# HERHSIANG

## MDS & MDispersion & HMail

## Series

## Mail Server

## 2023

### DKIM & DMARC verification mechanism setting method

Production of technical documents: HERHSIANG FREEDY

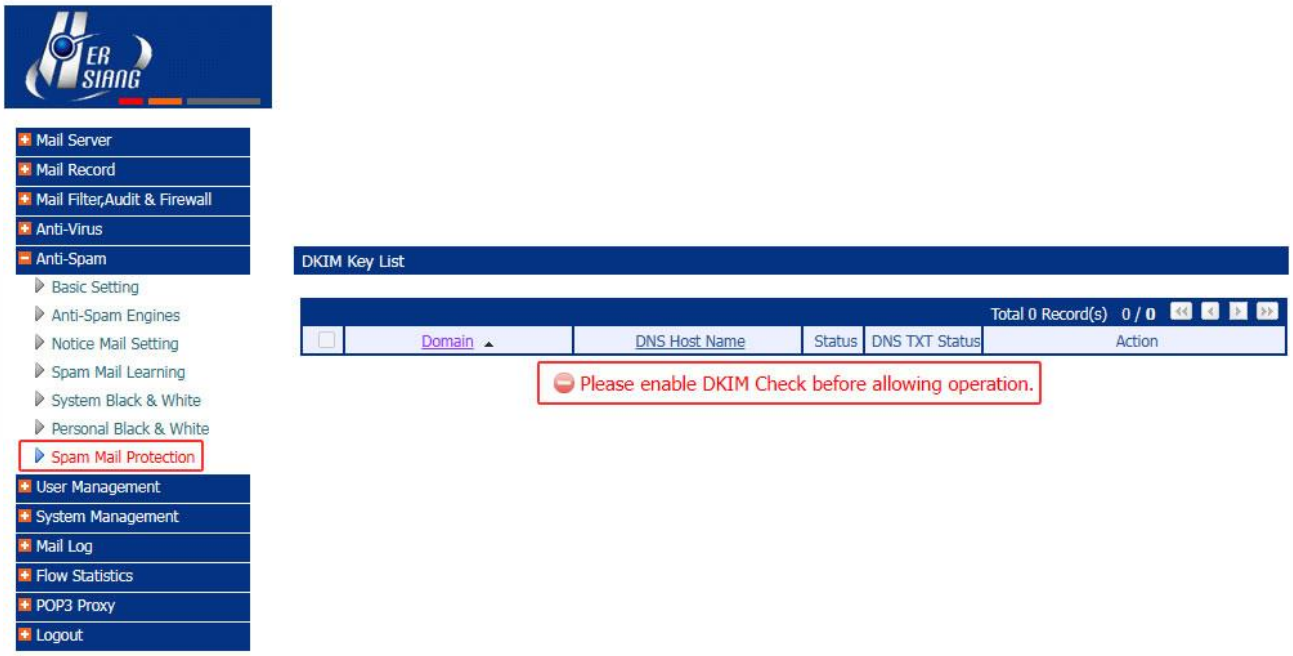
Verification mechanism description:
DKIM (DomainKeys Identified Mail), domain verification mail, used to prevent mail content from being tampered with
It is generated following the built-in function of MArchive mail archiving server, and is set in the management domain DNS SERVER.

DMARC is used to assist SPF and DKIM. Following the DKIM function built into the device, DKIM takes effect and DMARC takes effect automatically.

