Hermes SEG Build 211019 Update

> **This is a MAJOR update that introduces many breaking changes.** This update will install and configure Nginx HTTP server which will enable the Admin and User Consoles to be accessible over Ports **80** and **443** in lieu of Apache HTTP sever over port 9080.

This update will install new packages from the Ubuntu repositories. Ensure your appliance has access to the Internet before proceeding.

It's important to understand that after this update is installed, Hermes SEG wil no longer be accessible over port 9080. You must instead access Hermes SEG over port 80 and 443. You must adjust any port forwards you may have in your firewall from port 9080 to port 80 and 443 and completely disable access to port 9080.

When the update has finished installing, it will prompt you to reboot your system. The normal method of going to **System --> System Reboot & Shutdown** will not work for this update. You must instead reboot your system by using the command console and typing the following command:

```
sudo reboot
```

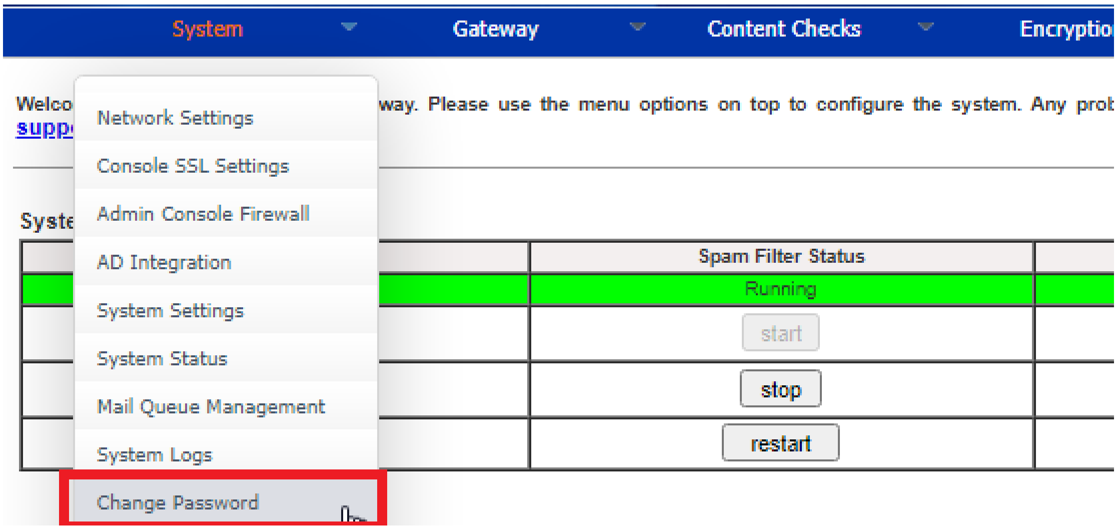
After the system reboots, you must access the Hermes SEG Admin console by using the following address where **<SYSTEM_IP>** is your system IP address (Do NOT use port 9080):

```
https://<SYSTEM_IP>/admin/
```

This update will reset the admin system account password back to **ChangeMe2!**. After rebooting your system, you must login with the username of **admin** and the password of **ChangeMe2!**.

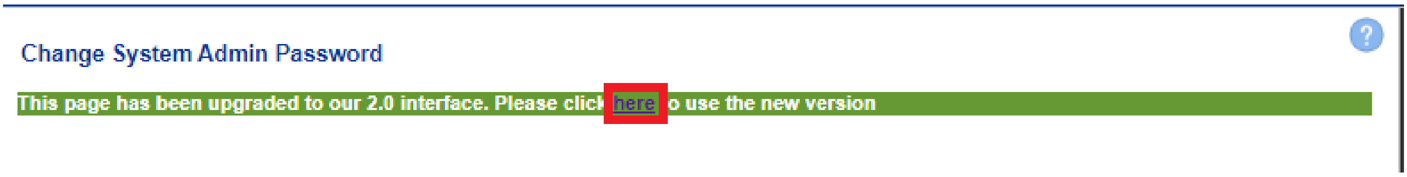
Change the password by navigating to **System --> Change Password** (**Figure 1**):

Figure 1



In the **Change System Admin Password** screen, click the link to use the **2.0 interface** (**Figure 2**):

