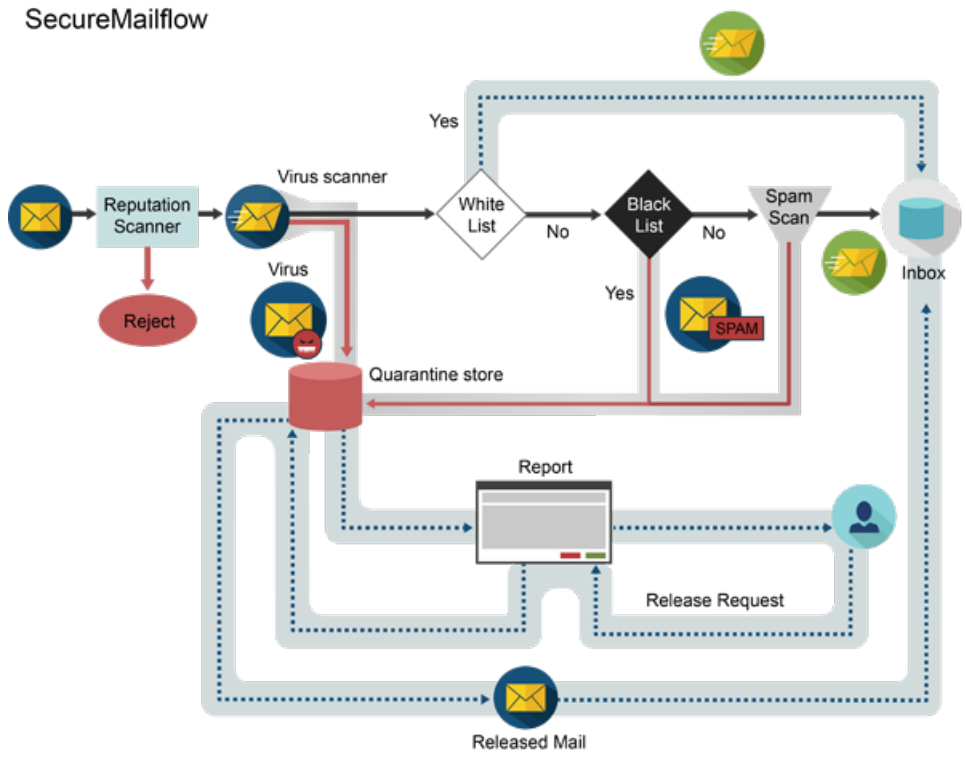
SkyConnect SecureMailFlow Administration FAQs

How does the SecureMailFlow work?

The SecureMailFlow service in Mithi Skyconnect is designed to protect your inbox from spam and virus mails. It also helps prevent your recipients from receiving spam mail, which you may send inadvertently. This service sits in the inbound and outbound mail flow path and ensures that every mail which you receive from the Internet is scanned for spam and virus. Any mail detected as a spam/virus as per the rules and policies defined in the SecureMailFlow service, is either rejected or quarantined into a separate storage per domain. The SecureMailFlow service is an integral part of the Mithi SkyConnect service for all our customers and is configured to scan all inbound mail and outbound mail.



Working of the Inbound Mail flow

The MX pointers for our customers' domains point to the SecureMailFlow servers, such that all inbound mail traffic (from Internet) for the domains lands on these servers. After determining the reputation and technical cleanliness of the source of connection for the mail, these servers first scan the mail for containing any virus. If the mail contains a virus, it is simply quarantined, with no further scanning. This action applies (overrules) even if the sender is whitelisted. Once the mail passes the virus stage, and the sender is not whitelisted or blacklisted, it's content and attachments are scanned for objectionable "patterns" and if found, the mail is marked as a spam and quarantined.

Working of the Outbound Mail flow

Any mail sent by any user of our customer (outbound), is not scanned for spam. The outbound mail scanning is enabled for the domain on request. If enabled all outgoing mail are scanned for viruses. If any virus infection is

detected, the mail is simply quarantined.

