Have you set up email for your website using CyberPanel? Are users complaining that their email messages are not being received or are ending up in spam? How can you fix this? Since CyberPanel aims to be the best website hosting panel in the community, setting up of this stuff should also be nearly automated. The development team is already working to make this process as simple as possible for the User or the System Administrator, but for the time being, here is a tutorial to explain the manual way of setting up of DKIM, SPF and DMARC using a domain which is hosted on CyberPanel.

## What are DKIM, SPF and DMARC and Why Should You Even Bother With Them?

SPF stands for Sender Policy Framework and is just a DNS text record at your domain which tells the mail services and the receptors to receive the email from the server IP’s provided in your SPF record.

DKIM stands for Domain Keys Identified Mail. In this method, each email message is signed by your server and the receiver checks the messages with the DKIM public key, which is provided in your domain’s DNS. It’s basically used to verify that the email has originated from the actual source and hasn’t been tampered with in between.

DMARC (Domain-based Message Authentication, Reporting and Conformance) utilizes both SPF and DKIM and states a policy for both tools above. It allows you to set an email address to which can be sent reports about the statistics of email messages for the specified domain.

These are the 3 tools which are most used these days to make email messages more secure. Email services like Gmail mostly send messages to spam if they don’t have one of the 3 aforementioned methods of verification. The reason why many mail services may mark your messages as spam is that they also rely heavily on the IP’s reputation, and whether that IP has a valid PTR (rDNS) or not. For the PTR record, you have to ask your provider to change the rDNS record to match your domain as it helps for the email receptors to identify that the mails are coming from the right place! But, if your server’s IP address is listed in their Blacklist, the messages will get rejected. You should contact your provider to either change your server’s IP or ask the email services to de-list your IP.

Your IP Address can be checked for any blacklist using this tool: <https://www.ultratools.com/tools/spamDBLookupResult>

## Creating an Email Account

Let’s create an email account first, then send a test email from that account to your Gmail account for testing. The message will most probably end up in spam. That’s not an issue, as in this article we will be fixing it with those 3 tools that are extensively used in Gmail.



## Setting up an SPF Record.

In this article, we will be using the domain ‘talkshosting.com’ for configuring these 3 things on the CyberPanel installation. It is assumed that you have already installed CyberPanel on your VPS / Dedicated Server and have made your website with it. If not, please read [CyberPanel’s Documentation](http://docs.cyberpanel.net/doku.php?id=installation).

1. Proceed to your website’s DNS section in your CyberPanel installation or your current DNS hosting provider. (If you want to host your own DNS server with CyberPanel as well, then please read the [Documentation.](http://docs.cyberpanel.net/doku.php?id=dns)
2. Add the following TXT record at the root (@) of your domain. It tells the mail receivers to accept messages from the IP mentioned and to mark email from other sources as “Neutral” (or, spam in GMAIL).

v=spf1 a mx ip4:192.100.1.64 ?all

(Insert your Server IP after ip4: , use this type of record if you are using only your current server for sending mails, if you are sending mails from services like Google suite or some other servers too, then please go to <https://mxtoolbox.com/SPFRecordGenerator.aspx> and make your own spf record accordingly)

1. After adding the SPF record, try sending an email again from the account that you created earlier to a Gmail account. Gmail should now say that the message is “mailed-by : talkshosting.com”. This confirms that the Sender Policy Framework is in Action!



## Installing and Setting up OpenDKIM

OpenDKIM is a library which generates the DKIM keys and signs them for our email messages.

### Step 1 : Install OpenDKIM

yum install opendkim -y

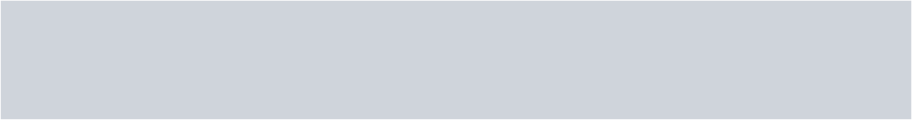
Now that the opendkim libraries are installed, lets create the DKIM keys!

### Step 2 : Generate DKIM keys

Execute the following command to generate DKIM public & private keys in the folder “/etc/opendkim/keys”.

opendkim-default-keygen

You should see something like this :



Now, inside /etc/opendkim/keys, there will be 2 files, namely default.private (which is the private key for the domain) and default.txt, (which is the public key we will publish in our DNS record so that mail receivers can identify our signed mails).

### Step 3 : Editing Configurations!

We will now edit some configuration files according to our requirements.

#### 1. Editing /etc/opendkim.conf

We recommend using SFTP and NotePad++ while editing config files for better spacing and syntax and to avoid any mistakes. You can also use nano or vim editors through the console, or whatever suits you.

