



YubiOn FIDO Logon Standalone

End User Guide



SOFTGIKEN Co., Ltd.

August 2026 Edition

Contents

Contents.....	2
Chapter 1. Introduction.....	3
1.1 What FIDO Logon Is	3
1.2 Who This Guide Is For.....	3
1.3 What You Need	3
1.4 How This Guide Is Organized	3
Chapter 2. Registering Your Authenticator	4
2.1 When Your Administrator Registers It in Advance	4
2.2 When You Register It Yourself (at First Sign-In)	4
Chapter 3. Signing In with Your Authenticator	9
3.1 How the Sign-In Screen Looks	9
3.2 Signing In for the First Time	10
3.3 Signing In from the Second Time On	13
3.4 Signing In over Remote Desktop (RDP).....	13
Chapter 4. About the PIN	15
4.1 What the PIN Is For.....	15
4.2 Setting and Changing the PIN.....	15
4.3 Cautions About the PIN	15
Chapter 5. If Something Goes Wrong	18
5.1 You Forgot or Lost Your Authenticator.....	18
5.2 You Forgot the PIN, or the Authenticator Is Locked.....	18
5.3 Signing In with a Recovery Code (Emergency)	18
5.4 The Screen Locked When You Removed the Authenticator.....	20
5.5 The FIDO Tile Does Not Appear on the Sign-In Screen	20
Appendix Glossary	21
Contact	22

Chapter 1. Introduction

1.1 What FIDO Logon Is

On a computer where **YubiOn FIDO Logon Standalone** (hereafter "this product") is installed, you can sign in to Windows with your **FIDO2 authenticator (a security key such as a YubiKey)** instead of typing your password every time.

Signing in with an authenticator has the following advantages.

- It is **more secure**, because it resists shoulder surfing and impersonation.
- Once your password has been stored, you can sign in with **just your PIN and a touch** from then on.

1.2 Who This Guide Is For

This guide is intended for **general users (end users)** of a Windows computer on which this product has been installed.

Installing and configuring the product on the computer is handled separately by your system administrator. If your authenticator has not been registered yet, please contact your administrator.

1.3 What You Need

- A **FIDO2 authenticator** issued to you by your administrator, or one that is already registered
- The **PIN** set on that authenticator (or biometrics such as a fingerprint)

Do not forget your PIN. Signing in requires the PIN (or biometrics) in addition to the authenticator itself. If you enter the wrong PIN a certain number of times, the authenticator may become locked.

1.4 How This Guide Is Organized

Chapter	Contents
Chapter 1 Introduction	Overview of FIDO logon
Chapter 2 Registering Your Authenticator	First-time registration (when required)
Chapter 3 Signing In with Your Authenticator	Day-to-day sign-in
Chapter 4 About the PIN	Setting, changing, and cautions
Chapter 5 If Something Goes Wrong	What to do when you have trouble
Appendix Glossary	Explanation of terms

Chapter 2. Registering Your Authenticator

To use FIDO logon, an authenticator must be registered to your account in advance.

How that registration happens depends on your environment. **Which of the two applies is determined by your administrator's settings.**

2.1 When Your Administrator Registers It in Advance

If your administrator has already registered an authenticator to your account, no additional registration is required. Go on to the sign-in steps in Chapter 3.

2.2 When You Register It Yourself (at First Sign-In)

If your environment is configured to require you to register, you register the authenticator at your first sign-in, **after entering your Windows password**. There is no dedicated registration screen; you continue on the usual sign-in screen.

No explanatory message appears on the first screen. When you select the tile, only a passwordbox is shown. What you enter here is your **Windows password** (not the PIN of your authenticator).

1. On the sign-in screen, select the **FIDO logon tile** for your account.

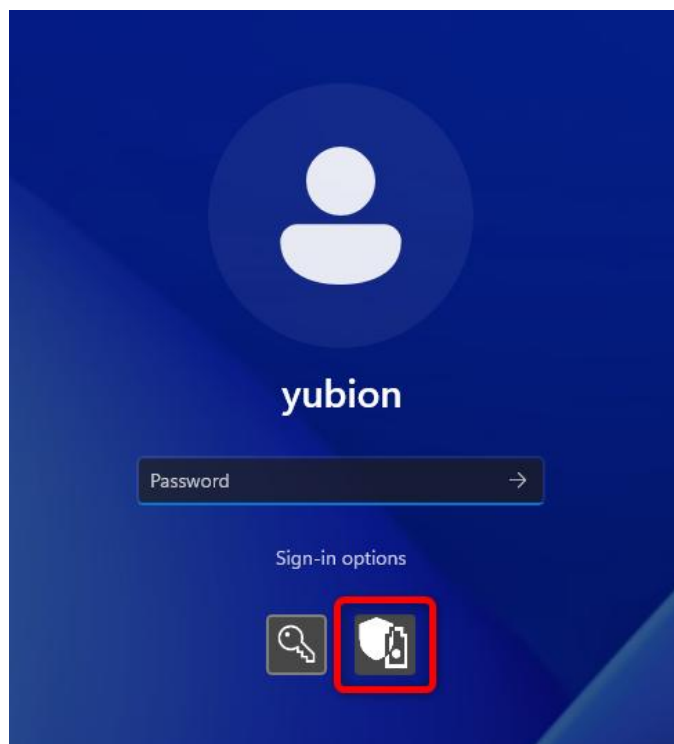


Figure: Selecting the FIDO logon tile

2. **A password box appears. Enter your Windows password** and press Enter or the arrow ("→") button. If the password is wrong, an error message appears and you are returned to the box.

