HERHSIANG
MArchive Series Archive Server
2023
DKIM & DMARC verification mechanism setting method

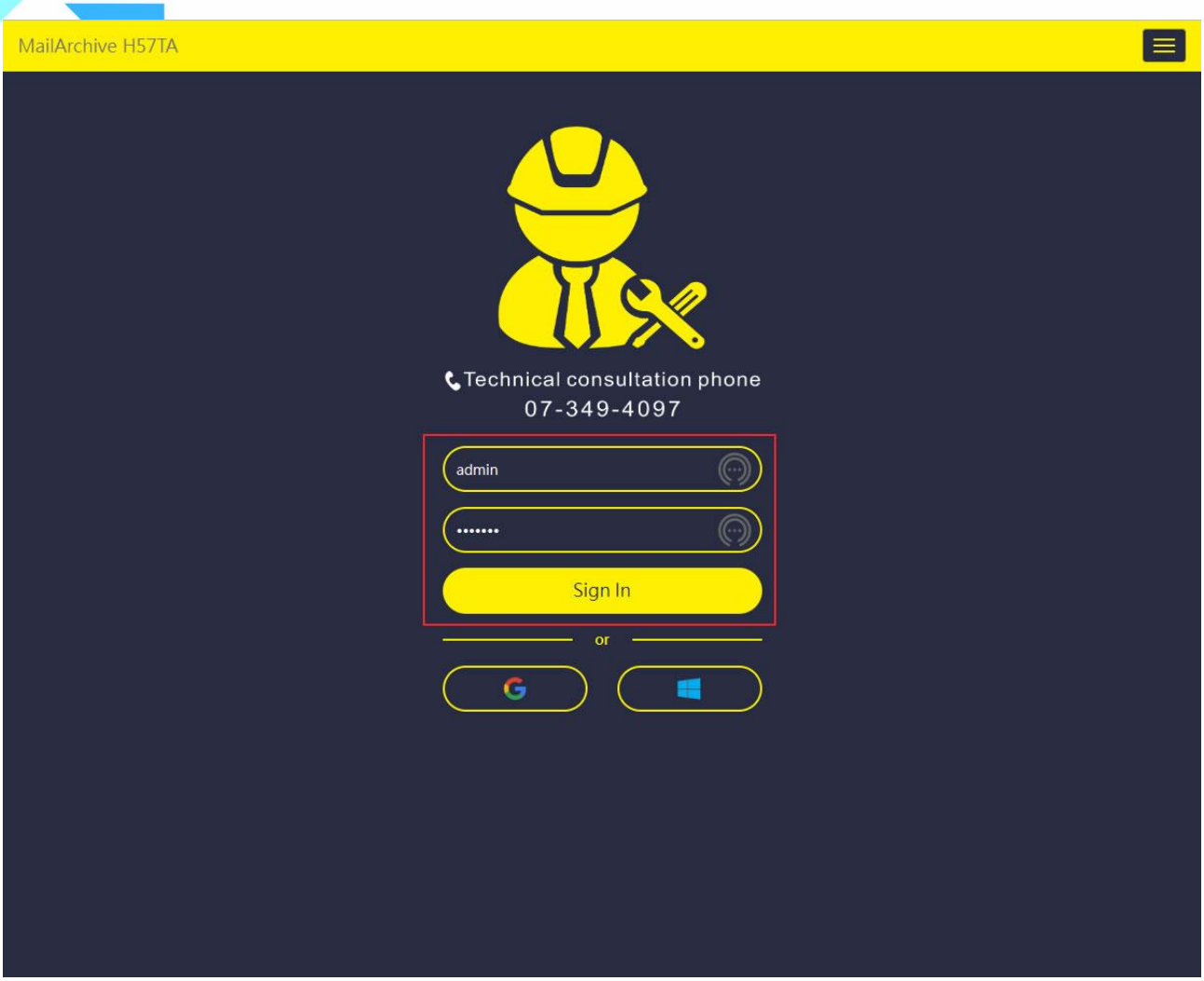
Production of technical documents: HERHSIANG FREEDY

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.

