



YubiOn FIDO Logon Standalone

Quick Start Guide for Administrators



SOFTGIKEN Co., Ltd.

August 2026 Edition

Contents

Contents.....	2
About This Guide.....	3
Overall Flow	3
What to Prepare.....	3
STEP 1: Install the Product	5
STEP 2: Register the License.....	6
Start the Settings Tool	6
Register the License File.....	6
STEP 3: Register a Master Key	10
STEP 4: Assign an Authenticator to a User	13
STEP 5: Issue Recovery Codes	17
STEP 6: Enable Authenticator Logon	19
STEP 7: Try Signing In	20
STEP 8: Enable Secure Mode.....	23
If Something Goes Wrong	25
The FIDO Logon Tile Does Not Appear on the Sign-In Screen	25
An Authenticator Cannot Be Registered (Assigned) in the Settings Tool	25
The License Shows "Machine Mismatch" or "OS Edition Mismatch"	25
An Authenticator Was Lost, or the PIN Was Forgotten or Locked.....	25
What to Read Next	26
Contact	26

About This Guide

This guide describes the shortest single path for **installing YubiOn FIDO Logon Standalone** (hereafter "this product") **on one computer and getting it to the point where you can sign in to Windows with an authenticator** (a FIDO2 security key such as a YubiKey).

- **Estimated time:** about 30 minutes (if you already have the license file)
- **Audience:** administrators trying this product for the first time
- **Assumed knowledge:** operating Windows with administrator privileges

Optional settings, operational design, and detailed specifications are not covered. For those, see the separate **Administrator Manual**. The end of each STEP points to the corresponding chapter.

Overall Flow

STEP	Contents
STEP 1	Install the product
STEP 2	Register the license
STEP 3	Register a master key
STEP 4	Assign an authenticator to a user
STEP 5	Issue recovery codes
STEP 6	Enable authenticator logon
STEP 7	Try signing in
STEP 8	Enable secure mode

About the order of the STEPs STEP 3 (master key) and STEP 5 (recovery codes) are done before authenticator logon is enabled. This is because STEP 6 cannot be completed while no authenticator exists, and because you must not lose every means of signing in if all authenticators become unusable. **Follow the steps in order.**

What to Prepare

Item	Notes
A computer running a supported OS	Windows 10 (20H2 or later) / Windows 11 / Windows Server 2022 or later
The MSI installer	The server edition and the client edition are separate files. Obtain the one that matches the OS type of the computer

Item	Notes
A license file	If you do not have one yet, obtain the machine code in STEP 2 and request a license from the issuer
A FIDO2 authenticator	Any FIDO2-capable authenticator can be used, not only a YubiKey
Administrator privileges	Required to install the product and to operate the settings tool

Note This guide assumes use at the local console (signing in directly at the computer). FIDO logon over RDP has additional requirements; see Chapter 2 of the Administrator Manual.

STEP 1: Install the Product

1. Run the **MSI installer** that matches the OS type.
2. Follow the on-screen instructions to complete the installation.
3. When installation finishes, the Windows service YubiOnFidoStandaloneService starts automatically.

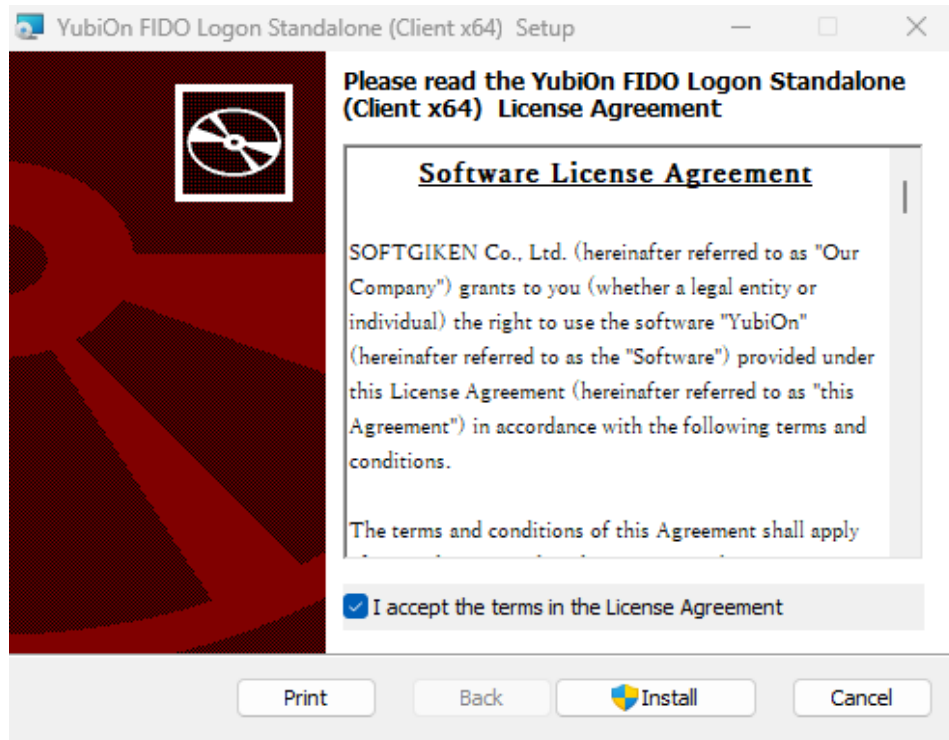


Figure: The MSI installer wizard

If **"Windows protected your PC" appears** this is the standard Microsoft Defender SmartScreen confirmation screen. Select **More info** and then **Run anyway** to continue.

At this point FIDO logon is not yet enabled. Continue to STEP 2.

For details, see Chapter 3 "Installation" of the Administrator Manual.

STEP 2: Register the License

A valid license is required for this product to work. FIDO logon does not work while the license is not valid.

Start the Settings Tool

Everything from STEP 2 on is done in the **settings tool**.

1. On the Start menu, open **All apps** and select **YubiOn FIDO Logon Standalone Settings Tool**.
2. Select **Yes** in the User Account Control (UAC) prompt.

