Using SMTP Authentication in FortiMail

Worried about a brute force password attack? SMTP authentication mitigates the problem by tracking the IP addresses of the offending client attempting to connect to the box. SMTP authentication can detect, block, and punish hackers. This recipe guides you through the process of enabling SMTP authentication and checking the SMTP authentication score and record.

Enabling SMTP Authentication

First we'll need to enable SMTP authentication.

Go to **Dashboard** > **Console**. Enter the following commands to enable the feature. And if there is a gateway before the mail server, add the gateway to the exempt list.

```
config system security authserver
  set status enable
      config exempt-list
    edit 1
      set sender-ip-mask 172.20.140.232/32
    next
  end
end
```

Checking SMTP Authorization Score and Record

With SMTP authentication enabled, we can now look at a few things you can perform in the CLI:

1. You can display and delete automatically added IP addresses:
   #diagnose system authserver auto-exempt display
   and to delete the IP address, enter
   #diagnose system authserver auto-exempt delete xxxx
2. You can display the iptables statistics for currently blocked IP addresses: #diagnose system authserver iptables ipv4
3. You can get the authentication records for a specific IP address:
   #diagnose system authserver records 172.20.140.230
4. You can get the authentication status of a specific IP address, showing you if it's safe or if it's blocked:
   #diagnose system authserver status 172.20.140.231