field, they automatically change every letter to lowercase, so it will be difficult to enter the base64-encoded Key, it will look like:

SCROLL TO TOP

```
mail._domainkey in txt "v=dkim1; k=rsa; p=migfma0gcsqgsib3dqeabaqaa4gnadcbiqkgqc5n3lnvvrygpcrsoqn+awtpe+igyckbppo8hhbcffciiv10hwo4
```

Which will not be the correct key. You have to contact your webhoster then to change the interface.

You can check if your Key is valid with: <http://dkimcore.org/tools/keycheck.html>

^ [Jon](#) September 6, 2014

1 If my mail server is `sub.domain.com`, is it still safe to replace all `example.com` with `sub.domain.com` in the tutorial?



---

^ Jon September 6, 2014

0 My DKIM is still showing neutral.

---

^ ionutzbf February 24, 2015

0 same here! i have a domain.com hosted on bluehost and subdomain.domain.com poting A to the server. how should i install in this case?

---

^ Jon September 6, 2014

0 Do you have more info on config to pass `*DomainKeys` `test`?

---

^ xxar October 27, 2014

1 DomainKeys != DKIM.

DomainKeys authentication is deprecated: DKIM is the successor to DomainKeys.

Trying to "pass" the DomainKeys component of the check recommended in this guide (provided by [check-auth@verifier.port25.com](mailto:check-auth@verifier.port25.com)), is absolutely **unnecessary**.

If you see "DKIM check: pass" in the authentication report, then you're good.

-xxar

---

^ aoemaster September 10, 2014

0

```
Sep 10 19:34:04 sd-65686 postfix/cleanup[38857]: warning: connect to Milter service inet:localhost:12301: Connection refused
```

in /var/log/mail.warn

---

^ seeekr October 13, 2014

0 Works like a charm! The only thing that's really annoying is those example.com URLs... it would be so easy to add a simple JS (based on jQuery or whatever) that would give us the option of auto-replacing ALL occurrences of "example.com" on this page with whatever domain name we need to set and gone is the tedious step of "copy into text editor - edit - copy again". I could volunteer to write such a thing if you want.

---

^ vuzgo October 27, 2014

1 Theres also a nice website to test the email: <http://www.mail-tester.com/>

---

^ george.levin.es November 4, 2014

0 I'm a getting a public key not available message my TXT entry looks like:

```
mail._domainkey.mail          "v=DKIM1; h=rsa-sha256; k=rsa; s=email; "          "p=MIGfMA0GCSqGSIb3DQEBAQUA" SCROLL TO TOP
```

---

my MX entry looks like:

```
10          mail.example.com
```

any help is appreciated.

i feel like there's weird formatting with the opendkim keygen but i have no idea how to change that other than manually remove whitespace which seems like it would mess things up.

but i don't know anything.

---

^ [gsucks](#) December 23, 2014

0 u can check ur dns record in here:

<http://www.protodave.com/tools/dkim-key-checker/>

---

^ [gsucks](#) December 23, 2014

1 in the digital ocean DNS records its wrong  
its not

```
it's
```mail._domainkey.``
```

I was gettin this error:

```
```Result:          permerror (key "mail._domainkey.mydomain.com" doesn't exist)```
```

thank you for the tutorial, worked like a charm! :) anyway the check-auth@verifier.port25.com is still failing, but on gmail I got

```
Authentication-Results: mydomain.com; dkim=pass
reason="1024-bit key; insecure key"
header.d=eempe.net header.i=@mydomain.com header.b=J3sMKpms;
dkim-adsp=pass; dkim-atps=neutral
```

---

^ [planetacancun](#) August 14, 2015

1 When I added the TXT record on digitalocean DNS I was missing the "." at the end of the domain and getting "permerror" ej.  
mail.\_domainkey.example.com. <- that last dot makes a difference ;) 2 hours later I check on <http://www.protodave.com/tools/dkim-key-checker/> and all good. I <3 this article.

---

^ [petsoukos](#) April 21, 2016

0 It doesn't accept the dot (.) at the end. Every time I try to enter the domain with the dot (.) at the end, it just disappears and leaves just the mail.\_domainkey in the field. How did you force it to allow the dot at the end?

---

^ [petsoukos](#) April 21, 2016

1 Oh, I saw in the Zone File below the entries, that DO is adding the domain with the dot (.) at the end, automagically. So no need to enter in the TXT record mail.domainkey.yourdomain.tld. If you just enter mail.domainkey and check the Zone File below, you'll see that the domain will get attached at the end.

SCROLL TO TOP

---

^ [diguliu](#) May 7, 2016

0 I had the same doubt but on gandi.net adding the final "!" throws a syntax error, so you don't even have an option. I suppose it adds "automagically" as [@petsoukos](#) reported too.


---

^ [AndreyO](#) January 7, 2015


0 For some reason I get

DKIM check details:  
Result: neutral (message not signed)


---

^  [AndreyO](#) January 7, 2015  
0 [deleted]


---

^  [AndreyO](#) January 7, 2015  
0 Solved

---


^  [KaMilml](#) October 9, 2016  
0 how u solved it? please help me :)

---


^  [abhishekkjain20](#) February 20, 2015  
1 Restarting OpenDKIM: No /usr/sbin/opendkim found running; none killed.  
opendkim: /etc/opendkim.conf: refile:/etc/opendkim/SigningTable: dkimfdbopen(): No such file or directory  
opendkim.

I am getting above error on sudo service opendkim restart. Please help!!!


---

^  [alexmironmiron](#) October 27, 2016  
0 Some file is corrupt.  
Try to recreate /etc/opendkim.conf with the same content. And restart opendkim.


---

^  [ionutzbf](#) February 24, 2015  
0 I have a domain.com hosted on bluehost and subdomain.domain.com poting A to the server. How should I install in this case?

---

^  [thigas88](#) March 23, 2015  
0 Whtas this?  
OpenDKIM Filter: Unable to create listening socket

---

^  [taek](#) April 2, 2015  
1 If Domainkey is neutural.... Check your postfix version with command below

```
sudo postconf mail_version
```

If Postfix version higher than 2.6, set "milter\_protocol" value 6 instead of 2.

```
milter_protocol = 6
```

And it is more easier to spam test from <http://www.mail-tester.com/>

Hope this helps anyone who has same issue with me.

SCROLL TO TOP

Load More Comments



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



Copyright © 2016 DigitalOcean™ Inc.

[Community](#) [Tutorials](#) [Questions](#) [Projects](#) [Tags](#) [Newsletter](#) [RSS](#) 

[Distros & One-Click Apps](#) [Terms, Privacy, & Copyright](#) [Security](#) [Report a Bug](#) [Get Paid to Write](#) [Shop](#)

[SCROLL TO TOP](#)