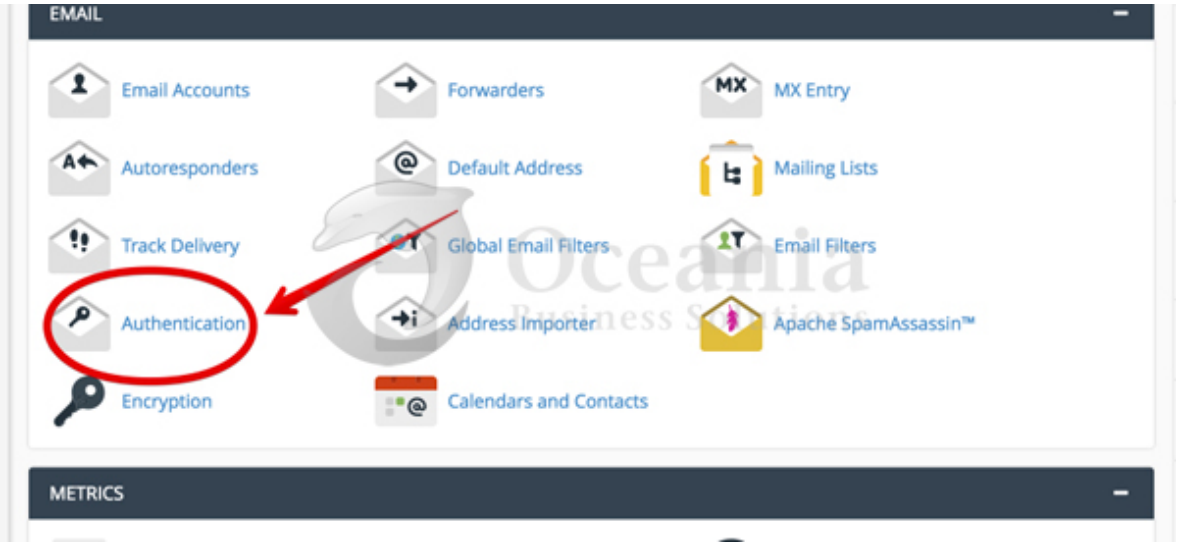
DKIM and SPF – Email Authentication in cPanel

DKIM (DomainKeys Identified Mail) is a means of verifying incoming email. It ensures that incoming messages are unmodified and from the sender from whom they claim to be. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication. For more information please visit http://www.dkim.org

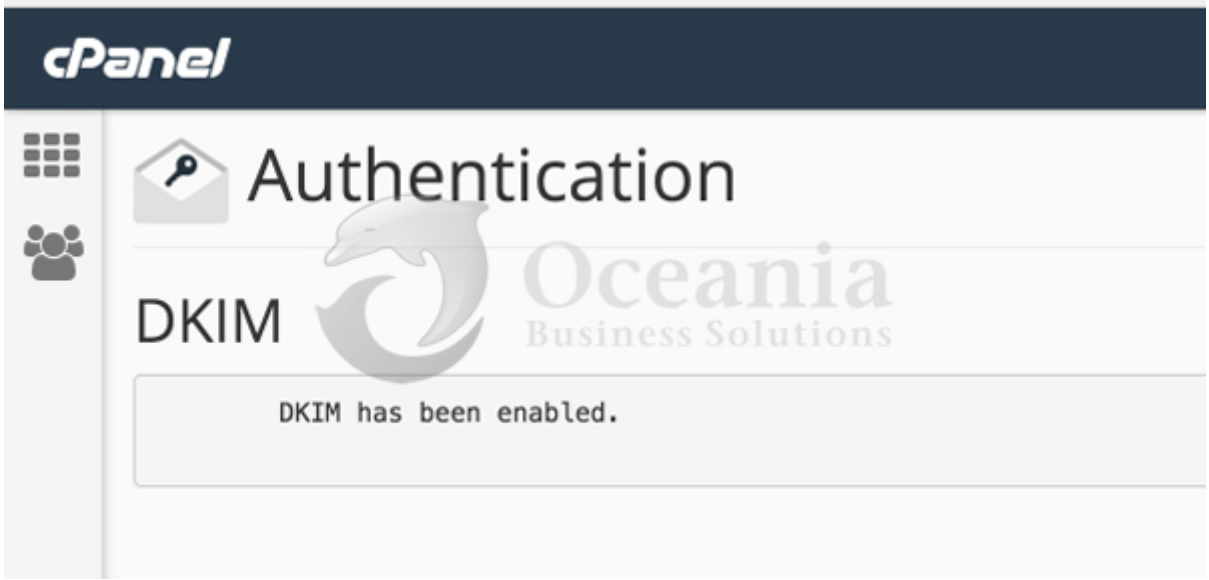
SPF (Sender Policy Framework) system allows you to specify servers and IP addresses that are authorized to send mail from your domain(s). This feature works to prevent outgoing spam messages using your domain from other computers and servers. If someone tries to send emails spoofing your domain in their email address, the receiving servers will check if you authorized them to send email – failing which such spam will be rejected.

