cornerstone

# Customer Email Configuration

Recommendations to improve email delivery rates for Cornerstone CSX customers sending emails with a from-address of @customer domain from their Cornerstone portal

*Last Updated : March 2023*

# Overview

At Cornerstone OnDemand we strive to provide the best possible service to our customers, however with over 100 million users using our highly configurable platform, email message delivery can get complicated.

Customers who configure their Cornerstone portal to send emails to a “public” email service such as hotmail.com, live.com, gmail.com, yahoo.com etc. run a high risk of slow or blocked email delivery. Emails sent from Cornerstone under an @customer domain could be filtered out by email spoof detection methods employed by the recipient’s mail servers.

This document presents the methods and techniques recommended by Cornerstone to improve email delivery rates to your Cornerstone portal users.

## SPF (Sender Policy Framework) Records

The SPF (Sender Policy Framework) standard is a DNS record that defines the mail servers and IP addresses authorized to send messages for your domain. This is the first step to authenticate your emails sent from Cornerstone. When an email message is sent, the recipient’s mail servers check that the mail comes from one of the authorized domains. If it doesn’t come from an authorized domain, the message will be identified as spam.

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.

The customer’s DNS or email administrator should modify their SPF record to include Cornerstone’s email servers (listed below) as authorized email delivery sources for the @customer domain. This reduces the SPAM score with many third-party vendors thus improving email delivery rates.

**Customer Action:**

- You should add to the SPF record the relevant IPs for the region in which you are hosted (*Note: This is not where you are located but where you are hosted with Cornerstone).* If you are unsure, speak to Cornerstone GCS (Global Customer Support) to confirm your Swimlane location.
- SPF record must be set up for each @customer domain being used by the customer within their Cornerstone portal to send emails.
- Customer should add all servers that send email on their behalf to the SPF record, not just Cornerstone servers.

If there is an existing SPF record, then for example if you were in the Japan region you should append the text below to it: `"ip4:18.180.127.81 ip4:54.64.30.13”`

- **Cornerstone Email Server IP addresses**

For those in LAX (Equinix) you need to add five IPs

| | |
|---|---|
| 208.185.229.41 | la4prd1.mx.csod.com |
| 208.185.229.42 | la4prd2.mx.csod.com |
| 208.185.229.43 | la4prd3.mx.csod.com |
| 208.185.229.44 | la4prd4.mx.csod.com |
| 208.185.229.45 | la4prd5.mx.csod.com |

For most AWS regions, there are two IPs to add. For customers using our AWS Data Centers, please note these IPs are different and are as follows (note the region indicated is where you are hosted rather than where you are physically located)

ues1.mx.csod.com / 35.80.141.6  (US)
ues2.mx.csod.com / 44.229.121.55 (US)
les1.mx.csod.com / 18.168.51.200 (UK)
les2.mx.csod.com / 18.168.140.58 (UK)
ees1.mx.csod.com / 3.123.206.219 (EU – FRA SL1)
ees2.mx.csod.com / 3.68.129.51 (EU – FRA SL1)
aes1.mx.csod.com / 3.105.238.148  (AU)
aes2.mx.csod.com / 3.106.50.25 (AU)
jes1.mx.csod.com / 18.180.127.81 (JP)
jes2.mx.csod.com / 54.64.30.13 (JP)

**For customers on FR please also add the EU IPs above**

fes1.mx.csod.com/ 35.181.156.191 (FR – CDG SL1)
fes2.mx.csod.com/ 13.36.253.151(FR – CDG SL1)
frs1.mx.csod.com/15.236.171.222(FR RESTRICTED- CDG SL4)
frs2.mx.csod.com/13.37.17.159(FR RESTRICTED – CDG SL4)

## Email Relay + SPF Records (for best email deliverability)

Cornerstone will relay (transfer) **ALL** emails (customer email messages to the recipients within @customer domain and emails to external recipients, who have addresses hosted by public domains or email services outside customer’s organization) through to the customer’s email server securely. Customer’s email server is then responsible for sending of all emails to the recipients. This guarantees the best delivery results because emails will pass spam-prevention techniques as customer’s own email server is fully authorized to send emails from @customer domain.

We still recommend to use SPF records in addition to relay i.e. adding our sending IPs to the SPF Record (see SPF above section above). This helps improve email delivery rates where emails are sent from a different @customer domain or may not go via the relay.

**Customer Action:**

- In order to begin this process, please have your email server administrator answer the questions in the Appendix 1 and provide those details to Cornerstone GCS (Global Customer Support) along with the GCS Case request to set up email relay for your portal.
  *Note: In order to implement this solution, Cornerstone Engineers will work with the customer's email server administrator as there are many configurable options.*
- Customer's DNS or email administrator should modify their SPF record as specified in the "SPF Records" section above.

## DKIM Emails + SPF Records

Domain Keys Identified Mail (DKIM) is an email signing and 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.

**Customer Action:**

- To enable this solution please contact your Cornerstone Account Manager or Customer Success Manager to set up a project to create the relevant setup.
  Useful reference : https://cornerstoneondemand.my.site.com/s/articles/How-to-enable-DomainKeys-Identified-Mail-DKIM?language=en_US
- We recommend our customers to use SPF records i.e. adding our sending IPs to the SPF Record (see "SPF Records" section above) as this helps improve email deliverability. Please note that there are still items out of Cornerstone's control, which could delay email delivery to recipients.

## Email Server Safelist

- In addition to the techniques above, we always suggest customers work with their email server administrators to safelist all Cornerstone Email Server IP addresses
- This will ensure the customer'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 customer's email servers, it will not help with external/public domain email deliveries.*

- In cases where Customers have external/public domain email users, we suggest customers validate all destination email addresses (user record email ID's) set up in their Cornerstone portal, 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 Cornerstone IP addresses which leads to delays and in turn email delivery failures to you.

## Good email setup hygiene

- We recommend that customers never set the "from address" to an invalid address (e.g. noreply@customer.domain) within their Cornerstone portal Email configuration. This can often trigger SPAM detection and have a negative impact on email deliverability.
- We suggest to either setup a valid email someone can reply to (such as a shared mailbox or similar). This will help improve email delivery.

# Appendix 1 (Email Relay setup questionnaire)

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

1) What FROM address or domain will email be sent from? Your Cornerstone System administrator can provide this information as it is customizable in the Cornerstone Application.
2) Should we relay emails to your MX record or are there specific email servers or IP addresses we should be using?
3) 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.
4) How many concurrent connections does your email server prefer?
5) How many messages per connection does your email server prefer?
6) Please confirm you have safelisted all Cornerstone Email Server IP addresses.
7) Email relays are global to Cornerstone and not environment specific. If you wish to use / test an email relay for a specific environment you should only configure that email within the desired environment portal (pilot, stage, or production).
8) Please provide the SMTP hostname and required port of the server where you want Cornerstone to relay the emails to.

*Note: - Cornerstone allows for authentication based SMTP. If you have an authentication on your email server you will need to please provide the username and password.*