

HERHSIANG

MDS & MDispersion & HMail

Series

Mail Server

2023

DKIM & DMARC verification mechanism setting method





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



System administrator login

帳號 :	<input type="text" value="admin"/>	
密碼 :	<input type="password" value="*****"/>	
		<input type="button" value="登入"/>

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.



- ✦ 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 Key List

	Domain	DNS Host Name	Status	DNS TXT Status	Action
Total 0 Record(s) 0 / 0					

Please enable DKIM Check before allowing operation.

2. Enable DKIM verification function.



- ✦ 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	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Legal Source	<input checked="" type="radio"/> Not be handled <input type="radio"/> Decrease Spam Score : <input type="text" value="5"/>
May Be Risky	<input checked="" type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input type="radio"/> Add Spam Score : <input type="text" value="5"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - May be risky]"/>
Illegal Source	<input checked="" type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input type="radio"/> Add Spam Score : <input type="text" value="5"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - Illegal]"/>

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.

The screenshot shows the 'DKIM Key List' interface. At the top, there is a table with columns: Domain, DNS Host Name, Status, DNS TXT Status, and Action. Below the table is an 'Add' button. The main section is titled 'Add DKIM Key' and 'Setup'. It contains the following fields:

- Domain: herhsiang.com
- Enable: Enabled Disabled
- Front String: hh2048
- Key size: 1024 2048

At the bottom right, there are 'Build Key' and 'Return' buttons.

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.

The screenshot shows the 'Modify DKIM Key' interface. It contains the following fields:

- Domain: herhsiang.com
- Enable: Enabled Disabled
- DNS Host Name: hh2048.domainkey
- TXT Information: "v=DKIM1; k=rsa; "p=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs3uKacsNnlYQFP5vIZSb7v1ExDQL3/TrcysuLZ0pRQ8K T5Nabuh8Qg4fV5EdkxwzLmJJYRAsgcjSu1xAp4w+zt+nj2ZKhIXYL575GdKQ+XxRIVwkRNx8byRXECDgcvhGZgetP Xq8/M2AS41HY8P59akHu7Xn5BgFajC174FOvmJWIAyTw9QQulj20SGOUeOWKwNOR5h7cCeMm09" "4xMuDtgajHvDDHBz37rWQseOwyEaqYVZ0CxByw8+ufU1cMnuF87MJ41vLcRi9exJfYsOvs9n9QHkLNUjprWWIc SDIkAbaEK1fbiSP30YAgePEhZrUvi0VWNcmQfSQTNHLrFdJwIDAQAB"
- Key size: 1024 2048

At the bottom, there are 'Apply', 'Rebuild Key', 'Reset', and 'Return' buttons.

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.



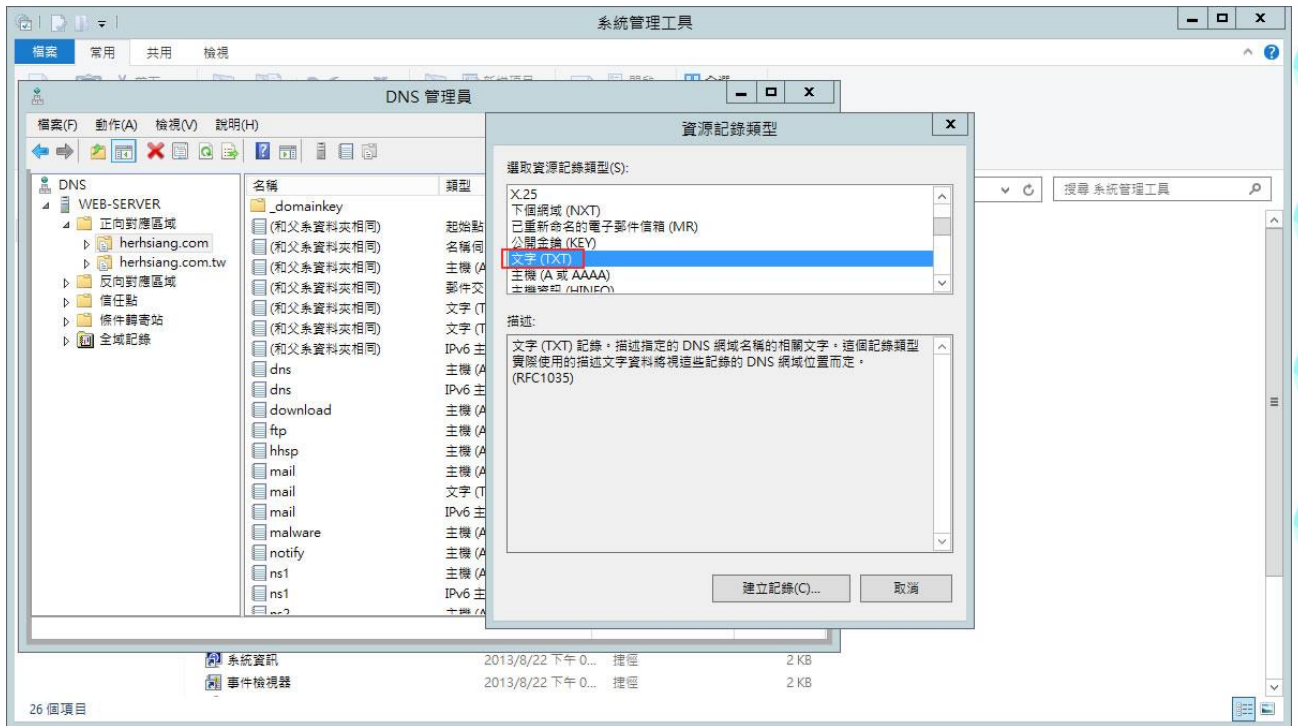
- Mail Server
- Mail Record
- Mail Filter,Audit & Firewall
- Anti-Virus
- Anti-Spam
 - Basic Setting
 - Anti-Spam Engines
 - Notice Mail Setting
 - Spam Mail Learning
 - System Black & White
 - Personal Black & White
 - Spam Mail Protection
- User Management
- System Management
- Mail Log
- Flow Statistics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