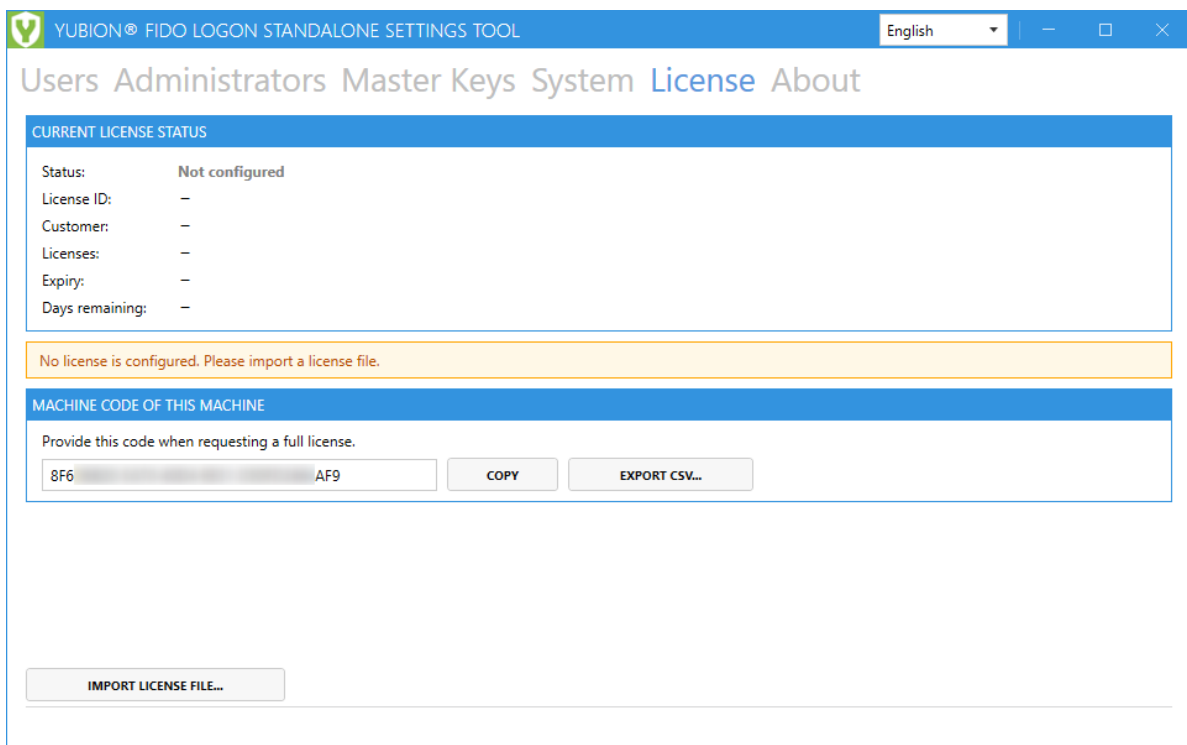


Figure: The main window of the settings tool

Register the License File

1. Open the **License** tab.

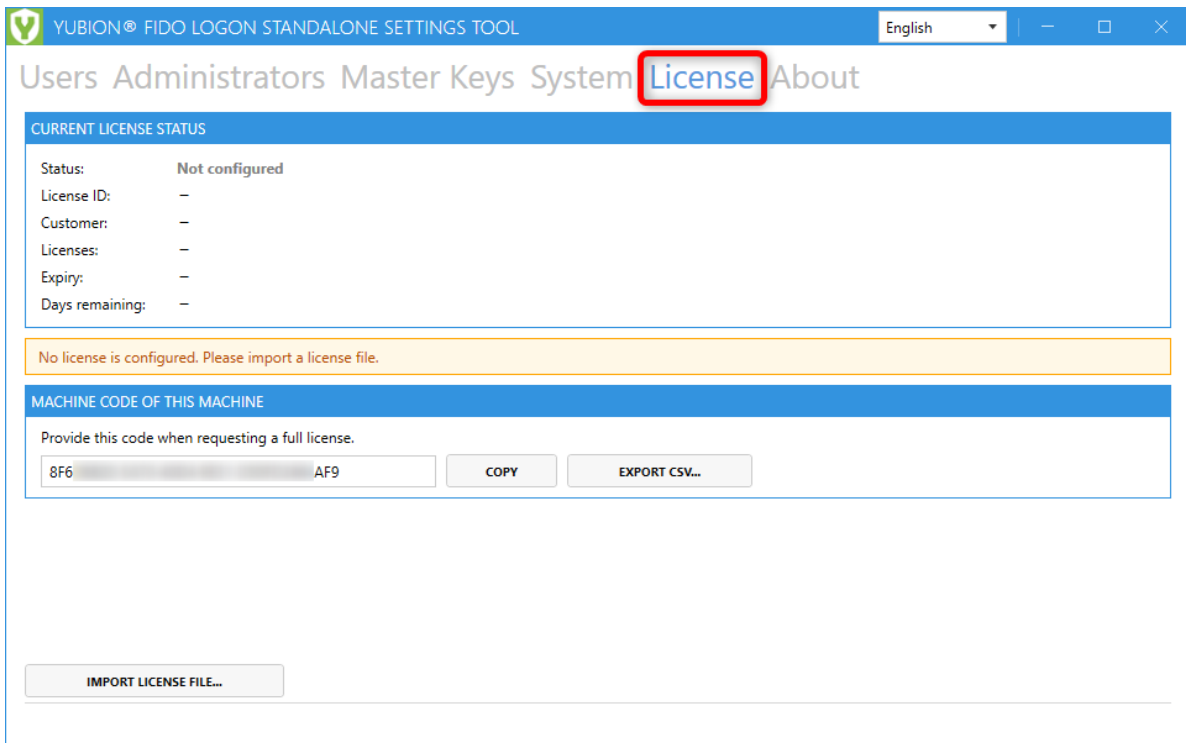


Figure: The License tab

- If you do not have a license file yet, obtain the value in **Machine Code of This Machine** with **Copy**, and submit it to the license issuer to request a license.

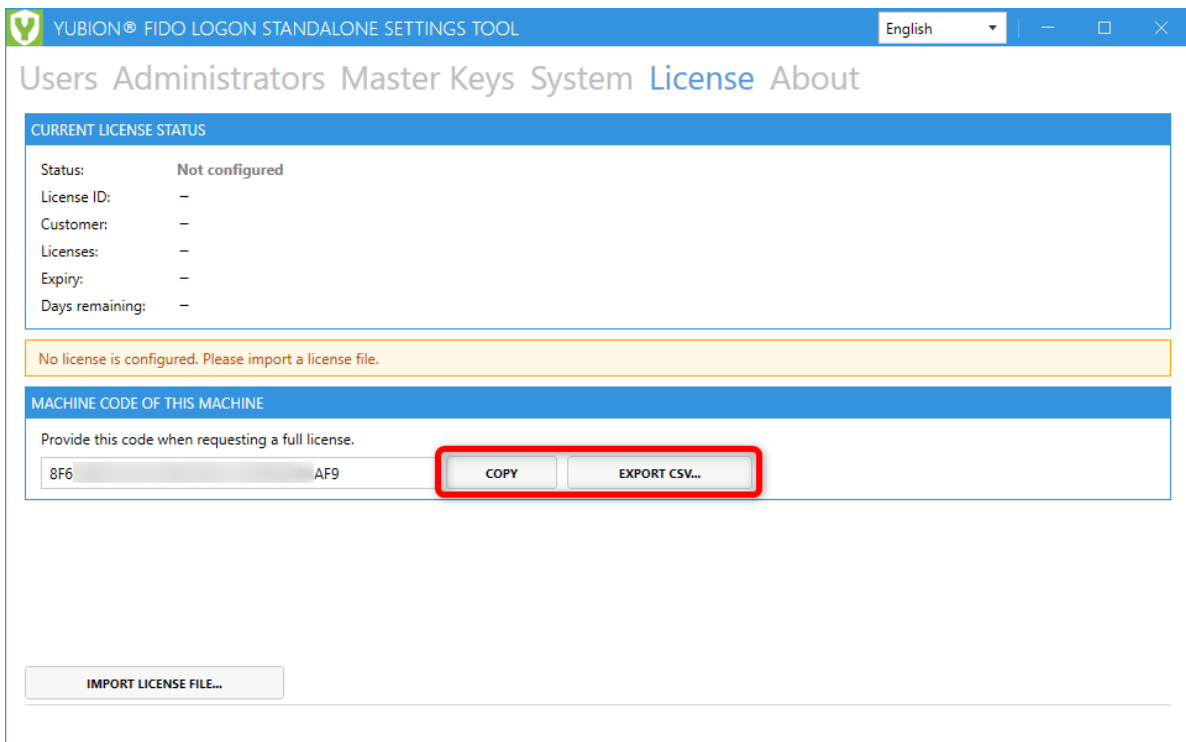


Figure: The button for copying the machine code

- Select **Import License File...** and specify the license file you received.