Quarantine Management

The quarantine store can be managed by the administrators of our customers. They get access to the **Quarantine management console** of SecureMailFlow, from where they can search for and release specific mail if required. Accessing this console is primarily required to seek out false positives (a mail that was actually a clean mail but got detected as spam) and release them to the end users.

What causes the email domain being rejected by the security appliance or gateway security service at the customer end? How does Mithi's Cloud based Email Hosted service deal with it?

There could be several reasons for this and the exact reason is best given by the team supporting that security service or appliance. However, generally the following points can be considered

- If only mail from specific senders of your domain is being rejected, most likely those email ids are blacklisted on the appliance or these email ids are sending spam due to which the appliance is rejecting these mail.
- Due to continuous spamming activity from your domain or IP address, the reputation of your source (IP and email domain) becomes poor (possibly on a rating scale), due to which the mail are rejected by the appliance.
- The IP address of your outgoing relay server is blacklisted on the spam cop sites, which reduces its reputation and may cause the appliance to reject mail.

If you notice, the common thread essentially (root cause) is that there is a lot of spam generated from the domain users (internal spam). The way to protect against this happening is to ensure that email originating from your domain is always as clean as possible.

What is a false positive and a false negative?

A “false positive” is a “clean mail” that was mistakenly detected as a spam mail by the spam scanning engine.

With anti-spam detection enabled, the content of each email sent through the SecureMailflow service is scanned and searched for patterns that are more or less likely to be seen in spam and phish emails. To do this, the SecureMailFlow service contains a set of rules called spam rules, which are constantly updated via streaming updates.

Each rule is assigned a score and on analyzing an email, the engine adds the score of all rules triggered to give a total score called the spam score. The engine compares the spam core to defined threshold-based actions in the anti-spam settings. Sometimes the score determined by the Spam detection engine does not reflect the correct nature of an email, which causes a false positive detection, or lets the mail pass through as a false negative detection.

IMPORTANT: Mithi cannot divulge the meaning of spam rules for security reasons. This could allow spammers to bypass the anti-spam solution.

What level of spam protection does SecureMailFlow offer?

The SecureMailFlow service offers a guarantee on the following (based on a back to back guarantee from Mithi's vendor of email security.

- Spam protection: Guaranteed 99.9% spam detection
- Virus protection: Guaranteed 0 email viruses will pass through
- False positives: Guaranteed less than 0.003% false positive rate.

What is mail scrubbing?

As the word "scrubbing" implies, it is the process of scanning, analysing and cleaning the mail flow of viruses and spam using a variety of security engines and techniques.

If an admin forgets the password for the SecureMailFlow console, would it be possible for the Mithi Team to help reset it ?

Yes the Mithi team can do this for you. Please raise a ticket to the Mithi Support team.
(https://docs.mithi.com/home/how-to-access-mithi-help-desk#raising-a-ticket)

How long are the spam and virus messages kept in my quarantine store?

They are retained for a period of 30 days. This is not configurable per customer/domain.

Can individual users on Mithi SkyConnect get daily spam reports from the system? Can we view all the mail blocked by the Spam checker and release them if required?

The spam and virus report (mail events) for each user (the entire domain) will be sent to the respective user (if the reports feature is enabled for the domain). This report will come direct from SecureMailflow and will have all the details of every mail sent and received, every mail rejected for spam with reason.This report will give options to allow, disallow email ids and domains and also release mail which are quarantined in case they are false positives. In addition to this, the IT administrator of the domain has access to the SecureMailflow console, which allows him to search amongst all the mail traffic of the domain, release mail, whitelist, blacklist etc.

Since there are no daily mail reports now, how will my user know if any valid mail is quarantined ?

A valid mail getting quarantined is a "false positive". Our partner for SecureMailFlow is one of the most mature and among the top providers of email security worldwide. As part of their SLA, they provide a guarantee on a very low level of false positives (less then 0.003%).

Keeping this in mind, considering that the with this level of false positive rates guaranteed, the end users will have no use for the reports, we took the decision to simplify the end user operations and disable end users quarantine reports.

If any of your users misses a mail that was expected (barring newsletters and news subscriptions which are most likely to get quarantined), please educate them to refer these cases to you and you can search in the quarantine for these mails and release them.

