



Setting Up Email for your **.cpa** Domain

Once you've registered your **.cpa** domain you will want to start using it for your email and other services. In this document we will discuss:

- Choosing an email service for your **.cpa** domain
- Adding email to your **.cpa** domain
- Common setup issues

This document will help guide you through the process of choosing a vendor, setting up your email, and troubleshooting common setup issues.

Choosing an email service for your **.cpa** domain

To start using email with your **.cpa** domain you will first need to procure an email service. The most popular service providers for email are Microsoft Office 365 and Google GSuite, however there are other options. Let's first discuss the Microsoft and Google solutions.

Microsoft Office 365

Office 365 is one of the most common and popular of the Email and office suites. It has many versions that you can subscribe to based upon your needs and budget and is a great fit for a small to enterprise scale firms. Best of all it includes all of the Microsoft Office applications that we are all so familiar with. For more information or to purchase Office 365 go to <https://www.office.com>.

Google Workspace (formerly GSuite)

Google Workspace is equally popular as Office 365 and has a similar design and look and feel. While Microsoft's architecture is primarily based on installed applications at the desktop, Google was designed from the ground up to run over the internet and consists of lightweight web-based applications. This digital suite is also well suited for small to enterprise scale firms. For more information or to purchase Google Workspace go to <https://workspace.google.com>.

EnCirca Email Service

If all that you need is email and would like to avoid the expense and complexity of administering a full-blown Digital Suite, then you want to consider EnCirca's basic email service. A basic email service will also include spam filtering and auto-responders (out-of-office). This service is a great fit for individuals and small firms who want an email service that is inexpensive and easy to manage. For more information or to purchase Google Workspace go to <https://www.encirca.com/email-packages/>.

Please note that you can choose any email provider you like and are not restricted to the vendors noted in this document.

Adding Email to your .cpa domain

Once you have subscribed to an email service you will need to add it to your .cpa domain. Please refer to your email service provider for their setup instructions as they will vary based on the email service you choose.

Nearly all of the email service providers require the creation of one or more DNS (domain name system) records. These records tell the other email systems on the internet who the email provider is for your .cpa domain and how to send email to you. You can think of DNS as the address book for internet-based services.

By default EnCirca is your DNS provider and the EnCirca portal is where you will need to go to create these DNS records. You can access the EnCirca portal directly at this URL <https://manage20.encirca.com/>.

Please note that if you moved your DNS service to another provider, such as Cloudflare, CPA Site Solutions, Wix, etc.... as part of your webhosting setup then you will need to use their DNS service to create your email DNS records.

Frequently Used Terms

Below are definitions of common terms you may come across while setting up your email.

DNS – DNS is the Domain Name System that gives information to everything trying to communicate with that domain name. A DNS record shows where the website files are located, where to route email, whether or not to trust email sent and received on the domain name, and other relevant information about the domain name. It's also a way to verify that you're the website owner of a domain name (some websites such as Google's Search Console and Bing Webmaster Tools require a DNS record to be added in order to verify ownership).

DMARC – DMARC stands for Domain-based Message Authentication, Reporting & Conformance. DMARC is an email authentication protocol designed to give domain name owners the ability to protect their domain name from unauthorized use.

DKIM – DKIM stands for DomainKeys Identified Mail. DKIM is an email authentication method designed to detect forged email addresses in email.

SPF – SPF stands for Sender Policy Framework. SPF is used to indicate whether or not a web host is authorized to send email for a particular domain name. SPF is one of the original methods designed to show that a particular sender is authorized to send email on behalf of that particular domain name.

Common Email Issues

Below are some of the more common issues you may encounter when setting up your email.

You are not receiving email messages

Symptom: You can send emails and others receive them, but you do not receive any new email, including replies to the emails you sent.

Cause: This is most often caused by the DNS MX records being setup incorrectly. Either there is a typo in the record or there is some other misconfiguration.

The DNS MX record is used to identify where email for your domain needs to be sent to for you to receive it. If you host your email in Office 365 then the MX record(s) will point to Microsoft servers. The specific instructions for the DNS MX record you need to create will be provided by Microsoft during your Office 365 setup. The same applies for all email systems, the vendor that hosts your email with will provide the MX record instructions.

Some people are not receiving your email messages

Symptom: You receive emails but some people are telling you that they are not receiving the messages you send.

Cause: This is most often caused by your anti-spam DNS records not being setup properly. These records include SPF (Sender Preferred Framework) and others. Double-check your DNS TXT record to ensure that it is setup properly.

Note that some companies also block all emails from domains that were registered less than 60-days prior. So if your .cpa domain was registered less than 60 days ago there is a chance that the company you are trying to send to is using a security system that uses this metric to block potential spam. Many fraudsters use recently registered domains in their spam distribution and to combat this some companies have adopted this method.

Emails you send are going to the recipients Junk folder

Symptom: Recipients report that your email is going to their junk folder.

Cause: This is most likely caused by improperly configured SPF, DKIM or DMARC settings. Double-check your email setup instructions from your service provider.