Step 5: Go live

Pre-requisites

The fifth and the last step of on-boarding (https://docs.mithi.com/home/how-to-get-started-using-skyconnect) your mailing domain on Sky Connect is the Go live step. Before starting the preparation for the go live, it is assumed that

1. The domain has been provisioned on SkyConnect (https://docs.mithi.com/home/how-to-create-your-skyconnect-domain)
2. The users, aliases and distribution lists or groups have been provisioned (https://docs.mithi.com/home/how-to-provision-users-distribution-lists-in-skyconnect)
3. The integration with your organization's setup (https://docs.mithi.com/home/how-to-integrate-skyconnect-with-your-setup) is complete
4. The data migration strategy (https://docs.mithi.com/home/how-to-migrate-user-data-in-skyconnect) has been worked out and all data that had to be migrated prior to the Go live has been completed.

Preparation

1. Identify your domain host, verify the login credentials and get familiar with the console

2. Make the list of changes to be made to the DNS during switch over or go live.

During the switch over or Go live (https://docs.mithi.com/home/how-to-go-live-with-skyconnect#go-live), you will be required to make changes in the DNS records of your domain in your DNS host. The table below gives the records that will have to be update and the source from where you can get the values to be entered.

DKIM keys and their values	DKIM Key and its value will be generated and provided by the Mithi team
A list of servers to be added to SPF	A Sender Policy Framework (SPF) record indicates which mail servers are authorized to send mail for a domain. Email recipient servers perform a check: “Is this email coming from an authorized mail server?” If not, then the email in question is more likely to be spam. Your SPF DNS record lets the recipient server perform this verification. The SPF check verifies that an email comes from authorized servers. **The list of email servers on SkyConnect will be provided by Mithi.** **For other applications that deliver mail directly, such as as application servers, bulk mailing services etc, get the list from the teams managing them.**
MX	Will be provided by Mithi
DMARC	Will be provided by Mithi

CNAME	Will be provided by Mithi

3. Make a CSV to be uploaded with the COS change

During the Go Live process, the COS (https://docs.mithi.com/home/how-to-provision-users-and-update-user-properties-one-at-a-time-in-skyconnect#understanding-class-of-service-or-cos) for all the users has to be changed to **skyconnectusercos** or **skyconnectadmincos**, depending on whether the user has admin rights.

Once the domain is live on SkyConnect (when MX is pointing to the Trend servers), all new user addition should be done with either skyconnectusercos or skyconnectadmincos.

A CSV with the user id and the post go live COS values (https://mithidocs.knowledgeowl.com/home/how-to-provision-users-and-update-user-properties-in-bulk-using-the-skyconnect-admin-panel) has to be kept ready for application.

4. Decide on the switch over date and time

To reduce the number of possible bounced messages when you change your domain's MX records, we recommend scheduling the change for an evening or weekend or other time when your email volume is low.

5. Inform your end users

All end users need to be informed about:

1. The switch over date
2. The internal helpline which they can contact for assistance

Users who access their accounts using a web client will need to be informed about

1. The URL to the new web client and the link to the videos explaining the working of the new client
2. Instructions to import their personal address books (https://docs.mithi.com/home/how-to-access-contacts-using-baya-v3-web-client), signatures, vacation replies (https://docs.mithi.com/home/how-to-access-email-using-baya-v3-web-client) and calendars from the old system
3. Instructions on what they will see when they login to the new web client (whether they will see old mail or will only new mail will be available on first time login – this depends on the [data migration strategy])

Users who access their accounts from desktop or mobile clients will need to be informed about

1. Instructions to add new accounts (https://docs.mithi.com/home/skyconnect-user-guide) in the desktop/mobile clients.
2. Instructions on securing and viewing older mail depending on the data migration strategy (https://mithidocs.knowledgeowl.com/home/how-to-migrate-user-data-in-skyconnect).

