

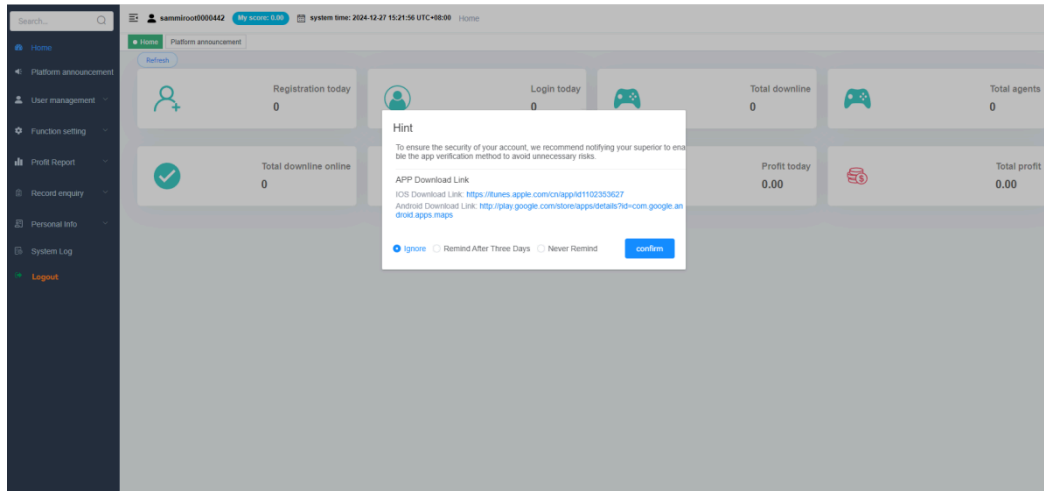
User Manual

To ensure your account's safety and reliability, it is recommended to use Google Authenticator for two-factor authentication when logging in !

Specific Steps:

1) How to Enable Permissions

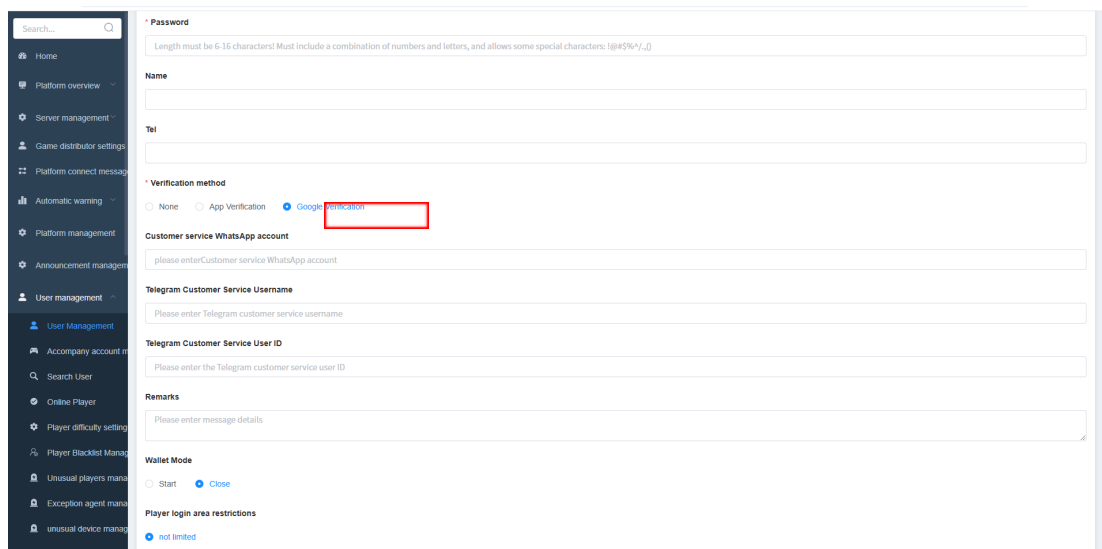
If your account is a standard agent account and your superior has not enabled the verification method for you, a prompt box will appear, as shown below:



You can notify your superior agent to enable Google Authenticator two-factor verification permissions for you via the backend.

This operation can be performed in the backend under **[User Management]** – **[Account Management]**, by selecting **[Google Verification]** in the **[Verification Method]** section.