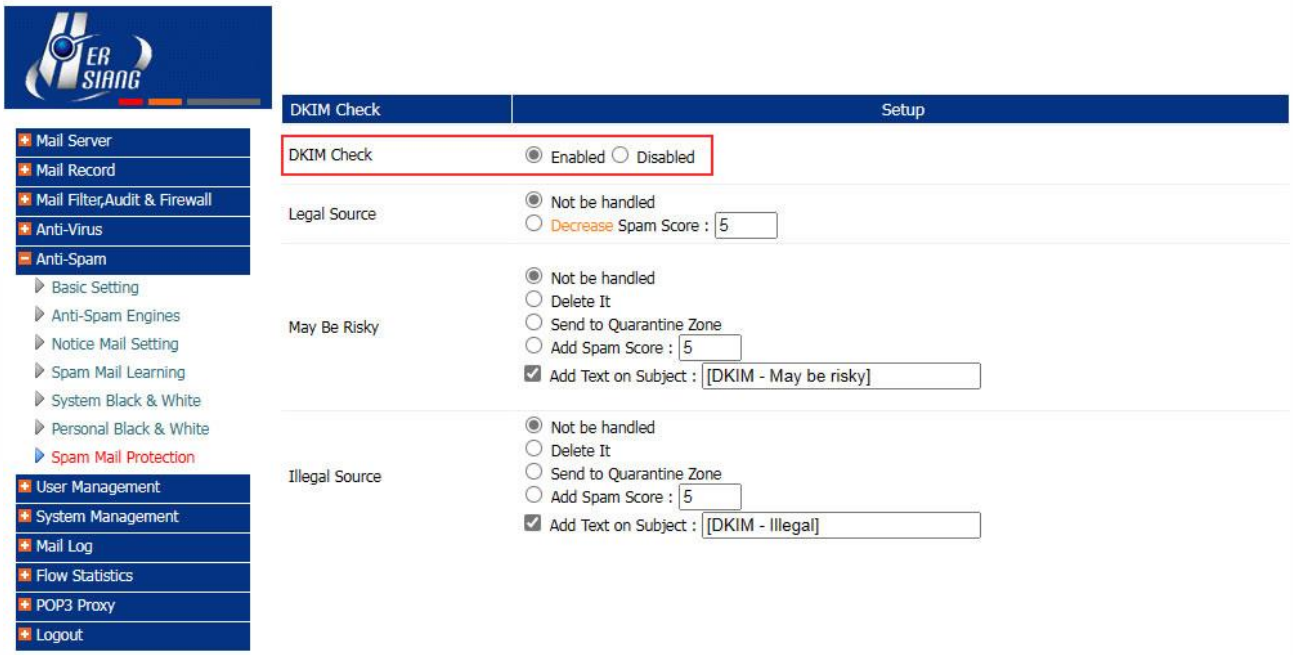
The following input IP&account&password are based on the factory default value and domain input. Take the official website domain herhsiang.com.tw as an example. If the IP&account&password has been modified, please replace it with the modified IP&account&password input

How to configure MDS/MDispersion/HMail mail server to generate DKIM:
1. Enter https://192.168.168.168:88 in the browser to log in to the mail archive management interface, and enter the management account /
   Password: admin / adminpw


1. After entering the screen, select Spam Protection on the left column, move down to the DKIM public and private key, and it will display that you must enable the DKIM verification function before allowing the operation.

