



# Mail Server Solution

Website  
www.sharetech.com.tw/en-us

Sales Info  
sales@sharetech.com.tw

Tech Support  
help@sharetech.com.tw



## Stop Spam & Email Fraud

### — Protect with ShareTech

Email is the main business tool and the biggest attack target. Spam, phishing, and spoofed emails hurt efficiency and cause losses.

The solution is SPF, DKIM, & DMARC.

#### SPF: Sender Authentication – Stop Forged “Senders”

An SPF record is set in the sender domain’s DNS to list which mail server IPs are authorized to send on behalf of that domain.

When mail arrives, the receiving server checks whether the sender’s IP is in the list.

Like a “gatekeeper,” SPF ensures the email comes through the right door, reducing spam and forged sender addresses.

SPF Check	Setup
SPF 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"/>
Risky Source	<input type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input checked="" type="radio"/> Add Spam Score : <input type="text" value="3"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[Sender may be risky]"/>
Illegal Source	<input type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input checked="" type="radio"/> Add Spam Score : <input type="text" value="3"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[Sender is illegal]"/>
Invalid SPF Record	<input type="radio"/> Not be handled <input checked="" type="radio"/> Add Spam Score : <input type="text" value="3"/>

SPF Check: When the mail server receives an external sending request, SPF checks whether the sender's source is authorized, then processes it according to the policy.

Invalid SPF Record: SPF result is none or permerror, which means the record cannot be evaluated – most often because the sender has not set up SPF.

Illegal Source: SPF result is fail.

Risky Source: SPF result is softfail.

Legal Source: SPF result is pass or neutral.

## DKIM: Message Integrity – Prevent Tampering

The sending server adds a digital signature to the email, generated using a private key.

The receiving server retrieves the public key from the sender's DNS, decrypts the signature, and checks if the content was modified.

Like a "wax seal" on a letter, DKIM ensures no one tampers with the message in transit.

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 type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input checked="" type="radio"/> Add Spam Score : <input type="text" value="3"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - May be risky]"/>
Illegal Source	<input type="radio"/> Not be handled <input type="radio"/> Delete It <input type="radio"/> Send to Quarantine Zone <input checked="" type="radio"/> Add Spam Score : <input type="text" value="3"/> <input checked="" type="checkbox"/> Add Text on Subject : <input type="text" value="[DKIM - Illegal]"/>

DKIM Check: When enabled, the system uses the DKIM protocol to validate emails.

If the sender's domain is in the DKIM key list and has a DNS TXT record, the message is signed with the domain's private key. The signature is added to the header, allowing other servers to retrieve the public key from DNS and verify the email's authenticity.

DKIM Key List					
Total 9 Record(s) 1 / 1					
<input type="checkbox"/>	Domain	DNS Host Name	Status	DNS TXT Status	Action
<input type="checkbox"/>	ben.com	dk1._domainkey			
<input type="checkbox"/>	freeip.cf	s1.2022._domainkey		No TXT Information	
<input type="checkbox"/>	freeip.cf	s1._domainkey			
<input type="checkbox"/>	homesrv.work	186.74.sharetech._domainkey			

Legal Source: DKIM result is pass.

May Be Risky: DKIM result is neutral or permerror.

Illegal Source: DKIM result is fail.

## DMARC: Policy Enforcement – Decide How to Handle Suspicious Mail

DMARC builds on SPF and DKIM, defining policies in DNS to tell receiving servers what to do if validation fails.

- **none**: Take no action, only log
- **quarantine**: Place in quarantine
- **reject**: Block delivery
- **rua**: Statistical report recipient
- **ruf**: Failure report recipient

DMARC can also send reports back to the sender, allowing businesses to see if anyone is spoofing their domain.

DMARC acts as the “referee” – deciding whether an email gets delivered, quarantined, or rejected.

DMARC Check	Setup
Status	✔ Running...
DMARC Check	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Illegal Source	<input type="radio"/> Follow the sending domain owner policy(Rejected/Separate/Not be handled) <input checked="" 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@freeip.cf"/>
The Receivers Of The Failure Report	<input type="text" value="allen6@freeip.cf (allen6)"/> <input type="text" value="x01@freeip.cf (x01)"/>
Send Statistical Report Regularly	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Statistical Report Delivery Time	<input type="text" value="16:00"/>
The Sender Of The Statistical Report	<input type="text" value="root@freeip.cf"/>
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)

DMARC Check: When enabled, the system detects spoofing to avoid phishing or spam.

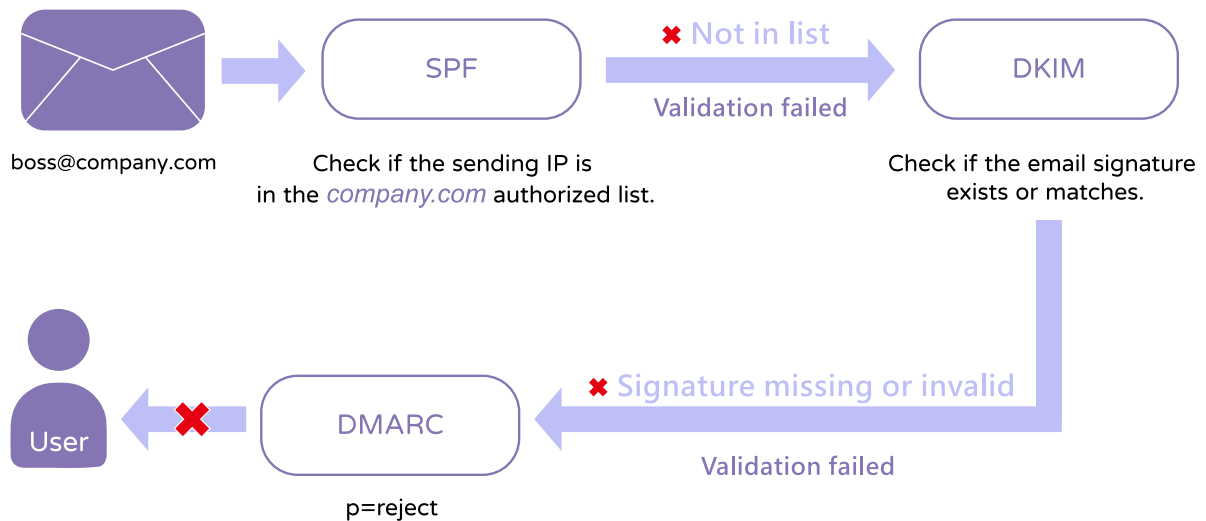
It requires SPF or DKIM to be enabled first.

Illegal Source: If DMARC fails, the action follows the sender's DMARC policy. If no DMARC record exists, no action is taken.

Example:

v=DMARC1; p=reject; rua=mailto:dmarc\_report@domain.com; ruf=mailto:dmarc\_report@domain.com;

**Example: Suppose an email claims to be from *boss@company.com*, asking the finance department to transfer funds.**



**ShareTech Mail Server includes SPF, DKIM, and DMARC plus antivirus, anti-spam, auditing, and encryption – ensuring your email system is:**

- Cleaner (fewer spam emails)
- Safer (blocks spoofing & phishing)
- More trustworthy (better deliverability & brand reputation)

A single investment, lifetime updates, total email protection.

 Contact us at [sales@sharetech.com.tw](mailto:sales@sharetech.com.tw)