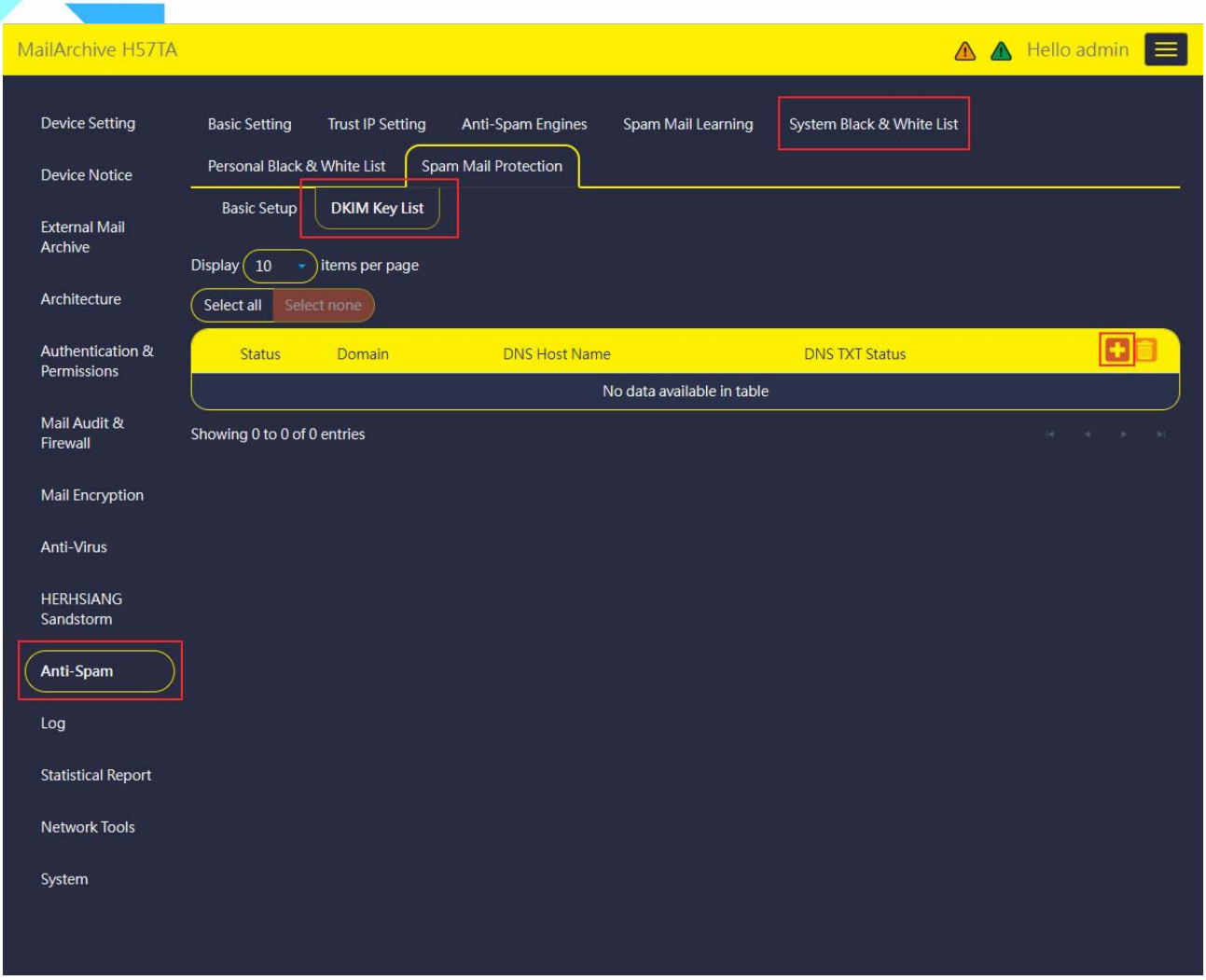
DMARC is used to assist SPF and DKIM. Following the DKIM function built into the device, DKIM takes effect and DMARC takes effect automatically.

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 MArchive archive server is configured to generate DKIM:
1. Enter https://192.168.2.1:88 in the browser to log in to the email archive management interface, and enter the management account / Password: admin / adminpw