Figure 2

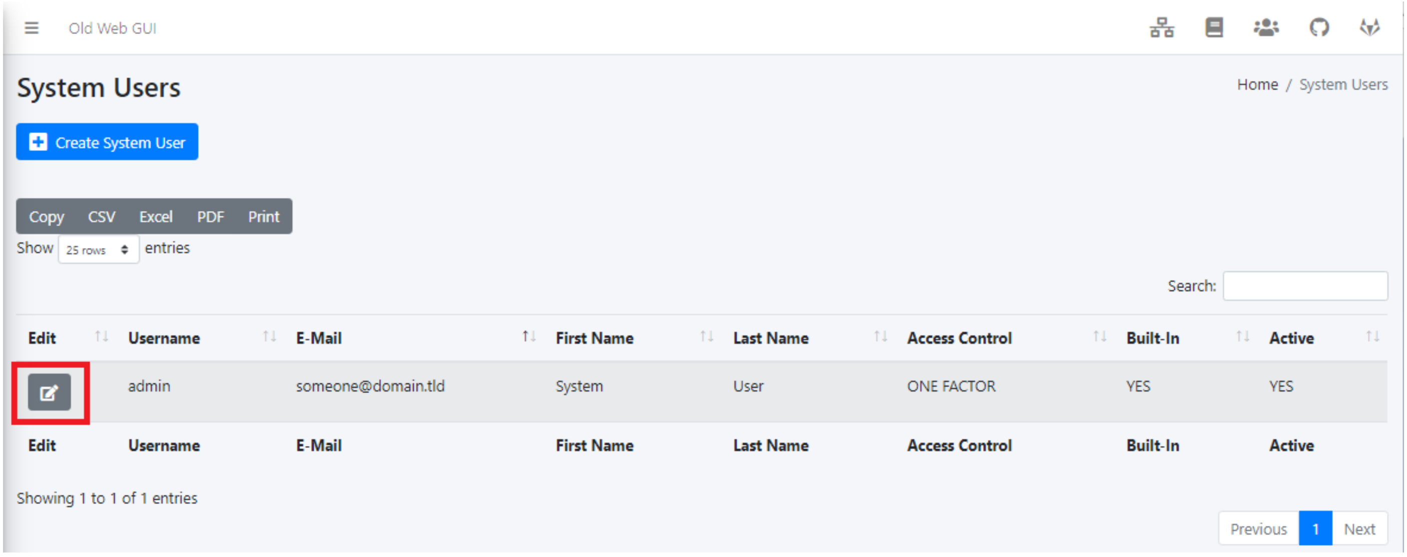


Change System Admin Password

This page has been upgraded to our 2.0 interface. Please clicl here o use the new version

In the **System Users** screen, click the **Edit** button for the **admin** account (**Figure 3**):

