namecheap.com

# Namecheap.com Knowledgebase • cPanel Email Authentication Tool – SPF and DKIM Records (cPanel Email FAQs)

As you may know, if mail service is unauthenticated you can face the following issues:

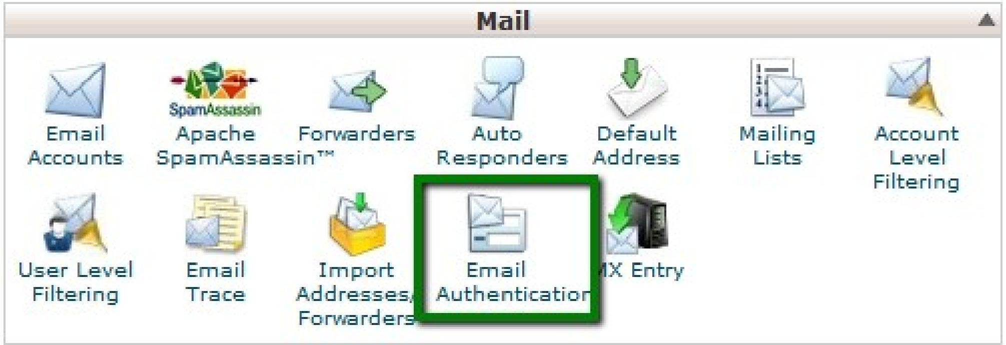
- emails you send are delivered to Spam/Junk folders

- emails you send bounce with "SPF record failure" error
- your Inbox gets numerous "Failed delivery" bounce backs of the emails you never sent

In the first case, recipient mail server looks up SPF record for your domain, and if it is not added / does not match actual outgoing server IP address, such a mail delivery will fail. Such checking mechanism is implemented in order to make sure email comes from a legitimate sender and verified sender.

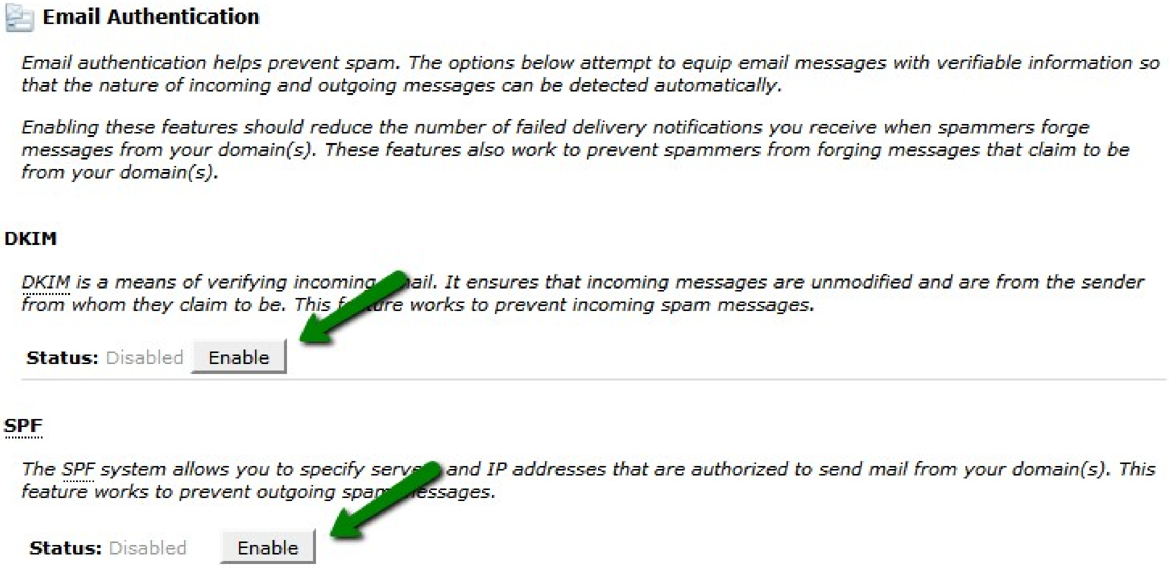
Second situation takes place when there is no SPF/DKIM configured for your domain or they are configured incorrectly, which lets unauthorized party to forge emails using @yourdomain.com mailbox. Such cases are called **mail spoofing**.

**Email Authentication** is an effective set of anti-spoofing and anti-spamming tools available in cPanel.



It consists of two major components – **SPF** and **DKIM records** setup.

