# *SpamTitan on Demand Quick Setup*

### 1. Load the License and Configure SpamTitan

Via System Setup->License load the license you received via email. Configure SpamTitan see SpamTitan Administrators Guide

### 2. Configure / Edit your MX records

The MX record(s) for your mail domain(s) need to be changed to point to the new SpamTitan IP address you have received. Once you have changed your MX records it will take up to 1 day for the changes to be propagated globally.

### 3. Restrict inbound mail to SpamTitan

Via your Firewall set or change the rule for SMTP (tcp/25) to only allow mail from the new SpamTitan IP address. On SpamTitan set the destination server for your domains to be the external IP address of your mail server normally your Firewall's external IP address. Use the same setting for Dynamic Recipient Verification.

### 3. Route outbound mail via SpamTitan

If required you can route your outbound mail via SpamTitan in this case you need to either

- Add the external IP address of your mail server normally the Firewall to the Trusted Networks section of System Setup->Mail Relay , or
- Set up SMTP SASL and you will need to allow access to your LDAP (tcp/389) for the SpamTitan IP address.

### 4. Load an SSL certificate to allow users manage their quarantine reports

Via Settings->SSL load a valid SSL cert or create a self-signed certificate.
Via Settings->Acccess/Authentication enable HTTPS and disable HTTP.
Via Quarantine->Settings enable Use HTTPS.

**Notes:** It takes up to 15 minutes to deploy. Please change the admin password.
Never change the assigned IP address.