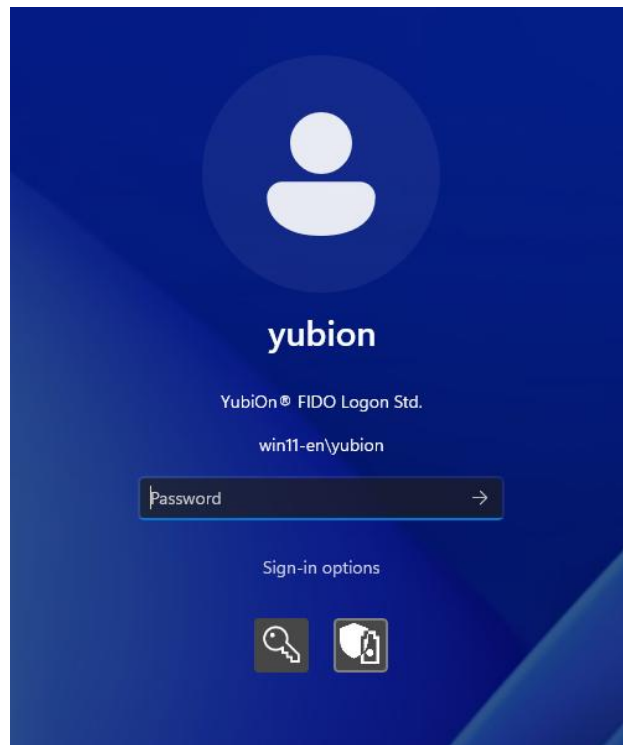


Figure: Entering the Windows password

3. Once the password is verified, "**Connect your FIDO key.**" is displayed. **Connect your authenticator** to the computer (insert it, for a USB key).

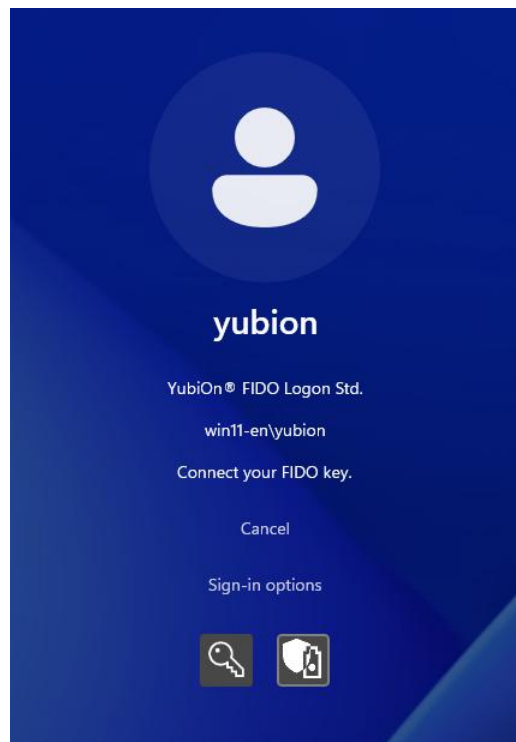


Figure: Prompt to connect the authenticator

4. If **no PIN has been set** on the authenticator, "**Set a new PIN on your authenticator.**" is displayed. Enter the new PIN (4 characters or more) and the confirmation PIN, then submit. "**Setting the PIN. Touch your FIDO key.**" is then displayed.

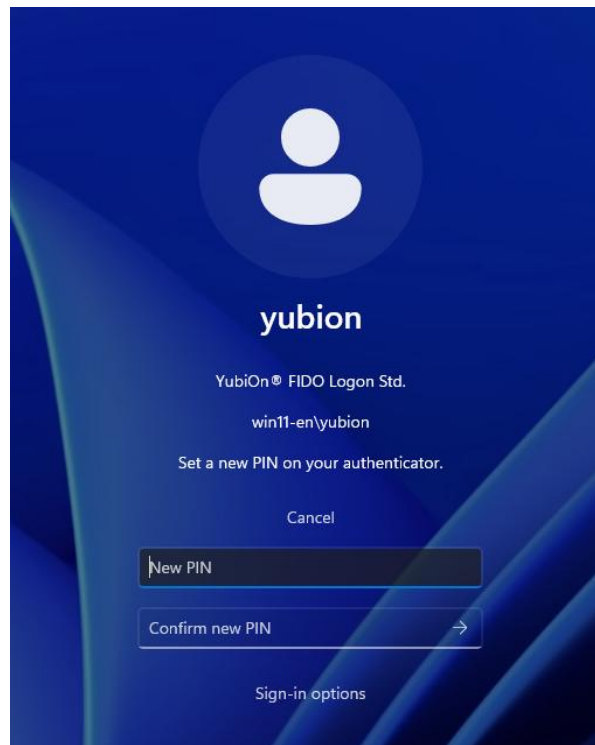


Figure: Setting a new PIN on the authenticator

5. When "**Enter the PIN for your FIDO key.**" is displayed, **enter your PIN** (if you set a PIN in step 4, enter that PIN).