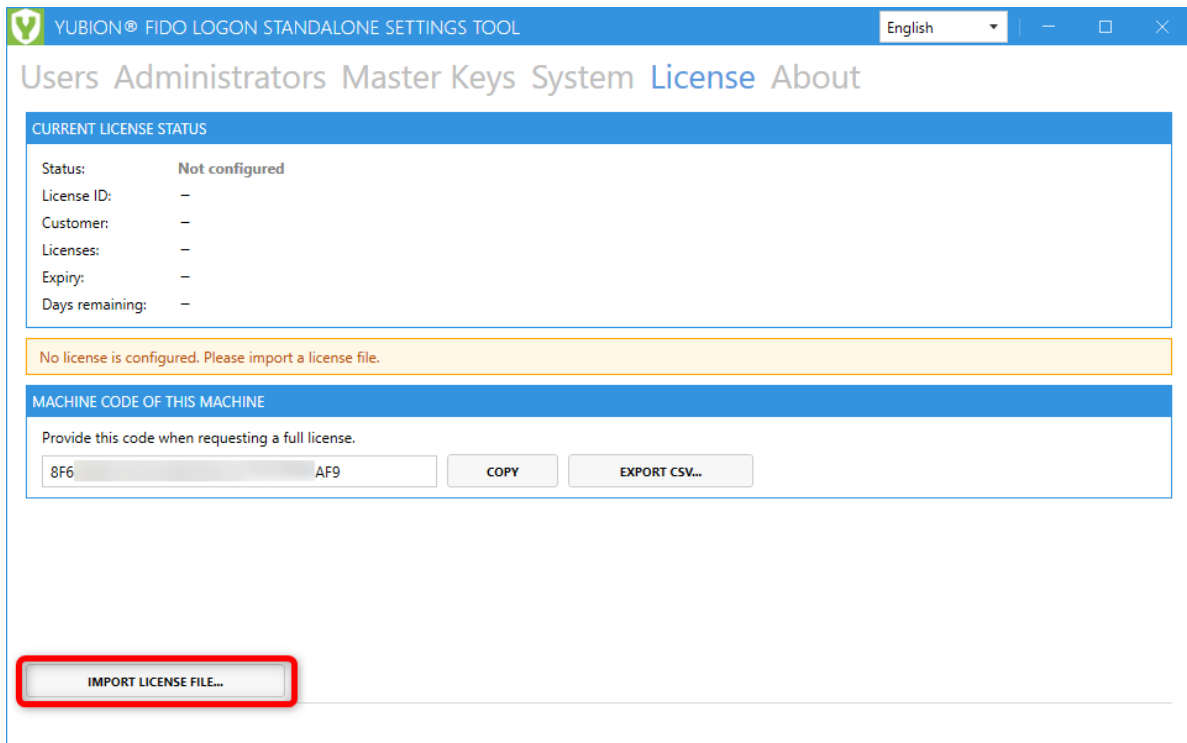


Figure: The Import License File button

4. Confirm that the license status becomes **Valid**.

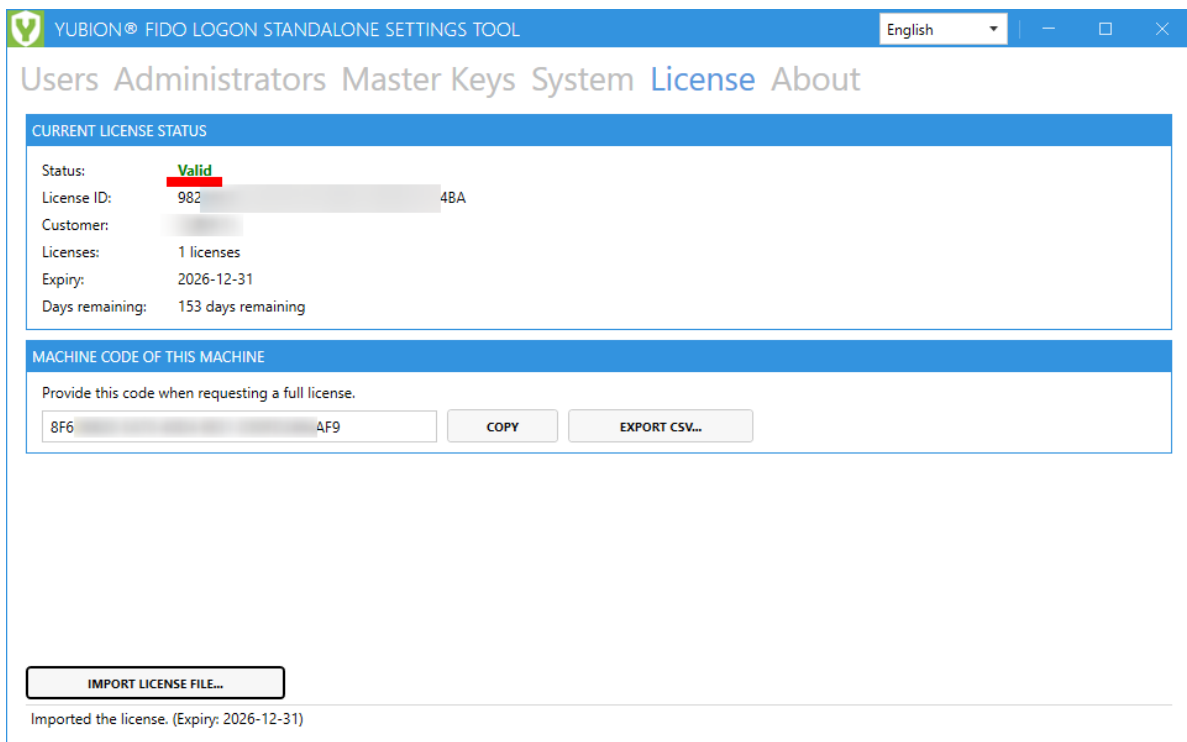


Figure: The license activated

If the license cannot be imported a license is tied to both the **computer (machine code)** and the **OS type (server / client)**. If **Invalid (machine mismatch)** or **Invalid (OS edition mismatch)** is shown, check that the file was issued for this computer and that the OS type matches.

For details, see Chapter 5 "Registering the License" of the Administrator Manual.

STEP 3: Register a Master Key

A **master key** is an administrator authenticator that **can sign in to any Windows account**, regardless of assignment. It is your fallback when a user's authenticator breaks, is lost, or becomes PIN-locked.

Registering one here also satisfies the prerequisite for STEP 6, "Enable authenticator logon" (at least one authenticator usable for signing in must exist).

