

On-boarding Deliverability Procedure

Emails can be blocked for a number of reasons, however the most common ones are IP address being blocked by the recipient's email hosting server, our domain name is invalid or being blocked and the email message is being labelled as spam or spoof.

To get around this we recommend the following measures:

Whitelist IP Ranges

The IP ranges that Adestra send emails from could be whitelisted. This might be the simplest solution as they'll be able to let through anything that comes from these addresses. Their ranges are as follows

- 46.236.37.0/24
- 185.54.72.0/22
- 81.29.79.128/26
- 185.187.116.0/24

Allowing Domains

We have two different domains

- live.risk.net
- email.risk.net

Live.risk.net is new and is used on account and service emails whilst email.risk.net is used for all Risk.net marketing emails. In the same way that we can add email addresses to safe senders then IT teams can whitelist domains.

Regardless of what we set the From Address as, the actual server log for any email sent by Adestra will show the email using either email.risk.net or live.risk.net. This is also picked up by the recipient server and accepted or rejected.

Add to safe sender - From addresses that we use across the business

- Info@risk.net – BB8 account emails
- subscription@live.risk.net– welcome, trials, renewals & invoice
- e-alerts@risk.net – newsletters
- forename.surname@infopro.digital.com – general marketing

These links below will show the customer how to perform an IP whitelist

Common Internal Email Servers:

[G-Suite](#)

[Microsoft 365](#)

[Microsoft Exchange Server 2010, 2013, 2016, 2019](#)

Common Spam Filters and Appliances:

[Barracuda](#)

[Spam Titan \(Page 98\)](#)

[Mimecast](#)