



Mail Server Solution

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

Sales Info
sales@sharetech.com.tw

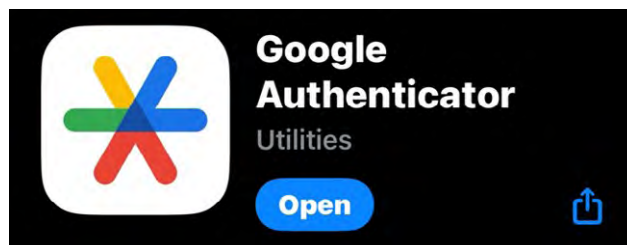
Tech Support
help@sharetech.com.tw



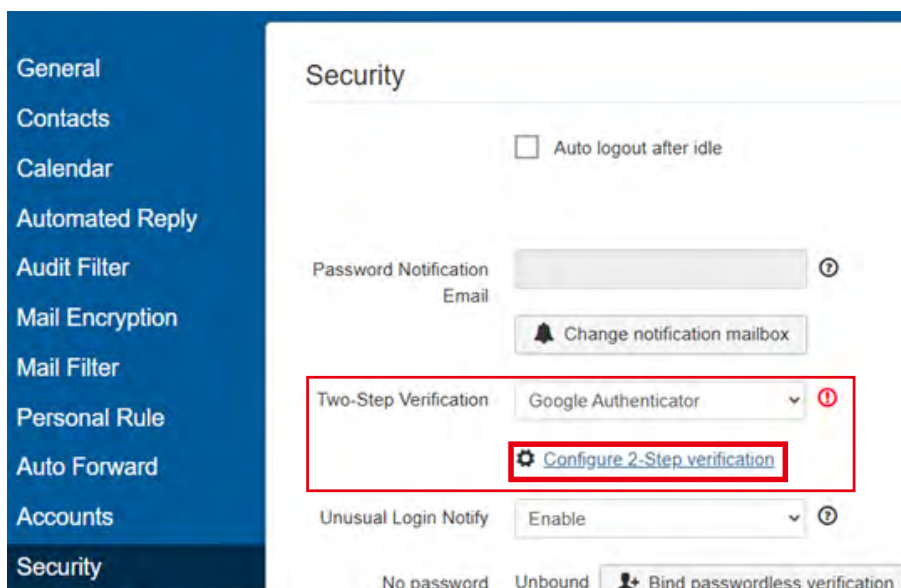
How to Bind and Verify Google Authenticator with New Webmail and MS Admin Interface

Binding Google Authenticator to New Webmail

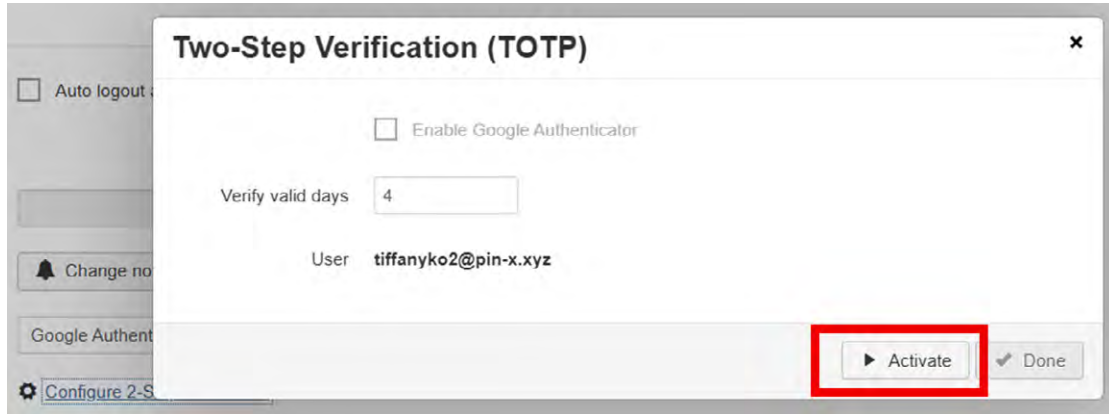
1. Download the [Google Authenticator](#) app on your mobile phone.