Figure 3



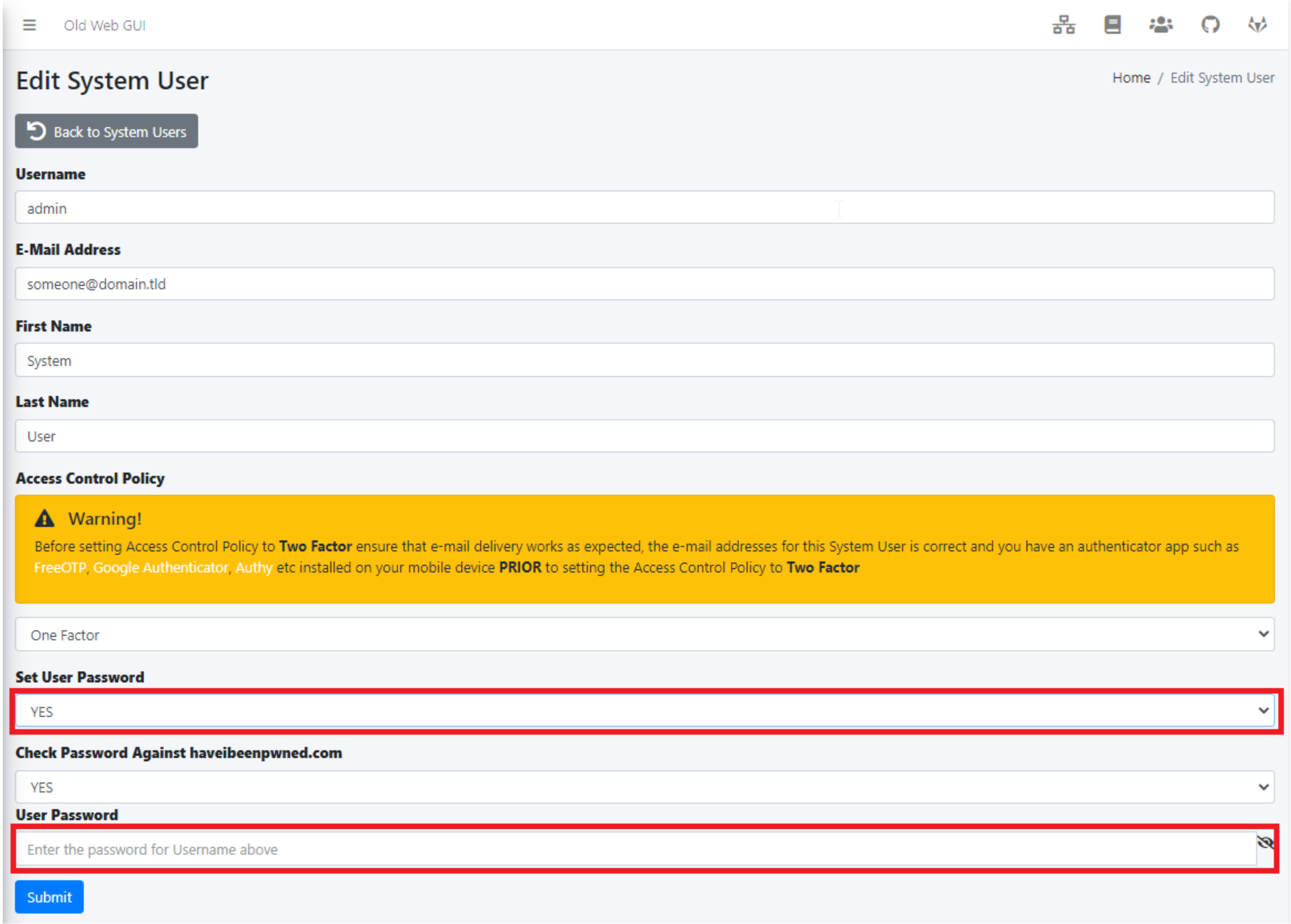
System Users

Edit	Username	E-Mail	First Name	Last Name	Access Control	Built-In	Active
	admin	someone@domain.tld	System	User	ONE FACTOR	YES	YES
Edit	Username	E-Mail	First Name	Last Name	Access Control	Built-In	Active

Showing 1 to 1 of 1 entries

In the **Edit System User** screen set the **Set User Password** drop-down to **YES**, enter a new password in the **User Password** field and click the **Submit** button (**Figure 4**):

Figure 4



≡ Old Web GUI

Edit System User

Home / Edit System User

Back to System Users

Username

admin

E-Mail Address

someone@domain.tld

First Name

System

Last Name

User

Access Control Policy

Warning!

Before setting Access Control Policy to **Two Factor** ensure that e-mail delivery works as expected, the e-mail addresses for this System User is correct and you have an authenticator app such as FreeOTP, Google Authenticator, Authy etc installed on your mobile device **PRIOR** to setting the Access Control Policy to **Two Factor**

