

OpenDKIM

So today we are going to have a short guide on how to install and configure OpenDKIM on your Linux server. First, we are going to start by updating your current server:

```
sudo apt-get update
```

Next we need to install OpenDKIM which is an open source implementation of the DKIM sender authentication system:

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

Alright now that it is installed, we need to edit the main configuration file for OpenDKIM:

```
sudo vi /etc/opendkim.conf
```

1. We will uncomment the below lines
 - a. Canonicalization – simple
 - i. We will change Canonicalization to relaxed/simple
 - b. Mode - sv
 - c. SubDomains – no
2. Add the below lines below #ADSPAction continue line. If your file does not have #ADSPAction continue line, then add them below SubDomains – no.
 - a. AutoRestart – yes
 - b. AutoRestartRate – 10/1M
 - c. Background – yes
 - d. DNSTimeout – 5
 - e. SignatureAlgorithm – rsa-sha256

At the bottom of the file add the below lines, (If you are using Ubuntu 18.04, the UserID is already added and set to opendkim.

```
#OpenDKIM user
UserID      opendkim

# Map domains in From addresses to keys used to sign messages
KeyTable    refile:/etc/opendkim/key.table
SigningTable refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternallIgnoreList  /etc/opendkim/trusted.hosts

# A set of internal hosts whose mail should be signed
InternalHosts       /etc/opendkim/trusted.hosts
```

Below is what your /etc/opendkim.conf file should look like:

```
josh@Ubuntu-VirtualBox: ~
6 SysLog yes
7 # Required to use local socket with MTAs that access the socket as a non-
8 # privileged user (e.g. Postfix)
9 UMask 002
10
11 # Sign for example.com with key in /etc/dkimkeys/dkim.key using
12 # selector '2007' (e.g. 2007._domainkey.example.com)
13 #Domain example.com
14 #KeyFile /etc/dkimkeys/dkim.key
15 #Selector 2007
16
17 # Commonly-used options; the commented-out versions show the defaults.
18 Canonicalization simple
19 Mode sv
20 SubDomains no
21
22 AutoRestart yes
23 AutoRestartRate 10/1M
24 Background yes
25 DNSTimeout 5
26 SignatureAlgorithm rsa-sha256
27
28 # Always oversign From (sign using actual From and a null From to prevent
29 # malicious signatures header fields (From and/or others) between the signer
30 # and the verifier. From is oversigned by default in the Debian package
31 # because it is often the identity key used by reputation systems and thus
32 # somewhat security sensitive.
33 OversightHeaders From
34
35 # List domains to use for RFC 6541 DKIM Authorized Third-Party Signatures
36 # (ATPS) (experimental)
37 ##
38 ## Specifies a configuration file to be passed to the Unbound library that
39 ##
40 ## Specifies a file from which trust anchor data should be read when doing
41 ## DNS queries and applying the DNSSEC protocol. See the Unbound documentation
42 ## at http://unbound.net for the expected format of this file.
43
44 TrustAnchorFile /usr/share/dns/root.key
45
46
47 #OpenDKIM user
48
49 UserID opendkim
50
51 # Map domains in From addresses to keys used to sign messages
52 KeyTable refile:/etc/opendkim/key.table
53 SigningTable refile:/etc/opendkim/signing.table
54
55 # Hosts to ignore when verifying signatures
56 ExternalIgnoreList /etc/opendkim/trusted.hosts
57
58 # A set of internal hosts whose mail should be signed
59 InternalHosts /etc/opendkim/trusted.hosts
-- INSERT --
```

Now we need to create the Signing Table, Key Table, and Trusted Hosts files. We will start by creating the directory structure for OpenDKIM:

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

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

Next we will change the owner of these from root to opendkim, making sure that only opendkim user can read and write to the keys directory.

```
sudo chown -R opendkim:opendkim /etc/opendkim
```

```
sudo chmod go-rw /etc/opendkim/keys
```

Then we create the signing table.

```
sudo vi /etc/opendkim/signing.table
```

Once created and open add the below line to the file

```
*@your-domain.com default._domainkey.your-domain.com
```

Save and close.

Next comes the key table

```
sudo vi /etc/openssh/ssh-keygen.conf
```

Once created and open add the below line to the file

```
Default._domainkey.your-domain.com your-domain.com:default:/etc/openssh/keys/your-domain.com/default.private
```

Save and close the file.