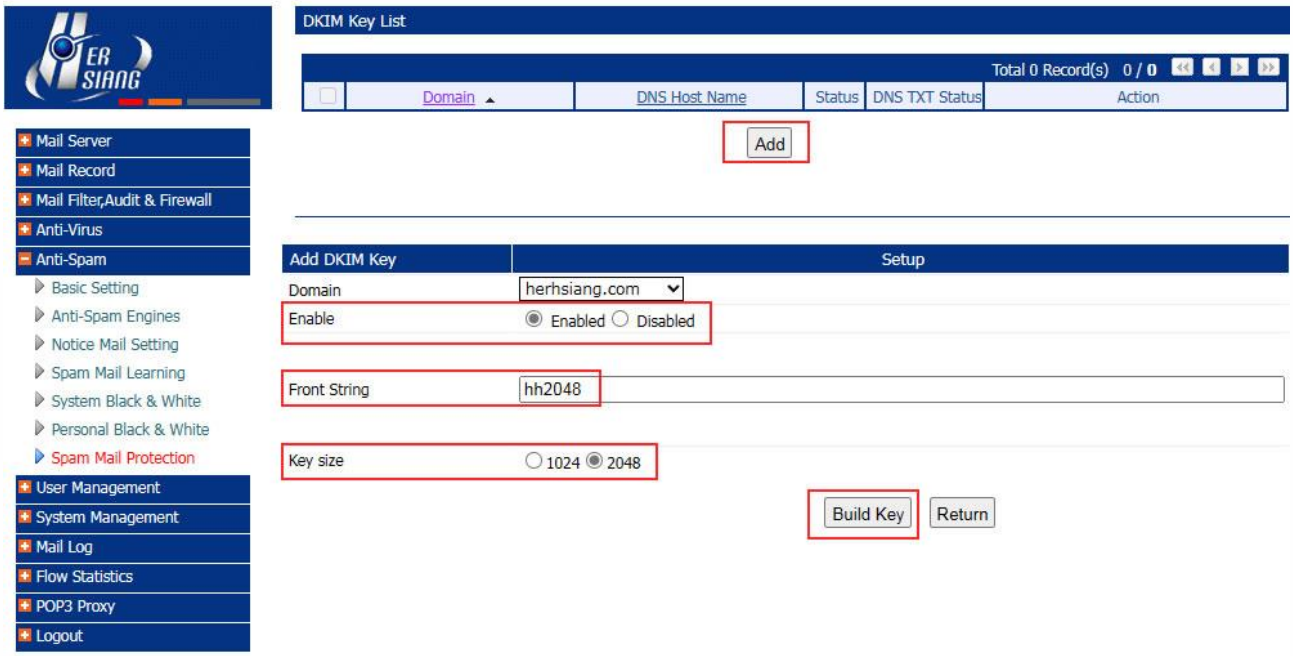



2. Enable DKIM verification function.

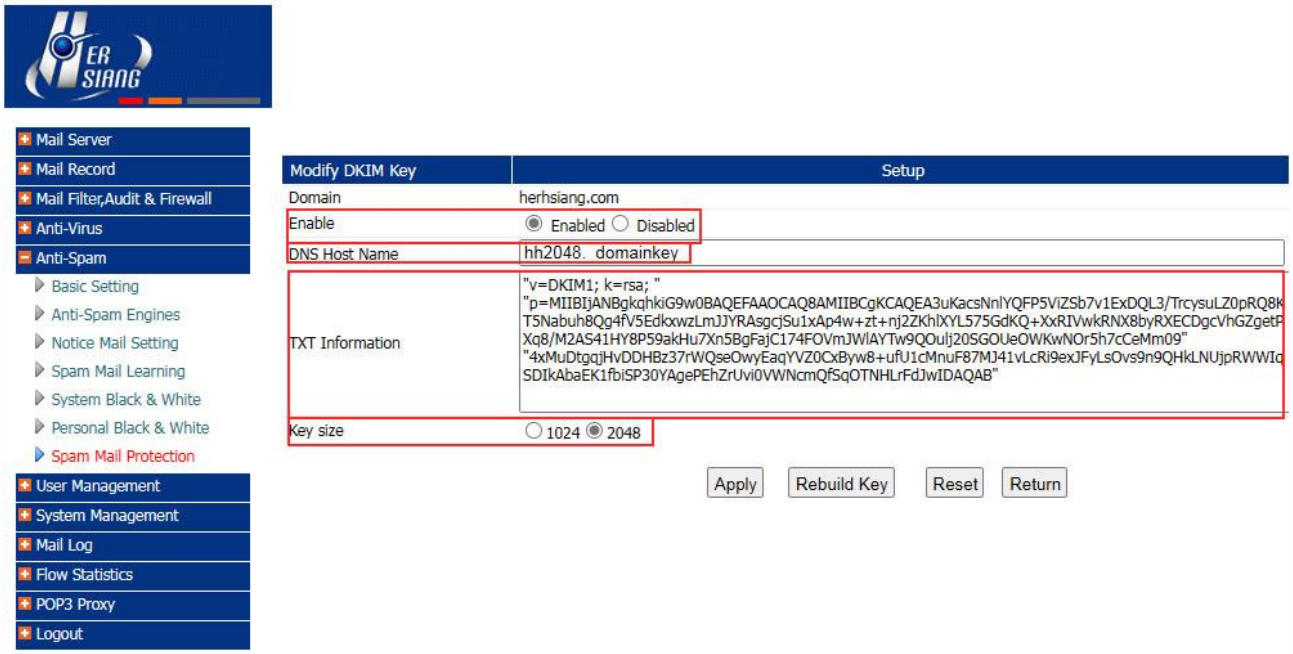



3. Add DKIM public and private options, enter your own domain, please customize the prefix string, please choose the key size, 1024 general DNS Server and hosting are acceptable, 2048 general DNS Server and hosting may not be acceptable or even Additional fees are required, 1024 and 2048 have some escrows that require additional fees, 2048 is relatively safe, and the acceptance of the other party is relatively improved and generates relative own domain