1. Open the **Master Keys** tab.

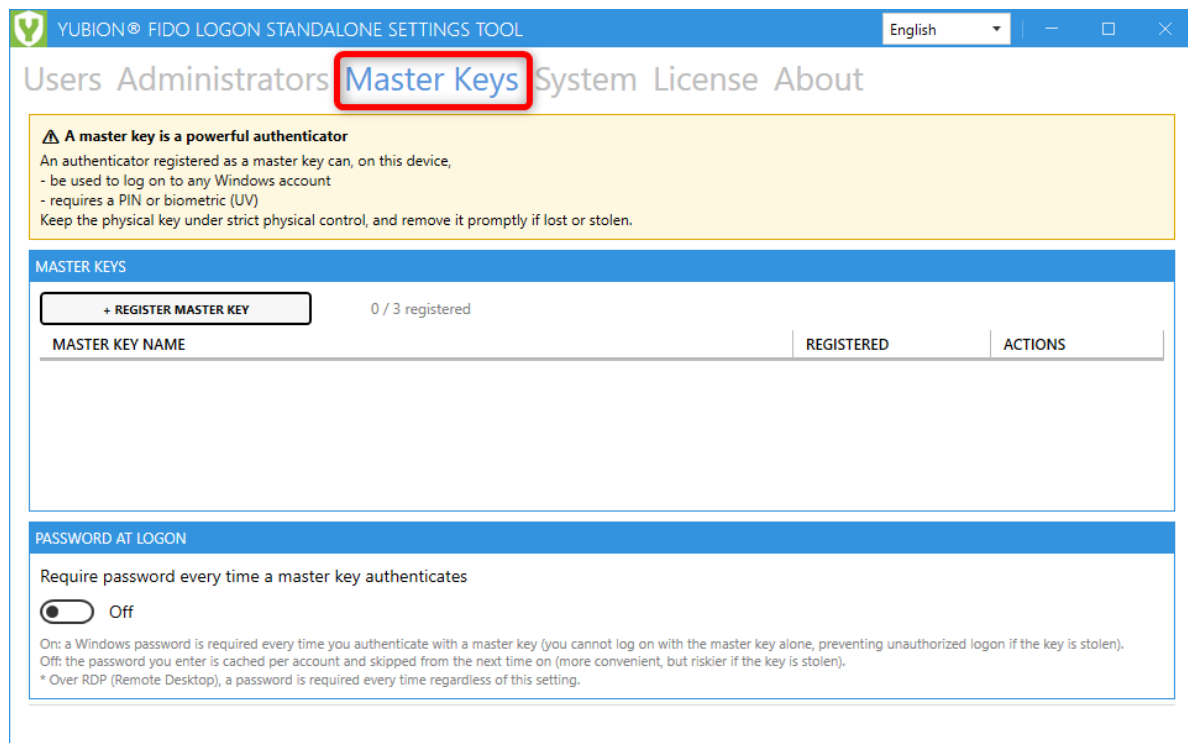


Figure: The Master Keys tab

2. Select **+ Register Master Key**.

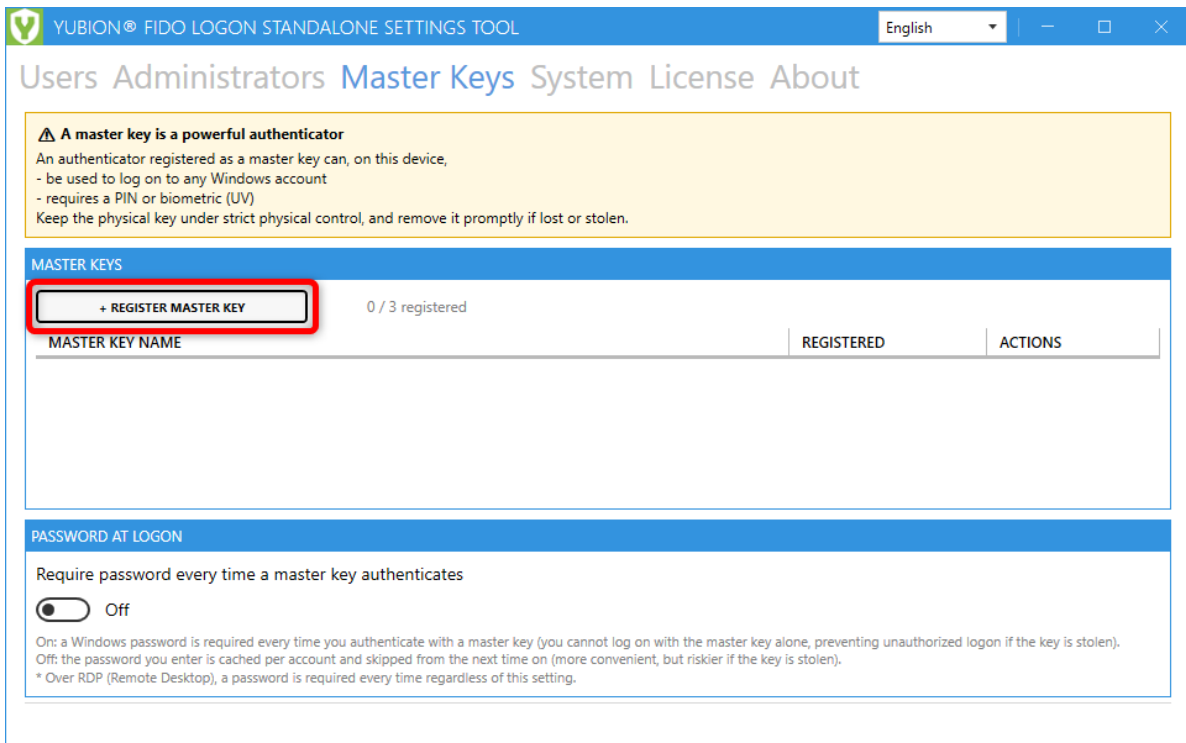


Figure: Selecting the "+ Register Master Key" button

3. In the confirmation dialog stating that the key can sign in to any Windows account, select **Yes**.

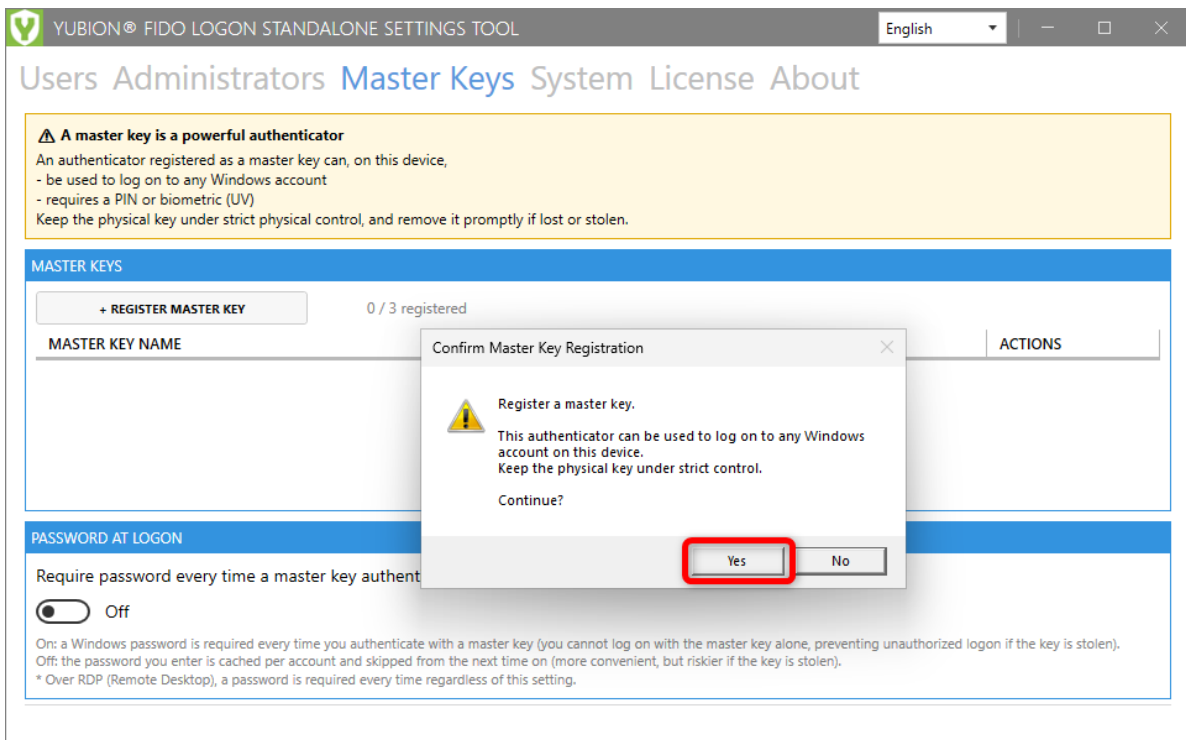


Figure: The master key registration confirmation dialog

4. Connect the authenticator, enter the PIN (or use biometrics), and touch the authenticator. If the authenticator has no PIN, you are asked to set one here (4 characters minimum).

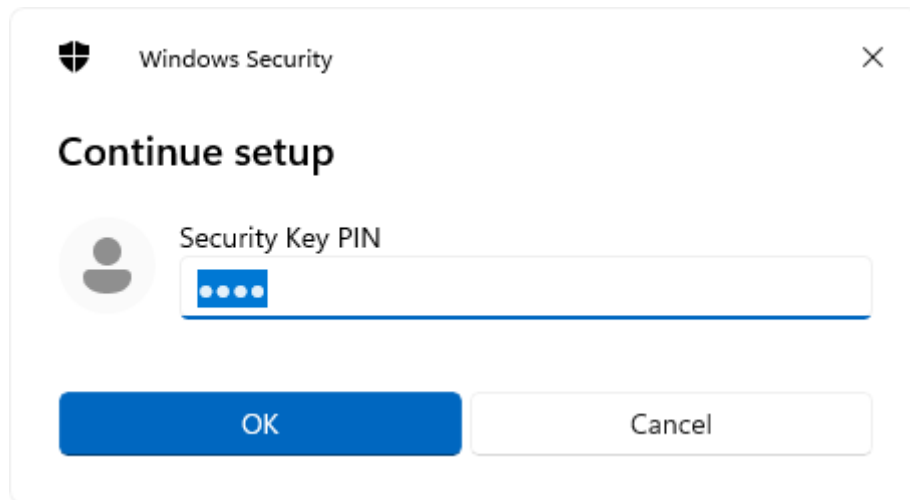


Figure: The PIN entry dialog

5. In the name dialog, enter a name that is easy to manage (for example, Admin YubiKey). Registration is complete when it is added to the master key list.

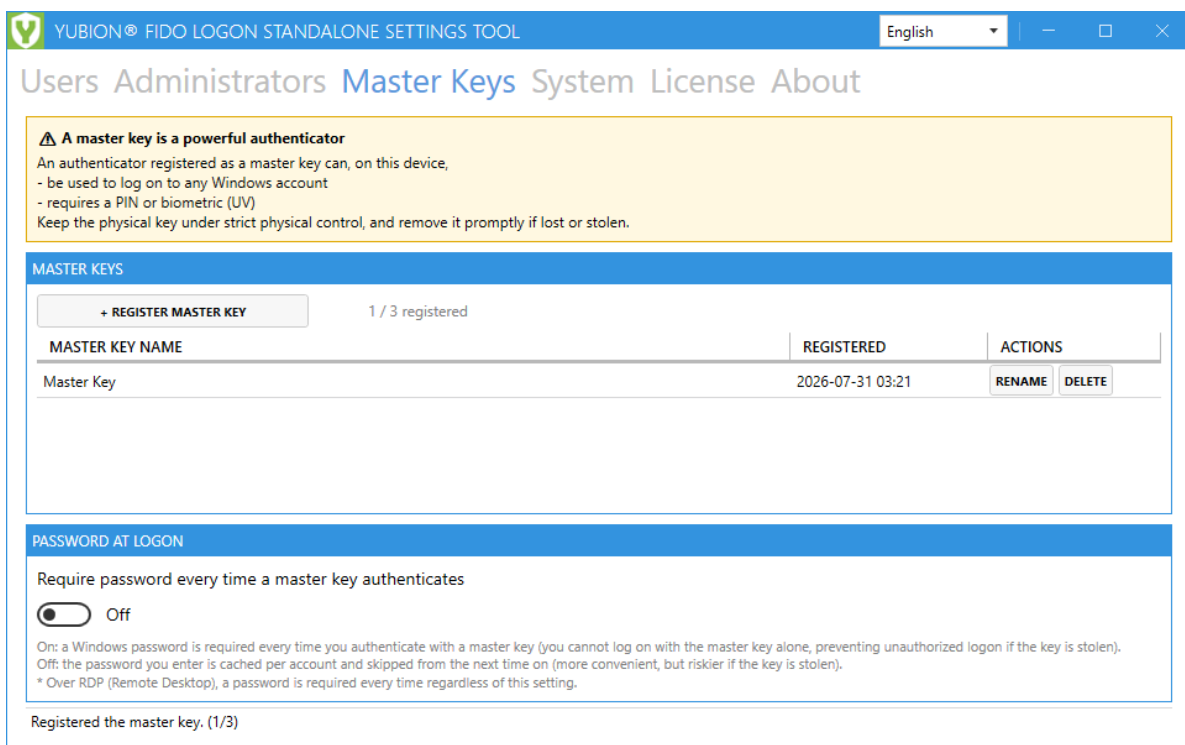


Figure: The master key added to the list

Caution A master key is a powerful key that can sign in to any account. **Keep it under personal physical control and do not share it.** If it is lost, delete it from the settings tool promptly.

For details, see Chapter 9 "Managing Master Keys" of the Administrator Manual.