6. Inform Mithi Customer Care about the switch over date and time

Inform Mithi Customer Care about the switch over time, so that they can be on stand-by to assist you.

7. Notify key contacts of the change (optional)

To avoid confusion over any bounced messages, you may want to let some or all of your contacts know about the upcoming change to your email system.

Make sure to include the date and time of the planned change, instructions to resend any bounced messages, and any alternative contact channels people can use for time-sensitive issues. You can emphasize that any downtime should be brief, and that no messages will be lost during the transition; some may simply need to be resent.

Go Live

Step 1: Change the Class of Service for all the users.

Change the Class of service for the users provisioned from **prevsystemusercos** to **skyconnectusercos** or **skyconnectadmincos**, depending on whether the user has admin rights. This step should be done by uploading a csv with the new user properties (https://docs.mithi.com/home/how-to-provision-users-and-update-user-properties-in-bulk-using-the-skyconnect-admin-panel#step-2-add-new-users-and-update-user-properties) that can be uploaded from the Admin Panel (https://docs.mithi.com/home/how-to-use-the-admin-panel-of-skyconnect)

Step 2: Access the DNS console and update the DNS records

Following is the **sample table** showing DNS values for the **sample domain net-it.com**.

Record Type	Hostname	Value	Description
MX	net-it.com	MX 1 mx1.mithi.com MX 1 mx2.mithi.com	Adding MX records routes all inbound mail traffic for your domains to our SecureMailFlow service. **Note: Replace all existing MX records for the domains. Priority to be kept to 0**

TXT	net-it.com	v=**spf1** include:mem.mithi.com include:[app server] -all	1. Replace the entry for the existing mail server with **mem.mithi.com** **2. Make sure that all the application servers which send out mail for your domain are also listed in the SPF records. (Each application server will have to be included)** **(The list of SPF records has to be ready as mentioned in the preparation step above)** 3: Replace soft fail with hard fail. Soft fail is specified by ~all and a hard fail by -all.

TXT	TM-DKIM-20180222144920._domainkey.net-it.com	v=DKIM1; k=rsa; p={ }	A DomainKeys Identified Mail (DKIM) record adds a digital signature to emails your organization sends. Email recipient servers perform a check: “Does the signature match?” If so, then the email hasn’t been modified and is from a legitimate sender. Your DKIM DNS record lets the recipient server perform this verification. The DKIM check verifies that the message is signed and associated with the correct domain. To get the digital signature to be added to your DNS please write to us and we will generate the **DKIM key** and its **value** to be added to your DNS. As with SPF, all the sources should support DKIM
TXT	_dmarc.net-it.com	v=DMARC1; p=none; sp=none; pct=100	DMARC specifications build on SPF and DKIM and when implemented appropriately enable organizations to reduce spam and phishing emails sent to their customers and employees from unauthorized senders and domains.

Note: Please ensure that there is no other record (A/CNAME) configured for the above mentioned names. If there is, please remove those records.

Note : CNAME Access records are the secure access host names/URLs for your end users. This target host name is in the format .mithiskyconnect.com and comes built in with SSL support. These will be configured by Mithi in the mithiskyconnect.com (https://mithiskyconnect.com) DNS server.

Step 3: Confirm the changes

Once you have updated the DNS entries, verify the changes using popular network diagnostic and lookup tools available on internet. The steps below are for Network Tools

1. Go to the Network Tools (https://mxtoolbox.com/NetworkTools.aspx) site.
2. Select DNS Records and click on **Advanced Tools**
3. Specify the **domain name** and select **Go**
4. The DNS entries for your domain will be displayed.

Post Go Live

1. Post go live, test the following using the web client and desktop/mobile clients:
    a. Access to the new mail boxes
    b. Internal and external mail flow
    c. Mail flow from connected applications
    d. Global Address book
2. Disable the catchall user for the domain (This was required during the phase where the domain was hosted on the server but not live.)