Change the following lines shown below in /etc/opendkim.conf. Remember to change the domain to the one you are using!

Mode sv

Canonicalization relaxed/simple

Domain talkshosting.com

#KeyFile /etc/opendkim/keys/default.private

KeyTable refile:/etc/opendkim/KeyTable

SigningTable refile:/etc/opendkim/SigningTable

ExternalIgnoreList refile:/etc/opendkim/TrustedHosts

InternalHosts refile:/etc/opendkim/TrustedHosts

#### 2. Editing /etc/opendkim/KeyTable

The KeyTable file defines the path of the private key for the domain.

Edit the KeyTable file in /etc/opendkim/KeyTable using your preffered text editor and replace ‘talkshosting.com’ with your domain name.

default.\_domainkey.talkshosting.com talkshosting.com:default:/etc/opendkim/keys/default.private

#### 3. Editing /etc/opendkim/SigningTable

The SigningTable file tells the OpenDKIM service how to apply the keys. We will be signing messages sent from any email address of our domain, i.e. \*@talkshosting.com. Therefore, edit the SigningTable file in /etc/opendkim/SigningTable like this :

\*@talkshosting.com default.\_domainkey.talkshosting.com

Remember to replace “talkshosting.com” with your domain name!

#### 4. Editing /etc/opendkim/TrustedHosts

Now, edit the TrustedHosts file inside /etc/opendkim/TrustedHosts and append the server’s hostname and domain name below the localhost ip (127.0.0.1). The domain/hostname should be a FQDN (Fully Qualified Domain Name) meaning it should point to your server’s IP!

# OPENDKIM TRUSTED HOSTS

# To use this file, uncomment the #ExternalIgnoreList and/or the #InternalHosts

# option in /etc/opendkim.conf then restart OpenDKIM. Additional hosts

# may be added on separate lines (IP addresses, hostnames, or CIDR ranges).

# The localhost IP (127.0.0.1) should always be the first entry in this file.

127.0.0.1

talkshosting.com

#### 5. Editing Postfix Config File (/etc/postfix/main.cf)

Finally, Edit the Config file of your SMTP service present in /etc/postfix/main.cf and append the following lines at the end :

smtpd\_milters = inet:127.0.0.1:8891

non\_smtpd\_milters = $smtpd\_milters

milter\_default\_action = accept

### Step 4 : Enabling OpenDKIM and Restarting the Postfix Service.

Now, we will start the OpenDKIM service and restart our SMTP service by entering the following commands on the server Console :

systemctl start opendkim

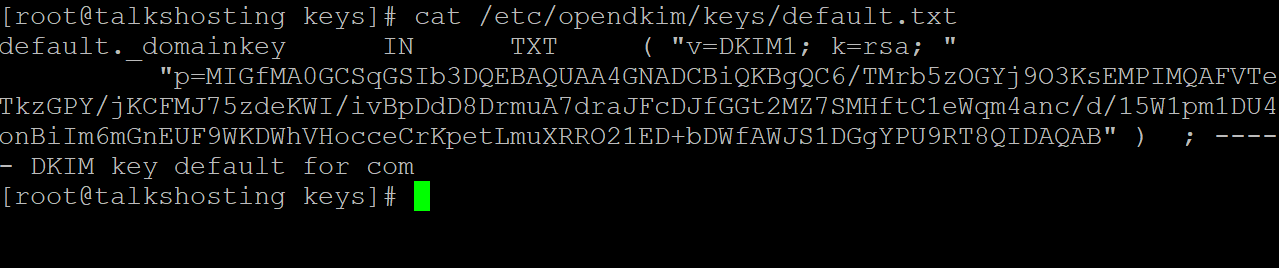
systemctl enable opendkim

systemctl restart postfix

### Step 5 : Publishing the DKIM Record to Our DNS!

Now that the DKIM is configured and working, the DKIM records should be published to the domain’s DNS so that the mail receptors can identify the keys from the public record which we are now going to publish.

We will use the output of ‘/etc/opendkim/keys/default.txt’ for our DNS record.



We will rephrase this record as follows and post it in our DNS as a TXT record with the name default.\_domainkey:

"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6/TMrb5zOGYj9O3KsEMPIMQAFVTeTkzGPY/jKCFMJ75zdeKWI/ivBpDdD8DrmuA7draJFcDJfGGt2MZ7SMHftC1eWqm4anc/d/15W1pm1DU4onBiIm6mGnEUF9WKDWhVHocceCrKpetLmuXRRO21ED+bDWfAWJS1DGgYPU9RT8QIDAQAB"



## Adding the DMARC Record

As mentioned above, DMARC utilizes both SPF and DKIM and itself is also a DNS record, which is added to the Domain’s DNS.