verification data. Add public and private keys->Enable switch and select Enable, press Generate key.



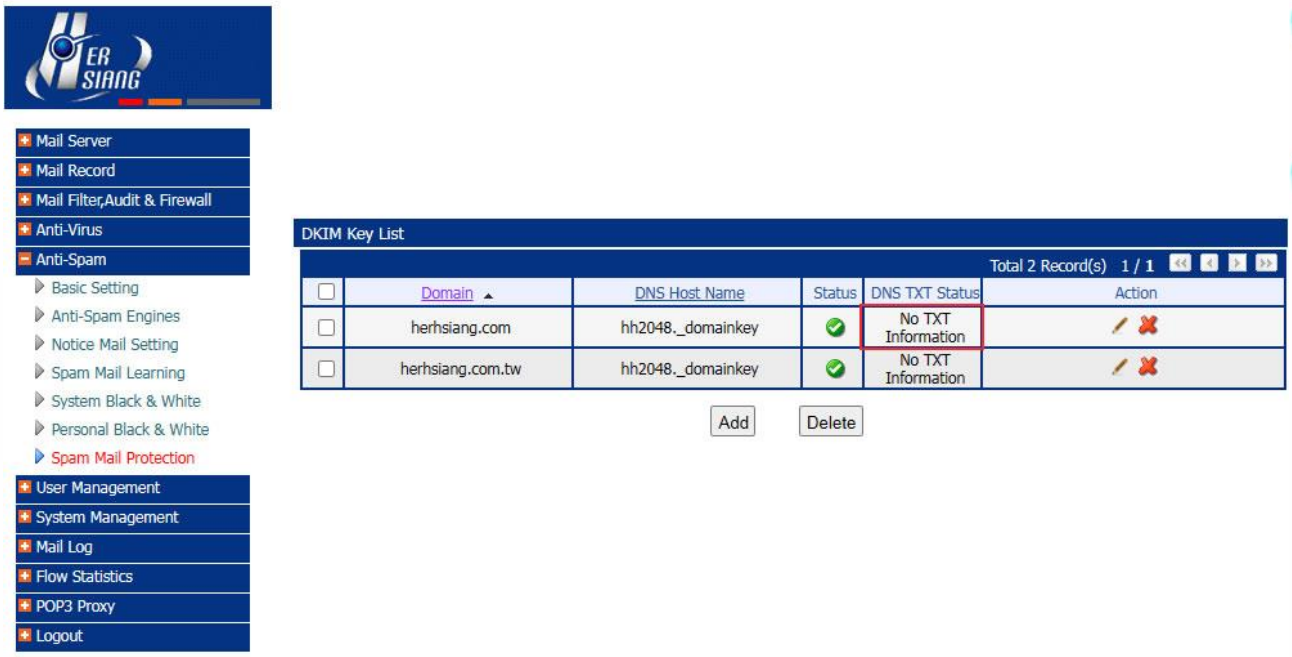

4.Select Enable, copy the corresponding parameters, add the parameters to the self-managed DNS Server or hosted DNS as TXT, copy the DNS host name and TXT data and other parameters to Notepad for backup, press Apply, if you want to restart To generate a new key, please press Regenerate Key.




