Stop Email Delivery Issues: Verify Your Domain

Last Modified on 02/19/2024 4:01 pm EST

Overview

When Order Time sends an email the email displays as it is coming from your email address even though the email is actually sent from the Order Time server. This helps the recipient of your email to recognize the from address on the email. This also ensures that all replies will be directed to your email address.

Sometimes, when the receiving Email Server detects that the domain (your domain) and the server it is sent from (Order Time Server) are different a false warning will show up when the email is opened by the recipient. The email can also be falsely flagged and placed in the recipient's SPAM folder.

DNS Record Validation

To avoid this DNS records can be added to your DNS settings, this may be where your domain is hosted (GoDaddy, Network Solutions etc.), authorizing the Order Time email server to send email on your behalf. Domain Verification is not required. However, it is recommended to you use your own custom email domain. If you use a non-custom domain, such as addresses ending in @gmail.com or @yahoo.com, you can't use this feature, as you won't have access to the account DNS settings.

If you allow Order Time to send email on behalf of your email domain, Order Time stops sending messages from *ordertime.com*, and sends them from your domain, completely preserving your branding.

DNS Settings have a different location depending on your registrar

The process of adding a C Name entry is different for different domain registrars. For example, here are the instructions for **GoDaddy**, **Namecheap**, **Network Solutions**, and **Google Domains**.

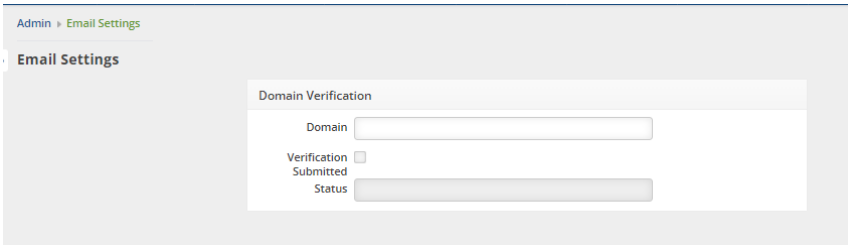
Let's Get Started

Step 1: Make sure you have access to the DNS settings. This is likely the same account where your domain is registered. (See the info above)

Step 2: Login to Order Time and go to the Admin page by clicking your company's name at the top right

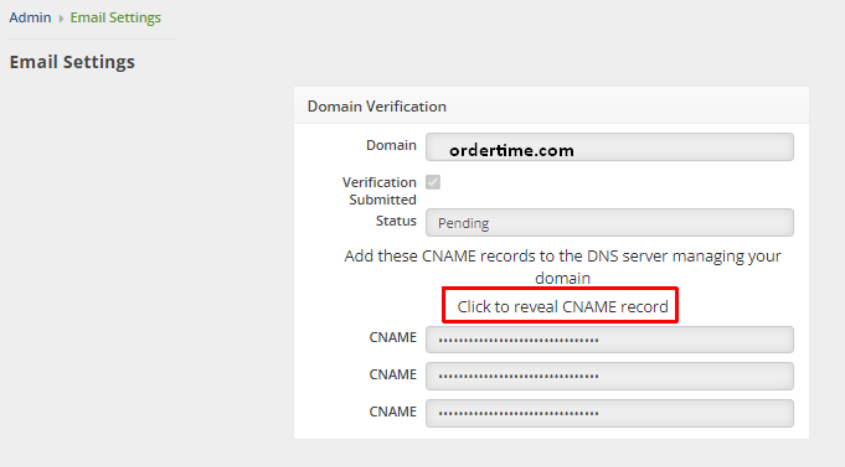
Step 3: Click Domain Verification in the Settings section

Step 4: On the Domain Verification page, enter your domain into the Domain field similar format to ordertime.com



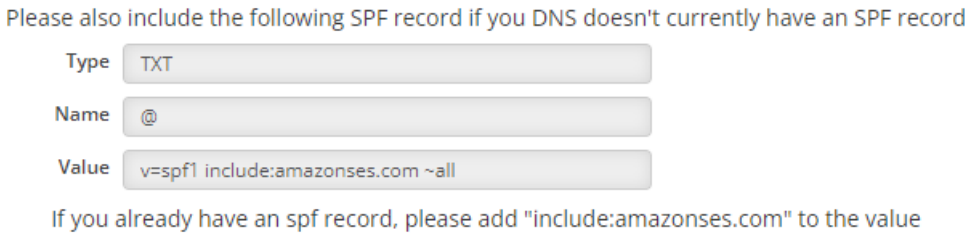
Step 5: Now you should see the CNAME records that you will need to enter into your DNS host

If you do not see the CNAME records, click on Click to reveal CNAME record as shown in the red box



Step 6: Next go login to your domain DNS settings and create the CNAME records

Step 7: Next add the SPF Record found at the bottom as a TXT record. This step is important because it provides authority and will add legitimacy to all the emails you send from Order Time, this keeps your emails from ending up in your customer's SPAM box.



Step : Return to the Domain Verification page in Order Time to check the Status of the verification

FYI - Email sending is disabled by default during the 30 day trial period. Contact us at support@ordertime.com and we can verify your identity to enable this feature in your trial sandbox.

Issues with DMARC Policies

What is DMARC? Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol that uses Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to detect email spoofing. In order to comply with DMARC, messages must be authenticated through either SPF or DKIM, or both.

After going through domain verification, if messages that you send to other domains come back as Bounced due to DMARC, most likely soft bounced, you may need to setup a DMARC policy on your domain via a DNS record.

Please follow the instructions in this document: **Complying with DMARC authentication protocol in Amazon SES**

FYI - Email sending is disabled by default during the 30 day trial period. Contact us at support@ordertime.com and we can verify your identity to enable this feature in your trial sandbox.