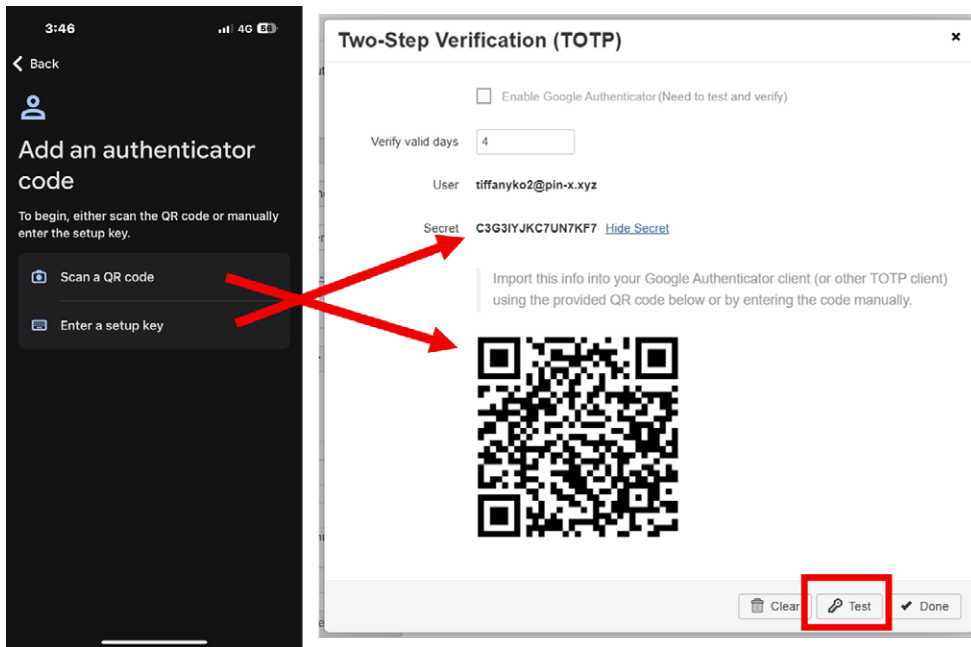
2. [New Webmail](#) > [Settings](#) > [Security](#) > [Two-Step Verification](#), select [Google Authenticator](#), and click [Configure 2-Step Verification](#).



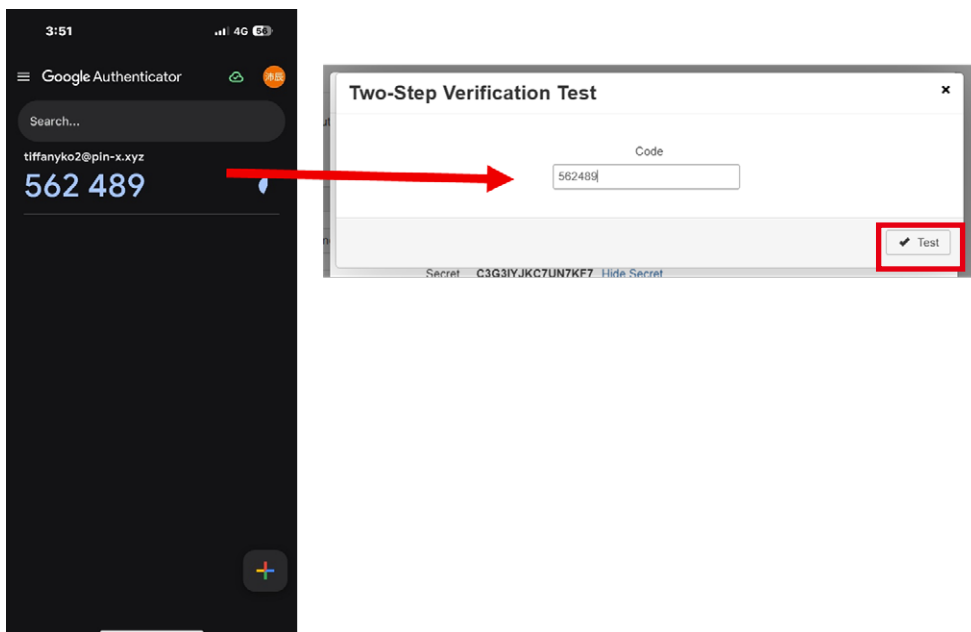
3. Click [Activate](#).



4. Open the Google Authenticator app. Choose [Scan a QR code](#) or [Enter a setup key](#). Then click [Test](#) on the New Webmail page.