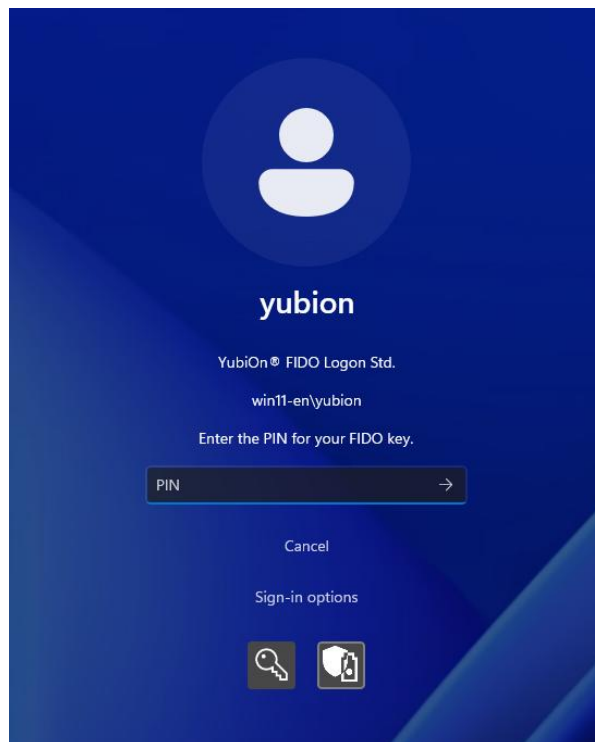


Figure: Entering the PIN

6. When "**Touch your FIDO key.**" is displayed, **touch** the authenticator.

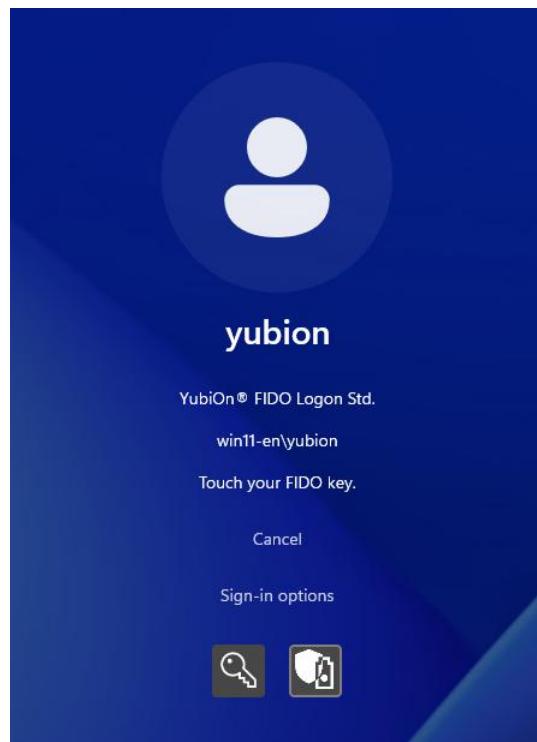


Figure: Prompt to touch the authenticator

7. When "**Touch your FIDO key once more to finish setup.**" is displayed, **touch it once more** (you do not need to re-enter the PIN).

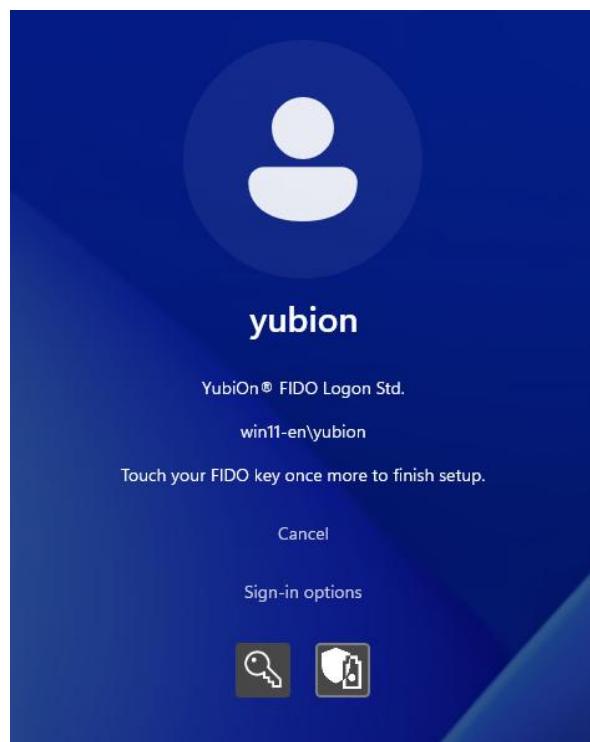


Figure: Prompt to touch the key to finish registration

8. When registration is complete, you are signed in. From the second time on, you no longer need to enter your password (depending on your administrator's settings, you may be asked for it every time).

Keep your PIN safe and do not forget it. Never tell your PIN to anyone else.

Chapter 3. Signing In with Your Authenticator

This chapter describes the basic steps for signing in to Windows with a FIDO2 authenticator.

3.1 How the Sign-In Screen Looks

Depending on your environment, the Windows sign-in screen appears in one of the following ways.

