

Two-Factor Authentication (TOTP) and IDExpert Tokens User Guide

Version 1.2 · Last updated: 2026/08/14

Who this guide is for

Anyone who holds an account issued by the **Institute of Information Science** (IIS) or the **Research Center for Information Technology Innovation** (CITI), Academia Sinica, and whose account is **currently valid**. You do not have to be IIS or CITI staff — it applies equally to members of other Academia Sinica units and to external users who were granted an account on request.

Why you should complete the setup now

The new two-factor authentication (TOTP) and IDExpert tokens are being rolled out in stages, and internal systems, Webmail, VPN and other services **are being switched over on different schedules**. Services that have not yet switched still use their existing sign-in methods, so completing the setup will not change how you sign in to them today.

As services switch over, **you will not be able to sign in to the ones that have switched until your setup is complete**. The Account System itself is only accessible from the internal network, so if you are off-site when that happens and cannot sign in to the VPN with a verification code because your setup is not yet complete, you could end up in a situation where completing the setup requires a connection, and the connection requires the completed setup. In that situation, you will need to contact the Center of Computer Service for assistance.

IDExpert tokens are **not mandatory**, but they will become one of the available sign-in methods once services switch over. If your employment category is within the eligible range (see Chapter 3), **we recommend setting up an IDExpert token as well**, so that you have more than one way to sign in later on. Since the rollout is **already under way**, and completing the setup does not affect services that have not yet switched, it is best to complete it soon, before a service you rely on switches over.

Contents

1. Before You Begin

- 1.1 What Each Account Type Needs to Set Up
- 1.2 What You Will Need
- 1.3 How to Access the Account System

2. Setting Up Two-Factor Authentication (TOTP)

- 2.1 Sign In to the Account System
- 2.2 Open the Setup Page and Request a Setup Link
- 2.3 Open the Link in the Email and Enter Your Password
- 2.4 Scan the QR Code to Finish
- 2.5 What Changes After Setup

3. Setting Up IDExpert Tokens

- 3.1 Open "IDExpert Tokens" and Unlock
- 3.2 Understanding the Token Screen
- 3.3 Setting Up a Mobile APP Token
- 3.4 Setting Up a FIDO Key Token
- 3.5 Testing a Token
- 3.6 Delete, Rebuild and Reset

4. Changing Phones or Losing Your Authenticator

- 4.1 If You Can Still Sign In
- 4.2 If You Can No Longer Sign In

5. Frequently Asked Questions

6. Contact

1. Before You Begin

1.1 What Each Account Type Needs to Set Up

There are two account types, and the requirements differ:

Account type	Two-factor authentication (TOTP)	IDExpert tokens
Regular account	Required (see Chapter 2)	Available to certain employment categories only, up to 3 (see Chapter 3)
Disposable account	Required (see Chapter 2)	Not available ; the menu item will not appear

1.2 What You Will Need

- Your **account name and password**.
- A smartphone with an **authenticator app** installed. Google Authenticator is recommended, but Microsoft Authenticator and others work just as well.
- The **IDExpert app** on your phone, if you plan to set up a Mobile APP token.
- Your FIDO security key, or a device with biometrics (fingerprint / face), if you plan to set up a FIDO Key token.

1.3 How to Access the Account System

The Account System is only accessible from the **internal network**. Open the following address in your browser:

<https://as.iis.sinica.edu.tw/account/>

- **If the page opens** — carry on with Chapter 2.
- **If it does not open** (connection timeout, page not found) — connect to the **IIS / CITI VPN** first, then try again.

How to request and connect to the VPN (**this page is in Chinese only**):

<https://www.iis.sinica.edu.tw/zh/page/ComputerCenter/ComputerAndInternet/VPN.html>

If your account does not have VPN permission, or the page still does not open after you connect to the VPN, please contact the Center of Computer Service (see Chapter 6).

2. Setting Up Two-Factor Authentication (TOTP)

Two-factor authentication adds a second step to signing in: on top of your password, you enter a **one-time code** generated by an authenticator app. Every account — regular and disposable alike — has to be set up this way, and you only need to do it once.

2.1 Sign In to the Account System

1 Sign in with your account and password

Open the Account System in your browser, enter your username and password, and click “Log in”.