STEP 4: Assign an Authenticator to a User

The administrator registers, in advance, the authenticator a user will use for FIDO logon. **Start by registering one for your own account to verify the behavior.**

1. Open the **Users** tab.

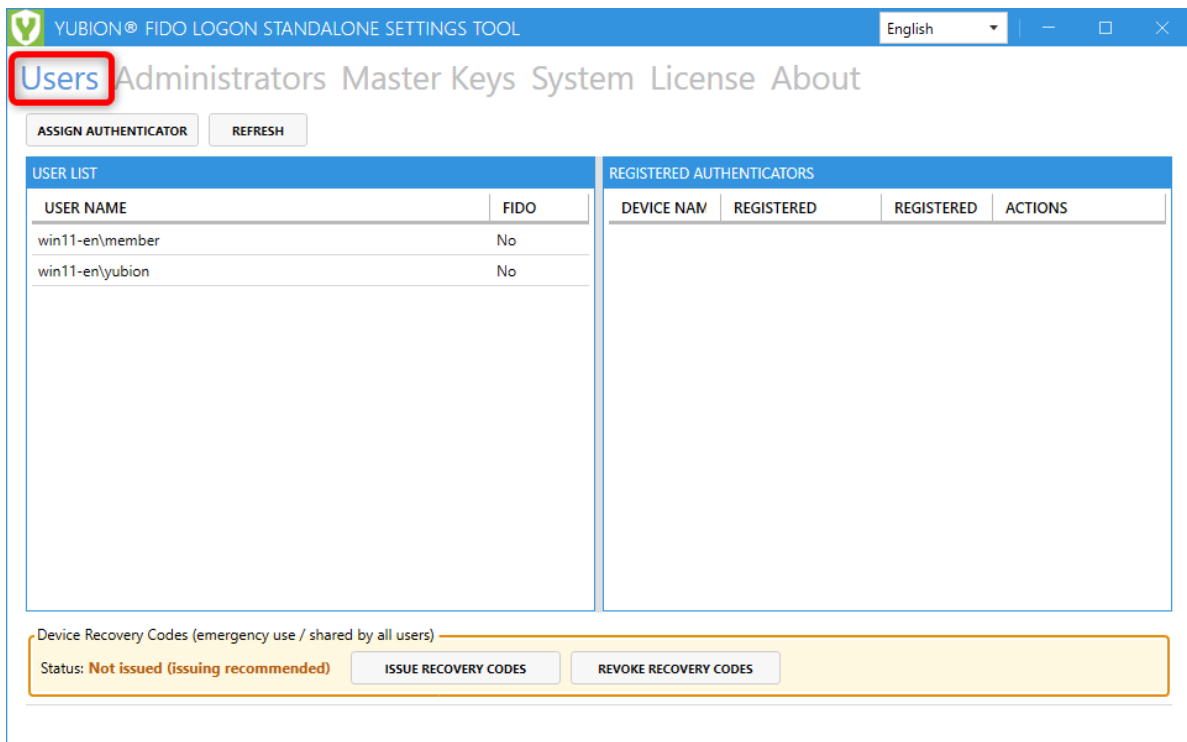


Figure: The Users tab

2. Select the target Windows account.

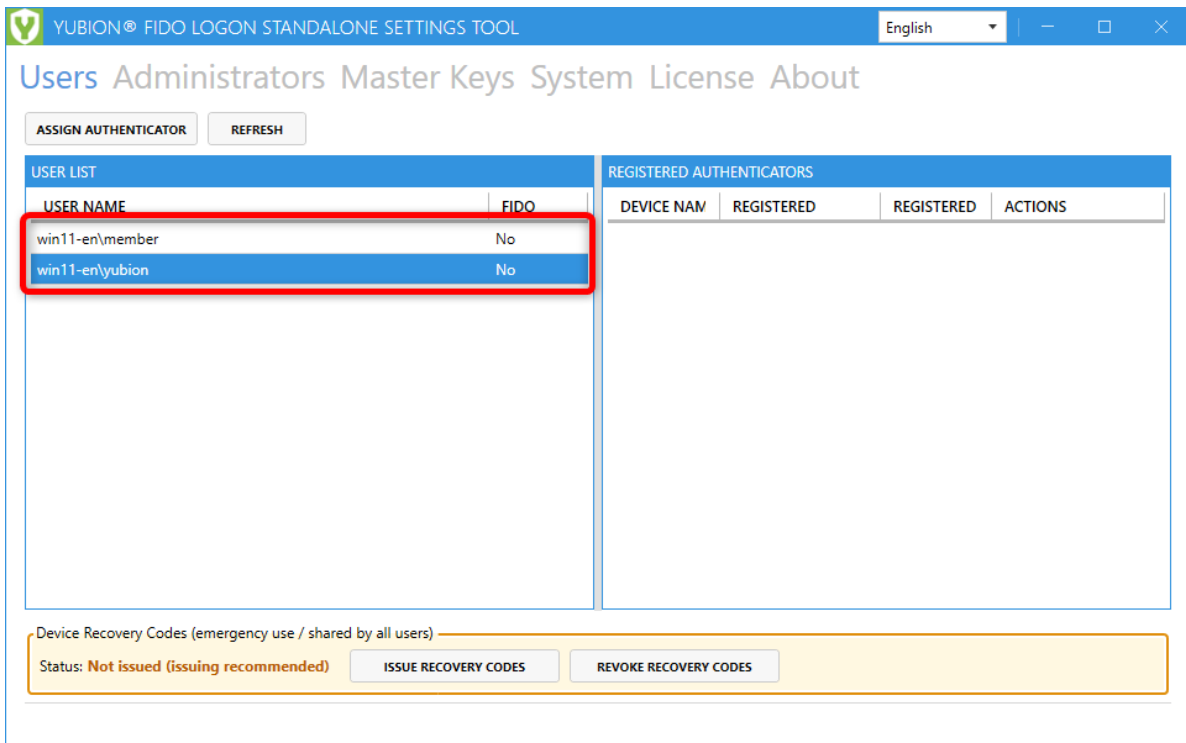


Figure: Selecting the target Windows account

3. Select **Assign Authenticator**.

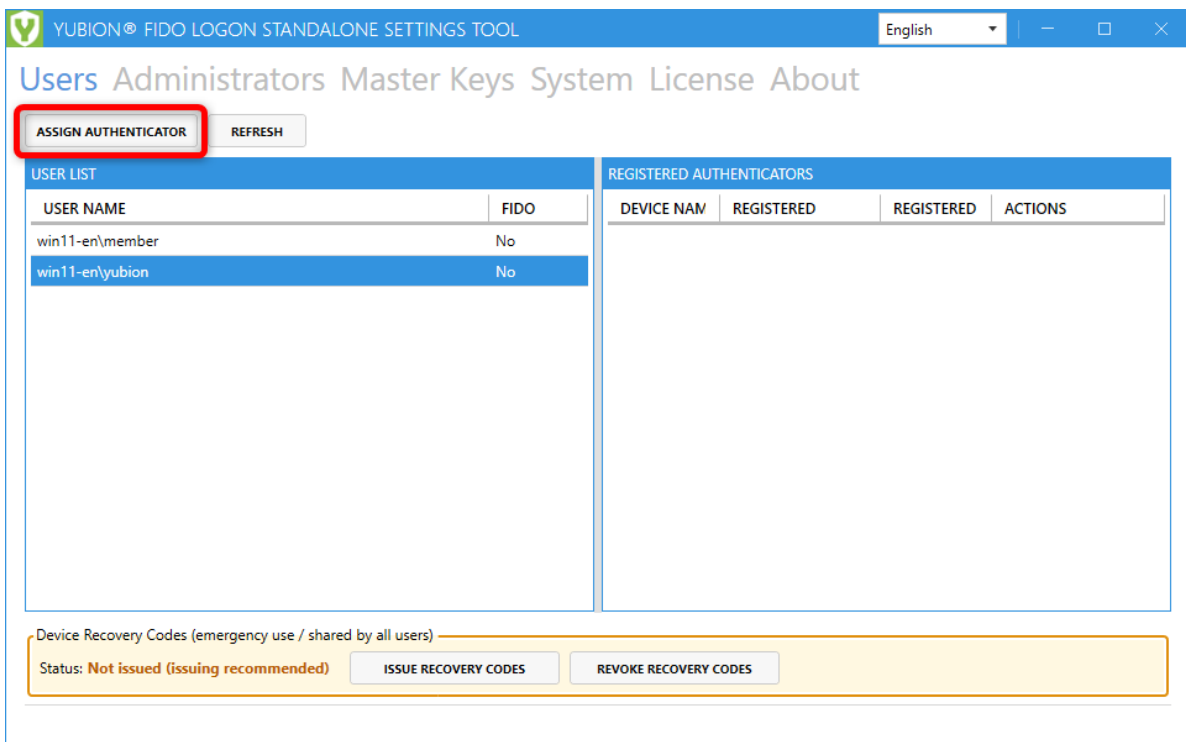


Figure: Selecting the "Assign Authenticator" button

4. Connect the authenticator, enter the PIN (or use biometrics), and touch the authenticator.

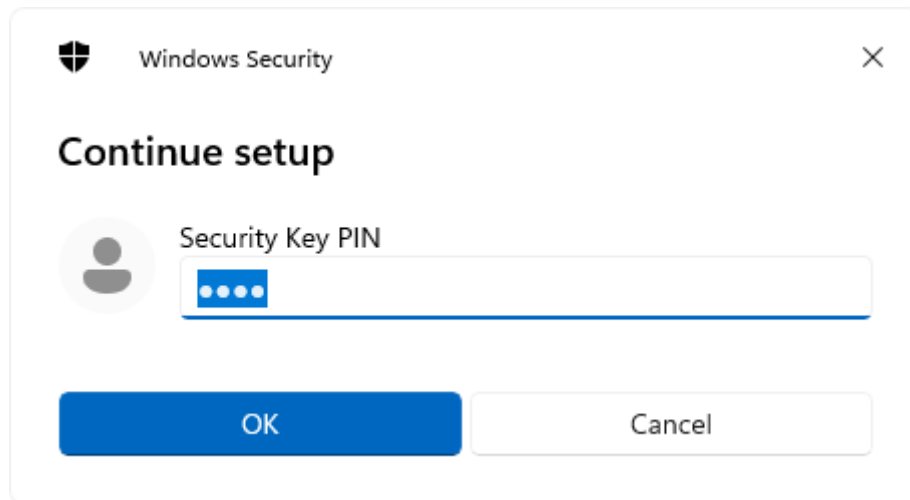


Figure: The PIN entry dialog

5. In the name dialog, enter a name (for example, YubiKey5-NFC). Registration is complete when it is added to the **Registered Authenticators** list.