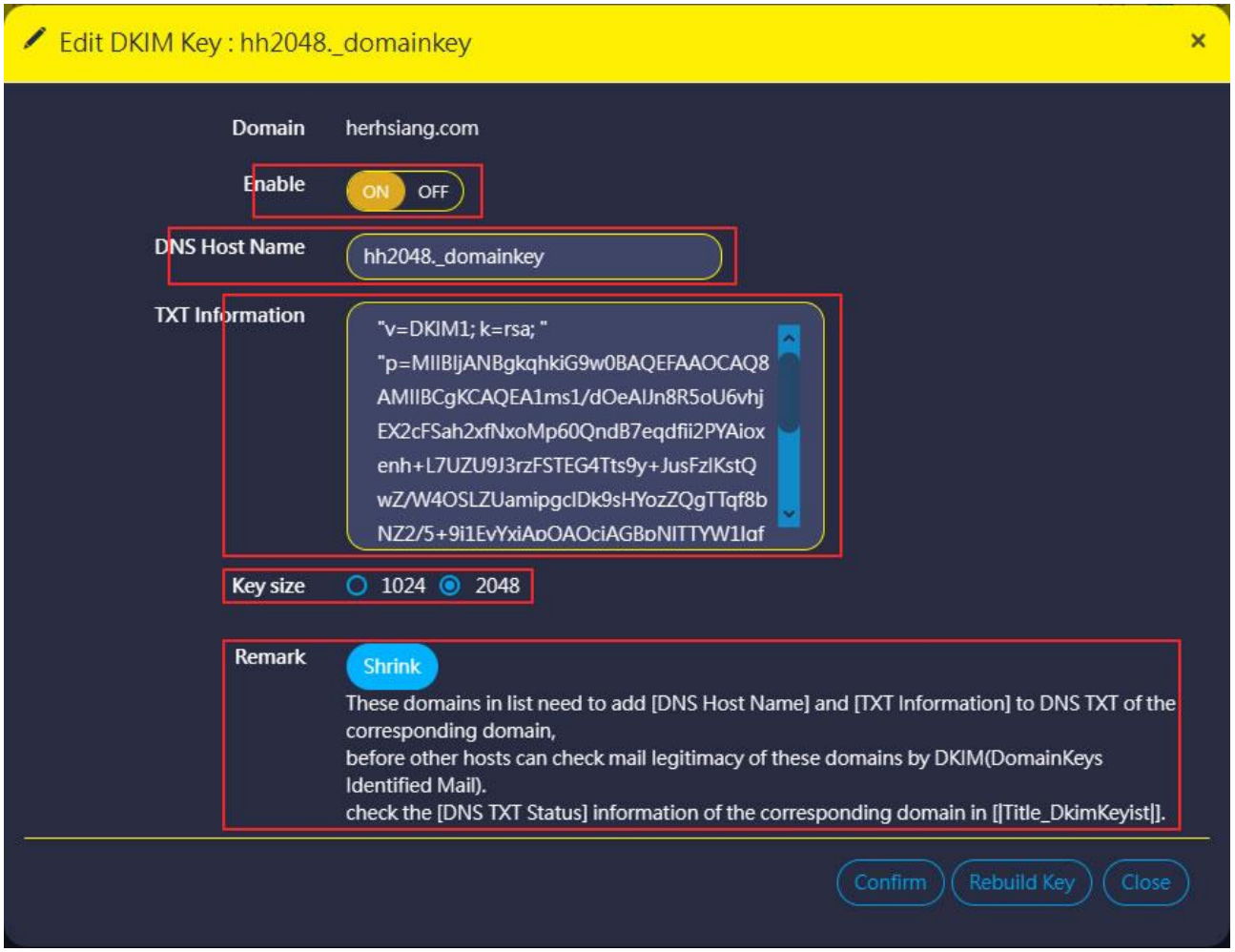


2. After entering the screen, select spam in the left column, select spam protection in the upper column, select DKIM public and private key list, and press the + symbol to add