Click on **Enable** and the records will be added to the DNS zone of *all* hosted domains automatically



**Email Authentication**

*Email authentication helps prevent spam. The options below attempt to equip email messages with verifiable information so that the nature of incoming and outgoing messages can be detected automatically.*

*Enabling these features should reduce the number of failed delivery notifications you receive when spammers forge messages from your domain(s). These features also work to prevent spammers from forging messages that claim to be from your domain(s).*

**DKIM**

*DKIM is a means of verifying incoming email. It ensures that incoming messages are unmodified and are from the sender from whom they claim to be. This feature works to prevent incoming spam messages.*

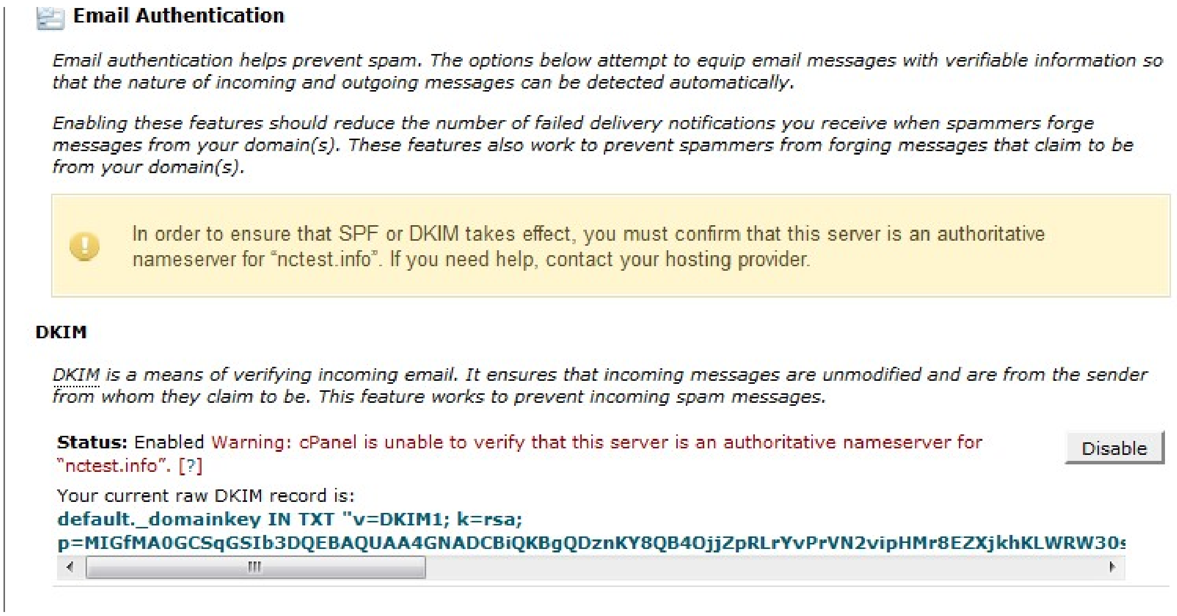
**Status:** Disabled

**SPF**

*The SPF system allows you to specify servers and IP addresses that are authorized to send mail from your domain(s). This feature works to prevent outgoing spam messages.*

**Status:** Disabled

**NOTE:** you may see the following warning about authoritative nameservers right after enabling



**Email Authentication**

*Email authentication helps prevent spam. The options below attempt to equip email messages with verifiable information so that the nature of incoming and outgoing messages can be detected automatically.*

*Enabling these features should reduce the number of failed delivery notifications you receive when spammers forge messages from your domain(s). These features also work to prevent spammers from forging messages that claim to be from your domain(s).*

In order to ensure that SPF or DKIM takes effect, you must confirm that this server is an authoritative nameserver for "nctest.info". If you need help, contact your hosting provider.