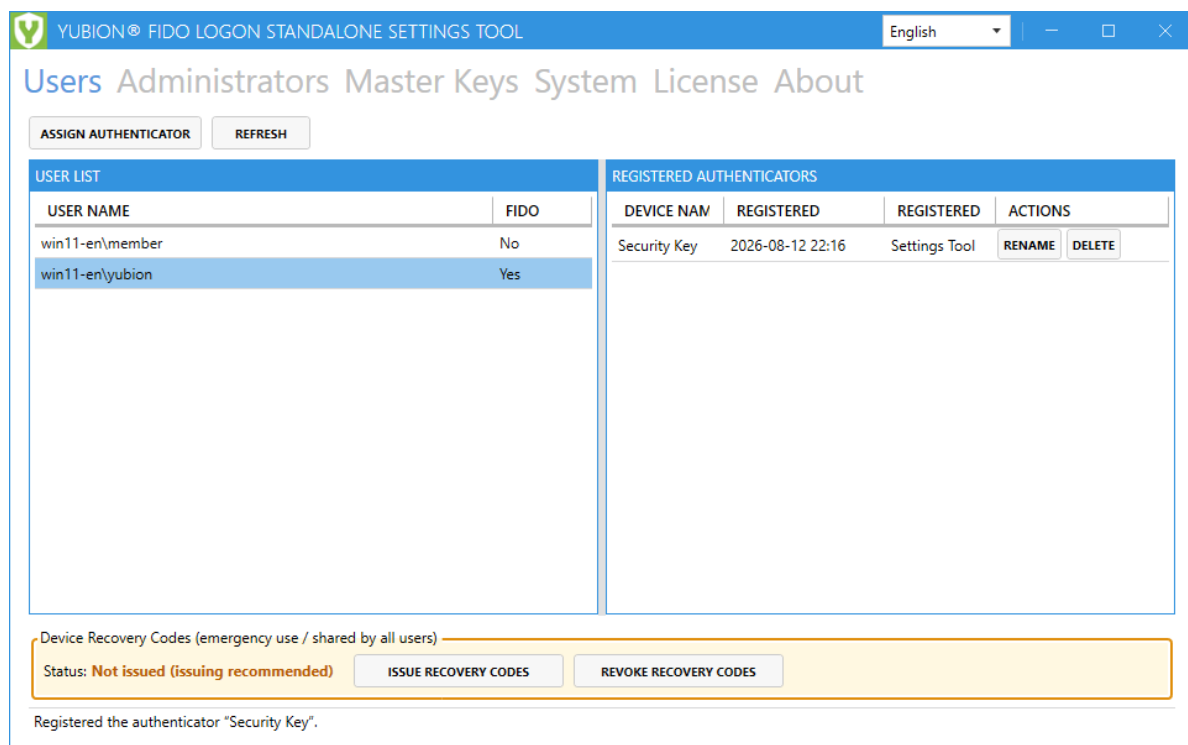


Figure: The authenticator added to the Registered Authenticators list

If the target user is not in the list the list shows only accounts that already have a **user profile** on that computer (accounts that have signed in at least once). Have the user sign in once first.

Note Account names appear in the list in the following formats, depending on the account type.

- **Local account:** ComputerName\AccountName
- **Microsoft account:** MicrosoftAccount\AccountName
- **Active Directory account:** DomainName\AccountName
- **Entra ID (Azure AD) account:** AzureAD\EmailAddress

For details, see Chapter 8 "Registering and Managing User Authenticators" of the Administrator Manual. The same chapter also describes self-registration, where users register their own authenticator at first sign-in.

STEP 5: Issue Recovery Codes

Recovery codes are the only way to sign in for an emergency **without using an authenticator at all**. An authenticator locks after repeated wrong PIN entries, and this product cannot detect that lock. If every registered authenticator and master key becomes unusable and no recovery codes have been issued, **you will not be able to sign in, and no settings change can restore access**.

Important Issuing recovery codes must be treated as a **mandatory step when deploying a computer**.

1. At the bottom of the **Users** tab, in the **Device Recovery Codes (emergency use / shared by all users)** group, select **Issue Recovery Codes**.

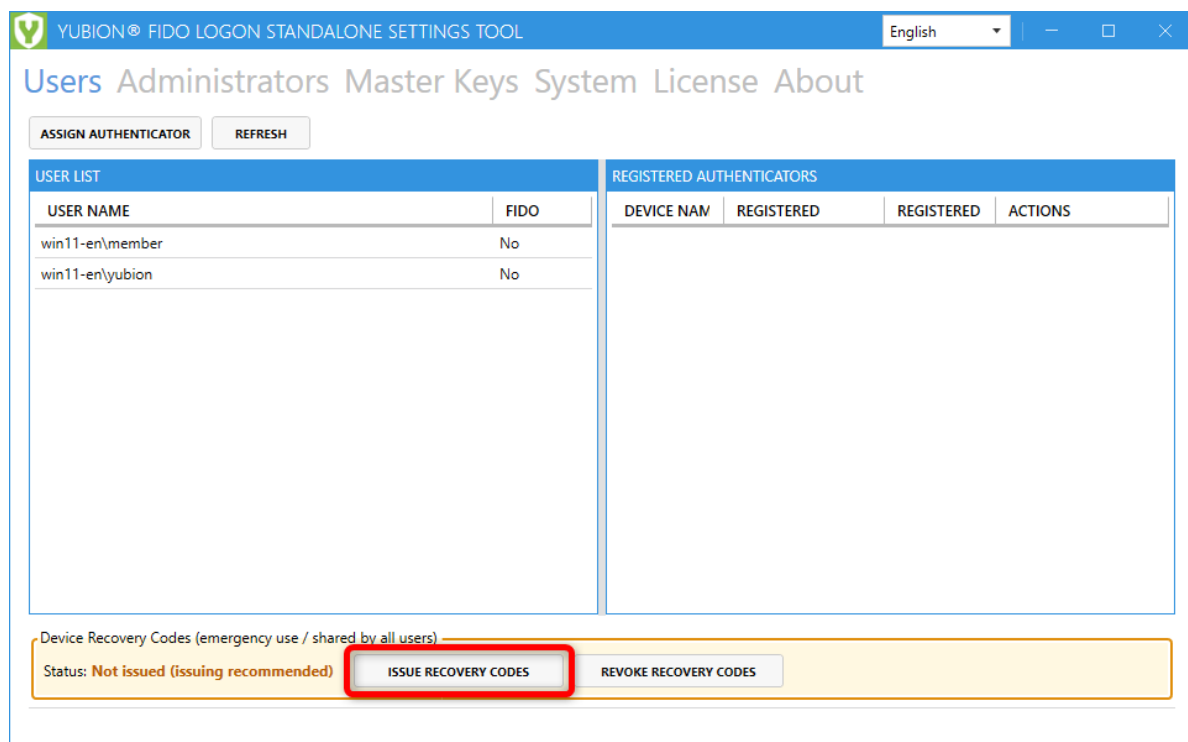


Figure: The Issue Recovery Codes button

2. **Store the 10 codes that are displayed in a safe place**, using **Copy to Clipboard** or **Save to Text File**.