- **When authenticator logon is mandatory:** only this product's FIDO logon tile is shown.

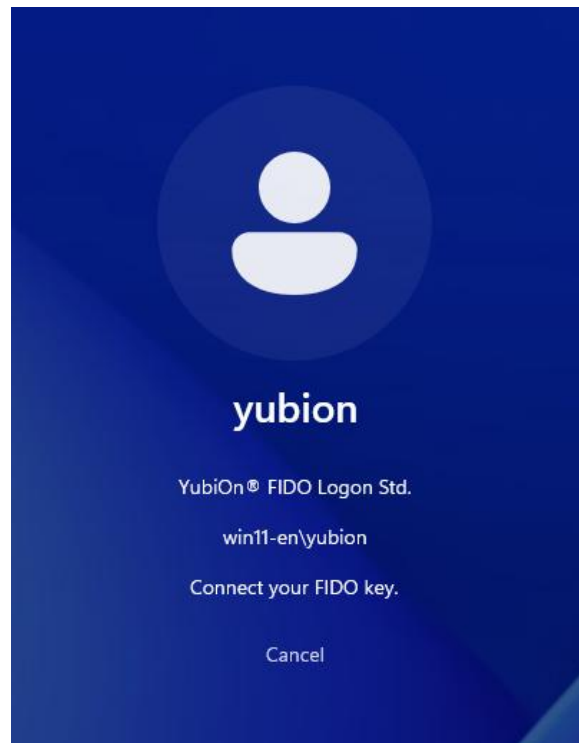


Figure: When authenticator logon is mandatory

- **Otherwise:** selecting **Sign-in options** shows the FIDO logon tile alongside the icon for the conventional password tile.

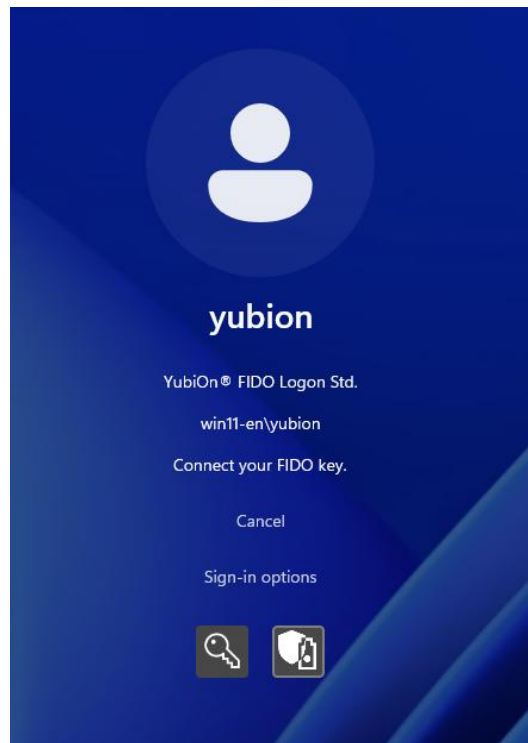


Figure: When authenticator logon is not mandatory (two or more tiles under Sign-in options)

If "No FIDO authenticator is registered for this account." is displayed no authenticator has been registered to your account. Please contact your administrator.

3.2 Signing In for the First Time

The first time, you are asked to enter your **Windows password** once, after authenticating with your authenticator.

1. On the sign-in screen, select the **FIDO logon tile** for your account. If the password tile is shown, choose the FIDO logon icon from **Sign-in options**.

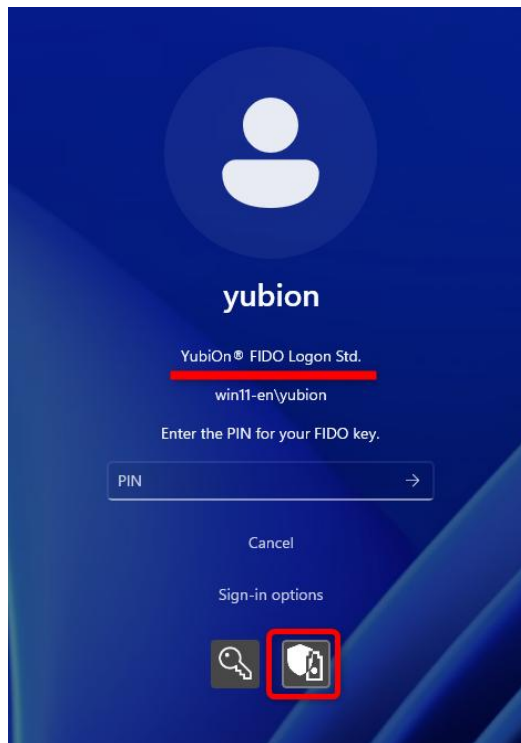


Figure: Selecting the FIDO logon tile

2. **Connect your authenticator** to the computer.
3. When "**Enter the PIN for your FIDO key.**" is displayed, enter the **PIN (or biometrics)** of your authenticator.