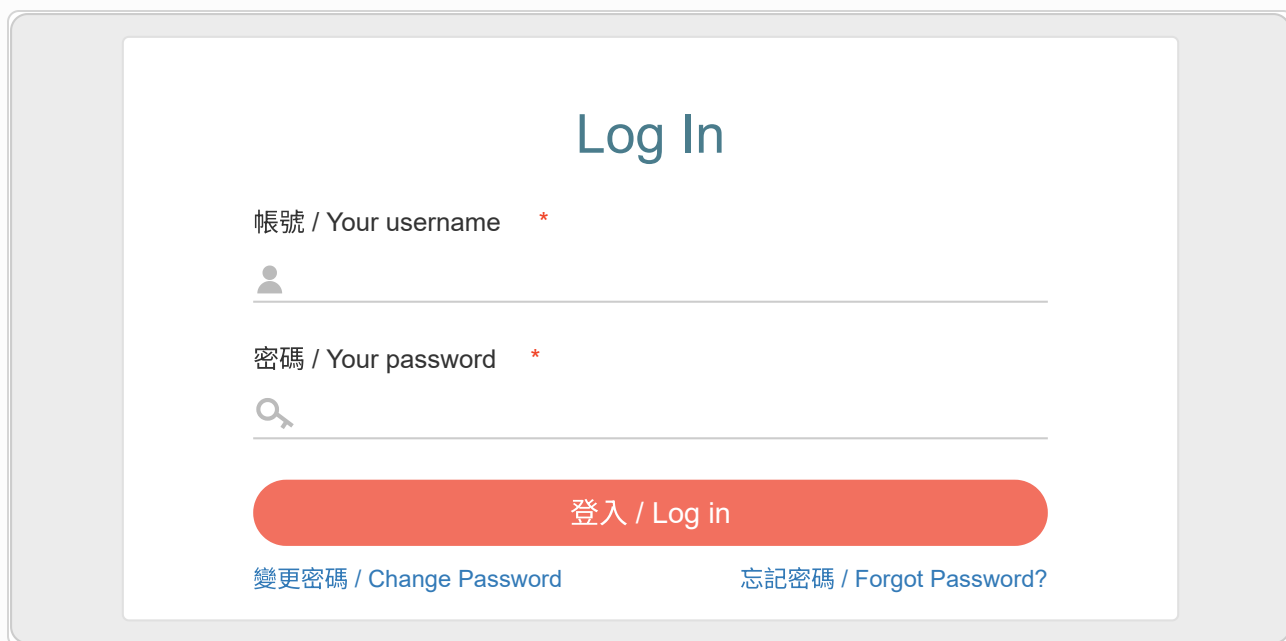


Figure 2-1 Sign-in page (labels are shown in both Chinese and English)

Note

Signing in to the Account System itself currently requires **only your account and password** — no one-time code. The code is used for the purposes described in Section 2.5.

2.2 Open the Setup Page and Request a Setup Link

2 Use the menu under your name

After signing in, your name appears in the top-right corner. Click it to open the menu and choose “**Authenticator App (TOTP)**”.

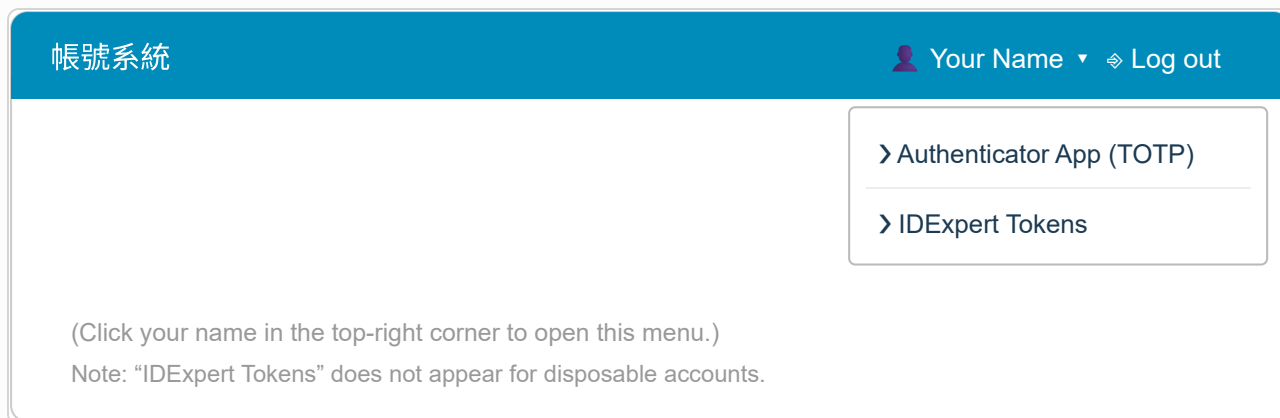


Figure 2-2 The menu under your name

3 Check your status and start the setup

The page shows “Your OTP verification status”. On your first visit this reads **Not Enabled** in red; click “**Click here to set up**”.