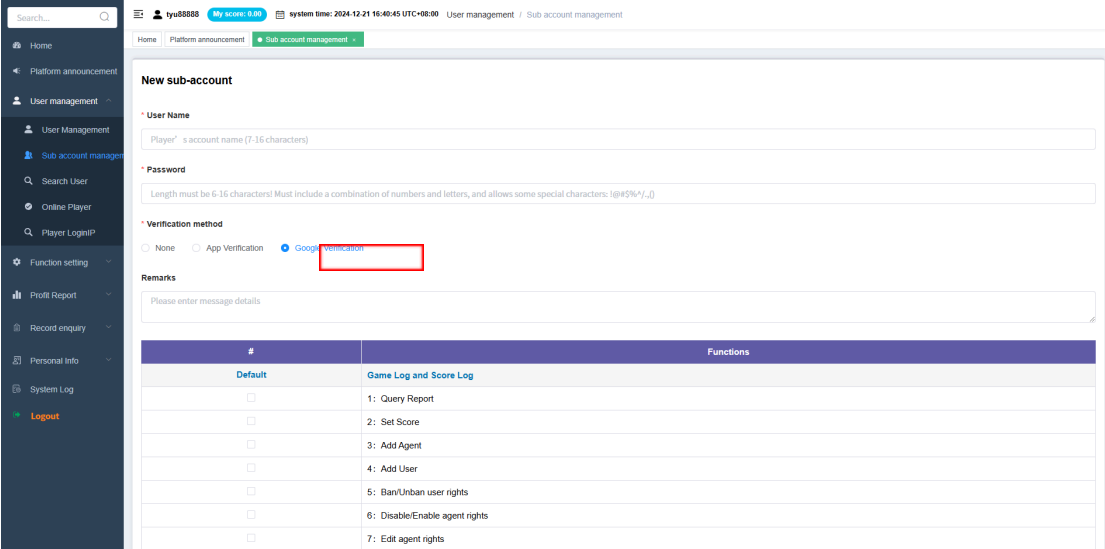
As shown below:



If your account is an agent sub-account, the agent master account can enable Google Authenticator two-factor verification permissions for you.

This operation can be performed in the backend under **[User Management]** – **[Sub-Account Management]**, by selecting **[Google Verification]** in the **[Verification Method]** section.

As shown below:



New sub-account

* **User Name**
Player's account name (7-16 characters)

* **Password**
Length must be 6-16 characters! Must include a combination of numbers and letters, and allows some special characters: !@#%&*~_~

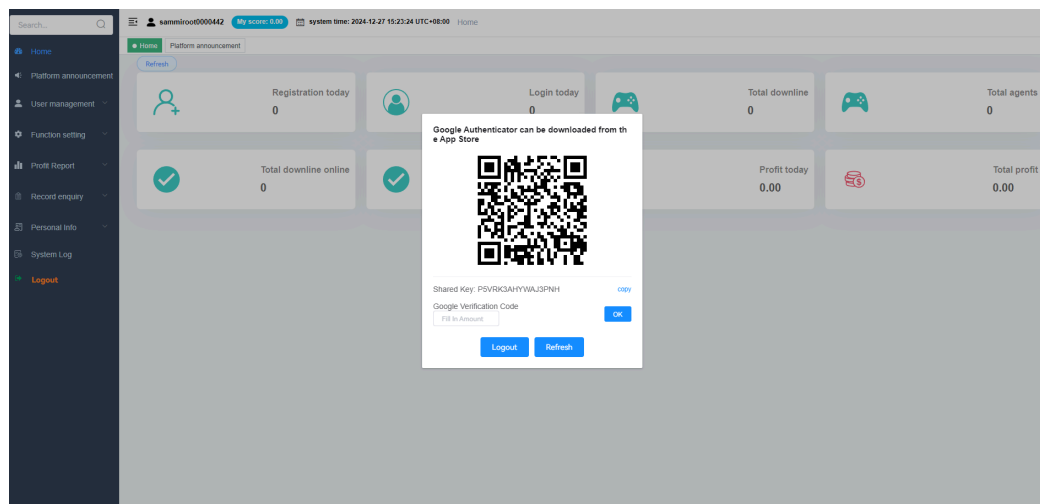
* **Verification method**
☐ None ☐ App Verification ☒ Google Verification