One Factor

Set User Password

YES

Check Password Against haveibeenpwned.com

YES

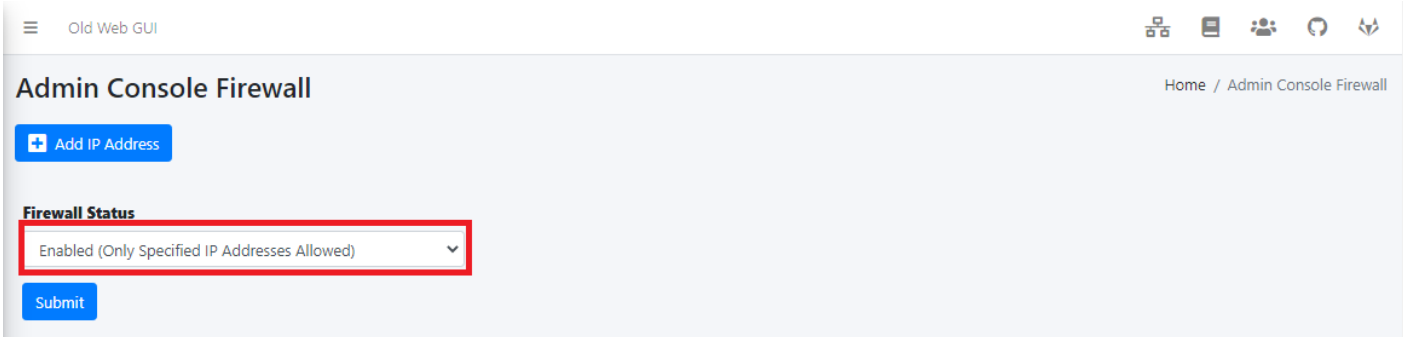
User Password

Enter the password for Username above

Submit

This update will disable the **Admin Console Firewall**. Re-enable the firewall by navigating to **System --> Admin Console Firewall**, set the **Firewall Status** drop-down to **Enabled** and click the **Submit** button (**Figure 5**):

Figure 5



≡ Old Web GUI

Admin Console Firewall

Home / Admin Console Firewall

Add IP Address

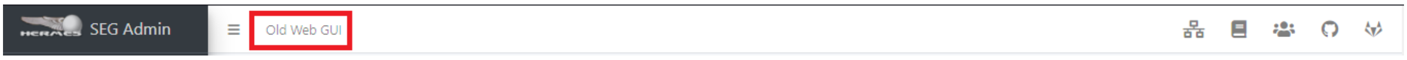
Firewall Status

Enabled (Only Specified IP Addresses Allowed)

Submit

You must edit the **Secure Portal address** and remove the port 9080 from the URL. Click on the **Old Web GUI** link on top of the page (**Figure 6**):

Figure 6



SEG Admin ≡ Old Web GUI

In the Old Web GUI, navigate to **Encryption --> Encryption Settings** under the **Secure Portal Address** field, remove the port number part. For example, if you had the following Secure Portal Address:

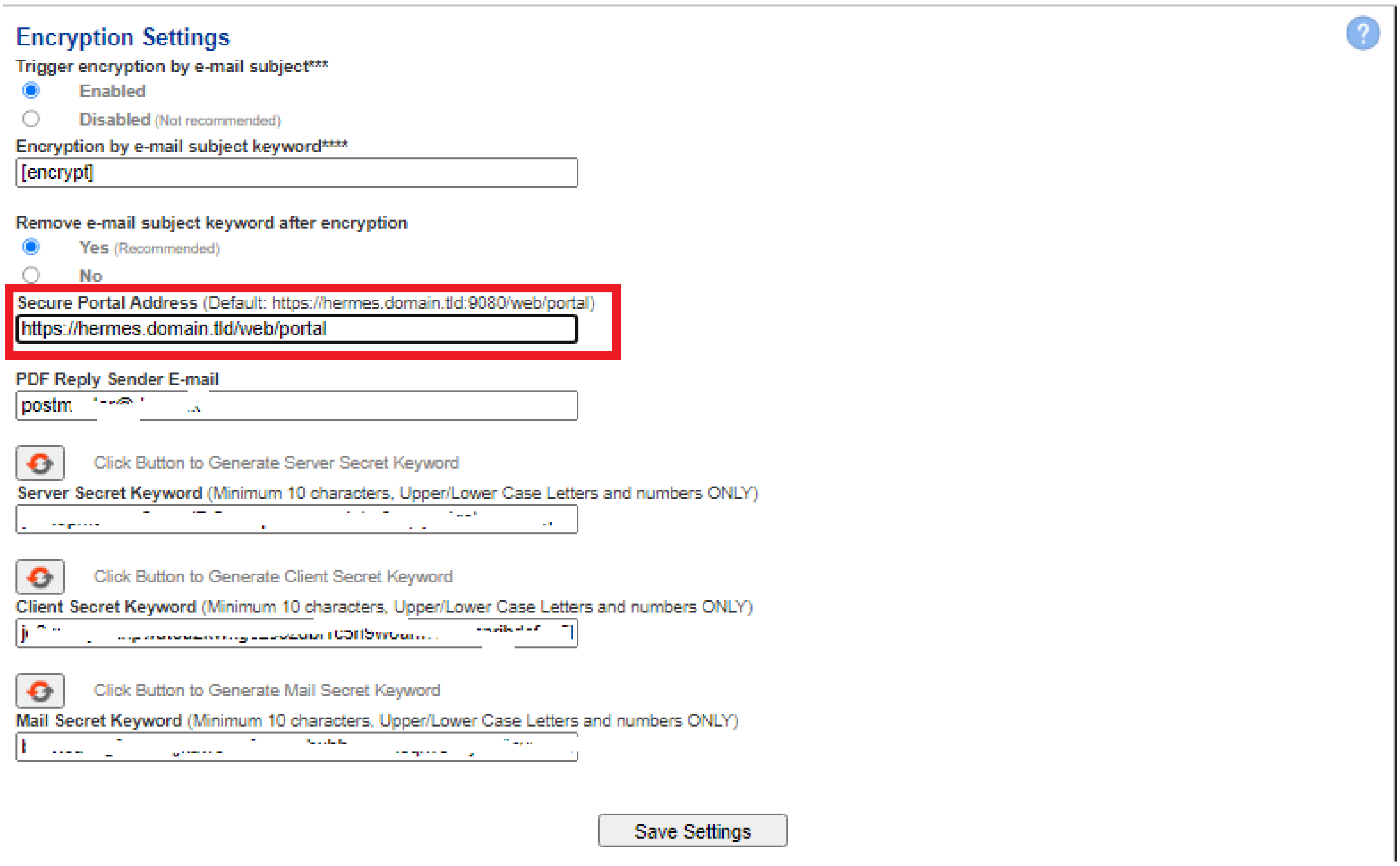
```
https://hermes.domain.tld:9080/web/portal
```