5. After step 5 is confirmed, a picture will be generated showing that it has been

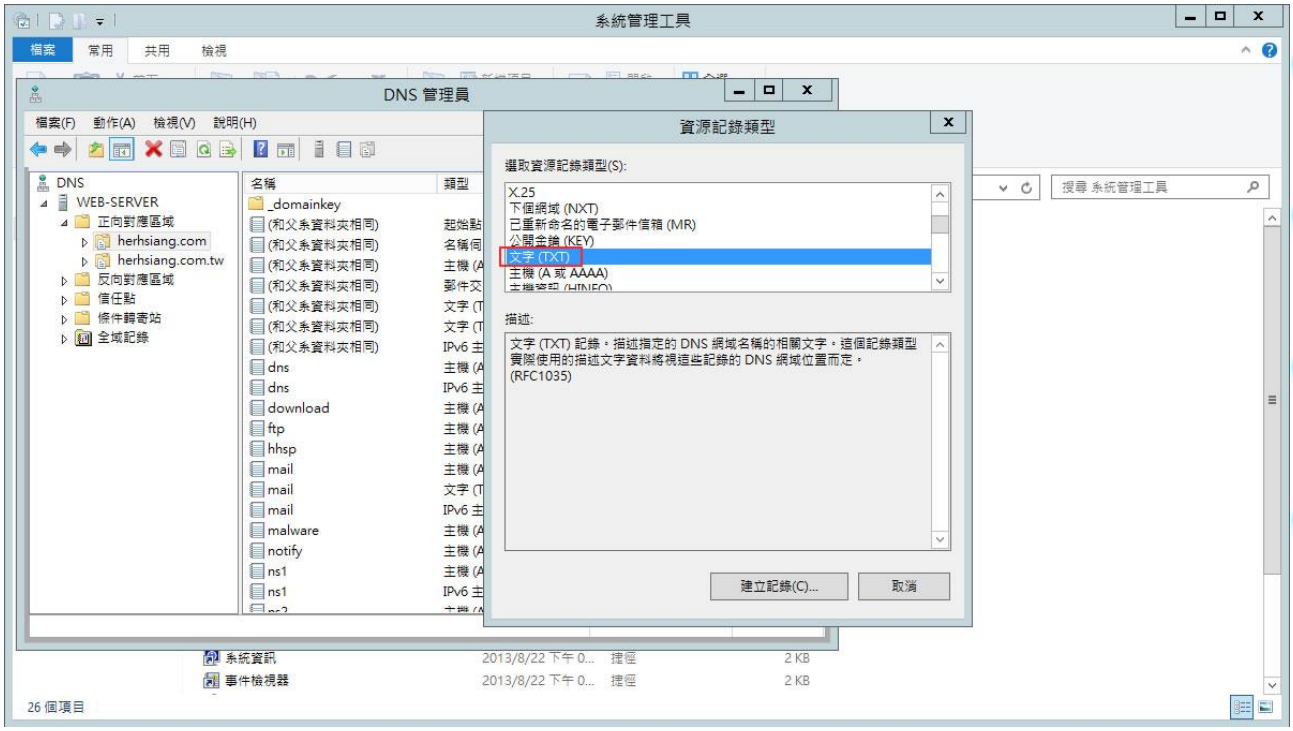
added successfully, but the DKIM key parameter has not been added to DNS Server and hosted DNS, so the device detection shows that there is no TXT data.

P.S. Some DNS servers and hosting do not accept the special characters generated by the key, but it is not necessarily invalid. Please use the Google gmail.com email account to detect. Please search Google for the relevant test method for the detection method, which will not be explained here.