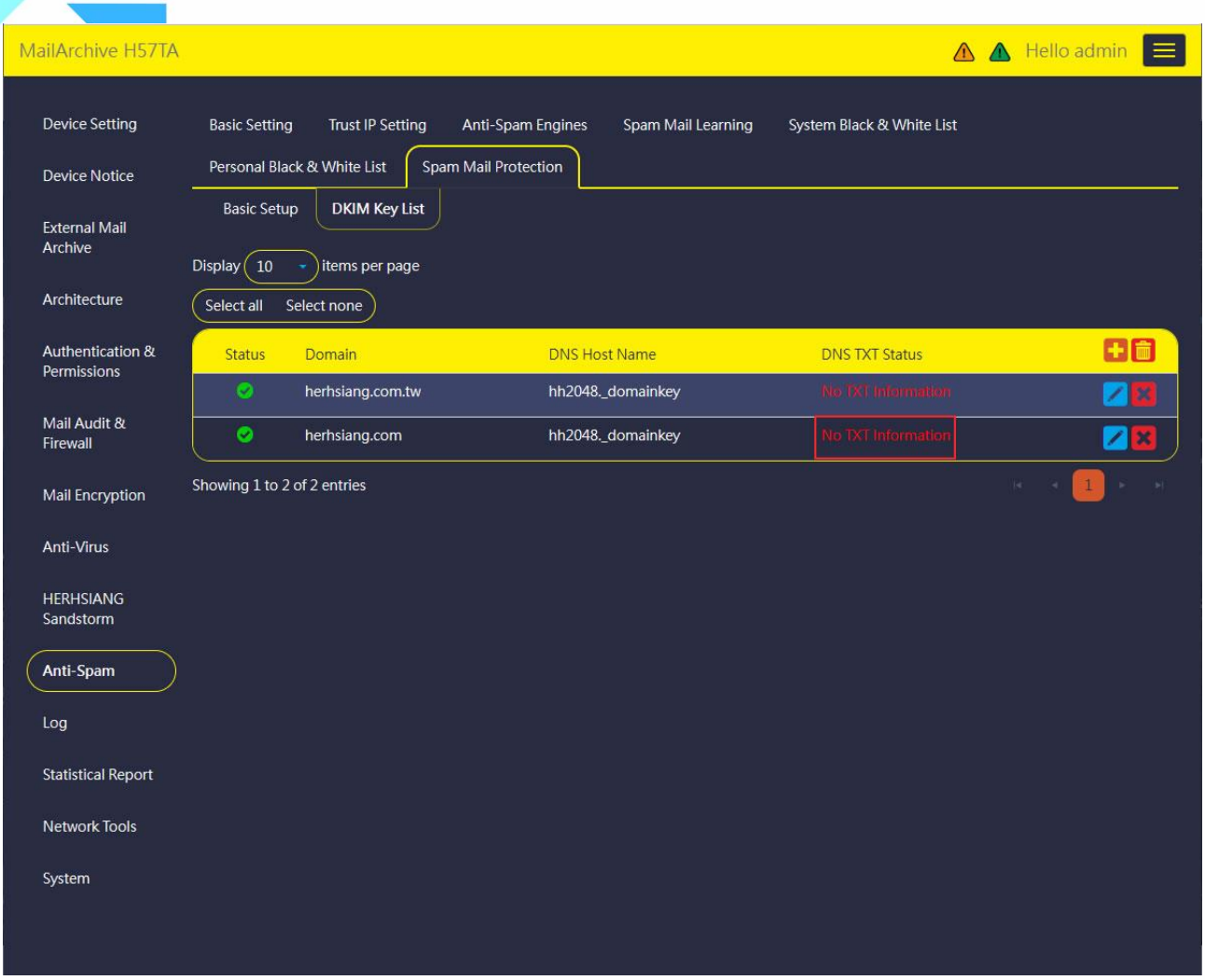
3. Select your own domain, please customize the prefix string, and select the key size, 1024 is acceptable to general DNS servers and hosting, 2048 is not necessarily acceptable to general DNS servers and hosting or even requires additional fees, 1024 and 2048 Some hosting needs to be paid additionally, 2048 is relatively safe and the acceptance rate of the other party is relatively increased, according to the new addition and the verification data generated relative to its own domain.

4. Select enable, first click on the description, the description says to copy the corresponding parameters, add the parameters to the self-managed DNS Server or managed DNS as TXT, copy the parameters such as the DNS host name and TXT data to Notepad for later use , press OK, if you want to regenerate a new key, please press Regenerate Key.