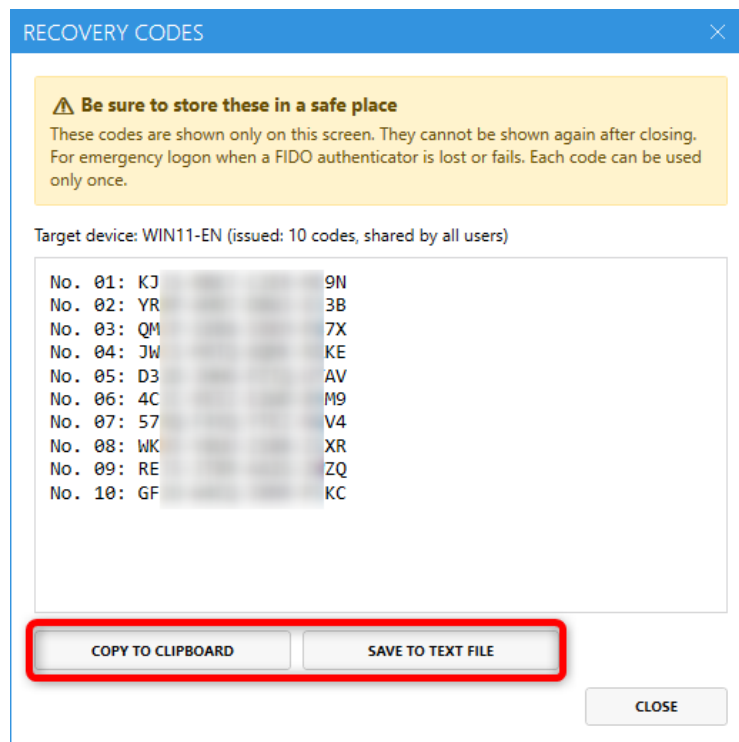


Figure: The recovery code dialog

The codes are shown only once, right after they are issued. They cannot be shown again after you close the dialog. Be sure to store them at this point.

- Recovery codes are issued **per computer (shared by all users)**, 10 at a time. Each code can be used only once.
- A recovery code alone is not enough to sign in. **The Windows password is required as well.**

For details, see Chapter 10 "Managing Recovery Codes" of the Administrator Manual.

STEP 6: Enable Authenticator Logon

Now apply what you have configured so far to the actual sign-in screen.

1. Open the **System** tab.
2. Turn on **Enable authenticator logon (add this product's CP to sign-in options)**.

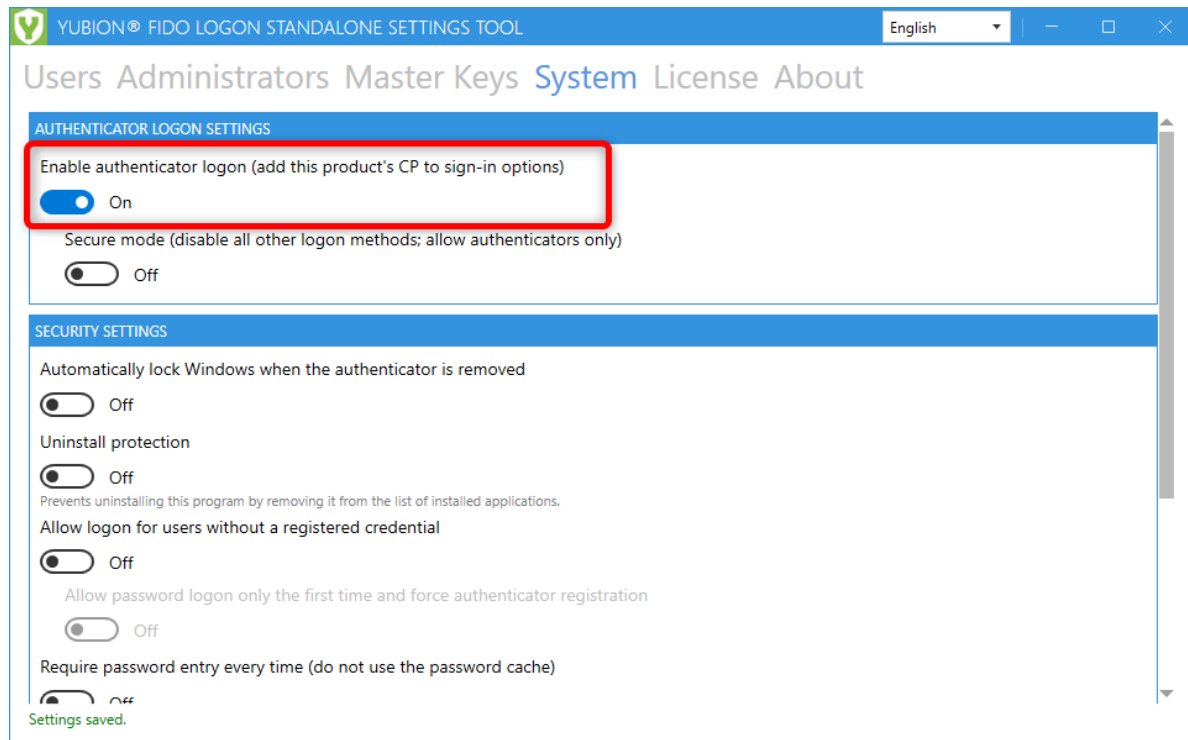


Figure: The Enable authenticator logon setting

The FIDO logon tile now appears on the Windows sign-in screen.

- **It cannot be turned on while no authenticator usable for signing in exists** (this is not an issue if STEP 3 and STEP 4 are done).
- If every registered authenticator and master key is deleted so that none remain, this setting automatically turns itself off again.

For details, see Chapter 7 "Basic Settings" of the Administrator Manual.

STEP 7: Try Signing In

Sign in for real to confirm that the settings took effect. Sign out of Windows (or lock it).

1. On the sign-in screen, select this product's **FIDO logon tile**.

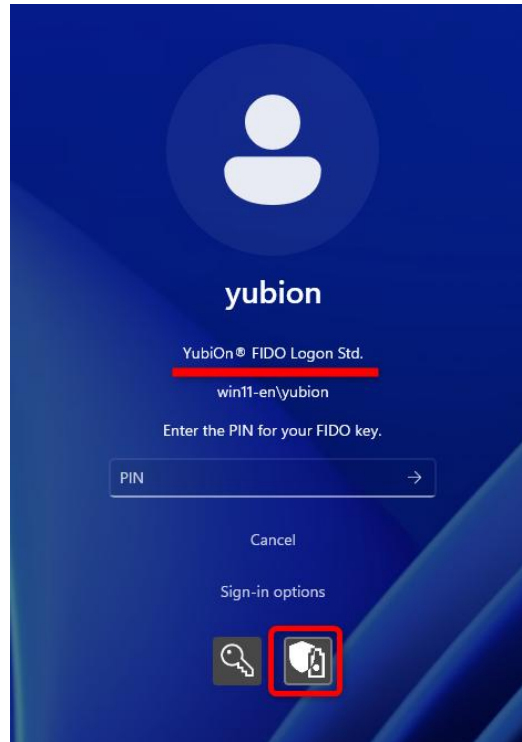


Figure: Selecting the FIDO logon tile

2. Connect the authenticator and enter the **PIN**.

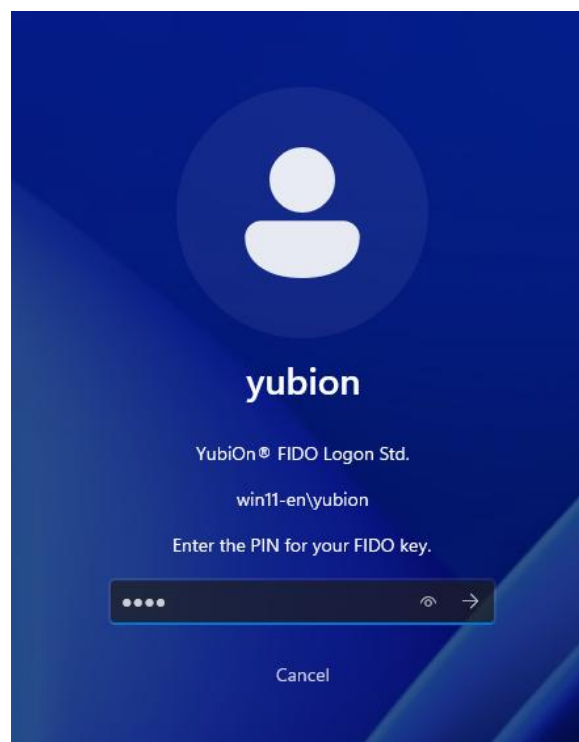


Figure: Entering the PIN

3. Touch the authenticator.

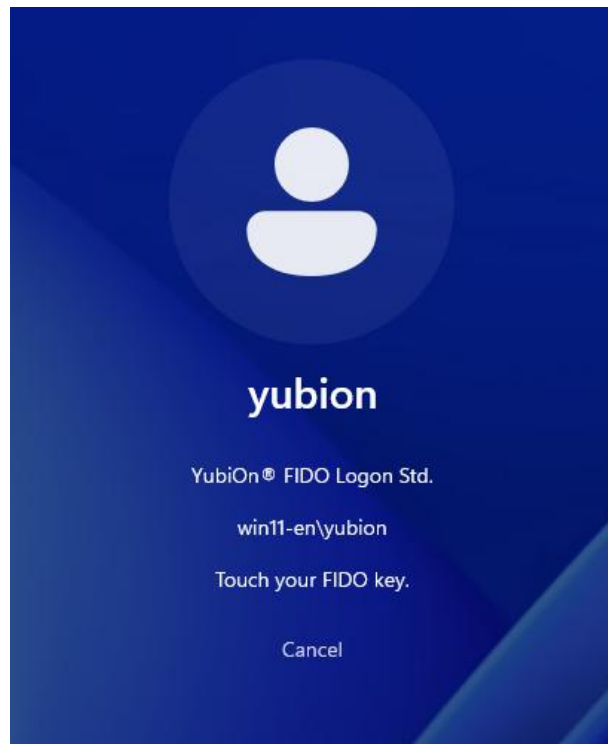


Figure: Prompt to touch the authenticator

4. **The first time only**, you are asked for your Windows password. Enter it to complete the sign-in.