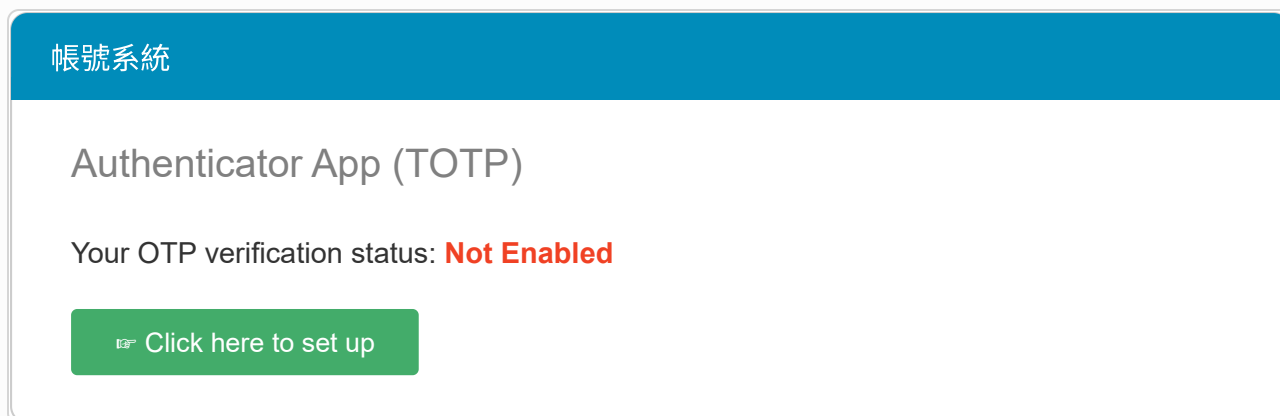


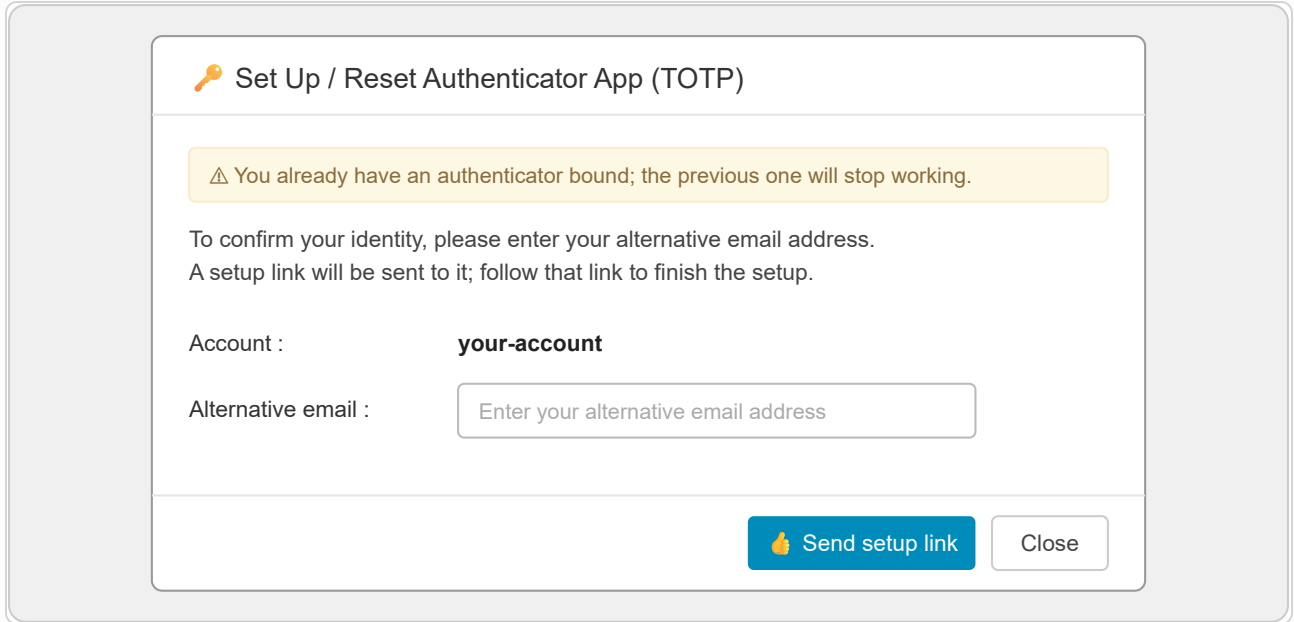
Figure 2-3 Authenticator App (TOTP) page, not yet enabled

If it says “Enabled”

You have already set this up, and the button reads “**Click here to reconfigure**”. There is no need to do it again unless you are moving to a new phone or want to start over. Note that registering again immediately stops the previous entry in your authenticator app from working.

4 Enter your alternative email to request a setup link

A dialog opens. Enter your **alternative email address** (it must match the one registered on your account) and click “**Send setup link**”.



 Set Up / Reset Authenticator App (TOTP)

 You already have an authenticator bound; the previous one will stop working.

To confirm your identity, please enter your alternative email address.
A setup link will be sent to it; follow that link to finish the setup.

Account : **your-account**

Alternative email :

 Send setup link

Figure 2-4 The dialog for entering your alternative email

Once the link has been sent, the dialog closes automatically and a green “The setup link has been sent” message appears on the page.

If it says the address does not match

If you have **no alternative email registered**, or you can no longer receive mail there, please contact the Center of Computer Service (see Chapter 6).

2.3 Open the Link in the Email and Enter Your Password

5 Open the link before it expires

You will receive an email titled "Set Up Your Authenticator App (TOTP)". Open the link before the deadline stated in the email — you have 30 minutes — and note that it can only be used **once**.