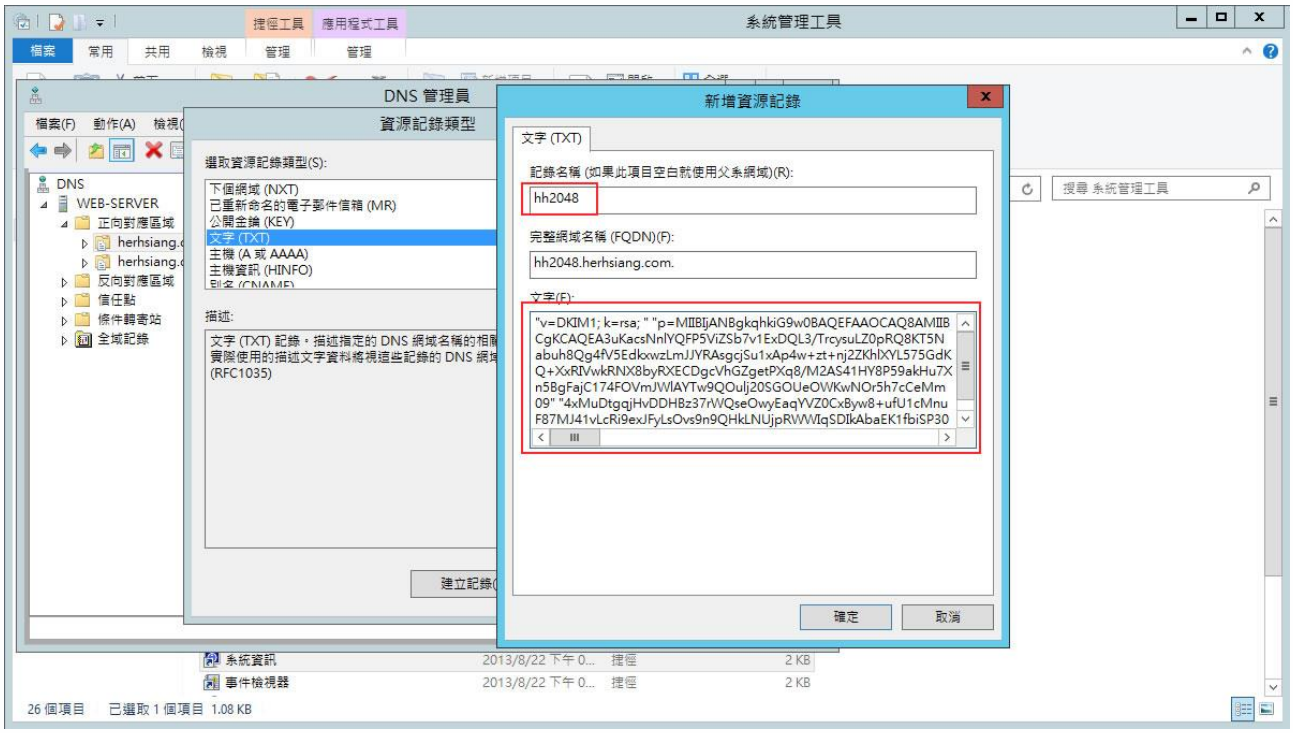



6. Parameter Format Description
   hh2048._domainkey.herhsiang.com (prefix + own domain is the domain set by DKIM in DNS Server or hosted DNS TXT description, not the main domain herhsiang.com)

