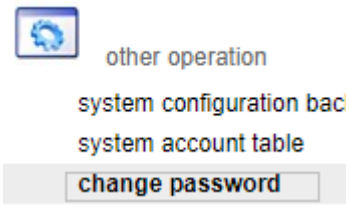
SYSTEM ADMINISTRATION MANUAL FOR STEEP

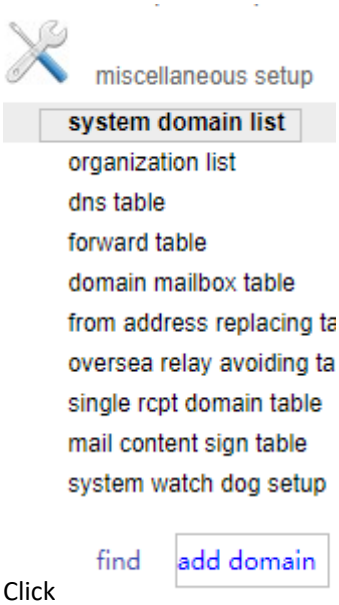
This manual introduces how to operate the steep administration user interface.

1. Change administrator's password

The first thing is to change administrator's password when you log into system first time.



2. Domain list management



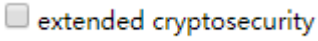
Click to add domain into system, please specify the "end date", which will make the domain out-of-date after the domain expires. Domain default password is empty if you don't specify it.

If you want to edit the domain information or expand the limitation, please click "view & edit"

maximum space	maximum users	operation
100G	10	view & edit | delete

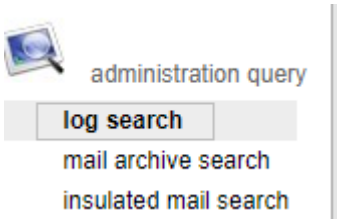
click 

to change domain's password in "edit domain" page



feature control the password expiration of accounts under the domain, the period can be specified in domain administration with "configuration -> default password expire date". You also can specify the "password expire date" in "user list" of domain administration.

3. Log search



You can search smtp and delivery information in "search log" page.
You can specify the IP address (can be full address like "192.168.1.1" or partial address like "192.168"), from address or domain (test.com for domain without @), rpct to address or domain, time range.

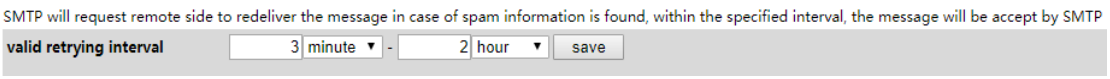
2019/07/19 21:15:50 remote MTA IP: 192.168.1.210, FROM: test@mail.com, TO: test1@test.com return OK, queue-id:55

2019/07/19 21:15:50 SMTP message queue-ID: 55, FROM: test@mail.com, TO: test1@test.com message /u-data/m1/v1/1/eml/1563585350.6.mail1.herculiz.com is delivered OK

Smtp log item and delivery log item are associated with the queue-ID.
If a mail is intercepted by anti-spamming filter, log item looks like below

2019/07/19 21:15:16 remote MTA IP: 192.168.1.210, FROM: test@mail.com, TO: test1@test.com dubious mail is cut! reason: 000041 you are now sending spam mail!

"Dubious mail" normal represents temporary reject by smtp server with the code 450, which allow the remote side redeliver the mail in a while. The smtp server will accept message when remote side delivery the mail next time. The valid interval can be set in the page "system setup->basis setup"



If you get "illegal mail" in the log item, which means the anti-spam filter consider the mail as spam and reject the mail with the code 550.

4. Anti-spam setup

If the anti-spamming filter misjudges one mail as spam, you can avoid misjudgment by:

1. **IP white list**

   There are 3 types of white list, normal white list means avoid some type of anti-spam method, this type is a bit professional, for a normal user, please do not choose this type. Extended white list forces the smtp server accept all connection request without any auditing method plus the normal white functionality. The absolute white list accepts all from the IP address. We recommend the user to use absolute white list for avoiding misjudgment.

2. **tagging address list**

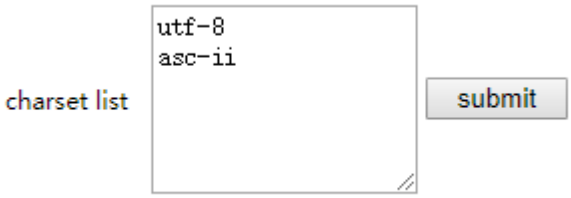
If we want to accept all mail from some specified sender or to some receiver, please add the address into the tagging address list.

3. **domain white list**

You can also add domain name into domain white list for avoiding misjudgment. Most anti-spam method can be avoided but still there're some methods cannot be avoided by this white list.

4. **keyword list upload**

Anti-spam filter will reject mail immediately at the time of smtp session. You must specify the charset first before you upload the keyword list file



The anti-spam filter will only intercept the mail with the charset, and the charset of uploading lists must be the first charset in the charset list.

5. **anonymous keyword**

Anonymous keyword is also a keyword list, the difference between "keyword list upload" and "anonymous keyword" is that the "anonymous keyword" will be isolated after smtp session, which means the sender of mail will not get the bounce mail if the mail is recognized by "anonymous keyword" anti-spam method.

6. **IP-domain table**

If a domain has SPF record, the anti-spam system will check that record and comparing it with the source IP of smtp session. If a domain doesn't have SPF record, you also can specify the forcible check on that domain by add item into IP-domain table. IP class should like this 202.94:64.89:41.126: IP ranges should be separated by ":"

5. Miscellaneous Setup

1. dns table

   If delivery cannot get a domain's record or you want to redirect mail of certain domain to certain IP address(es), you can specify item in "dns table". IP addresses should be separated by ":" like "192.168.1.100:192.168.1.101:"

2. forward table

   If you want to forward mails to some destination mailbox, please add items in this page. Supervised object can be either email address or domain.

3. organization list

   This feature is for associating domains for public address book in outlook (NSPI), accounts under each domain can see all addresses of associated domains. Please first add organization before associating the domains.