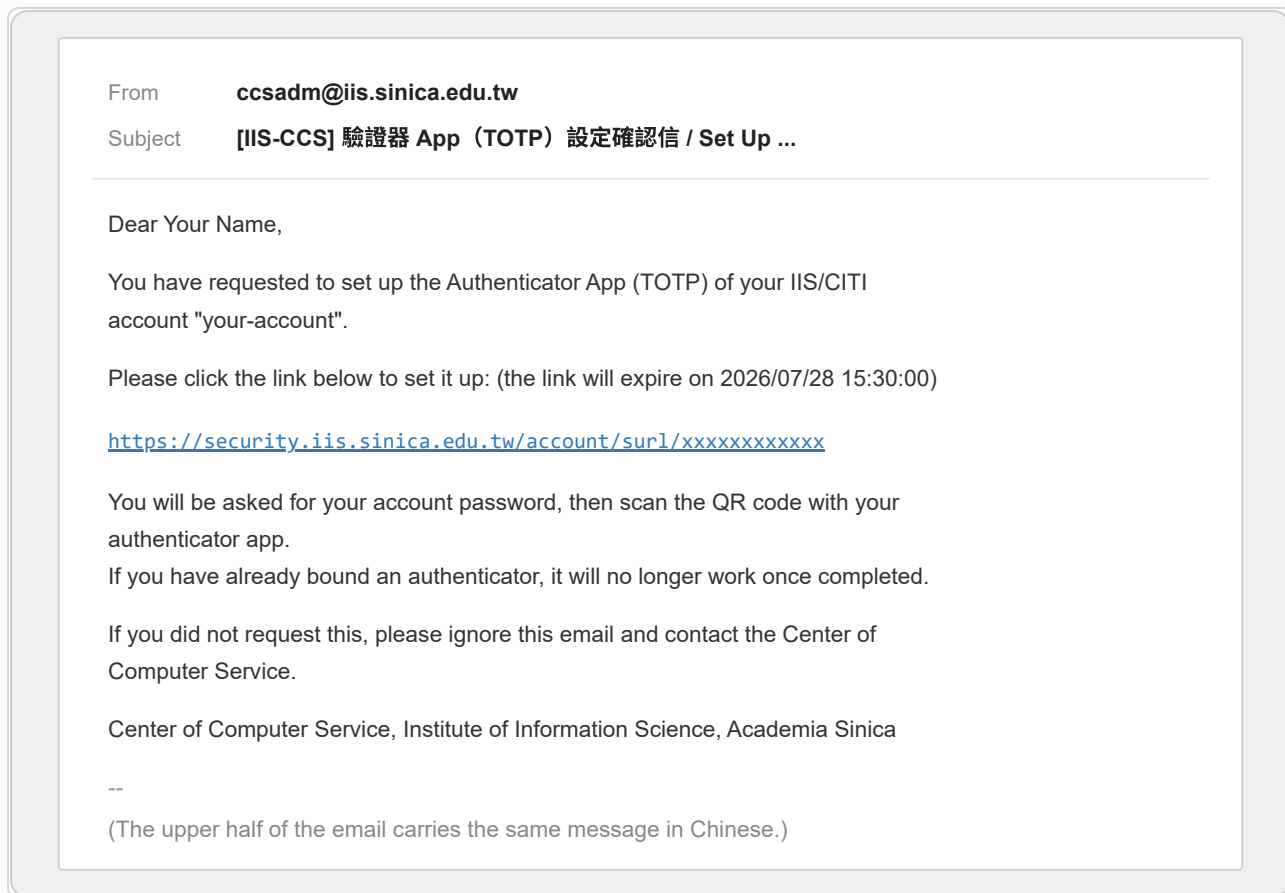


Figure 2-5 The setup confirmation email (one email, Chinese and English)

If you request more than one link

Every click of "Send setup link" creates a new link and **immediately invalidates the previous one**. If you requested several, be sure to use the link in the **most recent** email.

6 Enter your account password

The page that opens asks for **the password of that account**, along with an “I’m not a robot” check. The QR code appears only after both are accepted.

設定／重新綁定驗證器 App (TOTP)
Set Up / Reset Authenticator App (TOTP)

To confirm your identity, please enter the password of this account.

帳號 Account Name : your-account

密碼 Password :

☐ I'm not a robot

✓ 下一步 Next

Figure 2-6 After opening the link, you must enter your password first

2.4 Scan the QR Code to Finish

7 Scan, then enter the 6-digit code

A **QR code** and a **Secret Key** appear. Open the authenticator app on your phone and choose "Scan a QR code". If you cannot scan it, switch to manual entry in the app and type in the Secret Key shown on screen instead.

Once scanned, the authenticator app starts showing a 6-digit code that changes every 30 seconds. Type the code **currently displayed** into the "OTP" field and click "**Finish**".

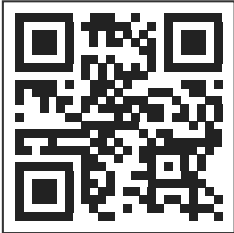
Once the setup is complete, a separate "setup notification" email is sent to your alternative email address. If you receive one for a change you did not make, contact the Center of Computer Service immediately (see Chapter 6).

