



# Mail Server Solution

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

✉ Sales Info  
sales@sharetech.com.tw

✉ Tech Support  
help@sharetech.com.tw



## [Zero Trust x Identity Authentication]

### OTP and Biometrics in Action

As cyber threats grow more complex, traditional username-password logins are no longer enough to protect corporate email. ShareTech integrates two-factor authentication to help enterprises implement Zero Trust security in email systems—and further eliminates the default administrator account (“admin”) login—ensuring that only verified users gain access.

#### The Problem: When passwords fail, trust breaks.

Email is the core of business communication—and a favorite target for attackers. From weak passwords to phishing, compromised accounts can lead to data breaches, financial losses, and reputational harm. To mitigate these risks, companies need more than training—they need [strong identity authentication](#) and [Zero Trust access controls](#).

#### The Solution: Two-Factor Authentication to Enforce Zero Trust

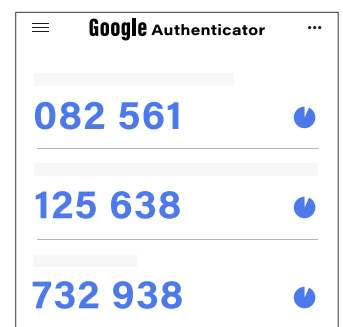
ShareTech enhances email security with Two-Factor Authentication (2FA), adding an extra layer of identity authentication to reduce account hijacking risks.

##### • Google Authenticator – OTP Verification

In the age of AI and advanced attacks, relying on usernames and passwords alone is dangerously insufficient. To counter this, ShareTech integrates Google Authenticator as a One-Time Password (OTP) verification tool for both end users and administrators.

Whether accessing [Webmail or the admin interface](#), users can enable 2FA to receive a real-time, six-digit OTP from the Google Authenticator app. Users simply scan a QR code to bind their account, allowing them to receive a one-time code for future logins.

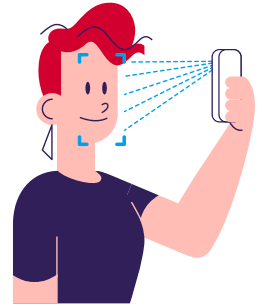
This approach helps prevent brute-force attacks, phishing, or internal privilege misuse. Admins can enforce OTP use to ensure that all email accounts comply with secure identity controls.



### • ShareTech Authenticator – Biometric Authentication

To further enhance both [security and user experience](#), ShareTech offers its own biometric login mechanism for email access. Users can opt to log in using [fingerprint or facial recognition](#), minimizing the risks of password leakage or impersonation.

Once a device is paired with ShareTech Authenticator, users only need to enter their username—no password required—to log in quickly and securely with biometric authentication. It's especially suitable for high-risk roles such as executives, finance, or legal personnels and can be rolled out organization-wide for seamless mailbox protection.



ShareTech also plans to expand biometric authentication to [the admin interface](#), advancing Zero Trust enforcement throughout the email environment.

### Conclusion: From Passwords to Identity Trust

Zero Trust is a strategic mindset—not just a technology. In email systems, it starts with verifying every login instead of assuming trust. With Google Authenticator OTP and ShareTech's biometric login, [and the removal of easily targeted default admin account](#), organizations can boost email security while simplifying identity authentication.

ShareTech is committed to helping organizations build a more trusted and secure email future. Contact us to learn more:

✉ [sales@sharetech.com.tw](mailto:sales@sharetech.com.tw)

🌐 [www.sharetech.com.tw](http://www.sharetech.com.tw)