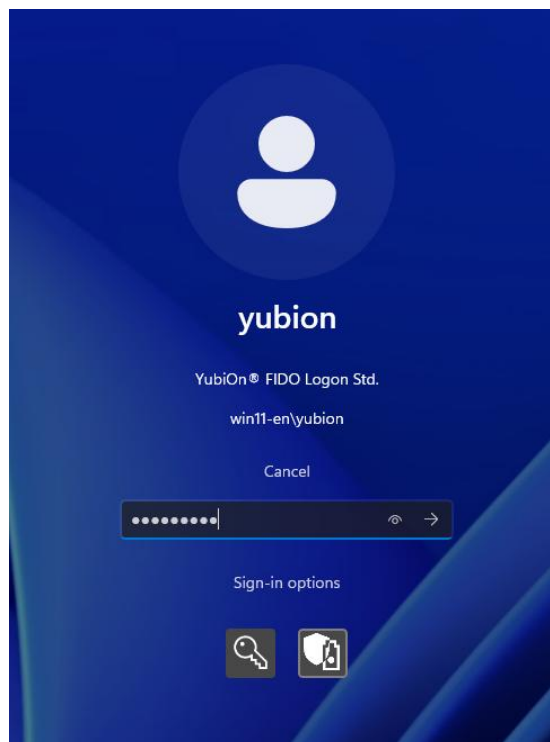


Figure: Entering the Windows password

The password you enter is stored encrypted on the computer, so **from the second time on you can sign in with just the PIN and a touch.**

At this point, password-only sign-in is still possible. To forbid signing in without an authenticator, go on to STEP 8.

The user-facing sign-in procedure is described in the separate **End User Guide.**

STEP 8: Enable Secure Mode

Turning on **secure mode** disables all other sign-in methods (such as passwords) and **restricts sign-in to authenticators only**. Turn it on when you move to production use.

Warning Once secure mode is on, **users without a registered authenticator can no longer sign in with a password**. Before turning it on, make sure all of the following are true.

- **Every user of that computer has an authenticator registered** (STEP 4)
- **A master key is registered** (STEP 3)
- **Recovery codes have been issued and stored safely** (STEP 5)

1. Open the **System** tab.
2. Turn on **Secure mode (disable all other logon methods; allow authenticators only)**.

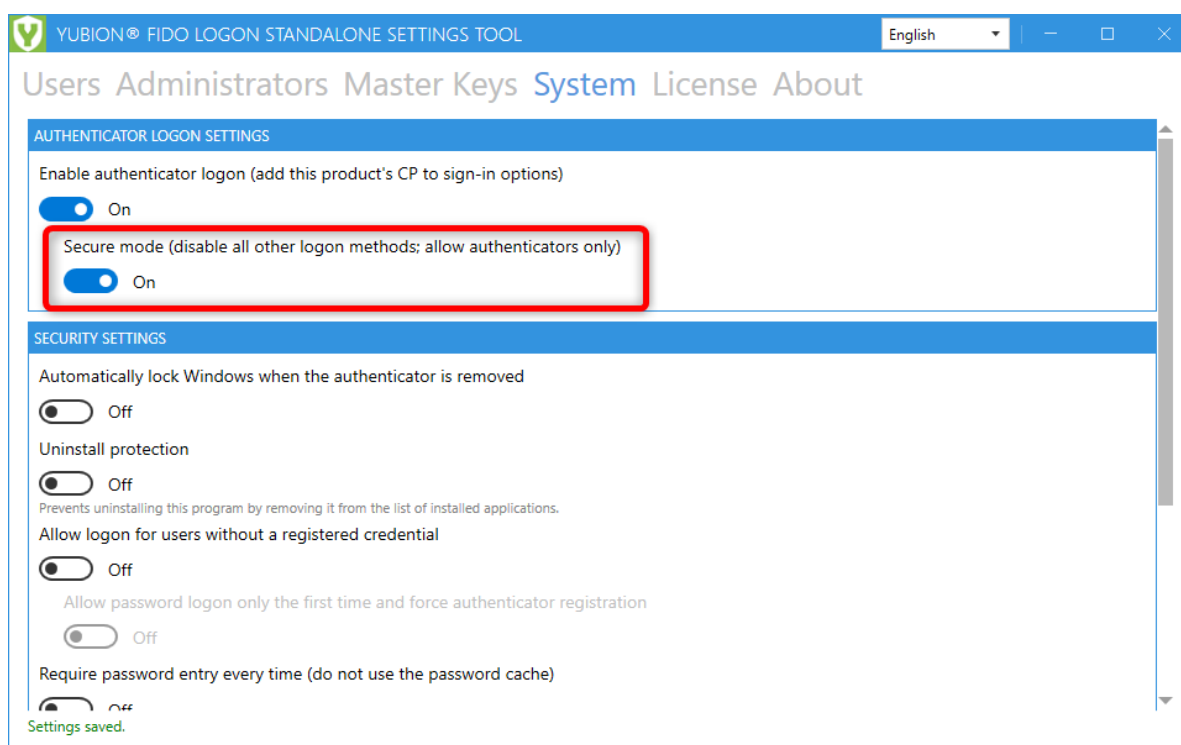


Figure: The Secure mode setting

3. Sign out and confirm that no tile other than FIDO logon appears on the sign-in screen.
- **Enable authenticator logon** (STEP 6) is a prerequisite for turning this on.
 - **Secure mode is not required for signing in over RDP**. However, when it is off, password logon remains available over RDP as well, so turn it on if you want FIDO authentication to be mandatory over RDP too.

For details, see Chapter 7 "Basic Settings" of the Administrator Manual. For preparations in case every authenticator becomes PIN-locked, also see Chapter 8 "Preparing for Authenticator Lockout Caused by Wrong PIN Entry".

If Something Goes Wrong

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

Check the following in order.

1. Is the license status **Valid** (STEP 2)? If it is not, the tile is not shown.
2. Is **Enable authenticator logon** turned on (STEP 6)?
3. Is an authenticator registered for the target user (STEP 4)?

An Authenticator Cannot Be Registered (Assigned) in the Settings Tool

1. **Is Windows "Passkey access" turned off?** If **Passkey access** under **Settings** → **Privacy & security** → **Passkeys** is **off**, authenticators and master keys cannot be registered. Turn it **on** and try again (this item exists only in relatively recent versions of Windows 11).
2. **Is the target user shown in the list?** Only accounts with an existing profile are listed (STEP 4).
3. **Does the authenticator support FIDO2?** U2F (CTAP1) only keys cannot be registered by default.

The License Shows "Machine Mismatch" or "OS Edition Mismatch"

- Check whether you have registered a license file issued for another computer, or one for a different OS type (server / client).
- **On a computer whose chassis or motherboard has been replaced**, the machine code changes and the existing license cannot be used. Request a re-issue with the new machine code. Note that **reinstalling the OS does not change the machine code**.

An Authenticator Was Lost, or the PIN Was Forgotten or Locked

- Tell the user to sign in for an emergency with a **recovery code** (STEP 5). The Windows password is required as well.
- The administrator can sign in on the user's behalf with a **master key** (STEP 3).
- Delete the lost authenticator from the **Users** tab of the settings tool.

For anything not covered here, see Chapter 13 "Troubleshooting" of the Administrator Manual.

What to Read Next

Features and operations not covered here are described in the following chapters of the Administrator Manual.

What you want to know	Where to look (Administrator Manual)
Requirements for signing in over RDP	Chapter 2 System Requirements and Operating Environment
Renewing the license and applying it to many computers at once	Chapter 5 Registering the License
Requiring FIDO authentication to launch the settings tool	Chapter 6 Launch Authentication for the Settings Tool (Optional)
Behavior settings such as auto-lock on authenticator removal and uninstall protection	Chapter 7 Basic Settings
Letting users register their own authenticator (self-registration)	Chapter 8 Registering and Managing User Authenticators
Preparing for authenticator PIN lockout	Chapter 8 Registering and Managing User Authenticators
Transferring settings and credentials to another computer (export / import)	Chapter 11 Transferring Settings and Credentials
Checking the event log and collecting support information	Chapter 12 Operation and Maintenance
List of settings and list of event IDs	Appendix B / Appendix C

Distribute the separate **End User Guide** for user-facing instructions.

Contact

For inquiries about installing, configuring, or operating this product, contact the **reseller** you purchased it from, or the **YubiOn Support Desk (SOFTGIKEN Co., Ltd.)**.