Cornerstone
realize your potential

At Cornerstone OnDemand we strive to provide the best possible service to our clients, however with over 40 million users using our highly configurable platform, email message delivery can get tricky.

This becomes an issue for clients who configure the Cornerstone Application to fake (spoof) their sender email domain – because all emails are sent from Cornerstone under @client domain – to send to a "public" email service such as hotmail.com, live.com, gmail.com, or yahoo.com. These clients run a high risk of slow or blocked email delivery due to the types of spam prevention techniques in use by these organizations.

To improve email delivery rates for clients sending to public domains, we suggest the following methods and techniques.

1. Email Relay + SPF Records (preferable for best delivery results)

Cornerstone will relay all company email messages (to the recipients within @client domain) through the client's email server securely to ensure the best delivery rate possible. This guarantees the email will pass all spam-prevention techniques since the client's own email server is fully authorized to send email from the @client domain name within client's organization, and messages are not rejected or caught in the Spam folder.

All emails to recipients, who have addresses hosted by public domains or email services outside client's organization, will be sent directly to the far end email servers. To address this, it's recommended to setup SPF records properly. This will ensure acceptable email delivery; however, there are still items out of Cornerstone's control, which could delay email delivery to these recipients.

In order to implement this solution Cornerstone Engineers will work with the client's email server administrator as there are many configurable options. In order to begin this process, please have your email server administrator answer the questions in the Appendix 1 and provide that response back to Cornerstone Engineers. Then client's DNS or email administrator should modify their SPF (Sender Policy Framework) record to include Cornerstone's email severs as authorized email delivery sources for the @client domain. An example SPF record is provided in the "SPF Records" option below.

Cornerstone Email Server List as of July 2018. Cornerstone owns all IP addresses in the range of:

- 208.185.229.0/24
- 208.185.235.0/24
- 148.59.108.0/23
- 148.59.106.0/23

We suggest adding our entire block of IP addresses, however specific email server IP addresses are listed below:

208.185.229.41	la4prd1.mx.csod.com	208.185.235.43	ld4prd3.mx.csod.com
208.185.229.42	la4prd2.mx.csod.com	208.185.235.45	ld4prd5.mx.csod.com
208.185.229.43	la4prd3.mx.csod.com	148.59.107.25	cdg.mx.csod.com
208.185.229.44	la4prd4.mx.csod.com	148.59.109.25	fra.mx.csod.com
208.185.229.45	la4prd5.mx.csod.com		
208.185.235.41	ld4prd1.mx.csod.com		
208.185.235.42	ld4prd2.mx.csod.com		

2. SPF Records

Slightly different to the above option, Cornerstone will deliver all email messages directly to the far end email server(s). This will ensure adequate email delivery; however, there are still items out of Cornerstone's control, which could delay email delivery.

To implement this solution the client's DNS or email administrator should modify their SPF (Sender Policy Framework) record to include Cornerstone's email severs (listed above) as authorized email delivery sources for the @client domain.

If there is an existing SPF record, then please append the text below to it:

```
"ip4:208.185.229.0/24 ip4:208.185.235.0/24 ip4:148.59.108.0/23 ip4:148.59.106.0/23"
```

Please note that the customer should add all servers that send email on their behalf to the SPF record, not just CSOD servers.

3. DKIM Emails

Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing and allows Cornerstone to take responsibility for transmitting a message directly to the far end email server(s) in a way that can be verified by mailbox providers. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. This verification is made possible through cryptographic authentication.

To enable this solution please contact your Cornerstone Account Manager or Client Success Manager to setup a project to create the relevant setup.

Email Server Safelist

In addition to the techniques above, we always suggest clients work with their email server administrators to add to any safelist all of Cornerstone's email severs (listed above). This will ensure the client's email server trusts email sent from Cornerstone and does not introduce any delays in email delivery.

Note: Safelisting Cornerstone's email servers will enable delivery to the client's email servers, it will not help with public e-mail domains.

Lastly, we suggest all clients validate all destination email addresses to ensure they are valid. Many times, "public" email services will decrease Cornerstone's email reputation score when invalid email addresses are used, which could result in adding to a block list or rate limiting our IP address which leads to delays and in turn email delivery failures.

Appendix 1

Please provide the following information in order to setup an email relay:

- What FROM address or domain will email be sent from? Most likely your HR administrator can provide this information as it is customizable in the Cornerstone Application.
- Should we relay emails to your MX record or are there specific email servers or IP addresses we should be using?
- Should we require TLS or request TLS encryption on emails? If required emails will not be delivered unless a successful TLS tunnel can be established.
- How many concurrent connections does your email server prefer?
- How many messages per connection does your email server prefer?
- Please confirm you have safelisted all Cornerstone IP addresses listed in the Cornerstone Email Server List (see above).