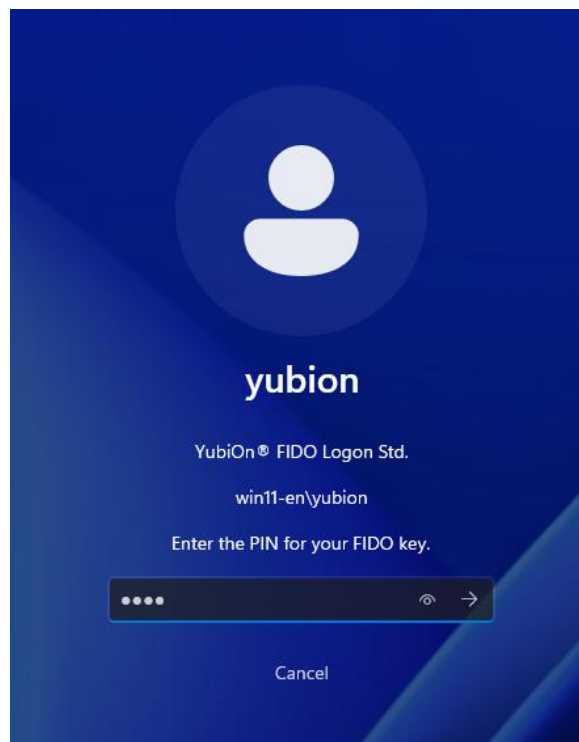


Figure: Entering the PIN

4. When "**Touch your FIDO key.**" is displayed and the authenticator starts blinking, **touch the sensor.**

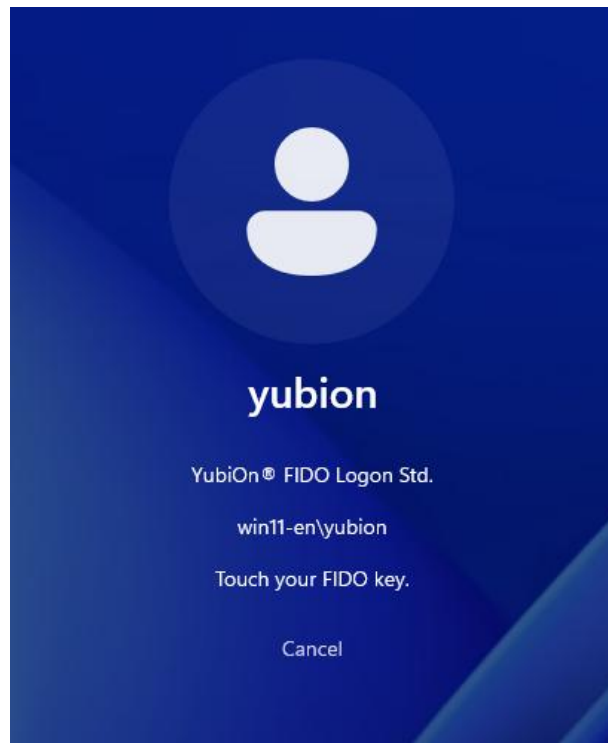


Figure: Prompt to touch the authenticator

5. When authentication succeeds, a **Windows password box** appears. Enter your password to sign in.

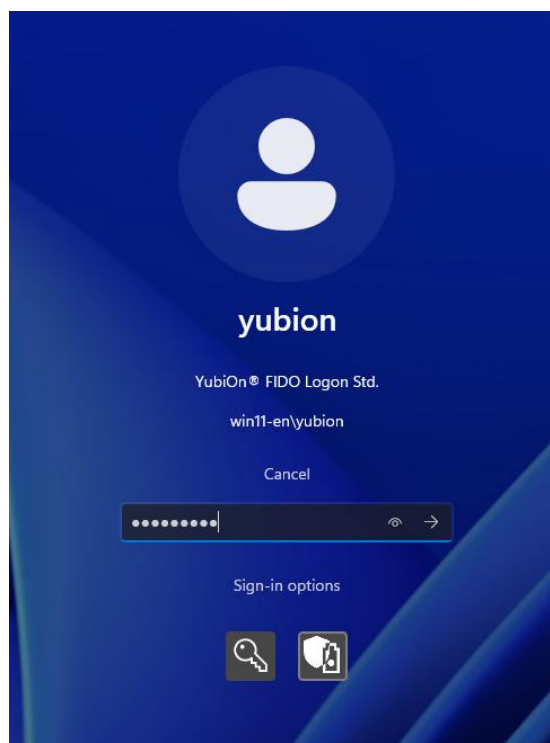


Figure: Entering the Windows password

The password you enter is stored securely on the computer (the **password cache**). **It is stored only in encrypted form and cannot be decrypted unless your authenticator is connected.**

3.3 Signing In from the Second Time On

Once your password has been stored, you no longer need to enter it.

1. Select the **FIDO logon tile**.
2. Connect your authenticator and **enter your PIN (or use biometrics)**.
3. **Touch** the authenticator.
4. When authentication succeeds, you are signed in automatically.

The flow is the same as steps 1 to 4 of the previous section, "Signing In for the First Time"; **only the final Windows password entry is gone.**

If you are asked for your password every time depending on your administrator's settings, a password may be required at every sign-in. In addition, with some authenticators (such as U2F-only keys), the password cannot be stored by design, so it must be entered every time.

3.4 Signing In over Remote Desktop (RDP)

You can also sign in with your authenticator over a Remote Desktop connection. However, where you operate the key is different.