5. Enter the code and click [Test](#).



6. You can set the validity period of the verification. Setting it to 0 means verification will be required every time.

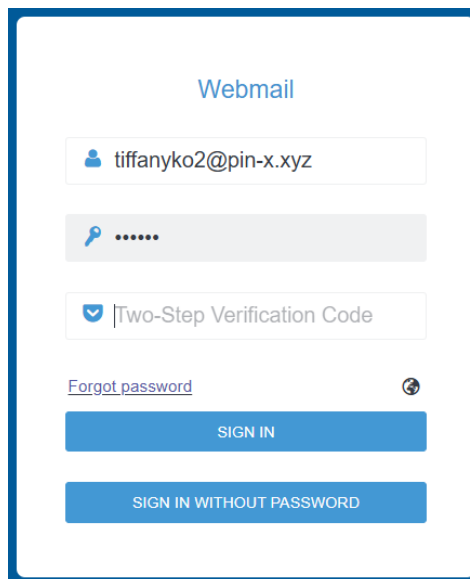
The value can range from 0 up to the number set in [Admin Interface > Mail Filter,Audit & Firewall > Mail Firewall > WebMail Two-Step Verification > Verification Validity Days](#). In this case, the range is 0–4 days. Click [Done](#) to complete the binding.



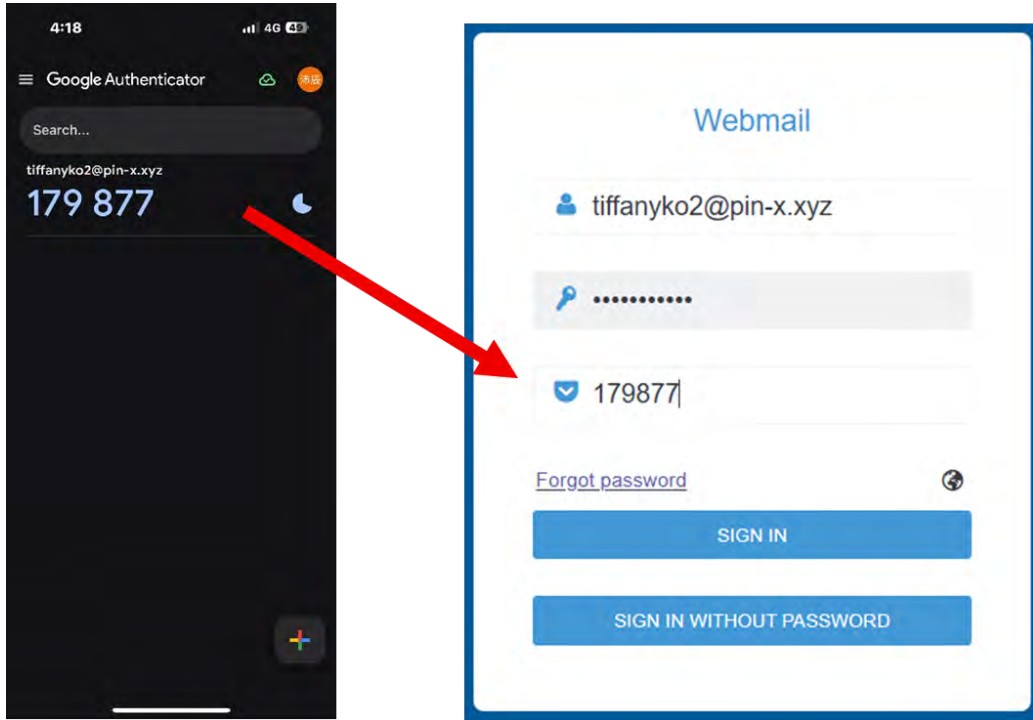
WebMail Two-Step Verification	Setup
Failure Block IP	Within 1 minute, the same source IP verification failed <input type="text" value="20"/> times, blocking IP
Failed User	User accumulated <input type="text" value="30"/> verification failures, blocked for 5 minutes
Verification Valid Days	<input type="radio"/> User defined <input checked="" type="radio"/> Administrator setting <input type="radio"/> Validate every time <input checked="" type="radio"/> No more verification is required within <input type="text" value="4"/> days after verification is successful