7. The example is WINDOWS SERVER DNS SERVER, add text TXT, press create record

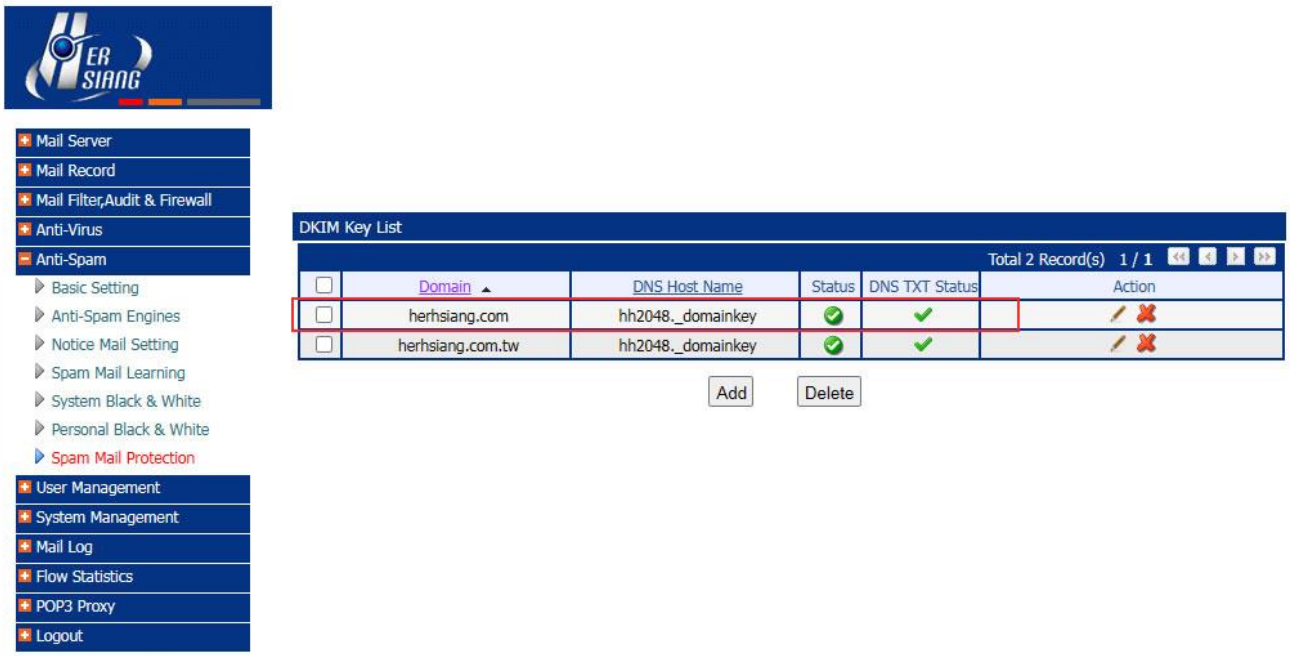



8. Copy the DKIMR key parameters copied to Notepad into the TXT setting field, and press OK to add TXT parameters successfully.




9. After it takes effect, the test again shows that the TXT data is set successfully, which means that the DKIM verification mechanism is set. Please make sure that

the SPF verification mechanism has taken effect. Both SPF and DKIM are valid. The DMARC verification mechanism will also automatically take effect.




10. Start the DKIM verification function, that is, complete the DKIM and DMARC verification mechanism of our domain

- Mail Server
- Mail Record
- Mail Filter,Audit & Firewall
- Anti-Virus
- Anti-Spam
  - Basic Setting
  - Anti-Spam Engines
  - Notice Mail Setting
  - Spam Mail Learning
  - System Black & White
  - Personal Black & White
  - Spam Mail Protection
- User Management
- System Management
- Mail Log
- Flow Statistics
- POP3 Proxy
- Logout

| DKIM Check | Setup |
|---|---|
| DKIM Check | (●) Enabled ( ) Disabled |
| Legal Source | (●) Not be handled<br>( ) Decrease Spam Score : 5 |
| May Be Risky | (●) Not be handled<br>( ) Delete It<br>( ) Send to Quarantine Zone<br>( ) Add Spam Score : 5<br>[✓] Add Text on Subject : [DKIM - May be risky] |
| Illegal Source | (●) Not be handled<br>( ) Delete It<br>( ) Send to Quarantine Zone<br>( ) Add Spam Score : 5<br>[✓] Add Text on Subject : [DKIM - Illegal] |

| DMARC Check | Setup |
|---|---|
| Status | ✔ Running... |
| DMARC Check | (●) Enabled ( ) Disabled |
| Illegal Source | (●) Follow the sending domain owner policy(Rejected/Separate/Not be handled)<br>( ) Not be handled |
| Delivery Failure Report | ( ) Enabled (●) Disabled |
| The Sender Of The Failure Report | root@herhsiang.com.tw |
| The Receivers Of The Failure Report | |
| Send Statistical Report Regularly | ( ) Enabled (●) Disabled |
| Statistical Report Delivery Time | 00:00 |
| The Sender Of The Statistical Report | root@herhsiang.com.tw |
| Statistical Report Test | Test Mail |
| Ignore Domains That Do Not Generate Statistical Reports | |
| Remove Expired Record Time | 3 Day(s) |

Apply Reset