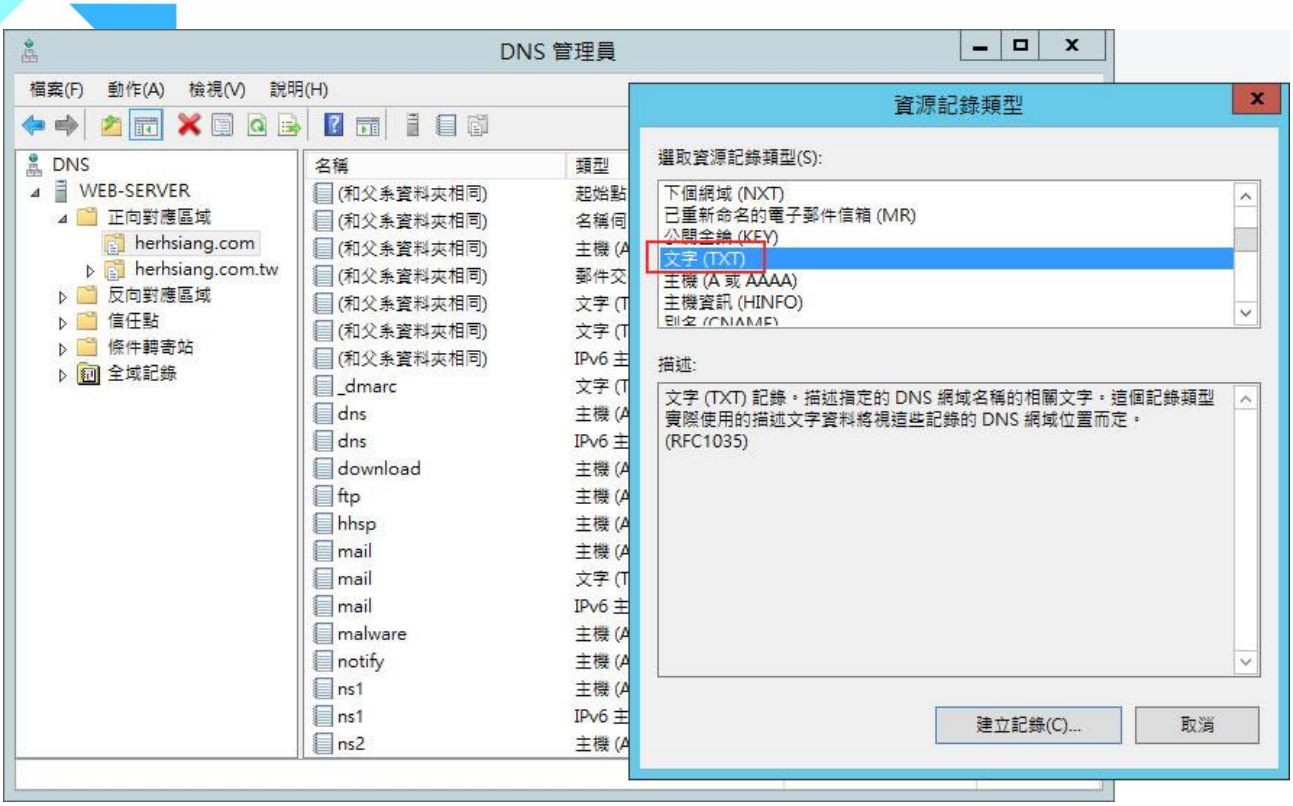
5. After step 4 is confirmed, a picture will appear showing that it has been added successfully, but the DKIM key parameter has not been added to DNS Server and hosted DNS, so the device detection shows that there is no TXT data.

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.