設定／重新綁定驗證器 App (TOTP)

Set Up / Reset Authenticator App (TOTP)

If you have already bound an authenticator, it will stop working once completed.

1. Install and open an authenticator app (Google Authenticator recommended), then scan the QR code below or manually enter the Secret Key.



Secret Key : AAAABBBBCCCCDDDEEEFFFFFGGGGHHHH

2. Enter the 6-digit code from your authenticator app below, then click "Finish".

OTP:

Finish

Figure 2-7 Scan the QR code and enter the one-time code

If you see “OTP verification failed. Please re-enter.”

1. Try again with the **latest** 6-digit code in the app (it changes every 30 seconds).
2. Set your phone’s date and time to **automatic** — if its clock drifts too far, verification will fail.
3. Make sure you scanned or typed the QR code / Secret Key from **this** session.

2.5 What Changes After Setup

At present, the code for this new entry is used for two things:

- Unlocking the “**IDExpert Tokens**” page in the Account System (see Section 3.1).
- Signing in to services as they move to the new two-factor authentication — you will be told when each one changes over.

Important: keep using your existing sign-in method

Services still use their existing authentication for now and are **not affected by this setup**.

Therefore:

- When signing in to internal systems, Webmail or VPN, **keep doing what you do today** — do not switch to the code created here.
- **Do not delete** any existing entry in your authenticator app, or you will break your current sign-in.
- After this setup you will see **two entries** in your authenticator app. That is expected; they are independent and do not affect each other.

How to tell the two entries apart

The entry created here appears as “**IIS Account**” followed by your account name. Use the entry that matches the service you are signing in to.

Keep it safe

Your authenticator app is tied to this phone. See Chapter 4 for what to do if you change or lose it.

3. Setting Up IDEXpert Tokens

This chapter applies to **regular accounts only**. If you have a disposable account, the feature is not available to you and “IDExpert Tokens” will not appear in the menu.

The feature is also limited to people **currently employed at IIS or CITI** whose employment falls into one of the following three categories:

- **Research staff** — including Distinguished Research Fellow, Research Fellow, Associate Research Fellow, Assistant Research Fellow, Research Technician, Associate Research Technician, Assistant Research Technician, Adjunct Research Fellow and Corresponding Research Fellow.
- **Full-time staff** — including postdoctoral scholars, doctoral-level contract staff, project staff, contract administrative and research assistants, international graduate students and student helpers.
- **Students on stipend** — including doctoral students, master’s students and undergraduates.

Eligibility is determined by the personnel records and is checked continuously — it is not a one-time setting. If your employment later changes (for example when you leave or move to a different type of post) or your account passes its valid period, your IDEXpert user status is set to disabled automatically and your tokens can no longer be used for verification. The tokens themselves are **not deleted**, and if you become eligible again the status returns to normal automatically.

If your employment is not in one of these categories (for example joint-appointment or visiting, temporary or business-purpose staff, or if you have resigned or retired), the page will say so when you open it, and you will only be able to delete or reset an existing token — not set up a new one. If you believe your employment category has been recorded incorrectly, please contact the Center of Computer Service.

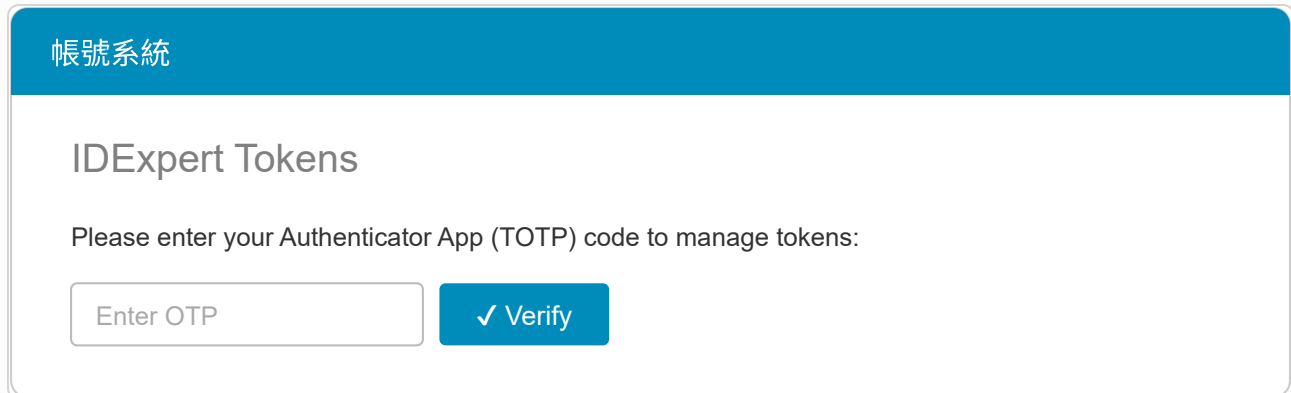
IDExpert tokens are an alternative multi-factor method and come in two kinds: **Mobile APP** (push notification / OTP) and **FIDO Key** (hardware security key / biometrics). You may have up to **3** tokens in total across both kinds.

