Step 3: Go Live

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-clrstream#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. **This list should include your email servers and other servers that deliver mail directly, such as as application servers, bulk mailing services etc,.**
MX	Will be provided by Mithi
DMARC	Will be provided by Mithi

3. 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.

4. 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.

5. 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

1: Access the DNS console and update the DNS records

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

Record Type	Hostname	Value	Description
MX	net-it.com	in.hes.trendmicro.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:[mail servers] include:[app servers] -all	1. Make sure that all the mail and 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.

2: 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

Post go live, test the following using the web client and desktop/mobile clients:

1. Internal and external mail flow
2. Mail flow from connected applications
3. In case of ClrStream Continuity, ensure that inbound and outbound mails are delivered to the secondary mailboxes.