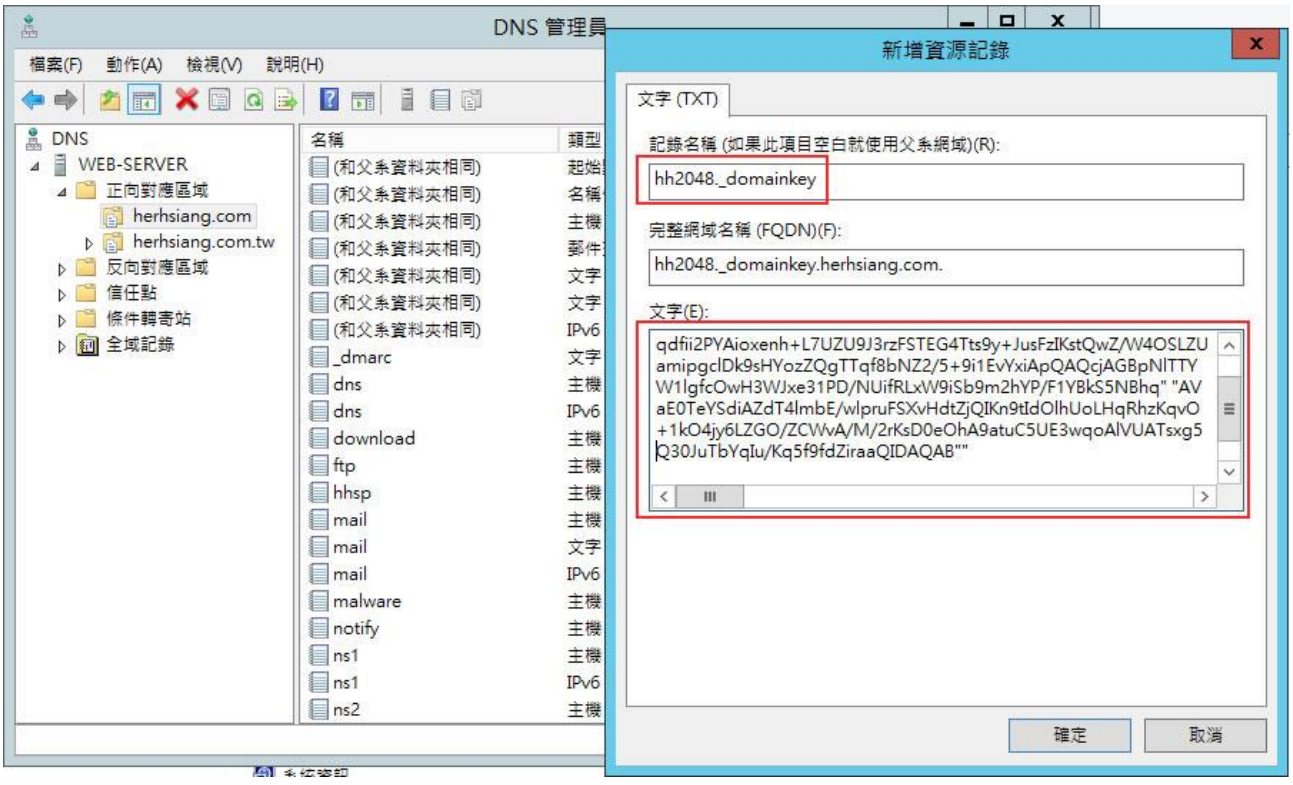


6. Parameter Format Description
   hh2048._domainkey.herhsiang.com (prefix + own domain is the domain set by DKIM in DNS Server or hosted DNS TXT description, not the main domain herhsiang.com)

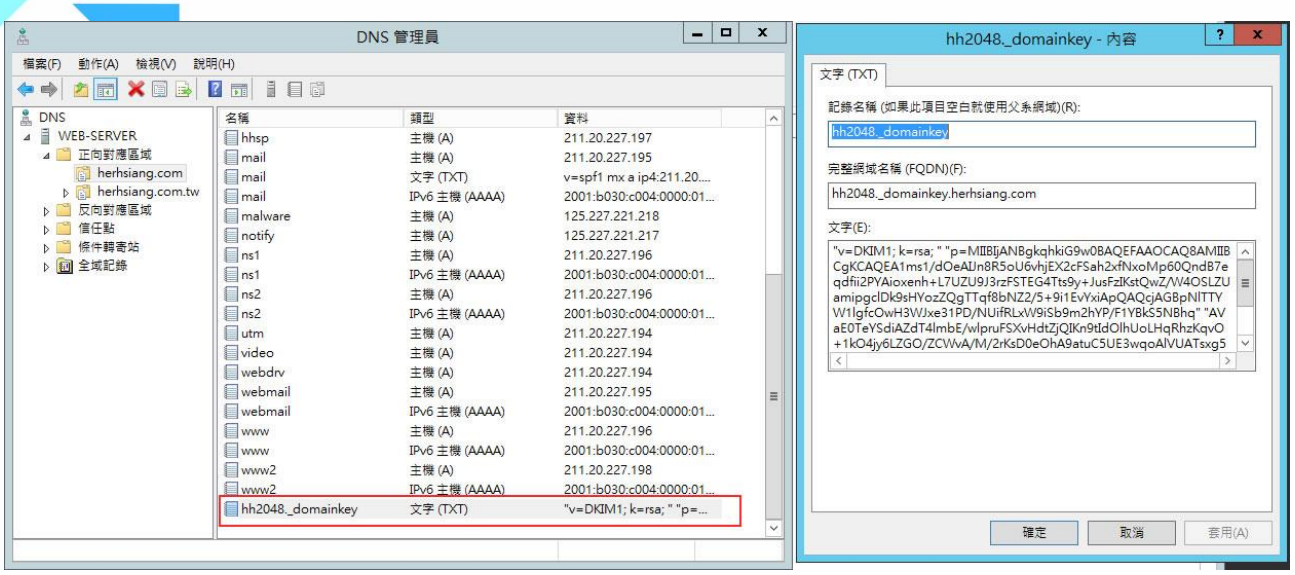
7. The example is WINDOWS SERVER DNS SERVER, add text TXT, press create record