Logging in to New Webmail with Google Authenticator

1. On the login page, enter your account and password, then click [SIGN IN](#).

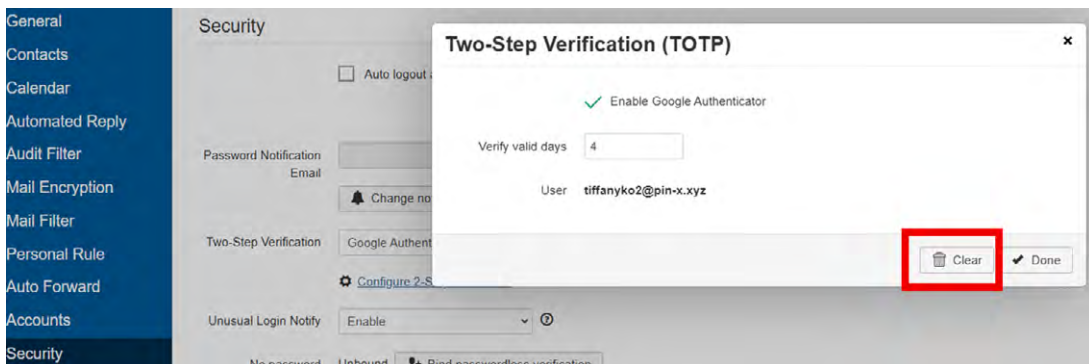


2. Open the Google Authenticator app, enter the verification code, and you're done.



Unbinding Google Authenticator from New Webmail

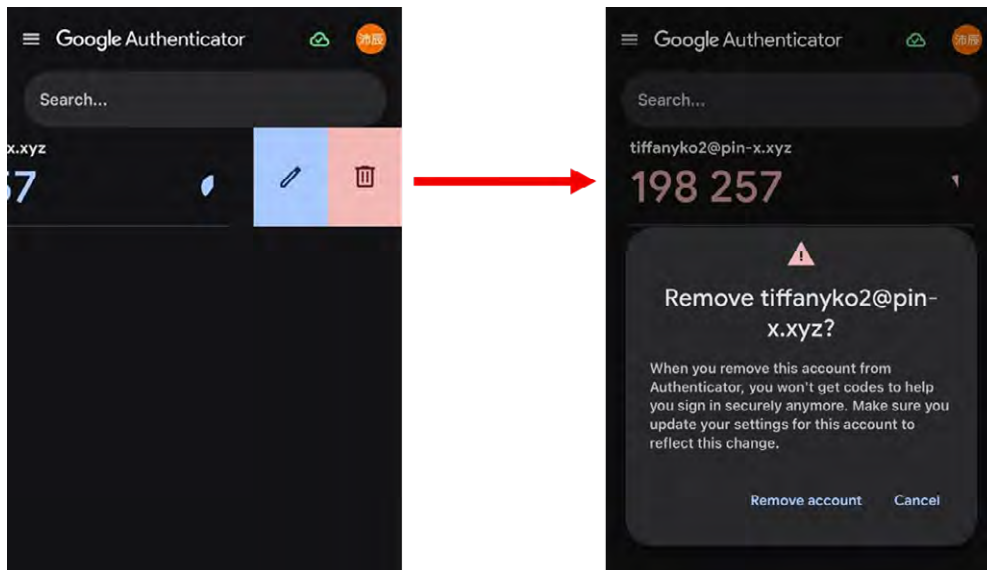
1. [New Webmail](#) > [Settings](#) > [Security](#) > [Two-Step Verification](#) > [Configure 2-Step Verification](#), click [Clear](#).