Remarks
Please enter message details

#	Functions
Default	Game Log and Score Log
☐	1: Query Report
☐	2: Set Score
☐	3: Add Agent
☐	4: Add User
☐	5: Ban/Unban user rights
☐	6: Disable/Enable agent rights
☐	7: Edit agent rights

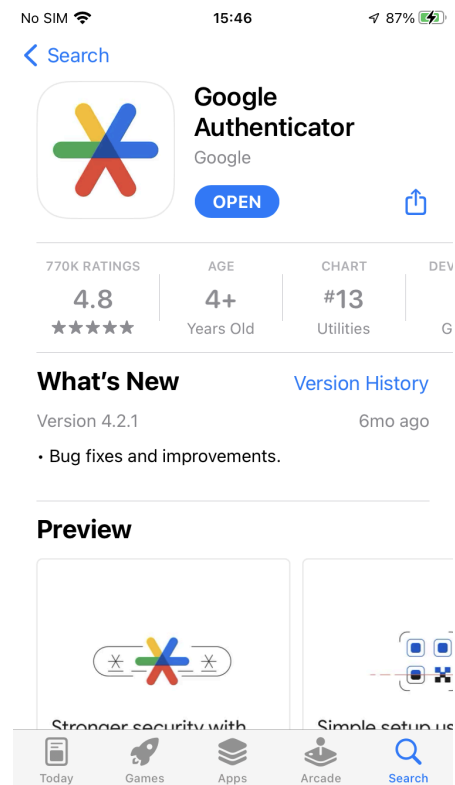
After enabling, when you log in to the backend, a QR code will pop up, prompting you to download Google Authenticator from the app store. At this point, you will be unable to continue operating in the backend.

As shown below:



2) Download the App

Based on your phone's operating system, you can download Google Authenticator from the app store.

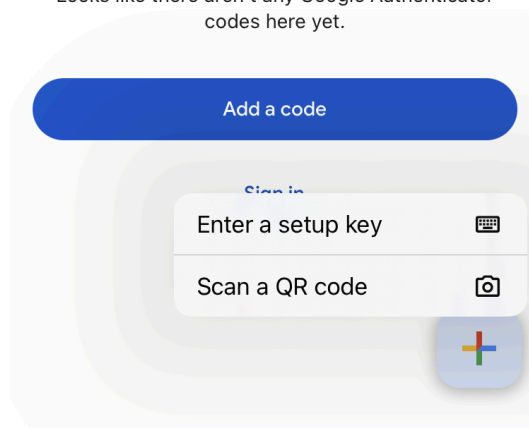


3) Open Google Authenticator and Bind to the Backend

1. After downloading, open Google Authenticator, and click **[+]** to select either **[Scan QR Code]** or **[Enter Setup Key]**, as shown below:

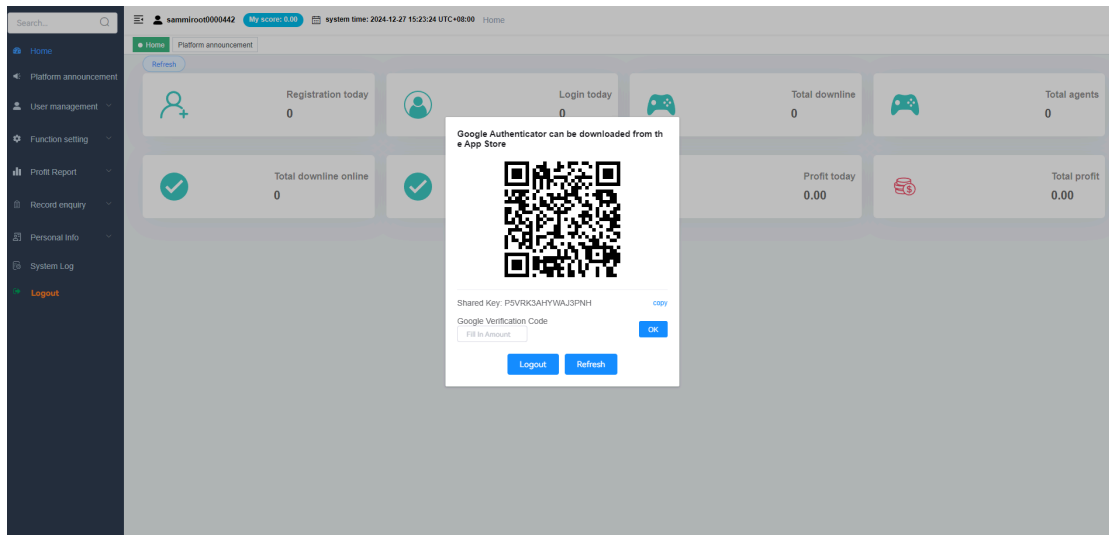


Looks like there aren't any Google Authenticator codes here yet.