3.1 Open “IDExpert Tokens” and Unlock

1 Unlock with your one-time code

Choose “IDExpert Tokens” from the menu under your name. For security, this page must be unlocked with a TOTP code every time you open it:

- If you have **not** finished Chapter 2 yet, the page shows a message in red along with a link, “Go to Authenticator App (TOTP) Setup”. Do that first.
- Otherwise, enter the code currently shown in your authenticator app and click “**Verify**”.



The screenshot shows a web interface for 'IDExpert Tokens'. At the top is a blue header bar with the text '帳號系統' (Account System) in white. Below the header, the title 'IDExpert Tokens' is displayed in a large, dark font. Underneath the title, a message reads: 'Please enter your Authenticator App (TOTP) code to manage tokens:'. Below this message is a form consisting of a text input field with the placeholder text 'Enter OTP' and a blue button with a white checkmark icon and the text 'Verify'.

Figure 3-1 The IDExpert Tokens page must be unlocked with a one-time code

3.2 Understanding the Token Screen

2 What is on the screen

Once unlocked, the token screen appears. At the top, “IDExpert User Status” applies to **your IDExpert account as a whole**, next to how many tokens you have issued so far; below that, Mobile APP and FIDO Key each have their own card, and each card has its own “Token Status”. Tokens you have not created yet show “Not Issue”.

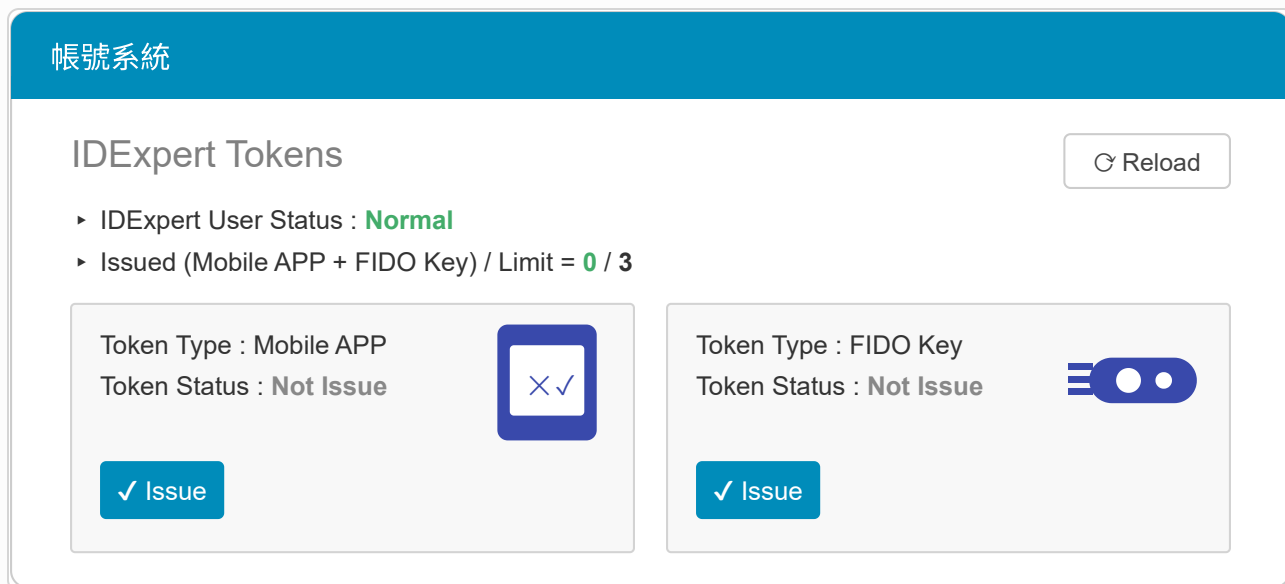


Figure 3-2 Token screen with no tokens issued yet

If “IDExpert User Status” is not “Normal”

A message appears at the top of the screen, and the “Issue”, “Register” and verification buttons are hidden — in these states IDExpert will not accept a new token, and verification is bound to fail. You can still use “Delete” and “Reset” to remove existing tokens. Please contact the Center of Computer Service to check your account status. “Locked” is the one exception: it is a temporary state after repeated failed verifications, so the buttons stay visible and it clears by itself — just try again a little later.

“Token Status” shows which stage a token has reached:

Status	Not Issue Not created yet — click “Issue” to add it.
	Pending Registration Issued but not yet registered — click “Register”.
	Active Registered and ready to use.
	Pending Binding Pending Activation Disabled Other states — contact the Center of Computer Service if one persists.

3.3 Setting Up a Mobile APP Token

3 Issue the token

On the **Mobile APP** card, click **"Issue"**. The status changes to **"Pending Registration"** and a **"Register"** button appears.

4 Register by scanning with the IDExpert app

Click **"Register"**. A window opens with download links for the IDExpert app and a QR code. Install and open the **IDExpert app** on your phone first, then use it to scan the QR code.