Remove the **:9080** from it so it looks like below:

```
https://hermes.domain.tld/web/portal
```

Click the **Save Settings** button and after settings are saved, click the **Apply Settings** button (**Figure 6**):

Figure 6



Encryption Settings

Trigger encryption by e-mail subject***

● Enabled

○ Disabled (Not recommended)

Encryption by e-mail subject keyword****

[encrypt]

Remove e-mail subject keyword after encryption

● Yes (Recommended)

○ No

Secure Portal Address (Default: https://hermes.domain.tld:9080/web/portal)

https://hermes.domain.tld/web/portal

PDF Reply Sender E-mail

postm[redacted]

Click Button to Generate Server Secret Keyword

Server Secret Keyword (Minimum 10 characters, Upper/Lower Case Letters and numbers ONLY)

[redacted]

Click Button to Generate Client Secret Keyword

Client Secret Keyword (Minimum 10 characters, Upper/Lower Case Letters and numbers ONLY)

[redacted]

Click Button to Generate Mail Secret Keyword

Mail Secret Keyword (Minimum 10 characters, Upper/Lower Case Letters and numbers ONLY)

[redacted]

In the Old Web GUI, navigate to **Content Checks --> Antispam Settings** under the **User Portal Address** field, remove the port number part. For example, if you had the following Secure Portal Address:

