SYNAQ Securemail Technical Requirements and System Limits

OVERVIEW

OUR COMMITMENT TO SECURITY AND STABLE SERVICE DELIVERY

While the SYNAQ Acceptable Usage Policy ('AUP', viewable here), service definitions, configurations, and limitations as defined in this document are considered complete as of the time of this publication, our service pledge to our clients requires us to stay competitive in an ever changing email environment.

As such, as new threats emerge and evolve in the real world, our services will likewise adapt to meet and combat them. Therefore, in the interests of protecting our clients and the services they rely on, from time to time it will be imperative that we add to or amend the documentation contained herein. All changes made to this document will be driven by our commitment to providing our clients a secure, stable and reliable service. As such, we will require you to understand and agree to the following:

This is a living document, changing as needed to meet current and future service needs. As and when such adjustments are made, they will be considered part of this document, binding you to observe the limitations and service configurations contained herein.

Addenda or amendments to this document will be designed to complement and enhance the service and the protection we offer our clients. As such, this clause will not void any prior agreement or negotiated exceptions (see below) entered with our clients, other than in the case of infringement or abuse as already covered in this document and in the terms of our AUP.

SERVICE CONFIGURATION OVERRIDES OR LIMIT EXCEPTIONS

Any Limit Exceptions (LE) and Service Configuration Overrides (SCO) negotiated with, and implemented, for a client, by SYNAQ, are made in good faith.

Should a case arise where SYNAQ has implemented SCO's or LE's for a client, and the client's usage of the service violates the spirit of the SYNAQ Acceptable Usage Policy ('AUP', viewable here), or is deemed to be abusive, harmful to other users of the service, or disruptive to the health of the Securemail service; SYNAQ reserves the right to revoke all LE's and/or revert all SCO's, and bind the client to the limits and configuration defaults as specified in this document.

SMTP Authentication Requirements

Securemail offers its clients two methods of SMTP Authentication for outgoing email transmission, namely:

1. SMTP Authentication with a Username and Password. This method is normally implemented using a Smart Host[1] configuration implemented on the client's on-premise email services, but in certain circumstances it may be implemented on a per-sending user basis.
2. IP Address Authentication, where a client's provisioned email domain or domains are allowed to relay mail outbound from a client's static public IP Address or range of IP Addresses, without the need to use SMTP Authentication (as in 1 above).

MINIMUM REQUIREMENTS FOR SMTP AUTHENTICATION WITH USERNAME AND PASSWORD PER SENDER ADDRESS

Securemail requires that clients create SMTP Authentication passwords using at a minimum, the following password policy:

- Minimum password length = 8
- Minimum upper case characters = 1
- Minimum lower case characters = 1
- Minimum punctuation symbols = 1
- Minimum numeric characters = 1

SENDER VERIFICATION ON THE CLIENT'S SERVER

When using either of these methods the client's mailbox server must support Sender Verification in the form of a SMTP Protocol lookup, to confirm a sender is indeed a valid and real mailbox or email alias on their mailbox server.

SMTP TRANSMISSION LIMITS

Securemail is not a bulk email service. However, SYNAQ will allow its clients, on a case-by-case basis, to declare named bulk-sending email addresses.

In such cases, SYNAQ will then engage in negotiations with the client to provide specialised bulk mail routing for these accounts to ensure the client's business needs are met while the Securemail system as whole and its other clients are not adversely affected.

SMTP - MESSAGE RECIPIENT LIMITS

- No more than 50 recipients per message.
- No more than 200 recipients per sender address per 5 minutes.

SMTP – MAIL SUBMISSION RATE LIMITS:

Mail throttling, (implemented as a SMTP temporary defer) is enforced by Securemail when the following submission rates are exceeded:

- Submission exceeds 200 emails per sending host per 5 minutes.
- Submission exceeds 200 emails per sender address per minute

USE OF EMAIL ADDRESS LISTS

SYNAQ will not discourage the use of sending to email address lists, provided that all lists only consist of valid and legitimate contacts and do not contravene the Unsolicited Bulk Email (UBE) or Unsolicited Commercial Email (UCE) regulations as stipulated in the AUP. Any sending address or SMTP username which routinely, or excessively exceeds the threshold for invalid recipient addresses will be considered as sending UBE or UCE, and the account will be locked out to protect other users and to protect the integrity of the Securemail service.

SMTP - INVALID RECIPIENT LIMITS

- No more than 2 invalid recipients per message.
- No more than 10 invalid recipe ents per sender address per 5 minutes.

Domain Relay Limits

Securemail will only relay email for domains that are owned by and registered to the client. Securemail will not relay any Freemail or Internet Service Provider generic domains E.g. gmail.com, yahoo.com, hotmail.com, telkomsa.net, webmail.co.za etc.