To add it to your DNS zone, set the record’s name as “\_dmarc” and its content to “v=DMARC1; p=none” which is the standard form of DMARC. You can also go advanced and set up your own DMARC rules following its guidelines, but for now, we will just leave it at that.



All of our work is done! Send a test email from your domain for which you’ve configured the DKIM and DMARC.

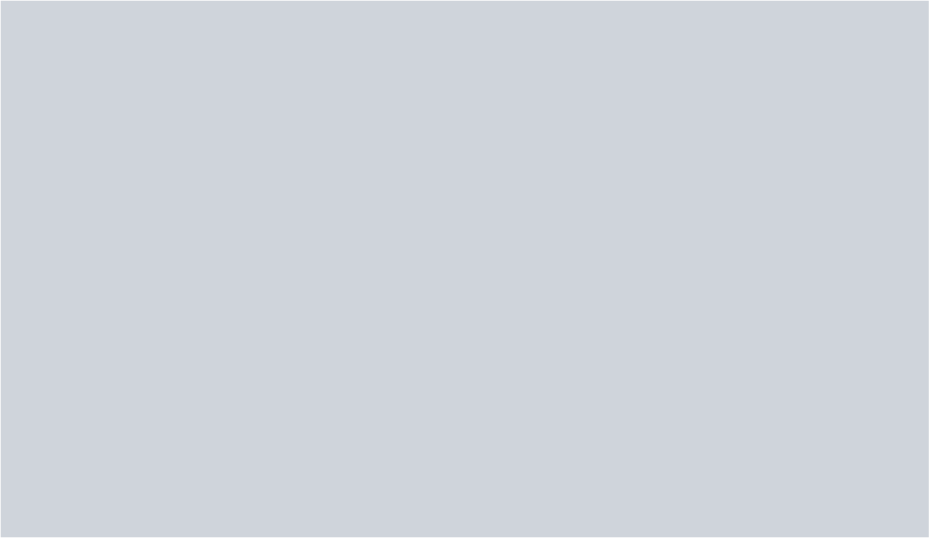
After sending the email, the Mail Logs (on the left side of CyberPanel) will also show that the mails are now being signed and the DKIM-signature is being added!

talkshosting postfix/cleanup[4328]: 45B7F1BF8: message-id=<3ff9359b8ae0c063f7628a0a52b6cdd0@talkshosting.com>

talkshosting opendkim[3443]: 45B7F1BF8: DKIM-Signature field added (s=default, d=talkshosting.com)

talkshosting postfix/qmgr[3688]: 45B7F1BF8: from=<admin@talkshosting.com>, size=1193, nrcpt=1 (queue active)

If we send email to a Gmail account, the mail will land straight in the Inbox if all the requirements are met, and it will show mailed-by : talkshosting.com, signed-by : talkshosting.com, just like this:



If you see this above info, then Congratulations! You have succesfully configured all three tools that are used commonly for verification purposes!

If you want to go advanced, click on the small arrow on the right side of the Gmail message, and select ‘Show Original.’ It will open advanced details in a new popup and you can see there that all three things we aimed to do are done. Gmail is now marking our email as SPF, DKIM and DMARC passed!



Thanks for reading this tutorial. The Development team is working to get this process as automated as possible. But in the meantime, if you have any troubles in getting this all working, try waiting for DNS propagation as it can cause issues in some cases. Nonetheless, feel free to hop in the CyberPanel’s Discord server and ask anything!

## Setting up Thunderbird for Sending/Receiving mails

### Step 1 : Download and Install Thunderbird Client.

Download Thunderbird from <https://www.mozilla.org/en-US/thunderbird/> and install it using all the default settings.

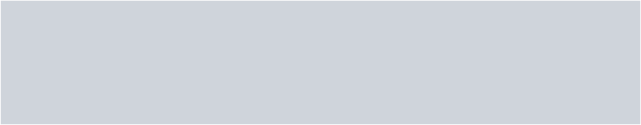
### Step 2 : Add DNS records for IMAP/POP3 and SMTP

For Thunderbird to work, lets add some DNS records so that Thunderbird will automatically get our server’s IP addresses. In our case, we’ll use IMAP for receiving and SMTP protocol for sending emails. IMAP is a relatively newer protocol, it helps in getting the mails synced across all devices If you are using more than 1 device for sending/receiving mails!

Therefore, we will setup 2 A records, both pointing to our VPS IP.

If you plan to use POP3, setup a DNS record for POP3.talkshosting.com

Enter your domain name in place of talkshosting.com!