2. Complete the two-step verification to finish unbinding.

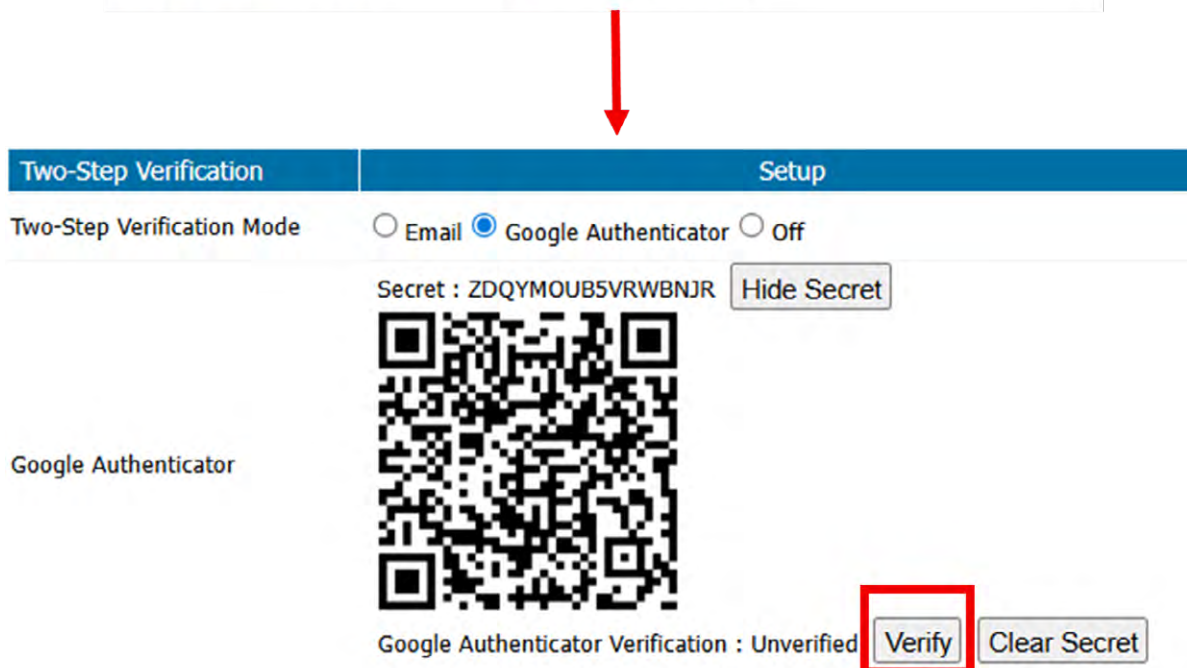
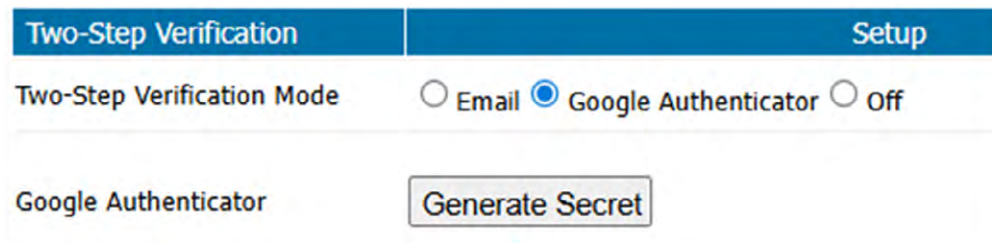


- On the Google Authenticator app, swipe left to remove the unbound account. This prevents confusion from duplicate account names if you bind the same account again.