We assume you are already logged into cPanel of your web hosting account. Click on **Email Authentication** link under Mail to proceed.



By default Email Authentication is disabled. To enable each one, click the **Enable** button.

DKIM is enabled with just a click of a button.

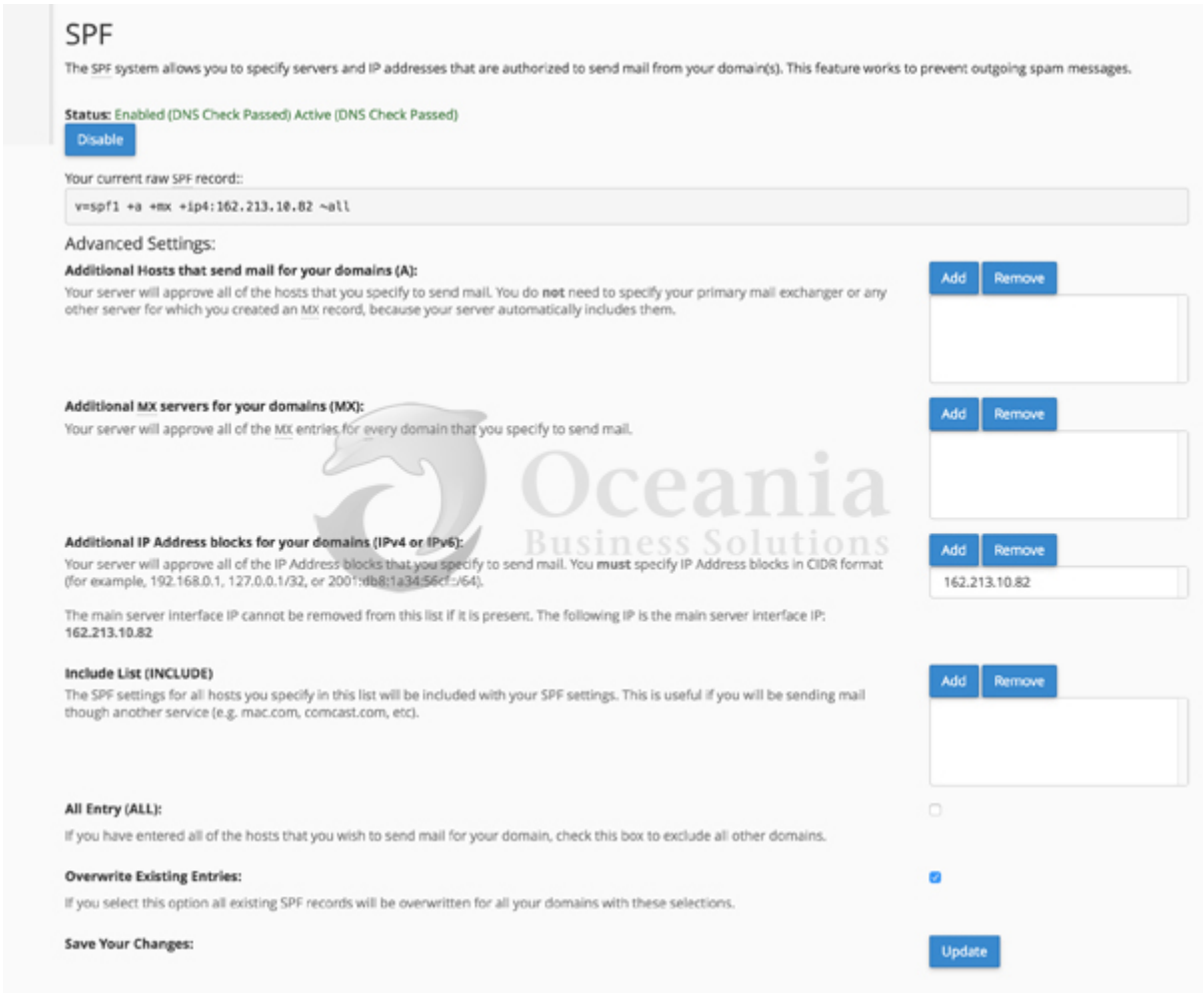


No further configuration is required for DKIM. The Email Authentication screen will show you if it is active.

To enable SPF, click **Enable** button.

When SPF is enabled, a new TXT DNS Record is added to your domain's DNS zone. It uses your domain's Mail Exchanger (MX) record, A record and the IPv4 address. In most cases this default setting is good enough to authorize these servers to send email.

In addition to default configuration of SPF, the Email Authentication screen allows you to add additional hosts and make changes to the SPF record.



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

Enabling DKIM and SPF 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).