For how long are the spam/virus logs/reports maintained on the clean mail service of Mithi Skyconnect?

They are retained for a period of 30 days. This is not configurable per customer/domain.

Why Black list & White list provision is not available?

Considering the guarantees provided by our email security partner, which is a spam detection rate of 99.9% and a false positive rate of 0.003%, we feel that there wont be many cases needing a white list or a black list. We are in effect delegating the heavy listing of spam detection to the email security service entirely.

Thus we have disabled the interface, which allows our customers to add or remove white lists or black lists.

However if in any condition, you feel the need for this, all you need to do is raise a query about it to our helpdesk via support@mithi.com.We will review the case and help you decide if the action is necessary.

What should users do if they receive spam mails?

In the rare case if a user does receive a spam in their inbox, please forward that mail as an attachment to our help desk for analysis. Our team will share this with the Global Threat protection network of our email security partner for further analysis.

Can I change the password of my login to the Secure Mail Flow console of my domains in SecureMailFlow?

Yes, you can. Refer the topic How do I change the password of my login to the Secure Mail Flow console of my account? (https://docs.mithi.com/home/how-login-to-the-secure-mail-flow-console#changing-the-password-from-the-console)

Will the sender mail having the same Sender-Id and Recipient-Id will pass through SecureMailFlow ?

On an inbound path, there is no genuine case to receive a mail from a local sender (user on Mithi SkyConnnect), hence these mails are all potential spam. In all likelihood, these would be detected by our email security vendor's Threat protection system and such mails would be marked as spam and quarantined.

I as a customer of Mithi SkyConnect manage multiple domains, will I be able to manage them from a single console login?

Yes, you will be given access to a console via a login id and password. This will allow you to manage the quarantine, and spam rules for all your domains and all the users within all these domains.

Why it is displayed on the SecureMailFlow Console that " Data Collected within last 2 hours may not displayed" . Does this mean that the current logs cannot be displayed ?

In the backend, as mails are transacted, the information is fed back to the console via a series of flows. The priority is given to the actual flow and it may be possible that depending on the load, updating of the console may be slowed down. In most cases however, we have observed that the updates to the console are quite quick.

Can I search for specific mail in my Quarantine store?

Sure you can. For more information refer the topic How to search for a specific mail in my Quarantine store? (https://docs.mithi.com/home/how-to-search-through-the-quarantine-using-the-secure-mail-flow-console)

Can we check the reason of blocking of mail in Quarantine ? If yes, where ?

Yes sure you can. Search for the mail in the Logs (https://docs.mithi.com/home/how-to-track-mail-flow-using-logs-in-the-secure-mail-flow-console) and check the last column, which gives the reason for the quarantine.

If I have a virus mail for multiple recipients and one of them is whitelisted, will the mail with virus be delivered to the whitelisted id?

No. Virus mails are isolated before any further processing of rules, which include whitelisting as well. Refer to the diagram of the mail flow in the topic Secure Mail Flow Overview (https://docs.mithi.com/home/what-is-secure-mail-flow-service-in-skyconnect) to understand how this works.

Does Spam/Virus protection start immediately when a new user is added? Or do I need to do anything on the SecureMailFlow console?

There is nothing for you to do on the Secure Mail Flow system when you add users to your domains. Secure Mail Flow has been configured only with your domains and it is ready to receive mail for any user on your domain. Technically any user @ your domain.

So as soon as you add a user, the spam protection engine is active immediately.

What are the applicable mail flow policies on the Secure Mail Flow service (clean mail service) of Mithi SkyConnect?

The SecureMailFlow service has the following global rules/restrictions deployed. These are besides the controls deployed on the mail server end where your users will directly connect to send and receive mail. These are documented herea.

Maximum mail size permitted on the Inbound and Outbound path is: 50 MBb.

There is no limit on the attachment size, as long as the total mail flow size is within the above specified limitc.

RBL checks on the Inbound path are configured to scan for low reputation connections and discard them before entry.d.

All mail detected as spam/virus are isolated into a quarantine system.