Connect the authenticator to the computer in front of you (the client). Inserting it into the remote computer will not work. Also, **the PIN entry and the touch happen on the screen of the computer in front of you, not on the remote screen.**

1. **Connect the authenticator to the computer in front of you.**
2. Start **Remote Desktop Connection**, enter the name of the computer to connect to, and connect.
3. If you are asked for a **user name and Windows password** when connecting, enter them (this is standard Windows behavior). Authentication with your authenticator is then requested separately.
4. The **FIDO logon tile** for your account appears on the sign-in screen of the remote computer.
5. **"Operate the security key on the client side."** is displayed. The Windows security dialog (security key PIN entry) appears **on the screen of the computer in front of you**, so **enter your PIN** there.
6. **Touch** the authenticator connected to the computer in front of you.
7. When authentication succeeds, you are signed in. The first time only, you are then asked to enter your **Windows password** (the same flow as [Signing In for the First Time](#)).

If nothing appears on the computer in front of you minimize the Remote Desktop window and make sure the local screen is not hidden behind it. The security dialog appears on your local computer, not on the remote one.

When you connect from a different computer the password is cached separately for each computer you connect from, so the first time you connect from a new computer you may be asked for your Windows password again.

Note using Remote Desktop requires your administrator to prepare the environment (supported OS and Group Policy). Authenticator logon cannot be used in an environment that is not set up for it. If it does not work, please contact your administrator.

Chapter 4. About the PIN

4.1 What the PIN Is For

The PIN is the code that confirms that it is really you using the authenticator. You can sign in only when the authenticator itself and the PIN (or biometrics such as a fingerprint) are both present.

4.2 Setting and Changing the PIN

- The first time you use an authenticator that has no PIN, you are asked to set one during registration (4 characters or more).
- To change the PIN, sign in to Windows and go to **Settings** → **Accounts** → **Sign-in options** → **Security key** → **Manage**. In the **Windows Hello setup** dialog that appears, select **Change** under **Security Key PIN**.

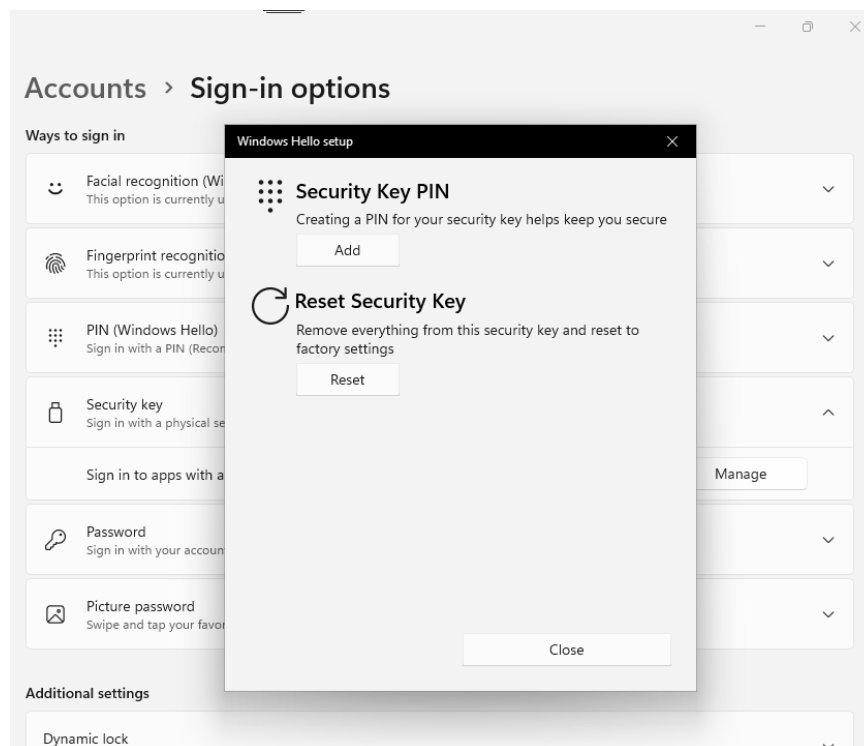


Figure: Changing the security key PIN from Windows Settings

Caution Running **Reset Security Key** on the same screen **erases everything registered on the authenticator** and you will no longer be able to sign in. Use it only when your administrator instructs you to.

4.3 Cautions About the PIN

If you enter the wrong PIN repeatedly, the authenticator stops working. This happens in two stages.

- **Stage 1 (temporary block):** after several consecutive mistakes, the key is temporarily blocked and "**PIN authentication is blocked. Remove the security key and insert it again.**" is displayed. Remove the authenticator and insert it again, and you can enter the PIN once more.