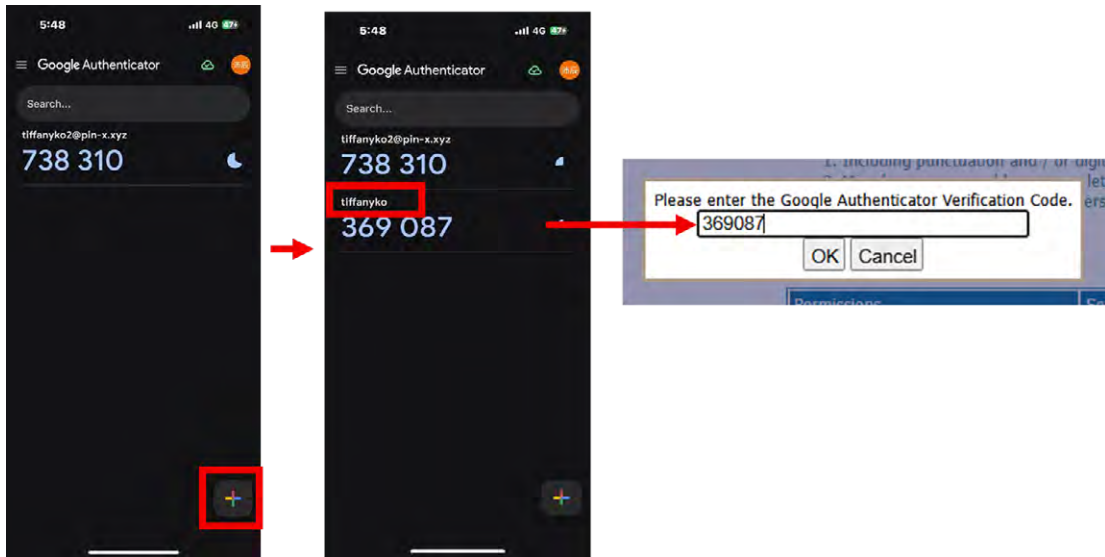


Binding Google Authenticator to MS Admin Interface

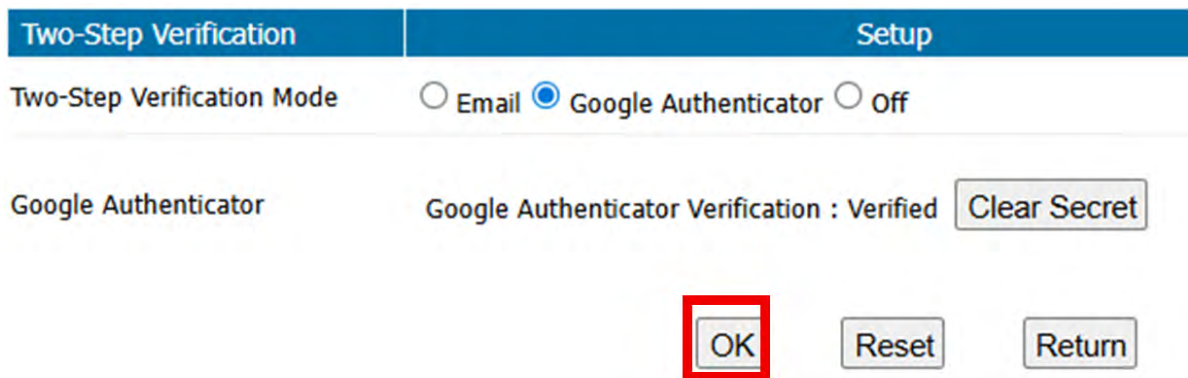
- [Admin Interface](#) > [System Management](#) > [Administrator Accounts](#), select the admin account you want to configure > [Two-Step Verification](#) > choose [Google Authenticator](#) > [Generate Secret](#) > [Verify](#).



2. Open the Google Authenticator app, tap **+**, and scan the QR code or enter the key.
Enter the verification code to complete the binding.

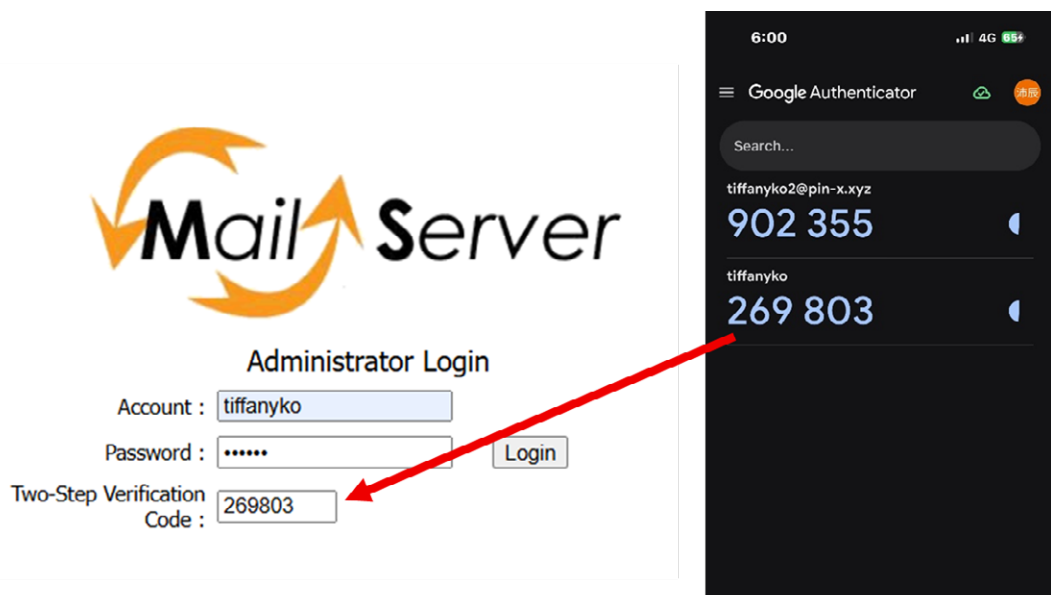


3. Remember to click **OK** to save the setting!



Logging in to MS Admin Interface with Google Authenticator

1. On the login page, enter your account and password, then click **Login**.
Open the Google Authenticator app, enter the verification code, and login will be successful.



Unbinding Google Authenticator from MS Admin Interface

1. [Admin Interface](#) > [System Management](#) > [Administrator Accounts](#), select the admin account you want to unbind > [Two-Step Verification](#) > [Clear Secret](#) > [off](#) > [OK](#)



2. On the Google Authenticator app, swipe left to remove the unbound account. This prevents confusion from duplicate account names if you bind the same account again.