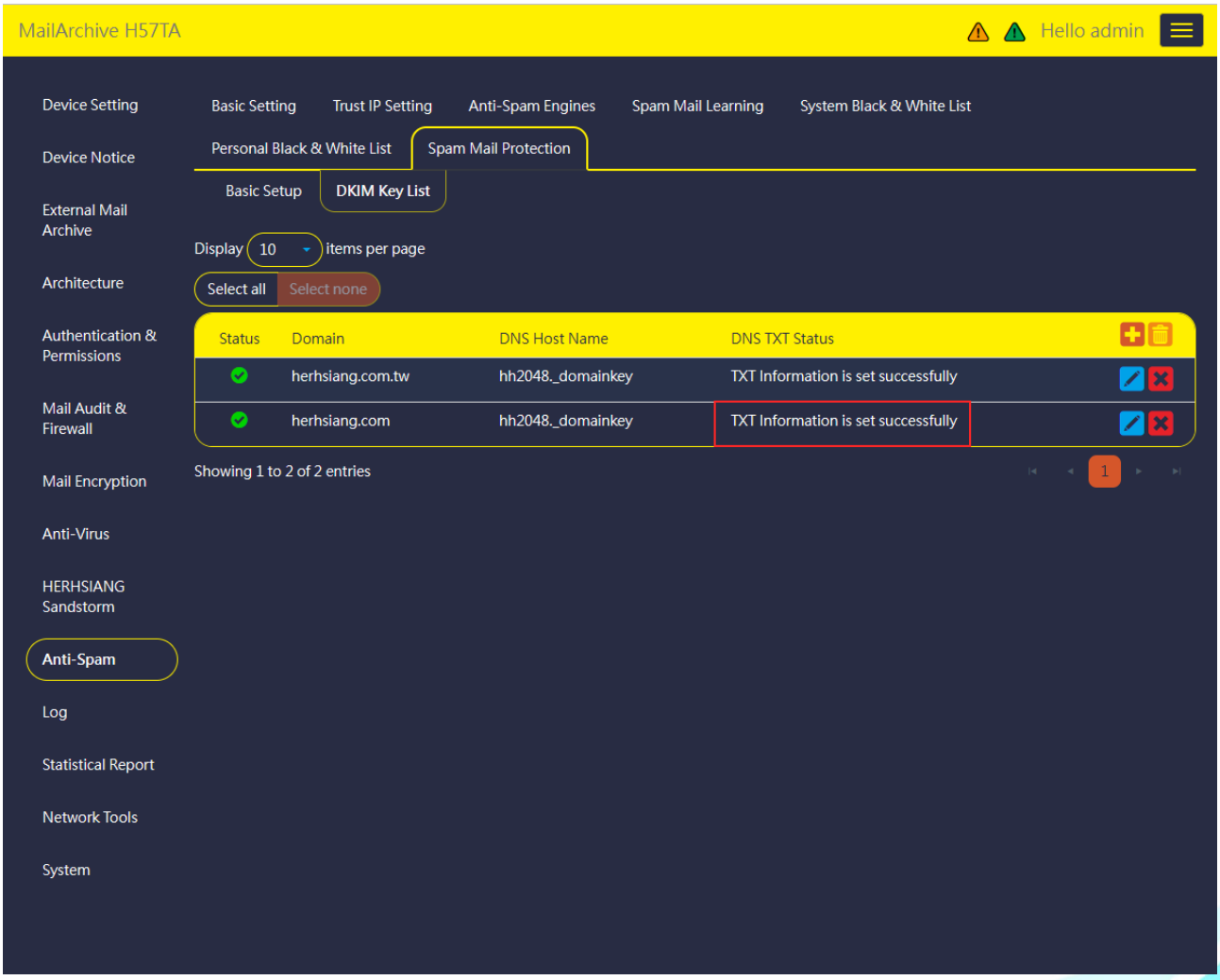
8. Copy the DKIMR key parameters copied to Notepad into the TXT setting field, and press OK to add TXT parameters successfully.



9. Check the configuration data again



10. After the belt takes effect, the test again shows that the TXT data setting is successful, that is, 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.



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