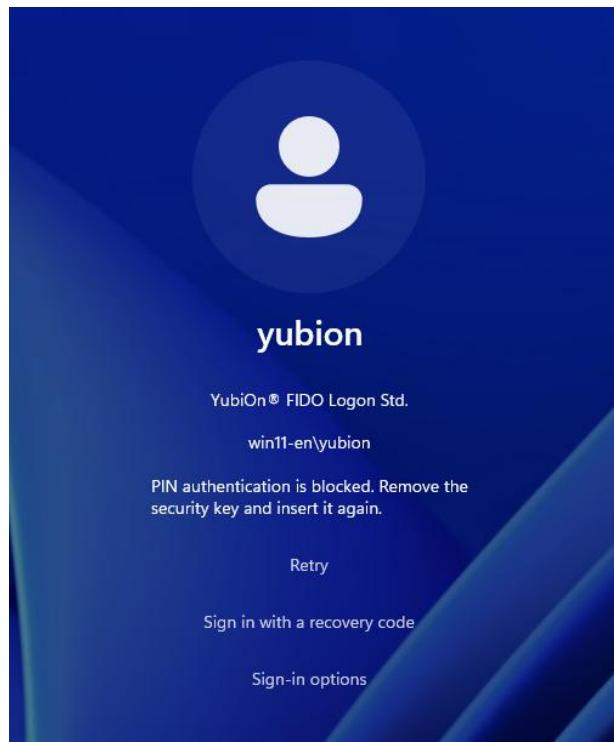


Figure: PIN authentication temporarily blocked (recovered by reinserting the key)

- **Stage 2 (permanent block):** if you keep entering the wrong PIN, the key is blocked completely and "**The PIN is blocked. Please reset the security key.**" is displayed. At that point **the authenticator cannot be used until it is reset (initialized). Resetting erases everything registered on it, so your administrator will have to register the authenticator again.**

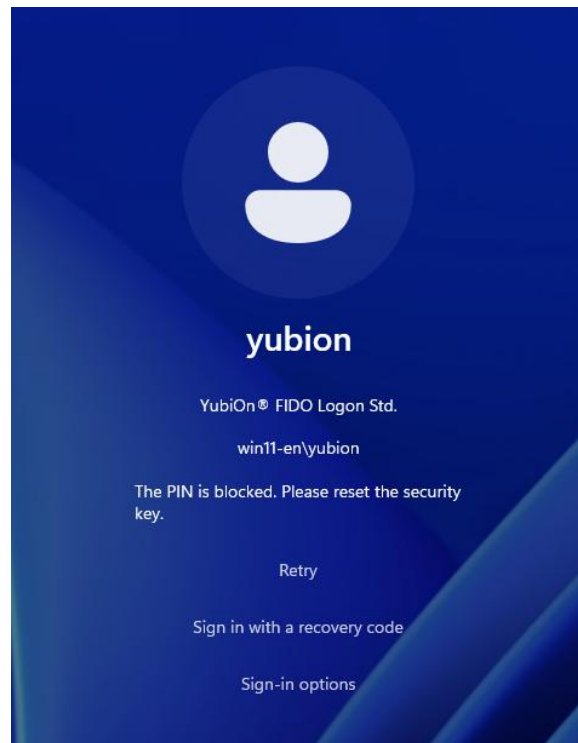


Figure: PIN blocked completely (a reset is required)

Other points to keep in mind:

- **The number of remaining attempts is not shown on screen.** If you keep guessing when you are unsure of the PIN, the key can become unusable before you realize it. Stop trying as soon as you are unsure, and consult your administrator.
- Do not tell your PIN to anyone, and choose one that is hard to guess. **Be careful not to forget it.**

Check this in advance in case your authenticator stops working, it is reassuring to confirm beforehand whether **a spare authenticator is registered** for you, or whether **you have a recovery code** at hand. If you have neither, consult your administrator.

Chapter 5. If Something Goes Wrong

5.1 You Forgot or Lost Your Authenticator

- **You cannot sign in without your authenticator.** If you do not have it with you, you may be able to sign in for an emergency using a **recovery code** issued by your administrator (see below).
- **If you lost it, contact your administrator immediately.** The administrator will disable the authenticator to prevent misuse.

5.2 You Forgot the PIN, or the Authenticator Is Locked

First, check the message shown on the sign-in screen.

- **"PIN authentication is blocked. Remove the security key and insert it again."**
→ Remove the authenticator and insert it again, and you can enter the PIN once more.
- **"The PIN is blocked. Please reset the security key."**
→ That authenticator **cannot be used until it is reset**. Resetting it yourself erases everything registered on it and requires re-registration, so **contact your administrator first**.

The ways to sign in are as follows.

- If a **spare authenticator** is registered for you, you can sign in with that.
- If you have a **recovery code**, you can sign in for an emergency by following [Signing In with a Recovery Code \(Emergency\)](#) below.
- If you have neither, **contact your administrator** (the administrator may be able to sign in on your behalf).

5.3 Signing In with a Recovery Code (Emergency)

When your authenticator cannot be used, you can sign in for an emergency with a **recovery code** issued by your administrator.

1. Select the **FIDO logon tile** and attempt FIDO authentication.
2. When authentication fails or is canceled, a **Sign in with a recovery code** link appears in the tile.