**DKIM**

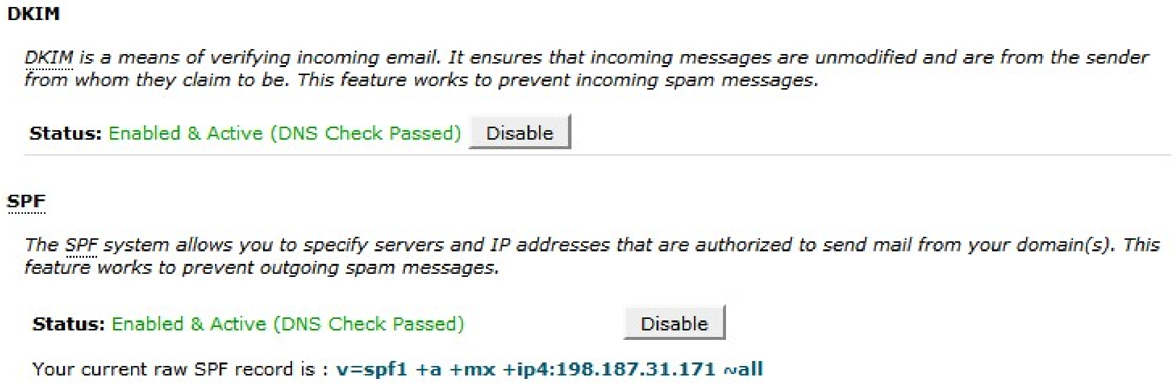
*DKIM is a means of verifying incoming email. It ensures that incoming messages are unmodified and are from the sender from whom they claim to be. This feature works to prevent incoming spam messages.*

**Status:** Enabled Warning: cPanel is unable to verify that this server is an authoritative nameserver for "nctest.info". [?]

Your current raw DKIM record is:

```
default._domainkey IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDznKY8QB4OjjZpRLrYvPrVN2vipHMr8EZXjkhKLWRW30s
```

Allow some time to pass for the records to propagate and refresh the page afterwards.
The warnings should go away and DNS checks will be passed



**DKIM**

*DKIM is a means of verifying incoming email. It ensures that incoming messages are unmodified and are from the sender from whom they claim to be. This feature works to prevent incoming spam messages.*

**Status:** Enabled & Active (DNS Check Passed)

**SPF**

*The SPF system allows you to specify servers and IP addresses that are authorized to send mail from your domain(s). This feature works to prevent outgoing spam messages.*

**Status:** Enabled & Active (DNS Check Passed)

Your current raw SPF record is : **v=spf1 +a +mx +ip4:198.187.31.171 ~all**

## SPF record

Nowadays the vast majority of spam emails have *fake data in the «From» field*. Spammers and fraudsters use special tools to send

their mail on behalf of a real owner of the e-mail address.
**SPF record** (acronym for Sender Policy Framework) is an effective and simple method which lets you avoid such issues. If your domain name has correct SPF record then you can be sure nobody is able to send fake e-mails on behalf of your domain name.

*The main idea of SPF record* is that an owner of domain name publishes the information about IP addresses that are authorized to send mail from this domain name. The receiving server compares the information in the envelope sender address with the information published by domain name owner. If these details match then e-mail is delivered.

**NOTE 1:** sometimes cPanel automatically fetches incorrect server outgoing IP address. This happens when we have to change outgoing mail IP due to poor mail reputation or blacklists. Please get in touch with us via Live Chat or Ticket and we will gladly re-check if the correct IP is added to your SPF record.

**NOTE 2:** SPF record has its own specific syntax. It is strongly recommended to get familiar with SPF record syntax documentation if you are going to customize the record manually.

**NOTE 3:** SPF record is added to your domain DNS zone as TXT record. There are cases when you need to add another TXT record to verify your domain name ownership for some service. It is *not recommended* to modify existing SPF record, it is better to add a new one instead.

## DKIM Record

**DKIM** (DomainKeys Identified Mail) is another way of e-mail authentication. This method uses information about domain which is published by the domain owner. That information allows receiving server to verify if the e-mail message was sent by legal owner of that domain name.
Once TXT record which contains DKIM has been added to DNS zone a special code is added to *the headers of outgoing e-mails*. Receiving servers compare these headers with the information in DNS zone and if it matches then the e-mail is delivered.

**NOTE:** DomainKeys(DK) and DomainKeys Identified Mail (DKIM) are separate things.

DomainKeys(DK) are not available on our shared servers as DK implementation was converted to DKIM and extended in a number of ways as of Cpanel 11.32 and later releases.

Some of the differences between DomainKeys and DKIM include:

- Multiple signature algorithms (as opposed to just one available with DomainKeys)

- More options with regard to canonicalization, that validates both header and body
- The ability to delegate signing to third parties
- The ability for DKIM to self-sign the DKIM-Signature header field – to protect against its being modified
- The ability for wildcard option on some parameters
- The ability to support signature timeouts in DNS

If having DomainKeys for you is a must, we suggest upgrading to VPS/Dedicated server where you will be able to setup this feature.

These simple actions will let you be sure that no one is able to send spam on your behalf and your e-mail will not be delivered to spam folders.

This is it!

Need any help? Contact our Helpdesk