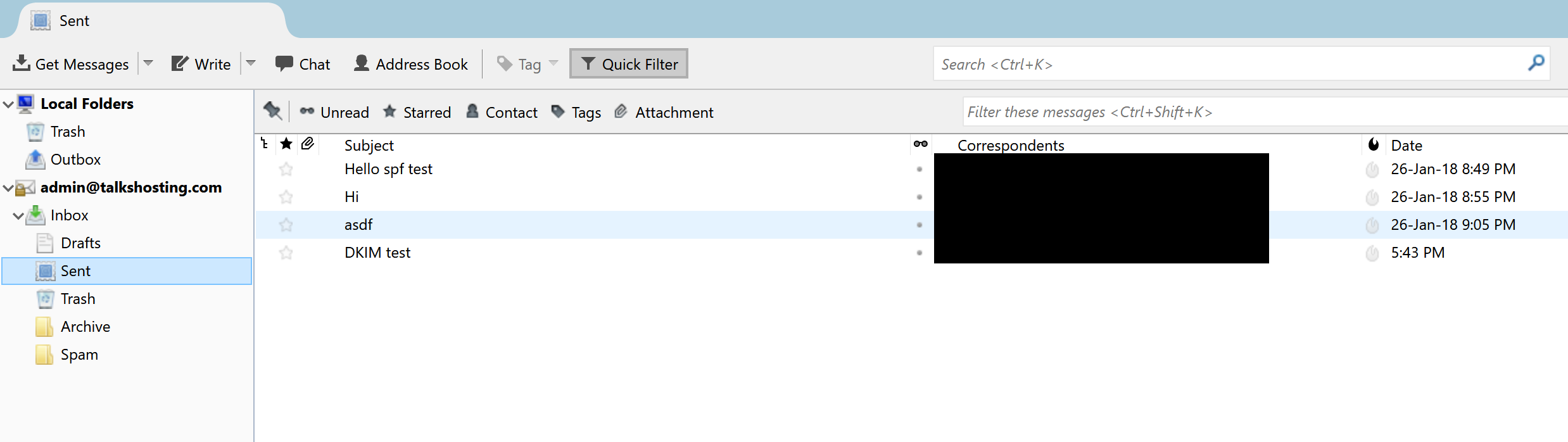


### Step 3 : Launch Thunderbird

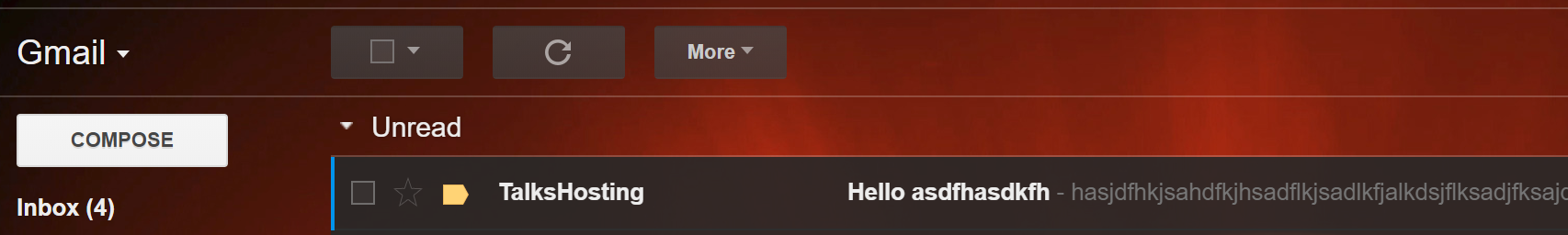
1. Right after Thunderbird is launched, it will ask you to create a new email account. Select ‘Skip this and use my existing email’ and enter Name, Email and Password which you have created in CyberPanel’s email section.
2. Select ‘IMAP (Remote Folders)’ option and click on Done

If you encounter any security issues like the one below, just click on Confirm Security Exception! It is due to the fact that CyberPanel generates Self-Signed Certificates during installation for email security purposes.

1. You will now see your inbox. Congratulations! All of the email you’ve previously received and all of the email you’ve sent previously with other devices will now be synchronized and downloaded to your Thunderbird!



1. Let’s Send a test email to see if the Remote Sending is working as well…
2. Click on Write > Message on the Toolbar and address your email to any address, in our case, we’ll send it to a Gmail account.
3. Click Send, and you may face another security issue for SMTP.yourdomain.com. Click on Confirm Security Exception.



Congratulations, after following these steps, you should have Configured Thunderbird for Sending/Receive emails succesfully! You can also setup Thunderbird on other devices using the exact same settings and all of the email sent and received will be synchronized in between!

Thanks for reading this Article, if you have any issues with any of the steps mentioned above, please ask in the comment section or hop in our Discord server for any support!

Discord server link : <https://discord.gg/mcvXehH>