2. Scan the QR code displayed on the backend or copy the shared key and enter the received verification code, as shown below:

(Scanning is valid permanently; you do not need to scan again for future logins unless you change your phone. In that case, you must request unbinding from your superior. Instructions for unbinding are provided at the end of the document.)



PS: If you are logging into the backend using a PC, it is recommended to use the QR code scanning method. If you are logging in via a mobile device, it is advisable to use the key method. The key method is shown below: (It is recommended to use your backend agent account as the account name.)

No SIM 15:46 87%

[< Back](#) Enter account details

Account name

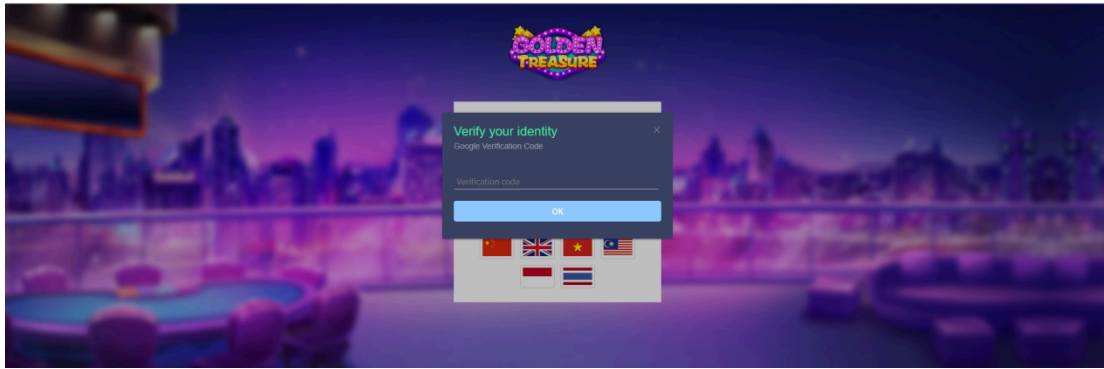
Your key

Type of key

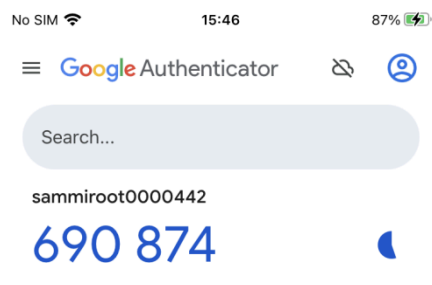
Time based

Add

3. When you log back into the backend, a Google Authentication confirmation screen will pop up. You need to complete the verification within 30 seconds, as shown below:



4. At this point, you need to open the Google Authenticator to view the verification code sent to the corresponding account and enter it into the verification box in the backend, as shown in the image below:



4) Google Authenticator Unbinding

If your phone is lost or you change your phone, you need to inform your superior agent/main account to unbind it for you.

Your superior needs to go to the [Edit] page of your account, click the [Unbind] button under the [Account Device] option to unbind it. After the unbinding, you will need to rebind it on the new phone in order to continue using this feature.

As shown in the image below:

Search...

Home

Platform overview

Server management

Game distributor settings

Platform connect message

Automatic warning

Platform management

Announcement management

User management

User Management

Sub account management

Accounting account management

Search User

Online Player

Player difficulty setting

Player Blacklist Management

Unusual players management

System Admin Management 100%

User Name OP123456

* Password

Length must be 6-16 characters! Must include a combination of numbers and letters, and allows some special characters: !@#\$%^&*~_.

Name

Tel

* Verification method

☐ None

☐ App Verification

☒ Google Verification

Key

*****BQWMMGJFY

[Unbind](#)

Customer service WhatsApp account

please enterCustomer service WhatsApp account

Telegram Customer Service Username

Please enter Telegram customer service username

Telegram Customer Service User ID

Please enter the Telegram customer service user ID