Security Settings for Fujitsu Interstage Email OpenId Provider

# Problem Statement

Email OpeId provider allow automatic Registration for new User. There is a potential risk of abuse the system to send spam email. We need to put some security measure to stop the spam.

There is currently two type of protection is added.

1)Added Recaptcha in the Registration form for Human verification.

2)Automatically put ip in blocked list if spam is detected.

# Human Verification (Recaptcha )

To stop automated spamming in registration process, Recaptcha feature is added in the Registration form.

Recaptcha is a free service provided by Google. To activate Recaptcha feature in the Email OpenId provider application, you need to set following two parameter in the configuration file.

captchaPublicKey=

captchaPrivateKey=

You can sign-in to Google to get “captchaPublicKey” and “captchaPrivateKey “ for your domain.

### Here is the address [reCAPTCHA](http://recaptcha.net/) where you can find more information. Follow the link [GET reCAPTCHA](http://www.google.com/recaptcha/whyrecaptcha) to get the reCaptcha key for your domain.

Use localhost in your Openid server registration form url ,in case you want to avoid the domain verification for testing

e.g. <http://localhost/eid/?openid.mode=register>

# Automatic IP Block

During startup Email OpenId provider application will generate a file “blockedIp.txt” in WEB-INF file if the file does not exists.

OpenId provider will keep track of registration attempt from a remote IP in the memory. Each time a new registration request is made and before sending a verifying email the remote IP the request is tracked.

If there is a previous record of this IP the registration attempt will be incremented, Otherwise a new entry for that IP will be entered.

Maximum number of record kept in memory is 1000. Once it reach the limit, it reduce to 30% based on the latest access record.

If there is 10 request from an remote IP in less than 30 minute, the IP address will be logged in the “blockedIp.txt” and deny any future request from that IP.

You can manually enter or remove an IP in the “blockedIp.txt” to block or unblock an IP.

The input parameters in the file are as follows.

192.168.0.12=block

192.168.0.13=block

Whenever an IP is put in the blocked list a log record is printed in System.out with the information of the I blocked IP and the attempted Email Addresses.