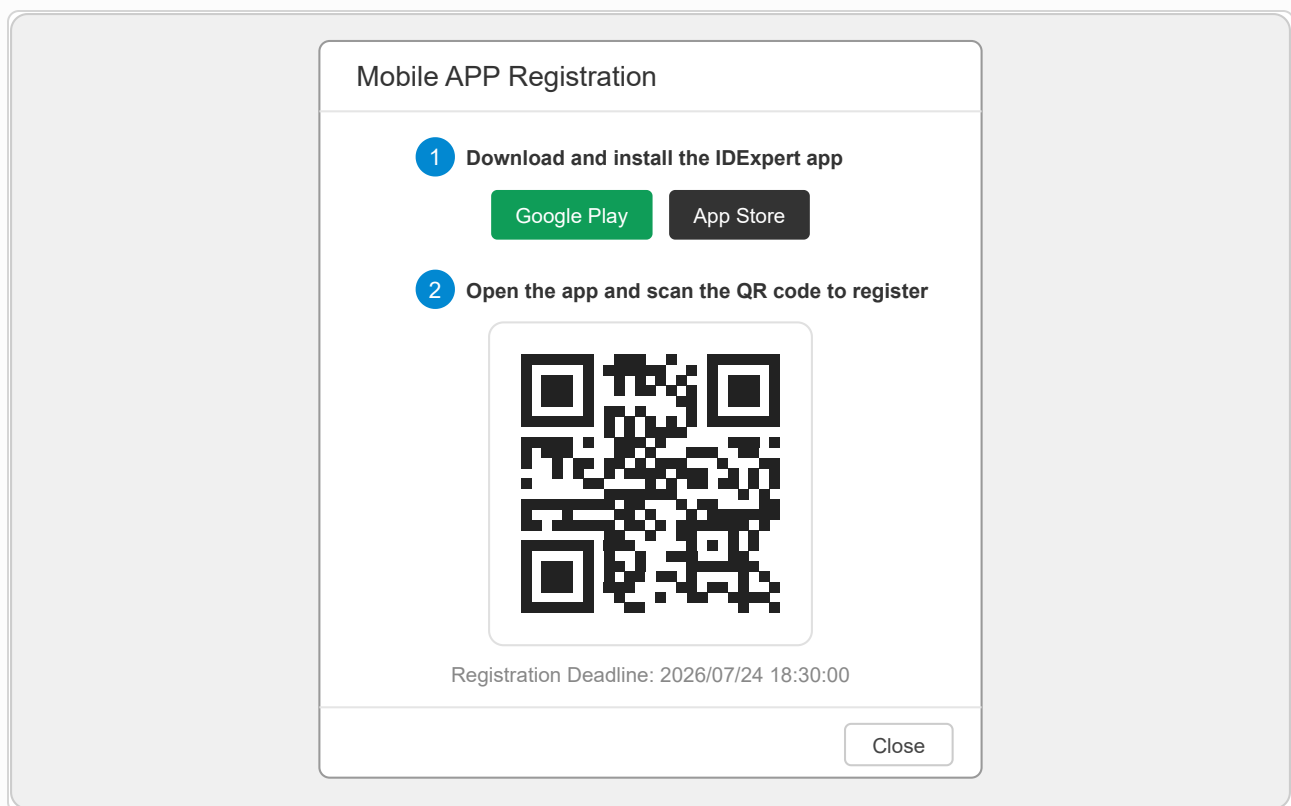


Figure 3-3 Mobile APP registration window

Note

The QR code comes with a **registration deadline**, shown at the bottom of the window, so scan it promptly. When you are done, close the window and click **"Reload"**; the card status then changes to **"Active"**. If the deadline passes, click **"Register"** again for a fresh QR code.

3.4 Setting Up a FIDO Key Token

5 Issue and register

On the **FIDO Key** card, click "**Issue**", then "**Register**" once the status shows "Pending Registration". Your browser will prompt you to register a security key — follow the prompt to **insert your FIDO key and touch it**, or use your device's biometrics (fingerprint / face).

You will then see "FIDO Key registration completed", and the card status changes to "Active".

Note

FIDO registration requires a browser and operating system that support WebAuthn (all recent mainstream browsers do). If you do not have a hardware key, some devices can use built-in biometrics as the authenticator instead.

3.5 Testing a Token

Once a token is "Active", the card offers test buttons so you can confirm it works:

Token type	Button	What it does
Mobile APP	Verify Push	Sends a push notification to your phone, which you approve in the IDExpert app. While it waits, the screen shows a "waiting for push" message.
	Verify OTP	Enter the code shown in the IDExpert app and click "Submit".
FIDO Key	Verify	Follow the browser prompt to touch your security key or use biometrics; on success you see "FIDO Key verification succeeded".

3.6 Delete, Rebuild and Reset

Token cards offer three further actions. You will not normally need them once your setup is complete:

Action	Applies to	What it does
Delete	Both kinds	Removes the token and frees up one of your three slots.
Rebuild	Both kinds	Deletes the token and issues it again — useful for starting over if one stops working properly.
Reset	FIDO Key only	Clears the existing registration and returns the token to “Pending Registration” so you can register it again.