And finally comes the trusted hosts file.

```
sudo vi /etc/openssh/ssh_config
```

Once created and open add the below lines to the file

```
127.0.0.1
```

```
localhost
```

```
*.your-domain.com
```

Save and close the file

And lastly comes the part that makes all the magic happen, we must generate the private/public keypair.

First, we will create a separate folder for your domain.

```
sudo mkdir /etc/openssh/keys/your-domain.com
```

Now we will generate the keys using the openssh-keygen tool.

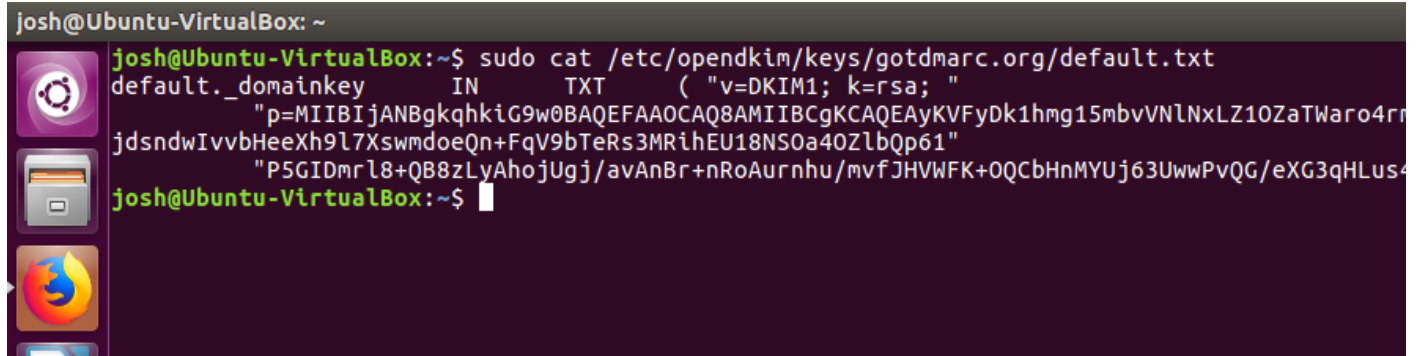
```
sudo openssh-keygen -b 2048 -d your-domain.com -D /etc/openssh/keys/your-domain.com -s default -v
```

Alright now we make openssh the owner of the private key

```
sudo chown openssh:openssh /etc/openssh/keys/your-domain.com/default.private
```

Now we will display the public key

```
sudo cat /etc/openskim/keys/your-domain.com/default.txt
```

A terminal window titled 'josh@Ubuntu-VirtualBox: ~' with a dark purple background. The prompt is 'josh@Ubuntu-VirtualBox:~\$'. The command 'sudo cat /etc/openskim/keys/gotdmarc.org/default.txt' is entered. The output shows a DNS record: 'default._domainkey IN TXT ("v=DKIM1; k=rsa; " "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYkVFyDk1hmg15mbvVNlNxLZ10ZaTWaro4rrjdsndwIvvbHeeXh9l7XswmdoeQn+FqV9bTeRs3MRihEU18NS0a40ZlbQp61" "P5GIDmrl8+QB8zLyAhojUgj/avAnBr+nRoAurnhu/mvfJHVWFK+OQCbHnMYUj63UwwPvQG/eXG3qHLus4")'. The prompt returns to 'josh@Ubuntu-VirtualBox:~\$'. On the left side of the terminal, there are three icons: a gear, a floppy disk, and the Ubuntu logo.

```
josh@Ubuntu-VirtualBox: ~
josh@Ubuntu-VirtualBox:~$ sudo cat /etc/openskim/keys/gotdmarc.org/default.txt
default._domainkey IN TXT ( "v=DKIM1; k=rsa; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYkVFyDk1hmg15mbvVNlNxLZ10ZaTWaro4rr
jdsndwIvvbHeeXh9l7XswmdoeQn+FqV9bTeRs3MRihEU18NS0a40ZlbQp61"
"P5GIDmrl8+QB8zLyAhojUgj/avAnBr+nRoAurnhu/mvfJHVWFK+OQCbHnMYUj63UwwPvQG/eXG3qHLus4
josh@Ubuntu-VirtualBox:~$
```

The string after the p parameter is your public key. We will copy and paste this record into your zones file for your domains DNS.

If you want to test your configuration enter the below command:

```
sudo openskim-testkey -d your-domain.com -s default -vvv
```

If everything is OK, you will see

```
Key OK
```

Thanks for making it this far again this is just a short how to on setting up OpenDKIM, if you have any questions about the various parameters openskim.org should have all the resources you need.