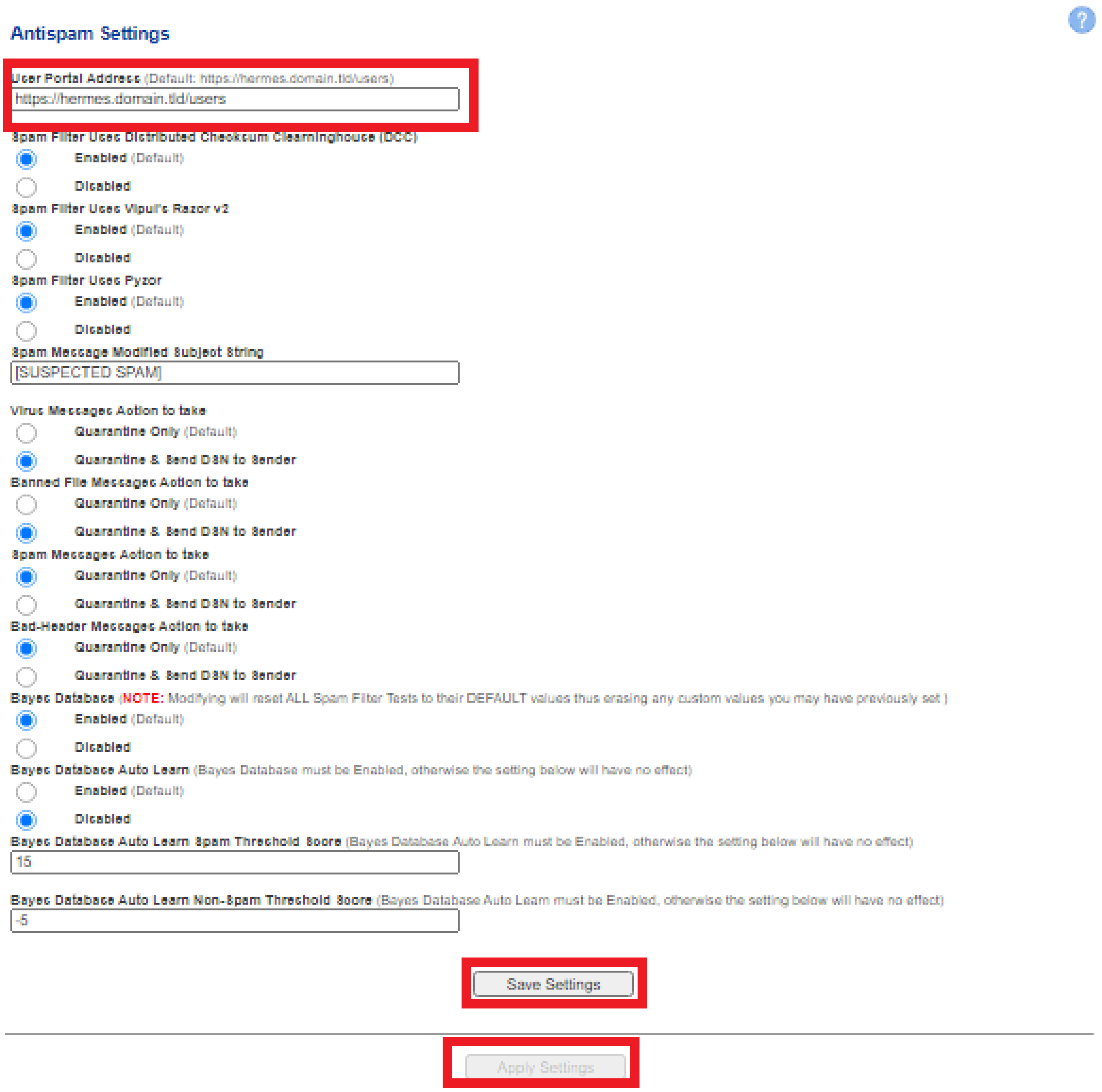
```
https://hermes.domain.tld:9080/users
```

Remove the **:9080** from it so it looks like below:

```
https://hermes.domain.tld/users
```

Click the **Save Settings** button and after settings are saved, click the **Apply Settings** button (**Figure 7**):

Figure 7



Antispam Settings

User Portal Address (Default: https://hermes.domain.tld/users)
https://hermes.domain.tld/users

Spam Filter Uses Distributed Checksum Clearinghouse (DCC)
● Enabled (Default)
○ Disabled

Spam Filter Uses Vipul's Razor v2
● Enabled (Default)
○ Disabled

Spam Filter Uses Pyzor
● Enabled (Default)
○ Disabled

Spam Message Modified Subject String
[SUSPECTED SPAM]

Virus Messages Action to take
○ Quarantine Only (Default)
● Quarantine & Send DSN to Sender

Banned File Messages Action to take
○ Quarantine Only (Default)
● Quarantine & Send DSN to Sender

Spam Messages Action to take
● Quarantine Only (Default)
○ Quarantine & Send DSN to Sender

Bad-Header Messages Action to take
● Quarantine Only (Default)
○ Quarantine & Send DSN to Sender

Bayes Database (NOTE: Modifying will reset ALL Spam Filter Tests to their DEFAULT values thus erasing any custom values you may have previously set)
● Enabled (Default)
○ Disabled

Bayes Database Auto Learn (Bayes Database must be Enabled, otherwise the setting below will have no effect)
○ Enabled (Default)
● Disabled

Bayes Database Auto Learn Spam Threshold Score (Bayes Database Auto Learn must be Enabled, otherwise the setting below will have no effect)
15

Bayes Database Auto Learn Non-Spam Threshold Score (Bayes Database Auto Learn must be Enabled, otherwise the setting below will have no effect)
-5

We highly recommend that you enable 2FA for the admin account by going to **System --> System Users** and setting the **Access Control Policy** to **Two Factor** and enrolling your mobile device.

We highly recommend that you remove the Apache2 package by going to a console prompt and typing the following command:

```
sudo apt remove apache2 && sudo apt autoremove
```

Revision #5
Created 26 November 2021 21:43:59 by Dino Edwards
Updated 4 December 2021 18:20:25 by Dino Edwards