iMail Best Practices Guide for Migrations – ver 1.1

Best Practices Guideline for Migrations

Purpose

The purpose of this document is to detail the best practices and recommendations from iMail when migrating onto iMail product offerings.

Securemail

Please take note of the following recommendations when migrating to Securemail:

- The first step would always be to ensure you can log into the Securemail UI or see the new customer under your profile that you have provisioned.
- Before cutting over, ensure you have checked that the delivery destination on UI is correct.
- Go through the rules section to ensure you are happy with the configurations for the relevant options (mail size, file type exceptions, etc.). Then you can also set up the relevant notifications you wish your users to receive.
- Configure quarantine reports based on company requirements.
- Ensure all relevant SPF, DKIM and DMARC records are in place.
- Cut over outbound first. It is recommended this be done after hours when mail flow is low. Set up the relevant outbound connection to Securemail from your mail server using auth. Send outbound test mails to ensure they get delivered. Check the UI to confirm that you can see your mails in the outbound message listing.
- It is strongly recommended that you do not configure each mail client to have their SMTP details pointing to Securemail. Users SMTP details should use the server hosting the mailbox and that server should have an outbound route to Securemail as described above.
- Once you have confirmed that the outbound is working, you can change your domains MX records to point to Securemail. Again, we highly recommend this be done after hours when mail flow is low. Send test mails and confirm receipt, then also check the Securemail UI to confirm you can see your mails in the inbound message listing.
- Configure your ITP setup.
- If you have Securemail premium, then set up your DLP configuration.

Cloud Mail

Please take note of the following recommendations when migrating to Cloud Mail:

- Ensure you can log into the reseller portal or see the new customer under your profile that you have provisioned.
- Confirm all mailboxes are present and that the display name information is correct.
- Confirm all mailboxes are the correct size and class.
- Set up the relevant resources and distribution lists.
- Ensure all relevant SPF, DKIM and DMARC records are in place.
- Ensure you can log into an account and send some outbound test mails and that they are going out and being delivered.
- Change the MX records of the domain to point to Cloud Mail. We recommend that you do this after hours or on a weekend depending on the number users. Send test mails to confirm mails are being received in the new mailboxes.
- Change all users' mail clients and phones to point to the Cloud Mail servers. Confirm new mails are syncing.
- Ingest old data into the platform. We recommend:
  - you do this after the MX records are changed to ensure that there are no mails that are lost during the transition.
  - that you stage the ingestion of user's data as all this data will have to be downloaded again per user.
  - 5 users migrated at any one given time per 10Mbps second that is free and available per link.
- A few different options exist for ingesting data, namely:
  - ingest the executive team's data first and then work down through the rest of the business.
  - only ingest the executive team's data.
  - just attach existing data to the users' mail clients as PST files and not ingest the data on the servers.
- Cloud Mail does have an archive mailbox option that can be used where all old data can be ingested into. It is very important to note that this mailbox does not retain folder structure and will be downloaded as an archive folder in the mail clients. This does mean the download sync concerns still exist as per above.

- There is also the option of purchasing Bit Titan licenses which will migrate all mail, folder structure, contacts, and calendars entries across the internet. The speed of this will depend on your connectivity speed.

Branding

Please take note of the following recommendations when migrating to Branding:

- Ensure you can log into the Branding and Securemail UI's or see the new customer under your profile that you have provisioned.
- Set up the relevant signatures and campaigns and run the relevant previews and tests.
- Ensure all relevant SPF, DKIM and DMARC records are in place.
- If you are not already a Securemail client, you will need to set up your outbound routing. It is recommended this be done after hours when mail flow is low. Set up the relevant outbound connection to Securemail from your mail server using auth. Send outbound test mails to ensure they get delivered. Check the UI to confirm that you can see your mails in the outbound message listing.
- Enable branding for one user. Send test mails and ensure it is rendering properly in your mail client (eg: Webmail, Outlook, Gmail). Once confirmed, enable this for all users.

SecureArchive

Please take note of the following recommendations when migrating to SecureArchive:

- Ensure you can log into the Archive UI or see the new customer under your profile that you have provisioned.
- Ensure all relevant SPF, DKIM and DMARC records are in place.
- Cut over outbound first. It is recommended this be done after hours when mail flow is low. Set up the relevant outbound connection to SecureArchive from your mail server using auth. Send outbound test mails to ensure they get delivered. Check the SecureArchive UI to confirm that you can see your outbound mails in the archive.

- Once the outbound has been confirmed, you can change your domains MX records to point to SecureArchive. Again, we highly recommend that you do this after hours when mail flow is low. Send test mails and confirm receipt, then check the SecureArchive UI to confirm you can see your mails in the archive.
- Configure a journal rule on your mail server to send all internal mail to the archive address supplied by iMail S upport. Once this has been set up, send an internal mail to another user, and then check the SecureArchive UI to confirm the mail is in the archive.