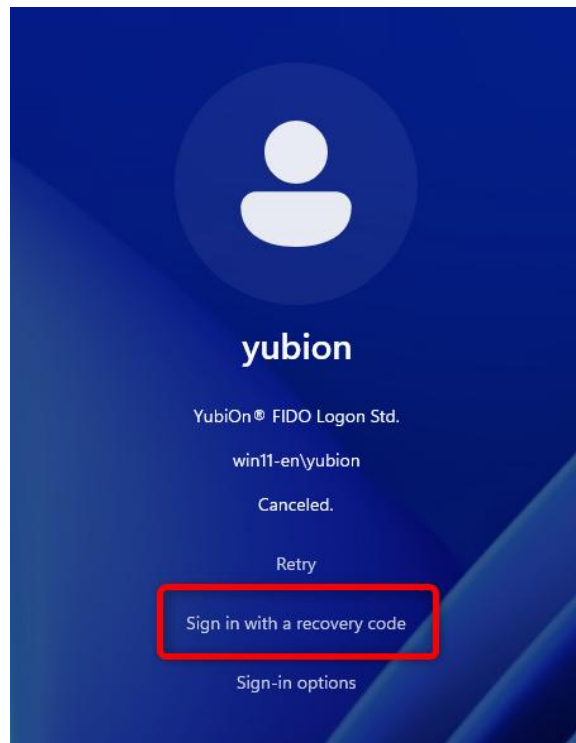


Figure: The "Sign in with a recovery code" link

3. Select the link and **enter the recovery code** you were given (in XXXX-XXXX-XXXX-XXXX format).

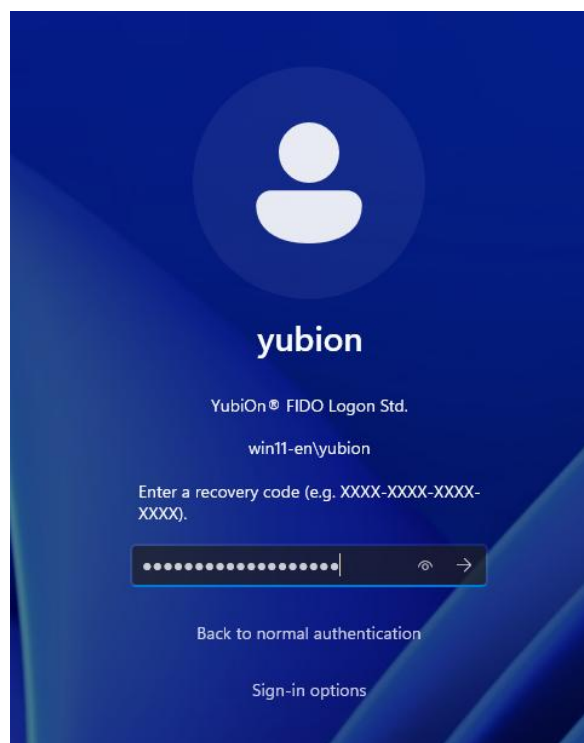


Figure: Entering the recovery code

4. When "**Recovery code verified. Enter your Windows password.**" is displayed, **enter your Windows password** to sign in.

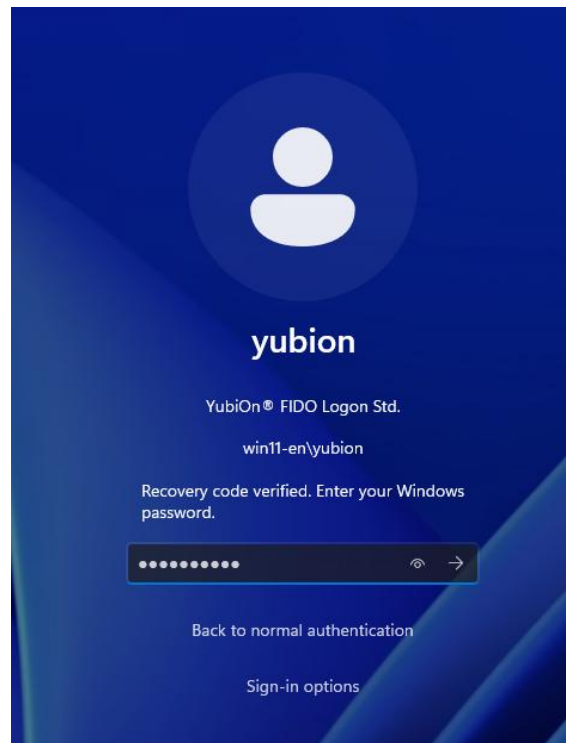


Figure: Entering the password after the recovery code is verified

Caution Each recovery code can be used **only once**. A recovery code alone is not enough to sign in; your Windows password is always required as well. If you have used them all or lost them, ask your administrator to issue new ones.

5.4 The Screen Locked When You Removed the Authenticator

Depending on your administrator's settings, **removing the authenticator may lock the screen automatically**. This is a safety feature. To sign in again, connect the authenticator and go through the sign-in steps.

5.5 The FIDO Tile Does Not Appear on the Sign-In Screen

- Check that the authenticator is properly connected.
- If it still does not appear, contact your administrator (the cause may be the license or the settings).

Appendix Glossary

Term	Description
FIDO2 authenticator	A security key such as a YubiKey. Used to sign in.
PIN	The code you enter when using the authenticator (4 characters or more).
Touch	Touching the sensor on the authenticator to confirm that a person is present.
Password cache	A mechanism that securely stores the Windows password you entered once on the computer, so that you do not have to enter it again.
Recovery code	An emergency sign-in code for use when the authenticator cannot be used. Issued by the administrator.
Security key	Another name for a FIDO2 authenticator. This is the term used in the Windows Settings screens.

Contact

If you have trouble using this product, please contact **your organization's system administrator** first.

Item	Contents
Product information	https://www.yubion.com/
Manufacturer	SOFTGIKEN Co., Ltd. (https://sgk.co.jp/)