DKIM Key List					
Total 2 Record(s) 1 / 1					
<input type="checkbox"/>	Domain ▲	DNS Host Name	Status	DNS TXT Status	Action
<input type="checkbox"/>	herhsiang.com	hh2048._domainkey	✓	No TXT Information	
<input type="checkbox"/>	herhsiang.com.tw	hh2048._domainkey	✓	No TXT Information	

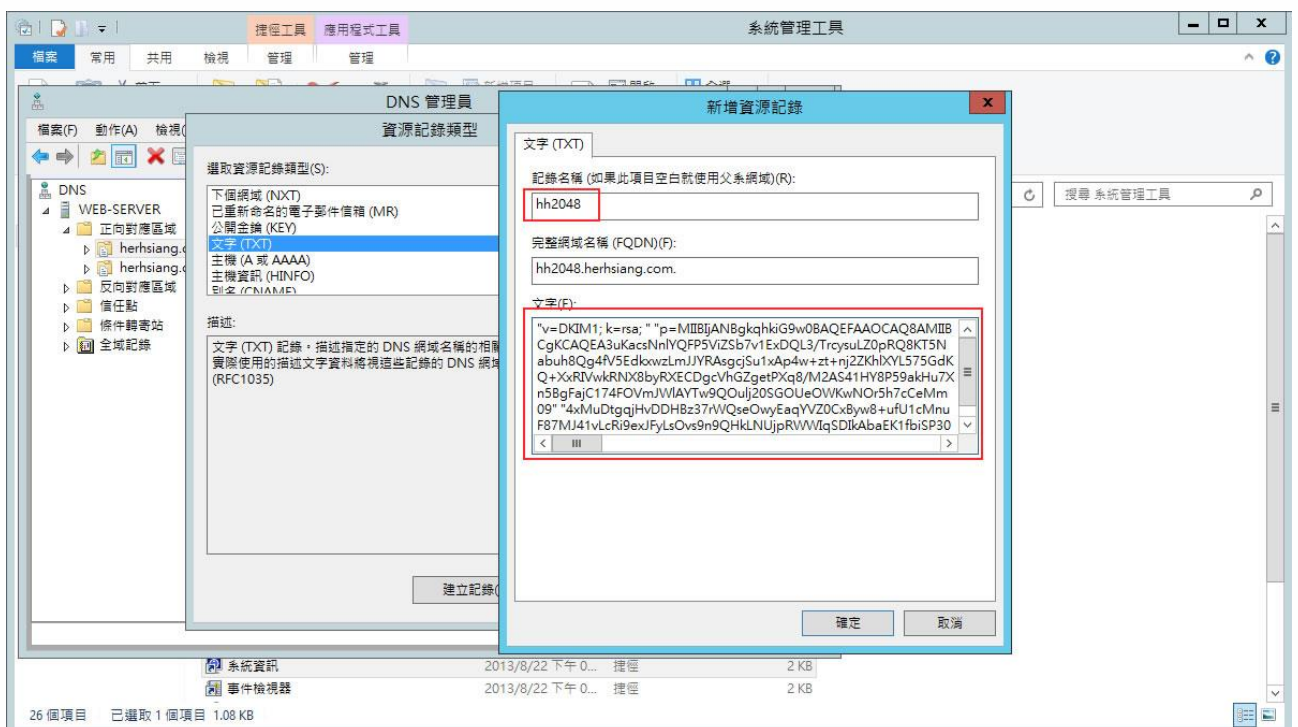
6. Parameter Format Description

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



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



- 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.



- ✦ 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 Key List Total 2 Record(s) 1 / 1

<input type="checkbox"/>	Domain ▲	DNS Host Name	Status	DNS TXT Status	Action
<input type="checkbox"/>	herhsiang.com	hh2048_domainkey	✔	✔	✂ ✖
<input type="checkbox"/>	herhsiang.com.tw	hh2048_domainkey	✔	✔	✂ ✖

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



DKIM Check	Setup
DKIM Check	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Legal Source	<input checked="" type="radio"/> Not be handled <input type="radio"/> Decrease Spam Score : <input type="text" value="5"/>
May Be Risky	<input checked="" type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input type="radio"/> Add Spam Score : <input type="text" value="5"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - May be risky]"/>
Illegal Source	<input checked="" type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input type="radio"/> Add Spam Score : <input type="text" value="5"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - Illegal]"/>



- ✦ 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

DMARC Check	Setup
Status	✔ Running...
DMARC Check	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Illegal Source	<input checked="" type="radio"/> Follow the sending domain owner policy(Rejected/Separate/Not be handled) <input type="radio"/> Not be handled
Delivery Failure Report	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
The Sender Of The Failure Report	<input type="text" value="root@herhsiang.com.tw"/>
The Receivers Of The Failure Report	<input type="text"/>
Send Statistical Report Regularly	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Statistical Report Delivery Time	<input type="text" value="00:00"/>
The Sender Of The Statistical Report	<input type="text" value="root@herhsiang.com.tw"/>
Statistical Report Test	<input type="text" value="Test Mail"/>
Ignore Domains That Do Not Generate Statistical Reports	<input type="text"/>
Remove Expired Record Time	<input type="text" value="3"/> Day(s)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	