Each action asks you to confirm before it goes ahead.

4. Changing Phones or Losing Your Authenticator

Whether you have changed phones, lost your phone, deleted the authenticator entry, or your account is new and not yet set up, follow whichever section below matches your situation.

4.1 If You Can Still Sign In

Sign in to the Account System, open “Authenticator App (TOTP)” as described in Section 2.2, then click “**Click here to reconfigure**”. From there the steps are exactly the same as the first-time setup: enter your alternative email to request a setup link, then follow Section 2.3 and Section 2.4 to open the link, enter your password and scan the new QR code.

Note

Once the new registration is complete, the **previous authenticator entry stops working immediately**. Use the new one from then on.

If you also need to move an IDEXpert Mobile APP token to a new phone, use “**Rebuild**” on the token card and register again from the new phone (see Section 3.3).

4.2 If You Can No Longer Sign In

If you can no longer sign in to the Account System — for example you lost your phone, or you are off-site and cannot use the VPN — please contact the **Center of Computer Service** (see Chapter 6).

Once your identity has been confirmed, they will send a one-time setup link to your **alternative email address**. From there the steps are the same as the self-service route: follow Section 2.3 and Section 2.4. At no point do they see **your authenticator secret key**.

Note

Once the new registration is complete, the **previous authenticator entry stops working immediately**. Use the new one from then on.

Security note

Once the setup is complete, a notification email goes to your **alternative email address**. If you receive one for a change you did not make, contact the Center of Computer Service immediately.

5. Frequently Asked Questions

Why was I not asked for a one-time code when signing in to the Account System?	Signing in to the Account System currently needs only your account and password. The code you create here unlocks the “IDExpert Tokens” page, and other services will start asking for it as they move to the new two-factor authentication.
After setup, do I use the new code for other services?	No. Internal systems, Webmail and VPN still use their existing authentication — carry on as you do today, and do not delete any existing entry in your authenticator app. See Section 2.5.
My authenticator app now shows two entries — did I register twice by mistake?	No — this is exactly what should happen. Your existing entry still covers the services you use today; the new one appears as “IIS Account” followed by your account name. The two are independent and do not affect each other.
The Account System address will not open.	It is only accessible from the internal network, so connect to the IIS / CITI VPN and try again. If it still will not open, contact the Center of Computer Service (see Chapter 6).
The setup link never arrived.	Check your spam folder first. If the address is correct and nothing has arrived, or you have no alternative email registered on your account, contact the Center of Computer Service (see Chapter 6).
The setup link will not open, or says it is no longer valid.	A link is valid for 30 minutes and can only be used once. Requesting another one also invalidates the previous link immediately , so always use the link in the most recent email. If it has expired, go back to the setup page and request a new one.
TOTP verification keeps failing.	(1) Use the latest 6-digit code (it changes every 30 seconds). (2) Set your phone’s date and time to automatic. (3) Make sure you used the QR code / Secret Key from this session.
I changed my phone — what now?	TOTP: open the “Authenticator App (TOTP)” page and set it up again; the previous entry stops working (see Section 4.1). IDExpert Mobile APP: use “Rebuild” on the token card, then register from the new phone.

I cannot find “IDExpert Tokens”.	It is available to regular accounts only. If you have a disposable account the option does not appear, and you only need to complete the TOTP setup.
IDExpert used to work for me. Why does it no longer work?	Eligibility is checked continuously against the personnel records. If your employment changes (for example when you leave or move to a different type of post) or your account passes its valid period, your IDExpert user status is set to disabled automatically and your tokens can no longer be used for verification — but they are not deleted , and the status returns to normal automatically if you become eligible again. See the start of Chapter 3.
The “Issue” button has disappeared.	There are two possible reasons. (1) You have reached the token limit — up to 3 tokens in total across Mobile APP and FIDO Key. The screen shows “Limit Reached”; delete a token you no longer need to free one up. (2) Your “IDExpert User Status” is not “Normal” — the Issue, Register and verification buttons are all hidden, and a message appears at the top of the screen. Please contact the Center of Computer Service (see Section 3.2). The most common cause is that your employment category is not among those the feature is open to — see the start of Chapter 3.
Why do I have to enter a code every time I open the IDExpert page?	This is by design — the “IDExpert Tokens” page is unlocked with a one-time code every time you open it.
I see “Operation too frequent, please try again later”.	Repeating an action too quickly (issuing, deleting, reloading, or requesting registration QR codes) is rate-limited for a short while to protect the system. Wait a moment and try again.
The Mobile APP registration QR code expired.	Registration QR codes expire after a short time. Go back to the token screen and click “Register” again for a new one.
The page says my account is disabled, locked, or not within its valid period.	That is about the account itself , not about this setup. Please contact the Center of Computer Service.

6. Contact

Center of Computer Service, Institute of Information Science, Academia Sinica

- Phone: +886-2-2788-3799 ext. 1301
- Online service desk: <https://eform.iis.sinica.edu.tw/surl/asApply/electronicDeviceIssues>